

プ

11.1

PAN-OS Web インターフェイスのヘル

docs.paloaltonetworks.com

Contact Information

Corporate Headquarters: Palo Alto Networks 3000 Tannery Way Santa Clara, CA 95054 www.paloaltonetworks.com/company/contact-support

About the Documentation

- For the most recent version of this guide or for access to related documentation, visit the Technical Documentation portal docs.paloaltonetworks.com.
- To search for a specific topic, go to our search page docs.paloaltonetworks.com/search.html.
- Have feedback or questions for us? Leave a comment on any page in the portal, or write to us at documentation@paloaltonetworks.com.

Copyright

Palo Alto Networks, Inc. www.paloaltonetworks.com

© 2023-2023 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.

Last Revised

July 10, 2023

Table of Contents

Web インターフェイスの基本	21
ファイアウォールの概要	22
機能と利点	23
前回のログイン時間およびログイン試行回数	25
当日のメッセージ	26
タスク マネージャ	27
言語	
アラーム	31
変更のコミット	
候補設定の保存	
変更を元に戻す	42
設定のロック	47
Global Find	
脅威詳細	50
AutoFocus インテリジェンス サマリー	53
設定テーブルのエクスポート	56
ブートモードの変更	58
ダッシュボード	61
Dashboard Widgets(ダッシュボード ウィジット)	62
ΔCC	65
ACC の両面辺合	
ACC のタゴ	
ACC のウィジェット	07
ACC のアクション	
ACC のアクショントの加田	73 72
テノねよし ワインツ下の処理	73 74
ノイルスの処理 - ローカル ノイルスわよびクローバル ノイルス	/4
監視	77
Monitor > Logs [監視 > ログ]	78
ログ タイプ	78
ログ アクション	
Monitor(監視) > External Logs(外部ログ)	90
Monitor(監視) > Automated Correlation Engine(自動相関エンジン)	92
[Monitor] > [自動相関エンジン] > [相関オブジェクト]	92
[Monitor] > [自動相関エンジン] > [相関されたイベント]	93

	Monitor > Packet Capture [監視 > パケット キャプチャ]	
	パケット キャプチャの概要	97
	カスタム パケット キャプチャの構成要素	97
	脅威パケット キャプチャの有効化	101
	Monitor > App Scope [監視 > アプリケーション スコープ]	103
	アプリケーション スコープの概要	103
	アプリケーション スコープのサマリー レポート	104
	アプリケーション スコープの変化モニター レポート	105
	アプリケーション スコープの脅威モニター レポート	107
	アプリケーション スコープの脅威マップ レポート	109
	アプリケーション スコープのネットワーク モニター レポート	110
	アプリケーション スコープのトラフィック マップ レポート	112
	Monitor > Session Browser [監視 > セッション ブラウザ]	114
	Monitor(監視) > Block IP List(ブロック IP リスト)	115
	ブロック IP リスト エントリ	115
	ブロック IP リスト エントリの表示または削除	116
	Monitor > Botnet [監視 > ボットネット]	118
	ボットネット レポートの設定	118
	ボットネットの設定	119
	モニター > loTデバイス	121
	IoT Devices (IoT デバイス) > Summary (概要)	121
	loTデバイス> アセットインベントリ	122
	Monitor(監視) > PDF Reports(PDF レポート)	124
	Monitor > PDF Reports > Manage PDF Summary {監視 > PDF レポート サマリーの管理]	> PDF 124
	Monitor > PDF Reports > User Activity Report [監視 > PDFレポート > 3 ザー アクティビティ レポート]	ユー 126
	Monitor > PDF Reports > SaaS Application Usage [監視 > PDFレポート Saasアプリケーションの使用状況]	> 128
	Monitor > PDF Reports > Report Groups [監視 > PDF レポート > レポー ループ]	ート グ 131
	Monitor > PDF Reports > Email Scheduler [監視 > PDF レポート > 電子 スケジューラ]	メール
	Monitor > Manage Custom Reports [監視 > カスタム レポートの管理]	133
	Monitor > Reports [監視 > レポート]	135
ポリ	シー	137
	ポリシーのタイプ	138
	ポリシールールの移動またはコピー	140
	監査コメント アーカイブ	141

監査コメント	141
設定ログ (コミット間)	141
ルール変更	142
ルールの使用状況ヒット数のクエリ	143
ルール ヒット数クエリのデバイス ルールの使用状況	144
Policies > Security [ポリシー > セキュリティ]	146
セキュリティポリシーの概要	146
セキュリティ ポリシー ルールの構成要素	147
ポリシーの作成と管理	162
セキュリティ ポリシー ルールのオーバーライドまたは取り消し	166
アプリケーションおよび使用状況	
セキュリティポリシー オプティマイザー	
Policies > NAT [ポリシー > NAT]	180
NAT ポリシーの General(全般)タブ	180
NAT の Original Packet(元のパケット)タブ	181
NAT の Translated Packet(変換済みパケット)タブ	
NAT の Active/Active HA Binding(アクティブ/アクティブ HA バイ	ンド)タ
ブ	187
NAT Target(宛先)タブ	
Policies > QoS [ポリシー > QoS]	
Policies > Policy Based Forwarding [ポリシー > ポリシー ベース フォワーテ	⁵ イン 105
ク」 ポリシューベーフフェトローゴノングの Compared (今年) カゴ	195
ホリシー ベース フォワーティングの General (主般) タブ	195
ホリシー ベース フォリーティングの Source (送信儿) タノ	170 。 <i>(</i> /运
ホリシーベース フォワーティングの Destination/Application/Servic 牛/アプリケーション/サービス)タブ	e(列) 198
ポリシー ベース フォワーディングの Forwarding(転送)タブ	
ポリシー ベース フォワーディングの Target (宛先) タブ	
Policies > Decryption 「ポリシー > 復号化]	
復号化の General (全般) タブ	202
復号化の Source(送信元)タブ	203
復号化の Destination(宛先)タブ	205
復号化の Service/URL Category(サービス/URL カテゴリ)タブ	205
復号化の Options(オプション)タブ	206
Decryption Target Tab(復号宛先タブ)	
ポリシー>ネットワーク パケット ブローカー	210
[ネットワーク パケット ブローカ全般] タブ	210
[ネットワーク パケット ブローカ ソース] タブ	211
[ネットワーク パケット ブローカ宛先] タブ	

ネットワーク パケット ブローカ アプリケーション/サービス/トラフィッ	ク
テノー・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	213
$(\pi) + (\gamma + \gamma + $	21J ⊞
ホットン シンパンシーシロ 20 ホッシー オンノイ (イック ルレルロ)及, 法	215
Policies(ポリシー) > Tunnel Inspection(トンネル検査)	217
トンネル検査ポリシーの構成要素	217
Policies > Application Override [ポリシー > アプリケーション オーバーライ ド1	225
アプリケーション オーバーライドの General(全般)タブ	226
アプリケーション オーバーライドの Source(送信元)タブ	227
アプリケーション オーバーライドの Destination(宛先)タブ	227
アプリケーション オーバーライドの Protocol/Application(プロトコル/フ	フプ
リケーション)タブ	228
Application Override Target Tab(アプリケーション オーバーライド宛先 ブ)	タ 229
Policies (ポリシー) > Authentication (認証)	230
認証ポリシー ルールの構成要素	230
認証ポリシーの作成と管理	237
Policies > DoS Protection [ポリシー > DoS プロテクション]	240
DoS プロテクションの General(全般)タブ	240
DoS プロテクションの Source(送信元)タブ	241
DoS プロテクションの Destination(宛先)タブ	243
DoS プロテクションの Option/Protection(オプション/防御)タブ	243
DoS Protection Target Tab [DoS プロテクション宛先タブ]	246
Policies > SD-WAN [ポリシー > SD-WAN]	248
SD-WAN General (全般) タブ	248
Source (送信元) タブ	249
Destination (宛先) タブ	250
SD-WAN Application/Service (アプリケーション/サービス) タブ	251
SD-WAN Path Selection (パス選択) タブ	253
SD-WAN Target (ターゲット) タブ	253
Objects	55
オブジェクトの移動、コピー、オーバーライド、取り消し	256
オブジェクトの移動またはコピー	256
オブジェクトのオーバーライド/取り消し	257
Objects > Addresses [オブジェクト > アドレス]	258
Objects > Address Groups [オブジェクト > アドレス グループ]	261
Objects > Regions [オブジェクト > 地域]	264

Objects > Dynamic User Groups [オブジェクト > 動的ユーザー グループ]20	65
Objects > Applications [オブジェクト > アプリケーション]20	67
アプリケーションの概要20	67
アプリケーションでサポートされる操作2	72
アプリケーションの定義2	76
Objects > Application Groups [オブジェクト > アプリケーション グループ]2	82
Objects > Application Filters [オブジェクト > アプリケーションフィルタ]28	83
Objects > Services [オブジェクト > サービス]28	85
Objects(オブジェクト) > Service Groups(サービス グループ)	88
Objects > Tags [オブジェクト > タグ]28	89
タグの作成	90
ルールベースをグループとして表示29	91
タグの管理29	95
Objects > Devices [オブジェクト > デバイス]29	98
Objects > External Dynamic Lists [オブジェクト > 外部動的リスト]	00
Objects(オブジェクト) > Custom Objects(カスタム オブジェクト)	07
Objects > Custom Objects > Data Patterns [オブジェクト > カスタム オブ ジェクト > データ パターン]	07
Objects(オブジェクト) > Custom Objects(カスタム オブジェクト) >	
Spyware/Vulnerability(スパイウェア/脆弱性)3	14
Objects > Custom Objects > URL Category [オブジェクト > カスタム オブジェク] > URL カテゴリ]	ト 19
Objects(オブジェクト) > Security Profiles(セキュリティ プロファイル)3	22
セキュリティ プロファイルのアクション3:	23
Objects > Security Profiles > Antivirus [オブジェクト > セキュリティ プロファイ) > アンチウイルス]	ル 28
Objects(オブジェクト) > Security Profiles(セキュリティ プロファイル) >	
Anti-Spyware Profile (アンチスパイウェア プロファイル)	32
Objects > Security Profiles > Vulnerability Protection [オブジェクト > セキュリテ	イ
ノロノアイル > 肥弱性防御]	41
Objects > Security Profiles > URL Filtering [オノンェクト > セキュリティ ノロノデ イル > URL フィルタリング]	48
URI フィルタリングの一般設定	49
URL フィルタリング カテゴリ 34	49
URL フィルタリング設定 3^{3}	53
ユーザー証明書検出 3	54
HTTP ヘッダの挿入	56
インライン分類	58
Objects > Security Profiles > File Blocking オブジェクト > セキュリティ プロファ	,
$4\mu > 7r4\mu$ $7\mu = 774\mu$	60

	Objects > Security Profiles > WildFire Analysis [オブジェクト > セキュリティ プロファイル > WildFire 分析]	1 63
	Objects > Security Profiles > Data Filtering [オブジェクト > セキュリティ プロフ イル > データ フィルタリング]	7 66
	Objects > Security Profiles > DoS Protection [オブジェクト > セキュリティ プロ ファイル > DoS プロテクション]3	68
	Objects > Security Profiles > Mobile Network Protection [オブジェクト > セキュリティプロファイル > モバイル ネットワーク プロテクション]) 73
	Objects(オブジェクト) > Security Profiles(セキュリティ プロファイル) > SCTP Protection(SCTP プロテクション)	83
	Objects > Security Profile Groups [オブジェクト > セキュリティ プロファイル グ ループ]	91
	Objects > Log Forwarding [オブジェクト > ログ転送]	93 98
	Objects > Decryption Profile [オブジェクト > 復号化プロファイル]	01
	復号化プロファイルの一般設定	01
	Settings to Control Decrypted Traffic(復号化されたトラフィックを制御す 設定)4	る 03
	復号化されていないトラフィックを制御するための設定4	11
	復号化された SSH トラフィックを制御するための設定4	12
	オブジェクト>パケット ブローカ プロファイル	14
	Objects > SD-WAN Link Management [オブジェクト > SD-WAN リンク管理]4	19
	Objects > SD-WAN Link Management > Path Quality Profile [オブジェクト SD-WAN リンク管理 > パス品質プロファイル]4	> 19
	Objects > SD-WAN Link Management > SaaS Quality Profile [オブジェクト SD-WAN リンク管理 > SaaS 品質プロファイル]4	> 20
	Objects > SD-WAN Link Management > Traffic Distribution Profile [オブジ クト > SD-WAN リンク管理 > トラフィック分散プロファイル]4	т 22
	Objects > SD-WAN Link Management > Error Correction Profile [オブジェク ト > SD-WAN リンク管理 > エラー修正プロファイル]4	ל 23
	Objects > Schedules [オブジェクト > スケジュール]	26
ネッ	トワーク4	29
	[Network] > [インターフェイス]	30
	ファイアウォール インターフェイスの概要4	31
	ファイアウォール インターフェイスの共通の構成要素4	31
	PA-7000 シリーズのファイアウォール インターフェイスの共通の構成要素	ე ⊿
	ボー・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	৩4 २८
	$\gamma \gamma $	32
	$\vec{N} - \vec{F} = \vec{V} - \vec{F} + \vec{V} - \vec{F} + $	37

バーチャル ワイヤー サブインターフェイス439	9
PA-7000 シリーズのレイヤー 2 インターフェイス440	C
PA-7000 シリーズのレイヤー 2 サブインターフェイス	2
PA-7000 シリーズのレイヤー 3 インターフェイス443	3
レイヤー 3 インターフェイス458	З
レイヤー 3 サブインターフェイス482	2
Log Card Interface(ログ カード インターフェイス)506	5
ログ カード サブインターフェイス	7
復号化ミラー インターフェイス508	З
Ethernet の集約(AE)インターフェイス グループ509	9
Ethernet の集約(AE)インターフェイス518	З
Network > Interfaces > VLAN [ネットワーク > インターフェイス > VLAN]531	1
Network > Interfaces > Loopback [ネットワーク > インターフェイス > ループバッ	
ク]	9
Network > Interfaces > Tunnel [ネットワーク > インターフェイス > トンネ	
<i>IV</i>]	2
Network > Interfaces > SD-WAN $[x y \land y$	5
$\forall VLAN$	נ ד
xyyyzyzyzyzyzyzyzyzyzyzyzyzyzyzyzyzyzyz	' ^
$\frac{1}{2} = \frac{1}{2} = \frac{1}$	ر ۸
$A = \int \nabla \nabla$	+
Network > Zolles $[xyyy - y > y - y]$	5
セイュリティ ノーンの概要	5
セキュリティ ノーンの構成安然	2
Network > VLANS $[\pi y + y - y > VLAN]$.	ך 1
Network > Virtual Wires [ネットワーク > ハーナヤル ワイヤー]	T T
Network > Virtual Routers [ネットワーク > 仮想ルーター]	3
仮想ルーターの一般設定573	3 1
一 一 前 り ル ー ト … … 572 572 572	4
ルート冉配信	1
CSDE 59/	۲ ۲
OSPE//3ID//6 590	+ 1
BGP 598	2 R
DOI 10 フルチキャスト 614	6
FCMP 421	ך 1
仮相ルーターの詳細ランタイム状能 42/	4
More Runtime Stats for a Logical Router (論理ルーターの詳細ランタイ)な	r
計情報)	7

Network (ネットワーク) > Routing (ルーティング) > Logical Routers (論理 ルーター)
Network(ネットワーク) > Routing(ルーティング) > Logical Routers(論 理 ルーター) > General(一般)645
Network > Routing > Logical Routers > Static [ネットワーク > ルーティング > 論理ルーター > スタティック]649
Network > Routing > Logical Routers > OSPF OSPF [の論理ルータ>ネット ワーク>ルーティング]653
Network > Routing > Logical Routers > OSPFv3 [OSPFv3 >の論理ルー ター>ネットワーク>ルーティング]658
Network > Routing > Logical Routers > RIPv2 [論理ルーター>ネットワー ク>ルーティング > RIPv2]
Network > Routing > Logical Routers > BGP [ネットワーク>ルーティング > 論理ルータ> BGP]666
Network > Routing > Logical Routers > Multicast [ネットワーク> ルーティン グ > 論理ルーター> マルチキャスト]
Network > Routing > Routing Profiles ネットワーク>ルーティング>ルーティングプ ロファイル
Network(ネットワーク) > Routing(ルーティング) > Routing Profiles(ルーティング プロファイル) > BGP681
Network > Routing > Routing Profiles > BFD [ネットワーク>ルーティング > ルーティング プロファイル > BFD]
Network > Routing > Routing Profiles > OSPF [ネットワーク>ルーティング > OSPF >ルーティング プロファイル]
Network > Routing > Routing Profiles > OSPFv3 [ネットワーク>ルーティング > OSPFv3 >ルーティング プロファイル]
Network > Routing > Routing Profiles > RIPv2 [ネットワーク>ルーティン グ>ルーティングプロファイル > RIPv2]
Network > Routing > Routing Profiles > Filters [ネットワーク>ルーティン グ>ルーティングプロファイル>フィルタ]
Network > Routing > Routing Profiles > Multicast [ネットワーク>ルーティン グ > マルチキャスト>ルーティングプロファイル]
Network > IPSec Tunnels [ネットワーク > IPSec トンネル]
IPSec VPN トンネル管理718
IPSec トンネルの [全般] タブ719
IPSec トンネルの Proxy IDs(プロキシ ID)タブ
ファイアウォールの IPSec トンネル状態724
IPSec トンネルの再起動または更新725
Network (ネットワーク) > GRE Tunnels (GRE トンネル)
GRE トンネル726
Network > DHCP [ネットワーク > DHCP]729

DHCP の概要729
DHCP アドレス730
DHCP サーバー
DHCP リレー735
DHCP クライアント735
Network > DNS Proxy [ネットワーク > DNS プロキシ]737
DNS プロキシの概要737
DNS プロキシ設定738
その他の DNS プロキシ アクション741
ネットワーク > プロキシ
Network > QoS [ネットワーク > QoS]746
QoS インターフェイス設定746
QoS インターフェイスの統計情報749
Network > LLDP [ネットワーク > LLDP]751
LLDP の概要
LLDP の構成要素751
Network(ネットワーク) > Network Profiles(ネットワーク プロファイ
ル)
Network > Network Profiles > GlobalProtect IPSec Crypto [ネットワーク > ネットワーク プロファイル]> GlobalProtect の IPSec 暗号]
Network > Network Profiles > IKE Gateways [ネットワーク > ネットワーク プロファイル > IKE ゲートウェイ]756
Network > Network Profiles > IPSec Crypto [ネットワーク > ネットワーク プ ロファイル > IPSec 暗号]768
Network > Network Profiles > IKE Crypto [ネットワーク > ネットワーク プロ ファイル > IKE 暗号]769
Network > Network Profiles > Monitor [ネットワーク > ネットワーク プロ ファイル > 監視]
Network > Network Profiles > Interface Mgmt [ネットワーク > ネットワーク プロファイル > インターフェイス管理]
Network > Network Profiles > Zone Protection [ネットワーク > ネットワーク プロファイル > ゾーンプロテクション]
Network(ネットワーク) > Network Profiles(ネットワーク プロファイ ル) > QoS
Network > Network Profiles > LLDP Profile [ネットワーク > ネットワーク プロファイル > LLDP プロファイル]804
Network > Network Profiles > BFD Profile [ネットワーク > ネットワークプロ ファイル > BFDプロファイル]
Network > Network Profiles > SD-WAN [ネットワーク > ネットワーク プロ ファイル > SD-WAN インターフェイス プロファイル]
ネットワーク > ネットワークプロファイル > MACsecプロファイル813

デバイス	15
Device(デバイス)> Setup(セットアップ)	317
Device > Setup > Management [デバイス > セットアップ > 管理]	318
Device > Setup > Operations [デバイス > セットアップ > 操作]	358
SNMP モニタリングの有効化	367
Device > Setup > HSM [デバイス > セットアップ > HSM]	371
ハードウェア セキュリティ モジュール プロバイダ設定	371
HSM 認証	372
ハードウェア セキュリティ操作	373
ハードウェア セキュリティ モジュール プロバイダ設定および状態	374
ハードウェア セキュリティ モジュール状態	375
Device > Setup > Services [デバイス > セットアップ > サービス]	377
グローバルおよび仮想システムのサービスの設定	377
グローバル サービス設定	378
サービス ルートの設定での IPv4 および IPv6 のサポート	381
宛先サービス ルート	385
Device(デバイス) > Setup(セットアップ) > Interfaces(インターフェイ ス)	287
Device $(\forall \forall \forall A \land \forall) > \text{Setun} (\forall \forall \forall \forall P \lor \forall) > \text{Telemetry} (\forall \forall \forall \forall \forall \forall)$	202
Device > Setup > Content-ID $[\vec{\tau}/\vec{T} X > T = T = T = T = T = T$	394
Device > Setup > WildFire $[\overline{\gamma}/\sqrt{\lambda} > \overline{\gamma}/\sqrt{\lambda} > WildFire]$	206
Device > Setup > Session [\vec{r} / \vec{A} > \vec{r}	200 213
セッション設定 () () () () () () () () () () () () ()	÷-0
ヤッション タイムアウト	÷19
TCP 設定	+ <u>-</u> ,
復号化設定:証明書取り消しチェック	726
復号化設定:フォワード プロキシ サーバーの証明書設定	727
復号化設定:SSL復号化設定	28
VPN セッション設定	729
デバイス >セットアップ >ACE	230
Device(デバイス) > Setup(セットアップ) > DLP) 31
Device > High Availability [デバイス > 高可用性]	233
HA 設定時の重要事項) 34
HA 一般設定	<i>3</i> 4
HA 通信	<i>2</i> 40
HA リンクおよびパス モニタリング	<i>4</i> 5
HA Active/Active Config(HA アクティブ/アクティブ 設定)) 49
Cluster Config (クラスタ設定)) 52

Device (デバイス) > Log Forwarding Card (ログ転送カード)	<i>•</i> 54
Device > Config Audit [デバイス > 設定監査]9	, 57
[Device] > [パスワード プロファイル]9	<i>9</i> 60
ユーザー名とパスワードの要件9	<i></i> 761
Device > Administrators [デバイス > 管理者]9	<i>9</i> 63
Device > Admin Roles [デバイス > 管理者ロール]	<i>9</i> 67
Device > Access Domain [デバイス > アクセス ドメイン]9	<i>7</i> 0
Device > Authentication Profile [デバイス > 認証プロファイル]9	71
認証プロファイル9	71
SAML Metadata Export from an Authentication Profile(認証プロファイル ら SAML メタデータをエクスポートする)9	か 981
Device > Authentication Sequence [デバイス > 認証シーケンス]) 84
Device (デバイス) > IoT Security (IoTセキュリティ) > DHCP Server Log Ingestion (DHCPサーバーのログ取り込み)9	986
Device > Data Redistribution [デバイス > データの再配信]9) 89
Device > Data Redistribution > Agents [デバイス > データの再配信 > エー	
ジェント]9	989
Device > Data Redistribution > Clients [デバイス > データの再配信 > クラ- アント]9	√ 991
Device > Data Redistribution > Collector Settings [デバイス > データの再配 > コレクタ 設定]9]信)91
Device > Data Redistribution > Include/Exclude Networks [デバイス > デーの再配信 > 包含/除外ネットワーク]9	·タ 792
Device > Device Quarantine [デバイス > デバイス隔離]9	93
Device > VM Information Sources [デバイス > VM 情報の送信元]9	95
VMware ESXi サーバーおよび vCenter サーバーの VM 情報ソースを有効は するための設定9	⊆ }97
AWS VPC の VM 情報ソースを有効にするための設定9	999
Google Compute Engine の VM 情報ソースを有効にするための設定10)00
Device (デバイス) > Troubleshooting (トラブルシューティング)10)03
Security Policy Match セキュリティポリシー マッチ)03
QoS ポリシー マッチ10)05
Authentication Policy Match 認証ポリシー マッチチョン 10)07
復号化/SSL ポリシー マッチ10	908
NAT ポリシー マッチ10)09
ポリシー ベース フォワーディング ポリシー マッチ)11
DoS ポリシー マッチ10)13
routing1C)14
Wildfire をテスト1C)15
Threat Vault10)16

ping	1017
トレース ルート	1019
ログコレクタの接続性	1021
外部ダイナミック リスト	1022
更新サーバー	1023
クラウド ロギングサービスのステータスをテスト	1023
クラウド GP サービスのステータスをテスト	1024
Device > Virtual Systems [デバイス > 仮想システム]	1026
Device > Shared Gateways [デバイス > 共有ゲートウェイ]	1030
Device (デバイス) > Certificate Management (証明書の管理)	1031
Device > Certificate Management > Certificates [デバイス > 証明書の管理 > 証 書]	明 1032
ファイアウォールおよび Panorama 証明書の管理	1032
信頼できる既定証明機関の管理	1039
Device > Certificate Management > Certificate Profile [デバイス > 証明書の管理	目>
証明書プロファイル]	1041
Device > Certificate Management > OCSP Responder [デバイス > 証明書の管理 OCSP レスポンダ]	! > 1044
Device > Certificate Management > SSL/TLS Service Profile [デバイス > 証明書 理 > SSL/TLS サービス プロファイル]	の管 1046
Device > Certificate Management > SCEP [デバイス > 証明書の管理 > SCEP]?	1048
Device (デバイス) > Certificate Management (証明書の管理) > SSL Decryp Exclusion (SSL 復号化例外)	tion 1052
Device (デバイス) > Certificate Management (証明書の管理) > SSH Service Profile (SSH サービス プロファイル)	e 1055
Device > Response Pages [デバイス > 応答ページ]	1057
Device > Log Settings [デバイス > ログ設定]	1061
ログの転送先の選択	1061
アラーム設定の定義	1065
ログのクリア	1067
[Device] > [サーバー プロファイル]	1068
Device > Server Profiles > SNMP Trap [デバイス > サーバー プロファイル > SN トラップ]	IMP 1069
Device > Server Profiles > Syslog [デバイス > サーバー プロファイル > Syslog]	1072
Device > Server Profiles > Email [デバイス > サーバー プロファイル > 電子メー	
ル]	1074
Device (デバイス) > Server Profiles (サーバー プロファイル) > HTTP	1077
Device (デバイス) > Server Profiles (サーバー プロファイル) > NetFlow:	1081

Device > Server Profiles > RADIUS [デバイス > サーバー プロファイル > RADIUS]10	083
[Device (デバイス)] > [Server Profiles (サーバープロファイル)] > SCP10	086
Device > Server Profiles > TACACS+ [デバイス > サーバー プロファイル > TACA +]10	۸CS 087
Device > Server Profiles > LDAP [デバイス > サーバー プロファイル > LDAP] 10	189
Device > Server Profiles > Kerberos [デバイス > サーバー プロファイル > Kerberos]10	092
Device(デバイス) > Server Profiles(サーバー プロファイル) > SAML Identi Provider(SAML アイデンティティ プロバイダ)	ty 094
Device > Server Profiles > DNS [デバイス > サーバー プロファイル > DNS] 10	099
Device(デバイス) > Server Profiles(サーバー プロファイル) > Multi Factor Authentication(多要素認証)1	101
Device > Local User Database > Users [デバイス > ローカル ユーザー データベー > ユーザー]1	-ス 104
Device > Local User Database > User Groups [デバイス > ローカル ユーザー デ- ベース > ユーザー グループ]1	-タ 106
Device > Scheduled Log Export [デバイス > スケジュール設定されたログのエク ポート]1	ス 107
Device > Software [デバイス > ソフトウェア]1	109
Device > Dynamic Updates [デバイス > 動的更新]1	112
Device > Licenses [デバイス > ライセンス]1	117
Device > Support [デバイス > サポート]1	119
Device > Master Key and Diagnostics [デバイス > マスター キーおよび診断]1	121
マスターキーのデプロイ1	124
loT >デバイス>ポリシーの推奨事項1	126
デバイス > ポリシー>推奨 SaaS1	130
デバイス>ポリシー推奨>loTまたはSaaS>ポリシールールのインポート1	132
ユーザー ID11	.33
Device > User Identification > User Mapping [デバイス > User-ID > ユーザーマッ ング]1	, ピ 134
Palo Alto Networks User-IDエージェントの設定	134
サーバーの監視1	144
ユーザー マッピングのサブネットワークの許可または除外1	147
Device(デバイス) > User Identification(User-ID) > Connection Security(接 のセキュリティ)1	続 150
Device (デバイス) > User Identification (ユーザーID) > Terminal Server Agents (タ ミナル サーバー エージェント)1	، <u> </u>
Device > User Identification > Group Mapping Settings [デバイス > User-ID > グ ループマッピングの設定]1	153

デバイス>ユーザーの識別>信頼できる送信元アドレス	1159
Device(デバイス) > User Identification(ユーザー ID) > Authentication Po	rtal
Settings (認証ポータルの設定)	1160
デバイス > ユーザー識別 > クラウド ID エンジン	.1164
GlobalProtect	L 167
Network > GlobalProtect > Portals [ネットワーク > GlobalProtect > ポータ	
ル]	1168
GlobalProtect ポータルの General(全般)タブ	.1169
GlobalProtect ポータルの Authentication Configuration(認証設定)タ ブ	.1172
GlobalProtect ポータルの Portal Agent Data Collection(ポータル デー: 集)タブ	タ収 1175
GlobalProtect ポータルの Agent (エージェント) タブ	.1175
GlobalProtect ポータルの Clientless VPN (クライアントレス VPN) タブ	1214
GlobalProtect ポータルの Satellite (サテライト) タブ	1219
Network > GlobalProtect > Gateways [ネットワーク > GlobalProtect > ゲート イ1	ウェ 1223
「JGlobalProtect ゲートウェイの General(全般)タブ	1223
GlobalProtect ゲートウェイの Authentication (認証) タブ	1225
GlobalProtect ゲートウェイの Agent (エージェント) タブ	.1227
GlobalProtect ゲートウェイの Satellite (サテライト) タブ	1244
Network > GlobalProtect > MDM [ネットワーク > GlobalProtect > MDM]	.1248
Network(ネットワーク) > GlobalProtect > Clientless Apps(クライアントレ	バス
アプリケーション)	.1250
Network(ネットワーク) > GlobalProtect > Clientless App Groups(クライフ レス アプリケーション グループ)	ント 1252
Objects > GlobalProtect > HIP Objects [オブジェクト > GlobalProtect > HIP オ	ブ
ジェクト]	1253
HIP オブジェクトの General(全般)タブ	.1253
HIP オブジェクトの Mobile Device(モバイル デバイス)タブ	1256
HIP オブジェクトの Patch Management(パッチ管理)タブ	.1258
HIP オブジェクトの Firewall(ファイアウォール)タブ	.1259
HIP オブジェクトの Anti-Malware(アンチマルウェア)タブ	.1259
HIP オブジェクトの Disk Backup(ディスク バックアップ)タブ	.1260
HIP オブジェクトの Disk Encryption(ディスク暗号化)タブ	1261
HIP オブジェクトの Data Loss Prevention(データ損失防止)	1262
HIP オブジェクトの Certificate(証明書)タブ	.1262
HIP オブジェクトの Custom Checks(カスタム チェック)タブ	1263
Objects > GlobalProtect > HIP Profiles [オブジェクト > GlobalProtect > HIP フ	Ъ
ファイル]	1265

Device > GlobalProtect Client [デバイス > GlobalProtect クライアント]	1267
GlobalProtect アプリ ソフトウェアの管理	1267
GlobalProtect アプリのセットアップ	
GlobalProtect アプリの使用	1269
Panorama Web インターフェイス	1271
Panorama Web インターフェイスを使用する	1273
コンテキスト切り替え	1279
Panorama のコミット操作	1280
Panorama でのポリシーの定義	1294
レガシー モードの Panorama バーチャル アプライアンスのログ ストレー	ージ パー
ティション	1297
Panorama > Setup(セットアップ) > Interfaces(インターフェイス)	1299
Panorama > High Availability [Panorama > 高可用性]	1305
Panorama > Managed WildFire Clusters(管理対象 WildFire クラスタ).	1309
管理対象 WildFire クラスタのタスク	1309
管理対象 WildFire アプライアンスのタスク	
管理対象 WildFire の情報	1311
管理対象 WildFire クラスタおよびアプライアンスの管理	1317
Panorama > ファイアウォール クラスター	1333
ファイアウォールクラスタの作成と編集	1333
概要ビュー	1335
モニタリング	1337
Panorama > Administrators [Panorama > 管理者]	1340
Panorama > Admin Roles [Panorama > 管理者ロール]	1344
Panorama > Access Domains [Panorama > アクセス ドメイン]	1347
Panorama >スケジュール設定プッシュ	1349
スケジュール設定プッシュスケジューラ	1350
スケジュール設定のプッシュ実行履歴	1351
Panorama > Managed Devices(管理対象デバイス)	1353
管理対象ファイアウォールの管理	1353
管理対象ファイアウォールの情報	1355
ファイアウォールのソフトウェアとコンテンツの更新	1360
ファイアウォールのバックアップ	
Panorama > Device Quarantine [Panorama > デバイス隔離]	
Panorama > Managed Devices(管理対象デバイス) > Health(健	康状
態)	1364
Detailed Device Health on Panorama(Panorama のデバイス健康	犬態詳
細)	

Panorama > Templates [Panorama > テンプレート]	1371
テンプレート	1371
テンプレート スタック	
Panorama > Templates(テンプレート)> Template Variables	(テンプレート
の変数)	
Panorama > Device Groups [Panorama > デバイス グループ]	
Panorama > Managed Collectors [Panorama > 管理対象コレクタ]	
ログ コレクタの情報	1381
ログ コレクタの設定	1383
専用ログ コレクタのソフトウェアの更新	1393
Panorama > Collector Groups [Panorama > コレクタ グループ]	1395
コレクタ グループの設定	1395
コレクタグループの情報	1403
Panorama > Plugins (プラグイン)	
Panorama > SD-WAN	1406
SD-WAN Devices(SD-WAN デバイス)	1406
SD-WAN VPN Clusters(SD-WAN VPN クラスタ)	1409
SD-WAN Monitoring(SD-WAN モニタリング)	
SD-WAN Reports(SD-WAN レポート)	
Panorama > VMware NSX	1413
通知グループの設定	1413
サービス定義を作成する	1414
NSX Manager へのアクセスの設定	1415
ステアリング ルールの作成	
Panorama > Log Ingestion Profile (ログインジェスト プロファイル)	1420
Panorama > Log Settings [Panorama > ログ設定]	1421
Panorama > Server Profiles > SCP [Panorama > サーバー プロファイバ	V >
SCP]	1424
Panorama > Scheduled Config Export [Panorama > スクシュール設定 エクスポート]	された設定の 1425
Panorama > Software [Panorama > $\sqrt{7}$ hb_{\pm} 7]	1427
Panorama ソフトウェア再新の管理	1427
Panorama ソフトウェア更新信報の表示	1429
Panorama > Device Denloyment [Panorama > デバイスのデプロイ]	1430
ソフトウェアお上びコンテンツ面新の管理	1430
ソフトウェアおよびコンテンツ面新情報の表示	1434
フンテンツ田動的 再新の スケジョール 設定	1/25
ー・ノ・ノニショウショウションを示け更す	1 <i>1</i> 27
ファイアウォールのライヤンス管理	1438
ノノイノフォールのノイビンハ目生	

Panorama >デバイス登録認証キー	
デバイス登録認証キーの追加	

Web インターフェイスの基本

以下のトピックでは、ファイアウォールの概要と、基本的な管理タスクについて説明します。

- ファイアウォールの概要
- 機能と利点
- 前回のログイン時間およびログイン試行回数
- 当日のメッセージ
- タスクマネージャ
- 言語
- アラーム
- 変更のコミット
- 候補設定の保存
- 変更を元に戻す
- 設定のロック
- Global Find
- 脅威詳細
- AutoFocus インテリジェンス サマリー
- ブートモードの変更

ファイアウォールの概要

Palo Alto Networks[®]の次世代ファイアウォールはすべてのトラフィック(アプリケーション、脅威、コンテンツを含む)を検査し、ロケーションやデバイス タイプに関わらずそのトラフィックをユーザーに紐付けます。ユーザー、アプリケーション、コンテンツ(いずれも事業活動に欠かせない要素)はエンタープライズ セキュリティ ポリシーの設定に不可欠な要素になっています。これにより、ビジネス ポリシーに合わせてセキュリティを調整したり、理解・管理しやすいルールを作成することができるようになります。

お客様の組織は当社のセキュリティオペレーティングプラットフォームの一環である次世代 ファイアウォールを使って次のことを実現できます:

- すべてのトラフィック(ポートにかかわらず)を分類化することで、アプリケーション (SaaS アプリケーションを含む)、ユーザー、コンテンツのセキュリティを向上できます。
- ポジティブエンフォースメントモデルにより、すべての目的のアプリケーションを許可して 他をすべてブロックすることで攻撃の入り口を減らせます。
- セキュリティポリシーを適用して既知の脆弱性を狙ったエクスプロイト、ウイルス、ランサム攻撃ボット、スパイウェア、ボットネット、APT攻撃などのその他の未知のマルウェアをブロックできます。
- データおよびアプリケーションをセグメント化し、ゼロトラストの原則を適用することで データセンター(仮想化されたデータセンターを含む)を保護できます。
- オンプレミスおよびクラウド環境全体で一貫したセキュリティを適用できます。
- 場所に関係なくユーザやデバイスに、セキュリティオペレーティングプラットフォームを拡張することにより、安全なモバイルコンピューティングを導入できます。
- 一元的な可視性を実現してネットワークセキュリティを合理化することでデータを操作可能にし、サイバー攻撃を防ぐことができます。
- 有効な企業の認証情報を不正なウェブサイトに送信すること、攻撃者が盗んだ認証情報を 使って横方向に移動することを防ぎ、またネットワーク層に認証ポリシーを適用することで ネットワークのセキュリティ侵害を防ぐことで、認証情報を盗もうとする試みを把握・防止 します。

機能と利点

Palo Alto Networks の次世代ファイアウォールでは、ネットワークへのアクセスを許可されたトラフィックを詳細に制御できます。主な機能と利点は、以下のとおりです。

- アプリケーションベースでのポリシーの適用(App-ID[™]) アプリケーションタイプに従っ てアクセスを制御すると、プロトコルとポート番号以外の情報にも基づいてアプリケーションが識別されるため、アクセス制御の効果が大幅に向上します。App-IDサービスはリスクの 高いアプリケーションをブロックできるだけでなく、ファイル共有など、リスクの高い動作 もブロックできます。また、Secure Socket Layer (SSL)プロトコルで暗号化されたトラフィックの暗号を解読して検査できます。
- ユーザー ID (User-ID[™]) ユーザー ID 機能により管理者は、ネットワーク ゾーンとアドレスの代わりに (またはこれらに加えて)、ユーザーとユーザー グループに基づいてファイアウォール ポリシーを設定および適用できます。ファイアウォールは、Microsoft Active Directory、eDirectory、SunOne、OpenLDAP、および他のほとんどの LDAP ベースのディレクトリ サーバーなど、多くのディレクトリ サーバーと通信して、ユーザーとグループの情報をファイアウォールに提供できます。この情報を使用して、アプリケーションの安全な運用をユーザーまたはグループ単位で定義できます。たとえば管理者は、ある Web ベース アプリケーションの使用を会社内の 1 つの組織に許可し、それ以外の組織に許可しないことができます。また、ユーザーおよびグループに基づいてアプリケーションの特定のコンポーネントをよりきめ細かく制御するように設定することもできます(「User-ID」を参照)。
- 脅威阻止 ウイルス、ワーム、スパイウェア、およびその他の悪意のあるトラフィックから ネットワークを保護する脅威阻止サービスを、アプリケーションとトラフィックの送信元ご とに変えることもできます(「Objects(オブジェクト) > Security Profiles(セキュリティ プロファイル)」を参照)。
- URL フィルタリング アウトバウント接続をフィルタリングして、不適切な Web サイトへのアクセスの阻止もできます(「Objects(オブジェクト) > Security Profiles(セキュリティプロファイル) > URL Filtering(URL フィルタリング)」を参照)。
- トラフィックの可視性 幅広いレポート、ログ、および通知メカニズムにより、ネットワークアプリケーショントラフィックとセキュリティイベントを詳細に観察できます。Webインターフェイスの Application Command Center (ACC)を使用して、トラフィック量が最大のアプリケーションや、セキュリティリスクが最も高いアプリケーションを特定します(「監視」を参照)。
- 多機能なネットワーキングと速度 Palo Alto Networksのファイアウォールは、既存のファ イアウォールを補完したり、置き換えたりできます。また、どのネットワークにも透過的に インストールでき、スイッチまたはルーティング環境をサポートするように設定できます。 マルチギガビットの速度と単一パスアーキテクチャの実現により、ネットワーク遅延にほと んどまたはまったく影響することなく、これらのサービスが提供されます。
- GlobalProtect GlobalProtect[™] ソフトウェアは、世界中のどこからでも簡単かつ安全にログ インできるようにすることで、現場で使用されるノートパソコンなどのクライアント システ ムでセキュリティを確保します。
- フェールセーフ機能 高可用性(HA)のサポートにより、ハードウェアやソフトウェアに 障害が発生した場合に自動的にフェイルオーバーが実行されます(「Device(デバイス) > Virtual Systems(仮想システム)」を参照)。

- マルウェアの分析とレポート WildFire[™] クラウドベース分析サービスは、ファイアウォー ルを通過するマルウェアの詳細な分析とレポートを提供します。AutoFocus[™] の脅威インテ リジェンス サービスとの統合により、組織、業界、グローバル レベルのネットワーク トラ フィックに関連するリスクを評価できます。
- VM-Series ファイアウォール VM-Series ファイアウォールは仮想データ センター環境での 利用に適した PAN-OS[®] 仮想インスタンスを提供し、プライベート、パブリック、およびハ イブリッドのクラウド コンピューティング環境にとって理想的です。
- 管理および Panorama 各ファイアウォールを直観的な Web インターフェイスまたはコマンドライン インターフェイス(CLI)によって管理できます。また、Palo Alto Networks ファイアウォールの Web インターフェイスと非常によく似た Web インターフェイスを備えたPanorama[™]中央管理システムで、すべてのファイアウォールを一元的に管理することができます。

前回のログイン時間およびログイン試行回数

Palo Alto NetworksのファイアウォールやPanoramaの管理者アカウントなど権限付きのアカウントの不正使用を検知して悪用を予防する為、WebインターフェイスとCLI(コマンドラインインターフェイス)には、前回のログイン時間、およびお客様のユーザーネームで行われたログイン 試行回数がログイン時に表示されます。これにより、誰かがあなたの管理者認証情報を使用して攻撃しようとしている場合はすぐにそれを知ることができます。

Webインターフェイスヘログインすると、前回のログイン日時 ごがウィンドウの左下に表示されます。前回のログイン以降、1回以上ログインに失敗している場合は前回のログイン日時の右側に警告アイコンが表示されます。ログインの試行回数を確認する場合は、警告アイコンにカーソルを合わせるか、Failed Login Attempts Summary(ログイン試行回数のサマリー)ウィンドウを開きます(ここには管理者アカウント名、送信元 IP アドレス、ログイン失敗の理由が表示されます)。

自分が行っていないログイン試行が複数回あった場合、ネットワーク管理者の協力のもと、総当 たり攻撃を行っているシステムを特定し、ユーザーとホストコンピューターの検証を行い、悪意 のある活動を特定して排除します。前回のログイン表示によりアカウントに対する不正アクセス が確認された場合は、直ちにパスワードの変更と設定の検証を行い、設定内容に不審な変更点が 無いか確認してください。自分のアカウントを使用してログが削除された、あるいは不正に変更 されたかどうか判別が難しい場合は、元の正しい設定に戻してください。

当日のメッセージ

管理者が「本日のメッセージ」を設定した場合や、Palo Alto Networks のソフトウェアやコンテ ンツ リリースに本日のメッセージが組み込まれている場合、ユーザーが Web インターフェイス にログインすると「本日のメッセージ」ダイアログが自動的に表示されます。システムの再起動 が迫っている場合など、ユーザーが実行しようとするタスクに影響する、重要な情報を表示しま す。

1つのページにつき1つのメッセージが表示されます。ダイアログに Do not show again(今後は 表示しない)というオプションが含まれている場合、以降のログイン時に表示したくないメッ セージを非表示にすることができます。

Message of the Day (本日のメッセージ)に少しでも変更が加えられると、前回の ログイン時に Do not show again (今後は表示しない)を選択した場合でも、次回 のセッションで当該のメッセージが表示されます。変更されたメッセージを以降の セッションで表示したくない場合は、再度このオプションを選択する必要がありま す。

ダイアログページ内を移動する場合、ダイアログの側面に表示されている右向き(゜)と左向き (゜)の矢印をクリックするか、ダイアログ下部に表示されているページセレクター(●○)を クリックします。ダイアログのClose[閉じる]を選択した場合は、Webインターフェイスの下部 に表示されたメッセージ(回)をクリックすることで再び開くことができます。

本日のメッセージの設定を行う場合は、Device(デバイス) > Setup(設定) > Management(管理)を開き、バナーとメッセージの設定を編集します。

タスクマネージャ

前回ファイアウォールが再起動してから自分や他の管理者、または PAN-OS が開始したタスク (たとえば、手動コミットや自動 FQDN 更新)を表示する場合は、Web インターフェイス下部 の Tasks (タスク)をクリックします。タスク マネージャでは、以下の表に記載されている各タ スクの情報を表示したりアクションゴ実行したりできます。



一部の列はデフォルトでは非表示です。特定の列の表示/非表示の切り替えは、列の 見出しにあるドロップダウンリストを開き、Columns(列)を選択して、列名を選 択(表示)または選択解除(非表示)します。

フィールド/ボタン	詳説	
Q -	タスクをフィルタリングするには、いずれかの列の値に基づく テキスト文字列を入力して、Apply Filter(フィルタの適用) (→ を行います。たとえば、「 edl 」と入力すると、リス トがフィルタリングされて EDLFetch(外部動的リス トの取得)タスクのみ表示されます。フィルタリング を解除するには、Remove Filter(フィルタの削除) (× を行います。)
タイプ	タスクのタイプ(ログ要求、ライセンス更新、またはコミットなど)です。タスクに関連する情報(警告など)が長すぎて Messages(メッセージ)列に収まらない場合、Type(タイプ)の値をクリックすると詳細のすべてが表示されます。	
ステータス	タスクが、保留中(Queued(キュー追加済み)状態のコミットなど)、進行中(Active(アクティブ)状態のログ要求など)、完了、または失敗かどうかを示します。進行中のコミットの場合、このステータスには進行状況がパーセントで表示されます。	
ジョブ ID	タスクを識別するための数字です。CLI でジョブ ID を使用す ると、タスクのその他の詳細を確認できます。たとえば、コ ミット キューにあるコミット タスクの順番を確認するには、 以下のように入力します。 > ジョブ ID の表示 <i><iob-id< i="">></iob-id<></i>	
開始時間	タスクが開始した日時を示します。コミット タスクの場合、 開始時間はコミットがコミット キューに追加された日時を示 します。	-

フィールド/ボタン	詳説
メッセージ	タスクの詳細を表示します。エントリのメッセージが多すぎる 場合、タスクの Type(タイプ)をクリックするとメッセージ を表示できます。
	コミット タスクの場合、PAN-OS がコミット処理を開始した 時間が分かるように、コミットがキューから外された時間が メッセージに含まれます。コミットに対し管理者が入力した説 明文を表示する場合はCommit Description [コミットの詳細] を クリックします。詳細は、「変更のコミット」を参照してくだ さい。
操作	管理者または PAN-OS が開始した保留中のコミットをキャン セルする場合、x をクリックします。このボタンを使用できる のは、事前定義済みのロールである、スーパーユーザー、デバ イス管理者、仮想システム管理者、Panorama 管理者のいずれ かの権限を持つ管理者のみです。
管理者	タスクを開始した管理者を表示します。License Refresh などの自動タスクの場合、管理者は system となります。
	(Panorama managed firewalls) タスクが Panorama 管理者に よって開始された場合、管理者名には Panorama が付加され ます。たとえば、Panorama- <admin> のように表示します。</admin>
終了時間	タスクが終了した日時を示します。この列はデフォルトでは非 表示です。
表示	表示するタスクを次から選択します。
	• All Tasks(すべてのタスク)(デフォルト)
	 特定のタイプの All(すべて)のタスク(Jobs(ジョ ブ)、Reports(レポート)、または Log Requests(ログ要 求))
	 すべての Running (実行中)のタスク(進行中)
	 特定のタイプのすべての Running(実行中)のタスク (Jobs(ジョブ)、Reports(レポート)、または Log Requests(ログ要求))
	 (Panoramaのみ)2つ目のドロップダウンリストを使用して、Panorama(デフォルト)または特定の管理対象ファイアウォールのタスクを表示できます。
コミットキューのクリア	管理者または PAN-OS が開始した保留中のコミットをすべて キャンセルします。このボタンを使用できるのは、事前定義済 みのロールである、スーパーユーザー、デバイス管理者、仮想

フィールド/ボタン	詳説
	システム管理者、Panorama 管理者のいずれかの権限を持つ管 理者のみです。

言語

デフォルトでは、ファイアウォールにログインするために使用されるコンピュータに設定され ている言語によって、管理 Web インターフェイスに表示される言語が決まります。言語を手動 で変更する場合はLanguage(言語)をクリックし、Web インターフェイスの右下にあるドロッ プダウンリストから言語を選択し、OKをクリックします。Web インターフェイスが更新される と、選択した言語で Web インターフェイスが表示されます。



対応言語:フランス語、日本語、スペイン語、簡体中国語、繋体中国語。

アラーム

アラームとはファイアウォールが生成する、特定のイベントタイプ(暗号化や復号化の失敗な ど)の発生回数が、そのイベントタイプに設定されたしきい値を超えたことを示すメッセージ です(「アラーム設定の定義」を参照)。アラームを生成する際、ファイアウォールはアラー ムログを作成し、システムアラームダイアログを開き、アラームを表示します。ダイアログを 閉じた場合は、Web インターフェイスの下部に表示された Alarms(アラーム)(クムme) をクリックすることで再び開くことができます。ファイアウォールが特定のアラームのダイア ログを自動的に開かないようにする場合は、Unacknowledged Alarms [未承認のアラーム] を選 択し、Acknowledge [承認] をクリックし、アラームをAcknowledged Alarms [承認済みアラーム] 一覧に移動します。

変更のコミット

Web インターフェイスの右上にある Commit (コミット)をクリックして、ファイアウォール 設定の保留中の変更に対する操作:commit (activate), validate, or preview ご管理者や場所に基づ いてフィルタリングした保留中の変更をプレビュー、検証、コミットできます。特定の仮想シ ステム、共有ポリシーおよびオブジェクト、または共有デバイスおよびネットワーク設定を場所 (Location)にできます。

ファイアウォールはコミット作業をキューで処理するので、前回のコミットの進行中に新し いコミットを追加することができます。ファイアウォールは追加順にコミットを実行します が、FQDN 更新など、ファイアウォールによって開始されるオートコミットを優先します。た だし、管理者が開始したコミットが既にキューの上限まで追加されている場合、ファイアウォー ルが保留中のコミットの処理を終えるまで待機してから、新しいコミットを開始する必要があり ます。

コミットをキャンセルする場合や、保留中、実行中、完了済み、あるいは失敗したコミットの詳 細を表示する場合は、タスクマネージャを使用します。

Commit(コミット)ダイアログには、以下の表に記載されているオプションが表示されます。

フィールド/ボタン	の意味
すべての変更のコミット	管理権限対象のすべての変更をコミットします(デフォル ト)。このオプションを選択している場合、ファイアウォール がコミットする設定変更の範囲を手動でフィルタリングできま せん。代わりに、ログインに使用しているアカウントに割り当 てられた管理者ロールによって、コミット スコープが指定さ れます。
	 Superuser role (スーパーユーザー ロール) – ファイア ウォールはすべての管理者の変更をコミットします。
	 Custom role (カスタム ロール) – アカウントに割り当 てられた管理者ロール プロファイルの権限によって、コ ミット スコープが異なります(「Device (デバイス) > Admin Roles (管理者ロール)」を参照)。プロファイルに Commit For Other Admins (他の管理者向けのコミット)の 権限が含まれている場合、ファイアウォールはあらゆる管 理者が設定した変更をコミットします。管理者ロール プロ ファイルに Commit For Other Admins (他の管理者向けの コミット)の権限が含まれていない場合、ファイアウォー ルは本人の変更のみをコミットして、他の管理者の変更は コミットしません。
	アクセスドメインを実装している場合、ファイアウォー ルはそれらのドメインをコミットスコープのフィルタリン グに自動的に適用します(「Device(デバイス) > Access Domain(アクセスドメイン)」を参照)。管理ロールの種類

フィールド/ボタン	の意味
	に関係なく、ファイアウォールはアカウントに割り当てられた アクセス ドメインの設定変更のみをコミットします。
指定対象による変更のコ ミット	ファイアウォールがコミットする設定変更の範囲をフィルタリ ングします。ログインに使用しているアカウントに割り当てら れた管理ロールによって、フィルタリング オプションが決ま ります。
	 Superuser role(スーパーユーザーロール) – 特定の管理 者による変更や、特定の場所における変更へとコミットス コープを制限できます。
	 Custom role (カスタム ロール) – アカウントに割り当て られた管理者ロール プロファイルの権限によって、フィル タリング オプションが異なります(「Device (デバイス) > Admin Roles (管理者ロール)」を参照)。プロファイ ルに Commit For Other Admins (他の管理者向けのコミッ ト)の権限が含まれている場合、特定の管理者による変更 や特定の場所における変更に、コミット スコープを制限で きます。管理者ロール プロファイルに Commit For Other Admins (他の管理者向けのコミット)の権限が含まれてい ない場合、コミット スコープは、本人が特定の場所で加え た変更にしか制限できません。
	コミット スコープを以下のようにフィルタリングします。
	 Filter by administrator(管理者によるフィルタリング) – 他の管理者の変更をコミットできるロールの場合でも、 デフォルトでコミットスコープに含まれているのは本人 の変更のみです。コミットスコープに他の管理者を追加す るには<usernames>リンクをクリックし、管理者を選択し て、OKをクリックします。</usernames>
	 Filter by location(場所によるフィルタリング) – 変更の特定の場所を選択して、Include in Commit(コミットに含める)を有効にします。
	アクセスドメインを実装している場合、ファイアウォール はそれらのドメインに基づいてコミットスコープを自動的 にフィルタリングします(「Device(デバイス) > Access Domain(アクセスドメイン)」を参照)。管理ロールやフィ ルタリングの選択に関係なく、コミットスコープにはアカウ ントに割り当てられたアクセスドメインの設定変更のみが含 まれます。

フィールド/ボタン	の意味
	 設定をロードした(Device(デバイス) > Setup(セットアップ) > Operations(操作)) 後、Commit All Changes(すべての変更のコミット)を行ってください。
	仮想システムへの変更をコミットする場合、その仮想システム の同じルールベースのルールの追加、削除、位置変更を行った すべての管理者の変更を含める必要があります。
コミット スコープ	コミットする変更を含む場所を一覧表示します。リストに含ま れるのが変更のすべてであるか一部であるかは、複数の要因が 影響します。詳細は、「Commit All Changes(すべての変更の コミット)」および「Commit Changes Made By(指定対象に よる変更のコミット)」に記載されています。場所の種類は以 下のとおりです。
	 shared-object(共有オブジェクト) – 共有の場所で定義されている設定です。
	 policy-and-objects(ポリシーとオブジェクト) – マルチ仮 想システムが存在しないファイアウォールで定義されてい るポリシー ルールまたはオブジェクトです。
	 device-and-network(デバイスとネットワーク) – グローバルであり(インターフェイス管理プロファイルなど)、仮想システム専用でないネットワークおよびデバイス設定です。マルチ仮想システムが存在しないファイアウォールのネットワークおよびデバイス設定にも適用されます。
	 <virtual-system>- 複数の仮想システムを持つファイア ウォールでポリシー ルールまたはオブジェクトが定義さ れている仮想システムの名前。仮想システム専用のネット ワークおよびデバイス設定(ゾーンなど)も含まれます。</virtual-system>
場所タイプ	この列では保留中の変更の場所が分類されます。
	 Virtual Systems(仮想システム) – 特定の仮想システムで 定義されている設定です。
	 Other Changes (その他の変更) – 仮想システム専用でない設定です(共有オブジェクトなど)。
コミットに含める (部分的なコミットのみ)	コミットする変更を選択できます。デフォルトでは、Commit Scope (コミットスコープ)のすべての変更が選択されていま す。この列は、特定の管理者に基づく Commit Changes Made By (指定対象による変更のコミット)を選択しないと表示さ れません。

フィールド/ボタン	の意味
	依存関係が、コミットに含める変更に影響する 場合があります。たとえば、オブジェクトの追 加後に、別の管理者がそのオブジェクトを編集 した場合、その別の管理者の変更のコミット は、自身の変更も合わせてコミットしない限り できません。
場所タイプ別グループ	Commit Scope(コミット スコープ)の設定変更のリストを Location Type(場所タイプ)別にグループにします。
プレビューの変更	Commit Scope (コミットスコープ) で選択した設定を、実行中の設定と比較できるようにします。プレビューウィンドウでは色分けによって詳細が示されます(追加は緑色、変更は黄色、削除は赤色)。
	Web インターフェイスのセクションへの変更を一致させる場合、変更前後の Lines of Context(コンテキストの行)を表示 するようにプレビュー ウィンドウを設定できます。これらは 候補のファイルと、比較対象である実行中の設定から取得され ます。
	プレビュー結果は新しいブラウザ ウィンドウで 表示されるので、ブラウザでポップアップを許可しておく必要があります。プレビュー ウィンドウが開かない場合は、ポップアップを許可する手順についてブラウザのドキュメントを参照してください。
変更サマリー	変更をコミットする個別の設定を一覧表示します。Change Summary(変更サマリー)のリストでは、各設定の以下の情 報が表示されます。
	 Object Name(オブジェクト名) – ポリシー、オブジェクト、ネットワーク設定、またはデバイス設定を識別する名前です。
	 Type (タイプ) – 設定のタイプ (アドレス、セキュリティ ルール、ゾーンなど)です。
	 Location Type(場所タイプ) – 設定が仮想システムで定義 されているかどうかを示します。
	• Location(場所) – 設定が定義されている仮想システムの名前です。仮想システム専用でない設定の場合、列にShared(共有)と表示されます。
	• Operations(操作) – 最後のコミット以降、設定に実施された各操作(作成、編集、または削除)を示します。

フィールド/ボタン	の意味
	 Owner (オーナー) – 設定に直近の変更を加えた管理者です。
	• Will Be Committed(コミット予定) – 現在、設定がコミットに含まれているかを示します。
	 Previous Owners(前回のオーナー) – 直近の変更前に、 設定を変更した管理者です。
	必要に応じて、Group By(グループ化基準)を列名 (Type(タイプ)など)にできます。
	変更リストでオブジェクトを選択し、 Object Level Difference (オブジェクトレベルの差)を表示します。
コミットの検証	ファイアウォール設定の構文が正しく、意味が完全かどうかを 検証します。出力には、コミットが表示するであろうエラーや 警告が含まれます。これにはルール シャドウイングやアプリ ケーション依存関係の警告があります。検証プロセスを利用す ると、エラーを検出、修正してからコミットできます(実行中 の設定は変更されません)。固定のコミット ウィンドウがあ り、エラーなしでコミットを確実に実行したい場合に便利で す。
の意味	他の管理者に変更内容を示すための説明(最大 512 文字)を 入力できます。
	コミット イベントのシステム ログでは、512 文 字を超える説明は切り捨てられます。
コミットする	コミットを開始します。他のコミットが保留中の場合は、コ ミットはコミット キューに追加されます。
コミット状態	コミット中に進行状況を提供し、コミット後に結果を提供しま す。コミットの結果には、成功または失敗、コミットの変更の 詳細、およびコミットの警告が含まれます。以下の警告があり ます。
	• Commit (コミット)ー一般コミット警告を一覧表示します。
	 App Dependency (アプリケーションの依存関係)–既存の ルールに必要なアプリケーションの依存関係を一覧表示し ます。
	• Rule Shadow (ルール シャドウ)–シャドウ ルールを一覧表 示します。
候補設定の保存

設定候補の新しいスナップショットファイルを保存するか、既存の設定ファイルを上書きする 場合は、ファイアウォールまたは Panorama Web インターフェイスの右上にある Config(設 定) > Save Changes(変更の保存)を選択します。変更内容をコミットする前にファイア ウォールまたは Panorama が再起動した場合、保存したスナップショットに設定候補を戻して、 前回のコミット後の変更を復元できます。スナップショットに戻すには、Device(デバイス) > Setup(セットアップ) > Operations(操作)で Load named configuration snapshot(名前付き 設定スナップショットのロード)を選択します。再起動後に設定内容をスナップショットに戻さ ない場合、候補設定は前回コミットした設定内容(実行中の設定)のまま維持されます。

管理者または場所に基づいて、どの設定の変更を保存するかをフィルタリングできます。特定の 仮想システム、共有ポリシーおよびオブジェクト、または共有デバイスおよびネットワーク設定 を場所(Location)にできます。



ファイアウォールや Panorama が再起動しても変更内容が失わないために変更を定期的に保存してください。

変更を候補設定に保存しても、それらの変更は有効にはなりません。有効にするに は変更をコミットする必要があります。

Save Changes(変更の保存)ダイアログには、以下の表に記載されているオプションが表示されます。

フィールド/ボタン	の意味
Save All Changes(すべての 変更の保存)	管理特権対象のすべての変更を保存します(デフォルト)。こ のオプションを選択している場合、手動ではファイアウォール が保存する設定変更の範囲をフィルタリングできません。代わ りに、ログインに使用しているアカウントに割り当てられた管 理者ロールによって、保存範囲が指定されます。
	 Superuser role (スーパーユーザー ロール) – ファイア ウォールは管理者全員の変更を保存します。
	 Custom role (カスタム ロール) – アカウントに割り当て られた管理者ロール プロファイルの権限によって、保存範 囲が異なります(「Device (デバイス) > Admin Roles(管 理者ロール)」を参照)。プロファイルに Save For Other Admins (他の管理者向けの保存)の権限が含まれている場 合、ファイアウォールはあらゆる管理者が設定した変更を 保存します。管理者ロール プロファイルに Save For Other Admins (他の管理者向けの保存)の権限が含まれていない 場合、ファイアウォールは本人の変更のみを保存して、他 の管理者の変更は保存しません。
	アクセスドメインを実装している場合、ファイアウォールは それらのドメインを、保存範囲のフィルタリングに自動的に適

フィールド/ボタン	の意味
	用します(「Device(デバイス) > Access Domain(アクセス ドメイン)」を参照)。管理ロールの種類に関係なく、ファイ アウォールはアカウントに割り当てられたアクセスドメイン の設定変更のみを保存します。
Save Changes Made By(指 定対象による変更の保存)	ファイアウォールが保存する設定変更の範囲をフィルタリング します。ログインに使用しているアカウントに割り当てられた 管理ロールによって、フィルタリング オプションが決まりま す。
	 Superuser role(スーパーユーザー ロール) – 特定の管理 者による変更や、特定の場所における変更へと保存範囲を 制限できます。
	 Custom role (カスタム ロール) – アカウントに割り当て られた管理者ロール プロファイルの権限によって、フィル タリング オプションが異なります(「Device (デバイス) > Admin Roles (管理者ロール)」を参照)。プロファイ ルに Save For Other Admins (他の管理者向けの保存)の 権限が含まれている場合、特定の管理者による変更や特 定の場所における変更へと、保存範囲を制限できます。管 理者ロール プロファイルに Save For Other Admins (他の 管理者向けの保存)の権限が含まれていない場合、保存範 囲は、本人が特定の場所で加えた変更にしか制限できませ ん。
	保存範囲を以下のようにフィルタリングします。
	 Filter by administrator(管理者によるフィルタリング) – 他の管理者の変更を保存できるロールの場合でも、デフォ ルトで保存範囲に含まれているのは本人の変更のみです。 保存範囲に他の管理者を追加するには、<usernames> リ ンクをクリックし、管理者を選択して OK をクリックしま す。</usernames>
	 Filter by location(場所によるフィルタリング) – 特定の場 所の変更を選択して、Include in Save(保存に含める)を有 効にします。
	アクセスドメインを実装している場合、ファイアウォールは それらのドメインに基づいて、保存範囲を自動的にフィルタリ ングします(「Device(デバイス) > Access Domain(アクセ スドメイン)」を参照)。管理ロールやフィルタリングの選 択に関係なく、保存範囲にはアカウントに割り当てられたアク セスドメインの設定変更のみが含まれます。
Save Scope(保存範囲)	保存する変更を含む場所を一覧表示します。リストに含まれ るのが変更のすべてであるか一部であるかは、複数の要因が

フィールド/ボタン	の意味
	影響します。詳細は、「Save All Changes(すべての変更の保存)」および「Save Changes Made By(指定対象による変更の保存)」に記載されています。場所の種類は以下のとおりです。
	 shared-object(共有オブジェクト) – 共有の場所で定義されている設定です。
	 policy-and-objects(ポリシーとオブジェクト) – (ファイ アウォールのみ)マルチ仮想システムを含まないファイア ウォールで定義されているポリシールールまたはオブジェ クトです。
	 device-and-network(デバイスとネットワーク) – (ファ イアウォールのみ)グローバルであり(インターフェイス 管理プロファイルなど)、仮想システム専用でないネット ワークおよびデバイス設定です。
	 <virtual-system>-(Firewall only)複数の仮想システムを持つ firewall 上でポリシー規則またはオブジェクトが定義されて いる仮想システムの名前。仮想システム専用のネットワー クおよびデバイス設定(ゾーンなど)も含まれます。</virtual-system>
	 <device-group>–(Panorama only)ポリシー・ルールまたは オブジェクトが定義されているデバイス・グループの名 前。</device-group>
	 <template>-(Panorama のみ) 設定が定義されているテンプ レートまたはテンプレート スタックの名前。</template>
	 <log-collector-group>–(Panorama のみ) 設定が定義されて いる Collector Group の名前。</log-collector-group>
	 <log-collector>–(Panorama のみ) 設定が定義されている Log Collector の名前。</log-collector>
場所タイプ	この列では変更が行われた場所が分類されます。
	 Virtual Systems (仮想システム) – (ファイアウォールの み)特定の仮想システムで定義されている設定です。
	 Device Groups (デバイス グループ) – (Panorama のみ) 特定のデバイス グループで定義されている設定です。
	 Templates (テンプレート) – (Panorama のみ) 特定のテ ンプレートまたはテンプレート スタックで定義されている 設定です。
	 Collector Groups (コレクタ グループ) – (Panorama の み) コレクタ グループ設定固有の設定です。

フィールド/ボタン	の意味
Include in Save(保存に含め る) (一部の保存のみ)	保存する変更を選択できます。デフォルトでは、Save Scope(保存範囲)のすべての変更が選択されています。この 列は、特定の管理者に基づく Save Changes Made By(指定対 象による変更の保存)を選択しないと表示されません。
	依存関係が、保存に含まれる変更に影響する場合があります。たとえば、オブジェクトの追加後に、別の管理者がそのオブジェクトを編集した場合、その別の管理者の変更の保存は、自身の変更も合わせて保存しない限りできません。
場所タイプ別グループ	Save Scope(保存範囲)の設定変更のリストを Location Type(場所タイプ)別にグループ化します。
プレビューの変更	 Save Scope (保存範囲) で選択した設定を、実行中の設定と比較できるようにします。プレビュー ウィンドウでは色分けによって詳細が示されます(追加は緑色、変更は黄色、削除は赤色)。 Web インターフェイスのセクションへの変更を一致させる場合、変更前後の Lines of Context (コンテキストの行)を表示するようにプレビュー ウィンドウを設定できます。これらは候補のファイルと、比較対象である実行中の設定から取得されます。 プレビュー結果は新しいウィンドウで表示されるので、ブラウザーでポップアップを許可しておく必要があります。プレビューウィンドウが開かない場合はブラウザ設定を参照し、ポップアップブロックの解除を行ってください。
変更サマリー	 変更を保存する個別の設定を一覧表示します。Change Summary (変更サマリー)のリストでは、各設定の以下の情報が表示されます。 Object Name (オブジェクト名) – ポリシー、オブジェクト、ネットワーク設定、またはデバイス設定を識別する名前です。 Type (タイプ) – 設定のタイプ (アドレス、セキュリティルール、ゾーンなど)です。 Location Type (場所タイプ) – 設定が仮想システムで定義されているかどうかを示します。

フィールド/ボタン	の意味
	 Location(場所) – 設定が定義されている仮想システムの名前です。仮想システム専用でない設定の場合、列にShared(共有)と表示されます。
	• Operations(操作) – 最後のコミット以降、設定に実施された各操作(作成、編集、または削除)を示します。
	 Owner (オーナー) – 設定に直近の変更を加えた管理者です。
	 Will Be Saved (保存予定) – 保存作業に設定が含まれる予 定かどうかを示します。
	 Previous Owners(前回のオーナー) – 直近の変更前に、 設定を変更した管理者です。
	必要に応じて、Group By(グループ化基準)を列名 (Type(タイプ)など)にできます。
Save[保存]	選択した変更を、設定スナップショット ファイルに保存しま す。
	 Save All Changes (すべての変更の保存)を選択した場合、 ファイアウォールはデフォルトの設定スナップショット ファイル (.snapshot.xml)を上書きします。
	 Save Changes Made By(指定対象による変更の保存)を選 択した場合、新しい設定ファイルまたは既存の設定ファイ ルの Name(名前)を指定して、OK をクリックします。

変更を元に戻す

前回のコミット以降に候補設定に対して加えた変更を元に戻す場合は、ファイアウォールまたは Panorama Web インターフェイスの右上にある Config(設定) > Revert Changes(変更を元に 戻す)を選択します。変更を元に戻すと、その設定が実行中の設定の値に復元されます。管理者 または場所に基づいて、どの設定の変更を元に戻すかをフィルタリングできます。特定の仮想シ ステム、共有ポリシーおよびオブジェクト、または共有デバイスおよびネットワーク設定を場所 (Location)にできます。

ファイアウォールまたは Panorama が保留中または進行中のすべてのコミットの処理を完了す るまで、変更は元に戻せません。元に戻すプロセスを開始すると、ファイアウォールまたは Panorama が自動的に候補と実行中の設定をロックするため、他の管理者は設定を変更したり、 変更をコミットしたりできません。元に戻すプロセスが完了すると、ファイアウォールまたは Panorama が自動的にロックを解除します。

Revert Changes(変更を元に戻す)ダイアログには、以下の表に記載されているオプションが表示されます。

フィールド/ボタン	の意味
Revert All Changes(すべて の変更を元に戻す)	管理特権対象のすべての変更を元に戻します(デフォルト)。 このオプションを選択している場合、手動ではファイアウォー ルが元に戻す設定変更の範囲をフィルタリングできません。代 わりに、ログインに使用しているアカウントに割り当てられた 管理者ロールによって、元に戻す範囲が指定されます。
	 Superuser role(スーパーユーザーロール) – ファイア ウォールは管理者全員の変更を元に戻します。
	 Custom role (カスタム ロール) – アカウントに割り当 てられた管理者ロール プロファイルの権限によって、 元に戻す範囲が異なります(「Device(デバイス) > Admin Roles(管理者ロール)」を参照)。プロファイルに Commit For Other Admins(他の管理者向けのコミット)の 権限が含まれている場合、ファイアウォールはあらゆる管 理者が設定した変更を元に戻します。管理者ロール プロ ファイルに Commit For Other Admins(他の管理者向けの コミット)の権限が含まれていない場合、ファイアウォー ルは本人の変更のみを元に戻して、他の管理者の変更は元 に戻しません。
	管理者ロールプロファイルでは、コミットの権限が元に戻す権限にも適用されます。
	アクセスドメインを実装している場合、ファイアウォールは それらのドメインを、元に戻す範囲のフィルタリングに自動 的に適用します(「Device(デバイス) > Access Domain(ア クセスドメイン)」を参照)。管理者ロールの種類に関係な

フィールド/ボタン	の意味
	く、ファイアウォールはアカウントに割り当てられたアクセス ドメインの設定変更のみを元に戻します。
Revert Changes Made By(指定対象に基づいて変 更を元に戻す)	ファイアウォールが元に戻す設定変更の範囲をフィルタリング します。ログインに使用しているアカウントに割り当てられた 管理ロールによって、フィルタリング オプションが決まりま す。
	 Superuser role(スーパーユーザー ロール) – 特定の管理 者による変更や、特定の場所における変更へと元に戻す範 囲を制限できます。
	 Custom role (カスタム ロール) – アカウントに割り当て られた管理者ロール プロファイルの権限によって、フィル タリング オプションが異なります(「Device(デバイス) > Admin Roles(管理者ロール)」を参照)。プロファイ ルに Commit For Other Admins(他の管理者向けのコミッ ト)の権限が含まれている場合、特定の管理者による変 更や特定の場所における変更へと、元に戻す範囲を制限で きます。管理者ロール プロファイルに Commit For Other Admins(他の管理者向けのコミット)の権限が含まれてい ない場合、元に戻す範囲は、本人が特定の場所で加えた変 更にしか制限できません。
	元に戻す範囲を以下のようにフィルタリングします。
	 Filter by administrator(管理者によるフィルタリング) 他の管理者の変更を元に戻せるロールの場合でも、 デフォルトで元に戻す範囲に含まれているのは本人の 変更のみです。復帰スコープに他の管理者を追加するに は、<usernames>リンクをクリックし、管理者を選択し て、OKをクリックします。</usernames>
	 Filter by location(場所によるフィルタリング) – 特定の場所の変更を選択して、Include in Revert(元に戻す対象に含める)を有効にします。
	アクセスドメインを実装している場合、ファイアウォールは それらのドメインに基づいて、元に戻す範囲を自動的にフィル タリングします(「Device(デバイス) > Access Domain(ア クセスドメイン)」を参照)。管理者ロールやフィルタリン グの選択に関係なく、元に戻す範囲にはアカウントに割り当て られたアクセスドメインの設定変更のみが含まれます。
Revert Scope(元に戻す範 囲)	元に戻す変更を含む場所を一覧表示します。リストに含まれる のが変更のすべてであるか一部であるかは、複数の要因が影響 します。詳細は、「Revert All Changes(すべての変更を元に 戻す)」および「Revert Changes Made By(指定対象に基づ

フィールド/ボタン	の意味
	いて変更を元に戻す)」に記載されています。場所の種類は以 下のとおりです。
	 shared-object(共有オブジェクト) – 共有の場所で定義されている設定です。
	 policy-and-objects(ポリシーとオブジェクト) – (ファイ アウォールのみ)マルチ仮想システムを含まないファイア ウォールで定義されているポリシー ルールまたはオブジェ クトです。
	 device-and-network(デバイスとネットワーク) – (ファ イアウォールのみ)グローバルであり(インターフェイス 管理プロファイルなど)、仮想システム専用でないネット ワークおよびデバイス設定です。
	 <virtual-system>-(Firewall only)複数の仮想システムを持つ firewall 上でポリシー規則またはオブジェクトが定義されて いる仮想システムの名前。仮想システム専用のネットワー クおよびデバイス設定(ゾーンなど)も含まれます。</virtual-system>
	 <device-group>–(Panorama only)ポリシー・ルールまたは オブジェクトが定義されているデバイス・グループの名 前。</device-group>
	 <template>-(Panorama only)設定が定義されているテンプ レートまたはテンプレートスタックの名前。</template>
	 <log-collector-group>–(Panorama only)設定が定義されている Collector Group の名前。</log-collector-group>
	 <log-collector>–(Panorama only)設定が定義されている Log Collector の名前。</log-collector>
場所タイプ	この列では変更が行われた場所が分類されます。
	 Virtual Systems (仮想システム) – (ファイアウォールのみ)特定の仮想システムで定義されている設定です。
	 Device Group (デバイス グループ) – (Panorama のみ) 特定のデバイス グループで定義されている設定です。
	 Template (テンプレート) – (Panorama のみ) 特定のテ ンプレートまたはテンプレート スタックで定義されている 設定です。
	 Log Collector Group(ログコレクタグループ) – (Panoramaのみ)コレクタグループ設定固有の設定です。
	 Log Collector (ログコレクタ) – (Panorama のみ) ログ コレクタ設定固有の設定です。

フィールド/ボタン	の意味
	 Other Changes (その他の変更) – 前述の設定エリア(共 有オブジェクトなど)に固有でない設定。
Include in Revert(元に戻す 対象に含める) (一部を元に戻すのみ)	元に戻す変更を選択できます。デフォルトでは、Revert Scope(元に戻す範囲)のすべての変更が選択されていま す。この列は、特定の管理者に基づく Revert Changes Made By(指定対象に基づいて変更を元に戻す)を選択しないと表 示されません。
	依存関係が、元に戻す対象に含まれる変更に影響する場合があります。たとえば、オブジェクトの追加後に、別の管理者がそのオブジェクトを編集した場合、その別の管理者の変更も元に戻さないと、自身の変更を元に戻すことができません。
場所タイプ別グループ	Revert Scope(元に戻す範囲)の設定変更を Location Type(場所タイプ)別に一覧表示します。
プレビューの変更	Revert Scope(元に戻す範囲)で選択した設定を、実行中の設定と比較できるようにします。プレビューウィンドウでは色分けによって詳細が示されます(追加は緑色、変更は黄色、削除は赤色)。
	Web インターフェイスのセクションへの変更を一致させる場合、変更前後の Lines of Context(コンテキストの行)を表示 するようにプレビュー ウィンドウを設定できます。これらは 候補のファイルと、比較対象である実行中の設定から取得され ます。
	プレビュー結果は新しいウィンドウで表示されるので、ブラウザーでポップアップを許可しておく必要があります。プレビューウィンドウが開かない場合はブラウザ設定を参照し、ポップアップブロックの解除を行ってください。
変更サマリー	変更を元に戻す対象の個別の設定を一覧表示します。Change Summary(変更サマリー)のリストでは、各設定の以下の情 報が表示されます。
	 Object Name(オブジェクト名) – ポリシー、オブジェクト、ネットワーク設定、またはデバイス設定を識別する名前です。
	 Type (タイプ) – 設定のタイプ (アドレス、セキュリティ ルール、ゾーンなど)です。

フィールド/ボタン	の意味
	 Location Type(場所タイプ) – 設定が仮想システムで定義 されているかどうかを示します。
	 Location(場所) – 設定が定義されている仮想システムの名前です。仮想システム専用でない設定の場合、列にShared(共有)と表示されます。
	• Operations(操作) – 最後のコミット以降、設定に実施された各操作(作成、編集、または削除)を示します。
	 Owner (オーナー) – 設定に直近の変更を加えた管理者です。
	 Will Be Reverted (元に戻す予定) – 元に戻す作業に設定 が含まれる予定がどうかを示します。
	 Previous Owners(前回のオーナー) – 直近の変更前に、 設定を変更した管理者です。
	必要に応じて、Group By(グループ化基準)を列名 (Type(タイプ)など)にできます。
元に戻す	選択した変更を元に戻します。

設定のロック

同時ログイン セッション中にその他のファイアウォール管理者と設定タスクを調整できるよう にするため、Web インターフェイスではapply a configuration or commit lock(設定ロックまた はコミット ロックを適用) ロし、ロックが解除されるまで、その他の管理者が設定を変更した り変更をコミットしたりできないようにします。

1つ以上のロックが設定されている場合はWebインターフェイスの右上に閉じた南京錠(圖)が 表示され(括弧内にロックの数が表示されます)、開いた南京錠(圖)が表示されている場合は ロックされていないことを示します。どちらの場合も、南京錠をクリックすることでロックのダ イアログが表示し、以下のオプションやフィールドを編集することができます。

 管理者が候補設定を変更した際に、コミットを自動的にロックするようファイア ウォールを設定する場合は、Device > Setup > Management[デバイス > 設定 > 管 理]を開いて一般設定を編集し、Automatically Acquire Commit Lock [コミットロック の自動実施]を有効化し、OKをクリックして Commit [コミット]します。

変更を元に戻すと(Config(設定) > Revert Changes(変更を元に戻す))、ファ イアウォールでは候補および実行中設定が自動的にロックされるため、その他の管 理者は設定を編集したり変更をコミットしたりできません。元に戻すプロセスの完 了後、ファイアウォールではロックが自動的に解除されます。

フィールド/ボタン	の意味
admin	ロックを設定した管理者のユーザー名が表示されます。
場所	複数のvirtual system (仮想システム - vsys)を備えたファイア ウォールでは、ロックの範囲を特定の vsys または Shared(共 有)の場所に指定することができます。
タイプ	ロックのタイプには以下のものがあります。 • Config Lock[設定ロック] – 他の管理者が候補設定を変更 できないようにブロックします。スーパーユーザーまたは ロックをセットした管理者のみ解除することができます。
	 Commit Lock (コミットロック) – 他の管理者が候補設定の変更をコミットすることを阻止します。すべてのロックが解除されるまで、コミットキューは新規のコミットを受け付けません。このロックは、複数の管理者が同時ログインセッションにおいて変更を加え、ある管理者がセッションを完了する前に他の管理者が設定を終えてコミットを実行したような場合に発生する、設定の競合を防ぐためのものです。ロックを設定した管理者が実行したコミットが完了すると、ファイアウォールは自動的にロックを解除し

フィールド/ボタン	の意味
	ます。スーパーユーザーまたはロックをセットした管理者 は、手動でそれを解除することもできます。
コメント	最大 256 文字のコメントを入力できます。他の管理者にロック の理由を知らせる場合に便利です。
次の場所に作成	管理者がロックを設定した日時です。
ログイン状態	ロックを設定した管理者が現在ログイン中かどうかが表示され ます。
ロックの設定	ロックを設定する場合は、Take a Lock (ロック設定)を開き、Type (タイプ)を選択し、Location (場所) を指定し(複数の仮想システムをもつファイアウォールのみ)、任意のComments (コメント)を入力し、OKをクリックしてからClose (閉じる) をクリックします。
ロックの削除	ロックを解除する場合はロックを選択し、Remove Lock [ロッ クを解除]、次にOKをクリックし、最後にClose [閉じる] をク リックします。

Global Find

グローバル検索を使用すると、ファイアウォールまたは Panorama の候補設定に含まれる特定の 文字列 (IP アドレス、オブジェクト名、ポリシー名、脅威 ID、ルールの UUID、アプリケーショ ン名など)を検索できます。グローバル検索を使用して、外部ダイナミックリスト内のIPアドレ スを検索することができます。検索結果はカテゴリ別にグループ化され、Web インターフェイ スで設定場所へのリンクが表示されるので、当該文字列が出現する場所、または参照されている 場所をすべて簡単に見つけることができます。

グローバル検索を起動するには、Web インターフェイスの右上にある Search (検索)アイコン Qをクリックします。グローバル検索はすべての Web インターフェイス ページと場所で使用できます。以下に、検索を上手に行うためのグローバル検索の各種機能を示します。

- マルチ仮想システムが有効になっているファイアウォール上で検索を開始する場合、または 管理ロールが定義されている場合は、検索者にアクセス権のあるファイアウォールのエリア の検索結果のみが返されます。Panorama デバイス グループに関しても同様です。管理アク セス権のあるデバイス グループについてのみ、検索結果が表示されます。
- 検索テキストに含まれるスペースは、AND 演算子として処理されます。たとえば、「corp policy」を検索した場合、検索結果に表示されるには corp と policy の両方が含まれている 必要があります。
- 完全に一致するフレーズを検索するには、フレーズを引用符で囲みます。
- 以前の検索を再実行する場合、Global Find(グローバル検索)をクリックすると、直近 20 件の検索のリストが表示されます。リストの項目をクリックすると、その検索が再実行されます。この検索履歴は、管理者アカウントごとに固有のものです。

グローバル検索は検索可能な各フィールドに対して使用できます。たとえば、セキュリティ ポリシーの場合は、次のフィールドを検索できます。名前、タグ、ゾーン、アドレス、ユー ザー、HIP プロファイル、アプリケーション、UUID、およびサービス。検索を実行するには、 これらの任意のフィールドの横にあるドロップダウン リストをクリックして、Global Find(グ ローバル検索)をクリックします。たとえば、I3-vlan-trust という名前のゾーンで Global Find(グローバル検索)をクリックすると、そのゾーン名で設定全体が検索され、検索結果とし てそのゾーンが参照されているすべての場所が返されます。検索結果はカテゴリ別にグループ 化され、いずれかの項目にマウス カーソルを移動すると詳細が表示されます。また、項目をク リックすると、その項目の設定ページに移動します。

グローバル検索では、ファイアウォールがユーザーに割り当てる動的コンテンツ(ログ、アドレス範囲、または個別の DHCP アドレス)は検索されません。DHCP の場合、DHCP サーバー属性 (DNS エントリなど) は検索できますが、ユーザーに発行される個々のアドレスは検索できません。別の例は、ユーザーID[™]機能を有効にしたときにファイアウォールが収集するユーザー名です。この場合、User#ID データベース内に存在するユーザー名またはユーザー グループは、その名前またはグループが設定内に存在する場合 (ポリシー内にユーザー グループ名を定義している場合など)のみ検索可能です。一般に、ファイアウォールが設定に書き込む内容のみ検索できます。

その他の情報をお探しですか?

ファイアウォールまたは Panorama 設定の検索の詳細は、グローバル検索の使用に関するページ を参照してください。

脅威詳細

- Monitor (監視) > Logs (ログ) > Threat (脅威)
- [ACC] > [脅威アクティビティ]
- Objects(オブジェクト) > Security Profiles(セキュリティ プロファイル) > Anti-Spyware(アンチスパイウェア)/Vulnerability Protection(脆弱性防御)

ファイアウォールが実装する脅威シグネチャ、およびそのシグネチャをトリガーするイベントについては、Threat Details(脅威詳細)ダイアログを参照してください。脅威詳細は次のもののために提供されます。

- ファイアウォールが検出する脅威を記録する脅威ログ(Monitor(監視) > Logs(ログ) > Threat(脅威))
- ネットワークで検出される上位の脅威(ACC > Threat Activity(脅威アクティビティ))
- 適用を変更または除外する脅威シグネチャ(Objects(オブジェクト) > Security Profiles(セキュリティプロファイル) > Anti-Spyware(アンチスパイウェア)/ Vulnerability Protection(脆弱性防御))

脅威シグネチャが見つかり、それについて詳しく調べる必要がある場合は、Threat Name(脅威名)または脅威 ID にマウスを合わせて、Exception(例外)をクリックして脅威詳細を確認します。脅威詳細では、脅威シグネチャがセキュリティ ポリシーの例外として設定されているかどうかを簡単に確認し、特定の脅威に関するThreat Vault の最新情報を検索できます。Palo Alto Networks Threat Vault データベースはファイアウォールと統合されているため、ファイアウォール コンテキストで脅威シグネチャに関する詳細を参照したり、新しいブラウザ ウィンドウで Threat Vault 検索を起動して、ログに記録された脅威を検索したりすることができます。

参照している脅威のタイプに応じて、詳細には、次の表で説明する脅威詳細のすべてまたは一部 が組み込まれます。

脅威詳細	の意味
氏名	脅威シグネチャ名。
ID	一意の脅威シグネチャ ID。Threat Vault 検索を新しいブラウザ ウィ ンドウで開き、Palo Alto Networks の脅威データベースに含まれて いる、このシグネチャの最新情報を検索するには、View in Threat Vault (Threat Vault で表示)を選択します。脅威シグネチャの Threat Vault エントリには、シグネチャの更新を含む最初のコンテ ンツリリースと最後のコンテンツリリース、およびシグネチャのサ ポートに必要となる PAN-OS の最低バージョンなどの詳細が含まれ ることがあります。
の意味	シグネチャをトリガーする脅威についての情報。
重要度	脅威の重大度。通知、低、中、高、重要のいずれか。

脅威詳細	の意味
CVE	脅威に関連して、一般に知られているセキュリティの脆弱性。 ベンダー固有の ID には一般的に複数の脆弱性が含まれます が、CVE(Common Vulnerabilities and Exposures)識別子は、固有の 脆弱性に関する情報を検索するための最も便利な識別子です。
bugtraq id	脅威に関連付けられているバグトラック ID。
ベンダー ID	脆弱性のベンダー固有識別子。たとえば、MS16-148 は Microsoft の 1 つ以上の脆弱性のベンダー ID であり、APBSB16-39 は Adobe の 1 つ以上の脆弱性のベンダー ID です。
リファレンス	脅威について参考にすることができる調査資料。
プロファイルの免除	デフォルトのシグネチャアクション以外で、脅威シグネチャに適用 するアクションを定義するセキュリティプロファイル。脅威例外が 有効になるのは、除外プロファイルがセキュリティポリシールール に添付されているときのみです(例外が現在のセキュリティルール で使用されているかどうかを確認してください)。
現在のセキュリティ ルールで使用	脅威例外が有効 – この列にチェックマークが付いているということ は、ファイアウォールで脅威例外が適用されている(脅威例外を定義 する除外プロファイルがセキュリティ ポリシー ルールに添付されて いる)ということです。 この列にチェックマークが付いていない場合、ファイアウォールで は、推奨デフォルト シグネチャ アクションのみに基づいて脅威に対 処しています。
IP アドレスの免除	除外 IP アドレス – 脅威例外をフィルタリングする IP アドレスを追加 するか、既存の Exempt IP Addresses (除外 IP アドレス) を表示で きます。関連付けられているセッションに送信元 IP アドレスか宛先 IP アドレスがあり、それが除外 IP アドレスと一致するときに限り、 このオプションによって脅威例外が適用されます。その他すべての セッションでは、デフォルトのシグネチャ アクションに基づいて脅 威が対処されます。

脅威詳細を表示できない場合は、次の条件を確認してください。

- ファイアウォールの脅威防御ライセンスが有効である(Device(デバイス) > Licenses(ライセンス))。
- アンチウイルス、脅威、アプリケーションの最新コンテンツ更新がインストール されている。
- Threat Vault アクセスが有効である(Device (デバイス) > Setup (設定) > Management (管理)を選択し、Logging and Reporting (ログとレポート)の設定 を Enable Threat Vault Access (Threat Vault アクセスの有効化)に編集する)。
- デフォルトの(またはカスタムの) Antivirus, Anti-Spyware, and Vulnerability Protection security profiles(アンチウイルス、アンチスパイウェア、脆弱性防御 のセキュリティ プロファイル)がセキュリティ ポリシーに適用されている。

AutoFocus インテリジェンス サマリー

AutoFocus によって集められた脅威インテリジェンスの概要をグラフィカルに表示でき、以下のファイアウォールのアーチファクトの広がりとリスクを評価するのに役立ちます。

- IPアドレス
- URLプロテクションの
- ドメイン
- ユーザーエージェント(データフィルタリングログのUser Agent(ユーザーエージェント)列で確認できます)
- 脅威名(サブタイプ ウイルスおよび WildFire ウイルスの脅威のみ)
- ファイル名
- SHA-256 ハッシュ(WildFire への送信ログの File Digest(ファイル ダイジェスト)列で確認 できます)

AutoFocus Intelligence Summary (AutoFocus インテリジェンス サマリー) ウィンドウを表示する には、まずはアクティブな AutoFocus サブスクリプションを用意して AutoFocus 脅威インテリ ジェンスを有効化 (Device (デバイス) > Setup (セットアップ) > Management (管理)を選択して AutoFocus 設定を編集) する必要があります。

AutoFocus インテリジェンスを有効化した後、ログあるいは外部動的リストのアーチファクトに カーソルを合わせてドロップダウンリストを開き([×])、AutoFocusをクリックします:

- トラフィック、脅威、URLフィルタリング、WildFireへの送信、データフィルタリング、統合ログ(Monitor(監視) > Logs(ログ))を表示する。
- 外部動的リストエントリを表示する。

また、気になる、あるいは疑わしいアーチファクトを詳しく調査するために、ファイアウォール から AutoFocus 検索を起動することもできます。

フィールド/ボタン	の意味	
AutoFocus を検索	アーチファクトに対する AutoFocus 検索を起動する場合にクリックしま す。	
Analysis Information(分析情報)タブ		
セッション数	WildFire がアーチファクトを検出したプライベート セッションの数。プ ライベートセッションとは、お客様のサポートアカウントに関連付けられ たファイアウォールで実行されているセッションを指します。セッション バーにマウス カーソルを移動すると、月あたりのセッション数が表示さ	

サンプル	アーチファクトに関連付けられた組織サンプルおよびグローバル サン プル(ファイルと電子メール リンク)。WildFire 判定(安全、グレイ

フィールド/ボタン	の意味
	ウェア、マルウェア、フィッシング)でグループ化されます。Global(グ ローバル)はすべての WildFire 送信のサンプルを意味します。一 方、organization(組織)は組織が WildFire に送信するサンプルのみを意 味します。
	WildFire 判定をクリックすると、範囲(組織またはグローバル)と WildFire 判定でフィルタリングされたアーチファクトの AutoFocus 検索 が起動します。
一致するタグ	アーチファクトに一致する AutoFocus タ グ
	 プライベート タグ – サポート アカウントに関連付けられた AutoFocus ユーザーにのみ表示されます。
	 パブリック タグ – すべての AutoFocus ユーザーに表示されます。
	 Unit 42 タグ – 直接的なセキュリティ リスクを引き起こす脅威やキャンペーンを識別します。これらのタグは、Unit 42(Palo Alto Networks 脅威インテリジェンスおよび研究チーム)によって作成されます。
	● 情報タグ – コモディティ脅威を識別する Unit 42 タグ。
	タグにマウス カーソルを移動すると、そのタグの説明や他のタグの詳細 が表示されます。
	タグをクリックすると、そのタグの AutoFocus 検索が起動します。
	アーティファクトのタグをさらに表示するには、省略記号(…)をクリックしてアーチファクトに対する AutoFocus 検索を起動します。AutoFocus 検索結果の Tags (タグ)列に、アーチファクトに一致するその他のタグが表示されます。

Passive DNS (パッシブ DNS) タブ

Passive DNS (パッシブ DNS) タブには、アーチファクトに関連付けられたパッシブ DNS 履歴が表示されます。このタブには、アーチファクトが IP アドレス、ドメイン、または URL の場合の一致 情報のみが表示されます。

要求	DNS 要求を送信したドメイン。ドメインをクリックすると、そのドメインの AutoFocus 検索が起動します。
タイプ	DNS 要求タイプ(A、NS、CNAME など)。
応答	DNS 要求で解決された IP アドレスまたはドメイン。IP アドレスまたはド メインをクリックすると、AutoFocus 検索が起動します。
	Response(応答)列にプライベート IP アドレスは表示されません。

0

フィールド/ボタン	の意味
数	要求が作成された回数。
First Seen (最初)	パッシブ DNS 履歴で要求、応答、タイプの組み合わせが最初に出現した 日時。
Last Seen(最後に出現 した日時)	パッシブ DNS 履歴で要求、応答、タイプの組み合わせが最後に出現した 日時。

Matching Hashes (一致するハッシュ) タブ

Matching Hashes(一致するハッシュ)タブには、WildFire がアーチファクトを検出した直近のプラ イベート サンプルが 5 つ表示されます。プライベートサンプルとは、お客様のサポートアカウント に関連付けられたファイアウォールで検出されたサンプルを指します。

SHA256	サンプルの SHA-256 ハッシュ。ハッシュをクリックすると、そのハッ シュの AutoFocus 検索が起動します。
ファイルタイプ	サンプルのファイル タイプ。
作成日	WildFire がサンプルを分析して WildFire 判定を割り当てた日時。
更新日	WildFire がサンプルの WildFire 判定を更新した日時。
判定	サンプルの WildFire 判定(安全、グレイウェア、マルウェア、または フィッシング)。

設定テーブルのエクスポート

管理ユーザーは、ポリシー ルールベース、オブジェクト、管理対象デバイス、インターフェイ スのデータを表形式で PDF ファイルまたは CSV ファイルにエクスポートできます。エクスポー トされるデータは、Webインターフェイス上で閲覧できるデータです。フィルタリングされた データの場合、フィルタに一致するデータのみがエクスポートされます。フィルタを適用しない 場合、すべてのデータがエクスポートされます。

🏫 PDF ファイルへのエクスポートでは、英語の説明のみがサポートされます。

パスワードなどのすべての機密データは、ワイルドカード(*)記号で隠されています。

設定テーブルのエクスポートが成功すると、システム ログとダウンロード リンクが生成されま す。ダウンロード リンクを使用して、PDF または CSV ファイルをローカルに保存します。ダウ ンロード リンクを含むウィンドウを閉じると、その特定のエクスポートのダウンロード リンク は使用できなくなります。

エクスポート設 定	の意味
ファイル名	エクスポートされたデータを識別する名前(最大 200 文字)を入力します。 この名前は、エクスポートにより作成されるダウンロード ファイルの名前 になります。
ファイルタイプ	生成するエクスポート出力のタイプを選択します。PDF または CSV 形式の いずれかを選択できます。
Page Size(ページサ イズ)	デフォルトのページ サイズは Letter(レター)(8.5 x 11.1 インチ)で す。ページ サイズは変更できません。デフォルトでは、PDF は縦向きに生 成され、縦書きの向きに変更されて最大列数に対応します。
説明 (PDFのみ)	エクスポートに関するコンテキストと追加情報を提供するための説明(最 大 255 文字)を入力します。
Table Data(表 データ)	エクスポートする表データを表示します。以前に設定したフィルタリング 設定を消去する必要がある場合は、Show All Columns(すべての列を表 示)をクリックして、選択したポリシー タイプのすべてのポリシー ルール を表示します。これで、必要に応じて列を追加または削除したりフィルタ を適用したりできます。
Show All Columns(すべ ての列を表示)	すべてのフィルタを削除してすべての表の列を表示します。

表データをエクスポートするには、PDF/CSV をクリックして次の項目を設定します。

設定テーブルのダウンロード リンクを生成するには、Export(エクスポート)をクリックしま す。

ブートモードの変更

一部のファイアウォールは、デフォルトでゼロタッチプロビジョニング(ZTP)モードで起動しま す。ZTP 構成を選択する場合、起動時に入力は必要ありません。非 ZTP (標準) ファイアウォー ルを展開する場合は、Cli にアクセスして ZTP モードを終了する必要があります。



ZTP 機能にアクセスするには、パノラマ管理サーバーに ZTP プラグインをインス トールする必要があります。

STEP 1| ファイアウォールの電源を入れた後、PuTTY などのターミナル エミュレータを使用して、 次の CLI プロンプトを監視します。

ZTP モードを終了して、ファイアウォールを標準モード (はい/いいえ) [いいえ] で構成しますか?

はい と入力します。システムは、確認を求められます。もう一度 **yes**と入力して、ファイ アウォールを標準モードで起動します。



- STEP 2| (上記の CLI プロンプトに見当が付く場合)また、Web インターフェイスを使用してブート モードを変更することもできます。起動プロセスの前または実行中に、ファイアウォール のログイン画面に移動します。ZTP モードで起動を続行するか、標準モードに切り替え るかどうかを確認するメッセージが表示されます。標準モードを選択すると、ファイア ウォールは標準モードで再起動を開始します。
- STEP 3 標準モードを使用する場合は、ファイアウォールを手動で設定します。ZTP モードを使用 している場合、Panorama 管理サーバーで定義されているデバイス グループとテンプレー ト構成は、ZTP サービスによって自動的にファイアウォールにプッシュされます。
 - (標準モード)コンピュータの IP アドレスを 192.168.1.0/24 ネットワークのアドレス (192.168.1.2 など) に変更します。Web ブラウザーから、https://192.168.1.1 に移動しま す。プロンプトが表示されたら、デフォルトのユーザー名とパスワード(admin/admin)を使 用してWebインターフェイスにログインします。
 - (ZTP モード)Panorama 管理者から提供される指示に従って ZTP ファイアウォールを登録 します。シリアル番号 (S/N として識別される 12 桁の番号) と要求キー (8 桁の番号) を入

力する必要があります。これらの番号は、デバイスの背面に貼り付けられたステッカーに 表示されます。



ダッシュボード

ダッシュボード ウィジェットには、ソフトウェアのバージョン、各インターフェイスの状態、リソース使用率、ログタイプごとの 10 個までのエントリなど、ファイアウォールや Panorama[™] の一般的な情報が表示されます。ログ ウィジェットには、過去1時間のエントリが 表示されます。

「ダッシュボード ウィジェット」では、ダッシュボードの使用方法、および使用可能なウィジェットについて説明します。

Dashboard Widgets (ダッシュボード ウィジット)

デフォルトでは、**Dashboard**(ダッシュボード)には**3**列のレイアウトでウィジェットが表示されますが、**2**列のみを表示するようにダッシュボードをカスタマイズできます。

どのウィジェットを表示し、どのウィジェットを非表示にするのかも決められるため、監視対象 のみを表示できます。ウィジェットを表示するには、Widgets(ウィジェット)ドロップダウン リストからウィジェットのカテゴリを選択し、ダッシュボードに追加するウィジェットを選択し ます(名前がグレー表示になっているウィジェットはすでに表示されています)。ウィジェット を非表示にする(表示を停止する)には、ウィジェットを閉じます(ウィジェットのヘッダーの ×)。ファイアウォールと Panorama では、ログインしなおしてもウィジェットの表示設定は 保存されています(管理者ごとに個別に)。

ダッシュボードのデータが前回いつ更新されたのかは、Last updated(最終更新)タイムスタン プで判断します。Dashboard(ダッシュボード)全体を手動で更新したり(ダッシュボードの右 上の〇)、ウィジェットを個別に更新したり(各ウィジェットのヘッダーの〇)することが できます。Dashboard(ダッシュボード)全体の自動更新間隔(分単位)を選択するには、手動 ダッシュボード更新オプション(〇)の隣にあるラベルなしのドロップダウンを使用します: 自動更新間隔は1分、2分、または5分で設定できます。Dashboard(ダッシュボード)全体の 自動更新を無効にするには、Manual(手動)を選択します。

Dashboard Widgets(ダッシュ ボード ウィジット)	の意味

アプリケーション ウィジット

上位のアプリケー ション	セッション数が最も多いアプリケーションが表示されます。ブロック サイズでセッションの相対数を示し(マウス カーソルをブロックの 上に移動すると数が表示されます)、色でセキュリティのリスクを示 します(緑(リスク低)~赤(リスク高))。アプリケーションをク リックして、プロファイルを表示します。
上位のハイリスク アプリケーション	Top Applications(上位アプリケーション)と似ていますが、ここに はセッション数が最も多いハイリスク アプリケーションが表示されま す。
ACC リスク ファク タ	過去1週間の間に処理されたネットワーク トラフィックの平均リスク ファクタ(1~5)が表示されます。値が大きいほどリスクが大きくな ります。
システム ウィジット	
General Information	ファイアウォールあるいは Panorama 名およびモデル、Panorama の CPU および RAM、Panorama のシステムモード、PAN-OS [®] あるい

Dashboard Widgets(ダッシュ ボード ウィジット)	の意味
	情報、シリアル番号、CPU ID および UUID、アプリケーション、脅 威、URL フィルタリング定義のバージョン、現在の日次、前回の再起 動から経過した時間を表示します。
インターフェイス (ファイアウォール のみ)	各インターフェイスが、有効(緑)、無効(赤)、または不明な状態(グ レー)であることを示します。パワーオーバーイーサネット(PoE)をサ ポートするインターフェイスには、稲妻アイコンが付いています。イ ンターフェイス上にマウス カーソルを置くと、リンク設定とステータ ス情報が表示されます。リンク速度、リンク デュプレックス、PoE 情 報などの追加の詳細は、ポート タイプに基づいて表示されます。
システム リソース	管理 CPU の使用率、データプレーン使用率、およびセッション数 (ファイアウォールまたは Panorama で確立されたセッションの数) が表示されます。
HA	高可用性(HA)を有効にすると、ローカルおよびピアファイア ウォール/PanoramaのHA状態 – 緑(アクティブ)、黄(パッシ ブ)、黒(その他) – が表示されます。HAの詳細については、デバ イス > 高可用性または Panorama > 高可用性を参照してください。
HA Cluster HA クラ スタ	HA Cluster が有効な場合、クラスター統計と、クラスター内の各メン バーの HA4 および HA4_backup リンクのキープアライブ値を示しま す。
ロック	管理者が設定したロックを表示します。
ログインしている管 理者	現在ログインしている各管理者の送信元IPアドレス、セッションタイ プ(WebインターフェイスまたはCLI)、およびセッションの開始時 刻が表示されます。
PoE 電力バジェット (サポートされてい る firewall のみ)	パワーオーバーイーサネットを使用している場合、設定されているイ ンターフェイスの総電力バジェットおよび総割当電力を表示します。 ドーナツチャートは、firewallで使用可能な電力を確認し、PoEポート に接続する受電デバイス(PD)を決定するのに役立ちます。
ログウィジェット	
脅威ログ	脅威ログには、最新 10 エントリの脅威の ID、アプリケーション、お よび日時が表示されます。脅威 ID は、マルウェアに関する説明、また は URL フィルタリング プロファイルに違反する URL を示します。過 去 60 分間のエントリのみが表示されます。

Dashboard Widgets(ダッシュ ボード ウィジット)	の意味			
URL フィルタリング ログ	URL フィルタリング ログには、直近 60 分間に生成されたログの説明 と日時が表示されます。			
データ フィルタリ ング ログ	データフィルタリングログには、直近 60 分間に生成されたログの説 明と日時が表示されます。			
設定ログ	設定ログには、最新10エントリの管理者ユーザー名、クライアント (WebインターフェイスまたはCLI)、および日時が表示されます。過去 60 分間のエントリのみが表示されます。			
システムログ	システム ログには、最新 10 エントリの説明と日時が表示されます。			
	Config installed」エントリは、設定の変更が正常にコ ミットされたことを示します。過去 60 分間のエントリのみが表示されます。			

ACC

アプリケーション コマンド センター(ACC)は、ネットワーク内のアクティビティに関する実用的なインテリジェンスを提供する分析ツールです。ACCは、ファイアウォール ログを使用してネットワーク上のトラフィック トレンドをグラフィカルに表現します。このグラフィカル表現を使用して、データにアクセスし、ネットワークの使用パターン、トラフィック パターン、疑わしいアクティビティ、異常を含め、ネットワーク上のイベント間の関係を視覚化できます。

- ACC の画面紹介
- ACC のタブ
- ACC のウィジェット
- ACC のアクション
- タブおよびウィジットの処理
- フィルタの処理 ローカルフィルタおよびグローバルフィルタ

その他の情報をお探しですか?

「アプリケーション コマンド センターの使用 」を参照してください。

ACC の画面紹介

以下の表で、ACC タブと各コンポーネントの説明を示します。



ACC の画面紹介				
御<防 御}<{防 御>防 御<防 御}}				
2	ウィジェッ ト	各タブには、タブに関連付けられたイベントとトレンドを最適に表現す る、デフォルトのウィジット セットが含まれます。ウィジェットで、 バイト数(入力および出力)、セッション、コンテンツ(ファイルおよ びデータ)、URL カテゴリ、アプリケーション、ユーザー、脅威(有 害、安全、グレイウェア、フィッシング)、およびカウントのフィルタ を使用してデータを調べることができます。各ウィジェットの詳細は、 「ACC のウィジェット」を参照してください。		
3	時間	各ウィジットのチャートとグラフにはリアルタイム表示と履歴表示が用 意されています。カスタム範囲を選択するか、過去15分から最大過去 90日(または暦日で過去30日)までの範囲の事前定義済みの期間を選択 することができます。 データの表示に使用するデフォルトの期間は過去1時間です。画面に日 付と時間の間隔が表示されます。以下に例を示します。 11/11 10:30:00-01/12 11:29:59		
4	グローバル フィルタ	グローバルフィルタでは、すべてのタブに適用されるフィルタを設定できます。選択されたフィルタがチャートとグラフに適用された後にデータが表示されます。フィルタの使用方法の詳細は、「ACCのアクション」を参照してください。		
5	アプリケー ションの ビュー	アプリケーションのビューでは、ネットワークで使用中の許可されたア プリケーションと不許可のアプリケーション、またはネットワークで使 用中のアプリケーションのリスクレベルで ACC ビューをフィルタリング できます。緑色は許可されたアプリケーション、青色は不許可のアプリ ケーション、黄色は仮想システムまたはデバイスグループごとに許可状 態が異なるアプリケーションを示しています。		
6	リスク メー ター	リスクメーター(1=最低~5=最高)は、ネットワーク上の相対的なセ キュリティリスクを示します。リスクメーターではさまざまな要因が 使用されます。たとえば、ネットワーク上で確認されたアプリケーショ ンのタイプ、そのアプリケーションに関連付けられるリスクレベル、 ブロックされた脅威数によって確認される脅威のアクティビティとマル ウェア、侵入されたホスト、マルウェアのホストまたはドメインへのト ラフィックがあります。		

ACC の画面紹介					
7	送信元	ファイアウォールと Panorama [™] では、表示に使用するデータが異なりま す。以下のオプションを使用して、ACC のビューを生成するためのデー タを選択できます。			
		仮想システム(vsys):マルチ仮想システムが有効になっているファイア ウォールでは、Virtual System(仮想システム)ドロップダウンを使用し て、ACC の表示にすべての仮想システムを含めるか、選択した仮想シス テムのみを含めるかを変更できます。			
		デバイス グループ:Panorama では、 Device Group (デバイス グルー プ)ドロップダウンを使用して、ACC の表示にすべてのデバイス グルー プのデータを含めるか、選択したデバイス グループのデータのみを含め るかを変更できます。			
		データ送信元:Panoramaでは、表示にPanoramaを使用するか、Remote Device Data(リモートデバイスデータ)を使用するかも変更できます (ファイアウォールデータを管理)。データソースがPanoramaの場合、 特定のデバイスグループに応じて表示をフィルタリングできます。			
8	エクスポー ト	現在のタブに表示されているウィジットを PDF としてエクスポートでき ます。			

ACCのタブ

- Network Activity(ネットワークアクティビティ) ネットワーク上のトラフィックおよび ユーザーアクティビティの概要が表示されます。このビューは、使用頻度が上位のアプリ ケーション、トラフィックを生成した上位のユーザーとそのユーザーがアクセスしたバイト 数、コンテンツ、脅威、および URL の詳細、ならびにトラフィックと一致したセキュリティ ポリシールールのうち最も多く使用されたセキュリティ ルールに焦点を当てます。また、 ネットワークアクティビティを送信元または宛先のゾーン、領域、または IP アドレス別に表 示したり、入力インターフェイスまたは出力インターフェイス別に表示したり、ホスト情報 (ネットワーク上で最もよく使用されたデバイスのオペレーティングシステムなど)別に表示 したりできます。
- Threat Activity(脅威アクティビティ) ネットワーク上の脅威の概要が表示されます。 このタブは上位の脅威に焦点を当てます。たとえば、脆弱性、スパイウェア、ウイルス、 有害なドメインまたは URL にアクセスしているホスト、上位の WildFire 送信 (ファイル タイプ別およびアプリケーション別)、非標準ポートを使用しているアプリケーションで す。Compromised Hosts(侵入されたホスト)ウィジットは、すぐれた可視化技術を使用し て検出を補完します。これは、correlated events(相関イベント)タブ(Monitor(監視) > Automated Correlation Engine(自動相関エンジン) > Correlated Events(相関イベント)か らの情報を使用して、ネットワーク上の侵入されたホストを送信元ユーザーまたは IP アドレ スごとに重大度の順番で集約して表示します。
- Blocked Activity(ブロックされたアクティビティ) ネットワークに入ることができなかったトラフィックに焦点を当てます。このタブのウィジェットを使用すると、アプリケーション名、ユーザー名、脅威名、コンテンツ(ファイルとデータ)、およびトラフィックをブロックする拒否アクションの上位セキュリティルールによって拒否されたアクティビティを表示できます。
- Mobile Network Activity (モバイル ネットワーク アクティビティ) セキュリティ ポ リシー ルール設定から生成された GTP ログを使用して、ネットワークのモバイル トラ フィックが視覚的に表示されます。このビューには、対話形式のカスタマイズ可能な GTP Events (GTP イベント)、Mobile Subscriber Activity (モバイルサブスクライバアクティ ビティ)および GTP Rejection Cause (GTP 拒否理由) ウィジットが含まれます。これらの ウィジットに ACC フィルタを適用してドリルダウンし、必要な情報を分離できます。SCTP Security (SCTP セキュリティ)を有効にすると、このタブのウィジェットは、ファイア ウォール上の SCTP イベントの視覚的表現と詳細、および SCTP Association ID (SCTP アソ シエーション ID) ごとに送受信されるチャンクの数を表示します。
- Tunnel Activity(トンネルアクティビティ) トンネル検査ポリシーに基づいて ファイアウォールで検査されるトンネルトラフィックのアクティビティが表示されま す。トンネル ID、モニター タグ、ユーザー、トンネル プロトコル(Generic Routing Encapsulation (GRE)、General Packet Radio Service (GPRS) Tunneling Protocol for User Data (GTP-U)、非暗号化 IPSec など)に基づいて、トンネルの使用状況などの情報が表示 されます。
- GlobalProtect Activity-GlobalProtect 展開でのユーザーアクティビティの概要を表示します。情報には、ユーザー数とユーザーの接続回数、ユーザーが接続したゲートウェイ、接続の失敗回数と失敗の理由、認証方法の概要と使用された GlobalProtect アプリケーションのバージョン、および隔離されたエンドポイントの数が含まれます。

- SSL Activity (SSLアクティビティ) 復号化ポリシーおよびプロファイルに基づき、復号化されたTLS / SSLトラフィックと復号化されていないTLS / SSLトラフィックのアクティビティを表示します。非TLS アクティビティと比較したTLS アクティビティ、復号化されたトラフィックと復号化されていないトラフィックの比較、復号化障害の理由、TLS のバージョンおよびキー交換アクティビティの正常完了を確認することができます。この情報を使用し、復号化の問題を引き起こすトラフィックを特定します。次に、復号化ログおよびカスタム復号化レポートテンプレートを使用してより詳細な情報まで掘り下げ、該当するトラフィックに関するコンテキストを取得すると、問題を正確に診断して修正することができます。
- タブおよびウィジットの処理に記載されている通り、タブおよびウィジェットをカ スタマイズすることもできます。

ACCのウィジェット

各タブのウィジットを操作できます。フィルタを設定し、表示をドリルダウンしてカスタマイズ し、必要な情報に焦点を当てることができます。

Threat Activity						4 2	TEC
threats Home	1						⊨ ≝ ⊥
vulnerability							9.05M
virus	2.49k			2			
wildfire-virus	1.61k	2.00N	1	4.00M	6.00M	8.00M	10.00M
THREAT NAME			ID	SEVERI	THREAT TY	THREAT CATEG	COUNT
SSH User Authen	ticatio 3	For	40015	high	vulnerability	brute-force	8.9M 🔺
Microsoft Office	File with Macr	'os	39154	inform	vulnerability	code-execution	564.2k
Suspicious HTTP	Evasion Dete	ction	38635	mediu	vulnerability	code-execution	7.5k
SIP INVITE Metho	od Request Fl	boo	40016	high	vulnerability	brute-force	6.5k
Various Evasion T	echniques		35902	mediu	vulnerability	code-execution	5.8k
Cesanta Mongoos	se parse_mqtt	De	57956	critical	vulnerability	dos	5.2k
Citrix Application	Delivery Con	troll	57497	critical	vulnerability	info-leak	3.6k
IBM Tivoli Storage	e Manager Fa	stBa	38771	critical	vulnerability	overflow	3.5k
Virus/Win32.WG	eneric.ahohsd		3230	mediu	virus	pdf	3.5k
Various Evasion T	echniques		35670	high	vulnerability	code-execution	2.8k

各ウィジェットは以下の情報を表示するように構成されています。

{{御御御御御御御御御御御御御御御御御御御御御御御御御御御御御御御御御御御	データは以下の順で並べ替えが可能です。バイト、セッション、脅威、 カウント、ユーザー、コンテンツ、アプリケーション、URL、悪意のあ るもの、安全なもの、グレイウェア、フィッシング、ファイル(名)、 データ、プロファイル、オブジェクト、ポータル、ゲートウェイ、プロ ファイル。使用できるオプションはウィジェットによって異なります。
御}}<{[防 御>防	

御御御御御御御御(a);> < };> < };	防 【防 防 【防 防 ⑤ 〕	
2	グラフ	グラフ形式の表示オプションには、ツリーマップ、折れ線グラフ、横棒 グラフ、積み上げ領域グラフ、積み上げ棒グラフ、円グラフ、および マップがあります。使用できるオプションはウィジェットによって異な り、インタラクション操作はグラフタイプによって異なります。たとえ ば、非標準ポートを使用するアプリケーションのウィジェットでは、ツ リーマップと折れ線グラフのいずれかを選択できます。 表示をドリルダウンするには、グラフをクリックします。クリックした エリアがフィルタになり、選択対象が拡大し、選択対象のより詳細な情 報を表示できます。
3	表	グラフの作成に使用されたデータの詳細がグラフの下の表に表示されま す。 表内の要素に対して、ローカルフィルタまたはグローバルフィルタをク リックして設定できます。ローカルフィルタを使用した場合、グラフが 更新され、表がフィルタでソートされます。 グローバルフィルタを使用した場合、フィルタに固有の情報のみを表示 するように ACC 全体の表示が切り替わります。
4	アクション	 ウィジェットのタイトルバーで使用できるアクションを次に示します。 ビューの最大化 – ウィジェットを拡大して、より大きな画面スペースで表示できます。最大化ビューでは、デフォルトのウィジェット・ビューに表示される上位 10 項目以上のものを表示できます。 ローカル フィルターの設定 - ウィジェット内の表示を絞り込むフィルターを追加できます。フィルターの操作 - ローカル フィルターとグローバル フィルター を参照してください。 ログにジャンプ – ログに直接移動できます (Monitor > Logs > <log-type>)。ログは、グラフがレンダリングされる期間を使用してフィルター処理されます。</log-type> ローカル フィルターとグローバル フィルターを設定すると、ログ クエリは期間とフィルターを連結し、フィルターセットに一致するログのみを表示します。 Export-グラフをPDFとしてエクスポートできます。

各ウィジェットの詳細は、「ACC の使用」を参照してください。
ACCのアクション

ACC 表示のカスタマイズおよび絞り込みを行うには、タブの追加と削除、ウィジットの追加と 削除、ローカルおよびグローバルフィルタの設定、ウィジットの操作ができます。

- タブおよびウィジットの処理
- フィルタの処理 ローカル フィルタおよびグローバル フィルタ

タブおよびウィジットの処理

以下のオプションで、タブとウィジェットの使用およびカスタマイズ方法について説明します。

カスタムタブの追加

- 1. タブリストの横にある追加(+)を選択します。
- 2. View Name[表示名] を追加します。この名前は、タブの名前として使用されます。最 大 10 個のカスタム タブを追加できます。

タブを編集する。

タブを選択し、タブ名の横にある「編集」をクリックして、タブを編集します。

例:<u>Threat Activity</u>.

タブをデフォルトとして設定する

- 1. タブを編集する。
- 金選択し、現在のタブをデフォルトとして設定します。ファイアウォールにログインするたびにこのタブが表示されます。

タブの状態を保存する

- 1. タブを編集する。
- 2. 🛅 を選択し、現在のタブの設定をデフォルトとして保存します。

設定した可能性があるすべてのフィルタを含め、タブの状態が HA ピア全体に同期されます。

タブをエクスポートする

- 1. タブを編集する。
- よ を選択し、現在のタブをエクスポートします。タブがコンピュータに.txt ファイル としてダウンロードされます。ファイルをダウンロードするには、ポップアップを有効 にする必要があります。

タブをインポートする

- 1. カスタムタブの追加
- 2. 📥 を選択し、タブをインポートします。
- 3. テキスト (.txt) ファイルを参照して選択します。

ビューに含まれているウィジェットを表示する。

- 1. ビューを選択して編集 (🖉) をクリックします。
- 2. Add Widgets[ウィジェットの追加] のドロップダウンリストから選択済みのウィジェットを確認します。

ウィジットまたはウィジット グループを追加する。

- 1. 新しいタブを追加するか、事前定義済みのタブを編集します。
- 2. Add Widget[ウィジェットの追加] から、追加したいウィジェットを選択します。最 大12個のウィジェットを選択可能です。
- (任意) 2 列レイアウトを作成するには、Add Widget Group(ウィジェット グループ の追加)を選択します。ウィジェットを 2 列表示画面にドラッグ アンド ドロップでき ます。ウィジットをレイアウトにドラッグすると、ウィジットをドロップするためのプ レースホルダが表示されます。

ウィジット グループに名前を付けることはできません。

タブ、ウィジェット、またはウィジェットグループを削除する。

- カスタム タブを削除するには、タブを選択して削除(🔤 🙍)をクリックします。
 - 事前定義済みのタブを削除することはできません。
- ウィジェットあるいはウィジェットグループを削除する場合は、タブを編集してから削除 ([X])をクリックします。削除を取り消すことはできません。

デフォルト表示をリセットする。

事前定義済みの表示 (Blocked Activity[ブロックされたアクティビティ] 表示など) で、1つ または複数のウィジットを削除できます。レイアウトをリセットし、タブに含まれるウィ ジェットセットをデフォルトに戻す場合、タブを編集してからReset View[ビューのリセッ ト] をクリックします。

フィルタの処理 – ローカル フィルタおよびグローバル フィルタ

詳細情報に焦点を合わせて、ACCに表示する情報を細かく制御する場合はフィルタを使用します。

Local Filters[ローカル フィルタ] - ローカル フィルタは特定のウィジットに適用されます。
 ローカル フィルタを使用すると、グラフを操作し、表示をカスタマイズできるため、情報
 を詳細まで掘り下げて、監視する必要がある情報に特定のウィジットでアクセスできます。

ローカルフィルタを適用する方法は2つあり、グラフまたは表内で属性をクリックする 方法と、ウィジェット内で Set Filter(フィルタの設定)を選択する方法があります。Set Filter(フィルタの設定)により、再起動後も持続するローカルフィルタを設定できます。

• Global filters[グローバルフィルタ] - グローバルフィルタはACC全体に適用されます。グローバルフィルタを使用して、自分が最も注目しているデータを中心に表示し、関係のない情報を現在の表示から除外できます。たとえば、特定のユーザーとアプリケーションに関連するすべてのイベントを表示するには、ユーザーのIPアドレスを適用し、アプリケーションを指定して、グローバルフィルタを作成します。これで、そのユーザーとアプリケーションに関連する情報のみをACC上のすべてのタブとウィジェットに表示できます。グローバルフィルタはログイン間で持続されません。

グローバルフィルタは次の3つの方法で適用できます。

- Set a global filter from a table[表からグローバルフィルタを設定する] 任意のウィジット内の 表から属性を選択し、その属性をグローバルフィルタとして適用します。
- Add a widget filter to a global filter (グローバル フィルタにウィジェット フィルタを追加する) 属性にカーソルを合わせ、その右側にある矢印のアイコンをクリックします。これにより、ウィジェットで使用されているローカル フィルタが昇格し、属性がグローバルに適用され、ACC のすべてのタブの表示が更新されます。
- Define a global filter[グローバルフィルタを定義する] ACCのGlobal Filters[グローバルフィルタ] ペインを使用してフィルタを定義します。

ローカル フィルタを設定する。

- グラフの下の表で、属性をクリックし、その属性をローカルフィルタとして適用することもできます。
 - 1. ウィジェットを選択し、フィルタ(♡)をクリックします。
 - 2. 適用するフィルタを追加()します。
 - 3. Apply[適用] をクリックします。このフィルタは、再起動後も持続します。
 - ウィジットに適用されているローカルフィルタの数がウィジット名の横に 示されます。

表からグローバル フィルタを設定する。

表の中の属性にカーソルを合わせ、その右側に表示される矢印をクリックします。

Global Filters [グローバル フィルタ] ペインを使用して、グローバル フィルタを設定します。 適用したいフィルタを追加(①)します。

ローカル フィルタをグローバル フィルタにプロモートする。

- 1. ウィジット内の任意の表で、属性をクリックします。これにより、属性がローカル フィルタとして設定されます。
- 2. フィルタをグローバルフィルタに昇格させる場合は、属性にカーソルを合わせ、その右 側にある矢印をクリックします。

フィルタを削除する。

削除(⊖)をクリックして、フィルタを削除します。

- Global filters[グローバルフィルタ] [グローバルフィルタ] ペインにあります。
- Local filters[ローカルフィルタ] フィルタ([♥]) をクリックして、Set Local Filters [ロー カルフィルタの設定]ダイアログを表示し、フィルタを選択して削除します。

すべてのフィルタをクリアする。

- Global filters[グローバルフィルタ]-グローバルフィルタをClear all[すべてクリア]します。
- Local filters[ローカルフィルタ] ウィジェットを選択し、フィルタ(♥) をクリックします。次に、Set Local Filters [ローカルフィルタの設定] ウィジェットでClear all[すべてクリア] をクリックします。

フィルタの条件を反転させる。

属性を選択し、フィルタ条件を反転(◎)させます。

- Global filters[グローバルフィルタ] [グローバルフィルタ] ペインにあります。
- Local filters[ローカルフィルタ] フィルタ(♡) をクリックして、[ローカルフィルタの設定]ダイアログを表示し、フィルタを追加し、その条件を反転させます。

使用中のフィルタを表示する。

- Global filters[グローバルフィルタ] 適用されているグローバルフィルタの数が [グローバルフィルタ] の下の左ペインに表示されます。
- Local filters[ローカルフィルタ] ウィジットに適用されているローカルフィルタの数が ウィジット名の横に表示されます。フィルタを表示する場合は、Set Local Filters[ローカ ルフィルタの設定] をクリックします。



監視

以下のトピックでは、ネットワーク上のアクティビティをモニターするのに使用できるファイア ウォール レポートとログについて説明します。

- Monitor > Logs [監視 > ログ]
- Monitor (監視) > External Logs (外部ログ)
- Monitor (監視) > Automated Correlation Engine (自動相関エンジン)
- Monitor > Packet Capture [監視 > パケット キャプチャ]
- Monitor > App Scope [監視 > アプリケーション スコープ]
- Monitor > Session Browser [監視 > セッション ブラウザ]
- Monitor (監視) > Block IP List (ブロック IP リスト)
- Monitor > Botnet [監視 > ボットネット]
- モニター > loTデバイス
- Monitor (監視) > PDF Reports (PDF レポート)
- Monitor > Manage Custom Reports [監視 > カスタム レポートの管理]
- Monitor > Reports [監視 > レポート]

Monitor > Logs [監視 > ログ]

以下のトピックでは、ログのモニターに関する追加の情報について説明します。

知りたい内容	以下を参照
ログの種類を詳しく知りたい	ログタイプ
ログのフィルター	ログアクション
ログのエクスポート	
個別のログエントリの詳細を表示した い	
ログの表示を変更する	
その他の情報をお探しですか?	ログのモニターと管理

ログタイプ

• 監視 > ログ

ファイアウォールはロールベースの管理権限に基づいて、すべてのログを表示します。閲覧権限 のある情報のみが表示されます。これは、表示するログのタイプによって変化します。管理者権 限の詳細は、「Device(デバイス)> Admin Roles(管理者ロール)」を参照してください。

ログタイプ	の意味
トラフィック	各セッションの開始と終了のエントリが表示されます。 各エントリには、日時、送信元ゾーン、宛先ゾーン、ア ドレスおよびポート、アプリケーション名、フローに 適用されるセキュリティルール名、ルールアクション (allow、deny、または drop)、入力/出力インターフェイ ス、バイト数、およびセッション終了理由などが記載され ます。
	[タイプ] 列は、そのエントリがセッションの開始または終 了のどちらのエントリなのか、またはセッションが拒否ま たは廃棄されたのかどうかを示します。「drop」は、トラ フィックをブロックしたセキュリティルールが適用され て「いずれか」のアプリケーションが指定されたことを示 し、「deny」はルールが適用されてある特定のアプリケー ションが識別されたことを示します。 アプリケーションが識別される前にトラフィックが廃棄さ れた場合(あるルールにより特定のサービスのトラフィッ

ログタイプ	の意味
	クがすべて廃棄された場合など)、そのアプリケーションは 「not-applicable」として表示されます。
	トラフィックログを掘り下げ、個別のエントリ、アーチ ファクトおよびアクションについて、より詳細な情報を表 示します。
	 詳細 だクリックすると、セッションに関する詳細な情報 (ICMP エントリを使用して同じ送信元と宛先間の複数のセッションを集約するかどうかなど)が表示されます (Count (繰り返し回数)値は1より大きくなります)。 アクティブな AutoFocus[™] ライセンスが付与されたファイアウォール上で、ログエントリに含まれるIP アドレス、ファイル名、URL、ユーザーエージェント、脅威名、またはハッシュの横にカーソルを合わせ、表示されたドロップダウンリスト マ デバイスを Quarantine List (隔離リスト) (Device (デバイス) > Device Quarantine (デバイスの隔離))に追加するには、デバイスのHost ID (ホストID) ドロップダウンを開いて{>Block Device (デバイスのブロック)を 選択します (ポップアップダイアログ内)
脅威	ファイアウォールで生成された各セキュリティアラーム のエントリが表示されます。各エントリには、日時、脅威 の名前または URL、送信元および宛先ゾーン、アドレス、 ポート、アプリケーション名、フローに適用するセキュリ ティルール名、およびアラームアクション (allow (許可)ま たは block (ブロック)) と重大度が含まれています。 Type (タイプ)の列には、「ウイルス」または「スパイ ウェア」などの脅威の種類が表示されます。Name (名前) の列には脅威の内容または URL、Category (カテゴリ)の 列には脅威のカテゴリ (「keylogger」など)または URLの カテゴリが表示されます。
	脅威ログを掘り下げ、個別のエントリ、アーチファクトお よびアクションについて、より詳細な情報を表示します。 • 詳細
	(らうしい しんしょう (ううしん ううしょう (ううしょう ううしょう ううしょう ううしゅう ううしゅう (そのエント ううしゅう (そのエント)

ログ タイプ	の意味
	リを使用して同じ送信元と宛先間の同じタイプの複数の 脅威を集約するかどうかなど) が表示されます(Count (繰 り返し回数) 値は1より大きくなります)。
	 アクティブな AutoFocus ライセンスが付与され たファイアウォール上で、ログエントリに含まれ る IPアドレス、ファイル名、URL、ユーザーエー ジェント、脅威名、またはハッシュの横にカーソ ルを合わせ、表示されたドロップダウンメニュー (・ ・<!--</th-->
	 ローカルパケットキャプチャが 有効な場合は、ダウンロード
	() をクリックして、キャプチャされたパケットを表示し ます。ローカルパケットキャプチャを有効にするに は、Objects(オブジェクト) > Security Profiles(セ キュリティプロファイル)のサブセクションを参照して ください。
	 脅威に関する詳細を表示したり、脅威の除外を脅威 ログから直接迅速に設定したりするには、Name(名 前)列で脅威名をクリックします。Exempt Profiles(プ ロファイルの免除)リストには、アンチウイルス、アン チスパイウェア、脆弱性のカスタム防御プロファイル がすべて表示されます。脅威シグネチャの除外を設定 するには、セキュリティプロファイル名の左のチェッ クボックスをオンにし、変更を保存します。IP アド レスの除外を追加するには(1つのシグネチャにつき 100 個までの IP アドレス)、セキュリティプロファ イルを強調表示して、Exempt IP Addresses(IP アド レスの免除)セクションに IP アドレスを追加し、OK をクリックして保存します。除外の確認または変更を 行うには、関連するセキュリティプロファイルに移 動して Exceptions(例外)タブをクリックします。例 えば、脅威タイプがvulnerability(脆弱性)である場合 は、Objects(オブジェクト) > Security Profiles(セキュリ ティプロファイル)> Vulnerability Protection(脆弱性防 御)を選択し、関連するプロファイルをクリックしてか らExceptions(例外)タブをクリックしてか
	 デバイスを Quarantine List (隔離リスト) (Device (デ バイス)、 Device Quaranting (デバイスの厚離)) に迫

デバイスを Quarantine List(隔離リスト)(Device(デバイス) > Device Quarantine(デバイスの隔離))に追加するには、デバイスのHost ID(ホストID)ドロップダ

ログタイプ	の意味
	ウンを開いて {>Block Device (デバイスのブロック)を 選択します(ポップアップダイアログ内)。
URL フィルタリング	Web サイトへのアクセス、およびユーザーが認証情報を Web サイトに送信できるかどうかを制御する URL フィルタ のログを表示します。
	どの URL カテゴリをブロックまたは許可するのか、どれ に認証情報の送信を許可または禁止するのかなど、URL フィルタリング設定を定義するには、Objects(オブジェ クト)> Security Profiles(セキュリティ プロファイル)> URL Filtering(URL フィルタリング)を選択します。URL の HTTP ヘッダー オプションをログに記録することもでき ます。
	アクティブな AutoFocus ライセンスが付与され たファイアウォール上で、ログエントリに含まれ る IPアドレス、ファイル名、URL、ユーザーエー ジェント、脅威名、またはハッシュの横にカーソ ルを合わせ、表示されたドロップダウンメニュー (・) をクリックして、その分析結果の AutoFocus インテリジェ ンス サマリーを開きます。
WildFire への送信	ファイアウォールが WildFire [™] 分析のために転送した ファイルおよび電子メール リンクのログを表示しま す。WildFire はサンプルを分析して分析結果を返すことが でき、これにはサンプルに割り当てられた WildFire 判定 (安全、マルウェア、グレイウェア、フィッシング)が含 まれます。Action (アクション)列を参照すると、ファイ アウォールがセキュリティ ポリシー ルールに基づいてファ イルを許可したかブロックしたかを確認できます。
	アクティブな AutoFocus ライセンスが付与されたファイア ウォール上で、ログ エントリに含まれる IPアドレス、ファ イル名、URL、ユーザー エージェント、脅威名、または (File Digest (ファイル ダイジェスト)列にある) ハッシュの横 にカーソルを合わせ、表示されたドロップダウン メニュー (・) をクリックして、その分析結果の AutoFocus インテリジェ ンス サマリー を開きます。
データのフィルタリング	特定のファイルタイプのアップロードまたはダウンロード を防ぐファイアウォールやブロッキングプロファイルに保 護されたエリアからの、クレジットカードや社会保障番号 などの機密情報の流出を防ぐように設定したデータフィル

ログタイプ	の意味
	タリングプロファイルが適用されたセキュリティーポリ シーのログを表示します。
	ログエントリの詳細情報にアクセスす る場合のパスワード保護を設定するに は、
	リックします。そこでバスワートを入力して OR をク リックします。データ保護パスワードの変更方法または削 除方法の手順の詳細は、「Device(デバイス)> Response Pages(応答ページ)」を参照してください。
	各セッションで1回のみ、システムから入力 を要求されます。
HIP マッチ	GlobalProtect [™] ゲートウェイが、エージェントによってレ ポートされた生 HIP データを定義済み HIP オブジェクトお よび HIP プロファイルと比較するときに特定する、すべて の HIP マッチを表示します。その他のログとは異なり、HIP マッチは、セキュリティ ポリシーと一致していないときで もログに記録されます。詳細は、「Network(ネットワー ク) > GlobalProtect > Portals(ポータル)」を参照してく ださい。
	デバイスを Quarantine List(隔離リスト)(Device(デバ イス) > Device Quarantine(デバイスの隔離))に追加す るには、デバイスのHost ID(ホストID)ドロップダウンを 開いて{>Block Device(デバイスのブロック)を選択します (ポップアップダイアログ内)。
GlobalProtect	GlobalProtect 接続ログを表示します。この情報を使用して、GlobalProtect ユーザーとそのクライアント OS バージョンを特定し、接続とパフォーマンスの問題のトラブルシューティングを行い、ユーザーが接続するポータルとゲートウェイを特定します。
	デバイスを Quarantine List(隔離リスト)(Device(デバ イス) > Device Quarantine(デバイスの隔離))に追加す るには、デバイスのHost ID(ホストID)ドロップダウンを 開いて{>Block Device(デバイスのブロック)を選択します (ポップアップダイアログ内)。
IP-Tag	タグが特定の IP アドレスにいつ、どのように適用された のかという情報を表示します。この情報を使用すれば、特 定の IP アドレスがいつ、なぜアドレスグループに配置さ れ、どのポリシールールがそのアドレスに影響を与えるの か判断することができます。ログには Receive Time (受信時

を

間)(セッションの最初および最後のパケットが到達した日時)、Virtual System (仮想システム)、Source IP-Address (信元 IP アドレス)、Tag (タグ)、Event(イベント)、Timeout (タイムアウト)、Source Name (送信元名)、Source Type (送 信元タイプ)が含まれます。 User-ID TM マッピング情報のソース、User-ID エージェントがマッピン グを実行したタイミング、マッピングが期限切れになるま での残り時間など、IP アドレスとユーザー名のマッピング に関する情報を表示します。この情報を使用すると、User ID の問題をトラブルシューティングしやすくなります。た とえば、ファイアウオールが誤ったポリシールールをユー ザーご通用している場合は、ログを参照して、そのユー ザーご通用している場合は、ログを参照して、そのユー ザーが正しい IP アドレスにマッピングされているかどう か、およびグループの関連付けが正しいかどうかを検証で きます。 復号 GlobalProtect セッションを含む、復号化なしプロファイル が制御するトラフィックの復号化セッションは広び登台 なしのセッションに関する情報を表示します。 デフォルトでは、ログには失敗した SSL 復号化ハンドシェ イクに関する情報が表示されます。Decryption Policy (復 号ポリシー ルールのOptions (オプション) で、正常完了 した SSL 復号ハンドシェイクのログを有効化することがで きます。ログには、脆弱なプロトコルや暗号スイートを識 別する上での豊富な情報が表示されます。1年 〜 交換、暗号 化、および認証アルゴリズム)、バイバス済復号化のアク ディビティ、復号化の失敗およびその原因 (不完全な証明 書チェーン、クライアント認証、固定された証明書等)、 セッション経了の理由など)。例えば、この情報を利用 して、膨弱なプロトコルやアルゴリズムを使用するサイトを 許可するかどうかを決定を行います。ビジネス上アクセス する必要のない脆弱なサイトをプロックする方がよい場合 があります。 ファイアウォールが復号化せず、No Decryption (復号化 なしプロファイル)を適用するトラフィックの場合、ログ には、サーバー証明書の検証の問題でブロックされたセッ ションが表示されます。。 デフォルトの復号ログのサイズは 32MB です。ただし、 大量のトラフィックを復号化する場合、あるいは正常	ログタイプ	の意味
User-ID TM マッピング情報のソース、User-ID エージェントがマッピン グを実行したタイミング、マッピングが期限切れになるま での残り時間など、IP アドレスとユーザー名のマッピング に関する情報を表示します。この情報を使用すると、User ID の問題をトラブルシューティングしやすくなります。た とえば、ファイアウォールが認ったポリシー ルールをユー ザーご適用している場合は、ログを参照して、そのユー ザーが正しい IP アドレスにマッピングされているかどう か、およびグループの関連付けが正しいかどうかを検証で きます。 復号 GlobalProtect セッションを含む、復号化なしプロファイル が制御するトラフィックの復号化セッションよび復号化 なしのセッションに関する情報を表示します。 デフォルトでは、ログには失敗した SSL 復号化ハンドシェ イクに関する情報が表示されます。Decryption Policy (復 号ポリシー ルールのOptions (オプション)で、正常完了 した SSL 復号ハンドシェイクのログを有効化することがで きます。ログには、脆弱なプロトコルや暗号スイートを識 別する上での豊富な情報が表示されます(キー交換、暗号 化、および認証アルゴリズム)、バイパス済復号化のアク ディビティ、復号化の失敗およびその原因(不完全な証明 書チェーン、クライアント認証、固定された証明書等)、 セッション総了の理由など)。例えば、この情報を利用し て、脆弱なプロトコルやアルゴリズムを使用するサイトを 許可するかどうかを決定を行います。ビジネス上アクセス する必要のない脆弱なサイトをブロックする方がよい場合 があります。 ファイアウオールが復号化せず、No Decryption (復号化 なしプロファイル)を適用するトラフィックの場合、ログ には、サーバー証明書の検証の問題でブロックされたセッ ションが表示されます。 デフォルトの復号ログのサイズは 32MB です。ただし、 大量のトラフィックを復号化する場合、あるいは正常		間) (セッションの最初および最後のパケットが到達した日 時)、Virtual System (仮想システム)、Source IP-Address (送 信元 IP アドレス)、Tag (タグ)、Event (イベント)、Timeout (タイムアウト)、Source Name (送信元名)、Source Type (送 信元タイプ) が含まれます。
 復号 GlobalProtect セッションを含む、復号化なしプロファイルが制御するトラフィックの復号化セッションおよび復号化なしのセッションに関する情報を表示します。 デフォルトでは、ログには失敗した SSL 復号化ハンドシェイクに関する情報が表示されます。Decryption Policy(復号ポリシールールのOptions(オプション)で、正常完了した SSL 復号ハンドシェイクのログを有効化することができます。ログには、脆弱なプロトコルや暗号スイートを識別する上での豊富な情報が表示されます(キー交換、暗号化、および認証アルゴリズム)、バイパス済復号化のアクティビティ、復号化の失敗およびその原因(不完全な証明書チェーン、クライアント認証、固定された証明書等)、セッション終了の理由など)。例えば、この情報を利用して、脆弱なプロトコルやアルゴリズムを使用するサイトを許可するかどうかを決定を行います。ビジネス上アクセスする必要のない脆弱なサイトをブロックする方がよい場合があります。 ファイアウォールが復号化せず、No Decryption(復号化なしプロファイル)を適用するトラフィックの場合、ログには、サーバー証明書の検証の問題でブロックされたセッションが表示されます。 デフォルトの復号ログのサイズは 32MB です。ただし、大量のトラフィックを復号化する場合、あるいは正常 	User-ID [™]	マッピング情報のソース、User-ID エージェントがマッピン グを実行したタイミング、マッピングが期限切れになるま での残り時間など、IP アドレスとユーザー名のマッピング に関する情報を表示します。この情報を使用すると、User- ID の問題をトラブルシューティングしやすくなります。た とえば、ファイアウォールが誤ったポリシー ルールをユー ザーに適用している場合は、ログを参照して、そのユー ザーが正しい IP アドレスにマッピングされているかどう か、およびグループの関連付けが正しいかどうかを検証で きます。
完了した SSL 復号化ハンドシェイクのログ記録を有効 にする場合は、ログサイズを増やす必要がある場合が	復号	GlobalProtect セッションを含む、復号化なしプロファイル が制御するトラフィックの復号化セッションおよび復号化 なしのセッションに関する情報を表示します。 デフォルトでは、ログには失敗した SSL 復号化ハンドシェ イクに関する情報が表示されます。Decryption Policy(復 号ポリシールールのOptions(オプション)で、正常完了 した SSL 復号ハンドシェイクのログを有効化することがで きます。ログには、脆弱なプロトコルや暗号スイートを識 別する上での豊富な情報が表示されます(キー交換、暗号 化、および認証アルゴリズム)、バイパス済復号化のアク ティビティ、復号化の失敗およびその原因(不完全な証明 書チェーン、クライアント認証、固定された証明書等)、 セッション終了の理由など)。例えば、この情報を利用し て、脆弱なプロトコルやアルゴリズムを使用するサイトを 許可するかどうかを決定を行います。ビジネス上アクセス する必要のない脆弱なサイトをブロックする方がよい場合 があります。 ファイアウォールが復号化せず、No Decryption(復号化 なしプロファイル)を適用するトラフィックの場合、ログ には、サーバー証明書の検証の問題でブロックされたセッ ションが表示されます。 デフォルトの復号ログのサイズは 32MB です。ただし、 大量のトラフィックを復号化する場合、あるいは正常 完了した SSL 復号化ハンドシェイクのログ記録を有効 にする場合は、ログサイズを増やす必要がある場合が

ログタイプ	の意味
	Settings(ログとレポートの設定)およびLog Storage(ロ グストレージ)クォータの編集)。割り当てされていない ログスペースがない場合は、復号化ログのサイズと他のロ グのサイズの間のトレードオフを検討します。ログの記録 が多いほど、ログが消費するリソースも増大します。
GTP	幅広い GTP 属性に関する情報を含むイベントベース ログを 表示します。アプリケーション、送信元と宛先のアドレス とタイムスタンプなど、次世代ファイアウォールが識別す る TCP/IP 情報に加えて、GTP イベント タイプ、GTP イベ ント メッセージ タイプ、APN、IMSI、IMEI、エンド ユー ザー IP アドレスが含まれます。
トンネル検査	各検査済みトンネル セッションの開始と終了のエントリが 表示されます。このログには、受信時間(セッションの最 初と最後のパケットが届いた日時)、トンネル ID、モニ ター タグ、セッション ID、トンネル トラフィックに適用 されたセキュリティ ルールなどが含まれます。詳細は、 「Policies(ポリシー) > Tunnel Inspection(トンネル検 査)」を参照してください。
SCTP	ステートフル検査、プロトコル検証、および SCTP トラ フィックのフィルタリングを実行している間に、ファイア ウォールによって生成されたログに基づいて、SCTP イベ ントおよびアソシエーションを表示します。SCTP ログに は、SCTP イベント タイプ、チャンク タイプ、SCTP 原因 コード、Diameter アプリケーション ID、Diameter コマン ドコード、およびチャンクなど、広範囲の SCTP やそのペ イロード プロトコル属性に関する情報が含まれています。 この SCTP 情報は、送信元および宛先アドレス、送信元お よび宛先ポート、ルール、タイムスタンプなど、ファイア ウォールが識別する一般的な情報に加えて提供されます。 詳細は、「Objects(オブジェクト) > Security Profiles(セ キュリティ プロファイル) > SCTP Protection(SCTP プロ テクション)」を参照してください。
設定	設定変更操作に関するエントリが表示されます。各エント リには、日時、管理者のユーザー名、変更を行ったユー ザーのIPアドレス、クライアントのタイプ (Webインター フェイスまたはCLI)、実行されたコマンドのタイプ、コマン ドが成功したか失敗したか、設定パス、および変更前後の 値が含まれています。

ログ タイプ	の意味
システム<:so>システム	各システム イベントのエントリが表示されます。各エント リには、日時、イベントの重大度、およびイベントの説明 が含まれています。
アラーム	アラーム ログは、システムによって生成されたアラームの 詳細情報を記録します。このログの情報は、Alarms [アラー ム] ウィンドウでも報告されます。「アラーム設定の定義」 を参照してください。
authentication	認証ポリシールールによってアクセスが制御されている ネットワークリソースに、エンドユーザーがアクセスし ようとしたときに発生する認証イベントに関する情報が表 示されます。この情報を使用すると、アクセスの問題をト ラブルシューティングしやすくなり、必要に応じて認証ポ リシーを調整できるようになります。相関オブジェクトと ともに認証ログを使用すると、総当たり攻撃など、ネット ワークでの不審なアクティビティを特定することもできま す。 必要に応じて、認証タイムアウトをログに記録するように 認証ルールを設定できます。これらのタイムアウトは、
	リソースに何度でもアクセスできるという、その間 リソースに何度でもアクセスできるという、その期間に関 連します。タイムアウトに関する情報を確認すると、タイ ムアウトを調整するかどうか、およびその調整方法を判断 できます。
	 システムログには、GlobalProtect に関連する 認証イベント、および Web インターフェイスへの管理者アクセスに関連する認証イベントが記録されます。
統合	トラフィック、脅威、URLフィルタリング、WildFireへ の送信、データフィルタリングログエントリの最新情報 を一つの画面で表示します。総合ログビューでは、それ ぞれのログを個別に検索するかわりに、様々なタイプ のログをまとめて検証したりフィルタをかけることがで きます。または、フィルタフィールドの左にある矢印 をクリックして、traffic(トラフィック)、threat(脅 威)、url、data(データ)、および(または)wildfire を選 択することで、表示されるログタイプを指定することがで きます。
	アクティノな AutoFocus フイセンスか付与され たファイアウォール上で、ログ エントリに含まれ

ログタイプ	の意味
	る IPアドレス、ファイル名、URL、ユーザー エー ジェント、脅威名、またはハッシュの横にカーソ ルを合わせ、表示されたドロップダウン メニュー (・) をクリックして、その分析結果の AutoFocus インテリジェ ンス サマリー を開きます。
	ファイアウォールはロールベースの管理権限に基づいて、 すべてのログを表示します。統合ログを表示する際は、閲 覧権限のある情報のみが表示されます。例えば、WildFireへ の送信ログを閲覧する権限のない管理者が統合ログを表示 した場合は、WildFireへの送信ログは表示されません。管理 者権限の詳細は、「Device(デバイス)> Admin Roles(管 理者ロール)」を参照してください。
	AutoFocus 脅威インテリジェンス ポー タルで設定された統合ログを使用でき ます。AutoFocus 検索をセットアップ し、AutoFocus 検索フィルタを統合ログフィ ルタフィールドに直接追加できます。
	デバイスを Quarantine List(隔離リスト)(Device(デバ イス) > Device Quarantine(デバイスの隔離))に追加す るには、デバイスのHost ID(ホストID)ドロップダウンを 開いて{>Block Device(デバイスのブロック)を選択します (ポップアップダイアログ内)。

ログアクション

以下の表ではログアクションについて説明します。

操作	の意味
ログのフィ ルター	各ログページの上部にはフィルタフィールドがあります。フィールドにはIPア ドレスや時間範囲などの分析結果を入力し、一致するログエントリを検索する ことができます。フィールドの右側にあるアイコンから、フィルタの適用、ク リア、作成、保存、ロードを行うことができます。

操作	の意味	
	• フィルタの作成:	
	 ログエントリ内の分析結果をクリックし、その分析結果をフィルタに追加します。 	
	● Add[追	
	加](をクリックして、新しい検索基準を定義します。それぞれの一致条件に ついて、検索のタイプ(andまたはor)を指定するConnector[条件式]を 選択し、検索を行うAttribute[属性]を指定し、検索の範囲をOperator[演 算子]で定義し、ログエントリから探したいValue[値]を選択します。そ れぞれの一致条件をフィルタフィールドにAdd[追加]し、入力が終わっ たらフィールドをClose[閉じ]ます。以上が完了したらフィルタを適用 (→ できます。)
	 構文エラーを防ぐため、Value[値]の文字列が、hasまたはinなどのOperator[演算子]を含む場合、文字列を引用符で囲む必要があります。例えば、宛先国のフィルタリングを行いINDIAを検索する際にValue[値]としてINを使う場合は、フィルタを(dstloc eq "IN")と入力します。 	
	(receive_time in last-60-seconds)のログフィルタにより、表示されるログエントリおよびログページを時間とともに増加あるいは減少するように設定することができます。	
	 フィルタを適用 - 現在のフィルタに一致するロ グエントリを表示する場合は、フィルタを適用 	
	$(\rightarrow$)
	をクリックします。	
	● フィルタをクリア - フィルタフィールドをク リアする場合は Clear Filter [フィルタをクリ	
	77 71 (X)
	をクリックします。	,
	• フィルタを保存 - フィルタを保存	
)
	を選択し、名前を人力して OK をクリックします。	
	 休存しにノイルタを使用 - 休存したノイルタをノイー ルドに追加する場合は、Load Filter 「フィルタをロー 	
	ド] (ふ をクリックします。)

操作	の意味	
ログのエク スポート	現在のフィルタに一致したすべてのログをCSV形式のレ ポートにエクスポートする場合は、CSVでエクスポート (をクリックし、Download file[ファイルをダウンロード]します。レポートには デフォルトで最大2,000行のログを含むよう設定されています。CSV レポート の行数制限を変更する場合は、Device(デバイス) > Setup(セットアップ) > Management(管理) > Logging and Reporting Settings(ログとレポート の設定) > Log Export and Reporting(ログのエクスポートとレポート)を開 き、新しい Max Rows in CSV Export(CSV エクスポートの最大行数)を入力 します。)
ポリシー ア クションの 強調表示	 アクションと一致するログエントリを強調表示する場合に選択します。フィルタリングされたログは、次の色で強調表示されます。 緑 - 許可 黄 - 継続またはオーバーライド 赤 - 却下、ドロップ、drop-icmp、st-client、reset-server、reset- both、block-continue、block-override、block-url、drop-all、sinkhole 	-
ログの表示を変更する	 ログの表示をカスタマイズするには: 表示ログの自動更新間隔を変更する場合は、ドロップダウンリストから間隔を選択します(60 seconds[60 秒]、30 seconds[30 秒]、10 seconds[10 秒]、またはManual[手動])。 ページに表示されるログの数と順序を変更する - ログエントリは、10ページのブロック単位で取得されます。 ページの下部にあるページ送り機能を使用して、ログリスト内を移動します。 ページあたりのログエントリの数を変更するには、各ページのドロップダウンリストから行数を選択します(20、30、40、50、75、または100)。 結果を昇順または降順でソートするには、ASC または DESC ドロップダウンリストを使用します。 IP アドレスをドメイン名に解決する - Resolve Hostname(ホスト名の解決)をオンにすると、外部 IP アドレスがドメイン名に解決されます。 ログの表示順を変更する - ログを、受信時間が最新のものから降順で表示する場合はDESC[降順]を選択します。 	-
個別のログ エントリの	 各ログエントリに関する情報を表示するには: ログの詳細を表示する場合、エントリの詳細 ()

操作	の意味	
詳細を表示 する	クリックします。Adress[アドレス] ページで、送信元または宛先の IPアド レスから名前へのマッピングを定義している場合、IPアドレスの代わりに そのドメインまたはユーザー名が表示されます。関連付けられている IP ア ドレスを表示するには、名前の上にカーソルを移動します。	•
	 アクティブな AutoFocus ライセンスが付与されたファイア ウォール上で、ログエントリに含まれる IP アドレス、ファ イル名、URL、ユーザーエージェント、脅威名、またはハッ シュにカーソルを合わせ、表示されたドロップダウン リスト (をクリックして、その分析結果の AutoFocus インテリジェンス サマリーを 開きます。)

Monitor (監視) > External Logs (外部ログ)

Traps[™] Endpoint Security Manager (ESM) から、Panorama[™] が管理するログ コレクタに取り 込まれたログを表示するには、このページを使用します。Panorama で Traps ESM ログを表示す るには、次の手順を実行します。

- Traps ESM サーバーで、Panorama を Syslog サーバーとして設定し、Panorama に転送する ためのロギングイベントを選択します。イベントには、セキュリティ関連のイベント、ポリ シーの変更、エージェントや ESM サーバーのステータス変更、設定変更などがあります。
- 1つ以上の Managed Log Collector を使用して Panorama モードでデプロイされた Panorama で、ログインジェスト プロファイル (Panorama > Log Ingestion Profile (ログインジェスト プロファイル))を設定し、そのプロファイルを Traps ESM ログを格納する Collector Group (Panorama > Collector Groups [Panorama > コレクタ グループ]) にアタッチします。

外部ログはデバイス グループに関連付けられていないため、外部ログは**Device Group**を選択した場合のみ表示される:**All**(すべて)ログはファイアウォールから送信されないためです。

ログタイプ	の意味
監視 > External Logs (外部ログ) > Traps ESM (ESMをトラッ プします) > 脅威	この脅威イベントには、Traps エージェントにより報告されたすべて の防御イベント、通知イベント、暫定イベント、検出後イベントが含 まれます。
監視 > External Logs (外部ログ) > Traps ESM (ESMをトラッ プします) > システム	ESM サーバー システム イベントには、ESM のステータス、ライセン ス、ESM テクニカル サポート ファイル、および WildFire との通信に 関連する変更が含まれます。
監視 > External Logs (外部ログ) > Traps ESM (ESMを トラップします) > Policy(ポリシー)	ポリシー変更イベントには、ルール、保護レベル、コンテンツ更新、 ハッシュ制御ログ、および判定への変更が含まれます。
監視 > External Logs (外部ログ) > Traps ESM (ESMをトラッ プします) > エージェ ント	エンドポイントで発生するエージェント変更イベントには、コンテン ツ更新、ライセンス、ソフトウェア、接続状態、ワンタイムアクショ ンルール、プロセスとサービス、および検疫済みファイルへの変更 が含まれます。
監視 > External Logs (外部ログ) > Traps ESM (ESMをトラッ	ESM 設定変更イベントには、ライセンス、管理ユーザーと管理ロール、プロセス、制限設定、および条件へのシステム規模の変更が含まれます。

ログタイプ	の意味
プします) > コンフィ グ	

Panorama は、エンドポイント上の個々のセキュリティ イベントをネットワーク上のイベントと 相関させて、エンドポイントとファイアウォール間の疑わしいまたは悪意のあるアクティビティ を追跡できます。Panorama が識別する相関イベントを表示するには、「[Monitor] > [自動相関 エンジン] > [相関されたイベント]」を参照してください。

Monitor (監視) > Automated Correlation Engine (自動相関エンジン)

自動相関エンジンは、ネットワーク上のパターンを追跡し、疑わしい動作への拡散を示している イベントや、有害なアクティブティに達したイベントの相関付けを行います。このエンジンは、 個人のセキュリティ アナリストの役割を果たすものであり、ファイアウォール上のさまざまな ログ セットに分離されたイベントを調査し、特定のパターンがないかデータをクエリして、点 を結んで全体像を作り上げます。これにより、実用的な情報を得ることができます。

相関エンジンは、相関されたイベントを生成する相関オブジェクトを使用します。相関された イベントによって証拠が照合されます。これにより、関連がないように見えるいくつかのネット ワーク イベント間の共通点を追跡できるため、インシデント対応の機会が与えられます。

以下のモデルは自動相関エンジンをサポートします。

- Panorama M-Series アプライアンスおよびバーチャル アプライアンス
- PA-3200 シリーズ ファイアウォール
- PA-3400 シリーズ ファイアウォール
- PA-5200 シリーズ ファイアウォール
- PA-5400 シリーズ ファイアウォール
- PA-7000 シリーズ ファイアウォール

知りたい内容	以下を参照			
 相関オブジェクトとは何です か?	[Monitor] > [自動相関エンジン] > [相関オブジェクト]			
相関されたイベントとは何で すか?	[Monitor] > [自動相関エンジン] > [相関されたイベント]			
相関一致での一致の証拠をど こで確認できますか?				
相関一致のグラフィック表示 をどのように表示できますか?	ACC で Compromised Hosts(浸入されたホスト)ウィジットを表示してください。			
その他の情報をお探しです か?	自動相関エンジンの使用			

[Monitor] > [自動相関エンジン] > [相関オブジェクト]

エクスプロイトおよびマルウェアの拡散方法の進歩に対抗するため、相関オブジェクトはファイ アウォールでのシグネチャベースのマルウェア検出機能を拡張します。相関オブジェクトは、各 種ログ セット全体にわたって疑わしい動作パターンを識別するためのインテリジェンスを提供 し、調査に必要な証拠を収集して、イベントにすばやく応答します。

相関オブジェクトは、マッチングパターンや、検索を実行するために使用するデータソース、 パターン検索の対象期間を指定する定義ファイルです。パターンは、データソースをクエリする Boolean 型の条件構造です。各パターンに重大度およびしきい値が割り当てられます。しきい値 は、定義された期間内にパターンマッチが発生する回数です。パターンマッチが発生すると、 相関イベントがログに記録されます。

検索を実行するために使用するデータ ソースには、アプリケーション統計、トラフィック、ト ラフィック サマリー、脅威サマリー、脅威、データ フィルタリング、URL フィルタリングの各 ログを含めることができます。たとえば、相関オブジェクトの定義には、感染したホストの証 拠やマルウェア パターンの証拠がないかログをクエリするための一連のパターンのほか、トラ フィック内でのマルウェアの横方向の移動、URL フィルタリング、および脅威ログのパターン を含めることができます。

相関オブジェクトは Palo Alto Networks[®] により定義され、コンテンツ更新と共にパッケージ化 されます。コンテンツ更新を取得するには、有効な脅威防御ライセンスが必要です。

デフォルトでは、すべての相関オブジェクトが有効になっています。オブジェクトを無効化する 場合は、オブジェクトを選択して **Disable**[無効化]をクリックします。

相関オブジェ クト フィール ド	の意味
名前およびタ イトル	ラベルは、相関オジェクトで検出するアクティビティのタイプを示します。
ID	一意の番号を使用して相関オブジェクトを識別します。この番号は、6000 番 台です。
カテゴリ	ネットワーク、ユーザー、またはホストに与える脅威または損害の種類を要 約したもの。
状態	状態は、相関オブジェクトが有効 (アクティブ) か無効 (非アクティブ) かを示 します。
の意味	これには、ファイアウォールまたは Panorama でログを分析するための対象 となる一致条件を指定します。これは、有害なアクティビティまたはホスト の疑わしい動作を識別するために使用する拡散パターンまたは進捗パスを記 述するものです。

[Monitor] > [自動相関エンジン] > [相関されたイベント]

相関されたイベントはファイアウォールおよび Panorama での脅威検出機能を拡張し、ネット ワーク上のユーザーやホストの疑わしい動作や異常な動作の証拠を収集します。 相関オブジェクトを使用すると、特定の条件または動作を中心にして、複数のログソースにわたって共通点を追跡できます。相関オブジェクトに指定した一連の条件がネットワーク上で確認されると、各一致が、相関されたイベントとしてログに記録されます。

項目	の意味
一致時間	相関オブジェクトが一致をトリガーした時間。
更新時間	一致が最後に更新されたタイムスタンプ。
オブジェクト名	一致をトリガーした相関オブジェクトの名前。
送信元アドレス	トラフィックの送信元ユーザーの IP アドレス。
Source User (送信元ユー ザー)	ディレクトリ サーバーからのユーザーおよびユーザー グループの情報 (User-ID [™] が有効な場合)。
重要度	発生した損害の程度に基づいてリスクを分類するレベル。
概要	相関されたイベントに関して収集された証拠を要約する説明。
ホストID	デバイスの Host ID (ホスト ID) です。 デバイスをQuarantine List (隔離リスト) に追加するには (Device (デ バイス) > Device Quarantine (デバイスの隔離))、デバイスのHost ID (ホスト ID)の横の下矢印をクリックして、表示されるポップアップ ウィンドウでBlock Device (デバイスのブロック)を選択します。

相関されたイベントには、以下の表で示されている詳細が含まれます。

詳細ログビューを表示する場合は、エントリの詳細(

(

(

)をクリックします。詳細ログビュー

には、一致に関するすべての証拠が含まれます。

タブ	の意味
一致情報	Object Details [オブジェクトの詳細] - 一致をトリガーした相関オブジェクトに関する情報を提供します。相関オブジェクトの詳細は、「Monitor(監視) > Automated Correlation Engine(自動相関エンジン) > Correlation Objects(相関オブジェクト)」を参照してください。
	Match Details[一致の詳細] - 一致時間、一致の証拠の最終更新時間、イベントの重大度、イベントのサマリーを含む、一致の詳細のサマリー。

タブ	の意味
Match Evidence [一 致の根拠]	このタブには、相関されたイベントを裏付けるすべての証拠が含まれます。 セッションごとに収集された証拠に関する詳細情報が表示されます。

Correlated Events(相関されたイベント) タブの情報のグラフィック表示を参照してくださ い。ACC > Threat Activity(脅威アクティビティ)タブの Compromised Hosts(侵害されたホス ト)ウィジェットを参照してください。Compromised Hosts[侵入されたホスト]ウィジットで は、表示が送信元ユーザーと IP アドレスによって集約され、重大度でソートされます。

相関されたイベントがログに記録されたときの通知を設定するには、Device(デバイス) > Log Settings(ログ設定)タブまたは Panorama > Log Settings(ログ設定)タブに移動します。

Monitor > Packet Capture [監視 > パケット キャプチャ]

すべての Palo Alto Networks ファイアウォールにパケット キャプチャ (pcap) 機能が組み込ま れており、これを使用して、ファイアウォールのネットワーク インターフェイスを通過するパ ケットをキャプチャできます。その後、キャプチャしたデータをトラブルシューティングの目的 で使用したり、キャプチャしたデータを使用してカスタム アプリケーション シグネチャを作成 したりできます。



パケット キャプチャ機能を使用すると CPU に大きな負荷がかかるため、ファイア ウォールのパフォーマンスが低下する可能性があります。必要な場合にのみ、この 機能を使用してください。また、必要なパケットを収集した後は、この機能を必ず オフにしてください。

知りたい内容	以下を参照
ファイアウォールでパケット をキャプチャするために使用 できる他の方法は?	パケット キャプチャの概要
カスタム パケット キャプチャ を生成するには?	カスタム パケット キャプチャの構成要素
ファイアウォールで脅威が検 出されたときにパケット キャ プチャを生成するには?	脅威パケット キャプチャの有効化
パケット キャプチャをダウン ロードする場所は?	パケット キャプチャの概要

その他の情報をお探しですか?

 セキュリティ プロファイル に対して拡張パケット キャ プチャを有効にします。 	Device > Setup > Content-ID [デバイス > セットアップ > Content-ID]
 パケットキャプチャを使用してカスタムアプリケーションシグネチャを記述します。 	カスタム アプリケーションと脅威シグネチャ を参照してく ださい。
 パケットキャプチャをファ イアウォール管理者が表示 することを禁止します。 	「Web インターフェイス管理者のアクセス権限」を定義し ます。
 例を参照 	「パケット キャプチャの実行」を参照してください。

パケット キャプチャの概要

カスタム パケット キャプチャや脅威パケット キャプチャを実行するように Palo Alto Networks ファイアウォールを設定できます。

- Custom Packet Capture(カスタムパケットキャプチャ) すべてのトラフィックのパケットをキャプチャしたり、定義したフィルタに基づいてトラフィックのパケットをキャプチャしたりできます。たとえば、特定の送信元および宛先の IP アドレスまたはポートに対するパケットのみをキャプチャするようにファイアウォールを設定できます。これらのパケットキャプチャを使用して、ネットワークトラフィック関連の問題をトラブルシューティングしたり、アプリケーション属性を収集してカスタムアプリケーションシグネチャを作成したりできます(Monitor(監視) > Packet Capture(パケットキャプチャ))。ステージ(ドロップ、ファイアウォール、送受信)に基づいてファイル名を定義し、pcap が完了したら、Captured Files(キャプチャされたファイル)セクションで pcap をダウンロードします。
- Threat Packet Capture(脅威パケットキャプチャ) ファイアウォールでウイルス、スパ イウェア、または脆弱性が検出された場合にパケットをキャプチャします。この機能は、ア ンチウイルス、アンチスパイウェア、および脆弱性防御のセキュリティプロファイルで有効 にします。これらのパケットキャプチャによって、脅威を取り巻く状況が提供されるため、 攻撃が成功したかどうかを判断したり、攻撃者が使用した方法について詳細を確認したり できます。脅威に対するアクションを許可または通知するように設定する必要があります。 これを設定しない場合、脅威がブロックされ、パケットをキャプチャできません。このタイ プのパケットキャプチャは、Objects(オブジェクト) > Security Profiles(セキュリティ プロファイル)で設定します。pcap をダウンロード(↓)する場合は、Monitor(監視) > Threat(脅威)を選択します。

カスタムパケット キャプチャの構成要素

以下の表で、**Monitor**(監視) > **Packet Capture**(パケット キャプチャ)ページの構成要素について説明します。これらを使用して、パケット キャプチャの設定、パケット キャプチャの有効化、パケット キャプチャ ファイルのダウンロードを行います。

🚺 PA-220	DASHBOARD	ACC M	ONITOR	POLICIES	OBJECTS	NETWORK	DEVICE	Commit ~
								G (?
✓ G Logs 正 Traffic 同 Threat	Configure Filte	ering ters			Captured	Files	($\rightarrow \times$
₩IdFire Submissions ➡ WidFire Submissions ➡ Data Filtering ➡ HIP Match ➡ Hor Match ➡ Hor Match ➡ Ion Parag IS User-ID ➡ Decryption ➡ Tunnel Inspection ➡ Decryption	[0/4 Filters Se Filtering Configure Cap Packet Capture Q STAGE	t) OFF Pre-Pars turing ON FILE	e Match	OFF	File N	IAME	DATE	SIZE(MB)
System System Alarms Unified Packet Capture App Scope Summary Captor Change Monitor Threat Monitor Threat Monitor								

カスタムパ ケット キャプ チャの構成要 素	設定場所	の意味
フィルタの管 理	フィルタリングの設定	カスタムパケットキャプチャを有効にする場合、 フィルタを定義して、そのフィルタと一致するパ ケットのみをキャプチャする必要があります。こ れにより、pcap内で必要な情報を容易に見つけ ることができます。また、ファイアウォールでパ ケットキャプチャを実行するために必要とされる 処理能力を低減できます。
		Add[追加] をクリックし、新しいフィルタを追加 して、以下のフィールドを設定します。
		 ■ ID – フィルタの ID を入力または選択します。
		 Ingress Interface[入力インターフェイス] – どの入力インターフェイス上でトラフィックをキャプチャするかを選択します。
		 Source[送信元] – キャプチャするトラフィックの送信元 IP アドレスを指定します。
		 Destination[宛先] – キャプチャするトラフィックの宛先 IP アドレスを指定します。
		 Src Port[送信元ポート] – キャプチャするトラ フィックの送信元ポートを指定します。
		 Dest Port[宛先ポート] – キャプチャするトラ フィックの宛先ポートを指定します。

カスタムパ ケット キャプ チャの構成要 素	設定場所	の意味
		 Proto[プロトコル] – フィルタリングするプロトコル番号を指定します (1~255)。たとえば、ICMP のプロトコル番号は 1 です。 Non-IP[非 IP] – 非 IP トラフィックの処理方法を選択します (すべての IP トラフィックを除外する、すべての IP トラフィックを含める、IP トラフィックのみを含める、または IP フィルタを含めない)。非 IP トラフィックの例として、ブロードキャストや AppleTalk があります。 IPv6 – IPv6 パケットをフィルタに入れる場合は、このオプションをオンにします。
フィルタリン グ	フィルタリングの設定	フィルタの定義が終了したら、Filtering[フィルタ リング] をONに設定します。フィルタリングが OFF の場合、すべてのトラフィックがキャプチャ されます。
事前解析一致	フィルタリングの設定	このオプションの目的は、トラブルシューティン グを詳細に行うことです。パケットが入力ポート に入ると、いくつかの処理ステップを経て、事前 設定されたフィルタと一致するかどうか解析され ます。 何らかの障害によって、パケットがフィルタリン グ段階に到達しない場合があります。たとえば、 ルート検索に失敗した場合などに起こります。 Pre-Parse Match [事前解析一致] 設定を ON に設定 すると、システムに入力されるすべてのパケット に対して肯定一致がエミュレートされます。これ により、ファイアウォールはフィルタリングプロ セスに到達していないパケットをキャプチャでき るようになります。パケットがフィルタリング段 階に到達できれば、フィルタ設定に応じて処理さ れ、フィルタリング基準と一致しなければ破棄さ わます
パケット キャプチャ	キャプチャの設定	切り替えスイッチをクリックして、パケット キャ プチャを ON(オン)または OFF(オフ)にしま す。

カスタム パ ケット キャプ チャの構成要 素	設定場所	の意味
		少なくとも1つのキャプチャ ステージを選択する 必要がありますAdd[追加] をクリックし、以下を 指定します。
		• Stage[ステージ] – パケットをキャプチャする 時点を示します。
		 drop – パケット処理でエラーが生じ、パケットが破棄される時点を指定します。
		 firewall – パケットにセッション一致がある か、セッションの最初のパケットが正常に 作成される時点。
		 receive[受信] – データプレーン プロセッサ でパケットが受け取られる時点を指定しま す。
		 transmit[転送] – データプレーン プロセッ サでパケットが送信される時点を指定しま す。
		 File[ファイル] – キャプチャ ファイル名を指定 します。ファイル名は文字で始める必要があり ます。また、文字、数字、ピリオド、アンダー スコア、またはハイフンを使用できます。
		 Packet Count[パケット数] – キャプチャが停止 するまでの最大パケット数を指定します。
		 Byte Count (バイト数) – キャプチャが停止 するまでの最大バイト数を指定します。
キャプチャされたファイル	キャプチャされたファ イル	ファイアウォールで以前に生成されたカスタムパ ケット キャプチャのリストが含まれます。ファ イルをクリックすると、ファイルがコンピュー タにダウンロードされます。パケットキャプ チャを削除する場合は、削除したいものを選択 し、 Delete [削除] します。
		 File Name[ファイル名] – パケット キャプチャ ファイルのリストが表示されます。ファイル 名は、キャプチャ ステージに対して指定した ファイル名に基づきます。
		• Date[日付] – ファイルが生成された日付。
		 Size (MB)[サイズ (MB)] – キャプチャ ファイル のサイズ。

カスタム パ ケット キャプ チャの構成要 素	設定場所	の意味	
		パケットキャプチャをオンに切り替えて、その 後オフに切り替えた後に、リスト上に新しいす べての PCAP ファイルを表示する場合は、更新 (をクリックする必要があります。)
すべての設定 をクリア	設定	パケット キャプチャをオフにして、すべてのパ ケット キャプチャ設定をクリアするには、Clear All Settings[すべての設定をクリア] をクリックし ます。	
		これを行っても、セキュリティプロファイルに設定されたパケットキャプチャはオフになりません。セキュリティプロファイルでパケットキャプチャを有効にする方法の詳細は、「脅威パケットキャプチャの有効化」を参照してください。	

脅威パケット キャプチャの有効化

• Objects (オブジェクト) > Security Profiles (セキュリティ プロファイル)

ファイアウォールで脅威を検出したときにパケットをキャプチャできるようにするには、セキュ リティ プロファイルでパケット キャプチャ オプションを有効にします。

まず、**Objects**(オブジェクト) > **Security Profiles**(セキュリティ プロファイル)を選択し、 以下の表の説明に従って目的のプロファイルを変更します。

セキュリティ プ ロファイルのパ ケット キャプ チャ オプション	場所
Antivirus [アン チウイルス]	カスタムのアンチウイルス プロファイルを選択し、Antivirus[アンチウイル ス] タブで Packet Capture[パケットキャプチャ] を選択します。
アンチスパイ ウェア	カスタムのアンチスパイウェア プロファイルを選択し、DNS Signatures[DNS シグネチャ] タブをクリックします。Packet Capture[パ ケット キャプチャ] ドロップダウンリストで single-packetまたは extended-captureを選択します。

セキュリティ プ ロファイルのパ ケット キャプ チャ オプション	場所
脆弱性防御	カスタムの脆弱性防御プロファイルを選択し、Rules[ルール] タブ で、Add[追加] をクリックして新しいルールを追加するか、既存のルールを 選択します。次に、Packet Capture[パケット キャプチャ] ドロップダウン リストで single-packet または extended-capture を選択します。

アンチスパイウェアおよび脆弱性防御のプロファイルでは、例外時のパケットキャ プチャを有効にすることもできます。Exceptions[例外] タブをクリックし、シグネ チャのPacket Capture [パケットキャプチャ] 列でドロップダウンリストをクリック し、single-packetまたはextended-captureを選択します。

(任意)キャプチャした(グローバル設定に基づく)パケット数に基づいて脅威パケットキャ プチャの長さを定義するには、Device(デバイス) > Setup(セットアップ) > Content-IDを 選択し、Content-IDTM Settings(Content-IDTM 設定)セクションで Extended Packet Capture Length (packets)(拡張パケット キャプチャ長(パケット))フィールドを変更します(1 ~ 50 の範囲、デフォルトは 5)。

セキュリティ プロファイルでパケット キャプチャを有効にしたら、プロファイルがセキュリ ティ ルールに含まれていることを確認する必要があります。セキュリティ プロファイルをセ キュリティ ルールに追加する方法の詳細は「セキュリティ ポリシーの概要」を参照してくださ い。

セキュリティプロファイルでパケットキャプチャが有効化されている際にファイアウォールが脅 威を検出した場合、パケットキャプチャをダウンロード(↓)あるいはエクスポートすることが できます。

Monitor > App Scope [監視 > アプリケーション スコー プ]

以下のトピックでは、アプリケーション スコープの機能について説明します。

- アプリケーションスコープの概要
- アプリケーション スコープのサマリー レポート
- アプリケーション スコープの変化モニター レポート
- アプリケーションスコープの脅威モニターレポート
- アプリケーションスコープの脅威マップレポート
- アプリケーション スコープのネットワーク モニター レポート
- アプリケーション スコープのトラフィック マップ レポート

アプリケーション スコープの概要

アプリケーション スコープのレポートには、ネットワークの以下の内容がグラフ表示されま す。

- アプリケーション使用状況とユーザー アクティビティの変化
- ネットワーク帯域幅の大部分を占有しているユーザーやアプリケーション
- ネットワークの脅威

アプリケーションスコープのレポートを使用すると、異常な動作や予期しない動作をすばやく 見つけて、問題のある動作を特定できます。レポートはそれぞれ、ネットワークに関する動的 でユーザーがカスタマイズ可能なウィンドウに表示されます。レポートには、表示するデータ や範囲を選択するオプションがあります。Panorama では、表示される情報のData Source[デー タ ソース]を選択することもできます。デフォルトのデータソース (新しいPanoramaインストー ルの場合) では、管理対象ファイアウォールによって転送されたログを格納しているPanoramaの ローカルデータベースが使用されます。アップグレードの場合、デフォルトのデータソース はRemote Device Data[リモートデバイスデータ] (管理対象ファイアウォールのデータ) になり ます。管理対象ファイアウォールから直接データの集約ビューを取得および表示するには、ソー スを Panorama から Remote Device Data (リモート デバイス データ) に切り替える必要があり ます。

チャートの線や棒にポインタを置くかクリックすると、ACC に切り替わり、特定のアプリケー ション、アプリケーション カテゴリ、ユーザー、またはソースに関する詳しい情報が示されま す。

アプリケーション コマ ンド センターのチャー ト	の意味
概要	アプリケーション スコープのサマリー レポート

アプリケーション コマ ンド センターのチャー ト	の意味
変化モニター	アプリケーション スコープの変化モニター レポート
脅威モニター	アプリケーション スコープの脅威モニター レポート
脅威マップ	アプリケーション スコープの脅威マップ レポート
ネットワーク モニター	アプリケーション スコープのネットワーク モニター レポート
トラフィック マップ	アプリケーション スコープのトラフィック マップ レポート

アプリケーション スコープのサマリー レポート

サマリー レポートには、使用量が増加した、減少した、および帯域幅の占有量が多い上位 5 つ のアプリケーション、アプリケーション カテゴリ、ユーザー、および送信元のチャートが表示 されます。

サマリー レポートのチャートをPDF形式でエクスポートするには**Export**(エクスポート)(Labore)をクリックします。各チャートが1ページの PDF として出力に保存されます。 アプリケーション スコープのサマリー レポート



アプリケーション スコープの変化モニター レポート

変化モニターレポートには、指定した期間の変化が表示されます。たとえば、以下の図は、過 去 24 時間と比較して過去 1 時間に使用量が増加した上位のアプリケーションを示しています。 上位アプリケーションはセッション数によって決定され、パーセント別にソートされます。

アプリケーション スコープの変化モニター レポート



このレポートには、以下のオプションが表示されます。

変化モニター レポートのオプション	の意味
上部バー	
トップ 10	上位からいくつの項目を表に表示するかを指定し ます。
Application [アプリケーション]	レポートに含める項目を指定しま す。Application[アプリケーション]、Application Category[アプリケーションカテゴリ]、Source[送 信元]、Destination[宛先]
増加アプリケーション	指定期間を比較し増加した項目を表示します。
利用が減ったアプリケーション	指定期間を比較し減少した項目を表示します。

変化モニター レポートのオプション 	の意味
新規	指定期間を比較しあらたに検出された項目を表示 します。
ドロップ	指定期間を比較し検出されなくなった項目を表示 します。
フィルタ	フィルタを適用して、選択した項目のみを表示し ます。None (なし) を選択すると、すべてのエン トリが表示されます。
セッション情報やバイト情報を表示しま す。	セッション情報またはバイト情報のどちらを表示 するかを指定します。
ソート	パーセンテージまたは実増加のどちらでエントリ をソートするかを指定します。
エクスポート	グラフを .png イメージまたは PDF としてエクス ポートします。
下部バー	1
比較(間隔)	変化モニターの比較対象期間を指定します。

アプリケーション スコープの脅威モニター レポート

脅威モニターレポートには、選択した期間にわたって上位を占める脅威の数が表示されます。 たとえば、以下の図は、過去6時間における上位10件の脅威タイプを示しています。

アプリケーション スコープの脅威モニター レポート



Last 6 hours Last 12 hours Last 24 hours Last 7 days Last 30 days Last 60 days Last 90 days

チャートの下の凡例のように、各タイプの脅威が色分けして示されます。このレポートには、以 下のオプションが表示されます。

脅威モニター レポートのオプショ ン	の意味
上部バー	
トップ 10	上位からいくつの項目を表に表示するかを指定します。
脅威	測定する項目を指定します。Threat[脅 威]、Threat Category[脅威カテゴリ]、Source[送信 元]、Destination[宛先]
フィルタ	フィルタを適用して、選択した項目のみを表示します。
	情報を表示するグラフ(積み重ね棒グラフまたは積み重 ね面グラフ)を指定します。
脅威モニター レポートのオプショ ン	の意味
-----------------------	---
エクスポート	グラフを .png イメージまたは PDF としてエクスポート します。

下部バー

Last 6 hours Last 12 hours Last 24 hours Last 7 days Last 30 days Last 60 days 表示対象期間を指定します。

アプリケーション スコープの脅威マップ レポート

脅威マップ レポートには、重大度を含めた脅威の地理的ビューが表示されます。 アプリケーション スコープの脅威マップ レポート



Last 6 hours Last 12 hours Last 24 hours Last 7 days Last 30 days Last 60 days Last 90 days

チャートの下の凡例のように、各タイプの脅威が色分けして示されます。マップ上の国をクリッ クし、必要に応じてZoom In[拡大]とZoom Out[縮小]を行います。このレポートには、以下のオ プションが表示されます。

脅威マップ レポートのオプション	の意味
上部バー	
トップ 10	上位からいくつの項目を表に表示するかを指定します。
受信した脅威	インバウンド方向(外部から)の脅威を示します。
送信した脅威	アウトバウンド方向(外部へ)の脅威を示します。
フィルタ	フィルタを適用して、選択した項目のみを表示します。
ズームインおよびズームアウト	マップを拡大および縮小します。
エクスポート	グラフを .png イメージまたは PDF としてエクスポート します。
下部バー	

Last 6 hours Last 12 hours Last 24 hours Last 7 days Last 30 days Last 60 days 6

アプリケーション スコープのネットワーク モニター レポート

ネットワーク モニター レポートには、指定した期間にわたって複数のネットワーク アプリケー ションによって占有されていた帯域幅が表示されます。図の下の凡例のように、各タイプのネッ トワーク アプリケーションが色分けして示されます。たとえば、以下の図は、セッション情報 に基づく過去7日間のアプリケーション帯域幅を示しています。

アプリケーション スコープのネットワーク モニター レポート



Last 6 hours Last 12 hours Last 24 hours Last 7 days Last 30 days Last 60 days Last 90 days

このレポートには、以下のオプションが表示されます。

上部バー

トップ 10	上位からいくつの項目を表に表示するかを指定します。
Application [アプリケーション]	レポートに含める項目を指定します。Application[アプリ ケーション]、Application Category[アプリケーションカ テゴリ]、Source[送信元]、Destination[宛先]
フィルタ	フィルタを適用して、選択した項目のみを表示しま す。None[なし] を選択すると、すべてのエントリが表示 されます。
セッション情報やバイト情報を表 示します。	セッション情報またはバイト情報のどちらを表示するか を指定します。

ネットワーク モニター レポートの オプション	の意味
Litt 📚	情報を表示するグラフ(積み重ね棒グラフまたは積み重 ね面グラフ)を指定します。
エクスポート	グラフを .png イメージまたは PDF としてエクスポート します。

下部バー

Last 6 hours Last 12 hours Last 24 hours Last 7 days Last 30 days Last 60 days Last 90 days

変更措置が取られる期間を示します。

アプリケーション スコープのトラフィック マップレポート

トラフィック マップ レポートには、セッション数またはフロー数に応じて、トラフィック フローの地理的ビューが表示されます。

アプリケーション スコープのトラフィック マップ レポート



Last 6 hours Last 12 hours Last 24 hours Last 7 days Last 30 days Last 60 days Last 90 days

チャートの下の凡例のように、各タイプのトラフィックが色分けして示されます。このレポート には、以下のオプションが表示されます。

トラフィック マップ レポートのオプション	の意味
上部バー	
トップ 10	上位からいくつの項目を表に表示するかを 指定します。
受信トラフィック	受信トラフィックを表示します。
送信トラフィック	送信トラフィックを表示します。
セッション情報やバイト情報を表示します。	セッション情報またはバイト情報のどちら を表示するかを指定します。
ズームインおよびズームアウト	マップを拡大および縮小します。
エクスポート	グラフを .png イメージまたは PDF としてエ クスポートします。
下部バー	
Last 6 hours Last 12 hours Last 24 hours Last 7 days Last 30 days Last 60 days Last 90 days	変更措置が取られる期間を示します。

Monitor > Session Browser [監視 > セッション ブラウザ]

Monitor > Session Browser[監視 > セッションブラウザ]から、ファイアウォール上で現在実行 中のセッションの参照とフィルタを行います。このページのフィルタリングオプションの詳細 は、「ログアクション」を参照してください。

Monitor (監視) > Block IP List (ブロック IP リスト)

ブロック リストに IP アドレスを配置するようにファイアウォールを設定できます。これには、 次を含めいくつかの方法があります。

- Protect(保護)に対するアクションを含む DoS プロテクション ポリシー ルールを設定し、 そのルールに Classified DoS Protection(分類された DoS プロテクション)プロファイルを 適用します。このプロファイルにはブロック期間が含まれます。
- Block lp(ブロック IP) に対するアクションを含むルールを使用する Vulnerability Protection(脆弱性防御)プロファイルを使用してセキュリティ ポリシー ルールを設定し、 そのルールをゾーンに適用します。

ブロック IP リストは、PA-3200 シリーズ、PA-5200 シリーズ、および PA-7000 シリーズの ファイアウォールでサポートされます。

知りたい内容	以下を参照
ブロック IP リストの各フィー ルドは何を示しますか?	ブロック IP リスト エントリ
ブロック IP リストのエントリ をフィルタリング、操作、削 除する方法は?	ブロック IP リスト エントリの表示または削除
その他の情報をお探しです か?	アンチウイルス、アンチスパイウェア、および脆弱性防御 のセットアップ
	新規セッションのフラッド攻撃に対する Dos プロテクショ ン
	Monitor Blocked IP Addresses(ブロックされた IP アドレスのモニター)

ブロック IP リスト エントリ

• 監視 > Block IP List

以下の表で、ファイアウォールがブロックしている送信元 IP アドレスのブロック リスト エント リについて説明します。

項目	の意味
ブロック タイム	IP アドレスがブロック IP リストに入った月/日および時:分:秒です。

項目	の意味
タイプ	ブロック アクションのタイプです。ハードウェア(hw)またはソフ トウェア(sw)のいずれが IP アドレスをブロックしたのかを示しま す。
	脆弱性防御プロファイルを使用する DoS プロテクション ポリシー またはセキュリティ ポリシーを設定し、送信元 IPv4 アドレスから の接続をブロックするようにすると、それらのパケットが CPU ま たはパケット バッファ リソースを使用する前に、ハードウェアのト ラフィックをファイアウォールが自動的にブロックします。攻撃ト ラフィックがハードウェアのブロック容量を超えた場合、ファイア ウォールはソフトウェアを使用してトラフィックをブロックします。
送信元 IP アドレス	ファイアウォールがブロックしたパケットの送信元 IP アドレスで す。
Ingress ゾーン	ファイアウォールにパケットが入ったインターフェイスに割り当てら れたセキュリティ ゾーンです。
残り時間	IP アドレスのブロック IP リスト掲載残り時間(秒)です。
ブロック ソース	ブロック IP アクションが指定されている、分類された DoS プロテク ション プロファイルの名前または脆弱性防御オブジェクト名です。
ブロック済み IP 合 計: x/y(z% 使用)	ファイアウォールがサポートしている全体のブロック対象 IP アドレ スの数(y)のうちの、ブロック済み IP アドレスの数(x)、および ブロック済みの IP アドレスが使用している割合(z)です。

ブロック IP リストエントリの表示または削除

ブロック IP リストのエントリを操作して、エントリの詳細情報を表示し、必要に応じてエント リを削除します。

ブロック IP リスト エントリの表示または削除	
特定のブロック IP リスト情報を検索 する	列の値を選択すると、Filters(フィルタ)フィールドにフィルタが入力 され、右矢印をクリックすると、該当の値を持つエントリの検索が開 始されます。 フィルタを削除するには、X をクリックします。
現在の画面以外の ブロック IP リスト エントリを表示す る	Page(ページ)フィールドにページ番号を入力するか、一重矢印をク リックして次のページまたは前のページのエントリを表示します。二 重矢印をクリックすると、最後のページまたは最初のページのエント リが表示されます。

ブロック IP リスト エントリの表示または削除	
ブロック IP リスト 上の IP アドレスに 関する詳細情報を 表示する	エントリの Source IP Address(送信元 IP アドレス)をクリックする と、Network Solutions の Who Is にリンクされ、アドレスに関する情 報が表示されます。
ブロック IP リスト エントリを削除す る	 エントリを選択し、Delete(削除)をクリックします。 Webインターフェイスからサポートされているのはハードウェアエントリの削除のみです。ただし、CLIからはハードウェアとソフトウェアの両方のエントリの削除がサポートされています。
ブロック IP リスト 全体をクリアする	 Clear All (すべてクリア)をクリックすると、すべてのエントリが永久に削除されます。つまり、これらのパケットはブロックされなくなります。 Webインターフェイスからサポートされているのはハードウェアエントリのブロック IP リストのクリアのみです。ただし、ハードウェアとソフトウェアの両方のエントリのクリアは、CLI からサポートされています。

Monitor > Botnet [監視 > ボットネット]

ボットネットレポート機能により、ネットワーク内でボットネットに感染した可能性のあるホ ストを、挙動をもとに特定することができます。レポートには、各ホストのボットネット感染 の可能性が1から5の信頼性スコアで表示されます(5は感染の可能性が高いことを示します)。 レポートのスケジュールを設定したり、手動でレポートを実行する前に、不審と判定するトラ フィックのタイプを設定する必要があります。ボットネットレポートアウトプットの読み方に ついては PAN-OS[®] 管理者ガイドに記載されています。

- ボットネット レポートの設定
- ボットネットの設定

ボットネット レポートの設定

• Monitor > Botnet > Report Setting [監視 > ボットネット > レポート設定]

ボットネットレポートを生成する前に、ボットネット活動の可能性があるトラフィックを指定 する必要があります(「ボットネットレポートの設定」を参照してください)。毎日のレポー ト作成をスケジューリングする場合や手動で実行する場合は、Report Setting[レポート設定]を クリックし、以下のフィールドを入力します。レポートをエクスポートする場合は、レポート を選択し、Export to PDF[PDFにエクスポート]、Export to CSV[CSVにエクスポート]、あるい はExport to XML[XMLにエクスポート]を選択します。

ボットネット レポート の設定	の意味
ランタイムフレームの テスト	レポートの期間を選択します – Last 24 Hours(過去 24 時間)(デ フォルト)、または Last Calendar Day(前日の一日間)
今すぐ実行	今すぐに手動でレポートを生成する場合はRun Now[今すぐ実行]を クリックします。レポートはボットネットレポートダイアログの新 しいタブで表示されます。
行数	レポートに表示される行数を指定します(デフォルトは100)。
スケジュール設定	毎日自動的にレポートを生成する場合はこのオプションを選択しま す。デフォルトでは、このオプションが有効化されています。
クエリ ビルダー	(任意)レポートに送信元/宛先 IP アドレス、ユーザー、ゾーンな どの属性別にフィルタをかける場合は、クエリ ビルダーにクエリ を Add (追加)します。例えば、IPアドレス192.0.2.0から発信され るトラフィックにボットネット活動の可能性がないとわかっている 場合は、クエリにnot (addr.src in 192.0.2.0)を追加し、レ ポートからそのホストを除外することができます。

ボットネット レポート の設定	の意味
	 Connector[条件式] – 論理結合子 (and/or) を指定します。Negate[除外]を選択した場合、クエリに指定されたホストが
	レポートから除外されます。
	• Attribute[属性] - ノアイアワオールかホットネット活動を検索す るホストのゾーン、アドレス、またはユーザーを指定します。
	 Operator[演算子] – Attribute[属性]をValue[値]に関連付ける際の 演算子を指定します。
	● Value[値] – クエリに検出させる値を入力します。

ボットネットの設定

• Monitor > Botnet > Configuration [監視 > ボットネット > 設定]

ボットネット活動の可能性があるトラフィックのタイプを指定する場合は、Botnet[ボットネット]ページの右側にあるConfiguration[設定]をクリックし、以下のフィールドを入力します。レポートの設定後、手動で実行するか、定期的に実行するようにスケジュール設定を行うことができます(Monitor(監視) > PDF Reports(PDF レポート) > Manage PDF Summary(PDF サマリーの管理)を参照してください)。

デフォルトの Botnet レポート設定が最善です。デフォルトの値が誤検出を発生させていると考えられる場合は、Palo Alto Networks が値を再評価できるよう、サポートチケットを作成してください。

ボットネットの設定	の意味
HTTP トラフィック	レポートに含まれるHTTPトラフィックのタイプごとのCount[カウ ント数]をEnable[有効化]します。ここで設定したCount[カウント 数]分の各トラフィックイベントが発生すると、レポート上ではそ のトラフィックに関係したホストに対し高いスコアが割り当てられ ます(高いスコアはボットネット感染の可能性が高いことを示しま す)。イベント数が Count(数)より少ない場合、レポートにはよ り低い確度スコアが表示されるか、(特定のトラフィックタイプで は)ホストのエントリが表示されなくなります。
	 Malware URL visit[マルウェアURLへのアクセス](範囲は 2~1000、デフォルトは5) – マルウェアおよびボットネット の URL のフィルタリング カテゴリに基づき、既知のマルウェア URL に対して通信しているユーザーを特定します。
	 Use of dynamic DNS[動的DNSの使用](範囲は 2~1000、デ フォルトは 5) - マルウェア、ボットネット通信、またはエク スプロイトキットの可能性がある動的DNSクエリトラフィック を検索します。一般的に、動的DNSドメインはとてもリスクが

ボットネットの設定	の意味
	高いものとされています。多くの場合、マルウェアは IP アドレ スのブラックリストを回避する目的で動的 DNS を使用していま す。このようなトラフィックをブロックするために、URL フィ ルタリングを使うことも検討してください。
	 Browsing to IP domains[IPドメインを参照](範囲は 2~1000、 デフォルトは10) – URLではなく、IPドメインを参照するユー ザーを特定します。
	 Browsing to recently registered domains[最近登録されたドメインを参照](範囲は 2~1000、デフォルトは10) – 過去30日以内に登録されたドメイン名を持つサイトへのトラフィックを検索します。攻撃者、マルウェア、そしてエクスプロイトキットは多くの場合、新しく登録されたドメインを使用しています。
	 Executable files from unknown sites[不明サイトからの実行可能 ファイル](範囲は 2~1000、デフォルトは10) – 未知のURLサ イトから実行形式のファイルをダウンロードされた通信を特定 します。多くの感染例には実行ファイルが関係しているため、 その他の不審なトラフィックと結びついている場合はホストの 調査を優先的に行うことをお勧めします。
不明なアプリケーショ ン	不審かつ不明なTCPまたは不明なUDPアプリケーションに結びつい たトラフィックをレポートに含めるかどうかのしきい値を設定しま す。
	 Sessions Per Hour[1時間当たりのセッション](範囲 は1~3600、デフォルトは10) - 1時間当たり、指定した回数ま でのアプリケーションセッションに関わったトラフィックがレ ポートに加えられます。
	 Sessions Per Hour[1時間当たりの宛先の数](範囲は1~3600、 デフォルトは10) - 1時間当たり、指定した数までのアプリケー ションの宛先に関わったトラフィックがレポートに加えられま す。
	 Minimum Bytes[最小バイト数](範囲は1~200、デフォルトは50) - 指定したサイズ以上のアプリケーションペイロードのトラフィックがレポートに加えられます。
	 Maximum Bytes[最大バイト数](範囲は1~200、デフォルトは100) - 指定したサイズ以下のアプリケーションペイロードのトラフィックがレポートに加えられます。
IRC	IRCサーバーに関係するトラフィックを含める場合はこのオプショ ンを使用します。

モニター > loTデバイス

どこで使用できますか?	何が必要ですか?
• PAN-OS	(ファイアウォール) IoT セキュリティ サ ブスクリプション
	 (Panorama) Panorama > セットアッ プでIoTデバイスコンテキストクラウド サービスを有効にします

[IoT Devices] セクションでは、IoT SecurityのAlおよび機械学習機能を通じて、ネットワーク上のデバイスを可視化できます。これらのページにデータを表示するには、次世代ファイアウォールがIoTセキュリティサービスに加入している必要があります。

- IoT Devices (IoT デバイス) > Summary (概要)
- IoTデバイス> アセットインベントリ
 - PanoramaをPAN-OS 11.1にアップグレードしたら、IoTデバイスコンテキストクラ ウドサービスを有効にして、[IoT Devices (IoTデバイス)] > [Summary (サマリー)]ペー ジ[IoT Devices (IoTデバイス)] > [Asset Inventory (アセットインベントリ)]ページを表 示する必要があります。[Panorama > セットアップ]を選択し、[PAN-OSエッジサー ビス設定]セクションの編集アイコンをクリックします。表示される [PAN-OSエッ ジサービスの設定] パネルで、 [Enable IoT Device Context Cloud Service (IoTデバイ スコンテキストクラウドサービスを有効にする)]を選択し、 [OK]をクリックしま す。有効にしないとPanoramaはこれらのページを表示しません。
- IoT Devices (IoT デバイス) > Summary (概要)

どこで使用できますか ?	何が必要ですか?
• PAN-OS	 □ (ファイアウォール) IoT Security サブス クリプション □ (Panorama) [Panorama] > [セットアッ プ]でIoTデバイスコンテキストクラウド
	サービスを有効にします

IoT Securityは、AIと機械学習を使用して、ネットワークに接続されたデバイスを自動的に検出 して識別し、データが豊富で動的に更新されるインベントリを構築します。ファイアウォール がIoT Securityサービスに加入すると、同じテナントサービスグループ(TSG)のトラフィック ログにあるIoT Securityインスタンスを送信して分析します。また、ファイアウォールはIPアド レスとデバイスのマッピングを継続的に取得し、これにはIoT Securityによって監視および保護 されているデバイスのデバイスプロファイルやその他のデバイスID属性が含まれます。その後、 ファイアウォールはこれらのマッピングに一致するデバイスにインポートされたルールを適用できます。

このダッシュボードには、loT Securityがネットワーク上で検出した上位10のデバイスカテゴリ、デバイスプロファイル、オペレーティングシステムに関する有用な概要情報を表示するパネルが含まれています。

このページにアクセスすると、PAN-OSは最新のアップデート中にloT Securityから受信した データからコンテンツを生成します。その後、生成された出力を次の30分間キャッシュしま す。30分以内に離れて戻っても、以前と同じ情報が表示されます。ただし、30分後に戻ると、 その時間に新しく生成されたコンテンツが表示されます。

IoTデバイス> アセットインベントリ

どこで使用できますか?	何が必要ですか?
• PAN-OS	 (ファイアウォール) IoT セキュリティサ ブスクリプション (Panorama) Panorama > セットアッ プでIoTデバイスコンテキストクラウド
	サービスを有効にします

これは、IoT Securityが動的に検出してPAN-OSに提供したすべてのデバイスと関連デバイス属 性、および手動でインベントリに追加またはインポートしたすべてのデバイスを含むテーブルで す。ここでは、デバイスの表示、スタティックIPデバイスの一括インポート、個々のスタティッ クIPデバイスの追加、編集、アイデンティティの確認、デバイスIDオブジェクトの追加を行うこ とができます。

IoT アセットのインポート:デバイスのスタティックIPアドレスのリストがある場合 は、CSVファイルを使用してインポートできます。スタティックIPデバイスをインベントリに インポートするには、インポートし、モデルとして使用するサンプルCSVテンプレートをダウ ンロードし、インポートするデバイスの属性を追加します。IPアドレス、MACアドレス、ベン ダー、モデル、ホスト名、カテゴリ、プロファイル、OSグループ、OSバージョン。IPアドレス は必須です。その他の属性はすべてオプションです。CSVファイルが完成したら、再度インポー トします。インポートするファイルを選択し、「OK」をクリックします。

追加:loT Securityは、DHCPがデバイスにIPアドレスを動的に割り当てるネットワーク、ネット ワーク管理者がスタティックIPアドレスを手動で設定するネットワーク、および両方が組み合わ されたネットワークに展開できます。スタティックIPアドレスのデバイスを一括インポートでき るだけでなく、個別に追加することもできます。

スタティックIP デバイスを個別に追加するには、デバイスの IP アドレスと、オプションでいく つかの追加属性を知っている必要があります。[追加]をクリックし、[スタティックIPデバイス の追加]にIPアドレスおよびその他の属性値を入力して、[OK]をクリックします。追加すると、 ファイアウォールがIoT SecurityとPanorama(ファイアウォール管理に使用している場合)と通 信し、追加を同期します。 スタティックIP デバイスの設定を追加するだけでは、インベントリにデバイスを追加できません。IoT Securityは、設定されたスタティックIPアドレスを持つデバイスとの間で送受信されるネットワークトラフィックも検出する必要があります。その後、インベントリに追加されます。

編集:デバイス属性の欠落または誤適用に気付き、それが何かわかっている場合は、1つ以上のデバイスを選択して編集できます。選択または選択を行い、[Edit (編集)]をクリックし、別のホスト名を入力し、[OSグループ]、[プロファイル]、[モデル]、[ベンダー]、または[OSバージョン]に別の値を選択して、[OK]をクリックします。変更を選択した値だけが更新されます。他の値はすべてそのままです。編集後、ファイアウォールはloT SecurityとPanorama(ファイアウォール管理に使用されている場合)と通信し、変更を同期します。

デバイス ID の確認:デバイスのIDを確認すると、信頼スコアが即座に100%になり、PanoramaとIoT Securityに同期されます。

デバイス ID の作成:ポリシールールの推奨事項をインポートすると、ファイアウォールはデバ イス IDルールに必要なデバイス オブジェクトを自動的に生成します。この場合、デバイスオブ ジェクトを手動で作成する必要はありません。ただし、推奨ルールをインポートするのではな く、独自のセキュリティポリシールールを作成する場合は、このオプションを使用してデバイス オブジェクトを作成します。

Export[エクスポート]:アセットインベントリをダウンロードするには、CSV形式でエクスポートして保存します。これにより、インベントリ内のすべてのアセットがダウンロードされます。エントリごとに、デバイス名、デバイスプロファイル、デバイスカテゴリ、ベンダー、モデル、OSグループ、OSバージョン、IPアドレス、信頼度スコア、MACアドレス、最後に検出されたネットワークアクティビティを示すタイムスタンプを確認できます。

Monitor (監視) > PDF Reports (PDF レポート)

以下のトピックでは、PDF レポートについて説明します。

- Monitor > PDF Reports > Manage PDF Summary {監視 > PDF レポート > PDF サマリーの管理]
- Monitor > PDF Reports > User Activity Report [監視 > PDFレポート > ユーザー アクティビ ティ レポート]
- Monitor > PDF Reports > SaaS Application Usage [監視 > PDFレポート > Saasアプリケーションの使用状況]
- Monitor > PDF Reports > Report Groups [監視 > PDF レポート > レポート グループ]
- Monitor > PDF Reports > Email Scheduler [監視 > PDF レポート > 電子メール スケジューラ]

Monitor > PDF Reports > Manage PDF Summary {監視 > PDF レ ポート > PDF サマリーの管理]

PDF サマリー レポートには、各カテゴリの上位 5 件(上位 50 件ではない)のデータに基づき、既存のレポートから集められた情報が含まれています。このレポートには、別のレポートでは表示されないトレンド チャートも表示されます。

PDF サマリー レポート

			Nov 22, 2	013			
Applica	ation Usage		User Be Top 6 U	havior		paloaltone High	twork\binahara _{eat Risk} User
5	and the second pro-					Top 6 II	RI Catagorian
			User	Seccions	Bytes		
			paloaltonetwork/binah	6,420	43,249,831	Category	Count
3 0 0 0 0 0	1		paloaltonetworkl/benea	3,469	104,837,125	unknown	Barris Standard
2			paloaitonetworkytabre	1,115	1,182,034		
1 04/18	04/22	<u>—</u>	paloaltonetwork\kame	539	88,295		
Catego	ry Breakdown		Top 5 URL C	ategories			
						Top 5	Applications
	Restauctions (SE 07%)		Category		Count		
(A CONTRACTOR OF A CONTRACTOR A CONTRA	business-systems (14	LOHS)	huriners			Application	Sessions Byles
	unknown (11.03%)		computing-and-internet			Icmp	7,106 525,81
	general-Internet (1.73	N)	web-based-e-mail			msrpc	1,759 41,201,89
			finance-and-investment		0	unknown-udp	854 1,188,42
						dns	42 13,18
Top 5	Applications		Top 6 Destinati	on Countri	••	netbios-ns	20 5,07
Application	tessions By	he l	Destination	Sector 10	Count	Тор	6 Threats
ns in the second second	11,548 2.2	26,690	Reserved (10.0.0.0 - 10.25	5.255.255)	37,792		
mp	9,260 6	84,128	United States		5,225	No mate	hing data found
nknown-udo	5.537 2.7	58.854	Unknown		436		
al Constantine States	4,787 14,5	87,554	Reserved (192.168.0.0 - 19	2.168.255.	2 180		
isirpic	4,519 147,6	07,405	European Union		162		
Threa	t Types		Thre	at			
Top 6	Spyware		Top 6 Att	ackers		т	rends
Spywar	· Statistica (Count	Address	1000000	Count		
earchTech.com XXXP	omToolbar Dat	47	64.124.109.201.1426.aws.c	om	36	Bi	andwidth
hopnav Spyware Insta	 Market Market 	45	38.118.85.21		27	308	
In Bug retrieve weathe	r information	21	ug-in-f91.google.com		22		
tavista_Toolbar Get to	olbar cfg	1	carbon.paloaltonetworks.lo	cal	22	308	
			64.124.109.205.t426.aws.c	om	2	209	
Top 6 Vu	Inerabilities		Top 5 VI	otims		849MB	
			Address	ALC: NO.	Count	08	
No matchin	ng data found			and the second second second		the second se	
No matchir	ng data found		mjacobsen.paloaltonetwork	s local	44	04/16	04/22
No matchin	ng data found		mjacobsen.paioaitonetwork mjacobsen.paioaitonetwork	s local s local	44 31	04/16	04/22
No matchin	ng data found		mjacobsen.paloaltonetwork mjacobsen.paloaltonetwork 10.0.0.108	s.local s.local	44 31 10	04/18	04/22
No matchin	ng data found		mjacobsen, paloaltonetwork mjacobsen, paloaltonetwork 10.0.0.108 mrotolo-xp. paloa tonetwork	s.local s.local	44 31 10 8	Carre	64/22
No matchin	ng data found		mjacobsen, paloaitonetwork mjacobsen, paloaitonetwork 10.0.0.108 mrotolo-xp, paloaitonetwork esallaberry-xp, paloaitonetw	s.local s.local s.local iorks.local	44 31 10 8 5	2418	64/22 Threats
No matchir Top 6	ng data found Viruces		mjacobsen, paloaltonetwork mjacobsen, paloaltonetwork 10.0.0.108 mrotolo-xp, paloaltonetwork esallaberry-xp, paloaltonetwork Top 6 Attaoke	s.local s.local s.local iorks.local r Countrie	44 31 10 8 5	480	0422 Threats
No matchir Top 5	ng data found Viruces no data found		mjacobsen, paloatonetworn mjacobsen, paloatonetworn 10.0.0.108 mrotolo-xp.paloatonetwork esallaberry-xp.paloatonetw Top & Attaoke	s.local s.local s.local iorks.local r Countrier	44 31 10 8 6 5	480	0422
No matchir Top 5 No matchir	ng data found Viruses ng data found		miacobsen.paioationetworn miacobsen.paioationetworn 10.0.0.108 mrotoli-sp.paioationetwork esallaberry-sp.paioationetwork esallaberry-sp.paioationetwork Top 6 Attacke Country United States	s.local s.local s.local iorks.local r Countrie	44 31 10 8 6 5 5 7 7 1	480	04/22
No matchir Top 5 No matchir	ng data found Viruces ng data found		miacobsen paloation teori miacobsen paloation teori 10.0.0.100 mrobio-xp.paloation teori csallaberry-xp.paloation teor Top 6 Attaoke Country United States Reserved (10.0.0.0.10.25	s.local s.local orks.local r Countries 5.255.255)	44 31 10 8 5 5 7 00unt 91 22	440	0422

PDF サマリー レポートを作成するには、Add(追加)をクリックします。PDF Summary Reports(PDF サマリー レポート)ページが開き、使用可能なすべてのレポート項目が表示され ます。

PDF レポートの管理

PDF Summary Report		()
Name		
🖓 Threat Reports 🛛 🖓 Application Reports	Trend Reports 🖓 Traffic Reports	URL Filtering Reports 🛛 📙 Custom Reports
Top attacker sources X	Top victims by source X	High risk user - Top X
Top attacker X destinations	Top victims by X destination countries	High risk user - Top X threats
Top victim sources X	Top threats X	High risk user - Top X URL categories
Top victim destinations \times	Top spyware threats \times	Top application × categories (Pie Chart)
Top attackers by source X countries	Top viruses X	Top technology × categories (Pie Chart) ×
		OK Cancel

以下のオプションを1つ以上使用してレポートを設計します。

- レポートから除外する項目については除外([X])をクリックするか、該当するドロップダウンリストから項目をクリアします。
- 該当するドロップダウンリストから選択することで項目を追加することができます。
- 項目をドラッグアンドドロップして、レポートの別のエリアに移動します。

最大 18 個のレポート項目を使用できます。既に 18 個の項目が含まれている場合は、新たに項目を追加する前に既存の項目を削除する必要があります。

レポートを Save (保存) するには、レポート名を入力し、OK をクリックします。

PDF レポートを表示するには、 Monitor (監視) > Reports (レポート)を選択し、 PDF Summary Report (サマリー レポート) をクリックしてレポートを選択し、カレンダーの日付をクリックし て その日のレポートをダウンロードしてください。

新しい PDF サマリー レポートは、そのレポートが実行されるまで表示されません。レポートは毎日午前2時に自動的に実行されます。

Monitor > PDF Reports > User Activity Report [監視 > PDFレポート > ユーザー アクティビティ レポート]

個々のユーザーまたはユーザー グループのアクティビティの概要を示すレポートを作成するに は、このページを使用します。Add(追加) をクリックし、以下の情報を指定します。

ユーザー/グループ ア クティビティ レポー ト設定	の意味
氏名	レポートを識別する名前を入力します(最大 31 文字)。名前の大文 字と小文字は区別されます。また、一意の名前にする必要がありま す。文字、数字、スペース、ハイフン、およびアンダースコアのみを 使用してください。
タイプ	ユーザー アクティビティ レポートの場合:User[ユーザー] を選択し、 レポートの対象となるユーザーの Username[ユーザー名] または IP address[IPアドレス](IPv4 または IPv6)を入力します。
	グループ アクティビティ レポート:Group[グループ]を選択し、Group Name[グループ名]を入力します。
その他のフィルタ	ユーザー/グループ アクティビティ レポート用のフィルタを作成する には、Filter Builder(フィルタ ビルダー)を選択します。
期間	ドロップダウンリストからレポートの期間を選択します。

ユーザー/グループ ア クティビティ レポー ト設定	の意味	
Include Detailed Browsing	(任意)レポートに詳細なURLログを追加するには、このオプション をオンにします。	
	詳細な閲覧情報には、選択したユーザーまたはユー ザー グループの大量の (何千もの) ログが含まれる可能 性があり、その結果、レポートが非常に大きくなる可 能性があります。	

グループアクティビティレポートには、URLカテゴリ別ブラウザサマリーは含ま れません。その他すべての情報は、ユーザーアクティビティレポートとグループ アクティビティレポートで共通です。

オンデマンドでレポートを実行するには、[今すぐ実行]をクリックします。レポートに表示する 行の最大数を変更するには、「ログとレポートの設定」を参照してください。

レポートを保存するには、**OK** をクリックします。次に、レポートの電子メール配信を スケジューリングできます(Monitor(監視) > PDF Reports(PDF レポート) > Email Scheduler(電子メール スケジューラ))。

ログフィルタの追加

レポートをカスタマイズするには、ユーザー アクティビティ レポートとグループ アクティビ ティ レポートにログ フィルタを作成します。アプリケーション、アプリケーションの特性など に基づいてアクティビティ レポートをフィルタすることができます。たとえば、認証を取得し ていない SaaS アプリケーションに興味がある場合は、このアプリケーション特性に基づいて フィルタを作成できます。

ログ フィルタ フィールドの追加	の意味
ログ フィルタ テキスト ボックス	ログに適用するフィルタを書き込みます。複 数のフィルタを書き込むことができます。
結合子	追加のフィルタリングオプションを付けて フィルタを追加します。書き込んだフィルタ をコネクタに適用しない場合は、 Negate (除 外)ボックスを選択します。
属性	メニューから追加する属性を選択します。
演算子	属性が値と等しいかどうかを選択します。

ログフィルタフィールドの追加	の意味
值	属性の値を設定します。使用可能な場合、可 能な値を含むドロップダウン メニューが利用 可能になります。

Apply(適用)を選択すると、作成したフィルタをユーザー アクティビティまたはグループア クティビティ レポートに適用します。

Monitor > PDF Reports > SaaS Application Usage [監視 > PDFレ ポート > Saasアプリケーションの使用状況]

このページを使用して、ネットワークを通過する SaaS アプリケーションに関連するセキュリ ティリスクを要約した SaaS アプリケーション使用状況レポートを生成します。この事前定義済 みのレポートは、認可されたアプリケーションと認可されていないアプリケーションの比較を 示し、不利なホスティング特性を持つ危険な SaaS アプリケーションを要約し、詳細ページに各 カテゴリの最上位のアプリケーションをリストすることにより、アプリケーションのアクティビ ティをハイライト表示します。この詳細なリスク情報を使用して、ネットワーク上で許可または ブロックしたい SaaS アプリケーションのポリシーを適用することができます。

正確で有益なレポートを生成するには、ネットワーク上で許可されたアプリケーションにタグを 付ける必要があります(「Generate the SaaS Application Usage Report(SaaS アプリケーション 使用状況レポートの生成)」を参照)。この事前設定タグを持たないアプリケーションは、ファ イアウォールおよびPanoramaはネットワーク上で不許可となっているものと判断されます。不 許可の SaaS アプリケーションは情報セキュリティの脅威となる可能性があるため、ネットワー クで許可されたアプリケーションと不許可のアプリケーションを知っておくことが重要です。不 許可のアプリケーションはネットワーク上での動作を許されておらず、脅威に対する脆弱性とプ ライベート情報あるいは機密情報の漏えいに繋がる可能性があります。

すべてのファイアウォールまたはデバイスグループでアプリケーションに一貫して タグを付けるようにしてください。あるアプリケーションが一方の仮想システム上 では許可されたアプリケーションとしてタグ付けされ、もう一方では不許可とされ ている場合、あるいは Panorama では親デバイスグループで不許可とされていて、 子デバイスグループでは許可タグが付与されている場合(またはその逆)、SaaSア プリケーション使用状況レポートには結果が重複して記載されてしまいます。

ACC で Application View (アプリケーションのビュー)を By Sanctioned State (許可済み状態別)に設定すると、仮想システムまたはデバイス グループ間で異なる許可済み状態を持つアプリケーションを視覚的に特定できます。緑は許可されたアプリケーション、青は不許可のアプリケーションを示します。黄色のアプリケーションは、異なる仮想システムまたはデバイス グループに異なる許可済み状態があることを示します。

レポートの設定を行う場合は、Add[追加]をクリックし、以下の情報を指定します。

SaaS アプリケーショ ンの使用状況レポート の設定	の意味
氏名	レポートを識別する名前を入力します(最大 31 文字)。名前の大文 字と小文字は区別されます。また、一意の名前にする必要がありま す。文字、数字、スペース、ハイフン、およびアンダースコアのみを 使用してください。
期間	ドロップダウンリストからレポートの期間を選択します。レポートに は、現在の日付(レポートが生成された日)のデータが含まれます。
次からログを含める	選択したユーザー グループ、選択したゾーン、あるいはファイア ウォールまたは Panorama で設定されているすべてのユーザー グ ループおよびゾーンのうち、どれを対象としてレポートを生成するか をドロップダウン リストから選択します。
	 For a selected user group(選択したユーザー グループ) – ファイ アウォールまたは Panorama でどの User Group(ユーザー グルー プ)でログをフィルタリングするかを選択します。
	 For a selected zone(選択したゾーン) – ファイアウォールまた は Panorama でどの Zone(ゾーン)でログをフィルタリングする かを選択します。
	 For all user groups and zones (すべてのユーザー グループとゾーン) – すべてのグループを対象としてレポートを生成したり、表示するユーザー グループ(最大 25 個)を選択したりできます。25 を超えるグループがある場合、ファイアウォールまたはPanorama は上位 25 グループをレポートに表示し、残りのすべてのユーザー グループを Others (その他) グループに含めます。
レポートにユーザー グループ情報を含め る (Selected User Group (選択した	このオプションは、レポートに含めるユーザー グループでログを フィルタリングします。manage groups(グループを管理)リンク またはmanage groups for the selected zone(選択したゾーンのグ ループを管理)リンクを選択し、表示するユーザー グループ(最大 25個)を選択します。
ユーザー グルー プ)に対してレポー トを生成するように 選択している場合、 このオプションを使 用できません)	選択したゾーンの特定のユーザーグループに関するレポートを生成した場合、選択したどのグループのメンバーでもないユーザーは、Others(その他)と呼ばれるユーザー グループに割り当てられます。
ユーザー グループ	どのユーザー グループを対象としてレポートを生成するかを選択 します。このオプションは、Include logs from(次からログを含め

SaaS アプリケーショ ンの使用状況レポート の設定	の意味
	る)ドロップダウン リストで Selected User Group (選択したユー ザー グループ)を選択した場合にのみ表示されます。
ゾーン	どのゾーンを対象としてレポートを生成するかを選択します。このオ プションは、Include logs from (次からログを含める) ドロップダウ ンリストで Selected Zone (選択したゾーン)を選択した場合にのみ 表示されます。
	ザー グループ情報を含める)を選択できます。
詳細なアプリケー ションカテゴリ情報 をレポートに含める	SaaSアプリケーションの使用状況レポートのPDFは2つのパートから 構成されています。デフォルトでは両方のパートのレポートが生成さ れます。レポートの前半(10ページ分)はレポート対象期間にネッ トワーク上で使用された SaaS アプリケーションに焦点を当てていま す。
	レポートの後半部分(レポート前半に記載された各アプリケーション サブカテゴリのSaaSおよび非SaaSアプリケーションに関する詳細な 情報が含まれています)が不要な場合はこのオプションを未選択に しておいてください。レポートの後半部分には、各サブカテゴリの上 位のアプリケーション名や、ユーザー、ユーザー グループ、ファイ ル、転送バイト数、およびこれらのアプリケーションが生み出した脅 威に関する情報が含まれています。
	詳細情報を含まない場合、レポートは 10 ページ分の長さとなってい ます。
レポートの最大サブ カテゴリを次に制限	SaaS アプリケーション使用状況レポートですべてのアプリケーショ ン サブカテゴリを使用するかどうか、またはサブカテゴリの最大数 を 10、15、20、または 25 に制限するかどうかを選択します。
	サブカテゴリの最大数を減らした場合、レポートに含める SaaS および SaaS 以外のアプリケーション アクティブティ情報が制限されるため、詳細レポートが短くなります。

必要なときにRun Now[今すぐ実行]をクリックしてレポートを生成します。

必要に応じてこのレポートを生成することも、毎日、毎週、または毎月の周期で実行するように スケジュールすることもできます。レポートをスケジューリングするには、「schedule reports for email delivery(電子メール送信のスケジュール レポート)」を参照してください。

PA-220 および PA-220R のファイアウォールでは、SaaS アプリケーション使用状況レポートは 電子メールの PDF 添付ファイルとして送信されません。かわりに、電子メールにはリンクが記 載されており、ウェブブラウザでレポートを開くことができます。 このレポートの詳細については、レポートの管理を参照してください。

Monitor > PDF Reports > Report Groups [監視 > PDF レポート > レポート グループ]

レポート グループを使用すると、レポートのセットを作成できます。システムはそのレポート のセットをまとめ、オプションのタイトル ページとすべての構成レポートが含まれる1つの集 約された PDF レポートを送信することができます。

レポート グループの 設定	の意味
氏名	レポート グループ名を入力します(最大 31 文字)。名前の大文字と 小文字は区別されます。また、一意の名前にする必要があります。文 字、数字、スペース、ハイフン、およびアンダースコアのみを使用し てください。
タイトル ページ	レポートにタイトルページを追加するには、このオプションをオンに します。
役職	レポート タイトルとして表示される名前を入力します。
レポートの選択 / ウィジェット	 グループに含める各レポートを左の列で選択し、右の列に Add(追加)します。以下のレポートタイプを選択できます。 事前定義済みレポート カスタムレポート PDF サマリーレポート CSV Log View (ログビュー) – カスタムレポートを作成するたびに、ファイアウォールは同じ名前の Log View (ログビュー)レポートを自動的に作成します。Log View (ログビュー)レポートを自動的に作成します。Log View (ログビュー)には、カスタムレポートの内容を作成するためにファイアウォールが使用したログが表示されます。ログビューデータを含めるには、レポートグループを作成するときに Custom Reports (カスタムレポート)を追加し、一致する Log View (ログビュー)レポートを追加します。レポートグループに対して生成される集約レポートには、カスタムレポート・データが表示され、その後にログデータが表示されます。 レポートグループを保存すると、Report Groups (レポートグループ)、ページの Widgets (ウィジット)列に、グループに追加したレ

監視

レポート グループを使用するには、「Monitor(監視) > PDF Reports(PDF レポート) > Email Scheduler(電子メール スケジューラ)」を参照してください。

Monitor > PDF Reports > Email Scheduler [監視 > PDF レポート > 電子メール スケジューラ]

レポートの電子メール配信をスケジューリングするには、電子メールスケジューラを使用します。この設定を追加する前に、あらかじめレポートグループと電子メールプロファイルを定義しておく必要があります。「Monitor(監視) > PDF Reports(PDF レポート) > Report Groups(レポートグループ)」および「Device(デバイス) > Server Profiles(サーバープロファイル) > Email(電子メール)」を参照してください。

スケジューリングされたレポートは午前2時にレポートの生成処理を開始し、スケジューリン グされたすべてのレポートの生成が完了した後、電子メールが転送されます。

電子メール スケ ジューラ設定	の意味
氏名	スケジュールを識別する名前を入力します(最大 31 文字)。名前の 大文字と小文字は区別されます。また、一意の名前にする必要があり ます。文字、数字、スペース、ハイフン、およびアンダースコアのみ を使用してください。
レポート グループ	スケジューリングするレポート グループ(Monitor(監視) > PDF Reports (PDF レポート) > Report Groups (レポート グループ)) または SaaS アプリケーション使用状況レポート(Monitor(監視) > PDF Reports (PDF レポート) > SaaS Application Usage (SaaS アプ リケーション使用状況))を選択します。
電子メール プロファ イル	電子メール設定を定義するプロファイルを選択します。電子メー ル プロファイルの定義については、「Device(デバイス) > Server Profiles(サーバー プロファイル) > Email(電子メール)」を参照し てください。
繰り返し	レポートを生成して送信する頻度 (毎日、毎週月・火・水・木・金・ 土・日曜日、無効) を選択します。
電子メール アドレス のオーバーライド	電子メール プロファイルで指定したメール受信者の代わりに使用す る別の電子メール アドレスを入力します。
テスト電子メールの 送信	クリックすると、Email Profile(電子メール プロファイル)で定義し た電子メール アドレスにテスト電子メールが送信されます。

Monitor > Manage Custom Reports [監視 > カスタムレ ポートの管理]

カスタムレポートを作成し、必要に応じてまたは定期的に(毎晩)実行できます。事前定義済 みのレポートの場合は、Monitor(モニター) > Reports(レポート)を選択してください。



ファイアウォールがスケジュールされたカスタムレポートを生成した後で、設定を 変更して将来の出力を変更すると、そのレポートの過去の結果が無効になる危険が あります。スケジュール設定されたレポート設定を変更する必要がある場合は、新 しいレポートを作成することをお勧めします。

カスタムレポートを Add(追加)して、新しいレポートを作成します。既存のテンプレートに 基づいてレポートを作成するには、Load Template(テンプレートのロード)を行って、テンプ レートを選択します。Scheduled(スケジュール設定)された時間ではなく、またはその時間に 加えて、レポートを必要なときに生成するには、Run Now(今すぐ実行)をクリックします。 以下の設定を指定して、レポートを定義します。

カスタム レポートの設 定	の意味
氏名	レポートを識別する名前を入力します(最大 31 文字)。名前の大 文字と小文字は区別されます。また、一意の名前にする必要があり ます。文字、数字、スペース、ハイフン、およびアンダースコアの みを使用してください。
の意味	カスタム レポートの説明を入力します。
データベース	レポートのデータ ソースとして使用するデータベースを選択しま す。
スケジュール設定	レポートを毎晩実行する場合は、このオプションをオンにします。 その後、Monitor(監視) > Reports(レポート)を選択すると、レ ポートが利用可能になっています。
タイムフレーム	規定の時間枠を選択するか、Custom[カスタム]を選択して、日時の範囲を指定します。
ソート基準	ソート オプションを選択して、レポートに含める情報の量などを決 定し、レポートの編成を行います。使用可能なオプションは、選択 したデータベースによって異なります。
グループ化基準	グループ分けオプションを選択して、レポートに含める情報の量 などを決定し、レポートの編成を行います。使用可能なオプション は、選択したデータベースによって異なります。

カスタム レポートの設 定	の意味	
列	カスタムレポートで使用可能な列を選択し、選択した列に追加 (↔ します。Up(上へ)、Down(下へ)、Top(最上 部)、Bottom(最下部)を使用して、選択された列の並 び替えを行います。必要に応じて、選択済みの列を削除 (⊖ することができます。)
クエリ ビルダー	 レポートクエリを作成するには、以下を指定して、Add[追加]をクリックします。クエリが完成するまで、繰り返します。 Connector[条件式] – 追加する式の前に置く結合子(and/or)を選択します。 Negate[除外] – クエリを否定(除外)として解釈させるには、このオプションをオンにします。前述の例で、否定のオプションを選択すると、過去24時間以内に受け取られていないエントリ、または「untrust」ゾーンから受け取られていないエントリに対する照合が行われます。 Attribute[属性] – データ要素を選択します。使用可能なオプションは、選択したデータベースによって異なります。 Operator[演算子] – 属性が適用されるかどうかを決定する基準を選択します(= など)。使用可能なオプションは、選択したデータベースによって異なります。 Value[値] – 照合する属性値を指定します。 	

詳細は、「カスタム レポートの生成」を参照してください。

Monitor > Reports [監視 > レポート]

このファイアウォールでは、前日、または前の週の指定した日のトラフィック統計情報のさまざ まな「上位 **50**」レポートを作成できます。

レポートを表示するには、ページの右側にあるレポート カテゴリ(Custom Reports(カスタム レポート)など)を展開し、レポート名を選択します。ページの各セクションにレポートが表示 されます。各レポートに、選択した期間の情報を表示することができます。

デフォルトでは、ファイアウォールは前日分のすべてのレポートを表示します。他の日付のレ ポートを表示するには、ページの右下にあるカレンダーでレポートの生成日を選択します。

ファイアウォール以外のシステムでレポートを表示するには、エクスポート オプションを選択 します。

- PDF にエクスポート
- CSVにエクスポート
- XML にエクスポート



ポリシー

以下のトピックでは、ファイアウォール ポリシーのタイプ、ポリシーの移動またはコピー方 法、ポリシー設定について説明します。

- ポリシーのタイプ
- ポリシールールの移動またはコピー
- 監査コメントアーカイブ
- ルールの使用状況ヒット数のクエリ
- Policies > Security [ポリシー > セキュリティ]
- Policies > NAT [ポリシー > NAT]
- Policies > QoS [ポリシー > QoS]
- Policies > Policy Based Forwarding [ϑ リシー > ϑ リシー ベース フォワーディング]
- Policies > Decryption [ポリシー > 復号化]
- ポリシー>ネットワークパケットブローカー
- Policies (ポリシー) > Tunnel Inspection (トンネル検査)
- Policies (ポリシー) > Authentication (認証)
- Policies > DoS Protection [#リシー > DoS %ロテクション]
- Policies > SD-WAN [ポリシー > SD-WAN]

ポリシーのタイプ

ポリシーを使用すると、ルールを適用してアクションを自動化し、ファイアウォールの動作を制 御できます。ファイアウォールでは、以下のポリシーのタイプがサポートされています。

- 基本セキュリティポリシー アプリケーション、ゾーンとアドレス(送信元と宛先)ごと、および任意でサービス(ポートとプロトコル)ごとにネットワークセッションをブロックまたは許可します。ゾーンでは、トラフィックを送受信する物理または論理インターフェイスが識別されます。「Policies(ポリシー) > Security(セキュリティ)」を参照してください。
- ネットワークアドレス変換(NAT)ポリシー アドレスとポートを変換します。
 「Policies(ポリシー) > NAT」を参照してください。
- Quality of Services (QoS) ポリシー QoS が有効になっているインターフェイスを通過するトラフィックの処理を分類する方法を決定します。「Policies(ポリシー) > QoS」を参照してください。
- ポリシーベースの転送ポリシー ルーティングテーブルをオーバーライドして、トラフィックの出力インターフェイスを指定します。「Policies(ポリシー) > Policy Based Forwarding(ポリシーベースの転送)」を参照してください。
- 復号化ポリシー セキュリティ ポリシーのトラフィック復号化を指定します。ポリシー ごとに、復号化するトラフィックの URL のカテゴリを指定できます。SSH 復号は、SSH シェル アクセス以外にも SSH トンネリングを識別して制御するためにも使用されます。 「Policies(ポリシー) > Decryption(復号化)」を参照してください。
- トンネル検査ポリシー トンネリングされたトラフィックにセキュリティ、DoS プロテクション、QoS ポリシーを適用したり、トンネルアクティビティを表示したりします。 「Policies(ポリシー) > Tunnel Inspection(トンネル検査)」を参照してください。
- オーバーライドポリシー ファイアウォールのアプリケーション定義をオーバーライドします。「Policies(ポリシー) > Application Override(アプリケーションオーバーライド)」を参照してください。
- 認証ポリシー ネットワーク リソースにアクセスするエンド ユーザーの認証を定義します。
 「Policies(ポリシー) > Authentication(認証)」を参照してください。
- サービス拒否 (DoS) ポリシー DoS 攻撃から保護し、一致するルールに対応する保護アクションを実行します。「Policies(ポリシー) > DoS Protection(DoS プロテクション)」を参照してください。
- SD-WAN ポリシーは、リンクパスの正常性が承認され、コンフィグされた正常性メトリックより低下した場合に、送信元と宛先ゾーン間のリンクパス管理を決定します。「Policies (ポリシー) > SD-WAN」を参照してください。

Panorama[™] からプッシュされた共有ポリシーは、ファイアウォール Web インターフェイスで はオレンジ色で表示されます。これらの共有ポリシーは Panorama でのみ編集できます。ファイ アウォールでは編集できません。

ルールベースをグループとして表示をクリックして、ルールベースで使用されているすべてのタ ググループを表示します。多くのルールを持つルールベースではルールベースをグループとして 表示し、作成済みのルール階層を維持したまま各グループのタグ、カラーコード、ルール数を表示することで、表示をシンプルにすることができます。

ポリシールールの移動またはコピー

ポリシーを移動またはコピーする『際には、共有の場所を含め、自分がアクセス許可を与えられ ている Destination (宛先)(ファイアウォール上の仮想システム、またはPanorama上のデバイス グループ)を割り当てることができます。

ポリシー ルールを移動するには、Policies(ポリシー)タブでルールを選択し、Move(移動)をクリックして、Move to other vsys(他の vsys に移動)(ファイアウォールのみ)またはMove to different rulebase or device group (他のルールベースあるいはデバイスグループに移動)(Panorama のみ)を選択し、以下の表の各フィールドを指定して OK をクリックします。

ポリシーをコピーする場合は、**Policies**[ポリシー] タブで**Clone**[コピー]をクリックして、以下の 表の各フィールドを入力して**OK**をクリックします。

設定の移動/コピー	の意味
選択中のルール	操作対象として選択したポリシルールの名前と現在の場所(仮想 システムまたはデバイスグループ)が表示されます。
宛先	ポリシーまたはオブジェクトの新しい場所として、仮想システ ム、デバイス グループ、または共有を選択します。デフォルト値 は、Policies[ポリシー] または Objects[オブジェクト] タブで選択し た Virtual System[仮想システム] または Device Group[デバイス グ ループ] です。
ルール順序	他のルールに対するルール相対位置を選択します。
	 Move top[最上部へ] – 他のすべてのルールの前の位置を選択します。
	 Move bottom[最下部へ] – 他のすべてのルールの後の位置を選 択します。
	 Before rule[事前ルール] – 隣接するドロップダウンリストリストで直後のルールを選択します。
	• After rule[事後ルール] – 隣接するドロップダウンリスト リスト で直前のルールを選択します。
検証で最初に検出されたエ ラーに起因するエラーが発生 しました	このオプションをオンにすると(デフォルトはオン)、ファイア ウォールまたはPanoramaが、最初に検出したエラーを表示し、そ れ以上エラーをチェックしません。たとえば、移動するポリシー ルールで参照されているオブジェクトが [宛先] に存在しないと、 エラーが発生します。このオプションをオフにした場合、ファイ アウォールまたはPanoramaは、先に全てのエラーを検出してから それらを表示します。

監査コメントアーカイブ

Audit Comment Archiveを選択して、選択したルールの監査コメント履歴、構成ログ、および ルール変更履歴を表示します。

Security Policy	Security Policy Rule					
General Sour	rce Destination Application Service/URL Category Actions Usage					
Name	Social Networking Apps					
Rule Type	universal (default)	~				
Description						
_						
Tags	•	~ -				
Group Rules By Tag	None	\sim				
Audit Comment						
	Audit Comment Archive					
	U U					
	ок	Cancel				

- 監査コメント
- 設定ログ (コミット間)
- ルール変更

監査コメント

選択したポリシールールのAudit Comment (監査コメント)を表示します。フィルターを適用して 保存すれば、特定の監査コメントを素早く探し、表示された監査コメントを CSV 形式でエクス ポートできます。

項目	の意味
コミット時間	監査コメントがコミットされた時間です。
監査コメント	監査コメントの内容です。
管理者	監査コメントをコミットしたユーザー。
設定バージョ ン	設定のリビジョン番号です。0は、ポリシールールが初めて作成されて Panorama にコミットされたことを示します。

設定ログ(コミット間)

選択済みのポリシールールが各コミットの間に生成した設定ログを表示します。フィルターを 適用して保存すれば、特定の設定ログを素早く探し、表示された設定ログを CSV 形式でエクス ポートできます。

項目	の意味
時間	監査コメントがコミットされた時間です。
管理者	監査コメントの内容です。
コマンド	実行されたコマンドのタイプです。
変更前	変更が発生する前のルールの情報です。例:ルールの名前を変更した場合、 以前の名前が表示されます。
変更後	変更が発生した後のルールの情報です。例:ルールの名前を変更した場合、 新しい名前が表示されます。
デバイス名	監査コメントが変更される前のデバイスの名前です。

ルール変更

選択済みのポリシールールの構成バージョンを表示・比較し、どのような変更が発生したのか分 析できます。比較したいポリシールールの2つの構成バージョンをドロップダウンリストで選 択します。

Audit Comment Archive for Security Rule test-rule					0	
Audit Comments Config Logs (between commits) Rule Changes						
31 0	Committed On 2020/06/10 13:48:46 by admin	\sim	[32 C	ommitted On 2020/06/10 13:53:23 by admin	✓ Go
1	test-rule {			1	test-rule {	
2	target {			2	target {	
3	negate no ;			3	negate no ;	
4	}			4	}	
5	source-imei any ;			5	source-imei any ;	
6	source-imsi any ;			6	source-imsi any ;	
7	source-nw-slice any ;			7	source-nw-slice any ;	
8	to <u>any</u> ;		600-	8	to <u>multicast</u> ;	
9	from any ;			9	from any ;	
10	source any ;			10	source any ;	
11	destination any ;			11	destination any ;	
12	source-user any ;		600-	12	source-user known-user ;	
13	category any ;			13	category any ;	
14	application any ;		600	14	application [facebook twitter];	
15	<pre>service application-default ;</pre>	_		15	service any ;	
16	source-hip any ;			16	source-hip any ;	
17	destination-hip any ;	17 destination-hip any ; 17 destination-hip any ;				

PAN-OS Web インターフェイスのヘルプ 11.1

ルールの使用状況ヒット数のクエリ

• ポリシー > ルールの使用状況

ルール使用状況のクエリを使用し、選択したルールベースを特定の期間でフィルタリングします。ルール使用状況のクエリを使用すれば、ポリシー ルールベースを素早くフィルタリン グして使用していないルールを特定・削除できるため、攻撃の入り口を減らすことができま す。PDF/CSVをクリックしてフィルタリングしたルールを PDF あるいは CSV 形式でエクス ポートします。Rule Usage Hit Count Query を使用するには、Policy Rule Hit Count設定(Device > Setup > Management [デバイス > セットアップ > 管理])を有効にする必要があります。

デフォルト設定では、ポリシールールベース内のルールの使用状況をクエリする際にName (名前)、Location (ロケーション)、Created (作成)、Modified (編集)、Rule Usage (ルールの使用状況)列が表示されます。列をさらに追加し、ポリシールールの詳細情報を確認できます。

タスク	の意味
ヒット数	
期間	選択したルールベースのクエリの対象期間を示します。事前定義済みの期間を 選択するか、Custom (カスタム)期間を設定します。
使用方法	クエリを行うルールの使用状況を選択します: Any (すべて)、Unused (未使 用)、Used (使用済み)、 あるいは Partially Used (一部使用済み) (Panorama の み)。
年	(カスタム期間のみ)ポリシー ルールベースのクエリの開始日時を選択しま す。
過去_日間の ルールのリ セットを除 外	このオプションを使用すれば、特定の期間(日数)中にユーザーが手動でリ セットしたルールが除外されます。
操作	
削除しま す。	選択したポリシー ルールの1つまたは複数削除します。
Enable [有効 化]	無効化になった場合、1つ以上の選択したポリシー ルールを有効にします。
無効化	選択したポリシー ルールの1つまたは複数無効化します。
PDF/CSV	現在 PDF または CSV 形式で表示されているフィルタ済ポリシー ルールをエ クスポートします。

タスク	の意味
Reset Rule Hit Counter(ルー ルヒットカ ウンターの リセット)	フィルタリングされ、現在表示されているSelected rules(選択されたルー ル)またはAll rules(すべてのルール)のルール使用状況データをリセットし ます。
タグ	1 つまたは複数のグループ タグを1 つまたは複数の選択したポリシー ルール に適用します。ポリシー ルールにタグを付けるには、グループ タグがすでに 存在している必要があります。
タグ外し	1つまたは複数のグループ タグを1つまたは複数の選択したポリシー ルール から削除します。

ルール ヒット数クエリのデバイス ルールの使用状況

Panorama 管理サーバーでポリシールールのルールの使用状況を閲覧する際、デバイスおよび仮想システムのルールの使用状況を確認できます。Reset Rule Hit Counter (ルール ヒット カウンターをリセット)して Hit Count (ヒット数)、First Hit (最初のヒット)、Last Hit (最後のヒット)をリセットします。

PDF/CSVをクリックしてフィルタリングしたルールを PDF あるいは CSV 形式でエクスポートします。

項目	の意味
デバイス グ ループ	デバイスあるいは仮想システムが属すデバイスグループです。
デバイス 名/仮想シス テム	デバイスグループあるいは仮想システムの名前です。
ヒット数	ポリシールールにマッチしたトラフィックの総数です。
最後のヒッ ト	ポリシールールにトラフィックが最後にマッチした日時です。
最初のヒッ ト	ポリシールールにトラフィックが最初にマッチした日時です。
最後の更新 の受信	デバイスから Panorama 管理サーバーに最後にルールの使用状況を受信した時の日時です。
項目	の意味
------	---
作成日時	ポリシールールが作成された日時です。
変更済	ポリシールールを最後に編集した日時です。ポリシールールが編集されていな い場合は列が空になります。
状態	デバイスの接続ステータス:Connected (接続済み)あるい はDisconnected (切断)。

セキュリティ ポリシー ルールは、セキュリティ ゾーンを参照して、アプリケーション、ユー ザーまたはユーザー グループ、およびサービス(ポートおよびプロトコル)に基づいて、 ネットワーク上のトラフィックを許可、制限、および追跡できるようにします。デフォルトで は、「rule1」という名前のセキュリティ ルールがファイアウォールに含まれています。この ルールでは、Trust ゾーンから Untrust ゾーンへのトラフィックがすべて許可されています。

知りたい内容	以下を参照
セキュリティ ポリシーとは?	セキュリティポリシーの概要 Panorama については、「ポリシールールの移動またはコ
	ピー」を参照してください。
セキュリティ ポリシー ルールを 作成する際に使用可能なフィー ルドは?	セキュリティ ポリシー ルールの構成要素
Web インターフェイスを使用し てセキュリティ ポリシー ルール を管理するには?	ポリシーの作成と管理 セキュリティ ポリシー ルールのオーバーライドまたは取り消し アプリケーションおよび使用状況 セキュリティポリシー オプティマイザー
その他の情報をお探しですか?	セキュリティ ポリ シー

セキュリティポリシーの概要

セキュリティポリシーを使用すると、ルールを適用し、アクションを実行できます。また、 必要に応じて、全般的または個別の指定を行うことができます。ポリシー ルールと受信トラ フィックに対し順番に照合されます。トラフィックに一致する最初のルールが適用されるため、 固有のルールを全般的ルールよりも先に設定する必要があります。たとえば、他のすべてのトラ フィック関連の設定が同じである場合、1つのアプリケーションに対応するルールがすべてのア プリケーションに対応するルールよりも上に来るようにしなければなりません。

 ネットワーク リソースへのアクセス試行時にエンド ユーザーの認証を確実に行う ために、ファイアウォールは認証ポリシーを評価してから、セキュリティ ポリシー を評価します。詳細は、「Policies(ポリシー) > Authentication(認証)」を参照 してください。

ユーザー定義のどのルールとも一致しないトラフィックには、デフォルト ルールが適用されま す。セキュリティ ルールベースの下部に表示されるデフォルト ルールは、すべてのイントラ ゾーン (ゾーン内) トラフィックを許可し、すべてのインターゾーン (ゾーン間) トラフィックを 拒否するよう事前定義されています。これらのルールは、事前定義済み設定に含まれ、デフォルトで読み取り専用ですが、Override[オーバーライド]して、タグ、アクション(許可または拒否)、ログ設定、セキュリティプロファイルなど、限定された複数の設定を変更することができます。

インターフェイスには、セキュリティ ポリシー ルールを定義する以下のタブが含まれていま す。

- General (全般) General (全般) タブを選択して、セキュリティ ポリシー ルールの名前 と説明を設定します。
- Source[送信元] Source[送信元]タブを選択して、トラフィックの送信元ゾーンまたは送信元 アドレスを定義します。
- User[ユーザー] User[ユーザー]タブを選択して、個々のユーザーまたはユーザーのグループのポリシーを適用します。ホスト情報プロファイル(HIP)が有効な GlobalProtect[™]を使用している場合、GlobalProtect が収集した情報に基づいてポリシーを適用することもできます。たとえば、ユーザーのアクセスレベルを、ファイアウォールにユーザーのローカル設定を通知する HIP によって判別することができます。HIP 情報を使用して、ホストで実行中のセキュリティプログラム、レジストリ値、およびホストにアンチウイルス ソフトウェアがインストールされているかどうかなど他の多くのチェックを基に、詳細なアクセス制御を行うことができます。
- Destination[宛先] Destination[宛先]タブを使用して、トラフィックの宛先ゾーンまたは宛 先アドレスを定義します。
- Application[アプリケーション] Application[アプリケーション]タブを選択して、アプリケーションまたはアプリケーション グループに基づいて、ポリシーがアクションを実行するように指定します。管理者は、既存の App-ID[™] シグネチャを使用し、カスタマイズして、独自のアプリケーションや、既存のアプリケーションの特定の属性を検出することもできます。カスタム アプリケーションは Objects(オブジェクト) > Applications(アプリケーション)で定義されます。
- Service/URL Category(サービス/URL カテゴリ) Service/URL Category(サービス/URL カテゴリ)タブを選択して、TCP や UDP のポート番号または URL カテゴリをポリシーの一 致条件として指定できます。
- Action[アクション] Action[アクション]タブから、定義されたポリシー属性に一致するトラフィックに基づいて実行されるアクションを定義します。
- Target (宛先) Target (宛先) タブを選択して、セキュリティ ポリシー ルールのデバイス またはタグを指定します。
- Usage (使用状況)–Usage (使用状況)タブを選択すれば、ルールで発見されたアプリケーションのかず、ルールで最後に新しいアプリケーションが発見された時、ヒット数データ、過去30日間のトラフィック、ルールが作成された時、最後に編集された時など、ルールの使用状況を確認できます。

セキュリティ ポリシー ルールの構成要素

以下のセクションでは、個々のセキュリティ ポリシー ルールの構成要素について説明します。 セキュリティ ポリシー ルールを作成する際には、以下に示す各オプションを設定できます。

セキュリティ ルール の構成要素	設定場所	の意味
ルール番号	該当なし	ファイアウォールが自動的に各ルールに番号を振り、 ルールが移動するとルールの順序が変更されます。特 定のフィルタに一致するようにルールをフィルタリン グすると、各ルールはルールベース内の全ルールのコ ンテクストで番号が振られ、評価順に従って並べられ ます。
		Panorama は独立してプレルールおよびポストルール に番号を振ります。Panorama が管理対象ファイア ウォールにルールをプッシュすると、付番の際に、 ルールベース内のプレルール、ファイアウォールルー ル、およびポストルールの階層が考慮され、その番号 がルールの並びと評価順に反映されます。
氏名	一般	ルールを識別する名前を入力します。名前の大文字 と小文字は区別され、文字、数字、スペース、ハイ フン、およびアンダースコアを含む最大 63 文字を 指定できます。ルール名はファイアウォールおよび Panorama 上で一意でなければなりません。また、 デバイス グループとその先祖または子孫デバイス グ ループ内でも一意でなければなりません。
ルールの種類		 ルールがゾーン内、ゾーン間、その両方のどれに適用 されるかを指定します。 universal[ユニバーサル] (デフォルト) - 指定さ れた送信元ゾーンおよび宛先ゾーン内の一致する すべてのインターゾーントラフィックとイントラ ゾーントラフィックにルールを適用します。たと えば、送信元ゾーンがAとBで、宛先ゾーンがA とBのユニバーサル ルールを作成するとします。 ルールは、ゾーンA内のすべてのトラフィック、 ゾーンB内のすべてのトラフィック、ゾーンAか らゾーンBへのすべてのトラフィック、ゾーンB からゾーンAへのすべてのトラフィックに適用さ れます。 intrazone[イントラゾーン] - 指定された送信元 ゾーン内の一致するすべてのトラフィックにルー ルを適用します (イントラゾーンルールには宛 先ゾーンを指定できません)。たとえば、送信元 ゾーンをAとBに設定するとします。ルールは、 ゾーンA内のすべてのトラフィック、ゾーンB内 のすべてのトラフィックに適用されますが、ゾー

セキュリティ ルール の構成要素	設定場所	の意味
		 ンAとゾーンB間のトラフィックには適用されません。 interzone[インターゾーン] – 指定された送信元 ゾーンおよび宛先ゾーン間の一致するすべてのト ラフィックにルールを適用します。たとえば、送 信元ゾーンをA、B、C、宛先ゾーンをA、Bに設 定したとします。ルールは、ゾーンAからゾーン B、ゾーンBからゾーンA、ゾーンCからゾーン A、ゾーンCからゾーンBへのトラフィックには 適用されますが、ゾーンA、B、またはC内のトラ フィックには適用されません。
の意味		ポリシーの説明を入力します(最大 1,024 文字)。
tags		ポリシーのタグを指定します。 ポリシータグとは、ポリシーをソートまたはフィル タリングできるキーワードや語句です。多数のポリ シーを定義していて、特定のキーワードでタグが付け られたポリシーを表示する場合に役立ちます。たとえ ば、特定のルールに「復号」や「復号なし」といった 特定の語でタグを付けたり、特定のデータセンター に関するポリシーにその場所の名前を使用したりでき ます。 デフォルトルールにタグを追加することもできま す。
Source Zone	送信元	送信元ゾーンを Add (追加) します (デフォルトは Any (すべて))。ゾーンは同じタイプ (Layer 2 [レ イヤー 2]、Layer 3 [レイヤー 3]、virtual wire [バー チャル ワイヤー]) である必要があります。新しいゾー ンを定義する手順については、「Network (ネット ワーク) > Zones (ゾーン)」を参照してください。 複数のゾーンを使用して管理を簡略化できます。たと えば、信頼されていない宛先ゾーンが指定されている 3 つの異なる内部ゾーン (マーケティング、販売、広 報) がある場合、すべてのケースを対象とした 1 つの ルールを作成できます。
送信元アドレス	送信元	送信元アドレス、アドレス グループ、または地域 を Add (追加) します (デフォルトは Any (すべ て))。ドロップダウンリストから選択するか、ド ロップダウンリストの下部にある Address (アドレ

セキュリティ ルール の構成要素	設定場所	の意味
		 ス)オブジェクト、Address Group(アドレスグループ)、またはRegions(地域)を選択して設定を行います。Objects(オブジェクト)>Addresses(アドレス)およびObjects(オブジェクト)>AddressGroups(アドレス/シープ)はそれぞれ、セキュリティポリシールールがサポートしているアドレスオブジェクトおよびアドレスグループのタイプを示します。 Negate (無効化)オプションを選択すると、指定したアドレスではなく、指定したゾーンからの送信元アドレスにルールが適用されます。
送信元ユーザー	送信元	このポリシーを適用する送信元ユーザーまたはユー ザー グループをAdd (追加)します: • any – ユーザー データに関係なく任意のトラ
		 フィックが含まれます。 pre-logon[ログイン前] – GlobalProtect を使用して ネットワークに接続しているが、自分のシステム にはログインしていないリモートユーザーが含ま れます。GlobalProtect エンドポイントのポータル に Pre-logon (プレログオン)オプションが設定さ れている場合、自分のマシンに現在ログインして いないユーザーは、ユーザー名 pre-logon として識 別されます。pre-logon ユーザー用のポリシーを作 成でき、また、ユーザーが直接ログインしていな くても、そのマシンは完全にログインしているか のようにドメインで認証されます。
		 known-user(既知のユーザー) – 認証されたす べてのユーザー(ユーザー データがマッピングさ れた IP アドレス)が含まれます。このオプション は、ドメインの「ドメイン ユーザー」グループに 相当します。
		 unknown[未知] – 認証されていないすべてのユー ザー(ユーザーにマップされていない IP アドレス) が含まれます。たとえば、unknown(未知)はゲ ストレベルのアクセスに使用できます。これら のユーザーは、ネットワーク上の IP アドレスを 持っていますが、ドメインに認証されず、ファイ アウォール上に IP アドレス対ユーザーのマッピン グ情報がないためです。
		 select[選択] – このウィンドウで選択したユーザー が含まれます。たとえば、1人のユーザー、個々の

セキュリティ ルール の構成要素	設定場所	の意味
		ユーザーのリスト、グループを追加したり、手動 でユーザーを追加する場合があります。
		⑦ ファイアウォールが User-ID [™] エージェ ントではなく、RADIUS、TACACS+、ま たは SAML アイデンティティ プロバイ ダ サーバーからユーザー情報を収集し ている場合、ユーザーのリストは表示さ れません。ユーザー情報を手動で入力す る必要があります。
送信元デバイス	送信元	ポリシー対象ホスト デバイスのAdd(追加):
		• any(すべて)—すべてのデバイスを含めます。
		 no-hip(HIPなし) – HIP 情報を必要としません。この設定により、HIP 情報を収集または送信できないサードパーティ デバイスからのアクセスが可能になります。
		 quarantine (隔離) –quarantine list (隔離リスト) のすべてのデバイスを含みます (Device (デバイ ス) > Device Quarantine (デバイスの隔離))。
		 select(選択) – 設定で選択されるデバイスが含ま れます。例えば、モデル、OS、OS ファミリー、ま たはベンダーに基づき、デバイスオブジェクトを 追加することができます。
送信元 HIP プロ ファイル	送信元	ホスト情報プロファイル (HIP) をAdd (追加) すると、 最新のセキュリティ パッチやアンチウイルス定義 がインストールされているかなどエンド ホストのセ キュリティ状態に関する情報を収集できます。ポリ シーの適用にホスト情報を使用することで、重要なリ ソースにアクセスするリモート ホストが適切に整備 された、セキュリティ標準に準拠した粒度の細かいセ キュリティを実現でき、その後に、ネットワーク リ ソースへのアクセスを許可できます。以下の送信元 HIP プロファイルがサポートされます。
		 any(任意) – HIP 情報に関係なく任意のエンドポ イントが含まれます。
		 select(選択) – 設定で選択した HIP プロファイ ルが含まれます。たとえば、1 つの HIP プロファ イルや HIP プロファイルのリストを追加したり、 手動で HIP プロファイルを追加できます。

セキュリティ ルール の構成要素	設定場所	の意味
		 no-hip(HIPなし) – HIP 情報を必要としません。この設定により、HIP 情報を収集または送信できないサードパーティ クライアントからのアクセスが可能になります。
送信元サブスクラ イバ	送信元	以下の形式で、5G または 4G ネットワークに 1 つま たは複数の送信元サブスクライバを Add(追加)しま す。
		 [any] (5Gのみ) IMSI を含む5GSubscription Permanent Identifier (SUPI、サブスクリプション永続識別 子)
		• IMSI(14 または 15桁)
		● ハイフン区切りの 11~15 桁の IMSI 値の範囲
		 6桁の IMSI プレフィックスです。プレフィックスの後にワイルドカードとしてアスタリスク(*)を付けます。
		• IMSI を指定する EDL
送信元機器		以下の形式で、5G または 4G ネットワークに 1 つま たは複数の送信元機器 ID を Add(追加)します。
		• [any]
		 (5Gのみ) International Mobile Equipment Identity (IMEI) を含む5G Permanent Equipment Identifier (PEI、永続機器識別子)
		● IMEI(11~16 桁の長さ)
		 Type Allocation Code(TAC、タイプ割り当てコード)の8桁のIMEIプレフィックス
		• IMEI を指定する EDL
ネットワーク スラ イス	送信元	以下の通り、5G ネットワークのネットワーク スライ ス サービス タイプ (SST) に基づき、1 つまたは複数 の送信元ネットワーク スライスをAdd (追加) しま す。
		• 標準(事前定義済)SST
		 eMBB(enhanced Mobile Broadband、拡張モバ イルブロードバンド) –ビデオ ストリーミング 等のより速度が高く、高データレートを実現し ます。

セキュリティ ルール の構成要素	設定場所	の意味
		 URLLC (Ultra-Reliable Low-Latency Communications、超高信頼低遅延通信) –重要 な loT (ヘルスケア、ワイヤレス決済、ホーム コントロール、車両通信)等、遅延に影響を受 けやすいミッション クリティカルなアプリケー ション向け。 MloT (Massive Internet of Things、大規模な モノのインターネットー例えば、スマートメー ター、スマート廃棄物管理、盗難防止、資産管 理、位置追跡等。 ネットワークスライス SST - 通信事業者固有-ス ライス名を選択し、指定します。スライス名の形
		式は、テキストの後にコンマ(,)と数字を付けま す(128~255 の範囲)。例えば、「Enterprise Oil2,145」と入力します。
Destination Zone	宛先	 宛先ゾーンを Add (追加) します (デフォルトは any (任意))。ゾーンは同じタイプ (Layer 2 [レイ ヤー2]、Layer 3 [レイヤー3]、virtual wire [バーチャ ルワイヤー])である必要があります。新しいゾーン を定義する手順については、「Network (ネットワー ク) > Zones (ゾーン)」を参照してください。 複数のゾーンを使用して管理を簡略化できます。たと えば、信頼されていない宛先ゾーンが指定されている 3つの異なる内部ゾーン (マーケティング、販売、広 報)がある場合、すべてのケースを対象とした1つの ルールを作成できます。 イントラゾーンルールは、送信元と宛 先が同じゾーン内にあるトラフィック にのみ一致するため、宛先ゾーンを定義 できません。イントラゾーンルールに 一致するゾーンを指定する場合、送信元
宛先アドレス		宛先アドレス、アドレス グループ、または地域を Add (追加) します (デフォルトは Any (すべて))。 ドロップダウンリストから選択するか、ドロップダ ウンリストの下部にある Address (アドレス) オ ブジェクトをクリックし、Address Group (アドレ スグループ)、またはRegions (地域)を選択して アドレス設定を指定します。Objects (オブジェク

セキュリティ ルール の構成要素	設定場所	の意味
		ト)>Addresses (アドレス)およびObjects (オブジェク ト)>AddressGroups (アドレスグループ)はそれぞれ、 セキュリティポリシー ルールがサポートしているア ドレスオブジェクトおよびアドレスグループのタイ プを示します。
		Negate (無効化)オプションを選択すると、指定したアドレスではなく、指定したゾーン内の宛先アドレスにルールが適用されます。
宛先デバイス		ポリシー対象ホスト デバイスのAdd(追加):
		● any(すべて)−すべてのデバイスを含めます。
		 quarantine (隔離) –quarantine list (隔離リスト) のすべてのデバイスを含みます (Device (デバイ ス) > Device Quarantine (デバイスの隔離))。
		 select(選択) – 設定で選択されるデバイスが含ま れます。例えば、モデル、OS、OS ファミリー、ま たはベンダーに基づき、デバイスオブジェクトを 追加することができます。
アプリケーション	Application [アプリケー ション]	セキュリティポリシールールについて、特定のアプ リケーションをAdd (追加)します。アプリケーション に複数の機能がある場合、アプリケーション全体また は個別の機能を選択できます。アプリケーション全体 を選択した場合、すべての機能が含まれ、将来、機能 が追加されるとアプリケーション定義が自動的に更新 されます。
		セキュリティポリシールールでアプリケーショング ループ、フィルタ、またはコンテナを使用している場 合は、Application(アプリケーション)列のオブジェ クトの上にマウスを置き、ドロップダウンリストを 開いて Value(値)を選択すると、オブジェクトの詳 細が表示されます。これにより、Object[オブジェク ト]に移動しなくても、ポリシーからアプリケーショ ンメンバーを直接表示することができます。

セキュリティ ルール の構成要素	設定場所	の意味
		常に一つあるいは複数のアプリケーションを指定することで、ネットワーク上で許可したいアプリケーションだけを許可し、攻撃の入り口を減らしてネットワークトラフィックをしっかり制御できるようにしてください。アプリケーションをany(すべて)に設定しないでくさい。そうするとすべてのアプリケーションのトラフィックが許可され、攻撃の入り口が増えてしまいます。
サービス	サービス /URL カテゴリ	特定の TCP または UDP のポート番号に制限したい サービスを選択します。ドロップダウンリスト リス トから以下のいずれかを選択します。
		 any - 選択したアプリケーションがすべてのプロトコルやポートで許可または拒否されます。 application-default (アプリケーション-デフォルト) - 選択したアプリケーションが、Palo Alto Networks[®] によって定義されたデフォルトのポートでのみ許可または拒否されます。このオプションは、許可ポリシーに使用することをお勧めします。標準以外のポートやプロトコルで実行されるアプリケーションは、意図的である場合を除き、動作と使用方法が望ましくない可能性があります。このオプションを許可ポリシーに使用することで、そうしたアプリケーションの実行を禁止できます。
		 このオプションを使用しても、ファイア ウォールはすべてのポートのすべてのア プリケーションをチェックしますが、 アプリケーションはデフォルトのポー ト/プロトコルでのみ許可されます。

セキュリティ ルール の構成要素	設定場所	の意味
		 大抵のアプリケーションの場合 はapplication-defaultを使用し、アプリケーションが標準的でないポートを使 用したり、他の悪意のある挙動を生じさ せたりしないようにします。アプリケー ションのデフォルトのポートが変わる と、ファイアウォールが自動的にルール を更新してデフォルトのポートを修正し ます。内部のカスタムアプリケーショ ンのように標準的でないポートを使用 するアプリケーションについては、アプ リケーションを修正するか、標準的でな いポートを指定するルールを作成し、対 象のアプリケーションを必要とするトラ フィックにのみルールを適用します。 Select(選択) – 既存のサービスをAdd(追 加)するか、Service(サービス)またはService
		Group (サービス グループ)を選択して新しいエ ントリを指定します。(または Objects (オブジェ クト) > Services (サービス) および Objects (オ ブジェクト) > Service Groups (サービス グルー プ)を選択します)。
URL カテゴリ		セキュリティ ルールを適用する URL カテゴリを選択 します。
		 URL カテゴリに関係なくすべてのセッションを許 可または拒否するには、any を選択します。
		 カテゴリを指定するには、ドロップダウンリスト リストから特定のカテゴリ (カスタム カテゴリを 含む)を Add (追加) します。Objects (オブジェ クト) > External Dynamic Lists (外部動的リス ト)を選択して、カスタム カテゴリを定義しま す。
アクション設定	操作	ルールで定義されている属性にマッチするトラフィッ クに対してファイアウォールが適用する Action (アク ション) を選択します:
		• Allow(許可)–(デフォルト)一致するトラ フィックを許可します。
		 Deny(拒否) – 一致するトラフィックをブロックし、拒否されるアプリケーションについて定義

セキュリティ ルール の構成要素	設定場所	の意味
		されたデフォルトのアクションの拒否を実行し ます。アプリケーションについてデフォルトで 定義されている拒否アクションを表示するには、 (Objects (オブジェクト) > Applications (アプ リケーション))でアプリケーションの詳細情報 を表示します。
		デフォルトの拒否アクションはアプリケーションに よって異なるため、ファイアウォールは、あるアプ リケーションについては、セッションをブロックして リセットを送信し、別のアプリケーションについては セッションを暗黙にドロップするといったアクション を実行します。
		 Drop[ドロップ] – アプリケーションをサイレン トにドロップします。TCP リセットはホストま たはアプリケーションに送信されません。ただ し、Send ICMP Unreachable(ICMP 送信到達不 能)を選択した場合を除きます。
		 Reset client[クライアントのリセット] – クライア ント側デバイスに TCP リセットを送信します。
		• Reset server[サーバーのリセット] – サーバー側デ バイスに TCP リセットを送信します。
		 Reset both client and server[クライアントおよび サーバー両方のリセット] – クライアント側とサー バー側の両方のデバイスに TCP リセットを送信し ます。
		 Send ICMP Unreachable (ICMP 送信到達不能) ーレイヤー3インターフェイスでのみ使用できま す。トラフィックのドロップや接続のリセットを 行うようにセキュリティポリシールールを設定 すると、トラフィックが宛先ホストに到達しない 場合があります。そのような場合は、ドロップさ れるすべての UDP トラフィックおよび TCP トラ フィックについて、トラフィックの送信元 IP アド レスに ICMP 到達不能応答を送信するようにファ イアウォールを設定できます。この設定を有効に すると、送信元は正規の手順に従ってセッション をクローズまたはクリアできるため、アプリケー ションの処理が中断するのを防ぐことができま す。
		ファイアウォールに設定されている ICMP 到達不能 パケット率を確認するには、(Device (デバイス) >

セキュリティ ルール の構成要素	設定場所	の意味
		Setup(セットアップ) > Session(セッション))の Session Settings(セッション設定)を表示します。
		事前定義済みのインターゾーンおよびイントラゾー ン ルールに定義されているデフォルト アクションを オーバーライドする方法については、「セキュリティ ルールのオーバーライドまたは取り消し」を参照して ください。
プロファイル設定	操作	セキュリティプロファイル ルールと一致する パケットに対してファイアウォールが実行す る追加チェックを指定するには、Antivirus(ア ンチウイルス)、Vulnerability Protection(脆 弱性防御)、Anti-Spyware(アンチスパイウェ ア)、URL Filtering(URL フィルタリング)、File Blocking(ファイルブロッキング)、Data Filtering(データフィルタリング)、WildFire Analysis(WildFire 分析)、Mobile Network Protection(モバイルネットワーク保護)、および SCTP Protection(SCTP 保護)の各プロファイルを選 択します。
		個々のプロファイルではなくプロファイル グループ を指定するには、Profile Type (プロファイル タイ プ)をGroup (グループ)と選択してから、Group Profile (グループ プロファイル)を選択します。
		新しいプロファイルやプロファイル グループを定 義するには、該当するプロファイルの隣のNew(新 規)をクリックするか、New Group Profile(新規プ ロファイル グループ)を選択します。
		Security Profiles(セキュリティ プロファイル)(ま たはプロファイル グループ)をデフォルト ルールに 関連付けることもできます。
ログ設定およびそ の他の設定	操作	ルールに一致するトラフィックのエントリをローカル トラフィック ログに生成するには、以下のオプショ ンを選択します。

セキュリティルール	設定場所	の意味
の構成要素		
		 Log At Session Start (セッション開始時にロ グ) (デフォルトではオフ) – セッション開始の トラフィック ログ エントリを生成します。
		 ACC でアクティブな GRE トンネル を表示するトンネル セッションやト ラブルシューティングが目的でない 限り、Log at Session Start (セッショ ン開始時にログ)を有効化しないでく ださい。例えば facebook-base から facebook-chat へ数パケットが生じた 後にアプリケーションが変更する場 合、セッション終了時のロギングは あまりリソースを消費せずにアプリ ケーションを正確に識別します。 Log At Session End (セッション終了時にロ
		グ)(デフォルトではオン) – セッション開始の トラフィック ログ エントリを生成します。
		 セッションの開始または終了のエントリ がログに記録される場合、drop []ドロッ プおよび deny [拒否]のエントリもログ に記録されます。
		 Log Forwarding Profile (ログ転送プロファイル) – ローカル トラフィック ログと脅威ログのエント リをリモートの宛先 (Panorama サーバーや Syslog サーバーなど) に転送するには、ドロップダウンリ スト リストから Log Forwarding Profile (ログ転送 プロファイル)を選択します。
		

セキュリティ ルール の構成要素	設定場所	の意味
		ログ転送プロファイルを作成・有効化し、専用の外部ストレージデバイスにログを送信します。ファイアウォールのログの保存領域には限界があり、容量が一杯になるとファイアウォールは最も古いログをパージするため、これによってログを保持できます。
		デフォルト ルールのログ設定を変更することもでき ます。以下のオプションを任意に組み合わせて指定し ます。
		 Schedule (スケジュール) – ルールを適用する日時を制限するには、ドロップダウンリストからスケジュールを選択します。必要に応じて、New (新規) スケジュールを定義します(「復号化された SSLトラフィックを制御するための設定」を参照)。
		 QoS Marking (QoSマーキング) – ルールに一 致するパケットの Quality of Services (QoS) の設定を変更するには、IP DSCP または IP Precedence (IP優先度)を選択して、QoS の 値を 2 進数形式で入力するか、事前に定義 されている値をドロップダウン リストから 選択します。QoS の詳細は、「サービス品 質 を参照してください。
		 Disable Server Response Inspection (サーバー レ スポンス検査の無効化) –サーバーからクライアン トに送信されるパケットの検査を無効にします。 このオプションはデフォルトで無効になっていま す。
		 最高のセキュリティ体制のために、 Disable Server Response Inspection を有効にしないでください。この オプションを選択すると、ファ イアウォールはクライアントから サーバーへのフローのみ検査しま す。server-to-clientのフローは検査さ れないため、これらのトラフィック フローに脅威があるかどうかを識別 できません。

セキュリティ ルール の構成要素	設定場所	の意味
基本	ルールの使用 状況	 Rule Created (ルールの作成時–ルールを作成した日時です。 Last Edited (最終変更)–ルールが最後に編集された日次です。
アクティビティ	ルールの使用 状況	 Hit Count (ヒット数)–トラフィックがルールにマッチ(ヒット)した回数の合計です。 First Hit (最初のヒット)–初めてルールがマッチした時です。 Last Hit (最後のヒット)–最後にルールがマッチした時です。
アプリケーション [applications]	ルールの使用 状況	 Applications Seen (発見されたアプリケーション)ールールが許可するアプリケーションの数です。 Last App Seen (最後に発見されたアプリケーションの数です。) Last App Seen (最後に発見されたアプリケーション)が 前に発見されたことがないアプリケーション)が 発見された時から経過した日数です。 Compare Applications & Applications Seen (アプ リケーションおよび発見されたアプリケーション) を比較)ークリックすると、ルールで設定されてい るアプリケーションとルールで発見されたアプリ ケーションを比較できます。このツールを使用す れば、ルールにマッチするアプリケーションを探 し、それらをルールに追加することができます。
トラフィック(過 去 30 日間)	ルールの使用 状況	 Bytes (バイト数)-過去 30 日間のルールのトラフィック量(バイト)です。 最も古いルールはトラフィックの 累積量が最も多くなりがちであるため、期間を 30 日より長くするとその ルールがリストの一番上に残り続けるでしょう。そのため、新しいルー ルに大量のトラフィックがあって も、古いルールの下にリストアップされる可能性があります。

セキュリティ ルール の構成要素	設定場所	の意味
任意 (すべての対象 デバイス) Panorama のみ	ターゲット	ポリシー ルールをデバイス グループのすべての管理 対象ファイアウォールにプッシュするには、有効化 (チェックをオン)にします。
デバイス Panorama のみ		ポリシー ルールをプッシュするデバイス グループに 関連付けられた 1 つまたは複数の管理対象ファイア ウォールを選択します。
tags Panorama のみ	-	指定したタグを持つデバイス グループ内の管理対象 ファイアウォールにポリシー ルールをプッシュする には、1つまたは複数のタグをAdd(追加)します。
これらの指定され たデバイスとタグ のみをターゲット に設定する		選択したデバイスとタグを除き、デバイス グルー プに関連付けられているすべての管理対象ファイア ウォールにポリシー ルールをプッシュするには、有 効化(チェックをオンに)します。
Panorama のみ		

ポリシーの作成と管理

Policies(ポリシー) > **Security**(セキュリティ)ページでは、セキュリティ ポリシーの追加、 変更、および管理が可能です。

タスク	の意味
コンテキスト の	新しいポリシールールをAdd (追加)するか、新しいルールのベースとなる ルールを選択してClone Rule (ルールをコピー)します。コピーされたルール 「rulen」が選択したルールの下に挿入されます。n は次に使用可能な整数 で、これによりルール名が一意になります。コピーの詳細は、「ポリシー ルールの移動またはコピー」を参照してください。
変更	設定を変更するルールを選択します。 Panorama からプッシュされたルールは、ファイアウォールでは読み取り専 用となるため、ローカルでは編集できません。
	Override(オーバーライド)およびRevert(元に戻す)アクションは、セキュリティルールベースの最下部に表示されるデフォルトルールにのみ適用されます。事前定義ルール、すなわち、すべてのイントラゾーントラフィックを許可し、すべてのインターゾーントラフィックを拒否するルールは、ファイアウォールに、ルールベース内の他のどのルールとも一致しないトラフィックの処理方法を指示するものです。これらのルールは事前定義済み設

タスク	の意味
	定に含まれるため、Override (オーバーライド)して一部のポリシー設定を編 集する必要があります。Panorama を使用している場合、デフォルト ルール を Override(オーバーライド)して、Device Groups(デバイス グループ) コンテキストまたはShared(共有)コンテキストでファイアウォールにプッ シュすることもできます。デフォルト ルールを元に戻すこともできます。こ れにより、事前定義済み設定や Panorama からプッシュされた設定が復元さ れます。詳細は「セキュリティ ルールのオーバーライドまたは取り消し」を 参照してください。
移動	ルールは、Policies(ポリシー)ページに列挙されている順序で、上から下 に評価されます。ネットワークトラフィックに対してルールを評価する順 序を変更するには、ルールを選択して、Move Up (上へ移動)、Move Down (下へ移動)、Move Top (最上部へ移動)、Move Bottom (最下部へ移動)、また はMove to a different rulebase or device group (別のルールベースあるいはデ バイスグループに移動)します。詳細は、「ポリシー ルールの移動またはコ ピー」を参照してください。
UUID のコ ピー	ルールの UUID をクリップボードにコピーし、設定やログを検索する際に使用できるようにします。
Delete(削 除)	既存のルールを選択してDelete (削除)します。
有効化/無効 化	ルールを無効にするには、選択して Disable (無効)にします。無効になっているルールを有効にするには、選択して Enable (有効)にします。
ルールの使用 状況のモニ ター	 ファイアウォールを前回再起動して以来使用されていないルールを特定したい場合は Highlight Unused Rules(未使用のルールをハイライト表示)します。未使用のルールの背景は点線で表示されます。その上で、ルールをDisable (無効)にするか、Delete (削除)するかを判断します。現在使用されていないルールは黄色い網掛けで表示されます。ポリシー ルールヒットカウントが有効である場合は、Hit Count(ヒット数)データはルールが使用されていないかどうかを判断するために使われます。

タスク	の意味										
							Si	ource			Dest
			NAME	TAGS	туре	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRES
		1	Block QUIC UDP	none	universat	🎮 13-vkin-truis):	any	any	any	Man-trust	any. 🔶
		2	Block QUIC	'none-	universal	🚝 13-vilan-tirust	auv	əriy.	any.	M-initiat-	any.
		3	ssh-access	none	universal	🛯 I3-vlan-trust	any	any	any	I3-untrust	any
					- tailorenation	022000000000	000000000000000000000000000000000000000	000000000000000000000000000000000000000		Sinkhole	00000
			smp-eame	none	universai	13-vian-trust	any	arry	arry	Sinkhole.	
		5	smb	none	universal	🛛 13-vlan-trust	any	any	any	Sinkhole	any
		6	Tsunami-filo-transfer	none	universal	🚝 13-vkin-trus)	any	arty.	any	Mainitrust-	any.
		•	Add 😑 Delete 💿 C	lone 🔞 Override	Revert	🕢 Enable 🚫 Di	isable Move 🗸 🛛 🕻	🗐 PDF/CSV 🔽 Hig	hlight Unused Rule	s	* >>
Rule Hit Counter (ルー ルヒットカ ウンターのリ セット)	Hit Count (ビット数) はホリシー ルールの総トラフィック ヒットを追跡し ます。総トラフィック ヒット数は再起動、アップグレード、データプレーン の再起動後も存続します。 あるいは、Reset Rule Hit Counter (ルールのヒット カウンターをリセッ ト) (最下部のメニュー) します。ヒット数統計を消去するには、All Rules (すべてのルール) を選択するか、指定のルールを選択して Selected rules (選択したルール) のヒット数統計のみをリセットします。										
	Hit (最初) 西暦) の 最後にと Hit (最初)	初 所 い 浅	のヒット ジ式で表 > トした・ のヒット)を表 示される ヒキュ ^ー)を表	示し ます。 リティ 示し	ます。 この値 ィポリ : ます。	日付は 直はリセ シーの日 日付は	hh:mm: ≤ットで ∃付を確 hh:mm:	ss year きませ 認する ss year	(時間 ん。 には、 (時間	:分:秒、 Last :分:秒、
	西暦)の	D开	ジ式で表示	示される	ます。	この値	直はリセ	ミットで	きませ	h_{\circ}	
列の表示/非 表示	Policies す。列名	(オ ムを	ペリシー) と選択すれ	のとこ hば表え	ろに剥 示を切	表示され 刃り替え	れる各列 こられま	削の表示 て。	;/非表元	示を切り)替えま

タスク	の意味	
	DASHBOARD AC NAME Image: Constraint of the second	C MONITOR POLICIES OBJECTS NETWORK Image: Comparing the second sec
フィルタの適 用	 リストにフィルタを適用するは ウンリストリストから選択し プダウンリストでFilter (フィル デフォルトルールはルー るため、常にフィルタリ す。 ポリシーに一致するものとして 表示するには、ルール名のドロ ビューワ)を選択します。 	こは、Filter Rules[フィルタ ルール] ドロップダ ます。フィルタを定義するには、項目のドロッ レタ)を選択します。 ールベースフィルタリングの対象外であ リング後のルールリストに表示されま てログに記録されたネットワーク セッションを コップダウンリスト リストでLog Viewer (ログ
	現在の値を表示するには、項 します。列メニューから項目 こともできます。たとえば、 示するには、Address (アドレ ドロップダウンリストでValue ジェクト]タブに移動しなくて る IP アドレスを迅速に確認で	目のドロップダウンリストでValue (値)を選択 を直接編集、フィルタリング、または削除する あるアドレス グループに含まれるアドレスを表 ス)列内のオブジェクトにカーソルを合わせ、 e (値)を選択します。これにより、Object[オブ も、アドレス グループのメンバーおよび対応す きます。
	オブジェクト名またはIPアドレ ブジェクトを検索する場合は はフィルターに一致した項目の ブジェクトに対しても有効で 場合、そのアドレスを含むポ OASHEOARD ACC MONITOR Q(1921662.13 GUICE UDRESS USER DEVIC	レスをもとに、ポリシー内で使用されているオ フィルターを使用します。フィルターの適用後 のみが表示されます。フィルターは埋め込みオ す。たとえば、10.1.4.8 でフィルタリングした リシーのみが表示されます。

タスク	の意味
ルールの プレビュー (<mark>Panoramaの</mark> み)	Preview Rules (ルールのプレビュー)から、ルールを管理対象ファイア ウォールにプッシュする前にルールのリストを表示することができます。大 量のルールに目を通しやすいように、各ルールベース内でルールの階層がデ バイスグループ(および管理対象ファイアウォール)ごとに視覚的に区別さ れて表示されます。
設定タイトル のエクスポー ト	最低限の読み取り専用アクセス権を持つ管理ロールは、ポリシールール ベースを PDF/CSV としてエクスポートできます。フィルターを適用して、 監査などの必要性に応じて具体的な表構成出力を作成することができま す。Web インターフェイスで表示可能な列のみがエクスポートされます。 「Configuration Table Export(設定バンドルのエクスポート)」を参照して ください。
使用されてい ないルールの 強調表示	トラフィックにマッチしないポリシールールをRule Usage (ルールの使用状 況)列でハイライト表示します。
グループ	 View Rulebase as Groups (ルールベースをグループで表示)のボックスに チェックを入れている場合にタグ グループを管理します。次の操作を実行で きます。 グループ内のルールを別のルールベースまたはデバイス グループに移動- 選択したタグ グループを別のデバイス グループに移動します。 すべてのルールのグループを変更する - 選択したタグ グループ内のルール をルールベース内の別のタグ グループに移動します。 グループ内のすべてのルールを削除する - 選択したタグ グループ内のすべ てのルールを削除します。 グループ内のすべてのルールをクローンする:選択したタグ グループ内の ルールをデバイス グループにクローンします。
ルールベース をグループと して表示	View Rulebase as Groups (ルールベースをグループとして表示)すれ ば、Group Rules by Tag (タグに基づいてルールをグループ化)で使用している タグを使ってポリシー ルールベースを表示できます。選択したタグ グループ に属すポリシールールが表示されます。
ポリシーマッ チのテスト	選択したポリシー ルールベースの保護ポリシーのテストを行い、正しいトラ フィックが拒否・許可されることを検証します。

セキュリティ ポリシー ルールのオーバーライドまたは取り消し

デフォルトのセキュリティルールである interzone-default と intrazone-default には事前定義済 みの設定がありますが、これは、ファイアウォールまたはPanorama上でオーバーライドできま す。ファイアウォールがデバイス グループからデフォルト ルールを受信する場合は、デバイス グループ設定もオーバーライドできます。オーバーライドが実行されるファイアウォールまた は仮想システムには、ローカルバージョンのルールが設定情報の中に格納されています。オー バーライド可能な設定は、フルセットの一部です(以下の表にセキュリティルールの一部を示し ます)。デフォルト セキュリティ ルールの詳細は、「Policies(ポリシー) > Security(セキュリ ティ)」を参照してください。

ルールをオーバーライドするには、ファイアウォールでは Policies(ポリシー) > Security(セ キュリティ)を、Panorama では Policies(ポリシー) > Security(セキュリティ) > Default Rules(デフォルト ルール)を選択します。名前列には、オーバーライド可能なルールの継承ア イコン(●)が表示されます。ルールを選択し、Override[オーバーライド] をクリックして、 以下の表に示した各設定を編集します。

オーバーライドしたルールを事前定義の設定または Panorama デバイス グループからプッシュされた設定に戻すには、ファイアウォールでは Policies(ポリシー) > Security(セキュリティ) > Default リティ)を、Panorama では Policies(ポリシー) > Security(セキュリティ) > Default Rules(デフォルト ルール)を選択します。名前列には、オーバーライドされた値を持つルール のオーバーライド アイコン(¹⁽¹⁾) が表示されます。ルールを選択して、Revert[元に戻す] をク リックし、Yes[はい] をクリックして操作を確定します。

デフォルト セキュリティ	の意味
ルールをオーバーライドする	
フィールド	

General [全般] タブ

氏名	ルールを識別する Name[名前] は読み取り専用であるため、 オーバーライドはできません。
ルールの種類	Rule Type[ルール タイプ] は読み取り専用であるため、オー バーライドはできません。
の意味	Description[説明] は読み取り専用であるため、オーバーライド はできません。
タグ	ドロップダウンリストから Tags [タグ]を選択します。 ポリシー タグとは、ポリシーをソートまたはフィルタリング できるキーワードや語句です。多数のポリシーを定義してい て、特定のキーワードでタグが付けられたポリシーを表示する 場合に役立ちます。たとえば、特定のセキュリティ ポリシー にDMZへのインバウンドのタグを付けたり、個々の復号化ポ リシーに「復号」または「復号なし」というタグを付けたり、 特定のデータセンターに関連付けられたポリシーにその場所の 名前を使用したりできます。

Actions [アクション] タブ

デフォルト セキュリティ ルールをオーバーライドする フィールド	の意味
アクション設定	 ルールに一致するトラフィックに対して適切な Action (アクション)を選択します。 Allow[許可] – (デフォルト)トラフィックを許可します。 Deny[拒否] – トラフィックをブロックし、ファイアウォールが拒否するアプリケーションについて定義されたデフォルトのアクションの拒否を実行します。アプリケーションについてデフォルトで定義されている拒否のアクションを表示するには、Objects (オブジェクト) > Applications (アプリケーション)でアプリケーションの詳細情報を表示します。 Drop[ドロップ] – アプリケーションンをサイレントにドロップします。ホストまたはアプリケーションに、TCP リセットメッセージは送信されません。 Reset client[クライアントのリセット] – クライアント側デバイスにTCP リセットメッセージを送信します。 Reset server[サーバーのリセット] – サーバー側デバイスにTCP リセットメッセージを送信します。 Reset both[両方のリセット] – クライアント側とサーバー側の両方のデバイスにTCP リセットメッセージを送信します。
プロファイル設定	 Profile Type (プロファイルタイプ) – プロファイルまたはプ ラットフォーム グループをセキュリティ ルールに割り当てま す。 デフォルトのセキュリティプロファイルによって実行さ れるチェック動作を指定するには、Profiles[プロファイ ル]を選択して、Antivirus[アンチウイルス]、Vulnerability Protection[脆弱性防御]、Anti-Spyware[アンチスパ イウェア]、URL Filtering[URLフィルタリング]、File Blocking[ファイルブロッキング]、Data Filtering[データ フィルタリング]、WildFire Analysis[WildFire分析]、SCTP Protection[SCTP プロテクション]、および Mobile Network Protection[モバイル ネットワーク プロテクション] の各プ ロファイルを選択します。 個々のプロファイルではなくプロファイルグループを割り 当てるには、Group[グループ]を選択し、ドロップダウンリ ストリストから Group Profile[グループプロファイル]を選 択します。

デフォルト セキュリティ ルールをオーバーライドする フィールド	の意味
	 新規プロファイル(Objects(オブジェクト) > Security Profiles(セキュリティプロファイル))またはプロファイ ルグループを定義するには、対応するプロファイルまたは グループプロファイルのドロップダウンでNew(新規)を クリックします。
ログ設定	以下のオプションを任意に組み合わせて指定します。 • Log Forwarding[ログ転送] – ローカル トラフィック ログ と脅威ログのエントリをリモートの宛先 (Panorama サー バーや Syslog サーバーなど) に転送するには、ドロップ ダウンリスト リストから Log Forwarding[ログ転送] プロ ファイルを選択します。セキュリティ プロファイルによっ て、脅威ログ エントリが生成されるかどうかが決まりま
	す。新規の Log Forwarding (ログ転送) プロファイルを定 義するには、ドロップダウン リストで Profile (プロファ イル)を選択します(「Objects(オブジェクト) > Log Forwarding(ログ転送)」を参照)。
	 ルールに一致するトラフィックのエントリをローカルトラフィックログに生成するには、以下のオプションを選択します。
	 Log at Session Start (セッション開始時にログ) – セッション開始のトラフィック ログ エントリを生成します (デフォルトではオン)。
	 Log at Session End (セッション終了時にログ) – セッション終了のトラフィック ログ エントリを生成します (デフォルトではオフ)。
	セッション開始またはセッション終了エントリをトラフィックログに含めるようにファイアウォールを設定した場合は、ドロップエントリと拒否エントリもトラフィックログに含められます。

アプリケーションおよび使用状況

- 2>ポリシー>セキュリティ>ポリシーオプティマイザー>新しいアプリビューアーでアプリが表示の数値をクリックするか、Compareをクリックします。
 - インターフェイスで新しいアプリケーションビューアーを表示するには、SaaS インラインセキュリティサブスクリプションが必要です。新しいアプリビュー アーには、コンテンツ配信アプリケーションに加えてクラウド配信アプリケー ションが含まれており、SaaS インラインセキュリティサブスクリプションがな い場合は、クラウド配信アプリケーションを受信しません。
- 2>ポリシー>セキュリティ>ポリシーオプティマイザー>ルールをアプリコントロールなし で App でクリックするか、比較 をクリックします。
- ポリシー.>セキュリティ>ポリシーオプティマイザー>未使用のアプリをクリックし、Appの数値をクリックするか、比較をクリックします。
- ポリシー > セキュリティをクリックし、アプリが見の番号をクリックします。

また、セキュリティ ポリシー ルールの Usage (使用状況) タブでCompare Applications & Applications Seen (アプリケーションおよび発見されたアプリケーションの比較)を行えば、ポー ト ベースのセキュリティ ポリシー ルールからアプリケーション ベースのセキュリティ ポリ シー ルールに移行する際に役立つツールを利用でき、Applications & Usage (アプリケーション および使用状況)でルールから使用していないアプリケーションを取り除くことができます。

項目	の意味
期間	アプリケーション情報の期間:
	 Anytime (全期間)–ルールを作成してから発見されたアプリケーションを表示します。
	 Past 7 days (過去 7 日間)-過去 7 日間に発見されたアプリケーションだけを表示します。
	 Past 15 days (過去7日間)–過去15日間に発見されたアプリケーションだけを表示します。
	 Past30 days (過去7日間)–過去30日間に発見されたア プリケーションだけを表示します。
ルールのアプリ	対象のルールで設定されている各アプリケーション、ある いはルールで特定のアプリケーションが設定されていない 場合はAny (すべて)になります。必要に応じてアプリケー ションをBrowse (参照)、Add (追加)、Delete (削除)でき、 そうするとアプリケーションがルールで設定され、Apps on Rule (ルールのアプリ) の隣にある丸で囲まれた数字で数 が分かります。この場所でアプリケーションを追加する方 法は、セキュリティポリシー ルールのApplication (アプリ ケーション)タブでアプリケーションを追加する際と同じで す。

項目	の意味
発見されたアプリ	ルールにマッチするファイアウォール上で許可され、発見 されたすべてのアプリケーションです。[見たアプリ]の横 の数字は、ルールで見られたアプリケーションの数を示し ます。
	 Applications (アプリケーション)-対象のルールで発見されたアプリケーションです。たとえば、ルールでウェブブラウジングトラフィックが許可されている場合(ルール上のアプリで見られるように)、Webブラウジングとして識別されるアプリケーションが多数あるため、多数のアプリケーションが見られるアプリの一覧に表示されることがあります。
	 Subcategory (サブカテゴリ)-アプリケーションのサブ カテゴリです。
	• Risk (リスク)–アプリケーションのリスク評価です。
	 First Seen (最初の発見)-ネットワーク上でアプリケー ションが初めて発見された日です。
	 First Seen (最後の発見)ーネットワーク上でアプリケー ションが最後に発見された日です。
	 First Seen (最初の発見) と Last Seen (最後の発見)の精度は1日であるため、ルールを定義した日は First Seen (最初の発見) と Last Seen (最後の発見)が同じ日付になります。
	• Traffic (30 days) (トラフィック (30 日)) –過去 30 日間 で発見されたトラフィックの量 (バイト)です。
	最も古いルールはトラフィックの累積量 が最も多くなりがちであるため、期間を 長くするとそのルールがリストの一番上 に残り続けるでしょう。そのため、新し いルールに大量のトラフィックがあって も、古いルールの下にリストアップされ る可能性があります。
発見されたアプリの操作	Apps Seen (発見されたアプリ)で行える操作:
	 Create Cloned Rule (ルールのコピーを作成)–現在の ルールをコピーします。ポートベースのルールからア プリケーション ベースのルールに移行する際、初めに ポートベースのルールをコピーしてからそのコピーを 編集することで、トラフィックを許可するアプリケー ション ベースのルールを作成します。ポリシーリスト

項目	の意味
	では、コピーしたルールがポートベースのルールの上 に挿入されます。必ずこの方法で移行を行い、許可した いトラフィックを誤って拒否することがないようにして ください。コピーしたルールが必要なアプリケーション を一部許可しない場合、後続のポートベースのルールに よってそれらが許可されます。ポートベースのルールを 監視して必要に応じて(コピーした)アプリケーション ベースのルールを調整します。必要なトラフィックだけ をアプリケーションベースのルールが許可しており、 不要なトラフィックだけがフィルタリングされてポート ベースのルールの対象になっていることが確実であれ ば、対象のポートベースのルールを安全に削除できま す。
	複製は、App Viewer で見られるアプリケーションに対 しても同様の利点を提供し、新たに識別されたクラウ ドアプリケーションとコンテンツ提供のアプリケーショ ンを、アプリケーションとアクセスを制御するためのセ キュリティポリシールールに移行することができます。
	複製されたルールにアプリケーションを個別に追加する 場合は、アプリケーション グループ内、またはアプリ ケーション フィルタで選択できます。
	 このルールに追加(新しいアプリビューアーでは使用できません) - [見たアプリ]からルールにアプリケーションを追加します。アプリケーションをルールに追加すると、Any(すべて)のアプリケーションベースのルールに追加するアプリケーションベースのルール(アプリケーションを許可するアプリケーションベースのルールに変わります(新しいアプリケーションベースのルールがポートベースのルールに置換される)。このルールは、その他のアプリケーションベースのルールと同様、ルールに追加しないアプリケーションをすべて拒否します。必ず、許可するアプリケーションをすべて判断し、それらをルールに追加することで、アプリケーションを誤って拒否することがないようにしてください。
	 Add to Existing Rule (既存のルールに追加)-Apps Seen (発見されたアプリ)から既存のアプリケーションベース (App-ID) のルールにアプリケーションを追加します。 たとえば、ポートベースのルールから App-ID ベースの ルールを複製し、ポートベースのルールに表示されるア プリケーションを後で App-ID ルールに追加できます。

新しい App Viewer で見たアプリケーションの場合、新 しいアプリが検出されると、新しく識別されたクラウ

項目	の意味
	ド ベースおよびコンテンツ ベースのアプリケーション を、賢明なセキュリティ ポリシー ルールに整理できま す。 既存のルールにアプリケーションを個別に追加する場合 は、アプリケーション グループ内、またはアプリケー
	ションフィルタで選択できます。
	 Match Usage (新しいアプリビューアーでは使用できません) - 表示されたすべてのアプリをルールに移動します (Match 使用状況 の後に[ルール上のアプリ]の下に表示されます)。リストアップされたすべてのアプリケーションをルールで許可しなければならないということが確実な場合、Match Usage (使用状況にマッチ)が非常に便利です。しかし、リストアップされたアプリケーションがすべてネットワーク上で許可するアプリケーションがすべてネットワーク上で許可するアプリケーションであることを確認する必要があります。ルールで発見されたアプリケーションが多い場合 (例えば webbrowsing を許可するルール)、ルールをコピーしてアプリケーション ベースのルールに移行する方が良いでしょう。Match Usage (使用状況にマッチ)は、よく知られたアプリケーションを伴うシンプルなルールに対して上手く機能します。例えば、ポート 22 用のポートベースのルールが SSH トラフィックしか発見していない(かつ、それしか発見しないはずである)場合、安全にMatch Usage (使用状況にマッチ)できます。
	Clone (コピー)、Add to Rule (ルールに追加)、およびAdd Apps to Existing Rule (既存のルールにアプリケーションを 追加)ダイアログは、アプリケーションが破損していないこ とを確認する際に役立ち、コピーあるいはルールに追加し ようとしているアプリケーションに関連する個々のアプリ ケーションをこれらのダイアログを使って含めることで、 今後もルールを適切に維持できるようになります。
複製されたルール>アプリケー ションを作成する	アプリケーションを選択し、個々のアプリケーションを複 製またはルールに追加します。
このルールに追加 既存のルール>アプリケーショ ンに追加	 Name (名前) (Clone (コピー) と Add Apps to Existing Rule (既存のルールにアプリケーションを追加) ダイアロ グのみ)。
	• Clone (コピー):コピーした新しいルールの名前を入力 します。
	 Add Apps to Existing Rule (既存のルールにアプリ ケーションを追加):アプリケーションを追加するルー ルを選択するか、ルールの名前を入力します。

項目	の意味
	 Applications (アプリケーション):
	 コンテナアプリケーションを追加(デフォルト):コン テナー内のすべてのアプリ、ルールに表示されるア プリ、およびルールで表示されていないコンテナー アプリを選択します。コンテナーに対して見られる 将来のアプリはルールに一致するため、アプリの変 更に伴って将来のアプリを将来の証拠にします。
	 発見された特定のアプリケーションを追加:ルールで 実際に表示されたアプリのみを選択します。(コンテ ナーアプリや機能アプリを手動で選択することもで きます)。
	Application:
	 ルールで表示された選択されたアプリケーションは 緑色で強調表示されています。
	 コンテナアプリ、灰色で強調表示され、その機能的 なアプリケーションが以下にリストされています。
	 ルールで確認されたが、Applications & Usage で選択 されなかったコンテナー内の機能アプリケーション (強調表示されていません)。
	 ルールで確認されていないコンテナー内の機能アプ リケーション (italicized).
	 ルールでアプリケーションが 最後に確認された日付
	 Dependent Applications (依存アプリケーション):
	 選択したアプリケーションを実行するために必要な アプリケーション。
	 Depends On-選択したアプリケーションの実行に必要な依存アプリケーション。
	 必須の-依存アプリケーションを必要とするアプリケーション。(依存アプリケーションに依存アプリケーションに依存アプリケーションがある場合があります)。
複製されたルール>アプリケー ション グループを作成する	Cloned Rule または 既存のルールにアプリケーションを追 加] ダイアログ ボックスの [アプリケーション グループ内
既存のルール>アプリケーショ ン グループに追加	のルールにアプリケーションを複製または追加する] ダイ アログ ボックスで<、アプリケーションを選択します。

項目	の意味
	 複製されたルール名または名:
	 複製されたルール名:コピーした新しいルールの名前 を入力します。
	 名前:アプリケーション グループを追加するルールを 選択するか、ルールの名前を入力します。
	 ポリシーアクション(クローンルールのみ) - クローン ルールのトラフィックを許可するか拒否するかを選択し ます。
	 アプリケーション グループに追加] - 既存のグループを 選択するか、新しい名前を入力して新しいアプリケー ション グループを作成します。
	 Applications (アプリケーション):
	 コンテナアプリケーションを追加(デフォルト):コン テナー内のすべてのアプリ、ルールに表示されるア プリ、およびルールで表示されていないコンテナー アプリを選択します。コンテナーに対して見られる 将来のアプリはルールに一致するため、アプリの変 更に伴って将来のアプリを将来の証拠にします。
	 発見された特定のアプリケーションを追加:ルールで 実際に表示されたアプリのみを選択します。(コンテ ナー アプリや機能アプリを手動で選択することもで きます)。
	Application:
	 ルールで表示された選択されたアプリケーションは 緑色で強調表示されています。
	 コンテナアプリ、灰色で強調表示され、その機能的 なアプリケーションが以下にリストされています。
	 ルールで確認されたが、Applications & Usage で選択 されなかったコンテナー内の機能アプリケーション (強調表示されていません)。
	 ルールで確認されていないコンテナー内の機能アプ リケーション (italicized).
	• ルールでアプリケーションが 最後に確認された日付

項目	の意味
	 Dependent Applications (依存アプリケーション):
	 選択したアプリケーションを実行するために必要な アプリケーション。
	 Depends On-選択したアプリケーションの実行に必要な依存アプリケーション。
	 必須の-依存アプリケーションを必要とするアプリケーション。(依存アプリケーションに依存アプリケーションに依存アプリケーションがある場合があります)。
複製されたルール>アプリケー ション フィルタを作成する 既存のルール>アプリケーショ	Cloned Rule または アプリケーションを既存のルール に追 加する] ダイアログ ボックスで、アプリケーションを選択 して、アプリケーション フィルタのルールに複製または追 加します。
ンフィルタに追加	 複製されたルール名 または 既存のルール名:
	 複製されたルール名:コピーした新しいルールの名前 を入力します。
	 既存のルール名:アプリケーションフィルタを追加 するルールを選択するか、ルールの名前を入力しま す。
	 ポリシーアクション(クローンルールのみ) - クローン ルールのトラフィックを許可するか拒否するかを選択し ます。
	 アプリケーションフィルタ名-既存のフィルタを選択するか、新しい名前を入力して新しいアプリケーションフィルタを作成します。
	アプリケーションフィルタはオブジェクト > アプリケー ションフィルタ と同じように機能します(「アプリケー ションフィルタを作成する)。クラウドベース (SaaS インラ イン セキュリティ サブスクリプションを使用) とコンテン ツベースのアプリケーションをフィルター処理し、既存ま たは新しいフィルターに追加できます。

セキュリティポリシー オプティマイザー

• Policies (ポリシー) > Security (セキュリティ) > Policy Optimizer (ポリシー オプティマイザー)

Policies (ポリシー) > Security (セキュリティ) > Policy Optimizer (ポリシー オプティマイザー)に は次の内容が表示されます:

新しい App Viewer - ファイアウォールに SaaS セキュリティ サブスクリプションがある場合、アプリケーション コントロール エンジンからダウンロードされた新しいクラウド アプリケーション。

- [アプリケーション コントロールなしの規則] アプリケーションが に設定されているルール は、任意のに設定されるため、ポートベースのルールを識別してアプリケーション ベースの ルールに変換できます。
- 未使用のアプリールールにマッチしたことがないアプリケーションを含むルール。
- Log Forwarding for Security Services Log Forwarding プロファイルを複数のルールに一括 でアタッチし、分析のために IoT Security やストレージ用に Cortex Data Lake などのサービ スにログを送信します。
- この機能を使用する前に、まず Security policy rules を構成して、転送ログを キャプチャし、拡張アプリケーション ログで ログ サービス を有効にする必要が あります。
- Rule Usage (ルールの使用状況) 多様な期間で未使用のルールを含め、さまざまな期間でのルール使用状況に関する情報。

項目	の意味
氏名	セキュリティポリシー ルールの名前です。
サービス	セキュリティポリシー ルールに関連するサービスです。
トラフィック(バイト、 30 日 間)	Traffic (30 days) (トラフィック(30 日)) –過去 30 日間で 発見されたトラフィックの量(バイト)です。
	最も古いルールはトラフィックの累積量が最 も多くなりがちであるため、期間を長くする とそのルールがリストの一番上に残り続ける でしょう。そのため、新しいルールに大量の トラフィックがあっても、古いルールの下に リストアップされる可能性があります。
許可されるアプリ	ルールが許可するアプリケーションです。 Application (ア プリケーション) ダイアログを開けば、そこでルールのアプ リケーションを追加・削除できます。
アプリケーション	(新しいアプリ ビューアー のみ)ルールで許可されるアプリ ケーション。
発見されたアプリ	ルールで発見されたアプリケーションの数です。数をク リックして Applications & Usage (アプリケーションおよび 使用状況) ダイアログを開くと、ルールで設定されているア プリケーションをルールで発見されたアプリケーションと 比較してアプリケーションを編集することができます。
新しいアプリが未発見の日数	最後にルールで新しいアプリケーションが見つかってから 経過した日数です。

項目	の意味
比較	Applications & Usage (アプリケーションおよび使用状況)ダ イアログを開くと、ルールで設定されているアプリケー ションをルールで発見されたアプリケーションと比較して ルールを編集することができます。
(Rule Usage) Last Hit(ルールの 使用状況、最終日ッと)	トラフィックがルールに最後にマッチした時です。
(Rule Usage) Last Hit(ルールの 使用状況、最終ヒット)	トラフィックがルールに最初にマッチした時です。
(Rule Usage) Hit Count(ルール の使用状況、ヒット数)	トラフィックがルールに一致した回数です。
変更済	ルールを最後に編集した日時。
作成日時	ルールが作成された日時。
Timeframe(期間)	データが表示される期間(日数)。
使用率	以下の情報が表示されます。
	 Any(すべて)(すべての)トラフィックがルール (使用済ルール)に一致する、あるいはしないか(未 使用ルール)にかかわらず、指定した期間でのファイア ウォール上のルール。
	 Unused(未使用)は、指定した期間でトラフィックが 一致しなかったことを示します。
	• Used(使用済)は、指定した期間でトラフィックが一 致したことを示します。
過去 xx 日の間にリセットされ たルールを除外する	指定された日数(1~5、000 日)内で Reset Rule Hit Counter (ルール ヒット カウンターをリセット)したルー ルは表示しません。例えば、これを使用して、トラフィッ クに一致する時間がなかった可能性のある新しいルールを 除外しつつ、ある期間内でトラフィックに一致しなかった 古いルールを調べることができます。
リセット日	ルールのヒットカウンターがリセットされた最終日付。
Log Forwarding Profile (Log Forwarding for Security Services のみ)	以下の情報が表示されます。 • All - Log Forwarding プロファイルがアタッチされてい るかどうかに関係なく、firewall に関するルール。

項目	の意味
	 None - Log Forwarding プロファイルがアタッチされて いないルール。
	 <profile-name> - 特定の Log Forwarding プロファイル がアタッチされているルール。</profile-name>
Attach Log Forwarding Profile (Log Forwarding for Security Services only)	Security ポリシー規則を選択した後、画面下部のこのオプ ションを使用してダイアログボックスを開き、選択した規 則にアタッチする Log Forwarding プロファイルを選択しま す。
	 Log Forwarding Profile - 選択したルールにアタッチする ログ転送プロファイルを選択します。
	 Enable Enhanced IoT Logging - 選択した Log Forwarding プロファイルが拡張アプリケーション ログ (EAL) をまだ転送していない場合に選択します。これに より、選択した Log Forwarding プロファイルでの EAL 転送が可能になります。

Policies > NAT [ポリシー > NAT]

ファイアウォールにレイヤー3インターフェイスを定義する場合、ネットワークアドレス変換 (NAT)ポリシーを設定 して、送信元または宛先の IP アドレスやポートに対して、パブリッ クおよびプライベートの変換を実施するかどうかを指定できます。たとえば、内部 (信頼されて いる) ゾーンからパブリック (信頼されていない) ゾーンに送信されるトラフィックの送信元プラ イベート アドレスをパブリック アドレスに変換できます。NAT は、バーチャル ワイヤー イン ターフェイスでもサポートされています。

NAT ルールは、送信元ゾーンと宛先ゾーン、送信元アドレスと宛先アドレス、およびアプリ ケーション サービス(HTTP など)に基づいています。セキュリティ ポリシーと同様に、NAT ポリシー ルールと受信トラフィックは順番に照合され、トラフィックに一致する最初のルール が適用されます。

必要に応じて、ローカル ルータに静的 ルートを追加し、パブリック アドレスへのトラフィック をすべてファイアウォールにルーティングします。場合によっては、ファイアウォールの受信イ ンターフェイスに静的 ルートを追加し、プライベート アドレスにトラフィックをルーティング して戻す必要があります。

以下の表に、NAT および NPTv6 (IPv6 ネットワーク間プレフィックス変換) の設定を説明します。

- NAT ポリシーの General (全般) タブ
- NAT の Original Packet (元のパケット) タブ
- NAT の Translated Packet (変換済みパケット) タブ
- NAT の Active/Active HA Binding (アクティブ/アクティブ HA バインド) タブ
- (Panorama のみ) NAT Target (宛先) タブ

その他の情報をお探しですか?

「NAT^{II}」を参照してください。

NAT ポリシーの General (全般) タブ

• Policies > NAT > General (ポリシー > NAT > 一般)

General[全般]タブを使用して、NATポリシーまたはNPTv6ポリシーの名前とその内容説明を設定します。タグを設定すると、大量のポリシーがある場合に、ポリシーのソートやフィルタリングを行うこともできます。作成するNATポリシーのタイプを選択します。ここで選択したタイプによって、Original Packet[元のパケット]タブおよびTranslated Packet[変換済みパケット]タブで使用できるフィールドが決まります。

NAT ルール - 一 般設定	の意味
氏名	ルールを識別する名前を入力します。名前の大文字と小文字は区別され、 文字、数字、スペース、ハイフン、およびアンダースコアを含む最大 63 文 字を指定できます。ルール名はファイアウォールおよび Panorama 上で一
NAT ルール - 一 般設定	の意味
--------------------------	--
	意でなければなりません。また、デバイス グループとその先祖または子孫 デバイス グループ内でも一意でなければなりません。
の意味	ルールの説明を入力します (最大 1024 文字)。
タグ	ポリシーにタグを付ける場合、タグを Add(追加)して指定します。
	ポリシー タグとは、ポリシーをソートまたはフィルタリングできるキー ワードや語句です。多数のポリシーを定義していて、特定のキーワードで タグが付けられたポリシーを表示する場合に役立ちます。
タグに基づいて ルールをグルー プ化	類似のポリシールールをグループ化するのに使用するタグを入力します。 グループタグを使用すれば、対象のタグに基づいてポリシールールベース を表示できます。Tag (タグ)に基づいてルールをグループ化することができ ます。
NAT タイプ	変換のタイプを指定します。
	● ipv4 – IPv4 アドレス間の変換に使用します。
	• nat64 – IPv6 と IPv4 間の変換に使用します。
	• nptv6 – IPv6 プレフィックス間の変換に使用します。
	1つの NAT ルールで IPv4 と IPv6 のアドレス範囲を組み合わせることはで きません。
監査コメント	ポリシールールの作成や編集を監査するために使用するコメントを入力し ます。監査コメントの大文字と小文字は区別され、文字、数字、スペー ス、ハイフン、およびアンダースコアを含む最大 256 文字を指定できま す。
監査コメント アーカイブ	ポリシールールの以前のAudit Comments (監査コメント)を表示します。監 査コメント アーカイブは CSV 形式でエクスポートできます。

NAT の Original Packet (元のパケット) タブ

• Policies > NAT > Original Packet [ポリシー > NAT > 元のパケット]

ファイアウォールで変換するパケットの送信元ゾーンと宛先ゾーンを定義するには、Original Packet(元のパケット)タブを選択します。必要に応じて、宛先インターフェイスとサービスの タイプを指定することもできます。同じタイプの複数の送信元と宛先ゾーンを設定し、そのルー ルを特定のネットワークやIPアドレスに適用することができます。

NAT ルール - 元のパ ケット設定	の意味
送信元ゾーン / 宛先 ゾーン	元のパケット (非 NAT) パケットについて、1つ以上の送信元ゾーン と宛先ゾーンを選択します (デフォルトは any)。ゾーンは同じタイプ (Layer 2 [レイヤー 2]、Layer 3 [レイヤー 3]、virtual wire [バーチャル ワイヤー]) である必要があります。新しいゾーンを定義する手順につ いては、「Network(ネットワーク) > Zones(ゾーン)」を参照し てください。 複数のゾーンを特定し、管理の手間を少なくすることができます。た とえば、複数の内部 NAT アドレスが同じ外部 IP アドレスに送信され るように設定できます。
宛先インターフェイ ス	ファイアウォールが変換するパケットの宛先インターフェイスを指定 します。異なるIPアドレスプールを持つ2つのISPにネットワークが接 続している場合、宛先インターフェイスを使用することで、IPアド レスを異なった方法で変換できます。
サービス	ファイアウォールが送信元または宛先アドレスを変換する対象とな るサービスを指定します。新しいサービス グループを定義するに は、Objects(オブジェクト) > Service Groups(サービス グルー プ)を選択します。
送信元アドレス / 宛 先アドレス	ファイアウォールが変換する送信元アドレスと宛先アドレスの組み合 わせを指定します。
	NPTv6 では、Source Address (送信元アドレス) と Destination Address (宛先アドレス) に設定されるプレフィックスを xxxx:xxx::/ yy という形式で指定する必要があります。アドレスにインターフェ イス識別子 (ホスト) 部分を定義することはできません。サポートされ ているプレフィックス長の範囲は /32 ~ /112 です。
	ポリシー > NAT > オリジナルパケットの FQDN オブジェクトとし て Pre-NATアドレスを設定する場合、宛先アドレス変換タイプ(ポ リシー > NAT > 変換パケット)を Dynamic IP(セッション分散あ り)として選択する必要があります。

NAT の Translated Packet (変換済みパケット) タブ

• Policy (ポリシー) > NAT > Translated Packet (変換済みパケット)

Source Address Translation (送信元アドレス変換) については、Translated Packet (変換済みパケット) タブを使用して、送信元に対して実行する変換のタイプ 🖬、アドレス、さらに場合によっては送信元の変換先であるポートを決定します。

公開 IP アドレスによるアクセスが必要な内部ホスト用に、宛先アドレス変換を設定することも できます。この場合、Original Packet(元のパケット)タブに内部ホストのパブリックな送信元 アドレスと宛先アドレスを定義し、Translated Packet(変換済みパケット)タブでStatic IP(静 的 IP) または Dynamic IP (with session distribution) (動的 IP (セッション配信付属)) を設定 し、Translated Address (変換後アドレス)を入力します。次に、公開アドレスがアクセスされ ると、内部ホストの内部 (宛先) アドレスに変換されます。

NAT ルール - 変 換済みパケット 設定	の意味
送信元アドレス の変換	変換タイプ (動的または静的 アドレス プール) を選択し、送信元アドレスの 変換後の IP アドレスまたはアドレス範囲 (アドレス 1 ~ アドレス 2) を入 力します (Translated Address (変換後アドレス))。アドレス範囲のサイズ は、以下のアドレス プールのタイプによって制限されます。
	 (PAN-OS 11.1.1 以降のリリース) Persistent Dynamic IP and Port (永続的なダイナミック IPおよびポート)- VoIP、ビデオ、クラウドベースのビデオ会議、音声会議、およびその他のアプリケーションは、多くの場合DIPPを使用し、Session Traversal Utilities for NAT(STUN)プロトコルが必要になる場合があります。DIPP NAT は対称 NAT を使用するため、STUN を使用するアプリケーションとの互換性の問題が発生する可能性があります。これらの課題を緩和するために、Persistent Dynamic IP and Port (永続的なダイナミック IPおよびポート) このようなアプリケーションとの接続に対する追加のサポートを提供します。DIPP の永続 NAT が有効になっている場合、プライベート送信元 IP アドレス/ポートのペアの特定のパブリック (変換された)送信元 IP アドレス/ポートのペアへのバインドは、同じ元の送信元 IP アドレス/ポートのペアで到着した後続のセッションでも保持されます。個々の NAT ポリシールールで永続的な DIPP を設定することができます。
	 Dynamic IP And Port(動的 IP およびポート) – アドレス選択は、送信 元 IP アドレスのハッシュに基づきます。特定の送信元 IP アドレスに対 して、ファイアウォールのすべてのセッションで同じ変換後の送信元ア ドレスが使用されます。動的 IP およびポート(DIPP)の送信元 NAT で は、NAT プール内の各 IP アドレスで約 64,000 個の連続するセッション がサポートされます。一部のモデルでは、オーバーサブスクリプション がサポートされます。その場合、1 つの IP で 64,000 個を超える連続す るセッションをホストできます。
	Palo Alto Networks [®] DIPP NAT では、使用可能な IP アドレ スとポートの数でサポートされる数よりも多くの NAT セッ ションがサポートされます。オーバーサブスクリプションで は、ファイアウォールは、IPアドレスとポートの組み合わせ を、PA-220、PA-400シリーズ、PA-800シリーズ、PA-1400シリー ズ、PA-3410、PA-3420、VM-50、VM-300、およびVM-1000- HVファイアウォールでは同時に2回、PA-3200シリーズ、PA-3430、 およびPA-3440ファイアウォールでは同時に4回、PA-5200シリー ズ、PA-5400シリーズ、PA-7050、PA-7080、VM-500、およ びVM-700ファイアウォールでは同時に8回、宛先IPアドレスが一意の場 合に使用できます。

NAT ルール - 変 換済みパケット 設定	の意味
	 Dynamic IP (動的 IP):指定した範囲で次に使用可能なアドレスを変換しますが、ポート番号は変更されません。最大32000 個の連続した IP アドレスがサポートされます。動的 IP プールには、複数のサブネットを含めることができるため、内部ネットワーク アドレスを 2 つ以上の別個のパブリック サブネットに変換できます。
	 Advanced (Dynamic IP/Port Fallback) (詳細 (動的IP/ポートのフォール バック)) – IP およびポートの変換を実行するほか、プライマリプール のアドレスを使い切った場合に使用するフォール バック プールを作成 するには、このオプションを使用します。Translated Address (変換後ア ドレス) オプションまたは Interface Address (インターフェイス アドレ ス) オプションを使用するとプールのアドレスを定義できます。後者の オプションは IP アドレスを動的に受け取るインターフェイス用です。代 替プールを作成するときには、アドレスがプライマリプールのアドレス と重複しないことを確認します。
送信元アドレス の変換(続)	 Static IP[静的 IP] – 変換に同じアドレスが常に使用され、 ポート番号は変更されません。たとえば、送信元の範囲が 192.168.0.1~192.168.0.10 で、変換の範囲が 10.0.0.1~10.0.0.10,の場 合、アドレス 192.168.0.2 は必ず 10.0.0.2 に変換されます。アドレス範 囲は事実上無制限です。
	NPTv6 送信元アドレスの変換には、Static IP(静的 IP)変換を使用す る必要があります。NPTv6 の場合、Translated Address(変換後アドレ ス)用に設定されたプレフィックスは xxxx:xxxx::/yy の形式でなければ ならず、アドレスにはインタフェース識別子(ホスト)部分を定義する ことはできません。サポートされているプレフィックス長の範囲は /32 ~/112 です。
	 None[なし] – 変換は実行されません。
双方向	(任意) Static IP (静的 IP) 送信元アドレス変換で、対応する変換 (NAT または NPTv6) を設定する変換の反対方向にも作成する場合は、双方向変換を有効 にします。
	双方向変換を有効にする場合は、双方向のトラフィックを制 御するセキュリティポリシーが設定されていることを必ず確 認しておく必要があります。このようなポリシーが設定され ていない場合、双方向変換機能により双方向のパケットが自 動的に変換されることになります。
宛先アドレスの 変換	ファイアウォールに宛先 NAT を実行させるには、次のオプションを設定し ます。通常は宛先 NAT を使用して、電子メール サーバーなどの内部サー バーにパブリック ネットワークからアクセスできるようにします。

NAT ルール - 変 換済みパケット 設定	の意味
変換タイプと変 換後アドレス	 ファイアウォールが宛先アドレスで実行する変換のタイプを選択します。 None[なし] (デフォルト) Static IP (静的 IP)-Translated Address (変換後アドレス) を IPアドレスまたは IPアドレスの範囲として、また元の宛先アドレスおよびポート番号が変換される Translated Port (変換後ポート) (1 ~ 65535) として入力します。Translated Port (変換済みポート) フィールドがブランクの場合、宛先ポートは変更されません。 NPTv6 では、宛先プレフィックス Translated Address (変換後アドレス) に設定するプレフィックスを「xxxx:xxxx:/yy」の形式で指定する必要があります。アドレスにインターフェイス識別子 (ホスト) 部分を定義することはできません。サポートされているプレフィックス長の範囲は/32 ~ /112 です。 IPTv6 では、厳密なプレフィックス変換が行われるため、変換済みポートはサポートされていません。ポートアドレスおよびホストアドレスのセクションは、変換されずにそのまま転送されます。
	 また、IPv4 の静的 IP 変換では Enable DNS Rewrite (DNS 書き換えを有効にする) こともできます (以下で説明しま す)。 Dynamic IP (with session distribution) (動的 IP (セッション配信あ り)) – ファイアウォールが変換されたアドレスを選択する、FQDN、 アドレスオブジェクト、またはアドレスグループであるTranslated Address (変換アドレス)を選択または入力します。DNS サーバーが FQDN に複数のアドレスを返す場合、またはアドレスオブジェクトま たはアドレス グループが複数のIPアドレスに変換された場合、ファイア ウォールは指定された Session Distribution Method (セッション配信方 式)を使用してそれらのアドレス間でセッションを配信します。
セッション配信 方式	 destination NAT (宛先NAT - DNAT)変換を Dynamic IP (動的IP) (セッション分散あり)になるように選択した場合、宛先変換アドレス (FQDN、アドレスオブジェクト、またはアドレス グループ) が複数のアドレスで解決できます。ファイアウォールがこれらのアドレス間でセッションを分散 (割り当て) する方法を選択して、バランス良くセッションを分散させることができます。 Round Robin (ラウンドロビン) - (デフォルト)新しいセッションをローテーションで IP アドレスに割り当てます。他のいずれかの分散方式を選択したよい環境を除き、この方式を使用します。

NAT ルール - 変 換済みパケット 設定	の意味
	 Source IP Hash (送信元 IP ハッシュ)–送信元 IP アドレスのハッシュに基づいて新しいセッションを割り当てます。単一の送信元 IP から来るインバウンド トラフィックがある場合は、Source IP Hash (送信元 IP ハッシュ)以外の方式を選択してください。
	 IP Modulo (IP モジュロ)-ファイアウォールはインバウンド パケットの 送信元および宛先 IP アドレスを考慮します。ファイアウォールは XOR 操作およびモジュロ操作を実行し、その結果、ファイアウォールが新し いセッションを割り当てる IP アドレスが決まります。
	 IP Hash (IP ハッシュ)–送信元および宛先 IP アドレスのハッシュを使用 して新しいセッションを割り当てます。
	 Least Sessions (最小数のセッション)–同時セッションが最も少ない IP アドレスに新しいセッションを割り当てます。短期間のセッションが多くある場合は、Least Sessions (最小数のセッション)を使用することでバランス良くセッションを分散させることができます。
Enable DNS Rewrite (DNS 書き換えを有効 にする)	宛先 NAT ポリシー ルール タイプが ipv4 で宛先アドレス変換タイプが Static IP (静的 IP)の場合、Enable DNS Rewrite (DNS 書き換えを有効にす る) オプションが利用可能です。宛先 NAT を使用し、ファイアウォールの 一方の側で DNS サービスを使用して、ファイアウォールの反対側のクラ イアントの FQDN を解決する場合は、DNS 書き換えを有効にすることが できます。DNS 応答がファイアウォールを通過するとき、ファイアウォー ルは、DNS 応答が NAT ポリシー ルールで一致する元の宛先アドレスまた は変換済み宛先アドレスを基準にして、DNS 応答の IPアドレスを書き換 えます。単一の NATポリシー ルールでは、ファイアウォールがルールに 一致するパケットに対して NAT を実行し、ルールに一致する DNS 応答の IPアドレスに対して NAT を実行します。NAT ルールと相対的に、ファイア ウォールが DNS 応答内の IP アドレスに対して NAT を実行する方法を逆ま たは順に指定する必要があります。
	 reverse(逆)–(デフォルト)パケットがルールの変換された宛先アドレスと一致する DNS 応答の場合、ルールが使用する逆変換を使用して DNS応答を変換します。例えば、ルールが 1.1.1.10 を 192.168.1.10 に変換する場合、ファイアウォールは 192.168.1.10 の DNS 応答を 1.1.1.10 に書き換えます。
	 forward(順)-パケットがルールの元の宛先アドレスと一致する DNS 応答の場合、ルールが使用するのと同じ変換を使用して DNS 応答を変換します。例えば、ルールが 1.1.1.10 を 192.168.1.10 に変換する場合、ファイアウォールは 1.1.1.10 の DNS 応答を 192.168.1.10 に書き換えます。

NAT の Active/Active HA Binding(アクティブ/アクティブ HA バ インド)タブ

• Policies > NAT > Active/Active HA Binding [ポリシー > NAT > アクティブ/アクティブHAバイ ンド]

Active/Active HA Binding(アクティブ/アクティブ HA バインド)タブは、ファイアウォールが アクティブ/アクティブの高可用性(HA)設定になっている場合にのみ使用できます。この設 定では、(静的または動的 NAT に関係なく)各送信元 NAT ルールをデバイス ID 0 またはデバ イス ID 1 にバインドし、各宛先 NAT ルールをデバイス ID 0、デバイス ID 1、または both(両 方)(デバイス ID 0 とデバイス ID 1)、あるいはアクティブ-プライマリのファイアウォールに バインドする必要があります。

以下のように、Active/Active HA Binding(アクティブ/アクティブ HA バインド)設定を選択 し、NAT ルールを HA ファイアウォールにバインドします。

- 0 NATルールをHAデバイスID 0 のファイアウォールにバインドします。
- 1 NATルールをHAデバイスID1のファイアウォールにバインドします。
- both[両方] NATルールをHAデバイスID 0 のファイアウォールとHAデバイスID 1 のファイア ウォールの両方にバインドします。この設定では動的IPや、動的IPおよびポートのNATはサ ポートされません。
- primary[プライマリ] NATルールをHAアクティブ-プライマリの状態にあるファイアウォー ルにバインドします。この設定では動的IPや、動的IPおよびポートのNATはサポートされま せん。

2つのHAピアが固有のNAT IPアドレスプールを持つ場合は、デバイス固有のNATルールを設定 することができます。

ファイアウォールが新しいセッションを作成すると、HAバインドはセッションに一致したNATルールを判別します。ルールの照合が行われるためには、バインドにセッションオーナー が含まれている必要があります。NATルールの照合はセッションを作成するファイアウォールが 行うものですが、セッションは、セッションオーナーにバインドされたNATルールと照合され、 そのうち1つのルールに基づいて変換されます。デバイス固有のルールの場合、ファイアウォー ルはセッション オーナーに関連付けられていないすべてのNATルールを飛ばして進みます。デ バイスID1のファイアウォールがセッションオーナーであり、セッションを作成するファイア ウォールになる場合を例にとってみましょう。デバイスID1は、セッションとNATルールを照 合する際に、デバイスID0にバインドされたすべてのルールを無視して照合を行います。

片方のピアに障害が発生した場合は、NAT変換を含め、もう一方のピアが、障害が発生したピアのセッション同期用トラフィックの処理を続けます。Palo Alto Networksでは、もう一方のデバイスIDにバインドされたNATルールを重複して作成することをお勧めしています。すなわち、同じ送信元変換アドレスと、同じ宛先変換アドレスを持つ2つの NAT ルールが存在し、各ルールがそれぞれのデバイス ID にバインドされます。この設定により、HA ピアは新しいセッションのセットアップタスクを実行し、自身のデバイス ID にバインドされている NAT ルールで NAT ルールの照合を実行できます。重複する NAT ルールがない場合、機能中のピアは NAT ポリシーの照合を試行しますが、セッションはファイアウォール独自のデバイスに固有のルールと一致しないため、ファイアウォールは自身のデバイス ID にバインドされていないその他の NAT ルールをすべて省略します。

その他の情報をお探しですか?

「NAT in Active/Active HA Mode(アクティブ/アクティブ HA モードの NAT)」 ©を参照して ください。

NAT Target (宛先) タブ

• (Panorama のみ) Policies (ポリシー) > NAT > Target (宛先)

Target(宛先)タブを選択して、ポリシー ルールをプッシュするデバイス グループ内の管理対象ファイアウォールを選択します。管理対象ファイアウォールを選択するか、タグを指定することにより、プッシュ先の管理対象ファイアウォールを指定することができます。さらに、指定済ファイアウォールを除き、すべての管理対象ファイアウォールにプッシュするポリシー ルールの宛先を設定することができます。

NAT ルール - 宛 先設定	の意味
任意 (すべての 対象デバイス)	ポリシー ルールをデバイス グループのすべての管理対象ファイアウォール にプッシュするには、有効化(チェックをオン)にします。
機器	ポリシー ルールをプッシュするデバイス グループに関連付けられた1つま たは複数の管理対象ファイアウォールを選択します。
tags	指定したタグを持つデバイス グループ内の管理対象ファイアウォールにポリシー ルールをプッシュするには、1つまたは複数のタグをAdd(追加)します。
これらの指定さ れたデバイスと タグのみをター ゲットに設定す る	選択したデバイスとタグを除き、デバイス グループに関連付けられてい るすべての管理対象ファイアウォールにポリシー ルールをプッシュするに は、有効化(チェックをオンに)します。

Policies > QoS [ポリシー > QoS]

QoS ポリシー レールを追加して、特定の QoS 処理を受け取るトラフィックを定義し、各 QoS ポリシー ルールの QoS クラス を割り当てて、割り当てたクラスのサービスが QoS 対象のイン ターフェイスから抜け出る際に関連ルールに一致するすべてのトラフィックに適用されるように 指定します。

PanoramaからファイアウォールにプッシュされたQoSポリシールールはオレンジ色で表示され、ファイアウォール上からは編集を行うことができません。

また、ファイアウォールの QoS 提供を完全に有効にするために、以下を実行します。

- □ サービスの各 QoS クラスの帯域幅制限を設定します(Network(ネットワーク) > Network Profiles(ネットワーク プロファイル) > QoS を選択して QoS プロファイルを追加または変更)。
- □ インターフェイス上で QoS を有効にします (Network (ネットワーク) > QoS を選択します)。

QoS のワークフロー、コンセプト、使用例の詳細は、「Quality of Service(サービス品質) [☎]」を参照してください。

新しいルールを Add(追加)するか、既存のルールをコピーして、以下のフィールドを定義します。

QoS ポリシー ルール設定

General [全般] タブ

氏名	ルールの識別に使用する名前(最大 63 文字)を入力します。名前 の大文字と小文字は区別されます。また、一意の名前にする必要が あります。文字、数字、スペース、ハイフン、およびアンダースコ アのみを使用してください。
の意味	任意の説明を入力します。
タグ	ポリシーにタグを付ける場合、タグを Add(追加)して指定しま す。 ポリシー タグとは、ポリシーをソートまたはフィルタリングでき るキーワードや語句です。多数のポリシーを定義していて、特定の キーワードでタグが付けられたポリシーを表示する場合に役立ちま す。たとえば、特定のセキュリティ ポリシーに DMZ へのインバウ ンドのタグを付けたり、復号ポリシーに「復号」と「復号なし」と いうタグを付けたり、特定のデータ センターに関するポリシーにそ の場所の名前を使用したりできます。
タグに基づいてルール をグループ化	類似のポリシールールをグループ化するのに使用するタグを入力 します。グループタグを使用すれば、対象のタグに基づいてポリ

QoS ポリシー ルール設定		
	シールール ベースを表示できます。 Tag (タグ) に基づいてルールを グループ化することができます。	•
監査コメント	ポリシールールの作成や編集を監査するために使用するコメントを 入力します。監査コメントの大文字と小文字は区別され、文字、数 字、スペース、ハイフン、およびアンダースコアを含む最大 256 文 字を指定できます。	_
監査コメント アーカイ ブ	ポリシールールの以前のAudit Comments (監査コメント)を表示し ます。監査コメント アーカイブは CSV 形式でエクスポートできま す。	_
Source [送信元] タブ		_
送信元ゾーン	送信元ゾーンを選択します(デフォルトは any(任意))。ゾーン は同じタイプ (Layer 2 [レイヤー 2]、Layer 3 [レイヤー 3]、virtual wire [バーチャル ワイヤー]) である必要があります。	_
送信元アドレス	IPv4 または IPv6 アドレスの送信元の組み合わせを指定します。識別されたアプリケーションの送信元アドレス情報は、これらのアドレスでオーバーライドされます。特定のアドレスを選択するには、ドロップダウンリストから select[選択する] を選択して、以下のいずれかを実行します。	
	• 使用可能な列で該当するアドレ	
	ス リ アドレスグループ	R
	の横にあるチェックボックスをオンにし、Add (追加) をクリック して選択内容を Selected (選択中の) 列に追加します。	
	 名前の最初の数文字を検索フィールドに入力します。入力した 文字で始まるすべてのアドレスおよびアドレスグループが一覧 表示されます。リスト内の項目を選択するとAvailable [使用可能] 列のオプションが有効化されます。この操作を必要な回数だけ 繰り返し、次に Add[追加] をクリックします。 	
	 1つ以上の IP アドレスを (1 行ごとに 1 つ) 入力します。ネット ワーク マスクは指定してもしなくてもかまいません。一般的な 形式は次のとおりです:<ip_address>/<mask></mask></ip_address> 	
	 アドレスを削除する場合は、Selected [選択済み] 列より希望のア ドレスを選択し、Delete [削除] をクリックするか、any[すべて] を選択して、すべてのアドレスおよびアドレスグループをクリ アします。 	

QoS ポリシー ルール設定		
	このポリシーまたは別のポリシーで使用できる新しいアドレスを追 加するには、New Address[新規アドレス] をクリックします。新し いアドレス グループを定義するには、Objects(オブジェクト) > Address Groups(アドレス グループ)を選択します。	-
Source User (送信元 ユーザー)	QoS ポリシーが適用される送信元のユーザーおよびグループを指定 します。	_
Negate	このタブで指定した情報に一致しないものに対してポリシーを適用 する場合は、このオプションを選択します。	_
Destination [宛先] タブ		_
宛先ゾーン	宛先ゾーンを選択します(デフォルトは any(任意))。ゾーン は同じタイプ (Layer 2 [レイヤー 2]、Layer 3 [レイヤー 3]、virtual wire [バーチャル ワイヤー]) である必要があります。	
宛先アドレス	IPv4 または IPv6 アドレスの送信元の組み合わせを指定します。識別されたアプリケーションの送信元アドレス情報は、これらのアドレスでオーバーライドされます。特定のアドレスを選択するには、ドロップダウンリストから select[選択する] を選択して、以下のいずれかを実行します。	
	 使用可能な列で該当するアドレ マ 	R
	アドレスグルー	V
	プ 横にあるチェックボックスをオンにし、Add (追加) をクリックし て選択内容を Selected (選択中の) 列に追加します。	の
	 名前の最初の数文字を検索フィールドに入力します。入力した 文字で始まるすべてのアドレスおよびアドレスグループが一覧 表示されます。リスト内の項目を選択するとAvailable [使用可能] 列のオプションが有効化されます。この操作を必要な回数だけ 繰り返し、次に Add[追加] をクリックします。 	
	 1つ以上の IP アドレスを (1 行ごとに 1つ) 入力します。ネット ワーク マスクは指定してもしなくてもかまいません。一般的な 形式は次のとおりです: <ip_address>/<mask>.</mask></ip_address> 	
	 アドレスを削除する場合は、Selected [選択済み] 列より希望のア ドレスを選択し、Delete [削除] をクリックするか、any[すべて] を選択して、すべてのアドレスおよびアドレスグループをクリ アします。 	
	このポリシーまたは別のポリシーで使用できる新しいアドレスを追 加するには、New Address[新規アドレス] をクリックします。	

QoS ポリシー ルール設定		
Negate	このタブで指定した情報に一致しないものに対してポリシーを適用 する場合は、このオプションを選択します。	
[アプリケーション] タブ		
Application [アプリ ケーション]	QoS ルールを適用する特定のアプリケーションを選択します。新し いアプリケーションまたはアプリケーション グループを定義する 場合は、Objects(オブジェクト) > Applications(アプリケーショ ン)を選択します。	
	アプリケーションに複数の機能がある場合、アプリケーション全体 または個別の機能を選択できます。アプリケーション全体を選択し た場合、すべての機能が含まれ、将来、機能が追加されるとアプリ ケーション定義が自動的に更新されます。	
	QoSルールでアプリケーション グループ、フィルタ、またはコ ンテナを使用している場合は、Application [アプリケーション] 列 のオブジェクトの上にマウスを置き、下向き矢印をクリックして Value[値] を選択すると、オブジェクトの詳細が表示されます。こ れにより、Objects(オブジェクト)タブに移動しなくても、ポリ シーから直接アプリケーション メンバーを簡単に表示できます。	
[サービス/URL カテゴリ] タブ		
サービス	特定の TCP や UDP のポート番号に制限するには、サービスを選択 します。ドロップダウンリスト リストから以下のいずれかを選択し ます。	

- any 選択したアプリケーションがすべてのプロトコルやポート で許可または拒否されます。
- application-default(アプリケーション-デフォルト) 選択したアプリケーションが、Palo Alto Networks によって定義されたデフォルトのポートでのみ許可または拒否されます。これは、許可ポリシーの推奨オプションです。
- Select[選択] Add[追加] をクリックします。既存のサービスを選 択するか、Service[サービス] または Service Group[サービス グ ループ] を選択して新しいエントリを指定します。

URL カテゴリ	QoS ルールを適用する URL カテゴリを選択します。
	 URL カテゴリに関係なくセッションでこの QoS ルールを照合で きるようにするには、Any[いずれか] を選択します。
	 カテゴリを指定するには、Add[追加] をクリックし、ドロップダ ウンリスト リストから特定のカテゴリ (カスタム カテゴリも含 む)を選択します。複数のカテゴリを追加できます。カスタム カ

テゴリの定義の詳細は、「Objects(オブジェクト) > External Dynamic Lists(外部動的リスト)」を参照してください。
Any [いずれか] (デフォルト) を選択すると、トラフィックに定義された Differentiated Services Code Point(DSCP)値またはIP優先度/Type of Service(ToS)にかかわらず、ポリシーをトラフィックに照合できます。
[コードポイント]を選択すると、トラフィックは、パケットの IP ヘッダーに定義された DSCP 値または ToS 値に基づいて QoS 処理 を受信できます。DSCP 値と ToS 値は、トラフィックに要求される サービス レベル (最優先、ベスト エフォート配信など) を示すため に使用されます。コードポイントをQoSポリシーの一致基準として 使用すると、セッションは、セッション開始時に検出されたコード ポイントに基づいてQoS処理を受信できます。
QoSポリシーにトラフィックを照合させるには、引き続きコードポ イントを Add[追加] します。
 コードポイント エントリに分かりやすい Name[名前] を付けます。
 QoSポリシーの一致条件として使用するコードポイントの Type[タイプ] を選択し、特定の Codepoint[コードポイント] 値を選択します。Codepoint Name[コードポイント名] と Binary Value[バイナリ値] を入力することにより、Custom Codepoint[カスタムコードポイント] を作成することもできま す。
ルールに割り当てる QoS クラスを選択して、OK をクリックしま す。クラス特性は、QoS プロファイルで定義します。QoS クラ スの設定方法の詳細は、「Network(ネットワーク) > Network Profiles(ネットワーク プロファイル) > QoS」を参照してくださ い。
 ポリシーを常時アクティブにしておく場合はNone [なし] を設定します。
 ドロップダウンリストからSchedule [スケジュール] (カレン ダーのアイコン)を選択し、単発の時間範囲またはルールがア クティブなあいだ繰り返される時間範囲を設定します。

Target Tab(対象タブ) (Panorama のみ)

QoS ポリシー ルール設定		
任意 (すべての対象デ バイス)	ポリシー ルールをデバイス グループのすべての管理対象ファイア ウォールにプッシュするには、有効化(チェックをオン)にしま す。	
機器	ポリシー ルールをプッシュするデバイス グループに関連付けられ た1つまたは複数の管理対象ファイアウォールを選択します。	
tags	指定したタグを持つデバイス グループ内の管理対象ファイアウォー ルにポリシー ルールをプッシュするには、1つまたは複数のタグ をAdd(追加)します。	
これらの指定された デバイスとタグのみを ターゲットに設定する	選択したデバイスとタグを除き、デバイス グループに関連付けられ ているすべての管理対象ファイアウォールにポリシー ルールをプッ シュするには、有効化(チェックをオンに)します。	

Policies > Policy Based Forwarding [ポリシー > ポリシー ベース フォワーディング]

通常、トラフィックがファイアウォールに到着すると、入力インターフェイスの仮想ルーター が、宛先 IP アドレスに基づいてルートを決定し、それによって出力インターフェイス、および 宛先セキュリティゾーンが決まります。ポリシーベースの転送(PBF)ルールを作成 Cして、送 信元ゾーン、送信元アドレス、送信元ユーザー、宛先アドレス、宛先アプリケーション、宛先 サービスなど、他の情報を指定して、出力インターフェイスを決定することができます。アプリ ケーションに関連付けられた宛先 IP アドレスおよびポートの最初のセッションは、アプリケー ション固有のルールには一致せず、後続の PBF ルール (アプリケーションが指定されない)か、 仮想ルーターの転送テーブルに従って転送されます。同じアプリケーションについて、その宛 先IP アドレスおよびポートの後続セッションはすべて、アプリケーション固有のルールに一致し ます。PBF ルールによる転送を確実に行うために、アプリケーション固有のルールを使用しな いことをお勧めします。

必要に応じて PBF ルールを使用して、トラフィックが追加の仮想システムを経由するように 「VSYS に転送」転送アクションで強制することができます。この場合、宛先仮想システムか らファイアウォールの特定の出力インターフェイス□を通じてパケットを転送する追加の PBF ルールを定義する必要があります。

以下の表では、ポリシーベースフォワーディング設定について説明します。

- ポリシーベースフォワーディングのGeneral(全般)タブ
- ポリシーベースフォワーディングの Source (送信元) タブ
- ポリシーベースフォワーディングの Destination/Application/Service (宛先/アプリケーション/サービス) タブ
- ポリシーベースフォワーディングの Forwarding (転送) タブ
- (Panorama のみ) ポリシー ベース フォワーディングの Target (宛先) タブ

その他の情報をお探しですか?

「Policy-Based Forwarding(ポリシー ベースの転送) 🖬 」を参照してください。

ポリシー ベース フォワーディングの General (全般) タブ

General[全般]タブを使用してPBFポリシーの名前と説明を設定します。タグを設定すると、大量のポリシーがある場合に、ポリシーのソートやフィルタリングにも使用できます。

項目	の意味
氏名	ルールを識別する名前を入力します。名前の大文字と小文字は区別 され、文字、数字、スペース、ハイフン、およびアンダースコアを 含む最大 63 文字を指定できます。ルール名はファイアウォールお よび Panorama 上で一意でなければなりません。また、デバイス グ

項目	の意味
	ループとその先祖または子孫デバイス グループ内でも一意でなけれ ばなりません。
の意味	ポリシーの説明を入力します (最大 1024 文字)。
タグ	ポリシーにタグを付ける場合、タグを Add(追加)して指定しま す。 ポリシー タグとは、ポリシーをソートまたはフィルタリングでき るキーワードや語句です。多数のポリシーを定義していて、特定の キーワードでタグが付けられたポリシーを表示する場合に役立ちま す。たとえば、特定のセキュリティ ポリシーに DMZ へのインバウ ンドのタグを付けたり、復号ポリシーに「復号」と「復号なし」と いうタグを付けたり、特定のデータ センターに関するポリシーにそ の場所の名前を使用したりできます。
タグに基づいてルール をグループ化	類似のポリシールールをグループ化するのに使用するタグを入力 します。グループタグを使用すれば、対象のタグに基づいてポリ シールール ベースを表示できます。Tag (タグ)に基づいてルールを グループ化することができます。
監査コメント	ポリシールールの作成や編集を監査するために使用するコメントを 入力します。監査コメントの大文字と小文字は区別され、文字、数 字、スペース、ハイフン、およびアンダースコアを含む最大 256 文 字を指定できます。
監査コメント アーカイ ブ	ポリシールールの以前のAudit Comments (監査コメント)を表示します。監査コメント アーカイブは CSV 形式でエクスポートできます。

ポリシーベースフォワーディングの Source (送信元) タブ

Source(送信元)タブを選択して、送信元ゾーンまたは送信元アドレスを定義し、送信元から 受信するトラフィックに転送ポリシーを適用するように設定します。

項目	の意味
送信元ゾーン	送信元ゾーン (デフォルトは any) を選択する場合は、Add[追加]を クリックしてドロップダウンリストから選択します。新しいゾー ンを定義する手順については、「Network(ネットワーク) > Zones(ゾーン)」を参照してください。
	複数のゾーンを使用して管理を簡略化できます。たとえば、信頼さ れていない宛先ゾーンが指定されている3つの異なる内部ゾーン

項目	の意味
	(マーケティング、販売、広報)がある場合、すべてのケースを対象 とした1つのルールを作成できます。
	ポリシーベースの転送では、レイヤー3タイプのゾーンのみがサポートされます。
送信元アドレス	Add[追加] をクリックして送信元アドレス、アドレス グループ、または地域を追加します (デフォルトは any)。ドロップダウンリストから選択するか、ドロップダウンリストの下部にある Address[アドレス]、Adress Group[アドレスグループ]、またはRegion[地域]をクリックして設定を行います。
Source User (送信元 ユーザー)	Add [追加]をクリックして、ポリシーを適用する送信元ユーザーまたはユーザー グループを選択します。以下の送信元ユーザー タイプがサポートされます。
	 any – ユーザー データに関係なく任意のトラフィックが含まれます。
	 pre-logon(ログオン前) – GlobalProtect[™]を使用してネット ワークに接続しているが、自分のシステムにはログインしてい ないリモート ユーザーが含まれます。GlobalProtect アプリの ポータルに Pre-logon(ログオン前)オプションが設定されてい る場合、自分のマシンに現在ログインしていないユーザーは、 ユーザー名 pre-logon として識別されます。pre-logon ユーザー 用のポリシーを作成でき、また、ユーザーが直接ログインして いなくても、そのマシンは完全にログインしているかのように ドメインで認証されます。
	 known-user[既知のユーザー] – 認証されたすべてのユーザー (ユーザー データがマップされた IP) が含まれます。このオプ ションは、ドメインの「ドメイン ユーザー」グループに相当し ます。
	 unknown[未知] – 認証されていないすべてのユーザー (ユー ザーにマップされていない IP アドレス) が含まれます。たとえ ば、unknown はゲスト レベルのアクセスに使用できます。これ らのユーザーは、ネットワーク上のIPを持っていますが、ドメイ ンに認証されず、ファイアウォール上にIPアドレス対ユーザーの マッピング情報がないためです。
	 select[選択] – このウィンドウで選択したユーザーが含まれます。たとえば、1人のユーザー、個々のユーザーのリスト、グループを追加したり、手動でユーザーを追加する場合があります。

項目	の意味
	⑦ ファイアウォールが User-ID [™] エージェントではな く、RADIUS、TACACS+、または SAML アイデンティ ティ プロバイダ サーバーからユーザー情報を収集し ている場合、ユーザーのリストは表示されません。 ユーザー情報を手動で入力する必要があります。

ポリシー ベース フォワーディングの Destination/Application/ Service (宛先/アプリケーション/サービス) タブ

Destination/Application/Service[宛先/アプリケーション/サービス]タブを使用して、転送ルール に一致するトラフィックに適用される宛先設定を定義します。

項目	の意味
宛先アドレス	Add (追加) をクリックして宛先アドレスあるいはアドレス グルー プを追加します(デフォルトは any)。デフォルトでは、ルール は、any IP アドレスに適用されます。ドロップダウンリストから 選択するか、ドロップダウンリストの下部にある Address (アドレ ス)、Adress Group (アドレスグループ)をクリックして設定を行いま す。
アプリケーション/サー ビス	 PBF ルールを適用する特定のアプリケーションを選択します。新しいアプリケーションを定義する方法については、「アプリケーションの定義」を参照してください。アプリケーショングループを定義する方法については、「Objects(オブジェクト) > Application Groups(アプリケーショングループ)」を参照してください。 アプリケーション固有のルールを PBF で使用することはお勧めできません。できるかぎり、サービスオブジェクト(プロトコルまたはアプリケーション
	によって使用されるレイヤー 4 ポート(TCP または UDP))を使用してください。
	これらのアプリケーションの詳細を表示するには、Application (ア プリケーション)列のオブジェクトの上にマウスを置き、下矢印を クリックして、Value (値)を選択します。これにより、Object (オブ ジェクト)タブに移動しなくても、ポリシーから直接アプリケーショ ン情報を簡単に表示できます。
	カスタムアプリケーション、アプリケーションフィ ルタ、アプリケーショングループは PBF ルールで使 用できません。

ポリシーベースフォワーディングの Forwarding (転送) タブ

Forwarding[転送]タブを使用して、転送ポリシーに一致するトラフィックに適用されるアクションおよびネットワーク情報を定義します。トラフィックは、ネクスト ホップ IP アドレスまたは 仮想システムに転送することも、ドロップすることもできます。

項目	の意味
操作	以下のいずれかのオプションを選択します。 • Forward[転送] – ネクストホップの IP アドレスと出力インター フェイス (指定したネクストホップに到達するためにパケットが 通るインターフェイス)を指定します。 • Forward To VSYS[VSYSに転送] – ドロップダウンリストから転
	 ・ Discard[破棄] - パケットを廃棄します。
	 No PBF[PBF なし] – パケットが通るパスを変更しません。この オプションは、ルールに定義された送信元/宛先/アプリケーショ ン/サービスの条件に一致するパケットを除外します。パケット の照合には、PBF の代わりにルーティングテーブルを使用しま す。ファイアウォールは、ルーティングテーブルを使用して、 一致したトラフィックをリダイレクト ポートから除外します。 Action (アクション) としてForward (転送)あるい はForward to VSYS (VSYS に転送)を使用し、Monitor (監視) プロファイルをトラフィックに適用できるよ うにします。(Action (アクション) がトラフィック を転送しない場合は Monitor (監視) プロファイルを 適用できません) 監視プロファイルは IP アドレスを 監視します。対象の IP アドレスへの接続が失敗する と、Monitor (監視) プロファイルがアクションを指定 します。
出口インターフェイス	パケットを特定の出力インターフェイスに向けます。
ネクストホップ	 パケットを特定のインターフェイスに向ける場合は、次のいずれかの方法でパケット用のネクストホップを指定します: IP Address (IP アドレス)–IP アドレスを選択し、さらに IPv4 あるいは IPv6 アドレスを使用するアドレス オブジェクトを選択(あるいはアドレス オブジェクトを新たに作成)します。 FQDN–FQDN を選択し、さらに FQDN を使用するアドレスオブジェクトを選択(あるいはアドレス オブジェクトを新たに作成)します。

項目	の意味
	 None (なし)-ネクストホップが存在せず、パケットがドロップ されます。
監視	(任意) モニタリングを有効にして、ターゲット IP Address[IP アドレス]またはNext Hop[ネクスト ホップ] IP アドレスとの接続を確認 します。Monitor (監視) を選択して、IP アドレスが到達不能な場合 のアクションを指定した(デフォルトまたはカスタム、Network (ネットワーク) > Network Profiles (ネットワーク プロファイル) > Monitor (監視)) モニタリング Profile (プロファイル) を関連付けま す。
	Monitor (監視) プロファイルを設定して監視を有効化し、出力インターフェイスでエラーが発生した場合やルートがダウンした場合に、ファイアウォールがプロファイル内のアクションを実行してサービスの中断を最小化あるいは防止できるようにします。
対称リターンの適用	(非対称ルーティング環境では必須)Enforce Symmetric Return(対称リターンの適用)を選択して、Next Hop Address(ネ クスト ホップ アドレス)リストに IP アドレスを入力します。
	対称リターンを有効にすると、リターン トラフィック(たとえ ば、LAN 上の信頼されたゾーンからインターネットへのトラフィッ ク)が、インターネットからトラフィックが入るときと同じイン ターフェイスを介して外向きに転送されます。
スケジュール	ルールを適用する日時を制限するには、ドロップダウンリストから スケジュールを選択します。新しいスケジュールを定義する手順に ついては、「復号化された SSL トラフィックのコントロールの設 定」を参照してください。

ポリシーベースフォワーディングの Target (宛先) タブ

• (Panorama のみ) Policies (ポリシー) > Policy Based Forwarding (ポリシー ベース フォワー ディング) > Target (宛先)

Target(宛先)タブを選択して、ポリシー ルールをプッシュするデバイス グループ内の管理対象ファイアウォールを選択します。管理対象ファイアウォールを選択するか、タグを指定することにより、プッシュ先の管理対象ファイアウォールを指定することができます。さらに、指定済ファイアウォールを除き、すべての管理対象ファイアウォールにプッシュするポリシー ルールの宛先を設定することができます。

NAT ルール - 宛 先設定	の意味
任意 (すべての 対象デバイス)	ポリシー ルールをデバイス グループのすべての管理対象ファイアウォール にプッシュするには、有効化(チェックをオン)にします。
機器	ポリシー ルールをプッシュするデバイス グループに関連付けられた1つま たは複数の管理対象ファイアウォールを選択します。
tags	指定したタグを持つデバイス グループ内の管理対象ファイアウォールにポ リシー ルールをプッシュするには、1つまたは複数のタグをAdd(追加)し ます。
これらの指定さ れたデバイスと タグのみをター ゲットに設定す る	選択したデバイスとタグを除き、デバイス グループに関連付けられてい るすべての管理対象ファイアウォールにポリシー ルールをプッシュするに は、有効化(チェックをオンに)します。

Policies > Decryption [ポリシー > 復号化]

トラフィックを復号するようにファイアウォールを設定して、可視化、管理、および 詳細なセキュリティを実現できます。復号化ポリシーは、SSL (Secure Sockets Layer) (IMAP(S)、POP3(S)、SMTP(S)、FTP(S)、Secure Shell (SSH) トラフィックなどの SSL カプセル化 プロトコルを含む) に適用できます。SSH復号を使用して、許可されていないアプリケーション やコンテンツがセキュアなプロトコルでトンネリングされないようにアウトバウンドおよびイン バウンドSSHトラフィックを復号化することができます。

復号化ポリシールールを追加して、復号化するトラフィックを定義することができます(URL の分類に基づいたトラフィックの復号化など)。復号化ポリシールールと受信トラフィックは順 番に照合されるため、より特定されたルールの方が全般的なルールよりも優先されます。

SSL フォワードプロキシの設定では、信頼された証明書を設定する必要があります。この証明書 はユーザーが接続中のサーバーが、ファイアウォールによって信頼された認証局によって著名 された証明書を保持している時にユーザーに提示されます。Device > Certificate Management > Certificates[デバイス > 証明書の管理 > 証明書]のページで証明書を作成し、証明書の名前をク リックして、Forward Trust Certificate[信頼された証明書の転送] チェックボックスをオンにし ます。

例えばファイアウォールは証明書のピンニングあるいはクライアント認証を使用するため、ファイアウォールは復号化を技術的に妨げるアプリケーションを復号化しません。

「List of Applications Excluded from SSL Decryption(SSL 復号化除外アプリケーションのリスト)」を参照してください。

以下の表では、復号化ポリシー設定について説明します。

- 復号化の General (全般) タブ
- 復号化の Source (送信元) タブ
- 復号化の Destination (宛先) タブ
- 復号化の Service/URL Category(サービス/URL カテゴリ)タブ
- 復号化の Options (オプション) タブ
- (Panorama のみ) Decryption Target Tab (復号宛先タブ)

その他の情報をお探しですか?

「Decryption(復号化) 🖬 」を参照してください。

復号化の General (全般) タブ

General[全般]タブを使用して、復号化ポリシーの名前と説明を設定します。タグを設定する と、大量のポリシーがある場合に、ポリシーのソートやフィルタリングを行うこともできます。

項目	の意味
氏名	ルールを識別する名前を入力します。名前の大文字と小文字は 区別され、文字、数字、スペース、ハイフン、およびアンダー スコアを含む最大 63 文字を指定できます。ルール名はファイ アウォールおよび Panorama 上で一意でなければなりません。 また、デバイス グループとその先祖または子孫デバイス グルー プ内でも一意でなければなりません。
の意味	ルールの説明を入力します (最大 1024 文字)。
タグ	ポリシーにタグを付ける場合、タグを Add (追加) して指定し ます。 ポリシー タグとは、ポリシーをソートまたはフィルタリングで きるキーワードや語句です。多数のポリシーを定義していて、 特定のキーワードでタグが付けられたポリシーを表示する場 合に役立ちます。たとえば、特定のセキュリティ ポリシーに DMZ へのインバウンドのタグを付けたり、復号ポリシーに「復 号」と「復号なし」というタグを付けたり、特定のデータ セ ンターに関するポリシーにその場所の名前を使用したりできま す。
タグに基づいてルールをグ ループ化	類似のポリシールールをグループ化するのに使用するタグを入 力します。グループタグを使用すれば、対象のタグに基づいて ポリシールール ベースを表示できます。Tag (タグ)に基づいて ルールをグループ化することができます。
監査コメント	ポリシールールの作成や編集を監査するために使用するコメントを入力します。監査コメントの大文字と小文字は区別され、文字、数字、スペース、ハイフン、およびアンダースコアを含む最大 256 文字を指定できます。
監査コメント アーカイブ	ポリシールールの以前のAudit Comments (監査コメント)を表示 します。監査コメント アーカイブは CSV 形式でエクスポート できます。

復号化の Source (送信元) タブ

Source[送信元]タブを使用して、送信元ゾーンまたは送信元アドレスを定義し、送信元から受信 するトラフィックに復号化ポリシーを適用するように設定します。

項目	の意味
送信元ゾーン	Add[追加] をクリックして送信元ゾーンを選択します (デフォルトは any)。ゾーンは同じタイプ (Layer 2 [レイヤー 2]、Layer 3 [レイヤー

項目	の意味
,	3]、virtual wire [バーチャル ワイヤー]) である必要があります。新 しいゾーンを定義する手順については、「Network(ネットワー ク) > Zones(ゾーン)」を参照してください。
	複数のゾーンを使用して管理を簡略化できます。たとえば、信頼されていない宛先ゾーンが指定されている3つの異なる内部ゾーン (マーケティング、販売、広報)がある場合、すべてのケースを対象 とした1つのルールを作成できます。
送信元アドレス	Add[追加] をクリックして送信元アドレス、アドレス グループ、ま たは地域を追加します (デフォルトは any)。ドロップダウンリスト から選択するか、ドロップダウンリストの下部にある Address[アド レス]、Adress Group[アドレスグループ]、またはRegion[地域]をク リックして設定を行います。Negate[上記以外]を選択すると、設定 したアドレス以外の任意のアドレスを指定したことになります。
Source User (送信元 ユーザー)	Add [追加]をクリックして、ポリシーを適用する送信元ユーザーまたはユーザー グループを選択します。以下の送信元ユーザー タイプがサポートされます。
	 any – ユーザー データに関係なく任意のトラフィックが含まれます。
	 pre-logon[ログオン前] – GlobalProtect を使用してネットワーク に接続しているが、自分のシステムにはログインしていないリ モート ユーザーが含まれます。GlobalProtect アプリのポータル に Pre-logon (ログオン前)オプションが設定されている場合、 自分のマシンに現在ログインしていないユーザーは、ユーザー 名 pre-logon として識別されます。pre-logon ユーザー用のポリ シーを作成でき、また、ユーザーが直接ログインしていなくて も、そのマシンは完全にログインしているかのようにドメイン で認証されます。
	 known-user[既知のユーザー] – 認証されたすべてのユーザー (ユーザー データがマップされた IP) が含まれます。このオプ ションは、ドメインの「ドメイン ユーザー」グループに相当し ます。
	 unknown[未知] - 認証されていないすべてのユーザー (ユー ザーにマップされていない IP アドレス) が含まれます。たとえ ば、unknown をゲスト レベルのアクセスに対して使用できま す。これらのユーザーは、ネットワーク上の IP を持っていま すが、ドメインに認証されず、ファイアウォール上に IP 対ユー ザーのマッピング情報がないためです。
	 select[選択] – このウィンドウで選択したユーザーが含まれます。たとえば、1人のユーザー、個々のユーザーのリスト、グループを追加したり、手動でユーザーを追加する場合があります。

項目	の意味
	⑦ ファイアウォールが User-ID [™] エージェントではな く、RADIUS、TACACS+、または SAML アイデンティ ティ プロバイダ サーバーからユーザー情報を収集し ている場合、ユーザーのリストは表示されません。 ユーザー情報を手動で入力する必要があります。

復号化の Destination (宛先) タブ

Destination (宛先)タブを使用して、宛先ゾーンまたは宛先アドレスを定義し、宛先へのトラフィックにポリシーを適用するように設定します。

項目	の意味
宛先ゾーン	Add[追加] をクリックして宛先ゾーンを選択します (デ フォルトは any)。ゾーンは同じタイプ (Layer 2 [レイヤー 2]、Layer 3 [レイヤー 3]、virtual wire [バーチャル ワイ ヤー]) である必要があります。新しいゾーンを定義するに は、Network > Zones [ネットワーク > ゾーン] を参照し てください。
	複数のゾーンを使用して管理を簡略化できます。たとえ ば、信頼されていない宛先ゾーンが指定されている3つの 異なる内部ゾーン (マーケティング、販売、広報) がある場 合、すべてのケースを対象とした1つのルールを作成でき ます。
宛先アドレス	Add[追加] をクリックして宛先アドレス、アドレス グルー プ、または地域を追加します (デフォルトは any)。ドロッ プダウンリストから選択するか、ドロップダウンリストの 下部にある Address[アドレス]、Adress Group[アドレスグ ループ]、またはRegion[地域]をクリックして設定を行いま す。Negate[上記以外]を選択すると、設定したアドレス以 外の任意のアドレスを指定したことになります。

復号化の Service/URL Category (サービス/URL カテゴリ) タブ

Service/URL Category[サービス/URLカテゴリ]タブでは、復号化ポリシーを、TCPポート番号に 基づいてトラフィックに、または任意のURLカテゴリ(またはカテゴリリスト)に適用できます。

項目	の意味
サービス	特定の TCP/UDP ポート番号に基づいて、復号化ポリシー をトラフィックに適用します。ドロップダウンリスト リス トから以下のいずれかを選択します。
	 any - 選択したアプリケーションがすべてのプロトコル やポートで許可または拒否されます。
	 application-default[アプリケーション-デフォルト] – 選 択したアプリケーションが、Palo Alto Networks によっ てアプリケーション用に定義されたデフォルトのポート でのみ復号化 (または復号化を免除) されます。
	 Select[選択] - Add[追加] をクリックします。既存の サービスを選択するか、新規の Service[サービス] ま たは Service Group[サービス グループ] を指定しま す。(またはObjects > Services [オブジェクト > サービ ス]とObjects(オブジェクト) > Service Groups(サー ビス グループ)を選択します)。
URL Category [URL カテゴリ] タブ	復号化ルールを適用する URL カテゴリを選択します。
	 URL カテゴリに関係なくすべてのセッションを照合する には、any を選択します。
	 カテゴリを指定するには、Add[追加] をクリックし、ドロップダウンリストリストから特定のカテゴリ(カスタムカテゴリも含む)を選択します。複数のカテゴリを追加できます。カスタムカテゴリの定義方法に関する詳細を参照してください。

復号化の Options(オプション)タブ

Options[オプション]タブを使用して、一致したトラフィックを復号化するかどうかを決定しま す。**Decrypt**[復号] が設定されている場合、復号化タイプを指定します。また、復号化プロファ イルを構成または選択して、復号化機能を追加することもできます。

項目	の意味
操作	トラフィックのdecrypt[復号] または no-decrypt[復号なし] を選 択します。
タイプ	ドロップダウンリストから復号化するトラフィックのタイプを 選択します。
	 SSL Forward Proxy - ポリシーが外部サーバー宛てのクライ アントトラフィックを復号化することを指定します。

項目	の意味
	 SSH Proxy - ポリシーが SSH トラフィックを復号化することを指定します。このオプションでは、ssh-tunnel App-ID を指定してポリシーの SSH トンネリングを制御できます。 SSL インバウンドインスペクション - ポリシーがインバウンド SSL トラフィックを復号することを指定します。 証明書 - インバウンド SSL トラフィックの宛先となる内部サーバーの証明書を追加します。
	 ・ ・ ・
	Web サーバーによってホストされているドメインの証明 書を追加することもできます。ポリシー規則ごとに最大 12 個の証明書がサポートされます。
復号化プロファイル	復号化プロファイルをポリシー ルールにアタッチして、トラフィックの特定の側面をブロックおよび制御します。復号化プロファイルの作成の詳細については、Objects > Decryption Profile [オブジェクト > 復号化プロファイル]を選択してください。
ログ設定	

正常完了した SSL ハンド	(オプション)正常に完了した SSL復号化ハンドシェイクの詳
シェイクのログへの記録	細ログを作成します。デフォルトで無効になっています。

項目	の意味
	 ログはストレージ容量を消費します。ログを 保存するリソースがあることを確認してから正 常に完了した SSL ハンドシェイクをログに記録 します。Device(デバイス) > Setup(セット アップ) > Management(管理) > Logging and Reporting Settings(ログとレポートの設定)を編 集して、現在のログメモリの割り当てを確認し、 ログタイプ間のログメモリに再割り当てを行いま す。
失敗した SSL ハンドシェイ クのログへの記録	失敗した SSL 復号化ハンドシェイクの詳細なログを作成する と、復号化の問題の原因を特定可能となります。デフォルトで 有効になっています。
	 ログはストレージ容量を消費します。より多くの(またはより少ない)ログストレージ容量を復号化ログに割り当てるには、ログメモリの割り当てを編集します(Device(デバイス) > Setup(セットアップ) > Management(管理) > Logging and Reporting Settings(ログとレポートの設定))。
ログ転送	GlobalProtect SSL ハンドシェイク(復号化)ログを転送する方 法および場所を指定します。

Decryption Target Tab(復号宛先タブ)

• (Panorama のみ) Policies (ポリシー) > Decryption (復号化) > Target (宛先)

[Target(宛先)]タブを選択して、ポリシー ルールをプッシュするデバイス グループ内の管理対象ファイアウォールを選択します。管理対象ファイアウォールを選択するか、タグを指定することにより、プッシュ先の管理対象ファイアウォールを指定することができます。さらに、指定済ファイアウォールを除き、すべての管理対象ファイアウォールにプッシュするポリシー ルールの宛先を設定することができます。

NAT ルール - 宛 先設定	の意味
任意 (すべての 対象デバイス)	ポリシー ルールをデバイス グループのすべての管理対象ファイアウォール にプッシュするには、有効化(チェックをオン)にします。
機器	ポリシー ルールをプッシュするデバイス グループに関連付けられた1つま たは複数の管理対象ファイアウォールを選択します。

NAT ルール - 宛 先設定	の意味
tags	指定したタグを持つデバイス グループ内の管理対象ファイアウォールにポ リシー ルールをプッシュするには、1つまたは複数のタグをAdd(追加)し ます。
これらの指定さ れたデバイスと タグのみをター ゲットに設定す る	選択したデバイスとタグを除き、デバイス グループに関連付けられてい るすべての管理対象ファイアウォールにポリシー ルールをプッシュするに は、有効化(チェックをオンに)します。

ポリシー>ネットワークパケットブローカー

ネットワークパケットブローカポリシールールは、アプリケーション、ユーザ、ゾーン、デバ イス、および IP アドレスに基づいて、サードパーティのセキュリティ アプライアンス (セキュ リティ チェーン)の外部チェーンに転送するトラフィックを定義します。ネットワークパケット ブローカーは、暗号化解除された TLS、非復号化 TLS、および TLS 以外のトラフィックをセキュ リティ チェーンに転送できます。パケット ブローカー プロファイルは、各ネットワークパケッ ト ブローカ ポリシー ルールにアタッチします。ポリシー ルールはセキュリティ チェーンに転 送するトラフィックを定義し、プロファイルは、ファイアウォール転送インターフェイス、ヘル ス モニタリング、複数のチェーン間のセッションの分散、チェーンのルーティング(レイヤ 3)ま たはトランスペアレント ブリッジ(レイヤ 1)のどちらを選択するかなど、そのトラフィックの転 送方法を定義します。

次の表に、ネットワーク パケット ブローカーのポリシー ルール設定とポリシー オプティマイ ザー オプションについて説明します。

- [ネットワークパケットブローカ全般] タブ
- [ネットワークパケットブローカソース] タブ
- [ネットワークパケットブローカ宛先] タブ
- ネットワークパケット ブローカアプリケーション/サービス/トラフィックタブ
- [ネットワークパケットブローカパスの選択] タブ
- ネットワーク パケット ブローカ ポリシー オプティマイザー ルールの使用法

[ネットワークパケットブローカ全般] タブ

[全般]タブを選択して、ポリシーの名前と説明を構成します。タグを設定すると、大量のポリ シーがある場合に、ポリシーのソートやフィルタリングを行うこともできます。

項目	の意味
氏名	ルールを識別する名前を入力します。名前の大文字と小文字は区別 され、文字、数字、スペース、ハイフン、およびアンダースコアを 含む最大 63 文字を指定できます。ルール名はファイアウォールお よび Panorama 上で一意でなければなりません。また、デバイス グ ループとその先祖または子孫デバイス グループ内でも一意でなけれ ばなりません。
の意味	ポリシーの説明を入力します (最大 1024 文字)。
タグ	ポリシーにタグを付ける場合、タグを Add(追加)して指定しま す。
	ポリシー タグとは、ポリシーをソートまたはフィルタリングできる キーワードや語句です。これは、多数のポリシーを定義し、特定の キーワードでタグ付けされたポリシーを表示する場合に便利です。

項目	の意味
	たとえば、このタグは、ネットワークロケーション、レイヤ3セ キュリティ チェーン、レイヤ1セキュリティ チェーンなどを示し ます。
タグに基づいてルール をグループ化	類似のポリシールールをグループ化するのに使用するタグを入力し ます。グループ タグを使用すると、これらのタグに基づいてポリ シー ルール ベースのグループを表示できます。
監査コメント	ポリシールールの作成や編集を監査するために使用するコメントを 入力します。監査コメントの大文字と小文字は区別され、文字、数 字、スペース、ハイフン、およびアンダースコアを含む最大 256 文 字を指定できます。
監査コメント アーカイ ブ	ポリシールールの以前のAudit Comments (監査コメント)を表示し ます。監査コメント アーカイブは CSV 形式でエクスポートできま す。

[ネットワークパケット ブローカ ソース] タブ

[Source] タブを選択して、ネットワーク パケット ブローカ セキュリティ チェーンに転送する トラフィックの送信元ゾーン、IP アドレス、ユーザ、およびデバイスを定義します。

項目	の意味
送信元ゾーン	送信元ゾーン (デフォルトは any) を選択する場合は、Add[追加]を クリックしてドロップダウンリストから選択します。新しいゾー ンを定義する手順については、「Network(ネットワーク) > Zones(ゾーン)」を参照してください。 複数のゾーンを追加して、管理を簡素化できます。
送信元アドレス	送信元アドレス、アドレス グループ、または地域を Add (追加) します (デフォルトは Any (すべて))。ドロップダウンリスト から選択するか、ドロップダウンリストの下部にある Address (ア ドレス) オブジェクト、Address Group (アドレスグループ)、ま たはRegions (地域)を選択して設定を行います。アドレス > と のオブジェクト > アドレス グループ のオブジェクトは、それぞ れ、ポリシー ルールがサポートするアドレス オブジェクトとアド レス グループの種類を記述します。
	Negate オプションを選択すると、指定したアドレスを除き、指定 したゾーンの送信元アドレスにルールが適用されます。

項目	の意味
送信元ユーザー	Add [追加]をクリックして、ポリシーを適用する送信元ユーザーまたはユーザー グループを選択します。以下の送信元ユーザー タイプがサポートされます。
	 any – ユーザー データに関係なく任意のトラフィックが含まれます。
	 pre-logon (ログオン前) – GlobalProtect[™]を使用してネット ワークに接続しているが、自分のシステムにはログインしてい ないリモート ユーザーが含まれます。GlobalProtect アプリの ポータルでログオン前オプションが構成されている場合、現在 コンピューターにログインしていないユーザーは、ログオン前 のユーザー名で識別されます。pre-logon ユーザー用のポリシー を作成でき、また、ユーザーが直接ログインしていなくても、 そのマシンは完全にログインしているかのようにドメインで認 証されます。
	 known-user[既知のユーザー] – 認証されたすべてのユーザー (ユーザー データがマップされた IP) が含まれます。このオプ ションは、ドメインの「ドメイン ユーザー」グループに相当し ます。
	 unknown[未知] – 認証されていないすべてのユーザー (ユーザー にマップされていない IP アドレス) が含まれます。たとえば、 ネットワーク上に IP を持つものの、ドメインに対して認証され ておらず、ファイアウォール上の IP アドレスとユーザーのマッ ピング情報を持たないため、ゲスト レベルのアクセスに不明な 情報を使用できます。
	 select[選択] – このウィンドウで選択したユーザーが含まれます。たとえば、1人のユーザー、個々のユーザーのリスト、グループを追加したり、手動でユーザーを追加する場合があります。
	⑦ ファイアウォールが User-ID [™] エージェントではな く、RADIUS、TACACS+、または SAML アイデンティ ティ プロバイダ サーバーからユーザー情報を収集し ている場合、ユーザーのリストは表示されません。 ユーザー情報を手動で入力する必要があります。
送信元デバイス	ポリシー対象ホスト デバイスのAdd(追加):
	• any (すべて) – すべてのデバイスを含めます。
	 no-hip(HIPなし) – HIP 情報を必要としません。この設定に より、HIP 情報を収集または送信できないサードパーティ デバ イスからのアクセスが可能になります。

項目	の意味
	 select(選択) – 設定で選択されるデバイスが含まれます。例えば、モデル、OS、OS ファミリー、またはベンダーに基づき、デバイスオブジェクトを追加することができます。

[ネットワークパケットブローカ宛先] タブ

[宛先] タブを選択して、宛先ゾーン、IP アドレス、およびトラフィックのデバイスを定義して、ネットワーク パケット ブローカ セキュリティ チェーンに転送します。

項目	の意味
Destination Zone	送信元ゾーン (デフォルトは any) を選択する場合は、Add[追加]を クリックしてドロップダウンリストから選択します。新しいゾー ンを定義する手順については、「Network(ネットワーク) > Zones(ゾーン)」を参照してください。 複数のゾーンを追加して、管理を簡素化できます。
宛先アドレス	 宛先アドレス、アドレス グループ、または地域を Add (追加) します (デフォルトは Any (すべて))。ドロップダウンリストから選択するか、ドロップダウンリストの下部にある Address (アドレス)オブジェクトをクリックし、Address Group (アドレスグループ)、またはRegions (地域)を選択してアドレス設定を指定します。アドレス > とのオブジェクト > アドレス グループのオブジェクトは、それぞれ、ポリシー ルールがサポートするアドレスオブジェクトとアドレス グループの種類を記述します。 Negate オプションを選択すると、指定したアドレスを除き、指定されたゾーンの宛先アドレスにルールが適用されます。
宛先デバイス	ポリシーの対象となるホスト デバイスを に追加するか、 Any を選 択してすべてのデバイスを含めます。

ネットワーク パケット ブローカ アプリケーション/サービス/ト ラフィック タブ

アプリケーション/サービス/トラフィック タブを選択して、ネットワークパケット ブローカ セ キュリティ チェーンに転送するトラフィックのタイプ、アプリケーション、およびサービスを 定義します。暗号化解除された TLS、非復号 TLS、および TLS 以外のトラフィックの任意の組み 合わせをセキュリティ チェーンに転送できます。

項目	の意味
トラフィックの種類	セキュリティ チェーンに転送するトラフィックタイプを選択しま す。1つのルールで、1種類、一部、またはすべてのトラフィック タイプを選択できます。
	 転送 TLS(復号された) トラフィック-(デフォルト) ネットワーク パケット ブローカ ポリシーにアタッチされたパケット ブローカ プロファイルで指定されたセキュリティ チェーンに復号化され た TLS トラフィックを転送します。
	 転送 TLS(非復号) トラフィック:ネットワーク パケット ブローカ ポリシーにアタッチされたパケット ブローカ プロファイルで指 定されたセキュリティ チェーンに、復号化されていない TLS ト ラフィックを転送します。
	 転送非 TLS トラフィック:クリアテキスト(TLS 以外)トラフィックを、ネットワーク パケット ブローカ ポリシーにアタッチされたパケット ブローカ プロファイルで指定されたセキュリティチェーンに転送します。
アプリケーション	Add ネットワークパケット ブローカ ポリシー ルールの特定のアプ リケーション。アプリケーションに複数の機能がある場合は、コン テナアプリケーションまたは個々の機能アプリケーションを選択で きます。コンテナー アプリケーションを選択すると、すべての機能 アプリケーションが含まれ、今後の機能アプリがコンテナー アプリ に追加されると、アプリケーション定義が自動的に更新されます。
サービス	特定の TCP または UDP のポート番号に制限したいサービスを選択 します。ドロップダウンリスト リストから以下のいずれかを選択し ます。
	 – (デフォルト) 選択したアプリケーションは、任意のプロトコル またはポートで転送されます。
	 アプリケーション既定-選択したアプリケーションは、Palo Alto Networks[®]で定義されているデフォルトのポートにある場合に のみ転送されます。(非標準のポートやプロトコルで動作するア プリケーションは、意図しない場合、望ましくないアプリケー ションの動作や使用法の兆候となり、意図的であれば、悪意の ある動作の兆候になる可能性があります。ただし、内部カスタ ムアプリケーションでは標準以外のポートが使用され、例外が 必要な場合があります。
	 Select (選択) – 既存のサービスをAdd (追加) する か、Service (サービス) またはService Group (サービス グループ)を選択して新しいエントリを指定します。(また は Objects (オブジェクト) > Services (サービス) および

項目	の意味
	Objects(オブジェクト) > Service Groups(サービス グルー プ)を選択します)。

[ネットワークパケットブローカパスの選択] タブ

[パス選択]タブ を選択して、ネットワークパケット ブローカ ポリシーで定義されたトラフィックに適用するパケット ブローカ プロファイルを選択します。ポリシーはセキュリティ チェーン に転送するトラフィックを定義し、プロファイルはトラフィックの転送方法を定義します(どのファイアウォール転送インターフェイスを使用するか、セキュリティ チェーンがルーティング されたレイヤ3チェーンかトランスペアレント ブリッジ レイヤ1チェーンか、ヘルス モニタリング方法など)。

ドロップダウンを使用して、以前に設定したプロファイルを選択するか、ポリシー ルール用の 新しいパケット ブローカ プロファイルを作成します。

ネットワーク パケット ブローカ ポリシー オプティマイザー ルー ルの使用法

ネットワーク パケット ブローカ ポリシー ルールの場合、ポリシー オプティマイザーは ルール 使用法 統計情報を表示します。さまざまな期間にわたるルールの使用状況を表示し、ルールが 期待どおりに使用されていない理由を調べたり、使用されていないルールや古いルールを削除し たりできます。

項目	の意味
Timeframe(期間)	データが表示される期間(日数)。
使用率	 任意指定された Timeframe を介してファイアウォール上のすべてのネットワークパケット ブローカ ポリシー ルールが、ルールに一致するかどうか (使用済みのルール) と一致しない (未使用のルール) に関係なく、 指定した Timeframe でトラフィックが一致していないルールを>Unused ルールに指定します。 指定した Timeframe でトラフィックが一致していないルールを>Unused ルールに指定します。
過去の「n」日間にリ セットされたルールを 除外する	Reset ルール ヒット カウンタ が指定した日数 (1 ~ 5,000 日) の 範囲内でルールを表示しないようにします。たとえば、特定の Timeframe 上のトラフィックに一致していない古いルールを調べ、 トラフィックを照合する時間がない新しいルールを除外できます。
氏名	ネットワーク パケット ブローカ ポリシー ルールの名前。

項目	の意味
パケットブローカー	 Profile: ポリシー ルールに関連付けられたパケット ブローカ プロファイルの名前。 トラフィックタイプ: ルールが制御するトラフィックのタイプ(復号化された TLS、非復号された TLS、および TLS 以外のトラフィック)。
ルールの使用状況	 ヒット数–トラフィックがルールに一致した回数。 最後のヒット:トラフィックがルールに一致した最新の時刻。 最初のヒット:トラフィックがルールに初めて一致した時。 リセット日付–ルールのヒットカウンタがリセットされた最後の日付。
変更済	ルールを最後に編集した日時。
作成日時	ルールが作成された日時。
Policies(ポリシー) > Tunnel Inspection(トンネル検 査)

以下のクリアテキスト トンネル プロトコルのトラフィック コンテンツを検査するようにファイ アウォールを設定できます。

- Generic Routing Encapsulation (GRE)
- General Packet Radio Service (GPRS) Tunneling Protocol for User Data (GTP-U) (GTP を サポートしているファイアウォールでのみサポート)
- 非暗号 IPSec トラフィック(IPSec および転送モードの AH IPSec の NULL 暗号化アルゴリズム)
- 拡張可能な仮想 LAN (VXLAN)

トンネル コンテンツ検査を使用して、これらのタイプのトンネルのトラフィックや、別のクリ アテキスト トンネルでネストされたトラフィック(たとえば、GRE トンネル内の Null 暗号化さ れた IPSec)に、セキュリティ、DoS プロテクション、QoS ポリシーを適用できます。

ファイアウォールが検査するパケットのトンネル プロトコルの種類を受信パケット照合時に特定したり、ファイアウォールでのパケットの廃棄または処理の継続の条件を指定したりするトンネル検査ポリシーを作成します。トンネル検査ログとトンネル アクティビティを ACC で表示して、トンネリングされたトラフィックが企業のセキュリティおよび使用ポリシーに沿っていることを確認できます。

ファイアウォールは、イーサネット インターフェイスおよびサブインターフェイス、AE イン ターフェイス、VLAN インターフェイス、VPN および LSVPN トンネルでのトンネル コンテン ツ検査をサポートします。この機能は、レイヤー 3、レイヤー 2、バーチャル ワイヤー、タップ デプロイメントでサポートされています。トンネル コンテンツ検査は、共有ゲートウェイと、 仮想システムから仮想システムへの通信で機能します。

知りたい内容	以下を参照
トンネル検査ポリシーを作成 する際に使用可能なフィール ドは?	トンネル検査ポリシーの構成要素
トンネル検査ログを表示する には?	Log Types and Severity Levels(ログタイプと重大度レベル)
その他の情報をお探しです か?	Tunnel Content Inspection (トンネル コンテンツ検査)

トンネル検査ポリシーの構成要素

トンネル検査ポリシー ルールを追加するには、**Policies**(ポリシー) > **Tunnel Inspection**(トン ネル検査)を選択します。ファイアウォールを使用して、クリアテキスト トンネルでネストさ れたトラフィック(GRE、GTP-U、非暗号化 IPSec、および VXLAN)のコンテンツを検査した り、トンネルコンテンツ検査を活用してこのような種類のトンネルにおけるトラフィックでセ キュリティ、DoS プロテクション、QoS ポリシーを適用できます。すべてのファイアウォール モデルは GRE の tunnel content inspection(トンネル コンテンツ検査)および非暗号化 IPSec トンネルをサポートしますが、GTP-U トンネルのトンネル コンテンツ検査をサポートするのは GTP をサポートしているファイアウォールのみです。以下の表で、トンネル検査ポリシーを設 定するフィールドについて説明します。

トンネル検査ポリ シーの構成要素	設定場所	の意味
氏名	一般	トンネル検査ポリシーの名前を入力します。最初 の文字は英数字で、0以上の数字、アルファベット 文字、アンダースコア、ハイフン、ピリオド、ス ペースを含めることができます。
の意味		(任意)トンネル検査ポリシーの説明を入力しま す。
tags		(任意)レポートまたはログのためのタグを入力 し、トンネル検査ポリシー対象のパケットを判別 できるようにします。
タグに基づいて ルールをグループ 化		類似のポリシールールをグループ化するのに使用 するタグを入力します。グループタグを使用すれ ば、対象のタグに基づいてポリシールール ベース を表示できます。 Tag (タグ) に基づいてルールをグ ループ化することができます。
監査コメント		ポリシールールの作成や編集を監査するために 使用するコメントを入力します。監査コメントの 大文字と小文字は区別され、文字、数字、スペー ス、ハイフン、およびアンダースコアを含む最大 256 文字を指定できます。
監査コメント アー カイブ		ポリシールールの以前のAudit Comments (監査コ メント)を表示します。監査コメント アーカイブは CSV 形式でエクスポートできます。
Source Zone	送信元	トンネル検査ポリシーを適用するパケットの送信 元ゾーンを Add(追加)します(デフォルトは Any(任意))。
送信元アドレス		(<u>任意</u>)トンネル検査ポリシーを適用するパケッ トの送信元 IPv4 または IPv6 アドレス、アドレ ス グループ、または地域アドレス オブジェクト

トンネル検査ポリ シーの構成要素	設定場所	の意味
		を Add(追加)します(デフォルトは Any(任 意))。
Source User (送 信元ユーザー)		(<mark>任意</mark>)トンネル検査ポリシーを適用するパケッ トの送信元ユーザーを Add(追加)します(デ フォルトは any(任意))。
Negate		(任意)これらの指定したアドレス以外の任意の アドレスを選択するには、Negate(上記以外)を 選択します。
Destination Zone	宛先	トンネル検査ポリシーを適用するパケットの宛 先ゾーンを Add(追加)します(デフォルトは Any(任意))。
宛先アドレス		(任意) トンネル検査ポリシーを適用するパケッ トの宛先 IPv4 または IPv6 アドレス、アドレス グループ、または地域アドレス オブジェクト を Add (追加) します (デフォルトは Any (任 意))。
Negate		(任意)これらの指定したアドレス以外の任意の アドレスを選択するには、Negate(上記以外)を 選択します。
トンネル プロトコ ル	検査	 ファイアウォールで検査するトンネルプロトコルを Add (追加) します。 GRE – ファイアウォールは、トンネルでGeneric Route Encapsulation を使用するパケットを検査します。 GTP-U – ファイアウォールは、トンネルでGeneral Packet Radio Service (GPRS)のユーザーデータ用トンネリングプロトコル (GTP-U)を使用するパケットを検査します。 Non-encrypted IPSec (非暗号 IPSec) – ファイアウォールは、トンネルで暗号化されていないIPSec (Null 暗号化 IPSec または転送モードのAH IPSec)を使用するパケットを検査します。 VXLAN–ファイアウォールは VXLAN のペイロードを検査し、トンネル内のカプセル化されたコンテンツやアプリケーションを見つけます。

トンネル検査ポリ シーの構成要素	設定場所	の意味
		リストからプロトコルを削除するには、プロトコ ルを選択して Delete (削除)します。
最大トンネル検査 レベル	検査 > 検査オプ ション	ファイアウォールがカプセル化の One Level(1段 階)(デフォルト)または Two Levels (Tunnel In Tunnel)(2 段階(トンネル内トンネル))を検査 するか指定します。検査は他のレイヤーでのみ行 われるため、VXLAN の場合はOne Level (1 レベ ル)を選択します。
最大トンネル検査 レベルを超えた場 合はパケットをド ロップ		(<u>任意</u>)最大トンネル検査レベルの指定値を上回 るレベルのカプセル化を含むパケットをドロップ します。
トンネル プロト コルが厳密なヘッ ダー チェックに 失敗した場合はパ ケットをドロップ		 (任意)プロトコルの RFC に準拠しないヘッダーを使用しているトンネルプロトコルを含むパケットをドロップします。準拠しないヘッダーは、不審なパケットを示唆します。このオプションにより、ファイアウォールは RFC 2890 に対して GRE ヘッダーを確認します。 (A) RFC 2890 よりも古い GRE のバー
		 ジョンを導入しているデバイスで、 ファイアウォールが GRE をトンネリ ングしている場合、このオプション は有効にしないでください。
トンネル内に不明 なプロトコルがあ る場合はパケット をドロップ		(<u>任意</u>)ファイアウォールが判別できないトンネ ル内のプロトコルを含むパケットをドロップしま す。
スキャンされた VXLAN トンネル を送信元に戻す		(任意)このオプションを有効化して、トラ フィックを元の VXLAN トンネルのエンドポイント (VTEP)に戻します。例えば、カプセル化された パケットを送信元の VTEP に戻す場合にこのオプ ションを使用します。レイヤー3、レイヤー3サ ブインターフェイス、集約インターフェイスレイ ヤー3、VLAN でのみサポートされています。
セキュリティ オプ ションの有効化	検査 > セキュリ ティ オプション	(任意)Enable Security Options(セキュリティ オプションの有効化)によって、トンネル コン テンツの個別のセキュリティ ポリシー処理用に

トンネル検査ポリ シーの構成要素	設定場所	の意味
		セキュリティ ゾーンが割り当てられます。内部 コンテンツの送信元は、指定した Tunnel Source Zone(トンネル送信元ゾーン)に属し、内部コ ンテンツの宛先は、指定した Tunnel Destination Zone(トンネル宛先ゾーン)に属すようになりま す。
		セキュリティオプションの有効化を行わない場 合、デフォルトでは、内部コンテンツの送信元は 外部トンネルの送信元と同じゾーンに属し、内 部コンテンツの宛先は外部トンネルの宛先と同じ ゾーンに属します。このため、内部コンテンツの 送信元と宛先は、それらの外部トンネルの送信元 ゾーンと宛先ゾーンに適用されるセキュリティポ リシーと同じ管理下に置かれます。
トンネル送信元 ゾーン		Enable Security Options(セキュリティ オプショ ンの有効化)を実行する場合、作成したトンネル ゾーンを選択すると、内部コンテンツはポリシー 実行の目的でこの送信元ゾーンを使用します。
		そうでない場合、デフォルトでは、内部コンテン ツの送信元は外部トンネルの送信元と同じゾーン に属し、外部トンネル送信元ゾーンのポリシーも 内部コンテンツ送信元ゾーンに適用されます。
トンネル宛先ゾー ン		Enable Security Options(セキュリティオプションの有効化)を実行する場合、作成したトンネル ゾーンを選択すると、内部コンテンツはポリシー 実行の目的でこの宛先ゾーンを使用します。
		そうでない場合、デフォルトでは、内部コンテン ツの宛先は外部トンネルの宛先と同じゾーンに属 し、外部トンネル宛先ゾーンのポリシーも内部コ ンテンツ宛先ゾーンに適用されます。
モニター名	検査 > モニター オ プション	(任意) ログとレポートでトラフィックを監視 する目的で、類似するトラフィックをまとめてグ ループ化するためのモニター名を入力します。
モニター タグ (番 号)		(任意) ログとレポート向けに類似するトラ フィックをまとめてグループ化するためのタグ番 号を入力します(範囲は1~16,777,215)。タグ 番号はグローバルに定義されます。

トンネル検査ポリ シーの構成要素	設定場所	の意味
		 このフィールドは、VXLAN プロト コルには適用されません。VXLAN ログは自動的に VXLAN ヘッダーの VXLAN ネットワーク識別子(VNI) を使用します。
セッション開始時 にログ		 (任意) このオプションを選択すると、トンネル 検査ポリシーに一致するクリアテキストトンネル セッションの開始時にログが生成されます。この 設定は、セッションに適用されるセキュリティポ リシールールの Log At Session Start (セッション 開始時にログ) 設定よりも優先されます。 トンネル ログはトラフィック ログとは別に保存 されます。外部トンネル セッション (GRE、非暗 号化 IPSec、または GTP-U) の情報はトンネル ロ グに保存され、内部トラフィック フローはトラ フィック ログに保存されます。別々に保存するこ とにより、ACC とレポート機能を使用してトンネ ルのアクティビティ (内部コンテンツのアクティ ビティと対照) を簡単にレポートできます。 トンネル ログのベストプラクティ スは、Log at Session Start (セッショ ン開始時にログ) を記録し、Log at Session End (セッション終了時にロ グ) を記録することです。これは、 ログを記録するためにトンネルが非 常に長寿命になる可能性があるため です。たとえば、GRE トンネルは ルーターの起動時に起動し、ルー ターが再起動されるまで終了しませ ん。セッション開始時にログを選択 しないと、ACC にアクティブな GRE トンネルが存在することはありませ ん。
セッション終了時 にログ		(任意)このオプションを選択すると、トンネ ル検査ポリシーに一致するクリアテキストトン ネルセッションの終了時にログがキャプチャさ れます。この設定は、セッションに適用される セキュリティポリシールールの Log At Session

トンネル検査ポリ シーの構成要素	設定場所	の意味
		End(セッション終了時にログ)設定よりも優先さ れます。
ログ転送		 (任意)トンネル検査ログを転送する場所 を指定するには、ドロップダウンからLog Forwarding(ログの転送)プロファイルを選択 します。(この設定は、トラフィックログに適 用されるセキュリティポリシールールのLog Forwarding(ログ転送)設定とは異なります)。
氏名	トンネル ID デフォルト設定で は、VXLAN ID を 設定していない場 合にすべてのトラ フィックが検査さ	(任意)最初の文字は英数字で、0以上の数字、 アルファベット文字、アンダースコア、ハイフ ン、ピリオド、スペースを含めることができる名 前。Name (名前)はグループ化している VNI を示し ます。名前は便宜上のものであり、ログ、監視、 レポートの要素にはなりません。
VXLAN ID (VNI)	れます。 VXLAN ID を設定 している場合、 これを一致条件と して使用してトラ	(Optional)単一の VNI、コンマで区切られた VNI の リスト、最大 1,600 万個の VNI の範囲 (区切り文字 としてハイフンを使用)、またはこれらの組み合わ せを入力します。例: 1-54,1024,1677011-1677038,94
	フィックの検査を 特定の VNI に限定 することができま す。	ポリシーごとの最大 VXLAN ID は 4,096 です。構 成メモリを保持するには、可能な限り範囲を使用 してください。
任意 (すべての対 象デバイス) Panorama のみ	ターゲット	ポリシー ルールをデバイス グループのすべての管 理対象ファイアウォールにプッシュするには、有 効化(チェックをオン)にします。
デバイス Panorama のみ		ポリシー ルールをプッシュするデバイス グループ に関連付けられた 1 つまたは複数の管理対象ファ イアウォールを選択します。
tags Panorama のみ		指定したタグを持つデバイス グループ内の管理対 象ファイアウォールにポリシー ルールをプッシュ するには、1つまたは複数のタグをAdd(追加)し ます。
これらの指定され たデバイスとタグ のみをターゲット に設定する		選択したデバイスとタグを除き、デバイス グルー プに関連付けられているすべての管理対象ファイ

トンネル検査ポリ シーの構成要素	設定場所	の意味
Panorama のみ		アウォールにポリシー ルールをプッシュするに は、有効化(チェックをオンに)します。

Policies > Application Override [ポリシー > アプリケー ション オーバーライド]

ファイアウォールによるネットワークトラフィックのアプリケーション分類方法を変更するに は、アプリケーションオーバーライドポリシーを指定します。たとえば、カスタムアプリケー ションのいずれかを制御する場合、アプリケーションオーバーライドポリシールールを使用す ると、ゾーン、送信元アドレスと宛先アドレス、ポート、およびプロトコルに従って、そのアプ リケーションのトラフィックを識別できます。「不明」として分類されたネットワーク・アプリ ケーションがある場合は、それらのネットワーク・アプリケーションに対して新しいアプリケー ション定義を作成できます (アプリケーションの定義を参照)。

ファイアウォールが App-ID を使用してアプリケーションを特定したり、脅威に対してレイヤー7検査を実行したりすることができなくなるため、可能な場合はアプリケーションオーバーライドポリシーを使用しないでください。内部の専有アプリケーションをサポートする場合、アプリケーションシグネチャを含むカスタムアプリケーションを作成し、ファイアウォールがレイヤー7検査を実行してアプリケーショントラフィックの脅威をスキャンできるようにすることが推奨されます。商用アプリケーションが App-ID を持っていない場合は、新しい App-ID をリクエストしてください。公開アプリケーション定義(デフォルトのポートあるいはシグネチャ)が変化し、ファイアウォールがアプリケーションを正しく識別できなくなる場合は、サポートチケットを作成して Palo Alto Networks が定義を更新できるようにしてください。その間、ファイアウォールがトラフィックのレイヤー7検査を実行し続けられるよう、カスタムアプリケーションを作成します。

セキュリティ ポリシーと同様に、必要に応じて全般的または個別のアプリケーション オーバー ライド ポリシーを使用できます。ポリシー ルールと受信トラフィックは順番に照合されるた め、より個別のルールの方が全般的なルールよりも上に来るようにする必要があります。

PAN-OS の App-ID エンジンは、ネットワーク トラフィックのアプリケーション特有のコンテン ツを識別してトラフィックを分類します。このため、カスタム アプリケーション定義では、単 純にポート番号を使用してアプリケーションを識別することができません。アプリケーション定 義には、トラフィック (送信元ゾーン、送信元 IP アドレス、宛先ゾーン、および宛先 IP アドレ スごとに制限されます) も含まれている必要があります。

アプリケーション オーバーライドを指定するカスタム アプリケーションを作成するには、以下 の手順を実行します。

- カスタムアプリケーションを作成する(アプリケーションの定義を参照)。アプリケーションの 使用目的がアプリケーションオーバーライドルールのみである場合、アプリケーションのシ グネチャを指定する必要はありません。
- カスタムアプリケーションの起動時に指定されるアプリケーションオーバーライドポリシーを定義します。通常ポリシーには、カスタムアプリケーションを実行しているサーバーのIPアドレスと、制限された送信元 IPアドレスのセットまたは送信元ゾーンが含まれています。

以下の表を使用して、アプリケーション オーバーライド ルールを設定します。

- アプリケーションオーバーライドの General (全般) タブ
- アプリケーションオーバーライドの Source (送信元) タブ
- アプリケーションオーバーライドの Destination (宛先) タブ
- アプリケーションオーバーライドの Protocol/Application (プロトコル/アプリケーション) タブ
- (Panorama のみ) Application Override Target Tab (アプリケーションオーバーライド宛先 タブ)

その他の情報をお探しですか?

「Use Application Objects in Policy(ポリシーでのアプリケーション オブジェクトの使用) ^{II}」 を参照してください。

アプリケーションオーバーライドの General (全般) タブ

General[全般] タブを使用して、アプリケーション オーバーライド ポリシーの名前と説明を設定 します。タグを設定すると、大量のポリシーがある場合に、ポリシーのソートやフィルタリング にも使用できます。

項目	の意味
氏名	ルールを識別する名前を入力します。名前の大文字と小文字は 区別され、文字、数字、スペース、ハイフン、およびアンダー スコアを含む最大 63 文字を指定できます。ルール名はファイ アウォールおよび Panorama 上で一意でなければなりません。 また、デバイス グループとその先祖または子孫デバイス グルー プ内でも一意でなければなりません。
の意味	ルールの説明を入力します (最大 1024 文字)。
タグ	ポリシーにタグを付ける場合、タグを Add (追加) して指定し ます。 ポリシー タグとは、ポリシーをソートまたはフィルタリングで きるキーワードや語句です。多数のポリシーを定義していて、 特定のキーワードでタグが付けられたポリシーを表示する場 合に役立ちます。たとえば、特定のセキュリティ ポリシーに DMZ へのインバウンドのタグを付けたり、復号ポリシーに「復 号」と「復号なし」というタグを付けたり、特定のデータ セ ンターに関するポリシーにその場所の名前を使用したりできま す。
タグに基づいてルールをグ ループ化	類似のポリシールールをグループ化するのに使用するタグを入 力します。グループタグを使用すれば、対象のタグに基づいて ポリシールール ベースを表示できます。Tag (タグ)に基づいて ルールをグループ化することを選択できます。

項目	の意味
監査コメント	ポリシールールの作成や編集を監査するために使用するコメン トを入力します。監査コメントの大文字と小文字は区別され、 文字、数字、スペース、ハイフン、およびアンダースコアを含 む最大 256 文字を指定できます。
監査コメント アーカイブ	ポリシールールの以前のAudit Comments (監査コメント)を表示 します。監査コメント アーカイブは CSV 形式でエクスポート できます。

アプリケーション オーバーライドの Source (送信元) タブ

Source[送信元]タブを使用して、送信元ゾーンまたは送信元アドレスを定義し、送信元から受信 するトラフィックにアプリケーション オーバーライド ポリシーを適用するように設定します。

項目	の意味
送信元ゾーン	送信元ゾーンを Add(追加)します(デフォルトは any(任意))。ゾーンは同じタイプ (Layer 2 [レイヤー 2]、Layer 3 [レイヤー 3]、virtual wire [バーチャル ワイ ヤー]) である必要があります。新しいゾーンを定義するに は、Network > Zones [ネットワーク > ゾーン] を参照し てください。
	複数のゾーンを使用して管理を簡略化できます。たとえ ば、信頼されていない宛先ゾーンが指定されている3つの 異なる内部ゾーン (マーケティング、販売、広報)がある場 合、すべてのケースを対象とした1つのルールを作成でき ます。
送信元アドレス	送信元アドレス、アドレス グループ、または地域を Add(追加)します(デフォルトは any(任意))。ド ロップダウンリストから選択するか、ドロップダウンリス トの下部にある Address[アドレス]、Adress Group[アドレ スグループ]、またはRegion[地域]をクリックして設定を行 います。
	Negate[上記以外]を選択すると、設定したアドレス以外の 任意のアドレスを指定したことになります。

アプリケーション オーバーライドの Destination (宛先) タブ

Destination (宛先)タブを使用して、宛先ゾーンまたは宛先アドレスを定義し、宛先へのトラフィックにポリシーを適用するように設定します。

項目	の意味
宛先ゾーン	Add[追加] をクリックして宛先ゾーンを選択します (デ フォルトは any)。ゾーンは同じタイプ (Layer 2 [レイヤー 2]、Layer 3 [レイヤー 3]、virtual wire [バーチャル ワイ ヤー]) である必要があります。新しいゾーンを定義するに は、Network > Zones [ネットワーク > ゾーン] を参照し てください。 複数のゾーンを使用して管理を簡略化できます。たとえ
	ば、信頼されていない宛先ゾーンが指定されている3つの 異なる内部ゾーン (マーケティング、販売、広報) がある場 合、すべてのケースを対象とした1つのルールを作成でき ます。
宛先アドレス	Add[追加] をクリックして宛先アドレス、アドレス グルー プ、または地域を追加します (デフォルトは any)。ドロッ プダウンリストから選択するか、ドロップダウンリストの 下部にある Address[アドレス]、Adress Group[アドレスグ ループ]、またはRegion[地域]をクリックして設定を行いま す。
	Negate[上記以外]を選択すると、設定したアドレス以外の 任意のアドレスを指定したことになります。

アプリケーション オーバーライドの Protocol/Application (プロ トコル/アプリケーション) タブ

Protocol/Application[プロトコル/アプリケーション] タブを使用して、プロトコル (TCPまたはUDP)、ポート、アプリケーションを定義して、ポリシーの一致条件にするアプリケーションの属性を詳細に指定できます。

項目	の意味
PROTOCOL	アプリケーション オーバーライドを許可するプロトコル(TCP ま たは UDP)を選択します。
ポート	指定した宛先アドレスのポート番号 (0 ~ 65535) またはポート番号 の範囲 (ポート 1 ~ ポート 2) を入力します。複数のポートまたは ポートの範囲はコンマで区切ります。
Application [アプリ ケーション]	前述のルール基準に一致するトラフィックフローのオーバーライド アプリケーションを選択します。カスタムアプリケーションをオー バーライドするときに実行される脅威検査はありません。この例外 は、脅威検査をサポートする事前に定義されたアプリケーションに オーバーライドする場合です。

項目 の意味 新しいアプリケーションを定義する方法については、 「Objects(オブジェクト) > Applications(アプリケーション)」 を参照してください。

Application Override Target Tab(アプリケーション オーバーラ イド宛先タブ)

 (Panorama のみ) Policies (ポリシー) > Application Override (アプリケーションオーバーラ イド) > Target (宛先)

[Target(宛先)]タブを選択して、ポリシー ルールをプッシュするデバイス グループ内の管理対象ファイアウォールを選択します。管理対象ファイアウォールを選択するか、タグを指定することにより、プッシュ先の管理対象ファイアウォールを指定することができます。さらに、指定済ファイアウォールを除き、すべての管理対象ファイアウォールにプッシュするポリシー ルールの宛先を設定することができます。

NAT ルール - 宛 先設定	の意味
任意 (すべての 対象デバイス)	ポリシー ルールをデバイス グループのすべての管理対象ファイアウォール にプッシュするには、有効化(チェックをオン)にします。
機器	ポリシー ルールをプッシュするデバイス グループに関連付けられた1つま たは複数の管理対象ファイアウォールを選択します。
tags	指定したタグを持つデバイス グループ内の管理対象ファイアウォールにポ リシー ルールをプッシュするには、1つまたは複数のタグをAdd(追加)し ます。
これらの指定さ れたデバイスと タグのみをター ゲットに設定す る	選択したデバイスとタグを除き、デバイス グループに関連付けられてい るすべての管理対象ファイアウォールにポリシー ルールをプッシュするに は、有効化(チェックをオンに)します。

Policies (ポリシー) > Authentication (認証)

認証ポリシーを使用すると、エンド ユーザーがネットワーク リソースにアクセスする前に、エ ンドユーザーの認証を行うことができます。

知りたい内容	以下を参照
認証ルールを作成する際に使 用可能なフィールドは?	認証ポリシー ルールの構成要素
Web インターフェイスを使用	認証ポリシーの作成と管理
して認証ポリシーを管理する	Panorama については、「ポリシールールの移動またはコ
には?	ピー」を参照してください。
その他の情報をお探しです	認証ポリ
か?	シーロ

認証ポリシー ルールの構成要素

ユーザーがリソースを要求したとき(たとえば、Web ページへのアクセス時)、ファイア ウォールが必ず認証ポリシーを評価します。一致するポリシー ルールに基づいて、ファイア ウォールは、ログインとパスワード、音声、SMS、プッシュ、またはワンタイム パスワード (OTP)認証のように、異なる要素(タイプ)のチャレンジに対応するようにユーザーに求めま す。ユーザーがすべての要素に対応すると、ファイアウォールはセキュリティ ポリシーを評価 して(「Policies(ポリシー) > Security(セキュリティ)」を参照)、リソースへのアクセスを 許可するかどうかを判断します。

A

ユーザーが Web ベースでないリソース(プリンタなど)に内部またはトンネル モードの GlobalProtect[™] ゲートウェイ ■経由でアクセスする場合、ファイアウォー ルは認証を求めません。代わりに、接続エラーメッセージが表示されます。これ らのリソースにユーザーがアクセスできるようにするには、認証ポータルをセッ トアップして、接続エラーが表示された場合はポータルにアクセスするようにユー ザーに伝えてください。認証ポータルのセットアップについては、御社の IT 部門に 相談してください。

以下の表で、認証ポリシールールの構成要素について説明します。ルールを追加する前に、 「認証ポリシーの作成と管理」に記載されている必要条件を満たしてください。

認証ルールの 構成要素	設定場所	の意味
ルール番号	該当なし	各ルールは自動的に付番され、ルールを移動する と順番も変更されます。特定のフィルタに一致す るルールをフィルタリングすると、 Policies (ポ

認証ルールの 構成要素	設定場所	の意味	
		リシー) > Authentication(認証)ページに、 各ルールと、ルールベースのルール全体の中 で番号が振られ、評価順における順番が一覧 表示されます。詳細は、ルールの並びと評価 順 ¹ 説明を参照してください。	・
氏名	一般	ルールを識別する名前を入力します。名前の大文 字と小文字は区別され、文字、数字、スペース、 ハイフン、およびアンダースコアを含む最大 63 文字を指定できます。ルール名はファイアウォー ルおよび Panorama 上で一意でなければなりませ ん。また、デバイス グループとその先祖または子 孫デバイス グループ内でも一意でなければなりま せん。	
の意味		ルールの説明を入力します (最大 1024 文字)。	-
タグ	_	ルールのソートおよびフィルタリングのためのタ グを選択します(「Objects(オブジェクト) > Tags(タグ)」を参照)。	_
タグに基づい てルールをグ ループ化		類似のポリシールールをグループ化するのに使用 するタグを入力します。グループタグを使用すれ ば、対象のタグに基づいてポリシールール ベース を表示できます。 Tag (タグ) に基づいてルールをグ ループ化することができます。	
監査コメント		ポリシールールの作成や編集を監査するために使 用するコメントを入力します。監査コメントの大 文字と小文字は区別され、文字、数字、スペー ス、ハイフン、およびアンダースコアを含む最大 256 文字を指定できます。	_
監査コメント アーカイブ		ポリシールールの以前のAudit Comments (監査コ メント)を表示します。監査コメント アーカイブ は CSV 形式でエクスポートできます。	-
Web プロキ シ認証をバイ パス		このオプションを選択すると、このポリシールー ルに一致するトラフィックが Web プロキシ認証 トラフィックをバイパスできるようになります。	-

認証ルールの 構成要素	設定場所	の意味
		このオプションを選択する場合、信頼できるデバイスの送信元 IPアドレスを含む アドレスオブジェクト、信頼できるデバイスの宛先 IP アドレスを含むカスタム URL カテゴリ、またはその両方を選択する必要があります。
Source Zone	送信元	ゾーンを Add (追加) して、指定したゾーンのイ ンターフェイスからのトラフィックにのみルール を適用します(デフォルトは any(任意))。 新しいゾーンを定義する手順については、 「Network(ネットワーク) > Zones(ゾー ン)」を参照してください。
送信元アドレス		アドレスまたはアドレス グループを Add (追 加) して、指定した送信元から発生したトラ フィックにのみルールを適用します(デフォルト は any (任意))。 Negate (上記以外) を選択すると、指定したアド レス以外の任意のアドレスを指定したことになり ます。 新しいアドレスやアドレス グループを定義する 手順については、「Objects (オブジェクト) > Addresses (アドレス)」、および「Objects (オ ブジェクト) > Address Groups (アドレス グルー プ)」を参照してください。
送信元ユーザー	感染	 ルールを適用する送信元ユーザーまたはユーザー グループを選択します。 any(任意) – 送信元ユーザーに関係なく任意 のトラフィックが含まれます。 pre-logon(ログオン前) – ユーザーは クライアントシステムにログインして いないが、ユーザーのクライアントシ ステムは GlobalProtect の pre-logon 機 能 ネットワークに接続している状態のリモート ユーザーが含まれます。 known-user(既知のユーザー) – ルールに よって認証が呼び出される以前に、ファイア

で

認証ルールの 構成要素	設定場所	の意味
		 ウォールで IP アドレスとユーザー名のマッピングが完了しているすべてのユーザーが含まれます。 unknown (未知) - ファイアウォールで IP アドレスとユーザー名のマッピングが行われていないすべてのユーザー名のマッピングが行われていないすべてのユーザーの含まれます。ルールによって認証が呼び出された後、ユーザーが入力したユーザー名に基づいて、ファイアウォールは未知のユーザーのユーザーマッピングを作成します。 Select (対象指定) - Source User (送信元ユーザー) リストに Add (追加) したユーザー およびユーザーグループのみが含まれます。 アァイアウォールが User- ID[™] エージェントではなく、RADIUS、TACACS+、またはSAML アイデンティティプロバイダサーバーからユーザー情報を収集している場合、ユーザー同刊を収集している場合、ユーザー同報を手動で入力する必要があります。
送信元 HIP プ ロファイル		ホスト情報プロファイル (HIP) をAdd (追加) する と、最新のセキュリティ パッチやアンチウイルス 定義があるかなどのエンド ホストのセキュリティ 状態に関する情報を収集できます。詳細や新しい HIP を定義する手順については、「Objects(オブ ジェクト) > GlobalProtect > HIP Profiles(HIP プ ロファイル)」を参照してください。
Destination Zone	宛先	ゾーンを Add (追加) して、指定したゾーン のインターフェイスに向かうトラフィックにの みルールを適用します(デフォルトは any(任 意))。新しいゾーンを定義する手順について は、「Network(ネットワーク) > Zones(ゾー ン)」を参照してください。
宛先アドレス		アドレスまたはアドレス グループを Add(追 加)して、指定した宛先にのみルールを適用しま す(デフォルトは any(任意))。

認証ルールの 構成要素	設定場所	の意味
		Negate(上記以外)を選択すると、指定したアドレス以外の任意のアドレスを指定したことになります。
		新しいアドレスやアドレス グループを定義する 手順については、「Objects(オブジェクト) > Addresses(アドレス)」、および「Objects(オ ブジェクト) > Address Groups(アドレス グルー プ)」を参照してください。
サービス	サービス/URL カテゴリ	以下のオプションを選択して、特定の TCP および UDP ポート番号のサービスにのみルールを適用し ます。
		 any(任意) – すべてのポート、およびプロト コルのサービスを指定します。
		 default(デフォルト) – Palo Alto Networks が定義するデフォルト ポートのサービスのみ を指定します。
		 Select (対象指定) – サービスまたはサービ ス グループを Add (追加) できるようにし ます。新しいサービスやサービス グループ を作成する手順については、「Objects (オ ブジェクト) > Services (サービス)」、 および「Objects (オブジェクト) > Service Groups (サービス グループ)」を参照してく ださい。
		 デフォルトではservice-httpが選択されています。Authentication Portal(認証ポータル)用に認証ポリシーを使用する場合はservice-httpsも有効化し、ファイアウォールがすべてのWebトラフィックについてユーザー対IPアドレスのマッピングを必ず学習するようにしてください。
URL カテゴリ		ルールを適用する URL カテゴリを選択します。
		 URL カテゴリに関係なくすべてのトラフィック を指定するには、any(任意)を選択します。
		 カテゴリを Add(追加)します。カスタ ムカテゴリを定義する手順については、 「Objects(オブジェクト) > Custom

構成要素	叹心吻ற	の意味
		Objects(カスタム オブジェクト) > URL Category(URL カテゴリ)」を参照してくださ い。
認証の実施	操作	ファイアウォールがユーザーを認証するために 使用する方式(Authentication Portal(認証ポー タル)またはブラウザチャレンジなど)と認 証プロファイルを指定するための認証の実施オ ブジェクトを選択します(Objects(オブジェ クト) > Authentication(認証))。認証プロ ファイルは、ユーザーが1つのチャレンジに 対応するか、多要素認証に対応するかを定義し ます(「Device(デバイス) > Authentication Profile(認証プロファイル)」を参照)。事前定 義済みか、カスタムの認証の実施オブジェクトを 選択できます。
		 ホストやサーバーを Authentication Portal (認証ポータル) ポリシーか ら除外しざるをえない場合は、no- captive-portalをAuthentication Enforcement (認証の適用)として指 定している認証プロファイルにそ れらを追加します。ただし、ファ イアウォールがユーザー対 IP アド レスのマッピングを学習する際は Authentication Portal (認証ポータ ル) ポリシーが役立つため、可能な 限りそれを使用してください。
タイムアウト		ユーザーがリソースに繰り返しアクセスする場合 に、ファイアウォールが1回だけユーザーに認証 を求める間隔を分単位で指定すると(デフォルト は 60)、ユーザーのワークフローの妨げとなる認 証チャレンジの頻度を減らすことができます。 Authentication Enforcement(認証の実施) オブジェクトで多要素認証を指定する場合、 ユーザーは各要素につき認証を1回行う必要 があります。ファイアウォールはタイムスタ ンプを記録して、要素の有効期限のタイムア ウト時にのみ、チャレンジを再発行します。 タイレスタンプを他のファイアウォールに更明

す

認証ルールの 構成要素	設定場所	の意味
		ると、最初にユーザーにアクセスを許可するファ イアウォールと、後にそのユーザーのアクセスを 制御するファイアウォールが異なる場合も、タイ ムアウトを適用できます。
		 Timeout (タイムアウト)は、強固なセキュリティ(認証のプロンプトを表示する間隔が短い)とユーザーエクスペリエンス(認証のプロンプトを表示する間隔が長い)の間のトレードオフになります。データセンターなどの重要なシステムやセンシティブな領域へのアクセスが対象である場合、できるだけ頻繁に認証を行うのが最適な選択になるでしょう。ネットワークの境界やユーザーエクスペリエンスが重要なビジネスの場合は、認証の頻度を減らすことが最適な選択になるでしょう。
ログ認証タイ ムアウト		認証要素に関連付けられているタイムアウトが期 限切れになるたびに、ファイアウォールで認証ロ グを生成する場合は、このオプションを選択し ます(デフォルトでは無効)。このオプション を有効にすると、アクセス問題のトラブルシュー ティングに利用できるデータが増えます。相関オ ブジェクトとともに認証ログを使用して、ネット ワーク上の不審なアクティビティを特定できます (総当たり攻撃など)。 このオプションを有効にするとログ トラフィックが増えます。

認証ルールの 構成要素	設定場所	の意味
ログ転送		ファイアウォールから Panorama または Syslog サーバーのような外部サービスに認証ログを 転送する場合は、ログ転送プロファイルを選 択します(「Objects(オブジェクト) > Log Forwarding(ログ転送)」を参照)。
任意 (すべて の対象デバイ ス) Panorama の み	ターゲット	ポリシー ルールをデバイス グループのすべての管 理対象ファイアウォールにプッシュするには、有 効化(チェックをオン)にします。
デバイス Panorama の み		ポリシー ルールをプッシュするデバイス グループ に関連付けられた1つまたは複数の管理対象ファ イアウォールを選択します。
tags Panorama の み		指定したタグを持つデバイス グループ内の管理対 象ファイアウォールにポリシー ルールをプッシュ するには、1つまたは複数のタグをAdd(追加)し ます。
これらの指定 されたデバイ スとタグのみ をターゲット に設定する		選択したデバイスとタグを除き、デバイス グルー プに関連付けられているすべての管理対象ファイ アウォールにポリシー ルールをプッシュするに は、有効化(チェックをオンに)します。
Panorama の み		

認証ポリシーの作成と管理

認証ポリシー ルールの作成と管理を行うには、Policies(ポリシー) > Authentication (認証) ページを選択します。

タスク	の意味
コンテキスト の	次の前提事項を実行してから、認証ポリシー ルールを作成してください。 □ User-ID [™] Authentication Portal (User-ID [™] 認証ポータル設定を行 います (Device (デバイス) > User Identification (ユーザーID) > Authentication Portal Settings (認証ポータル設定)参照)。ファイ

タスク	の意味
	アウォールでは Authentication Portal(認証ポータル)が使用され て、認証ルールによって要求される、最初の認証要素が表示されま す。Authentication Portal(認証ポータル)では、ファイアウォールは認 証 Timeout(タイムアウト)期間に関連付けられたタイム スタンプを記録 し、ユーザーマッピングを更新することもできます。
	 ファイアウォールがユーザー認証を行うサービスにアクセスする方法を 指定するサーバープロファイルを設定します(「Device(デバイス)> Server Profiles(サーバープロファイル)」を参照)。
	 認証設定を指定する認証プロファイルにサーバープロファイルを割り当てます(「Device(デバイス) > Authentication Profile(認証プロファイル)」を参照)。
	 認証方法を指定する認証実施オブジェクトに認証プロファイルを割り当て ます(「Objects(オブジェクト) > Authentication(認証)」を参照)。
	ルールを作成するには、次のいずれかのステップを実行してから、「認証ポ リシー ルールの構成要素」で説明するフィールドに情報を入力します。
	• [追加] をクリックします。
	 新しいルールのベースになるルールを選択し、Clone Rule(ルールの コピー)をクリックします。ファイアウォールは、コピーしたルール <rulename>#を選択したルールの下に挿入します。#は、ルール名を一意 にする次に使用可能な整数で、複製されたルールの新しい UUID を生成し ます。詳細は、「ポリシー ルールの移動またはコピー」を参照してくださ い。</rulename>
変更	ルールを変更するには、ルール名をクリックし、「認証ポリシー ルールの構 成要素」で説明するフィールドを編集します。
	⑦ ファイアウォールがルールを Panorama から受信すると、ルー ルは読み取り専用になります。ルールは Panorama のみで編集 可能です。
移動	ファイアウォールでは、トラフィックが照合されるとき、ルールが Policies(ポリシー) > Authentication(認証)ページでリストされてい る順序で上から下に評価されます。評価順序を変更するには、ルールを選 択して、Move Up(上へ)、Move Down(下へ)、Move Top(最上部 へ)、Move Bottom(最下部へ)のうちいずれかを選択します。詳細は、 「ポリシー ルールの移動またはコピー」を参照してください。
Delete(削 除)	既存のルールを削除するには、ルールを選択して Delete(削除)を選択します。

タスク	の意味
有効化/無効 化	ルールを無効化するには、ルールを選択して Disable (無効化)を選択しま す。無効化したルールを再び有効化するには、ルールを選択して Enable (有 効化)を選択します。
使用されてい ないルールの 強調表示	ファイアウォールの前回再起動時から、トラフィックを照合していないルー ルを特定する場合は、 Highlight Unused Rules (未使用のルールをハイライト 表示)を選択します。ハイライト表示すると、使用されていないルールを無 効化するのか削除するのかを判断できるようになります。このページでは、 使用されていないルールは黄色い網掛けでハイライト表示されます。
ルールの プレビュー (Panoramaの み)	Preview Rules(ルールのプレビュー)をクリックして、ルールを管理対象 ファイアウォールにプッシュする前にルールのリストを表示することができ ます。このページでは、各ルールベース内で、デバイス グループ(および管 理対象ファイアウォール)ごとにルール階層が視覚的に区別されており、多 くのルールに目を通しやすくなっています。

Policies > DoS Protection [ポリシー > DoS プロテク ション]

DoS プロテクション ポリシーを使用すると、送信元インターフェイス、ゾーン、アドレス、 ユーザーや、宛先インターフェイス、ゾーン、ユーザーに一致するパケットの拒否または許可を 指定して、個々の重要なリソースを DoS 攻撃から守ることができます。

また、保護アクションを選択し、DoS プロファイルを指定できます。プロファイルにはしきい 値(1秒あたりのセッションまたはパケット数)を設定して、アラームのトリガーや保護アク ションのアクティベートを適用したり、割合の上限を指定してそれを超えた場合にすべての新 しい接続をドロップしたりできます。これにより、インターフェイス、ゾーン、アドレス、国の セッション数を、セッション総数、送信元 IP アドレスおよび宛先 IP アドレスに基づいて制御で きます。たとえば、特定のアドレスまたはアドレス グループと送受信されるトラフィック、特 定のユーザーから受信するトラフィック、特定のサービスに使用するトラフィックを制御できま す。

ファイアウォールが DoS プロテクション ポリシー ルールを実施した後、ファイアウォールが最 も効率的な方法でリソースを使用することをセキュリティ ポリシー ルールが確認します。DoS プロテクション ポリシー ルールがパケットを拒否した場合、そのパケットがセキュリティ ポリ シー ルールに到達することはありません。

以下の表では、DoS プロテクション ポリシー設定について記載しています。

- DoS プロテクションの General (全般) タブ
- DoS プロテクションの Source (送信元) タブ
- DoS プロテクションの Destination (宛先) タブ
- DoS プロテクションの Option/Protection(オプション/防御)タブ
- (Panorama のみ) DoS Protection Target Tab [DoS プロテクション宛先タブ]

その他の情報をお探しですか?

「DoS Protection Profiles(DoS プロテクション プロファイル) ^{II}、および「Objects(オブ ジェクト) > Security Profiles(セキュリティ プロファイル) > DoS Protection(DoS プロテク ション)」を参照してください。

DoS プロテクションの General (全般) タブ

• ポリシー > DoS プロテクション > 一般

General (全般) タブを選択して、DoS プロテクション ポリシーの名前と説明を設定します。タ グを設定すると、大量のポリシーがある場合に、ポリシーのソートやフィルタリングを行うこと もできます。

項目	の意味
氏名	DoS プロテクション ポリシー ルールを識別する名前を入力します。名前の 大文字と小文字は区別され、文字、数字、スペース、ハイフン、およびアン

項目	の意味
	ダースコアを含む最大 63 文字を指定できます。ルール名はファイアウォー ルおよび Panorama 上で一意でなければなりません。また、デバイス グルー プとその先祖または子孫デバイス グループ内でも一意でなければなりませ ん。
の意味	ルールの説明を入力します (最大 1024 文字)。
tags	ポリシーにタグを付ける場合、タグを Add(追加)して指定します。
	ポリシー タグとは、ポリシーをソートまたはフィルタリングできるキーワー ドや語句です。タグは、多数のポリシーを定義していて、特定のキーワード でタグが付けられたポリシーを表示する場合に役立ちます。たとえば、特定 のセキュリティ ポリシーに DMZ へのインバウンドのタグを付けたり、復号 ポリシーに「復号」や「復号なし」というタグを付けたり、特定のデータ セ ンターに関するポリシーにその場所の名前を使用したりできます。
タグに基づい てルールをグ ループ化	類似のポリシールールをグループ化するのに使用するタグを入力します。グ ループタグを使用すれば、対象のタグに基づいてポリシールール ベースを表 示できます。Tag (タグ)に基づいてルールをグループ化することができます。
監査コメント	ポリシールールの作成や編集を監査するために使用するコメントを入力しま す。監査コメントの大文字と小文字は区別され、文字、数字、スペース、ハ イフン、およびアンダースコアを含む最大 256 文字を指定できます。
監査コメント アーカイブ	ポリシールールの以前のAudit Comments (監査コメント)を表示します。監査 コメント アーカイブは CSV 形式でエクスポートできます。

DoS プロテクションの Source (送信元) タブ

Source(送信元)タブを選択して、送信元インターフェイスまたは送信元ゾーン、および必要 に応じて送信元アドレスと送信元ユーザーを定義し、受信トラフィックに DoS ポリシー ルール を適用するように設定します。

項目	の意味
タイプ	DoS プロテクション ポリシー ルールを適用する送信元のタイプを選択します。
	 Interface(インターフェイス) – 指定されたインターフェイスまたはインターフェイス グループから送信されるトラフィックにルールを適用します。
	 Zone (ゾーン) – 指定されたゾーンのインターフェイスから送信される トラフィックにルールを適用します。

項目	の意味
	Add(追加)をクリックして、複数のインターフェイスまたはゾーンを選択 します。
送信元アドレ ス	Any (すべて)または Add(追加)を選択し、DoS プロテクション ポリシー ルールを適用する 1 つ以上の送信元アドレスを指定します。
	(任意)指定したアドレス以外の任意のアドレスにルールを適用するに は、Negate(上記以外)を選択します。
Source User (送信元ユー	DoS プロテクション ポリシー ルールを適用する 1 つ以上の送信元ユーザー を指定します。
ザー)	• any(すべて) – 送信元ユーザーに関係なくパケットが含まれます。
	 pre-logon(ログイン前) – GlobalProtect を使用してネットワークに接続しており、自分のシステムへのログインはしていないリモート ユーザーからのパケットが含まれます。GlobalProtect アプリのポータルにpre-logon(ログオン前)が設定されている場合、自分のマシンに現在ログインしていないユーザーは、ユーザー名 pre-logon として識別されます。pre-logon ユーザー用のポリシーを作成できるのに加えて、ユーザーが直接ログインしていなくても、ユーザーのマシンは完全にログインしているかのようにドメインで認証されます。
	 known-user(既知のユーザー) – 認証されたすべてのユーザー(ユー ザー データがマッピングされた IP アドレス)が含まれます。このオプ ションは、ドメインの「ドメイン ユーザー」グループに相当します。
	 unknown[未知] – 認証されていないすべてのユーザー (ユーザーにマップ されていない IP アドレス) が含まれます。たとえば、unknown (未知) は ゲスト レベルのアクセスに使用できます。これらのユーザーは、ネット ワーク上の IP アドレスを持っていますが、ドメインに認証されず、ファ イアウォール上に IP アドレス対ユーザー名のマッピング情報がないため です。
	 Select(選択) – このウィンドウで指定したユーザーが含まれます。たと えば、1人のユーザー、個々のユーザーのリスト、あるいはグループを選 択したり、手動でユーザーを追加したりできます。
	● ファイアウォールが User-ID [™] エージェントではな く、RADIUS、TACACS+、または SAML アイデンティティプロ バイダ サーバーからユーザー情報を収集している場合、ユー ザーのリストは表示されません。ユーザー情報を手動で入力す る必要があります。

DoS プロテクションの Destination (宛先) タブ

Destination(宛先)タブを選択して、宛先ゾーンまたは宛先インターフェイスおよび宛先アドレスを定義し、宛先へのトラフィックにポリシーを適用するように設定します。

項目	の意味
タイプ	DoS プロテクション ポリシー ルールを適用する宛先のタイプを選択します。
	 Interface (インターフェイス) – 指定されたインターフェイスまたは インターフェイス グループに送信されるパケットにルールを適用しま す。Add (追加)をクリックして、1つ以上のインターフェイスを選択し ます。
	 Zone (ゾーン) – 指定されたゾーンのインターフェイスに送信されるパケットにルールを適用します。Add(追加)をクリックして、1つ以上のゾーンを選択します。
宛先アドレス	Any (すべて)または Add(追加)を選択し、DoS プロテクション ポリシー ルールを適用する 1 つ以上の宛先アドレスを指定します。
	(任意)指定したアドレス以外の任意のアドレスにルールを適用するに は、Negate(上記以外)を選択します。

DoS プロテクションの Option/Protection(オプション/防御)タブ

Option/Protection(オプション/防御)タブを選択して、DoS プロテクション ポリシー ルール のオプションを設定します。たとえば、ルールを適用するサービスのタイプ、ルールに一致する パケットに対して実行するアクション、一致するトラフィックのログ転送をトリガーするかどう かなどを設定できます。ルールがアクティブになるスケジュールを定義できます。

また、しきい値レートを決定する aggregate(集約)DoS プロテクション プロファイルや classified(分類)DoS プロテクション プロファイルを選択することもできます。このしきい値 レートを超えると、ファイアウォールはアラームのトリガーなどの防御アクションを実行した り、ランダム早期ドロップなどのアクションをアクティベーションしたり、しきい値レートの上 限を超えるパケットをドロップしたりします。

項目	の意味
サービス	Add(追加)をクリックし、DoS プロテクション ポリシーを適用する 1 つ以 上のサービスを選択します。デフォルトは Any(すべて)のサービスです。 例えば、DoS ポリシーが Web サーバーを保護する場合、HTTP、HTTPS、そ の他の Web アプリケーション用の適切なサービス ポートを指定します。

項目	の意味
	重要なサーバーの場合は DoS 保護ルールを別途作成し、目標を 定めた攻撃を防ぐために使用していないサービス ポートを保護 します。
操作	DoS プロテクション ポリシー ルールに一致するパケットに対してファイア ウォールが実行するアクションを選択します。
	• Deny(拒否) – ルールに一致するすべてのパケットをドロップします。
	• Allow(許可) – ルールに一致するすべてのパケットを許可します。
	 Protect (保護)-指定した DoS 保護プロファイルで指定されている保護を ルールにマッチするパケットに適用します。ルールに一致するパケット は、DoS プロテクション プロファイルのしきい値レートに対してカウン トされ、最大レートを超えたときにアラームのトリガー、別のアクション のアクティベーション、パケット ドロップのトリガーが行われます。
	DoS 保護を適用する目的は DoS 攻撃を防ぐことであるため、基本的にProtect (保護)を使用する必要があります。Deny (拒否)は DoS トラフィックと共に正当なトラフィックをドロップし、またAllow (許可)は DoS 攻撃を防ぐことができません。グループ内で例外を設ける場合のみ、Deny (拒否)やAllow (許可)を使用するようにしてください。例えば、グループの大抵のメンバーから来るトラフィックを拒否しつつそのトラフィックの一部だけを許可したり、グループの大抵のメンバーから来るトラフィックを拒否しことができます。
スケジュール	DoS プロテクション ポリシー ルールが適用されるスケジュールを指定しま す。デフォルト設定の None(なし)はスケジュールがないことを示し、ポ リシーは常に適用されます。
	または、スケジュールを選択したり、新しいスケジュールを作成したりし て、DoS プロテクション ポリシー ルールが適用されるタイミングを制御 します。スケジュールの Name(名前)を入力します。マルチ仮想システ ム ファイアウォールの各仮想システムでこのスケジュールを共有するに は、Shared(共有)を選択します。Recurrence(繰り返し)に Daily(毎 日)、Weekly(毎週)、または Non-recurring(1 回限り)を選択しま す。Start Time(開始時間)と End Time(終了時間)を 24 時間ベースの 「時:分」の形式で追加します。
ログ転送	一致するトラフィックの脅威ログ エントリの外部サービス(Syslog サー バー、Panorama など)への転送をトリガーする場合、ログ転送プロファイ ルを選択するか、Profile(プロファイル)をクリックして新しいプロファイ ルを作成します。

項目	の意味
	 ファイアウォールはルール内のアクションにマッチするトラ フィックについてのみ、ログを記録してトラフィックを転送します。
	管理を簡単にするために、DoS ログを他の脅威ログと分けて、管理者(メールで)およびログサーバーの両方に直接転送します。
集約 (Aggregate)	集約 DoS 保護プロファイルは、DoS 保護ルールで指定されたデバイスの複合 グループに適用されるしきい値を設定してそれらのサーバーグループを保護 します。例えば、Alarm Rate (アラーム レート) のしきい値を 10,000 CPS に すると、グループ全体に向かう新しい CPS の合計が 10,000 CPS を超えるに ファイアウォールがアラーム メッセージを発動させます。
	しきい値レートを指定する Aggregate(集約)DoS プロテクション プロファ イルを選択します。このしきい値レートに基づいて、受信接続/秒によるア ラームのトリガー、アクションのアクティベーション、最大レートの超過が 発生します。すべての受信接続(集約)が、Aggregate(集約)DoS プロテ クション プロファイルで指定されたしきい値に対してカウントされます。
	Aggregate(集約)プロファイル設定が None(なし)の場合、集約ト ラフィックのしきい値設定がないことを意味します。「Objects(オブ ジェクト) > Security Profiles(セキュリティ プロファイル) > DoS Protection(DoS プロテクション)」を参照してください。
分類化 (Classified)	分類化 DoS 保護プロファイルは、DoS 保護ルールで指定された個々のデバイ スに適用されるしきい値を設定して個々の、あるいは小規模なグループの重 要なサーバーを保護します。例えば、Alarm Rate (アラーム レート)のしきい 値を 10,000 CPS にすると、ルールで指定された個々のいずれかのサーバー に向かう新しい CPS の合計が 10,000 CPS を超えるにファイアウォールがア ラーム メッセージを発動させます。
	このオプションを選択し、以下を指定します。
	 Profile(プロファイル) – このルールに適用する Classified(分類) DoS プロテクション プロファイルを選択します。
	 Address(アドレス) – source-ip-only(送信元 IP のみ)、destination- ip-only(宛先 IP のみ)、src-dest-ip-both(送信元 IP と宛先 IP の両方) のうち、どれに一致したときに受信接続がプロファイルのしきい値に対し てカウントされるのかを指定します。
	src-dest-ip-bothカウンターを追跡する場合、ファイアウォー ルは送信元 IP あるいは宛先 IP カウンターだけを追跡する場 合よりも多くのリソースを消費します。
	Classified(分類)DoS プロテクション プロファイルを指定した場合、送信 元 IP アドレス、宛先 IP アドレス、または送信元 IP アドレスと宛先 IP アド

項目	の意味
	レスのペアに一致する受信接続のみが、プロファイルで指定したしきい値に 対してカウントされます。たとえば、Max Rate(最大レート)が 100 cps で ある Classified(分類)DoS プロテクション プロファイルを指定し、ルール の Address(アドレス)設定に source-ip-only(送信元 IP のみ)を指定でき ます。この特定の送信元 IP アドレスの接続が 1 秒あたり 100 に制限されま す。
	 ファイアウォールがすべての IP アドレスの候補のカウンター を保存することはできないため、インターネットに接続された ゾーン用にsource-ip-onlyやsrc-dest-ip-bothを使用しないでくだ さい。境界のゾーンではdestination-ip-onlyを使用します。
	個々の重要なデバイスを保護する場合はdestination-ip-onlyを使 用します。
	インターネットに接続されていないゾーンで疑わしいホストを 監視する場合は source-ip-only および Alarm (アラーム) しきい値を 使用します。
	「Objects(オブジェクト) > Security Profiles(セキュリティ プロファイ ル) > DoS Protection(DoS プロテクション)」を参照してください。

DoS Protection Target Tab [DoS プロテクション宛先タブ]

• (Panorama のみ) Policies (ポリシー) > DoS Protection (DoS プロテクション) > Target (宛先)

[Target(宛先)]タブを選択して、ポリシー ルールをプッシュするデバイス グループ内の管理対 象ファイアウォールを選択します。管理対象ファイアウォールを選択するか、タグを指定するこ とにより、プッシュ先の管理対象ファイアウォールを指定することができます。さらに、指定済 ファイアウォールを除き、すべての管理対象ファイアウォールにプッシュするポリシー ルール の宛先を設定することができます。

NAT ルール - 宛 先設定	の意味
任意 (すべての 対象デバイス)	ポリシー ルールをデバイス グループのすべての管理対象ファイアウォール にプッシュするには、有効化(チェックをオン)にします。
機器	ポリシー ルールをプッシュするデバイス グループに関連付けられた1つま たは複数の管理対象ファイアウォールを選択します。

NAT ルール - 宛 先設定	の意味
tags	指定したタグを持つデバイス グループ内の管理対象ファイアウォールにポ リシー ルールをプッシュするには、1つまたは複数のタグをAdd(追加)し ます。
これらの指定さ れたデバイスと タグのみをター ゲットに設定す る	選択したデバイスとタグを除き、デバイス グループに関連付けられてい るすべての管理対象ファイアウォールにポリシー ルールをプッシュするに は、有効化(チェックをオンに)します。

Policies > SD-WAN [ポリシー > SD-WAN]

SD-WAN ポリシーを追加し、設定したヘルスジッター、遅延、およびパケット損失のヘルス メトリックに基づき、アプリケーション毎、または同じリンクを通過するアプリケーション グループのリンク パス管理設定を設定します。重要なアプリケーションの送信元と宛先間の 特定のパスで質の低下が発生した場合、SD-WAN ポリシールールは新しい最適なパスを選択 し、SD-WAN ポリシールールで割り当てられたパス品質プロファイルに従って機密性の高い重 要なアプリケーションが確実に実行されるようにします。

- SD-WAN General (全般) タブ
- Source (送信元) タブ
- Destination (宛先) タブ
- SD-WAN Application/Service (アプリケーション/サービス) タブ
- SD-WAN Path Selection (パス選択) タブ
- (Panorama のみ) SD-WAN Target (ターゲット) タブ

SD-WAN General (全般) タブ

• ポリシー > **SD-WAN** > 一般

General (全般) タブを選択し、SD-WAN ポリシーの名前と説明を設定します。タグを設定する と、大量のポリシーがある場合に、ポリシーのソートやフィルタリングにも使用できます。

項目	の意味
氏名	ルールを識別する名前を入力します。名前の大文字と小文字は 区別され、文字、数字、スペース、ハイフン、およびアンダー スコアを含む最大 63 文字を指定できます。ルール名はファイ アウォールおよび Panorama 上で一意でなければなりません。 また、デバイス グループとその先祖または子孫デバイス グルー プ内でも一意でなければなりません。
の意味	ルールの説明を入力します (最大 1024 文字)。
タグ	ポリシーにタグを付ける場合、タグを Add(追加)して指定し ます。 ポリシー タグとは、ポリシーをソートまたはフィルタリングで きるキーワードや語句です。多数のポリシーを定義していて、 特定のキーワードでタグが付けられたポリシーを表示する場合 に役立ちます。例えば、特定の SD-WAN ポリシーに、ルール が適用される特定のハブまたはブランチを特定する一意のタグ でタグ付けしたい場合。

項目	の意味
タグに基づいてルールをグ ループ化	類似のポリシールールをグループ化するのに使用するタグを入 力します。グループタグを使用すれば、対象のタグに基づいて ポリシールール ベースを表示できます。 Tag (タグ) に基づいて ルールをグループ化することを選択できます。
監査コメント	ポリシールールの作成や編集を監査するために使用するコメン トを入力します。監査コメントの大文字と小文字は区別され、 文字、数字、スペース、ハイフン、およびアンダースコアを含 む最大 256 文字を指定できます。
監査コメント アーカイブ	ポリシールールの以前のAudit Comments (監査コメント)を表示 します。監査コメント アーカイブは CSV 形式でエクスポート できます。

Source (送信元) タブ

• ポリシー > **SD-WAN** > 送信元

Source (送信元) タブを選択して、SD-WAN ポリシーが適用される着信パケットを定義する送信 元ゾーン、送信元アドレス、および送信元ユーザーを定義します。

項目	の意味
送信元ゾーン	送信元ゾーンを指定するには Add (追加) を選択して 1 つ以上のゾー ンを選択するか Any (任意) ゾーンを選択します。
	 複数のゾーンを指定して管理を簡略化できます。たとえば、異なる ゾーンに3つのブランチがあり、残りの一致条件とパス選択を3つ のブランチで同じにする場合、1つのSD-WANルールを作成し、3 つのブランチをカバーする3つの送信元ゾーンを指定できます。 SD-WAN ポリシールールでは、レイヤー3タイプの ゾーンのみがサポートされます。
送信元アドレス	送信元アドレスを指定するには、送信元アドレスまたは外部ダイナ ミック リスト (EDL) をAdd (追加)するか、ドロップダウンから選択 するか、Address (アドレス) を選択して新しいアドレス オブジェク トを作成します。または、Any (任意)の送信元アドレス (デフォル ト)を選択します。
Source User (送信元 ユーザー)	特定のユーザーを指定するには、 Add (追加) を選択し (タイプは 選 択を示します)、ユーザー、ユーザーのリスト、またはユーザーのグ ループを入力します。または、ユーザーのタイプを選択します。

項目	の意味
	 任意-(デフォルト)ユーザー データに関係なく、すべてのユー ザーを含めます。
	 ログオン前 – GlobalProtect[™] を使用してネットワークに接続 しているが、自分のシステムにはログインしていないリモート ユーザーが含まれます。GlobalProtect アプリのポータルに Pre- logon (ログオン前) オプションが設定されている場合、自分の マシンに現在ログインしていないユーザーは、ユーザー名 pre- logon として識別されます。pre-logon ユーザー用のポリシーを 作成でき、また、ユーザーが直接ログインしていなくても、そ のマシンは完全にログインしているかのようにドメインで認証 されます。
	 known-user(既知のユーザー) – 認証されたすべてのユーザー (ユーザー データがマッピングされた IP アドレス)が含まれ ます。このオプションは、ドメインの「ドメイン ユーザー」グ ループに相当します。
	 unknown[未知] – 認証されていないすべてのユーザー (ユー ザーにマップされていない IP アドレス) が含まれます。例え ば、unknown(不明) はゲスト レベルのアクセスに使用できま す。これらのユーザーは、ネットワーク上の IPアドレスを持っ ていますが、ドメインに認証されず、ファイアウォール上に IPアドレス対ユーザーのマッピング情報がないためです。
	● ファイアウォールが User-ID [™] エージェントではな く、RADIUS、TACACS+、または SAML アイデンティ ティ プロバイダ サーバーからユーザー情報を収集し ている場合、ユーザーのリストは表示されません。 ユーザー情報を手動で入力する必要があります。

Destination (宛先) タブ

• ポリシー > **SD-WAN** > 宛先

Destination (宛先) タブを選択して、SD-WAN ポリシー ルールが適用されるトラフィックを定義 する宛先ゾーンまたは宛先アドレスを定義します。

項目	の意味
宛先ゾーン	宛先ゾーンをAdd(追加)します (デフォルトは任意)。ゾーン はレイヤー3 である必要があります。新しいゾーンを定義する 手順については、「Network(ネットワーク) > Zones(ゾー ン)」を参照してください。

項目	の意味
	複数のゾーンを追加して管理を簡素化します。たとえば、信頼 されていない宛先ゾーンが指定されている3つの異なる内部 ゾーン (マーケティング、販売、広報) がある場合、すべての ケースを対象とした1つのルールを作成できます。
宛先アドレス	宛先アドレス、アドレス グループ、External Dynamic Lists (外 部ダイナミック リスト - EDL)、または地域をAdd (追加) しま す (デフォルトは Any (任意))。ドロップダウンリストから選択 するか、ドロップダウンリストの下部にある Address (アドレ ス)、Adress Group (アドレスグループ)をクリックして設定を行 います。
	Negate[上記以外]を選択すると、設定したアドレス以外の任意 のアドレスを指定したことになります。

SD-WAN Application/Service (アプリケーション/サービス) タブ

• ポリシー > **SD-WAN** > アプリケーション/サービス

Application/Service(アプリケーション/サービス)タブを選択して、SD-WAN ポリシールール が適用されるアプリケーションまたはサービスを指定し、アプリケーションまたはサービスに適 用されるプロファイル(パス品質、SaaS 品質、およびエラー修正プロファイル)を指定します 。

項目	の意味
Path Quality Profile (パス品 質プロファイル)	指定したアプリケーションとサービスに適用する最大ジッ ター、レイテンシー、およびパケット損失率のしきい値を決定 するパス品質プロファイルを選択します。パス品質プロファイ ルがまだ作成されていない場合は、New SD-WAN Path Quality Profile(新しい SD-WAN パス品質プロファイル)を作成する ことができます。
SaaS Quality Profile SaaS 品質プロファイル	SaaS 品質プロファイルを選択して、Software-as-a- Service (SaaS) アプリケーションへのダイレクト インターネッ ト アクセス (DIA) リンクを持つハブまたはブランチ ファイア ウォールの遅延、ジッター、およびパケット損失のパス品質し きい値を指定します。SaaS 品質プロファイルがまだ作成され ていない場合は、New SaaS Quality Profile (新しいSaaS品質 プロファイル) を作成することができます。デフォルト設定は None (なし) です。
Error Correction Profile エ ラーの修正プロファイル	Error Correction Profile (エラーの修正プロファイル)を選択 するか、新しいError Correction Profile(エラーの修正プロファ イル)を作成します。これで、ルールで指定されたアプリケー

項目	の意味
	ションまたはサービスの転送エラーの修正(FEC)またはパス の複製を制御するパラメータを指定します。このプロファイル は、ハブ ファイアウォールまたはブランチ ファイアウォールの いずれかで使用することができます。デフォルト設定は None (なし)です。
Applications(アプリケー ション)	SD-WAN ポリシー ルールに特定のアプリケーションをAdd (追加)するか Any (任意)を選択します。アプリケーションに複数の機能がある場合、アプリケーション全体または個別の機能を選択します。アプリケーション全体を選択した場合、すべての機能が含まれ、将来、機能が追加されるとアプリケーション定義が自動的に更新されます。
	SD-WAN ポリシー ルールでアプリケーション グループ、フィ ルタ、またはコンテナを使用している場合は、Application (アプ リケーション) 列のオブジェクトの上にマウスを置き、ドロップ ダウン リストを開いて Value (値)を選択すると、オブジェクト の詳細が表示されます。これにより、Object[オブジェクト]に 移動しなくても、ポリシーからアプリケーションメンバーを直 接表示することができます。
	レイテンシー、ジッター、またはパケット損失の 影響を受けるビジネスクリティカルなアプリケー ションのみを追加します。アプリケーション カテ ゴリまたはサブカテゴリが広すぎて、アプリケー ションごとの制御ができないため、追加しないで ください。
サービス	Add SD-WAN ポリシー規則の特定のサービスと、これらのサービスからのパケットを許可または拒否するポートを選択します。
	 any – 選択したサービスは、任意のプロトコルまたはポート で許可または拒否されます。
	 application-default – 選択したサービスは、デフォルトの Palo Alto Networks[®] で定義された ポートでのみ許可または 拒否されます。このオプションは、allow アクションを指定 するポリシーに推奨されます。このオプションは、意図的で ない場合でも、望ましくないサービスの動作と使用状況の兆 候となる可能性のある、異常なポートやプロトコルでサービ スが実行されないようにするためです。
項目	の意味
----	---
	 このオプションを使用すると、デフォルトのポートのみが SD-WAN ポリシーに一致し、アクションが適用されます。デフォルトポートにない他のサービスは、S1ecurity ポリシールールによっては許可される場合がありますが、SD-WAN ポリシーに一致せず、SD-WAN ポリシールールアクションは実行されません。
	ほとんどのサービスでは、application-defaultを使用して、サービスが非標準ポートを使用したり、その他の回避的な動作を起こさないようにします。サービスのデフォルトのポートが変わると、ファイアウォールが自動的にルールを更新してデフォルトのポートを修正します。内部カスタムサービスなど、非標準ポートを使用するサービスの場合は、サービスを変更するか、非標準ポートを指定するルールを作成し、サービスを必要とするトラフィックにのみルールを適用します。
	 Select–Add 既存のサービスを選択するか、Service または Service Group を選択して新しいエントリを指定します。(ま たは、Objects > Services および Objects > Service Groups を 選択します)。

SD-WAN Path Selection (パス選択) タブ

• ポリシー > SD-WAN > (パスの選択) Path Selection

Path Selection(パスの選択)タブを選択して、プライマリパスの品質がパス品質プロファイル で設定されたパス品質のしきい値を超えた場合にスワップするアプリケーションまたはサービス トラフィックのパスを定義します。

項目	の意味
トラフィック分散プロファ イル	ドロップダウンからトラフィック分散プロファイルを選択しま す。これにより、優先パスのパス正常性メトリックの1つが ルールのパス品質プロファイルで設定されたしきい値を超えた ときに、ファイアウォールがアプリケーションまたはサービス トラフィックの代替パスを選択する方法が決定します。

SD-WAN Target (ターゲット) タブ

• ポリシー > **SD-WAN** > ターゲット

Target (ターゲット**)** タブを選択して、SD-WAN ポリシー ルールをプッシュする管理対象デバイ スを選択します。このタブは、Panorama管理サーバーでのみサポートされています。

項目	の意味
任意(すべての対象デバイ ス)	SD-WAN ポリシー ルールを Panorama サーバ下のすべてのデ バイスにプッシュするには、有効化 (チェックをオン) にしま す。
機器	SD-WAN ポリシー ルールをプッシュする 1 つまたは複数のデ バイスを選択します。デバイスの状態、プラットフォーム、デ バイス グループ、テンプレート、タグ、または HA ステータス に基づいてデバイスをフィルタリングすることができます。
tags	ポリシーのタグを指定します。 ポリシー タグとは、ポリシーをソートまたはフィルタリングで きるキーワードや語句です。多数のポリシーを定義していて、 特定のキーワードでタグが付けられたポリシーを表示する場 合に役立ちます。たとえば、特定のルールに「復号」や「復号 なし」といった特定の語でタグを付けたり、特定のデータ セ ンターに関するポリシーにその場所の名前を使用したりできま す。 デフォルト ルールにタグを追加することもできます。
これらの指定されたデバイ スとタグのみをターゲット に設定する	有効 (チェックをオン) にすると、選択した Devices (デバイス) または指定した Tags (タグ) を除くすべてのデバイスにポリシー ルールがプッシュされます。

^{∞ paloalto} TECH**DOCS**

Objects

オブジェクトによりポリシールールの作成、実行スケジュールの設定、そして検索が可能になり、セキュリティプロファイルによりポリシールールで脅威防御を行うことができるようになり ます。

このセクションでは、セキュリティ プロファイルの設定方法と、ポリシーで使用できるオブ ジェクトについて説明します。

- オブジェクトの移動、コピー、オーバーライド、取り消し
- Objects (オブジェクト) > Addresses (アドレス)
- Objects > Address Groups [オブジェクト > アドレス グループ]
- Objects(オブジェクト) > Regions(地域)
- Objects (オブジェクト) > Applications (アプリケーション)
- Objects > Application Groups [オブジェクト > アプリケーション グループ]
- Objects > Application Filters [オブジェクト > アプリケーションフィルタ]
- Objects (オブジェクト) > Services (サービス)
- Objects (オブジェクト) >ServiceGroups
- Objects (オブジェクト) > Tags (タグ)
- Objects > Devices [オブジェクト > デバイス]
- Objects (オブジェクト) > GlobalProtect > HIP Objects (HIP オブジェクト)
- Objects(オブジェクト) > GlobalProtect > HIP Profiles(HIP プロファイル)
- Objects > External Dynamic Lists [オブジェクト > 外部動的リスト]
- Objects(オブジェクト) > Custom Objects(カスタム オブジェクト)
- Objects > Security Profiles > Mobile Network Protection [オブジェクト > セキュリティプロ ファイル > モバイル ネットワーク プロテクション]
- Objects (オブジェクト) > Security Profiles (セキュリティ プロファイル) > SCTP Protection (SCTP プロテクション)
- Objects > Log Forwarding [オブジェクト > ログ転送]
- Objects (オブジェクト) > Authentication (認証)
- Objects > Decryption Profile [オブジェクト > 復号化プロファイル]
- Objects > SD-WAN Link Management [オブジェクト > SD-WAN リンク管理]
- Objects (オブジェクト) > Schedules (スケジュール)

オブジェクトの移動、コピー、オーバーライド、取り 消し

既存のオブジェクトを編集する方法については以下のトピックを参照してください。

- オブジェクトの移動またはコピー
- オブジェクトのオーバーライド/取り消し

オブジェクトの移動またはコピー

オブジェクトを移動またはコピーする場合は、Shared(共有)場所を含め、自分がアクセス 許可を与えられている Destination(宛先)(ファイアウォール上の仮想システム、または Panorama[™] 上のデバイス グループ)を割り当てることができます。

オブジェクトルールを移動する場合は、Objects[オブジェクト] タブでオブジェクトを選択 し、Move[移動]をクリックして、Move to other vsys[他のvsysに移動](ファイアウォールの み)またはMove to other device group[他のデバイスグループに移動](Panoramaのみ)を選択 し、以下の表の各フィールドを入力してOKをクリックします。

オブジェクトをコピーする場合は、**Objects**[オブジェクト] タブで**Clone**[コピー]をクリックして、以下の表の各フィールドを入力して**OK**をクリックします。

設定の移動/コピー	の意味
選択したオブジェクト	操作対象として選択したポリシーまたはオブジェクトの名前と 現在の場所 (仮想システムまたはデバイス グループ) が表示さ れます。
宛先	ポリシーまたはオブジェクトの新しい場所として、仮想シス テム、デバイス グループ、または共有を選択します。デフォ ルト値は、Policies[ポリシー] または Objects[オブジェクト] タブで選択した Virtual System[仮想システム] または Device Group[デバイス グループ] です。
検証で最初に検出されたエ ラーに起因するエラーが発 生しました	このオプションをオンにすると(デフォルトはオン)、ファイ アウォールまたはPanoramaが、最初に検出したエラーを表示 し、それ以上エラーをチェックしません。たとえば、移動する ポリシー ルールで参照されているオブジェクトが [宛先] に存 在しないと、エラーが発生します。このオプションをオフにし た場合、ファイアウォールまたはPanoramaは、先に全てのエ ラーを検出してからそれらを表示します。

オブジェクトのオーバーライド/取り消し

Panorama では、ツリー階層の中でデバイス グループを 4 段階までネストさせることができま す。一番下のレベルのデバイスグループは、連続する上位レベルとして親、祖父母、曽祖父母 のデバイス グループを持つことができます。これらをまとめて先祖と呼び、一番下のレベルの デバイスグループはこれらからポリシーとオブジェクトを継承します。一番上のレベルのデバイ スグループは、子、孫、曾孫のデバイス グループを持つことができます。これらをまとめて子 孫と呼びます。子孫のオブジェクトをオーバーライドして、先祖のオブジェクトとは異なる値 を持たせることもできます。このオーバーライド機能はデフォルトで有効になっています。ただ し、共有オブジェクトまたはデフォルト (事前設定) オブジェクトをオーバーライドすることはで きません。Web インターフェイスでは、値を継承しているオブジェクトには ● アイコンが、 値がオーバーライドされている継承オブジェクトには ◎ アイコンが表示されます。

- Override an object[オブジェクトのオーバーライド] Objects[オブジェクト] タブを選択し、 オーバーライドされたオブジェクトの所属先となる子孫 Device Group[デバイスグループ] を 選択してから、Override[オーバーライド] をクリックして設定を編集します。オブジェクト の Name[名前] または Shared[共有] 設定をオーバーライドすることはできません。
- Revert an overridden object to its inherited values[オーバーライドしたオブジェクトの設定 値を継承した値に戻す] – Objects[オブジェクト] タブを選択し、オーバーライドされたオブ ジェクトが所属する子孫 Device Group[デバイスグループ] を選択してから、当該オブジェク トを選択し、Revert[元に戻す] をクリックした後、Yes[はい] をクリックして操作を確定しま す。
- Disable overrides for an object[オブジェクトのオーバーライドを無効化] Objects[オブジェ クト] タブを選択し、当該オブジェクトが存在する Device Group[デバイスグループ] を選択 してから、そのオブジェクトの名前をクリックし、Disable override[オーバーライドの無効 化] チェックボックスをオンにして、OK をクリックします。これにより、そのオブジェクト のオーバーライドが、選択した Device Group(デバイス グループ)からオブジェクトを継承 するすべてのデバイス グループで無効になります。
- Replace all object overrides across Panorama with the values inherited from the Shared location or ancestor device groups (Panorama 全体のすべてのオブジェクトオーバーライドを共有場所または先祖デバイス グループから継承した値で置換する) Panorama > Setup (セットアップ) > Management (管理)を選択し、Panorama 設定で Ancestor Objects Take Precedence (上位オブジェクトを優先)を選択して、OKをクリックします。この後、Panorama およびオーバーライドが含まれるデバイス グループに対してコミットを実行して、継承値をプッシュする必要があります。

Objects > Addresses [オブジェクト > アドレス]

アドレスオブジェクトには、IPv4 アドレスまたは IPv6 アドレス(単一の IP アドレス、アドレ スの範囲、またはサブネット)、FQDN、ワイルドカードのアドレス(IPv4 アドレスに続けて スラッシュ、ワイルドカード マスク)のいずれかを含めることができます。アドレス オブジェ クトを使用すると、インスタンスごとに手動で各アドレスを追加しなくても、すべてのポリシー ルールベース、フィルター、他のファイアウォール機能の送信元アドレスまたは宛先アドレスと 同じアドレスまたはアドレスグループを再利用できます。Web インターフェイスまたは CLI を 使用してアドレス オブジェクトを作成します。変更を加えると、オブジェクトが設定の一部に なります。

はじめに新規アドレスをAdd(追加)してから以下の値を指定します。

アドレス オブジェクト の設定	の意味
氏名	 このオブジェクトの一部として含めるアドレスを記述する名前(最大63文字)を入力します。この名前は、セキュリティポリシールールを定義するときにアドレスのリストに表示されます。大文字と小文字を区別し、一意の名前を入力する必要があります。文字、数字、スペース、ハイフン、アンダースコアのみが使用できます。 ファイアウォール上の仮想ルーターまたは論理ルーターのスタティックルートの設定中に、ネクストホップルータのIPアドレスを入力できます。Palo Alto Networksファイアウォールは、ネクストホップIPアドレスをアドレスオブジェクトとして扱います。したがって、ネクストホップIPアドレス ([Network (ネットワーク]] > [Virtual Router (仮想ルーター)] > [Static Routes (静的ルート)])の値を、設定されているアドレスオブジェクト名([Objects (オブジェクト]) > [Addresses (アドレス]))と同じに設定すると、アドレスオブジェクトへの変更はネクストホップIPアドレスの値にも反映されます。つまり、アドレスオブジェクト([Objects (オブジェクト]] > [Addresses (アドレス)])の名前を変更すると、ネクストホップIPアドレスも変更されます。
共有	 このアドレスオブジェクトを共有する場合は、以下を含むこのオプションを選択します。 マルチ vsys ファイアウォール上のすべての仮想システム(vsys)-この選択を解除すると、Objects(オブジェクト)タブで選択したVirtual System(仮想システム)のみに対してアドレスオブジェクトが公開されます。

アドレス オブジェクト の設定	の意味
	 Panorama上のすべてのデバイス グループ-この選択を解除する と、Objects(オブジェクト)タブで選択したDevice Group(デ バイスグループ)のみに対してアドレスオブジェクトが公開さ れます。
オーバーライドの無効 化(Panoramaのみ)	このアドレスオブジェクトの設定が、このオブジェクトを継承した デバイス グループで管理者によりオーバーライドされることを防止 するには、このオプションを選択します。デフォルトではこの選択 はオフになっており、管理者は、このオブジェクトを継承するデバ イス グループの設定をオーバーライドできます。
の意味	オブジェクトの説明を入力します (最大1023 文字)。
タイプ	アドレスオブジェクトの型およびエントリを指定します:
	 IP Netmask (IP ネットマスク)-IPv4またはIPv6アドレス、またはIPアドレスの範囲を次の表記で入力します: ip_address / maskまたはip_address。ここでのmaskはアドレスのネットワーク部分に使用される有効な2進数の桁数です。Ipv6アドレスの場合は、ホスト部を指定せずにネットワーク部のみを指定することをお勧めします。以下に例を示します。
	 192.168.80.150/32 – 1つのアドレスを示します。
	• 192.168.80.0/24 – 192.168.80.0 から 192.168.80.255
	• 2001:db8::/32
	• 2001:db8:123:1::/64
	 IP Range (IP 範囲)-次の形式を使用してアドレスの範囲を入力します。ip_address-ip_address (範囲の両端が IPv4 アドレスであるか、または両方が IPv6 アドレスです)。以下がその例です。2001:db8:123:1::1-2001:db8:123:1::22
	 IP Wildcard Mask (IP ワイルドカードマスク)–IPv4 アドレスに 続けてスラッシュ、ワイルドカードマスク(0から始める必要 があります)という形式で IP ワイルドカード アドレスを入力し ます。例:10.182.1.1/0.127.248.0。ワイルドカードマスクのゼ ロ(0)ビットは、比較対象のビットが、0がカバーする IP アド レスのビットと一致しなければならないことを示します。マス クの1ビットはワイルドカードビットであり、比較対象のビッ トが、1がカバーする IP アドレスのビットと一致する必要がな いことを示します。IP アドレスおよびワイルドカードマスクを バイナリに変換します。マッチングを説明するために、バイナ

アドレス オブジェクト の設定	の意味
	リの抜粋 0011 では、ワイルドカード マスク 1010 は 4 つの一 致 (0001、0011、1001、および 1011) になります。
	タイプ IP Wildcard Mask のアドレス オブジェク トは、Security ポリシー ルールでのみ使用できま す。
	 FQDN-ドメイン名を入力します。FQDN はコミット時に最初に解決されます。TTL が最低 FQDN 更新時間以上である場合、FQDN のエントリは後に FQDN の TTL に基づいて更新されます。そうでない場合、FQDN のエントリは Minimum FQDN Refresh Time (最低 FQDN 更新時間)に更新されます。FQDN は、システムの DNS サーバーまたは DNS プロキシ オブジェクト (プロキシが設定されている場合)によって解決されます。
解決	アドレスタイプを選択し、IP アドレスまたは FQDN を入力した ら、Resolve(解決)をクリックして(ファイアウォールまたは Panorama の DNS 設定に基づいて)関連する FQDN または IP アド レスをそれぞれ表示します。
	アドレスオブジェクトを FQDN から IP ネットマスクに変更す ることができます。FQDN から IP ネットマスクに変更するに は、Resolve (解決)をクリックして、FQDN が解決する IP アド レスを確認してから、Use this address (このアドレスを使用)し ます。アドレス オブジェクト タイプが IP ネットマスクに動的に変 更され、選択した IP アドレスがテキスト フィールドに表示されま す。
	または、アドレスオブジェクトを IP ネットマスクから FQDN に変 更するには、Resolve (解決)をクリックして IP ネットマスクが解 決する DNS 名を表示し、FQDN を選択して、Use this FQDN (こ の FQDN を使用)します。タイプが FQDN に変更され、テキスト フィールドに FQDN が表示されます。
tags	このアドレスオブジェクトに適用するタグを選択または入力し ます。ここでタグを定義することも、Objects(オブジェクト) > Tags(タグ)タブを使用して新しいタグを作成することもできま す。

Objects > Address Groups [オブジェクト > アドレス グ ループ]

セキュリティ ポリシーの作成を簡略化するには、同じセキュリティ設定が必要なアドレスをア ドレス グループにまとめます。アドレス グループは、静的または動的にすることができます。

ダイナミックアドレスグループ:動的アドレスグループには、タグの検索とタグベースのフィルタを使用してメンバーがダイナミックに入力されます。動的アドレスグループは、広範囲に及ぶ仮想インフラストラクチャがあり、仮想マシンの場所/IPアドレスが頻繁に変更される場合に非常に便利です。たとえば、高度なフェイルオーバーで仮想マシンが頻繁にセットアップまたはプロビジョニングされていて、ファイアウォールの設定/ルールを変更せずに新しいマシンとの間で送受信されるトラフィックにポリシーを適用する場合などです。

ポリシーで動的アドレス グループを使用するには、以下のタスクを実行する必要がありま す。

- 動的アドレス グループを定義し、ポリシー ルール内で参照します。
- ファイアウォールに IP アドレスと対応するタグを通知して、動的アドレス グループのメンバーを構成できるようにします。これを行うには、ファイアウォール上で XML API を使用する外部スクリプトを使用するか、VMware ベースの環境の場合は Device (デバイス) > VM Information Sources (VM 情報の送信元)を選択してファイアウォールの設定を編集します。

動的アドレス グループには、静的に定義したアドレス オブジェクトも含めることができま す。アドレス オブジェクトを作成し、動的アドレス グループに割り当てたものと同じタグを 適用すると、その動的アドレス グループには、そのタグに一致するすべての静的オブジェク トと動的オブジェクトが含まれます。そのため、タグを使用して動的オブジェクトと静的オ ブジェクトの両方を同じ アドレス グループにまとめることができます。

 動的アドレスオブジェクト:静的アドレスグループには、静的なアドレスオブジェクト、動的 アドレスグループ、またはアドレスオブジェクトと動的アドレスグループの両方の組み合わ せを含めることができます。

アドレスオブジェクトを作成するには、Add[追加]をクリックし、以下のフィールドを入力 します。

アドレス グループ設定	の意味
氏名	アドレス グループを表す名前 (最大 63 文字) を入力します。この名 前は、セキュリティ ポリシーを定義するときにアドレスのリストに 表示されます。名前の大文字と小文字は区別されます。また、一意 の名前にする必要があります。文字、数字、スペース、ハイフン、 およびアンダースコアのみを使用してください。
共有	以下に対してアドレスグループを公開する場合は、このオプション を選択します。

アドレスグループ設定	の意味
	 multi-vsys ファイアウォールの各仮想システム (vsys)。この選 択を解除すると、Objects[オブジェクト] タブで選択したVirtual System[仮想システム] のみに対してアドレスグループが公開さ れます。
	 Panorama 上の各デバイス グループ。この選択を解除すると、Objects[オブジェクト] タブで選択したDevice Group[デバイスグループ] に対してのみアドレスグループが公開されます。
オーバーライドの無効 化(Panoramaのみ)	このアドレス グループ オブジェクトの設定が、このオブジェクト を継承したデバイス グループで管理者によりオーバーライドされ ることを防止するには、このオプションを選択します。デフォルト でこのオプションはオフになっており、管理者は、このオブジェク トを継承するデバイス グループの設定をオーバーライドできます。
の意味	オブジェクトの説明を入力します (最大1023 文字)。
タイプ	Static[静的] または Dynamic[動的] を選択します。
	動的 アドレス グループを作成するには、一致条件を使用してグ ループに含めるメンバーをまとめます。AND または OR 演算子を 使用して、Match[一致] 条件を定義します。否定はサポートされて いません。
	一致条件に使用する属性のリストを表示するには、送 信元/ホストにアクセスして属性を取得できるように ファイアウォールを設定しておく必要があります。設 定した情報送信元の各仮想マシンをファイアウォール に登録します。ファイアウォールは、マシンをポーリ ングして、ファイアウォールの変更なしに IP アドレ スまたは設定の変更を取得できます。
	静的 アドレス グループの場合、Add[追加] をクリックし、1 つ以上 のAddresses[アドレス]を選択します。Add[追加] をクリックし、オ ブジェクトまたはアドレス グループをアドレス グループに追加し ます。グループには、アドレス オブジェクト、静的と動的の両方の アドレス グループを含めることができます。
tags	このアドレス グループに適用するタグを選択または入力します。タ グの詳細は、「Objects(オブジェクト) > Tags(タグ)」を参照 してください。
メンバー数およびアド レス	アドレス グループを追加したら、 Objects (オブジェクト) > Address Groups(アドレス グループ)ページの Members Count(メンバー数)列に、グループ内のオブジェクトが動的また は静的のどちらの方法で作成されたかが示されます。

アドレス グループ設定	の意味
	 静的アドレス グループの場合、アドレス グループのメンバー数 を参照できます。
	 タグを使用してメンバーを動的に作成したアドレスグループ、 または静的メンバーと動的メンバーの両方を含むアドレスグ ループの場合、メンバーを参照するには、Address(アドレス) 列の More(詳細)リンクをクリックします。これで、アド レスグループに登録された IP アドレスを参照できます。
	 Type(タイプ)は、IP アドレスが静的アドレスオブジェクト であるか、動的に登録されるものであるかを示し、IP アドレ スを表示します。
	 Action(アクション)を使用すると、IPアドレスから Tags(タグ)をUnregister(登録解除)できます。リンクを クリックして、登録元をAdd(追加)し、登録解除するタグ を指定します。

Objects > Regions [オブジェクト > 地域]

ファイアウォールでは、特定の国や他の地域に適用されるポリシー ルールを作成できます。地域は、セキュリティポリシー、復号化ポリシー、DoS ポリシーの送信元および宛先を指定するときにオプションとして利用できます。セキュリティポリシールールのオプションとして地域を含めるには、国の標準リストから選択するか、このセクションで説明されている地域設定を使用してカスタム地域を定義します。

地域設定	の意味
リージョン	地域を説明するドロップダウンメニューから名前を選択します。こ の名前は、セキュリティ ポリシーを定義するときにアドレスのリス トに表示されます。
デバイス稼働場所	緯度と経度を指定する場合は、このオプションを選択して値 (xxx.xxxxx 形式)を指定します。この情報は、App-Scopeのトラ フィックマップおよび脅威マップに使用されます。「Monitor(監 視) > Logs(ログ)」を参照してください。
addresses	以下のいずれかの形式を使用して IP アドレス、IP アドレス範囲、 または地域を識別するサブネットを指定します。 x.x.x.x x.x.x.xy.y.y.y x.x.x.x/n

以下の表では、地域設定について説明します。

Objects > Dynamic User Groups [オブジェクト > 動的 ユーザー グループ]

動的ユーザー グループを作成するには Objects(オブジェクト) > Dynamic User Groups (動的 ユーザー グループ)、 Add (追加) を選択して、以下の設定を構成します。

Dynamic User Group Settings (動的ユーザー グループ設定)	の意味
氏名	動的ユーザー グループを説明する Name (名前) を入力します (最大 63 文字)。この名前は、セキュリティ ポリシー ルールを定義すると きに送信元ユーザー リストに表示されます。名前は一意で、英数 字、スペース、ハイフン、およびアンダースコアのみを使用してい る必要があります。
の意味	オブジェクトの Description (説明) を入力します (最大1,023 文字)。
Shared (Panorama only)	動的ユーザー グループの一致条件を Panorama 上のすべてのデバイ ス グループで使用できるようにする場合は、このオプションを選択 します。
	Panoramaは、グループのメンバーをデバイスグルー プと共有しません。
	このオプションをオフにすると、動的ユーザー・グループの一致基 準は、Objects タブで選択した Device Group でのみ使用可能にな ります。
オーバーライドを無効 にする (Panorama のみ)	管理者が、オブジェクトを継承するデバイス グループのこの動的 ユーザー グループの設定をオーバーライドすることを禁止する場合 はこのオプションを選択します。デフォルトでこのオプションはオ フになっており、管理者は、このオブジェクトを継承するデバイス グループの設定をオーバーライドできます。
一致	Add Match Criteria (条件の追加)から AND または OR 演算子を使用 した動的ユーザー グループのメンバーを定義し、複数のタグを含め ます。否定はサポートされていません。
	Add Match Criteria (条件の追加)をすると、既存のタグ のみが表示されます。既存のタグを選択するか、新し いタグを作成できます。

Dynamic User Group Settings (動的ユーザー グループ設定)	の意味
tags	(任意)動的ユーザーグループオブジェクトに適用する静的オブ ジェクトタグを選択または入力します。これにより、グループ のメンバーではなく、動的ユーザーグループオブジェクト自体 にタグが付けられます。選択したタグを使用すると、一致条件 に関係なく関連アイテムをグループ化できます。タグの詳細は、 「Objects(オブジェクト) > Tags(タグ)」を参照してくださ い。

動的ユーザー グループを追加すると、グループの次の情報を表示できます。

Dynamic User Groups Column (動 的ユーザー グループ列)	の意味
場所 (Panorama のみ)	動的ユーザー グループの一致条件が、Panorama のすべ てのデバイス グループ (Shared (共有)) で使用できるか、 選択したデバイス グループで使用できるかを特定しま す。
Users	動的ユーザー グループのユーザーのリストを表示するに は 詳細 を選択します。
	 グループに含めるタグをユーザーに追加するには、 Register Users (新規ユーザーの登録)から、ユーザー に適用する Registration Source(登録ソース) と Tags (タグ)を選択します。ユーザーのタグがグループの条 件に一致すると、ファイアウォールはユーザーを動的 ユーザー グループに追加します。
	 (任意) Timeout (タイムアウト) を分単位で指定し (デ フォルトは 0、範囲は 0 ~ 43,200)、指定した時間が 経過したときにユーザーをグループから削除します。
	 (任意) Users (ユーザー) をグループに Add (追加)、またはグループから Delete (削除) します。
	 ユーザーからタグを削除してグループのメンバー にならないようにするには、ユーザーを選択し、 Unregister Users (ユーザーの登録解除)をしてか ら Registration Source (登録ソース) と Tags (タグ)を 選択します。
	 ユーザーの動的ユーザー グループ リストを確認また は変更したら Close (終了)をクリックします。

Objects > Applications [オブジェクト > アプリケーション]

以下のトピックでは、Applications(アプリケーション)ページについて説明します。

確認すべき情報	以下を参照
Applications(アプリケーショ ン)ページに表示されるアプ リケーションの設定と属性を 理解する	アプリケーションの概要 アプリケーションでサポートされる操作
新規アプリケーションを追 加するか、既存のアプリケー ションを変更する	アプリケーションの定義

アプリケーションの概要

Applications (アプリケーション)ページには、アプリケーションの相対セキュリティリスク(1~5)など、各アプリケーション定義のさまざまな属性が表示されます。リスク値は、アプリケーションでファイルを共有できるか、誤用が起こりやすいか、ファイアウォールの回避を試行するか、などの基準に基づいています。値が大きいほどリスクが大きくなります。

ページ上部のアプリケーションブラウザエリアには、以下のように、表示内容のフィルタに使 用できる属性が表示されます。各エントリの左側にある数字は、その属性があるアプリケーショ ンの合計数を表しています。

CATEGORY ^	SUBCATEGORY A	RISK A	TAGS ^	CHARACTERISTIC ^
1267 business-systems	54 audio-streaming	1359 1	76 Enterprise VoIP	37 Data Breaches
634 collaboration	23 auth-service	842 2		634 Evasive
508 general-internet	39 database	533 2	18 G Suite	658 Excessive Bandwidth
322 media	85 email	050 3	19 Palo Alto Networks	46 FEDRAMP
502 networking	67 encrypted-tunnel	359 4		1 FINRA
2 unknown	45 erp-crm	142 5	1676 Web App	108 HIPAA
	349 file-sharing		1448 No tag	83 IP Based Restrictions
	*			

週次のコンテンツリリースには、新しいデコーダとシグネチャを開発するためのコンテクストが定期的に含まれています。

以下の表では、アプリケーションの詳細情報について説明します。カスタム アプリケーション および Palo Alto[®] Networks アプリケーションには、これらのフィールドの一部またはすべてが 表示されます。

アプリケーションの詳細情報	の意味
氏名	アプリケーションの名前です。

アプリケーションの詳細情報	の意味
の意味	アプリケーションの説明 (最大 255 文字)。
追加情報	アプリケーションに関する追加情報が掲載されている Web ソース (Wikipedia、Google、および Yahoo!) にリンクします。
標準ポート	アプリケーションがネットワークとの通信に使用するポートで す。
依存	このアプリケーションの実行に必要な他のアプリケーションの リストです。選択したアプリケーションを許可するポリシー ルールを作成する場合は、そのアプリケーションが依存する他 のすべてのアプリケーションも許可することを確認する必要が あります。
暗黙的に使用	選択したアプリケーションが依存しているものの、暗黙的にサ ポートされているため、選択したアプリケーションを許可する ためにセキュリティ ポリシー ルールに追加する必要のないそ の他のアプリケーション。
以前の識別	新規の App-ID [™] 、または変更された App-ID について、その アプリケーションの以前の ID を表します。これにより、アプ リケーションの変化に応じてポリシーを変更する必要がある かどうかを査定できます。App-ID を無効にすると、そのアプ リケーションに関連付けられたセッションは、そのアプリケー ションの以前の ID でポリシーと照合されます。同様に、無効 にされた App-ID は、そのアプリケーションの以前の ID でロ グに記録されます。
アクションの拒否	App-IDは、デフォルトの拒否アクションと共に作成されま す。デフォルトの拒否アクションは、アプリケーションが拒 否アクションの指定されたセキュリティポリシールールに含ま れているときのファイアウォールの応答方法を指定したもので す。デフォルトの拒否アクションとして、サイレント ドロッ プまたは TCP リセットを指定できます。このデフォルトアク ションはセキュリティポリシー内でオーバーライドできます。
特徴	
セキュリティを回避する	ファイアウォールを通り抜けるために、ポートやプロトコルを 本来の用途とは異なる目的に使用すること。
帯域幅を消費する	通常の使用において 1 Mbps 以上の帯域幅を定常的に消費する こと。

の意味
不正な目的に使用されることが多いこと。また、ユーザーの意 図を超えて攻撃されるように容易に設定できてしまうこと。
ファイアウォールでは、Software as a Service (SaaS) を次のよ うなサービスとして分類します。すなわち、ソフトウェアとイ ンフラストラクチャはアプリケーション サービス プロバイダ によって所有および管理されているが、ユーザーがデータに対 するフル コントロール (データの作成、アクセス、共有、転送 の実行権限をどのユーザーに付与するかも含む) を保有してい るサービスです。
アプリケーションの特徴という観点から見ると、SaaS アプリ ケーションと Web サービスは異なります。Web サービスと は、ホストされたアプリケーションであり、ユーザーがデー タを所有しないサービス (Pandora など) と、多数の購読者が 社交目的で投稿したデータの共有を主要機能とするサービス (LinkedIn、Twitter、Facebook など) があります。
ネットワークを介してシステム間でファイルを転送できるこ と。
他のアプリケーションを自分のプロトコル内で転送できるこ と。
アプリケーションがマルウェアに感染した状態で配布される こと (マルウェアは、アプリケーションを利用して、伝播、拡 散、攻撃、データの不正入手を行うことが知られている)。
一般に公表されている脆弱性があること。
ユーザーが 100 万人を超える可能性があること。
 他のアプリケーションシグネチャとの照合を続行するように ファイアウォールに指示します。このオプションをオフにする と、ファイアウォールは、最初にシグネチャが一致した後、ア プリケーションシグネチャとの照合を停止します。 トラフィックを許可するセキュリティ ポリシー ルールで脆弱性保護プロファイルを構成した 場合、ファイアウォールはこのオプションの有 効/無効にかかわらず、他のアプリケーションの スキャンを続行します。

SaaS 特性

アプリケーションの詳細情報	の意味
情報漏洩	過去3年以内に信頼できない情報源に安全な情報を公開した可 能性があるアプリケーション。
悪質なサービス利用規約	企業データを危険にさらすおそれのある利用規約が記載された アプリケーション。
証明書がない	SOC1、SOC2、SSAE16、PCI、HIPAA、FINRAA、また はFEDRAMPなどの業界プログラムまたは証明書に準拠してい ないアプリケーション。
財政的実行可能性が低い	今後 18~24 ヶ月以内に中断する可能性のあるアプリケーション。
IP 制限がない	ユーザーアクセスのための IP ベースの制限がないアプリケー ション。

分類

カテゴリ	 以下のアプリケーション カテゴリがあります。 business-system コラボレーション 一般インターネット メディア networking 未知
サブカテゴリ	アプリケーションが分類されるサブカテゴリです。カテゴリが 異なると、関連付けられるサブカテゴリも異なります。たとえ ば、collaboration カテゴリのサブカテゴリには、email、file- sharing、instant-messaging、internet-conferencing、social- business、social-networking、voip-video、web-posting があります。一方、business-system カテゴリのサブカ テゴリには、auth-service、database、erp-crm、general- business、management、office-programs、software- update、storage-backup があります。
テクノロジ	 アプリケーション技術は以下のうちの1つに分類されます。 クライアント/サーバー1つ以上のクライアントがネット ワーク上のサーバーと通信するクライアント/サーバーモデ ルを使用したアプリケーション。

アプリケーションの詳細情報	の意味
	 ネットワークプロトコル一般に、システム間の通信に使用 され、ネットワーク操作を容易にするアプリケーション。 大部分の IP プロトコルが含まれます。 ピアツーピア通信の簡素化を図るため、中央のサーバーを 介することなく他のクライアントと直接やり取りして情報 を交換するアプリケーション。 ブラウザベースWeb ブラウザに依存して機能するアプリ ケーション。
リスク	アプリケーションに割り当てられたリスクです。
	この設定をカスタマイズするには、Customize(カスタマイ ズ)リンクをクリックして値(1 ~ 5)を入力し、OK をク リックします。
tags	アプリケーションに割り当てられたタグ。
	Edit Tags (タグの編集) で、アプリケーションのタグを追加ま たは削除します。
オプション	
セッション タイムアウト	非アクティブ状態になってからアプリケーションがタイムアウトするまでの時間 (指定可能範囲は 1 ~ 604800 秒) です。このタイムアウトは、TCP または UDP 以外のプロトコルに適用されます。TCP と UDP は、この表の次の行を参照してください。
	この設定をカスタマイズするには、Customize[カスタマイズ] リンクをクリックして値を入力し、OK をクリックします。
TCP タイムアウト (秒)	TCP アプリケーション フローを停止するタイムアウト (指定可 能範囲は 1 ~ 604800 秒) です。
	この設定をカスタマイズするには、 Customize [カスタマイズ] リンクをクリックして値を入力し、 OK をクリックします。
	値 0 は、グローバル セッション タイマー (TCP の場合 3600 秒) が使用されることを示します。
UDP タイムアウト (秒):	UDPアプリケーションフローを停止するタイムアウト(指定可 能範囲は1~604800秒)です。
	この設定をカスタマイズするには、Customize[カスタマイズ] リンクをクリックして値を入力し、OK をクリックします。
TCP Half Closed(秒)	最初の FIN パケットを受信してから、2 つ目の FIN パケット または RST パケットを受信するまで、セッションがセッショ

アプリケーションの詳細情報	の意味
	ン テーブル内に保持される最大時間 (秒)。タイマーが期限切 れになるとセッションが閉じられます (指定可能範囲は 1 ~ 604800 秒)。
	デフォルト:このタイマーがアプリケーションレベルで設定さ れていない場合、グローバル設定が使用されます。
	この値がアプリケーション レベルで設定されている場合、 その値でグローバル TCP Half Closed [TCP半閉鎖] 設定がオー バーライドされます。
TCP Time Wait(秒)	2 つ目の FIN パケットまたは RST パケットを受信してから、 セッションがセッション テーブル内に保持される最大時間 (秒)。タイマーが期限切れになるとセッションが閉じられます (指定可能範囲は 1 ~ 600 秒)。
	デフォルト:このタイマーがアプリケーションレベルで設定さ れていない場合、グローバル設定が使用されます。
	この値がアプリケーション レベルで設定されている場合、そ の値でグローバル TCP Time Wait [TCP待機] 設定がオーバーラ イドされます。
App-ID 対応	App-ID が有効か無効かを示します。App-IDを無効にすると、 そのアプリケーションのトラフィックは、セキュリティポリ シーとログの両方で、Previously Identified As[以前の識別内 容] に指定したApp-IDで処理されます。コンテンツリリース バージョン 490 の後に追加されたアプリケーションの場合、 新規アプリケーションのポリシーへの影響を確認する際にア プリケーションを無効にすることができます。ポリシーをレ ビューした後、App-ID を enable[有効化] することも可能で す。以前有効にしたアプリケーションを disable[無効化] する こともできます。multi-vsys ファイアウォールでは、各仮想シ ステムで App-ID を個別に無効化できます。

ファイアウォールで APP-ID を使用してアプリケーションを識別できない場合、トラフィックは 不明 ([unknown-tcp] または [unknown-udp]) として分類されます。この動作は、完全に HTTP を エミュレートするアプリケーションを除き、すべての不明なアプリケーションに適用されます。 詳細についてはMonitor > Botnet [監視 > ボットネット]を参照してください。

不明なアプリケーションの新しい定義を作成し、その新しいアプリケーション定義のセキュリ ティ ポリシーを定義できます。さらに、同じセキュリティ設定が必要なアプリケーションをア プリケーション グループにまとめることで、セキュリティ ポリシーの作成を簡略化できます。

アプリケーションでサポートされる操作

必要に応じて、このページで以下の操作を実行できます。

アプリケーションでサ ポートされる操作	の意味
アプリケーション名による検索	 特定のアプリケーションを検索する場合は、Search(検索)フィールドにアプリケーションの名前または説明を入力してEnterキーを押します。ドロップダウンリストには、特定のアプリケーションの検索や絞り込みを行ったり、All(すべて)のアプリケーション、Custom applications(カスタムアプリケーション)、Disabled applications(カスタムアプリケーション)、たはTagged applications(タグ付けされたアプリケーション)、またはTagged applications(タグ付けされたアプリケーション)を表示することができます。 該当するアプリケーションが表示され、同時にフィルタ列が更新されて、検索条件に一致するアプリケーションの統計値が表示されます。検索は、文字列に部分的に一致します。セキュリティポリシーを定義すると、保存したフィルタに一致するすべてのアプリケーションに適用されるルールを作成できます。このようなルールは、フィルタに一致するコンテンツの更新によって新しいアプリケーションが追加されると動的に更新されます。 ページに表示されているアプリケーション属性で絞り込みを行う場合は、フィルタリングの基準として使用する項目をクリックします。たとえば、collaborationカテゴリのみをリストに表示する場合は、collaboration(コラボレーション)をクリックすると、そのカテゴリのアプリケーションのみがリストに表示されます。
	・その他の列にフィルタを適用するには、列のエントリを選択します。フィルタリングは連続的です。カテゴリフィルタ、サブカテゴリフィルタ、テクノロジフィルタを適用すると、明示的にテクノロジのフィルタを適用していなくても、自動的にTechnology (テクノロジ) 列が制限され、選択した

カテゴリとサブ カテゴリに一致するテクノロジのみが表示されます。フィルタを適用するたびに、アプリケーション リス

アプリケーションでサ ポートされる操作	の意味	
	トが自動的に更新されます。新しいアプリケーションフィル タを作成する方法については、「Objects(オブジェクト) > Application Filters(アプリケーションフィルタ)」を参照し てください。	
新しいアプリケーション を追加	新しいアプリケーションを追加する方法については、「アプリ ケーションの定義」を参照してください。	
アプリケーションの詳細 を表示、またはカスタマ イズする	標準ポート、特性、リスクやその他の情報を含め、アプリケー ションの詳細を表示する場合はアプリケーション名のリンクを クリックします。アプリケーション設定の詳細は、「アプリケー ションの定義」を参照してください。 アプリケーション名の左にあるアイコンに黄色い鉛筆 (が表示されている場合、そのアプリケーションがカスタムアプリ ケーションであることを示しています。)
アプリケーションの無効化	特定の(または複数の)アプリケーションを Disable (無効化)す ると、アプリケーションシグネチャがトラフィックと照合されな くなります。一致するアプリケーションをブロック、許可、また は実施するように定義されたセキュリティルールは、アプリケー ションを無効にすると、アプリケーショントラフィックに適用さ れません。新しいコンテンツリリースバージョンに含まれるア プリケーションは無効にしたほうがよいことがあります。そうし たアプリケーションが一意に識別されると、アプリケーションの ポリシーが適用されるかどうかが変わる可能性があるからです。 たとえば、新しいコンテンツバージョンのインストール前の状態 では、Web ブラウジングトラフィックとして識別されたアプリ ケーションがファイアウォールに許可されていたとします。とこ ろがコンテンツの更新をインストールした後、一意に識別された アプリケーションが、Web ブラウジングトラフィックを許可す るセキュリティルールに一致しなくなってしまうことがありま す。このような場合は、アプリケーションを無効にして、そのア プリケーションシグネチャに一致したトラフィックが引き続き Web ブラウジングトラフィックとして分類され許可されるよう にしたほうが適切です。	
アプリケーションの有効 化	無効化されたアプリケーションを選択して Enable(有効化)する ことにより、設定済みのセキュリティ ポリシーに従ってそのアプ リケーションを管理できます。	
アプリケーションのイン ポート	アプリケーションをインポートするには、Import[インポート] を クリックします。ファイルを参照して選択し、Destination[宛先]	

アプリケーションでサ ポートされる操作	の意味
	ドロップダウンリストからターゲットの仮想システムを選択しま す。
アプリケーションのエク スポート	アプリケーションをエクスポートする場合は、アプリケーショ ンのオプションを選択してExport[エクスポート] をクリックしま す。プロンプトに従ってファイルを保存します。
アプリケーション設定 テーブルのエクスポート	PDF/CSV 形式のすべてのアプリケーション上の情報をエクス ポートします。Web インターフェイスで表示される列のみエクス ポートされます。Export Configuration Table Data(設定バンドル データのエクスポート)を参照してください。
新しいコンテンツ リリー スのインストール後のポ リシーへの影響を評価す る	コンテンツリリースバージョンのインストール前とインストール 後における、アプリケーションに対するポリシーの実施状況を確 認する場合は、Review Policies (ポリシーの確認)を行います。[ポ リシーのプレビュー] ダイアログを使用すると、ダウンロード したコンテンツ リリース バージョンに含まれている新規アプ リケーションによるポリシーへの影響を確認できます。Policy Review (ポリシーのプレビュー) ダイアログでは、既存のセキュ リティ ポリシー ルールの保留中のアプリケーション (コンテン ツリリース バージョンでダウンロードされているが、ファイア ウォールにインストールされていないアプリケーション) を追 加または削除できます。保留中のアプリケーションのポリシーを 変更しても、対応するコンテンツ リリース バージョンがインス トールされるまで有効になりません。Policy Review (ポリシー のプレビュー) ダイアログは、Device (デバイス) > Dynamic Updates (動的更新) ページでコンテンツ リリース バージョンを ダウンロードおよびインストールする際にも使用できます。
アプリケーションにタグ 付けする	SaaSアプリケーションのタグ付け用にsanctioned[許可済み] という名前のタグが事前設定されています。SaaSアプリケーションとは、そのアプリケーション特性の詳細においてSaas=yesと識別されているものを指しますが、許可済みタグはすべてのアプリケーションに使用可能なものです。
	 アプリケーションにsanctioned (許可)というタグを 付け、例えば SaaS アプリケーションの利用状況 レポートを検証する際やネットワーク上のアプリ ケーションを評価する際に、許可された SaaS アプ リケーションのトラフィックと許可されていない SaaS アプリケーションのトラフィックとを区別し ます。

アプリケーションでサ ポートされる操作	の意味
	アプリケーションを選択して、Edit Tags(タグの編集)をクリック し、ドロップダウンから事前定義済みのSanctioned(許可済み)タ グを選択して、ネットワークで明示的に許可するアプリケーショ ンを特定します。また、SaaS アプリケーション使用状況レポート を生成すると(「Monitor(監視) > PDF Reports(PDF レポー ト) > SaaS Application Usage(Saas アプリケーションの使用状 況)」を参照)、ネットワーク上で使用されている許可済みのア プリケーションの統計値と未許可の SaaS アプリケーションの統 計値を比較することができます。
	アプリケーションを許可済みとタグ付けする場合、以下の制限が 課せられます。
	 許可済みのタグは、アプリケーショングループに適用すること ができません。
	 許可済みのタグはShared[共有] レベルでは適用することができ ません。デバイスグループあるいは仮想システムにつき1つの アプリケーションのみタグ付けすることができます。
	 許可済みのタグは、facebookコンテナアプリの一部であるfacebookメールなど、コンテナアプリに含まれるアプリケーションには使用することができません。
	さらに、Remove tag[タグの除去] またはOverride tag[タグのオー バーライド] をすることも可能です。オーバーライドのオプショ ンは、デバイスグループの設定をPanoramaからのプッシュにより 継承したファイアウォールのみにおいて使用可能です。

アプリケーションの定義

ポリシーを適用する際にファイアウォールの評価対象とする新しいカスタムアプリケーション をAdd[追加] する場合は、Objects[オブジェクト] > Applications[アプリケーション] のページを 使用します。

新しいアプリケーショ ン設定	の意味
Configuration [設定] タブ	
氏女	マプリケーションタ(目上の古字)なりもります。この名前は

氏名	アプリケーション名(最大 31 文字)を入力します。この名前は、
	セキュリティ ポリシーを定義するときにアプリケーションのリス
	トに表示されます。名前の大文字と小文字は区別されます。また、
	一意の名前にする必要があります。文字、数字、スペース、ピリオ

新しいアプリケーショ ン設定	の意味
	ド、ハイフン、およびアンダースコアのみを使用してください。先 頭は文字にする必要があります。
共有	以下に対してアプリケーションを公開する場合は、このオプション を選択します。
	 multi-vsys ファイアウォールの各仮想システム (vsys)。この選択 を解除すると、Objects[オブジェクト] タブで選択した Virtual System[仮想システム] のみに対してアプリケーションが公開さ れます。
	 Panorama 上の各デバイス グループ。この選択を解除する と、Objects[オブジェクト] タブで選択した Device Group[デバ イスグループ] のみに対してアプリケーションが公開されます。
オーバーライドの無効 化(<mark>Panoramaのみ</mark>)	管理者が、このオブジェクトを継承するデバイス グループのこのア プリケーション オブジェクトの設定をオーバーライドすることを防 ぐには、このオプションを選択します。デフォルトでこのオプショ ンはオフになっており、管理者は、このオブジェクトを継承するデ バイス グループの設定をオーバーライドできます。
の意味	アプリケーションの一般的な説明を入力します (最大 255 文字)。
カテゴリ	アプリケーションのカテゴリ (email や database など) を選択しま す。このカテゴリは、Top Ten Application Categories(トップ 10 のアプリケーション カテゴリ)チャートの生成に使用され、フィル タリングに使用できます(「ACC」を参照)。
サブカテゴリ	アプリケーションのサブカテゴリ (email や database など)を選択し ます。このサブカテゴリは、Top Ten Application Categories(トッ プ 10 のアプリケーション カテゴリ)チャートの生成に使用され、 フィルタリングに使用できます(「ACC」を参照)。
テクノロジ	アプリケーションのテクノロジを選択します。デフォルトで は、Technology 列は表示されません。テクノロジー列を表示し て、アプリケーションフィルターに追加するテクノロジーを選択し ます。
親アプリケーション	このアプリケーションの親アプリケーションを指定します。この設 定は、セッションが親アプリケーションとカスタム アプリケーショ ンの両方に一致する場合に適用されます。ただし、カスタム アプリ ケーションの方が詳細であるためカスタム アプリケーションがレ ポートされます。

新しいアプリケーショ ン設定	の意味
リスク	アプリケーションに関連付けられているリスク レベル (1 = 最低 ~ 5 = 最高) を選択します。
特徴	アプリケーションを危険にさらす可能性のあるアプリケーションの 特徴を選択します。各特徴の詳細は「特徴」を参照してください。

Advanced Tab(詳細タブ)

ポート	アプリケーションで使用するプロトコルが TCP や UDP の場 合、Port[ポート] を選択してプロトコルとポート番号の組み合わせ を 1 つ以上入力します (1 行ごとに 1 エントリ)。一般的な形式は以 下のとおりです。
	<protocol>/<port></port></protocol>
	ここで、 <port>は、単一のポート番号を、dynamicは動的ポート割 り当てになります。</port>
	例:TCP/dynamic または UDP/32
	セキュリティ ルールのサービス列に app-default を使用すると、こ の設定が適用されます。
IP プロトコル	TCP や UDP 以外の IP プロトコルを指定するには、IP Protocol[IP プロトコル] を選択してプロトコル番号 (1 ~ 255) を入力します。
ICMP タイプ	Internet Control Message Protocol バージョン 4 (ICMP) タイプを指定するには、ICMP Type[ICMPタイプ] を選択し、タイプの番号を入力します (範囲は 0 ~ 255)。
ICMP6 タイプ	Internet Control Message Protocol バージョン 6 (ICMPv6) タイプを 指定するには、ICMP6 Type[ICMP6 タイプ] を選択し、タイプの番 号を入力します (範囲は 0 ~ 255)。
まったくない	プロトコルに依存しないシグネチャを指定するには、None[なし] を選択します。
タイムアウト	アイドル状態のアプリケーションフローが停止するまでの秒数(範囲は0~604800秒)を入力します。0は、アプリケーションのデフォルトのタイムアウトが使用されることを示します。この値は、すべてのケースで TCP および UDP 以外のプロトコルに使用されます。また、TCP タイムアウトと UDP タイムアウトが指定されていない場合は、TCP と UDP のタイムアウトに使用されます。

新しいアプリケーショ ン設定	の意味
TCP タイムアウト	アイドル状態のTCPアプリケーションフローが停止するまでの秒数 (範囲は0~604800秒)を入力します。0 は、アプリケーションの デフォルトのタイムアウトが使用されることを示します。
UDP タイムアウト	アイドル状態のUDPアプリケーションフローが停止するまでの秒数 (範囲は0~604800秒)を入力します。0は、アプリケーションの デフォルトのタイムアウトが使用されることを示します。
TCPハーフクローズド	最初のFINを受信してから、2つ目のFINまたはRSTを受信するまでの間、セッションがセッションテーブル内に保持される最大時間を入力します。タイマーが期限切れになるとセッションが閉じられます。
	デフォルト:このタイマーがアプリケーションレベルで設定 されていない場合、グローバル設定が使用されます(範囲 は1~604800秒)。
	この値がアプリケーション レベルで設定されている場合、その値で グローバル TCP Half Closed 設定がオーバーライドされます。
TCP待ち時間	2つ目のFINまたはRSTを受信してから、セッションがセッション テーブル内に保持される最大時間を入力します。タイマーが期限切 れになるとセッションが閉じられます。
	デフォルト:このタイマーがアプリケーションレベルで設定されてい ない場合、グローバル設定が使用されます(範囲は1~600秒)。
	この値がアプリケーション レベルで設定されている場合、その値で グローバル TCP Time Wait 設定がオーバーライドされます。
スキャン	セキュリティプロファイル(ファイルタイプ、データパターン、お よびウイルス)に基づいて、許可するスキャンタイプを選択しま す。

Signatures [シグネチャ] タブ

★上のセグメントに訳 文をまとめました★	Add[追加] をクリックして新しいシグネチャを追加し、以下の情報 を指定します。
	 Signature Name[シグネチャ名] – シグネチャの識別に使用する 名前を入力します。
	● Comment[コメント] − 任意で説明を入力します。
	• Ordered Condition Match[順番が付けられた条件の一致] – シグ ネチャの条件の定義順序が重要である場合に選択します。

新 ン

しいアプリケーショ 設定	の意味
	 Scope[範囲] – このシグネチャを現在のTransaction[トランザクション]のみに適用するか、またはユーザーSession[セッション] 全体に適用するかを選択します。
	シグネチャの識別条件を指定するこれらの条件は、ファイアウォー ルがアプリケーションパターンを識別し、トラフィックを制御する 場合に使用するシグネチャを生成する際に使用されます。
	 Add AND Condition (AND条件を追加) または Add OR Condition (OR条件を追加)をクリックして条件を追加します。グループ内 に条件を追加するには、グループを選択して Add Condition[条 件の追加] をクリックします。
	 ドロップダウンリストからOperator[演算子] を選択します。 選択肢にはPattern Match[パターンマッチ]、Greater Than[超 過]、Less Than[未満]、およびEqual To[等しい] があり、それぞ れについて以下のオプションを指定します。
	(パターン マッチの場合のみ)
	 Context[コンテクスト] – 使用可能なコンテクストから選択します。これらのコンテクストは動的コンテンツアップデートにより更新されます。
	 Pattern[パターン] – カスタムアプリケーションに適用された、一意のコンテクスト文字列を指定するための正規表現を指定します。
	 コンテクスト特定のため、パケット キャプチャ を実行してください。正規表現のパターンの ルールに関する詳細は「パターンのルールの構 文」を参照してください。
	(Greater Than (超過)、Less Than(未満)の場合)
	 Context[コンテクスト] – 使用可能なコンテクストから選択します。これらのコンテクストは動的コンテンツアップデートにより更新されます。
	 Value[値] – 一致検索を行う値を指定します(範囲 は0~4294967295)。
	• Qualifier and Value – (任意)修飾子/値のペアを追加します。
	(Equal To(等しい)の場合のみ)
	 Context(コンテクスト) – TCP または UDP 宛ての不明な要 求や応答(unknown-req-tcp など)、または動的コンテンツ

新しいアプリケーショ ン設定	の意味
	アップデートにより入手可能な追加コンテクスト(dnp3-req- func-code など)から選択します。
	TCPまたはUDPの不明な要求や応答の場合は、以下を指定し ます。
	 Position[位置] – ペイロードの最初の4バイトまたは2番目の4バイトのいずれかを選択します。
	 Mask[マスク] – 4 バイトの 16 進数値を指定します (たとえば、0xffffff00)。
	 Value[値] – 4 バイトの 16 進数値を指定します (たとえば、Oxaabbccdd)。
	他のコンテクストに関しては、そのアプリケーションに関連の ある Value [値] を指定します。
	グループ内で条件を移動するには、条件および Move Up[上へ] また は Move Down[下へ] を選択します。グループを移動するには、グ ループを選択して Move Up[上へ] または Move Down[下へ] を選択 します。グループ間で条件を移動することはできません。

アプリケーションの使用目的がアプリケーションオーバーライドルールのみである場合、アプリケーションのシグネチャを指定する必要はありません。

Objects > Application Groups [オブジェクト > アプリ ケーション グループ]

セキュリティ ポリシーの作成を簡略化するには、アプリケーション グループを作成して、同じ セキュリティ設定が必要なアプリケーションをまとめることができます(新しいアプリケーショ ンを定義するには、「アプリケーションの定義」を参照してください)。

新しいアプリケーショ ン グループ設定	の意味
氏名	アプリケーション グループを表す名前 (最大 31 文字)を入力しま す。この名前は、セキュリティ ポリシーを定義するときにアプリ ケーションのリストに表示されます。名前の大文字と小文字は区別 されます。また、一意の名前にする必要があります。文字、数字、 スペース、ハイフン、およびアンダースコアのみを使用してくださ い。
共有	以下に対してアプリケーショングループを公開する場合は、このオ プションを選択します。
	multi-vsys ファイアウォールの各仮想システム (vsys)。この選択 を解除すると、Objects[オブジェクト] タブで選択した Virtual System[仮想システム] のみに対してアプリケーショングループが公 開されます。
	Panorama 上の各デバイス グループ。この選択を解除する と、 Objects [オブジェクト] タブで選択した Device Group [デバイ スグループ] のみに対してアプリケーショングループが公開されま す。
オーバーライドの無効 化(Panoramaのみ)	このアプリケーション グループ オブジェクトの設定が、このオブ ジェクトを継承したデバイス グループで管理者によりオーバーラ イドされることを防止するには、このオプションを選択します。デ フォルトでこのオプションはオフになっており、管理者は、このオ ブジェクトを継承するデバイス グループの設定をオーバーライドで きます。
アプリケーション [applications]	Add[追加] をクリックし、このグループに含めるアプリケーショ ン、アプリケーション フィルタ、および他のアプリケーション グ ループを選択します。

Objects > Application Filters [オブジェクト > アプリ ケーションフィルタ]

アプリケーションフィルタは、繰り返される検索を簡略化するのに役立ちます。アプリケー ションフィルタを定義するには、新しいフィルタを Add(追加)して、その名前を入力しま す。ウィンドウの上部で、フィルタリングの基準として使用する項目をクリックします。たとえ ば、Collaboration [コラボレーション]カテゴリのみをリストに表示するには、collaboration をク リックします。

	Q) All	~	\times	Clear Filters				
	SUBCATEGORY A			RISK A	TAGS 🔿			CHARACTERISTIC
	85 email			47 1	45 Entorn	rice VolD		61 Evasive
	146 instant-messa	ging		59 0	45 Enterp	nse voir		92 Excessive Ba
	75 internet-conf	erencing		58 2	143 Web A	рр		3 FEDRAMP
	50 social-busines	.c		39 3				15 HIPAA
	130 social-networ	king		23 4			9 IP Based Res	
	98 voin-video			6 5				2 New App-ID
	50 web-nosting							60 No Certificat
	50 Heb posting			_				7.00
	LOCATION	CATEGORY	SUE	BCATEGORY	RISK	TAGS		
		collaboration	inter	net-conferencing	3	Web App		
		collaboration	voip	-video	2			
		collaboration	inter	net-conferencing	4	Web App		
		collaboration	voip	-video	1	Web App		
wn)								
		collaboration	inter	met-conferencing	1	Enterprise We	b App	
haring		collaboration	inter	met-conferencing	3	Enterprise We	b App	
		collaboration	voip	-video	1	Enterprise We	b App	
		collaboration	voip	-video	2	Web App		
		collaboration	inter	met-conferencing	3	Web App		
		collaboration	inter	met-conferencing	1	Enternrise		
Revert	↑ Move 🕞 Clone	🕢 Enable 🚫 Disab	le 🚽	Import Expor	t DPF/CSV R	eview Policies Edit	Tags	

その他の列にフィルタを適用するには、列のエントリを選択します。フィルタリングは連続的 で、カテゴリフィルタ、次にサブカテゴリフィルタ、テクノロジーフィルタ、リスクフィル タ、タグ、最後に特性フィルタの順に適用されます。

選択したフィルタに応じて、ページに表示されるアプリケーションのリストが自動的に更新され ます。

Objects > Services [オブジェクト > サービス]

特定のアプリケーションにセキュリティ ポリシーを定義する場合、1つ以上のサービスを選択して、アプリケーションが使用できるポート番号を制限できます。デフォルトのサービスは、any (すべて) で、すべての TCP ポートと UDP ポートが許可されます。HTTP サービスとHTTPS サービスは事前に定義されていますが、他のサービスの定義を追加することができます。多くの場合、一緒に割り当てられるサービスをサービス グループに組み合わせて、セキュリティ ポリシーの作成を簡略化することができます (オブジェクト>サービス グループ を参照)。

さらに、サービス オブジェクトを使用してサービス ベースのセッション タイムアウトを指定 することができます。つまり、同じグループのユーザーまたはグループが同じ TCP または UDP サービスを使用していても、異なるタイムアウトを適用することができます。 アプリケーショ ンベースのセキュリティ ポリシーをカスタム アプリケーションと共にアプリケーションベース のセキュリティ ポリシーに適用すると、カスタム アプリケーションのタイムアウトを容易に維 持できます。

サービス設定	の意味
氏名	サービス名 (最大 63 文字) を入力します。この名前は、セキュリ ティポリシーを定義するときにサービスリストに表示されます。名 前の大文字と小文字は区別されます。また、一意の名前にする必要 があります。文字、数字、スペース、ハイフン、およびアンダース コアのみを使用してください。
の意味	サービスの説明を入力します (最大 1023 文字)。
共有	 以下に対してサービスオブジェクトを公開する場合は、このオプションを選択します。 multi-vsys ファイアウォールの各仮想システム (vsys)。この選択を解除すると、Objects[オブジェクト] タブで選択した Virtual System[仮想システム]のみに対してサービスオブジェクトが公開されます。 Panorama 上の各デバイス グループ。この選択を解除すると、Objects[オブジェクト] タブで選択したDevice Group[デバイスグループ] のみに対してサービスオブジェクトが公開されます。
オーバーライドの無効 化(Panoramaのみ)	管理者が、オブジェクトを継承するデバイス グループのこのサービ スオブジェクトの設定をオーバーライドすることを禁止する場合は このオプションを選択してください。デフォルトでこのオプション はオフになっており、管理者は、このオブジェクトを継承するデバ イス グループの設定をオーバーライドできます。

以下の表では、サービス設定について説明します。

サービス設定	の意味
PROTOCOL	サービスで使用するプロトコル (TCP または UDP) を選択します。
Destination port	サービスで使用する宛先ポート番号 (0 ~ 65535) またはポート番号 の範囲 (ポート 1 ~ ポート 2) を入力します。複数のポートまたは ポートの範囲はコンマで区切ります。宛先ポートは必須です。
Source port	サービスで使用する送信元ポート番号 (0 ~ 65535) またはポート番号の範囲 (ポート 1 ~ ポート 2) を入力します。複数のポートまたはポートの範囲はコンマで区切ります。送信元ポートは任意です。
セッション タイムアウ ト	以下のサービスに対するセッションタイムアウトを定義します。 Inherit from application (アプリケーションから継承) (デフォルト) – サービス ベースのタイムアウトは適用されず、アプリケーションのタイムアウトが適用されます。 Operation (オーバーライド) サービスに対するカスクレカッ
	 Override (オーハーフィト) ーサービスに対するカスタムセッション タイムアウトを定義します。TCPタイムアウト、TCP ハーフクローズド、および TCP 待機時間フィールドへの値の入力を続行します。

次の設定は、アプリケーション タイムアウトを無効にして、サービスのカスタム セッション タイムアウトを作成する場合にのみ表示されます。

TCP タイムアウト	データの送信が開始された後に TCP セッションを開いたままにで きる最大時間を秒単位で設定します。これが期限切れになるとセッ ションが閉じます。 範囲は 1 ~ 604800 です。デフォルト値は 3600 秒です。
TCPハーフクローズド	 接続の一方の側だけが接続を終了しようとしたときにセッションが開いたままになる最大時間(秒)を設定します。 この設定は次の場合に適用されます。 ファイアウォールが最初の FIN パケットを受信した後(接続の一方の側がセッションを終了しようとしていることを示す)、第2の FIN パケットを受信する前(接続の相手側がセッションを終了していることを示す)、 RST パケットを受信する前の期間(接続のリセットを示す)。 タイマーが期限切れになるとセッションが閉じます。 範囲は 1~604800 です。デフォルト値は120 秒です。
TCP 待機時間	セッションを終了するために必要な 2 つの FIN パケットのうちの 2 番目を受信した後、または接続をリセットするために RST パケット

サービス設定	の意味
	を受信した後、セッションが開いたままになる最大時間を、秒単位 で設定します。
	タイマーが期限切れになるとセッションが閉じます。
	範囲は 0 ~600 です。デフォルト値は 15 秒です。

Objects(オブジェクト) > Service Groups(サービス グループ)

セキュリティ ポリシーの作成を簡略化するには、セキュリティ設定が同じであることが多 いサービスをサービス グループにまとめます。新しいサービスを定義する方法については、 「Objects(オブジェクト) > Services(サービス)」を参照してください。

以下の表では、サービス グループ設定について説明します。

サービス グループ設定	の意味
氏名	サービス グループ名 (最大 63 文字) を入力します。この名前は、セ キュリティ ポリシーを定義するときにサービスのリストに表示され ます。名前の大文字と小文字は区別されます。また、一意の名前に する必要があります。文字、数字、スペース、ハイフン、およびア ンダースコアのみを使用してください。
共有	以下に対してサービスグループを公開する場合は、このオプション を選択します。
	 multi-vsys ファイアウォールの各仮想システム (vsys)。この選択 を解除すると、Objects[オブジェクト] タブで選択した Virtual System[仮想システム] のみに対してサービスグループが公開さ れます。
	 Panorama 上の各デバイス グループ。この選択を解除する と、Objects[オブジェクト] タブで選択したDevice Group[デバイ スグループ] のみに対してサービスグループが公開されます。
オーバーライドの無効 化(<mark>Panorama</mark> のみ)	管理者が、オブジェクトを継承するデバイス グループのこのサービ ス グループ オブジェクトの設定をオーバーライドすることを禁止 する場合はこのオプションを選択してください。デフォルトでこの オプションはオフになっており、管理者は、このオブジェクトを継 承するデバイス グループの設定をオーバーライドできます。
サービス	Add[追加] をクリックしてグループにサービスを追加します。ド ロップダウンリストから選択するか、ドロップダウンリストの下部 にある Service[サービス] をクリックして設定を指定します。設定 の詳細は、Objects(オブジェクト) > Services(サービス)を参照 してください。
Objects > Tags [オブジェクト > タグ]

タグを使用すると、キーワードまたは語句を使用してオブジェクトをグループ化できます。アド レスオブジェクト、アドレスグループ(静的および動的)、アプリケーション、ゾーン、サー ビス、サービスグループ、およびポリシールールにタグを適用できます。SD-WAN インター フェイスプロファイルを使用して、イーサネットインターフェースにリンクタグを適用するこ ともできます。タグを使用すると、オブジェクトをソートまたはフィルタリングしたり、オブ ジェクトを色で視覚的に識別したりできます。タグに色を付けると、Policy(ポリシー)タブに表 示されるオブジェクトに背景色が付けられます。

タグを使ってルールをグループ化するには、事前にそのタグを作成しておく必要があります。タ グでグループ化したルールを適用した後、View Rulebase as Groups (ルールベースをグループと して表示)し、割り当てられたタグに基づいてポリシー ルールベースが表示されることを確認し ます。ルールベースをグループとして閲覧する際、ポリシーの順序と優先順位が保持されます。 このビューでグループ タグを選択すれば、すべてのルールをタグでグループ化して表示できま す。

アプリケーションのタグ付けには**Sanctioned**[許可済み] という事前設定済みのタグを使用可能 です(**Objects > Applications**[オブジェクト > アプリケーション])。これらのタグは、正確 なMonitor(監視) > PDF Reports(PDF レポート) > SaaS Application Usage(Saas アプリ ケーションの使用状況)に必要です。

知りたい内容	以下を参照		
タグの作成方法	タグの作成		
ルールベースをグループとし て表示する方法は?	ルールベースをグループとして表示		
タグ付けされたルールを検索 する。	タグの管理		
タグを使用してルールをグ ループ分けする。			
ポリシーで使用されているタ グを確認する。			
タグをポリシーに適用しま す。			
その他の情報をお探しです か?	 タグを使用したオブジェクトのグループ化および視覚的な区別 SD-WAN Link Tag (SD-WAN リンク タグ) 		

タグの作成

オブジェクト > tags

Tags (タグ**)**を選択し、タグの作成、色の割り当て、タグの削除、名前の変更、コピーができま す。各オブジェクトには最大 64 個のタグを付けることができます。オブジェクトに複数のタグ がある場合、適用された最初のタグの色が表示されます。

ファイアウォールで、**Tags** (タグ)タブを選択すると、ファイアウォール上でローカルに定 義したタグ、または Panorama からファイアウォールにプッシュされたタグが表示されま す。Panorama の**Tags** (タグ)タブには、Panorama で定義したタグが表示されます。このタブに は、ファイアウォール上に定義された VM 情報の送信元から動的に取得され動的 アドレス グ ループを形成するタグ、または XML あるいは REST API を使用して定義されたタグは表示され ません。

新規のタグを作成すると、ファイアウォールまたはPanoramaで現在選択されている仮想システムまたはデバイスグループで、そのタグが自動的に作成されます。

タグ設定	の意味			
氏名	一意のタグ名 (最大 127 文字) を入力します。名前では大文字と小 文字は区別されません。			
共有	 以下に対してタグを公開する場合は、このオプションを選択します。 multi-vsys ファイアウォールの各仮想システム (vsys)。この選択を解除すると、Objects (オブジェクト) タブで選択した Virtual System (仮想システム)のみに対してタグが公開されます。 Panorama 上の各デバイス グループ。このオプションを無効化(クリア)すると、Objects (オブジェクト) タブで選択した Device Group (デバイスグループ) のみに対してタグが公開されます。 			
オーバーライドの無効 化(Panoramaのみ)	管理者が、このタグを継承するデバイス グループのこのタグの設定 をオーバーライドすることを防ぐには、このオプションを選択しま す。デフォルトでこのオプションはオフになっており、管理者は、 このタグを継承するデバイス グループの設定をオーバーライドでき ます。			
カラー	ドロップダウン リストのカラー パレットから、色を選択します (デフォルトは None (なし))。			
コメント	タグの用途を示すラベルまたは説明を追加します。			

• タブの追加:タグをAdd (追加)して次の各フィールドを入力します:

Policies[ポリシー] タブでポリシーを作成または編集する際に、新規のタグを作成することもできます。タグは、現在選択されているデバイス グループまたは仮想システムで自動的に作成されます。

- タグの編集:編集、名称変更、あるいは色を割り当てるタグをクリックします。
- タグの削除:Delete (削除)をクリックしてタグを選択します。事前定義されたタグを削除する ことはできません。
- タグの移動またはコピー:タグを移動またはコピーするオプションを使用すると、マルチ仮想システムが有効になっているファイアウォール上の異なるデバイスグループまたは仮想システムにタグをコピーまたは移動できます。

Move or Clone [移動またはクローン]を実行しタグを選択します。Destination (宛先) となる場所(デバイス グループまたは仮想システム)を選択します。検証プロセスにおいて、エラーの表示を行う前にオブジェクトに含まれるすべてのエラーを検出させたい場合は、Error out on first detected error in validation (検出中に最初にエラーを検出した時点でエラーを表示)のオプションを無効化(クリア)します。デフォルトではこのオプションが有効になっているため、検証プロセスは最初のエラーが検出された時点で停止され、そのエラーのみが表示されます。

 タグをオーバーライドする/元に戻す(Panoramaのみ):タグの作成時に Disable override (オーバーライドの無効化)オプションを選択していない場合は、Override (オーバーライド)オ プションを使用できます。Override (オーバーライド)オプションを使用すると、共有または先 祖デバイス グループから継承したタグに割り当てられたカラーをオーバーライドできます。 現在のデバイス グループがLocation (場所)になります。また、Disable override (オーバーライ ドを無効化)して今後のオーバーライドの試みを防ぐこともできます。

タグに加えた最近の変更を取り消す場合は変更を**Revert (**取り消し**)**ます。タグを元に戻す と、Location[場所] フィールドに、タグの継承元のデバイス グループまたは仮想システムが 表示されます。

ルールベースをグループとして表示

ポリシー > <Rulebase Type>

View Rulebase as Groups (ルールベースをグループとして表示)すれば、グループ タグを使って ポリシー ルールベースを表示できます。ルールベースをグループとして閲覧する際、ポリシー の順序と優先順位が保持されます。このビューでグループ タグを選択すれば、すべてのルール をタグでグループ化して表示できます。

ルールベースをグループとして表示しながら、Group (グループ)をクリックすれば選択したタグ グループ内のすべてのルールを移動、変更、削除、コピーできます。次の表は、ルールベースを グループとして表示する際に利用できるルールの管理オプションを示しています。

オプション	の意味
グループ内の結果を別	選択したルールベースあるいはデバイスグループ内のすべてのポリ
のルールベースあるい	シールールを別のタグ グループに移動させます。

オプション	の意味
はデバイスグループに 移動	
すべてのルールのグ ループを変更	選択したタグ グループ内のすべてのルールを別のタグ グループに 移動させます。
グループ内のすべての ルールを移動	ルールベース内の選択したタグ グループに含まれるすべてのルール を移動させます。
グループ内のすべての ルールを削除	選択したタグ グループ内のすべてのルールを削除します。
グループ内のすべての ルールをコピー	選択したタグ グループ内のすべてのルールをコピーします。

グループ内の結果を別のルールベースあるいはデバイスグループに移動

ルールベースを整理する必要がある場合、移動したいルールを含んでいるタグ グループを選択 して**Move Rules in Group to Different Rulesbase or Device Group (**グループ内のルールを別の ルールベースあるいはデバイスグループに移動**)**し、(個々のルールを個別に移動するのではな く)それらを別のルールベースあるいはデバイスグループに割り当て直します。タグ グループ 内のルールを別のデバイスグループに移動する前に、デバイスグループがすでに存在していなく てはなりません(移動中は作成できません)。さらに、タグ グループ内のルールを同じデバイ スグループ内の別のルールベースに移動できます。

ルールを別のルールベースあるいはデバイスグループに移動させる場合は次の項目を入力しま す:

項目	の意味			
宛先	ポリシールールを移動させる対象のデバイスグループです。			
(<mark>Panorama のみ</mark>)宛 先タイプ	ルールを宛先デバイスグループのPre-Rulebase (プレ ルールベー ス)あるいはPost-Rulebase (ポスト ルールベース)のどちらに移動す るのか選択します。			
ルール順序	ルールをルールベースのどこに移動するのか選択します。選択肢は 以下のとおりです。			
	 Move Top (最上部へ移動)–ルールを宛先デバイスグループの ルールベースの一番上に移動します。 			
	 Move Bottom (最下部へ移動)–ルールを宛先デバイスグループの ルールベースの最後に移動します。 			
	 Before Rule (ルールの前)–ルールを宛先デバイスグループのルー ルベース内で選択したルールの前に移動します。 			

項目	の意味				
	 After Rule (ルールの後)–ルールを宛先デバイスグループのルー ルベース内で選択したルールの後に移動します。 				
検証で最初に検出され たエラーに起因するエ ラーが発生しました	このボックスにチェックを入れれば、検証中にエラーが発生した 場合にエラーを表示する方法を指定できます。チェックを入れた場 合、各エラーが個別に表示されます。チェックを入れない場合、各 エラーが集約されて単一のエラーとして表示されます。				
	検証中にエラーが検出されるとルールの移動ジョブが失敗し、宛先 デバイスグループにルールが移動されません。				

すべてのルールのグループを変更

各ルールを編集するのではなく、Change Group of All Rules (すべてのルールのグループを変 更)してポリシールールセット全体をあるタグ グループから既存の別のタグ グループに移動させ ます。新しいタグ グループに移動させる際、タグ グループ ルールのルールの順序が保持されま すが、新しいルールを宛先タグ グループ内のルールの前に置くか、後ろに置くかを選択できま す。

ルールを別のタグ グループに移動させるには、宛先タグ グループと移動させるルールの配置場 所を指定します。

項目	の意味
表示順序の Group (グ ループ) を選択します	宛先タグ グループを選択します。
最上部へ移動	Move Top (最上部へ移動)はルールを宛先タグ グループの一番上に 挿入します。
最下部へ	Move bottom (最下部へ移動)はルールを宛先タグ グループの一番下に挿入します。

グループ内のすべてのルールを移動

各ルールの順序を個別に変えるのではなく、Move All Rules in Group (グループ内のすべての ルールを移動)して選択中のタグ グループ内のすべてのルールをルール階層の上下に移動させま す。新しいタグ グループに移動させる際、タグ グループ ルール内の移動されたルールの順序が 保持されますが、ルールを宛先タグ グループ内のルールの前に置くか、後ろに置くかを選択で きます。

ルールを移動させるには、宛先タググループと移動させるルールの配置場所を指定します。

項目	の意味
表示順序の Group (グ ループ) を選択します	宛先タグ グループを選択します。
最上部へ移動	Move Top (最上部へ移動)はルールを宛先タグ グループの前に挿入 します。
最下部へ	Move bottom (最下部へ移動)はルールを宛先タグ グループの後に挿入します。

グループ内のすべてのルールを削除

Delete All Rules in Group (グループ内のすべてのルールを削除)で選択したタグ グループに関連 する使用していない、あるいは不要なルールを削除することで、セキュリティリスクを減らし、 ポリシー ルールベースを整理し、ルールの管理を簡単にすることができます。

グループ内のすべてのルールをコピー

タグ グループ内の既存のポリシールールを手作業で作成し直すのではなく、Clone All Rules in Group (グループ内のすべてのルールをコピー)すれば、任意のルールベースおよびデバイスグループに含まれる選択済みのタグ グループ内のルールを素早く複製できます。タグ グループ内のルールを別のデバイスグループにコピーする前に、デバイスグループがすでに存在していなくてはなりません(コピー中は作成できません)。さらに、タグ グループ内のルールを同じデバイスグループ内の別のルールベースにコピーできます。

複製されたルールには、ルール名と次の形式が付加されます: <Rule Name> -1 .最初にコ ピーしたルールと同じ場所にルールをコピーし、かつ名前が変化しない場合、名前が付与されま す。たとえば、<Rule Name>-2、<Rule Name>-3 などです。

項目	の意味
宛先	コピー対象のポリシールールのターゲット デバイスグループ。
(<mark>Panorama のみ</mark>)宛 先タイプ	ルールを宛先デバイスグループのPre-Rulebase (プレ ルールベー ス)あるいはPost-Rulebase (ポスト ルールベース)のどちらにコピー するのか選択します。
ルール順序	ルールをルールベースのどこにコピーするのか選択します。選択肢 は以下のとおりです。
	 Move Top (最上部へ移動)-コピーしたルールを宛先デバイスグ ループのルールベースの一番上に挿入します。
	 Move Bottom (最下部へ移動)-コピーしたルールを宛先デバイス グループのルールベースの最後に挿入します。

ルールをコピーする場合は以下のフィールドを設定します。

項目	の意味				
	 Before Rule (ルールの前)-コピーしたルールを宛先デバイスグ ループのルールベース内で選択したルールの前に挿入します。 				
	 After Rule (ルールの後)-コピーしたルールを宛先デバイスグ ループのルールベース内で選択したルールの後に挿入します。 				
検証で最初に検出され たエラーに起因するエ ラーが発生しました	このオプションを選択すれば、検証中にエラーが発生した場合にエ ラーを表示する方法を指定できます。有効な場合、各エラーが個別 に表示されます。無効(クリア)な場合、各エラーが集約されて単 一のエラーとして表示されます。				
	検証中にエラーが検出されるとルールのコピージョブが失敗し、宛 先デバイスグループにルールがコピーされません。				

タグの管理

ルールをグループ タグでグループ化した際に実行できるアクションを次の表に示します。

ルールにタグ付けする。

- 1. View Rules as Groups (ルールをグループとして表示)を選択します。
- 2. 右ペインで一つ以上のルールを選択します。
- 3. グループ タグのドロップダウンリストでApply Tag to the Selected Rules (選択中のルー ルにタグを適用)します。

🛱 Filter
Append Rule
Move Selected Rule(s)
 Apply Tag to the Selected Rule(s)
UnTag Selected Rule(s)
🔍 Global Find: none

4. 選択したルールにタグを追加します。



グループタグに割り当てられたルールを表示します。

- 1. View Rulebase as Groups (ルールベースをグループとして表示)してルールが割り当て られているグループ タグを表示します。
- 2. 右ペインが更新され、選択したいずれかのタグを含むルールおよびグループ タグが表示されます。
- グループ タグを選択し、対象のグループに割り当てられているルールを表示します。 グループ タグが割り当てられていないルールはnone (なし)グループのところにリスト アップされます。

ルールのタグを外す。

- 1. View Rulebase as Groups (ルールベースをグループとして表示)してルールが割り当て られているグループ タグを表示します。
- 2. 右ペインで一つ以上のルールを選択します。
- 3. グループ タグのドロップダウンリストでApply Tag to the Selected Rules (選択中のルー ルにタグを適用)します。



4. 選択したルールのタグを削除します。さらに、ルールに割り当てられたタグをDelete All (すべて削除)することができます。



タグを使用してルールを並べ替える。

View Rulebase as Groups (ルールベースをグループとして表示**)**しながら、グループ タグ内の ルールを一つ以上選択し、ルール番号にカーソルを合わせてドロップダウンリストで**Move** Selected Rule(s) (選択中のルールを移動)を選択します。選択中のグループ タグに含まれるす べてのルールを移動する場合は、ルールを選択しないでください。

none (3)	1-3	4	test-rule2		
		- 5	test-rule5		
GroupTag2 (4)	🛱 Filter				
GroupTag3 (1)	Append Rule				
GroupTag (1)		Move Selected Rule(s)			
	2	Apply Tag to the Selected Rule(s)			
	2	UnTag	Selected Rule(s)		
	٩	Global	Find: GroupTag2		

move rule (ルールの移動) ウィンドウのドロップダウンリスト リストからグループ タグを 選択し、ドロップダウンリスト リストで選択したタグの Move Before (前に移動) するの か、Move After (後に移動) するのかを選択します。

選択したタグに適用する新しいルールを追加する。

View Rulebase as Groups (ルールベースをグループとして表示)しながら、グループ タグに カーソルを合わせてドロップダウンリストでAppend Rule (ルールを付与)を選択します。

グループ タグに割り当てられたルールのリストの最後に新しいルールが追加されます。

グループタグを検索します。

View Rulebase as Groups (ルールベースをグループとして表示)しながら、グループ タグに カーソルを合わせてドロップダウンリストでGlobal Find (グローバル検索)を選択します。

none (3)	1-3	4	test-rule2
GroupTag2 (1)	6	Filter	
GroupTag3 (1)	Đ	Appen	d Rule
GroupTag (1)	٢	Move 9	Selected Rule(s)
	2	Apply ⁻	Fag to the Selected Rule(s)
	\geq	UnTag	Selected Rule(s)
	٩	Global	Find: GroupTag2

タグ設定バンドルのエクスポート。

管理ロールは、**PDF/CSV** 形式でオブジェクト構成テーブルをエクスポートし、フィルタを 適用して、必要な列だけを含むようにテーブル出力をカスタマイズすることができます。エ クスポート ダイアログに表示される列のみがエクスポートされます。Export Configuration Table Data(設定バンドルデータのエクスポート)を参照してください。

Objects > Devices [オブジェクト > デバイス]

Device Dictionary(デバイス ディクショナリ)とも呼ばれるこのページには、デバイス オブ ジェクトのメタデータが含まれています。既存のデバイス オブジェクトの情報を確認するか、 新しいデバイスオブジェクトを追加します。セキュリティ ポリシーの一致条件としてデバイ ス オブジェクトを使用すると、デバイス ベースのポリシーを作成することができます。ファイ アウォールはダイナミック更新し、セキュリティ ポリシーを新規および既存のデバイスに適用 します。Palo Alto Networks は動的更新によって Device Dictionary を更新します。この更新は Device > Dynamic Updates > Device-ID Content で表示できます。

Button/Field(ボタン/フィールド)	の意味
氏名	デバイス オブジェクト名です。
場所	デバイス オブジェクトのデバイス グループの場所で す。
カテゴリ	デバイス オブジェクトのカテゴリです(例えば、ビ デオオーディオ会議)。
プロファイル	デバイス オブジェクトのデバイス プロファイルで す。
モデル	デバイス オブジェクトのモデルです。
OS バージョン	デバイス オブジェクトの OS バージョンです。
OS Family OS ファミリー	デバイス オブジェクトの OS ファミリーです。
ベンダー	デバイス オブジェクトのベンダーです。
コンテキストの	Add(追加)をクリックして新しいデバイスオブ ジェクトを追加します。Name(名称)および、 必要に応じて、Description(説明)を入力しま す。Select additional metadata for the device, such as Category(カテゴリ)、OS、Model(モデル)等の 追加のデバイスに関するメタデータを選択します。 デバイスのリストをBrowse(参照)して、追加する デバイスを選択することもできます。OK をクリック して変更を確定します。
削除します。	不要となったデバイス オブジェクトを選択し て、 Delete (削除)します。
移動	移動するデバイス オブジェクトを選択し て、 Move (移動)します。

Button/Field(ボタン/フィールド)	の意味
コピー	新しいデバイス プロファイルのベースとなるデバイ ス オブジェクトを選択し、Clone(クローン)しま す。
PDF/CSV	デバイスのリストを PDFまたはCSV 形式でエクス ポートします。必要に応じ、フィルタを適用して、 より具体的な出力を作成することができます。Web インターフェイスで表示可能な列のみがエクスポー トされます。「Configuration Table Export(設定バ ンドルのエクスポート)」を参照してください。

Objects > External Dynamic Lists [オブジェクト > 外部 動的リスト]

外部ダイナミックリストは、ポリシーで使用できる IP アドレス、URL、ドメイン 名、International Mobile Equipment Identities(IMEI)、または、ポリシールールでトラフィッ クをブロックまたは許可するために使用できる International Mobile Subscriber ID(IMSI)のイ ンポートされたリストに基づくアドレス オブジェクトです。このリストは、ファイアウォール からアクセスできる Web サーバーに保存されたテキスト ファイルでなければなりません。デ フォルトでは、ファイアウォールは管理(MGT)インターフェースを使用してこのリストを取 得します。

Palo Alto Networks はアクティブな脅威防止ライセンスを持つユーザーに、組み込み型の悪意の あるホストをブロックするために使用できる動的な IP リストを複数提供しています。このリス トは、最新の脅威の調査に基づいて毎日更新されます。

IP アドレス一覧は、ポリシー規則の送信元と送信先のアドレス オブジェクトとして使用でき ます。URL Filtering プロファイル内の URL リスト (Objects > Security Profiles > URL フィルタ リング) または Security ポリシー規則の一致基準として使用でき、ドメイン リスト (Objects > Security Profiles > Anti-Spyware Profile) を指定したドメイン名のシンクホールとして使用できま す。

すべてのセキュリティ ポリシー ルールの中で一意の送信元を持つ最大 30 個の外部動的リスト を各ファイアウォール モデルで使用できます。ファイアウォールでサポートされる、各リス ト タイプの最大エントリ数はファイアウォール モデルによって異なります(各外部動的リス ト タイプのさまざまなファイアウォール制限を参照してください)。リスト項目は、外部動的 リストがポリシー規則で使用されている場合にのみ、最大値にカウントされます。モデルがサ ポートするエントリの最大数を超えると、firewall は System ログを生成し、制限を超えるエン トリをスキップします。ポリシー ルールで現在使用されている IP アドレス、ドメイン、およ び URL、IMEI、IMSI の数と、ファイアウォールでサポートされる合計数を確認するには、List Capacities(容量の表示)を選択してください(ファイアウォールのみ)。

外部動的リストは、評価された順序で上から下に表示されます。リストの順序を変更するには、 ページの下部にある方向コントロールを使用します。最も重要なエントリを含む外部動的リスト を一番上に移動して、容量制限に達する前にそれらがコミットされるようにすることができま す。

Group By Type が有効になっている場合、外部動的リストの順序を変更することはできません。

外部動的リストをホストするサーバーから最新バージョンの外部動的リストを取得するには、外 部動的リストを選択し、Import Now をクリックします。

Palo Alto Networks の悪意のある IP アドレス フィードの設定を削除、コピー、編集 することはできません。

新しい外部ダイナミックリストを作成してAdd(追加)し、以下の表に示す設定を行います。

外部ダイナミックリストの 設定	の意味
氏名	外部動的リストを識別する名前(最大32文字)を入力します。 この名称で、ポリシー ルール適用リストを識別します。
Shared (複数の仮想システ ム (multi-vsys) および Panorama のみ)	以下に対して外部動的リストを公開する場合は、このオプショ ンを有効化します。 • multi-vsys ファイアウォールの各仮想システム (vsys)。 このオプションを無効化 (クリア) すると、Objects (オブ ジェクト) タブで選択した Virtual System (仮想システム)の みに対して外部ダイナミック リストが公開されます。 • Panorama 上の各デバイス グループ。 このオプションを無効化 (クリア) すると、Objects (オブ ジェクト) タブで選択した Device Group (デバイス グループ) のみに対して 外部ダイナミック リストが公開されます。
オーバーライドの無効化 (Panoramaのみ)	この外部ダイナミックリストオブジェクトの設定が、このオ ブジェクトを継承したデバイス グループで管理者によりオー バーライドされることを防止するには、このオプションを有 効化します。デフォルトでこのオプションは無効(クリア)に なっており、管理者は、このプロファイルを継承するデバイス グループの設定をオーバーライドできます。
ソース URL のテスト (ファイアウォールのみ)	 外部ダイナミックリストをホストするサーバーにファイア ウォールが接続できることを確認するには、Test Source URL(送信元 URL のテスト)を行います。 このテストでは、サーバーが正常に認証されたか どうかは確認されません。
Create List(リストの作成)	タブ
タイプ	以下の外部動的リストのタイプから選択してください。

Predefined IP List(事前定義済み IP リスト) – Palo Alto
 Networks がBulletproof IPアドレス、既知の悪意のある IPア

外部ダイナミックリストの 設定	の意味
IP アドレ ス、URL、お よびドメイン	ドレス、またはリスクの高い IPアドレスとして識別したリス トをリスト エントリの情報源として使用します(アクティブ な脅威防御ライセンスが必要です)。
石を1つの リストに混在 させることは	 Predefined URL List(事前定義済み URL リスト)–Palo Alto Networks が信頼性が高いと識別したドメインのリストを使 用して、このドメインを認証ポリシーから除外します。
できません。 それぞれのリ ストには1つ のタイプのエ ントリのみを 含めることが できます。	 IP List (IP リスト) (デフォルト)–各リストには、IPv4 または IPv6 アドレス、アドレス範囲、およびサブネットを含めることができます。リストには、1行につきIPアドレス、範囲、またはサブネットのうち1つのみが記載されている必要があります。例:
	192.168.80.150/32 2001:db8:123:1::1 または 2 001:db8:123:1::/64 192.168.80.0/24 2001:db8 :123:1::1 - 2001:db8:123:1::22
	上記の例では、最初の行は 192.168.80.0 から 192.168.80.255 までのすべてのアドレスを示しています。 「192.168.20.0/24」、「192.168.20.40-192.168.20.50」な ど、サブネットや IPアドレス範囲は 1 つの IPアドレス エン トリとしてカウントされ、複数の IPアドレスとしてはカウン トされません。
	 Domain List(ドメインリスト) – 各リストでは1行につき1 つまでのドメイン名エントリを持たせることが可能です。例:
	<pre>www.p301srv03.paloalonetworks.com ftp.examp le.co.uk test.domain.net</pre>
	外部動的リストに含まれるドメインのリストの場合、firewall は重大度が中程度のスパイウェアタイプのカスタム署名の セットを作成し、ドメインのカスタムリストにシンクホール アクションを使用できるようにします。
	• URL List[URLリスト] – それぞれのリストでは1行につき1つ までのURLエントリを持たせることが可能です。例:
	<pre>financialtimes.co.in www.wallaby.au/joey ww w.exyang.com/auto-tutorials/How-to-enter-Da ta-for-Success.aspx *.example.com/*</pre>
	各 URL リストの既定のアクションは [許可] です 。デフォル ト アクションを編集するには、「Objects(オブジェクト)

外部ダイナミックリストの 設定	の意味
	 > Security Profiles(セキュリティプロファイル) > URL Filtering(URLフィルタリング)」を参照してください。 IP、Domain、または URL リストのエントリを作成するとき は、External Dynamic List Formatting Guidelines を参照して ください。
タイプ(続く)	 Subscriber Identity List (サブスクライバ ID リスト) -各 リストには、3G、4G、または 5G ネットワークのサブスク ライバ ID が含まれています。Source(送信元)フィールド に、ファイアウォールがリストにアクセスする際の URL を 入力します。 Equipment Identity List(機器 ID リスト) -各リストに は、3G、4G、または 5G ネットワークの機器 ID が含まれて います。Source(送信元)フィールドに、ファイアウォール がリストにアクセスする際の URL を入力します。 外部動的リストと静的エントリがサポートする 必要がある 3G、4G、および 5G ネットワーク 識別子の合計数に基づいて、購入する firewall モデルを決定します。
の意味	外部動的リストの説明を入力します(最大255文字)。
送信元	 外部ダイナミックリストが事前定義済み IP リストの場合、Palo Alto Networks - Bulletproof IP addresses(防弾 IPアドレス)、Palo Alto Networks - High risk IP addresses(高リスク IPアドレス)、または、Palo Alto Networks - Known malicious IP addresses (悪意のある既知の IP アドレス)をリストの送信元に選択します。
	 外部ダイナミックリストが事前定義済み URL リストの場合、デフォルト設定は panw-auth-portal-exclude-list となります。
	 外部ダイナミック リストが IP リスト、ドメイン リスト、または URL リストの場合は、テキスト ファイルを含む HTTP または HTTPS URL パスを入力します(例えば、http://192.0.2.20/myfile.txt)。
	 外部動的リストがドメインリストの場合、サブドメインを 含むように 自動的に展開できます。このオプションによ り、PAN-OS[®] ソフトウェアが外部ダイナミック リストの ファイルでリストアップされているドメイン名の低レベル コ ンポーネントをすべて評価できるようになります。このオプ ションはデフォルトでは無効になっています。

外部ダイナミックリストの 設定	の意味
	 外部ダイナミック リストがサブスクライバ ID リストまたは 機器 ID リストの場合は、リストを含む URL パスを入力しま す。
	外部ダイナミックリストにサブドメインが含まれている場合、展開された上記項目が、アプライアンスモデルの容量に加算されます。サブドメインを手動で定義するには、この機能を無効にします。ただし、この機能を無効にすると、サブドメインは、リストで明示的に定義しない限り、ポリシー規則によって評価されません。
Certificate Profile (IP List, Domain List, or URL List only)	外部ダイナミックリストに HTTPS URL が含まれる場合、既 存の証明書プロファイルを選択(ファイアウォールおよび Panorama)するか、新しい Certificate Profile(証明書プロ ファイル)を作成(ファイアウォールのみ)して、リストを ホストする Web サーバーを認証します。証明書プロファイ ルの設定方法の詳細は、「Device(デバイス) > Certificate Management(証明書管理) > Certificate Profile(証明書プロ ファイル)」を参照してください。
	デフォルト:なし(証明書フロファイルの無効化) ポリシーの適用に使用できる外部動的リストの数を最大化するには、同じ証明書プロファイルを使用して、同じソース URL から外部動的リストを認証します。これらのリストは、1つの外部動的リストとしてのみカウントされます。それ以外の場合、異なる証明書プロファイルを使用する同じソース URL からの外部動的リストは、一意の外部動的リストとしてカウントされます。
Client Authentication [クラ イアントの認証]	HTTP BASIC認証を要求する外部ダイナミックリスト ソースに アクセスする際にファイアウォールで使用するユーザー名とパ スワードを追加するには、このオプションを有効化します(デ フォルトでは無効)。この設定は、外部ダイナミックリストに HTTPS URL が含まれる場合にのみ使用できます。
	• Username(ユーザー名) – リストにアクセスするための有 効なユーザー名を入力します。
	 Password/Confirm Password (パスワード/パスワード再入力) – ユーザー名のパスワードを入力し、確認します。

外部ダイナミックリストの 設定	の意味
アップデートを確認	 ファイアウォールが Web サーバからリストを取得する頻度を指定します。間隔は、Every Five Minutes (デフォルト)、Hourly、Daily、Weekly、または Monthly に設定できます。この間隔は前回のコミットの時間からの相対値です。たとえば、5分間隔を選択した場合、最後のコミットが1時間前であれば、コミットは5分後に行われます。コミットは、リストを参照するすべてのポリシー規則を更新します。 firewall はアクティブな Threat Prevention ライセンスを使用してコンテンツの更新を動的に受信するため、事前定義された IP リストの頻度を指定する必要はありません。

List Entries and Exceptions (リスト エントリおよび例外) タブ

リスト エントリ	外部ダイナミックリストのエントリを表示します。	
	 Add an entry as a list exception (手動例 外としてエントリを追加する) -最大 100 個のエントリを選択し、Submit (送信) (→ します。)
	 View an AutoFocus threat intelligence summary for an item (項目に関する AutoFocus 脅威インテリジェンス サマ リーを表示する) –エントリにカーソルを合わせ、ドロップ ダウンで AutoFocus を選択します。項目のサマリーを表示 するには、AutoFocus ライセンスを持っており、AutoFocus 脅威インテリジェンスを有効化する必要があります (Device (デバイス) > Setup (セットアップ) > Management (管理)を選 択して AutoFocus 設定を編集します)。 	
	 Check if an IP address, domain, or URL is in the external dynamic list (IP アドレス、ドメイン、または URL が外部ドメインリストに含まれているかどうかを確認する) –フィルタフィールドに値を入力して、Apply Filter (フィルタを適用) (→ します。Clear Filter ([X])をクリックして完全なリストに戻ります。 	
手動例外	外部ダイナミックリストの例外を表示します。 • Edit an exception(例外の編集)–例外を選択して、変更を 加えます。	_

)

外部ダイナミックリストの 設定	の意味
	 Manually enter an exception (例外を手動で入力) –新しい 例外を手動で Add (追加) します。
	 Remove an exception from the Manual Exceptions list (手動 例外リストからの例外の削除) – 例外を選択して Delete (削 除)します。
	 Check if an IP address, domain, or URL is in the Manual Exceptions list (IP アドレス、ドメイン、または URL が 手動例外リストに含まれているかを確認する) –フィル タフィールドに値を入力し、Apply Filter (フィルタを適 用) (→ します。Clear Filter ([X])をクリックすると、完全なリスト に戻ります。Manual Exceptions リストに重複するエントリ がある場合、変更を外部動的リストに保存することはできま せん。

)

Objects(オブジェクト) > Custom Objects(カスタム オブジェクト)

ポリシーに適用して使用する、データパターン、脆弱性とスパイウェアのシグネチャ、およびURLカテゴリをカスタマイズして作成します。

- Objects > Custom Objects > Data Patterns [オブジェクト > カスタム オブジェクト > データ パターン]
- Objects(オブジェクト) > Custom Objects(カスタムオブジェクト) > Spyware/ Vulnerability(スパイウェア/脆弱性)
- Objects > Custom Objects > URL Category [オブジェクト > カスタム オブジェクト > URL カ テゴリ]

Objects > Custom Objects > Data Patterns [オブジェクト > カス タムオブジェクト > データ パターン]

確認すべき情報	以下を参照
データ パターンを作成する。	データ パターン設定
正規表現データ パターンの構文の詳 細といくつかの例を確認する。	正規表現データ パターンの構文 正規表現データ パターンの例

以下のトピックでは、データ パターンについて説明します。

データパターン設定

フィルタリング対象とする機密情報のカテゴリを定義する場合は、Objects(オブジェクト) > Custom Objects(カスタムオブジェクト) > Data Patterns(データ パターン)のページを使用します。データフィルタリングプロファイルの定義の詳細は「Objects(オブジェクト) > Security Profiles(セキュリティ プロファイル) > Data Filtering(データフィルタリング)」を参照してください。

次の3種類のデータパターンを作成し、ファイアウォールで機密情報をスキャンするときに使用できます。

- 事前定義済み ファイルで社会保障番号とクレジットカード番号をスキャンするには、事前 定義済みのデータパターンを使用します。
- 正規表現 正規表現を使用して、カスタム データ パターンを作成します。
- ファイル プロパティ ファイルで特定のファイル プロパティおよび値をスキャンします。

データ パターン設定	の意味
氏名	データ パターン名(最大 31 文字)を入力します。名前の大文字と 小文字は区別されます。また、一意の名前にする必要があります。 文字、数字、スペース、ハイフン、およびアンダースコアのみを使 用してください。
の意味	データ パターンの説明を入力します (最大 255 文字)。
共有	 以下に対してデータパターンを公開する場合は、このオプションを 選択します。 multi-vsys ファイアウォールの各仮想システム (vsys)。この選択 を解除すると、Objects[オブジェクト] タブで選択した Virtual System[仮想システム] のみに対してデータパターンが公開され ます。 Panorama 上の各デバイス グループ。この選択を解除する
	と、 Objects [オブジェクト] タブで選択した Device Group [デバイ スグループ] のみに対してデータパターンが公開されます。
オーバーライドの無効 化(<mark>Panoramaのみ</mark>)	管理者が、このオブジェクトを継承するデバイス グループのこの データ パターン オブジェクトの設定をオーバーライドすることを 防ぐには、このオプションを選択します。デフォルトでこのオプ ションはオフになっており、管理者は、このオブジェクトを継承す るデバイス グループの設定をオーバーライドできます。
パターン タイプ	作成するデータ パターンのタイプを以下から選択します。 • 事前定義済みのパターン • 正規表現 • ファイル プロパティ
事前定義済みのパター ン	Palo Alto Networks では、クレジット カード番号や社会保障番号 など、特定タイプの情報をファイルでスキャンするため、事前定義 済みのデータ パターンを提供しています。事前定義済みのパター ンに基づいてデータ フィルタリングを設定するには、パターンを Add(追加)して以下を選択します。
	 Name (石町) - 磁台アータのノイルタリンクに使用する、事前 定義済みのパターンを選択します。事前定義済みのパターンを 選択すると、Description(説明)には情報が自動的に入力され ます。 事前定義済みパターンを検出する File Type (ファイル タイ プ)を選択します。
正規表現	カスタム データ パターンを Add(追加)します。分かりやすい Name(名前)をパターンに付けて、データ パターンをスキャンす

データ パターン設定	の意味
	る File Type(ファイル タイプ)を設定し、Data Pattern(データ パターン)を定義する正規表現を入力します。
	正規表現のデータ パターンの構文に関する詳細と例については、以 下を参照してください。
	• 正規表現データ パターンの構文
	• 正規表現データパターンの例
ファイル プロパティ	ファイル プロパティおよび関連付けられている値をスキャンする データ パターンを構築します。たとえば、ドキュメントのタイトル に「機密」、「社内」、「秘密」などの語句が含まれる Microsoft Word ドキュメントと PDF をフィルタリングするデータ パターン を Add (追加) します。
	● Name(名前)に分かりやすいデータ パターン名を入力します。
	 スキャンする File Type (ファイル タイプ)を選択します。
	 特定の値をスキャンする File Property(ファイル プロパ ティ)を選択します。
	• スキャンする Property Value(プロパティ値)を入力します。

正規表現データ パターンの構文

データパターンを作成するための一般的なパターン要件と構文は、有効化するパターンマッチ ングエンジンによって異なります(Classic (クラシック)またはEnhanced(拡張)があり、拡 張がデフォルトです)。

Pattern Requirements(パター ンの要件)	Classic(クラシック)	Enhanced(拡張)
Pattern length(パ ターンの長さ)	7つのリテラル文字が必要です。 これには、ピリオド(.)、ア スタリスク(*)、プラス記号 (+)、または範囲([az])。	リテラル文字2文字が必要で す。
大文字と小文字を区 別しない	あらゆる語句のバリエーション を照合できるように、可能性の ありえるすべての文字列のパ ターンを定義します。 例:confidential (機密)と指定 されたすべての文書に一致さ せるには、「confidential」、 「Confidential」、および	サブパターンで i オプションを使 用できます。 例: ((?i)\bconfidential\b) は ConfiDential と一致します

Pattern Requirements(パター ンの要件)	Classic(クラシック)	Enhanced(拡張)
	「CONFIDENTIAL」を含むパ ターンを作成する必要がありま す。	

PAN-OS[®]の正規表現の構文は、従来の正規表現エンジンと似ていますが、それぞれのエンジン はすべて異なります。Classic Syntax(クラシック構文)およびEnhanced Syntax(拡張構文)の 表では、PAN-OS パターンマッチングエンジンでサポートされている構文について説明してい ます。

Classic Syntax (クラシック構文)

Pattern Syntax(パターン構 文)	の意味
0	任意の1文字に一致します。
不明	直前の文字または表現に 0 または 1 回一致します。かっこ内に 一般式を含める必要があります。 例: (abc)?
*	直前の文字または表現に 0 回以上一致します。かっこ内に一般 式を含める必要があります。 例: (abc)*
+	直前の文字または正規表現に1回以上一致します。かっこ内に 一般式を含める必要があります。 例: (abc)+
	 「または」を指定します。 ① 代替の従属文字列はかっこ内に含める必要があります。 例: ((bif) (scr) (exe))は、bif、scr、または exe に一致します。
-	範囲を指定します。 例: [c-z] は、c ~ z の任意の文字列に一致します。
[]	指定された任意の文字に一致します。

Pattern Syntax (パターン構 文)	の意味
	例: [abz] はa、b、または z に一致します。
^	指定された文字以外の任意の文字に一致します。 例: [abz] は指定された文字a、b、または z 以外の任意の文字 に一致します。
{}	最小値と最大値を含む文字列に一致します。 例: {10-20} は、10 ~ 20 バイトの文字列に一致します。固定 文字列の前に直接指定する必要があり、ハイフン (-)のみを使 用できます。
	任意の文字に対してリテラル一致を実行します。指定した文字の前にバックスラッシュ記号(\)を付ける必要があります。
&	アンパサンド (&) は特殊文字であるため、文字列で & を検索す るには、 & を使用する必要があります。

Enhanced Syntax(拡張構文)

強化されたパターンマッチングエンジンは、すべてのClassic Syntax(クラシック構文)および 以下の構文をサポートします。

Pattern Syntax (パターン構文)	の意味
-------------------------	-----

Shorthand character classes (速記文字クラス)

数字や空白等の特定の種類の文字を表す記号です。大文字を使用すると、この省略文字クラ スを無効にすることができます。

\s	任意の空白文字に一致します。
	例: \s は、スペース、タブ、改ページ、または フォームフィードに一致します。
\d	数字 [0-9] と一致します。
	例: \d は 0に一致します。
\w	ASCII文字 [A-Za-z0-9_] に一致します。
	例: \w\w\wはPANと一致します。
\v	すべての Unicode 改行文字を含む垂直方向の空白 文字と一致します。

Pattern Syntax(パターン構文)	の意味
	例: \v 垂直方向の空白文字に一致します。
\h	タブおよびすべての「スペース区切り」ユニコー ド文字を含む水平方向の空白に一致します。
	例: \h は水平方向の空白文字に一致します。

Bounded repeat quantifiers(有界性反復数量詞)

前の文字を繰り返す回数を指定します。

{n}	正確に数(n)回に一致します。 例: a{2} は aaと一致します。
{n,m}	{n,m} はnからm回一致します。 例: a{2,4} は aa、aaa、および aaaa と一致し ます。
{n, }	{n,} は少なくとも n 回一致します。 例: a{2,} は aaaaaaab の aaaaa と一致します.

Anchor characters (アンカー文字)

式に一致する場所を指定します。

٨	文字列の先頭で一致します。複数行モード (m) が有効な場合は、すべての改行後にも一致します。
	例:文字列 abc がある場合、 ^a は a と一致します が、bは文字列の先頭に現れておらず、 ^b は何に も一致しません。
\$	文字列の最後、または文字列の最後の改行文字の 前で一致します。複数行モード(m)が有効な場 合、すべての改行の前にも一致します。
	例:文字列abcがある場合、c \$はcと一致します が、aは文字列の最後にないので、a\$は何にも一 致しません。
\A	文字列の先頭で一致します。複数行モード(m) が有効な場合でも、改行後で一致しません。

Pattern Syntax(パターン構文)	の意味
\Ζ	文字列の最後で、最後の改行の前で一致します。 複数行モード(m)が有効になっている場合で も、他の改行の前に一致しません。
\z	文字列の絶対文字列最後で一致します。改行前で は一致しません。

Option modifiers (オプション修飾子)

サブパターンの動作を変更します。(?<option>)を有効にするか、(?-<option>)を無効にする。

i	大文字と小文字を区別しません。
	例: ((?i)\bconfidential\b) は ConfiDential と一致します
m	行の最初と最後でへと\$を一致させます。
S	 を改行文字を含むすべてに一致させます。
x	正規表現トークン間の空白を無視します。

正規表現データ パターンの例

有効なカスタム パターンの例を以下に示します。

- .*((Confidential)|(CONFIDENTIAL))
 - 任意の場所から「Confidential」または「CONFIDENTIAL」という言葉を検索します。
 - 最初の「.*」は、ストリームの任意の場所を検索することを指定します。
 - デコーダが大文字小文字を区別するかどうかに応じて、上のパターンは「confidential」(す べて小文字)に一致しないことがあります。
- .*((Proprietary & amp Confidential)|(Proprietary and Confidential))
 - 「Proprietary & Confidential」または「Proprietary and Confidential」を検索します。
 - 「Confidential」の検索よりも詳細な検索です。
- .*(Press Release).*((Draft)|(DRAFT)|(draft))
 - さまざまな形式の単語 draft が後に続く「Press Release」を検索します。これに一致する 場合は、プレス リリースの公開準備が整っていないことを示します。
- .*(Trinidad)
 - 「Trinidad」などのプロジェクト コード名を検索します。

313

Objects(オブジェクト) > Custom Objects(カスタム オブジェクト) > Spyware/Vulnerability(スパイウェ ア/脆弱性)

ファイアウォールでは、ファイアウォールの脅威エンジンを使用してカスタムのスパイウェア シグネチャと脆弱性シグネチャを作成する機能がサポートされています。スパイウェアのフォン ホーム通信や脆弱性の悪用を特定するためのカスタム正規表現パターンを記述できます。作成し たスパイウェアと脆弱性のパターンは、カスタム脆弱性プロファイルで使用できます。ファイア ウォールは、カスタム定義されたパターンがネットワークトラフィックに含まれていないか検 索し、脆弱性の悪用に対して指定されたアクションを実行します。

週次のコンテンツリリースには、新しいデコーダとシグネチャを開発するためのコンテクストが定期的に含まれています。

カスタム シグネチャを定義するときに任意で時間属性を含めることができます。これを行うに は、攻撃に対してアクションをトリガーする間隔ごとにしきい値を指定します。しきい値に達し た場合にのみアクションが実行されます。

アンチスパイウェアプロファイルのシグネチャを定義する場合は、Custom Spyware Signature[カスタムスパイウェアシグネチャ] のページを使用します。脆弱性防御プロファイル のシグネチャを定義するには、Custom Spyware Signature[カスタム脆弱性シグネチャ] ページを 使用します。

カスタムの脆弱性およ びスパイウェア シグネ チャの設定 	の意味
Configuration [設定] タブ	×
脅威 ID	その設定で使用する識別子の数値を入力します(スパ イウェアシグネチャの範囲は、15000~18000 および 6900001~7000000、脆弱性シグネチャの範囲は、41000~45000 および 6800001~6900000)。
氏名	脅威の名前を指定します。
共有	以下に対してカスタムシグネチャを公開する場合は、このオプショ ンを選択します。
	 multi-vsys ファイアウォールの各仮想システム (vsys)。この選択 を解除すると、Objects[オブジェクト] タブで選択した Virtual System[仮想システム] のみに対してカスタムシグネチャが公開 されます。

カスタムの脆弱性およ びスパイウェア シグネ チャの設定	の意味
	 Panorama 上の各デバイス グループ。この選択を解除する と、Objects[オブジェクト] タブで選択したDevice Group[デバイ スグループ] のみに対してカスタムシグネチャが公開されます。
オーバーライドの無効 化(Panoramaのみ)	このシグネチャの設定が、このシグネチャを継承したデバイス グ ループで管理者によりオーバーライドされることを防止するには、 このオプションを選択します。デフォルトでは、この選択は解除さ れています。つまり、管理者は、シグネチャを継承するすべてのデ バイス グループで設定をオーバーライドできます。
コメント	任意でコメントを入力します。
重要度	脅威の重大度を示すレベルを割り当てます。
デフォルトのアクショ ン	脅威の条件を満たしたときに実行されるデフォルトのアクションを 割り当てます。アクションのリストについては、「セキュリティ プ ロファイルのアクション」を参照してください。
指示	脅威を評価する方向 (クライアントからサーバー、サーバーからク ライアント、その両方) を指定します。
影響を受けるシステム	脅威によって影響を受ける対象 (クライアント、サーバー、そのどちらか、その両方) を指定します。脆弱性シグネチャには適用されますが、スパイウェア シグネチャには適用されません。
CVE	CVE (Common Vulnerability Enumeration) を、追加情報および分析のための外部参照として指定します。
ベンダー	脆弱性のベンダー識別子を、追加情報および分析のための外部参照 として指定します。
Bugtraq	Bugtraq (CVE と類似) を、追加情報および分析のための外部参照として指定します。
リファレンス	必要に応じて、追加の分析または情報用にリンクを追加します。こ の情報は、ユーザーが ACC、ログ、または脆弱性プロファイルから 脅威をクリックすると表示されます。
Signatures [シグネチャ]	タブ
標準シグネチャ	Standard[標準] を選択し、新しいシグネチャをAdd[追加] します。

カスタムの脆弱性およ びスパイウェア シグネ チャの設定	の意味				
	 Standard[標準] – シグネチャの識別に使用する名前を入力します。 				
	● Comment[コメント] – 任意で説明を入力します。				
	 Ordered Condition Match[順番が付けられた条件の一致] – シグ ネチャの条件の定義順序が重要である場合に選択します。 				
	 Scope[範囲] – このシグネチャの適用対象 (現在のトランザク ションのみ、またはユーザー セッション全体) を選択します。 				
	Add Or Condition[Or条件を追加] または Add And Condition[And条件を追加] をクリックして条件を追加します。グループ内に条件を 追加するには、グループを選択して Add Condition[条件の追加] を クリックします。シグネチャに条件を追加して、条件として定義 したパラメータが真の場合にトラフィックのシグネチャが生成さ れるようにします。ドロップダウンリストからOperator[演算子] を 選択します。演算子によって、カスタムシグネチャがトラフィッ クと一致するために真である必要がある条件のタイプが決まりま す。Less Than[未満]、Equal To[等しい]、Greater Than[超過]、また は Pattern Match[パターンマッチ] 演算子を選択します。				
	 Pattern Match[パターンマッチ] 演算子を選択する際には、以下 が真になるように指定すると、シグネチャがトラフィックと一 致します。 				
	• Context[コンテクスト] – 使用可能なコンテクストから選択します。				
	• Pattern[パターン] – 正規表現を指定します。正規表現のパ ターンのルールに関する詳細は「パターンのルールの構文」 を参照してください。				
	• Qualifier and Value[修飾子と値] – 任意で修飾子/値のペアを 追加します。				
	• Negate[否定] – Negateを選択すると、定義済みのパターン マッチ条件が真でない場合のみ、カスタムシグネチャがトラ フィックと一致します。これにより、特定の条件が満たされ				

カスタムの脆弱性およ びスパイウェア シグネ チャの設定	の意味
	たとき、カスタム シグネチャがトリガーされないようにでき ます。
	Negate 条件だけのカスタム シグネチャを作成す ることはできません。Negate 条件を指定するに は、少なくとも1つの肯定条件を含める必要が あります。また、シグネチャの範囲がセッショ ンに設定されている場合、トラフィックと一致 させるには、Negate 条件を最後の条件に設定し ないようにしてください。
	トラフィックがシグネチャとシグネチャの例外の両方に一致 する場合、新しいオプションを使用してシグネチャの生成 を無効にすることで、カスタム脆弱性またはスパイウェアシ グネチャの例外を定義できます。このオプションを使用する と、通常ならスパイウェアまたは脆弱性攻撃として分類され るネットワーク内の特定のトラフィックを許可できます。そ の場合、パターンに一致するトラフィックについてのみ、シ グネチャが生成されます。パターンには一致するが、パター ンの例外にも一致するトラフィックは、シグネチャ生成の対 象から除外され、関連するポリシー アクション (ブロックや ドロップなど) も実行されません。たとえば、リダイレクトさ れた URL に対して生成されるシグネチャを定義し、同時に、 信頼されたドメインにリダイレクトされた URL についてはシ グネチャを生成しないという例外も作成できるようになりま した。
	• Equal To[等しい]、Less Than[未満]、または Greater Than[超過] の演算子を選択する場合は、以下が真になるように指定する と、シグネチャがトラフィックと一致します。
	 Context[コンテクスト] – TCP または UDP の未知のリクエス トまたは応答から選択します。
	 Position[位置] – ペイロードの最初の4バイトまたは2番目の4バイトのいずれかを選択します。
	 Mask[マスク] – 4 バイトの 16 進数値を指定します (たとえば、0xfffff00)。
	 Value[値] – 4 バイトの 16 進数値を指定します (たとえば、Oxaabbccdd)。
組み合わせシグネチャ	Combination[組み合わせ]を選択し、以下の情報を指定します。

カスタムの脆弱性およ びスパイウェア シグネ チャの設定	の意味				
	Combination Signatures[組み合わせシグネチャ]を選択し、シグネ チャを定義する条件を以下のように指定します。				
	 Add AND Condition[AND条件を追加] または Add OR Condition[OR条件を追加] をクリックして条件を追加します。 グループ内に条件を追加するには、グループを選択して Add Condition[条件の追加] をクリックします。 				
	 グループ内で条件を移動するには、条件を選択して Move Up[上 へ] または Move Down[下へ] をクリックします。グループを移 動するには、グループを選択して Move Up[上へ] または Move Down[下へ] をクリックします。グループ間で条件を移動するこ とはできません。 				
	Time Attribute[時間属性] を選択し、以下の情報を指定します。				
	 Number of Hits[ヒット数] – ポリシーベースのアクションをトリガーするしきい値を、指定した秒数 (1 ~ 3600) のヒット数 (1 ~ 1000) として指定します。 				
	 Aggregation Criteria[集約基準] – ヒットの追跡方法 (送信元 IP ア ドレス、宛先 IP アドレス、または送信元 IP アドレスと宛先 IP アドレスの組み合わせ) を指定します。 				
	 グループ内で条件を移動するには、条件を選択して Move Up[上 へ] または Move Down[下へ] をクリックします。グループを移 動するには、グループを選択して Move Up[上へ] または Move Down[下へ] をクリックします。グループ間で条件を移動するこ とはできません。 				

Objects > Custom Objects > URL Category [オブジェクト > カスタム オブジェクト > URL カテゴリ]

カスタムURLカテゴリのページを使用してURLのカスタムリストを作成し、URLフィルタリング プロファイルまたはポリシールールの一致条件に使用します。カスタム URL カテゴリでは URL エントリを個別に追加したり、あるいは URL のリストを含むテキストファイルをインポートす ることができます。

カスタムカテゴリに追加される URL エントリの大文字と小文字は区別されます。

以下の表では、カスタム URL 設定について説明します。

カスタム URL カテゴリ設定	の意味
氏名	カスタム URL カテゴリの識別に使用する名前(最大 31 文字) を入力します。URLフィルタリングポリシーを定義する場合 と、ポリシールールのURLカテゴリの一致条件のカテゴリリス トにこの名前が表示されます。名前の大文字と小文字は区別 されます。また、一意の名前にする必要があります。文字、数 字、スペース、ハイフン、およびアンダースコアのみを使用し てください。
の意味	URL カテゴリの説明を入力します (最大 255 文字)。
タイプ	カテゴリ タイプを選択します。 • Category Match (カテゴリの一致)- Category Match (カテ ゴリの一致)を選択して、指定したすべての URL カテゴリに 一致する URL を含む新しいカスタム カテゴリを定義します (URL はリスト内のすべてのカテゴリに一致する必要があり ます)。2~4 個のカテゴリを指定します。 • URL リスト- URL リスト を選択して、カテゴリの URL リス トを追加またはインポートします。このカテゴリ タイプに は、PAN-OS 9.0 より前に追加された URL も含まれていま す。
共有	以下に対してURLカテゴリを公開する場合は、このオプション を選択します。 • multi-vsys ファイアウォールの各仮想システム (vsys)。この オプションを無効化 (クリア) すると、Objects (オブジェク ト) タブで選択した Virtual System (仮想システム) のみに対 してURLカテゴリが公開されます。

カスタム URL カテゴリ設定	の意味					
	 Panorama 上の各デバイス グループ。このオプションを無効化(クリア)すると、Objects (オブジェクト) タブで選択した Device Group (デバイスグループ)のみに対して URL カテゴリが公開されます。 					
オーバーライドの無効化 (Panoramaのみ)	このカスタム URL オブジェクトの設定が、このオブジェクト を継承したデバイス グループで管理者によりオーバーライド されることを防止するには、このオプションを選択します。デ フォルトでこのオプションは無効化されており、管理者は、こ のオブジェクトを継承するデバイス グループの設定をオーバー ライドできます。					
サイト	カスタム URL カテゴリのサイトを管理します (追加またはイン ポートされる各 URL は最大 255 文字です)。					
	 Add (追加)–URL をAdd (追加)します(一行につきピアは一つのみ)。各 URL は「www.example.com」の形式で入力できます。また、「*.example.com」など、ワイルドカードを含むこともできます。サポートされている形式の詳細については、Objects > Security Profiles > URL Filtering [オブジェクト > セキュリティプロファイル > URL フィルタリング]のBlock List を参照してください。 					
	 Import (インポート) – URL リストが含まれているテ キストファイルを参照してImport (インポート) しま す。1行あたり1つのURLのみを入力します。各 URL は 「www.example.com」の形式で入力できます。また、 「*.example.com」など、ワイルドカードを含むこともでき ます。サポートされている形式の詳細については、Objects > Security Profiles > URL Filtering [オブジェクト > セキュリ ティ プロファイル > URL フィルタリング] の Block List を参 照してください。 					
	 Export (エクスポート)–リストに含まれるカスタム URL エントリをExport (エクスポート) (テキストファイルとしてエクスポート) します。 					
	• Delete (削除)–エントリをDelete (削除)してリストから URL を取り除きます。					

カスタム URL カテゴリ設定	の意明	ŧ
		URL フィルタリングプロファイルで使用した カスタムカテゴリを削除する場合は、アク ションをNone (なし) に設定する必要がありま す。Objects > Security Profiles > URL Filtering [オ ブジェクト > セキュリティ プロファイル > URL フィルタリング]のCategoryアクションを参照して ください。

Objects(オブジェクト) > Security Profiles(セキュリ ティプロファイル)

セキュリティ プロファイルでは、セキュリティ ポリシーで脅威から保護します。それぞれのセ キュリティ ポリシー ルールには、1 つ以上のセキュリティ プロファイルを含めることができま す。以下のプロファイル タイプを使用できます。

- アンチウイルス プロファイル ワーム、ウイルス、トロイの木馬から保護したり、スパ イウェアのダウンロードをブロックしたりします。「Objects(オブジェクト) > Security Profiles(セキュリティ プロファイル) > Antivirus(アンチウイルス)」を参照してください。
- アンチスパイウェア プロファイル 侵入されたホストのスパイウェアから外部指揮統制 (C2) サーバーに対する phone-home 通信またはビーコン通信の試みをブロックします。「Objects(オブジェクト) > Security Profiles(セキュリティ プロファイル) > Anti-Spyware Profile(アンチスパイウェア プロファイル)」を参照してください。
- 脆弱性防御プロファイル システムの脆弱性の悪用やシステムへの不正アクセスを防止 します。「Objects(オブジェクト) > Security Profiles(セキュリティ プロファイル) > Vulnerability Protection(脆弱性防御)」を参照してください。
- URL フィルタリング プロファイル 特定の Web サイトや Web サイト カテゴリ (ショッピン グやギャンブルなど) へのユーザーのアクセスを制限します。「Objects(オブジェクト) > Security Profiles(セキュリティ プロファイル) > URL Filtering(URL フィルタリング)」を 参照してください。
- ファイルブロッキングプロファイル 選択したファイル タイプの指定したセッションフロー方向(インバウンド、アウトバウンド、両方)のトラフィックをブロックします。「Objects(オブジェクト) > Security Profiles(セキュリティプロファイル) > File Blocking(ファイルブロッキング)」を参照してください。
- WildFire[™] 分析プロファイル WildFire アプライアンスまたは WildFire クラウドでローカル に実行されるファイル分析を指定します。「Objects(オブジェクト) > Security Profiles(セ キュリティ プロファイル) > WildFire Analysis(WildFire 分析)」を参照してください。
- データフィルタリングプロファイル クレジットカード番号や社会保障番号などの機密情報が、保護されたネットワークから漏出するのを防ぎます。「Objects(オブジェクト)> Security Profiles(セキュリティプロファイル)> Data Filtering(データフィルタリング)」を参照してください。
- DoS プロテクション プロファイルは、大量の単一および複数セッション攻撃からファ イアウォールを保護するために DoS プロテクション ポリシー ルールで使用されます。 「Objects(オブジェクト) > Security Profiles(セキュリティ プロファイル) > DoS Protection(DoS プロテクション)」を参照してください。
- Mobile Network Protection (モバイルネットワーク プロテクション) プロファイルを使用 すると、ファイアウォールは GTP トラフィックを検査、検証、およびフィルタリングできま す。

個々のプロファイルの他に、一緒に適用されることが多いプロファイルをまとめて Objects (オ ブジェクト) > Security Profile Groups (セキュリティ プロファイル グループ) からセキュリ ティ プロファイル グループを作成することもできます。

セキュリティプロファイルのアクション

アクションには、脅威イベントに対するファイアウォールの応答方法を指定します。Palo Alto Networks で定義されている脅威やウイルス シグネチャには、デフォルト アクションが用意 されています。デフォルト アクションは通常、Alert(アラート)または Reset Both(両方の リセット)に設定されています。前者は、通知用に有効にしたオプションを使用して通知され ます。後者は、接続の両側をリセットします。ただし、デフォルト アクションは、ファイア ウォール上で定義またはオーバーライドできます。アンチウイルス プロファイル、アンチスパ イウェア プロファイル、脆弱性防御プロファイル、カスタム スパイウェア オブジェクト、カス タム脆弱性オブジェクト、または DoS プロテクション プロファイルを定義する際には、以下の アクションを適用できます。

操作	の意味	アンチウ イルスプ ロファイ ル	アンチスパ イウェアプ ロファイル	脆弱性 防御プロ ファイル	カスタム オブジェク ト – スパ イウェアと 脆弱性	DoS プロ テクション プロファイ ル
Reset Both [デ フォルト]	各脅威に対して内 部的に指定されて いるデフォルトア クションが実行さ れます。 アンチウイルスプ ロファイルの場 合、ウイルスシグ ネチャのデフォル トアクションが実 行されます。	~	~	~	_	ランダ ム早期ド ロップ
Allow [許 可]	アプリケーション トラフィックが許 可されます。	~	1	~	~	_

操作	の意味	アンチウ イルスプ ロファイ ル	アンチスパ イウェアプ ロファイル	脆弱性 防御プロ ファイル	カスタム オブジェク ト – スパ イウェアと 脆弱性	DoS プロ テクション プロファイ ル
	● Allow 前アシンはシグチまたプフイル関すロを成まん り クョ 、ネャ はロア に連るグ生しせ。					
Alert [ア ラート]	各アプリケーショ ントラフィックフ ローのアラートが 生成されます。ア ラートは脅威ログ に保存されます。					✓ 撃(cps) アでれーき達合ー成す がれ
操作	の意味	アンチウ イルスプ ロファイ ル	アンチスパ イウェアプ ロファイル	脆弱性 防御プロ ファイル	カスタム オブジェク トースパ イウェアと 脆弱性	DoS プロ テクション プロファイ ル
---	---	---------------------------	-------------------------	---------------------	---------------------------------------	-------------------------------
Drop [ド ロップ]	アプリケーション トラフィックが廃 棄されます。	~	~	~	~	_
Reset Client [ク ライア ントのリ セット]	TCP の場合、クラ イアント側の接続 がリセットされま す。 UDP の場合、接続 が廃棄されます。	1	~	\$	1	
Reset Server [サーバー のリセッ ト]	TCP の場合、サー バー側の接続がリ セットされます。 UDP の場合、接続 が廃棄されます。	~	~	~	~	_
Reset Both [両 方のリ セット]	 TCP の場合、クラ イアント側とサー バー側の両方の接 続がリセットされ ます。 UDP の場合、接続 が廃棄されます。 	~	1	1	1	
Block IP [ブロック IP]	送信元からのトラ フィックまたは送 信元と宛先のペア からのトラフィッ クが指定した期 間(設定可能)ブ ロックされます。		~	~	~	~
Sinkhole [シンク ホール]	このアクション では、悪質なド メインに向けられ たDNSクエリをシ ンクホールIPアドレ スに転送します。	_	_	_	_	_

操作	の意味	アンチウ イルスプ ロファイ ル	アンチスパ イウェアプ ロファイル	脆弱性 防御プロ ファイル	カスタム オブジェク ト – スパ イウェアと 脆弱性	DoS プロ テクション プロファイ ル
	このアクションは Palo Alto Networks DNS シグネチャお よびObjects(オ ブジェクト)> External Dynamic Lists(外部動的リ スト)に含まれる カスタム ドメイン で使用することが できます。					
ランダム 早期ップ ランダム ソウキド ロップ	1 秒あたりの接続 数が、DoS プロテ クション ルールに 適用される DoS プ ロテクション プロ ファイルの Activate Rate (アクティ ベート率)しき い値に達すると、 ファイアウォー ルによってランダ ムにパケットがド ロップされます。		_	_	_	~
SYN Cookie	1 秒あたりの接続 数が、DoS プロテ クション ルールに 適用される DoS プ ロテクション プロ ファイルの Activate Rate (アクティ ベート率)しき い値に達すると、 ファイアウォール によって、クライ アントからの SYN を認証するための SYN Cookie が生成 されます。					



ポリシー ルールで使用されているプロファイルは削除できません。まず、ポリシー ルールからプロファイルを削除する必要があります。

Objects > Security Profiles > Antivirus [オブジェクト > セキュリティ プロファイル > アンチウイルス]

Antivirus Profiles[アンチウイルス プロファイル] ページを使用して、定義されたトラフィック に対するファイアウォールのウイルス スキャンのオプションを設定します。ウイルス検査対象 のアプリケーションと、ウイルス検出時に実行するアクションを設定します。デフォルトのプ ロファイルでは、表示されているすべてのプロトコル デコーダがウイルス検査の対象になりま す。Simple Mail Transport Protocol (SMTP)、Internet Message Access Protocol (IMAP)、および Post Office Protocol Version 3 (POP3) ではアラートが生成され、他のアプリケーションでは検出 されたウイルスのタイプに応じてデフォルトのアクション (アラートまたは拒否) が実行されま す。次にプロファイルは、特定のゾーンを通過するトラフィックから検査対象のトラフィックを 判別するため、セキュリティ ポリシー ルールに適用されます。

カスタマイズしたプロファイルを使用して、信頼されたセキュリティ ゾーン間のトラフィック に対するアンチウイルスの検査を最小限に抑え、インターネットなどの信頼されていないゾー ンから受信したトラフィックや、サーバーファームなどの機密性の高い宛先に送信されるトラ フィックの検査を最大化できます。

新しいアンチウイルスプロファイルを追加する場合は、Add (追加) を選択し、以下の設定を行い ます。

項目	の意味
氏名	プロファイル名(最大 31 文字)を入力します。この名前は、セキュ リティ ポリシーを定義するときにアンチウイルス プロファイルのリ ストに表示されます。名前の大文字と小文字は区別されます。また、 一意の名前にする必要があります。文字、数字、スペース、ハイフ ン、ピリオド、およびアンダースコアのみを使用してください。
の意味	プロファイルの説明を入力します (最大 255 文字)。
Shared (Panorama only)	 以下に対してプロファイルを公開する場合は、このオプションを選択します。 multi-vsys ファイアウォールの各仮想システム (vsys)。この選択を解除すると、Objects[オブジェクト] タブで選択した Virtual System[仮想システム]のみに対してプロファイルが公開されます。 Panorama 上の各デバイス グループ。この選択を解除すると、Objects[オブジェクト] タブで選択した Device Group[デバイスグループ]のみに対してプロファイルが公開されます。
オーバーライドの無 効化(Panoramaの み)	管理者が、プロファイルを継承するデバイス グループのこのアンチ ウイルス プロファイルの設定をオーバーライドすることを禁止する 場合はこのオプションを選択してください。デフォルトでこのオプ

項目	の意味
	ションはオフになっており、管理者は、このプロファイルを継承する デバイス グループの設定をオーバーライドできます。
[アクション] タブ	
FTP や HTTP など、様	々なタイプのトラフィックに対するアクションを指定します。
Enable Packet Capture(パケット キャプチャを有効に する)	識別されたパケットをキャプチャする場合は、このオプションを選択 します。
WildFireのリアルタ イムシグネチャ検索 を長押し	ファイアウォールがリアルタイムシグネチャクラウドに対してリアル タイムシグネチャの検索を完了するまでパケットをホールドしたい場 合は、このオプションを選択します。
	 また、ホールドモードを完全に有効にする前に、Device > Setup > Content-ID [デバイス > セットアップ > Content-ID]で Hold for WildFire Real Time Signature Look Up (WildFireリアルタイム シグネチャルックアップのホールド)をグローバルに有効化する必要があります。
デコーダとアクション	ウイルスを検査するトラフィックのタイプごとに、ドロップダウン リストからアクションを選択します。標準のウイルス対策シグネチャ (Signature Action(シグネチャアクション)列)、WildFire システ ムが生成したシグネチャ(WildFire Signature Action(WildFire シグ ネチャアクション)列)、および WildFire インライン ML モデルリ アルタイムで検出した悪意のある脅威(WildFire インライン ML ア クション列)に対して、多様なアクションを定義することができま す。 環境によっては、アンチウイルス シグネチャに長めのソーク時間 を必要とするため、このオプションでは、Palo Alto Networks が提 供する 2 つのアンチウイルス シグネチャ タイプに異なるアクショ ンを設定できます。たとえば、標準のアンチウイルス シグネチャ は、リリースされるまでのソーク時間がより長い (24 時間) のに対 し、WildFire シグネチャは脅威が検出されてから 15 分以内に生成 されてリリースされます。このため、アクションに block ではな く、WildFire シグネチャに基づく alert を選択する必要が生じること もあります。

項目	の意味
	 デフォルトのアンチウイルス プロファイルをコピー してすべてのデコーダの Action (アクション) および WildFire Action (WildFire アクション) をreset-bothに設定 し、そのプロファイルをトラフィックを許可するすべ てのセキュリティポリシールールに適用することで、 セキュリティを最大限に高めることができます。
Application Exceptions and Actions(アプリケー ション例外とアク ション)	Applications Exception (アプリケーション例外) 表では、検査対象 外のアプリケーションを定義することができます。たとえば、特定の アプリケーションを除くすべての HTTP トラフィックをブロックする には、そのアプリケーションが例外になるようにアンチウイルス プ ロファイルを定義します。Block[ブロック] は HTTP デコーダに対す るアクションで、Allow[許可] はアプリケーションの例外です。アプ リケーション例外ごとに、脅威の検出時に実行するアクションを選択 します。アクションのリストについては、「セキュリティ プロファ イルのアクション」を参照してください。
	アプリケーションを検索するには、アプリケーション名をテキスト ボックスに入力します。一致するアプリケーションのリストが表示さ れ、選択ができるようになります。
	正当なアプリケーションにウイルスが含まれていると 誤って判断された場合(誤検出)、TACを使ってサ ポートケースを開始し、Palo Alto Networks が誤って検 出されたウイルスを分析して修正できるようにしてく ださい。問題が解決されたら、プロファイルから例外 を削除します。

Signature Exceptions Tab(シグネチャ例外タブ)

Signature Exception (シグネチャの例外) タブを使用して、アンチウイルスプロファイルで無 視する脅威のリストを定義します。

検出されたウイルスが実際にはウイルスでないことが確実である場合のみ(誤検出)、例外を作成します。誤検出が見つかったと考えられる場合は、TACを使ってサポートケースを開始し、Palo Alto Networks が誤って検出されたウイルスシグネチャを分析して修正できるようにしてください。問題が解決されたら、プロファイルからすぐに例外を削除します。

脅威 ID	無視したい特定の脅威を追加する場合は、脅威IDを1つずつ入力 し、Add[追加] をクリックします。Threat ID は、Threat ログの情報
	の一部として表示されます。「Monitor(監視) > Logs(ログ)」を 参照してください。

WildFire Inline ML Tab (WildFire $4 \vee 5 4 \vee ML \otimes 7$)

項目	の意味
WildFire Inline ML(W の機械学習モデルを使 す。	/ildFire インライン ML)タブを使用して、ファイアウォール ベース 用したファイルのリアルタイム WildFire 分析を有効化した設定にしま
Palo Alto Networ プルを WildFire の分析時に誤検 さらに、将来の〕	ks では、Wildfire インライン ML が有効化されている場合、サン クラウドに転送することを推奨しています。これにより、次回 知をトリガするサンプルを自動的に修正することができます。 更新に向けて、ML モデルを改善するデータの提供となります。
モデル ラインナップ	利用可能な WildFire インラインML モデルのそれぞれに、以下のアク ション設定のいずれかを選択することができます。
	 有効化 (プロトコル毎のアクションを継承) – トラフィックは、 Action (アクション) タブのデコーダ セクションにある WildFire Inline ML Action (WildFire インライン ML アクション) 列におけ る選択に従い、検査されます。
	 アラートのみ(アラートより厳密なアクションをオーバーライドする) –トラフィックは、Action(アクション)タブのデコーダセクションにある WildFire Inline ML Action(WildFire インライン MLアクション)列における選択に従い、検査されます。重大度レベルがアラートよりも高いアクション(ドロップ、クライアントのリセット、サーバーリセット、両方リセット)はアラートで上書きされ、アラートを生成して脅威ログに保存し、トラフィックを通過させることができます。
	 無効化(すべてのプロトコル対象) – トラフィックは、ポリシーアクションなしでトラフィックの通過を許可されます。
File Exceptions(ファイ ル例外)	 File Exceptions (ファイル例外) 表を使用すると、誤検知等の分析しない特定のファイルを定義することができます。 新しいファイル例外エントリを作成するには、新しいエントリをAdd(追加)し、適用から除外するファイルの部分ハッシュ、ファイル名、および説明を指定します。 既存のファイル例外を検索するには、テキストボックスにハッシュ値、ファイル名、または説明の一部を入力します。入力した値のいずれかに一致するファイル例外のリストが表示されます。 部分ハッシュは脅威ログで検索可能です (Monitor (監)
	 部分ハッシュは脅威ログで検索可能です(Monitor(監視) > Logs(ログ) > Threat(脅威)。

Objects(オブジェクト) > Security Profiles(セキュリ ティプロファイル) > Anti-Spyware Profile(アンチス パイウェアプロファイル)

アンチスパイウェア プロファイルをセキュリティ ポリシー ルールに関連付けることで、ネット ワーク上のシステムにインストールされたスパイウェアや多様なタイプのコマンドアンドコント ロール(C2)マルウェアによって起動された接続を検出できます。セキュリティ ポリシー ルー ルに割り当てる2つの事前定義済みアンチスパイウェア プロファイルのどちらかを選択できま す。各プロファイルには、脅威の重大度別に整理された事前定義ルールのセットが用意されてい ます。各脅威シグネチャには、Palo Alto Networks によって指定されたデフォルト アクション が含まれています。

- Default(デフォルト) デフォルト プロファイルは、署名の作成時に Palo Alto Networks コンテンツパッケージで指定される通り、重大度がCritical、High、Medium、Low のシグニ チャに対してデフォルトのアクションを採用します。情報として分類されたイベントのシグ ニチャ ポリシーは含まれません。
- Strict strict プロファイルは、重要、高、中の重大度の脅威のシグネチャファイルに定義されているアクションをオーバーライドして、reset-bothアクションに設定します。デフォルトアクションは、低および情報の重大度を持つ脅威とみなされます。
- カスタムのプロファイルを作成することもできます。たとえば、信頼されたセキュリティ ゾーン間のトラフィックのアンチスパイウェア検査における厳重度を軽減して、インター ネットから受信したトラフィック、またはサーバーファームなどの保護資産に送信されるト ラフィックの検査の厳重度を最大化するといったことができます。

以下の表では、アンチスパイウェア プロファイル □ 設定について説明します。

アンチスパイウェア プ ロファイル設定	の意味
氏名	プロファイル名(最大 31 文字)を入力します。この名前は、セ キュリティポリシーを定義するときにアンチスパイウェアプロファ イルのリストに表示されます。名前の大文字と小文字は区別されま す。また、一意の名前にする必要があります。文字、数字、スペー ス、ハイフン、ピリオド、およびアンダースコアのみを使用してく ださい。
の意味	プロファイルの説明を入力します (最大 255 文字)。
共有(Panorama の み)	以下に対してプロファイルを公開する場合は、このオプションを選 択します。
	 multi-vsys ファイアウォールの各仮想システム (vsys)。この選択 を解除すると、Objects[オブジェクト] タブで選択した Virtual

アンチスパイウェア プ ロファイル設定	の意味
	 System[仮想システム] のみに対してプロファイルが公開されます。 Panorama 上の各デバイス グループ。この選択を解除すると、Objects[オブジェクト] タブで選択した Device Group[デバイスグループ] のみに対してプロファイルが公開されます。
オーバーライドの無効 化(Panoramaのみ)	管理者が、プロファイルを継承するデバイス グループのこのアンチ スパイウェア プロファイルの設定をオーバーライドすることを禁止 する場合はこのオプションを選択してください。デフォルトでこの オプションはオフになっており、管理者は、このプロファイルを継 承するデバイス グループの設定をオーバーライドできます。

Signature Policies Tab (シグネチャ ポリシー タブ)

アンチスパイウェア ルールでは、カスタム重大度を定義し、任意の脅威(入力したテキスト を含む名前を持つ特定の脅威、そしてアドウェアなどの脅威カテゴリ)に対して取るべきア クションを定義することができます。

新しいルールを Add(追加)します。または、既存のルールを選択して Find Matching Signatures(一致するシグネチャの検索)を選択し、そのルールに基づいて脅威シグネチャを フィルタリングできます。

ルール名	ルール名を指定します。
脅威名	すべてのシグネチャを照合する場合はanyと入力します。または、 シグネチャ名の一部として入力されたテキストを含むすべてのシグ ネチャを照合するテキストを入力します。
カテゴリ	カテゴリを選択するか、 any (すべて) を選択してすべてのカテゴリ にマッチさせます。
操作	各脅威のアクションを選択します。アクションのリストについて は、「セキュリティ プロファイルのアクション」を参照してくださ い。
	Default[デフォルト] アクションは、Palo Alto Networks によっ て提供された各シグネチャの一部である事前定義のアクション に基づきます。シグネチャのデフォルトのアクションを表示す るには、Objects(オブジェクト) > Security Profiles(セキュリ ティプロファイル) > Anti-Spyware(アンチスパイウェア)を 選択し、Add(追加)を選択するか、既存のプロファイルを選 択します。Exceptions(例外)タブをクリックして Show all signatures(すべてのシグネチャの表示)をオンにすると、すべて のシグネチャと関連する Action(アクション)のリストが表示され ます。

アンチスパイウェア プ ロファイル設定	の意味
	 事前定義済みのstrict (厳格)なプロファイルの Action (アクション) 設定を使用することで、セキュリティを 最大化できます。
パケット キャプチャ	識別されたパケットをキャプチャする場合は、このオプションを選 択します。
	高度なインラインクラウド分析エンジンを使用して検出された脅威は、パケットキャプチャデータを生成しません。
	脅威が検出されたときに1つのパケットをキャプチャするに は、single-packet、1~50個のパケットをキャプチャするに は、extended-capture オプションを選択します(デフォルトは5 パケットです)。extended-capture では、脅威ログを分析すると きに脅威についてより詳細なコンテクストを得られます。パケット キャプチャを表示する場合は、Monitor(監視) > Logs(ログ) > Threat(脅威)を選択し、関心のあるログエントリを見つけて、 第2列にある緑の下矢印をクリックします。キャプチャするパケッ トの数を定義するには、Device(デバイス) > Setup(セットアッ プ) > Content-IDを選択し、Content-ID [™] 設定を編集します。
	特定の脅威に対するアクションが許可されている場合、ファイア ウォールは脅威ログをトリガせず、パケットをキャプチャしませ ん。アクションがアラートである場合は、パケット キャプチャを シングル パケット キャプチャまたは拡張キャプチャに設定できま す。すべてのブロッキングアクション(ドロップ、ブロック、およ びリセットアクション)は、単一のパケットをキャプチャします。 デバイス上のコンテンツ パッケージは、デフォルトのアクションを 決定します。
	● 重大度が critical (重 要)、high(高)、medium(中)のイベントに対して拡張キャプチャを有効化します。デフォルトの拡張キャプチャの値(5パケット)を使用することで、大抵の場合に脅威を分析するための十分な情報を得られます。(パケットキャプチャのトラフィックが多すぎると、パケットキャプチャをドロップするおそれがあります)重大度が高いイベントと比べて情報のキャプチャがそれ程役立たず、低い値のトラフィックが比較的多く発生するため、重大度が informational (通知)以下のイベントに対して拡張キャプチャを有効化しないでください。

アンチスパイウェア プ ロファイル設定	の意味
重要度	重大度レベル (critical[重要]、high[高]、medium[中]、low[低]、また は informational[通知]) を選択します。

Signature Exceptions Tab(シグネチャ例外タブ)

特定のシグネチャに対するアクションを変更できます。たとえば、特定のシグネチャセット についてアラートを生成し、他のすべてのシグネチャに一致するすべてのパケットをブロッ クできます。脅威例外は、通常、誤検出が発生したときに設定します。=脅威例外の管理を容 易にするために、脅威例外を Monitor(監視) > Logs(ログ) > Threat(脅威)リストから 直接追加できます。新規の脅威から保護されるように、または誤検出に対する新しいシグネ チャがインストールされるように、最新のコンテンツ更新を取得してください。

例外	アクションを割り当てようとしている脅威をそれぞれEnable (有効 化) するか、All (すべて) を選択してリストにあるすべての脅威に対 するアクションを有効化します。このリストは、選択したホスト、 カテゴリ、および重大度によって異なります。リストが空の場合、 現在の選択に対応する脅威がないことを表します。
	IP Address Exemptions (IP アドレスの除外)を使用して、脅威例外を フィルタリングする IP アドレスを追加します。脅威例外に IP アド レスが追加されている場合、そのシグネチャの脅威例外アクション は、例外の IP アドレスにマッチする送信元あるいは宛先 IP アドレ スを持つセッションがシグネチャをトリガーした場合にのみ、ルー ルのアクションをオーバーライドします。シグネチャあたり最大 100 個の IP アドレスを追加できます。このオプションでは、特定 の IP アドレスの例外を作成するために新しいポリシー ルールと新 しい脆弱性プロファイルを作成する必要はありません。
	スパイウェアとして識別されたシグネチャが脅威でないことが確かな場合(誤検出)のみ、例外を作成するようにしてください。誤検出が見つかったと考えられる場合は、TACを使ってサポートケースを開始し、Palo Alto Networks が誤って検出されたシグネチャを分析して修正できるようにしてください。問題が解決されたらすぐ、プロファイルから例外を削除します。

DNS Policies Tab (**DNS** ポリシー タブ)

DNS Policies(DNS ポリシー) 設定は、ネットワーク上の感染したホストを特定する追加の 方法です。これらのシグネチャは、DNS ベースの脅威に関連付けられているホスト名に対す る特定の DNS ルックアップを検出します。

個別のポリシー アクション、ログの重大度レベル、およびパケット キャプチャ設定を使用して、特定の DNS シグネチャ 送信元を設定することができます。マルウェアドメインの DNS

アンチスパイウェア プ ロファイル設定	の意味
クエリを実行するホスト DNS クエリに対してシン 設定)内のシンクホール I	はボットネットレポートに表示されます。さらに、マルウェアの / クホールを行う場合は、DNS Sinkhole Settings (DNS シンクホール P を指定できます。
DNS シグネチャ ソー ス	DNSクエリが発生した場合にアクションを強制的に実施する対象の リストを選択できます。デフォルトの DNS シグネチャ ポリシーの オプションは 2 つあります:
	 Palo Alto Networks コンテンツーダイナミックなコンテンツ更 新を通じて更新される、ローカルのダウンロード可能なシグネ チャです。
	 DNS セキュリティーDNS データのプロアクティブな分析を実行 するクラウドベースの DNS セキュリティサービスであり、Palo Alto Networks DNS シグネチャ データベース全体へのリアルタ イムのアクセスを提供します。
	このサービスを使用するには、脅威防止ライセン スに加えて DNS セキュリティ ライセンスを購入し てアクティベートする必要があります。
	 外部動的リスト –ドメインリストとして動作するEDLを使用して、アラートリストとして選択したドメインに対して特定のアクションを適用できます。既定では、ドメインリストのポリシー アクションは [許可] に設定されています。
	 EDL 許可リストは、DNS セキュリティで指定され たドメイン ポリシーアクションよりも優先されま せん。その結果、EDL のエントリと DNS セキュリ ティドメイン カテゴリに一致するドメインがあ る場合、EDL が許可のアクションで明示的に構成 されている場合でも、DNS セキュリティで指定さ れたアクションは適用されます。DNS ドメインの 例外を追加する場合は、アラート アクションを使 用して EDL を構成するか、DNS 例外 タブにある DNS ドメイン/FQDN 許可リスト に追加します。
	デフォルト設定では、ローカルでアクセスできる Palo Alto Networks DNS シグネチャ コンテンツの DNS シグネチャはシン クホールされますが、クラウドベースの DNS セキュリティでは 許可するように設定されています。DNS セキュリティを使用す るシンクホールを有効化したい場合、DNS クエリのアクション をシンクホールに設定する必要があります。シンクホールに使用 されるデフォルトのアドレスは Palo Alto Networks のものです (sinkhole.paloaltonetworks.com)。このアドレスは静的ではな

アンチスパイウェア プ ロファイル設定	の意味
	く、ファイアウォールや Panorama のコンテンツアップデートを通 じて変更される場合があります。
	新しいリストを追加する場合はAdd (追加)し、以前作成済の、タ イプがドメインの外部動的リストを選択します。新しいリストを 作成する方法については、「Objects(オブジェクト) > External Dynamic Lists(外部動的リスト)」を参照してください。
ログ重大度	ファイアウォールが DNS シグネチャに一致するドメインを検出し たときに記録される、ログの重大度レベルを指定することができま す。
Policy Action(ポリ シーアクション)	既知のマルウェア サイトに対して DNS ルックアップが実行され たときに実行するアクションを選択します。ここではalert (アラー ト)、allow (許可)、block (ブロック)、sinkhole (シンクホール)を使 用できます。Palo Alto Networks DNSシグネチャのデフォルトアク ションはsinkhole (シンクホール)です。
	 DNS シンクホール アクションを使用すると、管理者は、ファイアウォールがローカル DNS サーバーよりもインターネット側にある(ファイアウォールが DNS クエリの発行元を認識できない)場合も含め、DNSトラフィックを使用してネットワーク上の感染ホストを特定することができます。脅威防御ライセンスがインストールされていて、セキュリティプロファイルでアンチスパイウェアプロファイルが有効な場合、DNSベースのシグネチャが、マルウェアドメインへの DNS クエリによってトリガーします。ファイアウォールがローカル DNS サーバーよりもインターネット側にある通常のデプロイメントでは、脅威ログは、実際の感染ホストではなくローカル DNS リゾルバをトラフィックの送信元として識別します。マルウェア DNS クエリをシンクホールすると、有害なドメインへのクエリに対する応答を偽装することで、この可視性の問題が解決されます。そのため、悪意のあるドメイン(たとえば、コマンドアンドコントロールなど)への接続を試みるクライアントは、代わりに管理者が指定した IP アドレスへに接続を試みることになります。こうすることで、感染ホストをトラフィックログ内で容易に特定できます。シンクホール IP への接続を試みるホストはすべて、マルウェアに感染している可能性が高いためです。 ファイアウォールが DNS クエリの元の送信者を確認できない際(典型的には、ファイアウォールがローカル DNS サーバーのノースにあたる場合)に DNS シンクホールを有効化し、感染ホストを識別できるようにします。トラフィックをシンクホールできない場合はブロックしてください。

アンチスパイウェア プ ロファイル設定	の意味
パケット キャプチャ	識別されたパケットをキャプチャする場合は、任意の送信元に対し てこのオプションを選択します。
	シンクホールされたトラフィックに対するパケット キャプチャを有効化し、それを分析して感染ホストに ついての情報を得られるようにしてください。
DNS シンクホールの設 定	DNS シグネチャ ソース用のシンクホール アクションを定義し た後、シンクホールに使用する IPv4 アドレスおよび(もしく は) IPv6 アドレスを指定します。デフォルトでは、シンクホール のIPアドレスはPalo Alto Networksサーバーに設定されています。 こうすることで、トラフィックログを使用し、あるいはシンクホー ルのIPアドレスでフィルタをかけるカスタムレポートを作成し、感 染したクライアントを特定することができます。
	以下は、DNS要求がシンクホールに掛けられた場合に発生するイベ ントの流れです。
	感染したクライアント コンピュータ上の有害なソフトウェアが DNS クエリを送信して、インターネット上の有害なホストを解決 します。
	クライアントの DNS クエリが内部 DNS サーバーに送信され、ファ イアウォールの反対側にある公開 DNS サーバーをクエリします。
	DNS クエリは、指定した DNS シグネチャ データベース ソース内 の DNS エントリと一致するため、シンクホール アクションがクエ リに対して実行されます。
	感染したクライアントは、そのホストでセッションを開始しようとしますが、代わりに偽装 IP アドレスを使用します。偽装 IP アドレスは、アンチスパイウェア プロファイルの [DNS シグネチャ] タブでシンクホール アクションが選択されたときに定義されたアドレスです。
	管理者は、脅威ログに有害な DNS クエリがあるというアラート通 知を受け取り、トラフィック ログ内のシンクホール IP アドレスを 検索して、シンクホール IP アドレスでセッションを開始しようと しているクライアント IP アドレスを容易に特定できます。
DNS レコード タイプ をブロックする	ブロックする暗号化された DNS クエリで使用される DNS リソース レコードの種類を選択します。これにより、DNS 解決プロセス中 にクライアントがクライアント hello を暗号化するのを防ぎ、キー 情報の交換をブロックします。
	オプションには、SVCB (タイプ 64)、HTTPS (タイプ 65)、および ANY (タイプ 255) があります。



DNS Exceptions Tab(**DNS**例外 タブ)

DNS シグネチャ例外により、特定の脅威 ID をポリシー適用から除外したり、承認済ドメイン送信元のドメインまたは FQDN 許可リストを指定したりすることができます。

ポリシーから除外したい特定の脅威を追加するには、Threat ID (脅威 ID)を選択あるいは 検索してEnable (有効化)をクリックします。各エントリがオブジェクトのThreat ID (脅威 ID)、Name (名称)、および FQDN を提示します。

ドメインまたは FQDN 許可リストをAdd(追加)するには、許可リストの場所および適切な 説明を入力します。

Inline Cloud Analysis Tab

Inline Cloud Analysis では、高度な C2 脅威のリアルタイム分析の設定を、検出エンジンごとに有効にして構成できます。

Enable cloud inline analysis - 利用可能なすべてのディープ インライン クラウド分析エンジン で高度な C2 脅威のリアルタイム分析を可能にします。

利用可能な分析エンジ ン	脅威カテゴリを表す使用可能な分析エンジンごとに、対応する脅威 が検出されたときに firewall が強制する次のいずれかのアクション を選択できます。
	 Allow(許可する) –Web サイトが許可され、ログエントリは 生成されません。
	 Alert(アラート) –Web サイトが許可され、URL フィルタリン グログにログエントリが生成されます。
	 Drop - トラフィックをドロップします。リセット アクションは ホスト/アプリケーションに送信されません。
	• Reset-Client - クライアント側の接続をリセットします。
	• Reset-Server - サーバー側の接続をリセットします。
	 Reset-Both – クライアント側とサーバー側の両方で接続をリ セットします。
	すべての分析エンジンのデフォルトのアクションはア ラートです。

アンチスパイウェア プ ロファイル設定	の意味	
インライン クラウド分 析から除外する	インライ ドレス例 用して指 カスタム は Addre て、使用 プを選択	イン クラウド分析エンジンをバイパスする URL または IP ア 列外リストを選択できます。例外は、URLやIPアドレスを使 定できます。URL 例外には EDL (外部動的リスト) または A URL カテゴリが含まれ、IP アドレス例外には EDL また ess オブジェクトが含まれます。Add(追加)をクリックし 引可能なオプションを表示して選択します。次のリストタイ できます。
	• EDL Exter	JRL — 一連の URL またはカスタム URL カテゴリを含む nal Dynamic Lists です。
	• IP Ad 内で知	dress – External Dynamic List または Address オブジェクト 定義された IP アドレス リスト。
		IP アドレスと URL の例外は、誤検知の場合など、 特定された脅威が危険を引き起こさない場合にの み作成してください。

Objects > Security Profiles > Vulnerability Protection [オ ブジェクト > セキュリティプロファイル > 脆弱性防御]

セキュリティ ポリシー ルールでは脆弱性防御プロファイルを指定できます。このプロファイル では、システムの脆弱性を悪用するバッファ オーバーフローや不正コードの実行などに対する 保護レベルを定義します。脆弱性防御機能では、以下の2つの事前定義済みプロファイルを使 用できます。

- default プロファイルでは、default アクションがすべてのクライアントおよびサーバーの重大 度が critical、high、medium の脆弱性に適用されます。low および informational の脆弱性防 御イベントは検出されません。デバイス上の Palo Alto Networks のコンテンツ パッケージが デフォルトのアクションを決定します。
- strict プロファイルでは、block 応答がすべてのクライアントおよびサーバーの重大度が critical、high、medium のスパイウェア イベントに適用され、default アクションが low およ び informational の脆弱性防御イベントに使用されます。

カスタマイズしたプロファイルを使用して、信頼されたセキュリティゾーン間のトラフィック に対する脆弱性の検査を最小限に抑え、インターネットなどの信頼されていないゾーンから受信 したトラフィックや、サーバーファームなどの機密性の高い宛先に送信されるトラフィックの 保護を最大化できます。脆弱性防御プロファイルをセキュリティポリシーに適用する方法につ いては、「Policies(ポリシー) > Security(セキュリティ)」を参照してください。

トラフィックを許可するすべてのセキュリティポリシールールに脆弱性保護プロ ファイルを適用し、バッファオーバーフロー、不正なコードの実行、およびクライ アント側およびサーバー側の脆弱性を狙ったその他の攻撃から保護します。

Rules [ルール] 設定では、有効にする一連のシグネチャと、一連のシグネチャのいずれかがトリガーされたときに実行するアクションを指定します。

例外設定では、特定のシグネチャに対するレスポンスを変更できます。たとえば、シグネチャに 一致するすべてのパケットをブロックするが選択したシグネチャに一致するパケットはブロック しないでアラートを生成するということが可能です。Exception[例外] タブでは、フィルタリン グ機能がサポートされています。

Vulnerability Protection[脆弱性防御] ページには、一連のデフォルト列が表示されます。列を選 択するオプションを使用すれば、その他の情報列を表示できます。列ヘッダーの右側にある矢印 をクリックし、Columns [カラム] サブメニューから列を選択します。

脆弱性防御プロファイ ル設定	の意味
氏名	プロファイル名(最大 31 文字)を入力します。この名前は、セ キュリティポリシーを定義するときに脆弱性防御プロファイルの リストに表示されます。名前の大文字と小文字は区別されます。 また、一意の名前にする必要があります。文字、数字、スペース、

以下の表では、脆弱性防御プロファイル設定について説明します。

脆弱性防御プロファイ ル設定	の意味
	ハイフン、ピリオド、およびアンダースコアのみを使用してくださ い。
の意味	プロファイルの説明を入力します (最大 255 文字)。
共有(Panorama の み)	以下に対してプロファイルを公開する場合は、このオプションを選 択します。
	 multi-vsys ファイアウォールの各仮想システム (vsys)。この選択 を解除すると、Objects[オブジェクト] タブで選択した Virtual System[仮想システム] のみに対してプロファイルが公開されま す。
	 Panorama 上の各デバイス グループ。この選択を解除する と、Objects[オブジェクト] タブで選択した Device Group[デバ イスグループ] のみに対してプロファイルが公開されます。
オーバーライドの無効 化(<mark>Panoramaのみ</mark>)	管理者が、プロファイルを継承するデバイス グループのこの脆弱性 防御プロファイルの設定をオーバーライドすることを禁止する場合 はこのオプションを選択してください。デフォルトでこのオプショ ンはオフになっており、管理者は、このプロファイルを継承するデ バイス グループの設定をオーバーライドできます。
Rules (ルール) タブ	
ルール名	ルールの識別に使用する名前を指定します。
脅威名	照合するテキスト文字列を指定します。ファイアウォールは、この テキスト文字列のシグネチャ名を検索して一連のシグネチャをルー ルに適用します。
CVE	指定した CVE に一致する場合にのみシグネチャを適用するに は、CVE (Common Vulnerabilities and Exposures) を指定します。
	各 CVE の形式は CVE-yyyy-xxxx になります。ここで、yyyy は 年、xxxx は一意識別子です。このフィールドで文字列の照合を実行 できます。たとえば、2011 年の脆弱性を検索するには「2011」と 入力します。
ホスト タイプ	ルールのシグネチャをクライアント側、サーバー側、またはいずれ か (any) に限定するかどうかを指定します。
重要度	指定した重大度にも一致する場合にのみシグネチャ を適用するには、照合する重大度 (informational[通

脆弱性防御プロファイ ル設定	の意味
	知]、low[低]、medium[中]、high[高]、または critical[重要]) を選択 します。
操作	ルールがトリガーされたときに実行するアクションを選択します。 アクションのリストについては、「セキュリティ プロファイルのア クション」を参照してください。
	Default[デフォルト] アクションは、Palo Alto Networks によっ て提供された各シグネチャの一部である事前定義のアクション に基づきます。シグネチャのデフォルトのアクションを表示す るには、Objects(オブジェクト) > Security Profiles(セキュリ ティプロファイル) > Vulnerability Protection(脆弱性防御)を 選択し、Add(追加)をクリックするか、既存のプロファイルを 選択します。Exceptions(例外)タブをクリックして Show all signatures(すべてのシグネチャの表示)をオンにすると、すべて のシグネチャと関連する Action(アクション)のリストが表示され ます。
	 セキュリティを最大限に高めるために、クライ アントおよびサーバー両方の critical (重要)、high (高)、medium (中)の重大度を持つイベントに 対する Action (アクション)をreset-bothに設定 し、Informational (通知) および Low (低)の重大度を持 つイベントに対してデフォルトのアクションを使用し てください。
パケット キャプチャ	識別されたパケットをキャプチャする場合は、このオプションを選 択します。
	高度なインラインクラウド分析エンジンを使用して検 出された脅威は、パケットキャプチャデータを生成し ません。
	脅威が検出されたときに1つのパケットをキャプチャするに は、single-packet、1~50個のパケットをキャプチャするに は、extended-capture オプションを選択します(デフォルトは5 パケットです)。extended-capture では、脅威ログを分析すると きに脅威についてより詳細なコンテクストを得られます。パケット キャプチャを表示する場合は、Monitor(監視)>Logs(ログ)> Threat(脅威)を選択し、関心のあるログエントリを見つけて、 第2列にある緑の下矢印をクリックします。キャプチャするパケッ トの数を定義するには、Device(デバイス)>Setup(セットアッ プ)>Content-IDを選択し、Content-ID 設定を編集します。

脆弱性防御プロファイ ル設定	の意味
	特定の脅威に対するアクションが許可されている場合、ファイア ウォールは脅威ログをトリガせず、パケットをキャプチャしませ ん。アクションがアラートである場合は、パケット キャプチャを シングル パケット キャプチャまたは拡張キャプチャに設定できま す。すべてのブロッキングアクション(ドロップ、ブロック、およ びリセットアクション)は、単一のパケットをキャプチャします。 デバイス上のコンテンツ パッケージは、デフォルトのアクションを 決定します。
	● 重大度が critical (重要)、high (高)、medium (中)のイベント用に拡張キャプチャを、重大度が low (低)のイベント用に単一パケット キャプチャを有効化します。デフォルトの拡張キャプチャの値 (5パケット)を使用することで、大抵の場合に脅威を分析するための十分な情報を得られます。(パケット キャプチャのトラフィックが多すぎると、パケット キャプチャをドロップするおそれがあります)重大度が高いイベントと比べて情報のキャプチャがそれ程役立たず、低い値のトラフィックが比較的多く発生するため、informationa (通知)のイベントに対してパケットキャプチャを有効化しないでください。
	ログに記録するトラフィックを判断するために使用す るロジックと同じものを使用して拡張パケット キャ プチャを適用します(ブロックするトラフィックを含 め、ログに記録するトラフィックの拡張キャプチャを 行います)。

Exceptions [例外] タブ

有効化	アクションを割り当てようとしている脅威に対してEnable[有効化] をそれぞれ選択するか、All[すべて]を選択してリストにあるすべて の脅威に対するアクションを有効化します。このリストは、選択し たホスト、カテゴリ、および重大度によって異なります。リストが 空の場合、現在の選択に対応する脅威がないことを表します。
ID	
ベンダー ID	指定したベンダー ID に一致する場合にのみシグネチャを適用する には、ベンダー ID を指定します。
	たとえば、Microsoft のベンダー ID の形式は MSyy-xxx になります。ここで、yy は 2 桁の年で、xxx は一意識別子です。たとえ

脆弱性防御プロファイ ル設定	の意味	
	ば、2009 年の Microsoft を照合するには Search (検索) フィールド に「MS09」と入力します。	
脅威名	見つかった脅威が実際には脅威でないことが定かな場合のみ(誤検出)、脅威例外を作成します。誤検出が見つかったと考えられる場合は、TACを使ってサポートケースを開始し、Palo Alto Networks が誤って検出された脅威を調査できるようにしてください。問題が解決されたら、プロファイルからすぐに例外を削除します。	-
	脆弱性シグネチャ データベースには、総当たり攻撃を表すシグ ネチャが格納されています。たとえば、Threat ID 40001 は FTP 総当たり攻撃でトリガーされます。総当たり攻撃のシグネチャ は、特定の時間のしきい値で条件が発生した場合にトリガーさ れます。総当たり攻撃のシグネチャのしきい値は事前に設定され ています。これは、(Custom[カスタム] オプションが選択された 状態で)Vulnerability[脆弱性] タブの脅威の名前の横にある編集	
	(をクリックして変更できます。単位時間あたりのヒット数やしきい 値の適用先 (送信元、宛先、または送信元と宛先の組み合わせ) を指 定できます。)
	しきい値は、送信元 IP、宛先 IP、または送信元 IP と宛先 IP の組み 合わせに適用できます。	
	デフォルトのアクションが、かっこに囲まれて表示されます。	
IP アドレス免除	IP Address Exemptions(IP アドレスの除外)列をクリックして、 脅威例外をフィルタリングする IP アドレスを Add(追加)しま す。脅威例外に IP アドレスを追加する場合、そのシグネチャの 脅威例外アクションは、送信元または宛先 IP アドレスのいずれか が例外の IP アドレスに一致するセッションによってシグネチャが トリガーされる場合にのみ、ルールのアクションよりも優先され ます。シグネチャあたり最大 100 個の IP アドレスを追加できま す。10.1.7.8 や 2001:db8:123:1::1 などのユニキャス IP アドレス (ネットマスクのないアドレス)を入力する必要があります。IP ア ドレスの除外を追加すると、特定の IP アドレスの例外を作成する ために新しいポリシー ルールと新しい脆弱性プロファイルを作成す る必要がなくなります。	-
		-

rule

脆弱性防御プロファイ ル設定	の意味
CVE	[CVE] 列には、CVE (Common Vulnerabilities and Exposures)の識別 子が表示されます。これらは、公開されている情報セキュリティの 脆弱性に対応する共通の一意の識別子です。
ホスト	
カテゴリ	脆弱性のカテゴリに一致する場合にのみシグネチャを適用するに は、脆弱性のカテゴリを選択します。
重要度	
操作	各ドロップダウンリストからアクションを選択するか、リストの上 部にある Action[アクション] のドロップダウンリストからアクショ ンを選択してすべての脅威に同じアクションを適用します。
パケット キャプチャ	識別されたパケットをキャプチャする場合は、 Packet Capture (パ ケット キャプチャ)を選択します。
すべてのシグネチャの 表示	Show all signatures (すべてのシグネチャの表示)を有効化して、 すべてのシグネチャをリスト表示します。Show all signatures (す べてのシグネチャの表示)が無効化されている場合は、例外のシグ ネチャのみがリスト表示されます。

Inline Cloud Analysis Tab

Inline Cloud Analysis を使用すると、コマンドインジェクションと SQL インジェクション の脆弱性を、検出エンジンごとにリアルタイム分析するための設定を有効にして構成できま す。

Enable cloud inline analysis - 使用可能なすべてのインライン クラウド分析エンジンでコマン ドインジェクションと SQL インジェクションの脆弱性を検出するために使用されるインライ ンディープ ラーニング検出エンジンを有効にします。

利用可能な分析エンジ ン	脆弱性カテゴリを表す使用可能な分析エンジンごとに、対応する脆 弱性が検出されたときにファイアウォールが適用する次のいずれか のアクションを選択できます。
	• Allow - 要求は許可され、ログエントリは生成されません。
	• Alert - 要求が許可され、Threat ログエントリが生成されます。
	• Reset-Client - クライアント側の接続をリセットします。
	• Reset-Server - サーバー側の接続をリセットします。
	 Reset-Both – クライアント側とサーバー側の両方で接続をリ セットします。

脆弱性防御プロファイ ル設定	の意味	
	すべての分析エンジンのデフォルトのアクションはア ラートです。	
インライン クラウド分 析から除外する	インライン クラウド分析エンジンをバイパスする URL または IP ア ドレス例外リストを選択できます。例外は、URLやIPアドレスを使 用して指定できます。URL 例外には EDL (外部動的リスト) または カスタム URL カテゴリが含まれ、IP アドレス例外には EDL また は Address オブジェクトが含まれます。Add (追加) をクリックし て、使用可能なオプションを表示して選択します。次のリストタイ プを選択できます。	
	 EDL URL – 一連の URL またはカスタム URL カテゴリを含む External Dynamic Lists です。 	
	 IP Address – External Dynamic List または Address オブジェクト 内で定義された IP アドレス リスト。 	
	IPアドレスと URL の例外は、誤検知の場合など、 特定された脅威が危険を引き起こさない場合にの み作成してください。	

Objects > Security Profiles > URL Filtering [オブジェクト > セキュリティ プロファイル > URL フィルタリング]

URL フィルタリング プロファイルを使用すれば、Web コンテンツへのアクセスを制御できるだけでなく、ユーザーが Web コンテンツとやり取りする方法を制御することもできます。

確認すべき情報	以下を参照
URL カテゴリに基づいて Web サイトへ のアクセスを制御する。	URL フィルタリング カテゴリ
企業認証情報の送信を検出して、ユー ザーが認証情報を送信できる URL カテ ゴリを判断します。	ユーザー証明書検出 URL フィルタリング カテゴリ
エンドユーザーが最も厳格なセーフ サーチ設定を使用していない場合に検索 結果をブロックします。	URL フィルタリング設定
HTTP ヘッダーのロギングを有効にす る。	URL フィルタリング設定
カスタム HTTP ヘッダを使用する Web サイトへのアクセスを制御する。	HTTP ヘッダの挿入
クラウドとローカルのインライン分類を 有効にして、悪意のあるコンテンツがな いかリアルタイムでWebページを分析し ます。	インライン分類
その他の情報をお探しですか?	 URL フィルタリングを設定する方法を詳しく学びます。
	 URL カテゴリを使用して を使用して、資格情報フィッシングを防止する。
	 カスタム URL カテゴリを作成する手順については、「Objects(オブジェクト) > Custom Objects(カスタム オブジェクト) > URL Category(URL カテゴリ)」を参照してください。 適用する URL のリストをインポートするに
	は、Objects > External Dynamic Lists [オブジェ クト > 外部動的リスト] を選択します。

URL フィルタリングの一般設定

以下の表では、一般的な URL フィルタリング設定について説明します。

一般設定	の意味
氏名	プロファイル名(最大 31 文字)を入力します。この名前は、セ キュリティ ポリシーを定義するときに URL フィルタリング プロ ファイルのリストに表示されます。名前の大文字と小文字は区別 されます。また、一意の名前にする必要があります。文字、数字、 スペース、ハイフン、およびアンダースコアのみを使用してくださ い。
の意味	プロファイルの説明を入力します (最大 255 文字)。
共有	 以下に対してプロファイルを公開する場合は、このオプションを選択します。 multi-vsys ファイアウォールの各仮想システム (vsys)。この選択を解除すると、Objects[オブジェクト] タブで選択した Virtual System[仮想システム]のみに対してプロファイルが公開されます。 Panorama 上の各デバイス グループ。この選択を解除すると、Objects[オブジェクト] タブで選択した Device Group[デバイスグループ]のみに対してプロファイルが公開されます。
オーバーライドの無効 化(Panoramaのみ)	管理者が、このプロファイルを継承するデバイス グループでこの URL フィルタリング プロファイルの設定をオーバーライドするこ とを禁止するには、このオプションを選択します。デフォルトでこ のオプションはオフになっており、管理者は、このプロファイルを 継承するデバイス グループの設定をオーバーライドできます。

URL フィルタリング カテゴリ

Objects(オブジェクト) > **Security Profiles**(セキュリティ プロファイル) > **URL Filtering**(**URL** フィルタリング) > **Categories**(カテゴリ)を選択して、URL に基づく Website へのアクセスを制御します。

カテゴリ設定	の意味
カテゴリ	Web アクセスおよび使用状況ポリシーを定義できる URL カテゴリと リストを表示します。デフォルトでは、Site Access(サイトアクセ ス)権限と User Credential Submission(ユーザー証明書送信)権限 は、すべてのカテゴリで Allow(許可)に設定されます。

カテゴリ設定	の意味
	URL カテゴリおよびリストは 3 つのドロップダウンリストにグルー プ化されています:
	 Custom URL Categories – カスタム URL カテゴリを定義するには Objects > Custom Objects > URL Category [オブジェクト > カスタ ムオブジェクト > URL カテゴリ]を選択します。URL のリストあ るいは複数の事前定義済みカテゴリに基づいてカスタム URL カテ ゴリを決定できます。
	 External Dynamic URL Lists – Objects > External Dynamic Lists [オ ブジェクト > 外部動的リスト]を選択すると、firewall は Web サー バーから URL のリストをインポートできます。
	 Pre-defined Categories (事前定義済みカテゴリ)—PAN-DB、Palo Alto Networks URL、IP クラウド データベースが定義した URL カ テゴリをすべて列挙します。
	 ・ ・ ・
	ブロックポリシーを段階的に導入する場合は、カテ ゴリをcontinue (続行)に設定してカスタム応答ページ を作成するようにし、ユーザーに利用規約を周知さ せ、脅威をもたらす可能性があるサイトに訪問して いるということを知らせるようにします。適切な期 間の後、悪意のある可能性があるこれらのサイトを ブロックするポリシーに移行します。
サイト アクセス	 URL カテゴリごとに、ユーザーがそのカテゴリの URL にアクセスしようとしたときに実行する操作を選択します。 alert[アラート] – Webサイトへのアクセスを許可しますが、ユーザーがそのURLにアクセスするたびにURLログにアラートが追加されます。
	 ブロックしないトラフィックのカテゴリに対する Action (アクション) としてalert (アラート)を設定し、 アクセスの試みをログに記録し、トラフィックに対する可視性を得られるようにします。

カテゴリ設定	の意味
	• allow[許可] – Webサイトへのアクセスが許可されます。
	 allow (許可)はブロックされないトラフィックをロ グに記録しないため、アクセスの試みをログに記録 し、トラフィックに対する可視性を得たい場合は、 トラフィックのカテゴリに対する Action (アクショ ン)としてalert (アラート)を設定してください。
	 block (ブロック)- Web サイトへのアクセスがブロックされます。URL カテゴリへの Site Access (サイト アクセス) をブロックに設定すると、User Credential Submission (ユーザー証明書送信) 権限も自動的にブロックに設定されます。
	 continue (続行)-ユーザーに警告ページを表示し、Web サイトに アクセスしないよう促します。その後、ユーザーが警告を無視す ることにした場合は Web サイトへのアクセスをContinue (続行)す る選択を行う必要があります。
	プロキシ サーバーを使用するように設定されているク ライアント マシンでは、続行(警告)ページは正しく 表示されません。
	 override (オーバーライド) – 応答ページを表示して、有効な パスワードを入力してサイトにアクセスするようにユーザーに要 求します。パスワードやその他のオーバーライド設定を行う場合 は、Device (デバイス) > Setup (設定) > Content ID (コンテ ンツ ID)を開き、URL 管理者オーバーライド設定を編集します (「Device (デバイス) > Setup (設定) > Content-ID (コンテン ツ ID)」の管理設定の表も参照してください)。
	プロキシ サーバーを使用するように設定されているク ライアント マシンでは、オーバーライド ページは正し く表示されません。
	 none (なし) (カスタムURLカテゴリのみ) – カスタムURLカテゴリを作成してあり、ファイアウォールにURLデータベースベンダーからURLフィルタリングカテゴリを継承させる場合はアクションをnone (なし) に設定します。アクションをnone (なし) に設定することで、URLフィルタリングプロファイルに含まれるカスタムカテゴリを無視するような柔軟な設定が可能になり、ポリシールール(セキュリティ、復号化、およびQoS)の一致条件としてカスタムURLカテゴリを使用し、例外を設定したり、異なるアクションを実行させることができます。カスタムURLカテゴリを削除する場合は、そのカスタムカテゴリが使用されているすべてのプロファイルでアクションをnone[なし] に設定する必要があります。カスタム URL カテゴリの詳細は、「Objects(オ

カテゴリ設定	の意味
	ブジェクト)> Custom Objects(カスタム オブジェクト)> URL Category(URL カテゴリ)」を参照してください。
ユーザー証明書送信	URL カテゴリごとに User Credential Submissions (ユーザー証明書 送信)を選択し、ユーザーが有効な企業認証情報をそのカテゴリの URL に送信することを許可または禁止します。URL カテゴリに基づ いてユーザー認証情報の送信を制御する前に、認証情報送信検出を有 効にする必要があります(User Credential Detection(ユーザー証明 書送信)タブを選択)。
	Site Access(サイト アクセス)をブロックに設定した URL カテゴリ では、ユーザー認証情報送信も自動的にブロックするように設定され ます。
	 alert (アラート) – 認証情報を Web サイトに送信することを ユーザーに許可しますが、ユーザーがこのカテゴリのサイトに認 証情報を送信するたびに、URL フィルタリング ログを生成しま す。
	 allow (許可) (デフォルト) – ユーザーが認証情報を Web サイトに送信することを許可します。
	 block (ブロック) – ユーザーが認証情報を Web サイトに送信することをブロックします。デフォルトのアンチフィッシング応答ページでは、ユーザー認証情報送信がブロックされます。
	 continue (続行) – 応答ページを表示し、ユーザーが Continue (続行)を選択して認証情報をサイトに送信することを要求します。 デフォルトでは、アンチフィッシング続行ページを表示し、認証 情報の送信が勧められないサイトにユーザーが認証情報を送信し ようとしたとき、ユーザーに警告します。カスタム応答ページを 作成してフィッシングの企てについてユーザーに警告するか、そ の他の Web サイトで有効な企業認証情報を再利用しないように ユーザーを教育するかを選択できます。
URL カテゴリを チェック	クリックして PAN-DB URL フィルタリング データベースにアクセス します。そこでは、URL または IP アドレスを入力してカテゴリ情報 を表示できます。
動的 URL フィルタリ ング(デフォルトで 無効)	URL を分類するためのクラウド検索を有効にする場合に選択しま す。URL の分類にローカル データベースを使用できない場合、この オプションが呼び出されます。
(BrightCloud のみに 設定可能)	5秒のタイムアウト中に URL を解決できない場合、応答は「Not resolved URL」として表示されます。

カテゴリ設定	の意味	
		PAN-DBを使用する場合、このオプションはデフォルト で有効にされており、設定できません。

URL フィルタリング設定

Objects(オブジェクト) > **Security Profiles**(セキュリティ プロファイル) > **URL Filtering**(**URL** フィルタリング) > **URL Filtering Settings**(**URL** フィルタリング設定)を選択す ると、安全な検索設定が適用され、HTTP ヘッダのログが有効になります。

URL フィルタリング 設定	内容
コンテナ ページのみ ログを記録 デフォルト:enabled [有効化]	 指定したコンテンツタイプに一致するURLのみを記録する場合は、このオプションを選択します。セッション中にファイアウォールはアドバタイズメントやコンテンツリンクなどのログ関連のWebリンクをログに記録しないため、関連するURLをログに記録しつつ、ロギングおよびメモリの読み込みが削減されます。 送信元の元のIPアドレスをマスクするプロキシを使用する場合、HTTP Header Logging (HTTP ヘッダのロギング) X-Forwarded-Forオプションを有効化し、Webページのリクエストを開始したユーザーの元のIPアドレスを保持します。
セーフ サーチ適用の 有効化	厳密なセーフサーチフィルタリングを適用する場合は、このオプショ ンを選択します。
デフォルト:disabled この機能を使用する 場合、URL フィルタ リング ライセンスは 不要です。	多くの検索エンジンには、検索クエリ リターン トラフィックでア ダルト画像やアダルト動画を除外するセーフ サーチ設定が備わって います。セーフ サーチの適用を有効にする設定を選択すると、ユー ザーが最も厳密なセーフ サーチ設定を検索クエリで使用していな い場合、ファイアウォールでは検索結果がブロックされます。ファ イアウォールでは次の各プロバイダーのセーフ サーチを使用できま す。Google、Yahoo、Bing、Yandex、YouTube。これは、ベスト エ フォート設定であり、すべての Web サイトで機能することを検索プ ロバイダが保証しているわけではありません。
	セーフ サーチを使用するには、この設定を有効にしてから、URL フィルタリング プロファイルをセキュリティ ポリシー ルールに添付 する必要があります。これにより、ファイアウォールは、一致する検 索クエリ リターン トラフィックのうち、最も厳密なセーフ サーチ設 定を使用していないトラフィックをブロックします。

URL フィルタリング 設定	内容	
	Yahooアカウントにログイン中にYahoo Japan (yahoo.co.jp)で検索を実行する場合は、検索設定のロッ クオプションも有効にする必要があります。	
	ユーザーが他の検索プロバイダを使用して この機能を迂回しないようにするには、URL フィルタリングプロファイルで search-engines カテゴリをブロックするように設定してか ら、Bing、Google、Yahoo、Yandex、YouTube へのアク セスを許可します。	
HTTP ヘッダのロギ ング	HTTP ヘッダーのロギングを有効にすると、サーバーに送信された HTTP 要求に含まれる属性を表示できます。有効な場合、以下の属 性-値ペアの1つ以上が URL フィルタリング ログに記録されます。	
	 ユーザーエージェント – ユーザーが URL へのアクセスに使用する Web ブラウザ。この情報は、HTTP 要求でサーバーに送信されます。たとえば、ユーザーエージェントは Internet Explorer または Firefox である可能性があります。ログ内のユーザーエージェント値は最大 1024 文字をサポートします。 	
	 参照 – ユーザーを別の Web ページにリンクした Web ページの URL。要求された Web ページにユーザーをリダイレクト (参照) した送信元です。ログ内の参照値は最大 256 文字をサポートしま す。 	
	 x-forwarded-for – Web ページを要求したユーザーの IP アドレス を保持するヘッダー フィールド オプション。特にネットワーク上 にプロキシ サーバーがある場合や、送信元 NAT を実装している場 合は、すべての要求がプロキシ サーバーの IP アドレスまたは共通 の IP アドレスから送信されているかのようにユーザーの IP アドレ スがマスクされてしまうため、これによりユーザーの IP アドレス を識別できて役立ちます。ログ内の x-forwarded-for 値は最大 128 文字をサポートします。 	

ユーザー証明書検出

Objects(オブジェクト) > **Security Profiles**(セキュリティ プロファイル) > **URL Filtering**(**URL** フィルタリング) > **User Credential Detection**(ユーザー認証情報検知)を選択 すると、ユーザーが認証情報書を送信した際にファイアウォールが検出できるようになります。 ユーザー認証情報検知を設定して URL カテゴリで指定されたサイトにのみユーザー が認証情報を送信できるようにし、信頼されていないカテゴリのサイトに認証情報 を送信するのを防ぐことで、攻撃の入り口を減らします。ユーザー認証情報の送信 のために URL フィルタリング プロファイルですべての URL カテゴリをブロックす る場合は、認証情報をチェックする必要はありません。

ファイアウォールでは、3つの方法のいずれかが使用されて、Webページに送信される、有効 な認証情報が検出されます。それぞれの方法では User-ID[™] が必要であり、これによってファイ アウォールは、Webページに送信されるユーザー名とパスワードを有効な企業認証情報と比較 できるようになります。これらの方法のいずれかを選択して、URL カテゴリに基づいて資格情 報フィッシングを防止する ■を続行します。



ユーザーの認証情報を監視するには、トラフィックを 復号 するようにファイア ウォールを設定する必要があります。

ユーザー証明書検出の 設定	の意味
IP ユーザー	この認証情報検出方法では、有効なユーザー名の送信がチェックされ ます。この方法を使用すると、有効な企業ユーザー名を含む認証情報 の送信を(付随するパスワードに関係なく)検出できます。ファイア ウォールでは、セッションの送信元 IP アドレスにログインしたユー ザーにユーザー名が一致することが確認されて、ユーザー名の一致 が判断されます。この方法を使用する場合、ファイアウォールは、 送信されるユーザー名を IP アドレスとユーザー名のマッピングテー ブルと照合します。この方法を使用するには、「Map IP Addresses to Users (IP アドレスとユーザーのマッピング)」で説明されている ユーザーマッピング方法のいずれかを使用できます。
グループ マッピング	ファイアウォールは、制限されているサイトにユーザーが送信する ユーザー名が有効な企業ユーザー名と一致するかどうかを判断しま す。これを行うため、ファイアウォールは、送信されるユーザー名を ユーザーとグループのマッピングテーブルのユーザー名のリストと 照合し、ユーザーが制限されているカテゴリのサイトに企業ユーザー 名を送信することを検出します。
	この方法では、LDAP グループ メンバーシップに基づい て企業ユーザー名の送信のみがチェックされるため、設定 は簡単ですが、誤検出が多くなる傾向があります。この 方法を使用するには、グループマッピングを有効にする 必要があります。
Domain Credential(ドメイン 証明書)	この認証情報検出方法では、ファイアウォールによって、有効な企業 ユーザー名と関連パスワードをチェックできます。ファイアウォール は、ユーザーが送信するユーザー名とパスワードが、同じユーザーの 企業ユーザー名とパスワードと一致するかどうかを判断します。

ユーザー証明書検出の 設定	の意味
	これを行うため、ファイアウォールは、送信される認証情報を有効な 企業ユーザー名とパスワードと照合し、送信されるユーザー名が、 ログインユーザーの IP アドレスに対応することを確認できる必要が あります。このモードは Windows ベースの User-ID エージェント のみでサポートされ、User-ID エージェントが読み取り専用ドメイ ンコントローラ (RODC) にインストールされていて、User-ID 認証 情報サービス アドオンが装備されている必要があります。この方法 を使用するには、認証ポリシー、認証ポータル、GlobalProtect.™な ど、サポートされているユーザー マッピング方式のいずれかを使用 して、ユーザー ID から に IP アドレスをユーザー にマップする必要 があります™
	ファイアウォールが有効な企業認証情報の送信のチェックに使用で きる方法の詳細、およびフィッシング防御を有効にする手順につい ては、「Prevent Credential Phishing(認証情報フィッシングの防 止)」
有効なユーザー名検 出済みログ重大度	ファイアウォールが、有効なユーザー名の Web サイトへの送信を検 出したことを示すログの重大度を設定します。
	このログ重大度は、認証情報送信の権限が、アラート、ブロック、 継続のいずれかになっている Web サイトに、有効なユーザー名が 送信されるイベントに関連付けられます。認証情報の送信が許可 されている Web サイトに、ユーザーが有効なユーザー名を送信す ることを記録するログの重大度は通知になります。認証情報の送信 の許可やブロックを行う URL カテゴリの確認または調整を行うに は、Categories(カテゴリ)を選択してください。
	◎ ログの重大度を medium (中) 以上に設定してください。

HTTP ヘッダの挿入

ファイアウォールが HTTP ヘッダとその値を HTTP 要求に挿入して Web アプリケーションへ のアクセスを管理できるようにするには、Objects (オブジェクト) > Security Profiles (セキュリ ティ プロファイル) > URL Filtering (URL フィルタリング) > HTTP Header Insertion (HTTP ヘッ ダ挿入)を選択します。

ファイアウォールは、HTTP/1.x トラフィックのヘッダ挿入のみをサポートします。 ファイアウォールは、HTTP/2 トラフィックのヘッダ挿入をサポートしていませ ん。 定義済みの HTTP ヘッダ挿入タイプに基づいて挿入エントリを作成することも、独自のカスタム タイプを作成することもできます。ヘッダ挿入は通常、カスタム HTTP ヘッダに対して実行され ますが、標準 HTTP ヘッダを挿入することもできます。

ヘッダ挿入は、次の場合に発生します。

- 1. HTTP 要求が、1つまたは複数の HTTP ヘッダ挿入エントリが設定されたSecurity (セキュリ ティ) ポリシー ルールと一致する。
- 2. 指定されたドメインが、HTTP ホスト ヘッダにあるドメインと一致する。
- 3. アクションはブロック以外です。

ファイアウォールは、GET、POST、PUT、および HEAD メソッドに対してのみ HTTP ヘッダ挿入を実行できます。

HTTP ヘッダの挿入を有効にし、識別されたヘッダーが要求にない場合、ファイアウォールは ヘッダを挿入します。識別されたヘッダが要求にすでに存在する場合、ファイアウォールはヘッ ダ値を指定した値で上書きします。

挿入エントリを Add (追加) 追加するか、既存の挿入エントリを選択して変更します。必要に 応じて、挿入項目を選択してから Delete (削除) することもできます。

新しい HTTP ヘッダ挿入エントリのデフォルトのブロック リスト アクションは block (ブロック)です。別のアクションが必要な場合は、URL フィルタリング カ テゴリ に移動して適切なアクションを選択します。または、目的のアクションで構 成されたプロファイルに挿入エントリを追加します。

HTTP ヘッダの挿入設 定	の意味
氏名	HTTP ヘッダ挿入エントリの Name (名前)。
タイプ	作成するエントリの Type (タイプ) 。エントリは、事前定義済みまた はカスタムのいずれかです。ファイアウォールはコンテンツ更新を使 用して、事前定義済みエントリを入力・管理します。
	HTTP ヘッダにユーザー名を含める場合は Dynamic Fields(動的 フィールド)を選択します。
ドメイン	ヘッダ挿入は、このリスト内のドメインが HTTP 要求の Host ヘッダ と一致すると発生します。
	定義済みのエントリを作成する場合、ドメイン リストはコンテンツ 更新であり事前定義されています。ほとんどの使用例ではこれで十分 ですが、必要に応じてドメインを追加または削除できます。
	カスタムエントリを作成するには、少なくとも1つのドメインをこの リストに Add(追加)します。
	各ドメイン名は最大 256 文字まで入力することができ、エントリ ごとに最大 50 のドメインを識別できます。アスタリスク (*) をワイ

HTTP ヘッダの挿入設 定	の意味
	ルドカード文字として使用できます。これは、指定されたドメイン (* .etrade.com など) へのすべての要求に一致します。
ヘッダー	定義済みのエントリを作成する場合、ヘッダ リストはコンテンツ更 新により事前作成されます。ほとんどの使用例ではこれで十分です が、必要に応じてヘッダを追加または削除できます。
	カスタム エントリを作成するときは、このリストに1つ以上のヘッ ダ (合計5つまで) を追加します。
	ヘッダ名には 100 文字まで使用できますが、スペースは使用できま せん。
	ユーザー名を HTTP ヘッダに含める場合は X-Authenticated-User を 選択してから Value (値)を選択するか、新しいヘッダを Add (追加) し ます。
値	最大16K文字を使用して値を設定します。ヘッダ値は、指定したド メインの HTTP ヘッダに含める情報によって異なります。例えば、 SaaS アプリケーションへのユーザー アクセスを管理 するには 事前定 義済みタイプ を選択するか カスタム エントリを使用します。
	HTTP ヘッダにユーザ名を含めるには、セキュリティ デバイスに要求 されるドメインとユーザー名の形式を選択します。
	• (\$domain)\(\$user)
	• WinNT://(\$domain)/(\$user)
	または、 (\$user) および (\$domain) ダイナミック トークンを使用 してカスタム形式を入力します((\$user)@(\$domain)など)。
	ファイアウォールは、グループ マッピング プロファイルのプライマ リ ユーザー名を使用して、ユーザーとドメインのダイナミック トー クンを入力します。
	各 (\$user) および (\$domain) ダイナミックトークン は、値ごとに1回だけ使用します。
ログ	このヘッダ挿入エントリのロギングを有効にするには、Log(ロ グ)を選択します。

インライン分類

Objects > Security Profiles > URL Filtering > Inline Categorization を選択し、リアルタイムの Web ページ分析を有効にして構成します。

項目の意味

Inline Categorization タブを使用して、リアルタイムの Web ページ分析を有効にし、URL 例外を管理します。

リアルタイム URL 分析は、firewall ベースの検出メカニズムとしてローカルで利用でき、クラウドでは Advanced URL Filtering サービスの一部として利用できます。

- ローカルのインライン分類を有効にする firewall ベースの機械学習モデルを使用して URL トラフィックをリアルタイムで分析し、悪意のあるフィッシングの亜種や JavaScript エク スプロイトがネットワークに侵入するのを検出して防止します。
- クラウドのインライン分類を有効にする-ローカルのインライン ML で使用される分析エンジンを補完する機械学習ベースの検出器を使用して、疑わしい Web ページ コンテンツをクラウドに転送して補足分析を行うことで、URL のリアルタイム分析を可能にします。

例外	インライン分類を使用して分析したくない特定の Web サイトに対し て 例外URL を定義できます。
	URL 例外を追加するには、まず有効な EDL(外部ダイナミック リスト)またはカスタム URL カテゴリを定義する必要がありま す。Add(追加)をクリックして、使用可能なオプションを表示して 選択します。

Objects > Security Profiles > File Blocking [オブジェクト > セキュリティ プロファイル > ファイル ブロッキング]

ファイル ブロッキング プロファイルをセキュリティ ポリシー ルールに割り当てて (Policies(ポリシー) > Security(セキュリティ))、ユーザーが指定のファイル タイプを アップロードまたはダウンロードすることを禁止したり、指定のファイル タイプをアップロー ドまたはダウンロードしようとしたときにアラートを生成したりできます。

事前定義済みのstrict (厳格)なプロファイルを適用することで、セキュリティを最大 化できます。strict (厳格)なプロファイルがブロックするファイル形式を使用する 重要なアプリケーションをサポートしなければならない場合は、strict (厳格)なプロ ファイルをコピーして必要なファイル形式の例外だけを適用します。対象のファ イル形式を必要とする送信元、宛先、ユーザーだけに例外を許すセキュリティポリ シールールに、コピーしたプロファイルを適用します。また、Direction (方向)を使 用して例外をアップロードあるいはダウンロードに制限することもできます。

Windows PE ファイルを一部ブロックしない場合は、未知のファイルをすべて WildFire に送信して分析を行ってください。ユーザーアカウントについては Action (アクション)をcontinue (続行)に設定し、悪意のある Web サイト、メール、ポップ アップがユーザーに意図せず悪意のあるファイルをダウンロードさせるドライブ バイダウンロード攻撃を防ぎます。自分が開始していないファイル転送を求める Continue (続行) プロンプトが表示された場合、危険なダウンロードを行おうとして いる可能性があるということをユーザーに周知させてください。

以下の表では、ファイル ブロッキング プロファイル設定について説明します。

ファイル ブロッキング プロファイル設定	の意味
氏名	プロファイル名(最大 31 文字)を入力します。この名前は、セ キュリティ ポリシーを定義するときにファイル ブロッキング プロ ファイルのリストに表示されます。名前の大文字と小文字は区別 されます。また、一意の名前にする必要があります。文字、数字、 スペース、ハイフン、およびアンダースコアのみを使用してくださ い。
の意味	プロファイルの説明を入力します (最大 255 文字)。
共有(Panorama の み)	以下に対してプロファイルを公開する場合は、このオプションを選 択します。
	 multi-vsys ファイアウォールの各仮想システム (vsys)。この選択 を解除すると、Objects[オブジェクト] タブで選択した Virtual
ファイル ブロッキング プロファイル設定	の意味
--	--
	 System[仮想システム] のみに対してプロファイルが公開されます。 Panorama 上の各デバイス グループ。この選択を解除すると、Objects[オブジェクト] タブで選択した Device Group[デバイスグループ] のみに対してプロファイルが公開されます。
オーバーライドの無効 化(<mark>Panoramaのみ</mark>)	管理者が、プロファイルを継承するデバイス グループのこのファイ ル ブロッキング プロファイルの設定をオーバーライドすることを 禁止する場合はこのオプションを選択してください。デフォルトで このオプションはオフになっており、管理者は、このプロファイル を継承するデバイス グループの設定をオーバーライドできます。
ルール	1つ以上のルールを定義して、選択したファイル タイプで実行する アクション (存在する場合) を指定します。ルールを追加するには、 以下を指定して Add[追加] をクリックします。
	 Name(名前) – ルール名(最大 31 文字)を入力します。 Applications[アプリケーション] – ルールを適用するアプリケーションを選択するか、any[すべて]を選択します。
	 File Types[ファイルタイプ] – ファイルタイプのフィールドをク リックし、Add[追加] をクリックするとサポートされているファ イルタイプの一覧が表示されます。プロファイルに追加したい ファイルタイプをクリックし、必要に応じファイルタイプを追 加します。Any[すべて] を選択した場合、設定したアクションが すべてのファイルタイプに対して実行されます。
	 Direction[方向] – ファイル転送の方向 (Upload、Download、または Both) を選択します。
	 Action[アクション] – 選択したファイル タイプの検出時に実行 するアクションを選択します。
	● alert[アラート] – エントリが脅威ログに追加されます。
	 continue[継続] – ダウンロードがリクエストされたことを通知して、続行するかどうかを確認するようにユーザーに求めるメッセージが表示されます。この目的は、認識されないダウンロード(ドライブバイダウンロードとも呼ばれる)の可能性があることをユーザーに警告し、そのダウンロードの続行または停止をユーザーが選択できるようにすることです。
	continue(続行)アクションを使用してファイル ブロッキン グ プロファイルを作成する場合、選択できるアプリケーショ ンは web-browsing のみです。その他のアプリケーションを 選択すると、ユーザーには続行ページのプロンプトが表示さ

ファイル ブロッキング プロファイル設定	の意味
	れないため、セキュリティ ポリシー ルールに一致するトラ フィックはファイアウォールを通過しません。
	 block[ブロック] – ファイルがブロックされます。

Objects > Security Profiles > WildFire Analysis [オブジェ クト > セキュリティ プロファイル > WildFire 分析]

WildFire 分析プロファイルでは、WildFire アプライアンスまたは WildFire クラウドでローカル に実行される WildFire ファイル分析を指定します。ファイル タイプ、アプリケーション、ま たはファイルの送信方向 (アップロードまたはダウンロード) に応じて、パブリック クラウドま たはプライベート クラウドにトラフィックを転送するよう指定できます。作成した WildFire分 析プロファイルをポリシーに追加することによって (Policies > Security [ポリシー > セキュリ ティ]) 、そのプロファイルの設定をそのポリシーに一致する任意のトラフィック(たとえば、 そのポリシーに定義されているURLカテゴリ)に適用できるようになります。

事前定義済みのデフォルトプロファイルを使用し、未知のファイルをすべて WildFire に転送して分析を行います。さらに、WildFire アプライアンスのコンテン ツ更新を毎分ダウンロードおよびインストールするよう設定し、常に最新のサポー トを得られるようにします。

WildFire 分析プロファイルの設定		
氏名	WildFire 分析プロファイルの分かりやすい名前 (最大 31 文字) を入 力します。この名前は、セキュリティ ポリシー ルールを定義する 際に選択候補となる WildFire 分析プロファイルのリストに表示さ れます。名前の大文字と小文字は区別されます。また、一意の名前 にする必要があります。文字、数字、スペース、ハイフン、および アンダースコアのみを使用してください。	
の意味	(任意) プロファイル ルールまたはプロファイルの用途の説明です (255 文字まで)。	
共有(Panorama の み)	 以下に対してプロファイルを公開する場合は、このオプションを選択します。 multi-vsys ファイアウォールの各仮想システム (vsys)。この選択を解除すると、Objects[オブジェクト] タブで選択した Virtual System[仮想システム]のみに対してプロファイルが公開されます。 Panorama 上の各デバイス グループ。この選択を解除すると、Objects[オブジェクト] タブで選択した Device Group[デバイスグループ]のみに対してプロファイルが公開されます。 	
オーバーライドの無効 化(Panoramaのみ)	管理者が、プロファイルを継承するデバイス グループのこの脆弱性 防御プロファイルの設定をオーバーライドすることを禁止する場合 はこのオプションを選択してください。デフォルトでこのオプショ ンはオフになっており、管理者は、このプロファイルを継承するデ バイス グループの設定をオーバーライドできます。	

WildFire 分析プ	ロファイルの設定
ルール	
ルール	WildFire パブリック クラウドまたは WildFire アプライアンス (プラ イベート クラウド) にトラフィックを転送して分析するように指定 する 1 つ以上のルールを定義します。
	 プロファイルに追加する任意のルールの分かりやすい Name[名前] (最大 31 文字) を入力します。
	 Application[アプリケーション] を追加して、任意のアプリケー ショントラフィックがルールと照合され、指定した分析用の宛 先に転送されるようにします。
	 そのルール用の定義済みの分析用の宛先で分析する File Type[ファイルタイプ] を選択します。
	WildFire プライベート クラウド(WildFire アプライア ンスによってホストされる)は、APK、Mac OS X、 アーカイブ、および Linux ファイルの分析をサポート していません。
	 送信の Direction[方向] に応じてトラフィックにルールを適用します。アップロード トラフィック、ダウンロード トラフィック、またはその両方にルールを適用できます。
	• Analysis(分析)で転送するトラフィックの宛先を選択します。
	ハイブリッド クラウド展開では、プライベート クラウドとパブリック クラウドの両方のルールに一致するファイルは、注意措置としてプライベートクラウドにのみ転送されます。
	 ルールと照合されるすべてのトラフィックを WildFire パブ リック クラウドに転送して分析する場合は、public-cloud を 選択します。
	 ルールと照合されるすべてのトラフィックを WildFire アプラ イアンスに転送して分析する場合は、private-cloud を選択し ます。

インライン クラウド解析

インライン クラウド解	このオプションを選択すると、Advanced WildFire インラインクラ
析を有効にする	ウド分析が有効になります。
ルール	Advanced WildFireインラインクラウド分析に転送するトラフィックを指定するルールを1つ以上定義します。

WildFire 分析プロファイルの設定	
	 プロファイルに追加する任意のルールの分かりやすい Name[名前] (最大 31 文字)を入力します。
	 Application[アプリケーション]を追加して、任意のアプリケーショントラフィックがルールと照合され、指定した分析用の宛先に転送されるようにします。
	 そのルール用の定義済みの分析用の宛先で分析する File Type[ファイルタイプ] を選択します。
	 送信の Direction[方向] に応じてトラフィックにルールを適用します。ルールはダウンロードトラフィックに適用できます。
	 一部のオンラインサービスから複数のファイルを 同時にダウンロードすると、ファイルは現在PAN- OSでサポートされていない形式でアーカイブされ ます。これらのファイルはアーカイブ解除されず に分析されます。
	 Advanced WildFire インラインクラウド分析がマルウェアを検出 したときに実行するアクションを指定します。

Objects > Security Profiles > Data Filtering [オブジェクト > セキュリティ プロファイル > データ フィルタリング]

データフィルタリングを使用すると、ファイアウォールはクレジットカード番号、社会保障番号、社内ドキュメントなどの機密情報を検出し、このようなデータが安全なネットワークから漏出するのを防ぐことができます。データフィルタリングを有効にする前に、Objects(オブジェクト) > Custom Objects(カスタムオブジェクト) > Data Patterns(データパターン)を選択し、フィルタリングするデータのタイプ(社会保障番号や社外秘と記載されたドキュメントのタイトルなど)を定義します。複数のデータパターンオブジェクトを1つのデータフィルタリングプロファイルに追加できます。セキュリティポリシールールに割り当てると、ファイアウォールは各データパターンの許可されたトラフィックをスキャンし、データフィルタリング

データ フィルタリング プロファイル設定	の意味
氏名	プロファイル名(最大 31 文字)を入力します。この名前は、セ キュリティ ポリシーを定義するときにログ転送プロファイルのリス トに表示されます。名前の大文字と小文字は区別されます。また、 一意の名前にする必要があります。文字、数字、スペース、ハイフ ン、およびアンダースコアのみを使用してください。
の意味	プロファイルの説明を入力します (最大 255 文字)。
共有(Panorama の み)	 以下に対してプロファイルを公開する場合は、このオプションを選択します。 multi-vsys ファイアウォールの各仮想システム (vsys)。この選択を解除すると、Objects[オブジェクト] タブで選択した Virtual System[仮想システム]のみに対してプロファイルが公開されます。 Panorama 上の各デバイス グループ。この選択を解除すると、Objects[オブジェクト] タブで選択した Device Group[デバイスグループ]のみに対してプロファイルが公開されます。
オーバーライドの無効 化(Panoramaのみ)	管理者が、プロファイルを継承するデバイス グループのこのデータ フィルタリング プロファイルの設定をオーバーライドすることを禁 止する場合はこのオプションを選択してください。デフォルトでこ のオプションはオフになっており、管理者は、このプロファイルを 継承するデバイス グループの設定をオーバーライドできます。
データ キャプチャ	フィルタによってブロックされたデータを自動的に収集するア場合 は、このオプションを選択します。

データ フィルタリング プロファイル設定	の意味
	 Settings (設定) ページの Manage Data Protection (デー タ保護の管理) にキャプチャしたデータを表示するた めのパスワードを指定します。「Device (デバイス) > Setup (セットアップ) > Management (管理)」 を参照してください。
データ パターン	フィルタリングで使用する既存のデータ パターンを追加する か、New(新規)を選択して新しいデータ パターン オブジェクト を設定します(Objects(オブジェクト) > Custom Objects(カス タム オブジェクト) > Data Patterns(データ パターン))。
アプリケーション [applications]	 フィルタリングルールに含めるアプリケーションを指定します。 表示されているすべてのアプリケーションにフィルタを適用するには、any[すべて]を選択します。これを選択してもすべてのアプリケーションがブロックされるわけではなく、表示されているアプリケーションのみがブロックされます。 Add[追加]をクリックして個々のアプリケーションを指定します。
ファイル タイプ	 フィルタリング ルールに含めるファイル タイプを指定します。 表示されているすべてのファイル タイプにフィルタを適用する には、any[すべて] を選択します。これを選択してもすべての ファイル タイプがブロックされるわけではなく、表示されてい るファイル タイプのみがブロックされます。 Add[追加] をクリックして個々のファイル タイプを指定します。
指示	フィルタを適用する方向 (アップロード、ダウンロード、または両 方) を指定します。
アラートしきい値	アラートをトリガーするまでのファイルのデータ パターン検出回数 を指定します。
ブロックしきい値	データ パターンがこの回数以上出現するファイルをブロックしま す。
ログ重大度	このデータ フィルタリング プロファイル ルールに一致するイベン トで記録されるログ重大度を定義します。

Objects > Security Profiles > DoS Protection [オブジェ クト > セキュリティ プロファイル > DoS プロテクショ ン]

DoS プロテクション プロファイルは、高精度のターゲット指定ができるように設計され、ゾー ンプロテクション プロファイルを補強します。DoS プロテクション プロファイルでは、(DoS プロテクション ポリシーで指定した)アラームやアクションをトリガーする 1 秒あたりの新 規接続数(CPS)のしきい値レートを指定します。DoS プロテクション プロファイルでは、 最大 CPS レートやブロックされた IP アドレスをブロック IP リストに保持する時間も指定しま す。DoS 保護ポリシールール内で DoS 保護プロファイルを指定し、そこでさらにルールにマッ チさせるパケットの条件を指定します。ポリシールールはプロファイルを適用するデバイスを決 定します。



DoS 保護プロファイル、および重要な個々のデバイスあるいは小規模のデバイス グループ、特に WEB サーバーやデータベースサーバーなどのインターネットに接続 されたデバイスを保護するポリシーを作成します。

DoS プロテクション プロファイルを設定できます。集約プロファイル、分類化プロファイル、 あるいは各タイプのうち一つを DoS 保護ポリシールールに適用できます。両方のプロファイル タイプを単一のルールに適用すると、ファイアウォールは初めに集約プロファイルを適用してか ら、必要な場合に分類化プロファイルを適用します。

- 分類化 DoS 保護プロファイルでは、Classified (分類化)がType (タイプ)として選択されています。分類化 DoS 保護プロファイルをアクションがProtect (保護)の DoS 保護ルールに適用する際、ファイアウォールは、パケットが指定のアドレス タイプ (source-ip-only (宛先 IP のみ)、destination-ip-only (宛先 IP のみ)、src-dest-ip-both (送信元 IP と宛先 IP の両方))に一致した場合にプロファイルの CPS のしきい値に対して接続をカウントします。
- 集約 DoS 保護プロファイルでは、Aggregate (集約)がType (タイプ)として選択されています。アクションがProtect (保護)である DoS 保護ルールを集約 DoS 保護プロファイルに適用する際、ファイアウォールはルールの条件を満たすすべての接続(ルールで指定されたデバイス グループの合計接続数)をプロファイルの CPS しきい値に対して加味します。

DoS プロテクション プロファイルを DoS プロテクション ポリシーに適用する方法については、 「Policies(ポリシー) > DoS Protection(DoS プロテクション)」を参照してください。 マルチ仮想システム(マルチ vsys)がある環境で、以下を設定している場合は、

- 仮想システム間の通信が可能な外部ゾーン
- 仮想システムが外部通信に共通インターフェイスおよび1 つの *IP* アドレスを共 有できる共有ゲートウェイ

以下のゾーンおよび DoS プロテクション メカニズムが、外部ゾーンで無効になり ます。

- SYN cookies
- IPフラグメント
- ICMPv6

IP フラグメントと **ICMPv6** 防御を有効にするには、共有ゲートウェイ用のゾーンプ ロテクションプロファイルを作成します。

共有ゲートウェイで SYN フラッドから保護するには、ランダム早期ドロップまたは SYN Cookie のいずれかを設定した SYN フラッド防御プロファイルを適用できます。 外部ゾーンでは、SYN フラッド防御にランダム早期ドロップのみを使用できます。

DOS プロテクション プロファイルの設定

氏名	プロファイル名(最大 31 文字)を入力します。この名前は、セ キュリティ ポリシーを定義するときにログ転送プロファイルのリス トに表示されます。名前の大文字と小文字は区別されます。また、 一意の名前にする必要があります。文字、数字、スペース、ハイフ ン、およびアンダースコアのみを使用してください。
の意味	プロファイルの説明を入力します (最大 255 文字)。
共有(Panorama の み)	以下に対してプロファイルを公開する場合は、このオプションを選 択します。
	 multi-vsys ファイアウォールの各仮想システム (vsys)。この選択 を解除すると、Objects[オブジェクト] タブで選択した Virtual System[仮想システム] のみに対してプロファイルが公開されま す。
	 Panorama 上の各デバイス グループ。この選択を解除する と、Objects[オブジェクト] タブで選択した Device Group[デバ イスグループ] のみに対してプロファイルが公開されます。

DOS プロテクション プロファイルの設定	
オーバーライドの無効 化(Panoramaのみ)	管理者が、プロファイルを継承するデバイス グループのこの DoS プロテクション プロファイルの設定をオーバーライドすることを禁 止する場合はこのオプションを選択してください。デフォルトでこ のオプションはオフになっており、管理者は、このプロファイルを 継承するデバイス グループの設定をオーバーライドできます。
タイプ	以下のいずれかのプロファイル タイプを選択します。
	 Aggregate (集約) – プロファイルで設定された DoS のしき い値がルール条件 (このルール条件に基づいてプロファイル が適用される) に一致するすべての接続に適用されます。例え ば、SYN フラッドのAlarm Rate (アラーム レート)のしきい値が 10,000 CPS である集約ルールは、DoS ルールにマッチするすべ てのデバイスの合計接続数をカウントします。グループの合計 CPS が 10,000 CPS を超えると、デバイス間でどのように CPS が分散されているかに関わらず、アラームが発生します。
	 Classified (分類) – プロファイルで設定された DoS のしきい 値が、分類条件(送信元 IP アドレス、宛先 IP アドレス、また は送信元 IP アドレスと宛先 IP アドレスのペア)を満たす各接続 に適用されます。例えば、SYN フラッドのAlarm Rate (アラーム レート)のしきい値が 10,000 CPS である分類化ルールはデバイス 毎に最大 10,000 CPS を許容し、DoS ルールで指定された任意の デバイスが 10,000 CPS を超えるとアラームを発生させます。

Flood Protection [フラッド防御] タブ

SYN Flood(SYN フ ラッド)タブ	タブに記載されたタイプのフラッド防御を有効化する場合はこのオ プションを選択し、以下を指定します。
UDP Flood [UDP フ ラッド] タブ	 Action (アクション) – (SYN Flood (SYN フラッド)の み) DoS プロテクション ポリシー アクションが Protect (保
ICMP Flood [ICMP フ ラッド] タブ	護)で、CPS が Activate Rate(アクティベート率)に達した場 合にファイアウォールが実行するアクション。以下のいずれか を選択します。
ICMPv6 Flood (ICMPv6 フラッド) タブ	 Random Early Drop (ランダム早期ドロップ) – 1 秒あたりの接続数が Activate Rate (アクティベート率) しきい値に達
Other IP Flood (その他 の IP フラッド) タブ	すると、ランダムにパケットをドロップします。

DOS プロテクション プロファイルの設定		
	 SYN cookie – SYN フラッド攻撃中に接続をドロップせずに済むように SYN Cookie を使用して受信確認を生成します。 	
	 ・正当なトラフィックを公正に扱い、しかしファイ アウォール リソースを多く消費する SYN Cookie から始めます。CPU とメモリの使用率を監視 し、SYN Cookie がリソースを多く消費しすぎてい る場合は RED に切り替えます。ネットワーク(イ ンターネット)の末端で大量の DoS 攻撃を防止す る専用の DDoS 防止デバイスがない場合は、必ず RED を使用します。 	
	 Alarm Rate (アラーム レート) – DoS アラームを生成するしき い値レート (CPS)を指定します (範囲は 0 ~ 2,000,000 cps、 デフォルトは 10,000 cps)。 	
	分類化プロファイルの場合、しきい値をデバイスの平均 CPS レートよりも 15~20% 高く設定して通常の変動に対応させ、ア ラームが多すぎる場合にしきい値を調整するというのがベスト プラクティスになります。集約プロファイルの場合、しきい値 をグループの平均 CPS レートよりも 15~20% 高く設定すること がベストプラクティスになります。必要に応じてしきい値を監 視して調整します。	
	 Activate Rate(アクティベート率) – DoS 応答が起動されるしきい値レート(cps)を指定します。DoS 応答は、DoS プロテクションプロファイルの Action(アクション)フィールドで設定します(Random Early Drop(ランダム早期ドロップ)またはSYN cookies)。Activate Rate(アクティベート率)の範囲は0~2,000,000 cps で、デフォルトは 10,000 cps です。 	
	プロファイルの Action(アクション)が Random Early Drop(ランダム早期ドロップ)(RED)の場合、1 秒あたりの 受信接続数が Activate Rate(アクティベート率)しきい値に 達すると、RED が発生します。CPS レートを増やすと、アルゴ リズムに従って RED レートが増加します。ファイアウォール は、CPS レートが Max Rate(最大レート)しきい値に達するま で RED を繰り返します。	
	分類化プロファイルは CPS の限界を厳密に個々のデバイスに 適用します。その限界は保護するデバイスの能力に基づいて決 定するため、ユーザーは徐々に CPS をスロットルする必要が無 く、Activate Rate (アクティベート レート)をMax Rate (最大レー ト)と同じしきい値に設定することができます。Max Rate (最大 レート)に達する前に個々のサーバーに向かうトラフィックをド ロップし始めたい場合のみ、Activate Rate (アクティベート レー ト)をMax Rate (最大レート)より低く設定します。集約プロファ	

DOS プロテクション プロファイルの設定	
	イルの場合、しきい値をグループのピーク時 CPS レートよりも ほんの少し大きな値に設定します。必要に応じてしきい値を監 視して調整します。
	 Max Rate(最大レート) – ファイアウォールで許容する1秒 あたりの受信接続数のしきい値を設定します。Max Rate(最大 レート)しきい値に達すると、ファイアウォールは新しい接続 を100%ドロップします(範囲は2~2,000,000 cps、デフォル トは40,000 cps)。
	分類化プロファイルの場合はフラッドが生じないよう、保護し ているデバイスの能力に基づいてMax Rate (最大レート)を決定 します。集約プロファイルの場合、Max Rate (最大レート)をグ ループの能力の 80~90% に設定します。必要に応じてしきい値 を監視して調整します。
	 Block Duration(ブロック期間) – 問題のある IP アドレスをブロック IP アドレスに保持し、この IP アドレスの接続をブロックする秒数を指定します。ブロック期間(範囲は 1 ~ 21,600、デフォルトは 300 秒)に到達したパケットは、Alarm Rate(アラーム レート)、Activate Rate(アクティベート率)、またはMax Rate(最大レート)しきい値に対してカウントされません。

Resources Protection [リソース保護] タブ

セッション	リソース保護を有効化する場合は、このオプションを選択します。
最大同時セッション数	同時セッションの最大数を指定します。
	 Aggregate(集約)プロファイルタイプの場合、DoSプロテクションルール(このルールに基づいて DoSプロテクションプロファイルが適用される)に該当するすべてのトラフィックにこの制限が適用されます。
	 Classified (分類) プロファイル タイプの場合、分類(送信元 IP、宛先 IP、または送信元 IP と宛先 IP の組み合わせ)に基づい て、DoS プロテクション プロファイルが適用される DoS プロテ クション ルールに該当するトラフィックにこの制限が適用され ます。

Objects > Security Profiles > Mobile Network Protection [オブジェクト > セキュリティプロファイル > モバイル ネットワーク プロテクション]

モバイル ネットワーク プロテクションプロファイルにより、ファイアウォールは 5G サービ スベース アーキテクチャ(SBA)トラフィックの GTP および HTTP/2 を検査することがで きます。このプロファイルを表示するには、Device(デバイス) > Setup(セットアップ) > Management(管理)で GTP セキュリティを有効にする必要があります。

このプロファイルのオプションを使用して、5G HTTP/2、GTP v1-C、GTP v2-C、GTP-U、および PFCP のステートフルインスペクションを有効にして、GTPv1-C、GTP v2-C、GTP-U のプロトコル検証を有効にし、GTP-U コンテンツインスペクションを有効にして GTP-U トンネル内のユーザ データをスキャンします。また、APN、IMSI/IMSI-Prefix、および RAT に基づいて GTPセッションをフィルタリングし、エンドユーザーの IPアドレスのなりすましを防ぐこともできます。

GTP 検査プロファイル 設定

GTP 検査

GTP-C	 ファイアウォールで GTPv1-C または GTPv2-C あるいはその両 方を検索できるようにするには、Stateful Inspection (ステート フル検査)を選択します。ステートフル インスペクションを有 効にすると、firewall は送信元 IP、送信元ポート、宛先 IP、宛先 ポート、プロトコル、および Tunnel Endpoint ID(TEID)を使用し て GTP セッションを追跡します。また、GTP トンネルを確立す るために使用される各種 GTP メッセージの順序をチェックして 検証します。TEID は GSN トンネル エンドポイントを一意に識 別します。アップリンク用のトンネルとダウンリンク用のトン ネルは区別され、異なる TEID が使用されます。
	 有効性チェックエラー時にファイアウォールが実行する Action(アクション)(Block(ブロック)またはAlert(アラート))を選択します。アラートアクションでは、トラフィックを許可してログを生成します。ブロックアクションでは、トラフィックを拒否してログを生成します。 ファイアウォールがペイロードのGTPヘッダーおよび情報要素(IE)で実行する必要のある有効性チェックを指定します。ファイアウォールは、上記で選択したブロックアクションまたはア
	 ラート アクションを使用してエラーを処理します。検証するように firewall を構成できます。 Reserve IE – 予約済みの IE 値を使用する GTPv1-C または GTPv2-C メッセージをチェックします

GTP 検査プロファイル 設定	
	 Order of IE (GTPv1-C のみ) - GTPv1-C メッセージ内の IE の順 序が正確であることを確認します。
	 Length of IE-無効な IE の長さを持つ GTPv1-C または GTPv2-C メッセージをチェックします。
	 ヘッダーの予約済みフィールド – ヘッダーに無効な値または 予約値を使用する不正な形式のパケットをチェックします。
	 サポートされていないメッセージの種類 - 不明または不正な メッセージの種類をチェックします。
GTP-U	GTPv1-C および/または GTPv2-C のステートフル検査を有効にす ると、GTPU-U ステートフル検査が自動的に有効になります。
	GTP-U ペイロードの以下の有効性チェックを指定できます。
	• Reserved IE(予約済み IE) – ペイロードに予約済み IE 値が使 用されている GTP-U メッセージをチェックします。
	 Out of order IE(順序が不適切な IE) – GTP-U メッセージの IE の順序が正しいかどうかをチェックします。
	 Length of IE (IE の長さ) – IE の長さが無効なメッセージを チェックします。
	 ヘッダー内のスペアフラグ - ヘッダーに無効な値または予約値 を使用する不正な形式のパケットをチェックします。
	 Unsupported message type (サポートされていないメッセージ タイプ) – 未知または不正なメッセージ タイプをチェックしま す。
	また、以下の許可アクション、ブロック アクション、またはアラー ト アクションを設定できます。
	 End User IP Address Spoofing (エンドユーザーの IP アドレス スプーフィング) – 加入者ユーザーの機器から送信された GTP- U パケットの送信元 IP アドレスが、トンネルのセットアップ 中に変換された、対応する GTP-C メッセージの IP アドレスと 同じでない場合にブロックまたはアラートするようにファイア ウォールを設定します。
	 PFCP ステートフル インスペクションを有効にした 場合、このオプションは使用できません。
	 GTP-in-GTP – GTP-in-GTP メッセージの検出時にブロックまた はアラートするようにファイアウォールを設定できます。検出 すると、ファイアウォールは重大度が critical (重要)の GTP ロ グを生成します。

GTP 検査プロファイル 設定	
	 GTP-U セッション開始時のログ:GTP-U セッションの開始時に、 関連付けられた IP アドレスとトンネル エンドポイント ID を GTP ログに記録します。
	 GTP-U セッション終了時のログ:GTP-U セッションの終了時に、 関連付けられた IP アドレスとトンネル エンドポイント ID を GTP ログに記録します。
	 4G および 3G の場合、GTP-U パケット内のユーザ データ ペイロードを検査して適用するには、GTP-U コンテンツインスペクション を有効にします。GTP-U コンテンツを検査すると、GTP-C メッセージから学習した IMSI および IMEI 情報とGTP-U パケットのカプセル化された IP トラフィックを相関できます。
5G-C	5G の場合、5G-HTTP2 を有効にして、5G HTTP/2 制御パケットの 検査を有効化します。これには、サブスクライバ ID、機器ID、お よびネットワーク スライス情報を含めることができます。これによ り、加入者 ID (IMSI)、機器 ID (IMEI)、および HTTP/2 メッセージ から取得したネットワーク スライス ID 情報を、GTP-U パケットに カプセル化された IP トラフィックと相互に関連付けできます。 5G-HTTP2 を有効化すると、そのプロファイルの GTP-C が無効化 されます。
PFCP	 パケット転送制御プロトコル(PFCP)の場合、ステートフルインスペクションを有効にして PFCP トラフィックを検査します。PFCP トラフィックに対してステートフルインスペクションを有効にすると、ファイアウォールは MEC とリモート サイトまたはセントラルサイトの間のトラフィックを検査して、サービス拒否 (DOS) やスプーフィングなどの攻撃を防ぎます。 このオプションを有効にすると、GTP-U エンドユーザー IP アドレススプーフィングのアクションは使用できなくなります。 文の状態チェックを指定できます。 関連メッセージのチェック:順序が不順であるか、拒否されたPFCP 関連メッセージがないかチェックします。 セッションメッセージ のチェック:PFCP セッションメッセージが故障しているか、拒否されたメッセージがないかチェックします。 チェックシーケンス番号:PFCP のシーケンス番号が PFCP 要求メッセージのシーケンス番号:PFCP のシーケンス番号が PFCP 要求メッセージのシーケンス番号:PFCP のシーケンス番号が PFCP 要求

GTP 検査プロファイル 設定	
	次に、チェックが失敗したときにファイアウォールに使用する Action (許可、アラート、または ブロック)を指定できます。
	PFCP アソシエーションまたはセッションの先頭または末尾に、 ファイアウォールでログを作成するかどうかも選択できます。
製品連携	
UEIP相関	加入者ID と機器ID の User Equipment (UE: ユーザ機器) IP アドレスへの関連付けとマッピングを可能にします。
モード	 Loose:(デフォルト) ファイアウォール は、GTP-U 内部トラ フィックを検出すると、送信元アドレスまたは宛先アドレスを 照会して、相関する IMEI または IMSI 情報を見つけます。結果 がない場合、ファイアウォール はトラフィックを転送します。
	 Strict:GTP-U クエリが結果を返さない場合にトラフィックをドロップします。
送信元	加入者レベルおよび機器レベルのセキュリティポリシーの適用の ためにコントロールプレーンとユーザプレーン情報を関連付ける ためにファイアウォールで使用するソースを選択します。ファイ アウォールは、加入者ID(SUPIまたはIMSI)、機器ID(PEIまた はIMEI)、ユーザー機器(UE)のIPアドレスなど、5G/4G識別情 報を処理および抽出するために選択した送信元タイプのトラフィッ クを検査し、5G/4G加入者IPトラフィックと関連付けます。
	 PFCP–IPacket Forwarding Control Protocol (PFCP) トラフィックを検査します。
	Control and User Plane Separation (CUPS) を使用し た展開の場合は、 [PFCP] を選択します。
	 RADIUS–IRemote Authentication Dial-In Service (RADIUS) ト ラフィックを検査します。
UEIP開始時のログ	ファイアウォール が UE に IP アドレスを割り当てるときに、UEIP 相関イベントをログに記録します。
UEIP終了時のログ	ファイアウォール が割り当てられた IP アドレスを解放したとき に、UEIP 相関イベントをログに記録します。
フィルタリング オプショ	1ン
RAT フィルタリング	すべての無線アクセス テクノロジ(RAT)がデフォルトで許可さ れます。GTP-C の PDP 作成要求およびセッション作成要求メッ セージは、RAT フィルタに基づいてフィルタリングまたは許可され

GTP 検査プロファイル 設定	
	ます。モバイル コア ネットワークにアクセスするためにユーザー の機器で使用される以下の RAT に基づいて、許可、ブロック、ア ラートするかどうかを指定できます。
	• UTRAN
	• GERAN
	• WLAN
	• GAN
	● HSPA の進化
	• EUTRAN
	• 仮想
	EUTRAN-NB-IoT
	• LTE-M
	• NR
	5G-HTTP2 を有効化すると、以下の RAT を使用できます。
	• WLAN
	• EUTRAN
	• 仮想
	• NR
IMSI フィルタリング	IMSI(国際モバイル加入者識別番号)は、加入者識別モジュール (SIM)カードでプロビジョニングされた GSM、UMTS、LTE ネッ トワークの加入者に関連付けられた一意の ID です。
	通常、IMSI は 15 桁の数値(8 バイト)で表されますが、これより も短い場合もあります。IMSI は、以下の 3 つの部分で構成されま す。
	 3桁で構成されるモバイル国コード(MCC)。MCCは、モバイ ル加入者の居住国を一意に識別します。
	 2桁(欧州標準)または3桁(北米標準)で構成されるモバイ ルネットワークコード(MNC)。MNCは、モバイル加入者の ホーム PLMN を識別します。
	• PLMN 内のモバイル加入者を識別するモバイル加入者識別番号 (MSIN)。
	IMSI Prefix (IMSI プレフィックス)では、MCC と MNC を組み合 わせて、特定の GTP からのトラフィックをallow (許可)、block (ブ ロック)、あるいはalert (アラート)できます。デフォルトでは、すべ ての IMSI が許可されます。

GTP 検査プロファイル 設定	
	IMSI または IMSI プレフィックスを手動で入力するか、それらが 含まれる CSV ファイルをファイアウォールにインポートできま す。IMSI には、310* や 240011* などのワイルドカードを含めるこ とができます。 ファイアウォールでは、最大 5,000 個の IMSI または IMSI プレ フィックスがサポートされています。
ΑΡΝ <i>J</i> イルタリンク	アクセスホイント名(APN)は、ユーサーの機器でインターネットに接続するために必要な GGSN/PGW への参照です。5G では、 データネットワーク名(DNN)の形式に APN があります。APN は、1つまたは2つの識別子で構成されます。
	 GGSN/PGW(必要に応じてモバイルステーションによって要求されるサービス)が接続される外部ネットワークを定義する APNネットワーク識別子。APNのこの部分は必須です。
	 GGSN/PGW がある PLMN GPRS/EPS バックボーンを定義する APN オペレータ識別子。APN のこの部分は任意です。
	デフォルトでは、すべての APN が許可されます。APN フィルタ では、APN 値に基づいて GTP トラフィックを許可、ブロック、 アラートすることができます。GTP-C の PDP 作成要求およびセッ ション作成要求メッセージは、APN フィルタリングに定義された ルールに基づいてフィルタリングまたは許可されます。
	APN フィルタリング リストを手動でファイアウォールに追加また はインポートできます。APN の値には、ネットワーク ID または ネットワークのドメイン名(example.com など)、および必要に応 じてオペレータ ID を含める必要があります。
	APN フィルタリングの場合、ワイルドカード「*」を使用すると、 すべての APN を照合できます。「*」と他の文字の組み合わせ は、ワイルドカードではサポートされていません。たとえば、 「internet.mnc *」は通常の APN として扱われ、internet.mnc で始 まるすべてのエントリをフィルタリングしません。
	ファイアウォールでは、最大 1,000 個の APN フィルタがサポート されています。

GTP Tunnel Limits (**GTP** トンネル制限)

宛先当たりの許可され	GGSN などの宛先 IP アドレスへの GTP-U トンネルの最大数を制限
た最大同時トンネル数	できます。(範囲は 0~1000,000,000 トンネル)
宛先当たりの最大同時 トンネル数でのアラー ト	ある宛先に対して確立された GTP-U トンネルの最大数に達したと きにファイアウォールがアラートをトリガーするしきい値を指定し

GTP 検査プロファイル 設定	
	ます。設定したトンネル制限に達すると、重大度が high(高)の GTP ログ メッセージが生成されます。
ロギング頻度	設定した GTP トンネル制限を超えたときにファイアウォールがカ ウントするイベント数。この数を超えるとログが生成されます。こ の設定を使用して、ログに記録されるメッセージ量を削減できます (範囲は 0~1000,000,000、デフォルトは 100)。
超過請求の保護	ファイアウォールの Gi/SGi ファイアウォールとして機能する仮想 システムを選択します。Gi/SGi ファイアウォールは、PGW/ GGSN から Gi/SGi インターフェイスを通過してインターネットなどの外 部 PDN (パケット データ ネットワーク)へ送信されるモバイル加 入者の IP トラフィックを検査し、モバイル加入者のインターネッ ト アクセスを保護します。
	GGSN がエンドユーザー IP アドレス プールから以前に使用した IP アドレスをモバイル加入者に割り当てると、超過請求が発生する可 能性があります。インターネット上の悪意のあるサーバーが以前 の加入者のために開始されたセッションを終了せずにこの IP アド レスにパケットを送信し続けると、このセッションは Gi ファイア ウォールで開いたままになります。(PDP 削除メッセージまたは セッション削除メッセージによって)GTP トンネルが検出される か、タイムアウトしたときにデータが配信されないようにするため に、超過請求保護が有効になっているファイアウォールは、加入者 に属しているすべてのセッションをセッション テーブルから削除 するように Gi/SGi ファイアウォールに通知します。GTP セキュリ ティと SGi/Gi ファイアウォールは同じ物理ファイアウォールに設 定する必要がありますが、仮想システムは異なっていても問題あり ません。GTP-C イベントに基づいてセッションを削除するには、 ファイアウォールにすべての関連するセッション情報が必要です。 これが可能なのは、モバイル コア ネットワークで SGi + S11 また は S5 インターフェイス(GTPv2)および Gi + Gn インターフェイ ス(GTPv1)からのトラフィックを管理している場合だけです。

その他のログ設定

デフォルトでは、ファイアウォールは許可された GTP または PFCP メッセージをログに記録 しません。大量のログを生成するため、必要に応じてトラブルシューティングを行うため、 許可された GTP および PFCP メッセージのロギングを選択的に有効にできます。このタブで は、許可されたログ メッセージ以外にもユーザー ロケーション情報のロギングを選択的に有 効化できます。

GTPv1-C の許可された	GTPv1-C のステートフル検査が有効になっている場合、許可され
メッセージ	た GTPv1-C メッセージのロギングを選択的に有効化できます。こ
	れらのメッセージで生成されるログは、必要に応じて問題をトラブ
	ルシューティングするのに役立ちます。

GTP 検査プロファイル 設定	
	デフォルトでは、ファイアウォールは許可されたメッセージをログ に記録しません。許可された GTPv1-C メッセージのロギング オプ ションは、以下のとおりです。
	 Tunnel Management(トンネル管理) – これらの GTPv1-C メッセージは、SGSN と GGSN などのネットワーク ノードの 特定のペア間でカプセル化された IP パケットとシグナル メッ セージを送信する GTP-U トンネルの管理に使用されます。こ れには、PDP コンテキスト作成要求、PDP コンテキスト作成 応答、PDP コンテキスト更新要求、PDP コンテキスト更新応 答、PDP コンテキスト削除要求、PDP コンテキスト削除応答な どのメッセージが含まれます。
	 Path Management (パス管理) – 通常、これらの GTPv1-C メッセージは、ピアがアライブ状態かどうかを確認するために GSN または無線ネットワーク制御局 (RNC) から他の GSN また は RNC に送られます。これには、エコー要求およびエコー応答 等のメッセージが含まれます。
	 Others (その他) – これらのメッセージには、場所の管理、モビリティの管理、RAN 情報の管理、およびマルチメディアブロードキャスト マルチキャスト サービス (MBMS) などのメッセージが含まれます。
ユーザー ロケーション を記録	エリア コードやセル ID などのユーザー ロケーション情報を GTP ログに含めることができます。
パケット キャプチャ	GTP イベントをキャプチャできるようになります。
GTPv2-Cの許可された メッセージ	GTPv2-Cのステートフル検査が有効になっている場合、許可された GTPv2-C メッセージのロギングを選択的に有効化できます。これらのメッセージで生成されるログは、必要に応じて問題をトラブルシューティングするのに役立ちます。
	デフォルトでは、ファイアウォールは許可されたメッセージをログ に記録しません。許可された GTPv2-C メッセージのロギング オプ ションは、以下のとおりです。
	 Tunnel Management(トンネル管理) – これらの GTPv2-C メッセージは、SGW と PGW などのネットワーク ノードの特 定のペア間でカプセル化された IP パケットとシグナル メッセー ジを送信する GTP-U トンネルの管理に使用されます。これに は、以下のメッセージ タイプが含まれます。セッション作成要 求、セッション作成応答、ベアラ作成要求、ベアラ作成応答、 ベアラ変更要求、ベアラ変更応答、セッション削除要求、およ びセッション削除応答。

GTP 検査プロファイル 設定	
	 Path Management (パス管理) – 通常、これらの GTPv2-C メッセージは、ピアがアライブ状態かどうかを確認するために SGW または PGW などのネットワーク ノードから他の SGW ま たは PGW に送信されます。これには、エコー要求およびエコー 応答等のメッセージが含まれます。 Others (その他) – これらのメッセージには、モビリティの管 理や 3GPP 以外のアクセスに関連するメッセージなどが含まれ ます。
GTP-U の許可された メッセージ	GTPv2-C または GTPv1-C のステートフル検査を有効にした場合 に、許可済み GTP-U メッセージのロギングを選択的に有効化する ことができます。これらのメッセージで生成されるログは、必要に
	応して問題をトラブルシューティング 9 るのに役立らま 9 。 許可された GTP-U メッセージのロギング オプションは、以下のと おりです。
	 Tunnel Management (トンネル管理) – これらはエラー兆候などの GTP-U シグナル メッセージです。
	 Path Management (パス管理) – これらの GTP-U メッセージ は、ピアがアライブ状態かどうかを確認するためにネットワー クノード (eNodeB など)から別のネットワークノード (SGW など)に送られます。これには、エコー要求/応答などのメッ セージが含まれます。
	 G-PDU – G-PDU (GTP-U PDU) は、モバイル コア ネットワー クのネットワーク ノード内のユーザー データ パケットを送信す るために使用され、GTP ヘッダーと T-PDU で構成されます。
新しい GTP-U 当たり のログされた G-PDU パケット	ファイアウォールで GTP-U PDU が検査されていることを確認する には、このオプションを有効にします。ファイアウォールは、新し い GTP-U トンネルごとに指定した数の G-PDU パケットのログを生 成します(範囲は 1~10、デフォルトは 1)。
5G-C Allowed Messages(5G-Cの許 可されたメッセージ)	N11を選択し、許可された N11 メッセージのログを選択的に有効化します。N11 メッセージは、トラブルシューティングに役立ち、多様な手順により、N11 インターフェース経由で交換されるHTTP/2 メッセージをより詳しく可視化します。このフィールドは、モバイルネットワーク保護プロファイルの 5G-C タブで 5G-HTTP2 を有効化した場合にのみ利用可能です。
PFCPの許可されたメッ セージ	PFCP に対してステートフル インスペクションを有効にした場合 に、許可された PFCP メッセージのロギングを選択的に有効にでき ます。これらのメッセージで生成されるログは、必要に応じて問題 をトラブルシューティングするのに役立ちます。

GTP 検査プロファイル 設定	
	許可される PFCP メッセージのロギング・オプションは、以下のと おりです。
	 セッション確立:これらの PFCP メッセージは、GTP-U トンネルの確立を含むセッションを設定します。
	 セッション変更:これらの PFCP メッセージは、セッション ID または PDR ID が変更された場合 (たとえば、4G から 5G ネット ワークに移動した結果として) 送信されます。これには、PFCP セッション変更要求や PFCP セッション変更応答などのメッセー ジが含まれます。
	 セッション削除:これらの PFCP メッセージは、関連リソースの 解放を含む PFCP セッションを終了します。

Objects(オブジェクト) > Security Profiles(セキュリ ティプロファイル) > SCTP Protection(SCTP プロテ クション)

ファイアウォールでSCTPチャンクの検証とフィルタリングを行う方法を指定する、Stream Control Transmission Protocol (SCTP)(ストリーム制御伝送プロトコル(SCT))プロテク ション プロファイルを作成します。このプロファイルタイプをセキュリティ プロファイルの 下に表示するには、SCTP セキュリティ(Device(デバイス) > Setup(セットアップ) > Management(管理) > General Settings(一般設定))を有効にする必要があります。また、 マルチホーム環境で SCTP エンドポイントごとの IP アドレス数を制限することもできるほか、 ファイアウォールが SCTP イベントを記録するタイミングを指定することもできます。SCTP プ ロテクション プロファイルを作成したら、ゾーンのセキュリティ ポリシー ルールにプロファイ ルを適用する必要があります。

SCTP セキュリティをサポートするファイアウォール モデルには、事前定義済みの SCTP プロ テクション プロファイル (デフォルト - ss7) がそのまま使用できます。また、default-ss7 プロ ファイルを新しい SCTP プロテクション プロファイルの基礎として複製できます。Object (オ ブジェクト) > Security Profiles (セキュリティ プロファイル) > SCTP Protection (SCTP プロ テクション)を選択し、default-ss7 (デフォルト-ss7)を選ぶと、この定義済みプロファイル のアラートを引き起こす操作コードが表示されます。

SCTP プロテクション プロファイル設定	
氏名	SCTP プロテクション プロファイルの名前を入力します。
の意味	SCTP プロテクション プロファイルの説明を入力します。

SCTP Inspection SCTP インスペクション

不明なチャンク	不明なチャンク (RFC3758、RFC4820、RFC4895、RFC4960、RFC5061、 または RFC 6525で定義されないチャンク)を含む SCTP を受 信する場合のファイアウォールのアクションを選択します:
	 allow(許可)(デフォルト) –パケットに変更を加えない で通過させます。
	 alert (アラート) –パケットを変更せずに通過さ せ、SCTP ログを生成させます (これらのログには ログストレージを割り当てる必要があります。詳細 は、Logging and Reporting Settings (ロギングおよびレ ポート設定) のところにある Log Storage (ログストレー ジ) タブ: Device (デバイス) > Setup (セットアップ) > Management (管理) を参照してください。

SCTP プロテクション プロファイル設定	
	 block (ブロック) –パケットを渡す前にチャンクを無効にし、SCTP ログを生成します。
Chunk Flags チャンクフラグ	RFC4960 と矛盾するチャンク フラグを持つ SCTP パケットを 受信したときに、ファイアウォールの動作を選択します。
	 allow(許可)(デフォルト)-パケットに変更を加えない で通過させます。
	 alert (アラート) -パケットを変更せずに通過させ、SCTP ログを生成させます (これらのログにはログストレージを割り当てる必要があります。詳細は、Logging and Reporting Settings (ロギングおよびレポート設定) のところにある Log Storage (ログストレージ) タブ:Device (デバイス) > Setup (セットアップ) > Management (管理)を参照してください。 block (ブロック) -パケットをドロップし、SCTP ログを生成します。
Invalid Length 不正な長さ	無効な長さの SCTP チャンクを受信したときに、ファイア ウォールの動作を選択します。
	 allow (許可) (デフォルト) –パケットまたはチャンクに 変更を加えないで通過させます。
	 block (ブロック) ーパケットを破棄して SCTP ログを生成 します(これらのログにはログ ストレージを割り当てる必 要があります。Log Storage (ログ ストレージ) タブを参照 してください。
マルチホーミングのIPアドレ スの制限数:	ファイアウォールがアラート メッセージを生成する前 に、SCTP エンドポイントに設定できる IP アドレスの最大数 を入力します(範囲は 1~8、デフォルトは 4)。
	SCTP マルチホーミングは、ピアとの関連付けのために複数の IP アドレスをサポートするエンドポイントの機能です。エン ドポイントへの1つのパスが失敗すると、SCTP は、そのア ソシエーションに提供されている他の宛先 IP アドレスの1つ を選択します。
ログ設定	許可されたチャンク、アソシエーションの開始と終了、およ び状態の失敗イベントの SCTP ログを生成する設定の任意の 組み合わせを選択します。
	 Log at Association Start アソシエーション開始時にロギン グ
	• Log at Association End アソシエーション終了時にロギング

SCTP プロテクション プロファイル設定	
	 Log Allowed Association Initialization Chunks 許可された アソシエーション初期化チャンクをロギング
	 Log Allowed Heartbeat Chunks 許可されたハートビート チャンクをロギング
	 Log Allowed Association Termination Chunks 許可された アソシエーション終了チャンクをロギング
	• Log All Control Chunks すべての制御チャンクをロギング
	 Log State Failure Events ログ状態 失敗イベント
	ファイアウォールが SCTP ログを保存する場合は、SCTP ログ ストレージを割り当てる必要があります(詳細は、Logging and Reporting Settings (ロギングおよびレポート設定) のとこ ろにある Log Storage (ログ ストレージ) タブ: Device(デバ イス)> Setup(セットアップ)> Management(管理)を参 照してください。

フィルタリング オプション

SCTP Filtering SCTP フィルタリング

氏名	SCTP フィルタの名前を入力します。
氏名 PPID	 SCTP フィルタの名前を入力します。 SCTP フィルタの PPID を指定します。 any (すべて) -ファイアウォールは、PPID を含むすべてのSCTP データチャンクで指定したアクションを実行します。 3GPP PUA 3GPP RNA LCS-AP M2UA M3UA NBAP RUA S1AP SBc-AP SUA Y2AD
	 有効な PPID 値(ドロップダウン リストにない値)を入力 します。たとえば、H.323 の PPID 値は 13 です。

SCTP プロテクション プロファイル設定	
	各 SCTP フィルタで指定できる PPID は 1 つだけです が、SCTP 保護プロファイルに複数の SCTP フィルタを指定で きます。
操作	ファイアウォールが指定した PPID を含むデータ チャンクに かかる処理を指定します。
	 allow(許可)(デフォルト)-チャンクに変更を加えない で通過させます。
	 alert (アラート) -チャンクを変更せずに通過させ、SCTP ログを生成させます(これらのログにはログストレージを割り当てる必要があります。詳細は、Logging and Reporting Settings (ロギングおよびレポート設定)のところにある Log Storage (ログストレージ) タブ:Device (デバイス) > Setup (セットアップ) > Management (管理)を参照してください。
	 block (ブロック) –パケットを渡す前にチャンクを無効にして SCTP ログを生成します (これらのログのログストレージを割り当てる必要があります。詳細は、Logging and Reporting Settings (ロギングおよびレポート設定)のところにある Log Storage (ログストレージ) タブ: Device (デバイス) > Setup (セットアップ) > Management (管理)を参照してください。

SCTP パケットは、リスト内のフィルタと上から下に一致します。プロファイル用に複数の SCTP フィルタを作成する場合は、SCTP フィルタの順序が異なります。SCTP フィルタリン グリストで相対優先度を変更するには、フィルタを1つ選択してMove Up(上へ)または Move Down(下へ)移動します。

ダイアメーター フィルタリング

氏名	ダイアメーター フィルタの名前を入力します。
操作	ファイアウォールが実行する、ダイアメーター アプリケー ション ID、コマンド コード、および AVP を含むダイアメー ター チャンクで実行するアクションを指定します。検査さ れたチャンクが、指定されたダイアメーター アプリケーショ ン ID と、指定されたダイアメータ コマンド コードのすべて と、指定されたダイアメータ AVP のいずれかを含む場合は、 以下の操作を行います。
	 allow(許可)(デフォルト)-チャンクに変更を加えない で通過させます。
	 alert (アラート) –チャンクを変更せずに通過させ、SCTP ログを生成させます(これらのログには

SCTP プロテクション プロファイル設定	
	ログストレージを割り当てる必要があります。詳細 は、Logging and Reporting Settings (ロギングおよびレ ポート設定) のところにある Log Storage (ログストレー ジ) タブ: Device (デバイス) > Setup (セットアップ) > Management (管理) を参照してください。 block (ブロック) –パケットを渡す前にチャンクを無効 にして SCTP ログを生成します (これらのログのログスト レージを割り当てる必要があります。詳細は、Logging and Reporting Settings (ロギングおよびレポート設定) のところ
	にある Log Storage (ログストレージ) タブ:Device(デバイス) > Setup(セットアップ) > Management(管理)を 参照してください。
ダイアメーター アプリケー ション ID	 ファイアウォールが指定された処理を行うチャンクのダイア メーター アプリケーション ID を指定します。 すべて 3GPP-Rx 3GPP-S6a/S6d 3GPP-S6c 3GPP-S9 3GPP-S13/S13 3GPP-Sh ダイアメーター基礎アカウンティング
	 ダイアメーター一般メッセージ ダイアメーター クレジット制御 また、ダイアメーター アプリケーション ID の数値を入力す ることもできます(範囲は 0~4、294,967,295)。ダイア メーター フィルタは、1つのアプリケーション ID しか持つことができません。
ダイアメーター コマンド コード	ファイアウォールが指定された処理を行うチャンクのダイア メーター コマンド コード を指定します。any(すべて)を 選択し、ドロップダウンリストからダイアメーター コマン ド コードの 1 つを選択するか、または特定の値を入力します (範囲は0~16,777,215)。ドロップダウンには、選択した ダイアメーター アプリケーション ID に適用されるコマンド コードのみが含まれています。複数のダイアメーター コマン ド コードをダイアメーター フィルタに追加することができま す。

SCTP プロテクション プロファ	マイル設定
ダイアメーター AVP	ファイアウォールが指定された処理を行うチャンクの ダイアメーター属性値ペア(AVP)コードを指定しま す。1つ以上の AVP コードまたは値を入力します(範囲 は1~16,777,215)。

プロファイル用に複数のダイアメーターフィルタを作成する場合は、ダイアメーターフィルタの順序が異なります。ダイアメーターフィルタリングリストで相対優先度を調節するには、フィルタを1つ選択してMove Up(上へ)または Move Down(下へ)移動します。

SS7 Filtering SS7 フィルタリング

氏名	SS7 フィルタの名前を入力します。
操作	ファイアウォールが指定した SS7 フィルタ要素 を含む SS7 チャンクにかかる処理を指定します。検査されるチャンクが SCCP 発呼者 SSN と指定された SCCP 発呼者 グローバル タイ トル (GT) 値および指定された運用コードのいずれかを含む 場合:
	 allow(許可)(デフォルト)-チャンクに変更を加えない で通過させます。
	 alert (アラート) -チャンクを変更せずに通過させ、SCTP ログを生成させます (これらのログにはログストレージを割り当てる必要があります。詳細は、Logging and Reporting Settings (ロギングおよびレポート設定)のところにある Log Storage (ログストレージ) タブ: Device (デバイス) > Setup (セットアップ) > Management (管理)を参照してください。 block (ブロック) -パケットを渡す前にチャンクを無効にして SCTP ログを生成します (これらのログのログストレージを割り当てる必要があります。詳細は、Logging and Reporting Settings (ロギングおよびレポート設定)のところにある Log Storage (ログストレージ) タブ: Device (デバイス) > Setup (セットアップ) > Management (管理)を参照してください。
SCCP Calling Party SSN SCCP 発呼者 SSN	ファイアウォールが指定された処理を行うチャンクの SCCP 発呼者 SSN を指定します。any-map(すべてのマップ)を選 択するか、SCCP 発呼者 SSN の1つをドロップダウンリスト からAdd(追加)します。 • HLR(MAP)
	• VLR(MAP)
	MSC(MAP)
	• EIR(MAP)

SCTP プロテクション プロファ	イル設定
	 GMLC(MAP) gsmSCF(MAP) SIWF(MAP) SGSN(MAP) GGSN(MAP) CSS(MAP) CAP INAP SCCP 管理 SS7フィルタは、SCCP 発呼者 SSNを1つしか持つことができ
SCCP Calling Party GT SCCP 発呼者 GT	 ス e れ。 ファイアウォールが指定された処理を行うチャンクの SCCP 発呼者 GT 値を指定します。Any (すべて)を選択するか、 最大 15 桁の数値を Add (追加)します。また、プレフィックスを使用して、SCCP 発呼者 GT 値のグループを入力することもできます。以下に例を示します。876534*。複数の SCCP 発呼者 GT値を SS7 フィルタに追加できます。 SCCP 発呼者 SSN のが以下の場合:INAP と SCCP Management (SCCP 管理)では、このオプションは無効になります。
運用コード	ファイアウォールが指定された処理を行うチャンクの運用 コードを指定します。 次の SCCP 発呼者 SSNの場合は、any (すべて) ドロップダ ウンリストからすべてまたは運用コードを選択するか、特定 の値 (範囲は1~255) を入力します。 HLR(MAP) VLR(MAP) SIR(MAP) EIR(MAP) GMLC(MAP) SIWF(MAP) SIWF(MAP) SGSN(MAP) GGSN(MAP) CSS(MAP)

SCTP プロテクション プロファイル設定	
	SCCP 発呼者 SSN のが以下の場合:CAP の場合は、値を入力し ます(1~255)。
	SCCP 発呼者 SSN のが以下の場合:INAP と SCCP Management (SCCP 管理)では、このオプションは無効にな ります。
	複数の運用 コードを SS7 フィルタに追加することができま す。
プロファイル田に複数の SS7 ~	7、山々を作成する埋合け SC7 フィ山々の順向が異たりま

プロファイル用に複数の SS7 フィルタを作成する場合は、SS7 フィルタの順序が異なりま す。SS7 フィルタリング リストで相対優先度を調節するには、フィルタを1つ選択してMove Up(上へ)または Move Down(下へ)移動します。

Objects > Security Profile Groups [オブジェクト > セ キュリティ プロファイル グループ]

ファイアウォールでは、セキュリティプロファイルのセットを指定してセキュリティプロファ イルグループを作成する機能がサポートされています。セキュリティプロファイルグループ は、1つの単位として処理でき、セキュリティポリシーに追加できます。たとえば、脅威セ キュリティプロファイルグループを作成して、アンチウイルス、アンチスパイウェア、および 脆弱性防御の各プロファイルを追加し、その後、セキュリティポリシールールを作成してその 脅威プロファイルを追加することができます。

同時に割り当てられることが多いアンチウイルス、アンチスパイウェア、脆弱性防御、URL フィルタリング、およびファイル ブロッキングの各プロファイルをプロファイル グループにま とめることで、セキュリティ ポリシーの作成を簡略化できます。

新しいセキュリティ プロファイルを定義するには、Objects(オブジェクト) > Security Profiles(セキュリティ プロファイル)を選択します。

セキュリティ プロファ イル グループ設定	の意味
氏名	プロファイル グループ名(最大 31 文字)を入力します。この名前 は、セキュリティ ポリシーを定義するときにプロファイルのリス トに表示されます。名前の大文字と小文字は区別されます。また、 一意の名前にする必要があります。文字、数字、スペース、ハイフ ン、およびアンダースコアのみを使用してください。
共有(Panorama の み)	 以下に対してプロファイルグループを公開する場合は、このオプションを選択します。 multi-vsys ファイアウォールの各仮想システム (vsys)。この選択を解除すると、Objects[オブジェクト] タブで選択した Virtual System[仮想システム] のみに対してプロファイルグループが公開されます
	 Panorama 上の各デバイス グループ。この選択を解除すると、Objects[オブジェクト] タブで選択したDevice Group[デバイスグループ] のみに対してプロファイルグループが公開されます。
オーバーライドの無効 化(Panoramaのみ)	管理者が、オブジェクトを継承するデバイス グループのこのセキュ リティ プロファイル グループ オブジェクトの設定をオーバーライ ドすることを禁止する場合はこのオプションを選択してください。 デフォルトでこのオプションはオフになっており、管理者は、この オブジェクトを継承するデバイス グループの設定をオーバーライド できます。

以下の表では、セキュリティプロファイル設定について記載しています。

セキュリティ プロファ イル グループ設定	の意味
プロファイル	グループに含めるアンチウイルス、アンチスパイウェア、脆弱性防御、URLフィルタリング、およびファイルブロッキングの各プロファイルを選択します。データフィルタリングプロファイルも、セキュリティプロファイル グループに含めることができます。 「Objects(オブジェクト) > Security Profiles(セキュリティプロファイル) > Data Filtering(データフィルタリング)」を参照してください。

Objects > Log Forwarding [オブジェクト > ログ転送]

デフォルトでは、ファイアウォールで生成されるログはそのローカルストレージにのみ存在します。ただし、Panorama[™]、ログサービス、または外部サービス(syslog サーバーなど)を使用して、ログ転送情報を定義し、そのプロファイルをセキュリティ、認証、DoS 保護、およびトンネル検査のポリシールールに割り当てることにより、ログ情報を集中的に監視できます。ログ転送プロファイルは、次の Log Types(ログタイプ)の転送先を定義します。データフィルタリング、GTP、SCTP、脅威、トラフィック、トンネル、URL フィルタリング、およびWildFire[®]送信ログなど。

コンプライアンス、冗長性、分析の実行、一元的な監視、脅威の挙動のレビュー、 長期的なパターンなど、ログを Panorama あるいは外部ストレージに転送する理 由には様々なものがあります。さらに、ファイアウォールのログの保存容量には 限りがあり、保存領域が一杯になったら古いログを削除します。脅威ログおよび WildFire ログを必ず転送するようにしてください。

他のログタイプを転送するには、「Device(デバイス) > Log Settings(ログ設定)」を参照してください。

PA-7000 シリーズのファイアウォールでログを転送したり、ファイルを WildFire[®] に転送するには、まず PA-7000 シリーズのファイアウォールでLog Card Interface (ログカードインターフェイス)を設定する必要があります。このイン ターフェイスを設定すると、ファイアウォールは自動的にこのポートを使用しま す。特別な設定は不要です。PA-7000 シリーズネットワーク処理カード (NPC)の いずれかにデータポートをログ カード インターフェイス タイプとして設定し、使 用するネットワークがログ サーバと通信できることを確認してください。WildFire 転送の場合、ネットワークは WildFire クラウドまたは WildFire アプライアンス(あ るいはその両方)と正常に通信する必要があります。

ログ転送プロファイル の設定	の意味
氏名	プロファイルを識別する名前を入力します(最大 64 文字)。この 名前は、セキュリティ ポリシー ルールを定義するときにログ転送 プロファイルのリストに表示されます。大文字と小文字を区別し、 一意の名前を入力する必要があります。文字、数字、スペース、ハ イフン、アンダースコアのみが使用できます。
共有(Panorama の み)	以下に対してプロファイルを公開する場合は、このオプションを選 択します。 • マルチ vsys ファイアウォール上のすべての仮想システ ム(vsys)-このオプションを無効 (クリア) にすると プロ

以下の表で、ログ転送プロファイルの設定について説明します。

ログ転送プロファイル の設定	の意味
	ファイルは Objects(オブジェクト)タブで選択したVirtual System(仮想システム)のみで利用可能になります。
	 Panorama 上のすべてのデバイス グループーこのオプションを 無効(クリア)にすると、プロファイルは Objects(オブジェクト)タブで選択したDevice Group(デバイスグループ)のみで 利用可能になります。
Cortex Data Lake への 拡張アプリケーション ロギングを有効にしま す(トラフィックおよ び URL ログを含む) (Panorama のみ)	Palo Alto Networks クラウドサービス用の強化されたアプリケー ションログは、Cortex Data Lake サブスクリプションで利用するこ とができます。強化されたアプリケーションロギングにより、Palo Alto Networks クラウドサービス環境で実行されるアプリのネット ワーク アクティビティに対する可視性を向上させることを目的とし たデータをファイアウォールが収集できるようになります。
オーバーライドの無効 化(<mark>Panoramaのみ</mark>)	このログ転送プロファイルの設定が、このプロファイルを継承した デバイス グループで管理者によりオーバーライドされることを防 止するには、このオプションを選択します。デフォルトでこのオプ ションは無効(クリア)になっており、管理者は、このプロファイ ルを継承するデバイス グループの設定をオーバーライドできます。
の意味	このログ転送プロファイルの目的を説明します。
一致リスト(ラベルな し)	1つ以上(最大 64 個)の一致リストプロファイルを Add(追加)し、転送先のほか、ファイアウォールでどのログを送信するかを制御するログ属性ベースのフィルタ、ログに対して実行するアクション(自動タグ付けなど)を指定します。一致リストプロファイルごとに次の2つのフィールド(名前と説明)を入力します。
名前(一致リスト プロ ファイル)	一致リスト プロファイルを識別する名前を入力します(最大 31 文 字)。
説明(一致リスト プロ ファイル)	この一致リスト プロファイルの目的を説明します(最大 1,023 文字)。
ログ タイプ	この一致リストのプロファイルが適用されるログの種類を選択し ます。認証(auth)、data(データ)、gtp、sctp、threat(脅 威)、traffic(トラフィック)、tunnel(トンネル)、URL、また は WildFire。
フィルタ	デフォルトでは、ファイアウォールは、選択された Log Type(ロ グタイプ)の All Logs(すべてのログ)を転送します。ログの一部 を転送するには、ドロップダウン リストから既存のフィルタを選 択するか、Filter Builder(フィルタ ビルダー)を選択して新しい

ログ転送プロファイル の設定	の意味
	フィルタを追加します。新しいフィルタの各クエリに対して、以下 のフィールドを指定して、クエリを Add(追加)します。
	 Connector(条件式) – クエリの結合ロジック(AND/OR)を 選択します。ロジックに否定を適用する場合は、Negate(否 定)を選択します。たとえば、信頼されていないゾーン からのログ転送を防ぐには、Negate(上記以外)を選択 し、Attribute(属性)として Zone(ゾーン)、Operator(演算 子)として equal(等しい)を選択して、Value(値)列に信頼 されていないゾーンの名前を入力します。
	 Attribute(属性) – ログの属性を選択します。使用可能な属性 は、Log Type(ログタイプ)によって異なります。
	 Operator(演算子) – 属性を適用するかどうかを決定する基準を選択します(equal(等しい)など)。使用可能な基準は、Log Type(ログタイプ)によって異なります。
	 ● Value[値] – 照合する属性値を指定します。
	フィルタが一致するログを表示またはエクスポートするに は、[フィルタリングされたログの表示]を選択します。これによ り、Monitorタブと同様のオプションが用意されます (Monitor (モ ニタ) > Logs (ログ) > Traffic (トラフィック)など)。
Panorama Panorama/Logging Service (Panorama の み)	ログコレクタまたは Panorama 管理サーバーにログを転送す る場合、あるいはログをロギング サービスに転送する場合 は、Panorama を選択します。
	このオプションを有効にする場合、configure log forwarding to Panorama(Panorama へのログ転送を設定)する必要があります。
	また、ロギング サービスを使用するには、Device(デバイス) > Setup (セットアップ) > Management(管理)でロギング サービ スを Enable(有効)にする必要があります。
SNMP	ログを SNMP トラップとして転送するには、1 つ以上の SNMP トラップ サーバー プロファイルを Add (追加) します (「Device (デバイス) > Server Profiles (サーバー プロファイ ル) > SNMP Trap (SNMP トラップ)」を参照)。
電子メール	ログを電子メール通知として転送するには、1つ以上の電子メール サーバー プロファイルを Add (追加) します(「Device (デバイ ス) > Server Profiles (サーバー プロファイル) > Email (電子メー ル)」を参照)。
Syslog	ログを Syslog メッセージとして転送するには、1 つ以上の Syslog サーバー プロファイルを Add(追加)します(「Device(デバイ

ログ転送プロファイル の設定	の意味
	ス) > Server Profiles(サーバー プロファイル) > Syslog」を参 照)。
НТТР	ログを HTTP 要求として転送するには、1 つ以上の HTTP サーバー プロファイルを Add(追加)します(「Device(デバイス) > Server Profiles(サーバー プロファイル) > HTTP」を参照)。
ビルトイン アクション	実行するアクションをAdd(追加)する際、Tagging(タグ付け) とIntegration(統合)の2種類の組み込みアクションから選択でき ます。 • タグを付ける-ログエントリ内の送信元または宛先 IP アドレス に対してタグを自動的に追加または削除して、ファイアウォー ルまたは Panorama の User-ID エージェントあるいはリモート の User-ID エージェントに IP アドレスとタグのマッピングを 登録します。これにより、イベントに応答し、セキュリティ ポ リシーを動的に適用できます。IP アドレスにタグを付けること ができ、ダイナミックアドレス グループを使用してポリシーを 動的に適用できることで、可視性が向上し、適切なコンテクス トが与えられ、詳細な制御が可能になり、IP アドレスがネット ワーク上のどの場所に移動してもセキュリティ ポリシーを一貫 して適用できます。
	 アクションを Add(追加)し、そのアクションを説明する名前を入力します。
	 タグ付けの対象の IP アドレスを選択します(Source Address(送信元アドレス)または Destination Address(宛 先アドレス))。
	ログ エントリに送信元 IP アドレスまたは宛先 IP アドレスを含 むすべてのログ タイプに対してアクションを実行できます。相 関ログおよび HIP マッチ ログでは、送信元 IP アドレスにのみ タグを付けることができます。システム ログおよび設定ログで は、アクションを設定することはできません。これらのログ タ イプのログ エントリに IP アドレスが含まれないためです。
	 アクション(Add Tag(タグの追加)または Remove Tag(タ グの除去))を選択します。
	 IP アドレスとタグのマッピングを、このファイアウォールまたは Panorama の Local User-ID (ローカル User-ID) エージェントに登録するか、Remote User-ID (リモート User-ID) エージェントに登録するかを選択します。
	 IP アドレスとタグのマッピングを Remote User-ID (リモート User-ID) エージェントに登録するには、転送を有効にする
ログ転送プロファイル の設定	の意味
-------------------	---
	HTTP サーバー プロファイルを選択します(Device (デバイス) > Server Profiles (サーバー プロファイル) > HTTP)。 • IP 対タグの Timeout (タイムアウト)を指定すれば、IP アドレス対タグのマッピングを保持する期間(分)を設定できます。タイムアウトを0にすると、IP 対タグのマッピングがタ
	 イムアウト しなくなります (範囲は 0~43200 (30 日)、 ケフォルトは 0)。 ダイムアウトを設定できるのはAdd Tag (タグの追加)アクションだけです。 ターゲットの送信元または宛先 IP アドレスに対して適用または削除する Tags (タグ)を入力または指定します。
	 統合–Azure の VM-Series ファイアウォールでのみ使用可能 です。このオプションを使用すると、選択したログをAzure- Security-Center-Integration アクションを使用して Azure セキュ リティ センターに転送できます。
	ログ転送プロファイル フィルタに基づき、デバイスを Quarantine List(隔離リスト)に追加するには、[Quarantine(隔離)]を選択し ます。

Objects (オブジェクト) > Authentication (認証)

認証実施オブジェクトでは、ネットワーク リソースにアクセスするエンド ユーザーを認証する ために使用する方式とサービスを指定します。オブジェクトを認証ポリシー ルールに割り当て ると、認証ポリシー ルールは、トラフィックがルールに一致すると、該当の認証方式とサービ スを呼び出します(Policies(ポリシー) > Authentication(認証)を参照)。

ファイアウォールには、あらかじめ定義された読み取り専用の以下の認証実施オブジェクトがあります。

- default-browser-challenge (デフォルト ブラウザ チャレンジ) ファイアウォールは ユーザー認証情報を透過的に取得します。このアクションを選択した場合、configure Authentication Portal (認証ポータルの設定) ■時に Kerberos シングル サインオン (SSO) または NT LAN Manager (NTLM) 認証を有効化する必要があります。Kerberos SSO 認証に 失敗すると、ファイアウォールは NTLM 認証に戻ります。NTLM を設定していない場合、 または NTLM 認証に失敗した場合、ファイアウォールは、事前定義済みの default-webform (デフォルト Web フォーム) で指定された認証方式にフォールバックします。
- default-web-form (デフォルト Web フォーム) –ユーザーを認証するために、ファイア ウォールは、configure Authentication Portal (認証ポータルの設定) ■時に指定された証明 書プロファイルまたは認証プロファイルを使用します。認証プロファイルを指定した場合、 ファイアウォールはプロファイル内のすべての Kerberos SSO 設定を無視し、認証情報を入力 するための Authentication Portal (認証ポータル) ページをユーザーに表示します。
- default-no-captive-portal (デフォルト キャプティブ ポータルなし) ファイアウォールは ユーザーを認証せずにセキュリティ ポリシーを確認します。
- カスタムの認証実施オブジェクトを作成する前に以下の操作を行ってください。
- 認証サービスへの接続方法を指定するサーバープロファイルを設定します(Device(デバイス) > Server Profiles(サーバープロファイル)を参照)。
- Kerberos シングル サインオン パラメータなどの認証設定を指定する認証プロファイルに サーバー プロファイルを割り当てます(Device(デバイス) > Authentication Profile(認証 プロファイル)を参照)。

カスタムの認証実施オブジェクトを作成するには、Add(追加)をクリックして、以下のフィー ルドを入力します。

認証強度設定	の意味
氏名	分かりやすい名前(最大 31 文字)を入力し、認証ルールを作成する ときにオブジェクトを容易に特定できるようにします。名前の大文字 と小文字は区別されます。また、一意の名前にする必要があります。 文字、数字、スペース、ハイフン、およびアンダースコアのみを使用 してください。
共有(Panorama の み)	以下に対してオブジェクトを公開する場合は、このオプションを選択 します。

認証強度設定	の意味
	 multi-vsys ファイアウォールの各仮想システム (vsys)。この選択 を解除すると、Objects (オブジェクト) タブで選択した Virtual System (仮想システム) のみに対してオブジェクトが公開されま す。 Panorama 上の各デバイス グループ。この選択を解除する と、Objects (オブジェクト) タブで選択した Device Group (デ バイス グループ) のみに対してオブジェクトが公開されます。
オーバーライドの無 効化(Panoramaの み)	この認証強度オブジェクトの設定が、このオブジェクトを継承したデ バイスグループで管理者によりオーバーライドされることを防止する には、このオプションを選択しますデフォルトでこのオプションはオ フになっており、管理者は、このオブジェクトを継承するデバイス グループの設定をオーバーライドできます。
認証方式	方式を選択します。
	 browser-challenge (ブラウザチャレンジ) – ファイアウォール はユーザー認証情報を透過的に取得します。このアクションを 選択する場合、選択するAuthentication Profile (認証プロファイ ル) で KerberosSSO を有効にする必要があります。 web-form (Web フォーム) – ユーザーを認証 するために、ファイアウォールは、configure Authentication Portal (認証ポータルの設 定)
	に指定された証明書プロファイル、または認証実施オブジェクト で選択された Authentication Profile(認証プロファイル)を使用 します。Authentication Profile(認証プロファイル)を選択した 場合、ファイアウォールはプロファイル内のすべての Kerberos SSO 設定を無視し、認証情報を入力するためのAuthentication Portal(認証ポータル)ページをユーザーに表示します。
	 no-captive-portal (キャノティノ ホータルなし) – ノァイア ウォールはユーザーを認証せずにセキュリティ ポリシーを確認し ます。
認証プロファイル	ユーザーの身元を確認するために使用するサービスを指定した認証プ ロファイルを選択します。
メッセージ	ユーザーのトラフィックが認証ルールをトリガーするときに、 ユーザーに表示される最初のチャレンジ認証でどのように応答す るかの指示を入力します。メッセージは、Authentication Portal Comfort Page(認証ポータル確認ページ)に表示されます。メッ セージを入力しない場合、デフォルトの Authentication Portal Comfort Page(認証ポータルコンフォートページ)が表示されます (Device(デバイス) > Response Pages(応答ページ)を参照)。

時

認証強度設定	の意味
	 ファイアウォールは、Authentication Profile(認証プロ ファイル)のAuthentication(認証)タブ(Device(デ バイス)>Authentication Profile(認証プロファイ ル)を参照)で定義された最初の認証チャレンジ (ファクター)に対してのみAuthentication Portal Comfort Page(認証ポータルコンフォートページ)を表 示します。多重認証(MFA)チャレンジをプロファイ ルのFactors(ファクター)タブで定義している場合、 ファイアウォールはMFA Login Page(MFA ログイン ページ)を表示します。

Objects > Decryption Profile [オブジェクト > 復号化プ ロファイル]

復号化プロファイルを使用すると、復号化のために指定した SSL および SSH トラフィックの特定の側面、および明示的に復号化から除外したトラフィックをブロックして制御できます。作成した復号化プロファイルは復号化ポリシーに追加できます。この復号化ポリシーに一致するすべてのトラフィックがプロファイル設定を基準に処理されるようになります。

ファイアウォールにはデフォルトの復号化プロファイルが設定されており、新規の復号化ポ リシーに自動的に含められます(デフォルトの復号化プロファイルを変更することはできませ ん)。Add[追加] をクリックして新規の復号化プロファイルを作成するか、既存のプロファイルを 選択し、それを Clone[コピー] または変更してください。

確認すべき情報	以下を参照
新しい復号化プロファイルを追加す る。	復号化プロファイルの一般設定
復号化されたトラフィックのポート ミラーリングを有効にする。	
復号化された SSL トラフィックのブ ロックと制御を行う。	復号化された SSL トラフィックを制御するための設 定
復号化から除外したトラフィック (医療サービスまたは金融サービ スとして分類されたトラフィックな ど)のブロックと制御を行う。	復号化されていないトラフィックを制御するための 設定
復号化された SSL トラフィックのブ ロックと制御を行う。	復号化された SSH トラフィックを制御するための設 定

復号化プロファイルの一般設定

次の表では、復号化プロファイルの一般設定について説明します。

復号化プロファイ ル – 一般設定	の意味
氏名	プロファイル名 (最大 31 文字) を入力します。この名前は、復号化ポリ シーを定義するときに復号化プロファイルのリストに表示されます。名 前の大文字と小文字は区別されます。また、一意の名前にする必要があ ります。文字、数字、スペース、ハイフン、およびアンダースコアのみ を使用してください。

復号化プロファイ ル – 一般設定	の意味
共有(Panorama のみ)	 以下に対してプロファイルを公開する場合は、このオプションを選択します。 multi-vsys ファイアウォールの各仮想システム (vsys)。この選択を解除すると、Objects[オブジェクト] タブで選択した Virtual System[仮想システム] のみに対してプロファイルが公開されます。 Panorama 上の各デバイス グループ。この選択を解除すると、Objects[オブジェクト] タブで選択した Device Group[デバイスグループ] のみに対してプロファイルが公開されます。
オーバーラ イドの無効化 (<mark>Panoramaのみ</mark>)	管理者が、このプロファイルを継承するデバイス グループのこの復号 化プロファイルの設定をオーバーライドすることを防ぐには、このオ プションを選択します。デフォルトでこのオプションはオフになってお り、管理者は、このプロファイルを継承するデバイス グループの設定を オーバーライドできます。
復号化ミラー イン ターフェイス (AWS の VM- Series ファ イアウォー ル、Azure、NSX エディショ ン、Citrix SDX を 除くすべてのモデ ルをサポートしま す。)	 復号化ポートミラーリングに使用する Interface[インターフェイス] を選択します。 復号化ポートミラーリングを有効にするには、復号化ポートミラーライセンスを取得およびインストールして、ファイアウォールを再起動する必要があります。
転送のみ (AWS の VM- Series ファ イアウォー ル、Azure、NSX エディショ ン、Citrix SDX を 除くすべてのモデ ルをサポートしま す。)	セキュリティポリシーの適用後のみ、復号化されたトラフィックをミ ラーリングする必要がある場合は、Forwarded Only[転送のみ] を選択し ます。このオプションを指定すると、ファイアウォール内を転送された トラフィックのみがミラーリングされます。このオプションは、復号化 されたトラフィックを他の脅威検出デバイス(DLP デバイスや他の侵入 防止システム(IPS)など)に転送する場合に役立ちます。この項目の 選択を解除すると(デフォルトではオフ)、ファイアウォールは、イン ターフェイスへのすべての復号化されたトラフィックをセキュリティポ リシー検索の前にミラーリングします。これにより、イベントの再生を 行い、脅威を生成するトラフィックやドロップアクションをトリガーす るトラフィックを分析することができます。

Settings to Control Decrypted Traffic(復号化されたトラフィックを制御する設定)

以下の表は、ファイアウォールがフォワード プロキシ復号化またはインバウンドインスペク ション(SSL Protocol Settings(SSL プロトコル設定)タブを含む)を使用して復号化したトラ フィックを制御する上で使用可能な設定を示しています。この設定を使用して、外部サーバー証 明書の状態、サポートされていない暗号スイートやプロトコルバージョンの使用、復号化を処 理するためのシステムリソースの可用性といった基準に基づいて TLS セッションを制限または ブロックできます。

SSL Decryption(SSL 復 の意味 号化)タブの設定

SSL FORWARD PROXY (SSL フォワード プロキシ) タブ

フォワード プロキシを使用して復号化された TLS トラフィックを制限またはブロックするための各種オプションを選択します。

Server Certificate Validation(サーバー証明書検証) – 復号化されたトラフィックのサーバー証明書を制御するオプションを選択できます。

期限切れ証明書のセッ ションをブロック	サーバー証明書の期限が切れている場合、TLS 接続を終了します。 これにより、ユーザーは期限切れの証明書を受け入れて TLS セッ ションを続行することができなくなります。
発行者が信頼されてい	サーバー証明書の発行者が信頼されていない場合、TLS 接続を終了
ないセッションをブ	します。
ロック	
証明書の状態が不明な	サーバーが証明書失効状態として「不明」を返す場合に、TLS セッ
セッションをブロック	ションを終了します。証明書失効状態は、証明書の信頼性が失効し
します	ているかどうかを示します。

SSL Decryption(SSL 復 号化)タブの設定	の意味
	証明書ステータスが不明であるセッションをブロックし、セキュリティを強化します。しかし、様々な理由で証明書ステータスが不明になることがあるため、これによってセキュリティが厳格になりすぎる可能性があります。未知の証明書ステータスをブロックすることでビジネスに必要なサイトが影響を受ける場合は、証明書ステータスが不明であるセッションをブロックしないでください。
サーバ証明書(SAN/ CN)とのSNIの不一致に 関するブロック・セッ ション	サーバ名表示 (SNI) がサーバ証明書と一致していないセッション を自動的に拒否します。明示プロキシまたは透過プロキシを設定す る場合は、このオプションを有効にすることを推奨します。詳細 については、「PAN-OS Networking Administrator`s Guide (PAN- OS ネットワーキング管理者ガイド)」の「Configure a Web Proxy (Webプロキシの設定)」を参照してください。
証明書の状態のチェッ クがタイムアウトした セッションをブロック します	ファイアウォールが証明書の状態サービスからの応答を待機するよう設定された時間内に証明書の状態を取得できない場合、TLS セッションを終了します。Certificate Status Timeout(証明書の有効期限)の値は、証明書プロファイルを作成または変更する際に設定できます(Device(デバイス) > Certificate Management(証明書の管理) > Certificate Profile(証明書プロファイル))。
	ステータスチェックがタイムアウトする際にセッションをブロック することは、強固なセキュリティと優れたユーザーエクスペリエン スのトレードオフになります。証明書無効化サーバーの応答が遅い 場合は、タイムアウト時のブロックによって有効な証明書を持つサ イトがブロックされるおそれがあります。有効な証明書をタイムア ウトさせることに不安を感じる場合は、証明書取り消しチェック (CRL)およびオンライン証明書ステータスプロトコル(OCSP) のタイムアウトの値を大きくすることができます。
証明書の延長を制限	動的なサーバー証明書で使用される証明書の拡張を、鍵の用途およ び拡張鍵の用途に制限します。
証明書のコモンネーム (CN) 値を SAN 拡張項 目に追加	firewall を有効にして、Forward Proxy 復号化の一部としてクライア ントに提示する偽装証明書に Subject Alternative Name (SAN) 拡張 を追加します。サーバー証明書に共通名 (CN) のみが含まれている 場合、firewall はサーバー証明書 CN に基づいて偽装証明書に SAN 拡張を追加します。

SSL Decryption(SSL 復 号化)タブの設定	の意味
	このオプションは、ブラウザが SAN を使用するためにサーバー証 明書を必要とし、CN に基づく証明書マッチングをサポートしなく なった場合に便利です。これにより、エンド・ユーザーが要求され た Web リソースに引き続きアクセスでき、サーバー証明書に CN のみが含まれている場合でも、firewall がセッションの暗号化解除 を続行できるようになります。 証明書の CN 値を SAN 拡張機能に追加して、要求さ れた Web リソースへのアクセスを確保します。
Unsupported Mode Chec ない TLS アプリケーショ	cks(サポートされていないモードのチェック) – サポートされてい ンを制御するオプションを選択します。
サポートされていない バージョンのセッショ ンをブロック	 PAN-OS が「client hello」メッセージをサポートしていない場合にセッションを終了します。PAN-OSは、SSLv3、TLSv1.0、TLSv1.1、TLSv1.2、およびTLSv1.3をサポートします。 サポートされていないバージョンのセッションを常にブロックし、脆弱なプロトコルを使用するサイトにアクセスできなくします。SSL Protocol Settings (SSL プロトコル設定)タブで最低 Protocol Version (プロトコルバージョン)を TLSv1.2 に設定し、脆弱なバージョンのプロトコルを使用するサイトをブロックします。ビジネス上の目的でアクセスする必要があるサイトが脆弱なプロトコルを使用している場合、その脆弱なプロトコルを許可する復号化プロファイルを別途作成し、脆弱なプロトコルを許可しなければならない対象のサイトだけに適用される復号化ポリシールールでそれを指定します。
暗号スイートがサポー トされていないセッ ションをブロック	 TLS ハンドシェークで暗号スイートが指定されていて、PAN-OS で サポートされていない場合、セッションを終了します。 サポートしない暗号スイートを使用するセッション をブロックします。SSL Protocol Settings (SSL プロト コル設定)タブで、許可する暗号スイート(暗号化ア ルゴリズム)を設定します。ユーザーが脆弱な暗号ス イートを使用するサイトに接続するのを許可しないで ください。

SSL Decryption(SSL 復 号化)タブの設定	の意味
クライアント認証を使 用するセッションをブ	フォワード プロキシ トラフィックのクライアント認証を使用する セッションを終了します。
	重要なアプリケーションで必要にならない限り、クラ イアント認証を伴うセッションをブロックします。そ のアプリケーションが必要な場合は、別の復号化プ ロファイルを作成し、クライアント認証が必要なトラ フィックにのみそれを適用しなければなりません。
Failure Checks(エラー・ に実行するアクションを	チェック) – 復号化の処理でシステム リソースを使用できない場合 選択します。
リソースを使用できな い場合にセッションを ブロック	復号化を処理するためのシステム リソースが使用できない場合、 セッションを終了します。
	リソースが利用できない場合にセッションをブロックするかどう かは、強固なセキュリティと優れたユーザーエクスペリエンスのト レードオフになります。リソースが利用できない場合にセッション をブロックしない場合、リソースが影響を受ける際に復号化したい トラフィックをファイアウォールが復号化できなくなります。しか し、リソースが利用できない場合にセッションをブロックすると、 普段はアクセスできるサイトが一時的にアクセスできなくなる可能 性があるため、ユーザーエクスペリエンスが影響を受けるおそれが あります。
HSM を使用できない 場合にセッションをブ ロック	証明書の署名にハードウェア セキュリティ モジュール (HSM) を使 用できない場合は、セッションを終了します。
	HSM を利用できない場合にセッションをブロックするかどうか は、HSM が利用できない場合に暗号化されたトラフィックを扱う 方法や秘密鍵の取得元など、組織のコンプライアンス規則によって 異なります。
Block downgrade on no resources (リソースが ない場合ダウングレー ドをブロックオス)	(TLSv1.2 にダウングレードする代わりに)TLSv1.3 ハンドシェイ クを処理するシステムリソースが利用できない場合は、セッション を終了します。
	「リソー人か利用でさない場合にセッションをフロックするかとうか」

^(a) リソースが利用できない場合にセッションをブロックするかどうか は、強固なセキュリティと優れたユーザーエクスペリエンスのト レードオフになります。TLSv1.3 リソースが利用できない場合、ハ ンドシェイクの TLSv1.2 へのダウングレードをブロックすると、 ファイアウォールはセッションをドロップします。ハンドシェイク のダウングレードをブロックしない場合、TLSv1.3 ハンドシェイク

SSL Decryption(SSL 復 号化)タブの設定	の意味
	でリソースが利用できない場合、ファイアウォールは TLSv1.2 にダ ウングレードします。
クライアント拡張	
ストリップ ALPN	ファイアウォールはデフォルトで HTTP/2 トラフィックを処 理・検査します。しかし、ファイアウォールがStrip ALPN (ALPN をストリップ)するように指定することで、HTTP/2 を無効化 できます。このオプションを選択すると、ファイアウォールは ALPN (Application-Layer Protocol Negotiation) TLS 拡張に含まれ るすべての値を削除します。 HTTP/2 接続を保護するために ALPN を使用するため、この TLS 拡 張用に指定されている値がない場合、ファイアウォールは HTTP/2
	トラフィックを HTTP/1.1 にダウングレードするか、それを未知の TCP トラフィックに分類化します。

 サポートされていないモードおよび失敗モードについては、セッション情報が 12時間キャッシュされます。このため、同じホストとサーバーペア間の以降の セッションは復号化されません。代わりにこれらのセッションをブロックする 場合は、オプションを有効にしてください。

SSL INBOUND INSPECTION (SSL インバウンド インスペクション) タブ

インバウンドインスペクションを使用して復号化されたトラフィックを制限またはブロック するための各種オプションを選択します。

Unsupported Mode Checks(サポートされていないモードのチェック) – サポートされていないモードが TLS トラフィックで検出された場合にセッションを制御するオプションを選択します。

サポートされていない	PAN-OS が「client hello」メッセージをサポートし
バージョンのセッショ	ていない場合にセッションを終了します。PAN-OS
ンをブロック	は、SSLv3、TLSv1.0、TLSv1.1、TLSv1.2、および TLSv1.3 をサ
	ポートします。

SSL Decryption(SSL 復 号化)タブの設定	の意味
	 サポートされていないバージョンのセッションを常に ブロックし、脆弱なプロトコルを使用するサイトにア クセスできなくします。SSL Protocol Settings (SSL プ ロトコル設定)タブで最低 Protocol Version (プロトコル バージョン)を TLSv1.2 に設定し、脆弱なバージョン のプロトコルを使用するサイトをブロックします。ビ ジネス上の目的でアクセスする必要があるサイトが脆 弱なプロトコルを使用している場合、その脆弱なプロ トコルを許可する復号化プロファイルを別途作成し、 脆弱なプロトコルを許可しなければならない対象のサ イトだけに適用される復号化ポリシー ルールでそれ を指定します。
暗号スイートがサポー トされていないセッ ションをブロック	 暗号スイートが PAN-OS でサポートされていない場合、セッション を終了します。 サポートしない暗号スイートを使用するセッション をブロックします。SSL Protocol Settings (SSL プロト コル設定)タブで、許可する暗号スイート(暗号化ア ルゴリズム)を設定します。ユーザーが脆弱な暗号ス イートを使用するサイトに接続するのを許可しないで ください。
Failure Checks(エラー・ ションを選択します。	チェック) – システム リソースを使用できない場合に実行するアク
リソースを使用できな い場合にセッションを ブロック	復号化を処理するためのシステム リソースが使用できない場合、 セッションを終了します。 リソースが利用できない場合にセッションをブロックするかどう かは、強固なセキュリティと優れたユーザーエクスペリエンスのト レードオフになります。リソースが利用できない場合にセッション をブロックしない場合、リソースが影響を受ける際に復号化したい トラフィックをファイアウォールが復号化できなくなります。しか し、リソースが利用できない場合にセッションをブロックすると、 普段はアクセスできるサイトが一時的にアクセスできなくなる可能 性があるため、ユーザーエクスペリエンスが影響を受けるおそれが あります。
HSM を使用できない 場合にセッションをブ ロック	セッション キーの復号化にハードウェア セキュリティ モジュール (HSM) を使用できない場合は、セッションを終了します。 HSM を利用できない場合にセッションをブロックするかどうか は、HSM が利用できない場合に暗号化されたトラフィックを扱う

SSL Decryption(SSL 復 号化)タブの設定	の意味
	方法や秘密鍵の取得元など、組織のコンプライアンス規則によって 異なります。
Block downgrade on no resources(リソースが ない場合ダウングレー	(TLSv1.2 にダウングレードする代わりに)TLSv1.3 ハンドシェイ クを処理するシステムリソースが利用できない場合は、セッション を終了します。
トをノロックする)	リソースが利用できない場合にセッションをブロックするかどうか は、強固なセキュリティと優れたユーザーエクスペリエンスのト レードオフになります。TLSv1.3 リソースが利用できない場合、ハ ンドシェイクの TLSv1.2 へのダウングレードをブロックすると、 ファイアウォールはセッションをドロップします。ハンドシェイク のダウングレードをブロックしない場合、TLSv1.3 ハンドシェイク でリソースが利用できない場合、ファイアウォールは TLSv1.2 にダ ウングレードします。

SSL PROTOCOL SETTINGS (SSL プロトコル設定) タブ

TLS セッション トラフィックのプロトコル バージョンと暗号スイートを適用する以下の各設 定を選択します。

プロトコル バージョン	TLS セッションでの最小/最大プロトコル バージョンの使用を強制 します。
最小バージョン	 TLS 接続の確立に使用できる最小プロトコルバージョンを設定します。 Min Version (最低バージョン)を TLSv1.2 に設定して最大限のセキュリティを提供します。サイトが TLSv1.2 をサポートしているかどうか確認し、本当に正当なビジネス上の目的がサイトにあるかどうか判断します。TLSv1.2 をサポートしていないながらアクセスする必要があるサイトについては、サイトがサポートしている最も強固なプロトコルバージョンを指定した復号化プロファイルを別途作成し、脆弱なバージョンの使用を必要なサイトと必要な送信元(ゾーン、アドレス、ユーザー)のみに制限する復号化ポリシールールにそれを適用します。
最大バージョン	TLS 接続の確立に使用できる最大プロトコル バージョンを設定しま す。最大 オプションを選択して、最大バージョンを指定しない場合 もあります。その場合、選択した最小バージョンと等しいかそれ以 降のバージョンがサポートされます。

SSL Decryption(SSL 復 号化)タブの設定	の意味
	 Max Version (最大バージョン)をMax (最大)に設定し、 プロトコルが改善されたらファイアウォールが自動的 にそれをサポートできるようにします。 ただし、復号化ポリシーがモバイル アプリケーショ ンをサポートしており、その多くがピンニング証明 書を使用している場合は、Max Version (最大バージョ ン)を TLSv1.2 に設定します。TLS v1.3 は、以前の TLS バージョンでは暗号化されていなかった証明書情報を 暗号化するため、ファイアウォールは証明書情報に 基づいて復号化の除外を自動的に追加できません。 これは、一部のモバイル アプリケーションに影響を 与えます。したがって、TLSv1.3を有効にすると、 そのトラフィックに対して復号しないポリシーを作 成しない限り、ファイアウォールが一部のモバイル アプリケーショントラフィックをドロップする可能 性があります。ビジネスに使用するモバイル アプリ ケーションがわかっている場合は、それらのアプリ ケーション用に個別の復号化ポリシーとプロファイ ルを作成して、他のすべてのトラフィックに対して TLSv1.3を有効にできるようにすることを検討してく ださい。
キー交換アルゴリズム	TLS セッションにおいて、選択したキー交換アルゴリズムの使用を 強制します。 3 つのアルゴリズム(RSA、DHE、ECDHE)すべてがデフォルトで 有効化されています。DHE(Diffie-Hellman)およびECDHE(楕円 曲線 Diffie-Hellman)は、転送プロキシあるいはインバウンドイン スペクション復号化用のPerfect Forward Secrecy(PFS)を可能に します。
暗号化アルゴリズム	TLS セッションでの選択した暗号化アルゴリズムの使用を適用します。

SSL Decryption(SSL 復 号化)タブの設定	の意味
	脆弱な3DESやRC4暗号化アルゴリズムはサポートしないでください。(TLSv1.2以降のバージョンを最低 プロトコルバージョンとして使用する際、ファイア ウォールは自動的にこれら2つのアルゴリズムをブ ロックします)例外を設けて脆弱なプロトコルバー ジョンをサポートしなければならない場合は、復号化 プロファイルの3DESおよびRC4のチェックを外します。3DESあるいはRC4暗号化アルゴリズムを使用するサイトにアクセスしなければならないビジネス上の目的がある場合は、復号化プロファイルを別途作成してそれを対象のサイト用の復号化ポリシールールにのみ適用します。
認証アルゴリズム	 TLS セッションでの選択した認証アルゴリズムの使用を適用します。 古く脆弱な MD5 アルゴリズムをグロックします(デフォルト設定ではブロックされます)。SHA1 認証を使用する必要なサイトがない場合は、SHA1 をブロックします。SHA1 を使用するサイトにアクセスしなければならないビジネス上の目的がある場合は、復号化プロファイルを別途作成してそれを対象のサイト用の復号化ポリシールールにのみ適用します。

復号化されていないトラフィックを制御するための設定

No Decryption(復号化なし)タブを使用すると、復号化なしアクション(Policies(ポリシー) > Decryption(復号化) > Action(アクション))が設定された復号化ポリシーに一致するトラ フィックをブロックする設定を有効にできます。以下のオプションを使用すると、セッションの サーバー証明書を制御できます。ただし、ファイアウォールはセッショントラフィックを復号 化および検査しません。

No Decryption (復号化 なし)タブの設定	の意味
期限切れ証明書のセッ ションをブロック	サーバー証明書の期限が切れている場合、SSL 接続を終了します。 これにより、ユーザーは期限切れの証明書を受け入れて SSL セッ ションを続行することができなくなります。
	証明書が失効したセッションをブロックし、安全でな いおそれのあるサイトにアクセスできなくします。

No Decryption (復号化 なし)タブの設定	の意味
発行者が信頼されてい ないセッションをブ ロック	サーバー証明書の発行者が信頼されていない場合、SSL 接続を終了 します。
	発行者を信頼できない場合は中間者攻撃、リプレイ攻 撃、その他の攻撃が示唆されるため、発行者を信頼で きないセッションをブロックします。

復号化された SSH トラフィックを制御するための設定

以下の表に、復号化されたインバウンドおよびアウトバウンド SSH トラフィックを制御するための設定を説明します。これらの設定を使用すると、未サポートのアルゴリズムの使用、SSH エラーの検出、SSH プロキシ復号化を処理するためのリソースの可用性など、さまざまな基準に基づいて、SSH トンネル トラフィックを制限またはブロックできます。

SSH Proxy (SSH プ の意味 ロキシ**)** タブの設定

Unsupported Mode Checks(サポートされていないモードのチェック) – サポートされてい ないモードが SSH トラフィックで検出された場合にセッションを制御するこれらのオプショ ンを使用します。サポートされている SSH バージョンは、SSH バージョン 2 です。

サポートされてい ないバージョンの セッションをブ	「client hello」メッセージが PAN-OS でサポートされていない場合、 セッションを終了します。
	・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・
アルゴリズムがサ ポートされていな いセッションをブ ロック	クライアントまたはサーバーで指定されたアルゴリズムが PAN-OS でサ ポートされていない場合、セッションを終了します。

SSH Proxy (SSH プ ロキシ) タブの設定	の意味
	 ・サポートされていないアルゴリズムを使用するセッション を常にブロックし、脆弱なアルゴリズムを使用するサイト にアクセスできなくします。
Failure Checks(エ システム リソースを	ラー チェック) – SSH アプリケーション エラーが発生した場合、および を使用できない場合に実行するアクションを選択します。

SSH エラー時に セッションをブ ロック	SSH エラーが発生した場合、セッションを終了します。
リソースを使用で きない場合にセッ ションをブロック	復号化を処理するためのシステムリソースが使用できない場合、セッ ションを終了します。 リソースが利用できない場合にセッションをブロックするかどうかは、 強固なセキュリティと優れたユーザーエクスペリエンスのトレードオフ になります。リソースが利用できない場合にセッションをブロックしな い場合、リソースが影響を受ける際に復号化したいトラフィックをファ イアウォールが復号化できなくなります。しかし、リソースが利用でき ない場合にセッションをブロックすると、普段はアクセスできるサイト が一時的にアクセスできなくなる可能性があるため、ユーザーエクスペ リエンスが影響を受けるおそれがあります。

オブジェクト>パケット ブローカ プロファイル

Packet Broker プロファイルは、ファイアウォールが、追加のセキュリティインスペクション と適用を提供するインラインのサードパーティ製セキュリティアプライアンスのセットである セキュリティチェーンにトラフィックを転送する方法を定義します。このプロファイルは、セ キュリティチェーンへの接続に使用されるファイアウォールインターフェイス、セキュリティ チェーンの種類(ルーティングレイヤ3またはレイヤ1透過ブリッジ)、レイヤ3セキュリティ チェーン内の最初と最後のアプライアンス、複数のレイヤ3チェーン間のセッション配信(ロー ドバランシング)、およびパスまたはHTTP 遅延の障害に対するヘルスモニタリングとアクショ ンを定義します。パケットブローカプロファイルをパケットブローカポリシールールにア タッチします。ポリシールールはセキュリティチェーンに転送するトラフィックを定義し、プ ロファイルはそのトラフィックを転送する方法を定義します。

パケット ブローカ プロファイルを設定する前に、ファイアウォール上のレイヤ3インターフェ イスを2つ以上専用にして、トラフィックをセキュリティチェーンに転送する必要がありま す。

- **1.** Network (ネットワーク) > Interfaces (インターフェイス) > Ethernet (イーサネット) を選択します。
- 2. パケット ブローカ転送に使用するインターフェイスを選択します。
- 3. インターフェイスタイプをレイヤ3に設定します。
- 4. advanced > Other Info を選択します。
- 5. ネットワーク パケット ブローカー を選択して、インターフェイスを有効にします。
- 6. 別のイーサネット インターフェイスで、これらの手順を繰り返します。複数の専用接続を(た とえば、複数のセキュリティ チェーンに接続する場合)、専用接続ごとにイーサネット イン ターフェイスのペアを設定します。

パケット ブローカ プロ ファイルの設定	の意味	
氏名	プロファイルに分かりやすい名前を付けます。	
の意味	必要に応じて、プロファイルの設定または目的を記述します。	
General [全般] タブ		
Security Chain Type セ キュリティ チェーン タイプ	 ファイアウォールが復号化されたトラフィックを転送するセキュリティチェーンのタイプを選択します。 Routed (Layer 3) (ルート化 (レイヤー3)): このタイプのセキュリティチェーンのデバイスは、レイヤ3インターフェイスを使用してセキュリティチェーンネットワークに接続します。 各インターフェイスには、IPアドレスとサブネットマスクが割り当てられている必要があります。スタティックルートを使用してセキュリティチェーンデバイスを構成するか、動的ルー 	

パケット ブローカ プロ ファイルの設定	の意味
	ティングを使用して、受信および送信トラフィックをセキュリ ティ チェーン内の次のデバイスに送信してからファイアウォー ルに戻します。
	 Transparent Bridge(トランスペアレント・ブリッジ):トラン スペアレントブリッジセキュリティチェーンネットワークで は、すべてのセキュリティチェーンデバイスに、セキュリティ チェーンネットワークに接続された2つのトランスペアレン トブリッジモードインターフェイスがあります。透過ブリッ ジインターフェイスには、IPアドレス、サブネットマスク、デ フォルトゲートウェイ、またはローカルルーティングテーブル がありません。セキュリティチェーンアプライアンスは、1つ のインターフェイスでトラフィックを受信し、トラフィックを 分析してセキュリティを適用し、トラフィックは次のセキュリ ティチェーンデバイスにもう一方のインターフェイスを送信し ます。
IPv6を有効にする	(トランスペアレント ブリッジ モードのみ)IPv6 トラフィック転送 を有効にします。
フロー方向	トラフィックが1つのファイアウォールインターフェイスから セキュリティチェーンに入り、もう一方のファイアウォールイ ンターフェイスにセキュリティを終了するか、またはトラフィッ クが両方のファイアウォールインターフェイスからセキュリティ チェーンを出入りできるかを選択します。
	 双方向: ファイアウォールはInterface #1 を介してすべてのトラ フィックをセキュリティ チェーンに転送し、Interface #2 のセ キュリティ チェーンからトラフィックを受信します。
	両方のインターフェイスが同じゾーンになければ なりません。
	 双方向: ファイアウォールは Interface #1 を介してクライアント からサーバーへのトラフィックをセキュリティ チェーンに転送 し、Interface #2 のセキュリティ チェーンからトラフィックを受 信します。
	ファイアウォールは、サーバーからクライアントへのトラ フィックを Interface #2 を介してセキュリティ チェーンに転送 し、Interface #1 のセキュリティ チェーンからトラフィックを受 信します。
	選択するフローの方向は、セキュリティ チェーン内のアプライアン スの種類によって異なります。たとえば、セッションの両側を検査

パケット ブローカ プロ ファイルの設定	の意味
	できるステートレス デバイスがセキュリティ チェーンに含まれて いる場合、単方向フローを選択できます。
インターフェイス #1	ファイアウォールがセキュリティ チェーンとのトラフィックの転
インターフェイス #2	ローカ インターフェイス。このヘルプ トピックの冒頭で説明さ れているように、各インターフェイスをネットワーク パケット ブ ローカ インターフェイスとして設定する必要があります。

セキュリティ チェーン タブ

ネットワーク パケット ブローカ ファイアウォール インターフェイスの1組のレイヤ3セ キュリティ チェーン (ロード バランシングまたは冗長性の場合)を1つまたは複数設定しま す。Routed (レイヤ3) セキュリティ チェーン タイプの場合、トラフィックを転送する場所を 指定するために少なくとも1つのセキュリティ チェーンを構成する必要があります。複数の セキュリティ チェーンの場合、スイッチまたは他のデバイスはファイアウォールとチェーン 間のルーティングを処理する必要があります。

_	
0	
=	
 =	
	•

このタブのオプションは、レイヤ3(ルーティング済み) セキュリティ チェーン でのみ使用できます。

Enable [有効化]	セキュリティチェーンを有効にします。
氏名	セキュリティ チェーンに分かりやすい名前を付けます。
最初のデバイス	セキュリティ チェーンの最初と最後のデバイスの IPv4 アドレスを 入力するか、または新しいアドレス オブジェクトを定義して、デバ イスを簡単に参照します。
最後のデバイス	
Session Distribution Method セッション配 信方式	複数の Routed (レイヤ 3) セキュリティ チェーンに転送する場合 は、ファイアウォールが複数のセキュリティ チェーン間でセッショ ンを分散するために使用する方法を選択します。
	• IP Modulo–firewall は送信元 IP アドレスと宛先 IP アドレスの IP モジュロハッシュに基づいてセッションを割り当てます。
	 IP ハッシューfirewall は、送信元と宛先の IP アドレスとポート番号の IP ハッシュに基づいてセッションを割り当てます。
	 Round Robin-firewall はセキュリティ チェーン間でセッション を均等に割り当てます。
	 Lowest Latency – firewall は、最小の待機時間でより多くのセッションをセキュリティチェーンに割り当てます。このメソッドを期待どおりに機能させるには、Health Monitor タブで Latency Monitoring と HTTP Monitoring も有効にする必要が

パケット ブローカ プロ ファイルの設定	の意味
	あります。
ヘルス モニタ タブ	
ヘルスチェックに失敗 した場合	ヘルスチェック (Path 監視、HTTP モニタリング、または HTTP モ ニタリング遅延) を有効にした場合、チェーン (または複数のチェー ンがある場合はすべてのチェーン) が失敗した場合の動作も決定し ます。複数のチェーンがあり、1 つ以上のチェーンがヘルスチェッ クに失敗しても少なくとも 1 つのチェーンが正常である場合、ファ イアウォールは Session 分散方法 に基づいて残りのチェーンにト ラフィックを分散します。ファイアウォールネットワークパケッ トブローカーのペアに関連付けられたすべてのチェーンがインター フェースしている場合は、次のことができます。
	 バイパスセキュリティチェーン:ファイアウォールは、障害が 発生したチェーンではなく、宛先にトラフィックを転送しま す。ファイアウォールは、設定済みのセキュリティプロファイ ルと保護をトラフィックに適用します。
	 ブロック セッション:ファイアウォールはセッションをブロック します。
ヘルスチェック失敗条 件	複数のヘルスチェックを設定する場合(チェーン上の3つのヘルス チェックすべてを設定できます)、ファイアウォールで障害を定義す る方法を構成します。
	 OR Condition- 選択したヘルスチェックが失敗すると、稼働状態 チェックの失敗 アクションが発生します。
	 AND 条件: 選択したヘルスチェックがすべて失敗すると、ヘルス チェックの失敗 アクションが発生します。
パス モニタリング	パス、HTTP 待ち時間、または HTTP 監視を有効にするか、3つの
遅延モニタリング	 ¬ ハルステェックの組み合わせを使用して、セキュリティ チェーンで 障害が発生したタイミングを特定し、障害が発生したタイミングを − 決定するメトリックを構成します。
HTTP 監視	 パス監視–デバイスの接続性を確認します。ping カウン ト、ping 間隔 (秒)、および回復の保持時間を秒単位で設定します。
	 HTTP 監視-デバイスの可用性と応答時間をチェックします。HTTP カウントと HTTP 間隔を秒単位で設定します。
	• HTTP 監視遅延–デバイスの処理速度と効率をチェックします。 最大待機時間をミリ秒単位で設定し、待機時間を秒単位で設定 し、ログの待機時間を超えるログ待機時間を設定します。HTTP 監視待ち時間を選択すると、HTTP 監視 が自動的に選択されま

パケット ブローカ プロ ファイルの設定	の意味	
	す。遅延監視を有効にするには、両方を選択する必要がありま す。	

Objects > SD-WAN Link Management [オブジェクト > SD-WAN リンク管理]

SD-WAN ポリシー ルールで指定されたアプリケーションとサービスのセットに適用するプロファイルを作成します。各プロファイル タイプは、SD-WAN リンク管理のさまざまな側面を制御します。

- Objects > SD-WAN Link Management > Path Quality Profile [オブジェクト > SD-WAN リンク 管理 > パス品質プロファイル]
- Objects > SD-WAN Link Management > SaaS Quality Profile [オブジェクト > SD-WAN リンク 管理 > SaaS 品質プロファイル]
- Objects > SD-WAN Link Management > Traffic Distribution Profile [オブジェクト > SD-WAN リンク管理 > トラフィック分散プロファイル]
- Objects > SD-WAN Link Management > Error Correction Profile [オブジェクト > SD-WAN リ ンク管理 > エラー修正プロファイル]

Objects > SD-WAN Link Management > Path Quality Profile [オブ ジェクト > SD-WAN リンク管理 > パス品質プロファイル]

SD-WAN を使用すると、一意のネットワーク品質要件を持つアプリケーション、アプリケー ションフィルタ、アプリケーション グループ、サービス、サービス オブジェクト、およびサー ビス グループ オブジェクトの各セットのパス品質プロファイルを作成し、SD-WAN ポリシー ルールでそのプロファイルを参照できます。プロファイルでは、レイテンシー、ジッター、パ ケットロスの3つのパラメータに最大しきい値を設定します。SD-WAN リンクがいずれかのし きい値を超えると、ファイアウォールは、このプロファイルを適用した SD-WAN ルールに一致 するパケットに新しい最適パスを選択します。

各パス品質パラメータの感度設定により、プロファイルが適用されるアプリケーションにとって より重要な(推奨される)パラメータをファイアウォールに示すことができます。ファイアウォー ルは、設定が中または低のパラメータよりも、設定が高のパラメータを重視します。例えば、一 部のアプリケーションはジッターやレイテンシーよりもパケット損失の影響を受けやすいため、 ファイアウォールは最初にパケット損失を検査します。

レイテンシー、ジッター、およびパケット損失の感度設定をデフォルト設定(中)のままにする か、3つのパラメータすべてを同じ設定にした場合、プロファイルの優先順位はパケット損失、 レイテンシー、ジッターとなります。

デフォルトでは、ファイアウォールは200 ミリ秒毎に 最後3つの測定値の平均を取り、レイテンシーおよびジッターを測定し、スライディング ウィンドウ方式でパス品質を測定します。SD-WAN インターフェイス プロファイルを設定するときに、積極的または緩和的なパス モニタリングを選択することにより、この動作を変更できます。

	パス品質プロファイルの設定
氏名	パス品質プロファイルのName (名前) を任意の組み合わせで、最大 31 文字の英数字で、アンダースコア、ハイフン、スペース、ピリオ ドを使用して入力します。
共有(Panorama の み)	選択すると、Panorama 上のすべてのデバイス グループと、構成を プッシュするマルチ vsys ハブまたはブランチ上のすべての仮想シス テムでパス品質プロファイルを使用できるようになります。
オーバーライドの無効 化(Panoramaのみ)	選択すると、管理者は、プロファイルを継承するデバイス グループ でこのパス品質プロファイルの設定を上書きできなくなります。([共 有] が選択されている場合、[上書きを無効にする] は使用できませ ん)。
レイテンシー (ミリ秒)	Threshold (しきい値)–パケットがファイアウォールを出て SD-WAN トンネルの反対側の端に到着し、しきい値を超過する前にファイ アウォールに戻るまでの許容ミリ秒数を入力します (範囲は 10 ~ 2,000、デフォルトは 100)。
	Sensitivity (感度) –high(高)、medium(中)、またはlow(低)を 選択します(デフォルトはmedium(中))。
ジッター (ミリ秒)	Threshold (しきい値) –ミリ秒数を入力します(範囲は 10~1,000、 デフォルトは 100)。
	Sensitivity (感度) –high(高)、medium(中)、またはlow(低)を 選択します(デフォルトはmedium(中))。
Packet Loss (パケット 損失率) (%)	Threshold (しきい値)–しきい値を超えるまでのリンクのパケット損 失率を入力します (範囲は 1 ~ 100.0、デフォルトは 1)。
	Sensitivity (感度)–パケット損失の感度設定は効果を持たないため、 デフォルト設定はそのまま(medium(中))にします。

Objects > SD-WAN Link Management > SaaS Quality Profile [オブ ジェクト > SD-WAN リンク管理 > SaaS 品質プロファイル]

SD-WAN を使用すると、Software-as-a-Service(SaaS)品質プロファイルを作成し、ハブまた はブランチ ファイアウォールとサーバー側 SaaS アプリケーション間のパスの健全性の質を測 定し、パスの健全性の質が低下した場合の SaaS アプリケーションの信頼性とスワップ パスの 正確なモニタリングが可能となります。これにより、ファイアウォールは、別のDirect Internet Access(DIA、ダイレクト インターネット アクセス)リンクにフェイルオーバーするタイミン グを正確に決定することができます。 SaaS 品質プロファイルを使用すると、アプリケーション アクティビティを監視するアダプティ ブ ラーニング アルゴリズムを利用して、あるいはアプリケーションの IPアドレス、FQDN、ま たは URL を使用し、SaaS アプリケーションを指定して、監視する SaaS アプリケーションを指 定できます。

	SaaS Quality Profile Settings(SaaS 品質プロファイルの設定)
氏名	英数字、アンダースコア、ハイフン、スペース、およびピリオドを 使用して、パス品質プロファイル名を入力します。
共有(Panorama の み)	チェックをオン(有効化)にすると、SaaS 品質プロファイルをすべ てのデバイスグループ間で共有します。
Disable Override(オーバー ライドの無効化 (Panoramaのみ)	管理対象ファイアウォールでローカルに SaaS 品質プロファイル設定 を上書きする機能を無効にするには、チェックをオン(有効化)に します。

SaaS Monitoring Mode SaaS 管理モード

Adaptive 適応学習	SaaS アプリケーション セッション アクティビティは、送受信アク ティビティに関して監視され、パスヘルスステータスは、SD-WAN インターフェースで追加のヘルス確認を実施することなく自動的に 取得されます。このオプションはデフォルトで選択されています。
Static IP Address 静的 IP アドレス	IP Address/Object(IPアドレスまたはオブジェクト)–アプリケー ションの IPアドレスを使用して監視する SaaS アプリケーションを 指定します。
	 IP address (IP アドレス) – SaaS アプリケーションの IPアドレ スです。
	 Probe Interval (Sec) (プローブ間隔、秒単位) –ファイアウォー ルがファイアウォールと SaaS アプリケーション間のパスの質の 状態をプローブする間隔を秒単位で指定します。デフォルトは 3 秒です。
	最大4個のスタティック IPアドレスがサポートされます。
	FQDN-アプリケーションの完全修飾ドメイン名(FQDN)を使用し て監視する SaaS アプリケーションを指定します。
	 FQDN – SaaS アプリケーションの FQDN です。FQDN を指定するには、FQDN の address object (アドレスオブジェクト)を設定する必要があります。
	SaaS アプリケーションを正常に監視するには、SaaS アプリケー ションの FQDN が解決可能でなければなりません。

	SaaS Quality Profile Settings(SaaS 品質プロファイルの設定)
	 Probe Interval (Sec) (プローブ間隔、秒単位) –ファイアウォー ルがブランチのファイアウォールと SaaS アプリケーション間の パスの質の状態をプローブする間隔を秒単位で指定します。デ フォルトは3秒です。
HTTP/HTTPS	HTTP または HTTPS URL を使用して監視する SaaS アプリケーショ ンを指定します。
	 Monitored URL(監視対象 URL) – SaaS アプリケーションの HTTP または HTTPS URL。
	 Probe Interval (sec) (プローブ間隔、秒単位) –ファイアウォール がファイアウォールと SaaS アプリケーション間のパスの質の状態をプローブする間隔を秒単位で指定します。デフォルトは3秒です。

Objects > SD-WAN Link Management > Traffic Distribution Profile [オブジェクト > SD-WAN リンク管理 > トラフィック分散 プロファイル]

このトラフィック分散プロファイルでは、セッションの分散と、パスの品質が低下したときに より適切なパスにフェイルオーバーするためにファイアウォールが使用する方法を選択します。 ファイアウォールが SD-WAN トラフィックを転送するリンクを決定する際に考慮するリンク タ グを追加します。作成した各 SD-WAN ポリシー ルールにトラフィック分散プロファイルを適用 します。

	トラフィック分散プロファイル
氏名	最大 31 の英数字、ハイフン、スペース、アンダースコア、ピリオドを使用 して、トラフィック分散プロファイル名を入力します。
共有	このトラフィック分散プロファイルをすべてのデバイス グループ(ハブとブ ランチの両方)で使用する場合は、[共有(Shared (共有))] を選択します。
Best Available Path (利用でき る最適なパス)	コストを考慮せず、アプリケーションが拠点から外への任意のパスを使用 できるようにするには Best Available Path (利用可能な最適なパス)を選択 します。ファイアウォールはトラフィックを分散し、パス品質メトリック に基づいてリスト内のすべてのリンク タグに属するリンクの中からリンク にフェイルオーバーすることで、ユーザーに最高のアプリケーション エク スペリエンスを提供します。
Top Down Priority (トップ ダウン優先)	最後の手段としてのみ、またはバックアップ リンクとしてのみ使用した いコストの高いリンクや容量の少ないリンクがある場合は、Top Down Priority (トップダウン優先) 方式を選択し、それらのリンクを含むタグをこ

	トラフィック分散プロファイル
	のプロファイルのLink Tags (リンクタグ)のリストの最後に配置します。 ファイアウォールは、まずリストの先頭のリンクタグを使用してセッショ ンのトラフィックをロードするリンクおよびフェイルオーバーするリン クを決定します。トップリンクタグのどのリンクも適していない場合、 ファイアウォールはリストの2番目のリンクタグからリンクを選択しま す。2番目のリンクタグ内のどのリンクも修飾されていない場合、ファイ アウォールが最後のリンクタグで修飾されたリンクを見つけるまで、この プロセスが必要に応じて続行されます。関連付けられているすべてのリン クが過負荷であり、品質のしきい値を満たすリンクがない場合、ファイア ウォールは Best Available Path (最適なパス)方法を使用して、トラフィッ クを転送するリンクを選択します。 アプリケーションのジッター、レイテンシー、パケットロスが設定された しきい値を超えると、ファイアウォールはリンクタグのトップダウンリス トの先頭からフェイルオーバー先のリンクを探します。
Weighted Session Distribution (重 み付きセッショ ン分散)	ISP および WAN リンクに手動で (ルールに一致する) トラフィックをロードし、電圧低下時にフェイルオーバーを必要としない場合は Weighted Session Distribution (重み付きセッション分散) を選択します。1つのタグでグループ化されたインターフェースが取得する新規セッションのスタティックな割合を適用する際に、リンクロードを手動で指定します。大規模ブランチのバックアップや大規模なファイルの転送など、遅延の影響を受けず、多くのリンク帯域幅容量を必要とするアプリケーションには、この方法を選択します。ただし、リンクで電圧低下が発生した場合、ファイアウォールは一致するトラフィックを別のリンクにリダイレクトしないことに留意します。
Link Tags (リン ク タグ)	このプロファイルのために選択したリンク選択プロセス中にファイア ウォールに考慮させる リンク タグ を追加します。Top Down Priority (トッ プダウン優先) 方式を選択する場合、タグの順序が重要です。Move Up (上 に移動) または Move Down (下に移動) でタグの順序を変更できます。
重み	重み付きセッション分散方式を選択する場合は、追加した各リンク タグご とに割合を入力します。割合の合計は 100% でなければなりません。

Objects > SD-WAN Link Management > Error Correction Profile [オブジェクト > SD-WAN リンク管理 > エラー修正プロファイル]

音声、VoIP、ビデオ会議等、パケットの損失や破損に影響を受けやすいアプリケーション が SD-WAN トラフィックに含まれている場合、エラー訂正の手段として、Forward Error Correction (FEC、転送エラー修正)またはパケット複製のいずれかを適用することができま す。FEC を使用すると、受信ファイアウォール(デコーダ)は、エンコーダがアプリケーショ ン フローに埋め込むパリティ ビットを使用することにより、損失したパケットや破損したパ ケットを回復することができます。エラー訂正の代替方法であるパケット複製では、アプリケー ション セッションが 1 つのトンネルから 2 番目のトンネルに複製されます。どちらの方法で も、追加の帯域幅および CPU オーバーヘッドが必要となります。従って、FEC またはパケット 複製は、この方法を使用することによるメリットがあるアプリケーションにのみ適用します。こ れらの方法のいずれかを使用するには、Error Correction Profile(エラーの修正プロファイル) を作成し、特定のアプリケーションの SD-WAN ポリシー ルールで参照します。

(また、ファイアウォールがエラー修正で選択可能なインターフェースを、SD-WAN Interface Profile(SD-WAN インターフェース プロファイル)で、インターフェースが Eligible for Error Correction Profile interface selection(エラーの修正プロファイル インターフェース選択に適格)を明らかにして指定する必要があります。)

	Error Correction Profile(エラーの修正プロファイル)
名前	最大 31 文字の英数字を使用して、エラーの修正プロファイルの 判別しやすい名称を追加します。
共有	選択すると、Panorama のすべてのデバイス グループと、設定を プッシュするマルチvsys ハブまたはブランチ上のすべてのvirtual system (仮想システム - vsys) でエラーの修正プロファイルを使 用できるようになります。
オーバーライドを無効に する	管理者が、このプロファイルを継承するデバイス グループのこ のエラーの修正プロファイルの設定をオーバーライドすること を防ぐ場合に選択します。(Shared(共有)が選択されている 場合、Disable override(オーバーライドの無効化)は利用でき ません。)
Activation Threshold (Packet Loss %)(アク ティベーションのしきい 値、パケット損失率)	パケット損失がこの割合を超えると、Error Correction Profile(エラーの修正プロファイル)が適用される SD-WAN ポ リシールールで設定されたアプリケーションに対して FEC また はパケット複製がアクティブ化されます。範囲は 1 ~ 99、デ フォルトは 2 です。
Forward Error Correction / Packet Duplication(転送エラー の修正 / パケットの複 製)	転送エラーの修正(FEC)を採用するか、パケットの複製を採用 するかを選択します。パケットの複製は、FEC よりもさらに多 くのリソースを必要とします。
Packet Loss Correction Ratio パケット損失の修正 率	(Forward Error Correction (転送エラーの修正)のみ)データ パケットに対するパリティビット率。エンコーダがデコーダに 送信するデータパケットに対するパリティビットの比率が高い ほど、デコーダがパケット損失を修復できる可能性が高まりま す。ただし、比率が上がるほど冗長性も増大するため、帯域幅 のオーバーヘッドが高まります。これは、エラー修正を実現上 のトレードオフとなります。以下の事前定義済み比率から選択 します。

	Error Correction Profile(エラーの修正プロファイル)
	 10% (20:2) (デフォルト) 20% (20:4) 30% (20:6) 40% (20:8) 50% (20:10) パリティの割合は、エンコーディングファイアウォールの発信 トラフィックに適用されます。例えば、ハブのパリティ比率が 50%、ブランチのパリティ比率が 20%の場合、ハブは 20%の 比率を受け取り、ブランチは 50%の比率を受け取ります。
Recovery Duration (ms) (ミリ秒単位の回復 時間)	受信ファイアウォール(デコーダ)が受信したパリティパケットを使用して、損失したデータパケットのパケット回復を実行する際の最大時間(ミリ秒)。範囲は1~5,000、デフォルトは1,000です。 ファイアウォールは、受信したデータパケットを直ちに宛先に送信します。ファイアウォールは損失したデータパケットのパケットのリカバリをデータブロックのリカバリ期間中に実行します。リカバリ期間が終了すると、該当するブロックに関連付けられたパリティビットは破棄されます。 エンコーダはRecovery Duration(リカバリ期間)の値をデコーダに送信します。デコーダのリカバリ期間の設定は影響ありません。

Objects > Schedules [オブジェクト > スケジュール]

デフォルトでは、セキュリティポリシールールが常に有効化されています(毎日かつ常時)。 セキュリティ ポリシー ルールを特定の時間に制限するには、スケジュールを定義して該当す るポリシーに適用します。スケジュールごとに、固定の日時範囲、あるいは日次または週次の 定期スケジュールを指定できます。スケジュールをセキュリティ ポリシーに適用するには、 「Policies(ポリシー) > Security(セキュリティ)」を参照してください。



定義したスケジュールでセキュリティ ポリシー ルールが起動されると、適用されたセキュリティ ポリシー ルールは新しいセッションにのみ影響します。既存のセッションはスケジュールされたポリシーの影響を受けません。

スケジュール設定	の意味
氏名	スケジュール名を入力します(最大 31 文字)。この名前は、セ キュリティ ポリシーを定義するときにスケジュールのリストに表示 されます。名前の大文字と小文字は区別されます。また、一意の名 前にする必要があります。文字、数字、スペース、ハイフン、およ びアンダースコアのみを使用してください。
共有(Panorama の み)	以下に対してスケジュールを公開する場合は、このオプションを選 択します。
	 multi-vsys ファイアウォールの各仮想システム (vsys)。この選択 を解除すると、Objects[オブジェクト] タブで選択した Virtual System[仮想システム] のみに対してスケジュールが公開されま す。
	 Panorama 上の各デバイス グループ。この選択を解除する と、Objects[オブジェクト] タブで選択した Device Group[デバ イスグループ] のみに対してスケジュールが公開されます。
オーバーライドの無効 化(Panoramaのみ)	このスケジュールの設定が、このスケジュールを継承したデバイス グループで管理者によりオーバーライドされることを防止するに は、このオプションを選択します。デフォルトでは、この選択は解 除されています。つまり、管理者は、スケジュールを継承するすべ てのデバイス グループで設定をオーバーライドできます。
繰り返し	スケジュールのタイプを選択します(Daily(毎日)、Weekly(毎 週)、または Non-Recurring(1 回限り))。
1日1回	Add(追加)をクリックし、Start Time(開始時間)とEnd Time(終了時間)を 24 時間形式(HH:MM)で指定します。

スケジュール設定	の意味
週	Add(追加)をクリックし、Day of Week(曜日)を選択し て、Start Time(開始時間)と End Time(終了時間)を 24 時間形 式(HH:MM)で指定します。
1 回限り	Add(追加)をクリックし、Start Date(開始日)、Start Time(開 始時間)、End Date(終了日)、および End Time(終了時間)を 指定します。

ネットワーク

以下のトピックでは、ファイアウォールのネットワーク設定について説明します。

- [Network] > [インターフェイス]
- Network > Zones $[\hat{x} \vee \hat{V} \mathcal{V}]$
- Network > VLANs [ネットワーク > VLAN]
- Network > Virtual Wires [ネットワーク > バーチャル ワイヤー]
- Network > Virtual Routers [ネットワーク > 仮想ルーター]
- Network (ネットワーク) > Routing (ルーティング) > Logical Routers (論理ルーター)
- Network > IPSec Tunnels [ネットワーク > IPSec トンネル]
- Network (ネットワーク) > GRE Tunnels (GRE トンネル)
- Network > DHCP [ネットワーク > DHCP]
- Network > DNS Proxy [ネットワーク > DNS プロキシ]
- Network > Proxy
- Network > QoS [ネットワーク > QoS]
- Network > LLDP [ネットワーク > LLDP]
- Network(ネットワーク) > Network Profiles(ネットワーク プロファイル)

その他の情報をお探しですか?

PAN-OS ネットワーク管理者ガイド 『では、ネットワーク インターフェイス、複数の仮想ルー タのサポート、静的ルート、ダイナミック ルーティング プロトコル、およびファイアウォール 上のネットワークをサポートするその他の主要な機能に関する情報を提供します。

[Network] > [インターフェイス]

ファイアウォール インターフェイス (ポート) により、ファイアウォールは、ファイアウォール 内の他のインターフェイスや、他のネットワーク デバイスに接続することが可能です。以下の トピックでは、各種インターフェイス タイプとそれらの設定方法について説明します。

確認すべき情報	以下を参照
ファイアウォール インター フェイスとは何ですか?	ファイアウォール インターフェイスの概要
ファイアウォール インター フェイスの知識がありませ ん。ファイアウォール イン ターフェイスの構成要素は何 ですか?	ファイアウォール インターフェイスの共通の構成要素 PA-7000 シリーズのファイアウォール インターフェイスの 共通の構成要素
ファイアウォール インター	物理インターフェイス (Ethernet)
フェイスはすでに理解しています。特定のインターフェー	タップ インターフェイス
スタイプの設定情報はどうす	HAインターフェイス
れは確認できますか?	バーチャル ワイヤー インターフェイス
	バーチャル ワイヤー サブインターフェイス
	PA-7000 シリーズのレイヤー 2 インターフェイス
	PA-7000 シリーズのレイヤー 2 サブインターフェイス
	PA-7000 シリーズのレイヤー 3 インターフェイス
	レイヤー3インターフェイス
	レイヤー3サブインターフェイス
	Log Card Interface(ログ カード インターフェイス)
	ログ カード サブインターフェイス
	復号化ミラー インターフェイス
	Ethernet の集約(AE)インターフェイス グループ
	Ethernet の集約(AE)インターフェイス
	論理インターフェイス
	Network > Interfaces > VLAN [ネットワーク > インターフェ イス > VLAN]
	Network > Interfaces > Loopback [ネットワーク > インター フェイス > ループバック]

確認すべき情報	以下を参照
	Network > Interfaces > Tunnel [ネットワーク > インター フェイス > トンネル]
	Network > Interfaces > SD-WAN [ネットワーク > インター フェイス > SD-WLAN]
	ネットワーク > インターフェイス > PoE
	Network > Interfaces > Cellular (ネットワーク>インター フェイス>セルラー)
その他の情報をお探しです か?	ネットワーク

ファイアウォール インターフェイスの概要

ファイアウォール データ ポートのインターフェイス設定により、トラフィックがファイア ウォールを出入りできるようになります。Palo Alto Networks[®] ファイアウォールは、さまざま な展開をサポートするようにインターフェイスを構成できるため、複数の展開で同時に動作でき ます。例えば、バーチャル ワイヤー、レイヤー 2、レイヤー 3、およびタップ モードに対応す るようにファイアウォールの Ethernet インターフェイスを設定できます。ファイアウォールで サポートされるインターフェイスを以下に示します。

- Physical Interfaces (物理インターフェイス)-ファイアウォールは、トラフィックを異なる伝送速度で送受信する2種類のメディア (銅線と光ファイバー)をサポートします。イーサネットインターフェイスは、さまざまなタイプとして設定できます。具体的には、タップ、高可用性 (HA)、ログカード (インターフェイスおよびサブインターフェイス)、復号化ミラー、バーチャル ワイヤー (インターフェイスおよびサブインターフェイス)、レイヤー2(インターフェイスおよびサブインターフェイス)、レイヤー2(インターフェイスおよびサブインターフェイス)、レイヤー3(インターフェイスおよびサブインターフェイスターフェイス)、および Aggregate Ethernet として設定できます。使用可能なインターフェイスタイプおよび伝送速度は、ハードウェア モデルごとに異なります。
- Logical Interfaces (論理インターフェス)-これらには、仮想ローカル エリア ネットワーク (VLAN) インターフェイス、ループバック インターフェイス、トンネル インターフェイス、 および SD-WAN インターフェイスが含まれます。VLAN、SD-WAN またはトンネル イン ターフェイスを定義する前に、物理インターフェイスをセットアップする必要があります。

ファイアウォール インターフェイスの共通の構成要素

多くのインターフェイスタイプに共通する構成要素を表示し、その設定を行う場合 はNetwork[ネットワーク] > Interfaces[インターフェイス]を選択します。

PA-7000 シリーズのファイアウォール インターフェイスを設定する場合、または Panorama[™]を使用して任意のファイアウォールのインターフェイスを設定する場合、それらに固有または個別の構成要素の説明に関しては Common Building Blocks for PA-7000 Series Firewall Interfaces (PA-7000 シリーズのファイアウォール イン ターフェイスの共通の構成要素)を参照してください。

ファイアウォール イ ンターフェイスの構 成要素	の意味
インターフェイス (インターフェイス 名)	インターフェイス名は事前に定義されており、変更することはで きません。ただし、サブインターフェイス、集約インターフェイ ス、VLANインターフェイス、ループバック インターフェイス、トン ネル インターフェイス、SD-WAN インターフェイスには、数値のサ フィックスを付加できます。
インターフェイスタ イプ	 イーサネット インターフェイス (Network (ネットワーク) > Interfaces (インターフェイス) > Ethernet (イーサネット)) では、 以下のインターフェイス タイプを選択できます。 Tap HA Decrypt Mirror (復号化ミラー) (VM-Series NSX、Citrix SDX、AWS、Azure を除くすべてのファイアウォール上でサポート。) バーチャルワイヤー レイヤー2 レイヤ 3 Log Card (ログカード) (PA-7000シリーズのファイアウォールのみ) Aggregate Ethernet (AE)
管理プロファイル	Management Profile(管理プロファイル)(Network(ネットワー ク) > Interfaces(インターフェイス) > <if-config> Advanced(詳 細) > Other Info(その他の情報))を選択し、このインターフェ イスを介したファイアウォールの管理に使用できるプロトコル (SSH、Telnet、HTTP など)を定義するプロファイルを選択します。</if-config>
リンク ステート	 Ethernetインターフェイスの場合、リンク状態は、インターフェイスが現在アクセス可能で、かつネットワークを経由してトラフィックを受信できるかどうかを示します。 緑色 - 設定済み、かつ接続中です 赤色 - 設定済みですが、接続が停止しているか無効です 灰色 - 設定されていません リンク状態のアイコンの上にポインタを置くと、インターフェイスの リンク速度とデュプレックス設定を示すツール情報が表示されます。
IPアドレス	(任意)Ethernet、VLAN、ループバック、またはトンネルの IPv4 ア ドレスまたは IPv6 アドレスを設定します。IPv4アドレスの場合は、 更にインターフェイスのアドレスモードType[タイプ]を選択できま
ファイアウォール イ ンターフェイスの構 ^{成要素}	の意味
---	--
瓜女糸	す。Static[スタティック]、DHCP Client[DHCPクライアント]、また はPPPoEを選択できます。
仮想ルーター(VR)	インターフェイスに仮想ルーターを割り当てるか、Virtual Router(仮 想ルーター)をクリックして新しい仮想ルーターを定義します (「Network(ネットワーク)> Virtual Routers(仮想ルーター)」を 参照)。None[なし] を選択すると、現在インターフェイスに割り当て られているルーターが解除されます。
タグ(サブインター フェイスのみ)	サブインターフェイス用のVLANTag[タグ] (0 ~ 4094) を入力します。
VLAN	Network(ネットワーク)> Interfaces(インターフェイス)> VLAN を開き、既存の VLAN を変更するか、新しく Add(追加)します (Network(ネットワーク)> VLANsを参照)。None[なし] を選択 すると、現在インターフェイスに割り当てられているVLANが解除さ れます。レイヤー2インターフェイス間の切り替えを有効にする、 または VLAN インターフェイス経由のルーティングを有効にするに は、VLAN オブジェクトを設定する必要があります。
仮想システム(vsys)	ファイアウォールが複数の仮想システムをサポートし、その機能が 有効の場合は、インターフェイスの仮想システム (vsys) を選択する か、Virtual System[仮想システム] リンクをクリックして新しい vsys を定義します。
セキュリティゾーン	新規の定義を行うには、インターフェイスのSecurity Zone(セ キュリティ ゾーン)(Network(ネットワーク) > Interfaces(イ ンターフェイス) > <if-config> Config(設定))を選択する か、Zone(ゾーン)を選択します。None[なし]を選択すると、現在 インターフェイスに割り当てられているゾーンが解除されます。</if-config>
機能	イーサネットインターフェイスの場合、この列は、以下の機能が有効 かどうかを示します。 業
	DNSプロキシ
	GlobalProtect [™] ゲートウェイ対応

ファイアウォール イ ンターフェイスの構 成要素	の意味
	い リンク集約制御プロトコル (LACP)
	→ リンク レイヤー検出プロトコル (LLDP)
	NDP モニター
	E Contra de la con
	Netflow プロファイル
	る。 QoSプロファイル
	SD-WAN
コメント	インターフェイスの機能または目的の説明。

PA-7000 シリーズのファイアウォール インターフェイスの共通の構成要素

以下の表は、Network[ネットワーク] > Interfaces[インターフェイス] > Ethernet [イーサネット]ページの構成要素のうち、PA-7000 シリーズのファイアウォール インターフェイスを設定 する場合、または Panorama を使用して任意のファイアウォール インターフェイスを設定する 場合に固有のまたは個別の構成要素を示しています。インターフェイスを新しく作成する場合は Add Interface[インターフェイスの追加] ボタンをクリックし、既存のインターフェイスを編集す る場合はその名前 ([Ethernet1/1] など) をクリックします。

PA-7000 シリーズのファイアウォールでは、1つのデータポートでLog Card Interface(ログカードインターフェイス)を設定する必要があります。

PA-7000 シリーズの ファイアウォール イン ターフェイスの構成要 素	の意味
スロット	インターフェイスのスロット番号 (1 ~ 12) を選択します。ス ロットが複数あるのは、PA-7000 シリーズのファイアウォールの みです。Panorama を使用して他のファイアウォール モデルのイ

PA-7000 シリーズの ファイアウォール イン ターフェイスの構成要 素	の意味
	ンターフェイスを設定する場合は、 Slot 1 (スロット 1)を選択 します。
インターフェイス (イ ンターフェイス名)	選択したSlot[スロット]に関連付けられているインターフェイス の名前を選択します。

タップインターフェイス

• Network > Interfaces > Ethernet [ネットワーク > インターフェイス > イーサネット] タップ インターフェイスを使用して、ポートのトラフィックをモニターできます。

タップ インターフェイスを設定するには、設定されていないインターフェイスの名前 ([Ethernet1/1] など) をクリックし、以下の情報を指定します。

タップ イン ターフェイス設 定	設定場所	の意味
インターフェ イス名	イーサネット インターフェ	インターフェイス名は事前に定義されており、変更するこ とはできません。
コメント		インターフェイスの説明 (省略可) を入力します。
インターフェ イスタイプ		Tap [タップ] を選択します。
Netflowプロ ファイル		入力インターフェイスを通過する単方向 IP トラフィック を NetFlow サーバにエクスポートする場合は、サーバ プ ロファイルを選択するか、 Netflow Profile をクリックし て新しいプロファイルを定義します(Device (デバイス) > Server Profiles (サーバー プロファイル) > NetFlowを参 照)。None[なし] を選択すると、現在インターフェイスに 割り当てられているNetFlowサーバーが解除されます。
仮想システム	イーサネット インターフェ イス > 設定	ファイアウォールが複数の仮想システムをサポートし、そ の機能が有効の場合は、インターフェイスの仮想システム を選択するか、Virtual System[仮想システム] リンクをク リックして新しいvsysを定義します。

タップ <i>イン</i> ターフェイス設 定	設定場所	の意味
セキュリティ ゾーン		インターフェイス用のセキュリティゾーンを選択する か、 Zone [ゾーン] をクリックして新しいゾーンを定義しま す。 None [なし] を選択すると、現在インターフェイスに割 り当てられているゾーンが解除されます。
リンク速度	イーサネット インターフェ イス > 上級 > リンク設定	インターフェイス速度を Mbps 単位で選択するか、auto を 選択してファイアウォールが自動的に速度を決定するよう にします。
リンクデュプ レックス		インターフェイスの伝送モードを、フル デュプレックス (full)、ハーフ デュプレックス (half)、オート ネゴシエー ション (auto) から選択します。
リンク ステー ト		インターフェイスの状態を、有効 (up)、無効 (down)、自動 決定 (auto) から選択します。
PoE Rsvd Pwr	イーサネット インターフェ イス > 上級 > PoE 設定 (サポートされ ているファイ アウォールの み)	PoE が有効になっている場合、割り当てられる電力量を Watts で選択します。
PoE イネーブ ル		このインターフェイスで PoE を有効にする場合に選択しま す。

HAインターフェイス

• Network > Interfaces > Ethernet [ネットワーク > インターフェイス > イーサネット]

HA (高可用性) インターフェイスにはそれぞれ固有の機能があります。一方のインターフェイス は設定の同期とハートビート機能を持ち、もう一方のインターフェイスは状態の同期機能を持っ ています。アクティブ/アクティブの高可用性が有効になっている場合、ファイアウォールは、3 つ目の HA インターフェイスを使用してパケットを転送できます。

 一部の Palo Alto Networks ファイアウォールには、HA 専用の物理ポートがあります (制御リンク用とデータ リンク用)。専用ポートのないファイアウォールの場合、HA に使用するデータ ポートを指定する必要があります。HA の詳細は「Device(デバ イス) > Virtual Systems(仮想システム)」を参照してください。

HA インターフェイスを設定するには、設定されていないインターフェイスの名前 ([Ethernet1/1] など)をクリックし、以下の情報を指定します。

HA インター フェイス設定	設定場所	の意味
インターフェ イス名	イーサネット インターフェ	インターフェイス名は事前に定義されており、変更すること はできません。
コメント		インターフェイスの説明 (省略可) を入力します。
インターフェ イスタイプ	-	HA を選択します。
リンク速度	イーサネット インターフェ イス > 上級 >	インターフェイス速度を Mbps 単位で選択するか、auto を 選択してファイアウォールが自動的に速度を決定するように します。
リンクデュプ レックス	リンク設定	インターフェイスの伝送モードを、フル デュプレックス (full)、ハーフ デュプレックス (half)、オート ネゴシエーショ ン (auto) から選択します。
リンク ス テート		インターフェイスの状態を、有効 (up)、無効 (down)、自動決 定 (auto) から選択します。
PoE Rsvd Pwr	イーサネット インターフェ	PoE が有効になっている場合、割り当てられる電力量を Watts で選択します。
PoE イネーブ ル	PoE 設定 (サポートさ れているファ イアウォール のみ)	このインターフェイスで PoE を有効にする場合に選択しま す。

バーチャルワイヤーインターフェイス

• Network > Interfaces > Ethernet [ネットワーク > インターフェイス > イーサネット]

バーチャル ワイヤーは論理的に 2 つの Ethernet インターフェイスを結合し、すべてのトラ フィック、または選択した VLAN タグを持つトラフィックのみをインターフェイス間で渡すこ とができます (スイッチングまたはルーティング サービスは使用できません)。また、バーチャ ル ワイヤー サブインターフェイスを作成し、IP アドレス、IP 範囲、またはサブネットに基づい てトラフィックを分類することもできます。バーチャル ワイヤーでは、隣接ネットワーク デバ イスへの変更は必要ありません。バーチャル ワイヤーは、同じ媒体の 2 つの Ethernet インター フェイス (銅線または両方の光ファイバ)を結束するか、カッパーインターフェイスを光ファイ バインターフェイスに結束することができます。

バーチャル ワイヤーを設定するには、バインドする 2 つのインターフェイス (Network > Interfaces > Ethernet) を決定し、次の表の説明に従って設定を構成します。

バーチャルワイヤー用に既存のインターフェイスを使用する場合は、まずそのイン ターフェイスを、すべての関連付けられたセキュリティゾーンから削除します。

バーチャル ワ イヤー イン ターフェイス 設定	設定場所	の意味
インターフェ イス名	イーサネット インターフェ	インターフェイス名は事前に定義されており、変更すること はできません。
コメント		インターフェイスの説明 (省略可) を入力します。
インターフェ イスタイプ	-	[バーチャル ワイヤー]を選択します。
バーチャルワ イヤー	イーサネット インターフェ イス > 設定	バーチャルワイヤーを選択するか、Virtual Wire(バーチャ ルワイヤー)をクリックして新しいバーチャル ワイヤーを定 義します (Network(ネットワーク) > Virtual Wires(バー チャル ワイヤー)を参照)。None[なし] を選択すると、現在 インターフェイスに割り当てられているバーチャルワイヤー が解除されます。
仮想システ ム(vsys)		ファイアウォールが複数の仮想システムをサポートし、その 機能が有効の場合は、インターフェイスの仮想システムを選 択するか、Virtual System[仮想システム] リンクをクリック して新しいvsysを定義します。
セキュリティ ゾーン		インターフェイス用のセキュリティゾーンを選択する か、 Zone [ゾーン] をクリックして新しいゾーンを定義しま す。 None [なし] を選択すると、現在インターフェイスに割 り当てられているゾーンが解除されます。
リンク速度	イーサネット インターフェ イス > 上級 > リンク設定	インターフェイス速度を Mbps 単位で選択するか、auto を 選択してファイアウォールが自動的に速度を決定するように します。
リンクデュプ レックス		インターフェイスの伝送モードを、フル デュプレックス (full)、ハーフ デュプレックス (half)、オート ネゴシエーショ ン (auto) から選択します。バーチャル ワイヤーの両方のイ ンターフェイスは同じ転送モードである必要があります。
リンク ス テート	1	インターフェイスの状態を、有効 (up)、無効 (down)、自動決 定 (auto) から選択します。

バーチャル ワ イヤー イン ターフェイス 設定	設定場所	の意味
PoE Rsvd Pwr	イーサネット インターフェ イフ 、 ト級 、	PoE が有効になっている場合、割り当てられる電力量を Watts で選択します。
PoE イネーブ ル	イス > 上級 > PoE 設定 (サポートさ れているファ イアウォール のみ)	このインターフェイスで PoE を有効にする場合に選択しま す。
LLDP の有効 化	イーサネット インターフェ イス > 上級 > LLDP	選択すると、インターフェイスでリンク レイヤー検出プロト コル (LLDP) が有効になります。LLDP は、リンク レイヤー で機能し、隣接するデバイスとその機能を検出します。
プロファイル		LLDP が有効の場合は、インターフェイスに割り当てる LLDP プロファイルを選択するか、LLDP Profile(LLDP プロ ファイル)をクリックして新しいプロファイルを作成しま す(「Network(ネットワーク) > Network Profiles(ネッ トワーク プロファイル) > LLDP Profile(LLDP プロファイ ル)」を参照)。ファイアウォールでグローバルなデフォル ト設定を使用するように設定する場合はNone[なし]を選択 します。
HAパッシブ ステートを有 効にする		LLDP が有効化されている場合、これを選択すると、HA の パッシブ ファイアウォールが LLDP についてそのピアと事前 にネゴシエートした後にファイアウォールがアクティブにな るように設定されます。 LLDP が有効化されていない場合、これを選択すると、LLDP パケットが HA のパッシブ ファイアウォールを単に通過する ように設定されます。

バーチャル ワイヤー サブインターフェイス

• Network > Interfaces > Ethernet [ネットワーク > インターフェイス > イーサネット]

バーチャル ワイヤー (vwire) サブインターフェイスでは、VLAN タグまたは VLAN タグと IP 分 類子の組み合わせによってトラフィックを分離し、タグの付いたトラフィックを異なるゾーンと 仮想システムに割り当ててから、定義された条件に一致するトラフィックのセキュリティ ポリ シーを適用できます。

バーチャル ワイヤー インターフェイスを追加するには、そのインターフェイスの行を選択 し、Add Subinterface をクリックし、次の情報を指定します。

バーチャル ワ イヤー サブイ ンターフェイ ス設定	の意味
インター フェイス名	読み取り専用の Interface Name[インターフェイス名] フィールドには、選択 したvwireインターフェイスの名前が表示されます。サブインターフェイス を識別する数値サフィックス (1 ~ 9999) を隣のフィールドに入力します。
コメント	サブインターフェイスの説明(省略可)を入力します。
タグ	サブインターフェイス用のVLAN Tag[タグ] (0 ~ 4094) を入力します。
Netflowプロ ファイル	入力サブインターフェイスを通過する単方向 IP トラフィックを NetFlow サーバにエクスポートする場合は、サーバ プロファイルを選択する か、Netflow Profile をクリックして新しいプロファイルを定義しま す(Device (デバイス) > Server Profiles (サーバー プロファイル) > NetFlow を参照)。None[なし] を選択すると、サブインターフェイスから現 在の NetFlow サーバー割り当てが削除されます。
IP による分 類	Add[追加] をクリックし、IP アドレス、IP 範囲、またはサブネットを入力す ると、この vwire サブインターフェイスのトラフィックを分類できます。
バーチャル ワイヤー	仮想ワイヤを選択するか、Virtual Wire をクリックして新しいワイヤを定義 します (Network > Virtual Wires [ネットワーク > バーチャル ワイヤー] を参 照)。None[なし] を選択すると、現在サブインターフェイスに割り当てられ ているバーチャルワイヤーが解除されます。
仮想システ ム(vsys)	ファイアウォールが複数の仮想システムをサポートし、その機能が有効な 場合は、サブインターフェイスの仮想システム (vsys) を選択するか、Virtual System[仮想システム] リンクをクリックして新しい vsys を定義します。
セキュリ ティゾーン	サブインターフェイス用のセキュリティゾーンを選択するか、Zone[ゾーン] をクリックして新しいゾーンを定義します。現在サブインターフェイスに割 り当てられているゾーンを解除する場合はNone[なし]を選択します。

PA-7000 シリーズのレイヤー2インターフェイス

• Network > Interfaces > Ethernet [ネットワーク > インターフェイス > イーサネット]

レイヤ2インターフェイスを設定するには、ネットワーク > インターフェイス > イーサネット を選択します。設定されていないインターフェイス(ethernet1/1 など)の名前をクリックし、次 の情報を指定します。

レイヤー 2 イ ンターフェイ ス設定	設定場所	の意味
インターフェ イス名	イーサネット インターフェ	インターフェイス名は事前に定義されており、変更すること はできません。
コメント		インターフェイスの説明 (省略可) を入力します。
インターフェ イスタイプ	-	Layer2[レイヤー 3] を選択します。
Netflowプロ ファイル		入力インターフェイスを通過する単向性の IP トラフィッ クを NetFlow サーバーにエクスポートする場合は、サー バー プロファイルを選択するか、Netflow Profile (Netflow プロファイル)をクリックして新しいプロファイルを定 義します(「Device (デバイス) > Server Profiles (サー バープロファイル) > NetFlow」を参照)。None[なし] を選択すると、現在インターフェイスに割り当てられてい るNetFlowサーバーが解除されます。
VLAN	イーサネット インターフェ イス > 設定	レイヤー2インターフェイス間の切り替えを有効にする場 合、または VLAN インターフェイス経由のルーティングを 有効にする場合は、既存の VLAN を選択するか、VLAN をク リックして新しい VLAN を定義します(「Network(ネット ワーク) > VLAN」を参照)。None[なし] を選択すると、現 在インターフェイスに割り当てられているVLANが解除され ます。
仮想システ ム(vsys)		ファイアウォールが複数の仮想システムをサポートし、その 機能が有効の場合は、インターフェイスの仮想システムを選 択するか、Virtual System[仮想システム] リンクをクリック して新しいvsysを定義します。
セキュリティ ゾーン		インターフェイス用のSecurity Zone[セキュリティゾーン]を 選択するか、Zone[ゾーン] をクリックして新しいゾーンを定 義します。None[なし] を選択すると、現在インターフェイ スに割り当てられているゾーンが解除されます。
リンク速度	イーサネット インターフェ イス > 上級	インターフェイス速度を Mbps 単位で選択するか、auto を 選択して、ファイアウォール が自動的に速度を決定するよう にします。
リンクデュプ レックス		インターフェイスの伝送モードを、フル デュプレックス (full)、ハーフ デュプレックス (half)、オート ネゴシエーショ ン (auto) から選択します。

レイヤー 2 イ ンターフェイ ス設定	設定場所	の意味
リンク ス テート		インターフェイスの状態を、有効 (up)、無効 (down)、自動決 定 (auto) から選択します。
LLDP の有効 化	イーサネット インターフェ イス > 上級 > LLDP	選択すると、インターフェイスでリンク レイヤー検出プロト コル (LLDP) が有効になります。LLDP は、リンク レイヤー で機能し、隣接するデバイスとその機能を検出します。
LLDPプロ ファイル		LLDP が有効の場合は、インターフェイスに割り当てる LLDP プロファイルを選択するか、LLDP Profile(LLDP プロ ファイル)をクリックして新しいプロファイルを作成しま す(「Network(ネットワーク) > Network Profiles(ネッ トワーク プロファイル) > LLDP Profile(LLDP プロファイ ル)」を参照)。ファイアウォールでグローバルなデフォル ト設定を使用するように設定する場合はNone[なし] を選択 します。
HAパッシブ ステートを有 効にする		LLDP が有効化されている場合はこのオプションを選択する ことで、パッシブなファイアウォールがアクティブに切り替 わる前に、もう一方のピアと LLDP の取り決めを行うように なります。

PA-7000 シリーズのレイヤー2 サブインターフェイス

• Network > Interfaces > Ethernet [ネットワーク > インターフェイス > イーサネット]

物理レイヤー2インターフェイスとして設定された各 Ethernet ポートについては、ポートで受信するトラフィックに割り当てられる VLAN タグごとに追加の論理レイヤー2インターフェイス(サブインターフェイス)を定義できます。レイヤー2サブインターフェイス間の切り替えを 有効にするには、それらのサブインターフェイスに同じ VLAN オブジェクトを割り当てます。

PA-7000 シリーズ レイヤー 2 インターフェイスを設定するには、その物理インターフェイスの 行を選択した後、Add Subinterface(サブインターフェイスの追加)をクリックし、以下の情報 を指定します。

レイヤー 2 サ ブインター フェイス設定	の意味
インターフェ イス名	読み取り専用のインターフェイス名の欄には、選択した物理インターフェイ スの名前が表示されます。サブインターフェイスを識別する数値サフィック ス (1 ~ 9999)を隣のフィールドに入力します。

レイヤー 2 サ ブインター フェイス設定	の意味
コメント	サブインターフェイスの説明 (省略可) を入力します。
タグ	サブインターフェイス用のVLANTag[タグ] (0 ~ 4094) を入力します。
Netflowプロ ファイル	入力サブインターフェイスを通過する単向性の IP トラフィックを NetFlow サーバーにエクスポートする場合は、サーバー プロファイルを選択する か、Netflow Profile (Netflow プロファイル)をクリックして新しいプロ ファイルを定義します (Device (デバイス) > Server Profiles (サーバー プロ ファイル) > NetFlowを参照)。現在サブインターフェイスに割り当てられ ているNetFlowサーバーを解除する場合は、None[なし]を選択します。
VLAN	レイヤー2インターフェイス間の切り替えを有効にする場合、または VLAN インターフェイス経由のルーティングを有効にする場合は、VLAN を選択す るか、VLAN をクリックして新しい VLAN を定義します(「Network(ネッ トワーク) > VLAN」を参照)。現在サブインターフェイスに割り当てられ ているVLANを解除する場合はNone[なし] を選択します。
仮想システ ム(vsys)	ファイアウォールが複数の仮想システムをサポートし、その機能が有効な 場合は、サブインターフェイスの仮想システム (vsys) を選択するか、Virtual System[仮想システム] リンクをクリックして新しい vsys を定義します。
セキュリティ ゾーン	サブインターフェイス用のセキュリティゾーンを選択するか、 Zone [ゾーン] をクリックして新しいゾーンを定義します。現在サブインターフェイスに割 り当てられているゾーンを解除する場合はNone[なし] を選択します。

PA-7000 シリーズのレイヤー3インターフェイス

• Network > Interfaces > Ethernet [ネットワーク > インターフェイス > イーサネット]

レイヤー3インターフェイスを設定するには、インターフェイス(例えば ethernet1/1)を選択して次の情報を指定します。

レイヤー 3 イン ターフェイス設定	設定場所	の意味
インターフェイ ス名	イーサネッ トインター フェイス	インターフェイス名は事前に定義されており、変更する ことはできません。
コメント		インターフェイスの説明 (省略可) を入力します。

レイヤー 3 イン ターフェイス設定	設定場所	の意味
インターフェイ スタイプ		[レイヤー 3] を選択します。
Netflowプロファ イル		入力インターフェイスを通過する単向性の IP トラ フィックを NetFlow サーバーにエクスポートする場 合は、サーバー プロファイルを選択するか、Netflow Profile (Netflow プロファイル) をクリックして新しい プロファイルを定義します (「Device (デバイス) > Server Profiles (サーバー プロファイル) > NetFlow」を 参照)。None[なし]を選択すると、現在インターフェイ スに割り当てられているNetFlowサーバーが解除されま す。
仮想ルーター(VR)	イーサネッ トインター フェイス > コンフィグ	仮想ルーターを選択するか、Virtual Router(仮想ルー ター)をクリックして新しい仮想ルーターを定義します (Network(ネットワーク) > Virtual Routers(仮想ルー ター)を参照)。None[なし] を選択すると、現在イン ターフェイスに割り当てられているルーターが解除され ます。
仮想システ ム(vsys)		ファイアウォールが複数の仮想システムをサポートし、 その機能が有効の場合は、インターフェイスの仮想シス テム (vsys) を選択するか、Virtual System[仮想システム] リンクをクリックして新しい vsys を定義します。
セキュリティ ゾーン		インターフェイス用のセキュリティゾーンを選択する か、 Zone [ゾーン] をクリックして新しいゾーンを定義し ます。 None [なし] を選択すると、現在インターフェイス に割り当てられているゾーンが解除されます。
SD-WAN を有効 にする	イーサネッ トインター フェイス > IPv4	SD-WAN を有効にする を選択して、イーサネット イン ターフェイスの SD-WAN 機能を有効にします。
タイプ		IPv4 アドレス タイプをインターフェイスに割り当てる方 法を選択します。
		 Static[静的] – IP アドレスを手動で指定する必要があります。
		 PPPoE – ファイアウォールがPPPoE (Point-to-Point Protocol over Ethernet) 用のインターフェイスを使用 します。
		 DHCP Client[DHCP クライアント] – インターフェイス が DHCP (Dynamic Host Configuration Protocol) クライ

レイヤー 3 イン ターフェイス設定	設定場所	の意味
		アントとして機能し、ダイナミックに割り当てられた IP アドレスを受信できます。
		アクティブ/アクティブ高可用性 (HA) モード のファイアウォールは、PPPoE や DHCP ク ライアントをサポートしません。
		選択した IP アドレス方式に応じて、タブに表示されるオ プションは異なります。

IPv4 アドレス **Type**[タイプ] = 静的

IP	ク イーサネッ トインター フェイス > IPv4	 Add[追加] をクリックし、以下のいずれかの手順を実行して、インターフェイスのスタティック IP アドレスとネットワークマスクを指定します。 CIDR (Classless Inter-Domain Routing)表記法の ip_address/maskの形式(例: 192.168.2.0/24)でエントリを入力します。 タイプが IP netmask[IP ネットマスク]の既存のアドレ
		スオブジェクトを選択します。 • Adress[アドレス] をクリックし、タイプが IP netmask[IP ネットマスク] のアドレスオブジェクトを 作成します。
		インターフェイスに対して複数の IP アドレスを入力でき ます。IP アドレスの最大数は、ファイアウォールが使用 する転送情報ベース (FIB) によって決まります。 IP アドレスを削除するには、アドレスを選択して Delete[[削除]] をクリックします。

IPv4 アドレス **Type**[タイプ] = **PPPoE**

Enable [有効化]	イーサネッ トインター フェイス > IPv4 > PPPoE > 一 般	PPPoE 終端点用のインターフェイスを有効化する場合に 選択します。
username		ポイントツーポイント接続用の Username (ユーザー名) を 入力します。
パスワード/再入 力 パスワード		ユーザー名のパスワードを入力し、確認します。

レイヤー 3 イン ターフェイス設定	設定場所	の意味
PPPoE クライア ント ランタイム 情報の表示		(任意)接続を確立するためにファイアウォールがイン ターネットサービスプロバイダ(ISP)とネゴシエートし たパラメータを表示するダイアログを開きます。表示さ れる具体的な情報は、ISP ごとに異なります。
認証	イーサネッ トインター フェイス > IPv4 > PPPoE > 上 級	PPPoE通信用の認証プロトコルを選択します。CHAP (Challenge-Handshake Authentication Protocol)、PAP (Password Authentication Protocol)、またはデフォルトの Auto(ファイアウォールがプロトコルを決定)のいずれ かから選択します。None[なし]を選択すると、現在イン ターフェイスに割り当てられているプロトコルが解除さ れます。
スタティック ア ドレス		以下のいずれかの手順を実行して、インターネット サー ビス プロバイダが割り当てた IP アドレスを指定します (デフォルト値なし)。
		 CIDR (Classless Inter-Domain Routing)表記法の ip_address/maskの形式(例: 192.168.2.0/24)でエン トリを入力します。
		 タイプが IP netmask[IP ネットマスク]の既存のアドレスオブジェクトを選択します。
		 Adress[アドレス] をクリックし、タイプが IP netmask[IP ネットマスク] のアドレスオブジェクトを 作成します。
		 None[なし] を選択すると、インターフェイスから現在のアドレス割り当てが削除されます。
Automatically create default route pointing to peer(ピアを 指すデフォルト ルートを自動的 に作成)		接続時に自動的に PPPoE ピアを指し示すデフォルト ルートを自動的に作成する場合に選択します。
デフォルト ルー ト メトリック		(任意)ファイアウォールとインターネットサービスプ ロバイダ間のルートについて、デフォルトルートへの関 連付けと、パス選択の際に使用するルートメトリック (優先度)を入力します(範囲は1~65,535)。数値が 小さいほど優先度が高くなります。

レイヤー 3 イン ターフェイス設定	設定場所	の意味
アクセス コンセ ントレータ		(<u>任意</u>)ファイアウォールが接続するインターネット サービスプロバイダ側のアクセスコンセントレータの名 前を入力します(デフォルトなし)。
サービス		(任意)サービス文字列を入力します(デフォルトな し)。
Passive		パッシブモードを使用する場合に選択します。パッシブ モードでは、PPPoE エンド ポイントはアクセス コンセン トレータが最初のフレームを送信するまで待機します。

IPv4 アドレス **Type**[タイプ] = **DHCP**

Enable [有効化]	イーサネッ トインター フェイス > IPv4	インターフェイスの DHCP クライアントを有効化する場 合に選択します。
サーバー提供の デフォルト ゲー トウェイを指す デフォルト ルー トを自動的に作 成		DHCP サーバーによって提供されるデフォルト ゲート ウェイを指し示すデフォルト ルートを自動的に作成する 場合に選択します。
ホスト名の送信		ファイアウォール (DHCP クライアントとして) にイン ターフェイスのホスト名 (Option 12) を DHCP サーバー に送信させる場合に選択します。Send Hostname (ホスト 名の送信) を行う場合、デフォルトでファイアウォールの ホスト名がホスト名フィールドで選択されます。その名 前を送信するか、カスタム ホスト名 (大文字および小文 字、数字、ピリオド、ハイフン、アンダースコアを含む 最長 64 文字) を入力します。
デフォルト ルー ト メトリック		ファイアウォールと DHCP サーバー間のルートについ て、デフォルト ルートに関連付け、パス選択に使用す るルートメトリック (優先度) を入力します(任意、範囲 は1~65,535、デフォルトなし)。数値が小さいほど優先 度が高くなります。
DHCP クライア ント ランタイム 情報の表示		DHCP のリース状態、ダイナミック IP アドレス割り当 て、サブネット マスク、ゲートウェイ、サーバー設定 (DNS、NTP、ドメイン、WINS、NIS、POP3、および SMTP)など、DHCP サーバーから受信したすべての設定 を表示する場合に選択します。

レイヤー 3 イン ターフェイス設定	設定場所	の意味
インターフェー スでの IPv6 の有 効化	イーサネッ トインター フェイス > IPv6	このインターフェイスの IPv6 アドレスを有効にする場合 に選択します。
インターフェイ ス ID		64 ビット拡張一意識別子 (EUI-64) を 16 進数形式で入力 します (例: 00:26:08:FF:FE:DE:4E:29)。このフィールド を空白のままにすると、ファイアウォールが、物理イン ターフェイスの MAC アドレスから生成された EUI-64 を 使用します。アドレスの追加時に Use interface ID as host portion[ホスト部分にインターフェイス ID を使用] オプ ションを選択すると、ファイアウォールがそのアドレス のホスト部分にインターフェイス ID を使用します。
アドレス		Add[追加] をクリックして、IPv6 アドレスごとに以下のパ ラメータを設定します。
		 Address(アドレス) – IPv6 アドレスとプレフィッ クス長を入力します(例: 2001:400:f00::1/64)。 既存のIPv6アドレスオブジェクトを選択すること や、Address[アドレス] をクリックしてアドレスオブ ジェクトを作成することもできます。
		 Enable address on interface (インターフェイス上のア ドレスを有効にする) – インターフェイスの IPv6 ア ドレスを有効にする場合に選択します。
		 Use interface ID as host portion(ホスト部分にイン ターフェイス ID を使用) – IPv6 アドレスのホスト部 分に Interface ID(インターフェイス ID)を使用する 場合に選択します。
		 Anycast(エニーキャスト) – 最も近いノードを経由 するルーティングを含める場合に選択します。
		 Send Router Advertisement (ルーター通知を送信) – この IP アドレスのルーター通知 (RA) を有効にする 場合に選択します。(インターフェイスのグローバルの Enable Router Advertisement[ルーター通知を有効化す る] オプションも有効化しておく必要があります)。RA の詳細は、「ルーター通知を有効にする」を参照して ください。
		残りのフィールドは、RA を有効にした場合にのみ適用 されます。
		 Valid Lifetime(有効なライフタイム) – ファイア ウォールがアドレスを有効とみなす時間(秒)で す。有効なライフタイムは、Preferred Lifetime(優)

レイヤー 3 イン ターフェイス設定	設定場所	の意味
		先ライフタイム)以上でなければなりません(デ フォルトは 2,592,000)。
		 Preferred Lifetime (優先ライフタイム) – 有効 なアドレスが優先される時間(秒)です。この時 間内は、ファイアウォールがこのアドレスを使用 してトラフィックを送受信できます。優先ライフ タイムの期限後は、ファイアウォールがこのアド レスを使用して新しい接続を確立することはでき ませんが、既存の接続は Valid Lifetime(有効なラ イフタイム)の期限まで有効です(デフォルトは 604,800)。
		 On-link(オンリンク) – プレフィックス内にアド レスがあるシステムにルーターなしで到達可能であ る場合に選択します。
		 Autonomous(自律型) – 通知されたプレフィック スとインターフェイス ID を組み合わせて、システ ムが IP アドレスを独自に作成できる場合に選択し ます。
重複アドレス検 出を有効にする	イーサネットインター	重複アドレス検出(DAD)を有効にする場合に選択し、 セクション内の他のフィールドの設定を行います。
DAD 試行回数	フェイス > IPv6 > Address Resolution (アドレス解 決)	ネイバー要請間隔 (NS Interval (NS 間隔)) の内にDADを試 行する回数を指定します(範囲は 1 ~ 10、デフォルトは 1)。この回数を超えるとネイバーに障害があるとみなさ れます。
到達可能時間		クエリと応答が正常に行われた後引き続きネイバーに到 達可能な時間(秒)を指定します(範囲は1~36,000、 デフォルトは30)。
NS 間隔 (ネイ バー要請間隔)		DADの試行秒数を指定します(範囲は1~10、デフォルトは1)。この秒数を超えると障害があるとみなされます。
NDP モニタリン グの有効化		NDP(Neighbor Discovery Protocol)モニタリン グを有効にする場合に選択します。有効になっ ていると、NDP モニター(Features (機能)列の
		を選択し、ファイアウォールで検出されたネイバーに関 する情報(IPv6 アドレス、対応する MAC アドレスおよ

レイヤー 3 イン ターフェイス設定	設定場所	の意味
		び User-ID など)を(ベストケース ベースで)表示でき ます。
ルーター通知を 有効にする	イーサネッ トインター フェイス > IPv6 > ルー ター アドバ タイズメン ト	 IPv6 インターフェイスでステートレス アドレス自動設定 (SLAAC) を行う場合に選択してこのセクション内の他のフィールドを設定します。ルーター通知 (RA) メッセージを受信する IPv6 DNS クライアントは、この情報を使用します。 RA により、ファイアウォールが、スタティックに設定されていない IPv6 ホストのデフォルト ゲートウェイとして機能し、ホストにアドレス設定の IPv6 プレフィックスを提供できます。別の DHCPv6 サーバーをこの機能と併用すると、DNS および他の設定をクライアントに提供できます。
		これはインターフェイスのクローハル設定です。IPアト レスごとに RA オプションを設定する場合は、IP アドレス テーブルの Add(追加)をクリックしてアドレスを設定 します。IP アドレスに RA オプションを設定する場合は、 インターフェイスの Enable Router Advertisement[ルー ター通知を有効にする] オプションを選択する必要があり ます。
最小間隔 (秒)		ファイアウォールが送信する RA 間の最小間隔(秒)を指 定します(範囲は 3 ~ 1,350、デフォルトは 200)。ファ イアウォールは、設定した最小値と最大値の間のランダ ムな間隔で RA を送信します。
最大間隔(秒)		ファイアウォールが送信する RA 間の最大間隔(秒)を指定します(範囲は 4 ~ 1,800、デフォルトは 600)。ファ イアウォールは、設定した最小値と最大値の間のランダ ムな間隔で RA を送信します。
ホップ制限		クライアントに適用する、送信パケットのホップ制限を 指定します(範囲は 1 ~ 255、デフォルトは 64)。ホッ プ制限を指定しない場合は 0 を入力します。
リンク MTU		クライアントに適用するリンクの最大転送単位 (MTU) を 指定します。リンクMTUを指定しない場合は unspecified (指定しない)を選択します(範囲は 1,280 ~ 9,192、デ フォルトは unspecified)。
到達可能時間 (ミ リ秒)		到達可能確認メッセージを受信後ネイバーに到達可能で あると想定するためにクライアントが使用する到達可能

レイヤー 3 イン ターフェイス設定	設定場所	の意味
		時間 (ミリ秒) を指定します。到達可能時間を指定しない 場合は unspecified (指定しない) を選択します(範囲は 0 ~ 3,600,000、デフォルトはunspecified)。
リトランスミッ ション時間 (ミリ 秒)		ネイバー要請メッセージを再送信するまでにクライアン トが待機する時間を決定するリトランスミッションタイ マーを指定します。リトランスミッション時間を指定し ない場合は unspecified (指定しない) を選択します(範囲 は 0 ~ 4,294,967,295、デフォルトはunspecified)。
ルーターの有効 期間 (秒)		クライアントがファイアウォールをデフォルトゲー トウェイとして使用する時間を指定します(範囲は 0~9,000、デフォルトは1,800)。0は、ファイアウォー ルがデフォルトゲートウェイではないことを示します。 有効期間が過ぎると、クライアントがそのデフォルト ルーターリストからファイアウォールエントリを削除し て、別のルーターをデフォルトゲートウェイとして使用 します。
ルーター設定		ネットワーク セグメントに複数の IPv6 ルーターがある 場合は、クライアントがこのフィールドを使用して優先 ルーターを選択します。セグメントの他のルーターとの 比較において、RA が通知するファイアウォール ルーター の優先度を High、Medium (デフォルト)、Low の中から 選択します。
管理された設定	-	アドレスを DHCPv6 経由で使用できることをクライアン トに示す場合に選択します。
整合性チェック	イーサネッ トインター フェイス > IPv6 > ルー ター広告 (続 き)	他のルーターから送信された RA がリンク上で一貫した情報を通知していることをファイアウォールで確認する場合に選択します。ファイアウォールでは、システム ログの不一致が記録されます。タイプは ipv6nd です。
その他の設定		他のアドレス情報(DNS 関連の設定など)を DHCPv6 経 由で使用できることをクライアントに示す場合に選択し ます。
ルーター通知に DNS 情報を含め る	イーサネッ トインター フェイス > IPv6 > DNS のサポート	ファイアウォールがこの IPv6 のイーサネット インター フェイスからの NDP ルーター通知 (RA) メッセージで DNS 情報を送信できるようにする場合に選択します。 この表の他の DNS Support (DNS サポート) フィール ドは、このオプションを選択した場合にのみ表示されま す。

レイヤー 3 イン ターフェイス設定	設定場所	の意味
SERVER		1つ以上の再帰 DNS(RDNS)サーバー アドレスを Add(追加)し、ファイアウォールがこの IPv6 Ethernet インターフェイスから NDP ルーター通知によって送信で きるようにします。RDNS サーバーは、ルート DNS サー バーと権限のある DNS に一連の DNS ルックアップ要求 を送信し、最終的に DNS クライアントに IP アドレスを 提供します。
		ファイアウォールがリストの上から下の順に NDP ルー ター通知で受信者に送信する RDNS サーバーを最大 8 個 設定できます。その後、受信者は同じ順序でこれらのア ドレスを使用します。サーバーの順序を変更するには、 サーバーを選択して Move Up(上へ)移動したり Move Down(下へ)移動したりします。サーバーが必要なく なったら、そのサーバーをリストから Delete(削除)し ます。
有効期間	-	IPv6 DNS クライアントがルーター通知を受信した後 に、RDNS サーバーを使用してドメイン名を解決できる最 大秒数を入力します(範囲は最大間隔(秒)の値からそ の 2 倍までで、デフォルトは 1,200 です)。
サフィックス		 DNS 検索リスト (DNSSL) の1つ以上のドメイン名 (サフィックス) を Add (追加) および設定します。最大長は255 バイトです。 DNS 検索リストは、DNS クライアント ルーターが DNS クエリに名前を入力する前に非修飾ドメイン名に (1つずつ) 追加するドメインサフィックスのリストです。これにより、DNS クエリで完全修飾ドメイン名が使用されます。たとえば、DNS クライアントがサフィックスのない「quality」の DNS クエリを送信しようとすると、ルーターはピリオドと DNS 検索リストの最初の DNS サフィックスをその名前に追加して DNS クエリを送信します。リストの最初の DNS サフィックスが「company.com」の場合、ルーターの DNS クエリの完全修飾ドメイン名は FQDN になります。 DNS クエリに失敗すると、ルーターはリストの 2 番目の DNS サフィックスを非修飾名に追加して、新しい DNS クエリを送信します。ルーターは DNS ルックアップが成功するか (残りのサフィックスは無視されます)、ルーターがリストのすべてのサフィックスを試行するまで DNS サフィックスを試行します。

レイヤー 3 イン ターフェイス設定	設定場所	の意味
		ネイバー検出 DNSSL オプションで DNS クライアント ルーターに提供するサフィックスを使用してファイア ウォールを設定します。DNSSL オプションを受信する DNS クライアントは、その非修飾 DNS クエリでサフィッ クスを使用します。
		DNS 検索リストに対して最大 8 個のドメイン名(サ フィックス)を設定し、ファイアウォールでそれらを NDP ルーター通知に含めて受信者に送信できます(上 から下の順に送信します)。その後、受信者は同じ順序 でこれらのアドレスを使用できます。順序を変更するに は、サフィックスを選択して Move Up(上へ)移動した り Move Down(下へ)移動したりします。サフィック スが必要なくなったら、そのサフィックスを Delete(削 除)します。
有効期間		IPv6 DNS クライアントがルーター通知を受信した後 に、DNS 検索リストのドメイン名(サフィックス) を使用できる最大秒数を入力します(範囲は最大間隔 (秒)の値からその2倍までで、デフォルトは1,200で す)。
SD-WAN イン ターフェイス ス テータス	イーサネッ トインター フェイス > SD-WAN	IPv4 タブで SD-WAN を有効にする を選択すると、ファ イアウォールは SD-WAN インターフェイス ステータス を表示します。有効。Enable SD-WAN(SD-WANの有効 化)を実行しなかった場合、Disabled(無効化)と表示 されます。
SD-WAN イン ターフェイス プ ロファイル		このイーサネット インターフェースに適用する SD-WAN インターフェイス プロファイルを選択するか、新しい SD-WAN インターフェース プロファイルを追加します。
		 SD-WAN インターフェイス プロファイル を適用する前に、インターフェイスの SD-WAN を有効にする 必要があります。
Upstream NAT (アップストリー ム NAT)		NAT を実行するデバイスが背後で SD-WAN ハブまたはブ ランチが存在する場合は、ハブまたはブランチのアップ ストリーム NAT をEnable(有効化)にします。
NAT IP Address Type(NAT IP ア ドレス タイプ)		IPアドレス割り当ての種類を選択して、その NAT 実行デ バイスのパブリック インターフェースの IPアドレスまた は FQDN を指定するか、DDNS がアドレスを取得するよ うに指定します。これで、自動 VPN が、アドレスをハブ

レイヤー 3 イン ターフェイス設定	設定場所	の意味
		またはブランチのトンネル エンドポイントとして使用す ることができます。
		 Static IP (スタティック IP) – Type (タイプ)を IP Address (IPアドレス) または FQDNと選択して、IPv4 アドレスまたは FQDN を入力します。
		 DDNS–Dynamic DNS (DDNS) が、アップストリーム NAT デバイスの IPアドレスを取得します。
リンク速度	イーサネットインター	インターフェイス速度を 10、100、1000Mbps のいずれか から選択するか、 auto [自動] を選択します。
リンクデュプ レックス	- フェイス > 上級	インターフェイスの伝送モードを、フル デュプレックス (full)、ハーフ デュプレックス (half)、オート ネゴシエー ション (auto) から選択します。
リンク ステート	-	インターフェイスの状態を、有効 (up)、無効 (down)、自 動決定 (auto) から選択します。
管理プロファイ ル	イーサネッ トインター フェイス > 上級 > その 他の情報	このインターフェイスを介したファイアウォールの管理 に使用できるプロトコル (SSH、Telnet、HTTP など) を定 義するプロファイルを選択します。None[なし] を選択す ると、現在インターフェイスに割り当てられているプロ ファイルが解除されます。
MTU		このインターフェイスで送信されるパケットの最大転送 単位(MTU)をバイト数で入力します(576~9,192、 デフォルトは 1,500)。ファイアウォールの両側のマシ ンが Path MTU Discovery (PMTUD)を実行し、インター フェイスが MTU を超えるパケットを受信すると、ファイ アウォールが送信元にパケットが大きすぎることを示す ICMP フラグメント要求メッセージを返します。
TCP MSS の調整		ヘッダーのバイト数に対応できるようにインターフェイ スの MTU バイト サイズ以内の値で最大セグメント サイ ズ (MSS)を調整する場合は選択します。MTUバイトサ イズとMSS調整サイズはMSSバイトサイズと等しい値に なり、これはIPによって異なります。
		 IPv4 MSS Adjustment Size (IPv4 MSS調整サイズ) – 範囲は40~300、デフォルトは40です。
		 IPv6 MSS Adjustment Size (IPv6 MSS調整サイズ) – 範囲は60~300、デフォルトは60です。

レイヤー 3 イン ターフェイス設定	設定場所	の意味
		ネットワークを通るtunnel[トンネル]のMSSを小さくする 必要がある場合はこれらの設定を行ってください。フラ グメント化を行わないパケットのバイト数がMSSよりも 大きい場合、この設定を行うことでサイズが調整される ようになります。 カプセル化によりヘッダーが延長されるので、MSS調整 サイズはMPLSヘッダーやVLANタグを持つトンネルト ラフィックよりも大きく設定しておくことをお勧めしま
		す。
タグのないサブ インターフェイ ス		このレイヤー3インターフェイスに属するすべてのサ ブインターフェイスにタグを付けないように指定しま す。PAN-OS [®] は、パケットの宛先に基づいて、タグのな いサブインターフェイスを入力インターフェイスとして 選択します。宛先がタグのないサブインターフェイスの IP アドレスの場合は、サブインターフェイスにマッピン グされます。これは、反対方向のパケットで、送信元ア ドレスをタグのないサブインターフェイスの IP アドレス に変換する必要があることも示します。この分類メカニ ズムにより、すべてのマルチキャスト パケットとブロー ドキャスト パケットが、サブインターフェイスではなく 基本インターフェイスに割り当てられます。OSPF (Open Shortest Path First) ではマルチキャストを使用するため、 ファイアウォールはタグのないサブインターフェイスで OSPF をサポートしていません。
IPアドレス MAC アドレス	イーサネッ トインター フェイス > 上級 > ARP エントリ	1 つ以上のスタティック ARP(Address Resolution Protocol)エントリを追加するには、Add(追加)をク リックし、IP アドレスとそれに関連付けられたハード ウェア(MAC)のアドレスを入力します。エントリを削 除するには、エントリを選択して Delete[削除] をクリッ クします。静的 ARP エントリによって、指定したアドレ スの ARP 処理が減り、中間者攻撃が防止されます。
IPv6 アドレス MAC アドレス	イーサネッ トインター フェイス > 上級 > ND エントリ	NDP(Neighbor Discovery Protocol)のネイバー情報を指定するには、Add(追加)をクリックし、ネイバーの IP アドレスと MAC アドレスを入力します。
NDP プロキシの 有効化	イーサネッ トインター フェイス >	選択すると、インターフェイスで NDP(Neighbor Discovery Protocol)プロキシが有効になります。ファ イアウォールは、このリストの IPv6 アドレスの MAC ア ドレスを要求する ND パケットに応答します。ファイア

レイヤー 3 イン ターフェイス設定	設定場所	の意味
	上級 > NDP プロキシ	ウォールはND応答において、これらのアドレスに宛てら れたパケットに応答するプロキシとして機能することを 伝えるために、そのインターフェイスのMACアドレスを 送信します。
		NPTv6 (Network Prefix Translation IPv6) を使用する場合 は、Enable NDP Proxy[NDP プロキシの有効化] を選択す ることをお勧めします。
		Enable NDP Proxy[NDPプロキシの有効化]が選択され ている場合、検査文字列を入力し、フィルタの適用 (→
		をクリックすることで、膨大なアドレスエントリの絞込 を行うことができます。
アドレス	-	Add[追加] をクリックし、1 つ以上の IPv6 アドレス、IP 範囲、IPv6 サブネット、またはファイアウォールが NDP プロキシとして機能するアドレス オブジェクトを入力し ます。これらのアドレスの1つは、NPTv6 の送信元変換 のアドレスと同じであることが理想的です。アドレスの 順序は問題になりません。
		アドレスがサブネットワークの場合、ファイアウォール は、サブネットのすべてのアドレスに対してND応答を 送信します。したがって、ファイアウォールのIPv6ネイ バーも追加し、Negate[除外] を選択し、これらのIPアド レスに応答しないようにファイアウォールに指示するこ とをお勧めします。
Negate		あるアドレスに対して Negate [除外] チェック ボックスを オンにすると、NDPプロキシは、そのアドレスを拒否す るようになります。Negate は、指定した IP アドレス範囲 または IP サブネットの一部に対して実行できます。
LLDP の有効化	イーサネッ トインター フェイス > 上級 > LLDP	選択すると、インターフェイスでリンク レイヤー検出プ ロトコル (LLDP) が有効になります。LLDP は、リンク レ イヤーで機能し、隣接するデバイスとその機能を検出し ます。
LLDPプロファイ ル		LLDP が有効の場合は、インターフェイスに割り当てる LLDP プロファイルを選択するか、LLDP Profile(LLDP プロファイル)をクリックして新しいプロファイ ルを作成します(「Network(ネットワーク) > Network Profiles(ネットワーク プロファイル) > LLDP Profile(LLDP プロファイル)」を参照)。ファイア

)

レイヤー 3 イン ターフェイス設定	設定場所	の意味
		ウォールでグローバルなデフォルト設定を使用するよう に設定する場合はNone[なし] を選択します。
HAパッシブス テートを有効に する		LLDP が有効化されている場合はこのオプションを選択す ることで、パッシブなファイアウォールがアクティブに 切り替わる前に、もう一方のピアと LLDP 取り決めを行う ことを許可することができます。
設定	イーサネットインター	Settings (設定)を選択して DDNS フィールドを設定できる ようにします。
Enable [有効化]	フェイス > 上級 > DDNS	インターフェースで DDNS を有効化します。初めに DDNS を有効化してから設定を行う必要があります。 (DDNS の設定が終わっていない場合は有効化せずに保 存し、部分的な設定を保持することができます)
更新間隔(日 数)	-	FQDN にマッピングされた IP アドレスを更新するため にファイアウォールが DDNS サーバーに送信する更新間 隔(日数)を入力します(範囲は1~30、デフォルトは 1)。
		また、ファイアウォールはDHCP サーバー からインターフェイスの新しい IP アドレス を受診した際も DDNS を更新します。
証明書プロファ イル		証明書プロファイルを作成して DDNS サービスを検証し ます。DDNS サービスは、認証局(CA)が署名した証明 書をファイアウォールに提供します。
ホスト名		DDNS サーバーに登録されたインターフェイスのホスト 名 (例:host123.domain123.com、or host123) を入力し ます。DNS がドメイン名として許可している有効な文字 を使った構文になっていることを確認する以外、ファイ アウォールはホスト名の検証を行いません。
ベンダー	-	DDNS サービスをこのインターフェイスに提供する DDNS ベンダー(およびバージョン)を選択します。
		DuckDNS v1
		DynDNS v1
		 FreeDNS Afraid.org Dynamic API v1
		FreeDNS Afraid.org v1
		No-IP v1

レイヤー 3 イン ターフェイス設定	設定場所	の意味
		 Palo Alto Networks DDNS :SD-WAN AE インターフェ イスおよび SD-WAN レイヤ 3 サブインターフェイス に使用する必要があります。
		 ファイアウォールが特定の日で失効すると 示唆する DDNS サービスの古いバージョン を選択する場合、新しいバージョンに移動 させます。
		ベンダー名に続くName (名前)およびValue (値)フィールド は、ベンダー固有のものです。読み取り専用フィールド は、ファイアウォールが DDNS サービスに接続するため に使用するパラメーターを示しています。DDNS サービ スプロバイダーが提供するパスワード、DDNS サーバー からの応答がない場合にファイアウォールが使用するタ イムアウトなど、他のフィールドを設定します。
IPv4 タブ - IP	-	インターフェイスで設定した IPv4 アドレスを追加し、 それを選択します。選択されたすべての IP アドレスは DDNS プロバイダー(ベンダー)に登録されています。
IPv6 タブ - IPv6		インターフェイスで設定した IPv6 アドレスを追加し、 それを選択します。選択されたすべての IP アドレスは DDNS プロバイダー(ベンダー)に登録されています。
ランタイム情報 の表示		DDNS 登録を表示します: DDNS プロバイダー、解決さ れた FQDN、マッピングされた IPアドレス(アスタリス ク(*) はプライマリ IP アドレスを示します)。トラブル シューティングを目的として、各 DDNS プロバイダーに はホスト名の更新状態を示す独自の返却コードおよび返 却日が必要になります。

レイヤー3インターフェイス

Network > Interfaces > Ethernet [ネットワーク > インターフェイス > イーサネット]
 トラフィックをルーティングできるイーサネット レイヤー3 インターフェイスをコンフィグします。

レイヤー 3 イ ンターフェイ ス設定	設定場所	の意味
インターフェ イス名	レイヤ 3 イン ターフェイス	読み取り専用の Interface Name[インターフェイス名] フィー ルドには、選択した物理インターフェイスの名前が表示され ます。
コメント		インターフェースの分かりやすい説明を入力します。
インターフェ イスタイプ		[レイヤー 3] を選択します。
Netflow プロ ファイル		入力インターフェイスを通過する単向性の IP トラフィック を NetFlow サーバーにエクスポートする場合は、Netflow プロファイルを選択するか、Netflow Profile (Netflow プ ロファイル)を選択して新しいプロファイルを作成しま す(「Device (デバイス) > Server Profiles (サーバー プロファイル) > NetFlow」を参照)。None[なし]を 選択すると、現在インターフェイスに割り当てられてい るNetFlowサーバーが解除されます。
仮想ルー ター(VR)	レイヤ 3 イン ターフェイス > 設定	インターフェイスに仮想ルーターを割り当てるか、Virtual Router (仮想ルーター)をクリックして新しい仮想ルー ターを定義します (「Network (ネットワーク) > Virtual Routers (仮想ルーター)」を参照)。None[なし]を選択す ると、現在インターフェイスに割り当てられているルーター が解除されます。
論理ルーター		論理ルーターをインターフェースに割り当てるか、Logical Router をクリックして新しい論理ルーターを定義します (論 理ルーター>ネットワーク>ルーティング を参照)。None を 選択して、現在の論理ルーターの割り当てをインターフェイ スから削除します。
仮想システム		ファイアウォールが複数の仮想システムをサポートし、そ の機能が有効の場合は、インターフェースの仮想システム (vsys) を選択するか、virtual system (仮想システム - vsys) リ ンクを選択して新しい vsys を定義します。
セキュリティ ゾーン		インターフェース用のセキュリティゾーンを選択する か、Zone[ゾーン]を選択して新しいゾーンを定義しま す。None[なし] を選択すると、現在インターフェイスに割 り当てられているゾーンが解除されます。

レイヤー 3 イ ンターフェイ ス設定	設定場所	の意味
SD-WAN を 有効にする	レイヤ3イン ターフェイス > IPv4	SD-WAN を有効にする を選択して、イーサネット インター フェイスの SD-WAN 機能を有効にします。
Bonjour Reflector の 有効化		(PA-220、PA-800、および PA-3200 シリーズのみ) このオ プションを有効にすると、このオプションで受信および転送 された Bonjour マルチキャスト通知およびクエリを、このオ プションを有効にした他のすべての L3 および AE インター フェースとサブインターフェースにファイアウォールが転 送します。これにより、セキュリティまたは管理目的でトラ フィックをルーティングする際にセグメンテーションを採用 しているネットワーク環境でのユーザーアクセスおよびデバ イスの検出可能性を確保することができます。このオプショ ンは最大 16 のインターフェースで有効化することができま す。
IP	レイヤ 3 イン ターフェイス > IPv4, Type = Static	 を追加し、次の手順のいずれかを実行して、インターフェ イスまたは AE インターフェイスの静的 IP アドレスとネット ワークマスクを指定します。 CIDR (Classless Inter-Domain Routing) 表記法の <i>ip_address/mask</i> の形式(例: 192.168.2.0/24)でエントリ を入力します。 タイプが IP netmask[IP ネットマスク]の既存のアドレス オブジェクトを選択します。 タイプが IP netmask (IP ネットマスク)のアドレスオブ ジェクトを作成します。 インターフェイスに対して複数の IP アドレスを入力できま す。IP アドレスの最大数は、システムが使用する転送情報 ベース (FIB) によって決まります。 不要になった IP アドレスを Delete (削除)します。
Next Hop Gateway (ネ クストホップ ゲートウェ イ)		Enable SD-WAN(SD-WAN の有効化)を選択した場合 は、SD-WAN ゲートウェイの IPv4 アドレスを入力します。
有効化	レイヤ 3 イン ターフェイス > IPv4 > 一	Point-to-Point Protocol Over Ethernet (PPPoE)の終端のイン ターフェイスをアクティベートするには、Enable (有効)を 選択します。インターフェイスは、デジタル加入者線 (DSL) モデムはあるが接続を終了する他の PPPoE デバイスがない

レイヤー 3 イ ンターフェイ ス設定	設定場所	の意味
	般、タイプ = PPPoE	DSL 環境での接続をサポートする PPPoE 終端ポイントで す。
username	-	ISP がポイントツーポイント接続用に提供したユーザー名を 入力します。
パスワードと パスワードの 確認		パスワードを入力し、パスワードを確認します。
PPPoE クラ イアント ラ ンタイム情報 の表示		PPPoE インターフェイスに関する情報を選択して表示します。
認証	レイヤ 3 イン ターフェイス > IPv4 > 詳 細、タイプ = PPPoE	 認証方式を選択します。 CHAP-ファイアウォールは、PPPoE インターフェイス で Challenge Handshake Authentication Protocol (ハンド シェーク認証プロトコルのチャレンジ) -RFC-1994-を使 用します。 PAP-(デフォルト)ファイアウォールは、PPPoE イン ターフェイスで Password Authentication Protocol (パス ワード認証プロトコル - PAP)を使用します。PAP はユー ザー名とパスワードをプレーン テキストで送信するた め、CHAP よりも安全性が低くなります。 auto (自動) -ファイアウォールは、PPPoE サーバーと認 証方法 (CHAP または PAP) を交渉します。
スタティック アドレス		PPPoE サーバーから使用する IPv4 アドレスを要求しま す。PPPoE サーバーは、そのアドレスまたは別のアドレスを 割り当てる場合があります。
ピアを指す デフォルト ルートを自動 的に作成		PPPoE サーバーによって提供されるデフォルト ゲートウェ イを指し示すデフォルト ルートを自動的に作成する場合はこ のオプションを選択します。
デフォルト ルート メト リック		PPPoE 接続のデフォルト ルート メトリック (優先度レベル) を入力します (デフォルトは 10)。数値の低いルートほど、 ルート選択時の優先順位が高くなります。たとえば、メト

レイヤー 3 イ ンターフェイ ス設定	設定場所	の意味
		リックが 10 のルートは、メトリックが 100 のルートよりも 前に使用されます。
アクセス コ ンセントレー タ		ISP からアクセス コンセントレータの名前が提供されている 場合は、それを入力します。ファイアウォールは、IPS 側の このAccess Concentrator(アクセス コンセントレータ)に 接続します。これは、0 ~ 255 文字の文字列値です。
サービス		ファイアウォール (PPPoE クライアント) は、PPPoE サー バーに要求されたサービス要求を提供することが可能です。 これは、0 ~ 255 文字の文字列値です。
Passive		ファイアウォール (PPPoE クライアント) は、PPPoE サー バーが接続を開始するのを待ちます。これが有効化されてい ない場合、ファイアウォールは接続を開始します。
有効化	レイヤ3イン ターフェイス > IPv4、タイ プ = DHCP ク ライアント	インターフェイスがDynamic Address Group (ダイナミック ホスト コンフィグレーション プロトコル - DHCP) クライア ントとして機能し、ダイナミックに割り当てられた IPアドレ スを受信できるようにします。
サーバー提供 のデフォルト ゲートウェイ を指すデフォ ルト ルート を自動的に作 成		ファイアウォールがデフォルト ゲートウェイへのスタティッ ク ルートを作成する設定にするには、このオプションを選択 します。デフォルト ゲートウェイは、クライアントがファイ アウォールのルーティング テーブルでルートを維持する必要 がない多くの宛先にアクセスしようとしている場合に便利で す。
ホスト名の送 信		DHCP クライアント インターフェイスにホスト名を割り 当て、そのホスト名 (オプション 12) を DHCP サーバーに 送信するには、このオプションを選択します。DHCP サー バーは、ホスト名を DNS サーバーに登録できます。その 後、DNS サーバーがホスト名から動的 IP アドレスへの解決 を自動的に管理できるようになります。外部ホストがホス ト名に基づいてインターフェイスを識別できる必要があり ます。デフォルトの値は system-hostname であり、これ はDevice (デバイス) > Setup (セットアップ) > Management (管理) > General Settings (一般設定) でユーザーが設定する

レイヤ ー3 イ ンターフェイ ス設定	設定場所	の意味
		ファイアウォールのホスト名です。または、大文字と小文 字、数字、ピリオド、ハイフン、下線を含む最大 64 文字で インターフェイスのホスト名を入力することができます。
デフォルト ルート メト リック	レイヤ 3 イン ターフェイス > IPv4 、タイ プ = DHCP ク ライアント	ファイアウォールと DHCP サーバー間のルートのデフォル ト ルート メトリック (優先順位レベル) を入力します (範囲は 1~65535、デフォルト メトリックなし)。数値の低いルー トほど、ルート選択時の優先順位が高くなります。たとえ ば、メトリックが 10 のルートは、メトリックが 100 のルー トよりも前に使用されます。
DHCP クライ アント ラン タイム情報の 表示		DHCP リース ステータス、ダイナミックIP アドレスの割 り当て、サブネット マスク、ゲートウェイ、サーバー設定 (DNS、NTP、ドメイン、WINS、NIS、POP3、SMTP)等、ク ライアントが DHCP サーバーから継承したすべての設定を 表示する場合は、このオプションを選択します。
インター フェースでの IPv6 の有効 化	レイヤ 3 イン ターフェイス > IPv6	このインターフェイスの IPv6 アドレスを有効にする場合に 選択します。
SD-WAN を 有効にする		SD-WAN を有効にする を選択して、イーサネット インター フェイスの SD-WAN 機能を有効にします。
インターフェ イス ID		64 ビット拡張一意識別子 (EUI-64) を 16 進数形式で入力し ます (00:26:08:FF:FE:DE:4E:29 など)。このフィールドを空白 のままにすると、ファイアウォールが、物理インターフェイ スの MAC アドレスから生成された EUI-64 を使用します。 アドレスの追加時に Use interface ID as host portion[ホスト 部分にインターフェイス ID を使用] オプションを選択する と、ファイアウォールがそのアドレスのホスト部分にイン ターフェイス ID を使用します。
アドレス	レイヤ 3 イン ターフェイス > IPv6 > アド レス割り当 て、タイプ = 静的	IPv6 アドレスとプレフィックス長を追加します (2001:400:f00::1/64 など)。または、既存の IPv6 アドレス オブジェクトを選択するか、新しい IPv6 アドレス オブジェ クトを作成します。
インターフェ イス上のアド レスを有効に する		インターフェースで IPv6 アドレスを有効化します。

レイヤー 3 イ ンターフェイ ス設定	設定場所	の意味
ホスト部分に インターフェ イス ID を使 用		IPv6 アドレスのホスト部分に Interface (インターフェイス) ID を使用する場合に選択します。
エニーキャス ト	-	最も近いノードを経由するルーティングを含める場合に選択 します。
Next Hop Gateway (ネ クストホップ ゲートウェ イ)		変数を選択するか、ネクストホップゲートウェイの IPv6 ア ドレスを入力します。
ルーター通知 を送信	レイヤ 3 イン ターフェイス > IPv6 > アド レス割り当 て、タイプ = 静的	この IP アドレスのルーター通知 (RA) を有効にする場合に選 択します。(インターフェイスのグローバルの Enable Router Advertisement[ルーター通知を有効化する] オプションも 有効化しておく必要があります)。RA の詳細は、この表の 「Enable Router Advertisement (ルーター通知を有効にす る)」を参照してください。以下のフィールドは Enable Router Advertisement (ルーター通知を有効にする) 場合にの み適用されます。
		 Valid Lifetime (有効なライフタイム)–ファイアウォールが アドレスを有効とみなす時間(秒)です。有効なライフタ イムは、Preferred Lifetime[優先ライフタイム]以上でな ければなりません。デフォルトは2,592,000です。
		 Preferred Lifetime (優先ライフタイム)-有効なアドレス が優先される時間(秒)です。この時間内は、ファイア ウォールがこのアドレスを使用してトラフィックを送受 信できます。優先ライフタイムの期限後は、ファイア ウォールがこのアドレスを使用して新しい接続を確立す ることはできませんが、既存の接続は Valid Lifetime (有 効なライフタイム)の期限まで有効です。デフォルトは 604,800です。
		 On-link(オンリンク) – プレフィックス内にアドレスが あるシステムにルーターなしで到達可能である場合に選 択します。
		 Autonomous(自律型) – 通知されたプレフィックスと インターフェイス ID を組み合わせて、システムが IP アド レスを独自に作成できる場合に選択します。

レイヤー 3 イ ンターフェイ ス設定	設定場所	の意味
ルーターがア ドバタイズし たルートを受 け入れる	レイヤ 3 イン ターフェイス > IPv6 > アド レス割り当 て、タイプ = DHCPv6 クラ イアント	DHCPv6 クライアントが DHCPv6 サーバからの RA を受け 入れることを許可する場合に選択します。
デフォルト ルート メト リック		インターフェイスから ISP へのルートのデフォルト ルート メトリックを入力します。範囲は 1 から 65,535 です。デ フォルトは 10 です。
優先		DHCPv6 クライアント インターフェイス (low、medium、 または high) のプリファレンスを選択して、2 つのインター フェイス (それぞれが冗長性のために異なる ISP に接続され ている) がある場合に、一方の ISP のインターフェイスにも う一方の ISP のインターフェイスよりも高い優先順位を割り 当てることができます。優先インターフェイスに接続され ている ISP は、ホスト側のインターフェイスに送信するデリ ゲートされたプレフィックスを提供する ISP になります。イ ンターフェイスのプリファレンスが同じ場合、両方の ISP が 委任されたプレフィックスを提供し、ホストが使用するプレ フィックスを決定します。
IPv6 アドレ スを有効にす る	レイヤ 3 イン ターフェイス > IPv6 > アド レス割り当 て、タイプ = DHCPv6 ク ライアント > DHCPv6 オプ ション	この DHCPv6 クライアント用に受信した IPv6 アドレスを有 効にします。
非一時アドレス		ファイアウォールの非一時アドレスを、委任側ルータと ISP に面するこの DHCPv6 クライアント インターフェイスに割 り当てるように要求します。(このアドレスタイプは、一時 アドレスよりも寿命が長くなります)。
一時アドレス		委任ルータと ISP に面するこの DHCPv6 クライアント イン ターフェイスに割り当てるファイアウォールの一時アドレス を要求します。[一時アドレス] を選択すると、アドレスが短

レイヤー 3 イ ンターフェイ ス設定	設定場所	の意味
		期間使用されることを意図しているため、セキュリティのレ ベルが高くなります。
迅速なコミッ ト		Solicit、Advertise、Request、および Reply メッセージのプロセスではなく、Solicit および Reply メッセージの DHCP プロセスを使用する場合に選択します。
プレフィック ス委任を有効 にする	レイヤ3イン ターフェイス > IPv6 > アド レス割りプ = DHCPv6 クラ イアント > プ レフィックス 委任	プレフィックス委任を有効にして、ファイアウォールがプレ フィックス委任機能をサポートできるようにします。つま り、インターフェイスはアップストリーム DHCPv6 サーバ からプレフィックスを受け入れ、選択したプレフィックス プールにプレフィックスを配置し、そこからファイアウォー ルが RA 経由でホストにプレフィックスを委任します。イン ターフェイスのプレフィックス委任を有効または無効にする 機能により、ファイアウォールは複数の ISP (インターフェ イスごとに 1 つの ISP)をサポートできます。このインター フェイスでプレフィックス委任を有効にすると、プレフィッ クスを提供する ISP が制御されます。
DHCP プレ フィックス長 のヒント		選択すると、ファイアウォールが優先 DHCPv6 プレフィッ クス長を DHCPv6 サーバに送信できるようになります。
DHCP プレ フィックス長 (ビット)		 DHCPv6 サーバにヒントとして送信される優先 DHCPv6 プレフィックス長を 48 ~ 64 ビットの範囲で入力しま す。DHCPv6 サーバには、選択したプレフィックス長を送信 する裁量権があります。 たとえば、プレフィックス長 48 を要求する と、サブネット (64-48) に 16 ビットが残り、 委任するにはそのプレフィックスの多くのサブ ディビジョンが必要であることを示します。一 方、プレフィックス長 63 を要求すると、2つ のサブネットのみを委任するために 1 ビットが 残ります。128ビットのうち、ホストアドレス 用にさらに64ビットあります。インターフェ イスは /48 プレフィックスを受け取ることがで きますが、たとえば /64 プレフィックスをデリ ゲートします。これは、ファイアウォールがデ リゲーションするプレフィックスを細分化して いることを意味します。

レイヤー 3 イ ンターフェイ ス設定	設定場所	の意味
プレフィック ス プール名		 ファイアウォールが受信したプレフィックスを保存するプレフィックス プールの名前を入力します。名前は一意で、最大 63 文字の英数字、ハイフン、ピリオド、およびアンダースコアを含む必要があります。 認識しやすいように、ISP を反映したプレフィックス プール名を使用します。
Enable [有効 化]	Enable [有効 化] IPv4 パラ メータを適用 する レイヤ 3 イン ターフェイス > IPv6 > タイ プ = PPPoEv6 クライアント > 一般	そのインターフェイスを有効化します。
IPv4 パラ メータを適用 する		既に PPPoE クライアント (IPv4) 用のインターフェースが設 定されている場合は、オプションで PPPoEv6 クライアント に IPv4 パラメーターを適用できます。(コピーされるパラ メータは、認証タイプ、ユーザー名、パスワード、アクセス コンセントレータ名、サービス、パッシブ設定です)。
		その後、PPPoE IPv4 クライアントでパラメータを再設定す ると、新しい設定が PPPoE IPv6 クライアントにコピーされ ます。いずれかのクライアントのパラメータを再設定する と、セッションが再確立され、トラフィックが中断されま す。
		PPPoE IPv4 クライアントと PPPoE IPv6 クライアントを個 別に構成する場合でも、2 つのクライアントに同じ認証タイ プ、ユーザー名、パスワード、アクセスコンセントレータ 名、サービス、パッシブ設定を設定する必要があります。
Passive		PPPoEv6 クライアント (インターフェイス) に PPPoEv6 サー バーが接続を開始するまで待機させたい場合は、[Passive (パッシブ)] を選択します。Passiveが選択されていない場 合、インターフェースは接続を開始できます。
認証	-	インターフェースの認証タイプを選択します。
		 CHAP:ファイアウォールは Challenge Handshake Authentication Protocol (CHAP)を使用します。
		 PAP – (デフォルト) インターフェイスはパスワード認証 プロトコル (PAP) を使用します。PAP はユーザー名とパ スワードをプレーンテキストで送信するため、CHAP より も安全性が低くなります。
		 auto (自動): インターフェイスが PPPoEv6 サーバと認証 方法(CHAP または PAP)をネゴシエートします。

レイヤー 3 イ ンターフェイ ス設定	設定場所	の意味
		このインターフェイスを PPPoE IPv4 クライアントとしても 設定した場合は、2 つのクライアントに同じ認証タイプ、 ユーザー名、パスワード、アクセスコンセントレータ名、お よびサービスを設定する必要があります。
username		認証用のユーザー名を入力します。
パスワードと パスワードの 確認		パスワードを入力し、パスワードを確認します。
アクセス コ ンセントレー タ		接続するアクセスコンセントレータの名前を ISP から指示 された場合は、その名前を入力します (0 ~ 255 文字の文字 列)。
サービス		インターフェイスを PPPoEv6 クライアントとして PPPoEv6 サーバーに特定のサービスを要求する場合は、サービスを入 力します (0 ~ 255 文字の文字列)。
ルーターがア ドバタイズし たルートを受 け入れる	レイヤ 3 イン ターフェイス > IPv6 > タイ プ = PPPoEv6	PPPoEv6 クライアントがルーターアドバタイズメント (RA) を受け入れることを許可するように選択します。
デフォルト ルート メト リック	>フィアント >アドレス割 り当て	インターフェイスから ISP へのルータのデフォルトルートメ トリックを指定します。範囲は 1 ~ 65,535、デフォルトは 10 です。
優先		PPPoE クライアントインターフェイスのプリファレンスを 設定します。高 (デフォルト)、中、または低。インターフェ イスが 2 つある (冗長性のためにそれぞれ異なる ISP に接続 されている)場合は、一方の ISP のインターフェイスに、他 方の ISP のインターフェイスよりも高い優先順位を割り当て ることができます。優先インターフェイスに接続されている ISP は、ホスト側のインターフェイスに送信するデリゲート されたプレフィックスを提供する ISP になります。クライア ントのインターフェイスのプリファレンスが同じ場合、両方 の ISP が委任されたプレフィックスを提供し、ホストが使用 するプレフィックスを決定します。
自動構成を有 効にする	レイヤ 3 イン ターフェイス > IPv6 > タイ	選択すると、IPv6 制御プロトコル (IPv6CP) インターフェイ ス識別子と RA からのプレフィックス (SLAAC を使用) を使用
レイヤー 3 イ ンターフェイ ス設定	設定場所	の意味
----------------------------------	---	--
	プ = PPPoEv6 クライアント > アドレス割 り当て > オー トコンフィグ	して、PPPoEv6 クライアントインターフェイスの IPv6 アド レスがファイアウォールに自動設定されます。
Enable [有効 化]	レイヤ3イン ターフェイス > IPv6 > タイ プ = PPPoEv6 クライアン ト > アドレ ス割り当て > DHCPv6	PPPoEv6 クライアントが DHCPv6 を使用できるようにします。
IPv6 アドレ スを有効にす る	レイヤ3イン ターフェイス > IPv6 > タイ	PPPoEv6 クライアントが DHCPv6 サーバーによって割り当 てられたアドレスを使用できるようにします。
迅速なコミッ ト	プ = PPPoEv6 クライアン ト > アドレ ス割り当て > DHCPv6 > DHCPv6 オプ ション	DHCPv6のプロセスとし て、Solicit、Advertise、Request、Replyの4メッセージでは なく、SolicitとReplyの2メッセージを使用することを選択し ます。
DUID タイプ		インターフェイスが DHCPv6 サーバーに対して自身を識別 するために使用する DHCPv6 固有識別子 (DUID) タイプを選 択します。
		 DUID-LLT-タイムスタンプで連結されたインターフェイスのリンクレイヤアドレス。 DUID LL インターフェイスのリンク層マドレス
		 DUID-LLーインターノエイスのリンク増ブトレス。
プレフィック ス委任を有効 にする	レイヤ3イン ターフェイス > IPv6 > タイ プ = PPPoEv6 クライアン ト > アドレ ス割り当て > DHCPv6 > プ レフィックス 委任	アドレス割り当てに DHCPv6 を選択した場合は、[Prefix Delegation (プレフィックス委任)] と [Enable Prefix Delegation (プレフィックス委任を有効にする)] を選択しま す。つまり、インターフェイスはアップストリーム DHCPv6 サーバからプレフィックスを受け入れ、そのプレフィックス をプレフィックス プールに配置し、そこからファイアウォー ルが RA 経由でホストにプレフィックスを委任します。イン ターフェイスのプレフィックス委任を有効または無効にする 機能により、ファイアウォールは複数の ISP (インターフェ イスごとに 1 つの ISP) をサポートできます。このインター フェイスでプレフィックス委任を有効にすると、プレフィッ

レイヤー 3 イ ンターフェイ ス設定	設定場所	の意味
		クスを提供する ISP が制御されます。委任されたプレフィッ クスはホスト側のインターフェイスで使用され、その IPv6 アドレスは MAC アドレスと EUI-64 入力で構成されます。
DHCP プレ フィックス長 のヒント		選択すると、ファイアウォールが優先 DHCPv6 プレフィッ クス長を DHCPv6 サーバに送信できるようになります。
DHCP プレ フィックス長 (ビット)		DHCPv6 サーバに送信させたい DHCPv6 プレフィックスの 長さを入力します。範囲は 0 ~ 128 で、デフォルトは 48 で す。DHCPv6 サーバには、選択したプレフィックス長を送信 することが可能です。
		たとえば、プレフィックス長 48 を要求する と、サブネット (64-48分) に 16 ビットが残 り、委任するにはそのプレフィックスの多く のサブディビジョンが必要であることを示しま す。プレフィックス長 63 を要求すると、2つ のサブネットのみを委任するために 1 ビットが 残ります。128ビットのうち、ホストアドレス 用にさらに64ビットあります。
		インターフェイスは /48 プレフィックスを受け取ることができますが、たとえば /64 プレフィックスをデリゲートします。これは、ファイアウォールがデリゲーションするプレフィックスを細分化していることを意味します。
プレフィック ス プール名		ファイアウォールが受信したプレフィックスを保存するプー ルのプレフィックスプール名を入力します。名前は一意で、 最大 63 文字の英数字、ハイフン、ピリオド、およびアン ダースコアを含む必要があります。
		○ 認識してすいように、「」」を反映したフレ フィックスプール名を使用します。
名前	レイヤ3イン ターフェイス	プール名 (最大 63 文字の英数字、ハイフン、ピリオド、アン ダースコア) を入力してプールを追加します。
アドレス タ イプ	> IPVO > アト レス割り当 て、タイプ = 継承	以下のうち1つを選択します。 • GUA from Pool:選択されたプレフィックス プールからの グローバル ユニキャスト アドレス(GUA)。

レイヤー 3 イ ンターフェイ ス設定	設定場所	の意味
		 ULA–Unique Local Address は、プライベート ネットワー ク内の接続用のアドレス範囲 fc00::/7 のプライベート ア ドレスです。DHCPv6 サーバーがない場合は、ULA を選 択します。
インターフェ イスで有効に する		インターフェイスでアドレスを有効にします。
プレフィック ス プール		GUA を取得するプレフィックス プールを選択します。
割り当てタイ プ	レイヤ 3 イン ターフェイス > IPv6 > アド レス割り当 て、タイプ= 継承	 割り当てタイプを選択します。 Dynamic:DHCPv6 クライアントは、継承されたインターフェイスを構成するための識別子を選択します。 Dynamic with Identifier - 0 から 4,000 の範囲の識別子を選択し、DHCPv6 クライアント全体で一意の識別子を維持する責任があります。
ルーター通知 を送信		インターフェイスから LAN ホストにルータ アドバタイズメ ント(RA)を送信する場合に選択します。
オンリンク		プレフィックス内にアドレスを持つシステムがルーターなし で到達できるかどうかを選択します。
自主的な		システムが、アドバタイズされたプレフィックスとインター フェイス ID を組み合わせて IPv6 アドレスを個別に作成でき るかどうかを選択します。
Duplicate Address Detection (重 複アドレス検 出) を有効に する	レイヤ3イ ンターフェ イス > IPv6 > Address Resolution (アドレス解 決)	重複アドレス検出(DAD)を有効にする場合に選択し、セク ション内の他のフィールドの設定を行います。
DAD 試行回 数		ネイバー要請間隔 (NS Interval (NS 間隔)) の内にDADを試 行する回数を指定します(範囲は 1 ~ 10、デフォルトは 1)。この回数を超えるとネイバーに障害があるとみなされ ます。

レイヤー 3 イ ンターフェイ ス設定	設定場所	の意味	
Reachable Time (到達可 能時間) (秒)		クエリと応答が正常に行われた後引き続きネイバーに到達可 能な時間(秒)を指定します(範囲は1~36,000、デフォ ルトは30)。	
NS 間隔 (秒)		失敗が示されるまでの DAD 試行の秒数を指定します (範囲は 1 から 3,600、デフォルトは 1)。	
NDP モニタ リングの有効 化		NDP(Neighbor Discovery Protocol)モニ タリングを有効にする場合に選択します。 有効にすると、NDP(Features(機能)列 の を選択し、IPv6 アドレス、対応する MAC アドレス、ユー ザー ID(ベストケース ベースの場合)等、ファイアウォー ルが検出したネイバーに関する情報を表示することができま す。)
ルーター通知 を有効にする	レイヤ 3 イン ターフェイス > IPv6 > ルー ターアドバ タイズメン ト、タイプ = 静的またはタ イプ = 継承	ネイバー検出を IPv6 インターフェイスで提供するには、こ のセクションのその他のフィールドを選択して設定します。 ルーター通知 (RA) メッセージを受信する IPv6 DNS クライ アントは、この情報を使用します。 RA により、ファイアウォールが、スタティックに設定さ れていない IPv6 ホストのデフォルト ゲートウェイとして 機能し、ホストにアドレス設定の IPv6 プレフィックスを提 供できます。別の DHCPv6 サーバーをこの機能と併用する と、DNS および他の設定をクライアントに提供できます。 これはインターフェイスのグローバル設定です。IP アド レスごとに RA オプションを設定する場合は、IP アドレス テーブルの IPv6 アドレスを Add (追加) してコンフィグしま す。IPv6 アドレスに RA オプションを設定する場合は、イン ターフェイスの Enable Router Advertisement (ルーター通知 を有効にする) 必要があります。	
最小間隔(秒)		ファイアウォールが送信する RA 間の最小間隔(秒)を指定 します(範囲は 3 ~ 1,350、デフォルトは 200)。ファイア ウォールは、コンフィグした最小値と最大値の間のランダム な間隔で RA を送信します。	
最大間隔(秒)		ファイアウォールが送信する RA 間の最大間隔(秒)を指定 します(範囲は 4 ~ 1,800、デフォルトは 600)。ファイア ウォールは、コンフィグした最小値と最大値の間のランダム な間隔で RA を送信します。	

レイヤー 3 イ ンターフェイ ス設定	設定場所	の意味
ホップ制限		送信パケットのクライアントに適用するホップ制限を指定す る (範囲は 1 ~ 255、デフォルトは 64)、 または unspecified (未指定)を選択します。これはシステムのデフォルトにマッ ピングされます。
リンク MTU	レイヤ3イン ターフェイス > IPv6 > ルー ターアドバ タイズメン	クライアントに適用するリンク最大伝送単位 (MTU) を 指定する (範囲は 1,280 ~ 1,500)、またはデフォルトで unspecified (未指定)に指定します。これはシステムのデフォ ルトにマッピングされます。
到達可能時間 (ミリ秒)	- タイスメン ト、タイプ = 静的またはタ イプ = 継承	到達可能確認メッセージを受信後ネイバーに到達可能である と想定する際にクライアントが使用する到達可能時間 (ミリ 秒)を指定します (範囲は 0 ~ 3,600,000) またはデフォルト の unspecified (未指定)に指定します。これはシステムのデ フォルトにマッピングされます。
リトランス ミッション時 間 (ミリ秒)		ネイバー要請メッセージを再送信するまでにクライアントが 待機する時間 (ミリ秒単位) を決定するリトランスミッション タイマーを指定します (範囲は 0 ~ 4,294,967,295) またはデ フォルトの unspecified (未指定)に指定します。これはシステ ムのデフォルトにマッピングされます。
ルーターの有 効期間 (秒)		クライアントがファイアウォールをデフォルトゲートウェ イとして使用する時間を秒単位で指定します(範囲は 0 ~ 9,000、デフォルトは 1,800)。0は、ファイアウォールがデ フォルト ゲートウェイではないことを示します。有効期間が 過ぎると、クライアントがそのデフォルト ルーター リスト からファイアウォール エントリを削除して、別のルーターを デフォルト ゲートウェイとして使用します。
ルーター設定		ネットワーク セグメントに複数の IPv6 ルーターがある場合 は、クライアントがこのフィールドを使用して優先ルーター を選択します。セグメントの他のルーターとの比較におい て、RA が通知するファイアウォール ルーターの優先度を High、Medium (デフォルト)、Low の中から選択します。
管理された設 定	レイヤ3イン ターフェイス > IPv6 > ルー ターアドバ タイズメン ト、タイプ=	アドレスを DHCPv6 経由で使用できることをクライアント に示す場合に選択します。
その他の設定		他のアドレス情報(DNS 関連の設定など)を DHCPv6 経由 で使用できることをクライアントに示す場合に選択します。

レイヤ ー3 イ ンターフェイ ス設定	設定場所	の意味
整合性チェッ ク	静的またはタ イプ = 継承	他のルーターから送信された RA がリンク上で一貫した情報 を通知していることをファイアウォールで確認する場合に選 択します。ファイアウォールでは、システム ログの不一致が 記録されます。タイプは ipv6nd です。
ルーター通知 に DNS 情報 を含める	レイヤ 3 イン ターフェイス > IPv6 > DNS サポート、タ イプ = 静的	DNS サポートは、[ルーター アドバタイズメント] タブで Enable Router Advertisement を選択した場合に使用できま す。 ファイアウォールがこの IPv6 イーサネット インターフェイ スから NDP ルーター通知で DNS 情報を送信するように選 択します。その他の DNS サポート フィールド(Server (サー バー)、Lifetime (ライフタイム)、Suffix (サフィックス)、およ びLifetime (ライフタイム) は、このオプションを選択した後 にのみ表示されます。
SERVER		 1つ以上の再帰 DNS (RDNS) サーバー アドレスを Add (追加) し、ファイアウォールがこの IPv6 Ethernet インターフェイスから NDP ルーター通知によって送信できるようにします。RDNS サーバーは、一連の DNS ルックアップ要求をルート DNS および権威 DNS サーバーに送信し、最終的にIP アドレスを DNS クライアントに提供します。 最大 8 個の RDNS サーバーを設定し、ファイアウォールでNDP ルーター通知に含めて受信者に送信できます(設定の上から下の順に送信します)。その後、受信者は同じ順序でこれらを使用できます。サーバーの順序を変更するには、サーバーを選択して Move Up (上へ)移動したり Move Down (下へ)移動したりします。サーバーが必要なくなったら、そのサーバーをリストから Delete (削除) します。
有効期間		IPv6 DNS クライアントがルーター通知を受信した後 で、RDNS サーバーを使用してドメイン名を解決できるよう になるまでの最長時間 (秒) を入力します (範囲はMax Interval (最大間隔) (秒)からMax Interval (最大間隔) (秒)の 2 倍、デ フォルトは 1,200)。
ドメイン検索 リスト	レイヤ 3 イン ターフェイス > IPv6 > DNS サポート、タ イプ = 静的	DNS 検索リスト (DNSSL) のドメイン名 (サフィックス) を1つ以上 Add (追加) します。最大長は255 バイトです。 DNS 検索リストは、DNS クライアント ルーターが DNS ク エリに名前を入力する前に非修飾ドメイン名に (1つずつ) 追加するドメイン サフィックスのリストです。これによ り、クエリで完全修飾ドメイン名が使用されます。たとえ

レイヤ ー3 イ ンターフェイ ス設定	設定場所	の意味
	レイヤ 3 イン ターフェイス > IPv6 > DNS のサポート	ば、DNS クライアントがサフィックスのない「quality」と いう名前の DNS クエリを送信しようとすると、ルーターは ピリオドと DNS 検索リストの最初の DNS サフィックスを 名前に追加して DNS クエリを送信します。リストの最初の DNS サフィックスが「company.com」の場合、ルーターの クエリの完全修飾ドメイン名は「quality.company.com」に なります。
		DNS クエリに失敗すると、ルーターはリストの2番目の DNS サフィックスを非修飾名に追加して、新しい DNS クエ リを送信します。ルーターは、DNS ルックアップが成功す るまで(残りのサフィックスは無視)、またはルーターがリ ストのすべてのサフィックスを試すまで、DNS サフィック スを使用します。
		ネイバー検出 DNSSL オプションで DNS クライアント ルー ターに提供するサフィックスにより、ファイアウォールを設 定します。DNSSL オプションを受信する DNS クライアント は非修飾 DNS クエリでそのサフィックスを使用します。
		NDP ルーターアドバタイズメントとしてファイアウォール が上から順に送信するDNS検索リストオプションには、最 大8つのドメイン名(サフィックス)を設定できます。受信 者は同じ順番でこれを使用します。順序を変更するには、サ フィックスを選択して Move Up(上へ)移動したり Move Down(下へ)移動したりします。サフィックスが必要なく なったら、そのサフィックスを Delete(削除)します。
有効期間		IPv6 DNS クライアントがルーター通知を受信した後 に、DNS 検索リストのドメイン名 (サフィックス) を使用で きる最大秒数を入力します (範囲はMax Interval (最大間隔) (秒)の値からMax Interval (最大間隔) (秒)の 2 倍までで、デ フォルトは 1,200 です)。
DNS 再帰 ネーム サー バー	レイヤ 3 イ ンターフェ イス > IPv6 > DNS サポー ト、タイプ = DHCPv6 クライアン ト、PPPoEv6 クライアン	 以下を有効にして選択します。 DHCPv6:DHCPv6 サーバに DNS 再帰ネーム サーバ情報 を送信させます。 Manual:DNS 再帰ネーム サーバを手動で設定します。 Manual, Add を選択した場合、firewall がこの IPv6 VLAN インターフェースから NDP ルーター通知 を送信するために、再帰 DNS (RDNS) Server (例え ば、2001:4860:4860:0:0:8888) の IPv6 アドレス。RDNS サーバーは、ルート DNS サーバーと権限のある DNS サー

レイヤー 3 イ ンターフェイ ス設定	設定場所	の意味
	ト、または継 承	バーに一連の DNS ルックアップ要求を送信し、最終的に DNS クライアントに IP アドレスを提供します。
		最大 8 個の RDNS サーバーを設定し、ファイアウォールで それらを NDP ルーター通知に含めて受信者に送信できます (設定の上から下の順に送信します)。その後、受信者は 同じ順序でこれらを使用できます。サーバーの順序を変更す るには、サーバーを選択して Move Up(上へ)移動したり Move Down(下へ)移動したりします。サーバーが必要な くなったら、そのサーバーをリストから Delete(削除)しま す。クライアントが特定の RDNS サーバーを使用してドメイ ン名を解決できる最大時間である Lifetime を秒単位で入力し ます。範囲は 4 から 3,600 です。デフォルトは 1,200 です。
ドメイン検索 リスト	レイヤ 3 イ ンターフェ	以下を有効にして選択します。
2201	イス > IPv6 >	• DHCPv6 - DHCPv6 サーバーにドメイン検索リスト情報を 送信させます。
	ト、タイプ = DHCPv6	 Manual (手動) - ドメイン検索リストを手動で構成します。
	クライアン ト、 PPPoEv6 クライアン ト、または継 承	[Manual (手動)]、[Add (追加)] を選択し、DNS 検索リスト (DNSSL) に 1 つ以上の [Domain (ドメイン)] 名(サフィック ス)を設定する場合。サフィックスの最大長は 255 バイトで す。
		DNS 検索一覧は、DNS クライアント ルーターが DNS クエ リに名前を入力する前に非修飾ドメイン名に (一度に 1つ ずつ) 追加するドメイン サフィックスの一覧であり、DNS クエリで完全修飾ドメイン名を使用します。たとえば、 サフィックスなしの「quality」という名前の DNS クエリ を DNS クライアントが送信しようとしています。この場 合、ルーターはピリオドと、DNS 検索リストの 1 番目の DNS サフィックスを名前に付加し、DNS クエリを転送しま す。リストの最初の DNS サフィックスが「company.com」 の場合、ルータからの DNS クエリは完全修飾ドメイン名 「quality.company.com」に対するものです。
		DNS クエリが失敗した場合、ルータはリストの2番目の DNS サフィックスを非修飾名に追加し、新しい DNS クエリ を送信します。ルータは、DNS ルックアップが成功する(残 りのサフィックスを無視する)か、ルータがリスト上のすべ てのサフィックスを試行するまで、DNS サフィックスを試 みます。

レイヤー 3 イ ンターフェイ ス設定	設定場所	の意味
		近隣探索 DNSSL オプションで DNS クライアント ルーター に提供するサフィックスを使用してファイアウォールを構 成します。DNSSL オプションを受信する DNS クライアント は、非修飾 DNS クエリでサフィックスを使用します。
		クライアントが特定のドメイン検索リストを使用できる最大 時間である Lifetime を秒単位で入力します。範囲は 4 から 3,600 です。デフォルトは 1,200 です。
		ファイアウォールが NDP ルータ アドバタイズメントで受 信者に送信する DNS 検索リストには、最大 8 つのドメイン 名(サフィックス)を設定できます。不要になったサフィック スをリストから削除します。
SD-WAN イ ンターフェイ ス ステータ ス	レイヤ 3 イン ターフェイス > SD-WAN	IPv4 タブで SD-WAN を有効にする を選択すると、ファイ アウォールは SD-WAN インターフェイス ステータスを表示 します。有効。Enable SD-WAN (SD-WANの有効化)を実 行しなかった場合、Disabled (無効化)と表示されます。
SD-WAN イ ンターフェイ ス プロファ イル		このイーサネット インターフェースに適用する SD-WAN インターフェイス プロファイルを選択するか、新しい SD- WAN インターフェース プロファイルを追加します。
		SD-WAN インターフェイス プロファイルを適用する前に、インターフェイスの SD-WAN を 有効にする 必要があります。
Upstream NAT (アップ ストリーム NAT)	-	NAT を実行するデバイスが背後で SD-WAN ハブまたはブラ ンチが存在する場合は、ハブまたはブランチのアップスト リーム NAT をEnable(有効化)にします。
NAT IP Address Type(NAT IP アドレス タイプ)		IPアドレス割り当ての種類を選択して、その NAT 実行デ バイスのパブリック インターフェースの IPアドレスまたは FQDN を指定するか、DDNS がアドレスを取得するように指 定します。これで、自動 VPN が、アドレスをハブまたはブ ランチのトンネル エンドポイントとして使用することができ ます。
		 Static IP (スタティック IP) – Type (タイプ) を IP Address (IPアドレス) または FQDNと選択して、IPv4 ア ドレスまたは FQDN を入力します。

レイヤー 3 イ ンターフェイ ス設定	設定場所	の意味
		 DDNS–Dynamic DNS (DDNS) が、アップストリーム NAT デバイスの IPアドレスを取得します。
リンク速度	イーサネット インターフェ イス > 上級 >	インターフェイス速度を Mbps 単位で選択するか、auto を 選択してファイアウォールが自動的に速度を決定するように します。
リンクデュプ レックス	リンク設定	インターフェイスの伝送モードを、フル デュプレックス (full)、ハーフ デュプレックス (half)、オート ネゴシエーショ ン (auto) から選択します。
リンク ス テート		インターフェイスの状態を、有効 (up)、無効 (down)、自動決 定 (auto) から選択します。
PoE Rsvd Pwr	イーサネット インターフェ イフ 、 ト級 、	PoE が有効になっている場合、割り当てられる電力量を Watts で選択します。
PoE イネーブ ル	- イス > 上級 > PoE 設定 (サポートさ れているファ イアウォール のみ)	このインターフェイスで PoE を有効にする場合に選択しま す。
管理プロファ イル	レイヤ 3 イン ターフェイス > 上級 > その 他の情報	このインターフェイスを介したファイアウォールの管理に使 用できるプロトコル (SSH、Telnet、HTTP など) を定義する Management (管理) プロファイルを選択します。None[なし] を選択すると、現在インターフェイスに割り当てられている プロファイルが解除されます。
MTU		このインターフェイスで送信されるパケットの最大転送単位 (MTU)をバイト数で入力します(範囲は 576 ~9,192、 デフォルトは 1,500)。ファイアウォールの両側のマシンが Path MTU Discovery (PMTUD)を実行し、インターフェイス が MTU を超えるパケットを受信すると、ファイアウォール が送信元にパケットが大きすぎることを示す ICMP フラグメ ント要求メッセージを返します。
TCP MSS の 調整		ヘッダーのバイト数に対応できるようにインターフェイス の MTU バイト サイズ以内の値で最大セグメント サイズ (MSS)を調整する場合は選択します。MTUバイトサイズ とMSS調整サイズはMSSバイトサイズと等しい値になり、こ れはIPによって異なります。

レイヤー 3 イ ンターフェイ ス設定	設定場所	の意味
		 IPv4 MSS Adjustment Size (IPv4 MSS調整サイズ) – 範囲 は40~300、デフォルトは40です。
		 IPv6 MSS Adjustment Size (IPv6 MSS調整サイズ) – 範囲 は60~300、デフォルトは60です。
		ネットワークを通るtunnel[トンネル]のMSSを小さくする必 要がある場合はこれらの設定を行ってください。フラグメン ト化を行わないパケットのバイト数がMSSよりも大きい場 合、この設定を行うことでサイズが調整されるようになりま す。
		カプセル化によりヘッダーが延長されるので、MSS調整サイ ズはMPLSヘッダーやVLANタグを持つトンネルトラフィック よりも大きく設定しておくと便利です。
タグのない サブインター フェイス	-	このインターフェイスに対応するサブインターフェイスがタ グ付けされていない場合は、このオプションを選択します。
IP アドレス MAC アドレ ス	レイヤ 3 イン ターフェイス > 上級 > ARP エントリ	1つ以上のスタティックARP(Address Resolution Protocol) エントリを追加する場合は、IPアドレスとそれに関連付け られたハードウェア(メディアアクセス制御、略称MAC) のアドレスをAdd[追加] します。エントリを削除するには、 エントリを選択して Delete[削除] をクリックします。静的 ARP エントリが ARP プロセシングを減少させます。
IPv6 アドレ ス MAC アドレ ス	レイヤ 3 イン ターフェイス > 上級 > ND エントリ	Neighbor Discovery Protocol (ネイバー検出プロトコル - NDP) のネイバー情報を指定する場合は、ネイバーの IPv6 ア ドレスと MAC アドレスをAdd (追加) します。
NDP プロキ シの有効化	レイヤ 3 イン ターフェイス > 上級 > NDP プロキシ	インターフェイスで NDP(Neighbor Discovery Protocol)を 有効にします。ファイアウォールは、このリストの IPv6 ア ドレスの MAC アドレスを要求する ND パケットに応答しま す。ND に対する応答として、ファイアウォールは、そのイ ンターフェイス独自の MAC アドレスを送信します。これに より、ファイアウォールは、リスト内のアドレス宛のパケッ トを受信するようになります。
		NPTv6 (Network Prefix Translation IPv6) を使用する場合 は、NDP プロキシを有効にすることをお勧めします。
		Enable NDP Proxy[NDPプロキシの有効化] を選択した場合、 膨大なAddress[アドレス] のエントリを絞り込む場合は、

レイヤー 3 イ ンターフェイ ス設定	設定場所	の意味
		フィルタ条件を入力しフィルタの適用アイコン (灰色の矢印) をクリックします。
アドレス		1つ以上のIPv6アドレス、IP範囲、IPv6サブネット、または ファイアウォールがNDPプロキシとして機能するアドレス オブジェクトを入力する場合はAdd(追加)をクリックしま す。これらのアドレスの1つは、NPTv6の送信元変換のア ドレスと同じであることが理想的です。アドレスの順序は問 題になりません。
		アドレスがサブネットワークの場合、ファイアウォールは、 サブネットのすべてのアドレスに対してND応答を送信しま す。したがって、ファイアウォールのIPv6ネイバーも追加 し、Negate[除外]をクリックし、これらのIPアドレスに応答 しないようにファイアウォールに指示することをお勧めしま す。
Negate		あるアドレスを Negate(除外)し、そのアドレスで NDP プロキシを止めます。Negate は、指定した IP アドレス範囲または IP サブネットの一部に対して実行できます。
LLDP の有効 化	レイヤ 3 イ ンターフェ イス > 上級 > LLDP	インターフェイスの Link Layer Discovery Protocol (リンクレ イヤー検出プロトコル - LLDP) を有効にします。LLDP はリ ンクレイヤーで機能し、ネイバーとの間で LLDP データユ ニットを送受信することにより、ネイバー デバイスとその機 能を検出します。
LLDPプロ ファイル	-	LLDPプロファイルを選択するか、新しい LLDP Profile (LLDP プロファイル)を作成します。プロファイルでは、LLDP モー ドの設定、Syslog および SNMP 通知の有効化、および LLDP ピアに送信するオプションの TLV (Type-Length-Values) の設 定を行えます。
設定	レイヤ 3 イ ンターフェ	Settings (設定)を選択して DDNS フィールドを設定できるようにします。
Enable [有効 化]	コム> 上叙 > DDNS	インターフェースで DDNS を有効化します。初めに DDNS を有効化してから設定を行う必要があります。(DDNS の設 定が終わっていない場合は有効化せずに保存し、部分的な設 定を保持することができます)
更新間隔(日 数)		FQDN にマッピングされた IP アドレスを更新するために ファイアウォールが DDNS サーバーに送信する更新間隔 (日数)を入力します(範囲は1~30、デフォルトは 1)。

レイヤー 3 イ ンターフェイ ス設定	設定場所	の意味
		また、ファイアウォールはDHCP サーバーから インターフェイスの新しい IP アドレスを受診 した際も DDNS を更新します。
証明書プロ ファイル		証明書プロファイルを作成して DDNS サービスを検証しま す。DDNS サービスは、認証局(CA)が署名した証明書を ファイアウォールに提供します。
ホスト名		DDNS サーバーに登録されたインターフェイスのホスト 名(例:host123.domain123.com、or host123)を入力し ます。DNS がドメイン名として許可している有効な文字 を使った構文になっていることを確認する以外、ファイア ウォールはホスト名の検証を行いません。
ベンダー	レイヤ 3 イ ンターフェ イス > 上級 > DDNS	 DDNS サービスをこのインターフェイスに提供する DDNS ベンダー(およびバージョン)を選択します。 DuckDNS v1 DynDNS v1 FreeDNS Afraid.org Dynamic API v1 FreeDNS Afraid.org v1 No-IP v1 Palo Alto Networks DDNS (DDNS、SD-WAN AE サブイ ンターフェイス、および SD-WAN レイヤ 3 サブインター フェイスを使用した SD-WAN フル メッシュに適用されま す) ⑦ ファイアウォールが特定の日で失効すると示唆 する DDNS サービスの古いバージョンを選択 する場合、新しいバージョンに移動させます。 ベンダー名に続く Name (名前)およびValue (値)フィールド は、ベンダー固有のものです。読み取り専用フィールドは、 ファイアウォールが DDNS サービスに接続するために使用 するパラメーターを示しています。DDNS サービスプロバイ ダーが提供するパスワード、DDNS サーバーからの応答がない場合にファイアウォールが使用するタイムアウトなど、他 のフィールドを設定します。
IPv4 Tab (タ ブ)		インターフェイスで設定した IPv4 アドレスを追加してか ら、それを選択します。IPv4 アドレスは DDNS プロバイ ダーが許容している数までしか選択できません。選択された

レイヤー 3 イ ンターフェイ ス設定	設定場所	の意味
		すべての IP アドレスは DDNS プロバイダー(ベンダー)に 登録されています。
IPv6 Tab (タ ブ)		インターフェイスで設定した IPv6 アドレスを追加してか ら、それを選択します。IPv6 アドレスは DDNS プロバイ ダーが許容している数までしか選択できません。選択された すべての IP アドレスは DDNS プロバイダー(ベンダー)に 登録されています。
ランタイム情 報の表示		DDNS 登録を表示します:DDNS プロバイダー、解決された FQDN、マッピングされた IPアドレス(アスタリスク(*) はプライマリ IP アドレスを示します)。トラブルシュー ティングを目的として、各 DDNS プロバイダーにはホスト 名の更新状態を示す独自の返却コードおよび返却日が必要に なります。

レイヤー3サブインターフェイス

• Network > Interfaces > Ethernet [ネットワーク > インターフェイス > イーサネット]

物理レイヤー3インターフェイスとして設定された各 Ethernet ポートについては、追加の論 理レイヤー3インターフェイス (サブインターフェイス) を定義できます。ISP が PPPoE over 802.1Q をサポートしている場合は、レイヤ3サブインターフェイスで PPPoE をイネーブルに できます。この機能を使用すると、ISPが使用するVLANと一致するVLANを選択できます。この 機能は、イーサネット インターフェイスごとに1つの VLAN に制限されています。

また、SD-WAN AE インターフェイスのレイヤ 3 サブインターフェイスを設定することもできま す。SD WAN AE インターフェイス グループを作成し、グループと サブインターフェイスの追 加 を選択し、次の情報を指定します。

PA-7000 シリーズ レイヤー 3 インターフェイスを設定するには、物理インターフェイスを選択 した後、Add Subinterface(サブインターフェイスを追加)して以下の情報を指定します。

レイヤー 3 サブイ ンターフェイス設 定	設定場所	の意味
インターフェイ ス名	レイヤー 3 サ ブインター フェイス	読み取り専用の Interface Name[インターフェイス名] フィールドには、選択した物理インターフェイスの名前 が表示されます。サブインターフェイスを識別する数値 サフィックス(1~9,999)を隣のフィールドに入力しま す。

レイヤー 3 サブイ ンターフェイス設 定	設定場所	の意味
コメント		サブインターフェイスの説明 (省略可) を入力します。
タグ	-	サブインターフェイスの VLAN タグ(1 ~ 4,094)を入 力します。使いやすさを高めるために、インタフェース 名の数値サフィックスと同じ数字を使用します。
Netflowプロファ イル		入力サブインターフェイスを通過する単向性の IP ト ラフィックを NetFlow サーバーにエクスポートする場 合は、サーバー プロファイルを選択するか、Netflow Profile (Netflow プロファイル) をクリックして新し いプロファイルを定義します (Device (デバイス) > Server Profiles (サーバー プロファイル) > NetFlowを 参照)。現在サブインターフェイスに割り当てられてい るNetFlowサーバーを解除する場合は、None[なし]を選 択します。
仮想ルーター(VR)	レイヤー 3 サ ブインター フェイス > 設 定	インターフェイスに仮想ルーターを割り当てる か、Virtual Router(仮想ルーター)をクリックして 新しい仮想ルーターを定義します(「Network(ネッ トワーク)> Virtual Routers(仮想ルーター)」を参 照)。None[なし] を選択すると、現在インターフェイス に割り当てられているルーターが解除されます。
仮想システ ム(vsys)		ファイアウォールが複数の仮想システムをサポートし、 その機能が有効な場合は、サブインターフェイスの仮想 システム (vsys) を選択するか、Virtual System[仮想シス テム] リンクをクリックして新しい vsys を定義します。
セキュリティ ゾーン		サブインターフェイス用のセキュリティゾーンを選択す るか、Zone[ゾーン] をクリックして新しいゾーンを定義 します。現在サブインターフェイスに割り当てられてい るゾーンを解除する場合はNone[なし] を選択します。
SD-WAN を有効 にする	レイヤー3サ ブインター フェイス >	レイヤ3インターフェイスまたは SD-WAN AE インター フェイス グループのレイヤ3サブインターフェイスで SD-WAN を有効にする場合に選択します。
Enable Bonjour Reflector(Bonjour Reflector の有効 化)	, IF V↔	(PA-220、PA-800、および PA-3200 シリーズのみ)この オプションを有効にすると、このオプションで受信およ び転送された Bonjour マルチキャスト通知およびクエリ を、このオプションを有効にした他のすべての L3 およ び AE インターフェースとサブインターフェースにファ イアウォールが転送します。これにより、セキュリティ

レイヤー 3 サブイ ンターフェイス設 定	設定場所	の意味
		または管理目的でトラフィックをルーティングする際に セグメンテーションを採用しているネットワーク環境で のユーザーアクセスおよびデバイスの検出可能性を確保 することができます。このオプションは最大 16 のイン ターフェースで有効化することができます。
タイプ		サブインターフェイスに IPv4 アドレスを割り当てる方法 を選択します。
		 静的- >IP アドレスとサブネット マスクを手動で 追加し、次ホップ ゲートウェイ を入力する必要があります。
		 PPPoE:サブインターフェイスがイーサネット上の ポイントツーポイント プロトコル(PPPoE)クライア ントとして機能し、サーバの IP アドレス、DNS 情 報、MTU などの他の情報とともに ISP から IPv4 アド レスを受信できるようにします。
		 DHCP Client[DHCP クライアント] – サブインター フェイスが DHCP (Dynamic Host Configuration Protocol) クライアントとして機能し、ダイナミック に割り当てられた IP アドレスを受信できます。
		高可用性(HA)アクティブ/アクティブ構成のファイアウォールは、DHCP クライアントをサポートしません。
		選択した IP アドレス方式に応じて、タブに表示されるオ プションは異なります。
IP	レイヤー 3 サ ブインター フェイス > IPv4, Type = Static	Add (追加)をクリックし、以下のいずれかの手順を実 行して、インターフェイスのスタティック IP アドレスと ネットワーク マスクを指定します。
		 CIDR (Classless Inter-Domain Routing) 表記法の ip_address/maskの形式(例: 192.168.2.0/24)でエン トリを入力します。
		 タイプが IP netmask[IP ネットマスク]の既存のアドレスオブジェクトを選択します。
		 タイプが IP netmask (IP ネットマスク)のアドレス オブジェクトを作成します。

レイヤー 3 サブイ ンターフェイス設 定	設定場所	の意味
		インターフェイスに対して複数の IP アドレスを入力でき ます。IP アドレスの最大数は、システムが使用する転送 情報ベース (FIB) によって決まります。
		不要になった IP アドレスを Delete(削除)します。
有効化	レイヤー 3 サ ブインター フェイス > IPv4、タイプ = PPPoE > 一 般	PPPoE サブインターフェイスを有効にします。
ユーザー名	レイヤー 3 サ ブインター フェイス > IPv4、タイプ = PPPoE > 一 般	選択する認証タイプのユーザー名を入力します。
パスワード	レイヤー 3 サ ブインター フェイス > IPv4、タイプ = PPPoE > 一 般	選択する認証タイプのパスワードを入力し、Confirm Passwordを入力します。
認証	レイヤー3サ ブインター フェイス > IPv4、タイプ = PPPoE > 上 級	 PPPoE サブインターフェイスの認証のタイプを選択します。 None-(default).[なし] が選択されている場合、firewall は auto 認証を使用します。 CHAP-Firewall はチャレンジハンドシェイク認証プロトコル (CHAP) を使用します。 PAP-Firewall はパスワード認証プロトコル (PAP) を 使用します。PAP はユーザ名とパスワードをプレーン テキストで送信するため、CHAP よりも安全性が低く なります。 auto (自動) -ファイアウォールは、PPPoE サーバーと 認証方法 (CHAP または PAP) を交渉します。
スタティック ア ドレス	レイヤー 3 サ ブインター	PPPoE サーバがその IPv4 アドレスをサブインターフェ イスに割り当てるように要求するには、スタティック ア

レイヤー 3 サブイ ンターフェイス設 定	設定場所	の意味
	フェイス > IPv4、タイプ = PPPoE > 上 級	ドレスを指定します。(PPPoE サーバーは、その裁量に より、要求されたアドレスまたは別のアドレスを割り当 てることができます。デフォルト設定は None (なし) で す。
ピアを指すデ フォルト ルート を自動的に作成	レイヤー 3 サ ブインター フェイス > IPv4、タイプ = PPPoE > 上 級	PPPoE サーバーが提供するデフォルト ゲートウェイを指 す既定のルートを作成します。
デフォルト ルー ト メトリック	レイヤー 3 サ ブインター フェイス > IPv4、タイプ = PPPoE > 上 級	PPPoE 接続のデフォルトのルート メトリック(優先度レベル)を入力します。範囲は 1 から 65,535 です。デフォルトは 10 です。数値の低いルートほど、ルート選択時の優先順位が高くなります。たとえば、メトリックが 10 のルートは、メトリックが 100 のルートよりも前に使用されます。
アクセス コンセ ントレータ	レイヤー 3 サ ブインター フェイス > IPv4、タイプ = PPPoE > 上 級	ISP から提供されたアクセス コンセントレータの名前を 入力します(0 ~ 255 文字の文字列値)。ファイアウォー ル は、このアクセス コンセントレータに接続します。
サービス	レイヤー 3 サ ブインター フェイス > IPv4、タイプ = PPPoE > 上 級	ISP が提供したサービスを入力します (0 から 255 文字の 文字列値)。
Passive	レイヤー 3 サ ブインター フェイス > IPv4、タイプ = PPPoE > 上 級	PPPoE クライアント (ファイアウォール) が PPPoE サー バーが接続を開始するのを待機させる場合は、[パッシ ブ] を選択します。[パッシブ] が選択されていない場合、 ファイアウォール は接続を開始できます。
有効化	レイヤー 3 サ ブインター フェイス >	インターフェイスの DHCP クライアントを有効化する場合に選択します。

レイヤー 3 サブイ ンターフェイス設 定	設定場所	の意味
サーバー提供の デフォルト ゲー トウェイを指す デフォルト ルー トを自動的に作 成	IPv4, Type = DHCP	DHCP サーバーによって提供されるデフォルト ゲート ウェイを指し示すデフォルト ルートを自動的に作成する 場合に選択します。
ホスト名の送信		ファイアウォール (DHCP クライアントとして) にイ ンターフェイスのホスト名 (Option 12) を DHCP サー バーに送信させる場合に選択します。デフォルトで Send Hostname (ホスト名の送信) を行う場合、デフォルトで ファイアウォールのホスト名がホスト名フィールドで選 択されます。その名前を送信するか、カスタム ホスト名 (大文字および小文字、数字、ピリオド、ハイフン、ア ンダースコアを含む最長 64 文字) を入力します。
デフォルト ルー ト メトリック		(任意)ファイアウォールとDHCPサーバー間のルート について、デフォルトルートへの関連付けと、パス選択 の際に使用するルートメトリック(優先度)を入力しま す(範囲は1~65535、デフォルトなし)。数値が小さい ほど優先度が高くなります。
DHCP クライア ント ランタイム 情報の表示		DHCPのリース状態、ダイナミックIPアドレス割り当 て、サブネットマスク、ゲートウェイ、サーバー設 定 (DNS、NTP、ドメイン、WINS、NIS、POP3、お よびSMTP) など、DHCPサーバーから受信したすべて の設定を表示する場合はShow DHCP Client Runtime Info[DHCPクライアントのランタイム情報を表示] を選択 します。
インターフェー スでの IPv6 の有 効化	レイヤー3サ ブインター フェイス > IPv6	このインターフェイスの IPv6 アドレスを有効にする場合 に選択します。
SD-WAN を有効 にする		[Enable SD-WAN (SD-WANを有効にする)] を選び、サブ インターフェイスで SD-WAN を有効にします。
インターフェイ ス ID		64 ビット拡張一意識別子 (EUI-64) を 16 進数形式で入 力します (例: 00:26:08:FF:FE:DE:4E:29)。このフィール ドを空白のままにすると、ファイアウォールが、物理イ ンターフェイスの MAC アドレスから生成された EUI-64 を使用します。アドレスの追加時に Use interface ID as host portion[ホスト部分にインターフェイス ID を使用]

レイヤー 3 サブイ ンターフェイス設 定	設定場所	の意味
		オプションを選択すると、ファイアウォールがそのア ドレスのホスト部分にインターフェイス ID を使用しま す。
タイプ		IPv6 アドレスのタイプを選択します。Static, DHCPv6 Client, or Inherited.
アドレス	レイヤー 3 サ ブインター フェイス > IPv6 > アドレ ス割り当て、 タイプ = 静的	IPv6 アドレスとプレフィックス長を追加します (たとえ ば、2001:400:f00::1/64) 。または、IPv6 アドレス オブ ジェクトを選択するか、新しいアドレス オブジェクトを 作成することもできます。
インターフェイ ス上のアドレス を有効にする		インターフェースで IPv6 アドレスを有効化します。
ホスト部分にイ ンターフェイス ID を使用		IPv6 アドレスのホスト部分に Interface (インターフェイス) ID を使用する場合に選択します。
エニーキャスト		最も近いノードを経由するルーティングを含める場合に 選択します。
RA を送信する	レイヤー 3 サ ブインター フェイス > IPv6 > アドレ ス割り当て、 タイプ = 静的	この IP アドレスのルーター通知 (RA) を有効にす る場合に選択します。(インターフェイスで Router Advertisement を有効にする必要があります)。RA の詳 細は、この表の「Enable Router Advertisement (ルー ター通知を有効にする)」を参照してください。残りの フィールドは、RAを送信した場合に適用されます。
		 有効な有効期間(秒):ファイアウォールがそのアドレスを有効と見なす時間の長さ(秒単位)。有効なライフタイムは、Preferred Lifetime[優先ライフタイム]以上でなければなりません。デフォルトは2,592,000です。
		 Preferred Lifetime (秒):有効なアドレスが優先される時間の長さ(秒単位)(ファイアウォールがそのアドレスを使用してトラフィックを送受信できることを意味します)。優先ライフタイムの期限後は、ファイアウォールがこのアドレスを使用して新しい接続を確立することはできませんが、既存の接続は Valid Lifetime (有効なライフタイム)の期限まで有効です。デフォルトは 604,800 です。

レイヤー 3 サブイ ンターフェイス設 定	設定場所	の意味
		 On-link (オンリンク) – プレフィックス内にアドレ スがあるシステムにルーターなしで到達可能である場 合に選択します。
		 Autonomous(自律型) – 通知されたプレフィックス とインターフェイス ID を組み合わせて、システムが IP アドレスを独自に作成できる場合に選択します。
ルーターがアド バタイズした ルートを受け入 れる	レイヤー3サ ブインター フェイス > IPv6 > アド レス割り当 て、タイプ = DHCPv6 クラ イアント	DHCPv6 クライアントが DHCPv6 サーバからの RA を受け入れることを許可する場合に選択します。
デフォルト ルー ト メトリック		インターフェイスから ISP へのルートのデフォルト ルー ト メトリックを入力します。範囲は 1 から 65,535 で す。デフォルトは 10 です。
優先		DHCPv6 クライアント インターフェイス (low、medium、または high) のプリファレンスを選択 して、2 つのインターフェイス (それぞれが冗長性のた めに異なる ISP に接続されている) がある場合に、一方 の ISP のインターフェイスにもう一方の ISP のインター フェイスよりも高い優先順位を割り当てることができ ます。優先インターフェイスに接続されている ISP は、 ホスト側のインターフェイスに送信するデリゲートされ たプレフィックスを提供する ISP になります。インター フェイスのプリファレンスが同じ場合、両方の ISP が委 任されたプレフィックスを提供し、ホストが使用するプ レフィックスを決定します。
IPv6 アドレスを 有効にする	レイヤー3サ ブインター フェイス > IPv6 > アド レス割り当 て、タイプ= DHCPv6 ク ライアント > DHCPv6 オプ ション	この DHCPv6 クライアント用に受信した IPv6 アドレス を有効にします。
非一時アドレス		ファイアウォールの非一時アドレスを、委任側ルータと ISP に面するこの DHCPv6 クライアント インターフェイ スに割り当てるように要求します。非一時アドレスは、 一時アドレスよりも有効期間が長くなります。非一時ア ドレスは更新できます。

レイヤー 3 サブイ ンターフェイス設 定	設定場所	の意味
		インターフェイスに非一時アドレスまた は一時アドレスのどちらを要求するかは、 ユーザーの裁量とDHCPv6サーバーの機能 に基づきます。一部のサーバーは、一時的 なアドレスしか提供できません。ベストプ ラクティスは、非一時アドレスと一時アド レスの両方を選択することであり、その場 合、ファイアウォールは非一時アドレスを 優先します。
一時アドレス		委任ルータと ISP に面するこの DHCPv6 クライアント インターフェイスに割り当てるファイアウォールの一時 アドレスを要求します。[一時アドレス]を選択すると、 アドレスが短期間使用されることを意図しているため、 セキュリティのレベルが高くなります。一時アドレスは 更新される場合と更新されない場合があります。
迅速なコミット		Solicit、Advertise、Request、および Reply メッセージ のプロセスではなく、Solicit および Reply メッセージの DHCP プロセスを使用する場合に選択します。
プレフィックス 委任を有効にす る	レイヤー3サ ブインター フェイス > IPv6 > アド レス割り当 て、タイプ= DHCPv6 クラ イアント > プ レフィックス 委任	プレフィックス委任を有効にして、ファイアウォール がプレフィックス委任機能をサポートできるようにし ます。つまり、インターフェイスはアップストリーム DHCPv6 サーバからプレフィックスを受け入れ、選択 したプレフィックス プールにプレフィックスを配置 し、そこからファイアウォールが RA 経由でホストにプ レフィックスを委任します。インターフェイスのプレ フィックス委任を有効または無効にする機能により、 ファイアウォールは複数の ISP (インターフェイスごとに 1 つの ISP)をサポートできます。このインターフェイス でプレフィックス委任を有効にすると、プレフィックス を提供する ISP が制御されます。
DHCP プレ フィックス長の ヒント		選択すると、ファイアウォールが優先 DHCPv6 プレ フィックス長を DHCPv6 サーバに送信できるようになり ます。
DHCP プレ フィックス長 (ビット)		DHCPv6 サーバにヒントとして送信される優先 DHCPv6 プレフィックス長を 48 ~ 64 ビットの範囲で入力しま す。

レイヤー 3 サブイ ンターフェイス設 定	設定場所	の意味
	レイヤー3サ	たとえば、プレフィックス長48を要求 すると、サブネット(64-48)に16ビット が残り、委任するにはそのプレフィック スの多くのサブディビジョンが必要であ ることを示します。一方、プレフィック ス長63を要求すると、2つのサブネット のみを委任するために1ビットが残りま す。128ビットのうち、ホストアドレス用 にさらに64ビットあります。
プレフィックス プール名		ファイアウォールが受信したプレフィックスを保存する プレフィックス プールの名前を入力します。名前は一意 で、最大 63 文字の英数字、ハイフン、ピリオド、およ びアンダースコアを含む必要があります。 ② 認識しやすいように、 <i>ISP</i> を反映したプレ フィックス プール名を使用します。
Enable [有効化]		そのインターフェイスを有効化します。
IPv4 パラメータ を適用する	 ブインター フェイス > IPv6 > タイプ = PPPoEv6 ク ライアント > 一般 	PPPoE クライアント(IPv4)用にインターフェイスがすで に設定されている場合は、オプションで IPv4 パラメータ を PPPoEv6 クライアントに適用できます。(コピーされ るパラメータは、認証タイプ、ユーザ名、パスワード、 アクセスコンセントレータ名、サービス、およびパッシ ブ設定です)。
		その後、PPPoE IPv4 クライアントでパラメータを再設 定すると、新しい設定が PPPoE IPv6 クライアントにコ ピーされます。いずれかのクライアントのパラメータを 再設定すると、セッションが再確立され、トラフィック が中断されます。
		PPPoE IPv4 クライアントと PPPoE IPv6 クライアント を個別に設定する場合でも、同じ認証タイプ、ユーザー 名、パスワード、アクセス コンセントレータ名、サービ ス、パッシブ設定を使用して 2 つのクライアントを設定 する必要があります。
Passive		PPPoEv6 クライアント (インターフェイス) に PPPoEv6 サーバーが接続を開始するまで待機させたい場合 は、[Passive (パッシブ)] を選択します。Passiveが選択さ

レイヤー 3 サブイ ンターフェイス設 定	設定場所	の意味
		れていない場合、インターフェースは接続を開始できま す。
認証	-	インターフェースの認証タイプを選択します。
		 CHAP – インターフェースは Challenge Handshake Authentication Protocol (CHAP) を使用します。
		 PAP-インターフェースはパスワード認証プロトコル (PAP)を使用します。PAP はユーザ名とパスワードを プレーンテキストで送信し、CHAP よりも安全性が低 くなります。
		 自動–インターフェイスは、PPPoEv6 サーバと認証方 式(CHAP または PAP)をネゴシエートします。
		このインターフェイスも PPPoE IPv4 クライアントとし て設定した場合は、2 つのクライアントを同じ認証タイ プ、ユーザー名、パスワード、アクセス コンセントレー タ名、サービス、パッシブ設定で設定する必要がありま す。
username	-	認証用のユーザー名を入力します。
パスワードとパ スワードの確認	-	パスワードを入力し、パスワードを確認します。
アクセス コンセ ントレータ	_	ISPから接続先のアクセスコンセントレータの名前が通 知された場合は、それを入力します(0~255文字の文字 列)。
サービス	-	インターフェイスを PPPoEv6 クライアントとして使用 して、PPPoEv6 サーバに特定のサービスを要求する場合 は、サービス(0 ~ 255 文字の文字列)を入力します。
ルーターがアド バタイズした ルートを受け入 れる	レイヤー3サ ブインター フェイス > IPv6 > タイプ = PPPoFv6 ク	PPPoEv6 クライアントがルーター アドバタイズメント (RA) を受け入れることを許可する場合に選択します。
デフォルト ルー ト メトリック	ライアント > アドレス割り 当て	インターフェイスから ISP へのルータのデフォルトルー トメトリックを指定します。範囲は 1 ~ 65,535、デフォ ルトは 10 です。

レイヤー 3 サブイ ンターフェイス設 定	設定場所	の意味
優先		PPPoE クライアントインターフェイスのプリファレン スを設定します。高 (デフォルト)、中、または低。イン ターフェイスが 2 つある (冗長性のためにそれぞれ異 なる ISP に接続されている)場合は、一方の ISP のイン ターフェイスに、他方の ISP のインターフェイスよりも 高い優先順位を割り当てることができます。優先イン ターフェイスに接続されている ISP は、ホスト側のイン ターフェイスに送信するデリゲートされたプレフィック スを提供する ISP になります。クライアントのインター フェイスのプリファレンスが同じ場合、両方の ISP が委 任されたプレフィックスを提供し、ホストが使用するプ レフィックスを決定します。
自動構成を有効 にする	レイヤー3サ ブインター フェイス > IPv6 > タイプ = PPPoEv6 ク ライアント > アドレス割り 当て > オート コンフィグ	選択すると、IPv6 制御プロトコル (IPv6CP) インターフェ イス識別子と RA からのプレフィックス (SLAAC を使用) を使用して、PPPoEv6 クライアントインターフェイスの IPv6 アドレスがファイアウォールに自動設定されます。
Enable [有効化]	レイヤー3サ ブインター フェイス > IPv6 > タイ プ = PPPoEv6 クライアン ト > アドレ ス割り当て > DHCPv6	PPPoEv6 クライアントが DHCPv6 を使用できるように します。
IPv6 アドレスを 有効にする	レイヤー3サ ブインター フェイス > IPv6 > タイ プ = PPPoEv6 クライアン ト > アドレ ス割り当て > DHCPv6 >	PPPoEv6 クライアントが DHCPv6 サーバーによって割 り当てられたアドレスを使用できるようにします。
迅速なコミット		DHCPv6のプロセスとし て、Solicit、Advertise、Request、Replyの4メッセージで はなく、SolicitとReplyの2メッセージを使用することを 選択します。

レイヤー 3 サブイ ンターフェイス設 定	設定場所	の意味
DUID タイプ	DHCPv6 オプ ション	インターフェイスが DHCPv6 サーバーに対して自身を識 別するために使用する DHCPv6 固有識別子 (DUID) タイ プを選択します。
		 DUID-LLT-タイムスタンプで連結されたインター フェイスのリンクレイヤアドレス。
		• DUID-LL-インターフェイスのリンク層アドレス。
プレフィックス 委任を有効にす る	レイヤー3サ ブインター フェイス > IPv6 > タイ プ = PPPoEv6 クライアン ト > アドレ ス割り当て > DHCPv6 > プ レフィックス 委任	アドレス割り当てに DHCPv6 を選択した場合は、[Prefix Delegation (プレフィックス委任)] と [Enable Prefix Delegation (プレフィックス委任を有効にする)] を選択 します。つまり、インターフェイスはアップストリーム DHCPv6 サーバからプレフィックスを受け入れ、そのプ レフィックスをプレフィックス プールに配置し、そこか らファイアウォールが RA 経由でホストにプレフィック スを委任します。インターフェイスのプレフィックス委 任を有効または無効にする機能により、ファイアウォー ルは複数の ISP (インターフェイスごとに 1 つの ISP) をサ ポートできます。このインターフェイスでプレフィック ス委任を有効にすると、プレフィックスを提供する ISP が制御されます。委任されたプレフィックスはホスト側 のインターフェイスで使用され、その IPv6 アドレスは MAC アドレスと EUI-64 入力で構成されます。
DHCP プレ フィックス長の ヒント		選択すると、ファイアウォールが優先 DHCPv6 プレ フィックス長を DHCPv6 サーバに送信できるようになり ます。
DHCP プレ フィックス長 (ビット)		DHCPv6 サーバに送信させたい DHCPv6 プレフィック スの長さを入力します。範囲は 0 ~ 128 で、デフォルト は 48 です。DHCPv6 サーバには、選択したプレフィッ クス長を送信することが可能です。
		たとえば、プレフィックス長 48 を要求すると、サブネット (64-48分)に 16 ビットが残り、委任するにはそのプレフィックスの多くのサブディビジョンが必要であることを示します。プレフィックス長 63 を要求すると、2 つのサブネットのみを委任するために1ビットが残ります。128ビットのうち、ホストアドレス用にさらに64ビットあります。

レイヤー 3 サブイ ンターフェイス設 定	設定場所	の意味
		 インターフェイスは /48 プレフィックスを 受け取ることができますが、たとえば /64 プレフィックスをデリゲートします。これ は、ファイアウォールがデリゲーションす るプレフィックスを細分化していることを 意味します。
プレフィックス プール名		ファイアウォールが受信したプレフィックスを保存する プールのプレフィックスプール名を入力します。名前は 一意で、最大 63 文字の英数字、ハイフン、ピリオド、 およびアンダースコアを含む必要があります。 ② 認識しやすいように、 <i>ISP</i> を反映したプレ フィックスプール名を使用します。
名前	レイヤー 3 サ ブインター フェイス > IPv6 > アドレ ス割り当て、 タイプ = 継承	Add プール名を入力してプールを作成します。名前に は、最大 63 文字の英数字、ハイフン、ピリオド、およ びアンダースコアを使用できます。
アドレス タイプ		以下のうち1つを選択します。 • GUA from Pool:選択されたプレフィックス プールか らのグローバル ユニキャスト アドレス(GUA)。 • ULA–Unique Local Address は、プライベート ネット ワーク内の接続用のアドレス範囲 fc00::/7 のプライ ベート アドレスです。DHCPv6 サーバーがない場合 は、ULA を選択します。
インターフェイ スで有効にする		インターフェイスでアドレスを有効にします。
プレフィックス プール		GUA を取得するプレフィックス プールを選択します。
割り当てタイプ	レイヤー 3 サ ブインター フェイス > IPv6 > アドレ ス割り当て、 タイプ = 継承	 割り当てタイプを選択します。 Dynamic:DHCPv6 クライアントは、継承されたイン ターフェイスを構成するための識別子を選択します。 Dynamic with Identifier - 0 から 4,000 の範囲の識別 子を選択し、DHCPv6 クライアント全体で一意の識別 子を維持する責任があります。

レイヤー 3 サブイ ンターフェイス設 定	設定場所	の意味
ルーター通知を 送信		インターフェイスから LAN ホストにルータ アドバタイ ズメント(RA)を送信する場合に選択します。
オンリンク		プレフィックス内にアドレスを持つシステムがルーター なしで到達できるかどうかを選択します。
自主的な		システムが、アドバタイズされたプレフィックスとイン ターフェイス ID を組み合わせて IPv6 アドレスを個別に 作成できるかどうかを選択します。
重複アドレス検 出を有効にする	レイヤー 3サブイン	重複アドレス検出(DAD)を有効にする場合に選択し、 セクション内の他のフィールドの設定を行います。
DAD 試行回数	ターフェイ ス > IPv6 > Address Resolution (アドレス解 決)	ネイバー要請間隔 (NS Interval (NS 間隔)) の内にDADを 試行する回数を指定します(範囲は 1 ~ 10、デフォルト は 1)。この回数を超えるとネイバーに障害があるとみ なされます。
Reachable Time (到達可能時間) (秒)		到達可能性確認メッセージを受信した後にネイバーが到 達可能であると想定するためにクライアントが使用する 時間の長さを秒単位で指定します(範囲は 10 ~ 36,000、 デフォルトは 30)。
NS 間隔 (秒)		障害が示されるまでの DAD 試行の秒数であるネイバー 送信要求 (NS) 間隔を指定します (範囲は 1 から 3,600、 デフォルトは 1)。
NDP モニタリン グの有効化		NDP(Neighbor Discovery Protocol)モニタリン グを有効にする場合に選択します。有効にする と、NDP(([機能] 列)を選択して、IPv6 アドレス、対応する MAC ア ドレス、ユーザ ID(ベストケースベース)など、ファイア ウォールが検出したネイバーに関する情報を表示できま す。
ルーター通知を 有効にする	レイヤー3サ ブインター フェイス > IPv6 > ルー ターアドバ タイズメン ト、タイプ=	ネイバー検出を IPv6 インターフェイスで提供するには、 このセクションのその他のフィールドを選択して設定し ます。ルーター通知 (RA) メッセージを受信する IPv6 DNS クライアントは、この情報を使用します。 RA により、ファイアウォールが、スタティックに設定 されていない IPv6 ホストのデフォルト ゲートウェイと して機能し、ホストにアドレス設定の IPv6 プレフィック

)

レイヤー 3 サブイ ンターフェイス設 定	設定場所	の意味
	静的またはタ イプ=継承	スを提供できます。別の DHCPv6 サーバーをこの機能と 併用すると、DNS および他の設定をクライアントに提供 できます。
		これはインターフェイスのグローバル設定です。IP ア ドレスごとに RA オプションを設定する場合は、IP アド レス テーブルのアドレスを Add(追加)して設定しま す。IP アドレスに RA オプションを設定する場合は、イ ンターフェイスの Enable Router Advertisement(ルー ター通知を有効にする)必要があります。
最小間隔(秒)	-	ファイアウォールが送信する RA 間の最小間隔(秒)を 指定します(範囲は 3 ~ 1,350、デフォルトは 200)。 ファイアウォールは、設定した最小値と最大値の間のラ ンダムな間隔で RA を送信します。
最大間隔(秒)	_	ファイアウォールが送信する RA 間の最大間隔(秒)を 指定します(範囲は 4 ~ 1,800、デフォルトは 600)。 ファイアウォールは、設定した最小値と最大値の間のラ ンダムな間隔で RA を送信します。
ホップ制限		クライアントに適用する、送信パケットのホップ制限を 指定します(範囲は1~255、デフォルトは64)。ホッ プ制限を指定しない場合は0を入力します。
リンク MTU	-	クライアントに適用するリンクの最大転送単位 (MTU) を指定します。リンクMTUを指定しない場合は unspecified (指定しない) を選択します(範囲は 1,280 ~ 9,192、デフォルトは unspecified)。
到達可能時間 (ミ リ秒)	-	到達可能確認メッセージを受信後ネイバーに到達可能で あると想定するためにクライアントが使用する到達可能 時間 (ミリ秒)を指定します。到達可能時間を指定しない 場合は unspecified (指定しない)を選択します(範囲は 0 ~ 3,600,000、デフォルトはunspecified)。
リトランスミッ ション時間 (ミリ 秒)		ネイバー要請メッセージを再送信するまでにクライアン トが待機する時間を決定するリトランスミッションタイ マーを指定します。リトランスミッション時間を指定し ない場合は unspecified (指定しない)を選択します(範囲 は 0 ~ 4,294,967,295、デフォルトはunspecified)。

レイヤー 3 サブイ ンターフェイス設 定	設定場所	の意味
ルーターの有効 期間 (秒)		クライアントがファイアウォールをデフォルトゲート ウェイとして使用する時間を秒単位で指定します(範囲 は0~9,000、デフォルトは1,800)。0は、ファイア ウォールがデフォルトゲートウェイではないことを示し ます。有効期間が過ぎると、クライアントがそのデフォ ルトルーターリストからファイアウォールエントリを 削除して、別のルーターをデフォルトゲートウェイとし て使用します。
ルーター設定		ネットワーク セグメントに複数の IPv6 ルーターがある 場合は、クライアントがこのフィールドを使用して優 先ルーターを選択します。セグメントの他のルーターと の比較において、RA が通知するファイアウォール ルー ターの優先度を High、Medium (デフォルト)、Low の中 から選択します。
管理された設定		アドレスを DHCPv6 経由で使用できることをクライアン トに示す場合に選択します。
その他の設定		他のアドレス情報(DNS 関連の設定など)を DHCPv6 経由で使用できることをクライアントに示す場合に選択 します。
ルーター設定	レイヤー 3 サ ブインター フェイス > IPv6 > ルー ターアドバ タイズメン ト、タイプ = 静的またはタ イプ = 継承	異なるルータに RA を送信するインターフェイスが 2 つ以上ある場合は、ルータ プリファレンスを設定しま す。High、Medium、または Low は、相対プライオリ ティを示す RA がアドバタイズするプライオリティであ り、ホストはプライオリティの高いルータのプレフィッ クスを使用します。
管理された設定		アドレスを DHCPv6 経由で使用できることをクライアン トに示す場合に選択します。
その他の設定		他のアドレス情報(DNS 関連の設定など)を DHCPv6 経由で使用できることをクライアントに示す場合に選択 します。
整合性チェック		他のルーターから送信された RA がリンク上で一貫した 情報を通知していることをファイアウォールで確認する 場合に選択します。ファイアウォールでは、システム ロ グの不一致が記録されます。タイプは ipv6nd です。

レイヤー 3 サブイ ンターフェイス設 定	設定場所	の意味
ルーター通知に DNS 情報を含め る	レイヤー 3 サ ブインター フェイス > IPv6 > DNS サポート、タ イプ = 静的	この IPv6 Ethernet インターフェイスから NDP ルーター 通知によって DNS 情報を送信するファイアウォールの ために選択します。この表の他の DNS Support (DNS サ ポート)フィールドは、このオプションを選択した場合 にのみ表示されます。
SERVER		1つ以上の再帰 DNS (RDNS) サーバー アドレスを Add (追加) し、ファイアウォールがこの IPv6 Ethernet インターフェイスから NDP ルーター通知によって送信 できるようにします。RDNS サーバーは、一連の DNS ルックアップ要求をルート DNS および権威 DNS サー バーに送信し、最終的に IP アドレスを DNS クライアン トに提供します。
		最大で8個のRDNSサーバーを設定でき、ファイア ウォールはこれをNDPルーター通知によってリストの 上から下の順序で受信者へと送信し、受信者は同じ順序 でこれを使用します。サーバーの順序を変更するには、 サーバーを選択して Move Up(上へ)移動したり Move Down(下へ)移動したりします。サーバーが必要なく なったら、そのサーバーをリストから Delete(削除)し ます。
有効期間		IPv6 DNS クライアントがルーター通知を受信した後 で、RDNS サーバーを使用してドメイン名を解決できる ようになるまでの最長時間(秒数)を入力します(範囲 は最大間隔(秒)から最大間隔の2倍、デフォルトは 1,200)。
ドメイン検索リ スト	レイヤー 3 サ ブインター フェイス > IPv6 > DNS サポート、タ イプ = 静的	DNS 検索リスト (DNSSL) のドメイン名 (サフィック ス) を1つ以上 Add (追加) します。最大長は255 バイ トです。 DNS 検索リストは、DNS クライアント ルーターが DNS クエリに名前を入力する前に非修飾ドメイン名に (1つ ずつ) 追加するドメイン サフィックスのリストです。 これにより、クエリで完全修飾ドメイン名が使用され ます。たとえば、DNS クライアントがサフィックスの ない「quality」という名前の DNS クエリを送信しよう とすると、ルーターはピリオドと DNS 検索リストの 最初の DNS サフィックスを名前に追加して DNS クエ リを送信します。リストの最初の DNS サフィックスが 「company.com」の場合、ルーターのクエリの完全修飾 ドメイン名は「quality.company.com」になります。

レイヤー 3 サブイ ンターフェイス設 定	設定場所	の意味
		DNS クエリに失敗すると、ルーターはリストの2番目の DNS サフィックスを非修飾名に追加して、新しい DNS クエリを送信します。ルーターは、DNS ルックアップ が成功するまで(残りのサフィックスは無視)、また はルーターがリストのすべてのサフィックスを試すま で、DNS サフィックスを使用します。
		ネイバー検出 DNSSL オプションで DNS クライアン ト ルーターに提供するサフィックスにより、ファイア ウォールを設定します。DNSSL オプションを受信する DNS クライアントは非修飾 DNS クエリでそのサフィッ クスを使用します。
		最大で 8 個のドメイン名(サフィックス)を DNS 検索 リスト オプションに設定でき、ファイアウォールはこ れをNDP ルーター通知によってリストの上から下の順 序で受信者へと送信し、受信者は同じ順序でこれを使用 します。順序を変更するには、サフィックスを選択して Move Up(上へ)移動したり Move Down(下へ)移動 したりします。サフィックスが必要なくなったら、その サフィックスを Delete(削除)します。
有効期間	-	IPv6 DNS クライアントがルーター通知を受信した後 に、DNS 検索リストのドメイン名(サフィックス) を使用できる最大秒数を入力します(範囲は最大間隔 (秒)の値からその2倍までで、デフォルトは 1,200 で す)。
DNS 再帰ネーム	レイヤー	以下を有効にして選択します。
サーバー	3 サブイン ターフェイ	• DHCPv6:DHCPv6 サーバに DNS 再帰ネーム サーバ情 報を送信させます。
	DNS サポー	• Manual:DNS 再帰ネーム サーバを手動で設定します。
ト、タイプ = DHCPv6 クライアン ト、 PPPoEv6 クライアン ト、または継 承	Manual, Add を選択した場合は、firewall がこの IPv6 VLAN インターフェイスから NDP ルーター アドバタ イズメントを送信するための再帰 DNS(RDNS) Server の IPv6 アドレスです。RDNS サーバーは、ルート DNS サーバーと権限のある DNS サーバーに一連の DNS ルッ クアップ要求を送信し、最終的に DNS クライアントに IP アドレスを提供します。	
		最大 8 個の RDNS サーバーを設定し、ファイアウォー ルでそれらを NDP ルーター通知に含めて受信者に送信 できます(設定の上から下の順に送信します)。その

レイヤー 3 サブイ ンターフェイス設 定	設定場所	の意味
		後、受信者は同じ順序でこれらを使用できます。サー バーの順序を変更するには、サーバーを選択して Move Up(上へ)移動したり Move Down(下へ)移動したり します。サーバーが必要なくなったら、そのサーバーを リストから Delete(削除)します。クライアントが特定 の RDNS サーバーを使用してドメイン名を解決できる最 大時間である Lifetime を秒単位で入力します。範囲は 4 から 3,600 です。デフォルトは 1,200 です。
ドメイン検索リ スト レイヤー 3 サブイン ターフェイ ス > IPv6 > DNS サポー ト、タイプ = DHCPv6 クライアン ト、 PPPoEv6 クライアン ト、または継 承	 以下を有効にして選択します。 DHCPv6 - DHCPv6 サーバーにドメイン検索リスト情報を送信させます。 Manual (手動) - ドメイン検索リストを手動で構成します。 [Manual (手動)]、[Add (追加)]を選択し、DNS 検索リスト (DNSSL) に 1 つ以上の [Domain (ドメイン)] 名(サ) 	
	ト、PPPOEVO クライアン ト、または継 承	フィックス)を設定する場合。サフィックスの最大長は 255 バイトです。 DNS 検索一覧は、DNS クライアント ルーターが DNS クエリに名前を入力する前に非修飾ドメイン名に (一度 に 1 つずつ) 追加するドメイン サフィックスの一覧であ り、DNS クエリで完全修飾ドメイン名を使用します。 たとえば、サフィックスなしの「quality」という名前の DNS クエリを DNS クライアントが送信しようとしてい ます。この場合、ルーターはピリオドと、DNS 検索リス トの 1 番目の DNS サフィックスを名前に付加し、DNS クエリを転送します。リストの最初の DNS サフィック スが「company.com」の場合、ルータからの DNS クエ リは完全修飾ドメイン名「quality.company.com」に対す るものです。
		DNS クエリが失敗した場合、ルータはリストの2番目 の DNS サフィックスを非修飾名に追加し、新しい DNS クエリを送信します。ルータは、DNS ルックアップが成 功する(残りのサフィックスを無視する)か、ルータがリ スト上のすべてのサフィックスを試行するまで、DNS サ フィックスを試みます。 近隣探索 DNSSL オプションで DNS クライアント ルー ターに提供するサフィックスを使用してファイアウォー ルを構成します。DNSSL オプションを受信する DNS ク

レイヤー 3 サブイ ンターフェイス設 定	設定場所	の意味
		ライアントは、非修飾 DNS クエリでサフィックスを使用します。 クライアントが特定のドメイン検索リストを使用できる 最大時間である Lifetime を秒単位で入力します。範囲は 4 から 3,600 です。デフォルトは 1,200 です。 ファイアウォールが NDP ルータ アドバタイズメント で受信者に送信する DNS 検索リストには、最大 8 つ のドメインタ(サフィックス)を設定できます。サフィッ
		クスを選択し、Move Up(上へ)または Move Down (下へ)を選択して順序を変更するか、不要になったサ フィックスをリストから Delete(削除)します。
SD-WAN イン ターフェイス プ ロファイル	レイヤー3サ ブインター フェイス > SD-WAN	このサブインターフェイスに割り当てる SD-WAN イン ターフェイス プロファイルを選択するか、新しいプロ ファイルを作成します。
管理プロファイ ル	レイヤー 3 サ ブインター フェイス > 上 級 > その他の 情報	Management Profile[管理プロファイル] – このインター フェイスを介したファイアウォールの管理に使用できる プロトコル (SSH、Telnet、HTTP など) を定義するプロ ファイルを選択します。None[なし] を選択すると、現在 インターフェイスに割り当てられているプロファイルが 解除されます。
MTU		このインターフェイスで送信されるパケットの最大転 送単位(MTU)をバイト数で入力します(範囲は 576 ~9,192、デフォルトは 1,500)。ファイアウォールの両 側のマシンが Path MTU Discovery (PMTUD)を実行し、 インターフェイスが MTU を超えるパケットを受信する と、ファイアウォールが送信元にパケットが大きすぎる ことを示す ICMP フラグメント要求メッセージを返しま す。
TCP MSS の調整	レイヤー 3 サ ブインター フェイス > 上 級 > その他の 情報	ヘッダーのバイト数に対応できるようにインターフェイ スの MTU バイト サイズ以内の値で最大セグメント サイ ズ (MSS)を調整する場合は選択します。MTUバイトサ イズとMSS調整サイズはMSSバイトサイズと等しい値に なり、これはIPによって異なります。
		 IPv4 MSS Adjustment Size (IPv4 MSS調整サイズ) – 範囲は40~300、デフォルトは40です。

レイヤー 3 サブイ ンターフェイス設 定	設定場所	の意味
		 IPv6 MSS Adjustment Size (IPv6 MSS調整サイズ) – 範囲は60~300、デフォルトは60です。
		ネットワークを通るtunnel[トンネル]のMSSを小さくす る必要がある場合はこれらの設定を行ってください。フ ラグメント化を行わないパケットのバイト数がMSSより も大きい場合、この設定を行うことでサイズが調整され るようになります。
		カプセル化によりヘッダーが延長されるので、MSS調整 サイズはMPLSヘッダーやVLANタグを持つトンネルトラ フィックよりも大きく設定しておくと便利です。
IPアドレス MAC アドレス	レイヤー 3 サ ブインター フェイス > 上 級 > ARP エ ントリ	1つ以上のスタティックARP(Address Resolution Protocol)エントリを追加する場合は、IPアドレスとそ れに関連付けられたハードウェア(メディアアクセス制 御、略称MAC)のアドレスをAdd[追加]します。エント リを削除するには、エントリを選択して Delete[削除] を クリックします。静的 ARP エントリが ARP プロセシン グを減少させます。
IPv6 アドレス MAC アドレス	レイヤー 3 サ ブインター フェイス > 上 級 > ND エン トリー	NDP(Neighbor Discovery Protocol)のネイバー情報を 指定する場合は、ネイバーのIPアドレスとMACアドレス をAdd[追加] します。
NDP プロキシの 有効化	レイヤー 3 サ ブインター フェイス > 上 級 > NDP プ ロキシ	インターフェイスで NDP (Neighbor Discovery Protocol) を有効にします。ファイアウォールは、この リストの IPv6 アドレスの MAC アドレスを要求する ND パケットに応答します。ND に対する応答として、ファ イアウォールは、そのインターフェイス独自の MAC ア ドレスを送信します。これにより、ファイアウォール は、リスト内のアドレス宛のパケットを受信するように なります。
		は、NDP プロキシを有効にすることをお勧めします。
		Enable NDP Proxy[NDPプロキシの有効化] を選択した場合、膨大なAddress[アドレス] のエントリを絞り込む場合は、フィルタ条件を入力しフィルタの適用アイコン (灰色の矢印) をクリックします。

レイヤー 3 サブイ ンターフェイス設 定	設定場所	の意味
アドレス		1つ以上のIPv6アドレス、IP範囲、IPv6サブネット、またはファイアウォールがNDPプロキシとして機能するアドレスオブジェクトを入力する場合はAdd(追加)をクリックします。これらのアドレスの1つは、NPTv6の送信元変換のアドレスと同じであることが理想的です。アドレスの順序は問題になりません。
		アドレスがサブネットワークの場合、ファイアウォー ルは、サブネットのすべてのアドレスに対してND応答 を送信します。したがって、ファイアウォールのIPv6ネ イバーも追加し、Negate[除外] をクリックし、これら のIPアドレスに応答しないようにファイアウォールに指 示することをお勧めします。
Negate		あるアドレスを Negate(除外)し、そのアドレスで NDP プロキシを止めます。Negate は、指定した IP アド レス範囲または IP サブネットの一部に対して実行できま す。
設定	レイヤー 3 サ ブインター フェイス > 上 級 > DDNS	Settings (設定)を選択して DDNS フィールドを設定でき るようにします。
Enable [有効化]		インターフェースで DDNS を有効化します。初めに DDNS を有効化してから設定を行う必要があります。 (DDNS の設定が終わっていない場合は有効化せずに保 存し、部分的な設定を保持することができます)
更新間隔(日 数) フェ- 級>	レイヤー 3 サ ブインター フェイス > 上 級 > DDNS	FQDN にマッピングされた IP アドレスを更新するため にファイアウォールが DDNS サーバーに送信する更新間 隔(日数)を入力します(範囲は1~30、デフォルトは 1)。
		また、ファイアウォールはDHCP サーバー からインターフェイスの新しい IP アドレス を受診した際も DDNS を更新します。
証明書プロファ イル		証明書プロファイルを作成して DDNS サービスを検証し ます。DDNS サービスは、認証局(CA)が署名した証明 書をファイアウォールに提供します。
ホスト名		DDNS サーバーに登録されたインターフェイスのホスト 名(例:host123.domain123.com、or host123)を入力 します。DNS がドメイン名として許可している有効な文
レイヤー 3 サブイ ンターフェイス設 定	設定場所	の意味
------------------------------------	---	---
		字を使った構文になっていることを確認する以外、ファ イアウォールはホスト名の検証を行いません。
ベンダー	レイヤー 3 サ ブインター フェイス > 上 級 > DDNS	 DDNS サービスをこのインターフェイスに提供する DDNS ベンダー(およびバージョン)を選択します。 DuckDNS v1 DynDNS v1 FreeDNS Afraid.org Dynamic API v1 FreeDNS Afraid.org v1 No-IP v1 Palo Allo Networks DDNS- SD-WAN AE サブインターフェイスまたは SD-WAN レイヤ 3 サブインターフェイスの場合は、このベンダーを選択する必要があります。 ファイアウォールが特定の日で失効すると示唆する DDNS サービスの古いバージョンを選択する場合、新しいバージョンに移動させます。 ベンダー名に続く Name (名前)およびValue (値)フィールドは、ベンダー固有のものです。読み取り専用フィールドは、マァイアウォールが DDNS サービスに接続するために使用するパラメーターを示しています。DDNS サービスプロバイダーが提供するパスワード、DDNS サーバーからの応答がない場合にファイアウォールが使用す
IPv4 タブ - IP		インターフェイスで設定した IPv4 アドレスを追加してか ら、それを選択します。IPv4 アドレスは DDNS プロバ イダーが許容している数までしか選択できません。選択 されたすべての IP アドレスは DDNS プロバイダー(ベ
IPv6 タブ - IPv6		ンダー)に登録されています。 インターフェイスで設定した IPv6 アドレスを追加してか ら、それを選択します。IPv6 アドレスは DDNS プロバ イダーが許容している数までしか選択できません。選択 されたすべての IP アドレスは DDNS プロバイダー(ベ ンダー)に登録されています。

レイヤー 3 サブイ ンターフェイス設 定	設定場所	の意味
ランタイム情報 の表示	レイヤー 3 サ ブインター フェイス > 上 級 > DDNS	DDNS 登録を表示します:DDNS プロバイダー、解決さ れた FQDN、マッピングされた IPアドレス(アスタリス ク(*) はプライマリ IP アドレスを示します)。トラブ ルシューティングを目的として、各 DDNS プロバイダー にはホスト名の更新状態を示す独自の返却コードおよび 返却日が必要になります。

Log Card Interface (ログカードインターフェイス)

• Network > Interfaces > Ethernet [ネットワーク > インターフェイス > イーサネット]

LPC(Log Processing Card)がある PA-7000 シリーズ ファイアウォールでログ転送を設定する 場合は、1 つのデータ ポートを Log Card(ログ カード)タイプとして設定する必要がありま す。これは、このファイアウォール モデルのトラフィックおよびロギング機能が管理(MGT) インターフェイスの機能を超えるためです。ログ カードのデータ ポートは、Syslog、電子メー ル、SNMP(Simple Network Management Protocol)、Panorama ログ転送、WildFire[™] ファイ ル転送のログ転送を実行します。

- ファイアウォールで Log Card (ログカード)タイプに設定できるポートは1個のみです。ログ転送を有効にして Log Card (ログカード)タイプでインターフェイスを設定していないと、変更をコミットしようとしたときにエラーが発生します。

この情報は、ログ処理カード(LPC)の設定に関するものです。Log Forwarding Card (LFC)を設定する方法については、Device (デバイス) > Log Forwarding Card (ログ転送カード)を参照してください。

ログ カード インターフェイスを設定するには、設定されていないインターフェイス(Ethernet 1/16 など)を選択し、次の表で説明する設定を構成します。

ログ カード イ ンターフェイス 設定	設定場所	の意味
スロット	イーサネット インターフェ イス	インターフェイスのスロット番号 (1 ~ 12) を選択します。
インターフェ イス名		インターフェイス名は事前に定義されており、変更するこ とはできません。
コメント		インターフェイスの説明 (省略可) を入力します。
インターフェ イスタイプ		Log Card[ログカード] を選択します。

ログ カード イ ンターフェイス 設定	設定場所	の意味
IPv4	イーサネッ トインター フェイス > Log Card Forwarding (ログカード転 送)	ネットワークで IPv4 が使用されている場合は、以下を定 義します。 • IP address[IP アドレス] – ポートの IPv4 アドレス。 • Netmask[ネットマスク] – ポートの IPv4 アドレスの ネットワーク マスク。 • Default Gateway[デフォルトゲートウェイ] – ポートの デフォルトゲートウェイのIPv4アドレス。
IPv6	-	ネットワークで IPv6 が使用されている場合は、以下を定 義します。 • IP アドレス: ポートの IPv6 アドレス。 • デフォルト ゲートウェイ: ポートのデフォルト ゲート ウェイの IPv6 アドレス。
リンク速度	イーサネット インターフェ イス > 上級	インターフェイスの速度(10、100、または1000 Mbps)を 選択するか、auto(デフォルト設定)を選択して、接続ご とにファイアウォールに自動的に速度を決定させます。ス ピード設定が不可のインターフェイスについてはautoのみ 設定可能です。 後続速度は最低1000 Mbps以上に設定する ことをおすすめします。
リンクデュプ レックス		接続の種類に応じて、インターフェイスの伝送モードをフ ルデュプレックス (full)、ハーフデュプレックス (half)、自 動ネゴシエート (auto) から選択します。デフォルト設定 はautoです。
リンク ステー ト		接続に応じて、インターフェイスの状態を、有効 (up)、無 効 (down)、自動決定 (auto) から選択します。デフォルト設 定はautoです。

ログ カード サブインターフェイス

• Network > Interfaces > Ethernet [ネットワーク > インターフェイス > イーサネット]

Log Card Interface (ログ カード インターフェイス)を追加するには、そのインターフェイスの 行を選択し、Add Subinterface をクリックし、次の情報を指定します。

ログ カード サブインター フェイス設定	設定場所	の意味
インター フェイス名	LPC サブイ ンターフェ イス	読み取り専用のInterface Name[インターフェイス名] フィー ルドには、選択したログカードインターフェイスの名前が表 示されます。サブインターフェイスを識別する数値サフィッ クス (1 ~ 9999) を隣のフィールドに入力します。
コメント	-	インターフェイスの説明 (省略可) を入力します。
タグ	_	サブインターフェイス用のVLANTag[タグ] (0 ~ 4094) を入 力します。
		◎ ス番号と同じにしてください。
仮想システ ム(vsys)	LPC サブイ ンターフェ イス > コン フィグ	LPC (Log Processing Card) サブインターフェイスの割り当て 先の仮想システム (vsys) を選択します。Virtual Systems[仮 想システム] リンクをクリックして新しいvsysを追加する こともできます。LPC サブインターフェイスを vsys に割り 当てると、そのインターフェイスは、ログ カードからログ (Syslog、電子メール、SNMP) を転送するすべてのサービス の送信元インターフェイスとして使用されます。
IPv4	イーサネッ トインター フェイス > Log Card Forwarding (ログカード 転送)	ネットワークで IPv4 が使用されている場合は、以下を定義 します。 • IP address[IP アドレス] – ポートの IPv4 アドレス。 • Netmask[ネットマスク] – ポートの IPv4 アドレスのネッ トワーク マスク。 • Default Gateway[デフォルトゲートウェイ] – ポートのデ フォルトゲートウェイのIPv4アドレス。
IPv6		ネットワークで IPv6 が使用されている場合は、以下を定義 します。 • IP アドレス: ポートの IPv6 アドレス。 • デフォルト ゲートウェイ: ポートのデフォルト ゲートウェ イの IPv6 アドレス。

復号化ミラー インターフェイス

• Network > Interfaces > Ethernet [ネットワーク > インターフェイス > イーサネット]

復号化ポート ミラー機能を使用するには、Decrypt Mirror[復号化ミラー] インターフェイ ス タイプを選択する必要があります。この機能では、ファイアウォールからの復号化され たトラフィックのコピーを作成して、トラフィック収集ツールに送信できます。このツール は、NetWitness や Solera などの生パケット キャプチャを受信してアーカイブや分析を行うこ とができます。フォレンジックや履歴調査の目的で、または DLP (情報漏洩対策) 機能に包括的 なデータ キャプチャを必要とする組織では、この機能が不可欠です。この機能を有効にするに は、フリー ライセンスを取得してインストールする必要があります。



パブリック クラウド プラットフォーム向け VM-Series (AWS、Azure、Google Cloud Platform)、VMware NSX、Citrix SDX では復号化ポート ミラーリングは使用できません。

復号化ミラー インターフェイスを設定するには、設定されていないインターフェイスの名前 ([Ethernet1/1] など) をクリックし、以下の情報を指定します。

復号化ミラー イ ンターフェイス の設定	の意味
インターフェイ ス名	インターフェイス名は事前に定義されており、変更することはできません。
コメント	インターフェイスの説明 (省略可) を入力します。
インターフェイ スタイプ	Decrypt Mirror[復号化ミラー] を選択します。
リンク速度	インターフェイスの速度 (10、100、または 1000 Mbps) を選択する か、auto を選択してファイアウォールに自動的に速度を決定させます。
リンクデュプ レックス	インターフェイスの伝送モードを、フル デュプレックス (full)、ハーフ デュプレックス (half)、オート ネゴシエーション (auto) から選択します。
リンク ステー ト	インターフェイスの状態を、有効 (up)、無効 (down)、自動決定 (auto) から 選択します。

Ethernet の集約(AE)インターフェイス グループ

[Network (ネットワーク)] > [Interfaces (インターフェース)] > [Ethernet] > [Add Aggregate Group (集約グループの追加)]

Aggregate Ethernet (集約イーサネット - AE)インターフェースグループは、IEEE 802.1AX リン ク集約を使用し、複数のイーサネット インターフェースを、そのファイアウォールと他のネッ トワークデバイスまたはファイアウォールへ接続する、一つの仮想インターフェイスにまとめま す。AEインターフェイスグループは、組み合わされたインターフェイスの間のロードバランス を行うことでピア同士の帯域幅を増加させます。また、1つのインターフェイスが障害を起こし た場合も残りのインターフェイスがトラフィックをサポートするため、冗長性の確保にも役立ち ます。SD-WAN はレイヤ3インターフェイスの AE インターフェイス グループをサポートします。

AEインターフェイスグループの設定を行う前に、それが使用するインターフェイスの設定を 行う必要があります。特定の集約グループに割り当てたインターフェースに関しては、ハード ウェアメディアが異なる場合があります(例えば、光ファイバと銅線を混在させることも可 能)。ただし、帯域幅(1Gbps、10Gbps、40Gbps、100Gbps)およびインターフェースタイプ (HA3、バーチャル ワイヤ、レイヤー 2、レイヤー 3 など)は同一である必要があります。

追加可能な AE インターフェース グループは、ファイアウォールのモデルにより異なりま す。Product Selection tool(製品選択ツール)では、各ファイアウォール モデルがサポートす る 最大集約インターフェース が示されます。各 AE インターフェース グループには最大 8 つま でのインターフェースを設定することができます。

PA-3200 シリーズ、PA-5200 シリーズ、および PA-7000 シリーズ firewall では、QoS は最初の 8 つの AE インターフェイス グループでのみサポートされます。

VMware ESXiおよびKVM上のVMシリーズを含むパPalo Alto Networksのファイア ウォールはすべてAEインターフェイスグループをサポートしています。他のプラ イベートまたはパブリッククラウドに導入されたVMシリーズファイアウォール はAEインターフェイスグループをサポートしません。

以下のファイアウォールモデルに限り、アクティブ/アクティブの高可用性(HA) 環境におかれた HA3(パケット転送)インターフェイスを集約することができます。

- PA-220
- PA-800シリーズ
- PA-3200シリーズ
- PA-5200シリーズ

AE インターフェイス グループを設定する場合は、Add Aggregate Group(集約グループを追加)し、以下の表で説明されている項目を設定してから、インターフェイスをグループに割り当てます(「Ethernet の集約(AE)インターフェイス」を参照)。

集約インター フェイス グ ループの設定	設定場所	の意味
インターフェ イス名	Ethernet の集 約インター フェイス	読み取り専用のInterface Name[インターフェイス名] フィー ルドには aeが設定されています。隣のフィールドに AE イ ンターフェース グループを識別するサフィックスの数字を 入力します。サフィックスの数字の範囲は、そのファイア

集約インター フェイス グ ループの設定	設定場所	の意味
		ウォールのモデルがサポートする数に依存します。Product Selection tool(製品選択ツール)で、各ファイアウォール モデルがサポートする 最大集約インターフェース数 をご参 照ください。
コメント		(任意)インターフェイスの説明を入力します。
インターフェ イスタイプ		インターフェイス タイプを選択します。このタイプによっ て、残りの設定要件やオプションが制御されます。
		 HA – インターフェースがアクティブ/アクティブ デプロ イメント環境の2つのファイアウォール間のHA3リンク である場合にのみ選択します。必要に応じて、Netflow Profile (Netflow プロファイル)を選択して、LACP タブ の設定を行います(「LACP を有効化」参照)。
		 Virtual Wire (バーチャル ワイヤ) – (オプション) NetFlow Profile (プロファイル)を選択して、Virtual Wire Settings (バーチャル ワイヤ設定)の説明に従い、Config (構成) タブとAdvanced (詳細) タブで設定を構成します。
		 Layer 2 (レイヤ 2) – (オプション) NetFlow Profile (NetFlowプロファイル)を選択し、Layer Interface Settings (レイヤ 2 インターフェース設定)の説 明に従い、Config (設定)タブとAdvanced (詳細)タブ で設定を構成します。また、必要に応じ、LACPタブを設 定します (LACPを有効化参照)。
		 Layer 3 (レイヤ 3) (オプション) – NetFlow Profile (NetFlow プロファイル)を選択し、Layer 3 Interface Settings (レイヤー3 インターフェース設定)の 説明に従い、Config (設定) タブ、IPv4またはIPv6タ ブ、およびAdvanced (詳細) タブで設定を構成します。 必要に応じ、LACP タブを構成します(LACPを有効化を 参照)。SD-WAN はレイヤ 3 インターフェイスとサブ インターフェイスの AE インターフェイス グループをサ ポートします。
Netflowプロ ファイル		入力インターフェースを通過する単向性 IP トラフィッ クを NetFlow サーバにエクスポートする場合は、サーバ プロファイルまたはNetflow Profile (Netflow プロファ イル)を選択して、新しいプロファイルを定義します (「Device (デバイス) > Server Profiles (サーバ プロ ファイル) > NetFlow」を参照)。None[なし]を選択する

集約インター フェイス グ ループの設定	設定場所	の意味
		と、現在AEインターフェイスグループに割り当てられてい るNetFlowサーバーが解除されます。
LACP を有効 化	Ethernet の集 約インター フェイス > LACP	AE インターフェイス グループのリンク集約制御プロトコル (LACP) を有効にする場合に選択します。LACP はデフォル トで無効になっています。 LACPを有効化した場合、ファイアウォールとそのLACPピア が直接接続されているかどうかに関わらず、物理リンクレイ ヤーおよびデータリンクレイヤーにおいてインターフェイス 障害が自動的に検知されます。(LACP を使用しない場合、 インターフェース障害の自動検出が実行されるのは、直接接 続されたピア間の物理レイヤのみとなります。)ホット スペ アを設定した場合、LACP により待機中のインターフェイス へ自動フェイルオーバーを行うことが可能になります(「最 大ポート」を参照)。
モード		 ファイアウォールの LACP モードを選択します。2 つの LACP ピア間では、片方をアクティブ、もう片方をパッシブ に設定することが推奨されます。両方ともパッシブの場合は LACP が機能しません。 Passive[パッシブ] (デフォルト) – ファイアウォールがピ ア デバイスからの LACP 状態のクエリにパッシブに応答 します。 Active[アクティブ] – ファイアウォールがピア デバイス の LACP の状態 (使用可能または無応答) をアクティブに クエリします。
トランスミッ ション率	-	ファイアウォールがピア デバイスとクエリおよび応答をやり とりする間隔を選択します。 • Fast[高速] – 毎秒 • Slow[低速] (デフォルト) – 30秒毎
高速フェール オーバー		インターフェイスがダウンしたときに、1秒以内にファイア ウォールを動作中のインターフェイスにフェイルオーバーさ せたい場合に選択します。それ以外の場合は、標準の IEEE 802.1AX 定義の速度 (3 秒以上) でフェールオーバーが生じま す。
システム優先 度	Ethernet の集 約インター	ポートの優先順位に関してファイアウォールまたはそのピア がもう一方をオーバーライドするかどうかを決定する数字で す(以下のMax Ports(最大ポート)参照)。

集約インター フェイス グ ループの設定	設定場所	の意味
	フェイス > LACP (続き)	● 数値が小さいほど優先度は高くなります(範囲 は 1 ~ 65,535、デフォルトは 32,768)。
最大インター フェイス		LACP 集約グループで任意の時点でアクティブにできるイン ターフェースの数 (1~8)。この値は、そのグループに割り当 てるインターフェースの数以上にすることはできません。 割り当てられたインターフェイスの数がアクティブなイン ターフェイスの数を上回ると、ファイアウォールがインター フェースのLACPポート優先度に従って、どのインターフェ イスがスタンバイモードかを判断します。LACP ポートの優 先度は、グループの個々のインターフェイスを設定する際に 設定します(「Ethernet の集約(AE)インターフェイス」 を参照)。
HAパッシブ ステートを有 効にする		HA アクティブ/パッシブ環境にデプロイされたファイア ウォールでは、フェイルオーバー実行前にパッシブファイア ウォールがアクティブなピアと事前に LACP をネゴシエート する設定を選択します。事前にネゴシエートを実行すること で、パッシブなファイアウォールがアクティブに切り替わる 際にLACPのネゴシエートを行う必要がなくなるので、フェ イルオーバーの作業が高速化されます。
Same System MAC Address for Active- Passive HA(アク ティブ/パッ シブ HA に同 ーシステム MAC アドレ スを使用す る)	Ethernetの集 約インター フェイス > LACP (続き)	 これは、HA アクティブ/パッシブ設定で展開されたファイ アウォールにのみ適用されます。アクティブ/アクティブ設 定のファイアウォールには一意の MAC アドレスが必要で す。 HAファイアウォールのピアは同じシステム優先度を設定さ れています。ただし、アクティブ/パッシブ デプロイメント では、同一の MAC アドレスを割り当てるかどうかにより、 それぞれのシステム ID が同じこともあれば、異なる場合も あります HAモードのLACPピアが仮想化されている場 合は(ネットワークに1つのデバイスとして 表示される)、ファイアウォールに同一のシ ステムMACアドレスを使用すると、フェイル オーバー時の待機時間が最小限に抑えられま す。LACPピアが仮想化されていない場合は、 ファイアウォールごとに一意のMACアドレス すると、フェイルオーバーの待機時間が最小限 に抑えられます。

集約インター フェイス グ ループの設定	設定場所	の意味
		LACP は、MAC アドレスを使用して、各 LACP ピアのシ ステム ID を取得します。ファイアウォール ペアおよびピ アペアに同一のシステム優先度の値が設定されている場合 は、LACP がシステム ID の値を使用して、ポート優先度に 応じてどちらがもう一方をオーバーライドするかを判断し ます。両方のファイアウォールの MAC アドレスが同じ場合 は、両者のシステム ID も同じで、LACP ピアのシステム ID よりも大きいか小さくなります。HA ファイアウォールに一 意の MAC アドレスが設定されている場合は、一方のシステ ム ID は LACP ピアよりも大きく、もう一方は小さいことが あります。後者の場合は、ファイアウォールでフェイルオー バーが発生したときに、LACP ピアとアクティブになるファ イアウォール間のポート優先度が切り替わります。
MAC アドレ ス	Ethernet の集 約インター フェイス > LACP (続き)	Use Same System MAC Address(同じシステムMACアドレ スを使用する)場合は、システムが生成した MAC アドレス を選択するか、アクティブ/パッシブのHAペアのファイア ウォールの両方のファイアウォールに独自の MAC アドレス を入力します。アドレスがグローバルに一意であることを確 認する必要があります。
SD-WAN イ ンターフェイ ス プロファ イル	Ethernet の集 約インター フェイス > SD-WAN	AE インターフェイスグループに適用する SD-WAN インター フェイスプロファイルを選択するか、新しいプロファイルを 作成します。ユーザーは、各AEサブインターフェイスに別々 のプロファイルを適用します。
管理プロファ イル	Ethernet の集 約インター フェイス > 上 級 > その他の 情報	このインターフェイスを介したファイアウォールの管理に使 用できるプロトコル (SSH、Telnet、HTTP など) を定義する Management (管理) プロファイルを選択します。None[なし] を選択すると、現在インターフェイスに割り当てられている プロファイルが解除されます。
MTU		このインターフェイスで送信されるパケットの最大転送単位 (MTU)をバイト数で入力します(範囲は 576 ~9,192、 デフォルトは 1,500)。ファイアウォールの両側のマシンが Path MTU Discovery (PMTUD)を実行し、インターフェイス が MTU を超えるパケットを受信すると、ファイアウォール が送信元にパケットが大きすぎることを示す ICMP フラグメ ント要求メッセージを返します。
TCP MSS の 調整		ヘッダーのバイト数に対応できるようにインターフェイス の MTU バイト サイズ以内の値で最大セグメント サイズ (MSS)を調整する場合は選択します。MTUバイトサイズ

集約インター フェイス グ ループの設定	設定場所	の意味
		とMSS調整サイズはMSSバイトサイズと等しい値になり、こ れはIPによって異なります。
		 IPv4 MSS Adjustment Size (IPv4 MSS調整サイズ) – 範囲 は40~300、デフォルトは40です。
		 IPv6 MSS Adjustment Size (IPv6 MSS調整サイズ) – 範囲 は60~300、デフォルトは60です。
		ネットワークを通るtunnel[トンネル]のMSSを小さくする必要がある場合はこれらの設定を行ってください。フラグメント化を行わないパケットのバイト数がMSSよりも大きい場合、この設定を行うことでサイズが調整されるようになります。
		カプセル化によりヘッダーが延長されるので、MSS調整サイ ズはMPLSヘッダーやVLANタグを持つトンネルトラフィック よりも大きく設定しておくと便利です。
タグのない サブインター フェイス	_	このインターフェイスに対応するサブインターフェイスがタ グ付けされていない場合は、このオプションを選択します。
IP アドレス MAC アドレ ス	Ethernet の集 約インター フェイス > 上 級 > ARP エ ントリ	1つ以上のスタティックARP(Address Resolution Protocol) エントリを追加する場合は、IPアドレスとそれに関連付け られたハードウェア(メディアアクセス制御、略称MAC) のアドレスをAdd[追加] します。エントリを削除するには、 エントリを選択して Delete[削除] をクリックします。静的 ARP エントリが ARP プロセシングを減少させます。
IPv6アドレ ス MAC アドレ ス	Ethernet の集 約インター フェイス > 上 級 > ND エン トリ	Neighbor Discovery Protocol (ネイバー検出プロトコル - NDP) のネイバー情報を指定する場合は、ネイバーの IPv6 ア ドレスと MAC アドレスをAdd (追加) します。
NDP プロキ シの有効化	Ethernet の集 約インター フェイス > 上 級 > NDP プ ロキシ	インターフェイスで NDP(Neighbor Discovery Protocol)を 有効にします。ファイアウォールは、このリストの IPv6 ア ドレスの MAC アドレスを要求する ND パケットに応答しま す。ND に対する応答として、ファイアウォールは、そのイ ンターフェイス独自の MAC アドレスを送信します。これに より、ファイアウォールは、リスト内のアドレス宛のパケッ トを受信するようになります。 NPTv6 (Network Prefix Translation IPv6) を使用する場合
		は、NDP プロキシを有効にすることをお勧めします。

集約インター フェイス グ ループの設定	設定場所	の意味
		Enable NDP Proxy[NDPプロキシの有効化] を選択した場合、 膨大なAddress[アドレス] のエントリを絞り込む場合は、 フィルタ条件を入力しフィルタの適用アイコン (灰色の矢印) をクリックします。
アドレス	-	1つ以上のIPv6アドレス、IP範囲、IPv6サブネット、または ファイアウォールがNDPプロキシとして機能するアドレス オブジェクトを入力する場合はAdd(追加)をクリックしま す。これらのアドレスの1つは、NPTv6の送信元変換のア ドレスと同じであることが理想的です。アドレスの順序は問 題になりません。
		アドレスがサブネットワークの場合、ファイアウォールは、 サブネットのすべてのアドレスに対してND応答を送信しま す。したがって、ファイアウォールのIPv6ネイバーも追加 し、Negate[除外]をクリックし、これらのIPアドレスに応答 しないようにファイアウォールに指示することをお勧めしま す。
Negate		あるアドレスを Negate(除外)し、そのアドレスで NDP プロキシを止めます。Negate は、指定した IP アドレス範囲または IP サブネットの一部に対して実行できます。
LLDP の有効 化	Ethernet の集 約インター フェイス > 上 級 > LLDP	インターフェイスの Link Layer Discovery Protocol (リンクレ イヤー検出プロトコル - LLDP) を有効にします。LLDP はリ ンクレイヤーで機能し、ネイバーとの間で LLDP データユ ニットを送受信することにより、ネイバー デバイスとその機 能を検出します。
LLDPプロ ファイル		LLDPプロファイルを選択するか、新しい LLDP Profile (LLDP プロファイル)を作成します。プロファイルでは、LLDP モー ドの設定、Syslog および SNMP 通知の有効化、および LLDP ピアに送信するオプションの TLV (Type-Length-Values) の設 定を行えます。
設定	Ethernetの集 約インター フェイス > 上 級 > DDNS	Settings (設定)を選択して DDNS フィールドを設定できるようにします。
Enable [有効 化]		インターフェースで DDNS を有効化します。初めに DDNS を有効化してから設定を行う必要があります。(DDNS の設 定が終わっていない場合は有効化せずに保存し、部分的な設 定を保持することができます)

集約インター フェイス グ ループの設定	設定場所	の意味
更新間隔(日 数)		FQDN にマッピングされた IP アドレスを更新するために ファイアウォールが DDNS サーバーに送信する更新間隔 (日数)を入力します(範囲は1~30、デフォルトは 1)。
		インラーフェイスの新しいIP アドレスを支診 した際も DDNS を更新します。
証明書プロ ファイル		証明書プロファイルを作成して DDNS サービスを検証しま す。DDNS サービスは、認証局(CA)が署名した証明書を ファイアウォールに提供します。
ホスト名		DDNS サーバーに登録されたインターフェイスのホスト 名 (例:host123.domain123.com、or host123) を入力し ます。DNS がドメイン名として許可している有効な文字 を使った構文になっていることを確認する以外、ファイア ウォールはホスト名の検証を行いません。
ベンダー	Ethernet の集 約インター	DDNS サービスをこのインターフェイスに提供する DDNS ベンダー(およびバージョン)を選択します。
	フェイス > 上 級 > DDNS	DuckDNS v1
		DynDNS v1
		FreeDNS Afraid.org Dynamic API v1
		 FreeDNS Afraid.org v1 No-IP v1
		 Palo Alto Networks DDNS (DDNS、SD-WAN AE サブイ ンターフェイス、および SD-WAN レイヤ 3 サブインター フェイスを使用した SD-WAN フル メッシュに適用されま す)
		 ファイアウォールが特定の日で失効すると示唆 する DDNS サービスの古いバージョンを選択 する場合、新しいバージョンに移動させます。
		ベンダー名に続くName (名前)およびValue (値)フィールド は、ベンダー固有のものです。読み取り専用フィールドは、 ファイアウォールが DDNS サービスに接続するために使用 するパラメーターを示しています。DDNS サービスプロバイ ダーが提供するパスワード、DDNS サーバーからの応答がな

集約インター フェイス グ ループの設定	設定場所	の意味
		い場合にファイアウォールが使用するタイムアウトなど、他 のフィールドを設定します。
IPv4 Tab (タ ブ)		インターフェイスで設定した IPv4 アドレスを追加してか ら、それを選択します。IPv4 アドレスは DDNS プロバイ ダーが許容している数までしか選択できません。選択された すべての IP アドレスは DDNS プロバイダー(ベンダー)に 登録されています。
IPv6 Tab (タ ブ)		インターフェイスで設定した IPv6 アドレスを追加してか ら、それを選択します。IPv6 アドレスは DDNS プロバイ ダーが許容している数までしか選択できません。選択された すべての IP アドレスは DDNS プロバイダー(ベンダー)に 登録されています。
ランタイム情 報の表示		DDNS 登録を表示します:DDNS プロバイダー、解決された FQDN、マッピングされた IPアドレス(アスタリスク(*) はプライマリ IP アドレスを示します)。トラブルシュー ティングを目的として、各 DDNS プロバイダーにはホスト 名の更新状態を示す独自の返却コードおよび返却日が必要に なります。

Ethernet の集約(AE) インターフェイス

• Network > Interfaces > Ethernet [ネットワーク > インターフェイス > イーサネット]

Aggregate Ethernet (AE) Interfaceを構成するには、まず Aggregate Ethernet (AE) Interface Groupを追加します。次に、そのグループに割り当てるインターフェイスの名前をクリックしま す。特定のグループに割り当てるインターフェイスのうち、ハードウェアメディアは異なる場 合があります(たとえば、光ファイバと銅線を混在させることもできます)が、帯域幅とイン ターフェイスタイプ(レイヤ3など)は同じでなければなりません。さらに、インターフェイ スのタイプは、AE インターフェイスグループに対して定義されたタイプと同じでなければなり ません。ただし、各インターフェイスの設定時にタイプを Aggregate Ethernet(Ethernet の集 約)に変更します。グループに割り当てる各インターフェイスに以下の情報を指定します。

 AE インターフェイス グループに対するリンク集約制御プロトコル(LACP)を有効にした場合は、そのグループのすべてのインターフェイスに対して同じ Link Speed (リンク速度) と Link Duplex (リンク デュプレックス)を選択します。値が一致していない場合は、コミット操作時に警告が表示され、PAN-OS がデフォルトのより高い速度およびフル デュプレックスを設定します。

集約インター フェイス設定	設定場所	の意味
インターフェ イス名	Ethernet の集 約インター フェイス	インターフェイス名は事前に定義されており、変更すること はできません。インターフェイス名の ae の後に数字を入力 します。
コメント		(<u>任意</u>) インターフェイスの説明を入力します。
インターフェ イスタイプ		Aggregate Ethernet[Ethernet の集約] を選択します。
集約グループ		インターフェイスを集約グループに割り当てます。
リンク速度	Ethernet の集 約インター フェイス > 上 級 > リンク設 定	インターフェイス速度を Mbps 単位で選択するか、auto を 選択してファイアウォールが自動的に速度を決定するように します。
リンクデュプ レックス		インターフェイスの伝送モードを、フル デュプレックス (full)、ハーフ デュプレックス (half)、オート ネゴシエーショ ン (auto) から選択します。
リンク ス テート		インターフェイスの状態を、有効 (up)、無効 (down)、自動決 定 (auto) から選択します。
PoE Rsvd Pwr	Ethernetの集 約インター	PoE が有効になっている場合、割り当てられる電力量を Watts で選択します。
PoE イネーブ ル	ンエイス・エ 級 > PoE 設定 (サポートさ れているファ イアウォール のみ)	このインターフェイスで PoE を有効にする場合に選択しま す。
LACP ポート 優先順位		ファイアウォールがこのフィールドを使用するのは、集約 グループのリンク集約制御プロトコル (LACP) が有効になっ ている場合のみです。割り当てられたインターフェイスの 数がアクティブなインターフェイスの数 (Max Ports (最大 ポート)フィールド)を上回ると、ファイアウォールがイン ターフェイスの LACP ポート優先度に従って、どのインター フェイスがスタンバイ モードかを判断します。数値が小さい ほど優先度は高くなります (範囲は1~65535、デフォルト は32768)。
仮想ルー ター(VR)	Ethernet の集 約インター	Ethernet の集約インターフェイスを割り当てる仮想ルーター を選択します。

集約インター フェイス設定	設定場所	の意味
セキュリティ ゾーン	フェイス > 設 定	Ethernet の集約インターフェイスを割り当てるセキュリティ ゾーンを選択します。
SD-WAN を 有効にする	Ethernetの集 約インター フェイス > IPv4	インターフェイスの SD-WAN 機能を有効にする場合に選択 します。
Enable Bonjour Reflector(Bon Reflector の 有効化)	Ethernetの集 約インター jogr _エ イス > IPv4	(PA-220、PA-800、および PA-3200 シリーズのみ) このオ プションを有効にすると、このオプションで受信および転送 された Bonjour マルチキャスト通知およびクエリを、このオ プションを有効にした他のすべての L3 および AE インター フェースとサブインターフェースにファイアウォールが転 送します。これにより、セキュリティまたは管理目的でトラ フィックをルーティングする際にセグメンテーションを採用 しているネットワーク環境でのユーザーアクセスおよびデバ イスの検出可能性を確保することができます。このオプショ ンは最大16のインターフェースで有効にすることができま す。
インター フェースでの IPv6 の有効 化	Ethernetの集 約インター フェイス > IPv6	このインターフェイスの IPv6 を有効にする場合に選択しま す。
インターフェ イス ID		64 ビット拡張一意識別子 (EUI-64) を 16 進数形式で入力し ます (例: 00:26:08:FF:FE:DE:4E:29)。このフィールドを空白 のままにすると、ファイアウォールが、物理インターフェイ スの MAC アドレスから生成された EUI-64 を使用します。 アドレスの追加時に Use interface ID as host portion (ホス ト部分にインターフェイス ID を使用) すると、ファイア ウォールがそのアドレスのホスト部分にインターフェイス ID を使用します。
アドレス	Ethernet の集 約インター フェイス > IPv6 > アドレ ス割り当て、 タイプ = 静的	IPv6 アドレスとプレフィックス長を追加します (2001:400:f00::1/64 など)。または、既存の IPv6 アドレス オブジェクトを選択するか、新しい IPv6 アドレス オブジェ クトを作成します。
インターフェ イス上のアド レスを有効に する		インターフェースで IPv6 アドレスを有効化します。

集約インター フェイス設定	設定場所	の意味
ホスト部分に インターフェ イス ID を使 用		IPv6 アドレスのホスト部分に Interface (インターフェイス) ID を使用する場合に選択します。
エニーキャス ト		最も近いノードを経由するルーティングを含める場合に選択 します。
ルーター通知 を送信	Ethernet の集 約インター フェイス > IPv6 > アドレ ス割り当て、 タイプ = 静的	この IP アドレスのルーター通知 (RA) を有効にする場合に選 択します。(インターフェイスのグローバルの Enable Router Advertisement[ルーター通知を有効化する] オプションも 有効化しておく必要があります)。RA の詳細は、この表の 「Enable Router Advertisement (ルーター通知を有効にす る)」を参照してください。以下のフィールドは Enable Router Advertisement (ルーター通知を有効にする) 場合にの み適用されます。
		 Valid Lifetime (有効なライフタイム)–ファイアウォールが アドレスを有効とみなす時間(秒)です。有効なライフタ イムは、Preferred Lifetime[優先ライフタイム]以上でな ければなりません。デフォルトは2,592,000です。
		 Preferred Lifetime (優先ライフタイム)–有効なアドレス が優先される時間(秒)です。この時間内は、ファイア ウォールがこのアドレスを使用してトラフィックを送受 信できます。優先ライフタイムの期限後は、ファイア ウォールがこのアドレスを使用して新しい接続を確立す ることはできませんが、既存の接続は Valid Lifetime (有 効なライフタイム)の期限まで有効です。デフォルトは 604,800です。
		 On-link (オンリンク) – プレフィックス内にアドレスが あるシステムにルーターなしで到達可能である場合に選 択します。
		 Autonomous(自律型) – 通知されたプレフィックスと インターフェイス ID を組み合わせて、システムが IP アド レスを独自に作成できる場合に選択します。
ルーターがア ドバタイズし たルートを受 け入れる	Ethernet の集 約インター フェイス > IPv6 > アド レス割り当 て、 Type	DHCPv6 クライアントが DHCP サーバからの RA を受け入 れることを許可する場合に選択します。

集約インター フェイス設定	設定場所	の意味
デフォルト ルート メト リック	= DHCPv6 Client	インターフェイスから ISP へのルートのデフォルト ルート メトリックを入力します。範囲は 1 から 65,535 です。デ フォルトは 10 です。
優先		DHCPv6 クライアント インターフェイス (low、medium、 または high) のプリファレンスを選択して、2 つのインター フェイス (それぞれが冗長性のために異なる ISP に接続され ている) がある場合に、一方の ISP のインターフェイスにも う一方の ISP のインターフェイスよりも高い優先順位を割り 当てることができます。優先インターフェイスに接続され ている ISP は、ホスト側のインターフェイスに送信するデリ ゲートされたプレフィックスを提供する ISP になります。イ ンターフェイスのプリファレンスが同じ場合、両方の ISP が 委任されたプレフィックスを提供し、ホストが使用するプレ フィックスを決定します。
IPv6 アドレ スを有効にす る	Ethernet の集 約インター フェイス > IPv6 > アド レス割り当 て、タイプ = DHCPv6 ク ライアント > DHCPv6 オプ ション	この DHCPv6 クライアント用に受信した IPv6 アドレスを有 効にします。
非一時アドレス		 firewall の非テンポラリーアドレスを、委任ルータと ISP に 面するこの DHCPv6 クライアント インターフェイスに割り 当てるように要求します。テンポラリーアドレスよりも長い 有効期間を選択します。
一時アドレス		委任ルータと ISP に面するこの DHCPv6 クライアント イン ターフェイスに割り当てるファイアウォールの一時アドレス を要求します。[一時アドレス]を選択すると、アドレスが短 期間使用されることを意図しているため、セキュリティのレ ベルが高くなります。
迅速なコミッ ト		Solicit、Advertise、Request、および Reply メッセージのプロセスではなく、Solicit および Reply メッセージの DHCP プロセスを使用する場合に選択します。

集約インター フェイス設定	設定場所	の意味
プレフィック ス委任を有効 にする	Ethernet の集 約インター フェイス > IPv6 > アド レス割り当 て、タイプ = DHCPv6 クラ イアント > プ レフィックス 委任	プレフィックス委任を有効にして、firewall がプレフィック ス委任機能をサポートできるようにします。つまり、イン ターフェイスはアップストリーム DHCPv6 サーバからプレ フィックスを受け入れ、選択したプレフィックス プールに プレフィックスを配置し、そこから firewall が SLAAC を介 してホストにプレフィックス委任を有効または無効にする機能に より、firewall は複数の ISP (インターフェイスごとに 1 つの ISP)をサポートできます。このインタフェースでプレフィッ クス委任を有効にすると、プレフィックスを提供する ISP を 制御します。DHCP サーバーから受信した委任されたプレ フィックスは、それを要求したインターフェイスでは使用で きません。
DHCP プレ フィックス長 のヒント		選択すると、ファイアウォールが優先 DHCPv6 プレフィッ クス長を DHCPv6 サーバに送信できるようになります。
DHCP プレ フィックス長 (ビット)		 DHCPv6 サーバにヒントとして送信される優先 DHCPv6 プレフィックス長を 48 ~ 64 ビットの範囲で入力します。 たとえば、プレフィックス長 48 を要求すると、サブネット (64-48) に 16 ビットが残り、委任するにはそのプレフィックスの多くのサブディビジョンが必要であることを示します。一方、プレフィックス長 63 を要求すると、2つのサブネットのみを委任するために 1 ビットが残ります。128ビットのうち、ホストアドレス用にさらに64ビットあります。
プレフィック ス プール名		ファイアウォールが受信したプレフィックスを保存するプレ フィックス プールの名前を入力します。名前は一意で、最大 63 文字の英数字、ハイフン、ピリオド、およびアンダース コアを含む必要があります。 認識しやすいように、 <i>ISP</i> を反映したプレ フィックス プール名を使用します。
名前	Ethernet の集 約インター フェイス > IPv6 > アドレ	Add プール名を入力してプールを作成します。名前には、最大 63 文字の英数字、ハイフン、ピリオド、およびアンダースコアを使用できます。

集約インター フェイス設定	設定場所	の意味
アドレスタ	ス割り当て、 タイプ = 継承	以下のうち1つを選択します。
イプ		 GUA from Pool:選択されたプレフィックス プールからの グローバル ユニキャスト アドレス(GUA)。
		 ULA -Unique Local Address (ユニーク・ローカル・ア ドレス)は、プライベート・ネットワーク内で接続する ためのアドレス範囲fc00::/7のプライベート・アドレス です。DHCP サーバーがない場合は、ULA を選択しま す。DHCPv6 サーバには、選択したプレフィックス長を 送信することが可能です。
インターフェ イスで有効に する	_	(GUA)インターフェイスのアドレスを有効にします。
プレフィック ス プール	-	(GUA)インターフェイスのアドレスを有効にします。
割り当てタイ プ	Ethernet の集 約インター フェイス > IPv6 > アドレ ス割り当て、	 (GUA)割り当てタイプを選択します。 Dynamic:DHCPv6 クライアントは、継承されたインターフェイスを構成するための識別子を選択します。 DHCPv6クライアントの識別子を0から4,000の範囲で選
	タイプ = 継承	択し、DHCPv6クライアント間で一意な識別子を維持する 必要があります。
インターフェ イスでアドレ スを有効にす る		(ULA)インターフェイスのアドレスを有効にします。
アドレス		(ULA)アドレスを入力します。
ホスト部分に インターフェ イス ID を使 用		(ULA)インターフェイス ID を IPv6 アドレスのホスト部分と して使用する場合に選択します。
エニーキャス ト		(ULA)IPv6 アドレスをエニーキャスト アドレスにする場合に 選択します。つまり、複数のロケーションが同じプレフィッ クスをアドバタイズでき、IPv6 はルーティング プロトコル のコストやその他の要因に基づいて、最も近いと見なされる ノードにエニーキャスト トラフィックを送信します。

集約インター フェイス設定	設定場所	の意味
ルーター通知 を送信		インターフェイスから LAN ホストにルータ アドバタイズメ ント(RA)を送信する場合に選択します。
オンリンク		プレフィックス内にアドレスを持つシステムがルーターなし で到達できるかどうかを選択します。
自主的な		システムが、アドバタイズされたプレフィックスとインター フェイス ID を組み合わせて IPv6 アドレスを個別に作成でき るかどうかを選択します。
重複アドレス 検出を有効に する	Ethernetの集 約インター フェイス > IPv6 > アドレ ス解決	重複アドレス検出(DAD)を有効にして、DAD Attempts(DAD 試行回数)の数値を指定できるようにする 場合に選択します。
DAD 試行回 数		ネイバー要請間隔 (NS Interval (NS 間隔)) の内にDADを試 行する回数を指定します(範囲は 1 ~ 10、デフォルトは 1)。この回数を超えるとネイバーに障害があるとみなされ ます。
到達可能時間		クエリと応答が正常に行われた後引き続きネイバーに到達可 能な時間(秒)を指定します(範囲は1~36,000、デフォ ルトは30)。
NS 間隔 (秒)		DAD 試行の失敗が示されるまでの時間を秒単位で指定します (範囲は1から3,600、デフォルトは1)。
NDP モニタ リングの有効 化		Neighbor Discovery Protocol のモニタリン グを有効にする場合に選択します。有効に なっていると、NDP(Features(機能)列の を選択し、ファイアウォールで検出されたネイバーの IPv6
		アドレス、対応する MAC アドレスおよび User-ID などの情 報を(ベストケース ベースで)表示できます。
ルーター通知 を有効にする	集約された イーサネット インターフェ イス > IPv6 >	IPv6 インターフェイスのネイバー検出を指定して、このセク ションの他のフィールドを設定する場合に選択します。ルー ター通知(RA)メッセージを受信する IPv6 DNS クライアン トは、この情報を使用します。
	ルーター広告	RA により、ファイアウォールが、スタティックに設定さ れていない IPv6 ホストのデフォルト ゲートウェイとして 機能し、ホストにアドレス設定の IPv6 プレフィックスを提

集約インター フェイス設定	設定場所	の意味
		供できます。別の DHCPv6 サーバーをこの機能と併用する と、DNS および他の設定をクライアントに提供できます。
		これはインターフェイスのグローバル設定です。IP アドレス ごとに RA オプションを設定する場合は、IP アドレステーブ ルの IPv6 アドレスを Add (追加) してコンフィグします。IP アドレスに RA オプションを設定する場合は、インターフェ イスの Enable Router Advertisement (ルーター通知を有効 にする) 必要があります。
最小間隔(秒)		ファイアウォールが送信する RA 間の最小間隔(秒)を指定 します(範囲は 3 ~ 1,350、デフォルトは 200)。ファイア ウォールは、設定した最小値と最大値の間のランダムな間隔 で RA を送信します。
最大間隔(秒)		ファイアウォールが送信する RA 間の最大間隔(秒)を指定 します(範囲は 4 ~ 1,800、デフォルトは 600)。ファイア ウォールは、設定した最小値と最大値の間のランダムな間隔 で RA を送信します。
ホップ制限		クライアントに適用する、送信パケットのホップ制限を指定 します(範囲は 1 ~ 255、デフォルトは 64)。ホップ制限 を指定しない場合は 0 を入力します。
リンク MTU		クライアントに適用するリンクの最大転送単位 (MTU) を指 定します。リンクMTUを指定しない場合は unspecified (指定 しない) を選択します(範囲は 1,280 ~ 9,192、デフォルト は unspecified)。
到達可能時間 (ミリ秒)		到達可能確認メッセージを受信後ネイバーに到達可能で あると想定するためにクライアントが使用する到達可能時 間(ミリ秒)を指定します。到達可能時間を指定しない場 合は unspecified (指定しない)を選択します(範囲は $0 \sim$ 3,600,000、デフォルトはunspecified)。
リトランス ミッション時 間 (ミリ秒)		ネイバー要請メッセージを再送信するまでにクライアントが 待機する時間(ミリ秒)を決定するリトランスミッションタ イマーを指定します。リトランスミッション時間を指定しな い場合は unspecified (指定しない)を選択します(範囲は 0 ~ 4,294,967,295、デフォルトはunspecified)。
ルーターの有 効期間 (秒)		クライアントがファイアウォールをデフォルトゲートウェ イとして使用する時間を秒単位で指定します(範囲は0~ 9,000、デフォルトは1,800)。0は、ファイアウォールがデ フォルトゲートウェイではないことを示します。有効期間が

集約インター フェイス設定	設定場所	の意味
		過ぎると、クライアントがそのデフォルト ルーター リスト からファイアウォール エントリを削除して、別のルーターを デフォルト ゲートウェイとして使用します。
ルーター設定		ネットワーク セグメントに複数の IPv6 ルーターがある場合 は、クライアントがこのフィールドを使用して優先ルーター を選択します。セグメントの他のルーターとの比較におい て、RA が通知するファイアウォール ルーターの優先度を High、Medium (デフォルト)、Low の中から選択します。
管理された設 定		アドレスを DHCPv6 経由で使用できることをクライアント に示す場合に選択します。
その他の設定	-	他のアドレス情報(DNS 関連の設定など)を DHCPv6 経由 で使用できることをクライアントに示す場合に選択します。
整合性チェッ ク	集約された イーサネット インターフェ イス > IPv6 > ルーター広告 (続き)	他のルーターから送信された RA がリンク上で一貫した情報 を通知していることをファイアウォールで確認する場合に選 択します。ファイアウォールでは、システム ログの不一致が 記録されます。タイプは ipv6nd です。
ルーター通知 に DNS 情報 を含める	Ethernetの 集約イン ターフェイ ス > IPv6 > DNS サポー ト、Type = Static	ファイアウォールがこの IPv6 の Ethernet の集約インター フェイスからの NDP ルーター通知 (RA) メッセージで DNS 情報を送信する場合に選択します。この表の他の DNS Support (DNS サポート) フィールドは、このオプ ションを選択した場合にのみ表示されます。(DNS Support タブは、Router Advertisement タブの Enable Router Advertisement の後に使用できます。
サーバー		ファイアウォールがこの IPv6 の Ethernet の集約インター フェイスからの NDP ルーター通知で送信する 1 つ以上の 再帰 DNS (RDNS) サーバー アドレスを Add (追加) しま す。RDNS サーバーは、ルート DNS サーバーと権限のある DNS サーバーに一連の DNS ルックアップ要求を送信し、最 終的に DNS クライアントに IP アドレスを提供します。
		ファイアウォールがリストの上から下の順に NDP ルーター 通知で受信者に送信する RDNS サーバーを最大 8 個設定で きます。その後、受信者は同じ順序でこれらのアドレスを 使用します。サーバーを選択し、Move Up(上へ)または Move Down(下へ)を選択してサーバーの順序を変更する か、不要になったサーバーを Delete(削除)します。

集約インター フェイス設定	設定場所	の意味
有効期間		IPv6 DNS クライアントがルーター通知を受信した後 に、RDNS サーバーを使用してドメイン名を解決できる最大 秒数を入力します(範囲は最大間隔(秒)の値からその2倍 までで、デフォルトは 1,200 です)。
ドメイン検索 リスト		 DNS 検索リスト (DNSSL) の1つ以上のドメイン名 (サ フィックス) を Add (追加) および設定します。サフィック スの最大長は 255 バイトです。 DNS 検索リストは、DNS クライアント ルーターが DNS クエリに名前を入力する前に非修飾ドメイン名に (1つず つ) 追加するドメイン サフィックスのリストです。これ により、DNS クエリで完全修飾ドメイン名が使用されま す。たとえば、DNS クライアントがサフィックスのない 「quality」という名前の DNS クエリを送信しようとする と、ルーターはピリオドと DNS 検索リストの最初の DNS サフィックスを名前に追加して DNS クエリを送信します。 リストの最初の DNS サフィックスが「company.com」 の場合、ルーターの DNS クエリの完全修飾ドメイン名は 「quality.company.com」になります。 DNS クエリに失敗すると、ルーターはリストの 2 番目の DNS サフィックスを非修飾名に追加して、新しい DNS クエ リを送信します。ルーターは DNS ルックアップが成功する か (残りのサフィックスを試行するまで DNS サフィック スを試行します。 ネイバー検出 DNSSL オプションで DNS クライアント ルー ターに提供するサフィックスを使用してファイアウォール を設定します。DNSSL オプションを受信する DNS クライア ントは、その非修飾 DNS クエリでサフィックスを使用します。 ファイアウオールがリストの上から下の順に NDP ルーター 通知で受信者に送信する DNS 検索リストのドメイン名 (サ フィックス) を最大 8 個設定できます。受信者は同じ順序で これらを使用します。サフィックスを選択し、Move Up (上 へ) または Move Down (下へ)を選択してサフィックスの 順序を変更するか、不要になったサフィックスをリストから Delete (削除) します。
有効期間	Ethernet の 集約イン ターフェイ ス > IPv6 >	IPv6 DNS クライアントがルーター通知を受信した後 に、DNS 検索リストのドメイン名(サフィックス)を使用

集約インター フェイス設定	設定場所	の意味
	DNS サポー ト、Type = Static	できる最大秒数を入力します(範囲は最大間隔(秒)の値か らその2倍までで、デフォルトは1,200です)。
DNS 再帰 ネーム サー バー	Ethernet の集 約インター フェイス > IPv6 > DNS サポート、種 類 = DHCPv6 クライアント または継承	 以下を有効にして選択します。 DHCPv6:DHCPv6 サーバに DNS 再帰ネーム サーバ情報 を送信させます。 Manual:DNS 再帰ネーム サーバを手動で設定します。 Manual, Add を選択した場合、firewall は、この IPv6 VLAN インターフェイスから NDP ルーター アドバタイズメントを 送信するために、再帰 DNS (RDNS) Server アドレスを使用し ます。RDNS サーバーは、ルート DNS サーバーと権限のあ る DNS サーバーに一連の DNS ルックアップ要求を送信し、 最終的に DNS クライアントに IP アドレスを提供します。 最大 8 個の RDNS サーバーを設定し、ファイアウォールで それらを NDP ルーター通知に含めて受信者に送信できます (設定の上から下の順に送信します)。その後、受信者は 同じ順序でこれらを使用できます。サーバーの順序を変更す るには、サーバーを選択して Move Up (上へ) 移動したり Move Down (下へ) 移動したりします。サーバーが必要な くなったら、そのサーバーをリストから Delete (削除) しま す。 クライアントが特定の RDNS サーバーを使用してドメイン 名を解決できる最大時間である Lifetime (秒単位) を入力しま す。範囲は 4 から 3,600 です。デフォルトは 1,200 です。
ドメイン検索 リスト	Ethernet の集 約インター フェイス > IPv6 > DNS サポート、種 類 = DHCPv6 クライアント または継承	 以下を有効にして選択します。 DHCPv6:DHCPv6 サーバにドメイン検索リスト情報を送信させます。 Manual - ドメイン検索リストを手動で構成します。 Manual、Add を選択し、DNS 検索リスト (DNSSL)に1つ以上の Domain 名(サフィックス)を設定する場合。サフィックスの最大長は 255 バイトです。 DNS 検索リストは、DNS クライアント ルーターが DNS クエリに名前を入力する前に非修飾ドメイン名に(1つずつ)追加するドメインサフィックスのリストです。これにより、DNS クエリで完全修飾ドメイン名が使用されます。たとえば、サフィックスなしの「quality」という名前の DNS クエリを DNS クライアントが送信しようとしています。この場合、ルーターはピリオドと、DNS 検索リス

集約インター フェイス設定	設定場所	の意味
		トの1番目のDNSサフィックスを名前に付加し、DNSク エリを転送します。リストの最初のDNSサフィックスが 「company.com」の場合、ルーターのDNSクエリの完全修 飾ドメイン名は「quality.company.com」になります。
		DNS クエリに失敗すると、ルーターはリストの2番目の DNS サフィックスを非修飾名に追加して、新しい DNS クエ リを送信します。ルーターは DNS ルックアップが成功する か(残りのサフィックスは無視されます)、ルーターがリス トのすべてのサフィックスを試行するまで DNS サフィック スを試行します。
		ネイバー検出 DNSSL オプションで DNS クライアント ルー ターに提供するサフィックスにより、ファイアウォールを設 定します。DNSSL オプションを受信する DNS クライアント は非修飾 DNS クエリでそのサフィックスを使用します。
		DNS 検索リストに対して最大 8 個のドメイン名(サフィッ クス)を設定し、ファイアウォールでそれらを NDP ルー ター通知に含めて受信者に送信できます(設定の上から下の 順に送信します)。その後、受信者は同じ順序でこれらのア ドレスを使用できます。サフィックスを選択し、Move Up (上へ)または Move Down(下へ)を選択して順序を変 更するか、不要になったサフィックスをリストから Delete (削除)します。
		クライアントが特定のドメイン検索リストを使用できる最大 時間である Lifetime を秒単位で入力します。範囲は4から 3,600 です。デフォルトは 1,200 です。

Network > Interfaces > VLAN [ネットワーク > インター フェイス > VLAN]

VLAN インターフェイスは、ルーティング情報をレイヤー3ネットワーク (IPv4 および IPv6) に提供できます。VLAN インターフェイスには、1つ以上のレイヤー2 Ethernet ポート (「PA-7000 シリーズ レイヤー2 インターフェイス」を参照)を追加できます。

VLAN イン ターフェイス 設定	設定場所	の意味
インターフェ イス名	VLAN イン ターフェイス	読み取り専用の Interface Name[インターフェイス名] フィー ルドにはvlanが設定されています。インターフェイスを識別 する数値サフィックス(1 ~ 9,999)を隣のフィールドに入 力します。
コメント		インターフェイスの説明 (省略可) を入力します。
Netflowプロ ファイル		入力インターフェイスを通過する単向性の IP トラフィッ クを NetFlow サーバーにエクスポートする場合は、サー バー プロファイルを選択するか、Netflow Profile (Netflow プロファイル)をクリックして新しいプロファイルを定 義します(「Device (デバイス) > Server Profiles (サー バー プロファイル) > NetFlow」を参照)。None[なし] を選択すると、現在インターフェイスに割り当てられてい るNetFlowサーバーが解除されます。
VLAN	VLAN イン ターフェイス > 設定	VLAN を選択するか、VLAN をクリックして新しい VLAN を定義します(「Network(ネットワーク) > VLANs」を参 照)。None[なし] を選択すると、現在インターフェイスに割 り当てられているVLANが解除されます。
仮想ルー ター(VR)		インターフェイスに仮想ルーターを割り当てるか、Virtual Router (仮想ルーター)をクリックして新しい仮想ルー ターを定義します (「Network (ネットワーク) > Virtual Routers (仮想ルーター)」を参照)。None[なし]を選択す ると、現在インターフェイスに割り当てられているルーター が解除されます。
仮想システ ム(vsys)		ファイアウォールが複数の仮想システムをサポートし、そ の機能が有効の場合は、インターフェイスの仮想システム (vsys) を選択するか、Virtual System[仮想システム] リンクを クリックして新しい vsys を定義します。

VLAN イン ターフェイス 設定	設定場所	の意味
セキュリティ ゾーン		インターフェイス用のセキュリティゾーンを選択する か、Zone[ゾーン] をクリックして新しいゾーンを定義しま す。None[なし] を選択すると、現在インターフェイスに割 り当てられているゾーンが解除されます。

IPv4 アドレス

タイプ	VLAN イン ターフェイス > IPv4	IPv4 アドレス タイプをインターフェイスに割り当てる方法 を選択します。
		 Static[静的] – IP アドレスを手動で指定する必要があります。
		 DHCP Client[DHCP クライアント] – インターフェイスが DHCP (Dynamic Host Configuration Protocol) クライアン トとして機能し、ダイナミックに割り当てられた IP アド レスを受信できます。
		高可用性(HA)アクティブ/アクティブ構成の ファイアウォールは、DHCP クライアントをサ ポートしません。
		選択した IP アドレス方式に応じて、タブに表示されるオプ ションは異なります。

IPv4アドレス、タイプ=静的

IP	VLAN イン ターフェイス > IPv4	Add[追加] をクリックし、以下のいずれかの手順を実行し て、インターフェイスのスタティック IP アドレスとネット ワーク マスクを指定します。
		 CIDR (Classless Inter-Domain Routing)表記法の ip_address/maskの形式(例: 192.168.2.0/24)でエントリ を入力します。
		 タイプが IP netmask[IP ネットマスク]の既存のアドレス オブジェクトを選択します。
		 タイプが IP netmask (IP ネットマスク)のアドレス オブ ジェクトを作成します。
		インターフェイスに対して複数の IP アドレスを入力できま す。IP アドレスの最大数は、システムが使用する転送情報 ベース (FIB) によって決まります。
		不要になった IP アドレスを Delete(削除)します。

VLAN イン ターフェイス	設定場所	の意味
設定		

IPv4 アドレス、タイプ = DHCP クライアント

有効化	VLAN イン ターフェイス > IPv4	インターフェイスの DHCP クライアントを有効化する場合 に選択します。
サーバー提供 のデフォルト ゲートウェイ を指すデフォ ルト ルート を自動的に作 成		DHCP サーバーによって提供されるデフォルト ゲートウェ イを指し示すデフォルト ルートを自動的に作成する場合に選 択します。
ホスト名の送 信		ファイアウォール (DHCP クライアントとして) にインター フェイスのホスト名 (Option 12) を DHCP サーバーに送 信させる設定を行う場合に選択します。デフォルトで Send Hostname (ホスト名の送信) を行う場合、ファイアウォール のホスト名がホスト名フィールドで選択されます。その名前 を送信するか、カスタム ホスト名 (大文字および小文字、数 字、ピリオド、ハイフン、アンダースコアを含む最長 64 文 字) を入力します。
デフォルト ルート メト リック		ファイアウォールと DHCP サーバー間のルートについて は、必要に応じてルート メトリック(優先順位レベル)を入 力し、それをデフォルト ルートに関連付けて、パスの選択で 使用します(範囲は 1 ~ 65,535、デフォルトはなし)。数 値が小さいほど優先度が高くなります。
DHCP クライ アント ラン タイム情報の 表示		DHCP のリース状態、ダイナミック IP アドレス割り当 て、サブネット マスク、ゲートウェイ、サーバー設定 (DNS、NTP、ドメイン、WINS、NIS、POP3、および SMTP)など、DHCP サーバーから受信したすべての設定を 表示する場合に選択します。

IPv6アドレス、タイプ=静的

IPv6 の有効 > IPv6	インター	VLAN イン	このインターフェイスの IPv6 アドレスを有効にする場合に
化	フェースでの	ターフェイス	選択します。
	IPv6 の有効 化	> IPv6	

VLAN イン ターフェイス 設定	設定場所	の意味
インターフェ イス ID		64 ビット拡張一意識別子 (EUI-64) を 16 進数形式で入力し ます (例: 00:26:08:FF:FE:DE:4E:29)。このフィールドを空白 のままにすると、ファイアウォールが、物理インターフェイ スの MAC アドレスから生成された EUI-64 を使用します。 アドレスの追加時に Use interface ID as host portion[ホスト 部分にインターフェイス ID を使用] オプションを選択する と、ファイアウォールがそのアドレスのホスト部分にイン ターフェイス ID を使用します。
アドレス	VLAN イン ターフェイス > IPv6 > アド レス割り当て	IPv6 アドレスとプレフィックス長を追加します (2001:400:f00::1/64 など)。または、既存の IPv6 アドレス オブジェクトを選択するか、新しい IPv6 アドレス オブジェ クトを作成します。
インターフェ イス上のアド レスを有効に する		インターフェイスで IPv6 アドレスを有効にします。
ホスト部分に インターフェ イス ID を使 用		IPv6 アドレスのホスト部分に Interface (インターフェイス) ID を使用する場合に選択します。
エニーキャスト		最も近いノードを経由するルーティングを含める場合に選択 します。
RA を送信す る	VLAN イン ターフェイス > IPv6 > アド レス割り当て	この IPv6 アドレスのルータ アドバタイズメント(RA)を 有効にする場合に選択します。このオプションを選択す る場合は、[Router Advertisement タブの Enable Router Advertisement も必要になります。
		残りのフィールドは、Send RA を有効にした場合にのみ適用 されます。
		 Valid Lifetime – firewall がアドレスを有効と見なす時間の長さ(秒単位)。有効なライフタイムは、Preferred Lifetime[優先ライフタイム]以上でなければなりません。 デフォルトは 2,592,000 です。
		 Preferred Lifetime (優先ライフタイム)–有効なアドレス が優先される時間(秒)です。この時間内は、ファイア ウォールがこのアドレスを使用してトラフィックを送受 信できます。優先有効期間が終了すると、firewall はその

VLAN イン ターフェイス 設定	設定場所	の意味
		アドレスを使用して新しい接続を確立できなくなります が、既存の接続は Valid Lifetime を超えるまで有効で す。デフォルトは 604,800 です。
		 On-link(オンリンク) – 通知されたプレフィックス内に IP アドレスがあるシステムにルーターなしで到達可能な 場合に選択します。
		 Autonomous(自律型) – 通知されたプレフィックスと インターフェイス ID を組み合わせて、システムが IP アド レスを独自に作成できる場合に選択します。

IPv6 アドレス、タイプ = DHCPv6 クライアント

ルーターがア ドバタイズし たルートを受 け入れる	VLAN イン ターフェイス > IPv6 > アド レス割り当 て、タイプ = DHCPv6 クラ イアント	DHCPv6 クライアントが DHCP サーバからの RA を受け入 れることを許可する場合に選択します。
デフォルト ルート メト リック		インターフェイスから ISP へのルートのデフォルト ルート メトリックを入力します。範囲は 1 から 65,535 です。デ フォルトは 10 です。
優先		DHCPv6 クライアント インターフェイス (low、medium、 または high) のプリファレンスを選択して、2 つのインター フェイス (それぞれが冗長性のために異なる ISP に接続され ている) がある場合に、一方の ISP のインターフェイスにも う一方の ISP のインターフェイスよりも高い優先順位を割り 当てることができます。優先インターフェイスに接続され ている ISP は、ホスト側のインターフェイスに送信するデリ ゲートされたプレフィックスを提供する ISP になります。イ ンターフェイスのプリファレンスが同じ場合、両方の ISP が 委任されたプレフィックスを提供し、ホストが使用するプレ フィックスを決定します。
IPv6 アドレ スを有効にす る	VLAN イン ターフェイス > IPv6 > アド レス割り当 て、タイプ = DHCPv6 ク ライアント > DHCPv6 オプ ション	この DHCPv6 クライアント用に受信した IPv6 アドレスを有 効にします。
非一時アドレ ス		firewall の非一時アドレスを、委任側ルータと ISP に面する この DHCPv6 クライアント インターフェイスに割り当てる ように要求します。インターフェイスのセキュリティ レベル が低いことが許容される場合は、[非一時アドレス] を選択し ます (アドレスの寿命が長いため)。

VLAN イン ターフェイス 設定	設定場所	の意味
		インターフェイスに非一時アドレスまたは一時 アドレスのどちらを要求するかは、ユーザー の裁量とDHCPv6サーバーの機能に基づきま す。一部のサーバーは、一時的なアドレスしか 提供できません。ベストプラクティスは、非一 時アドレスと一時アドレスの両方を選択するこ とであり、その場合、ファイアウォールは非一 時アドレスを優先します。
一時アドレス		委任ルータと ISP に面するこの DHCPv6 クライアント イン ターフェイスに割り当てるファイアウォールの一時アドレス を要求します。[一時アドレス]を選択すると、アドレスが短 期間使用されることを意図しているため、セキュリティのレ ベルが高くなります。
迅速なコミッ ト		Solicit、Advertise、Request、および Reply メッセージのプロセスではなく、Solicit および Reply メッセージの DHCP プロセスを使用する場合に選択します。
プレフィック ス委任を有効 にする	VLAN イン ターフェイス > IPv6 > アド レス割り当 て、タイプ = DHCPv6 クラ イアント > プ レフィックス 委任	プレフィックス委任を有効にして、firewall がプレフィック ス委任機能をサポートできるようにします。つまり、イン ターフェイスはアップストリーム DHCPv6 サーバからプレ フィックスを受け入れ、選択したプレフィックス プールに プレフィックスを配置し、そこから firewall が SLAAC を介 してホストにプレフィックスを委任します。インターフェ イスのプレフィックス委任を有効または無効にする機能に より、firewall は複数の ISP (インターフェイスごとに 1 つの ISP)をサポートできます。このインタフェースでプレフィッ クス委任を有効にすると、プレフィックスを提供する ISP を 制御します。DHCP サーバーから受信した委任されたプレ フィックスは、それを要求したインターフェイスでは使用で きません。
DHCP プレ フィックス長 のヒント		選択すると、ファイアウォールが優先 DHCPv6 プレフィッ クス長を DHCPv6 サーバに送信できるようになります。
DHCP プレ フィックス長 (ビット)		DHCPv6 サーバにヒントとして送信される優先 DHCPv6 プ レフィックス長を 48 ~ 64 ビットの範囲で入力します。

VLAN イン ターフェイス 設定	設定場所	の意味
		 たとえば、プレフィックス長48を要求すると、サブネット(64-48)に16ビットが残り、 委任するにはそのプレフィックスの多くのサブディビジョンが必要であることを示します。一方、プレフィックス長63を要求すると、2つのサブネットのみを委任するために1ビットが残ります。128ビットのうち、ホストアドレス用にさらに64ビットあります。
プレフィック ス プール名	7	ファイアウォールが受信したプレフィックスを保存するプレ フィックス プールの名前を入力します。名前は一意で、最大 63 文字の英数字、ハイフン、ピリオド、およびアンダース コアを含む必要があります。 認識しやすいように、 <i>ISP</i> を反映したプレ フィックス プール名を使用します。

IPv6アドレス、タイプ=継承

名前	VLAN イン ターフェイス > IPv6 > アド レス割り当 て、タイプ = 継承	Add プール名を入力してプールを作成します。名前には、最 大 63 文字の英数字、ハイフン、ピリオド、およびアンダー スコアを使用できます。
アドレスタ		以下のうち1つを選択します。
イプ		 GUA from Pool:選択されたプレフィックス プールからの グローバル ユニキャスト アドレス(GUA)。この GUA を 取得することが、プレフィックス委任を使用する目標で す。 ULA:一意のローカル アドレスは、プライベート ネット ワーク内の接続用のアドレス範囲 fc00::/7 のプライベー ト アドレスです。DHCP サーバーがない場合は、ULA を 選択します。
インターフェ イスで有効に する		インターフェイスでアドレスを有効にします。
プレフィック ス プール		GUA を取得するプレフィックス プールを選択します。

VLAN イン ターフェイス 設定	設定場所	の意味
割り当てタイ プ	VLAN イン ターフェイス > IPv6 > アド レス割り当 て、タイプ = 継承	 割り当てタイプを選択します。 Dynamic:DHCPv6 クライアントは、継承されたインターフェイスを構成するための識別子を選択します。 Dynamic with Identifier - 0 から 4,000 の範囲の識別子を選択し、DHCPv6 クライアント全体で一意の識別子を維持する責任があります。
ルーター通知 を送信		インターフェイスから LAN ホストにルータ アドバタイズメ ント(RA)を送信する場合に選択します。
オンリンク		プレフィックス内にアドレスを持つシステムがルーターなし で到達できるかどうかを選択します。
自主的な		システムが、アドバタイズされたプレフィックスとインター フェイス ID を組み合わせて IPv6 アドレスを個別に作成でき るかどうかを選択します。
重複アドレス 検出を有効に する	VLAN イン ターフェイ ス > IPv6 > Address Resolution (アドレス解 決)	重複アドレス検出(DAD)を有効にする場合に選択します。 これにより DAD Attempts(試行回数)を指定できます。
DAD 試行回 数		ネイバー要請間隔 (NS Interval (NS 間隔)) の内にDADを試 行する回数を指定します(範囲は 1 ~ 10、デフォルトは 1)。この回数を超えるとネイバーに障害があるとみなされ ます。
到達可能時間		クエリと応答が正常に行われた後引き続きネイバーに到達可 能な時間(秒)を指定します(範囲は1~36,000、デフォ ルトは30)。
NS 間隔 (秒)		DADの試行秒数を指定します(範囲は 1 ~ 10、デフォルトは 1)。この秒数を超えると障害があるとみなされます。
NDP モニタ リングの有効 化		Neighbor Discovery Protocol のモニタリン グを有効にする場合に選択します。有効に なっていると、NDP(Features(機能)列の を選択し、ファイアウォールで検出されたネイバーの IPv6 アドレス、対応する MAC アドレスおよび User-ID などの情 報を(ベストケース ベースで)表示できます。

設定	VLAN イン ターフェイス 設定	設定場所	の意味
----	--------------------------------	------	-----

IPv6 アドレス、タイプ=スタティックまたはタイプ=継承

ルーター通知 を有効にする	VLAN イン ターフェイス > IPv6 > ルー ター アドバ タイズメン ト、タイプ = 静的またはタ イプ - 継承	IPv6 インターフェイスのネイバー検出を指定して、このセクションの他のフィールドを設定する場合に選択します。ルーター通知(RA)メッセージを受信する IPv6 DNS クライアントは、この情報を使用します。
		RA により、ファイアウォールが、スタティックに設定さ れていない IPv6 ホストのデフォルト ゲートウェイとして 機能し、ホストにアドレス設定の IPv6 プレフィックスを提 供できます。別の DHCPv6 サーバーをこの機能と併用する と、DNS および他の設定をクライアントに提供できます。
		これはインターフェイスのグローバル設定です。IP アドレ スごとに RA オプションを設定する場合は、アドレスを IP アドレス テーブルに Add(追加)して設定します。IP アド レスに RA オプションを設定する場合は、インターフェイス の Enable Router Advertisement(ルーター通知を有効にす る)必要があります。
最小間隔(秒)		ファイアウォールが送信する RA 間の最小間隔(秒)を指定 します(範囲は 3 ~ 1,350、デフォルトは 200)。ファイア ウォールは、設定した最小値と最大値の間のランダムな間隔 で RA を送信します。
最大間隔(秒)	-	ファイアウォールが送信する RA 間の最大間隔(秒)を指定 します(範囲は 4 ~ 1,800、デフォルトは 600)。ファイア ウォールは、設定した最小値と最大値の間のランダムな間隔 で RA を送信します。
ホップ制限	-	クライアントに適用する、送信パケットのホップ制限を指定 します(範囲は 1 ~ 255、デフォルトは 64)。ホップ制限 を指定しない場合は 0 を入力します。
リンク MTU	VLAN イン ターフェイス > IPv6 > ルー ター アドバ	クライアントに適用するリンク最大伝送単位 (MTU) を 指定する (範囲は 1,280 ~ 1,500)、またはデフォルトで unspecified (未指定)に指定します。これはシステムのデフォ ルトにマッピングされます。
到達可能時間 (ミリ秒)	ト、タイプ = 静的またはタ イプ = 継承	到達可能確認メッセージを受信後ネイバーに到達可能である と想定する際にクライアントが使用する到達可能時間 (ミリ 秒)を指定します (範囲は 0 ~ 3,600,000) またはデフォルト

VLAN イン ターフェイス 設定	設定場所	の意味
		の unspecified (未指定)に指定します。これはシステムのデ フォルトにマッピングされます。
リトランス ミッション時 間 (ミリ秒)		ネイバー要請メッセージを再送信するまでにクライアントが 待機する時間 (ミリ秒単位) を決定するリトランスミッション タイマーを指定します (範囲は 0 ~ 4,294,967,295) またはデ フォルトの unspecified (未指定)に指定します。これはシステ ムのデフォルトにマッピングされます。
ルーターの有 効期間 (秒)		クライアントがファイアウォールをデフォルトゲートウェ イとして使用する時間を秒単位で指定します(範囲は 0 ~ 9,000、デフォルトは 1,800)。0は、ファイアウォールがデ フォルト ゲートウェイではないことを示します。有効期間が 過ぎると、クライアントがそのデフォルト ルーター リスト からファイアウォール エントリを削除して、別のルーターを デフォルト ゲートウェイとして使用します。
ルーター設定		ネットワーク セグメントに複数の IPv6 ルーターがある場合 は、クライアントがこのフィールドを使用して優先ルーター を選択します。セグメントの他のルーターとの比較におい て、RA が通知するファイアウォール ルーターの優先度を High、Medium (デフォルト)、Low の中から選択します。
到達可能時間 (ミリ秒)	VLAN イン ターフェイス > IPv6 > ルー ター アドバ タイズメン ト、タイプ = 静的またはタ イプ = 継承	到達可能確認メッセージを受信後ネイバーに到達可能である と想定する際にクライアントが使用する到達可能時間(ミリ 秒)を指定します(範囲は 0 ~ 3,600,000)またはデフォルト の unspecified (未指定)に指定します。これはシステムのデ フォルトにマッピングされます。
リトランス ミッション時 間 (ミリ秒)		ネイバー要請メッセージを再送信するまでにクライアントが 待機する時間 (ミリ秒単位) を決定するリトランスミッション タイマーを指定します (範囲は 0 ~ 4,294,967,295) またはデ フォルトの unspecified (未指定)に指定します。これはシステ ムのデフォルトにマッピングされます。
ルーターの有 効期間 (秒)		クライアントがファイアウォールをデフォルトゲートウェ イとして使用する時間を秒単位で指定します(範囲は 0 ~ 9,000、デフォルトは 1,800)。0は、ファイアウォールがデ フォルト ゲートウェイではないことを示します。有効期間が 過ぎると、クライアントがそのデフォルト ルーター リスト からファイアウォール エントリを削除して、別のルーターを デフォルト ゲートウェイとして使用します。
ネットワーク

VLAN イン ターフェイス 設定	設定場所	の意味
ルーター設定		ネットワーク セグメントに複数の IPv6 ルーターがある場合 は、クライアントがこのフィールドを使用して優先ルーター を選択します。セグメントの他のルーターとの比較におい て、RA が通知するファイアウォール ルーターの優先度を High、Medium (デフォルト)、Low の中から選択します。
管理された設 定	-	アドレスを DHCPv6 経由で使用できることをクライアント に示す場合に選択します。
その他の設定	-	他のアドレス情報(DNS 関連の設定など)を DHCPv6 経由 で使用できることをクライアントに示す場合に選択します。
整合性チェッ ク		他のルーターから送信された RA がリンク上で一貫した情報 を通知していることをファイアウォールで確認する場合に選 択します。ファイアウォールでは、システム ログの不一致が 記録されます。タイプは ipv6nd です。

IPv6 アドレス、DNS サポート (タイプ = 静的)

ルーター通知 に DNS 情報 を含める	VLAN イン ターフェイス > IPv6 > DNS サポート、タ イプ = 静的	DNS サポートは、[ルーター アドバタイズメント] タブで Enable Router Advertisement を選択した場合に使用できま す。 ファイアウォールがこの IPv6 イーサネット インターフェイ スから NDP ルーター通知で DNS 情報を送信するように選択 します。その他の DNS サポート フィールド (サーバー、有 効期間、ドメイン検索リスト、および有効期間) は、このオ プションを選択した後にのみ表示されます。
サーバー		1つ以上の再帰 DNS (RDNS) サーバー アドレスを Add (追加) し、ファイアウォールがこの IPv6 Ethernet インター フェイスから NDP ルーター通知によって送信できるように します。RDNS サーバーは、一連の DNS ルックアップ要求 をルート DNS および権威 DNS サーバーに送信し、最終的に IP アドレスを DNS クライアントに提供します。
		最大8個のRDNSサーバーを設定し、ファイアウォールで NDPルーター通知に含めて受信者に送信できます(設定 の上から下の順に送信します)。その後、受信者は同じ順 序でこれらを使用できます。サーバーの順序を変更するに は、サーバーを選択して Move Up(上へ)移動したり Move Down(下へ)移動したりします。サーバーが必要なくなっ たら、そのサーバーをリストから Delete(削除)します。

VLAN イン ターフェイス 設定	設定場所	の意味
有効期間		IPv6 DNS クライアントがルーター通知を受信した後 で、RDNS サーバーを使用してドメイン名を解決できるよう になるまでの最長時間 (秒) を入力します (範囲はMax Interval (最大間隔) (秒)からMax Interval (最大間隔) (秒)の 2 倍、デ フォルトは 1,200)。
ドメイン検索 リスト		 DNS 検索リスト (DNSSL) のドメイン名 (サフィックス) を1つ以上 Add (追加) します。最大長は255 バイトです。 DNS 検索リストは、DNS クライアント ルーターが DNS ク エリに名前を入力する前に非修飾ドメイン名に (1つずつ) 追加するドメイン サフィックスのリストです。これによ り、クエリで完全修飾ドメイン名が使用されます。たとえ ば、DNS クライアントがサフィックスのない「quality」と いう名前の DNS クエリを送信しようとすると、ルーターは ピリオドと DNS 検索リストの最初の DNS サフィックスを 名前に追加して DNS クエリを送信します。リストの最初の DNS サフィックスが「company.com」の場合、ルーターの クエリの完全修飾ドメイン名は「quality.company.com」に なります。 DNS クエリに失敗すると、ルーターはリストの 2 番目の DNS サフィックスを非修飾名に追加して、新しい DNS クエ リを送信します。ルーターは、DNS ルックアップが成功す るまで(残りのサフィックスは無視)、またはルーターがリ ストのすべてのサフィックスを試すまで、DNS サフィック スを使用します。 ネイバー検出 DNSSL オプションで DNS クライアント ルー ターに提供するサフィックスにより、ファイアウォールを設 定します。DNSSL オプションを受信する DNS クライアント は非修飾 DNS クエリでそのサフィックスを使用します。 NDP ルーターアドバタイズメントとしてファイアウォール が上から順に送信するDNS検索リストオプションには、最 大8つのドメイン名 (サフィックス) を設定できます。受信 者は同じ順番でこれを使用します。順序を変更するには、サ フィックスを選択して Move Up (上へ) 移動したり Move Down (下へ) 移動したりします。サフィックスが必要なく なったら、そのサフィックスを Delete (削除) します。
有効期間		IPv6 DNS クライアントがルーター通知を受信した後 に、DNS 検索リストのドメイン名 (サフィックス) を使用で きる最大秒数を入力します (範囲はMax Interval (最大間隔)

ネットワーク

VLAN イン ターフェイス 設定	設定場所	の意味
		(秒)の値からMax Interval (最大間隔) (秒)の 2 倍までで、デ フォルトは 1,200 です)。

IPv6 アドレス、DNS サポート (種類 = DHCPv6 クライアントまたは種類 = 継承)

DNS 再帰 ネーム サー バー	VLAN イン ターフェイス > IPv6 > DNS サポート、種 類 = DHCPv6 クライアント または種類 = 継承	 以下を有効にして選択します。 DHCPv6:DHCPv6 サーバに DNS 再帰ネーム サーバ情報 を送信させます。 Manual:DNS 再帰ネーム サーバを手動で設定します。 Manual, Add を選択した場合、firewall は、この IPv6 VLAN インターフェイスから NDP ルーター アドバタイズメントを 送信するために、再帰 DNS (RDNS) Server アドレスを使用し ます。RDNS サーバーは、ルート DNS サーバーと権限のあ る DNS サーバーに一連の DNS ルックアップ要求を送信し、 最終的に DNS クライアントに IP アドレスを提供します。 最大 8 個の RDNS サーバーを設定し、ファイアウォールで それらを NDP ルーター通知に含めて受信者に送信できます (設定の上から下の順に送信します)。その後、受信者は同 じ順序でこれらを使用できます。サーバーを選択し、不要に なったサーバーの順序を変更するには [Move Up (上へ移動)] または [Move Down (下へ移動)] または [Delete (消去)] サー バーを選択します。
有効期間		IPv6 DNS クライアントがルーター通知を受信した後 に、RDNS サーバーを使用してドメイン名を解決できる最大 秒数を入力します(範囲は最大間隔(秒)の値からその2倍 までで、デフォルトは 1,200 です)。
ドメイン検索 リスト	VLAN イン ターフェイス > IPv6 > DNS サポート、種 類 = DHCPv6 クライアント または種類 = 継承	 以下を有効にして選択します。 DHCPv6:DHCPv6 サーバにドメイン検索リストを送信させます。 Manual - ドメイン検索リストを手動で構成します。 Manual、Add を選択し、DNS 検索リスト (DNSSL) に 1 つ以上の Domain 名(サフィックス)を設定する場合。サフィックスの最大長は 255 バイトです。 DNS 検索リストは、DNS クライアント ルーターが DNS クエリに名前を入力する前に非修飾ドメイン名に(1 つずつ)追加するドメインサフィックスのリストです。これにより、DNS クエリで完全修飾ドメイン名が使用されま

VLAN イン ターフェイス 設定	設定場所	の意味
		す。たとえば、サフィックスなしの「quality」という名前 の DNS クエリを DNS クライアントが送信しようとしてい ます。この場合、ルーターはピリオドと、DNS 検索リス トの 1 番目の DNS サフィックスを名前に付加し、DNS ク エリを転送します。リストの最初の DNS サフィックスが 「company.com」の場合、ルーターの DNS クエリの完全修 飾ドメイン名は「quality.company.com」になります。
		DNS クエリに失敗すると、ルーターはリストの2番目の DNS サフィックスを非修飾名に追加して、新しい DNS クエ リを送信します。ルーターは DNS ルックアップが成功する か(残りのサフィックスは無視されます)、ルーターがリス トのすべてのサフィックスを試行するまで DNS サフィック スを試行します。
		ネイバー検出 DNSSL オプションで DNS クライアント ルー ターに提供するサフィックスにより、ファイアウォールを設 定します。DNSSL オプションを受信する DNS クライアント は非修飾 DNS クエリでそのサフィックスを使用します。
		DNS 検索リストに対して最大 8 個のドメイン名(サフィッ クス)を設定し、ファイアウォールでそれらを NDP ルー ター通知に含めて受信者に送信できます(設定の上から下の 順に送信します)。その後、受信者は同じ順序でこれらのア ドレスを使用できます。サフィックスを選択し、Move Up または Move Down の順序を変更するか、不要になったとき にリストからサフィックスを Delete します。
有効期間		IPv6 DNS クライアントがルーター通知を受信した後 に、DNS 検索リストのドメイン名(サフィックス)を使用 できる最大秒数を入力します(範囲は最大間隔(秒)の値か らその 2 倍までで、デフォルトは 1,200 です)。
上級	· · · · · · · · · · · · · · · · · · ·	

管理プロファ イル	VLAN イン ターフェイス > 上級 > その 他の情報	Management Profile[管理プロファイル] – このインターフェ イスを介したファイアウォールの管理に使用できるプロトコ ル (SSH、Telnet、HTTP など) を定義するプロファイルを選 択します。None[なし] を選択すると、現在インターフェイ スに割り当てられているプロファイルが解除されます。
MTU		このインターフェイスで送信されるパケットの最大転送単位 (MTU)をバイト数で入力します(範囲は 576 ~9,192、 デフォルトは 1,500)。ファイアウォールの両側のマシンが Path MTU Discovery (PMTUD)を実行し、インターフェイス

VLAN イン ターフェイス 設定	設定場所	の意味
		が MTU を超えるパケットを受信すると、ファイアウォール が送信元にパケットが大きすぎることを示す ICMP フラグメ ント要求メッセージを返します。
TCP MSS の 調整		ヘッダーのバイト数に対応できるようにインターフェイス の MTU バイト サイズ以内の値で最大セグメント サイズ (MSS)を調整する場合は選択します。MTUバイトサイズ とMSS調整サイズはMSSバイトサイズと等しい値になり、こ れはIPによって異なります。
		 IPv4 MSS Adjustment Size (IPv4 MSS調整サイズ) – 範囲 は40~300、デフォルトは40です。
		 IPv6 MSS Adjustment Size (IPv6 MSS調整サイズ) – 範囲 は60~300、デフォルトは60です。
		ネットワークを通るtunnel[トンネル]のMSSを小さくする必要がある場合はこれらの設定を行ってください。フラグメント化を行わないパケットのバイト数がMSSよりも大きい場合、この設定を行うことでサイズが調整されるようになります。
		カプセル化によりヘッダーが延長されるので、MSS調整サイ ズはMPLSヘッダーやVLANタグを持つトンネルトラフィック よりも大きく設定しておくと便利です。
IPアドレス MAC アドレ ス インターフェ イス	VLAN イン ターフェイス > 上級 > ARP エントリ	1つ以上のスタティックアドレス解決プロトコル (ARP) エ ントリを追加するには、Add[追加] をクリックし、IPアドレ スとそれに関連付けられたハードウェア (メディアアクセス 制御、略称 MAC) のアドレスを入力して、ハードウェアア ドレスにアクセスできるレイヤー3インターフェイスを選 択します。エントリを削除するには、エントリを選択して Delete[削除] をクリックします。静的 ARP エントリによっ て、指定したアドレスの ARP 処理が減り、中間者攻撃が防 止されます。
IPv6アドレ ス MAC アドレ ス	VLAN イン ターフェイス > 上級 > ND エントリー	NDP(Neighbor Discovery Protocol)のネイバー情報を指定 するには、Add(追加)をクリックし、ネイバーの IPv6 ア ドレスと MAC アドレスを入力します。
NDP プロキ シの有効化	VLAN イン ターフェイス	選択すると、インターフェイスで NDP (Neighbor Discovery Protocol) プロキシが有効になります。ファイアウォール は、このリストの IPv6 アドレスの MAC アドレスを要求す る ND パケットに応答します。ND に対する応答として、

VLAN イン ターフェイス 設定	設定場所	の意味
	> 上級 > NDP プロキシ	ファイアウォールは、そのインターフェイス独自の MAC ア ドレスを送信し、基本的には、これらのアドレス宛のパケッ トを要求します。
		(推奨)NPTv6 (Network Prefix Translation IPv6) を使用する 場合は、NDPプロキシを有効化します。
		Enable NDP Proxy[NDPプロキシの有効化] を選択した場合、 フィルタ条件を入力しフィルタを適用(緑色の矢印をクリッ ク)することで、膨大なAddress[アドレス] のエントリから 絞り込みを行うことができます。
アドレス		1つ以上のIPv6アドレス、IP範囲、IPv6サブネット、または ファイアウォールがNDPプロキシとして機能するアドレスオ ブジェクトを入力する場合はAdd[追加]をクリックします。 これらのアドレスの1つは、NPTv6の送信元変換のアドレ スと同じであることが理想的です。アドレスの順序は問題に なりません。
		アドレスがサブネットワークの場合、ファイアウォールはサ ブネットのすべてのアドレスに対して ND 応答を送信しま す。したがって、ファイアウォールの IPv6 ネイバーも追加 し、Negate (除外) をクリックして、これらの IP アドレス に応答しないようファイアウォールに指示設定することをお 勧めします。
Negate	-	あるアドレスに対して Negate [除外] チェック ボックスをオ ンにすると、NDPプロキシは、そのアドレスを拒否するよう になります。Negate は、指定した IP アドレス範囲または IP サブネットの一部に対して実行できます。
設定	VLAN イン ターフェイ	Settings (設定) を選択して DDNS フィールドを設定できるようにします。
有効化	⊣	インターフェースで DDNS を有効化します。初めに DDNS を有効化してから設定を行う必要があります。(DDNS の設 定が終わっていない場合は有効化せずに保存し、部分的な設 定を保持することができます)
更新間隔(日 数)		FQDN にマッピングされた IP アドレスを更新するために ファイアウォールが DDNS サーバーに送信する更新間隔 (日数)を入力します(範囲は1~30、デフォルトは 1)。

VLAN イン ターフェイス 設定	設定場所	の意味
		また、ファイアウォールはDHCP サーバーから インターフェイスの新しい IP アドレスを受診 した際も DDNS を更新します。
証明書プロ ファイル	-	DDNS サービスを検証するために作成した(あるいは新しく 作成する)証明書プロファイルを選択します。DDNS サービ スは、認証局(CA)が署名した証明書をファイアウォール に提供します。
ホスト名		DDNS サーバーに登録されたインターフェイスのホスト 名(例:host123.domain123.com、or host123)を入力し ます。DNS がドメイン名として許可している有効な文字 を使った構文になっていることを確認する以外、ファイア ウォールはホスト名の検証を行いません。
ベンダー	-	DDNS サービスをこのインターフェイスに提供する DDNS ベンダー(およびバージョン番号)を選択します: • DuckDNS v1
		DynDNS v1
		FreeDNS Afraid.org Dynamic API v1
		 FreeDNS Afraid.org v1 No JDv1
		 ⑦ ファイアウォールが特定の日で失効すると示唆 する DDNS サービスの古いバージョンを選択 する場合、新しいバージョンに移動させます。
		ベンダー名に続くName (名前)およびValue (値)フィールド は、ベンダー固有のものです。ファイアウォールが DDNS サービスに接続するために使用するパラメーターを示す読み 取り専用フィールドもあります。DDNS サービスプロバイ ダーが提供するパスワード、DDNS サーバーからの応答がな い場合にファイアウォールが使用するタイムアウトなど、他 のフィールドを設定します。
IPv4 タブ - IP		インターフェイスで設定した IPv4 アドレスを追加し、それ を選択します。選択されたすべての IP アドレスは DDNS プ ロバイダー(ベンダー)に登録されています。

VLAN イン ターフェイス 設定	設定場所	の意味
IPv6 タブ - IPv6	Ethernet Interface (イーサネッ トインター フェイス) > Advanced (詳細) > DDNS(cont)	インターフェイスで設定した IPv6 アドレスを追加し、それ を選択します。選択されたすべての IP アドレスは DDNS プ ロバイダー(ベンダー)に登録されています。
ランタイム情 報の表示		DDNS 登録を表示します:DDNS プロバイダー、解決された FQDN、マッピングされた IPアドレス(アスタリスク(*) はプライマリ IP アドレスを示します)。トラブルシュー ティングを目的として、各 DDNS プロバイダーにはホスト 名の更新状態を示す独自の返却コードおよび返却日が必要に なります。

Network > Interfaces > Loopback [ネットワーク > イン ターフェイス > ループバック]

以下のフィールドを使用して、ループバック インターフェイスを設定します。

ループバック インターフェ イス設定	設定場所	の意味
インターフェ イス名	ループバック インターフェ イス	読み取り専用のInterface Name[インターフェイス名] フィー ルドには loopbackが設定されています。インターフェイス を識別する数値サフィックス (1 ~ 9999) を隣のフィールド に入力します。
コメント		インターフェイスの説明 (省略可) を入力します。
Netflowプロ ファイル		入力インターフェイスを通過する単向性の IP トラフィッ クを NetFlow サーバーにエクスポートする場合は、サー バー プロファイルを選択するか、Netflow Profile (Netflow プロファイル) をクリックして新しいプロファイルを定 義します (「Device (デバイス) > Server Profiles (サー バー プロファイル) > NetFlow」を参照)。None[なし] を選択すると、現在インターフェイスに割り当てられてい るNetFlowサーバーが解除されます。
仮想ル ー ター(VR)	ループバック インターフェ イス > コン フィグ	インターフェイスに仮想ルーターを割り当てるか、Virtual Router (仮想ルーター)をクリックして新しい仮想ルー ターを定義します (「Network (ネットワーク) > Virtual Routers (仮想ルーター)」を参照)。None[なし]を選択す ると、現在インターフェイスに割り当てられているルーター が解除されます。
仮想システ ム(vsys)		ファイアウォールが複数の仮想システムをサポートし、そ の機能が有効の場合は、インターフェイスの仮想システム (vsys) を選択するか、Virtual System[仮想システム] リンクを クリックして新しい vsys を定義します。
セキュリティ ゾーン		インターフェイス用のセキュリティゾーンを選択する か、 Zone [ゾーン] をクリックして新しいゾーンを定義しま す。 None [なし] を選択すると、現在インターフェイスに割 り当てられているゾーンが解除されます。
管理プロファ イル	トンネルイン ターフェイス	Management Profile[管理プロファイル] – このインターフェ イスを介したファイアウォールの管理に使用できるプロトコ

ループバック インターフェ イス設定	設定場所	の意味
	 上級 > その 他の情報 	ル (SSH、Telnet、HTTP など) を定義するプロファイルを選 択します。None[なし] を選択すると、現在インターフェイ スに割り当てられているプロファイルが解除されます。
MTU	-	このインターフェイスで送信するパケットの最大転送単位 (MTU)をバイト数で入力します(576~9,192、デフォ ルトは 1,500)。ファイアウォールの両側のマシンが Path MTU Discovery (PMTUD)を実行し、インターフェイスが MTU を超えるパケットを受信すると、ファイアウォールが 送信元にパケットが大きすぎることを示す ICMP フラグメン ト要求メッセージを返します。
TCP MSS の 調整		ヘッダーのバイト数に対応できるようにインターフェイス の MTU バイト サイズ以内の値で最大セグメント サイズ (MSS)を調整する場合は選択します。MTUバイトサイズ とMSS調整サイズはMSSバイトサイズと等しい値になり、こ れはIPによって異なります。
		 IPv4 MSS Adjustment Size[IPv6 MSS調整サイズ] – 範囲 は40~300、デフォルトは40です。
		 IPv6 MSS Adjustment Size[IPv6 MSS調整サイズ] – 範囲 は60~300、デフォルトは60です。
		ネットワークを通るtunnel[トンネル]のMSSを小さくする必要がある場合はこれらの設定を行ってください。フラグメント化を行わないパケットのバイト数がMSSよりも大きい場合、この設定を行うことでサイズが調整されるようになります。
		カプセル化によりヘッダーが延長されるので、MSS調整サイ ズはMPLSヘッダーやVLANタグを持つトンネルトラフィック よりも大きく設定しておくと便利です。

IPv4 アドレスの場合

IP	ループバック インターフェ イス > IPv4	Add[追加] をクリックし、以下のいずれかの手順を実行し て、インターフェイスのスタティック IP アドレスとネット ワーク マスクを指定します。
		 /32 のサブネット マスクで IPv4 アドレスを入力します。 例: 192.168.2.1/32。/32 サブネット マスクのみがサポートされています。
		 タイプが IP netmask[IP ネットマスク]の既存のアドレス オブジェクトを選択します。

ループバック インターフェ イス設定	設定場所	の意味
		 Adress[アドレス] をクリックし、タイプが IP netmask[IP ネットマスク] のアドレスオブジェクトを作成します。
		インターフェイスに対して複数の IP アドレスを入力できま す。IP アドレスの最大数は、システムが使用する転送情報 ベース (FIB) によって決まります。
		IP アドレスを削除するには、アドレスを選択して Delete[[削 除]] をクリックします。

IPv6 アドレスの場合

インター フェースでの IPv6 の有効 化	ループバック インターフェ イス > IPv6	このインターフェイスの IPv6 アドレスを有効にする場合に 選択します。
インターフェ イス ID		64 ビット拡張一意識別子 (EUI-64) を 16 進数形式で入力し ます (例: 00:26:08:FF:FE:DE:4E:29)。このフィールドを空白 のままにすると、ファイアウォールが、物理インターフェイ スの MAC アドレスから生成された EUI-64 を使用します。 アドレスの追加時に Use interface ID as host portion[ホスト 部分にインターフェイス ID を使用] オプションを選択する と、ファイアウォールがそのアドレスのホスト部分にイン ターフェイス ID を使用します。
アドレス		Add[追加] をクリックして、IPv6 アドレスごとに以下のパラ メータを設定します。
		 Address[アドレス] – IPv6 アドレスとプレフィックス長を 入力します (例: 2001:400:f00::1/64)。既存のIPv6アドレ スオブジェクトを選択することや、Address[アドレス] を クリックしてアドレスオブジェクトを作成することもで きます。
		 Enable address on interface (インターフェイス上のアドレスを有効にする) – インターフェイスの IPv6 アドレスを有効にする場合に選択します。
		 Use interface ID as host portion (ホスト部分にインターフェイス ID を使用) – IPv6 アドレスのホスト部分に Interface ID (インターフェイス ID) を使用する場合に選択します。
		 Anycast(エニーキャスト) – 最も近いノードを経由する ルーティングを含める場合に選択します。

Network > Interfaces > Tunnel [ネットワーク > イン ターフェイス > トンネル]

以下のフィールドを使用して、トンネル インターフェイスを設定します。

トンネル イン ターフェイス 設定	設定場所	の意味
インターフェ イス名	トンネルイン ターフェイス	読み取り専用のInterface Name[インターフェイス名] フィー ルドにはtunnelが設定されています。インターフェイスを識 別する数値サフィックス (1 ~ 9999) を隣のフィールドに入 力します。
コメント		インターフェイスの説明 (省略可) を入力します。
Netflowプロ ファイル		入力インターフェイスを通過する単向性の IP トラフィッ クを NetFlow サーバーにエクスポートする場合は、サー バー プロファイルを選択するか、Netflow Profile (Netflow プロファイル)をクリックして新しいプロファイルを定 義します (「Device (デバイス) > Server Profiles (サー バー プロファイル) > NetFlow」を参照)。None[なし] を選択すると、現在インターフェイスに割り当てられてい るNetFlowサーバーが解除されます。
仮想ルー ター(VR)	トンネルイン ターフェイス > コンフィグ	インターフェイスに仮想ルーターを割り当てるか、Virtual Router (仮想ルーター)をクリックして新しい仮想ルー ターを定義します (「Network (ネットワーク) > Virtual Routers (仮想ルーター)」を参照)。None[なし]を選択す ると、現在インターフェイスに割り当てられているルーター が解除されます。
仮想システ ム(vsys)		ファイアウォールが複数の仮想システムをサポートし、そ の機能が有効の場合は、インターフェイスの仮想システム (vsys) を選択するか、Virtual System[仮想システム] リンクを クリックして新しい vsys を定義します。
セキュリティ ゾーン		インターフェイス用のセキュリティゾーンを選択する か、 Zone [ゾーン] をクリックして新しいゾーンを定義しま す。 None [なし] を選択すると、現在インターフェイスに割 り当てられているゾーンが解除されます。
管理プロファ イル	トンネルイン ターフェイス	Management Profile[管理プロファイル] – このインターフェ イスを介したファイアウォールの管理に使用できるプロトコ

トンネル イン ターフェイス 設定	設定場所	の意味
	> 上級 > その 他の情報	ル (SSH、Telnet、HTTP など) を定義するプロファイルを選 択します。None[なし] を選択すると、現在インターフェイ スに割り当てられているプロファイルが解除されます。
MTU		このインターフェイスで送信するパケットの最大転送単 位(MTU)をバイト数で入力します(576~9,192、デフォ ルトは 1,500)。ファイアウォールの両側のマシンが Path MTU Discovery (PMTUD)を実行し、インターフェイスが MTU を超えるパケットを受信すると、ファイアウォールが 送信元にパケットが大きすぎることを示す ICMP フラグメン ト要求メッセージを返します。

IPv4 アドレスの場合

IP	トンネルイン ターフェイス > IPv4	Add[追加] をクリックし、以下のいずれかの手順を実行し て、インターフェイスのスタティック IP アドレスとネット ワーク マスクを指定します。
		 CIDR (Classless Inter-Domain Routing) 表記法の ip_address/maskの形式(例: 192.168.2.0/24)でエント リを入力します。
		 タイプが IP netmask[IP ネットマスク]の既存のアドレス オブジェクトを選択します。
		 Adress[アドレス] をクリックし、タイプが IP netmask[IP ネットマスク] のアドレスオブジェクトを作成します。
		インターフェイスに対して複数の IP アドレスを入力できま す。IP アドレスの最大数は、システムが使用する転送情報 ベース (FIB) によって決まります。
		IP アドレスを削除するには、アドレスを選択して Delete[[削 除]] をクリックします。

IPv6 アドレスの場合

インター フェースでの IPv6 の有効 化	トンネルイン ターフェイス > IPv6	このインターフェイスの IPv6 アドレスを有効にする場合に 選択します。
インターフェ イス ID	トンネルイン ターフェイス > IPv6	64 ビット拡張一意識別子 (EUI-64) を 16 進数形式で入力し ます (例: 00:26:08:FF:FE:DE:4E:29)。このフィールドを空白 のままにすると、ファイアウォールが、物理インターフェイ スの MAC アドレスから生成された EUI-64 を使用します。

トンネル イン ターフェイス 設定	設定場所	の意味
		アドレスの追加時に Use interface ID as host portion[ホスト 部分にインターフェイス ID を使用] オプションを選択する と、ファイアウォールがそのアドレスのホスト部分にイン ターフェイス ID を使用します。
アドレス		Add[追加] をクリックして、IPv6 アドレスごとに以下のパラ メータを設定します。
	 Address[アドレス] – IPv6 アドレスとプレフィックス長を 入力します (例: 2001:400:f00::1/64)。既存のIPv6アドレ スオブジェクトを選択することや、Address[アドレス] を クリックしてアドレスオブジェクトを作成することもで きます。 	
		 Enable address on interface (インターフェイス上のアドレスを有効にする) – インターフェイスの IPv6 アドレスを有効にする場合に選択します。
		 Use interface ID as host portion(ホスト部分にインターフェイス ID を使用) – IPv6 アドレスのホスト部分に Interface ID(インターフェイス ID)を使用する場合に選択します。
		 Anycast(エニーキャスト) – 最も近いノードを経由する ルーティングを含める場合に選択します。

Network > Interfaces > SD-WAN [ネットワーク > イン ターフェイス > SD-WLAN]

Panorama で自動 VPN 設定を使用している場合、自動 VPN 設定がSD-WAN インターフェース を作成します。この場合、仮想 SD-WAN インターフェースを作成および設定する必要はありま せん。

Panorama で自動 VPN 設定を使用していない場合は、仮想 SD-WAN インターフェースを作成 して、特定のハブあるいはインターネット等の同じ宛先に接続する1つまたは複数の物理 SD-WAN 対応のイーサネットインターフェースメンバーを追加します。

Panorama がマルチ vsys ファイアウォールを管理している場合は、すべての SD-WAN 対応インターフェイスおよび構成を vsys1 で設定する必要があります。

SD-WAN は、マルチ VSYS ファイアウォールの複数の仮想システムにまたがる SD-WAN 構成をサポートしません。

SD-WAN インターフェイス設定

インターフェイ ス名	読み取り専用の Interface Name (インターフェイス名) フィールドに はsdwanが設定されています。仮想 SD-WAN インターフェイスを特定する 数値サフィックス (1 ~ 9,999) を隣のフィールドに入力します。
	Auto VPNは、.901、.902などの番号が付けられたSD-WANインターフェイスを作成します。したがって、SD-WANインターフェイスを手動で作成する場合は、SD-WANインターフェイス名にsdwan.90x形式を使用しないでください。同様に、Auto VPNはIPv6インターフェイス用に.9016という番号のSD-WANインターフェイスを作成するので、SD-WANインターフェイス名にはsdwan.9016を使用しないでください。
コメント	インターネット または 米国西部のハブなど、わかりやすくインターフェ イスの説明を入力することがベストプラクティスです。コメントを使用す ると、ログやレポートで自動生成された名前を解読するよりも、インター フェイスを特定しやすくなります。
Link Tag (リン ク タグ)	SD-WAN リンクにタグを付けます。たとえば、格安ブロードバンドやバッ クアップなど。
PROTOCOL	仮想SD-WANインターフェイスの種類を示すプロトコルを選択します。 • ipv4 は IPv4 DIA 仮想インターフェイスを示します。 • ipv6 は IPv6 DIA 仮想インターフェイスを示します。 • none は VPN トンネル仮想インターフェイスを示します。

Config Tab (設定タブ)

SD-WAN インタ-	ーフェイス設定
仮想ルー ター(VR)	インターフェイスに仮想ルーターを割り当てるか、Virtual Router(仮想ルーター)を選択して新しい仮想ルーターを定義します (「Network(ネットワーク)> Virtual Routers(仮想ルーター)」を参 照)。None[なし] を選択すると、現在インターフェイスに割り当てられて いるルーターが解除されます。
仮想システ ム(vsys)	ファイアウォールが複数の仮想システムをサポートし、その機能が有効に なっている場合は、インターフェイスに vsys1 を選択する必要がありま す。
セキュリティ ゾーン	インターフェース用のセキュリティゾーンを選択するか、 Zone [ゾーン] を 選択して新しいゾーンを定義します。 None [なし] を選択すると、現在イン ターフェイスに割り当てられているゾーンが解除されます。仮想 SD-WAN インターフェースおよび仮想 SD-WAN のすべてのインターフェースメン バーは、同じセキュリティゾーン内にある必要があります。このため、ブ ランチから同じ宛先へのすべてのパスに同じセキュリティポリシー ルール が適用されます。

Advanced Tab (詳細タブ)

インターフェイ	この仮想 SD-WAN インターフェイスを構成する レイヤー3 イーサネット
ス	インターフェイス (Direct Internet Access [DIA] 用) または仮想 VPN トンネ
	ル インターフェイス (ハブ用) を選択します。ファイアウォールの仮想 ルー
	ターは、この仮想 SD-WAN インターフェイスを使用して、SD-WAN トラ
	フィックを DIA あるいはハブの場所にルーティングします。インターフェ
	イスには異なるタグを付けることができます。複数のインターフェースを
	入力する場合は、すべて同じタイプ (VPN トンネルまたは DIA) を選択しま
	す。

ネットワーク>インターフェイス>PoE

サポートされているインターフェイスで Power over Ethernet(PoE)を設定して、firewall から接続された受電デバイス(PD)に電力を転送できます。この画面には、すべてのインターフェイスの PoE 設定の概要と、PoE 設定で定義された電力バジェット、割り当て、および使用方法が表示されます。

次の表に、Interfaces PoE の詳細 テーブルの各列の概要を示します。

列	詳説
インターフェイス	インターフェイス名とそれに対応する物理ポート。
PoE対応	インターフェイスで PoE が有効になっている場合は、Yes を示しま す。
Operational Status(運用ステー タス)	インターフェイス上の PoE の現在のステータスを表示します。Legend 表を参照して、この列の値を確認してください。
接続確認	firewallと受電デバイスの間に接続が存在する場合に表示されます。
クラス	電源出力、電源タイプ、および IEEE 規格に基づく PoE クラス情報を 表示します。
割り当て電力(W)	インターフェイスによって割り当てられた Watts 単位の電力量。
使用電力(W)	インターフェイスによって現在使用されている Watts の電力量。
消費電力(W)	インターフェイスによって消費された Watts 単位の電力量。
RSVD電力/最大電 力(W)	インターフェイスによって予約された電力量が、Watts の最大電力ポ テンシャルに対して保持される電力量。
Fault	特定のポートで PoE 接続でエラーが発生した場合に詳細を表示します。
ブラックリストの理 由	ブラックリストに登録されているポートの詳細を表示します。None は、ポートがブラックリストに登録されていないことを示します。

上記の Interfaces PoE 詳細 テーブルの特定の列では、省略された用語を使用して、ステータ ス、エラー、またはその他の状況を伝えます。次の Legend の表では、各省略された用語につい て説明します。

略語	用語
割り当て	割り当て済み
4月	Approved(承認済み)
設定	設定
接続チェック	接続確認
Covc	クラス過電流
Den	電源拒否
Dis	無効化
ディスク	切断
DS	二重シグネチャ
Ena	有効化
Flt	Fault
NOFLT	Faultなし
Opr	稼働中
Pcut	停電
Prgto	パワーグッドタイムアウト
Pwr	出力
Rsvd	予約済み
ショート	短絡
シャット	シャットダウン
Sig	シグナルペア
ソフト	software
Sp	スペアペア
SS	単一シグネチャ

略語	用語
TooHigh	静電容量が予想よりも高い
TooLow	PD抵抗が低すぎます
Tstart	最大許容値を超える突入電流
UN	未知
水	ワット

Network > Interfaces > Cellular (ネットワーク>インター フェイス>セルラー)

[追加]をクリックし、次のフィールドを使用してセルラーインターフェイスを設定します。

セルラーイン ターフェイス の設定	設定場所	の意味
スロット	セルラーイン ターフェース	インターフェイスに使用する Slot (スロット) を選択します。 • シャーシベースのシステムを使用しない場合は、スロッ ト 1 を使用します。
インターフェ イス名		使用するインターフェイス名を選択します。
コメント		オプションで、インターフェイスに関するコメントを入力し ます。
Netflowプロ ファイル		入力インターフェイスを通過する単向性の IP トラフィッ クを NetFlow サーバーにエクスポートする場合は、サー バー プロファイルを選択するか、Netflow Profile (Netflow プロファイル)をクリックして新しいプロファイルを定 義します (「Device (デバイス) > Server Profiles (サー バー プロファイル) > NetFlow」を参照)。None[なし] を選択すると、現在インターフェイスに割り当てられてい るNetFlowサーバーが解除されます。
仮想ルー ター(VR)	セルラーイン ターフェース > コンフィグ	インターフェイスに仮想ルーターを割り当てるか、New Virtual Router (新しい仮想ルーター)をクリックして新 しい仮想ルーターを定義します(「Network (ネットワー ク) > Virtual Routers (仮想ルーター)」を参照)。None[な し]を選択すると、現在インターフェイスに割り当てられて いるルーターが解除されます。
論理ルーター		インターフェイスに論理ルータを割り当てるか、 [New Logical Router (新しい論理ルーター)] をクリックして新 しい論理ルータを定義します (Network (ネットワーク) > Routing (ルーティング) > Logical Routers (論理ルー ター)を参照)。 None を選択して、現在の論理ルーターの 割り当てをインターフェイスから削除します。
セキュリティ ゾーン		インターフェイス用のセキュリティゾーンを選択する か、[New Zone (新しいゾーン)] をクリックして新しいゾー

セルラーイン ターフェイス の設定	設定場所	の意味
		ンを定義します。None[なし] を選択すると、現在インター フェイスに割り当てられているゾーンが解除されます。
ラジオ	-	Radio (ラジオ)の設定を選択します。
		 Off-(デフォルト値)無線設定とセルラー インターフェイ スを無効にします。
		 On-無線設定とセルラー インターフェイスを有効にします。
		このオプションを使用すると、トラブルシューティング中に 無線設定をリセットできます。
GPS		GPS 設定を選択します。
		GPSオプションを有効にするには、GPSオプションと同様に[ラジオ]オプションでも[オン]を選択する必要があります。
		 Off-(デフォルト値)GPS 設定を無効にします。 On-GPS設定を有効にします。
プライマリ SIM スロット	-	インターフェイスに使用するファイアウォールまた はPanorama SIMカードが格納されているプライマリSIMス ロットを選択します。
ネットワーク 提供のデフォ ルト ゲート ウェイを指す デフォルト ルートを自動 的に作成	セルラーイン ターフェース > IPv4	ネットワークが提供するデフォルトゲートウェイを指すデ フォルトルートをファイアウォールまたはPanoramaで自動 的に作成するかを選択します。このオプションはデフォル トで有効になっており、ネットワークが提供するデフォルト ゲートウェイへのデフォルトルートを作成します。
デフォルト ルート メト リック		デフォルト ルート メトリックを指定して、ルートのメト リックを定義します。ルーティング プロトコルで同一の宛先 ネットワークへの複数のルートが存在する場合、メトリック 値が最も小さいルートが優先されます。デフォルトは 10 で す。指定できる範囲は1 ~ 65535です。
リンク ス テート	セルラーイン ターフェース > 上級	インターフェイスの リンク状態 を選択します。 • auto (自動)–インターフェイスはピア接続がある場合にだ け使用できます。

セルラーイン ターフェイス の設定	設定場所	の意味
		 up-インターフェイスを使用できます。 down-インターフェイスは使用できません。
スロット	セルラーイン ターフェース > 上級 > ス ロット	スロットを選択します。同時にアクティブにできるSIMス ロットは1つのみです。デフォルトでは、SIM1がア クティブなSIMスロットです。ファイアウォールまた はPanoramaが5分以内にセッションを確立できない場合、代 替SIMスロットでセッションを確立しようとします。
固定		SIMスロットの不正使用を防ぐためにPINを要求するには、 スロットのPINを入力します。
ピンの確認	-	スロットのピンの確認にもう一度PINを入力します。
APN プロ ファイル		SIMカードがデフォルトで使用するAPNプロファイルを 指定します。カスタムAPNプロファイルで上書きしない 限り、SIMスロットはこのAPNプロファイルを使用しま す。APNプロファイルを指定しない場合、ファイアウォール またはPanoramaはデフォルトの自動APNプロファイルを使 用します。カスタムAPNプロファイルを指定する必要がある 場合は、[Cellular Interface (セルラーインターフェース)] > [Advanced (詳細)] > [APN Profile (APNプロファイル)]を選択 して指定できます。
APN プロ ファイル	セルラーインターフェース	デフォルトの APN プロファイルを追加します。
認証タイプ	> 上級 > APN プロファイル	認証タイプを選択してください。
		 None-(デフォルト)ファイアウォールまた はPanoramaは、APN への接続に認証を必要としません。
		 CHAP-Challenge Handshake Authentication Protocol (CHAP)を使用して APN に接続します。
		 PAP-パスワード認証プロトコル(PAP)を使用してAPNに接続する
		 auto-ファイアウォールまたはPanoramaがサービスプ ロバイダーに基づいて認証タイプを自動的に検出できる ようにする。初期認証タイプへの接続に失敗した場合、 ファイアウォールまたはPanoramaは代替認証タイプで接 続を試みます。
APN		APN を入力します。

セルラーイン ターフェイス の設定	設定場所	の意味
username		アカウントのユーザー名を入力します。
パスワード	-	アカウントのパスワードを入力します。
パスワードの 確認		アカウントの Confirm Password (パスワードの確認) にもう 一度パスワードを入力します。
管理プロファ イル	セルラーイン ターフェース > 上級 > その 他の情報	インターフェイスに使用する管理プロファイルを選択しま す(Network > Network Profiles > Interface Mgmt [ネットワー ク > ネットワーク プロファイル > インターフェイス管理]を 参照)。
MTU		最大転送単位(MTU)値を指定します。デフォルト値 は1428バイトです。範囲は576~1500バイトです。
TCP MSS の 調整		遅延の問題が発生した場合にパケットサイズを調整するに は、TCP MSS を調整して最大セグメントサイズを設定しま す。
IPv4 MSS 調 整	-	IPv4 MSS 調整値を指定します。デフォルトは40です。指定 できる範囲は40 ~ 300です。

ネットワーク>インターフェイス>フェイルオープン

特定のファイアウォールモデルには、電源またはオペレーティングシステムの障害が発生した場合にパススルー接続を提供するように構成できるフェールオープンポートがあります。この機能はデフォルトでは無効になっているため、 有効化するには[Enable Fail Open (フェールオープンを有効にする)]を選択する必要があります。

次のファイアウォールは次のフェールオープンをサポートしています。

Firewall Model(ファイアウォール モデル)	フェールオープンポート
PA-450R	ポート3および4

Network > Zones [ネットワーク > ゾーン]

以下のトピックでは、ネットワークのセキュリティ ゾーンについて説明します。

確認すべき情報	以下を参照
セキュリティーゾー ンの目的とは?	セキュリティ ゾーンの概要
セキュリティ ゾーン の設定で使用できる フィールドは?	セキュリティ ゾーンの構成要素
その他の情報をお探 しですか?	インターフェイスやゾーンを用いたネットワークのセグメント化

セキュリティ ゾーンの概要

ファイアウォールの物理インターフェイスと仮想インターフェイスをグループ化し、ネットワークの特定のインターフェイスを通過するトラフィックを制御し、ログに記録するためセキュリティゾーンを利用します。ファイアウォールのインターフェースでトラフィックの処理を行う場合は、インターフェースをいずれかのセキュリティゾーンに割り当てる必要があります。ゾーンには同じタイプの複数のインターフェイスを割り当てることができますが(タップ、レイヤー2、またはレイヤー3インターフェイスなど)、各インターフェイスは1つのゾーンにしか属せません。

ファイアウォールのポリシールールは、セキュリティーゾーンを使用してトラフィックの送信 元と宛先を識別します。トラフィックはゾーン内を自由に流れますが、異なるゾーン間におい て許可するセキュリティ ポリシー ルールが定義されない限り流れません。インターゾーントラ フィックを許可または拒否するには、セキュリティ ポリシー ルールで送信元ゾーンと宛先ゾー ン (インターフェイスではない)を参照する必要があります。また、それらのゾーンは同じタ イプでなければなりません。たとえば、ある レイヤー 2の ゾーンからのトラフィックのうちセ キュリティ ポリシー ルールが許可または拒否できるのは、別のレイヤー 2の ゾーンに向かうも ののみです。

セキュリティゾーンの構成要素

セキュリティ ゾーンを定義するには、Add(追加)をクリックし、以下の情報を指定します。

セキュリティ ゾーン設 定	の意味
氏名	ゾーン名(最大31文字)を入力します。この名前は、セキュリティ ポリシーの定義時とインターフェイスの設定時にゾーンのリストに 表示されます。名前の大文字と小文字は区別されます。また、仮

セキュリティ ゾーン設 定	の意味
	想ルーター内で一意の名前にする必要があります。文字、数字、ス ペース、ハイフン、ピリオド、およびアンダースコアのみを使用し てください。
場所	このフィールドは、ファイアウォールが複数の仮想システム (vsys) をサポートし、その機能が有効な場合にのみ表示されます。この ゾーンが適用されているvsysを選択してください。
タイプ	 ゾーンタイプ(Tap (タップ)、Virtual Wire (バーチャ ルワイヤー)、Layer2 (レイヤー2)、Layer3 (レイヤー 3)、External (外部)、または Tunnel (トンネル))を選択し、 ゾーンに割り当てられていないそのタイプの Interfaces (インター フェイス)をすべて表示します。Layer 2 [レイヤー2] およびLayer 3 [レイヤー3] ゾーンタイプでは、該当タイプの イーサネットイン ターフェイスとサブインターフェイスがすべて表示されます。ゾーンに割り当てたいインターフェイスをAdd[追加]します。 1つのファイアウォール上の、複数の仮想システム間のトラフィッ クをコントロールする場合に外部ゾーンを使用します。複数の仮想 システムをサポートするファイアウォールで、Multi Virtual System Capability[マルチ仮想システム機能] が有効化されている場合のみ 表示されます。外部ゾーンの詳細は、「ファイアウォール内に残る VSYS 間トラフィック」を参照してください。 インターフェイスは、1つの仮想システムの1つのゾーンにのみ属す
インターフェイス	このゾーンに1つ以上のインターフェイスを追加します。
ゾーン プロテクション プロファイル	このゾーンからの攻撃にファイアウォールが対応する方法を指 定したプロファイルを選択します。新しいプロファイルを作成 する手順については、「Network(ネットワーク) > Network Profiles(ネットワーク プロファイル) > Zone Protection(ゾーン プロテクション)」を参照してください。各ゾーンをゾーン プロテ クション プロファイルで保護することがベストプラクティスになり ます。
パケット バッファ保護 の有効化	パケット バッファ保護(Device (デバイス) > Setup (セットアップ) > Session (セッション)) をグローバルに設定し、各ゾーンに適用し ます。ファイアウォールは入力ゾーンのみにパケット バッファ保護 を適用します。バッファ使用率基準のパケット バッファ保護は、 デフォルトで有効化されています。あるいは、レイテンシに基づ き、Packet Buffer Protection (パケット バッファ保護) を設定する 方法もあります。各ゾーンでパケット バッファ保護を有効化して

セキュリティ ゾーン設 定	の意味
	ファイアウォールのバッファを保護することがベストプラクティス です。
ネット検査の有効化	ゾーン保護プロファイルに関連付けられたセキュリティゾーンのカ スタムルールを使用して、L3&L4ヘッダー検査の有効化を容易にし ます。L3 および L4 ヘッダー インスペクションのグローバル設定 は、firewall (デバイス > セットアップ > セッション) でも有効にす る必要があります。
ログ設定	 ゾーンプロテクションログを外部システムに転送するためのLog Forwarding(ログ転送)プロファイルを選択します。 デフォルトと指定されたログ転送プロファイルがある場合は、新しいセキュリティゾーンを定義するときに、そのプロファイルがこのドロップダウンリストで自動的に選択されます。新しいセキュリティゾーンを設定するときに別のLog Forwarding(ログ転送)の 選択を続行すると、このデフォルト設定をいつでもオーバーライドできます。新しいログ転送プロファイルを定義または追加する(およびプロファイルをデフォルトに指定してこのドロップダウンリストで自動選択されるようにする)には、New(新規)をクリックします(「Objects(オブジェクト) > Log Forwarding(ログ転送)」を参照)。 Panorama テンプレートのゾーンを設定している場合
	は、Log Setting(ログ設定)ドロップダウンリストに 一覧表示されるのは共有されたログ転送プロファイル のみです。共有されていないプロファイルを指定する には、名前を入力する必要があります。
User-IDの有効化	IP アドレスからユーザー名へのマッピング(検出)を行うように User-ID [™] を設定した場合は、Enable User Identification (ユーザー ID を有効化)してマッピング情報をこのゾーンのトラフィックに適 用することがベストプラクティスになります。このオプションを無 効にした場合、ゾーン内のトラフィックのユーザーマッピング情報 がファイアウォール ログ、レポート、およびポリシーから除外され ます。
	デフォルト設定では、このオプションを選択した場合、ファイア ウォールは、ゾーンのすべてのサブネットワークのトラフィック にユーザーマッピング情報を適用します。情報の適用先をゾーン内 の特定のサブネットワークに制限するには、Include List[許可リス ト]とExclude List[除外リスト]を使用します。

セキュリティ ゾーン設 定	の意味
	 User-ID は信頼されたゾーンでのみ有効にしてください。外部の信頼されていないゾーン(インターネットなど)で User-ID およびクライアントによるプローブを有効にすると、保護されたネットワークの外にプローブが送信される可能性があります。これにより、User-ID エージェントのサービスアカウント名、ドメイン名、暗号化されたパスワード ハッシュの情報が漏洩し、保護されているリソースに攻撃者が不正アクセスできるようになる場合があります。 User-IDがゾーンに対して検出を実行するのは、User-IDがモニターするネットワーク範囲内にゾーンが含まれる場合に限られます。ゾーンがこの範囲に含まれていない場合、たとえ Enable User Identification[ユーザーIDの有効化]を選択しても、ファイアウォールはユーザーマッピング情報をゾーンのトラフィックに適用しません。詳細は「ユーザーマッピングのサ
	ブネットワークの許可または除外」を参照してくださ い。
User-ID ACL 許可リス ト	デフォルトでは、このリストでサブネットワークを指定しない場 合、ファイアウォールは、ログ、レポート、およびポリシーで使用 するために、検出したユーザーマッピング情報をゾーンのすべての トラフィックに適用します。
	ユーザー マッピング情報の適用先をゾーン内の特定のサブネッ トワークに制限するには、サブネットワークごとに Add[追加] をクリックし、アドレス (またはアドレス グループ) オブジェク トを選択するか、IP アドレス範囲 (10.1.1.1/24 など) を入力しま す。Include List (許可リスト) はホワイト リストであり、他のす べてのサブネット ワークの除外は暗黙的に実行されます。Exclude List (除外リスト) に追加する必要はありません。
	Exclude List[除外リスト]にエントリを追加するのは、Include List[許可リスト]の一部のサブネットワークのユーザーマッピ ング情報を除外する場合のみです。たとえば、Include List[許 可リスト]に 10.0.0.0/8 を追加し、Exclude List[除外リスト]に 10.2.50.0/22 を追加した場合、ファイアウォールは、10.2.50.0/22 を除く、10.0.0.0/8 のずべてのゾーンサブネットワークのユーザー マッピング情報を許可し、10.0.0.0/8 の外部のすべてのゾーンサブ ネットワークの情報を除外します。

セキュリティ ゾーン設 定	の意味
	 User-ID がモニターするネットワーク範囲に含まれ るサブネットワークのみを許可できます。詳細は、 「ユーザーマッピングのサブネットワークの許可ま たは除外」を参照してください。
User-ID ACL 除外リス ト	Include List(許可リスト)の一部のサブネットワークのユーザー マッピング情報を除外するには、アドレス(またはアドレスグルー プ)オブジェクトを Add(追加)するか、除外するサブネットワー クごとに IP アドレス範囲を入力します。
	 Exclude List[除外リスト]にエントリを追加したが、Include List[許可リスト]にはエントリを追加しない場合、ファイアウォールは、追加したサブネットワークだけではなく、ゾーン内のすべてのサブネットワークのユーザーマッピング情報を除外します。
NAT 導入前の識別	[Pre-NAT Identification (NAT 導入前の識別)] エリアのフィール ドは、e将来のリリース用に予約されています。e

Network > VLANs [ネットワーク > VLAN]

このファイアウォールでは、IEEE 802.1Q 標準に準拠する VLAN がサポートされています。ファ イアウォールに定義されたレイヤー 2 インターフェイスをそれぞれ VLAN に関連付けることが できます。同じ VLAN を複数のレイヤー 2 インターフェイスに割り当てることができますが、 各インターフェイスは 1 つの VLAN にのみ属することができます。

VLAN 設定	の意味
氏名	VLAN 名(最大 31 文字)を入力します。この名前は、インター フェイスを設定するときに VLAN のリストに表示されます。名前の 大文字と小文字は区別されます。また、一意の名前にする必要があ ります。文字、数字、スペース、ハイフン、およびアンダースコア のみを使用してください。
VLAN インターフェイ ス	トラフィックを VLAN の外部にルーティングできるようにするに は、Network(ネットワーク) > Interfaces(インターフェイス) > VLAN を選択します。
インターフェイス	VLAN のファイアウォール インターフェイスを指定します。
スタティック MAC 設 定	MAC アドレスが到達するために経由する必要のあるインターフェ イスを指定します。これは、学習したインターフェイス対 MAC の マッピングよりも優先されます。

Network > Virtual Wires [ネットワーク > バーチャルワ イヤー]

ファイアウォールで2つのバーチャルワイヤーインターフェイスを指定(Network(ネットワーク) > Interfaces(インターフェイス)した後にバーチャルワイヤーを定義するには、Network(ネットワーク) > Virtual Wires(バーチャルワイヤー)を選択します。

バーチャル ワイヤー設 定	の意味
バーチャル ワイヤー名	バーチャル ワイヤー名 (最大 31 文字) を入力します。この名前は、 インターフェイスを設定するときにバーチャル ワイヤーのリストに 表示されます。名前の大文字と小文字は区別されます。また、一意 の名前にする必要があります。文字、数字、スペース、ハイフン、 およびアンダースコアのみを使用してください。
インターフェイス	表示されたリストから、バーチャル ワイヤー設定用の イーサネットインターフェイスを 2 つ選択します。リストには、バーチャル ワイヤー インターフェイス タイプで、他のバーチャル ワイヤーに 割り当てられていないインターフェイスのみが表示されます。 バーチャル ワイヤー インターフェイスの詳細は、「バーチャル ワ イヤー インターフェイス」を参照してください。
タグを許可	 バーチャルワイヤーで許可されるトラフィックのタグ番号 (0~4094)またはタグ番号の範囲(タグ1~タグ2)を入力します。タグ値0(デフォルト)は、タグのないトラフィックを示します。複数のタグまたはタグ範囲はコンマで区切ります。除外されたタグ値を持つトラフィックは廃棄されます。 受信パケットまたは送信パケット上でタグ値が変更されます。
	パることはありません。 バーチャル ワイヤー サブインターフェイスを使用する場合に Tag Allowed[タグを許可] リストを指定すると、リスト内のタグを持 つすべてのトラフィックが親バーチャル ワイヤーに分類されま す。バーチャル ワイヤー サブインターフェイスでは、親の Tag Allowed[タグを許可] リストに存在しないタグを使用する必要があ ります。
マルチキャスト ファイ アウォール設定	セキュリティ ルールをマルチキャスト トラフィックに適用できる ようにする場合に選択します。この設定が有効になっていないと、 マルチキャスト トラフィックがバーチャル ワイヤー全体に転送さ れます。

ネットワーク

バーチャル ワイヤー設 定	の意味
リンク状態パス スルー	リンクのダウン状態が検出されたときにバーチャル ワイヤー ペア のもう一方のインターフェイスをダウンさせる場合に選択します。 このオプションを無効化した場合あるいは選択しない場合、接続状 況はバーチャルワイヤーを通じて反映されません。

Network > Virtual Routers [ネットワーク > 仮想ルー ター]

手動で定義したスタティックルートを使用するか、あるいはレイヤー3のルーティングプロトコ ルに参加することで他のサブネットへのルートを取得する場合は、ファイアウォールに仮想ルー ターを設定しておく必要があります。ファイアウォールに定義されたレイヤー3インターフェ イス、ループバックインターフェイス、および VLAN インターフェイスはそれぞれ、仮想ルー ターに関連付けられている必要があります。各インターフェイスは、1つの仮想ルーターにのみ 属することができます。

仮想ルーターを定義するには、一般的な設定のほかに、ネットワークで必要とされるスタティックルートまたはダイナミックルーティングプロトコルの組み合わせが必要になります。また、ルート再配信やECMPなど、その他の機能を設定することも可能です。

確認すべき情報	以下を参照
仮想ルーターに必要な要素	仮想ルーターの一般設定
設定:	静的ルート
	ルート再配信
	RIP
	OSPF
	OSPFv3IPv6
	BGP
	IP マルチキャスト
	ECMP
仮想ルーターに関する情報を 表示する。	仮想ルーターの詳細ランタイム状態
その他の情報をお探しです か?	ネットワーク

仮想ルーターの一般設定

 Network > Virtual Routers > Router Settings > General [ネットワーク > 仮想ルーター > ルー ター設定 > 全般]

すべての仮想ルーターでは、以下の表に従ってレイヤー3インターフェイスと管理距離のメト リックを割り当てる必要があります。

仮想ルーターの一般設 定	の意味
氏名	仮想ルータを表す名前を指定します (最大 31 文字)。名前の大文字 と小文字は区別されます。また、一意の名前にする必要がありま す。文字、数字、スペース、ハイフン、およびアンダースコアのみ を使用してください。
インターフェイス	仮想ルーターに含めるインターフェイスを選択します。これにより、仮想ルーターのルーティング テーブルでの発信インターフェイ スとして使用することもできます。
	インターフェイス タイプを指定する方法については 「Network(ネットワーク) > Interfaces(インターフェイス)」 を参照してください。
	インターフェイスを追加すると、その接続済みルートが自動的に追 加されます。
管理上の距離	以下の管理距離を指定します。
	• Static routes[スタティックルート] - 範囲は10 ~ 240、デフォル トは10です。
	 OSPF Int[OSPF内部] – 範囲は10 ~ 240、デフォルトは30です。
	 OSPF Ext[OSPF外部] – 範囲は10 ~ 240、デフォルトは110です。
	• IBGP - 範囲は10~240、デフォルトは200です。
	• EBGP - 範囲は10 ~ 240、デフォルトは20です。
	• RIP - 範囲は10~240、デフォルトは120です。

静的ルート

Network > Virtual Routers > Static Routes [ネットワーク > 仮想ルーター > スタティック ルート]

任意で1つ以上のスタティックルートを入力します。Pv4 または IPv6 アドレスを使用してルート を指定する場合は、IPまたはIPv6 タブをクリックします。通常、ここでデフォルト ルートを設 定 (0.0.0.0/0) するために必要になります。デフォルト ルートは、他の方法ではバーチャル ルー タのルーティング テーブルに見つからない宛先に適用されます。

スタティック ルートの 設定	の意味
名前	スタティック・ルートを識別する名前を入力します (最大 63 文 字)。名前の大文字と小文字は区別されます。また、一意の名前にす

スタティック ルートの 設定	の意味
	る必要があります。文字、数字、スペース、ハイフン、およびアン ダースコアのみを使用してください。
宛先	CIDR (Classless Inter-Domain Routing) 表記法でIPアドレスとネットワークマスクを入力します。 <i>ip_address/mask</i> (たとえば、IPv4の場合は 192.168.2.0/24、IPv4 の場合は 2001:db8::/32)。あるいは、タイプが IP ネットマスクのアドレス オブジェクトを作成できます。
インターフェイス	パケットを宛先に転送するインターフェイスを選択するか、ネクス トホップ設定を指定するか、その両方を行います。
ネクストホップ	以下のいずれかを選択します。
	 IP Address (IP アドレス)-ネクストホップ ルーターの IP アドレスを入力する、あるいは IP ネットマスク型のアドレスオブジェクトを選択または作成する場合に選択します。IPv4 の場合は/32、IPv6 の場合は /128 のネットマスクがアドレスオブジェクトに求められます。
	 アァイアウォールで仮想ルータのスタティック ルートを設定しているときに、ネクストホップ ルータのIPアドレスを入力できます。Palo Alto Networksファイアウォールは、ネクストホッ プIPアドレスをアドレスオブジェクトとして扱い ます。したがって、ネクストホップIPアドレス ([Network (ネットワーク)] > [Virtual Router (仮想 ルーター)] > [Static Routes (静的ルート)])の値を、 設定されているアドレスオブジェクト名 ([Objects (オブジェクト)] > [Addresses (アドレス)]) と同じに 設定すると、アドレスオブジェクトへの変更はネ クストホップIPアドレスの値にも反映されます。 つまり、アドレスオブジェクト([Objects (オブジェ クト)] > [Addresses (アドレス)])の名前を変更する と、ネクストホップIPアドレスも変更されます。
	 Next VR[次のVR] – ファイアウォールの仮想ルータをネクストホップとして選択します。これにより、1つのファイアウォール内の仮想ルーター間で内部的にルーティングできます。
	 FQDN-ネクストホップを FQDN で識別する場合に選択します。その後、FQDN 型のアドレスオブジェクトを選択するか、FQDN 型のアドレスオブジェクトを新規作成します。
	 Discard[破棄] – この宛先のトラフィックを廃棄する場合に選択 します。

スタティック ルートの 設定	の意味
	 None[なし] – ルートのネクスト ホップが存在しない場合に指定 します。
管理距離	スタティック ルートのアドミニストレーティブ ディスタンス(10 ~ 240、デフォルトは 10)を指定します。
メトリック	スタティック ルートの有効なメトリック(1 ~ 65535)を指定しま す。
ルート テーブル	どのルート テーブルにファイアウォールがスタティック ルートを インストールするか選択します。
	 Unicast (ユニキャスト) – ユニキャスト ルート テーブルに ルートをインストールします。
	 Multicast (マルチキャスト) – マルチキャスト ルート テーブ ルにルートをインストールします。
	 Both(両方) – ユニキャストとマルチキャストのルート テーブ ルにルートをインストールします。
	 No Install (インストールしない) – ルート テーブル (RIB) にルートをインストールしません。ルートが削除されるまで、 ファイアウォールは参考のためにスタティック ルートを維持し ます。
BFDプロファイル	PA-400 シリーズ、PA-3200 シリーズ、PA-3400 シリー ズ、PA-5200 シリーズ、PA-5400 シリーズ、PA-7000 シリーズ、 または VM シリーズ ファイアウォールのスタティック ルートに対 して双方向フォワーディング検出(BFD)を有効にするには、次のい ずれかを選択します。
	• default (デフォルトのBFD設定)
	 ファイアウォール上で作成したBFDプロファイルです。
	 新しいBFDプロファイルを作成する場合はNew BFD Profile[新しいBFDプロファイル]
	スタティックルートでBFDを無効化する場合はNone (Disable BFD)[なし(BFD無効)] を選択します。
	スタティックルートでBFDを使用する場合:
	 スタティックルートの両端にあるファイアウォールとピアの両 方でBFDセッションがサポートされている必要があります。
	 スタティックルートのNext Hop[ネクストホップ]のタイプはIP Address[IPアドレス]に設定し、有効なIPアドレスを入力する必 要があります。
スタティック ルートの 設定	の意味
---------------------------	--
	 Interface[インターフェイス]の設定をNone[なし]にすることはできません。DHCPアドレスを使用している場合でも、インターフェイスを選択する必要があります。
パス モニタリング	スタティック ルートでパス モニタリングを有効化する場合に選択 します。
障害条件	firewall が監視対象パスをダウンし、スタティック ルートをダウン と見なす条件を選択します:
	 Any –スタティック ルートの監視対象の宛先のいずれかが ICMP によって到達不能である場合、firewall はスタティック ルートを RIB および FIB から削除し、同じ宛先に向かう次に低いメトリッ クを持つダイナミック ルートまたはスタティック ルートを FIB に追加します。
	 All – スタティック ルートのすべての監視対象宛先が ICMP に よって到達できない場合、firewall はスタティック ルートを RIB および FIB から削除し、同じ宛先に向かうメトリックが次に低 いダイナミック ルートまたはスタティック ルートを FIB に追加 します。
	All を選択して、監視対象の宛先がメンテナンスのために単にオフ ラインになっている場合に、単一の監視対象宛先がスタティック ルート障害を通知する可能性を回避します。
プリエンプティブ ホー ルド タイム (分)	ダウンしたパス モニターが Up (アップ)状態を維持しなければ ならない分数を入力します。パス モニターがメンバーである監視 対象宛先すべてを評価し、Up (アップ)を維持すると、ファイア ウォールはスタティック ルートを RIB に再インストールします。 リンクがダウンしたりフラッピングしたりせずにタイマーの期間が 過ぎた場合、リンクは安定していると見なされて、パス モニター は Up (アップ)を維持できます。また、ファイアウォールはスタ ティック ルートを RIB に再度追加できます。
	ホールド タイム中にリンクのダウンやフラッピングが発生した 場合、パス モニターはエラーとなります。タイマーはダウンし たモニターが Up (アップ)状態に戻ったときに再度開始しま す。Preemptive Hold Time (プリエンプティブ ホールド タイ ム)が0の場合、パス モニターがアップになると即座にファイア ウォールがスタティック ルートを RIB に再インストールします。 範囲は 1 ~ 1,440、デフォルトは 2 です。
氏名	監視対象宛先の識別に使用する名前を入力します(最大 31 文 字)。

スタティック ルートの 設定	の意味
Enable [有効化]	スタティック ルートのこの特定の宛先のパス モニタリングを有効 化する場合に選択します。ファイアウォールは ICMP Ping をこの宛 先に送信します。
送信元IP	 監視対象宛先に対する ICMP Ping で送信元としてファイアウォール が使用する IP アドレスを選択します。 インターフェイスに複数の IP アドレスがある場合は、1つ選択 します。 インターフェイスを選択した場合、ファイアウォールはデフォ ルトでインターフェイスに割り当てられている最初の IP アドレ スを使用します。 DHCP (Use DHCP Client address) (DHCP (DHCP クライアン トレス アドレスの使用))を選択した場合、ファイアウォール は DHCP がインターフェイスに割り当てたアドレスを使用し ます。DHCP アドレスを確認するには、Network (ネットワー
	ク) > Interfaces (インターフェイス) > Ethernet (イーサネット)を選択して、イーサネット インターフェイスの行にある Dynamic DHCP Client (動的 DHCP クライアント)をクリック します。Dynamic IP Interface Status (動的 IP インターフェイス 状態) ウィンドウに IP アドレスが表示されます。
宛先IP	ファイアウォールがパスを監視する対象の、堅牢で安定した IP ア ドレスまたはアドレス オブジェクトを入力します。監視対象宛 先と、スタティック ルートの宛先は、同じアドレス ファミリー (IPv4 または IPv6)を使用してください。
Ping Interval (sec)(Ping 間隔 (秒))	ファイアウォールがパスを監視する頻度を定める ICMP Ping 間隔を 秒数で指定します(監視対象宛先に Ping を送信する頻度。範囲は 1 ~ 60、デフォルトは 3)。
Ping 数	監視対象宛先から ICMP Ping パケットが返ってこない場合に、リ ンクがダウンしているとファイアウォールが見なすまでの、ICMP Ping パケットの連続数を指定します。Any(任意)または All(す べて)のエラー条件に基づき、パスモニタリングがエラー状態にな ると、ファイアウォールはスタティック ルートを RIB から削除し ます(範囲は 3 ~ 10、デフォルトは 5)。
	たとえば、Ping 間隔が 3 秒で、Ping 数 5 個において Ping が存在 しない(直近 15 秒間の間、ファイアウォールは Ping を受信し ていない)場合、パス モニタリングはリンク エラーを検出しま す。パス モニタリングがエラー状態で、ファイアウォールが 15 秒の後に Ping を受信した場合、リンクの状態はアップと見なさ れます。Any(任意)または All(すべて)のエラー条件に基づ

スタティック ルートの 設定	の意味
	き、Any(任意)または All(すべて)の監視対象宛先に対するパス モニタリングの状態はアップと見なすことができます。また、プリ エンプティブ ホールド タイムが開始されます。

ルート再配信

 Network > Virtual Router > Redistribution Profiles [ネットワーク > 仮想ルーター > 再配信プロ ファイル]

再配信プロファイルは、目的のネットワーク動作に応じて、ファイアウォールにおけるフィルタ リング、優先順位の設定、アクションの実行を管理します。ルート再配信を使用すると、スタ ティック ルートと他のプロトコルで取得されたルートを、指定したルーティング プロトコル経 由で通知できます。

再配信プロファイルを有効にするには、ルーティングプロトコルに適用する必要があります。 再配信ルールがないと、各プロトコルば別個に実行され、それぞれの範囲外では通信しません。 再配信プロファイルは、すべてのルーティングプロトコルが設定され、その結果のネットワー クトポロジが確立した後に追加または変更できます。

再配信プロファイルを RIP および OSPF プロトコルに適用するには、エクスポート ルールを定 義します。Redistribution Rules[ルールの再配信] タブで再配信プロファイルを BGP に適用しま す。以下の表を参照してください。

再配信プロファイル設 定	の意味
氏名	再配信プロファイルを Add(追加)して、プロファイル名を入力し ます。
優先順位	このプロファイルの優先度 (範囲は1~255) を入力します。プロ ファイルは順番に照合されます (優先度の昇順)。
再配信	このウィンドウの設定に基づいてルート再配信を実行するかどうか を選択します。
	 Redist[再配信あり] – 一致した候補ルートを再配信するには、 オンにします。このオプションをオンにした場合、新しいメト リック値を入力します。メトリック値が小さいほど適切なルー トになります。
	• No Redist[再配信なし] – 一致した候補ルートを再配信しない場合、オンにします。

General Filter [一般的なフィルタ] タブ

再配信プロファイル設 定	の意味	
タイプ	候補ルートのルートタイプを指定します。	-
インターフェイス	候補ルートの転送インターフェイスを指定するためのインターフェ イスを選択します。	-
宛先	候補ルートの宛先を指定するには、宛先 IP アドレスまたはサ ブネット (形式は x.x.x または x.x.x.r/n) を入力して Add[追 加] をクリックします。エントリを削除する場合は、削除 (^{C)} をクリックします。)
ネクストホップ	候補ルートのゲートウェイを指定するには、ネクス トホップを示す IP アドレスまたはサブネット (形式 は x.x.x.x または x.x.x.x/n) を入力して Add[追加] を クリックします。エントリを削除する場合は、削除 (^〇 をクリックします。)

OSPF Filter [OSPF フィルタ] タブ

パス タイプ	候補OSPFルートのルートタイプを指定します。	
エリア	候補 OSPF ルートのエリア識別子を指定します。OSPF area ID[OSPFエリアID](形式は x.x.x.x)を入力し、Add[追加] をクリッ クします。	_
	エントリを削除する場合は、削除 (〇 をクリックします。)
タグ	OSPF タグ値を指定します。数値でタグ値 (1 ~ 255) を入力 し、Add [追加] をクリックします。	
	エントリを削除する場合は、削除 (〇 をクリックします。)

BGP Filter [BGP フィルタ] タブ

コミュニティ	BGP ルーティング ポリシーのコミュニティを指定します。
拡張コミュニティ	BGP ルーティング ポリシーの拡張コミュニティを指定します。

RIP

• Network > Virtual Routers > RIP [ネットワーク > 仮想ルーター > RIP]

RIP(ルーティング情報プロトコル)の設定には、以下の一般設定が含まれます。

RIP 設定	の意味
Enable [有効化]	RIP を有効化する場合に選択します。
デフォルト ルートの拒 否	(<mark>推奨)RIP</mark> 経由でデフォルト ルートを学習しない場合に選択しま す。
BFD	PA-400 Seres、PA-3200 シリーズ、PA-3400 シリーズ、PA-5200 シリーズ、PA-5400 シリーズ、PA-7000 シリーズ、および VM シ リーズ firewall の仮想ルータに対して RIP の双方向フォワーディン グ検出(BFD)をグローバルにイネーブルにするには、次のいずれか を選択します。
	• default(デフォルトのBFD設定が含まれるプロファイルです)
	 ファイアウォール上で作成したBFDプロファイルです。
	 新しいBFDプロファイルを作成する場合はNew BFD Profile[新しいBFDプロファイル]
	すべてのRIPインターフェイスでBFDを無効化する場合はNone (Disable BFD)[なし(BFD無効)]を選択します。シングルRIPのイン ターフェイスでは、BFDを無効化することができません。

- さらに、以下のタブのRIP設定を指定する必要があります。
- Interfaces[インターフェイス]:「RIP Interfaces Tab(RIP のインターフェイス タブ)」を参照 してください。
- Timers[タイマー]:「RIP Timer Tab(RIP タイマー タブ)」を参照してください。
- Auth Profiles[認証プロファイル]:「RIP Auth Profiles Tab (RIP の認証プロファイル タブ)」 を参照してください。
- Export Rules[ルールのエクスポート]:「RIP Export Rules Tab (RIP の エクスポート ルール タブ)」を参照してください。

RIP の Interfaces (インターフェイス) タブ

• Network > Virtual Routers > RIP > Interfaces [ネットワーク > 仮想ルーター > RIP > インター フェイス]

以下のフィールドを使用して RIP インターフェイスを設定します。

RIP - インターフェイス 設定	の意味
インターフェイス	RIP プロトコルを実行するインターフェイスを選択します。
Enable [有効化]	これらの設定を有効にするには、オンにします。
通知	デフォルトルートを、指定したメトリック値でRIPピアに通知する 場合は、これをオンにします。
メトリック	ルータ通知のメトリック値を指定します。Advertise[通知]を可能に した場合のみ、このフィールドが表示されます。
認証プロファイル	プロファイルを選択します。
モード	normal[ノーマル]、passive[パッシブ]、または send-only[送信のみ] を選択します。
BFD	RIPインターフェイスでBFDを有効化する場合は(仮想ルーターの レベルでRIP用のBFDが無効化されていない限り、RIP用のBFD設定 をオーバーライドすることになります)、以下のうち一つを選択し ます。
	• default(デフォルトのBFD設定が含まれるプロファイルです)
	 ファイアウォール上で作成したBFDプロファイルです。
	 新しいBFDプロファイルを作成する場合はNew BFD Profile[新しいBFDプロファイル]
	RIPインターフェイスでBFDを無効化する場合はNone (Disable BFD)[なし(BFD無効)] を選択します。

RIP O Timers (\Diamond \checkmark \neg) \Diamond \checkmark

• Network > Virtual Router > RIP > Timers [ネットワーク > 仮想ルーター > RIP > タイマー]

以下の表はRIPのルート更新や失効をコントロールするタイマーをあらわしています。

RIP - タイマー設定	の意味
RIP タイミング	
間隔 (秒)	タイマ間隔を秒単位で指定します。この時間は、他の [RIP Timing] のフィールドで使用されます (範囲は1~60)。
更新間隔	ルート更新通知間の間隔数を入力します (範囲は1~3600)。

RIP - タイマー設定	の意味
失効の間隔	ルートが最後に更新されてから有効期限が切れるまでの間隔数を入 力します (範囲は1 ~ 3600)。
削除間隔	ルートの有効期限が切れてから削除されるまでの間隔数を入力しま す (範囲は1 ~ 3600)。

RIPの Auth Profiles (認証プロファイル) タブ

• Network > Virtual Router > RIP > Auth Profiles [ネットワーク > 仮想ルーター > RIP > 認証プ ロファイル]

デフォルト設定では、ファイアウォールはネイバー間のRIPメッセージを認証しません。ネイバー間のRIPメッセージを認証する場合は認証プロファイルを作成し、仮想ルーター上でRIPを実行中のインターフェイスにそれを適用します。以下の表に、Auth Profiles[認証プロファイル]タブの設定を示します。

RIP - 認証プロファイル 設定	の意味
プロファイル名	RIP メッセージを認証するための認証プロファイル名を入力します。
パスワード タイプ	パスワードのタイプを選択します (Simple [簡易パスワード] または MD5)。
	• Simple[簡易パスワード] を選択した場合、簡易パスワードを入力 して確認します。
	 MD5 を選択した場合は、Key-ID[キーID] (0 ~ 255)、Key[キー]、および任意の Preferred[優先] 状態など、1 つ以上のパスワード エントリを入力します。エントリごとに Add[追加] をクリックしてから、OK をクリックします。送信 メッセージの認証に使用する鍵を指定するには、Preferred[優先] オプションを選択します。

RIPの **Export Rules**(エクスポートルール)タブ

• Network > Virtual Router > RIP > Export Rules [ネットワーク > 仮想ルーター > RIP > ルールの エクスポート]

RIPエクスポートのルールを設定することで、仮想ルーターがピアに送信可能なルートをコント ロールすることができます。

RIP - エクスポート ルー ル設定	の意味
デフォルト ルートの再 配信を許可	ファイアウォールからピアにデフォルト ルートを再配信することを 許可する場合に選択します。
再配信プロファイル	Add[追加]をクリックし、目的のネットワーク動作に基づいて、 ルート再配信、フィルタ、優先度、アクションを変更できる再配信 プロファイルを選択または追加します。「ルートの再配信」を参照 してください。

OSPF

• Network > Virtual Router > OSPF [ネットワーク > 仮想ルーター > OSPF]

OSPF(Open Shortest Path First)プロトコルを設定するには、以下の一般設定を指定する必要があります(任意の BFD は保続)。

OSPF 設定	の意味
Enable [有効化]	OSPF プロトコルを有効化する場合に選択します。
デフォルト ルートの拒 否	(<mark>推奨</mark>)OSPF 経由でデフォルト ルートを学習しない場合に選択し ます。
ルーターID	この仮想ルーターの OSPF インスタンスに関連付けられているルー タ ID を指定します。OSPF プロトコルでは、このルータ ID を使用 して OSPF インスタンスを一意に識別します。
BFD	PA-400 シリーズ、PA-3200 シリーズ、PA-3400 シリー ズ、PA-5200 シリーズ、PA-5400 シリーズ、PA-7000 シリー ズ、または VM シリーズ ファイアウォール の仮想ルータに対して OSPF の双方向フォワーディング検出(BFD)をグローバルにイネーブ ルにするには、次のいずれかを選択します。
	• default(デフォルトのBFD設定)
	 ファイアウォール上で作成したBFDプロファイルです。
	 新しいBFDプロファイルを作成する場合はNew BFD Profile[新しいBFDプロファイル]
	すべてのOSPFインターフェイスでBFDを無効化する場合はNone (Disable BFD)[なし(BFD無効)]を選択します。シングルOSPFのイ ンターフェイスでは、BFDを無効化することができません。

また、以下のタブで OSPF 設定を指定する必要があります。

- Areas[エリア]:「OSPF Areas Tab(OSPF エリア タブ)」を参照してください。
- Auth Profiles[認証プロファイル]:「OSPF Auth Profiles Tab(OSPF の認証プロファイル タブ)」を参照してください。
- Export Rules[ルールのエクスポート]:「OSPF Export Rules Tab (OSPF の エクスポート ルール タブ)」を参照してください。
- Advanced[詳細]:「OSPF Advanced Tab(OSPF の詳細タブ)」を参照してください。

OSPFのAreas (エリア) タブ

Network > Virtual Router > OSPF > Areas [ネットワーク > 仮想ルーター > OSPF > エリア]
 以下のフィールドでは、OSPF エリア設定について説明します。

OSPF - エリア設定	の意味
エリア	
エリア ID	OSPF パラメータを適用可能なエリアを設定します。 エリアの識別子を x.x.x.x の形式で入力します。この識別子を受け入 れたネイバーのみが同じエリアに属します。
タイプ	 次のいずれかのオプションを選択します。 Normal - 制限はなく、エリアはあらゆる種類のルートを運べます。 Stub - エリアからの外部への経路がありません。エリア外にある宛先に到達するには、別のエリアに接続されている境界を通過する必要があります。このオプションを選択した場合、他のエリアからこのタイプの LSA (Link State Advertisement)を受け入れるには Accept Summary[サマリーの受け入れ]を選択します。また、スタブ領域へのアドバタイズメントにデフォルト経路 LSA を、関連するメトリック値 (範囲は 1 から 255) と共に含めるかどうかを指定します。
	 スタブエリア Area Border Router (ABR) インターフェイスの Accept Summary オプションが無効になっている場合、OSPF エリアは Totally Stubby Area (TSA) として動作し、ABR はサマリー LSAを伝搬しません。 NSSA (Not-So-Stubby Area) - OSPF ルート以外のルートによってのみ、エリアを直接離れることができます。このオプションを選択した場合、このタイプの LSA を受け入れるには Accept Summary[サマリーの受け入れ]を選択します。Advertise Default Route[デフォルト ルートの通知] を選択して、スタブエリアへの通知にデフォルト ルート LSA とそれに関連付けられたメトリック値 (1 ~ 255) を含めるかどうかを指定します。さらに、デフォルト LSA の通知に使用するルート タイプを選択します。

OSPF - エリア設定	の意味
	す。External Range セクションの Add をクリックし、NSSA を 介して学習された外部ルートを他のエリアにアドバタイズまた は抑制する場合は、範囲を入力します。
範囲	Add[追加] をクリックし、エリア内の LSA 宛先アドレスをサブネットに集約します。サブネットと一致する LSA の通知を有効にするか、停止して、OK をクリックします。別の範囲を追加する場合は、この操作を繰り返します。
インターフェイス	エリアに含めるインターフェイスを Add(追加)し、以下の情報を 入力します。
	• Interface[インターフェイス] – インターフェイスを選択します。
	• Enable[有効化] – OSPF インターフェイス設定を有効にします。
	 Passive (パッシブ) – OSPF インターフェイスで OSPF パケットを送受信しない場合に選択します。このオプションをオンにすると OSPF パケットは送受信されませんが、インターフェイスは LSA データベースに追加されます。
	 Link type[リンクタイプ] – このインターフェイスを経由してア クセス可能なすべてのネイバーを、OSPF helloメッセージのマ ルチキャストによって自動的に検出させる場合は、Broadcast[ブ ロードキャスト]を選択します(Ethernetインターフェイスな ど)。自動的にネイバーを検出する場合は、P2p(ポイントツー ポイント)を選択します。ネイバーを手動で定義する必要がある 場合は、P2mp(ポイントツーマルチポイント)を選択します。ネ イバーを手動で定義できるのは、p2mp モードの場合のみです。
	• Metric[メトリック] – このインターフェイスの OSPF メトリック を入力します (0 ~ 65535)。
	 Priority[優先順位] - このインターフェイスの OSPF 優先度を 入力します (0 ~ 255)。OSPF プロトコルでは、この優先度に 基づいて、ルータが指名ルータ (DR) または バックアップ DR (BDR) として選択されます。値が 0 の場合、ルーターが DR また は BDR として選択されることはありません。
	 Auth Profile[認証プロファイル] – 以前に定義した認証プロファ イルを選択します。
	 BFD - OSPFピアのインターフェイスで双方向フォワーディン グの検知(BFD)を有効化する場合は(仮想ルーターのレベル でOSPF用のBFDが無効化されていない限り、OSPF用のBFD設定 をオーバーライドすることになります)、以下のうち一つを選 択します。
	• default(デフォルトのBFD設定)

• ファイアウォール上で作成したBFDプロファイルです。

OSPF - エリア設定	の意味
,	 新しいBFDプロファイルを作成する場合はNew BFD Profile[新しいBFDプロファイル]
	 OSPFピアのインターフェイスでBFDを無効化する場合 はNone (Disable BFD)[なし(BFD無効)]を選択します。
	 Hello Interval (sec)[Hello間隔(秒)] – OSPFプロセスが直接接続されているネイバーにHelloパケットを送信する間隔(秒数)です(範囲は0~3600、デフォルトは10)。
	 Dead Counts[失敗許容回数] – Hello 間隔の試行回数で、この 回数を超えても OSPF がネイバーから Hello パケットを受信し ない場合、OSPF はネイバーがダウンしているものとみなしま す。Hello Interval[Hello間隔]に Dead Counts[失敗許容回数] を 乗じた数が、失敗タイマーの値です(範囲は3~20、デフォルト は4)。
	 Retransmit Interval (sec) (再送信間隔(秒)) – OSPFがネイバー からリンク状態通知(LSA)を待機する秒数で、この時間を過ぎ るとOSPFがLSAを再送信します(範囲は0~3600、デフォルト は10)。
	 Transit Delay (sec) (トランジット遅延(秒)) – LSA の秒単位の 遅延時間です。この時間を過ぎると、インターフェイスから送 信されます(範囲は 0 ~ 3600、デフォルトは 1)。
Interface(インター フェイス)(続き)	 Graceful Restart Hello Delay (sec) (グレースフル リスタート Hello パケット遅延(秒)) – アクティブ/パッシブ高可用性 が設定されている場合に、OSPF インターフェイスに適用され ます。Graceful Restart Hello Delay (グレースフル リスタート Hello パケット遅延)は、ファイアウォールが 1 秒間隔でグレー ス LSA パケットを送信する期間です。この期間は、リスタート 中のファイアウォールから Hello パケットが送信されません。 リスタート中は、失敗タイマー(Hello Interval (Hello 間隔) に Dead Counts (失敗許容回数)を乗じた数) もカウントダウン されます。失敗タイマーの時間が短かすぎる場合は、Hello パ ケットが遅延したときに、グレースフル リスタート中に隣接 がダウンします。そのため、失敗タイマーを Graceful Restart Hello Delay (グレースフル リスタート Hello パケット遅延)の 値の4倍以上にすることをお勧めします。たとえば、Hello Interval (Hello 間隔)が10秒で、Dead Counts (失敗許容回 数)が4回の場合、失敗タイマーは40秒になります。Graceful Restart Hello Delay (グレースフル リスタート Hello パケット遅 延)が 10秒に設定されていれば、10 秒遅延しても失敗タイ マーの 40 秒以内に十分に収まるため、グレースフル リスタート 中に隣接がタイムアウトになることがありません (範囲は 1 ~ 10、デフォルトは 10)。

OSPF - エリア設定	の意味
仮想リンク	バックボーンエリアの接続を維持または拡張するには、仮想リンク 設定を指定します。この設定は、エリア境界ルータに対して、バッ クボーンエリア内 (0.0.0.0) で定義する必要があります。Add[追加] をクリックし、バックボーンエリアに含める仮想リンクごとに以下 の情報を入力して、OK をクリックします。
	• Name[名前] – 仮想リンクの名前を入力します。
	 Neighbor ID[ネイバー ID] – 仮想リンクの反対側のルータ (ネイバー) のルータ ID を入力します。
	 Transit Area[トランジットエリア] – 仮想リンクが物理的に含まれる中継エリアのエリア ID を入力します。
	• Enable[有効化] – 仮想リンクを有効にするには、オンにします。
	 Timing[タイミング] – デフォルトのタイミング設定のまま使用することをお勧めします。
	 Auth Profile[認証プロファイル] – 以前に定義した認証プロファ イルを選択します。

OSPFの Auth Profiles (認証プロファイル) タブ

• Network > Virtual Router > OSPF > Auth Profiles [ネットワーク > 仮想ルーター > OSPF > 認 証プロファイル]

以下のフィールドでは、OSPF 認証プロファイル設定について説明します。

OSPF - 認証プロファイ ル設定	の意味
プロファイル名	認証プロファイルの名前を入力します。OSPF メッセージを認証す るには、最初に認証プロファイルを定義し、次に OSPF タブでその プロファイルをインターフェイスに適用します。
パスワード タイプ	パスワードのタイプを選択します (Simple [簡易パスワード] または MD5)。
	• Simple[簡易パスワード] を選択した場合は、パスワードを入力し ます。
	 MD5 を選択した場合は、Key-ID[キーID] (0 ~ 255)、Key[キー]、および任意の Preferred[優先] 状態など、1 つ以上のパスワード エントリを入力します。エントリごとに Add[追加] をクリックしてから、OK をクリックします。送信 メッセージの認証に使用する鍵を指定するには、Preferred[優先] オプションを選択します。

 Network > Virtual Router > OSPF > Export Rules [ネットワーク > 仮想ルーター > OSPF > ルー ルのエクスポート]

以下の表では、OSPF ルートをエクスポートするためのフィールドについて説明します。

OSPF - エクスポート ルール設定	の意味
デフォルト ルートの再 配信を許可	OSPF 経由でデフォルト ルートの再配信を許可する場合に選択します。
氏名	再配信プロファイルの名前を選択します。値には IP サブネットま たは有効な再配信プロファイル名を指定する必要があります。
新規パス タイプ	適用するメトリック タイプを選択します。
新規タグ	一致したルート用に 32 ビット値のタグを指定します。
メトリック	(<u>任意</u>)エクスポートされたルートに関連付けられてパス選択に使 用されるルート メトリックを指定します (範囲は 1 ~ 65535)。

OSPFの Advanced (詳細) タブ

• Network > Virtual Router > OSPF > Advanced [ネットワーク > 仮想ルーター > OSPF > 詳細]

以下のフィールドでは、RFC 1583 の互換性、OSPF タイマー、およびグレースフル リスタート について説明します。

OSPF - 詳細設定	の意味
RFC 1583 の互換性	RFC 1583(OSPF バージョン 2)との互換性を確保する場合に選択 します。
タイマー	• SPF Calculation Delay (sec)[SPF計算遅延(秒)] - このタイマー により、新しいトポロジ情報の受信から、SPF計算を実行するま での遅延時間を調整することができます。指定する値が低けれ ばそれだけ OSPF の再収束が速くなります。ファイアウォール とピアリングしているルーターは、収束時間の最適化と同様の 方法で調整する必要があります。
	 LSA Interval (sec)[LSA間隔(秒)] - このオプションは、同 ーLSA(同一ルーター、同一タイプ、同一LSA ID)の2つのイ ンスタンスの伝送間の最小時間を指定します。RFC 2328 の MinLSInterval と同等です。低い値を指定すると、トポロジが変 更された場合の再収束時間が短縮されます。

OSPF - 詳細設定	の意味
グレースフル リスター ト	• Enable Graceful Restart[グレースフルリスタートを有効化] - こ の機能が有効なファイアウォールは、ファイアウォールが一時 的にダウンして移行が実行されている間も、ファイアウォール を経由するルートを引き続き使用するように近隣のルーターに 指示します(デフォルトで有効)。
	 Enable Helper Mode[ヘルパーモードを有効化] - このモードが有 効なファイアウォールは、隣接デバイスの再起動中もそのデバ イスへの転送を継続します(デフォルトで有効)。
	 Enable Strict LSA Checking[厳密なLSAチェックを有効化] - トポロジが変更された場合、この機能により、OSPFへルパーモードが有効なファイアウォールのヘルパーモードが終了します(デフォルトで有効)。
	 Grace Period (sec) (猶予時間(秒)) – 隣接デバイスの再確 立中またはルーターの再起動中にピア デバイスがこのファイア ウォールに向けた転送を継続する秒数です(範囲は 5 ~ 1,800、 デフォルトは 120)。
	 Max Neighbor Restart Time (ネイバー再起動の最大時間) – ファイアウォールをヘルパー モード ルーターとして使用できる 最大猶予時間(秒)です。ピアデバイスのグレースLSAで提供 される猶予時間の方が長い場合、ファイアウォールはヘルパー モードになりません(範囲は5~1800、デフォルトは140)。

OSPFv3IPv6

• Network > Virtual Router > OSPFv3 [ネットワーク > 仮想ルーター > OSPFv3]

OSPFv3 (Open Shortest Path First v3) プロトコルを設定するには、以下の表の最初の3つの設定を指定する必要があります(BFD は任意)。

OSPFv3 設定	の意味
Enable [有効化]	OSPF プロトコルを有効化する場合に選択します。
デフォルト ルートの拒 否	OSPF 経由でデフォルト ルートを学習しない場合に選択します。
ルーターID	この仮想ルーターの OSPF インスタンスに関連付けられているルー タ ID を指定します。OSPF プロトコルでは、このルータ ID を使用 して OSPF インスタンスを一意に識別します。
BFD	PA-400 シリーズ、PA-3200 シリーズ、PA-3400 シリー ズ、PA-5200 シリーズ、PA-5400 シリーズ、PA-7000 シリー ズ、および VM シリーズ ファイアウォール の仮想ルータに対し

OSPFv3設定	の意味
	て、OSPFv3の双方向フォワーディング検出(BFD)をグローバルに イネーブルにするには、次のいずれかを選択します。
	• default(デフォルトのBFD設定)
	 ファイアウォール上で作成したBFDプロファイルです。
	 新しいBFDプロファイルを作成する場合はNew BFD Profile[新しいBFDプロファイル]
	仮想ルーターのすべての OSPFv3 インターフェイスで BFD を無効 化する場合は None (Disable BFD)(なし(BFD 無効))を選択しま す。シングル OSPFv3 のインターフェイスでは、BFD を無効化す ることができません。

さらに、以下のタブで OSPFv3 の設定を指定します。

- Areas[エリア]:「OSPFv3 Areas Tab(OSPFv3 エリア タブ)」を参照してください。
- Auth Profiles[認証プロファイル]:「OSPFv3 Auth Profiles Tab (OSPFv3 の認証プロファイル タブ)」を参照してください。
- Export Rules[ルールのエクスポート]:「OSPFv3 Export Rules Tab (OSPFv3 の エクスポート ルール タブ)」を参照してください。
- Advanced[詳細]:「OSPFv3 Advanced Tab(OSPFv3 詳細タブ)」を参照してください。

OSPFv3の Areas (エリア) タブ

• Network > Virtual Router > OSPFv3 > Areas [ネットワーク > 仮想ルーター > OSPFv3 > エリ ア]

以下のフィールドを使用して、OSPFv3 エリアを設定します。

OSPFv3 - エリア設定	の意味
authentication	この OSPF エリアに指定する認証プロファイルの名前を選択し ます。
タイプ	次のいずれかを選択します。 • Normal - 制限はありません。エリアはすべてのタイプのルー トを伝送できます。
	 Stub - エリアからのコンセントがありません。エリア外にあ る宛先に到達するには、別のエリアに接続されている境界を 通過する必要があります。このオプションを選択した場合、 他のエリアからこのタイプの LSA (Link State Advertisement) を受け入れるには Accept Summary[サマリーの受け入れ] を 選択します。また、スタブ領域へのアドバタイズメントにデ

OSPFv3 - エリア設定	の意味
	フォルト経路 LSA を、関連するメトリック値 (1 から 255) と 共に含めるかどうかを指定します。
	スタブ エリア Area Border Router (ABR) インターフェイスの Accept Summary オプションが無効になっている場合、OSPF エリアは Totally Stubby Area (TSA) として動作し、ABR はサマ リー LSA を伝搬しません。
	 NSSA (Not-So-Stubby Area) - エリアを直接離れることは可能 ですが、OSPF ルート以外のルートによってのみエリアを離 れることができます。このオプションを選択した場合、この タイプの LSA を受け入れるには Accept Summary[サマリー の受け入れ] を選択します。スタブエリアへの通知にデフォ ルトルート LSA とそれに関連付けられたメトリック値 (1 ~ 255) を含めるかどうかを指定します。さらに、デフォルト LSA の通知に使用するルート タイプを選択します。External Ranges セクションの Add をクリックし、NSSA を介して学 習された外部ルートを他のエリアにアドバタイズまたは抑制 する場合は、範囲を入力
範囲	Add[追加] をクリックし、エリア内のLSA宛先 IPv6アドレスを サブネットに集約します。サブネットと一致する LSA の通知を 有効にするか、停止して、OK をクリックします。別の範囲を 追加する場合は、この操作を繰り返します。
インターフェイス	Add[追加] をクリックし、エリアに含めるインターフェイスご とに以下の情報を入力して、OK をクリックします。
	• Interface[インターフェイス] – インターフェイスを選択します。
	 Enable[有効化] – OSPF インターフェイス設定を有効にします。
	 インスタンス ID - OSPFv3 インスタンス ID 番号を入力します。
	 Passive (パッシブ) – OSPF インターフェイスで OSPF パ ケットを送受信しない場合に選択します。このオプションを オンにすると OSPF パケットは送受信されませんが、イン ターフェイスは LSA データベースに追加されます。
	 Link type[リンクタイプ] – このインターフェイスを経由 してアクセス可能なすべてのネイバーを、OSPF helloメッ セージのマルチキャストによって自動的に検出させる場合 は、Broadcast[ブロードキャスト]を選択します(Ethernetイ ンターフェイスなど)。自動的にネイバーを検出する場合 は、P2p(ポイントツーポイント)を選択します。ネイバーを 手動で定義する必要がある場合は、P2mp(ポイントツーマル

OSPFv3 - エリア設定	の意味
	チポイント) を選択します。ネイバーを手動で定義できるの は、p2mp モードの場合のみです。
	• Metric[メトリック] – このインターフェイスの OSPF メト リックを入力します (0 ~ 65535)。
	 Priority[優先順位] – このインターフェイスの OSPF 優先度 を入力します (0 ~ 255)。OSPF プロトコルでは、この優先 度に基づいて、ルータが指名ルータ (DR) または バックアッ プ DR (BDR) として選択されます。値が 0 の場合、ルーター が DR または BDR として選択されることはありません。
	 Auth Profile[認証プロファイル] – 以前に定義した認証プロ ファイルを選択します。
	 BFD - OSPFv3ピアのインターフェイスで双方向フォワー ディングの検知(BFD)を有効化する場合は(仮想ルー ターのレベルでOSPFv3用のBFDが無効化されていない限 り、OSPFv3用のBFD設定をオーバーライドすることになり ます)、以下のうち一つを選択します。
	• default(デフォルトのBFD設定)
	• ファイアウォール上で作成したBFDプロファイルです。
	 新しいBFDプロファイルを作成する場合はNew BFD Profile[新しいBFDプロファイル]
	OSPFv3ピアのインターフェイスでBFDを無効化する場合 はNone (Disable BFD)[なし(BFD無効)] を選択します。
	 Hello Interval (sec)[Hello間隔(秒)] – OSPFプロセスが直接接続されているネイバーにHelloパケットを送信する間隔(秒数)です(範囲は0~3600、デフォルトは10)。
	 Dead Counts[失敗許容回数] – Hello 間隔の試行回数で、この回数を超えても OSPF がネイバーから Hello パケットを受信しない場合、OSPF はネイバーがダウンしているものとみなします。Hello Interval[Hello間隔]に Dead Counts[失敗許容回数]を乗じた数が、失敗タイマーの値です(範囲は3~20、デフォルトは4)。
	 Retransmit Interval (sec) (再送信間隔 (秒)) – OSPFがネイバー からリンク状態通知 (LSA) を待機する秒数で、この時間を過 ぎるとOSPFがLSAを再送信します(範囲は0~3600、デフォ ルトは10)。
	 Transit Delay (sec) (トランジット遅延(秒)) – ファイア ウォールのインターフェイスが LSA の送信を待機させる秒数 です(範囲は 0 ~ 3,600、デフォルトは 1)。

OSPFv3 - エリア設定	の意味
インターフェイス(続き)	 Graceful Restart Hello Delay (sec) (グレースフルリスタート Hello パケット遅延(秒)) – アクティブ/パッシブ高可用性が設定されている場合に、OSPF インターフェイスに適用されます。Graceful Restart Hello Delay (グレースフルリスタート Hello パケット遅延)は、ファイアウォールが1秒間隔でグレース LSA パケットを送信する期間です。この期間は、リスタート中のファイアウォールから Hello パケットが送信されません。リスタート中は、失敗タイマー(Hello Interval (Hello 間隔)に Dead Counts (失敗許容回数)を乗じた数)もカウントダウンされます。失敗タイマーの時間が短かすぎる場合は、Hello パケットが遅延したときに、グレースフルリスタート中に隣接がダウンします。そのため、失敗タイマーを Graceful Restart Hello Delay (グレースフルリスタート Hello パケットが遅延)の値の4倍以上にすることをお勧めします。たとえば、Hello Interval (Hello 間隔)が10秒で、Dead Counts (失敗許容回数)が4回の場合、失敗タイマーは40秒になります。Graceful Restart Hello Delay (グレースフルリスタート Hello パケット遅近)が10秒に設定されていれば、10秒遅延しても失敗タイマーの40秒以内に十分に収まるため、グレースフルリスタート中に隣接がタイムアウトになることがありません(範囲は1~10、デフォルトは10)。 Neighbors[ネイバー] – p2pmp インターフェイスの場合、このインターフェイスを介して到達可能なすべてのネイバーに対するネイバーIP アドレスを入力します。
仮想リンク	 バックボーンエリアの接続を維持または拡張するには、仮想リンク設定を指定します。設定は、エリア境界ルーターに対して定義する必要があり、バックボーン・エリア (0.0.0.0) 内で定義する必要があります。Add[追加] をクリックし、バックボーンエリアに含める仮想リンクごとに以下の情報を入力して、OKをクリックします。 Name[名前] - 仮想リンクの名前を入力します。 Instance ID[インスタンス ID] - OSPFv3 インスタンス ID 番号を入力します。 Neighbor ID[ネイバー ID] - 仮想リンクの反対側のルータ (ネイバー) のルータ ID を入力します。 Transit Area[トランジットエリア] - 仮想リンクが物理的に含まれる中継エリアのエリア ID を入力します。 Enable[有効化] - 仮想リンクを有効にするには、オンにします。

OSPFv3 - エリア設定	の意味
	 Timing[タイミング] – デフォルトのタイミング設定のまま使用することをお勧めします。
	 Auth Profile[認証プロファイル] – 以前に定義した認証プロファイルを選択します。

OSPFv3の(認証プロファイル)タブ

Network > Virtual Router > OSPFv3 > Auth Profiles [ネットワーク > 仮想ルーター > OSPFv3 > 認証プロファイル]

以下のフィールドを使用して、OSPFv3の認証を設定します。

OSPFv3 - 認証プロ ファイル設定	の意味	
プロファイル名	認証プロファイルの名前を入力します。OSPF メッセージ を認証するには、最初に認証プロファイルを定義し、次に OSPF タブでそのプロファイルをインターフェイスに適用 します。	
SPI	リモート ファイアウォールからピアへのパケット トラ バーサルのセキュリティ パラメータ インデックス (SPI) を 指定します。	
PROTOCOL	以下のいずれかのプロトコルを指定します。 • ESP – Encapsulating Security Payload プロトコル。 • AH – Authentication Header プロトコル。	
暗号化アルゴリズ ム	 以下のいずれかを指定します。 None[なし] - 暗号化アルゴリズムは使用されません。 SHA1(デフォルト) - Secure Hash Algorithm 1。 SHA256 - Secure Hash Algorithm 2。256 ビット ダイ ジェストの 4 つのハッシュ関数のセット。 SHA384 - Secure Hash Algorithm 2。384 ビット ダイ ジェストの 4 つのハッシュ関数のセット。 SHA512 - Secure Hash Algorithm 2。512 ビット ダイ ジェストの 4 つのハッシュ関数のセット。 MD5 - MD5 メッセージ ダイジェスト アルゴリズム。 	
キー/再入力キー	認証鍵を入力して確認します。	

OSPFv3 - 認証プロ ファイル設定	の意味
暗号化 (ESP プロト コルのみ)	 以下のいずれかを指定します。 3des(デフォルト) – 56 ビットの 3 つの暗号化鍵を使用する Triple Data Encryption Algorithm (3DES) を適用します。 aes-128-cbc – 128 ビットの暗号化鍵を使用して AES (Advanced Encryption Standard)を適用します。 aes-192-cbc – 192 ビットの暗号化鍵を使用して AES (Advanced Encryption Standard)を適用します。 aes-256-cbc – 256 ビットの暗号化鍵を使用して AES (Advanced Encryption Standard)を適用します。 aes-256-cbc – 256 ビットの暗号化鍵を使用して AES (Advanced Encryption Standard)を適用します。 null – 暗号化は使用されません。
キー/再入力キー	暗号化鍵を入力して確認します。

OSPFv3の **Export Rules** (エクスポート ルール) タブ

 Network (ネットワーク) > Virtual Router (仮想ルーター) > OSPFv3 > Export Rules (エク スポート ルール)

以下のフィールドを使用して、OSPFv3 ルートをエクスポートします。

OSPFv3 - エクス ポート ルール設定	の意味
デフォルト ルート の再配信を許可	OSPF 経由でデフォルト ルートの再配信を許可する場合に 選択します。
氏名	再配信プロファイルの名前を選択します。値には IP サブ ネットまたは有効な再配信プロファイル名を指定する必要 があります。
新規パス タイプ	適用するメトリック タイプを選択します。
新規タグ	一致したルート用に 32 ビット値のタグを指定します。
メトリック	(任意)エクスポートされたルートに関連付けられてパス 選択に使用されるルート メトリックを指定します (範囲は 1 ~ 65535)。

OSPFv3の Advanced (詳細) タブ

• Network(ネットワーク) > Virtual Router(仮想ルーター) > OSPFv3 > Advanced(詳細)

以下のフィールドを使用して SPF 計算用トランジット ルーティングを無効にし、OSPFv3 のタ イマーとグレースフル リスタートを設定します。

このファイアウォールから送信されるルーター LSA に R ビットを設定して、ファイアウォールがアクティブでない ことを示す場合に選択します。この状態のファイアウォー ルはOSPFv3に参加しますが、その他のルーターはトラン ジットトラフィックを送信しません。この状態でも、ロー
カルトラフィックは引き続きファイアウォールに転送され ます。トラフィックをデバイス周辺に再ルーティングしな がらそのファイアウォールにも到達できるため、これは デュアルホームネットワークで保守を行う場合に役立ちま す。
 SPF Calculation Delay (sec) (SPF 計算遅延(秒)) – これは、新しいトポロジ情報の受信と SPF 計算の情報間で遅延時間を調整できる遅延タイマーです。指定する値が低ければそれだけ OSPF の再収束が速くなります。ファイアウォールとピアリングしているルーターは、収束時間の最適化と同様の方法で調整する必要があります。 LSA Interval (sec)[LSA 間隔(秒)] – このオプションは、同一 LSA (同一ルーター、同一タイプ、同一 LSA ID)の2つのインスタンスの伝送間の最小時間を指定します。RFC 2328 の MinLSInterval と同等です。低い値を指定すると、トポロジが変更された場合の再収束時間が短縮されます。
 Enable Graceful Restart[グレースフルリスタートを有効化] - この機能が有効なファイアウォールは、ファイアウォールが一時的にダウンして移行が実行されている間も、ファイアウォールを経由するルートを引き続き使用するように近隣のルーターに指示します(デフォルトで有効)。 Enable Helper Mode[ヘルパーモードを有効化] - このモードが有効なファイアウォールは、隣接デバイスの再起動中もそのデバイスへの転送を継続します(デフォルトで有効)。 Enable Strict LSA Checking[厳密なLSAチェックを有

OSPFv3 - 詳細設定	の意味
	り、OSPFヘルパーモードが有効なファイアウォールの ヘルパーモードが終了します(デフォルトで有効)。
	 Grace Period (sec) (猶予時間(秒)) – 隣接デバイスの再確立中またはルーターの再起動中にピア デバイスがこのファイアウォールに向けた転送を継続する秒数です(範囲は 5 ~ 1,800、デフォルトは 120)。
	 Max Neighbor Restart Time[ネイバー再起動の最大時間] - ファイアウォールをヘルパーモードルーターとして使用できる最大猶予時間(秒)です。ピアデバイスのグレースLSAで提供される猶予時間の方が長い場合、ファイアウォールはヘルパーモードになりません(範囲は5~800、デフォルトは140)。

BGP

• Network > Virtual Router > BGP [ネットワーク > 仮想ルーター > BGP]

Border Gateway Protocol(BGP)では、以下の表の説明に従って BGP の基本設定を指定 し、BGP を有効にしてルーター ID と AS 番号を設定する必要があります。また、BGP ピア グ ループの一部として BGP ピアを設定する必要があります。

ネットワークで必要な場合は、以下のタブで残りの BGP 設定を指定します。

- General[一般]:「BGP の General (全般) タブ」を参照してください。
- Advanced[詳細]:「BGP の Advanced (詳細) タブ」を参照してください。
- Peer Group[ピアグループ]:「BGP の Peer Group (ピア グループ) タブ」を参照してください。
- Import[インポート]:「BGPの Import(インポート)および Export(エクスポート)タブ」を 参照してください。
- Export[エクスポート]:「BGPの Import(インポート)および Export(エクスポート)タブ」 を参照してください。
- Conditional Adv[条件付き通知]:「BGP の Conditional Adv(条件付き通知)タブ」を参照して ください。
- Aggregate[集約]:「BGP の Aggregate(集約)タブ」を参照してください。
- Redist Rules[ルールの再配信]:「BGP の Redist Rules(再配信ルール)タブ」を参照してくだ さい。

BGPの基本設定

仮想ルーターで BGP を使用するには、BGP を有効にしてルーター ID と AS 番号を設定する必要 があります。BFD の有効化は任意です。

BGP 設定	設定場所	の意味
有効化	BGP	BGP を有効にする場合に選択します。
ルーターID		仮想ルーターに割り当てる IP アドレスを入力します。
AS 番号		ルーターID に基づいて、仮想ルーターが属する AS の番号を 入力します (範囲は 1 ~ 4,294,967,295)。
BFD		PA-400 シリーズ、PA-3200 シリーズ、PA-3400 シリー ズ、PA-5200 シリーズ、PA-5400 シリーズ、PA-7000 シ リーズ、または VM シリーズ firewall の仮想ルータに対して BGP の双方向フォワーディング検出(BFD)をグローバルにイ ネーブルにするには、次のいずれかを選択します。
		• default (デフォルトのBFD設定)
		● ファイアウォールの既存の BFD プロファイル
		• 新しい BFD プロファイルの作成
		すべてのBGPインターフェイスでBFDを無効化する場合 はNone (Disable BFD)[なし(BFD無効)]を選択します。シ ングルBGPのインターフェイスでは、BFDを無効化すること ができません。
		グローバルに BFD を有効化あるいは無効化 する場合、BGP を実行中のすべてのインター フェイスが停止され、BFD の機能で再起動され ます。これにより、BGP トラフィックが中断 される可能性があります。よって、BGP イン ターフェイスで BFD を有効化する場合は、こ のような再収斂が実働トラフィックに影響を与 えないようなオフピーク時に行うようにしてく ださい。

BGPの General (全般) タブ

Network > Virtual Router > BGP > General [ネットワーク > 仮想ルーター > BGP > 全般]
 以下のフィールドを使用して、BGP の全般設定を指定します。

BGP の全般設 定	設定場所	の意味
デフォルト ルートの拒否	BGP > 一般	BGP ピアから通知されるデフォルト ルートを無視する場合 に選択します。

BGP の全般設 定	設定場所	の意味	
ルートのイン ストール		グローバル ルーティング テーブルに BGP ルートをインス トールする場合に選択します。	
MED の集約		ルートの MED (Multi-Exit Discriminator) 値が異なる場合でも ルート集約を有効にするには、オンにします。	
デフォルト ローカル設定		異なるパスで設定を決定するためにファイアウォールで使用 できる値を指定します。	
ASフォー マット	-	2-byte [2 バイト] (デフォルト) または 4-byte [4 バイト] 形式 を選択します。これは、相互運用性のために設定します。	
常に MED を 比較		別の AS 内のネイバーから受け取ったパスの MED 比較を有 効にします。	-
決定論的 MED 比較	-	iBGP ピア(同じ AS 内の BGP ピア)から通知されたルート の中からルートを選択するための MED 比較を有効にしま す。	
認証プロファ イル	-	新しい認証プロファイルを Add(追加)し、以下の設定を指 定します。	
		 Profile Name[プロファイル名] – プロファイルの識別に使用する名前を入力します。 	
		 Secret/Confirm Secret[シークレット/再入力 シークレット] – BGP ピア通信に使用するパスフレーズを入力し、確認します。 	
		不要になったプロファイルは削除 (〇 します。)

BGPの Advanced (詳細) タブ

• Network > Virtual Router > BGP > Advanced [ネットワーク > 仮想ルーター > BGP > 詳細]

BGP の詳細設定には、さまざまな機能が含まれます。複数の BGP AS で ECMP を実行できま す。(更新パケットのなりすましを防止するために)AS_PATH 属性の最初の AS として各自の AS をリストするように eBGP ピア に要求できます。BGP グレースフル リスタートを設定でき ます。これは、ルート フラッピング(増減)の影響を最小限に抑えるために BGP の再起動中に 転送状態を BGP ピアで保持できるかどうかを示す方法です。AS の BGP ピアリングがフル メッ シュにならないように、ルート リフレクタと AS コンフェデレーションを設定できます。ルート ダンペニングを設定して、BGP ネットワークが不安定な場合やルートがフラッピングしている 場合に不要なルーターの収束を回避できます。

BGP の詳細設 定	設定場所	の意味
ECMP の複 数の AS のサ ポート	BGP > 上級	仮想ルーターの ECMP を有効にして、複数の BGP AS で ECMP を実行できるようにする場合に選択します。
EBGP 用の First AS の実 施		ファイアウォールは、AS_PATH 属性の最初の AS として eBGP ピアの各自の AS 番号をリストしていない eBGP ピア からの受信更新パケットをドロップします。これにより、隣 接する AS 以外の AS から送信されたなりすまし更新パケッ トや誤った更新パケットが BGP でこれ以上処理されること を回避できます。デフォルトで有効になっています。
グレースフル リスタート		グレースフル リスタート オプションをアクティベーション します。
		 Stale Route Time[ルート停滞時間] - ルートが膠着状態を 持続できる時間を指定します(範囲は1~3600 秒、デ フォルトは120秒)。
		 Local Restart Time[ローカル再起動時間] - ファイアウォー ルの再起動にかかる秒数を指定します。この値はピアに 通知されます(範囲は1~3600、デフォルトは120)。
		 Max Peer Restart Time[最大ピア再起動時間] - ファイア ウォールがピアデバイス再起動時の猶予時間として許容 する最大秒数を指定します(範囲は1~3600秒、デフォ ルトは120秒)。
リフレクタ クラスタ ID		リフレクタ クラスタを示す IPv4 識別子を指定します。AS の ルート リフレクタ (ルーター)は、学習したルートをそのピ アに再通知します。そのため、フル メッシュ接続ですべての ピアがルートを相互に通知する必要はありません。ルート リ フレクタにより、設定が簡略化されます。
コンフェデ レーション メンバー AS		BGP コンフェデレーション内でのみ表示される AS 番号の識 別子(サブ AS 番号とも呼ばれます)を指定します。BGP コ ンフェデレーションを使用して AS をサブ AS に分割し、フ ル メッシュ ピアリングを削減します。
プロファイル のダンペニン グ	BGP > 詳細 (続き)	ルート ダンペニングは、フラッピングしているルートの通知 を停止するかどうかを判断する方法です。ルート ダンペニン グにより、ルート フラッピングに起因するルーターの再収束 の回数を削減できます。以下の設定があります。
		 Profile Name[ノロノアイル名] – フロファイルの識別に使用する名前を入力します。

BGP の詳細設 定	設定場所	の意味
		• Enable[有効化] – プロファイルをアクティベーションしま す。
		• Cutoff[カットオフ] - ルート停止のしきい値を指定し、この値を超えるとルート通知が停止されるようにします (範囲は0.0~1000.0、デフォルトは1.25)。
		 Reuse[再利用] – ルート停止のしきい値を指定します (範囲は 0.0 ~ 1000.0、デフォルトは 5)。この値を下回ると ルートは再度使用されます。
		 Max.Max. Hold Time[最大ホールドタイム] – ルートの不 安定度に関係なく、ルートを停止できる時間の最大長を 指定します (範囲は 0 ~ 3600 秒、デフォルトは 900 秒)。
		 Decay Half Life Reachable (到達可能のライフ半減) – ファイアウォールでルートが到達可能とみなされてか ら、ルートの安定性メトリックを 1/2 にするまでの時間 を指定します (範囲は 0 ~ 3600 秒、デフォルトは 300 秒)。
		 Decay Half Life Unreachable(到達不能のライフ半減) ファイアウォールでルートが到達不能とみなされてから、ルートの安定性メトリックを 1/2 にするまでの時間を指定します(範囲は 0 ~ 3600 秒、デフォルトは 300 秒)。
		不要になったプロファイルは削除 (〇 します。

BGPの**Peer Group** (ピア グループ) タブ

• Network > Virtual Router > BGP > Peer Group [ネットワーク > 仮想ルーター > BGP > ピア グ ループ]

BGP ピア グループは、ピア グループのタイプ(例: EBGP)などの設定や、仮想ルーターが更新 パケットで送信する AS_PATH リストからプライベート AS 番号を削除するための設定を共有す る一連の BGP ピアです。BGP ピア グループにより、同じ設定のピアを複数設定する必要がなく なります。グループに属する BGP ピアを設定するには、1 つ以上の BGP ピア グループを設定 する必要があります。

BGP ピア グ ループ設定	設定場所	の意味
名前	BGP > ピア グループ	ピア グループの識別に使用する名前を入力します。

)

BGP ピア グ ループ設定	設定場所	の意味
Enable [有効 化]		ピア グループをアクティベーションする場合に選択します。
集約済みコ ンフェデレー ション AS パ ス		設定した集約済みコンフェデレーション AS へのパスを含める場合に選択します。
Soft Reset with Stored Info(保存し た情報を使用 したソフト リセット)		ピア設定の更新後にファイアウォールのソフト リセットを実 行する場合に選択します。
タイプ		ピアまたはグループのタイプを指定し、関連設定を指定しま す (この表に後述されているImport Next Hop [ネクストホッ プのインポート] およびExport Next Hop [ネクストホップの エクスポート] の説明を参照) 。
		 IBGP – 以下を指定します。
		 ネクストホップのエクスポート
		 EBGP Confed[EBGPコンフェデレーション] – 以下を指定 します。
		 ネクストホップのエクスポート
		 IBGP Confed[IBGPコンフェデレーション] – 以下を指定 します。
		 ネクストホップのエクスポート
		• EBGP – 以下を指定します。
		 ネクストホップのインポート
		 ネクストホップのエクスポート
		 Remove Private AS (プライベート AS の削除) (BGP で AS_PATH 属性からプライベート AS 番号を強制的に 削除する場合に選択します)。
ネクスト		ネクストホップのインポートのオプションを選択します。
ホップのイン ポート		 Original (オリジナル) – 元のルート通知で提供されたネクストホップアドレスを使用します。

BGP ピア グ ループ設定	設定場所	の意味
		 Use Peer (ピアの使用) – ピアの IP アドレスをネクスト ホップ アドレスとして使用します。
ネクスト		ネクストホップのエクスポートのオプションを選択します。
ホップのエク スポート		 Resolve(解決) – 転送情報ベース(FIB)を使用してネ クストホップアドレスを解決します。
		 Original (オリジナル) – 元のルート通知で提供されたネ クスト ホップ アドレスを使用します。
		 Use Self(自己の使用) – ネクスト ホップ アドレスを仮 想ルーターの IP アドレスで置き換えて転送パスに含まれ るようにします。
プライベート AS の削除		AS_PATH リストからプライベート AS を削除する場合に選択します。
名前	BGP > ピア グループ > ピ	新しい BGP ピアを追加し、識別に使用する名前を入力します。
Enable [有効 化]		ピアをアクティベーションするには、オンにします。
ピアAS		ピアの AS を指定します。
MP-BGP 拡張 の有効化	BGP > ピア グループ > ピ ア > アドレッ シング	ファイアウォールで RFC 4760 に従って IPv4 および IPv6 の Multiprotocol BGP Address Family Identifier(マルチ プロトコル BGP アドレス ファミリー ID)オプションと Subsequent Address Family Identifier(後続のアドレス ファ ミリー ID)オプションをサポートできるようになります。
アドレス ファミリー タイプ		このピアの BGP セッションでサポートされるアドレス ファ ミリー(IPv4 または IPv6)を選択します。
後続のアド レス ファミ リー		このピアの BGP セッションで使用される後続のアドレス ファミリー プロトコル(Unicast(ユニキャスト)または Multicast(マルチキャスト))を選択します。
ローカル ア ドレス – イ ンターフェイ ス		ファイアウォール インターフェイスを選択します。

ネットワーク

BGP ピア グ ループ設定	設定場所	の意味
ローカル ア ドレス – IP		ローカル IP アドレスを選択します。
ピア アドレ スータイプお よびアドレス		 ピアを識別するアドレスのタイプを選択します: IP-IPを選択し、さらに IP アドレスを使用するアドレス オブジェクトを選択(あるいは IP アドレスを使用するア ドレス オブジェクトを新たに作成)します。 FQDN-FQDN を選択し、さらに FQDN を使用するアド レス オブジェクトを選択(あるいは FQDN を使用するア ドレス オブジェクトを選択(あるいは FQDN を使用するア ドレス オブジェクトを新たに作成)します。
認証プロファ イル	BGP > ピア グループ > ピ ア > 接続オプ ション	プロファイルを選択するか、ドロップダウンから New Auth Profile(新規認証プロファイル)を選択します。プロファ イルのName(名前)、Secret(シークレット)、Confirm Secret(再入力 シークレット)を入力します。
キープ アラ イブ間隔		ピアから受け取ったルートがホールド タイム設定に従って停止されるまでの時間を指定します(範囲は 0 ~ 1,200 秒、デフォルトは 30 秒)。
マルチ ホッ プ	-	IP ヘッダーの TTL (time-to-live) 値を指定します(範囲は 0~255、デフォルトは 0)。デフォルト値の 0 を指定する と、eBGP の場合は 1 が使用されます。デフォルト値の 0 を 指定すると、iBGP の場合は 255 が使用されます。
オープン遅延 時間		ピア TCP 接続を開いてから最初の BGP Open メッセージ を送信するまでの遅延時間を指定します(範囲は 0 ~ 240 秒、デフォルトは 0 秒)。
ホールドタイ ム		ピアからの連続する KEEPALIVE または UPDATE メッセージ 間の想定経過時間を指定します。この時間が過ぎるとピア接 続が閉じられます(範囲は 3 ~ 3,600 秒、デフォルトは 90 秒)。
アイドル ホールド タ イム		アイドル状態で待機する時間を指定します。この時間が経過 すると、ピアへの接続が再試行されます(範囲は 1 ~ 3,600 秒、デフォルトは 15 秒)。
受信接続 リモート ポート		受信ポート番号を指定し、このポートへのトラフィックを Allow(許可)します。

BGP ピア グ ループ設定	設定場所	の意味
送信接続 - ローカル ポート		送信ポート番号を指定し、このポートからのトラフィックを Allow(許可)します。
リフレクタ クライアント	BGP > ピア グループ > ピ ア > 上級	リフレクタ クライアントのタイプを選択します(Non- Client(非クライアント)、Client(クライアン ト)、Meshed Client(メッシュ クライアント)のいずれ か)。リフレクタ クライアントから受信したルートは、すべ ての内部および外部 BGP ピアで共有されます。
ピアリング タイプ		双方向ピアを指定するか、未指定のままにします。
最大プレ フィックス		ピアからインポートする IP プレフィックスの最大数を指定 します(1 ~ 100,000 または無制限)。
送信側ループ 検出の有効化		有効にすると、ファイアウォールは更新でルートを送信する 前に、BGP RIB 内のルートの AS_PATH 属性をチェックし、 ピアAS番号がAS_PATHリストに含まれていないことを確認 します。ピアAS番号がAS_PATHリストにある場合、ファイ アウォールはルートをアドバタイズしません。通常、ループ は受信側で検出されます。しかし、この最適化機能では、送 信側でループ検出を実行します。この機能を無効にして、受 信機にループ検出を実行させます。
BFD		BGP ピアで双方向フォワーディングの検出(BFD)を使用 する際は(仮想ルーターのレベルで BGP 用の BFD が無効化 されていない限り、BGP 用の BFD 設定をオーバーライドす ることになります)、グローバル BGP BFD プロファイルを 引き継ぐ場合は既存の BFD プロファイルであるデフォルト プロファイル(デフォルトの BFD 設定) Inherit-vr-global- setting を選択し、新しい BFD プロファイルを作成する場 合は New BFD Profile(新規 BFD プロファイル)を選択し ます。None (Disable BFD)[なし(BFD無効)]を選択する と、BGPピアのBFDが無効化されます。

BGP ピア グ ループ設定	設定場所	の意味
		 グローバルにBFDを有効化あるいは無効化する 場合、BGPを実行中のすべてのインターフェイ スが停止され、BFDの機能で再起動されます。 これにより、すべてのBGPトラフィックが中断 される可能性があります。インターフェイス上 でBFDを有効化すると、ファイアウォールがピ アとのBGP接続を停止し、インターフェイス上 でBFDのプログラミングを行います。BGP接続 が停止されたことをピアデバイスが検知する と、実働トラフィックに影響を与える再収斂を 行う可能性があります。よって、BGPインター フェイスでBFDを有効化する場合は、このよう な再収斂が実働トラフィックに影響を与えない ようなオフピーク時におこなうようにしてくだ さい。

BGPのImport (インポート) および Export (エクスポート) タブ

- Network > Virtual Router > BGP > Import[ネットワーク > 仮想ルーター > BGP > インポート]
- Network > Virtual Router > BGP > Export [ネットワーク > 仮想ルーター > BGP > エクスポート]

BGP ルートをインポートまたはエクスポートする新しいインポート ルールまたはエクスポート ルールを Add (追加) します。

BGP のイン ポートおよび エクスポート 設定	設定場所	の意味
ルール	BGP > イン ポートまたは エクスポート > 一般	ルールの識別に使用する名前を指定します。インポートルー ルは最大 63 文字です。エクスポートルールの最大文は 31 文字です。ルールは英数字で始まる必要があり、英数字、ア ンダースコア (_)、ハイフン (-)、ドット (.) 、およびスペース の組み合わせを含めることができます。
Enable [有効 化]		ルールをアクティベーションする場合に選択します。
Used By [使 用者]		このルールを使用するピア グループを選択します。

ネットワーク

BGP のイン ポートおよび エクスポート 設定	設定場所	の意味
AS パスの正 規表現	BGP > イン ポートまたは エクフポート	AS パスをフィルタリングするための正規表現を指定します。
コミュニティ の正規表現	→一致	コミュニティ文字列をフィルタリングするための正規表現を 指定します。
拡張コミュニ ティの正規表 現		拡張コミュニティ文字列をフィルタリングするための正規表 現を指定します。
MED		ルートをフィルタリングするための Multi-Exit Discriminator 値を 0 ~ 4、294、967、295 の範囲で指定します。
ルート テー ブル		Import Rule(インポート ルール)では、一致するルート のインポート先のルート テーブル(unicast, multicast, or both.)
		Export Rule(エクスポート ルール)では、一致するルート のエクスポート先のルート テーブル。unicast, multicast, or both.
アドレス プ レフィックス		ルートをフィルタリングするための IP アドレスまたはプレ フィックスを指定します。
ネクストホッ プ		ルートをフィルタリングするためのネクスト ホップ ルー ターまたはサブネットを指定します。
送信元ピア	1	ルートをフィルタリングするためのピア ルーターを指定しま す。
操作	BGP > イン ポートまたは エクスポート > 操作	照合条件を満たしたときに実行するアクション(Allow(許 可)または Deny(拒否))を指定します。
ダンペニング		アクションが Allow(許可)の場合のみ、ダンペニング パラ メータを指定します。
ローカル設定		アクションが Allow(許可)の場合のみ、ローカル優先メト リックを指定します。
MED		アクションが Allow(許可)の場合のみ、MED 値を指定し ます(0 ~ 65,535)。

ネットワーク

BGP のイン ポートおよび エクスポート 設定	設定場所	の意味
重み		アクションが Allow (許可)の場合のみ、重み値を指定しま す(0 ~ 65,535)。
ネクストホッ プ		アクションが Allow (許可)の場合のみ、ネクスト ホップ ルーターを指定します。
元		基となるルートのパス タイプを指定します。IGP、EGP、また動作設定がAllow[許可]となっている場合のみ、incomplete [不完全] から選択します。
AS パス制限	-	アクションが Allow(許可)の場合のみ、AS パス制限を指 定します。
ASパス		AS パスを指定します。動作設定がAllow[許可]となっ ている場合のみ、ASパスにNone [なし]、Remove[削 除]、Prepend[プリペンド]、Remove and Prepend[削除およ びプリペンド] のいずれかを指定します。
コミュニティ	-	コミュニティオプションを指定します。動作設定がAllow [許可] の場合のみ、コミュニティオプションにNone[な し]、Remove All[すべて削除]、Remove Regex[正規表現の削 除]、Append[付加]、Overwrite[上書き] のいずれかを指定し ます。
拡張コミュニ ティ		コミュニティオプションを指定します。動作設定がAllow [許可] の場合のみ、コミュニティオプションにNone[な し]、Remove All[すべて削除]、Remove Regex[正規表現の削 除]、Append[付加]、Overwrite[上書き] のいずれかを指定し ます。
		不要になったルールは Delete(削 除)

BGPの Conditional Adv(条件付き通知)タブ

• Network > Virtual Router > BGP > Conditional Adv [ネットワーク > 仮想ルーター > BGP > 条 件付き通知] BGP 条件付き通知では、ピアリングまたは到達の失敗を含め、ローカル BGP ルーティング テー ブル(LocRIB)で優先ルートを使用できない場合に通知するルートを制御できます。これは、1 つの AS を別の AS より優先してルートを強制する場合に便利です。たとえば、インターネット に対して複数の ISP を経由するリンクがあり、優先プロバイダへの接続が失われない限り、他の プロバイダではなく優先プロバイダにトラフィックをルーティングする場合に有用です。

条件付き通知では、優先ルート(Address Prefix(アドレス プレフィックス))と、優先ルート を識別する他の属性(AS Path Regular Expression(AS パスの正規表現)など)を指定する非存 在フィルタを設定します。非存在フィルタと一致するルートがローカル BGP ルーティング テー ブルで見つからない場合にのみ、ファイアウォールは通知フィルタで指定された代替ルート(他 の非優先プロバイダへのルート)の通知を許可します。

条件付き通知を設定するには、Conditional Adv(条件付き通知)タブを選択して、条件付き通知を Add(追加)し、以下の表の説明に従って値を設定します。

BGP の条件付 き通知設定	設定場所	の意味
Policy(ポリ シー)	BGP > 条件付 きアドバタイ ズ	この条件付き通知ポリシー ルールの名前を指定します。
Enable [有効 化]		この条件付き通知ポリシー ルールを有効にする場合に選択し ます。
Used By [使 用者]		この条件付き通知ポリシー ルールを使用するピア グループ を Add(追加)します。
Non Exist Filter(非存 在フィルタ)	BGP > 条件付 きアドバタイ ズ > 存在しな いフィルター	優先ルートのプレフィックスを指定するには、このタブを 使用します。このタブは、ローカル BGP ルーティングテー ブルで使用可能な場合に通知するルートを指定します。プレ フィックスが通知され非存在フィルタと一致すると、通知が 停止します。 非存在フィルタを Add(追加)して、このフィルタの識別に 使用する名前を指定します。
Enable [有効 化]		非存在フィルタをアクティベーションする場合に選択しま す。
AS パスの正 規表現		AS パスをフィルタリングするための正規表現を指定します。
コミュニティ の正規表現		コミュニティ文字列をフィルタリングするための正規表現を 指定します。
拡張コミュニ ティの正規表 現		拡張コミュニティ文字列をフィルタリングするための正規表 現を指定します。

BGP の条件付 き通知設定	設定場所	の意味
MED		ルートをフィルタリングするための MED 値を指定します (範囲は 0 ~ 4、294、967、295)。
ルート テー ブル		一致するルートが存在するかどうかを確認するためにファイ アウォールで検索するルートテーブル(unicast(ユニキャ スト)、multicast(マルチキャスト)、both(両方))を指 定します。一致するルートがそのルートテーブルに存在しな い場合にのみ、ファイアウォールは代替ルートの通知を許可 します。
アドレス プ レフィックス		優先ルートの正確な Network Layer Reachability Information (NLRI) プレフィックスを Add (追加) しま す。
ネクストホッ プ		ルートをフィルタリングするためのネクスト ホップ ルー ターまたはサブネットを指定します。
送信元ピア		ルートをフィルタリングするためのピア ルーターを指定しま す。
Advertise Filters(通知 フィルタ)	BGP > 条 件付きアド バタイズ > Advertise Filters (通知 フィルタ)	非存在フィルタのルートがローカル ルーティング テーブル で使用できない場合に通知する、ローカル RIB ルーティング テーブルのルートのプレフィックスを指定するには、このタ ブを使用します。 通知されるプレフィックスが非存在フィルタと一致しない と、通知が行われます。 通知フィルタを Add (追加) して、このフィルタの識別に使 用する名前を指定します。
Enable [有効 化]		フィルタをアクティベーションする場合に選択します。
AS パスの正 規表現		AS パスをフィルタリングするための正規表現を指定します。
コミュニティ の正規表現		コミュニティ文字列をフィルタリングするための正規表現を 指定します。
拡張コミュニ ティの正規表 現		拡張コミュニティ文字列をフィルタリングするための正規表 現を指定します。

BGP の条件付 き通知設定	設定場所	の意味
MED		ルートをフィルタリングするための MED 値を指定します (範囲は 0 ~ 4、294、967、295)。
ルート テー ブル		一致するルートが条件付きで通知される場一致するルート が条件付きで通知される場合にファイアウォールで使用す るルート テーブル: unicast, multicast, or both.合にファイア ウォールで使用するルート テーブル:
アドレス プ レフィックス		優先ルートを使用できない場合に通知するルートの正確な Network Layer Reachability Information(NLRI)プレフィッ クスを Add(追加)します。
ネクストホッ プ		ルートをフィルタリングするためのネクスト ホップ ルー ターまたはサブネットを指定します。
送信元ピア		ルートをフィルタリングするためのピア ルーターを指定しま す。

BGPの Aggregate (集約) タブ

• Network > Virtual Router > BGP > Aggregate [ネットワーク > 仮想ルーター > BGP > 集約]

ルート集約は、特定のルート(プレフィックス長が長いルート)を1つのルート(プレフィッ クス長が短いルート)にまとめて、ファイアウォールで送信する必要のあるルーティング通知を 削減し、ルート テーブルのルートを少なくする操作です。

BGP の集約設 定	設定場所	の意味
名前	BGP > 集約	集約ルールの名前を入力します。
プレフィック ス		長いプレフィックスを集約するために使用されるサマリー プ レフィックス(IP アドレス/プレフィックス長)を入力しま す。
Enable [有効 化]		ルートのこの集約を有効にする場合に選択します。
概要		ルートを要約する場合に選択します。
AS セット		この集約ルールを対象としてファイアウォールで集約ルート の AS パスに一連の AS 番号(AS セット)を含める場合に選
BGP の集約設 定	設定場所	の意味
-----------------------	---------------------------------------	--
		択します。AS セットは、集約された個々のルートの元の AS 番号の順不同リストです。
氏名	BGP > 集約 > フィルターの	一致したルートを停止する属性を定義します。停止フィルタ を Add(追加)して名前を入力します。
Enable [有効 化]	השולאנ ו	停止フィルタを有効にする場合に選択します。
AS パスの正 規表現		集約するルートをフィルタリングするための AS_PATH の正 規表現を指定します。たとえば、^5000 は AS 5000 から学 習したルートを意味します。
コミュニティ の正規表現		集約するルートをフィルタリングするためのコミュニティの 正規表現を指定します。たとえば、500:.* は 500:x が含まれ るコミュニティに一致します。
拡張コミュニ ティの正規表 現		集約するルートをフィルタリングするための拡張コミュニ ティの正規表現を指定します。
MED		集約するルートをフィルタリングする MED を指定します。
ルート テー ブル	-	停止する(通知しない)集約ルートに使用するルート テー ブル(unicast(ユニキャスト)、multicast(マルチキャス ト)、またはboth(両方))を指定します。
アドレス プ レフィックス		通知を停止する IP アドレスを入力します。
ネクストホッ プ		停止する BGP プレフィックスのネクスト ホップ アドレスを 入力します。
送信元ピア		(停止する)BGP プレフィックスの受信元ピアの IP アドレ スを入力します。
氏名	BGP > 集約 > Advertise Filters(通知	フィルタに一致するルートをファイアウォールからピアに通 知する通知フィルタの属性を定義します。Add(追加)をク リックし、通知フィルタの名前を入力します。
Enable [有効 化]	711271	通知フィルタを有効にする場合に選択します。

BGP の集約設 定	設定場所	の意味
AS パスの正 規表現		通知するルートをフィルタリングするための AS_PATH の正 規表現を指定します。
コミュニティ の正規表現		通知するルートをフィルタリングするためのコミュニティの 正規表現を指定します。
拡張コミュニ ティの正規表 現		通知するルートをフィルタリングするための拡張コミュニ ティの正規表現を指定します。
MED		通知するルートをフィルタリングするための MED 値を指定 します。
ルート テー ブル	-	集約ルートの通知フィルタに使用するルート テーブル (unicast(ユニキャスト)、multicast(マルチキャスト)、 またはboth(両方))を指定します。
アドレス プ レフィックス		BGP で通知する IP アドレスを入力します。
ネクストホッ プ		BGP で通知する IP アドレスのネクスト ホップ アドレスを入 力します。
送信元ピア		BGP で通知する、プレフィックスの受信元ピアの IP アドレ スを入力します。
	BGP > 集約 >	集約ルートの属性を定義します。
ローカル設定	集約ルート属 性	範囲が0~4、294、967、295のローカル設定。
MED	-	範囲が 0 \sim 4、294、967、295 の Multi Exit Discriminator。
重み		範囲が0~65,535の重み。
ネクストホッ プ		ネクスト ホップ IP アドレス。
元		ルートの元: igp、egp、 または incomplete 。
AS パス制限		範囲が1~255のASパス制限。
ASパス		タイプを選択します。None(なし)または Prepend(プリ ペンド)。

BGP の集約設 定	設定場所	の意味
コミュニティ		タイプを選択します。None(なし)、Remove All(すべて 削除)、Remove Regex(正規表現の削除)、Append(付 加)、Overwrite(上書き)。
拡張コミュニ ティ	-	タイプを選択します。None(なし)、Remove All(すべて 削除)、Remove Regex(正規表現の削除)、Append(付 加)、Overwrite(上書き)。

BGPの Redist Rules (再配信ルール) タブ

• Network > Virtual Router > BGP > Redist Rules [ネットワーク > 仮想ルーター > BGP > ルール の再配信]

以下の表の説明に従って設定を指定し、BGP ルートを再配信するためのルールを作成します。

BGP の再配信 ルール設定	設定場所	の意味
デフォルト ルートの再配 信を許可	BGP > 再配布 ルール	ファイアウォールから BGP ピアにデフォルト ルートを再配 信することを許可します。
氏名		最初に IP サブネットを Add(追加)するか再配信ルールを 作成します。
Enable [有効 化]		この再配信ルールを有効にする場合に選択します。
ルート テー ブル		ルートの再配信先のルート テーブル(unicast(ユニキャス ト)、multicast(マルチキャスト)、またはboth(両方)) を指定します。
メトリック		1~65,535の範囲でメトリックを入力します。
発信元の設定	-	再配信されるルートの発信元(igp、egp 、または incomplete (不完全)を選択します。 incomplete (不完 全)の値は、接続済みルートを示します。
MED の設定		再配信されるルートの MED を 0 ~ 4、294、967、295 の範 囲で入力します。
ローカル設定		再配信されるルートのローカル設定を0~ 4、294、967、295の範囲で入力します。

BGP の再配信 ルール設定	設定場所	の意味
AS パス制限 の設定		再配信されるルートの AS パス制限を 1 ~ 255 の範囲で入力 します。
コミュニティ の設定		10 進数または 16 進数、あるいは AS:VAL のフォーマットで 32 ビットの値を選択するか入力します。AS と VAL はそれぞ れ 0 から 65,535 までの範囲の値です。最大 10 個のコミュ ニティを入力します。
拡張コミュニ ティの設定		16 進数、TYPE:AS:VAL または TYPE:IP:VAL のフォーマッ トで 64 ビットの値を力します。TYPE は 16 ビット、AS や IP は 16 ビット、VAL は 32 ビットです。最大 5 個の拡張コ ミュニティを入力します。

IP マルチキャスト

Network > Virtual Router > Multicast [ネットワーク > 仮想ルーター > マルチキャスト]
 マルチキャストプロトコルを設定する場合は、以下の標準設定を指定する必要があります。

マルチキャスト設定	の意味
Enable [有効化]	マルチキャストルーティングを有効化する場合に選択します。

さらに、以下のタブの設定を指定する必要があります。

- Rendezvous Point[ランデブーポイント]:「Multicast Rendezvous Point Tab(マルチキャストのRendezvous Point(ランデブーポイント)タブ)」を参照してください。
- Interfaces[インターフェイス]:「Multicast Interfaces Tab(マルチキャストの Interfaces (イン ターフェイス) タブ)」を参照してください。
- SPT Threshold[SPTしきい値]:「Multicast SPT Threshold Tab(マルチキャストの SPT Threshold (SPT しきい値) タブ)」を参照してください。
- Source Specific Address Space[送信元固有のアドレススペース]:「Multicast Source Specific Address Tab(マルチキャストの Source Specific Address(送信元固有のアドレス)タブ)」
 を参照してください。
- Advanced[詳細]:「Multicast Advanced Tab (マルチキャストの Advanced (詳細) タブ)」を 参照してください。

マルチキャストの Rendezvous Point (ランデブー ポイント) タブ

• Network > Virtual Router > Multicast > Rendezvous Point [ネットワーク > 仮想ルーター > ラ ンデブー ポイント]

以下のフィールドを使用して、IP マルチキャストのランデブーポイントを設定します。

マルチキャスト設定 - ランデブー ポイント	の意味
RP タイプ	この仮想ルーターで実行するランデブー ポイント(RP)のタイプ を選択します。静的 RP は、他の PIM ルータで明示的に設定する必 要がありますが、候補 RP は自動的に選択されます。
	 None (なし) – この仮想ルーターで実行中の RP がない場合に選択します。
	 Static[静的] – RP用のスタティックIPアドレスを指定し、ドロップダウンリストから RP Interface[RPインターフェイス]および RP Address[RPアドレス]のタイプを選択します。このグループ用に選択したRPではなく指定したRPを使用する場合は、Override learned RP for the same group[取得した同じグループの RP のオーバーライド]を選択します。
	 Candidate[候補] – この仮想ルーターで実行中の RP 候補に以下 の情報を指定します。
	 RP Interface[RP インターフェイス] – RP のインターフェイス を選択します。有効なインターフェイス タイプとしてループ バック、L3、VLAN、Aggregate Ethernet、トンネルなどがあ ります。
	• RP Address [RP アドレス] – RP の IP アドレスを選択します。
	 Priority[優先順位] – 候補 RP メッセージの優先度を指定しま す (デフォルトは 192)。
	 Advertisement interval[通知間隔] – 候補 RP メッセージの通知間隔を指定します。
	 Group list[グループリスト] – Static[静的] または Candidate[候 補] を選択した場合、Add[追加] をクリックし、RP の候補となる グループのリストを指定します。
リモート ランデブー	Add[追加] をクリックし、以下を指定します。
ポイント	● IP address[IP アドレス] – RP の IP アドレスを指定します。
	 Override learned RP for the same group(取得した同じグループのRPのオーバーライド) – このグループで選ばれた RP ではなく指定した RP を使用する場合に選択します。
	 Group[グループ] – 指定したアドレスが RP として機能するグ ループのリストを指定します。

マルチキャストの Interfaces (インターフェイス) タブ

 Network > Virtual Router > Multicast > Interfaces [ネットワーク > 仮想ルーター > マルチキャ スト > インターフェイス] 次のフィールドを使用して、IGMP、PIM、およびグループアクセス権設定を共有するマルチ キャストインターフェイスを設定します。

マルチキャスト設定 - インターフェイス	の意味
氏名	インターフェイス グループの識別に使用する名前を入力します。
の意味	任意の説明を入力します。
インターフェイス	インターフェイス グループに属する 1 つ以上のファイアウォール インターフェイスを Add(追加)し、マルチキャスト グループの アクセス許可、IGMP 設定、および PIM 設定を共有します。
グループ許可	PIM Any-Source Multicast(ASM)または PIM Source-Specific Multicast(SSM)に参加するマルチキャスト グループを指定しま す。
	 Any Source (いずれかの送信元) – Group (グループ) インターフェイス グループ内のインターフェイス上のいずれかの送信元 からのマルチキャスト トラフィックを受信できるマルチキャストグループを識別する Name (名前) を Add (追加) します。デフォルトでは、グループはAny Source (いずれかの送信元) リストに Included (追加済み)です。グループ設定を削除 せずにグループを簡単に除外するには、Included (追加済み)の 選択を解除します。
	 Source Specific (ソース指定) -インターフェイス グループ内 のインターフェイスでマルチキャスト トラフィックが許可さ れているマルチキャスト Group (グループ) と Source (送信 元) IP アドレスの組の Name (名前) を Add (追加) します。 デフォルトでは、グループと送信元はソース指定のリストに Included (追加済み)です。グループとソースのペアを構成を削 除せずに簡単に除外するには、Included (追加済み)の選択を 解除します。
IGMP	IGMP トラフィックの設定を指定します。マルチ キャスト レシー バ対向インターフェイスの場合は、IGMP を有効にする必要があり ます。
	 Enable(有効化) – IGMP 設定を有効にする場合に選択します。
	 IGMP Version[IGMP バージョン] – インターフェイスで実行する バージョン (1、2、または 3) を選択します。
	 Enforce Router-Alert IP Option (ルーター アラート IP オプションの適用) – IGMPv2 または IGMPv3 の場合にルーター アラート IP オプションを要求するには、このオプションを選択しま

マルチキャスト設定 - インターフェイス	の意味
	す。IGMPv1 との互換性を確保するには、これを無効にする必要 があります。
	 Robustness(頑強性) – ネットワーク上のパケット損失を考慮 するための整数値を選択します(範囲は1~7、デフォルトは2) 。パケット損失が頻繁に発生する場合は高い値を選択します。
	 Max Sources(最大ソース) – このインターフェイス グループ で許可する送信元特定メンバシップの最大数を指定します(範 囲は 1 ~ 65,535 または unlimited(無制限))。
	 Max Groups(最大グループ) – このインターフェイス グルー プで許可するマルチキャスト グループの最大数を指定します (範囲は 1 ~ 65,535 または unlimited (無制限))。
	• Query Configuration – 以下を指定します。
	 Query interval (クエリ間隔) – 一般的なクエリと受信者からの応答の最大時間を指定します。
	 Max Query Response Time(最大クエリ応答時間) – 一般的 なクエリと受信者からの応答間の最大時間を指定します。
	 Last Member Query Interval[最終メンバー照会間隔] – グルー プまたは送信元特定クエリメッセージ (グループからの脱退 を示すメッセージに応答して送信されたメッセージも含む) 間 の間隔を指定します。
	 Immediate Leave(すぐに終了) – 脱退メッセージを受信し たときにすぐにグループから脱退させる場合に選択します。
PIM	Protocol Independent Multicast (PIM) 設定を指定します。
	 Enable(有効化) – このインターフェイスにおける PIM メッ セージの受信や送信を許可する場合に選択します。インター フェイスによるマルチキャスト トラフィックの転送を有効にす る必要があります。
	 Assert Interval (アサート間隔) – PIM 転送者を選択するため に、PIM アサート メッセージ間の間隔を指定します。
	 Hello Interval[Hello 間隔] – PIM hello メッセージ間の間隔を指定します。
	 Join Prune Interval (プルーン参加間隔) – PIM 参加メッセージ 間(および PIM プルーン メッセージ間)の秒数を指定します。 デフォルトは60 です。
	 DR Priority (DR 優先順位) – このインターフェイスの指定ルー ターの優先順位を指定します。
	 BSR Border(BSR ボーダー) – インターフェイスをブートスト ラップ境界として使用する場合に選択します。

マルチキャスト設定 - インターフェイス	の意味
	 PIM Neighbors (PIM ネイバー) – PIM を使用して通信するネ イバーのリストを Add (追加)します。

マルチキャストの SPT Threshold (SPT しきい値) タブ

• Network > Virtual Router > Multicast > SPT Threshold [ネットワーク > 仮想ルーター > SPT し きい値]

最短パスツリー(SPT)しきい値は、仮想ルーターがマルチキャスト グループまたはプレフィックスのマルチキャスト ルーティングを、共有ツリー配信(ランデブー ポイントからの送信元)からソースツリー(最短パスツリーまたは SPT としても知られる)配信に切り替えるポイントを定義します。マルチキャスト グループまたはプレフィックスの SPT しきい値を Add(追加)します。

SPT しきい値	の意味
マルチキャスト グルー プ/プレフィックス	グループまたはプレフィックスへのスループットがしきい値設定に 達したときに、マルチキャスト ルーティングが SPT 配信に切り替 わるマルチキャスト アドレスまたはプレフィックスを指定します。
しきい値 (kbps)	マルチキャストルーティングが対応するマルチキャストグループま たはプレフィックスのSPT配信に切り替えるポイントを指定するに は、次の設定を選択します。
	 0(最初のデータパケットをオンにする) – (デフォルト) グ ループまたはプレフィックスのマルチキャストパケットが到達 すると、仮想ルータは SPT ディストリビューションに切り替え ます。
	 なし(spt に切り替えない) – 仮想ルータはこのグループまたは プレフィックスにマルチキャスト トラフィックを転送し続けま す。
	 任意のインターフェイスおよび任意の期間(範囲 は1~4,294,967,295)で、対応するマルチキャストグループま たはプレフィックスに到達できるマルチキャストパケットから の合計キロビット数を入力します。スループットがこの数に達 すると、仮想ルータは SPT ディストリビューションに切り替わ ります。

マルチキャストの送信元固有のアドレス空白タブ

 Network > Virtual Router > Multicast > Source Specific Address Space [ネットワーク > 仮想 ルーター > マルチキャスト > 送信元固有のアドレス スペース] 特定の送信元からのマルチキャスト パケットを受信できるマルチキャスト グループを Add (追加) します。これらは、Multicast (マルチキャスト) > Interfaces (インターフェイス) > Group Permissions (グループ権限) タブに指定したのと同じマルチキャスト グループと名前です。

マルチキャスト設定 - 送信元特定アドレス空 間	の意味
氏名	ファイアウォールで送信元特定マルチキャスト(SSM)サービスを 提供するときの提供先のマルチキャスト グループを識別します。
グループ	特定の送信元からのマルチキャスト パケットを受信できるマルチ キャスト グループ アドレスを指定します。
含まれる	マルチキャスト グループを SSM アドレス空間に含める場合に選択 します。

マルチキャストの Advanced (詳細) タブ

• Network > Virtual Router > Multicast > Advanced [ネットワーク > 仮想ルーター > マルチキャ スト > 詳細]

セッション終了後にマルチキャスト ルートがルーティング テーブルに残る時間を設定します。

マルチキャストの詳細 設定	の意味
ルートのエイジアウト 秒数	セッション終了後にマルチキャストルートがルーティングテーブル に残る秒数を設定することができます(範囲は210~7200、デフォ ルトは210)。

ECMP

 Network > Virtual Routers > Router Settings > ECMP [ネットワーク > 仮想ルーター > ルー ター設定 > ECMP]

ECMP(Equal Cost Multiple Path)処理はネットワーキング機能の一つで、これを使用するとファイアウォールは、同じ宛先に対する等コストのルートを最大4つ使用できます。この機能を使用しないときに、同じ宛先に対する等コストのルートが複数ある場合、仮想ルーターは、それらのルートのいずれかをルーティングテーブルから選択し、その転送テーブルに追加します。選択したルートが使用不能でない限り、他のルートは使用しません。仮想ルーターで ECMP 機能を有効にすると、ファイアウォールは、宛先に対する等コストのパスをその転送テーブル内に最大4つ持つことができ、以下のことが可能になります。

• 複数の等コストリンクでの同じ宛先への負荷分散フロー(セッション)。

- 一部のリンクを未使用のままにせず、同じ宛先に対するすべてのリンクで使用可能な帯域幅 を利用する。
- リンクに障害が発生した場合、同じ宛先に向かう別の ECMP メンバーにトラフィックを動的 に切り替える。ルーティングプロトコルまたは RIB テーブルが代替パス/ルートを選択する のを待つ必要はありません。これにより、リンク障害時のダウン タイムを削減できます。

ECMP 負荷分散は、パケット レベルではなく、セッション レベルで実行されます。つまり、 ファイアウォールは、パケットを受信するたびではなく、新規セッションの開始時に等コストの パスを選択します。

● 既存の仮想ルーターでECMPを有効化、無効化、または変更する場合、ルーターは システムに対し仮想ルーターを再起動させるため、既存のセッションが強制終了される恐れがあります。

仮想ルーターの ECMP を設定するには、仮想ルーターを選択し、Router Settings(ルーター設定)で ECMP タブを選択した後、説明に従って ECMP 設定を指定します。

確認すべき情報	以下を参照
ECMP を設定する際に使用可 能なフィールドは?	ECMP 設定
その他の情報をお探しです か?	ECMP

ECMP 設定

• Network > Virtual Routers > Router Settings > ECMP [ネットワーク > 仮想ルーター > ルー ター設定 > ECMP]

以下のフィールドを使用して、ECMP(Equal-Cost Multiple Path) 設定を指定します。

ECMP 設定	の意味
Enable [有効化]	ECMP を Enable(有効化)します。
	● 既存の仮想ルーターでECMPを有効化、無効化、または変更する場合、システムが仮想ルーターを再起動し、既存のセッションが終了させられる場合があります。
対称リターン	(任意) Symmetric Return[対称リターン] を選択すると、関連付け られた入力パケットが到着した際と同じインターフェイスから戻り パケットが出力されます。つまり、ファイアウォールは、ECMP イ ンターフェイスではなく、戻りパケットを送信する入力インター フェイスを使用します。そのため、Symmetric Return(対称リター

ECMP 設定	の意味
	ン)の設定でオーバーライドされます。この動作は、サーバーから クライアントに移動するトラフィックに対してのみ発生します。
Strict Source Path(ス トリクト送信元パス)	ファイアウォール出口で発信される IKE および IPSec トラフィック は、デフォルトで、ECMP ロードバランシング方式が決定するイン ターフェースから出力されます。Strict Source Path(ストリクト送 信元パス)を有効化して、ファイアウォールで発信された IKE およ び IPSec トラフィックが、確実に IPSec トンネルの送信元 IPアドレ スが所属する物理インターフェースから出力される設定にします。 ファイアウォールに同じ宛先への等価コスト パスを提供する複数の ISP がある場合は、Strict Source Path(ストリクト送信元パス)機 能を有効にします。ISP は通常、Reverse Path Forwarding(RPF、 逆パス フォワーディング)の確認(または IPアドレス スプーフィ ングを防ぐ別の確認)を実行して、そのトラフィックが到着した 同じインターフェースから出ていることを確認します。ECMPはデ フォルトで(出口インターフェースとして送信元インターフェース を選択する代わりに)設定された ECMP メソッドに基づいて出力 インターフェースを選択するため、ISP が期待する通りでない場合 があり、ISP が正当なリターン トラフィックをブロックする可能性 があります。このユースケースでは、Strict Source Path(ストリク ト送信元パス)を有効にして、ファイアウォールが IPSec トンネル の送信元 IPアドレスが属するインターフェースである出口インター フェースを使用しています。
最大パス	等コストのパスの最大数を選択します:RIB から FIB にコピーされ うる宛先ネットワーク用(2、3、または 4、デフォルトは 2)。
メソッド	仮想ルーターで使用するECMP 負荷分散アルゴリズムを以下から1 つ選択します。ECMP 負荷分散は、パケット レベルではなく、セッ ション レベルで実行されます。つまり、ファイアウォール (ECMP) は、パケットを受信するたびではなく、新規セッションの開始時に 等コストのパスを選択します。
	 IP Modulo(IP モジュロ)(デフォルト) – 仮想ルーターが、パケットヘッダー内の送信元 IPアドレスと宛先 IPアドレスのハッシュを使用してセッション負荷を分散して、使用する ECMP ルートを決定します。
	 IP Hash (IP ハッシュ) –使用する ECMP ルートを決定する IP ハッシュ方法は2通りあります。
	 IP Hash (IP ハッシュ)を選択する場合、デフォルトではファ イアウォールは送信元 IP アドレスと宛先 IP アドレスのハッ シュを使用します。
	 Use Source Address Only(送信元アドレスのみを使用)(PAN-OS 8.0.3 以上のリリースで利用可能)を選択す

ECMP 設定	の意味
	ると、ファイアウォールは同じ送信元 IPアドレスに所属する セッションすべてを常に同じパスをとることを保証します。
	 Use Source/Destination Ports(送信元/宛先ポートを使用)も 選択している場合、ファイアウォールはいずれかのハッシュ計 算にポートを含めます。負荷分散をさらにランダム化するため に、Hash Seed[ハッシュ シード]値(整数)を入力することもで きます。
	 Weighted Round Robin (重み付きラウンドロビン) – このアル ゴリズムを使用すると、多様なリンクの容量および速度を考慮す ることができます。このアルゴリズムを選択すると、Interface dialog (インターフェース ダイアログ)が開きます。Add (追 加)を選択して、重み付きラウンドロビングループに含め るInterface (インターフェース)を選択します。インターフェイ スごとに、使用するWeight (重みづけ)を入力します (1~255 の範囲、100がデフォルト)。特定の等コストパスの重みづけが 高いほど、新規セッションでその等コストのパスが選択される頻 度が高くなります。より高速のリンクに低速のリンクよりも高い 重みづけを与え、より多くの ECMP トラフィックがより高速のリ ンクを通過させる設定にします。さらに別のインターフェイスお よび重みを Add (追加)します。
	 Balanced Round Robin[均等ラウンドロビン] – 受信 ECMP セッションをリンク全体に均等に分散します。

仮想ルーターの詳細ランタイム状態

仮想ルーターのスタティック ルートまたはルーティング プロトコルを設定した 後、Network(ネットワーク) > Virtual Routers(仮想ルーター)を選択し、最後の列の More Runtime Stats(ランタイム状態の詳細)を選択すると、仮想ルーターの詳細情報が表示され ます。たとえば、ルート テーブル、転送テーブル、設定したルーティング プロトコルとスタ ティック ルートが表示されます。このウィンドウで提供される仮想ルーターの詳細情報は1 面に収まりません。このウィンドウには、以下のタブが表示されます。

- Routing[ルーティング]:「Routing Tab(ルーティングタブ)」を参照してください。
- **RIP**:「**RIP** Tab(**RIP** タブ)」を参照してください。
- **BGP**:「BGP Tab(BFP タブ)」を参照してください。
- Multicast[マルチキャスト]:「Multicast Tab(マルチキャスト タブ)」を参照してください。
- **BFD Summary Information**(**BFD** サマリー情報):「**BFD Summary Information Tab**(**BFD** サ マリー情報)」を参照してください。

Routing Tab (ルーティングタブ)

以下の表は、仮想ルーターのルート テーブル、転送テーブル、スタティック ルートのモニタリ ング テーブルのランタイム統計について示しています。

Runtime Stat(ラン タイム統計)	の意味
ルート テーブル	
ルート テーブル	ユニキャストまたはマルチキャストのルート テーブルを表示するに は、Unicast(ユニキャスト)または Multicast(マルチキャスト)を選 択します。
アドレス ファミ リーの表示	テーブルに表示するアドレスのグループの種類を制御するには、IPv4 Only(IPv4 のみ)、IPv6 Only(IPv6 のみ)、または IPv4 and IPv6(IPv4 および IPv6)(デフォルト)を選択します。
宛先	仮想ルータが到達できるネットワークの IPv4 アドレスおよびネットマ スクまたは IPv6 アドレスおよびプレフィックス長。
ネクストホップ	宛先ネットワーク方向のネクスト ホップにあるデバイスの IP アドレ ス。ネクスト ホップが 0.0.0.0 の場合は、デフォルト ルートを表しま す。
メトリック	ルートのメトリック。ルーティング プロトコルで同一の宛先ネットワー クへの複数のルートが存在する場合、メトリック値が最も小さいルート が優先されます。各ルーティング プロトコルは異なるタイプのメトリッ クを使用します。たとえば、RIP はホップ数を使用します。
重み	ルートの重みです。たとえば、BGP で同一の宛先への複数のルートがあ る場合、最も重みが大きいルートが優先されます。
flags	• A?B – アクティブかつ、BGP 経由で学習したもの
	 AC – アクティブかつ、内部インターフェイスの結果(接続済み) - 宛先 = ネットワーク
	 AH – アクティブかつ、内部インターフェイスの結果(接続済み) - 宛先 = ホストのみ
	 AR – アクティブかつ、RIP 経由で学習したもの
	 AS – アクティブかつ、スタティック
	 S-非アクティブ(このルートがより高いメトリックを持っているため)かつ、スタティック
	• O1 – OSPF 外部タイプ -1
	● O1 – OSPF 外部タイプ -2
	• Oi – OSPF エリア内
	 Oo – OSPF エリア問

Runtime Stat (ラン タイム統計)	の意味
エイジ	ルーティング テーブルのルート エントリのエイジ。スタティック ルー トには、エイジはありません。
インターフェイス	ネクストホップに到達するために使用される仮想ルーターの出力イン ターフェイス。
レートの	テーブルのランタイム統計を更新する場合にクリックします。

転送テーブル

ファイアウォールは最適なルート(ルートテーブル(RIB)から宛先ネットワーク)を選択し、FIB に配置します。

アドレス ファミ リーの表示	表示するルート テーブルの種類を制御するには、IPv4 Only(IPv4 の み)、IPv6 Only(IPv6 のみ)、または IPv4 and IPv6(IPv4 および IPv6)(デフォルト)を選択します。
宛先	ルート テーブルから選択された、仮想ルーターが到達できるネットワー クの最適な IPv4 アドレスおよびネットマスク、または IPv6 およびプレ フィックス長です。
ネクストホップ	宛先ネットワーク方向のネクスト ホップにあるデバイスの IP アドレ ス。ネクスト ホップが 0.0.0.0 の場合は、デフォルト ルートを表しま す。
flags	 u – ルートの状態はアップです。 h – ルートはホストに向かいます。 g – ルートはゲートウェイに向かいます。 e – ファイアウォールは等価コスト マルチパス (ECMP) を使用して このルートを選択しています。 * – ルートは、宛先ネットワークに向かう優先パスです。
インターフェイス	ネクスト ホップに到達するために仮想ルーターが使用する出力インター フェイス。
MTU	最大転送単位(MTU)です。この宛先への TCP パケット 1 つあたりで ファイアウォールが転送する最大バイト数を示します。
レートの	テーブルのランタイム統計を更新する場合にクリックします。
フタティックルートのエータリング	

スタティック ルートのモニタリング

Runtime Stat(ラン タイム統計)	の意味
	仮想ルーターが到達できるネットワークの IPv4 アドレスおよびネット マスクまたは IPv6 アドレスおよびプレフィックス長です。
ネクストホップ	宛先ネットワーク方向のネクスト ホップにあるデバイスの IP アドレ ス。ネクスト ホップが 0.0.0.0 の場合は、デフォルト ルートを表しま す。
メトリック	ルートのメトリック。同一の宛先ネットワークへの複数のスタティック ルートが存在する場合、ファイアウォールはメトリック値が最も小さい ルートを優先します。
重み	ルートの重みです。
flags	 A?B - アクティブかつ、BGP 経由で学習したもの AC - アクティブかつ、内部インターフェイスの結果(接続済み) - 宛先 = ネットワーク AH - アクティブかつ、内部インターフェイスの結果(接続済み) - 宛先 = ホストのみ AR - アクティブかつ、RIP 経由で学習したもの AS - アクティブかつ、スタティック S - 非アクティブ (このルートがより高いメトリックを持っているため)かつ、スタティック O1 - OSPF 外部タイプ -1 O1 - OSPF 外部タイプ -2 Oi - OSPF エリア内 Oo - OSPF エリア問
インターフェイス	ネクストホップに到達するために使用される仮想ルーターの出力イン ターフェイス。
パス モニタリング (フェール オン)	 このスタティック ルートでパス モニタリングが有効である場合、Fail On (フェイル オン) は以下を示します。 All (すべて) – スタティック ルートの監視対象の宛先がすべてダウ ンしている場合に、ファイアウォールはスタティック ルートがダウ ンしていると見なして、フェイルオーバーします。 Any (任意) – スタティック ルートの監視対象の宛先いずれかがダ ウンしている場合に、ファイアウォールはスタティック ルートがダ

Runtime Stat (ラン タイム統計)	の意味
	スタティック ルートのパス モニタリングが無効である場合、Fail On(フェイル オン)は Disabled(無効)を示します。
ステータス	監視対象の宛先への ICMP ping に基づく静的ルートのステータス:静的 ルートのUp、Down、またはパスの監視は Disabled (無効)です。
レートの	テーブルのランタイム統計を更新します。

[**RIP**] タブ

以下の表は、仮想ルーターの RIP のランタイム状態を示しています。

RIP のランタイム状 態	の意味
------------------	-----

Summary [サマリー]タブ

間隔(秒)	間隔の秒数です。RIP はこの値(期間)を使用して、更新、失効、削除 の間隔を管理します。
更新間隔	仮想ルーターがピアに送信する RIP ルート通知更新の間隔。
失効の間隔	仮想ルーターがピアから受信した最後の更新以降の間隔で、この間隔を 超えると、仮想ルーターは、ピアからのルートを使用不可としてマーク します。
削除間隔	ルートが使用不可としてマークされた後、更新を受信しなかった場合 に、ファイアウォールがルートをルーティング テーブルから削除するま での間隔です。

Interface [インターフェイス]タブ

アドレス	RIP が有効な仮想ルーターのインターフェイスの IP アドレス。
認証タイプ	認証のタイプ。simple password [簡易パスワード]、MD5、またはnone [なし] があります。
送信許可	チェック マークが付いている場合、このインターフェイスは、RIP パ ケットの送信が許可されています。
受信許可	チェック マークが付いている場合、このインターフェイスは、RIP パ ケットの受信が許可されています。

RIP のランタイム状 態	の意味
デフォルト ルート の通知	チェック マークが付いている場合、RIP は、デフォルト ルートをピアに 通知します。
デフォルト ルート メトリック	デフォルト ルートに割り当てられたメトリック (ホップ数)。メトリック 値が低いほど、ルーティング テーブルでの優先度が高くなり、優先パス として選択されやすくなります。
キー ID	ピアに対して使用される認証キー。
優先	認証の優先キー。

Peer [ピア]タブ

ピア アドレス	仮想ルーターの RIP インターフェイスに対するピアの IP アドレス。
最終更新	このピアから最終更新を受信した日時。
RIPバージョン	ピアが実行している RIP バージョン。
無効なパケット	このピアから受信した無効なパケット数。ファイアウォールが RIP パ ケットを解析できない理由として、ルート境界を x バイト超えた、パ ケット内のルート数が多すぎる、サブネットが不適切、アドレスが無 効、認証が失敗した、メモリが不十分などが考えられます。
無効なルーター	このピアから受信した無効なルート数。原因として、ルートが無効、イ ンポートが失敗した、メモリが不十分などが考えられます。

[**BGP**] タブ

以下の表は、仮想ルーターの BGP のランタイム状態を示しています。

BGP のランタイム 状態	の意味
Summary [サマリー]タブ	
ルーター ID	BGP インスタンスに割り当てられたルーター ID。
デフォルト ルート の拒否	Reject Default Route [デフォルト ルートの拒否] オプションが設定され ているかどうかを示します。このオプションを設定すると、仮想ルー ターは、BGP ピアが通知したデフォルト ルートをすべて無視します。

BGP のランタイム 状態	の意味
デフォルト ルート の再配信	Allow Redistribute Default Route [デフォルト ルートの再配信を許可] オ プションが設定されているかどうかを示します。
ルートのインス トール	Install Route [ルートのインストール] オプションが設定されているかど うかを示します。このオプションを設定すると、仮想ルーターは、グ ローバル ルーティング テーブルに BGP ルートをインストールします。
グレースフル リス タート	Graceful Restart [グレースフル リスタート] が有効かどうかを示します (サポート)。
AS サイズ	選択されている AS フォーマット サイズが 2 バイトと 4 バイトのいずれ であるのかを示します。
ローカル AS	仮想ルーターが属する AS の番号。
ローカル メンバー AS	ローカル メンバー AS の番号 (仮想ルーターがコンフェデレーションに 含まれている場合にのみ有効)。仮想ルーターがコンフェデレーションに 含まれていない場合、このフィールドは 0 です。
クラスタ ID	設定済みの リフレクタ クラスタ ID が表示されます。
デフォルト ローカ ル設定	仮想ルーターに設定されたデフォルト ローカル設定が表示されます。
常に MED を比較	Always Compare MED [常に MED を比較] オプションが設定されている かどうかを示します。このオプションを設定すると、比較が有効にな り、別の AS 内のネイバーから受け取ったルートの中からルートを選択 できます。
MED に関係なく 集約	Aggregate MED [MED の集約] オプションが設定されているかどうかを 示します。このオプションを設定すると、ルートの MED 値が異なる場 合でも、ルート集約が有効になります。
決定論的 MED 処 理	Deterministic MED [決定論的 MED 比較] オプションが設定されている かどうかを示します。このオプションを設定すると、比較が有効にな り、IBGP ピア (同じ AS 内の BGP ピア) から通知されたルートの中から ルートを選択できます。
現在の RIB 出力エ ントリ	RIB 出力テーブルのエントリ数。
ピーク RIB 出力エ ントリ	任意の一時点で割り当てられた 隣接 RIB 出力ルートのピーク数。

BGP のランタイム の意味 状態

Peer [ピア]タブ

氏名	ピアの名前。
グループ	このピアが属するピア グループの名前。
ローカル IP	仮想ルーターの BGP インターフェイスの IP アドレス。
ピア IP	ピアの IP アドレス。
ピアAS	ピアが属している AS。
パスワード セット	認証が設定されているかどうかが [はい] または [いいえ] で示されます。
ステータス	Active[アクティブ]、Connect[接続]、Established[確立済み]、Idle[待機 中]、OpenConfirm、OpenSentなど、ピアの状態を示します。
状態の期間 (秒)	ピアの状態の期間。

Peer Group [ピア グループ] タブ

グループ名	ピア グループの名前。
タイプ	設定されたピア グループのタイプ (EBGP や IBGP など)。
コンフェデレー ションの集約AS	Aggregate Confederation AS [コンフェデレーション AS の集約] オプ ションが設定されているかどうかが [はい] または [いいえ] で示されま す。
ソフト リセット サポート	ピア グループでソフト リセットがサポートされているかどうかが [は い] または [いいえ] で示されます。BGP ピアに対するルーティング ポリ シーが変更されると、ルーティング テーブルの更新に影響が及ぶ場合 があります。BGP セッションに対しては、ハード リセットよりもソフ ト リセットが優先されます。これは、ソフト リセットでは、BGP セッ ションをクリアせずにルーティング テーブルを更新できるからです。
ネクスト ホップ セルフ	このオプションが設定されているかどうかが [はい] または [いいえ] で示 されます。
次のホップ サード パーティ	このオプションが設定されているかどうかが [はい] または [いいえ] で示 されます。

BGP のランタイム 状態	の意味
プライベート AS の削除	更新が送信される前に、プライベート AS 番号が AS_PATH 属性から削 除されるかどうかを示します。
Local RIB [ローカル	RIB]タブ
プレフィックス	ローカル RIB (Routing Information Base) のネットワーク プレフィックス およびサブネット マスク。
フラグ	* は、ルートが最良の BGP ルートとして選択されたことを示します。
ネクストホップ	プレフィックス方向のネクスト ホップの IP アドレス。
ピア	ピアの名前。
重み	プレフィックスに割り当てられた重み属性。ファイアウォールが同じ プレフィックスへのルートを複数持っている場合は、重みが最も大きい ルートが IP ルーティング テーブルにインストールされます。
ローカル設定.	ルートのローカル設定属性。これは、出口が複数ある場合、プレフィッ クス方向の出口を選択するために使用されます。低いローカル設定より も高いローカル設定が優先されます。
ASパス	プレフィックス ネットワークへのパス内の AS のリスト。このリスト は、BGP 更新で通知されます。
元	プレフィックスの元属性。BGP はどのようにルートについて学習した か。
MED	ルートの MED (Multi-Exit Discriminator) 属性。MED は、ルートのメト リック属性です。これは、ルートを通知する AS によって、外部 AS に 提案されます。高い MED よりも低い MED が優先されます。
フラップ数	ルートのフラップの数。
RIB Out [RIBアウト]タブ	

プレフィックス	RIB (Routing Information Base) のネットワーク ルーティング エントリ。
ネクストホップ	プレフィックス方向のネクスト ホップの IP アドレス。
ピア	仮想ルーターがこのルートを通知するピア。

BGP のランタイム 状態	の意味
ローカル設定.	プレフィックスにアクセスためのローカル設定属性。これは、出口が 複数ある場合、プレフィックス方向の出口を選択するために使用されま す。低いローカル設定よりも高いローカル設定が優先されます。
ASパス	プレフィックス ネットワークへのパス内の AS のリスト。
元	プレフィックスの元属性。BGP はどのようにルートについて学習した か。
MED	プレフィックスに対する MED (Multi-Exit Discriminator) 属性。MED は、ルートのメトリック属性です。これは、ルートを通知する AS に よって、外部 AS に提案されます。高い MED よりも低い MED が優先さ れます。
高度なステータス	ルートの通知状態。
集約ステータス	このルートが他のルートと集約されるかどうかを示します。

[マルチキャスト]タブ

以下の表は、仮想ルーターの IP マルチキャストのランタイム状態を示しています。

マルチキャストの ランタイム状態	の意味
FIBタブ	
グループ	転送情報ベース(FIB)のルートエントリ。仮想ルーターがパケットを

	転送するマルナキャストクルーノアトレス。
送信元	グループのマルチキャストパケットの送信元アドレス。
受信インターフェ イス	グループのマルチキャスト パケットが到着するインターフェイス。
送信インターフェ イス	仮想ルータがグループのマルチキャスト パケットを転送するインター フェイス。

IGMP Interface [IGMPインターフェイス]タブ

インターフェイス	IGMP が有効になっているインターフェイス。
----------	-------------------------

マルチキャストの ランタイム状態	の意味 	
バージョン	仮想ルータ上で実行する IGMP (Internet Group Management Protocol) のバージョン 1、2、または 3。	
クエリ実行者	インターフェイスに接続されたマルチアクセス セグメント上の IGMP ク エリ実行者の IP アドレスです。	
クエリ実行者の アップ タイム	IGMP クエリ実行者がアップしている秒数です。	
クエリ実行者の失 効時間	他のクエリ実行者の現行タイマーが期限切れになるまでの残り秒数。	
頑強性	IGMP インターフェイスの頑強性	
グループ制限	IGMP が同時に処理できるインターフェイス毎の最大グループ数です。	
送信元制限	IGMP が同時に処理できるインターフェイス毎の最大ソース数です。	
すぐに終了	Immediate Leave [すぐに終了] が設定されているかどうかが [はい] ま たは [いいえ] で示されます。Immediate Leave [すぐに終了] を設定する と、インターフェイスに IGMP グループ固有のクエリを送信せずに、仮 想ルーターが転送テーブルからインターフェイスを削除します。	

IGMP Membership [IGMPメンバーシップ]タブ

インターフェイス	グループが所属するインターフェイスの名前。
グループ	インターフェイスが属するマルチキャスト グループのアドレス。
送信元	グループへのマルチキャスト パケットを送信している送信元の IP アド レス。
アップ タイム	メンバーシップがアップしている時間の秒数。
失効時間	メンバーシップが失効するまでの残り時間の秒数です。
フィルタ モード	送信元を許可するか除外します。仮想ルーターを設定し、すべてのトラフィックを許可する、この送信元 (許可) からのトラフィックのみを許可する、またはこの送信元 (除外) を除くすべての送信元からのトラフィックを含めるようにします。
有効期限の除外	インターフェイスの除外状態が期限切れになるまでの残り秒数。

マルチキャストの ランタイム状態	の意味
V1 ホスト タイ	インターフェイスに接続された IP サブネットに IGMP バージョン 1 メ
マー	ンバーが存在しないとローカル ルーターが想定するまでの残り時間。
V2 ホスト タイ	インターフェイスに接続された IP サブネットに IGMP バージョン2 メン
マー	バーが存在しないとローカル ルーターが想定するまでの残り時間。

PIM Group Mapping [PIMグループマッピング]タブ

グループ	ランデブー ポイントにマップされたグループの IP アドレス。
RP	グループのランデブー ポイントの IP アドレス。
元	どこで仮想ルーターが RP について学習したかを示します。
PIM モード	[ASM] または [SSM]。
非アクティブ	グループから RP へのマッピングが非アクティブであるかどうかを示し ます。

PIMインターフェイスタブ

インターフェイス	PIM に参加しているインターフェイスの名前。	
アドレス	インターフェイスの IP アドレス。	
DR	インターフェイスに接続されたマルチアクセス セグメント上の宛先ルー ターの IP アドレスです。	
送信間隔	設定されている Hello 間隔 (秒)	
結合/プルーニン グ間隔	Join および Prune メッセージ用に設定された間隔(秒)です。	
アサート間隔	アサート メッセージを送信するために仮想ルーター用に設定された PIM アサート間隔(秒)です。PIM はアサート メカニズムを使用してマルチ アクセス ネットワーク用の PIM フォワーダーを選出し始めます。	
DR 優先順位	インターフェイスに接続されたマルチアクセス セグメント上の宛先ルー ター用に設定された優先順位です。	
BSR ボーダー	「はい」または「いいえ」は、インターフェイスがエンタープライズ LAN の境界にあるブートストラップ ルーター(BSR)である仮想ルー ターにあるかどうかを示します。	

マルチキャストの の意味 ランタイム状態

PIM Neighbor [PIMネイバー]タブ

インターフェイス	仮想ルーターのインターフェイスの名前です。
アドレス	インターフェイスから到達可能な PIM ネイバーの IP アドレス。
セカンダリ アドレ ス	インターフェイスから到達可能な PIM ネイバーのセカンダリ IP アドレ ス。
アップ タイム	ネイバーがアップしている時間の長さ。
失効時間	仮想ルーターがネイバーから hello パケットを受信していないためにそのネイバーが期限切れになるまでの残り時間の長さ。
生成 ID	ランダムに生成された 32 ビットの値であり、インターフェイス上で PIM フォワーダーが起動あるいは再起動する度(ルーター自体が再起動 する場合を含む)に生成され直します。
DR 優先順位	このネイバーからの最後の PIM hello メッセージで仮想ルーターが受信 した指定ルーターの優先順位。

BFD Summary Information (BFD サマリー情報) タブ

BFD サマリー情報には、以下のデータが含まれます。

BFD サマリー情報 のランタイム状態	の意味
インターフェイス	BFD を実行しているインターフェイス。
PROTOCOL	インターフェイスで BFD を実行しているスタティック ルート(スタ ティック ルートの IP アドレス ファミリー)またはダイナミック ルー ティング プロトコル。
ローカル IP アド レス	BFD を設定したインターフェイスの IP アドレス。
隣接 IP アドレス	BFD ネイバーの IP アドレス。
状態	ローカルおよびリモートBFDピアのBFDの状態:admin down(管理者ダ ウン)、down(ダウン)、init(初期設定)、またはup(アップ)。

BFD サマリー情報 のランタイム状態	の意味	
アップ タイム	BFD のアップタイム(時間、分、秒、ミリ秒)。	
ディスクリミネー タ (ローカル)	ローカル BFD ピアのディスクリミネータ。ディスクリミネータは、複 数の BFD セッションを識別するためにピアで使用されるゼロ以外の一 意の値です。	
ディスクリミネー タ(リモート)	リモート BFD ピアのディスクリミネータ。	
エラー	BFD エラーの数。	
セッションの詳細	Details (詳細) をクリックすると、セッションの BFD 情報 (ローカル およびリモート ネイバーの IP アドレス、最後に受信したリモート診断 コード、送信および受信したコントロール パケットの数、エラーの数、 状態の変化を引き起こした最後のパケットに関する情報など)が表示さ れます。	

More Runtime Stats for a Logical Router (論理ルーターの詳細ラ ンタイム統計情報)

論理ルーターのスタティック ルートまたはルーティング プロトコルを設定した 後、Network(ネットワーク) > 論理ルーターを選択し、最後の列の More Runtime Stats(ラ ンタイム状態の詳細)を選択すると、論理ルーターの詳細情報が表示されます。たとえば、ルー トテーブル、転送テーブル、設定したルーティング プロトコルとスタティック ルートが表示さ れます。このウィンドウで提供される論理ルーターの詳細情報は1画面に収まりません。この ウィンドウには、以下のタブが表示されます。

- Routing (Stats for a Logical Router) (ルーティング、論理ルーターの統計情報)
- BGP (論理ルータの統計情報)

論理ルーターのルーティング統計情報

 Network > Routing > Logical Routers > More Runtime Stats (ネットワーク>ルーティング > 論 理ルータ > その他のランタイム統計)

以下の表は、仮想ルーターのルート テーブル、転送テーブル、スタティック ルートのモニタリ ング テーブルのランタイム統計について示しています。

Runtime Stat(ランタイム統計) の意味

ルート テーブル

Runtime Stat(ランタイム統計)	の意味
アドレス ファミリーの表示	テーブルに表示するアドレスのグループの種類を制御す るには、IPv4 Only(IPv4 のみ)、IPv6 Only(IPv6 の み)、または IPv4 and IPv6(IPv4 および IPv6)(デ フォルト)を選択します。
宛先	論理ルータが到達できるネットワークの IPv4 アドレス およびネットマスクまたは IPv6 アドレスおよびプレ フィックス長。
ネクストホップ	宛先ネットワーク方向のネクスト ホップにあるデバ イスの IP アドレス。ネクスト ホップが 0.0.0.0 の場合 は、デフォルト ルートを表します。
PROTOCOL	ルートがスタティック ルートまたは接続ルートである か等、BGP を通じて取得した情報を示します。
メトリック	ルートのメトリック。ルーティングプロトコルで同一 の宛先ネットワークへの複数のルートが存在する場合、 メトリック値が最も小さいルートが優先されます。各 ルーティングプロトコルは異なるタイプのメトリック を使用します。たとえば、RIP はホップ数を使用しま す。
選択済み	フィールドは、有効化されているとtrue(オン)、有効 化されていない場合は空白のままです。
エイジ	ルーティング テーブルのルート エントリのエイジ。
アクティブ	フィールドは、有効化されているとtrue(オン)、有効 化されていない場合は空白のままです。
インターフェイス	ネクストホップに到達するために使用される論理ルー ターの出力インターフェイス。
レートの	テーブルのランタイム統計を更新する場合にクリックし ます。

転送テーブル

ファイアウォールは最適なルート(ルート テーブル(RIB)から宛先ネットワーク)を選択し、FIB に配置します。

Runtime Stat(ランタイム統計)	の意味
宛先	ルート テーブルから選択された、論理ルーターが到達 できるネットワークの最適な IPv4 アドレスおよびネッ トマスク、または IPv6 およびプレフィックス長です。
ネクストホップ	宛先ネットワーク方向のネクスト ホップにあるデバ イスの IP アドレス。ネクスト ホップが 0.0.0.0 の場合 は、デフォルト ルートを表します。
MTU	最大転送単位(MTU)です。この宛先への TCP パケット1つあたりでファイアウォールが転送する最大バイト 数を示します。
flags	 u – ルートの状態はアップです。 h – ルートはホストに向かいます。 g – ルートはゲートウェイに向かいます。 e – ファイアウォールは等価コストマルチパス (ECMP)を使用してこのルートを選択しています。 * – ルートは、宛先ネットワークに向かう優先パスです。
インターフェイス	ネクスト ホップに到達するために論理ルーターが使用 する出力インターフェイス。

スタティック ルートのモニタリング

宛先	論理ルーターが到達できるネットワークの IPv4 アドレ スおよびネットマスクまたは IPv6 アドレスおよびプレ フィックス長です。
ネクストホップ	宛先ネットワーク方向のネクスト ホップにあるデバ イスの IP アドレス。ネクスト ホップが 0.0.0.0 の場合 は、デフォルト ルートを表します。
メトリック	ルートのメトリック。同一の宛先ネットワークへの複 数のスタティック ルートが存在する場合、ファイア ウォールはメトリック値が最も小さいルートを優先しま す。
インターフェイス	ネクストホップに到達するために使用される論理ルー ターの出力インターフェイス。

Runtime Stat(ランタイム統計)	の意味
パス モニタリング (フェール オン)	このスタティック ルートでパス モニタリングが有効 である場合、Fail On(フェイル オン)は以下を示しま す。
	 All(すべて) – スタティック ルートの監視対象の宛 先がすべてダウンしている場合に、ファイアウォー ルはスタティック ルートがダウンしていると見なし て、フェイルオーバーします。
	 Any(任意) – スタティック ルートの監視対象の 宛先いずれかがダウンしている場合に、ファイア ウォールはスタティック ルートがダウンしていると 見なして、フェイルオーバーします。
	スタティック ルートのパス モニタリングが無効である 場合、Fail On(フェイル オン)は Disabled(無効)を 示します。
ステータス	監視対象の宛先への ICMP ping に基づく静的ルートの ステータス:静的ルートのUp、Down、またはパスの監 視は Disabled (無効)です。
レートの	テーブルのランタイム統計を更新します。

論理ルーターの BGP 統計情報

論理ルーターの BGP のランタイム統計情報を以下の表で示しています。

BGP のランタイム状態	の意味
Summary [サマリー]タブ	
enabled [有効化]	BGP enabled(BGPを有効化する): yes(はい)また はno(いいえ)。
ルーターID	論理ルーターのルーター IDです。
ローカル AS	論理ルーターが所属する ASです。
Enforce First AS(First AS を適 用する)	フィールドは、有効化されているとtrue(オン)、有効化 されていない場合は空白のままです。
高速外部フェイルオーバー	フィールドは、有効化されているとtrue(オン)、有効化 されていない場合は空白のままです。

BGP のランタイム状態	の意味
デフォルト ローカル プレファ レンス	デフォルト ローカル プレファレンスの設定が完了しまし た。
グレースフル リスタート	フィールドは、有効化されているとtrue(オン)、有効化 されていない場合は空白のままです。
最大ピア再起動時間(秒)	グレースフル リスタートの最大ピア再起動時間に設定され た秒数。
ステール ルート時間(秒)	グレースフル リスタートのステール ルート時間に設定さ れた秒数。
常に MED を比較	フィールドは、有効化されているとtrue(オン)、有効化 されていない場合は空白のままです。
決定論的 MED 比較	フィールドは、有効化されているとtrue(オン)、有効化 されていない場合は空白のままです。
Peer [ピア]タブ	
氏名	ピアの名前。
ピア グループ	このピアが属するピア グループの名前。
ローカル IP	論理ルーターの BGP インターフェースの IP アドレス。
ローカル AS	ローカル BGP ファイアーウォールが所属する AS です。
ピア IP	ピアの IP アドレス。
REMOTE AS(リモートAS)	ピアが所属する AS です。
Up/Down(アップ/ダウン)	ピアはUp(アップ)または Down(ダウン)です。
国家	設立
Peer Group [ピア グループ] タブ	

氏名	ピア グループの名前。
タイプ	設定済ピア グループのタイプ (EBGP や IBGP 等)。
キープアライブ(秒)	キープアライブ時間(秒単位)

BGP のランタイム状態	の意味
ホールド タイム(秒)	ホールド タイム(秒単位)
ір	フィールドは、有効化されているとtrue(オン)、有効化 されていない場合は空白のままです。
IPv6	フィールドは、有効化されているとtrue(オン)、有効化 されていない場合は空白のままです。
分 Probe Interval (sec) (秒単位 でのプローブ間隔)	秒単位での最小ルート間隔。
ユニキャスト	フィールドは、有効化されているとtrue(オン)、有効化 されていない場合は空白のままです。
ルーティングする	
氏名	ルーティング テーブルの IPv4 または IPv6 ルート: IPv4 ま たは IPv6 アドレスおよびプレフィックスの長さ。
ASパス	パス上の次の AS。
Best Path(最適経路)	フィールドは、有効化されているとtrue(オン)、有効化 されていない場合は空白のままです。
MED	0または空白
メトリック	0または空白
ネットワーク	
ネクストホップ	ルート(名)として識別されるネットワークに到達するた めのネクストホップ IP アドレス。
元	ルートの発信元:IGP または incomplete(不完全)
path	パスの次のAS。
パスの発信元	外部と表示。
ピア名	
プレフィックス	
プレフィックスの長さ	

BGP のランタイム状態	の意味
有効	フィールドは、有効化されているとtrue(オン)、有効化 されていない場合は空白のままです。
重み	ルートの重みです。

Network(ネットワーク) > Routing(ルーティング) > Logical Routers(論理ルーター)

手動で定義したスタティック ルートを使用するか、レイヤー3のルーティングプロトコルに参加することで他のサブネットへのルートを取得する場合は(ダイナミック ルート)、ファイアウォールに論理ルーターを設定しておく必要があります。ファイアウォールに定義されたレイヤー3インターフェイス、ループバックインターフェイス、および VLAN インターフェイスはそれぞれ、論理ルーターに関連付けられる必要があります。各インターフェイスが所属できるのは、1つの論理ルーターのみです。

論理ルーターは、**Device**(デバイス) > **Setup**(セットアップ) > **Management**(管理) のGeneral Settings(一般設定)でAdvanced Routing(詳細ルーティング)を有効にすると使用 可能になります。次に、コミットしてファイアウォールを再起動します。

論理ルーターを定義するには、ネットワークの必要に応じて、レイヤー3インターフェイスを 論理ルーターに追加し、静的ルートと動的ルーティングプロトコルの任意の組み合わせを構成 する必要があります。ECMP や BFD などの他の機能を構成することもできます。

確認すべき情報	以下を参照
論理ルーターの必須要素	論理ルーター全般設定
設定:	静的ルート
	フィルタ
	OSPF
	OSPF ルーティング プロファイル
	OSPFv3IPv6
	OSPFv3 Routing Profiles (OSPFv3 ルーティング プロ ファイル)
	BGP
	BGP Routing Profiles (BGP ルーティング プロファイル)
	マルチキャスト
	Multicast Routing Profiles (マルチキャストルーティ ングプロファイル)
	RIPv2
	RIPv2 ルーティングプロファイル
	BFD Routing Profiles (BFD ルーティングプロファイ ル)

確認すべき情報	以下を参照
論理ルーターに関する情報を表示し	More Runtime Stats for a Logical Router (論理ルー
ます。	ターの詳細ランタイム統計情報)

Network (ネットワーク) > Routing (ルーティング) > Logical Routers (論理 ルーター) > General (一般)

Advanced Routing (**Device** > セットアップ > 管理) を有効にすると、firewall は静的ルーティン グと動的ルーティングに 論理ルータ を使用します。論理ルーターには、以下の表に示される通 り、ルーター名およびレイヤー3インターフェースを割り当てる必要があります。

オプションで、論理ルーターのEqual Cost Multiple Path (ECMP)を設定することが可能で す。ECMP 処理はネットワーキング機能の一つであり、これを使用すると、ファイアウォール は、同じ宛先に対する等コストのルートを最大4つ使用することができます。この機能を使用 しないときに、同じ宛先に対する等コストのルートが複数ある場合、仮想ルーターは、それらの ルートのいずれかをルーティングテーブルから選択し、その転送テーブルに追加します。選択 したルートが使用不能でない限り、他のルートは使用しません。仮想ルーターで ECMP 機能を 有効にすると、ファイアウォールは、宛先に対する等コストのパスをその転送テーブル内に最大 4つ持つことができ、以下のことが可能になります。

- 複数の等コストリンクでの同じ宛先への負荷分散フロー(セッション)。
- 一部のリンクを未使用のままにせず、同じ宛先に対するすべてのリンクで使用可能な帯域幅 を利用する。
- リンクに障害が発生した場合、同じ宛先に向かう別の ECMP メンバーにトラフィックを動的 に切り替える。ルーティングプロトコルまたは RIB テーブルが代替パス/ルートを選択する のを待つ必要はありません。これにより、リンク障害時のダウン タイムを削減できます。

ECMP 負荷分散は、パケット レベルではなく、セッション レベルで実行されます。 つまり、ファイアウォールは、パケットを受信するたびではなく、新規セッション の開始時に等コストのパスを選択します。

Logical Router General Settings(論理ルーターの一 般設定)	の意味
氏名	論理ルーターを説明する名称を指定します(最大 31 文字)。 名前の大文字と小文字は区別されます。また、一意の名前にす る必要があります。文字、数字、ハイフン、およびアンダース コアのみを使用してください。
インターフェイス	
インターフェイス	論理ルーターに含めるレイヤー3インターフェースを追加し ます。このインターフェースは、論理ルーターのルーティング

Logical Router General Settings(論理ルーターの一 般設定)	の意味
	テーブルでの発信インターフェースとして使用することができ ます。
	インターフェイス タイプを指定する方法については 「Network(ネットワーク) > Interfaces(インターフェイ ス)」を参照してください。
	論理ルータにインタフェースを追加すると、その接続された ルートがグローバル RIB に自動的に追加されます。

管理上の距離

スタティック	範囲は1~255です。デフォルトは10です。
静的 IPv6	範囲は1~255です。デフォルトは10です。
OSPF イントラ エリア	範囲は1~255です。デフォルトは110です。
OSPF インターエリア	範囲は 1 ~ 255 です。デフォルトは 110 です。
OSPF 外部	範囲は 1 ~ 255 です。デフォルトは 110 です。
OSPFv3 イントラエリア	範囲は 1 ~ 255 です。デフォルトは 110 です。
OSPFv3 インターエリア	範囲は 1 ~ 255 です。デフォルトは 110 です。
OSPFv3 外部	範囲は 1 ~ 255 です。デフォルトは 110 です。
内部としての BGP	範囲は1~255です。デフォルトは200です。
外部としての BGP	範囲は 1 ~ 255 です。デフォルトは 20 です。
BGP ローカル ルート	範囲は1~255です。デフォルトは20です。
RIP	範囲は1~255です。デフォルトは120です。

ECMP

Enable [有効化]	論理ルーターのEqual Cost Multiple Path(ECMP)を有効化し ます。
対称リターン	(任意)Symmetric Return[対称リターン] を選択すると、関連 付けられた入力パケットが到着した際と同じインターフェイス から戻りパケットが出力されます。つまり、ファイアウォール

Logical Router General Settings(論理ルーターの一 般設定)	の意味
	は、ECMP インターフェイスではなく、戻りパケットを送信 する入力インターフェイスを使用します。そのため、負荷分散 は、Symmetric Return[対称リターン] の設定でオーバーライド されます。この動作は、サーバーからクライアントに移動する トラフィックに対してのみ発生します。
Strict Source Path(ストリ クト送信元パス)	ファイアウォール出口で発信される IKE および IPSec トラ フィックは、デフォルトで、ECMP ロードバランシング方式 が決定するインターフェースから出力されます。Strict Source Path (ストリクト送信元パス)を有効化して、ファイアウォー ルで発信された IKE および IPSec トラフィックが、確実に IPSec トンネルの送信元 IPアドレスが所属する物理インター フェースから出力される設定にします。ファイアウォールに 同じ宛先への等価コスト パスを提供する複数の ISP がある場 合は、Strict Source Path (ストリクト送信元パス)機能を有 効にします。ISP は通常、Reverse Path Forwarding (RPF、逆 パス フォワーディング)の確認 (または IPアドレス スプー フィングを防ぐ別の確認)を実行して、そのトラフィックが 到着した同じインターフェースから出ていることを確認しま す。ECMPはデフォルトで、(出口インターフェースを選択するた め、ISP が期待する通りでない場合があり、ISP は正当なリター ントラフィックをブロックする可能性があります。このユース ケースでは、Strict Source Path (ストリクト送信元パス)を有 効にして、ファイアウォールが IPSec トンネルの送信元 IPアド レスが属するインターフェースである出口インターフェースを 使用しています。
最大パス	等価パスの最大数を入力します。RIB から FIB にコピーできる、(2、3、または 4)から宛先ネットワークへ。デフォルトは 2です。
Load-Balancing Method 負 荷分散方法	 仮想ルーターで使用するECMP 負荷分散アルゴリズムを以下から1つ選択します。ECMP 負荷分散は、パケットレベルではなく、セッションレベルで実行されます。つまり、ファイアウォール (ECMP) は、パケットを受信するたびではなく、新規セッションの開始時に等コストのパスを選択します。 IP モジュロ - デフォルトでは、仮想ルーターは、このオプションを使用してセッションを負荷分散します。このオプションでは、パケットヘッダーの送信元および宛先 IP アドレスのハッシュを使用して、使用する ECMP ルートを決定します。

Logical Router General Settings(論理ルーターの一 般設定)	の意味
	 IP Hash(IP ハッシュ) –使用する ECMP ルートを決定する IP ハッシュ方法は2通りあります。
	 IP Hash (IP ハッシュ)を選択する場合、デフォルトでは ファイアウォールは送信元 IP アドレスと宛先 IP アドレス のハッシュを使用します。
	 あるいは、Use Source Address Only(送信元アドレスの み使用)(PAN-OS 8.0.3 とそれ以降のリリースで使用可 能)を選択できます。この IP ハッシュ方法は、同じ送信 元 IP アドレスに属するすべてのセッションが常に同じパ スを使用するようにします。
	 オプションで、Use Source/Destination Ports(ソース/宛 先ポートの使用)を選択して、いずれかのハッシュ計算 にポートを含めることができます。負荷分散をさらにラ ンダム化するために、Hash Seed[ハッシュ シード]値(整 数)を入力することもできます。
	 Weighted Round Robin[重み付きラウンドロビン] - このアルゴリズムを使用すると、さまざまなリンクの容量や速度を考慮できます。このアルゴリズムを選択すると、Interface [インターフェイス] ウィンドウが開きます。Add[追加]をクリックし、重み付きラウンドロビングループに含めるInterface[インターフェイス]を選択します。インターフェイスごとに、使用するWeight[重み]を入力します。Weight[重み]は、デフォルトで100に設定されています。重みの範囲は1~255です。特定の等コストのパスの重みが大きくなるほど、その等コストのパスが新規セッションで選択される頻度が高くなります。高速のリンクには、低速のリンクよりも大きな重みを与える必要があります。これにより、一層多くのECMPトラフィックが高速のリンクを通過するようになります。別のインターフェイスと重みを追加するには、Add[追加]を再びクリックします。 Balanced Round Robin[均等ラウンドロビン] - 受信 ECMP hm ションをリンククケイロビン] ー 受信 ECMP
リブフィルター	セッションをリンク主体に均等に力取しより。
	Padiateikutian ルートマップな躍切すてか。 新しいルートマップ
Irv4 - DUr ルートイツノ	を作成して、グローバル RIB に追加される IPv4 BGP ルートを 制御します。デフォルト設定は None (なし) です。
Logical Router General Settings(論理ルーターの一 般設定)	の意味
---	---
IPv4 - OSPFv2 ルート マッ プ	Redistribution 経路マップを選択するか、新しい経路マップを作成して、グローバル RIB に追加される IPv4 OSPFv2 経路を制御します。デフォルト設定は None (なし) です。
IPv4 - スタティック ルート マップ	Redistribution 経路マップを選択するか、新しい経路マップを作成して、グローバル RIB に追加される IPv4 静的経路を制御します。デフォルト設定は None (なし) です。
IPv4 - RIP Route-Map	Redistribution ルートマップを選択するか、新しいルートマップ を作成して、グローバル RIB に追加される RIP ルートを制御し ます。デフォルト設定は None (なし) です。
IPv6 - BGP Route-Map	Redistribution ルートマップを選択するか、新しいルートマップ を作成して、グローバル RIB に追加される IPv6 BGP ルートを 制御します。デフォルト設定は None (なし) です。
IPv6 - OSPFv3 Route-Map	Redistribution 経路マップを選択するか、新しい経路マップを作成して、グローバル RIB に追加される IPv6 OSPFv3 経路を制御します。デフォルト設定は None (なし) です。
IPv6 - Static Route-Map	Redistribution 経路マップを選択するか、新しい経路マップを作成して、グローバル RIB に追加される IPv6 静的経路を制御します。デフォルト設定は None (なし) です。

Network > Routing > Logical Routers > Static [ネットワーク > ルーティング > 論理ルーター > スタティック]

オプションで、Advanced Routing Engine 上の論理ルーターに1つ以上のスタティックルート を追加します。IPv4 または IPv6 を選択し、IPv4 または IPv6 アドレスを使用してルートを追 加します。通常、デフォルトルートの設定 (0.0.0.0/0) が必要です。デフォルト ルートは、論理 ルーターのルーティングテーブルにない宛先に適用されます。

スタティック ルートの設 定	の意味
氏名	スタティックルートの識別に使用する名前を入力します(最大 31文字)。名前の大文字と小文字は区別されます。また、一意の 名前にする必要があります。文字、数字、ハイフン、およびアン ダースコアのみを使用してください。

スタティック ルートの設 定	の意味
宛先	CIDR (Classless Inter-Domain Routing) 表記法でIPアドレス とネットワークマスクを入力します。 <i>ip_address/mask</i> (た とえば、IPv4 の場合は 192.168.2.0/24、IPv4 の場合は 2001:db8::/32)。あるいは、タイプが IP ネットマスクのアドレス オブジェクトを作成できます。
インターフェイス	パケットを宛先に転送する発信インターフェースを選択するか、 ネクストホップ設定を指定するか、その両方を行います。この ルートのネクストホップにルートテーブルのインターフェース を使用するのではなく、ファイアウォールが使用するインター フェースをより厳密に制御するインターフェイスを指定します。 デフォルト設定は None (なし) です。
ネクストホップ	以下のいずれかを選択します。
	 IP Address または IPv6 Address – ネクストホップルーターの / IPv6 アドレスを入力するか、IP Netmask タイプのアドレスオ ブジェクトを選択または作成します。IPv4 の場合は /32、IPv6 の場合は /128 のネットマスクがアドレス オブジェクトに求め られます。IPv6 ネクストホップ アドレスを使用するためには、 (レイヤー 3 インターフェイスの設定を行う際に) Enable IPv6 on the interface (インターフェイスでの IPv6 の有効化) を実行 する必要があります。
	 Next LR - 次の論理ルータを Next Hop にするために選択します。
	• FQDN – Fully Qualified Domain Name を Next Hop として入力 します。
	 Discard[破棄] – この宛先のトラフィックを廃棄する場合に選択 します。
	 None – (既定) ルートにネクストホップがない場合に選択します。例えば、ポイントツーポイント接続の場合はパケットの進行方向が一つだけなので、ネクストホップは不要です。
管理距離	スタティック ルートの管理距離を指定します(範囲は 10 ~ 240 で す。
メトリック	スタティック ルートの有効なメトリックを指定します (範囲は 1 ~ 65,535、デフォルトは 10)。
BFDプロファイル	BFD プロファイルを選択するか、スタティック ルートに適用する 新しいプロファイルを作成します。デフォルトは 0 なし(BFD を無 効にする)0 です。

スタティック ルートの設 定	の意味
パス モニタリング	パスの監視を続行する場合に選択します。
Enable [有効化]	スタティック ルートの パス モニタリングを有効にします。
障害条件	firewall が監視対象パスをダウンし、スタティック ルートをダウン と見なす条件を選択します:
	 Any-(デフォルト)スタティックルートの監視対象の宛先のいずれかが ICMP によって到達不能である場合、firewall は RIB および FIB からスタティックルートを削除し、同じ宛先に向かう次に低いメトリックを持つ動的ルートまたはスタティックルートを FIB に追加します。
	 All – スタティック ルートのすべての監視対象宛先が ICMP に よって到達できない場合、firewall はスタティック ルートを RIB および FIB から削除し、同じ宛先に向かうメトリックが次 に低いダイナミック ルートまたはスタティック ルートを FIB に 追加します。
	All を選択して、監視対象の宛先がメンテナンスのために単にオフ ラインになっている場合に、単一の監視対象宛先がスタティック ルート障害を通知する可能性を回避します。
プリエンプティブ ホー ルド タイム (分)	ダウンしたパス モニターが Up (アップ)状態を維持しなければ ならない分数を入力します。パス モニターがメンバーである監視 対象宛先すべてを評価し、Up (アップ)を維持すると、ファイア ウォールはスタティック ルートを RIB に再インストールします。 リンクがダウンしたりフラッピングしたりせずにタイマーの期間 が過ぎた場合、リンクは安定していると見なされて、パス モニ ターは Up (アップ)を維持できます。また、ファイアウォールは スタティック ルートを RIB に再度追加できます。
	ホールド タイム中にリンクのダウンやフラッピングが発生した 場合、パス モニターはエラーとなります。タイマーはダウンし たモニターが Up (アップ)状態に戻ったときに再度開始しま す。Preemptive Hold Time (プリエンプティブ ホールド タイ ム)が0の場合、パス モニターがアップになると即座にファイア ウォールがスタティック ルートを RIB に再インストールします。 範囲は 1 ~ 1,440、デフォルトは 2 です。
氏名	監視対象の宛先の名前を (最大 31 文字) 追加します。名前の大文 字と小文字は区別されます。また、一意の名前にする必要があり ます。文字、数字、ハイフン、およびアンダースコアのみを使用 してください。

スタティック ルートの設 定	の意味
Enable [有効化]	スタティック ルートのこの特定の宛先のパス モニタリングを有効 化する場合に選択します。ファイアウォールは ICMP Ping をこの 宛先に送信します。
送信元IP	 監視対象宛先に対する ICMP Ping で送信元としてファイアウォールが使用する IP アドレスを選択します。 インターフェイスに複数の IP アドレスがある場合は、1つ選択します。
	 インターフェイスを選択した場合、ファイアウォールはデフォ ルトでインターフェイスに割り当てられている最初の IP アドレ スを使用します。
	 DHCP (DHCP クライアント アドレスを使用) を選択した場合、 ファイアウォールは DHCP がインターフェイスに割り当て たアドレスを使用します。DHCP アドレスを確認するには、 Network (ネットワーク) > Interfaces (インターフェイス) > Ethernet (イーサネット) を選択して、イーサネット インター フェイスの行にある Dynamic DHCP Client (動的 DHCP クライ アント)をクリックします。Dynamic IP Interface Status (動的 IP インターフェイス状態) ウィンドウに IP アドレスが表示され ます。 PPPOE (PPPoE クライアントアドレスを使用)
宛先IP	ファイアウォールがパスを監視する対象の、堅牢で安定した IP ア ドレスまたはアドレス オブジェクトを入力します。モニター対象 の宛先と静的経路宛先は、同じアドレス・ファミリー (IPv4 または IPv6) を使用する必要があります。
Ping Interval (sec) (Ping 間隔(秒))	ICMP ping 間隔を秒単位で指定して、firewall がパスをモニターする頻度 (モニター対象宛先に ping を実行する) を決定します。範囲は1から60です。デフォルトは3です。
Ping 数	監視対象宛先から ICMP Ping パケットが返ってこない場合に、リ ンクがダウンしているとファイアウォールが見なすまでの、ICMP Ping パケットの連続数を指定します。Any (任意) または All (す べて)のエラー条件に基づき、パスモニタリングがエラー状態に なると、ファイアウォールはスタティックルートを RIB から削除 します (範囲は 3 ~ 10、デフォルトは 5)。 たとえば、Ping 間隔が 3 秒で、Ping 数 5 個において Ping が存在
	しない(亘近 15 秒间の间、ファイアワオールは Ping を受信し ていない)場合、パス モニタリングはリンク エラーを検出しま す。パス モニタリングがエラー状態で、ファイアウォールが 15

スタティック ルートの設 定	の意味
	秒の後に Ping を受信した場合、リンクの状態はアップと見なされます。Any(任意)または All(すべて)のエラー条件に基づき、Any(任意)または All(すべて)の監視対象宛先に対するパスモニタリングの状態はアップと見なすことができます。また、プリエンプティブホールドタイムが開始されます。

Network > Routing > Logical Routers > OSPF OSPF [の論理ルー タ>ネットワーク>ルーティング]

この表は、Advanced Routing Engine 上の論理ルータの configure OSPFv2 エリアに対する設定 を示しています。

OSPF 設定	の意味	
Enable [有効化]	論理ルーターの OSPF を有効にします。	
ルーターID	ルータ ID を IPv4 アドレスの形式で入力します。	
BFDプロファイル	OSPF に Bidirectional Forwarding Dectection を適用す る場合は、BFD プロファイルを選択するか、新しいプ ロファイルを作成します。デフォルトは 0 なし(BFD を 無効にする)0 です。	
グローバル一般タイマー	Global Timer プロファイルを選択するか、OSPF に適用 する新しいプロファイルを作成します。	
グローバル インターフェイス タイ マー	OSPF Interface Timer を選択するか、OSPF に適用する 新しい Timer を作成します。	
再配信プロファイル	OSPF 再配布プロファイルを選択するか、新しいプロ ファイルを作成して、IPv4 静的経路、接続経路、IPv4 BGP 経路、または IPv4 デフォルト経路を OSPF リン ク状態データベースに再配布します。	
エリア		
エリア ID	エリア ID で識別されるエリアを x.x.x.x 形式で追加し ます。この識別子を受け入れたネイバーのみが同じエ リアに属します。	
タイプ	·	

OSPF 設定	の意味
認証	Authentication プロファイルを選択するか、新しいプ ロファイルを作成します。
タイプ	OSPF エリアのタイプを選択します。
	 Normal[通常] – 制限はありません。エリアではすべてのタイプのルートを使用できます。
	 Stub[スタブ] – エリアからの出口はありません。エ リア外の目的地に到達するには、トラフィックは他 のエリアに接続する Area Border Router (ABR)を通 過する必要があります。
	 NSSA(Not-So-Stubby-Area):トラフィックは、OSPF ルート以外のルートによってのみエリアを離れるこ とができます。
概要なし	(Stub および NSSA エリアのみ)エリアが Type 3 Summary LSA を受信しないようにし、エリア内のトラ フィックを減らす場合に選択します。
デフォルトの情報の発信元	(NSSA エリアのみ)OSPF がデフォルト経路を発信する ようにする場合に選択します。
メトリック	(NSSA エリアのみ)デフォルトルートのメトリックを入 力します。範囲は 1 ~ 16,777,214 です。デフォルトは 10 です。
Metric-type (メトリック タイプ)	(NSSA エリアのみ) Type 1 または Type 2
ABR	論理ルーターが Area Border ルーターの場合に選択して、次の4つのフィールドを構成できるようにします。
リストのインポート	アクセス リストを選択するか、新しいアクセス リスト を作成して、IPv4 送信元アドレスに基づいてエリアに 入るネットワーク ルートをフィルタリングします。
エクスポートリスト	アクセスリストを選択するか、新しいアクセスリス トを作成して、そのエリアで発信されたネットワーク ルートをフィルタリングし、ルートが他のエリアにア ドバタイズされることを許可または禁止します。
Inbound Filter-List インバウンド フィルタリスト	プレフィックス リストを選択するか、新しいプレ フィックス リストを作成して、エリアに入ってくる

OSPF 設定	の意味
	ネットワーク プレフィックスをフィルタリングしま す。
Outbound Filter-List アウトバウン ドフィルタリスト	プレフィックス リストを選択するか、新しいプレ フィックス リストを作成して、そのエリアで発生し たネットワーク プレフィックスをフィルタリングし、 ルートが他のエリアにアドバタイズされないようにし ます。
IPv4 プレフィックス	(NSSA エリアのみ) ABR が選択され、エリア・タイプ が NSSA の場合、Add は、外部サブネットのグループ を単一のタイプ 7 LSA に要約するための IPv4 接頭部で あり、次にタイプ 5 LSA に変換され、Advertise を選択 するとバックボーンにアドバタイズされます。
範囲	·
IP アドレス/ネットマスク	IP アドレス/ネットマスクを追加します。この範囲に一 致するルーティング情報を持つ Type-3 Summary LSA (リンク状態アドバタイズメント)は、そのエリアにこ の範囲の少なくとも1つのエリア内ネットワーク (つま り、ルーターまたはネットワーク LSA で記述)が含ま れている場合、バックボーンエリアにアナウンスされ ます。
代える	エリアに指定された IP アドレス/ネットマスクからの 少なくとも 1 つのエリア内ネットワークが含まれてい る場合、この IP アドレス/ネットマスクを持つ Type-3 Summary LSA がバックボーンにアナウンスされるよう に、代替 IP アドレス/ネットマスクを入力します。
通知	サブネットに一致する LSA を送信する場合に選択します。

インターフェイス

インターフェイス	エリアに含める各インターフェイスを追加します。
Enable [有効化]	インターフェイスを有効にします。
MTU 無視	隣接関係を確立しようとするときに最大伝送単位 (MTU)の不一致を無視する場合に選択します (デフォ ルトは使用不可です。MTU 一致チェックが行われま す)。RFC 2328 では、インターフェース MTU を「フ ラグメンテーションなしで、関連するインターフェー

OSPF 設定	の意味
	スから送信できる最大の IP データグラムのバイト単位 のサイズ」と定義しています。
Passive	インターフェイスが OSPF パケットを送受信できない ようにする場合に選択します。ただし、インターフェ イスは引き続きリンク状態データベースに含まれま す。インターフェイスをパッシブにすることができま す, 例えば、スイッチに接続する場合, ルータがない場 所で Hello パケットを送信したくないので、.
リンク タイプ	リンクの種類を選択します。
	 Broadcast – インターフェイスを介してアクセス可能なすべてのネイバーは、Ethernet インターフェイスなどのマルチキャスト OSPF Hello メッセージによって自動的に検出されます。
	 p2p(ポイントツーポイント) - ネイバーを自動的に検出します。
	 p2mp(ポイントツーマルチポイント):ネイバーを手動 で定義する必要があります。このインターフェイス を介して到達可能なすべてのネイバーの Neighbor IP アドレスと、各ネイバーの Priority を追加しま す。範囲は 0~255、デフォルトは 1 です。
優先順位	インターフェイスの優先度を入力します。指定ルー タ(DR)またはバックアップ DR(BDR)として選択される ルータの優先順位。範囲は 0 ~ 255 です。デフォルト は 1 です。ゼロが設定されている場合、ルータは DR か BDR として選択されません。
タイマー プロファイル	Timer Profile を選択するか、インターフェイスに適用 する新しいファイルを作成します。このプロファイル は、OSPF に適用された Global Interface Timer プロ ファイルをオーバーライドします。
認証	Authentication Profile を選択するか、インターフェイ スに適用する新しい Profile を作成します。このプロ ファイルは、[タイプ] タブで適用された Authentication プロファイルをオーバーライドします。
BFDプロファイル	BFD プロファイルまたは Inherit-vr-global-setting (既 定) を選択するか、新しい BFD プロファイルを作成す るか、None (BFD を無効にする) を選択します。この

OSPF 設定	の意味	
	プロファイルは、OSPF 用に構成されたプロファイル をオーバーライドします。	
コスト	インターフェイスのコストを指定します。範囲は1~ 65,535 です。デフォルトは10です。	
仮想リンク		
氏名	仮想リンクの名前を入力します。	
Enable [有効化]	仮想リンクを有効にします。	
エリア		
ルーターID		
タイマー プロファイル	Timer Profile を選択するか、仮想リンクに適用する 新しいファイルを作成します。このプロファイル は、OSPF に適用された Global Interface Timer プロ ファイルをオーバーライドします。	
認証	Authentication Profile を選択するか、仮想リンクに適 用する新しいファイルを作成します。このプロファイ ルは、[タイプ] タブで適用された Authentication プロ ファイルをオーバーライドします。	
上級		
rfc-1583 の互換性	OSPF ルーティング テーブル内の自律システム境界 ルータ (ASBR) への 1 つの最適ルートを許可する RFC 1583 との互換性を強制する場合に選択します。デフォ ルトは無効で、OSPF ルーティング テーブルがルー ティング テーブル内の複数の intra-AS パスを維持でき るため、ルーティング ループが防止されます。	
Graceful Restart-Graceful Restartの有効化	論理ルータ用の Enable Graceful Restart ;デフォルトは 有効になっています。	
ヘルパー モードを有効にする	論理ルータ用の Enable Graceful Restart Helper モー ド;デフォルトは有効になっています。	
厳密な LSA チェックを有効化する	Strict LSA Checking の有効化は、ヘルパー ルーターに ヘルパー モードの実行を停止させ、リンク状態通知が ネットワーク トポロジの変更を示している場合、正常	

OSPF 設定	の意味
	な再起動プロセスを停止させます。デフォルトは有効 になっています。
猶予期間 (秒)	firewall がダウンまたは使用不可になった場合に、論 理ルーターが正常な再始動を実行する秒数を指定しま す。範囲は 5 ~ 1,800 です。デフォルトは 120 です。
最大ネイバー再起動時間(秒)	範囲は 5 ~ 1,800 です。デフォルトは 140 です。

Network > Routing > Logical Routers > OSPFv3 [OSPFv3 > の論理 ルーター>ネットワーク>ルーティング]

この表は、Advanced Routing Engine 上の論理ルータの configure OSPFv3 エリアに対する設定 を示しています。

OSPFv3設定	の意味
Enable [有効化]	論理ルーターで OSPFv3 を有効にします。
ルーターID	ルーター ID を IPv6 アドレスの形式で入力し ます。
BFDプロファイル	OSPF に Bidirectional Forwarding Dectection を適用する場合は、BFD プロファイルを選択 するか、新しいプロファイルを作成します。 デフォルトは None (BFD を無効にする) で す。
グローバル一般タイマー	Global Timer プロファイルを選択する か、OSPFv3 に適用する新しいプロファイル を作成します。
グローバル インターフェイス タイマー	OSPFv3 Interface Timer を選択する か、OSPFv3 に適用する新しいものを作成し ます。
再配信プロファイル	OSPFv3 Redistribution プロファイルを選択す るか、新しいプロファイルを作成して、IPv6 静的経路、接続経路、IPv6 BGP 経路、また は IPv6 デフォルト経路を OSPFv3 リンク状 態データベースに再配布します。

エリア

OSPFv3 設定	の意味
エリア ID	Area ID で識別される領域を IPv4 アドレス形 式で追加します。この識別子を受け入れたネ イバーのみが同じエリアに属します。
タイプ	
認証	Authentication プロファイルを選択するか、 新しいプロファイルを作成します。
タイプ	OSPFv3 エリアのタイプを選択します。
	 Normal[通常] – 制限はありません。エリ アではすべてのタイプのルートを使用でき ます。
	 Stub[スタブ] – エリアからの出口はあり ません。エリア外の目的地に到達するに は、トラフィックは他のエリアに接続する Area Border Router (ABR) を通過する必要 があります。
	 NSSA(Not-So-Stubby-Area):トラフィック は、OSPFv3 ルート以外のルートによって のみエリアを離れることができます。
概要なし	(Stub および NSSA のみ)エリアがタイプ 3 Summary LSA を受信しないようにし、エリ ア内のトラフィックを減らす場合に選択しま す。
デフォルトの情報の発信元	(NSSA のみ)OSPFv3 がデフォルト経路を発信 するようにする場合に選択します。
メトリック	(NSSA のみ)デフォルトルートのメトリックを 入力します。範囲は 1 ~ 16,777,214 です。デ フォルトは 10 です。
メトリックの種類	(NSSA のみ) Type 1 または Type 2 を選択し ます。
ABR	論理ルータが Area Border Router (エリア 0 を含む複数のエリアにインタフェースを持つ ルータ) で、次の 4 つのフィールドを設定で きる場合に選択します。

OSPFv3設定	の意味
リストのインポート	アクセスリストを選択するか、新しいアクセ スリストを作成して Type-3 LSA をフィルタ リングします。指定された領域に Type-3 要 約 LSA としてアナウンスされたパスに適用さ れます。
エクスポートリスト	アクセス リストを選択するか、新しいアクセ ス リストを作成して、指定したエリアからの エリア内パスから発信された他のエリアにア ナウンスされた Type-3 サマリー LSA をフィ ルタリングします。
Inbound Filter-List インバウンドフィルタリス ト	プレフィックス リストを選択するか、新しい プレフィックス リストを作成して、エリアに 入ってくる Type-3 サマリー LSA をフィルタ リングします。
Outbound Filter-List アウトバウンドフィルタ リスト	プレフィックス リストを選択するか、新しい プレフィックス リストを作成して、エリアか ら Type-3 サマリー LSA をフィルタリングし ます。
IPv6 プレフィックス	(NSSA のみ) ABR が有効になっている場合 は、IPv6 プレフィックスを追加して外部サブ ネットのグループを 1 つの Type-7 LSA に要 約し、Type-5 LSA に変換され、Advertise を 選択するとバックボーンにアドバタイズされ ます。
範囲	
IPv6 アドレス/ネットマスク	IPv6 アドレス/ネットマスクを追加します。 この範囲に一致するルーティング情報を持つ Type-3 Summary LSA は、エリアにこの範囲 の少なくとも 1 つのエリア内ネットワーク (つまり、ルーターまたはネットワーク LSA で記述) が含まれている場合、バックボーン エリアにアナウンスされます)。
通知	LSA 内の一致するサブネットをバックボー ン領域にアドバタイズする場合に選択しま す。Advertise が No に設定されている場 合、エリア内に存在する一致する intra-area

OSPFv3設定	の意味
	プレフィックスはバックボーン・エリアにア ドバタイズされません。
インターフェイス	·
インターフェイス	エリアに含めるインターフェイスを追加しま す。
Enable [有効化]	インターフェイスを有効にします。
MTU 無視	隣接関係を確立しようとするときに最大伝送 単位 (MTU) の不一致を無視する場合に選択し ます (デフォルトは使用不可です。MTU 一致 チェックが行われます)。
Passive	このインターフェイスから OSPF Hello パ ケットを送信しないようにし、ローカル ルー タがネイバーとの OSPF 隣接関係を作成し ないようにする場合に選択します。ただし、 インターフェイスは引き続きリンク状態デー タベースに含まれます。インターフェイスを パッシブにすることができます,例えば、ス イッチに接続する場合,ルータがない場所で Hello パケットを送信したくないので、.
インスタンス ID	OSPFv3 のインスタンスは1つだけ許可され るため、0に設定したままにしておきます。 デフォルトは0です。
リンク タイプ	リンクの種類を選択します。
	 Broadcast – インターフェイスを介し てアクセス可能なすべてのネイバー は、Ethernet インターフェイスなどの OSPFv3 Hello メッセージをマルチキャス トすることによって自動的に検出されま す。 p2p(ポイントツーポイント) - ネイバーを 自動的に検出します。 p2mp(ポイントツーマルチポイント):ネイ バーを手動で定義する必要があります。こ のインターフェイスを介して到達可能なす べてのネイバーの Neighbor IPv6 アドレス

OSPFv3設定	の意味
	と、各ネイバーの Priority を追加します。 範囲は 0 ~ 255、 デフォルトは 1 です。
優先順位	インターフェイスの優先度を入力します。指 定ルータ(DR)またはバックアップ DR(BDR)と して選択されるルータの優先順位。範囲は 0 ~ 255 です。デフォルトは 1 です。ゼロが設 定されている場合、ルータは DR か BDR と して選択されません。
タイマー プロファイル	Timer Profile を選択するか、インターフェイ スに適用する新しいファイルを作成します。 このプロファイルは、OSPFv3 に適用された Global Interface Timer プロファイルをオー バーライドします。
認証	Authentication Profile を選択するか、イン ターフェイスに適用する新しい Profile を作 成します。このプロファイルは、[タイプ] タ ブで適用された Authentication プロファイル をオーバーライドします。
BFDプロファイル	BFD プロファイルまたは Inherit-vr-global- setting (既定) を選択するか、新しい BFD プ ロファイルを作成するか、None (BFD を無 効にする) を選択します。このプロファイル は、OSPFv3 用に構成されたプロファイルを オーバーライドします。
コスト	インターフェイスのコストを指定します。 範囲は 1 ~ 65,535 です。デフォルトは 10 で す。
仮想リンク	
氏名	ABR にバックボーン・エリアへの物理リンク がない場合は、バックボーン・エリアへの物 理リンクを持つ近隣 ABR (同じエリア内) への 仮想リンクを構成します。仮想リンクの名前 を入力します。
Enable [有効化]	仮想リンクを有効にします。

OSPFv3設定	の意味
エリア	バックボーン エリアへの物理リンクを持つネ イバー ABR があるトランジット エリアを選 択します。
ルーターID	仮想リンクのリモート エンドにあるネイバー ABR の Route ID を入力します。
タイマー プロファイル	Timer Profile を選択するか、仮想リンクに適 用する新しいファイルを作成します。このプ ロファイルは、OSPFv3 に適用された Global Interface Timer プロファイルと、インター フェイスに適用された OSPFv3 インターフェ イス タイマー プロファイルをオーバーライ ドします。
認証	Authentication Profile を選択するか、仮想リ ンクに適用する新しいファイルを作成しま す。このプロファイルは、[Type] タブに適 用された Authentication プロファイルとイン ターフェイスに適用された Authentication プ ロファイルをオーバーライドします。
上級	
R ビットと v6 ビットを無効にする	この論理ルータから送信されたルータ LSA の R-bit および V6-bit をクリアして、firewall が アクティブでないことを示す場合に選択しま す。この状態の場合、firewall は OSPFv3 に 参加しますが、転送トラフィックまたは IPv6 データグラムは送信しません。この状態で も、ローカルトラフィックは引き続きファイ アウォールに転送されます。トラフィックを デバイス周辺に再ルーティングしながらその ファイアウォールにも到達できるため、これ はデュアルホームネットワークで保守を行う 場合に役立ちます。RFC 5340 を参照してく ださい。
Graceful Restart- Graceful Restartを有効にす る	論理ルータ用の Enable Graceful Restart ;デ フォルトは有効になっています。
ヘルパー モードを有効にする	論理ルータ用の Enable Graceful Restart Helper モード;デフォルトは有効になってい ます。

OSPFv3 設定	の意味
厳密な LSA チェックを有効化する	有効にすると、ヘルパー ルーターがヘルパー モードの実行を停止し、リンク状態通知が ネットワーク トポロジの変更を示している場 合に正常な再起動プロセスを停止させます。 デフォルトは有効になっています。
猶予期間 (秒)	firewall がダウンまたは使用不可になった場合に論理ルーターが正常な再始動を実行する 秒数を入力します。範囲は 5 ~ 1,800 です。 デフォルトは 120 です。
最大ネイバー再起動時間(秒)	論理ルータが Helper Mode にあるときに、 論理ルータがネイバーから受け入れる Grace Period の秒数を入力します。範囲は 5 ~ 1,800 です。デフォルトは 140 です。

Network > Routing > Logical Routers > RIPv2 [論理ルーター>ネットワーク>ルーティング > RIPv2]

この表は、Advanced Routing Engine 上の論理ルータの configure RIPv2 インターフェイスに対する設定を示しています。

RIPv2 設定	の意味
Enable [有効化]	論理ルーターの RIPv2 を有効にします。
default-information originate	デフォルトルートがルーティング エンジンの RIB に存在しない場合でも、そのルートをア ドバタイズします。
BFDプロファイル	Bidirectional Forwarding Detection (BFD) プ ロファイルを RIPv2 に適用します。デフォル ト設定は None (なし) です。
グローバル一般タイマー	RIPv2 Global Timer Profile を選択し て、Update Interval、Expire Interval、および Delete Interval を設定します。デフォルト設 定は None (なし) です。
認証プロファイル	RIPv2 Authentication Profile を選択し て、MD5 または単純パスワード認証を適用

RIPv2 設定	の意味
	します。デフォルト設定は None (なし) で す。
再配信プロファイル	RIPv2 Redistribution Profile を選択し て、IPv4 静的経路、コネクティド経路、BGP AFI IPv4 経路、または OSPFv2 経路を RIPv2 に再配布します。デフォルト設定は None (な し) です。
グローバルインバウンド配布リスト	配布リストを選択して、受け入れる着信経路 を制御します。デフォルトは None です。
グローバル送信配布リスト	配布リストを選択して、RIP ネイバーにアド バタイズするルートを制御します。デフォル ト設定は None (なし) です。
インターフェイス	RIPv2 ルーティングに参加できるインター フェイスを追加します。
Enable [有効化]	インターフェイスで RIPv2 を使用できるよう にします。
スプリットホライズン	以下のいずれかを選択します。
	 split-horizon - ルートを受信したのと同じ インターフェイスでルートをアドバタイズ しません。
	 no-split-horizon – スプリット ホライズン を無効にします。
	 no-split-horizon-with-poison-reverse – ア ドバタイズメントを受信したのと同じイン ターフェイスに戻すことを許可し、これら のルートのメトリックを RIP で許可される 最大値 (16) に設定します。
モード	インターフェイスのモードを選択します。
	 active – インターフェイスはネットワー クをアドバタイズし、RIP 更新を送信しま す。
	 passive – インターフェイスはネットワー クをアドバタイズしますが、RIP 更新は 送信しません。(ネットワークに RIP ルー ターがないため、インターフェイスで RIP

RIPv2 設定	の意味
	更新を送信する理由がない場合に便利で す。
	 send-only – firewall がエンドノード で、RIP にプレフィックスをアドバタイ ズするだけで、スタティック ルートまた はデフォルト ルートを使用して外部プレ フィックスに到達する場合に使用できま す。
認証	論理ルーター・レベルで適用したプ ロファイルをオーバーライドする場合 は、Authentication プロファイルを選択しま す。
BFDプロファイル	デフォルトでは、インターフェースは RIPv2 の論理ルーターに適用した BFD プロファ イルを継承します。あるいは、別の BFD プロファイルを選択するか (論理ルータの RIPv2 に対して BFD が無効になっていない限 り)、None (BFD を使用不可にする) を選択し てインターフェースの BFD を使用不可にし ます。
Interface Inbound Distribute List—Access-List インターフェイス インバウンド配布リスト - アクセスリスト	アクセス リストを選択して、このインター フェイスに来るルートを制御します。
Interface Inbound Distribute List-Metric イン ターフェイス インバウンド配布リスト - メト リック	着信経路に適用するメトリックを指定します。範囲は1~16です。
Interface Outbound Distribute List—Access- List インターフェイス アウトバウンド配布リ スト - アクセス リスト	このインターフェイスを RIP ネイバーにアド バタイズするルートを制御するアクセス リス トを選択します。
Interface Outbound Distribute List—Metric イ ンターフェイス アウトバウンド配布リスト - メトリック	アドバタイズされたルートに適用するメト リックを指定します。範囲は 1 ~ 16 です。

Network > Routing > Logical Routers > BGP [ネットワーク>ルー ティング > 論理ルータ> BGP]

この表では、Advanced Routing Engine 上の論理ルーターの構成 BGP、ピア グループ、ピア、 ネットワーク、再配布ポリシー、および集約ルートの設定について説明します。

BGP 設定	詳説
 一般	
有効化	論理ルーター用 BGP の有効化
ルーターID	Router ID (ルーター ID) を論理ルーター用の BGP に割り当てます (通常、ルーター ID が一意となるIPv4 アドレスを指定します)。
ローカル AS	ルーター ID に基づき、論理ルーターが所属するローカルの AS を割 り当てます(2バイトまたは4バイトの AS 番号は 1~4,294,967,295 の範囲)。
グローバル BFD プロ ファイル	BFD プロファイルを選択するか、BGP にグローバルに適用する新し い BFD プロファイルを作成します。デフォルトは 0 なし(BFD を無 効にする)0 です。
ルートのインストール	学習した BGP ルートをグローバル ルーティング テーブルにインス トールする場合に選択します。デフォルトは無効です。
高速フェールオーバー	選択すると、BGP は、保留時間の期限が切れるのを待たずに、隣接 するピアへのリンクがダウンした場合に、そのピアとのセッション を終了します。EBGP の高速フェイルオーバーはデフォルトで有効 化されています。ファイアウォールが BGP ルーティングを不必要に 撤回する原因となる場合は、EBGP 高速フェイルオーバーを無効化 します。
グレースフル シャッ トダウン	BGP が RFC 8326 に基づく代替パスを選択して伝搬できるように、 保守操作中に BGP が eBGP ピアリング リンクの優先順位を下げる ように選択します。デフォルトは無効です。
ECMP の複数の AS の サポート	ECMP を設定し、複数の BGP AS で ECMP を実行する場合は有効化 します。
First AS を適用	AS_PATH 属性の最初の AS として EBGP ピアの各自の AS 番号を リストしていない EBGP ピアからの受信更新メッセージをファイア ウォールにドロップさせることを選択します。(デフォルトで有効 化されています。)
デフォルト ローカル プレファレンス	同じ宛先への異なるパス間の優先度を決定するために使用できる デフォルトのローカルプリファレンス値を指定します。範囲は 0 ~ 4,294,967,295 です。デフォルトは 100 です。
グレースフル リス タート – 有効化	BGPの正常な再起動を有効にして、BGPの再起動中にパケット転送が中断されないようにします (デフォルトは有効になっています)。

BGP 設定	詳説
ステール ルート時間 (秒)	ルートが膠着状態を持続可能な時間を指定します(範囲は 1~3600 秒、デフォルトは 120 秒)。
最大ピア再起動時間 (秒)	ローカル デバイスがグレース ピリオド中のピア デバイスの再起動 時間として許容する時間の最大長を秒単位で指定します(範囲は 1 ~ 3600、デフォルトは 120 秒)。
ローカル再起動時刻	ローカル装置が再始動を待機する時間を秒単位で指定します。範囲 は 1 ~ 3,600 です。デフォルトは 120 です。この値はピアにアドバ タイズされます。
パス選択 – 常に MED を比較	別の AS 内のネイバーから受け取ったパスを選択するには、この比較を有効化します。デフォルトは「無効化」です。MED(multi exit discriminator)オプションは、ネイバーに AS への優先パスを通知する外部メトリックです。低い値が高い値に優先されます。
決定論的 MED 比較	iBGP ピア(同じ AS 内の BGP ピア)がアドバタイズしたルートから 選択することを選びます。デフォルトで有効になっています。
ピア グループ	
名前	BGP ピア グループを名前で追加します (最大 63 文字)。名前は、 英数字、アンダースコア (_)、ハイフン (-)、またはドット (.) で始ま り、0 個以上の英数字、アンダースコア (_)、ハイフン (-)、ドットを 含む必要があります。スペースは使用できません。この名前は、論 理ルーター内およびすべての論理ルーターで固有でなければなりま せん。
有効化	ピアグループを [Enable(有効化)] します。
タイプ	ピアグループのタイプを IBGP(内部 BGP、AS 内のピアリング)、 または EBGP(外部BGP-2つの AS 間のピアリング)と選択しま す。
IPv4 アドレス ファミ リ	AFI IPv4 プロファイルを選択または作成して、プロファイル内の設 定をピア・グループに適用します。デフォルトは Noneです。
IPv6アドレスファミ リ	AFI IPv6 プロファイルを選択または作成して、プロファイル内の設 定をピア・グループに適用します。デフォルトは None です。
IPv4 フィルタリング プロファイル	BGP Filtering Profile (IPv4 AFI の場合) のエレメントをピア・グルー プに適用します。デフォルトは None です。

BGP 設定	詳説
IPv6 フィルタリング プロファイル	BGP Filtering Profile (IPv6 AFI の場合) の要素をピア グループに適用 します。デフォルトは None です。
認証プロファイル	Authentication プロファイルを選択または作成して、ピア グループ 内の BGP ピア間の MD5 認証を制御します。デフォルトは None で す。
タイマー プロファイ ル	ピアグループに適用するBGPタイマープロファイルを選択または作 成します。デフォルトは None です。タイマーは、ルートをアドバ タイズするキープアライブおよび更新メッセージに影響します。
マルチ ホップ	IP ヘッダーのtime-to-live (Time-To-Live - TTL) 値を設定します。 範囲は 0 ~ 255 です。0 に設定すると、デフォルト値が使用されま す。EBGP の場合は 1、IBGP の場合は 255 を指定します。
Dampening プロファ イル	Dampening プロファイル を選択または作成して、フラッピング ルートが安定するまで使用しないようにペナルティを科す方法を決 定します。デフォルト設定は None (なし) です。
ピア	
名前	最大 63 文字を含む BGP ピアを名前で追加します。名前は、英数 字、アンダースコア (_)、ハイフン (-)、またはドット (.) で始まり、0 個以上の英数字、アンダースコア (_)、ハイフン (-)、ドットを含む必 要があります。スペースは使用できません。この名前は、論理ルー ター内およびすべての論理ルーターで固有でなければなりません。
有効化	BGP ピアを有効化します。
Passive	ピアが近隣とのセッションを開始できないようにする場合に選択し ます。デフォルトは無効です。
ピア AS	ピアの所属先となる AS を入力します。範囲は 1から4,294,967,295 です。
ピア-アドレス指定	
継承	• Yes - (デフォルト) ピアがピア グループから AFI および後続の AFI

継承	 Yes - (デフォルト) ピアがピア グループから AFI および後続の AFI (SAFI) 構成を継承する場合に選択します。 No - ピアに適用する AFI プロファイルと Filtering プロファイルを 作成して、ピア グループ設定を上書きする場合に選択します。
ローカル アドレス –	BGP 設定中の [Layer 3 Interface(レイヤー3 インターフェイス)]
インターフェイス	を選択します。静的 IPアドレスで構成されたインターフェースと

BGP 設定	詳説
	DHCP クライアントとして構成されたインターフェースが選択可 能です。DHCP がアドレスを割り当てるインターフェースを選択す ると、IPアドレスは None(なし)と表示されます。このインター フェースには DHCP が後で IPアドレスを割り当てます。論理ルー ターの More Runtime Stats(ランタイム統計詳細)を表示すると、 アドレスを確認することができます。
IP アドレス	インターフェースに複数の IP アドレスが存在する場合は、使用する IPアドレスとネットマスクを入力します。
ピア アドレス - タイ プ	IP または FQDN を選択し、ピアの IP アドレスまたは FQDN を入力 します。
IPv4 アドレス ファミ リ	((Available if Inherit No) の場合は使用可能) デフォルト プロファイ ルを選択するか、AFI IPv4 プロファイルを作成してプロファイルの 設定をピアに適用するか、継承 (Peer-Group から継承)を選択しま す<デフォルトは none (IPv4 AFI を無効にする) です。
IPv6アドレスファミ リ	(Available if Inherit No)の場合に使用可能}) AFI IPv6 プロファイルを 選択または作成してプロファイルの設定をピアに適用するか、継承 (Peer-Group から継承)>2} を選択します を選択します。デフォルト は none (IPv6 AFI を無効にする) です。
IPv4 フィルタリング プロファイル	((Available if Inherit No) の場合は使用可能) Unicast または Multicast フィルタリング用の IPv4 AFI を指定する BGP Filtering Profile を選 択または作成し、ピアに適用します。または、継承 (Peer-Group か ら継承) を選択します。デフォルトは none (IPv4 Filtering を無効に する) です。
IPv6 フィルタリング プロファイル	((Available if Inherit No) の場合は使用可能) IPv6 AFI およびUnicastを 指定する BGP Filtering Profile を選択または作成し、ピアに適用しま す。または、継承 (Peer-Group から継承) を選択します。デフォルト は none (IPv6 フィルタリングを無効にする) です。

Peer-Connection Options(ピア-接続オプション) この設定により、ピアが所属するピア グループに構成した設定と同じオプションが上書きされます。

認証プロファイル	認証プロファイルを選択または作成します。デフォルトは inherit (Inherit from Peer-Group) で、これによりピアはピア・グループに指 定された Auth プロファイルを使用します。
タイマー プロファイ ル	タイマープロファイルを選択または作成します。デフォルト設定は inherit (Inherit from Peer-Group で、ピアはピア・グループに指定 された Timer Profile を使用します。

BGP 設定	詳説
マルチ ホップ	IP ヘッダーに TTL 値を指定します。範囲は 0 ~ 255 です。デフォル トは inherit (Peer-Group から継承) です。
Dampening プロファ イル	Dampening Profile を選択または作成します。このファイルで、フ ラッピング ルートが安定するまで使用しないようにペナルティを科 す方法を決定します。デフォルトは inherit (Peer-Group から継承) で、ピアはピア グループに指定された Dampening Profile を使用し ます。

Peer-Advanced(ピアー詳細)

送信側ループ検出の有 効化	ファイアウォールがアップデートでルートを送信する前に、BGP RIB でルートの AS_PATH 属性をチェックして、相手の AS 番号が AS_PATH リストにないことを確認する場合に選択します。ピアの AS 番号が AS_PATH リストにある場合、ファイアウォールはルート をアドバタイズしません。通常、受信側はループを検出しますが、 この最適化機能では送信側がループ検出を行います。受信機にルー プ検出を実行させるには、この機能を無効にします。
BFDプロファイル	ピアに適用する BFD プロファイルを選択または作成するか、ピアの None (BFD を無効にする) を選択します。デフォルトは Inherit-vr- global-setting (Inherit Protocol's Global BFD Profile) です。

常にネットワーク ルートをアドバタイズ する	設定済みのネットワーク ルートを、到達可能かどうかに関係な く、BGP ピアに常にアドバタイズする場合に選択します。この チェックを外すと、firewall はローカルルートテーブルを使用して解 決された場合にのみネットワークルートをアドバタイズします。デ フォルトで有効になっています。
IPv4 / IPv6	IPv4 または IPv6 を選択して、ネットワーク プレフィックスの種類 を指定します。
ネットワーク	Add 対応する IPv4 または IPv6 ネットワーク アドレス。一致する ネットワーク アドレスを持つサブネットは、論理ルータの BGP ピ アにアドバタイズされます。
ユニキャスト	一致するルートをすべての BGP ピアの Unicast (ユニキャスト) ルーティング テーブルにインストールする場合に選択します。
マルチキャスト	(IPv4 のみ)すべての BGP ピアの Multicast ルーティング テーブルに 一致するルートをインストールする場合に選択します。

BGP 設定	詳説
バックドア	(IPv4 のみ)iBGP 接続 (OSPF など) に変更される可能性のある IGP 接続に対して選択して、BGP が AS の外部にプレフィックスをアドバタイズしないようにし、代わりにルートを AS 内に保持します。内部的には、プレフィックスのアドミニストレーティブ ディスタンスが延長され、プレフィックスは優先されませんが、他の場所でリンク障害が発生した場合に必要になった場合でも使用できます。
再配信	
IPv4 再配布プロファ イル	BGP Redistribution Profile (IPv4 AFI を指定する) を選択または作成して、静的経路、接続経路、または OSPF 経路の任意の組み合わせを BGP に再配布します。デフォルト設定は None (なし) です。
IPv6 再配布プロファ イル	BGP Redistribution Profile (IPv6 AFI を指定する) を選択または作成して、静的経路、接続経路、または OSPFv3 経路の任意の組み合わせを BGP に再配布します。デフォルト設定は None (なし) です。
集約ルート	
名前	集約経路ポリシーを名前で追加します。
詳説	集約経路ポリシーの有用な説明を入力します。
有効化	集約経路ポリシーを使用可能にする場合に選択します。デフォルト で有効になっています。
概要のみ	 Summary Prefix のみを近隣ユーザーにアドバタイズし、要約された ルートにはアドバタイズしない場合に選択します。これにより、ト ラフィックが減少し、ネイバーのルーティングテーブルのサイズが 不必要に増加するのが回避されます (デフォルトは無効です)。集約 ルートと集約ルートを構成する個々のルートの両方をアドバタイズ する場合は、チェックを外したままにします。 Summary Only と Suppress Map は相互に排他的です。 両方を指定することはできません。 Summary Only を使用するが、個々のルートをアドバタ イズする場合は、個々のルートに一致する Unsuppress
	Map ルートマップを含む BGP Filtering Profile を作成します。
AS セット	速択すると、果約ルートを構成する AS 番号のリストを含むプレ フィックスがアドバタイズされます。(デフォルトは無効です。)

BGP 設定	詳説
同じ MED のみを集計 する	同じ Multi-Exit Discriminator (MED) 値を持つルートのみを集約する 場合に選択します。デフォルトは有効になっています。
タイプ	集約ルートのタイプを選択します。IPv4あるいは IPv6
概要プレフィックス	要約する経路を計算し、IP アドレス/ネットマスクまたはアドレス・ オブジェクトを指定して、それらの経路にまたがる Summary Prefix を入力します。
マップを抑制	 ルートマップを選択するか、新しいルートを作成して、個々のルートが集約されないようにします。デフォルトは None です。 卸制ルートマップの目的は、特定のルートがアドバタイズメントに集約されないようにすることです。したがって、ルートマップでは、permit は、集約されないように抑制するルートです (deny は集計されないよう に抑制します)。 Summary Only と Suppress Map は相互に排他的です。 両方を指定することはできません。
属性マップ	Summary Prefix の属性情報を設定するには、BGP ルート マップを 選択するか、新しいルート マップを作成します。一致条件を許可し ません。デフォルトは None で、この場合、Summary Prefix にはデ フォルトの属性があります。

Network > Routing > Logical Routers > Multicast [ネットワーク> ルーティング > 論理ルーター> マルチキャスト]

次の表に、Advanced Routing Engine 上の論理ルータの IPv4 マルチキャストを設定するための設 定を示します。

IPv4 Multicast Settings (IPv4 マルチキャスト設定)	詳説
マルチキャストプロトコ	論理ルータのマルチキャストプロトコルを有効にする場合に選択
ルを有効にする	します。

スタティック

名前

Add mroute の名前 (最大 31 文字)。名前は、英数字、アンダース コア (_)、またはハイフン (-) で始まり、0 個以上の英数字、アン

IPv4 Multicast Settings (IPv4 マルチキャスト設定)	詳説
	ダースコア (_)、またはハイフン (-) を含む必要があります。ドッ ト (.) またはスペースは使用できません。
宛先	RPF チェックを行うマルチキャスト・ソースである宛先 (IPv4 ア ドレス/マスク) を入力します。
インターフェイス	マルチキャスト ソースへのユニキャスト ルートの出力インター フェイスを選択します。
ネクストホップ	送信元に向かうネクストホップの IPv4 アドレスを入力します。
優先	mroute のプリファレンスを入力します。範囲は 1 ~ 255 です。

PIM - General PIM-一般

有効化	PIM を有効にします。
RPF Lookup Mode (RPF ルックアップ モード)	Reverse-Path Forwarding (RPF) ルックアップモードを選択して、 論理ルータがマルチキャストパケットに含まれる送信元アドレ スに到達する発信インターフェイスを検索する場所を決定しま す。RIB に格納されている発信インターフェイスがマルチキャス トパケットが到着したインターフェイスと一致する場合、論理 ルータはパケットを受け入れて転送します。それ以外の場合は、 パケットをドロップします。
	 mrib-then-urib – 最初にマルチキャスト RIB を調べ、次にユニ キャスト RIB を調べます。
	• mrib-only - マルチキャスト RIB のみを検索します。
	• urib-only - ユニキャスト RIB のみを検索します。
インターフェイス一般タ イマー	インターフェイスタイマープロファイルを選択するか、新しいプ ロファイルを作成します。
ルートのエイジアウト秒 数	マルチキャスト・グループとソースの間のセッション終了後にマ ルチキャスト経路がmRIBに残る秒数を指定してください。範囲は 210~7,200です。デフォルトは 210 です。
マルチキャスト SSM 範 囲	Source-Specific Multicast (SSM) を設定するには、マルチキャスト トラフィックを受信側に配信するために許可される送信元アドレ スを指定するプレフィックスリストを選択します。デフォルトは None (プレフィックスリストなし) です。
グループアドレス	マルチキャスト・グループまたは接頭部の Shortest-Path Tree (SPT) しきい値を構成するには、接頭部リストを選択するか、新

IPv4 Multicast Settings (IPv4 マルチキャスト設定)	詳説
	規作成することによって、 Add をグループ・アドレス (配布ツ リーを指定するマルチキャスト・グループまたは接頭部) にしま す。
しきい値	グループまたは接頭部の SPT しきい値を指定します。
	 0 (switch on first data packet) - (デフォルト) 論理ルータは、 グループ/プレフィックスの最初のデータ パケットを受信する と、グループ/プレフィックスの共有ツリーから SPT に切り替 わります。
	 ・論理ルータがそのマルチキャストグループ/プレフィックス のSPT 配布に切り替える任意のインターフェイスで、任意の 期間にわたってマルチキャストグループ/プレフィックスに 到達できるキロビット/秒の合計数を入力します。範囲は0~ 4,294,967,295です。
	 never (SPT に切り替えない) – PIM ルーターは引き続き共有ツ リーを使用して、マルチキャスト グループ/プレフィックスに パケットを転送します。
グループ許可	
ソース グループリスト	特定の送信元からのマルチキャストパケットやマルチキャストパ ケットを特定の宛先マルチキャストグループに許可して論理ルー タを通過させるには、アクセスリストを選択します。デフォルト は None (アクセス リストなし) で、特定のソース グループまたは マルチキャスト グループが PIM グループのアクセス許可の対象 にならないことを意味します。
PIM-インターフェイス	
名前	インターフェースの名前を入力します (最大 31 文字)。名前は、 英数字、アンダースコア (_)、またはハイフン (-) で始まり、0 個 以上の英数字、アンダースコア (_)、またはハイフン (-) を含む必 要があります。ドット (.) またはスペースは使用できません。
詳説	インターフェイスの説明を入力します。

インターフェイスの Designated Router 優先度を指定して、PIM 参加メッセージ、PIM レジスタ メッセージ、およびプルーニン
クメッセーンをRendezvous Point (RP) に転送9 るルータを制
御します。範囲は1~4,294,967,295 です。デフォルトは1で
す。LAN 上の PIM デバイスのうち、DR 優先度が設定されている
場合、優先度が最も高いデバイスが DR として選択されます。

IPv4 Multicast Settings (IPv4 マルチキャスト設定)	詳説
送信 Bsm	Bootstrap Messages の伝搬を許可する場合に選択します (デフォルトで有効)。
タイマー プロファイル	インターフェイスのタイマー プロファイルは、インターフェイス のタイマー プロファイルを選択してオーバーライドしない限り、 一般 PIM セクションから継承されます。デフォルトは None で す。
ネイバー フィルタ	アクセス リストを使用して、論理ルータの PIM ネイバーになる ことを許可または拒否するデバイスのプレフィックスを指定しま す。デフォルトは None (no access list) です。
PIM - Rendezvous Point	
RP タイプ	静的 RP および/または候補 RP を設定します。それらは相互に排 他的ではありません。
	 Static RP - マルチキャスト グループへの RP の静的マッピン グを確立します。PIM ドメイン内の他の PIM ルータで同じ RP を明示的に設定する必要があります。 RP 候補 なし
インターフェイス	RP がマルチキャスト パケットを送受信する RP インターフェ イスを選択します。有効なインターフェイス タイプは La1yer3 インターフェイス(Ethernet、ループバック、VLAN、Aggregate Ethernet (AE)、トンネル、およびサブインターフェイスを含む)で す。
アドレス	インターフェイスのアドレス/プレフィックスの長さを選択しま す。選択した RP インターフェイスの IP アドレスがリストに入力 されます。
同じグループの学習済み RP を上書きする	(Static RP only)この静的 RP を RP として機能させる場合に選択し ます(Group List のグループに対して選択された RP の代わりに)。
Group List (グループリス ト)	アクセス リストを選択または作成して、静的 RP が RP として 機能するマルチキャスト グループを指定します。デフォルトは None (no access list) です。
優先順位	(Candidate RP のみ)候補 RP の優先順位を指定します。範囲は 0 ~ 255 です。デフォルトは 192 です。優先順位の値が低いほど、優 先順位が高いことを示します。

IPv4 Multicast Settings (IPv4 マルチキャスト設定)	詳説
広告間隔	(Candidate RP のみ)候補 RP が他のルーターにアドバタイズメン トを送信する頻度(秒単位)を指定します。範囲は 1 から 26,214 で す。デフォルトは 60 です。
IPv4 アドレス	Add インターフェイスの IPv4 Address を選択してインターフェ イスを作成します。
Group List (グループリス ト)	候補 RP が受け入れるグループを制御するには、IPv4 アクセス リ ストであるグループ リストを選択または作成します。デフォルト は None (no access list) です。アクセス リストが適用されない場 合、論理ルータはすべてのグループの RP としてアドバタイズを 開始します。
オーバーライド	Group List のグループに対して動的に学習(選択)される RP ではな く、静的に設定したリモート RP を RP として機能させる場合に 選択します。デフォルトは無効です。
IGMP	
IGMP を有効にする	IGMP を有効にします。
動的	
インターフェイス	Add インターフェイス。
バージョン	IGMP バージョン2または3を選択します。
頑強性	 ロバスト性の値を選択します。範囲は1から7です。デフォルトは2です。ファイアウォールが位置するサブネットがパケットを紛失しやすい場合はこの値を増加させます。 (Robustness * QueryInterval) + MaxQueryResponseTimeは、結合メッセージが論理ルータで有効である期間を決定します。論理ルータがグループ離脱メッセージを受信した場合、Robustness * LastMemberQueryIntervalは、論理ルータがグループ離脱エントリを削除する前に待機する時間の長さです。結合メッセージの場合、ロ
	バスト性の値1は無視されます。Leave Group メッ セージの場合、論理ルータは Robustness 値を Last Member Query Count としても使用します。

IPv4 Multicast Settings (IPv4 マルチキャスト設定)	詳説
Group Filter グループ フィルター	アクセス リストを選択または作成して、ダイナミック IGMP を 使用するプレフィックスを制御します。デフォルトは None (no access list) です。
Max Groups 最大グルー プ	IGMP がインターフェイスに対して同時に処理できるグループ の最大数を入力します。範囲は 1 ~ 65,525 です。デフォルトは unlimited で、これは範囲内の最高値を意味します。
Max Sources 最大ソース	IGMP がインターフェイスに対して同時に処理できるソースの 最大数を入力します。範囲は 1 ~ 65,525 です。デフォルトは unlimited で、これは範囲内の最高値を意味します。
クエリ プロファイル	作成した IGMP Interface Query Profile を選択するか、インター フェイスに適用する新しいファイルを作成します。
Router Alert オプション のない IGMP パケットの ドロップ	着信 IGMPv2 または IGMPv3 パケットに IP Router Alert オプション、RFC 2113 がないか、ドロップされるように要求する場合に 選択します。デフォルトは無効です。

スタティック

名前	Add 静的 IGMP インターフェイスを名前で指定します (最大 31 文 字)。名前は、英数字、アンダースコア (_)、またはハイフン (-) で 始まり、0 個以上の英数字、アンダースコア (_)、またはハイフン (-) を含む必要があります。ドット (.) またはスペースは使用でき ません。
インターフェイス	スタティック IGMP インターフェイスにするインターフェイスを 選択します。
グループアドレス	スタティック IGMP メンバーのマルチキャスト・グループ・アド レスを入力します。
送信元アドレス	スタティック IGMP メンバーがマルチキャストを受信する送信元 アドレスを入力します。

MSDP - 一般

有効化	論理ルータのマルチキャスト送信元探索プロトコル(MSDP)を有効 にします。
グローバルタイマー	グローバル MSDP タイマー プロファイルを選択するか、default プロファイルを選択するか、新しいグローバル MSDP タイマー プロファイルを作成します。default プロファイルを選択した場

IPv4 Multicast Settings (IPv4 マルチキャスト設定)	詳説
	合、[キープアライブ間隔] は 60 に設定され、[メッセージ タイム アウト] は 75 に設定され、[接続再試行間隔] は 30 に設定されま す。既定値は None で、既定値が適用されることを意味します。
グローバル認証	グローバル認証プロファイルを選択するか、新しいプロファイル を作成します。デフォルト設定は None (なし) です。
発信元 ID:インターフェ イス	論理ルータが送信元アクティブ(SA)メッセージの RP インター フェイスとして使用するインターフェイスを選択します。発信元 ID の IP アドレスを指定する場合は、発信元 IP インターフェイス を構成する必要があります。インターフェイスが設定されていな い場合は、IP アドレスを空のままにする必要があります。
発信元 ID:IP	論理ルータが SA メッセージの RP アドレスとして使用する IP ア ドレス(プレフィックス長付き)を選択または入力します。発信元 IP アドレスが設定されていない場合、論理ルータは PIM RP アド レスを使用して SA メッセージをカプセル化します。
MSDP - ピア	
ピア	ピア名を追加します (最大 63 文字)。名前は英数字、アンダース コア (_)、またはハイフン (-) で始まる必要があり、英数字、アン ダースコア、またはハイフンの組み合わせを含めることができま す。ドット (.) またはスペースは使用できません。
送信元インターフェイス	MSDP ピアとの TCP 経由の MSDP 接続を確立するために使用す る送信元インターフェイスを入力します。
送信元インターフェイ ス:IP	送信元インターフェイスの IP アドレスを選択します。デフォルト 設定は None (なし) です。
ピア アドレス タイプ	 ピアアドレスのタイプを選択します。 IP-(デフォルト)をクリックし、アドレスオブジェクトを選択するか、IPアドレスを入力します。 FQDN:ピアの完全修飾ドメイン名を入力します。ドロップダウンリストには、アドレスオブジェクトとして設定されているすべての FQDN 名が表示されます。
REMOTE AS(リモー トAS)	MSDP ピアが配置されているリモート AS の BGP 自律システム番号を入力します。
認証	以下のいずれかを実行します。

IPv4 Multicast Settings (IPv4 マルチキャスト設定)	詳説
	 [全般(General)] ページで MSDP に適用したグローバル認証プロファイルを上書きする、このピアに適用する認証プロファイルを選択します。
	 inherit (グローバル認証から継承)–グローバル認証プロファイル (デフォルト)。
	 None:グローバル認証プロファイルを上書きするこのピアへの 認証を無効にします。
最大SA	SA キャッシュがこの MSDP ピアから受け入れるソースアクティ ブ(SA)エントリの最大数を入力します。範囲は 0 から 1,024 で す。デフォルトは 0 です。この最大値に達すると、このピアから の新しい SA メッセージはドロップされます。
ピア インバウンド SA フィルター	アクセスリストを選択するか、新しいアクセスリストを作成し て、このピアからの着信 SA メッセージをフィルタリングしま す(不要なグループをブロックします)。デフォルト設定は None (なし) です。アクセスリストでは、フィルタリングする(S,G)ペア の送信元アドレス、またはフィルタリングする(S,G)ペアの宛先(グ ループ)アドレス、またはその両方を指定できます。
ピア アウトバウンド SA フィルター	アクセスリストを選択するか、新しいアクセスリストを作成し て、このピアに伝播される発信 SA メッセージをフィルタリン グします(不要なグループをブロックします)。デフォルト設定 は None (なし) です。アクセスリストでは、フィルタリングす る(S,G)ペアの送信元アドレス、またはフィルタリングする(S,G)ペ アの宛先(グループ)アドレス、またはその両方を指定できます。

Network > Routing > Routing Profiles ネットワー ク>ルーティング>ルーティングプロファイル

Advanced Routing Engine では、BGP、BFD、OSPF、OSPFv3、マルチキャスト、RIPv2、およびフィルターに属性を簡単かつ一貫して適用するためのルーティングプロファイルを作成します。

Network (ネットワーク) > Routing (ルーティング) > Routing Profiles (ルーティング プロファイル) > BGP

論理ルーターの場合は、BGP ルーティング プロファイル を使用して、BGP ピア グ ループ、ピア、または再配布ルールに構成を効率的に適用します。たとえば、Timer Profile、Authentication Profile、および BGP Filtering Profiles を BGP ピア グループまたはピア に適用できます。IPv4 および IPv6 の Address Family (AFI) プロファイルをピア グループまたは ピアに適用できます。IPv4 および IPv6 の再配信プロファイルを BGP 再配信に適用することが できます。

BGP Routing	業設
Profiles (BGP ルーティ	
ングプロファイル)	

BGP Auth Profile(**BGP** 認証プロファイル)

名前	Authentication プロファイルの名前を入力します (最大 63 文字)。 名前は、英数字、アンダースコア (_)、ハイフン (-)、またはドッ ト (.) で始まり、0 個以上の英数字、アンダースコア (_)、ハイフン (-)、ドットを含む必要があります。スペースは使用できません。
シークレット	Secret(シークレット)および Confirm Secret(シークレットの確認)を入力します。Secret (シークレット) は、MD5 認証における キーとして使用されます。

BGP タイマー プロファイル

名前	Timers プロファイルの名前を入力します (最大 63 文字)。名前は、 英数字、アンダースコア (_)、ハイフン (-)、またはドット (.) で始ま り、0 個以上の英数字、アンダースコア (_)、ハイフン (-)、ドット を含む必要があります。スペースは使用できません。
Keep Alive Interval	ピアから受け取ったルートが待機時間設定に従って停止されるま
(sec)(秒単位のキープ	での間隔(秒単位)を設定します(範囲は 0 ~ 1,200、デフォル
アライブ間隔)	トは 30)。

BGP Routing Profiles(BGP ルーティ ング プロファイル)	詳説
Hold Time (sec)(秒単位 の待機時間)	ピアからの連続する キープアライブ または 更新メッセージ間の想 定経過時間(秒単位)を指定します。この時間が過ぎるとピア接 続が閉じられます(範囲は 3 ~ 3,600、デフォルトは 90)。
再接続再試行間隔	アイドル状態で待機してからピアへの接続を再試行する秒数を入 力します (範囲は 1 ~ 3,600、デフォルトは 15)。
オープン遅延時間(秒)	ピアへの TCP 接続を開いてから、BGP 接続を確立するために最初 の BGP Open メッセージを送信するまでの遅延の秒数を入力しま す (範囲は 0 ~ 240、デフォルトは 0)。
Minimum Route Advertise Interval (sec)(ルート アドバ タイズメント最小間 隔(秒))	ルートまたはルートの撤回をアドバタイズする2つの連続する更 新メッセージ(BGPスピーカー[ファイアウォール]がBGPピアに 送信するメッセージ)の間に必要とされるおおよその最小間隔を 秒単位で入力します(範囲は1~600、デフォルトは30)。

BGP Address Family Profile (BGP アドレス ファミリー プロファイル)

名前	Address Family Identifier (AFI) プロファイルの名前を入力します (最大 63 文字)。名前は、英数字、アンダースコア (_)、ハイフン (-)、またはドット (.) で始まり、0 個以上の英数字、アンダースコ ア (_)、ハイフン (-)、ドットを含む必要があります。スペースは使 用できません。
AFI	AFI プロファイルのタイプ (IPv4 または IPv6) を選択します。
ユニキャスト/マルチ キャスト	Subsequent Address Family Identifier (SAFI) タイプを選択します。
SAFI を有効にする	ユニキャストまたはマルチキャスト SAFI (あるいはその両方) を有 効にするプロファイルを選択します。BGP プロファイルを有効に するには、少なくとも 1 つの SAFI を有効にする必要があります。 両方の SAFI を有効にすることができます。
経路が保存されたピア のソフト再構成	選択すると、firewall は、BGP ピアの設定が更新された後に、自身 のソフトリセットを実行します。(デフォルトは有効になっていま す。
ピアへのすべてのパス をアドバタイズする	ネットワーク内のマルチパス機能を保持するために、すべてのパ スをネイバーにアドバタイズします。

BGP Routing Profiles(BGP ルーティ ング プロファイル)	詳説
Advertise the bestpath for each neighboring AS 各隣接 AS のベストパス をアドバタイズする	すべての自律型システムの汎用パスではなく、BGP がそれぞれ隣 接する AS のベスト パス(最適経路)をアドバタイズする設定を 有効化します。すべての自律システムに同じパスをアドバタイズ する場合は、これを無効化します。
Override ASNs in outbound updates if AS-Path equals Remote-AS(AS-Path が Remote-AS と等しい場 合、アウトバウンド更 新で ASN をオーバーラ イドする)	同じ AS (AS 64512 等) に所属する複数のサイトがあり、サイト 間に別の AS が存在する場合は、BGP AS オーバーライド機能を使 用することができます。2 つのサイト間のルーターは、AS64512 にアクセスすることができるルートをアドバタイズする更新を受 信します。更新が AS64512 にもあるために、2 番目のサイトが更 新をドロップしないために、中間ルーターは AS64512 を独自の ASN (AS 64522 等) に置き換えます。
Route Reflector Client(ルートリフレク タのクライアント)	BGP ピアを iBGP ネットワーク内の BGP Route Reflector Client に するために有効にします。
Originate Default Route(デフォルトルー トの発信)	すべてのデフォルトルートをアドバタイズする場合に選択しま す。特定の宛先へのルートのみをアドバタイズする場合は無効に します。
デフォルトの発信ルー トマップ	ルート マップを Originate Default Route フィールドに適用する と、アドバタイズする既定のルートのタイプを指定できます。
Allow AS in AS を許可す る	ファイアウォール自体の自律型システム(AS)番号を含むルート を許可するかどうかを指定します。
	 Origin(発信元) –ファイアウォール自体の AS が AS_PATH に 存在する場合であっても、ルートを許容します。
	 Occurrence(発生数) –ファイアウォール自体の AS が AS_PATH に含まれる可能性がある回数です。
	 None(なし) –(デフォルト設定) 実行されるアクションはありません。
番号プレフィックス	ピアから受け入れるプレフィックスの最大数を入力します。範囲 は 1 ~ 4,294,967,295 です。デフォルトは 1,000 です。
Threshold (%)(しきい 値)	プレフィックスの最大数のしきい値の割合を入力します。ピアが しきい値を超えてアドバタイズした場合、ファイアウォールは指 定のアクション(警告または再起動)を実行します。範囲は1~ 100です。

BGP Routing Profiles(BGP ルーティ ング プロファイル)	詳説
アクション	プレフィックスの最大数の超過後にファイアウォールが BGP 接続 に対して実行するアクションを指定します。ログ内のメッセージ のWarning Only(警告のみ)または BGP ピア接続の Restart(再 起動)を実行します。
ネクストホップ	ネクストホップの選択:
	• None - 元のネクストホップが保持されます。
	 Self(セルフ) –ネクストホップ計算を無効にして、ルートを ローカル ネクストホップでアドバタイズします。
	 Self Force(セルフフォース) –評価されたルートのネクスト ホップを強制的に自身に設定します。
プライベート AS の削除	ファイアウォールが別の AS 内のピアに送信する更新に含まれる AS_PATH 属性のプライベート AS 番号を BGP に強制的に削除させ る場合は、以下のいずれかを選択します。
	• All(すべて)–すべての非公開 AS 番号を削除します。
	 Replace AS (ASの置換え) – すべての非公開 AS 番号をファイ アウォールの AS 番号に置き換えます。
	 None(なし) –(デフォルト設定) 実行されるアクションはありません。
Send Community(コ ミュニティ送信)	アウトバウンド更新メッセージで送信する BGP コミュニティ属性 のタイプを選択します。
	• All (すべて) – すべてのコミュニティを送信します。
	 Both(両方) –標準コミュニティおよび拡張コミュニティを送信します。
	• Extended(拡張)–拡張コミュニティを送信します。
	● Large(大型)−大型コミュニティを送信します。
	• Standard(標準)–標準コミュニティを送信します。
	• None (なし) – いずれのコミュニティも送信しません。
ORFリスト	ピア グループまたはピアがプレフィックス リストを送信したり、 プレフィックス リストを受信したりして、送信元で送信ルート フィルタリング (ORF) を実装する機能をアドバタイズし、Updates で不要なプレフィックスを送受信することを最小限に抑えます。 以下のいずれかを選択します。
BGP Routing Profiles(BGP ルーティ ング プロファイル)	詳説
--	--
	 none – (デフォルト設定) ピア グループまたはピア (この AFI プ ロファイルが適用されている場所) には ORF 機能がありません。
	 both – ピア グループまたはピアが send とプレフィックス リスト、receive がプレフィックス リストを ORF を実装できることをアドバタイズします。
	 receive – ピア グループまたはピアが ORF を実装するためのプレフィックスリストを受信できることをアドバタイズします。 ローカル・ピアは、リモート・ピアの ORF 機能と接頭部リストを受け取り、これをアウトバウンド経路フィルターとして実装します。
	 send – ピア グループまたはピアがプレフィックス リストを送信して ORF を実装できることをアドバタイズします。リモート・ピア (受信機能を持つ)は、ORF 機能を受け取り、送信側に経路をアドバタイズするときに、受信した接頭部リストをアウトバウンド経路フィルターとして実装します。
	ORF を実装するには、次の手順を実行します。
	 Address Family プロファイルで ORF 機能を指定します。 ピア グループまたは送信者であるピアの場合は、ピア グルー プ/ピアが受信するプレフィックスのセットを含むプレフィック スリストを作成します。
	3. BGP フィルタリングプロファイルを作成し、[受信プレフィック スリスト] で、作成したプレフィックスリストを選択します。
	 BGP ピア グループの場合、作成した Address Family プロファ イルを選択してピア グループに適用します。送信者の場合は、 作成したフィルタリングプロファイル(プレフィックスリストを 示す)も選択します。ピア・グループまたはピアが ORF レシー バーのみである場合、Filtering Profile は必要ありません。ORF 受信機能を示すために必要なのは Address Family プロファイル だけです。

BGP 減衰プロファイル

名前	ダンプニング プロファイルの名前を入力します(最大 63 文字)。名 前は、英数字、アンダースコア (_)、ハイフン (-)、またはドット (.) で始まり、0 個以上の英数字、アンダースコア (_)、ハイフン (-)、 ドットを含む必要があります。スペースは使用できません。
詳説	ダンプニング プロファイルの説明を入力します。

ネットワーク

BGP Routing Profiles(BGP ルーティ ング プロファイル)	詳説
制限を抑制	抑制値(フラッピングに対するペナルティの累積値)を入力すると、 その時点でピアから来るすべてのルートがダンプニングされま す。範囲は 1 ~ 20,000 です。デフォルトは 2,000 です。
再利用制限	Half Life で説明されている手順に基づいてルートを再利用できる タイミングを制御する値を入力します。範囲は 1 ~ 20,000 です。 デフォルトは 750 です。
半減期(分)	half-life 時間の分数を入力して、フラッピングルートに適用され る安定性メトリック (ペナルティ)を制御します。範囲は1~45で す。デフォルトは15です。安定性メトリックは1,000から始ま ります。ペナルティが課せられたルートが安定すると、Half Life タイマーは有効期限が切れるまでカウントダウンし、その時点で ルータに適用される次の安定性メトリックは前の値(500)の半分に すぎません。安定性メトリックが Reuse Limit の半分以下になる まで、連続したカットが続行され、その後、安定性メトリックが ルータから削除されます。
最大抑制時間 (分)	ルートがどれほど不安定であったかに関係なく、抑制できる最大 分数を入力します。範囲は1~255です。デフォルトは 60 です。
BGP Redistribution Profil	e(BGP 再配信プロファイル)
名前	再配布 プロファイルの名前を入力します (最大 63 文字)。名前は、 英数字、アンダースコア (_)、ハイフン (-)、またはドット (.) で始ま り、0 個以上の英数字、アンダースコア (_)、ハイフン (-)、ドット を含む必要があります。スペースは使用できません。
IPv4 / IPv6	再配信されるルートのタイプを指定するには、IPv4 または IPv6 Address Family Identifier (AFI、アドレス ファミリー ID)を選択 します。
スタティック	Static および Enable を選択して、IPv4 または IPv6 スタティック ルート (選択した AFI に一致する) を BGP に再配布します。
メトリック	BGP に再配信されるスタティック ルートに適用するメトリックを 入力します(範囲は 1~65,535)。
ルートマップ	Route Map を選択して、再配布する静的経路を決定する一致基準 を指定します。デフォルト設定は None (なし) です。ルートマッ プセットの設定に Metric Action と Metric Value が含まれている場 合、それらは再配布ルートに適用されます。それ以外の場合は、

ネットワーク

BGP Routing Profiles (BGP ルーティ ングプロファイル)	詳説
	この再配布プロファイルで構成されたメトリックが再配布ルート に適用されます。
接続済み	Connected および Enable を選択して、IPv4 または IPv6 接続ルート (選択した AFI に一致する) を BGP に再配布します。
メトリック	BGP に再配信される接続済ルートに適用するメトリックを入力し ます(範囲は 1~65,535)。
ルートマップ	Route Map を選択して、再配布する接続ルートを決定する一致基準を指定します。デフォルト設定は None (なし) です。ルートマップセットの設定に Metric Action と Metric Value が含まれている場合、それらは再配布ルートに適用されます。それ以外の場合は、この再配布プロファイルで構成されたメトリックが再配布ルートに適用されます。
OSPF	(IPv4 のみ) OSPFv2 ルートを BGP に再配布するには、OSPF と Enable を選択します。
メトリック	BGP に再配布される OSPF ルートに適用するメトリックを入力し ます(範囲は 1 ~ 65,535)。
ルートマップ	Route Map を選択して、再配布する OSPF 経路を決定する一致基準を指定します。デフォルト設定は None (なし) です。ルートマップセットの設定に Metric Action と Metric Value が含まれている場合、それらは再配布ルートに適用されます。それ以外の場合は、この再配布プロファイルで構成されたメトリックが再配布ルートに適用されます。
RIP	(IPv4 のみ) RIP ルートを BGP に再配布するには、RIP と Enable を 選択します。
メトリック	BGP に再配布される RIP ルートに適用するメトリックを入力しま す(範囲は 1 ~ 65,535)。
ルートマップ	Route Map を選択して、再配布する RIP 経路を決定する一致基準 を指定します。デフォルト設定は None (なし) です。ルートマッ プセットの設定に Metric Action と Metric Value が含まれている場 合、それらは再配布ルートに適用されます。それ以外の場合は、 この再配布プロファイルで構成されたメトリックが再配布ルート に適用されます。

ネットワーク

BGP Routing Profiles(BGP ルーティ ング プロファイル)	詳説
OSPFv3IPv6	(IPv6 のみ) OSPFv3 ルートを BGP に再配布するには、OSPFv3 と Enable を選択します。
メトリック	BGP に再配布される OSPFv3 経路に適用するメトリックを入力し ます(範囲は 1 から 65,535 です)。
ルートマップ	Route Map を選択して、再配布する OSPFv3 経路を決定する一致 基準を指定します。デフォルト設定は None (なし) です。ルート マップセットの設定に Metric Action と Metric Value が含まれて いる場合、それらは再配布ルートに適用されます。それ以外の場 合は、この再配布プロファイルで構成されたメトリックが再配布 ルートに適用されます。

BGP フィルタリング プロファイル

名前	BGP Filtering プロファイルの名前を入力します(最大 63 文字)。名前は、英数字、アンダースコア (_)、ハイフン (-)、またはドット (.) で始まり、0 個以上の英数字、アンダースコア (_)、ハイフン (-)、ドットを含む必要があります。スペースは使用できません。
詳説	BGP Filtering プロファイルの説明を入力します。
AFI	IPv4 または IPv6 Address Family Identifier を選択して、フィル ター処理するルートの種類を指定します。
Unicast Inbound Filter List	AS パス アクセス リストを選択するか、新しいアクセス リストを 作成して、ピアからルートを受信するときに、同じ AS Path を持 つルートのみがピア グループまたはピアからインポートされ、 ローカル BGP RIB に追加されるように指定します。
インバウンド配布リス ト	アクセスリスト(Source Address のみ、Destination Address は使用 しません)を使用して、BGP が受信する BGP ルーティング情報を フィルタリングします。単一の Filtering Profile 内のインバウンド 接頭部リストと相互に排他的です。
受信プレフィックス リ スト	プレフィックス リストを使用して、BGP が受信する BGP ルー ティング情報をネットワーク プレフィックスに基づいてフィル ター処理します。単一のフィルタリングプロファイル内のインバ ウンド配布リストと相互に排他的です。
インバウンドルート マップ	ルート マップを使用すると、ローカル BGP RIB (一致基準) に許 可されるルートをさらに詳細に制御し、ルートの属性を設定しま

BGP Routing Profiles(BGP ルーティ ング プロファイル)	詳説
	す(オプションの設定)。例えば、経路の AS Path の前に AS を付け ることによって、経路の優先順位を制御できます。
送信フィルタリスト	AS Path アクセス リストを選択するか、新しい AS Path アクセス リストを作成して、同じ AS Path を持つルートのみがピア ルー タ(このフィルタが適用されるピア グループまたはピア)にアドバタ イズされるように指定します。
Outbound Distribute List アウトバウンド配布 リスト	アクセスリストを使用して、宛先の IP アドレスに基づいて、BGP がアドバタイズする BGP ルーティング情報をフィルタリングし ます。単一のフィルタリングプロファイル内のOutbound Prefix Listと相互に排他的です。
Outbound Prefix List (アウトバウンド・プレ フィックス・リスト)	プレフィックス リストを使用して、ネットワーク プレフィックス に基づいて、BGP がアドバタイズする BGP ルーティング情報を フィルター処理します。単一のフィルタリングプロファイル内の アウトバウンド配布リストと相互に排他的です。
発信ルート マップ	ルート マップを使用すると、BGP がアドバタイズするルート (一 致基準) をさらに細かく制御し、アドバタイズされたルートの属性 を設定できます。
Conditional Advertisement–Exist– Exist Map (条件付きアド バタイズメント - 存在 - 存在マップ)	ルートマップを選択または作成して、条件付きアドバタイズメン トの一致基準を指定します。これらのルートがローカル BGP RIB に存在する場合、Advertise Map によって指定されたルートがアド バタイズされます。このフィールドのルートマップの Match 部分 のみが有効になります。Set 部分は無視されます。
Conditional Advertisement-Exist- Advertise Map (条件付 きアドバタイズメント - 存在 - アドバタイズマッ プ)	ルート マップを選択または作成して、条件が満たされた場合に アドバタイズするルートを指定します(Exist Map からのルートは ローカル BGP RIB に存在します)。このフィールドのルートマップ の Match 部分のみが有効になります。Set 部分は無視されます。
Conditional Advertisement–Non- Exist–Non Exist Map (条件付きアドバタイズ メント - 存在しない - 存 在しないマップ)	ルートマップを選択または作成して、条件付きアドバタイズメン トの一致基準を指定します。これらのルートがローカル BGP RIB に存在しない場合、Advertise Map によって指定されたルートがア ドバタイズされます。このフィールドのルートマップの Match 部 分のみが有効になります。Set 部分は無視されます。

BGP Routing Profiles(BGP ルーティ ング プロファイル)	詳説
Conditional Advertisement—Non- Exist—Advertise Map (条 件付きアドバタイズメ ント - 存在しない - アド バタイズマップ)	ルート マップを選択または作成して、条件が満たされた場合にア ドバタイズするルートを指定します(Non-Exist Map からのルート はローカル BGP RIB に存在しません)。このフィールドのルート マップの Match 部分のみが有効になります。Set 部分は無視され ます。
マップの抑制を解除	ルート集約またはルート減衰から抑制を解除するルートのルート マップを選択または作成し、それらをアドバタイズします。
Multicast —Unicast から の 継承	(IPv4 AFI のみ)Multicast ルートをフィルタリングするための Unicast 設定を継承する場合に選択します。それ以外の場合 は、Unicast フィルターについて、この表の説明に従ってマルチ キャスト・フィルターを構成します。

Network > Routing > Routing Profiles > BFD [ネットワーク>ルー ティング > ルーティング プロファイル > BFD]

Bidirectional Forwarding Detection profile を作成します。

BFD Routing Profiles (BFD ルーティングプロ ファイル)	詳説
名前	BFD プロファイルの名前を入力します(最大 63 文字)。名前は、英数字、アンダースコア (_)、またはハイフン(-) で始まり、0 個以上の 英数字、アンダースコア(_)、またはハイフン (-) を含む必要があります。ドット(.) または スペースは使用できません。
モード	 モードを選択: Active-(デフォルト) BFD はピアへの制御パケットの送信を開始します。最低でも1つのBFDピアがアクティブに設定されている必要があります。両方がアクティブでも構いません。 Passive[パッシブ] - BFDはピアからコントロールパケットが送られてくるまで待機し、要求に応じて応答を行います。

BFD Routing Profiles (BFD ルーティングプロ ファイル)	詳説
希望する最低Tx間隔(ミリ秒)	BFD プロトコルが BFD 制御パケットを送 信する最小間隔 (ミリ秒単位)。したがっ て、送信間隔をピアとネゴシエートしてい ます。PA-7000シリーズ、PA-5200シリー ズ、PA-5400シリーズ、およびPA-3400シ リーズの範囲は50~10,000です。PA-3200シ リーズの範囲は100~10,000です。PA-400シ リーズの範囲は150~10,000です。VM シ リーズの範囲は200~10,000です。デフォ ルトは 1,000 です。
必要な最小Rx間隔(ミリ秒)	BFD が BFD 制御パケットを受信でき る最小間隔 (ミリ秒単位)。PA-7000シ リーズ、PA-5200シリーズ、PA-5400シ リーズ、およびPA-3400シリーズの範囲 は50~10,000です。PA-3200シリーズの範囲 は100~10,000です。PA-400シリーズの範囲 は150~10,000です。ゲフォルトは 1,000 で す。
検知時間乗数値	範囲は2~255です。デフォルトは3です。 ローカルシステムはリモートシステムから受 信したDetection Time Multiplier (検知時間 乗数)を同意済みのリモートシステムの送信 間隔 (Required Minimum Rx Interval (最低 Rx 間隔要件)および最後に受信したDesired Minimum Tx Interval (目標の最低 Tx 間隔)の うち、いずれか大きい方)で掛けることで検 知時間を算出します。検知時間が過ぎるまで にBFDがピアからのBFDコントロールパケッ トを受信しない場合、障害が発生しているこ とを意味します。
ホールドタイム(ミリ秒単位)	リンクが起動してから BFD 制御パケット を送信するまでの遅延 (ミリ秒単位)。Hold Time は BFD Active モードにのみ適用されま す。BFD が Hold Time 中に BFD 制御パケッ トを受信すると、BFD はそれらを無視しま す。範囲は 0 ~ 120,000 です。デフォルトは 0 で、送信ホールド・タイムが使用されない ことを意味します。BFD は、リンクが確立さ

BFD Routing Profiles (BFD ルーティングプロ ファイル)	詳説 れた直後に BFD 制御パケットを送受信しま
	,
マルチホップの有効化	BGP マルチホップで BFD を有効にします。
最低Rx TTL值	BGP がマルチホップ BFD をサポートしてい る場合、BFD 制御パケットで BFD が受け入 れる (受信する) 最小有効時間(ホップ数)を入 力します。範囲は 1 ~ 254 です。デフォルト はありません。

Network > Routing > Routing Profiles > OSPF [ネットワーク>ルー ティング > OSPF >ルーティング プロファイル]

OSPF ルーティング プロファイル を追加して、論理ルーター用に OSPFv2 を効率的に構成します。

OSPF ルーティング プロファイル	の意味
OSPF グローバル タイマー プロファ	イル
氏名	プロファイルの名前を入力します (最大 63 文字)。名前 は、英数字、アンダースコア (_)、またはハイフン (-) で 始まり、0 個以上の英数字、アンダースコア (_)、または ハイフン (-) を含む必要があります。ドット (.) またはス ペースは使用できません。
LSA 最小到着	同じ LSA (同じアドバタイズメント ルータ ID、同じ LSA タイプ、および同じ LSA ID) の 2 つのインスタンスの 送信間の最小時間(秒単位)を入力します。設定された 間隔よりも早く同じ LSA が到着すると、LSA はドロッ プされます。範囲は 1 ~ 10 です。デフォルトは 5 で す。LSA の最小到着は、RFC 2328 の MinLSInterval と 同等です。低い値を指定すると、トポロジが変更された 場合の再収束時間が短縮されます。
SPF - 初期遅延	論理ルータがトポロジの変更を受信してから最短パス優先(SPF)計算を実行するまでの初期遅延(秒単位)を入力します。範囲は 0~600 です。デフォルトは 5 です。指定する値が低ければそれだけ OSPF の再収束が速くなります。ファイアウォールとピアリングしているルーター

OSPF ルーティング プロファイル	の意味
	は、同じ遅延時間の値を使用することで、収束時間を最 適化する必要があります。
初期保留時間	連続する SPF 計算間の初期ホールド時間 (秒単位) を入 力します。範囲は 0 ~ 600 です。デフォルトは 5 です。
最大保留時間	最大ホールド時間(秒単位)を入力します。これは、ホー ルド時間が安定するまでスロットルする最大値です。範 囲は 0 ~ 600 です。デフォルトは 5 です。

OSPF インターフェイス認証プロファイル

氏名	Authentication プロファイルの名前を入力します(最大 63 文字)。名前は、英数字、アンダースコア(_)、また はハイフン(-)で始まり、0 個以上の英数字、アンダー スコア(_)、またはハイフン(-)を含む必要があります。 ドット(.)またはスペースは使用できません。
タイプ	 認証のタイプを1つ選択します。 Password – Password (最大8文字) と Confirm Password を入力します。 MD5 – Add は、MD5 キー ID (範囲は0~255) と Key (最大16文字、スペースを除く任意の文字) で
	す。Preferred を選択して、MD5 キーを他の MD5 キーよりも優先します。

OSPF インターフェイス タイマー プロファイル

氏名	プロファイルの名前を入力します (最大 63 文字)。名前 は、英数字、アンダースコア (_)、またはハイフン (-) で 始まり、0 個以上の英数字、アンダースコア (_)、または ハイフン (-) を含む必要があります。ドット (.) またはス ペースは使用できません。
送信間隔	firewall が近隣関係を維持するためにインターフェース を送信する Hello パケット間の間隔 (秒単位) を入力しま す。範囲は 1 から 3600 です。デフォルトは 10 です。
デッドカウント	OSPF がネイバーから hello パケットを受信していない ネイバーに対して、OSPF がそのネイバーをダウンと 見なすまでに Hello Interval が発生する回数を入力しま す。範囲は 3 から 20 です。デフォルトは 4 です。

OSPF ルーティング プロファイル	の意味
再送信間隔	隣接するルータへの LSA 再送信間の秒数を入力しま す。範囲は 1 ~ 1800 です。デフォルトは 5 です。
Transmit Delay (送信遅延)	インターフェイス経由で Link State Update Packet を送 信するために必要な秒数を入力します。更新パケット内 の Link State Advertisements は、送信される前にこの番 号だけ経過時間がインクリメントされます。範囲は 1 ~ 1800 です。デフォルトは 1 です。
グレースフルリスタートこんにち は遅延 (秒)	Graceful Restart Hello Delay (秒単位) を入力します。 これは、Active/Passive High Availability が設定され ているときに OSPF インターフェイスに適用されま す。Graceful Restart Hello Delay は、firewall が 1 秒間 隔で Grace LSA パケットを送信する時間の長さです。こ の期間は、リスタート中のファイアウォールから Hello パケットが送信されません。再起動中は、デッドタイ マー (Hello IntervalにDead Countを乗じたもの) もカ ウントダウンしています。失敗タイマーの時間が短かす ぎる場合は、Hello パケットが遅延したときに、グレー スフル リスタート中に隣接がダウンします。したがっ て、デッドタイマーは、Graceful Restart Hello Delay の 値の少なくとも 4 倍にすることをお勧めします。たとえ ば、Hello Interval が 10 秒で Dead Count が 4 の場合、 デッド タイマーは 40 秒になります。Graceful Restart Hello Delay が 10 秒に設定されている場合、hello パ ケットの 10 秒の遅延は 40 秒のデッド タイマー内に 収まるので、グレースフル リスタート中に隣接関係が タイムアウトすることはありません。範囲は 1 ~ 10 で す。デフォルトは 10 です。
OSPF 再配布プロファイル	
正 夕	プロファイルの久益を入力します(県十42 立今) 夕益

氏名	プロファイルの名前を入力します (最大 63 文字)。名前 は、英数字、アンダースコア (_)、またはハイフン (-) で 始まり、0 個以上の英数字、アンダースコア (_)、または ハイフン (-) を含む必要があります。ドット (.) またはス ペースは使用できません。
IPv4 スタティック	プロファイルのこの部分を構成できるようにする場合に 選択します。
Enable [有効化]	OSPF への IPv4 静的経路再配布を使用可能にします。

OSPF ルーティング プロファイル	の意味
メトリック	OSPF に再配布される静的経路に適用する Mectric を指 定してください (範囲は 1 から 65,535)。
メトリックの種類	次に • Type 1 • Type 2(デフォルト)
ルートマップの再配分	Redistribution Route Map を選択または作成して、OSPF に再配布される IPv4 静的経路を制御し、その属性を設 定します。デフォルト設定は None (なし) です。ルート マップセットの設定に Metric Action と Metric Value が 含まれている場合、それらは再配布ルートに適用されま す。それ以外の場合は、この再配布プロファイルで構成 されたメトリックが再配布ルートに適用されます。同様 に、ルートマップ セット設定の Metric Type は、この 再配布プロファイルで設定された Metric Type よりも優 先されます。
接続済み	プロファイルのこの部分を構成できるようにする場合に 選択します。
Enable [有効化]	OSPF への接続ルート再配布を有効にします。
メトリック	OSPF に再配布される接続経路に適用する Metric を指 定します (範囲は 1 から 65,535)。
メトリックの種類	次に • Type 1 • Type 2 (デフォルト)
ルートマップの再配分	Redistribution Route Map を選択または作成して、OSPF に再配布される接続ルートを制御し、その属性を設定し ます。デフォルト設定は None (なし) です。ルートマッ プセットの設定に Metric Action と Metric Value が含ま れている場合、それらは再配布ルートに適用されます。 それ以外の場合は、この再配布プロファイルで構成され たメトリックが再配布ルートに適用されます。同様に、 ルートマップ セット設定の Metric Type は、この再配 布プロファイルで設定された Metric Type よりも優先さ れます。
RIPv2	プロファイルのこの部分を構成できるようにする場合に 選択します。

OSPF ルーティング プロファイル	の意味
Enable [有効化]	OSPF への RIPv2 経路再配布を使用可能にします。
メトリック	OSPFに再配布されるRIPv2経路に適用するMetricを指定 してください(範囲は0から4,294,967,295です)。
メトリックの種類	次に Type 1
	• Type 2 (デフォルト)
ルートマップの再配分	Redistribution Route Map を選択または作成して、OSPF に再配布される RIPv2 経路を制御し、その属性を設定 します。デフォルト設定は None (なし) です。ルート マップセットの設定に Metric Action と Metric Value が 含まれている場合、それらは再配布ルートに適用されま す。それ以外の場合は、この再配布プロファイルで構成 されたメトリックが再配布ルートに適用されます。同様 に、ルートマップ セット設定の Metric Type は、この 再配布プロファイルで設定された Metric Type よりも優 先されます。
BGP AFI IPv4	プロファイルのこの部分を構成できるようにする場合に 選択します。
Enable [有効化]	OSPF への BGP IPv4 ルートの再配布を有効にします。
メトリック	OSPF に再配布される BGP IPv4 経路に適用する Mectric を指定します(範囲は 0 から 4,294,967,295)。
メトリックの種類	次に • Type 1 • Type 2 (デフォルト)
ルートマップの再配分	Redistribution Route Map を選択または作成して、OSPF に再配布される BGP IPv4 ルートを制御し、その属性を 設定します。デフォルト設定は None (なし) です。ルー トマップセットの設定に Metric Action と Metric Value が含まれている場合、それらは再配布ルートに適用され ます。それ以外の場合は、この再配布プロファイルで構 成されたメトリックが再配布ルートに適用されます。同 様に、ルートマップ セット設定の Metric Type は、こ の再配布プロファイルで設定された Metric Type よりも 優先されます。

OSPF ルーティング プロファイル	の意味
IPv4 デフォルト ルート	プロファイルのこの部分を構成できるようにする場合に 選択します。
いつも	ルーターにデフォルト経路がない場合でも、IPv4 デ フォルト経路を常に作成して OSPF に再配布する場合に 選択します。デフォルトは有効になっています。
Enable [有効化]	OSPF への IPv4 デフォルト経路再配布を使用可能にします。
メトリック	OSPFに再配布されるIPV4省略時経路に適用 するMetricを指定してください(範囲は0か ら4,294,967,295です)。
メトリックの種類	次に Type 1 Type 2 (デフォルト)

Network > Routing > Routing Profiles > OSPFv3 [ネットワー ク>ルーティング > OSPFv3 >ルーティング プロファイル]

OSPFv3 ルーティング プロファイル を追加して、論理ルーター用に OSPFv3 を効率的に構成します。

OSPFv3 Routing Profiles (OSPFv3 ルーティング プロファイル)	の意味
OSPFv3 グローバル タイマー プロファイル	
氏名	プロファイルの名前を入力します (最大 63 文字)。名前 は、英数字、アンダースコア (_)、またはハイフン (-) で 始まり、0 個以上の英数字、アンダースコア (_)、また はハイフン (-) を含む必要があります。ドット (.) また はスペースは使用できません。
LSA 最小到着	firewall が SPF ツリーを再計算する最小間隔を入力 します。範囲は 1 から 10 です。デフォルトは 5 で す。firewallは、より大きな間隔で(設定よりも頻度が低 い)再計算します。
SPF スロットル-初期遅延	論理ルータがトポロジの変更を受信してから最短パス 優先(SPF)計算を実行するまでの初期遅延(秒単位)を入

OSPFv3 Routing Profiles (OSPFv3 ルーティング プロファイル)	の意味
	力します。範囲は0~600です。デフォルトは5で す。
初期保留時間	最初の2つの連続する SPF 計算間の初期ホールド時間 (秒単位)を入力します。範囲は0~600です。デフォ ルトは5です。後続の各ホールド時間は、ホールド時 間が最大ホールド時間に達するまで、前のホールド時 間の2倍の長さです。
最大保留時間	ホールド時間が安定するまで増加する最大値を入力し ます。範囲は 0 ~ 600 です。デフォルトは 5 です。
OSPFv3 認証プロファイル	
氏名	Authentication プロファイルの名前を入力します(最大 63 文字)。名前は、英数字、アンダースコア(_)、また はハイフン(-) で始まり、0 個以上の英数字、アンダー スコア(_)、またはハイフン(-) を含む必要があります。 ドット(.) またはスペースは使用できません。
SPI	Security Policy Index を入力します。これは、OSPFv3 隣接関係の両端間で一致する必要があります。
PROTOCOL	認証プロトコルを選択します。 ESP (Encapsulating Security Payload) (推奨) または AH (Authentication header).
Authentication-Type	認証タイプを選択します。
	• SHA1(デフォルト)Secure Hash Algorithm 1
	• SHA256
	 SHA384 SHA512
	• MD5
	• なし
+	認証キーを 16 進形式で入力します: xxxxxxxx[- xxxxxxxx]合計5つのセクションとConfirm Keyを使用 します。
Encryption—Algorithm	(ESP のみ)暗号化アルゴリズムを選択します。3des(デフォルト)

OSPFv3 Routing Profiles (OSPFv3 ルーティング プロファイル)	の意味
	• aes-128-cbc
	• aes-192-cbc
	• aes-256-cbc
	• null
キー	(ESP のみ) 暗号化キーを 16 進形式で入力します。ESP 暗号化の種類と Confirm Key に基づいて正しいセク ション数を使用します。
	 3des – キーに合計 6 つの 16 進セクションを使用します。
	 aes-128-cbc - キーに合計 4 つの 16 進セクションを 使用します。
	 aes-192-cbc - キーに合計 6 つの 16 進セクションを 使用します。
	 aes-256-cbc - キーに合計 8 つの 16 進セクションを 使用します。

OSPFv3 インターフェイス タイマー プロファイル

氏名	プロファイルの名前を入力します(最大 63 文字)。名前 は、英数字、アンダースコア(_)、またはハイフン(-)で 始まり、0 個以上の英数字、アンダースコア(_)、また はハイフン(-)を含む必要があります。ドット(.)また はスペースは使用できません。
送信間隔	OSPFv3 が Hello パケットを送信する間隔 (秒単位) を 入力します。範囲は 1 ~ 3,600 です。デフォルトは 10 です。
デッドカウント	OSPFv3 がネイバーのダウンと見なすまでに、OSPFv3 がネイバーから Hello パケットを受信していない状態 で、ネイバーから Hello Interval が発生する回数を入 力します。範囲は 3 から 20 です。デフォルトは 4 で す。
再送信間隔	OSPFv3 が LSA を再送信する前に、OSPFv3 が近隣か ら LSA を受信するのを待機する秒数を入力します (範 囲は 1 から 1,800 です)。デフォルトは 5 です。

OSPFv3 Routing Profiles (OSPFv3 ルーティング プロファイル)	の意味
Transmit Delay (送信遅延)	OSPFv3 が SLA をインターフェイスから送信する前に LSA の送信を遅らせる秒数を入力します。範囲は 1 ~ 1,800 です。デフォルトは 1 です。
グレースフルリスタートこんにちは 遅延 (秒)	Graceful Restart Hello Delayを数秒で入力します。 範囲は 1 から 10 です。デフォルトは 10 です。この 設定は、Active/Passive HA が構成されているときに OSPFv3 インターフェイスに適用されます。Graceful Restart Hello Delay は、firewall が 1 秒間隔で Grace LSA パケットを送信する秒数です。この間、再起動中 の firewall から Hello パケットは送信されません。再起 動中、デッド タイム (Hello Interval に Dead Count を 掛けた値) もカウントダウンされます。失敗タイマーの 時間が短かすぎる場合は、Hello パケットが遅延したと きに、グレースフル リスタート中に隣接がダウンしま す。したがって、デッドタイマーは、Graceful Restart Hello Delay の値の少なくとも 4 倍にすることをお勧め します。
OSPFv3 再配布プロファイル	
氏名	プロファイルの名前を入力します (最大 63 文字)。名前 は、英数字、アンダースコア (_)、またはハイフン (-) で 始まり、0 個以上の英数字、アンダースコア (_)、また はハイフン (-) を含む必要があります。ドット (.) また はスペースは使用できません。
IPv6 スタティック	プロファイルのこの部分の構成を許可する場合に選択 します。
Enable [有効化]	プロファイルの IPv6 静的部分を有効にします。
メトリック	OSPFv3 に再配布される静的経路に適用する Mectric を指定してください (範囲は 1 から 65,535)。
メトリックの種類	Type 1 または Type 2 を選択します。
ルートマップの再配分	Redistribution Route Map を選択または作成し て、OSPFv3 に再配布される IPv6 静的経路を制御 し、それらの属性を設定します。デフォルト設定は None (なし) です。ルートマップセットの設定に Metric Action と Metric Value が含まれている場合、それらは 再配布ルートに適用されます。それ以外の場合は、こ の再配布プロファイルで構成されたメトリックが再配

OSPFv3 Routing Profiles (OSPFv3 ルーティング プロファイル)	の意味
	布ルートに適用されます。同様に、ルートマップ セッ ト設定の Metric Type は、この再配布プロファイルで 設定された Metric Type よりも優先されます。
接続済み	プロファイルのこの部分の構成を許可する場合に選択 します。
Enable [有効化]	プロファイルの接続部分を有効にします。
メトリック	OSPFv3 に再配布される Connected 経路に適用する Mectric を指定してください (範囲は 1 から 65,535)。
メトリックの種類	Type 1 または Type 2 を選択します。
ルートマップの再配分	Redistribution Route Map を選択または作成し て、OSPFv3 に再配布される接続済み経路を制御し、 その属性を設定します。デフォルト設定は None (な し) です。ルートマップセットの設定に Metric Action と Metric Value が含まれている場合、それらは再配布 ルートに適用されます。それ以外の場合は、この再配 布プロファイルで構成されたメトリックが再配布ルー トに適用されます。同様に、ルートマップ セット設定 の Metric Type は、この再配布プロファイルで設定さ れた Metric Type よりも優先されます。
BGP AFI IPv6	プロファイルのこの部分の構成を許可する場合に選択 します。
Enable [有効化]	プロファイルの BGP AFI IPv6 部分を有効にします。
メトリック	OSPFv3 に再配布される BGP IPv6 経路に適用 する Mectric を指定してください (範囲は 0 から 4,294,967,295)。
メトリックの種類	Type 1 または Type 2 を選択します。
ルートマップの再配分	Redistribution Route Map を選択または作成し て、OSPFv3 に再配布される BGP IPv6 経路を制御し、 その属性を設定します。デフォルト設定は None (な し) です。ルートマップセットの設定に Metric Action と Metric Value が含まれている場合、それらは再配布 ルートに適用されます。それ以外の場合は、この再配 布プロファイルで構成されたメトリックが再配布ルー トに適用されます。同様に、ルートマップ セット設定

OSPFv3 Routing Profiles (OSPFv3 ルーティング プロファイル)	の意味
	の Metric Type は、この再配布プロファイルで設定さ れた Metric Type よりも優先されます。
IPv6 デフォルト ルート	プロファイルのこの部分の構成を許可する場合に選択 します。
Always	ルーターにデフォルト経路がない場合でも、IPv6 デ フォルト経路を常に作成して OSPFv3 に再配布する場 合に選択します。デフォルトは有効になっています。
Enable [有効化]	プロファイルの IPv6 Default Route 部分を有効にしま す。
メトリック	OSPFv3に再配布されるIPV6省略時経路に適 用するMetricを指定してください(範囲は0か ら4,294,967,295です)。
メトリックの種類	Type 1 または Type 2 を選択します。

Network > Routing > Routing Profiles > RIPv2 [ネットワーク>ルー ティング>ルーティングプロファイル > RIPv2]

RIPv2 ルーティング・プロファイル を追加して、論理ルーター用に RIPv2 を効率的に構成します。

RIPv2 ルーティングプロファイル	の意味
RIPv2 グローバル タイマー プロファイル	
氏名	プロファイルの名前を入力します(最大 63 文 字)。名前は、英数字、アンダースコア(_)、 またはハイフン(-)で始まり、0個以上の英数 字、アンダースコア(_)、またはハイフン(-) を含む必要があります。ドット(.)またはス ペースは使用できません。
更新間隔	定期的にスケジュールされたルーティング更 新メッセージ間の秒数を入力します。範囲は 5~2,147,483,647です。デフォルトは 30で す。

RIPv2 ルーティングプロファイル	の意味
Expire Interval (有効期限間隔)	ルートが更新されずにルーティング テーブ ルに存在できる秒数を入力します。範囲は 5 ~ 2,147,483,647 です。デフォルトは 180 で す。有効期限間隔に達した後も、Delete 間隔 に達するまで、ルートは更新メッセージに含 まれます。
Delete Interval (削除間隔)	Delete Interval に秒数を入力します。範囲は 5 ~ 2,147,483,647 です。デフォルトは 120 です。ルーティング テーブル内の期限切れ のルートが Delete Interval に達すると、ルー ティング テーブルから削除されます。
RIPv2 認証プロファイル	
氏名	プロファイルの名前を入力します(最大 63 文 字)。名前は、英数字、アンダースコア(_)、 またはハイフン(-)で始まり、0 個以上の英数 字、アンダースコア(_)、またはハイフン(-) を含む必要があります。ドット(.)またはス ペースは使用できません。
タイプ	認証の種類として、md5 (RIP MD5 認証方式 を使用) または パスワード (簡易パスワード認 証) を選択します。
パスワード	(簡易パスワード認証) パスワード (最大 16 文 字) と Confirm Password を入力します。
MD5	(<mark>RIP MD5 認証</mark>)MD5 キー ID を入力します。 範囲は 0 ~ 255 です。
キー	(RIP MD5 認証) MD5 キー (最大 16 文字) と キーの確認 を入力します。
パケットを送信するときにこのキーを使用し ます	(RIP MD5 認証)このキーを Preferred キーに する場合に選択します。
RIPv2 再配布プロファイル	·
氏名	プロファイルの名前を入力します (最大 63 文 字)。名前は、英数字、アンダースコア (_)、 またはハイフン (-) で始まり、0 個以上の英数 字、アンダースコア (_)、またはハイフン (-)

RIPv2 ルーティングプロファイル	の意味
	を含む必要があります。ドット (.) またはス ペースは使用できません。
IPv4 スタティック	プロファイルのこの部分の構成を許可する場 合に選択します。
有効 (既定) または無効にする	プロファイルのIPv4静的部分を有効にしま す。
メトリック	RIPv2に再配布される静的経路に適用す るMetricを指定してください(範囲は1か ら65,535です)。
ルートマップ	Redistribution Route Map を選択または作成 して、RIPv2 に再配布される IPv4 静的経路を 制御し、それらの属性を設定します。デフォ ルト設定は None (なし) です。ルートマッ プセットの設定に Metric Action と Metric Value が含まれている場合、それらは再配布 ルートに適用されます。それ以外の場合は、 この再配布プロファイルで構成されたメト リックが再配布ルートに適用されます。
接続済み	プロファイルのこの部分の構成を許可する場 合に選択します。
有効 (既定) または無効にする	プロファイルの接続部分を有効にします。
メトリック	RIPv2に再配布される接続経路に適用す るMetricを指定してください(範囲は1か ら65,535です)。
ルートマップ	Redistribution Route Map を選択または作成 して、どの接続経路を RIPv2 に再配布する かを制御し、その属性を設定します。デフォ ルト設定は None (なし) です。ルートマッ プセットの設定に Metric Action と Metric Value が含まれている場合、それらは再配布 ルートに適用されます。それ以外の場合は、 この再配布プロファイルで構成されたメト リックが再配布ルートに適用されます。
BGP AFI IPv4	プロファイルのこの部分の構成を許可する場 合に選択します。

RIPv2 ルーティングプロファイル	の意味
有効 (既定) または無効にする	プロファイルの BGP AFI IPv4 部分を有効に します。
メトリック	RIPv2 に再配布される BGP IPv4 経路に適用 する Mectric を指定してください (範囲は 0 から 4,294,967,295)。
ルートマップ	Redistribution Route Map を選択または作成 して、RIPv2 に再配布される BGP IPv4 経 路を制御し、それらの属性を設定します。 デフォルト設定は None (なし) です。ルー トマップセットの設定に Metric Action と Metric Value が含まれている場合、それらは 再配布ルートに適用されます。それ以外の場 合は、この再配布プロファイルで構成された メトリックが再配布ルートに適用されます。
OSPFv2	プロファイルのこの部分の構成を許可する場 合に選択します。
有効 (既定) または無効にする	プロファイルの OSPFv2 部分を有効にしま す。
メトリック	RIPv2に再配布されるOSPFv2経路に適用 するMetricを指定してください(範囲は0か ら4,294,967,295です)。
ルートマップ	Redistribution Route Map を選択または作成 して、RIPv2 に再配布される OSPFv2 経路を 制御し、それらの属性を設定します。デフォ ルト設定は None (なし) です。ルートマッ プセットの設定に Metric Action と Metric Value が含まれている場合、それらは再配布 ルートに適用されます。それ以外の場合は、 この再配布プロファイルで構成されたメト リックが再配布ルートに適用されます。

Network > Routing > Routing Profiles > Filters [ネットワー ク>ルーティング>ルーティングプロファイル>フィルタ]

Add filters をプロファイルに適用し、たとえば、RIB へのルート受け入れ、ピアへのルート通知、条件付き通知、設定属性、ルート集約、ルート再配布などを制御する設定を簡単かつ一貫して適用します。

フィルタ	の意味
フィルタ アクセス リスト	
氏名	アクセス・リストの名前を入力します(最大63文字)。名 前は、英数字、アンダースコア(_)、またはハイフン(-) で始まり、0個以上の英数字、アンダースコア(_)、また はハイフン(-)を含む必要があります。ドット(.)または スペースは使用できません。
の意味	説明を入力します。
タイプ	IPv4 または IPv6を 選択します。
Seq	 Add エントリ(ルール)を作成し、このアクセスリストの ルールのリストにルールのシーケンス番号を入力しま す。範囲は 1 ~ 65,535 です。 シーケンス番号の間に未使用の番号を残し て、後で追加のルールを挿入できるように します。
操作	エントリに Deny または Permit を選択します。アクセス リストは暗黙的な Deny Any で終わります。
送信元アドレス	 (IPv4 のみ)次のいずれかを選択します。 Address - 後続の Address フィールドに IPv4 アドレスを入力し、Wildcard マスクを入力してアドレスの範囲を示します。マスク内のゼロ (0) は、そのビットがアドレス内の対応するビットと一致しなければならないことを示します。マスク内の1(1)は、「Don't care (ケアしない)」ビットを示します。 任意 なし
宛先アドレス	 (IPv4 のみ)次のいずれかを選択します。 Address - 後続の Address フィールドに IPv4 アドレスを入力し、Wildcard マスクを入力してアドレスの範囲を示します。マスク内のゼロ (0) は、そのビットがアドレス内の対応するビットと一致しなければならないことを示します。マスク内の1(1)は、「Don't care (ケアしない)」ビットを示します。 任意

フィルタ	の意味
	 なし
送信元アドレス	(IPv6 のみ)次のいずれかを選択します。
	 Address – 後続の Address フィールドに、IPv6 アドレスを入力します。 任音
	 なし
このアドレスの完全一致	(IPv6 のみ)IPv6 送信元アドレスの完全一致のみに一致 する場合に選択します。Source Address が Any または None の場合は使用できません。
フィルタ プレフィックス リスト	
氏名	接頭部リストの名前を入力します (最大 63 文字)。名前 は、英数字、アンダースコア (_)、またはハイフン (-) で 始まり、0 個以上の英数字、アンダースコア (_)、または ハイフン (-) を含む必要があります。ドット (.) またはス ペースは使用できません。
の意味	説明を入力します。
タイプ	IPv4 または IPv6を 選択します。
Seq	Add エントリ (ルール) を作成し、このプレフィックス リ ストのルールのリストにルールのシーケンス番号を入力 します。範囲は 1 ~ 65,535 です。
	シーケンス番号の間に未使用の番号を残して、後で追加のルールを挿入できるようにします。
操作	エントリに Deny または Permit を選択します。プレ フィックス リストは、暗黙的な Deny Any で終わりま す。
プレフィックス	以下のいずれかを選択します。
	 Network any (ネットワーク任意)
	 Entry – IPv4 または IPv6 Network をスラッシュと プレフィックス長で入力します。オプションで、プ レフィックスの長さを Greater Than or Equal にす る必要があるプレフィックス長を入力します (範囲 は、IPv4 の場合は 0~32、IPv6 の場合は 0~128)。

フィルタ	の意味
	オプションで、プレフィックスの長さを Less Than or Equal にする必要があるプレフィックス長を入力 します (範囲は、IPv4 の場合は 0 ~ 32、IPv6 の場合 は 0 ~ 128)。たとえば、プレフィックス長が 25 以 上、プレフィックス長が 26 以下のネットワークが 192.168.3.0/24 と入力します。 • なし

AS パス アクセス リストをフィルタ

氏名	AS パス アクセス・リストの名前を入力します(最大63文 字)。名前は、英数字、アンダースコア (_)、またはハイフ ン (-) で始まり、0 個以上の英数字、アンダースコア (_)、 またはハイフン (-) を含む必要があります。ドット (.) ま たはスペースは使用できません。
の意味	説明を入力します。
Seq	 Add エントリ(ルール)を作成し、このアクセスリストの ルールのリストにルールのシーケンス番号を入力しま す。範囲は1~65,535です。 シーケンス番号の間に未使用の番号を残し て、後で追加のルールを挿入できるように します。
操作	エントリに Deny または Permit を選択します。 AS パスアクセスリストは、暗黙的な Permit Any ルールで終わります。AS パス アクセスリストを使用して、自律システム を拒否します。
AS パス 正規表現	AS パスに正規表現を入力します。

フィルタ コミュニティ リスト

氏名	コミュニティー・リストの名前を入力します(最大 63 文 字)。名前は、英数字、アンダースコア(_)、またはハイフ ン(-) で始まり、0個以上の英数字、アンダースコア()
	またはハイフン (-) を含む必要があります。ドット (.) またはスペースは使用できません。

フィルタ	の意味
の意味	コミュニティー・リストの説明を入力します。
タイプ	Regular、Large、または Extended コミュニティを選択 します。
Seq	Add エントリ (ルール) を作成し、このリストのルールの リストにルールのシーケンス番号を入力します。範囲は 1~65,535 です。 ② シーケンス番号の間に未使用の番号を残し て、後で追加のルールを挿入できるように します。
操作	Deny または Permit を選択します。リストは暗黙の Deny Any ルールで終わります。
コミュニティ	リストから既知のコミュニティーの1つを選択するか、 コミュニティーを入力します。
	ž

ルート マップ BGP のフィルタリング

氏名	BGP ルート マップの名前を入力します(最大 63 文字)。 名前は、英数字、アンダースコア (_)、またはハイフン (-) で始まり、0 個以上の英数字、アンダースコア (_)、また はハイフン (-) を含む必要があります。ドット (.) または スペースは使用できません。
の意味	ルートマップの説明を入力します。

Entry Tab 入力タブ

Seq	Add エントリ (ルール) を作成し、このルート マップの ルールのリストにルールのシーケンス番号を入力しま す。範囲は 1 ~ 65,535 です。
	シーケンス番号の間に未使用の番号を残して、後で追加のルールを挿入できるようにします。
の意味	ルートマップエントリの説明を入力します。
操作	Deny または Permit を選択します。

フィルタ	の意味
Match Tab 「マッチ」タブ	
ASパスアクセスリスト	AS パス アクセス リストを選択します。
定期的なコミュニティ	一致基準のコミュニティー・リストを選択します。
大規模なコミュニティ	一致基準のコミュニティー・リストを選択します。
拡張コミュニティ	一致基準のコミュニティー・リストを選択します。
メトリック	メトリックを入力します。範囲は 0 ~ 4,294,967,295 で す。
インターフェイス	インターフェイスを選択します。
元	egp, igp, incomplete, or none を選択します。
タグ	タグを入力します。範囲は 1 ~ 4,294,967,295 です。
ローカル設定	ローカルプリファレンスを入力します。範囲は0~ 4,294,967,295 です。
ピア	ローカル (Static または Redistributed Routes) または none を選択します。
IPv4 / IPv6	照合するアドレス ファミリとして IPv4 または IPv6 を選 択します。
Address-Access List	照合するアドレスを指定するアクセス リストを選択しま す。デフォルト設定は None (なし) です。
Address—Prefix List	照合するプレフィックスを指定するプレフィックス リス トを作成します。これは、ピアから受信したプレフィッ クス、または別のプロトコルから再配布されたプレ フィックスと一致します。デフォルト設定は None (なし) です。
Next Hop—Access List	照合するネクストホップを指定するアクセス リストを選 択します。デフォルト設定は None (なし) です。
Next Hop—Prefix List	照合するネクストホップを指定するプレフィックスリス トを選択します。デフォルト設定は None (なし) です。

フィルタ	の意味
Route Source–Access List	(IPv4 のみ)照合するルート ソースを指定するアクセス リストを選択します。デフォルト設定は None (なし) で す。
Route Source–Prefix List	(IPv4 のみ)照合するルート ソースを指定するプレフィッ クス リストを選択します。デフォルト設定は None (な し) です。
Set Tab ([設定] タブ)	
BGP アトミック集約を有効にす る	ルートは集約されているため、そのルートを あまり具体性の低いルートとしてマークしま す。ATOMIC_AGGREGATEは、ルート集約のために情 報が失われたことをパスに沿って BGP スピーカーに警 告するよく知られた任意属性であるため、集約パスが 宛先への最適なパスではない可能性があります。一部 のルーターがアグリゲーターによって集約されると、 アグリゲーターは集約されたルートにルーター ID を AGGREGATOR-ID 属性にアタッチし、集約されたルー ターからのATOMIC_AGGREGATE情報が保持されたかど うかに基づいて、AS_PATH 属性を設定します。
Aggregator—Aggregate AS	Aggregator AS を入力します。Aggregator 属性には、集約ルートを発信したルーターの AS 番号と IP アドレスが含まれます。IP アドレスはルート集約を実行するルータの Router ID です。範囲は 1 ~ 4,294,967,295 です。
Aggregator—Router ID	アグリゲーターの Router ID (通常はループバック・アド レス) を入力します。
IPv4 / IPv6	設定する住所のタイプを選択します。
IPv6 ネクストホップ優先グロー バル アドレス	(IPv6 のみ)IPv6 には、リンク ローカル アドレス、グロー バル ユニキャスト アドレス、エニーキャスト アドレ ス、マルチキャスト アドレスの 4 つのアドレス タイプ があります。IPv6 Nexthop Prefer Global Address によ り、firewall はグローバル ユニキャスト アドレスを優先 します。
送信元アドレス	設定する/プレフィックス長のソースアドレスを選択しま す。
IPv4 ネクストホップ	(IPv4 のみ) none、peer-address (use Peer Address)、または unchanged を選択します。

フィルタ	の意味
IPv6 ネクストホップ	(IPv6 のみ) none または peer-address (Use Peer Address) を選択します。
ローカル設定	ローカル設定を入力します。範囲は 0 ~ 4,294,967,295 です。
タグ	タグを入力します。範囲は 1 ~ 4,294,967,295 です。
メトリックアクション	None, set, add, または subtract を選択します。
メトリック値	メトリックを入力します。範囲は 0 ~ 4,294,967,295 で す。
重み	重量を入力します。範囲は 0 ~ 4,294,967,295 です。
元	egp , igp , incomplete , or none を選択します。
発信者 ID	オリジネーター ID を設定します。
通常のコミュニティの削除	削除する Regular Comunity を入力します。
大規模なコミュニティの削除	削除する Large Comunity を入力します。
Regular Community–Overwrite Regular Community (Regular Community – 通常のコミュニ ティを上書きする)	Regular Comunity を Regular Community フィールドで追加されたもので上書きする場合に選択します。
定期的なコミュニティ	Regular Comunityを追加します。
Large Community—Overwrite Regular Community	Large Community フィールドで追加されたもので Large Community を上書きする場合に選択します。
大規模なコミュニティ	Large Community を追加します。
ASPath Exclude (ASPath 除外)	除外するAS_PATHを追加します。
AS パス プリペンド	先頭にAS_PATHを追加します。

ルート マップの再配布をフィルタ

氏名

Redistribution 経路マップの名前を入力します(最大 63 文字)。名前は、英数字、アンダースコア(_)、またはハ イフン(-)で始まり、0個以上の英数字、アンダースコア

フィルタ	の意味
	(_)、またはハイフン (-) を含む必要があります。ドット (.) またはスペースは使用できません。
の意味	ルートマップの説明を入力します。
ソースプロトコル	再配布するソースプロトコルを選択します。
宛先プロトコル	ルートを再配布するプロトコルを選択します。
Entry (エントリ)	
Seq	シーケンス番号を入力します。範囲は1~65,535です。
	シーケンス番号の間に未使用の番号を残して、後で追加のルールを挿入できるようにします。
の意味	ルート マップ ルールの説明を入力します。
操作	Deny または Permit 一致するルートが再配布されなくなります。
一致	
AS パス アクセス リスト	AS パス アクセス リストを選択します。
定期的なコミュニティ	通常のコミュニティに入ります。
大規模なコミュニティ	大規模なコミュニティに入ります。
拡張コミュニティ	拡張コミュニティに入る
メトリック	範囲は 0 ~ 4,294,967,295 です。
インターフェイス	インターフェイスを選択します。
元	egp, igp, incomplete, or none を選択します。
タグ	タグを入力します。範囲は 1 ~ 4,294,967,295 です。
ローカル設定	ローカルプリファレンスを入力します。範囲は 0 ~ 4,294,967,295 です。

フィルタ	の意味
ピア	ローカル (静的または Redistributed Routes) または none を選択します。
Address—Access List	アクセスリストを選択します。
Address-Prefix List	プレフィックス リストを選択します。
Next Hop—Access List	アクセスリストを選択します。
Next Hop—Prefix List	プレフィックス リストを選択します。
Route Source–Access List	アクセスリストを選択します。
Route Source-Prefix List	プレフィックス リストを選択します。

セット

メトリックアクション	None, set, add, または subtract を選択します。
メトリック値	Metric Action の選択に基づいて、メトリック先の値を set に、メトリックに add に、または一致するルートの メトリックから subtract の値を入力します。範囲は 0 ~ 4,294,967,295 です。
メトリックの種類	Type 1 または Type 2 を選択します。
タグ	範囲は 1 ~ 4,294,967,295 です。

Network > Routing > Routing Profiles > Multicast [ネットワー ク>ルーティング > マルチキャスト>ルーティングプロファイル]

マルチキャスト・ルーティング・プロファイルを追加して、論理ルーターの IPv4 マルチキャストを効率的に構成します。

Multicast Routing Profiles (マ ルチキャストルーティングプロ ファイル)	詳説
フルチナッフト IDVA DIM インタ	ニフェノフ カノフニ プロファノル

マルチキャスト IPv4 PIM インターフェイス タイマー プロファイル

名前

プロファイルの名前を入力します (最大 31 文字)。名前は、 英数字、アンダースコア (_)、またはハイフン (-) で始ま り、0 個以上の英数字、アンダースコア (_)、またはハイフ

Multicast Routing Profiles (マ ルチキャストルーティングプロ ファイル)	詳説
	ン (-) を含む必要があります。ドット (.) またはスペースは使 用できません。
アサート間隔	論理ルータがマルチアクセス ネットワーク上の他の PIM ルータに PIM フォワーダを選択しているときに送信する PIM Assert メッセージ間の秒数を入力します。範囲は 1 か ら 65,534 です。デフォルトは 177 です。
送信間隔	論理ルータがインターフェイス グループ内の各インター フェイスから PIM ネイバーに送信する PIM Hello メッセー ジ間隔(秒)を入力します。範囲は 1 ~ 180 です。デフォ ルトは 30 です。
プルーン インターバル に ジョ インする	論理ルータがマルチキャスト ソースに向けてアップスト リームに送信する PIM 結合メッセージ間(および PIM プ ルーン メッセージ間)の秒数を入力します。範囲は 60 ~ 600 です。デフォルトは 60 です。
マルチキャスト IPv4 IGMP インターフェイス クエリ プロファイル	
名前	プロファイルの名前を入力します (最大 31 文字)。名前は、 英数字、アンダースコア (_)、またはハイフン (-) で始ま り、0 個以上の英数字、アンダースコア (_)、またはハイフ ン (-) を含む必要があります。ドット (.) またはスペースは使 用できません。
最大クエリ応答時間	受信側がグループのマルチキャストパケットの受信を希望 しないと論理ルータが判断するまでに、IGMP メンバーシッ プクエリメッセージに受信者が応答できる最大秒数を入力 します。範囲は 1~25 です。デフォルトは 10 です。
クエリ間隔	IGMP メンバーシップ間の秒数を入力します 論理ルータが 受信側に送信するメッセージに問い合わせて、受信側がグ ループのマルチキャスト パケットを引き続き受信するかど うかを判断します。範囲は 1 ~ 1,800 です。デフォルトは 125 です。
Last Member Ouery Interval	受信側が Leave Group メッセージを送信した後に論理ルー

受信側が Leave Group メッセージを送信した後に論理ルー ターが送信する Group-Specific Query に受信者が応答でき る秒数を入力します。範囲は 1~25 です。デフォルトは 1 です。
です。

Multicast Routing Profiles (マ ルチキャストルーティングプロ ファイル)	詳説
退会メッセージを受信したら すぐにグループを離れる	これを有効にすると、マルチキャストグループにメンバー が1つしかなく、論理ルータがそのグループの IGMP Leave メッセージを受信すると、この設定により、論理ルータ は Last Member Query Interval の有効期限が切れるのを 待つのではなく、マルチキャストルーティング情報ベー ス(mRIB)およびマルチキャスト転送情報ベース(mFIB)からそ のグループと発信インターフェイスを直ちに削除します。 この設定を有効にすると、ネットワークリソースが節約さ れます。デフォルトは無効です。

マルチキャスト MDSP 認証プロファイル

名前	MSDP 認証プロファイルを名前で追加します(最大 63 文 字)。名前は英数字、アンダースコア (_)、またはハイフン (-) で始まる必要があり、英数字、アンダースコア、またはハ イフンの組み合わせを含めることができます。ドット (.) ま たはスペースは使用できません。
シークレット	シークレットを入力します(英数字、!、@、#、%、およ び^を使用できます)。Confirm Secret.

マルチキャスト MDSP タイマー プロファイル

名前	MSDP タイマー プロファイルを名前で追加します(最大 63 文字)。名前は英数字、アンダースコア (_)、またはハイフン (-) で始まる必要があり、英数字、アンダースコア、または ハイフンの組み合わせを含めることができます。ドット (.) またはスペースは使用できません。
キープ アライブ間隔	値を秒単位で入力します。範囲は1から60です。デフォ ルトは60です。ピアとのMSDPトランスポート接続が確 立されると、接続の各側はこの間隔でキープアライブメッ セージを相手側送信して、MSDPセッションをアクティブ に保ちます。タイマーが期限切れになると、ピアはキープ アライブメッセージを送信し、タイマーをリセットしま す。メッセージタイムアウト間隔中にキープアライブメッ セージまたはSAメッセージが受信されない場合、MSDP セッションはリセットされます。
メッセージ タイムアウト	MSDP ピアが他のピアからのキープアライブ メッセージを 待機してからダウンを宣言する間隔の値を秒単位で入力し ます。範囲は1から75です。デフォルトは75です。

Multicast Routing Profiles (マ ルチキャストルーティングプロ ファイル)	詳説
接続再試行間隔	ピアリング セッションがリセットされてからピアリング セッションの再確立を試みるまでの待機間隔の値を秒単位 で入力します。範囲は1から60です。デフォルトは30で す。

Network > IPSec Tunnels [ネットワーク > IPSec トンネ ル]

Network > IPSec Tunnels[ネットワーク > IPSec トンネル] を使用して、ファイアウォール間の IPSec VPNトンネルを設定および管理します。これは、IKE/IPSec VPN セットアップのフェーズ 2 の部分です。

確認すべき情報	以下を参照
IPSec VPN トンネルを管理す る。	IPSec VPN トンネル管理
IPSec トンネルを設定する。	IPSec トンネルの [全般] タブ
	IPSec トンネルの Proxy IDs(プロキシ ID)タブ
IPSec トンネルの状態を表示 する。	ファイアウォールの IPSec トンネル状態
IPSec トンネルを再起動また は更新する。	IPSec トンネルの再起動または更新
その他の情報をお探しです か?	IPSec トンネルのセットアップ

IPSec VPN トンネル管理

• Network > IPSec Tunnels [ネットワーク > IPSec トンネル]

以下の表は、IPSec VPN トンネルの管理方法を示しています。

IPSec VPN トンネルを管理するフィールド	
コンテキストの	新しい IPSec VPN トンネルを Add(追加)します。新しいトンネル の設定方法については「IPSec トンネルの General(全般)タブ」を 参照してください。
削除します。	不要になったトンネルを Delete(削除)します。
Enable [有効化]	無効になっていたトンネルを Enable(有効化)します(トンネルは デフォルトで有効化されます)。

IPSec VPN トンネルを管	理するフィールド
無効化	使用しておらず、まだ削除できないトンネルを Disable (無効化)し ます。
PDF/CSV	PDF/CSV 形式のすべての IPSec トンネル設定をエクスポートしま す。フィルタを適用してテーブルの出力をカスタマイズし、必要な 列のみを含めることができます。エクスポート ダイアログに表示 される列のみがエクスポートされます。Export Configuration Table Data(設定バンドルデータのエクスポート)を参照してください。

IPSec トンネルの [全般] タブ

• Network (ネットワーク) > IPSec Tunnels (IPSec トンネル) > General (全般)

IPSec トンネルをセットアップするには、次のフィールドを使用します。

IPSec トンネルの全般設 定	の意味
氏名	トンネルを識別する Name(名前)を入力します(最大 63 文 字)。名前の大文字と小文字は区別されます。また、一意の名前に する必要があります。文字、数字、スペース、ハイフン、およびア ンダースコアのみを使用してください。
	このフィールドの制限文字数の 63 文字には、ブロキシ ID およびト ンネル名が含まれ、コロンで区切られています。
トンネルインターフェ イス	既存のトンネルインターフェイスを選択するか、New Tunnel Interface[新規トンネルインターフェイス]をクリックします。ト ンネルインターフェイスの作成の詳細は「Network(ネットワー ク)> Interfaces(インターフェイス)> Tunnel(トンネル)」を参 照してください。
IPv4 / IPv6	IPv4 または IPv6 を選択し、トンネルのエンドポイントの IP アドレス タイプを設定します。
タイプ	自動的に生成されるセキュリティ キーを使用するのか、手動で入力 するセキュリティ キーを使用するのかを選択します。Auto key[自 動キー] を使用することをお勧めします。
自動キー	Auto Key[自動キー]を選択する場合、以下の内容を指定します。
	 IKE Gateway (IKE ゲートウェイ) – IKE ゲートウェイの設定の 詳細は「Network (ネットワーク) > Network Profiles (ネット ワーク プロファイル) > IKE Gateways (IKE ゲートウェイ)」 を参照してください。

Π

PSec トンネルの全般設 E	の意味
	 IPSec Crypto Profile[IPSec 暗号化プロファイル] – 既存のプロファイルを選択するか、デフォルトのプロファイルを使用します。新しいプロファイルを定義するには、New(新規)をクリックし、「Network (ネットワーク) > Network Profiles (ネットワークプロファイル) > IPSec Crypto (IPsec 暗号)」の指示に従ってください。
	 Show Advanced Options[詳細オプションの表示] をクリックする と、残りのフィールドにアクセスできます。
	 Enable Replay Protection (リプレイ プロテクションを有効にする) – リプレイ攻撃から保護する場合に選択します。
	リプレイ防止は IPSec のサブプロトコルであり、インターネット技術標準化委員会 (IETF) コメントの要求 (RFC) 6479 の一部です。アンチリプレイ プロトコルは、ハッカーが送信元から宛先に移動するパケットを挿入または変更するのを防ぐために使用され、ネットワーク内の2つのノード間の安全な接続を確立するために、単方向セキュリティアソシエーションを使用します。
	セキュリティで保護された接続が確立されると、アンチリプレ イプロトコルはパケットシーケンス番号を使用してリプレイ攻 撃を打ち破ります。送信元がメッセージを送信すると、パケッ トにシーケンス番号が追加されます。シーケンス番号は0から 始まり、後続のパケットごとに1ずつ増分されます。宛先は、 スライディングウィンドウ 形式の番号のシーケンスを保持し、 検証された受信パケットのシーケンス番号のレコードを保持 し、スライディング ウィンドウの最下位(古すぎるパケット)ま たは既にスライディング ウィンドウに表示されているパケット (複製または再生パケット)よりも低いシーケンス番号を持つすべ てのパケットを拒否します。受け入れられたパケットは、検証 後にスライディング ウィンドウを更新し、ウィンドウの中で最 も低いシーケンス番号が既に満杯の場合は、その番号を置き換 えます。
	再生保護を有効にする場合は、使用するのアンチリプレイウィンドウを選択します。64、128、256、512、1024、2048、または4096のアンチリプレイウィンドウサイズを選択できます。 デフォルトは1024です。
	 Copy TOS Header[TOS ヘッダーのコピー] – 元の TOS 情報を保持するため、カプセル化されたパケットの内部 IP ヘッダーから外部 IP ヘッダーに TOS (Type of Service) フィールドをコピーします。ECN(Explicit Congestion Notification) フィールドもコピーされます。
IPSec トンネルの全般設 定	の意味
----------------------------	--
	 IPSec Mode - IPSec モードを指定します。ヘッダーを含むパケット全体を暗号化するには、Tunnel モードを選択します。暗号化後、新しい IP ヘッダーがパケットに追加されます。ペイロードのみを暗号化し、元の IP ヘッダーを保持するには、Transport モードを選択します。
	 Add GRE Encapsulation (GRE カプセル化の追加)–IPSec トンネル 内でカプセル化された GRE ヘッダーを追加する場合に選択しま す。ファイアウォールは他のベンダーのトンネル エンドポイン トとの相互運用性を確保するために IPSec ヘッダーの後で GRE ヘッダーを生成します。つまり、GRE トンネルを IPSec トンネ ルと共有します。
	 Tunnel Monitor(トンネルモニター) – デバイス管理者にトンネルの障害についてアラートを送信し、別のインターフェイスへの自動フェイルオーバーを実行する場合に選択します。
	モニタニングする場合は、トンネルインターフェ イスに IP アドレスを割り当てる必要があります。
	 Destination IP[宛先 IP] – トンネルが正常に動作しているかどうかを判別するためにトンネルモニターが使用する、トンネルの反対側の IP アドレスを指定します。
	 Profile[プロファイル] – トンネルで障害が発生した場合に実行されるアクションを決める、既存のプロファイルを選択します。モニタープロファイルに指定されたアクションが待機/回復の場合、ファイアウォールは、トンネルが機能するようになるまで待機し、ルートテーブルで代替パスを探すことはしません。フェイルオーバーアクションを使用する場合、ファイアウォールはルートテーブルを調べ、宛先に到達するために使用できる代替ルートがないか確認します。詳細は「Network(ネットワーク)> Network Profiles(ネットワークプロファイル)> Monitor(監視)」を参照してください。
手動キー	Manual Key[手動キー] を選択する場合、以下の内容を指定します。
	 Local SPI[ローカル SPI] – ローカル ファイアウォールからピア へのパケット トラバーサルのローカル セキュリティ パラメータ インデックス (SPI) を指定します。SPI は、IPSec トラフィック フローの区別を支援するために IPSec トンネルのヘッダーに追加 されている 16 進インデックスです。
	 Interface[インターフェイス] – トンネルの終端であるインター フェイスを選択します。
	 Local Address[ローカル アドレス] – トンネルの終端となるロー カル インターフェイスの IP アドレスを選択します。

IPSec トンネルの全般設 定	の意味		
	 Remote SPI[リモート SPI] – リモート ファイアウォールからピアへのパケット トラバーサルのリモート セキュリティ パラメータ インデックス (SPI) を指定します。 		
	 Protocol[プロトコル] – トンネルを経由するトラフィックのプロ トコルを選択します (ESP または AH)。 		
	 Authentication[認証] – トンネル アクセスの認証タイプを選択します (SHA1、SHA256、SHA384、SHA512、MD5、またはなし)。 		
	 Key/Confirm Key[キー/確認キー] – 認証鍵を入力して確認します。 		
	 Encryption[暗号化] – トンネル トラフィックの暗号化オプションを3des、aes-128-cbc、aes-192-cbc、aes-256-cbc、des、またはnull [暗号化なし] の中から選択します。 		
	 Key/Confirm Key[キー/確認キー] – 暗号化鍵を入力して確認します。 		
GlobalProtectサテライ ト	GlobalProtect Satellite[GlobalProtect サテライト]を選択する場合は、以下の設定項目を指定します。		
	• Name[名前] – トンネルを識別する名前を入力します (最大 31 文 字)。名前の大文字と小文字は区別されます。また、一意の名前 にする必要があります。文字、数字、スペース、ハイフン、お よびアンダースコアのみを使用してください。		
	 Tunnel Interface(トンネルインターフェイス) – 既存のトンネルインターフェイスを選択するか、New Tunnel Interface(新規トンネルインターフェイス)をクリックします。 		
	 Portal Address (ポータルアドレス) – GlobalProtect[™] ポータ ルの IP アドレスを入力します。 		
	 Interface(インターフェイス) – ドロップダウン リストから、GlobalProtect ポータルに到達するための出力インターフェイスを選択します。 		
	 Local IP Address(ローカル IP アドレス) – GlobalProtect ポー タルに接続する出力インターフェイスの IP アドレスを入力しま す。 		
	• 詳細オプション		
	 Publish all static and connected routes to Gateway(静的なすべての接続済みルートをゲートウェイに公開) – サテライトが接続されている GlobalProtect ゲートウェイにすべてのルートを公開する場合に選択します。 		

IPSec トンネルの全般設 定	の意味
	 Subnet[サブネット] – Add[追加] をクリックして、サテライトの 場所のローカル サブネットを手動で追加します。他のサテライ トが同じサブネット情報を使用している場合は、すべてのトラ フィックをそのトンネル インターフェイス IP に NAT を行う必 要があります。また、この場合はサテライトがルートを共有す ることはできないため、すべてのルーティングはトンネル IP を 介して行われます。
	 External Certificate Authority(外部認証局) – 外部 CA を使用して証明書を管理する場合に選択します。証明書を生成した後は、それらの証明書をサテライトにインポートし、Local Certificate[ローカル証明書]および Certificate Profile[証明書プロファイル]の選択が必要になります。

IPSec トンネルの Proxy IDs (プロキシ ID) タブ

• Network (ネットワーク) > IPSec Tunnels (IPSec トンネル) > Proxy IDs (プロキシ ID)

IPSec Tunnel Proxy IDs[IPSecトンネルの プロキシID] は、以下の2つのタブに分かれていま す。IPv4 および IPv6どちらのタイプもヘルプは同様の内容です。IPv4 と IPv6 の違いは、以下 の表の Local[ローカル] フィールドと Remote[リモート] フィールドに示されています。

IPSec Tunnel Proxy IDs[IPSecトンネルの プロキシID] タブは、IKEv2 のトラフィック セレクタ を指定する場合にも使用されます。

プロキシ ID IPv4 および IPv6 の設定	の意味
プロキシ ID	Add[追加] をクリックし、プロキシを識別する名前を入力します。 IKEv2 トラフィック セレクタの場合、このフィールドは名前として 使用されます。
ローカル	 IPv4の場合:x.x.x./maskの形式(たとえば、10.1.2.0/24)でIPアドレスまたはサブネットを入力します。 IPv6:IPアドレスとプレフィックス長を xxx::xxx::xxx::xxx::xxx::xxx::xxx:/prefix-length 形式で入力します(つまり、IPv6の規則に従い、たとえば、2001:DB8:0::/48のように入力します)。
	IPv6 アドレッシングでは、すべてのゼロを記述する必要はありません。先行するゼロは省略でき、連続するゼロの1つのグループは隣り合う2つのコロン (::) で置き換えることができます。

プロキシ ID IPv4 および IPv6 の設定	の意味	
	IKEv2 トラフィック セレクタの場合、このフィールドは送信元 IP アドレスに変換されます。	
リモート	ピアで必要な場合は、以下のようにします。 IPv4 の場合: IP アドレスまたはサブネットを x.x.x.x/mask 形式で入	
	力します (たとえば、10.1.1.0/24 のように入力します)。	
	iFV0 00場合は、iF / Fレスと/レノイ///入設を xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/prefix-length 形式で入力し ます (つまり、IPv6 の規則に従い、たとえば、2001:DB8:55::/48 の ように入力します)。	
	IKEv2 トラフィック セレクタの場合、このフィールドは宛先 IP ア ドレスに変換されます。	
PROTOCOL	ローカルおよびリモート ポートのプロトコルとポート番号を指定し ます。	
	Number – プロトコル番号 (サードパーティ デバイスとの相互運用 性を実現するために使用) を指定します。	
	• Any – TCP や UDP トラフィックを許可します。	
	 TCP – ローカルおよびリモートの TCP ポート番号を指定します。 	
	 UDP – ローカルおよびリモートの UDP ポート番号を指定します。 	
	設定された各プロキシ ID は、ファイアウォールの IPSec VPN トン ネル容量に影響しません。	
	このフィールドは、IKEv2 トラフィック セレクタとしても使用され ます。	

ファイアウォールの IPSec トンネル状態

• Network > IPSec Tunnels [ネットワーク > IPSec トンネル]

現在定義されている IPSec VPN トンネルの状態を表示するには、IPSec Tunnels[IPSec トンネル] ページを開きます。このページには、以下の状態情報が表示されます。

- Tunnel Status (first status column) (トンネルの状態(最初の状態列)) 緑は、IPSec フェーズ 2 セキュリティ アソシエーション (SA) トンネルを表します。赤は、IPSec フェーズ 2 SA が使 用できないか、有効期限が切れていることを表します。
- IKE Gateway Status (IKE ゲートウェイの状態) 緑は、IKE フェーズ1SA または IKEv2 IKE SA が有効であることを表します。赤は、IKE フェーズ1SA が使用できないか、有効期限が 切れていることを表します。

 Tunnel Interface Status (トンネル インターフェイスの状態) – 緑は (トンネル モニターが 無効である、またはトンネル モニターの状態がアップでありモニタリング IP アドレスにアク セス可能であるため) トンネル インターフェイスがアップしていることを表します。赤は、 トンネル モニターが有効で、リモート トンネル モニタリング IP アドレスがアクセス不可で あるために、トンネル インターフェイスがダウンしていることを表します。

IPSec トンネルの再起動または更新

• Network > IPSec Tunnels [ネットワーク > IPSec トンネル]

トンネルのステータスを表示する場合は、Network(ネットワーク) > IPSec Tunnels(IPSec ト ンネル)を開きます。最初の Status(状態)列には、トンネル情報へのリンクがあります。再起 動または更新するトンネルをクリックし、Tunnel Info[トンネル情報]を開きます。リストのエン トリのいずれかをクリックし、次のいずれかをクリックします。

- Restart(再起動) 選択したトンネルを再起動します。再起動すると、トラフィックのトン ネル通過が中断されます。
- Refresh(更新) IPSec SA の現在の状態を表示します。

Network (ネットワーク) > GRE Tunnels (GRE トンネル)

GRE(Generic Routing Encapsulation)トンネル プロトコルは、ペイロードのプロトコルをカ プセル化するキャリア プロトコルです。GRE パケット自体が転送プロトコル(IPv4 あるいは IPv6)内でカプセル化されます。GRE トンネルはファイアウォールおよびルーター(あるいは 別のファイアウォール)間のポイントツーポイントの論理リンク内の 2 つのエンドポイントに 接続します。Palo Alto Networks のファイアウォールは GRE トンネルのターミネーションをサ ポートしています。

確認すべき情報	以下を参照
GREトンネルの構成要素	GRE トンネル
他のベンダーのトンネル エンドポイントとの 相互運用性を確保する方法	IPSec トンネルを作成する際、Add GRE Encapsulation (GRE カプセル化を追加)を選択 します。
その他の情報をお探しですか?	GRE トンネル

GREトンネル

• Network (ネットワーク) > GRE Tunnels (GRE トンネル)

まずはトンネル インターフェイスを設定します(Network (ネットワーク) > Interfaces (インター フェイス) > Tunnel (トンネル))。次に GRE (generic routing encapsulation)トンネルを追加し て次の情報を提供し、作成したトンネル インターフェイスを参照します:

GRE トンネル フィールド	の意味
氏名	GRE トンネルの名前です。
Interface	ローカル GRE トンネル エンドポイント (ソース インターフェイス) (イーサネット インターフェイスあるいはサブインターフェ イス)、集約イーサネット(AE)インター フェイス、ループバック インターフェイス、 あるいは VLAN インターフェイスとして使用 するインターフェイスを選択します。
ローカル アドレス	トンネル インターフェイスのアドレスとして 使用するインターフェイスのローカル IP ア ドレスを選択します。

GRE トンネル フィールド	の意味
ピアアドレス	GRE トンネルのもう一方の末端の IP アドレ スを入力します。
トンネルインターフェイス	設定したトンネル インターフェイスを選択 します。(ルーティングのために、このイン ターフェイスはネクストホップであるときに トンネルを特定します)
TTL	GRE パケットにカプセル化された IP パケッ トの TTL を入力します(範囲は 1~255、デ フォルトは 64)。
ERSPAN	選択すると、ファイアウォールIが GRE ト ンネルを介して送信される Encapsulated Remote Switched Port Analyzer (ERSPAN) データのカプセル化を解除できま す。ERSPAN を使用してミラー化されたト ラフィックを GRE トンネル経由で ファイ アウォールに送信し、IoT Security などの Security サービスで使用するようにネット ワーク スイッチを設定できます。データを カプセル化解除した後、ファイアウォールI は TAP ポートで受信したトラフィックを検 査する方法と同様にデータを検査します。 次に、拡張アプリケーション ログ (EAL) と トラフィック、脅威、WildFire、URL、デー タ、GTP (GTP が有効な場合)、SCTP (SCTP が有効になっている場合)、トンネル、認証、 および復号化ログを作成します。ファイア ウォール は、これらのログをログ サービス に転送し、そこで IoT Security がデータにア クセスして分析します。
ToS ヘッダーのコピー	元の TOS(Type of Service)情報を保持する ため、カプセル化されたパケットの内部 IP ヘッダーから外部 IP ヘッダーに TOS フィー ルドをコピーする際に選択します。
キープアライブ	GRE トンネルのキープアライブ機能を有効 化する場合に選択します(デフォルト設定 では無効)。キープアライブを有効化する場 合、デフォルト設定では GRE トンネルがダ ウンする際は 10 秒間隔で 3 つの応答されな いキープアライブ パケット(リトライ)を受 け取り、GRE トンネルが復帰する際は 10 秒

GRE トンネル フィールド	の意味
	間隔で5つのホールドタイマー間隔を受け取 ります。
間隔 (秒)	ローカル側の GRE トンネルがトンネル ピア に送信するキープアライブ パケット間の間 隔、キープアライブ パケットが成功した後に ファイアウォールがトンネル ピアとの通信を 再び確立するまでに各ホールドタイマーが待 機する間隔を設定します(範囲は 1~50、デ フォルトは 10)。
再試行	キープアライブ パケットが返されない際、 ファイアウォールがトンネル ピアがダウンし ているとみなすまでの間隔を設定します(範 囲は 1~255、デフォルトは 3)。
ホールドタイム	ファイアウォールがトンネル ピアと再び接 続を確立するまでの間、キープアライブパ ケットが成功する間隔を設定します(範囲は 1~64、デフォルトは5)。

Network > DHCP [ネットワーク > DHCP]

DHCP (Dynamic Host Configuration Protocol) は、TCP/IP およびリンク レイヤーの設定パラ メータを提供し、また TCP/IP ネットワーク上で動的に設定されたホストにネットワーク アド レスを提供する標準プロトコルです。Palo Alto Networks ファイアウォールのインターフェイス は、DHCP サーバー、クライアント、またはリレー エージェントとして機能できます。これら の役割を別々のインターフェイスに割り当てることで、ファイアウォールは複数の役割を果たす ことができます。

確認すべき情報	以下を参照
DHCPについて。	DHCP の概要
DHCP サーバーがアドレスを 割り当てる方法。	DHCP アドレス

ファイアウォールで以下の機能のインターフェイスを設定する。

	DHCP サーバー
	DHCPリレー
	DNS プロキシ
その他の情報をお探しです か?	DHCP

DHCP の概要

• Network > DHCP [ネットワーク > DHCP]

DHCP では、通信のクライアント-サーバー モデルが使用されます。このモデルにはファ イアウォールが担うことのできる、次の3つの役割が含まれています。DHCPクライアン ト、DHCPサーバー、およびDHCPリレーエージェント。

- DHCPクライアント(ホスト)として機能するファイアウォールは、DHCPサーバーにIPア ドレスやその他の設定を要求できます。クライアントファイアウォールのユーザーは、設定 の時間と手間を省くことができます。また、DHCPサーバーから継承されるネットワークの アドレス計画やその他のネットワークリソースおよびオプションを把握する必要もありません。
- DHCPサーバーとして機能するファイアウォールは、クライアントにサービスを提供できます。DHCPのアドレスメカニズムのいずれかを使用することで、管理者は設定時間を節約でき、クライアントでネットワーク接続が不要になったときに、限られた数のIPアドレスを再利用できます。サーバーは、IPアドレスとDHCPオプションを多数のクライアントに配信することもできます。

DHCPリレーエージェントとして機能するファイアウォールは、ブロードキャストおよびユニキャストDHCPメッセージをリッスンし、それらをDHCPクライアントおよびサーバー間でリレーします。

DHCP は、トランスポート プロトコルとして、User Datagram Protocol(UDP)、RFC 768を使用します。クライアントからサーバーに送信される DHCP メッセージは、ウェルノウン ポート 6(UDP – ブートストラップ プロトコルおよび DHCP)に送信されます。サーバーからクライ アントに送信される DHCP メッセージは、ポート 68 に送信されます。

DHCP アドレス

DHCP サーバーからクライアントへの IP アドレスの割り当てまたは送信を行う方法は 3 つあります。

- Automatic allocation[自動割り当て] DHCP サーバーは、その IP Pools[IP プール] から永 久的な IP アドレスをクライアントに割り当てます。ファイアウォールで Lease[リース] が Unlimited[無制限] として指定されている場合、永久的な割り当てになります。
- Dynamic allocation[動的な割り当て] DHCP サーバーは、リースと呼ばれる最大期間で、アドレスの IP Pools[IP プール]の再利用可能な IP アドレスをクライアントに割り当てます。このアドレス割り当て方法は、顧客の IP アドレス数が限られている場合に便利です。この方法では、ネットワークへの一時的なアクセスのみが必要なクライアントに IP アドレスを割り当てることができます。
- Static allocation[静的な割り当て] ネットワーク管理者はクライアントに割り当てる IP アドレスを選択し、DHCP サーバーはその IP アドレスをクライアントに送信します。静的なDHCPの割り当ては恒久的なものです。これを行う場合は、DHCPサーバーを設定し、クライアントファイアウォールのMAC Address[MACアドレス] に対応するように Reserved Address[予約済みアドレス] を選択します。クライアントが切断 (ログオフ、再起動、停電など) しても、DHCP の割り当てはそのまま保持されます。

たとえば、LAN 上にプリンタがあり、DNS で LAN のプリンタの名前と IP アドレスが関連付 けられているために、その IP アドレスが頻繁に変わらないようにする場合、IP アドレスの静 的な割り当てが役立ちます。また、クライアントファイアウォールが何か重要な用途で使用 されていて、ファイアウォールがオフになったり、プラグが抜かれたり、再起動したり、停 電が発生したりしても、同じIPアドレスを保持する必要がある場合にも便利です。

Reserved Address[予約済みアドレス]を設定するときは、以下の点に注意してください。

- これは、IP Pools[IP プール]のアドレスです。複数の予約済みアドレスを設定できます。
- Reserved Address[予約済みアドレス] を設定していない場合、サーバーのクライアントは、リースの有効期限が切れたり、再起動したりすると、プールから新しい DHCP の割り当てを受信します(Lease[リース]を Unlimited[無制限] に設定している場合は除く)。
- IP Pools[IPプール]のすべてのアドレスを Reserved Address[予約済みアドレス]として割り当てると、アドレスを要求する次のDHCPクライアントに自由に割り当てることができる動的なアドレスがなくなります。
- Reserved Address[MAC アドレス] を設定せずに MAC Address[予約済みアドレス] を設定 できます。この場合、DHCPサーバーは、どのファイアウォールにも Reserved Address[予 約済みアドレス] を割り当てません。プールのいくつかのアドレスを予約し、DHCP を使 用せずに FAX やプリンタなどに静的に割り当てることができます。

DHCP サーバー

• Network > DHCP > DHCP Server [ネットワーク > DHCP > DHCP サーバー]

以下のセクションでは、DHCP サーバーの各構成要素について説明します。DHCP サーバーを 設定する前に、仮想ルーターおよびゾーンに割り当てられるレイヤー 3 Ethernet またはレイ ヤー 3 VLAN インターフェイスを設定しておく必要があります。また、DHCP サーバーからクラ イアントに割り当てるように指定できる、ネットワーク計画の有効な IP アドレス プールを把握 している必要もあります。

DHCP サー バー設定	設定場所	の意味
インターフェ イス	DHCP サーバー	DHCP サーバーとして機能するインターフェイス の名前。
モード		enabled[有効] モードまたは auto[自動] モード を選択します。Auto[自動] モードでは、サー バーが有効になりますが、ネットワークで別の DHCP サーバーが検出された場合は無効になりま す。disabled[無効] 設定を指定すると、サーバー が無効になります。
新しい IP を 割り当てる ときに IP に Ping する	DHCP サーバー > リース	Ping IP when allocating new IP[新しい IP を割 り当てるときに IP に Ping する] をクリックす ると、サーバーは、IP アドレスに ping してか ら、そのアドレスをクライアントに割り当てま す。pingが応答を受信した場合、そのアドレスは すでに別のファイアウォールに使用されているた め、割り当てできないということを意味します。 サーバーがプールから次のアドレスを割り当てま す。このオプションを選択した場合は、表示され ている [プローブ IP] 列にチェック マークが付け られます。
リース		 リースのタイプを指定します。 Unlimited[無制限] を指定すると、サーバーはIP Pools [IP プール] から動的に IP アドレスを選択し、クライアントに永久的に割り当てます。 Timeout[タイムアウト]により、リースの継続時間が決まります。Days[日] およびHours[時間] の数値を入力し、必要に応じてMinutes[分] の数値を入力します。

DHCP サーバーを追加するときは、以下の表に示す設定を行います。

DHCP サー バー設定	設定場所	の意味
IPプール		 DHCP サーバーがアドレスを選択する IP アドレスのステートフル プールを指定し、DHCP クライアントに割り当てます。 単一のアドレス、192.168.1.0/24 などのアドレス/<マスクの長さ>、または 192.168.1.10-192.168.1.20 などのアドレスの範囲を入力できます。
予約済みアド レス		必要な場合は、DHCP サーバーで動的に割り当て ない IP プール内の IP アドレス (x.x.x. 形式) を指 定します。 MAC Address[MACアドレス] (xx:xx:xx:xx 形 式) も一緒に指定した場合は、その MACアドレ スに関連付けられたファイアウォールがDHCPを 通じてIPアドレスを要求した際に、Reserved Address[予約済みアドレス] がそのフィアア ウォールに割り当てられます。
継承ソース	DHCP サーバー > オプ ション	None[なし] (デフォルト)を選択するか、各種 サーバーの設定を DHCP サーバーに配信する ソース DHCP クライアント インターフェイスま たは PPPoE クライアント インターフェイスを選 択します。Inheritance Source[継承ソース] を指 定する場合は、このソースからinherited[継承]す る以下のオプションを 1 つ以上選択します。 継承ソースを指定する利点の 1 つは、ソース DHCP クライアントのアップストリームである サーバーから DHCP オプションがすばやく転送 されることです。また、継承ソースのオプション が変更されても、クライアントのオプションが常 に最新の状態に維持される点も挙げられます。た とえば、継承ソースファイアウォールでNTPサー バー (Primary NTP[プライマリNTP]サーバーと して識別されているサーバー) を置き換えると、 クライアントは自動的にPrimary NTP[プライマ リNTP]サーバーとして新しいアドレスを継承し ます。
継承ソース状 態のチェック		Inheritance Source (継承ソース)を選択した場合、Check inheritance source status (継承ソース状態のチェック)をクリックすると、Dynamic IP Interface Status (動的 IP インターフェイス状

DHCP サー バー設定	設定場所	の意味
		態)ウィンドウが開き、DHCP クライアントから 継承されたオプションが表示されます。
ゲートウェイ	DHCP サーバー > オプ ション (続き)	この DHCP サーバーと同じ LAN 上にはないデ バイスに到達するために使用するネットワーク ゲートウェイ (ファイアウォールのインターフェ イス) の IP アドレスを指定します。
サブネット マスク		IP Pools[IP プール] のアドレスに適用するネット ワーク マスクを指定します。
オプション		以下のフィールドでドロップダウンリストをク リックし、None (なし) または inherited (継 承済み)を選択するか、そのサービスにアクセ スするために DHCP サーバーがクライアント に送信するリモート サーバーの IP アドレスを 入力します。inherited (継承済み)を選択する と、DHCP サーバーはソース DHCP クライアン トから、Inheritance Source (継承ソース) とし て指定された値を継承します。
		DHCP サーバーはこれらの設定をクライアントに 送信します。
		 Primary DNS[プライマリ DNS]、Secondary DNS[セカンダリ DNS] – 優先および代替 DNS (Domain Name System) サーバーの IP アドレ ス。
		 Primary WINS[プライマリ WINS]、Secondary WINS[セカンダリ WINS] – 優先および代替 WINS (Windows Internet Naming Service) サー バーの IP アドレス。
		 Primary NIS[プライマリ NIS]、Secondary NIS[セカンダリ NIS] – 優先および代替 NIS (Network Information Service) サーバーの IP アドレス。
		 Primary NTP[プライマリ NTP]、Secondary NTP[セカンダリ NTP] – 使用可能な NTP (Network Time Protocol) サーバーの IP アドレ ス。
		 POP3 Server[POP3 サーバー] – POP3 (Post Office Protocol version 3) サーバーの IP アドレス。

DHCP サー バー設定	設定場所	の意味
		 SMTP Server[SMTP サーバー] – Simple Mail Transfer Protocol (SMTP) サーバーの IP アド レス。 DNS Suffix[DNS サフィックス] – 解決できな い非修飾ホスト名が入力されたときにクライ アントがローカルで使用するサフィックス。
カスタム DHCP オプ ション		Add[追加] をクリックし、DHCP サーバーから クライアントに送信するカスタム オプション のName[名前]を入力します。
		Option Code [オプションコード](範囲 は1~254)を入力します。
		Option Code 43[オプション コード 43] を入力す ると、Vendor Class Identifier (VCI) [ベンダー ク ラス ID (VCI)] フィールドが表示されます。クラ イアントのオプション 60 から受信した VCI と比 較する一致基準を入力します。ファイアウォール は、クライアントのオプション 60 から受信した VCI を検査し、専用の DHCP サーバー テーブル で一致する VCI を検索し、それに対応する値を オプション 43 のクライアントに返します。VCI 一致基準は、文字列または 16 進値です。16 進 値のプレフィックスは「Ox」にする必要がありま す。
		Inherited from DCHP server inheritance source (DHCP サーバーの継承元から継承)を 選択すると、サーバーは、そのオプションコー ドの値を継承元から継承します。ユーザーが Option Value (オプション値)を入力する必要は ありません。
		このオプションの代わりに、以下の方法を使用す ることもできます。
		Option Type [オプションタイプ]: IP Address(IPアドレス)、ASCII、また はHexadecimal(16進数)を選択し、Option Value(オプション値)に使用するデータのタイ プを指定します。
		Option Value[オプション値] で Add[追加] をク リックし、カスタム オプションの値を入力しま す。

DHCPリレー

• Network > DHCP > DHCP Relay [ネットワーク > DHCP > DHCP リレー]

firewall インターフェイスを DHCP リレーエージェントとして設定する前に、Layer 3 Ethernet または Layer 3 VLAN インターフェイスを設定し、そのインターフェイスを仮想ルータとゾー ンに割り当てたことを確認してください。そのインターフェイスでクライアントとサーバー 間の DHCP メッセージを渡すことができるようにします。それぞれのインターフェイスは、 最大で8つの外部IPv4 DHCPサーバーと8つの外部IPv6 DHCPサーバーへメッセージを転送す ることができます。クライアントのDHCPDISCOVERメッセージは、設定されたすべてのサー バーに送信され、ファイアウォールは、要求を行ったクライアントに最初に応答したサーバー のDHCPOFFERメッセージをリレーします。

DHCP リレー設定	の意味
インターフェイス	DHCP リレー エージェントになるインターフェイスの名前。
IPv4 / IPv6	指定する DHCP サーバーと IP アドレスのタイプを選択します。
DHCP サーバー IP アドレス	DHCP メッセージのリレー先およびリレー元の DHCP サーバーの IP アドレスを入力します。
インターフェイス	DHCP サーバーの IP アドレス プロトコルとして IPv6 を選択し、マル チキャスト アドレスを指定した場合は、出力インターフェイスも指定 する必要があります。

DHCP クライアント

- Network > Interfaces > Ethernet > IPv4 [ネットワーク > インターフェイス > イーサネット > IPv4]
- Network > Interfaces > VLAN > IPv4 [ネットワーク > インターフェイス > VLAN > IPv4]

DHCP クライアントとしてファイアウォール インターフェイスを設定する前に、レイヤー3 Ethernet またはレイヤー3 VLAN インターフェイスが設定されていることと、インターフェイ スが仮想ルーターおよびゾーンに割り当てられていることを確認します。このタスクは、DHCP を使用してファイアウォールのインターフェイスの IPv4 アドレスを要求する必要がある場合に 実行します。

DHCP クライアント設定	の意味
タイプ	インターフェイスを DHCP クライアントとして設定する場合 は、DHCP Client[DHCP クライアント] を選択し、次にEnable[有 効化] を選びます。
サーバー提供のデフォ ルト ゲートウェイを指	ファイアウォールがデフォルト ゲートウェイへのスタティック ルートを作成します。これは、ファイアウォールのルーティング

DHCP クライアント設定	の意味
すデフォルト ルートを 自動的に作成	テーブルにルートを保持する必要がないため、クライアントが多 数の宛先にアクセスする場合に便利です。
デフォルト ルート メト リック	必要に応じて、ファイアウォールと DHCP サーバー間のルート の Default Route Metric[デフォルト ルート メトリック] (優先順 位レベル) を入力します。数値の低いルートほど、ルート選択時 の優先順位が高くなります。たとえば、メトリックが10のルー トは、メトリックが100のルートよりも前に使用されます(範囲 は1~65535、デフォルトはなし)。
DHCP クライアント ラ ンタイム情報の表示	DHCP のリース状態、ダイナミック IP 割り当て、サブネット マスク、ゲートウェイ、サーバー設定 (DNS、NTP、ドメイ ン、WINS、NIS、POP3、および SMTP) など、DHCP サーバーか ら受信したすべての設定が表示されます。

Network > DNS Proxy [ネットワーク > DNS プロキシ]

DNS サーバーは、ドメイン名から IP アドレス、および IP アドレスからドメイン名を解決する サービスを実行します。ファイアウォールを DNS プロキシとして設定すると、ファイアウォー ルはクライアントとサーバー間の中継役として機能します。また、DNS キャッシュからのクエ リを解決したり、クエリを別の DNS サーバーに送信したりすることで、DNS サーバーとしても 機能します。このページは、ファイアウォールがどのような方法で DNS プロキシとして機能す るかを設定する場合に使用します。

知りたい内容	以下を参照
ファイアウォール プロキシ DNS の 要求方法。	DNS プロキシの概要
DHCP プロキシの設定方法。	DNS プロキシ設定
スタティック FQDN から IP アドレ スへのマッピングの設定方法。	
DNS プロキシの管理方法。	その他の DNS プロキシ アクション
その他の情報をお探しですか?	DNS

DNS プロキシの概要

• Network > DNS Proxy [ネットワーク > DNS プロキシ]

DNS サーバーとして機能するようにファイアウォールを設定できます。まず、DNS プロキシを 作成し、プロキシを適用するインターフェイスを選択します。次に、DNS プロキシ キャッシュ にドメイン名が見つからない場合(およびドメイン名がプロキシ ルールに一致しない場合) にファイアウォールが DNS クエリを送信するデフォルトのプライマリおよびセカンダリ DNS サーバーを指定します。

ドメイン名に基づいて DNS クエリを別の DNS サーバーに転送するには、DNS プロキシ ルール を作成します。複数の DNS サーバーを指定すると、DNS クエリを確実にローカライズし、効率 を向上させることができます。たとえば、企業の DNS クエリはすべて企業の DNS サーバーに 転送し、他のクエリはすべて ISP DNS サーバーに転送できます。

以下のタブを使用して、(デフォルトのプライマリおよびセカンダリ DNS サーバー以外 に)DNS プロキシを定義します。各タブのフィールドについては、「DNS Proxy Settings (DNSプロキシ設定)」で説明します。

Static Entries (スタティックエントリ) – DNS クエリに対してファイアウォールがキャッシュしてホストに送信する FQDN と IP アドレスのスタティック マッピングを設定できます。

- DNS Proxy Rules (DNS プロキシ ルール) ドメイン名と、対応するプライマリおよびセカ ンダリ DNS サーバーを指定して、ルールに一致するクエリを解決できます。DNS プロキシ キャッシュにドメイン名が見つからない場合、ファイアウォールは、(クエリが到達するイ ンターフェイス上の) DNS プロキシで一致するドメイン名を検索し、その一致結果に基づい てクエリを DNS サーバーに転送します。一致する結果がない場合、ファイアウォールはクエ リをデフォルトのプライマリおよびセカンダリ DNS サーバーに送信します。ルールに一致す るドメインのキャッシングを有効にできます。
- Advanced (詳細)-DNS プロキシ オブジェクトを使用してファイアウォールが生成する DNS/ FQDN クエリを解決する場合は、キャッシュ (Cache (キャッシュ)を選択) と Cache EDNS Responses (キャッシュ EDNS 応答) を有効にする必要があります。Advanced (詳細) タブで は、TCP クエリと UDP クエリの再試行を制御することもできます。ファイアウォールは、設 定されたインターフェイスで TCP または UDP DNS クエリを送信します。DNS クエリの応答 が1つの UDP パケットに対して長すぎる場合、UDP クエリは TCP に切り替えられます。

DNS プロキシ設定

Add(追加) をクリックし、DNS プロキシとして機能するようにファイアウォールを設定でき ます。最大 256 個の DNS プロキシをファイアウォールに設定できます。

DNS プロキシ設定	設定場所	の意味
Enable [有効化]	DNSプロキシ	この DNS プロキシを有効にする場合に選択します。
氏名		DNS プロキシオブジェクトの識別に使用する名前を 指定します (最大 31 文字)。名前の大文字と小文字は 区別されます。また、一意の名前にする必要があり ます。文字、数字、スペース、ハイフン、およびア ンダースコアのみを使用してください。
場所		DNS プロキシ オブジェクトの適用先の仮想システム を指定します。
		 Shared (共有):プロキシはすべての仮想シス テムに適用されます。Shared[共有]を選択した場 合、Server Profile[サーバー プロファイル]フィー ルドは使用できません。代わりに、Primary (プラ イマリ)および Secondary (セカンダリ)の DNS サーバー IP アドレスまたはアドレス オブジェク トを入力します。
		 この DNS プロキシを使用する仮想システムを 選択します。最初に仮想システムを設定する 必要があります。 Device[デバイス] > Virtual Systems[仮想システム] に移動し、仮想システム を選択してから、DNS Proxy[DNSプロキシ] を選 択します。

DNS プロキシ設定	設定場所	の意味
継承ソース (共有場所のみ)		デフォルトの DNS サーバー設定を継承する送信元を 選択します。これは一般的に、ファイアウォールの WAN インターフェイスが DHCP または PPPoE でア ドレス指定される支社の導入で使用されます。
継承ソース状態の チェック (共有場所のみ)		DHCP クライアント インターフェイスおよび PPPoE クライアント インターフェイスに現在割り当てられ ているサーバー設定を確認する場合に選択します。 これには、DNS、WINS、NTP、POP3、SMTP、ま たは DNS サフィックスなどが含まれます。
Primary/Secondary (共有場所のみ)		このファイアウォールが(DNS プロキシとし て)DNS クエリを送信するデフォルトのプライマリ およびセカンダリ DNS サーバーの IP アドレスを指 定します。プライマリ DNS サーバーが見つからない と、ファイアウォールはセカンダリ DNS サーバーを 使用します。
サーバ プロファイ ル (仮想システムの場 所のみ)		新規 DNS サーバー プロファイルを選択または作成 します。仮想システムの場所を [共有] として指定し た場合は、このフィールドは表示されません。
インターフェイス		DNS プロキシとして機能するインターフェイスを Add(追加)します。複数のインターフェイスを追 加できます。インターフェイスから DNS プロキシを 削除する場合は、それを選択して Delete(削除)し ます。
		DNS プロキシをサービス ルート機能専用で使用し ている場合は、インターフェイスは不要です。宛先 サービス ルートで送信元 IP アドレスを設定する場 合、インターフェイスを持たない DNS プロキシとと もに宛先サービス ルートを使用します。そうしない 場合、DNS プロキシは、送信元として使用するイン ターフェイス IP アドレスを選択します(DNS サービ ス ルートが設定されていない場合)。
氏名	DNS プロキシ > DNS プロキ	CLI 経由でエントリを参照および変更できるようにす るには、名前が必要です。
このマッピングに よって解決されるド		このマッピングで解決されるドメインのキャッシン グを有効にする場合に選択します。

DNS プロキシ設定	設定場所	の意味
メインのキャッシン グをオンにする		
ドメイン名		ファイアウォールが受信 FQDN を比較する 1 つ以上 のドメイン名を Add (追加) します。FQDN がルー ルのいずれかのドメインに一致すると、ファイア ウォールはこのプロキシに指定されたプライマリ/セ カンダリ DNS サーバーにクエリを転送します。ルー ルからドメイン名を削除するには、ドメイン名を選 択して Delete (削除) をクリックします。
DNSサーバプロ ファイル (共有場所のみ)		仮想システムの DNS 設定(ファイアウォールがドメ イン名のクエリを送信するプライマリおよびセカン ダリ DNS サーバーなど)を定義する DNS サーバー プロファイルを選択または追加します。
Primary/Secondary (仮想システムの場 所のみ)		ファイアウォールが一致するドメイン名のクエリを 送信するときの宛先となるプライマリおよびセカン ダリ DNS サーバーのホスト名または IP アドレスを 入力します。
氏名	DNS プロキシ	スタティック エントリの名前を入力します。
FQDN	> スタティッ クエントリ	Address (アドレス) フィールドで定義されたスタ ティック IP アドレスにマッピングするための完全修 飾ドメイン名 (FQDN) を入力します。
アドレス		このドメインにマッピングする1つ以上のIPアドレ スをAdd(追加)します。ファイアウォールがこれ らのすべてのアドレスをDNS応答に含め、クライア ントは使用するIPアドレスを選択します。アドレス を削除するには、アドレスを選択して Delete[削除] をクリックします。
TCP クエリ	DNS プロキシ > 上級	TCP を使用する DNS クエリを有効にする場合に選 択します。ファイアウォールでサポートする同時 に保留する TCP DNS 要求の最大数(Max Pending Requests(リクエスト最大保留数))を指定します (範囲は 64 ~ 256、デフォルトは 64)。
UDP クエリの再試 行	DNS プロキシ > 上級	 UDP クエリの再試行の設定を指定します。 Interval(間隔) – 応答を受信しなかった場合に DNS プロキシが別の要求を送信するまでの時間 (秒)(範囲は1~30、デフォルトは2)。

DNS プロキシ設定	設定場所	の意味
		 Attempts(試行回数) – DNSP が次の DNS サー バーを試行するまでの最大試行回数(最初の試行 は除く)(範囲は 1 ~ 30、デフォルトは 5)。
Cache	DNS プロキシ > 上級	ファイアウォールが生成するクエリにこの DNS プロ キシオブジェクトを使用する場合 (つまり、Device (デバイス) > Setup (セットアップ) > Services (サー ビス) > DNS、または Device(デバイス) > Virtual Systems (仮想システム) で、virtual system (仮想シス テム - vsys) と General (全般) > DNS プロキシを選択) Cache を有効にする必要があります。次に、以下を 指定します。
		 Enable TTL(TTLの有効化) – ファイアウォー ルがプロキシオブジェクトの DNS エントリを キャッシュする時間の長さを制限します。TTL は デフォルトで無効になっています。次に、Time to Live (sec)(有効時間(秒))を入力します – こ れはプロキシオブジェクトのキャッシュされたす べてのエントリが削除されるまでの秒数です。新 しい DNS 要求は解決して再度キャッシュする必 要があります。範囲は 60~86,400 です。デフォ ルトの TTL はありません。エントリはファイア ウォールのキャッシュ メモリがなくなるまで保持 されます。
		 Cache EDNS Responses (キャッシュ EDNS 応 答)-ファイアウォールが生成するクエリにこ の DNS プロキシ オブジェクトを使用する場合 は、DNS (EDNS) 応答のキャッシュ拡張メカニズ ムを有効にする必要があります。FQDN アドレス オブジェクトのクエリが成功するには、ファイア ウォールが DNS 応答をキャッシュできる必要が あります。

その他の DNS プロキシ アクション

ファイアウォールをDNSプロキシとして設定した後、Network[ネットワーク] > DNS Proxy [DNSプロキシ] ページで以下のアクションを実行し、DNSプロキシ設定を管理できます。

- Modify[変更] DNS プロキシを変更するには、DNSプロキシ設定の名前をクリックします。
- Delete[削除] DNS プロキシエントリを選択し、Delete[削除] をクリックすると、DNSプロ キシ設定が削除されます。

Disable[無効化] – DNSプロキシを無効にするには、DNSプロキシエントリの名前をクリックし、Enable[有効化] を選択解除します。無効になっている DNS プロキシを有効にするには、DNS プロキシエントリの名前をクリックし、Enable[有効化] を選択します。

ネットワーク > プロキシ

プロキシ構成オプションを使用できるかどうかは、プロキシの種類によって異なります。プロキシを構成するには、最初に configure a DNS プロキシ オブジェクト する必要があります。

プロキシフィールド	詳説
プロキシの有効化	
プロキシ タイプ	使用するプロキシの種類を選択します。
	• None - プロキシは非アクティブ化されています。
	 Explicit - 要求に構成済みのプロキシの宛先 IP ア ドレスが含まれ、クライアント ブラウザーがプロ キシに直接要求を送信するようにプロキシを構成 します。
	 Transparent - リクエストに Web サーバーの宛先 IP アドレスが含まれ、クライアント ブラウザーが プロキシにリダイレクトされるようにプロキシを 構成します。
	 ・透過プロキシを正常に設定するに は、特定の宛先 NAT(DNAT)ポリ シー ルールが必要です。完全な手 順については、PAN-OS Networking Administrator's Guide のドキュメン トを参照してください。
	 Palo Alto Networks Service Proxy-ダウンスト リームネットワーク内のファイアウォールから アップストリームネットワーク内の宛先に通信を 転送するようにプロキシを設定します。ファイア ウォールは、単一のプロキシとして動作すること

プロキシ フィールド	詳説
	も、一連のプロキシの1つとして動作することも できます。
	 このプロキシモードは、PAN- OS 11.0.1-h2以降を実行してい るPA-1400、PA-3400、VM-300、VM-500、VM-700フェ イアウォールでサポートされていま す。ファイアウォールがこのプロ キシタイプをサポートし、ここに オプションとして表示するには、 次のCLIコマンドを入力し、ファイ アウォールを再起動します。set system setting paloalto- networks-service-proxy on
プロキシ設定	
接続タイムアウト	プロキシが Web サーバーからの応答を待機する時 間 (秒単位) を指定します。範囲は 1 から 60 秒で、デ フォルトは 5 秒です。指定した時間が経過しても応 答がない場合、プロキシは接続を閉じます。
リスニング インターフェイス 明示的 プロキシのみ	firewall がプロキシに再ルーティングするトラフィッ クをチェックするレイヤ 3(L3)インターフェイスを指 定します。
アップストリームインターフェース	アップストリーム インターフェイスを選択します。 ・ ループバック インターフェイスを使用 している場合は、そのインターフェイ スを Upstream Interface として指定し ます。
プロキシIP	firewall がプロキシ (リスニング インターフェイス) に 再ルーティングするトラフィックをチェックするイ ンターフェイスの IP アドレスを指定します。
DNS プロキシ	プロキシ接続に使用する DNS プロキシ オブジェク ト を選択します。
CONNECT と SNI のドメインが同じ であることを確認する 明示的プロキ シのみ	このオプションを有効にすると、CONNECT 要求と HTTP ヘッダーのサーバー名表示 (SNI) フィールドの 間に異なるドメインを指定することによって引き起

プロキシ フィールド	詳説
	こされるドメイン・フロンティング・アタックを防 止できます。
認証サービスの種類 明示的プロキシ のみ	ユーザーの認証に使用するサービスの種類を選択し ます。
	 SAML/CAS - SAML 2.0 ベースの認証サービス、 または Cloud Identity Engine で使用可能な認証 サービスを使用します。
	Cのオプションには、Prisma Access、Cloud Services 3.2.1 プラグ イン、およびアドオン Web プロキ シライセンスが必要です。
	 Kerberos Single Sign On - Kerberos Single Sign-On Service を使用してユーザーを認証します。
	このオプションに は、Panorama、Web プロキシ ライ センス、および firewall.
	で Kerberos Single Sign-On Service を使用する認 証プロファイルが必要です。
	 認証なし-すべての明示的な Web プロキシ トラ フィックを認証から免除します。
	 このオプションを選択すると、す べてのプロキシ接続が認証されず、 ファイアウォールまたはPanoramaは 認証イベントのログを作成しません。
認証プロファイル 明示的プロキシの み	前のオプションで選択した Authentication サービ ス・タイプ に使用する認証プロファイルを選択しま す。

Network > QoS [ネットワーク > QoS]

以下のトピックでは、サービス品質(QoS)について説明します。

確認すべき情報	以下を参照
インターフェイスの帯域幅制 限を設定し、インターフェイ スから出ていくトラフィック の QoS を適用する。	QoS インターフェイス設定
QoS 対応のインターフェイス から出ていくトラフィックを モニターする。	QoS インターフェイスの統計情報
その他の情報をお探しです か?	QoSの詳細なワークフロー、コンセプト、使用例について はサービス品質を参照してください。
	ー致したトラフィックに QoS クラスを割り当てるに は、Policies(ポリシー)> QoS を選択します。最大 8 つ の QoS クラスの帯域幅制限および優先度を定義する場合に は、Network(ネットワーク)> Network Profiles(ネット ワーク プロファイル)> QoS を選択します。

QoS インターフェイス設定

インターフェイスの帯域幅制限を設定し、インターフェイスからの出力トラフィックにQoSを 適用する場合は、インターフェイス上でQoSを有効にします。QoS インターフェイスを有効に するには、QoS プロファイルをインターフェイスに追加する必要があります。QoS は物理イン ターフェイスでサポートされますが、ファイアウォール モデルによっては、サブインターフェ イスやイーサネットの集約(AE)インターフェイスでもサポートされます。お使いのファイア ウォール モデルでサポートされている QoS 機能を確認するには、Palo Alto Networks の製品比 較ツールを参照してください。

最初に QoS インターフェイスの Add (追加) または編集を行い、次に以下の表に記載されてい るように設定します。

QoS インター フェイス設定	設定場所	の意味
インターフェ イス名	QoS インター フェース > 物 理インター フェース	QoS を有効にするファイアウォール インターフェイスを選 択します。

QoS インター フェイス設定	設定場所	の意味	
最大保証帯 域 出力側 (Mbps)		このインターフェイスを介してファイアウォールから出力 されるトラフィックの最大スループット(Mbps)を入力 します。値はデフォルトで0で、ファイアウォール制限 (PAN-OS 7.1.16以降のリリースでは 60,000 Mbps、PAN- OS 7.1.15以前のリリースでは16,000)を指定します。 Egress Max(最大保証帯域出力側)は必須 フィールドではありませんが、QoSインター フェイスのこの値は常に定義しておくことをお 勧めします。	
このインター フェイスの QoS 機能を オンにする		選択したインターフェイスで QoS を有効にする場合に選択 します。	
クリア テキ スト トンネルイン ターフェイス	QoS インター フェース > 物 理インター フェース > デ フォルトのプ	クリア テキスト トラフィックおよびトンネル トラフィック のデフォルトの QoS プロファイルを選択します。それぞれ にデフォルトのプロファイルを指定する必要があります。ク リア テキスト トラフィックの場合、デフォルトのプロファ イルはすべてのクリア テキスト トラフィックに一括適用さ	
トンネルイン ターフェイス	ロファイル	れます。トンネルトラフィックの場合、デフォルトのプロ ファイルは、詳細設定セクションで特定のプロファイルが割 り当てられていない各トンネルに個別に適用されます。QoS プロファイルを定義する手順については、「Network(ネッ トワーク) > Network Profiles(ネットワーク プロファイ ル) > QoS」を参照してください。	
最低保証帯 域 出力側 (Mbps)	QoSイン ターフェー ス > Clear	このインターフェイスからのクリア テキストまたはトンネル 対象トラフィックに保証される帯域幅を入力します。	
最大保証帯 域 出力側 (Mbps) Tunneled Traffic (クリ ア テキスト トラフィッ ク/トンネ リング トラ フィック)	このインターフェイスを介してファイアウォールから出力さ れるクリア テキストまたはトンネル通過するトラフィック の最大スループット(Mbps)を入力します。値はデフォル トで0で、ファイアウォール制限(PAN-OS 7.1.16以降のリ リースでは 60,000 Mbps、PAN-OS 7.1.15以前のリリース では16,000)を指定します。クリア テキストまたはトンネ ル通過するトラフィックの Egress Max(最大保証帯域出力 側)は、物理インターフェイスの Egress Max(最低保証帯 域出力側)以下でなければなりません。		

QoS インター フェイス設定	設定場所	の意味	
コンテキスト の		 クリアテキストトラフィックの処理内容をより詳細に定 義する場合は、Clear Text Traffic [クリアテキストトラ フィック] タブで Add [追加] をクリックします。個々のエ ントリをクリックして、以下の設定を指定します。 	
		• Name[名前] – ここでの設定の識別に使用する名前を入 力します。	
		 QoS Profile[QoS プロファイル] – 指定したインター フェイスとサブネットに適用する QoS プロファイル を選択します。QoS プロファイルを定義する手順に ついては、「Network(ネットワーク) > Network Profiles(ネットワーク プロファイル) > QoS」を参照 してください。 	
		 Source Interface[送信元インターフェイス] – 送信元側 のファイアウォール インターフェイスを選択します。 	
	 宛先インターフェイス -(PA-3200 Series、 PA-5200 Series、 PA-5400 Series、 PA-7000 Series のみ) トラ フィックが意図されている宛先インターフェイスを選 択します。 		
		 Source Subnet[送信元サブネット] – 送信元のサブネットを選択すると、そのサブネットからのトラフィックのみに各設定が適用されます。デフォルト値の any [いずれか]をそのまま使用すると、指定したインターフェイスからのすべてのトラフィックに対して各設定が適用されます。 	
		 特定のトンネルに対するデフォルトプロファイルの割り 当てをオーバーライドする場合は、Tunneled Traffic [トン ネル対象トラフィック] タブで Add [追加] をクリックし、 以下の設定を指定します。 	
		 Tunnel Interface[トンネルインターフェイス] – ファ イアウォールのトンネルインターフェイスを選択しま す。 	
		 QoS Profile[QoS プロファイル] – 指定したトンネルイ ンターフェイスに適用する QoS プロファイルを選択し ます。 	
		たとえば、ファイアウォールに対して 45 Mbps で接続する サイトと T1 で接続するサイトを設定するとします。このと き、T1 サイトには接続が過負荷状態にならないように制限 の厳しい QoS 設定を適用する一方で、45 Mbps で接続する サイトにはより柔軟な設定を適用できます。	

QoS インター フェイス設定	設定場所	の意味	
		クリアテキストまたはトンネル対象トラフィックのエントリ を削除する場合は、エントリを空白にして Delete [削除] をク リックします。	
		[クリア テキスト] または [トンネル対象トラフィック] セク ションが空白のままの場合、[物理インターフェイス] タブの [デフォルト プロファイル] セクションで指定した値が使用さ れます。	

QoS インターフェイスの統計情報

• Network (ネットワーク) > QoS > Statistics (統計)

QoSインターフェイスで、設定済のQoSインターフェイスの帯域幅、セッション、およびアプリケーションの情報を表示する場合はStatistics [統計]を選択します。

QoS 統計情報	の意味		
帯域幅	選択したノードとクラスの帯域幅チャートがリアルタイムで表示されま す。この情報は2秒ごとに更新されます。		
	● QoS クラスに設定された Egress Max (最大保証帯域 出力 側) と Egress Guaranteed (最低保証帯域 出力側)の制限 は、QoS 統計情報画面では若干異なる値で表示される場合が あります。これは、ハードウェア エンジンが帯域幅の制限と カウンタを集約する方法によって発生する正常動作です。帯 域幅の使用率グラフにはリアルタイムの値と数量が表示され るため、運用上の問題はありません。		
アプリケー ション [applications]	選択した QoS ノードやクラスのアクティブなアプリケーションすべてのリ ストが表示されます。		
送信元ユーザー	選択した QoS ノードやクラスのアクティブな送信元ユーザーすべてのリス トが表示されます。		
宛先ユーザー	選択した QoS ノードやクラスのアクティブな宛先ユーザーすべてのリスト が表示されます。		
セキュリティ ルール数	選択した QoS ノードやクラスに一致し、それを適用するセキュリティ ルールのリストが表示されます。		

ネットワーク

QoS 統計情報	の意味
QoS ルール	選択した QoS ノードやクラスに一致し、それを適用する QoS ルールのリ ストが表示されます。

Network > LLDP [ネットワーク > LLDP]

リンク レイヤー検出プロトコル (LLDP) では、リンク レイヤーの隣接するデバイスとその機能を 自動的に検出できます。

確認すべき情報	以下を参照
LLDP について。	LLDP の概要
LLDP を設定する。	LLDP の構成要素
LLDP プロファイルを設定す る。	Network > Network Profiles > LLDP Profile [ネットワーク > ネットワーク プロファイル > LLDP プロファイル]
その他の情報をお探しですか?	LLDP

LLDP の概要

LLDP を使用すると、ファイアウォールは、LLDP データ ユニット (LLDPDU) を含む Ethernet フ レームをネイバーとの間で送受信できます。受信デバイスは、情報を MIB に保存します。MIB にアクセスするには、SNMP (Simple Network Management Protocol) を使用します。ネットワー ク デバイスは、LLDP によってネットワーク トポロジをマッピングし、接続されているデバイ スの機能を学習できます。これによってトラブルシューティングが容易になります。特にそれ が顕著なのは、ネットワーク トポロジでファイアウォールが基本的に検出されないようなバー チャル ワイヤーのデプロイにおいてです。

LLDP の構成要素

ファイアウォールでLLDPを有効にする場合は、Edit [編集] をクリックしてEnable[有効化] をク リックします。デフォルト設定が環境に適していない場合は、以下の表に示す4つの設定を必要 に応じて行います。表の残りのエントリは、状態とピアの統計を示しています。

LLDP 設定	設定場所	の意味
送信間隔 (秒)	LLDP 一般	LLDPDUが送信される間隔(秒数)を指定します (範囲は1~3600、デフォルトは30)。
送信遅延 (秒)		TLV (Type-Length-Value) 要素が変更された後に送 信されるLLDP発信の遅延間隔秒数を指定します。 多数のネットワーク変更により LLDP 変更の数が急 増した場合、またはインターフェイスがフラップし た場合は、この遅延により、セグメントが LLDPDU であふれることが防止されます。Transmit Delay[送 信遅延] の値は、Transmit Interval[送信間隔] よりも

LLDP 設定	設定場所	の意味
		小さくする必要があります(範囲は1~600、デフォ ルトは2)。
ホールド タイムの 間隔数		TTLホールドタイムの合計を求めるために Transmit Interval[送信間隔] で乗算される値を指定します(範 囲は1~100、デフォルトは4)。
		TTL ホールド タイムは、ファイアウォールがピアか らの情報を有効であるとして保持する時間の長さで す。TTL ホールド タイムの最大値は、乗数値にかか わらず 65535 秒です。
通知間隔		MIBが変更されたときにSyslog およびSNMPトラッ プ通知が送信される間隔(秒数)を指定します(範 囲は1~3600、デフォルトは5)。
スパイグラスフィ ルタ	LLDP > ステー タス	必要に応じて、フィルタ行にデータ値を入力し、灰 色の矢印をクリックします。これにより、そのデー タ値を含む行のみが表示されます。フィルタをクリ アするには、赤色の X をクリックします。
インターフェイス		LLDP プロファイルが割り当てられているインター フェイスの名前。
タイプ		LLDP プロファイルが割り当てられているインター フェイス タイプ(レイヤ 2、レイヤ 3、仮想ワイヤ、 タップ、HA、集約イーサネットなど)。
LLDP		LLDP の状態で、enabled [有効] またはdisabled [無 効] のいずれかです。
HA プレネゴシエー ション	-	HA プレネゴシエーションステータス:有効または無効。LLDP プレネゴシエーションにより、HA アク ティブ/パッシブ シナリオでのフェールオーバーが 高速化されます。
モード		インターフェイスのLLDPモード:Tx/Rx、Txのみ、 またはRxのみです。
プロファイル		インターフェイスに割り当てられたプロファイルの 名前。
送信合計		インターフェイスから送信された LLDPDU の数。

LLDP 設定	設定場所	の意味
ドロップされた送 信		エラーが原因でインターフェイスから送信されな かった LLDPDU の数。エラーの例としては、送信 する LLDPDU をシステムが作成中に発生した長さ のエラーなどがあります。
受信合計		インターフェイスで受信した LLDP フレームの数。
ドロップされた TLV		受信時に破棄された LLDP フレームの数。
エラー		インターフェイスで受信した TLV (Time-Length- Value) 要素のうち、エラーが含まれていたものの 数。TLV エラーのタイプとしては、1 つ以上の必須 TLV が欠落している、順序が適切でない、範囲外 の情報が含まれている、長さのエラーなどがありま す。
認識不可		インターフェイスで受信した TLV のうち、LLDP ローカル エージェントで認識されないものの 数。TLV が認識されない原因としては、たとえ ば、TLV のタイプが予約済みの TLV の範囲内にある ことなどが挙げられます。
エージアウト済み		適切な TTL が期限切れになったために受信 MIB から削除された項目の数。
LLDP 統計のクリア		LLDP 統計をすべてクリアする場合に選択します。
スパイグラスフィ ルタ	LLDP > ピア	必要に応じて、フィルタ行にデータ値を入力し、灰 色の矢印をクリックします。これにより、そのデー タ値を含む行のみが表示されます。フィルタをクリ アするには、赤色の X をクリックします。
ローカル インター フェイス		隣接するデバイスを検出したファイアウォール上の インターフェイス。
Remote Chassis ID		ピアのシャーシ ID。MAC アドレスが使用されま す。
ポート ID	LLDP > ピア (続 き)	ピアのポート ID。
氏名		ピアの名前。

LLDP 設定	設定場所	の意味
詳細		More Info[詳細情報] をクリックすると、必須および 任意のTLVに基づくリモートピアの詳細が表示され ます。
シャーシのタイプ		シャーシのタイプは MAC アドレスです。
MAC アドレス		ピアの MAC アドレス。
システム名		ピアの名前。
システムの説明		ピアの説明。
ポートの説明		ピアのポートの説明。
ポートのタイプ		インターフェイス名。
ポート ID		ファイアウォールは、インターフェイスの ifname を使用します。
システムの機能	-	システムの機能。O はその他、P はリピータ、B は ブリッジ、W はワイヤレス LAN、R はルーター、T は電話を表します。
有効になっている 機能		ピアで有効になっている機能。
管理アドレス		ピアの管理アドレス。

Network (ネットワーク) > Network Profiles (ネット ワーク プロファイル)

以下のトピックでは、ネットワーク プロファイルについて説明します。

- Network > Network Profiles > GlobalProtect IPSec Crypto [ネットワーク > ネットワーク プロ ファイル]> GlobalProtect の IPSec 暗号]
- Network > Network Profiles > IKE Gateways [ネットワーク > ネットワーク プロファイル > IKE ゲートウェイ]
- Network > Network Profiles > IPSec Crypto [ネットワーク > ネットワーク プロファイル > IPSec 暗号]
- Network > Network Profiles > IKE Crypto [ネットワーク > ネットワーク プロファイル > IKE 暗号]
- Network > Network Profiles > Monitor [ネットワーク > ネットワーク プロファイル > 監視]
- Network > Network Profiles > Interface Mgmt [ネットワーク > ネットワーク プロファイル > インターフェイス管理]
- Network > Network Profiles > Zone Protection [ネットワーク > ネットワークプロファイル > ゾーンプロテクション]
- Network (ネットワーク) > Network Profiles (ネットワーク プロファイル) > QoS
- Network > Network Profiles > LLDP Profile [ネットワーク > ネットワーク プロファイル > LLDP プロファイル]
- Network > Network Profiles > BFD Profile [ネットワーク > ネットワークプロファイル > BFDプロファイル]
- Network > Network Profiles > SD-WAN [ネットワーク > ネットワーク プロファイル > SD-WAN インターフェイス プロファイル]
- ネットワーク > ネットワークプロファイル > MACsecプロファイル

Network > Network Profiles > GlobalProtect IPSec Crypto [ネット ワーク > ネットワーク プロファイル]> GlobalProtect の IPSec 暗 号]

GlobalProtect IPSec Crypto Profiles[GlobalProtect の IPSec暗号化プロファイル] ページを使用し て、GlobalProtect ゲートウェイとクライアント間の VPN トンネルで認証および暗号化を行うた めのアルゴリズムを指定します。アルゴリズムを追加する順序は、ファイアウォールがアルゴリ ズムを適用する順序であり、トンネルのセキュリティとパフォーマンスに影響する場合がありま す。この順番を変更する場合は、テンプレートを選択して Move Up[上へ]またはMove Down[下 へ] をクリックします。



GlobalProtect ゲートウェイとサテライト(ファイアウォール)間の VPN トンネル については、「Network(ネットワーク) > Network Profiles(ネットワーク プロ ファイル) > IPSec Crypto(IPSec 暗号)」を参照してください。

GlobalProtect の IPSec 暗号化プロファイル設定		
氏名	プロファイルの識別に使用する名前を入力します。名前は大文字小 文字を区別し、一意の名前にする必要があります。最大 31 文字を 使用できます。文字、数字、スペース、ハイフン、およびアンダー スコアのみを使用してください。	
暗号化	Add[追加] をクリックし、目的の暗号化アルゴリズムを選択しま す。セキュリティを最大限に高めるため、降順で順序を以下のよう に変更します。 aes-256-gcm, aes-128-gcm, aes-128-cbc.	
authentication	Add[追加] をクリックし、認証アルゴリズムを選択します。現在の オプションは、sha1 のみです。	

Network > Network Profiles > IKE Gateways [ネットワーク > ネットワーク プロファイル > IKE ゲートウェイ]

このページを使用して、ゲートウェイを管理または定義します。このページには、ピアゲート ウェイに対して Internet Key Exchange (IKE) プロトコル ネゴシエーションを実行するために必要 な設定情報が含まれています。また、量子コンピュータからの攻撃に耐える IKEv2 VPN を作成 するために必要な設定情報が含まれています。これは、IKE/IPSec VPN セットアップのフェーズ 1の部分です。

IKE ゲートウェイを管理、設定、再起動、または更新する方法については、以下を参照してください。

- IKE ゲートウェイ管理
- IKE ゲートウェイの [全般] タブ
- IKE ゲートウェイの Advanced Options (詳細オプション) タブ
- IKE ゲートウェイの再起動または更新

IKE ゲートウェイ管理

Network > Network Profiles > IKE Gateways [ネットワーク > ネットワーク プロファイル > IKE ゲートウェイ]

以下の表は、IKE ゲートウェイの管理方法を示しています。

IKE ゲートウェイの管 理	の意味
コンテキストの	新しい IKE ゲートウェイを作成するには、Add[追加] をクリック します。新しいゲートウェイの設定方法は「IKE ゲートウェイの General(全般)タブ」および「IKE ゲートウェイの Advanced Options(詳細オプション)タブ」を参照してください。
IKE ゲートウェイの管 理	の意味
-------------------	--
削除します。	ゲートウェイを削除するには、ゲートウェイを選択して Delete [削 除] をクリックします。
Enable [有効化]	無効になっているゲートウェイを有効にするには、ゲートウェイを 選択して Enable[有効化] をクリックします。デフォルト設定では、 ゲートウェイは有効になっています。
無効化	ゲートウェイを無効にするには、ゲートウェイを選択して Disable[無効化] をクリックします。
PDF/CSV	最低限の読み取り専用アクセス権を持つ管理ロールは、オブジェクト設定を PDF/CSV としてエクスポートできます。フィルターを適用して、監査などのためのより具体的な表構成出力を作成することができます。Web インターフェイスで表示可能な列のみがエクスポートされます。「Configuration Table Export(設定バンドルのエクスポート)」を参照してください。

IKE ゲートウェイの [全般] タブ

Network (ネットワーク) > Network Profiles (ネットワーク プロファイル) > IKE Gateways (IKE ゲートウェイ) > General (一般)

以下の表は、configure an IKE gateway(IKE ゲートウェイの設定)の最初の手順を示していま す。IKE は、IKE/IPSec VPN プロセスのフェーズ1です。この設定の実行後、「IKE Gateway Advanced Options Tab(IKE ゲートウェイの詳細オプション タブ)」を参照してください。

IKE ゲートウェイの一般 設定	の意味
氏名	ゲートウェイを識別するName(名前)を入力します(最大 31 文 字)。名前の大文字と小文字は区別されます。また、一意の名前にす る必要があります。文字、数字、スペース、ハイフン、およびアン ダースコアのみを使用してください。
バージョン	ゲートウェイにサポートされていて、ピアゲートウェイと必ず 使用する必要のあるIKEバージョンを選択します。IKEv1 only mode(IKEv1限定モード)、IKEv2 only mode(IKEv2限定モー ド)、またはIKEv2 preferred mode(IKEv2優先モード)。IKEv2 優先モードでは、ゲートウェイが IKEv2 をネゴシエートします。こ れは、ピアが IKEv2 もサポートしている場合に使用されます。そ れ以外の場合、ゲートウェイは IKEv1 にフォールバックします。

IKE ゲートウェイの一般 設定	の意味
	 ポスト量子IKE VPNを設定するには、IKEv2専用モー ドまたはIKEv2優先モードを使用する必要があります。量子コンピュータからの攻撃に抵抗するポスト量 子機能をサポートしているのはIKEv2 VPNだけです。
アドレス タイプ	ゲートウェイが使用する IP アドレスのタイプを選択しま す。IPv4あるいは IPv6
インターフェイス	VPN トンネルに対する出力ファイアウォール インターフェイスを 選択します。
ローカル IP アドレス	トンネルのエンドポイントとなるローカル インターフェイスの IP アドレスを選択または入力します。
Peer IP Address	次のいずれかの設定を選択し、ピアの対応する情報を入力します。
Туре	 Dynamic (動的) ーピア IP アドレスまたは FQDN 値が不明な場合は、このオプションを選択します。ピア IP アドレス タイプが動的の場合、IKE ゲートウェイ ネゴシエーションを開始するのはピアまでです。 IP-IPv4 アドレスまたは IPv6 アドレス、もしくは IPv4 または IPv6 アドレスであるアドレス オブジェクトとして Peer Address (ピア アドレス) を入力します。
	 FQDN-FQDN または FQDN を使用するアドレス オブジェクト として Peer Address (ピア アドレス)を入力します。
	複数の IP アドレスに解決される FQDN または FQDN アドレス オブジェクトを入力すると、ファイアウォールは次のように IKE ゲートウェイのアドレス タイプ(IPv4 または IPv6)と一致する アドレス セットから優先アドレスを選択します。
	 IKE セキュリティ アソシエーション(SA)がネゴシエートされていない場合、優先アドレスは最小値のIPアドレスです。
	 アドレスが IKE ゲートウェイによって使用され、返されたアドレスのセット内にある場合は、そのアドレスが使用されます(最小であるかどうかにかかわらず)。
	 アドレスが IKE ゲートウェイによって使用されているが、返 されたアドレスのセットに含まれていない場合は、新しいア ドレスが選択されます。

IKE ゲートウェイの一般 設定	の意味
	FQDN または FQDN アドレスオブジェクトを使用す ると、ピアが動的 IP アドレス変更の対象となる環境 での問題が軽減されます(この IKE ゲートウェイピ アアドレスを再設定する必要があります)。
authentication	認証タイプを選択します。ピア ゲートウェイで実行される Pre- Shared Key(事前共有鍵)または Certificate(証明書)を選択しま す。選択に応じて「事前共有鍵フィールド」または「証明書フィー ルド」を参照してください。
事前共有鍵フィールド	
事前共有鍵/ 事前共有鍵の確認	Pre-Shared Key(事前共有鍵)を選択した場合は、トンネル間の対称認証に使用される単一のセキュリティキーを入力します。Pre-Shared Key(事前共有鍵)の値は、管理者が最大 255 文字の ASCII または ASCII 以外の文字を使用して作成する文字列です。辞書攻撃で解読されにくいキーを生成します。必要に応じて、事前共有鍵生成プログラムを使用します。
ローカルID	ローカル ゲートウェイのフォーマットと ID を定義します。この フォーマットと ID は、IKEv1 フェーズ 1 SA および IKEv2 SA の両 方を確立するために、事前共有鍵とともに使用されます。
	以下のタイプから1つを選択し、値を入力します。FQDN (ホスト 名)、IP address(IP アドレス)、KEYID (HEXのバイナリフォー マットID文字列)、またはUser FQDN(ユーザーFQDN)(電子メー ル アドレス)
	値を指定しない場合、ゲートウェイはローカルIPアドレスを Local Identification(ローカル ID)として使用します。
ピアID	ピア ゲートウェイのタイプと ID を定義します。このタイプと ID は、IKEv1 フェーズ 1 SA および IKEv2 SA の確立時に、事前共有鍵 とともに使用されます。
	以下のタイプから1つを選択し、値を入力します。FQDN (ホスト 名)、IP address(IP アドレス)、KEYID (HEXのバイナリフォー マットID文字列)、またはUser FQDN(ユーザーFQDN)(電子メー ル アドレス)
	値を指定しない場合、ゲートウェイはピアの IP アドレスを Local Identification(ローカル ID)として使用します。

証明書フィールド

KE ゲートウェイの一般 設定	の意味
ローカル証明書	Authentication[認証] のタイプとして Certificate[証明書] をドロッ プダウンリストから選択した場合は、ファイアウォール上にすでに 存在する証明書を選択します。
	以下の方法で証明書をImport[インポート]したり、新しい証明書 をGenerate[生成]したりすることもできます。
	Import[インポート]:
	 Certificate Name[証明書名] – インポートする証明書の名前を入 力します。
	 Shared[共有] – この証明書を複数の仮想システムで共有する場合にクリックします。
	 Certificate File[証明書ファイル] – Browse[参照] をクリックし、 証明書ファイルが配置されている場所に移動します。ファイル を選択してOpen[開く]をクリックします。
	• File Format[ファイル フォーマット] – 以下のいずれかを選択します。
	 Base64 Encoded Certificate (PEM)[Base64 エンコード済み証 明書 (PEM)] – 鍵ではなく、証明書が含まれます。クリアテキ ストです。
	 Encrypted Private Key and Certificate (PKCS12)[暗号化された秘密鍵と証明書 (PKCS12)] – 証明書と鍵の両方が含まれます。
	 Private key resides on Hardware Security Module[秘密鍵はハードウェアセキュリティモジュール上にあります] – ファイアウォールが、鍵が存在する HSM サーバーのクライアントである場合にクリックします。
	 Import Private Key[秘密鍵のインポート] – 証明書ファイルとは 別のファイル内に存在するため、秘密鍵をインポートする必要 がある場合にクリックします。
	 Block Private Key Export(秘密鍵のエクスポートをブロック する) – Import Private Key(秘密鍵のインポート)を選択す ると、スーパー ユーザーを含む管理者は秘密鍵をエクスポー トできないようにします。
	 Key File[キー ファイル] – キー ファイルを参照し、インポー トするキー ファイルに移動します。このエントリは、ファ イル フォーマットとして PEM を選択した場合に使用可能で す。
	 Passphrase[パスフレーズ]およびConfirm Passphrase[パスフレーズの確認] – 鍵にアクセスするために入力します。

IKE ゲートウェイの一般 設定	の意味
ローカル証明書名(続	Generate[生成]する場合
2)	 Certificate Name[証明書名] – 作成する証明書の名前を入力します。
	 Common Name[共通名] – 共通名を入力します。これは、証明書 に表記されるIPアドレスまたはFQDNです。
	• Shared[共有] – この証明書を複数の仮想システムで共有する場合にクリックします。
	 Signed By[署名者] – Select External Authority (CSR) [外部認証局 (CSR)] を選択するか、ファイアウォールの IP アドレスを入力し ます。このエントリは、CA である必要があります。
	 Certificate Authority[認証局] – ファイアウォールがルート CA の場合にクリックします。
	 Block Private Key Export(秘密鍵のエクスポートをブロック する) – Import Private Key(秘密鍵のインポート)を選択する と、スーパー ユーザーを含む管理者の秘密鍵のエクスポートを ブロックします。
	 OCSP Responder (OCSP レスポンダ) – 証明書が有効かどうか を追跡する OCSP を入力します。
	 Algorithm[アルゴリズム] – 証明書の鍵を生成するために RSA または Elliptic Curve DSA を選択します。
	 Number of Bits[ビット数] – 鍵のビット数として 512、1024、2048、または 3072 を選択します。
	 Digest[ダイジェスト] – ハッシュからの文字列を元に戻す方法として、MD5、SHA1、SHA256、SHA384、または SHA512 を選択します。
	 Expiration (days)[有効期限 (日)] – 証明書が有効である日数を入 力します。
	 Certificate Attributes[証明書の属性]Type(タイプ) – 必要に応じて、証明書に追加で含める属性タイプをドロップダウンリストから選択します。
	 Value[値] – 属性の値を入力します。
HTTP 証明書の交換	 ハッシュ & URL 方式を使用して証明書の取得場所をピアに通知するには、HTTP Certificate Exchange (HTTP 証明書の交換)をクリックし、Certificate URL (証明書 URL)を入力します。Certificate URL (証明書 URL)は、証明書を保存するリモートサーバーの URL です。

	の意味
	ピアもハッシュ & URL をサポートしていることがわかった場合 は、SHA1 ハッシュ & URL 交換を通じて証明書が交換されます。
	IKE 証明書ペイロードを受信すると、ピアは HTTP URL を参照し、 そのサーバーから証明書を取得します。次に、ピアは、証明書ペイ ロードに指定されたハッシュを使用して、HTTP サーバーからダウ ンロードした証明書をチェックします。
ローカルID	ローカル ピアが証明書でどのように識別されるかを指定します。 以下のタイプから1つを選択し、値を入力します。Distinguished Name[識別名](件名)、FQDN(ホスト名)、IP address、また はUser FQDN(電子メールアドレス)
ピアID	リモート ピアが証明書でどのように識別されるかを指定します。 以下のタイプから1つを選択し、値を入力します。Distinguished Name[識別名](件名)、FQDN(ホスト名)、IP address、また はUser FQDN(電子メールアドレス)
ピア ID チェック	Exact [完全] または Wildcard[ワイルドカード] を選択します。こ の設定は、証明書の検証のために検査されるピア ID に適用され ます。たとえば、Peer Identificationがdomain.com に等しい名前 で、Exact (完全)を選択した場合、IKE ID ペイロードの証明書に 指定されたピア IDが mail.domain2.com であったとすると、IKE ネ ゴシエーションは失敗します。しかし、Wildcard (ワイルドカー ド)を選択した場合、名前文字列のワイルドカードアスタリスク (*)の前にある文字はすべて一致する必要がありますが、* の後の 文字は異なっていてもかまいません。
ピア ID と証明書ペイ ロード ID の不一致を 許可する	ピア ID が証明書ペイロードに一致しなくても IKE SA を正常に確立 できるように柔軟性を持たせる場合に選択します。
証明書プロファイル	プロファイルを選択するか、新しい Certificate Profile (証明書プ ロファイル)を作成します。このプロファイルにより、ローカル ゲートウェイからピアゲートウェイへと送信される証明書に適用 される証明書オプションが設定されます。「Device(デバイス) > Certificate Management(証明書の管理) > Certificate Profile(証明 書プロファイル)」を参照してください。
ピアの拡張鍵使用の厳 密な検証を有効にする	鍵の使用方法を厳密に制御する場合に選択します。

IKE ゲートウェイの Advanced Options (詳細オプション) タブ

Network (ネットワーク) > Network Profiles (ネットワーク プロファイル) > IKE Gateways (IKE ゲートウェイ) > Advanced Options (詳細オプション)

パッシブモードやNATトラバーサル、IKEv2ポスト量子VPN、IKEv1デッドピア検出な ど、IKEゲートウェイの詳細設定を行います。

IKE ゲートウェイの詳細 オプション	の意味
パッシブ モードを有効 にする	クリックすると、ファイアウォールは IKE 接続に応答するのみ で、IKE 接続を開始しなくなります。
NAT トラバーサルを有 効にする	クリックすると、IKE および UDP プロトコルで UDP カプセル化が 使用され、中間 NAT デバイスを通過できるようになります。
	NAT トラバーサルは、IPsec VPN 端点の間にあるデバイスでネッ トワーク アドレス変換 (NAT) が設定されている場合に有効にしま す。
IKEv1 タブ	
交換モード	auto[自動]、aggressive[アグレッシブ]、または main[メイン] を 選択します。auto[自動] モード (デフォルト) の場合、デバイス は、main[メイン] モードと aggressive[アグレッシブ] モードの両方 のネゴシエーション要求を受け入れることができますが、可能なと きはいつでもネゴシエーションを開始し、main[メイン] モードで鍵 交換を行えます。ピア デバイスは同一の鍵交換モードで設定し、最 初のデバイスから開始されたネゴシエーション リクエストを受け入 れられるようにする必要があります。
IKE 暗号化プロファイ ル	既存のプロファイルを選択するか、デフォルト プロファイルを維持 するか、新しいプロファイルを作成します。IKEv1 と IKEv2 用に選 択したプロファイルは異なる場合があります。 IKE 暗号化プロファイルの詳細は「Network(ネットワーク)> Network Profiles(ネットワーク プロファイル)> IKE Crypto(IKE 暗号)」を参照してください。
フラグメンテーション を有効にする	クリックすると、ローカル ゲートウェイが IKE フラグメント パ ケットを受信できるようになります。最大フラグメント パケット サイズは 576 バイトです。
Dead Peer Detection	クリックして有効にし、間隔 (2 ~ 100秒) と再試行回数 (2 ~ 100) を入力します。デッドピア検知 (DPD) は、非アクティブまたは使用 不能な IKE ピアを識別します。ピアが使用不能になった場合の失わ れたリソースの復元に役立ちます。

IKE ゲートウェイの詳細 オプション	の意味
IKEv2の[詳細オプショ:	ン (Advanced Options)]の[全般 (General)]タブ
IKE 暗号化プロファイ ル	既存のプロファイルを選択するか、デフォルト プロファイルを維持 するか、新しいプロファイルを作成します。IKEv1 と IKEv2 用に選 択したプロファイルは異なる場合があります。 IKE 暗号化プロファイルの詳細は「Network(ネットワーク)> Network Profiles(ネットワーク プロファイル)> IKE Crypto(IKE 暗号)」を参照してください。
Cookie の厳密な検証	クリックすると、IKE ゲートウェイで Strict Cookie Validation[Cookie の厳密な検証] が有効になります。
	 Strict Cookie Validation[Cookie の厳密な検証] を有効にする と、IKEv2 Cookieが常に検証されるようになります。イニシエー タは、Cookieを含む IKE_SA_INITを送信する必要があります。
	 Strict Cookie Validation[Cookieの厳密な検証] を無効にすると (デフォルト設定)、VPNセッションの設定であるグローバルな Cookie Activation Threshold[Cookieアクティベーションのしき い値] と照らして、ハーフオープン SA の数が確認されます。 ハーフオープン SA の数が Cookie Activation Threshold[Cookie アクティベーションのしきい値] を超えた場合、イニシエータ は、Cookie を含む IKE_SA_INIT を送信する必要があります。
ライブネス チェック	IKEv2 の Liveness Check[ライブネス チェック] は常にオンになって います。すべての IKEv2 パケットは、ライブネス チェックのため に使用されます。このボックスをクリックすると、ピアがアイドル 状態になって所定の秒数が経過したときに、空の情報パケットが送 信されます。範囲:2~100デフォルト:5.
	必要な場合、IKEv2 パケットを送信しようとする側は、ライブネス チェックを最大 10 回試行します (すべての IKEv2 パケットがリト ランスミッション設定に影響します)。応答が得られない場合、送 信側は IKE_SA と CHILD_SA を閉じて削除します。送信側は、別の IKE_SA_INIT を送信して、もう一度やり直します。
IKEv2 の[Advanced Options (詳細オプション)] [PQ PPK] タブ	
ポスト・クアンタムの 事前共有鍵 (PPK) を有 効にする	Enable Post-Quantum Pre-Shared Key(PPK) –Post-Quantum Pre-Shared Key(PPK)を使用して量子コンピュータによる攻撃に 耐えるポスト量子VPNを作成するには、PPKを有効にし、IKEv2を サポートするVPNで設定します。PPKはIKEv1ではサポートされて いません。 Enable Post-Quantum Pre-Shared Key(PPK) はデフォ ルトで無効になっています。

П

KE ゲートウェイの詳細 †プション	の意味
	ネゴシエーションモード:
	 Preferred (優先)-応答ピアが PPK (RFC 8784)をサポートしている場合、PPK を使用します。ピアが RFC 8784 をサポートしていない場合、IKEv2 ハンドシェイクは古典的な鍵交換(Diffie-Hellman)にフォールバックします。これがデフォルトのネゴシエーションモードです。
	 Mandatory (必須)—応答ピアは RFC 8784 PPK をサポートする必要があります。応答側のピアが RFC 8784 をサポートしていない場合、開始側のピアは接続を中止します。
	PPK KeyID-関連するPPKを識別する名前です。開始ピア のPPKはPPK KeyIDを応答ピアに送信し、応答ピアが関連す るPPKを検索できるようにします。
	Post-Quantum Pre-shared Key(PPK) :その KeyID に関連付け られた秘密鍵。PPKはピア間で転送されないため、Harvest Now, Decrypt Later攻撃に対してネイティブに脆弱ではなく、Shorのアル ゴリズムに対しても脆弱ではありません。
	 IKEv2 ピアが PPK を使用してネゴシエートするには、 両方のピアの IKEv2 ゲートウェイに設定されている KeyID と PPK のペアがまったく同じである必要があり ます。イニシエータが、対応する KeyID と PPK のペ アを持たないレスポンダとピアリングしようとする と、その試みは中止されます。
	「アクティベート (Activate)」-ファイアウォールで使用できる PPK を表示します。少なくとも1つのPPKをアクティブにする必要 があります。ファイアウォールは、アクティブ化されたPPKからラ ンダムにPPKを選択し、応答するピアとのIKEv2ピアリングを開始 します。PPK のアクティブ化と非アクティブ化は、PPK の追加時 または編集時に行います。RFC 8784 によると、ファイアウォール が PPK を選択すると、IKEv2 ゲートウェイのライフタイム中(IKE キーの再生成経由を含む)はその PPK を使用します。ファイア ウォールは、非アクティブ化されたPPKを選択から除外します。
	PPK KeylDとPPKのペアは10個まで追加できます。 [Add Post- Quantum Pre-shared Key (ポスト量子事前共有鍵の追加)] ダイアロ グボックスで、次の手順を実行します。
	 PPK KeyID-PPK Secret (事前共有鍵文字列)を識別する名前。 「PPK_ID1」や「Super_Strong_PPK5」など、任意の文字列値を 使用できます。
	● PPKシークレット-32-128文字(16-64バイト)の範囲の文字

PPKンークレット-32-128文子(16-64バイト)の範囲の文字
 列。文字列が長いほど鍵は強くなります。PPKシークレットは、

IKE ゲートウェイの詳細 オプション	の意味
	そのPPK KeylDに関連付けられます。任意の文字列を入力することも、ファイアウォールで自動的にStrong PPKを生成させることもできます。
	64文字(32バイト)以上の文字列を設定します。
	ファイアウォールはピア間でPPKを送信することはないた め、Harvest Now, Decrypt Later攻撃に対してネイティブに脆 弱ではなく、Shorのアルゴリズムに対しても脆弱ではありませ ん。
	 [Commin PPK Secret (PPK) - クレットを確認)] - [PPK Secret (PPK Secret)] 文字列は、 [PPK Secret (PPK Secret)] フィールドに入力した文字列と正確に一致している必要があり ます。
	 [Activate (アクティベート)] –IKEv2 ピアリングに使用する PPK をアクティブにするには、このボックスをオンにします。 新しいPPKはデフォルトでアクティブになります。PPKを無効に するには、チェックボックスをオフにします。PPKを追加すると き、およびPPKを選択して編集するときに、PPKをアクティブ化 および非アクティブ化できます。
	 [PPK length (characters) (PPKの長さ(文字数))] -ファイ アウォールに PPK Secret を入力する代わりに強力な PPK Secret を生成させることを選択した場合、このフィールドには自動生 成される PPK 刺の長さが設定されます。デフォルトは32文字 (最小長)ですが、セキュリティ向上のために、64文字(32バ イト)以上の文字列を生成します。
	 [Generate Strong PPK (強力なPPKの生成)] –ファイアウォー ルで [PPK length (characters) (PPKの長さ(文字数)] フィールドで指定した長さの PPK Secret 文字列を生成する場合 にクリックします。
	ファイアウォールに強力なPPKシークレットを生成させると、 [強力なPPKシークレット]ダイアログボックスに結果が表示 されます。文字列を選択してコピーし、[PPK Secret (PPKシーク レット)]フィールドと [Confirm PPK Secret (PPKシークレットの 確認)]フィールドに文字列を貼り付け、秘密を安全な場所に保存 してピアの管理者に伝え、ピアにインストールすることができ ます。16進文字列のみをコピーし、先頭の「PPK:」はコピー

IKE ゲートウェイの詳細 オプション	の意味
	しないでください。たとえば、生成されたPPKが次のように表示 されるとします。
	PPK:2b02b6ea61241c29180998458c2e27a616進文字列
	のみをコピーして貼り付けます。
	2b02b6ea61241c29180998458c2e27a6
	PPKシークレットの文字列は、漏洩しないように注意してガードしてください。文字列を別の管理者に伝える必要がある場合は、暗号化メールなどの安全なメカニズムを使用してください。悪徳業者がPPKシークレットを入手した場合、量子コンピュータとショアのアルゴリズムで暗号鍵を解読できる可能性が高くなる。

IKE ゲートウェイの再起動または更新

• Network > IPSec Tunnels [ネットワーク > IPSec トンネル]

トンネルのステータスを表示する場合は、Network(ネットワーク) > IPSec Tunnels(IPSec ト ンネル)を開きます。2番目の状態列には、IKE情報へのリンクがあります。再起動または更新 するゲートウェイをクリックします。IKE Info [IKE 情報] ページが開きます。リストのエントリ のいずれかをクリックし、次のいずれかをクリックします。

- Restart(再起動) 選択したゲートウェイを再起動します。再起動すると、トラフィックのトンネル通過が中断されます。IKEv1とIKEv2の再起動の動作は、以下のように異なります。
 - IKEv1 フェーズ1SA またはフェーズ2SA は、別々に再起動(クリア)でき、そのSA のみが影響を受けます。
 - IKEv2 IKEv2 SA を再起動すると、子 SA(IPSec トンネル)がすべてクリアされます。 IKEv2 SA を再起動すると、基礎となる IPSec トンネルもすべてクリアされます。

IKEv2 SA に関連付けられている IPSec トンネル (子 SA) を再起動しても、その IKEv2 SA に は影響が及びません。

• Refresh (更新) – IKE SA の現在の状態を表示します。

Network > Network Profiles > IPSec Crypto [ネットワーク > ネットワーク プロファイル > IPSec 暗号]

IPSec SA ネゴシエーション (フェーズ 2) に基づいて、VPN トンネルでの認証および暗号化のプロトコルとアルゴリズムを指定する場合は、Network > Network Profiles > IPSec Crypto[ネットワーク > ネットワークプロファイル > IPSec暗号化] ページを使用します。



GlobalProtect ゲートウェイとクライアント間の VPN トンネルについては、 「Network(ネットワーク) > Network Profiles(ネットワーク プロファイル) > GlobalProtect IPSec Crypto(GlobalProtect の IPSec 暗号)」を参照してください。

IPSec 暗号化プロファイ ル設定	の意味
氏名	プロファイルを識別するName (名前)を入力します(最大 31 文 字)。名前の大文字と小文字は区別されます。また、一意の名前に する必要があります。文字、数字、スペース、ハイフン、およびア ンダースコアのみを使用してください。
IPSec プロトコル	 VPN トンネルを横断するデータを保護するためのプロトコルを選択します。 ESP - Encapsulating Security Payload (ESP) プロトコルは、データの暗号化、ソースの認証、およびデータ整合性の検証を行います。 AH - Authentication Header (AH) プロトコルは、ソースの認証とデータ整合性の検証を行います。 緩続の機密性(暗号化)および認証を提供できるESPプロトコルを使用します。
暗号化 (ESP プロトコ ルのみ)	Add[追加]をクリックし、目的の暗号化アルゴリズムを選択しま す。セキュリティを最大限に高めるには、Move Up および Move Down を使用して、順序 (上から下へ)を aes-256-gcm、aes-256- cbc、aes-192-cbc、aes-128-gcm、aes-128-ccm (VM-Series firewall ではこのオプションをサポートしていません)、aes-128-cbc、およ び 3des に変更します。null (暗号化なし)を選択することもできま す。
認証	Add[追加] をクリックし、目的の認証アルゴリズムを選択します。 セキュリティを最大限に高めるため、項目を選択してMove Up[上 へ]アイコンまたはMove Down[下へ]アイコンをクリックし、以

IPSec 暗号化プロファイ ル設定	の意味		
	下のように順序が降順になるように変更します。sha512, sha384, sha256, sha1, md5.IPSec Protocol[IPSec プロトコル] が ESP の場合 は、none[なし] (認証なし) を選択することもできます。		
	 md5およびsha1は安全ではないため、sha256あるい はそれより強固な認証を使用します。短期間のセッ ションではsha256を、金融取引のように極めてセ キュアな認証が必要なトラフィックではsha384以上 を使用します。 		
DH グループ	インターネット キー交換 (IKE) の Diffie-Hellman (DH) グループを 選択します: group1, group2, group5, group14, group15, group16, group19, group20, group21 を選択します。セキュリティを最も強 化するには、数値が最も大きいグループを選択します。IKE フェー ズ1でファイアウォールが作成する鍵を更新しない場合は、[no- pfs] (no perfect forward secrecy) を選択します。ファイアウォール は、IPSec セキュリティ アソシエーション (SA) ネゴシエーションで 現在の鍵を再利用します。		
有効期間	単位を選択し、ネゴシエートされた鍵の有効期間を入力します(デ フォルト設定は1時間)。		
ライフサイズ	任意の単位を選択し、鍵が暗号化に使用できるデータ サイズを入力 します。		

Network > Network Profiles > IKE Crypto [ネットワーク > ネット ワーク プロファイル > IKE 暗号]

IKE Crypto Profiles(IKE 暗号化プロファイル)ページを使用して、識別、認証、および暗号化のプロトコルとアルゴリズムを指定します(IKEv1 または IKEv2、フェーズ 1)。

アルゴリズムまたはグループのリスト順序を変更する場合は、項目を選択して、Move Up[上 へ]またはMove Down[下へ]をクリックします。この順序によって、リモート ピアと設定をネゴ シエートするときに最初に選択される設定が決まります。リストの1番上にある設定から試行 され、成功するまでその下にある設定が順次試行されていきます。

IKE 暗号化プロファイル 設定	の意味
氏名	プロファイルの名前を入力します。

IKE 暗号化プロファイル 設定	の意味
DH グループ	DH (Diffie-Hellman) グループの優先 度を選択します。Add をクリック し、group1、group2、group5、group14、group15、group16、group19、grou または group21 を選択します。セキュリティを最大限に高めるた め、項目を選択し、Move Up[上へ] または Move Down[下へ] をク リックして、識別子の数値がより大きいグループがリストの上位に 表示されるように移動します。たとえば、group14 を group2 より も上に移動します。
authentication	 ハッシュアルゴリズムの優先度を指定します。Add[追加] をク リックしてアルゴリズムを選択します。セキュリティを最大限に 高めるため、項目を選択してMove Up[上へ]アイコンまたはMove Down[下へ]アイコンをクリックし、以下のように順序が降順にな るように変更します。 SHA512 sha384 sha256 sha1 md5
	 non-auth (認証なし) 暗号化に AES-GCM アルゴリズムを使用する場合、認 証設定を none-auth (認証なし) に選択する必要があり ます。ハッシュは、選択した DH グループに基づいて 自動的に選択されます。DH グループ 19 とそれ以下 では、sha256 とします。DH グループ 20 は sha384 を使用します。
暗号化	 適切なEncapsulating Security Payload (ESP) 認証グループを選択 します。Add[追加] をクリックしてアルゴリズムを選択します。 セキュリティを最大限に高めるため、項目を選択してMove Up[上 へ]アイコンまたはMove Down[下へ]アイコンをクリックし、以下 のように順序が降順になるように変更します。 aes-256-gcm (IKEv2 が必要です。DH グループは、グループ 20 に設定する必要があります。 0 aes-128-gcm 0 (IKEv2 が必要です。DH グループは グループ 19 に設定されています) aes-256-cbc aes-192-cbc

IKE 暗号化プロファイル 設定	の意味	
	• aes-128-cbc	
	3desIPv6	
	 aes-256-gcm および aes-128-gcm アルゴリズムには、 認証が組み込まれています。したがって、上記の場合は、Authentication(認証)設定をnone-auth (認証なし)に選択する必要があります。 	
キーの有効期間	時間の単位を選択し、ネゴシエートされたIKEフェーズ1キーの有 効期間(デフォルトは8時間)を選択します。	
	 IKEv2 – キーの有効期間が切れる前に、SAのキーを再生成 する必要があります。そうしないと、有効期限が切れたとき に、SAは新しいフェーズ1キーネゴシエーションを開始する必 要があります。 	
	 IKEv1 – 有効期限が切れないうちに前もってフェーズ1キーを 再生成することはありません。IKEv1 IPSec SA の有効期限が切 れてはじめて、IKEv1 フェーズ1キー再生成が起動されます。 	
IKEv2 多重認証	認証カウントを決定するために、キーの有効期間で乗算される値を 指定します(0~50の範囲、デフォルト設定は 0)。認証カウント は、ゲートウェイが IKEv2 IKE SA キー再生成を実行できる回数で あり、この回数だけ実行した後は、IKEv2 再認証をやり直す必要が あります。値として 0を指定すると、再認証機能が無効になりま す。	

Network > Network Profiles > Monitor [ネットワーク > ネット ワーク プロファイル > 監視]

IPSec トンネルをモニターしたり、ポリシーベースの転送(PBF)ルールのネクストホップデバイスをモニターしたりするには、モニタープロファイルを使用します。どちらの場合も、モニタープロファイルは、リソース (IPSec トンネルまたはネクストホップデバイス)が使用できなくなった場合に実行するアクションを指定するために使用されます。モニタープロファイルは 任意ですが、サイト間の接続を持続し、PBF ルールを確実に維持するのに非常に効果的です。 モニタープロファイルの設定には以下の設定が使用されます。

項目	の意味
氏名	モニター プロファイルの識別に使用する名前を入力します (最大 31 文字)。名前の大文字と小文字は区別されます。また、一意の名前に

項目	の意味
	する必要があります。文字、数字、スペース、ハイフン、およびア ンダースコアのみを使用してください。
操作	トンネルを使用できないときに実行するアクションを指定します。 ハートビート喪失の許容発生回数がしきい値に達すると、指定した アクションがファイアウォールによって実行されます。
	 wait-recover – トンネルが回復するまで待機します。他のアクションは実行しません。パケットは、PBF ルールに従って引き続き送信されます。
	 fail-over – トラフィックをバックアップパスにフェイルオーバーします (使用可能な場合)。ファイアウォールはルーティングテーブル検索を使用してこのセッション中のルーティングを判別します。
	どちらの場合も、早く回復できるようにファイアウォールによって 新しい IPsec 鍵がネゴシエートされます。
間隔	ハートビート間隔(範囲は 2~10、デフォルトは 3)を指定しま す。
しきい値	ハートビートの喪失回数のしきい値を指定します(範囲は 2~10、 デフォルトは 5)。この回数を超えると指定したアクションがファ イアウォールによって実行されます。

Network > Network Profiles > Interface Mgmt [ネットワーク > ネットワーク プロファイル > インターフェイス管理]

インターフェイス管理プロファイルは、ファイアウォールインターフェイスがアクセスを許容 するサービスやIPアドレスを定義することで、ファイアウォールを不正なアクセスから保護し ます。インターフェイス管理プロファイルは、サブインターフェイスを含めたレイヤー3イーサ ネットインターフェイス、および理論インターフェイス(集約グループ、VLAN、ループバッ ク、およびトンネルインターフェイス)に割り当てることができます。Interface Management プロファイルを割り当てるには、Network > Interface を参照してください。 Telnet、SSH、HTTP、または HTTPS を許可するインターフェース管理プロファ イルを、インターネットまたはエンタープライズ・セキュリティー境界内の他 の非トラステッド・ゾーンからのアクセスを許可するインターフェースに接続 しないでください。これには、GlobalProtect ポータルまたはゲートウェイを設定 したインターフェイスが含まれます。GlobalProtect は、ポータルまたはゲート ウェイへのアクセスを可能にするためのインターフェイス管理プロファイルを必 要としません。firewallsとPanoramaへのアクセスを保護する方法の詳細について は、Adminstrative Access Best Practices を参照してください。

GlobalProtect ポータルまたはゲートウェイを構成したインターフェイスに Telnet、SSH、HTTP、または HTTPS を許可するインターフェイス管理プロファイル をアタッチしないでください。これは、管理インターフェイスをインターネットに 公開するため

項目	の意味		
氏名	プロファイル名 (最大 31 文字) を入力します。この名前は、インター フェイスを設定するときにインターフェイス管理プロファイルのリス トに表示されます。名前の大文字と小文字は区別されます。また、一 意の名前にする必要があります。文字、数字、スペース、ハイフン、 およびアンダースコアのみを使用してください。		
管理サービスの管理	 Telnet - ファイアウォールCLIにアクセスする際に使用します。Telnetはプレーンテキストを使用しますが、SSHよりは機密性が劣ります。 		
	インターフェイス上の管理トラフィックには、Telnet の代わりに SSH を有効化してください。		
	 SSH - ファイアウォールCLIに安全にアクセスする場合に使用します。 		
	 HTTP - ファイアウォールウェブインターフェイスにアクセス する際に使用します。HTTPはプレーンテキストを使用します が、HTTPSよりは機密性が劣ります。 		
	インターフェイス上の管理トラフィックには、HTTP の代わりに HTTPS を有効化してください。		
	 HTTPS - ファイアウォールウェブインターフェイスに安全にアクセ スする場合に使用します。 		
Network Services(ネット ワーク サービス)	 Ping - 外部サービスとの接続をテストする場合に使用します。 例えば、インターフェイスに対してpingを行い、Palo Alto NetworksアップデートサーバーからPAN-OSソフトウェアやコンテ ンツのアップデートが受信可能な状態かどうか確認することができ ます。 		

項目	の意味
	 HTTP OCSP - ファイアウォールをオンライン証明書状態プロトコル (OCSP) のレスポンダとして設定する場合に使用します。詳細は、「Device (デバイス) > Certificate Management (証明書の管理) > OCSP Responder (OCSP レスポンダ)」を参照してください。
	 SNMP - SNMPマネージャーからのファイアウォール状態クエリを 処理する場合に使用します。詳細は、「SNMP モニタリングの有効 化」を参照してください。
	 Response Pages[応答ページ] - 以下の応答ページを有効化する場合 に使用します。
	 Authentication Portal (認証ポータル) - Authentication Portal (認証ポータル)の応答ページを提供するために使 用されるポートは、NTLMの場合はポート 6080、SSL/TLS サーバープロファイルのないAuthentication Portal (認証 ポータル)の場合は 6081、SSL/TLS サーバープロファイル のAuthentication Portal (認証ポータル)の場合は 6082 です。 詳細は、「Device (デバイス) > User Identification (ユーザー ID) > Authentication Portal Settings (認証ポータルの設定)」 を参照してください。
	 URL Admin Override (URL 管理オーバーライド) - 詳細は、 「Device (デバイス) > Setup (セットアップ) > Content-ID」 を参照してください。
	 User-ID:ファイアウォール間でユーザー マッピングの データ再配 布 を有効にするために使用します。
	 User-ID Syslog Listener-SSL[User-ID Syslogリスナー-SSL] - PAN- OS統合User-IDエージェントによるSSL経由のsyslogメッセージの回 収を許可する場合に使用します。詳細は、「監視対象サーバーに対 するアクセスの設定」を参照してください。
	 User-ID Syslog Listener-UDP[User-ID Syslogリスナー-SSL] - PAN- OS統合User-IDエージェントによるUDP経由のsyslogメッセージの 回収を許可する場合に使用します。詳細は、「監視対象サーバーに 対するアクセスの設定」を参照してください。
アクセス許可IPアド レス	インターフェイスで許可されるアクセス元の IPv4 または IPv6 アドレ スのリストを入力します。

Network > Network Profiles > Zone Protection [ネットワーク > ネットワークプロファイル > ゾーンプロテクション]

ゾーンに適用するゾーン プロテクション プロファイルにより、最も一般的なフラッド、偵察 行為、その他のパケットベース攻撃、および IP 以外のプロトコルの使用、および特定のセキュ リティ グループ タグ (SGT) を持つ 802.1Q (Ethertype 0x8909) のヘッダーから保護されま す。Zone Protection (ゾーン プロテクション) プロファイルは、入力ゾーン (トラフィックが ファイアウォールに進入するゾーン) における幅広い保護を目的とするもので、特定のエンドホ ストや特定の宛先ゾーンに進入するトラフィックを阻止するものではありません。ゾーンには 1 つのゾーン プロテクション プロファイルを関連付けることができます。

ゾーンプロテクションプロファイルを各ゾーンに適用し、IPフラッド、偵察行為、パケットベースの攻撃、非 IPプロトコルの攻撃を防ぐ保護層を追加します。 ファイアウォール上のゾーンプロテクションは、インターネットの境界に位置する 専用の DDoS デバイスの後に来る2つ目の保護層でなければなりません。

ファイアウォールのゾーン プロテクション機能を強化するには、特定のゾーン、インターフェ イス、IP アドレス、またはユーザーを対象とした DoS プロテクション ポリシー(Policies(ポ リシー) > DoS Protection(DoS プロテクション))を設定します。



ゾーンプロテクションは1秒あたりのパケット数(pps)ではなく、1秒あたりの 新しい接続数(cps)に基づくため、パケットに対するセッション一致がない場合に のみ適用されます。パケットが既存のセッションに一致する場合は、ゾーンプロテ クション設定をバイパスします。

確認すべき情報	以下を参照
ゾーン プロテクション プロ ファイルを作成する方法は?	 ゾーンプロテクションプロファイルの構成要素 フラッド防御 偵察行為防御 パケットベースの攻撃保護 プロトコル保護 イーサネット SGT 保護 L3 & L4 ヘッダー インスペクション

ゾーン プロテクション プロファイルの構成要素

ゾーン プロテクション プロファイルを作成するには、プロファイルを **Add**(追加)して、名前 を付けます。

ゾーン プロテ クション プロ ファイル設定	設定場所	の意味
氏名	ネットワーク > ネットワー ク プロファ イル > ゾーン	プロファイル名(最大 31 文字)を入力します。この名前 は、ゾーンを設定するときに Zone Protection(ゾーン プロ テクション)プロファイルのリストに表示されます。名前の 大文字と小文字は区別されます。また、一意の名前にする必

ゾーン プロテ クション プロ ファイル設定	設定場所	の意味
	プロテクショ ン	要があります。文字、数字、スペース、およびアンダースコ アのみを使用してください。
の意味		Zone Protection(ゾーン プロテクション)プロファイルの 任意の説明を入力します。

以下のような、ゾーンで必要となる保護のタイプに合わせて設定を組み合わせ、引き続きゾーン プロテクション プロファイルを作成します。

- フラッド防御
- 偵察行為防御
- パケットベースの攻撃保護
- プロトコル保護
- イーサネット SGT 保護

複数の仮想システムがある環境で、以下を有効にしている場合は、

- 仮想システム間の通信が可能な外部ゾーン
- 仮想システムが外部通信に共通インターフェイスおよび1 つの IP アドレスを共 有できる共有ゲートウェイ

以下のゾーンおよび DoS プロテクション メカニズムが、外部ゾーンで無効になり ます。

- SYN cookies
- IPフラグメント
- ICMPv6

共有ゲートウェイ用に IP フラグメントと ICMPv6 防御を有効にするには、共有ゲートウェイ用のゾーン プロテクション プロファイルを個別に作成する必要があります。

共有ゲートウェイで SYN フラッドから保護するには、ランダム早期ドロップまたは SYN Cookie のいずれかを設定した SYN フラッド防御プロファイルを適用できます。 外部ゾーンでは、SYN フラッド防御にランダム早期ドロップのみを使用できます。

フラッド防御

• [ネットワーク > ネットワーク プロファイル > ゾーン プロテクション > フラッド防御]

SYN、ICMP、ICMPv6、SCTP INIT、UDP パケットのフラッド防御に加えて、その他のタイプの IP パケットのフラッディングに対する保護を提供するプロファイルを設定します。レートは 1 秒あたりの接続数です。 たとえば、既存のセッションに一致しない受信 SYN パケットは新しい 接続と見なされます。

ゾーン プロテ クション プロ ファイル設定 – フラッド防 御	設定場所	の意味
SYN	ネットワーク > ネッ トワーク プロファイ ル 、 ゾーン プロテク	SYN フラッドに対する防御を有効にする場合に選択 します。
操作	ル > ソーン フロテク ション > フラッド防 御	SYN フラッド攻撃に対して実行するアクションを選 択します。
		 Random Early Drop (ランダム早期ドロップ) – フ ラッド攻撃を軽減するために SYN パケットを廃棄 します。
		 フローが Alert[アラート] 率のしきい値を上回 ると、アラームが生成されます。
		 フローが Activate (アクティベート)率のしき い値を上回ると、ファイアウォールはフローを 制限するために個々の SYN パケットをランダ ムに廃棄します。
		 フローが Maximum(最大)率のしきい値を上回ると、すべての受信 SYN パケットを廃棄します。
	 SYN Cookies (SYN Cookie) – ファイアウォー ルがプロキシのように動作し、SYN をインター セプト、SYN の宛先であったサーバーの代わり に Cookie を生成して、元の送信元に Cookie 付 き SYN-ACK を送信します。送信元が Cookie 付 き ACK をファイアウォールに返したときにの み、ファイアウォールは送信元を有効とみなし て、SYN をサーバーに転送します。このアクショ ンをお勧めします。 	
		SYN クッキー がアクティブ化されている場合、 ファイアウォールは SYN/ACK のプロキシ時にこれらの値を認識しないため、サーバーが送信する TCP オプションを受け入れなくなります。したがって、TCP サーバーのウィンドウ サイズやMSS 値などの値は、TCP ハンドシェイク中にネゴシエートできず、ファイアウォールは独自の既定

ゾーン プロテ クション プロ ファイル設定 – フラッド防 御	設定場所	の意味
		値を使用します。サーバーへのパスの MSS がファ イアウォールの既定の MSS 値よりも小さい場合、 パケットをフラグメント化する必要があります。
		SYN Cookie は正当なトラフィックを 公正に扱いますが、RED よりも多く のファイアウォールリソースを消費 します。SYN Cookie がリソースを多 く消費しすぎている場合は RED に切 り替えてください。大量の DoS 攻撃 を防止する専用の DDoS 防止デバイ スがファイアウォールの前に存在し ない場合は、必ず RED を使用しま す。
アラーム レート(接 続数/秒)	Network (ネット ワーク) > Network Profiles (ネット ワーク プロファ イル) > Zone Protection (ゾーン プロテクション) > Flood Protection (フ ラッド防御) (cont) (続き)	 アラームのトリガーとなる、1秒あたりにゾーンが 受信する SYN パケット数(既存のセッションに一致 しない)を入力します。ダッシュボードおよび脅威 ログ(Monitor(監視) > Packet Capture(パケット キャプチャ))でアラームを確認できます。範囲は 0~2,000,000です。デフォルトは 10,000です。 ◎ 通常の変動に対応し、アラームが多す ぎる場合はしきい値を調整するには、 平均ゾーン CPS レートを 15~20%上 回るしきい値に設定します。
アクティ ベーション (接続/秒)		ゾーンプロテクションプロファイルで指定したアク ションのトリガーとなる、1秒あたりにゾーンが受 信する SYN パケット数(既存のセッションに一致し ない)を入力します。ファイアウォールはアルゴリ ズムを使用して、攻撃の割合が Maximum(最大) 率に到達するまで、攻撃の増加に合わせて廃棄する パケットの数を徐々に増やします。ファイアウォー ルは、受信する割合が Activate(アクティベート) のしきい値を下回ると、SYN パケットの廃棄を停止 します。RED の場合、範囲は 1~2,000,000 で、デ フォルトは 10,000 です。SYN クッキーの場合、範 囲は 0~2,000,000 で、デフォルトは 0 です。

ゾーン プロテ クション プロ ファイル設定 	設定場所	の意味
御		 ・正当なトラフィックのスロットルを回 避し、必要に応じてしきい値を調整す るには、ゾーンのピーク CPS レートの すぐ上にしきい値を設定します。
最大 (接 続/秒)		 1秒あたりにゾーンが受信する SYN パケットの最大数(既存のセッションに一致しない)を入力します。最大値を超過した分のパケットは廃棄されます。範囲は1~2,000,000です。デフォルトは RED の場合は 40,000です。デフォルトは SYN クッキーの場合 1,000,000です。このしきい値を超えると、CPS レートがしきい値を下回るまで新しい接続がブロックされます。 ⑦ ファイアウォール リソースを消費するその他の機能を考慮して、ファイアウォールの容量の 80~90% にしきい値を設定します。
ICMP	Network(ネット ワーク) > Network	ICMP フラッドに対する防御を有効にする場合に選択 します。
アラーム レート(接 続数/秒)	Profiles(ネット ワーク プロファ イル) > Zone Protection(ゾーン プロテクション) > Flood Protection(フ ラッド防御) (cont)(続き)	攻撃アラームのトリガーとなる、1秒あたりにゾー ンが受信する ICMP エコー要求の数(既存のセッ ションに一致しない ping)を入力します。範囲は 0 ~ 2000000、デフォルトは 10,000。
アクティ ベーション (接続/秒)		1 秒あたりにゾーンが受信する ICMP パケット数 (既存のセッションに一致しない)を入力します。 入力値を超過した分の ICMP パケットは廃棄されま す。ファイアウォールはアルゴリズムを使用して、 攻撃の割合が Maximum (最大)率に到達するまで、 攻撃の増加に合わせて廃棄するパケットの数を徐々 に増やします。ファイアウォールは、受信する割合 が Activate (アクティベート)のしきい値を下回る

ゾーン プロテ クション プロ ファイル設定 – フラッド防 御	設定場所	の意味 と JCMD パケットの感音を停止します。 範囲は 1
		 2、ICMPハグットの廃棄を停止します。範囲は1 ~ 2,000,000、デフォルトは 10,000 です。 正当なトラフィックのスロットルを回 避し、必要に応じてしきい値を調整す るには、ゾーンのピーク CPS レートの すぐ上にしきい値を設定します。
最大 (接 続/秒)		1 秒あたりにゾーンが受信する ICMP パケットの最 大数(既存のセッションに一致しない)を入力し ます。最大値を超過した分のパケットは廃棄されま す。範囲は 1 ~ 2,000,000、デフォルトは 40,000 で す。
		ファイアウォール リソースを消費す るその他の機能を考慮して、ファイア ウォールの容量の 80~90% にしきい値 を設定します。
SCTP 初期化	Network (ネット ワーク) > Network Profiles (ネット ワーク プロファ イル) > Zone Protection (ゾーン プロテクション) > Flood Protection (フ ラッド防御) (cont) (続き)	開始(INIT)チャンクを含むストリーム制御伝送プ ロトコル(SCTP)パケットのフラッドに対する保 護を有効にする場合に選択します。INIT チャンクは 他のチャンクとバンドルできないので、パケットは SCTP INIT パケットと呼ばれます。
アラーム レート(接 続数/秒)		攻撃アラームのトリガーとなる、1秒あたりにゾー ンが受信する SCTP INIT パケット数(既存のセッ ションに一致しない)を入力します。範囲は 0 ~ 2,000,000 です。デフォルトのファイアウォール モードごとのパケット数は以下の通りです。
		• PA-5280 -10,000
		• PA-5260-7,000
		 PA-5250-5,000 PA-5220-3.000
		• VM-700-1,000
		• VM-500-500
		• VM-300-250
		• VM-100-200

ゾーン プロテ クション プロ ファイル設定 – フラッド防 御	設定場所	の意味 • VM-50-100
アクティ ベーション (接続/秒)		1 秒あたりにゾーンが受信する SCTP INIT パケット 数(既存のセッションに一致しない)を入力しま す。入力値を超過した分の SCTP INIT パケットは廃 棄されます。ファイアウォールはアルゴリズムを使 用して、攻撃の割合が Maximum (最大)率に到達す るまで、攻撃の増加に合わせて廃棄するパケットの 数を徐々に増やします。ファイアウォールは、受信 する割合が Activate (アクティベート)のしきい値 を下回ると、SCTP INIT パケットの廃棄を停止しま す。範囲は1~2,000,000 です。ファイアウォール モ デルごとのデフォルトは、アラーム レートと同じで す。
最大 (接 続/秒)	Network (ネット ワーク) > Network Profiles (ネット ワーク プロファ イル) > Zone Protection (ゾーン プロテクション) > Flood Protection (フ ラッド防御) (cont) (続き)	 1秒あたりにゾーンが受信する SCTP INIT パケット の最大数(既存のセッションに一致しない)を入力 します。最大値を超過した分のパケットは廃棄され ます。範囲は1~2,000,000 です。デフォルトのファ イアウォール モードごとのパケット数は以下の通り です。 PA-5280-20,000 PA-5260-14,000 PA-5250-10,000 PA-5220-6,000 VM-700-2,000 VM-500-1,000 VM-500-1,000 VM-300-500 VM-100-400 VM-50-200
UDP	Network (ネット ワーク) > Network Profiles (ネット ワーク プロファ イル) > Zone Protection (ゾーン プロテクション) >	UDP フラッドに対する防御を有効にする場合に選択 します。
アラーム レート(接 続数/秒)		攻撃アラームのトリガーとなる、1 秒あたりにゾー ンが受信する UDP パケット数(既存のセッションに 一致しない)を入力します。範囲は 0 ~ 2000000、 デフォルトは 10,000。

ゾーン プロテ クション プロ ファイル設定 – フラッド防 御	設定場所	の意味
	Flood Protection(フ ラッド防御) (cont)(続き)	 ・通常の変動に対応し、アラームが多す ぎる場合はしきい値を調整するには、 平均ゾーン CPS レートを 15~20%上 回るしきい値に設定します。
アクティ ベーション (接続/秒)		 UDPパケットのランダム廃棄のトリガーとなる、1 秒あたりにゾーンが受信する UDPパケット数(既存のセッションに一致しない)を入力します。ファイアウォールはアルゴリズムを使用して、攻撃の割合が Maximum(最大)率に到達するまで、攻撃の増加に合わせて廃棄するパケットの数を徐々に増やします。ファイアウォールは、受信する割合がActivate(アクティベート)のしきい値を下回ると、UDPパケットの廃棄を停止します。範囲は1~2,000,000、デフォルトは10,000です。
最大 (接 続/秒)		 1秒あたりにゾーンが受信する UDP パケットの最大数(既存のセッションに一致しない)を入力します。最大値を超過した分のパケットは廃棄されます。範囲は1~2,000,000、デフォルトは 40,000 です。 ⑦ ファイアウォールリソースを消費するその他の機能を考慮して、ファイアウォールの容量の 80~90% にしきい値を設定します。
ICMPv6	Network(ネット ワーク) > Network	ICMPv6 フラッドに対する防御を有効にする場合に 選択します。
アラーム レート(接 続数/秒)	Profiles $(\ddot{x} \lor \lor \lor$ $\neg \neg $	攻撃アラームのトリガーとなる、1 秒あたりにゾー ンが受信する ICMPv6 エコー要求の数(既存のセッ ションに一致しない ping)を入力します。範囲は 0 ~ 2000000、デフォルトは 10,000。

ゾーン プロテ クション プロ ファイル設定 – フラッド防 御	設定場所	の意味
	ラッド防御) (cont)(続き)	 通常の変動に対応し、アラームが多す ぎる場合はしきい値を調整するには、 平均ゾーン CPS レートを 15 ~ 20% 上 回るしきい値に設定します。
アクティ ベーション (接続/秒)		 1秒あたりにゾーンが受信する ICMPv6 パケット数 (既存のセッションに一致しない)を入力します。 入力値を超過した分の ICMPv6 パケットは廃棄されます。ファイアウォールはアルゴリズムを使用して、攻撃の割合が Maximum(最大)率に到達するまで、攻撃の増加に合わせて廃棄するパケットの数を徐々に増やします。ファイアウォールは、受信する割合が Activate(アクティベート)のしきい値を下回ると、ICMPv6 パケットの廃棄を停止します。範囲は 1~2,000,000、デフォルトは 10,000 です。 ○ 正当なトラフィックのスロットルを回避し、必要に応じてしきい値を調整するには、ゾーンのピーク CPS レートのすぐ上にしきい値を設定します。
最大 (接 続/秒)		 1秒あたりにゾーンが受信する ICMPv6 パケットの 最大数(既存のセッションに一致しない)を入力し ます。最大値を超過した分のパケットは廃棄されま す。範囲は 1 ~ 2,000,000、デフォルトは 40,000 で す。 ◎ ファイアウォール リソースを消費す るその他の機能を考慮して、ファイア ウォールの容量の 80 ~ 90% にしきい値 を設定します。
その他の IP	Network(ネット ワーク) > Network Profiles(ネット	その他の IP(TCP 以外、ICMP 以外、ICMPv6 以 外、SCTP 以外、UDP 以外)フラッドに対する防御 を有効にする場合に選択します。
アラーム レート(接 続数/秒)	イル) > Zone Protection(ゾーン プロテクション) > Flood Protection(フ	攻撃アラームのトリガーとなる、1秒あたりに ゾーンが受信するその他の IP パケット(TCP 以 外、ICMP 以外、ICMPv6 以外、SCTP 以外、UDP 以 外のパケット)の数(既存のセッションに一致しな

ゾーン プロテ クション プロ ファイル設定 – フラッド防 御	設定場所	の意味
	ラッド防御) (cont)(続き)	 い)を入力します。範囲は 0 ~ 2000000、デフォルトは 10,000。 通常の変動に対応し、アラームが多すぎる場合はしきい値を調整するには、平均ゾーン CPS レートを 15 ~ 20%上回るしきい値に設定します。
アクティ ベーション (接続/秒)		その他の IP パケットのランダム廃棄のトリガーと なる、1 秒あたりにゾーンが受信するその他の IP パ ケット (TCP 以外、ICMP 以外、ICMPv6 以外、UDP 以外のパケット)の数(既存のセッションに一致し ない)を入力します。ファイアウォールはアルゴリ ズムを使用して、攻撃の割合が Maximum(最大)率 に到達するまで、攻撃の増加に合わせて廃棄するパ ケットの数を徐々に増やします。ファイアウォール は、受信する割合が Activate (アクティベート)の しきい値を下回ると、その他の IP パケットの廃棄を 停止します。範囲は 1~2,000,000、デフォルトは 10,000 です。
		避し、必要に応じてしきい値を調整す るには、ゾーンのピーク CPS レートの すぐ上にしきい値を設定します。
最大 (接 続/秒)		1 秒あたりにゾーンが受信するその他の IP パケット (TCP 以外、ICMP 以外、ICMPv6 以外、UDP 以外 のパケット)の最大数(既存のセッションに一致し ない)を入力します。最大値を超過した分のパケッ トは廃棄されます。範囲は 1 ~ 2,000,000、デフォ ルトは 40,000 です。
		ファイアウォール リソースを消費す るその他の機能を考慮して、ファイア ウォールの容量の 80~90% にしきい値 を設定します。

偵察行為防御

Network > Network Profiles > Zone Protection > Reconnaissance Protection [ネットワーク > ネットワーク プロファイル > ゾーン プロテクション > 偵察行為防御]

以下の設定で偵察行為防御を定義します。

ゾーン プロテ クション プロ ファイル設定 - 偵察行為防 御	設定場所	の意味
TCP ポート スキャン	ネットワーク > ネットワー	Enable (有効にする)は、TCPポートスキャンに対する保護を 設定します。
UDP ポート スキャン	ク ノロファ イル > ゾーン プロテクショ ン > 値察行為	Enable (有効にする)は、UDP ポート スキャンに対する保護 を設定します。
ホスト ス イープ	- ン > 偵察行為 防御 	Enable (有効にする)は、ホスト スイープに対する保護を設定 します。
IP プロトコル スキャン		Enable (有効にする)は、IP プロトコル スキャンに対する保護 を設定します。
操作	的作	以下の偵察行為に対してシステムが実行するアクションを指 定します。
		 Allow (許可)-ポート スキャン、ホスト スイープ、IP プロ トコルスキャンの偵察を許可します。
		 (Default (デフォルト)Alert (アラート)-ポート スキャン、ホスト スイープ、IP プロトコル スキャンのいずれかが、指定された時間間隔内で、指定されたしきい値を満たすたびにアラートを生成します。
		• Block[ブロック] – 指定した時間間隔が終わるまで、送 信元から宛先へ向けた後続のパケットをすべて廃棄しま す。
		 Block IP[ブロックIP] - 指定したDuration[持続時間]に わたり、後続のパケットをすべて廃棄します(範囲 は1~3600、単位は秒数)。Track By(追跡区分)によ り、送信元をブロックするか、あるいは送信元-宛先間 トラフィックをブロックするかを選択できます。すな わち、指定した時間間隔あたり単一の送信元から行わ れた制限回数以上の試みをブロックするか(制限の厳し い設定です)、または、特定の送信元と宛先のペアをも つ試みをブロックします(制限が比較的緩やかな設定で す)。

ゾーン プロテ クション プロ ファイル設定 – 偵察行為防 御	設定場所	の意味
		内部で行う脆弱性テストスキャンを除き、偵察行為スキャンをすべてブロックします。
間隔 (秒)		TCP または UDP ポート スキャンおよび IP プロトコル スキャンの探知を行う時間間隔(秒)です(範囲は 2 ~ 65,535、デフォルトは 2)。 ホスト スイープの探知を行う時間間隔(秒)です(範囲は 2 ~ 65,535、デフォルトは 10)。
しきい値 (イ ベント)		 指定されたアクションをトリガーする、指定された時間間隔内に検出されたポートスキャン、ホストスイープ、または IP プロトコルスキャンイベントの数(範囲は 2~65、535、デフォルトは 100)。 値 値察行為の試みをブロックする前に、デフォルトのイベントしきい値を使用していくつかのパケットをログに記録して分析を行います。
送信元アドレ スの除外		 偵察行為防御から除外する IP アドレス。リストは、最大 20 件の IP アドレスまたはネットマスク アドレス オブジェクト をサポートします。 Name (名称) -除外するアドレスの分かりやすい名称を 入力します。 Address Type (アドレス タイプ) -ドロップダウン リス トから IPv4 または IPv6 を選択します。 Address (アドレス) -ドロップダウン リストからアドレ スまたはアドレス オブジェクトを選択するか、手動で入 力します。 脆弱性テストを実行する、信頼できる内部グ ループの IP アドレスのみを除外します。

パケットベースの攻撃保護

Network > Network Profiles > Zone Protection > Packet Based Attack Protection [ネットワーク > ネットワーク プロファイル > ゾーン プロテクション > パケット ベースの攻撃保護]

Packet Based Attack protection (パケットベースの攻撃保護)を設定して、以下のパケットタイプをドロップできます。

- IP ドロップ
- TCP ドロップ
- ICMP ドロップ
- IPv6 Drop[IPv6ドロップ]:
- ICMPv6 ドロップ

IP ドロップ

ゾーンで受信した特定の IP パケットにどう対応するのかをファイアウォールに指示する場合 は、以下の設定を行います。

ゾーン プロテ クション プ ロファイル設 定 – パケット ベースの攻撃 防御	設定場所	の意味
スプーフされ た IP アドレ ス	ネットワーク > ネットワー クプロファ イル > ゾーン プロテクショ ン > パケット ベースの攻撃 保護 > IP ド ロップ	 入口パケットの送信元 IPアドレスがルーティング可能であ り、ルーティングインターフェイスが入口インターフェイス と同じゾーンにあることを確認してください。いずれかの条 件が真でない場合は、パケットを破棄します。 ファイアウォールは、このチェック中にポリ シーベース転送(PBF)ルールを考慮しません。 ルーティングテーブル(RIB)にリストされてい るルート、つまり CLI 出力の下にリストされて いるルートのみを考慮して、の出力ルーティ ング ルート を表示します。 なりすまし IP アドレスのパケットを内部ゾー ンでのみドロップし、必ず入力か所で送信元ア ドレスがファイアウォールのルーティングテー ブルとマッチすることを確認するようにしてく ださい。
厳密な IP アドレス チェック		 両方の条件が真であることを確認します。 送信元 IPアドレスは、入口インターフェイスのサブネットブロードキャスト IPアドレスではありません。 送信元 IPアドレスは、正確な入口インターフェイスを介してルーティングが可能です。 いずれかの条件が真でない場合は、パケットを破棄します。

ゾーン プロテ クション プ ロファイル設 定 – パケット ベースの攻撃 防御	設定場所	の意味
		 ファイアウォールは、このチェック中にポリ シーベース転送(PBF)ルールを考慮しません。 ルーティングテーブル(RIB)にリストされてい るルート、つまり CLI 出力の下にリストされて いるルートのみを考慮して、の出力ルーティン グ ルート を表示します。
		共通基準(CC) モードに設定されたファイアウォール については、破棄されたパケットのログを記録すること ができます。ファイアウォール Web インターフェイス で、Device (デバイス) > Log Settings (ログ設定)を開き ます。ログの管理のセクションで、Selective Audit[選択的監 査] を選択し、Packet Drop Logging[パケット破棄のログ] を 有効化します。
フラグメン トされたトラ フィック	-	フラグメント化されたIPパケットの廃棄
IP オプション のドロップ	_	このグループでこの設定を選択することで、ファイアウォー ルが、これらの IP オプションを含むパケットをドロップで きるようにします。
ストリクト ソース ルー ティング		 Strict Source Routing [ストリクト ソース ルーティング] IP オ プションが設定されたパケットを廃棄します。ストリクト ソース ルーティングは、データグラムのソースがルーティン グ情報を提供し、そのルーティング情報によってゲートウェ イまたはホストがデータグラムを送信するオプションです。 ジース ルーティングによって宛先 IP アドレス を一致条件として使用するセキュリティポリ シールールを攻撃者がバイパスできるようにな スキサーフトリン・フォーラ・ハングさた(
	_	るにめ、ストリクト ソース <i>ルーティンクを</i> 使 用するパケットをドロップします。
ルーズ ソー ス ルーティ ング		Loose Source Routing [ルーズ ソース ルーティング] IP オプ ションが設定されたパケットを廃棄します。ルーズ ソース ルーティングは、データグラムのソースがルーティング情 報を提供し、ゲートウェイまたはホストが多くの中間ゲート

ネットワーク

ゾーンプロテ クションプ ロファイル設 定 – パケット ベースの攻撃 防御	設定場所	の意味 ウェイの任意のルートを選択して、ルートの次のアドレスに
		 データグラムを送信できるオプションです。 ツースルーティングによって宛先 IP アドレス を一致条件として使用するセキュリティポリ シールールを攻撃者がバイパスできるようにな るため、ルーズ ソース ルーティングを使用す るパケットをドロップします。
タイムスタン プ		Timestamp [タイムスタンプ] IP オプションが設定されたパ ケットを廃棄します。
レコード ルート		Record Route [レコード ルート] IP オプションが設定された パケットを廃棄します。データグラムにこのオプションが含 まれるとき、データグラムをルーティングする各ルーターは 独自の IP アドレスをヘッダーに追加し、受信者へのパスを 提供します。
セキュリティ	_	セキュリティ オプションが定義されている場合、パケットを 廃棄します。
ストリーム ID	_	ストリーム ID が定義されている場合、パケットを廃棄します。
未知		クラスと番号が不明な場合、パケットを廃棄します。 〇〇 未知のパケットを破棄します。
異常な形式		RFC 791、1108、1393、2113 に基づいてクラス、番号、長 さの組み合わせに誤りがある場合、パケットを廃棄します。

TCP ドロップ

ゾーンで受信する特定の TCP パケットに対する対応方法をファイアウォールに指示する場合 は、以下の設定を行います。

ゾーン プロテ クション プ ロファイル設 定 – パケット ベースの攻撃 防御	設定場所	の意味
重複する TCP セグメントの 不一致	ネットワーク > ネットワー クプロファ イル > ゾーン プロテクショ ン > パケット ベースの攻 撃ロップ	攻撃者は、重複するけれども異なるデータを利用し接続を構 築して、接続の不正な解釈を引き起こすことがあります。攻 撃者は、IP スプーフィングとシーケンス番号予測を利用して ユーザーの接続をインターセプトし、攻撃者のデータを挿入 することがあります。重複の不一致をレポートし、セグメン トデータが以下のシナリオに一致しない場合にパケットを廃 棄するためには、この設定を使用します。 • セグメントが別のセグメント内にある。 • セグメントが別のセグメントの一部と重複する。 • セグメントが別のセグメントを完全に含んでいる。 この保護メカニズムは、シーケンス番号を使用して、TCP データストリーム内のどこにパケットが存在するかを判別し ます。 重複する TCP セグメントが一致しないパケッ トをドロップします。
スプリット ハンドシェイ ク		 一般的な 3 ウェイ ハンドシェークがセッション確立手順で 使用されない場合、TCP セッションの確立を防ぎます。許可 されないバリエーションの例として、4 ウェイまたは 5 ウェ イのスプリット ハンドシェークや同時オープン セッション の確立手順があります。 Palo Alto Networks の次世代ファイアウォールは、Split Handshake (スプリット ハンドシェーク)を設定しない場 合、スプリット ハンドシェークや同時オープン セッション の確立のためのセッションおよびすべてのレイヤー 7 プロセ スを適切に処理します。これをゾーン プロテクションプロ ファイルに対して設定し、プロファイルをゾーンに適用する 場合は、標準的な 3 ウェイ ハンドシェークを使用して、そ のゾーンのインターフェイスの TCP セッションを確立する 必要があります。バリエーションは許可されません。

ネットワーク

ゾーン プロテ クション プ ロファイル設 定 – パケット ベースの攻撃 防御	設定場所	の意味
データとの TCP SYN		3 ウェイ ハンドシェーク時の TCP SYN パケットにデータが 含まれる場合、TCP セッションの確立を防ぎます。デフォル トで有効になっています。
データとの TCP SYNACK		3 ウェイ ハンドシェーク時の TCP SYN-ACK パケットにデー タが含まれる場合、TCP セッションの確立を防ぎます。デ フォルトで有効になっています。
非 SYN TCP の拒否		 TCPセッションセットアップの最初のパケットがSYNパケットではない場合にパケットを拒否するかどうかを決定します。 Global[グローバル] - CLI で割り当てたシステム全体の設定を使用します。 はい - 非 SYN TCP を拒否します。 いいえ - 非 SYN TCP を担否します。 いいえ - 非 SYN TCP を受け入れます。 ① 非 SYN TCP トラフィックを受け入れると、ブロックの発生後にクライアント接続やサーバー接続が設定されていない場合にファイル ブロッキングポリシーが正常に動作しない可能性があります。 びーンでトンネル コンテンツ検査を設定してRematch Sessions (セッションの再マッチング)を有効化する場合、そのゾーンでのみReject Non-SYN TCP (SYN TCP 以外を拒否)し、トンネルコンテンツ検査ポリシーを有効化あるいは編集することでファイアウォールが既存のトンネルセッションをドロップしないようにします。
非対称パス		 同期していないACKまたはウィンドウ外のシーケンス番号を 含むパケットを破棄するかバイパスするかを決定します。 Global[グローバル] - TCP Settings (TCPの設定) または CLI で割り当てたシステム全体の設定を使用します。 drop[ドロップ] - 非対称パスを含むパケットをドロップ します。

ネットワーク

ゾーンプロテ クションプ ロファイル設 定 – パケット ベースの攻撃 防御	設定場所	の意味
		 bypass[バイパス] – 非対称パスを含むパケットでスキャン をバイパスします。
TCP オプショ ンの除去		TCP パケットから TCP タイムスタンプまたは TCP Fast Open オプションを除去するかどうかを決定します。
TCP タイムス タンプ	ネットワーク > ネットワー クプロファ イル > ゾーン プロテクショ ン > パケット ベースの攻 撃保護 > TCP ドロップ	パケットのヘッダーにTCPタイムスタンプがあるかどうかを 判断し、ある場合はヘッダーから除去します。
TCP Fast Open		TCP 3 ウェイハンドシェーク時の TCP SYN または SYN- ACK パケットから TCP Fast Open オプション(およびある 場合はデータ ペイロード)を除去します。 これを選択しない(無効にする)場合、TCP Fast Open オプ ションは許可されます。これによりデータ配信が含まれるた め、接続セットアップのスピードが維持されます。これは、 データとの TCP SYN、およびデータとの TCP SYN-ACK とは 独立して機能します。デフォルトで無効になっています。
マルチパス TCP (MPTCP) オプション		 TCP 拡張である MPTCP は、クライアントから宛先ホストへの接続で同時に複数のパスを使用し、接続を維持できるようにします。デフォルトでは、グローバル MPTCP 設定に基づき、MPTCP サポートは無効です。 このプロファイルに関連するセキュリティ ゾーンの MPTCP設定を、以下のように確認または調整します。 no (いいえ) – MPTCP サポートを有効にします(MPTCP オプションを除去しない)。 yes (はい) – MPTCP サポートを無効にします(MPTCP オプションを除去する)。これを設定すると、MPTCP には TCP への下位互換性があるため、MPTCP 接続が標準TCP 接続に変換されます。
ゾーン プロテ クション プ ロファイル設 定 – パケット ベースの攻撃 防御	設定場所	の意味
---	------	--
		 (デフォルト)global (グローバル) – グローバル MPTCP 設定に基づいて、MPTCP をサポートします。 グローバル MPTCP 設定はデフォルトでは yes (はい) に設定されているため、MPTCP は無効です (MPTCP オプションはパケットから除去されます)。TCP Settings (TCP設定)のStrip MPTCP option (Strip MPTCP オプション)を使用するか、以下の CLI コマンド を使用して、global MPTCP setting (グローバル MPTCP 設定)を確認または調整することができます。
		# set deviceconfig setting tcp strip-mptcp- option <yes no> (# デバイス設定設定 tcp sltrip -mptcp-option を設定する <yes no>)</yes no></yes no>

ICMP ドロップ

ゾーンで受信した特定の ICMP パケットをドロップするようにファイアウォールに指示する場合 は、以下の設定を選択して有効にします。

ゾーン プロテ クション プ ロファイル設 定 – パケット ベースの攻撃 防御	設定場所	の意味
ICMP ping ID 0	ネットワーク > ネットワー	ICMP pingパケットの識別子の値が0の場合、パケットを廃棄 します。
ICMP フラグ メント	ク フロファ イル > ゾーン プロテクショ ン > パケット ベースの攻撃 保護 > ICMP ドロップ	ICMPフラグメントで構成されるパケットを廃棄します。
ICMP 大型 パケット (>1024)		1024バイトを超えるICMPパケットを廃棄します。
エラー メッ セージととも に組み込まれ		エラーメッセージが組み込まれているICMPパケットを廃棄 します。

ゾーン プロテ クション プ ロファイル設 定 – パケット ベースの攻撃 防御	設定場所	の意味
ている ICMP を破棄		
ICMP TTL 失 効エラーを抑 制		ICMP TTL の有効期限切れメッセージの送信を停止します。
ICMP フラグ メント要求 メッセージを 抑制		インターフェイスの MTU を超えたパケットに対する ICMP フラグメント要求メッセージの送信を停止し、フラグメント なし (DF) ビットを設定します。この設定により、ファイア ウォールの背後のホストで PMTUD プロセスが実行されなく なります。

IPv6 Drop[IPv6ドロップ]:

ゾーンで受信した特定の IPv6 パケットをドロップするようにファイアウォールに指示する場合は、以下の設定を選択して有効にします。

ゾーン プロテ クション プ ロファイル設 定 – パケット ベースの攻撃 防御	設定場所	の意味
タイプ 0 の ルーティング ヘッダー	ネットワーク > ネットワー ク プロファ	タイプ0のルーティングヘッダーを含むIPv6パケットを廃 棄します。タイプ 0 のルーティング ヘッダーについては、 『RFC 5095』を参照してください。
IPv4 互換ア ドレス	イル > ソーシ プロテクショ ン > パケット ベースの攻撃 保護 > IPv6 Drop[IPv6ド ロップ]:	RFC 4291 IPv4互換用IPv6アドレスとして定義された IPv6パ ケットを破棄します。
エニーキャス ト送信元アド レス		エニーキャスト送信元アドレスを含むIPv6パケットを廃棄し ます。
不要なフラグ メントヘッ ダー		最終フラグメントフラグ (M=0) を含み、オフセットがゼロ のIPv6パケットを破棄します。

ネットワーク

ゾーン プロテ クション プ ロファイル設 定 – パケット ベースの攻撃 防御	設定場所	の意味
1280 バイト 未満の ICMP の MTU (パ ケットが大き すぎる)		最大転送単位(MTU)が1,280バイト未満の場合は、パケッ トが大きすぎるというICMPv6メッセージを含むIPv6パケッ トを破棄します。
ホップ バイ ホップ拡張		ホップバイホップオプション拡張ヘッダーを含むIPv6パケッ トを廃棄します。
Routing extension(ル- ティング拡 張)	_	ルーティング拡張ヘッダーを含むIPv6パケットを破棄しま す。ルーティング拡張ヘッダーを含むパケットは、宛先に向 かう際に1つ以上の中間ノードを経由します。
宛先の拡張		宛先オプション拡張を含むIPv6パケットを破棄します。宛先 オプション拡張には、パケットの宛先のみを対象としたオプ ションが含まれています。
拡張子ヘッ ダー内の無 効な IPv6 オプ ション		無効なIPv6オプションが拡張ヘッダーに含まれているIPv6パ ケットを破棄します。
ゼロ以外の予 約フィールド		ヘッダーの予約フィールドがゼロに設定されていないIPv6パ ケットを破棄します。

ICMPv6 ドロップ

ゾーンで受信した特定の ICMPv6 パケットに対して、対応方法をファイアウォールに指示する 場合は、以下の設定を選択して有効にします。

ゾーン プロテ クション プ ロファイル設 定 – パケット ベースの攻撃 防御	設定場所	の意味
ICMPv6 宛先 に到達不能 - 明示的なセ キュリティ ルールの一致 が必要です	ネットワーク > ネットワー クプロファ イル > ゾー ンプロテク ション > パ ケット ベー スの攻撃保護 > ICMPv6 ド ロップ	メッセージが既存のセッションと関連付けられている場合で も、ICMPv6 宛先到達不能メッセージがセキュリティ ルール と明確に一致している必要があります。
ICMPv6 パ ケットが大き すぎます - 明 示的なセキュ リティルー ルの一致が必 要です		メッセージが既存のセッションと関連付けられている場合で も、ICMPv6 パケット超過メッセージがセキュリティ ルール と明確に一致している必要があります。
ICMPv6 時間 超過 - 明示的 なセキュリ ティルール の一致が必要 です		メッセージが既存のセッションと関連付けられている場合で も、ICMPv6 の時間超過メッセージがセキュリティ ルールと 明確に一致している必要があります。
ICMPv6 パラ メータの問題 - 明示的なセ キュリティ ルールの一致 が必要です		メッセージが既存のセッションと関連付けられている場合で も、ICMPv6 のパラメータ エラー メッセージがセキュリティ ルールと明確に一致している必要があります。
ICMPv6 リダ イレクト - 明 示的なセキュ リティルー ルの一致が必 要です		メッセージが既存のセッションと関連付けられている場合で も、ICMPv6 のリダイレクト メッセージがセキュリティ ルー ルと明確に一致している必要があります。

プロトコル保護

Network (ネットワーク) > Network Profiles (ネットワーク プロファイル) > Zone Protection (ゾーン プロテクション) > Protocol Protection (プロトコル保護)

ファイアウォールは通常、レイヤー2ゾーン間とバーチャル ワイヤー ゾーン間の IP 以外のプロトコルを許可します。プロトコル保護を使用すると、レイヤー2 VLAN またはバーチャル ワイヤーのセキュリティゾーン間あるいはゾーン内において、IP 以外のどのプロトコルを許可するか(包含による)、拒否するか(除外による)を制御できます。IP 以外のプロトコルの例として、AppleTalk、Banyan VINES、Novell、NetBEUI や、Generic Object Oriented Substation Event (GOOSE) などの Supervisory Control and Data Acquisition (SCADA) システムが挙げられます。

ゾーン プロテクション プロファイルでプロトコル保護を設定した後、レイヤー 2 VLAN または バーチャル ワイヤーの入力セキュリティ ゾーンにプロファイルを適用します。

インターネットに接続されたゾーンでプロトコル保護を有効化し、使用しないプロトコルから来るレイヤー2トラフィックがネットワークに侵入しないようにします。

ゾーン プロテ クション プロ ファイル設定 – プロトコル 保護	設定場所	の意味
ルールの種類	ネットワーク > ネットワー クプロファ イル > ゾーン プロテクショ ン > プロトコ ル保護	プロトコル保護用に作成するリストのタイプを以下のように 指定します。 • Include List(許可リスト) – このリスト
		のプロトコルのみが許可されます。ただ し、IPv4(0x0800)、IPv6(0x86DD)、ARP(0x0806)、VLAN タグ フレーム(0x8100)は許可されます。その他のプロ トコルはすべて暗黙的に拒否(ブロック)されます。
		 Exclude List(除外リスト) – このリスト のプロトコルのみが拒否されます。その他 のプロトコルはすべて暗黙的に許可されま す。IPv4(0x0800)、IPv6(0x86DD)、ARP(0x0806)、VLAN タグフレーム(0x8100)は除外できません。

ゾーン プロテ クション プロ ファイル設定 – プロトコル 保護	設定場所	の意味
		 許可リストを使用し、使用するレイヤー2プロトコルのみを許可して他のプロトコルをすべて拒否します。これにより、ネットワーク上で使用しないプロトコルを拒否することで攻撃の入り口を減らすことができます。ファイアウォールは、除外リストに追加したプロトコルのみを拒否し、リストにないその他すべてのプロトコルを許可します。Protocol Protection(プロトコル保護)を設定しない場合、すべてのレイヤー2プロトコルが許可されます。
プロトコル名	_	リストに追加する Ethertype コードに対応するプロト コル名を入力します。ファイアウォールはプロトコル 名が Ethertype コードに一致することを確認しません が、Ethertype コードがプロトコル フィルタを特定します。
Enable [有効 化]	_	リストの Ethertype コードをEnable(有効化)します。しか し、テストのためにプロトコルを削除せずに無効にする場合 は、無効にしてください。
Ethertype (16 進数)	-	 Ox で始まる 16 進数の Ethertype コード(プロトコル) を入力します(範囲は 0x0000 ~ 0xFFFF)。リストには Ethertype を 64 個まで登録できます。 以下に Ethertype コードの参考資料をいくつか示します。 IEEE の 16 進数 Ethertype
		 standards.ieee.org/develop/regauth/ethertype/eth.txt http://www.cavebear.com/archive/cavebear/Ethernet/ type.html

イーサネット SGT 保護

 Network (ネットワーク) > Network Profiles (ネットワーク プロファイル) > Zone Protection (ゾーン プロテクション) > Ethernet SGT Protection (イーサネット SGT 保護)

Cisco TrustSec ネットワークのファイアウォールの場合、除外するレイヤ2セキュリティ グループ タグ (SGT) のリストを使用してゾーン プロテクション プロファイルを作成しま す。Zone Protection (ゾーン プロテクション) プロファイルをレイヤー2、仮想ワイヤー、あ るいはタップ インターフェイスに適用します。802.1Q (Ethertype 0x8909) ヘッダーを持つ着 信パケットにリスト内の SGT と一致する SGT があると、ファイアウォールはパケットをドロップします。

ゾーン プロテクション プロ ファイル設定 	 設定場所 	の意味
Layer 2 SGT Exclude List(レ イヤー2 SGT 除外リスト)	ネットワーク > ネットワー ク プロファイル > ゾーン プ ロテクション > イーサネット SGT 保護	Security Group Tags(SGT、 セキュリティ グループ タ グ)のリスト名を入力しま す。
タグ		ゾーンに適用されるゾーン プロテクション プロファイ ルのこのリストと SGT が一 致する場合、除外(ドロッ プ)するパケットのヘッダー にレイヤー 2SGT を入力しま す(0~65,535 の範囲)。
Enable [有効化]		Enable (有効化)(デフォ ルト)すると、Ethernet SGT protection(イーサネット SGT)保護用リストを除外し ます。除外リストを無効化す るには、 Enable (有効化)オ プションの選択を解除しま す。

L3 & L4 ヘッダー インスペクション

• ネットワーク>ネットワークプロファイル>ゾーン保護>L3およびL4ヘッダー検査

L3 & L4 ヘッダー インスペクションがグローバルに有効になっている場合、ファイアウォールは サポートされているプロトコル(IP/IPv6、ICMP/ICMPv6、TCP および UDP)内の脆弱性を検出し て防止し、ユーザ指定のカスタム ルールに一致するパケットをログに記録またはブロックでき ます。さらに、ヘッダー インスペクション カスタム ルールを使用して、セキュリティ ゾーンご とにネット インスペクション (ネットワーク ゾーン)を有効にする必要があります。

既存のルールを追加、削除、複製したり、ゾーン保護プロファイルによって評価されるカスタム ルールの優先順位と動作ステータスを定義したりできます。

ゾーン保護プロファイルで L3 および L4 ヘッダー インスペクションを設定した後、そのプロファイルを入力セキュリティ ゾーンに適用します。



Palo Alto Networks では、L3 および L4 ヘッダー検査の設定と有効化は、この機能を 有効にすると同時に動作できるゾーンの数が限られているため、カスタム ルールに 一致するパケットを検出して処理することが予想されるセキュリティ ゾーンでのみ 行うことを推奨します。

ゾーン保護プロ ファイル設定: 3	設定場所	詳説
および L4 ヘッ ダー検査		

Configuration [設定] タブ

一般

ルール	ネットワーク > ネットワーク プロファイル > ゾーン プロテ クション > L3 & L4 ヘッダー イ ンスペクション	カスタム ルールを識別する名前を入力します (最大 31 文字)。
脅威 ID		カスタムルール設定の脅威 ID 番号を指定します(脆 弱性シグネチャの範囲は 41000-45000 および 6800001-6900000)。
コメント		カスタムルールを説明するオプションのコメントを入 力します。
パケット キャプ チャ		カスタム ルールに一致する脆弱性が検出されたとき に、パケット キャプチャを有効にします。ファイア ウォールにパケット キャプチャを記録させたくない 場合は、ドロップダウンから single-packet または extended-capture、または disable を選択します。ま た、パケットがドロップされた場合に send icmp 到達 不能パケットを送信する して、セッションが許可され ていないことをクライアントに通知することもできま す。
IP の免除		カスタムルールを適用しない IP アドレスを入力しま す。

プロパティ

ログ重大度	ネットワーク > ネットワーク プロファイル > ゾーン プロテ クション > L3 & L4 ヘッダー イ ンスペクション	ファイアウォールがカスタム・ルールに一致する脆弱 性を検出したときに記録されるログ重大度レベルを指 定します。
ログ間隔		一致するイベントの最大ログ頻度 (秒単位) を指定しま す。
アクション		カスタムルールに一致する脆弱性がヘッダーで検出 されたときに実行するポリシーアクションを指定しま す。用意されているオプション:
		● allow [許可]
		• Alert [アラート]

ネットワーク

ゾーン保護プロ ファイル設定 :L3 および L4 ヘッ ダー検査	設定場所	詳説
		ドロップクライアントのリセット
		 サーバーのリセット
		• 両方のリセット

リファレンス

CVE	ネットワーク > ネットワーク プロファイル > ゾーン プロテ クション > L3 & L4 ヘッダー イ ンスペクション	脅威に関連付けられている既知のセキュリティ脆弱性 の識別子。共通脆弱性識別子(CVE)は、ベンダー固有 のIDが一般的に複数の脆弱性を含むため、固有の脆弱 性に関する情報を見つけるための最も有用な識別子で す。
Bugtraq		脆弱性に関連付けられた bugtraq 識別子 (CVE に類 似)。追加のバックグラウンドおよび分析の詳細のため の外部参照として使用できます。
ベンダー		脆弱性のベンダー固有識別子。
リファレンス		追加の分析または背景情報へのリンク。

Signature [シグネチャ] タブ

コメント	ネットワーク > ネットワーク プロファイル > ゾーンプロテ	オプションのコメントを入力して、カスタムルールシ グネチャの詳細を説明します。
OR 条件		カスタム署名に Or 条件 値を指定します。
AND 条件	- クジョン・L3 & L4 ヘッダー イ ンスペクション	以下を構成して、カスタム署名の And Condition を追 加します。
		 And 条件 - カスタム署名の And 条件値を指定します。
		 Operator – カスタム署名がヘッダーの内容と一 致するために真でなければならない条件のタイプ を定義します。Greater Than、Less Than、Equal To、Range、または Event 演算子から選択します。

ゾーン保護プロ ファイル設定:L 3 および L4 ヘッ ダー検査	設定場所	詳説
		 Context - 使用可能なコンテキスト オプションから 選択します。
		選択内容によっては、条件を有効にするために指定 する必要があるコンテキストや演算子に関連する他 のフィールドがある場合があります。
		追加条件は、Or Condition の下に第2レ ベルのエントリとして追加されます。

Network (ネットワーク) > Network Profiles (ネットワークプ ロファイル) > QoS

QoS プロファイルを Add (追加) して、最大 8 個のサービスクラスの帯域幅制限および優先順 位を定義します。保証帯域幅制限と最大帯域幅制限は、個別のクラスにも、ひとまとめのクラス にも設定することができます。優先順位によって、競合がある場合のトラフィックの処理方法が 決まります。

ファイアウォールで QoS を完全に提供できるようにするには、以下の手順も必要です。

- □ QoS 処理を受信するトラフィックを定義します(Policies(ポリシー) > QoS を選択して、QoS ポリシーを追加または変更します)。
- □ インターフェイス上で QoS を有効にします(Network(ネットワーク) > QoS を選択しま す)。

QoSの詳細なワークフロー、コンセプト、使用例については、「Quality of Service(サービス品 質) ^{II}」を参照してください。

QoS プロファイル設定	
プロファイル名	プロファイルの識別に使用する名前を入力します (最大 31 文字)。 名前の大文字と小文字は区別されます。また、一意の名前にする必 要があります。文字、数字、スペース、ハイフン、およびアンダー スコアのみを使用してください。
最大保証帯域 出力側	このインターフェイスを介してファイアウォールから出力される トラフィックの最大スループット(Mbps)を入力します。値は デフォルトで 0 で、ファイアウォール制限(PAN-OS 7.1.16以降 のリリースでは 60,000 Mbps、PAN-OS 7.1.15 以前のリリースで は16,000)を指定します。

QoS プロファイル設定	
	QoS プロファイルの Egress Max(最低保証帯域 出力側)は、QoS が有効になっている物理インターフェイスに定義された Egress Max(最低保証帯域 出力側)の値以下でなければなりません。 「Network(ネットワーク) > QoS」を参照してください。
	Egress Max(最大保証帯域出力側)は必須フィールドではありませんが、QoSプロファイルのこの値は常に定義しておくことをお勧めします。
最低保証帯域 出力側	このプロファイルで保証する帯域幅 (Mbps) を入力します。出力 側の最大保証帯域を超過した場合、ファイアウォールはベストエ フォート制でトラフィックを通過させます。
	Egress Guaranteed および Egress Max の値を Mbps またはパーセン テージで設定できます。これらの値をパーセンテージで設定する場 合は、次の考慮事項を考慮する必要があります。
	 クラスあたりの Egress Guaranteed (%) は、Egress Guaranteed 値ではなく、Egress Max 値を使用して計算されます。
	 プロファイル Egress Guaranteed は、クラスあたりの Egress Guaranteed (%) の合計に Egress Max を掛けた値に等しくなりま す。
	以下に例を示します。 Egress Max は 100 Mbps として設定されて います。クラス 1 に設定された保証パーセンテージは 30%、クラ ス 2 の場合は 20%、クラス 3 の場合は 5%、クラス 4 に設定され た保証率は 1% です。この構成により、合計パーセンテージは 56% として保証されます。この場合、プロファイル Egress Guaranteed は 56Mbps (56% x 出力最大) です。これは、クラス 1 Egreress Guaranteed が 30Mbps、Class 2 Egress Guaranteed が 20Mbps で あることも意味します。
クラス	Add をクリックし、個々の QoS クラスの処理方法を指定します。 構成するクラスを1つ以上選択できます。
	 Class – クラスを構成しない場合でも、QoS ポリシーに含めることができます。その場合、トラフィックは QoS 全体に対する制限の対象になります。QoS ポリシーに一致しないトラフィックは、クラス4に割り当てられます。
	• Priority - クリックして選択し、クラスに割り当てます。
	• real-time
	• hígh
	• meaium
	• IOW

QoS プロファイル設定	
	競合が発生すると、低い優先度が割り当てられているトラフィック は削除されます。リアルタイム優先度は、独自の個別のキューを使 用します。
	 Egress Max - クリックして、このクラスの最大スループット (Mbps 単位) を入力します。値はデフォルトで0で、ファイ アウォール制限(PAN-OS 7.1.16 以降のリリースでは 60,000 Mbps、PAN-OS 7.1.15 以前のリリースでは16,000)を指定しま す。QoS クラスの Egress Max は、QoS プロファイルの Egress Max 以下である必要があります。
	これは必須フィールドではありませんが、QoS プロ ファイルの Egress Max 値を常に定義することをお勧 めします。
	• Egress Guaranteed – このクラスの保証帯域幅 (Mbps) をクリッ クして入力します。あるクラスに対し割り当てられた保証帯 域は、そのクラスのために確保されているわけではなく、未 使用の帯域はすべてのクラスで使用可能な状態になっていま す。ただし、トラフィック クラスの出力保証帯域幅を超える と、firewall はそのトラフィックをベストエフォート方式で通過 します。

Network > Network Profiles > LLDP Profile [ネットワーク > ネットワーク プロファイル > LLDP プロファイル]

リンクレイヤー検出プロトコル (LLDP) プロファイルでは、ファイアウォールの LLDP モードの設定、Syslog および SNMP 通知の有効化、および LLDP ピアに送信するオプションの TLV (Type-Length-Values)の設定を行えます。LLDP プロファイルを設定した後、そのプロファイルを1つ以上のインターフェイスに割り当てます。

LLDP の設定および監視の方法などについて詳しくは、LLDP をご確認ください。

LLDP プロファイル設 定	の意味
氏名	LLDP プロファイルの名前を指定します。
モード	LLDPの動作モードを選択してください。transmit-receive[送受 信]、transmit-only[送信のみ]、またはreceive-only[受信のみ]。
SNMP Syslog 通知	SNMP トラップと Syslog 通知を有効にします。これは、グローバ ルNotification Interval[通知間隔]で実行されます。有効にした場合、 ファイアウォールは、Device(デバイス) > Log Settings(ログ設

LLDP プロファイル設 定	の意味
	定) > System(システム) > SNMP Trap Profile(SNMP トラップ プ ロファイル)および Syslog Profile(Syslog プロファイル)の設定に 従って、SNMP トラップと Syslog イベントの両方を送信します。
ポートの説明	ファイアウォールの ifAlias オブジェクトをPort Description [ポートの 説明] の TLV で送信できるようにします。
システム名	ファイアウォールの sysName オブジェクトをSystem Name [システム 名] の TLV で送信できるようにします。
システムの説明	ファイアウォールの sysDescr オブジェクトをSystem Description [シス テムの説明] の TLV で送信できるようにします。
システムの機能	インターフェイスのデプロイメント モード (L3、L2、またはバーチャ ル ワイヤー) を以下のマッピングによりSystem Capabilities [システム の機能] の TLV で送信できるようにします。
	• L3 の場合、ファイアウォールは、ルーター (ビット 6)の機能と他の ビット (ビット 1) を通知します。
	 L2 の場合、ファイアウォールは、MAC ブリッジ (ビット 3) の機能 と他のビット (ビット 1) を通知します。
	 バーチャル ワイヤーの場合、ファイアウォールは、リピーター (ビット 2)の機能と他のビット (ビット 1) を通知します。
	SNMP MIB により、インターフェイスで設定された複数の機能が単一 エントリに結合されます。
管理アドレス	Management Address[管理アドレス]を[管理アドレス]のTLVで送信 できるようにします。管理アドレスは4つまで入力でき、指定した 順に送信されます。順序を変更する場合は、Move Up[上へ]または Move Down[下へ]をクリックします。
氏名	管理アドレスの名前を指定します。
インターフェイス	IP アドレスが管理アドレスになるインターフェイスを選択しま す。None[なし] を指定した場合は、IPv4またはIPv6を選択する場所の 隣のフィールドにIPアドレスを入力できます。
IP の選択肢	IPv4 または IPv6 を選択した後、管理アドレスとして送信する IP アドレスを隣のフィールドで選択または入力します。Management Address[管理アドレス] の TLV が有効の場合は、1 つ以上の管理アド レスが必要です。管理 IP アドレスを設定しない場合は、送信する管理 アドレスとして送信インターフェイスの MAC アドレスが使用されま す。

双方向フォワーディング検知(BFD)は、リンク障害の極めて素早い検知を可能にし、さらに別 ルートへのフェイルオーバーを早めます。

確認すべき情報	以下を参照
BFDについて	BFD の概要
BFDプロファイルの作成時に入力できる フィールドについて	BFD プロファイルの構成要素
仮想ルーターの BFD ステータスを参照 する。	BFD のサマリーと詳細を表示
その他の情報をお探しですか?	詳細については、BFDと構成してください。 次の目的で BFD を設定する。 静的ルート BGP OSPF OSPFv3IPv6 RIP

BFDの概要

BFDとは、インターフェイス、データリンク、または実際の転送エンジンを含む、2つの転送 エンジンの間の双方向パスにおいて発生した障害を検出するプロトコルです。PAN-OS導入環 境下では、以下のうち1つのエンジンがファイアウォールのインターフェイスとなり、他方が 隣接して設定されたBFDピアとなります。2つのエンジンの間のBFD障害検知は極めて速いた め、Helloパケットやハートビートを用いてリンクモニタリングや、頻繁にダイナミックルー ティングのヘルスチェックを行った場合よりも素早いフェイルオーバーが可能になります。

BFDが障害を検出した場合、ルーティングプロトコルに対し、ピアに向かうパスを代わりのものに切り替えるよう通知します。BFDがスタティックルート用に設定されている場合、ファイアウォールはRIBおよびFIBのテーブルから障害の発生したルートを除外します。

BFDをサポートしているインターフェイスタイプには、物理イーサネット、AE、VLAN、トン ネル(サイト間VPNおよびLSVPN)、およびレイヤー3インターフェイスのサブインターフェイ スがあります。それぞれのスタティックルートあるいはダイナミックルーティングプロトコル について、BFDの有効化または無効化し、デフォルトBFDプロファイルを選択するか、あるい はBFDプロファイルを設定することができます。

BFD プロファイルの構成要素

Network > Network Profiles > BFD Profile [ネットワーク > ネットワークプロファイル > BFDプロファイル]

デフォルトのBFDプロファイルあるいは作成したBFDプロファイルを適用することで、スタ ティックルートやダイナミックルーティングプロトコルでBFDを有効化することができます。デ フォルトプロファイルではデフォルトのBFD設定を使用しており、これを変更することはできま せん。BFDプロファイルを新しくAdd[追加]し、以下の項目を指定することも可能です。

BFD プロファイ ル設定	の意味
氏名	BFDプロファイルの名前を入力します(最大31文字)。名前の大文字と小文 字は区別されます。また、ファイアウォール上で重複していない名前にす る必要があります。文字、数字、スペース、ハイフン、およびアンダース コアのみを使用してください。
モード	 BFDの動作モード: Active[アクティブ] - BFDがコントロールパケットの送信を開始します (デフォルト)。最低でも1つのBFDピアがアクティブに設定されてい る必要があります。両方がアクティブでも構いません。 Passive[パッシブ] - BFDはピアからコントロールパケットが送られてく るまで待機し、要求に応じて応答を行います。
希望する最 低Tx間隔(ミ リ秒)	 BFDプロトコルにBFDコントロールパケットを送信させたい間隔の最低値です(ミリ秒単位)。PA-7000シリーズ、PA-5450、PA-5430、PA-5420、PA-5410、および PA-3400シリーズの最小値は 50 です。PA-3200シリーズの最小値は100です。PA-400の最小値は150です。VM シリーズの最小値は 200 です(最大値は 10,000、既定値は 1000)。 1つのインターフェイスにおいて複数のプロトコルで異なるBFDプロファイルを使用している場合、BFDプロファイルにはすべて同じDesired Minimum Tx Interval[希望する最低Tx間隔]を設定してください。
最低Rx間隔要 件(ミリ秒)	BFDがBFDコントロールパケットを受信できる間隔の最低値です(ミリ秒 単位)。PA-7000 シリーズ、PA-5450、PA-5430、PA-5420、PA-5410、 および PA-3400 シリーズの最小値は 50 です。PA-3200シリーズの最小値 は100です。PA-400の最小値は150です。VM シリーズの最小値は 200 で す(最大値は 10,000、既定値は 1000)。
検知時間乗数値	ローカルシステムはリモートシステムから受信したDetection Time Multiplier (検知時間乗数)を同意済みのリモートシステムの送信間隔 (Required Minimum Rx Interval (最低 Rx 間隔要件)および最後に受信し

BFD プロファイ ル設定	の意味
	たDesired Minimum Tx Interval (目標の最低 Tx 間隔)のうち、いずれか大 きい方)で掛けることで検知時間を算出します。検知時間が過ぎるまでに BFD がピアからの BFD コントロールパケットを受信しない場合、障害が発 生していることを意味します(範囲は 2~50、デフォルトは 3)。
ホールドタイム (ミリ秒単位)	リンクが確立されてからファイアウォールがBFDコントロールパケットを 送信するまでに待機する時間です(ミリ秒単位)。Hold Time[待機時間] はBFDアクティブモードのみに適用されます。ファイアウォールが Hold Time(ホールドタイム)内に BFD コントロール パケットを受信した場 合、それを無視します(範囲は0~120000、デフォルトは 0)。デフォ ルトで設定されている0とは、送信Hold Time[待機時間]を使用しないとい うことです。リンクが確立すると、ファイアウォールは直ちにBFDコント ロールパケットの送受信を行います。
マルチホップの 有効化	マルチホップでBFDを有効化します。BGP導入環境にのみ適用されます。
最低Rx TTL值	マルチホップBFDがサポートされている場合に、BFDが受信する最低Time- to-Live値(ホップ数)です。BGP導入環境にのみ適用されます(範囲 は1~254、デフォルトなし)。

BFD のサマリーと詳細を表示

• Network > Virtual Routers [ネットワーク > 仮想ルーター]

以下の表で、BFD サマリー情報について説明します。

BFD情報の表示	
BFDサマリーの表示	Network > Virtual Routers[ネットワーク > 仮 想ルーター] を開き、詳細を確認したい仮想ルー ターの行で More Runtime Stats[ランタイム状 態の詳細] をクリックします。BFD Summary Information[BFDサマリー情報]のタブを選択しま す。
BFDの詳細の表示	BFD Details を表示するには、目的のインターフェ イスの行で details を選択します。

SD-WAN インターフェイス プロファイルを作成して、リンク タグによって物理リンクをグループ化し、リンクの速度とファイアウォールがそれらのリンクを監視する頻度を制御します。

	SD-WAN インターフェイス プロファイル
氏名	SD-WAN インターフェイス プロファイル名を最大 31 文字の英数字を使用して入力します。名前は英数字で始まる必要があり、文字、数字、アンダースコア (_)、ハイフン (-)、ピリオド (.)、スペースを使用できます。
場所	マルチ vsys デバイスの仮想システムを選択します。
Link Tag (リンク タグ)	このプロファイルがインターフェイスに割り当てる Link Tag (リンク タ グ) を選択するか、新しいタグを追加します。リンク タグは、パスの選択 およびフェイルオーバー中にファイアウォールが選択する物理リンク (異 なる ISP) を束ねます。
の意味	プロファイルのわかりやすい説明を入力することがベストプラクティス です。
リンク タイプ	 事前定義済みリストから物理 Link Type (リンクのタイプ)を 選択します。(リンクタイプには、ADSL/DSL、Cable modem (ケーブルモデム)、Ethernet(イーサネット)、Fiber (ファイ バ)、LTE/3G/4G/5G、MPLS、Microwave/Radio (マイクロ波 / ラジ オ波)、Satellite (衛星)、WiFi、Private Link1、Private Link2、Private Link3、Private Link4 もしくは その他).が提供されています)。PAN- OS 11.1.3では、SD-WANプラグイン3.2.1以降のリリースで、追加 のポイントツーポイントのプライベートリンクタイプであるPrivate Link1、Private Link2、Private Link3、Private Link4がサポートされてい ます。 ファイアウォールは、終端し、イーサネット接続としてファイアウォー ルに引き渡すすべての CPE デバイスをサポートすることが可能です。例 えば、WiFi アクセスポイント、LTE モデム、レーザーマイクロ波 CPE はすべて、イーサネット ハンドオフで終端可能です。

	SD-WAN インターフェイス プロファイル	
	PAN-OS SD-WAN をサポートするために使用されるイン ターフェイスにゾーンが定義されている既存の PAN-OS 展開の場合、Panorama は、次の条件下でインターフェイスの ゾーン名を事前定義された SD-WAN ゾーンの1つに自動的 に構成する場合があります。	
	1。SD-WANインターフェイスは、インターフェイスプ ロファイルでポイントツーポイントのプライベートリ ンクタイプ(MPLS、Satellite、Private Link1、Private Link2、Private Link3、Private Link4、またはMicrowave)と して設定されます。	
	 2.VPN Data Tunnel Support チェックボックスは、SD-WAN インターフェイスプロファイルで無効(オフ)になっていま す。これにより、SD-WAN VPN トンネルの外部にクリアテ キストでトラフィックを転送するように PAN-OS に指示し ます。Private Link1、Private Link2、Private Link3、および Private Link4 のリンクタイプは、SD-WAN ブランチファイ アウォールから SD-WAN ハブファイアウォールへの平文 トラフィックをサポートしていないため、これらのプライ ベートリンクタイプを設定する場合は、VPN データトンネ ルサポートオプションを有効にしておく必要があります。 Hub firewall では、条件 #1 が満たされると、ゾーン名は "zone-to-branch" として構成されます。ブランチ firewall では、条件 #1 と条件 #2 の両方が満たされると、ゾーン 名は "zone-to-hub" として構成されます。Panoramaはこ のステップを自動化して構成を簡素化し、ハブとブランチ 	
	のfirewall間の適切な通信を確保します。古いゾーン名を参 照する既存の firewall ポリシーがある場合は、新しい事前定 義された SD-WAN ゾーン名を反映するようにポリシーを更 新する必要があります。	
Maximum Download (最大 ダウンロード) (Mbps)	ISP からの最大ダウンロード速度をMbpsで指定します (1 ~100,000 の範囲、デフォルト値はなし)。ISP にリンク速度を問い合わせる か、speedtest.net 等のツールを使用してリンクの最大速度をサンプリン グし、十分に時間をかけて最大値の平均を取ります。	
Maximum Upload (最大アップロー ド) (Mbps)	ISP からの最大アップロード速度をMbpsで指定します (1 ~100,000 の範囲、デフォルト値はなし)。ISP にリンク速度を問い合わせる	

	SD-WAN インターフェイス プロファイル
	か、speedtest.net 等のツールを使用してリンクの最大速度をサンプリン グし、十分に時間をかけて最大値の平均を取ります。
エラー修正プロ ファイル イン ターフェイスの 選択対象	この(プロファイルを適用する)設定を選択すると、インターフェー スがエンコーディングファイアウォールの対象となり、Forward Error Correction(FEC、転送エラーの修正)またはパケット複製の対象として 選択されます。この設定の選択を解除し、プロファイルを適用するコス ト高のリンク(インターフェース)でコスト高の FEC またはパケットの 複製が使用されない設定にすることができます。プロファイルで指定さ れたLink Type(リンクタイプ)が、デフォルト設定のEligible for Error Correction Profile interface selection(エラー修正プロファイル インター フェースの選択対象)が選択されるかどうかを決定します。
VPN Data Tunnel	Profile(エラー修正フロファイル)を作成します。 ブランチからハブへのトラフィックとリターントラフィックが、セキュ
データ トンネル サポート)	リティを強化するために VPN トンネルを通過するか (テノオルトで有効)、暗号化のオーバーヘッドを回避するために VPN トンネルの外部を通過するかを決定します。
	 直接インターネット接続またはケーブルモデム、ADSL、その他のイン ターネット接続などのインターネット ブレイクアウト機能を備えたパ ブリック リンク タイプでは、VPN Data Tunnel Support (VPN データ トンネル サポート)を有効のままにします。
	 Private Linkタイプ(MPLS、サテライト、マイクロ波など) で、Private Linkタイプ(Private Link1、Private Link2、Private Link3、Private Link4 以外はインターネットブレークアウト機能な し)の VPN データトンネルサポートを無効にできます。ただし、 この場合、トラフィックが VPNトンネル外に送信されるため、トラ フィック傍受をされないようにする必要があります。
	 (SD-WAN Plugin 3.2.1以降のリリース) Private Link1、Private Link2、Private Link3、Private Link4のリンクタイプは、SD-WANブラ ンチファイアウォールからSD-WANハブファイアウォールへのプレー ンテキストトラフィックをサポートしていないため、これらのPrivate Linkタイプを設定するときは、VPNデータトンネルサポートを有効に したままにする必要があります。
	 多くのブランチには、ハブに接続しているプライベート MPLS リン クにフェイルオーバーし、ハブからインターネットに到達する必要が ある DIA トラフィックがあります。VPN Data Tunnel Support (VPN データトンネルサポート)の設定は、プライベート データが VPN ト ンネルを通過するか、あるいはトンネル外を通過するかを決定し、 フェイルオーバートラフィックはその他の接続を使用します(プライ ベートデータフローは使用しません)。ファイアウォールはゾーンを

	SD-WAN インターフェイス プロファイル
	使用して、プライベート MPLS トラフィックからの DIA フェイルオー バー トラフィックをセグメント化します。
VPN Failover Metric (VPN フェ イルオーバー メ トリック)	(PAN-OS 10.0.3 以降のリリース)DIA AnyPath を設定する場合、DIA が フェールオーバーするハブ仮想インターフェイスまたはブランチ仮想イ ンターフェイスにバンドルされている個々の VPN トンネルのフェール オーバー順序を指定する方法が必要です。VPN トンネルのVPN Failover Metric (VPN フェイルオーバーメトリック)を指定します(リンク)。 範囲は 1~65,535、デフォルトは 10 です。メトリック値が低いほど、 フェイルオーバー中に選択されるトンネル(このプロファイルを適用す るリンク)の優先度は高くなります。
	例えば、メトリックを低い値に設定して、プロファイルをブロードバ ンド インターフェースに適用します。次に、ブロードバンドがフェイ ルオーバーした後にのみ使用されるように、高コストの LTE インター フェースに適用させる高メトリック設定の別のプロファイルを作成しま す。
	ハブにリンクが1つしかない場合、そのリンクはすべての 仮想インターフェイスとDIAトラフィックをサポートし ます。特定の順序でリンクの種類を使用する場合は、トラ フィック配信プロファイルを[Top Down Priority (上位の優 先度)]を指定するハブに適用し、[リンクタグ]に優先順序 を指定する必要があります。(代わりにベストパスを指定 するトラフィック分布プロファイルを適用すると、ファイ アウォールはコストに関係なくリンクを使用して、ブラン チへの最適なパスを選択します。要約すると、トラフィッ ク配布プロファイルのリンクタグ、ハブ仮想インターフェ イス に適用されるリンクタグ、および VPN フェールオー バーメトリックは、トラフィック分散プロファイルがの 上位ダウンプライオリティを指定した場合にのみ機能しま す。
パス モニタリン グ	この SD-WAN インターフェイス プロファイルを適用するインターフェ イスをファイアウォールが監視するパス モニタリング モードを選択しま す。 • Aggressive (アグレッシブ)–(LTE および衛星を除くすべてのリンク タ イプのデフォルト) ファイアウォールは一定の頻度でプローブ パケッ トを SD-WAN リンクの反対側に送信します。
	ブラウンアウトおよびブラックアウト条件の高速検出と フェールオーバーが必要な場合は、Aagressiveモードを 使用してください。

	SD-WAN インターフェイス プロファイル	
	 Relaxed (リラックスド)–(LTE および衛星のリンクタイプのデフォルト) ファイアウォールのプローブ パケットセットを送信する間隔が数秒空くため、(Probe Idle Time (プローブ アイドル時間)) パス モニタリングの頻度が低下します。Probe Idle Time (プローブ アイドル時間) が経過すると、ファイアウォールは設定された Probe Frequency (プローブ頻度) で7秒間プローブを送信します。 	
	Relaxed モードは、低帯域幅のリンクがある場合、使用 量によって課金されるリンク (LTE など)、または高速検 出がコストと帯域幅の保持ほど重要でない場合は、使用 してください。	
Probe Frequency (プローブ頻度) (秒間)	ファイアウォールがプローブ パケットを SD-WAN リンクの反対側の端 に送信する 1 秒あたりの回数であるプローブ頻度を入力します(範囲は 1 ~5、デフォルトは 5)。	
Probe Idle Time (プローブ アイド ル時間) (秒)	Relaxed (リラックスド) パス モニタリングを選択した場合、ファイア ウォールがプローブ パケットのセット間で待機する時間である Probe Idle Time (プローブ アイドル時間) (秒) を設定することができます (範囲は 1~60、デフォルトは 60)。	
Failback Hold Time (フェール バック 保持時間) (秒)	ファイアウォールが回復したリンクが確立されたままになるのをファイ アウォールが待機する時間(秒単位)を入力します。この時間が経過す ると、ファイアウォールはフェイルオーバー後にそのリンクを優先リン クとして復元します (20 ~ 120 の範囲、デフォルトは 120)。フェール バック 保持時間は、優先リンクとして回復したリンクの復帰が早過ぎ、 すぐに再度失敗することを防ぎます。	

ネットワーク>ネットワークプロファイル>MACsecプロファイル

[今後使用するために予約済み]



デバイス

ファイアウォールの基本的なシステム設定と管理タスクのフィールドリファレンスは、以下の セクションを参照してください。

- Device (デバイス) > Setup (セットアップ)
- Device > High Availability [デバイス > 高可用性]
- Device (デバイス) > Log Forwarding Card (ログ転送カード)
- Device > Config Audit [デバイス > 設定監査]
- [Device] > [パスワード プロファイル]
- Device > Administrators [デバイス > 管理者]
- Device > Admin Roles [デバイス > 管理者ロール]
- Device > Access Domain [デバイス > アクセスドメイン]
- Device > Authentication Profile [デバイス > 認証プロファイル]
- Device > Authentication Sequence [デバイス > 認証シーケンス]
- [Device] > [ユーザー ID]
- Device (デバイス) > IoT Security (IoTセキュリティ) > DHCP Server Log Ingestion (DHCPサー バーのログ取り込み)
- Device > Data Redistribution [デバイス > データの再配信]
- Device > Device Quarantine [デバイス > デバイス隔離]
- Device > VM Information Sources [デバイス > VM 情報の送信元]
- Device (デバイス) > Troubleshooting (トラブルシューティング)
- Device > Virtual Systems [デバイス > 仮想システム]
- Device > Shared Gateways [デバイス > 共有ゲートウェイ]
- Device (デバイス) > Certificate Management (証明書の管理)
- Device > Response Pages [デバイス > 応答ページ]
- Device > Log Settings [デバイス > ログ設定]
- [Device] > [サーバー プロファイル]
- Device > Local User Database > Users [デバイス > ローカル ユーザー データベース > ユー ザー]
- Device > Local User Database > User Groups [デバイス > ローカル ユーザー データベース > ユーザー グループ]
- Device > Scheduled Log Export [デバイス > スケジュール設定されたログのエクスポート]
- Device > Software [デバイス > ソフトウェア]
- Device > GlobalProtect Client [デバイス > GlobalProtect クライアント]

- Device > Dynamic Updates [デバイス > 動的更新]
- Device > Licenses [デバイス > ライセンス]
- Device > Support [デバイス > サポート]
- Device > Master Key and Diagnostics [デバイス > マスター キーおよび診断]
- IoT >デバイス>ポリシーの推奨事項
- デバイス > ポリシーの推奨事項 > SaaS
- デバイス>ポリシー推奨>IoTまたはSaaS>ポリシールールのインポート

Device (デバイス) > Setup (セットアップ)

- Device > Setup > Management [デバイス > セットアップ > 管理]
- Device > Setup > Operations [デバイス > セットアップ > 操作]
- Device > Setup > HSM [デバイス > セットアップ > HSM]
- Device > Setup > Services [デバイス > セットアップ > サービス]
- Device $(\vec{r} \land \vec{r} , \vec{r}$
- Device $(\vec{\tau} \vee \vec{T} \wedge \vec{T})$ > Setup $(t \vee \nabla \vec{T})$ > Telemetry $(\tau \vee \nabla \vec{T})$
- Device > Setup > Content-ID [デバイス > セットアップ > Content-ID]
- Device > Setup > WildFire [デバイス > セットアップ > WildFire]
- Device > Setup > Session [デバイス > セットアップ > セッション]
- Device (デバイス) > Setup (セットアップ) > DLP

Device > Setup > Management [デバイス > セットアップ > 管理]

- デバイス>セットアップ>管理
- Panorama > セットアップ > 管理

管理設定を行うには、ファイアウォールで Device(デバイス) > Setup(セットアップ) > Management(管理)を選択します。

Panorama テンプレートを使用して管理するファイアウォールを設定するには、Panorama[™] で Device(デバイス) > Setup(セットアップ) > Management(管理)を選択しま す。Panorama の管理設定を行うには、Panorama > Setup(セットアップ) > Management(管 理)を選択します。

以下の管理設定は、記載されていない限り、ファイアウォールと Panorama の両方に適用されます。

- 一般設定
- 認証設定
- ポリシー ルールベース設定
- Panorama設定Device(デバイス) > Setup(セットアップ) > Management(管理)(Panorama に接続するためにファイアウォールで指定する設定)
- Panorama設定Panorama > Setup (セットアップ) > Management (管理) (ファイアウォー ルに接続するために Panorama で指定する設定)
- ロギングおよびレポート設定
- ログインタフェース(PA-5450のみ)
- バナーとメッセージ
- パスワード複雑性設定
- AutoFocus[™]
- Cortex Data Lake
- SSH Management Profiles Settings (SSH 管理プロファイルの設定)
- PAN-OS エッジ サービスの設定

項目	の意味
一般設定	
ホスト名	ホスト名を入力します(最大 31 文字)。名前は大文字と 小文字が区別され、一意である必要があり、文字、数字、 ピリオド、ハイフン、およびアンダースコアのみを含める ことができます。

項目	の意味
	 値を入力しない場合、PAN-OS[®]はファイアウォールモデル(PA-5220_2等)をデフォルトとして使用します。 必要に応じて、DHCPサーバーが提供するホスト名を使用するようにファイアウォールを設定することもできます。 「DHCPサーバーが提供するホスト名を使用する(ファイアウォールのみ)」を参照してください。 一意のホスト名を設定し、管理するデバイスを識別しやすくします。
ドメイン	ファイアウォールのネットワーク ドメイン名を入力します (最大 31 文字)。 必要に応じて、DHCP サーバーが提供するドメインを使用 するようファイアウォールと Panorama を設定することも できます。「DHCP サーバーが提供するドメインを使用す る(ファイアウォールのみ)」を参照してください。
DHCP サーバーが提供するホ スト名を使用する(ファイア ウォールのみ)	(管理インターフェイスの IP タイプが DHCP Client (DHCP クライアント)の場合のみ適用されます) 管理インターフェイスに DHCP サーバーから受信したドメ イン (DNS サフィックス)を使用させる場合はこのオプ ションを選択します。Hostname(ホスト名)フィールド に指定されている値は、サーバーからのホスト名(有効な 場合)で上書きされます。
DHCP サーバーが提供するド メインを使用する(ファイア ウォールのみ)	(管理インターフェイスの IP タイプが DHCP Client (DHCP クライアント)の場合のみ適用されます) 管理インターフェイスに DHCP サーバーから受信したドメ イン (DNS サフィックス)を使用させる場合はこのオプ ションを選択します。Domain (ドメイン)フィールドに 指定されている値は、サーバーからのドメインで上書きさ れます。
ログイン バナー	WebインターフェイスのログインページのName [ユーザー 名] およびPassword [パスワード] のフィールドの下に表示 するテキスト(最大3,200文字)を入力します。
管理者にログインバナーの承認 を強制する	ログインページのログインバナーの上にI Accept and Acknowledge the Statement Below(以下の内容を受諾し 同意します)との一文を表示し、管理者に選択させる場 合、このオプションを選択します。管理者はこのメッセー ジの内容を理解し、受諾しない限りLogin(ログイン)で きません。

項目	の意味
SSL/TLS Service Profile	 既存の SSL/TLS サービス プロファイルを割り当てるか、新しいプロファイルを作成して、証明書と管理インターフェイスで許可される SSL/TLS プロトコル設定を指定します(De1vice > Certificate Management > SSL/TLS サービスプロファイルを参照)。firewall または Panorama は、この証明書を使用して、管理(MGT)インターフェイスまたはHTTP/HTTPS 管理トラフィックをサポートするその他のインターフェイスを介して Web インターフェイスにアクセスする管理者を認証します(Network > Network Profiles > Interface Mgmt を参照)。None (なし) (デフォルト)を選択した場合、ファイアウォールまたは Panorama は事前定義済みの証明書を使用します。
タイム ゾーン	ファイアウォールのタイム ゾーンを選択します。
表示言語	ドロップダウンリストから、PDF レポートの言語を選択し ます。「Monitor (監視) > PDF Reports (PDF レポート) > Manage PDF Summary (PDF サマリーの管理)」を参照 してください。 Webインターフェイスに特定の言語設定が設定されている 場合でも、PDFレポートにはこのLocale [表示言語] の設定 で指定した言語が使用されます。
日付	 ファイアウォールの日付を設定します。現在の日付 (YYYY/MM/DD 形式)を入力するか、ドロップダウンリストから日付を選択します。 ◎ NTP サーバー (Device (デバイス) > Setup (セットアップ) > Services (サービ ス))を定義することもできます。
時間	ファイアウォールの時刻を設定します。現在の時刻を 24 時間形式で入力するか、ドロップダウン リストから時刻を 選択します。

項目	の意味
	 NTP サーバー(Device(デバイス) > Setup(セットアップ) > Services(サービス))を定義することもできます。
シリアル番号 (Panorama バーチャル アプラ イアンスのみ)。	Panorama のシリアル番号を入力します。シリアル番号 は、Palo Alto Networks [®] から送信された受注処理電子 メールに記載されています。
緯度	ファイアウォールの緯度(-90.0から90.0)を入力します。
経度	ファイアウォールの経度(-180.0から180.0)を入力しま す。
コミットロックの自動実施	 候補設定を変更するときにコミットロックが自動的に適用 されるようにするには、このオプションを選択します。詳細は、「変更内容のロック」を参照してください。 Automatically Acquire Commit Lock (コミット ロックの自動実施)を有効化し、最初の管理 者が変更をコミットするまでの間、他の管理 者が設定を変更できないようにします。
証明書有効期限チェック	 デバイス内の証明書の有効期限が近づいた時に警告メッセージを作成するようにファイアウォールに指示します。 Certificate Expiration Check (証明書有効期限 チェック)を有効化し、デバイス内の証明書 の有効期限が近づいた時に警告メッセージを 作成します。
マルチ仮想システム機能	この機能をサポートするファイアウォールで複数の仮想 システムの使用を有効にします(「Device(デバイス) > Virtual Systems(仮想システム)」を参照)。

項目	の意味
	 ファイアウォールでマルチ仮想システムを有効化するには、640を超える異なるユーザーグループをファイアウォールポリシーで参照することはできません。必要に応じて、参照するユーザーグループの数を減らしてください。この後にマルチ仮想システムの有効化と追加を行うと、ポリシーは追加されたマルチ仮想システムごとに640個のユーザーグループを参照することができます。
URL フィルタリング データ ベース (Panorama のみ)	Panoramaで使用するURLフィルタリングベンダーを選択し ます。 brightcloud または paloaltonetworks (PAN-DB)か ら選択してください。
ハイパーバイザによって割り当 てられた MAC アドレスの使用 (VM-Series ファイアウォール のみ)	PAN-OS カスタム スキーマを使用して MAC アドレスを生成するのではなく、ハイパーバイザによって割り当てられた MAC アドレスを VM-Series ファイアウォールで使用するには、このオプションを選択します。
	このオプションを有効にして、インターフェイスに IPv6 アドレスを使用する場合、インターフェイス ID に EUI-64 形式は使用できません。EUI-64 形式では IPv6 アドレスが インターフェイスの MAC アドレスから導出されます。高 可用性(HA)アクティブ/パッシブ設定で EUI-64 形式が 使用されると、コミット エラーが発生します。
GTP セキュリティ	GPRS トンネリング プロトコル (GTP) トラフィック内の 制御プレーン メッセージとユーザー データプレーン メッ セージを検査する機能を有効にするには、このオプショ ンを選択します。GTP トラフィックに対してポリシーを 適用できるようにモバイル ネットワーク プロテクション を設定するには、「Objects(オブジェクト) > Security Profiles(セキュリティ プロファイル) > Mobile Network Protection(モバイル ネットワーク プロテクション)」を 参照してください。
SCTP セキュリティ	ストリーム制御伝送プロトコル(SCTP)パケットと チャンクの検査とフィルタリング、および SCTP 開始 (INIT)フラッド防御の適用を有効にするには、このオ プションを選択します。「Objects(オブジェクト) > Security Profiles(セキュリティ プロファイル) > SCTP Protection(SCTP プロテクション)」を参照してくだ さい。SCTP INIT フラッド防御については、「Configure

項目	の意味
	SCTP INIT Flood Protection(SCTP INIT フラッド防御の設 定)」を参照してください。
Advanced Routing(高度なルー ティング)	このオプションを選択すると、論理ルータ上のスタティッ ク・ルート、BGP、OSPFv2、OSPFv3、IPv4 マルチキャ スト、および RIPv2 をサポートする拡張ルーティング・エ ンジンが使用可能になります。新しいルーティングエンジ ンへの変更を有効化するには(あるいは従来のルートエン ジンに復元するには)、コミットしてファイアウォールを 再起動する必要があります。
IPアドレスの重複サポートを許 可	(PAN-OS 11.1.4 以降リリース) IP アドレス サポートを 有効にするには、このオプションを選択します。このオプ
(PA-1400 シリーズおよび VM シリーズのファイアウォールの み)	ションを使用すると、インターフェイスが異なる論理ルー タに属している場合に、複数のレイヤ3ファイアウォール インターフェイスで同じ IP アドレスを使用できます。ま た、次のいずれかの組み合わせも使用できます。
	 異なるゾーンで同じ仮想システム。
	• 同じゾーンで異なる仮想システム。
	• 異なるゾーンと異なる仮想システム。
	IPアドレスの重複サポートには、Advanced Routing Engineが必要です。拡張ルーティングを有効にします。 その後、重複するIPアドレスサポートを有効にできます。 重複するIPアドレスを設定する前に、標準の手順に従って ファイアウォールをコミットし、再起動します。重複す るIPアドレスを静的に設定したり、インターフェイスに動 的に割り当てることができます。すべてのレイヤ3イン ターフェイスタイプ(イーサネット、VLAN、トンネル、 ループバック、集約イーサネット(AE)、および AE サブ インターフェイス)は、重複した IP アドレスをサポートし ます。 管理インターフェイスは、IPアドレスの重複をサポートし ていません。
Tunnel Acceleration(トンネル 高速化)	GRE トンネル、VXLAN トンネル、GTP-U トンネルを通 過するトラフィックのパフォーマンスおよびスループット を向上するには、このオプションを選択します。このオプ ションはデフォルトで有効化されています。
	 GRE and VXLAN tunnel acceleration (GRE および VXLAN トンネル高速化) – PA-3200 シリーズファ イアウォールおよび PA-7000-NPC と SMC-B を備え

項目	の意味
	たPA-7000 シリーズのファイアウォールでサポートさ れています。
	 GTP-U tunnel acceleration (GTP-U トンネル高速化) – PA-7000-NPC および SMC-B を備えたPA-7000 シリー ズのファイアウォールでサポートされています。GTP- U トンネル トラフィックにトンネル高速化を設定する には、Tunnel Acceleration (トンネル高速化) を有効化 し、GTP を有効化し、GTP-U プロトコルのトンネル コ ンテンツ インスペクション (TCI) ポリシー ルールを使 用せずに設定し、モバイル ネットワーク プロテクショ ン プロファイルが添付されたセキュリティ ポリシー ルールは、GTP トラフィックを許可する必要がありま す。
	Tunnel Acceleration(トンネル高速化)を無 効化または再度有効化してコミットする場合 は、ファイアウォールを再起動する必要があ ります。

Device Certificate(デバイス証明書)

証明書の取得	クリックして、Palo Alto Networks カスタマー サポート ポータル (CSP)から生成された ワン タイム パスワード (OTP) を入力します。CSP で Panorama を正常に認証し、 ゼロタッチプロビジョニング (ZTP)、loT、デバイス テ レメトリ、エンタープライズ Data Loss Prevention (デー タ損失防止 - DLP)等のクラウドサービスを活用するには デバイス証明書が必要です。デバイス証明書を正常にイン ストールすると、以下のように表示されます。
	 Current Device Certificate Status (現在のデバイス証明 書のステータス)–デバイス証明書の現在のステータス (有効、無効、または 有効期限切れ)
	 Not Valid Before (以前は無効)ーデバイス証明書がいつ有効になるかを示すタイムスタンプ。
	• Not Valid After (以降は無効)-デバイス証明書の有効期 限が切れ、デバイス証明書が 無効 または 有効期限切 れになるときを示すタイムスタンプ。
	 Last Fetched Message (最後にフェッチされたメッセージ)-デバイス証明書が正常にインストールされた、またはデバイス証明書のインストールに失敗したことを示すメッセージ。

項目	の意味
	 Last Fetched Status (最後にフェッチしたステータ ス)-デバイス証明書のフェッチのステータス (成功 また は 失敗)。
	 Last Fetched Timestamp (最後にフェッチしたタイムス タンプ)
認証設定	
認証プロファイル	ファイアウォールでローカルに定義されたものではなく、 外部サーバーで定義された管理者アカウントを認証するた めにファイアウォールで使用する認証プロファイル(ま たはシーケンス)を選択します(「Device(デバイス) > Authentication Profile(認証プロファイル)」を参照)。 外部管理者がログインすると、ファイアウォールは認証お よび承認情報(管理ロールなど)を外部サーバーに要求し ます。
	外部管理者の認証を有効にするには、認証プロファイルで 指定されたサーバー タイプに基づいて追加の手順が必要で す。そのサーバー タイプは次のとおりです。
	• RADIUS
	• TACACS+
	• SAML
	 管理者は SAML を使用して Web インター フェイスとの認証を行うことができます が、CLI との認証を行うことはできません。
	外部管理者の認証を無効にするには、None(なし)を選 択します。
	ローカルで(ファイアウォールで)定義した管理者アカウ ントの場合、ファイアウォールは、そのアカウントに割り 当てられた認証プロファイルを使用して認証を行います (「Device(デバイス) > Administrators(管理者)」を 参照)。
証明書プロファイル	ファイアウォールの Web インターフェイスに証明書に基 づいてアクセスするよう設定された管理者のクライアン ト証明書を検証するための証明書プロファイルを選択し ます。証明書プロファイルの設定手順は、「Device(デ バイス) > Certificate Management(証明書の管理) > Certificate Profile(証明書プロファイル)」を参照してく ださい。

項目	の意味
	証明書プロファイルを設定し、証明書プロ ファイルで定義されているルート CA 証明書 を使って認証を行うために管理者のホストマ シンが適切な証明書を確実に持っている状態 にします。
アイドルタイムアウト	 Web インターフェイスまたは CLI 上でアクティビティがな い場合に管理者を自動的にログアウトするまでの最大時間 (分単位)を入力します(範囲は 0~1,440、デフォルト は 60)。値 0 は、アクティビティがなくても自動ログア ウトはトリガーされないことを意味します。 Web インターフェイスページ (Dashboard (ダッシュボード)、システ ムアラームダイアログなど)の手動更新 および自動更新で、Idle Timeout (アイド ルタイムアウト)カウンターがリセット されます。自動更新をサポートするペー ジを使用しているときにファイアウォー ルのタイムアウトを適用するには、更新間 隔を Manual (手動)に設定するか、更新 間隔をこの Idle Timeout (アイドルタイム アウト)よりも大きな値に設定してください。Auto Refresh(自動更新)はACC タブで 無効にすることもできます。 Idle Timeout (アイドルタイムアウト)を 10 分 に設定し、管理者がファイアウォールのセッ ションを開いたままにしている場合に未認証 のユーザーがファイアウォールにアクセスす るのを防ぎます。
API キーの有効期間	API キーの有効期間(分単位)を入力します(範囲は0~ 525,600、デフォルトは0)。値を0にすると、API キー が失効しなくなります。 以前に生成した API キーをすべて向こうにする場合 はExpire All API Keys (API キーをすべて失効)させます。既 存のキーがすべて使用できなくなり、それらの API キーを 使って行っている作業をすべて行えなくなるため、このオ プションは注意して使用してください。

項目	の意味
	API キーを参照している現在の実装の機能を 保ちながらキーを交換できるよう、保守期間 中にこの作業を行ってください。
API キーの前回の失効	API キーが最後に失効した時のタイムスタンプを表示します。キーをリセットしたことがない場合、このフィールドは値を持ちません。
最大試行回数	ファイアウォールが許容する、Web インターフェイスお よび CLI への最大ログイン試行回数(0~10)を入力し ます。この回数を超えると管理者アカウントがロックアウ トされます。値0を指定すると、無制限にログインを試行 できます。デフォルト値は、通常の運用モードのファイア ウォールでは0、FIPS-CC モードのファイアウォールでは 10です。ログイン試行回数を制限することで、ファイア ウォールを総当たり攻撃から保護できます。
	(Panorama managed firewall only) Panorama のテンプレートまたはテンプレートスタック構成から失敗した試行設定を管理する場合、サポートされる最小値は1です。
	 Failed Attempts[最大試行回数] を 0 以外の 値に設定しても、Lockout Time[ロックアウ ト時間] を 0 のままにしておくと、Failed Attempts[最大試行回数] は無視され、ユー ザーはロックアウトされません。
	Failed Attempts (試行失敗回数)の値を5以下 に設定し、入力ミスに備えてある程度猶予を 持たせつつ、悪意のあるシステムがブルート フォースによってファイアウォールにログイ ンしようとするのを防ぎます。
ロックアウト時間	Failed Attempts (最大試行回数)の制限に達した後、Web インターフェイスおよび CLI への管理者のアクセスをファ イアウォールがロックアウトする時間(分)を入力します (範囲は 0 ~ 60)。値を 0 (デフォルト)にすると、別の 管理者がアカウントのロックを手動で解除するまでロック アウトが適用されます。

項目	の意味
	 Failed Attempts (試行失敗回数)を 0 以外の値にしながら、Lockout Time (ロックアウト時間)を 0 のままにしている場合、設定された試行失敗回数に達した後、別の管理者が手動でアカウントをロック解除するまでの間、ユーザーがロックされます。
	Lockout Time (ロックアウト時間)を 30 分以上 に設定し、攻撃者が続けてログインを試みるのを防ぎます。
最大セッション数	 全ての管理者アカウントとユーザーアカウントに許可される同時セッション数を入力します(0~4の範囲)。 「0(デフォルト)」の値は、無制限の同時セッション数が許可されることを意味します。
最大セッション時間	アクティブで非アイドルの管理者が継続してログイン状態 を維持することが可能な分数を入力します(60~1,499の 範囲)。この最大セッション時間に達すると、セッション が終了します。新たなセッションを開始するには再認証が 必要になります。デフォルト値は0(30日)に設定されて います。手動で入力することはできません。なにも値が入 力されない場合、Max Session Time(最大セッション時 間)はデフォルトの0に設定されます。
	FIPS-CC モードでの範囲は 60~1,499、デ フォルト値は 720 です。なにも値が入力され ない場合、Max Session Time(最大セッショ ン時間)はデフォルトの 720 に設定されま す。

ポリシー ルールベース設定

ポリシーのタグが必須	新しいポリシールールを作成する際に1つ以上のタグを求めます。このオプションを有効化する際にすでにポリシールールが存在する場合、対象のルールを後で編集する際に 1つ以上のタグを追加する必要があります。
ポリシーの説明が必須	新しいポリシールールを作成する際に Description (説明) を 追加することを求めます。このオプションを有効化する際
項目	の意味
---	--
	にすでにポリシールールが存在する場合、対象のルールを 後で編集する際に Description (説明)を追加する必要があり ます。
ポリシーにタグあるいは説明が なければコミット失敗	ポリシールールにタグあるいは説明を追加していない場 合、強制的にコミットを失敗させます。このオプションを 有効化する際にすでにポリシールールが存在する場合、対 象のルールを後で編集する際にタグや説明を追加しなけれ ば、コミットが失敗します。 コミットを失敗させる場合、Require tag on policies (ポリ シーのタグが必須)あるいはRequire description on policies
	(ホリシーの説明が必須)を使用9 る必要がありま9。
ポリシーの監査コメントが必要	新しいポリシールールを作成する際にAudit Comment (監査コメント)を求めます。このオプションを有効化する際にすでにポリシールールが存在する場合、対象のルールを後で編集する際にAudit Comment (監査コメント)を追加する必要があります。
監査コメントの正規表現	監査コメントに必要なコメント書式パラメーターを指定し ます。
Wildcard Top Down Match Mode (フィアウォールのみ)	(PAN-OS 10.2.1 以降の 10.2 リリース)Wildcard Top Down M1atch Mode がイネーブルになっている場合、パケット がワイルドカードマスク付きの送信元または宛先 IP アド レスを使用する セキュリティ ポリシールールに一致し、 マスクがオーバーラップすると、ファイアウォール はマス キングに基づいてすべてのアドレスビットに完全に一致す る最初の一致ルールを (トップダウン順で) 選択します。デ フォルトは無効です。重複するワイルドカードマスクが一 致する場合、ファイアウォール はワイルドカードマスク内 で最も長く一致するプレフィックスを持つルールを選択し ます。
ポリシー ルール ヒット数	ファイアウォールで設定したポリシー ルールとトラフィッ クの一致頻度を追跡します。有効にすると、各ルールと 一致するトラフィックの合計 Hit Count (ヒット数) と、 ルールが Created (作成)、Modified (変更)、First Hit (最初 にヒット)、Last Hit (最後にヒット) した日時が表示されま す。
ポリシーアプリケーションの使 用状況	

項目

の意味

Panorama Settings(Panorama の設定):Device > Setup > Management [デバイス > セット アップ > 管理]

ファイアウォール、または Panorama のテンプレートに以下の設定を定義します。これらの 設定によって、ファイアウォールから Panorama への接続が確立されます。

Panorama の接続設定とオブジェクト共有設定も定義する必要があります。以下を参照して ください。(Panorama Settings (Panorama 設定) : Panorama > Setup (セットアップ) > Management (管理))。

ファイアウォールは Panorama と認証を行う際、AES256により暗号化された SSL 接続を使用します。デフォルトでは、Panorama とファイアウォールは、事前定義済みの 2,048 ビット証明書を使用して互いに認証を行い、SSL 接続を使用して設定管理とログ収集を行います。Panorama、ファイアウォール、ログコレクタ間の SSL 接続のセキュリティをさらに強化するには、「保護されたクライアント通信」を参照し、ファイアウォールと Panorama またはログコレクタ間のカスタム証明書を設定してください。

管理	firewall が Panorama によって管理されるか、 Cloud Service によって管理されるかを指定します。
(Manage By Panorama only)パノ ラマサーバー	PanoramaサーバーのIPアドレスまたはFQDNを入力して ください。Panoramaが高可用性(HA)設定に含まれてい る場合、2番目の Panorama Servers[Panorama サーバー] フィールドにセカンダリPanoramaサーバーのIPアドレスま たはFQDNを入力します。
認証キー (ファイアウォールのみ)	Panorama で生成された デバイス登録認証キー を入力します。
Panorama からデータを受信す る際のタイムアウト	Panorama から TCP メッセージを受信する際のタイムアウトを入力します(秒単位)(範囲は 1 ~ 240、デフォルトは 240)。
Panorama ヘデータを送信する 際のタイムアウト	Panorama に TCP メッセージを送信する際のタイムアウト (秒単位)を入力します(範囲は 1 ~ 240、デフォルトは 240)。
Panorama に SSL 送信を行う際 の再試行カウント	Panorama に Secure Socket Layer(SSL)メッセージを 送信する際の許容再試行回数を入力します(範囲は 1 ~ 64、デフォルトは 25)。
自動コミット復旧を有効にする	有効にすると、設定がコミットされてファイアウォールに プッシュされたときや、設定が正常にプッシュされた後

項目	の意味
	に、設定された間隔で、ファイアウォールが Panorama管 理サーバへの接続を自動的に検証することができます。
	この機能を有効にすると、ファイアウォールが Panorama管理サーバへの接続を確認できない場合、ファ イアウォールと Panorama 管理は自動的にその設定を以前 の実行中の設定に戻して接続を回復します。
Panorama 接続を確認するため の試行回数	自動コミット復旧を有効にすると、ファイアウォールが Panorama管理サーバへの接続をテストする回数を設定し ます。
再試行の間隔 (秒)	自動コミット回復を有効にすると、ファイアウォールが Panorama管理サーバへの接続をテストする試行回数の間 隔を秒単位で設定します。
保護されたクライアント通信	Secure Client Communication(保護されたクライアント 通信)を有効にすると、ファイアウォールは(デフォル ト証明書の代わりに)設定済みのカスタム証明書を使用し て、Panorama またはログ コレクタへの SSL 接続を認証し ます。
	 None(なし)(デフォルト) – デバイス証明書は設定 されず、デフォルトの事前定義済みの証明書が使用され ます。
	 Local (ローカル) – ファイアウォールは、ファイア ウォールで生成されたか既存のエンタープライズ PKI サーバーからインポートされたローカルのデバイス証明 書および対応する秘密鍵を使用します。
	 Certificate (証明書) – 生成またはインポートした ローカル デバイスの証明書を選択します。この証 明書を、(ファイアウォールのシリアル番号のハッ シュに基づく)ファイアウォール固有の証明書とし たり、Panorama に接続するすべてのファイアウォー ルで使用する共通のデバイス証明書としたりできま す。
	 Certificate Profile(証明書プロファイル) – ドロッ プダウンリストから証明書プロファイルを選択しま す。証明書プロファイルは、クライアント証明書を 検証するための CA 証明書と、証明書失効状態を確 認する方法を定義します。

項目	の意味
	 SCEP – ファイアウォールは、Simple Certificate Enrollment Protocol (SCEP) サーバーで生成されたデ バイス証明書と秘密鍵を使用します。
	 SCEP Profile (SCEP プロファイル) –ドロッ プダウンで Device (デバイス) > Certificate Management (証明書管理) > SCEP を選択しま す。SCEP プロファイルは、エンタープライズ PKI 内 の SCEP サーバーに対してクライアント デバイスを 認証するために必要な情報を Panorama に提供しま す。
	 Certificate Profile (証明書プロファイル) –ド ロップダウンで Device (デバイス) > Certificate Management (証明書管理) > Certificate Profile (証 明書プロファイル) を選択します。証明書プロファ イルは、クライアント証明書を検証するための CA 証明書と、証明書失効状態を確認する方法を定義し ます。
	 Customize Communication(カスタマイズ通信)-ファ イアウォールは、設定されたカスタム証明書を使用し て、選択したデバイスを認証します。
	 Panorama Communication (Panorama 通信) –ファ イアウォールは設定されたクライアント証明書を使 用して Panorama と通信します。
	 PAN-DB Communication (PAN-DB 通信) –ファイ アウォールは設定されたクライアント証明書を使用 して PAN-DB アプライアンスと通信します。
	 WildFire Communication (WildFire 通信)–ファイア ウォールは設定されたクライアント証明書を使用し て WildFire[®] アプライアンスと通信します。
	 Log Collector Communication (ログコレクタ通信) –ファイアウォールは設定されたクライアント証明書を使用してログコレクタと通信します。
	 Check Server Identity (サーバー アイデンティティ のチェック)–(Panorama と ログ コレクタ通信のみ) ファイアウォールは、共通名 (CN)をサーバーの IPア ドレスまたは FQDN と照合し、サーバーのアイデン ティティを確認します。
Panorama ポリシーとオブジェ クトを無効/有効にする	このオプションはファイアウォールのPanorama Settings [Panorama設定] を編集する場合にのみ表示されます (Panoramaのテンプレートにはありません)。

項目	の意味
	Disable Panorama Policy and Objects [Panorama ポリシー とオブジェクトを無効にする] を選択すると、ファイア ウォールに対するデバイスグループのポリシーとオブジェ クトの適用が無効になります。デフォルトでは、この操 作により、ファイアウォールから伝播されたポリシーと オブジェクトも削除されます。デバイスグループのポリ シーとオブジェクトのローカルコピーをファイアウォー ルで保管する場合は、このオプションをクリックしたとき に開くダイアログボックスのImport Panorama Policy and Objects before disabling [無効にする前に Panorama ポリ シーとオブジェクトをインポート]を選択します。コミッ トを実行すると、これらのポリシーとオブジェクトはファ イアウォール設定の一部となり、Panorama による管理の 対象外となります。
	マルチ vsys ファイアウォールの場合は、ま ずテンプレート構成をインポートしてから、 デバイス グループの設定をインポートし て、Panorama プッシュ構成を正常に無効に する必要があります。
	通常の操作状況下では、Panorama 管理を無効にすること は不要であるうえに、ファイアウォールのメンテナンスと 設定が複雑になりかねません。このオプションは通常、 ファイアウォールでデバイス グループの定義とは異なる ルールとオブジェクト値が必要な場合に適用されます。た とえば、テストのためにファイアウォールを本番環境から ラボ環境に移動する場合などです。
	ファイアウォールのポリシーおよびオブジェクト管理 を Panorama に戻すには、 Enable Panorama Policy and Objects [Panorama ポリシーとオブジェクトを有効にする] をクリックします。
デバイスとネットワーク テンプ レートを無効/有効にする	このオプションはファイアウォールの Panorama Settings [Panorama設定] を編集する場合にのみ表示されます (Panoramaのテンプレートにはありません)。
	ファイアウォールに対するテンプレート情報(デバイスと ネットワーク設定)の適用が無効化する場合は、Disable Device and Network Template [デバイスとネットワーク テンプレートを無効にする] を選択します。デフォルトで は、この操作により、ファイアウォールからテンプレー ト情報も削除されます。テンプレート情報のローカルコ ピーをファイアウォールで保管する場合は、ボタンをク リックしたときに開いたダイアログボックスの Import

 Device and Network Templates before disabling [無効に する前にデバイスとネットワークテンプレートをイン ポート]のオプションを選択します。コミットを実行する と、テンプレート情報はファイアウォール設定の一部とな り、Panorama ではその情報が管理の対象外となります。 マルチ vsys ファイアウォールの場合は、ま ずテンプレート構成をインポートしてから、 デバイス グループの設定をインポートし て、Panorama プッシュ構成を正常に無効に する必要があります。 通常の操作状況下では、Panorama 管理を無 効にすることは不要であるうえに、ファイア ウォールのメンテナンスと設定が複雑になり かねません。このオプションは通常、ファイ アウォールでテンプレートの定義とは異なる デバイスとネットワーク設定値が必要な場合 に適用されます。たとえば、テストのために ファイアウォールを本番環境からラボ環境に 移動する場合などです。
テンプレートを再度受け入れるようにファイアウォールを
設定するには、Enable Device and Network Templates[デ バイスとネットワーク テンプレートを有効にする] をク リックします。

Panorama Settings(Panorama の設定):Panorama > Setup > Management [Panorama > セットアップ > 管理]

Panorama を使用してファイアウォールを管理する場合、Panorama で以下の設定を行いま す。これらの設定により、Panorama から管理対象ファイアウォールへの接続に関するタイム アウトおよび SSL メッセージ試行回数と、オブジェクト共有パラメータが決まります。

ファイアウォール、または Panorama のテンプレートにも Panorama 接続設定を定義する必要があります。 Panorama Settings(Panorama 設定): Device(デバイス) > Setup(セットアップ) > Management(管理)を参照してください。

ファイアウォールは Panorama と認証を行う際、AES256により暗号化された SSL 接続を使用します。デフォルトでは、Panorama とファイアウォールは、 事前定義済みの 2,048 ビット証明書を使用して互いに認証を行い、SSL 接続を 使用して設定管理とログ収集を行います。これらの SSL 接続のセキュリティを さらに強化するには、「Customize Secure Server Communication(保護された サーバー通信のカスタマイズ)」を参照し、Panorama とそのクライアント間の カスタム証明書を設定してください。

項目	の意味
デバイスへのデータ受信のタイ ムアウト	すべての管理対象ファイアウォールから TCP メッセージを 受信するときのタイムアウト(秒単位)を入力します(範 囲は 1 ~ 240、デフォルトは 240)。
デバイスへのデータ送信のタイ ムアウト	すべての管理対象ファイアウォールに TCP メッセージを送 信するときのタイムアウト(秒単位)を入力します(範囲 は1~240、デフォルトは240)。
デバイスに送信される SSL のカ ウントの再試行	管理対象ファイアウォールに Secure Socket Layer(SSL) メッセージを送信するときの許容再試行回数を入力します (範囲は 1 ~ 64、デフォルトは 25)。
未使用のアドレスとサービス オ ブジェクトをデバイスと共有	すべてのPanorama共有オブジェクトおよびデバイスグ ループ固有のオブジェクトを管理対象ファイアウォールで 共有するには、このオプションを選択します(デフォルト で有効)。
	このオプションを無効にすると、アプライアンスによっ て Panorama ポリシー内のアドレス、アドレスグループ、 サービス、およびサービスグループオブジェクトへの参照 がチェックされ、参照されないオブジェクトは共有されま せん。このオプションにより、アプライアンスから管理対 象ファイアウォールに必要なオブジェクトのみが送信され るようになり、オブジェクトの総数が削減されます。
	デバイス グループ内の特定のデバイスを対象とするポリ シー ルールがある場合、そのポリシーで使用されているオ ブジェクトは、そのデバイス グループで使用されていると 見なされます。
上位で定義されたオブジェクト が優先されます	階層内の異なるレベルのデバイスグループに同じタイプ と名前のオブジェクトがあり、それらの値が異なる場合、 先祖(上位)グループのオブジェクト値が子孫(下位)グ ループのオブジェクト値よりも優先されることを指定する には、このオプションを選択します(デフォルトでは無 効)。つまり、デバイスグループのコミットを実行する と、すべての値が先祖の値でオーバーライドされます。同 様に、このオプションでは、共有オブジェクトの値が、デ バイスグループ内にある同じタイプと名前のオブジェクト の値をオーバーライドします。 このオプションを選択すると、Find Overridden
	ンクが表示されます。

項目	の意味
オーバーライドされたオブジェ クトの検索	このオプション (Panorama 設定の下部)を選択すると、 すべてのシャドー オブジェクトのリストが表示されます。 シャドー オブジェクトは、Shared (共有)場所にあるオ ブジェクトで、デバイス グループ内に同じ名前の、値が 異なるオブジェクトがあります。このリンクは、Objects defined in ancestors will take higher precedence (上位で定 義されたオブジェクトが優先されます)を指定した場合に のみ表示されます。
グループでのレポートとフィル タリングの有効化	ファイアウォールから受け取ったユーザー名、ユーザー グループ名、およびユーザー名とグループ間のマッピン グ情報を Panorama でローカルに保存するには、このオ プションを選択します(デフォルトでは無効)。このオ プションは Panorama のすべてのデバイス グループにグ ローバルに適用されます。ただし、各デバイス グループ のレベルでローカル ストレージを有効にする必要もあり ます。これを行うには、Master Device(マスター デバイ ス)を指定し、ファイアウォールをStore users and groups from Master Device(マスター デバイスからのユーザーと グループを保存する)に設定します。
Secure Communication Settings (安全な通信の設定):Panorama > Setup > Management [Panorama > セットアップ > 管理]	
保護されたサーバー通信のカス タマイズ	 Custom Certificate Only(カスタム証明書のみ) – 有効にすると、Panoramaは、管理対象のファイアウォールおよびログコレクタとの認証用のカスタム証明書のみを受け付けます。
	 SSL/TLS Service Profile (SSL/TLS サービス プロファ イル) – ドロップダウン リストから SSL/TLS サー ビス プロファイルを選択します。このプロファイル は、Panorama との通信でファイアウォールが使用でき

と、クライアントから提供された証明書チェーンの認証 に使用できるルート CA を定義します。
Authorization List(承認リスト) –次のフィールドを使 用して新しい承認プロファイルを Add(追加)および 設定し、Panorama に接続できるクライアント デバイス の承認基準を設定します。Authorization List(承認リス

る証明書およびサポートされる SSL/TLS バージョンを

 Certificate Profile(証明書プロファイル) – ドロップ ダウンリストから証明書プロファイルを選択します。
 この証明書プロファイルは、証明書失効チェックの動作

定義します。

項目	の意味
	ト)は、最大 16 件のプロファイルのエントリをサポー トします。
	 Identifier (識別子) –Select Subject (サブジェクト) または Subject Alt (サブジェクト代替) を選択します。認証識別子としてのName (名前) を付けます。
	 Type (タイプ) – Subject Alt (サブジェクト代替) の場合。Name (名前) が識別子である場合、識別 子のタイプとしてIP、hostname (ホスト名)、また はe-mail (電子メール) を選択します。Subject (サ ブジェクト)を選択した場合、common name (共通 名) が識別子タイプになります。
	 Value(値) – 識別子の値を入力します。
	 Authorize Clients Based on Serial Number (シリアル番号に基づいてクライアントを承認) –Panorama は、クライアント デバイスをデバイスのシリアル番号のハッシュに基づいて承認します。
	 Check Authorization List(承認リストのチェック) – Panorama はクライアント デバイスの ID を認証リスト と照合して確認します。デバイスはリストの1基準のみ と一致するだけで承認されます。一致がない場合、デバ イスは承認されません。
	 Disconnect Wait Time (min) (切断待機時間(分)) 管理対象デバイスとの現在の接続を終了する まで Panorama が待機する時間(分単位)。その 後、Panorama は、設定済みの「保護されたサーバー通 信」設定を使用して、管理対象デバイスとの接続を再度 確立します。待機時間は、保護されたサーバー通信の設 定がコミットされた後に開始されます。
保護されたクライアント通信	Secure Client Communication (保護されたクライアント通 信)を使用すると、クライアント Panorama は (デフォル トで事前定義される証明書の代わりに)設定済みのカスタ ム証明書を使用して、HA ペアの Panorama アプライアン スまたは WildFire アプライアンスへの SSL 接続を認証しま す。
	• Predefined(事前定義済み)(デフォルト)–デバイス 証明書は設定されず、デフォルトの事前定義済みの証明 書が使用されます。
	• Local (ローカル) – Panorama は、ファイアウォールで 生成されたか既存のエンタープライズ PKI サーバーから

項目	の意味
	インポートされたローカルのデバイス証明書および対応 する秘密鍵を使用します。
	 Certificate(証明書) – ローカルのデバイス証明書 を選択します。
	 Certificate Profile(証明書プロファイル) – ドロッ プダウン リストから証明書プロファイルを選択しま す。
	 SCEP – Panorama は、Simple Certificate Enrollment Protocol (SCEP) サーバーで生成されたデバイス証明 書と秘密鍵を使用します。
	 SCEP Profile (SCEP プロファイル) – ドロップダウンリストから SCEP プロファイルを選択します。
	 Certificate Profile(証明書プロファイル) – ドロッ プダウン リストから証明書プロファイルを選択しま す。
	• Customize Communication(カスタマイズ通信)
	 HA Communication (HA 通信) – Panorama は HA ピアとの HA 通信に設定されたクライアント証明書 を使用します。
	 WildFire Communication (WildFire 通信) – Panorama は設定されたクライアント証明書を使用し て WildFire アプライアンスと通信します。

ロギングおよびレポート設定

以下を変更するには、このセクションを使用します。

- レポートおよび以下のログタイプの有効期間およびストレージ割り当て。設定は、高可用 性ペア間で同期されます。
 - ファイアウォールで生成され、ローカルに保管されているすべてのタイプのログ (「Device(デバイス) > Setup(セットアップ) > Management(管理)」を参 照)。設定は、ファイアウォールのすべての仮想システムに適用されます。
 - Panorama モードの M-Series アプライアンスまたは Panorama 仮想アプライアンスが ローカルに生成して保存するログ:システム、設定、アプリケーション統計、User-ID[™] ログ(Panorama > Setup(セットアップ) > Management(管理))
 - レガシーモードの Panorama バーチャル アプライアンスでローカルに生成されたまた はファイアウォールから収集されたすべてのタイプのログ(「Panorama > Setup(セッ トアップ) > Management(管理)」を参照)。



ファイアウォールから Panorama ログ コレクタに送信されるログについて は、ストレージ割り当てと有効期間を各コレクタ グループで設定します (「Panorama > Collector Groups(コレクタ グループ)」を参照)。

項目	の意味
• ユーザーアクティビティレポ	ートの計算およびエクスポートの属性
 ファイアウォールまたは Panorama で作成された事前定義済みレポート 	
Log Storage (ログストレージ) タ	ログ タイプごとに、次の設定を指定します。
ブ	● Quota(割り当て) – ハードディスク上に割り当てる
(Panorama 管理サーバー、	ログ ストレージの割り当て(パーセント)。Quota[割
および PA-5200 シリーズと	り当て]の値を変更すると 関連付けられたディスクの

わよび PA-5200 シリースと PA#7000 シリーズのファイア ウォールを除くすべてのファイ アウォール モデル) 1) スーレ シの副りョて (スーピント)。Quota[副 り当て]の値を変更すると、関連付けられたディスクの 割り当てが自動的に変更されます。すべての値の合計が 100%を超える場合、メッセージが赤で表示され、設定 を保存しようとする場合にエラー メッセージが表示さ

項目		の意味
項日	Logging and Reporting Settings(ログ とレポートの設 定)を編集する 場合(Panorama > Setup(セッ トアップ) > Management(管 理))、Panorama はこのタブ を表示しま す。Panorama テンプレートを 使用ってファイ アウォールの設 定を行う場合は (「Device(デ バイス) > Setup(セッ トアップ) > Management(管 理))、「Single Disk Storage(シ ングル ディスク ストレージ)タ ブおよび Multi Disk Storage(マ ルチ ディスクス トレージ)タブ」 を参照してください。	 の意味 れます。これが発生する場合、合計が 100% の上限を超えないようにパーセンテージを調整します。 VM-Series ファイアウォールはデフォルトでSCTP ログストレージ、SCTP Summary (SCTP サマリー)、Hourly SCTP Summary (1時間ごとの SCTP サマリー)、Daily SCTP Summary (1 日ごとの SCTP サマリー)、Weekly SCTP Summary (1週間ごとのSCTP サマ リー)、C 0%の割り当てがあるため、これらのファイアウォールには SCTP 情報を記録するためのパーセントを割り当てる必要があります。 Max Days (最大日数) - ログの有効期間(日数)(範囲は 1~2,000)。ファイアウォールまたは Panorama アプライアンスは、指定した期間を超えるログを自動的に削除します。デフォルトでは、有効期間はありません。つまり、ログを無期限に使用できます。 ファイアウォールまたは Panorama アプライアンスは、ログの作成中にログを検証し、有効期間または割り当てサイズを超えているログを削除します。 週次サマリーログは、ファイアウォールがログを削除する各タイミングの間に有効期限のしきい値に達すると、次の削除の前にしきい値を超える可能性があります。ログ割り当てが最大サイズに達した場合、新しいログエントリは最も古いログエントリを上書きして作成されます。ログ割り当てサイズを小さくする場合、ファイアウォールまたはPanoramaはその変更をコミットした際に最も古いログを削除します。HA アクティブパッジブ設定の場合、パッシブ プピアはロログを一般す
		 生してアクティブになるまでログを削除しません。 Core Files (コアファイル) – ファイアウォールでシステム プロセスの障害が発生した場合、プロセスの 詳細と障害の原因が含まれるコアファイルが生成されます。コアファイルが大きすぎてデフォルトのコアファイル保存場所 (/var/cores パーティション) に入らない場合、large-core ファイル オプション

項日	の意味
	を有効にして、代替のより大きな保存場所(/opt/ panlogs/cores)を割り当てることができます。Palo Alto Networks サポートエンジニアは、割り当てられた ストレージを必要に応じて増やすことができます。
	large-core ファイル オプションを有効または無効にす るには、コンフィギュレーション モードから次の CLI コマ ンドを入力し、コンフィギュレーションを コミット しま す。
	<pre># set deviceconfig setting management larg e-core [yes no]</pre>
	コア ファイルをエクスポートするには、操作モードから SCP を使用する必要があります。
	<pre>> scp export core-file large-corefile</pre>
	Palo Alto Networks サポート エンジニアのみ がコア ファイルのコンテンツを解釈できます。
	 Restore Defaults(デフォルトを復元) – デフォルト値 に戻すには、このオプションを選択します。
Session Log Storage(セッ ション ログ ストレージ)タ ブおよび Management Log Storage(管理ログ ストレー ジ)タブ	PA-5200 シリーズと PA-7000 シリーズのファイアウォー ルは、管理ログとセッションログを別々のディスクに 保存します。ログのセットごとにタブを選択し、Log Storage(ログ保存エリア)タブで説明されている設定を指 定します。
(PA-5200 シリーズおよび PA#7000 シリーズのファイア ウォールのみ)	 Session Log Storage (セッションログストレージ) – Session Log Quota (セッションログ割り当て)を選択 し、トラフィック、脅威、URL フィルタリング、HIP マッチ、User-ID、GTP/トンネル、SCTP、および認証 のログのほか、拡張脅威の PCAP に対して割り当てと有 効期間を設定します。
	 Management Log Storage(管理ログストレージ) – システム、設定、およびアプリケーション統計のログ のほか、HIP レポート、データフィルタリングキャプ

項目	の意味
	チャ、アプリケーション PCAP、およびデバッグ フィル タ PCAP に対して割り当てと有効期間を設定します。
Single Disk Storage(シングル ディスクストレージ)タブおよ び Multi Disk Storage(マルチ ディスクストレージ)タブ	Panorama テンプレートを使用してログ割り当てと有効期間を設定する場合、テンプレートに割り当てられたファイアウォールに基づいて、次のタブの1つ、または両方の設定を指定します。
(Panorama テンプレートの み)	 PA-5200 シリーズと PA-7000 シリーズのファイア ウォール – Multi Disk Storage (マルチ ディスクス トレージ)を選択し、Session Log Storage (セッショ ンログストレージ)タブおよび Management Log Storage (管理ログストレージ)タブの設定を指定しま す。
	 PA-5200 Series ファイアウォールはデ フォルトでSCTP ログストレージ、SCTP Summary (SCTP サマリー)、Hourly SCTP Summary (1時間ごとの SCTP サマリー)、Daily SCTP Summary (1 日ごとの SCTP サマリー)、Weekly SCTP Summary (1週間ごとのSCTP サマ リー)に 0%の割り当てがあるため、これ らのファイアウォールには SCTP 情報を記 録するためのパーセントを割り当てる必 要があります。
	 その他のファイアウォールモデル – Single Disk Storage (シングルディスクストレージ)を選択 し、Session Log Quota (セッションログ割り当て)を 選択して、Log Storage (ログ保存エリア)タブの設定 を指定します。
Log Export and Reporting (ログ のエクスポートとレポート) タ	必要に応じて、ログのエクスポートとレポートに関する次 の設定を指定します。
ブ	 Number of Versions for Config Audit[設定監査のバージョン数] - 保存可能な設定監査のバージョン数を入力します (デフォルトは 100)。この数を超えると最も古いバージョンが廃棄されます。保存されたバージョンを使用して、設定の変更の監査と比較を行うことができます。 Number of Versions for Config Packang (設定バック)
	 Number of versions for Config Backups (設定ハック アップのバージョン数) – (Panorama のみ) 保存可能な設 定バックアップ数を入力します (デフォルトは 100)。こ

項目	の意味
	の数を超えると最も古い設定バックアップが廃棄されま す。
	 Max Rows in CSV Export (CSV エクスポートの最大行数) – トラフィック ログビューの Export to CSV (CSVにエクスポート)で生成される CSV レポートに表示される行の最大数を入力します(範囲は 1 ~ 1,048,576、デフォルトは 65,535)。
	 Max Rows in User Activity Report (ユーザー アクティ ビティレポートの最大行数) – 詳細なユーザー ア クティビティレポートでサポートされる最大行数を 入力します(範囲は 1 ~ 1,048,576、デフォルトは 5,000)。
Log Export and Reporting (ログ のエクスポートとレポート) タ ブ (続き)	 Average Browse Time (sec) (平均ブラウズ時間(秒)) Monitor (監視) > PDF Reports (PDF レポート) > User Activity Report (ユーザー アクティビティ レポート)のブラウズ時間(秒単位)の計算方法を調整するには、この変数を設定します(範囲は 0 ~ 300、デフォルトは 60)。
	計算対象としては、Web 広告やコンテンツ配信ネット ワークとして分類されたサイトは無視されます。ブラウ ズ時間の計算は、URL フィルタリングログに記録され たコンテナページに基づきます。計算に含めるべきで はない外部サイトからコンテンツをロードするサイトが 多くあるため、コンテナページがこの計算の基準とし て使用されます。コンテナページの詳細は、コンテナ ページを参照してください。平均ブラウズ時間の設定 は、管理者が想定するユーザーが Web ページを閲覧す る平均時間です。平均ブラウズ時間が経過した後に行わ れたリクエストは、新しいブラウズアクティビティと 見なされます。計算対象からは、最初のリクエスト時間 (開始時間) から平均ブラウズ時間までの間にロードされ る新しい Web ページは無視されます。この動作は、任 意の Web ページ内にロードされる外部サイトを除外す るために設計されています。例:平均ブラウズ時間が2分 に設定されている場合は、ユーザーがWebページを開 き、そのページを5分間閲覧しても、そのページのブラ ウズ時間は2分になります。ユーザーがあるページを閲 覧する時間を判断する方法がないため、このような動作 が設定されています。

項目	の意味
	20)。最初のページのロードからページロードしきい 値までの間に発生するリクエストは、ページの要素と 見なされます。ページロードしきい値の範囲外で発生 するリクエストは、ページ内のリンクをユーザーがク リックしたものと見なされます。ページロードしきい 値は、Monitor(監視) > PDF Reports(PDF レポー ト) > User Activity Report(ユーザー アクティビティ レポート)の計算にも使用されます。
	 Syslog HOSTNAME Format (Syslog HOSTNAME 形式) – syslog メッセージ ヘッダーで FQDN、ホスト名、または IP アドレス(IPv4 または IPv6)を使用するかどうかを選択します。このヘッダーは、メッセージの送信元のファイアウォールまたは Panorama 管理サーバーを識別します。
	 Report Runtime(レポートの実行時間) – ファイア ウォールまたは Panorama アプライアンスで毎日の定 期的なレポートの生成を開始する時刻(デフォルトは 2 a.m.)を選択します。
	 Report Expiration Period (レポートの有効期間) – レ ポートの有効期間(日単位)を設定します(範囲は 1 ~ 2,000)。デフォルトでは、有効期間はありません。 つまり、レポートを無期限に使用できます。ファイア ウォールまたは Panorama アプライアンスは、システム 時間に基づき、有効期限を過ぎたレポートを毎晩午前 2 時に削除します。
	 Stop Traffic when LogDb full (LogDb 容量超過時トラフィック転送を停止) – (ファイアウォールのみ、デフォルトでは無効) ログデータベースに空きがない場合にファイアウォール経由のトラフィックを停止する場合は、このオプションを選択します。
	 Enable Threat Vault Access (Threat Vault アクセスの有 効化) – (デフォルトでは有効)ファイアウォールは Threat Vault にアクセスし、検出された脅威に関する最 新情報を収集できます。この情報は、脅威ログと、ACC に示された上位の脅威アクティビティで利用できます。
	 Enable Log on High DP Load (DP 高負荷時にログを有効にする) – (ファイアウォールのみ、デフォルトでは無効)ファイアウォールのパケット処理の負荷によりCPU 使用率が100%に達した場合にシステムログエン

項目	の意味 トリを生成することを指定するには、このオプションを	
	選択します。 Enable Log on High DP Load (DP 負荷が大きい際にログを有効化)すれば、管理者が調査を行って CPU 使用率が高くなっている原因を特定できるようになります。	
	高い CPU 負荷により、CPU がすべてのパ ケットを処理するのに十分なサイクルを 確保できないため、動作が遅くなる可能 性があります。システム ログでこの問題 のアラートが通知 (ログ エントリが毎分生 成) されるため、問題の原因を調査できま す。	
	 Enable High Speed Log Forwarding (高速ログ転送の有効化) (PA-5200 シリーズ、PA-5450、およびPA-7000 シリーズ ファイアウォールのみ; デフォルトでPA-5450 でのみ有効になっています) – ベストプラクティスとして、このオプションを選択すると、最大120,000 ログ/秒の最大レートでログが Panorama に転送されます。無効にすると、ファイアウォールはログをPanorama に単に最高 80,000 ログ/秒の割合で転送します。 このオプションを有効にした場合、ファイアウォールはログをローカルに保存しません。つまり、ログは Dashboard (ダッシュボード)、ACC、またはMonitor (監視) タブに表示されません。また、このオプションを使用するには、Panorama へのログ転送を設定 る必要があります。 	す
	 Log Collector Status (ログコレクタのステータス)-ファ イアウォールが分散ログ収集アーキテクチャへの接続を 成功させ、そこにログを送信しているかどうかを示す ステータスを表示します。ファイアウォールがログを Logging Service(Cortex Data Lake) に送信するようにも 構成されている場合は、Logging Service セクションの Logging Service Status (ロギングサービスのステータス) 	
(Panorama のみ)	 Buffered Log Forwarding from Device (デバイスから転送するログのバッファ) – (デフォルトでは有効) Panorama への接続が失われた場合にファイアウォールでそのハード ディスク (ローカル ストレー 	

項目	の意味
	ジ)にログエントリをバッファすることを許可しま す。Panorama との接続が復元したときに、ファイア ウォールはログエントリを Panorama に転送します。 バッファに使用できるディスク領域は、そのファイア ウォール モデルのログストレージの割り当て、および ロール オーバーを保留しているログの量によって異な ります。使用可能な領域がなくなると、新しいイベント をロギングできるように最も古いエントリが削除されま す。
	 Panorama への接続がダウンした場合にロ グが損失するのを防ぐために、Buffered Log Forwarding from Device (バッファによ るデバイスからのログ転送)を有効化しま す。
	 Get Only New Logs on Convert to Primary (プライマリ への変換時に新しいログのみを取得) (デフォルトでは 無効) –このオプションは、ログをネットワークファ イルシステム (NFS) に書き込む、レガシーモードの Panorama バーチャル アプライアンスにのみ適用されま す。NFS ロギングでは、プライマリ Panorama が NFS にマウントされます。そのため、ファイアウォールはア クティブなプライマリ Panorama のみにログを送信しま す。このオプションでは、HA フェイルオーバーが発生 してセカンダリ Panorama が (プライマリに昇格した後 に) NFS へのロギングを再開した場合、新しく生成さ れたログのみをファイアウォールから Panorama に送信 するように設定できます。このオプションを有効にする のは、通常、Panorama への接続が復元されるまで長時 間かかったときに、ファイアウォールが大量のバッファ 済みログを送信しないようにするためです。
	 Only Active Primary Logs to Local Disk (アクティブ なプライマリ ログのみをローカル ディスクに保存) (デフォルトでは無効) –このオプションは、レガシー モードの Panorama バーチャル アプライアンスにの み適用されます。このオプションでは、アクティブな Panorama のみがローカル ディスクにログを保存するよ うに設定できます。
	 Pre-Defined Reports(事前定義済みレポート)(デフォルトで有効) – アプリケーション、トラフィック、 脅威、URLフィルタリング、ストリーム制御伝送プロトコル(SCTP)の事前定義済みレポートは、ファイアウォールとPanoramaで使用できます。SCTPの事前定

T

項目	の意味
	 義済みのレポートは、SCTP セキュリティが Device(デバイス) > Setup(セットアップ) > Management(管理) > General Settings(一般設定)で有効になった後にファイアウォールと Panorama で使用可能になります。
	ファイアウォールは、1時間ごとの結果の生成(お よび表示用にその結果が集約およびコンパイルされ るPanoramaへの送信)にメモリリソースを使用するた め、メモリ使用量が減るように、重要ではないレポート を無効にできます。レポートを無効にする場合は、その レポートのオプションをオフにします。
	事前定義済みレポートの生成を全体的に有効または無効 にするには、Select All(すべて選択)または Deselect All(すべての選択を解除)をクリックします。
	レポートを無効にする前に、そのレポートがグループレポートや PDF レポートで使用されていないことを確認してください。一連のレポートに割り当てられた定義済みレポートを無効にすると、レポートのセット全体にデータが含まれます。
	 ログ管理アクティビティ(デフォルトで無効) - 管理者 がファイアウォール CLI で操作コマンドを実行する か、Web インターフェイスをナビゲートしたときに監 査ログを生成するかどうかを指定します。監査ログを生 成して転送する前に、syslog サーバーを正常に構成する 必要があります。
	 操作コマンド-管理者が CLI で操作コマンドまたはデ バッグ コマンドを実行するか、Web インターフェイ スからトリガーされる操作コマンドを実行するとき に監査ログを生成します。PAN-OS の操作コマンド とデバッグ コマンドの完全なリストについては、CLI 操作コマンド階層 を参照してください。
	 Ul Actions- 管理者が Web インターフェイスを移動 するときに監査ログを生成します。これには、構成 タブ間のナビゲーションやタブ内の個々のオブジェ クト間のナビゲーションが含まれます。たとえば、 管理者が ACC から Policies タブに移動すると、監査 ログが生成されます。さらに、監査ログは、管理者 が オブジェクト > アドレス から オブジェクト > タグ に移動すると生成されます。

項目	の意味
	 Syslog Server - 監査ログを転送するターゲット syslog サーバー プロファイルを選択します。
ログインターフェース (PA-5450	のみ)
IP アドレス	ログ インターフェイス ポートの IP アドレスを入力しま す。
	ログ・インターフェースが IP アドレスで構成されている場合、特定のサービスにサービス経路が指定されていない限り、すべてのログ転送は、管理インターフェース (デフォルト)による処理からログ・インターフェースに自動的に切り替わります。特定のサービス経路は、ログ・インターフェースによって優先順位が付けられます。
ネットマスク	ログ インターフェイスの IP アドレスのネットワーク マス クを指定します。
デフォルト ゲートウェイ	デフォルト ゲートウェイの IP アドレスを入力して、送信 ログのパスを有効にします。
IPv6 アドレス	ネットワークで IPv6 が使用されている場合は、以下を定 義します。
	 IPv6 アドレス – ログインターフェイス ポートの IPv6 アドレス。
	 IPv6 デフォルトゲートウェイ – ポートのデフォルト ゲートウェイの IPv6 アドレス。
リンク速度	インターフェイス速度を Mbps で選択するか、auto (デ フォルト)を選択して、ファイアウォールが接続に基づい て速度を自動的に決定するようにします。スピード設定が 不可のインターフェイスについてはautoのみ設定可能で す。
リンクデュプレックス	インターフェイスの伝送モードを、フル デュプレックス (full)、ハーフ デュプレックス (half)、オート ネゴシエー ション (auto) から選択します。
リンク ステート	接続に応じて、インターフェイスの状態を、有効 (up)、無 効 (down)、自動決定 (auto) から選択します。デフォルト設 定はautoです。

項目	の意味
ログインターフェイスの統計情 報	Show Statistics を選択して、パケットの統計情報とエラーを表示します。

バナーとメッセージ

Message of the Day (本日のメッセージ) ダイアログですべてのメッセージを表示するに は、「本日のメッセージ」を参照してください。

本日のメッセージを設定して **OK** をクリックすると、その後ログインする管理 者や、画面の更新を行ったアクティブな管理者に対し、新しいメッセージや アップデートされたメッセージが即座に表示されるようになります(コミット する必要はありません)。これにより他の管理者に対し、間もなく実行予定の コミットを実行前に通知することができます。

当日のメッセージ (チェック ボックス)	管理者が Web インターフェイスヘログインする時に「本 日のメッセージ」ダイアログを表示させる場合はこのオプ ションを選択してください。
当日のメッセージ (テキスト入力フィールド)	「本日のメッセージ」ダイアログ用のテキスト(最 大3,200文字)を入力してください。
今後は表示しないオプションの 有効化	 「本日のメッセージ」ダイアログにDo not show again (今後は表示しない)オプションを含める場合はこちらを選択してください (デフォルトでは無効)。このオプションを使用すると、以降のログインで管理者に同じメッセージが表示されなくなります。 Message of the Day [本日のメッセージ]のテキストを編集した場合、Do not show again [今後は表示しない]を選択した管理者にもそのメッセージが表示されます。変更したメッセージを以降のセッションで表示したくない場合、メッセージが再度変更されない限り、管理者はこのオプションを再度選択する必要があります。
	「本日のメッセージ」のヘッダーを入力します(デフォル トはMessage of the Dayです)。
背景の色	「本日のメッセージ」ダイアログ用の背景色を選択してく ださい。デフォルト(None [なし])は薄いグレーの背景で す。

項目	の意味
Icon(アイコン)	「本日のメッセージ」のテキストの上に表示する、事前設 定済のアイコンを選択します。
	 None[なし] (デフォルト)
	• I
	γ (?)
	● 情
	報
	• <u>警</u>
ヘッダーバナー	ヘッダーバナーに表示するテキストを入力してください (最大3,200文字)。
ヘッダーの色	ヘッダーの背景色を選択します。デフォルト(None [な し])は透明な背景です。
ヘッダーの文字色	ヘッダーテキストの文字色を選択します。デフォルト (None [なし])は黒です。
ヘッダーとフッターに同じバ ナーを使用する	フッターバナーにヘッダーバナーと同じテキストと配色 を割り当てたい場合はこのオプションを選択してくださ い(デフォルトでは有効)。このオプションを有効化する と、フッターバナー用のテキスト入力欄と色のフィールド はグレー表示になります。
フッターバナー	フッターバナーに表示するテキストを入力してください (最大 3,200 文字)。
フッターの色	フッターの背景色を選択します。デフォルト(None [な し])は透明な背景です。
フッターの文字色	フッターテキストの文字色を選択します。デフォルト (None [なし])は黒です。
パスワード複雑性設定	
enabled [有効化]	ローカル アカウントのパスワードの最小要件を有効にし ます。この機能を使用すると、定義されたパスワード要件 が、ファイアウォールのローカル管理者アカウントで確実 に順守されます。

項目	の意味
	これらのオプションのサブセットを使用したパスワードプ ロファイルを作成し、設定をオーバーライドしたり、特定 のアカウントに適用したりすることもできます。詳細は、 「Device(デバイス) > Password Profiles(パスワードプ ロファイル)」を参照してください。アカウントで使用で きる有効な文字の詳細は、「ユーザー名とパスワードの要 件」を参照してください。
	パスワードの最大長は 64 文字です。
	高可用性(HA)を設定してある場合は、パスワード複雑 性のオプションを設定するときに必ずプライマリ ピアを使 用し、変更を加えた後にすぐにコミットしてください。
	指定した Password Hash(パスワード ハッシュ)の対象 のローカル データベース アカウントにパスワード複雑性 設定は適用されません(「Device > Local User Database > Users」を参照)。
	醸園なパスワードを必須にして、ブルート フォースによるネットワークアクセス攻撃が成功するのを防ぎます。最低文字数を設定し、大文字、小文字、数字、特殊文字をそれ ぞれ1文字以上求めます。さらに、パスワードで同じ文字を過剰に繰り返したりユーザー 名を使用したりするのを防ぎ、パスワードを 再利用する頻度を制限し、定期的なパスワードの変更期間を設定することでパスワードを 長期間使用し続けられないようにします。パ スワード要件が厳格であれば、攻撃者がパス ワードをハッキングすることが難しくなります。パスワード強度のベストプラクティスに 従ってください。
最小文字数	パスワードの最小長を要求します (範囲は 1 ~ 16 文字)。
	- ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・
最少大文字数	大文字の最小数が必要です (範囲は 0~16 文字です)。
最少小文字数	小文字の最小数が必要です(範囲は0~16文字です)。

項目	の意味
最少数字数	最小数の数字が必要です (範囲は 0~16 個の数字です)。
最少特殊文字数	特殊 (英数字以外の) 文字の最小数が必要です (範囲は 0 から 16 文字です)。
繰り返し文字のブロック	パスワードに許可される順次重複文字の数を指定してくだ さい(範囲は3から16です)。
	値を3に設定すると、パスワードのシーケンスに同じ文字 を3回含めることができますが、同じ文字を4回以上順番 に使用すると、パスワードは許可されません。
	たとえば、値が3に設定されている場合、システムは パスワード test111 または 111test111 を受け入れます が、test1111 は受け入れません。
ユーザー名を含むパスワードを 禁止 (逆順を含む)	アカウントユーザー名(またはそれを逆読みにしたもの) をパスワードに使用できないようにする場合は、このオプ ションを選択します。
文字が異なる新規パスワード	管理者が自分のパスワードを変更するときに、文字は指定 した値によって異なる必要があります。
初回ログイン時にパスワードの 変更を要求	管理者がファイアウォールに初めてログインする際にパス ワードの変更を求めるプロンプトを表示するには、このオ プションを選択します。
パスワードの再使用禁止制限	指定した数に基づいて、以前のパスワードを再使用しない ように要求します。たとえば、値を「4」に設定すると、 直近の4つのパスワードを再使用することができなくなり ます(範囲は0~50)。
パスワード変更期間のブロック (日)	指定した日数が経過するまで、ユーザーはパスワードを変 更できません(範囲は 0 ~ 365 日)。
パスワード有効期限(日数)	管理者は、日数(範囲は 0 ~ 365 日)で定期的にパスワー ドを変更する必要があります。たとえば、値を「90」に設 定すると、管理者に 90 日ごとにパスワードの変更を求め るプロンプトが表示されます。
	失効の警告を 0 ~ 30 日の範囲で設定して猶予期間を指定 することもできます。
失効の警告期間(日数)	Required Password Change Period (パスワード有効 期限)が設定されている場合は、ユーザーに対してこ のExpiration Warning Period (失効の警告期間)を使用す

項目	の意味
	ることで、必要な変更日前に指定された日数(0~30の範 囲)が残っていない場合に、各ログイン時にパスワードを 変更するようプロンプトを表示させることができます。
失効後の管理者ログイン回数 (カウント)	必要な変更日の後に、管理者が指定した回数ログインでき るようにします(範囲は 0~3)。たとえば、この値を 3 に設定してアカウントの有効期限が切れた場合、アカウン トがロックアウトされる前にパスワードを変更せずに 3 回 以上ログインできます。
失効後の猶予期間 (日数)	アカウントが失効しても、管理者はここで指定した期間 (日数)はログインできます(範囲は 0 ~ 30 日)。
AutoFocus [™]	·
enabled [有効化]	 ファイアウォールとAutoFocusポータルの接続を有効化することで、脅威インテリジェンスデータの取得や、ファイアウォールとAutoFocusを統合的に検索することが可能になります。 AutoFocus に接続されると、ファイアウォールにはトラフィック、脅威、URL フィルタリング、WildFireへの送信、およびデータフィルタリングのログエントリに関する AutoFocus データが表示されるようになります(Monitor(監視) > Logs(ログ))。これらのタイプのログエントリ(IPアドレスやURLなど)から分析結果をクリックし、それに対するAutoFocus調査結果と統計のサマリーを表示することができます。さらにその分析結果に対し、ファイアウォールから直接、拡張AutoFocus検索を行うことができます。 ファイアウォールで AutoFocus ライセンスが有効かどうか確認してください(Device(デバイス) > Licenses(ライセンス管理]にあるいずれかのオプションを使用してライセンスをアクティベートしてください。
AutoFocus URL	AutoFocus URLを入力します。 https:// autofocus.paloaltonetworks.com:10443
クエリタイムアウト(秒数)	ファイアウォールが AutoFocus に対し脅威インテリジェン スデータのクエリを行う際の試行継続時間(秒単位)を設

項目	の意味
	定します。AutoFocusポータルが指定した時間内に応答し ない場合、ファイアウォールは接続を切断します。

Cortex Data Lake

このセクションを使用して、Cortex Data Lake にログを転送するように VM-Series とハード ウェアベースのファイアウォールを設定します。以下に説明するオプションを設定するため の完全なワークフローは次のとおりです。

- Cortex Data Lake へのLogging (ログ)の開始 (Panorama なし)
- Cortex Data Lake へのLogging (ログ)の開始 (Panorama マネージドファイアウォール用)

Logging Service (ログサービス)の名前は、Cortex Data Lake に変更されました。 ただし、一部のファイアウォール機能とボタンでは、引き続きLogging Service (ログサービス)と表示されます。

Cortex Data Lake の有効化	このオプションを選択すると、ファイアウォール (Panorama を使用している場合は、選択した Template に属する ファイアウォール がログを Cortex Data Lake (Cortex Data Lake は以前は Logging Service と呼ばれてい ました)に転送できます。
	Log Forwarding (Objects > Log Forwarding を構成した後、 ファイアウォール はログを Cortex Data Lake に直接転送 します。これは Panorama が管理する ファイアウォール にも当てはまります。
Enable Duplicate Logging (重複 ログを有効にする) (Panorama マネージドファイアウォールの み)	Enable Duplicate Logging (重複ログを有効にする) により、Cortex Data Lake へのログの送信に加えて、Panorama および分散 Log Collectors (ログ コレクター) へのログの送信が続行されます。
	このオプションにより、Cortex Data Lake を評価すること ができます–有効にすると、選択したテンプレートに属す るファイアウォールは、ログのコピーを Cortex Data Lake と Panorama または 分散ログ収集 アーキテクチャの両方 に保存します。
Enable Enhanced Application Logging(高度なアプリケー ション ロギングの有効化)	Enable Enhanced Application Logging (高度なアプリケー ションロギングの有効化) は、ファイアウォールが Palo Alto Networks アプリケーションのネットワーク可視性 を高めるデータを収集する場合に実行します。たとえ ば、このネットワークの可視性の向上により、Palo Alto Networks Cortex XDR アプリは、通常のネットワークアク ティビティのベースラインをより適切に分類して確立でき

項目	の意味
	るため、ファイアウォールは攻撃を示す可能性のある異常 な動作を検出できます。
	Enhanced Application Logging には、Logging Service (Cortex Data Lake) ライセンスが必要です。これらのログ は表示できません。これらのログは、Palo Alto Networks アプリケーションによってのみ使用されるように設計され ています。
リージョン	ファイアウォールがログを転送する Cortex Data Lake (Logging Service) インスタンスの地理的リージョンを選 択します。Cortex ハブ にログインして、Cortex Data Lake インスタンスが展開されているリージョンを確認 します (ハブで、トップ メニュー バーの設定ギアを選択 し、Manage Apps (アプリの管理)を選択します)。
PA-7000 シリーズおよび PA-5200 シリーズ ファイア ウォールの CortexDataLake へ の接続数	(PA-7000 シリーズ および PA-5200 シリーズのファイ アウォールのみ) ファイアウォールから Cortex Data Lake にログを送信するための接続数を指定します(範囲は 1 ~ 20、デフォルトは 5)。ファイアウォール上で request logging-service-forwarding status の CLI コマン ドを使用し、ファイアウォールおよび Cortex Data Lake 間 のアクティブな接続数を確認できます。
Panorama なしのオンボード (Panorama によって管理されて いない ファイアウォールの場 合)	Panoramaが管理していないファイアウォールを有効化し て、Cortex Data Lake にログを送信する事ができます。こ れを実行するには、まず Cortex Data Lake アプリケーショ ンでキーを生成する必要があります。このキーにより、 ファイアウォールは Cortex Data Lake を認証して安全に接 続できます。生成後にキーを入力し、ファイアウォールを 有効にして、Cortex Data Lake へのログの転送を開始しま す。
ロギング サービスのステータス	Cortex Data Lake への接続のステータスを表示しま す。Show Status (ステータスを表示)して次のチェックの詳 細を表示します:
	 License (ライセンス)–OK または Error (エラー) であ り、ファイアウォールがログを Cortex Data Lake に転 送するための有効なライセンスを持っているかどうかを 示します。
	 Certificate (証明書)–OK または Error (エラー) であ り、ファイアウォールが Cortex Data Lake に認証する ために必要となる証明書を正常に取得したかどうかを示 します。

項目	の意味
	 Customer Info (顧客情報)–OK または Error (エラー) で、Cortex Data Lake を使用するために必要となる顧客 ID 番号をファイアウォールが持っているかどうかを示 します。ステータスがOKである場合は顧客 ID 番号も表 示されます。
	 Device Connectivity (デバイスの接続性)–ファイア ウォールが正常に Cortex Data Lake に接続されたかど うかを示します。

SSH Management Profiles Settings (SSH 管理プロファイルの設定)

サーバ プロファイル	ネットワーク上の CLI 管理接続用の SSH セッションに適 用される SSH サービス プロファイルの種類の一つです。 既存のサーバ プロファイルを適用するには、プロファイル を選択して、[OK]をクリックし、変更をCommit(コミッ ト)します。
	プロファイルをアクティブにするには、CLI から SSH サービスの再始動を実行する必要が あります。
	詳細については、Device > Certificate Management >SSH Service Profile を参照してください。

アカウンティングサーバー設定

アカウンティングサーバープロ	TACACS+ アカウンティング クライアントが TACACS+ ア
ファイル	カウンティング サーバに接続できるようにするために使用
	する TACACS+ サーバ プロファイルを選択します。

PAN-OS エッジ サービスの設定

サードパーティのデバイスの評 決を有効にする	このオプションは、将来のリリースのために予約されてい ます。このオプションを有効にすると、機能はありませ ん。
接続ステータス	ファイアウォールのエッジサービスへの接続の状態(接続済 みまたは切断済み)を表示します。
ユーザー コンテキスト クラウ ド サービスを有効にする	このオプションを選択すると、firewall がユーザ コンテキ スト クラウド サービスに接続され、クラウド ID エンジン を使用して、firewall およびデバイス間のマッピングやタ グなどの情報の再配布を表示および管理できます。

項目	の意味
接続ステータス	ユーザーコンテキストクラウドサービスへのfirewallの接続 のステータス(接続済みまたは切断済み)を表示します。

Device > Setup > Operations [デバイス > セットアップ > 操作]

以下のタスクを行うことで、Panorama[™] およびファイアウォールで実行中の設定と候補設定を 管理することができます。Panorama[™]仮想アプライアンスを使用している場合、このページの 設定を使用して、レガシー モードの Panorama仮想アプライアンスのログ ストレージ パーティ ションを設定することもできます。

候補設定に加えた変更を有効化する場合はその変更をコミットする必要がありま す。この時点で、変更内容は実行中の設定の一部になります。ベスト プラクティス として、定期的に候補設定を保存することをお勧めします。

設定ファイル、ログ、レポート、およびその他のファイルを SCP サーバーにエク スポートし、それらのファイルを他のファイアウォールや Panorama M-Series ま たは仮想アプライアンスにインポートする場合は CLI で Secure Copy (SCP) コマ ンド を使用することができます。ただし、以下のモデルでは、ログ データベー スはエクスポートやインポートを行うには大きすぎるので、ログ データベース全 体のエクスポートやインポートはサポートされていません。PA-7000 Seriesファイ アウォール(すべての PAN-OS[®] リリース)、Panorama 6.0 以降を実行している Panorama 仮想アプライアンス、および Panorama M-Series アプライアンス(すべて の Panorama リリース)。

機能	の意味
設定の管理	
最後に保存された設定 に戻します	候補設定のデフォルトのスナップショット(.snapshot.xml)(Web インターフェイスの右上にある Config (設定) > Save Changes (変 更の保存)を選択して作成または上書きするスナップショット)を 復元します。
	(Panorama のみ) Select Device Groups & Templates (デバイスグ ループおよびテンプレートを選択)を使用し、元に戻す特定のデバ イスグループ、テンプレート、あるいはテンプレート スタック設定 を選択します。デバイスグループおよびテンプレート管理者は、自 身に割り当てられたアクセスドメイン用のデバイスグループ、テン プレート、あるいはテンプレート スタックだけを選択できます。
実行中の設定に戻す	現在の実行中の設定が復元されます。この操作によって、前回のコ ミット以降に候補設定に対してすべての管理者が加えたすべての変 更が取り消されます。特定の管理者の変更のみを元に戻すには、 「変更を元に戻す」を参照してください。

機能	の意味
	(Panorama のみ) Select Device Groups & Templates (デバイスグ ループおよびテンプレートを選択)を使用し、元に戻す特定のデバ イスグループ、テンプレート、あるいはテンプレート スタック設定 を選択します。デバイスグループおよびテンプレート管理者は、自 身に割り当てられたアクセスドメイン用のデバイスグループ、テン プレート、あるいはテンプレート スタックだけを選択できます。
名前付き設定スナップ ショットの保存	デフォルトのスナップショット(.snapshot.xml)を上書きしない、 候補設定のスナップショットを作成します。スナップショットの Name(名前)を入力するか、上書きする既存の名前付きスナップ ショットを選択します。
	(Panorama のみ) Select Device Groups & Templates (デバイスグ ループおよびテンプレートを選択)を使用し、保存する特定のデバ イスグループ、テンプレート、あるいはテンプレート スタック設定 を選択します。デバイスグループおよびテンプレート管理者は、自 身に割り当てられたアクセスドメイン用のデバイスグループ、テン プレート、あるいはテンプレート スタックだけを選択できます。
候補設定の保存	現在の候補設定で候補設定のデフォルトスナップショット (.snapshot.xml)を作成または上書きします。これは、Web イン ターフェイスの右上にある Config(設定) > Save Changes(変更 の保存)を選択した場合の動作と同じです。特定の管理者の変更の みを保存するには、「候補設定の保存」を参照してください。
	(Panorama のみ) Select Device Groups & Templates (デバイスグ ループおよびテンプレートを選択)を使用し、保存する特定のデバ イスグループ、テンプレート、あるいはテンプレート スタック設定 を選択します。デバイスグループおよびテンプレート管理者は、自 身に割り当てられたアクセスドメイン用のデバイスグループ、テン プレート、あるいはテンプレート スタックだけを選択できます。
名前付きの設定スナッ プショットのロード (ファイアウォール)	現在の候補設定を以下のいずれかで上書きします。 • 名前を付けた候補設定のスナップショット(デフォルトのス ナップショットでけたく)
あるいは	 インポートして名前を付けた実行中の設定。
名前付きの Panorama 設定スナップショット のロード	• 現在実行中の設定。
	設定はそのロード先のファイアウォールまたは Panorama に存在す る必要があります。
	設定の Name (名前)を選択し、Decryption Key (復号化キー)を 入力します。このキーはファイアウォールまたは Panorama のマ スター キーです (「Device > Master Key and Diagnostics」を参 照)。設定内のすべてのパスワードと秘密鍵を復号化するには、こ のマスター キーが必要です。インポートした設定をロードする場

機能	の意味
	合、インポート元のファイアウォールまたは Panorama のマスター キーを入力する必要があります。ロード操作が終了すると、設定の ロード先のファイアウォールまたは Panorama のマスター キーでパ スワードと秘密鍵が再度暗号化されます。
	設定に含まれるすべてのルール用に新しい UUID を生成する場合 (例えば、設定を別のファイアウォールから読み込むものの、設 定を読み込む際に固有のルールを維持したい場合)、スーパーユー ザーがRegenerate Rule UUIDs for selected named configuration (選 択した名前付き設定の ルール UUID を再生成)し、すべてのルール に対して新しい UUID を生成する必要があります。
	(Panorama のみ)オブジェクト、ポリシー、デバイスグループあ るいはテンプレート、あるいはテンプレート設定を指定し、次の 項目を選択することで名前付き設定から部分的に設定を読み込みま す:
	 Load Shared Objects (共有オブジェクトの読み込み)-すべてのデバイスグループおよびテンプレート設定と共に共有オブジェクトだけを読み込みます。
	 Load Shared Policies (共有ポリシーの読み込み) すべてのデバイ スグループおよびテンプレート設定と共に共有ポリシーだけを 読み込みます。
	 Select Device Groups & Templates (デバイスグループおよびテン プレートを選択)–読み込むデバイスグループ、テンプレート、 あるいはテンプレート スタック設定を指定します。デバイスグ ループおよびテンプレート管理者は、自身に割り当てられたア クセスドメイン用のデバイスグループ、テンプレート、あるい はテンプレート スタックだけを選択できます
	 Retain Rule UUIDs (ルールの UUID を保持)–現在アクティブな設定の UUID を保持します。
設定バージョンのロー ド(ファイアウォー	ファイアウォールまたは Panorama に保存されている現在実行中の 設定の以前のバージョンで現在の候補設定を上書きします。
あるいは	設定の Name (名前) を選択し、Decryption Key (復号化キー) を 入力します。このキーはファイアウォールまたは Panorama のマ スクー キーです (「Device > Master Key and Disconsting 」 をお
Panorama 設定バー ジョンのロード	照)。設定内のすべてのパスワードと秘密鍵を復号化するには、このマスターキーが必要です。ロード操作が終了すると、マスターキーでパスワードと秘密鍵が再度暗号化されます。
	(Panoramaのみ)オブジェクト、ポリシー、デバイスグループあるいはテンプレート、あるいはテンプレート設定を指定し、次を選択することで名前付き設定から部分的に設定を読み込みます:

機能	の意味
	 Load Shared Objects (共有オブジェクトの読み込み)-すべてのデバイスグループおよびテンプレート設定と共に共有オブジェクトだけを読み込みます。
	 Load Shared Policies (共有ポリシーの読み込み)すべてのデバイ スグループおよびテンプレート設定と共に共有ポリシーだけを 読み込みます。
	 Select Device Groups & Templates (デバイスグループおよびテン プレートを選択)-読み込むデバイスグループ、テンプレート、 あるいはテンプレート スタック設定を指定します。デバイスグ ループおよびテンプレート管理者は、自身に割り当てられたア クセスドメイン用のデバイスグループ、テンプレート、あるい はテンプレート スタックだけを選択できます
名前付き設定スナップ ショットのエクスポー ト	現在実行中の設定、候補設定のスナップショット、または前回イン ポートした設定(候補または実行中の設定)をエクスポートしま す。ファイアウォールは、設定済みの名前が付与されたXMLファ イルとして設定をエクスポートします。スナップショットはネット ワーク上の任意の場所に保存することができます。
	(Panorama のみ) Select Device Groups & Templates (デバイスグ ループおよびテンプレートを選択)を使用し、エクスポートする特 定のデバイスグループ、テンプレート、あるいはテンプレート ス タック設定を選択します。デバイスグループおよびテンプレート 管理者は、自身に割り当てられたアクセスドメイン用のデバイスグ ループ、テンプレート、あるいはテンプレート スタックだけを選択 できます。
設定バージョンのエク スポート	実行中の Version [バージョン] の設定をXMLファイルとしてエクス ポートします。
	(Panorama のみ) Select Device Groups & Templates (デバイスグ ループおよびテンプレートを選択)を使用し、エクスポートする特 定のデバイスグループ、テンプレート、あるいはテンプレート ス タック設定を選択します。デバイスグループおよびテンプレート 管理者は、自身に割り当てられたアクセスドメイン用のデバイスグ ループ、テンプレート、あるいはテンプレート スタックだけを選択 できます。
Panorama およびデバ イスの設定バンドルの エクスポート (Panorama のみ)	Panorama 実行中の設定のバックアップと各管理対象ファイア ウォールの最新バージョンの生成とエクスポートを行います。設 定バンドルを毎日作成して SCP または FTP サーバーにエクスポー トするプロセスを自動化するには、Panorama > Scheduled Config Export を参照してください。

機能	の意味
デバイスの設定バンド ルのエクスポートまた はプッシュ	ファイアウォールを選択し、Panorama に保存されているファイア ウォール設定に対して以下のいずれかの操作を実行するように求め られます。
(Panorama のみ)	 ファイアウォールに設定を Push & Commit[プッシュ & コミッ ト] する。この操作により、ファイアウォールがクリーニング (ファイアウォールからローカル設定が削除) され、Panorama に保存されているファイアウォール設定がプッシュされます。 ファイアウォール設定をインポートしたら、Panorama で管理で きるように、このオプションを使用してそのファイアウォール をクリーンアップします。
	 ・ 設定をロートせすにファイアワォールに Export[エクスホート] する。設定をロードするには、ファイアウォール CLI にアクセス し、設定モード コマンド load device-state を実行する必要があ ります。このコマンドを使用すると、Push & Commit[プッシュ & コミット]オプションと同じようにファイアウォールがクリー ンアップされます。
	 FW マスター キー を使用して、エクスポートされたデバイス 構成バンドルを、管理対象ファイアウォールに展開されたマス ター キーで暗号化します。FW マスター キー を入力し、を入力 して FW マスター キー を確認します。
デバイス状態のエクス ポート (ファイアウォールの み)	ファイアウォールの状態の情報をバンドルとしてエクスポートしま す。実行中の設定に加え、状態の情報にはPanoramaからプッシュ されたデバイスグループ設定やテンプレート設定が含まれます。 ファイアウォールが GlobalProtect [™] ポータルの場合、バンドルに は証明書情報、ポータルが管理するサテライトの一覧、およびサテ ライト認証情報が含まれています。ファイアウォールまたはポータ ルを交換した場合、代替のものに状態のバンドルをインポートする ことで、エクスポートしておいた情報を復元することができます。
	ファイアウォールの状態のエクスポートを手動で実行する か、スケジュール設定されたXML APIスクリプトを作成し、 リモートサーバーにファイルをエクスポートする必要があり ます。サテライト証明書は頻繁に変更される可能性があるの で、この操作を定期的に行う必要があります。
	CLIでファイアウォール状態ファイルを作成するには、設定モー ドで save device state コマンドを実行します。ファイルに は、device_state_cfg.tgz という名前が付けられ、/opt/ pancfg/mgmt/device-state に保存されます。ファイアウォー ル状態ファイルをエクスポートするための操作コマンドは、scp export device-state です(tftp export device-state も使用できます)。

機能	の意味
	XML あるいは REST API の使用方法の詳細 は、『PAN-OS および Panorama API ガイ ド ば を参照してください。
名前付き設定スナップ ショットのインポート	ネットワーク上から実行中の設定あるいは候補設定をインポートします。Browse[参照] をクリックして、インポートする設定ファイルを選択します。
デバイス状態のイン ポート (ファイアウォールの み)	Export device state (デバイス状態のエクスポート)オプショ ンを選択する場合、ファイアウォールからエクスポートしてお いた状態情報のバンドルをインポートします。実行中の設定に 加え、状態の情報にはPanoramaからプッシュされたデバイスグ ループ設定やテンプレート設定が含まれます。ファイアウォール がGlobalProtectポータルの場合、バンドルには、証明書情報、サテ ライトの一覧、およびサテライト認証情報が含まれています。ファ イアウォールまたはポータルを交換した場合、代替のものに状態の バンドルをインポートすることで情報を復元します。
Panorama にデバイス 設定をインポート (Panorama のみ)	ファイアウォール設定を Panorama にインポートします。ネット ワークおよびデバイス設定を格納するテンプレートが Panorama に よって自動的に作成されます。ファイアウォールの仮想システム (vsys) ごとに、ポリシーおよびオブジェクト設定を格納するデバイ スグループが Panorama によって自動的に作成されます。デバイ スグループは、階層内の Shared (共有)場所の1つ下のレベルに ありますが、インポートの完了後に別の親デバイスグループに再 割り当てすることもできます(「Panorama > VMware NSX」を参 照)。
	 Panorama のコンテンツ (アプリケーションおよび脅威 データベースなど)のバージョンは、設定のインポー ト元となるファイアウォール上のバージョンと同じか それ以上である必要があります。
	以下のインポート オプションを設定します。
	 Device[デバイス] – Panorama が設定をインポートする ファイアウォールを選択します。ドロップダウンリストに は、Panoramaに接続されていて、かつどのデバイスグループや テンプレートにも割り当てられていないファイアウォールのみ が表示されます。個々の vsys ではなく、ファイアウォール全体 のみを選択できます。
	 FW マスター キー を使用:このオフションを有効にすると、管理 対象ファイアウォールに展開されたマスター キーを使用してイ ンポートされたファイアウォール設定を復号化できます。FW マ

J

機能	の意味
	スターキーを入力し、を入力して FW マスターキー を確認し ます。複数のファイアウォールのインポートされた構成を復号 化する場合、ファイアウォールはすべて同じマスターキーを使 用する必要があります。
	 Template Name[テンプレート名] – インポートしたデバイスお よびネットワーク設定を格納するテンプレートの名前を入力し ます。マルチ vsys ファイアウォールの場合、このフィールドは 空白になります。他のファイアウォールの場合、デフォルト値 はファイアウォール名になります。既存のテンプレートの名前 を使用することはできません。
	 Device Group Name Prefix (デバイス グループ名の接頭 辞) (マルチ vsys ファイアウォールのみ) – 必要に応じて、各 デバイス グループ名のプレフィックスとして文字列を追加しま す。
	 Device Group Name[デバイス グループ名] – マルチ vsys ファ イアウォールの場合、デフォルトで各デバイス グループに vsys 名が設定されます。他のファイアウォールの場合、デフォルト 値はファイアウォール名になります。デフォルト名は編集でき ますが、既存のデバイス グループ名を使用することはできませ ん。
	 Import devices' shared objects into Panorama's shared context(デバイスの共有オブジェクトを Panorama の共有コン テクストにインポート)(デフォルトで有効)–Panorama は、 ファイアウォールの Shared(共有)に属するオブジェクトを Panorama の Shared(共有)にインポートします。
	Panoramaは、マルチ仮想システムを有効にしていないファイアウォールではすべてのオブジェクトを共有とみなします。このオプションを無効にすると、Panoramaは、Shared(共有)ではなくデバイスグループに共有ファイアウォールオブジェクトをコピーします。この設定には、以下の例外があります。
	 共有ファイアウォールオブジェクトの名前と値が既存の共有 Panoramaオブジェクトと同じである場合、インポートではそのファイアウォールオブジェクトは除外されます。
	 共有ファイアウォールオブジェクトの名前または値が共有 Panoramaオブジェクトと異なる場合、Panoramaはそのファ イアウォールオブジェクトを各デバイスグループにインポー トします。
	 テンプレートにインポートされる設定で共有ファイアウォー ルオブジェクトを参照している場合、このオプションを選択
機能	の意味
---------	---
	したかどうかに関係なく、Panoramaはそのオブジェクトを Shared [共有] にインポートします。
	 共有ファイアウォールオブジェクトで、テンプレートにイン ポートされる設定を参照している場合、このオプションを選 択したかどうかに関係なく、Panoramaはそのオブジェクトを デバイスグループにインポートします。
	 Rule Import Location[ルールのインポート場所] – Panorama が ポリシーをプレ ルールとしてインポートするのか、ポスト ルー ルとしてインポートするのかを選択します。選択内容に関係な く、Panorama はデフォルトのセキュリティ ルール (intrazone- default および interzone-default) をポスト ルールベースにイン ポートします。
	 Panorama に、インポートするファイアウォール ルールと同じ名前のルールがある場合、Panorama には両方のルールが表示されます。ただし、ルー ル名は一意である必要があるため、Panorama でコ ミットを実行する前にいずれかのルールを削除し ないと、コミットに失敗します。
デバイスの操作	·
再起動	ファイアウォールまたは Panorama を再起動するには、Reboot Device (デバイスの再起動)を実行します。デバイスからログア ウトされ、ソフトウェア (PAN-OSまたは Panorama)およびアク ティブな設定が再度ロードされます。次に既存のセッションが終 了してログが記録され、シャットダウンを実行した管理者の名前 のもとでシステムログエントリが作成されます。保存またはコミッ トされていない設定の変更は失われます(「Device (デバイス) > Setup (セットアップ) > Operations (操作)」を参照)。
	● 運用 CLI 操作コマンドを使用します。
	request restart system
シャットダウン	ファイアウォールや Panorama のグレースフルシャットダウンを実 行する場合は、Shutdown Device(デバイスのシャットダウン)ま たはShutdown Panorama(Panoramaのシャットダウン)をクリッ クし、確認のプロンプトが表示された場合に Yes(はい)を実行し ます。保存またはコミットされていない設定の変更は失われます。 すべての管理者がログオフされ、以下のプロセスが発生します。 ・ すべてのログイン セッションがログオフされます。

機能	の意味
	 すべてのシステム プロセスが停止します。
	• 既存のセッションが終了し、ログに記録されます。
	 シャットダウンを開始した管理者名を示すシステム ログが作成 されます。このログエントリを書き込めない場合は、警告が表 示され、システムはシャットダウンしません。
	 ディスクドライブが正常にアンマウントされ、ファイアウォー ルまたは Panorama の電源がオフになります。
	ファイアウォールまたは Panorama の電源を入れるには、電源のプ ラグを抜いてから差し込み直す必要があります。
	 Web インターフェイスを使用できない場合は、次の CLI 操作コマンドを使用します。
	request shutdown system
データプレーンの再起 動	Restart Dataplane をクリックすると、ファイアウォールのデータ を再起動せずに再起動します。このオプションは、Panorama また は PA-220、PA-800 シリーズ、または VM-Series firewall では使用 できません。
	Web インターフェイスが利用できない場合は、次の CLI コマンドを使用します:
	リクエスト再起動データプレーン
	PA-7000 シリーズ ファイアウォールでは、各NPCにデータプレー ンがあるため、コマンド
	要求シャーシ再起動スロットを実行してNPCを再起動してこの操作 を実行できます。
その他	

カスタム ロゴ	Custom Logo(カスタム ロゴ) をクリックすると以下の任意の内 容をカスタマイズします。
	 Login Screen(ログイン画面)の背景イメージ
	 Main UI (メイン UI) (Web インターフェイス) ヘッダーのイ メージ
	 PDF Report Title Page (PDF レポートのタイトルページ)のイメージ。「Monitor (監視) > PDF Reports (PDF レポート) > Manage PDF Summary (PDF サマリーの管理)」を参照してください。
	• PDF Report Footer(PDF レポート フッター)のイメージ

機能	の意味	
	<u>گ</u>	Upload
	(<image/>)イメージファイル を 前にアップロードしたイメージをプレビューまたは削除 (以)
	します。	
	デフォルトのロゴに戻るには、エントリを削除して Commit (コ ミット)します。	
	Login Screen (ログイン画面) と Main UI (メ イン UI) では、表示されるイメージを表示 (できます。必要であれば、ファイアウォールはイメージを収縮させ て収まるようにします。PDF レポートの場合、ファイアウォールは イメージを切り取らずに自動的にサイズ変更します。すべてのケー スにおいて、プレビューは推奨されるイメージのサイズを表示しま す。) ± t
	任意のロゴイメージの最大サイズは、128KB です。サポートさ れるファイルの種類は png と jpg です。インターレースされたイ メージファイル、アルファチャネルを含むイメージ、および GIF ファイルの種類は PDF レポートの生成に干渉するため、ファイア ウォールはサポートしていません。そのイメージの作成者に連絡し てアルファチャンネルの削除を依頼するか、使用するグラフィック スソフトウェアでアルファチャンネル機能を含めずにファイルを保 存してください。	<i>,</i> , ,
	PDF レポートの生成方法の詳細は、「Monitor(監視) > PDF Reports(PDF レポート) > Manage PDF Summary(PDF サマリー の管理)」を参照してください。	
SNMP のセットアップ	SNMP モニタリングを有効化します。	
ストレージパー ティションの設定 (<mark>Panorama のみ</mark>)	レガシー モードの Panorama バーチャル アプライアンスのログス トレージ パーティション。	

SNMP モニタリングの有効化

• Device > Setup > Operations [デバイス > セットアップ > 操作]

SNMP (Simple Network Management Protocol) は、ネットワーク上のデバイスをモニターする 標準プロトコルです。SNMPマネージャでサポートされているSNMPバージョン(SNMPv2cま たはSNMPv3)を使用するようにファイアウォールを設定する場合は、Operations [操作] ペー ジを使用します。ファイアウォールから収集される統計情報を解釈できるように SNMP マネー ジャにロードする必要のある MIB のリストは『サポートされる MIB 』』を参照してください。 ネットワーク上の SNMP トラップ の宛先と通信するファイアウォールを有効にするサーバー プロファイルを設定するには、「Device(デバイス) > Server Profiles(サーバー プロファイ ル) > SNMP Trap(SNMP トラップ)」を参照してください。SNMP MIB は、ファイアウォー ルが生成するすべての SNMP トラップを定義します。SNMP トラップは一意のオブジェクト ID (OID)を識別し、個々のフィールドは変数バインド (varbind) リストとして定義されます。SNMP Setup(SNMP のセットアップ)をクリックし、以下の設定を指定して SNMP マネージャからの SNMP GET 要求を許可します。

項目	の意味
場所	ファイアウォールの物理的な場所を指定します。ログまたはトラップ が生成された場合、この情報により、通知を生成したファイアウォー ルをSNMPマネージャで識別することができます。
お問い合わせ	ファイアウォールの管理者の名前や電子メール アドレスを入力しま す。この設定は、標準システム情報の MIB でレポートされます。
イベント固有のト ラップ定義を使用	このオプションはデフォルトで選択されており、ファイアウォー ルは、それぞれのSNMPトラップのイベントタイプに基づいた一意 のOIDを使用します。このオプションをオフにすると、すべてのト ラップのOIDが同じになります。
バージョン	SNMPバージョンを選択します。 V2c (デフォルト)または V3 。この 選択内容により、ダイアログに表示される残りのフィールドが決まり ます。

SNMP V2c の場合

SNMP コミュニティ 名	コミュニティ文字列を入力します。コミュニティ文字列は、SNMPマ ネージャおよびモニター対象デバイスの SNMP コミュニティを識別 し、SNMP GET (統計情報要求) やトラップ メッセージを交換すると きにコミュニティ メンバーを相互認証するためのパスワードとして機 能します。コミュニティ文字列には最大 127 文字を含めることができ ます。また、すべての文字を使用でき、大文字と小文字が区別されま す。
	 デフォルトのコミュニティ文字列 public は使用しないでください。SNMPメッセージにはクリア テキストのコミュニティ文字列が含まれているため、コミュニティメンバーシップ(管理者アクセス)を定義するときにネットワークのセキュリティ要件を考慮してください。

名前/表示	1つ以上のビューのグループをSNMPマネージャのユーザーに割り当 てて、ユーザーがファイアウォールから取得できるMIBオブジェクト

SNMP V3 の場合

項目	の意味
	(統計情報)を制御できます。各ビューは、ペアになっている OID と ビット単位のマスクです。OID で MIB を指定し、マスク (16 進数形 式) で、その MIB 内 (一致部分を含む) または MIB 外 (一致部分を含ま ない) でアクセスできるオブジェクトを指定します。
	たとえば、OID が 1.3.6.1、照合の Option[オプション] が include[包 含]、Mask[マスク] が 0xf0 の場合、ユーザーが要求するオブジェ クトの OID の最初の 4 つのノード (f = 1111) が 1.3.6.1 に一致して いる必要があります。オブジェクトの残りのノードは一致している 必要はありません。この例の場合、1.3.6.1.2 はマスクに一致します が、1.4.6.1.2 は一致しません。
	ビューのグループごとに Add[追加] をクリックし、グループの Name[名前] を入力します。次に、グループに Add[追加] するビューご とに以下を設定します。
	 View[表示] – ビューの名前を指定します。名前には、最大 31 文字 (英数字、ピリオド、アンダースコア、またはハイフン)を含めるこ とができます。
	 OID – MIB の OID を指定します。
	● Option [オプション] − MIB に適用する照合ロジックを選択します。
	 Mask[マスク] – 16 進数形式のマスクを指定します。
	すべての管理情報にアクセスできるようにするには、最 上位 OID 1.3.6.1 を使用し、Mask[マスク] を 0xf0 に設定 して、照合の Option[オプション] を include[包含] に指定 します。
Users	SNMPユーザーアカウントにより、ファイアウォールがトラップを転送するときやSNMPマネージャがファイアウォールの統計情報を取得する際に、認証、プライバシー、およびアクセス制御を行うことができます。ユーザーごとに、Add[追加]をクリックして以下の設定を指定します。
	 Users[ユーザー] – SNMP ユーザー アカウントを識別するユー ザー名を指定します。ファイアウォールで設定するユーザー名 は、SNMPマネージャで設定したユーザー名と一致する必要があり ます。ユーザー名には最大 31 文字を使用できます。
	• View[表示] – ユーザーにビューのグループを割り当てます。
	 Auth Password[認証パスワード] – ユーザーの認証パスワードを指定します。ファイアウォールは、トラップの転送時や統計情報要求に応答する際に、このパスワードを使用してSNMPマネージャの認証を受けます。パスワードには、8~256文字のあらゆる文字を使用できます。

項目	の意味
	 Priv Password[専用パスワード] – ユーザーの専用パスワードを指定します。パスワードには、8~256 文字のあらゆる文字を使用できます。
	 認証プロトコル:ファイアウォールはセキュア ハッシュ アルゴリズム (SHA) を使用してパスワードをハッシュします。
	• SHA-1, SHA-224, SHA-256, SHA-384, SHA-512
	 プライバシー プロトコル:ファイアウォールは、パスワードと高度 な暗号化標準 (AES) アルゴリズムを使用して、SNMP トラップと統 計情報要求への応答を暗号化します。
	• AES-128 , AES-192 , AES-256

Device > Setup > HSM [デバイス > セットアップ > HSM]

ハードウェア セキュリティ モジュール(HSM)を設定し、操作を実行し、HSM の状態を表示 するには、Device(デバイス) > Setup(セットアップ) > HSM を選択します。

確認すべき情報	以下を参照
ハードウェア セキュリティ モ ジュール(HSM)の目的と、 設定手順の詳細を確認できる 場所は?	ハードウェア セキュリティ モジュールによるキーの安全確 保 [┏]
設定:	ハードウェア セキュリティ モジュール プロバイダ設定
	HSM 認証
ハードウェア セキュリティ操 作の実行	ハードウェア セキュリティ操作
HSM の状態を表示する方法 は?	ハードウェア セキュリティ モジュール プロバイダ設定およ び状態
	ハードウェア セキュリティ モジュール状態

ハードウェア セキュリティ モジュール プロバイダ設定

ファイアウォールにハードウェアセキュリティモジュール(HSM)を設定する場合は、ハード ウェアセキュリティモジュールプロバイダの設定を編集します。

ハードウェア セキュ リティ モジュール プ ロバイダ設定	の意味
プロバイダが設定さ れました	HSM ベンダーを選択します。
	 None(なし)(デフォルト)-ファイアウォールはどの HSM に も接続しません。
	SafeNet Network HSM
	● Thales CipherTrust・マネージャー HSM
	nCipher nShield Connect
	HSM サーバー バージョンは、ファイアウォールの HSM client version(HSM クライアント バージョン)

デバイス

ハードウェア セキュ リティ モジュール プ ロバイダ設定	の意味
	■ と 互換性がある必要があります。
モジュール名	HSM のモジュール名を追加します。31 文字以下の任意の ASCII 文字 列を指定できます。独立または高可用性の SafeNet HSM 設定を構成 する場合は、最大 16 のモジュール名を追加できます。
サーバー アドレス	設定するすべての HSM の IPv4 アドレスを指定します。
HA (SafeNet Network のみ)	(任意)高可用性設定で SafeNet HSM モジュールを設定する場合は このオプションを選択します。各 HSM モジュールのモジュール名と サーバー アドレスを設定する必要があります。
自動回復の再試行 (SafeNet Network のみ)	ファイアウォールが HSM への接続の回復を試行する回数を指定し ます(範囲は 0 ~ 500、デフォルトは 0)。この試行回数に達する と、HSM HA 性設定内の別の HSM にフェイルオーバーします。
高可用性グループ名 (SafeNet Network のみ)	HSM HA グループで使用されるグループ名を指定します。この名前 はファイアウォールの内部で使用されます。31 文字以下の任意の ASCII 文字列を指定できます。
ファイルシステムの アドレスの削除 (nCipher nShield Connect のみ)	nShield Connect HSM 設定で使用されるリモート ファイルシステムのIPv4アドレスを設定します。

HSM 認証

「ハードウェアセキュリティモジュールのセットアップ」を選択し、ファイアウォールを nCipher nShield Connect および SafeNet ネットワーク HSM に認証するための次の設定を行いま す。

HSM モジュール認証	
サーバー名	ドロップダウンで HSM サーバー名を選択して、自動または手動生成 された証明書を使用して認証および信頼を確立するかどうかを選択し ます。 • 自動

HSM モジュール認証		
	•	手動
		Manual(手動)を選択した場合、HSM サーバーが手動で生成した 証明書をインポートしてインストールする必要があります。HSM クライアント証明書をエクスポートして HSM サーバーにインス トールします。
管理者パスワード	H: ワ	SM に対するファイアウォールの認証を行う HSM の管理者パス ードを入力します。

「HSM 接続アカウントのセットアップ」を選択し、以下の設定を行って Thales CipherTrust Manager HSM に対してファイアウォールを認証します。HSM の暗号ユーザーを認証するに は、「HSM 暗号ユーザーアカウントの設定」を選択します。

HSM モジュール認証	
サーバー名	ドロップダウンリストからHSMサーバー名を選択します。この名前 は、ファイアウォールの HSM プロバイダーを選択したときに入力し た名前と一致する必要があります。
証明書をインポート する	認証用にインポートする証明書を選択します。 • HSM サーバー CA 証明書 • HSM クライアント証明書 • HSM クライアントプライベートキー

HSM アカウント	
username	HSM アカウントのユーザー名を入力します。
パスワード	HSM アカウントのパスワードを入力します。

ハードウェア セキュリティ操作

Hardware Security Module (ハードウェアセキュリティモジュール) (HSM)または HSM に接続 されたファイアウォールで操作を実行するには、Device (デバイス) > Setup (セットアップ) > HSM を選択し、次のハードウェア セキュリティ操作のいずれかを選択します。

ハードウェア セキュリティ操作	
ハードウェアセキュリティ モジュールのセットアッ	HSM を認証するようにファイアウォールを設定します。

ハードウェア セキュリティ操作	
プ(nCipher nShield Connectお よびSafeNetネットワーク)	
HSM 接続アカウントの設定 (Thales CipherTrust マネー ジャーのみ)	Thales CipherTrust Manager HSM で認証するようにファイ アウォールを設定します。必要な認証証明書をインポート するために使用します。
HSM 接続の再起動 (Thales CipherTrust マネージャーのみ)	PAN-OS の状態を更新し、古い証明書を削除して新しい証 明書を追加します。
HSM 暗号ユーザーアカウント の設定 (Thales CipherTrust マ ネージャーのみ)	Thales CipherTrust マネージャーサーバーで定義されたユー ザーアカウントに接続するようにユーザーアカウントを設 定します。
詳細情報を表示	HSM サーバー、HSM 高可用性ステータス、および HSM ハードウェアに関する情報を表示します。
Remote Filesystem (リモート ファイルシステム) と同期する (nCipher nShield Connect のみ)	nShield Connect リモート ファイルシステムからファイア ウォールにキー データを同期します。
構成のリセット (nCipher nShield Connectおよ びSafeNetネットワーク)	ファイアウォールへのすべての HSM 接続を削除しま す。HSM 設定をリセットした後、すべての認証手順を繰り 返す必要があります。
HSM クライアントのバージョ ンを選択する(SafeNet ネット ワークのみ)	HSM クライアント(ファイアウォール)上で実行されてい るソフトウェアのバージョンを選択できます。HSM サー バー クライアントのバージョンは、ファイアウォールの HSM サーバー バージョンと互換性がある必要があります。 クライアント サーバー バージョンの互換性マトリックスに ついては、HSM ベンダーのドキュメントを参照してください。
HSM 構成のクリア (Thales CipherTrust マネージャーのみ)	HSM 設定に関連する接続、証明書、およびユーザーを削除 します。設定をクリアした後、HSM プロバイダーを [None (なし)] に切り替えて削除を完了します。

ハードウェア セキュリティ モジュール プロバイダ設定および状 態

Hardware Security Module Provider(ハードウェア セキュリティ モジュールの詳細)セクションには、HSM 設定および HSM の接続状態が表示されます。

Hardware Security Module Details ハードウェア セキュリティ モジュールの詳細		
プロバイダが設定さ れました	ファイアウォールで設定されている HSM ベンダーを選択します。 • なし • SafeNet Network HSM • Thales CipherTrust・マネージャー HSM • nCipher nShield Connect	
НА	(<mark>SafeNet Network のみ</mark>)オンにすると、HSM 高可用性が設定され ます。	
高可用性グループ名	(<mark>SafeNet Network のみ</mark>)ファイアウォールに設定される HSM 高可 用性のグループ名。	
リモート ファイルシ ステムのアドレス	(nShield Connect のみ) リモート ファイルシステムのアドレス。	
ファイアウォール送 信元アドレス	HSM サービスに使用されるポートのアドレス。デフォルトでは、こ のアドレスには管理ポート アドレスが設定されます。Device(デバ イス) > Setup(セットアップ) > Services(サービス)の Services Route Configuration(サービス ルートの設定)を使用して、別の ポートを指定できます。	
HSM Client Version on Firewall ファイ アウォールの HSM クライアントのバー ジョン	インストール済の HSM クライアントのバージョンを表示します。	
HSM が保護するマス ター キー	オンにした場合、HSM でマスター キーが保護されます。	
ステータス	ファイアウォールが接続されて HSM に認証されている場合は緑で 表示されます。ファイアウォールが認証されていない場合、または HSM へのネットワーク接続がダウンしている場合は赤で表示されま す。 HSM 接続の詳細は、「ハードウェア セキュリティ モジュール状態」 を参照してください。	

ハードウェア セキュリティ モジュール状態

Hardware Security Module Status(ハードウェア セキュリティ モジュール状態)には、認証に成功 した HSMs に関する以下の情報が含まれます。表示は設定された HSM プロバイダによって異な ります。

ハードウェア セキュリティ モジュール状態		
SafeNet Network HSM	 Serial Number(シリアル番号) – HSM パーティションが正常に 認証された場合、その HSM パーティションのシリアル番号が表示 されます。 	
	 Partition(パーティション) – ファイアウォールで割り当てられた HSM のパーティション名。 	
	 Module State(モジュール状態) – HSM 接続の現在の動作状態。HSM がこの表に表示されている場合、このフィールドにはAuthenticated(認証済み)と表示されます。 	
nCipher nShield	● Name(名前) – HSM のサーバー名。	
Connect HSM	 IP address(IP アドレス) – ファイアウォールで割り当てられた HSMのIP アドレス。 	
	 Module State(モジュール状態) – HSM 接続の現在の動作状態。 ファイアウォールが HSM に正常に認証された場合、この設定には Authenticated(認証済み)と表示されます。認証が失敗した場合 は、Not Authenticated(認証されていません)と表示されます。 	
Thales CipherTrust •	● Name(名前) – HSM のサーバー名。	
マネージャー HSM	 IP address(IP アドレス) – ファイアウォールで割り当てられた HSMのIP アドレス。 	
	 Module State(モジュール状態) – HSM 接続の現在の動作状態。 この設定は、ファイアウォールがHSMへの認証に成功した場合に 「Reachable (到達可能)」と表示されます。 	

Device > Setup > Services [デバイス > セットアップ > サービス]

以下のトピックでは、ファイアウォールにおけるグローバルおよび仮想システムのサービス設定 について説明します。

- グローバルおよび仮想システムのサービスの設定
- グローバル サービス設定
- サービス ルートの設定での IPv4 および IPv6 のサポート
- 宛先サービス ルート

グローバルおよび仮想システムのサービスの設定

マルチ仮想システムが有効になっているファイアウォールにおいて、効率的な動作のためにファイアウォールまたはその仮想システムが使用するサービスを設定する際に、それ ぞれ Global (グローバル)タブと Virtual Systems (仮想システム)タブを表示する場合 は、Services (サービス)を選択します。(ファイアウォールが1つの仮想システムの場合、ま たはマルチ仮想システムが無効になっている場合、Virtual Systems (仮想システム)タブは表示 されません)。

ファイアウォール全体のサービスを設定する場合は、Global [グローバル] タブを使用します。これらの設定は、サービスの設定がカスタマイズされていない仮想システムのデフォルト値としても使用されます。

- DNS サーバー、更新サーバー、プロキシサーバーのそれぞれの宛先 IP アドレスを定義する場合は Services (サービス)を編集します。専用のNTPタブを使用して、Network Time Protocol設定を編集します。Service (サービス)で使用可能なオプションのフィールドに関する説明については、表 12 を参照してください。
- DNS、電子メール、LDAP、RADIUS、Syslogなどのサービスを提供する際の、ファイア ウォールと他のサーバー/デバイス間の通信方法を指定する場合は、Service Features [サー ビス機能] から、Service Route Configuration [サービスルートの設定] をクリックします。グ ローバル サービス ルートを設定するには、以下の2つの方法があります。
 - Use Management Interface for all [すべてに管理インターフェイスを使用] オプションでは、外部サーバーとのファイアウォールサービス通信はすべて強制的に管理インターフェイス (MGT) を使用して行われます。このオプションを選択する場合、ファイアウォールとサービスを提供するサーバーまたはデバイスとの間の通信を許可するように MGT インターフェイスを設定する必要があります。MGT インターフェイスを設定する場合は、Device(デバイス) > Setup(セットアップ) > Management(管理)を開き、設定を編集します。
 - Customize[カスタマイズ]オプションでは、サービスが応答時に宛先インターフェイス および宛先 IP アドレスとして使用する、特定の送信元インターフェイスおよび送信元 IP アドレスを設定することで、サービス通信を詳細に制御できます。(たとえば、ファ イアウォールと電子メールサーバー間のすべての電子メール通信に使用する特定の送信 元 IP/インターフェイスを設定し、Palo Alto Networks サービスには別の送信元 IP/イン

ターフェイスを使用できます)。同じ設定にカスタマイズする1つ以上のサービスを選 択し、Set Selected Service Routes[選択されたサービスルートの設定] をクリックしま す。サービスは表13に記載されています。この表では、サービスが Global(グローバ ル)ファイアウォールまたは Virtual Systems(仮想システム)用に設定できるかどうか、 およびサービスで IPv4/IPv6 の送信元アドレスがサポートされているかどうかがわかりま す。

Destination[宛先] タブは、カスタマイズ可能な別のグローバル サービス ルート機能です。これ は、Service Route Configuration(サービス ルートの設定)ウィンドウに表示されます。「宛先 サービス ルート」を参照してください。

1つの仮想システムのサービス ルートを指定するには、Virtual Systems[仮想システム] タブを使用します。場所 (仮想システム) を選択し、Service Route Configuration[サービス ルートの設定] をクリックします。Inherit Global Service Route Configuration (グローバル サービス ルート設定の継承)を選択するか、仮想システムのサービス ルートを Customize (カスタマイズ) します。設定をカスタマイズする場合、IPv4 または IPv6 を選択します。同じ設定にカスタマイズする 1 つ以上のサービスを選択し、Set Selected Service Routes[選択されたサービス ルートの設定] をクリックします。カスタマイズ可能なサービスは、表 13 を参照してください。

共有仮想マシンと特定の仮想システム間の DNS クエリを制御およびリダイレクトするため に、DNS プロキシおよび DNS サーバー プロファイルを使用できます。

グローバル サービス設定

• Device > Setup > Services [デバイス > セットアップ > サービス]

共有仮想マシンと特定の仮想システム間の DNS クエリを制御およびリダイレクトするため に、DNS プロキシおよび DNS サーバー プロファイルを使用できます。

グローバル サー ビス設定	の意味
本サービス	
更新サーバー	Palo Alto Networks から更新ファイルをダウンロードする サーバーの IP アドレスまたはホスト名を表します。現在値 は、updates.paloaltonetworks.com です。テクニカル サポートから指示が ない限り、この設定は変更しないでください。
更新サーバー ID の確認	このオプションを有効にすると場合、信頼された機関によって署名された SSL 証明書がソフトウェアまたはコンテンツパッケージのダウンロード 元のサーバーにあるかどうかをファイアウォールまたは Panorama が確認 します。これにより、ファイアウォールまたは Panorama サーバーと更新 サーバー間の通信に新たなレベルのセキュリティを追加します。 更新サーバーの身元を検証し、信頼できる機関が署名した SSL 証明書をサーバーが持っていることを確認します。

グローバル サー ビス設定	の意味
DNS 設定	ファイアウォールが FQDN アドレスオブジェクト、ログ、およびファイア ウォール管理をサポートするために開始するすべての DNS クエリに対し て、DNS サービスのタイプを選択します。
	 Servers (サーバ)ードメイン名を解決するプライマリおよびセカンダリ DNS サーバー。
	 [DNS Proxy Object (DNS プロキシ オブジェクト)] –ファイアウォー ルに設定されている DNS プロキシを選択するか、新しい DNS プロキシ を作成してドメイン名解決を行います。DNS プロキシを有効にする場 合は、Cache (キャッシュ) および EDNS Cache Responses (EDNS キャッ シュ応答) (Network > DNS Proxy (DNS プロキシ) > Advanced (詳細)) を 有効にする必要があります。
プライマ リDNSサー バー	[Servers (サーバー)] を選択した場合は、ファイアウォールからの DNS クエリのプライマリ DNS サーバーの IP アドレスを入力します。たとえ ば、更新サーバーを検索し、ログの DNS エントリを解決したり、FDQN ベースのアドレス オブジェクトを解決したりする場合などです。
セカンダリ DNS サーバー	(<u>任意</u>) [Servers (サーバー)] を選択した場合は、プライマリ サーバーを 使用できない場合に使用するセカンダリ DNS サーバーの IP アドレスを入 力します。
最低 FQDN 更 新時間(秒単 位)	 ファイアウォールが DNS から受信する FQDN を更新する頻度の限界を設定します。TTL がこのMinimum FQDN Refresh Time (最低 FQDN 更新時間)(秒単位)以上である間、ファイアウォールは FQDN の TTL に基づいて FQDN を更新します。TTL がこの Minimum FQDN Refresh Time (最低 FQDN 更新時間)未満である場合、ファイアウォールはこの Minimum FQDN Refresh Time (最低 FQDN 更新時間)に基づいて FQDN を更新します (つまり、ファイアウォールはこの設定よりも速い TTL を受け付けません)。ファイアウォールが FQDN を解決する DNS サーバーまたは DNS プロキシ オブジェクトから DNS 応答を受信すると、タイマーが開始されます (範囲は 0 ~ 14,400、デフォルトは 30)。0に設定すると、ファイアウォールが DNS 内の TTL の値に基づいて FQDN を更新し、最低 FQDN 更新時間を適用しなくなります。 ONS 内の FQDN の TTL が短く、しかし FQDN の解決が TTL の期間ほど頻繁に変わらず、高速な更新が不要である場合、最低の FQDN Refresh Time (FQDN 更新時間)を設定して不要な FODN の更新を試みたいとうにする必要があります
_{占い FQDN} エ ントリのタイム アウト(分)	ネットワークのエフーか発生したり DNS サーバーに到達できなかったり する場合(FQDN が更新を受け取っていない場合)にファイアウォール が古い FQDN 解決を使用し続ける期間(分単位)を指定します(範囲は

グローバル サー ビス設定	の意味
	0~10,080、デフォルトは 1,440)。値を 0 にすると、ファイアウォールが 古いエントリを使用し続けなくなります。このタイムアウトを過ぎてもま だ DNS サーバーに到達できない場合。FODN のエントリが解決不能にな
	ります(古い解決が削除されます)。
	
	できるよう十分長くしてください。

プロキシ サーバーセクション

SERVER	ファイアウォールがプロキシサーバーを使用して Palo Alto Networks 更新 サービスにアクセスする必要がある場合は、プロキシ サーバーの IP アドレ スまたはホスト名を入力します。
ポート	プロキシ サーバーのポートを入力します。
感染	プロキシ サーバーにアクセスするときに管理者が入力するユーザー名を入 力します。
パスワード/再 入力 パスワー ド	プロキシ サーバーにアクセスするときに管理者が入力するパスワードを入 力して確認します。
Use proxy to send logs to Cortex Data Lake Cortex Data Lake への ログの送信にプ ロキシを使用す る	ファイアウォールのプロキシ サーバー経由での CortexDataLake へのログ 送信を有効化します。
NTP	
NTP サーバー アドレス	ファイアウォールのクロックを同期するために使用する NTP サーバーの IP アドレスまたはホスト名を入力します。プライマリ サーバーが使用不能に なった場合、ファイアウォールのクロック同期に使用するセカンダリ NTP サーバーの IP アドレスまたはホスト名を入力します。(任意)

グローバル サー ビス設定	の意味
	 NTP サーバーがすべてのネットワークのファイアウォールの クロックを同期させる際、予定中のジョブが通常通りに実行 され、また複数のデバイスが関わる問題の根本原因を特定す るためにタイムスタンプを活用できます。プライマリ NTP サーバーに到達できない場合に備えてプライマリおよびセカ ンダリ NTP サーバーを設定します。
認証タイプ	NTP サーバーからの日時更新をファイアウォールが認証できるように指定 できます。NTP サーバーごとに、ファイアウォールで使用する認証のタイ プを選択します。
	 None(なし)(デフォルト) – NTP 認証を無効にするにはこのオプションを選択します。
	 Symmetric Key(対称キー) – ファイアウォールで対称キー交換(共 有秘密)を使用して NTP サーバーからの日時更新を認証するには、こ のオプションを選択します。Symmetric Key(対称キー)を選択した場 合、続けて次の値を指定します。
	• Key ID(キーID) – キーID(1~65534)を入力します。
	 Algorithm(アルゴリズム) –NTP 認証に使用する MD5 アルゴリズ ムまたは SHA1 アルゴリズムを選択します。
	 Authentication Key/Confirm Authentication Key(認証キー/再入力 認証キー) – 認証アルゴリズムの認証キーを入力し、確認します。
	 Autokey(自動キー) – ファイアウォールで自動キー(公開鍵暗号化) を使用して NTP サーバーからの日時更新を認証するには、このオプ ションを選択します。
	NTP サーバー認証を有効化し、NTP サーバーがクライアント を承認して同期された更新を提供できるようにします。

サービス ルートの設定での IPv4 および IPv6 のサポート

次の表は、グローバル システムと仮想システムの IPv4 と IPv6 でサービス ルート設定がサポートされるかどうかを示しています。

サービス ルートの設定	Global		仮想シス テム (vsys)	
	IPv4	IPv6	IPv4	IPv6
AutoFocus-AutoFocus [™] サーバー。	1	_	_	_

サービス ルートの設定	Global		仮想シス テム (vsys)	
	IPv4	IPv6	IPv4	IPv6
CRL ステータス – 証明書失効リスト (CRL) サーバー。	~	~	_	_
データサービス:ファイアウォール データ プレーンから Palo Alto Networks クラウド サービスにデータを送信します。データ転 送を高速化し、データ損失を防ぐために最 適化されています。 IoT セキュリティ、エンタープライズ DLP、および SaaS セキュリティに必要で す。	~	~	~	~
		~		
Panorama によってプッシュされる更新 – Panorama [™] からデプロイされるコンテン ツ更新とソフトウェア更新。	~	~	_	_
DNS –Domain Name System サーバー。 * 仮想システムの場合、DNS は DNS サー バー プロファイルで実行されます。	1	~	✓ *	✓ *
外部動的リスト – 外部動的リストの更新。	1	1	_	_
電子メールー電子メール サーバー。	1	1	1	1
HSM-ハードウェア セキュリティ モ ジュール サーバー。	1	_	_	~
HTTP-HTTP 転送。	~	~	~	~
Kerberos-Kerberos 認証サーバー。	1	_	1	~
LDAP — Lightweight Directory Access Protocol サーバー。	1	1	1	
MDM-モバイル デバイス管理サーバー。	~	~	_	_
多要素認証 – 多要素認証(MFA)サー バー。	~	~	~	~

サービス ルートの設定	Global		仮想シス テム (vsys)	
	IPv4	IPv6	IPv4	IPv6
NetFlow – ネットワーク トラフィック統計 情報を収集する NetFlow。	~	~	~	1
NTP -Network Time Protocol サーバー。	~	~	_	_
Palo Alto Networks サービス – Palo Alto Networks [®] およびパブリック WildFire [®] サーバーからの更新。pre-10.0 telemetry data (10.0 以前のテレメトリ データ) を Palo Alto Networks に転送するサービス ルートでもあります。(現在のテレメトリ サポートでは、データを Cortex Data Lake に転送します。この場合、上記サービス ルートは使用されません。)	1	_	_	_
Panorama-Panorama 管理サーバー。	1	1	_	_
Panorama ログ転送 – (PA-5200 シリーズ ファイアウォールのみ)ファイアウォール からログ コレクタへのログ転送。	~	~	_	_
プロキシ – ファイアウォールへのプロキシ として機能するサーバー。	~	~	_	_
RADIUS – Remote Authentication Dial-in User Service サーバー。	1	~	~	~
SCEP – クライアント証明書の要求およ び配信用Simple Certificate Enrollment Protocol。	~	~	~	_
SNMP トラップ – Simple Network Management Protocol トラップ サーバー。	~	_	~	_
Syslog – システム メッセージ ログ用の サーバー。	1	~	~	~
TACACS+ – 認証、認可、課金(AAA) サービスを行う Terminal Access Controller Access-Control System Plus(TACACS+) サーバー。	1	~	~	1

サービス ルートの設定	Global		仮想シス テム (vsys)	
	IPv4	IPv6	IPv4	IPv6
UID Agent – User-ID エージェント サー バー。	~	~	-	~
URL Updates — Uniform Resource Locator (URL) 更新サーバー。	~	~	_	_
す。Device(デバイス)>(情報ソー ス).が有効にする VM モニター–フィル タを適用してテーブルの出力をカスタマイ ズし、必要な列のみを含めることができま す。	1	1	1	~
 仮想マシンを監視しているパブリッククラウド展開のVMシリーズファイアウォールは、MGTインターフェイスを使用する必要があります。エクスポートダイアログに表示される列のみがエクスポートされます。 				
Wildfire Private ー プライベート Palo Alto Networks WildFire サーバー。	~	_	_	_

Global (グローバル) サービス ルートをカスタマイズする場合は、Service Route Configuration (サービス ルート設定) を選択し、IPv4 または IPv6 タブで、利用可能なサー ビスのリストからサービスを選択します。複数のサービス ルートを設定して、Set Selected Service Routes (選択したサービス ルート)を設定して、複数のサービス ルートを同時に設 定することもできます。ドロップダウン リストでSource Address(送信元アドレス)の選択 内容を制限するには、Source Interface(送信元インターフェイス)を選択してから Source Address(送信元アドレス)を選択します。Any(いずれか)に設定された送信元インター フェイスの場合、使用可能なインターフェイスの中から任意の送信元アドレスを選択できま す。Source Address(送信元アドレス)には、選択したインターフェイスに割り当てられている IPv4 または IPv6 アドレスが表示されます。選択した IP アドレスは、サービス トラフィックの 送信元になります。ファイアウォールでサービスルートの管理インターフェイスを使用する場合 は、Use default(デフォルトを使用)できます。 ただし、パケットの宛先IPアドレスが設定さ れた宛先IPアドレスと一致する場合、送信元IPアドレスは宛先に設定された送信元アドレスに設 定されます。宛先は各サービスを設定するときに設定されるため、宛先アドレスを定義する必要 はありません。たとえば、Device(デバイス) > Setup(設定) > Services(サービス)で DNS サーバーを定義すると、DNS クエリの宛先が設定されます。サービスに IPv4 と IPv6 の両方の アドレスを指定できます。

Global (グローバル) サービス ルートをカスタマイズするもう1つの方法は、Service Route Configuration (サービス ルート設定) 選んでから Destination (宛先) を選択することです。 受信パケットが比較される Destination (宛先) IP アドレスを指定します。パケットの宛先ア ドレスが設定済みの宛先 IP アドレスと一致する場合、送信元 IP アドレスは宛先に設定された送 信元アドレスに設定されます。ドロップダウン リストでSource Address (送信元アドレス) の 選択内容を制限するには、Source Interface (送信元インターフェイス) を選択してから Source Address (送信元アドレス) を選択します。Any [いずれか] に設定された送信元インターフェイ スの場合、使用可能なインターフェイスの中から任意の送信元アドレスを選択できます。MGT ソース インターフェイスを選択すると、ファイアウォールはサービスルートに MGT インター フェイスを使用します。

Virtual System (仮想システム) のサービス ルートを設定する場合、Inherit Global Service Route Configuration (グローバルサービスルート設定の継承)を選択すると、仮想システムの すべてのサービスがグローバルサービスルート設定を継承します。あるいは、Customize(カスタ マイズ)を選択し、IPv4 または IPv6 を選択して、サービスを選択します。また、複数のサービ スと Set Selected Service Routes (選択したサービス ルートを選択する)を選択することもでき ます。Source Interface[送信元インターフェイス] には、以下の3つの選択肢があります。

- Inherit Global Setting(グローバル設定の継承) 選択したサービスがこれらのサービスの グローバル設定を継承します。
- Any[いずれか] 使用可能な任意のインターフェイス (特定の仮想システムのインターフェイス) から送信元アドレスを選択できます。
- ドロップダウンリストからのインターフェイス-Source Address(送信元アドレス)のドロップダウンをこのインターフェイスの IP アドレスに制限します。

Source Address[送信元アドレス] の場合、ドロップダウンリストからアドレスを選択します。 サービスが選択されている場合、サーバーの応答がこの送信元アドレスに送信されます。

宛先サービス ルート

• Device > Setup > Services > Global [デバイス > セットアップ > サービス > グローバル]

Global (グローバル) タブで、Service Route Configuration (サービス ルートの設定)、Customize (カスタマイズ)の順にクリックすると、Destination (宛先) タブが表示されます。宛先サービス ルートは、(Virtual Systems[仮想システム] タブではなく) Global[グローバル] タブでしか使用できないため、個々の仮想システムのサービス ルートは、その仮想システム に関連付けられていないルート テーブル エントリをオーバーライドできません。

宛先サービス ルートを使用して、サービスの Customize(カスタマイズ)リストでサポートされていない、カスタマイズされたサービスのリダイレクトを追加できます。宛先サービス ルートは、転送情報ベース (FIB) ルート テーブルをオーバーライドするようにルーティングをセットアップする方法です。宛先サービス ルートの設定は、ルート テーブル エントリをオーバーライドします。これらは、サービスに関連している場合もあれば、関連していない場合もあります。

以下のような場合に Destination[宛先] タブを使用します。

- サービスにアプリケーションサービスルートがない場合。
- 1つの仮想システム内で、複数の仮想ルーター、または仮想ルーターと管理ポートの組み合わせを使用する場合。

宛先サービス ルートの設定	の意味
宛先	Destination[宛先]のIPアドレスを入力します。このアドレスと一致する宛先アドレスを持つ着信パケットは、このサービスルートに指定したSource Address(発信元アドレス)を発信元として使用します。
送信元インターフェイス	Source Address(送信元アドレス)のドロップダウンを 制限するには、Source Interface(送信元インターフェイ ス)を選択します。Any(すべて)を選択すると、Source Address(送信元アドレス)のドロップダウンですべての インターフェイス上のすべての IP アドレスを使用できるよ うになります。MGT を選択すると、ファイアウォールは サービスルートに MGT インターフェイスを使用します。
送信元アドレス	サービスルートの Source Address(送信元アドレス)を選 択します。 このアドレスは宛先から戻ってくるパケットに 使用されます。宛先アドレスのサブネットは入力する必要 がありません。

Device(デバイス) > Setup(セットアップ) > Interfaces(インターフェイス)

このページを使用して、すべてのファイアウォール モデルの管理(MGT)インターフェイスと PA-5200 シリーズ ファイアウォールの補助インターフェイス(AUX-1 および AUX-2)の接続、 許可されるサービス、および管理アクセスを設定します。

インターフェイスごとに IP アドレス、ネットマスク(IPv4)、またはプレフィックス長 (IPv6)、およびデフォルト ゲートウェイを常に指定することをお勧めします。MGT インター フェイスに関するこれらの設定のいずれか(たとえば、デフォルト ゲートウェイ)を省略した 場合、今後の設定変更でファイアウォールにアクセスできるのは、コンソール ポートからのみ になります。

M-500 アプライアンス、あるいは Panorama バーチャル アプライアンスの MGT イ ンターフェイスを設定するには、「Panorama > Setup (セットアップ) > Interfaces (インターフェイス)」を参照してください。

MGT インターフェイスの代わりにループバック インターフェイスを使用してファ イアウォールを管理できます(「Network(ネットワーク) > Interfaces(インター フェイス) > Loopback(ループバック)」を参照)。

項目	の意味
IPv4 / IPv6 (MGT インターフェ イスのみ)	IPv4 または IPv6 を 選択します。
タイプ	IPv4の場合、[タイプ]で次のいずれかを選択します。
(MGT インターフェ イスのみ)	 Static (スタティック)-この表の下に記載されている IPv4 または IPv6 アドレス(またはその両方)とデフォルト ゲートウェイを手動 で入力します。 DHCP Client [DHCPクライアント] - ファイアウォール
	がDHCPサーバーを見つけるためにDHCP DiscoverまたはDHCP Requestメッセージを送信できるよう、MGTインターフェイス をDHCPクライアントとして設定します。これに対する応答とし て、サーバーはMGTインターフェイス用のIPアドレス(IPv4)、 ネットマスク(IPv4)、そしてデフォルトゲートウェイを提供 します。AWSおよびAzureにおけるVM-Seriesファイアウォール を除き、VM-Seriesファイアウォールでは管理インターフェイス のDHCPがデフォルトでオフになっています。DHCPクライアン トを選択する場合は、オプションで次のクライアントオプション のいずれかまたは両方を選択します。

項目	の意味
	 Send Hostname(ホスト名を送信) - MGT インターフェイス は、そのホスト名を DHCP オプション 12 の一部として DHCP サーバーに送信します。
	 Send Client Id(クライアント ID を送信) - MGT インターフェ イスは、そのクライアント識別子を DHCP オプション 61 の一 部として送信します。
	IPv6の場合は、 IPv6を有効化します。
	Type (種類) については次のいずれかを選択します。
	 [Static (スタティック)] – [IPv6 Address/Prefix Length] を手動 で入力します。この表の後半で説明します。
	 ダイナミック-オプションについては、この表の後半で説明します。
DHCP クライアント ランタイム情報の表 示	DHCP Client [DHCPクライアント] を選択した場合、任意でShow DHCP Client Runtime Info [DHCPクライアントランタイム情報を表 示] をクリックすると動的IPインターフェイスの状態を参照すること ができます。
	 インターフェイス - MGT インターフェイスを示します。
	• IPアドレス - インターフェイスのIPアドレスです。
	 ネットマスク - どのビットがネットワークまたはサブネットワー クで、どのビットがホストであるかを示す、IPアドレスのサブ ネットマスクです。
	 ゲートウェイ - MGTインターフェイスから出て行くトラフィック 用のデフォルトゲートウェイ。
	 プライマリ/セカンダリNTP - MGTインターフェイスが使用するNTPサーバーのIPアドレスを2つまで表示します。DHCPサーバーがNTPサーバーアドレスを返した場合、ファイアウォールはNTPサーバーアドレスを手動で設定していなかった場合のみそれらを認識します。NTPサーバーアドレスを手動で設定している場合、ファイアウォールがDHCPサーバーから送られてきたアドレスで上書きすることはありません。
	 リースタイム - そのDHCP IPアドレスが割り当てられている時間 (日/時間/分/秒)を表示します。
	 失効時間 - DHCPリースが無効となる年月日、時間/分/秒およびそのタイムゾーンを表示します。
	 DHCP サーバー - MGT インターフェイスの DHCP クライアントに 応答する DHCP サーバーの IP アドレスを表示します。
	 ドメイン - MGTインターフェイスが属するドメイン名を表示します。

項目	の意味
	 DNSサーバー - MGTインターフェイスが使用するDNSサーバーのIPアドレスを2つまで表示します。DHCPサーバーがDNSサーバーアドレスを返した場合、ファイアウォールはDNSサーバーアドレスを手動で設定していなかった場合のみそれらを認識します。DNSサーバーアドレスを手動で設定している場合、ファイアウォールがDHCPサーバーから送られてきたアドレスで上書きすることはありません。 必要に応じて、MGT インターフェイスに割り当てられた IP アドレスの DHCP リースを Renew (更新) することもできます。完了したら、ウィンドウをClose [閉じ]ます。
Λυν 1 / Λυν 2 <i>(</i>	補助インターフェイフを右効にするにけ、以下のいずれかのオ
Aux 17 Aux 2 (m 助1/補助2) (PA-5200 シリーズ	^{補助インス} フェイスを有効にするには、以下のドリイ(かのオ プションを選択します。これらのインターフェイスは以下の目的 で10Gbps(SFP+)のスループットを提供します。
(FA-5200 シリース ファイアウォールの み)	 ファイアウォール管理トラフィック – Web インターフェイスおよび CLI にアクセスしてファイアウォールを管理するときに管理者が使用するネットワーク サービス (プロトコル)を有効にする必要があります。
	 Web インターフェイスには HTTP ではなく HTTPS を有 効にして、CLI には Telnet ではなく SSH を有効にしてく ださい。
	 ファイアウォール ピア間の高可用性(HA)同期 – インター フェースを設定した後、そのインターフェースを HA の Control Link(制御リンク)として選択する必要があります(Device(デ バイス) > High Availability(高可用性) > General(全般))。
	 Log forwarding to Panorama (Panorama へのログ転送) – Panorama Log Forwarding (Panorama ログ転送) サービスを有効 にしてサービス ルートを設定する必要があります(「Device(デ バイス) > Setup (セットアップ) > Services (サービス)」を参 照)。
IPアドレス(IPv4スタ ティック)	[IPv4 Static (IPv4スタティック)]を選択した場合は、インターフェ イスにIPv4アドレスを割り当てます。または、ループバックイン ターフェイスの IP アドレスを割り当ててファイアウォールを管理す ることもできます(「Network(ネットワーク) > Interfaces(イン ターフェイス) > Loopback(ループバック)」を参照)。デフォル トでは、入力する IP アドレスはログ転送の送信元アドレスです。
ネットマスク (IPv4ス タティック)	IPv4 アドレスをインターフェイスに割り当てた場合は、ネットワー ク マスク (例: 255.255.255.0) を入力する必要もあります。

項目	の意味
デフォルト ゲート ウェイ(IPv4)	IPv4 アドレスをインターフェイスに割り当てた場合は、デフォルト ゲートウェイにも IPv4 アドレスを割り当てる必要があります(ゲー トウェイはインターフェイスと同じサブネット上にある必要がありま す)。
IPv6アドレス/プレ フィックス長(スタ ティック)	[IPv6 Static (IPv6スタティック)]を選択した場合は、インターフェ イスにIPv6アドレスを割り当てます。ネットマスクを示すには、プレ フィックス長を入力します(例: 2001:db8:300::1/64)。
IPv6 アドレス、タイ プ (ダイナミック)	[IPv6 Type (Pv6タイプ)]を[Dynamic (ダイナミック)]に選択した場合、MGTインターフェイスはIPv6 SLAAC/DHCPv6クライアントです。DHCPv6クライアントオプションの任意の組み合わせを選択します。
	 [Non Temporary Address (一時的でないアドレス)] – (デフォ ルト)このアドレスタイプは、 [Temporary Address (一時アドレ ス)]よりも長いライフスパンを持ちます。
	 [Temporary Address (一時アドレス)] を選択すると、アドレスが短期間使用されることを意図しているため、セキュリティのレベルが高くなります。
	 Rapid Commit (迅速なコミット)-送信請求、アドバタイズ、要求、および応答メッセージ (4 つのメッセージ) のプロセスではなく、送信請求メッセージと応答メッセージ (2 つのメッセージ) のDHCPv6 プロセスを使用することを選択します。
	 DUID タイプー管理インターフェイスが DHCPv6 サーバへの識別 に使用する DHCPv6 ユニークID。
	 duid-type-llt-DUID-LLT。タイムスタンプと連結された管理インターフェイスのリンクレイヤアドレス。
	 duid-type-II-DUID-LL。管理インターフェイスのリンクレイヤアドレス。
デフォルトゲート ウェイタイプ (IPv6)	インターフェイスに IPv6 アドレスを割り当てた場合は、デフォルト IPv6 ゲートウェイ アドレスも割り当てまたは受信する必要がありま す。デフォルトゲートウェイのアドレス割り当てのタイプを選択しま す。
	 [Static (スタティック)]–[Default IPv6 Gateway Address (デフォ ルトIPv6ゲートウェイアドレス)](ゲートウェイはインターフェ イスと同じサブネット上にある必要があります)を入力しま す(例:2001:db8:300::5)。
	 Dynamic (ダイナミック)-ファイアウォールは、Router Solicitation (RS:ルータ送信要求)に応じてネイバールータ(ゲー トウェイ)から送信される Router Advertisement (RA:ルータア

項目	の意味
	ドバタイズメント)メッセージから IPv6 デフォルト ゲートウェ イアドレスを学習します。リンクに接続されているルータが 1つ だけの場合、ルータの RA メッセージの送信元アドレスがデフォ ルト ゲートウェイ アドレスとして設定されます。リンクに複数 のルータが接続されている場合、ファイアウォールはデフォル トゲートウェイアドレスを、ルータプリファレンス値が最も高い (Low、Medium、または High) RA メッセージの送信元アドレス に設定します。 [Dynamic (ダイナミック)]を選択すると、[Show Gateway Address Info (ゲートウェイアドレス情報を表示)] できます。
速度	 インターフェイスのデータ速度とデュプレックスオプションを 設定します。フルデュプレックスまたはハーフデュプレックス で、10Mbps、100Mbps、1Gbpsのいずれかを選択できます。ファイ アウォールにインターフェイス速度を決定させるには、デフォルトの オートネゴシエート設定を使用します。 この設定は、隣接するネットワーク機器のポート設定 と一致する必要があります。設定を確実に一致させる には、オートネゴシエートを選択します(隣接する機)
	器がこのオプションをサポートする場合)。
MTU	このインターフェイスで送信されるパケットの最大転送単位 (MTU)をバイト数で入力します(範囲は 576 ~ 1,500、デフォル トは 1,500)。
管理サービスの管理	• HTTP - ファイアウォールの Web インターフェイスにアクセスす るには、このサービスを使用します。
	 HTTPはプレーンテキストを使用しますが、HTTPSよりは安全性が劣ります。このため、インターフェイス上の管理トラフィックには、HTTPの代わりにHTTPSを有効化することをお勧めします。 Talact ファイアウェールのCLUにアクセフするには、このサービ
	• Teiner - ノディアウォールのCLI にアクセスするには、このサービスを使用します。
	 Telnetはプレーンテキストを使用しますが、SSHより は安全性が劣ります。このため、インターフェイス 上の管理トラフィックには、Telnetの代わりに SSH を有効化することをお勧めします。
	• HTTPS - ファイアウォールの Web インターフェイスに安全にアク セスするには、このサービスを使用します。

デバイス

項目	の意味
	 SSH - ファイアウォールの CLI に安全にアクセスするには、この サービスを使用します。
Network	インターフェイスで有効にするサービスを選択します。
Services(ネット ワーク サービス)	 HTTP OCSP - ファイアウォールをオンライン証明書状態プロ トコル(OCSP)レスポンダとして設定するには、このサービ スを使用します。詳細は、「Device(デバイス) > Certificate Management(証明書の管理) > OCSP Responder(OCSP レスポ ンダ)」を参照してください。
	 Ping - 外部サービスとの接続をテストするには、このサービスを 使用します。例えば、インターフェイスに対してpingを行い、Palo Alto NetworksアップデートサーバーからPAN-OSソフトウェアや コンテンツのアップデートが受信可能な状態かどうか確認するこ とができます。高可用性(HA)配置の場合、HAピアはpingを使用 してハートビートのバックアップ情報を交換します。
	 SNMP - SNMP マネージャーからのファイアウォール統計情報の クエリを処理するには、このサービスを使用します。詳細は、 「SNMP モニタリングの有効化」を参照してください。
	• User-ID - このサービスを使用して、firewalls 間でのユーザー マッ ピングの data 再配布 を有効にします。
	 User-ID Syslog Listener-SSL(User-ID Syslogリスナー-SSL) - PAN-OS 統合 User-ID[™] エージェントによる SSL 経由の syslog メッセージの収集を有効化するには、このサービスを使用しま す。詳細は、「監視対象サーバーに対するアクセスの設定」を参 照してください。
	 User-ID Syslog Listener-UDP(User-ID Syslogリスナー-UDP) - PAN-OS 統合 User-ID エージェントによる UDP 経由の syslog メッ セージの収集を有効化するには、このサービスを使用します。詳 細は、「監視対象サーバーに対するアクセスの設定」を参照して ください。
アクセス許可IPアド レス	管理者がインターフェイスを通じてファイアウォールにアクセスする ために使用できる IP アドレスを入力します。空のリスト(デフォル ト)は、どの IP アドレスからもアクセスできることを示します。
	このリストを空白のままにしないでください。ファイ アウォール管理者の IP アドレスのみを指定して、不正 アクセスを阻止してください。

Device(デバイス) > Setup(セットアップ) > Telemetry(テレメトリ)

テレメトリは、脅威とサポートの分析を目的としてデータを収集および送信し、アプリケーショ ンロジックを有効にするプロセスです。テレメトリを収集して Palo Alto Networks に送信する には、まず宛先リージョンを選択する必要があります。Cortex Data Lake ライセンスを現在保持 している組織の場合、宛先リージョンは、Cortex Data Lake インスタンスが存在するリージョン に制限されます。

テレメトリデータは、使用中の Palo Alto Networks の製品とサービスを管理および設定能力を 向上させるアプリケーションを強化する目的で使用されます。上記アプリケーションは、デバ イスの状態、パフォーマンス、容量のプランニング、および設定に関する可視性を向上させま す。Palo Alto Networks はまた、脅威防止力を改善し、製品の使用上のメリットを最大化する上 で上記データを継続的に使用しています。

Device (デバイス) > **Setup (**セットアップ**)** > **Telemetry (**テレメトリ**)** を選択し、現在収集された テレメトリのカテゴリを確認します。上記カテゴリを変更するには、テレメトリ ウィジェット を編集します。ファイアウォールで収集しないカテゴリを選択解除し、変更内容をコミットしま す。

ファイアウォールに次回のテレメトリ送信間隔で Palo Alto Networks に送信するデータのライ ブの例を取得させるには、Generate Telemetry File(テレメトリ ファイルの生成)を実行しま す。

テレメトリ送信を完全に無効にするには、Enable Telemetry(テレメトリを有効化する)が チェックされていないことを確認して変更をコミットします。

Device > Setup > Content-ID [デバイス > セットアップ > Content-ID]

Content-ID[™] タブを使用して、URL フィルタリング、データ保護、およびコンテナ ページの設 定を定義します。

Content-ID設定	の意味
URL フィルタリング	
URL コンティニュー タ イムアウト	同一カテゴリの URL に対して Continue (続行) を再度押す前に、 ユーザーが Continue (続行) アクションに従う間隔を指定します (範 囲は 1 ~ 86,400 分、デフォルトは 15)。
URL 管理オーバーライ ド タイムアウト	ユーザーが Admin Override (管理オーバーライド) パスワードを入 力してから、ユーザーが同じカテゴリの URL のパスワードを再入 力するまでの間隔を指定します (範囲は 1 ~ 86,400 分、デフォルト は15 分)。
カテゴリ検索のクライ アント要求を保持	このオプションを有効にすると、ファイアウォールがローカル キャッシュで URL のカテゴリ情報を見つけられない場合に、PAN- DB にクエリを送信するときに Web 要求を保持するように指定で きます。
	 このオプションはデフォルトでは無効になっています。ベスト プラクティスの URL フィルタリング プロファイルの一部として有効にします。
末尾のスラッシュを追 加	firewall を有効にして、カスタム URL カテゴリのドメイン エントリ (paloaltonetworks.com など) および末尾のスラッシュまたはア スタリスクのワイルドカード (*) に end を含まない URL リスト タイ プの外部動的リストを末尾にスラッシュ (/) を追加します。
	末尾のスラッシュは、firewall がエントリと一致すると見な し、URL フィルタリング ポリシー ルールを適用できる URL を制限 します。
	 ワイルドカード(*または ^)のないドメインエントリの場合、末尾のスラッシュは、指定されたドメインとそのサブディレクトリに一致するものを制限します。
	 ワイルドカードを含むドメイン エントリの場合、末尾のスラッシュは、指定されたパターンに準拠する URL に一致します。
	URL カテゴリ例外 では、末尾のスラッシュについて詳しく説明 し、URL リストの書式設定のガイドラインを示します。

Content-ID設定	の意味
	このオプションはデフォルトでは有効になっています。
カテゴリ検索タイムア ウト (秒)	カテゴリが 未解決であると判断する前に、ファイアウォールが URL のカテゴリの検索を試行する時間を秒単位で指定します (範囲 は 1 ~ 60 秒、デフォルトは 2) 。
URL 管理ロックアウト タイムアウト	3回失敗した後、ユーザーが URL Admin Override (URL 管理オー バーライド) パスワードの使用をロックアウトされる期間を指定し ます (範囲は 1 ~ 86,400 分、デフォルトは 30 分)。
PAN-DB サーバー (プライベート PAN- DB サーバーに接続す る場合に必須)	ネットワーク上のプライベート PAN-DB サーバーの IPv4 アドレ ス、IPv6 アドレス、または FQDN を指定します。最大 20 エント リを追加できます。 デフォルトでは、ファイアウォールはパブリック PAN-DB クラウ
	ドに接続します。プライベート PAN-DB ソリューションは、ファ イアウォールがパブリック クラウド内の PAN-DB サーバーに直接 アクセスすることを許可しないエンタープライズ向けです。ファ イアウォールは、URL データベース、URL 更新、URL 検索で Web ページを分類できるように、この PAN-DB サーバーのリストに含 まれるサーバーにアクセスします。
URL 管理オーバーライド	<u> </u>

URL 管理オーバーライ ドの設定	URL管理オーバーライド用に構成する仮想システムごとに、Add を実行し、URLフィルタリングプロファイルがページをブロック し、Override アクションが指定された場合に適用される設定を 指定します。詳細については、Objects > Security Profiles > URL Filtering を参照してください。
	• Location (場所)–(マルチvsys ファイアウォールのみ) ドロップダ ウンから 仮想システム を選択します。
	 Password/Confirm Password [パスワード/パスワード再入力] – ブロックページをオーバーライドするためにユーザーが入力す る必要があるパスワードを入力します。
	 SSL/TLS Service Profile[SSL/TLS サービス プロファイル] – 指定 したサーバーを介してリダイレクトするときに通信を保護する ための証明書および許可された TLS プロトコル バージョンを指 定するには、SSL/TLS サービス プロファイルを選択します。詳 細は、「Device(デバイス) > Certificate Management(証明書 の管理) > SSL/TLS Service Profile(SSL/TLS サービス プロファ イル)」を参照してください。
	 Mode[モード] – ブロックページが透過的に配信されるか (ブ ロックされた Web サイトから発信したように見える)、指定

Content-ID設定	の意味
	したサーバーにユーザーをリダイレクトするかを決定しま す。 Redirect (リダイレクト) を選択した場合、次に、リダイレク トするための IP アドレスを入力します。
	エントリを Delete (削除) することもできます。
HTTP/2 設定	
接続ログ	ファイアウォール が HTTP/2 接続セッションをトンネル監視ログ エントリとしてログに記録できるようにします。
Content Cloud Settings	(コンテンツクラウドの設定)
サービス URL	 Cloud-Delivered Security Services サーバー URL。 アジア太平洋-apac.hawkeye.services- edge.paloaltonetworks.com Europe (欧州)-eu.hawkeye.services-
	edge.paloaltonetworks.com
	 イモリスーuk.hawkeye.services- edge.paloaltonetworks.com
	 米国-us.hawkeye.services- edge.paloaltonetworks.com

URL インライン クラウド分類

最大待機時間 (秒)	結果を返すインライン クラウド分類 の最大許容処理時間を秒単位 で指定します。
最大待機時間で許可	ファイアウォールが最大待機時間に達したときに allow のアクショ ンを実行できるようにします。このオプションの選択を解除する と、ファイアウォール アクションがブロックに設定されます。
ログ トラフィックがス キャンされない	ファイアウォール が、特定の高度な Web ページ脅威の存在を示す が、インライン クラウド分類 によって処理されていない URL 分類 要求をログに記録できるようにします。

WildFire インラインクラウド分析

最大レイテンシ (ミリ	Advanced WildFire インラインクラウド分析が結果を返すまでの最
秒)	大許容処理時間をミリ秒単位で指定します。範囲は1~240,000
	ミリ秒です。デフォルトは 30,000 ミリ秒です。

Content-ID設定	の意味
	ファイアウォールが最大待機時間に達したときに allow のアクショ ンを実行できるようにします。このオプションの選択を解除する と、ファイアウォール アクションがブロックに設定されます。
ログ トラフィックがス キャンされない	ファイアウォールが、マルウェアのように見えるがまだ処理されて いないAdvanced WildFire Inline Cloud Analysisリクエストをログに 記録できるようにします。
Content-ID設定	
復号化されたコンテン ツの転送を許可	このオプションを有効にすると、ポート ミラーリングまたは解析の ために WildFire [®] にファイルを送信するときに、復号化されたコン テンツを外部サービスに転送するようにファイアウォールを設定す ることができます。
	② このオプションを有効化し、復号化されたトラフィック内のすべての未知のファイルを WildFire に送信して分析を行います。
	マルチ仮想システム (multi-vsys) 機能が有効化されているファイア ウォールの場合、このオプションを仮想システムごとに個々に有 効にします。Device(デバイス) > Virtual Systems(仮想システ ム)を選択し、復号化されたコンテンツの転送を有効にする仮想シ ステムを選択します。このオプションは、仮想システム ダイアログ で使用できます。
拡張パケット キャプ チャ長	Anti-Spyware(アンチスパイウェア)および Vulnerability Protection(脆弱性防御)プロファイルで拡張キャプチャオプショ ンが有効になっている場合にキャプチャするパケット数を設定しま す(範囲は1~50、デフォルトは5)。
TCP App-ID [™] 検査 キューを超過するセグ メントを転送	このオプションを有効にすると、App-ID キューが 64 セグメントの 制限を超えたときに、セグメントが転送され、アプリケーションを unknown-tcp として分類できます。次のグローバル カウンターを 使用して、このオプションを有効または無効にしたかどうかに関係 なく、キュー制限を超えるセグメントの数を表示します。
	appid_exceed_queue_limit
	ファイアウォールがTCPセグメントを転送しつつも、App-ID検査 キューに空きが無いためApp-ID検査が省略されるということを防ぎ たい場合はこのオプションを選択してください。

Content-ID 設定	の意味
	② このオプションはデフォルトで無効になっており、セキュリティを最大限に高めるために無効のままにしておく必要があります。
	このオプションを無効にすると、64 を超えるセグメ ントが App-ID 処理を待っているストリームで待機時 間が長くなることがあります。
TCPコンテンツ検査 キューを超過するセグ メントを転送	このオプションを有効にすると、TCP セグメントが転送され、TCP コンテンツ検査キューがいっぱいになったときにコンテンツ検査が スキップされます。ファイアウォールはコンテンツエンジンから の応答を待つ間、64個のセグメントをキューに追加することがで きます。ファイアウォールがセグメントを転送し、コンテンツ検査 キューに空きがないためにコンテンツ検査を省略した場合、次のグ ローバル カウンターの値が増加します。
	ctd_exceed_queue_limit
	ファイアウォールがTCPセグメントを転送しつつも、コンテンツ検 査キューに空きが無いためコンテンツ検査が省略されるというこ とを防ぎたい場合はこのオプションを選択してください。このオプ ションを無効にすると、ファイアウォールはキュー制限を超過した セグメントを破棄し、次のグローバル カウンターの値が増加しま す。
	ctd_exceed_queue_limit_drop
	これらのグローバルカウンターはTCPおよびUDPの両方のパケット に適用されます。グローバル カウンターを表示した後で設定を変更 する場合は、次のコマンドを使用して CLI 内から設定を変更できま す。
	デバイス構成の設定 CTD TCP-bypass-exceed-queue を設 定する

Content-ID設定	の意味
	 Cのオプションはデフォルトで有効になっていますが、Palo Alto Networksでは、セキュリティを最大限に高めるためにこのオプションを無効にすることをお勧めします。ただし、ドロップされたトラフィックのTCP 再送信のために、このオプションを無効にすると、一部のアプリケーション (特に high-volume トラフィック環境)のパフォーマンスが低下し、機能が失われる可能性があります。
UDPコンテンツ検査 キューを超過するデー タグラムを転送	このオプションを有効にすると、UDP データグラムが転送さ れ、UDP コンテンツ検査キューがいっぱいになったときにコンテ ンツ検査がスキップされます。ファイアウォールはコンテンツ エ ンジンからの応答を待つ間、64 個のデータグラムをキューに追 加することができます。ファイアウォールがデータグラムを転送 し、UDP コンテンツ検査キューのオーバーフローのためにコンテ ンツ検査を省略した場合、次のグローバル カウンターの値が増加し ます。
	ctd_exceed_queue_limit
	ファイアウォールがデータグラムを転送しつつも、UDPコンテンツ 検査キューに空きが無いためコンテンツ検査が省略されるというこ とを防ぎたい場合はこのオプションを選択してください。このオプ ションが無効化された場合、ファイアウォールはキュー制限を超過 したデータグラムを破棄し、次のグローバルカウンターの値を 増 加させます。
	ctd_exceed_queue_limit_drop
	これらのグローバルカウンターはTCPおよびUDPの両方のパケット に適用されます。グローバル カウンターを確認した後、設定を変更 するように決定した場合は、CLI から次のコマンドを使用して設定 を変更できます。
	デバイス設定の設定 CTD UDP-bypass-exceed-queue を設 定する

Content-ID 設定	の意味	
	 このオプションはデフォルトで有効になっていますが、Palo Alto Networksでは、セキュリティを最大限に高めるためにこのオプションを無効にすることをお勧めします。ただし、パケットがドロップされたためにこのオプションを無効にすると、一部のアプリケーション(特に high-volume トラフィック環境)のパフォーマンスが低下し、機能が失われる可能性があります。 	
HTTP 部分レスポンス を許可する	この HTTP 部分応答 オプションにより、クライアントはファイル の一部のみを取得することができるようになります。転送の途中経 路にある次世代ファイアウォールが悪意のあるファイルの検知と破 棄を行った場合、RSTパケットにてTCPセッションを強制終了しま す。ブラウザにHTTPレンジオプションを実装すると、ファイルの 残りの部分を取得するために新しいセッションを開始できるように なります。これにより、最初のセッションに対するコンテクストの 欠損を理由にファイアウォールが同じシグネチャをトリガーしてし まうことを防ぐと同時に、ウェブブラウザでファイルを再構築し、 悪意のあるファイルを転送することができます。これを防ぐには、 必ずこのオプションを無効にしてください。	
Content-ID設定	の意味	ŝ
--------------	-----	---
		HTTP 部分応答を許可する はデフォルトでファイア ウォールで有効になっています。これにより、最大 限の可用性が提供されますが、サイバー攻撃が成功 するリスクが高まります。最大限のセキュリティのた めに、このオプションを無効にして、悪意のあるアク ティビティのためにファイアウォールが元のセッショ ンを終了した後に、Webブラウザが新しいセッション を開始してファイルの残りの部分を取得するのを防 ぎます。HTTP 部分応答を無効にすると、RANGE ヘッ ダーを使用する HTTP-based データ転送に影響し、特 定のアプリケーションでサービス異常が発生する可能 性があります。HTTP 部分応答を無効にした後、ビジ ネス クリティカルなアプリケーションの動作を検証 します。 ビジネスクリティカルなアプリケーションの動作を検証 します。 ビジネスクリティカルなアプリケーション でHTTPデータ転送の中断が発生した場合は、その特 定のアプリケーションに対してApplication Overrideポ リシーを作成できます。Application Overrideポ リシーを作成し、ソースと宛先を指定してルールを制限 します (最小特権アクセスの原則)。必要な場合を除 き、Application Override ポリシー を作成し、ソースと宛先を指定してルールを制限 します (最小特権アクセスの原則)。必要な場合を除 き、Application Override ポリシーの詳細について は、「https://knowledgebase.paloaltonetworks.com/ KCSArticleDetail?id=kA10g000000CIVLCA0を参照し てください。

リアルタイム シグネチャ検索

DNS シグネチャ ルッ クアップのタイムアウ ト(ms)	ファイアウォールが DNS セキュリティ サービスにクエリを送る期 間をミリ秒単位で指定します。指定した期間中にクラウドが応答し ない場合、ファイアウォールはリクエストしたクライアントのた めに関連する DNS 応答をリリースします(範囲は 0~60,000、デ フォルトは 100)。
WildFireのリアルタイ ムシグネチャ検索を長 押し	WildFire リアルタイムシグニチャ検索保留モードをアンチウイルス プロファイルごとに使用するオプションを有効にします。

Content-ID設定	の意味
	 このオプションだけでは、WildFire リアルタイムシグ ネチャ検索保留モードは有効になりません。さらに、 特定のウイルス対策セキュリティプロファイル内で WildFire Real Time Signature Look Up の保留を有効に する必要があります。
WildFire リアルタイム シグニチャ検索タイム アウト (ミリ秒)	ファイアウォールがリアルタイムシグネチャクラウドに照会して リアルタイムシグネチャ検索を行うまでの時間をミリ秒単位で指 定します。リアルタイムシグネチャクラウドが指定された期間の 終了前に応答しない場合、ファイアウォールはユーザ指定のリア ルタイムWildFireシグネチャタイムアウト時のアクションを要求 元のクライアントに適用します(範囲は1000~5000、デフォルト は1000)。
リアルタイム WildFire シグニチャタイムアウ ト時のアクション	シグネチャ検索が設定済みの WildFire リアルタイムシグネチャ検 索タイムアウト設定を超えたときに実行するアクションを指定しま す。 Allow (許可)–パケットは解放され、ファイルは引き続きクライ アントに送信されます。 Peset Both (両方をリセット) - クライアント側とサーバー側の両
	方の接続をリセットします。
X-Forwarded-For ヘッダ	
X-Forwarded-For ヘッ ダの使用	X-Forwarded-For for User-ID とセキュリティ ポリシーの同時有効化はできません。
	 Disabled (無効化) – 無効化の場合、ファイアウォールはクラ イアント要求の X-Forwarded-For (X-Forwarded-For - XFF) ヘッ ダーから IPアドレスを読み取りません。
	 Enable for User-ID – このオプションを有効にすると、firewall がインターネットとプロキシー・サーバーの間にデプロイさ れ、クライアント IP アドレスを隠すプロキシー・サーバーの間 にファイアウォールがデプロイされるときに、Web サービスに 対するクライアント要求の X-Forwarded-For (XFF) ヘッダーから IP アドレスを読み取るように指定します。User-ID は、読み取っ た IP アドレスを、ポリシーで参照されているユーザー名と照合 します。そのため、このポリシーを使用して、関連付けられて いるユーザーやグループのアクセスを制御してログに記録でき

Content-ID 設定	の意味
	ます。ヘッダーに複数の IP アドレスが含まれている場合、User- ID は一番左側のエントリを使用します。
	場合によって、ヘッダー値が IP アドレスではなく文字列になっ ていることがあります。文字列がユーザー名と一致し、User- ID がそのユーザー名を IP アドレスにマッピングしている場合、 ファイアウォールはそのユーザー名をポリシー内のグループ マッピングの参照で使用します。該当の文字列の IP アドレス マッピングが存在しない場合、ファイアウォールは、送信元 ユーザーを any または unknown に設定しているポリシー ルー ルを起動します。
	URL フィルタリング ログの Source User (送信元ユーザー) フィールドに、一致したユーザー名が表示されます。User-ID が 照合を実行できない場合、または IP アドレスに関連付けられた ゾーンで User-ID が有効化されていない場合、Source User (送 信元ユーザー)フィールドには、プレフィックス x-fwd-for 付 きの XFF IP アドレスが表示されます。
	 User-ID で XFF ヘッダーを使用して、元のクライア ント IP アドレスがログに表示され、問題の調査に 役立つようにします。
	 Enable for Security Policy-このオプションを有効にすると、プロキシサーバーやロードバランサー等のアップストリームデバイスがクライアントとファイアウォール間に展開されている場合に、ファイアウォールがWebサービスのクライアント要求のX-Forwarded-For (X-Forwarded-For - XFF) ヘッダーからIPアドレスを読み取る指定が可能です。プロキシサーバーまたはロードバランサーのIPアドレスは、要求送信元IPとしてクライアントIPアドレスを置き換えます。その後、ファイアウォールはXFF ヘッダー内のIPアドレスを使用してポリシーを適用できます。
	ファイアウォールは、XFF フィールドに最後に追加された IP アドレスを使用します。要求が複数のアップストリームデバイスを通過する場合、ファイアウォールは最後に追加された IP アドレスに基づいてポリシーを適用します。
X-Forwarded-For (X- Forwarded-For - XFF) ヘッダーの削除	このオプションを有効にすると、ファイアウォールがインターネットとプロキシサーバー間にデプロイされている場合、Webサービスを要求しているクライアントのIPアドレスが含まれる X-Forwarded-For (XFF) ヘッダーが削除されます。ファイアウォールによって要求を転送する前にヘッダーの値がゼロに設定されるため、転送されるパケットには内部送信元 IP 情報が含まれなくなります。

Content-ID 設定	の意味
	このオプションを有効にした場合も、ポリシーのユー ザー属性では XFF ヘッダーの使用は無効になりませ ん。ファイアウォールは、ユーザー属性に使用した後 でのみ XFF 値をゼロに設定します。
	 User-ID での XFF ヘッダの使用を有効にすると、パケットを転送する前にユーザーを追跡する機能を損なうことなくユーザーのプライバシーを保護するために、XFF ヘッダのストリップも有効になります。両方のオプションを有効化することで、元の IP アドレスを転送しないことでユーザーのプライバシーを保護しつ、元のユーザーの IP アドレスを追跡してログに記録できるようになります。
コンテンツ ID 機能	
データ保護の管理	クレジットカード番号や社会保障番号など重要な情報を含むログへ のアクセスに対し拡張防御を追加します。
	Manage Data Protection (データ保護の管理) をクリックして、以下のタスクを実行します。
	 Set Password – 構成されていない場合は、新しいパスワードを 入力して確認します。
	 Change Password (パスワードの変更)–以前のパスワードを入力し、新しいパスワードを入力して確認します。
	 Delete Password (パスワードの削除)–パスワードと保護されて いたデータを削除します。
Container Pages	これらの設定を使用して、ファイアウォールがコンテンツ・タ イプに基づいて追跡またはログに記録する URL のタイプ (アプリ ケーション/pdf、アプリケーション/soap+xml、アプリケーション/ xhtml+、テキスト/html、テキスト/プレーン、テキスト/xml など) を指定します。Location [場所] のドロップダウンリストから選択し た仮想システムごとにコンテナページが設定されます。仮想システ ム に明示的なコンテナ ページが定義されていない場合、ファイア ウォールはデフォルトのコンテンツ タイプを使用します。
	Add (追加)してコンテンツ タイプを入力するか、既存のコンテンツ タイプを選択します。
	仮想システムの新しいコンテンツ タイプを追加すると、コンテンツ タイプのデフォルトのリストがオーバーライドされます。仮想シス テムに関連付けられているコンテンツ タイプがない場合、コンテン ツ タイプのデフォルトのリストが使用されます。

Content-ID 設定	の意味	
脅威対策インライン クラウド分析		
最大レイテンシ (ミリ 秒)	脅威防御インライン クラウド分析 が結果を返す最大処理時間を秒 単位で指定します。	
最大待機時間で許可	ファイアウォールが最大待機時間に達したときに allow のアクショ ンを実行できるようにします。このオプションの選択を解除する と、ファイアウォール アクションがブロックに設定されます。	
ログ トラフィックがス キャンされない	ファイアウォール が、高度で回避的な command-and-control (C2) 脅威の存在を示す異常な特性を示すトラフィック要求をログに記録 できるようにしますが、脅威対策インライン クラウド分析 アナラ イザーによって処理されていません。	

Device > Setup > WildFire [デバイス > セットアップ > WildFire]

ファイアウォールと Panorama で WildFire を設定するには、Device(デバイス) > Setup(セットアップ) > WildFire を選択します。WildFire クラウドと WildFire アプライアンスの両方を使用して、ファイル分析を実行できます。レポートされるファイル サイズ制限とセッション情報を設定することもできます。WildFire 設定を入力したら、WildFire Analysis(WildFire 分析)プロファイル(Objects(オブジェクト) > Security Profiles(セキュリティ プロファイル) > WildFire Analysis(WildFire 分析))を作成して、WildFire クラウドまたは WildFire アプライアンスに転送するファイルを指定できます。

 復号化されたコンテンツを WildFire に転送するには、「Forward Decrypted SSL Traffic for WildFire Analysis(復号化された SSL トラフィックを WildFire Analysis 用に転送する)」を参照してください。

WildFire 設定	の意味
一般設定	
WildFire パブリック クラウド	wildfire.paloaltonetworks.com と入力して、分析のために United States でホストされている WildFire グローバル クラウド (米 国) にファイルを送信します。または、WildFire 地域クラウドに分析 用のファイルを送信することもできます。地域クラウドは、ユーザー の場所に応じて、ユーザーが期待するデータ プライバシーに準拠す るように設計されています。

WildFire 設定	の意味
	 ・リージョナル WildFire クラウドにサンプルを転送し、 データのプライバシーおよびコンプライアンスに関す る現地特有の規則を確実に遵守できるようにします。 リージョナル クラウド:
	• 欧州—eu.wildfire.paloaltonetworks.com
	• 日本—jp.wildfire.paloaltonetworks.com
	 シンガポー
	<pre>N-sg.wildfire.paloaltonetworks.com</pre>
	 United Kingdom -uk.wildfire.paloaltonetworks.com
	 Canada—ca.wildfire.paloaltonetworks.com
	 Australia -au.wildfire.paloaltonetworks.com
	 Germany -de.wildfire.paloaltonetworks.com
	 India-in.wildfire.paloaltonetworks.com
	 スイスー ch.wildfire.paloaltonetworks.com
	 ポーランドー pl.wildfire.paloaltonetworks.com
	 インドネシ アーid wildfire paloaltonetworks com
	 ◆ 」はいにはいに、こりなことのにていていたりてもm ◆ 台湾 - tw.wildfire.paloaltonetworks.com
	 フランス-
	fr.wildfire.paloaltonetworks.com
	 カタール-
	qatar.wildfire.paloaltonetworks.com

WildFire 設定	の意味
WildFire プライベー ト クラウド	WildFire アプライアンスの IPv4 または IPv6 アドレスあるいは FQDN を指定します。
	ファイアウォールは、指定されたアプライアンスに分析用のファイル を送信します。
	Panorama は脅威 ID を WildFire アプライアンスから収集します。こ れにより、デバイス グループで設定したアンチスパイウェア プロ ファイル (DNS シグネチャのみ) とアンチウイルス プロファイル に脅威の例外を追加できます。また、Panorama は WildFire アプラ イアンスから情報を収集し、PAN-OS 7.0 よりも前のソフトウェア バージョンを実行しているファイアウォールから受信した WildFire Submissions (WildFire への送信) ログで不足しているフィールドを 入力できます。
ファイル サイズ制限	WildFire サーバーに転送される最大ファイル サイズを指定します。 ファイルのサイズ制限に関するベストプラクティスのすべての推奨事 項に関して、上限が大き過ぎてファイアウォールが複数の巨大なゼロ デイファイルを同時に転送できない場合は、ファイアウォールで利 用できるバッファ領域のサイズに基づいて調整を行い、上限を下げて ください。バッファ領域が大きい場合は、ファイルサイズの上限をベ ストプラクティスの推奨事項よりも大きくすることができます。ファ イアウォール リソースに負担をかけない有効な上限の設定として、 最初に参考になるのがベストプラクティスの推奨事項です。指定可能 な範囲は以下のとおりです。
	 pe (Portable Executable) - 範囲は 1 ~ 50MB、デフォルトは 16MB です。
	Ø PE ファイルのサイズを 16MB に設定します。
	 apk (Android アプリケーション) - 範囲は1~50MB、デフォルトは10 MBです。
	APK ファイルのサイズを 10MB に設定します。
	 pdf(ポータブルドキュメントフォーマット) – 範囲は 100KB ~ 51,200KB、デフォルトは 3,072KB です。
	PDF ファイルのサイズを 3,072KB に設定します。
	 ms-office (Microsoft Office) - 範囲は 200KB ~ 51,200KB、デ フォルトは 16,384KB です。
	ms-office ファイルのサイズを 16,384KB に設定しま す。

WildFire 設定	の意味
	 jar (パッケージ化された Java クラスファイル) - 範囲は1~ 20MB、デフォルトは5MBです。
	jar ファイルのサイズを 5MB に設定します。
	• flash(Adobe Flash) - 範囲は 1 ~ 10MB、デフォルトは 5MB で す。
	⑦ フラッシュファイルのサイズを 5MB に設定します。
	 MacOSX(DMG/MAC-APP/MACH-O PKG ファイル) - 範囲は1 ~ 50MB、デフォルトは10MBです。
	MacOSX ファイルのサイズを 1MB に設定します。
	 archive (RAR と 7z ファイル) - 範囲は 1 ~ 50MB、デフォルトは 50MB です。
	アーカイブファイルのサイズを 50MB に設定します。
	 linux (ELF ファイル) - 範囲は 1 ~ 50MB、デフォルトは 50MB です。
	Linux ファイルのサイズを 50MB に設定します。
	 script (スクリプト) (JScript、VBScript、PowerShell、Shell Script ファイル) –範囲は 10 ~ 4096KB、デフォルトは 20KB です。
	スクリプトファイルのサイズを 20KB に設定しま す。
	実行中のPAN-OSのバージョンやコンテンツリリースにより、直前の値が変化する可能性があります。有効範囲を表示するには、Size Limit(サイズ制限)フィールドをクリックします。使用可能な範囲とデフォルト値がポップアップで表示されます。
安全なファイルのレ ポート	このオプションを有効にすると (デフォルトでは無効)、WildFire で 分析され、安全と判定されたファイルが、Monitor[監視] > WildFire Submissions [WildFire への送信] ログに表示されます。
	ファイアウォールでこのオプションが有効な場合でも、WildFire で安 全と見なされた電子メール リンクは、処理されるリンクの量が多く なる可能性があるため、ログに記録されません。

WildFire 設定	の意味
レポートのグレイ ウェア ファイル	このオプションを有効にすると (デフォルトでは無効)、WildFire で 分析され、グレイウェアと判定されたファイルが、 Monitor[監視] > WildFire Submissions [WildFire への送信] ログに表示されます。
	 ファイアウォールでこのオプションが有効な場合で も、WildFire でグレイウェアと判定された電子メール リンクは、処理されるリンクの量が多くなる可能性があるため、ログに記録されません。
	グレイウェアファイルのレポートを有効化し、セッション情報、ネットワークアクティビティ、ホストアクティビティ、および分析に役立つその他の情報をログに記録します。
セッション情報設定	
設定	WildFire サーバーに転送する情報を指定します。デフォルト設定では すべてが選択されており、次のような脅威イベントを防ぐ対策を行う ために統計情報やその他の指標を得られるよう、すべてのセッション 情報を転送することがベストプラクティスになります。
	 Source IP[送信元 IP] – 疑わしいファイルを送信した送信元 IP アドレス。
	 Source Port[送信元ポート] – 疑わしいファイルを送信した送信元 ポート。
	● Destination IP[宛先 IP] – 疑わしいファイルの宛先 IP アドレス。
	● Destination Port[宛先ポート] – 疑わしいファイルの宛先ポート。
	 Vsys[仮想システム] – 見込まれるマルウェアを識別したファイア ウォール 仮想システム。
	 Application[アプリケーション] – ファイルの送信に使用された ユーザー アプリケーション。
	● User[ユーザー] – ターゲット対象のユーザー名。
	• URL – 疑わしいファイルに関連付けられた URL。
	● Filename[ファイル名] – 送信されたファイルの名前。
	 Email sender [電子メール送信者] – SMTPおよびPOP3トラフィックで悪意のある電子メールリンクが検出されると、WildFireログとWildFireの詳細レポートに送信者名が表示されます。
	 Email recipient [電子メール受信者] – SMTPおよびPOP3ト ラフィックで悪意のある電子メールリンクが検出される と、WildFireログとWildFireの詳細レポートに受信者名が表示され ます。

WildFire 設定	の意味	
	 Email subject [電子メール件名] – SMTPおよびPOP3トラフィック で悪意のある電子メールリンクが検出されると、WildFireログと WildFireの詳細レポートに電子メールの件名が表示されます。 	
インラインクラウド分析設定		
ファイル サイズ制限	 Advanced WildFire Inline Cloud Analysis が送信してマルウェアを分析できる最大ファイルサイズを表示します。制限より大きいファイルサイズは、Advanced WildFireクラウドでは処理されません。 	
	レノンで派法するために定対的に更利されより。	

インラインセッション情報設定

設定	Advanced WildFire Inline Cloud Analysis で処理のためにサンプルを送 信するときに、Advanced WildFire クラウドに転送する情報を指定し ます。デフォルト設定ではすべてが選択されており、次のような脅威 イベントを防ぐ対策を行うために統計情報やその他の指標を得られる よう、すべてのセッション情報を転送することがベストプラクティス になります。
	 Source IP[送信元 IP] – 疑わしいファイルを送信した送信元 IP アドレス。
	• Source Port[送信元ポート] – 疑わしいファイルを送信した送信元 ポート。
	• Destination IP[宛先 IP] – 疑わしいファイルの宛先 IP アドレス。
	• Destination Port[宛先ポート] – 疑わしいファイルの宛先ポート。
	 Vsys[仮想システム] – 見込まれるマルウェアを識別したファイア ウォール 仮想システム。
	 Application[アプリケーション] – ファイルの送信に使用された ユーザーアプリケーション。
	● User[ユーザー] – ターゲット対象のユーザー名。
	• URL – 疑わしいファイルに関連付けられた URL。
	● Filename[ファイル名] – 送信されたファイルの名前。
	 Email sender [電子メール送信者] – SMTPおよびPOP3トラフィックで悪意のある電子メールリンクが検出されると、WildFireログとWildFireの詳細レポートに送信者名が表示されます。
	 Email recipient [電子メール受信者] – SMTPおよびPOP3ト ラフィックで悪意のある電子メールリンクが検出される

WildFire 設定	の意味
	と、WildFireログとWildFireの詳細レポートに受信者名が表示され ます。
	 Email subject [電子メール件名] – SMTPおよびPOP3トラフィック で悪意のある電子メールリンクが検出されると、WildFireログと WildFireの詳細レポートに電子メールの件名が表示されます。

Device > Setup > Session [デバイス > セットアップ > セッション]

Device [デバイス] > Setup 設定 > Session [セッション] を開き、セッションのエイジアウト時間、復号化証明書設定、およびグローバルなセッション関連の設定(IPv6トラフィックのファイアウォール設定、ポリシー変更時の既存のセッションへのセキュリティポリシーの再マッチングなど)を設定します。このタブには、以下のセクションがあります。

- セッション設定
- セッション タイムアウト
- TCP 設定
- 復号化設定:証明書取り消しチェック
- 復号化設定:フォワード プロキシ サーバーの証明書設定
- 復号化設定:SSL復号化設定
- VPN セッション設定

セッション設定

以下の表では、セッション設定について説明します。

セッション設定	の意味
セッションの再マッ チング	ファイアウォールで、新しく設定されたセキュリティポリシールー ルをすでに進行中のセッションに適用するには、Edit[編集]をクリッ クし、Rematch Sessions[セッションの再マッチング]を選択します。 この機能はデフォルトで有効になっています。この設定が無効な場 合、ポリシールールの変更は、変更がコミットされた後に開始された セッションにのみ適用されます。
	たとえば、Telnet を許可する関連ポリシー ルールが設定されている ときに Telnet セッションを開始し、その後、Telnet を拒否するポ リシー ルールの変更をコミットした場合、ファイアウォールは変更 されたポリシー ルールを現在のセッションに適用してブロックしま す。
	 Rematch Sessions (セッションの再マッチング)を有効化し、最新のセキュリティポリシールールを現在アクティブなセッションに適用します。
ICMPv6 トークンバ ケット サイズ	ICMPv6 エラー メッセージの帯域制限に対応するバケット サイズを 入力します。トークンバケットサイズは、ICMPv6エラーパケットの バーストをどの程度許容するかを制御するトークンバケットアルゴリ

セッション設定	の意味
	ズムのパラメータです(範囲は10~65535パケット、デフォルトは 100)。
ICMPv6 エラー パ ケット速度	ファイアウォール全体として1秒間に許容される ICMPv6 エラー パケットの平均数を入力します(範囲は 10~65,535、デフォルト は100)。この値はすべてのインターフェイスに適用されます。ファ イアウォールが ICMPv6 エラー パケット速度に達した場合、ICMPv6 トークンバケットを使用して、ICMPv6 エラー メッセージのスロッ トリングが有効になります。
IPv6 ファイアウォー ルの有効化	 IPv6トラフィックのファイアウォール機能を有効化する場合は、IPv6 Firewalling [IPv6ファイアウォール設定]のEdit [編集] をクリックします。 IPv6ファイアウォールを有効にしない場合、ファイアウォールはすべての IPv6ベースの設定を無視します。インターフェースで IPv6トラフィックを有効化する場合でも、IPv6ファイアウォールを機能させるには、IPv6 Firewalling (IPv6ファイアウォール設定)オプションも有効化する必要があります。
ERSPAN サポート	firewall を有効にして Generic Routing Encapsulation (GRE) トンネル を終了し、Encapsulated Remote Switched Port Analyzer (ERSPAN) データをカプセル化解除します。これは、IoT セキュリティなどのセ キュリティ サービスに役立ちます。ネットワークスイッチはネット ワークトラフィックをミラーリングし、ERSPAN を使用して GRE ト ンネルを介して firewall に送信します。データをカプセル化解除した 後、firewall は TAP ポートで受信したトラフィックを検査する方法と 同様にデータを検査します。次に、拡張アプリケーション ログ (EAL) とトラフィック、脅威、WildFire、URL、データ、GTP (GTP が有効 な場合)、SCTP (SCTP が有効になっている場合)、トンネル、認証、お よび復号化ログを作成します。firewall は、これらのログをログ サー ビスに転送し、そこで IoT Security がデータにアクセスして分析しま す。
Jumbo Frame を有効 にする グローバル MTU	 Ethernet インターフェイスでジャンボ フレームのサポートを有効に する場合に選択します。ジャンボ フレームの最大伝送単位(MTU) は 9,192 バイトで、特定のモデルでのみ使用できます。 Enable Jumbo Frame [ジャンボ フレームを有効にする] をオフにす ると、Global MTU [グローバルMTU] がデフォルトの 1,500 バイト に設定されます(範囲は 576~1,500)。

セッション設定	の意味
	 Enable Jumbo Frame(ジャンボ フレームを有効にする)をオンに すると、Global MTU(グローバル MTU)がデフォルトの 9,192 バイトに設定されます(範囲は 9,192 ~ 9,216 バイト)。
	ジャンボフレームは、通常のパケットと比較して最大5倍のメモリを消費し、利用可能なパケットバッファの数を20%削減できます。これにより、順不同、アプリケーション識別、およびその他のそのようなパケット処理タスク専用のキューサイズが削減されます。PAN-OS 8.1以降では、ジャンボフレームのグローバル MTU 設定を有効にしてファイアウォールを再起動すると、パケットバッファが再配信されてジャンボフレームをより効率的に処理します。
	ジャンボ フレームが有効で、インターフェイスに具体的な MTU が 設定されていない場合、それらのインターフェイスでは自動的にジャ ンボ フレームのサイズが継承されます。そのため、ジャンボ フレー ムを有効にする前に、ジャンボ フレームの使用を許可しないイン ターフェイスがある場合、その MTU を 1,500 バイトか別の値に設 定する必要があります。インターフェイス用に MTU を設定する場 合(Network(ネットワーク) > Interfaces(インターフェイス) > Ethernet(イーサネット))、「PA-7000 シリーズ レイヤー 3 イン ターフェイス」を参照してください。
DHCP Broadcast Session DHCP ブロー ドキャスト セッショ ン	ファイアウォールが DHCP サーバーとして機能している場合は、 このオプションを選択し、DHCP ブロードキャスト パケットのセッ ション ログを有効にします。DHCP ブロードキャスト セッションオ プションを使用すると、loT セキュリティその他のサービスで使用す る DHCP の拡張アプリケーション ログ(EALログ)を生成すること ができます。このオプションを有効にしない場合、ファイアウォール は DHCP ブロードキャスト パケットのログを作成せずにパケットを 転送します。
L3 & L4 ヘッダー イ ンスペクション	レイヤ3およびレイヤ4ヘッダー インスペクションをイネーブルに します。このオプションを選択すると、ゾーンプロテクションプロ ファイルを介してL3およびL4ヘッダーフィールドに基づいてカス タム脅威シグネチャを書き込み、特定のloT デバイスに存在する脆弱 性など、標準のシグネチャ更新では通常は対処されない脆弱性から防 御します。
	設定変更を有効にするには、firewallを再起動する必要 があります。

セッション設定	の意味
NAT64 IPv6 最 小MTU	IPv6 変換済みトラフィックのグローバル MTU を入力します。デフォ ルトの 1,280 バイトは、IPv6 トラフィック標準の最小 MTU に基づき ます(範囲は 1,280~9,216)。
NAT オーバーサブス クリプション率	DIPP NAT オーバー サブスクリプション率を選択します。これは、 ファイアウォールが同じ変換済み IP アドレスとポートのペアを同時 に使用できる回数です。オーバーサブスクリプション率を小さくす ると、送信元デバイス変換数が少なくなりますが、提供される NAT ルールのキャパシティは大きくなります。
	 Platform Default(プラットフォームのデフォルト) – オーバー サブスクリプション率の明示的な設定はオフになり、モデルの デフォルトのオーバー サブスクリプション率が適用されます。 ファイアウォール モデルのデフォルトの率については、https:// www.paloaltonetworks.com/products/product-selection.html を参 照してください。
	 1x-1回。これは、オーバー サブスクリプションがないことを意味します。ファイアウォールは、同時に同じ変換済み IP アドレスとポートペアを複数回使用することはできません。
	• $2x - 2 \square_{\circ}$ • $4x - 4 \square_{\circ}$ • $8x - 8 \square_{\circ}$
ICMP 到達不能パ ケット率/秒	ファイアウォールが1秒間に送信できる ICMP 到達不能応答の最大数 を定義します。この制限は、IPv4 パケットと IPv6 パケットで共有さ れます。
	デフォルト値は200メッセージ/秒です(範囲は1~65,535)。
セッション保持時間 自動短縮	アイドル状態のセッションの保持時間短縮を有効にします。
	セッション保持時間短縮を有効にして、しきい値(%)と倍率を設定 する場合はこのオプションを選択します。
	セッションテーブルが Accelerated Aging Threshold[セッション保 持時間短縮の開始しきい値] (% フル) に達すると、PAN-OS により Accelerated Aging Scaling Factor[セッション保持時間短縮倍率] がす べてのセッションのエージング計算に適用されます。デフォルトの短 縮倍率は 2 で、保持時間短縮が設定されているアイドル時間の 2 倍 の速さで行われます。設定されているアイドル時間を 2 で除算する と、タイムアウト時間が 1/2 に短縮されます。セッションの保持時 間短縮を計算するために、PAN-OS では、(そのセッションタイプ に)設定されているアイドル時間を短縮倍率で除算して、短縮された タイムアウトを決定します。

セッション設定	の意味
	例えば、短縮倍率が 10 の場合、通常は 3,600 秒後にタイムアウトするセッションが、10 倍速い 360 秒(1/10 の時間)でタイムアウトします。
	 保持時間短縮のしきい値を設定し、許容できるスケー リング要素を設定することで、セッション テーブルが 一杯になり始めた際にセッション テーブルの空きを素 早く作ります。
パケット バッファ保 護	PAN-OS 10.0 以降、パケット バッファ保護はデフォルトでグローバ ルおよび各ゾーンで有効化されています。パケット バッファ保護を グローバルおよび各ゾーンで有効化したままにして、ファイアウォー ルバッファを DoS 攻撃や攻撃的なセッションや送信元から保護する のがベスト プラクティスです。このオプションは、システム リソー スの不具合や正常なトラフィックがドロップされる原因となる不正な トラフィックや攻撃から、ファイアウォールの受信バッファを保護し ます。パケット バッファ保護は、問題のあるセッションを特定し、 ランダム早期検出 (RED) を防御の最前線として使用し、乱用が続く場 合はセッションを破棄するか、問題のある IPアドレスをブロックし ます。特定の IP アドレスから多量の小さいセッションもしくは急速 なセッション作成(またはその両方)をファイアウォールが検出した 場合、その IP アドレスをブロックします。
	ファイアウォール パケット バッファの使用率のベースラインを計測 してファイアウォールの能力を把握し、必ずファイアウォールのサイ ズが適切に設定されていることを確認し、攻撃以外ではバッファ使用 率が急増しないようにしてください。
	 Alert (%) (アラート(%)) – このしきい値をパケットバッファ の使用率が10秒より長い時間超えている場合、ファイアウォー ルはログイベントを毎分作成します。パケットバッファ保護が グローバルな範囲で有効になると、ファイアウォールがログイベ ントを生成します(範囲は0%~99%、デフォルトは50%)。値が 0%の場合、ファイアウォールはログイベントを作成しません。 デフォルトのしきい値から始め、必要に応じて値を調整します。
	 Activate (アクティベート) (%) – このしきい値に到達すると、ファ イアウォールは最も危険性の高いセッションの軽減を開始します (範囲は 0% ~ 99%、デフォルトは 80%)。値が 0% の場合、ファイ アウォールは RED を適用しません。デフォルトのしきい値から始 め、必要に応じて値を調整します。
Packet Buffer Protection(パケッ ト バッファ プロテク ション) (続く)	 (PAN-OS10.0 以降のリリースを実行するハードウェアファイア ウォール)使用率(上記)に基づくパケットバッファ保護の代わ りに、Buffering Latency Based(バッファリングレイテンシベー ス)を有効化して以下の設定を行うことにより、CPU 処理レイテ

セッション設定	の意味
	ンシに基づいてパケット バッファ保護をトリガーすることができ ます。
	 Latency Alert (milliseconds) (レイテンシ アラート (ミリ秒)) ーレイテンシがこのしきい値を超えると、ファイアウォール が毎分アラート ログ イベントの生成を開始します(範囲は 1~20,000、デフォルトは 50)。
	 Latency Activate (milliseconds) (レイテンシアクティブ化(ミリ 秒)) –レイテンシがこのしきい値を超えると、ファイアウォー ルが受信パケットの Random Early Detection (RED、ランダム 早期検出) をアクティベートし、10 秒毎にアクティベートログ の生成を開始します(範囲は 1~20,000 ミリ秒、デフォルトは 200 ミリ秒)。
	 Latency Max Tolerate (milliseconds) (レイテンシ最大許容値 (ミリ秒)) レイテンシがこのしきい値と同等または超えると、ファイアウォールがほぼ 100%のドロップ率で RED を使用します(範囲は 1~20,000 ミリ秒、デフォルトは 500 ミリ秒)。
	現在のレイテンシが、Latency Activate (レイテンシアクティ ベート) しきい値と、Latency Max Tolerate (レイテンシ最大許 容) しきい値の間の値である場合、ファイアウォールは RED ドロップ確率を以下のように計算します: (現在のレイテンシ - Latency Activate (レイテンシアクティベート) しきい値) / (Latency Max Tolerate (レイテンシ最大許容) しきい値 - Latency Activate (レイテンシアクティベート) しきい値)。例えば、現 在のレイテンシが 300 である場合、Latency Activate (レイテン シアクティベート) は 200、Latency Max Tolerate (レイテンシ 最大許容値) は 500であり、したがって (300-200)/(500-200) = 1/3となり、ファイアウォールは約 33%の RED ドロップ確率を 使用することになります。
Packet Buffer Protection(パケッ ト バッファ プロテク ション)(続く)	 Block Hold Time (ブロック保持時間) (秒)-セッションが廃棄される まで、または送信元 IPアドレスがブロックされ前にセッションの 継続が許可される時間 (秒単位) (範囲は 0 ~ 65,535、デフォルト は 60)。RED により軽減されたセッションをこのタイマーで監視 して、設定済みのしきい値を超えるバッファ使用率または遅延の プッシュが続いているかどうかを確認します。ブロック ホールド タイム経過後も不正な動作が継続する場合、セッションは廃棄さ れます。値が 0 の場合、ファイアウォールは、パケット バッファ 保護に基づくセッション廃棄を実施しません。デフォルトの値か ら始めてパケット バッファの使用率または遅延を監視し、必要に 応じて値を調整します。
	 Block Duration (フロック期間) (秒)-この時間 (秒) の間、廃棄され たセッションが廃棄されたままになるか、ブロックされた IPアド レスがブロックされたままとなります (範囲は 1 ~ 15,999,999、

セッション設定	の意味
	デフォルトは 3,600)。IPアドレスを1時間ブロックすることがビジネス条件のペナルティとして厳しすぎる場合を除き、デフォルト 値を使用してください。この場合、期間を短縮できます。パケットバッファの使用率または遅延を監視し、必要に応じて期間を調整します。
	ネットワークアドレス変換(NAT)により、パケッ トバッファの使用率が増加することがあります。これ によってバッファの使用率が影響を受ける場合は、ブ ロックホールドタイムを短くして個々のセッションを 早めにブロックしてブロック期間を減らし、背後のIP アドレスから来る他のセッションが不当にペナルティ を受けないようにします。
マルチキャストルートの設定バッファ	マルチキャストルートの設定バッファを有効化する場合はこのオプ ションを選択してください(デフォルトでは無効)。この機能は、対 応するマルチキャストグループにマルチキャストルートまたは転送 情報ベース(FIB)エントリが存在しない場合、マルチキャストセッ ションにおいてファイアウォールが最初のパケットを保存できるよう にするものです。デフォルト設定において、ファイアウォールは新し いセッションの最初のマルチキャストパケットのバッファを行わず、 代わりに、最初のパケットを使用してマルチキャストルートを確立し ます。これがマルチキャストトラフィックにおける通常の動作です。 コンテンツサーバーがファイアウォールに直接接続され、使用してい るカスタムアプリケーションがセッションの最初のパケットが破棄さ れているケースに対応できない場合にのみ、マルチキャストルートの 設定バッファを有効化する必要があります。
マルチキャストルー トの設定バッファサ イズ	マルチキャスト ルートの設定バッファを有効化した場合は、バッファ サイズを調整し、フローごとのバッファ サイズを指定することが可能です(範囲は 1 ~ 2,000、デフォルトは 1,000)。ファイアウォールは最大で5,000パケットをバッファすることができます。

セッション タイムアウト

セッションタイムアウト設定では、ファイアウォール上でセッションが非アクティブになって から PAN-OS がそのセッションを保持する期間を定義します。デフォルトでは、プロトコルの セッション タイムアウト期間が切れると、PAN-OS がセッションを閉じます。破棄セッション タイムアウトは、PAN-OS がセキュリティ ポリシー ルールに基づいてセッションを拒否した後 も、セッションが開いたままになる最大時間を定義します。

ファイアウォールでは、特に TCP、UDP、ICMP、および SCTP セッションに対して複数のタイ ムアウトを定義できます。他のすべてのタイプのセッションには、Default(デフォルト)のタ イムアウトが適用されます。これらのタイムアウトはすべてグローバルです。つまり、ファイア ウォール上にあるそのタイプのすべてのセッションに適用されます。

グローバル設定に加え、Objects(オブジェクト) > Applications(アプリケーション)タブで は個々のアプリケーションのタイムアウトを柔軟に定義できます。そのアプリケーションで使 用可能なタイムアウトは、Options [オプション] ウィンドウに表示されます。ファイアウォール は、アプリケーションのタイムアウトを確立済み状態のアプリケーションに適用します。アプリ ケーションのタイムアウトが設定されると、グローバルな TCP、UDP、または SCTP セッショ ンタイムアウトがオーバーライドされます。

このセクションのオプションを使用して、TCP、UDP、ICMP、および SCTP 固有の、ならびに その他すべてのタイプのセッションのグローバル セッション timeout settings(タイムアウト設 定)を定義します。

最適なのはデフォルトの値であり、デフォルトの値を使用することがベストプラクティスになり ます。ただし、ネットワークのニーズに合わせてこれらの値を変更できます。低すぎる値を設定 すると、わずかなネットワーク遅延に反応してファイアウォールとの接続の確立に失敗する可能 性があります。高すぎる値を設定すると、エラーの検出が遅れる可能性があります。

Session Timeouts Settings(セッション タイムアウト設定)	の意味
Reset Both [デフォル ト]	非 TCP/UDP、非 SCTP、または非 ICMP のセッションが応答なしで 開いた状態を維持できる最大秒数です(範囲は 1 ~ 15,999,999、デ フォルトは 30)。
デフォルトの破棄	ファイアウォールで設定されたセキュリティ ポリシー ルールに 基づき、PAN-OS がセッションを拒否した後に非 TCP / UDP / SCTP セッションが開いたままになる最大時間(秒単位)(範囲 は1~15,999,999、デフォルトは 60)。
TCP の破棄	ファイアウォールで設定されたセキュリティ ポリシー ルールに基づき、PAN-OS がセッションを拒否した後に TCP セッションが開いたままになる最大時間(秒単位)(範囲は1~15,999,999、デフォルトは 90)。
UDP の破棄	ファイアウォールで設定されたセキュリティ ポリシー ルールに基づき、PAN-OS がセッションを拒否した後に UDP セッションが開いたままになる最大時間(秒単位)(範囲は1~15,999,999、デフォルトは 60)。
ICMP	ICMP セッションが ICMP 応答なしで開いた状態を維持できる最大 時間です(範囲は 1 ~ 15,999,999、デフォルトは 6)。
スキャン	ファイアウォールがセッションをクリアし、セッションが使用して いたバッファ リソースを回復するまでに、セッションが非アクティ ブでいられる最長時間 (秒単位)。非アクティブ時間とは、セッショ

デバイス

Session Timeouts Settings(セッション タイムアウト設定)	の意味
	ンがパケットまたはイベントによって最後に更新されてから経過し た時間のことです。(範囲は 5 ~ 30、デフォルトは 10)
ТСР	TCP セッションが Established (確立済み)状態になってから(ハンドシェークが完了し、必要に応じてデータ伝送が開始してから)応答なしで開いた状態を維持する最大時間です(範囲は1~15,999,999、デフォルトは3,600)。
TCP ハンドシェーク	SYN-ACK を受信してからそれに続く ACK を送信してセッションを 完全に確立するまでの最大秒数です(範囲は 1 ~ 60、デフォルトは 10)。
TCP初期設定	SYN を受信してから SYN-ACK を送信して TCP ハンドシェーク タイ マーを開始するまでの最大秒数です(範囲は 1 ~ 60、デフォルトは 5)。
TCPハーフクローズド	1 つ目の FIN を受信してから 2 つ目の FIN または RST を受信するま での最大秒数です(範囲は 1 ~ 604,800、デフォルトは 120)。
TCP待ち時間	2 つ目の FIN または RST を受信してからの最大秒数です(範囲は 1 ~ 600、デフォルトは 15)。
未検証のRST	検証できない RST(RST が TCP ウィンドウ内にあるが予期しない シーケンス番号が付けられているか、RST が非対称パスから送信さ れている)を受信してからの最大秒数です(範囲は 1 ~ 600、デ フォルトは 30)。
UDP	UDP セッションが UDP 応答なしで開いた状態を維持する最大秒数 です(範囲は 1 ~ 1,599,999、デフォルトは 30)。
Authentication Portal(認証ポータ ル)	Authentication Portal (認証ポータル) Web フォームの認証セッ ションのタイムアウト秒数です(デフォルトは 30、範囲は 1 ~ 1,599,999)。要求されたコンテンツにユーザーがアクセスするに は、このフォームに認証資格情報を入力して正常に認証される必要 があります。 Authentication Portal (認証ポータル) Web フォームの認証セッ ションのタイムアウト秒数です(デフォルトは 30、範囲は 1 ~ 1,599,999)。要求されたコンテンツにユーザーがアクセスするに は、このフォームに認証資格情報を入力して正常に認証される必要
SCTP 初期化	アッシュン。 ファイアウォールが SCTP アソシエーションの開始を停止する前 に、ファイアウォールが INIT ACK チャンクを受信する必要がある

デバイス

Session Timeouts Settings(セッション タイムアウト設定)	の意味
	SCTP INIT チャンクを受信した最大時間(秒単位)(範囲は1~60、 デフォルトは 5)。
SCTP COOKIE	ファイアウォールが SCTP アソシエーションの開始を停止する前 に、ファイアウォールがクッキーを使用して COOKIE ECHO チャン クを受信する必要がある状態 COOKIE パラメータの SCTP INIT ACK チャンクを受信した最大時間(秒単位)(デフォルトは 60)。
SCTP の破棄	ファイアウォールで設定されたセキュリティ ポリシー ルールに基 づき、PAN-OS がセッションを拒否した後に SCTP アソシエーショ ンが開いたままになる最大時間(秒単位)(範囲は1~604,800、デ フォルトは 30)。
SCTP	アソシエーションのすべてのセッションがタイムアウトする前に、 アソシエーションの SCTP トラフィックなしで経過できる最大時間 (秒単位)(範囲は1~604,800、デフォルトは3,600)。
SCTP シャットダウン	ファイアウォールが SHUTDOWN チャンクを無視する前に SHUTDOWN ACK チャンクを受け取るために SCTP SHUTDOWN チャンクが待機した後にファイアウォールが待機する最大時間(秒 単位)(範囲は1~600、デフォルトは 30)。

TCP 設定

以下の表では、TCP 設定について説明します。

TCP 設定	の意味
TCP順序外キューを 超過するセグメント を転送	ファイアウォールがTCP順序外キュー上限(1つのセッションあた り64個)を超えるセグメントを転送するように設定したい場合はこ のオプションを選択してください。このオプションを無効化すると、 ファイアウォールは順序外キュー上限を超えるセグメントを破棄しま す。このオプションが有効であることによりファイアウォールが廃棄 したセグメント数を確認する場合は、以下の CLI コマンドを実行しま す。
	カウンターグローバ ル tcp_exceed_flow_seg_limit の表示

TCP 設定	の意味	
	このオプションはデフォルトで無効になっており、多 くのセキュアデプロイにおいては設定をそのままにし てください。このオプションを無効化すると、順序外 セグメントを64個以上を受信する特定のストリームで 遅延が発生する可能性があります。TCP スタックは欠 落しているセグメントのリトランスミッションを処理 するため、接続が失われることはありません。	
チャレンジ ACK を許 可する / SYN に応答 して任意の ACK を許 可する	このオプションを有効にすると、サーバーが SYN/ACK ではなく ACK を使用してクライアント SYN に応答する場合に、チャレンジ ACK (任意の ACK とも呼ばれます) への応答が許可されます。たとえ ば、チャレンジ ACK は攻撃の軽減を目的としてサーバーから送信で き、firewall でこの設定を有効にすると、クライアントとサーバー間 の通信が可能になり、ハンドシェイクが状態から外れたり順序がずれ たりしてもチャレンジ ACK プロセスを完了できます。	
タイムスタンプオプ ションを持たないセ グメントを破棄	TCPタイムスタンプにはセグメントの送信日時が記録されているの で、ファイアウォールはそのタイムスタンプがセッションに対して有 効であるかどうか確認できるので、TCPシーケンス番号のラッピング を防止することができます。TCPタイムスタンプはラウンドトリップ 時間の算出にも使用されます。このオプションが有効な場合、ファイ アウォールはタイムスタンプが Null のパケットを廃棄します。この オプションが有効であることによりファイアウォールが廃棄したセグ メント数を確認する場合は、以下の CLI コマンドを実行します。	
	カウンターのグローバ ル tcp_invalid_ts_option の表示	
	このオプションはデフォルトで有効になっており、多くのセキュアデプロイにおいては設定をそのままにしてください。このオプションを有効化するとパフォーマンスが低下するという訳ではありません。ただし、ネットワークスタックが誤って Null TCP タイムスタンプオプション値でセグメントを生成している場合、このオプションが有効であることで接続の問題が発生する可能性があります。	
非対称パス	同期していない ACK またはウィンドウ外のシーケンス番号を含むパ ケットをドロップするかバイパスするかをグローバルに設定します。	
	• Drop[ドロップ] – 非対称パスを含むパケットをドロップします。	
	 Bypass[バイパス] – 非対称パスを含むパケットでスキャンをバイ パスします。 	

TCP 設定	の意味
	 個々の Zone Protection Profiles の設定を制御するに は、TCP ドロップ の Asymmetric Path 設定を変更しま す。
緊急データフラグ	TCPヘッダーに含まれる緊急ポインター(URGビットフラグ)をファ イアウォールに許容させる場合はこのオプションを使用してくださ い。TCPヘッダー内の緊急ポインターは、パケットを即時に処理させ る場合に使用され、パケットが緊急ポインターを持つ場合、ファイア ウォールはパケットを処理キューから外し、ホストのTCP/IPスタッ クで迅速に処理を行います。この処理はアウトオブバンド処理と呼ば れます。
	緊急ポインターの実装はホストによって異なるため、このオプショ ンを Clear (クリア) に設定することで、アウトオブバンド処理を 却下し、処理の不画一性を排除できます(デフォルト、および推奨 設定)。ペイロード内のアウトオブバンドのバイトはペイロードの 一部となり、パケットの緊急処理は行われません。また、Clear (ク リア)に設定することで、プロトコルスタック内のストリームをパ ケットの宛先ホストとして、ファイアウォールに確実かつ正確に認識 させることができます。このオプションが Clear (クリア)に設定さ れている間にファイアウォールが URG フラグを削除したセグメント 数を確認する場合は、以下の CLI コマンドを実行します。
	カウンターのグローバル tcp_clear_urg を表示
	 デフォルトでは、このフラグは Clear (クリア) に設定 されており、多くのセキュア デプロイにおいては設定 をそのままにしてください。これはパフォーマンス低 下につながるものではありませんが、ごく稀に、telnet などのアプリケーションが緊急データ機能を使用して いるような場合は TCP に影響する可能性があります。 このフラグを Do Not Modify (編集不可) に設定する場 合、ファイアウォールは TCP ヘッダーに URG ビット フ ラグを持つパケットを許容し、アウトオブバンド処理 が有効化されます (非推奨)。
フラグを持たないセ グメントを破棄	フラグを持たない不正なTCPセグメントはコンテンツ検査の回避に使用される場合があります。このオプションが有効な場合(デフォルト)、ファイアウォールは TCP ヘッダーにフラグが設定されていないパケットを廃棄します。このオプションによりファイアウォールが廃棄したセグメント数を確認する場合は、以下の CLI コマンドを実行します。

TCP 設定	の意味	
	カウンターグローバル tcp_flag_zero の表示	
	 このオプションはデフォルトで有効になっており、 多くのセキュア デプロイにおいては設定をそのまま にしてください。このオプションを有効化するとパ フォーマンスが低下するという訳ではありません。し かし、TCPフラグを持たないセグメントをネットワー クスタックが誤って生成している場合、このオプショ ンを設定すると接続に問題が発生する可能性がありま す。 	
Strip MPTCP option(MPTCP オプ ションの削除)	(マルチパス TCP)MPTCP 接続を標準 TCP 接続への変換を実現する ために、デフォルトでグローバルに有効化されています。	
	MCTCP を許可するには、の Multipath TCP (MPTCP) オ プション 設定を変更します。	
SIP TCP cleartext(SIP TCP クリアテキスト)	以下のいずれかのオプションを選択して、セグメント化された SIP ヘッダ検出時の SIP TCP セッションのクリアテキスト プロキシの動 作を設定します。	
	 Always Off(常にオフ) – クリアテキスト プロキシを無効化します。SIP メッセージのサイズが通常 MSS よりも小さい場合、および SIP メッセージが単一のセグメント内に収まる場合、またはTCP プロキシリソースを SSL フォワード プロキシまたは HTTP/2向けに予約する必要がある場合は、プロキシを無効化します。 	
	 Always enabled(常に有効化) –デフォルト設定です。すべての SIP over TCP セッションに TCP プロキシを使用して、適切な ALG 操作のための TCP セグメントの適切な再構成および順序付けを支 援します。 	
	 Automatically enable proxy when needed (必要に応じてプロキシ を自動的に有効にする) –選択すると、ALG が SIP メッセージの フラグメンテーションを検出したセッションでクリアテキスト プ ロキシが自動的に有効になります。SSL フォワード プロキシまた は HTTP/2 にも使用される場合、プロキシの最適化につながりま す。 	
TCP 再送信スキャン (PAN-OS 10.0.2以降)	有効化すると、再送信されたパケットの検出時に、元のパケットの チェックサムがスキャンされます。元のパケットと再送信されたパ ケットのチェックサムが異なる場合、再送信されたパケットは悪意の あるものと見なされ、ドロップされます。	

復号化設定:証明書取り消しチェック

Session [セッション] タブのDecryption Settings [復号化設定] から**Certificate Revocation** Checking [証明書失効チェック] を選択し、以下の表に記載されているパラメータを設定しま す。

セッション機能:証明書取り 消しチェック設定	の意味
有効化:CRL	証明書無効リスト(CRL)方式を使用して証明書の失効状態を検 証する場合は、このオプションを選択します。
	オンライン証明書状態プロトコル (OCSP) も有効にしている場合、ファイアウォールは最初に OCSP を試行し、OCSP サー バーが使用できない場合は CRL 方式を試行します。
	復号化証明書の詳細は「Keys and Certificates for Decryption(復号化のキーと証明書)」を参照してください。
受信のタイムアウト:CRL	証明書失効状態の検証用に CRL 方式を有効にしている場合、 ファイアウォールが CRL サービスからの応答を待つ秒数(1~ 60、デフォルトは 5)を指定します。
有効化:OCSP	OCSPを使用して証明書の失効状態を検証する場合は、このオプ ションを選択します。
受信のタイムアウ ト:OCSP	証明書失効状態の検証用に OCSP 方式を有効にしている場合、 ファイアウォールが OCSP レスポンダからの応答を待つ秒数(1 ~ 60、デフォルトは 5)を指定します。
証明書の有効期限	ファイアウォールが任意の証明書状態サービスからの応答を待 機する秒数(1~60、デフォルトは5)を指定します。この期 間が終了すると、定義済みのセッションブロックロジックが必 要に応じて適用されます。Certificate Status Timeout[証明書の 有効期限]は、以下のように OCSP/CRL の Receive Timeout[受 信の有効期限]に関連付けられます。
	 OCSP および CRL の両方を有効化する場合 – ファイアウォー ルは、Certificate Status Timeout[証明書の有効期限] の値また は 2 つの Receive Timeout[受信の有効期限] の値の合計のい ずれか小さい方の期間の経過後に、要求のタイムアウトを登 録します。
	 OCSP のみを有効化する場合 – ファイアウォール は、Certificate Status Timeout[証明書の有効期限] の値また は OCSP の Receive Timeout[受信の有効期限] の値のいずれ か小さい方の期間の経過後に、要求のタイムアウトを登録し ます。

セッション機能:証明書取り 消しチェック設定	の意味
	 CRL のみを有効化する場合 – ファイアウォール は、Certificate Status Timeout[証明書の有効期限] 値または CRL の Receive Timeout[受信の有効期限] 値のいずれか小さい 方の期間の経過後に、要求のタイムアウトを登録します。

復号化設定:フォワード プロキシ サーバーの証明書設定

Decryption Settings(復号化設定)(Session(セッション)タブ)で、SSL Forward Proxy Settings(SSL 転送プロキシ設定)を選択し、SSL/TLS Forward Proxy(SSL/TLS 転送プロキ シ)復号化のセッションを確立する時の RSA Key Size(RSA キーのサイズ)または ECDSA Key Size(ECDSA キーのサイズ)およびファイアウォールがクライアントに対して作動する認証の ハッシュ アルゴリズムを設定します。以下の表で、パラメータについて説明します。

セッション機能:フォワ	ード プロキシ サーバーの証明書設定
RSA キーのサイズ	以下のいずれかを選択します。
	 Defined by destination host (宛先ホストによる定義) (デフォルト) – 宛先サーバーが使用する鍵に基づいてファイアウォールで 証明書を生成する場合は、このオプションを選択します。
	 宛先サーバーが RSA 1,024 ビット鍵を使用する場合、ファイア ウォールはその鍵のサイズと SHA1 ハッシュ アルゴリズムを使 用して証明書を生成します。
	 宛先サーバーが 1,024 ビットよりも大きい鍵のサイズを使用する場合(2,048 ビットや 4,096 ビットなど)、ファイアウォールは、2,048 ビット鍵と SHA-256 アルゴリズムを使用する証明書を生成します。
	 1024 ビット RSA: 宛先サーバーが使用するキーサイズに関係なく、RSA 1,024 ビット 鍵と SHA-256 ハッシュ アルゴリズムを使用する証明書をファイアウォールで生成する場合は、このオプションを選択します。2013 年 12 月 31 日以降、公開認証局(CA)と一般的なブラウザでは、2048ビット未満のキーを使用するX.509証明書のサポートが制限されています。将来的にブラウザでは、セキュリティの設定に応じて、このような鍵が提示された場合、ユーザーに警告を表示したり、SSL/TLS セッション全体をブロックしたりする可能性があります。
	 2048 ビット RSA(2048 ビット RSA) – 宛先サーバーが使用 する鍵のサイズに関係なく、PAN-OS で RSA 2048 ビット鍵と SHA256 アルゴリズムを使用する証明書を生成する場合は、 このオプションを選択します。公開 CA と一般的なブラウザで

セッション機能 : フォワ [、]	ード プロキシ サーバーの証明書設定
	は、2048 ビット鍵よりも強固なセキュリティを提供する 1024 ビット鍵がサポートされています。
ECDSA キーのサイズ	以下のいずれかを選択します。
	 Defined by destination host (宛先ホストによる定義) (デフォルト) – 宛先サーバーが使用する鍵に基づいてファイアウォールで 証明書を生成する場合は、このオプションを選択します。
	 宛先サーバーが ECDSA 256 ビットまたは 384 ビット鍵を使用 する場合、ファイアウォールはその鍵のサイズを使用して証明 書を生成します。
	 宛先サーバーが 384 ビットよりも大きい鍵のサイズを使用する 場合、ファイアウォールは、521 ビット鍵を使用する証明書を 生成します。
	 256 ビット ECDSA(256 ビット ECDSA) – 宛先サーバーが使用 する鍵のサイズに関係なくファイアウォールで ECDSA 256 ビット 鍵を使用する証明書を生成する場合は、このオプションを選択し ます。
	 384 ビット ECDSA(384 ビット ECDSA) – 宛先サーバーが使用 する鍵のサイズに関係なくファイアウォールで ECDSA 384 ビット 鍵を使用する証明書を生成する場合は、このオプションを選択し ます。

復号化設定:SSL復号化設定

ユーザーが復号化された HTTPS 接続を介して Web サイトに移動する場合は、[SSL 復号化設定 ~]を選択して SSL/TLS ハンドシェイク のインスペクションを有効にします。ファイアウォー ル上のコンテンツおよび脅威検出 (CTD) エンジンは、セキュリティ ポリシールールに対してハ ンドシェイクの内容を評価します。この機能を使用するには、URL フィルタリング サブスクリ プションを持ち、SSL フォワード プロキシ または SSL インバウンド インスペクション を構成 し、セキュリティ ポリシー ルールで特定の URL カテゴリをブロックする必要があります。

SSL/TLS ハンドシェイク検査中にブロックされたサイトの URL フィルタリング応答 ページは表示されません。ブロックされたカテゴリからのトラフィックを検出した 後、ファイアウォールは HTTPS 接続をリセットし、ハンドシェイクを終了し、応 答ページによるユーザー通知を防ぎます。代わりに、ブラウザは標準の接続エラー メッセージを表示します。

SSL復号化設定	の意味
検査用に CTD ヘハンドシェークメッセージ を送信	復号化された Web セッション中に CTD が SSL/TLS ハンドシェイクを検査できるように するには、このオプションを選択します。

VPN セッション設定

Session [セッション] を開き、VPN Session Settings [VPNセッション設定] から、VPNセッショ ンを確立するファイアウォールに関連するグローバル設定を指定します。以下の表では、この設 定について説明します。

VPN セッション設定	の意味
Cookie アクティベー ションのしきい値	ファイアウォールごとの IKEv2 ハーフオープン IKE SA の最大許容 数を指定します。これを超えると、Cookie の検証がトリガーされま す。ハーフオープン IKE SA の数が Cookie アクティベーションのし きい値を超えると、レスポンダが Cookie を要求し、イニシエータは Cookie が含まれる IKE_SA_INIT で応答する必要があります。Cookie の検証に成功すると、別の SA セッションを開始できます。 値を 0 にすると、Cookie の検証が常にオンになります。 グローバル ファイアウォール設定の Cookie Activation Threshold (Cookie アクティベーションのしきい値) は、同様にグ ローバル設定である Maximum Half Opened SA (ハーフ オープン SA の最大数) (範囲は 0 ~ 65535、デフォルトは 500) 未満とする必 要があります。
ハーフ オープン SA の最大数	応答を取得せずにイニシエータがファイアウォールに送信できる IKEv2 ハーフオープン IKE SA の最大数を指定します。最大数に達す ると、ファイアウォールは新しい IKE_SA_INIT パケットに応答しなく なります(範囲は 1 ~ 65535、デフォルトは 65535)。
キャッシュされた証 明書の最大数	ファイアウォールがキャッシュできる、HTTP 経由で取得したピア認 証局 (CA) 証明書の最大数を指定します。この値は、IKEv2 ハッシュ および URL 機能でのみ使用されます(範囲は 1 ~ 4000、デフォルト は 500)。

デバイス >セットアップ >ACE

App-ID Cloud Engine(ACE)を有効または無効にします。ACE は既定で無効になっていま す。ACE を有効にするには、チェック ボックスをクリックして、ACE が無効にならないように します。



Device (デバイス) > Setup (セットアップ) > DLP

• デバイス > セットアップ > DLP

Enterprise Data Loss Prevention (DLP) クラウド サービスにスキャンされたファイルのネット ワーク設定を構成します。

項目	の意味
最大待機時間 (秒)	ファイアウォールがアクションを実行するまでの ファイル アップロードの最大待機時間を秒単位 (1~ 240 の間) で指定します。デフォルトは 60 です。
最大待機時間に対するアクション	 ファイル アップロードの待機時間が構成された Max Latency に達したときにファイアウォールが実行する アクションを指定します。 許可(デフォルト) - 最大待機時間に達した場合、 ファイアウォールはファイルのアップロードを
	 DLP クラウド サービスに継続できます。 ● Block: 構成された最大待機時間に達した DLP クラ
	ウドサービスへのファイルアップロードがファイ アウォールによってブロックされます。
最大ファイルサイズ(MB)	DLP クラウド サービスにアップロードする最大ファ イル サイズ (1 と 20) を適用します。デフォルトは 20 です。
最大ファイル サイズに対するアク ション	ファイルアップロードが設定された Max ファイル サ イズ に達したときにファイアウォールが実行するア クションを指定します。
	 許可(デフォルト) - ファイルが構成されている最大 ファイル サイズである場合、ファイアウォールは ファイルのアップロードを DLP クラウド サービ スに継続できます。
	 Block: ファイルが構成されている最大ファイル サイズである場合、ファイアウォールは DLP クラウド サービスへのファイルアップロードをブロックします。
ログファイルがスキャンされない	ファイルを DLP クラウド サービスにアップロードで きなかった場合に、データ フィルター ログにアラー トを生成する場合は、チェック (有効) します。

項目	の意味
任意のエラーに対するアクション	DLP クラウド サービスへのファイルアップロード中 にエラーが発生したときにファイアウォールが実行 するアクションを指定します。
	 許可(デフォルト) - アップロード中にエラーが発生した場合、ファイアウォールはファイルのアップロードを DLP クラウド サービスに継続できます。
	 Block: アップロード中にエラーが発生した場合、 ファイアウォールは DLP クラウド サービスへの ファイルアップロードをブロックします。

Device > High Availability [デバイス > 高可用性]

• Device > High Availability [デバイス > 高可用性]

冗長性確保のため、Palo Alto Networks 次世代ファイアウォールは、HA ペアあるいは HA クラ スタの high availability(高可用性■設定でデプロイします。2 つの HA ファイアウォールが HA ペアとして機能する場合、2 種類の HA 展開が可能です。

- active/passive (アクティブ/パッシブ) このデプロイ環境では、アクティブピアは2つの専用インターフェイスを通じて、設定内容とセッション情報をパッシブピアへ継続的に同期させます。アクティブなファイアウォールのハードウェアまたはソフトウェアにおいて障害が発生した場合、サービスを停止させることなく、パッシブなファイアウォールが自動的にアクティブに切り替わります。アクティブ/パッシブのHA導入環境は、バーチャルワイヤー、レイヤー2、またはレイヤー3のすべてのインターフェイスモードでサポートされています。
- active/active(アクティブ/アクティブ) このデプロイ環境では、両方のHAピアがアク ティブに設定されトラフィックの処理を行います。このような導入環境は非対称的なルー ティングを行っている場合や、動的ルーティングプロトコル(OSPF、BGP)に両方のピアを アクティブに保たせたい場合に適しています。アクティブ/アクティブHAは、バーチャルワ イヤーモードとレイヤー3モードのみにおいてサポートされます。アクティブ/アクティブの 導入環境では、HA1リンクとHA2リンクに加え、専用のHA3リンクが必要です。HA3リンク は、セッションセットアップと非対称トラフィック処理用のパケット転送リンクとして使用 されます。
 - HAペアでは、両方のピアが同じモデルで同じバージョンのPAN-OSおよびコンテンツリリースを実行し、同じセットのライセンスを使用している必要があります。

また、VM-Series ファイアウォールの場合、両方のピアが同じハイパーバイザに 存在していて、各ピアに同じ数の CPU コアが割り当てられている必要がありま す。

サポート対象ファイアウォールモデルでは、データセンター内およびデータセンター間セッションの存続可能性を目指し、HAファイアウォールのクラスタを作成することが可能です。リンクがダウンした場合、セッションはクラスタ内の別のファイアウォールにフェイルオーバーします。この同期は、複数のデータセンターに HA ピアが分散している場合、アクティブなデータセンターとスタンバイ データセンター間に HA ピアが分散している場合に役立ちます。別のユースケースに水平スケーリングがあります。このユースケースでは、HA クラスタ メンバーを単一のデータセンターに追加してセキュリティをスケーリングし、セッションの存続可能性を確保します。HA ペアは HA クラスタに所属させることが可能であり、この場合、クラスタ内の 2 つのファイアウォールとしてカウントされます。HA クラスタでサポートされるファイアウォールの数は、ファイアウォールのモデルによって異なります。

- HA 設定時の重要事項
- HA 一般設定
- HA 通信
- HA リンクおよびパス モニタリング

- HA Active/Active Config(HA アクティブ/アクティブ 設定)
- Cluster Config (クラスタ設定)

HA 設定時の重要事項

以下は、HAペアを構成する上での重要な考慮事項です。

- ローカル IP とピア IP に使用するサブネットは、仮想ルーターの他の場所で使用しないでください。
- それぞれのファイアウォールのOSとコンテンツリリースのバージョンは一致している必要が あります。一致していない場合はファイアウォールの同期が阻害される恐れがあります。
- HA ポートの LED は、アクティブ ファイアウォールが緑、パッシブ ファイアウォールが黄色 になります。
- ローカルファイアウォールとピアファイアウォールの設定を比較するには、Device[デバイス]タブのConfig Audit[設定監査] ツールを使用し、左の選択ボックスで対象のローカル設定を、右の選択ボックスでピア設定を選択します。
- Webインターフェイスからファイアウォールを同期する場合は、Dashboard[ダッシュボード]のHAウィジェットにある Push Configuration[設定をプッシュ]をクリックします。プッシュを行うファイアウォールの設定内容が、ピアファイアウォールの設定内容に上書きされます。アクティブファイアウォールのCLIからファイアウォールを同期する場合は、コマンド「request high-availability sync-to-remote running-config」を使用します。
 - 10ギガビットのSFP+ポートを使用するファイアウォールの高可用性(HA)ア クティブ/パッシブ設定では、フェイルオーバーが発生してアクティブファイア ウォールがパッシブ状態になる際に、10ギガビットEthernetポートを一度ダウン させてから再度開通させることでポートが更新されますが、ファイアウォール が再度アクティブになるまで送信機能は有効になりません。隣接するデバイスで ソフトウェアをモニターしている場合、ポートがダウンしてから再度開かれてい るため、ポートのフラッピングが発生していると見なされます。これは、1ギガ ビット Ethernet ポートなどの他のポートとは異なる動作です。他のポートでは無 効になった場合でも送信は許可されるため、隣接するデバイスでフラッピングは 検出されません。

HA一般設定

• Device (デバイス) > High Availability (高可用性) > General (一般)

高可用性(HA)ペアまたは HA クラスタ メンバーを設定するには、まず**Device**(デバイス) > High Availability(高可用性) > General(一般)を選択し、一般設定を行います。

高可用性の設定	の意味
General [全般] タブ	
HA Pair Settings(HA	Enable HA Pair(HA ペアを有効化)して HA ペアの機能をアクティ ベートし、以下の設定を行います。

高可用性の設定	の意味
ペアの設定)— Setup (セットアッ プ)	 Group ID[グループID] – HAペアの識別に使用する数値(1~63)を 入力します。このフィールドは複数のHAペアが同じブロードキャ ストドメインに存在する場合に設定が必須(かつ一意である必要が あります)となります。
	 Description(内容) – (任意) HA ペアの説明を入力します。
	 Mode[モード] – HA導入環境のタイプを設定します。Active Passive [アクティブ/パッシブ] またはActive Active [アクティブ/ア クティブ]
	 Device ID[デバイスID] – アクティブ/アクティブの設定の場合、デバイスIDを設定し、アクティブ-プライマリのピア(Device ID[デバイスID] を0に設定)とアクティブ-セカンダリのピア(Device ID[デバイスID]を1に設定)を設定します。
	• Enable Config Sync[設定の同期を有効化] – 設定内容をピア間で同期させる場合はこのオプションを選択します。
	構成の同期を有効化して、両方のデバイスが常に同じ設定となり、トラフィックを同じ方法で処理する設定にします。
	 Peer HA1 IP Address[ピアHA1のIPアドレス] – ピアファイアウォー ルのHA1インターフェイスのIPアドレスを入力します。
	 Backup Peer HA1 IP Address (バックアップ側ピア HA1 の IP アドレス) – ピアのバックアップ制御リンクの IP アドレスを入力します。
	 バックアップ ピア HA1 の IP アドレスを設定し、プラ イマリ リンクが失敗した場合でもバックアップ リン クが各ファイアウォールを同期させて最新の状態を保 つ設定にします。
アクティブ/パッシ ブ設定	 Passive Link State[パッシブリンクの状態] – 以下のうち1つを選択し、パッシブなファイアウォールのデータリンクの接続状態を保つかどうかを指定します。このオプションは AWS の VM-Series ファイアウォールでは使用できません。
	 shutdown(シャットダウン) –強制的にインターフェース リ ンクをダウン状態にします。これはデフォルトのオプション です。このオプションでは、ネットワークにループが起きません。
	 auto(自動) –物理的に接続されたリンクは、物理的には接続 中であっても無効化された状態を維持し、ARP 学習やパケット 転送には参与しません。接続が再開されるまでの時間が短縮さ れるので、フェイルオーバー中の収束時に役立ちます。ネット

高可用性の設定	の意味
	ワークループを防ぐため、ファイアウォールにレイヤー2イン ターフェイスが設定されている場合はこのオプションを選択し ないでください。
	 ファイアウォールにレイヤー2インターフェイスが設定されていない場合、Passive Link State (パッシブリンク状態)をauto (自動)に設定します。
	 Monitor Fail Hold Down Time (min) (分単位でのモニター障害時ホールドダウンタイム) -この値(1~60分)で、ファイアウォールがパッシブになる前に非稼働状態で待機する間隔を指定します。このタイマは、リンクまたはパスモニタリングの障害が原因でハートビートおよび hello メッセージが届かない場合に使用します。
選択設定	以下の設定を指定または有効化します。
	 Device Priority[デバイス優先度] – アクティブ ファイアウォールの 識別に使用する優先度の値を入力します。ペアの両方のファイア ウォールでプリエンプティブ機能が有効になっている場合、値が 低い(優先順位が高い)ファイアウォールがアクティブ ファイア ウォール(範囲は0~255)になります。 Preemptive(プリエンプティブ) – 優先順位の高いファイアウォー ルが障害から回復した後にアクティブ(アクティブ/パッシブ)あ るいはアクティブ-プライマリ(アクティブ/アクティブ)で動作を 再開することを有効化します。優先度値の高いファイアウォール の障害回復時に、アクティブまたはアクティブ-プライマリのファ イアウォールとしての動作を再開可能にするには、両方のファイア ウォールでプリエンプティブ オプションを有効化する必要がありま す。この設定が無効化の場合、優先度の高いファイアウォールが障 害から回復した後も、優先度が低いファイアウォールがアクティブ あるいはアクティブ-プライマリのまま動作します。
	 Preemptive (プリエンプティブ)オプションを有効化 するかどうかは、ビジネス要件によって異なります。 プライマリデバイスをアクティブデバイスとする必 要がある場合はPreemptive (プリエンプティブ)を 有効化し、失敗から回復した後、プライマリデバイ スがセカンダリデバイスに取って代わる設定にしま す。フェイルオーバーのイベントを最小限に減らす必 要がある場合はPreemptive (プリエンプティブ)オプ ションを無効化し、フェイルオーバー後に HA ペアに 再度フェイルオーバーさせずに、優先順位の高いファ イアウォールをプライマリファイアウォールにしま す。
高可用性の設定	の意味
---------	--
	 Heartbeat Backup[ハートビートバックアップ] – HAファイア ウォールで管理ポートを使用して、ハートビートおよびhelloメッ セージのバックアップパスを提供します。管理ポートの IP アドレ スは、HA ピアと HA1 制御リンク経由で共有されます。追加の設定 は必要ありません。
	 HA1 および HA1 バックアップ リンクに対してインバンド ポートを使用する場合はHeartbeat Backup (ハートビート バックアップ)を有効化します。HA1 あるいは HA1 バックアップ リンクに対して管理ポートを使用する場合はHeartbeat Backup (ハートビート バックアップ)を有効化しないでください。
	 HA Timer Settings(HA タイマー設定) –以下のいずれかの事前設 定プロファイルを選択します。
	 Recommended[推奨]:一般的なフェイルオーバータイマー設定 で使用します。別の設定が必要であることが確実な場合を除 き、Recommended (推奨)設定を使用することがベストプラク ティスになります。
	 Aggressive[アグレッシブ]:フェールオーバータイマー設定を高速 化するために使用されます。
	プロファイルに含まれる個々のタイマーのプリ セット値を表示するには、Advanced[詳細] および Load Recommended(推奨をロード)または Load Aggressive(アグレッシブをロード)を選択しま す。ハードウェアモデルの事前設定が画面に表示 されます。
	 Advanced[詳細]:以下の各タイマーに対して、ネットワーク要件 に合わせて値をカスタマイズできます。
	 Promotion Hold Time (ms) (ミリ秒単位のプロモーションホー ルドタイム) –パッシブピア (アクティブ/パッシブモードの場 合) またはアクティブ-セカンダリピア (アクティブ/アクティブ モードの場合) が、HA ピアとの通信が失われた後でアクティブ ピアまたはアクティブ-プライマリ ピアの役割を引き継ぐまでに 待機する時間をミリ秒単位で入力します。このホールド タイム は、ピアの障害宣言後にのみ開始されます。
	 Hello Interval (Hello間隔) –もう一方のファイアウォールの HA プログラムが動作していることを確認するための hello パケット の送信間隔をミリ秒単位で入力します(範囲は8,000~60,000、 デフォルトは8,000)。

高可用性の設定	の意味
	 Heartbeat Interval (ハートビート間隔) – HA ピアが ICMP ping の形式でハートビート メッセージを交換する頻度を指定します (範囲は1,000~60,000ミリ秒、デフォルトなし)。
	 Flap Max (最大フラップ) –フラップは、ファイアウォールが前回の非アクティブ状態発生から 15 分以内に再び非アクティブ状態になるとカウントされます。最大許容フラップ数を指定することができます(範囲は 0~16、デフォルトは 3)。フラップ数がこの最大数に達するとファイアウォールがサスペンドしたと判断され、パッシブファイア ウォールに引き継がれます。値 0を指定すると最大数は設定されません (何回フラップが発生してもパッシブ ファイアウォールは引き継がない)。
	 Preemption Hold Time (プリエンプション ホールド タイム) –パッシブ ピアまたはアクティブ・セカンダリ ピアがアクティブ ピアまたはアクティブ・プライマリ ピアとしての役割を引き継ぐまでの待機時間を分単位で入力します(範囲は 1~60、デフォルトは 1)。
	 Monitor Fail Hold Up Time (ms) (ミリ秒単位のモニター障害時ホールドアップタイム) パスモニターまたはリンクモニターに障害が発生した後にファイアウォールがアクティブ状態を維持する時間を指定します。隣接するデバイスの偶発的なフラッピングによる HAのフェイルオーバーを回避するためには、この設定が推奨されます(範囲は 0~60,000、デフォルトは 0)。
	 Additional Master Hold Up Time (ms) (ミリ秒単位の追加のマス ターホールドアップタイム) –Monitor Fail Hold Up Time (モニ ター障害時ホールドアップタイム) と同じイベントで適用される 追加の時間をミリ秒で指定します(範囲は0~60,000、デフォル トは 500)。追加の時間間隔は、アクティブ/パッシブモードのア クティブピアとアクティブ/アクティブモードのアクティブなプラ イマリピアにのみ適用されます。両方のピアで同じリンクまたはパ スモニターの障害が同時に発生した場合にフェイルオーバーを回避 するには、このタイマーを設定することが推奨されます。
SSH HA Profile Setting(SSH HA プ ロファイルの設定)	ネットワーク上の高可用性(HA)アプライアンスの SSH セッション に適用される SSH サービス プロファイルの種類の一つです。既存の HA プロファイルを適用するには、プロファイルを選択して、OK をク リックし、変更をCommit(コミット)します。
	プロファイルをアクティブにするには、CLIから SSH サービスの再始動を実行する必要があります。

高可用性の設定	の意味
	詳細については、Device(デバイス) > Certificate Management(証 明書の管理) > SSH Service Profile(SSH サービス プロファイル)を 参照してください。
Clustering Settings(クラスタ 化の設定)	クラスタ化の設定にアクセスするには、Enable Cluster Participation(クラスタ酸化を有効化)を実行します。HA クラスタ 化をサポートするファイアウォールは、メンバー ファイアウォール (ペアの個々のファイアウォールが合計にカウントされる個人または HA ペア)のクラスタを許可します。ファイアウォールのモデルがサ ポートするクラスタ毎のメンバー数は以下の通りです。
	 ● PA-3200 シリース:6 メンバー ● PA-5200 シリーズ:16 メンバー
	● PA-54508 メンバー
	• PA-7080 シリーズ:4 メンバー
	● PA-7050 シリーズ:6 メンバー
	クラスターの設定:
	 Cluster ID (クラスタ ID) を入力します。これはすべてのメンバーが セッション状態を共有することができる HA クラスタの一意の数値 ID です。(範囲は 1~99、デフォルトなし)。
	 Cluster Description (クラスタの説明) – クラスタの簡潔かつ役に 立つ説明。
	 Cluster Synchronization Timeout (min) (分単位のクラスタ同期タイ ムアウト) – (状態が不明であるため等)別のクラスタメンバー がクラスタの完全な同期を妨げている場合に、ローカルファイア ウォールがアクティブ状態になるまで待機する最大時間を分で指定 します (範囲は 0~30、デフォルトは0)。
	 Monitor Fail Hold Down Time (min) (分単位のモニター障害時ホー ルドダウンタイム-ダウンリンクがバックアップ済かを確認する ために再テストされるまでの時間(分)(範囲は1~60、デフォル トは1)。
操作コマンド	1

ローカルデバイスを サスペンド	ローカル HA ピアを一時停止状態にし、ファイアウォールの HA 機能 を一時的に無効にするには、以下の CLI 操作コマンドを使用します。
(またはローカルデ バイスを稼動状態に する)	• 高可用性状態の一時停止を要求する
	中断したローカル HA ピアを機能状態に戻すには、この CLI 操作コマ ンドを使用します。
	• 高可用性状態の機能を要求する

高可用性の設定	の意味
	フェイルオーバーのテストには、アクティブ(またはアクティブ-プラ イマリ)ファイアウォールの接続ケーブルを外します。

HA 通信

• Device (デバイス) > High Availability (高可用性) > HA Communications (HA 通信)

HA ペアまたは HA クラスタ化の HA リンクを設定するには、**Device**(デバイス) > **High** Availability(高可用性) > HA Communications(HA 通信)を選択します。

コントロールリン クHA ペアのファイアウォールでは、HA リンク で(HA1) /コン トロールリンク (HA1 バックアップ)を使用してデータを同期し、状態情報を管理します。専用の制御リンク および専用のバックアップ制御リンクを持っているファイアウォールの モデルもあります。例えば、PA-5200 Series ファイアウォールは HA1- A と HA1-B を持っています。この場合、Elections Settings (選出設定) で Heartbeat Backup (ハートビート バックアップ) オプションを有効化 する必要があります。制御リンク HA リンクに専用 HA1 ポートを使用 し、制御リンク (HA バックアップ)にデータ ポートを使用している場合 は、Heartbeat Backup (ハートビート バックアップ) オプションを有効に することをお勧めします。PA-220ファイアウォールなど専用のHAポートがないファイアウォー ルの場合は、制御リンク HA 投入アップと シランを有効にする必要があります。この場合、管理ポートが使 用されているため、Heartbeat Backup (ハートビートバックアップ) オプ ションを有効にする必要があります。この場合、管理ポートが使 用されているため、Heartbeat Backup (ハートビートバックアップ) オプ ションを有効にする必要はありません。ハートビートバックアップは管 理インターフェイス接続を使用して行われるためです。AWS の VM-Series ファイアウォールでは、管理ポートが HA1 リンクと して使用されます。()HA制御リンクにデータポートを使用する場合、制御メッ セージはデータプレーンの時 音が発生すると、ビア間 でHA制御リンク情報を通信することができず、フェイル オーバーが発生します。最善策は専用のHAポートを使用 することですが、専用のHAポートがないファイアウォール ルでは管理ポートを使用します。	HAリンク	の意味
	コントロール リン ク (HA1) /コン トロールリンク (HA1 バックアッ プ)	 HAペアのファイアウォールでは、HAリンク を使用してデータを同期し、状態情報を管理します。専用の制御リンク および専用のバックアップ制御リンクを持っているファイアウォールの モデルもあります。例えば、PA-5200 Series ファイアウォールは HA1- A と HA1-B を持っています。この場合、Elections Settings (選出設定) で Heartbeat Backup (ハートビート バックアップ) オプションを有効化 する必要があります。制御リンク HA リンクに専用 HA1 ポートを使用 し、制御リンク (HA バックアップ) にデータ ポートを使用している場合 は、Heartbeat Backup (ハートビート バックアップ) オプションを有効に することをお勧めします。 PA-220ファイアウォールなど専用のHAポートがないファイアウォー ルの場合は、制御リンクHA接続に管理ポートを設定し、制御リン クHA1バックアップ接続にタイプをHAに設定したデータポートイン ターフェイスを設定する必要があります。この場合、管理ポートが使 用されているため、Heartbeat Backup (ハートビートバックアップ) オプ ションを有効にする必要はありません。ハートビートバックアップ) オプ ションを有効にする必要はありません。ハートビートバックアップは管 理インターフェイス接続を使用して行われるためです。 AWS の VM-Series ファイアウォールでは、管理ポートが HA1 リンクと して使用されます。 HA制御リンクにデータポートを使用する場合、制御メッ セージはデータプレーンから管理プレーンに通信する必要 があるため、データプレーンで障害が発生すると、ピア間 でHA制御リンク情報を通信することができず、フェイル オーバーが発生します。最善策は専用のHAポートを使用 することですが、専用のHAポートがないファイアウォー ルでは管理ポートを使用します。

HAリンク	の意味
コントロール リン ク	アクティブ/パッシブ HA を設定する場合、またはアクティブ/アクティ ブ HA を設定する場合は、プライマリ HA 制御リンクとバックアップ HA 制御リンクに次の設定を指定します。
トロールリンク (HA1 バックアッ	 Port[ポート] – プライマリおよびバックアップの HA1 インターフェイスの HA ポートを選択します。バックアップの設定は任意です。
プ)	 IPv4/IPv6 Address[IPv4/IPv6 アドレス] – プライマリおよびバック アップの HA1 インターフェイスとなる HA1 インターフェイスの IPv4 または IPv6 アドレスを入力します。バックアップの設定は任意 です。
	PA-3200 シリーズのファイアウォールはバックアップ HA1 インターフェイス用の IPv6 アドレスをサポートしていないため、IPv4 アドレスを使用してください。
	 Netmask(ネットマスク) – プライマリおよびバックアップの HA1 インターフェイスの IP アドレスのネットワーク マスク(たとえば、 「255.255.255.0」)を入力します。バックアップの設定は任意で す。
	 Gateway[ゲートウェイ] – プライマリおよびバックアップの HA1 イ ンターフェイスのデフォルト ゲートウェイの IP アドレスを入力しま す。バックアップの設定は任意です。
	 Link Speed[リンク速度] – (専用 HAポートをもつモデルのみ)専用のHA1ポートにおけるファイアウォール間の制御リンクの速度を選択します。
	 Link Duplex[リンクデュプレックス] – (専用HAポートをもつモデルのみ) – 専用のHA1ポートにおけるファイアウォール間の制御リンクのデュプレックスオプションを選択します。
	 Encryption Enabled[暗号化を有効化] – HAキーをHAピアからエクス ポートしてこのファイアウォールにインポートした後で、暗号化を 有効にします。さらに、このファイアウォールのHAキーは、一度エ クスポートを行いHAピアにインポートする必要があります。プライ マリ HA1 インターフェイスについてこの設定を行います。キーのエ クスポートとインポートは証明書ページで行います(「Device(デ バイス) > Certificate Management(証明書の管理)> Certificate Profile(証明書プロファイル)」を参照)。
	 ファイアウォールが直接接続されていない際の暗号化 を有効にします(HA1 接続はトラフィックを検査、 処理、捕捉できるネットワーク デバイスを通過しま す)。
	 Monitor Hold Time (ms) (ホールド タイムのモニター (ミリ秒単位)) – 制御リンク障害によるピア障害を宣言するまでにファイア ウォールが待機する時間 (ミリ秒) を入力します (範囲は 1,000 ~

HAリンク	の意味
	60,000 ミリ秒、デフォルトは 3,000 ミリ秒)。このオプションは HA1 ポートの物理リンクの状態をモニターします。
データ リンク (HA2)	プライマリおよびバックアップデータリンクに次の設定を指定しま す。アクティブ/パッシブHAを設定するか、アクティブ/アクティ ブHAを次の通り設定します。

キレ

HAリンク	の意味
● HA2ッッッ ク設さてる、理ン障がる合 2ッ ッ ンのアルーー発し 「HA2ックアプリンが定れいと物リク害あ場はHバクアプリクフィオバが生ますキプラブオシンが効さてす HA2 の リングアプリンが定れいと物リク害あ場はHバクアプリクフィオバが生ますキプラブオシンが効さてす HA2 の いちょう (HA2 の) (HA2 0) (HA2 0	 Port[ポート] – HA ポートを選択します。プライマリおよびバック アップの HA2 インターフェイスについてこの設定を行います。バッ クアップの設定は任意です。 IP Address[IP アドレス] – プライマリおよびパックアップの HA2 イ ンターフェイスとなる HA インターフェイスの IPv4 または IPv6 アド レスを指定します。バックアップの設定は任意です。 Netmask[ネットマスク] – プライマリおよびパックアップの HA2 イ ンターフェイスとなる HA インターフェイスのネットワーク マスク を指定します。パックアップの設定は任意です。 Gateway[ゲートウェイ] – プライマリおよびパックアップの HA2 インターフェイスとなる HA インターフェイスのデフォルトゲー トウェイを指定します。パックアップの設定は任意です。ファイア ウォールのHA2 IPアドレスが同じサブネット 上にある場合、[ゲート ウェイ] フィールドは空白のままにしておく必要があります。 Enable Session Synchronization[セッション同期を有効にする] - セッ ション情報をパッシブ ファイアウォールと同期できるようにし、転 送オプションを選択します。 セッション回期を有効化し、セカンダリ デバイスが データプレーン内でセッションを保持し、ファイア ウォールが同期済みのセッションにパケットをマッ チさせて素早くパケットを転送できるようにします。 セッション同期を有効化しない場合はファイアウォー ルがセッションを再作成しなければならないため、遅 延が生じて接続がドロップされるおそれがあります。
る場	NJVプ 11.1 943 [©] 2024 Palo Alto Networks, Inc.
たし	

HA リンク	の意味
	• Transport[転送] – 以下のいずれかの転送オプションを選択します。
	 Ethernet[イーサネット] –ファイアウォールが逆並列で接続されているかスイッチを介して接続されている場合に使用します (Ethertype 0x7261)。
	 IP-レイヤー3転送が必要な場合に使用します (IP プロトコル番号 99)。
	 UDP-IP オプションでの場合と同じように、チェックサムがヘッ ダーのみではなくパケット全体に基づいて計算されることを利用 するために使用します (UDP ポート 29281)。UDPモードの利点 はUDPチェックサムにあり、セッション同期メッセージの整合性 を検証することができます。
	 (専用 HA ポートを備えるモデルのみ)Link Speed (リンク速度)[リンク速度] – 専用の HA2 ポートにおけるピア間の制御リンクの速度を選択します。
	 (専用HAポートをもつモデルのみ) Link Duplex (リンクデュプレックス) – 専用の HA2 ポートのピア間の制御リンクにデュプレックスオプションを選択します。
	 HA2 keep-alive(HA2 キープアライブ) – HA ピア間のHA2 データ リンクの健康状態の監視を有効化するには、このオプションを選択す ることがベストプラクティスになります。このオプションはデフォル トで無効化されていますが、片方、あるいは両方のピアで有効化する ことができます。有効化した場合、ピアはキープアライブメッセージ を使用してHA2接続をモニターし、設定したThreshold[しきい値]に 従って障害を検知します(デフォルトは10,000ミリ秒)。HA2キー プアライブを有効化した場合、HA2キープアライブ復旧アクションが 行われます。Action[アクション]を選択します。
	 Log Only[ログのみ] – HA2インターフェイスの障害を、重要イベントとしてシステムログに記録します。アクティブ/パッシブのデプロイ環境の場合、トラフィックを転送するファイアウォールはアクティブなピアのみなので、このオプションを選択してください。パッシブなピアはバックアップ状態にあり、トラフィックを転送していないため、スプリットデータパスは不要です。HA2バックアップリンクを設定していない場合、状態の同期は無効になっています。HA2パスが回復すると、情報ログが生成されます。
	 Split Datapath[スプリットデータパス] – アクティブ/アクティブのHAデプロイ環境の場合はこのオプションを選択し、それぞれのピアに対し、HA2インターフェイスの障害を検知した際はそれぞれのローカルステートとセッションテーブルの所有権を取るよう指示します。HA2の接続が無い場合、状態の同期とセッションの同期は行われません。同期とは、セッションテーブルを個別に管

HAリンク	の意味
	理し、各HAピアからのトラフィックの転送を正常に行えるように するためのものです。この状態を防ぐために、HA2バックアップ リンクを設定してください。
	 Threshold (ms) (しきい値(ミリ秒)) – キープアライブ メッセージ が失敗し、上記のいずれかのアクションがトリガーされるまでの期間 (範囲は 5,000 ~ 60,000 ミリ秒、デフォルトは 10,000 ミリ秒)。
Clustering Links(リンクのク ラスタ化)	HAクラスタリングを設定する場合、HA4 リンクの設定を行いま す。HA4 リンクは、同じクラスタ ID を持つすべてのクラスタ メンバー 間でセッション状態を同期する専用のクラスタ リンクです。クラスタ メンバー間の HA4 リンクは、クラスタ メンバー間の接続障害を検出し ます。
	 Port(ポート) – HA4 リンクとなる HA インターフェースを選択します(例えば、ethernet1 / 1等)
	 IPv4/IPv6 Address(IPv4 または IPv6 アドレス) – ローカル HA4 イ ンターフェースの IPアドレスを入力します。
	• Netmask(ネットマスク)–ネットマスクを入力します。
	 HA4 Keep-alive Threshold (ms) (HA4 キープアライブの秒単位のしき い値–ファイアウォールがクラスタメンバーからキープアライブを受 信し、クラスタメンバーが機能していることを確認すべき時間の長 さ(範囲は 5,000~60,000、デフォルトは 10,000)。
	Configure HA4 Backup settings(HA4 バックアップの設定):
	 Port(ポート) – HA4 バックアップリンクとなる HA インター フェースを選択します。
	 IPv4/IPv6 Address(IPv4 または IPv6 アドレス) – ローカル HA4 バックアップ リンクのアドレスを入力します。
	• Netmask(ネットマスク)–ネットマスクを入力します。

HA リンクおよびパス モニタリング

Device (デバイス) > High Availability (高可用性) > Link and Path Monitoring (リンクおよびパスのモニタリング)

HA フェイルオーバー条件を定義するには、HA リンクとパスのモニタリングを設定しま す。Device(デバイス) > High Availability(高可用性) > Link and Path Monitoring(リンクと パスのモニタリング)を選択します。 F۳)

Link and Path Monitoring(リンクおよびパスのモニタリング)機能は、AWS の VM-Series ファイアウォールでは使用できません。

VMware ESXi上のVMシリーズファイアウォールでは、リンク監視はサポートされま せん。パスモニタリングを有効にして、ターゲットIPアドレスまたはネクストホッ プIPアドレスとの接続を確認します。

HA リンクおよび パス モニタリング の設定	の意味
リンク モニタリ ング	 以下を指定します。 Enabled[有効] – リンクのモニタリングを有効にします。リンクのモニタリングによって、物理リンクまたは物理リンクのグループに障害が発生した場合にフェイルオーバーのトリガーになります。 Failure Condition[失敗条件] – モニターしているリンク グループの一部またはすべてに障害が発生した場合にフェイルオーバーが発生するかどうかを選択します。 パスモニタリングあるいはリンク モニタリングのいずれかを有効化・設定し、パスやリンクがダウンした場合にフェイルオーバーを発生させるようにします。パスモニタリングでは 1 つ以上のPath Group (パス グループ)を、リンク モニタリングでは 1 つ以上のLink Group (リンク グループ)を設定します。
Link Groups	特定の Ethernet リンクをモニターする 1 つ以上のリンク グループを定義 します。リンク グループを追加するには、以下を指定して Add[追加] を クリックします。 • Name[名前] – リンク グループ名を入力します。 • Enabled[有効] – リンク グループを有効にします。
	 Failure Condition(失敗条件) – 選択したリンクの一部またはすべて に障害が発生した場合にエラーを発生させるかどうかを選択します。 Interfaces[インターフェイス] – モニターする1つ以上の Ethernet イ ンターフェイスを選択します。
パス モニタリン グ	以下を指定します。 • Enabled (有効化) –結合または独立した Virtual Wire (バーチャルワ イヤ) パス モニタリング、VLAN パス モニタリング、および Virtual Router (仮想ルーター - VR)*のパス モニタリングに基づくパス監視を 有効にします。パスのモニタリングをオンにすると、ファイアウォー ルは指定した宛先 IP アドレスをモニターするために ICMP ping メッ

HA リンクおよび パス モニタリング	の意味
の設定	
	セージを送信し、レスポンスがあることを確認します。フェイルオー バー用に他のネットワーク デバイスのモニタリングが必要であった り、リンクのモニタリングのみでは不十分である場合に、バーチャル ワイヤー、レイヤー2、またはレイヤー3設定でパスのモニタリング を使用します。
	• Failure Condition (障害条件):
	 Any (いずれか) –(デフォルト) バーチャル ワイヤ、VLAN、またはVirtual Router (仮想ルーター - VR)*のパス モニタリングに失敗すると、ファイアウォールが HA フェイルオーバーをトリガーします。
	 All(すべて)–ファイアウォールは、バーチャル ワイヤ、VLAN、 および Virtual Router (仮想ルーター - VR)*のパス監視に障害が発生 した場合、HA フェイルオーバーをトリガーします(有効化されて いる上記 3 つのうちいずれか)。
	 * Advanced Routing(高度なルーティング)を有効にしている場合は、論理ルーターがVirtual Router(仮想ルーター- VR)に置き換わり、論理ルーターパスの監視を有効化可能です。
	 パスモニタリングあるいはリンクモニタリングのいずれかを有効化・設定し、パスやリンクがダウンした場合にフェイルオーバーを発生させるようにします。パスモニタリングでは1つ以上のPath Group (パスグループ)を、リンクモニタリングでは1つ以上のLink Group (リンクグループ)を設定します。
パス グループ	1つ以上のパス グループを定義して、そのインターフェース タイプの特定の宛先アドレスを監視しますAdd Virtual Wire Path(バーチャル ワイヤパスの追加)、および Add VLAN Path(VLAN パスの追加)、および Add Virtual Router Path(Virtual Router (仮想ルーター - VR)パスの追加)。 (Advanced Routing(高度なルーティング)を有効化している場合、Add Logical Router Path(論理ルーターパスの追加)を行うことが可能です。
	追加するパス モニタリングの種類毎に、以下を指定します。
	 Name(名称) –モニタリングするバーチャル ワイヤ、VLAN、またはVirtual Router (仮想ルーター - VR)*を選択します(ドロップダウンでの選択は、追加するパス モニタリングの種類により異なります)。
	 Source IP(送信元 IP) –バーチャル ワイヤおよびVLAN インター フェースの場合、ネクストホップ ルーターに送信される ping で使用

HA リンクおよび パス モニタリング D設定	の意味
	する送信元 IPアドレス(宛先 IPアドレス)を入力します。ローカル ルータでアドレスをファイアウォールにルーティングできる必要があ ります。(Virtual Router (仮想ルーター - VR)に関連付けられたパス グループの送信元 IP アドレスは、指定された宛先 IP アドレスの出力 インターフェースとしてルート テーブルに示されるインターネット IPアドレスとして自動的に設定されます。)
	 Enabled (有効化) –バーチャル ワイヤ、VLAN、または Virtual Router (仮想ルーター - VR)*のモニタリングを有効にする.
	• Failure Condition(障害条件):
	 Any(いずれか)(デフォルト)-ファイアウォールは、宛先 IP グ ループで ping 障害が発生した際、バーチャル ワイヤ、VLAN、また は Virtual Router (仮想ルーター - VR)* が失敗したと判断します。
	 All (すべて) –ファイアウォールは、すべての宛先 IP グループで ping 障害が発生した際、バーチャル ワイヤ、VLAN、または Virtual Router (仮想ルーター - VR)* が失敗したと判断します。
	 実際のHAフェイルオーバーは、パスモニタリングに 設定した障害条件によって判断されます。これは、バー チャルワイヤ、VLAN、およびVirtual Router (仮想ルー ター - VR)*パスモニタリング(有効化した方)を考慮に 入れるものです。
	 Ping Interval (Ping間隔) – 宛先 IPアドレスに送信される ping 間の間 隔を指定します(範囲は 200 ~ 60,000 ミリ秒、デフォルトは 200 ミ リ秒)。
	 Ping Count (Ping数) – 障害を宣言するまでに試行する Ping 数を指定します (範囲は 3 ~ 10 回、デフォルトは 10 回)。
	 * Advanced Routing(高度なルーティング)を有効にしている場合は、論理ルーターがVirtual Router(仮想ルーター-VR)に置き換わり、論理ルーターパスの監視を有効化可能です。

HA リンクおよび パス モニタリング の設定	の意味
Destination IP for Path Group(パ ス グループの宛 先 IP)	 Destination IP(宛先 IP) – パス グループを監視する 1 つまたは複数 の宛先 IPアドレス グループをAdd(追加)します。
	 Destination IP Group(宛先 IP グループ) – グループ名を入力します。
	 モニターする Destination IP(宛先 IPアドレス)を1つまたは複数Add(追加)します。
	 Enabled(有効化) – 宛先 IP グループを有効化する場合に選択します。
	 Failure Condition(障害条件):Any(いずれか)(グループ内の いずれかのIPアドレスで ping 障害が発生した場合、宛先グループ が失敗したと見なす設定にする場合)、またはAll(すべて)(グ ループ内のすべてのIPアドレスで ping 障害が発生した場合、宛先 グループが失敗したと見なす設定にする場合)を指定します。

HA Active/Active Config (HA アクティブ/アクティブ 設定)

• Device(デバイス) > High Availability(高可用性) > Active/Active Config(アクティブ/ア クティブ設定)

Active/Active HA(HA アクティブ/アクティブ)ペアの設定を行うには、**Device**(デバイス) > **High Availability**(高可用性) > **Active/Active Config**(アクティブ/アクティブ設定)を選択します。

アクティブ / アク ティブ設定	の意味
パケット転送	ピアによる、セッション設定用およびレイヤー7の検査用(App-ID、コ ンテンツID、および脅威検査)の、HA3リンクを経由したパケットの転 送をEnable[有効化] します。
[HA3 インター フェイス]:	アクティブ/アクティブのHAピア間のパケットの転送に使用しようとし ているデータインターフェイスを選択します。ここで使用するインター フェイスはタイプをHAに設定した専用のレイヤー2インターフェイスで ある必要があります。

アクティブ/アク ティブ設定	の意味
	 HA3リンクに障害が発生した場合、アクティブ-セカンダ リピアは機能停止状態に移行します。この状態に移行し ないようにするためには、HA3リンクとして2つ以上の物 理インターフェイスをもつリンク集約グループ(LAG) イ ンターフェイスを設定します。HA3バックアップリンクは ファイアウォールでサポートされていません。複数のイン ターフェイスをもつ集約グループにより、追加の容量とリ ンクの冗長性を確保し、HAピア間のパケット転送を補助 することができます。 HA3 インターフェイスを使用する場合は、すべての中継 ネットワークデバイスでジャンボ フレームを有効にする 必要があります。
VR 同期	HAピアに設定されたすべての仮想ルーターの同期を強制します。 仮想ルーターが動的ルーティングプロトコル用に設定されていない場 合はこのオプションを使用します。両方のピアが交換網を介して同じネ クストホップルーターに接続されている必要があり、スタティックルー ティングのみを使用している必要があります。
QoS 同期	すべての物理インターフェイスの QoS プロファイル選択を同期します。 両方のピアのリンク速度が同様で、すべての物理インターフェイスで同 じQoSプロファイルが必要な場合には、このオプションを選択します。 この設定は、Network[ネットワーク] タブの QoS 設定の同期に影響しま す。QoS ポリシーは、この設定に関係なく同期されます。
仮の保留時間 (秒)	HAがアクティブ/アクティブに設定されたファイアウォールで障害が発生すると、一時的な状態に入ります。暫定的な状態からアクティブ-セカンダリの状態に移行することにより、Tentative Hold Time [暫定的な状態の保留時間] がトリガーされ、ファイアウォールはパケットの処理を開始する前に、この時間中に隣接デバイスへのルーティングを試行してルートテーブルを埋めようとします。このタイマーを使用しない場合、ファイアウォールの回復時にただちにアクティブ-セカンダリ状態になり、必要なルートがないためパケットをサイレントに破棄します(デフォルトは 60 秒)。
セッション オー ナーの選択	セッションオーナーには、そのセッション内のすべてのレイヤー7検査 (App-ID、およびコンテンツID)、およびそのセッション内のすべて のトラフィックログを生成する役割があります。以下のオプションのう ち1つを選択し、パケットに対するセッションオーナーの決定方法を指 定します。
	 First packet[最初のパケット] – そのセッションの最初のパケットを 受信するファイアウォールをセッションオーナーとして指定する場合

アクティブ / アク ティブ設定	の意味
	はこのオプションを選択します。HA3 全体でトラフィックを最小化 し、データプレーン負荷をピアに分散したい場合にベストプラクティ スになります。
	 Primary Device[プライマリデバイス] – アクティブ-プライマリのファ イアウォールをすべてのセッションオーナーとして設定したい場合は このオプションを選択します。この場合、アクティブ-セカンダリの ファイアウォールが最初のパケットを受信すると、レイヤー7検査を 必要とするすべてのパケットをHA3リンクを経由してアクティブ-プ ライマリのファイアウォールへ転送します。
仮想アドレス	Add[追加]をクリックし、IPv4またはIPv6のタブを選択し、再度Add[追加]をクリックしてオプションを入力し、使用するHA仮想アドレスのタイプを指定します。フローティングまたはARPロードシェアリングペア内では複数の仮想アドレスのタイプを混在させることもできます。例えば、LANインターフェイスでARPロードシェアリングを使用し、WANインターフェイスではフローティングIPを使用することができます。
	 Floating[フローティング] – リンクまたはシステム障害が発生した 場合に、HAピア間で移動するIPアドレスを入力します。それぞれの ファイアウォールが1つを所有できるよう、2つのフローティングIPア ドレスを設定し、優先順位を設定します。どちらかのファイアウォー ルに障害が発生した場合、フローティングIPアドレスがHAピアに移 行されます。
	 Device 0 Priority[デバイス0優先順位] – デバイスIDが0のファイ アウォールにフローティングIPアドレスの優先所有権をもたせま す。最も低い値をもつファイアウォールの優先順位が最も高くな ります。
	 Device 1 Priority[デバイス0優先順位] – デバイスIDが1のファイ アウォールにフローティングIPアドレスの優先所有権をもたせま す。最も低い値をもつファイアウォールの優先順位が最も高くな ります。
	 Failover address if link state is down[リンク状態がダウンの場合アドレスをフェイルオーバー] – インターフェイスのリンク状態がダウンの場合に、ファイルオーバーアドレスを使用します。
	 Floating IP bound to the Active-Primary HA device[フローティン グIPをアクティブ-プライマリHAデバイスに固定] – フローティン グIPをアクティブ-プライマリピアに固定する場合はこのオプショ ンを選択します。片方のピアに障害が発生し、障害が発生した ファイアウォールが復旧して役割がアクティブ-セカンダリのピア に切り替わった後も、トラフィックは継続的に元のアクティブ-プ ライマリピアに送信されます。

アクティブ / アク ティブ設定	の意味
仮想アドレス(続 く)	 ARP Load Sharing[ARPロードシェアリング] – HAペアで共有し、ホストのゲートウェイサービスを提供するIPアドレスを入力します。ファイアウォールがホストと同じブロードキャストドメインにある場合にのみ、このオプションを選択する必要があります。Device Selection Algorithm[デバイス選択アルゴリズム]を選択します。
	 IP Modulo[IPモジュロ] – ARPリクエスト元IPアドレスのパリティ に基づいて、ARPリクエストに応答するファイアウォールが選択 されます。
	 IP Hash[IPハッシュ] – ARPリクエスト元IPアドレスのハッシュに 基づいて、ARPリクエストに応答するファイアウォールが選択さ れます。

Cluster Config (クラスタ設定)

• Device(デバイス) > High Availability(高可用性) > Cluster Config(クラスタ設定)

Device(デバイス) > **High Availability**(高可用性) > **Cluster Config**(クラスタ設定)を選択し、HA クラスタにメンバーを追加します。

Cluster Config (ク ラスタ設定)	の意味
コンテキストの	クラスター メンバーを Add(追加)します。ローカル ファイアウォール を追加する必要があります。また、HA ペアを使用している場合は、ペ アの両方の HA ピアをクラスタのメンバーとして追加する必要がありま す。
	 (サポート対象ファイアウォール)デバイスシリアル番号–クラスタ メンバーの一意のシリアル番号を入力します。
	 (Panorama (パノラマ)) Device (デバイス) –ドロップダウンでデバイスを選択して Device Name (デバイス名)を入力します。
	 HA4 IP Address(HA4 IP アドレス) – クラスタメンバーの HA4 リン クの IPアドレスを入力します。
	 HA4 Backup IP Address(HA4 バックアップ IP アドレス) – クラスタ メンバーのバックアップ HA4 リンクの IPアドレスを入力します。
	 Session Synchronization (セッション同期) – このクラスタメンバー とのセッション同期を有効にする場合に選択します。
	 Description(説明) – 役に立つ説明を入力します。

Cluster Config (ク ラスタ設定)	の意味
Delete(削除)	1つまたは複数のクラスタ メンバーを選択し、クラスターから Delete(削除)します。
Enable [有効化]	(サポート対象ファイアウォール) クラスタ メンバーが他のメンバーと セッションを同期するかどうかを指定することができます。デフォルト では、すべてのメンバーがセッションを同期することができます。1つま たは複数のメンバーの同期を無効にする場合は、Enable(有効化)を選 択し、1つまたは複数のメンバーの同期を再度有効にします。
Disable (無効 化)	(サポート対象ファイアウォール)1つまたは複数のメンバーを選択し て、他のメンバーとの同期を Disable (無効化)します。
レートの	(Panorama)Refresh(更新)を選択して、HA クラスタ 内の HA デバイ ス リストを再読み込みします。

Device (デバイス) > Log Forwarding Card (ログ転送カード)

• Device (デバイス) > Log Forwarding Card (ログ転送カード)

Log Forwarding カード (LFC) は、すべてのデータプレーン ログ (トラフィックや脅威など) を ファイアウォールから、Panorama、ファイアウォール データ レイク、または syslog サーバー などの 1 つ以上の外部ログ システムに転送する高性能ログ カードです。データプレーンロ グはローカルファイアウォールで使用できなくなったため、管理 Web インターフェイスか ら[ACC]タブが削除され、モニタ > ログ には管理ログ(設定、システム、アラーム)のみが含ま れます。

LFC 用のポートを設定する必要があります。ブレイクアウトケーブルを使用して LFC 1/1 を設定すると、最大 8 つの 10G ブレークアウト ポートにアクセスできます。これにより、最初のインターフェイスでポート 1 から 4 が自動設定され、2 番目のインターフェイスでポート 5 ~ 8 が自動設定されます。1 つまたは両方のインターフェイスを使用して、それぞれ最大 40G または80G 接続を提供できます。LFC に接続されているすべてのポートに対して LAG を使用するように、リンクされたデバイスを設定する必要があります。

LFC 1/9 を設定すると、最大 2 つの 40G ポートにアクセスできます。これにより、最初のイン ターフェイスでポート 9 が自動設定され、2 番目のインターフェイスでポート 10 が自動設定さ れます。1 つまたは両方のインターフェイスを使用して、それぞれ最大 40G または 80G 接続を 提供できます。LFC に接続されているすべてのポートに対して LAG を使用するように、リンク されたデバイスを設定する必要があります。

現在、LFC は LACP をサポートしていません。

デバイス カード > ログ転送 のポートを設定します。ファイアウォールはこれらのポートを使用してすべてのデータプレーンのログを Panorama や Syslog サーバーなどの外部システムに転送します。

LFC の要件および各コンポーネントに関する情報については、PA-7000 Series ハードウェアリファレンス ガイドを参照してください。

LFC インターフェイス用に次の表で示している設定を行います。

LFC インターフェ イス設定	の意味
氏名	インターフェイス名を入力します。LFC の場合は、ドロップダウン メ ニューから lfc1/1 または lfc1/9 を選択する必要があります。
コメント	インターフェイスの説明(省略可)を入力します。
IPv4	ネットワークで IPv4 が使用されている場合は、以下を定義します。 • IP address[IP アドレス] – ポートの IPv4 アドレス。

LFC インターフェ イス設定	の意味
	 Netmask[ネットマスク] – ポートの IPv4 アドレスのネットワークマ スク。
	 Default Gateway[デフォルトゲートウェイ] – ポートのデフォルト ゲートウェイのIPv4アドレス。
IPv6	ネットワークで IPv6 が使用されている場合は、以下を定義します。
	• IP アドレス: ポートの IPv6 アドレス。
	 デフォルトゲートウェイ:ポートのデフォルトゲートウェイの IPv6 アドレス。
リンク速度	インターフェイスの速度(10000または40000)を選択する か、auto(デフォルト設定)を選択して、接続ごとにファイアウォール に自動的に速度を決定させます。使用可能なインターフェイス速度は、 使用される名前(lfc1/1 または lfc1/9)によって異なります。スピード設定 が不可のインターフェイスについてはautoのみ設定可能です。
リンク ステート	接続に応じて、インターフェイスの状態を、有効 (up)、無効 (down)、自動決定 (auto) から選択します。デフォルト設定はautoです。
LACP ポート優先 順位	LACP は現在 LFC ではサポートされていません。

サブインターフェイスは、マルチ vsys が有効な場合のみ利用できます。LFC サブインターフェ イス を に設定するには、サブインターフェイスを追加し、次の表に示す設定を使用します。



外部サーバーへのログ転送は、LFC サブインターフェイスではまだサポートされて いません。ログを外部サーバーに転送するには、メインの LFC インターフェイスを 使用する必要があります。

LFC サブインター フェイス設定	の意味
インターフェイス 名	読み取り専用のInterface Name[インターフェイス名] フィールドには、 選択したログカードインターフェイスの名前が表示されます。サブイン ターフェイスを識別する数値サフィックス (1 ~ 9999) を隣のフィール ドに入力します。
コメント	インターフェイスの説明(省略可)を入力します。
タグ	サブインターフェイス用のVLANTag[タグ] (0 ~ 4094) を入力します。

LFC サブインター フェイス設定	の意味
	 使いやすさのため、タグはサブインターフェイス番号と同じにしてください。
仮想システ ム(vsys)	ログ転送カード(LFC)サブインターフェイスの割り当て先の仮想シス テム(vsys)を選択します。Virtual Systems[仮想システム]リンクをク リックして新しいvsysを追加することもできます。LFC サブインター フェイスを vsys に割り当てると、そのインターフェイスは、ログ カー ドからログ(Syslog、電子メール、SNMP)を転送するすべてのサービス の送信元インターフェイスとして使用されます。
IPv4	ネットワークで IPv4 が使用されている場合は、以下を定義します。
	● IP address[IP アドレス] – ポートの IPv4 アドレス。
	 Netmask[ネットマスク] – ポートの IPv4 アドレスのネットワークマ スク。
	 Default Gateway[デフォルトゲートウェイ] – ポートのデフォルト ゲートウェイのIPv4アドレス。
IPv6	ネットワークで IPv6 が使用されている場合は、以下を定義します。
	• IP アドレス: ポートの IPv6 アドレス。
	 デフォルトゲートウェイ:ポートのデフォルトゲートウェイの IPv6 アドレス。

Device > Config Audit [デバイス > 設定監査]

設定ファイル同士の差異を確認する場合は [Device (デバイス)] > [Config Audit (設定監査)]を順に 選ぶか、または Panorama > [Config Audit (設定監査)] を順に選択します。コミットまたは保存 された構成バージョンは、一度に 2 つしか比較できません。

Panoramaでは、Panorama上の構成バージョンに対してのみ構成監査を実行できますが、管理対象のファイアウォールに対しては実行できません。管理対象ファイアウォールの設定監査を実行するには、ファイアウォールのWebインターフェイスにアクセスする必要があります。

Config Audit Setting (設定監 査の設定)	の意味
バージョン	ファイアウォールまたはPanoramaでコミットされた構成バー ジョン。
	 ローカル候補–ファイアウォールまたはPanorama上の保留 中のコミットされていない設定。
	 (HA のみ)ピア候補–ファイアウォールまたは Panorama の HA ピアで保留中のコミットされていない設定。
	 (HA のみ) ピア実行–ファイアウォールまた はPanoramaの HA ピア上の現在の実行中の設定。
	 (ファイアウォールのみ) Merged Running config- Panorama から以前にプッシュされた構成バージョン。
	 (ファイアウォールのみ) Previously Merged Running config-Panorama からプッシュされた現在実行中の設定。
	 [Running (実行中)] –ファイアウォールまたはPanorama上の現在の実行中の設定。現在の実行中の設定の構成バージョン番号も表示されます。
	 [Committed Versions (コミットされたバージョン)] –ファ イアウォールまたはPanoramaの設定変更用にコミットさ れた構成バージョンのリスト。バージョンはデフォルトで config commit に割り当てられ、順次実行されます。
	 [Saved Versions] -ファイアウォールまたはPanoramaに 保存されている構成バージョンのリスト。
コミット担当者	設定変更をコミットした管理者。
コミット日	設定変更がコミットされた日付と時刻。形式は、月-日-年 時:分:秒です。
オブジェクト変更	コミットされた構成バージョンで追加 (∞ 削除

)、

Config Audit Setting (設定監 査の設定)	の意味
	 (□) または変更 (□) された設定オブジェクトの数を一覧表示します。
の意味	コミットに含まれる説明。コミットに説明が含まれていない場 合、このフィールドは空白です。
コンテキスト	ハイライト表示されたファイル同士の差異の前後に表示する行 数を指定する場合はContext [コンテクスト]のドロップダウン リストを使用します。表示する行数を増やすことで、検証結果 をWebインターフェイスの設定内容に反映させやすくなりま す。Context(コンテクスト)を All(すべて)に設定した場 合、結果には設定ファイル全体が含まれます。
バージョンを比較	[Compare Versions (バージョンを比較)]をクリックして構成監 査を開始します。
XML 差分	XMLファイルの違いを並べて表示し、選択した2つの構成バー ジョン間の追加(緑色)、変更(黄色)、削除(赤色)を示す 色を使用して、相違点を行ごとに強調表示します。
	Added Modified Deleted
	左側のXMLは選択された構成バージョンのうち古いもの、右側 のXMLは選択された構成バージョンのうち新しいものです。
変更サマリー	
オブジェクト名	影響を受けるオブジェクトの名前。
オブジェクト タイプ	影響を受ける設定オブジェクトのタイプ。
変更日時	設定オブジェクトの追加、削除、または編集が行われた時刻。 形式は、月-日-年時:分:秒です。
場所	影響を受けるオブジェクトが属するデバイスグループ、テンプ レートスタック、またはテンプレート。設定オブジェクトが共 有されている場合、Shared (共有)と表示されます。

設定変更が行われた設定コンテナ。次に該当する場合がありま す:

- [Device Group (デバイスグループ)]
- [Template (テンプレート)]

場所タイプ

Config Audit Setting (設定監 査の設定)	の意味
	• [Template Stack (テンプレートスタック)]
	• [Template Stack (テンプレートスタック)]
	• [Device Config (デバイス設定)]
	• [Mgt Config (管理設定)]
	スタンドアロンファイアウォールの場合、Mgt Config (管理設定)はデバイスの変更に適用されます。Panoramaの 場合、Panoramaの変更に適用されます。
変更者	設定オブジェクトを変更した管理者。
オペレーション	影響を受けたオブジェクトに対して実行される操作。
	• Set-新しい設定オブジェクトが追加されました。
	• 編集既存の設定オブジェクトが変更されました。
	 名前の変更:既存の設定オブジェクトの名前が変更されました。
	 移動–ルールベース内でのポリシールールの順序変更または 移動。
	• 削除設定オブジェクトが削除されました。
オブジェクト レベルの変更	選択した設定オブジェクトの2つの構成バージョン間の設定変 更を表示するXMLスニペット。

[Device] > [パスワード プロファイル]

- [Device] > [パスワード プロファイル]
- Panorama > Password Profiles (パスワード プロファイル)

個別のローカル アカウントの基本的なパスワード要件を設定するには、Device(デバイス) > Password Profiles (パスワード プロファイル) または Panorama > Password Profiles (パスワー ド プロファイル) を選択します。パスワード プロファイルは、すべてのローカル アカウントに 対して定義された Minimum Password Complexity (パスワード複雑性設定) ((Device (デバイ ス) > Setup (セットアップ) > Management (管理)) をオーバーライドします。

アカウントにパスワード プロファイルを適用するには、Device(デバイス) > Administrators(管理者)(ファイアウォールの場合)または Panorama > Administrators(管 理者)(Panoramaの場合)を選択し、アカウントを選択して、Password Profile(パスワード プロファイル)を選択します。



ローカル データベース認証を使用する管理者アカウントにパスワード プロ フィルを割り当てることはできません(「Device(デバイス) > Local User Database(ローカル ユーザー データベース) > Users(ユーザー)」を参照)。

パスワード プロファイルを作成するには、Add(追加)をクリックし、以下の表に従って情報 を指定します。

パスワード プロ ファイル設定	の意味
氏名	パスワード プロファイルを識別する名前を入力します(最大 31 文 字)。名前の大文字と小文字は区別されます。また、一意の名前にする 必要があります。文字、数字、スペース、ハイフン、およびアンダース コアのみを使用してください。
パスワード有効期 限(日数)	管理者は、日数(範囲は0~365日)で指定された期間ごとに定期的に パスワードを変更する必要があります。たとえば、値を「90」に設定す ると、管理者に90日ごとにパスワードの変更を求めるプロンプトが表 示されます。失効の警告を0~30日の範囲で設定して猶予期間を指定 することもできます。
失効の警告期間 (日数)	パスワード有効期限を設定した場合は、この設定により、強制パスワード変更日が近づくとユーザーがログインするたびにパスワードの変更を 求めるプロンプトを表示することができます(範囲は0~30日)。
失効後の管理者ロ グイン回数	アカウントが失効した後に、管理者はここで指定した回数だけログイン できます。たとえば、値を「3」に設定した場合、アカウントが失効し ても、管理者はアカウントがロックアウトされるまで3回ログインする ことができます(範囲は0~3回)。

パスワード プロ ファイル設定	の意味
失効後の猶予期間	アカウントが失効しても、管理者はここで指定した期間(日数)ログイ
(日数)	ンできます(範囲は 0 ~ 30 日)。

ユーザー名とパスワードの要件

PAN-OS および Panorama アカウントのユーザー名とパスワードに使用できる有効な文字を以下の表に示します。

アカウントの種類	ユーザー名とパスワードの制限
パスワード文字セット	パスワード フィールドの文字セットには制限がありません。
Remote Admin, SSL- VPN, or Authentication Portal (リモート管 理、SSL-VPN、または 認証ポータル)	 ユーザー名には以下の文字を使用できません。 バックティック() 角括弧 (< and >) アンパサンド (&) アスタリスク (*) アット記号 (@) 疑問符 (?) パイプ ()) 一重引用符 (') セミコロン (;) 二重引用符 (") ドル記号 (\$) かっこ ('(' と ')') コロン (':')
ローカル管理者アカウ ント	 ローカルユーザー名には以下の文字を使用できます。 小文字 (a ~ z) 大文字 (A ~ Z) 数字 (0 ~ 9) アンダースコア (_) ピリオド (.) ハイフン (-)

アカウントの種類	ユーザー名とパスワードの制限
	 ログイン名をハイフン(-)で開始することはできません。 管理者ユーザー名を数字のみで構成することはできません。少なくとも1つの英字または1つの正当な記号文字を含める必要があります。たとえば、1234_567、1234a789_、および c7897432 は有効なユーザー名です。12345678 は有効なユーザー名ではありません。
ローカル管理者パス ワード	 一般的に使用される単語や語句は、大文字と小文字の組み合わせにかかわらず、パスワードとして使用できません。 よく使われる単語やフレーズの例としては、 管理者、パスワード、パスワード、レットイン、pa55word、QwErTy、q1w2e3r4などがあります。

Device > Administrators [デバイス > 管理者]

ファイアウォールやPanoramaへのアクセス権は管理者アカウントにより制御されます。ファイ アウォール管理者には、1台のファイアウォールか、1台のファイアウォール上の仮想システム へのフル アクセス権または読み取り専用アクセス権を付与できます。ファイアウォールには、 フル アクセス権を持つ admin アカウントが事前に定義されています



Panorama 管理者を定義するには「Panorama > Managed Devices (管理対象デバイス) > Summary (サマリー)」を参照してください。

以下の認証オプションがサポートされています。

- パスワード認証 管理者がユーザー名とパスワードを入力してログインします。認証に証明 書は不要です。認証プロファイルと併用することや、ローカルデータベースの認証に使用す ることができます。
- クライアント証明書認証(Web) この認証方法ではユーザー名とパスワードが不要になり、ファイアウォールへのアクセス認証は証明書のみで行えるようになります。
- 公開鍵認証(SSH) 管理者がファイアウォールへのアクセスが必要なマシン上で公開/秘密 鍵のペアを生成し、ファイアウォールに公開鍵をアップロードするので、管理者がユーザー 名とパスワードを入力しなくても、安全にアクセスできるようになります。

管理者を追加するには、Add(追加)をクリックして以下の情報を入力します。

管理者アカウント設定	の意味
氏名	管理者のログイン名 (最大 31 文字) を入力します。名前の 大文字と小文字は区別されます。また、一意の名前にす る必要があります。英字、数字、ハイフン、ピリオド、 およびアンダースコアのみを使用してください。ログイ ン名をハイフン (-) で開始することはできません。
認証プロファイル	管理者の認証の認証プロファイルを選択します。この設定は、RADIUS、TACACS+、LDAP、Kerberos、SAML、 またはローカル データベース認証に使用できます。詳細 は「Device(デバイス)> Authentication Profile(認証プ ロファイル)」を参照してください。
クライアント証明書認証のみを 使用(Web)	Webアクセスのクライアント証明書認証を使用する場合 は、このオプションを選択します。このオプションを選 択すると、ユーザー名とパスワードは不要になり、ファ イアウォールへのアクセス認証は証明書のみで行えるよ うになります。
新しいパスワード 再入力 新しいパスワード	管理者のパスワードを入力し、パスワードを確認 します (最大 64 文字)。Setup(セットアップ) >

管理者アカウント設定	の意味
	Management(管理)を選択し、パスワードの最低の長さ を適用することもできます。
	ファイアウォール管理インターフェイスの 安全性を維持するため、管理パスワードを 定期的に変更することをお勧めします。 管理パスワードには、小文字、大文字、お よび数字を混在させてください。ファイア ウォールのすべての管理者用に、パスワー ド複雑性設定を構成することもできます。
公開キーの認証 (SSH) の使用	SSH公開キーの認証を使用する場合は、このオプション を選択します。Import Key[キーのインポート] をクリッ クし、公開キー ファイルを参照して選択します。アップ ロードした鍵は、読み取り専用テキスト エリアに表示さ れます。
	サポート対象の鍵ファイルのフォーマットは、IETF SECSH と OpenSSH です。サポート対象の鍵アルゴリズ ムは、DSA(1,024 ビット)と RSA(768 ~ 4,096 ビッ ト)です。
	公開キー認証に失敗した場合、ファイア ウォールは管理者に対しユーザーネームと パスワードを入力するようメッセージを表 示します。
管理者タイプ	この管理者にロールを割り当てます。このロールによっ て、管理者が表示および変更できる内容が決まります。
	Role Based [ロールベース] を選択した場合、ドロップダ ウンリストからカスタムロールプロファイルを選択しま す。詳細は「Device(デバイス)> Admin Roles(管理者 ロール)」を参照してください。
	Dynamic [動的] を選択した場合、以下の事前設定された ロールのいずれかを選択できます。
	 Superuser (スーパーユーザー) – ファイアウォール に対するフルアクセス権を持ち、新しい管理者アカウ ントや仮想システムを設定することができます。スー パーユーザー権限を持っていなければ、その他のスー パーユーザー権限を持つ管理者を作成することができ ません。
	 Superuser(読み取り専用スーパーユーザー) – ファ イアウォールに読み取り専用でアクセスできます。

管理者アカウント設定	の意味
	 Device administrator (デバイス管理者) – 新しいア カウントまたは仮想システムの定義を除き、選択した ファイアウォールに対するフル アクセス権が与えられ ます。
	 Device administrator (read-only) (読み取り専用デバイ ス管理者) – パスワード プロファイル (アクセス不 可) および管理者アカウント (ログイン中のアカウン トのみ表示可能) を除き、ファイアウォール設定の全 項目に対し読み取りアクセスが許可されます。
	 virtual system (仮想システム - vsys)管理者-ファイ アウォール上の特定の仮想システムへのアクセス権 を持ち、仮想システムを管理します (マルチ仮想シス テム機能が有効になっている場合)。仮想システム管 理者は、ネットワークインターフェイス、仮想ルー ター、IPSecトンネル、VLAN、仮想ワイヤー、GREト ンネル、DHCP、DNSプロキシ、QoS、LLDP、または ネットワークプロファイルにアクセスできません。
	 仮想システム管理者(読み取り専用)-ファイアウォー ル上の特定の仮想システムへの読み取り専用ア クセス権を持ち、仮想システムを表示します(マ ルチ仮想システム機能が有効になっている場合)。 読み取り専用アクセス権を持つ仮想システム管理 者は、ネットワークインターフェイス、仮想ルー ター、IPSecトンネル、VLAN、仮想ワイヤー、GREト ンネル、DHCP、DNSプロキシ、QoS、LLDP、または ネットワークプロファイルにアクセスできません。
仮想システム(vsys) (仮想システム管理者ロールの み)	Add [追加] をクリックして、管理者が管理できる仮想シス テムを選択します。
パスワードプロファイル	パスワード プロファイルを選択します (該当する場合)。 新しいパスワード プロファイルを作成する方法について は、「Device(デバイス)> Password Profiles(パスワー ド プロファイル)」を参照してください。

管理者アカウント設定	の意味
	管理者用のパスワードプロファイルを作成 し、設定した期間が過ぎたら管理者用パス ワードが必ず失効するようにします。定 期的に管理者用パスワードを変更すること で、保存した、あるいは盗まれた認証情報 を攻撃者が使用するのを防ぐことができま す。

Device > Admin Roles [デバイス > 管理者ロール]

管理者ユーザーのアクセス権限や役割を定義する、カスタマイズ可能な管理者ロールプロファイルを定義する場合は Device [デバイス] > Admin Roles[管理者ロール]を選択します。管理アカウントDevice(デバイス)> Administrators(管理者)を作成する際は、Admin Role profiles or dynamic roles(管理者ロールプロファイルや動的ロール) ■を割り当てます。



Panorama 管理者の管理者ロール プロファイルを定義するには、Panorama >管理者 ロール を参照してください。

ファイアウォールには一般的な用途で使用可能な3つのロールが事前定義されています。まず スーパーユーザーロールを使用して、ファイアウォールの初期設定および、セキュリティ管理 者、監査管理者、および暗号管理者の管理者アカウントを作成します。アカウントを作成し、 適切な共通基準管理者ロールを適用したら、それらのアカウントを使用してログインします。連 邦情報処理標準(FIPS)、または情報セキュリティ国際評価基準(CC)モードのデフォルトの スーパーユーザーアカウントは「admin」で、デフォルトのパスワードは「paloalto」に設定さ れています。標準操作モードでは、「admin」のデフォルトのパスワードは「admin」です。事 前定義の管理者ロールは、すべてのロールに監査証跡への読み取り専用のアクセス権があるとい う点を除き、機能が重複しないように作成されています(読み取りと削除のフルアクセス権があ る監査管理者は除く)。これらの管理者ロールは変更できず、以下のように定義されています。

- auditadmin 監査管理者は、ファイアウォールの監査データの定期的な確認を担当する責任 者です。
- cryptoadmin 暗号管理者は、ファイアウォールの安全な接続確立に関連する暗号要素の設定と保守を担当する責任者です。
- securityadmin セキュリティ管理者は、他の2つの管理ロールで対処されない、その他すべての管理タスク(セキュリティポリシーの作成など)を担当する責任者です。

管理者ロール プロファイルを追加する場合は、Add(追加)をクリックし、次の表で説明する 設定を指定します。

カスタムロールを作成し、管理者アクセスを各種の管理者が必要とするものだけに 制限します。各種の管理者について、Web UI、XML API、Command Line (コマンド ライン)、および REST API への読み取り専用アクセスを有効化、無効化、あるいは 設定します。

Administrator Role Setting (管理者ロール設定)		
氏名	管理者ロールの識別に使用する名前を入力します(最大 31 文 字)。名前の大文字と小文字は区別されます。また、一意の名前に する必要があります。文字、数字、スペース、ハイフン、およびア ンダースコアのみを使用してください。	
の意味	(任意)ロールの説明文を入力します(最大 255文字)。	

Administrator Role Setting(管理者ロール設定)		
ロール	 管理責任の範囲を選択します。 Device [デバイス] - 1つ以上の仮想システム(vsys)を持つかどうかに関らず、このロールはファイアウォール全体に適用されます。 仮想システムーこのロール ル ロール ロール ロール ロール ローク ロ	
Web UI	 アクセス権限を設定する場合は、特定のWeb インターフェイス機能 のアイコンをクリックします。 Enable [有効化] – 選択した機能に読み書きアクセスができます。 Read Only [読み取り専用] – 選択した機能に読み取り専用でアクセスできます。 Disable [無効化] – 選択した機能にアクセスできません。 	
XML API	特定のXML API 機能のアイコンをクリックして、許可するアクセス権限を設定しま す (Enable (有効) または Disable (無効))。	
コマンド行	 CLIアクセスのロールのタイプを選択します。デフォルトでは None (なし) に設定され、CLI へのアクセスは許可されていません。設定の選択肢は Role (ロール) の範囲によって異なります。 デバイス superuser (スーパーユーザー) - ファイアウォールに対するフルアクセス権を持ち、新しい管理者アカウントや仮想システムを設定することができます。スーパーユーザー権限を持っていなければ、その他のスーパーユーザー権限を持つ管理者を作成することができません。 superreader (スーパーリーダー) - ファイアウォールに読み取り専用でアクセスできます。 	

Administrator Role Setting(管理者ロール設定)		
	 deviceadmin(デバイス管理者) – 新しいアカウントまたは 仮想システムの定義を除き、選択したファイアウォールに対 するフルアクセス権が与えられます。 	
	 devicereader (デバイスリーダー) – パスワード プロファイ ル (アクセス不可)および管理者アカウント (ログイン中の アカウントのみ表示可能)を除き、ファイアウォール設定の 全項目に対し読み取りアクセスが許可されます。 	
	 仮想システム(vsys) 	
	 vsysadmin-選択されたファイアウォールの仮想システムに アクセスでき、仮想システムの特定の要素を作成・管理し ます。vsysadmin設定は、ファイアウォールレベルまたは ネットワークレベルの機能(スタティックおよびダイナミッ クルーティング、インターフェイスのIPアドレス、IPSecト ンネル、VLAN、仮想ワイヤー、仮想ルーター、GREトンネ ル、DHCP、DNSプロキシ、QoS、LLDP、またはネットワー クプロファイルなど)を制御できません。 	
	 vsysreader-選択されたファイアウォールの仮想システムおよび 仮想システム の特定の要素に対する読み取り専用のアクセスが可能です。vsysreader 設定は、ファイアウォールレベルまたはネットワーク レベルの機能 (スタティックおよびダイナミック ルーティング、インターフェイスの IPアドレス、IPSecトンネル、VLAN、仮想ワイヤー、仮想ルーター、GREトンネル、DHCP、DNSプロキシ、QoS、LLDP、またはネットワーク プロファイルなど) にアクセスできません。 	
REST API	任意の REST API	
	機能にアクセス権限を設定する場合はそれぞれのアイコン (Enable(有効化)、Read Only(読み取り専用)、また はDisable(無効化))をクリックします。	

Device > Access Domain [デバイス > アクセス ドメイン]

• Device > Access Domain [デバイス > アクセス ドメイン]

管理者のアクセスをファイアウォールで特定の仮想システムに制限するには、アクセ スドメインを設定します。ファイアウォールでアクセスドメインがサポートされるの は、RADIUS、TACACS+、SAMLアイデンティティプロバイダ(IdP)サーバーを使用して、管 理者の認証と承認を管理する場合のみです。アクセスドメインを有効にするには、以下を定義 する必要があります。

- 外部認証サーバーのサーバープロファイル 「Device (デバイス) > Server Profiles (サーバープロファイル) > RADIUS」、「Device (デバイス) > Server Profiles (サーバープロファイル) > TACACS+」、「Device (デバイス) > Server Profiles (サーバープロファイル) > SAML Identity Provider (SAML アイデンティティ プロバイダ)」を参照してください。
- RADIUS ベンダー固有属性(VSA)、TACACS+ VSA、SAML 属性のいずれか。

管理者がファイアウォールへのログインを試みると、ファイアウォールは管理者のアクセスド メインを外部サーバーに問い合わせます。外部サーバーは、関連付けられているドメインを返 し、ファイアウォールは、アクセスドメインで指定されている仮想システムに管理者を制限し ます。ファイアウォールが管理者の認証と承認に外部サーバーを使用しない場合、Device(デ バイス) > Access Domain(アクセスドメイン)の設定は無視されます。

Panorama では、アクセスドメインをローカルで管理することや、RADIUS
 VSA、TACACS+ VSA、SAML 属性を使用して管理することができます(「Panorama > Access Domains(アクセスドメイン)」を参照)。

アクセス ドメイン設定	の意味
氏名	アクセスドメインの名前(最大 31 文字)を入力します。名前 の大文字と小文字は区別されます。また、一意の名前にする必 要があります。文字、数字、ハイフン、アンダースコア、およ びピリオドのみを使用してください。
仮想システム	Available(使用可能)列で仮想システムを選択して Add(追 加)します。
	アクセスドメインは、仮想システムをサポートするファイア ウォールのみにおいてサポートされます。

Device > Authentication Profile [デバイス > 認証プロ ファイル]

管理者とエンド ユーザーを認証するための設定を構成するには、このページを使用します。ファイアウォールと Panorama では、ローカル、RADIUS、TACACS +、LDAP、Kerberos、SAML 2.0、多要素認証(MFA)サービスがサポートされます。

 認証プロファイルを1つ以上作成して外部認証を提供することで、管理を行いやす くなるようにすべての認証リクエストを一か所にまとめ、トラッキングなどのサー ビスを含む標準的な認証プロセスを使用します。認証が失敗した場合に複数の方 式を使う複数の認証プロファイルを作成して優先順位を付け(Device (デバイス) > Authentication Sequence (認証シーケンス))、ローカルのログインアカウントを1 つ以上作成してすべての外部方式が失敗した場合にフォールバックすることがベス トプラクティスになります。

このページを使用して、ファイアウォールまたは Panorama のサービス(Web インターフェイ スへの管理アクセスなど)を SAML アイデンティティ プロバイダ(IdP)で登録することもでき ます。サービスを登録すると、ファイアウォールや Panorama では IdP が使用され、サービスを 要求するユーザーを認証できます。サービスを登録するには、SAML メタデータを IdP で入力し ます。ファイアウォールと Panorama では、サービスに割り当てた認証プロファイルに基づいて SAML メタデータ ファイルが自動的に生成され、このメタデータ ファイルを IdP にエクスポー トできるため、登録が簡単です。

- 認証プロファイル
- SAML Metadata Export from an Authentication Profile (認証プロファイルから SAML メタ データをエクスポートする)

認証プロファイル

• Device > Authentication Profile [デバイス > 認証プロファイル]

Device(デバイス) > Authentication Profile(認証プロファイル)または Panorama > Authentication Profile(認証プロファイル)を選択し、認証プロファイルを管理します。新しい プロファイルを作成するには、プロファイルを Add(追加)して次のフィールドに情報を入力 します。

認証プロファイルを設定したら、CLIコマンド「test authentication」を使用して、ファイアウォールまたは Panorama 管理サーバーがバックエンド認証サーバーと通信できるかどうか、および認証要求が成功しているかどうかを調べます。 候補設定でauthentication tests(認証テスト) ■を実行できるため、コミットする前に設定が正しいかどうかを確認できます。

認証プロファイル設 定	の意味
氏名	プロファイルの識別に使用する名前を入力します。名前の大文字と 小文字は区別され、文字、数字、スペース、ハイフン、アンダースコ ア、およびピリオドのみを含む最大 31 文字を指定できます。名前は、 他の認証プロファイルや認証シーケンスに対して、現在の Location[場 所] (ファイアウォールまたは仮想システム) で一意である必要がありま す。
	マルチ仮想システムモードのファイアウォールで、認証プロファイルのLocation(場所)が仮想システムになっている場合、共有の場所の認証シーケンスと同じ名前を入力しないでください。同様に、プロファイルのLocation(場所)がShared(共有)になっている場合、仮想システムシーケンスと同じ名前を入力しないでください。このようなケースでは、同じ名前の認証プロファイルおよびシーケンスをコミットすることはできますが、参照エラーが発生する可能性があります。
場所	プロファイルを使用できる範囲を選択します。複数の仮想シス テム (vsys) があるファイアウォールの場合、vsys を選択する か、Shared[共有] (すべての仮想システム) を選択します。その他の 場合、Location(場所)を選択することはできません。この値は Shared(共有)(ファイアウォール)または Panorama として事前に定 義されています。プロファイルを保存すると、その[場所] を変更でき なくなります。

Authentication [認証]タブ

ファイアウォールでは、このタブで設定する認証サービスが起動されてから、Factors(ファ クター)タブで追加する多要素認証(MFA)サービスが起動されます。

ベンダー API ではなくて RADIUS によってファイアウォールを MFA ベンダー と統合する場合は、MFA サーバー プロファイルではなくて、そのベンダーの RADIUS サーバー プロファイルを設定する必要があります。

タイプ ユーザーに表示される最初の(時に唯一の)認証チャレンジを提供す るサービスのタイプを選択します。選択内容に応じて、そのサービス に定義する、その他の設定がダイアログに表示されます。オプション は次のとおりです:

- None (なし) 認証を使用しません。
- クラウド認証サービス:クラウド ID エンジンが提供するクラウド ベースの認証サービスを使用します。
| 認証プロファイル設
定 | の意味 |
|--|---|
| | Local Database (ローカル データベース) – ファイアウォール
のローカル認証データベースを使用します。このオプションは
Panorama では使用できません。 |
| | RADIUS – RADIUS (Remote Authentication Dial In User Service)
サーバーを使用します。 |
| | TACACS+ – TACACS+(Terminal Access Controller Access-Control
System Plus)サーバーを使用します。 |
| | LDAP – LDAP (Lightweight Directory Access Protocol) サーバーを
使用します。 |
| | • Kerberos – Kerberos サーバーを使用します。 |
| | • SAML – SAML 2.0 (Security Assertion Markup Language 2.0) アイ
デンティティ プロバイダ (IdP) を使用します。 |
| | 管理者は SAML を使用して、ファイアウォールまたは
Panorama Web インターフェイスに対して認証できます
が、CLI に対しては認証できません。 |
| サーバ プロファイ
ル
(RADIUS、TACACS
+、LDAP、Kerberos
のみ) | ドロップダウンリストから認証サーバー プロファイルを選択しま
す。Device (デバイス) > Server Profiles (サーバー プロファイル) >
RADIUS、Device (デバイス) > Server Profiles (サーバー プロファイル)
> TACACS +、Device (デバイス) > Server Profiles (サーバー プロファイ
ル) > LDAP、または Device (デバイス) > Server Profiles (サーバー プロ
ファイル) > Kerberosを参照。 |
| IdPサーバープロ
ファイル
(<mark>SAML のみ</mark>) | ドロップダウン リストから SAML アイデンティティ プロバイダのサー
バー プロファイルを選択します。Device (デバイス) > Server Profiles
(サーバー プロファイル) > SAML Identity Provider (SAML アイデンティ
ティ プロバイダ)を参照。 |
| RADIUS からユー
ザー グループを取
得
(RADIUS のみ) | RADIUS サーバーに定義されているベンダー固有属性(VSA)からユー
ザー グループ情報を収集するには、このオプションを選択します。
ファイアウォールではこの情報が使用され、認証しているユーザー
と許可リストのエントリが照合されます。ポリシーの適用やレポート
の生成に、この情報は使用されません。 |
| TACACS+ からユー
ザー グループを取
得
(TACACS+ のみ) | TACACS+サーバーに定義されているベンダー固有属性(VSA)から
ユーザー グループ情報を収集するには、このオプションを選択しま
す。ファイアウォールではこの情報が使用され、認証しているユー
ザーと許可リストのエントリが照合されます。ポリシーの適用やレ
ポートの生成に、この情報は使用されません。 |

デバイス

認証プロファイル設 定	の意味
ログイン属性 (<mark>LDAP のみ</mark>)	ユーザーを一意に識別し、そのユーザーのログイン ID として機能する LDAP ディレクトリ属性を入力します。
パスワード失効の 警告 (LDAP のみ)	認証プロファイルが GlobalProtect ユーザー用である場合、パスワード の有効期限が x 日後に切れるという通知メッセージを何日前からユー ザーに表示するのか、日数を入力します。デフォルトでは、通知メッ セージはパスワードの有効期限の 7 日前から表示されます(範囲は 1 ~ 255 日)。パスワードの期限が切れたユーザーは、VPN にアクセス できなくなります。
	 pre-logon 接続方式 を使用するように GlobalProtect エージェントを設定する ことも検討してみてください。これにより、パスワード の期限が切れた後でも、ユーザーはドメインに接続して パスワードを変更できます。
	ユーザーがパスワードを期限切れにしてしまった場合、管理者は仮 のLDAPパスワードを割り当て、ユーザーがVPNにログインできるよ うにすることもできます。このワークフローでは、ポータル設定の Cookie authentication for config refresh[設定更新のためのCookie認証] を Authentication Modifier[認証修飾子] に設定することをお勧めしてい ます(このように設定しない場合、仮のパスワードを使用してポータ ルへの認証を行うことができますが、ゲートウェイログインが失敗し てしまい、VPNへのアクセスが行えません)。
署名要求の証明書 (SAML のみ)	アイデンティティ プロバイダ (IdP) に送信する SAML メッセージへ の署名のためにファイアウォールで使用する証明書を選択します。こ のフィールドは、IdP Server Profile (IdP サーバ プロファイル)でSign SAML Message to IdP (IdP への SAML メッセージの署名) オプションを 有効にする場合に必要です。 (Device (デバイス) > Server Profiles (サー バプロファイル) > SAML Identity Provider (SAML アイデンティティプ ロバイダ) を参照)。その他の場合、SAML メッセージに署名するために 証明書を選択するかどうかは任意です。
	証明書および関連付けられている秘密鍵の生成またはインポートを行 うときには、証明書に指定されている鍵の用途の属性により、鍵の使 用方法が制御されます。
	 証明書で鍵の用途の属性が明示的にリストされている場合、属性の 1つはデジタル署名です。デジタル署名はファイアウォールで生成 する証明書では使用できません。このような場合は、エンタープラ イズ認証局(CA)、またはサードパーティ CA から証明書と鍵をイ ンポートする必要があります。

認証プロファイル設 定	の意味
	 証明書で鍵の用途の属性が指定されていない場合は、メッセージの署名も含めて、どのような目的にも鍵を使用できます。このような場合は、任意の方法で証明書と鍵を取得
	して SAML メッセージに署名できます。
	 Palo Alto Networks では、署名証明書を使用して、IdP に 送信する SAML メッセージの整合性を確保することをお 勧めしています。
シングルログアウ トの有効化 (<mark>SAML のみ</mark>)	 1つのサービスからログアウトしたユーザーが、すべての認証済みサービスからログアウトできるようにするには、このオプションを選択します。シングルログアウト(SLO)は、ユーザーがSAML認証でアクセスしたサービスにのみ適用されます。サービスが組織の外部にあるか組織の内部(ファイアウォールWebインターフェイスなど)にあるかは問いません。このオプションが適用されるのは、Identity Provider SLO URL(アイデンティティプロバイダ SLO URL)をIdPサーバープロファイルで入力した場合のみです。Authentication Portal(認証ポータル)ユーザーに対しては、SLOを有効化できません。 ユーザーのログアウト後、ファイアウォールで
	 は IP アドレスとユーザーネームのマッピング が自動的に削除されます。
証明書プロファイ ル	ファイアウォールで検証に使用する証明書プロファイルを選択しま す。
(SAML のみ)	 IdP サーバー プロファイルで指定されている Identity Provider Certificate (アイデンティティ プロバイダ証明書)です。IdP ではこ の証明書が使用されて、ファイアウォールに対して認証が行われま す。認証プロファイル設定を Commit (コミット)すると、ファイ アウォールでは証明書が検証されます。
	 シングルサインオン(SSO)とシングルログアウト(SLO)の認証のために IdP がファイアウォールに送信する SAML メッセージ。IdPは、IdPサーバープロファイルで指定されている Identity Provider Certificate(アイデンティティプロバイダ証明書)を使用してメッセージに署名します。
	Device (デバイス) > Certificate Management (証明書の管理) > Certificate Profile (証明書プロファイル)」を参照してください。
ユーザー ドメイン	ファイアウォールでは、認証しているユーザーと許可リス トのエントリの照合、および User-ID グループ マッピング

デバイス

認証プロファイル設 定	の意味
AND	đ
ユーザー名修飾子	に User Domain(ユーザー ドメイン)が使用されます。
(SAML およびクラ ウド認証サービス を除くすべての認 証タイプ)	Username Modifier(ユーザー名修飾子)を指定して、ユーザーがログ イン時に入力するドメインおよびユーザー名の形式を変更することが できます。ファイアウォールでは、変更された文字列が認証に使用さ れます。以下のオプションから選択します。
	 未変更のユーザー入力のみを送信するには、User Domain(ユー ザードメイン)を空白(デフォルト)のままにして、Username Modifier(ユーザー名修飾子)を変数 %USERINPUT%(デフォル ト)に設定します。
	 ユーザー入力の前にドメインを追加するには、User Domain(ユー ザードメイン)を入力して、Username Modifier(ユーザー名修飾 子)を %USERDOMAIN%\%USERINPUT%に設定します。
	 ユーザー入力にドメインを追加するには、User Domain(ユーザー ドメイン)を入力し、Username Modifier(ユーザー名修飾子)を %USERINPUT%@%USERDOMAIN%に設定します。
	 Username Modifier に %USERDOMAIN% 変数が含まれている場合、User Domain 値がユーザーが入力したドメイン文字列に置き換わります。%USERDOMAIN% 変数を指定して User Domain[ユーザードメイン]を空白のままにすると、ファイアウォールはユーザーが入力したドメイン文字列を削除します。ファイアウォールは、ドメイン名をUser-IDグループマッピングに適したNetBIOS名に解決します。これは親ドメインと子ドメインの両方に適応されます。User Domain 修飾子は、自動的に派生した NetBIOS 名よりも優先されます。
	 ファイアウォールがサーバプロファイル タイプを使用して、認証 シーケンスでユーザー入力のフォーマットをいつどのように変更す るかを決定できるようにするには Username Modifier (ユーザー名修 飾子) として Noneを手動で入力します。このオプションの詳細につ いては、『PAN-OS 管理者ガイド』の認証プロファイルおよびシー ケンスの設定を参照してください。
Kerberos レルム (SAML およびクラ ウド認証サービス を除くすべての認 証タイプ)	ネットワークで Kerberos シングル サインオン (SSO) がサポートされ ている場合、Kerberos Realm[Kerberos レルム] (最大 127 文字) を入 力します。これは、ユーザー ログイン名のホスト名部分です。例: ユーザー アカウント名が user@EXAMPLE.LOCAL の場合、レルムは EXAMPLE.LOCAL になります。

-"	8	17
アノ	17	

認証プロファイル設 定	の意味
Kerberos キータブ	ネットワークで Kerberos シングルサインオン(SSO)
(SAMLおよびクラ ウド認証サービス を除くすべての認 証タイプ)	 がサポートされている場合、Import(インポート)、Browse(参照)の順にクリックしてキータブファイルを見つけたらOKをクリックします。キータブには、SSO認証に必要となる、ファイアウォールのKerberosアカウント情報(プリンシパル名およびハッシュされたパスワード)が含まれています。各認証プロファイルに、1つのキータブを含めることができます。ファイアウォールは、認証中にまずキータブを使用してSSOを確立しようとします。これに成功した場合、アクセスを試行しているユーザーが許可リストに含まれていれば、認証は即座に成功します。含まれていない場合、認証プロセスは、指定したType(タイプ)の手動認証(ユーザー名/パスワード)にフォールバックします。Type(タイプ)にはKerberos以外のタイプも指定できます。 ファイアウォールがFIPS/CCモードの場合、アルゴリズムはaes128-cts-hmac-sha1-96またはaes256-cts-hmac-sha1-96に設定されている必要があります。それ以外の場合、des3-cbc-sha1またはarcfour-hmacも使用できます。ただし、キータブのアルゴリズムと、SSOを有効にするためにチケット発行サービスからクライアントに発行されるサービスチケットのアルゴリズムが一致していない場合、SSOプロセスは失敗します。サービスチケットで使用されるアルゴリズムは、Kerberos管理者が決定します。
ユーザー名属性 (SAML のみ)	IdP からのメッセージに含まれる、認証しているユーザーのユーザー名 を特定する SAML 属性を入力します(デフォルトは username)。IdP Server Profile (IdP サーバー プロファイル)にユーザー名属性を指 定するメタデータが含まれている場合、ファイアウォールでは、この フィールドにそのユーザー名属性が自動的に入力されます。ファイア ウォールでは、SAML メッセージから取得されたユーザー名が、認証 プロファイルの Allow List(許可リスト)のユーザーおよびユーザー グループと照合されます。SAML ログイン時に入力するドメイン/ユー ザー名の文字列を変更するようにファイアウォールを設定することは できないため、ログインユーザー名は Allow List(許可リスト)のエン トリと正確に一致する必要があります。必須の SAML 属性はこれのみ です。

認証プロファイル設 定	の意味
	SAML メッセージのサブジェクト フィールドには、ユー ザー名が表示されることがあります。ユーザー名属性に ユーザー名が表示されない場合、ファイアウォールでは サブジェクト フィールドが自動的にチェックされます。
ユーザー グループ 属性 (<mark>SAML のみ</mark>)	IdP からのメッセージで、認証しているユーザーのユーザー グループ を特定する SAML 属性を入力します (デフォルトは usergroup)。 IdP Server Profile (IdP サーバー プロファイル) にユーザー グループ属性 を指定するメタデータが含まれている場合、このフィールドでは、そ のユーザー グループ属性が自動的に使用されます。ファイアウォール ではグループ情報が使用され、認証しているユーザーと Allow List (許 可リスト)のエントリが照合されます。ポリシーやレポートに、この 情報は使用されません。
管理者ロール属性 (SAML のみ)	IdP からのメッセージで、認証しているユーザーの管理者ロールを特定 する SAML 属性を入力します(デフォルトは admin-role)。この属性 は、エンド ユーザーではなく、ファイアウォール管理者にのみ適用さ れます。IdP Server Profile(IdP サーバー プロファイル)に管理者ロー ル属性を指定するメタデータが含まれている場合、ファイアウォール では、このフィールドにその管理者ロール属性が自動的に入力されま す。ファイアウォールでは、事前定義(ダイナミック)ロールまたは 管理者ロール プロファイルが、SAML メッセージから取得したロール と照合され、ロールベースのアクセス制御が適用されます。ロールが 1 つのみの管理者に対して複数の管理者ロールの値が SAML メッセージ に含まれる場合は、管理者ロール属性の最初の(左端の)値のみが照 合されます。ロールが複数ある管理者の場合は、その属性の複数の値 が照合されます。
アクセス ドメイン 属性 (SAML のみ)	IdP からのメッセージで、認証しているユーザーのアクセスドメインを 特定する SAML 属性を入力します(デフォルトは access-domain)。こ の属性は、エンド ユーザーではなく、ファイアウォール管理者にのみ 適用されます。IdP Server Profile(IdP サーバー プロファイル)にアク セスドメイン属性を指定するメタデータが含まれている場合、ファイ アウォールでは、このフィールドにそのアクセスドメイン属性が自動 的に入力されます。ファイアウォールでは、ローカルに設定されてい るアクセスドメインが、SAML メッセージから取得したアクセスドメ インと照合され、アクセス制御が適用されます。アクセスドメインが 1 つのみの管理者に対して複数のアクセスドメインの値が SAML メッ セージに含まれる場合は、アクセスドメインが複数ある管理者の場合 は、その属性の複数の値が照合されます。
リージョン	クラウド ID エンジン インスタンスのリージョン エンドポイントを選 択します。

デバイス

認証プロファイル設 定	の意味
(クラウド認証サー ビスのみ)	選択するリージョンは、Cloud Identity Engine インスタン スをアクティベート するときに選択したリージョンと一 致する必要があります。
インスタンス (クラウド認証サー ビスのみ)	複数のインスタンスがある場合は、使用する Cloud Identity エンジンイ ンスタンスを選択します。
プロファイル (クラウド認証サー ビスのみ)	複数のクラウド ID エンジン ID プロバイダー プロファイル (ldP プロ ファイル) がある場合は、使用するクラウド ID エンジン ldP プロファ イルを選択します。
最大クロックス キュー(秒) (クラウド認証サー ビスのみ)	ファイアウォールが ldP から受信したメッセージを検証する時点 で、ldP とファイアウォールのシステム時間に対して許容される最大時 間差を秒単位で入力します(範囲は 1 ~ 900、デフォルトは 60)。時 間差がこの値を超える場合、検証(つまり、認証)は失敗します。
クラウドで多要素 認証を強制する (クラウド認証サー ビスのみ)	IdP が多要素認証を使用してログインすることをユーザーに要求するように構成されている場合は、クラウド で を強制的に多要素認証を有効 にします。
Factors(ファクター)タブ	
追加の認証ファク ターの有効化	ユーザーが最初の要素(Authentication(認証)タブの Type(タイ プ)フィールドに指定)に正常に応答した後で、追加の認証ファク ター(チャレンジ)をファイアウォールで起動する場合は、このオプ ションを選択します。

A	追加の認証ファクタは、認証ポリシーのみを使用する
U	エンドユーザー認証でサポートされます。GlobalProtect
	ポータルとゲートウェイへのリモートユーザー認証、ま
	たは PAN-OS パノラマ Web インターフェイスへの管理者
	認証では、その他のファクターはサポートされていませ
	ん。追加のファクターを設定することはできますが、こ
	れらの使用例に対しては強制されません。ただし、すべ
	ての認証使用例について、RADIUS または SAML を使用し
	て MFA ベンダーと統合することはできます。
夕雨	ま刻訂(MFA)たは田子フ羽訂プロフィノルた乳ウルチ

多要素認証(MFA)を使用する認証プロファイルを設定した ら、認証を実施するオブジェクト(Objects(オブジェクト)> Authentication(認証))にその認証プロファイルを割り当てた後、

認証プロファイル設 定	の意味
	そのオブジェクトを認証ポリシー ルール(Policies(ポリシー)> Authentication(認証))に割り当て、ネットワーク リソースへのアク セスを制御する必要があります。
度	ユーザーが最初の要素(Authentication(認証)タブの Type(タイ プ)フィールドで指定)に正常に応答した後、ファイアウォールが起 動する認証要素ごとに、MFA サーバープロファイル(Device(デバ イス) > ServerProfiles > Multi Factor Authentication(多要素認証)) を追加します。ファイアウォールでは、要素を提供する MFA サービ スのリストの上から下へと、順に各要素が起動されます。この順番 を変更する場合は、サーバープロファイルを選択して Move Up(上 へ)または Move Down(下へ)をクリックします。指定できる追加 要素は 3 つまでです。各 MFA サービスが提供する要素は 1 つです。 一部の MFA サービスでは、ユーザーが複数の要素のリストから 1 つ の要素を選択できます。ファイアウォールは、ベンダー API によっ て、これらの MFA サービスと統合します。その他の MFA vendor API integrations(MFA ベンダー API 統合)は、Applications(アプリケー ション)または Applications and Threats(アプリケーションと脅威) コンテンツ更新により定期的に追加されます。
Advanced Tab(詳細	タブ)
許可リスト	Add (追加)をクリックして all (すべて)を選択するか、このプロ ファイルで認証できる特定のユーザーおよびグループを選択します。 ユーザーが認証を行うと、ファイアウォールでは、関連付けられてい るユーザー名またはグループが、このリストのエントリと照合されま す。エントリを追加しないと、ユーザーの認証を行うことができませ ん。 アクセスを行わなければならない正当なビジネス上の理 由を持っているユーザーに認証を限定して攻撃の入り口 を減らすには、ユーザーあるいはユーザーグループを指 定し、all (すべて)は使用しないでください。
	 [ユーザードメイン]の値を入力した場合、[許可リスト]でドメインを指定する必要はありません。たとえば、User Domain (ユーザードメイン)が businessincで、ユーザー admin1を Allow List(許可リスト)に追加する場合、「admin1」と入力すれば、「businessinc \admin1」と入力したことになります。ディレクトリサービスにすでに存在するグループを指定するか、LDAPフィルタに基づいてカスタムグループを指定できます。

認証プロファイル設 定	の意味	
最大試行回数 (<mark>SAML を除</mark> くす べての認証タイ プ)	ファイアウォールで許容されるログイン連続試行回数(0~10)を入力 します。この回数を超えるとユーザーアカウントはロックアウトされ ます。値0を指定すると、無制限にログインを試行できます。デフォ ルト値は、通常の運用モードのファイアウォールでは0、FIPS-CC モー ドのファイアウォールでは10です。	
	 Failed Attempts (試行失敗回数)の値を5以下に設定し、入 カミスに備えてある程度猶予を持たせつつ、悪意のある システムがブルートフォースによってファイアウォール にログインしようとするのを防ぎます。 	
	 Failed Attempts[最大試行回数] を 0 以外の値に設定して も、Lockout Time[ロックアウト時間] を 0 のままにしてお くと、Failed Attempts[最大試行回数] は無視され、ユー ザーはロックアウトされません。 	
ロックアウト時間 (<mark>SAML</mark> を除くす べての認証タイ プ)	ユーザーが Failed Attempts(最大試行回数)の数値に達した場合に ファイアウォールがユーザー アカウントをロックアウトする時間(範 囲は 0 ~ 60 分、デフォルトは 0 分)を入力します。値を 0 にすると、 管理者が手動でユーザー アカウントをロック解除するまでロックアウ トが適用されます。	
	Lockout Time (ロックアウト時間)を 30 分以上に設定し、 攻撃者が続けてログインを試みるのを防ぎます。	
	 Lockout Time[ロックアウト時間] を 0 以外の値に設定して も、Failed Attempts[最大試行回数] を 0 のままにしてお くと、Lockout Time[ロックアウト時間] は無視され、ユーザーはロックアウトされません。 	

SAML Metadata Export from an Authentication Profile (認証プロ ファイルから SAML メタデータをエクスポートする)

• Device > Authentication Profile [デバイス > 認証プロファイル]

ファイアウォールや Panorama は、サービスを要求したユーザーを SAML アイデンティティ プ ロバイダ (IdP) を使用して認証できます。管理者の場合、サービスは Web インターフェイス へのアクセスになることもあります。エンド ユーザーの場合、サービスはネットワーク リソー スへのアクセスを可能にするAuthentication Portal (認証ポータル)または GlobalProtect であ る場合があります。サービスの SAML 認証を有効にするには、IdP でそのサービスの特定の情報 (SAML メタデータ形式)を入力して、サービスを登録する必要があります。ファイアウォール や Panorama は、サービスに割り当てた認証プロファイルに基づいて SAML メタデータファイ ルを自動生成することで登録を簡略化します。このメタデータ ファイルは ldP にエクスポート できます。メタデータのエクスポートは、ldP の各メタデータ フィールドに値を入力するよりも 簡単に行うことができます。

エクスポートファイルのメタデータの一部は、認証プロファイルに割り当てられた SAML IdP サーバー プロファイルから取得されます(Device(デバイス) > Server Profiles(サーバー プロファイル) > SAML Identity Provider(SAML アイデンティ ティ プロバイダ))。ただし、エクスポートファイルでは、SAML IdP サーバープ ロファイルで指定されたメソッドに関係なく、HTTP バインディングメソッドとし て常に POST が指定されます。IdP は POST メソッドを使用して SAML メッセージを ファイアウォールまたは Panorama に送信します。

認証プロファイルから SAML メタデータをエクスポートするには、Authentication(認証)列の SAML Metadata(メタデータ)リンクをクリックし、以下のフィールドを入力します。メタ データ ファイルを IdP にインポートする方法については、IdP のドキュメントを参照してください。

SAML メタデータのエ クスポート設定	の意味
Commands (コマン ド)	 SAML メタデータをエクスポートするサービスを選択します。 management(管理)(デフォルト) – Web インターフェイスへの管理者アクセスを提供します。 Authentication Portal(認証ポータル) – Authentication Portal(認証ポータル)を経由でネットワークリソースへのエンドユーザーアクセスを提供します。 global-protect(GlobalProtect) – GlobalProtect を介したネットワークリソースへのエンドユーザーアクセスを提供します。 選択内容により、ダイアログに表示されるフィールドが変わります。
[Management(管 理) Authentication Portal(認証ポータ ル) GlobalProtect] Auth Profile(認証プ ロファイル)	メタデータのエクスポート元である認証プロファイルの名前を入力し ます。デフォルト値は、 Metadata (メタデータ)リンクをクリック して開いたときのプロファイルです。
Management Choice(管理の選 択) (管理のみ)	 管理トラフィックで有効にするインターフェイス(MGT インターフェイスなど)を指定するためのオプションを選択します。 Interface (インターフェイス) – ファイアウォールのインターフェイスのリストからインターフェイスを選択します。 IP Hostname (IP ホスト名) – インターフェイスの IP アドレスまたはホスト名を入力します。ホスト名を入力する場合、DNS サー

SAML メタデータのエ クスポート設定	の意味
	バーのアドレス(A)レコードが IP アドレスにマッピングされて いる必要があります。
[Authentication Portal(認証ポータ ル) GlobalProtect] Virtual System(仮想 システム)	Authentication Portal(認証ポータル)設定または GlobalProtect ポータルを定義する仮想システムを選択します。
(Authentication Portal(認証ポー タル)または GlobalProtect のみ)	
IP ホスト名	サービスの IP アドレスまたはホスト名を入力します。
(Authentication Portal(認証ポー タル)または GlobalProtect のみ)	 Authentication Portal (認証ポータル) – Redirect Host (リダ イレクトホスト)のIPアドレスまたはホスト名を入力します (Device (デバイス) > User Identification (ユーザー ID) > Authentication Portal Settings (認証ポータル設定))。
	 GlobalProtect – GlobalProtect ポータルの Hostname (ホスト 名)または IP Address (IP アドレス)を入力します。
	ホスト名を入力する場合、DNS サーバーのアドレス(A)レコードが IP アドレスにマッピングされている必要があります。

Device > Authentication Sequence [デバイス > 認証シー ケンス]

- Device > Authentication Sequence [デバイス > 認証シーケンス]
- Panorama > Authentication Sequence [デバイス > 認証シーケンス]

ー部の環境では、ユーザーアカウントが複数のディレクトリ内に存在します(LDAP や RADIUSなど)。認証シーケンスとはログインの際にファイアウォールが使用する一連の認証プ ロファイルを指します。ファイアウォールは1つのプロファイルで正常にユーザーが認証される まで、リストの上から下へ順番に、認証、Kerberosシングルサインオン、許可リスト、アカウン トロックアウト値を含めたプロファイルをすべて試行し、各ユーザーに適用します。シーケンス のすべてのプロファイルで認証できなかった場合にのみ、ファイアウォールはアクセスを拒否し ます。認証プロファイルの詳細は「Device(デバイス)> Authentication Profile(認証プロファ イル)」を参照してください。



異なる認証方法を使用する複数の認証プロファイルを持つ認証シーケンスを設定し ます。2つ以上の外部認証方式、単一のローカル(内部)方式を設定し、接続の問 題で認証が妨げられないようにします。ローカル認証プロファイルをシーケンスの 最後のプロファイルにすることで、すべての外部認証が失敗した場合にのみそれを 使用するようにします。(外部認証はロギングやトラブルシューティング機能が含 まれる専用の、信頼できる一元的な認証サービスを提供します)

認証シーケンス設定	の意味
氏名	シーケンスの識別に使用する名前を入力します。名前の大文字と小文 字は区別され、文字、数字、スペース、ハイフン、アンダースコア、 およびピリオドのみを含む最大 31 文字を指定できます。名前は、他 の認証シーケンスや認証プロファイルに対して、現在の Location[場 所] (ファイアウォールまたは仮想システム) で一意である必要があり ます。
	複数の仮想システムがあるファイアウォールで、認証シーケンスの[場所]が仮想システム(vsys)になっている場合、共有の場所の認証プロファイルと同じ名前を入力しないでください。同様に、シーケンスのLocation(場所)がShared(共有)になっている場合、vsysのプロファイルと同じ名前を入力しないでください。このようなケースでは、同じ名前の認証シーケンスおよびプロファイルをコミットすることはできますが、参照エラーが発生する可能性があります。
場所	シーケンスを使用できる範囲を選択します。複数の仮想シス テム (vsys) があるファイアウォールの場合、vsys を選択する か、Shared[共有] (すべての仮想システム) を選択します。その他の

認証シーケンス設定	の意味
	場合、Location(場所)を選択することはできません。この値は Shared(共有)(ファイアウォール)または Panorama として事前に 定義されています。シーケンスを保存すると、その [場所] を変更で きなくなります。
認証に失敗したとき にシーケンスを終了 する	ログイン時にユーザが入力したクレデンシャルが認証シーケンス内 の任意の認証プロファイルと一致した場合(正規化の有無にかかわら ず)、ファイアウォールが残りの認証シーケンスを上から下への順序 で完了させるのではなく、ユーザを正常に認証できない場合、ファイ アウォールは認証シーケンスを中止します。
ドメインを使用して 認証プロファイルを 決定します	次のオプションは、LDAP 認証プロファイルにのみ適用され、デフォ ルトで有効になっています。
	User-IDドメインを使用して認証プロファイルを決定する:ドメイン名 を使用して認証プロファイルを順番にチェックする前に、ユーザーが ログイン時に入力するドメイン名を正規化します。(オプションです が、推奨)認証シーケンスを適用する前に、ユーザーがログイン時に 入力するドメイン名を正規化するには、User-IDドメインを使用して 認証プロファイルを決定するを選択します。
	このオプションを無効にすると、firewall はドメイン名を正規化せ ず、認証が成功しなかった場合でも、ドメイン名と認証プロファイル を上から下の順序で照合しようとします。
認証プロファイル	Add[追加] をクリックし、シーケンスに追加する各認証プロファイル のドロップダウンリストから選択します。リストの順番を変更するに は、プロファイルを選択して Move Up[上へ] または Move Down[下 へ] をクリックします。プロファイルを削除するには、プロファイル を選択して Delete[削除] をクリックします。
	多要素認証(MFA)サーバープロファイルまたは Security Assertion Markup Language(SAML)アイデン ティティプロバイダサーバープロファイルを指定する 認証プロファイルは追加できません。

Device (デバイス) > IoT Security (IoTセキュリティ) > DHCP Server Log Ingestion (DHCPサーバーのログ取り 込み)

IoT Security は、IP アドレスから MAC アドレスへのバインドに依存して、観察されたネット ワーク動作を IoT デバイスに帰属させ、それらを一意に追跡します。IoT セキュリティは通常、 次世代の firewall によって収集された DHCP トラフィックを使用して、IP アドレスと MAC ア ドレスのバインドを学習し、IP アドレスの変更を追跡します。ただし、DHCP データ パスに firewall を配置できない場合は、この方法を使用して DHCP サーバー ログを取り込み、DHCP トラフィックの可視性を拡張できます。

DHCP トラフィックをファイアウォールにルーティングしたり、ファイアウォールを経由したりすることが難しいネットワークでは、サーバー ログを syslog メッセージとしてファイアウォールに送信するように DHCP サーバーを構成します。次に、firewall は、メッセージをdhcp-syslog のサブタイプを持つ拡張アプリケーション ログ (EAL) として、ログサービスを介して IoT セキュリティに転送します。IoT Security はそれらを解析して IP アドレスと MAC アドレスのバインドを学習し、新しく学習したデバイスをインベントリに追加します。



前提条件

- 次世代の firewall で実行されている syslog サーバにメッセージを送信するように設定された syslog 機能を備えた DHCP サーバ
- 有効な IoT セキュリティ サブスクリプションを備えた PAN-OS 11.1 以降を実行する次世代 ファイアウォール

次世代のFirewall をセットアップする

1 つ以上の DHCP サーバーから syslog メッセージを受信するように次世代の firewall を設定し ます。firewall は、受信した syslog メッセージを EAL として自動的にロギング サービスに転送 し、ログ サービスはそれらを IoT セキュリティにストリーミングして解析および分析します。 **1.** 次世代ファイアウォールに DHCP サーバーを追加します。

次世代の firewall にログインし、**Device > IoT > + Add** を選択し、次のように構成して、**OK** をクリックします。

項目	の意味
名前	DHCP サーバーの名前を入力します。スペースを含めて最大 32 文字です。
詳説	後で参照できるように、DHCP サーバーに関するメモを入力します。ス ペースを含めて最大 256 文字です。
有効化	選択すると、firewall が DHCP サーバからの接続をリッスンし、接続が来 たときに処理できるようになります。
IPアドレス	DHCP サーバーがファイアウォールに接続する IP アドレスを入力しま す。アドレスは、IPv4 または IPv6 フォーマットにすることができま す。FQDN は許可されません。
プロトコル	 TCP、UDP、またはSSLを選択します。選択するときは、DHCPサーバーとfirewall間の接続にとって何が重要かを考慮するようにします。TCPは送信時の信頼性を提供しますが、セキュリティは提供しません。UDPは、処理オーバーヘッドが低く、速度が速いですが、信頼性とセキュリティに欠けています。SSLは信頼性とセキュリティを提供しますが、より多くのオーバーヘッドが発生します。 firewallは、ポート10514でTCPとUDPを使用したDHCPサーバー接続をリッスンし、ポート16514でSSLを使用した接続をリッスンします。

2. 前の手順を繰り返して、さらに DHCP サーバーを追加します。

必要に応じて、DHCP サーバーを追加して、ネットワーク全体の DHCP トラフィックの可視 性を拡張します。すべての次世代 firewall は、firewall あたり最大 100 台の DHCP サーバを サポートします。

シスログ用の DHCP サーバのセットアップ

サーバ ログの syslog メッセージを次世代 firewall の管理インターフェイスに送信するように DHCP サーバを設定します。firewall で設定されているのと同じプロトコルを使用するように DHCP サーバを設定します。TCP、UDP、または SSL。構成手順については、DHCP サーバーの ドキュメントを参照してください。

DHCP サーバーの接続状態を確認する

構成されているすべての DHCP サーバーを表示するには、Device > IoT を選択します。

DHCP サーバー名の横にある緑色の円は、そのサーバーが Panorama で設定されており、ローカルの次世代ファイアウォールの Web インターフェイスで表示した場合は読み取り専用であることを意味します。

TCPまたはSSLを使用しているDHCPサーバーが現在firewallに接続されている場合、[ステータ ス]列に「接続済み」と表示されます。UDPを使用する DHCP サーバーが過去2時間以内に接続 されている場合は、この列にも「接続済み」と表示されます。それ以外の場合は、[ステータス] 列は空になり、サーバーが現在ファイアウォールに接続されていないことを示します。

次の CLI コマンドは、DHCP サーバーの設定、接続の状態、loT Security に提供しているデータ を確認する場合にも役立ちます。

show iot dhcp-	all と入力すると、firewall に設定されているすべての DHCP
server status { all	サーバ、接続先のポート番号、および現在の接続ステータスを
server <server-< td=""><td>示すテーブルが表示されます。</td></server-<>	示すテーブルが表示されます。
	server <server-name></server-name> と入力すると、特定の DHCP サー バーとその最近のアクティビティに関する詳細情報が表示され ます。
show iot eal dhcp-	このコマンドは、DHCP サーバの syslog メッセージを伝送する
syslog-eal	EAL に関連する情報を表示します。

Device > Data Redistribution [デバイス > データの再配 信]

この設定は、ファイアウォールあるいは Panorama がデータを再配信する際に使用する方法を定 義します。

確認すべき情報	以下を参照
データ再配信エージェントを追加または削	Device > Data Redistribution > Agents [デバイス
除します。	> データの再配信 > エージェント]
データ再配信クライアントに関する情報を	Device > Data Redistribution > Clients [デバイス
表示します。	> データの再配信 > クライアント]
データ再配信エージェントのコレクタ名お	Device > Data Redistribution > Collector Settings
よび事前共有キーを設定します。	[デバイス > データの再配信 > コレクタ 設定]
データ再配信エージェントがデータを再配	Device > Data Redistribution > Include/Exclude
信する際に包含するあるいは除外するサブ	Networks [デバイス > データの再配信 > 包含/除
ネットワークを定義します。	外ネットワーク]

Device > Data Redistribution > Agents [デバイス > データの再配 信 > エージェント]

シリアルナンバーまたはホストとポートの情報を使用して、データ再配信エージェントを追加します。

Data Redistribution Agent Setup(データ再配信エージェント のセットアップ)	の意味
名前	データ再配信エージェント名を入力します(最大 31 文 字)。文字、数字、スペース、ハイフン、およびアン ダースコアのみを使用してください。
enabled [有効化]	データ再配信エージェントを有効化するには、このオプ ションを選択します。
次を使用してエージェントを追加	データ再配布エージェントの追加方法を選択します。
	 Serial Number – このオプションを選択し、シリアル 番号を選択します。

Data Redistribution Agent Setup(データ再配信エージェント のセットアップ)	の意味
	 Host and Port - このオプションを選択し、次のホス トおよびポート情報を入力します。
	• Host(ホスト)-ホスト名を入力します。
	 LDAP Proxy – ホストを LDAP proxy として使用 するには、このオプションを選択します。
	 Port – エージェントがリクエストをリッスンする ポート番号を入力します。
	 Collector Name – firewall または仮想システムを User-ID エージェントとして識別する Collector Name および Pre-Shared Key を入力します。
データ タイプ	再配信するデータの種類(IP User Mappings(IP ユーザー マッピング)、IP Tags(IP タグ)、User Tags(ユーザー タグ)、HIP、またはQuarantine List(隔離リスト))を選択します。

データ再配信エージェントを設定した後は、再配信エージェントに関する以下の情報を表示する ことができます。

データ再配布エージェント情報	Description
シリアルナンバー	エージェントの識別番号
Host	ホストの情報。
Collector Name	コレクター エージェントの名前。
HIP	エージェントのホスト情報プロファイル。
IP User Mappings	IP アドレスとユーザー名のマッピング情報。
IP Tags	IP アドレスとタグのマッピング情報。
Quarantine List	隔離中のデバイスの一覧を表示します。
Dynamic User Group	ユーザー名とタグのマッピング情報。
Connected	エージェントが再配布サービスに接続されて いるかどうかを示します。

Device > Data Redistribution > Clients [デバイス > データの再配 信 > クライアント]

Device(デバイス) > **Data Redistribution**(データ再配信) > **Clients**(クライアント)を選択して、それぞれの再配信クライアントに関する以下の情報を表示させます。

Redistribution Agent Information(再配信エー ジェントの情報)	の意味
ホスト情報	クライアント向けホスト情報。
ポート	配信クライアントが使用するポート。
Vsys ID	再配信クライアントが接続されている仮想シ ステムの ID。
バージョン	クライアントの PAN-OS のバージョン。
ステータス	配信クライアントの状態を表示します。
PDF/CSV	最低限の読み取り専用アクセス権を持つ管理 ロールは、データ再配信情報を PDF/CSV 形 式でエクスポートすることができます。
接続対象の更新	接続されている再配信クライアントすべての 情報を更新します。

Device > Data Redistribution > Collector Settings [デバイス > デー タの再配信 > コレクタ 設定]

ユーザー ID 再配信エージェントへの接続を設定するには、コレクタ名および事前共有鍵を入力します。

Data Redistribution Agent Setup Settings(データ再配信エージェン トのセットアップ設定)	の意味
コレクタ名	再配信エージェンを識別するには、Collector Name(コ レクタ名)(最大 255 文字の英数字)を入力します。
コレクタのPre-Shared Key(事前 共有鍵) / Confirm Collector Pre- Shared Key(コレクタの事前共有 鍵の確認)	コレクタの Pre-Shared Key (事前共有鍵) を入力して 確認します(最大 255 文字の英数字)。

Device > Data Redistribution > Include/Exclude Networks [デバイス > データの再配信 > 包含/除外ネットワーク]

[Include/Exclude Networks(包含/除外ネットワーク)]リストを使用し、再配信エージェントが マッピングを再配布する際に含めるか、除外するサブネットワークを定義します。

タスク	の意味
コンテキスト の	検出を特定のサブネットワークに制限したい場合は、サブネットワークプロ ファイルをAdd[追加] し、以下のフィールドを入力します。
	• Name[名前] – サブネットワークの識別に使用する名前を入力します。
	• Enabled[有効] – サーバー監視の際のサブネットワークの許可や除外を有 効化する場合はこのオプションを選択します。
	 Discovery[検出] – User-IDエージェントがサブネットワークをInclude[許可] するかExclude[除外] するかを選択します。
	 Network Address[ネットワークアドレス] – サブネットワークのIPアドレスの範囲を入力します。
	エージェントは、「すべてを除外」という暗黙のルールをリストに適用します。たとえば、Include(許可)オプションを指定してサブネットワーク 10.0.0.0/8 を追加すると、エージェントは、その他すべてのサブネットワー クがリストに追加されていない場合もこれらを除外します。明示的に包含し たサブネットワークの一部を除外する場合にのみ、Exclude(除外)オプショ ンを指定してエントリを追加します。たとえば、Include[包含]オプションを 指定して 10.0.0.0/8 を、Exclude[除外]オプションを指定して 10.2.50.0/22 を追加すると、ユーザー ID エージェントは、10.0.0.0/8 内のサブネットワー クのうち 10.2.50.0/22 を除くすべてを検出し、10.0.0.0/8 外のすべてのサ ブネットワークを除外します。Include(包含)プロファイルを追加せずに Exclude(除外)プロファイルを追加すると、エージェントは、追加したサ ブネットワークのみでなく、すべてのサブネットワークを除外します。
削除します。	リストからサブネットワークを削除する場合は、それを選択して Delete [削 除] します。
	ヒント:設定内容を消去せずに「許可/除外ネットワークリスト」からサブ ネットワークを削除する場合は、サブネットワークプロファイルの編集を行 い、Enabled[有効化] の選択を解除します。
カスタム許 可/除外ネッ トワーク	デフォルトでは、エージェントは、追加された順にサブネットワークを(上 から下に)評価します。評価順を変更するには、Custom Include/Exclude Network Sequence[許可/除外ネットワーク カスタム シーケンス] をクリック します。次に、サブネットワークに対してAdd[追加]、Delete[削除]、Move Up[上へ]、Move Down[下へ] の各コマンドを実行して、カスタムの評価順を 作成します。

Device > Device Quarantine [デバイス > デバイス隔離]

Device(デバイス) > **Device Quarantine**(デバイス隔離) ページには、隔離リストに登録され ているデバイスが表示されます。

次のアクションの結果として、デバイスが検疫リストに表示されます。

• システム管理者が、このリストに手動でデバイスを追加した。

デバイスを手動でAdd(追加)するには、Host ID(ホスト ID) およびオプションで、隔離 の必要があるデバイスのSerial Number(シリアル番号)を入力します。

- システム管理者は、トラフィック、GlobalProtect、Threat ログ、または Unified ログから Host ID 列を選択し、その列からデバイスを選択してから、Block Deviceを選択します
- デバイスは自動的に検疫リストに追加されます:
 - ログ転送プロファイルをセキュリティポリシールールで使用し、その一致リストに組み込みアクションがQuarantineに設定されている
 - ホスト ID は、GlobalProtect ログに自動的に表示されます。Host ID (ホスト ID) を Traffic (トラフィック)、Threat (脅威)、またはUnified (統合) ログに表示するには、ファイアウォールに、Source Device (送信元デバイ ス)がQuarantine (検疫) に設定されたセキュリティ ポリシー ルールが少な くとも 1 つ必要となります。この設定がセキュリティ ポリシーに存在しない と、Traffic (トラフィック)、Threat (脅威)、またはUnified (統合) ログ にHost ID (ホスト ID) が存在せず、ログ転送プロファイルは有効化されませ ん。
 - 組み込みアクションを Quarantineに設定し、HIP マッチ ログ設定を使用します。
 - ファイアウォールで、手動または自動で GlobalProtect デバイスを隔離リスト に追加し、デバイスのログインをブロックするためには、GlobalProtect サブ スクリプション ライセンスが必要です。
- APIを使用してデバイスが隔離リストに追加された。
- ファイアウォールが、再配信されたエントリの一部として隔離リストを受け取った(隔離リ ストが別の Panorama アプライアンスまたはファイアウォールから再配信された)。

Device Quarantine(デバイス隔離)テーブルには、以下のフィールドが含まれます。

項目	の意味
ホストID	ブロックされたホストの Host-ID(ホストID)。
理由	デバイスが隔離された理由。 Admin Add(管理者追加)という 理由は、管理者が手動でデバイスを表に追加したことを意味しま す。

項目	の意味
タイム スタンプ	管理者または Security(セキュリティ)ポリシー ルールがデバイ スを隔離リストに追加した時刻。
Source Device/App(送 信元デバイスまたはアプ リケーション)	デバイスを隔離リストに追加した Panorama、ファイアウォー ル、あるいはサードパーティのアプリケーションの IP アドレス。
シリアル番号	(オプション) 隔離されたデバイスのシリアル番号(既知の場 合)。
ユーザー名	(オプション) 隔離される際にデバイスにログインし たGlobalProtect クライアントユーザーのユーザー名。

隔離されたデバイスのリストを pdf または csv ファイルにエクスポートできます。

Device > VM Information Sources [デバイス > VM 情報 の送信元]

ここに挙げる送信元(VMware ESXiサーバー、VMware vCenterサーバー、Amazon Web Services Virtual Private Cloud (AWS-VPC)、Google Compute Engine(GCE))にデプロイされ た仮想マシン(VM)に対する変更内容をプロアクティブに追跡する場合はこのタブを使用しま す。

VM-Series NSXエディション製品の一部となっているESXiホストをモニターしており、仮想環境内の変更点を調べる場合は、VM情報ソースの代わりに動的アドレスグループを使用してください。M-Series NSXエディション製品の場合、NSXマネージャはIPアドレスの所属するNSXセキュリティグループの情報をPanoramaに提供します。NSXマネージャーはサービスプロファイルIDを使用して識別を行うので、NSXマネージャからの情報には動的アドレスグループにおける一致条件を定義するために必要な情報がすべて含まれています。このため、複数のNSXセキュリティグループにまたがってIPアドレスが重複している場合にも適切なポリシーを適用することができます。

最大 32 個のタグを IP アドレスに登録できます。

VM 情報ソースをモニターするには、以下の2つの方法があります。

 ファイアウォールは VMware ESXi サーバー、VMware vCenter サーバー、GCE インターフェ イス、および AWS-VPCs をモニターし、モニター対象ソースにゲストがプロビジョニングま たは変更された場合は変更内容を取得できます。ファイアウォールでは、最大 10 個のソース (構成されたすべての仮想システムのすべてのソースの累積)を構成できます。

ファイアウォールが高可用性(HA)構成で設定されている場合、次の条件が適用されます。

- アクティブ/パッシブ HA 設定-アクティブ ファイアウォールのみが VM 情報ソースをモニターします。
- アクティブ/アクティブセットアップでは、優先度の値が primary (プライマリ)のファ イアウォールのみが VM 情報ソースをモニターします。

VM 情報ソースとダイナミック アドレス グループによる同期動作と、仮想環境の変更をモニターする機能についての詳細は、『VM-Series デプロイメント ガイド』を参照してください。

- IP アドレス-ユーザー名のマッピングについては、Windows User ID エージェントまたはファ イアウォールに VM 情報ソースを設定して、VMware ESXi サーバーと vCenter サーバーをモ ニターし、サーバーに設定されたゲストがプロビジョニングまたは変更された場合は変更内 容を取得できます。Windows ユーザー ID エージェントは最大 100 個のソースをサポートし ます。ユーザー ID エージェントは AWS と Google Compute Engine で利用できません。
 - モニター対象の ESXi または vCenter Server の各 VM に VMware Tools がインス トールされていて実行中である必要があります。VMware Tools を使用して、各 VM に割り当てられた IP アドレスとその他の値を収集できます。

モニター対象 VM に割り当てられた値を収集するには、ファイアウォールで以下の表の属性を モニターする必要があります。

VMware ソースでモニターされる属性

- UUID
- 氏名
- ゲスト OS
- 注釈
- VM State 電源状態は、poweredOff、poweredOn、standBy、unknown です。
- バージョン
- ネットワーク 仮想スイッチ名、ポート グループ名、VLAN ID。
- コンテナ名 vCenter 名、データ センター オブジェクト名、リソース プール名、クラス タ名、ホスト、ホスト IP アドレス。

AWS-VPC でモニターされる属性

- アーキテクチャ
- ゲスト OS
- イメージ ID
- インスタンス ID
- インスタンスの状態
- インスタンス タイプ
- Key Name
- 配置 テナンシー、グループ名、可用性ゾーン
- プライベート DNS 名
- パブリック DNS 名
- サブネット ID
- Tag(key、value)(インスタンスごとに最大 18 個のタグをサポート)
- VPC ID

Google Compute Engine (GCE) 上でモニタリングする属性

- VM のホスト名
- マシン タイプ
- プロジェクト ID
- プラットフォーム(OS タイプ)

Google Compute Engine (GCE) 上でモニタリングする属性

- ステータス
- サブネットワーク
- VPC ネットワーク
- ゾーン

Add(追加) – VM モニタリングの新しいソースを追加するには、Add(追加)をクリックし、 モニターするソースに応じて詳細を入力します。

- VMware ESXi または vCenter サーバーの場合、「VMware ESXi サーバーおよび vCenter サーバーの VM 情報ソースを有効にするための設定」を参照してください。
- AWS-VPC の場合、「AWS VPC の VM 情報ソースを有効にするための設定」を参照してください。
- Google Compute Engine (GCE) の場合は、Settings to Enable VM Information Sources for Google Compute Engine (Google Compute Engine の VM 情報ソースを有効にするための設 定)を参照してください。

Refresh Connected (接続対象の更新) – 画面に表示される接続状況を更新します。これは、ファイアウォールとモニタリング対象のソース間の接続は更新しません。

Delete(削除)--選択した設定済みの VM 情報ソースを削除します。

PDF/CSV–VM 情報ソース設定テーブルを PDF またはカンマ区切り値(CSV)ファイルとして エクスポートします。「Configuration Table Export(設定バンドルのエクスポート)」を参照し てください。

VMware ESXi サーバーおよび vCenter サーバーの VM 情報ソー スを有効にするための設定

以下の表では、VMware ESXi および vCenter サーバー用に VM 情報の送信元を有効にするため に指定する設定について説明します。

Virtual Machine (仮想マシン - VM) のタグを取得するには、ファイアウォール に、VMware ESXi および vCenter サーバーで読み取り専用アクセス権のあるアカウ ントが必要です。

VMware ESXi または vCenter サーバーの VM 情報の送信元の有効化設定		
氏名	モニター対象ソースの識別に使用する名前を入力します(最大 31 文 字)。名前の大文字と小文字は区別されます。また、一意の名前にす る必要があります。文字、数字、スペース、ハイフン、およびアン ダースコアのみを使用してください。	

VMware ESXi または vCenter サーバーの VM 情報の送信元の有効化設定		
タイプ	モニター対象のホスト/ソースが ESXi server [ESXi サー バー]か、 vCenter server [vCenter サーバー]かを選択します。	
の意味	(任意)送信元の場所または機能を識別するラベルを追加します。	
ポート	ホスト/ソースのリスニング ポートを指定します。(デフォルト ポー トは 443)。	
enabled [有効化]	デフォルトでは、ファイアウォールと設定されたソース間の通信は 有効になっています。	
	モニター対象ソースとファイアウォール間の接続状態は、インター フェイスに以下のように表示されます。	
	 ● 接続済み 	
	• 一 切断	
	 保留。モニター対象ソースが無効になっている場合は、通信状態も黄色で表示されます。 	
	ホストとファイアウォール間の通信を無効にするには、 Enabled [有 効] のオプションをオフにします。	
タイムアウト	ホストが応答しない場合、モニター対象送信元への接続を切断す るまでの間隔を入力します(範囲は2~10時間、デフォルトは2時 間)。	
	(任意)デフォルト値を変更する場合は、Enable timeout when the source is disconnected (送信元切断時のタイムアウトを有効にする)を選択して、値を指定します。指定された制限に達した際、ホストがアクセス不能であるか応答しない場合は、ファイアウォールによって送信元への接続が閉じられます。	
送信元	モニターするホスト/ソースの FQDN または IP アドレスを入力しま す。	
username	送信元に対する認証に必要なユーザー名を指定します。	
パスワード	パスワードを入力し、確認のために再入力します。	
更新間隔	ファイアウォールが送信元から情報を取得する間隔(秒数)を指定 します(範囲は 5-600、デフォルトは5)。	

AWS VPC の VM 情報ソースを有効にするための設定

以下の表では、AWS VPC 用に VM 情報の送信元を有効にするために指定する設定について説明 します。

AWS VPC の VM 情報ソースを有効にするための設定		
氏名	モニター対象ソースの識別に使用する名前を入力します(最大 31 文字)。名前の大文字と小文字は区別されます。また、一意の名前 にする必要があります。文字、数字、スペース、ハイフン、およ びアンダースコアのみを使用してください。	
タイプ	AWS VPC を選択します。	
の意味	(<mark>任意</mark>)送信元の場所または機能を識別するラベルを追加しま す。	
enabled [有効化]	デフォルトでは、ファイアウォールと設定されたソース間の通信 は有効になっています。	
	モニター対象ソースとファイアウォール間の接続状態は、イン ターフェイスに以下のように表示されます。	
	• \bullet \bullet	
	接航済み	
	切断	
	• 保留。モニター対象ソースが無効になっている場合は、通信状 態も黄色で表示されます。	
	ホストとファイアウォール間の通信を無効にするには、 Enabled [有効] のオプションをオフにします。	
送信元	Virtual Private Cloud が存在する URI を追加します。例: ec2.us- west-1.amazonaws.com	
	The syntax is: ec2.< <i>your_AWS_region></i> .amazonaws.com; for AWS China it is: ec2. <aws_region>.amazonaws.com.cn</aws_region>	
アクセスキーID	AWS アカウントを所有するか、アクセスを許可されているユー ザーを一意に識別する英数字のテキスト文字列を入力します。	
	この情報は、AWS セキュリティ認証情報の一部です。ファイア ウォールでは、AWS サービスに対する API コールにデジタル署 名するための認証情報 (アクセス キー ID と秘密アクセス キー) が 要求されます。	

AWS VPC の VM 情報ソースを有効にするための設定	
秘密アクセス キー	パスワードを入力し、確認のために再入力します。
更新間隔	ファイアウォールが送信元から情報を取得する間隔(秒数)を指 定します(範囲は 60 ~ 1,200、デフォルトは 60)。
タイムアウト	ホストが応答しない場合、モニター対象ソースへの接続を閉じる までの時間(デフォルトは2時間)
	(任意) Enable timeout when the source is disconnected (送信 元切断時のタイムアウトを有効にする)を選択します。指定さ れた制限に達した際、送信元がアクセス不能であるか応答しない 場合は、ファイアウォールによって送信元への接続が閉じられま す。
VPC ID	モニターする AWS-VPC の ID を入力します (例: vpc-1a2b3c4d)。 この VPC 内にデプロイされている EC2 インスタンスのみがモニ ターされます。
	アカウントがデフォルトの VPC を使用するように設定されてい る場合、デフォルトの VPC ID が AWS アカウント属性の下にリ ストされます。

Google Compute Engine の VM 情報ソースを有効にするための設定

デバイス > VM 情報ソース > 追加

次の表は、Google Cloud Platform で Google Compute Engine インスタンスの VM 情報送信元を 有効にするために必要な設定について説明します。Google Compute Engine (GCE) インスタン スの監視を有効にして、特定のプロジェクトの Google Cloud ゾーンで実行中のインスタンスに 関するタグ、ラベル、その他のメタデータを取得するために、ファイアウォール(社内の仮想マ シンまたは仮想マシン内の Google Cloud)を許可します。Google Cloud Platform の VM-Series については、「VM-Series デプロイメント ガイド」を参照してください。

Google Compute Engine の VM 情報ソースを有効にするための設定	
氏名	モニター対象ソースの識別に使用する名前を入力します(最大 31 文字)。大文字と小文字を区別し、一意の名前を入力する必 要があります。文字、数字、スペース、ハイフン、アンダー スコアのみが使用できます。
タイプ	Google Compute Engine を選択します。

Google Compute Engine の VM 情報ソースを有効にするための設定	
の意味	(任意)送信元の場所または機能を識別するラベルを追加し ます。
enabled [有効化]	firewall と設定されたソース間の通信はデフォルトで有効に なっています。
	監視対象のソースと firewall 間の接続ステータスは、イン ターフェイスに次のように表示されます。
	• • Connected
	 Disconnected
	● ● -保留中または監視対象ソースが無効になっています。
	Enabled オプションをオフにして、構成済みのソースと firewall 間の通信を無効にします。
	通信を無効にすると、登録されているすべての IP アドレス とタグが、関連付けられた動的アドレス グループから削除さ れます。つまり、ポリシー ルールは このGoogle Cloud プロ ジェクトの GCE インスタンスには適用されません。
Service Authentication Type(サービス認証タイ プ)	GCE またはサービス アカウントで実行する VM-Series を選択 します。
	 VM-Series running on GCE (GCE で実行する VM-Series) –VM 監視を有効にするハードウェア ベースまた は VM Series のファイアウォールが Google Cloud Platform 内にデプロイされていない場合は、このオプションを選択 します。
	 Service Account (サービス アカウント) –Google Cloud Platform にデプロイされていないファイアウォールで Google Cloud Engine インスタンスを監視する場合は、こ のオプションを選択します。このオプションを使用する と、個々のエンドユーザー アカウントを使用せずに、仮想 マシンまたはアプリケーションに属する特別な Google ア カウントを使用できます。
	サービスアカウントには、Google API へのアクセスを 許可する IAM ポリシー(Compute Engine > Compute Viewer特権)が必要で、仮想マシンのメタデータ用に Google Cloud Project内の仮想マシンにクエリを実行できる ようにする必要があります。

Google Compute Engine の VM 情報ソースを有効にするための設定		
サービス アカウント認証情 報	(サービスアカウントのみ)サービス アカウントの資格情 報を含む JSON ファイルをアップロードします。このファイ ルにより、ファイアウォールはインスタンスに対して認証さ れ、メタデータへのアクセスが許可されます。	
	Google Cloud コンソール(IAM & admin (IAM および管理) > Service Accounts (サービス アカウント))にアカウントを 作成できます。アカウントを作成し、そのアカウントにキー を追加し、ファイアウォールにアップロードする必要がある JSON ファイルをダウンロードする方法については、Google のドキュメントを参照してください。	
プロジェクト ID	監視する Google Cloud Project を一意に識別する英数字の文 字列を入力します。	
Zone Name(ゾーン名)	ゾーン情報を最大 63 文字の文字列で入力します。例:us- west1-a.	
更新間隔	ファイアウォールが送信元から情報を取得する間隔(秒数) を指定します(範囲は 60 ~ 1,200、デフォルトは 60)。	
タイムアウト	ホストが応答しない場合、モニター対象ソースへの接続を閉 じるまでの時間(デフォルトは2時間)	
	(任意) Enable timeout when the source is disconnected (送 信元切断時のタイムアウトを有効にする)を選択します。指 定された制限に達した際、アクセス不能であるか応答しない 場合は、ファイアウォールによって送信元への接続が閉じら れます。ソースが切断されると、このプロジェクトから登録 されたすべての IP アドレスとタグが動的アドレス グループか ら削除されます。	

Device (デバイス) > Troubleshooting (トラブルシュー ティング)

- デバイス > トラブルシューティング
- Panorama > Managed Devices (管理対象デバイス) > トラブルシューティング

デバイスグループあるいはテンプレート設定の変更をコミットする前に、Webインターフェイ スから機能をテストし、変更によって現在アクティブな設定に接続性の問題が生じないこと、ポ リシーが正しくトラフィックを許可あるいは拒否していることを確認します。

- ポリシーマッチのテスト
 - Security Policy Match セキュリティポリシー マッチ
 - QoS ポリシー マッチ
 - Authentication Policy Match 認証ポリシーマッチ
 - 復号化/SSL ポリシー マッチ
 - NAT ポリシー マッチ
 - ポリシー ベース フォワーディング ポリシー マッチ
 - DoS ポリシー マッチ
- 接続性のテスト
 - routing
 - Wildfire をテスト
 - Threat Vault
 - ping
 - トレースルート
 - ログコレクタの接続性
 - 外部ダイナミックリスト
 - 更新サーバー
 - クラウドロギングサービスのステータスをテスト
 - クラウド GP サービスのステータスをテスト

Security Policy Match セキュリティポリシー マッチ

項目	の意味
設定をテスト	
テストを選択	実行するポリシーマッチ テストを選択します。

項目	の意味
(<mark>Panorama のみ</mark>)デバイ スを選択	Select device/VSYS (デバイス/VSYS を選択)し、ポリシーの 機能をテストするデバイスおよび仮想システムを指定しま す。Admin および device group & Template ユーザーには、そ のアクセスドメインに基づいてデバイスおよび仮想システムが 提示されます。さらに、Panorama 管理サーバーをデバイスと して選択することができます。
(<mark>Panorama のみ</mark>)選択し たデバイス	テスト用に選択したデバイスおよび仮想システムをリストアップします。
送信者	トラフィックの元であるゾーンを入力します。
受信者	トラフィックの宛先ゾーンを選択します。
送信元	トラフィックの元である IP アドレスを入力します。
宛先	トラフィックの宛先 IP アドレスを入力します。
Destination port	トラフィックの目的地である特定の宛先ポートを入力します。
Source User (送信元ユー ザー)	トラフィックの送信元であるユーザーを入力します。
PROTOCOL	ルーティングに使用する IP プロトコルを入力します。0~255 の値になります。
最初の許可ルールに至るま で、ルールのマッチ候補を すべて表示します。	最初にマッチしたルールの結果が得られるまでルールのマッチ 候補をすべて表示する場合はこのオプションを有効化します。 テスト結果で最初にマッチしたルールだけを返す場合はこれを 無効化(クリア)します。
Application [アプリケーショ ン]	テストするアプリケーション トラフィックを選択します。
カテゴリ	テストするトラフィックカテゴリを選択します。
(ファイアウォールの み)HIP マスクをチェック	ネットワークにアクセスしているエンド デバイスのセキュリ ティ状態をチェックする場合はこれを選択します。
結果	選択すると、実行したテストの Result Details (結果の詳細) が 表示されます。 (Panorama のみ) 複数の管理対象のデバイスに対してテスト を実行すると、テストされたデバイス毎に次の情報が Results

項目	の意味
	 Device Group (デバイスグループ)–トラフィックを処理しているファイアウォールが属すデバイスグループの名前です。
	 Firewall (ファイアウォール)ートラフィックを処理している ファイアウォールの名前です
	 Status (ステータス)-テストのステータスを示します:Success (成功)あるいはFailure (失敗)。
	 Result (結果)ーテストの結果を表示します。テストを行えなかった場合は次のいずれかが表示されます:
	• N/A (該当なし)-対象のデバイスに対して利用できない テストです。
	 Device not connected (デバイスが未接続)-デバイスの接続がドロップされました。
	 Shared policy disabled on device (デバイス上の共有ポリシーが無効)-Panorama からポリシーをプッシュすることを、デバイス上の Panorama 設定が許可していません。

QoS ポリシーマッチ

項目	の意味
設定をテスト	
テストを選択	実行するポリシーマッチ テストを選択します。
(<mark>Panorama のみ</mark>)デバイ スを選択	Select device/VSYS (デバイス/VSYS を選択)し、ポリシーの 機能をテストするデバイスおよび仮想システムを指定しま す。Admin および device group & Template ユーザーには、そ のアクセスドメインに基づいてデバイスおよび仮想システムが 提示されます。さらに、Panorama 管理サーバーをデバイスと して選択することができます。
(<mark>Panorama のみ</mark>)選択し たデバイス	テスト用に選択したデバイスおよび仮想システムをリストアップします。
送信者	トラフィックの元であるゾーンを入力します。
受信者	トラフィックの宛先ゾーンを選択します。

項目	の意味
送信元	トラフィックの元である IP アドレスを入力します。
宛先	トラフィックの宛先 IP アドレスを入力します。
Destination port	トラフィックの目的地である特定の宛先ポートを入力します。
Source User (送信元ユー ザー)	トラフィックの送信元であるユーザーを選択します。
PROTOCOL	ルーティングに使用する IP プロトコルを入力します。0〜255 の値になります。
Application [アプリケーショ ン]	テストするアプリケーション トラフィックを選択します。
カテゴリ	テストするトラフィックカテゴリを選択します。
コードポイント タイプ	テストするコードポイント エンコーディングのタイプを選択 します。
コードポイント値	コードポイントのエンコードの値を指定します: • DSCP-0~63 • ToS-0~7
結果	 選択すると、実行したテストの Result Details (結果の詳細) が 表示されます。 (Panorama のみ) 複数の管理対象のデバイスに対してテスト を実行すると、テストされたデバイス毎に次の情報が Results (結果) に表示されます。 Device Group (デバイスグループ)ートラフィックを処理し ているファイアウォールが属すデバイスグループの名前で す。 Firewall (ファイアウォール)ートラフィックを処理している ファイアウォールの名前です Status (ステータス)ーテストのステータスを示しま す: Success (成功)あるいはEailure (失敗).

項目	の意味
	 Result (結果)テストの結果を表示します。テストを行えな かった場合は次のいずれかが表示されます:
	 N/A (該当なし)-対象のデバイスに対して利用できない テストです。
	 Device not connected (デバイスが未接続)-デバイスの接続がドロップされました。
	 Shared policy disabled on device (デバイス上の共有ポリシーが無効)-Panorama からポリシーをプッシュすることを、デバイス上の Panorama 設定が許可していません。

Authentication Policy Match 認証ポリシーマッチ

項目	の意味
設定をテスト	
テストを選択	実行するポリシーマッチ テストを選択します。
(<mark>Panorama のみ</mark>)デバイ スを選択	Select device/VSYS (デバイス/VSYS を選択)し、ポリシーの 機能をテストするデバイスおよび仮想システムを指定しま す。Admin および device group & Template ユーザーには、そ のアクセスドメインに基づいてデバイスおよび仮想システムが 提示されます。さらに、Panorama 管理サーバーをデバイスと して選択することができます。
(<mark>Panorama のみ</mark>)選択し たデバイス	テスト用に選択したデバイスおよび仮想システムをリストアッ プします。
送信者	トラフィックの元であるゾーンを入力します。
受信者	トラフィックの宛先ゾーンを選択します。
送信元	トラフィックの元である IP アドレスを入力します。
宛先	トラフィックの宛先 IP アドレスを入力します。
カテゴリ	テストするトラフィック カテゴリを選択します。
結果	選択すると、実行したテストの Result Details (結果の詳細) が 表示されます。

項目	の意味
	(Panorama のみ)複数の管理対象のデバイスに対してテスト を実行すると、テストされたデバイス毎に次の情報が Results (結果)に表示されます。
	 Device Group (デバイスグループ)–トラフィックを処理しているファイアウォールが属すデバイスグループの名前です。
	 Firewall (ファイアウォール)ートラフィックを処理している ファイアウォールの名前です
	 Status (ステータス)-テストのステータスを示します:Success (成功)あるいはFailure (失敗)。
	 Result (結果)ーテストの結果を表示します。テストを行えな かった場合は次のいずれかが表示されます:
	 N/A (該当なし)-対象のデバイスに対して利用できない テストです。
	 Device not connected (デバイスが未接続)-デバイスの接続がドロップされました。
	 Shared policy disabled on device (デバイス上の共有ポリシーが無効) – Panorama からポリシーをプッシュすることを、デバイス上の Panorama 設定が許可していません。

復号化/SSL ポリシーマッチ

項目	の意味
設定をテスト	
テストを選択	実行するポリシーマッチ テストを選択します。
(<mark>Panorama のみ</mark>)デバイ スを選択	Select device/VSYS (デバイス/VSYS を選択)し、ポリシーの 機能をテストするデバイスおよび仮想システムを指定しま す。Admin および device group & Template ユーザーには、そ のアクセスドメインに基づいてデバイスおよび仮想システムが 提示されます。さらに、Panorama 管理サーバーをデバイスと して選択することができます。
(<mark>Panorama のみ</mark>)選択し たデバイス	テスト用に選択したデバイスおよび仮想システムをリストアッ プします。
送信者	トラフィックの元であるゾーンを入力します。
項目	の意味
----------------------------	--
受信者	トラフィックの宛先ゾーンを選択します。
送信元	トラフィックの元である IP アドレスを入力します。
宛先	トラフィックの宛先 IP アドレスを入力します。
Application [アプリケーショ ン]	テストするアプリケーション トラフィックを選択します。
カテゴリ	テストするトラフィック カテゴリを選択します。
結果	選択すると、実行したテストの Result Details (結果の詳細) が 表示されます。
	(Panorama のみ)複数の管理対象のデバイスに対してテスト を実行すると、テストされたデバイス毎に次の情報が Results (結果)に表示されます。
	 Device Group (デバイスグループ)ートラフィックを処理しているファイアウォールが属すデバイスグループの名前です。
	 Firewall (ファイアウォール)ートラフィックを処理している ファイアウォールの名前です
	 Status (ステータス)-テストのステータスを示します:Success (成功)あるいはFailure (失敗)。
	 Result (結果)-テストの結果を表示します。テストを行えなかった場合は次のいずれかが表示されます:
	• N/A (該当なし)-対象のデバイスに対して利用できない テストです。
	 Device not connected (デバイスが未接続)-デバイスの接続がドロップされました。

NAT ポリシー マッチ

項目	の意味
設定をテスト	
テストを選択	実行するポリシーマッチ テストを選択します。

項目	の意味
(<mark>Panorama のみ</mark>)デバイ スを選択	Select device/VSYS (デバイス/VSYS を選択)し、ポリシーの 機能をテストするデバイスおよび仮想システムを指定しま す。Admin および device group & Template ユーザーには、そ のアクセスドメインに基づいてデバイスおよび仮想システムが 提示されます。さらに、Panorama 管理サーバーをデバイスと して選択することができます。
(<mark>Panorama のみ</mark>)選択し たデバイス	テスト用に選択したデバイスおよび仮想システムをリストアップします。
送信者	トラフィックの元であるゾーンを入力します。
受信者	トラフィックの宛先ゾーンを選択します。
送信元	トラフィックの元である IP アドレスを入力します。
宛先	トラフィックの宛先 IP アドレスを入力します。
Source port	トラフィックの元である特定のポートを入力します。
Destination port	トラフィックの目的地である特定の宛先ポートを入力します。
PROTOCOL	ルーティングに使用する IP プロトコルを入力します。0~255 の値になります。
宛先インターフェイス	トラフィックの宛先であるデバイス上の宛先インターフェイス を入力します。
HA デバイス ID	HA デバイスの ID を入力します:
	• 0-プライマリ HA ピア
	• 1 -セカンダリ HA ピア
結果	選択すると、実行したテストの Result Details (結果の詳細) が 表示されます。
	(Panorama のみ)複数の管理対象のデバイスに対してテスト を実行すると、テストされたデバイス毎に次の情報が Results (結果)に表示されます。
	 Device Group (デバイスグループ)ートラフィックを処理しているファイアウォールが属すデバイスグループの名前です。
	 Firewall (ファイアウォール)–トラフィックを処理している ファイアウォールの名前です

項目	の意味
	 Status (ステータス)ーテストのステータスを示します:Success (成功)あるいはFailure (失敗)。
	 Result (結果)ーテストの結果を表示します。テストを行えな かった場合は次のいずれかが表示されます:
	 N/A (該当なし)-対象のデバイスに対して利用できない テストです。
	 Device not connected (デバイスが未接続)-デバイスの接続がドロップされました。
	 Shared policy disabled on device (デバイス上の共有ポリシーが無効)-Panorama からポリシーをプッシュすることを、デバイス上の Panorama 設定が許可していません。

ポリシー ベース フォワーディング ポリシー マッチ

項目	の意味
設定をテスト	
テストを選択	実行するポリシーマッチ テストを選択します。
(<mark>Panorama のみ</mark>)デバイ スを選択	Select device/VSYS (デバイス/VSYS を選択)し、ポリシーの 機能をテストするデバイスおよび仮想システムを指定しま す。Admin および device group & Template ユーザーには、そ のアクセスドメインに基づいてデバイスおよび仮想システムが 提示されます。さらに、Panorama 管理サーバーをデバイスと して選択することができます。
(<mark>Panorama のみ</mark>)選択し たデバイス	テスト用に選択したデバイスおよび仮想システムをリストアッ プします。
送信者	トラフィックの元であるゾーンを入力します。
インターフェイスから	トラフィックの送信元であるデバイス上のインターフェイスを 入力します。
送信元	トラフィックの元である IP アドレスを入力します。
宛先	トラフィックの宛先 IP アドレスを入力します。
Destination port	トラフィックの目的地である特定の宛先ポートを入力します。

項目	の意味
Source User (送信元ユー ザー)	トラフィックの送信元であるユーザーを入力します。
PROTOCOL	ルーティングに使用する IP プロトコルを入力します。0〜255 の値になります。
Application [アプリケーショ ン]	テストするアプリケーション トラフィックを選択します。
HA デバイス ID	HA デバイスの ID:
	• 0-プライマリ HA ピア
	● 1-セカンダリ HA ピア
結果	選択すると、実行したテストの Result Details (結果の詳細) が 表示されます。
	(Panorama のみ)複数の管理対象のデバイスに対してテスト を実行すると、テストされたデバイス毎に次の情報が Results (結果)に表示されます。
	 Device Group (デバイスグループ)ートラフィックを処理しているファイアウォールが属すデバイスグループの名前です。
	 Firewall (ファイアウォール)ートラフィックを処理している ファイアウォールの名前です
	 Status (ステータス)ーテストのステータスを示します: Success (成功)あるいはFailure (失敗)。
	 Result (結果)-テストの結果を表示します。テストを行えなかった場合は次のいずれかが表示されます:
	 N/A (該当なし)-対象のデバイスに対して利用できない テストです。
	 Device not connected (デバイスが未接続)-デバイスの接続がドロップされました。
	 Shared policy disabled on device (デバイス上の共有ポリシーが無効)-Panorama からポリシーをプッシュすることを、デバイス上の Panorama 設定が許可していません。

DoS ポリシーマッチ

項目	の意味
設定をテスト	
テストを選択	実行するポリシーマッチ テストを選択します。
(<mark>Panorama のみ</mark>)デバイ スを選択	Select device/VSYS (デバイス/VSYS を選択)し、ポリシーの 機能をテストするデバイスおよび仮想システムを指定しま す。Admin および device group & Template ユーザーには、そ のアクセスドメインに基づいてデバイスおよび仮想システムが 提示されます。さらに、Panorama 管理サーバーをデバイスと して選択することができます。
(<mark>Panorama のみ</mark>)選択し たデバイス	テスト用に選択したデバイスおよび仮想システムをリストアップします。
送信者	トラフィックの元であるゾーンを入力します。
受信者	トラフィックの宛先ゾーンを選択します。
インターフェイスから	トラフィックの送信元であるデバイス上のインターフェイスを 入力します。
宛先インターフェイス	トラフィックの宛先であるデバイス上の宛先インターフェイス を入力します。
送信元	トラフィックの元である IP アドレスを入力します。
宛先	トラフィックの宛先 IP アドレスを入力します。
Destination port	トラフィックの目的地である特定の宛先ポートを入力します。
Source User (送信元ユー ザー)	トラフィックの送信元であるユーザーを入力します。
PROTOCOL	ルーティングに使用する IP プロトコルを入力します。0~255 の値になります。
結果	選択すると、実行したテストの Result Details (結果の詳細) が 表示されます。 (Panorama のみ) 複数の管理対象のデバイスに対してテスト を実行すると、テストされたデバイス毎に次の情報が Results (結果) に表示されます。

項目	の意味
	 Device Group (デバイスグループ)ートラフィックを処理しているファイアウォールが属すデバイスグループの名前です。
	 Firewall (ファイアウォール)–トラフィックを処理している ファイアウォールの名前です
	 Status (ステータス)-テストのステータスを示します:Success (成功)あるいはFailure (失敗)。
	 Result (結果)ーテストの結果を表示します。テストを行えなかった場合は次のいずれかが表示されます:
	• N/A (該当なし)-対象のデバイスに対して利用できない テストです。
	 Device not connected (デバイスが未接続)-デバイスの接続がドロップされました。

routing

項目	の意味
テストを選択	除外する接続性テストを選択します。
(<mark>Panorama のみ</mark>)デバイ スを選択	Select device/VSYS (デバイス/VSYS を選択)し、ポリシーの 機能をテストするデバイスおよび仮想システムを指定しま す。Admin および device group & Template ユーザーには、そ のアクセスドメインに基づいてデバイスおよび仮想システムが 提示されます。さらに、Panorama 管理サーバーをデバイスと して選択することができます。
(<mark>Panorama のみ</mark>)選択し たデバイス	テスト用に選択したデバイスおよび仮想システムをリストアッ プします。
FiB ルックアップ、Mfib ルックアップ	 Lookup (ルックアップ) では次のいずれかを選択します: FiB-アクティブ ルートテーブル内でルートのルックアップ を実行します Mfib-アクティブ ルートテーブル内でマルチキャスト ルー トのルックアップを実行します
宛先IP	トラフィックの目的地である IP アドレスを入力します。
仮想ルーター(VR)	ルーティングのテストを行う特定の仮想ルーターを指定しま す。ドロップダウン リストから仮想ルーターを選択します。

項目	の意味
ECMP	
送信元IP	トラフィックの送信元である特定の IP アドレスを入力しま す。
Source port	トラフィックの送信元である特定のポートを入力します。
宛先IP	トラフィックの目的地である特定の IP アドレスを入力しま す。
Destination port	トラフィックの目的地である特定の宛先ポートを入力します。
結果	選択すると、実行したテストの Result Details (結果の詳細) が 表示されます。
	(Panorama のみ)複数の管理対象のデバイスに対してテスト を実行すると、テストされたデバイス毎に次の情報が Results (結果)に表示されます。
	 Device Group (デバイスグループ)–トラフィックを処理しているファイアウォールが属すデバイスグループの名前です。
	 Firewall (ファイアウォール)ートラフィックを処理している ファイアウォールの名前です
	 Status (ステータス)ーテストのステータスを示します:Success (成功)あるいはFailure (失敗)。
	 Result (結果)-テストの結果を表示します。テストを行えな かった場合は次のいずれかが表示されます:
	• N/A (該当なし)-対象のデバイスに対して利用できない テストです。
	 Device not connected (デバイスが未接続)-デバイスの接続がドロップされました。

Wildfire をテスト

項目	の意味
テストを選択	除外する接続性テストを選択します。
(<mark>Panorama のみ</mark>)デバイ スを選択	Select device/VSYS (デバイス/VSYS を選択)し、ポリシーの 機能をテストするデバイスおよび仮想システムを指定しま す。Admin および device group & Template ユーザーには、そ

項目	の意味
	のアクセスドメインに基づいてデバイスおよび仮想システムが 提示されます。さらに、Panorama 管理サーバーをデバイスと して選択することができます。
(<mark>Panorama</mark> のみ)選択し たデバイス	テスト用に選択したデバイスおよび仮想システムをリストアッ プします。
チャネル	WildFire チャンネルを選択します:PublicあるいはPrivate.
結果	選択すると、実行したテストの Result Details (結果の詳細) が 表示されます。
	(Panorama のみ) 複数の管理対象のデバイスに対してテスト を実行すると、テストされたデバイス毎に次の情報が Results (結果)に表示されます。
	 Device Group (デバイスグループ)ートラフィックを処理しているファイアウォールが属すデバイスグループの名前です。
	 Firewall (ファイアウォール)ートラフィックを処理している ファイアウォールの名前です
	 Status (ステータス)ーテストのステータスを示します:Success (成功)あるいはFailure (失敗)。
	 Result (結果)ーテストの結果を表示します。テストを行えな かった場合は次のいずれかが表示されます:
	 N/A (該当なし)-対象のデバイスに対して利用できない テストです。
	 Device not connected (デバイスが未接続)-デバイスの接続がドロップされました。

Threat Vault

項目	の意味
テストを選択	除外する接続性テストを選択します。
(<mark>Panorama のみ</mark>)デバイ スを選択	Select device/VSYS (デバイス/VSYS を選択)し、ポリシーの 機能をテストするデバイスおよび仮想システムを指定しま す。Admin および device group & Template ユーザーには、そ のアクセスドメインに基づいてデバイスおよび仮想システムが 提示されます。さらに、Panorama 管理サーバーをデバイスと して選択することができます。

項目	の意味
(<mark>Panorama のみ</mark>)選択し たデバイス	テスト用に選択したデバイスおよび仮想システムをリストアッ プします。
結果	選択すると、実行したテストの Result Details (結果の詳細) が 表示されます。
	(Panorama のみ)複数の管理対象のデバイスに対してテスト を実行すると、テストされたデバイス毎に次の情報が Results (結果)に表示されます。
	 Device Group (デバイスグループ)ートラフィックを処理しているファイアウォールが属すデバイスグループの名前です。
	 Firewall (ファイアウォール)ートラフィックを処理している ファイアウォールの名前です
	 Status (ステータス)ーテストのステータスを示します:Success (成功)あるいはFailure (失敗)。
	 Result (結果)ーテストの結果を表示します。テストを行えな かった場合は次のいずれかが表示されます:
	 N/A (該当なし)-対象のデバイスに対して利用できない テストです。
	 Device not connected (デバイスが未接続)-デバイスの接続がドロップされました。

ping

この ping のトラブルシューティング テストは、PAN-OS 9.0 以降のリリースを実行するファイ アウォールでのみサポートされています。

項目	の意味
テストを選択	除外する接続性テストを選択します。
(<mark>Panorama のみ</mark>)デバイ スを選択	Select device/VSYS (デバイス/VSYS を選択)し、ポリシーの 機能をテストするデバイスおよび仮想システムを指定しま す。Admin および device group & Template ユーザーには、そ のアクセスドメインに基づいてデバイスおよび仮想システムが 提示されます。さらに、Panorama 管理サーバーをデバイスと して選択することができます。
(<mark>Panorama のみ</mark>)選択し たデバイス	テスト用に選択したデバイスおよび仮想システムをリストアップします。

項目	の意味
ルーティングテーブルを バイパス、指定されたイン ターフェイスを使用	このオプションを有効化すると、ルーティングテーブルをバイ パスして指定されたインターフェイスを使用するようになりま す。設定済みのルーティングテーブルをテストする場合はこの オプションを無効化(クリア)します。
数	送信するリクエストの数を入力します。デフォルトのカウント は5です。
エコーリクエスト パケッ トをフラグメント化しない (IPv4)	テストでエコーリクエスト パケットをフラグメント化しない 場合はこのオプションを有効化します。無効化
IPv6 宛先を強制	テストで IPv6 宛先を強制的に使用します。
間隔	リクエスト間の遅延を秒単位で指定します(範囲は 1~2,000,000,000)。
送信元	エコーリクエストの送信元アドレスを入力します。
アドレスをシンボルで出力 しようとしない	テスト結果で IP アドレスを表示し、IP アドレスのホスト名を 解決しない場合はこのオプションを有効化します。IP アドレ スのホスト名を解決する場合は無効化(クリア)します。
パターン	16 進数のフィル パターンを指定します。
サイズ	リクエスト パケットのサイズをバイト数で入力します(範囲 は 0~65468)。
ToS	IP type-of-service の値を入力します(範囲は 1~255)。
TTL	ホップの IP time-to-live の値(IPv6 hop-limit の値)を入力し ます(範囲は 1~255)。
詳細な出力を表示	テスト結果の詳細な出力を表示します。
ホスト	リモートホストのホスト名およびIPアドレスを入力します。
結果	選択すると、実行したテストの Result Details (結果の詳細) が 表示されます。
	(Panorama のみ)複数の管理対象のデバイスに対してテスト を実行すると、テストされたデバイス毎に次の情報が Results (結果)に表示されます。

項目	の意味
	 Device Group (デバイスグループ)–トラフィックを処理しているファイアウォールが属すデバイスグループの名前です。
	 Firewall (ファイアウォール)ートラフィックを処理している ファイアウォールの名前です
	 Status (ステータス)ーテストのステータスを示します:Success (成功)あるいはFailure (失敗)。
	 Result (結果)ーテストの結果を表示します。テストを行えなかった場合は次のいずれかが表示されます:
	• N/A (該当なし)-対象のデバイスに対して利用できない テストです。
	 Device not connected (デバイスが未接続)-デバイスの接続がドロップされました。

トレースルート

項目	の意味
テストを選択	除外する接続性テストを選択します。
(<mark>Panorama のみ</mark>)デバイ スを選択	Select device/VSYS (デバイス/VSYS を選択)し、ポリシーの 機能をテストするデバイスおよび仮想システムを指定しま す。Admin および device group & Template ユーザーには、そ のアクセスドメインに基づいてデバイスおよび仮想システムが 提示されます。さらに、Panorama 管理サーバーをデバイスと して選択することができます。
(<mark>Panorama のみ</mark>)選択し たデバイス	テスト用に選択したデバイスおよび仮想システムをリストアップします。
IPv4 を使用	選択したデバイスの IPv4 アドレスを使用できるようにしま す。
IPv6 を使用	選択したデバイスの IPv6 アドレスを使用できるようにしま す。
最初の TTL	最初のアウトバウンド プローブ パケットで使用する time-to- live を入力します(範囲は 1~255)。
最大 TTL	最大の time-to-live ホップを入力します(範囲は 1~255)。

項目	の意味
ポート	プローブで使用するベース ポート番号を入力します。
ToS	IP type-of-service の値を入力します(範囲は 1~255)。
Wait 待機	レスポンスを待機する秒数を入力します(範囲は 1~99,999)。
一時停止	プローブ間で一時停止する時間をミリ秒単位で入力します(範 囲は 1~2,000,000,000)。
「don't fragment」ビットを 設定	パスが指定済みの最大トランスミッション ユニット(MTU) をサポートできない際に ICMP パケットを複数のパケットにフ ラグメント化しない場合はこのオプションを有効化します。
ソケット レベルのデバッグ を有効化	このオプションを有効化すると、ソケット レベルでデバッグ できるようになります。
ゲートウェイ	最大8つのルーズソースルートゲートウェイを指定します。
アドレスをシンボルで出力 しようとしない	テスト結果で IP アドレスを表示し、IP アドレスのホスト名を 解決しない場合はこのオプションを有効化します。IP アドレ スのホスト名を解決する場合は無効化(クリア)します。
ルーティングテーブルをバ イパスしてホストに直接送 信	指定済みのルーティングテーブルをバイパスしてホストを直に テストする場合はこのオプションを有効化します。
送信元	アウトバウンド プローブ パケットの送信元アドレスを入力し ます。
ホスト	リモートホストのホスト名およびIPアドレスを入力します。
結果	選択すると、実行したテストの Result Details (結果の詳細) が 表示されます。
	(Panorama のみ) 複数の管理対象のデバイスに対してテスト を実行すると、テストされたデバイス毎に次の情報が Results (結果)に表示されます。
	 Device Group (デバイスグループ)–トラフィックを処理しているファイアウォールが属すデバイスグループの名前です。
	 Firewall (ファイアウォール)ートラフィックを処理している ファイアウォールの名前です

項目	の意味
	 Status (ステータス)ーテストのステータスを示します:Success (成功)あるいはFailure (失敗)。
	 Result (結果)-テストの結果を表示します。テストを行えな かった場合は次のいずれかが表示されます:
	 N/A (該当なし)-対象のデバイスに対して利用できない テストです。
	 Device not connected (デバイスが未接続)-デバイスの接続がドロップされました。

ログコレクタの接続性

項目	の意味
テストを選択	除外する接続性テストを選択します。
(<mark>Panorama のみ</mark>)デバイ スを選択	Select device/VSYS (デバイス/VSYS を選択)し、ポリシーの 機能をテストするデバイスおよび仮想システムを指定しま す。Admin および device group & Template ユーザーには、そ のアクセスドメインに基づいてデバイスおよび仮想システムが 提示されます。さらに、Panorama 管理サーバーをデバイスと して選択することができます。
(<mark>Panorama のみ</mark>)選択し たデバイス	テスト用に選択したデバイスおよび仮想システムをリストアッ プします。
結果	選択すると、実行したテストの Result Details (結果の詳細) が 表示されます。
	(Panorama のみ)複数の管理対象のデバイスに対してテスト を実行すると、テストされたデバイス毎に次の情報が Results (結果)に表示されます。
	 Device Group (デバイスグループ)–トラフィックを処理しているファイアウォールが属すデバイスグループの名前です。
	 Firewall (ファイアウォール)–トラフィックを処理している ファイアウォールの名前です
	 Status (ステータス)–テストのステータスを示します:Success (成功)あるいはFailure (失敗)。

項目	の意味
	 Result (結果)テストの結果を表示します。テストを行えな かった場合は次のいずれかが表示されます:
	 N/A (該当なし)-対象のデバイスに対して利用できない テストです。
	 Device not connected (デバイスが未接続)-デバイスの接続がドロップされました。

外部ダイナミックリスト

項目	の意味
テストを選択	除外する接続性テストを選択します。
(<mark>Panorama のみ</mark>)デバイ スを選択	Select device/VSYS (デバイス/VSYS を選択)し、ポリシーの 機能をテストするデバイスおよび仮想システムを指定しま す。Admin および device group & Template ユーザーには、そ のアクセスドメインに基づいてデバイスおよび仮想システムが 提示されます。さらに、Panorama 管理サーバーをデバイスと して選択することができます。
(<mark>Panorama のみ</mark>)選択し たデバイス	テスト用に選択したデバイスおよび仮想システムをリストアップします。
URL テスト	接続をテストする URL を指定します。
結果	選択すると、実行したテストの Result Details (結果の詳細) が 表示されます。 (Panoramaのみ) 複数の管理対象のデバイスに対してテスト を実行すると、テストされたデバイス毎に次の情報が Results (結果) にま示されます
	 Device Group (デバイスグループ)ートラフィックを処理しているファイアウォールが属すデバイスグループの名前です。 Firewall (ファイアウォール)ートラフィックを処理している
	ファイアウォールの名前です Status (ステータス)ーテストのステータスを示します:Success (成功)あるいはFailure (失敗)。

項目	の意味
	 Result (結果)テストの結果を表示します。テストを行えな かった場合は次のいずれかが表示されます:
	 N/A (該当なし)-対象のデバイスに対して利用できない テストです。
	 Device not connected (デバイスが未接続)-デバイスの接続がドロップされました。

更新サーバー

項目	の意味
テストを選択	除外する接続性テストを選択します。
結果	選択すると、実行したテストの Result Details (結果の詳細) が 表示されます。
	(Panorama のみ)複数の管理対象のデバイスに対してテスト を実行すると、テストされたデバイス毎に次の情報が Results (結果)に表示されます。
	 Device Group (デバイスグループ)ートラフィックを処理しているファイアウォールが属すデバイスグループの名前です。
	 Firewall (ファイアウォール)ートラフィックを処理している ファイアウォールの名前です
	 Status (ステータス)ーテストのステータスを示します:Success (成功)あるいはFailure (失敗)。
	 Result (結果)ーテストの結果を表示します。テストを行えなかった場合は次のいずれかが表示されます:
	• N/A (該当なし)-対象のデバイスに対して利用できない テストです。
	 Device not connected (デバイスが未接続)-デバイスの接続がドロップされました。

クラウドロギングサービスのステータスをテスト

クラウド ロギング サービスへの接続ステータスをテストします。このテストは、バージョン 1.3 以降のクラウドサービス プラグインをインストールして実行する Panorama 管理サーバーで のみ利用できます。

項目	の意味
テストを選択	除外する接続性テストを選択します。
結果	選択すると、実行したテストの Result Details (結果の詳細) が 表示されます。
	複数の管理対象のデバイスに対してテストを実行すると、テストされたデバイス毎に次の情報が Results (結果) に表示されます。
	 Device Group (デバイスグループ)ートラフィックを処理しているファイアウォールが属すデバイスグループの名前です。
	 Firewall (ファイアウォール)ートラフィックを処理している ファイアウォールの名前です
	 Status (ステータス)ーテストのステータスを示します:Success (成功)あるいはFailure (失敗)。
	 Result (結果)ーテストの結果を表示します。テストを行えなかった場合は次のいずれかが表示されます:

クラウド GP サービスのステータスをテスト

GlobalProtect as a Service への接続ステータスをテストします。このテストは、バージョン 1.3 以降のクラウドサービス プラグインをインストールして実行する Panorama 管理サーバーでの み利用できます。

項目	の意味
テストを選択	除外する接続性テストを選択します。
結果	選択すると、実行したテストの Result Details (結果の詳細) が 表示されます。
	複数の管理対象のデバイスに対してテストを実行すると、テストされたデバイス毎に次の情報が Results (結果) に表示されます。
	 Device Group (デバイスグループ)ートラフィックを処理しているファイアウォールが属すデバイスグループの名前です。
	 Firewall (ファイアウォール)ートラフィックを処理している ファイアウォールの名前です
	 Status (ステータス)ーテストのステータスを示します:Success (成功)あるいはFailure (失敗)。

項目	の意味
	 Result (結果)-テストの結果を表示します。テストを行えな かった場合は次のいずれかが表示されます:

Device > Virtual Systems [デバイス > 仮想システム]

仮想システム(vsys)は、物理ファイアウォール内で個別に管理できる、独立した(仮想)ファ イアウォールインスタンスです。各 vsys は、独自のセキュリティ ポリシー、インターフェイ ス、および管理者による、独立したファイアウォールにすることができます。vsys では、ファ イアウォールで提供されるすべてのポリシー、レポート、および可視化機能の管理をセグメント 化できます。

たとえば、財務部門に関連付けられているトラフィックのセキュリティ機能をカスタマイズする 場合、財務 vsys を定義して、その部門のみに適用するセキュリティ ポリシーを定義できます。 ポリシーの管理を最適化するため、個々の vsys へのアクセスを許可する vsys 管理者アカウント を作成し、ファイアウォール全体とネットワーク機能で個別の管理者アカウントを使用できま す。こうすることで、財務部門の vsys 管理者が、財務部門のみのセキュリティ ポリシーを管理 できます。

ネットワーク機能 (スタティックおよびダイナミック ルーティング、インターフェイスの IPア ドレス、IPSec トンネルなど) は、ファイアウォール全体とそのすべての仮想システムに関係し ます。仮想システムの設定 (Device (デバイス) > Virtual Systems (仮想システム)) は、ファイア ウォール レベルおよびネットワーク レベルの機能 (スタティックおよびダイナミック ルーティ ング、インターフェイスの IPアドレス、IPSec トンネル、VLAN、バーチャル ワイヤ、仮想ルー ター、GRE トンネル、DHCP、DNS プロキシ、QoS、LLDP、ネットワーク プロファイル等) を 制御しません。各 vsys で、一連の物理および論理ファイアウォール インターフェイス (VLAN、 バーチャル ワイヤーなど) とセキュリティ ゾーンを指定できます。各 vsys でルーティングのセ グメント化が必要な場合、追加仮想ルーターの作成および割り当てを行い、必要に応じてイン ターフェイス、VLAN、バーチャル ワイヤーを割り当てる必要があります。

Panorama テンプレートを使用して vsys を定義する場合、1 つの仮想システムをデフォルトとし て構成できます。デフォルトの vsys と マルチ仮想システム機能 により、テンプレートのコミッ ト中にファイアウォールが vsys 固有の設定を受け入れるかどうかが決まります。

- マルチ仮想システム機能が有効になっているファイアウォールは、テンプレートで定義されている vsys に対して vsys 固有の設定を受け入れます。
- マルチ仮想システム機能が有効になっていないファイアウォールは、デフォルトのvsysに対してのみvsys固有の設定を受け入れます。デフォルトのvsysを構成しない場合、これらのファイアウォールはvsys固有の設定を受け付けません。
 - PA-400 シリーズ、PA-3200 シリーズ、PA-5200 シリーズ、PA-5400 シリーズ、 および PA-7000 シリーズファイアウォールは、複数の仮想システムをサポート します。ただし、PA-400 シリーズおよび PA-3200 シリーズ ファイアウォールに は、複数の仮想システムを有効にするためのライセンスが必要です。PA-220 お よび PA-800 Series ファイアウォールでは、マルチ仮想システムがサポートされ ていません。

マルチ仮想システムを有効にする前に、以下の点を考慮してください。

• vsys 管理者は、割り当てられた 仮想システム ごとに、セキュリティ ポリシーに必要なすべてのアイテムを作成・管理します。

- ゾーンは、vsys内のオブジェクトです。ポリシーまたはポリシーオブジェクトを定義する 前に、Policies (ポリシー) または Objects (オブジェクト) タブのドロップダウンから適切な Virtual System (仮想システム)を選択します。
- リモートログの宛先(SNMP、Syslog、および電子メール)、アプリケーション、サービス、 およびプロファイルをすべての仮想システム(共有)または1つのvsysで使用できるように設 定できます。
- 複数の仮想システムがある場合、単一の vsys を User-ID ハブとして選択し、IP アドレス対 ユーザー名のマッピング情報を仮想システム間で共有できます。
- グローバルに(ファイアウォール上のすべての仮想システムに対して)またはvsys固有のサービスルート(Device > Setup > Services [デバイス > セットアップ > サービス])を設定できます。
- vsysの名前変更はローカルのファイアウォールでのみ行うことができます。Panorama では vsysの名前変更はサポートしていません。Panorama で vsysの名前を変更する場合、完全に 新規の vsys になるか、新しい vsys 名がファイアウォール上の間違った vsys にマップされま す。

vsys を定義する前に、まずはマルチ vsys 機能をファイアウォール上で有効化する必要がありま す。Device (デバイス) > Setup (セットアップ) > Management (管理)を選択してGeneral Settings (一般設定)を編集し、Multi Virtual System Capability (マルチ仮想システム機能)を選択してか らOKをクリックします。これにより、Device(デバイス) > Virtual Systems(仮想システ ム)ページが追加されます。そのページを選択して以下の情報を指定し、vsysをAdd (追加)しま す。

仮想システム設 定	の意味
ID	vsysの識別子を整数で入力します。サポートされる仮想システムの数についての詳細は、ファイアウォールモデルのデータシートを参照してください。
	Panorama テンプレートを使用して vsys を設定する場合、このフィールドは表示されません。
氏名	vsysの識別に使用する名前(最大 31 文字)を入力します。名前の大文字 と小文字は区別されます。また、一意の名前にする必要があります。文 字、数字、スペース、ハイフン、およびアンダースコアのみを使用してく ださい。
	 Panorama テンプレートを使用して vsys 設定をプッシュする 場合、テンプレートの vsys 名はファイアウォールの vsys 名と 一致している必要があります。
復号化されたコ ンテンツの転送 を許可	ポート ミラーリング時または分析用の WildFire ファイルの送信時に復号化 されたコンテンツを仮想システムから外部のサービスに転送できるように

仮想システム設 定	の意味
	するには、このオプションを選択します。復号ポート ミラーリングも参照 してください。
General [全般] タブ	この vsys に DNS プロキシ ルールを適用する場合は、DNS Proxy オブジェ クトを選択します。(Network > DNS Proxy [ネットワーク > DNS プロキ シ]).
	特定の種類のオブジェクトを含める場合は、その種類(インターフェイス、VLAN、バーチャル ワイヤー、仮想ルーター、または識別可能な仮想システム)を選択して、ドロップダウンリストからオブジェクトを選択してAdd (追加)します。1つ以上のオブジェクトの種類を追加できます。オブジェクトを削除するには、オブジェクトを選択して Delete (削除)します。
[リソース] タブ	この vsys に許可される以下のリソース制限を指定します。各フィールド には、ファイアウォールモデルごとに異なる有効な範囲の値が表示されま す。デフォルト設定は0です。これは、vsys の制限がファイアウォールモ デルの制限と同じであることを意味します。ただし、特定の設定に関する 制限は各 vsys には反映されません。例えば、ファイアウォールに4つの 仮想システムがある場合、各仮想システムには、ファイアウォールごとに 許可されている復号化ルールの総数を設定することはできません。すべて の仮想システムの復号化ルールの総数がファイアウォールの制限に達する と、それ以上追加することはできません。
	• Sessions Limit[セッション制限] – セッションの最大数。
	 show session meter CLI コマンドを使用すると、ファ イアウォールがデータ プレーンごとに許可される最大セッション数、仮想システムで使用されている現在のセッション数、および仮想システムあたりのセッション数を表示します。PA-5200 シリーズおよび PA-7000 シリーズのファ イアウォールでは、仮想システムごとに複数のデータプ レーンが存在するため、使用されている現在のセッション数が最大セッション数制限より大きくなることがあります。PA-5200 シリーズまたは PA-7000 シリーズのファイ アウォールで設定する セッション制限は、データプレーンあたりであり、仮想システムごとに最大値が高くなります。
	• Security Rules (セキュリティルール) – セキュリティ ルールの最大数。
	• NAT Rules[NATルール] – NAT ルールの最大数。
	 Decryption Rules[復号化ルール] – 復号化ルールの最大数。 Occ Public [0-60] - 北山 - 0-60 小 - 北の見古教
	 QOS KUIES[QOS/ルール] - QOS ルールの最大级。 Application Override Pules[アプリケーションオーバーライドルール]
	 Application Override Rules[アプリケーションオーバーワイドルール] – アプリケーションオーバーライドルールの最大数。

仮想システム設 定	の意味
	 Policy Based Forwarding Rules (ポリシーベースフォワーディングルール) – ポリシーベース フォワーディング (PBF) ルールの最大数。
	• Authentication Rules - 認証ルールの最大数。
	 DoS Protection Rules (DoS プロテクションルール) – サービス拒否 (DoS) ルールの最大数。
	 Site to Site VPN Tunnels[サイト間 VPNトンネル] – サイト間VPNトンネルの最大数。
	 Concurrent GlobalProtect Tunnels[同時GlobalProtectトンネル] – 同時リ モートGlobalProtectユーザーの最大数。
	 Vsys 間ユーザー ID データ共有 – ユーザー ID データ・ハブを構成する には、スーパーユーザーまたは管理者特権が必要です。
	 この vsys を User-ID データ ハブ にする: ファイアウォール上の他の すべての仮想システムが共有マッピングにアクセスできるようにしま す。このオプションを有効にした後、共有する マッピングの種類 を 選択します。IP アドレス対ユーザ名マッピング(IP ユーザ マッピング)、 グループ マッピング(ユーザ グループ マッピング)、またはその両 方。
	 変更ハブ - どの vsys が User-ID データ ハブかを変更する場合は、新しい vsys を選択して、その vsys を User-ID データ ハブとして再割り当てします。Vsys をユーザー ID データ ハブとして使用しない場合は、[なし]を選択します。

Device > Shared Gateways [デバイス > 共有ゲートウェ イ]

共有ゲートウェイ[™]では、マルチ仮想システムで(通常はインターネット サービス プロバイダ などの共通アップストリーム ネットワークに接続される)外部通信に1つのインターフェイス を共有できます。すべての仮想システムは、1つの IP アドレスを使用する物理インターフェイ スを介して外部と通信します。すべての仮想システムのトラフィックは、共有ゲートウェイを介 し、1つの仮想ルーターを使用してルーティングされます。

共有ゲートウェイではレイヤー3インターフェイスを使用するため、レイヤー3インターフェ イスが少なくとも1つ共有ゲートウェイとして設定されている必要があります。仮想システム から共有ゲートウェイを介してファイアウォールを通過する通信には、2つの仮想システム間の 通信と同様のポリシーが必要です。[External vsys] ゾーンで仮想システムのセキュリティ ルール を定義できます。

共有ゲートウェイ設定	の意味
ID	ゲートウェイの識別子 (ファイアウォールでは使用しない)。
氏名	共有ゲートウェイの名前(最大 31 文字)を入力します。名前の大 文字と小文字は区別されます。また、一意の名前にする必要があり ます。文字、数字、スペース、ハイフン、およびアンダースコアの みを使用してください。名前のみが必須です。
DNSプロキシ	(任意)DNSプロキシが設定されている場合、ドメイン名のクエリ に使用するDNSサーバーを選択します。
インターフェイス	共有ゲートウェイが使用するインターフェイスを選択します。

Device(デバイス) > **Certificate** Management(証明書の管理)

- Device > Certificate Management > Certificates [デバイス > 証明書の管理 > 証明書]
- Device > Certificate Management > Certificate Profile [デバイス > 証明書の管理 > 証明書プロ ファイル]
- Device > Certificate Management > OCSP Responder [デバイス > 証明書の管理 > OCSP レス ポンダ]
- Device > Certificate Management > SSL/TLS Service Profile [デバイス > 証明書の管理 > SSL/ TLS サービス プロファイル]
- Device > Certificate Management > SCEP [デバイス > 証明書の管理 > SCEP]
- Device (デバイス) > Certificate Management (証明書の管理) > SSL Decryption Exclusion (SSL 復号化例外)
- Device(デバイス) > Certificate Management(証明書の管理) > SSH Service Profile(SSH サービス プロファイル)

Device > Certificate Management > Certificates [デバイ ス > 証明書の管理 > 証明書]

ネットワーク間の通信を安全に行うために、使用する証明書の管理(生成、インポート、更新、 削除、および取り消し)を行う場合は、Device(デバイス) > Certificate Management(証明 書の管理) > Certificates(証明書) > Device Certificates(デバイス証明書)のページを使用 します。ネットワークのHAピア間の通信を保護する高可用性(HA)キーをエクスポートおよ びインポートすることもできます。ファイアウォールが信頼する認証局(CA)を表示、有効 化、無効化する場合は、Device(デバイス) > Certificate Management(証明書の管理) > Certificates(証明書) > Default Trusted Certificate Authorities(信頼される既定認証局)の ページを使用します。



ファイアウォールおよび Panorama での証明書の使用方法の詳細は、証明書の管理 を参照してください。

- ファイアウォールおよび Panorama 証明書の管理
- 信頼できる既定証明機関の管理
- Device > Certificate Management > Certificate Profile [デバイス > 証明書の管理 > 証明書プロ ファイル]
- Device > Certificate Management > OCSP Responder [デバイス > 証明書の管理 > OCSP レスポンダ]
- Device > Certificate Management > SSL/TLS Service Profile [デバイス > 証明書の管理 > SSL/ TLS サービス プロファイル]
- Device > Certificate Management > SCEP [デバイス > 証明書の管理 > SCEP]
- Device > Master Key and Diagnostics [デバイス > マスター キーおよび診断]

ファイアウォールおよび Panorama 証明書の管理

- [Device] > [証明書の管理] > [証明書] > [デバイス証明書]
- [Panorama > 証明書の管理 > 証明書]

ファイアウォールまたは Panorama が Web インターフェイスへのアクセスの保護、SSL 復 号、または LSVPN などのタスクに使用する証明書を表示する場合は、Device(デバイス) > Certificate Management(証明書の管理) > Certificates(証明書) > Device Certificates(デバ イス証明書)または Panorama > Certificate Management(証明書の管理) > Certificates(証明 書) > Device Certificates(デバイス証明書)のページを開きます。

各証明書の用途の例は以下のとおりです。証明書を生成した後で、証明書の使用方法を定義して ください(「デフォルトの信頼できる証明機関の管理」を参照)。

Forward Trust(信頼できる転送) – ファイアウォールは、サーバー証明書に署名を行った認証局(CA)がファイアウォールのCAリストに存在する場合、SSLフォワードプロキシ復号化 □時にクライアントへ提示するサーバー証明書のコピーに署名する際にこの証明書を使用します。

- Forward Untrust(信頼できない転送) ファイアウォールは、サーバー証明書に署名を行った CA がファイアウォールの CA リストに存在しない場合、SSL フォワード プロキシ復号化
 □ 時にクライアントへ提示するサーバー証明書のコピーに署名する際にこの証明書を使用します。
- Trusted Root CA(信頼されたルート CA)-ファイアウォールは SSL Forward Proxy decryption (SSLフォワード プロキシ復号化 ^I、GlobalProtect ^I、URL Admin Override (URL 管理オーバーライド) ^I、およびAuthentication Portal (認証ポータル) ^I にこの証明書を 信頼できる CA として使用します。ファイアウォールには、既存の信頼された認証局が数多 く登録されたリストが設定されています。ここでの信頼されたルート認証局証明書とは、お 客様の組織が追加した信頼された認証局であり、予めインストールされている信頼された認 証局リストに含まれるものではありません。
- Certificate for Secure Syslog (保護された Syslog の証明書) Syslog サーバーに向けた Syslog メッセージでのログ配信 ■ を保護する際、ファイアウォールはこの証明書を使用しま す。

証明書を生成するには、Generate(生成)をクリックし、以下のフィールドを入力します。



証明書が生成された後で、証明書を管理するためのその他のサポート対象アクショ ンがページに表示されます。

証明書を生成するため の設定	の意味
証明書タイプ	証明書を生成するエンティティを選択します。
	Local(ローカル) – ファイアウォールまたは Panorama で証明書 を生成します。
	SCEP – SCEP (Simple Certificate Enrollment Protocol) サーバー で証明書を生成し、ファイアウォールまたは Panorama に送信しま す。
証明書名	(Required (必須)) 証明書を特定するための名前を入力します (ファイ アウォールでは最大 63 文字、Panorama では最大 31 文字使用でき ます)。名前の大文字と小文字は区別されます。また、一意の名前に する必要があります。文字、数字、スペース、ハイフン、およびア ンダースコアのみを使用してください。
SCEP プロファイル	(SCEP 証明書のみ) SCEP Profile (SCEP プロファイル)を選 択し、ファイアウォールまたは Panorama が SCEP サーバーと通 信する方法を定義して、SCEP 証明書の設定を定義します。詳細 は、「Device (デバイス) > Certificate Management (証明書の管 理) > SCEP」を参照してください。GlobalProtect ポータルとして 機能する firewall を構成して、SCEP 証明書をオンデマンドで要求 し、 明書をエンドポイントに自動的にデプロイできます。

 証明書を生成するため の設定	の意味
	Generate Certificate(証明書の生成)ダイアログの残りのフィー ルドは、SCEP 証明書に適用されません。Certificate Name(証 明書名)と SCEP Profile(SCEP プロファイル)を指定した ら、Generate(生成)をクリックします。
共通名(CN)	(必須)証明書に表示されるIPアドレスまたはFQDNを入力します。
共有	複数の仮想システム(vsys)が存在するファイアウォールで、証明 書をすべてのvsysで使用できるようにする場合は、Shared[共有] を 選択します。
署名者	証明書に署名するには、ファイアウォールにインポートした認証 局(CA)証明書を使用できます。証明書を自己署名することもで き、その場合はファイアウォールが CA になります。Panorama を 使用している場合、Panorama の自己署名証明書の生成に関するオ プションがあります。
	CA 証明書をインポートした場合、またはファイアウォールで CA 証明書を発行(自己署名)した場合、作成する証明書に署名できる CA がドロップダウン リストに表示されます。
	証明書署名要求 (CSR) を生成するには、External Authority (CSR)[外 部認証局 (CSR)] を選択します。ファイアウォールが証明書とキー ペアを生成したら、CSR をエクスポートして、署名のために CA に 送信できます。
認証局	ファイアウォールで証明書を発行する場合、このオプションを選択 します。
	証明書を認証局としてマークすることで、ファイアウォールでの他 の証明書の署名にこの証明書を使用できます。
Block Private Key Export(秘密鍵のエク スポートのブロック)	証明書を生成する際、このオプションを選択して、スーパーユー ザーを含む管理者すべてが秘密鍵をエクスポートできないようにし ます。
OCSP Responder(OCSP レ スポンダ)	OCSP レスポンダ プロファイルをドロップダウン リストから選択 します(「Device(デバイス)> Certificate Management(証明書 の管理)> OCSP Responder(OCSP レスポンダ)」を参照)。対 応するホスト名が証明書に表示されます。
アルゴリズム	証明書のキー発行アルゴリズムを選択します。RSAまたはElliptic Curve DSA(ECDSA)。

証明書を生成するため の設定	の意味
	ECDSA で使用される鍵のサイズは RSA アルゴリズムよりも小さい ため、SSL/TLS 接続を処理するときのパフォーマンスが向上しま す。また、ECDSA では、RSA 以上のセキュリティが確保されてい ます。ECDSA は、これをサポートするクライアント ブラウザとオ ペレーティング システムにお勧めですが、レガシー ブラウザとオ ペレーティング システムとの互換性のために RSA の選択が求めら れることがあります。
	 PAN-OS 6.1 より前のリリースを実行しているファイ アウォールでは、Panorama からプッシュした ECDSA 証明書が削除されます。また、これらのファイア ウォールでは、ECDSA 認証局(CA)によって署名さ れた RSA 証明書が無効になります。
	ハードウェア セキュリティ モジュール(HSM)を使用して、SSL フォワード プロキシまたはインバウンド インスペクション復号化 に使用する ECDSA 秘密鍵を保存することはできません。
ビット数	証明書の鍵長を選択します。
	ファイアウォールが FIPS-CC モードで、鍵生成の Algorithm(アル ゴリズム)が RSA の場合、生成される RSA キーは 2048 ビットま たは 3027 ビットである必要があります。Algorithm[アルゴリズム] が Elliptic Curve DSA の場合、両方の鍵長オプション (256 と 384) が機能します。
ダイジェスト	証明書の Digest[ダイジェスト] アルゴリズムを選択します。使用可 能なオプションは、鍵生成の Algorithm[アルゴリズム] によって異 なります。
	・ RSA – MD5、SHA1、SHA256、SHA384、または SHA512
	・ Elliptic Curve DSA – SHA256 または SHA384
	ファイアウォールがFIPS-CCモードに設定され、キー生成の Algorithm[アルゴリズム] が RSA の場合、Digest[ダイジェスト] ア ルゴリズムとしてSHA256、SHA384、またはSHA512を選択する 必要があります。Algorithm[アルゴリズム] が Elliptic Curve DSA の場合、両方の Digest[ダイジェスト] アルゴリズム (SHA256 と SHA384) が機能します。

証明書を生成するため の設定	の意味
	 TLSv1.2に依存するファイアウォールサービス(Web インターフェイスへの管理者アクセスなど)の要求時 に使用するクライアント証明書に、ダイジェストア ルゴリズムとして SHA512 を含めることはできませ ん。ファイアウォールサービスに SSL/TLS サービス プロファイルを設定するときは、クライアント証明書 で低いダイジェストアルゴリズム(SHA384 など) を使用するか、Max Version(最大バージョン)を TLSv1.1に制限する必要があります(「Device(デバ イス) > Certificate Management(証明書の管理) > SSL/TLS Service Profile (SSL/TLS サービス プロファ イル)」を参照)。
有効期限(日)	 証明書が有効な日数(デフォルトは 365)を指定します。 GlobalProtect サテライト設定で Validity Period[有効期間]を指定すると、このフィールドに入力した値はその値でオーバーライドされます。
証明書の属性	必要に応じて、Add[追加]をクリックし、証明書の発行先となるエ ンティティの識別に使用する追加の Certificate Attributes[証明書 の属性]を指定します。また、次のような属性を付加することがで きます。Country[国]、State[州]、Locality[地域]、Organization[組 織]、Department[部門]、およびEmail[電子メール]。更に、以下の うちーつのSubject Alternative [サブジェクトの代替名] フィールド を指定することができます。Host Name[ホスト名](サブジェクト 代替名: DNS)、IP(サブジェクト代替名: IP)、およびAlt Email[代 替電子メールアドレス](サブジェクト代替名: email)。

ハードウェア セキュリティ モジュール (HSM) を設定している場合、秘密鍵はファ イアウォールではなく外部 HSM ストレージに保存されます。

証明書を管理するためのその他のサポート対象アクション

証明書を生成すると、その詳細がページに表示され、以下のアクションを使用できます。

証明書を管理するため のその他のサポート対 象アクション	の意味
削除します。	証明書を選択して Delete (削除)します。
	ファイアウォールに復号化ポリシーが設定されている場合、用途がForward Trust Certificate(信頼できる証明書を転送)またはForward Untrust Certificate(信頼できない証明書を転送)に設定されている証明書を削除することができません。証明書の用途を変更する方法については、「信頼できる既定証明機関の管理」を参照してください。
無効化	無効にする証明書を選択し、 Revoke [無効化] をクリックします。証 明書はただちに「無効化」状態に設定されます。コミットは必要あ りません。
更新	証明書が期限切れになった場合、または間もなく期限切れになる場合、対応する証明書を選択して Renew[更新] をクリックします。証明書の有効期間 (日数) を設定して OK をクリックします。
	ファイアウォールが証明書を発行した CA である場合、ファイア ウォールはその証明書を、古い証明書と属性が同じでシリアル番号 が異なる新しい証明書に置き換えます。
	外部認証局(CA)が証明書に署名し、ファイアウォールがオンラ イン証明書状態プロトコル(OCSP)を使用して証明書の失効状態 を検証している場合、ファイアウォールは OCSP レスポンダ情報を 使用して証明書の状態を更新します。
インポート	証明書を Import(インポート)し、以下のように設定します。
	 証明書を識別する Certificate Name (証明書名) を入力します。
	 証明書ファイルを参照します。PKCS12をインポートすると、1つのファイルに証明書および秘密鍵の両方を含んでいます。PEM証明書をインポートした場合、ファイルには証明書のみが含まれています。
	• 証明書ファイルのFile Format[ファイル形式]を選択します。
	 この証明書の秘密キーの保存にHSMを使用している場合、Private key resides on Hardware Security Module[秘密鍵は ハードウェアセキュリティモジュール上にあります]を選択し ます。HSM の詳細は、「Device(デバイス) > Setup(セット アップ) > HSM」を参照してください。
	 必要に応じて Import Private Key(秘密鍵のインポート)を 行います(PEM 形式のみ)。証明書の File Format(ファ

証明書を管理するため のその他のサポート対 象アクション	の意味
	イル形式)として PKCS12 を選択した場合、選択した Certificate File(証明書ファイル)にキーが含まれていま す。PEM 形式を選択した場合、暗号化された秘密鍵ファイ ル(通常のファイル名は *.key)を参照します。両方の形 式について、Passphrase(パスフレーズ)および Confirm Passphrase(パスフレーズ再入力)を入力します。
	証明書をインポートして、Import Private Key(秘密鍵のイン ポート)を選択する場合、Block Private Key Export(秘密鍵の エクスポートをブロックする)を選択して、スーパー ユーザー を含む管理者が秘密鍵をエクスポートできないようにします。
	FIPS-CC モードの Palo Alto Networks ファイアウォー ルまたは Panorama サーバーに証明書をインポートする場合、Base64-Encoded Certificate (PEM) として証明書をインポートし、AES で秘密鍵を暗号化する必要があります。また、パスフレーズベースの鍵導出方法として SHA1 を使用する必要があります。
	PKCS12 証明書をインポートするには、(OpenSSL などのツールを 使用して)証明書を PEM 形式に変換します。変換中に使用するパ スワード フレーズが 6 文字以上であることを確認してください。
エクスポート	エクスポートする証明書を選択して Export(エクスポート)をク リックし、File Format(ファイル形式)を選択します。
	 Encrypted Private Key and Certificate (PKCS12)(暗号化された秘密鍵と証明書(PKCS12)) – エクスポートしたファイルには証明書とキーの両方が含まれます。
	 Base64 Encoded Certificate (PEM)(Base64 エンコード済み証明 書(PEM) – 秘密鍵も必要となる場合は、さらに Export Private Key(秘密鍵のエクスポート)を選択し、Passphrase(パスフ レーズ)および Confirm Passphrase(パスフレーズの再入力) を入力します。
	 Binary Encoded Certificate (DER) (バイナリエンコード済み証明 書(DER)) - キーはエクスポートできず、証明書のみがエクス ポート可能です。Export Private Key (秘密鍵のエクスポート) お よびパスフレーズのフィールドは使用しないでください。
HA キーのインポート	HA キーは、両方のファイアウォール ピア間で入れ替える必要があります。つまり、ファイアウォール 1 のキーをエクスポートして
HA キーのエクスポー ト	ファイアウォール2でインポートし、その逆も実行します。

証明書を管理するため のその他のサポート対 象アクション	の意味
	高可用性(HA)の鍵をインポートする場合は、Import HA Key[HAキーのインポート] をクリックし、Browse[参照] からイン ポートする鍵ファイルを指定します。
	HA の鍵をエクスポートするには、Export HA Key[HA キーのエク スポート] をクリックして、ファイルを保存する場所を指定しま す。
証明書の使用方法の定 義	名前列で証明書を選択し、証明書の用途に合ったオプションを選択 します。
PDF/CSV	最低限の読み取り専用アクセス権を持つ管理ロールは、管理対象の 証明書設定のバンドルを PDF/CSV としてエクスポートできます。 フィルターを適用して、監査などのためのより具体的な表構成出力 を作成することができます。Web インターフェイスで表示可能な 列のみがエクスポートされます。「Configuration Table Export(設 定バンドルのエクスポート)」を参照してください。

信頼できる既定証明機関の管理

 Trusted Certificate Authorities [デバイス > 証明書の管理 > 証明書 > デフォルトの信頼できる 証明機関]

ファイアウォールで信頼する事前に含まれた認証局 (CA) を表示、無効化、またはエクスポート するには、このページを使用します。事前にインストールされた CA のリストには、ファイア ウォールがインターネットへの接続を保護するために必要な証明書を発行する最も一般的で信頼 できる証明書プロバイダが含まれています。信頼のある各ルート CA に対して、名前、サブジェ クト、発行者、有効期限、有効性の状態が表示されます。

中間 CA はファイアウォールと信頼されたルート CA 間の信頼チェーンの一部ではないため、 ファイアウォールはデフォルトで中間 CA を信頼しません。ファイアウォールが信頼する中 間 CA と組織が必要とする追加の信頼できるエンタープライズ CA (Device (デバイス) > Certificate Management (証明書管理) > Certificates (証明書) > Device Certificates (デバイ ス証明書))を手動で追加する必要があります。

信頼できる証明機関設定	の意味
Enable [有効化]	CA を無効にした場合は、再び Enable(有効化)できます。
無効化	CA を選択して Disable (無効化) します。このオプションを使用 して、特定の CA のみを信頼したり、ローカル CA のみを信頼し てその他すべての CA を無効にしたりすることができます。

信頼できる証明機関設定	の意味
エクスポート	CA証明書を選択し、Export[エクスポート] します。証明書はオフ ラインで別のシステムにインポートしたり表示したりできます。

Device > Certificate Management > Certificate Profile [デバイス > 証明書の管理 > 証明書プロファイル]

- デバイス > 証明書の管理 > 証明書プロファイル
- Panorama > 証明書の管理 > 証明書プロファイル

証明書プロファイルでは、どの認証局(CA)証明書を使用してクライアント証明書を検証 するか、証明書失効状態をどのように検証するか、その状態でどのようにアクセスを制限 するかを定義します。Authentication Portal(認証ポータル)、GlobalProtect、サイト間の IPSec VPN、Dynamic DNS(DDNS)、Web インターフェースによるファイアウォールおよび Panorama へのアクセスの証明書認証を設定する際に、このプロファイルを選択します。これら の各サービスに別々の証明書プロファイルを設定できます。

証明書プロファイル設定	の意味
名前	(必須) プロファイルを識別する名前を入力します(ファイア ウォールでは最大 63 文字、Panorama では最大 31 文字使用で きます)。名前の大文字と小文字は区別されます。また、一意 の名前にする必要があります。文字、数字、スペース、ハイフ ン、およびアンダースコアのみを使用してください。
場所	プロファイルを使用できる範囲を選択します。複数の仮想シス テム (vsys) があるファイアウォールの場合、vsys を選択する か、Shared[共有] (すべての仮想システム) を選択します。その 他の場合、Location(場所)を選択することはできません。こ の値は Shared(共有)(ファイアウォール)または Panorama として事前に定義されています。プロファイルを保存すると、 その [場所] を変更できなくなります。
ユーザー名フィールド	GlobalProtect がポータルおよびゲートウェイ認証にのみ証 明書を使用する場合、PAN-OS ソフトウェアは Username Field(ユーザー名フィールド)ドロップダウン リストで選択 された証明書フィールドをユーザー名として使用し、それを User-ID サービスの IP アドレスと照合します。
	• Subject (サブジェクト)共通名です。
	 Subject Alt(サブジェクト代替名) –メールまたはプリンシパル名です。
	• None(なし) – これは通常、GlobalProtect デバイスまた は pre-login 認証に使用されます。
ドメイン	PAN-OS ソフトウェアが User ID を介してユーザーをマッピン グできるように、NetBIOS ドメインを入力します。

証明書プロファイル設定	の意味
CA 証明書	(必須) CA Certificate (CA証明書) をAdd (追加)してプロファ イルに割り当てます。
	必要に応じて、ファイアウォールで Online Certificate Status Protocol (OCSP)を使用して証明書の失効状態を検証する場 合は、以下のフィールドを設定して、デフォルトの動作をオー バーライドします。ほとんどのデプロイメントでは、これらの フィールドは適用されません。
	 ファイアウォールはデフォルトで証明書の認証機関アク セス(AIA)情報を使って OCSP レスポンダ情報を抽出 します。AIA 情報をオーバーライドするには、Default OCSP URL(デフォルト OCSP URL)(http://または https://で始まる)を入力します。
	 デフォルトでは、ファイアウォールは CA Certificate[CA 証明書] フィールドで選択した証明書を使用して、OCSP 応答を検証します。検証に異なる証明書を使用するには、OCSP Verify CA Certificate[OCSP 検証 CA 証明書] フィールドでその証明書を選択します。
	さらに、証明書の署名に使用したテンプレートを識別す るTemplate Name (テンプレート名)を入力します。
CRL の使用	証明書無効リスト(CRL)を使用して証明書の失効状態を検証 する場合は、このオプションを選択します。
OCSP の使用	OCSPを使用して証明書の失効状態を検証する場合は、このオ プションを選択します。
	OCSP と CRL の両方を選択している場合、ファイ アウォールはまず OCSP を試行します。OCSP レ スポンダを使用できない場合に限り、CRL 方式に フォールバックします。
CRL 受信の有効期限	ファイアウォールが CRL サービスからの応答を待機する期間 (1 ~ 60 秒)を指定します。
OCSP 受信の有効期限	ファイアウォールが OCSP レスポンダからの応答を待機する 期間(1~60秒)を指定します。
証明書の有効期限	ファイアウォールが任意の証明書状態サービスからの応答を待 機する期間(1~60秒)を指定します。この期間が終了する と、定義したセッションブロックロジックが適用されます。

証明書プロファイル設定	の意味
証明書状態が不明な場合に セッションをブロック	OCSPまたはCRLサービスから証明書の失効状態がunknown [不明] と返された際にファイアウォールでそのセッションをブロックする場合は、このオプションを選択します。その他の場合は、ファイアウォールはセッションを続行します。
タイムアウト時間内に証明 書状態を取得できない場合 にセッションをブロック	ファイアウォールでOCSPまたはCRL要求のタイムアウトを登 録した後にセッションをブロックする場合は、このオプション を選択します。その他の場合は、ファイアウォールはセッショ ンを続行します。
証明書が認証側デバイスに 発行されなかった場合セッ ションをブロック	(GlobalProtect のみ) クライアント証明書の件名のシリアル 番号属性が、GlobalProtect アプリケーションがエンドポイン トに対してレポートする host ID (ホストID) と一致しない場 合にファイアウォールでセッションをブロックする場合は、こ のオプションを選択します。その他の場合は、ファイアウォー ルはセッションを許可します。このオプションはGlobalProtect 証明書認証のみに適用されます。

Device > Certificate Management > OCSP Responder [デバイス > 証明書の管理 > OCSP レスポンダ]

証明書の失効状態を検証するための Online Certificate Status Protocol (OCSP) レスポンダ (サーバー)を定義する場合は、Device (デバイス) > Certificate Management (証明書の管 理) > OCSP Responder (OCSP レスポンダ)のページを開きます。

OCSP を有効にするには、OCSP レスポンダを追加するだけでなく、以下のタスクを実行する必要があります。

- ファイアウォールと OCSP サーバー間の通信を有効にする: Device(デバイス) > Setup(設定) > Management(管理)を選択し、Management Interface Settings(管理インターフェイス設定) セクションから HTTP OCSP サービスを選び、OK をクリックします。
- ファイアウォールで送信 SSL/TLS トラフィックを復号化する場合に、必要に応じて宛 先サーバー証明書の失効状態を検証させる方法: Device(デバイス) > Setup(設定) > Sessions(セッション)を選択し、Decryption Certificate Revocation Settings(復号化証 明書失効の設定)をクリックし、OCSP セクションで Enable(有効化)を選択し、Receive Timeout(受信の有効期限)(ファイアウォールが OCSP 応答を待機する期間)を入力して OK をクリックします。
- 必要に応じて、OCSP レスポンダとしてファイアウォールを設定するために、OCSP サービスで使用するインターフェイスにインターフェイス管理プロファイルを追加します。 最初に、Network(ネットワーク) > Network Profiles(ネットワークプロファイル) > Interface Mgmt(インターフェイス管理)を選択し、Add(追加)をクリックして、HTTP OCSP を選択し、OK をクリックします。次に、Network(ネットワーク) > Interfaces(インターフェイス)を選択し、ファイアウォールが OCSP サービスに使用するインターフェイスの名前をクリックし、Advanced(詳細) > Other info(その他の情報)を選択し、設定したインターフェイス管理プロファイルを選択して、OK、Commit(コミット)の順にクリックします。



証明書が取り消された場合に通知を受け取り、適切な作業を行ってポータルおよび ゲートウェイへの接続を保護できるよう、OCSP レスポンダを有効化します。

OCSP レスポンダ設定	の意味
氏名	レスポンダの識別に使用する名前 (最大 31 文字) を入力しま す。名前では大文字と小文字を区別します。英字、数字、 スペース、ハイフン、およびアンダースコアのみを使用 し、一意である必要があります。
場所	レスポンダを使用できる範囲を選択します。複数の仮想シ ステム (vsys) があるファイアウォールの場合、vsys を選択 するか、Shared[共有] (すべての仮想システム) を選択しま す。その他の場合、[場所] を選択することはできません。
OCSP レスポンダ設定	の意味
--------------	---
	この値は [共有] として事前に定義されています。レスポン ダを保存すると、その [場所] を変更できなくなります。
ホスト名	OCSP レスポンダのホスト名 (推奨) または IP アドレスを入 力します。PAN-OS はこの値から URL を自動的に導出し、 検証する証明書にその URL を追加します。ファイアウォー ルを OCSP レスポンダとして設定する場合、ホスト名は、 ファイアウォールが OCSP サービスに使用するインター フェイスの IP アドレスに解決される必要があります。

Device > Certificate Management > SSL/TLS Service Profile [デバイス > 証明書の管理 > SSL/TLS サービス プ ロファイル]

- Device > Certificate Management > SSL/TLS Service Profile [デバイス > 証明書の管理 > SSL/ TLS サービス プロファイル]
- Panorama > Certificate Management > SSL/TLS Service Profile [Panorama > 証明書の管理 > SSL/TLS サービス プロファイル]

SSL/TLS サービス プロファイルでは、SSL/TLS を使用するファイアウォール サービスまたは Panorama サービス(Web インターフェイスを使用する管理アクセスなど)のサーバー証明書お よびプロトコル バージョンまたはバージョンの範囲を指定します。プロトコル バージョンを定 義することで、サービスを要求するクライアント システムとの通信の保護に使用できる暗号ス イートをプロファイルで制限できます。

ファイアウォール サービスまたは Panorama サービスを要求するクライアントシステムでは、SSL/TLS サービス プロファイルで指定されている証明書を発行した認証局(CA)証明書を証明書信頼リスト(CTL)に含める必要があります。これを含めない場合、ユーザーがサービスを要求したときに証明書エラーが発生します。ほとんどのサードパーティ CA 証明書がクライアント ブラウザにデフォルトで表示されます。エンタープライズまたはファイアウォール生成の CA 証明書が発行者の場合、その CA 証明書をクライアント ブラウザの CTL に適用する必要があります。

プロファイルを追加するには、Add(追加)をクリックし、以下の表に従ってフィールドを入力します。

SSL/TLS サービス プロファイル の設定	の意味
氏名	プロファイルの識別に使用する名前を入力します(最大 31 文字)。名前では大文字と小文字を区別します。英字、数 字、スペース、ハイフン、およびアンダースコアのみを使 用し、一意である必要があります。
共有	ファイアウォールに複数の仮想システム(vsys)がある 場合、このオプションを選択すると、プロファイルを すべての仮想システムで使用できます。デフォルトで は、このオプションはオフになっており、プロファイル は、Device(デバイス)タブの Location(場所)ドロップ ダウンリストで選択した vsys でのみ使用できます。
証明書	サーバー証明書を選択、インポート、または生成し、プロ ファイルに関連付けます(「ファイアウォール証明書およ び Panorama 証明書の管理」を参照)。

SSL/TLS サービス プロファイル の設定	の意味
	← SSL/TLS サービスには認証局 (CA) 証明書は使 用せずに、署名付き証明書のみを使用しでく ださい。
最小バージョン	サービスで使用できる TLS の最も古いバージョン(Min Version(最小バージョン))と最も新しいバージョン
最大バージョン	 (Max Version (最大バージョン))を選択します。 TLSv1.0、TLSv1.1、TLSv1.2、TLSv1.3、または Max(最大) (入手可能な最新バージョン)。
	PAN-OS 8.0 またはそれ以降のリリースで実行する FIPS/CC モードのファイアウォールでは、 TLSv1.1 は サポートされている TLS バージョンの中で最も古いも のです。TLSv1.0 は選択しないでください。
	TLSv1.2 を使用するファイアウォール サービスを要求 する場合、使用するクライアント証明書に SHA512 を ダイジェスト アルゴリズムとして含めることはでき ません。クライアント証明書でより低いダイジェスト アルゴリズム(SHA384 など)を使用するか、サービ スのMax Version(最大バージョン)を TLSv1.1 に制 限する必要があります。
	 できるだけ強固なバージョンのプロトコルを 使用し、ネットワークのセキュリティを最大 化します。可能な場合はMin Version (最低バー ジョン)をTLSv1.2に、Max Version (最大バー ジョン)をMax (最大)にしてください。

Device > Certificate Management > SCEP [デバイス > 証明書の管理 > SCEP]

SCEP (Simple Certificate Enrollment Protocol) は、エンドポイント、ゲートウェイ、サテライト デバイスに対し、個別の証明書を発行するメカニズムを備えています。SCEP 設定を作成する場合は、Device (デバイス) > Certificate Management (証明書の管理) > SCEPを選択します。

🍙 SCEP プロファイルの作成方法の詳細については、

Deploying Certificates Using SCEP(SCEP を使用する証明書の導入)

を参照してください

新しい SCEP 設定を始める場合は、Add(追加)をクリックし、以下のフィールドに情報を入力します。

SCEP 設定	の意味
氏名	この SCEP 設定に、SCEP_Example など、分かりやすい名前を指定 します。この名前により、それぞれのSCEPプロファイルと設定プ ロファイル中に含まれるその他のインスタンスが区別されます。
場所	マルチ仮想システムのあるシステムの場合はプロファイルの場所を 選択します。ここで設定する場所はSCEP設定が入手できる場所を 示します。

ワンタイムパスワード(チャレンジ)

SCEPチャレンジ	(任意) SCEP ベースの証明書発行の安全性を高めたい場合は、 各回の証明書要求について公開鍵基盤(PKI)およびポータルと の間に SCEP チャレンジレスポンス機能(1 回限りのパスワード (OTP))を設定することができます。
	この機能の設定後はバックグラウンドで動作するため、追加の入力が必要になることはありません。
	選択するチャレンジ機能により、OTP のソースが決まりま す。Fixed(固定)を選択する場合は、PKI の SCEP サーバーから登 録チャレンジパスワードをコピーし、Fixed(固定)に設定したと きに表示される、ポータルの Password(パスワード)ダイアログ にその文字列を入力します。ポータルが証明書を要求するたびに、 このパスワードが使用されて PKI で認証されます。Dynamic(動 的)を選択する場合は、任意のユーザー名およびパスワード(多く の場合は PKI 管理者の認証情報となります)と、ポータルのクライ アントがこれらの認証情報を送信する SCEP Server URL(サーバー

SCEP 設定	の意味
	URL)を入力します。各回の証明書要求に対し SCEP サーバーが 透過的に OTP パスワードを生成する場合、ユーザー名およびパス ワードが変更されることはありません。(各回の証明書要求の後で 「The enrollment challenge password is(登録チャレンジパスワー ド)」のフィールドに表示された OTP は画面更新時に変更されま す)。PKIはそれぞれの新しいパスワードをポータルへ透過的に受 け渡し、また、証明書要求に対してそれらのパスワードを使用しま す。
	 連邦情報処理標準(FIPS)に準拠するため 米国連邦情報処理標準(FIPS)を順守するため、Dynamic(動的)を選択し、HTTPSを使用する Server URL(サーバー URL)を指定し、SCEP Server SSL Authentication(SCEP サーバー SSL 認証)を有効化します。(FIPS-CCの実施についてはファイア ウォールのログインページおよびファイアウォールの ステータスバーに表示されます。)
設定	
サーバー URL	ポータルがリクエストを行い、SCEP サーバーからクライアント証 明書を入手する URL を入力します。例:
	<pre>http://<hostname ip="" or="">/certsrv/mscep/.</hostname></pre>
CA-IDENT 名	SCEP サーバーの識別に使用する文字列を入力します。最大 で255文字です。
サブジェクト	デバイスおよび任意でユーザーに関する識別情報を含むようにサ ブジェクトを設定し、証明書署名要求(CSR)でこの情報を SCEP サーバーに提供します。
	エンドポイントのクライアント証明書の要求に使用すると、 エンドポイントはデバイスに関する識別情報を送信し、これに はホスト ID 値が含まれます。GUID(Windows)、インター フェイスのMACアドレス(Mac)、Android ID(Androidデバイ ス)、UDID(iOSデバイス)、あるいはGlobalProtectが割り当て る一意の名前(Chrome)など、ホストIDの値はデバイスの種類に よって異なります。サテライト デバイスの証明書の要求に使用する とき、ホスト ID 値はデバイスのシリアル番号になります。
	追加情報を CSR に指定するには、サブジェクト名を入力します。 サブジェクトは、 <attribute>=<value>の形式で識別される名前にし て、コモンネーム(CN)キーを含める必要があります。以下に例 を示します。</value></attribute>

SCEP 設定	の意味
	O=acme,CN=acmescep
	CN を指定するには、以下の2つの方法があります。
	 (推奨)トークンベースの CN – サポートされるいずれかのトー クン、\$USERNAME、\$EMAILADDRESS、\$HOSTID を入力しま す。ポータルが必ず特定のユーザー用の証明書をリクエストす るよう、ユーザー名あるいはメールアドレスの変数を使用しま す。デバイスのみに対する証明書をリクエストするには、hostid 変数を指定します。GlobalProtect ポータルがエージェントに SCEP 設定をプッシュするとき、サブジェクト名の CN の部分 は、証明書の所有者が持つ実際の値(ユーザー名、hostid、ある いはメール アドレス) に置き換えられます。以下に例を示しま す。
	O=acme,CN=\$HOSTID
	 Static CN[静的CN] – 指定する CN は、SCEP サーバーで発行されるすべての証明書のサブジェクトとして使用されます。以下に例を示します。
	O=acme,CN=acmescep
サブジェクトの代替名 タイプ	None(なし)以外のタイプを選択した場合は、それぞれの値を入 力するためのダイアログが表示されます。
	 RFC 822 Name (RFC822 名) – 証明書のサブジェクトまたは サブジェクト代替名拡張子に電子メールアドレス名を入力しま す。
	 DNS Name[DNS名] - 証明書の検証に使用するDNS名を入力します。
	 Uniform Resource Identifier (URI)[ユニフォームリソース識別子(URI)] - クライアントが証明書を取得するURIリソース名を入力します。
暗号設定	 Number of Bits(ビット数) – 証明書のキー用に Number of Bits(ビット数)を選択します。ファイアウォールがFIPS- CCモードの場合、生成されるキーは最低でも2048ビット以上 である必要があります。(FIPS-CCの実施についてはファイア ウォールのログインページおよびファイアウォールのステータ スバーに表示されます。)
	 Digest[ダイジェスト] – 証明書のDigest[ダイジェスト] ア ルゴリズムを選択します。SHA1、SHA256、SHA384、ま たはSHA512。ファイアウォールがFIPS-CCモードに設定

SCEP 設定	の意味
	されている場合、Digest[ダイジェスト] アルゴリズムとし てSHA256、SHA384、またはSHA512を選択する必要がありま す。
デジタル証明書として 使用	デジタル署名の検証を行う際に、証明書に含まれる秘密鍵を使用す るようにエンドポイントを設定する場合はこのオプションを選択し てください。
キーの暗号化に使用	SCEPサーバーが発行する証明書を通して確立されたHTTPS接続を 経由して交換されたデータをクライアントのエンドポイントで暗号 化する際に、証明書に含まれる秘密鍵を使用するよう設定する場合 はこのオプションを選択します。
CA 証明書フィンガー プリント	(任意) ポータルが正しい SCEP サーバーに確実に接続されるようにするために、CA Certificate Fingerprint (CA 証明書フィン ガープリント)を入力します。SCEP サーバー インターフェイスの Thumbprint (サムプリント) フィールドからフィンガープリントを 入手してください。
	SCEP サーバーの管理ユーザー インターフェイスにログインします (「http://<ホスト名または IP>/CertSrv/mscep_admin/」など)。 サムプリントをコピーし、CA Certificate Fingerprint (CA 証明書 フィンガープリント) に入力します。
SCEP サーバー SSL 認 証	SSL を有効にするには、SCEP サーバーのルート CA Certificate (CA 証明書)を選択します。また、必要に応じ てClient Certificate[クライアント証明書] を選択し、SCEPサーバー とGlobalProtectポータルの間の相互SSL認証を有効にすることも可 能です。

Device (デバイス) > Certificate Management (証明 書の管理) > SSL Decryption Exclusion (SSL 復号化例 外)

SSL 復号化例外 □ を表示して管理します。復号化例外には、事前定義済み例外とカスタム例外 の2種類があります。

- 事前定義済み例外では、ファイアウォールが復号化するときに中断する可能性があるアプリケーションとサービスを暗号化したまま残すことができます。Palo Alto Networks では、事前定義済み復号化例外を定義し、事前定義済み例外リストの更新と追加を、アプリケーションと脅威のコンテンツ更新の一部として定期的に配信しています。事前定義済み例外はデフォルトで有効ですが、必要に応じてこの例外を無効化できます。
- カスタム復号化例外を作成すると、サーバートラフィックを復号化から除外できます。対象 サーバーからのトラフィックや対象サーバーへのトラフィックはすべて暗号化されたまま残 ります。

⑦ アプリケーション、送信元、宛先、URL カテゴリ、サービスに基づいて、トラ フィックを復号化から除外 □ することもできます。

このページの設定を使用して、復号化例外の変更や追加や、復号化例外を管理を行ってください。

SSL 復号化例外の設定 の意味

復号化例外の変更または追加

ホスト名	カスタム復号化例外を定義するには、Hostname(ホスト名)を入力 します。ファイアウォールは、ホスト名を、クライアントから要求さ れた SNI またはサーバー証明書で提示された CN と比較します。ファ イアウォールは、定義されたドメインを含む CN をサーバーから提示 された場合、セッションを復号化から除外します。
	アスタリスク(*)をワイルドカードとして使用して、ドメインに関 連付けられた複数のホスト名の復号化除外を設定できます。アスタリ スクは、キャレット(^)が URL カテゴリの例外に対して動作するのと 同じように動作し、各アスタリスクは、ホスト名の1つの可変サブド メイン(ラベル)を制御します。これにより、具体的な除外と一般的な 除外の両方を作成できます。以下に例を示します。
	 mail.*.com は mail.company.com と一致します が、mail.company.sso.com には一致しません。
	 *.company.com は tools.company.com と一致します が、eng.tools.company.com には一致しません。
	 ..company.com は eng.tools.company.com と一致しますが、eng.company.com には一致しません。

SSL 復号化例外の設定	の意味
	 ..*.company.com は corp.exec.mail.company.com と一致します が、corp.mail.company.com には一致しません。
	 mail.google.* は mail.google.com に一致します が、mail.google.uk.com には一致しません。
	 mail.google.*.* は mail.google.co.uk と一致します が、mail.google.com には一致しません。
	video-stats.video.google.comを復号化から除外 し、video.google.comを除外するには、 [SSL復号化除外]リストに *.*.google.comを追加します。
	ホスト名はエントリごとに一意である必要があります。事前定義済み エントリがファイアウォールに配信され、それが既存のカスタムエ ントリと一致する場合は、カスタムエントリが優先されます。
	事前定義済み復号化例外のホスト名を編集することはできません。
共有	マルチ仮想システム ファイアウォールのすべての仮想システムで復 号化例外を共有するには、Shared(共有)を選択します。
	事前定義済み復号化例外はデフォルトでは共有されますが、事前定義 済みエントリとカスタム エントリの両方を、特定の仮想システムで 有効にしたり無効にしたりすることができます。
の意味	(任意)復号化から除外するアプリケーションについて、そのアプリ ケーションが復号化時に中断する理由などを説明します。
除外	アプリケーションを復号化から除外します。復号化から除外していた アプリケーションの復号化を開始するには、このオプションを無効に します。
復号化例外の管理	
Enable [有効化]	1 つ以上のエントリを Enable(有効化)して、復号化から除外しま す。

無効化	1つ以上の事前定義済み復号化例外を Disable(無効化)します。
	復号化例外では 復号化時に由断するアプリケーションが識別され

復号化例外では、復号化時に中断するアブリケーションが識別され るため、いずれかのエントリを無効にすると、アプリケーションはサ ポートされなくなります。ファイアウォールがアプリケーションの復 号化を試し、そのアプリケーションは中断します。特定の暗号化済み アプリケーションがネットワークに入らないようにする場合は、この オプションを使用できます。

SSL 復号化例外の設定	の意味
廃止された機能を表 示	Palo Alto Networks が復号化例外として定義しなくなった事前定義済 みエントリを表示するには、Show obsoletes(廃止された機能を表 示)します。
	廃止されたエントリの詳細:
	事前定義済み復号化例外の更新(事前定義済みエントリの削除を含 む)は、アプリケーションと脅威のコンテンツ更新の一部としてファ イアウォールに配信されます。Exclude from decryption(復号化か ら除外)が有効になっている事前定義済みエントリは、そのエント リを含まなくなったコンテンツ更新をファイアウォールが受信する と、SSL 復号化例外のリストから自動的に削除されます。
	ただし、Exclude from decryption(復号化から除外)が無効になって いる事前定義済みエントリは、そのエントリを含まなくなったコンテ ンツ更新をファイアウォールが受信した後でも SSL 復号化リストに 残ります。Show obsoletes(廃止された機能を表示)すると、無効と なって現在は適用されていない事前定義済みエントリが表示され、必 要に応じて手動で削除できるようになります。
Show Local Exclusion Cache(ローカル除 外キャッシュの表 示)	Show Local Exclusion Cache (ローカル除外キャッシュの表示) 固定証明書、クライアント認証、サポート対象外の暗号等、 復号化の妨げとなる技術的な状況により、ファイアウォールが 自動的に復号化から除外したサイトを表示します。Local SSL Decryption Cache (ローカルSSL復号化キャッシュ)は、SSL Decryption Exclusion List (SSL 復号化例外リスト) (Device (デバ イス) > Certificate Management (証明書管理) > SSL Decryption Exclusion (SSL 復号化例外))とは異なります。SSL 復号化例外リス トには、Palo Alto Networks が特定し、ユーザーが復号化例外を追加 できるサイトが含まれています。トラフィックを制御する復号化ポリ シー ルールに関連付けられた復号化プロファイルの設定に基づき、 ファイアウォールがローカルで検出された復号化例外をローカル SSL 復号化キャッシュに設定します。
	効します。例外エントリには、それぞれ、アプリケーション、サー バー、ファイアウォールがサイトを復号化から自動的に除外した理 由、トラフィックに適用された復号化プロファイル、およびVsysに関 する情報が含まれています。

Device (デバイス) > Certificate Management (証明書 の管理) > SSH Service Profile (SSH サービス プロファ イル)

SSH サービス プロファイルを使用すると、データの整合性を暗号化および保護する暗号化、 キー交換、およびメッセージ認証コードのアルゴリズムを制限することができます。具体的に は、このプロファイルは、コマンドライン インターフェース(CLI)と、ネットワーク上の管理 接続および高可用性(HA)アプライアンス間の SSH セッション中のデータ保護を強化するもの です。また、新たに SSH ホストキーを生成し、SSH キーの再生成を開始するしきい値(データ 量、時間間隔、およびパケット数)を指定することも可能です。

SSH サービス プロファイルを設定するには、HA またはManagement - Server(管理 - サー バー) プロファイルをAdd(追加)して、必要に応じて以下の表のフィールドに入力し、 OK をクリックして、変更を Commit(コミット) します。

プロファイル適用プロセスは、プロファイルの種類により異なります。

- HA プロファイルを適用するには、Device(デバイス) > High Availability(高可用性) > General(一般)を選択します。SSH HA Profile Setting(SSH HA プロファイル設定)で、既 存のプロファイルを選択します。OK をクリックし、変更を Commit (コミット) します。
- Management Server(管理サーバー) プロファイルを適用するには、Device > Setup > Management [デバイス > セットアップ > 管理]を選択します。SSH 管理プロファイル設定 で、既存のプロファイルを選択します。OK をクリックし、変更を Commit (コミット) しま す。
 - プロファイル適用後、CLIから SSH サービスの再起動を実行し、プロファイルをアクティベートする必要があります。

SSH Service Profile Settings(SSH サービス プ ロファイルの設定)	の意味
名前	プロファイル名を入力します(最大 31 文 字)。大文字と小文字を区別し、一意の名前 を入力する必要があります。文字、数字、ス ペース、ハイフン、アンダースコアのみが使 用できます。
Ciphers(暗号)	サーバーが SSH セッション暗号化に関して サポートする暗号化アルゴリズムを選択しま す。
KEX	SSH セッション中にサーバーがサポートする キー交換アルゴリズムを選択します。

SSH Service Profile Settings(SSH サービス プ ロファイルの設定)	の意味
MAC	SSH セッション中にサーバーがサポートする メッセージ認証コードのアルゴリズムを選択 します。
Hostkey	ホストキーの種類とキーの長さを選択し、指 定したホストキーのアルゴリズムとキーの長 さを持つ新しいキー ペアを生成します。
データ	SSH キーを再生成する前に送信されるデー タの最大量(メガバイト単位)を設定します (範囲は 10~4000、デフォルトは選択した 暗号の値です)。
間隔	SSH キー再生成までの最大時間間隔(秒単 位)を設定します(範囲は 10~3600、時間 ベースのキー再生成なしがデフォルト)。
パケット数	 SSH キー再生成前のパケットの最大数(2ⁿ)を設定します。 このパラメーターを構成しない場合、セッションは2²⁸パケット後にキーを再設定します。キー更新の頻度を高めるには、12から27の範囲の値を指定します。

Device > Response Pages [デバイス > 応答ページ]

カスタム応答ページは、ユーザーが URL にアクセスしようとするときに表示される Web ページ です。リクエストされた Web ページまたはファイルの代わりにダウンロードおよび表示される カスタム HTML メッセージを入力できます。

仮想システムごとに固有のカスタム応答ページを使用できます。以下の表に、ユーザーメッセー ジをサポートするカスタム応答ページのタイプを示します。

カスタム応答ページのタイプ	の意味
アンチウイルス ブロック ページ	ウイルス感染が原因でアクセスがブロックされたことを示しま す。
アプリケーション ブロック ページ	アプリケーションがセキュリティ ポリシー ルールでブロック されたためにアクセスがブロックされたことを示します。
Authentication Portal Comfort Page(認証ポータ ル確認ページ)	ユーザーがログイン認証情報を入力して、認証ポリシールー ル(「Policies(ポリシー) > Authentication(認証)」を参 照)に従ったサービスにアクセスできるよう、ファイアウォー ルでこのページが表示されます。この認証チャレンジへの応 答方法をユーザーに知らせるメッセージを入力します。ファ イアウォールは、認証ルール(「Objects(オブジェクト) > Authentication(認証)」を参照)に割り当てられた認証実施 オブジェクトで指定された認証プロファイルに基づいて、ユー ザーを認証します。
	図連する認証実施オブジェクトにメッセージを 入力することで、認証ルールごとに固有の認 証手順を表示できます。このオブジェクトで 定義されたメッセージは、Authentication Portal Comfort Page(認証ポータル確認ページ)ページ で定義されたメッセージをオーバーライドしま す。
データ フィルタリング ブ ロック ページ	センシティブな情報が検出されたため、コンテンツがデータ フィルタリング プロファイルと照らし合わされてブロックさ れます。
ファイル ブロッキング続行 ページ	ダウンロードの続行が必要なことを確認するユーザーのための ページです。このオプションは、セキュリティプロファイル で Continue(続行)機能が有効になっている場合にのみ使用 できます。[Objects] > [セキュリティプロファイル] > [ファイ ルブロッキング] の順に選択します。

カスタム応答ページのタイプ	の意味
ファイル ブロッキング ブ ロック ページ	ファイルへのアクセスがブロックされているためアクセスがブ ロックされたことを示します。
GlobalProtect アプリケー ションのヘルプ ページ	GlobalProtect ユーザー用のカスタム ヘルプページ (GlobalProtect のステータスパネルにある設定メニューから アクセス可能)です。
GlobalProtect ポータルのロ グイン ページ	GlobalProtect ポータルのウェブページに認証しようとしてい るユーザー用のログインページです。
GlobalProtect ポータルの ホーム ページ	GlobalProtect ポータルのウェブページに正常に認証するユー ザー用のホームページです。
GlobalProtect アプリケー ションのウェルカム ページ	GlobalProtect に正常に接続するユーザー用のウェルカム ページです。
MFA ログイン ページ	認証ポリシー ルール(「Policies(ポリシー)> Authentication(認証)」を参照)に従ったサービスへのアク セス時にユーザーが多重認証(MFA)チャレンジに応答でき るよう、ファイアウォールでこのページが表示されます。この MFA チャレンジへの応答方法をユーザーに知らせるメッセー ジを入力します。
SAML 認証内部エラー ペー ジ	SAML 認証に失敗したことをユーザーに通知するページ。この ページには、ユーザーが認証を再試行するためのリンクが含ま れます。
SSL 証明書エラー通知ペー ジ	SSL 証明書が無効になっていることを示す通知です。
SSL 復号オプトアウト ペー ジ	ファイアウォールが検査のためSSLセッションを復号すること を表示するユーザー警告ページ
URL フィルタリングおよび カテゴリー致ブロック ペー ジ	URL フィルタリング プロファイルが原因で、または URL カテ ゴリがセキュリティ ポリシー ルールでブロックされているた め、アクセスがブロックされたことを示します。
URL フィルタリングの続行 とオーバーライド ページ	ユーザーがブロックをバイパスできるよう一旦ブロックさせて おくページです。たとえば、ページが不適切にブロックされて いると思われる場合は、 Continue [続行] をクリックして該当の ページに進めます。
	オーバーライド ページで、この URL をブロックするポリシー をオーバーライドするには、ユーザーにパスワードの入力が 求められます。オーバーライド パスワードの設定手順の詳細

カスタム応答ページのタイプ	の意味
	は、「URL 管理オーバーライド」セクションを参照してくだ さい。
URL フィルタリング セーフ サーチの適用ブロック ペー ジ	Safe Search Enforcement (セーフ サーチを適用) オプション が有効になっている URL フィルタリング プロファイルを使 用したセキュリティ ポリシー ルールによって、アクセスがブ ロックされたことを示します。
	Bing、Google、Yahoo、Yandex、または YouTube を使用し て検索が実行され、ブラウザ、または、検索エンジンアカウ ント設定でセーフ サーチが厳密(高い)に設定されていない 場合、このページが表示されます。このブロック ページで、 セーフ サーチ設定を厳密に設定するように指示されます。
アンチフィッシング ブロッ クページ	ユーザーが Web ページで企業の有効な認証情報(ユーザー 名またはパスワード)を入力しようとしたときに、その Web ページへの認証情報の送信がブロックされている場合、ユー ザーにこのページが表示されます。ユーザーは引き続きサイト にアクセスできますが、関連する Web フォームに企業の有効 な認証情報を送信することはできません。
	認証情報の検出を有効にして、URL カテゴリに基づいて Web ページへの認証情報の送信を制御するには、Objects(オブ ジェクト) > Security Profiles(セキュリティ プロファイル) > URL Filtering(URL フィルタリング)を選択します。
アンチフィッシング 続行 ページ	このページは、企業の認証情報(ユーザー名とパスワード) をWebサイトに送信することに対してユーザーに警告を表示 します。認証情報の送信に対してユーザーに警告を表示するこ とで、企業の認証情報をユーザーが再利用することを阻止でき るほか、フィッシングの可能性についてユーザーを教育するこ とができます。ユーザーがサイトに認証情報を送信しようと したときに、そのサイトに対してユーザー証明書送信権限が continue(続行)に設定されている(「Objects(オブジェク ト) > Security Profiles(セキュリティ プロファイル) > URL Filtering(URL フィルタリング)」を参照)場合、このページ が表示されます。サイトで認証情報を入力するには、ユーザー は Continue(続行)を選択する必要があります。

必要に応じて、Response Pages[応答ページ]の下で以下の機能を実行できます。

カスタム HTML 応答ページをインポートするには、変更するページ タイプのリンクをクリックし、import/export [インポート/エクスポート] をクリックします。ページを参照して指定します。インポートが成功したかどうかを示すメッセージが表示されます。インポートを成功させるには、ファイルは必ず HTML 形式にしてください。

- カスタムHTML応答ページをエクスポートするには、該当のページタイプの Export[エクス ポート] をクリックします。ファイルを開くか、ディスクに保存するかを選択し、常に同じオ プションを使用する場合はAlways use the same option[常に同じオプションを使用] を選択し ます。
- Application Block[アプリケーションブロック] ページや SSL Decryption Opt-out[SSL復号化オ プトアウト] ページを有効化または無効化する場合は、該当のページタイプのEnable[有効化] をクリックします。必要に応じてEnable[有効化] を選択、または選択を解除してください。
- 以前にアップロードしたカスタムページの代わりにデフォルトの応答ページを使用するには、カスタムブロックページを削除してコミットします。これで、デフォルトのブロックページが新しいアクティブページに設定されます。

Device > Log Settings [デバイス > ログ設定]

アラームの設定、ログのクリア、Panorama、ロギングサービスやその他外部デバイスへのログ 転送の有効化を行うには、Device(デバイス) > Log Settings(ログ設定) を選択します。

- ログの転送先の選択
- アラーム設定の定義
- ログのクリア

ログの転送先の選択

デバイス > ログ設定

ログ設定ページでは、ログ転送を次のように設定できます。

- Panorama、SNMPトラップレシーバ、電子メールサーバー、Syslog サーバー、および HTTPサーバー-また、ログエントリの送信元または宛先 IP アドレスに対して、タグを追加 または削除できます。システム ログと設定ログ以外のすべてのログ タイプはタグ機能をサ ポートしています。
- ロギングサービス-ロギングサービスのサブスクリプションがあり、ロギングサービス (Device (デバイス) > Setup (セットアップ) > Management (管理))を有効にしている 場合、Panorama/ロギングサービスへのログ転送を設定すると、ファイアウォールはロギン グサービスにログを送信します。Panorama はログにアクセスしてログを表示し、レポート を生成するためにログサービスに照会します。
- Azure Security Center Azure Security Center との統合は Azure の VM-Series ファイア ウォールでのみ利用できます。
 - Azure Security Center から VM-Series ファイアウォールを起動した場合は、ログ転送プロ ファイルを含むセキュリティ ポリシー ルールが自動的に有効になります。
 - Azure Marketplace から VM-Series ファイアウォールを起動した場合、またはカスタム Azure テンプレートを使用している場合は、Azure Security Center にシステムログ、ユー ザー ID ログ、および HIP 一致ログを転送するために Azure-Security-Center-Integration を手動で選択し、他のログタイプのログ転送プロファイルを使用します(「Objects(オ ブジェクト) > Log Forwarding(ログ転送)」を参照してください)。



Security Center の無料のレイヤーは、Azure サブスクリプションで自動的に有効になります。

以下の log types (ログタイプ) ■を転送することができます。システム、設定、ユーザー ID、HIP 一致、および相関ログ。各ログタイプの宛先を指定する場合、一致リスト プロファイ ルを Add (追加) して(最大 64 個)、以下の表に記載されているようにフィールドを設定しま す。

トラフィック、脅威、WildFire への送信、URL フィルタリング、データ フィルタリ **(**] ング、トンネル検査、GTP、および認証ログを転送する場合、ログ転送プロファイ ルを設定する必要があります(「Objects(オブジェクト) > Log Forwarding(ログ 転送)」を参照)。

ー致リスト プロファイ ル設定	の意味
氏名	一致リスト プロファイルを識別する名前を入力します(最大 31 文字)。有効な名前はアルファベット文字で始まる必要がありま す。名前には、ゼロ、アルファベット文字、下線(_)、ハイフン (-)、ピリオド(.)、またはスペースを使用できます。
フィルタ	 デフォルトでは、一致リストプロファイルを追加したタイプの All Logs (すべてのログ)をファイアウォールは転送します。一部のログを転送するには、ドロップダウン リストを開いて既存のフィルタを選択するか、Filter Builder (フィルタ ビルダー)を選択して新しいフィルタを追加します。新しいフィルタの各クエリに対して、以下のフィールドを指定して、クエリを Add (追加) します。 Connector (条件式) – クエリの結合ロジック (AND/OR)を選択します。ロジックに否定を適用する場合は、Negate (否定)を選択します。たとえば、信頼されていないゾーンからのログ転送を防ぐには、Negate (上記以外)を選択し、Attribute (属性) として Zone (ゾーン)、Operator (演算子) として equal (等しい)を選択します。ログタイプによりを用できる属性が異なります。 Attribute (属性) – ログの属性を選択します。ログタイプにより使用できる属性が異なります。 Operator (演算子) – 属性を適用するかどうかを決定する基準を選択します (equal (等しい)など)。ログタイプにより使用できる基準が異なります。 Value[値] – 照合する属性値を指定します。 イルタが一致するログを表示またはエクスポート このタブでは Monitoring (モニタリング) タブのページと同じオプションが表示されます (Monitoring (モニタリング) タブのページと同じオプションが表示されます (Monitoring (モニタリング) メブの コルターはAll Logs (すべてのログ)です)。重大度ごとに別々のログ転送方式を指定し、Forward Method (転送方式)を設定してから残りの重大度に対して作業を繰り返します。
の意味	この一致リスト プロファイルの目的を説明します(最大 1,023 文 字)。

1062

す

デバイス

一致リスト プロファイ ル設定	の意味
Panorama/ロギング サービス	 ロギングサービス、ログコレクタまたは Panorama 管理サーバーにログを転送する場合、Panorama/Logging Service (Panorama/ロギングサービス)を選択します。このオプションを有効にする場合、configure log forwarding to Panorama (Panorama へのログ転送を設定) 相関ログをファイアウォールからPanoramaへ転送することはできません。Panoramaは受信したファイアウォールのログに応じて相関ログを生成します。
SNMP	ログを SNMP トラップとして転送するには、1つ以上の SNMP トラップ サーバー プロファイルを Add(追加)します (「Device(デバイス) > Server Profiles(サーバー プロファイ ル) > SNMP Trap(SNMP トラップ)」を参照)。
電子メール	ログを電子メール通知として転送するには、1つ以上の電子メール サーバー プロファイルを Add (追加) します(「Device (デバイ ス) > Server Profiles (サーバー プロファイル) > Email (電子メー ル)」を参照)。
Syslog	ログを Syslog メッセージとして転送するには、1つ以上の Syslog サーバー プロファイルを Add(追加)します(「Device(デバイ ス) > Server Profiles(サーバー プロファイル) > Syslog」を参 照)。
НТТР	ログを HTTP 要求として転送するには、1つ以上の HTTP サーバー プロファイルを Add(追加)します(「Device(デバイス) > Server Profiles(サーバー プロファイル) > HTTP」を参照)。
ビルトイン アクション	実行するアクションをAdd(追加)する際、Tagging(タグ付け) とIntegration(統合)の2種類の組み込みアクションから選択でき ます。

©2024 Palo Alto Networks, Inc.

す

ー致リスト プロファイ レ設定	の意味
	 タグ付け-ログエントリに送信元または宛先 IP アドレスを含む すべてのログタイプにおいては、必要に応じて以下の設定を編 集して、アクションを追加できます。
	相関ログと HIP マッチ ログの送信元 IP アドレスに のみタグ付けできます。システム ログと設定ログ では、ログ エントリに IP アドレスが含まれないた め、アクションを設定できません。
	 アクションを Add(追加)し、そのアクションを説明する名 前を入力します。
	 自動でタグ付けする IP アドレス(Source Address(送信元ア ドレス)または Destination Address(宛先アドレス))を選 択します。
	 アクション(Add Tag(タグの追加)または Remove Tag(タ グの除去))を選択します。
	 IP アドレスとタグのマッピングを、このファイアウォールまたは Panorama の Local User-ID(ローカル User-ID) エージェントに登録するか、Remote User-ID(リモート User-ID) エージェントに登録するかを選択します。
	 IP アドレスとタグのマッピングを Remote User-ID(リモート User-ID)エージェントに登録するには、転送を有効にする HTTP サーバー プロファイルを選択します(Device(デバイ ス) > Server Profiles(サーバープロファイル) > HTTP)。
	 IP 対タグの Timeout (タイムアウト)を指定すれば、IP アドレス対タグのマッピングを保持する期間(分)を設定できます。タイムアウトを0にすると、IP 対タグのマッピングがタイムアウトしなくなります(範囲は 0~43200(30 日)、デフォルトは 0)。
	タイムアウトを設定できるのはAdd Tag (タグの 追加)アクションだけです。
	 ターゲットの送信元または宛先 IP アドレスに対して適用また は削除する Tags(タグ)を入力または指定します。
	 統合-Azure の VM-Series ファイアウォールでのみ使用可能です。名前を Add(追加)し、このアクションを使用して、選択したログを Azure Security Center に転送します。このオプションが表示されない場合は、Azure Security Center で Azure サブスクリプションが有効になっていない可能性があります。

ー致リスト プロファイ ル設定	の意味
	ログ転送プロファイル フィルタに基づき、デバイスを Quarantine List(隔離リスト)に追加するには、[Quarantine(隔離)]を選択し ます。

アラーム設定の定義

• Device > Log Settings [デバイス > ログ設定]

CLI および Web インターフェイス用のアラームを設定する場合は、アラーム設定を使用しま す。以下のイベントに関する通知を設定することができます。

- 指定したしきい値および指定した時間間隔内でセキュリティ ルール (またはルールのグループ) が一致する。
- 暗号化/復号化エラーのしきい値に達する。
- 各ログタイプのログデータベースの上限に近い。デフォルトでは、空きディスク領域の90% が使用された場合に通知されるように割り当てが設定されています。アラームを設定する と、ディスクがいっぱいになってログが消去される前に対処できます。

アラームを設定した場合、Web インターフェイス下部の Alarms(アラーム)(<u>Alarms</u>)を クリックして現在のリストを表示することができます。

アラームを追加するには、次の表で説明するアラーム設定を編集します。

アラーム ログの設定	の意味
アラームの有効化	Enable Alarms(アラームを有効化)した場合のみ、アラームが表示されます。
	 アラームを無効にすると、アクションが必要となる重 大イベントについて、ファイアウォールによって警 告されなくなります。たとえば、マスターキーの期 限が近付いていることをアラームよって通知されると します。キーを変更する前にキーの期限が切れると、 ファイアウォールは再起動してメンテナンスモード になり、出荷時の設定へのリセットが必要になりま す。
CLI アラーム通知の有 効化	アラームが発生するたびに CLI アラーム通知を有効にします。
Web アラーム通知の有 効化	ウィンドウを開いてユーザー セッションに関するアラーム (ユー ザー セッションの発生や承認のタイミングなど) を表示します。

アラーム ログの設定	の意味
警告アラームの有効化	未承認のアラームが存在する場合、管理者がWebインターフェイ スにログインすると管理者のコンピューター上で警告アラーム音 が15秒ごとに再生されます。管理者がすべてのアラームを承認する まで、警告音が再生されます。 アラームの表示と承認を行う場合はAlarms[アラーム] をクリックし てください。
	この機能は、ファイアウォールが FIPS-CC モードに設定されている 場合にのみ使用できます。
暗号化/復号化エラー しきい値	アラームが生成されるまでの暗号化/復号化の失敗回数を指定しま す。
<ログタイプ> ログ DB	ログのデータベースが指定した最大サイズのパーセンテージに達し た場合にアラームを生成します。
セキュリティ違反のし きい値/ セキュリティ違反時間	Security Violations Time Period(セキュリティ違反時間)設定 で指定した期間(秒数)内に、特定の IP アドレスまたはポート が、Security Violations Threshold(セキュリティ違反のしきい 値)設定で指定した回数分、拒絶ルールにヒットした場合、アラー ムが生成されます。
違反のしきい値/ 違反の期間/ セキュリティ ポリシー タグ	Violations Time Period[違反の期間] フィールドで指定した期間に一 連のルールが Violations Threshold[違反のしきい値] フィールドで 指定したルール制限違反数に達した場合、アラームが生成されま す。セッションが明示的な拒否ポリシーに一致するときに、違反が 数えられます。
	Security Policy Tags[セキュリティ ポリシー タグ] を使用して、 ルールの制限しきい値でアラームが生成されるタグを指定します。 これらのタグは、セキュリティ ポリシーを定義するときに指定でき るようになります。
選択的監査	選択的監査のオプションはファイアウォールがFIPS-CCモードに設 定されている場合のみ使用できます。 以下の設定を指定します。
	 FIPS-CC Specific Logging[FIPS-CC固有のログ] – 情報セキュリ ティ国際評価基準 (CC) に準拠するために必要な詳細なログ記録 が有効になります。
	 Packet Drop Logging[パケット破棄のログ] - ファイアウォールが 破棄したパケットを記録します。

アラーム ログの設定	の意味
	 Suppress Login Success Logging[ログイン成功ログの抑制] – ファイアウォールへの管理者ログイン成功のログ記録が停止さ れます。
	 Suppress Login Failure Logging[ログイン失敗ログの抑制] – ファ イアウォールへの管理者ログイン失敗のログ記録が停止されま す。
	 TLS Session Logging[TLSセッションのログ] - TLSセッション確立 のログを記録します。
	 CA (OCSP/CRL) Session Establishment Logging[CA (OCSP/ CRL) セッション確立ログ] - ファイアウォールがオンライン証 明書状態プロトコルまたは証明書無効リストのサーバーリクエ ストを使用して証明書失効状態を確認するよう要求した場合 に、ファイアウォールと認証局との間のセッション確立のログ を記録します。(デフォルトで無効化されています。)
	 IKE Session Establishment Logging[IKEセッション確立ログ]- ファイアウォール上のVPNゲートウェイがピアと認証を行った 場合にIPSec IKEセッションの確立ログを記録します。この場 合のピアとは、Palo Alto Networksファイアウォール、あるい はVPN接続の開始と終了に使用される他のセキュリティデバイ スが該当します。IKEゲートウェイに固定されたインターフェイ スの名前がログに記載されます。IKEゲートウェイ名が設定され ている場合はこれも表示されます。このオプションを無効化す るとIKEのログイベントの記録がすべて停止されます。(デフォ ルトで有効化されています。)
	 Suppressed Administrators[抑制された管理者] – リストに記載された管理者による、ファイアウォールの設定変更に関するログ記録を停止します。

ログのクリア

• Device > Log Settings [デバイス > ログ設定]

ログ設定のページでログの管理をする際にファイアウォール上のログを削除することができま す。クリアするログタイプをクリックし、**Yes**(はい)をクリックして要求を確定します。



ログおよびレポートを自動的に削除したい場合は、有効期限を設定することができ ます。詳細は、「Logging and Reporting Settings(ロギングおよびレポート設定」 を参照してください。

[Device] > [サーバー プロファイル]

以下のトピックでは、ファイアウォール上で設定できるサーバー プロファイル設定について説 明します。

- Device > Server Profiles > SNMP Trap [デバイス > サーバー プロファイル > SNMP トラップ]
- Device > Server Profiles > Syslog [デバイス > サーバー プロファイル > Syslog]
- Device > Server Profiles > Email [デバイス > サーバー プロファイル > 電子メール]
- Device $(\vec{r} \cdot \vec{n} \cdot \vec{n} \cdot \vec{n})$ > Server Profiles $(\psi \vec{n} \vartheta \cdot \vec{n} \cdot \vec{n})$ > HTTP
- Device (デバイス) > Server Profiles (サーバー プロファイル) > NetFlow
- Device > Server Profiles > RADIUS [デバイス > サーバー プロファイル > RADIUS]
- [Device (デバイス)] > [Server Profiles (サーバープロファイル)] > SCP
- Device > Server Profiles > TACACS+ [デバイス > サーバー プロファイル > TACACS+]
- Device > Server Profiles > LDAP [デバイス > サーバー プロファイル > LDAP]
- Device > Server Profiles > Kerberos [デバイス > サーバー プロファイル > Kerberos]
- Device (デバイス) > Server Profiles (サーバー プロファイル) > SAML Identity Provider (SAML アイデンティティ プロバイダ)
- Device > Server Profiles > DNS [デバイス > サーバー プロファイル > DNS]
- Device (デバイス) > Server Profiles (サーバー プロファイル) > Multi Factor Authentication (多要素認証)

Device > Server Profiles > SNMP Trap [デバイス > サー バー プロファイル > SNMP トラップ]

SNMP (Simple Network Management Protocol) は、ネットワーク上のデバイスをモニターする 標準プロトコルです。システム イベントやネットワーク上の脅威に関するアラートを通知す るために、モニター対象デバイスから SNMP マネージャ (トラップ サーバー) に SNMP トラッ プが送信されます。ファイアウォールまたは Panorama から SNMP マネージャにトラップを 送信できるようにするサーバー プロファイルを設定するには、Device(デバイス) > Server Profiles(サーバー プロファイル) > SNMP Trap(SNMP トラップ)を選択するか、Panorama > Server Profiles(サーバー プロファイル) > SNMP Trap(SNMP トラップ)を選択しま す。SNMP GET メッセージ(SNMP マネージャからの統計情報要求)を有効にするには、 「SNMPモニタリングの有効化」を参照してください。

サーバー プロファイルを作成したら、SNMP トラップを送信するようにファイアウォールをト リガーするログ タイプを指定する必要があります(「Device(デバイス) > Log Settings(ロ グ設定)」を参照)。トラップを解釈できるように SNMP マネージャにロードする必要があ る MIB のリストについては、「Supported MIBs(サポートされる MIB) □」を参照してくださ い。

\leq	
	,

システム ログの設定またはログのプロファイルで使用されるサーバー プロファイ ルは削除しないでください。

SNMP トラップ サー バー プロファイルの設 定	の意味
氏名	SNMP プロファイルの名前を入力します(最大 31 文字)。名前の 大文字と小文字は区別されます。また、一意の名前にする必要があ ります。文字、数字、スペース、ハイフン、およびアンダースコア のみを使用してください。
場所	プロファイルを使用できる範囲を選択します。複数の仮想シス テム (vsys) があるファイアウォールの場合、vsys を選択する か、Shared[共有] (すべての仮想システム) を選択します。その他の 場合、Location(場所)を選択することはできません。この値は Shared(共有)(ファイアウォール)または Panorama として事前 に定義されています。プロファイルを保存すると、その[場所]を変 更できなくなります。
バージョン	SNMPバージョンを選択します。V2c(デフォルト)またはV3。この選択内容により、ダイアログに表示される残りのフィールドが決まります。どちらのバージョンでも、最大4つの SNMP マネージャを追加できます。

SNMP トラップ サー バー プロファイルの設 定	の 意味 	
	認証およびその他の機能を提供する SNMPv3 を使用 し、ネットワーク接続が保護された状態を保ちます。	
SNMP V2c の場合		
氏名	SNMP マネージャの名前を指定します。名前には、最大 31 文字 (英数字、ピリオド、アンダースコア、またはハイフン) を含めるこ とができます。	
SNMP マネージャ	SNMP マネージャの FQDN または IP アドレスを指定します。	
コミュニティ	コミュニティ文字列を入力します。これは、SNMP マネージャおよ びモニター対象デバイスの SNMP コミュニティを識別し、トラッ プの転送時にコミュニティ メンバーを相互認証するためのパスワー ドとしても機能します。コミュニティ文字列には最大 127 文字を含 めることができます。また、すべての文字を使用でき、大文字と小 文字が区別されます。 デフォルトのコミュニティ文字列は使用しないでく ださい (コミュニティ文字列をpublic (パブリック)あ るいはprivate (プライベート)に設定しないでくださ い)。複数の SNMP サービスを使用する場合に競合 が起きないよう、一意のコミュニティ文字列を使用 します。SNMP メッセージにはクリア テキストのコ ミュニティ文字列が含まれているため、コミュニティ メンバーシップ (管理者アクセス)を定義するときに ネットワークのセキュリティ要件を考慮してくださ い。	
SNMP V3 の場合		
氏名	SNMP マネージャの名前を指定します。名前には、最大 31 文字 (英数字、ピリオド、アンダースコア、またはハイフン) を含めるこ とができます。	
SNMP マネージャ	SNMP マネージャの FQDN または IP アドレスを指定します。	
感染	SNMPユーザー アカウントの識別に使用する名前を指定します(最大31文字)。ファイアウォールで設定するユーザー名は、SNMPマネージャで設定したユーザー名と一致する必要があります。	

デバイス

SNMP トラップ サー バー プロファイルの設 定	の意味
エンジン ID	ファイアウォールのエンジンIDを指定します。SNMPマネージャと ファイアウォールが相互の認証を行う場合、トラップメッセージ はこの値を使用して一意にファイアウォールを識別します。この フィールドを空白のままにすると、メッセージではファイアウォー ルシリアル番号が EnginelD[エンジンID] として使用されます。値 は、16 進数形式 (Ox のプレフィックスと、5 ~ 64 バイトの数値 を表す 10 ~ 128 文字 (バイトあたり 2 文字)) で入力する必要があ ります。高可用性 (HA) 設定のファイアウォールの場合、トラッ プを送信したHAピアをSNMPマネージャが識別できるようにこの フィールドを空白のままにします。空白にしないと、値が同期さ れ、両方のピアで同じEnginelD[エンジンID] が使用されます。
認証パスワード	SNMP ユーザーの認証パスワードを指定します。ファイアウォー ルはこのパスワードを使用して SNMP マネージャの認証を受けま す。パスワードには、8 ~ 256 文字のあらゆる文字を使用できま す。
専用パスワード	SNMP ユーザーの専用パスワードを指定します。パスワードに は、8 ~ 256 文字のあらゆる文字を使用できます。
認証プロトコル	SNMP マネージャ パスワードの Secured Hash アルゴリズム (SHA) を選択します。SHA-1 、 SHA-224 、 SHA-256 、 SHA-384 、また は SHA-512 を選択できます。
プライバシープロトコ ル	SNMP トラップと統計要求への応答の高度暗号化標準 (AES) を選択 します。AES-128 、 AES-192 、または AES-256 を選択できます。

Device > Server Profiles > Syslog [デバイス > サーバー プロファイル > Syslog]

ファイアウォール、Panorama、およびログコレクタのログを Syslog メッセージとして Syslog サーバーに転送するためのサーバー プロファイルを設定でするには、Device(デバイス) > Server Profiles(サーバー プロファイル) > Syslog または Panorama > Server Profiles(サー バー プロファイル) > Syslog を選択します。Syslog サーバー プロファイルを定義するに は、Add(追加)をクリックして、New Syslog Server(新規 Syslog サーバー)の各フィールド を指定します。

- システム、設定、ユーザー ID、HIP マッチ、および相関ログ用の Syslog サーバー プロファイルを選択するには、「Device(デバイス) > Log Settings(ログ設 定)」を参照してください。
 - トラフィック、脅威、Wildfire、URLフィルタリング、データフィルタリング、 トンネル検査、認証、および GTP ログ用の Syslog サーバー プロファイルを選択 するには、「Objects(オブジェクト) > Log Forwarding(ログ転送)」を参照 してください。
 - ファイアウォールの、システムまたは設定ログの設定や、ログ転送プロファイル において使用されているサーバープロファイルは削除できません。

Syslog サーバーの設定	の意味
氏名	Syslog プロファイルの名前(最大 31 文字)を入力します。名前の 大文字と小文字は区別されます。また、一意の名前にする必要があ ります。文字、数字、スペース、ハイフン、およびアンダースコア のみを使用してください。
場所	プロファイルを使用できる範囲を選択します。複数の仮想シス テム (vsys) があるファイアウォールの場合、vsys を選択する か、Shared[共有] (すべての仮想システム) を選択します。その他の 場合、Location(場所)を選択することはできません。この値は Shared(共有)(ファイアウォール)または Panorama として事前 に定義されています。プロファイルを保存すると、その[場所]を変 更できなくなります。

Servers [サーバー]タブ

氏名	Add(追加)をクリックし、Syslog サーバーの名前(最大 31 文
	字)を入力します。名前の大文字と小文字は区別されます。また、
	一意の名前にする必要があります。文字、数字、スペース、ハイフ
	ン、およびアンダースコアのみを使用してください。

Syslog サーバーの設定	の意味	
SERVER	Syslog サーバーの IP アドレスまたは FQDN を入力してください	
転送	Syslog メッセージの転送方法を UDP、TCP、SSL から選択します。	
	 SSLを使用し、Syslog サーバーに送信するデータを暗号化して保護します。データはクリアテキストの状態で UDP あるいは TCP を介して送信されるため、途中で読み取ることが可能です。 	
ポート	Syslog サーバーのポート番号を入力します。UDP の標準ポートは 514、SSL の標準ポートは 6514 で、TCP の場合はポート番号を指 定する必要があります。	
format	使用するSyslog形式を指定します。BSD(デフォルト)また はIETF。	
ファシリティ	Syslog の標準値のいずれかを選択します。Syslog サーバーがfacility [ファシリティ] フィールドを使用してメッセージを管理する方法に 対応する値を選択します。Facility(ファシリティ)フィールドの 詳細は、RFC 3164(BSD フォーマット)または RFC 5424(IETF フォーマット)を参照してください。	
Custom Log Format Tab [カスタム ログ フォーマット] タブ		
ログ タイプ	ログタイプをクリックして、カスタムログ形式を指定するための ダイアログボックスを開きます。ダイアログボックスで、フィー ルドをクリックしてLog Format [ログ形式] エリアに追加します。 その他のテキスト文字列は、Log Format [ログ形式] エリアで直接 編集できます。OK をクリックして設定を保存します。カスタムロ グ 使用できる各フィールドの説明を確認してください。 カスタムログで使用できるフィールドの詳細は、「Device(デバ イス) > Server Profiles(サーバープロファイル) > Email(電子 メール)」を参照してください。	
エスケープ	エスケープ シーケンスを指定します。Escaped characters[エスケー プする文字] はスペースなしでエスケープする文字の一覧です。	

で

Device > Server Profiles > Email [デバイス > サーバー プロファイル > 電子メール]

ログを電子メール通知として転送するためには、サーバプロファイルを設定 し、Device (デバイス) > Server Profiles (サーバプロファイル) > Email (電子メール) または Panorama (パノラマ) > Server Profiles (サーバプロファイル) > Email (電子メール) を選択します。電子メール サーバー プロファイルを定義するには、プロファイルを Add (追加) し、電子メール通知設定を指定します。

- システム、設定、ユーザー ID、HIP マッチ、および相関ログ用の電子メール サーバプロファイルを選択するには、「Device(デバイス) > Log Settings(ロ グ設定)」を参照してください。
 - トラフィック、脅威、Wildfire、URLフィルタリング、データフィルタリング、 トンネル検査、認証、および GTP ログ用の電子メール サーバ プロファイルを選 択するには、「Objects(オブジェクト) > Log Forwarding(ログ転送)」を参 照してください。
 - 「Monitor(監視) > PDF Reports (PDF レポート) > Email Scheduler (電子 メール スケジューラ)」で電子メール レポートをスケジュールすることもでき ます。
 - ファイアウォールの、システムまたは設定ログの設定や、ログ転送プロファイル において使用されているサーバープロファイルは削除できません。

電子メール通知設定	の意味
氏名	サーバー プロファイルの名前を入力します(最大 31 文字)。名前 の大文字と小文字は区別されます。また、一意の名前にする必要が あります。文字、数字、スペース、ハイフン、およびアンダースコ アのみを使用してください。
場所 (仮想システムのみ)	プロファイルを使用できる範囲を選択します。複数の仮想シス テム (vsys) があるファイアウォールの場合、vsys を選択する か、Shared[共有] (すべての仮想システム) を選択します。その他の 場合、Location(場所)を選択することはできません。この値は Shared(共有)(ファイアウォール)または Panorama として事前 に定義されています。プロファイルを保存すると、その[場所]を変 更できなくなります。

電子メール通知設定	の意味
Servers [サーバー]タブ	
氏名	サーバーを識別する名前を入力します(最大 31 文字)。この フィールドは単なるラベルであり、既存の電子メールサーバーのホ スト名である必要はありません。
電子メール表示名	電子メールの From[送信者] フィールドに表示される名前を入力し ます。
送信者	送信元の電子メール アドレス(security_alert@company.com な ど)を入力します。
受信者	受信者の電子メール アドレスを入力します。
追加の受信者	別の受信者の電子メール アドレスを入力します (任意)。追加できる のは 1 名の受信者のみです。複数の受信者を追加するには、配布リ ストの電子メール アドレスを追加します。
電子メール ゲートウェ イ	電子メールを送信するサーバーの IPアドレスまたはホスト名を入力 します。
PROTOCOL	メール送信に使用するプロトコルを選択します(Unauthenticated SMTP(未認証 SMTP) または SMTP over TLS)。
ポート	デフォルト(SMTP の場合は25、TLS の場合は 587)と異なる場合、電子メール送信に使用するポート番号を入力します。
TLS バージョン	使用する TLS バージョンを選択します(1.2 または 1.1)。
(SMTP over TLS のみ)	 最新の TLS バージョンを使用することがベストプラク ティスであり、強く推奨されます。
認証方法	Authentication(認証) 方法を選択します。
(SMTP over TLS のみ)	 Auto(自動) – クライアントとサーバーが認証方法を決定する ことを許可します。
	• Login(ログイン)–ユーザー名とパスワードに Base64 エン コーディングを使用し、別々に送信します。
	• Plain(プレーン)–ユーザー名とパスワードに Base64 エンコー ディングを使用し、一緒に送信します。
証明書プロファイル (SMTP over TLS のみ)	電子メールサーバーの認証に使用するファイアウォールの証明書プ ロファイルを選択します。

電子メール通知設定	の意味
ユーザー名 (SMTP over TLS のみ)	電子メールを送信するアカウントのユーザー名を入力します。
パスワード (<mark>SMTP over TLS</mark> のみ)	電子メールを送信するアカウントのパスワードを入力します。
パスワードの確認 (<mark>SMTP over TLS のみ)</mark>	電子メールを送信するアカウントのパスワードを確認します。
接続のテスト (SMTP over TLS のみ)	電子メール サーバーとファイアウォール間の接続を確認します。

Custom Log Format Tab [カスタム ログ フォーマット] タブ

ログ タイプ	ログ タイプをクリックして、カスタム ログ形式を指定するた めのダイアログ ボックスを開きます。ダイアログ ボックスで、 フィールドをクリックしてLog Format [ログ形式] エリアに追加しま す。 OK をクリックして変更内容を保存します。
Escaping(エスケー プ)	スペースを入れずにエスケープ文字を指定し(文字通りに解釈 される文字はありません)、エスケープシーケンスにEscape Character(エスケープ文字)を指定します。

Device(デバイス) > Server Profiles(サーバー プロ ファイル) > HTTP

ログを転送するためのサーバー プロファイルを設定するには、Device(デバイス) > Server Profiles(サーバー プロファイル) > HTTP を選択するか、Panorama > Server Profiles(サー バー プロファイル) > HTTP を選択します。ファイアウォールを設定して、ログを HTTP(S) 宛先に転送したり、API を公開している任意の HTTP ベースのサービスと統合したりできるほ か、HTTP リクエストの URL、HTTP ヘッダー、パラメータ、ペイロードをニーズに合わせて変 更できます。また、HTTP サーバー プロファイルを使用して、PAN-OS が統合されている User-ID エージェントを実行しているファイアウォールにアクセスし、ファイアウォールにより生成 されたログの送信元または宛先 IP アドレスに 1 つ以上のタグを登録できます。

▲ HTTP サーバー プロファイルを使用してログを転送するための手順:

- システム、設定、ユーザー ID、HIP マッチ、および相関ログの場合は、 「Device(デバイス) > Log Settings(ログ設定)」を参照してください。
- トラフィック、脅威、Wildfire、URLフィルタリング、データフィルタリング、 トンネル検査、認証、および GTP ログの場合は、「Objects(オブジェクト)> Log Forwarding(ログ転送)」を参照してください。

HTTP サーバー プロファイルを使用してログを転送している場合、その HTTP サーバー プロファイルを削除できません。ファイアウォールまたは Panorama の サーバー プロファイルを削除するには、そのプロファイルへのすべての参照を Device (デバイス) > Log settings (ログ設定)または Objects (オブジェクト) > Log Forwarding (ログ転送)のプロファイルから削除する必要があります。

HTTP サーバー プロファイルを定義するには、新しいプロファイルを Add(追加)し、以下の 表の項目を設定します。

HTTP サーバー設定	の意味
氏名	サーバープロファイルの名前を入力します(最大 31 文字)。名前 の大文字と小文字は区別されます。また、一意の名前にする必要が あります。有効な名前はアルファベット文字で始まる必要があり ます。名前には、ゼロ、アルファベット文字、下線(_)、ハイフン (-)、ドット(.)、またはスペースを使用できます。
場所	サーバー プロファイルを使用できる範囲を選択します。複数の仮 想システム (vsys) があるファイアウォールの場合、vsys を選択す るか、Shared[共有] (すべての仮想システム) を選択します。その他 の場合、Location(場所)を選択することはできません。この値は

HTTP サーバー設定	の意味
	Shared(共有)(ファイアウォール)または Panorama として事 前に定義されています。プロファイルを保存すると、Location(場 所)を変更できなくなります。
Tag Registration(タグ 登録)	タグ登録では、ログエントリ内の送信元または宛先 IP アドレスに 対してタグを追加または削除したり、HTTP(S)を使用してファイ アウォールの User-ID エージェントにマッピングする IP アドレス とタグを登録したりできます。その後、このタグをフィルタリング 基準として使用してグループメンバーを決定する動的アドレス グ ループを定義できるほか、タグに基づいてポリシー ルールを IP ア ドレスに適用できます。
	接続の詳細を Add(追加)し、ファイアウォールの User-ID エー ジェントへの HTTP(S)アクセスを有効にします。
	Panorama の User-ID エージェントにタグを登録するのにサーバー プロファイルは不要です。また、Windows サーバーで実行されて いる User-ID エージェントに、HTTP サーバー プロファイルを使用 してタグを登録することはできません。
Servers [サーバー]タブ	
氏名	HTTP (S) サーバーを Add (追加) し、名前 (最大 31 文字) また はリモートの User-ID エージェントを入力します。有効な名前は 一意であり、アルファベット文字で始まる必要があります。名前 には、ゼロ、アルファベット文字、下線 (_)、ハイフン (-)、ドット (.)、またはスペースを使用できます。
	サーバー プロファイルには最大 4 つのサーバーを含めることがで きます。
アドレス	HTTP(S) サーバーの IP アドレスを入力します。
	タグ登録の場合は、User-ID エージェントとして設定されている ファイアウォールの IP アドレスを指定します。
PROTOCOL	いずれかのプロトコルを選択します:HTTP または HTTPS。
ポート	サーバー、またはファイアウォールにアクセスするためのポート番 号を入力します。デフォルトの HTTP ポートは 80、HTTPS ポート は 443 です。
	タグ登録の場合、ファイアウォールは HTTP または HTTPS を使用 して、User-ID エージェントとして設定されているファイアウォー ルの Web サーバーに接続します。

HTTP サーバー設定	の意味	
TLS バージョン	サーバーの SSL がサポートしている TLS バージョンを選択します。 デフォルトは 1.2 です。	
証明書プロファイル	サーバーとの TLS 接続に使用する証明書プロファイルを選択します。	
	ファイアウォールは、サーバーへの安全な接続を確立する際に、指 定された証明書プロファイルを使用してサーバー証明書を検証しま す。	
HTTP 方式	サーバーがサポートする HTTP 方式を選択します。選択できるの は、GET、PUT、POST(デフォルト)、および DELETE です。	
	User-ID エージェントの場合、GET 方式を使用します。	
username	選択した HTTP 方式を実行するためのアクセス権限を持つユーザー 名を入力します。	
	タグをファイアウォールの User-ID エージェントに登録する場合 は、スーパーユーザー ロールを持つ管理者のユーザー名である必要 があります。	
パスワード	サーバー、またはファイアウォールと認証を行うためのパスワード を入力します。	
サーバー接続のテスト	サーバーへのネットワーク接続をテストするには、サーバーと Test Server Connection(サーバー接続のテスト)を選択します。	
	このテストでは、User-ID エージェントを実行しているサーバーへ の接続はテストされません。	
Payload Format(ペイロードの形式)タブ		
ログ タイプ	HTTP 転送で使用できるログ タイプが表示されます。ログ タイプ をクリックして、カスタム ログ形式を指定するためのダイアログ ボックスを開きます。	
format	デフォルト形式、事前定義済みの形式、またはユーザーが定義した カスタム ペイロード形式のうち、ログ タイプでどの形式を使用す るかが表示されます。	
事前定義済みの形式	サービスまたはベンダーでログを送信するための形式を選択しま す。事前定義済みの形式はコンテンツ更新によってプッシュされ、 ファイアウォールまたは Panorama に新しいコンテンツ更新がイン ストールされるたびに変わる可能性があります。	

HTTP サーバー設定	の意味
氏名	カスタム ログ形式の名前を入力します。
URI の形式	HTTP(S)を使用してどのリソースにログを送信するかを指定しま す。 カスタム形式を作成する場合、URI は HTTP サービス上のリソース のエンドポイントになります。ファイアウォールは、ユーザーが事 前に定義した IP アドレスに URI を付加して、HTTP リクエストの URL を構築します。URI とペイロードの形式が、サードパーティ ベンダーが要求する構文に一致することを確認してください。選択 したログ タイプでサポートされる任意の属性を HTTP ヘッダー、 パラメータと値のペア、およびリクエスト ペイロード内で使用でき ます。
HTTP ヘッダー	ヘッダーとそれに対応する値を追加します。
パラメータ	オプションのパラメータと値が含まれます。
ペイロード	外部 Web サーバーへの HTTP メッセージにペイロードとして含め るログ属性を選択します。
テストログの送信	外部 Web サーバーがリクエストを正しいペイロード形式で受信す ることを検証するには、このボタンをクリックします。
Device(デバイス) > Server Profiles(サーバー プロ ファイル) > NetFlow

Palo Alto Networks ファイアウォールは、そのインターフェイス上の IP トラフィックに関する 統計を NetFlow フィールドとして NetFlow コレクタにエクスポートできます。NetFlow コレ クタは、セキュリティ、管理、アカウント管理、およびトラブルシューティングの目的でネッ トワーク トラフィックを分析するために使用するサーバーです。すべての Palo Alto Networks ファイアウォールで NetFlow バージョン 9 がサポートされます。このファイアウォールでは、 双方向ではなく、一方向の NetFlow のみをサポートします。ファイアウォールでは、インター フェイス上のすべての IP トラフィックに対して NetFlow 処理が実行されます。サンプリング NetFlow はサポートされていません。レイヤー 3、レイヤー 2、Virtualwire、tap、VLAN、ルー プバック、およびトンネルの各インターフェイスの NetFlow レコードをエクスポートできま す。Ethernet の集約インターフェイスでは、集約グループのレコードをエクスポートできま すが、グループ内の個々のインターフェイスのレコードをエクスポートできません。ファイア ウォールは NetFlow の標準およびエンタープライズ (PAN-OS 固有) テンプレートをサポート します。NetFlow コレクタはこのテンプレートを使用して NetFlow フィールドを解読します。 ファイアウォールは、次のエクスポートされたデータのタイプに基づいてテンプレートを選択し ます。IPv4またはIPv6トラフィック、NATを使用するかどうか、フィールドは標準のものかエン タープライズ固有のものか。

NetFlow エクスポートを設定するには、NetFlow サーバー プロファイルを Add (追加) し、 エクスポートしたデータを受け取る NetFlow サーバーと、エクスポート パラメータを指定 します。インターフェイスにプロファイルを割り当てると(「Network(ネットワーク) > Interfaces(インターフェイス)」を参照)、ファイアウォールは、そのインターフェイス上の すべてのトラフィックの NetFlow データを指定のサーバーにエクスポートします。

Netflow 設定	の意味
氏名	Netflow サーバー プロファイルの名前を入力します(最大 31 文 字)。名前の大文字と小文字は区別されます。また、一意の名前に する必要があります。文字、数字、スペース、ハイフン、およびア ンダースコアのみを使用してください。
テンプレート更新レー ト	ファイアウォールは定期的に各 Netflow テンプレートを更新して、 (エクスポートされたデータのタイプが変わった場合は) どのテン プレートを使用するかを再評価し、選択したテンプレートのフィー ルドに変更があれば適用します。NetFlow コレクタの要件に従っ て、ファイアウォールが NetFlow テンプレートを更新するレート を Minutes (分) (範囲は 1 ~ 3,600、デフォルトは 30) および Packets (パケット) (エクスポートされたレコード – 範囲は 1 ~ 600、デフォルトは 20) で指定します。どちらかのしきい値を超え ると、ファイアウォールはテンプレートを更新します。必要な更新 レートは、NetFlow コレクタに応じて異なります。サーバープロ

Netflow 設定	の意味
	ファイルに複数の NetFlow コレクタを追加する場合、更新レート が最も速いコレクタの値を使用します。
アクティブ タイムアウ ト	ファイアウォールが各セッションのデータ レコードをエクスポート する頻度(分単位)を指定します(範囲は 1 ~ 60、デフォルトは 5)。NetFlow コレクタがトラフィック統計を更新する頻度に基づ いて、頻度を設定します。
PAN-OS フィールド タ イプ	Netflow レコードの App-ID および User-ID サービスの PAN-OS 特定フィールドをエクスポートします。
Servers (サーバー)	
氏名	サーバーを識別する名前を指定します(最大 31 文字)。名前の大 文字と小文字は区別されます。また、一意の名前にする必要があり ます。文字、数字、スペース、ハイフン、およびアンダースコアの みを使用してください。
SERVER	サーバーのホスト名または IP アドレスを指定します。プロファイ ルごとに最大 2 つのサーバーを追加できます。
ポート	サーバー アクセス用のポート番号を指定します(デフォルトは 2055)。

Device > Server Profiles > RADIUS [デバイス > サーバー プロファイル > RADIUS]

認証プロファイルで参照する Remote Authentication Dial-In User Service (RADIUS) サー バーの設定を行うには、Device (デバイス) > Server Profiles (サーバー プロファイル) > RADIUSを選択するか、Panorama > Server Profiles (サーバー プロファイル) > RADIUSを 選択します (「Device (デバイス) > Authentication Profile (認証プロファイル)」を参 照)。RADIUS を使用し、(GlobalProtect ポータル、またはAuthentication Portal (認証ポー タル)経由で)ネットワーク リソースにアクセスするエンド ユーザー、およびファイアウォー ル、または Panorama でローカルに定義されている管理者を認証できるほか、RADIUS サーバー で外部で定義された管理者の認証と承認ができます。

RADIUS サーバー設定	の意味
プロファイル名	サーバー プロファイルを識別する名前を入力します(最大 31 文 字)。名前の大文字と小文字は区別されます。また、一意の名前 にする必要があります。文字、数字、スペース、ハイフン、およ びアンダースコアのみを使用してください。
場所	プロファイルを使用できる範囲を選択します。複数の仮想シス テム (vsys) があるファイアウォールの場合、vsys を選択する か、Shared[共有] (すべての仮想システム) を選択します。その他 の場合、Location(場所)を選択することはできません。この値 は Shared(共有)(ファイアウォール)または Panorama として 事前に定義されています。プロファイルを保存すると、その[場 所] を変更できなくなります。
管理者使用のみ	管理者アカウントでのみ認証にプロファイルを使用できるように 指定するには、このオプションを選択します。複数の仮想システ ムを持つファイアウォールでは、Location[場所] が Shared[共有] になっている場合にのみこのオプションが表示されます。
タイムアウト	 認証要求がタイムアウトするまでの時間を秒単位で入力します (範囲は1~120、デフォルトは3)。 RADIUS サーバープロファイルを使用してファイア ウォールを MFA サービスと統合する場合、この時 間を入力して、認証チャレンジに応答できるだけの 十分な時間をユーザーに与えます。たとえば、MFA サービスがワンタイムパスワード(OTP)を要求す る場合、ユーザーには自分のエンドポイントデバ イスで OTP を確認し、MFA ログインページに OTP を入力するまでの時間が必要です。

RADIUS サーバー設定	の意味
Authentication Protocol(認証プロトコ ル)	ファイアウォールで RADIUS サーバーへの接続を保護するために 使用する Authentication Protocol (認証プロトコル)を選択しま す。
	 PEAP-MSCHAPv2-(デフォルト) Microsoft Challenge- Handshake Authentication Protocol (MSCHAPv2) による保護 EAP (PEAP) は、暗号化されたトンネルでユーザー名とパス ワードの両方を送信することにより、PAP または CHAP に対 するセキュリティを強化します。
	 PEAP with GTC(GTC 付属の PEAP) – 暗号化されたトンネ ルで1回限りのトークンを使用するには、汎用トークン カー ド(GTC)で保護された EAP(PEAP)を選択します。
	 EAP-TTLS with PAP(PAP付属のEAP-TTLS) – 暗号化され たトンネル内のPAPのプレーンテキスト証明書を転送するに は、トンネルを通過する転送レイヤーセキュリティ(TTLS) およびPAPでEAPを選択します。
	 CHAP – RADIUS サーバーが EAP または PAP をサポートしない、またはその用途として構成しない場合、CHAP(Challenge-Handshake Authentication Protocol)を選択します。
	 PAP – RADIUS サーバーが EAP または CHAP をサポートしない、または RADIUS サーバーを CHAP 用に構成しない場合、Password Authentication Protocol (PAP)を選択します。
有効期限が切れた後に ユーザーがパスワードを 変更できるようにする	(GlobalProtect 4.1 以降の PEAP-MSCHAPv2)GlobalProtect ユーザーが期限切れのパスワードを変更できるようにするには、 このオプションを選択します。
Make Outer Identity Anonymous 外部アイデ ンティティを匿名化	(PEAP-MSCHAPv2、GTC 付属の PEAP、または PAP 付属の EAP-TTLS)このオプションはデフォルトで有効になっており、 サーバーとの認証後にファイアウォールが作成する外部トンネル でユーザーの ID を匿名化します。
	 一部の RADIUS サーバー設定では、匿名の外部 ID はサポートされていない可能性があり、オプション をクリアする必要があります。クリアすると、ユー ザー名はクリアテキストで送信されます。
証明書プロファイル	(PEAP-MSCHAPv2、GTC 付属の PEAP、または PAP 付属の EAP-TTLS) RADIUS サーバー プロファイルに関連付ける証明書 プロファイルを選択または設定します。ファイアウォールはこの Certificate Profile (証明書プロファイル) を使用して RADIUS サー バーの認証を受けます。

RADIUS サーバー設定	の意味
再試行	タイムアウト後のリトライ回数を指定します (範囲は1~5、デ フォルトは 3)。
Servers (サーバー)	適切な順序で各サーバーの情報を設定します。
	• Name[名前] – サーバーの識別に使用する名前を入力します。
	 RADIUS Server[RADIUS サーバー] – サーバーの IP アドレスまたは FQDN を入力します。
	 Secret/Confirm Secret[シークレット/再入力 シークレット] – ファイアウォールと RADIUS サーバー間の接続の検証と暗号 化に使用する鍵を入力し、確認します。
	 Port (ポート) – 認証要求に使用するサーバー ポート (範囲は 1 ~ 65,535、デフォルトは 1812) を入力します。

[Device (デバイス)] > [Server Profiles (サーバープロファ イル)] > SCP

どこで使用できますか?	何が必要ですか ?
NGFW (PAN-OS or Panorama)	□ サポートライセンス
• Panorama [™] 管理サーバー。	□ (Panorama) デバイス管理ライセンス

デバイス > サーバープロファイル > SCP またはPanorama > サーバープロファイル > RADIUS を選択して、ネットワーク経由でファイルを安全にコピーおよび転送し、コンテンツアッ プデートを NGFW に自動的にダウンロードしてインストールできるように Secure Copy Protocol (SCP) サーバーを設定します。

DHCP サーバー設定	の意味
プロファイル名	サーバー プロファイルを識別する名前を入力します(最大 31 文 字)。名前の大文字と小文字は区別されます。また、一意の名前 にする必要があります。文字、数字、スペース、ハイフン、およ びアンダースコアのみを使用してください。
SERVER	サーバーの IP アドレスまたは FQDN を入力します。
ポート	ファイル転送用のサーバーポートを入力します(範囲は 1~65,535、デフォルトは 22)。
username	SCP サーバーへのアクセスに使用するユーザー名を入力します。
パスワード パスワードの確認	SCP サーバーへのアクセスに使用されるユーザー名のパスワードを(大文字と小文字を区別して)入力し、確認します。
path	SCP サーバー上のターゲットアップロードディレクトリのパスを 入力します。
指紋	SSH ホストキーを入力して、NGFW と SCP サーバ間の接続を識 別および認証します。

Device > Server Profiles > TACACS+ [デバイス > サー バー プロファイル > TACACS+]

ファイアウォールまたは Panorama が、Terminal Access Controller Access-Control System Plus (TACACS+) サーバーにどのようにアクセスするかを定義するための設定を行う □に は、Device (デバイス) > Server Profiles (サーバー プロファイル) > TACACS+ ま たは Panorama > Server Profiles (サーバー プロファイル) > TACACS+ を選択します (「Device (デバイス) > Authentication Profile (認証プロファイル)」を参照)。TACACS + を使用し、(GlobalProtect ポータル、またはAuthentication Portal (認証ポータル) 経由 で) ネットワーク リソースにアクセスするエンド ユーザー、およびファイアウォールまたは Panorama でローカルに定義されている管理者を認証できるほか、TACACS+ サーバーで外部で 定義された管理者の認証と承認ができます。

TACACS+ サーバー設 定	の意味
プロファイル名	サーバー プロファイルを識別する名前を入力します(最大 31 文 字)。名前の大文字と小文字は区別されます。また、一意の名前に する必要があります。文字、数字、スペース、ハイフン、およびアン ダースコアのみを使用してください。
場所	プロファイルを使用できる範囲を選択します。複数の仮想シス テム (vsys) があるファイアウォールの場合、vsys を選択する か、Shared[共有] (すべての仮想システム) を選択します。その他の 場合、Location(場所)を選択することはできません。この値は Shared(共有)(ファイアウォール)または Panorama として事前に 定義されています。プロファイルを保存すると、その[場所]を変更 できなくなります。
管理者使用のみ	管理者アカウントでのみ認証にプロファイルを使用できるように指定 するには、このオプションを選択します。マルチvsysファイアウォー ルでは、Location[場所] が Shared[共有] になっている場合にのみこの オプションが表示されます。
タイムアウト	認証要求がタイムアウトするまでの時間を秒単位で入力します(範囲 は1~20、デフォルトは3)。
Authentication Protocol(認証プロ トコル)	ファイアウォールで TACACS+ サーバーへの接続を保護するために使 用する Authentication Protocol(認証プロトコル)を選択します。
	 CHAP – Challenge-Handshake Authentication Protocol (CHAP) はデフォルトのプロトコルです。PAPよりも安全なため、このプ ロトコルをお勧めします。

TACACS+ サーバー設 定	の意味
	 PAP – TACACS+ サーバーが CHAP をサポートしない、また は TACACS+ サーバーを CHAP 用に構成しない場合、Password Authentication Protocol (PAP)を選択します。
	 Auto – ファイアウォールは最初に CHAP を使用して認証を試み ます。TACACS+ サーバーが応答しない場合、ファイアウォールは PAP にフォールバックします。
すべての認証に単一 接続を使用	すべての認証で同じTCPセッションを使用する場合は、このオプショ ンを選択します。このオプションでは、認証イベントごとに個別の TCP セッションを開始および破棄するために必要な処理を回避できる ため、パフォーマンスが向上します。
Servers (サーバー)	Add[追加] をクリックして、TACACS+ サーバーごとに以下の設定を 指定します。
	 Name[名前] - サーバーの識別に使用する名前を入力します。 TACACS+ Server[TACACS+ サーバー] – TACACS+ サーバーの IP アドレスまたは FQDN を入力します。
	 Secret/Confirm Secret[シークレット/再入力 シークレット] – ファ イアウォールとTACACS+サーバー間の接続の検証と暗号化に使用 する鍵を入力し、確認します。
	• Port[ポート] – 認証要求に使用するサーバーのポート (デフォルト は 49) を入力します。

Device > Server Profiles > LDAP [デバイス > サーバー プロファイル > LDAP]

- デバイス > サーバー プロファイル > LDAP
- **Panorama >** サーバー プロファイル > **LDAP**

認証プロファイルで参照する Lightweight Directory Access Protocol(LDAP)サーバーの設定を 行うごには、LDAP サーバープロファイルをAdd (追加)あるいは選択しますDevice (デバイス) > Authentication Profile (認証プロファイル)」を参照)。LDAP を使用し、(GlobalProtect ポータ ル、またはAuthentication Portal(認証ポータル)経由で)ネットワーク リソースにアクセスす るエンド ユーザー、およびファイアウォール、または Panorama でローカルに定義されている 管理者を認証できます。

LDAP サーバー設定	の意味
プロファイル名	プロファイルの識別に使用する名前を入力します (最大 31 文字)。名 前の大文字と小文字は区別されます。また、一意の名前にする必要が あります。文字、数字、スペース、ハイフン、およびアンダースコア のみを使用してください。
場所	プロファイルを使用できる範囲を選択します。複数の仮想シス テム (vsys) があるファイアウォールの場合、vsys を選択する か、Shared[共有] (すべての仮想システム) を選択します。その他の 場合、Location(場所)を選択することはできません。この値は Shared(共有)(ファイアウォール)または Panorama として事前に 定義されています。プロファイルを保存すると、その[場所]を変更 できなくなります。
管理者使用のみ	管理者アカウントでのみ認証にプロファイルを使用できるように指定 するには、このオプションを選択します。複数の仮想システムを持つ ファイアウォールでは、Location[場所] が Shared[共有] になっている 場合にのみこのオプションが表示されます。
Server List(サー バーリスト)	LDAP サーバーごとにホストの Name (名前)、IP アドレスまたは FQDN (LDAP Server (LDAP サーバー))、および Port (ポート) (デフォ ルトは 389) をAdd (追加) します。
タイプ	ドロップダウンリストからサーバータイプを選択します。
ベースDN	ユーザーまたはグループ情報の検索を絞り込むための、ディレクトリ サーバーのルート コンテクストを指定します。

LDAP サーバー設定	の意味
バインド DN	ディレクトリ サーバーのログイン名 (識別名)を指定します。
	バインド DN アカウントには、LDAP ディレクトリを参照する権限が必要です。
パスワード/再入力 パスワード	バインド アカウントのパスワードを指定します。エージェントは暗 号化したパスワードを設定ファイルに保存します。
バインドのタイムア ウト	ディレクトリ サーバーに接続するときの時間制限(秒)を指定しま す(範囲は1~30、デフォルトは30)。
検索のタイムアウト	ディレクトリ検索を実行するときの時間制限(秒)を指定します(範 囲は 1 ~ 30、デフォルトは 30)。
再試行間隔	システムが LDAP サーバーへの接続試行に失敗してから次に接続を試みるまでの間隔を秒単位で指定します(範囲は 1 ~ 3600、デフォルトは 60)。
SSL/TLS で保護され た接続を要求	ファイアウォールで SSL または TLS を使用してディレクトリサー バーと通信する場合は、このオプションを選択します。プロトコル は、サーバー ポートによって異なります。
	 389(デフォルト) – TLS(具体的には、ファイアウォールは、最初のプレーンテキスト接続を TLS にアップグレードする StartTLS 操作を使用します)
	• 636 – SSL
	 その他の任意のポート – ファイアウォールはまずTLSの使用しようと試みます。ディレクトリ サーバーで TLS がサポートされていない場合は、SSL にフォールバックします。
	セキュリティが向上するためこのオプションを使用することがベストプラクティスであり、デフォルトの状態で選択されています。
SSL セッションの サーバー証明書の確 認	SSL/TLS 接続のためにディレクトリ サーバーから提供される証明書 をファイアウォールで検証する場合は、このオプションを選択します (デフォルトではオフ)。証明書のについて、ファイアウォールは以 下の2点を検証します。
	 証明書が信頼されていて有効であること。ファイアウォールで証明書を信頼するには、そのルート認証局(CA)とすべての中間証明書が Device(デバイス) > Certificate Management(証明書の管理) > Certificates(証明書) > Device Certificates(デバイス証明書)の下にある証明書ストアに含まれている必要があります。

LDAP サーバー設定	の意味
	 証明書名は LDAP サーバーのホストの Name[名前] と一致していなければなりません。ファイアウォールは、まず証明書の「サブジェクト代替名」属性が一致しているかどうかをチェックし、次に「サブジェクト DN」属性を試行します。証明書でディレクトリサーバーの FQDN が使用されている場合、LDAP Server[LDAPサーバー] フィールドに FQDN を使用しないと、名前の照合に失敗します。
	検証に失敗すると、接続できません。この検証を有効にする場合 は、Require SSL/TLS secured connection[SSL/TLSで保護された接続 を要求] を選択する必要があります。
	 ファイアウォールが SSL セッションのサーバー証明書 を検証できるようにし、セキュリティを向上させます。

Device > Server Profiles > Kerberos [デバイス > サー バー プロファイル > Kerberos]

ユーザーが Active Directory ドメインコントローラまたは Kerberos V5 準拠の認証サーバー とネイティブに認証できるようにサーバー プロファイルを設定 ■するには、Device(デバイ ス) > Server Profiles(サーバー プロファイル) > Kerberos を選択するか、Panorama > Server Profiles(サーバー プロファイル) > Kerberosを選択します。Kerberos サーバー プロファイ ルを設定したら、そのサーバー プロファイルを認証プロファイルに割り当てることができます (「Device(デバイス) > Authentication Profile(認証プロファイル)」を参照)。Kerberos を使用し、(GlobalProtect ポータル、またはAuthentication Portal(認証ポータル)経由で) ネットワーク リソースにアクセスするエンド ユーザー、およびファイアウォール、または Panorama でローカルに定義されている管理者を認証できます。

4	

Kerberos 認証を使用するには、IPv4 アドレスでバックエンド Kerberos サーバーにア クセスできる必要があります。IPv6 アドレスはサポートされません。

Kerberos サーバー設 定	の意味
プロファイル名	サーバーを識別する名前を入力します(最大 31 文字)。名前の大文 字と小文字は区別されます。また、一意の名前にする必要がありま す。文字、数字、スペース、ハイフン、およびアンダースコアのみを 使用してください。
場所	プロファイルを使用できる範囲を選択します。複数の仮想シス テム (vsys) があるファイアウォールの場合、vsys を選択する か、Shared[共有] (すべての仮想システム) を選択します。その他の 場合、Location(場所)を選択することはできません。この値は Shared(共有)(ファイアウォール)または Panorama として事前に 定義されています。プロファイルを保存すると、その [場所] を変更 できなくなります。
管理者使用のみ	管理者アカウントでのみ認証にプロファイルを使用できるように指定 するには、このオプションを選択します。複数の仮想システムを持つ ファイアウォールでは、Location[場所] が Shared[共有] になっている 場合にのみこのオプションが表示されます。
Servers (サーバー)	Kerberos サーバーごとに、Add[追加] をクリックして以下の設定を指定します。
	• Name[名前] – サーバーの名前を入力します。
	 Kerberos Server[Kerberos サーバー] – サーバーの IPv4 アドレス または FQDN を入力します。

Kerberos サーバー設 定	の意味
	 Port(ポート) – サーバーと通信するためのポート(範囲は1~ 65,535、デフォルトは88)を入力します(任意)。

Device(デバイス) > Server Profiles(サーバー プロ ファイル) > SAML Identity Provider(SAML アイデン ティティ プロバイダ)

このページを使用して、Security Assertion Markup Language(SAML)2.0 アイデンティティプ ロバイダ(IdP)をファイアウォールまたは Panorama に登録します。ネットワーク リソースへ のアクセスを制御する SAML サービス プロバイダとしてファイアウォールまたは Panorama が 機能できるようにするには、登録の手順が必要です。管理者およびエンド ユーザーがリソース を要求すると、サービス プロバイダは認証のためにユーザーを IdP にリダイレクトします。エ ンド ユーザーは、GlobalProtect またはAuthentication Portal(認証ポータル)ユーザーになる ことができます。管理者をファイアウォールおよび Panorama でローカルで管理できます。ま た、IdP アイデンティティ ストアで外部で管理することもできます。各ユーザーが 1 つのリソー スにログインした後で複数のリソースに自動的にアクセスできるように、SAML シングル サイ ンオン(SSO)を設定できます。また、SAML シングル ログアウト(SLO)を設定することもで きます。これを使用すると、各ユーザーは、いずれか 1 つのサービスからログアウトすること で、SSO 対応のすべてのサービスから同時にログアウトできます。

認証シーケンスでは、SAML IdP サーバー プロファイルを指定する認証プロファイ ルがサポートされません。

ほとんどの場合、SSO を使用して同じモバイル デバイス上の複数のアプリケーションにアクセスできません。

Authentication Portal (認証ポータル) ユーザーに対しては、SLO を有効化できません。

SAML IdP サーバー プロファイルを作成する最も簡単な方法は、登録情報が含まれるメタデー タファイルを IdP から Import (インポート) することです。インポートした値と共にサーバー プロファイルを保存したら、プロファイルを編集して値を変更できます。IdP からメタデー タファイルが提供されない場合は、サーバー プロファイルを Add (追加) して、情報を手動 で入力できます。サーバー プロファイルを作成したら、そのサーバー プロファイルを特定の ファイアウォールまたは Panorama サービスの認証プロファイルに割り当てることができます (「Device (デバイス) > Authentication Profile (認証プロファイル)」を参照)。

SAML アイデンティ ティ プロバイダ サー バー設定	の意味
プロファイル名	サーバーを識別する名前を入力します(最大 31 文字)。名前の大文 字と小文字は区別されます。また、一意の名前にする必要がありま す。文字、数字、スペース、ハイフン、およびアンダースコアのみを 使用してください。

SAML アイデンティ ティ プロバイダ サー バー設定	の意味
場所	プロファイルを使用できる範囲を選択します。複数の仮想シス テムがあるファイアウォールの場合、仮想システムを選択する か、Shared(共有)(すべての仮想システム)を選択します。その 他の場合、Location(場所)を選択することはできません。この値は Shared(共有)(ファイアウォール)または Panorama として事前に 定義されています。プロファイルを保存すると、その [場所] を変更 できなくなります。
管理者使用のみ	管理者アカウントでのみ認証にプロファイルを使用できるように指定 するには、このオプションを選択します。複数の仮想システムを持つ ファイアウォールでは、Location[場所] が Shared[共有] になっている 場合にのみこのオプションが表示されます。
アイデンティティ プ ロバイダ ID	ldP の識別子を入力します。この情報は ldP が提供します。
アイデンティティ プ ロバイダ証明書	ファイアウォールに送信する SAML メッセージに IdP が署名するた めに使用する証明書を選択します。IdP がファイアウォールに送信 するメッセージの整合性を確保するには、IdP 証明書を選択する必 要があります。認証局 (CA) の発行に対して IdP 証明書を検証するに は、IdP サーバー プロファイルを参照するいずれかの認証プロファイ ルで Certificate Profile (証明書プロファイル)を指定する必要がありま す (「Device (デバイス) > Authentication Profile (認証プロファイル)」 を参照)。
	証明書とそれに関連付けられる秘密鍵を生成、またはインポート する場合、証明書に指定されたキーの使用属性によってキーの使 用目的が制御されることに注意してください。証明書で鍵の用途 の属性が明示的にリストされている場合、属性の1つはデジタル 署名です。デジタル署名はファイアウォールで生成する証明書で は使用できません。このような場合は、エンタープライズ認証局 (CA)、またはサードパーティ CA から証明書と鍵をインポートす る必要があります。証明書で鍵の用途の属性が指定されていない 場合は、メッセージの署名も含めて、どのような目的にも鍵を使 用できます。このような場合は、任意の方法で証明書と鍵を取得
	して SAML メッセージに署名できます。
	ldP 証明書では、以下のアルゴリズムがサポートされます。
	 公開鍵アルゴリズム – RSA(1,024 ビット以上)および ECDSA(すべてのサイズ)。FIPS/CC モードのファイアウォー ルでは、RSA(2,048ビット以上)および ECDSA(すべてのサイ ズ)がサポートされます。

SAML アイデンティ ティ プロバイダ サー バー設定	の意味
	 シグネチャアルゴリズム – SHA1、SHA256、SHA384、 および SHA512。FIPS/CC モードのファイアウォールで は、SHA256、SHA384、および SHA512 がサポートされます。
アイデンティティ プ ロバイダ SSO URL	IdP から通知されたシングル サインオン(SSO)サービス用の URL を入力します。 メタデータ ファイルをインポートしてサーバー プロファイルを作成 する場合、そのファイルに複数の SSO URL が指定されていると、
	ファイアウォールは、POST またはリダイレクト バインド方式を指定 している最初の URL を使用します。
	する URL を使用することを強くお勧めします。
アイデンティティ プ ロバイダ SLO URL	ldP から通知されたシングル ログアウト(SLO)サービス用の URL を入力します。
	メタデータ ファイルをインポートしてサーバー プロファイルを作 成する場合、そのファイルに複数の SLO URL が指定されていると、 ファイアウォールは、POST またはリダイレクト バインド方式を指定 している最初の URL を使用します。
	SAML では HTTP もサポートされますが、HTTPS を使用 する URL を使用することを強くお勧めします。
SSO SAML HTTP バ インディング	Identity Provider SSO URL(アイデンティティ プロバイダ SSO URL) に関連付けられている HTTP バインディングを選択します。 ファイアウォールはバインドを使用して SAML メッセージを IdP に送 信します。オプションは次のとおりです:
	• POST – ファイアウォールは base64 エンコード済みの HTML 形 式を使用してメッセージを送信します。
	 Redirect(リダイレクト) – ファイアウォールは、base64 エン コード済みおよび URL エンコード済みの SSO メッセージを URL パラメータ内で送信します。
	複数の SSO URL を持つ IdP メタデータ ファイルをイン ポートした場合、ファイアウォールは、POST またはリ ダイレクト方式を使用する最初の URL のバインドを使 用します。ファイアウォールは、他のバインドを使用 する URL を無視します。

SAML アイデンティ ティ プロバイダ サー バー設定	の意味
SLO SAML HTTP バ インディング	Identity Provider SLO URL(アイデンティティ プロバイダ SLO URL)に関連付けられている HTTP バインディングを選択します。 ファイアウォールはバインドを使用して SAML メッセージを IdP に送 信します。オプションは次のとおりです:
	• POST – ファイアウォールは base64 エンコード済みの HTML 形 式を使用してメッセージを送信します。
	 Redirect(リダイレクト) – ファイアウォールは、base64 エン コード済みおよび URL エンコード済みの SSO メッセージを URL パラメータ内で送信します。
	
アイデンティティ プ ロバイダ メタデータ	このフィールドは、IdP からファイアウォールにアップロードした IdP メタデータ ファイルを Import (インポート) した場合にのみ表示されます。このファイルでは、新しい SAML IdP サーバー プロファイルの値と署名証明書を指定します。ファイルをBrowse (参照) し、Profile Name (プロファイル名) と Maximum Clock Skew (最大クロックスキュー)を指定して、OK をクリックすると、プロファイルが作成されます。必要に応じて、プロファイルを編集し、インポートされた値を変更できます。
アイデンティティ プ ロバイダ証明書の検	信頼チェーンを検証し、オプションで ldP 署名証明書の失効ステータ スを検証するには、このオプションを選択します。
託	このオプションを有効にするために、認証局 (CA) が IdP の署名証明 書を発行する必要があります。IdP の署名証明書を発行した CA を含 む証明書プロファイルを作成する必要があります。認証プロファイル で、IdP 証明書を検証するための SAML サーバ プロファイルおよび証 明書プロファイルを選択します (「Device (デバイス) > Authentication Profile (認証プロファイル)」を参照)。
	IdP 署名証明書が自己署名証明書である場合、信頼チェーンはあり ません。その場合は、このオプションを有効にすることはできませ ん。ファイアウォールは Validate Identity Provider Certificate (アイ デンティティ プロバイダ証明書の検証) オプションを有効にするか どうかに関係なく、設定するアイデンティティプロバイダ証明書に 対して SAML 応答またはアサーションのシグネチャを常に検証しま

SAML アイデンティ ティ プロバイダ サー バー設定	の意味
	す。ldP が自己署名証明書を提供する場合は、PAN-OS 11.1 を使用し て CVE-2020-2021 への影響を軽減していることを確認します。
IdP への SAML メッ セージの署名	IdP に送信するメッセージをファイアウォールで署名することを指定 するには、このオプションを選択します。ファイアウォールでは、 認証プロファイルで指定した Certificate for Signing Requests(署 名要求の証明書)が使用されます(「Device(デバイス) > Authentication Profile(認証プロファイル)」を参照)。 ② 署名証明書を使用することで、IdP に送信するメッセー ジの整合性が確保されます。
最大クロック ス キュー	ファイアウォールが IdP から受信したメッセージを検証する時点 で、IdP とファイアウォールのシステム時間に対して許容される最 大時間差を秒単位で入力します(範囲は 1 ~ 900、デフォルトは 60)。時間差がこの値を超える場合、検証(つまり、認証)は失敗 します。

Device > Server Profiles > DNS [デバイス > サーバー プ ロファイル > DNS]

仮想システムの設定を簡略化するために、DNSサーバープロファイルでは、設定されている 仮想システム、DNSサーバーの継承ソースまたはプライマリ/セカンダリDNSアドレス、およ びDNSサーバーに送信されるパケットで使用する送信元インターフェイスと送信元アドレス (サービスルート)を指定できます。送信元インターフェイスと送信元アドレスは、DNSサー バーからの応答の宛先インターフェイスと宛先アドレスとして使用されます。

DNS サーバー プロファイルは仮想システム専用で、グローバルな共有の場所では使用できません。

DNS サーバー プロファ イル設定	の意味
氏名	DNS サーバー プロファイルの名前を付けます。
場所	プロファイルを適用する仮想システムを選択します。
継承ソース	DNS サーバーのアドレスを継承しない場合、None[なし] を選択します。継承する場合は、プロファイルが設定を継承する DNS サーバーを指定します。
継承ソース状態の チェック	継承ソースの情報を確認する場合にクリックします。
プライマリ DNS	プライマリDNSサーバーのIPアドレスを指定します。
セカンダリ DNS	セカンダリDNSサーバーのIPアドレスを指定します。
サービスルートIPv4	DNSサーバーに送信されるパケットの送信元がIPv4になるように 指定する場合、このオプションを選択します。
送信元インターフェイ ス	DNS サーバーに送信されるパケットで使用する送信元インター フェイスを指定します。
送信元アドレス	DNS サーバーに送信されるパケットの IPv4 送信元アドレスを指定します。
サービスルートIPv6	DNSサーバーに送信されるパケットの送信元がIPv6になるように 指定する場合、このオプションを選択します。
送信元インターフェイ ス	DNS サーバーに送信されるパケットで使用する送信元インター フェイスを指定します。

DNS サーバー プロファ イル設定	の意味
送信元アドレス	DNS サーバーに送信されるパケットの IPv6 [送信元アドレス] を指 定します。

Device (デバイス) > Server Profiles (サーバー プロ ファイル) > Multi Factor Authentication (多要素認 証)

このページを使用して、多重認証(MFA)サーバープロファイルを設定し、ファイアウォール を MFA サーバーにどのように接続するかを定義します。MFA では、最高機密のリソースを保 護できす。この方法では、攻撃者は単一認証要素を侵害して(たとえば、ログイン認証情報を 盗んで)ネットワークにアクセスし、ネットワークを横断することはできません。サーバープ ロファイルを設定したら、認証を要求するサービスの認証プロファイルにサーバープロファイ ルを割り当てます(「Device(デバイス) > Authentication Profile(認証プロファイル)」を参 照)。

次の認証ユースケースでは、firewall は RADIUS および SAML を使用して多要素認証 (MFA) ベンダーと統合されます:

- GlobalProtect[™] ポータルおよびゲートウェイを介したリモートユーザー認証。
- PAN-OS および Panorama[™] Web インターフェイスでの 管理者認証。
- 認証ポリシーによる認証。

さらに、ファイアウォールは API を使用して MFA vendors(MFA ベンダー)と統合して、エン ドユーザ認証のみ(GlobalProtect 認証または管理者認証ではない)の認証ポリシーによる MFA の適用も可能です。

MFAを設定するための完全な手順口では、サーバープロファイルの作成に加えて追加のタスクが必要です。

認証シーケンスでは、MFA サーバー プロファイルを指定する認証プロファイルが サポートされません。

ファイアウォールが RADIUS を介して MFA ベンダーと統合している場 合、RADIUS サーバー プロファイルを設定します(「Device(デバイス) > Server Profiles(サーバー プロファイル) > RADIUS」を参照)。ファイアウォールは RADIUS を介してあらゆる MFA ベンダーをサポートします。

MFA サーバー設定	の意味
プロファイル名	サーバーを識別する名前を入力します(最大 31 文字)。名前の大文 字と小文字は区別されます。また、一意の名前にする必要がありま す。文字、数字、スペース、ハイフン、およびアンダースコアのみを 使用してください。

MFA サーバー設定	の意味
場所	複数の仮想システム(vsys)があるファイアウォールでは、vsys ま たは Shared(共有)の場所を選択します。プロファイルを保存する と、その Location(場所)を変更できなくなります。
証明書プロファイル	サーバーへの安全な接続をセットアップするときにファイアウォール で MFA サーバー証明書を検証するために使用する認証局(CA)証明 書を指定する Certificate Profile(証明書プロファイル)を選択しま す。詳細は、「Device(デバイス) > Certificate Management(証明 書の管理) > Certificate Profile(証明書プロファイル)」を参照して ください。
MFA ベンダー/値	MFA ベンダーの MFA Vendor(MFA ベンダー)を選択し、ベンダー 属性ごとに Value(値)を入力します。属性はベンダーによって異な ります。正しい値については、ベンダーのドキュメントを参照してく ださい。
	• Duo v2:
	 API Host(API ホスト) – Duo v2 サーバーのホスト名。
	 Integration Key(統合キー)および Secret Key(シークレット キー) - ファイアウォールはこれらのキーを使用して Duo v2 サーバーとの認証を行い、サーバーに送信する認証要求に署名 します。これらのキーを保護するため、ファイアウォール上の マスター キーによってこれらのキーが自動的に暗号化されま す。これにより、これらのキーのプレーンテキスト値はファイ アウォール ストレージのどの場所にも表示されなくなります。 キーを取得するには、Duo v2 管理者に問い合わせてください。
	 Timeout(タイムアウト) – API Host(API ホスト)との通信 を試みているときにファイアウォールがタイムアウトするまで の時間を秒単位で入力します(範囲は 5 ~ 600、デフォルトは 30)。この間隔は、API ホストとユーザーのエンドポイント デ バイスとの間のタイムアウトよりも長くする必要があります。
	 Base URI (ベース URI) – 組織が Duo v2 サーバー用のローカルの認証プロキシ サーバーをホストしている場合、そのプロキシ サーバーの URI (デフォルトは /auth/v2) を入力します。
	Okta Adaptive:
	• API Host(API ホスト) – Okta サーバーのホスト名。
	 Base URI(ベース URI) – 組織が Okta サーバー用のローカルの認証プロキシ サーバーをホストしている場合、そのプロキシサーバーの URI(デフォルトは /api/v1)を入力します。
	 Token(トークン) – ファイアウォールはこのトークンを使用 して Okta サーバーとの認証を行い、サーバーに送信する認証 要求に署名します。トークンを保護するため、ファイアウォー

MFA サーバー設定	の意味
	 ル上のマスター キーによってトークンが自動的に暗号化されます。これにより、トークンのプレーンテキスト値はファイアウォール ストレージのどの場所にも表示されなくなります。トークンを取得するには、Okta 管理者に問い合わせてください。 Organization(組織) – API Host (API ホスト)内の組織のサ
	 ブドメイン。 Timeout(タイムアウト) – API Host(API ホスト)との通信 を試みているときにファイアウォールがタイムアウトするまで の時間を秒単位で入力します(範囲は 5 ~ 600、デフォルトは 30)。この間隔は、API ホストとユーザーのエンドポイント デ バイスとの間のタイムアウトよりも長くする必要があります。
	PingID:
	 Base URI (ベース URI) – 組織が PingID サーバー用のローカルの認証プロキシ サーバーをホストしている場合、そのプロキシ サーバーの URI (デフォルトは /pingid/rest/4) を入力します。
	 Host name (ホスト名) – PingID サーバーのホスト名を入力し ます(デフォルトは idpxnyl3m.pingidentity.com)。
	 Use Base64 Key (Base64 キーを使用)および Token (トー クン) – ファイアウォールはこのキーとトークンを使用して PinglD サーバーとの認証を行い、サーバーに送信する認証要求 に署名します。このキーとトークンを保護するため、ファイア ウォール上のマスター キーによってこのキーとトークンが自 動的に暗号化されます。これにより、このキーとトークンのプ レーンテキスト値はファイアウォール ストレージのどの場所に も表示されなくなります。値を取得するには、PinglD 管理者に 問い合わせてください。
	 PingID Client Organization ID (PingID クライアント組織 ID) – 組織の PingID 識別子。
	 Timeout(タイムアウト) – Host name(ホスト名)で指定 された PinglD サーバーとの通信を試みているときにファイア ウォールがタイムアウトするまでの時間を秒単位で入力します (範囲は 5 ~ 600、デフォルトは 30)。この間隔は、PinglD サーバーとユーザーのエンドポイント デバイスとの間のタイム アウトよりも長くする必要があります。

Device > Local User Database > Users [デバイス > ロー カル ユーザー データベース > ユーザー]

ファイアウォールの管理者 (Authentication Portal (認証ポータル)のエンドユーザー 、および GlobalProtect ポータル と GlobalProtect ゲートウェイ への認証を行うエンドユーザーの認証情報をファイアウォールのローカル データベースに保管するようにセットアップできます。ローカル データベース認証では、外部の認証サービスは不要です。すべてのアカウント管理をファイアウォールで実行します。ローカル データベースを作成し、(オプションで)ユーザーをグループに割り当て(「Device(デバイス) > Local User Database(ローカル ユーザーデータベース) > User Groups(ユーザー グループ)」を参照)た後、ローカル データベースに基づいて Device(デバイス) > Authentication Profile(認証プロファイル)を設定できます。

ローカル ユーザーをデータベースに Add (追加) するには、以下の表の説明に従って設定を行います。

Local User Setting(ローカル ユーザー設定)	の意味
氏名	ユーザーを識別する名前を入力します(最大 31 文字)。名前は大文 字と小文字を区別せず、一意である必要があります。文字、数字、ス ペース、ハイフン、およびアンダースコアのみを使用してください。
場所	ユーザーアカウントを使用できる範囲を選択します。複数の仮想 システム (vsys) があるファイアウォールの場合、vsys を選択する か、Shared[共有] (すべての仮想システム) を選択します。その他の 場合、Location(場所)を選択することはできません。この値は Shared(共有)(ファイアウォール)または Panorama として事前に 定義されています。ユーザーアカウントを保存すると、その[場所] を変更できなくなります。
モード	 以下のいずれかの認証オプションを指定します。 Password[パスワード] – ユーザーのパスワードを入力および確認します。 Password Hash[パスワード ハッシュ] – ハッシュされたパスワード文字列を入力します。これは、たとえば、既存の UNIX アカウントの認証情報を再利用するときに、プレーンテキストのパスワードがわからず、ハッシュされたパスワードのみを把握している場合に便利です。ファイアウォールは、ハッシュ値の生成に

ローカルデータベース認証を使用する管理者アカウントに対して、Device(デバイス) > Password Profiles (パスワードプロファイル)を設定することはできません。

Local User Setting(ローカル ユーザー設定)	の意味
	使用するアルゴリズムに関係なく、最大 63 文字の任意の文字列 を受け入れます。運用 CLI コマンド request password-hash password は、通常モードと CC/FIPS モードで SHA256 アルゴ リズムを使用します。
	 ファイアウォールに設定した Minimum Password Complexity (パスワード複雑性設定) パラメータ (Device (デバイス) > Setup (セットアップ) > Management (管理))は、Password Hash (パスワー ドハッシュ)を使用するアカウントに適用されませ ん。
Enable [有効化]	ユーザーアカウントをアクティベートする場合は、このオプションを 選択します。

Device > Local User Database > User Groups [デバイス > ローカル ユーザー データベース > ユーザー グループ]

ユーザー グループ情報をローカル データベースに追加するには、Device(デバイス) > Local User Database(ローカル ユーザー データベース) > User Groups(ユーザー グループ)を選択 します。

ローカル ユーザー グルー プ設定	の意味
氏名	グループを識別する名前を入力します(最大 31 文字)。名前 は大文字と小文字を区別せず、一意である必要があります。文 字、数字、スペース、ハイフン、およびアンダースコアのみを 使用してください。
場所	ユーザー グループを使用できる範囲を選択します。複数の仮想 システム (vsys) があるファイアウォールの場合、vsys を選択す るか、Shared[共有] (すべての仮想システム) を選択します。その 他の場合、Location(場所)を選択することはできません。こ の値は Shared(共有)(ファイアウォール)または Panorama として事前に定義されています。ユーザー グループを保存する と、その [場所] を変更できなくなります。
すべてのローカル ユー ザー	Add[追加] をクリックし、グループに追加するユーザーを選択します。

Device > Scheduled Log Export [デバイス > スケジュー ル設定されたログのエクスポート]

ログのエクスポートをスケジューリングロしてログを FTP (File Transfer Protocol: ファイル転送 プロトコル)サーバーに CSV 形式で保存したり、SCP (Secure Copy: セキュア コピー)を使用 してファイアウォールとリモート ホスト間でデータを安全に転送したりできます。ログのプロ ファイルには、スケジュールと FTP サーバーの情報が含まれています。たとえば、プロファイ ルを使用して、毎日 3:00 AM に前日のログを収集して特定の FTP サーバーに保存するように指 定できます。

スケジュール設定され たログのエクスポート 設定	の意味
氏名	プロファイルの識別に使用する名前を入力します(最大 31 文字)。名 前の大文字と小文字は区別されます。また、一意の名前にする必要が あります。文字、数字、スペース、ハイフン、およびアンダースコア のみを使用してください。 プロファイルを作成した後でこの名前を変更することはできません。
の意味	説明 (最大 255 文字) を入力します (任意)。
Enable [有効化]	ログのエクスポートのスケジューリングを有効にする場合は、このオ プションを選択します。
ログ タイプ	ログタイプを選択します(traffic(トラフィッ ク)、threat(脅威)、gtp、sctp、tunnel(トンネ ル)、userid、auth、url、data(データ)、hipmatch、また はwildfire)。デフォルトはtrafficです。
エクスポートの開始 予定時刻(毎日)	エクスポートを開始する時刻(hh:mm)を 24 時間形式(00:00 ~ 23:59)で入力します。
PROTOCOL	ファイアウォールからリモート ホストへのログのエクスポートに使 用するプロトコルを選択します。 • FTP – このプロトコルは安全ではありません。
	 SCP – このプロトコルは安全です。残りのフィールドを入力したら、Test SCP server connection (SCPサーバー接続のテスト)をクリックして、ファイアウォールと SCP サーバー間の接続テストを行い、SCP サーバーのホスト キーを検証して受け入れる必要があります。

Add[追加]をクリックし、以下の詳細を入力します。

スケジュール設定され たログのエクスポート 設定	の意味
ホスト名	エクスポートに使用する FTP サーバーのホスト名または IP アドレス を入力します。
ポート	FTP サーバーで使用するポート番号を入力します。デフォルトは 21 です。
path	エクスポートした情報の保存に使用する FTP サーバー上のパスを指 定します。
FTP パッシブモード の有効化	エクスポートにパッシブモードを使用する場合は、このオプションを 選択します。デフォルトでは、このオプションはオンになっていま す。
username	FTP サーバーへのアクセスに使用するユーザー名を入力します。デ フォルトはanonymousです。
パスワード/再入力 パスワード	FTP サーバーへのアクセスに使用するパスワードを入力します。ユー ザーが anonymous の場合、パスワードは必要ありません。
SCP サーバー接続の テスト (SCP プロトコルの み)	 Protocol を SCP に設定した場合は、このボタンをクリックしてファ イアウォールと SCP サーバー間の接続をテストする必要がありま す。ポップアップ ウィンドウが表示され、SCP サーバのクリア テキ スト Password を入力してから Confirm Password を入力するように 要求されます。 Panorama テンプレートを使用してログのエクスポー トスケジュールを設定する場合、テンプレート設定 をファイアウォールにコミットした後にこの手順を実 行する必要があります。テンプレートのコミットが完 了したら、各ファイアウォールにログインし、ログの エクスポートスケジュールを開いて、Test SCP server connection (SCP サーバー接続のテスト)をクリックし

Device > Software [デバイス > ソフトウェア]

使用可能なソフトウェア リリースの表示、リリースのダウンロードまたはアップロード、 リリースのインストール(サポート ライセンスが必要)、ファイアウォールからのソフト ウェア イメージの削除、またはリリース ノートの表示を行う場合は **Device**(デバイス) > **Software**(ソフトウェア)を選択します。

ソフトウェアのバージョンをアップグレードまたはダウンロードする前に以下を確認してくださ い。

- 現在のRelease Notes(リリースノート)を参照し、新機能の説明とリリースのデフォルト動作の変更を表示し、ソフトウェアをアップグレードするための移行パスを表示する。
- アップグレードとダウングレードに関する考慮事項とアップグレード手順については、PAN-OS[®] 11.1 New Features Guide を参照してください。
- ファイアウォールの日時設定が現在の日時になっている。PAN-OSソフトウェアはデジタル 署名されており、ファイアウォールは新バージョンをインストールする前に署名を確認し ます。ファイアウォールに現在以外の日付が設定されていると、ファイアウォールはソフト ウェア署名の日付が誤って未来になっていると認識し、以下のメッセージを表示します。

Decrypt failed:GnuPG edit non-zero, with code 171072 Failed to load into PAN software manager.

ソフトウェア オプショ ン フィールド	の意味
バージョン	Palo Alto Networks 更新サーバーで現在入手可能なソフトウェ アバージョンが一覧表示されます。Palo Alto Networks から新 しいソフトウェア リリースを入手可能かどうかをチェックする には、Check Now[今すぐチェック] をクリックします。ファイア ウォールがサービス ルートを使用して更新サーバーに接続し、新し いバージョンをチェックします。適用可能な更新がある場合は、そ の更新がリストの最上部に表示されます。
サイズ	ソフトウェア イメージのサイズを示します。
リリース日	Palo Alto Networks がリリースを公開した日時を示します。
使用可能	対応するバージョンのソフトウェア イメージがファイアウォールに アップロードまたはダウンロードされていることを示します。
現在インストール済み	対応するバージョンのソフトウェア イメージがアクティベーション されていて、ファイアウォールで現在実行されているかどうかを示 します。

以下の表に、Software[ソフトウェア]ページの使用方法を示します。

ソフトウェア オプショ ン フィールド	の意味
操作	対応するソフトウェア イメージで現在実行可能な以下のようなアク ションを示します。
	 Validate – 対応するソフトウェア バージョンが Palo Alto Networks Update Server で入手可能です。Download をクリッ クして、利用可能なソフトウェア バージョンと、更新サーバー または SCP サーバーからのソフトウェアまたはコンテンツの依 存関係を示します。
	 Install [インストール] – 対応するソフトウェア バージョンが ファイアウォールにダウンロード済みまたはアップロード済み です。ソフトウェアをInstall [インストール] する場合はクリッ クします。アップグレード プロセスの完了時に再起動が必要で す。
	 Reinstall [再インストール] - 対応するソフトウェアバージョンが 以前インストールされていました。このバージョンをReinstall [再インストール] する場合はクリックします。
リリース ノート	対応するソフトウェア更新のリリース ノートへのリンクが提供され ます。このリンクは、Palo Alto Networks 更新サーバーからダウン ロードする更新の場合にのみ使用でき、アップロードされた更新で は使用できません。
	以前にダウンロードまたはアップロードしたソフトウェア イメー ジをファイアウォールから削除します。アップグレードの必要が ない古いリリースの基本イメージのみを削除してください。たとえ ば、10.1 を実行している場合は、ダウングレードが必要でない限 り、10.0 の基本イメージを削除できます。
今すぐチェック	Palo Alto Networks から新しいソフトウェア更新を入手可能かどう かをチェックします。
	ソフトウェアアップデートの確認に問題があります か?一般的な接続の問題の解決策については、この記 事を参照してください。
アップロード	ファイアウォールがアクセスできるコンピュータからソフトウェ ア更新イメージをインポートします。通常、この操作はファイ アウォールがインターネットにアクセスできない場合に実行しま す。Palo Alto Networks 更新サーバーから更新をダウンロードする には、インターネットにアクセスできる必要があります。アップ ロードを行う場合、インターネットに接続されたコンピュータか ら Palo Alto Networks の Web サイトにアクセスし、サポート サ イト(ソフトウェア アップデート)からソフトウェア イメージを

ソフトウェア オプショ ン フィールド	の意味
	ダウンロードし、アップデート内容をコンピュータにダウンロー
	ドし、ファイアウォールの Device(デバイス) > Software(ソ
	フトウェア)を選択してソフトウェア イメージの Upload(アッ
	プロード)を行います。高可用性 (HA) 設定の場合、Sync To Peer
	[ピアと同期] のオプションを選択し、インポートしたソフトウェ
	アイメージをHAピアにプッシュします。アップロードが完了する
	と、Software(ソフトウェア)ページに、アップロードおよびダ
	ウンロードしたソフトウェアと同一の情報(バージョンやサイズ
	など)と、Install(インストール)/Reinstall(再インストール)の
	オプションが表示されます。アップロードしたソフトウェアの場
	合、Release Notes [リリースノート] のオプションは無効化されて
	います。

Device > Dynamic Updates [デバイス > 動的更新]

- Device > Dynamic Updates [デバイス > 動的更新]
- Panorama > Dynamic Updates [Panorama > 動的更新]

Palo Alto Networks は、動的更新を通じて、新規および変更されたアプリケーション、脅威保 護、loT セキュリティ用のデバイスのディクショナリーファイル、および GlobalProtect データ ファイルを含む更新を定期的に投稿します。設定を変更することなく、ファイアウォールはこれ らの更新を取得し、それを使ってポリシーを適用できます。アプリケーションおよび一部のアン チウイルス アップデートはサブスクリプションなしで利用できます。その他はお使いのサブス クリプションに紐付いています。

最新の更新ファイルを表示し、各更新ファイルのリリースノートを読み、ダウンロードおよびイ ンストールする更新ファイルを選択できます。以前にインストールした更新のバージョンに戻す こともできます。

動的更新のスケジュールを設定すると、ファイアウォールが新しい更新の有無を確認し、ダウン ロードまたはインストールする頻度を定義することができます。特に、アプリケーションや脅威 のコンテンツの更新では、脅威の更新の背後に新しいアプリケーションや変更されたアプリケー ションの更新を計画するスケジュールを設定できます。 これにより、ファイアウォールに常に 最新の脅威防止機能を備えつつ、新規および変更されたアプリケーションがセキュリティ ポリ シーにどのように影響するかを評価する時間が長くなります。

Dynamic Updates Options (動的更新オプ ション)	の意味
バージョン	Palo Alto Networks 更新サーバーで現在入手可能なバージョンが 一覧表示されます。Palo Alto Networks から新しいソフトウェ アリリースを入手可能かどうかをチェックするには、Check Now[今すぐチェック] をクリックします。ファイアウォールが サービス ルートを使用して更新サーバーに接続し、新しいコンテ ンツリリース バージョンをチェックします。適用可能な更新が ある場合は、その更新がリストの最上部に表示されます。
最終チェック	ファイアウォールが最後に更新サーバーに接続して更新があるか どうかをチェックした日時が表示されます。
スケジュール	 更新を取得する頻度をスケジューリングできます。 動的コンテンツアップデートの頻度およびタイミング (Recurrence (繰返し)と時間)を設定し、またスケジュール設定されたアップデートのDownload Only (ダウンロードのみ)行うか、Download and Install (ダウンロードとインストール)を行うかを設定することが可能です。 Antivirus and Applications and Threats (ウイルス対策とアプリケーションと脅威の更新)では、ファイアウォールがインストー

Dynamic Updates Options (動的更新オプ ション)	の意味
	ルする前にコンテンツ更新を利用できる最小時間を設定するオプ ションがあります。ごくまれに、コンテンツの更新にエラーが発 生する可能性があり、このしきい値は、ファイアウォールが指定 された時間、利用可能かつ顧客環境で機能しているコンテンツリ リースのみをダウンロードすることを保証します。
	アプリケーションと脅威のコンテンツの更新では、新規および変 更されたアプリケーションでコンテンツの更新に特に適用される しきい値を設定することもできます。拡張アプリケーションのし きい値は、新しいアプリケーションや変更されたアプリケーショ ンが導入する変更に基づいてセキュリティポリシーを評価し、調 整するための時間が長くなります。
	WildFire の更新にはシグネチャをリアルタイムで取得するオプ ションがあり、シグネチャが生成されると即座にアクセスでき ます。検体確認中にダウンロードされたシグネチャはファイア ウォールキャッシュに保存され、高速(ローカル)検索に使用す ることができます。さらに、カバレッジの最大化に向けて、リア ルタイムのシグネチャが有効化されている場合、ファイアウォー ルは定期的に追加のシグネチャパッケージを自動的にダウンロー ドします。この補足シグネチャはファイアウォールキャッシュに 追加され、ステールとなり更新されるか、新しいシグネチャで上 書きされるまで使用することができます。
	Application and Threat (アプリケーションと脅威) のコンテンツの更新を常に有効にして、アプリケー ションの可用性と最新の脅威の両方を保護する方法 については、「アプリケーションと脅威の更新に関 するベストプラクティス」を参照してください
ファイル名	ファイル名が一覧表示されます。ファイル名にはコンテンツの バージョン情報が含まれます。
機能	コンテンツバージョンに含めることができるシグネチャのタイプ が一覧表示されます。 アプリケーションおよび脅威コンテンツリリースバージョンの場 合、このフィールドには、Apps, Threats [アプリケーションおよ び脅威] を確認するためのオプションが表示されることがありま す。このオプションをクリックすると、ファイアウォールにイン ストールされた最後のコンテンツ リリース バージョンから使用 できるようになった新しいアプリケーション シグネチャが表示 されます。New Applications (新しいアプリケーション) ダイア ログを使用して、新しいアプリケーションを Enable (有効化) /

Dynamic Updates Options (動的更新オプ ション)	の意味
	Disable (無効化) することもできます。一意に識別されるアプリ ケーションがポリシーに影響を及ぼさないようにするため、コン テンツ リリースに含まれる新しいアプリケーションを無効にする 場合があります (未知だったアプリケーションが識別され、以前 とは異なって分類されると、コンテンツのインストール前後でア プリケーションの処理が変わる可能性があります)。
	デバイス ディクショナリーの場合、このフィールドは IoT で、IoT Security の略で、Device-ID に基づくセキュリティ ポリ シー ルールを正確に適用する上でデバイス ディクショナリを重 要なコンポーネントとして使用するクラウド セキュリティ サー ビスです。
タイプ	ダウンロードにフル データベース更新が含まれているか、増分更 新が含まれているかを示します。
サイズ	コンテンツ更新パッケージのサイズが表示されます。
SHA256	ファイルの整合性を検証するために使用されるチェックサム。
リリース日	Palo Alto Networks がコンテンツ リリースを公開した日時。
ダウンロード済み	この列のチェック マークは、対応するコンテンツ リリース バー ジョンがファイアウォールにダウンロード済みであることを示し ます。
現在インストール済み	この列のチェック マークは、対応するコンテンツ リリース バー ジョンがファイアウォールで現在実行されていることを示しま す。
操作	対応するソフトウェア イメージで現在実行可能な以下のようなア クションを示します。 • Download (ダウンロード) – 対応するコンテンツリリース バージョンを Palo Alto Networks 更新サーバーから入手でき ます。コンテンツリリース バージョンをダウンロードする には、Download (ダウンロード) をクリックします。ファ イアウォールがインターネットに接続できない場合は、イン ターネットに接続できるコンピュータからCustomer Support Portal (カスタマー サポート ポータル) サイトにアクセス し、Dynamic Updates (動的更新)を選択します。必要なコ ンテンツリリースバージョンを検索して Download (ダウン ロード) をクリックして、ローカル コンピュータに更新パッ ケージを保存します。次にファイアウォールへソフトウェアイ

Dynamic Updates Options(動的更新オプ ション)	の意味
	メージを手動でUpload [アップロード] します。また、アプリ ケーションおよび脅威コンテンツ リリース バージョンをダウ ンロードすると、リリースに含まれる新しいアプリケーション シグネチャの影響を受けるReview Policies (ポリシーを確認)す るためのオプションが有効になります。
	 Review Policies (ポリシーの確認) (アプリケーションおよび脅威コンテンツのみ) – コンテンツリリースバージョンに含まれる新しいアプリケーションによるポリシーへの影響を確認します。コンテンツ更新のインストール前後のアプリケーションの処理を評価するには、このオプションを使用します。Policy Review (ポリシーのレビュー) ダイアログを使用して、保留中のアプリケーション (コンテンツリリースバージョンでダウンロードされたが、ファイアウォールにインストールされていないアプリケーション)を既存のセキュリティポリシーに追加または既存のセキュリティポリシーから削除することもできます。保留中のアプリケーションのポリシーを変更しても、その変更は、対応するコンテンツリリースバージョンがインストールされるまで有効になりません。
	 Review Apps (アプリのレビュー) (アプリケーションと脅威 コンテンツのみ) – ファイアウォールにインストールされた 最後のコンテンツ リリース バージョンから使用できるように なった新規および変更済みアプリケーション シグネチャが表 示されます。重要なアプリケーションの適用に影響を与える可 能性のある変更がコンテンツ更新によって導入された場合、そ れらのアプリケーションにはポリシー レビューの推奨として マークされます。Review Policies (ポリシーの確認) をクリッ クすると、コンテンツの更新が既存のセキュリティ ポリシー にどのように影響するのかを確認したり、アプリケーションの ポリシーの影響を確認するまでアプリケーションを無効にする ことができます。
	 Install [インストール] – 対応するコンテンツリリースバージョンがファイアウォールにダウンロード済みです。アップデートをInstall [インストール] する場合にクリックします。新しいアプリケーションおよび脅威コンテンツリリースバージョンをインストールすると、Disable new apps in content update[コンテンツ更新での新しいアプリケーションの無効化] オプションが表示されます。このオプションにより、最新の脅威に対する保護を有効にしながら、新しいアプリケーションシグネチャの影響のためにポリシーの更新を準備した後でアプリケーションを柔軟に有効にできます(以前に無効にしたアプリケーションを有効にするには、Dynamic Updates(動的更新)ページの Apps, Threats (アプリケーションおよび脅威)を選択す

Dynamic Updates Options(動的更新オプ ション)	の意味
	るか、Objects(オブジェクト) > Applications(アプリケー ション)を選択します)。 • Revert [戻す] – 対応するコンテンツリリースバージョンが以 前にダウンロードされていて、同じバージョンを再インストー ルする場合はRevert [戻す] をクリックします。
ドキュメント	対応するバージョンのリリース ノートへのリンクが提供されま す。
×	以前にダウンロードしたコンテンツ リリース バージョンをファ イアウォールから削除します。
アップロード	ファイアウォールがPalo Alto Networksアップデートサーバーに アクセスできない場合、Palo Alto Networksサポートサイトの動 的更新のセクションから動的更新を手動でアップロードすること ができます。コンピュータにアップデートをダウンロードしたの ちに、更新内容をファイアウォールへUpload [アップロード] しま す。次に Install From File(ファイルからインストール)を選択 し、ダウンロードしたファイルを選択します。
ファイルからインストー ル	更新ファイルをファイアウォールへ手動でアップロードしたの ちに、このオプションを使用してファイルをインストールしま す。Package Type [パッケージタイプ] のドロップダウンリスト からインストールする更新のタイプを選択し(Application and Threats [アプリケーションおよび脅威]、Antivirus [アンチウイ ルス]、またはWildFire)、OKをクリック、インストールしたい ファイルを選択し、再度OKをクリックしインストールを開始し ます。
Device > Licenses [デバイス > ライセンス]

すべてのファイアウォール モデルでライセンスをアクティベートするには、Device(デバイ ス) > Licenses(ライセンス)を選択します。Palo Alto Network からサブスクリプションを購 入すると、1 つ以上のライセンス キーを有効にするための認証コードが送信されます。

VM-Series ファイアウォールの場合、このページで仮想マシン (VM) を非アクティブにすること もできます。

以下のアクションは、Licenses (ライセンス) ページで実行できます。

- Retrieve license keys from license server (ライセンス サーバーからライセンス キーを取得) サポートポータルでアクティベート済みで、かつ認証コードを必要とする購入済みのサブス クリプションを有効化する場合に選択します。
- Activate feature using authorization code (認証コードを使用した機能のアクティベーション)サポートポータルでアクティベートされておらず、かつ認証コードを必要とする購入済みのサブスクリプションを有効化する場合に選択します。次に、認証コードを入力し、OKをクリックします。
- Manually upload license key (ライセンス キーの手動アップロード):ファイアウォールがラ イセンス サーバーに接続されておらず、ライセンス キーを手動でアップロードする場合は、 ライセンス キー ファイルを https://support.paloaltonetworks.com からダウンロードして ローカルに保存します。Manually upload license key (ライセンス キーの手動アップロード) をクリックし、Browse(参照)をクリックしてファイルを選択し、OK をクリックします。
 - URLフィルタリングのライセンスを有効化する場合は、ライセンスをインストールし、データベースをダウンロードし、Activate [アクティベート]をクリックする必要があります。URLフィルタリングにPAN-DBを使用している場合、初期シードデータベースをDownload [ダウンロード] してから Activate [アクティベート]をクリックする必要があります。

CLIコマンド request url-filtering download paloaltonetworks < region name>を実行することもできます。

- Deactivate VM [VMのディアクティベート]:このオプションは、永久ライセンスおよび期間 ベースのライセンスをサポートするBring Your Own Licenseモデルの VM-Seriesファイア ウォールで使用できます。オンデマンドライセンスモデルでは、この機能はサポートされて いません。VM-Seriesファイアウォールのインスタンスが必要なくなった場合、Deactivate VM [VMのディアクティベート]をクリックします。このオプションを使用すると、すべての アクティブなライセンス(サブスクリプションライセンス、VM キャパシティライセンス、 およびサポート資格)を解放できます。ライセンスのクレジットはアカウントに戻るため、 必要に応じて VM-Series ファイアウォールの新しいインスタンスにライセンスを適用できま す。ライセンスがディアクティベートされると、VM-Seriesファイアウォールの機能が無効化 され、ファイアウォールはライセンスのない状態になります。しかし、設定はそのまま保存 されます。
 - VM-Series ファイアウォールがインターネットに直接アクセスできない場合、Continue Manually(手動で続行)をクリックします。ファイアウォールは、トークンファイル

を生成します。Export license token [ライセンストークンのエクスポート] をクリック し、トークンファイルをローカルコンピュータに保存して、ファイアウォールを再起 動します。Palo Alto Networks Support ポータルにログインし、Assets(アセット) > Devices(デバイス)を選択し、Deactivate VM(VMのディアクティベート)をクリック して、このトークン ファイルを使用してディアクティベートのプロセスを完了します。

- Continue [続行] をクリックして、VM-Seriesファイアウォールのライセンスをディア クティベートします。ライセンスの非アクティブ化プロセスを完了するには、Reboot Now[今すぐ再起動] をクリックします。
- ディアクティベートを中止してDeactivate VM [VMのディアクティベート] ウィンドウを閉じる場合はCancel [キャンセル] をクリックします。
- Upgrade VM Capacity (VM キャパシティのアップグレード):このオプションでは、現在ラ イセンスのある VM-Series ファイアウォールのキャパシティをアップグレードできます。 キャパシティをアップグレードしても、アップグレード前に VM-Series ファイアウォールで 使用していたすべての設定とサブスクリプションは維持されます。
 - ファイアウォールがライセンスサーバーに接続できる場合は、Authorization Code(認証コード)を選択し、Authorization Code(認証コード)フィールドに認証コードを入力し、Continue(続行)をクリックして、キャパシティのアップグレードを開始します。
 - ファイアウォールがライセンスサーバーに接続できない場合は、License Key (ライセンスキー)を選択し、Complete Manually (手動で実行)をクリックしてトークンファイルを生成し、トークンファイルをローカルコンピュータに保存します。次にPalo Alto Networks Support ポータルにログインし、Assets (アセット) > Devices (デバイス)を選択し、Deactivate License(s) (ライセンスのディアクティベート)をクリックして、トークンファイルを使用します。VM-Series ファイアウォールのライセンスキーをローカルコンピュータにダウンロードし、ライセンスキーをファイアウォールに追加し、Continue (続行)をクリックしてキャパシティのアップグレードを完了します。
 - ファイアウォールがライセンスサーバーに接続でき、認証コードがない場合は、Fetch from license server (ライセンスサーバーから取得)を選択し、キャパシティのアップグ レードを試みる前にライセンスサーバーでファイアウォールのキャパシティ ライセンス をアップグレードします。次に、ライセンスサーバーでライセンスがアップグレードされ たことを確認した後、Continue(続行)をクリックしてキャパシティのアップグレードを 開始します。

Device > Support [デバイス > サポート]

- Device > Support [デバイス > サポート]
- Panorama > Support [Panorama > サポート]

サポート関連のオプションを表示する場合は Device(デバイス) > Support(サポート)また は Panorama > Support(サポート)を選択します。Palo Alto Networks の連絡先、サポートの 有効期限、ファイアウォールのシリアル番号に基づいた Palo Alto Networks からの製品および セキュリティ アラートを表示できます。

必要に応じて、このページで以下の機能を実行します。

- Support(サポート) デバイスのサポート状態に関する情報と、認証コードを使用してサポートをアクティベーションするためのリンクを提供します。
- Production Alerts/Application and Threat Alerts (実働アラート/アプリケーションおよび脅威アラート) これらのアラートは、このページにアクセスしたとき、またはページを更新したときに Palo Alto Networks 更新サーバーから取得されます。実働アラートの詳細、またはアプリケーションおよび脅威アラートの詳細を表示する場合はそのアラート名をクックします。実働アラートは、大規模なリコールが発生した場合またはそのリリースに関する緊急の問題が発生した場合に通知されます。アプリケーションおよび脅威アラートは、重大な脅威が検出されたときに通知されます。
- Links(リンク) デバイスを管理しやすくしたり、サポート連絡先情報にアクセスしたりするための共通のサポートリンクを提供します。
- Tech Support File (テクニカル サポート ファイル) Generate Tech Support File (テクニカル サポート ファイルの生成) をクリックして、ファイアウォールで発生している可能性のある問題のトラブルシューティングに対して、サポート チームが使用できるシステムファイルを生成します。ファイルを生成したら、Download Tech Support File[テクニカルサポートファイルのダウンロード] をクリックしてファイルを取得し、そのファイルをPalo AltoNetworksサポート部門に送信します。
 - ブラウザがダウンロード後に自動的にファイルを開くよう設定している場合はその機能を無効化し、ブラウザでサポートファイルをダウンロードしても開封・抽出を行わないようにする必要があります。
- Stats Dump File:統計ダンプファイルを生成するをクリックして、過去7日間のネット ワークトラフィックを要約する一連のXMLレポートを生成します。レポートが生成され たら、Download Stats Dump File[Stats Dumpファイルをダウンロード] することができま す。Palo Alto Networks または認定パートナーのシステムエンジニアが、このレポートを使 用してセキュリティ ライフサイクルレビュー(SLR)を生成します。SLRは、ネットワークで 検出されたものとその関連ビジネスやセキュリティリスクを明らかにし、通常は評価プロセ スの一部として使用されます。SLR の詳細は、Palo Alto Networks または認定パートナーのシ ステムエンジニアにお問い合わせください。

Panorama[™]管理サーバーによって管理されるファイアウォールの場合、一度に1つの管理対象ファイアウォールに対して統計ダンプファイルを生成したり、Panorama が管理するすべてのファイアウォールに対して1つの統計ダンプファイルを生成したりできます。

Core Files (コアファイル) – ファイアウォールでシステム プロセス エラーが発生した場合、プロセスとエラーの理由に関する詳細が記載されたコアファイルが生成されます。Download Core Files をクリックして使用可能なコアファイルの一覧を表示し、コアファイル名をクリックしてダウンロードします。問題解決のサポートを受けるには、ファイルのダウンロード後に Palo Alto Networks サポート ケースにアップロードします。

コアファイルの内容は、Palo Alto Networks サポートエンジニアのみが解釈できます。

Debug and Management Pcap Files – ファイアウォールでパケット キャプチャの失敗が発生した場合、失敗した理由のデバッグと管理の詳細を含むパケット キャプチャ (pcap) ファイルが生成されます。Download Debug and Management Pcap Files をクリックして使用可能なpcap ファイルのリストを表示し、pcap ファイル名をクリックしてダウンロードします。問題解決のサポートを受けるには、ファイルのダウンロード後に Palo Alto Networks サポートケースにアップロードします。

Device > Master Key and Diagnostics [デバイス > マス ター キーおよび診断]

- デバイス > マスターキーおよび診断
- Panorama > マスターキーおよび診断

ファイアウォールまたは Panorama ですべてのパスワードと秘密鍵(CLI にアクセスする管理者 を認証するための RSA キーなど)を暗号化するマスター キーを編集します。パスワードとキー を暗号化すると、それらのプレーンテキスト値がファイアウォールまたは Panorama のどの場所 にも表示されなくなるため、セキュリティが向上します。

デフォルトのマスターキーを復元するための唯一の方法は、工場出荷時設定へのリセットロを実行することです。

デフォルト キーを使用する代わりに新しいマスター キーを設定し、安全な場所にキーを保 管して定期的に変更することをお勧めします。プライバシーを強化するには、ハードウェア セキュリティ モジュールを使用してマスター キーを暗号化します(「Device(デバイス) > Setup(セットアップ) > HSM」を参照)。ファイアウォールまたは Panorama 管理サーバーご とに一意のマスター キーを設定した場合、攻撃者は 1 つのアプライアンスのマスター キーを取 得しても、他のアプライアンスのパスワードと秘密鍵にアクセスできません。ただし、次の場合 は、複数のアプライアンスで同じマスター キーを使用する必要があります。

- 高可用性(HA) 設定 ファイアウォールまたは Panorama を HA 設定でデプロイする場合、 ファイアウォールまたは Panorama 管理サーバーのペアで同じマスター キーを使用します。 同じマスター キーを使用しない場合、HA 同期が機能しません。
- Panorama 管理 WildFire アプライアンスと Log Collectors :Panorama、WildFire アプライアン ス、および管理対象コレクタに同じマスターキーを設定する必要があります。同じマスター キーを使用しない場合、Panorama からのプッシュ操作が失敗します。

マスター キーを設定するには、マスター キーの設定を編集し、以下の表に従って適切な値を入力します。

マスター キーおよび診 断の設定	の意味
マスターキー	ー意のマスターキーを設定する場合に有効化します。デフォルトの マスターキーを使用する場合は無効化(クリア)します。
現在のマスター キー	ファイアウォールでのすべての秘密鍵とパスワードの暗号化で現在 使用されている鍵を指定します。
新規マスター キー マスター鍵の確認	マスター キーを変更するには、16 文字の文字列を入力して新しい キーを確認します。

マスター キーおよび診 断の設定	の意味	
ライフ タイム	マスターキーが失効するまでの期間をDays (日数) および Hours (時間) で指定します。範囲は 1 ~ 438,000 日 (50年間) です。 現在のキーが失効する前に新しいマスター キーを設定す る必要があります。マスター キーが失効すると、ファイア ウォールまたは Panorama は自動的にメンテナンス モード で再起動されます。この場合、工場出荷時設定へのリセッ ト 実行する必要があります。	を -
リマインダーの時間	マスター キーが失効する前にファイアウォールで失効アラームを生 成するまでの Days(日数)と Hours(時間)を入力します。ファ イアウォールは System Alarms(システム アラーム)ダイアログを 自動的に開いてアラームを表示します。	

マスター キーおよび診 断の設定	の意味
	 スケジュール済みメンテナンスウィンドウで、有効期限が切れる前に新しいマスターキーを設定する時間が十分取れるよう、リマインダーを設定します。Time for Reminder (リマインダーの時間)が期限に達し、ファイアウォールまたは Panorama が通知ログを送信したら、Lifetime (有効期間)の有効期限切れを待たずに、マスターキーを変更します。グループ化されたデバイスの場合、すべてのデバイス (Panorama管理のファイアウォールやファイアウォール HAペアなど)を追跡し、グループ内にあるいずれかのデバイスでリマインダー値が期限に達したら、マスターキーを変更します。 失効アラームを表示するには、Device (デバイス) > Log Settings (ログ設定)を選択し、Alarm Settings (アラームを有効化)します。
HSM に保管	 ハードウェアセキュリティモジュール(HSM)でマスターキーを 暗号化する場合にのみ、このオプションを有効にします。DHCPク ライアントや PPPoE などのダイナミックインターフェイスで HSM を使用することはできません。 HSM 設定は、HA モードのピアファイアウォール間では同期され ません。したがって、HA ペアの各ピアは異なる HSM ソースに接 続できます。Panorama を使用していて両方のピアの設定の同期を 維持する必要がある場合、Panorama テンプレートを使用して管理 対象ファイアウォールの HSM ソースを設定します。 PA-220 は HSM をサポートしていません。
マスターキーの自動更 新	指定した日数および時間数でマスターキーを自動更新する場合に有 効化します。無効化(クリア)すると、設定したキーの寿命が過ぎ たらマスターキーが失効するようになります。
	マスター キーの暗号化を延長する Days(日数)と Hours(時間 数)を指定(範囲は 1 時間 ~ 730 日)することで、Auto Renew with Same Master Key (同じマスターキーを自動更新)します。

マスター キーおよび診 断の設定	の意味 	
	Auto Renew Master Key (マスターキーの自動更新)を 有効にする場合は、デバイスが一意の暗号化を使い切らないように、合計時間 (有効期間と自動更新時間)を 設定します。たとえば、デバイスが2年半でマスター キーの一意の暗号化の数を消費することが見込まれる 場合、Lifetime (有効期間)を2年間に設定し、Time for Reminder (リマインダーの時間)を60日間に設定できます。Auto Renew Master Key (マスターキーの自動更新)は60~90日間に設定し、Lifetime (有効期間)の期限が切れる前に新しいマスターキーを設定する時間の余裕があるようにします。ただし、ベストプラクティスは、有効期限が切れる前にマスターキーを変更して、デバイスが暗号化を繰り返さないようにすることです。	
Common Criteria(共 通基準)	共通基準モードでは、別のオプションを使用して、暗号化アルゴリ ズム自己テストとソフトウェア整合性自己テストを実行できます。 また、この2つの自己テストを実行する時刻を指定するためのスケ ジューラも用意されています。	

マスターキーのデプロイ

管理対象のファイアウォール、ログコレクタ、WF-500 アプライアンスの既存のマスターキーを Panorama から直接更新あるいはデプロイします。

項目	の意味
マスターキー(のデプロイ
フィルタ	表示する管理対象デバイスをプラットフォーム、デバイスグループ、テンプ レート、タグ、HA ステータス、ソフトウェアバージョンに基づいてフィルタ リングします。
デバイス名	管理対象ファイアウォールの名前です。
ソフトウェ ア バージョ ン	管理対象デバイスで実行されているソフトウェア バージョンです。
ステータス	管理対象デバイスの接続ステータス(Connected (接続済 み)、Disconnected (未接続)、Unknown (不明))です。

項目	の意味		
マスターキー	マスターキーのデプロイジョブのステータス		
デバイス名	管理対象ファイアウォールの名前です。		
ステータス	マスターキーのデプロイジョブのステータスです。		
result	マスターキーのデプロイジョブの結果です。OKあるいはFAIL (失敗)になり ます。		
進捗	マスターキーのデプロイジョブの進捗状況(%)です。		
詳細:	マスターキーのデプロイジョブの詳細です。ジョブが失敗した場合、失敗した 理由を示す詳細がここに表示されます。		
概要			
進捗	マスターキーのデプロイジョブの進捗状況を示すプログレスバーを表示しま す。次の情報が表示されます:		
	• Results Succeeded (成功した結果)-マスターキーを正常にデプロイできた デバイスの数です。		
	 Results Pending (保留中の結果)-マスターキーのデプロイジョブが現在保留 されているデバイスの数です。 		
	• Results Failed (失敗した結果)-マスターキーのデプロイジョブが失敗した デバイスの数です。		

loT >デバイス>ポリシーの推奨事項

loT Security からのポリシー ルールの推奨事項に関する情報を表示します。loT Security は、 ファイアウォールがネットワーク上のトラフィックから収集したメタデータを使用して、デバイ スに許可する動作を決定し、適用するセキュリティ ポリシー ルールの推奨事項を生成します。

Button/Field(ボタン/フィールド)	の意味
プロファイル	デバイスプロファイルを選択すると、そ のデバイスの推奨セキュリティポリシー ルールが表示されます。このリストは、loT Securityポータルのプロファイルページにあり ます。PAN-OS ルールベースにインポートす るルールを選択し、次にポリシールールをイ ンポートします。
ポリシーのインポートの詳細	ポリシールールをインポートしたら、「ファ イルと虫めがね」アイコンをクリックする と、そのルールに関する次の詳細を表示でき ます。
	 インポート先:ルールがインポートされた仮 想システム (次世代ファイアウォール内)ま たはデバイスグループ (Panorama)
	 ルール名:ルール名。プロファイル名とアプリケーション名をハイフンで連結したもの
	 ユーザ:ポリシーをインポートした管理者の 名前
	 新しい更新の適用先?ポリシールールがインポート後に更新された(Yes)か、更新されなかったか(No)の表示
	 インポート時間:ポリシールールがインポー トされた日付と時刻
	 更新時間:ポリシールールが最後に更新された日付と時刻
インポート先	次世代ファイアウォールの場合、これはポリ シー ルールの推奨事項がインポートされた仮 想システムを示します。Panoramaの場合、ポ リシー ルールの推奨事項がインポートされた デバイス グループが表示されます。

Button/Field(ボタン/フィールド)	の意味
ポリシー ルール名	ポリシールールの名前。デフォルトではデバ イスプロファイル名とアプリケーション名を 連結したものです。
推奨デバイス グループ	(Panorama) IoT Security が次世代の firewall か ら受信したログ内のゾーンとデバイス グルー プについて学習した後、ポリシー ルールとし て提案したものがデバイス グループとなりま す
送信元デバイスプロファイル	ポリシー ルールの推奨事項によってトラ フィックが許可されるデバイス プロファイ ル。
送信元ゾーン	ポリシー ルールの推奨事項によってトラ フィックが許可される送信元ゾーン。これは 未使用で、常に空です。
送信元ユーザー	ポリシー ルール推奨のソース ユーザー。これ は未使用で、常に空です。
送信元デバイス	ポリシー ルールの推奨のソース デバイス。こ れは未使用で、常に空です。
送信元アドレス	ポリシー ルールの推奨事項の送信元アドレ ス。これは未使用で、常に空です。
宛先デバイス グループのプロファイル	ポリシー ルールの推奨事項によってトラ フィックが許可される宛先デバイス プロファ イル。
宛先デバイスの IP	ポリシー ルールの推奨事項によってトラ フィックが許可されるデバイスの IP アドレ ス。
宛先の FQDN	ポリシー ルールの推奨事項によってトラ フィックが許可される完全修飾ドメイン名 (FQDN)。
宛先ゾーン	ポリシー ルールの推奨事項によってトラ フィックが許可される宛先ゾーン。これは未 使用で、常に空です。
宛先セキュリティプロファイル	ポリシー ルールの推奨事項で許可されるセ キュリティ プロファイル。

Button/Field(ボタン/フィールド)	の意味
宛先URLカテゴリ	ポリシー ルールの推奨事項によってトラ フィックが許可される URL フィルタリング カ テゴリ。
目的地の地理的位置	宛先がネットワークの内部ゾーン (プライベー ト) にあるか、外部ゾーン (インターネット) に あるか、または両方 (プライベートとインター ネット) にあるかを識別します。
サービス	サービスはポリシールール推奨です。これは 未使用で、常に空です。
アプリケーション [applications]	ポリシー ルールの推奨事項で許可されている アプリケーション。
tags	 ポリシールールの推奨事項のポリシールールを識別するタグ。 ポリシールールのタグを変更しないでください。タグを変更すると、firewallはポリシーマッピングを再構築できなくなります。
操作	このポリシー ルールの推奨事項に対するアク ション(通常 allow)を識別します。
利用可能な新しいアップデート	この列は使用されません。
このファイアウォールのみを表示	(ファイアウォールI) IoT Securityは、アクティ ブ化されたすべてのポリシー セット内のルー ルを Panorama およびすべての次世代ファイ アウォールに自動的にプッシュします。そ の結果、ファイアウォールには適用されな いルールがいくつか存在する可能性がありま す。ローカル firewall に適用されるルールのみ を表示するには、view only this firewall を使 用します。
インポートポリシールール	Panoramaまたはファイアウォールが IoT Security からポリシールールの推奨事項を取 得したら、ポリシールールベースにインポー トするポリシーを1つ以上選択し、[Import Policy Rule (ポリシールールのインポート)] を クリックします。表示される Import Policy

Button/Field(ボタン/フィールド)	の意味
	Rule ダイアログボックスで、インポートす る場所 (Panorama のデバイスグループとファ イアウォールの仮想システム) を選択しま す。firewall でローカルに定義されたルールの 前に推奨されるポリシー ルールを追加するに は ルール前 を選択し、ローカルで定義され たルールの後に ルールベース を選択します。 ルールベース内のポリシー・ルールの名前を 選択して選択したポリシールールを後でイン ポートするか、「No Rule Selection (ルール選 択なし)」を選択して選択したルールを一番上 にインポートします。
	ポリシールール推奨をルールベースに再度イ ンポートすると、インポートされたルール によって以前にインポートされた同じ名前の ルールが置き換えられ、初めてルールベース にインポートした後に行った編集内容が上書 きされます。ルールレコメンデーションを同 じルールベースに再インポートする必要はあ りませんが、Panoramaの異なるデバイスグ ループのルールベースにルールレコメンデー ションを複数回インポートする場合がありま す。[Imported To (インポート先)] 列にエント リがあれば、どのルール推奨事項が以前にイ ンポートされたかがわかります。

デバイス > ポリシー>推奨 SaaS

Prisma SaaS からのポリシー ルールの推奨事項に関する情報を表示し、ポリシーをファイア ウォールにインポートします。

項曰	の音味
送信元ユーザー	ポリシー ルールの推奨事項をファイアウォー ルに送信した管理者。
送信元デバイス	ポリシー ルールの推奨のソース デバイス。
場所	このポリシー ルールの推奨事項が利用可能な Panorama のデバイス グループ。
セキュリティ プロファイル	ポリシー ルールの推奨事項で許可されている セキュリティ プロファイル。
アプリケーション [applications]	ポリシー ルールの推奨で許可されるアプリ ケーションまたはアプリケーション グルー プ。アプリケーション グループ名をクリック すると、そのグループ内の個々のアプリケー ションが表示されます。
tags	 ポリシールール推奨事項のポリシールールを 識別するタグ。 ポリシールールのタグは変更し ないでください。タグを変更す ると、firewallはポリシーマッピ ングを再構築できません。
の意味	Prisma SaaS 管理者がポリシー ルールの推奨 事項に与える説明。
Active Recommendation(アクティブ推奨事 項)	 このポリシー ルールの推奨事項が active-現在、Prisma SaaS セキュリティ ポリシーで使用されています。 削除-Prisma SaaS 管理者によってポリシー から削除されました。ファイアウォール管 理者はポリシー ルールをインポートでき なくなり、ポリシーマッピングをファイ アウォールから削除し、ファイアウォール ルールベースからセキュリティポリシー ルールを削除する必要があります。削除さ

デバイス

項目	の意味
	れたルールをファイアウォールルールベー スに残さない。
操作	このポリシー ルールの推奨事項に対するアク ションを示します (許可 または deny 。
New Update Available(最新更新が使用可 能)	ポリシールールレコメンデーションの新しい 更新があることを示します。アプリケーショ ン列でアプリケーションの変更を確認してく ださい。変更に同意する場合は、ルールを選 択し、ポリシールールを選択してポリシーを 更新します。プリスマ・サアスから輸入しな ければならないこと。ポリシールールの推奨 更新をインポートすると、ファイアウォール はセキュリティポリシールールと関連オブ ジェクトを動的に更新します。
インポートポリシールール	プリズム SaaS から選択したポリシー ルール の推奨事項をインポートします。
Remove Policy Mapping ポリシー マッピン グの削除	 デバイスのポリシー ルールの推奨事項が不要となった場合は、Remove Policy Mapping(ポリシーマッピングの削除)を実行することができます。 ポリシールールの推奨事項に対応するポリシールールも削除する必要があります。
ポリシールールを同期	SaaS 管理者がポリシーの推奨事項を削除 し、ポリシーマッピングを削除してセキュリ ティポリシールールを削除した場合、情報が 同期しなくなった場合、削除されたルールが ルールの推奨事項リストに残る可能性があり ます。同期ポリシールールを同期します。

デバイス>ポリシー推奨>IoTまたはSaaS>ポリシー ルールのインポート

ポリシー規則の推奨事項をセキュリティポリシー規則ベースにインポートするようにこれらの設 定を構成し、[**OK**]をクリックします。

Button/Field(ボタン/フィールド)	の意味
場所	ルールをインポートする仮想システム(次世 代ファイアウォール内)または1つ以上のデバ イスグループ(Panorama内)を選択します。
推奨される場所	次世代ファイアウォールから受信したログに ゾーンやデバイスグループに関する情報が含 まれている場合、さまざまなポリシールール の場所が提案される可能性があります。その 場合は、オプションとしてここに表示されま す。
宛先タイプ	firewall でローカルに定義されたルールの前 に推奨されるポリシー ルールを追加するに は ルール前 を選択し、ローカルで定義された ルールの後に ルールベース を選択します。
事後ルール	規則ベースのポリシー規則の名前を選択し て、選択したポリシー規則をインポートする か、 [No Rule Selection (ルール選択なし)] を選択して選択した規則を一番上にインポー トします。
の意味	インポートするルールの推奨事項について、 後で参照できるように便利な説明を追加しま す。



ユーザーID

ユーザーID(User-ID[™])は、アプリケーション アクティビティおよびポリシーを単純に IP ア ドレスと結び付ける代わりに、ユーザー名やユーザー グループに結び付け、LDAP等の様々な企 業ディレクトリや端末サービスをシームレスに統合する、Palo Alto Networks[®] の次世代のファ イアウォール機能です。User-ID を設定するとアプリケーション コマンド センター(ACC)、 アプリケーション スコープ、レポート、およびログのすべてに、ユーザーの IP アドレスに加え ユーザー名が含まれるようになります。

- Device > User Identification > User Mapping [デバイス > User-ID > ユーザーマッピング]
- Device (デバイス) > User Identification (User-ID) > Connection Security (接続のセキュリ ティ)
- Device (デバイス) > User Identification (ユーザーID) > Terminal Server Agents (ターミナル サーバー エージェント)
- Device > User Identification > Group Mapping Settings [デバイス > User-ID > グループマッピ ングの設定]
- デバイス>ユーザ識別>信頼できる送信元アドレス
- Device (デバイス) > User Identification (ユーザー ID) > Authentication Portal Settings (認証ポータルの設定)
- デバイス>ユーザー識別>クラウドIDエンジン

その他の情報をお探しですか?

「User-ID^{II}」を参照してください。

Device > User Identification > User Mapping [デバイス > User-ID > ユーザーマッピング]

IP アドレスとユーザー名をマッピングするように、ファイアウォールで実行される PAN-OS 統合 User-ID エージェントを設定します。

確認すべき情報	以下を参照
PAN-OS 統合 User- ID エージェントを設 定する。	Palo Alto Networks User-IDエージェントの設定
User-ID エージェン トがユーザー マッピ ング情報用に監視す るサーバーへのアク セスを管理する。	サーバーの監視
ファイアウォールが IP アドレスをユー ザー名にマッピング する際に含める、あ るいは除外するサブ ネットワークを管理 する。	ユーザー マッピングのサブネットワークの許可または除外
その他の情報をお探 しですか?	Configure User Mapping Using the PAN-OS IntegratedUser-IDAgent (PAN-OS 統合 User-ID エージェントを使用したユーザー マッピングの設 定) ^{II}

Palo Alto Networks User-IDエージェントの設定

User-IDエージェントがユーザーマッピングを行う際に使用する方法は、ここでの設定内容に定義されます。

確認すべき情報	以下を参照
クライアントシステム、Windows Remote Management(WinRM)over HTTP あ るいは HTTPS のプローブを行ってユー ザーマッピング情報のためにサーバーを 監視するために、Windows Management	サーバー監視アカウント

0

確認すべき情報	以下を参照
Instrumentation(WMI)を使用するよう User-ID エージェントを有効化します。	
「User-ID エージェントによるユーザー マッ ピング情報のサーバー ログを監視する」	サーバー モニタリング
ユーザーマッピング情報入手のため、User- IDエージェントがクライアントシステムのプ ローブを行えるように設定する方法	クライアントのプローブ
ユーザーがローミングして新しいIPアドレス を取得していても、ファイアウォールが最新 のユーザーマッピング情報を保有しているよ うに設定する方法	Cache
ユーザーマッピング情報入手のため、User- IDエージェントがSyslogメッセージの構文解 析を行うよう設定する方法	Syslog のフィルタ
マッピング処理から特定のユーザー名を除外 するようにUser-IDエージェントを設定する 方法	ユーザー リストを無視

サーバー監視アカウント

 デバイス>ユーザーID>ユーザーマッピング>Palo Alto Networks User-IDエージェントの 設定>サーバー監視アカウント

クライアントシステム、Windows Remote Management(WinRM)over HTTP あるいは over HTTPS のプローブを行ってユーザーマッピング情報のためにサーバーを監視する際にWindows Management Instrumentation(WMI)を使用するよう PAN-OS 統合 User-ID エージェントを設定する場合は、以下のフィールドを入力します。

また、HTTP または HTTPS 経由で Windows Remote Management (WinRM) を使用してサーバー 監視を認証するように Kerberos サーバーを構成することで、監視対象サーバーに対するアクセ スの設定することもできます。 WMI プローブは、エンドポイントからレポートされたデータを信頼するため、セキュリティの高いネットワークではこの方法を使用して User-ID マッピング情報を取得しないことをお勧めします。Active Directory(AD)セキュリティ イベント ログまたは Syslog メッセージを解析するか、XML API を使用してマッピング情報を取得するように User-ID エージェントを設定する場合、WMI プローブを無効にすることをお勧めします。

WMI プローブを使用する場合、信頼されていない外部インターフェイスでは有効に しないでください。エージェントが、ネットワーク外で User-ID エージェント サー ビス アカウントのユーザー名、ドメイン名、パスワード ハッシュなどの機密情報 を含む WMI プローブを送信してしまうことになります。攻撃者は、この情報を悪 用してネットワークに侵入し、さらなるアクセス権を取得する可能性があります。

アクティブディレクトリ認証 設定	の意味
ユーザー名	ファイアウォールがWindowsリソースへアクセスする際に使 用する、アカウントのドメイン認証情報(User Name[ユー ザー名]およびPassword[パスワード])を入力します。ア カウントがクライアントコンピュータに対しWMIクエリ を行い、Microsoft Exchange サーバーおよびドメインコン トローラの監視を行う際には許可が必要となります。User Name[ユーザー名]にはdomain\usernameの構文を使用してく ださい。サーバー認証に Kerberos を使用することを監視対象 サーバーに対するアクセスの設定する場合は、Kerberos User Principal Name (UPN)を入力します。
ドメインの DNS 名	監視対象サーバーの DNS 名を入力します。サーバー認証に Kerberos を使用し監視対象サーバーに対するアクセスの設 定場合は、Kerberos Realm ドメインを入力します。>時にトラ ンスポート プロトコルとして WinRM-HTTP を使用している 場合は、この設定を構成する必要があります。
パスワード/再入力 パス ワード	ファイアウォールが Windows リソースへアクセスする際に使 用するアカウントのパスワードを入力して確認します。
Kerberosサーバプロファイ ル	レルムへのアクセスを制御して WinRM over HTTP あるいは over HTTPS を使用する監視対象サーバーからセキュリティ ログおよびセッション情報を取得する Kerberos サーバー用の Kerberos サーバープロファイルを選択します。



PAN-OS 統合 User-ID エージェントに、サーバーの監視とクライアントのプローブ を行わせるよう完全な手順で設定する場合は、アクティブディレクトリ認証設定の 定義の他に、いくつかの追加タスクを行う必要があります。 サーバー モニタリング

 デバイス > ユーザー ID > ユーザー マッピング > Palo Alto Networks User-IDエージェントの 設定 > サーバーモニター

User-ID エージェントがサーバーのセキュリティ イベント ログでログオン イベントを検索して IP アドレスをユーザー名にマッピングできるようにするには、以下の表の説明に従って設定を 指定していきます。



Windows Serverログ、Windows Serverセッション、または eDirectoryサーバーでクエ リの負荷が大きい場合は、クエリ間の遅延の観測値が、指定された頻度または間隔 を大きく超える可能性があります。

PAN-OS 統合 User-ID エージェントに、サーバーの監視を行わせるよう完全な手順 で設定する場合は、サーバーの監視の設定の他に、いくつかの追加タスクを行う必要があります。

サーバー モニタリング設定	の意味
セキュリティ ログの有効化	Windowsサーバーに対するセキュリティログのモニタリング を有効化する場合はこのオプションを選択します。
サーバーログのモニター頻度(秒)	ファイアウォールが Windows サーバー セキュリティ ログに 対しユーザー マッピング情報のクエリを行う頻度を秒単位で 指定します(範囲は 1 ~ 3600、デフォルトは 2)。この値 は、ファイアウォールが前回のクエリの処理を終了してから ファイアウォールが次のクエリを送信するまでの間隔です。 の の が レス対ユーザーのマッピングを利用できる可 能性があります。ファイアウォールがログを関 する頻度が多すぎる場合、ドメインコントロー ラ、メモリ、CPU、User-ID ポリシーの適用に影 響を与えるおそれがあります。2~30秒の範囲 の値から始め、パフォーマンスに及ぼす影響、 あるいはユーザーマッピングの更新頻度に基づ いて値を調整します。
セッションの有効化	監視対象のサーバーにおけるユーザーセッションの監視を有効 化する場合はこのオプションを選択してください。ユーザーが サーバーに接続するごとにセッションが作成されます。ファイ アウォールはこの情報を使用してユーザーのIPアドレスを特定 することができます。

サーバー モニタリング設定	の意味
	 Enable Session (セッションの有効化) は行わないでください。この設定では、すべてのユーザーセッションを読み取ることができるようにUser-ID エージェントにサーバーオペレータ権限のある Active Directory アカウントが必要です。 代わりに、Syslog または XML API 統合を使用して、(Windows オペレーティングシステムだけでなく) すべてのデバイスタイプとオペレーティングシステムのログインおよびログアウトイベントをキャプチャするソース (ワイヤレスコントローラや NAC など)を監視する必要があります。
サーバー セッションの読み 取り頻度(秒)	ファイアウォールがWindowsサーバーユーザーセッションに 対しユーザーマッピング情報のクエリを行う頻度を秒単位で指 定します(範囲は1~3600、デフォルトは10)。この値は、 ファイアウォールが前回のクエリの処理を終了してから次のク エリを開始するまでの間隔です。
Novell eDirectoryクエリ間 隔(秒)	ファイアウォールがNovell eDirectoryサーバーに対しユーザー マッピング情報のクエリを行う頻度を秒単位で指定します(範 囲は1~3600、デフォルトは30)。この値は、ファイアウォー ルが前回のクエリの処理を終了してから次のクエリを開始する までの間隔です。
Syslog サービス プロファイ ル	SSL/TLSサービスプロファイルを選択します。このプロファ イルには、証明書および許可されているSSL/TLSバージョン が指定されており、User-IDサービスがモニターするファイア ウォールと任意のSyslog Sender間の通信に使用されます。詳 細は、「Device(デバイス) > Certificate Management(証明 書の管理) > SSL/TLS Service Profile(SSL/TLS サービスプロ ファイル)」および「Syslog Filters(Syslog フィルタ)」を参 照してください。none[なし]を選択した場合、ファイアウォー ルは、事前定義された自己署名証明書を使用します。

クライアントのプローブ

 デバイス>ユーザーID>ユーザーマッピング>Palo Alto Networks User-IDエージェントの 設定>クライアントのプローブ セキュリティの高いネットワークや、信頼されていない外部インターフェイスでク ライアントのプローブを有効にしないでください。外部の信頼されていないゾーン でクライアントの調査を有効にすると、攻撃者がネットワークの外部にプローブを 送信し、User-ID エージェント サービスのアカウント名、ドメイン名、および暗号 化されたパスワード ハッシュが漏洩する可能性があります。

代わりに、Palo Alto Network は、ドメイン コントローラや Syslog または XML API との統合など、分離された信頼できるソースからユーザー マッピング情報を収集して、あらゆる種類のデバイスまたはオペレーティング システムからユーザー マッピング情報を安全にキャプチャすることを強くお勧めします。

ユーザー マッピング プロセスが識別する各クライアント システムについて、Windows 管理イ ンストルメンテーション (WMI) クライアントプローブ © を実行するように、PAN-OS 統合ユー ザー ID エージェントを構成できます。User-ID エージェントは、学習した各 IP アドレスを定期 的にプローブし、同じユーザーがまだログインしていることを確認します。ユーザー マッピン グが存在しない IP アドレスがファイアウォールで発生すると、アドレスがエージェントに送信 されてプローブが直ちに行われます。クライアントに対するプローブの設定を変更する場合は、 以下のフィールドを編集してください。クライアントをプローブするように PAN-OS 統合ユー ザー ID エージェントを構成するための の完全な手順 © では、WMI クライアントのプローブ設 定の構成以外にも追加のタスクが必要です。

クライアントに対するプロー ブ設定	の意味
プローブの有効化	WMI によるプローブを有効化する場合は、このオプションを 選択します。
プローブ間隔(分)	プローブ間隔を分単位で入力します(範囲は1~1440、デフォ ルトは20)。この値は、ファイアウォールが前回のリクエス トの処理を終了してから次のリクエストを開始するまでの間隔 です。
	大規模な導入環境では、ユーザーマッピング処理により識別された各クライアントをプローブするための時間を確保するため、間隔を適切に設定することが重要です。たとえば、ユーザーが6,000人で間隔が10分の場合は、各クライアントから1秒あたり10回のWMI要求が必要になります。
	プローブリクエストの負荷が大きい場合は、リクエスト間の遅延の観測値が、指定された間隔を大きく超える可能性があります。

Cache

 デバイス > ユーザー ID > ユーザー マッピング > Palo Alto Networks User-IDエージェントの 設定 > Cache

ユーザーがローミングして新しい IP アドレスを取得していても、ファイアウォールが最 新のユーザー マッピング情報を保有しているようにするため、ユーザー マッピングを ファイアウォール キャッシュから削除するタイムアウトを設定します。このタイムアウト は、Authentication Portal (認証ポータル) 以外の方法で学習したユーザー マッピングに適用さ れます。Authentication Portal (認証ポータル) で学習したマッピングの場合は、Authentication Portal (認証ポータル) 設定 (Device (デバイス) > User Identification (User-ID) > Captive Portal Settings (キャプティブ ポータルの設定)、Timer (タイマー) フィールドおよびIdle Timer (アイドル タイマー) フィールド) でタイムアウトを設定します。

ドメインが含まれていなくても User-ID ソースから収集したユーザー名を照合するには、ドメインなしで一致するユーザー名を許可するようにファイアウォールを設定します。組織内のユーザー名がドメイン間で重複していない場合にのみ、このオプションを使用してください。

キャッシュ設定	の意味
ユーザー ID タイムアウトを 有効にする	ユーザーマッピングエントリに対してタイムアウト値を適用す る場合はこのオプションを選択します。そのエントリのタイム アウト値に達した場合、ファイアウォールはそれを削除し、新 しくマッピングを行います。これにより、ユーザーがローミン グして新しいIPアドレスを取得していても、ファイアウォール には最新のユーザーマッピング情報が保管されるようになりま す。
	 このタイムアウトを有効化し、ファイアウォー ルが最新のユーザー対 IP アドレスのマッピング を必ず維持するようにしてください。
User-IDタイムアウト(分)	ユーザー マッピングエントリ用のタイムアウト値を分単位で 入力します(範囲は 1 ~ 3,600、デフォルトは 45)。
	 タイムアウトの値を DHCP リースの存続期間の 半分、あるいは Kerberos チケットの存続期間に 設定します。
	マッピング情報を再配信するようにファイア ウォールを設定すると、各ファイアウォールで は、転送ファイアウォールで設定されているタ イムアウトではなく、そのファイアウォールで 設定されているタイムアウトに応じて、受信し たマッピングエントリが削除されます。

キャッシュ設定	の意味
ドメインなしで一致する ユーザー名を許可する	ドメインが User-ID 送信元によって提供されない場合、ファイ アウォールがユーザーを照合できるようにするには、このオプ ションを選択します。ユーザーの誤認を防ぐため、ドメイン間 でユーザー名が重複していない場合にのみ、このオプションを 選択してください。
	 このオプションを有効にする前に、ファイア ウォールが LDAP サーバーからグループマッピ ングを取得したことを確認します。

Syslog のフィルタ

 デバイス > ユーザー ID > ユーザー マッピング > Palo Alto Networks User-IDエージェントの 設定 > Syslog のフィルタ

User-ID エージェントは、Syslog Parse プロファイルを使用して、エージェントが IP アド レスからユーザー名へのマッピング情報を監視する syslog 送信者から送信された syslog messages (Syslog メッセージ) C をフィルタリングします(「Configure Access to Monitored Servers (監視対象サーバーに対するアクセスの設定)」を参照)。各プロファイルでは、次の イベント タイプのいずれかの Syslog メッセージを解析できますが、両方とも解析することはで きません。

- 認証(ログイン)イベント ユーザー マッピングをファイアウォールに追加するために使用 します。
- ログアウトイベント 現行でなくなったユーザーマッピングを削除するために使用します。IPアドレスの割り当てが頻繁に変わる環境では、期限切れのマッピングを削除すると便利です。

Palo Alto Networks では、アプリケーション コンテンツ更新を通じてファイアウォールに事前 定義済み Syslog 解析プロファイルを提供しています。ベンダーが新しいフィルタを開発するた びにプロファイルのリストを動的に更新するには、これらの動的コンテンツ アップデートをス ケジュールします(「Device(デバイス)> Dynamic Updates(動的更新)」を参照)。事前 定義済みプロファイルはどのファイアウォールにでも適用できますが、設定したカスタム プロ ファイルは、Device(デバイス)> User Identification(ユーザー ID) > User Mapping(ユー ザーマッピング)で選択した仮想システム(Location(場所))にのみ適用されます。

User-ID エージェントが Syslog メッセージを解析するには、Syslog メッセージが次の条件を満たしている必要があります。

- 各メッセージは1行の文字列であること。改行(\n)または復帰と改行(\r\n)が行区切りの区切り文字であること。
- 各メッセージの最大サイズは 8,000 byte (バイト)であること。
- UDP上で送信されたメッセージは1つのパケットに含まれること。SSL上で送信されたメッ セージは複数パケットにまたがることができる。1つのパケットは複数のメッセージを含む ことができる。

カスタム プロファイルを設定する場合は、Add(追加)をクリックし、次の表で説明する設定 を指定します。この表のフィールドの説明では、次の形式になっている Syslog メッセージのロ グイン イベントの例を使用します。

[2005年7月5日(火) 13:15:04 CDT]管理者認証の成功 User:domain\johndoe_4 ソース:192.168.0.212

User-ID エージェントが Syslog 送信元のユーザー マッピング情報を解析するように 設定する完全な手順 Cでは、Syslog 解析プロファイルを作成する他にもさらにタス クが必要です。

項目	の意味
Syslog 解析プロファイル	プロファイルの名前を入力します(英数字最大63文字)。
の意味	プロファイルの説明を入力します(英数字最大255文字)。
タイプ	ユーザー マッピング情報をフィルタリングする解析のタイプ を指定します。
	 Regex Identifier(正規表現識別子) – Syslog メッセージからユーザーマッピング情報の特定と抽出を行うための検索パターンを示す正規表現(regex)を設定する場合は、Event Regex(イベント正規表現)、Username Regex(ユーザー名正規表現)、および Address Regex(アドレス正規表現)を指定します。ファイアウォールはSyslog メッセージ内の認証イベントまたはログアウトイベントを照合し、一致するメッセージ内のユーザー名とIPアドレスを照合する際に正規表現を使用します。 Field Identifier(フィールド識別子) – 認証イベントまたはログアウトイベントで照合を行う文字列を指定し、Syslog メッセージでユーザーマッピング情報を識別
	する場合は、Event String(イベント文字列)、Username Prefix(ユーザー名プレフィックス)、Username Delimiter(ユーザー名区切り文字)、Address Prefix(アド レスプレフィックス)、Address Delimiter(アドレス区切 り文字)、および Addresses Per Log(ログ毎のアドレス) のフィールドを使用します。
	ダイアログの残りのフィールドは、選択内容に従って変わりま す。次の行の説明に従ってフィールドを設定してください。
イベントの正規表現	成功した認証イベントまたはログアウト イベントを示す正規 表現を入力します。この表で使用するメッセージ例の場合、 正規表現 (authentication\ success) によって、文字列 authentication success の最初の {1} インスタンスが抽

項目	の意味
	出されます。スペースの前の円記号は、スペースを特殊文字と して扱わないように正規表現エンジンに指示する標準の正規表 現エスケープ文字です。
ユーザー名の正規表現	認証成功またはログアウトのメッセージのユーザー名フィー ルドを識別する正規表現を入力します。この表で使用するメッ セージ例の場合、正規表現 User:([a-zA-Z0-9\\\]+) は 文字列 User:johndoe_4 に一致し、acme\johndoe1 をユー ザー名として抽出します。
アドレスの正規表現	認証成功またはログアウトのメッセージの IP アドレス部分 を識別する正規表現を入力します。この表で使用するメッ セージ例では、正規表現 Source:([0-9]{1,3}\.[0-9] {1,3}\.[0-9]{1,3}\.[0-9]{1,3}) は IPv4 アドレス Source:192.168.0.212 と一致し、192.168.0.212 が IP ア ドレスとしてユーザー名マッピングに追加されます。
イベントの文字列	認証成功またはログアウトのメッセージを識別するために照合 する文字列を入力します。この表で使用するメッセージ例の場 合は、文字列 authentication success を入力します。
ユーザー名のプレフィック ス	認証またはログアウトの Syslog メッセージにおいて、ユー ザー名フィールドの先頭を識別するために照合する文字列を 入力します。このフィールドでは、\s (スペース) や \t (タ ブ)等の正規表現がサポートされません。この表で使用する メッセージ例では、User:によってユーザー名フィールドの 先頭を識別しています。
ユーザー名の区切り文字	認証またはログアウトのメッセージ内のユーザー名フィールドの終了を示すユーザー名の区切り文字を入力します。1つのスペースを示すには \s(メッセージ例を参照)、タブを示すには \tを使用します。
アドレス プレフィックス	Syslog メッセージで IP アドレス フィールドの先頭を識別す るために照合する文字列を入力します。このフィールドで は、\s(スペース)や \t(タブ)等の正規表現がサポートさ れません。この表で使用するメッセージ例では、Source: に より、アドレス フィールドの先頭が識別されています。
アドレスの区切り文字	認証成功またはログアウトのメッセージにおける IP アドレス フィールドの末尾を示すために使用される照合文字列を入力 します。たとえば、区切り文字が行区切りであることを示すに は、\n を入力します。

項目	の意味
Addresses Per Log ログ毎の	ファイアウォールで解析する IP アドレスの最大数を入力しま
アドレス数	す(デフォルトは 1、範囲は 1 ~ 3)。

ユーザーリストを無視

 デバイス>ユーザー ID>ユーザーマッピング> Palo Alto Networks User-IDエージェントの 設定>ユーザーリストを無視

除外ユーザーリストでは IP アドレスとユーザーネームのマッピングが不要なアカウントを定 義します(キオスク アカウントなど)。リストの設定を行う場合はAdd[追加] をクリックして ユーザー名を記入します。アスタリスクをワイルドカード文字として使用しte複数のユーザー ネームと一致させることが可能ですが、エントリの最後の文字としてのみ使用できます。たとえ ば、corpdomain\it-admin* は corpdomain のドメイン内で it#admin から始まるユーザー名をも つすべての管理者と一致します。ユーザーマッピングから除外するエントリを最大5,000個まで 追加することができます。



クライアントではなく、ユーザー ID エージェントであるファイアウォールの無視 ユーザーリストを定義します。クライアントファイアウォールで無視ユーザーリス トを定義した場合、リスト内のユーザーは再配布中にマッピングされます。

サーバーの監視

• Device > User Identification > User Mapping [デバイス > User-ID > ユーザーマッピング]

Microsoft Exchangeサーバー、Active Directory(AD)ドメインコントローラ、Novell eDirectoryサーバー、またはUser-IDエージェントがログインイベントの監視を行ってい るSyslog送信元などの定義を行う場合は、サーバーモニタリングセクションを使用します。

- 監視対象サーバーに対するアクセスの設定
- 監視対象サーバーに対するアクセスの管理
- ユーザーマッピングのサブネットワークの許可または除外

監視対象サーバーに対するアクセスの設定

Server Monitoring(サーバー モニタリング)セクションを使用して、ファイアウォールの監視 対象のサーバーを指定するサーバー プロファイルを Add (追加)します。

少なくとも 2 つの User-ID モニタ対象サーバを設定して、サーバがダウンした場合でも、firewall が IP address-to-username マッピングを学習できるようにします。



サーバーを監視するように PAN-OS 統合 User-ID エージェントを完全な手順で設定 するには、サーバー プロファイルの作成以外にいくつかの追加タスクを行う必要が あります。

サーバー モニタ リング設定	の意味		
氏名	サーバーの名前を入力します。		
の意味	サーバーの説明を入力します。		
enabled [有効 化]	このサーバーに対するログのモニタリングを有効化する場合はこのオプ ションを選択します。		
タイプ	 サーバータイプを選択します。選択内容により、このダイアログに表示されるフィールドが変わります。 Microsoft Active Directory Microsoft Exchange Novell eDirectory Syslog Sender 		
転送プロトコル (Microsoft ア クティブディ レクトリおよ び Microsoft Exchange の み)	 転送プロトコルを選択します: WMI - (デフォルト) Windows Management Instrumentation (WMI) を使用して、学習した各 IP アドレスを調査し、同じユーザーがまだログインしていることを確認します。 WinRM-HTTP - HTTP 経由で Windows リモート管理 (WinRM) を使用して、サーバー上のセキュリティ ログとセッション情報を監視します。firewall は、Kerberos セッション キーを使用してペイロードを暗号化します。 WinRM-HTTPS - HTTPS 経由で Windows Remote Management (WinRM) を使用して、サーバー上のセキュリティ ログとセッション情報を監視します。Kerberos 認証を使用して Windows サーバーとのサーバー証明書の検証を要求するには、グローバル サービス設定で NTP を構成し、証明書プロファイルで Root CA を選択してください (Device > User Identification > Connection Security)。 		
ネットワーク アドレス	監視対象サーバーのサーバー IP アドレスまたは FQDN を入力してくださ い。サーバー認証で Kerberos を使用する場合、FQDN を入力する必要があ ります。このオプションは、Type(タイプ)が Novell eDirectory の場合 にはサポートされていません。		
サーバ プロ ファイル (Novell eDirectory の み)	Novell eDirectory サーバーに接続するための LDAP サーバー プロファイル を選択します(Device (デバイス) > Server Profiles (サーバー プロファ イル) > LDAP)。		

サーバー モニタ リング設定	の意味
接続タイプ (<mark>Syslog</mark> 送信 元のみ)	User-ID エージェントが UDP ポート (514) と SSL ポート (6514) の どちらで Syslog メッセージをリッスンするかを選択します。SSL を選択 した場合、Enable Server Monitoring (サーバー モニタリングの有効化) で選択した Syslog Service Profile (Syslog サービス プロファイル) によ り、Syslog 送信元との接続保護のために許可される SSL/TLS バージョン と、ファイアウォールが使用する証明書が決まります。
	 PAN-OS 統合 User-ID エージェントを使用して IP アドレスからユーザー名へのマッピングを行う場合は、セキュリティのために SSL を選択することをお勧めします。UDP を選択する場合、Syslog 送信元とクライアントの両方が保護された専用のネットワーク上にあることを確認し、信頼されていないホストから UDP トラフィックをファイアウォールに送信できないようにしてください。
フィルタ (<mark>Syslog</mark> 送信 元のみ)	サーバー Type (タイプ) が Syslog Sender (Syslog 送信元) の場合、この サーバーから受信した Syslog メッセージからユーザー名および IP アドレ スを抽出する際に使用する Syslog 解析プロファイルを Add (追加) しま す。カスタム プロファイル (「Syslog フィルタの管理」を参照) または事 前定義済みプロファイルを追加できます。プロファイルごとに、以下のよ うに Event Type (イベント タイプ)を設定します。
	 login(ログイン) – User-ID エージェントはログイン イベントの Syslog メッセージを解析し、ユーザー マッピングを作成します。
	 logout(ログアウト) – User-ID エージェントはログアウト イベントの Syslog メッセージを解析し、現行でなくなったユーザー マッピングを削除します。IP アドレスが動的に割り当てられるネットワークでは、自動 削除によって、エージェントが各 IP アドレスを現在関連付けられている ユーザーに対してのみマッピングするようになるため、ユーザーマッピングの精度が向上します。
	事前定義済みの Syslog 解析プロファイルを追加する場合、名前を確認して、ログインとログアウトイベントのどちらへの一致を意図されているのか判断してください。
デフォルト ド メイン名 (<mark>Syslog 送信</mark> 元のみ)	(任意) サーバーの Type (タイプ) が Syslog Sender (Syslog 送信者) で ある場合は、ドメイン名を入力して、現在のドメイン名を Syslog メッセー ジのユーザー名に上書きするか、Syslog メッセージにドメインが含まれて いない場合はユーザー名に追加します。

監視対象サーバーに対するアクセスの管理

User-IDエージェントがユーザーマッピング情報の監視を行っているサーバーへのアクセスを制御する場合はサーバーモニタリングセクションで以下のタスクを行ってください。

タスク	の意味
ライセンス 情報の表示	それぞれの監視対象のサーバーにおいて、User Mapping (ユーザーマッピン グ)ページではUser-IDエージェントからサーバーへの接続状況が表示されま す。サーバーをAdd[追加] するとファイアウォールは接続を試みます。接続試 行が成功すると、サーバー モニタリング セクションの Status (状態) 列には Connected (接続済み)と表示されます。ファイアウォールから接続できな かった場合、Status (状態列)には Connection refused (接続が拒否され ました) や Connection timeout (接続タイムアウト) などのエラー状態 が表示されます。
	サーバー モニタリング セクションの他のフィールドの表示内容の詳細は、 「監視対象サーバーに対するアクセスの設定」を参照してください。
コンテキス トの	監視対象サーバーへのアクセスを設定する場合は、User-ID エージェントに マッピング情報を監視させるサーバーをそれぞれ Add(追加)します。
削除しま す。	ユーザーマッピング処理(検出)からサーバーを削除したい場合は、そのサー バーを選択し、Delete[削除]します。 ヒント:設定内容を消去せずに「検出」からサーバーを削除する場合は、サー バーエントリの編集を行い、Enabled[有効化]の選択を解除します。
知っておく べき最も重 要な十ヶ条 を	Microsoft Active Directoryドメインコントローラは、DNSを使用して自動的 にDiscover[検出] することができます。ファイアウォールは、Device(デ バイス) > Setup(セットアップ) > Management(管理)のページにある General Settings(一般設定)セクションの Domain(ドメイン)フィールド に入力したドメイン名に基づいてドメイン コントローラを検出します。ファ イアウォールはドメインコントローラを検出するとサーバーモニタリングリス トにエントリを作成するので、それを使用してサーバーを監視対象に追加する ことができます。
	Discover[検出] 機能はドメインコントローラのみに使用できます。ExchangeサーバーやeDirectoryサーバーには使用できません。

ユーザーマッピングのサブネットワークの許可または除外

• Device > User Identification > User Mapping [デバイス > User-ID > ユーザーマッピング]

IPアドレスからユーザー名へのマッピング(検出)を行う際にUser-IDエージェントが許可/除 外するサブネットワークを定義する場合は、「許可/除外ネットワーク」リストを使用します。 デフォルト設定において、このリストにサブネットワークを追加していない場合、パブリック IPv4 アドレスをもつクライアント システムで WMI プローブを行う場合を除き、User-ID エー ジェントはすべてのサブネットワークを対象として User-ID の送信元の検出を試行します。(パ ブリック IPv4 アドレスは RFC 1918 および RFC 3927 の範囲外にあるものを指します)

パブリックIPv4アドレスにおけるWMIプローブを有効化する場合は、これらのサブネットワークをリストに追加し、Discovery[検出] オプションをInclude[許可] に設定する必要があります。 他のファイアウォールにユーザーマッピング情報を再配信する C ようにファイアウォールを構成すると、リストで指定した検出制限が再配信される情報に適用されます。



含有および除外リストを使用し、ファイアウォールがユーザーマッピングを使用す るサブネットを定義します。

許可/除外ネットワークリストでは以下のタスクを行うことができます。

タスク	の意味
コンテキスト の	検出を特定のサブネットワークに制限したい場合は、サブネットワークプロ ファイルをAdd[追加] し、以下のフィールドを入力します。
	• Name[名前] – サブネットワークの識別に使用する名前を入力します。
	• Enabled[有効] – サーバー監視の際のサブネットワークの許可や除外を有 効化する場合はこのオプションを選択します。
	 Discovery[検出] – User-IDエージェントがサブネットワークをInclude[許可] するかExclude[除外] するかを選択します。
	 Network Address[ネットワークアドレス] – サブネットワークのIPアドレスの範囲を入力します。
	ユーザー ID エージェントは、すべてを除外という暗黙のルールをリスト に適用します。たとえば、Include(許可)オプションを指定してサブネッ トワーク 10.0.0.0/8 を追加すると、User-ID エージェントは、その他すべ てのサブネットワークがリストに追加されていない場合もこれらを除外し ます。Exclude[除外]オプションを指定してエントリを追加するのは、明 示的に包含したサブネットワークの一部を除外する場合だけです。たとえ ば、Include[包含]オプションを指定して 10.0.0.0/8 を、Exclude[除外]オプ ションを指定して 10.2.50.0/22 を追加すると、ユーザー ID エージェント は、10.0.0.0/8 内のサブネットワークのうち 10.2.50.0/22 を除くすべてを検 出し、10.0.0.0/8 外のすべてのサブネットワークを除外します。Include[許 可] プロファイルを一切追加せずに Exclude[除外] プロファイルを追加する と、User-IDエージェントは、追加したサブネットワークだけでなく、すべて のサブネットワークを除外します。
削除します。	リストからサブネットワークを削除する場合は、それを選択して Delete [削 除] します。

タスク	の意味
	ヒント:設定内容を消去せずに「許可/除外ネットワークリスト」からサブ ネットワークを削除する場合は、サブネットワークプロファイルの編集を行 い、Enabled[有効化] の選択を解除します。
カスタム許 可/除外ネッ トワーク	デフォルトでは、ユーザーIDエージェントは、追加された順(上から下)に サブネットワークを評価します。評価順を変更するには、Custom Include/ Exclude Network Sequence[許可/除外ネットワーク カスタム シーケンス] をクリックします。次に、サブネットワークに対してAdd[追加]、Delete[削 除]、Move Up[上へ]、Move Down[下へ]の各コマンドを実行して、カスタム の評価順を作成します。

Device (デバイス) > User Identification (User-ID) > Connection Security (接続のセキュリティ)

User-ID 接続セキュリティ設定の編集 () で、ファイアウォールが使用する証明書プロファイルを選択し、Windows User-ID エージェントによって提供された証明書を検証します。ファイアウォールは、選択した証明書プロファイルを使用して User-ID エージェントの ID を検証します。これは、エージェントによって提供されたサーバー証明書を検証することで実現します。

タスク	の意味
User-ID 証明 書プロファ イル	ドロップダウンから、Windows User-ID エージェントを認証するときに 使用する証明書プロファイルを選択するか、New Certificate Profile(新 規証明書プロファイル)を選択して新しい証明書プロファイルを作成しま す。None(なし)を選択すると、証明書プロファイルが削除されて、代わり にデフォルトの認証が使用されます。 サーバー認証に監視対象サーバーに対するアクセスの設定Kerberos を使用す るときに Windows サーバーとのサーバー証明書の検証を要求するには、グ ローバル サービス設定 で NTP を構成し、証明書プロファイルとして Root CA を選択してください。
Remove All(すべて 削除)(テ ンプレート 設定のみ)	選択したテンプレートの User-ID 接続セキュリティ設定に割り当てられた証明 書プロファイルを削除します。

Device (デバイス) > User Identification (ユーザーID) > Terminal Server Agents (ターミナル サーバー エージェ ント)

同じ IPアドレスを共有する複数のユーザーをサポートしているシステムでは、ターミナル サー バー (TS) エージェントはそれぞれのユーザーにポート レンジを割り当てることで各ユーザーを 識別します。ファイアウォールがユーザーおよびユーザー グループに基づいたポリシーを適用 できるよう、TS エージェントは、接続されているすべてのファイアウォールに対し、ユーザー に割り当てられたポート レンジを通知します。

すべてのファイアウォール モデルで最大 5,000 個のマルチユーザー システムからユーザー名と ポートのマッピング情報を収集できます。ファイアウォールがマッピング情報を収集できる TS エージェントの数は、firewall model(ファイアウォール モデル)によって異なります。



TSエージェントへのアクセスを設定する前に、TSエージェントのインストールと設 定を行う必要があります。ターミナルサーバーユーザー用のユーザーマッピング を完全な手順で設定する場合は、TSエージェントへの接続の設定の他に、いくつか の追加タスクを行う必要があります。

TSエージェ	ントへのア	クセスを制御す	る場合は以下の	Dタスクを実行し	ます。
--------	-------	---------	---------	----------	-----

タスク	の意味
情報を表示 / 接続対象の 更新	Terminal Server Agents (ターミナル サーバー エージェント)のページにおい て、Connected (接続済) 列にはファイアウォールから TSエージェントへの接 続ステータスが表示されます。緑のアイコンが表示されている場合は正常に接 続されていることを示し、黄色いアイコンの場合は接続が無効、赤いアイコン の場合は接続に失敗したことを意味します。ページを開いてから接続状態が変 化した可能性がある場合は、Refresh Connected [接続対象の更新] をクリック して表示を更新します。
コンテキス トの	TS エージェントへのアクセスを設定する場合は、エージェントを Add(追 加)し、以下のフィールドを設定します。
	• Name (名前) – TS エージェントの識別に使用する名前を入力します(最 大31文字)。名前の大文字と小文字は区別されます。また、一意の名前に する必要があります。文字、数字、スペース、ハイフン、およびアンダー スコアのみを使用してください。
	 Host (ホスト) – TS エージェントがインストールされているターミナルサー バーの静的 IP アドレスあるいはホスト名を入力します。
	 Port(ポート) – TS エージェント サービスがファイアウォールと通信する際に使用するポート番号を入力します(デフォルトは 5009)。
	• Alternative IP Hosts(代替 IP ホスト) – TS エージェントがインストール されているターミナル サーバーに、送信トラフィックの送信元 IP アドレス

タスク	の意味
	として表示される可能性がある IP アドレスが複数ある場合、最大 8 個の静 的 IP アドレスあるいはホスト名を Add(追加)および入力します。
	 Enabled(有効化) – ファイアウォールがこの TS エージェントと通信でき るようにする場合は、このオプションを選択します。
削除しま す。	TSエージェントへの接続を可能にしている設定内容を削除する場合は、その エージェントを選択し、Delete[削除] をクリックします。
PDF/CSV	最低限の読み取り専用アクセス権を持つ管理ロールは、デバイス設定バンドル を PDF/CSV としてエクスポートできます。フィルターを適用して、監査など のためのより具体的な表構成出力を作成することができます。Web インター フェイスで表示可能な列のみがエクスポートされます。「Configuration Table Export(設定バンドルのエクスポート)」を参照してください。
Device > User Identification > Group Mapping Settings [デバイス > User-ID > グループマッピングの設定]

• デバイス > ユーザー ID > グループ マッピング設定

ユーザーとユーザー グループに基づいてセキュリティ ポリシーやレポートを定義する場合 は、ディレクトリ サーバーで指定および管理されるグループのリストと対応するメンバーのリ ストをファイアウォールで取得する必要があります。ファイアウォールは、Microsoft Active Directory (AD) 、Novell eDirectory、Sun ONE Directory Server を含む、さまざまな LDAP ディレクトリ サーバーをサポートしています。

各ファイアウォールまたは Panorama がすべてのポリシーで参照できる個別ユーザー グループ の数は model(モデル)によって異なります。しかし、モデルに関わらず、グループ マッピン グ設定を作成する前に LDAP サーバープロファイルを設定する必要があります(Device (デバイ ス) > Server Profiles (サーバープロファイル) > LDAP)。



ユーザー名をグループにマッピングする完全な手順では、グループマッピング設定 の作成の他に、いくつかの追加タスクを行う必要があります。

必要に応じて以下のフィールドを入力してAdd (追加)し、グループマッピング設定を作成します。グループマッピング設定を削除する場合は、当該のものを選択して Delete (削除)します。グループマッピング設定を削除せずに無効化したい場合は、設定の編集を行い Enabled (有効化)オプションの選択を解除します。

 同じ Distinguished Name (識別名-DN)または LDAP サーバーを使用する複数のグ ループマッピング設定を作成する場合、グループマッピング設定に重複するグ ループを含めることはできません (例えば、1つのグループマッピング設定の追加リ ストに、異なるグループマッピング設定する等)。

グループマッピ ング設定 – サー バープロファイ ル	設定場所	の意味
氏名	デバイス > ユーザー ID > グ ループ マッピング設定	グループマッピング情報の識別に使用する 名前(最大31文字)を入力します。名前の 大文字と小文字は区別されます。また、一 意の名前にする必要があります。文字、数 字、スペース、ハイフン、およびアンダー スコアのみを使用してください。
サーバ プロファ イル	デバイス > ユーザー ID > グループ マッピング設定 > サーバ プロファイル	このファイアウォールのグループ マッピン グに使用する LDAP サーバー プロファイル を選択します。

グループマッピ ング設定 – サー バープロファイ ル	設定場所	の意味
更新間隔		ファイアウォール ポリシーが使用するグ ループの更新情報を取得するため、ファイ アウォールが LDAP ディレクトリ サーバー と接続を行う間隔を秒数で指定します(範 囲は 60 ~ 86,400 秒)。
ユーザー ドメイ ン		 デフォルトでは、User Domain (ユーザードメイン)は空白になっています。空白のままにすると、ファイアウォールが、Active Directory サーバーのドメイン名を自動的に検出します。このフィールドに値を入力した場合、ファイアウォールがLDAPソースから取得したドメイン名はオーバーライドされます。入力値には NetBIOS 名を指定する必要があります。 このフィールドは、LDAP
Group Objects(グルー プ オブジェク ト)		 Search Filter[検索フィルタ] – LDAPクエ リを入力し、取得および追跡の対象とす るグループを指定します。 Object Class[オブジェクトクラス] – グ ループの定義を入力します。デフォルト はobjectClass=groupで、グループSearch Filter[検索フィルタ] に一致するディレク

グループマッピ ング設定 – サー バープロファイ ル	設定場所	の意味
		定されているすべてのオブジェクトが取 得されます。
User Objects		 Search Filter[検索フィルタ] – LDAPクエ リを入力し、取得および追跡の対象とす るユーザーを指定します。 Object Class[オブジェクトクラス] – ユーザーオブジェクトの定義を入力し ます。たとえば、Active Directory の場 合、objectClass はuserになります。
enabled [有効化]		グループマッピングにおけるサーバープロ ファイルを有効化する場合はこのオプショ ンを選択します。
管理対象デバイ スのリストを取 得		GlobalProtect デプロイメントの場合、こ のオプションを選択してファイアウォー ルがディレクトリ サーバー(アクティブ ディレクトリなど)からシリアル番号を 取得できるようにします。そうすること で、GlobalProtect が接続中のエンドポイン トのステータスを識別子、エンドポイント のシリアル番号の有無に基づいて HIP ベー スのセキュリティ ポリシーを適用できるよ うになります。
ユーザー属性	Device > User Identification > Group Mapping Settings > User and Group Attributes	ユーザーを識別するためにディレクトリ属 性を指定します。 • Primary ユーザー名 – User-ID ソースが ユーザー名に提供する属性を指定します

グループマッピ ング設定 – サー バープロファイ ル	設定場所	の意味
		(たとえば、userPrincipalName また は sAMAccountName)
		 プライマリユーザー名 は、firewall が U1ser-ID ソースから他の形式を受け 取った場合でも、firewall がログ、レポート、お よびポリシー構成でユー ザーを識別する方法です。 フォーマットを指定しな い場合、ファイアウォー ルはデフォルトでActive DirectoryにsAMAccountNameフォー マットを使用し、Novell eDirectoryとSun ONE Directory Serverにuidフォーマット を使用します。
		 E-Mail (メール)–User-ID のソースがメー ルアドレス用に提供する属性を指定しま す。デフォルトは mail です。
		 Alternate ユーザー名 1-3 – User-ID ソースが送信できる形式に対応する属性 を最大 3 つまで指定します。
		Active Directory サーバー を構成する場合、Alternate Username 1 は既定で userPrincipalName で す。
グループ属性		User-ID のソースがグループを識別するために使用する属性を指定します:
		 Group Name (グループ名)–User-ID の ソースがグループ名属性用に使用する 属性を指定します。アクティブディレ クトリ のデフォルトはname で、Novell eDirectory または Sun ONE Directory Server のデフォルトはcnです。

グループマッピ ング設定 – サー バープロファイ ル	設定場所	の意味
		 Group Member (グループメンバー)– User-ID のソースがグループメンバー用 に使用する属性を指定します。デフォル トは member です。 E-Mail (メール)–User-ID のソースがメー
		ルアドレス用に使用する属性を指定しま す。デフォルトは mail です。
使用可能なグ ループ 含まれたグルー プ	デバイス > ユーザー ID > グ ループ マッピング設定 > グ ループインクルードリスト	 セキュリティルールの作成時にファイアウォールが表示するグループの数を制限する場合は、これらのフィールドを入力してください。LDAPツリーを探索して、ルールで使用するグループを見つけます。グループを含めるには、グループを含めるには、グループを選択して Available Groups (利用可能なグループ)リストに追加します(グループをリストから削除するには、グループを Included Groups (含めるリスト)で選択して削除します(ファイアウォールが LDAP ディレクトリツリー全体からでなく、必要なグループからのみユーザーグループマッピングを取得できるよう、必要なグループだけを含めてください。
氏名	デバイス > ユーザー ID > グ ループマッピング設定 > カ	LDAP ディレクトリ内の既存のユーザー グ ループに一致しないユーザー属性に基づい
LDAP フィルタ	スタムグループ	 てファイアウォール ポリシーを設定できる よう、LDAP フィルタに基づいてカスタム グループを作成します。 User-ID サービスは、フィルタに一致する すべての LDAP ディレクトリ ユーザーを カスタム グループにマッピングします。 既存のアクティブディレクトリグループ ドメイン名と同じ識別名 (DN)のカスタム ムグループを作成すると、ファイアウォー

0

0

グループマッピ	 設定場所	の意味
ング設定 – サー バープロファイ ル		
		ルは、その名前が参照されるすべての場所 (たとえば、ポリシーやログ内)でカスタ ムグループを使用します。カスタムグルー プを作成する場合は、以下のフィールドを 設定してAdd (追加)します。
		 Name[名前] – 現在のファイアウォール または仮想システムにおけるグループ マッピング設定の中で一意のカスタムグ ループ名を入力します。
		 LDAP Filter[LDAPフィルタ] – 最 大2,048文字のフィルタを入力します。
		 LDAP 検索を高速化し て、LDAP ディレクトリ サーバーのパフォーマンスの低下 を最小限に抑えるには、索引 付きの属性のみをフィルタに 使用します。LDAP フィルタ はファイアウォールで検証されません。
		Included Groups (含まれたグループ)リ ストと Custom Group (カスタム グルー プ)リストの合計最大数は 640 エントリで す。
		カスタム グループを削除するには、グルー プを選択して Delete (削除)します。カ スタム グループのコピーを作成する場合 は、任意のグループを選択して Clone (コ ピー)してから、必要に応じフィールドを 編集します。
		 カスタム グループを追加またはコピーしたら、変更を <i>Commit</i>(コミット)して、 新しいカスタム グループをポリシーやオブジェクトで使用できるようにする必要があります。

デバイス>ユーザーの識別>信頼できる送信元アドレス

Explicit Proxy では、特定の IP アドレスからのトラフィックのみが X-Authenticated-User (XAU) プロトコルを使用して認証されます。address object を作成し、次に Edit を信頼できる送信元 アドレス構成を作成し、アドレス オブジェクトを追加して、明示的なプロキシの認証に XAU を許可する IP アドレスを指定します。詳細については、「Secure Mobile Users with an Explicit Proxy」を参照してください。

信頼できる送信元アドレス フィールド	詳説	
有効化	信頼できる送信元アドレスの構成を有効にす るには、このオプションを選択します。	
信頼できる送信元アドレス	Add 信頼できる送信元アドレス。これらの送 信元アドレスからの着信要求に含まれる X- Authenticated-User (XAU) は、明示的プロキ シに対して信頼されます。	
	必要に応じて、信頼できる送信元アドレス の一覧を Search したり、送信元アドレスを Delete したりすることもできます。	

Device (デバイス) > User Identification (ユーザー ID) > Authentication Portal Settings (認証ポータルの 設定)

Authentication Portal (認証ポータル) で SSL/TLS サービス プロファイル (Device (デバイス) > Certificate Management (証明書の管理) > SSL/ TLS Service Profile (SSL/TLS サービス プロファイル))、認証プロファイル (Device (デバイス) > Authentication Profile (認証プロファイル))、または 証明書プロファイル (Device (デバイス) > Certificate Management (証明書の管 理) > Certificate Profile (証明書プロファイル)) を使用する場合、開始前にプロ ファイルを設定します。Authentication Portal (認証ポータル)を完全な手順 で設 定する場合は、これらのプロファイルの設定に加え、いくつかの追加タスクを行う 必要があります。

認証ポリシーを適用するには、*Enable Authentication Portal*(認証ポータルの有効化)を行う必要があります(「Policies(ポリシー) > Authentication(認証)」を 参照)。

項目	の意味
Enable Authentication Portal(認証 ポータルの有効 化)	Authentication Portal(認証ポータル)を有効化する場合は、このオプショ ンを選択します。
アイドル タイ マー (分)	Authentication Portal (認証ポータル) セッション用のユーザー TTL (time-to-live) を分単位で入力します (範囲は 1 ~ 1,440、デフォル トは 15) 。このタイマーは、Authentication Portal (認証ポータル) ユー ザーのアクティビティが発生するたびにリセットされます。ユーザーのア イドル時間が Idle Timer (アイドル タイマー)の値を超えると、PAN-OS はAuthentication Portal (認証ポータル) ユーザー マッピングを削除する ため、そのユーザーは再びログインを行う必要があります。
タイマー (分)	これは TTL の最大値を分単位で示すもので、Authentication Portal(認証 ポータル)セッションのマッピングが保持される最大の時間となります (範囲は 1 ~ 1,440、デフォルトは 60)。この時間が経過するとPAN- OSはマッピングを削除するので、セッションがまだアクティブな状態で あっても、ユーザーは再度認証を行う必要があります。このタイマーは期

項目	の意味
	限切れのマッピングをなくすためのものであり、Idle Timer(アイドル タ イマー)の値をオーバーライドします。
	失効 Timer (タイマー) は常に Idle Timer (アイドルタイ マー) よりも長く設定してください。
SSL/TLS Service Profile	リダイレクト要求をセキュリティ保護するためのファイアウォール サーバー証明書と許可されたプロトコルを指定するには、SSL/TLS サー ビスプロファイルを選択します(Device(デバイス) > Certificate Management(証明書の管理) > SSL/TLS Service Profile(SSL/TLS サービ スプロファイル))。None(なし)を選択した場合、ファイアウォールは SSL 接続にローカルのデフォルト証明書を使用します。
	 SSL/TLS Service Profile (SSL/TLS サービス プロファイル) でMin Version (最低バージョン)をTLSv1.2に、Max Version (最大バー ジョン)をMax (最大)に設定し、SSL/TLS プロトコルの脆弱性 を最大限に保護します。Max Version (最大バージョン)をMax (最大)に設定することで、より強固なプロトコルが利用できる ようになり次第、ファイアウォールが必ず最新のバージョン を使用するようになります。
	証明書エラーを表示せずに透過的にユーザーをリダイレクトするに は、Web要求のリダイレクト先となるインターフェイスの IPアドレスと 一致する証明書に関連付けられたプロファイルを割り当てる必要がありま す。
認証プロファイ ル	認証プロファイル (Device (デバイス) > Authentication Profile (認 証プロファイル))を選択して、トラフィックが認証ポリシー ルール (Policies (ポリシー) > Authentication (認証))に一致する場合にユー ザーを認証できます。ただし、Authentication Portal Settings (認証ポータ ルの設定)で選択した認証プロファイルは、いずれかのデフォルトの認証 実施オブジェクト (Objects (オブジェクト) > Authentication (認証)) を参照するルールにのみ適用されます。初期状態ではすべての認証ルール がデフォルトのオブジェクトを参照しているため、これは一般的に PAN- OS 8.0 にアップグレードした直後が適しています。カスタム認証実施オブ ジェクトを参照するルールの場合、オブジェクトの作成時に認証プロファ イルを選択します。
インバウン ド認証プロ ンプト用の GlobalProtect ネットワーク ポート (UDP)	GlobalProtect [™] が多要素認証(MFA)ゲートウェイからインバウ ンド認証プロンプトを受信するために使用するポートを指定しま す。(range is 1 to 65,536; default is 4,501).多要素認証をサポートす るには、GlobalProtect エンドポイントは MFA ゲートウェイからの インバウンド UDP プロンプトを受信および承認する必要がありま す。GlobalProtect エンドポイントが指定のネットワーク ポートで、信頼 できるファイアウォールまたはゲートウェイから UDP メッセージを受

項目	の意味
	信すると、GlobalProtect は認証メッセージを表示します(「Customize the GlobalProtect Agent(GlobalProtect エージェントのカスタマイ ズ) で を参照)。
モード	firewall が認証のための Web 要求をキャプチャする方法を選択します。
	 Transparent – firewall は認証ルールに従って Web 要求をインターセプトし、元の宛先 URL を偽装して、HTTP 401 メッセージを発行してユーザーに認証を求めるプロンプトを表示します。ただし、ファイアウォールには宛先 URL の実際の証明書がないため、保護されたサイトへのアクセスを試みるユーザーのブラウザには証明書エラーが表示されます。したがって、このモードは、Layer 2 や仮想ワイヤの展開など、絶対に必要な場合にのみ使用してください。
	 Redirect – firewall は認証ルールに従って Web リクエストをインター セプトし、指定された リダイレクトホスト にリダイレクトします。 ファイアウォールは HTTP 302 リダイレクトを使用して、ユーザーに 認証を求めるプロンプトを表示します。リダイレクトは優れたエンド ユーザーエクスペリエンスを提供するため(Redirect (リダイレクト)は タイムアウトが失効した際にリマップしないため、証明書エラーを表 示せず、ブラウジングをシームレスにするセッション Cookie を許可し ます)、Redirect (リダイレクト)を使用することがベストプラクティス になります。ただし、入力 Layer 3 インターフェイスに割り当てられた Interface Management プロファイルで応答ページを有効にする必要があ ります (詳細については、Network > Network Profiles > Interface Mgmt および PA-7000 Series Layer 3 Interface を参照してください)。
	リダイレクトモードのもう1つの利点は、セッション Cookie が使用でき ることで、ユーザーはタイムアウトの期限が切れるたびに再マッピングを 行うことなく、認証済みサイトの閲覧を続行できます。ある IP アドレスか ら別の IP アドレス(企業 LAN から無線ネットワークなど)にローミング するユーザーは、セッションが開かれている限り IP アドレスが変化しても 再認証する必要がないため、このモードが特に役立ちます。
	ブラウザーが信頼済みサイトにのみ資格情報を提供するため、認証ポータルが Kerberos SSO を使用する場合、リダイレクト モードが必要です。リダイレクト モードは、認証ポータルが多要素認証 (MFA)を使用する場合にも必要です。
セッション Cookie	 Enable[有効化] – セッションCookieを有効にする場合は、このオプションを選択します。
(リダイレクト モードのみ)	

項目	の意味	
	 Timeout[タイムアウト] – セッションCookieがEnable[有効化] されている場合、このタイマーで設定する値がCookieが有効な時間(分)となります(範囲は60~10080、デフォルトは1,440)。 	
	 タイムアウトの値を十分短く設定し、ユーザーマッピン グの項目が古くならず、かつ単一のセッション中にユー ザーにログインを複数回求めないようにすることで優れた ユーザーエクスペリエンスを提供できるだけの長さにしま す。480 分(8時間)以下の値から始め、必要に応じて値 を調整します。 	
	 Roaming(ローミング) – セッションがアクティブな間に IP アドレス が変化しても Cookie を保持させたい場合(エンドポイントが有線ネッ トワークから無線ネットワークに移動した場合など)は、このオプショ ンを選択します。ユーザーは、Cookieがタイムアウトになった場合また はブラウザを閉じた場合に再認証を行う必要があります。 	
ホストのリダイ レクト (リダイレクト モードのみ)	ファイアウォールがWeb要求をリダイレクトする宛先となるレイヤー3イン ターフェイスの、IPアドレスに解決されるイントラネットホスト名を指定 します。	
	 ユーザーが Kerberos シングル サインオン (SSO) で 認証を行う場合、Redirect Host (ホストのリダイレクト)は、Kerberos キータブで指定したホスト名と同じにする 必要があります。 	
証明書プロファ イル	証明書プロファイル(Device(デバイス) > Certificate Management(証 明書の管理) > Certificate Profile(証明書プロファイル))を選択 して、トラフィックが認証ポリシー ルール(Policies(ポリシー) > Authentication(認証))に一致する場合にユーザーを認証できます。	
	この認証タイプの場合、Authentication Portal(認証ポータル)はユーザー のエンドポイント ブラウザにクライアント証明書の提供を求めるプロンプ トを表示します。そのため、クライアント証明書を各ユーザー システムに デプロイする必要があります。さらに、ファイアウォールにクライアント 証明書を発行した認証局(CA)証明書をインストールして、CA 証明書を 証明書プロファイルに割り当てる必要があります。これは、Mac OSおよび Linux エンドポイントで Transparent(メッセージを表示しない)認証を有 効にする唯一の認証方法です。	

デバイス>ユーザー識別>クラウド ID エンジン

Add クラウド ID エンジン プロファイルをファイアウォールに接続し、クラウド ID エンジンを ユーザー識別情報のソースとして使用します。Cloud Identity Engine プロファイルを作成する場 合、Cloud Identity Engine アプリで構成したオンプレミスまたはクラウドベースのディレクトリ のユーザーおよびグループ情報に基づいて、ユーザーベースまたはグループベースのセキュリ ティポリシーを適用できます。また、削除 プロファイルを作成するか、現在のクラウド ID エン ジン プロファイルの PDF/CSV をエクスポートすることもできます。

ファイアウォール上で Cloud Identity Engine プロファイルを構成するには、install デ バイス証明書と activate のハブ上のクラウド ID エンジン インスタンスを構成する 必要があります。

プロファイルを検索するには、フィルター (Q) および フィルタの適用 (→) としてキーワードを 入力します。

Cloud Identity Engine 設定	の意味
氏名	クラウド ID エンジン プロファイルに 名前 (最大 31 文字) を入力します。名前の大文字と小文字は区別さ れます。また、一意の名前にする必要があります。文 字、数字、スペース、ハイフン、およびアンダースコ アのみを使用してください。
インスタンス	Cloud Identity Engine プロファイルを設定するには、 次の情報を入力します。
	 Region- Cloud Identity Engine インスタンスのリージョン エンドポイントを選択します。
	選択するリージョンは、Cloud Identity Engine インスタンスを activate するときに選択したリージョ ンと一致する必要があります。
	 Cloud Identity Engine インスタンス – 複数のイン スタンスがある場合は、使用する Cloud Identity Engine インスタンスを選択します。
	 ドメイン-使用するディレクトリが含まれているドメインを選択します。
	 Update Interval (分) – firewall が DS からの更新 を入力します。デフォルトは 60 分で、範囲は 5 ~ 1440 です。

Cloud Identity Engine 設定	の意味
	Cloud Identity Engine プロファイルの構成が終了した ら、プロファイルが Enabled であることを確認しま す。
ユーザー属性	各ユーザー属性 名前 に ディレクトリ属性 を選択しま す。プライマリ ユーザー名 を選択する必要がありま す。その他のフィールドはすべてオプションです。
グループ属性	グループ属性 名前 ごとに ディレクトリ属性 を選択し ます。グループ名 を選択する必要があります。残り のフィールドはオプションです。
デバイス属性	(GlobalProtect のみ)) GlobalProtect を使用していてシ リアル番号の確認を有効にしている場合は、エンド ポイントシリアル番号 を選択して、クラウド ID エン ジンが管理対象エンドポイントからシリアル番号を収 集できるようにします。この情報は、エンドポイント が GlobalProtect によって管理されていることを確認 するために、ディレクトリにシリアル番号が存在する かどうかを確認するために GlobalProtect ポータルに よって使用されます。

1166

TECH**DOCS**

GlobalProtect

GlobalProtect[™] はモバイル ユーザーを管理する完全なインフラストラクチャを提供し、使用しているデバイスや場所にかかわらず、すべてのユーザーの安全なアクセスを可能にします。以下のファイアウォール Web インターフェイス ページでは、GlobalProtect の構成要素を設定および管理できます。

- Network > GlobalProtect > Portals [ネットワーク > GlobalProtect > ポータル]
- Network > GlobalProtect > Gateways [ネットワーク > GlobalProtect > ゲートウェイ]
- Network > GlobalProtect > MDM [ネットワーク > GlobalProtect > MDM]
- Network (ネットワーク) > GlobalProtect > Clientless Apps (クライアントレス アプリケーション)
- Network (ネットワーク) > GlobalProtect > Clientless App Groups (クライアントレスアプ リケーション グループ)
- Objects > GlobalProtect > HIP Objects [オブジェクト > GlobalProtect > HIP オブジェクト]
- Objects > GlobalProtect > HIP Profiles [オブジェクト > GlobalProtect > HIP プロファイル]
- Device > GlobalProtect Client [デバイス > GlobalProtect クライアント]

その他の情報をお探しですか?

GlobalProtect インフラストラクチャのセットアップ詳細、ポリシーを適用するためのホスト 情報の使用方法、一般的な GlobalProtect のデプロイの設定手順といった GlobalProtect の詳細 は「GlobalProtect Administrator's Guide(GlobalProtect 管理者ガイド)『」を参照してくださ い。

Network > GlobalProtect > Portals [ネットワーク > GlobalProtect > ポータル]

GlobalProtect[™] ポータルのセットアップと管理を行うには、Network(ネットワーク) > GlobalProtect > Portals(ポータル)を選択します。このポータルは、GlobalProtect インフラス トラクチャの管理機能を提供します。GlobalProtect ネットワークに参加するすべてのエンドポ イントは、その設定をポータルから受信します。これには、使用可能なゲートウェイの情報や、 アプリでゲートウェイへの接続に必要になるクライアント証明書に関する情報が含まれます。 ポータルは更に、macOS および Windows エンドポイント用の GlobalProtect アプリ ソフトウェ アの動作と配布を制御しています。Linux エンドポイントの場合、サポート サイトからソフト ウェアを入手する必要があります。たとえば、モバイルデバイス用の GlobalProtect アプリケー ションは、iOS デバイスの場合は Apple App Store を通じて配布され、Android デバイスの場合 は Google Play を通じて配布され、Windows Phone および他の Windows UWP デバイスの場合 は Microsoft ストアを通じて配布されます。また、Chromebook 用の GlobalProtect アプリケー ションは、Chromebook Management Console または Google Play を通じて配布されます。

ポータル設定を追加するには、Add[追加] をクリックして GlobalProtect Portal [GlobalProtect ポータル] ダイアログを開きます。

確認すべき情報	以下を参照
GlobalProtectポータル用に設定す る必要がある一般設定	GlobalProtect ポータルの General(全般)タブ
ポータル設定に認証プロファイルを 割り当てる方法	GlobalProtect ポータルの Authentication (認証) タブ
GlobalProtect アプリケーションが エンドポイントから収集するデータ をどうすれば定義できますか?	GlobalProtect ポータルの Portal Agent Data Collection(ポータル データ収集)タブ
設定可能なクライアント認証のオプ ション	GlobalProtect ポータルの Agent Authentication(エー ジェント認証)タブ
オペレーティングシステム、ユー ザー、および(または)ユーザーグ ループを指定し、特定のデバイスグ ループに対して設定を割り当てる方 法	GlobalProtect ポータルの Agent Config Selection Criteria(エージェント設定の選択条件)タブ
内部ゲートウェイの設定と優先順位 を指定する方法	GlobalProtect ポータルの Agent Internal(エージェン ト内部)タブ
外部ゲートウェイの設定と優先順位 を指定する方法	GlobalProtect ポータルの Agent External(エージェン ト外部)タブ

確認すべき情報	以下を参照
異なるタイプのユーザー用に個別の クライアント設定を作成する方法	GlobalProtect ポータルの Agent (エージェント) タブ
GlobalProtect アプリの表示設定と 動作設定のうちカスタマイズ可能な 項目	GlobalProtect ポータルの Agent App(エージェント ア プリケーション)タブ
データ収集オプションの設定方法	GlobalProtect ポータルの Agent Data Collection(エー ジェント データ収集)タブ
GlobalProtect アプリをインストー ルしなくても Web アプリケー ションにアクセスできるように GlobalProtect ポータルを設定する 方法	GlobalProtect ポータルの Clientless VPN (クライアント レス VPN) タブ
サテライトとして動作するファイア ウォールまでVPN接続を延長する方 法	GlobalProtect ポータルの Satellite (サテライト) タブ
その他の情報をお探しですか?	ポータルのセットアップ手順の詳細は、 『GlobalProtect Administrator's Guide(GlobalProtect 管理者ガイド)』の「Configure a GlobalProtect Portal(GlobalProtect ポータルの設定)」を参照して ください。

GlobalProtect ポータルの General (全般) タブ

• ネットワーク > グローバルプロテクト > ポータル > <portal-config> > 一般

General (全般)タブを選択し、GlobalProtect アプリケーションが GlobalProtect ポータルに接 続するために使用するネットワーク設定を定義します。また、必要に応じてGlobalProtectの ログインページを無効化したり、カスタムポータルログインやヘルプページを指定すること ができます。カスタム ページを作成およびインポートする方法の詳細は、『GlobalProtect Administrator's Guide (GlobalProtect 管理者ガイド)』の「Customize the Portal Login, Welcome, and Help Pages(ポータル ログインページ、ウェルカム ページ、ヘルプ ページのカ スタマイズ)」を参照してください。

GlobalProtect ポータル の設定	の意味
氏名	ポータルの名前を入力します(最大 31 文字)。名前の大文字と小 文字は区別されます。また、一意の名前にする必要があります。文

GlobalProtect ポータル の設定	の意味
	字、数字、スペース、ハイフン、およびアンダースコアのみを使用 してください。
場所	マルチ仮想システムモードになっているファイアウォールの場 合、Location[場所] はGlobalProtectポータルを使用できる仮想シス テム(vsys)になります。マルチvsysモードに設定されていない ファイアウォールの場合、Location[場所] は選択できません。ポー タルを保存すると、その Location[場所] を変更できなくなります。
Network Settings [ネット	・ワーク設定]
Interface	リモートク エンドポイントおよびファイアウォールからの通信の 入り口となるファイアウォールインターフェイスの名前を選択しま す。
	Telnet、SSH、HTTP、または HTTPS を許可するイン ターフェイス管理プロファイルを、GlobalProtect ポー タルまたはゲートウェイを設定したインターフェイス に接続しないでください。これにより、管理インター フェイスがインターネットに公開されるためです。管 理ネットワークへのアクセスを保護する方法の詳細に ついては、Adminstrative Access Best Practices を参 照してください。
IP アドレス	GlobalProtect ポータル Web サービスを実行する IP アドレスを指定します。IP Address Type(IP アドレス タイプ)を選択して、IP Address(IP アドレス)を入力します。
	 IP アドレス タイプは、IPv4(IPv4 トラフィックの場合のみ)、IPv6(IPv6 トラフィックの場合のみ)、または IPv4 and IPv6(IPv4 および IPv6)です。ネットワークがデュアル スタック構成をサポートしているときは、IPv4 and IPv6(IPv4 および IPv6)を使用します。これにより IPv4 と IPv6 が同時に動作します。 IP アドレスは IP アドレス タイプに対応するものでなければな りません なとえば IPv4 の担合け 172 14 10 IPv4 の担合け
	りょせん。たこえば、IPV4 の場合は 172.10.1.0、IPV6 の場合は 21DA:D3:0:2F3b のように指定します。
	 IPv4 and IPv6(IPv4 および IPv6)を選択した場合、それぞれの タイプに適切な IP アドレスを入力します。

ログ設定

GlobalProtect ポータル の設定	の意味
正常完了した SSL ハン ドシェイクのログへの	(オプション)正常に完了した SSL復号化ハンドシェイクの詳細ロ グを作成します。デフォルトで無効になっています。
百二亦次	 ログはストレージ容量を消費します。ログを保存するリソースがあることを確認してから正常に完了した SSL ハンドシェイクをログに記録します。Device(デバイス) > Setup(セットアップ) > Management(管理) > Logging and Reporting Settings(ログとレポートの設定)を編集して、現在のログメモリの割り当てを確認し、ログタイプ間のログメモリに再割り当てを行います。
失敗した SSL ハンド シェイクのログへの記 録	失敗した SSL 復号化ハンドシェイクの詳細なログを作成すると、復 号化の問題の原因を特定可能となります。デフォルトで有効になっ ています。
	 ログはストレージ容量を消費します。より多くの(またはより少ない)ログストレージ容量を復号化ログに割り当てるには、ログメモリの割り当てを編集します(Device(デバイス) > Setup(セットアップ) > Management(管理) > Logging and Reporting Settings(ログとレポートの設定))。
ログの転送	GlobalProtect SSL ハンドシェイク(復号化)ログを転送する方法および場所を指定します。
Appearance [表示設定]	
ポータルのログイン ページ	(任意) ユーザーがポータルへのアクセスに使用する、カスタムロ グインページを選択します。factory-default[出荷時のデフォルト] ページを選択するか、カスタムページをImport[インポート] するこ とができます。デフォルト設定はNone[なし] です。このページに Web ブラウザからアクセスできないようにする場合、このページ を Disable (無効化) します。
ポータルのランディン グ ページ	(任意)ポータルのカスタム ランディング ページを選択しま す。factory-default[出荷時のデフォルト] ページを選択するか、カ スタムページをImport[インポート] することができます。デフォル ト設定はNone[なし] です。
アプリケーションのへ ルプ ページ	(任意)GlobalProtectを使用するユーザーの補助を行うカスタム ヘルプページを選択します。factory-default[出荷時のデフォルト] ページを選択するか、カスタムページをImport[インポート] するこ

GlobalProtect ポータル の設定	の意味
	とができます。出荷時のデフォルト ヘルプ ページは GlobalProtect アプリ ソフトウェアで提供されます。カスタム ヘルプ ページを 選択する場合、GlobalProtect ポータルは GlobalProtect ポータル 設定を含むヘルプ ページを提供します。デフォルトの None(な し)のままにすると、GlobalProtect アプリはページを表示せずに メニューからオプションを削除します。

GlobalProtect ポータルの Authentication Configuration (認証設定) タブ

• ネットワーク > グローバルプロテクト > ポータル > <portal-config> > 認証

Authentication (認証)タブを選択し、様々な GlobalProtect[™] ポータルの設定を行います:

- ポータルおよびサーバーが認証に使用するSSL/TLSサービスプロファイルです。サービスプロファイルです。サービスプロファイルは認証のその他の設定から独立しています。
- 第一にユーザーエンドポイントのオペレーティングシステムに、次に任意で設定された認証 プロファイルに基づく、固有の認証スキームです。
- (任意) GlobalProtectにおいて、ユーザー認証用に特定の証明書プロファイルを使用できる ようにするCertificate Profile[証明書プロファイル]です。クライアントが提示する証明書は 証明書プロファイルと一致している必要があります(セキュリティスキームの一部としてク ライアントの証明書が設定されている場合)。

GlobalProtect ポータ	の意味
ルの認証設定	

Server Authentication [サーバー認証]

SSL/TLS Service Profile	既存のSSL/TLSサービスプロファイルを選択します。このプロファ イルでは、管理インターフェイスのトラフィックの安全を確保す るために使用する証明書と、使用を許可するプロトコルを指定しま す。Common Name (CN)(共通名 (CN))と、該当する場合はプ ロファイルに関連付けられている証明書のSubject Alternative Name (SAN)(サブジェクト代替名 (SAN))フィールドが、IP アドレスま たは General (一般設定)タブで選択した Interface (インターフェイ ス)の FQDN と一致する必要があります。
	 GlobalProtect の VPN 設定では、信頼できるサードパー ティ CA の証明書または内部のエンタープライズ CA が 生成した証明書に関連付けられているプロファイルを使 用してください。

GlobalProtect ポータ ルの認証設定	の意味
Client Authentication	[クライアントの認証]
氏名	このクライアント認証設定を識別する名前を入力します。(クライア ント認証設定は SSL/TLS サービスプロファイルからは独立していま す)
	複数のクライアント認証構成を作成し、オペレーティングシステムで 区別できます。たとえば、Windows エンドポイントに対しては1つ の一意の認証プロファイルを追加し、もう1つの認証プロファイルを macOS エンドポイントに追加できます。
	同じ OS に対して複数のクライアント認証構成を追加できますが、ファイアウォールは常にリストの上部にある認証プロファイルを選択して、その特定の OS を使用するすべてのユーザーを認証します。
	GlobalProtect が pre-logon (ログオン前)モード(ユーザーがシステ ムにログオンする前)のアプリに適用する設定、または任意のユー ザーに適用する設定を作成することもできます。(Pre-logonでは、 ユーザーがGlobalProtect にログインする前に、GlobalProtectゲート ウェイに向けたVPNトンネルを確立します)
OS	エンドポイントのオペレーティングシステム(OS)固有のクラ イアント認証プロファイルを適用する場合は、OS(Any(すべ て)、Android、Chrome、iOS、Linux、Mac、Windows、または WindowsUWP)をAdd(追加)します。OSは設定同士を第一に区別 するものです。(区別の詳細についてはAuthentication Profile [認証プ ロファイル]を参照してください)
	Browser[ブラウザ] およびSatellite[サテライト] の追加オプションで は、特定のシナリオ用の認証プロファイルを指定することができま す。GlobalProtect アプリ(Windows および Mac)をダウンロードす るWeb ブラウザから、ポータルにアクセスするユーザーを認証する 際に使用する認証プロファイルを指定する場合は、Browser(ブラウ ザ)を選択します。サテライト(LSVPN)の認証時に使用する認証プ ロファイルを指定する場合はSatellite[サテライト]を選択します。
認証プロファイル	OSによるクライアント認証設定の区別に加え、認証プロファイ ルを設定することで更に区分していくことが可能です。(New Authentication Profile[新規認証プロファイル]を作成するか、既存のも のを選択することができます。)1つのOSに対し複数の認証オプショ ンを設定したい場合は、複数のクライアント認証プロファイルを作成 することができます。

GlobalProtect ポータ ルの認証設定	の意味
	 Gateways[ゲートウェイ]にLSVPNを設定する場合、ここで認証プロファイルを選択しない限り、その設定を保存することができません。また、サテライトの認証にシリアル番号を使用しようとしている場合、ファイアウォールのシリアル番号が見つからない場合や、検証が行えなかったときのために、ポータル認証プロファイルを設定しておく必要があります。 「Device (デバイス) > Authentication Profile (認証プロファイル)」も参照してください。
Username Label ユーザー名のラベル	GlobalProtect ポータル ログイン用のカスタム ユーザー名ラベルを 指定します。たとえば、ユーザー名(のみ)、またはメールアドレ ス(username@domain)。
パスワード ラベル	GlobalProtect ポータル ログイン用のカスタム ポータル ラベルを指定 します。たとえば、パスワード(トルコ語)またはパスコード(2 重 認証、トークンベース認証)
認証メッセージ	ログインに必要な認証情報のタイプをエンドユーザーに伝えるメッ セージを入力するか、デフォルトのメッセージのままにしておいてく ださい。メッセージの最大文字数は256文字です。
ユーザー認証情報あ るいはクライアント 証明書による認証を 許可	No (いいえ)を選択すると、ユーザーがユーザー認証情報およびクラ イアント証明書の両方を使ってゲートウェイに認証する必要がありま す。Yes (はい)を選択すると、ユーザーがユーザー認証情報あるいはク ライアント証明書のいずれかを使ってゲートウェイに認証できるよう になります。
証明書プロファイル	
証明書プロファイル	(任意) ユーザーのエンドポイントから受信するクライアント証明書 を照合する際にポータルが使用するCertificate Profile[証明書プロファ イル] 選択します。証明書プロファイルを使用すると、ユーザーはクラ イアントの証明書がこのプロファイルと一致する場合にのみ認証を行 うことができます。
	Allow Authentication with User Credentials OR Client Certificate (ユー ザー認証情報あるいはクライアント証明書による認証を許可)オプショ ンをNo (いいえ)に設定する場合はCertificate Profile (証明書プロファ イル)を選択する必要があります。Allow Authentication with User Credentials OR Client Certificate (ユーザー認証情報あるいはクライ アント証明書による認証を許可)オプションをYes (はい)に設定する場 合、Certificate Profile (証明書プロファイル)は任意項目です。

GlobalProtect ポータ ルの認証設定	の意味
	証明書プロファイルはOSの種類に依存しません。またこのプロファ イルは、認証プロファイルをオーバーライドし、暗号化された Cookie による認証を可能にする、Authentication Override(認証のオーバー ライド)を有効にした場合もアクティブなままです。

GlobalProtect ポータルの Portal Agent Data Collection (ポータル データ収集) タブ

Network > GlobalProtect > Portals > <portal-config> > Portal Data Collection to GlobalProtectを 選択して、ユーザーがポータルに正常にログインした後に、GlobalProtect アプリがエンドポイ ントから収集し、構成選択基準データで送信するデータを定義します。

GlobalProtect ポータルのデータ収集設定	の意味
証明書プロファイル	GlobalProtect アプリケーションが送信 したマシン証明書にマッチさせるために GlobalProtect ポータルが使用する証明書プロ ファイルを選択します。
カスタム チェック	アプリで収集するカスタム ホスト情報を定義 します。
	 Windows – 特定のレジストリキーやキー 値のチェックをAdd[追加] します。
	 Mac – 特定のplistやキー値のチェック をAdd (追加) します。

GlobalProtect ポータルの Agent (エージェント) タブ

• ネットワーク > グローバルプロテクト > ポータル > <portal-config> > エージェント

Agent (エージェント)タブを選択してエージェント設定を定義します。GlobalProtectポータルは、まず接続が確立されてからデバイスへ設定を適用します。

ポータルは、信頼されたルート認証局(CA)証明書や中間証明書を自動的に適用するように 設定することも可能です。GlobalProtectゲートウェイやGlobalProtectモバイルセキュリティマ ネージャーが使用しているサーバー証明書をエンドポイントが信頼しない場合、エンドポイント がゲートウェイやモバイルセキュリティマネージャーに向けたHTTPS接続を確立する際にこれ らの証明書が必要になります。ポータルはここに指定した証明書を、クライアント設定と共にク ライアントへプッシュします。

信頼できるルート認証局証明書を追加する場合は、既存の証明書をAdd[追加] するか、新し くImport[インポート] してください。SSLフォワードプロキシの復号化に必要な信頼できるルー ト認証局証明書を(表示することなく)クライアントの証明書ストアにインストールする場合 は、Install in Local Root Certificate Store[ローカルのルート証明書ストアにインストール] を選 択します。

 GlobalProtect アプリケーションが GlobalProtect ポータルおよびゲートウェイの身元 を検証するために使用する、信頼できるルート CA 証明書を指定します。信頼でき るルート CA を発行したのと同じ認証局によって署名されていない証明書をポータ ルあるいはゲートウェイが提示すると、GlobalProtect アプリケーションはそのポー タルあるいはゲートウェイと接続を確立できません。

異なるタイプのユーザーごとに異なる設定が必要な場合は、それぞれに対して別個にエージェ ント設定を作成し、その設定をサポートすることができます。ポータルはその後、ユーザー 名/グループ名やクライアントの OSにより、適用するエージェント設定を判別します。セキュ リティルール評価によって、ポータルはリストの先頭から一致する項目を検索します。一致項 目を発見すると、ポータルは対応する設定をアプリに配信します。そのため、複数のエージェ ント設定がある場合、設定を具体的なもの(つまり、特定のユーザーまたは特定のオペレー ティングシステム用の設定)から汎用的なものへと並べることが重要です。設定の並び替えに は、Move Up[上へ] および Move Down[下へ] を使用します。必要に応じて新しいエージェン ト設定をAdd[追加] してください。ポータルの設定方法とエージェント設定の作成方法の詳細 は、『GlobalProtect Administrator's Guide(GlobalProtect 管理者ガイド)』の「GlobalProtect Portals(GlobalProtect ポータル)」を参照してください。新しいエージェント設定を Add(追 加)するか、既存の設定を変更した場合、Configs(設定)ウィンドウが開き、5 つのタブが表 示されます。詳細を以下の表に記載します。

- GlobalProtect ポータルの Agent Authentication (エージェント認証) タブ
- GlobalProtect ポータルの Agent Config Selection Criteria (エージェント設定の選択条件) タブ
- GlobalProtect ポータルの Agent Internal (エージェント内部) タブ
- GlobalProtect ポータルの Agent External (エージェント外部) タブ
- GlobalProtect ポータルの Agent HIP Data Collection(エージェント HIP データ収集)タブ

GlobalProtect ポータルの Agent Authentication (エージェント認証) タブ

ネットワーク > グローバルプロテクト > ポータル > <portal-config> > エージェント > <agent-config> > 認証

Authentication (認証)タブを選択し、エージェント設定に適用される認証設定を行います。

GlobalProtect ポータルのクライア ント認証設定	の意味
Authentication [認証]タブ	
氏名	このクライアント認証の設定に付ける分かりやすい名前

GlobalProtect ポータルのクライア ント認証設定	の意味
クライアント証明書	(任意)エンドポイントヘクライアント証明書を配信す る送信元を選択すると、その送信元が証明書をゲート ウェイに提示するようになります。相互SSL認証を設定 する場合はクライアント証明書が必要となります。
	モバイルデバイスのポータル構成にクライアント証明書を含める場合、クライアント証明書パスフレーズはポータル構成に保存されるため、ゲートウェイ構成ではクライアント証明書認証のみを使用できます。さらに、クライアント証明書は、ポータル構成から証明書を取得した後にのみ使用できます。
	ポータルクライアント設定のpre-logonでSCEPが設定さ れている場合、ポータルはマシン証明書を生成し、その 証明書はゲートウェイの認証や接続に使用するシステム 証明書ストアに保存されます。
	SCEP を通じて PKI が生成した証明書を使用する代わり にファイアウォールの Local(ローカル)な証明書を使 用する場合は、ファイアウォールに既にアップロード済 みの証明書を選択してください。
	内部 CA を使用して証明書をエンドポイントに配 布する場合、None(なし)を選択します(デフォル ト)。None(なし)を選択した場合、ポータルはエン ドポイントに対し証明書をプッシュしません。
ユーザー認証情報の保存	アプリ上にユーザー名およびパスワードを保存する場合 はYes(はい)を選択し、接続の都度、手動入力あるい はエンドポイントを通じて表示を行わずにパスワードの 提供を求める場合はNo(いいえ)を選択します。ユー ザーの接続時に、ユーザー名のみを保存しておきたい場 合はSave Username Only[ユーザー名のみ保存]を選択 してください。生体ログインを許可するには Only with User Fingerprint (ユーザーの指紋のみ)を選択します。 エンドポイントで生体サインオンが有効になっている場 合、指紋スキャンがエンドポイントの信頼できる指紋テ ンプレートと一致すると、GlobalProtect は保存された ユーザー資格情報を使用します。

GlobalProtect ポータルのクライア ント認証設定	の意味
	認証されていないユーザーが重要なリ ソースや機密情報にアクセスしやすくな るため、ユーザー認証情報を保存しない でください。ユーザーが GlobalProtect に 接続する度に認証情報を手動で入力する 必要があります。
認証のオーバーライド	
Cookieを生成して認証をオーバー ライド	暗号化された、エンドポイント固有のCookieをポータル に生成させる場合はこのオプションを選択します。ユー ザーがポータルで認証を行ったのちに、ポータルはこ のCookieをエンドポイントに送信します。
認証オーバーライドの Cookie を受 け入れる	暗号化された有効な Cookie を使用してエンドポイント 認証を行うようポータルを設定する場合はこのオプショ ンを選択してください。有効なCookieをエンドポイント が提示した場合、ポータルはそのポータル自身が暗号化 したCookieであることを確認し、復号化を行ってユー ザーを認証します。
Cookie 有効期間	Cookieが有効な時間数、日数、あるいは週数を指定します。一般的な有効期間は24時間です。範囲は1~72時間、1~52週間、あるいは1~365日です。Cookieが 失効した場合、ユーザーはログイン認証情報を再度入力する必要があり、この入力をうけてポータルは新しいCookieを暗号化してユーザーエンドポイントに送信します。
Cookie を暗号化/復号化する証明 書	 Cookieの暗号化と復号化に使用する証明書を選択します。 Cookieの暗号化および復号化用に、ポータルとゲートウェイで同じ証明書を使用するよう設定されていることを確認してください。(証明書をゲートウェイクライアント設定の一部として設定します。「Network(ネットワーク) > GlobalProtect > Gateways(ゲートウェイ)」を参照してください)

Components that Require Dynamic Passwords (Two-Factor Authentication) (ダイナミックパ スワードが必要な構成要素(2重認証))

GlobalProtect ポータルのクライアの意味 ント認証設定

1回限りのパスワード(OTP)などのダイナミックパスワードがGlobalProtectでサポートされるように設定する場合は、ダイナミックパスワードの入力を求めるポータルまたはゲートウェイタイプを指定します。2重認証が有効化されていない環境において、GlobalProtectはログイン認証情報(ADなど)と証明書を用いた通常の認証形式を使用します。

2重認証用のポータルまたはゲートウェイタイプを有効化すると、ユーザーがポータルで1度 目の認証を行ったのち、そのポータルまたはゲートウェイは認証情報と2つ目のOTP(あるい はその他のダイナミックパスワード)の提示を求めます。

しかし、認証オーバーライドも同じく有効化している場合、(ユーザーが新しいセッショ ンで認証されると、)認証情報の再入力を行う代わりに、(Cookieの有効期間内に限 り、)ユーザーの認証には暗号化されたCookieが使用されます。このため、Cookieが有効 である限り、ユーザーは認証の画面表示を行うことなくログインすることが可能になりま す。Cookieの有効期限を指定する必要があります。

ポータル	ポータルへの接続にダイナミックパスワードを使用する 場合はこのオプションを選択します。
Internal gateways - all(内部ゲート ウェイ - すべて)	内部ゲートウェイへの接続にダイナミックパスワードを 使用する場合はこのオプションを選択します。
外部ゲートウェイ - 手動のみ	Manual[手動] ゲートウェイとして設定されている外部 ゲートウェイへの接続にダイナミックパスワードを使用 する場合はこのオプションを選択します。
External gateways - auto discovery(外部ゲートウェイ - 自 動検出)	アプリが自動検出可能なその他のゲートウェイ (Manual (手動)に設定されていないゲートウェイ) への接続にダイナミックパスワードを使用する場合はこ のオプションを選択します。

GlobalProtect ポータルの Agent Config Selection Criteria (エージェント設定の選択 条件) タブ

ネットワーク > グローバルプロテクト > ポータル > <portal-config> > エージェント > <agent-config> > Config Selection Criteria (設定選択条件)

Config Selection Criteria (設定選択条件)タブを選択し、管理対象および管理対象外のエンドポイントが両方あるデプロイ環境でエンドポイントの種類を識別するために使用する一致条件を設定します。ポータルは指定された設定をエンドポイントの種類に基づいてエンドポイントにプッシュできます。

GlobalProtect ポータルの設定選択条件の設定 の意味

User/User Group [ユーザー/ユーザー グループ] タブ

GlobalProtect ポータルの設定選択条件の設定	の意味
OS	エンドポイントのオペレーティングシステ ム (OS) を一つ以上Add (追加)し、どのエン ドポイントがこの設定を受信するのか指定 します。ポータルはエンドポイントのOSを 自動的に検知し、そのOS用のクライアント 設定を適用します。Any (任意)の OS ある いは特定の OS (Android、Chrome、iOS、 IoT、Linux、Mac、Windows、または WindowsUWP) を選択できます。
ユーザー/ユーザー グループ	この設定を適用する特定のユーザーまたは ユーザーグループを Add (追加) します。
	 コーザーグループを選択す る前にグループマッピング を設定する必要があります (Device (デバイス) > User Identification (User-ID) > Group Mapping Settings (グ ループマッピング設定))。 この設定をすべてのユーザーにデプロイする には、User/User Group (ユーザー/ユーザー グループ)のドロップダウンリストでany (す べて)を選択します。この設定をプレログオ ンモードの GlobalProtect アプリケーション を使用しているユーザーにのみデプロイす る場合は、User/User Group (ユーザー/ユー ザーグループ)のドロップダウンリストでpre- logon (プレログオン)を選択します。
デバイスチェック	1
マシン アカウントはデバイスのシリアル番号 と共に存在	エンドポイントのシリアル番号がアクティブ ディレクトリに存在するかどうかに応じて一 致条件を設定します。
証明書プロファイル	GlobalProtect アプリケーションが送信 したマシン証明書にマッチさせるために GlobalProtect ポータルが使用する証明書プロ ファイルを選択します。
カスタム チェック	

GlobalProtect ポータルの設定選択条件の設定	の意味
カスタム チェック	マッチさせるカスタム ホスト情報を定義する 場合はこのオプションを選択します。
	 レジストリキーまたは plist を 使用してカスタムチェックを作 成する場合は、それを [Portal Data Collection (ポータルデータ 収集)] タブに追加する必要があ ります (ネットワーク > グロー バルプロテクト > ポータル > <portal-config> > ポータル デー タ収集)。</portal-config>
レジストリ キー	Windows エンドポイントに特定のレジスト リキーがあるかチェックする場合は、マッチ させるRegistry Key (レジストリキー)をAdd (追加)します。指定したレジストリキー)をAdd (追加)します。指定したレジストリキーまた はキーの値が欠損しているエンドポイント のみを照合する場合は、Key does not exist or match the specified value data (キーが存 在しないか、指定した値データと一致しな い)のオプションを有効化します。特定の 値を照合するには、Registry Value (レジス トリの値) と Value Data (値データ)を入力し てAdd (追加)します。指定されたレジストリ 値を持たないエンドポイントを照合するに は、Negate を選択します。Negateオプショ ンを選択する場合は、[値のデータ]フィー ルドを空のままにしておく必要があります。 GlobalProtect ポータルのカスタム チェック でレジストリ値の Negate オプションを選択 できます。指定されたレジストリ値がありま せん (レジストリ値が存在しないことに一致 します)。

GlobalProtect ポータルの設定選択条件の設定	の意味
	 レジストリ値を Negate オプ ションで設定し、Value Data フィールドを空白のままにする と、Negate はレジストリ値を 処理します。Negateオプショ ンと値データ照合は相互に排 他的であり、バリューデータ とNegateオプションを一緒に設 定することはできません。
Plist	macOS エンドポイントのプロパティリスト (plist) に特定のエントリがあるかチェック する場合は、Plist名をAdd (追加)します。指 定したplistを持たないエンドポイントのみを 照合する場合は、Plist does not exist (Plistが 存在しない) オプションを有効化します。plist 内の特定のキー/値ペアによって照合するに は、Key (キー)と対応するValue (値)をAdd (追 加)します。指定されたキーまたは値を明示 的に持たないエンドポイントを照合する場合 は、Negate (除外)を選択します。

GlobalProtect ポータルの Agent Internal (エージェント内部) タブ

ネットワーク > グローバルプロテクト > ポータル > <portal-config> > エージェント > <agent-config> > 内部

Internal (内部)タブを選択し、エージェント設定用の内部ゲートウェイ設定を行います。

GlobalProtect ポータル の内部設定	の意味
内部ホスト検出	
内部ホスト検出	企業ネットワークの内部にいるかどうか、GlobalProtect アプリに 判断させる場合はこのオプションを選択します。これは、エンター プライズネットワークでトンネルが必要ない場合、またはエンド ポイントが内部ゲートウェイと通信するように構成されている場 合に、エンドポイントに適用されます。内部ホスト検出機能の選択 は、これらのエンドポイントのベストプラクティスです。ただし、 内部ゲートウェイの構成はオプションです。
	ユーザーがログインしようとすると、アプリは指定された IPアド レス を使用して、指定された ホスト名 に対して内部ホストの逆引 き DNS ルックアップを実行します。ホストは参照ポイントとして

GlobalProtect ポータル の内部設定	の意味
	機能し、到達可能である必要はありませんが、逆引き DNS ルック アップは、エンドポイントが企業ネットワーク内にある場合にのみ 成功する必要があります。アプリがホストを検出した場合、エンド ポイントはネットワーク内にあり、アプリは内部ゲートウェイ (構 成されている場合)に接続するか、GlobalProtect アプリは接続状態 を内部として表示します。アプリが内部ホストを見つけられなかっ た場合、エンドポイントはネットワークの外部にあり、アプリは外 部ゲートウェイの1つへのトンネルを確立します。
	 IP アドレス タイプは、IPv4 (IPv4 トラフィックのみ)、IPv6 (IPv6 トラフィックのみ)、またはその両方です。 ネットワークがデュアル スタック構成をサポートしているとき は、IPv4 と IPv6 を使用します。これにより IPv4 と IPv6 が同時 に動作します。
	 IP アドレスは IP アドレス タイプに対応するものでなければなりません。たとえば、IPv4 の場合は 172.16.1.0、IPv6 の場合は21DA:D3:0:2F3b のように指定します。
	 IPv4 と IPv6 を選択した場合、それぞれのタイプに適切な IP ア ドレスを入力します。
ホスト名	内部ネットワーク内で上記のIPアドレスに解決するHostname[ホス ト名] を入力します。
内部ゲートウェイ	
アプリがアクセス要求	内部ゲートウェイを Add [追加] し、以下の情報を指定します。
を行い、さらに、HIP レポートを提供する (GlobalProtect Portals Agent Data Collection Tab (GlobalProtect ポータルのエージェン ト データ収集) で HIP が有効にされている場 合)内部ゲートウェイ を指定します。	 Name[名前] – ゲートウェイを識別するラベル(最大31文字)を 入力します。名前の大文字と小文字は区別されます。また、一 意の名前にする必要があります。文字、数字、スペース、ハイ フン、およびアンダースコアのみを使用してください。
	 Address[アドレス] – ゲートウェイ用のファイアウォールイン ターフェイスのIPアドレスまたはFQDN。ここで指定する値は ゲートウェイサーバー証明書の共通名(CN)およびSAN(指定 されている場合)と一致させる必要があります。例えば、証明 書の生成にFQDNを使用した場合、ここにFQDNを入力する必要 があります。

 Source Address(送信元アドレス) – エンドポイントの送信 元アドレスまたはアドレスプールです。ユーザーが接続す ると、GlobalProtectはデバイスの送信元アドレスを認識し ます。送信元アドレスプールに含まれている IP アドレスの GlobalProtect アプリのみが、このゲートウェイで認証し、HIP レポートを送信できます。

GlobalProtect ポータル の内部設定	の意味
	 DHCP Option 43 Code (DHCP オプション 43 コード) (Windows および Mac のみ) - ゲートウェイ選択用の DHCP サブオプション コードを指します。Specify one or more sub-option codes (in decimal). サブオプション コードを指定します(10 進数)。GlobalProtect アプリは、サブオプション コードで定義された値からゲートウェイ アドレスを読み取ります。

GlobalProtect ポータルの **Agent External**(エージェント外部)タブ

ネットワーク > グローバルプロテクト > ポータル > <portal-config> > エージェント > <agent-config> > External (外部)

External (外部)タブを選択し、エージェント設定用の外部ゲートウェイ設定を行います。

GlobalProtect ポータル の外部設定	の意味
Cutoff Time (sec)(カットオフ時間 (秒))	最適なゲートウェイを選択する際、使用可能なゲートウェイが 応答するまでアプリが待機する時間を秒単位で指定します。以降 の接続要求において、アプリはそのカットオフ時間内に応答した ゲートウェイとの接続を試行します。値が0の場合、アプリは App(アプリ)タブの AppConfigurations(アプリ設定)にある TCP Connection Timeout(TCP 接続のタイムアウト)を使用しま す(範囲は0~10、デフォルトは5)。
外部ゲートウェイ	
企業ネットワーク外か らトンネルを確立す る場合にアプリが接続 を試行する対象となる ファイアウォールのリ ストを指定します。	 外部ゲートウェイをAdd[追加] し、以下の情報を指定します。 Name[名前] - ゲートウェイを識別するラベル(最大31文字)を入力します。名前の大文字と小文字は区別されます。また、一意の名前にする必要があります。文字、数字、スペース、ハイフン、およびアンダースコアのみを使用してください。 アドレス - ゲートウェイが設定されているファイアウォールインターフェイスの IP アドレスまたは FQDN。値は、ゲートウェイサーバー証明書の CN(および指定されている場合はSAN)と一致させる必要があります。たとえば、証明書の生成にFQDNを使用した場合、ここに FQDNも入力する必要があります。 Source Region(送信元地域) - エンドポイントの送信元地域です。GlobalProtect はユーザーが接続した際にエンドポイントの地域を認識して、その地域に設定されたゲートウェイの選択では、

GlobalProtect ポータル の外部設定	の意味
	送信元地域が考慮されてから、ゲートウェイの優先順位が考慮 されます。 Priority(優先順位) – アプリが使用するゲー トウェイを判別しやすいように値(Highest(最 高)、High(高)、Medium(中)、Low(低)、Lowest(最 低)、Manual only(手動のみ)のいずれか)を選択しま す。Manual only(手動のみ)を選択すると、エンドポイントで Auto Discovery(自動検出)が有効である場合に GlobalProtect アプリはこのゲートウェイへの接続を試行しません。このアプ リは、まず、指定されたすべてのゲートウェイに Highest(最 高)、High(高)、または Medium(中)の優先度で接続し、 最速で応答するゲートウェイとトンネルを確立します。優先 度の高いゲートウェイに到達できない場合、次にアプリは優先 度の低い値を持つ追加のゲートウェイに接続します(Manual only(手動のみ)のゲートウェイは除く)。
	 Manual[手動] – ユーザーが手動でゲートウェイを選択(あるいは切り替え)できるようにする場合はこのオプションを選択します。GlobalProtect アプリは、Manual(手動)に設定されている外部ゲートウェイであれば、どのゲートウェイにも接続することができます。アプリが他のゲートウェイに接続する場合、既存のトンネルは接続が解除され、新しいトンネルが確立されます。手動ゲートウェイでは、プライマリゲートウェイとは異なる認証方式を使用することもできます。エンドポイントが再起動された場合や、再検出が実行された場合、GlobalProtectエージェントはプライマリゲートウェイに接続します。この機能は、ネットワークの保護されたセグメントにアクセスするために、特定のゲートウェイに一時的に接続する必要があるユーザーグループが存在する場合に役立ちます。

サードパーティ VPN

サードパーティ VPN	GlobalProtect が対象指定されたサードパーティ VPN クライアント と競合しないよう、GlobalProtect アプリにこれらを無視するよう に設定する場合は、VPN クライアントの名前を Add(追加)しま す。リストから名前を選択するか、フィールドに名前を入力しま
	す。GlobalProtectはここで指定したVPNクライアントのルート設定 を無視するようになります。

GlobalProtect ポータルの Agent App (エージェント アプリケーション) タブ

ネットワーク > グローバルプロテクト > ポータル > <portal-config> > エージェント > <agent-config> > アプリケーション

App (アプリ**)**タブを選択し、ユーザーがシステム上にインストールされた GlobalProtect ア プリをどのように操作するかを指定します。作成した各種のGlobalProtect設定ごとに、異な るアプリ設定を定義できます。GlobalProtect App Customization(GlobalProtectアプリケー ションのカスタマイズ)設定の最新アップデートについては、GlobalProtect Administrator's Guide(GlobalProtect 管理者ガイド)を参照してください。

GlobalProtect アプリの設定	の意味
ウェルカム ページ	GlobalProtect に接続したエンドユーザーに対して表示 するウェルカムページを選択します。factory-default[出 荷時のデフォルト] ページを選択するか、カスタムペー ジをImport[インポート] することができます。デフォル ト設定はNone[なし] です。
アプリケーション設定	
接続手段	 On-demand (Manual user initiated connection) (オン デマンド (ユーザーによる手動接続)) – ユーザー は GlobalProtectアプリケーションを起動し、当該の GlobalProtect 認証情報を入力する必要があります。 このオプションは、主にリモートアクセス接続に使 用します。
	 User-logon (Always On) (ユーザー ログオン (常時オン)) – ユーザーがエンドポイントにログインするとGlobalProtect アプリはポータルへの接続を自動的に確立します。応答として、ポータルはアプリに適切なエージェント設定を返します。その後、アプリはポータルから受信したエージェント設定に指定されているゲートウェイのうちの1つとトンネルを確立します。
	 Pre-logon (ログオン前) – これにより、リモートの Windows および Mac ユーザーは常に企業ネットワークに接続された状態になります。また、ユーザーがエンドポイントにログインした際のユーザーログオン スクリプトとドメイン ポリシーの適用を可能にします。社内と同じようにエンドポイントから企業ネットワークに接続できるため、ユーザーはパスワードの失効時に新しいパスワードでログインしたり、パスワードを忘れた場合にパスワード復元によるサポートを利用したりできます。pre-logonを使用すると、GlobalProtectアプリケーションはユーザーがエンドポイントにログインする前にGlobalProtect ゲートウェイへの VPN トンネルを確立します。エンドポイントはゲートウェイに対し、事前にインストールされたマシン証明書を提示することで認証要求を行います。次に、Windows エンド

GlobalProtect アプリの設定	の意味
	ポイントでは、ゲートウェイは VPN トンネルをログ オン前ユーザーからエンドポイントにログインした ユーザー名に再割り当てします。Mac エンドポイン トでは、アプリは接続を切断し、ユーザー用に新し い VPN トンネルを作成します。
	pre-logon 接続方式は 2 種類あります。いずれも、同 様の pre-logon 機能をユーザーがエンドポイントにロ グインする前に実施します。ただし、ユーザーがエ ンドポイントにログインした後は、pre-logon 接続方 式によって、GlobalProtect アプリの接続が確立され るタイミングが異なります。
	 Pre-logon (Always On) (ログオン前(常時 オン)) – GlobalProtectアプリケーション は、GlobalProtect ゲートウェイへの接続および 再接続を自動的に試行します。モバイルデバイ スはログオン前機能をサポートしていないため、 この接続方法が指定されている場合、デフォルト でUser-logon (Always On) (ユーザーログオン (常 時オン)) 接続方法になります。
	 Pre-logon then On-demand (pre-logon 後オン デマンド) –ユーザーは GlobalProtectアプリ ケーションを起動してから当該の接続を手動で 開始する必要があります。モバイル デバイスは pre-logon 機能をサポートしていないため、この 接続方式が指定された場合、デフォルトは On- demand (Manual user initiated connection)(オン デマンド(ユーザーによる手動接続))接続方式 となります。
GlobalProtect アプリ設定の更新間 隔(時間)	GlobalProtect ポータルがアプリの設定を更新する間隔 (時間数)を指定します(範囲は1~168、デフォルト は24)。
ユーザーによるグローバルプロテ クトアプリの接続解除を許可	ユーザーがGlobalProtectアプリを切断できるかどうかを 指定します。許可されている場合は、アプリを切断する 前に行う必要があること(ある場合)を指定します。
	 Allow(許可) – すべてのユーザーが必要に応じて GlobalProtect アプリを無効化できます。
	 Disallow (許可しない) – エンドユーザーが GlobalProtect アプリを切断できないようにします。
	 Allow with Comment (コメント付きで許可) – ユー ザーはエンドポイントの GlobalProtectアプリケー

GlobalProtect アプリの設定	の意味
	ションへの接続を解除できますが、その際、無効化 する理由を送信する必要があります。
	GlobalProtect アプリは、ユーザーに次のことを要求 します。
	• アプリを切断する理由を指定します。
	 表示されるリストから、インターネットの速度が 遅い、待ち時間が遅いなどの理由を選択します。
	切断の理由は、表示を構成して GlobalProtect (常時オンモード)を切断 する次の理由を表示する場合にのみ表 示されます。接続解除の理由を表示す るように GlobalProtect アプリを構成し なかった場合、エンドユーザーはアプ りから切断する理由を指定するように 求められます。
	 Allow with Passcode (パスコードで許可)-ユーザーが パスコードを入力してGlobalProtectアプリケーショ ンを切断できるようにします。このオプションを選 択すると、ユーザーは、パスワードと同様に入力時 に表示されることがないパスコードの入力と再入力 を行う必要があります。一般的に、管理者は予期し ない出来事によりユーザーがGlobalProtect VPNを 使用してネットワークに接続できなくなる前にユー ザーにパスコードを配布しておきます。パスコード は電子メールで送信するか、企業のWebサイトに掲 示することで配布することができます。
	 Allow with Ticket (チケットで許可) – このオプ ションでは、ユーザーが GlobalProtect への接続を 解除しようとすると、エンドポイントに 16 進数の 8 桁のチケット要求ナンバーを表示するチャレンジ レスポンス機構が有効化されます。次にユーザー はファイアウォール管理者またはサポートチーム に連絡し(セキュリティ保護のため、電話をお勧 めします)、この番号を伝える必要があります。 管理者またはサポート担当者は、ファイアウォー ル (Network (ネットワーク) > GlobalProtect > Portals (ポータル))で、Generate Ticket (チケッ ト生成)をクリックし、チケット Request (リクエ スト)番号を入力して Ticket (チケット)番号を取 得できます (16 進数の 8 桁)。管理者またはサポー ト担当はこのチケットナンバーをユーザーに伝え、
GlobalProtect アプリの設定	の意味
--	---
	ユーザーがこれをチャレンジフィールドに入力する とアプリの接続は解除されます。
GlobalProtect(常時接続モード) を切断する理由を以下に表示して	GlobalProtect(常時接続モード)から切断する理由を指 定します。
ください	設定基準:
	• 理由を最大4つまで設定できます。
	 理由をカンマで区切ります(例:理由1、理由2、理 由3、理由4)。
	 理由1つあたりの最大文字数は30文字です。
	 デフォルトでは、設定された理由の末尾には常に 「その他の理由」オプションが含まれているため、 ユーザーは必要に応じてカスタムオプションを入力 できます。
ユーザーが GlobalProtect App を アンインストールできるようにす る (Windows のみ)	ユーザーが GlobalProtectアプリのアンインストールを 許可されているか、許可されている場合は、アプリをア ンインストールする前にユーザーが何をする必要がある かを指定します。
	 Allow (許可)-必要に応じて、すべてのユーザーが GlobalProtectアプリをアンインストールできるよう にします。
	 Disallow (許可しない)-エンドユーザーによ るGlobalProtectアプリのアンインストールを許可し ません。
	 Allow with Password (パスワードで許可する)– GlobalProtectアプリをアンインストールするため のパスワードを強制します。このオプションでは、 ユーザーがアンインストールを続行する前に、パ スワードを入力して確認する必要があります。パス ワードは電子メールで送信するか、企業の Web サイ トに掲示することで配布することができます。
	このオプションには、リリースバージョン 8196-5685 以降が必要です。
ユーザーが GlobalProtect アプリを アップグレードできるようにする	エンドユーザーによる GlobalProtectアプリケーション のソフトウェア アップデートの可否、そして許可する よう設定した場合は、アップグレードのタイミング指定 の可否を設定します。
	 Disallow(無効) – ユーザーはアプリのアップグ レードを行うことができません。

GlobalProtect アプリの設定	の意味
	 Allow Manually(手動を許可) – ユーザーは GlobalProtect アプリで Check Version (バージョン の確認)を選択することで、アップグレードの確認 と実行を手動で行うことができます。
	 Allow with Prompt(プロンプト付きで許可)(デ フォルト) – ファイアウォールで新しいバージョン が起動された場合にプロンプトを表示し、ユーザー は任意のタイミングでアップグレードを行うことが できます。
	 Allow Transparently(メッセージを表示せずに実行) – ポータルで新しいバージョンが使用可能になるとアプリのソフトウェアを自動的にアップグレードします。
	 Internal (内部) – ポータルで新しいバージョンが 使用可能になるとアプリのソフトウェアを自動的 にアップグレードしますが、エンドポイントが企業 ネットワークに内部接続するまで待機します。これ により、低帯域幅の接続を使用したアップグレード による遅延を防ぎます。
ユーザーが GlobalProtect App	ユーザーが、Globalprotectアプリから手動でサインアウ トすることを許可するかを指定します。
からロクアワトできるようにする} (Windows、macOS、iOS、Android、 のみ)	●hYes (はい)(デフォルト)-必要に応じて、すべてのユー ザーが GlobalProtectアプリからサインアウトできる ようにします。
	 No (いいえ) – エンドユーザーに GlobalProtect アプ リからのサインアウトを許可しないでください。
	このオプションには、リリースバージョン 8196-5685 以降が必要です。
シングル サインオンを使用する (Windows)	シングルサインオン(SSO)を無効化する場合はNo[いいえ]を選択します。SSO が有効化されている場合、GlobalProtect アプリはユーザーの Windows ログイン認証情報を使用して自動的に認証を行い、GlobalProtect ポータルおよびゲートウェイに接続します。GlobalProtectはサードパーティ認証情報をラップすることができるので、サードパーティの認証情報プロバイダを使用してWindowsログイン認証情報をラップしている場合でも認証と接続を行うことができます。
Smart Card PIN (Windows) にシン グルサインオンを使用	この設定を使用すると、スマート カードを使用してシ ングル サインオン (SSO) で認証するエンド ユーザー が、シームレスな SSO エクスペリエンスを実現するた

GlobalProtect アプリの設定	の意味
(Windows 10 以降) コンテンツ リリース バー ジョン 8451-6911以降および GlobalProtect アプリ バージョン 6.0.0 以降が必要です。	めに、スマートカード Personal Identification Number (PIN) を GlobalProtect アプリに再入力することなく接続 できます。GlobalProtect が PIN をキャッシュできるの は、スマートカード プロバイダーが許可している場合 のみであることに注意してください。 「スマートカードPINにSSOを使用する」を有効にする
	前に、エントユーリーエントホイントに事前にサフロイ された設定を設定します。次に、この設定を有効にする には、Yesを選択します。
Single Sign-On (シングル サインオ ン - SSO) を使用します (macOS)	シングルサインオン (SSO) を無効化する場合は No [いいえ] を選択します。SSO が有効化されている場合 (デフォルト)、GlobalProtect アプリは macOS ログイン認証情報を使用して自動的に認証を行い、GlobalProtect ポータルおよびゲートウェイに接続します。
	このオプションには、リリースバージョン 8196-5685 以降が必要です。
Clear Single Sign-On Credentials on Logout(ログアウト時にサインオ ンの認証情報を消去) (Windows のみ)	ユーザーのログアウト後もサインオン認証情報を保存し ておく場合はNo[いいえ] を選択します。ユーザーのロ グアウト時に消去し、次回ログイン時に再度認証情報の 入力を求める場合はYes[はい](デフォルト)を選択し ます。
認証の失敗時にはデフォルトの認 証を使用	Kerberos認証のみを使用する場合はNo[いいえ] を選択 します。Kerberos 認証が失敗したときにデフォルトの 認証方法を使用して認証を再試行する場合は Yes(は い)(デフォルト)を選択します。この機能は Mac お よび Windows エンドポイントでのみサポートされてい ます。
SAML 認証に既定のブラウザを使 用 (リリースバージョン 8284-6139 以降の GlobalProtect アプリ 5.2 以 降が必要)	Security Assertion Markup Language (SAML) 認 証によってエンドユーザーを認証するように GlobalProtect ポータルを構成した場合は、Yes を選択 して、Chrome、Firefox、Safari などのの既定のシス テムブラウザー で保存したユーザー資格情報を使用し て、GlobalProtect に同じログインを利用して SAML 対 応アプリケーションに接続できるようにします。クラウ ド認証サービスで SAML を使用している場合は、この 設定を有効にする必要があります。
	は、Windows、macOS、Linux、Android、および iOS エンドポイントの既定のブラウザーが SAML 認証に既

GlobalProtect アプリの設定	の意味
	定のシステム ブラウザーを使用できるように、事前に 設定 を変更する必要があります。
	谷接続が既定のブラウザーで新しいタ ブを開かないようにするには、認証オー バーライドを構成します。
VPN 接続タイムアウトの自動復元	ネットワークの不安定化やエンドポイントの状態の変 化によりトンネルが切断されたときに、GlobalProtect アプリが実行する動作を指定するタイムアウト値 (0~180分)を入力します。デフォルトは 30 です。
	 O-トンネルが切断された後に GlobalProtect がトン ネルを再確立しようとしないように、この機能を無 効にします。
	 1-180-ここで指定したタイムアウト値を超えない 期間、トンネルがダウンした場合、GlobalProtect がトンネル接続を再確立しようとするように、こ の機能を有効にします。たとえば、タイムアウト 値が 30 分の場合、トンネルが 45 分間切断された 場合、GlobalProtect はトンネルを再確立しようと しません。ただし、トンネルが 15 分間切断され た場合、分数がタイムアウト値を超えていないた め、GlobalProtect は再接続を試みます。
	 VPN 常時オンが機能しており、タイムアウト値が切れる前にユーザーが外部ネットワークから内部ネットワークに切り替えると、GlobalProtect はネットワーク探索を実行しません。その結果、GlobalProtect は最後の既知の外部ゲートウェイへのトンネルを再確立します。内部ホスト検出をトリガするには、GlobalProtect コンソールからネットワークの再検出を選択する必要があります。
VPN 接続の復元試行間の待機時間 (分)	Automatic Restoration of VPN Connection Timeout(VPN 接続タイムアウトの自動復元)を有効に したときに、最後に接続されたゲートウェイとの接続を 再確立する試行の間に、GlobalProtect アプリが待機す る時間を秒単位で入力します。ネットワークの状態に応 じて、より長い待機時間または短い待機時間を指定しま

GlobalProtect アプリの設定	の意味
	す。指定できる範囲は1~60秒で、デフォルトは5秒 です。
エンドポイントトラフィックポリ シーの適用 (Windows 10 以降および macOS 11 以降のみ) コンテンツ リリース バージョ ン 8450-6909 以降および GlobalProtect アプリ 6.0.0 以降が 必要	エンドポイントが GlobalProtect に接続されていると きに物理アダプター上のトラフィックを防止するよう に、エンドポイント・トラフィック・ポリシーの適用 を構成します。これにより、悪意のある受信接続、物 理アダプターにバインドしてトンネルをバイパスするア プリケーション、ルーティングテーブルを改ざんして GlobalProtect トンネルをバイパスするエンド ユーザー など、セキュリティを妨害しようとする試みから保護さ れます。
	 No - エンドポイントトラフィックポリシーの適用を
	 TCP/UDP トンネル IP アドレス タイプに基づくトラフィック: TCP/UDP トラフィックに対するエンドポイントトラフィック ポリシーの適用を有効にします。この機能は、トンネル IP アドレス タイプに基づくトラフィックに対して有効になります。トンネルが IPv4 の場合、この機能は IPv4 トラフィックにのみ適用されます。トンネルが IPv6 の場合、この機能は IPv6 トラフィックにのみ適用されます。
	 すべてのTCP/UDPトラフィック:トンネルIPアドレスタイプに関係なく、すべてのTCP/UDPトラフィックに対してエンドポイントトラフィックポリシーの適用を有効にします。トンネルIPアドレスタイプがIPv4の場合、エンドポイントトラフィックポリシーの適用はすべてのTCP/UDP(IPv4またはIPv6)トラフィックに適用されます。トンネルIPアドレスタイプがIPv6の場合、エンドポイントトラフィックポリシーの適用はすべてのTCP/UDP(IPv4またはIPv6)トラフィックに適用されます。
	 すべてのトラフィック:トンネル IP アドレスタイプに 関係なく、すべての TCP、UDP、ICMP、およびその 他のすべてのプロトコルに対してエンドポイントト ラフィック ポリシーの適用を有効にします。
ネットワークアクセスの際に必ず GlobalProtect 接続を利用する	すべてのネットワーク トラフィックに GlobalProtect トンネルを通過するように強制する場合は Yes(は い)を選択します。ネットワーク アクセスのために GlobalProtect を必要とせず、GlobalProtect が無効また

GlobalProtect アプリの設定	の意味
	は切断されている場合でもユーザーがインターネットに アクセスできる状態の場合は、 No (いいえ)(デフォ ルト)を選択します。
	トラフィックがブロックされる前にユーザーに指示を 出す場合、Traffic Blocking Notification Message(トラ フィック ブロックの通知メッセージ)を設定し、さら に任意でメッセージを表示するタイミングを指定します (Traffic Blocking Notification Delay(トラフィックブ ロックの通知の遅延))。
	キャプティブポータルへの接続を確立するために必要な トラフィックを許可するには、Captive Portal Exception Timeout(キャプティブポータルの例外タイムアウ ト)を指定します。ユーザーは、タイムアウトの時間が 過ぎるまでの間にポータルに認証する必要があります。 追加の指示を提供するには、Captive Portal Detection Message (キャプティブポータルの検知メッセージ)を設 定し、任意でメッセージを表示するタイミングを指定し ます(Captive Portal Notification Delay (キャプティブ ポータルの通知の遅延))。
	 ・ ・ 大抵の場合、デフォルトの選択肢(No(いいえ))を使用することになります。Yes (はい)を選択すると、エンタープライズ内 の内部ゲートウェイあるいはエンタープ ライズネットワーク外の外部ゲートウェ イにアプリが接続するまで、エンドポイ ントを出入りするすべてのネットワーク トラフィックがブロックされます。 ・
ネットワーク アクセス のGlobalProtect接続の強制が有効 で、GlobalProtect接続が確立され ていない場合に、指定されたホス ト/ネットワークへのトラフィック を許可する	必要に応じて、ネットワークアクセスに GlobalProtect を適用しても接続が確立されない場合に、アクセスを許 可する最大 10 個の IPアドレスまたはネットワーク セ グメントを設定できます。複数の値はコンマで区切り、 エントリ間にスペースを追加しないでください。除外 を設定すると、GlobalProtectが切断されているときに ユーザーがローカルリソースにアクセスできるように なり、ユーザーエクスペリエンスを向上させることがで きます。たとえば、GlobalProtect が接続されていない 場合、GlobalProtect は link-local アドレスを除外して、 ローカル ネットワーク セグメントまたはブロードキャ ストドメインへのアクセスを許可できます。
Enforce GlobalProtect Connection for Network Access が有効	ネットワーク アクセスに対して GlobalProtect 接続を強 制するときにアクセスを許可する完全修飾ドメイン名

GlobalProtect アプリの設定	の意味
で、GlobalProtect Connection が 確立されていない場合、指定され た FQDN へのトラフィックを許可 する (Windows および macOS 10.15.4 以降) コンテンツ リリース バージョン 8284-6139 以降と GlobalProtect アプリ 5.2 以降が必要です。	 (FQDN)を指定します。ネットワークアクセスに対して GlobalProtect 接続を適用し、GlobalProtect が接続を確 立できない場合に、アクセスを許可する完全修飾ドメイ ン名を最大 40 個まで構成できます。FQDN 除外を構成 することで、GlobalProtect が切断されたときにエンド ユーザーが特定のリソースにアクセスできるようにす ることで、ユーザーエクスペリエンスを向上させるこ とができます。たとえば、エンドポイントは、Enforce GlobalProtect for Network Access (ネットワークアクセ スに対するGlobalProtectの適用)機能が有効になってい る場合でも、認証を目的としたクラウドホストIDプロバ イダー (IdP) またはリモートデバイス管理サーバと通信 することができます。 macOS の最近の変更により、一度 に読み込まれる複数のネットワー ク拡張機能に対して FQDN 除外を 使用して GlobalProtect 接続を強制 することは、Enforce GlobalProtect Connection for Network Access が有効 で、GlobalProtect Connection が確立さ れていない場合、DnsClient.Net設定が 有効で、Cortex XDR が実行されている 場合に、GlobalProtect で Allow traffic to specified FQDN へのトラフィックを許可す る環境など、特定の状況では機能しませ ん。
キャプティブポータルの例外タイ ムアウト (秒)	ネットワークアクセスに GlobalProtect を適用する一 方で、ユーザーがキャプティブ ポータルに接続するた めの十分な猶予期間を設定する場合、タイムアウトの 秒数を指定します(範囲は 0 ~ 3600)。たとえば、 値が 60 の場合、GlobalProtect がキャプティブ ポータ ルを検出した後 1 分以内に、ユーザーはキャプティブ ポータルにログインする必要があります。値が 0 の場 合、GlobalProtect はユーザーがキャプティブ ポータル に接続することを許可せず、即座にアクセスをブロック します。
キャプティブ ポータルの検出時 にデフォルトのブラウザで Web ページを自動的に起動する	ユーザーがキャプティブ ポータルにシームレスにログ インできるように、キャプティブ ポータルの検出時 にデフォルトの Web ブラウザを自動的に起動するに は、デフォルトの Web ブラウザの起動時に Web トラ フィックを開始する最初の接続試行に使用する Web サ イトの完全修飾ドメイン名または IP アドレスを入力し

GlobalProtect アプリの設定	の意味
	ます(最大長は 256 文字)。次に、キャプティブ ポータル はこのウェブサイト接続の試行を一旦遮断し、デフォル トのウェブブラウザをキャプティブ ポータルのログイ ンページにリダイレクトします。このフィールドが空の 場合 (デフォルト)、GlobalProtect はキャプティブ ポー タルの検出時にデフォルトの Web ブラウザを自動的に 起動しません。
トラフィックブロックの通知遅延 (秒)	通知メッセージを表示するタイミングを指定する場合、 値に秒数を指定します。ネットワークが到達可能となっ た後、GlobalProtect は通知を表示するまでのカウント ダウンを開始します(範囲は 5 ~ 120、デフォルトは 15)。
Display Traffic Blocking Notification Message(トラフィッ クブロックの通知メッセージの表 示)	GlobalProtect がネットワーク アクセスに必要な場合 にメッセージを表示するかどうかを指定します。メッ セージを無効化する場合は No (いいえ)を選択しま す。メッセージを有効化する場合は Yes (はい)を 選択します (GlobalProtect が切断されている状態で ネットワークは到達可能であることを検出したとき に、GlobalProtect はメッセージを表示します)。
トラフィックブロックの通知メッ セージ	GlobalProtect がネットワーク アクセスに必要な場 合にユーザーに表示する通知メッセージをカスタマ イズします。GlobalProtect が切断されている状態で ネットワークは到達可能であることを検出したとき に、GlobalProtect はメッセージを表示します。メッ セージによって、トラフィックがブロックされている理 由を示し、接続する手順を提示できます。以下に例を示 します。
	ネットワークにアクセスするには、まず GlobalPr otect に接続します。
	メッセージは 512 文字以下にしてください。
ユーザーがトラフィックブロック の通知を無視することを許可	トラフィック ブロック通知を常に表示する場合は No(いいえ)を選択します。デフォルトの値は Yes(はい)に設定されており、ユーザーは通知を無視 できます。
Display Captive Portal Detection Message(キャプティブポータル の検知メッセージの表示)	GlobalProtect がキャプティブ ポータルを検出したとき にメッセージを表示するかどうかを指定します。メッ セージを表示する場合は Yes(はい)を選択します。 メッセージを表示しない場合は No(いいえ)(デフォ

GlobalProtect アプリの設定	の意味
	ルト)を選択します(GlobalProtect がキャプティブ ポータルを検出したとき、GlobalProtect はメッセージ を表示しません)。
	 キャプティブポータルの検知メッセージ を有効化すると、キャプティブポータル の例外タイムアウトの85秒前にメッセージが表示されます。そのため、Captive Portal Exception Timeout (キャプティブ ポータルの例外タイムアウト)が90秒 以下の場合、メッセージはキャプティブ ポータルが検出された5秒後に表示され ます。
キャプティブポータルの検知メッ セージ	GlobalProtect がネットワークを検出した場合に、キャ プティブ ポータルに接続するための追加手順をユー ザーに表示する通知メッセージをカスタマイズします。 以下に例を示します。
	GlobalProtectは、お客様がインターネットに接続 するためのネットワークアクセスを一時的に許可して います。インターネットプロバイダの指示に従ってく ださい。接続をタイムアウトにした場合は、Global Protect を開き、[接続] をクリックして再試行し ます。
	メッセージは 512 文字以下にしてください。
認証(キャプティブ)ポータルの 通知の遅延(秒)	キャプティブ ポータルの検出メッセージを有効にする と、キャプティブ ポータルの検出後、GlobalProtect が 検出メッセージを表示するまでの遅延を秒単位で指定で きます (範囲は 1 ~ 120、デフォルトは 5)。
クライアントの証明ストアの検索	証明書のタイプ、またはアプリが個人用証明書スト アで検索する証明書を選択します。GlobalProtect アプリは、ポータルやゲートウェイへの認証を行 い、GlobalProtect ゲートウェイへのVPNトンネルを確 立する際にこの証明書を使用します。

GlobalProtect アプリの設定	の意味
	 ログイン後にユーザーストアを使用する場合は、ログオン前のユーザープロファイルにユーザーとマシンストアを使用することをお勧めします。ログオン前のユーザーはマシンストアのみを使用しますが、このパラメーターをマシンのみに設定すると、アプリがGlobalProtectポータルから構成を取得するまで、ユーザーはユーザーストアを使用できなくなります。
	 User (ユーザー) – ユーザー アカウントのローカル な証明書を使用して認証を行います。
	 Machine[マシン] – エンドポイントのローカルな証明 書を使用して認証を行います。この証明書はエンド ポイントの使用を許可されているすべてのユーザー に適用されます。
	 User and machine[ユーザーおよびマシン](デフォルト) – ユーザー証明書およびマシン証明書を使用して認証します。
SCEP 証明書更新期間(日)	SCEPが生成した証明書を失効前に更新するための機能 です。ポータルが PKI システムの SCEP サーバーに対 し、新しい証明書の要求を証明書失効日の最大何日前 に行うかを指定します(範囲は 0 ~ 30、デフォルトは 7)。0を指定すると、ポータルはクライアント設定を 更新する際に、クライアント証明書の自動更新を行いま せん。
	アプリが新しい証明書を取得できるようにする場合、 ユーザーは更新期間内にログインする必要があります (ユーザーがこの期間内にログインしない場合、ポータ ルは新しい証明書の要求を行いません)。
	例えば、クライアント証明書の有効期間が90日、証明 書更新期間が7日だったとします。証明書有効期間の 最後7日間のうちにユーザーがログインした場合、ポー タルは証明書を生成し、更新されたクライアント設定 と共にダウンロードします詳細は「GlobalProtect App Config Refresh Interval (hours)(GlobalProtect アプリ設 定の更新間隔(時間))」を参照してください。
クライアント証明向けの拡張キー 使用 OID	このオプションを使用して、macOS または Windows エ ンドポイントに複数の証明書がインストールされている 場合に、証明書選択プロセスを簡素化および改善する

GlobalProtect アプリの設定	の意味
(Windows および macOS のみ)	ために選択するクライアント証明書を決定するために GlobalProtect が使用するオブジェクト識別子 (OID) を 指定します。
	既定では、GlobalProtect はクライアント認証の目的 (OID 1.3.6.1.5.5.7.3.2)を指定する証明書を自動的に フィルター処理するため、クライアント認証に関連 付けられた OID を指定する必要はありません。ただ し、GlobalProtect で選択する証明書を区別するために 別の OID を使用する場合は、証明書の作成時に別の 証明書使用法を指定し、Extended Key Usage OID for Client Certificate を対応する OID に設定することがで きます。最も一般的に使用される OID のいくつかは次 のとおりです。
	 1.3.6.1.5.5.7.3.1 - Server Authentication (サーバー認証)
	• 1.3.6.1.5.5.7.3.3-Code Signing コード署名
	• 1.3.6.1.5.5.7.3.4-Email Protection 電子メール保護
	 1.3.6.1.5.5.7.3.5–IPSec End System IPSec エンドシ ステム
	• 1.3.6.1.5.5.7.3.6–IPSec トンネル
	• 1.3.6.1.5.5.7.3.7-IPSec ユーザ
	• 1.3.6.1.5.5.7.3.8—Time Stamping タイムスタンプ
	• 1.3.6.1.5.5.7.3.9-OCSP Signing OCSP 署名
スマートカードの取り外し時に接 続を維持 (Windows のみ)	クライアント証明書を含むスマート カードをユーザー が取り外したときに接続を維持する場合は Yes(は い)を選択します。ユーザーがスマート カードを取り 外したときに接続を終了する場合は No(いいえ)(デ フォルト)を選択します。
詳細ビューの有効化	アプリのユーザーインターフェイスを基本的な最小限 のビューに制限する場合は、No(いいえ)を選択しま す。
ユーザーがウェルカムページを終 了できるようにする	ユーザーが接続を開始するたびにウェルカムページを 表示する場合は、No(いいえ)を選択します。この制 約をかけることで、コンプライアンス維持のために組織 から求められる利用規約などの重要な情報をユーザーが 忘れてしまわないようにすることができます。

GlobalProtect アプリの設定	の意味
トンネルを作成する前にユーザー に利用規約に同意してもらう	Yes を選択すると、エンド ユーザーが企業ポリシーに 準拠するための利用規約に同意し、GlobalProtect に接 続する前に会社の利用規約を確認するページを表示する 必要があります。
	このオプションを [はい]に設定する前に、 ネット ワーク > GlobalProtect > ポータル > <i><portal_config< i=""> > General)を介して GlobalProtect ウェルカム ページを 構 成する必要があります。</portal_config<></i>
ネットワーク オプションの再検出 の有効化	ユーザーによる手動ネットワーク再検出を行えないよう にする場合は、No(いいえ)を選択します。
[ホスト プロファイルの再送信] オ プションを有効にする	ユーザーが手動で最新 HIP の再送信をトリガーできな いようにする場合は、No(いいえ)を選択します。
ポータル アドレスの変更をユー ザーに許可する	GlobalProtect アプリの Home(ホーム)タブの Portal(ポータル)フィールドを無効化する場合 は、No(いいえ)を選択します。しかしこの場合、 ユーザーは接続するポータルを指定できなくなってしま うので、デフォルトポータルアドレスをWindowsレジ ストリまたはMac plistに入れておく必要があります。
	 Windows registry (Windowsレジストリ) – HKEY_LOCAL_MACHINE\SOFTWARE\PaloAlto Networks\GlobalProtect\PanSetup、キー はPortal
	 Mac plist-/Library/Preferences/ com.paloaltonetworks.GlobalProtect.pansetup.plis キーは Portal
	ポータル アドレスの事前デプロイの詳細 は、GlobalProtect 管理者ガイドの「Customizable App Settings(カスタマイズ可能なアプリ設定)」を参照し てください。
ユーザーが無効なポータルサー バー証明書で続行できるようにす る	ポータル証明書が無効なときにアプリがポータルとの接 続を確立できないようにする場合は、 No (いいえ)を 選択します。
GlobalProtect アイコンの表示	エンドポイントで GlobalProtect アイコンを非表示にす る場合は、No(いいえ)を選択します。アイコンが非 表示の場合、ユーザーはトラブルシューティングの参 照、パスワードの変更、ネットワークの再検出、また はオンデマンド接続の実行などの特定のタスクを行えま せん。しかし、ユーザーの操作が必要な場合、HIP通知

GlobalProtect アプリの設定	の意味
	メッセージ、ログインプロンプト、および証明書ダイア ログは表示されるようになっています。
ユーザースイッチトンネルの名前 変更のタイムアウト(秒) (Windowsのみ)	リモート ユーザーが Microsoft のリモート デスクトッ ププロトコル (RDP) を使用してエンドポイントにロ グインしたのち、GlobalProtect ゲートウェイでの認証 状態を保つ秒数を指定します(範囲は0~600、デフォ ルトは 0)。リモートユーザーに一定の時間内に認証を 求めることで、セキュリティを保つことができます。
	新しいユーザーを認証しトンネルをそのユーザー用に切 り替えると、ゲートウェイはトンネルの名称を変更しま す。
	0を指定するとユーザートンネルの名称は変更されま せんが、即座に強制終了されるようになります。この 場合、リモートユーザーは新しいトンネルを与えられ、 ゲートウェイへの認証の際、制限時間は設けられません (設定済みのTCPタイムアウトを除く)。
Pre-Logon Tunnel Rename Timeout (sec) (pre-logon トンネルの名 前変更のタイムアウト (秒)) (Windows のみ)	この設定は、エンドポイントをゲートウェイに接続する pre-logon トンネルを GlobalProtect がどのように処理 するのかを管理します。
	値が -1 の場合、ユーザーがエンドポイントにログイ ンした後、pre-logon トンネルはタイムアウトしませ ん。GlobalProtect はトンネルの名称を変更して、ユー ザーに割り当て直します。なお、名称を変更できなかっ た場合やユーザーが GlobalProtect ゲートウェイにログ インしない場合でも、トンネルは持続します。
	値が0の場合、ユーザーがエンドポイントにログオン したとき、GlobalProtect は pre-logon トンネルの名 称を変更する代わりに、即座に pre-logon トンネルを 終了します。この場合、ユーザーに pre-logon トンネ ル経由での接続を許可するのではなく、GlobalProtect がユーザー用の新しいトンネルを開始します。通 常、Connect Method (接続方式)を Pre-logon then On-demand (pre-logon 後オンデマンド) (最初のログ オン後に手動による接続開始をユーザーに強制)に設定 している場合、この設定が一番便利です。
	ユーザーがエンドポイントにログオンした後もログオ ン前トンネルがアクティブのままでいられる秒数を1 ~7200の値で示します。この期間、GlobalProtect は pre-logonトンネルにポリシーを適用します。タイム アウト時間内にユーザーが GlobalProtect ゲートウェ イで認証した場合、GlobalProtect はトンネルをユー

GlobalProtect アプリの設定	の意味
	ザーに割り当て直します。タイムアウト時間内にユー ザーが GlobalProtect ゲートウェイで認証しなかった 場合、GlobalProtect は pre-logon トンネルを終了しま す。
Preserve Tunnel on User Logoff Timeout (ユーザー ログオフ タイ ムアウト時にトンネルを保持) (秒)	ユーザーがエンドポイントからログアウトした後に GlobalProtect が既存の VPN トンネルを保持できる ようにするには、Preserve Tunnel on User Logoff Timeout (ユーザートンネルのログアウト タイムアウ トを保持)の値を指定します (範囲は0~600秒、デ フォルトは0秒です)。デフォルト値の 0 を選択する と、GlobalProtect はユーザーのログアウト後にトンネ ルを保持しません。
Custom Password Expiration Message(カスタムのパスワード 有効期限メッセージ) (LDAP 認証のみ)	パスワードの失効が近づいてきた場合に表示するカス タムメッセージを作成します。メッセージの長さは最 大200文字までです。
Automatically Use SSL When IPSec Is Unreliable (IPSec が信頼できな い場合に SSL を自動的に使用) (時 間)	GlobalProtect アプリケーションに Automatically Use SSL When IPSec Is Unreliable (IPSec を信頼できない場 合に自動的に SSL を使用) する時間 (時間単位) を指定し ます (範囲は 0 ~ 168 時間)。このオプションを指定す ると、GlobalProtect アプリケーションは指定された期 間中、IPSec トンネルを確立しようとしなくなります。 このタイマーは、トンネルのキープアライブがタイムア ウトしたことで IPSec トンネルがダウンする度に開始さ れます。
	デフォルトの値である 0 を採用すると、アプリが IPSec トンネルを正常に確立できた場合に SSL トンネルを確 立するというフォールバックが行われません。IPSec トンネルを確立できない場合にのみ SSL トンネルに フォールバックします。
IPSec から SSL へのフォールバッ ク通知の表示 コンテンツ リリース バージョ ン 8387-6595 以降および GlobalProtect アプリ バージョン 6.0 以降が必要です。	接続が IPSec から SSL に変更されたことを示す通知メッ セージをユーザーに表示させたくない場合は、No を選 択します。デフォルトでは、ユーザーに通知されます。
SSL 接続のみ	ユーザーが IPSec の代わりに SSL を使用することを選択 できるようにするには、Yes を選択します。

GlobalProtect アプリの設定	の意味
GlobalProtect アプリのバージョン 6.0 以降が必要です。	
GlobalProtect 接続 MTU(バイト 単位)	GlobalProtectアプリケーションがゲートウェイに接続す る際に使用する 1,000~1,420 バイトのGlobalProtect接 続最大伝送ユニット (MTU) 値を入力します。デフォ ルトは 1,400 バイトです。標準の1,500 バイト以下の MTU 値を必要とするネットワーク経由で接続するエン ドユーザーの接続エクスペリエンスを最適化すること ができます。MTU サイズを小さくすることで、VPN ト ンネル接続が複数のインターネットサービスプロバイ ダ (ISP) を経由し、MTU が 1,500 バイト未満のネット ワークパスを経由する場合に、フラグメンテーションに よって生じるパフォーマンスおよび接続性の問題を解消 することができます。
内部のゲートウェイ接続の最大試 行回数	GlobalProtectアプリケーションから内部ゲートウェイ に対する接続が失敗した場合に接続を再試行する回数 の上限を入力します(範囲は0~100、デフォルトは 0)。0の場合、GlobalProtectアプリは接続の再試行を 行いません。この値を増やすことで、内部ゲートウェイ が最初の接続試行時に一時的にダウンしていた場合や、 最初の試行時に到達不能であったものの、設定した試行 回数のうちに復旧した場合に、アプリはゲートウェイへ 自動的に接続することができます。また、この値を増や すことで、内部ゲートウェイが最新のユーザー情報およ びホスト情報を確実に受信できるようになります。
高度な内部ホスト検出を有効にする	GlobalProtect アプリによる内部ホスト検出の実行中 に、追加のセキュリティレイヤーを追加します。高度 な内部ホスト検出により、アプリは内部ゲートウェイ のサーバー証明書を検証するだけでなく、内部ホストの リバース DNS ルックアップを実行して、アプリが企業 ネットワーク内にあるかどうかを判断します。 [はい]を選択して、内部ホストの検出中に内部ホス トの逆引き DNS ルックアップを実行するだけでな く、GlobalProtect アプリが内部ゲートウェイのサー バー証明書を検証できるようにします。 内部ゲートウェイのサーバー証明書を検証せずに GlobalProtect アプリが内部ホスト検出を実行するに は、[いいえ](既定)を選択します。
ポータルの接続のタイムアウト (秒)	ポータルへの接続要求に対し応答がなかった場合に、 接続要求がタイムアウトするまでの秒数です(範囲

GlobalProtect アプリの設定	の意味
	は1~600、デフォルトは 30)。ファイアウォールが 777-4484 より前のアプリケーションおよび脅威のコン テンツバージョンを実行している場合、デフォルトは 30です。コンテンツ リリース バージョン 777-4484 で 始まる場合、デフォルトは 5 です。
TCP 接続のタイムアウト(秒)	TCP 接続の両端のいずれかからの応答がないために、 接続要求がタイムアウトするまでの秒数 (範囲は 1 ~ 600)。ファイアウォールが 777-4484 より前のアプリ ケーションおよび脅威のコンテンツ バージョンを実行 している場合、デフォルトは60 です。コンテンツ リ リース バージョン 777-4484 で始まる場合、デフォル トは 5 です。
TCP 受信のタイムアウト(秒)	TCP 要求の応答が一部欠損している場合に、TCP 接続 がタイムアウトするまでの秒数です(範囲は1 ~ 600、 デフォルトは 30)。
ユーザーに GlobalProtect ユーザー セッションの拡張を許可	ユーザーが突然アプリセッションからログアウトしない ように、GlobalProtectアプリケーションのログイン有効 期間セッションを期限切れ前に延長すること。
	[Yes (はい)]を選択すると、ユーザーはGlobalProtectア プリのログイン有効期間セッションを期限切れになる前 に延長して、アプリセッションの突然のログアウトを防 ぐことができます。
	有効期限が切れる前にユーザーがGlobalProtectアプリの ログイン有効期間セッションを延長できないようにする には、[No (いいえ)](デフォルト)を選択します。
HIP 修復プロセスのタイムアウト (秒) コンテンツ リリース バージョ ン8699-7991 以降と GlobalProtect アプリ 6.2.0 以降が必要です。	HIP修復プロセスタイムアウト (秒)を設定し て、GlobalProtectアプリがHIPプロセスチェックに失敗 した場合にHIPプロセス修復スクリプトを実行できるタ イムアウト期間を設定します。
	デフォルトでは、このフィールドは0に設定されており、機能が無効であることを示します。1~600秒の値を入力して、修復スクリプトが終了するまでの時間を指定します。
拡張スプリット トンネル クライア ント証明書公開鍵 コンテンツ リリース バージョ ン8699-7991 以降と GlobalProtect アプリ 6.2.0 以降が必要です。	エンドポイントがスプリットトンネル設定ファイルをホ ストする Web サーバーに接続するために使用できる拡 張スプリットトンネルクライアント証明書公開鍵を指定 します。

GlobalProtect アプリの設定	の意味
スプリット トンネル オプション	Network > GlobalProtect > GlobalProtect > GlobalProtect > Gateway> Client Settings > (Client Config) > Split Tunnel < Domain and Applicationで GlobalProtect ゲートウェイで構成されたドメインを除 外または包めるか、トラフィックに対して分割トンネル ドメインand/orで分割 DNS 機能を有効にするかどうか を指定します。
	Network Traffic Only – Network > GlobalProtect > Gateway> Agent > Client Setting > (Client Config) > Split Tunnel > Domain and Apapplicationion で GlobalProtect ゲートウェイで構成されているドメインを含めるか除外 するかに従って、トラフィックに対して split-tunnel ド メインのみを有効にするには、このオプションを選択し ます。
	Both Network Traffic and DNS – Network > GlobalProtect > Gateway> Agent > Client Set >> (Client Config) > Split Tunnel < Domain and Application で GlobalProtect ゲートウェイで構成されているドメイン を含めるか除外するかに従って、トラフィックに対して 分割トンネルドメインと分割 DNS の両方を有効にする には、このオプションを選択します。 このオプションでは、コンテンツリリース バージョ
トンネルによって割り当てられた DNS サーバーを使用するすべての FQDN を解決する (Windows のみ)	ン8284-6139以降が必要になります。 (GlobalProtect 4.0.3 およびそれ以降のリリー ス) GlobalProtect トンネルが Windows エンドポイント に接続されている場合の DNS 解決設定を行います。
	 Yes (はい) (デフォルト)を選択すると、エンド ポイントが物理アダプタに設定されている DNS サー バーに DNS クエリを送信するのではなく、Windows エンドポイントがゲートウェイで構成した DNS サー バーとのすべての DNS クエリを解決できるようにな ります。
	 No (いいえ)を選択すると、ゲートウェイで構成された DNS サーバーへの最初の照会が解決されない場合、Windows エンドポイントが物理アダプタに設定された DNS サーバーに DNS 照会を送信できるようになります。このオプションは、すべてのアダプタのすべての DNS サーバーを再帰的に照会するネイティブ Windows の動作を保持しますが、一部のDNS 照会を解決するための待機時間が長くなる可能性があります。

GlobalProtect アプリの設定	の意味
	GlobalProtect アプリ 4.0.2 およびそれ以前のリリー スの DNS 設定を行うには、Update DNS Settings at Connect(接続時に DNS 設定を更新する)オプション を使用します。
Prisma Accessのエージェントモー ド コンテンツ リリース バージョン 8700-7994 以降と GlobalProtect アプリ 6.2.0 以降が必要で す。Prisma Access 4.0 推奨または それ以降が必要です。	デフォルトでは、Prisma Accessのエージェント モードはトンネルモードに設定されています。つま り、GlobalProtectアプリは、定義したスプリットトン ネルルールに基づいて、インターネットとプライベート アプリへのアクセスを保護するためにGlobalProtectへ のトンネルを確立します。GlobalProtectアプリの明示的 なプロキシ機能を有効にして、GlobalProtectまたはサー ドパーティのVPNを介してプライベートアプリへのオン デマンドアクセスを提供しながら、インターネットトラ フィックの常時セキュリティを有効にしたい場合は、次 のエージェントモードのいずれかを構成できます。
	プロキシを選択すると、GlobalProtectアプリ は、PACファイルで定義されている転送ルールに基づい てトラフィックをPrisma Accessにプロキシできます。 その後、サードパーティの VPN を使用してプライベー トアプリへのアクセスを保護できます。
	GlobalProtect アプリが PAC ファイルで定義したルー ルに基づいてインターネットトラフィックを明示的な プロキシに送信できるようにするには、[Tunnel and Proxy (トンネルとプロキシ)] を選択します。残りのトラ フィックについては、GlobalProtectアプリケーション は、定義したスプリットトンネリングルールを使用し て、トンネルを介して送信するトラフィックを決定しま す。
Update DNS Settings at Connect(接続時の DNS 設定の更 新)	(GlobalProtect 4.0.2 およびそれ以前のリリー ス)GlobalProtect トンネルの DNS サーバー設定を行い ます。
(Windows のみ) (Deprecated (廃 止))	 No (いいえ) (デフォルト)を選択すると、ゲート ウェイで構成された DNS サーバーへの最初の照会が 解決されない場合、Windows エンドポイントが物理 アダプタに設定された DNS サーバーに DNS 照会を 送信できるようになります。このオプションは、す べてのアダプタのすべての DNS サーバーを再帰的に 照会するネイティブ Windows の動作を保持します が、一部の DNS 照会を解決するための待機時間が長 くなる可能性があります。

GlobalProtect アプリの設定	の意味
	 Yes (はい)を選択すると、エンドポイントの物理 アダプタに設定されている DNS サーバーの代わり に、ゲートウェイで構成した DNS サーバーとのすべ ての DNS 照会を Windows エンドポイントが解決で きるようになります。このオプションを有効にする と、GlobalProtect はゲートウェイの DNS 設定を厳 密に適用し、すべての物理アダプタのスタティック 設定を上書きします。
	 この設定を有効にすると(Yes(はい))、GlobalProtectは以前に保存したDNS設定の復元をさせないために失敗し、その結果、エンドポイントがDNSクエリを解決することを防ぎますできなくなります。この機能は廃止され、このシナリオが発生しないように改良された実装に置き換えられています。以前にこの機能を使用していた場合は、GlobalProtectアプリ4.0.3以降にアップグレードすることを推奨します。 GlobalProtectアプリ4.0.3およびそれ以降のリリースでDNS設定を行うには、Resolve All FQDNs Using DNSServers Assigned by the Tunnel(トンネルによって割り当てられたDNSサーバーを使用するすべてのFQDNを解決する)オプションを使用します。
プロキシ自動構成 (PAC) ファイル の URL	[はい] を選択して、プロキシ自動構成 (PAC) ファイルの URL を GlobalProtect アプリからエンドポイントにプッ シュします。
	プロキシ設定を構成するためにエンドポイントにプッ シュするプロキシ自動構成 (PAC) ファイルの URL を指 定します。最大長は 256文字です。次のプロキシ自動構 成 (PAC) ファイルの URL メソッドがサポートされてい ます。
	 Proxy Auto-Config (PAC) 標準 (例: http:// pac.<hostname ip="" or="">/proxy.pac)。</hostname>
	• Web Proxy Auto-Discovery Protocol (WPAD)標準 (例: http://wpad. <hostname ip="" or="">/wpad.dat)。</hostname>
Detect Proxy for Each Connection(接続ごとにプロキシ を検出)	ポータル接続用のプロキシを自動検出し、以降の接続 にそのプロキシを使用する場合は No [いいえ] を選択し

GlobalProtect アプリの設定	の意味
(Windowsのみ)	てください。接続のたびにプロキシを自動検出する場合 は Yes [はい](デフォルト)を選択してください。
Tunnel Over Proxy をセットアップ (Windows および Mac のみ)	GlobalProtect にプロキシを使用させるか、バイパス させるか指定します。GlobalProtect にプロキシをバ イパスするよう求める場合はNo (いいえ)を選択しま す。GlobalProtect にプロキシを使用するよう求める場 合はYes (はい)を選択します。GlobalProtect プロキシの 使用に応じて、エンドポイントの OS、トンネル タイ プ、ネットワーク トラフィックの挙動が異なります。
Send HIP Report Immediately if Windows Security Center (WSC) State Changes (Windows セキュ リティー センター (WSC) の状態 が変更された場合に HIP レポート を即座に送信) (Windows のみ)	Windows セキュリティー センター(WSC)の状態が 変更された際に、GlobalProtect アプリに HIP データを 送信させない場合は No(いいえ)を選択してくださ い。WSC の状態が変更された際に即座に HIP データを 送信する場合は Yes(はい)(デフォルト)を選択しま す。
Enable Inbound Authentication Prompts from MFA Gateways(MFA ゲートウェイか らのインバウンド認証プロンプト の有効化)	多要素認証(MFA)をサポートするに は、GlobalProtect エンドポイントはゲートウェイから のインバウンド UDP プロンプトを受信および承認す る必要があります。GlobalProtect エンドポイントがプ ロンプトを受け取り、受信確認できるようにする場合 は Yes (はい)を選択します。GlobalProtect でゲート ウェイからの UDP プロンプトをブロックする場合は No (いいえ) (デフォルト)を選択します。
Network Port for Inbound Authentication Prompts (UDP)(イ ンバウンド認証プロンプト用の ネットワーク ポート(UDP))	MFA ゲートウェイからのインバウンド認証プロンプト の受け取りに GlobalProtect エンドポイントが使用する ポート番号を指定します。デフォルト ポートは 4501 で す。ポートを変更するには、1 ~ 65535 の数値を指定 します。
Trusted MFA Gateways(信頼され た MFA ゲートウェイ)	GlobalProtect エンドポイントが多要素認証において信 頼するファイアウォールまたは認証ゲートウェイのリス トを指定します。GlobalProtect エンドポイントが指定 されたネットワーク ポートで UDP メッセージを受信し た場合、UDP プロンプトが信頼されたゲートウェイか ら来ているときにのみ、GlobalProtect は認証メッセー ジを表示します。
インバウンド認証メッセージ	追加認証が必要なリソースにユーザーがアクセスしよう としたときに表示する通知メッセージをカスタマイズ します。ユーザーが追加認証が必要なリソースにアク

GlobalProtect アプリの設定	の意味
	セスしようとすると、GlobalProtect はインバウンド認 証プロンプトを含む UDP パケットを受信し、このメッ セージを表示します。UDP パケットには、Configure Multi-Factor Authentication(多要素認証の設定)時に 指定する認証ポータルページの URL も含まれていま す。GlobalProtect は自動的に URL をメッセージに付加 します。以下に例を示します。
	追加の認証を必要とする保護リソースにアクセスしよ うとしました。認証に進む
	メッセージは255文字以下にしてください。
IPv6 優先	GlobalProtect エンドポイントの通信用の優先プロトコ ルを指定します。優先プロトコルを IPv4 に変更する場 合は No(いいえ)を選択します。デュアル スタック 環境で IPv6 を優先接続にする場合は Yes(はい)(デ フォルト)を選択します。
パスワード メッセージを変更	ユーザーが Active Directory(AD)パスワードを変更 したときにパスワード ポリシーまたは要件を指定する メッセージをカスタマイズします。以下に例を示しま す。
	パスワードには、少なくとも 1 つの数字と 1 つの 大文字を含める必要があります。
	簡体字中国語などの2バイトのUnicode 言語の場合、 メッセージは255 文字以下でなければなりません。日 本語の場合、メッセージは128 文字以下にしてください。
Log Gateway Selection Criteria(ゲートウェイ選択基準の ログへの記録)	GlobalProtectアプリケーションがゲートウェイの選 択基準のログをファイアウォールに送信する設定にす るには、YES(はい)を選択します。デフォルト設定 はNone(なし)です。アプリケーションは、ゲート ウェイ選択基準の拡張ログをファイアウォールに送信し ません。
Autonomous DEM and GlobalProtect App Log Collection for Troubleshootingを有効にする コンテンツ リリース バージョ ン 8350-14191 以降が必要で	GlobalProtect アプリが Report an Issue オプションを 表示できるようにするにはYes.を選択して、エンド ユーザーがトラブルシューティングログと診断ログ を Cortex Data Lake に直接送信できるようにします。 ポータルからクライアント証明書としてプッシュされ

GlobalProtect アプリの設定	の意味
す。GlobalProtect アプリ 5.2.5 以 降が必要です。	る Cortex Data Lake 証明書を構成して、Report an Issue オプションを表示する必要があります。この証明書 は、クライアントがログを送信するときに Cortex Data Lake に対して認証するために使用されます。この設定 が No (既定) に設定されている場合、GlobalProtect ア プリは Report an Issue オプションを表示せず、エンド ユーザーはトラブルシューティング ログと診断ログを Cortex Data Lake に送信できません。
自律 DEM 更新通知の表示	ADEM エージェントが更新されるたびにユーザーに通 知を表示できるようにするには、Yes を選択します。
これらの宛先 Web サーバーに関 する診断テストを実行する コンテンツ リリース バージョ ン 8350-14191 以降が必要で す。GlobalProtect アプリ 5.2.5 以 降が必要です。	最大 10 個の HTTPS ベースの宛先 URL を入力して、 プローブのパフォーマンス テストを開始します。これ らの診断テストは、Enable Autonomous DEM および GlobalProtect App Log Collection for Troubleshooting を選択した場合にのみ実行されます。入力する宛先 URL には、IP アドレスまたは完全修飾ドメイン名 (https://10.10.10.10/resource.html、https://webserver/ file.pdf、https://google.com など)を指定できます。
Prisma Access 用の自律 DEM エンドポイント エージェント (Windows & Mac のみ) Windows 10 および macOS で のみ動作します。コンテンツリ リースバージョン8393-6628以 降。GlobalProtect アプリ 5.2.6 以 降が必要です。	GlobalProtect アプリのインストール中に Autonomous DEM (ADEM) エンドポイント エージェントをインス トールするかどうかを指定し、エンド ユーザーがアプ リからユーザー エクスペリエンス テストを有効または 無効にできるようにします。
	 Install and user can enable/disable agent from GlobalProtectを選択すると、GlobalProtect アプリ のインストール中に ADEM エンドポイント エー ジェントをインストールし、エンド ユーザーが GlobalProtect アプリからユーザー エクスペリエンス テストを有効または無効にできるようにします。
	 Install and user cannot enable/disable agent from GlobalProtectを選択すると、GlobalProtect アプリ のインストール中に ADEM エンドポイント エー ジェントをインストールし、エンド ユーザーが GlobalProtect アプリからユーザー エクスペリエンス テストを有効または無効にできないようにします。
	 Do Not Install(デフォルト)を選択する と、GlobalProtect アプリのインストール中に ADEM エンドポイント エージェントをインストールしない ようにします。

GlobalProtect アプリの設定	の意味
隔離メッセージに追加されたデバ イス	デフォルトでは、GlobalProtect は、エンド ユーザーの デバイスが検疫されると、次のメッセージを表示しま す。
	このデバイスからのネットワークへのアクセスは、組 織のセキュリティ ポリシーに従って制限されていま す。IT 管理者に問い合わせてください。
	この既定のメッセージは、最大 512 文字の独自のカス タム メッセージに置き換えることができます。
隔離メッセージから削除されたデ バイス	デフォルトでは、エンドユーザーのデバイスが検疫から 削除されたときに、GlobalProtect は次のメッセージを 表示します。
	このデバイスからのネットワークへのアクセスは、組 織のセキュリティ ポリシーに従って復元されました 。
	この既定のメッセージは、最大 512 文字の独自のカス タム メッセージに置き換えることができます。
起動時にステータスパネルを表示 (Windows のみ)	Yes (はい)を選択すると、ユーザーが初めて接続を確立 する際に自動的に GlobalProtect のステータスパネルを 表示します。No (いいえ)を選択すると、ユーザーが初 めて接続を確立する際に GlobalProtect のステータスパ ネルが表示されません。
グローバルプロテクト UI をユー ザー入力に対して保持できるよう にする	Yes を選択すると、エンド ユーザーが資格情報を入力 しているときに、GlobalProtect アプリが画面にステー タス パネルを引き続き表示できるようにします。
(Windows 10 以降および macOS)	
コンテンツ リリース バージョン 8450-6909 以降と GlobalProtect アプリ 6.0.0 以降が必要です。	
GlobalProtect アプリの無効化	

パスコード/パスコードの再入力	Allow User to Disable GlobalProtect App[ユーザーに
	よるGlobalProtectアプリの無効化] の設定がAllow with
	Passcode[パスコードで許可] の場合、パスコードの入
	力と再入力を行います。パスコードはパスワードと同じ
	ように、記録して安全な場所に保管してください。新規

GlobalProtect アプリの設定	の意味	
	のGlobalProtectユーザーに対してパスコードを配布する 場合は、電子メールを使用するか、企業ウェブサイトの サポートエリアに掲示する方法があります。	
	エンドポイントが VPN 接続を確立できず、その機 能が使用できない状況であれば、ユーザーはアプリ のインターフェイスにこのパスコードを入力して GlobalProtect アプリを無効化し、VPN を使用せずにイ ンターネットへアクセスすることができます。	
ユーザーが切断できる最大回数	ユーザーがファイアウォールへの接続を行う前 にGlobalProtectを無効にできる最大回数を指定します。 デフォルトの0に設定すると、ユーザーは回数の制限を 受けることなくアプリを無効化することができます。	
切断タイムアウト (分)	GlobalProtect アプリを切断できる最大分数を指定しま す。ここで指定した時間が経過すると、アプリはファイ アウォールへの接続を試みます。デフォルトのOに設定 すると、時間の制限を受けることなく無効化することが 可能になります。	
	(※) 無効化タイムアウトの値を設定し、ユー ザーがアプリを無効化できる期間を制限 します。これにより、タイムアウトの期 間が過ぎた際に GlobalProtect に VPN を 再び確立させることで、ユーザーおよび ユーザーによるリソースへのアクセスを 保護することができます。	
Endpoint Security Managerの設定		
Mobile Security Manager	モバイルデバイス管理(MDM)にGlobalProtect Mobile Security Managerを使用している場合、GP-100アプラ イアンス上のデバイスチェックイン(登録)インター フェイスのIPアドレスまたはFQDNを入力します。	
登録ポート	モバイルエンドポイントが登録のためにGlobalProtect Mobile Security Managerに接続する際に使用するポート 番号。Mobile Security Manager はデフォルトでポート 443 をリッスンするように設定されています。	

GlobalProtect アプリの設定	の意味
	このポート番号のままに設定しておけ ば、モバイルエンドポイントのユーザー は登録を行う際にクライアント証明書の 提示を求められません(使用可能な値は 443、7443、および 8443)。

GlobalProtect ポータルの **Agent HIP Data Collection**(エージェント **HIP** データ収 集)タブ

ネットワーク > グローバルプロテクト > ポータル > <portal-config> > エージェント > <agent-config> > HIP データ収集

HIP Data Collection (HIP データ収集)タブを選択し、アプリが HIP レポートでエンドポイントから収集するデータを定義します:

GlobalProtect HIP デー タ収集設定	の意味
HIP データの収集	アプリに HIP データの収集と送信を行わせたくない場合はこのオプ ションを解除します。
	 GlobalProtect を有効化し、HIP ベースのポリシーを適用するための HIP データを収集することで、ファイアウォールがエンドポイントから得た HIP データをユーザーが定義して適切なポリシーに適用する HIP プロファイルおよび/または HIP オブジェクトとマッチできるようにします。
Max Wait Time (sec)(最大待機時間 (秒))	アプリが HIP データの検索を行う秒数を指定します。この時間が経 過すると入手したデータが送信されます(範囲は 10~60、デフォ ルトは 20)。
証明書プロファイル	GlobalProtect アプリケーションが送信したマシン証明書にマッチ させるために GlobalProtect ポータルが使用する証明書プロファイ ルを選択します。
カテゴリの除外	アプリによる HIP データ収集の対象外とするホスト情報カテゴ リを指定する場合は、Exclude Categories (カテゴリの除外)を 選択します。HIP収集から除外するCategory[カテゴリ](data- loss-preventionなど)を選択します。カテゴリの選択後、特定の Vendor (ベンダー)を Add(追加)したのちに、そのベンダーの特 定の製品を Add(追加)することで、必要に応じて除外内容を詳 細に設定することが可能です。各ダイアログの設定を保存する場合 はOKをクリックします。

GlobalProtect HIP デー タ収集設定	の意味
	(GlobalProtectアプリバージョン6.2.0以降およびコンテンツリ リースバージョン8699-7991が必要) ベンダー全体を除外したく ないが、特定のパッチをベンダーから除外する場合は、ベンダー を追加した後、次の形式を使用してパッチ名またはパッチ番号、 およびオプションでHIPレポートからパッチ更新を除外する日付を 指定できます。除外:[kb-article-id1:MM/DD/YYYY]、[kb- article-id2:MM/DD/YYYY]
	ここで、kb-article-idは属性の名前または番号(例: <kb- article-id>2267602)、MM/DD/ YYYYはHIPレポートからパッチを除外する日付を指定します。日付 を設定しない場合、パッチは無期限にHIPレポートから除外されま す。日付を設定することを選択した場合、パッチは指定された日付 まで除外されます。</kb-
カスタム チェック	アプリで収集するカスタムホスト情報を定義する場合はCustom Checks (カスタムチェック)を選択します。たとえば、HIPオブ ジェクト作成対象のVendor [ベンダー] リストやProduct [製品] リス トに含まれていない必須アプリケーションがある場合、カスタム チェックを作成して、アプリケーションがインストールされている か (対応するWindowsレジストリキーまたはMac plistキーががあ るか)、あるいは実行中か (対応する実行中プロセスがあるかどう か)を判定できます。
	 Windows – 特定のレジストリキーやキー値のチェックをAdd[追加] します。
	● Mac – 特定のplistやキー値のチェックをAdd[追加] します。
	 Process List (プロセスリスト) – エンドポイントで実行中かど うかをチェックする対象のプロセスを Add (追加) します。た とえば、ソフトウェア アプリケーションが実行しているかどう かを判別するには、実行可能ファイルの名前をプロセス リスト に追加します。プロセスはWindows タブおよびMacタブのいず れにも追加できます。

GlobalProtect ポータルの Clientless VPN (クライアントレス VPN) タブ

• ネットワーク > グローバルプロテクト > ポータル > <portal-config> > クライアントレス VPN

GlobalProtect ポータルを設定して、HTML、HTML5、JavaScript テクノロジを使用する一般 的なエンタープライズ Web アプリケーションへの安全なリモート アクセスを提供できるよ うになりました。ユーザーは GlobalProtect ソフトウェアをインストールすることなく、SSL 対応の Web ブラウザから安全なアクセスを利用できます。これは、パートナーや契約業者を アプリケーションにアクセスできるようにしたり、個人デバイスなどの管理対象外のアセッ トを安全に利用できるようにしたりしなければならない状況に便利です。この機能を使用す る場合、GlobalProtect ポータルからクライアントレス VPN をホストするファイアウォール に GlobalProtect サブスクリプションをインストールする必要があります。以下の表に示すよ うに、Clientless VPN (クライアントレス VPN)タブを選択して GlobalProtect Clientless VPN (GlobalProtect クライアントレス VPN) 設定をポータルに設定できます。

GlobalProtect ポータ ルのクライアントレス 設定	の意味
General [全般] タブ	
クライアントレス VPN	Clientless VPN(クライアントレス VPN)を選択し、以下のようにク ライアントレス VPN セッションの一般的な情報を指定します。
ホスト名	Web アプリケーションのランディング ページをホストす る GlobalProtect ポータルの IP アドレスまたは FQDN で す。GlobalProtect クライアントレス VPN は、このホスト名でアプリ ケーション URL を書き直します。
	 ネットワークアドレス変換(NAT)を使用して GlobalProtect ポータルへのアクセスを提供する場合、 入力する IP アドレスまたは FQDN は GlobalProtect ポー タルの NAT IP アドレス(公開 IP アドレス)と一致する ものであるか、NAT IP アドレスに解決できるものであ る必要があります。
セキュリティゾーン	クライアントレス VPN 設定用のゾーンです。このゾーンで定義さ れたセキュリティ ルールが、ユーザーがアクセスできるアプリケー ションの種類を制御します。
DNSプロキシ	アプリケーション名を解決する DNS サーバーです。DNS Proxy(DNS プロキシ) サーバーを選択するか、New DNS Proxy(新しい DNS プロキシ)を設定します(Network(ネットワー ク) > DNS Proxy(DNS プロキシ))。
ログイン ライフタイ ム	クライアントレス SSL VPN セッションの有効期間 を、Minutes(分)(範囲は 60 ~ 1,440)、または Hours(時 間)(範囲は 1 ~ 24、デフォルトは 3)の数値で指定します。指定 した時間が経過すると、ユーザーは再認証して、新しいクライアント レス VPN セッションを開始しなければなりません。
非アクティビティ タ イムアウト	クライアントレス SSL VPN セッションのアイドル状態を許可する期間を、Minutes(分)(範囲は 5 ~ 1,440、デフォルトは 30)、または Hours(時間)(範囲は 1 ~ 24)の数値で指定します。指定した時間内にユーザーのアクティビティがない場合、ユーザーは再認証し

GlobalProtect ポータ ルのクライアントレス 設定	の意味
	て、新しいクライアントレス VPN セッションを開始しなければなり ません。
最大ユーザー	同時にポータルにログインさせることができるユーザーの上限です (デフォルトは 10、範囲は 1 以上で上限なし)。ユーザー数の上限 に達した場合、以降のクライアントレス VPN ユーザーはポータルに ログインできません。

Applications $(\mathcal{P}\mathcal{T}\mathcal{V}\mathcal{V}\mathcal{F}\mathcal{V}\mathcal{T})$ $\mathcal{P}\mathcal{T}$

アプリケーションか らユーザーへのマッ ピング	ユーザーを公開されたアプリケーションに照合する Applications to User Mapping (アプリケーションからユーザーへのマッピング)を Add (追加) します。このマッピングを通じて、アプリケーション にアクセスするクライアントレス VPNを使用できるユーザーまた はユーザー グループを管理します。アプリケーションおよびアプ リケーション グループを定義してから、それらをユーザーにマッ ピングしてください (Network (ネットワーク) > GlobalProtect > Clientless Apps (クライアントレス アプリケーション)、お よび Network (ネットワーク) > GlobalProtect > Clientless App Groups (クライアントレス アプリケーション グループ))。
	 Name(名前) – マッピングの名前を入力します(最大 31 文字)。大文字と小文字を区別し、一意の名前を入力する必要があります。文字、数字、スペース、ハイフン、アンダースコアのみが使用できます。
	 Display application URL address bar (アプリケーションの URL ア ドレスバーの表示)-ユーザーがアプリのランディングページに公 開されていないアプリを起動するためのアプリケーション URL ア ドレスバーを表示するには、このオプションを選択します。 有効 にすると、ユーザーはページ上の Application URL (アプリケー ション URL) リンクをクリックしてURLを指定できます。
ユーザー/ユーザー グループ	現在のアプリケーション設定の適用対象に個別のユーザーや ユーザー グループを Add(追加)できます。これらのユーザー は、GlobalProtect クライアントレス VPN を使用して、設定対象のア プリケーションを起動する権限を持ちます。
	 グループを選択する前にグループマッピングを設定する必要があります(Device(デバイス) > User Identification(User-ID) > Group Mapping Settings(グループマッピング設定))。

GlobalProtect ポータ ルのクライアントレス 設定	の意味
	ユーザーやグループだけでなく、これらの設定をユーザーやグループ に適用するタイミングを指定できます。
	 any(すべて) – アプリケーション設定はすべてのユーザーに適用されます(対象ユーザーやユーザー グループを Add(追加)する必要はありません)。
	 select(対象指定) – アプリケーション設定はこのリストに Add(追加)したユーザーおよびユーザーグループにのみ適用さ れます。
アプリケーション [applications]	個別のアプリケーションまたはアプリケーション グループをマッピ ングに Add (追加) できます。設定に追加された Source Users (送 信元ユーザー) は、GlobalProtect クライアントレス VPN を使用し て、追加済みのアプリケーションを起動できます。

Crypto Settings (暗号設定) タブ

プロトコル バージョ ン	必要な TLS/SSL バージョンの下限と上限を選択します。TLS バー ジョンが大きいほど、接続の安全性は高くなります。選択肢に は、SSLv3、TLSv1.0、TLSv1.1、TLSv1.2 が含まれます。
キー交換アルゴリズ ム	キー交換用のサポート対象アルゴリズム タイプを選択します。選 択肢には、RSA、Diffie-Hellman(DHE)、エフェメラル楕円曲線 Diffie-Hellman(ECDHE)が含まれます。
暗号化アルゴリズム	サポート対象の暗号化アルゴリズムを選択します。AES128 以上をお 勧めします。
認証アルゴリズム	サポート対象の認証アルゴリズムを選択します。選択肢は次の通りで す。 MD5, SHA1, SHA256 , または SHA384.SHA256 以上をお勧めし ます。
サーバー証明書の確 認	アプリケーションがサーバー証明書を提示したときに発生する可能性 がある以下の問題について、対応アクションを有効にします。
	 Block sessions with expired certificate(証明書が期限切れのセッションをブロック) – サーバー証明書の期限が切れている場合、アプリケーションへのアクセスをブロックします。
	 Block sessions with untrusted issuers(発行者が信頼されていない セッションをブロック) – サーバー証明書が信頼されていない認 証局から発行されたものである場合、アプリケーションへのアク セスをブロックします。

GlobalProtect ポータ ルのクライアントレス 設定	の意味
	 Block sessions with unknown certificate status (証明書の状態が 不明なセッションをブロック) – OCSP または CRL サービスが unknown (不明)の証明書失効状態を返す場合、アプリケーショ ンへのアクセスをブロックします。
	 Block sessions on certificate status check timeout (証明書の状態 のチェックがタイムアウトしたセッションをブロック) – 証明 書の状態のサービスからの応答を受信する前に、証明書の状態の チェックがタイムアウトした場合、アプリケーションへのアクセ スをブロックします。
Proxy (プロキシ) タブ	м
氏名	GlobalProtect ポータルが公開されたアプリケーションにアクセスす るために使用するプロキシサーバーを識別するための、最大 31 文字 のラベルです。大文字と小文字を区別し、一意の名前を入力する必要 があります。文字、数字、スペース、ハイフン、アンダースコアのみ が使用できます。
ドメイン	プロキシ サーバーがサービスを提供するドメインを追加します。
プロキシの使用	GlobalProtect ポータルがプロキシ サーバーを使用して公開されてい るアプリケーションにアクセスできるようにする場合に選択します。
SERVER ポート	プロキシ サーバーのホスト名(または IP アドレス)とポート番号を 指定します。
感染 パスワード	プロキシ サーバーへのログインに必要なユーザー名とパスワードを 指定します。確認のためにパスワードは再度入力してください。
Advanced Settings (詳約	田設定) タブ

除外ドメイン リスト	(任意) Rewrite Exclude Domain List (再書き込み除外ドメイン リス
のリライト	ト)にドメイン名、ホスト名、またはIP アドレスを Add(追加)し
	ます。クライアントレス VPN はリバース プロキシとして機能し、公
	開されているアプリケーションが返すページを変更します。リモート
	ユーザーがその URL にアクセスすると、要求が GlobalProtect ポータ
	ルを通過します。一方、ポータル経由でアクセスする必要のないペー
	ジがアプリケーションに含まれていることもあります。再書き込み
	ルールから除外し、再書き込みできないようにするドメインを指定し
	てください。

GlobalProtect ポータ ルのクライアントレス 設定	の意味
	ホストおよびドメイン名では、パスはサポートされません。ホストお よびドメイン名のワイルドカード文字(*)は、名前の最初でのみ使 用できます。(*.etrade.com など)。

GlobalProtect ポータルの Satellite (サテライト) タブ

• ネットワーク > グローバルプロテクト > ポータル > <portal-config> > サテライト

サテライトとは、GlobalProtect アプリとして機能して GlobalProtect ゲートウェイへの VPN 接 続を確立できるようにする、Palo Alto Networks[®] ファイアウォール(通常は支社に設置)で す。GlobalProtect アプリと同様に、サテライトは、初期設定をポータルから受信します。これ には、サテライトがすべての設定済みゲートウェイに接続して VPN 接続を確立できるようにす るための証明書と VPN 設定ルーティング情報が含まれます。

支社ファイアウォールにGlobalProtectサテライト設定を定義する前に、WAN接続とのインターフェイスを設定し、セキュリティゾーンとポリシーをセットアップして支社LANがインターネットと通信できるようにします。その後、以下の表に示すように、Satellite (サテライト)タブを選択してGlobalProtect サテライト設定をポータルに設定できます。

GlobalProtect ポータル のサテライト設定	の意味
一般	 Name[名前] – GlobalProtectポータルのサテライト設定につける 名前を指定します。
	 Configuration Refresh Interval (hours)[設定の更新間隔(時間)] サテライトデバイスが設定の更新があるかどうかポータル を確認する間隔を指定します(範囲は1~48時間、デフォルト は24時間)。
機器	ファイアウォール Serial Number(シリアル番号)を使用してサテ ライトを Add(追加)します。ポータルは、接続を要求している ユーザーを識別するために、シリアル番号またはログイン資格情報 を受け入れることができます。
	初めてポータルに対してサテライトを認証するには、サテライト管 理者はユーザー名とパスワードを提供する必要があります。サテ ライトが正常に認証されると、サテライトのホスト名 が自動的に ポータルに追加されます。
ユーザー/ユーザー グ ループの登録	ポータルはシリアル番号を使用して、あるいは使用せず にEnrollment User/User Group[登録ユーザー/登録ユーザーグルー プ] 設定を使用してサテライトと設定を照合します。

GlobalProtect ポータル のサテライト設定	の意味
	この設定で制御するユーザーまたはグループを Add(追加)しま す。
	 設定を特定のグループに制限する場合は、ファ イアウォールのグループマッピングを有効に する必要があります(Device(デバイス) > User Identification(User-ID) > Group Mapping Settings(グループマッピング設定))。
ゲートウェイ	Add[追加] をクリックして、この設定のサテライトがIPSecトンネ ルを確立できるゲートウェイのIPアドレスまたはホスト名を入力 します。ゲートウェイを設定するインターフェイスの FQDN また は IP アドレスを Gateways[ゲートウェイ] フィールドに入力しま す。IP アドレスは、IPv6、IPv4、またはそれら両方の形で指定でき ます。デュアル スタック環境で IPv6 接続を指定して優先する場合 は、IPv6 Preferred (IPv6 優先)を選択します。
	(任意)設定に複数のゲートウェイを追加している場合、Routing Priority (ルーターの優先順位)を使用すると、優先されるゲート ウェイをサテライトが選択できます(範囲は 1 ~ 25)。数値が 低いほど優先順位が高くなります(使用可能なゲートウェイの場 合)。サテライトは、ルーティングメトリックを算出するために ルーティングの優先順位を10倍します。
	 ゲートウェイによって公開されたルートはスタティックルートとしてサテライトにインストールされます。スタティックルートのメトリックは、ルーティングの優先順位の10倍です。複数のゲートウェイがある場合、必ずルーティングの優先順位も設定して、バックアップゲートウェイによって通知される同じルートよりも高いメトリックになるようにしてください。たとえば、プライマリゲートウェイとバックアップゲートウェイのルーターの優先順位をそれぞれ1と10に設定した場合、サテライトは10をプライマリゲートウェイのメトリックとして使用し、100をバックアップゲートウェイのメトリックとして使用します。
	Publish all static and connected routes to Gateway(静的なすべ ての接続済みルートをゲートウェイに公開)(Network(ネット ワーク) > IPSec tunnels(IPSecトンネル) > <tunnel(トンネ ル) > Advanced(詳細) –GlobalProtect Satellite on the <tunnel > General(一般))を選択した場合のみ使用可能)を設定した場</tunnel </tunnel(トンネ

GlobalProtect ポータル のサテライト設定	の意味	
	合、サテライトはさらにネットワーク情報とルーティング情報を ゲートウェイと共有します。	
信頼されたルート CA	Add[追加] をクリックしてからゲートウェイサーバー証明書を発行 するために使用するCA証明書を選択します。サテライトの信頼で きるルート CA 証明書は、ポータルのエージェント設定と同時にエ ンドポイントにプッシュされます。	
	 ・ ・ ・	
	 ゲートウェイサーバー証明書の発行の際に使用するルートCA証明書がポータル上に存在しない場合、Import[インポート]またはGenerate[生成]が可能です。 	
クライアント証明書		
ローカル	 Issuing Certificate(証明書の発行) – ポータルが使用する証 明書を発行するルート CA を選択します。認証が完了するとサ テライトに対し証明書が発行されます。必要な証明書がファイ アウォールにまだない場合は、Import(インポート)または Generate(生成)することができます。 	
	 証明書がファイアウォールに存在しない場合は、発行 証明書を Import (インポート)または Generate (生 成)することができます。 	
	 OCSP Responder (OCSPレスポンダ) – ポータルおよびゲート ウェイが提示した証明書の失効状態を検証するためにサテライ トが使用する OCSP レスポンダを選択します。ここで None (な 	

GlobalProtect ポータル のサテライト設定	の意味
	し)を選択すると、証明書の失効状態の検証に OCSP は使用さ れません。
	 証明書が取り消された場合に通知を受け取り、適切な作業を行ってポータルおよびゲートウェイへの接続を保護できるよう、サテライト OCSP レスポンダを有効化します。サテライト OCSP レスポンダを有効化するには、Certificate Revocation Checking (証明書の失効チェック)設定でCRLおよびOCSPも有効化する必要があります(Device (デバイス) > Setup (セットアップ) > Session (セッション) > Decryption Settings (復号化設定))。
	 Validity Period(有効期間)(日数) – GlobalProtect サテライト証明書の有効期間を指定します(範囲は 7 ~ 365、デフォルトは 7)。
	 Certificate Renewal Period (証明書更新期間) (日数) – 証明 書有効期間満了の何日前に自動更新を行うかを指定します(範 囲は3~30、デフォルトは3)。
SCEP	 SCEP – クライアント証明書を生成するための SCEP プロファイ ルを選択します。プロファイルがドロップダウンリストにない 場合、New[新規] のプロファイルを作成することができます。 Certificate Renewal Period(証明書更新期間)(日数) – 証明 書有効期間満了の何日前に自動更新を行うかを指定します(範 囲は 3 ~ 30、デフォルトは 3)。

Network > GlobalProtect > Gateways [ネットワーク > GlobalProtect > ゲートウェイ]

GlobalProtect ゲートウェイを設定するには、Network(ネットワーク) > GlobalProtect > Gateways (ゲートウェイ)を選択します。ゲートウェイは GlobalProtect アプリ、または GlobalProtect サテライトに VPN 接続を提供します。

GlobalProtect ゲートウェイのダイアログから新規のゲートウェイ設定をAdd (追加)するか、既存のゲートウェイ設定を編集する場合はそれを選択します。

確認すべき情報	以下を参照
GlobalProtectゲートウェイ用に設 定可能な一般設定	GlobalProtect ゲートウェイの General(全般)タブ
ゲートウェイクライアント認証の設 定方法	GlobalProtect ゲートウェイの Authentication(認証) タブ
アプリがゲートウェイと VPN トン ネルを確立できるようにトンネルと ネットワークを設定する方法	GlobalProtect ゲートウェイの Agent(エージェント) タブ
サテライトがサテライトとして機能 するゲートウェイとVPN接続が確立 できるようにトンネルとネットワー クを設定する方法	GlobalProtect ゲートウェイの Satellite (サテライト) タ ブ
その他の情報をお探しですか?	ポータルのセットアップ手順の詳細は、 『GlobalProtect Administrator's Guide (GlobalProtect 管理者ガイド)』の「Configure GlobalProtect Gateways(GlobalProtect ゲートウェイの設定)」を 参照してください。

GlobalProtect ゲートウェイの General (全般) タブ

• ネットワーク > グローバルプロテクト > ゲートウェイ > <gateway-config> > 一般

アプリが接続するゲートウェイインターフェイスを定義し、ゲートウェイがエンドポイントを認証する方法を指定する場合は、General (全般)タブを選択します。

GlobalProtect ゲート ウェイの一般設定	の意味
氏名	ゲートウェイの名前を入力します (最大 31 文字)。名前の大文字と 小文字は区別されます。また、一意の名前にする必要があります。 文字、数字、スペース、ハイフン、およびアンダースコアのみを使 用してください。
場所	マルチ仮想システムモードになっているファイアウォールの場 合、Location[場所] はGlobalProtectゲートウェイを使用できる仮 想システム (vsys) になります。マルチ仮想システムモードに なっていないファイアウォールの場合、Location[場所] フィールド はGlobalProtect Gateway [GlobalProtectゲートウェイ] ダイアログ に表示されません。 ① ゲートウェイの設定を保存すると、その Location[場 所] は変更できなくなります。
ネットワーク設定エリア	
Interface	リモートエンドポイント用の入力インターフェイスとして使用する ファイアウォールインターフェイスの名前を選択します。(既存の インターフェイスを選択する必要があります)
	Telnet、SSH、HTTP、または HTTPS を許可するイン ターフェイス管理プロファイルを、GlobalProtect ポー タルまたはゲートウェイを設定したインターフェイス に接続しないでください。これにより、管理インター フェイスがインターネットに公開されるためです。管 理ネットワークへのアクセスを保護する方法の詳細に ついては、Adminstrative Access Best Practices を参 照してください。
IP アドレス	(任意)ゲートウェイアクセス用のIPアドレスを指定します。IP Address Type(IP アドレスタイプ)を選択して、IP Address(IP アドレス)を入力します。
	 IP アドレス タイプは、IPv4(IPv4 トラフィックのみ)、IPv6(IPv6 トラフィックのみ)、または IPv4 and IPv6(IPv4 および IPv6)です。ネットワークがデュアル スタック構成をサポートしているときは、IPv4 and IPv6(IPv4 および IPv6)を使用します。これにより IPv4 と IPv6 が同時に動作します。

IP アドレスは IP アドレス タイプに対応するものでなければな りません。たとえば、IPv4 の場合は 172.16.1.0、IPv6 の場合は 21DA:D3:0:2F3b のように指定します。IPv4 and IPv6(IPv4 および
GlobalProtect ゲート ウェイの一般設定	の意味
	IPv6)を選択した場合、それぞれのタイプに適切なアドレスを入力 します。
ログ設定	
正常完了した SSL ハン ドシェイクのログへの 記録	 (オプション)正常に完了した SSL復号化ハンドシェイクの詳細ロ グを作成します。デフォルトで無効になっています。 ログはストレージ容量を消費します。ログを保 存するリソースがあることを確認してから正常 に完了した SSL ハンドシェイクをログに記録しま す。Device(デバイス) > Setup(セットアップ) > Management(管理) > Logging and Reporting Settings(ログとレポートの設定)を編集して、現在 のログメモリの割り当てを確認し、ログタイプ間の ログメモリに再割り当てを行います。
失敗した SSL ハンド シェイクのログへの記 録	 失敗した SSL 復号化ハンドシェイクの詳細なログを作成すると、復号化の問題の原因を特定可能となります。デフォルトで有効になっています。 ログはストレージ容量を消費します。より多くの(またはより少ない)ログストレージ容量を復号化ログに割り当てるには、ログメモリの割り当てを編集します(Device(デバイス) > Setup(セットアップ) > Management(管理) > Logging and Reporting Settings(ログとレポートの設定))。
ログの転送	GlobalProtect SSL ハンドシェイク(復号化)ログを転送する方法お よび場所を指定します。

GlobalProtect ゲートウェイの Authentication (認証) タブ

• ネットワーク > グローバルプロテクト > ゲートウェイ > <gateway-config> > 認証

SSL/TLSサービスプロファイルを指定し、クライアント認証の詳細を設定する場合 は、Authentication (認証)を選択します。複数の認証設定を追加することができます。

GlobalProtectゲートウェイの認証設定	起
SSL/TLS Service Profile	このGlobalProtectゲートウェイを保護するためのSSL/ TLSサービスプロファイルを選択します。サービス プロ ファイルのコンテンツの詳細については、「Device(デ

GlobalProtectゲートウェイの認証設定	
	バイス) > Certificate Management(証明書の管理) > SSL/TLS Service Profile(SSL/TLS サービス プロファイル)」を参照してください。
クライアント認証エリア	
氏名	この設定を識別するための一意の名前を入力します。
OS	デフォルトの状態では、この設定がすべてのエンドポ イントに適用されます。エンドポイントのリストを OS (Android、Chrome、iOS、IoT、Linux、Mac、Windows、 または WindowsUWP)、Satellite (サテライト) デバイ ス、またはサードパーティの IPSec VPN クライアント (X- Auth)でさらに詳細に設定することができます。
	数ある設定内容は第一にOSにより区別されます。1つ のOSに対し複数の設定が必要な場合、認証プロファイ ルごとに個別の設定を行っていくことが可能です。
	設定は、最も詳細なものをリストの一番 上に、最も大まかなものを一番下に配置 することをお勧めします。
認証プロファイル	ゲートウェイへのアクセスを認証する認証プロファイル またはシーケンスをドロップダウンリストから選択しま す。「Device(デバイス)> Authentication Profile(認 証プロファイル)」を参照してください。
	 クライアント認証の場合、必ず認証プロ ファイルが2要素認証でRADIUSあるいは SAMLを使用するようにします。RADIUS や SAMLを使用しない場合は、認証プロ ファイルに加えて証明書プロファイルを 設定する必要があります。
Username Label ユーザー名のラベ ル	GlobalProtect ゲートウェイ ログイン用のカスタム ユー ザー名ラベルを指定します。たとえば、ユーザー名(の み)、またはメールアドレス(username@domain)。
パスワード ラベル	GlobalProtect ゲートウェイ ログイン用のカスタム パ スワード ラベルを指定します。たとえば、パスワード (トルコ語)またはパスコード(2 重認証、トークン ベース認証)

GlobalProtectゲートウェイの認証設;	老
認証メッセージ	このゲートウェイにログインする場合に使用すべき認証 情報をエンドユーザに知らせるためのメッセージを入力 するか、デフォルトのメッセージのままにしておくこと が可能です。メッセージは最大で256文字までです。
ユーザー認証情報あるいはクライ アント証明書による認証を許可	No (いいえ)を選択すると、ユーザーがユーザー認証情報およびクライアント証明書の両方を使ってゲートウェイに認証する必要があります。Yes (はい)を選択すると、ユーザーがユーザー認証情報あるいはクライアント証明書のいずれかを使ってゲートウェイに認証できるようになります。

証明書プロファイル

証明書プロファイル	(任意) ユーザーのエンドポイントから受信するこれ らのクライアント証明書を照合する際にゲートウェイ が使用する証明書プロファイルを選択します。証明書プ ロファイルを使用すると、クライアントの証明書がこの プロファイルと一致する場合にのみゲートウェイがユー ザーを認証します。
	Allow Authentication with User Credentials OR Client Certificate (ユーザー認証情報あるいはクライアント証 明書による認証を許可)オプションをNo (いいえ)に設定 する場合はCertificate Profile (証明書プロファイル)を選 択する必要があります。Allow Authentication with User Credentials OR Client Certificate (ユーザー認証情報ある いはクライアント証明書による認証を許可)オプション をYes (はい)に設定する場合、Certificate Profile (証明書 プロファイル)は任意項目です。 証明書プロファイルはOSの種類に依存しません。
Block login for quarantined devices(隔離済デバイスからのロ グインをブロックする)	Quarantine List (隔離リスト)に含まれる GlobalProtect クライアント デバイスのゲートウェイへのログインを ブロックするかどうかを指定します (Device (デバイ ス) > Device Quarantine (デバイスの隔離))。

GlobalProtect ゲートウェイの Agent (エージェント) タブ

• ネットワーク > グローバルプロテクト > ポータル > <portal-config> > エージェント

アプリがゲートウェイと VPN トンネルを確立できるようにするトンネル設定を定義する場合は、Agent (エージェント)タブを選択します。さらに、このタブでは VPN のタイムアウト、DNS および WINS のネットワークサービスを指定したり、セキュリティ ポリシー ルール

の HIP プロファイルに合致した場合、あるいは合致しなかった場合にエンドユーザーに表示する HIP 通知メッセージを設定できます。

以下のタブでエージェントの設定を行います。

- Tunnel Settings [トンネル設定]タブ
- Client Settings(クライアント設定)タブ
- Client IP Pool (クライアント IP プール) タブ
- Network Services (ネットワーク サービス) タブ
- Connection Settings (接続設定) タブ
- Video Traffic(動画トラフィック)タブ
- HIP Notification (HIP 通知) タブ

Tunnel Settings [トンネル設定]タブ

ネットワーク > グローバルプロテクト > ゲートウェイ > <gateway-config> > エージェント > <agent-config> > トンネル設定

Tunnel Settings (トンネル設定)タブを選択してトンネリングを有効化し、トンネルのパラメーターを設定します。

外部ゲートウェイを設定する場合は、トンネルパラメータが必要になります。内部ゲートウェイ を設定する場合、トンネルパラメータの設定は必須ではありません。

GlobalProtect ゲート ウェイ クライアントの トンネル モード設定	の意味
トンネル モード	トンネルモードを有効にする場合は、 Tunnel Mode [トンネルモー ド] を選択して、以下の設定を指定します。
	 Tunnel Interface[トンネルインターフェイス] – ゲートウェイへのアクセス用のトンネルインターフェイスを選択します。
	 Max User(最大ユーザー数) – 認証、HIP更新、および GlobalProtect アプリ更新のために同時にゲートウェイにアクセ スできるユーザーの最大数を指定します。ユーザーが最大数を 超えた場合、ユーザーの最大数に達したことを示すエラーメッ セージが表示され、後続のユーザーはアクセスを拒否されます (範囲はプラットフォームによって異なり、フィールドが空の 場合に表示されます)。
	 Enable IPSec(IPSecを有効化) – エンドポイントトラフィック でIPSecモードを使用可能にし、IPSecをプライマリにして、SSL- VPNをフォールバック方式にするには、このオプションを選択 します。以下のオプションはIPSecが有効化されるまで使用でき ません。

GlobalProtect ゲート ウェイ クライアントの トンネル モード設定	の意味
	 GlobalProtect IPSec Crypto[GlobalProtect の IPSec 暗号] – VPN トンネルの認証および暗号化アルゴリズムを指定す る GlobalProtect の IPSec 暗号化プロファイルを選択しま す。default[デフォルト] プロファイルでは、AES-128-CBC暗 号化とSHA1認証が使用されます。詳細は、「Network(ネッ トワーク)> Network Profiles(ネットワーク プロファイル)> GlobalProtect IPSec Crypto(GlobalProtect の IPSec 暗号)」を 参照してください。
	 Enable X-Auth Support[X-Auth サポートの有効化] – IPSec が 有効化されている場合にGlobalProtectゲートウェイのExtended Authentication (X-Auth) サポートを有効にするには、このオ プションを選択します。X-Auth サポートにより、X-Auth をサ ポートするサード パーティ IPSec VPN クライアント (Apple iOS および Android デバイスの IPSec VPN クライアント、Linux の VPNC クライアントなど) は、GlobalProtect ゲートウェイとの VPN トンネルを確立できます。X-Auth オプションにより、VPN クライアントから特定の GlobalProtect ゲートウェイへのリモー ト アクセスが可能になります。X-Auth アクセスで利用できる GlobalProtect 機能は限定されるため、GlobalProtect アプリケー ションを使用することで、GlobalProtect が iOS および Android デバイスに提供するセキュリティ機能セットすべてへのアクセ スを簡略化することを検討してください。
	X-Auth Support[X-Authサポート] を選択すると Group Name [グ ループ名] および Group Password [グループパスワード] のオプ ションが有効化されます。
	 グループ名とグループのパスワードが指定されている場合、 最初の認証フェーズでは、双方がこの資格証明を使用して認 証する必要があります。第2認証フェーズでは有効なユーザー 名とパスワードが必要です。認証セクションで設定された認 証プロファイルを通じて検証されます。 グループ名とグループパスワードが定義されていたい場合
	最初の認証フェーズは、サードパーティ VPN クライアントに よって提示された有効な証明書に基づきます。その後この証 明書は、認証セクションで設定された証明書プロファイルを 通じて検証されます。
	 デフォルトでは、IPSecトンネルの確立に使用されたキーの 有効期限が切れたときに、ユーザーに再認証は要求されません。ユーザーに再認証を要求する場合は、Skip Auth on IKE Rekey[IKEキー再生成での認証をスキップ]の選択を解除しま す。

Client Settings(クライアント設定)タブ

ネットワーク > グローバルプロテクト > ゲートウェイ > <gateway-config> > エージェント > <agent-config> > クライアント設定

GlobalProtect アプリによりゲートウェイとのトンネルを確立する際のエンドポイントの仮想 ネットワーク アダプタを設定する場合は、Client Settings (クライアント設定)タブを開きます。



一部の Client Settings(クライアント設定)オプションは、トンネル モードを有効 にして、Tunnel Settings(トンネル設定)タブでトンネル インターフェイスを定義 した後にのみ使用可能になります。

GlobalProtect ゲートウェイ クライ アント設定およびネットワーク設定	の意味
Config Selection Criteria (設定選択条	件) タブ
氏名	クライアント設定の識別に使用する名前(最大31文 字)を入力します。名前の大文字と小文字は区別されま す。また、一意の名前にする必要があります。文字、数 字、スペース、ハイフン、およびアンダースコアのみを 使用してください。
Source User (送信元ユーザー)	この設定を適用する特定のユーザーまたはユーザーグ ループを Add (追加) します。
	 ユーザーやユーザー グループを選択する 前にグループマッピングを設定する必要 があります(Device(デバイス) > User Identification(User-ID) > Group Mapping Settings(グループマッピング設定))。
	この設定をすべてのユーザーにデプロイするに は、Source User (送信元ユーザー)のドロップダウンリ ストでany (すべて)を選択します。この設定をプレロ グオンモードの GlobalProtect アプリケーションを使用 しているユーザーにのみデプロイする場合は、Source User (送信元ユーザー)のドロップダウンリストでpre- logon (プレログオン)を選択します。
	1 ユーザーがSource User (送信元ユー ザー)、OS、およびSource Address (送信元 アドレス)の一致基準にすべてマッチする 場合のみ、クライアント設定がデプロイ されます。

GlobalProtect ゲートウェイ クライ アント設定およびネットワーク設定	の意味
OS	エンドポイントのオペレーティングシステムに基づい てこの構成を展開するには、次の OS をAdd (追加) しま す。Android、Chrome、iOS、IoT、Linux、Mac、 Windows、WindowsUWP。また、この値をAny (すべ て) に設定することで、エンドポイントのオペレーティ ングシステムに関係なく、ユーザーやユーザーグループ ごとに設定を適用させることができます。
送信元アドレス	ユーザーの場所に基づいてこの設定をデプロイする場合 は、送信元のRegion (地域)あるいはローカル IP Address (IP アドレス) (IPv4 および IPv6) をAdd (追加)します。 この設定をすべてのユーザーの場所にデプロイする場 合、Region (地域)やIP Address (IP アドレス)を指定しな いでください。また、この機能は GlobalProtect アプリ ケーションの古いリリースではサポートされていないた め、ユーザーが GlobalProtect アプリケーション 4.0 以 前のリリースを実行している場合はこれらのフィールド を空にする必要があります。
	 接続中のユーザーの場所がRegion (地域)あるいはIP Address (IP アドレス)に一致する場合に、Source Address (送信元アドレス)のマッチが成功します。
	ユーザーがSource User (送信元ユー ザー)、OS、およびSource Address (送信元 アドレス)の一致基準にすべてマッチする 場合のみ、クライアント設定がデプロイ されます。

Authentication Override (認証オーバーライド) タブ

認証のオーバーライド	ユーザーが認証プロファイルまたは証明書プロファイル で指定された認証スキームで認証を行ったのちに、ゲー トウェイがユーザーの認証を行う際に、保護された、デ バイス固有の暗号化されたCookieを使用できるようにし ます。
	a 9 o

GlobalProtect ゲートウェイ クライ アント設定およびネットワーク設定	の意味
	 Generate cookie for authentication override[認証 オーバーライド用Cookieを生成] – Cookieが有効であ る間、ユーザーがゲートウェイとの認証を行うたび にエージェントはこのCookieを提示します。
	• Cookie Lifetime[Cookieの有効期間] – Cookieが有 効な時間数、日数、あるいは週数を指定します。 一般的な有効期間は24時間です。範囲は1~72時 間、1~52週間、あるいは1~365日です。Cookieが 失効した場合、ユーザーはログイン認証情報を再度 入力する必要があり、この入力をうけ、ゲートウェ イは新しいCookieを暗号化してユーザーデバイスに 送信します。
	 Accept cookie for authentication override[Cookieに よる認証オーバーライドを許可] – ゲートウェイが暗 号化されたCookieによる認証を許可するよう設定す る場合はこのオプションを選択します。エージェン トがCookieを提示すると、ゲートウェイはユーザー を認証する前に、そのCookieが同じゲートウェイ自 身が暗号化したものであるかどうかを検証します。
	 Certificate to Encrypt/Decrypt Cookie[Cookie暗号 化/復号化時の証明書] – Cookieの暗号化と復号化を 行う際にゲートウェイが使用する証明書を選択しま す。
	● Cookieの暗号化および復号化用に、ポータ ルとゲートウェイが共に同じ証明書を使 用するよう設定されていることを確認し てください。
IP Pools(IP プール)タブ	

IP Pools (IP ブール)	タブ
-------------------	----

認証サーバーからの Framed-IP- Address 属性の取得	GlobalProtectゲートウェイを有効にし、外部認証サー バーを使用して固定IPアドレスを割り当てる場合は、こ のオプションを選択します。このオプションを有効化し た場合、GlobalProtectゲートウェイは、認証サーバー のFramed-IP属性を使用してデバイス接続用のIPアドレ スを割り当てます。
認証サーバー IP プール	リモートユーザーに割り当てるIPアドレスのサブ ネットまたは範囲をAdd[追加]します。トンネル が確立されると、GlobalProtectゲートウェイは、 認証サーバーのFramed-IP-Adress属性を使用して この範囲のIPアドレスを接続デバイスに割り当て

GlobalProtect ゲートウェイ クライ アント設定およびネットワーク設定	の意味
	ます。IPv4 アドレス(192.168.74.0/24 および 192.168.75.1-192.168.75.100 など)または IPv6 アド レス(2001:aa::1-2001:aa::10 など)を追加できます。
	Retrieve Framed-IP-Address attribute from authentication server[認証サーバーからのFramed- IP-Adress属性の取得] を有効化している場合にの みAuthentication Server IP Pool[認証サーバーIPプール] の設定と有効化が行えるようになります。
	記証サーバーの IP プールには、すべての 同時接続ユーザーをサポートするのに十 分な IP アドレスが含まれている必要が あります。IP アドレスは固定的に割り当 てられ、ユーザーの接続が切断された後 も保持されます。異なるサブネットの複 数の範囲を設定し、システムがクライア ントの他のインターフェイスと競合しな いIP アドレスを割り当てられるようにして ください。
	ネットワーク内のサーバーおよびルーターは、こ のIPプールからファイアウォールにトラフィックを ルーティングする必要があります。たとえば、ネッ トワーク192.168.0.0/16では、リモートユーザー は192.168.0.10といったアドレスの割り当てを受けるこ とができます。
IP プール	リモートユーザーに割り当てるIPアドレスの範囲 をAdd[追加] します。トンネルが確立されると、 この範囲のアドレスを使用してリモート ユーザー のエンドポイントにインターフェイスが作成され ます。IPv4 アドレス(192.168.74.0/24 および 192.168.75.1-192.168.75.100 など)または IPv6 アド レス(2001:aa::1-2001:aa::10 など)を追加できます。

GlobalProtect ゲートウェイ クライ アント設定およびネットワーク設定	の意味
	競合を回避するには、IPプールには、す べての同時接続ユーザーをサポートする のに十分な IP アドレスが含まれている必 要があります。ゲートウェイでは、クラ イアントと IP アドレスのインデックスが 保持されるため、次回接続時に自動的に 同じ IP アドレスがクライアントに割り当 てられます。異なるサブネットの複数の 範囲を設定し、システムがクライアント の他のインターフェイスと競合しないIPア ドレスを割り当てられるようにしてくだ さい。
	ネットワーク内のサーバーおよびルーターは、こ のIPプールからファイアウォールにトラフィックを ルーティングする必要があります。たとえば、ネッ トワーク 192.168.0.0/16 では、リモート ユーザーに 192.168.0.10 といったアドレスを割り当てることがで きます。

Split Tunnel(トンネルの分割)タブ

Access Route(アクセスルート)タブ

ローカルネットワークへの直接ア クセスなし	このオプションは、ユーザーがGlobalProtectに接続して いるときに、Windows、macOS、Linuxエンドポイント (LinuxエンドポイントはGlobalProtectアプリバージョ ン6.0.0以降を実行している必要があります)でローカ ルネットワークアクセスを有効または無効にする場合に 使用します。このオプションを有効にすると、ユーザー はGlobalProtectに接続している間、プロキシやプリンタ などのローカルリソースに直接トラフィックを送信でき ません。アクセスルート、宛先ドメイン、およびアプ リケーションに基づくスプリットトンネルトラフィッ クは、引き続き正常に動作します。
	このオプションは、Windows、macOS、およびLinuxエ ンドポイントでサポートされています(Linuxエンドポ イントはGlobalProtectアプリバージョン6.0.0以降を実 行している必要があります)。

GlobalProtect ゲートウェイ クライ アント設定およびネットワーク設定	の意味
	 不正なWi-Fiアクセスポイントなどの信頼できないネットワークでのリスクを軽減するため、 [No direct access to local network (ローカルネットワークに直接アクセスしない)]設定を有効にします。
包含	VPN トンネルに含めるルートを Add(追加)します。 ゲートウェイがこれらのルートをリモート ユーザーの エンドポイントにプッシュして、VPN 接続経由で送信 できるユーザー エンドポイントを指定します。
	IPv6 または IPv4 サブネットを含めることができま す。On PAN-OS 8.0.2以降のリリースでは、最大100の アクセスルートを使用して、スプリットトンネル ゲートウェイ設定にトラフィックを含めることがで きます。GlobalProtectアプリケーションのバージョ ン4.1.x以降と組み合わせない限り、最大1,000件のアク セスルートを使用できます。
	 すべてのサブネットあるいはアドレスオ ブジェクトを含めるには、0.0.0.0/0 およ び ::/0 をアクセス ルートとして Include (含 有)します。
除外	VPN トンネルから除外するルートを Add (追加) しま す。これらのルートは、仮想アダプタ(トンネル)では なく、エンドポイントの物理アダプタ経由で送信されま す。
	VPN トンネル経由で送信するルートは、トンネルに含 めるルート、トンネルから除外するルート、またはその 両方の組み合わせの形で定義できます。たとえば、スプ リット トンネルを設定し、リモート ユーザーが VPN ト ンネルを経由せずにインターネットに直接アクセスでき るようにすることができます。除外するルートは、想定 外のトラフィックが除外されることのないように、包含 するルートよりも細かく指定してください。
	IPv6 または IPv4 サブネットを除外できます。ファイ アウォールは、スプリット トンネル ゲートウェイ設 定で最大100の除外アクセスルートをサポートしま す。GlobalProtect アプリケーション 4.1 以降のリリー スと組み合わせない限り、最大 200 の除外アクセス ルートを使用できます。Chromebook で Android を実行 しているエンドポイントのアクセスルートを除外するこ

GlobalProtect ゲートウェイ クライ アント設定およびネットワーク設定	の意味
	とはできません。Chromebook では IPv4 ルートのみが サポートされています。
	スプリットトンネリングを有効にしない場合、すべて の要求はトンネルを介してルーティングされます(スプ リットトンネリングなし)。この場合、インターネット の要求はすべてファイアウォールを通過して、ネット ワークに出ていきます。この方法により、部外者がユー ザーのエンドポイントにアクセスし、そのエンドポイン トをブリッジとして利用して社内ネットワークに侵入す るのを防ぐことができます。

Domain and Application tab (ドメインとアプリケーション) タブ

Include Domain(ドメインのイン クルード)	宛先ドメインとポート(オプション) に基づいて VPN ト ンネルに含む Software as a Service (SaaS) またはパブ リック クラウド アプリケーションを追加します。ゲー トウェイがこれらのアプリケーションをリモート ユー ザーのエンドポイントにプッシュして、VPN 接続経 由で送信できるユーザー エンドポイントを指定しま す。ICMP は含まれていません。エントリを最大 200 個 まで追加することができます。
	たとえば、 *.office365.com ドメインを追加して、 すべての Office 365 トラフィックが VPN トンネルを通 過できるようにします。
	各ドメインにポート一覧を設定できます。ポートが設定されていない場合、指定されたドメインのすべてのポートがこのポリシーの対象となります。
Exclude Domain(ドメインを除外 する)	宛先ドメインとポート(オプション)に基づいて VPN ト ンネルに含まない Software as a Service (SaaS) またはパ ブリック クラウド アプリケーションを追加します。こ れらのアプリケーションは、仮想アダプタ(トンネル) ではなく、エンドポイントの物理アダプタで送信されま す。エントリを最大 200 個まで追加することができま す。
	たとえば、 *.ringcentral.com ドメインを追加し て、VPN トンネルからすべての RingCentral トラフィッ クを除外します。

GlobalProtect ゲートウェイ クライ アント設定およびネットワーク設定	の意味
	各ドメインにポート一覧を設定できま す。ポートが設定されていない場合、指 定されたドメインのすべてのポートがこ のポリシーの対象となります。
	スプリットトンネリングを有効にしない場合、すべて の要求はトンネルを介してルーティングされます(スプ リットトンネリングなし)。この場合、インターネット の要求はすべてファイアウォールを通過して、ネット ワークに出ていきます。この方法により、外部エンドが エンドポイントにアクセスして内部ネットワークにアク セスできなくなる可能性があります。
Include Client Application Process Name(クライアント アプリケー ションのプロセス名をインクルー ド)	VPN トンネルにトラフィックを含める各アプリケー ション プロセスの完全なパスを追加 します。ゲート ウェイがこれらのアプリケーションをリモート ユー ザーのエンドポイントにプッシュして、VPN 接続経由 で送信できるユーザー エンドポイントを指定します。 エントリを最大 200 個まで追加することができます。
	たとえば、/Application/Safari.app/Contents/ MacOS/Safariを追加すると、すべての Safari ベース のトラフィックが macOS エンドポイント上の VPN ト ンネルを通過できるようになります。
Exclude Client Application Process Name(クライアント アプリケー ションのプロセス名を除外する)	VPN トンネルからトラフィックを除外する各アプリ ケーション プロセスの完全なパスを追加 します。これ らのアプリケーションは、仮想アダプタ(トンネル) ではなく、エンドポイントの物理アダプタで送信されま す。エントリを最大 200 個まで追加することができま す。
	たとえば、RingCentral アプリケーションからトラ フィックを除外するには、次のようにします。
	 Windows エンドポイントの場合、%AppData %\Local\RingCentral\SoftPhoneApp \Softphone.exe および %AppData% \Local\RingCentral\SoftPhoneApp \SoftphoneMapiBridge.exeを追加します。
	 macOS エンドポイントの場合、/Applications/ RignCentral for Mac.app/Contents/MacOS/ Softphone を追加します。
	スプリットトンネリングを有効にしない場合、すべて の要求はトンネルを介してルーティングされます(スプ

GlobalProtect ゲートウェイ クライ アント設定およびネットワーク設定	の意味
	リットトンネリングなし)。この場合、インターネット の要求はすべてファイアウォールを通過して、ネット ワークに出ていきます。この方法により、外部エンドが エンドポイントにアクセスして内部ネットワークにアク セスできなくなる可能性があります。
[Network Services] タブ	
DNS サーバー	このクライアント設定を持つ GlobalProtect アプリケー ションが DNS クエリを送る先となる DNS サーバーの IP アドレスを指定します。各 IP アドレスをコンマで区 切れば複数の DNS サーバーを追加できます。
DNS サフィックス	解決できない非修飾ホスト名が入力されたときにエンド ポイントがローカルで使用する DNS サフィックスを指 定します。カンマで区切って複数の DNS サフィックス (最大 100 個)を入力できます。

Client IP Pool (クライアント IP プール) タブ

ネットワーク > グローバルプロテクト > ゲートウェイ > <gateway-config> > エージェント > <agent-config> > クライアント IP プール

IPv4 または IPv6 アドレスを GlobalProtect[™] ゲートウェイに接続するすべてのエンドポイント に割り当てるために使用されるグローバル IP プールを設定するには、Client IP Pool (クライアン ト IP プール)タブを選択します。

GlobalProtect ゲートウェイ クライアントの IP プール構成設定	の意味
IP プール	リモートユーザーに割り当てる IPv4 または IPv6 アドレスの範囲をAdd(追加)します。 トンネルが確立されると、GlobalProtect ゲー トウェイは、そのトンネルを経由してこの範 囲の IP アドレスを接続するすべてのエンド ポイントに割り当てます。

GlobalProtect ゲートウェイ クライアントの IP プール構成設定	の意味
	 ゲートウェイレベル (Network > GlobalProtect > Gateways > <gateway-config></gateway-config> > GlobalProtect Gateway Configuration > Agent > Client IP Pool) で IP プールを構成し ない場合、クライアントレベ ル (Network > GlobalProtect > Gateways > <gateway-config></gateway-config> > GlobalProtect Gateway Configuration > Agent > Client Settings > <client-setting> > Configs > IP Pools) で IP プール を構成しないでください。</client-setting>

Network Services (ネットワーク サービス) タブ

ネットワーク > グローバルプロテクト > ゲートウェイ > <gateway-config> > エージェント > <agent-config> > Network Services (ネットワーク サービス)

GlobalProtect アプリによりゲートウェイとのトンネルを確立する際のエンドポイントの仮想 ネットワーク アダプタに割り当てられる DNS 設定を行う場合は、Network Services (ネット ワーク サービス)タブを開きます。



Network Services (ネットワーク サービス) オプションは、トンネル モードを有効 にしていて、Tunnel Settings (トンネル設定) タブでトンネル インターフェイスを 定義している場合にのみ使用できます。

GlobalProtect ゲート ウェイ クライアントの ネットワーク サービス 設定	の意味
継承ソース	選択された DHCP クライアントまたは PPPoE クライアント イン ターフェイスから GlobalProtect アプリ設定に、DNS サーバーや その他の設定を配信する継承ソースを選択します。この設定によ り、DNSサーバーやWINSサーバーなどのすべてのクライアント ネットワーク設定は、[継承ソース] で選択されたインターフェイス の設定から継承されます。
継承ソース状態の チェック	クライアントインターフェイスに現在割り当てられているサーバー の設定を参照する場合は、継承ソースをクリックします。

GlobalProtect ゲート ウェイ クライアントの ネットワーク サービス 設定	の意味
プライマリ DNS セカンダリ DNS	クライアントに DNS を提供するプライマリ サーバーおよびセカン ダリ サーバーの IP アドレスを入力します。
プライマリ WINS セカンダリ WINS	エンドポイントに Windows Internet Naming Service (WINS) を提供 するプライマリ サーバーおよびセカンダリ サーバーの IP アドレス を入力します。
DNS サフィックスの継 承	継承ソースからDNSサフィックスを継承する場合は、このオプショ ンを選択します。
DNS サフィックス	解決できない非修飾ホスト名が入力されたときにエンドポイントが ローカルで使用するサフィックスをAdd(追加)します。カンマで 区切って複数のサフィックス(最大100個)を入力できます。

Connection Settings(接続設定)タブ

ネットワーク > グローバルプロテクト > ゲートウェイ > <gateway-config> > エージェント > <agent-config> > 接続設定

Connection Settings (接続設定)タブを選択し、GlobalProtect[™] アプリのタイムアウト設定および 認証用 Cookie の使用制限を定義します。

GlobalProtect ゲート	の意味
ウェイ クライアントの	
トンネル モード接続設	
定	

Timeout configuration

ログイン ライフタイム	1回のゲートウェイ ログイン セッションに許可される日数、時間 数、または分数を指定します。
ログインの有効期間が 切れる前に通知	時間を分単位で設定し (デフォルトは 30 分)、GlobalProtect アプリ でログイン有効期間の有効期限通知を表示するようにスケジュール します。Notify Before Lifetime Expires は、Login Lifetime より小 さくする必要があります。
ログイン有効期限切れ メッセージ	デフォルトのログイン有効期間の有効期限メッセージを変更し、ロ グイン有効期間セッションの有効期限が近づいたときにユーザーに

GlobalProtect ゲート ウェイ クライアントの トンネル モード接続設 定	の意味
	表示するカスタムメッセージを作成できます。メッセージの最大長 は 127 文字です。
アイドル タイムアウト	非アクティブ・セッションが自動的にログアウトされるまでの時 間(分単位)を指定します(トンネル・モードの範囲は5~43200分、 非トンネル・モードの範囲は120~43200分、デフォルトは180分 です)。GlobalProtect アプリが VPN トンネルを経由してトラフィッ クをルーティングしていない場合、またはゲートウェイが構成され た期間内にエンドポイントから HIP チェックを受信しない場合、 ユーザーは GlobalProtect からログアウトされます。
非アクティブログアウ ト前に通知 (分)	非アクティブログアウト前の通知時間を分単位で設定(デフォルト は30分)して、アプリで非アクティブログアウト通知の表示をスケ ジュールします。非アクティブログアウト前に通知は、非アク ティブログアウト期間より短くする必要があります。
非アクティブ ログアウ ト メッセージ	既定のメッセージを変更し、非アクティブなセッションの有効期限 が近づいたときにユーザーに表示するカスタム メッセージを作成で きます。メッセージの最大長は 127 文字です。
管理者が開始したログ アウト時にユーザーに 通知する	管理者が開始したログアウトが発生した後にアプリがユーザーに通 知を表示する場合は、このオプションを有効にします。
管理者ログアウト メッ セージ	デフォルトのメッセージを変更し、管理者がログアウトを開始した 後にユーザーに表示するカスタムメッセージを作成できます。メッ セージの最大長は 127 文字です。
認証用 Cookie 使用制限	
SSL VPN の自動復元を 無効化	このオプションを有効化すると、SSL VPN トンネルの自動復元が行 われなくなります。
	このオプションを有効化すると、GlobalProtect が Resilient VPN をサポートしなくなります。
認証用 Cookie 使用制 限(VPN トンネルの自 動復元あるいけ認証の	このオプションを有効化すると、次のいずれかの条件に基づいて認証用 Cookie の使用が制限されます:
オーバーライド用)	 認祉用 Cookie の発効対象である元の送信元 IP-認祉用 Cookie の使用を、Cookie の元の発効対象であるエンドポイントのパブ リックな送信元 IP を持つエンドポイントに制限します。

GlobalProtect ゲート ウェイ クライアントの トンネル モード接続設 定	の意味
	 元の送信元 IP ネットワーク範囲-認証用 Cookie の使用を、宛 先ネットワーク IP アドレス範囲内のパブリックな送信元 IP アド レスを持つエンドポイントに制限します。Source IPv4 Netmask (送信元 IPv4 ネットマスク)を入力して IPv4 アドレスの範囲を指 定するか、Source IPv6 Netmask (送信元 IPv6 ネットマスク)を入 力して IPv6 アドレスの範囲を指定します。
	いずれかのネットマスクを0に設定した場合、指定した IP ア ドレス タイプでこのオプションが無効になります。例えば、 ポータルあるいはゲートウェイがいずれかの IP アドレス タイ プ(IPv4 あるいは IPv6)だけをサポートしている、あるいはい ずれかの IP アドレス タイプでのみこのオプションを有効化した い場合(ポータルあるいはゲートウェイが IPv4 および IPv6 を サポートしている場合)、ネットマスクを0に設定できます。任 意のゲートウェイ設定で一つのネットマスクだけを0に設定でき ます。両方のネットマスクを同時に0に設定することはできませ ん。
	デフォルトのSource IPv4 Netmask (送信元 IPv4 ネットマス ク)の値32を採用する場合、Cookie の元の発効対象であるエ ンドポイントのパブリックな IPv4 アドレスと同じアドレスに 認証用 Cookie の使用が制限されます。デフォルトの Source IPv6 Netmask (送信元 IPv6 ネットマスク)の値128を採用する場 合、Cookie の元の発効対象であるエンドポイントのパブリック な IPv6 アドレスと同じアドレスに認証用 Cookie の使用が制限 されます。

Video Traffic(動画トラフィック)タブ

ネットワーク > グローバルプロテクト > ゲートウェイ > <gateway-config> > エージェント > <agent-config> > ビデオ トラフィック

Video Traffic (動画トラフィック**)**タブを選択し、VPN トンネルから動画ストリーミングのトラフィックを除外します。

GlobalProtect ゲート ウェイ 動画トラフィッ ク設定	の意味
トンネルから動画アプ	動画 ストリーミング トラフィックを VPN トンネルから除外できる
リケーションを除外	ようにするには、このオプションを選択します。

GlobalProtect ゲート ウェイ 動画トラフィッ ク設定	の意味
アプリケーション [applications]	VPN トンネルから除外したい動画ストリーミング アプリケーショ ンを Add(追加)または Browse(参照)します。
	この動画リダイレクトは、次のアプリケーションの動画トラフィッ ク タイプに適用されます。
	Youtube
	Dailymotion
	Netflix
	他の動画ストリーミング アプリケーションでは、次の動画タイプの みをリダイレクトできます。
	• MP4
	• WebM
	• MPEG
	動画ストリーミング トラフィックは、VPN トンネルからのみ除外 できます。動画 ストリーミング アプリケーションを除外しない場 合、すべてのリクエストはトンネル経由でルーティングされます (スプリット トンネリングは行われません)。この場合、インター ネットの要求はすべてファイアウォールを通過して、ネットワーク に出ていきます。この方法により、外部エンドがエンドポイントに アクセスして内部ネットワークにアクセスできなくなる可能性があ ります。

HIP Notification(**HIP** 通知)タブ

ネットワーク > グローバルプロテクト > ゲートウェイ > <gateway-config> > エージェント > <agent-config> > HIP通知

ホスト情報プロファイル(HIP)を含むセキュリティルールが適用された際にエンドユーザーに 表示される通知メッセージを定義する場合はHIP Notification (HIP通知)タブを開きます。

これらのオプションはHIPプロファイルを作成しセキュリティプロファイルに追加済みの場合の み使用可能です。

GlobalProtect エージェ ントの HIP 通知設定	の意味
HIP通知	HIP通知をAdd[追加] し、オプションを設定します。Match Message(一致メッセージ)、Not Match Message(不一致メッ セージ)のいずれか、あるいは両方の通知を Enable(有効化)し、 さらに Show Notification As(通知の表示方法)を System Tray

GlobalProtect エージェ ントの HIP 通知設定	の意味
	Balloon(システム トレイ バルーン)または Pop Up Message(ポッ プ アップ メッセージ)として表示するかどうかを指定することがで きます。さらに一致あるいは不一致のメッセージ内容を指定するこ とができます。
	これらの設定を使用して、ホストシステムに必須のアプリケーショ ンがインストールされていないことを示す警告メッセージを表示 するなど、エンドユーザーにマシンの状態を通知します。Match Message(一致メッセージ)の場合、Include Mobile App List(一致 したアプリケーションのリストをメッセージに含める)オプション を有効化して、HIP マッチをトリガーしたアプリケーションを表示 させることもできます。
	 HIP通知メッセージではリッチHTML形式を使用し、外部のWebサイトやリソースへのリンクを含めることができます。リッチテキスト設定ツールバーのリンク(

GlobalProtect ゲートウェイの Satellite (サテライト) タブ

• ネットワーク > グローバルプロテクト > ゲートウェイ > <gateway-config> > サテライト

サテライトとは、GlobalProtect アプリとして機能して GlobalProtectゲートウェイへのVPN接 続を確立できるようにする、Palo Alto Networksファイアウォール(通常は支社に設置)で す。Satellite (サテライト) タブを選択して、ゲートウェイ トンネル設定およびネットワーク設 定を定義し、サテライトが VPN 接続を確立できるようにします。また、サテライトが通知する ルートを設定することもできます。

GlobalProtect ゲート ウェイのサテライト設 定	の意味
[トンネル設定] タブ	
トンネル設定	Tunnel Configuration [トンネル設定]を選択し、ドロップダウンリ ストから既存の Tunnel Interface [トンネルインターフェイス]、ある いは New Tunnel Interface [新規のトンネルインターフェイス]を選 択します。詳細は「 Network (ネットワーク) > Interfaces (イン ターフェイス) > Tunnel (トンネル)」を参照してください。

GlobalProtect ゲート ウェイのサテライト設 定	の意味
	 Replay attack detection (リプレイ攻撃の検出) – リプレイ攻撃 から保護します。
	 Replay attack detection (リプレイ攻撃検知)を有効 化し、サテライトトンネル設定が有効な場合に GlobalProtect サテライトをリプレイ攻撃から保護 します。
	 Copy TOS[TOSのコピー] – 元のTOS(Type of Service)情報を 保持するため、カプセル化されたパケットの内部IPヘッダーから 外部IPヘッダーに TOSヘッダーをコピーします。
	 Configuration refresh interval (hours)[設定の更新間隔(時間)] ポータルに設定の更新があるかどうかサテライトデバイスに 確認させる間隔を指定します(範囲は1~48時間、デフォルト は2時間)。
トンネル モニタ	サテライトがゲートウェイトンネル接続をモニターし、接続に失敗 した場合にバックアップゲートウェイにフェイルオーバーできるよ うにする場合は、Tunnel Monitoring[トンネルモニタリング]を選択 します。
	 Destination Address(宛先アドレス) – ゲートウェイへの接続 があるかどうかを判断するために使用するトンネルモニターの IPv4 または IPv6 アドレス(ゲートウェイで保護されるネット ワークの IP アドレスなど)を指定します。または、トンネルイ ンターフェイスに IP アドレスを設定した場合はこのフィールド を空白のままにでき、トンネルモニターは代わりにトンネルイ ンターフェイスを使用して接続がアクティブかどうかを判断し ます。
	 Tunnel Monitor Profile[トンネルモニタープロファイル] – 別のゲートウェイへのFailover[フェイルオーバー]は、LSVPNでサポートされている唯一のトンネルモニタリングプロファイルのタイプです。
	 Tunnel Monitoring (トンネルモニタリング)を有効 化してTunnel Monitoring Profile (トンネルモニタ リング プロファイル)を設定し、サテライトトンネ ル設定が有効な場合にフェイルオーバーの動作を 制御します。
暗号化プロファイル	IPSec Crypto Profile[IPSec暗号化プロファイル] を選択するか、新 しいプロファイルを作成します。暗号ファイルにより、VPNトン ネルでの識別、認証、および暗号化のためのプロトコルとアルゴ リズムが決まります。LSVPNの両方のトンネルエンドポイントが

GlobalProtect ゲート ウェイのサテライト設 定	の意味
	組織内の信頼されるファイアウォールであるので、一般にはESPプ ロトコル、DH group2、AES 128 CVC暗号化、およびSHA-1認証 を使用するデフォルトのプロファイルを使用できます。詳細は 「Network(ネットワーク) > Network Profiles(ネットワーク プ ロファイル) > GlobalProtect IPSec Crypto(GlobalProtect の IPSec 暗号)」を参照してください。
[ネットワーク設定] タブ	
継承ソース	選択された DHCP クライアントまたは PPPoE クライアント イン ターフェイスから GlobalProtect サテライト設定に、DNS サーバー やその他の設定を伝搬する継承ソースを選択します。この設定によ り、DNSサーバーなどのすべてのネットワーク設定は、Inheritance Source [継承ソース] で選択したインターフェイスの設定から継承さ れます。
プライマリ DNS セカンダリ DNS	サテライトに DNS を提供するプライマリ サーバーおよびセカンダ リ サーバーの IP アドレスを入力します。
DNS サフィックス	Add[追加] をクリックして、解決できない非修飾ホスト名が入力さ れたときにサテライトがローカルで使用するサフィックスを入力し ます。複数のサフィックスをカンマで区切って入力できます。
DNS サフィックスの継 承	解決できない非修飾ホスト名が入力されたときに、DNSサフィッ クスをサテライトに送信してローカルで使用する場合は、このオプ ションを選択します。
IP プール	このセクションを使用して、VPNトンネルの確立時にサテライトデ バイスのトンネルインターフェイスに割り当てるIPアドレスの範囲 をAdd[追加] します。IPv6 または IPv4 アドレスを指定できます。
	 IPプールには、すべての同時接続ユーザーをサポート するのに十分な IP アドレスが含まれている必要があ ります。IPアドレスはダイナミックに割り当てられ、 サテライトの接続が切断された後は保持されません。 異なるサブネットの複数の範囲を設定することによ り、システムは、サテライトの他のインターフェイス と競合しない IP アドレスをサテライトに割り当てる ことができます。 ネットワーク内のサーバーおよびルーターは、このIPプールから

GlobalProtect ゲート ウェイのサテライト設 定	の意味
	す。たとえば、ネットワーク 192.168.0.0/16 では、サテライトに 192.168.0.10 といったアドレスを割り当てることができます。
	ダイナミック ルーティングを使用している場合、サテライトについ て指定した IP アドレスが、ゲートウェイおよびサテライトでトン ネル インターフェイスに手動で割り当てた IP アドレスと重複しな いようにしてください。
アクセス ルート	Add[追加] をクリックして、ルートを以下のように入力します。
	 サテライトからのすべてのトラフィックをトンネルを経由してルーティングする場合、このフィールドは空白のままにします。 一部のトラフィックのみをゲートウェイ経由でルーティングするには(スプリットトンネルと呼ばれます)、トンネルする必要のある宛先サブネットを指定します。この場合、サテライトは独自のルーティングテーブルを使用して、指定したアクセスルートの宛先になっていないトラフィックをルーティングします。たとえば、企業ネットワークの宛先になっているトラフィックのみをトンネルし、ローカルサテライトを使用して安全なインターネットアクセスを可能にすることができます。 サテライト間のルーティングを有効にするには、各サテライトによって保護されたネットワークのサマリールートを入力します。

Route Filter (\mathcal{N} - \mathcal{N} - \mathcal{N}) \mathcal{P}

公開されたルートの受 け入れ	サテライトによって通知されたルートをゲートウェイのルーティン グテーブルに受け入れる場合は、Accept published routes(公開さ れたルートの受け入れ)を有効にします。このオプションを選択し ない場合、ゲートウェイはサテライトが通知するルートを受け入れ ることができません。
許可されたサブネット	サテライトによって通知されるルートの受け入れをさらに制限す る場合は、許可するサブネットを Add[追加] して、ゲートウェイが ルートを受け入れるサブネットを定義します。サテライトによって 通知されたサブネットのうち、リストに含まれないものは除外され ます。たとえば、LAN 側ですべてのサテライトが、192.168.x.0/24 サブネットで設定されている場合、ゲートウェイでは許可された ルート 192.168.0.0/16 を設定できます。この設定を行うと、ゲー トウェイは192.168.0.0/16サブネットにあるサテライトからのみ、 ルートを受け入れます。

Network > GlobalProtect > MDM [ネットワーク > GlobalProtect > MDM]

Mobile Security Manager を使用してエンド ユーザーのモバイル エンドポイントを管理してい て、HIP が有効なポリシーを適用している場合、Mobile Security Manager と通信して管理対象 エンドポイントの HIP レポートを取得するようにゲートウェイを設定する必要があります。

Mobile Security Manager の MDM 情報を Add (追加) して、ゲートウェイで Mobile Security Manager と通信できるようにします。

GlobalProtect MDM 設 定	の意味
氏名	Mobile Security Manager の名前を入力します(最大 31 文字)。名 前の大文字と小文字は区別されます。また、一意の名前にする必要 があります。文字、数字、スペース、ハイフン、およびアンダース コアのみを使用してください。
	ファイアウォールがマルチ仮想システムモードに設定されている場 合、MDM 設定に Mobile Security Manager を使用可能な仮想シス テム(vsys)が表示されます。マルチ仮想システムモードに設定さ れていないファイアウォールの場合、このフィールドは MDM のダ イアログに表示されません。Mobile Security Manager を保存する と、その場所を変更できなくなります。
接続設定	
SERVER	ゲートウェイがHIPレポートを取得するために接続する、Mobile Security ManagerのインターフェイスのIPアドレスまたはFQDNを 入力します。このインターフェイスへのサービス ルートがあること を確認します。
接続ポート	接続ポートはMobile Security ManagerがHIPレポート要求を リッスンする場所を示します。デフォルトポートは5008で す。GlobalProtect Mobile Security Managerはこのポートをリッス ンします。サードパーティの Mobile Security Manager を使用する 場合、サーバーが HIP レポート要求をリスンするポートの番号を入 力します。
クライアント証明書	HTTPS接続を確立する際にゲートウェイがMobile Security Managerに提示するクライアント証明書を選択します。この証明書 は、Mobile Security Managerが相互認証を使用するように設定され ている場合にのみ必要になります。

GlobalProtect MDM 設 定	の意味
信頼されたルート CA	Add[追加] をクリックし、HIPレポートを取得するためにゲート ウェイが接続するインターフェイスの証明書を発行するために使 用されたルートCA証明書を選択します。(このサーバー証明書は Mobile Security Manager のエンドポイント チェックイン インター フェイス用に発効された証明書と異なるものでも構いません。) ルートCA証明書を必ずインポートし、このリストに追加してくだ さい。

Network(ネットワーク) > GlobalProtect > Clientless Apps(クライアントレス アプリケーション)

GlobalProtect クライアントレス VPN を経由してアクセスできるアプリケーションを追加 するには、Network(ネットワーク) > GlobalProtect > Clientless App(クライアントレス アプリケーション)を選択します。個々のクライアントレス アプリケーションを追加した 後、Network(ネットワーク) > GlobalProtect > Clientless App Groups(クライアントレスア プリケーション グループ)を選択して、アプリケーション グループを定義できます。

GlobalProtect クライアントレス VPN は、HTML、HTML5、および JavaScript テクノロジを使用 する一般的なエンタープライズ Web アプリケーションへの安全なリモートアクセスを提供しま す。ユーザーは GlobalProtect ソフトウェアをインストールすることなく、SSL 対応の Web ブ ラウザから安全なアクセスを利用できます。これは、パートナーや請負業者によるアプリケー ションへのアクセスを有効にする必要がある場合や、管理対象でないアセット(個人用デバイス など)を安全に有効にする必要がある場合に便利です。

この機能を使用するには、GlobalProtect クライアントレス VPN の動的更新が必要です。また、GlobalProtect ポータルからクライアントレス VPN をホストしているファイアウォールに GlobalProtect サブスクリプションをインストールする必要があります。

クライアントレス アプ リケーション設定	の意味
氏名	アプリケーションの分かりやすい名前を入力します(最大 31 文 字)。名前の大文字と小文字は区別されます。また、一意の名前に する必要があります。文字、数字、スペース、ハイフン、およびア ンダースコアのみを使用してください。
場所	マルチ仮想システムモードになっているファイアウォールの場 合、Location[場所] はGlobalProtectゲートウェイを使用できる仮 想システム(vsys)になります。マルチ仮想システムモードに なっていないファイアウォールの場合、Location[場所] フィール ドはGlobalProtect Gateway [GlobalProtectゲートウェイ] ダイア ログに表示されません。ゲートウェイの設定を保存すると、その Location[場所] は変更できなくなります。
アプリケーションの ホーム URL	アプリケーションが配置されている URL を入力します(最大 4095 文字)。
アプリケーションの説 明	(<u>任意</u>)アプリケーションの説明を入力します(最大 255 文字)。 文字、数字、スペース、ハイフン、およびアンダースコアのみを使 用してください。

クライアントレス アプ リケーション設定	の意味
アプリケーションのア イコン	(任意)公開するアプリケーション ページでアプリケーションを識 別するためのアイコンをアップロードします。アイコンを参照して アップロードすることができます。

Network (ネットワーク) > GlobalProtect > Clientless App Groups (クライアントレス アプリケーション グ ループ)

GlobalProtect クライアントレス VPN を経由してアクセスできるアプリケーションをグループ化 するには、Network(ネットワーク) > GlobalProtect > Clientless App Groups(クライアント レス アプリケーション グループ)を選択します。既存のクライアントレス アプリケーションを グループに追加したり、グループの新しいクライアントレス アプリケーションを設定したりで きます。複数のアプリケーションを同時に作業する場合にグループは便利です。たとえば、標準 の SaaS アプリケーション セット(Workday、JIRA、Bugzilla など)があり、これらをクライア ントレス VPN アクセスで設定したいと考える場合があります。

クライアントレス ア プリケーション グ ループ設定	の意味
氏名	アプリケーション グループの分かりやすい名前を入力します(最大 31 文字)。大文字と小文字を区別し、一意の名前を入力する必要があ ります。文字、数字、スペース、ハイフン、アンダースコアのみが使 用できます。
場所	マルチ仮想システムモードになっているファイアウォールの場 合、Location[場所] はGlobalProtectゲートウェイを使用できる仮 想システム (vsys) になります。マルチ仮想システムモードに なっていないファイアウォールの場合、Location[場所] フィールド はGlobalProtect Gateway [GlobalProtectゲートウェイ] ダイアログに 表示されません。ゲートウェイの設定を保存すると、その Location[場 所] は変更できなくなります。
アプリケーション [applications]	ドロップダウン リストから Application (アプリケーション) を Add (追加) するか、新しいクライアントレス アプリケーションを設 定してグループに追加します。新しいクライアントレス アプリケー ションを設定するには、「Network (ネットワーク) > GlobalProtect > Clientless Apps (クライアントレス アプリケーション)」を参照し てください。

Objects > GlobalProtect > HIP Objects [オブジェクト > GlobalProtect > HIP オブジェクト]

ホスト情報プロファイル(HIP)のオブジェクトを定義するには、Objects(オブジェクト) > GlobalProtect > HIP Objects(HIP オブジェクト)を選択します。HIPオブジェクトは、ポリ シーを適用する場合に使用する、アプリが送信した生データに対してフィルタをかける際の一致 条件を定めるものです。例えば生のホストデータにエンドポイントが所有している数種類のアン チウイルスパッケージに関する情報が含まれる場合に、企業で必要としている特定のアプリに関 する情報のみを選別する必要があります。この場合、適用したい特定のアプリケーションに一致 するHIPオブジェクトを作成します。

必要なHIPオブジェクトがどれであるか判別する場合は、ホスト情報をどのように使用してポリ シーを適用するかを明確化させることをお勧めします。HIPオブジェクト自体は、セキュリティ ポリシーで使用するHIPプロファイルを作成するための構成要素にすぎないということに注意し てください。そのため、オブジェクトをシンプルにし、たとえば、特定のタイプの必須ソフト ウェアがあるか、特定のドメインのメンバーか、特定のエンドポイント OS があるかなど、1つ の条件にのみ一致させることが必要になる場合があります。こうすることで、HIPで補完された 非常に粒度の細かいポリシーを柔軟に作成することができます。

HIP オブジェクトを作成するには、Add[追加] をクリックしてHIP Object [HIP オブジェクト] ダ イアログを開きます。各フィールドへの入力内容の説明については、以下の表を参照してくださ い。

- HIP オブジェクトの General (全般) タブ
- HIP オブジェクトの Mobile Device (モバイル デバイス) タブ
- HIP オブジェクトの Patch Management (パッチ管理) タブ
- HIP オブジェクトの Firewall (ファイアウォール) タブ
- HIP オブジェクトの Anti-Malware (アンチマルウェア) タブ
- HIP オブジェクトの Disk Backup(ディスク バックアップ)タブ
- HIP オブジェクトの Disk Encryption(ディスク暗号化)タブ
- HIP オブジェクトの Data Loss Prevention (データ損失防止)
- HIP オブジェクトの Certificate (証明書) タブ
- HIP オブジェクトの Custom Checks (カスタム チェック) タブ

HIP で補完されたセキュリティ ポリシーを作成する方法の詳細は、『GlobalProtect Administrator's Guide(GlobalProtect 管理者ガイド)』の「Configure HIP-Based Policy Enforcement(HIP ベースのポリシー適用の設定)」を参照してください。

HIP オブジェクトの General (全般) タブ

• オブジェクト > グローバルプロテクト > HIP オブジェクト > <hip-object> > 一般

General (全般) タブを選択して、新しい HIP オブジェクトの名前を指定したり、ドメイン、オペレーティング システム、ネットワーク接続のタイプなど、一般的なホスト情報と照合するためのオブジェクトを設定したりします。

HIP オブジェクトの 一般設定	の意味
氏名	HIP オブジェクトの名前を入力します(最大 31 文字)。名前の大文 字と小文字は区別されます。また、一意の名前にする必要がありま す。文字、数字、スペース、ハイフン、およびアンダースコアのみを 使用してください。
共有	Shared[共有] を選択した場合、現行のHIPオブジェクトは以下で使用 可能になります。
	ファイアウォールのすべての仮想システム(vsys)(マルチ仮想シス テムモードのファイアウォールにログインしている場合)。この選択 を解除すると、Objects[オブジェクト] タブのドロップダウンリストか ら選択した Virtual System[仮想システム] のみに対してオブジェクト が公開されます。マルチ仮想システムモードに設定されていないファ イアウォールの場合、このオプションはHIPオブジェクトのダイアロ グに表示されません。
	Panorama [™] のすべてのデバイス グループ。この選択を解除する と、Objects[オブジェクト] タブのドロップダウンリストから選択した Device Group[デバイスグループ] のみに対してオブジェクトが公開さ れます。
	オブジェクトを保存すると、その Shared[共有] 設定を変更できなくなります。現在の Location(場所)を確認する場合は、 Objects(オブジェクト) > GlobalProtect > HIP Objects(HIP オブジェクト)を選択します。
の意味	(任意)説明を入力します。
ホスト情報	ホスト情報を設定する場合のオプションを有効化する場合はこのオプ ションを選択します。
管理対象	エンドポイントが管理対象かどうかに基づいてフィルタリングしま す。管理対象のエンドポイントを照合する場合は、Yes (はい)を選択 します。管理対象以外のエンドポイントを照合する場合は、No (いい え)を選択します。
オーバーライドの無 効化(Panoramaの み)	Objects[オブジェクト] タブで選択した Device Group[デバイスグループ] の子孫デバイス グループのHIPオブジェクトに対するオーバーラ イドアクセスを制御します。管理者が、継承した値をオーバーライド することで、オブジェクトのローカルコピーを子孫デバイスグループ に作成することを禁止したい場合はこのオプションを選択してくださ

HIP オブジェクトの 一般設定	の意味
	い。デフォルトでは、このオプションは解除(オーバーライドが有効 化)されています。
ドメイン	ドメイン名による照合を行うには、ドロップダウンリストから演算子 を選択して、照合文字列を入力します。
OS	ホストOSによる照合を行う場合は、最初のドロップダウンリストから Contains[含む] を選択し、2つ目のドロップダウンリストからベン ダーを選択し、3つ目のドロップダウンリストでOSバージョンを選択 するか、あるいはAll[すべて] を選択して、選択したベンダーのすべて のOSバージョンで照合を行うことができます。
クライアント バー ジョン	特定のバージョン番号による照合を行うには、ドロップダウンリスト から演算子を選択して、テキスト ボックスに照合する (または除外す る) 文字列を入力します。
ホスト名	特定のホスト名の全体または一部による照合を行うには、ドロップダ ウンリストから演算子を選択して、テキスト ボックスに照合する (ま たは、選択した演算子によっては除外する) 文字列を入力します。
ホストID	ホスト ID は、GlobalProtect がホストの識別のために割り当てる、一 意の ID です。ホスト ID の値は、デバイス タイプによって異なりま す。
	 Windows – レジストリ(HKEY_Local_Machine\Software \Microsoft\Cryptography\MachineGuid)に保存されているマシン GUID
	 macOS – 最初の組み込み物理ネットワーク インターフェイスの MAC アドレス
	Android—Android ID
	• ios-udid
	• Linux-システム DMI テーブルから取得した製品 UUID
	 Chrome – GlobalProtect によって割り当てられた、長さが 32 文字の一意の英数字
	特定のホスト ID による照合を行うには、ドロップダウン リストから 演算子を選択して、テキスト ボックスに照合する(または、選択した 演算子によっては除外する)文字列を入力します。
シリアル番号	エンドポイントのシリアル番号の全体または一部による照合を行うに は、ドロップダウンリストから演算子を選択してから、照合文字列を 入力します。

HIP オブジェクトの 一般設定	の意味
ネットワーク	このフィールドを使用して、特定のモバイル デバイス ネットワーク設 定によるフィルタリングを有効にします。この一致基準はモバイル デ バイスのみに適用されます。
	ドロップダウンリストから演算子を選択し、2つ目のドロップダウン リストからフィルタリング基準にするネットワーク接続のタイプを選 択します。Wifi、Mobile[モバイル]、Ethernet(Is Not[ではない] フィ ルタの場合のみ選択可能)、またはUnknown[不明]。ネットワークタ イプを選択したら、指定可能な場合は、追加の照合文字列を入力しま す。たとえば、モバイル「Carrier[通信事業者]」やWiFi「SSID」など を指定できます。

HIP オブジェクトの Mobile Device (モバイル デバイス) タブ

 オブジェクト > グローバルプロテクト > HIP オブジェクト > <hip-object> > モバイル デバイ ス

Mobile Device (モバイル デバイス) タブを選択して、GlobalProtect アプリケーションを実行するモバイル デバイスから収集されたデータによる HIP 照合を有効にします。

モバイルデバイスの属性を収集し、HIP 実施ポリシーで使用するに
 は、GlobalProtect に MDM サーバーが必要です。GlobalProtect は現在、AirWatch
 MDM サーバーとの HIP 統合をサポートしています。

HIP オブジェクトのモバ イル デバイス設定	の意味
モバイル デバイス	GlobalProtect アプリが稼動しているモバイル デバイスから収集し たホスト データに対するフィルタリングを有効化し、Device(デ バイス)、Settings(設定)、および Apps(アプリ)タブを有効化 する場合は、このオプションを選択します。
Device (デバイス) タブ	• Model[モデル] – 特定のデバイス モデルによる照合を行うに は、ドロップダウンリストから演算子を選択し、照合文字列を 入力します。
	 Tag[タグ] – GlobalProtect Mobile Security Manager に定義され たタグ値による照合を行うには、最初のドロップダウンリスト から演算子を選択し、2 つ目のドロップダウンリストからタグを 選択します。
	• Phone Number[電話番号] – デバイスの電話番号の全体または一 部による照合を行うには、ドロップダウンリストから演算子を 選択し、照合文字列を入力します。

HIP オブジェクトのモバ イル デバイス設定	の意味
	 IMEI – IMEI (International Mobile Equipment Identity) による照 合を行うには、ドロップダウンリストから演算子を選択し、照 合文字列を入力します。
Settings(設定)タブ	 Passcode[パスコード] – デバイスにパスコードが設定されているかどうかに基づいてフィルタリングします。パスコードが設定されているデバイスを照合する場合は、Yes[はい]を選択します。パスコードが設定されていないデバイスを照合するには、no(いいえ)を選択します。
	 Rooted/Jailbroken[root 化/jailbreak] – デバイスが root 化また は jailbreak されているかどうかに基づいてフィルタリングしま す。root化またはjailbreakされているデバイスを照合する場合 は、Yes[はい]を選択します。root化またはjailbreakされていな いデバイスを照合する場合は、No[いいえ]を選択します。
	 Disk Encryption[ディスク暗号化] – デバイス データが暗号化 されているかどうかに基づいてフィルタリングします。ディス ク暗号化が有効なデバイスを照合するには、yes (はい) を選択 します。ディスク暗号化が有効ではないデバイスを照合するに は、no(いいえ)を選択します。
	 Time Since Last Check-in[最後のチェックインからの経過時間] デバイスが最後に MDM にチェックインした日時に基づいて フィルタリングします。ドロップダウンリストから演算子を選 択し、チェックイン期間の日数を指定します。たとえば、過去 5 日以内にチェックインされていないデバイスを照合するための オブジェクトを定義できます。
Apps(アプリ)タブ	 Apps[アプリ] – (Androidデバイスのみ)デバイスにインストー ルされているアプリケーションに基づいて、また、マルウェア に感染したアプリケーションがデバイスにインストールされて いるかどうかに基づいたフィルタリングを有効にする場合は、 このオプションを選択します。
	• Criteria[一致条件] タブ
	 Has Malware(マルウェア感染) – マルウェアに感染し たアプリがインストールされているデバイスを照合する には、Yes(はい)を選択します。マルウェアに感染した アプリがインストールされていないデバイスを照合する には、No(いいえ)を選択します。一致条件として Has Malware(マルウェア感染)を使用しない場合は、None(な し)を選択します。

HIP オブジェクトのモバ イル デバイス設定	の意味
	• Include[含める] タブ
	 Package (パッケージ) – 特定のアプリがインストールされているデバイスを照合するには、アプリをAdd(追加)して、一意のアプリ名をリバース DNS 形式で入力します。たとえば、com.netflix.mediaclient に続けて、対応するアプリHash(ハッシュ)を入力します。GlobalProtect アプリはこれを計算し、デバイス HIP レポートで送信します。

HIP オブジェクトの Patch Management (パッチ管理) タブ

• オブジェクト > グローバルプロテクト > HIP オブジェクト > <hip-object> > パッチ管理

Patch Management (パッチ管理) タブを選択して、GlobalProtect エンドポイントのパッチ状態 による HIP 照合を有効にします。

HIP オブジェクトのパッ チ管理設定	の意味
パッチ管理	ホストのパッチ管理ステータスに対する照合を有効化し、Criteria (一致条件) およびVendor (ベンダー) タブを有効化する場合はこのオ プションを選択します。
Criteria (一致条件) タブ	 以下の設定を指定します。 Is Installed[インストール済み] – パッチ管理ソフトウェアがホストにインストールされているかどうかによって照合します。 Is Enabled[有効] – パッチ管理ソフトウェアがホストで有効かどうかによって照合します。Is Installed[インストール済み]の選択が解除されている場合、このフィールドは自動的にnone[なし]に設定され、編集ができなくなります。 Severity(重大度) – 論理演算子のリストから重大度を選択し、指定した重大度値のパッチがホストから欠落しているかどうかを照合します。 GlobalProtect 重大度値と OPSWAT 重大度格付けの間で次のマッピングを使用して、各値の意味を理解してください。 0-低 1-中 2-重要
	 3-極めて重大

HIP オブジェクトのパッ チ管理設定	の意味
	 Check[チェック] – エンドポイントのパッチが欠落しているかどうかによって照合します。
	 Patches[パッチ] – ホストに特定のパッチが適用されているか どうかによって照合します。Add (追加)をクリックし、チェッ クする特定のパッチの KB アーティクル ID を入力します。例え ば、Microsoft Office 2010 (KB3128031) 32-Bit Edition の更新を チェックする場合は3128031を入力します。
Vendor(ベンダー)タ ブ	ホスト上で検索して照合する、パッチ管理ソフトウェアや製品の 特定のベンダーを定義します。Add[追加]をクリックして、ドロッ プダウンリストからVendor[ベンダー]を選択します。必要に応じ て、Add(追加)をクリックして、特定のProduct(製品)を選択 します。OKをクリックして設定を保存します。

HIP オブジェクトの Firewall (ファイアウォール) タブ

オブジェクト > グローバルプロテクト > HIP オブジェクト > <hip-object> > ファイアウォール
 Firewall (ファイアウォール) タブを選択して、GlobalProtect エンドポイントのファイアウォール
 ソフトウェア状態に基づく HIP 照合を有効にします。

HIP オブジェクトのファイアウォール設定

ホストのファイアウォールソフトウェア状態による照合を有効化する場合は、**Firewall**[ファイアウォール] を選択します。

- インストール済み ファイアウォール ソフトウェアがホストにインストールされているか どうかによって照合します。
- Is Enabled[有効] ファイアウォール ソフトウェアがホストで有効かどうかによって照合します。Is Installed[インストール済み]の選択が解除されている場合、このフィールドは自動的にnone[なし]に設定され、編集ができなくなります。
- Vendor and Product[ベンダーおよび製品] ホスト上で検索して照合する特定のファイア ウォール ソフトウェア ベンダー/製品を定義します。Add[追加] をクリックして、ドロッ プダウンリストからVendor[ベンダー] を選択します。必要に応じて、Add[追加] をクリッ クして、特定のProduct[製品]を選択します。OK をクリックして設定を保存します。
- Exclude Vendor[ベンダーの除外] 特定のベンダーのソフトウェアがないホストを照合す る場合は、このオプションを選択します。

HIP オブジェクトの Anti-Malware (アンチマルウェア) タブ

• オブジェクト > グローバルプロテクト > HIP オブジェクト > <hip-object> > マルウェア対策

Anti-Malware (アンチマルウェア) タブを選択して、GlobalProtect エンドポイントのアンチウイ ルスあるいはアンチスパイウェア対象範囲に基づく HIP 照合を有効にします。

HIP オブジェクトのアンチマルウェア設定

ホストのアンチウィルスまたはアンチスパイウェア対象範囲に基づいた照合を有効にするに は、Anti-Malware(アンチマルウェア)を選択します。追加の一致条件を定義します。

- Is Installed(インストール済み) アンチウィルスまたはアンチスパイウェア ソフトウェ アがホストにインストールされているかどうかによって照合します。
- Real Time Protection (リアルタイム保護) リアルタイムのアンチウィルスまたはアンチ スパイウェア保護がホストで有効かどうかによって照合します。Is Installed[インストール 済み]の選択が解除されている場合、このフィールドは自動的にNone[なし]に設定され、 編集ができなくなります。
- Virus Definition Version[ウイルス定義バージョン] 指定された日数内にウイルス定義が 更新されたかどうか、またはリリースバージョンのどちらに基づいて照合を行うかを指定 します。
- Product Version (製品バージョン) アンチウィルスまたはアンチウイルスソフトウェ アの特定のバージョンに対して照合を行います。検索するバージョンを指定するには、ド ロップダウンリストから演算子を選択して、製品バージョンを表す文字列を入力します。
- 最終スキャン時間 最後にアンチウィルスまたはアンチスパイウェア スキャンが実行された時間に基づいて照合を行うかどうかを指定します。ドロップダウンリストから演算子を選択し、照合するDays(日)数またはHours(時間)数を指定します。
- ベンダーおよび製品 ホスト上で検索して照合する特定のアンチウィルスまたはアンチスパイウェア ソフトウェア ベンダー/製品を定義します。Add(追加)をクリックして、ドロップダウンリストからVendor(ベンダー)を選択します。必要に応じて、Add[追加]をクリックして、特定のProduct[製品]を選択します。OK をクリックして設定を保存します。
- Exclude Vendor[ベンダーの除外] 特定のベンダーのソフトウェアがないホストを照合す る場合は、このオプションを選択します。

HIP オブジェクトの Disk Backup(ディスク バックアップ)タブ

 オブジェクト > グローバルプロテクト > HIP オブジェクト > <hip-object> > ディスク バック アップ

Disk Backup (ディスク バックアップ**)** タブを選択して、GlobalProtect エンドポイントのディスク バックアップ状態に基づく HIP 照合を有効にします。

HIP オブジェクトのディスク バックアップ設定

ホストのディスクバックアップ状態による照合を有効にするには、**Disk Backup**[ディスクバックアップ] を選択し、追加の照合条件を以下のように定義します。
HIP オブジェクトのディスク バックアップ設定

- Is Installed[インストール済み] ディスク バックアップ ソフトウェアがホストにインス トールされているかどうかによって照合します。
- Last Backup Time[最終スキャン時間] 最後にディスク バックアップが実行された時間に 基づいて照合を行うかどうかを指定します。ドロップダウンリストから演算子を選択し、 照合するDays[日]数またはHours[時間]数を指定します。
- Vendor and Product[ベンダーおよび製品] ホスト上で検索して照合する、特定のディス クバックアップ ソフトウェアベンダーまたは製品を定義します。Add[追加] をクリックし て、ドロップダウンリストからVendor[ベンダー] を選択します。必要に応じて、Add[追 加] をクリックして、特定のProduct[製品]を選択します。OK をクリックして設定を保存し ます。
- Exclude Vendor[ベンダーの除外] 特定のベンダーのソフトウェアがないホストを照合す る場合は、このオプションを選択します。

HIP オブジェクトの Disk Encryption (ディスク暗号化) タブ

• オブジェクト > グローバルプロテクト > HIP オブジェクト > <hip-object> > ディスク暗号化

Disk Encryption (ディスク暗号化**)** タブを使用して、GlobalProtect エンドポイントのディスク暗 号化状態に基づく HIP 照合を有効にします。

HIP オブジェクトのディ スク暗号化設定	の意味
ディスク暗号化	ホストのディスク暗号化状態による照合を有効にする場合は、Disk Encryption(ディスク暗号化)を選択します。
基準	以下の設定を指定します。
	 Is Installed[インストール済み] – ディスク暗号化ソフトウェア がホストにインストールされているかどうかによって照合しま す。
	 Encrypted Locations[暗号化された場所] – Add[追加] をクリック して、照合時にディスクが暗号化されているかチェックするド ライブまたはパスを指定します。
	• Encrypted Locations[暗号化された場所] – 暗号化されているか どうかをチェックするホスト上の特定の場所を入力します。
	 State[状態] – 暗号化された場所の状態を照合する方法を指定します。ドロップダウンリストから演算子を選択し、有効な状態 (full[フル]、none[なし]、partial[一部]、not-available[使用不可]) を選択します。
	OK をクリックして設定を保存します。

HIP オブジェクトのディ スク暗号化設定	の意味
ベンダー	エンドポイント上で検索して照合する、特定のディスク暗号化ソフ トウェアベンダーまたは製品を定義します。Add[追加] をクリック して、ドロップダウンリストからVendor[ベンダー] を選択します。 必要に応じて、Add[追加] をクリックして、特定のProduct[製品]を 選択します。OK をクリックして設定を保存し、Disk Encryption (ディスク暗号化) タブに戻ります。

HIP オブジェクトの Data Loss Prevention (データ損失防止)

 オブジェクト > グローバルプロテクト > HIP オブジェクト > <hip-object> > データ損失防 止(DLP)

GlobalProtect エンドポイントがデータ損失防止ソフトウェアを稼働しているか否かに基づいて HIP 照合を設定する場合は、Data Loss Prevention (データ損失防止)タブを開きます。

HIP オブジェクトのデータ損失防止設定

ホスト(Windows ホストのみ)のデータ損失防止(DLP)による照合を有効にする場合 は、Data Loss Prevention (データ損失防止)を選択し、追加の照合条件を以下のように定義し ます。

- Is Installed[インストール済み] DLP ソフトウェアがホストにインストールされているか どうかによって照合します。
- Is Enabled(有効) DLP ソフトウェアがホストで有効かどうかによって照合します。Is Installed[インストール済み]の選択が解除されている場合、このフィールドは自動的 にnone[なし]に設定され、編集ができなくなります。
- Vendor and Product[ベンダーおよび製品] ホスト上で検索して照合する特定の DLP ソフトウェア ベンダー/製品を定義します。Add[追加] をクリックして、ドロップダウンリストからVendor[ベンダー]を選択します。必要に応じて、Add[追加] をクリックして、特定のProduct[製品]を選択します。OK をクリックして設定を保存します。
- Exclude Vendor[ベンダーの除外] 特定のベンダーのソフトウェアがないホストを照合す る場合は、このオプションを選択します。

HIP オブジェクトの Certificate (証明書) タブ

• オブジェクト > グローバルプロテクト > HIP オブジェクト > <hip-object> > 証明書

Certificate (証明書)タブを選択すれば、証明書プロファイルや他の証明書属性に基づいて HIP マッチを有効化できます。

証明書HIPオブジェクトは、WindowsとmacOSでのみサポートされています。

HIP オブジェクトの証明書設定

Validate Certificate (証明書の検証)を選択すれば、証明書プロファイルおよび証明書属性に基づいてマッチを有効化できます。その後、次のように一致条件を定義します:

- Certificate Profile (証明書プロファイル)-HIP レポートで送信されるマシン証明書を検証す るために GlobalProtect ゲートウェイが使用する証明書プロファイルを選択します。
- Certificate Field (証明書フィールド)-マシン証明書に対してマッチを行うために使用する 証明書属性を選択します。
- Value (値)-- 属性の値を設定します。

HIP オブジェクトの Custom Checks (カスタム チェック) タブ

オブジェクト > グローバルプロテクト > HIP オブジェクト > <hip-object> > カスタムチェック

Custom Checks (カスタム チェック**)** タブを選択して、GlobalProtect ポータルに定義されている カスタム チェックに基づく HIP 照合を有効にします。HIP収集にカスタムチェックを追加する方 法の詳細は、「Network(ネットワーク)> GlobalProtect > Portals(ポータル)」を参照してく ださい。

HIP オブジェクトのカス タム チェック設定	の意味
カスタム チェック	GlobalProtectポータルに定義されているカスタムチェックによるHIP照合を有効化する場合は、Custom Checks[カスタムチェック] を選択します。
プロセス リスト	ホスト システムに特定のプロセスがあるかチェックするに は、Add[追加] をクリックし、プロセス名を入力します。デフォ ルトでは、アプリは実行中のプロセスがあるかチェックしま す。特定のプロセスが実行していないかどうかを確認する場合 は、Running(実行中)の選択を解除します。プロセスは、オペ レーティングシステム レベルのプロセスまたはユーザー空間のア プリケーション プロセスとすることができます。
レジストリ キー	Windowsホストに特定のレジストリキーがあるかチェックする場合は、Add[追加] をクリックし、照合する Registry Key[レジストリキー] を入力します。指定したレジストリ キーまたはキーの値が 欠損しているホストのみを照合する場合は、Key does not exist or match the specified value data(キーが存在しないか、指定した値 データと一致しない)のボックスを選択します。
	特定の値を照合するには、Add[追加] をクリックし、Registry Value[レジストリ値] と Value Data[値データ] を入力します。指定

HIP オブジェクトのカス タム チェック設定	の意味
	された値または値データを明示的に持たないホストを照合するに は、Negate[除外] を選択します。
	OK をクリックして設定を保存します。
Plist	Macホストのプロパティリスト (plist) に特定のエントリがあるか チェックする場合は、Add[追加] をクリックし、Plist名を入力しま す。指定したplistを持たないホストのみを照合する場合は、Plist does not exist[Plistが存在しない] を選択します。
	plist 内の特定のキー/値ペアによって照合するには、Add[追加] を クリックし、照合する Key[キー] と対応する Value[値] を入力しま す。指定されたキーまたは値を明示的に持たないホストを照合する 場合は、Negate[除外] を選択します。
	OK をクリックして設定を保存します。

Objects > GlobalProtect > HIP Profiles [オブジェクト > GlobalProtect > HIP プロファイル]

HIP が有効化されたセキュリティポリシーを設定する場合に使用する HIP プロファイル(モニ タリングまたはセキュリティポリシー適用のためにまとめて評価される HIP オブジェクトのコ レクション)を作成するには、Objects(オブジェクト) > GlobalProtect > HIP Profiles(HIP プロファイル)を選択します。HIPプロファイルを作成する場合は、Booleanロジックを使用 し、以前に作成したHIPオブジェクト(と他のHIPプロファイル)を組み合わせることができま す。これにより、作成したHIP プロファイルに対してトラフィックフローを評価し、一致か不一 致かを判定することができます。一致が見つかった場合、対応するポリシールールが適用されま す。一致がなければ、他のポリシー照合条件と同様に、フローは次のルールと照合して評価され ます。

HIP プロファイルを作成するには、Add[追加] をクリックします。以下の表では、[HIPプロファ イル] ダイアログの各フィールドに入力する内容について説明します。HIP で補完されたセキュ リティ ポリシーを作成するために GlobalProtect とワークフローをセットアップする方法の詳 細は、『GlobalProtect Administrator's Guide(GlobalProtect 管理者ガイド)』の「Configure HIP-Based Policy Enforcement(HIP ベースのポリシー適用の設定)」を参照してください。

HIP プロファイル設定	の意味
氏名	プロファイルの名前を入力します (最大 31 文字)。名前の大文字と 小文字は区別されます。また、一意の名前にする必要があります。 文字、数字、スペース、ハイフン、およびアンダースコアのみを使 用してください。
の意味	(任意)説明を入力します。
共有	現在のHIPプロファイルを以下で使用可能にする場合はShared[共 有]を選択します。 • ファイアウォールのすべての仮想システム(vsys)(マルチ仮 想システムモードのファイアウォールにログインしている場 合)。この選択を解除すると、Objects[オブジェクト] タブのド ロップダウンリストで選択した Virtual System[仮想システム]の みに対してプロファイルが公開されます。マルチ仮想システム モードに設定されていないファイアウォールの場合、このオプ
	 Panorama のすべてのデバイス グループ。この選択を解除すると、Objects[オブジェクト] タブのドロップダウンリストで選択したDevice Group[デバイスグループ]のみに対してプロファイルが公開されます。

HIP プロファイル設定	の意味
	プロファイルを保存すると、その Shared[共有] 設定を変更できなく なります。Objects > GlobalProtect > HIP Profiles を選択して、現 在の Location を表示します。
オーバーライドの無効 化(<mark>Panoramaのみ</mark>)	このチェックボックスを使用して、 Objects [オブジェクト] タブで 選択した Device Group [デバイスグループ] の子孫デバイスグループ のHIPプロファイルへのオーバーライドアクセスを制御します。管 理者が、継承した値をオーバーライドすることで、プロファイルの ローカルコピーを子孫デバイスグループに作成することを禁止した い場合はこのオプションを選択してください。デフォルトでは、こ のオプションは解除(オーバーライドが有効化)されています。
一致	[条件の追加] をクリックして、[HIP オブジェクト/プロファイル ビ ルダー] を開きます。
	 一致条件として使用する最初の HIP オブジェクト またはプロファイルを選択し、HIP Objects/Profiles Builder (HIP オブジェクト/プロファイル ビルダー) ダイアログの Match (一致) テキスト ボックスに追加 (① ② ② ② ○ <
	続けて、作成するプロファイルに必要なだけ一致条件を追加して、 追加した条件の間に適切なBoolean演算子(ANDまたはOR)を選 択します(ここでも必要に応じてNOTを使用します)。
	複雑なBoolean式を作成する場合は、Match[一致]のテキストボッ クス内の適切な位置に手動でかっこを追加して、HIPプロファイル が意図したロジックを使用して評価されるようにします。たとえ ば、以下の式は、ホストが FileVault ディスク暗号化(Mac OSシス テム)または TrueCrypt ディスク暗号化(Windowsシステム)を使 用していて、指定されたドメインに属し、Symantec アンチウイル スクライアントをインストールしている場合、そのホストからのト ラフィックに HIP プロファイルが一致することを示します。
	(("MacOS" および "FileVault") または ("Windows" お よび "TrueCrypt")) および "Domain" および "Symantec AV"
	新しいHIPプロファイルへのオブジェクトおよびプロファイルの追 加が終了したら、 OK をクリックします。

)

Device > GlobalProtect Client [デバイス > GlobalProtect クライアント]

以下のトピックでは、GlobalProtect アプリのセットアップおよび管理方法について説明します。

確認すべき情報	以下を参照
GlobalProtect ソフトウェアのリ リースについての詳細を確認してく ださい。	GlobalProtect エージェントソフトウェアの管理
GlobalProtect ソフトウェアをイン ストールする。	GlobalProtect エージェントのセットアップ
GlobalProtect ソフトウェアを使用 する。	GlobalProtect エージェントの使用
その他の情報をお探しですか?	GlobalProtect クライアント ソフトウェアのセット アップ手順の詳細は、GlobalProtect 管理者ガイドの 「GlobalProtect アプリ ソフトウェアのデプロイ」を参 照してください。

GlobalProtect アプリ ソフトウェアの管理

ポータルをホストしているファイアウォールに GlobalProtect アプリ ソフトウェアをダウンロー ドして起動する場合は、Device(デバイス) > GlobalProtect Client(GlobalProtect クライア ント)を選択します(ファイアウォールのみ)。以降、ポータルに接続したエンドポイントは アプリ ソフトウェアをダウンロードするようになります。ポータルで指定するエージェント設 定では、ポータルがエンドポイントにソフトウェアをプッシュする際の方法とタイミングを定 義します。この設定により、アプリが接続した際に自動的にアップグレードが行われるのか、 エンドユーザーにアップグレードのプロンプトが表示されるのか、あるいはすべてまたは特 定のユーザーに対しアップグレードを禁止するかどうかを決定します。詳細は、「ユーザーに よる GlobalProtect アプリのアップグレードを許可」を参照してください。GlobalProtect アプ リ ソフトウェアの配布オプションとソフトウェアのデプロイ手順の詳細は、『GlobalProtect Administrator's Guide (GlobalProtect 管理者ガイド)』の「GlobalProtect アプリ ソフトウェアの デプロイ」を参照してください。

GlobalProtect アプリを初めてダウンロードしてインストールする場合、エンドポイントのユーザーは管理者権限でログインする必要があります。その後のアップグレードでは、管理者権限は必要ありません。

GlobalProtect クライア ントの設定	の意味
バージョン	このバージョンナンバーは Palo Alto Networks 更新サーバーで入手 可能な GlobalProtect アプリ ソフトウェアのバージョンを示してい ます。Palo Alto Networks から新しいアプリ ソフトウェアリリース を入手可能かどうか確認する場合は、Check Now(今すぐチェッ ク)をクリックします。ファイアウォールはサービスルートを使用 して更新サーバーに接続し、新しいバージョンの有無をチェックし ます。適用可能な更新がある場合は、リストの最上部に表示されま す。
サイズ	アプリ ソフトウェア バンドルのサイズ。
リリース日	Palo Alto Networks がリリースを公開した日時。
ダウンロード済み	この列にチェック マークがある場合、対応するアプリ ソフトウェ ア パッケージのバージョンがファイアウォールにダウンロード済み であることを示します。
現在アクティベーショ ン済み	この列にチェック マークがある場合、対応するアプリ ソフトウェ ア パッケージのバージョンがファイアウォールでアクティブ化済み であり、アプリを接続するとダウンロードできることを示します。 一度にアクティブ化できるソフトウェアのバージョンは1つのみで す。
操作	現在、対応するアプリ ソフトウェア パッケージに対して以下のア クションを実行できることを示します。
	 Download (ダウンロード) – 対応するアプリソフトウェアのバージョンを Palo Alto Networks 更新サーバーから入手可能です。ダウンロードを開始する場合はDownload[ダウンロード]をクリックします。ファイアウォールがインターネットにアクセスできない場合、インターネットに接続されたコンピュータでカスタマーサポートサイトにアクセスして Updates (更新) > Software Updates (ソフトウェア更新)を選択し、新しいアプリソフトウェアバージョンを検索してローカル コンピュータにDownload (ダウンロード)します。次にファイアウォールへアプリソフトウェアを手動でUpload (アップロード)します。
	 Activate (アクティベート) – 対応するアプリソフトウェア バージョンはファイアウォールにダウンロード済みですが、ア プリはまだダウンロードできません。Activate (アクティベー ト)をクリックしてソフトウェアをアクティベートし、アプリ をアップグレードできる状態にします。手動でファイアウォー ルにアップロードしたソフトウェア更新をアクティベートする 場合は、Activate From File[ファイルからアクティベート]をク リックして、アクティベートするバージョンをドロップダウン

GlobalProtect クライア ントの設定	の意味
	リストから選択します(Currently Activated[現在アクティベー ト済み] として表示するには画面の更新が必要になる場合があり ます)。
	 Reactivate(再アクティベート) – 対応するアプリソフトウェ アはアクティベート済みで、クライアントがダウンロードでき る状態です。ファイアウォール上で一度にアクティブ化できる GlobalProtect アプリソフトウェアのバージョンは1つのみのた め、エンドユーザーが現在アクティブなバージョン以外のバー ジョンにアクセスする必要がある場合、その別のバージョン をActivate(アクティベート)してCurrently Active(アクティ ベート済み)にする必要があります。
リリース ノート	対応するアプリ バージョンの GlobalProtect リリース ノートへのリ ンクを提供します。
X	以前にダウンロードしたアプリ ソフトウェア イメージをファイア ウォールから削除します。

GlobalProtect アプリのセットアップ

GlobalProtect アプリは、エンドポイントにインストールされ、ポータルとゲートウェイとの GlobalProtect 接続をサポートするアプリケーションです。このアプリは GlobalProtect サービス (PanGP サービス)がサポートします。

ホストのオペレーティングシステムで正しいインストールオプション (32 ビットまたは 64 ビット)を選択するようにしてください。64ビットのホストにインストールする場合、初期インストールには64ビットブラウザとJavaの組み合わせを使用してください。

アプリをインストールするには、インストーラファイルを開いて、画面に表示される指示に従 います。

GlobalProtect アプリの使用

GlobalProtect アプリを起動し、GlobalProtect ステータスパネルの設定メニューから Settings(設定)を選択すると表示される GlobalProtect設定パネルのタブには、ステータスと 設定に関する有用な情報が含まれ、接続の問題のトラブルシューティングに役立つ情報が表示されます。

一般タブーGlobalProtect アカウントに関連付けられているユーザー名とポータルを表示します。このタブからポータルを追加、削除、または変更することもできます。

- Connection tab (接続タブ) –GlobalProtect アプリ用に設定されたゲートウェイを表示し、 各ゲートウェイに関する次の情報を提供します。
 - Gateway Name (ゲートウェイ名)
 - トンネルのステータス
 - 認証状態
 - 接続タイプ
 - ゲートウェイ IP アドレスまたは FQDN(外部モードでのみ使用可能)
 - 内部モードの場合、Connection(接続)タブには使用可能なゲートウェイー覧が 表示されます。外部モードの場合、Connection(接続)タブには接続先のゲート ウェイと、ゲートウェイに関する追加の詳細(ゲートウェイの IP アドレスや稼 働時間など)が表示されます。
- Host Profile tab (ホスト プロファイル タブ) –GlobalProtect がホスト情報プロファイル (HIP) を介してセキュリティポリシーを監視および実施するために使用するエンドポイン ト データを表示します。HIP データをゲートウェイに手動で再送信するには、Resubmit Host Profile (ホストプロファイルの再送信) をクリックします。
- Troubleshooting tab(トラブルシューティングタブ) macOS エンドポイントでは、このタブで Collect Logs(ログを収集)し、Logging Level(ロギングレベル)を設定できます。Windowsエンドポイントでは、このタブで Collect Logs(ログを収集)し、Logging Level(ロギングレベル)を設定し、次の情報を表示してトラブルシューティングを支援します。
 - Network Configurations(ネットワーク構成) 現在のシステム設定を表示します。
 - **Routing Table**[ルーティングテーブル] GlobalProtect 接続の現在のルート指定方法につい ての情報を表示します。
 - Sockets[ソケット] 現在アクティブな接続のソケット情報を表示します。
 - Logs (ログ) GlobalProtect アプリとサービスのログを表示することができます。
 ログ タイプとデバッグ レベルを選択します。Start[開始] をクリックするとログが開始し、Stop[停止] をクリックするとログが停止します。
- Notification tab (通知タブ) GlobalProtect アプリ上でトリガされる通知の一覧を表示しま す。特定の通知の詳細を表示するには、通知をダブルクリックします。



Panorama Web インターフェイス

Panorama[™]は、Palo Alto Networks[®]の次世代ファイアウォール製品のための中央管理システム です。Panorama を使用すると、1 つの場所からネットワーク上のすべてのアプリケーション、 ユーザー、コンテンツを管理し、ここから得られる情報を使用してネットワークを制御および 保護するポリシーを作成することができます。Panorama からポリシーとファイアウォールの中 央管理を行うことで、ファイアウォールの分散ネットワークを管理して、運用の効率性を向上 させることができます。Panorama は、専用ハードウェア(M-Series)アプライアンス、および VMware バーチャル アプライアンス(ESXi サーバーまたは vCloud Air プラットフォームで稼 働)として使用できます。

Panorama Web インターフェイスのビューと設定の大半は、ファイアウォールの Web インター フェイスと同じですが、以下のトピックでは、Panorama、ファイアウォール、ログ コレクタを 管理する Panorama Web インターフェイス独自のオプションについて記載します。

- Panorama Web インターフェイスを使用する
- コンテキスト切り替え
- Panorama のコミット操作
- Panorama でのポリシーの定義
- レガシー モードの Panorama バーチャル アプライアンスのログ ストレージ パーティション
- Panorama > Setup (セットアップ) > Interfaces (インターフェイス)
- Panorama > High Availability [Panorama > 高可用性]
- Panorama > Managed WildFire Clusters (管理対象 WildFire クラスタ)
- Panorama > Administrators [Panorama > 管理者]
- Panorama > Admin Roles [Panorama > 管理者ロール]
- Panorama > Access Domains [Panorama > アクセスドメイン]
- Panorama >スケジュール設定プッシュ
- Panorama > Managed Devices (管理対象デバイス)
- Panorama > Managed Devices(管理対象デバイス) > Health(健康状態)
- Panorama > Templates [Panorama > テンプレート]
- Panorama > Device Groups [Panorama > デバイス グループ]
- Panorama > Managed Collectors [Panorama > 管理対象コレクタ]
- Panorama > Collector Groups [Panorama > コレクタ グループ]
- Panorama > Plugins (プラグイン)
- Panorama > SD-WAN
- Panorama > VMware NSX
- Panorama > Log Ingestion Profile (ログインジェスト プロファイル)
- Panorama > Log Settings [Panorama > ログ設定]

- Panorama > Server Profiles > SCP [Panorama > サーバー プロファイル > SCP]
- Panorama > Scheduled Config Export [Panorama > スケジュール設定された設定のエクスポート]
- Panorama > Software [Panorama > ソフトウェア]
- Panorama > Device Deployment [Panorama > デバイスのデプロイ]
- Panorama >デバイス登録認証キー

その他の情報をお探しですか?

中央管理のための Panorama のセットアップや使用の詳細は、『Panorama Administrator's Guide (Panorama 管理者ガイド) 『』を参照してください。

Panorama Web インターフェイスを使用する

Panorama とファイアウォールの Web インターフェイスの外観は同じです。ただし、Panorama の Webインターフェイスには、Panorama を管理したり、Panorama を使用してファイアウォールやログ コレクタを管理したりするための追加のオプションと Panorama 固有のタブが含まれます。

Panorama のいくつかの Web インターフェイス ページのヘッダーまたはフッターに以下の共通 フィールドが表示されます。

Common Field (共通 フィールド)	の意味	
追加	左側のメニューの上にある Context (コンテキスト)ドロップダウ ンリストを使用して、Panorama の Web インターフェイスとファイ アウォールの Web インターフェイスを切り替えることができます (「コンテキスト切り替え」を参照)。	•
G	 Dashboard (ダッシュボード) タブと Monitor (監視) タブのタブ ヘッダーにある更新 (をクリックすると、それらのタブのデータを手動で更新できます。タブ ヘッダーの右側にあるラベルなしのドロップダウン リストを使用 して、自動更新間隔を分単位(1 min (1分)、2 mins (2分)、また は 5 mins (5分)) で選択することもできます。自動更新を無効にす るには、Manual (手動)を選択します。)
アクセス ドメイン	 アクセスドメインでは、(Context (コンテキスト)ドロップダウン リストを使用して)特定のデバイスグループ、テンプレート、およ び個々のファイアウォールへのアクセスを定義します。管理者とし てログインし、複数のアクセスドメインが自分のアカウントに割り 当てられている場合、Dashboard (ダッシュボード)、ACC、および Monitor (監視)の各タブには、Web インターフェイスのフッターで 選択した Access Domain (アクセスドメイン) に関する情報 (ログ データなど)のみが表示されます。 アカウントに割り当てられているアクセスドメイン が1つのみの場合、Web インターフェイスに Access Domain (アクセスドメイン)ドロップダウンリストは 表示されません。 	-
デバイス グループ	デバイス グループは、グループとして管理するファイアウォールと 仮想システムで構成されます(「Panorama > Device Groups(デバイ ス グループ)」を参照)。Dashboard(ダッシュボード)、ACC、 および Monitor(監視)の各タブには、タブ ヘッダーで選択し	-

Common Field (共通 フィールド)	の意味
	た Device Group(デバイス グループ)に関する情報(ログ デー タなど)のみが表示されます。Policies(ポリシー)タブおよび Objects(オブジェクト)タブでは、特定のDevice Group(デバイ ス グループ)の設定またはすべてのデバイス グループ(Shared(共 有)を選択)の設定を指定できます。
テンプレート	テンプレートは、共通のネットワーク設定とデバイス設定を持つ ファイアウォールのグループであり、テンプレートスタックはテン プレートの組み合わせです(「Panorama > Templates(テンプレー ト)」を参照)。Network(ネットワーク)タブおよび Device(デ バイス)タブでは、特定の Template(テンプレート)またはテンプ レートスタックの設定を指定できます。編集できるのは、個々のテ ンプレート内の設定のみです。そのため、テンプレートスタックを 選択した場合、これらのタブ内の設定は読み取り専用で表示されま す。
表示基準:デバイス モード	 デフォルトでは、Network(ネットワーク)タブおよび Device(デバイス)タブには、複数の仮想システムと VPN をサポートする、通常の操作モードのファイアウォールで使用できる設定と値が表示されます。ただし、以下のオプションを使用してタブをフィルタリングすることで、編集したいモード固有の設定のみを表示できます。 Mode(モード)ドロップダウン リストで、Multi VSYS(マルチ VSYS)、Operational Mode(操作モード)、およびVPN Mode(VPNモード)オプションを選択または選択解除します。 特定のファイアウォールのモード設定を反映するようにすべてのモードオプションを設定するには、View by:(閲覧方法:) Device(デバイス)ドロップダウン リストでそのファイアウォールを選択します。

Panorama タブには、Panorama とログ コレクタを管理するための以下のページが提供されます。

Panorama ページ	の意味
セットアップ	以下のタスクを実行するには、 Panorama > Setup (セットアップ)を選 択します。
	 一般設定(Panorama のホスト名など)と、認証、ログ、レポート、AutoFocus[™]、バナー、本日のメッセージ、パスワード複雑性に関する設定を指定する。これらの設定は、ファイアウォールで指定する設定(Device(デバイス) > Setup(セットアップ) > Management(管理)を選択)と似ています。

Panorama ページ	の意味
	 設定のバックアップと復元、Panoramaの再起動、Panoramaの シャットダウンを行う。これらの操作は、ファイアウォールで 実行する操作(Device(デバイス) > Setup(セットアップ) > Operations(操作)を選択)と似ています。
	 DNS、NTP、および Palo Alto Networks 更新用サーバーとの接続 を定義する。これらの設定は、ファイアウォールで指定する設定 (Device(デバイス) > Setup(セットアップ) > Services(サービ ス)を選択)と似ています。
	 Panorama インターフェイス用のネットワーク設定を定義する。Panorama > Setup(セットアップ) > Interfaces(インターフェイス)の順に選択します。
	 WildFire[™] アプライアンスに関する設定を指定する。これらの設定は、ファイアウォールで指定する設定(Device(デバイス) > Setup(セットアップ) > WildFireを選択)と似ています。
	 ハードウェアセキュリティモジュール(HSM)の設定管理これらの 設定は、ファイアウォールで指定する設定(Device(デバイス) > Setup(セットアップ) > HSMを選択)と似ています。
HA	一対のPanorama管理サーバーに高可用性(HA)環境を設定しま す。[Panorama] > [高可用性] の順に選択します。
設定監査	設定ファイル間の差異を確認できます。Device(デバイス) > Config Audit(設定監査)の順に選択します。
パスワード プロ ファイル	Panorama管理者用にパスワードプロファイルを設定することができま す。Device(デバイス) > Password Profiles(パスワード プロファイ ル)の順に選択します。
administrators	Panorama 管理者アカウントを設定できます。Panorama > Administrators(管理者)の順に選択します。
	管理者アカウントがロックアウトされている場合、Administrators(管理者)ページのLocked User(ロックされたユーザー)列にロックが表示されます。このロックをクリックしてアカウントのロックを解除できます。
管理者ロール	Panorama にアクセスする管理者のアクセス権限や役割を制御する管理 ロールを定義できます。Panorama > Admin Roles(管理者ロール)の順 に選択します。
アクセス ドメイン	デバイス グループ、テンプレート、テンプレート スタック、および ファイアウォールの Webインターフェイスへの管理者アクセスを制御で

Panorama ページ	の意味
	きます。Panorama > Access Domains(アクセスドメイン)の順に選択 します。
認証プロファイル	Panoramaへのアクセスを認証するプロファイルを指定できま す。Device(デバイス) > Authentication Profile(認証プロファイ ル)の順に選択します。
認証シーケンス	Panoramaへのアクセス許可に使用する一連の認証プロファイルを指定で きます。Device(デバイス) > Authentication Sequence(認証シーケン ス)の順に選択します。
ユーザー ID	User-ID エージェントとの相互認証に向けてカスタム証明書プロ ファイルを設定することができます。Device(デバイス) > User Identification(ユーザー ID) > Connection Security(接続のセキュリ ティ)を選択します。
Data Redistribution(デー タの再配信)	他のファイアウォールまたは Panorama 管理システムにデータを 選択的に再配信することができます。Device(デバイス) > Data Redistribution(データの再配信)を選択します。
Managed Devices(管理対 象デバイス)	ファイアウォールを管理対象デバイスとして Panorama に追加する、 ファイアウォールの接続状況とライセンス状態を表示する、ファイア ウォールにタグを付ける、ファイアウォールのソフトウェアとコンテン ツを更新する、設定のバックアップをロードするなど、ファイアウォー ルを管理できます。Panorama > Managed Devices(管理対象デバイス) > Summary(サマリー)を選択します。
テンプレート	Device(デバイス)タブおよびNetwork(ネットワーク)タブの設定 オプションを管理できます。テンプレートとテンプレートスタックを使 用すると、同じまたは似た設定を持つ複数のファイアウォールを導入す る場合の管理作業を軽減できます。Panorama > Templates(テンプレー ト)の順に選択します。
デバイスグループ	デバイス グループを設定することで、機能、ネットワーク セグメン ト、または地理的な場所に基づいてファイアウォールをグループ化でき ます。デバイス グループには、物理ファイアウォール、仮想ファイア ウォール、および仮想システムを含めることができます。
	通常、デバイス グループ内のファイアウォールには、類似のポリシー 設定が必要です。デバイス グループでは、Panorama の Policies [ポリ シー]および Objects [オブジェクト]タブを使用して、管理対象ファイア ウォールのネットワーク全体のポリシーを管理する階層的な手段を実装 できます。デバイス グループを最大 4 レベルのツリー階層でネストでき ます。子孫グループは、先祖グループおよび共有場所のポリシーおよび

Panorama n	の意味
	オブジェクトを自動的に継承します。Panorama > Device Groups(デバ イス グループ)の順に選択します。
管理対象コレクタ	ログコレクタを管理できます。Panoramaを使用してログコレクタを 設定するため、ログコレクタのことを管理対象コレクタと呼ぶことも あります。管理対象コレクタは、Panorama 管理サーバー(Panorama モードの M-Series アプライアンスまたは Panorama バーチャル アプ ライアンス)にローカルに存在できるほか、専用ログコレクタ(ロ グコレクタ モードの M-Series アプライアンス)とすることができま す。[Panorama] > [管理対象コレクタ] の順に選択します。
	専用ログ コレクタのソフトウェア更新をインストールすることもできま す。
	Panorama 管理サーバーを専用ログ コレクタに変換することができます。
コレクタ グループ	コレクタ グループを管理できます。コレクタ グループはログ コレクタ を論理的にグループ化するため、設定の適用やファイアウォールの割り 当てを一括で行うことができます。Panorama はログをログ コレクタ内 のすべてのディスクおよびコレクタ グループ内のすべてのメンバーに均 ーに分散します。[Panorama] > [コレクタ グループ] の順に選択します。
プラグイン	VMware NSX など、サードパーティ統合用のプラグインを管理できま すPanorama > VMware NSX の順に選択します。
VMware NSX	NSX Manager と Panorama 間の通信を有効にすることで、VM-Series ファイアウォールのプロビジョニングを自動化できます。Panorama > VMware NSX の順に選択します。
証明書の管理	証明書、証明書プロファイル、鍵を設定および管理できます。「ファイ アウォールおよび Panorama 証明書の管理」を参照してください。
ログ設定	SNMP(Simple Network Management Protocol)トラップ レシー バ、Syslog サーバー、電子メール サーバー、および HTTP サーバーにロ グを転送できます。[Device] > [ログ設定] の順に選択します。
サーバー プロファ イル	Panorama にサービスを提供するさまざまなサーバー タイプのプロファ イルを設定できます。以下のいずれかを選択して、特定のサーバー タイ プを設定します。
	 Device > Server Profiles > Email [デバイス > サーバー プロファイル > 電子メール]
	 Device (デバイス) > Server Profiles (サーバー プロファイル) > HTTP

Panorama ページ	の意味	
	 Device > Server Profiles > SNMP Trap [デバイス > サーバー プロファ イル > SNMP トラップ] 	
	 Device > Server Profiles > Syslog [デバイス > サーバー プロファイル > Syslog] 	
	 Device > Server Profiles > RADIUS [デバイス > サーバー プロファイ ル > RADIUS] 	
	 Device > Server Profiles > TACACS+ [デバイス > サーバー プロファイル > TACACS+] 	
	 Device > Server Profiles > LDAP [デバイス > サーバー プロファイル > LDAP] 	
	 Device > Server Profiles > Kerberos [デバイス > サーバー プロファイ ル > Kerberos] 	
	 Device (デバイス) > Server Profiles (サーバー プロファイル) > SAML Identity Provider (SAML アイデンティティ プロバイダ) 	
スケジュールされ た設定のエクス ポート	Panorama とファイアウォールの設定を FTP サーバーや Secure Copy (SCP) サーバーに毎日エクスポートできます。Panorama > Scheduled Config Export (スケジュールされた設定のエクスポート)の 順に選択します。	
software	Panorama ソフトウェアを更新できます。[Panorama] > [ソフトウェア] の順に選択します。	
ダイナミック更新	最新のアプリケーション定義や、アンチウイルス シグネチャ(脅威阻 止ライセンスが必要)などの新しいセキュリティ上の脅威に関する情報 を表示し、新しい定義で Panorama を更新できます。[Device] >[ダイナ ミック更新] の順に選択します。	
support	Palo Alto Networks社の製品およびセキュリティ警告にアクセスできます。Device(デバイス) > Support(サポート)の順に選択します。	
デバイスのデプロ イ	ファイアウォールやログ コレクタにソフトウェアやコンテンツの更新を デプロイできます。Panorama > Device Deployment(デバイスのデプロ イ)の順に選択します。	
マスターキーおよ び診断	Panoramaで秘密鍵を暗号化するためのマスターキーを指定できます。デフォルトでは、新しいマスター キーを指定しなくても、Panorama は秘密鍵を暗号化形式で保管します。Device(デバイス) > Master Key and Diagnostics(マスター キーおよび診断)の順に選択します。	

コンテキスト切り替え

各 Panorama Web インターフェイス ページのヘッダーで、左側のメニューの上にある Context (コンテキスト)のドロップダウンリストから、Panorama Web インターフェイスと ファイアウォール Web インターフェイスを切り替えることができます。ファイアウォールを選 択するとWeb インターフェイスが更新され、選択したファイアウォールのすべてのページとオ プションが表示されるので、ローカルで管理を行うことができます。ドロップダウンリストに は、管理アクセス権のあるファイアウォール(Panorama > Access Domains(アクセスドメイ ン)を参照)のうち、Panorama に接続されているファイアウォールのみが表示されます。

フィルタを使用すると、プラットフォーム(モデル)、デバイス グループ、テンプレート、タ グ、HA 状態ごとにファイアウォールを検索できます。フィルタ バーにテキスト文字列を入力し て、デバイス名ごとに検索することもできます。

高可用性 (HA) モードにあるファイアウォールのアイコンは、HA 状態を示す色付きの背景で表示されます。

Panorama のコミット操作

Web インターフェイスの右上にある **Commit**(コミット)をクリックし、Panorama 設定の保留 中の変更や、Panorama がファイアウォール、ログ コレクタ、WildFire クラスタおよびアプライ アンスにプッシュする変更の操作を選択します。

- Commit (コミット) > Commit to Panorama (Panorama にコミット) Panorama 管理 サーバーの設定で行った変更をアクティベーションします。また、このアクションでは、デ バイス グループ、テンプレート、コレクタ グループ、WildFire クラスタおよびアプライア ンスの変更をファイアウォール、ログ コレクタ、WildFire クラスタおよびアプライアンスに プッシュすることなく Panorama 設定にコミットします。Panorama 設定にのみコミットする ことで、ファイアウォール、ログ コレクタ、WildFire クラスタおよびアプライアンスでまだ アクティベーションの準備ができていない変更を保存できます。
 - Panorama 8.0 以降のリリースでは、設定を管理対象デバイスにプッシュすると、実行中の設定(Panorama にコミットされた設定)がプッシュされます。Panorama 7.1 以前のリリースでは、コミットされていない変更が含まれる候補設定がプッシュされます。そのため、Panorama 8.0 以降のリリースでは、最初に変更を Panorama にコミットしないと、管理対象デバイスに変更をプッシュできません。
- Commit(コミット) > Push to Devices(デバイスにプッシュ) Panorama の実行中の設定 をデバイス グループ、テンプレート、コレクタ グループ、WildFire クラスタおよびアプライ アンスにプッシュします。
- Commit (コミット) > Commit and Push (コミットしてプッシュ) すべての設定変更を ローカルの Panorama 設定にコミットしてから、Panorama の実行中の設定をデバイス グ ループ、テンプレート、コレクタ グループ、WildFire クラスタおよびアプライアンスにプッ シュします。

保留中の変更を管理者または場所でフィルタリングし、それらの変更のみをコミット、プッシュ、検証、またはプレビューできます。場所は、特定のデバイス グループ、テンプレート、コレクタ グループ、ログ コレクタ、WildFire アプライアンスおよびクラスタ、共有設定、Panorama 管理サーバーになります。

Auto-Commit (自動コミット)- 自動コミットと呼ばれる自動コミットは、再起動時に Panorama 構成ファイルに含まれる実行構成を Panorama に再適用する PAN-OS 機能です。これはバック グラウンド プロセスであり、自動コミットが完了するまでの時間は、構成の複雑さとサイズに よって異なる場合があります。自動コミットは、検証プロセスがすべての PAN-OS 構成コミッ トに含まれているため、Panorama の再起動後の構成検証の形式としても機能します。

変更をコミットすると、実行中の設定の一部になります。コミットされていない変更は、候補設定の一部になります。Panorama はコミット要求をキューで処理するので、前回のコミットの進行中に新しいコミットを追加することができます。Panorama は追加された順番でコミットを実行しますが、Panorama が追加した自動コミット(FQDN 更新など)を優先的に行います。ただし、管理者が開始したコミットがすでにキューの上限まで追加されている場合、新しいコミットを行う前に、Panorama が保留中のコミットを完了するまで待つ必要があります。タスクマネージャ(全国の)を使用してコミットのキューをクリアしたり、コミットの詳細を確認することができます。設定変更、コミットプロセス、コミット検証、コミットキューの詳細について

はPanoramaのコミット及び検証作業を参照してください。また、候補設定の保存、変更の取り 消し、ローカル設定のインポート、エクスポート、ロードを行うこともできます(Device(デバ イス) > Setup(セットアップ) > Operations(操作))。

以下のオプションを使用して、設定変更のコミット、検証、またはプレビューを行うことができます。

フィールド/ボタン の意味

以下のオプションは、Commit (コミット) > Commit to Panorama (Panorama にコミット) または Commit (コミット) > Commit and Push (コミットしてプッシュ)を選択して Panorama にコミットする場合に適用されます。

すべての変更のコミット	管理権限対象のすべての変更をコミットします(デフォル ト)。このオプションを選択するときに、Panorama がコミッ トする設定変更のスコープを手動でフィルタリングすることは できません。代わりに、ログインに使用しているアカウントに 割り当てられた管理者ロールによって、コミット スコープが 指定されます。
	 Superuser role (スーパーユーザー ロール) – Panorama は すべての管理者の変更をコミットします。
	 Custom role(カスタムロール) – アカウントに割り当て られた管理者ロールプロファイルの権限によってコミッ トスコープが決まります(Panorama > Admin Roles(管 理者ロール))。プロファイルに Commit For Other Admins(他の管理者のコミット)の権限が含まれている場 合、Panorama はすべての管理者が設定した変更をコミット します。管理者ロールプロファイルに Commit For Other Admins(他の管理者のコミット)の権限が含まれていない 場合、Panorama はその管理者の変更のみをコミットし、他 の管理者の変更はコミットしません。
	アクセスドメインを実装している場合、Panorama はそれらの ドメインを自動的に適用して、コミットスコープをフィルタ リングします(「Panorama > Access Domains(アクセスドメ イン)」を参照)。管理ロールに関係なく、Panorama はアカ ウントに割り当てられたアクセスドメインの設定変更のみを コミットします。
指定対象による変更のコ ミット	Panorama がコミットする設定変更のスコープをフィルタリン グします。ログインに使用しているアカウントに割り当てられ た管理ロールによって、フィルタリングオプションが決まり ます。
	 Superuser role(スーパーユーザーロール) – 特定の管理 者による変更や、特定の場所における変更へとコミットス コープを制限できます。

フィールド/ボタン	の意味
	 Custom role (カスタム ロール) – アカウントに割り当 てられた管理者ロール プロファイルの権限によってフィ ルタリング オプションが決まります (Panorama > Admin Roles (管理者ロール))。プロファイルに Commit For Other Admins (他の管理者向けのコミット)の権限が含ま れている場合、特定の管理者による変更や特定の場所にお ける変更に、コミット スコープを制限できます。管理者 ロール プロファイルに Commit For Other Admins (他の 管理者向けのコミット)の権限が含まれていない場合、コ ミット スコープは、本人が特定の場所で加えた変更にしか 制限できません。
	コミット スコープを以下のようにフィルタリングします。
	 Filter by administrator(管理者によるフィルタリング) – 他の管理者の変更をコミットできるロールの場合でも、 デフォルトでコミットスコープに含まれているのは本人 の変更のみです。コミットスコープに他の管理者を追加す るには<usernames>リンクをクリックし、管理者を選択し て、OKをクリックします。</usernames>
	 Filter by location(場所によるフィルタリング) – 変更の特定の場所を選択して、Include in Commit(コミットに含める)を有効にします。
	アクセスドメインを実装している場合、Panorama はそれらの ドメインに基づいてコミットスコープを自動的にフィルタリ ングします(「Panorama > Access Domains(アクセスドメイ ン)」を参照)。管理ロールやフィルタリングの選択に関係な く、コミットスコープにはアカウントに割り当てられたアク セスドメインの設定変更のみが含まれます。
	 設定をロードした(Device(デバイス) > Setup(セットアップ) > Operations(操作)) 後、Commit All Changes(すべての変更のコミット)を行ってください。
	デバイス グループへの変更をコミットする場合、そのデバイ ス グループの同じルールベースのルールを追加、削除、また は順序変更を行ったすべての管理者の変更を含める必要があり ます。
コミット スコープ	コミットする変更を含む場所を一覧表示します。リストに含ま れるのが変更のすべてであるか一部であるかは、複数の要因が 影響します。詳細は、「Commit All Changes(すべての変更の コミット)」および「Commit Changes Made By(指定対象に

フィールド/ボタン	の意味
	よる変更のコミット)」に記載されています。場所の種類は以 下のとおりです。
	 shared-object(共有オブジェクト) – 共有の場所で定義されている設定です。
	 <device-group>:ポリシー規則またはオブジェクトが定義されているデバイス・グループの名前。</device-group>
	 <template> - 設定が定義されているテンプレートまたはテ ンプレート スタックの名前。</template>
	 <log-collector-group> – 設定が定義されている Collector Group の名前。</log-collector-group>
	 <log-collector> – 設定が定義されている Log Collector の名前。</log-collector>
	 <wildfire-appliances> - 設定が定義されている WildFire アプ ライアンスのシリアル番号。</wildfire-appliances>
	 <wildfire-appliance-clusters> - 設定が定義されている WildFire クラスターの名前。</wildfire-appliance-clusters>
場所タイプ	この列では保留中の変更の場所が分類されます。
	• Panorama – Panorama 管理サーバー設定固有の設定。
	 Device Group(デバイス グループ) – 特定のデバイス グ ループで定義されている設定。
	 Template(テンプレート) – 特定のテンプレートまたはテ ンプレート スタックで定義されている設定。
	 Log Collector Group(ログコレクタグループ) – コレクタ グループ設定固有の設定。
	 Log Collector (ログコレクタ) – ログコレクタ設定固有の 設定。
	 WildFire Appliance Clusters (WildFire アプライアンス クラスタ) – WildFire アプライアンス クラスタ設定固有の設定。
	 WildFire Appliances (WildFire アプライアンス) – WildFire アプライアンス固有の設定。
	 Other Changes (その他の変更) – 前述の設定エリア(共有オブジェクトなど)に固有でない設定。
オブジェクト タイプ	構成変更のオブジェクト・タイプを表示します。
	たとえば、ネットワーク プロファイル (Network > Network Profiles) を構成した場合、profiles が表示されます。

フィールド/ボタン	の意味
	アドレス グループ (Objects > Address Groups) を構成する と、address-group が表示されます。
管理者	構成を変更した管理者の名前。
コミットに含める (部分的なコミットのみ)	コミットする変更を選択できます。デフォルトでは、Commit Scope (コミットスコープ)のすべての変更が選択されていま す。この列は、特定の管理者に基づく Commit Changes Made By (指定対象による変更のコミット)を選択しないと表示さ れません。
	♥ 私存国际が、コミットに占める変更に影響する 場合があります。たとえば、オブジェクトの追 加後に、別の管理者がそのオブジェクトを編集 した場合、その別の管理者の変更のコミット は、自身の変更も合わせてコミットしない限り できません。
Group by Type (タイプ別に グループ化)	Commit Scope(コミット スコープ)の設定変更のリストを Location Type(場所タイプ)別にグループにします。
プレビューの変更	Commit Scope (コミットスコープ)で選択した設定を、実行中の設定と比較できるようにします。プレビューウィンドウでは色分けによって詳細が示されます(追加は緑色、変更は黄色、削除は赤色)。
	Web インターフェイスのセクションへの変更を一致させる場合、変更前後の Lines of Context(コンテキストの行)を表示 するようにプレビュー ウィンドウを設定できます。これらは 候補のファイルと、比較対象である実行中の設定から取得され ます。
	プレビュー結果は新しいブラウザ ウィンドウで 表示されるので、ブラウザでポップアップを許 可しておく必要があります。プレビュー ウィン ドウが開かない場合は、ポップアップを許可す る手順についてブラウザのドキュメントを参照 してください。
変更サマリー	変更をコミットする個別の設定を一覧表示します。Change Summary(変更サマリー)のリストでは、各設定の以下の情 報が表示されます。

フィールド/ボタン	の意味
	 Object Name(オブジェクト名) – ポリシー、オブジェクト、ネットワーク設定、またはデバイス設定を識別する名前です。
	 Type (タイプ) – 設定のタイプ (アドレス、セキュリティ ルール、ゾーンなど)です。
	 Location Type(場所タイプ) – 設定が定義されている場所(Device Groups(デバイスグループ)、Templates(テンプレート)、Collector Groups(コレクタグループ)、WildFire Appliances(WildFire アプライアンス)、またはWildfire Appliance Clusters(WildFire アプライアンススクラスタ))を示します。
	 Location(場所) – 設定が定義されているデバイス グループ、テンプレート、コレクタ グループ、WildFire クラスタまたは WildFire アプライアンスの名前。これらの場所で定義されていない設定の列には、Shared(共有)が表示されます。
	• Operations(操作) – 最後のコミット以降、設定に実施された各操作(作成、編集、または削除)を示します。
	 Owner (オーナー) – 設定に直近の変更を加えた管理者です。
	• Will Be Committed(コミット対象) – 設定がコミットに含まれるかどうかを示します。
	 Previous Owners(前回のオーナー) – 直近の変更前に、 設定を変更した管理者です。
	必要に応じて、Group By(グループ化基準)を列名 (Type(タイプ)など)にできます。
コミットの検証	Panorama 設定の構文が正しく、完全な意味を成しているかど うかを検証します。出力には、コミットが表示するであろう エラーや警告が含まれます。これにはルール シャドウイング やアプリケーション依存関係の警告があります。検証プロセス を利用すると、エラーを検出、修正してからコミットできます (実行中の設定は変更されません)。固定のコミット ウィン ドウがあり、エラーなしでコミットを確実に実行したい場合に 便利です。

以下のオプションは、Commit(コミット) > Push to Devices(デバイスにプッシュ)または Commit(コミット) > Commit and Push(コミットしてプッシュ)を選択して設定変更を管 理対象デバイスにプッシュする場合に適用されます。

すべての変更をプッシュ

管理者権限を持つすべての変更をプッシュします (デフォル ト)。このオプションを選択すると、Panorama がプッシュする

フィールド/ボタン	の意味
	設定変更の範囲を手動でフィルタリングすることはできません。代わりに、ログインに使用したアカウントに割り当てられた管理者の役割によって、プッシュ範囲が決まります。
	 Superuser role – Panorama はすべての管理者の変更をプッシュします。
	 Custom role – アカウントに割り当てられた Admin Role プロファイルの特権によってプッシュ スコープが決まります (Panorama > Admin Roles を参照)。プロファイルに Commit For Other Admins への特権が含まれている場合、Panorama はすべての管理者によって構成された変更をプッシュしま す。Admin Role プロファイルに Push For Other Admins へ の権限が含まれていない場合、Panorama は自分の変更のみ をプッシュし、他の管理者の変更はプッシュしません。
	アクセスドメインを実装している場合、Panorama はそれらの ドメインを自動的に適用してプッシュスコープをフィルタリン グします (Panorama > Access Domains を参照)。あなたの管理 役割に関係なく、Panorama は、アカウントに割り当てられた アクセスドメインの設定変更のみをプッシュします。
Push Changes Made By (変 更のプッシュ作成者)	P1anorama がプッシュする構成変更の範囲をフィルター処理 します。ログインに使用しているアカウントに割り当てられた 管理ロールによって、フィルタリングオプションが決まりま す。
	 Superuser role - プッシュ スコープを特定の管理者が行った 変更と特定の場所の変更に制限できます。
	 Custom role(カスタムロール) – アカウントに割り当 てられた管理者ロールプロファイルの権限によってフィ ルタリングオプションが決まります(Panorama > Admin Roles(管理者ロール))。プロファイルに Push For Other Admins への特権が含まれている場合は、プッシュ範囲を特 定の管理者によって構成された変更と特定の場所の変更に 制限できます。Admin Role プロファイルに Push For Other Admins への特権が含まれていない場合は、プッシュ範囲を 特定の場所に加えた変更のみに制限できます。
	プッシュスコープを次のようにフィルター処理します。
	 Filter by administrator – 自分の役割で他の管理者の変更を プッシュできる場合でも、プッシュ スコープには既定で自 分の変更のみが含まれます。プッシュ スコープに他の管理 者を追加するには、<usernames> リンクをクリックし、管 理者を選択して OK をクリックします。</usernames>

フィールド/ボタン	の意味
	 Filter by location – Include in Push への変更の特定の場所を 選択します。 アクセスドメインを実装している場合、Panorama はそれらの ドメインに基づいてプッシュスコープを自動的にフィルタリン グします (Panorama > Access Domains を参照)。管理者の役割 とフィルターの選択に関係なく、プッシュ スコープには、ア カウントに割り当てられたアクセスドメインの構成変更のみ が含まれます。
スコープのプッシュ	 プッシュする変更のある場所を表示します。デフォルトでス コープに含まれる場所は、以下のどのオプションを選択するか によって異なります。 Commit (コミット) > Commit and Push (コミットして プッシュ) – スコープには、Panorama コミットを必要と する変更のあるすべての場所が含まれます。
	 Commit > Push to Devices – スコープには、Panorama の実 行構成と Unof Sync であるエンティティ (firewalls、仮想 システム、Log Collectors、WildFire クラスター、WildFire アプライアンス) に関連付けられているすべての場所が 含まれます (同期状態については、Panorama > Managed Devices > Summary および Panorama > Managed Collectors を参照してください)。
	どちらを選択しても、Panorama は以下で Push Scope (プッ シュ スコープ)をフィルタリングします。
	 Administrators(管理者) – Panorama は、Commit Scope(コミットスコープ)と同じフィルタを適用します (「Commit All Changes(すべての変更のコミット)」ま たは「Commit Changes Made By(指定対象による変更のコ ミット)」を参照)。
	 Access domains (アクセスドメイン) – アクセスドメインを実装している場合、Panorama はそれらのドメインに基づいて Push Scope (プッシュスコープ)を自動的にフィルタリングします(「Panorama > Access Domains (アクセスドメイン)」を参照)。管理ロールやフィルタリングの選択に関係なく、スコープにはアカウントに割り当てられたアクセスドメインの設定変更のみが含まれます。
	デフォルトの場所を受け入れる代わりに、 Push Scope (プッ シュ スコープ)の <mark>選択内容の編集</mark> を行うことができます。
	[Commit(コミット)] > [Push to Devices (デバイスにプッシュ)] を順に選択すると、設定のプッシュをスケジュールできます。

フィールド/ボタン	の意味
場所タイプ	この列では保留中の変更の場所が分類されます。
	 Device Groups(デバイス グループ) – 特定のデバイス グ ループで定義されている設定。
	 Templates (テンプレート) – 特定のテンプレートまたは テンプレート スタックで定義されている設定。
	 Log Collector Groups(ログコレクタグループ) – コレク タグループ設定固有の設定。
	 WildFire Clusters (WildFire クラスタ) – WildFire クラス タ設定固有の設定。
	 WildFire Appliances (WildFire アプライアンス) – WildFire アプライアンス設定固有の設定。
オブジェクト タイプ	構成変更のオブジェクト・タイプを表示します。
	たとえば、ネットワーク プロファイル (Network > Network Profiles) を構成した場合、profiles が表示されます。アドレ ス グループ (Objects > Address Groups) を構成した場合、アド レス グループ が表示されます。
エンティティ	 この列には、各デバイスグループまたはテンプレートのプッシュ操作に含まれるファイアウォール(デバイス名またはシリアル番号別)または仮想システム(名前別)が表示されます。Edit Selectionsは、影響を受ける firewalls または仮想システムのリストを変更して、構成の変更をプッシュします。 ② 変更をコレクタグループにプッシュする場合、操作には、グループのメンバーであるすべてのログコレクタが含まれます(表示されていないログコレクタも対象となります)。
管理者	構成を変更した管理者の名前。
プッシュに含める	プッシュする変更を選択できます。デフォルトでは、Push Scope 内のすべての変更が選択されます。この列は、Push Changes Made By 特定の管理者を選択した場合にのみ表示さ れます。
選択内容の編集	 プッシュ操作に含めるエンティティを選択する場合にクリックします。 デバイス グループとテンプレート ログ コレクタ グループ WildFire アプライアンスおよびクラスタ

フィールド/ボタン	の意味
	Panorama では、まだ Panorama 設定にコミット されていない変更をプッシュすることはできま せん。
デバイス グループとテンプ レート	Edit Selections(選択内容の編集)を行い、Device Groups(デバイス グループ)または Templates(テンプレー ト)を選択して、以下の行のオプションを表示します。
フィルタ	 テンプレート、テンプレートスタック、あるいはデバイスグ ループや関連するファイアウォールやバーチャルシステムのリストから絞り込みを行います。 コミット状態、デバイス状態、タグ、および高可用性(HA) ステータス別に、管理対象ファイアウォールをフィルタリング することもできます。
氏名	プッシュ操作に含めるテンプレート、テンプレート スタッ ク、デバイス グループ、ファイアウォール、あるいは仮想シ ステムを選択します。
最終コミット状態	ファイアウォールおよび仮想システム設定が、テンプレートも しくは Panorama のデバイス グループ設定と同期されている かを示しています。
HA 状態	登録されたファイアウォールの高可用性(HA)状態を示しま す。 • Active [アクティブ] - 正常なトラフィック処理状態 • Passive [パッシブ] - 正常なバックアップ状態 • Initiating [始動中] - ファイアウォールの起動後最大60秒は この状態におかれます • Non-functional [機能停止中] - エラー状態 • Suspended [保留中] - 管理者がファイアウォールをサスペン ドしていることを示します • Tentative [一時的な状態] - アクティブ/アクティブ環境にお けるリンクまたはパスのモニタリングイベント用
変更保留中の (Panorama) コ ミット	選択したファイアウォールおよび仮想システムに変更をプッ シュする前に、Panorama コミットが必要か(yes(はい)) か否か(no(いいえ))を示します。
Preview Changes(変更のプ レビュー)列	Preview Changes(変更のプレビュー)を行って、Push Scope(プッシュ スコープ)で選択した設定と Panorama の実 行中の設定を比較します。Panorama は、Device Groups(デ

フィールド/ボタン	の意味
	バイス グループ)または Templates(テンプレート)タブで 選択したファイアウォールおよび仮想システムの結果のみが 表示されるように出力をフィルタリングします。プレビュー ウィンドウでは色分けによって詳細が示されます(追加は緑 色、変更は黄色、削除は赤色)。
	プレビュー結果は新しいブラウザ ウィンドウで 表示されるので、ブラウザでポップアップを許 可しておく必要があります。プレビュー ウィン ドウが開かない場合は、ポップアップを許可す る手順についてブラウザのドキュメントを参照 してください。
すべて選択	リスト中のすべてのエントリを選択します。
すべての選択を解除	リスト中のすべてのエントリの選択を解除します。
すべて展開	テンプレート、テンプレート スタック、またはデバイス グ ループに割り当てられたファイアウォールおよび仮想システム を表示します。
すべて縮小表示	テンプレート、テンプレートスタック、またはデバイスグルー プのみを表示します(割り当てられたファイアウォールや仮想 システムは表示されません)。
HA ピアのグループ化	高可用性(HA) 設定のピアであるファイアウォールをグルー プ化します。こうすることでリストには、アクティブのファイ アウォール(アクティブ/アクティブ設定ではアクティブ-プラ イマリ)が最初に表示され、パッシブのファイアウォール(ア クティブ/アクティブ設定ではアクティブ-セカンダリ)はかっ こ内に表示されます。これで、HAモードのファイアウォール を簡単に識別できます。共有ポリシーをプッシュする場合に、 個々のピアではなくグループ化されたペアにプッシュできま す。
	 アクティブ/パッシブ環境のHAピアにおいては、 設定内容を同時にプッシュできるよう、両方の ファイアウォールかそれぞれの仮想システムを 同じデバイスグループ、テンプレート、または テンプレートスタックに入れることも検討して みてください。

フィールド/ボタン	の意味
検証	選択したファイアウォールおよび仮想システムにプッシュする 設定を検証する場合にクリックします。タスク マネージャが 自動的に開き、検証の状態が表示されます。
フィルタが選択されていま す	特定のファイアウォールもしくは仮想システムを表示したい 場合は、それらを選択した状態で Filter Selected(選択項目で フィルタ)を選択してください。
候補設定とのマージ	(デフォルトで選択)Panorama からプッシュされた設定変更 を、管理者がターゲットファイアウォール上でローカルに実 装した保留中の設定変更とマージします。プッシュ操作によ り、PAN-OS [®] がトリガーされて、マージされた変更がコミッ トされます。この選択を解除すると、ファイアウォールの候補 設定がコミットから除かれます。
	 ファイアウォール管理者にファイアウォール上 でローカルに変更をコミットすることを許可し ていて、Panoramaから変更をコミットすると きにそれらの変更を含めない場合は、このオプ ションの選択を解除します。
	また、Panorama から変更をプッシュする前に、ファイア ウォールで設定の監査を行い、ローカルな変更を確認すること を推奨します(「Device(デバイス) > Config Audit(設定監 査)」を参照)。
デバイスおよびネットワー ク テンプレートを含める (Device Groups(デバイス グループ)タブのみ)	(デフォルトで選択)1回の操作でデバイスグループの変更と 関連付けられたテンプレートの変更の両方を選択したファイア ウォールおよび仮想システムにプッシュします。これらの変更 を個別の操作でプッシュする場合は、このオプションを解除し てください。
テンプレートの値を適用	テンプレートまたはテンプレートスタックで定義されている オブジェクトを使用して、すべてのローカル設定を上書きしま す。これには、ローカルに設定されたオブジェクトと、ローカ ルで上書きされた Panorama からプッシュされたオブジェクト が含まれます。オブジェクトがファイアウォールでローカルに 設定されているが、テンプレートまたはテンプレートスタッ クで構成されていない場合、ファイアウォール上で変更され ず、削除されません。この設定はデフォルトで無効になってお り、Panoramaから管理対象ファイアウォールへのプッシュご とに有効(チェック)する必要があります。

フィールド/ボタン	の意味
	 Force Template Values (テンプレートの値を適用)が有効な設定をプッシュする場合、ファイアウォールのオーバーライドされたすべての値がテンプレートの値で上書きされます。このオプションを使用する前にファイアウォールのオーバーライドされた値をチェックし、コミットによって予期せぬネットワークの障害が発生したり、これらのオーバーライドされた値によって問題が生じたりしないことを確認してください。
ログ コレクタ グループ	Edit Selections (選択内容の編集)を行い、プッシュ操作に含める Log Collector Groups (ログコレクタグループ)を選択します。このタブには、以下のオプションが表示されます。
	 Select All(すべて選択) – リスト中のすべてのコレクタ グ ループを選択します。
	 Deselect All (すべての選択を解除) – リスト中のすべての コレクタ グループの選択を解除します。
WildFire アプライアンスお よびクラスタ	Edit Selections (選択内容の編集)を行い、WildFire Appliances and Clusters (WildFire アプライアンスおよびクラ スタ)を選択して、以下のオプションを表示します。
フィルタ	WildFire アプライアンスおよびクラスタのリストをフィルタリ ングします。
氏名	Panorama が変更をプッシュする WildFire アプライアンスおよ びクラスタを選択します。
最終コミット状態	WildFire アプライアンスおよびクラスタ設定が Panorama と同 期しているかどうかを示します。
既定の選択なし	有効 (チェック) を有効にして、既定で選択されているデバイ スを削除して、プッシュ先の特定のデバイスを手動で選択しま す。Panorama がプッシュするデフォルトデバイスは、影響を 受けたデバイスグループとテンプレート設定の変更に基づいて います。

フィールド/ボタン	の意味	
	この設定を有効にすると、デバイスへのプッ シュ(コミット > デバイスへのプッシュ および コミット > コミットとプッシュ)が永続的であ り、設定を有効にした管理者アカウントに固有 です。この設定を1回のプッシュで有効にする と、この設定は無効になるまで、以降のすべて のプッシュで有効になります。	
デバイス グループのプッ シュの検証	Push Scope(プッシュ スコープ)リストでデバイス グループ にプッシュする設定を検証します。タスク マネージャが自動 的に開き、検証の状態が表示されます。	
テンプレートのプッシュの 検証	Push Scope(プッシュ スコープ)リストでテンプレートに プッシュする設定を検証します。タスク マネージャが自動的 に開き、検証の状態が表示されます。	
場所タイプ別グループ	Location Type(場所タイプ)を使用して Push Scope(プッ シュ スコープ)リストをグループ化する場合に選択します。	
以下のオプションは、Panorama 設定をコミットする場合、または変更をデバイスにプッシュ する場合に適用されます。		
の意味	他の管理者が変更内容を理解するのに役立つ説明(最大 512 文字)を入力します。	
	コミットイベントのシステム ログでは、512 文 字を超える説明は切り捨てられます。	
Commit (コミット) / Push (プッシュ) /Commit and Push (コミットして プッシュ)	コミットを開始したり、他のコミットが保留中の場合にコミッ ト要求をコミット キューに追加したりします。	

Panorama でのポリシーの定義

Panorama[™]のDevice Groups(デバイス グループ)を使用すると、ファイアウォール ポリシー を一元的に管理できます。Panorama 上に定義されるポリシーは、プレ ルールまたはポスト ルールとして作成されます。プレ ルールとポスト ルールにより、階層的な方法でポリシーを実 装できます。

共有コンテクストのプレルールとポストルールは、共有コンテクストですべての管理対象ファ イアウォールの共有ポリシーとして、またはデバイス グループ コンテクストで特定のデバイス グループ用として定義できます。プレルールとポスト ルールは Panorama で定義を行った後に 管理対象デバイスにプッシュされるため、管理対象ファイアウォールでルールの表示はできます が、編集は Panorama でしか行えません。

- Pre Rules[プレルール] ルール順序の先頭に追加され、最初に評価されるルールです。プレルールを使用すれば、組織の利用規約に対する遵守を徹底させることができます。例えば、プレルールによって特定の URL カテゴリへのアクセスをブロックしたり、すべてのユーザーの DNS トラフィックを許可することができます。
- Post Rules (ポストルール) ルール順序の末尾に追加され、プレルールとファイアウォー ルでローカルに定義されているルールの後に評価されるルールです。通常、ポストルールに は、App-ID[™]、User-ID[™]、またはサービスに基づいてトラフィックへのアクセスを拒否する ルールが含まれます。
- Default Rules (デフォルト ルール) プレ ルール、ポスト ルール、ローカル ファイア ウォール ルールのいずれとも一致しないトラフィックをファイアウォールで処理する方法を 指定するルールです。これらのルールは、事前定義済みの Panorama 設定の一部です。これ らのルールで選択した設定を Override (オーバーライド)して編集を有効にするには、「セ キュリティ ルールのオーバーライドまたは取り消し」を参照してください。

Preview Rules(ルールのプレビュー)をクリックして、ルールを管理対象ファイアウォールに プッシュする前に、すべてのルールのリストを表示することができます。大量のルールに目を通 しやすいように、各ルールベース内でルールの階層がデバイスグループ(および管理対象ファイ アウォール)ごとに視覚的に区別されて表示されます。

新しいルールを追加する際、ルールの静的な運用データが表示されます。UUID(Universally Unique Identifier)列にはルールの 36 文字の UUID が表示されます。ファイアウォールはルー ル毎に UUID を生成します。しかし、ルールを Panorama からプッシュ送信している場合、同じ UUID を持つこれらのルールも Combined Rules Preview (複合ルールのプレビュー)に表示され ます。Created (作成済み)列には、ルールをルールベースに追加した日時が表示されます。さら に、ルールを最後に編集した日時がModified (編集日時)列に表示されます。PAN-OS 9.0 にアッ プグレードする前にポリシールールが作成された場合、First Hit (最初のヒット)のデータを使用 してCreated (作成)日が決定されます。対象のルールで利用できるFirst Hit (最初のヒット)のデー タがない場合、ファイアウォールあるいは Panorama の管理サーバーが PAN-OS 9.0 にアップグ

ルールの追加または編集を Panorama で行うと、対象タブが表示されます。このタブを使用 して、ルールが定義されている Device Group(デバイス グループ)(または共有の場所)の 特定のファイアウォールまたは子孫デバイス グループにルールを適用できます。Target(対 象)タブでは Any(すべて)(デフォルト)を選択でき、ルールはすべてのファイアウォー ルと子孫デバイス グループに適用されます。特定のファイアウォールまたはデバイス グルー プを対象にするには、Any(すべて)を選択解除してファイアウォールまたはデバイス グルー プを名前ごとに選択します。特定のファイアウォールまたはデバイス グループを除外するに は、Any(すべて)を選択解除して、指定のファイアウォールとデバイス グループを名前ごと に選択し、Target to all but these specified devices(指定したデバイスを除くすべてを対象にす る)を選択します。デバイス グループとファイアウォールのリストが長い場合は、フィルタを 適用して、属性(プラットフォームなど)ごとに、または名前と一致する文字列ごとに、エント リを検索できます。

Panorama でルールを正常に追加してプッシュすると、Rule Usage(ルールの使用状況)で、 ルールがデバイス グループ内のすべてのデバイスで Used(使用)されているか、デバイスグ ループ内の一部のデバイスによって Partially Used(部分的に使用)されているか、またはデバ イスグループ内のデバイスによって Unused(使用されていない)かが表示されます。Panorama は、Policy Rule Hit Count(ポリシー ルール ヒット数)(デフォルトで有効)で管理されたファ イアウォールに基づいてルールの使用状況を判断します。Panorama コンテクストでは、デバイ ス グループ全体の共有ポリシー ルールの、ルールの使用状況を表示できます。さらに、コンテ クストを個々のデバイス グループに変更し、デバイス グループ内のすべてのデバイスでのポリ シー ルールの合計使用状況を表示することもできます。Preview Rules (ルールのプレビュー)で は、該当のデバイス グループの各ポリシー ルールの Hit Count (ヒット数)、Last Hit (最後のヒッ ト)、First Hit (最初のヒット)が表示されます。総トラフィック ヒット数、および最初と最後の ヒットのタイムスタンプは、再起動、アップグレード、およびデータプレーンの再起動イベント を通じて維持されます。「Monitor Policy Rule Usage(ポリシー ルール使用状況のモニター)」 を参照してください。

Group Rules by Tag (タグに基づいてルールをグループ化)してタグを適用することでポリシー ルールのようにグループ化することで、ルールの機能に対する可視性を高め、ルールベース全体 にかけてポリシールールを管理しやすくなります。タグに基づいてグループ化されたルールはタ ググループのリストを表示しますが、ルールの優先順位リストを維持します。ルールをタググ ループの最後に追加したり、ルールを別のタググループに移動したり、タググループ内のルー ルにタグを追加したり、グループタグを使ってフィルタリングや検索を行ったりできます。

ポリシールールに対する変更を追跡するには、変更の内容およびルールを作成あるいは編集した 理由を示すAudit Comment (監査コメント)を追加します。監査コメントを入力し、設定変更をコ ミットしたら、監査コメントがAudit Comment Archive (監査コメント アーカイブ)に保存され、 そこで選択したルールの過去の監査コメントをすべて閲覧できるようになります。監査コメント はグローバル検索で検索できます。監査コメント アーカイブは読み取り専用です。

Policies(ポリシー)タブにアクセスできる管理ユーザーは、Webインターフェイスに表示されるポリシー ルールを PDF/CSV 形式でエクスポートできます。Export Configuration Table Data (設定バンドルデータのエクスポート)を参照してください。

ポリシーを作成するには、各ルールベースの関連するセクションを表示します。

- Policies > NAT [ポリシー > NAT]
- Policies > QoS [ポリシー > QoS]
- Policies > Policy Based Forwarding [ϑ] ϑ > ϑ +
- Policies > Decryption [ポリシー > 復号化]
- ポリシー>ネットワークパケットブローカー

- Policies (ポリシー) > Tunnel Inspection (トンネル検査)
- Policies > Application Override [""" lightarrow "" lig
- Policies (ポリシー) > Authentication (認証)
- Policies > DoS Protection [ポリシー > DoS プロテクション]
- Policies > SD-WAN [ポリシー > SD-WAN]
レガシー モードの Panorama バーチャル アプライアン スのログ ストレージ パーティション

• Panorama > Setup > Operations [Panorama > セットアップ > 操作]

デフォルトでは、レガシー モードの Panorama バーチャル アプライアンスには、すべてのデー タ用に 1 つのディスク パーティションがあり、10.89GB がログ ストレージに割り当てられてい ます。ディスク サイズを拡大しても、ログ ストレージ容量は拡大しません。次のオプションを 使用して、ログ ストレージ容量を変更してください。

- ネットワークファイルシステム(NFS) NFS ストレージをマウントするオプションを使用できるのは、レガシー モードになっていて VMware ESXi サーバーで動作する Panorama バーチャル アプライアンスのみです。NFS ストレージをマウントするには、Miscellaneous(その他)セクションで Storage Partition Setup(ストレージパーティションの設定)を選択して Storage Partition(ストレージパーティション)を NFS V3 に設定し、Table(表)の説明に従って設定を構成します。NFS Storage Settings(NFS ストレージ設定)。
- デフォルト内部ストレージ デフォルトの内部ストレージパーティションに戻します(ESXi サーバーまたは vCloud Air プラットフォームの Panorama で、別の仮想ログ ディスクを以 前設定したか、NFS にマウントした場合にのみ該当)。デフォルトの内部ストレージパー ティションに戻すには、Miscellaneous(その他)セクションで Storage Partition Setup(ス トレージパーティションの設定)を選択し、Storage Partition(ストレージパーティショ ン)を Internal (内部)に設定します。
- 仮想ログディスク VMware ESXi バージョン 5.5 以降で動作している Panorama、または VMware vCloud Air プラットフォームで動作している Panorama では、別の仮想ディスクを 追加できます(8TB まで)。ただし、Panorama では元のディスクでデフォルトの 10.89GB ログストレージの使用が停止され、既存のログはすべて新しいディスクにコピーされます (ESXi の以前のバージョンでは、2TB までの仮想ディスクのみがサポートされます)。
 - ストレージパーティション設定を変更したら、Panorama を再起動する必要があります。Panorama > Setup(セットアップ) > Operations(操作)を選択して Reboot Panorama(Panoramaの再起動)を選択してください。

Panorama モードの Panorama バーチャル アプライアンスまたは M-Series アプラ イアンスでは、NFS ストレージを使用できません。

表 **1**:表:NFS ストレージ設定

Panorama スト レージ パーティ ションの設定 - NFS V3	の意味
SERVER	NFSサーバーのFQDNまたはIPアドレスを指定します。

Panorama スト レージ パーティ ションの設定 - NFS V3	の意味
ログディレク トリ	ログが保管されるディレクトリの完全パス名を指定します。
PROTOCOL	NFSサーバーとの通信に使用するプロトコル(UDPまたはTCP)を指定します。
ポート	NFSサーバーとの通信に使用するポートを指定します。
読み取りサイズ	NFS が読み取り可能な最大バイト数(範囲は 256 ~ 32,768)を指定します。
書き込みサイズ	NFS が書き込み可能な最大バイト数(範囲は 256 ~ 32,768)を指定します。
セットアップ時 にコピー	Panorama デバイスの起動時に NFS パーティションをマウントし、既存の ログをすべてサーバー上の宛先ディレクトリにコピーする場合に選択しま す。
ロギングパー ティションのテ スト	NFS パーティションのマウントのテストを実行し、成功メッセージまたは 失敗メッセージを確認する場合に選択します。

Panorama > Setup (セットアップ) > Interfaces (イン ターフェイス)

Panorama > Setup (セットアップ) > Interfaces (インターフェイス)

Panorama が使用するインターフェイスを設定する場合に、Panorama > Setup(セットアップ) > Interfaces (インターフェイス)を選択します。これにより、ファイアウォールとログ コレ クタの管理、ソフトウェアおよびコンテンツ更新のファイアウォールとログ コレクタへの適 用、ファイアウォールからのログ収集、コレクタ グループとの通信ができます。デフォルト では、Panorama は、ファイアウォールとログ コレクタとのすべての通信に管理(MGT)イン ターフェイスを使用します。



MGT インターフェイスのトラフィックを低減するには、更新の適用、ログ収集、 コレクタ グループ通信のための別のインターフェイスを設定します。ログトラ フィックの負荷が高い環境の場合、ログ収集用に複数のインターフェイスを設定で きます。また、管理トラフィックのセキュリティを向上するには、MGT インター フェイス用に、他のインターフェイスのサブネットよりも秘密性の高い個別のサブ ネット(IPv4 ネットマスクまたは IPv6 プレフィックス長)を定義できます。

インターフェイス	最高速 度	M-700 アプラ イアン ス	M-600 アプラ イアン ス	M-500 ア プライ アンス	M-300 アプラ イアン ス	M-200 ア プライ アンス	Panorama バー チャル アプライ アンス
管理(MGT)	1Gbps	1	1	1	1	1	~
イーサネッ ト1 (Eth1)	1Gbps	~	~	~	~	~	✓
イーサネッ ト2(Eth2)	1Gbps	_	~	~	_	~	~
イーサネッ ト3(Eth3)	1Gbps	_	~	~	_	~	~
イーサネッ ト4(Eth4)	10Gbps	_	~	~	_	_	~
イーサネッ ト5(Eth5)	10Gbps	_	~	~	_	_	~

すべての M-Series アプライアンス モデルのロギング レートを確認します。以下にリストされた ロギング レートを達成するには、M-Series アプライアンスがコレクタ グループ内の単一のログ コレクタである必要があり、M-Series モデルのすべてのロギング ディスクをインストールする 必要があります。例えば、M-500 アプライアンスで 30,000 ログ/秒を達成するには、1TB または 2TB のディスクで 12 のロギング ディスクすべてをインストールする必要があります。

モデルの能力お よび機能	M-700 アプ ライアンス	M-600 アプ ライアンス	<mark>M-500</mark> アプラ イアンス	M-300 アプ ライアンス	<mark>M-200</mark> アプラ イアンス
管理専用モード での Panorama の最大ロギング レート	ローカル ログ	ストレージはサ	+ポートされてい	いません	
Panorama モードでの Panorama の最 大ロギング レー ト	36,500 ロ グ/秒	25,000 ロ グ/秒	20,000 ロ グ/秒	16,500 ロ グ/秒	10,000 ロ グ/秒
ログコレク タモードでの Panorama の最 大ロギングレー ト	73,000 ロ グ/秒	50,000 ロ グ/秒	30,000 ロ グ/秒	33,000 ロ グ/秒	28,000 ロ グ/秒
アプライアンス 上の最大ログ保 存容量	48TB(12 個の 8TB RAID ディス ク)	48TB(12 個の 8TB RAID ディス ク)	 24TB (24 個の 2TB RAID ディス ク) 12TB (24 個の 1TB RAID ディス ク) 	16TB(4 個 の 8TB RAID ディスク)	16TB(4 個 の 8TB RAID ディスク)
アプライアンス 上のデフォルト ログ保存容量	16TB(4 個 の 8TB RAID ディスク)	16TB(4 個 の 8TB RAID ディスク)	4TB(4 個 の 2TB RAID ディスク)	16TB(4 個 の 8TB RAID ディスク)	16TB(4 個 の 8TB RAID ディスク)
アプライアンス 上の SSD 容量 (M-Series アプ ライアンスが生 成するログに使 用)	240GB	240GB	240GB	240GB	240GB

Panorama Web インターフェイス

モデルの能力お	M-700 アプ	M-600 アプ	M-500 アプラ	M-300 アプ	M-200 アプラ
よび機能	ライアンス	ライアンス	イアンス	ライアンス	イアンス
NFSを伴うログ ストレージ	利用不可				

インターフェイスを設定するには、インターフェイス名をクリックして、以下の表に記載されて いるように設定します。

常に、MGT インターフェイスの IP アドレス、ネットマスク(IPv4 の場合)または プレフィックス長(IPv6 の場合)、デフォルト ゲートウェイを指定してください。 設定の一部の値が省略された場合(デフォルト ゲートウェイなど)、以降の設定 変更ではコンソール ポート経由でしか Panorama にアクセスできなくなります。3 つの設定すべてを指定するまで、他のインターフェイスの設定はコミットできませ ん。この要件は、DHCP のみがインターフェイスをサポートするため、でサポート されるクラウド ハイパーバイザー 上の Panorama 仮想アプライアンスには適用され ません。

インターフェイス設 定	の意味
Eth1/Eth2/Eth3/ Eth4/Eth5	インターフェイスを有効にして設定する必要があります。MGT イン ターフェイスは例外で、これはデフォルトで有効になっています。
Public IP Address (パ ブリックIPアドレス)	ファイアウォールがプライベートIPアドレス (NAT) に変換されたパブ リックIPアドレスを使用して Panorama に接続する場合は、インター フェイスにパブリックIPアドレスを入力します。
IPアドレス (IPv4)	ネットワークで IPv4 アドレスを使用する場合、IPv4 アドレスをイン ターフェースに割り当てます。
ネットマスク (IPv4)	IPv4 アドレスをインターフェイスに割り当てた場合は、ネットワーク マスク(例: 255.255.255.0)を入力する必要もあります。
デフォルト ゲート ウェイ(IPv4)	IPv4 アドレスをインターフェイスに割り当てた場合は、デフォルト ゲートウェイにも IPv4 アドレスを割り当てる必要があります(ゲー トウェイはインターフェイスと同じサブネット上にある必要がありま す)。
IPv6 アドレス/プレ フィックス長	ネットワークで IPv6 アドレスを使用する場合、IPv6 アドレスをイン ターフェースに割り当てます。ネットマスクを示すには、IPv6 プレ フィックス長を入力します(例: 2001:400:f00::1/64)。

インターフェイス設 定	の意味
	 IPv6 アドレスは、プライベート クラウド環境 (ESXi、vCloud Air、KVM、または Hyper-V) に展開された すべての M-Series アプライアンスおよび Panorama バー チャル アプライアンスの MGT インターフェイスでサ ポートされています。パブリック クラウド環境 (Amazon Web Service (AWS)、AWS GovCloud、Microsoft Azure、 または Google Cloud Platform) に展開された Panorama バーチャル アプライアンスの MGT インターフェイスで は、IPv6 アドレスはサポートされていません。
デフォルト IPv6 ゲートウェイ	IPv6 アドレスをインターフェイスに割り当てた場合は、デフォルト ゲートウェイにも IPv6 アドレスを割り当てる必要があります(ゲー トウェイはインターフェイスと同じサブネット上にある必要がありま す)。
	IPv6 アドレスは、プライベート クラウド環境 (ESXi、vCloud Air、KVM、または Hyper-V) に展開された すべての M-Series アプライアンスおよび Panorama バー チャル アプライアンスの MGT インターフェイスでサ ポートされています。パブリック クラウド環境 (Amazon Web Service (AWS)、AWS GovCloud、Microsoft Azure、 または Google Cloud Platform) に展開された Panorama バーチャル アプライアンスの MGT インターフェイスで は、IPv6 アドレスはサポートされていません。
速度	 インターフェイスの速度を、フルデュプレックスまたはハーフデュプレックスの10Mbps、100Mbps、1Gbps、または10Gbps(Eth4 およびEth5 のみ)に設定します。Panorama にインターフェイス速度を決定させるには、デフォルトのオートネゴシエート設定を使用します。 この設定は、隣接するネットワーク機器のインターフェイス設定と一致させる必要があります。設定を確実に一致させるには、オートネゴシエートを選択します(隣接する機器がこのオプションをサポートする場合)。
MTU	このインターフェイスで送信されるパケットの最大転送単位(MTU) をバイト数で入力します(範囲は 576 ~ 1,500、デフォルトは 1,500)。
デバイス管理および デバイス ログ収集	ファイアウォールとログ コレクタの管理と、それらのログの収集をイ ンターフェイスで有効にします(デフォルトでは MGT インターフェ

インターフェイス設 定	の意味
	イスで有効)。複数のインターフェイスでこれらの機能の実施を有効 にできます。
コレクタ グループ 通信	インターフェイスでコレクタ グループ通信を有効にします(デフォル トは MGT インターフェイス)。この機能を実施できるインターフェ イスは 1 つのみです。
Syslog Forwarding Syslog の転送	Syslog を転送するインターフェースを有効にします(デフォルトは MGT インターフェイス)。この機能を実施できるインターフェイスは 1 つのみです。
デバイスのデプロイ	ファイアウォールとログ コレクタに対するソフトウェアおよびコン テンツ更新の適用をインターフェイスで有効にします(デフォルトは MGT インターフェイス)。この機能を実施できるインターフェイスは 1つのみです。
管理サービスの管理	 HTTP – Panorama Web インターフェイスへのアクセスを有効にします。HTTPはプレーンテキストを使用しますが、HTTPSよりは機密性が劣ります。 インターフェイス上の管理トラフィックには、HTTPの代わりに HTTPSを有効化してください。 Telnet – Panorama CLI へのアクセスを有効にします。Telnetはプレーンテキストを使用しますが、SSHよりは機密性が劣ります。 HTTPS – Panorama Web インターフェイスへの安全なアクセスを有効にします。 インターフェイス上の管理トラフィックには、Telnetの代わりに SSH を有効化してください。 SSH – Panorama CLI への安全なアクセスを有効にします。
ネットワーク接続性 サービス	 Ping サービスはどのインターフェイスでも使用できます。Panorama インターフェイスと外部サービス間の接続テストに Ping を使用でき ます。高可用性(HA) 配置の場合、HAピアはpingを使用してハート ビートのバックアップ情報を交換します。 次のサービスを使用できるのは、MGT インターフェイスのみです。 SNMP - Panorama が SNMP マネージャからの統計クエリを処理で きるようにします。詳細は、「SNMP モニタリングの有効化」を参 照してください。 User-ID - Panorama が User-ID エージェントから受信したユー ザーマッピング情報を再配信できるようにします。

Panorama Web インターフェイス

インターフェイス設 定	の意味
アクセス許可IPアド レス	このインターフェイスの Panorama に管理者がアクセスする際の IP ア ドレスを入力します。空のリスト(デフォルト)は、どの IP アドレス からもアクセスできることを示します。
	 このリストを空白のままにしないでください。不正アク セスを防ぐために、Panorama 管理者(のみ)の IP アド レスを指定します。

Panorama > High Availability [Panorama > 高可用性]

Panorama の高可用性(HA)を有効にするには、以下の表の説明に従って設定を指定します。

Panorama HA 設定	の意味	
セットアップ 編集 (をクリックして、以下	「の設定を行います。	_
Enable HA	HA を有効にする場合に選択します。	
ピア HA IP アドレス	ピアのMGTインターフェイスのIPアドレスを入力します。	
暗号化を有効	 MGT インターフェイスが有効になると、HA ピア間の通信が暗号化されます。暗号化を有効化する前に、それぞれのHAピアからHAキーをエクスポートし、もう一方のピアヘインポートしてください。Panorama > Certificate Management(証明書の管理) > Certificates(証明書)ページで HA キーをインポートおよびエクスポートします(「ファイアウォールおよび Panorama 証明書の管理」を参照)。 ● HA の接続は、暗号化が有効になっている場合は TCP ポート 28 を使用し、暗号化が有効になっていない場合は TCP ポート 28769 を使用します。 	
ホールド タイムの モニター (ミリ秒)	制御リンク障害に反応するまでにシステムが待機する時間(ミリ秒) を入力します(範囲は 1,000 ~ 60,000、デフォルトは 3,000)。	_

選択設定

編集

(

をクリックして、以下の設定を行います。

優先順位	この設定を行うことで、ファイアウォールのログを主となって受信
(Panoramaバー チャルアプライア ンスで必要になりま	するピア(プライマリ)が決定されます。HAペアでは、一方のデバ イスをPrimary [プライマリ] として割り当て、もう一方のデバイス をSecondary [セカンダリ] として割り当てます。
す)	レガシー モードの Panorama バーチャル アプライアンスのログ スト レージ パーティションを設定する場合、ログ ストレージに内部ディス ク (デフォルト)またはネットワーク ファイル システム (NFS)を使 用できます。NFSを設定した場合、プライマリの受信ピアのみがファ

Panorama HA 設定	の意味
	イアウォールのログを受信します。内部ディスクストレージを設定す ると、ファイアウォールはデフォルトでプライマリピアとセカンダリ ピアの両方にログを送信しますが、これはロギングおよびレポート設 定の Only Active Primary Logs to Local Disk(アクティブなプライマリ ログのみをローカルディスクに保存)を有効にして変更できます。
プリエンプティブ	プライマリ Panorama が障害から回復した後にアクティブな動作を再 開できるようにする場合に選択します。無効になっている場合、プラ イマリ Panorama が障害から回復した後も、セカンダリ Panorama が アクティブのまま動作します。
HA タイマー設定	ここでの設定内容は、後述のHA選択設定におけるフェイルオーバーの 速度を左右します。 • Recommended(推奨) – 標準(デフォルト)のフェイルオーバー
	タイマーを設定する場合に選択してください。一連の設定数値を表示する場合はAdvanced [詳細設定] からLoad Recommended [推奨設定の読込] を選択します。
	 Aggressive(アグレッシブ) – 高速のフェイルオーバー タイマー設定の場合に選択します。一連の設定数値を表示する場合はAdvanced [詳細設定] からLoad Agressive [アグレッシブ設定の読込] を選択します。
	• Advanced(詳細設定) – 残りの HA 選択設定を表示し、値をカス タマイズする場合に選択します。
	以下の設定の Recommended (推奨) および Aggressive (アグレッシブ)の値を確認してください。
プロモーション ホールド タイム (ミ リ秒)	プライマリ ピアがダウンしてからセカンダリ Panorama ピアがその役 目を引き継ぐまでに待機する時間をミリ秒単位で入力します(範囲は 0 から 60,000)。推奨(デフォルト)値は2000、アグレッシブの場合 は500です。
Hello Interval (ms)(Hello 間隔 (ミリ秒)	もう一方のピアが動作していることを確認するための hello パケット の送信間隔をミリ秒単位(範囲は 8,000 から 60,000)で入力します。 推奨(デフォルト)の場合もアグレッシブの場合も8000に設定されて います。
ハートビート間隔 (ミリ秒)	Panorama が HA ピアに ICMP ping を送る間隔をミリ秒単位で指定し ます(範囲は 1,000 から 60,000)。推奨(デフォルト)値は2000、 アグレッシブの場合は1000です。
Preemption Hold Time (min)(プリエ	この設定値は Preemptive [プリエンプティブ] を設定した場合にの み適用されます。フェイルオーバーの原因が解決され、パッシブな Panorama ピアがアクティブな状態に復帰する前に待機する時間を分

Panorama HA 設定	の意味
ンプション ホール ド タイム(分))	単位で入力します(範囲は1から60)。推奨(デフォルト)の場合も アグレッシブの場合も1に設定されています。
モニター障害時ホー ルド アップ タイム (ミリ秒)	パス モニターの障害後、Panorama がパッシブな状態への復帰を試 行するまでの待機時間をミリ秒単位で指定します(範囲は 0 から 60,000)。この待機中に障害が発生しても、パッシブピアはアクティ ブピアを引き継ぐことができません。待機時間を持たせることで、隣 接するデバイスの偶発的なフラッピングによるフェイルオーバーを回 避することができます。推奨(デフォルト)の場合もアグレッシブの 場合も0に設定されています。
追加のマスター ホールド アップ タ イム (ミリ秒)	優先度の高いピアがアクティブ ピアの役割を引き継ぐ前に、パッ シブ状態を維持する時間をミリ秒単位で指定します(範囲は 0 か ら 60,000)。推奨(デフォルト)値は7000、アグレッシブの場合 は5000です。

パスモニタリング

編集 ()

をクリックして、HA パス モニタリングの設定を行います。

enabled [有効化]	パスのモニタリングを有効化する場合に選択します。パスのモニタリ ングをオンにすると、Panorama は、ICMP pingメッセージを送信して レスポンスがあることを確認することで、指定した宛先IPアドレスを モニターします。
障害条件	モニターしているパスグループのAny[一部]またはAll[すべて]で応答で きない場合にフェイルオーバーを発生させるかどうかを選択します。

パス グループ

HAパスモニタリング用のパスグループを作成する場合は、Add[追加]をクリックし、以下の 項目を入力してください。

氏名	パスグループの名前を指定します。
enabled [有効化]	パス グループを有効にする場合に選択します。
障害条件	指定した宛先アドレスの Any(いずれか)または All(すべて)が応答 できない場合に、エラーを発生させるかどうかを選択します。
Ping 間隔	ICMP エコー メッセージによって宛先 IP アドレスへのパスが有効であることを確認する間隔をミリ秒単位で指定します(範囲は 1,000 ~ 60,000、デフォルトは 5,000)。

Panorama HA 設定	の意味
Ping 数	障害を宣言するまでの ping 試行回数を指定します(範囲は 3 ~ 10、 デフォルトは 3)。
宛先IP	モニターする宛先IPアドレスを1つ以上入力します。複数のアドレスを 入力する場合はコンマで区別してください。

Panorama > Managed WildFire Clusters (管理対象 WildFire クラスタ)

- Panorama > Managed WildFire Clusters (管理対象 WildFire クラスタ)
- Panorama > Managed WildFire Appliances (管理対象 WildFire アプライアンス)

Panorama M-Series またはバーチャル アプライアンスから、クラスタ内にある WildFire アプ ライアンスを管理できます。スタンドアロン アプライアンスとして管理することもできます。 クラスタの管理(Panorama > Managed WildFire Clusters(管理対象 WildFire クラスタ))と スタンドアロン アプライアンスの管理(Panorama > Managed WildFire Appliances(管理対象 WildFire アプライアンス))の管理および設定タスクには共通点が多いため、両方について以 下のトピックにまとめています。

WildFire アプライアンスを Panorama に追加した後、Web インターフェイスでこれらのアプラ イアンスをクラスタに追加してクラスタとして管理したり、スタンドアロン アプライアンスと して管理したりします。

- 管理対象 WildFire クラスタのタスク
- 管理対象 WildFire アプライアンスのタスク
- 管理対象 WildFire の情報
- 管理対象 WildFire クラスタおよびアプライアンスの管理

管理対象 WildFire クラスタのタスク

WildFire アプライアンス クラスタの作成と削除は、Panorama から行うことができます。あるクラスタから別のクラスタに設定をインポートする際、設定にかかる時間を節約することもできます。

タスク	の意味
クラスタの作成	必要に応じて Create Cluster(クラスタの作成)を行い、新しいクラ スタの名前を入力してから OK をクリックします。
	ローカルで設定し、WildFire アプライアンス ノードを個別に追加 して Panorama に追加した既存のクラスタは、WildFire ノードおよ びノードのロールとともにリストされます(Panorama > Managed WildFire Appliances(管理対象 WildFire アプライアンス))。
	クラスタ名は有効なサブドメイン名にする必要があり、小文字または 数字で始めて、ハイフンを使用できますが、ハイフンをクラスタ名の 最初と最後の文字にすることはできず、スペースやその他の文字は使 用できません。クラスタ名の最大文字数は 63 文字です。
	クラスタを作成したら、管理対象 WildFire アプライアンスをクラス タに追加して Panorama で管理できます。WildFire アプライアンスを

タスク	の意味
	Panorama に追加すると、アプライアンスは Panorama に自動的に登 録されます。
	Panorama には最大 10 個の管理対象 WildFire クラスタを作成でき、 各クラスタには 20 個までの WildFire アプライアンス ノードを含め ることができます。Panorama では、総計 200 個のスタンドアロン アプライアンスおよびクラスタ ノードを管理できます。
クラスタ設定のイン ポート	Import Cluster Config (クラスタ設定のインポート) により、既 存のクラスタ設定をインポートします。クラスタを選択してか ら Import Cluster Config (クラスタ設定のインポート) を行う と、Controller (コントローラ) と Cluster (クラスタ) には、選 択したクラスタの適切な情報が自動的に入力されます。Import Cluster Config (クラスタ設定のインポート) の前にクラスタを選 択しない場合は、Controller (コントローラ) を選択する必要があ り、Cluster (クラスタ) には、選択したコントローラ ノードに基づ いて自動的に情報が入力されます。
	設定をインホートしたら、Commit to Panorama(Panorama にコ ミット)により、インポートした候補設定を Panorama の実行中の設 定に保存します。
Panorama から削除	WildFire クラスタを Panorama から管理する必要がなくなった 場合は、Remove From Panorama (Panorama から削除)を実行 し、Yes (はい)を選択してアクションを確定します。クラスタを Panorama の管理から削除した後は、コントローラ ノードからそのク ラスタをローカルで管理できます。クラスタをローカルではなくて再 び中央管理する場合は、そのクラスタを Panorama アプライアンスに いつでも追加しなおすことができます。
WildFire クラスタ ア プライアンスからア プライアンス 通信の 暗号化	クラスター内の WildFire アプライアンス間のデータ通信を暗号化す るには、Secure Cluster Communication で Enable 暗号化を行いま す。
	WildFireは、アプライアンス間の通信に事前定義された証明書または カスタム証明書を使用します。カスタム証明書は、Customize Secure Server Communication を有効にし、Custom Certificate Only を有効 にした場合にのみ使用されます。
	WildFire クラスターが FIPS-CC モードで動作するには、暗号化が必要です。FIPS-CC モードで使用されるカスタム証明書は、FIPS-CC 要件を満たしている必要があります。
	セキュアなクラスター通信を有効にした後、管理対象の WildFire ア プライアンスをクラスターに追加できます。新しく追加されたアプラ イアンスは、セキュア・クラスター通信設定を自動的に使用します。

管理対象 WildFire アプライアンスのタスク

Panorama デバイスでは、スタンドアロン WildFire アプライアンスの追加、削除、管理ができま す。スタンドアロン アプライアンスを追加したら、WildFire アプライアンス クラスタにクラス タ ノードとして追加したり、個別のスタンドアロン アプライアンスとして管理したりすること ができます。

タスク	の意味
アプライアンスの追加	 Add Appliance (アプライアンスの追加)では、1つ以上の WildFire アプライアンスを Panorama アプライアンスに追加して中央管理しま す。各 WildFire アプライアンスのシリアル番号は個別の行(新しい 行)に入力します。Panorama では、合計 200 個までの WildFire クラ スタノードとスタンドアロン WildFire アプライアンスを管理できま す。 Panorama で管理する各 WildFire アプライアンスでは、次の WildFire アプライアンス CLI コマンドを使用して、Panorama アプライアンス (Panorama サーバー)、および必要に応じてバックアップ Panorama サーバーの IP アドレスまたは FQDN を設定します。
	<pre>set deviceconfig system panorama-server <ip-addres fqdn="" s="" =""> set deviceconfig system panorama-server-2 <ip-addr ess="" fqdn="" =""></ip-addr></ip-addres></pre>
設定のインポート	WildFire アプライアンスと Import Config(設定のインポート)を選択 し、そのアプライアンスの実行中の設定(のみ)を Panorama にイン ポートします。
	設定をインポートしたら、 Commit to Panorama (Panorama にコミット)により、インポートした候補設定を Panorama の実行中の設定に保存します。
削除	WildFire アプライアンスを Panorama から管理する必要がなくなった 場合は、アプライアンスを Remove(削除)し、Yes(はい)を選択し てアクションを確定します。アプライアンスを Panorama の管理から 削除した後は、CLIを使用してそのアプライアンスをローカルで管理 できます。アプライアンスをローカルではなくて再び中央管理する場 合は、必要に応じて、そのアプライアンスを Panorama アプライアン スにいつでも追加しなおすことができます。

管理対象 WildFire の情報

管理対象クラスタごとに次の情報を表示するには、Panorama > Managed WildFire Clusters(管理対象 WildFire クラスタ)を選択し(スタンドアロン アプライアンスをこのページから選択

して情報を表示することもできます)、スタンドアロン アプライアンスの情報を表示するに は、Panorama > Managed WildFire Appliances(管理対象 WildFire アプライアンス)を選択し ます。

特筆しない限り、次の表の情報は、WildFire クラスタとスタンドアロン アプライアンスの両方 に適用されます。クラスタまたはアプライアンスで以前に設定した情報は事前に入力されます。

管理対象 WildFire の 情報	の意味
アプライアンス	アプライアンスの名称。
	管理対象 WildFire クラスタ ビューには、クラスタ別に分類されたア プライアンスが表示され、クラスタに追加可能なスタンドアロン ア プライアンスが含まれ、シリアル番号(括弧内)とアプライアンス名 が含まれます(シリアル番号は名前の一部ではありません)。
シリアル番号 (管理対象 WildFire アプライアンス ビューのみ)	アプライアンスのシリアル番号管理対象 WildFire クラスタ ビューに は、アプライアンス名と同じ列にシリアル番号が表示されます(シリ アル番号は名前の一部ではありません)。
ソフトウェア バー ジョン	アプライアンスでインストールされて動作しているソフトウェアの バージョン。
IPアドレス	アプライアンスの IP アドレス。
接続済み	アプライアンスと Panorama の接続状態であり、接続済みまたは切断 のいずれかになります。
クラスタ名	アプライアンスがノードとして組み込まれているクラスタの名前。 スタンドアロン アプライアンスの場合、ここには何も表示されませ ん。
分析環境	分析環境(vm1、vm2、vm3、vm4、vm5)。各分析環境は、一連の オペレーティング システムとアプリケーションを表します。
	 vm-1 では、Windows XP、Adobe Reader 9.3.3、Flash 9、PE、PDF、Office 2003 以前の Office リリースがサポートされます。
	 vm-2 では、Windows XP、Adobe Reader 9.4.0、Flash 10n、PE、PDF、Office 2007 以前の Office リリースがサポートさ れます。
	 vm-3 では、Windows XP、Adobe Reader 11、Flash 11、PE、PDF、Office 2010 以前の Office リリースがサポートされます。

管理対象 WildFire の 情報	の意味
	 vm-4 では、Windows 7 の 32 ビット、Adobe Reader 11、Flash 11、PE、PDF、Office 2010 以前の Office リリースがサポートさ れます。
	 vm-5 では、Windows 7 の64 ビット、Adobe Reader 11、Flash 11、PE、PDF、Office 2010 以前の Office リリースがサポートさ れます。
コンテンツ	コンテンツ リリース バージョンのバージョン番号。
ロール	アプライアンスのロール:
	 Standalone (スタンドアロン) – アプライアンスはクラスタ ノードになっていません。
	 Controller (コントローラ) – アプライアンスはクラスタのコント ローラ ノードです。
	 Controller Backup (コントローラ バックアップ) – アプライアン スはクラスタのコントローラ バックアップ ノードです。
	 Worker (ワーカー) – アプライアンスは、クラスタのワーカー ノードです。
設定状態	アプライアンスの設定の同期状態。Panorama アプライアンスは WildFire アプライアンスの設定を確認し、アプライアンスの設定と Panorama でそのアプライアンス用に保存されている設定との間で設 定の違いをレポートします。
	 In Sync(同期されています) – アプライアンスの設定 は、Panorama で保存されている設定と同期しています。
	 Out of Sync(同期されていません) – アプライアンスの設定 は、Panorama で保存されている設定と同期していません。眼鏡に マウスを合わせると、同期の失敗の原因が表示されます。
クラスタ状態 (管理対象 WildFire クラスタ ページの み)	クラスタ状態には、クラスタノードごとに次の3種類の情報が表示 されます。
	• サービス使用可能(正常な動作状態):
	 wfpc(WildFire プライベート クラウド) – マルウェア サンプ ル分析とレポート サービス。
	 シグネチャ – ローカル シグネチャ生成サービス。

管理対象 WildFire の 情報	の意味
	 操作の進捗状況 – 操作名に続けてコロン(:)と状態が表示されます。
	• 操作 – 使用停止、中断、再起動の操作の状態。
	 進捗状況 – 操作状態の通知は各操作で同じであり、要求、継続 中、拒否、成功、失敗のいずれかになります。
	たとえば、ノードを中断して操作が継続中である場合、クラスタ 状態は suspend:ongoing と表示されます。ノードを再起動し て、操作が要求されたがまだ始まっていない場合、クラスタ状態 は reboot:requested と表示されます。
	 エラー条件:
	クラスタ状態には、次のエラー条件が表示されます。
	 クラスタ – cluster:offline または cluster:splitbrain。
	 サービス – service:suspended または service:none。
最終コミット状態	直近のコミットが成功した場合は Commit succeeded。直近のコ ミットが失敗した場合は commit failed。状態を選択して、前回の コミットに関する詳細を表示してください。
Utilization(使用率)>	View (表示)

ビュー	View クラスターまたはアプライアンスの使用率の統計。個々のアプ ライアンス (Panorama > Managed WildFire Appliances) のみを表示し たり、クラスター統計 (Panorama > Managed WildFire Clusters) のみ を表示できます。
	• A1ppliance-(スタンドアロン アプライアンスの表示のみ) アプライ アンスのシリアル番号。
	 Cluster-(Cluster view only)クラスター名。別のクラスターを選択して表示することもできます。
	• Duration - 統計が収集および表示される期間を表示します。さま ざまな期間を選択できます。
	• 15 Min
	Last Hour
	Last 24 hours (default)
	● 過去 7 日間
	• All

管理対象 WildFire の 情報	の意味
	Utilization View には 4 つのタブがあり、各タブで、構成済みの Duration に基づいて表示する内容を決定します。
General [全般] タブ	General(全般)タブには、クラスタまたはアプライアンスの集約済 みリソース使用率統計が表示されます。その他のタブには、リソース 使用率に関する詳細がファイル タイプ別に表示されます。
	 Total Disk Usage(合計ディスク使用率) – クラスタまたはアプラ イアンスの合計ディスク使用率。
	 Verdict(判定) – 判定の Total(合計)数、ファイルに 割り当てられた各判定タイプの数(Malware(マルウェ ア)、Grayware(グレイウェア)、Benign(安全))、Error(エ ラー)判定だった判定の数。
	 Sample Statistics(サンプル統計) – Submitted(送信済み)と Analyzed(分析済み)のサンプルの合計数、および分析が Pending(保留中)のサンプルの数。
	 Analysis Environment & System Utilization (分析環境とシステム 使用率):
	 File Type Analyzed(分析したファイルタイプ) – 分析 したファイルのタイプ(Executable(実行可能)、Non- Executable(実行可能以外)、Links(リンク))。
	 Virtual Machine Usage(仮想マシン使用率) – 分析された各ファイルタイプに使用された仮想マシンの数、および各ファイルタイプの分析に使用できる仮想マシンの数。たとえば、実行可能ファイルの場合、VM 使用率は 6/10(使用可能 VM 10 個中の VM 6 個)になることがあります。
	 Files Analyzed(分析済みファイル数) – 分析された各タイプのファイルの数。
Executable(実行 可能)タブ、Non- Executable(実 行可能以外)タ ブ、Links(リンク) タブ	Executable (実行可能)、Non-Executable(実行可能以 外)、Links(リンク)には、各ファイル タイプについて同じような 情報が表示されます。
	 Verdict(判定) – ファイルタイプ別の判定に関する詳細。結果は フィルタリングできます。
	 検索ボックス – 検索条件を入力し、判定をフィ ルタリングします。検索ボックスには、リストの ファイル タイプ(項目)の数が表示されます。 検索条件を入力したら、フィルタを適用するか (→ フィルタをクリアして

)、

管理対象 WildFire の 情報	の意味	
	(× 別の一連の条件を入力します。)
	 File Type(ファイルタイプ) – ファイルがタイプ別にリストされます。たとえば、Executable(実行可能)タブには.exeと.dll、Non-Executable(実行可能以外)タブには、.pdf、.jar、.doc、.ppt、.xls、.docx、.pptx、.xlsx、.rtf、class、ンク)タブには elink ファイル タイプの情報が表示されます。 	.swf、 Lin
	 各タブでは、File Type(ファイルタイプ)ごとに、Malware(マルウェア)、Grayware(グレイウェア)、Benign(安全)の判定の合計数、Error(エラー)判定の数、判定のTotal(合計)数が表示されます。 	
	 Sample Statistics(サンプル統計) – ファイル タイプ別のサンプ ル分析に関する詳細。 	
	 検索ボックス – Verdict(判定)の検索ボックスと同じです。 	
	 File Type(ファイル タイプ) – Verdict(判定)の File Type(ファイル タイプ)と同じです。 	
	 各タブでは、File Type(ファイルタイプ)ごとに、分析のために Submitted(送信済み)となったファイルの合計数、Analyzed(分析済み)の合計数、分析が Pending(保留中)の数が表示されます。 	

Firewalls Connected (接続済みファイアウォール) > View (表示)

表示、ビュー	クラスタまたはアプライアンスに接続しているファイアウォール に関する情報を View(表示)します。個別のアプライアンスのみ を表示するか(Panorama > Managed WildFire Appliances(管理対 象 WildFire アプライアンス))、クラスタ統計のみを表示します (Panorama > Managed WildFire Clusters(管理対象 WildFire クラス タ))。
	 Appliance(アプライアンス) – (スタンドアロンアプライアン スの表示のみ)アプライアンスのシリアル番号。
	 Cluster(クラスタ) – (クラスタの表示のみ)クラスタ名。別の クラスタを選択して表示することもできます。
	• Refresh(更新) – 表示を更新します。
Registered(登 録済み)タブ と Submitting Samples(サンプル 送信)タブ	Registered(登録済み)タブには、クラスタまたはアプライアンス に登録されているファイアウォールに関する情報が、そのファイア ウォールがサンプルを送信しているかどうかに関係なく表示されま す。

管理対象 WildFire の 情報	の意味	
	Submitting Samples(サンプル送信)タブには、WildFire クラスタま たはアプライアンスにサンプルをアクティブに送信しているファイア ウォールに関する情報が表示されます。	-
	これらのタブに表示される情報のタイプ、および情報をフィルタリン グする方法は、両方で同じです。	
	 検索ボックス – 検索条件を入力し、ファイアウォー ルのリストをフィルタリングします。検索ボックスに は、リストのファイアウォール(項目)の数が表示さ れます。検索条件を入力したら、フィルタを適用するか (→ フィルタをクリアして (× 別の一連の条件を入力します。 S/N – ファイアウォールのシリアル番号。 IP address(IP アドレス) – ファイアウォールの IP アドレス。 Model(モデル) – ファイアウォールのモデル番号。 Software Version(ソフトウェアバージョン) – ファイアウォー ルでインストールされて動作しているソフトウェアのバージョ ン。)、)

管理対象 WildFire クラスタおよびアプライアンスの管理

Panorama > Managed WildFire Clusters (管理対象 WildFire クラスタ)を選択し、クラスタ を選択して管理するか、WildFire アプライアンスを選択して(Panorama > Managed WildFire Appliances (管理対象 WildFire アプライアンス))スタンドアロン アプライアンスを管理しま す。Panorama > Managed WildFire Cluster (管理対象 WildFire クラスタ)ビューには、クラス タノード (クラスタのメンバーである WildFire アプライアンス)とスタンドアロン アプライア ンスがリストされるため、使用可能なアプライアンスをクラスタに追加できます。クラスタでは ノードを管理するため、クラスタノードを選択すると、限定された管理機能のみが提供されま す。

特筆しない限り、次の表の設定と説明は、WildFire クラスタと WildFire スタンドアロン アプラ イアンスの両方に適用されます。クラスタまたはアプライアンスで設定した情報は事前に入力さ れます。最初に Panorama の情報に変更や追加をコミットしてから、新しい設定をアプライアン スにプッシュする必要があります。



setting	の意味
氏名	クラスタまたはアプライアンスの Name(名前)、またはアプライア ンスのシリアル番号。
DNS の有効化 (WildFire クラスタ のみ)	クラスタの Enable DNS(DNS の有効化)を行います。
ファイアウォールの 登録先	ファイアウォールを登録するドメイン名。wfpc.service. <cluster- name>.<domain> という形式にしてくださ い。たとえば、デフォルトのドメイン名は wfpc.service.mycluster.paloaltonetworks.com です。</domain></cluster-
コンテンツ更新サー バー	Content Update Server(コンテンツ更新サーバー)の場所を入力す るか、デフォルトの wildfire.paloaltonetworks.com を使用 し、クラスタまたはアプライアンスが、コンテンツ配信ネットワーク インフラストラクチャで最も近いサーバーからコンテンツ更新を受信 するようにします。グローバル クラウドに接続すると、ローカルの 脅威の分析のみに依存するのではなく、クラウドに接続したすべての ソースからの脅威分析に基づいて、シグネチャと更新にアクセスでき るようになります。
サーバー アイデン ティティのチェック	証明書の共通名(CN)をサーバーの IP アドレスまたは FQDN と 照合し、更新サーバーのアイデンティティを確認するには、Check Server Identity(サーバー アイデンティティのチェック)を行いま す。
WildFire クラウド サーバー	グローバルの WildFire Cloud Server (WildFire クラ ウド サーバー)の場所を入力するか、デフォルトの wildfire.paloaltonetworks.com を使用し、クラスタまたはア プライアンスが最も近いサーバーに情報を送信できるようにします。 情報を送信するかどうか、およびどのような種類の情報をグローバル クラウド (WildFire Cloud Services (WildFire クラウド サービス)) に送信するかは選択できます。
サンプル分析イメー ジ	クラスタまたはアプライアンスがサンプル分析に使用する VM イメージを選択します(デフォルトは vm-5)。マルウェア テスト ファイル (WildFire API)を取得すると、サンプル分析の結果を確認できます。
WildFire クラウド サービス	クラスタまたはアプライアンスをグローバル WildFire クラウド サー バーに接続すると、Send Analysis Data(分析データの送信)、Send Malicious Samples(有害サンプルの送信)、Send Diagnostics(診 断の送信)をグローバル クラウドに対して行うかどうか、または 3 つの組み合わせのいずれかを選択できます。また、グローバルクラ

setting	の意味
	ウドで Verdict Lookup (判定ルックアップ)を実行するかどうかを 選択することもできます。グローバル クラウドに情報を送信する と、WildFire ユーザーのコミュニティ全体が利益を得ることになりま す。共有情報により、すべてのアプライアンスが有害トラフィックを 特定して、ネットワークを通過することを防止する能力が高まるため です。
サンプル データ保持	安全、グレイウェア、有害のサンプルを保持する日数。
	 Benign/Grayware(安全/グレイウェア)サンプル – 範囲は1~ 90、デフォルトは14です。
	 Malicious(有害)サンプルー最小は1で、最大はありません (無期限)です。デフォルトは無期限です。
分析環境サービス	Environment Networking (環境ネットワーク)では、仮想マシ ンがインターネットと通信できるようになります。Anonymous Networking (匿名ネットワーク)を選択してネットワーク通信を匿 名にすることができますが、Environment Networking (環境ネット ワーク)を選択してから Anonymous Networking (匿名ネットワー ク)を有効にする必要があります。
	ネットワーク環境が異なると、分析する必要があるドキュメント が多いか、分析する必要がある実行可能ファイルが多いかに応じ て、分析負荷のタイプが異なります。優先分析環境を設定すると、 環境のニーズに応じて、Executables(実行可能ファイル)または Documents(ドキュメント)に割り当てるリソースを増やすことがで きます。Default(デフォルト)割り当てでは、Executables(実行可 能ファイル)と Documents(ドキュメント)が均等になります。
	使用可能リソースの量は、クラスタに WildFire ノードがいくつある かによって決まります。
シグネチャ生成	クラスタまたはアプライアンスで、AV、DNS、URL シグネチャまた は3つの組み合わせを選択します。
アプライアンス タブ	J

ホスト名	WildFire アプライアンスのホスト名を入力します。
(スタンドアロン WildFire アプライア ンスのみ)	
Panorama サーバー	アプライアンスの IP アドレスか FQDN、またはクラスタを管理して いるプライマリ Panorama の IP アドレスか FQDN を入力します。

setting	の意味
Panorama サーバー 2	アプライアンスの IP アドレスか FQDN 、またはクラスタを管理して いるバックアップ Panorama の IP アドレスか FQDN を入力します。
ドメイン	アプライアンス クラスタまたはアプライアンスのドメイン名を入力 します。
プライマリDNSサー バー	プライマリ DNS サーバーの IP アドレスを入力します。
セカンダリ DNS サー バー	セカンダリ DNS サーバーの IP アドレスを入力します。
タイムゾーン	クラスタまたはアプライアンスに使用するタイム ゾーンを選択しま す。
緯度 (スタンドアロン WildFire アプライア ンスのみ)	緯度アプライアンスのホスト名を入力します。
経度 (スタンドアロン WildFire アプライア ンスのみ)	経度アプライアンスのホスト名を入力します。
プライマリ NTP サー バー	 プライマリ NTP サーバーの IP アドレスを入力し、認証タイ プを None (なし) (デフォルト)、Symmetric Key (対称 キー)、Autokey (自動キー)のいずれかに設定します。 認証タイプを Symmetric Key (対称キー)に設定すると、さらに 4 つ のフィールドが表示されます。 Key ID (キー ID) - 認証キー ID を入力します。 Algorithm (アルゴリズム) - SHA1 または MD5 への認証アルゴ リズムを設定します。 Authentication Key (認証キー) - 認証キーを入力します。 Confirm Authentication Key (再入力 認証キー) - 認証キー) - 認証キーを確 認のためにもう一度入力します。
セカンダリ NTP サー バー	セカンダリ NTP サーバーの IP アドレスを入力し、認証タイ プを None(なし)(デフォルト)、Symmetric Key(対称 キー)、Autokey(自動キー)のいずれかに設定します。

setting	の意味
	認証タイプを Symmetric Key(対称キー)に設定すると、さらに 4 つのフィールドが表示されます。
	• Key ID(キー ID) – 認証キー ID を入力します。
	 Algorithm(アルゴリズム) – SHA1 または MD5 への認証アルゴ リズムを設定します。
	 Authentication Key(認証キー) – 認証キーを入力します。
	 Confirm Authentication Key(再入力 認証キー) – 認証キーを確認のためにもう一度入力します。
ログイン バナー	ユーザーがクラスタまたはアプライアンスにログインするときに表示 されるバナー メッセージを入力します。
Logging(ログ)タブ	(System(システム)タブと Configuration(設定)タブを含む)
追加	転送するログ転送プロファイル (Panorama Managed WildFire Clusters Logging System または Panorama Managed WildFire Clusters Logging Configuration) を追加します。
	 SNMP トラップ レシーバへの SNMP トラップとしてのシステム ログまたは設定ログ
	 syslog サーバーへの syslog メッセージ
	• 電子メール サーバーへの電子メール通知
	● HTTP サーバーへの HTTP 要求
	その他のログ タイプはサポートされません(「Device(デバイス)> Log Settings(ログ設定)」を参照)。
	ログ転送プロファイルでは、どのログをどの宛先サーバーに転送する かを指定します。プロファイルごとに以下を設定します。
	 Name(名前) – ログ設定を識別する名前(最大 31 文字)。英 数字と下線のみを使用でき、スペースと特殊文字は使用できません。
	 Filter (フィルタ) – デフォルトでは、Panorama アプライアン スは、指定されたプロファイルの All Logs (すべてのログ) を転 送します。一部のログを転送するには、フィルタを選択するか (severity eq critical (重大度が重要)、severity eq high (重大度 が高)、severity eq informational (重大度が通知)、severity eq low (重大度が低)、severity eq medium (重大度が中))、Filter Builder (フィルタビルダー)を選択して新しいフィルタを作成し ます。
	 Description (説明) – 説明 (最大 1,023 又子) を人力し、フロファイルの目的について説明します。

setting	の意味
Add(追加)> Filter(フィルタ) > Filter Builder(フィ ルタ ビルダー)	新しいログフィルタを作成するには、Filter Builder(フィルタビル ダー)を使用します。Create Filter(フィルタの作成)を選択して フィルタを作成し、新しいフィルタのクエリごとに次の設定を指定し てからクエリを Add(追加)します。
	• Connector(条件式) – 論理結合子(and または or)を選択しま す。Negate(上記以外)を選択すると、指定した内容を除外し ます。たとえば、一部のログ説明の転送を回避するには、属性と して Description(説明)を選択して演算子として contains(含 む)を選択し、転送しない説明を識別する値として説明の文字列 を入力します。
	 Attribute(属性) – ログの属性を選択します。ログタイプにより オプションが異なります。
	 Operator(演算子) – 属性の適用方法を決める基準を選択します (contains(含む)など)。ログタイプによりオプションが異な ります。
	 Value[値] – 照合する属性値を指定します。
	• Add(追加) – 新しいフィルタを追加します。
	フィルタで一致するログの表示またはエクスポートを行うに は、View Filtered Logs(フィルタリングされたログの表示)を選択 します。
	 一致するログエントリを検索するには、検索フィールドに IP アドレスや時間範囲などのアーチファクトを入力します。
	 次のログを表示する期間を選択します。Last 15 Minutes(15 分前)、Last Hour(1 時間前)、Last 6 Hrs(6 時間前)、Last 12 Hrs(12 時間前)、Last 24 Hrs(24 時間前)、Last 7 Days(7 日前)、Last 30 Days(30 日前)、または All(全て)(デフォルト)。
	 期間ドロップダウンリストの右にあるオプションを使用し、フィルタの適用、クリア、追加、保存、ロードを行います。
	 フィルタの適用(→ – 検索フィールドの条件に一致するログエントリが表示されます。
	 フィルタのクリ ア (ア スールドをクリアします
	 新しいフィルタの追 ① ① ①
	– 新しい検索条件を定義します(Add Log Filter(ログフィル

)

(

setting	の意味
	タの追加)が表示されますが、これはフィルタの作成と同じで す)。
	 フィルタの保存(アイルタの名前を入力してから OK をクリックします。
	 ● 保存したフィルタを使用(□ 保存したフィルタをフィルタ フィールドに追加します。
	 CSV にエクスポート() CSV 形式のレポートにログをエクスポートし、Download file (ファイルをダウンロード) します。レポートにはデフォルトで最大2,000行のログを含むよう設定されています。CSVレポートの行数制限を変更する場合は、Device (デバイス) > Setup (セットアップ) > Management (管理) > Logging and Reporting Settings (ログとレポートの設定) > Log Export and Reporting (ログのエクスポートとレポート) を開き、新しいMax Rows in CSV Export (CSV エクスポートの最大行数) を入力します。
	ページごとに表示されるエントリの数と順序を変更でき、ページの左 下にあるページ送り機能を使用してログリスト内を移動できます。 ログエントリは、10ページのブロック単位で取得されます。
	 ページごと – ドロップダウン リストを使用し、ページごとのログ エントリの数を変更します(20、30、40、50、75、100)。
	 ASC(昇順)または DESC(降順) – 結果を昇順で(古いログエントリが先)ソートするには ASC(昇順)を選択し、降順で(新しいログエントリが先)ソートするには DESC(降順)を選択します。デフォルトは DESC(降順)です。
	 Resolve Hostname(ホスト名の解決) – 外部 IP アドレスをドメ イン名に解決する場合に選択します。
	 Highlight Policy Actions(ポリシーアクションの強調表示) – ア クションを選択し、アクションと一致するログエントリを強調表 示する場合に選択します。フィルタリングされたログは、次の色 で強調表示されます。
	 緑 - 許可 - 株 - (4)(また)(よう) こくじ
	 與 - 継続またはオーハーフィト 赤 - 却下、ドロップ、drop-icmp、st-client、reset- server、reset-both、block-continue、block-override、block- url、drop-all、sinkhole

)

)

Panorama Web インターフェイス

cotting	の音吐
setting	
削除します。	システム ログ リストまたは設定ログ リストから削除するログ転送設 定を選択してから Delete(削除)します。
認証タブ	
認証プロファイル	構成済みの認証プロファイルを選択して、WildFireアプライアンスまたは Panorama 管理者のログイン資格情報を検証する認証サービスを 定義します。
最大試行回数	管理者をロックアウトする前に、WildFireアプライアンスが CLI で許可するログイン試行失敗の回数を入力します(範囲は 0~10、デフォルトは 10)。ログイン試行回数を制限すると、総当たり攻撃からのWildFireアプライアンス保護に役立ちます。値0を指定すると、無制限にログインを試行できます。
	Failed Attempts (試行失敗回数)を0以外の値にしなが ら、Lockout Time (ロックアウト時間)を0のままにして いる場合、別の管理者がロックアウトされた管理者を 手動でロック解除するまで、管理者ユーザーは無期限 にロックアウトされます。他の管理者が作成されてい ない場合は、Panorama で Failed Attempts (試行失敗回 数) および Lockout Time (ロックアウト時間)の設定を再 構成し、構成変更を WildFireアプライアンスにプッシュ する必要があります。管理者がロックアウトされない ようにするには、Failed Attempts (試行失敗回数) および Lockout Time (ロックアウト時間)の両方にデフォルト値 の(0) を使用します。
	 Failed Attempts (試行失敗回数)の値を5以下に設定し、 入力ミスに備えてある程度猶予を持たせつつ、悪意のあるシステムが総当りで WildFireアプライアンスにログインしようとするのを防ぎます。
ロックアウト時間 (分)	Failed Attempts(最大試行回数)の制限に達した後、WildFireアプラ イアンスがWebインターフェイスおよびCLIへの管理者のアクセス をロックアウトする時間(分)を入力します(範囲は0~60、デフォ ルトは5)。値を0にすると、別の管理者がアカウントのロックを 手動で解除するまでロックアウトが適用されます。

setting	の意味
	► Failed Attempts (試行失敗回数)を0以外の値にしながら、Lockout Time (ロックアウト時間)を0のままにしている場合、別の管理者がロックアウトされた管理者を手動でロック解除するまで、管理者ユーザーは無期限にロックアウトされます。他の管理者が作成されていない場合は、Panorama で Failed Attempts (試行失敗回数)および Lockout Time (ロックアウト時間)の設定を再構成し、構成変更を WildFireアプライアンスにプッシュする必要があります。管理者がロックアウトされないようにするには、Failed Attempts (試行失敗回数)およびLockout Time (ロックアウト時間)の両方にデフォルト値の(0)を使用します。
	 Lockout Time (ロックアウト時間)を 30 分以上に設定 し、攻撃者が続けてログインを試みるのを防ぎます。
ldle Timeout (min)(分単位のアイ ドル タイムアウト)	 CLI でアクティビティがない場合、管理者が自動的にログアウトするまでの最大分数を入力します(範囲は 0~1,440、デフォルトはNone(なし))。値0は、アクティビティがなくても自動ログアウトはトリガーされないことを意味します。 <i>Idle Timeout (</i>アイドルタイムアウト)を10分に設定し、管理者がセッションを開いたままにしている場合に未認証のユーザーが WildFireアプライアンスにアクセスするのを防ぎます。
Max Session Count(最大セッ ション数)	管理者が同時に開くことができるアクティブなセッション数を入力します。デフォルトは0です。これは、WildFireアプライアンスで同時 にアクティブなセッションを無制限に持つことができることを意味します。
Max Session time(最大セッショ ン時間)	管理者が自動的にログアウトするまでにログイン可能な時間を分で入 力します。デフォルトは0です。これは、管理者がアイドル状態で あっても無期限にログイン可能であることを意味します。
Local Administrators(ロー カル管理者)	WildFire アプライアンスに固有の新しい管理者を追加し、設定しま す。この管理者は WildFireアプライアンス固有であり、このページで 管理されます(Panorama > Managed WildFire Appliances(管理対象 WildFireアプライアンス) > Authentication(認証))。
Panorama Administrators(Panor 管理者)	Panorama で設定された既存の管理者をインポートします。これらの ar筆理者は Panorama で作成され、WildFire アプライアンスにインポー トされます。

setting	の意味
Clustering(クラスタ) フェイス)タブ(管理	タブ(管理対象 WildFire クラスタのみ)および Interface(インター 対象 WildFire アプライアンスのみ)
アプライアンスを Pan スタに追加してノード	orama に追加してインターフェイスを管理し、アプライアンスをクラ のインターフェイスを管理する必要があります。
アプライアンス (Clustering(クラス タ)タブのみ)	クラスタノードを選択し、そのノードの Appliance(アプライア ンス)タブと Interfaces(インターフェイス)タブにアクセスしま す。Appliance(アプライアンス)タブのノード情報は事前に入力さ れ、ホスト名以外は設定できません。Interfaces(インターフェイ ス)タブにはノードのインターフェイスがリストされます。以下に記 載されるように管理するインタフェースを選択します。
	Interface Name Management
	Interface Name Analysis Environment Network
	Interface Name Ethernet2
	Interface Name Ethernet3
インターフェイス名 管理	管理インターフェイスは Ethernet0 です。管理インターフェイスの設 定を構成するか表示します。
	 Speed and Duplex(速度とデュプレックス) – auto- negotiate(デフォルト)、10Mbps-half-duplex、10Mbps-full- duplex、100Mbps-half-duplex、100Mbps-full-duplex、1Gbps- half-duplex、1Gbps-full-duplexのいずれかを選択します。
	• IP Address(IP アドレス) – インターフェイスの IP アドレスを入 力します。
	• Netmask(ネットマスク) – インターフェイスのネットマスクを 入力します。
	 Default Gateway(デフォルトゲートウェイ) – デフォルトゲートウェイの IP アドレスを入力します。
	 MTU – MTU をバイト単位で入力します(範囲は 576 ~ 1,500、 デフォルトは 1,500)。
	 Management Services(管理サービス) – サポートする管理サー ビスを有効にします。Ping、SSH、SNMP サービスをサポートで きます。
	プロキシ サーバーを使用してインターネットに接続する場合は、プ ロキシ設定を構成します。
	• Server(サーバー) – プロキシ サーバーの IP アドレス。
	 Port(ポート) – プロキシ サーバーで Panorama デバイス要求を 待ち受けるように設定されているポート番号。

setting	の意味	
	 User(ユーザー) – プロキシ サーバーで認証用に設定されている ユーザー名。 	I
	 Password (パスワード)および Confirm Password (再入力パス ワード) – プロキシ サーバーで認証用に設定されているパスワー ド 	
	 Clustering Services(クラスタ サービス)(Clustering(クラス タ)タブのみ) – HA サービスを選択します。 	
	 HA – 2つのコントローラ ノードがクラスタにある場合は、管理インターフェイスを HA インターフェイスとして設定し、管理情報を両方のクラスタ ノードで使用できるようにします。設定しているクラスタ ノードがプライマリ コントローラ ノードである場合は、それを HA インターフェイスとしてマークしてください。 	
	WildFire アプライアンスのイーサネット インターフェイスの使 用方法に応じて、プライマリ コントローラ ノードでは HA イ ンターフェイスとして、バックアップ コントローラ ノードで は HA バックアップ インターフェイスとして、Etherent2 また は Ethernet3 を設定することもできます。たとえば、Ethernet2 を HA と HA バックアップ インターフェイスとして使用でき ます。HA と HA バックアップ インターフェイスは、プライマ リ コントローラ ノードとバックアップ コントローラ ノードで 同じインターフェイス (管理、Ethernet2、Ethernet3) にする 必要があります。Ethernet1 を HA/HA バックアップ インター フェイスとして使用することはできません。	
	 HA Backup(HA バックアップ) – 設定しているクラスタ ノードがバックアップ コントローラ ノードである場合は、それをHA Backup(HA バックアップ)インターフェイスとしてマークします。 	
	インターフェイスで許可される IP アドレスを指定します。	
	 検索ボックス – 検索条件を入力し、許可される IP アドレスのリストをフィルタリングします。検索ボックスにはリストの IP アドレス(項目)の数が表示されるため、リストの長さが分かるようになっています。検索条件を入力したら、フィルタを適用するか(→ フィルタをクリアして)、
	(× 別の一連の条件を入力します。)
	 Add (追加) –権限のある IP アドレスを Add (追加) します。 	
	 Delete(削除) – 管理インターフェイス アクセスから削除する IP アドレスを選択して Delete(削除)します。 	

setting	の意味	
インターフェイス名 分析環境ネットワー ク	WildFire アプライアンス クラスタまたはスタンドアロン WildFire アプライアンスの分析環境ネットワーク インターフェイス (Ethernet1、VM インターフェイスとも呼ばれる)の設定を構成し ます。	-
	 Speed and Duplex(速度とデュプレックス) – auto- negotiate(デフォルト)、10Mbps-half-duplex、10Mbps-full- duplex、100Mbps-half-duplex、100Mbps-full-duplex、1Gbps- half-duplex、1Gbps-full-duplexのいずれかを設定します。 	
	• IP Address(IP アドレス) – インターフェイスの IP アドレスを入 力します。	
	• Netmask(ネットマスク) – インターフェイスのネットマスクを 入力します。	
	 Default Gateway(デフォルトゲートウェイ) – デフォルトゲートウェイの IP アドレスを入力します。 	
	 MTU – MTU をバイト単位で入力します(範囲は 576 ~ 1,500、 デフォルトは 1,500)。 	
	 DNS Server (DNS サーバー) – DNS サーバーの IP アドレスを入 力します。 	
	 Link State(リンク状態) – インターフェイスのリンク状態を Up(アップ)または Down(ダウン)に設定します。 	
	 管理サービス – インターフェイスで Ping サービスをサポートする 場合は、Ping を有効にします。 	
	インターフェイスで許可される IP アドレスを指定します。	
	 検索ボックス – 検索条件を入力し、許可される IP アドレスのリストをフィルタリングします。検索ボックスにはリストの IP アドレス(項目)の数が表示されるため、リストの長さが分かるようになっています。検索条件を入力したら、フィルタを適用するか 	
	 フィルタをクリアして)、
	(図の一連の冬姓を入力します)
	 Add(追加) – 権限のある IP アドレスを Add(追加)します。 	
	 Delete(削除) – 管理インターフェイス アクセスから削除する IP アドレスを選択して Delete(削除)します。 	
インターフェイス名 Etherrnet2	Ethernet2 インターフェイスと Ethernet3 インターフェイスには同じ パラメータを設定できます。	_
インターフェイス名 Etherrnet3	 Speed and Duplex(速度とデュプレックス) – auto- negotiate(デフォルト)、10Mbps-half-duplex、10Mbps-full- 	

setting	の意味
	duplex、100Mbps-half-duplex、100Mbps-full-duplex、1Gbps- half-duplex、1Gbps-full-duplex のいずれかを設定します。
	• IP Address(IP アドレス) – インターフェイスの IP アドレスを入 力します。
	• Netmask(ネットマスク) – インターフェイスのネットマスクを 入力します。
	 Default Gateway (デフォルト ゲートウェイ) – デフォルト ゲートウェイの IP アドレスを入力します。
	 MTU – MTU をバイト単位で入力します(範囲は 576 ~ 1,500、 デフォルトは 1,500)。
	 管理サービス – インターフェイスで Ping サービスをサポートする 場合は、Ping を有効にします。
	• Clustering Services(クラスタ サービス) – クラスタ サービスを 選択します。
	 HA – 2 つのコントローラ ノードがクラスタにある場合 は、Ethernet2 または Ethernet3 インターフェイスを HA イン ターフェイスとして設定し、管理情報を両方のクラスタ ノード で使用できるようにします。設定しているクラスタ ノードがプ ライマリ コントローラ ノードである場合は、それを HA イン ターフェイスとしてマークしてください。
	WildFire アプライアンスのイーサネット インターフェイスの使 用方法に応じて、プライマリ コントローラ ノードでは HA イ ンターフェイスとして、バックアップ コントローラ ノードで は HA バックアップ インターフェイスとして、管理インター フェイス(Etherent1)を設定することもできます。HA と HA バックアップ インターフェイスは、プライマリ コントロー ラ ノードとバックアップ コントローラ ノードで同じインター フェイス(管理、Ethernet2、Ethernet3)にする必要がありま す。Ethernet1 を HA/HA バックアップ インターフェイスとし て使用することはできません。
	 HA Backup(HA バックアップ) – 設定しているクラスタ ノードがバックアップ コントローラ ノードである場合は、それをHA Backup(HA バックアップ)インターフェイスとしてマークします。 Cluster Management(クラスタ管理) – クラスタ全体の管理 い気気に使用ます。 (2) たって、 (2) たい、 (2) たい、
	こ地信に使用9 るインターフェイスとして、Ethernet2 または Ethernet3 インターフェイスを設定します。
ロール	クラスタにメンバー アプライアンスがあるとき、アプライアン スのロールは、コントローラ、コントローラ バックアップ、ワー カーのいずれかにすることができます。クラスタのアプライアン

setting	の意味	
(Clustering (クラス タ)タブのみ)	スから各ロールに使用する WildFire アプライアンスを変更するに は、Controller(コントローラ)または Backup Controller(バック アップ コントローラ)を選択します。コントローラを変更すると、 ロール変更中にデータが失われます。	•
参照 (Clustering(クラス タ)タブのみ)	Clustering (クラスタ) タブには、クラスタの WildFire アプライアン ス ノードがリストされます。Browse (参照) により、Panorama デ バイスがすでに管理しているスタンドアロン WildFire アプライアン スを表示して追加します。	_
	 検索ボックス – 検索条件を入力し、ノードリストをフィル タリングします。検索ボックスにはリストのアプライアンス (項目)の数が表示されるため、リストの長さが分かるように なっています。検索条件を入力したら、フィルタを適用するか (→)
	フィルタをクリアして (× 別の一連の条件を入力します。)
	 ノード追加-(⊕)ノードをクラスタに追加します。 	
	クラスタに最初に追加する WildFire アプライアンスは、自動的にコ ントローラ ノードになります。2 番目に追加する WildFire アプライ アンスは、自動的にコントローラ バックアップ ノードになります。	
	最大で 20 個の WildFire アプライアンスをクラスタに追加できます。 コントローラ ノードとコントローラ バックアップ ノードを追加し たら、その後で追加するすべてのノードはワーカー ノードになりま す。	
削除します。 (Clustering(クラス タ)タブのみ)	1 つ以上のアプライアンスをアプライアンス リストから選択し、クラ スタから Delete(削除)します。コントローラ ノードを削除できる のは、クラスタに 2 つのコントローラ ノードがある場合のみです。	_
コントローラの管理 (Clustering(クラス タ)タブのみ)	Manage Controller (コントローラの管理)を選択し、クラスタに 属す WildFire アプライアンス ノードから Controller (コントロー ラ)と Controller Backup (コントローラ バックアップ)を指定しま す。現在のコントローラ ノードとバックアップ コントローラ ノード はデフォルトで選択されます。バックアップ コントローラ ノードを プライマリ コントローラ ノードと同じノードにすることはできませ ん。	-
通信タブ		-

`

setting	の意味
保護されたサーバー 通信のカスタマイズ	 SSL/TLS Service Profile (SSL/TLS サービス プロファイル) – ドロップダウン リストから SSL/TLS サービス プロファイルを選択します。このプロファイルは、WildFire との通信で接続デバイスが使用する証明書およびサポートされる SSL/TLS バージョンを定義します。
	• Certificate Profile(証明書プロファイル) – ドロップダウンリストから証明書プロファイルを選択します。この証明書プロファイルは、証明書失効チェックの動作と、クライアントから提供された証明書チェーンの認証に使用できるルート CA を定義します。
	 Custom Certificate Only(カスタム証明書のみ) – 有効にする と、WildFire は、接続デバイスとの認証用のカスタム証明書のみ を受け付けます。
	 Check Authorization List(承認リストのチェック) – WildFire に 接続しているクライアント デバイスを承認リストと照合します。 デバイスはリストの1項目のみと一致するだけで承認されます。 一致がない場合、デバイスは承認されません。
	 Authorization List(承認リスト) – クライアント デバイスの承認 条件を設定するには、Add(追加)を選択し、以下のフィールドを 入力します。Authorization List(承認リスト)は、最大 16 件のエ ントリをサポートします。
	 Identifier (識別子) –Select Subject (サブジェクト) または Subject Alt (サブジェクト代替) を選択します。認証識別子としてのName (名前) を付けます。
	 Type (タイプ) – Subject Alt (サブジェクト代替)の場合。Name (名前)を識別子として選択した場合、識別子のタイプとしてIP、hostname (ホスト名)、またはe-mail (電子メール)を選択します。Subject (サブジェクト)を選択した場合、共通名が識別子タイプになります。 Value (値) – 識別子の値を入力します。
保護されたクライア ント通信	Secure Client Communication (保護されたクライアント通信)を使用すると、WildFire は(デフォルトで事前定義される証明書の代わりに)設定済みのカスタム証明書を使用して、WildFire アプライアンスへの SSL 接続を認証します。
	 Predefined(事前定義済み) – (デフォルト)デバイス証明書は設定されていません。WaveFireはデフォルトの事前定義済み証明書を使用します。

setting	の意味
	 Local (ローカル) – WildFire は、ファイアウォールで生成され たか既存のエンタープライズ PKI サーバーからインポートされた ローカルのデバイス証明書および対応する秘密鍵を使用します。
	 Certificate(証明書):ローカルデバイス証明書を選択します。
	 Certificate Profile(証明書プロファイル):ドロップダウンリ ストから証明書プロファイルを選択します。
	 SCEP – WildFire は、Simple Certificate Enrollment Protocol (SCEP) サーバーで生成されたデバイス証明書と秘密鍵 を使用します。
	 SCEP Profile (SCEP プロファイル):ドロップダウン リストから SCEP プロファイルを選択します。
	 Certificate Profile(証明書プロファイル):ドロップダウンリ ストから証明書プロファイルを選択します。
Secure Cluster Communication 安全 なクラスタ通信	Enable(有効)を選択すると、WildFireアプライアンス間の通信 を暗号化します。デフォルトの証明書では、定義済みの証明書タ イプが使用されます。ユーザー定義のカスタム証明書を使用するに は、Customize Secure Server Communication(セキュリティで保護 されたサーバー通信のカスタマイズを構成)し、Custom Certificate Only(カスタム証明書のみ)を有効にする必要があります。
Panorama > ファイアウォール クラスター

• Panorama > Firewall クラスター

(CNシリーズおよびPA-7500シリーズのファイアウォールでのみ使用可能) Panorama の Firewall Clusters で、CN-Series または PA-Series Firewall Clusters (ファイアウォール クラス タ)を作成および構成し、クラスタの概要を表示し、ヘルス情報を監視します。PA-7500シリー ズファイアウォールだけがPAシリーズファイアウォールクラスタをサポートします。

[Firewall Clusters (ファイアウォールクラスタ)]でクラスタの詳細を表示するには、デバイス > プラグインから Panorama Clustering プラグインバージョン (PAN-OS バージョンと互換性のある) をインストールする必要があります。

- ファイアウォールクラスタの作成と編集
- 概要ビュー
- モニタリング

ファイアウォールクラスタの作成と編集

[Create Cluster (クラスタの作成)]を選択してクラスタを作成し、タイプを指定して[OK]をクリックします。次に、クラスタを選択して [クラスタの編集] 画面にアクセスし、メンバーを選択してクラスタをさらに構成します。

どのクラスタを編集用に表示するかを制御するには、[Clusters (クラスタ)]フィールドで[CN-Series (CN シリーズ)]、[PA-Series (PA シリーズ)]、または[All Clusters (すべてのクラスタ)]を選択します。

項目	詳説
クラスタ名	ゼロ個以上の英数字、下線 (_)、ハイフン (-)、ドット (.)、またはスペー スを含むクラスタ名を入力します。
クラスタ タイプ	クラスタのタイプを選択してください: CN (CN シリーズクラスタ)また は PA (PA シリーズクラスタ、NGFW クラスタ)。
説明	クラスタの説明を入力します。
Group-ID	グループ ID を 1 ~ 63 の範囲で入力します。デフォルトは 1 です。 グループ IDは、同じレイヤー2ネットワーク内の2つのHAペア(また はHAペアとNGFWクラスタ)がMACアドレスを共有する場合、MACアド レスを区別するのに役立ちます。
メンバー	クラスタのメンバーを選択してください
	PA シリーズクラスタの場合:

項目	詳説
	 メンバーは PA-7500 シリーズファイアウォール 2 台以下でなければ なりません。
	 潜在的なメンバーのリストには、PA-7500シリーズファイアウォールのみが表示されます。
	 クラスタメンバーとして最初に選択したノードが自動的にノード1 になります。

一般

デバイス	(PA シリーズクラスタのみ)デバイスのシリアル番号。設定不可。
ID	(PA シリーズクラスタのみ)ノード ID(1 または 2)、設定不可クラ スタメンバーを選択するときに最初に選択したノードが自動的にノード 1 になります。
コミュニケーショ ン	(PA シリーズクラスタのみ)[将来の使用に備えて予約済み。]

System Monitoring(システムモニタリング)

容量損失時の状態	(PA シリーズクラスタのみ) 次のいずれかを選択します。
	• degraded – 機能しているネットワークカードまたはデータ処理カード の数が、それぞれ設定された最小ネットワークカード数または最小 データ処理カード数を下回った場合に、ファイアウォールのノード状 態が DEGRADED として識別されるように指定します。
	 failed-機能しているネットワークカードまたはデータ処理カードの 数が、それぞれ設定された最小ネットワークカード数または最小デー タ処理カード数を下回った場合に、ファイアウォールのノード状態を FAILED として識別するように指定します。
最小ネットワーク カード	(PA シリーズクラスタのみ)機能するために必要なネットワークカードの最小数。範囲は1~7で、デフォルトは1です。クラスタがこの最小値を下回ると、クラスタの状態は、設定した(デグレードまたは障害が発生した)容量損失時の状態に移行します。
最小限のデータ処 理カード	(PA シリーズクラスタのみ)機能するために必要なデータ処理カード の最小数。範囲は1~7で、デフォルトは1です。クラスタがこの最小 値を下回ると、クラスタの状態は、設定した(デグレードまたは障害が 発生した)容量損失時の状態に移行します。

概要ビュー

過去5分間にファイアウォールによってキャプチャされた CN シリーズ クラスタまたはPA シ リーズ クラスタに関する情報を表示しますに関する情報を表示します。更新ボタンをクリック して、最新の詳細を読み込みます。

クラスタプラグインの可視性データはリアルタイムではなく、最大5分遅れます。

項目	詳説	
クラスタ名	ファイアウォール クラスタの名前。	
ソフトウェア バージョン	PAN-OS バージョン。	
クラスタで使 用されるプラ グイン	クラスタで使用されるプラグインのリスト。	
テンプレート スタック	クラスタに関連付けられたテンプレート スタックの名前。	
デバイス グ ループ	クラスタに関連付けられたデバイス グループの名前。	
クラスタの状 態	(CN シリーズ クラスタのみ) クラスタが影響を受けるかどうかが表示され ます。	
	(PA シリーズクラスタのみ) クラスタ内のすべてのノードのノードステータ スから導き出されるクラスタの状態を表示します。クラスタの状態は次のよ うになります。	
	● OK−すべてのノードが ONLINE 状態の場合。	
	 影響-少なくとも1つのノードが ONLINE 状態で、もう1つのノードが ONLINE 状態でない場合。 	
	 エラー-オンライン状態のノードが1つもない場合。 	
クラスタ タ イプ	クラスタのタイプ (CN または PA)。	
影響を受ける メンバー	影響を受けるクラスタ メンバーの数とその名前。	
システムログ の詳細	システムイベントの詳細。	

項目	詳説	
特定のエラー	クラスター内の特定のエラーのリスト。リンクをクリックすると、Monitor > Logs > System (view logs の下にあるエラーの詳細が表示されます。	
ポッド名	(CN シリーズクラスタのみ) ポッドの名前。	
CPU 数	使用されている CPU の数。	
設定同期ス テータス	(PA シリーズクラスタのみ) Panorama と PA クラスタ内のファイアウォー ル間の同期ステータスを設定します。ステータスは [In Sync (同期)] または [Out of Sync (同期外)] のいずれかとなります。クラスタへのファイアウォー ルの追加、コミット、プッシュが正常に完了すると、[Config Sync Status (設 定同期ステータス)]が[In Sync (同期中)]と表示されます。	
最終コミット 状態	 (PA シリーズクラスタのみ)最後に試行されたコミットの状態: コミット失敗 コミットが成功しました コミットは成功し、警告が表示されました コミットが元に戻されました 	
ノード同期ス テータス	 (PA シリーズクラスタのみ) ノードフローテーブルの同期ステータス: SYNC (同期) UPDATING (更新中) OUT_OF_SYNC (同期されていない) 	
Node Status(ノー ドステータ ス)	 (PA シリーズクラスタのみ) クラスタノードで発生する可能性のある状態: 不明-クラスタリングは有効化されていません。ノードは、Panorama からのクラスタ構成のプッシュまたはコミットによってクラスタリングが有効になるまで、この状態のままになります。 INIT-クラスタリングが有効になった後、ノードはUNKNOWN状態からINIT状態に移行します。ノードのクラスタ初期化が完了するまで、ノードはINIT状態のままです。タイムアウト後、ノードは ONLINE 状態に移行します。 ONLINE-ノードはトラフィックを渡し、期待どおりに動作しています。 DEGRADED:ソフト障害が発生すると、ノードはDEGRADED状態に移行します。すべての障害が解決された場合、ノードはDEGRADED状態からINIT状態に移行できます。 FAILED-ハード障害が発生すると、ノードはFAILED状態に移行します。 ノードは、すべての障害が解決された場合、FAILED状態からINIT状態に移行できます。 	

項目	詳説	
	 SUSPENDED- 管理者によってトリガーされます。SUSPENDED状態のもう1つの原因は、ノード状態がDEGRADED状態またはFAILED状態にフラップを繰り返す場合です。6回のフラップの後、ノードはSUSPENDED状態になります。管理者はノードの一時中断を解除できます。SUSPENDED状態はトラフィックポートがダウンしており、L7の連続性が許可されていません。 	

モニタリング

CN シリーズまたは PA シリーズのファイアウォールクラスタの状態情報を表示します。

🏫 クラスタプラグインの可視性データはリアルタイムではありません。

項目	詳説
マネージド ソフトウェア クラスター	ファイアウォール クラスタを選択します。
影響を受けた	影響を受けるファイアウォール クラスタのリスト。
	 CN クラスタまたは PA クラスター影響を受けた CN シリーズまたは PA シリーズのファイアウォールクラスタのそれぞれの数。
	 影響を受けるクラスタ – 影響を受けるクラスタのリスト。
	クリックすると、[相互接続ステータス]および[クラスタ使用率]ダッシュボー ドにクラスタに関する詳細情報が表示されます。
ОК	影響を受けない firewall クラスターのリスト。
	 CN クラスタまたは PA クラスターそれぞれ影響を受けない CN シリーズまたは PA シリーズのファイアウォールクラスタの数。
	 影響を受けるクラスタ – 影響を受けていないクラスタのリスト。
	クリックすると、[相互接続ステータス]および[クラスタ使用率]ダッシュボー ドにクラスタに関する詳細情報が表示されます。
相互接続ス	選択した時間枠のクラスタ相互接続の詳細を表示します。
テータス	[過去5分間]を選択して、次の詳細を表示します。
	• Cluster Name – ファイアウォール クラスタの名前。
	 Cluster Type (クラスタタイプ) – クラスタのタイプ(CN または PA)。
	 Cluster Creation Time (クラスタ作成時刻) – クラスタを作成した時刻。

項目	詳説	
	• Cluster State (クラスタの状態)– クラスタが影響を受けているかどうかを 表示。	
	 Current Cluster Detail (現在のクラスタの詳細) - 現在のクラスタ状態の リンクをクリックすると、影響を受けるクラスタの詳細が表示されま す。 	
	 Cluster Interconnect State (クラスタ相互接続の状態) – クラスタが影響を 受けているかどうかが表示されます。 	
	• Current Cluster Detail (現在のクラスタの詳細) – 現在の相互接続状態リンクをクリックして、影響を受ける相互接続の詳細を表示します。	
	 Traffic Interconnect:トラフィック相互接続のステータス。 	
	• External Connection – 外部接続のステータス。	
	• Impacted Links-影響を受けるリンクの数。	
	 Management Connectivity – 管理接続の数。 	
	● Impacted Cluster Member – 影響を受けるクラスタ メンバーのリスト。	
	 Time Stamp Hi-Res Uptime – アップタイムのタイム スタンプ。 	
	 Time Stamp Hi-Res Downtime – ダウンタイムのタイム スタンプ。 	
	過去5分以外の時間枠を選択すると、次の情報のみが表示されます。	
	 クラスタ名 	
	 クラスタ タイプ 	
	• クラスタ作成時間	
	• 現在のクラスタの状態	
	• クラスタ相互接続の状態	
	 トラフィックインターコネクト 	
	• 外部接続	
クラスター使 用率	ファイアウォールクラスタのスループット、メモリ、およびデータ使用率を 表示します。	
	Cluster Name - firewall cluster.	
	 Cluster Details - クラスター名のリンクをクリックして、選択したクラ スターのスループット、メモリー、およびデータ使用率の詳細を表示 します。 	
	• Cluster Type (クラスタタイプ) – クラスタのタイプ(CN または PA)。	
	• Cluster State – クラスタの状態を表示します。	
	 Cluster Throughput (クラスタスループット) (gbps) – ファイアウォールク ラスタのスループット (Gbps)。 	
	 CPS – 1 秒あたりの接続数。 	

項目	詳説
	 Session Count (Sessions) – セッション数。
	 Average Data Plane (%) Within Health Threshold (平均データプレーン(%) 状態基準値以内) – 平均データ プレーンしきい値 (パーセント)。
	 Management Plane CPU (%) - 管理プレーンの CPU 使用率 (パーセント)。
	 Management Plane Mem (%) - 管理プレーンのメモリ使用率(パーセント)。
	 Logging Rate (Log/Sec) – クラスタでログが生成されるレート。 DP Auto-Scale Status - データプレーンのオートスケールの詳細。

Panorama > Administrators [Panorama > 管理者]

Panorama > Administrators(管理者)を選択し、**P**anorama 管理者のアカウントを作成および管理します。

スーパーユーザー ロールを持つ管理者として Panorama にログインすると、Locked User(ロッ クされたユーザー)列のロック アイコンをクリックして他の管理者のアカウントのロックを 解除できます。ロックアウトされた管理者は Panorama を操作できません。Panorama は、 アカウントに割り当てられた Authentication Profile(認証プロファイル)で定義されてい る、Panorama へのアクセスの連続失敗許容試行回数を超えた管理者をロックアウトします (「Device(デバイス) > Authentication Profile(認証プロファイル)」を参照)。

管理者アカウントを作成するには、Add(追加)をクリックし、以下の表の説明に従って設定を 指定します。

管理者アカウント設定	の意味
氏名	管理者のログイン ユーザー名(最大 15 文字)を入力します。 この名前は、大文字と小文字が区別され、一意でなければなら ず、文字、数字、ハイフン、アンダースコアのみで構成されま す。
認証プロファイル	この管理者を認証する認証プロファイルまたは認証シー ケンスを選択します。詳細は、「Device(デバイス) > Authentication Profile(認証プロファイル)」または 「Device(デバイス) > Authentication Sequence(認証シー ケンス)」を参照してください。
クライアント証明書認証の みを使用(Web)	Web インターフェイス アクセスのクライアント証明書認証を 使用する場合に選択します。このオプションを選択すると、 ユーザー名(Name(名前))とパスワード(Password(パス ワード))は必要なくなります。
パスワード/再入力 パス ワード	管理者の大文字と小文字を区別するパスワード(最大 16 文字) を入力して確認します。セキュリティを確保するために、管理 者がパスワードを定期的に変更することをお勧めします。パス ワードには、小文字、大文字、および数字を組み合わせること をお勧めします。パスワードの強度を高めるために、必ずパス ワード強度のベストプラクティスに従ってください。
	デバイス グループおよびテンプレートの管理者は Panorama > Administrators (管理者) にアクセスすることができませ ん。この管理者のローカル パスワードを変更するには、管 理者は (Web インターフェイス下部の Logout (ログアウ ト)の横にある) ユーザー名をクリックします。Panorama > Administrators (管理者) へのアクセス権限を無効化された Panorama ロールを持つ管理者の場合も同様です。

管理者アカウント設定	の意味
	パスワード認証はAuthentication Profile[認証プロファイル]と 併用あるいは順に適用したり、ローカルデータベース認証と併 用することができます。
	パスワードの有効期限パラメータを設定するには、Password Profile (パスワード プロファイル) (「Device (デバイス) > Password Profiles (パスワード プロファイル) 」を参照) を 選択し、Minimum Password Complexity (パスワード複雑性設 定) パラメータ (「Device (デバイス) > Setup (セットアッ プ) > Management (管理) 」を参照) を設定します。ただ し、Panorama がローカルで認証する管理者アカウントのみが 対象となります。
公開キーの認証 (SSH) の使 用	SSH 公開キーの認証を使用する場合に選択します。Import Key (キーのインポート)をクリックし、Browse (参 照)して公開キーファイルを選択し、OK をクリックしま す。Administrator [管理者]ダイアログの読み取り専用テキス トエリアに、アップロードした鍵が表示されます。 サポート対象の鍵ファイルのフォーマットは、IETF
	SECSH と OpenSSH です。サポート対象の鍵アルゴリズム は、DSA(1,024 ビット)と RSA(768 ~ 4,096 ビット)で す。
	公開キーの認証が失敗すると、ログインとパス ワードプロンプトが表示されます。
管理者タイプ	タイプの選択によって、管理ロールのオプションが決まりま す。
	 Dynamic (動的) – Panorama および管理対象ファイア ウォールへのアクセス権を付与するロール。新しい機能が 追加されると、Panorama によってダイナミックロールの 定義が自動的に更新されます。ユーザーが手動で更新する 必要はありません。
	 Custom Panorama Admin(カスタム Panorama 管理) – 設定可能なロールであり、Panorama 機能に対する読み書きアクセス権または読み取り専用アクセス権を設定できます。また、Panorama 機能に対するアクセス権を一切与えない(アクセス権なし)ように設定することもできます。
	 Device Group and Template Admin (デバイス グループお よびテンプレート管理) – 設定可能なロールであり、こ の管理者に対して選択したアクセス ドメインに割り当てた デバイス グループとテンプレートの各機能に対する読み書 きアクセス権または読み取り専用アクセス権を設定できま

管理者アカウント設定	の意味
	す。また、これらの各機能に対するアクセス権を一切与え ない(アクセス権なし)ように設定することもできます。
管理者ロール	事前に定義されたロールを選択します:
(ダイナミック管理者タイプ)	 Superuser [スーパーユーザー] – Panoramaとすべてのデバ イス グループ、テンプレート、管理対象ファイアウォール に対する読み取り/書き込みのフル アクセス権が付与されま す。
	 Superuser (Read Only) [スーパーユーザー(読み取り専用)] Panorama とすべてのデバイス グループ、テンプレート、管理対象ファイアウォールに読み取り専用でアクセスできます。
	 Panorama administrator [Panorama 管理者] – Panorama に 対するフルアクセス権が付与されます。ただし、以下のア クションを除きます。
	 Panorama またはファイアウォールの管理者およびロー ルの作成、変更、削除。
	 Device (デバイス) > Setup (セットアップ) > Operations (操作)から設定のエクスポート、検証、取り消し、保 存、ロード、インポートを行います。
	 PanoramaタブからScheduled Config Export [スケジュー ル設定された設定のエクスポート] 機能を設定する。
プロファイル	カスタム Panorama ロールを選択します(「Panorama >
(カスタムPanorama管理用 管理者タイプ)	Managed Devices(管理対象デバイス)> Summary(サマリー)」を参照)。
管理者ロールに対するアク セスドメイン (デバイスグループおよびテ ンプレート管理用管理者タ イプ)	アクセスドメイン (最大 25 個) ごとに管理者に割り当てる には、ドロップダウンリストから Access Domain (アクセ スドメイン) を Add (追加) します (「Panorama > Access Domains (アクセスドメイン)」を参照)。次に、隣にある Admin Role (管理者ロール) セルをクリックし、ドロップダ ウンリストからカスタムの Device Group and Template (デ バイス グループとテンプレート) 管理者ロールを選択しま す (「Panorama > Managed Devices (管理対象デバイス) > Summary (サマリー)」を参照)。複数のドメインへのアク セス権を持つ管理者が Panorama にログインすると、Web イ ンターフェイスのフッターに Access Domain (アクセスドメ イン)ドロップダウンリストが表示されます。管理者は、割 り当てられた任意の Access Domain[アクセスドメイン]を選 択し、Panorama に表示する、モニタリングおよび設定データ をフィルタリングできます。Access Domain[アクセスドメイ

管理者アカウント設定	の意味
	 ン]を選択することで、Context[コンテクスト]のドロップダウンリストから表示されるファイアウォールも絞り込まれます。 <i>Radius</i> サーバーを使用して管理者を認証する場合、管理者のロールとアクセスドメインをRadius VSA にマッピングする必要があります。VSA 文字列の文字数には制限があるため、管理者に対してアクセスドメインとロールのペアの最大数 (25)を構成する場合、各アクセスドメインと各ロールの名前値を平均で9文字以下とする必要があります。
パスワードプロファイル	Password Profile (パスワード プロファイル)を選択します (「Device(デバイス) > Password Profiles(パスワード プ ロファイル)」を参照)。

Panorama > Admin Roles [Panorama > 管理者ロール]

管理者ロールのプロファイルは管理者のアクセス権限や役割を定義する、カスタマイズ可能な ロールです。たとえば、管理者に割り当てられたロールにより、生成できるレポート、あるいは 管理者が表示または変更できるデバイス グループやテンプレート設定を制御します。

デバイス グループおよびテンプレートの管理者の場合、管理者アカウントに割り当てられ た各アクセス ドメインに個別のロールを割り当てることができます(「Panorama > Access Domains(アクセス ドメイン)」を参照)。アクセス ドメインにロールをマッピングすると、 管理者が Panorama でアクセスできる情報を非常に詳細に制御できます。たとえば、データ セ ンター内のファイアウォールのすべてのデバイス グループが含まれるアクセス ドメインを設定 し、データ センター トラフィックの監視は許可されているが、ファイアウォールの設定は許可 されていない管理者にそのアクセス ドメインを割り当てるとします。この場合、すべてのモニ タリング権限を有効にするが、デバイス グループ設定へのアクセスは無効にするロールにアク セス ドメインをマッピングします。

管理者ロール プロファイルを作成するには、プロファイルを Add(追加)し、以下の表の説明 に従って設定を指定します。

Radius サーバーを使用して管理者を認証する場合、管理者のロールとアクセスドメインを Radius ベンダー固有の属性 (VSA) にマッピングしてください。

Panorama 管理者ロール 設定	の意味
氏名	管理者ロールの識別に使用する名前を入力します(最大 31 文 字)。この名前は、大文字と小文字が区別され、一意でなければな らず、文字、数字、スペース、ハイフン、アンダースコアのみで構 成されます。
の意味	(任意)ロールの説明を入力します。
ロール	scope of administrative responsibility(管理責任の範囲)を選択し ます。PanoramaまたはDevice Group and Template(デバイス グ ループとテンプレート)
Web UI	Panoramaコンテクスト(Web Ul list (Web Ul リスト))内の特定の 機能とファイアウォールコンテクスト(Context Switch Ul list (コン テクストの切り替えUlリスト))で許可されるアクセスのタイプを 以下のオプションから指定します。
	 Enable(許可)(一読み取りおよび書き込みアクセス

)

Panorama 管理者ロール 設定	の意味
	● Read Only[読み取り専用] (
	◎)−読み取りアクセスのみ
	• Disable (無
	効)(
XML API	Panorama と管理対象のファイアウォールについて XML API アクセ
(Panorama ロールのみ)	スの種類(Enable(有効化)、またはDisable(無効化)を選択し ます。
	 Report (レポート) – ファイアウォールレポートにアクセスできます。
	 Log(ログ) – ファイアウォールログにアクセスできます。
	 Configuration (設定) – Panorama およびファイアウォール設定の 取得または変更が許可されます。
	 Operational Requests(操作要求) – Panorama およびファイア ウォール上の操作コマンドの実行が許可されます。
	 Commit(コミット) – Panorama およびファイアウォール設定のコミットが許可されます。
	 User-ID Agent (User-ID エージェント) – User-ID エージェントにアクセスできます。
	 Export(エクスポート) – Panorama およびファイアウォール からのファイルのエクスポート(設定、ブロックページや応答 ページ、証明書、キーなど)が許可されます。
	 Import (インポート) – Panorama およびファイアウォールへの ファイルのインポート(ソフトウェア更新、コンテンツ更新、 ライセンス、設定、証明書、ブロックページ、カスタムログな ど)が許可されます。
コマンド行	CLIアクセスのロールのタイプを選択します。
(Panorama ロールのみ)	 None(なし) – Panorama CLI へのアクセスが無効です(デフォルト)。
	 superuser(スーパーユーザー) – Panorama へのすべてのアク セスが許可されます。
	 superreader(スーパーリーダー) – Panorama に対する読み取り専用のアクセス権が与えられます。

)

Panorama 管理者ロール 設定	の意味
	 panorama-admin (Panorama 管理者) – Panorama に対するフルアクセス権が付与されます。ただし、以下のアクションを除きます。 Panoramaの管理者およびロールの作成、変更、削除。
	 設定のエクスポート、検証、保存、ロード、インポートを行う。 設定のエクスポートのスケジュールを設定する。
REST API (Panorama ロールのみ)	Panorama および管理対象のファイアウォールのそれぞれの REST API エンドポイントに適用するアクセスのタイプ(Enable(有効 化)、Read Only(読み取り専用)、またはDisable(無効化))を 選択します。以下のカテゴリのエンドポイントにロール アクセスを 割り当てることができます。 Objects ・ポリシー ・ネットワーク ・デバイス
コンテキスト切り替え	
デバイス管理者の役割	Panorama 管理者が Panorama と管理対象ファイアウォール Web インターフェイス間でコンテキスト切り替えを行えるようにするには、デバイス管理ロールの名前を入力します。

Panorama > Access Domains [Panorama > アクセスド メイン]

アクセスドメインでは、特定のデバイスグループ(ポリシーおよびオブジェクトの管理)、テ ンプレート(ネットワークおよびデバイス設定の管理)、管理対象ファイアウォールのWebイ ンターフェイス(コンテクストの切り替え)および管理対象ファイアウォールのRESTAPI対し て、デバイスグループとテンプレートの管理者が与えられているアクセス権限を管理します。 最大で 4,000 個のアクセスドメインを定義してローカルで管理できます。また、RADIUS ベン ダー固有属性(VSA)、TACACS+ VSA、または SAML 属性を使用してそれらを管理することも できます。アクセスドメインを作成するには、ドメインを Add(追加)し、以下の表の説明に 従って設定を指定します。

アクセスドメイン設定	の意味
氏名	アクセスドメインの名前(最大 31 文字)を入力します。この 名前は、大文字と小文字が区別され、一意でなければならず、 文字、数字、ハイフン、アンダースコアのみで構成されます。
共有オブジェクト	共有場所からこのアクセスドメイン内のデバイスグループに 継承されるオブジェクトに対するアクセス権限を次のうちから 1つ選択します。権限に関係なく、管理者は共有オブジェクト またはデフォルト (事前定義済み) オブジェクトをオーバーライ ドできません。
	 read[読み取り] – 管理者は共有オブジェクトの表示とコ ピーができますが、共有オブジェクトに対してその他の操 作を実行することはできません。非共有オブジェクトの追 加または共有オブジェクトのコピーを行う場合、宛先を、 共有ではなく、アクセスドメイン内のデバイス グループに する必要があります。
	• write[書き込み] – 管理者は共有オブジェクトに対してすべての操作を実行できます。これがデフォルトの値です。
	 shared-only[共有のみ] – 管理者はオブジェクトを共有にの み追加できます。管理者は、共有オブジェクトの表示、編 集、および削除もできますが、共有オブジェクトの移動と コピーはできません。これを選択すると、管理者は、非共 有オブジェクトに対して表示以外のどの操作も実行できな くなります。
デバイスグループ	特定のデバイスグループに対する読み取り/書き込みアクセス を有効化あるいは無効化します。Enable All[すべて有効化]また はDisable All[すべて無効化]をクリックすることもできます。 あるデバイス グループに対して読み書きアクセス権を有効に すると、その子孫のデバイス グループに対して同じアクセス

アクセスドメイン設定	の意味
	権が自動的に有効になります。子孫のデバイス グループを手 動で無効にすると、その最上位の先祖のデバイス グループに 対するアクセス権が読み取り専用に自動的に変更されます。デ フォルトでは、すべてのデバイス グループに対してアクセス 権は無効になっています。
	リストに特定のデバイス グループのみを表示する場合、デバ イス グループ名を選択し、Filter Selected(選択項目でフィル タ)を行います。
	 共有オブジェクトに対するアクセス権を shared- only (共有のみ) に設定した場合、読み書きア クセス権を指定したすべてのデバイス グルー プに読み取り専用アクセス権が割り当てられま す。
テンプレート	割り当てるテンプレートまたはテンプレート スタックごと に、Add[追加] をクリックし、ドロップダウンリストからテン プレートまたはテンプレート スタックを選択します。
デバイス コンテクスト (アクセス ドメイン ページ のデバイス/仮想システムの 列に対応しています)	ローカル設定を行う管理者がコンテクストを切り替えるこ とのできるファイアウォールを選択します。リストに多くの ファイアウォールが表示される場合、Device State[デバイス状 態]、Platforms[プラットフォーム]、Device Groups[デバイス グループ]、Templates[テンプレート]、Tags[タグ]、および HA Status[HA 状態] でリストをフィルタリングできます。
ログ コレクタ グループ	割り当てるコレクタ グループごとに、ドロップダウンリスト からテンプレートまたはテンプレート スタックを選択してAdd (追加)します。

Panorama >スケジュール設定プッシュ

構成の変更を管理ファイアウォールにプッシュする場合の操作オーバーヘッドを単純化するに は、スケジュール設定プッシュを作成して、指定した日時に管理対象ファイアウォールに変更を 自動的にプッシュします。スケジュール設定のプッシュは、1回だけ実行するか、定期的なスケ ジュールで実行するように構成できます。

次のトピックでは、スケジュールされた構成プッシュに関する追加情報を提供します。

知りたい内容	以下を参照。
スケジュール設定プッシュを追加しま す。	スケジュール設定プッシュスケジューラ
スケジュール設定のプッシュ履歴を表 示します。	スケジュール設定のプッシュ実行履歴

スケジュール設 定のプッシュ情 報	の意味
名前	構成プッシュ スケジュールの名前。
Admin Scope (管理範囲)	他の管理者が行った構成変更をスケジュールされた構成に追加します。他 の管理者の構成変更をプッシュする機能は、Panorama 管理者ロールプロ ファイル (Panorama > Admin Roles) で定義されています。 <usernames> リ ンクをクリックして管理者を選択し、OK をクリックして他の管理者によ る構成変更を表示および選択します。 自分の役割で他の管理者の変更をプッシュできる場合でも、プッシュス コープには既定で自分の変更のみが含まれます。</usernames>
無効化	プッシュされたスケジュール設定が有効 (オフ) であるか、または無効 (オ ン) になっているか表示されます。
日付	日付(YYY/MM/DD)次の設定プッシュが行われる予定です。
繰り返し	スケジュールされた設定プッシュが1回のプッシュか、定期的なスケ ジュールプッシュ(月、週、または日)であるか。
時間	定期的なスケジュールでは、時刻(hh:mm)と構成プッシュが実行される 予定日。

スケジュール設 定のプッシュ情 報	の意味
	1 回限りのスケジュールでは、スケジュールされた構成プッシュがスケ ジュールされている時間(hh:mm)が実行されるようにスケジュールされ ます。
ステータス	最後にスケジュールされた構成プッシュの実行ステータス。スケジュー ルされた構成プッシュに関連付けられているすべての管理対象ファイア ウォールの完全な実行履歴を表示する場合にクリックします。
デバイス	スケジュールされた構成プッシュによる影響を受けた管理されたファイア ウォール。デバイス グループとテンプレートの変更に基づいて、影響を受 けたファイアウォールを表示します。

スケジュール設定プッシュスケジューラ

プッシュが発生するタイミングと頻度、どのデバイス グループとテンプレート構成をプッシュ し、どの管理対象ファイアウォールにプッシュするかをスケジュール パラメータを設定して、 管理されたファイアウォールへのスケジュールプッシュを作成します。デバイス グループまた は テンプレートの 最終コミット ステータスが out-of-syncである場合、Panorama はスケ ジュールされたデバイス グループとテンプレート構成のプッシュをマネージド ファイアウォー ルに実行します。

スケジュール された構成プッ シュ設定	詳説
名前	構成プッシュ スケジュールの名前。
無効化	スケジュール設定のプッシュを無効にする場合にオンにします。スケ ジュールされた構成プッシュを再度有効にするには、オフにします。
タイプ	特定の日時>設定をスケジュールするには、スケジュールを選択します。構成プッシュをスケジュールするには、定期的なスケジュール を選択します
日付	次の構成プッシュが実行される予定日。
時間	スケジュールされた構成プッシュ Date. で構成プッシュが実行されるよう にスケジュールされている時刻 (hh:mm:ss)
繰り返し	スケジュールされた構成プッシュが1回のプッシュ (なし) か、定期的なス ケジュールプッシュ (月、毎週、または 日単位 であるかどうか)。デフォル ト設定は None (なし) です。

スケジュール された構成プッ シュ設定	詳説
プッシュスコーン	プの選択
デバイスグルー プ	1つ以上のデバイス グループに関連付けられている管理対象ファイア ウォールを選択します。
	 デバイス候補の構成 とマージ(デフォルトで有効): Panorama からプッシュされた構成変更を、ターゲットファイアウォールにローカルで実装された保留中の構成変更とマージします。このプッシュは、マージされた変更をコミットする PAN-OS[®] ソフトウェアをトリガーします。この選択を無効にすると、ファイアウォールの候補構成はコミットによって除外されます。 デバイス テンプレートとネットワーク テンプレートを含める(デフォルトで有効):デバイスグループの変更と関連するテンプレートの変更の両方を、選択したファイアウォールと仮想システムに1回の操作でプッシュします。これらの変更を個別の操作としてプッシュするには、このオプションを無効にします。
テンプレート	 1つ以上のテンプレートスタックに関連付けられている管理ファイア ウォールを選択します。 デバイス候補の構成とマージ(デフォルトで有効): Panoramaからプッ シュされた構成変更を、ターゲットファイアウォールにローカルで実装 された保留中の構成変更とマージします。このプッシュは、PAN-OS ソ フトウェアをトリガーしてマージされた変更をコミットします。この選 択を無効にすると、ファイアウォールの候補構成はコミットによって除 外されます。

スケジュール設定のプッシュ実行履歴

スケジュールされた構成プッシュ実行履歴を表示して、特定のスケジュールの最後のプッシュが いつ発生したのかを把握し、影響を受けた管理されたファイアウォールの数を確認します。影響 を受ける管理対象ファイアウォールの総数から、管理対象ファイアウォールへの構成プッシュが 成功した回数と失敗した数を表示できます。失敗したプッシュのうち、管理対象ファイアウォー ルと Panorama 間の接続が切断または中断されたために、自動的に復元された構成を持つ管理対 象ファイアウォールの合計数を表示できます。

実行履歴情報	の意味
最終プッシュ時	スケジュールされた設定プッシュが発生した時刻(MM/DD / YYY
刻	HH:MM:SS)。

1351

実行履歴情報	の意味
デバイス	スケジュールされた構成プッシュに関連付けられた管理対象ファイア ウォールの合計数。
成功	プッシュが成功したスケジュール済み構成プッシュに関連付けられた管理 対象ファイアウォールの合計数。
失敗	プッシュが失敗したスケジュール済み構成プッシュに関連付けられた管理 対象ファイアウォールの合計数。
元に戻す	スケジュールされた構成のプッシュが失敗し、構成が元に戻された管理対 象ファイアウォールの合計数。
タスク	Panorama タスク マネージャーと構成プッシュに関連付けられているジョ ブを表示します。

Panorama > Managed Devices (管理対象デバイス)

Panorama が管理する Palo Alto Networks ファイアウォールを管理対象のデバイスといいま す。Panorama は同じメジャー リリースまたは以前のメジャー リリースを実行しているファイ アウォールを管理できますが、より新しいメジャー リリースを実行しているファイアウォール を管理できません。たとえば、PAN-OS 11.1 を実行している Panorama は、PAN-OS 11.1 以前 を実行している firewall を管理できます。また、Panorama より新しいメンテナンス リリースを 実行しているファイアウォールを管理することはお勧めしません。機能が期待どおりに機能し ない可能性があります。例えば、Panorama が PAN-OS 10.0.0 を実行している場合、PAN-OS 10.0.1 以降のメンテナンス リリースを実行しているファイアウォールを管理することは推奨さ れません。リリース情報の詳細については、PAN-OS 11.1 リリース ノート を参照してくださ い。サポートされている PAN-OS バージョンの詳細は End-of-Life Summary (サポート終了の概 要) を参照してください。

- 管理対象ファイアウォールの管理
- 管理対象ファイアウォールの情報
- ファイアウォールのソフトウェアとコンテンツの更新
- ファイアウォールのバックアップ

管理対象ファイアウォールの管理

ファイアウォールでは、以下の管理タスクを実行できます。

タスク	の意味
コンテキス トの	ファイアウォールを Add(追加)してシリアル番号を1行につき1つ入力 し、管理対象デバイスとして追加します。Managed Devices(管理対象デバイ ス)ウィンドウには、接続の状態、インストールされている更新、初期設定中 に設定されたプロパティなど、管理対象ファイアウォールの情報が表示されま す。
	Associate Devices (デバイスの関連付け)ボックスにチェックを入れ、ファイ アウォールをデバイスグループあるいはテンプレート スタックと関連付けま す。
	Panorama 管理サーバーが管理する、複数のファイアウォールを CSV 形式 でImport (インポート)します。サンプルの CSV ファイルをダウンロードでき ます。
	次に、各ファイアウォールの Panorama 管理サーバーの IP アドレスを入力し (「Device(デバイス)> Setup(セットアップ)> Management(管理)」 を参照)、Panorama でファイアウォールを管理できるようにします。

タスク	の意味
	⑦ ファイアウォールはAES-256により暗号化されたSSL接続を通じ てPanoramaに登録されます。Panoramaとファイアウォールは を2,048ビット証明書を使用して互いに認証をおこない、SSL接 続を使用して設定の管理とログ回収を行います。
Reassociate(関連付け)	再選択した一つ以上のファイアウォールを別のデバイスグループあるいはテンプ レート スタックに割り当て直します。
削除しま す。	Panoramaが管理するファイアウォールのリストからファイアウォールを削除 する場合は、1つ以上のファイアウォールを選択し、Delete (削除)します。
タグ	1つ以上のファイアウォールを選択し、Tag[タグ] をクリックして、最大31文 字のテキスト文字列を入力するか、既存のタグを選択します。空白は使用でき ません。Webインターフェイスに多くのファイアウォールが表示される場所 (ソフトウェアのインストール用のダイアログなど)では、タグを使用してリス トをフィルタリングできます。たとえば、「branch office」というタグを追加 すると、ネットワーク全体から支店のファイアウォールすべてを検索できま す。
インストー ル	ファイアウォールのソフトウェアおよびコンテンツ更新をInstall (インストー ル)します。
HA ピアのグ ループ化	高可用性(HA)設定のピアであるファイアウォールを Managed Devices(管理対象デバイス)ページでグループ化する場合は、Group HA Peers(HA ピアのグループ化)を選択します。この設定により操作の対象がグループ化され、各HAペアの両方のピアに操作を行うか、どちらにも操作を行わないかのいずれかに制限されます。
バックアッ プの管理	ファイアウォールのバックアップをManage (管理)します。
PDF/CSV	最低限の読み取り専用アクセス権を持つ管理ロールは、管理されるファイア ウォールのバンドルを PDF/CSV としてエクスポートできます。フィルターを 適用して、監査などのためのより具体的な表構成出力を作成することができ ます。Web インターフェイスで表示可能な列のみがエクスポートされます。 「Configuration Table Export(設定バンドルのエクスポート)」を参照してく ださい。
マスター キーのデプ ロイ	一つ以上のデバイスの新しいマスターキーをデプロイするか、既存のマスター キーを更新します。
Request OTP from CSP CSP か	管理されたファイアウォール用のワンタイムパスワード(OTP)を生成します。

タスク	の意味
ら OTP を要 求する	 カスタム選択デバイス:選択した管理対象ファイアウォール用の OTP を生成し、デバイス証明書をインストールして、パロアルトネットワークスクラウドサービスを活用します。
	 証明書のないデバイスをすべて選択:Palo Alto Networks クラウド サービス を活用するために、デバイス証明書が正常にインストールされていない管 理対象ファイアウォール用の OTP を生成します。
Upload OTP OTPのアッ プロード	カスタマー サポート ポータルから生成された OTP を貼り付けて、すべての 管理対象ファイアウォールのデバイス証明書をインストールします。

管理対象ファイアウォールの情報

Panorama > Managed Devices(管理対象デバイス) > Summary(サマリ)を選択し、管理対象 ファイアウォールごとに以下の情報を表示します。

管理対象ファイアウォールの 情報	の意味
デバイス グループ	ファイアウォールがメンバーとなっているデバイス グルー プの名前が表示されます。デフォルトではこの列は非表示 ですが、任意の列ヘッダーのドロップダウンリストを選択 し、Columns > Device Group[列] > デバイス グループ] を選択 することでこの列を表示できます。
	ファイアウォールグループに応じて、ページにクラスタ内のデ バイスが表示されます。各クラスタにヘッダー行があり、デバ イスグループ名、割り当てられたファイアウォールの合計数、 接続されたファイアウォールの数、階層内のデバイスグルー プのパスが表示されます。例えば、Datacenter (2/4 Devices Connected)(データセンター(接続済みデバイス2/4))の場 合:Shared (共有) > Europe (欧州) > Data center(データ センター)は、Data center(データセンター)というデバイ スグループに4つのメンバーファイアウォールが存在し(その うち2つは接続済み)、そのデバイスグループは Europe(欧 州)というデバイスグループの子であることを示します。任 意のデバイス グループを折りたたんだり展開したりすること で、そのファイアウォールを非表示にしたり表示したりできま す。
デバイス名	ファイアウォールのホスト名またはシリアル番号が表示されま す。

管理対象ファイアウォールの 情報	の意味
	VM-Series NSXエディションファイアウォールの場合、ファイ アウォール名にはESXiホストのホスト名が付加されます。例え ば、PA-VMの場合:Host-NY5105
仮想システム(vsys)	Multiple Virtual Systems [複数の仮想システム] モードになって いるファイアウォール上で利用できる仮想システムが一覧表示 されます。
モデル	ファイアウォールのモデルを表示します。
tags	各ファイアウォール / 仮想システムに定義されているタグが表 示されます。
シリアル番号	ファイアウォールのシリアル番号が表示されます。
操作モード	ファイアウォールの運用モードを選択します。FIPS-CC または 通常になります。
IPアドレス	ファイアウォール/仮想システムのIPアドレスが表示されま す。
	IPv4-ファイアウォール/仮想システムの IPv4 アドレスです。
	IPv6-ファイアウォール/仮想システムの IPv6 アドレスです。
Variables 変数	テンプレート固有の変数定義を、テンプレートスタック内の デバイスからコピーするか、既存の変数定義を編集してデバ イスの一意の変数を作成して作成します。デバイスがテンプ レートスタックに関連付けられていない場合、この列は空に なります。デフォルトでは、変数はテンプレートスタック から継承されます。「Create or Edit Variable Definition on a Device(デバイスの変数定義の作成または編集)」を参照して ください。
テンプレート	ファイアウォールが属するテンプレートスタックが表示されま す。
ステータス	Device State [デバイス状態] – Panorama とファイアウォール 間の接続の状態が示されます:接続済みまたは切断
	VM-Series のファイアウォールには別の2つの状態が存在する 可能性があります。

管理対象ファイアウォールの 情報	の意味
	止) (Panorama > Device Deployment (デバイスのデプロ イ) > Licenses (ライセンス)) を選択して仮想マシンが 停止し、ファイアウォールのすべてのライセンス/資格が 削除されていることを示します。非アクティブ化プロセス によって VM-Series ファイアウォールのシリアル番号が削 除されるため、非アクティブ化されたファイアウォールは Panorama から切断されます。
	 Partially deactivated[部分的に停止] – Panoramaからライセンスの停止プロセスが開始されたが、ファイアウォールがオフラインであり、Panoramaがファイアウォールと通信できないためプロセスがすべて完了していないことを示します。
	HA Status[HAの状態]–ファイアウォールが、以下の状態にあ ることを示します。
	• Active [アクティブ] - 正常なトラフィック処理状態
	• Passive [パッシブ] - 正常なバックアップ状態
	 Initiating [始動中] - ファイアウォールの起動後最大60秒は この状態におかれます
	• Non-functional [機能停止中] - エラー状態
	 Suspended [保留中] - 管理者がファイアウォールをサスペン ドしていることを示します
	 Tentative [一時的な状態] - アクティブ/アクティブ環境にお けるリンクまたはパスのモニタリングイベント用
	Shared Policy [共有ポリシー] – ファイアウォールのポリシー とオブジェクト設定が Panorama と同期しているかどうかを示 します。
	Template [テンプレート] – ファイアウォールのネットワーク とデバイス設定がPanoramaと同期しているかどうかを示しま す。
状態(続き)	Certificate (証明書) – 管理対象デバイスのクライアント証明 書の状態を示します。
	 Pre-defined(事前定義済み) – 管理対象デバイスでは、 事前定義済み証明書を使用して Panorama で認証しています。
	 Deployed (デプロイ済み) – カスタム証明書が管理対象デバイスで正常にデプロイされています。

管理対象ファイアウォールの 情報	の意味
	 Expires in N days N hours (N 日と N 時間で期限切れ) – 現在インストールされている証明書は、30 日未満で期限切 れとなります。
	 Expires in N minutes (N 分で期限切れ) – 現在インストー ルされている証明書は、1 日未満で期限切れとなります。
	 Client Identity Check Passed (クライアントアイデンティ ティチェック合格) – 証明書の共通名は、接続中デバイス のシリアル番号と一致します。
	 OCSP Status Unknown (OCSP の状態不明) – Panorama では、OCSP の状態を OCSP レスポンダから取得できません。
	 OCSP Status Unavailable (OCSP の状態使用不可) – Panorama は OCSP レスポンダに接続できません。
	 CRL Status Unknown (CRL の状態不明) – Panorama は CRL データベースから失効状態を取得できません。
	 CRL Status Unavailable (CRL の状態使用不可) – Panorama は CRL データベースに接続できません。
	 OCSP/CRL Status Unknown (OCSP/CRL の状態不明) – 両方とも有効であるとき、Panorama は OCSP または失効の 状態を取得できません。
	 OCSP/CRL Status Unavailable (OCSP/CRL の状態使用不可) – 両方とも有効であるとき、Panorama は OCSP または CRL データベースに接続できません。
	 Untrusted Issuer(信頼されていない発行者) – 管理対象デ バイスにカスタム証明書がありますが、サーバーはそれを 検証していません。
	Last Commit State [最終コミット状態] – ファイアウォールで 最後のコミットが失敗したか、成功したかを示します。
ソフトウェア バージョ ン アプリケーションお よび脅威 アンチウイル ス URL フィルタリング GlobalProtect [™] クライアン ト WildFire	ファイアウォールに現在インストールされているソフトウェア とコンテンツのバージョンが表示されます。詳細は、「ファイ アウォールのソフトウェアとコンテンツの更新」を参照してく ださい。
バックアップ	PAN-OSはファイアウォール上のコミットを行う 際、Panoramaに対し自動的にファイアウォールの設定のバッ クアップを送信します。設定のバックアップを参照し、必要に 応じそれを読み込む場合はManage[管理]をクリックします。

管理対象ファイアウォールの 情報	の意味
	詳細は、「ファイアウォールのバックアップ」を参照してくだ さい。
最後のマスターキーのプッ シュ	Panorama からファイアウォールへのマスターキーのデプロイ ステータスを表示します。
	ステータス–最後に行ったマスターキーのプッシュのステー タスを表示します。Success (成功)あるいはFailed (失 敗)のいずれかになります。マスターキーが Panorama から ファイアウォールにプッシュされていない場合はUnknown (不明)が表示されます。
	タイムスタンプーPanorama から最後にマスターキーをプッ シュした日時を表示します。

Containers(コンテナ)–コンテナ化済アプリケーションのワークロードを Kubernetes クラ スタで保護するために CN シリーズのファイアウォールをデプロイした場合は、以下の列を 使用します。

Container Number of Nodes(ノードのコンテナ 数)	Panorama に登録されているmanagement plane (管理プレーン - MP) (CN-Mgmt) に接続されているコンテナ化済ファイア ウォール データ プレーン (CN-NGFW) の数を表示します。 値は、CN-Mgmt ポッドの各ペアに対して 0~30 の CN-NGFW
	ポッドが可能です。
Container Notes(コンテナ メモ)	将来使用

デバイス変数定義の作成

デバイスを最初にテンプレートスタックに追加すると、テンプレートスタック内のデバイスか らコピーされたデバイス固有の変数定義を作成するか、Panorama > Managed Devices (管理対 象デバイス) > Summary (サマリー)を使用してテンプレート変数定義を編集することができ ます。デフォルトでは、すべての変数定義はテンプレートスタックから継承され、個々のデバ イスの変数定義をオーバーライドしたり、削除したりすることはできません。IP アドレスオブ ジェクトと IP アドレス リテラル (IPネットマスク、IP 範囲、FQDN)を、設定のすべての領 域、IKE ゲートウェイ構成 (インタフェース) および HA 設定 (グループ ID) のインタフェース に置き換えることができます。

デバイス変数定義の作成に関 する情報	の意味	
テンプレート スタック内の別のデバイスからデバイスの変数定義を複製しますか?		
いいえ	既存の変数定義を表示し、必要に応じて編集します。 「Panorama > Templates(テンプレート) > Template Variables(テンプレートの変数)」を参照してください	
あり。	ドロップダウン リストで変数定義を複製するデバイスを選択 し、複製する特定の変数定義を選択します。	

ファイアウォールのソフトウェアとコンテンツの更新

管理対象のファイアウォールにソフトウェアまたはコンテンツのアップデートをインストール する場合は、まずPanorama > Device Deployment (デバイスのデプロイ)のページを開き、 アップデートのダウンロードまたはそれをPanoramaへアップロードします。次に、 Panorama > Managed Devices (管理対象デバイス)ページを選択し、Install (インストール)をクリックし て、以下のフィールドを設定します。

管理(MGT)インターフェイスのトラフィックを削減するには、更新のデプロ イのために個別のインターフェイスを使用するように Panorama を設定します (「Panorama > Setup(セットアップ) > Interfaces(インターフェイス)」を参 照)。

ファイアウォール用ソフト ウェア/コンテンツの更新の インストール オプション	の意味
タイプ	インストールする更新のタイプを以下の中から選択しま す。PAN-OS Software[ソフトウェア]、GlobalProtect Client software [GlobalProtect クライアントソフトウェア]、Apps and Threats signiatures [アプリケーションおよび脅威] の シグネチャ、Antivirus signiature [アンチウイルス] シグネ チャ、WildFire、またはURL Filtering[URLフィルタリング]
ファイル	更新イメージを選択します。ドロップダウン リストに は、 Panorama > Device Deployment (デバイスのデプロイ) ページで Panorama にダウンロードまたはアップロードしたイ メージのみが表示されます。
フィルタ	デバイスリストに適用するフィルタを選択します。
機器	イメージをインストールするファイアウォールを選択します。

ファイアウォール用ソフト ウェア/コンテンツの更新の インストール オプション	の意味
デバイス名	ファイアウォール名
現在のバージョン	現在ファイアウォールにインストールされている Type [タイプ] のファイアウォールの更新バージョンです。
HA 状態	 ファイアウォールが、以下の状態にあることを示します。 Active [アクティブ] - 正常なトラフィック処理状態 Passive [パッシブ] - 正常なバックアップ状態 Initiating [始動中] - ファイアウォールの起動後最大60秒はこの状態におかれます Non-functional [機能停止中] - エラー状態 Suspended [保留中] - 管理者がファイアウォールをサスペンドしていることを示します Tentative [一時的な状態] - アクティブ/アクティブ環境におけるリンクまたはパスのモニタリングイベント用
HA ピアのグループ化	高可用性(HA)設定のピアであるファイアウォールをグループ 化する場合に選択します。
フィルタが選択されていま す	デバイスリストに特定のファイアウォールのみを表示する場合、対応するデバイス名を選択し、Filter Selected[選択項目でフィルタ]を行います。
デバイスにのみアップロー ド	イメージをファイアウォールにアップロードした際、ファイア ウォールを自動的に再起動させない場合に選択します。イメー ジはファイアウォールを手動で再起動するまでインストールさ れません。
インストール後にデバイス を再起動(ソフトウェアの み)	ソフトウェア イメージをアップロードし、インストールする場 合に選択します。インストール プロセスによって再起動がトリ ガーされます。
コンテンツ更新で新しいア プリケーションを無効にす る(アプリケーションと脅 威のみ)	前回インストールした更新にはない、新しく含まれているアプ リケーションを無効化する場合に選択します。これにより最 新の脅威を防ぎながらも、ポリシーアップデートを行ったの ちに、アプリケーションを有効化していくといった柔軟な対 応が可能です。アプリケーションを有効化したい場合、ファ イアウォールにログインして、Device [デバイス] > Dynamic Updates[動的更新] を開き、機能の列にあるApps [アプリ] をク リックして新しいアプリケーションを表示し、有効化したいア

ファイアウォール用ソフト ウェア / コンテンツの更新の インストール オプション	の意味
	プリケーションごとに Enable/Disable [有効化/無効化] の設定を 選びます。

ファイアウォールのバックアップ

• Panorama > Managed Devices [Panorama > 管理対象デバイス]

Panoramaでは、設定の変更を管理対象ファイアウォールにコミットするたびにその変更内容が 自動的にバックアップされます。ファイアウォールのバックアップを管理する場合は Panorama > Managed Devices (管理対象デバイス)を選択し、ファイアウォールの Backups (バックアッ プ)列にある Manage (管理)をクリックし、以下のいずれかのタスクを行います。



Panoramaデバイスに保存するファイアウォールの設定バックアップ数を設定する場合は、Panorama > Setupセットアップ > Management管理の順に選択し、[ロギン グおよびレポート設定]を編集します。次に、Log Export and Reporting[ログのエク スポートとレポート] タブを選択して、Number of Versions for Config Backups[設定 バックアップのバージョン数] フィールドに値(デフォルトは100)を入力します。

タスク	の意味
保存またはコミットされた設定 の詳細を表示する。	バックアップのVersion[バージョン]列で、保存またはされ た設定のファイル名またはコミットされた設定のバージョ ンナンバーをクリックし、関連するXMLファイルの内容を 表示します。
保存またはコミットされた設定 を設定候補に復元する。	バックアップのAction[動作]列で、Load[ロー ド]とCommit[コミット]をクリックします。
	ファイアウォールの設定をロードすると、ローカルデバ イス設定が元に戻されますが、Panoramaからプッシュさ れた設定は戻りません。ファイアウォールのバックアッ プのロード後、コンテキストスイッチを使用してファイア ウォールのWebインターフェースに切り替えるか、ファイ アウォールのWebインターフェーススをCommit(コミッ ト)で起動する必要があります。
保存された設定内容を削除す る。	バックアップのAction[動作]列で、Delete[削 除](× をクリックします。

)

Panorama > Device Quarantine [Panorama > デバイス隔離]

Panorama > Device Quarantine(デバイス隔離) ページには、隔離リストに登録されているデバイスが表示されます。以下のアクションで、デバイスがこのリストに表示ます。

• システム管理者が、このリストに手動でデバイスを追加した。

デバイスを手動でAdd(追加)するには、Host ID(ホスト ID) およびオプションで、隔離の必要があるデバイスのSerial Number(シリアル番号)を入力します。

- システム管理者が、Traffic(トラフィック)、GlobalProtect、またはThreat(脅威)ログからHost ID(ホスト ID)列を選択し、その列でデバイスを選択した後、Block Device(デバイスをブロックする)を選択した。
- 一致リストに Quarantine(隔離) と設定された組み込みアクションをがあるログ転送プロ ファイルを持つセキュリティ ポリシールールにデバイスが一致した。
 - Host ID (ホスト ID) は、自動的に GlobalProtect ログに表示されます。Host ID (ホスト ID) を Traffic (トラフィック)、Threat (脅威)、またはUnified (統 合) ログに表示するには、Panorama アプライアンスに、Source Device (送信 元デバイス)がQuarantine (隔離) に設定されたセキュリティ ポリシー ルール が少なくとも 1 つ必要となります。この設定がセキュリティ ポリシーに存在し ないと、Traffic (トラフィック)、Threat (脅威)、またはUnified (統合) ロ グにHost ID (ホスト ID) が存在せず、ログ転送プロファイルは有効化されませ ん。
- APIを使用してデバイスが隔離リストに追加された。
- Panorama アプライアンスが、再配信されたエントリの一部として隔離リストを受け取った(隔離リストが別の Panorama アプライアンスまたはファイアウォールから再配信された)。

Device Quarantine (デバイス隔離) テーブルには、以下のフィールドが含まれます。

項目	の意味
ホストID	ブロックされたホストの Host-ID(ホストID)。
理由	デバイスが隔離された理由。 Admin Add(管理者追加) という 理由は、管理者が手動でデバイスを表に追加したことを意味しま す。
タイム スタンプ	管理者または Security(セキュリティ)ポリシー ルールがデバイ スを隔離リストに追加した時刻。
Source Device/App(送 信元デバイスまたはアプ リケーション)	デバイスを隔離リストに追加した Panorama、ファイアウォー ル、あるいはサードパーティのアプリケーションの IP アドレス。
シリアル番号	(オプション) 隔離されたデバイスのシリアル番号(既知の場 合)。

項目	の意味
ユーザー名	(オプション) 隔離される際にデバイスにログインし たGlobalProtect クライアントユーザーのユーザー名。

Panorama > Managed Devices (管理対象デバイス) > Health (健康状態)

Panorama[™]では、管理対象ファイアウォールのハードウェア リソースとパフォーマンスを監 視できます。Panorama は、時間推移のパフォーマンス情報(CPU、メモリ、CPS、スループッ ト)、ロギング パフォーマンス、環境情報(ファン、RAID ステータス、電源など)およびコ ミット、コンテンツのインストール、ソフトウェア アップグレードなどのイベントを一元管理 します。ファイアウォールが計算されたベースラインから逸脱すると、Panorama はそれを逸脱 デバイスとして報告し、ハードウェアの問題を迅速に特定、診断、解決します。

このページでは次の操作も可能です。

詳細なデバイスヘルスチェックの閲覧。	Panoramaで管理されているデバイスの チェックステータス基準を閲覧する。
HA ピアのグループ化	潜在的な問題を特定し、ハードウェア リソー スやパフォーマンスの問題の影響を受ける ファイアウォールがあるかどうかを判断する ために、どのファイアウォールがグループ化 されているかを確認します。
PDF/CSV	最低限の読み取り専用アクセス権を持つ管理 ロールは、管理されるファイアウォールのバ ンドルを PDF/CSV 形式でエクスポートでき ます。フィルターを適用して、監査などで必 要なより具体的な表構成出力を作成すること ができます。Web インターフェイスで表示 される列のみエクスポートされます。Export Configuration Table Data(設定バンドルデー タのエクスポート)を参照してください。

Panorama > Managed Devices(管理対象デバイス) > Health(健康状態) > All Devices(全てのデバイス)

このページを使用して、各ファイアウォールについて次の情報を表示します。

ヘルスチェック情報	の意味
デバイス名	ファイアウォールのホスト名またはシリアル番号。

ヘルスチェック情報	の意味
	VM-Series NSXエディションファイアウォールの場合、ファイ アウォール名にはESXiホストのホスト名が付加されます。例え ば、PA-VMの場合:Host-NY5105
モデル	ファイアウォールのモデル。
デバイス	
スループット (キロビット)	時間経過に対するデータ スループット (5 分の平均) をキロ ビット/秒で測定します。
毎秒コネクション数 (CPS)	ファイアウォールの1秒あたりの総接続数(平均5分)。
セッション	
カウント(セッション)	時間の経過に伴う合計セッション数(平均5分)。
データ プレーン	
CPU (%)	データ プレーンの総 CPU 使用率。
管理プレーン(MP)	
CPU (%)	管理プレーンの総 CPU 使用率。
MEM (%)	管理プレーンの総メモリ使用率。
ロギング率(1 秒あたりの ログ数)	管理対象ファイアウォールの受信ログレート。
ファン情報	各ファントレイのファンの有無、現在の状態、RPM、およ び最後に障害が発生した日付を表示します。ファンの状態 は、A/B で表示されます。A は良好な稼働中のファンの数、B はファイアウォール上のファンの総数です。仮想ファイア ウォールは N/A で表示されます。
電源	パワーサプライの有無、現在の状態、最後に障害が発生した 日付のタイムスタンプを表示します。パワーサプライの状態 は、A/B で表示されます。A は良好な稼働中のパワーサプライ の数、B はデバイスに付いているパワーサプライの総数です。 仮想ファイアウォールは N/A で表示されます。
ポート	ファイアウォールで使用されている合計ポート数が表示されま す。ポートは、A/B で表示されます。A は良好な稼働中のポー トの数、B はデバイス上のポートの総数です。

Panorama > Managed Devices(管理対象デバイス) > **Health**(健康状態) > **Deviating Devices**(逸脱デバイス)

逸脱デバイス タブには、計算されたベースラインから逸脱しているメトリックを持つデバイス が表示され、その偏差メトリックが赤色で表示されます。ヘルスチェックベースライン測定指標 により、7日間にわたる所定のメトリックヘルスチェックパフォーマンスを平均化し、標準偏差 を加算することによって決定されます。

Al	All Devices Devices											
Q	Q.(4									4 it		
				Device		Session	Data Plane	Manager	nent Plane			
	DEVICE NAME	MODEL	HA STATUS	THROUGHPUT (KBPS)	CPS	COUNT (SESSIONS)	CPU (%)	CPU (%)	MEM (%)	LOGGING RATE (LOG/SEC)	FANS	POWE
	PA-7080	PA-7080		24117127	100992	23368878	30	18	13	0	18/18	2/8
		PA-5220	Active Primary	0	0	0	0	13	14	0	8/8	2/2
	Contract of the second s	PA-5220	Active Secondary	1	0	0	0	1	10	0	8/8	2/2
	PA-3260	PA-3260		8999	12658	63772	7	22	23	11329	3/3	2/2

図1:逸脱測定の例

Detailed Device Health on Panorama(Panorama のデバイス健康 状態詳細)

All Devices(すべてのデバイス)タブまたは Deviating Devices(逸脱デバイス)タブの Device Name(デバイス名)をクリックすると、個々のファイアウォールの詳細なデバイス健康状態履 歴を表示できます。Detailed Device(デバイス詳細)ビューは、時間フィルタを使用して健康状 態履歴を提供し、デバイスに関連付けられたメタデータを表示します。デバイスの健康状態情報 は、時間軸のデータをグラフで表示できるように、表またはウィジェットとして表示されます。

Manage the Detailed Device View (デバイス詳細ビューの管理)

Detailed Device(デバイス詳細)ビューには、ファイアウォールに関連付けられている説明メタ データとともに詳細なファイアウォールの健康状態情報が表示されます。該当する場合は、ウィ ジェットの追加オプションについては設定 (20) を、ウィジェットを拡大するには最大化パネル () を設定します。

項目	の意味
操作	
Time Filter(時間フィル タ)	ドロップダウンからデバイス健康状態を表示するには、時間 フィルタを選択します。時間フィルタは、Last 12 hours(12 時間前)、24 hours(24 時間)、7 days(7 日), 15 days(15日)、30 days(30 日)、または90 days(90日)か ら選択できます。
Show Average 平均を表示	すべての時間推移ウィジェットに表示される平均および標準 分布を選択します。None(なし)、Last 24 hours(24 時間

項目	の意味				
	前)、 7 days(7 日)、または 15 days(15 日)から選択でき ます。				
レートの	表示される情報を最新データに更新します。				
Print PDF(PDF で生成)	現在表示中のタブの PDF を生成します。				
	 ダウンロード場所を選択して PDF にアクセスするには、ポップアップを有効にする必要があります。 				

System Information (システム情報)

デバイスに関連する以下のメタデータです。IP アドレス、 ソフトウェアのバージョン、ウィルス対策ソフトのバー ジョン、HA 状態、シリアル番号、アプリと脅威のバージョ ン、Wildfire のバージョン、VSYS モード、モデル、およびデ
バイス モード。

セッション数

Sessions(セッション)タブにはファイアウォールを通過するセッション情報が表示されます。 この情報は6つのグラフで個別に表示されます。

項目	の意味
スループット	キロビット/秒 (Kbps) 単位で測定されたデータ スループット (平均5分間)。
セッション数	時間の経過に伴う合計セッション数(平均5分)。
Connections per Second(接続数/秒)	時間に対するデバイスの合計CPS(平均5分)
Packets per Second(毎秒パ ケット数)	デバイスを通過した1秒あたりの合計パケット数(平均5 分)
Global Session Table Utilization(グローバル セッション テーブル使用 率)(PA-7000、PA-5200 アプライアンスのみ)	グローバル セッション テーブルを持つファイアウォール(平 均 5 分)に対するグローバル セッション テーブルの時間に対 するパーセンテージ。

項目	の意味
Session Table Utilization(セッション テーブル使用率)	ファイアウォールの各データプレーンに対するセッション テーブル使用率の時間に対する割合(平均5分)を示します。
SSL Decrypted Sessions Info(SSL 復号化処理 セッ ション数)	時間の経過とともに暗号化された SSL セッションの数を示します(平均 5分)。
SSL Proxy Session Utilization(SSL 復号化処理 セッション使用率)	時間経過に伴うプロキシ セッションの利用率を示します(平 均 5 分)。

Environments(環境)

Environments(環境) タブには、パワーサプライ、ファン トレイ、ディスクドライブなどの ハードウェアの有無、状態、および動作状態が表示されます。このタブには以下のハードウェア ベースのファイアウォールのみ表示されます。

項目	の意味
Fan Status(ファンの状 態)	各ファントレイのファンの有無、現在の状態、RPM、およ び最後に障害が発生した日付を表示します。ファンの状態 は、A/B で表示されます。A は良好な稼働中のファンの数、B はファイアウォール上のファンの総数です。仮想ファイア ウォールは N/A で表示されます。
Power Supply(パワー サプ ライ)	パワーサプライの有無、現在の状態、最後に障害が発生した 日付のタイムスタンプを表示します。パワーサプライの状態 は、A/B で表示されます。A は良好な稼働中のパワーサプライ の数、B はデバイスに付いているパワーサプライの総数です。 仮想ファイアウォールは N/A で表示されます。
Thermal Status(熱状態)	デバイスの各スロットに関連するすべての熱アラームを表示し ます。アクティブなアラームがある場合、ファイアウォールは 正確な温度と場所に関するより詳しい情報もここに表示されま す。
System Disk Status(システ ム ディスク ステータス)	root、pancfg、panlogs、および panrepo マウントの使用可 能、使用中、および使用率を表示します。 システム ディスク ステータスには、RAID が有効になっている ファイアウォールのディスク名、サイズ、および RAID ステー タスも表示されます。
インターフェイス

(インターフェイス)タブには、ファイアウォール上のすべての物理インターフェイスのステー タスと統計情報が表示されます。

項目	の意味
インターフェイス名	インターフェイスの名称。インターフェイスを選択すると、選択したインターフェイスのBit Rate(ビットレート)、Packets per Second(1秒あたりのパケット数)、Errors(エラー)、 およびDrops(ドロップ)のグラフが表示されます。
ステータス	インターフェイスのステータス。Admin Up,Admin Down, Operational Up、または Operational Down。
Bit Rate ビットレート	送受信されたデータのビットレート(bps)を表示します。
Packets per Second(毎秒パ ケット数)	送受信されたデータの1秒あたりのパケット数を表示します。
エラー	送受信されたデータのエラー数を表示します。
Drops(破棄)	送受信されたデータでドロップした接続数を表示します。
スループット	キロビット/秒 (Kbps) 単位で測定されたデータ スループット (平均5分間)。

ロギング

(ロギング)タブには、ファイアウォールを管理するロギングレートと接続が表示されます。

項目	の意味
ロギング率	Panorama またはLog Collector (ログコレクタ) へのデバイス 転送ログの1分間の平均レートを表示します。
Logging Connections(ロギ ング接続)	使用可能なすべてのログ転送接続(アクティブまたは非アク ティブのステータスを含む)を表示します。
External Log Forwarding(外部ログ転 送)	さまざまな種類の外部ログ転送方式の送信、ドロップ、平均転 送速度(1 秒あたりのログ数)を表示します。

リソース

(リソース)タブには、ファイアウォールの CPU とメモリの統計情報が表示されます。

項目	の意味
Management Plane Memory(管理プレーンの メモリ)	管理プレーン メモリの時間推移 5 分間平均をパーセントで表示します。
Packet Buffers(パケット バッファ)	パケット バッファ 使用率の時間推移 5 分間平均をパーセン トで表示します。複数のデータ プレーン システムでは、この ディスプレイには異なる色の異なるデータプレーン、CPU、お よびパケット バッファが含まれています。
Packet Descriptors(パケッ ト記述子)	パケット記述子の使用率の時間推移 5 分間平均をパーセントで 表示します。複数のデータ プレーン システムでは、このディ スプレイには異なる色の異なるデータプレーン、CPU、および パケット バッファが含まれています。
CPU Management Plane(CPU 管理プレー ン)	管理プレーン CPU の時間推移 5 分間平均を表示します。
CPU Data Plane(CPU デー タ プレーン)	データプレーン CPU の時間あたりの平均 5 分間の平均コア使 用率を表示します。複数のデータプレーンを持つシステムで は、表示するデータプレーンを選択できます。
Mounts(ディスク領域使用 状況)	デバイス システム ファイル情報を表示します。ディスク領 域使用状況のName(名前)、Allocated(割り当て済み) (KB)、Used(使用済み)(KB)、およびAvail(使用可能) (KB)の各領域、およびUtilization(使用)率が表示されま す。

HA

(高可用性)タブには、ファイアウォールの HA ステータスとその HA ピアが表示されます。一番上のウィジェットには、デバイスとそのピアの設定とコンテンツのバージョンが表示されます。下のウィジェットには、前の HA フェールオーバーに関する情報と、それに関連する理由 (障害が発生したファイアウォールを含む)が表示されます。

Panorama > Templates [Panorama > テンプレート]

Device(デバイス)および Network(ネットワーク)タブでは、テンプレートまたはテンプ レート スタック(テンプレートの組み合わせ)を使用して、類似の設定を必要とする複数の ファイアウォールに共通の基本設定を適用できます。Panorama でファイアウォール設定を管理 する場合、デバイス グループ とテンプレートの組み合わせを使用します。デバイス グループで は、共有するポリシーおよびオブジェクトを管理し、テンプレートでは、共有するデバイスおよ びネットワーク設定を管理します。

テンプレートまたはテンプレート スタック作成用ダイアログで使用できる設定に加え て、Panorama > Templates(テンプレート)では以下の列が表示されます。

• **Type**[タイプ] - 記載されたエントリが、テンプレートあるいはテンプレートスタックのどちら であるかを示します。

操作	以下を参照
テンプレートを追加、コ ピー、編集、または削除する	テンプレート
テンプレート スタックの追 加、編集、または削除	テンプレート スタック
その他の情報をお探しです か?	テンプレートおよびテンプレート スタック テンプレートおよびテンプレート スタックの管理

• Stack[スタック] - テンプレートスタックに割り当てられたテンプレートを一覧表示します。

テンプレート

Panorama では、最大 1,024 個のテンプレートがサポートされます。以下の表に記載されてい るように、テンプレートを Add(追加)して設定てきます。テンプレートを作成した後、ファ イアウォールを管理する前に Configure a Template Stack(テンプレート スタックを設定)し、 テンプレートとファイアウォールをテンプレート スタックに追加する必要があります。テン プレートの設定後、Panorama で変更をコミットする必要があります(「Panorama Commit Operations(Panorama のコミット操作)」を参照)。



テンプレートを削除しても、Panorama によってファイアウォールにプッシュされ た値は削除されません。

テンプレートの設定	の意味
名前	テンプレート名を入力します(最大 63 文字)。この名前では、大文字と 小文字が区別されます。また、一意のものにしてください。文字、数

テンプレートの設定	の意味
	字、スペース、ハイフン、ピリオド、アンダースコアのみ使用できま す。
	この名前は、Device(デバイス)タブと Network(ネットワーク)タ ブの Template(テンプレート)ドロップダウン リストに表示されま す。これらのタブで変更した設定は、選択したTemplate[テンプレー ト]にのみ適用されます。
の意味	テンプレートの説明を入力します。

テンプレートスタック

テンプレートスタックを構成したり、テンプレートをテンプレートスタックに割り当てるこ とができます。ファイアウォールをテンプレートスタックに割り当てると、すべての設定を 各テンプレートに個別に追加するのではなく、ファイアウォールに必要な設定をすべてプッ シュすることができます。Panorama では、最大 1,024 個のスタックがサポートされます。Add Stack (スタックを追加)を利用して新しいテンプレートスタックを作成し、次の表の説明に 従って設定を構成できます。テンプレートスタックの設定後、Panorama で変更をコミットする 必要があります (「Panorama Commit Operations(Panorama のコミット操作)」を参照)。ま た、スタックに割り当てられたファイアウォールのネットワークとデバイスの設定を行った場合 は、テンプレートコミットを行い、設定をファイアウォールへプッシュする必要があります。

テンプレートスタックを削除したり、テンプレートスタックからファイアウォー ルを除外したりしても、Panoramaが以前そのファイアウォールにプッシュした値 は削除されません。ただし、テンプレートスタックからファイアウォールを除外 すると、Panoramaは新しい更新をそのファイアウォールにプッシュしなくなりま す。

テンプレート スタックの設定	の意味
氏名	スタック名 (最大 31 文字) を入力します。この名前は、大文 字と小文字が区別され、一意でなければならず、文字から 始まり、文字、数字、ハイフン、アンダースコアのみで構 成されます。スタック名および割り当てられたテンプレー トは、Device(デバイス)タブと Network(ネットワー ク)タブの Template(テンプレート)ドロップダウンリス トに表示されます。
の意味	スタックの説明を入力します。
softwareデバイス がPanoramaに登録されると自 動的にコンテンツをプッシュ する	Panorama で VM-Series または CN シリーズ firewalls をオ ンボーディングすると、最新のコンテンツ更新が自動的に firewall にプッシュされます。

テンプレート スタックの設定	の意味
テンプレート	スタックに組み込む各テンプレートを Add(追加)します (8 個まで)。
	テンプレートに設定が重複している場合、割り当てられた ファイアウォールに設定をプッシュするときに、リストの 上位にあるテンプレートの設定だけが Panorama によって プッシュされます。たとえば、テンプレート_A がリスト内 でテンプレート_B よりも上にあり、この2つのテンプレー トで Ethernet1/1 インターフェイスが定義されているとし ます。この場合、Panorama は Ethernet1/1 の定義をテン プレート_A からプッシュし、テンプレート_B からはプッ シュしません。リスト内のテンプレートの順番を変更する には、テンプレートを選択して Move Up(上へ)または Move Down(下へ)移動します。
	 Panorama では、スタック内のテンプレートの組み合わせが検証されないため、無効な関係が生じないように plan the order (順番付け)を行ってください。
機器	スタックに追加したいファイアウォールをそれぞれ選択し ます。
	リストに多くのファイアウォールが表示される場 合、Platforms(プラットフォーム)、Device Groups(デ バイス グループ)、Tags(タグ)、および HA Status(HA 状態)でリストをフィルタリングできます。
	 モード (VPN モード、マルチ vsys モード、または操作モード)が一致していない複数のファイアウォールを同じスタックに割り当てることができます。Panoramaは、モード固有の設定を、そのモードをサポートするファイアウォールにのみプッシュします。
すべて選択	リスト中の全てのファイアウォールを選択します。
すべての選択を解除	リスト中の全てのファイアウォールの選択を解除します。
HA ピアのグループ化	高可用性(HA)ピアであるファイアウォールをグループ化 します。HA に設定されたファイアウォールを簡単に識別 できるようになります。テンプレートスタックから設定を プッシュする場合は、個々のファイアウォールではなくグ ループ化されたペアにプッシュできます。

テンプレート スタックの設定	の意味
フィルタが選択されています	特定のファイアウォールのみを表示するには、該当のファ イアウォールを選択して、Filter Selected[選択項目でフィル タ]を実行します。
ユーザー ID マスター デバイス	Panorama をマッピング用の User-ID Master Device として 設定します。
Cloud Identity Engine	Add は、Cloud Identity Engine で構成した認証プロファイル を使用してユーザーを認証するための Cloud Identity Engine インスタンスです。
テンプレート	Add または Delete は、構成済みのテンプレートで す。Move Up または Move Down テンプレートを使用して 優先度を変更します。上部のテンプレートの優先順位が最 も高くなります。

Panorama > Templates(テンプレート) > Template Variables(テ ンプレートの変数)

- テンプレート変数の新規作成
- 既存のテンプレート変数の編集
- デバイスの変数定義の作成または編集

テンプレートやテンプレートスタックの変数(Panorama > Templates(テンプレート)) を定義することも、個々のデバイス(Panorama > Managed Devices(管理対象デバイス) > Summary(サマリー))の既存の変数を編集することもできます。変数は、パノラマを使用し てファイアウォール設定を管理するときに、柔軟性と再利便性を提供するテンプレートまたはテ ンプレートスタックで定義された設定コンポーネントです。変数を使って以下の項目を置き換 えることができます。

- 設定のすべての領域における IP アドレス(IP ネットマスク、IP 範囲、および FQDN を含む)。
- IKE ゲートウェイ設定(インターフェイス)および HA 設定(グループ ID)のインターフェ イス。
- SD-WAN 設定の設定要素(AS 番号、QoS プロファイル、最大出口、リンク タグ)。

ファイアウォールをテンプレート スタックに追加すると、テンプレートまたはテンプレート ス タック用に作成した変数が自動的に継承されます。

テンプレート変数情報	の意味
氏名	変数定義の名称。

テンプレート変数情報	の意味
テンプレート(デバイスと テンプレート スタック)	変数定義が属するテンプレートの名前を表示します。
タイプ	変数定義のタイプを表示します。
	 IP Netmask(IP ネットマスク) –静的 IP またはネットワーク アドレスを定義します。
	 IP Range(IP 範囲) – IP 範囲を定義します。たとえば、 「192.168.1.10-192.168.1.20」と入力します。
	• FQDN-完全修飾ドメイン名を定義します。
	 Group ID (グループ ID) –高可用性グループ ID を定義します。詳細は、「Configuration Guidelines for Active/Passive HA(アクティブ/パッシブ HAの設定ガイドライン)」を参照してください。
	 Device Priority (デバイスの優先順位) – デバイスの優先度 を定義し、アクティブ-パッシブ高可用性(HA)構成で、ア クティブロールを担うファイアウォールの優先度を示しま す。
	 Device ID(デバイス ID) – アクティブ-アクティブ高可用 性(HA)構成でデバイス優先度の値の割り当てに使用する デバイス ID を定義します。
	 Interface (インターフェイス) –ファイアウォール上のファ イアウォール インターフェイスを定義します。IKE ゲート ウェイ設定にのみ使用可能です。
	 AS Number (AS 番号) – BGP 設定で使用する自律型システム番号を定義します。
	 QoS Profile (QoS プロファイル) –QoS 設定で使用する Quality of Service (クオリティ オブ サービス - QoS) プロ ファイルを定義します。
	• Egress Max(最大保証帯域 出力側)QoSプロファイル設 定で使用する出力最大値を定義します。
	 Link Tag (リンク タグ) – SD-WAN 設定で使用するリンク タグを定義します。
值	変数定義用に設定された値を表示します。
追加(テンプレートとテン プレート スタック)	新しいテンプレート変数定義を Add (追加) します。
削除します。	既存のテンプレート変数定義を削除します。

テンプレート変数情報	の意味
コピー	既存のテンプレート変数定義を複製します。
オーバーライド(テンプ レート スタックとデバイ ス)	テンプレートスタックまたはデバイスから継承した既存のテン プレート変数定義をオーバーライドします。変数のタイプまた は名前を変更することはできません。また、デバイス固有の変 数をオーバーライドすることはできません。
元に戻す(テンプレート ス タックとデバイス)	テンプレートスタックまたはデバイスレベルでオーバーライ ドされた値をクリアするには 上書きされた変数を元のテンプ レート変数定義に戻します。
デバイスのみで使用される 値を取得する(デバイスの み)	選択した変数に、ファイアウォールで使用されている値を入力 します。Panorama が値を取得する前に、テンプレートまたは テンプレートのスタック変数を定義してファイアウォールに プッシュする必要があります。ファイアウォールから取得さ れた値は、テンプレートまたはテンプレートスタック変数を Override(オーバーライド)上書きして、デバイス固有の変数 を作成します。変数定義がファイアウォールにプッシュされて いない場合、Panorama はその変数に Value not found(値 が見つかりません)を返します。

テンプレート変数の新規作成

新しいテンプレート変数定義をAdd(追加)します。

テンプレート変数定義の新規 作成に関する情報	の意味
氏名	変数定義の名称。すべての変数定義名は、ドル記号(「 \$ 」) で始まる必要があります。
タイプ	変数定義のタイプを選択します。IP Netmask(IP ネット マスク)、IP Range(IPの範囲)、FQDN、Group ID(グ ループ ID)、Device Priority(デバイス優先度)、Device ID(デバイス ID)、Interface(インターフェース)、AS Number(AS番号)、QoS Profile(QoS プロファイ ル)、Egress Max(最大保証帯域 出力側)、または Link Tag(リンク タグ).
值	変数定義目的の値を入力します。

Panorama Web インターフェイス

既存のテンプレート変数の編集

テンプレートまたはテンプレートスタックのテンプレート変数定義は、変数を作成した後の 任意の時点(Panorama > Templates(テンプレート))で編集できます。テンプレート変数 をManage(管理)して変数を選択し、必要に応じて使用可能な値を編集します。

デバイスの変数定義の作成または編集

Panorama > Managed Devices(管理対象デバイス) > Summary(サマリー)に移動して、変数 定義を作成するか、Panorama テンプレートまたはテンプレート スタックからプッシュされたテ ンプレート変数を上書きします。テンプレート変数には以下が含まれます。

- 設定のすべての領域における IP アドレス(IP ネットマスク、IP 範囲、または FQDN)。
- IKE ゲートウェイ設定(インターフェイス)または HA 設定(グループ ID)のインターフェ イス。
- SD-WAN 設定の設定要素(AS 番号、QoS プロファイル、最大出口、リンク タグ)。

デバイス変数を作成すると、オーバーライドされたデバイス固有の変数を、個別に再作成する のではなく、同じテンプレートスタック内のデバイスからコピーすることができます。デフォ ルトでは、すべての変数定義はテンプレートまたはテンプレートスタックから継承され、オー バーライドのみ可能です。個々のデバイスの新しい変数定義を削除または作成することはできま せん。

テンプレートスタック内の既存のデバイスから変数定義をコピーするか、既存のデバイス変数定 義を Edit(編集)してデバイス変数定義を Create(作成)します。

Panorama > Device Groups [Panorama > デバイス グ ループ]

デバイス グループは、1つのグループとして管理するファイアウォールや仮想システムで構成 されます。たとえば、会社内の支店または個々の部門によるグループを管理するファイアウォー ルなどが考えられます。Panorama はポリシーを適用するときに、これらのグループを1つの単 位として処理します。ファイアウォールが属することができるデバイス グループは1つのみで すが、Panorama では仮想システムが個別のエンティティになるため、ファイアウォール内の仮 想マシンを異なるデバイス グループに割り当てることができます。

共有の場所に最大4レベルのツリー階層でデバイスグループをネストすることで、ファイア ウォールのネットワーク全域にわたり、多層的にポリシーを管理することができます。一番下 のレベルのデバイスグループは、連続する上位レベルとして親、祖父母、曽祖父母のデバイス グループを持つことができます。これらをまとめて先祖と呼び、一番下のレベルのデバイスグ ループはこれらからポリシーとオブジェクトを継承します。一番上のレベルのデバイスグルー プは、子、孫、曾孫のデバイスグループを持つことができます。これらをまとめて子孫と呼び ます。Panorama > Device Groups(デバイスグループ)を選択すると、Name(名前)列にこの デバイスグループ階層が表示されます。

デバイス グループの追加、編集、削除を行った場合は、Panorama コミットおよびデバイス グ ループのコミットを実行します(「Panorama のコミット操作」を参照)。次に、Panorama は設定変更をそのデバイス グループに割り当てられたファイアウォールへプッシュしま す。Panorama では、最大 1,024 個のデバイス グループがサポートされています。

デバイス グループを設定するには、デバイス グループを Add (追加)し、以下の表の説明に 従って設定を指定します。

デバイス グルー プ設定	の意味
氏名	グループを識別する名前を入力します(最大 31 文字)。名前は大文字と 小文字を区別し、デバイス グループ階層全体で一意である必要があり、文 字、数字、スペース、ピリオド、ハイフン、およびアンダースコアのみを 含めることができます。
の意味	デバイス グループの説明を入力します。
機器	デバイスグループに追加するファイアウォールをそれぞれ選択します。リ ストに多くのファイアウォールが表示される場合、Device State[デバイス 状態]、Platforms[プラットフォーム]、Templates[テンプレート]、または Tags[タグ] でリストをフィルタリングできます。[フィルタ] セクションの かっこの中には、これらの各カテゴリの管理対象ファイアウォールの数が 表示されます。

デバイス グルー プ設定	の意味
	デバイス グループが純粋に組織化を目的とした(つまり、他のデバイス グループが含まれる)ものである場合、そのデバイス グループにファイア ウォールを割り当てる必要はありません。
すべて選択	リスト中の全てのファイアウォールと仮想システムを選択します。
すべての選択を 解除	リスト中の全てのファイアウォールと仮想システムの選択を解除します。
HA ピアのグ ループ化	 高可用性(HA)設定のピアであるファイアウォールをグループ化する場合に選択します。これにより、リストには、アクティブ(アクティブ/アクティブ設定ではアクティブ・プライマリ)のファイアウォールが最初に表示されます。パッシブ(アクティブ/アクティブ設定ではアクティブ・セカンダリ)のファイアウォールはかっこ内に表示されます。これで、HA モードのファイアウォールを簡単に識別できます。共有ポリシーをプッシュする場合に、個々のピアではなくグループ化されたペアにプッシュできます。 アクティブ/パッシブ設定のHA ピアの場合は、両方のファイアウォールまたはそれらの仮想システムを同じデバイスグループに追加することを検討してください。これにより、両方のピアに設定を同時にプッシュできます。
フィルタが選択 されています	特定のファイアウォールもしくは仮想システムを表示したい場合は、それ らを選択した状態でFilter Selected[選択項目でフィルタ]を実行します。
親デバイス グ ループ	定義しているデバイスグループを基準として、その真上の階層にあるデ バイスグループ (または共有場所) を選択します(デフォルトはShared[共 有])。
マスターデバイス	 ユーザー名とユーザーグループに基づいてポリシールールおよびレポートを設定する場合、Master Device (マスターデバイス)を選択する必要があります。これは、Panorama がユーザー名、ユーザーグループ名、およびユーザー名とグループのマッピング情報を取得するファイアウォールです。 Master Device (マスターデバイス)を変更したり、None (なし)に設定したりすると、Panorama はその
	ファイアウォールから受信したすべてのユーザーおよびグ ループ情報を失います。
Store users and groups from Master	このオプションは、Master Device(マスター デバイス)を選択した場合 にのみ表示されます。このオプションを使用すると、Panorama は Master Device(マスター デバイス)から受信するユーザー名、ユーザー グループ

Panorama Web インターフェイス

デバイス グルー プ設定	の意味
Device(マス	名、およびユーザー名とグループのマッピング情報をローカルに保存でき
ター デバイス	ます。ローカル ストレージを有効にするには、 Panorama > Setup(セット
からのユーザー	アップ) > Management(管理)を選択して Panorama 設定を編集し、 グ
およびグループ	ループでのレポートとフィルタリングの有効化を行う必要もあります。
を保存)	

動的に追加されるデバイス プロパティ – 新しいデバイスがデバイス グループに追加される と、Panorama は指定された認証コードと PAN-OS ソフトウェア バージョンを新しいデバイ スに動的に適用します。これは、デバイス グループが Panorama の NSX サービス定義に関連 付けられていないと表示されません。

認証コード	このデバイス グループに追加されたデバイスに適用される認証コードを入 力します。
SW バージョン	このデバイス グループに追加されたデバイスに適用されるソフトウェア バージョンを選択します。

Panorama > Managed Collectors [Panorama > 管理対象 コレクタ]

Panorama 管理サーバー(Panorama モードの M-Series アプライアンスまたは Panorama バー チャル アプライアンス)は、専用ログ コレクタ(ログ コレクタ モードの M-Series アプライア ンスまたは Panorama バーチャル アプライアンス)を管理できます。また、各 Panorama 管理 サーバーには、ファイアウォールから直接受信したログを処理するためのローカルの事前定義済 みログ コレクタ(名前は default)があります。(レガシー モードの Panorama バーチャル アプ ライアンスは、専用のログ コレクタを使用せずに、ファイアウォールから直接受信するログを 保存します)。

Panorama を使用して専用ログコレクタを管理する場合は、ログコレクタを管理対象コレクタとして追加します。

操作	以下を参照
ログコレクタの情報を表示す る	ログコレクタの情報
ログ コレクタを追加、編集、 または削除する	ログコレクタの設定
ログ コレクタの Panorama ソ フトウェアを更新する	専用ログ コレクタのソフトウェアの更新
その他の情報をお探しです か?	ログとレポートの中央管理
	管理対象コレクタの設 定

ログコレクタの情報

Panorama > Managed Collectors (管理対象コレクタ)をを選択し、ログコレクタごとに以下の 情報を表示します。その他のパラメータは、ログコレクタの設定中に設定できます。

ログ コレクタの 情報	の意味
コレクタ名	ログコレクタを識別するための固有名です。この名前はログコレクタホス ト名として表示されます。

ログ コレクタの 情報	の意味	
シリアル番号	ログ コレクタとして機能している Panorama アプライアンスのシリアル番 号です。ログ コレクタがローカルの場合は、Panorama 管理サーバーのシ リアル番号です。	-
ソフトウェア バージョン	ログコレクタにインストールされているPanoramaソフトウェアのリリース バージョンを示します。	_
IPアドレス	ログコレクタ用管理インターフェイスのIPアドレスです。	_
接続済み	ログコレクタとPanoramaの接続状況を示します。	_
設定状態/詳細	ログコレクタの設定がPanoramaと同期されているかどうかを示します。	_
ランタイムス テータス/詳細	コレクタグループ内の他のログコレクタとの接続状況を示します。	_
ログ再配信状態	特定の操作(ディスクの追加など)を行った場合、ログコレクタはディス クペアにログの再配信を行います。この列は再配信プロセスの完了状態が パーセントで表示されます。	
最終コミット状 態	ログコレクタ上で行われた前回のコレクタグループコミットが成功したか 失敗したかを表示します。	_
ヘルス	ログ収集プロセスのヘルス ステータスに基づいて、ログ コレクタ のヘルス ステータスを示します。Log Collector が正常である場合は	_
	を表示し、1つ以上のログ収集プロセスで正常性が低下している場合	
	は表示します。	を
	 logd-管理されたファイアウォールから受信したログを取り込み、取り 込まれたログを vldmgr に転送する役割を担うプロセス。 	
	● vldmgr−VLD プロセスの管理を担当するプロセス。	
	 vlds-個々のログディスクの管理、ログディスクへのログの書き込み、 および ElasticSearch へのログの取り込みを担当するプロセス。 	
	• es-Log Collectorで実行されているElasticSearchプロセス。	
統計	ディスク情報、CPUパフォーマンス、平均ログ数/秒を参照する場合は、ロ グコレクタの設定を完了したのちに、Statistics(統計)をクリックしま す。レビュー中のログ範囲をよりよく理解するために、ログコレクタが受 信した最も古いログ情報を表示することもできます。	_



ログコレクタの設定

ログコレクタを管理するには、Panorama > Managed Collectors(管理対象コレクタ)を選択 します。新しいログコレクタを管理対象コレクタとして Add(追加)するとき、構成する設定 は、ログコレクタの場所、および Panorama を高可用性(HA)設定でデプロイしたかどうかに よって異なります。

- 専用ログコレクターログコレクタを追加しても、Interfaces (インターフェイス) タブは最 初からは表示されません。ログコレクタのシリアル番号 (Collector S/N (コレクタ シリアル 番号))を入力して OK をクリックしてから、ログコレクタを編集してインターフェイス設 定を表示する必要があります。
- 孤立(HA以外)またはアクティブ(HA)のPanorama管理サーバーにローカルなデフォルトログコレクタ Panorama管理サーバーのシリアル番号(Collector S/N(コレクタシリアル番号))を入力すると、Collector(コレクタ)ダイアログには、Disks(ディスク)設定、Communication(通信)設定、および一部のGeneral(全般)設定のみが表示されます。ログコレクタは、その他すべての設定の値をPanorama管理サーバーの設定から取得します。
- (HAのみ)パッシブ Panorama 管理サーバーにローカルなデフォルト ログ コレクタ Panorama はこのログ コレクタをリモートとして扱うため、専用ログ コレクタを設定する場合と同じように設定する必要があります。

	<u> </u>	
	=	
Υ.	_	

ログ コレクタを設定する完全な手順では、いくつかの追加タスクを行う必要が あります。

確認すべき情報	以下を参照
ログ コレクタを特定 し、Panorama 管理サーバーお よび外部サービスとの接続を 定義する。	ログコレクタの一般設定
ログコレクタ CLI へのアクセス を設定する。	ログコレクタ認証設定
専用ログ コレクタが、管理 トラフィック、コレクタ グ ループ通信、ログ収集に使用 するインターフェイスを設定 する。	ログ コレクタ インターフェイス設定

確認すべき情報	以下を参照
ファイアウォールから収集し たログを保管するRAIDディス クを設定する。	ログコレクタの RAID ディスク設定
ログ コレクタが Windows User-ID エージェントで認証す るように設定する。	接続のセキュリティ
Panorama、その他のログコレ クタ、ファイアウォールとの 通信用にセキュリティ設定を 構成する。	通信設定

ログコレクタの一般設定

• Panorama > Managed Collectors > General [Panorama > 管理対象コレクタ > 一般]

ログコレクタを識別し、Panorama 管理サーバー、DNS サーバー、NTP サーバーとの接続を定 義する場合は、以下の表に記載されている設定を行います。

ログ コレクタの 一般設定	の意味
コレクタ シリ アル番号	(必須)ログコレクタとして機能する Panorama アプライアンスのシリア ル番号を入力します。ログコレクタがローカルである場合、Panorama 管 理サーバーのシリアル番号を入力します。
コレクタ名	このログコレクタの識別に使用する名前を入力します(最大 31 文字)。 大文字と小文字を区別し、一意の名前を入力する必要があります。文字、 数字、スペース、ハイフン、アンダースコアのみが使用できます。 この名前はログコレクタホスト名として表示されます。
保護された Syslog の着信 証明書	Traps [™] ESM サーバーからログを安全に取り込むために管理対象コレクタ が使用しなければならない証明書を選択します。この証明書を着信証明書 と呼びます。これは、Panorama/管理対象コレクタが Traps ESM(クライ アント)がログを送信する宛先のサーバーであるためです。ログインジェ ストプロファイルの Transport(転送)プロトコルが SSL である場合、証 明書が必要です。
保護された Syslog の証明 書	syslog を外部の Syslog サーバーに安全に転送するための証明書を選択 します。証明書の Certificate for Secure Syslog (保護された Syslog の証 明書) オプションが選択されている必要があります(「ファイアウォー ルおよび Panorama 証明書の管理」を参照)。このログ コレクタが含ま れるコレクタ グループに Syslog サーバー プロファイルを割り当てる場

ログ コレクタの 一般設定	の意味
	合 (Panorama > Collector Groups (コレクタ グループ)、Panorama > Collector Groups (コレクタ グループ) > Collector Log Forwarding (コレ クタ ログ転送)を参照)、サーバー プロファイルの Transport (転送) プ ロトコルが SSL である必要があります (Device (デバイス) > Server Profiles (サーバープロファイル) > Syslogを参照)。
Panorama サー バー IP	このログコレクタを管理しているPanorama管理サーバーの IPアドレスを指 定します。
Panorama サー バー IP 2	Panorama管理サーバーがHA(高可用性)設定でデプロイされている場合、セカンダリピアのIPアドレスを指定します。
ドメイン	ログコレクタのドメイン名を入力します。
プライマ リDNSサー バー	プライマリ DNS サーバーの IP アドレスを入力します。ログ コレクタはこ のサーバーを使用して DNS クエリ(Panorama 管理サーバーの検索など) を処理します。
セカンダリ DNS サーバー	(任意)プライマリサーバーを使用できない場合は、使用するセカンダ リDNSサーバーのIPアドレスを入力します。
プライマリ NTP サーバー	プライマリ NTP サーバーの IP アドレスまたはホスト名を入力します (存在 する場合)。NTP サーバーを使用しない場合は、ログ コレクタの時刻を手 動で設定できます。
セカンダリ NTP サーバー	(任意)プライマリサーバーを使用できない場合、使用するセカンダリ NTPサーバーのIPアドレスまたはホスト名を入力します。
タイムゾーン	ログコレクタのタイムゾーンを選択します。
緯度	ログコレクタの緯度(-90.0から90.0)を入力します。トラフィックおよび 脅威マップがアプリケーションスコープ用にこの緯度を使用します。
経度	ログコレクタの経度(-180.0から180.0)を入力します。トラフィックおよ び脅威マップがアプリケーションスコープ用にこの経度を使用します。

ログコレクタ認証設定

• Panorama > Managed Collectors > Authentication [Panorama > 管理対象コレクタ > 認証]

ログ コレクタ モードの M-Series アプライアンスまたは Panorama バーチャル アプライアンス (専用ログ コレクタ)には、Webインターフェースがありません。CLIのみが提供されます。専 用ログ コレクタの設定の大部分は、Panorama 管理サーバーを使用して行うことができますが、 一部 CLI アクセスを必要とするものもあります。CLI アクセス用の認証設定を行う場合は、次の 表で説明する設定を行います。

ログコレクタ認 証設定	の意味
認証プロファイ ル	構成済みの認証プロファイルを選択して、Dedicated LogCollector(専用の ログ コレクタ)または Panorama 管理者のログイン資格情報を検証する認 証サービスを定義します。
最大試行回数	管理者をロックアウトする前に、Dedicated Log Collector(専用のログコ レクタ)が CLI で許可するログイン試行失敗の回数を入力します(範囲は 0~10、デフォルトは 10)。ログイン試行回数を制限すると、総当たり攻 撃からの WildFireアプライアンス保護に役立ちます。値 0 を指定すると、 無制限にログインを試行できます。
	 Failed Attempts (試行失敗回数)を0以外の値にして、Lockout Time (ロックアウト時間)を0のままにしている場合、別の 管理者がロックアウトされた管理者を手動でロック解除す るまで、管理者ユーザーは無期限にロックアウトされます。 他の管理者が作成されていない場合は、Panoramaで Failed Attempts (試行失敗回数) および Lockout Time (ロックアウト 時間)の設定を再構成し、構成変更をログコレクタにプッ シュする必要があります。管理者がロックアウトされない設 定にするには、Failed Attempts (試行失敗回数) とLockout Time (ロックアウト時間) に共にデフォルトの値(0)を 使用します。
	Failed Attempts (試行矢敗回奴)の値を5以下に設定し、人力 ミスに備えてある程度猶予を持たせつつ、悪意のあるシステ ムが総当たりの方法で専用のログコレクタにログインしよう とするのを防ぎます。
ロックアウト時 間 (分)	Failed Attempts(最大試行回数)の制限に達した後、専用のログコレクタ がWeb インターフェイスおよび CLI への管理者のアクセスをロックアウト する時間(分)を入力します(範囲は 0~60、デフォルトは 5)。値を 0 にすると、別の管理者がアカウントのロックを手動で解除するまでロック アウトが適用されます。

ログコレクタ認 証設定	の意味
	 Failed Attempts (試行失敗回数)を0以外の値にして、Lockout Time (ロックアウト時間)を0のままにしている場合、別の 管理者がロックアウトされた管理者を手動でロック解除す るまで、管理者ユーザーは無期限にロックアウトされます。 他の管理者が作成されていない場合は、Panoramaで Failed Attempts (試行失敗回数)および Lockout Time (ロックアウト 時間)の設定を再構成し、構成変更をログコレクタにプッ シュする必要があります。管理者がロックアウトされない設 定にするには、Failed Attempts (試行失敗回数)とLockout Time (ロックアウト時間)に共にデフォルトの値(0)を 使用します。 Lockout Time (ロックアウト時間)を 30 分以上に設定し、攻撃 者が続けてログインを試みるのを防ぎます。
Idle Timeout (min)(分単位 のアイドル タ イムアウト)	 CLI でアクティビティがない場合、管理者が自動的にログアウトするまでの最大分数を入力します(範囲は 0~1,440、デフォルトは None(なし))。値0は、アクティビティがなくても自動ログアウトはトリガーされないことを意味します。 管理者がセッションを開いたままにした場合に、権限を持た
	ないユーザーが Dedicated Log Collector (専用のログ コレク タ) にアクセスできないようにするには、Idle Timeout (アイ ドル タイムアウト)を 10 分に設定します。
Max Session Count(最大 セッション数)	管理者が同時に開くことができるアクティブなセッション数を入力しま す。デフォルトは0です。これは、Dedicated Log Collector(専用のログ コレクタ)で同時にアクティブなセッションを無制限に持つことができる ことを意味します。
Max Session time(最大セッ ション時間)	管理者が自動的にログアウトするまでにログイン可能な時間を分で入力し ます。デフォルトは0です。これは、管理者がアイドル状態であっても無 期限にログイン可能であることを意味します。
Local Administrators(カル管理者)	Dedicated LogCollector(専用のログコレクタ)の新しい管理者を追加し、 口設定します。この管理者は、Dedicated Log Collector(専用のログコレ クタ)に固有のものであり、以下のページで管理されます(Panorama > Managed Collectors(管理対象コレクタ) > Authentication(認証))。
Panorama Administrators(管理者)	Panorama で設定された既存の管理者をインポートします。この管理者は Paraouranana で作成され、Dedicated Log Collector(専用のログ コレクタ)に インポートされます。

- ログコレクタインターフェイス設定
 - Panorama > Managed Collectors (管理対象コレクタ) > Interfaces (インターフェイス)

デフォルトでは、専用ログコレクタ(ログコレクタモードの M-Series アプライアンス)で は、管理トラフィック、ログ収集、コレクタグループ通信に管理(MGT)インターフェイスが 使用されます。ただし、Palo Alto Networks では、ログ収集とコレクタグループ通信に個別の インターフェイスを割り当て、MGT インターフェイスのトラフィックを減らすことをお勧めし ています。その他のインターフェイスのサブネットよりも秘密性の高い MGT インターフェイス のサブネットを別途定義することで、セキュリティを向上させることができます。個別のイン ターフェイスを使用するには、まず Panorama 管理サーバーで個別のインターフェイスを設定す る必要があります(「Device(デバイス)> Setup(セットアップ)> Management(管理)」 を参照)。ログ収集とコレクタグループ通信に使用できるインターフェイスは、ログコレク タアプライアンスのモデルに応じて異なります。例えば、M-500 アプライアンスには次のイン ターフェイスがあります:イーサネット1(1Gbps)、イーサネット2(1Gbps)、イーサネッ ト3(1Gbps)、イーサネット4(10Gbps)、およびイーサネット5(10Gbps)

インターフェイスを設定するには、以下の表の説明に従ってリンクを選択して設定を構成しま す。

- MGTインターフェイスの設定を完了するには、IPアドレス、ネットマスク(IPv4の場合)、プレフィックス長(IPv6の場合)のいずれかと、デフォルトゲートウェイを指定する必要があります。不完全な設定をコミットした場合(デフォルトゲートウェイを省略した場合等)、追って設定を変更する場合はコンソールポート経由でのみファイアウォールまたは Panorama にアクセスすることができます。
- 必ず、完全な MGT インターフェイス設定をコミットしてください。IPアドレス、 ネットマスク(IPv4 の場合)、プレフィックス長(IPv6 の場合)のいずれかと、デ フォルト ゲートウェイを指定しない場合は、その他のインターフェースの設定をコ ミットできません。

ログ コレクタ イン ターフェイス設定	の意味
Eth1/Eth2/Eth3/	インターフェイスを有効にして設定する必要があります。MGT イン
Eth4/Eth5	ターフェイスは例外で、これはデフォルトで有効になっています。
速度とデュプレック	 インターフェイスのデータ速度とデュプレックスオプションを
ス	設定します。フルデュプレックスまたはハーフデュプレックス で、10Mbps、100Mbps、1Gbps、10Gbps(Eth4 と Eth5 のみ)のいずれかを選択できます。ログコレクタにインターフェイス速度を決定させるには、デフォルトのauto-negotiate(オートネゴシエート)設定を使用します。 この設定は、隣接するネットワーク機器のインターフェイス設定と一致する必要があります。

ログ コレクタ イン ターフェイス設定	の意味
IPアドレス (IPv4)	ネットワークで IPv4 アドレスを使用する場合、IPv4 アドレスをイン ターフェースに割り当てます。
ネットマスク (IPv4)	IPv4 アドレスをインターフェイスに割り当てた場合は、ネットワーク マスク(例: 255.255.255.0)を入力する必要もあります。
デフォルト ゲート ウェイ(IPv4)	IPv4 アドレスをインターフェイスに割り当てた場合は、デフォルト ゲートウェイに IPv4 アドレスを割り当てる必要もあります(ゲート ウェイは MGT インターフェイスと同じサブネット上にある必要があ ります)。
IPv6 アドレス/プレ フィックス長	ネットワークで IPv6 アドレスを使用する場合、IPv6 アドレスをイン ターフェースに割り当てます。ネットマスクを示すには、IPv6 プレ フィックス長を入力します(例: 2001:400:f00::1/64)。
デフォルト IPv6 ゲートウェイ	IPv6 アドレスをインターフェイスに割り当てた場合は、デフォルト ゲートウェイにも IPv6 アドレスを割り当てる必要があります(ゲー トウェイはインターフェイスと同じサブネット上にある必要がありま す)。
MTU	このインターフェイスで送信されるパケットの最大転送単位(MTU) をバイト数で入力します(範囲は 576 ~ 1,500、デフォルトは 1,500)。
デバイス ログ収集	ファイアウォールからのログ収集のインターフェイスを有効にしま す。ログ トラフィックが多いデプロイでは、複数のインターフェイス を有効にしてこの機能を実行できます。この機能は、MGT インター フェイスでデフォルトで有効になっています。
コレクタ グループ 通信	インターフェイスでコレクタ グループ通信を有効にします(デフォル トは MGT インターフェイス)。この機能を実施できるインターフェ イスは 1 つのみです。
Syslog Forwarding Syslog の転送	Syslog を転送するインターフェースを有効にします(デフォルトは MGT インターフェイス)。この機能を実施できるインターフェイスは 1 つのみです。
ネットワーク接続性 サービス	Ping サービスは任意のインターフェースで使用可能で、Log Collector(ログ コレクタ)インターフェースと外部サービスとの間で 接続をテストすることができます。
	次のサービスを使用できるのは、MGT インターフェイスのみです。
	• SSH – Panorama CLI への安全なアクセスを有効にします。

ログ コレクタ イン ターフェイス設定	の意味
	 SNMP – 統計クエリを SNMP マネージャーから受信するインター フェイスを有効にします。詳細は、「SNMP モニタリングの有効 化」を参照してください。
	 User-ID – ログ コレクタが User-ID エージェントから受信したユー ザーマッピング情報を再配信できるようにします。
アクセス許可IPアド レス	このインターフェイスでログ コレクタにアクセスできるクライアント システムの IP アドレスを入力します。
	リストを空にすると(デフォルト)、すべてのクライアント システム がアクセスできるようになります。
	 Palo Alto Networks では、このリストを空のままにしない ことを推奨します。Panorama 管理者(のみ)のクライ アントシステムを指定して、不正アクセスを阻止してく ださい。

ログコレクタの RAID ディスク設定

• Panorama > Managed Collectors > Disks [Panorama > 管理対象コレクタ > ディスク]

M-Series アプライアンスまたは Panorama バーチャル アプライアンスでログ ディスクを設定した後で、ログ コレクタ設定にそれを Add(追加)できます。

M-Series アプライアンスは通常、最初の RAID 1 ディスク ペアが A1 と A2 ベイにインストー ルされた状態で出荷されます。ソフトウェアでは、A1 と A2 ベイのディスク ペアに Disk Pair A (ディスク ペア A) という名前が付いています。残りのベイには順番に、Disk Pair B (ディス クペア B)、Disk Pair C (ディスク ペア C) というように名前が付きます。例えばい、M-500 アプライアンスでは、最大 12 個のディスク ペアがサポートされています。同一アプライアンス では 2TB または 1TB のディスクのペアをインストールできますが、ディスク サイズは各ペアの 両方のドライブで同一にする必要があります。

Panorama バーチャル アプライアンスでは、ストレージ容量が 24TB の 12 個までの仮想ログ ディスクがサポートされます。

新しいディスクペアを追加すると、ログコレクタはその既存のログをすべてのディスクに再配信します。この処理には、ログ1テラバイトごとに数時間かかる可能性があります。再配信プロセス中は、最大ログインジェスト率が低くなります。Panorama > Managed Collectors(管理対象コレクタ)ページの Log Redistribution State(ログ再配信状態)列には、プロセスの完了状況がパーセントで表示されます。



SNMP マネージャを使用して中央監視する場合は、panLogCollector MIB でログ統計を参照できます。

接続のセキュリティ

- デバイス>ユーザー ID> 接続のセキュリティ
- Panorama > ユーザー ID > 接続のセキュリティ

Windows User ID エージェントによって提示された証明書を検証するためにログコレクタが使用する証明書プロファイルを設定します。ログコレクタは、選択された証明書プロファイルを使用して、User ID エージェントによって提示されたサーバー証明書を検証し、エージェントのアイデンティティを検証します。

タスク	の意味
User-ID 証明書プロファイ ル	ドロップダウンリストでファイアウォールまたは Panorama がWindows User ID エージェントでの認証に使用する証明書プ ロファイルを選択するか、New Certificate Profile(新規証明書 プロファイル)を選択して証明書プロファイルを作成します。 証明書プロファイルを削除するには、None(なし)を選択しま す。

通信設定

• Panorama > Managed Collectors(管理対象コレクタ) > Communication(通信)

ログコレクタと Panorama、ファイアウォール、他のログコレクタ間でカスタムの証明書ベースの認証を設定するには、以下の表に記載されているように設定します。

通信設定	の意味
保護されたサーバー通信 – Secure Server Communication(保護されたサーバー通信)を有効 にすると、ログ コレクタに接続しているクライアント デバイスの識別情報が検証されます。	
SSL/TLS Service Profile	ドロップダウン リストから SSL/TLS サービス プロファイルを選択 します。このプロファイルはログ コレクタが提示する証明書を定義 し、ログ コレクタとの通信で可能な SSL/TLS バージョンの範囲を指 定します。
証明書プロファイル	ドロップダウン リストから証明書プロファイルを選択します。この 証明書プロファイルは証明書取り消しチェック動作を定義し、クライ アントが提示する証明書チェーンの認証で使用するルート CA を定義 します。
カスタム証明書のみ	有効化すると、管理対象ファイアウォールとログ コレクタの認証に 関して、ログ コレクタはカスタム証明書のみを受け入れます。

通信設定	の意味
シリアル番号に基づ いてクライアントを 承認	ログ コレクタは、クライアント デバイスのシリアル番号のハッシュ に基づいてクライアント デバイスを承認します。
承認リストのチェッ ク	このログ コレクタに接続しているクライアント デバイスまたはデバ イス グループを、認証リストに照らして確認します。
切断待機時間(分)	管理対象デバイスとの現行の接続を切断するまでにログコレクタが 待機する時間です。その後、ログコレクタは指定済みの保護された サーバー通信設定を使用して、管理対象デバイスとの通信を再構築し ます。待機時間は、保護されたサーバー通信の設定がコミットされた 後に開始されます。
承認リスト	 Authorization List (承認リスト) – Add (追加)を選択して、以下のフィールドで基準を設定します。 Identifier (識別子) –Select Subject (サブジェクト) またはSubject Alt (サブジェクト代替)を選択します。認証識別子としてのName (名前)を付けます。 Type (タイプ) – Subject Alt (サブジェクト代替)の場合。Name (名前)を識別子として選択した場合、識別子のタイプとして IP、hostname (ホスト名)、または e-mail (電子メール)を選択します。Subject (サブジェクト)を選択した場合、識別子のタイプとして共通名が使用されます。 Value (値) – 識別子の値を入力します。

保護されたクライアント通信 – Secure Client Communication (保護されたクライアント通信)を有効にすると、Panorama、ファイアウォール、他のログ コレクタとの SSL 通信でのロ グ コレクタの認証において、特定のクライアント証明書が使用されます。

証明書タイプ	通信の保護のために使用するデバイス証明書のタイプ(None(な し)、Local(ローカル)、または SCEP)を選択します。
まったくない	None(なし)を選択した場合、デバイス証明書は設定されず、保護 されたクライアント通信は使用されません。これがデフォルトの選択 です。
ローカル	ログ コレクタは、ログ コレクタで生成された、または既存のエン タープライズ PKI サーバーからインポートされた、ローカルのデバイ ス証明書と、対応する秘密鍵を使用します。
	Certificate (証明書) – ローカルのデバイス証明書を選択します。この証明書は、ファイアウォールに対して一意のものであっても(ログコレクタのシリアル番号のハッシュに基づく)、Panorama に接続し

通信設定	の意味
	ているすべてのログ コレクタで使用される共通のデバイス証明書で あっても構いません。
	Certificate Profile(証明書プロファイル) – ドロップダウン リスト から証明書プロファイルを選択します。この証明書プロファイルは、 ログ コレクタのサーバー認証の定義に使用します。
SCEP	ログコレクタは、Simple Certificate Enrollment Protocol (SCEP) サーバーで生成されたデバイス証明書と秘密鍵を使用します。
	SCEP Profile(SCEP プロファイル) – ドロップダウン リストから SCEP プロファイルを選択します。
	Certificate Profile(証明書プロファイル) – ドロップダウン リスト から証明書プロファイルを選択します。この証明書プロファイルは、 ログ コレクタのサーバー認証の定義に使用します。
サーバー アイデン ティティのチェック	共通名(CN)とサーバーの IP アドレスまたは FQDN の照合によって、クライアント デバイスがサーバーの識別情報を確認します。

専用ログ コレクタのソフトウェアの更新

• Panorama > Managed Collectors [Panorama > 管理対象コレクタ]

専用ログ コレクタにソフトウェア イメージをインストールする場合は、Panorama にイメージ をダウンロードまたはアップロードし(「Panorama > Device Deployment(デバイスのデプロ イ)」を参照)、Install(インストール)をクリックして、以下のフィールドを設定します。

Panorama 管理サーバーのオペレーティングシステムはローカルのデフォルトログ コレクタと共有されるため、ソフトウェア更新を Panorama 管理サーバーにインス トールすると、両方がアップグレードされます(「Panorama > Software(ソフト ウェア)」を参照)。

専用ログコレクタの場合、Panorama > Device Deployment (デバイスのデプロイ) > Software (ソフトウェア)を選択して、更新をインストールすることもできます (「ソフトウェアおよびコンテンツ更新の管理」を参照)。

管理(MGT)インターフェイスのトラフィックを削減するには、更新のデプロ イのために個別のインターフェイスを使用するように Panorama を設定します (「Panorama > Setup(セットアップ) > Interfaces(インターフェイス)」を参 照)。

ログ コレクタへのソ フトウェア更新のイ ンストールに関する フィールド	の意味
ファイル	ダウンロードまたはアップロードされたソフトウェアイメージを選択 します。
機器	ソフトウェアをインストールするログコレクタを選択します。ダイア ログには、それぞれのログコレクタにつき、以下の情報が表示されま す。
	• Device Name(デバイス名) - 専用ログ コレクタの名前です。
	 Current Version[現在のバージョン] - ログコレクタに現在インストールされているPanoramaソフトウェアのリリースバージョンを示します。 HA Status[HA状況] - ログコレクタの場合、この列は使用しません。専用ログコレクタにおいて高可用性はサポートされていませ
	h_{\circ}
フィルタが選択され ています	特定のログコレクタのみを表示する場合は、ログコレクタを選択し、Filter Selected[選択項目でフィルタ]を実行します。
Upload only to device (do not Install)(デバイスに アップロードするだ け(インストールは 行わない))	ログコレクタにソフトウェアをアップロードし、自動的に再起動させ ない場合に選択します。ログコレクタ CLI にログインして、request restart systemの操作コマンドを実行して手動で再起動を行うま で、イメージはインストールされません。
Reboot device after Install(インストー ル後にデバイスを再 起動)	ソフトウェアのアップロード後に自動的にインストールを行う場合に 選択します。インストール処理によりログコレクタは再起動されま す。

Panorama > Collector Groups [Panorama > コレクタ グ ループ

各コレクタ グループには最大 16 個のログ コレクタを割り当てることができ、またそれぞれに はログ転送用のファイアウォールを割り当てることができます。こうすることでPanoramaを使 用してログコレクタに対するクエリを行い、集約ログの表示と調査を行うことができます。



事前に定義されているコレクタ グループ(名前はデフォルト)には、Panorama 管 理サーバー上にローカルに存在する、事前に定義されたログ コレクタを含まれてい ます。

- コレクタ グループの設定
- コレクタグループの情報

コレクタ グループの設定

コレクタグループを設定する場合は、Add (追加)をクリックし、以下のパラメータを入力しま す。

コレクタグ ループ設定	設定場所	の意味
名前	Panorama > コレクタ グ ループ > 一般	このコレクタ グループを識別する名前を入力しま す(最大 31 文字)。名前の大文字と小文字は区 別されます。また、一意の名前にする必要があり ます。文字、数字、スペース、ハイフン、および アンダースコアのみを使用してください。
ログストレー ジ		コレクタ グループが受信するファイアウォール ロ グのストレージ割り当て合計と使用可能領域を示 します。 ストレージ割り当てリンクをクリックして、以下 のログ タイプのストレージ Quota(%)(割り当て (%))と有効期間(Max Days(最大日数))
		 Detailed Firewall Logs(詳細なファイアウォー ルログ) – トラフィック、脅威、HIP マッ チ、動的に登録された IP アドレス(IP タ グ)、拡張 PCAP、GTP とトンネル、アプリ統 計など、Device(デバイス) > Setup(セット アップ) > Logging and Reporting Settings(ロ ギングおよびレポート設定)のすべてのログ タイプが含まれます。

コレクタグ ループ設定	設定場所	の意味
		 Summary Firewall Logs (サマリー ファイア ウォール ログ) – トラフィック サマリー、 脅威サマリー、URL サマリー、GTP およびト ンネル サマリーのように、Device (デバイ ス) > Setup (セットアップ) > Logging and Reporting Settings (ロギングおよびレポー ト設定) のすべてのサマリー ログが含まれま す。 Infrastructure and Audit Logs (インフラスト ラクチャおよび監査ログ) – 設定、システ ム、User-ID、および認証ログが含まれます。 Palo Alto Networks Platform Logs (Palo Alto Networks プラットフォーム ログ) – Traps な どの Palo Alto Networks 製品からのログが含ま れます。 3rd Party External Logs (サードパーティ外部 ログ) – Palo Alto Networks が提供するその他 のベンダー統合のログが含まれます。 デフォルトの設定を使用する場合はRestore Defaults[デフォルトを復元]をクリックします。
最小保持期間 (日)		コレクタグループ内のすべてのログコレクタに おいて、Panoramaがログを保持する最小期間 (1~2000日)を入力します。現在の日付から最も 古いログの日付を引いた値が、定義した最小保持 期間よりも小さくなる場合、Panoramaはアラート 違反のシステムログを生成します。
コレクター グループのメ ンバー		このコレクタ グループに含めるログ コレクタを Add(追加)します(最大 16 個)。Panorama > Managed Collectors(管理対象コレクタ)ページ で使用可能なログ コレクタを追加できます。特 定のコレクタ グループのすべてのログ コレクタ が、同じモデルである必要があります(例えば、 すべての M-500 アプライアンス、またはすべて の Panorama バーチャル アプライアンス)。

コレクタグ ループ設定	設定場所	の意味
		 ログコレクタを既存のコレクタグ ループに追加すると、Panoramaは その既存のログをすべてのログコ レクタに再配信します。この処理に は、ログ1テラバイトごとに数時 間かかる可能性があります。再配信 プロセス中は、最大ロギング率が低 くなります。Panorama > Collector Groups(コレクタグループ)ページ の Log Redistribution State(ログ再配 信状態)列には、プロセスの完了状 況がパーセントで表示されます。
コレクタ間の ログ冗長性の 有効化		このオプションを選択した場合、コレクタグルー プ内の各ログのコピーが2つ作成され、それぞれ 異なるログコレクタに保存されます。この冗長性 により、いずれかのログコレクタが利用不可に なってもログは失われません。すべてのログがコ レクタグループに転送されていることを確認で き、すべてのログデータに関するレポートを実行 できます。ログ冗長性を利用できるのは、コレク タグループに複数のログコレクタがあり、各ログ コレクタのディスク数が同じ場合のみです。ログ の冗長性は、設定が有効になった後に新しく取り 込まれたログにのみ適用され、既存のログには適 用されません。
		Panorama > Collector Groups(コレクタ グルー プ)ページの Log Redistribution State(ログ再配 信状態)列には、プロセスの完了状況がパーセン トで表示されます。特定のコレクタ グループのす べてのログ コレクタが、同じモデルである必要が あります(例えば、すべての M-500 アプライア ンス、またはすべての Panorama バーチャル アプ ライアンス)。

コレクタグ ループ設定	設定場所	の意味
		⑦ 冗長性を有効にすると、作成されるログが多くなるため、この設定には、より大きなストレージ容量が必要です。冗長性を有効にすると、コレクタグループ内のログ処理トラフィックが2倍になり、最大ロギング率が半分になります。各ログコレクタが、受信する各ログのコピーを配信する必要があるためです。(コレクタグループの容量が不足すると、古いログが削除されます。)
設定リストの すべてのコレ クタに転送		優先リスト内のすべての Log Collector にログを 送信する場合に選択します。Panorama はラウン ドロビン負荷分散を使用して、ログを受信するロ グコレクタを適宜選択します。これはデフォルト では無効です。ログコレクタが使用不可になら ない限り、ファイアウォールはリストの最初のロ グコレクタにのみログを送信します(「Devices / Collectors(デバイス/コレクタ)」を参照)。
Secure Inter LC Communication キュア イン ター LC 通 信)の有効化) (セ	Collector Group(コレクタ グループ)内の Log Collectors(ログ コレクタ)間の相互 SSL 認証に カスタム証明書を使用できるようにします。
場所	Panorama > コレクタ グ	コレクタ グループの場所を指定します。
お問い合わせ	ルーノ イモーダリンク	連絡先メールアドレスを設定します(ログコレク タを監視するSNMP管理者の電子メールアドレス など)。
バージョン		Panorama管理サーバーとの通信に使用す るSNMPのバージョンを指定します。V2cまた はV3
		SNMPにより、接続状態、ディスクドライブ統計、ソフトウェアバージョン、平均CPU使用率、 平均ログ/秒、ログタイプ別の保存期間など、ログ コレクタに関する情報の収集ができるようになり ます。SNMP 情報は、コレクタ グループごとに利 用できます。

コレクタグ ループ設定	設定場所	の意味
SNMPコミュ ニティ名 (V2cのみ)		 SNMPマネージャおよびモニター対象デバイス(この場合はログコレクタ)のSNMPコミュニティを識別し、コミュニティメンバーを相互認証するためのパスワードとして機能するSNMP Community String [SNMPコミュニティ名]を入力します。 デフォルトのコミュニティ名 publicは、広く公開されていて安全ではないので使用しないでください。
ビュー (<mark>V3</mark> のみ)		SNMPビューのグループをAdd[追 加]し、Views[ビュー]内でグループ名を入力して ください。
		各ビューは、オブジェクト識別子(OID)とビッ ト単位のマスクの組み合わせです。OIDで管理 対象の情報ベース(MIB)を指定し、16進数 形式のマスクを使用して、そのMIB内(一致検 索)またはMIB外(不一致検索)でアクセス可能 なSNMPオブジェクトを指定します。
		グループ内のそれぞれのビューについて、以下の 設定を Add [追加] します。
		• View(ビュー) - ビューの名前を指定します。
		• OID - OIDを指定します。
		 Option[オプション](含めるか除外するか)- ビューにOIDを含めるか除外するかを選択して下さい。
		• Mask[マスク] – OIDに適用するフィルタのマス ク値を指定します(0xf0など)。
ユーザー (<mark>V3</mark> のみ)		それぞれのSNMP用に以下の設定をAdd[追加] し ます。
		• Users[ユーザー] - SNMPマネージャにおける ユーザー認証に使用するユーザー名を入力しま す。
		• View(ビュー) - ユーザーが使用できるビュー のグループを指定します。
		 Authpwd(認証パスワード) - SNMP マネージャにおけるユーザー認証に使用するパスワードを入力します(8文字以上)。パスワードの

コレクタグ ループ設定	設定場所	の意味
		 暗号化でサポートされているのはSecure Hash Algorithm (SHA)のみです。 Privpwd (専用パスワード) - SNMP マネー ジャに送信する SNMP メッセージを暗号化す る際の専用パスワードを入力します (8 文字以 上)。Advanced Encryption Standard (AES)の みがサポートされています。
デバイス/コ レクタ	Panorama > コレクタ グ ループ > デバイス ログ 転送	ログ転送設定リストは、どのファイアウォー ルからどのログ コレクタにログを転送するか を制御します。リストに Add (追加) するエ ントリごとに、Devices (デバイス) リストを Modify (変更) してファイアウォールを割り当て て、Collectors (コレクタ) リストにログ コレク タを Add (追加) します。
		デフォルトでは、リスト エントリで割り当てた ファイアウォールは、プライマリ(1 番目の)ロ グコレクタにのみ(使用可能である限り)ログを 送信します。プライマリログコレクタで障害が 発生すると、ファイアウォールはセカンダリロ グコレクタにログを送信します。セカンダリで 障害が発生すると、ファイアウォールは第 3 ロ グコレクタにログを送信します(以下同様)。 この順番を変更する場合は、ログコレクタを選択 してMove Up[上へ] ボタンまたは Move Down[下 へ]をクリックします。
		 [General]タブの基本設定リストで [転送]を選択すると、管理対象ファ イアウォールのデフォルトのログ転 送動作を上書きできます。
システム	Panorama > コレクタ グ	このコレクタ グループから外部サービスに転送す
設定	ループ > コレクタ のロ グ転送	るファイアワオール ロクのタイノことに、一致リ スト プロファイルを 追加 します。プロファイル
HIP マッチ		は転送りるロクと宛元サーハーを指定します。 ロファイルごとに、次の手順を実行します。
トラフィック	_	 [名前(Name)]:一致リストプロファイルを識別 するために最大 31 文字の名前を入力します。
脅威		 Filter(フィルタ) - デフォルトでは、この一 致リストプロファイルが適用されているタ イプの All Logs(すべてのログ)をファイア

コレクタグ ループ設定	設定場所	の意味
URL	_	ウォールは転送します。一部のログを転送す るには、既存のフィルタを選択するか、Filter Builder(フィルタ ビルダー)を選択して新し
データ WildFire	-	いフィルタを追加します。新しいフィルターの クエリごとに、次のフィールドを指定し、クエ リを追加します
製品連携	-	 コネクタ: コネクタ ロジック (and/or) を選
GTP		択します。Negate(上記以外)を選択す ると、指定した内容を除外します。たとえ
SCTP		は、信頼できないソーンからログか転送されないようにするには、Negateを選択し、
認証	_	属性として Zone を選択し、演算子として equal を選択し、[値] 列に信頼できないゾー ンの名前を入力します。
User-ID	-	 Attribute(属性) - ログの属性を選択しま
トンネル	-	す。オプションはログの種類によって異な ります。
IP-Tag	-	 Operator (演算子) - 属性をどのように ^{適田する}かを字める甘進を選切します
復号	-	適用するがを定める基準を選択しよす (equal(等しい)など)。オプションはロ グの種類によって異なります。
グローバルプ ロテクト		 Value - 照合する属性値を指定します。
		フィルタが一致するログを表示またはエクスポート するには、[View Filtered Logs]を選択します。 このタブでは Monitoring (モニタリング) タ ブのページと同じオプションが表示されます (Monitoring (モニタリング) > Logs (ログ) > Traffic (トラフィック) など)。
		 Description(説明) - この一致リストプロ ファイルの主旨に関する説明を最大 1,023 文字 で入力します。
		 Destination servers(宛先サーバー) - 各 サーバータイプにサーバープロファイルを Add(追加)します。サーバープロファイル を構成するには、Device > Server Profiles > SNMPトラップ、Device > Server Profiles > Syslog、Device > Server Profiles > Email、また は Device > Server Profiles > HTTP を参照して ください。

コレクタグ ループ設定	設定場所	の意味
		 ビルトインアクション - システム ログと構成 ログを除くすべてのログ タイプに対してアク ションを 追加 できます。
		 アクションにわかりやすい名前を入力します。
		 タグ付けする IP アドレス(Source Address(送信元アドレス)または Destination Address(宛先アドレス))を 選択します。Correlation ログおよび HIP Match ログ内のソース IP アドレスのみにタ グを付けることができます。
		 アクション(Add Tag(タグの追加)また は Remove Tag(タグの除去))を選択しま す。
		 タグをこの PanoramaのローカルUser- IDエージェントに登録するか、リモートの ユーザーIDエージェントに登録するかを選 択します。
		リモート デバイス User-ID Agent にタグ を登録するには、転送を有効にする HTTP サーバー プロファイルを選択します。
		 IP-Tag Timeout を設定して、IP address-to- tag マッピングが維持される時間を分単位で 設定します。タイムアウトを0に設定する と、IP-Tag マッピングはタイムアウトしま せん(範囲は0~43200(30日)、デフォルト は0です)。
		タイムアウトは Add Tag アク ションでのみ構成できます。
		 ターゲットの送信元または宛先の IP アドレスに適用または削除する Tags を入力または 選択します。
インジェスト プロファイル	Panorama > コレクタ グループ > Ingestion Rate(取り込みレー ト)	Panorama が Traps ESM サーバーからログを受信 できるようにするログ インジェスト プロファイ ルを Add (追加) します。新しいログ インジェ スト プロファイルを設定する手順については、 「Panorama > Log Ingestion Profile (ログ イン ジェスト プロファイル)」を参照してください。

コレクタグ ループ設定	設定場所	の意味
管理者アク ティビティを ログ	Panorama > コレクタ グ ループ > 監査	管理者アクティビティの監査ログを生成し、選択 した syslog サーバに転送するように Log Collector を設定します。
		 オペレーション・コマンド (デフォルトでは無効) - 管理者が CLI で操作コマンドまたはデバッグ・コマンドを実行するときに監査ログを生成します。PAN-OS の操作コマンドおよびデバッグ コマンドの完全なリストについては、CLIの操作コマンド階層 を参照してください。 Syslog Server :監査ログを転送するターゲットSyslog サーバプロファイルを選択します。

コレクタグループの情報

Panorama > Collector Groups コレクタグループ を選択し、コレクタグループごとに以下の情報 を表示します。その他のフィールドは、ログ コレクタの設定が完了した後に設定できます。

コレクタグルー プの情報	の意味
氏名	コレクタグループを識別するための名前です。
冗長性対応	コレクタグループのログの冗長性が有効化されているかどうかを示しま す。ログ コレクタの設定を完了または変更した後に、コレクタ グループの ログ冗長性を有効にできます。
コレクタ	コレクタグループに割り当てられたログコレクタを示します。
ログ再配信状態	特定の操作(ログ冗長性の有効化など)を行った場合、コレクタグループ はログコレクタに対しログの再配信を行います。この列は再配信プロセス の完了状態がパーセントで表示されます。

Panorama > Plugins ($\Im \neg \neg \gamma \land \gamma)$)

- Panorama > プラグイン
- デバイス > プラグイン

Panorama 上のサードパーティ統合をサポートするプラグインをインストール、削除、管理する 場合は、Panorama > Plugins(プラグイン)を選択します。

(VM-Series ファイアウォールでのみ利用可能) Device (デバイス) > Plugins (プラグイン)を選択 し、VM-Series ファイアウォール用のプラグインをインストール、削除、管理します。

プラグイン	の意味
アップロード	ローカル ディレクトリからプラグイン インストール ファイルをアップ ロードできます。これは、プラグインをインストールするものではありま せん。インストール ファイルをアップロードすると、インストール リンク がアクティブになります。
ファイル名	プラグイン ファイル名です。
	Panorama に vm_series プラグインをインストールすると Device (デバイス) > VM-Series ページが利用可能になり、そこでパブリック クラウド環境 (AWS、Azure、Google) にデプロイされた VM-Series ファイアウォール 上のテンプレート設定を管理およびコミットできるようになります。
バージョン	プラグイン バージョン ナンバーです。
プラットフォー ム	プラグインがサポートされているモデルです。
リリース日	このプラグイン バージョンのリリース日です。
サイズ	プラグイン ファイル サイズです。
インストール済 み	Panorama の各プラグインの現在のインストールの状態を提示します。
操作	 Install (インストール) – プラグインの特定のバージョンをインストールします。新しいバージョンのプラグインをインストールすると、以前インストールしたバージョンが上書きされます。
	• Delete (削除) – 指定されたプラグイン ファイルを削除します。
	• Remove Config(設定の削除) – このプラグインに関連するすべての設定を削除します。プラグインに関するすべての設定を完全に削除するに
プラグイン	の意味
-------	--
	は、Remove Config(設定の削除)を使用した後にUninstall(アンイン ストール)も実行する必要があります。
	VMware NSX の Panorama プラグインから構成を削除する場合、このア クションはサービス定義とサービス マネージャーのみを削除します。 ゾーン、デバイス グループ、テンプレートなど、他の関連する設定は 削除されません。さらに、Panorama HA 展開でこの操作を完了するに は、アクティブな構成を最初に削除し、セカンダリをアクティブにする フェールオーバーを開始してから、新しいアクティブ ピアで構成を削除 する必要があります。
	 Uninstall (アンインストール) – プラグインの最新インストールを削除 します。Panorama からプラグイン ファイルを削除するものではありま せん。プラグインをアンインストールした場合、そのプラグインに関連 するすべての設定が失われます。関連設定を完全に削除するときにのみ 使用します。

Panorama > SD-WAN

Panorama SD-WAN プラグインをダウンロードしてインストールし、レポートを一元管理、監 視、生成します。ブランチを適切なハブに追加して関連付けることにより、Panorama から SD-WAN トポロジを設定し、ブランチおよびハブ デバイスを適切なゾーンに関連付けます。SD-WAN トポロジを設定した後、設定済のすべてのデバイスとパスを含むパス ヘルス メトリック を監視し、アプリケーションとリンクの問題を区別して、経時のリンク パフォーマンスを把握 することができます。さらに、監査目的のレポートを生成することができます。

操作	以下を参照
ブランチ デバイスとハブ デバ イスを追加、編集、または削 除する	SD-WAN Devices(SD-WAN デバイス)
VPN クラスタを追加、編集、 または削除する	SD-WAN VPN Clusters(SD-WAN VPN クラスタ)
パスのヘルスを監視	SD-WAN Monitoring (SD-WAN モニタリング)
ヘルス レポートの生成	SD-WAN Reports(SD-WAN レポート)

SD-WAN Devices (SD-WAN デバイス)

• Panorama > SD-WAN > デバイス

SD-WAN デバイスは、VPN クラスタおよび SD-WAN トポロジを構成するブランチまたはハブです。

項目	の意味
氏名	SD-WAN デバイスを特定する名称を入力します。
タイプ	SD-WAN デバイスの Type (タイプ) を選択します。
	 Hub (ハブ) –すべてのブランチデバイスが VPN 接続を使用して接続 し、データセンターや事業本部等のプライマリオフィスまたは場所に 展開された集中型ファイアウォール。ブランチ間のトラフィックは、宛 先ブランチに向かう際にハブを通過します。ブランチはハブに接続し、 ハブの場所にある一元化されたリソースにアクセスします。ハブデバイ スは、トラフィックを処理し、ポリシー ルールを適用し、プライマリオ フィスまたは場所でのリンクスワッピングを管理します。
	• Branch(ブランチ)–VPN 接続を使用してハブに接続し、ブランチレベルでセキュリティを提供する物理的なブランチの場所に配置されたファイアウォール。ブランチはハブに接続し、一元化されたリソースにアク

項目	の意味
	セスします。ブランチデバイスは、トラフィックを処理し、ポリシー ルールを適用し、ブランチロケーションでのリンクスワッピングを管理 します。
ルーター名	SD-WAN ハブとブランチ間のルーティングに使用する仮想ルーターまたは論理ルーターを選択します。デフォルトでは、sdwan-default(sdwan-デフォルト) Virtual Router (仮想ルーター - VR)が作成され、Panorama によるルーター設定の自動プッシュが可能となります。
サイト	ハブまたはブランチを識別するユーザーフレンドリーなサイト名を入力し ます。例えば、ブランチ デバイスが展開されている都市名を入力します。
Link Tag (リン ク タグ)	(PAN-OS 10.0.3 以降のリリース)ハブの場合は、ハブ仮想インターフェイス 用に作成した Link Tag を選択して、ハブが DIA AnyPath に参加できるよう にします。自動 VPN は、このリンク タグを、個々のリンクではなく、ハ ブ仮想インターフェース全体に適用します。トラフィック分散プロファイ ルでこのリンク タグを参照し、このハブ仮想インターフェースへのフェイ ルオーバーの順序を示します。ブランチ デバイスでは、Auto VPN はこの タグを使用し、ハブ デバイスで終端する SD-WAN 仮想インターフェース の Link Tag(リンク タグ)フィールドにデータを入力します。
Zone Internet (ゾーン イン ターネット)	1つまたは複数のセキュリティ ゾーンを Add(追加) して、信頼されてい ない送信元との間で送受信されるトラフィックを識別します。
Zone Hub(ゾーン ハブ)	1つまたは複数のセキュリティ ゾーンを Add(追加) して、SD-WAN ハ ブ デバイスとの間で送受信されるトラフィックを識別します。
Zone Branch(ゾー ン ブランチ)	SD-WAN ブランチ デバイスとの間で送受信されるトラフィックを識別する ために、1 つまたは複数のセキュリティ ゾーンをAdd(追加)します。
Zone Internal(内部 ゾーン)	SD-WAN ブランチ デバイスとの間で企業ネットワーク上の信頼できるデバ イスから送信されたトラフィックを識別するために、1つまたは複数のセ キュリティ ゾーンをAdd(追加)します。

[BGP] タブ

BGP	BGP を有効にします。
ルーターID	BGP ルーター ID を指定します。ボーダー ゲートウェイ プロトコル (BGP)ルーター ID は、すべてのルーター間で一意である必要がありま す。

項目	の意味
	ルーター ID としてループバック アドレスを使用します。
Loopback Address(ルー プバック アド レス)	BGP ピアリングのスタティック ループバック IPv4 アドレスを指定します。
AS 番号	Autonomous System number(自律システム番号(AS 番号))を入力し、 一般的に定義されたインターネットへのルーティングポリシーを定義しま す。AS 番号は、ハブとブランチの場所毎で一意である必要があります。 パブリックにルーティング可能な AS 番号と干渉がないよ う、4 バイトのプライベート BGPAS 番号を使用します。
Redistribution Profile Name(再配信 プロファイル 名)	 再配信プロファイルを選択または作成し、ブランチからハブルーターに通信するローカルプレフィックスを制御します。デフォルトでは、ローカルに接続されるすべてのインターネットプレフィックスがハブの場所にアドバタイズされます。 Palo Alto Networks では、ISP から取得したブランチオフィスのデフォルトルートは再配信しません。
アップストリール	ム NAT タブ

Upstream NAT アップストリー ム NAT	アップストリーム NAT を有効にします。
SD-WAN イン ターフェイス	SD-WAN 用に設定されたインターフェイスを選択します。
NAT IP Address Type(NAT IP アドレス タイ プ)	 以下のいずれかを選択します。 Static IP - ハブまたはブランチに対して NAT を実行するデバイスの背後 にある SD-WAN ハブまたはブランチの場合。Auto VPN Configuration がそのアドレスをハブまたはブランチのトンネル エンドポイントとして 使用できるように、アップストリーム NAT 実行デバイス上のパブリッ クインターフェイスの IP アドレスまたは FQDN を指定する必要があり ます。IP Address を選択し、サブネット マスクなしで IPv4 アドレスを 入力するか、FQDN を選択します。
	 DDNS - ブランチに対して NAT を実行しているデバイスの背後にある SD-WAN ブランチ用。NAT デバイス上のインターフェイスの IP アドレ

項目	の意味
	スが Palo Alto Networks DDNS サービスから取得されることを示しま す。

VPN トンネル タブ

ToS ヘッダーの	(PAN-OS 10.2.1 およびそれ以降の 11.1 リリース)元の ToS 情報を保持す
コピー	るために、(サービスのタイプ)ToS フィールド(ToS ビットまたは DiffServ
	コード ポイント(DSCP)マーキング)を内部 IPv4 ヘッダーからカプセル化さ
	れたパケットの VPN ヘッダーにコピーします。ECN(Explicit Congestion
	Notification)フィールドもコピーされます。

SD-WAN VPN Clusters (SD-WAN VPN クラスタ)

• Panorama > SD-WAN > VPN クラスタ

SD-WAN ブランチ デバイスを 1 つまたは複数の SD-WAN ハブ デバイスに関連付けて、ブラン チとハブの所在地間の安全な通信を実現します。SD-WAN VPN クラスタ内のブランチ デバイス とハブ デバイスを関連付けると、ファイアウォールは、指定 VPN クラスタのタイプに基づき、 サイト間に必要な IKE および IPSecVPN 接続を作成します。

項目	の意味
氏名	VPN クラスタを識別する名称を入力します。
タイプ	 SD-WAN VPN クラスタの Type (タイプ) を選択します。 Hub Spoke (ハブスポーク) –プライマリ オフィスまたは所在地の中央ファイアウォールが、VPN 接続を使用して接続したブランチ デバイス間のゲートウェイとして機能する SD-WAN トポロジです。ブランチ間のトラフィックは、宛先ブランチに向かう際にハブを通過します。
ブランチ	1 つまたは複数のハブに関連付ける 1 つまたは複数のブランチ デバイスを Add(追加)します。
ハブ	1つまたは複数のブランチに関連付ける1つまたは複数のハブ デバイスを Add(追加)します。複数のハブが追加されている場合は、パスヘルス品 質メトリックを使用して、プライマリ ハブとセカンダリ ハブを制御しま す。

SD-WAN Monitoring (SD-WAN モニタリング)

• Panorama > SD-WAN > モニタリング

Monitoring(モニタリング)タブは、SD-WAN デバイスヘルスメトリックの概要ウィジェット をすべて表示するダッシュボードです。このツールは、パフォーマンスの問題が発生しているア プリケーションまたはリンクを迅速な特定を実現します。SD-WAN ネットワーク上のアクティ ビティに関する実用的なインテリジェンスを提供します。指定した期間内に、すべての VPN ク ラスタまたは特定の VPN クラスタのパス品質およびリンクのパフォーマンスを表示できます。

アプリケーションのパフォーマンスに影響を与えているブランチ ファイアウォールまたはハブ ファイアウォールがある VPN クラスタと正常な VPN クラスタの総数を一目で確認することが できます。以下のアプリケーションを表示して、VPN クラスタのヘルス状態を結び付けること ができます。

- App Performance (アプリのパフォーマンス)
 - Impacted (影響あり)-選択可能なパスのリストのパス品質プロファイルで指定されたしきい値以下のジッター、遅延、またはパケット損失のパフォーマンスがないパスの VPN クラスタ内の1つまたは複数のアプリケーション。
 - OK-VPN クラスタ内のアプリケーションが正常であり、ジッター、遅延、またはパケット損失のパフォーマンスが発生していません。
- Link Performance (リンクのパフォーマンス)
 - Error (エラー)-選択可能なパスのリストのパス品質プロファイルで指定されたしきい値以下のジッター、遅延、またはパケット損失のパフォーマンスがないパスの VPN クラスタ内の1つまたは複数のサイト。
 - Warning (警告)--VPN クラスタ内の複数のサイトに、メトリックの過去7日間の平均値と比較して低い、ジッター、遅延、またはパケット損失のパフォーマンス測定値のリンクがあります。
 - OK-VPN クラスタ内のリンクが正常であり、ジッター、遅延、またはパケット損失のパフォーマンスが発生していません。

🔶 PANORAMA	ر Device Groups ک DASHBOARD ACC MONITOR POLICIES OBJECTS NE	ETWORK DEVICE PANORAMA		à l'	ter €er Q		
Panorama 🗸					G ()		
CE SCEP	SD-WAN						
Log Ingestion Profile	All VPN Clusters			2020/07/24 03:06pm - 2020	/07/31 03:06 \v		
Log Settings				2020/07/24 15:06:00 to 202	0/07/31 15:06:00		
V Profiles	App Performance						
Svslog							
🔒 Email	🔀 Impacted			🕑 ОК			
🚯 НТТР							
RADIUS							
TACACS+	VDN Chustores 2 / 5			Chustore 3 / F			
LDAP	VPIN Clusters. Z / 5		VEN	Clusters. 0 / 5			
Kerberos			11.hz 2 (0				
Scheduled Config Export	Hubs. V 7 3		Hubs: 3 / 3				
Software •	Pronchos: 2 / 4		Branchas 2 (4				
Dynamic Updates	(Error Correction Initiated)						
는 Plugins 이 이 이 이 이 이 이 이 이 이 이 이 이 이 이 이 이 이 이							
Devices	Link Performance						
VPN Clusters	S Error	•• \\\/	arning				
Monitoring Reports		•••••	arriing	O K			
Licenses •							
🎒 Support 🔹 🔹							
One Device Deployment	VPN Clusters: 4 / 5	VPN Clusters: 0	s: 0 / 5 VPN Clusters: 1 / 5				
GlobalProtect Client							
🛃 Dynamic Updates 🔹	Hubs: 3 / 3	Hubs: O	bs: 0 / 3 Hubs: 0 / 3				
S Plugins							
Master Key and Diagnostics	Branches: 3 / 4	Branches: 0	nes: 0 / 4 Branches: 1 / 4				
Policy Recommendation	·						
< >							
admin Logout Last Login Time	: 07/29/2020 10:30:47 Session Expire Time: 08/29/2020 10:24:05			I active ≠= Tasks Language	🊧 paloalto		

目的のヘルス状態のすべての VPN クラスタの詳細を表示には、ウィジェットをクリックしま す。さらに、サイト フィルタを使用して、リンク通知、遅延偏差、ジッター偏差、パケット損

失偏差、あるいは影響を受けたアプリケーションに基づき VPN クラスタを表示させることができます。

🚺 PANORAMA	DASHBOARD	ACC MONITOR	POLICIES C	ups – DBJECTS	r Template	DEVICE	PANORAMA						📥 🔁	₽ırQ
Panorama 🗸														5 (?)
C SCEP	SD-WAN													0.0
📰 SSH Service Profile	All VPN Clusters > TR2-V	2020/07/24 020409 - 2020/07/21 02040											101.00.07	
R Log Ingestion Profile	2020/07/24 0506pm - 2020/07/30 050000000000000000000000000000000000										07/21 15:04:00			
Log Settings	Profile: Branch	2020/07/24 13:06:00 10 2020/07/31 13:06:00												
SNIMP Tran	App Performance	yp Performance												
System	Q												5	$(tems) \rightarrow \times$
🔒 Email											ERROR CORREC	TED SESSIONS /		
🚯 НТТР	APP A	SD-WAN POLICIE	c .		ORING		IEALTH		DVTES		IMPACTED SESS	SIONS / TOTAL	LINK TACS	
Padius	001.02	30-MAIL FOLICIE	2	3443 100111	oking	orr i	LOL III	ERROR CORRECTION AFFEIL	, DITES		323310143		CableMOdem	
CD SCP	insufficient-data	PD_Weighted		Disabled		• 0	к	PD	19.61 KB		133/0/155		Braodband	-
TACACS+	nto	Test PD		Disabled		• Im	npacted		125.42 K		0/3/1.2k		4G	
LUAP LUAP					Disabled								Braodband	
SAML Identity Provider													CableMOdem	
Scheduled Config Export	ssi	twitchhttps		Multiple	Multiple		к		6.16 MB	6.16 MB		0 / 0 / 3.4k		_
💁 Software 🔹		youtube												
💁 Dynamic Updates 🔹 🔹														-
S Plugins •	PDF/CSV													
V 🧐 SD-WAN	Link Performance													
NPN Clusters													10	itame > V
Monitoring	4				1		1							
Reports	DEVICE	LINK TAG	LINK TYPE		INTERFACE		LINK	APPLIED	INK NOTIFICAT	ONS LATENCY	I	TTER	PACKET LOSS	
Licenses	Branch-Vm100-HA2	No Data	No Data		No Data		ethemet1/4	•	0	😑 Warning	•	Warning	😑 Warning	
Support •	Branch-Vm100-HA1	Braodband	Fiber		ethernet1/2		tl_0102_01549900000069	PD	50	0 eWarning		Warning	😑 Warning	
Software	Branch-Vm100-HA1	No Data	No Data		No Data		tl_0103_01549900000069	•	9 49	😑 Warning	•	Warning	😑 Warning	
GlobalProtect Client	Branch-Vm100-HA2	No Data	No Data		No Data		ethernet1/2	-	0	Warning	•	Warning	Warning	
🛃 Dynamic Updates 🔹	Branch-Vm100-HA2	No Data	No Data		No Data		ethemet1/3		0	Warning		Warning	Warning	
∑} Plugins	Branch-Vm100-HA2	No Data	No Data		No Data		tl 0103 01549900000069		1	Warning		Warning	 Warning 	
🔍 Licenses 🔹	Branch-Vm100-HA1	4G	LTE/3G/4G/5	G	ethernet1/4		tl 0104 01549900000069		52	Warning		Warning	Warning	
Master Key and Diagnostics	Branch-Vm100-HA2	No Data	No Data		No Data		# 0102 0154990000069		1	- Warning		Warning	Warning	-
Policy Recommendation	PDF/CSV	110 0000	No Data		no para		0_0102_01047700000007			- warning		TTOTTING.	- marining	
admin Lopout Last Login Time	× 07/29/2020 10:30:47 L	Session Expire Time: 08/29/2	020 10:24:05	_		_			_		_	⊠ Lactive L %= To	sks Language 🦀	naloalto

SD-WAN Reports (SD-WAN レポート)

• Panorama > SD-WAN > レポート

監査目的で、指定された期間にヘルス劣化の頻度が最も高上位のアプリケーションまたはリンク のアプリケーションまたはリンクのパフォーマンスに関するレポートを生成します。レポート設 定後、レポートを表示するには、Run Now(今すぐ実行)する必要があります。レポートはエ クスポートすることができます。機能は現在利用できません。レポートをエクスポートできる 形式は?

項目	の意味
氏名	レポートの目的を識別する名称を入力します。
レポート タイ プ	 実行するレポートのタイプを選択します。 App Performance(アプリケーションのパフォーマンス) –SD-WAN内のすべてのアプリケーションのトラフィックのヘルスメトリックを詳細に示すレポートを生成します。 Link Performance(リンクのパフォーマンス) –SD-WAN内のリンクのトラフィックのヘルスメトリックを詳細に示すレポートを生成します。
Cluster(クラ スタ)	ドロップダウンでレポートを生成するクラスタを選択します。デフォルト では、all (すべて) が選択されています。

項目	の意味
Site(サイト)	ドロップダウンでレポートを生成するサイトを選択します。デフォルトで は、all (すべて)が選択されています。 クラスタにall (すべて)が選択されている場合は、クラスタに起因するすべ てのサイトのレポートを生成する必要があります。特定のクラスタが選択 されている場合は、レポートを生成する特定のサイトを選択することがで きます。
Application (ア プリケーショ ン) (App Performance Report Type (アプリケー ションパ フォーマンス タイプ) のみ)	ドロップダウンでレポートを生成するアプリケーションを選択します。デ フォルトでは、all (すべて) が選択されています。 サイトで all(すべて) が選択されている場合は、サイトに起因するすべての アプリケーションのレポートを生成する必要があります。特定のサイトが 選択されている場合は、レポートを生成する特定のアプリケーションを選 択することができます。
Link Tag(リン クタグ)(Link Performance Report Type (リンクのパ フォーマンス レポートタイ プ)のみ)	ドロップダウンでレポートを生成するリンク タグを選択します。デフォル トでは、all (すべて) が選択されています。 サイトに all (すべて) が選択されている場合は、サイトで作成されたすべて のリンク タグのレポートを生成する必要があります。特定のサイトが選択 されている場合は、レポートを生成する特定のリンク タグを選択すること ができます。
Link Type (\emptyset 2 2 9 4 7) (Link Performance Report Type ($\emptyset 2 2 0 0$) 7 4 - 7 2 2 2 4 - 7 4 7) $0 3$	ドロップダウンでレポートを生成するリンク タイプを選択します。デフォ ルトでは、all (すべて) が選択されています。 リンク タグに all (すべて) が選択されている場合は、リンク タグの下に作 成されたすべてのリンク タイプのレポートを生成する必要があります。特 定のリンク タグが選択されている場合は、レポートを生成する特定のリン ク タイプを選択することができます。
Top N(上位 N 件)	Top N(上位 N 件)アプリケーションまたはリンクを指定します。レポートに、パフォーマンスの高い上位 5、10、25、50、100、250、500、または1,000 位のアプリケーションまたはリンクを含める設定を選択することができます。デフォルトでは、5 が選択されています。
期間	レポートを実行する期間を設定します。デフォルトでは None (なし)が選 択されており、アプリケーションとリンクのすべてのパフォーマンス デー タを使用してレポートが生成されます。

Panorama > VMware NSX

VM-Series NSXエディションファイアウォールのプロビジョニングを自動化するには、NSX ManagerとPanorama間の通信を有効化する必要があります。PanoramaがVM-Seriesファイア ウォールをNSX Manage 上のサービスとして登録すると、NSX Managerには、新しい VM-Seriesファイアウォールをクラスタ内の各ESXiホストに1つ以上のインスタンスをプロビジョニ ングするために必要な設定が作成されます。

知りたい内容	以下を参照
グループに通知を設定するに は?	通知グループの設定
VM-Series NSXエディション ファイアウォールの設定を定 義するには?	サービス定義を作成する
PanoramaをNSX Managerと通 信するように設定するには?	NSX Manager へのアクセスの設定
VM-Series NSX エディション ファイアウォールのステアリ ング ルールを定義するには?	ステアリング ルールの作成
ダイナミックvSphere環境で、 ファイアウォールがポリシー を常に適用しておくよう設定 するには?	Objects (オブジェクト) > Address Groups (アドレスグ ループ)、および Policies (ポリシー) > Security (セキュ リティ)を選択します。
	Panorama とファイアウォールで仮想環境の変更点を詳しく 把握できるようにするには、セキュリティ ポリシーのプレ ルールの送信元および宛先アドレス オブジェクトとして動 的アドレス グループを使用します。
その他の情報をお探しです か?	「Set up a VM-Series NSX Edition Firewall(VM-Series NSX エディション ファイアウォールのセットアップ)」を参照 してください。

通知グループの設定

• Panorama > Notify Group (通知グループ)

以下の表では、Panorama 通知グループ設定について説明します。

通知グループ設定	の意味
氏名	通知グループの分かりやすい名前を入力します。
Notify Device(通知 デバイス)	ネットワークにデプロイされた仮想マシンへの追加または変更につい て通知を受ける必要があるデバイス グループのボックスをオンにし ます。
	新しい仮想マシンがプロビジョニングされたり、既存のマシンが 変更されたりすると、仮想ネットワークに対する変更内容はアップ デートとしてPanoramaに配信されます。このように設定された場 合、Panoramaは、指定したデバイスグループ内のファイアウォール が動的アドレスグループに登録されたIPアドレスへの変更を受信でき るように、ポリシールールで参照している動的アドレスオブジェクト の入力と更新を行います。
	通知を有効化する場合は、通知を有効化したいすべてのデバイスグ ループを必ず選択するようにしてください。デバイスグループを選択 できない場合は(チェックボックスが表示されない)、そのデバイス グループの階層により自動的に含まれていることを意味します。
	この通知プロセスによって、コンテクストが認識され、ネットワー ク上のアプリケーション セキュリティが維持されます。たとえば、 ハードウェアベースの境界ファイアウォールのグループがあり、新し いアプリケーションまたはWebサーバーがデプロイされた際に通知を 受ける必要がある場合、このプロセスは指定されたデバイスグループ についてダイナミックアドレスグループの自動更新を開始します。さ らに、ダイナミックアドレスオブジェクトを参照するすべてのポリ シールールには、新しくデプロイまたは変更されたアプリケーショ ンまたは Web サーバーが自動的に追加され、基準に基づいてセキュ アに有効にすることができます。

サービス定義を作成する

• Panorama > VMware NSX > Service Definitions (サービス定義)

サービス定義を使用することで、NSX Manager 上に VM-Series ファイアウォールをパートナー セキュリティ サービスとして登録することができます。Panoramaで32個のサービス定義を作成 し、NSX Managerに同期させることができます。

一般的に、ESXiクラスタ内のテナントごとに1つのサービス定義を作成します。それぞれのサービス定義には、ファイアウォールのデプロイに使用するOVF(PAN-OSバージョン)が指定してあり、ESXiクラスタにインストールされているVM-Seriesファイアウォールの設定内容が含まれています。設定内容を指定する場合は、サービス定義に、固有のテンプレート、固有のデバイスグループ、およびそのサービス定義を使用してデプロイされるファイアウォールのライセンス認証コードを含めておく必要があります。デプロイされたファイアウォールは、Panoramaに接続しサービス定義で指定されたデバイスグループ用の設定内容(そのファイアウォールが保護する各テナントや部門のゾーンを含む)とポリシー設定を受信します。

新しいサービス定義を追加する場合は、次の表の説明に従って設定します。

項目	の意味
氏名	NSX Managerに表示したいサービスの名前を入力します。
の意味	(任意) このサービス定義の目的または機能を説明するラベルを入力しま す。
デバイス グルー プ	これらのVM-Seriesファイアウォールを割り当てるデバイスグループまた はデバイスグループ階層を選択します。詳細は、「Panorama > VMware NSX」を参照してください。
テンプレート	VM-Seriesファイアウォールを割り当てるテンプレートを選択します。 詳細は、「Panorama > Templates(テンプレート)」を参照してください。
	サービス定義はそれぞれ固有のテンプレートまたはテンプレートスタッ クに割り当てる必要があります。
	テンプレートは複数のゾーン (NSX Service Profile Zones for NSX (NSX用 のNSXサービスプロファイルゾーン))を割り当てることが可能です。シ ングルテナント型のデプロイについては、テンプレートにゾーン (NSX Service Profile Zone)を1つ作成します。マルチテナント型のデプロイに ついては、それぞれのサブテナントごとにゾーンを作成します。
	新規のNSX Service Profile Zoneを作成した場合、そのゾーンはバーチャ ルワイヤーサブインターフェイスのペアに自動的に割り当てられます。 詳細は、「Network(ネットワーク)> Zones(ゾーン)」を参照してく ださい。
VM-Series の OVF URL	NSX Managerが、新しいVM-Seriesファイアウォールをプロビジョニング するためのOVFファイルにアクセスできるURL(IPアドレスまたはホスト 名とパス)を入力します。
グループに通知	ドロップダウン リストから通知グループを選択します。

NSX Manager へのアクセスの設定

• Panorama > VMware NSX > Service Managers (サービス マネージャ)

Panorama が NSX Manager と通信できるようにするには、Add(追加)をクリックし、以下の 表に記載されている設定を行います。

サービス マネー ジャ	の意味
サービス マ ネージャ名	VM-Series ファイアウォールをサービスとして識別するための名前を入力 します。この名前は、NSX Managerに表示され、VM-Seriesファイアウォー ルを要求に応じてデプロイするために使用されます。 63 文字以内で指定し、英字、数字、ハイフン、およびアンダースコアのみ を使用してください。
の意味	(任意)このサービスの目的または機能を説明するラベルを入力します。
NSX Manager URL	PanoramaがNSX Managerとの接続を確立するために使用するURLを指定します。
NSX Manager ログイン	NSX Manager に設定されている認証情報 (ユーザー名とパスワード) を入力 します。Panoramaは、これらの認証情報を使用してNSX Managerとの認証
NSX Manager パスワード	
NSX Manager パスワードの再 入力	
サービス定義	このサービスマネージャに関連するサービス定義を指定します。各サービ スマネージャは 32 個までのサービス定義をサポートします。

Panorama に変更内容をコミットすると、VMware サービス マネージャのウィンドウに Panorama と NSX Manager の間の接続状態が表示されるようになります。

同期状態	の意味
ステータス	Panorama と NSX Manager 間の接続状態が表示されます。
	正常な接続は登録済みとして表示されます - PanoramaとNSX Managerが同 期され、VM-SeriesファイアウォールはNSX Manager上のサービスとして登 録済みの状態になります。
	接続が失敗した場合、以下のようなステータスが表示されます。
	 Connected Error [接続エラー] - NSX Manager に到達できないか、NSX Manager へのネットワーク接続を確立できません。
	 Not authorized [認証不可] - アクセス資格情報(ユーザー名/パスワード)が正しくありません。

同期状態	の意味	
	 Unregistered [登録なし] - サービス、サービスマネージャ、またはサービスプロファイルが NSX Managerで使用できないか、削除されています。 Out of sync [同期されていません] - Panorama に定義されている設定が、NSX Manager に定義されている設定と異なります。失敗の原因を表示する場合はOut of sync [同期されていません]をクリックします。例えば、NSX Managerのサービス定義のうち、Panoramaで定義された名前と同じものがある可能性があります。このエラーを修正する場合は、エラーメッセージに表示されているサービス定義名を使用して、NSX Managerのサービス定義の検証を行います。PanoramaとNSX Managerの 設定内容が同期されるまで、Panoramaに新しいサービス定義を追加することはできません。 	
動的オブジェク トを同期	 Synchronize Dynamic Objects[動的オブジェクトを同期] をクリックして、NSX Managerからの動的オブジェクト情報の更新を開始します。動的オブジェクトを同期することで、仮想環境の変更に関するコンテクストを維持できます。また、ポリシールール内で使用される動的アドレスグループを自動的に更新させ、アプリケーションを安全に有効化することができます。 Panoramaでは、NSX Managerから動的に登録されたIPアドレスのみを表示できます。ファイアウォールに直接登録されたダ動的IPアドレスは表示されません。VM情報ソース(VM-Series NSXエディションファイアウォールではサポートされていません)を使用している場合、または XML APIを使用してIPアドレスをダ動的にファイアウォールに登録している場合に、動的Pアドレスの完全なリスト(Panoramaがプッシュしたものとローカルに登録されたもの)を表示する場合は、各ファイアウォールにログインする必要があります。 	
NSX設定の同期 化	Panorama で設定されたサービス定義を NSX Manager に同期する場合は NSX Config-Sync (NSX設定の同期化)を選択します。Panoramaで保留中 のコミットがある場合、このオプションは使用できません。 同期が失敗した場合はエラーメッセージの詳細を参照し、エラー がPanoramaとNSX Managerのどちらに起因するものか確認してくだ さい。例えば、NSX Managerのルールで参照されているサービス定義 をPanorama上で削除した場合、NSX Managerとの同期が失敗します。エ ラーメッセージに含まれている情報をもとに、エラーの原因と修正が必要 な箇所 (PanoramaあるいはNSX Manager)を特定します。	

ステアリング ルールの作成

• Panorama > VMware NSX > Steering Rules (ステアリングルール)

ステアリング ルールでは、クラスタのどのゲストからのどのトラフィックを VM-Series ファイ アウォールに進めるのかを決めます。

項目	の意味
Auto-Generate Steering Rules(ステアリ ングルールの自	次のように設定されているセキュリティ ルールに基づいて、ステアリン グ ルールを生成します。
	 NSX サービス マネージャーで登録されている、親または子のデバイス グループに属す。
	• ゾーンが、送信元および宛先と同じである(任意から任意でない)。
	 ゾーンが1つのみである。
	 静的アドレス グループ、IP 範囲、ネットマスクがポリシーに設定されていない。
	デフォルトの場合、Panorama によって生成されるステアリングルー ルでは NSX サービスが設定されず、NSX トラフィック ディレクショ ンは inout (両方向) に設定されます。ステアリングルールが生成され たら、各ステアリングルールを更新して、NSX トラフィック ディレク ションを変更したり、NSX サービスを追加したりすることができます。 ステアリングルールを自動生成すると、Panorama では次のフィールド (Description (内容) と NSX Services (NSX サービス)を除く) に情報 が自動的に入力されます。
氏名	NSX Manager に表示したいステアリング ルールの名前を入力します。 ステアリング ルールを自動生成すると、各ステアリング ルールにプレ フィックス「auto_」が追加され、セキュリティ ポリシー ルール名のス ペースは下線(_) で置き換わります。
の意味	(任意)このサービス定義の目的または機能を説明するラベルを入力します。
NSX トラフィッ ク ディレクショ	VM-Series ファイアウォールにリダイレクトされるトラフィックの方向 を指定します。
ン	 inout(両方向) – 両方向のルールを NSX で作成します。送信元と 宛先の間を移動する、特定タイプのトラフィックは、VM-Series ファ イアウォールにリダイレクトされます。Panorama では、このトラ フィック ディレクションが使用されてステアリング ルールが自動生成 されます。
	 in(受信) – 受信ルールを NSX で作成します。宛先から送信元に移 動する、特定タイプのトラフィックは、VM-Series ファイアウォール にリダイレクトされます。
	 out(発信) – 発信ルールを NSX で作成します。送信元から宛先に移動する、特定タイプのトラフィックは、VM-Series ファイアウォールにリダイレクトされます。

項目	の意味
NSX サービス	VM-Series ファイアウォールにリダイレクトするアプリケーション (Active Directory サーバー、HTTP、DNS など)トラフィックを選択し ます。
デバイス グルー プ	ドロップダウン リストからデバイス グループを選択します。選択したデ バイス グループにより、どのセキュリティ ポリシーをステアリング ルー ルに適用するのかが決まります。デバイス グループは、NSX サービス定 義と関連付けられている必要があります。
セキュリティ ポ リシー:	自動生成のステアリング ルールのベースになるセキュリティ ポリシー ルール。

Panorama > Log Ingestion Profile (ログインジェスト プロファイル)

ログインインジェスト プロファイルを使用して、Panorama が外部ソースからログを受信でき るようにします。PAN-OS 8.0.0 では、Panorama(Panorama モード)は、Syslog を使用して Traps ESM サーバーからログを取り込むことができる Syslog レシーバとして機能できます。新 しい外部ログ ソースのサポートと新しい Traps ESM バージョンの更新は、コンテンツ更新で プッシュされます。

ログインジェストを有効にするには、Panorama を Traps ESM サーバーの Syslog レシーバとし て設定し、Panorama でログインジェスト プロファイルを定義してログ コレクタ グループに割 り当てる必要があります。

新しい外部 Syslog インジェスト プロファイルを追加するには、プロファイルを Add(追加)し、以下の表の説明に従って設定を指定します。

項目	の意味
氏名	Syslog インジェスト プロファイルの名前を入力します。最大 255 個のプ ロファイルを追加できます。
ソース名	ログを送信する外部ソースの名前または IP アドレスを入力します。プロ ファイル内に最大 4 個のソースを追加できます。
ポート	Panorama がネットワーク経由のアクセスで使用するポートを入力しま す。Panorama は、このポートを使用して通信やリッスンを行います。 Traps ESM に 23000 ~ 23999 の値を選択します。Panorama と ESM 間 の通信を有効にするには、Traps ESM で同じポート番号を設定する必要 があります。
転送	TCP、UDP または SSL を選択します。SSL を選択した場合、Panorama > Managed Collectors(管理対象コレクタ) > General(全般)で保護された Syslog 通信の着信証明書を設定する必要があります。
外部ログ タイプ	ドロップダウンからログ タイプを選択します。
バージョン	ドロップダウンからバージョンを選択します。

Monitor (監視) > External Logs (外部ログ) を使用して、Traps ESM サーバーから Panorama に取り込まれたログに関する情報を表示します。

Panorama > Log Settings [Panorama > ログ設定]

以下のログタイプを外部サービスに転送する場合は、Log Settings(ログ設定)ページを使用します。

- Panorama 管理サーバー(Panorama モードの M-Series アプライアンスまたは Panorama バー チャル アプライアンス)がローカルに生成するシステム、設定、User-ID、および相関ログ。
- レガシーモードの Panorama バーチャル アプライアンスがローカルに生成、またはファイア ウォールから収集するすべてのタイプのログ。

ファイアウォールがログコレクタに送信するログに関しては、ログコレクタの 設定を完了して外部サービスへの転送を有効にします。

開始前に、外部サービス用にサーバー プロファイルを定義する必要があります(「Device(デ バイス) > Server Profiles(サーバー プロファイル) > SNMP Trap(SNMP トラップ)」、 「Device(デバイス) > Server Profiles(サーバー プロファイル) > Syslog」、「Device(デバ イス) > Server Profiles(サーバー プロファイル) > Email(電子メール)」、「Device(デバ イス) > Server Profiles(サーバー プロファイル) > HTTP」を参照)。次に、一致リスト プロ ファイルを Add(追加)して、以下の表に記載されているように設定します。

一致リスト プロファイ ル設定	の意味
氏名	一致リスト プロファイルを識別する名前を入力します(最大 31 文 字)。
フィルタ	デフォルトでは、一致リスト プロファイルを追加したタイプの All Logs (すべてのログ) を Panorama は転送します。一部のログを転 送するには、ドロップダウン リストを開いて既存のフィルタを選択 するか、Filter Builder (フィルタ ビルダー)を選択して新しいフィ ルタを追加します。新しいフィルタの各クエリに対して、以下の フィールドを指定して、クエリを Add (追加) します。
	 Connector(条件式) – クエリの結合ロジック(AND/OR)を 選択します。ロジックに否定を適用する場合は、Negate(否定)を選択します。たとえば、信頼されていないゾーン からのログ転送を防ぐには、Negate(上記以外)を選択し、Attribute(属性)として Zone(ゾーン)、Operator(演算子)として equal(等しい)を選択して、Value(値)列に信頼 されていないゾーンの名前を入力します。
	 Attribute(属性) – ログの属性を選択します。オプションは、 ログタイプによって異なります。
	 Operator(演算子) – 属性を適用するかどうかを決定する基準 を選択します(equal(等しい)など)。使用できるオプション は、ログタイプによって異なります。

ー致リスト プロファイ ル設定	の意味
	 Value(値) – クエリが照合する属性値を指定します。 フィルタが一致するログを表示またはエクスポートするには、View Filtered Logs(フィルタリングされたログの表示)を選択します。このタブでは Monitoring(モニタリング)タブのページと同じオプションが表示されます(Monitoring(モニタリング)>Logs(ログ)>Traffic(トラフィック)など)。
の意味	この一致リスト プロファイルの主旨に関する説明を最大 1,024 文 字で入力します。
SNMP	ログを SNMP トラップとして転送するには、1 つ以上の SNMP トラップ サーバー プロファイルを Add (追加) します (「Device (デバイス) > Server Profiles (サーバー プロファイ ル) > SNMP Trap (SNMP トラップ)」を参照)。
電子メール	ログを電子メール通知として転送するには、1つ以上の電子メール サーバー プロファイルを Add (追加) します(「Device (デバイ ス) > Server Profiles (サーバー プロファイル) > Email (電子メー ル)」を参照)。
Syslog	ログを Syslog メッセージとして転送するには、1つ以上の Syslog サーバー プロファイルを Add (追加) します(「Device(デバイ ス) > Server Profiles(サーバー プロファイル) > Syslog」を参 照)。
НТТР	ログを HTTP 要求として転送するには、1 つ以上の HTTP サーバー プロファイルを Add(追加)します(「Device(デバイス) > Server Profiles(サーバー プロファイル) > HTTP」を参照)。
ビルトイン アクション	 システム ログと設定ログ以外のすべてのログ タイプでアクション を設定できます。 アクションを Add (追加) し、そのアクションを説明する名前 を入力します。 タグ付けする IP アドレス (Source Address (送信元アドレ ス) または Destination Address (宛先アドレス)) を選択しま す。 アクション (Add Tag (タグの追加) または Remove Tag (タグ の除去))を選択します。 このデバイスのローカル User-ID エージェントにタグを配信す るか、リモート User-ID エージェントにタグを配信するかを選 択します。

一致リスト プロファイ ル設定	の意味
	 Remote device User-ID Agent(リモートデバイス User-ID エージェント)にタグを配信する場合は、転送できるようにする HTTP サーバープロファイルを選択します。
	 IP 対タグの Timeout (タイムアウト)を指定すれば、IP アドレス 対タグのマッピングを保持する期間(分)を設定できます。タ イムアウトを 0 にすると、IP 対タグのマッピングがタイムアウ トしなくなります(範囲は 0~43200(30日)、デフォルトは 0)。
	タイムアウトを設定できるのはAdd Tag (タグの追加)アクションだけです。
	 ターゲットの送信元または宛先 IP アドレスに対して適用また は削除する Tags (タグ)を入力または指定します。相関ログと HIP マッチ ログでは送信元 IP アドレスのみタグ付けできます。

Panorama > Server Profiles > SCP [Panorama > サーバー プロファイル > SCP]

• Panorama > Server Profiles > SCP [Panorama > サーバー プロファイル > SCP]

Panorama > サーバープロファイル > SCP を選択して、ネットワーク全体でファイルを安全にコ ピーおよび転送するためのセキュア コピー プロトコル (SCP) サーバーの設定を行います。エ アギャップされた Panorama[™]管理サーバーにより管理される管理対象ファイアウォール、ログ コレクタ、およびWildFire[®] アプライアンスに、コンテンツの更新を自動的にダウンロードして インストールすることができます。

DHCP サーバー設定	の意味
氏名	サーバー プロファイルを識別する名前を入力します(最大 31 文 字)。名前の大文字と小文字は区別されます。また、一意の名前 にする必要があります。文字、数字、スペース、ハイフン、およ びアンダースコアのみを使用してください。
SERVER	サーバーの IP アドレスまたは FQDN を入力します。
ポート	ファイル転送用のサーバーポートを入力します(範囲は 1~65,535、デフォルトは 22)。
username	SCP サーバーへのアクセスに使用するユーザー名を入力します。
パスワード パスワードの確認	SCP サーバーへのアクセスに使用されるユーザー名のパスワードを(大文字と小文字を区別して)入力し、確認します。
path	SCP サーバー上のターゲットアップロードディレクトリのパスを 入力します。
指紋	PanoramaとSCPサーバー間の接続を識別および認証するためのSSHホストキーを入力します。

Panorama > Scheduled Config Export [Panorama > スケ ジュール設定された設定のエクスポート]

Panorama およびファイアウォールで実行中のすべての設定のエクスポートをスケジュール設定 する場合、エクスポート タスクを Add(追加)して、以下の表に記載されているように設定し ます。

0

Panorama で高可用性(HA)が設定されている場合は、各ピアで以下の手順を実行して、フェイルオーバー後もスケジュール設定されたエクスポートが継続して実行されるようにする必要があります。Panorama は、スケジュール設定されたエクスポートを HA ピア間で同期しません。

スケジュール設定された設定 のエクスポート設定	の意味
氏名	設定のエクスポート ジョブを識別する名前を入力します(最 大 31 文字)。名前の大文字と小文字は区別されます。また、 一意の名前にする必要があります。文字、数字、ハイフン、お よびアンダースコアのみを使用してください。
の意味	任意の説明を入力します。
Enable [有効化]	エクスポート ジョブを有効にする場合に選択します。
エクスポートの開始予定時 刻 (毎日)	エクスポートを開始する時間を指定します (24 時間形 式、HH:MM 形式)。
PROTOCOL	Panoramaからリモートホストへのログのエクスポートに使用 するプロトコルを選択します。セキュアコピー(SCP)は保護 されたプロトコルである一方、FTPは保護されていません。
ホスト名	宛先のSCPまたはFTPサーバーの、IPアドレスまたはホスト名 を入力してください
ポート	ファイル転送先 FTP サーバーのポート番号を入力します。
path	宛先サーバー上の、エクスポートした設定を保存するフォルダ やディレクトリへのパスを指定します。
	例えば、設定バンドルが、Panoramaというトップフォルダの 中のexported_configというフォルダに保存されている場合、 各サーバータイプ用の構文は以下のようになります。
	• SCPサーバー://Panorama/exported_config
	・ FTPサーバー://Panorama/exported_config

スケジュール設定された設定 のエクスポート設定	の意味
	以下の文字: .(ピリオド)、+、 { および }、 /、 -、 _、 0-9、 a-z、および A-Z。このファイルPath (パス)ではスペースはサ ポートされていません。
FTP パッシブモードの有効 化	FTP パッシブ モードを使用する場合に選択します。
username	送信先での認証に必要なユーザー名を指定します。
パスワード/再入力 パス ワード	送信先での認証に必要なパスワードを指定します。 最長 15 文字のパスワードを使用します。ファイアウォールは SCP サーバーに接続しようと試みる際にパスワードを復号化 し、復号化されたパスワードは 63 文字以下でなければならな いため、パスワードが 15 文字を超えるとテスト SCP 接続にエ ラーが表示されます。
SCP サーバー接続のテスト	Panorama と SCP ホスト/サーバー間の通信をテストする場合 に選択します。 ポップアップ ウィンドウが表示され、SCP サーバ接続をテス トしてデータの安全な転送を有効にするために、クリア テキ スト Password を入力してから Password の確認 を入力する必 要があります。Panorama に HA 設定がある場合は、各 HA ピ アでこの手順を実行して、各ピアが SCP サーバに正常に接続 できるようにします。Panorama が SCP サーバーに正常に接続 できる場合。

Panorama > Software [Panorama > ソフトウェア]

このページでPanorama管理サーバーにあるPanoramaソフトウェアアップデートを管理します。

- Panorama ソフトウェア更新の管理
- Panorama ソフトウェア更新情報の表示

Panorama ソフトウェア更新の管理

次の表で説明するタスクを実行するには、Panorama > Software(ソフトウェア)を選択します。

デフォルトでは、ソフトウェアのアップデートがPanorama管理サーバーに最大2個 保存されます。新しいアップデート用の空き領域を確保するために、サーバーは最 も古いアップデートを自動的に削除します。Panorama によって保存されるソフト ウェアイメージの数を変更して、イメージを手動で削除し、空き領域を確保できま す。

バージョンの互換性についてはPanorama用コンテンツとソフトウェアのアップデートをインストールを参照してください。

タスク	の意味
今すぐチェック	Panorama がインターネットに接続されている場合は、Check Now(今す ぐチェック)をクリックして、最新のアップデート情報を表示することが できます(「Panorama ソフトウェア更新情報の表示」を参照してくださ い)。 Panoramaが外部ネットワークに接続されていない場合は、インターネット
	ブラウザを使用してソフトウェアアップデートのサイトから更新情報にアクセスしてください。
アップロード	Panorama がインターネットに接続されていない状態でソフトウェアイ メージをアップロードする場合に、インターネット ブラウザを使用してソ フトウェア アップデートのサイトにアクセスして必要なリリースを特定 し、Panorama がアクセス可能なコンピューターへソフトウェア イメージ をダウンロードする場合は、Panorama > Software(ソフトウェア)を選 択して Upload(アップロード)をクリックし、Browse(参照)からソフ トウェア イメージを選択して OK をクリックします。アップロードが完 了すると、Downloaded(ダウンロード済)列にチェックマークが表示さ れ、Action(アクション列には Install(インストール)と表示されます。
推奨リリース (PAN-OS 11.1.3以降)	優先リリースの一覧を表示するには、[Preferred Releases (優先リリース)]チェックボックスをオンにします。優先リリースは、最新かつ高度な機能を提供します。安定性と最適なパフォーマンスのために、優先リリースを使用していることを確認します。

タスク	の意味
	デフォルトでは、優先リリースと基本リリースの両方が選択されていま す。 Panoramaが外部ネットワークにアクセスできない場合は、ブラウザを使用 してソフトウェアアップデートサイトにアクセスし、優先リリースを確認 してください。
基本リリース (PAN-OS 11.1.3以降)	基本リリースのリストを表示するには、[Base Releases (基本リリース)]チェックボックスをオンにします。ベースリリースは、特定のリリースの最も初期のバージョンです。 デフォルトでは、優先リリースと基本リリースの両方が選択されます。 Panoramaが外部ネットワークに接続されていない場合は、ブラウザを使用 してソフトウェアアップデートのサイトから基本リリースにアクセスして ください。
検証	 Panorama がインターネットにアクセスできる場合は、Validate (Action 列) を目的のリリースにします。アップグレードするデバイスを選択し ([展開] 列)、アップグレード ソースとして Panorama を選択し、Download をク リックします。ダウンロードが完了すると、Downloaded (ダウンロード 済)列にチェックマークが表示されます。 SCP Server および Update Server は、PAN-OS 10.2.0 のダウン ロード ソース として利用できません。
インストール	ソフトウェア イメージを Install(インストール)します(Action(アク ション)列)。インストールが完了するとPanorama再起動の際に一度ログ アウトが行われます。
	 Panorama システム ファイルの破損を回避するため、Panorama では定期的にファイル システムの整合性チェック (FSCK) が実行されます。このチェックは、再起動を8回行った後、または前回のFSCKから90日経過した後の再起動で実行されます。FSCKが進行中であり完了するまでログインできない場合は、WebインターフェイスとSSHログイン 画面に警告が表示されます。この処理が終了する時間は、ストレージシステムのサイズによって異なり、大きなシステムの場合はPanoramaにログインできるようになるまで数時間かかることもあります。進捗状況を表示するには、Panoramaへのコンソールアクセスをセットアップします。

タスク	の意味
	変更、修正、既知の問題、互換性の問題、およびデフォルト動作の変更を 確認できます。
	Panoramaがインターネットに接続されていない場合は、インターネットブ ラウザを使用してソフトウェアアップデートのサイトにアクセスし、必要 なリリースをダウンロードしてください。
×	不要になった場合や他のイメージ用に空き容量を確保したい場合に、ソフ トウェアイメージを削除することができます。

Panorama ソフトウェア更新情報の表示

Panorama > Software(ソフトウェア)を選択し、以下の情報を表示します。Palo Alto Networksの最新情報を表示する場合は**Check Now**[今すぐチェック]をクリックします。

ソフトウェアと コンテンツの アップデート情 報	の意味
バージョン	Panoramaのソフトウェアバージョン
サイズ	ソフトウェアイメージのサイズ(メガバイト単位)
リリース日	Palo Alto Networksがアップデートを公開した日時
使用可能	イメージがインストール可能かどうかを示します
現在インストー ル済み	アップデートのインストールが完了するとチェックマークが表示されます。
操作	イメージに対して実行可能な操作(Download[ダウンロード]、Install[イン ストール]、Reinstall[再インストール])を示します。
リリース ノー ト	Release Notes[リリースノート]をクリックして目的のソフトウェアリリー スのリリースノートを参照し、リリースの変更、修正、既知の問題、互換 性の問題、およびデフォルト動作の変更を確認します。
X	不要になった場合やダウンロード/アップロード用に空き容量を確保したい 場合に、アップデートを削除することができます。

Panorama > Device Deployment [Panorama > デバイス のデプロイ]

Panorama を使用して、ソフトウェアおよびコンテンツ更新を複数のファイアウォールやログコレクタにデプロイしたり、ファイアウォール ライセンスを管理したりできます。

確認すべき情報	以下を参照
ソフトウェアおよびコンテン ツ更新をファイアウォールや ログ コレクタにデプロイす る。	ソフトウェアおよびコンテンツ更新の管理
インストール済みのソフト ウェアおよびコンテンツ更 新や、ダウンロードとインス トールが可能なソフトウェア およびコンテンツ更新を確認 する。	ソフトウェアおよびコンテンツ更新情報の表示
ファイアウォールやログコレ クタの自動アップデートのス ケジュールを設定したい	コンテンツ用動的更新のスケジュール設定
1 つまたは複数のファイア ウォールのコンテンツ バー ジョンを Panorama から元に 戻します。	Panorama でコンテンツ バージョンを元に戻す
ライセンスを表示、アクティ ベート、ディアクティベー ト、更新する。 ファイアウォールライセンス の状態を確認する	ファイアウォールのライセンス管理
その他の情報をお探しです か?	ライセンスの管理と更新

ソフトウェアおよびコンテンツ更新の管理

• Panorama > Device Deployment(デバイスのデプロイ) > Software(ソフトウェア)

Panorama の次のオプションにより、ソフトウェアとコンテンツのアップデートをファイア ウォールとログ コレクタにデプロイできます。 管理(MGT) インターフェイスのトラフィックを削減するには、更新のデプロ イのために個別のインターフェイスを使用するように Panorama を設定します (「Panorama > Setup(セットアップ) > Interfaces(インターフェイス)」を参 照)。

Panorama デバ イスのデプロイ のオプション	の意味
ダウンロード	インターネットに接続されているPanoramaでソフトウェアまたはコンテン ッのアップデートをデプロイしたい場合は、アップデートのDownload[ダ ウンロード]を行います。ダウンロードが完了すると、使用可能な列に「ダ ウンロード済み」と表示されます。ダウンロードが完了すると以下の操作 が可能になります。
	 PAN-OS/Panorama のソフトウェアやコンテンツのアップデートのイン ストール。
	 GlobalProtect[™] アプリまたは SSL VPN クライアント ソフトウェア アッ プデートの Activate(有効化)。
アップグレード	BrightCloud URLフィルタリングコンテンツのアップグレードが入手可能な 場合はUpgrade[アップグレード]をクリックします。アップグレードが正常 に行われたら、アップデートをファイアウォールにインストールします。
インストール	PAN-OS ソフトウェア、Panorama ソフトウェア、コンテンツ アップ デートをダウンロードまたはアップロードしたら、Action(操作)列の Install(インストール)をクリックし、以下のように選択します。
	 Devices[デバイス] - アップデートを適用するファイアウォールまたは ログコレクタを選択します。リストが長すぎる場合はフィルタを使用し ます。高可用性(HA)ピアであるファイアウォールをグループ化する 場合は、Group HA Peers[HAピアのグループ化]を選択します。HA に設 定されたファイアウォールを簡単に識別できるようになります。特定の ファイアウォールまたはログコレクタのみを表示する場合は、表示した いものを選択してFilter Selected[選択項目でフィルタ]を実行します。
	 Reboot device after install (インストール後にデバイスを再起動) (ソ フトウェアのみ) – インストール プロセスで自動的にファイアウォー ルまたはログ コレクタを再起動する場合に選択します。再起動するまで インストールは完了しません。
	 Disable new apps in content update (コンテンツアップデート時に新しいアプリケーションを無効にする) (アプリケーションと脅威のみ) 前回インストールしたアップデート内容と比較して、今回のアップデートに新しく含まれているアプリケーションを無効化する場合はこのオプションを選択します。これにより最新の脅威を防ぎながらも、ポリシーアップデートを行ったのちに、アプリケーションを有効化していくといった柔軟な対応が可能です。アプリケーションを有効化したい場

Panorama デバ イスのデプロイ のオプション	の意味
	合、ファイアウォールにログインして、 Device [デバイス] > Dynamic Updates[動的更新] を開き、機能の列にあるApps [アプリ] をクリックし て新しいアプリケーションを表示し、有効化したいアプリケーションご とにEnable/Disable [有効化/無効化] の設定を選びます。
	Panorama > Managed Devices (管理対象デバイス)を選択 してファイアウォール ソフトウェアとコンテンツのアッ プデートをインストールするか、Panorama > Managed Collectors (管理対象コントローラ)を選択して専用ログコレ クタのソフトウェア アップデートをインストールすることも できます。
アクティベート	GlobalProtect アプリ ソフトウェアのアップデートをダウンロードまた はアップロードしたら、Action(操作)列の Activate(アクティベー ト)をクリックし、以下のようにオプションを選択します。
	 Devices[デバイス] - アップデートをアクティベートするファイアウォー ルを選択します。リストが長すぎる場合はフィルタを使用します。 高可用性(HA)ピアであるファイアウォールをグループ化する場合 は、Group HA Peers[HAピアのグループ化]を選択します。HA に設定さ れたファイアウォールを簡単に識別できるようになります。特定のファ イアウォールのみを表示するには、該当のファイアウォールを選択し て、Filter Selected[選択項目でフィルタ]を実行します。
	 Upload only to device (デバイスにアップロードのみ行う) – PAN-OS にアップロードしたイメージを自動的にアクティベートしたくない場合 に選択します。ファイアウォールにログインし、アクティベートする必 要があります。
リリース ノー ト	Release Notes[リリースノート]をクリックして目的のソフトウェアリリー スのリリースノートを参照し、リリースの変更、修正、既知の問題、互換 性の問題、およびデフォルト動作の変更を確認します。
ドキュメント	希望のコンテンツリリースに関するリリースノートを参照したい場合 はDocumentation[ドキュメント]をクリックします。
×	ソフトウェアやコンテンツアップデートが不要になった場合や、ダウン ロード/アップロード用に空き容量を確保したい場合に、これらを削除する ことができます。
今すぐチェック	Check Now(今すぐチェック)し、ソフトウェアとコンテンツのアップ デートの情報を表示します。

Panorama デバ イスのデプロイ のオプション	の意味
アップロード	Panorama がインターネットに未接続の状態でソフトウェアやコンテンツ アップデートをデプロイしたい場合は、ソフトウェア アップデートまた は動的更新のサイトからコンピュータへアップデートをダウンロードし、 アップデートのタイプに対応した Panorama > Device Deployment (デバ イスのデプロイ) ページを選択して、Upload (アップロード) をクリック し、アップデートの Type (タイプ)を選び (コンテンツのアップデート のみ)、アップロードされたファイルを選択し、OK をクリックします。 タイプに基づき、以下の手順に従って更新のインストールまたはアクティ ベーションを行います。
	 PAN-OS or Panorama software (PAN-OS または Panorama ソフトウェア) - アップロードが完了すると、Downloaded (ダウンロード済み列にチェックマークが表示され、Action (アクション)列には Install (インストール)と表示されます。
	 GlobalProtect Client or SSL VPN Client software (GlobalProtect クライ アントまたは SSL VPN クライアント ソフトウェア) – ファイルからア クティベートします。
	• Dynamic updates(動的更新) – ファイルからインストールします。
推奨リリース (PAN-OS 11.1.3以降)	優先リリースの一覧を表示するには、[Preferred Releases (優先リリース)]チェックボックスをオンにします。優先リリースは、最新かつ高度な機能を提供します。安定性と最適なパフォーマンスのために、優先リリースを使用していることを確認します。
	デフォルトでは、優先リリースと基本リリースの両方が選択されていま す。
	Panoramaが外部ネットワークにアクセスできない場合は、ブラウザを使用 してソフトウェアアップデートサイトにアクセスし、優先リリースを確認 してください。
基本リリース (PAN-OS 11.1.3以降)	基本リリースのリストを表示するには、[Base Releases (基本リリース)]チェックボックスをオンにします。ベースリリースは、特定のリリースの最も初期のバージョンです。
	デフォルトでは、優先リリースと基本リリースの両方が選択されます。
	Panoramaが外部ネットワークに接続されていない場合は、ブラウザを使用 してソフトウェアアップデートのサイトから基本リリースにアクセスして ください。
ファイルからイ ンストール	コンテンツ アップデートのアップロード後、Install from File(ファイルか らインストール)をクリックしてコンテンツの Type(タイプ)を選択し、

Panorama デバ イスのデプロイ のオプション	の意味
	アップデートのファイル名を選び、さらにファイアウォールまたはログ コ レクタを選択します。
ファイルからア クティベーショ ン	GlobalProtect アプリ ソフトウェアのアップデートのアップロード 後、Activate from File(ファイルからアクティベート)をクリックし、 アップデートのファイル名を選び、ファイアウォールを選択します。
スケジュール	コンテンツ用動的更新をスケジュールする場合に選択します。

ソフトウェアおよびコンテンツ更新情報の表示

• Panorama > Device Deployment (デバイスのデプロイ) > Software (ソフトウェア)

Panorama > Device Deployment (デバイスのデプロイ) > Software (ソフトウェア) を選択 し、現在インストールされている、または、ダウンロードやインストールが可能な PAN-OS ソ フトウェア、GlobalProtect クライアント ソフトウェア、動的更新 (コンテンツ) を表示しま す。Dynamic Updates[動的更新]のページでは情報がコンテンツタイプ (アンチウイルス、アプ リケーションと脅威、URLフィルタリング、およびWildFire) によって整列され、最後に更新情 報を確認した日時が表示されています。Palo Alto Networksのソフトウェアやコンテンツの最新 情報を表示する場合はCheck Now[今すぐチェック]をクリックします。

ソフトウェアとコ	コンテンツのアップデート情報
バージョン	ソフトウェアまたはコンテンツアップデートのバージョン
ファイル名	アップデートファイルの名前
プラットフォー ム	アップデートが指定されたファイアウォールまたはログ コレクタ モデ ル。数字はハードウェア ファイアウォール モデル(たとえば、7000 は PA-7000 シリーズ ファイアウォールを指します)を、vm は VM-Series ファイアウォールであることを示し、m は M-Series アプライアンスである ことを示します。
機能	(コンテンツのみ)コンテンツバージョンに含まれている可能性があるシ グネチャタイプの一覧が表示されます。
タイプ	(コンテンツのみ)ダウンロードにフルデータベースアップデートが含ま れているか、増分更新が含まれているかを示します。
サイズ	アップデートファイルのサイズ
リリース日	Palo Alto Networksがアップデートを公開した日時

ソフトウェアとコンテンツのアップデート情報	
使用可能	(PAN-OSまたはPanoramaソフトウェアのみ)アップデートがダウンロー ド済みまたはアップロード済みであることを示します。
ダウンロード済 み	(SSL VPNクライアントソフトウェア、GlobalProtectクライアントソフト ウェア、またはコンテンツのみ)チェックマークはアップデートがダウン ロード済みであることを示します。
操作	アップデートに対して実行可能な操作を示しています。ダウンロード、 アップグレード、インストール、アクティベーション。
ドキュメント	(コンテンツのみ)希望するコンテンツリリースに関するリリースノート へのリンクが提供されます。
リリース ノー ト	(ソフトウェアのみ)希望するソフトウェアリリースに関するリリース ノートへのリンクが提供されます。
X	アップデートが不要になった場合や、ダウンロード/アップロード用に空き 容量を確保したい場合に、これを削除することができます。

コンテンツ用動的更新のスケジュール設定

 Panorama > Device Deployment > Dynamic Updates [Panorama > デバイスのデプロイ > 動的 更新]

更新の定期的な自動ダウンロードおよびインストールを設定する場合は、Schedules(スケ ジュール)をクリックし、Add(追加)を選び、以下の表に記載されているように設定します。

動的更新のスケジュール設定	
氏名	スケジュール設定するジョブを識別するための名前を入力します(最大 31 文字)。この名前は、大文字と小文字が区別され、一意でなければなら ず、文字、数字、ハイフン、アンダースコアのみで構成されます。
disabled	スケジュール設定したジョブを無効化する場合に選択します。
Download Source(送信 元のダウンロー ド)	コンテンツ更新のために Download Source(送信元のダウンロード)を選 択します。Palo Alto Networks Updates Server (パロアルトネットワークス の更新サーバ)または SCP サーバからコンテンツの更新のダウンロードを 選択できます。
SCP Profile(SCP プ ロファイル) (SCP のみ)	ダウンロード元の設定済 SCP プロファイルを選択します。

動的更新のスケジュール設定	
SCP Path(SCP パス) (SCP の み)	コンテンツ更新のダウンロード元となる SCP サーバー上の特定のパスを入 力します。
タイプ	スケジュールを設定したいコンテンツのタイプを選択します。App[アプリ ケーション]、App and Threat[アプリケーションと脅威]、Antivirus[アンチ ウイルス]、WildFire、またはURL Database[URLデータベース]。
繰り返し	Panorama が更新サーバーにチェックインする間隔を選択します。繰り返し オプションは、更新のタイプによって異なります。
時間	Daily [毎日] 更新の場合、24 時間形式で Time [時刻] を選択します。 Weekly [毎週] 更新の場合、 Day [曜日] と、24 時間形式で Time [時刻] を選択 します。
コンテンツ更新 での新しいアプ リケーションの 無効化	更新の Type (タイプ) を App (アプリケーション) または App and Threat (アプリケーションと脅威) に設定し、Action (アクション) を Download and Install (ダウンロードとインストール) に設定している場合 のみ、コンテンツ更新での新しいアプリケーションを無効化できます。 前回インストールした更新にはない、新しく含まれているアプリケーショ ンを無効化する場合に選択します。これにより最新の脅威を防ぎながら も、ポリシーアップデートを行ったのちに、アプリケーションを有効化し ていくといった柔軟な対応が可能です。アプリケーションを有効化したい 場合、ファイアウォールにログインして、Device [デバイス] > Dynamic Updates[動的更新] を開き、機能の列にあるApps [アプリ] をクリックし て新しいアプリケーションを表示し、有効化したいアプリケーションごと にEnable/Disable [有効化/無効化] の設定を選びます。
操作	 Download Only[ダウンロードのみ] - Panorama[™] は定期的に更新をダウンロードします。ファイアウォールおよびログコレクタには、更新を手動でインストールする必要があります。 Download and Install[ダウンロードおよびインストール] - Panoramaは定期的にアップデートをダウンロードし、自動的にインストールを行います。 Download and SCP(ダウンロードおよび SCP) – Panorama がコンテンツ更新パッケージをダウンロードして、指定された SCP サーバーに転送します。
機器	Devices[デバイス]を選び、定期的なコンテンツアップデートを受信させる ファイアウォールを選択します。

動的更新のスケジュール設定

ログ コレクタ

Log Collectors[ログコレクタ]を選び、定期的なコンテンツアップデートを 受信させる管理対象コレクタを選択します。

Panorama でコンテンツ バージョンを元に戻す

 Panorama > Device Deployment > Dynamic Updates [Panorama > デバイスのデプロイ > 動的 更新]

1 つまたは複数のファイアウォールへのアプリケーション、アプリケーションと脅威、ア ンチウィルス、WildFire、WildFire のコンテンツアップデートを、以前にインストールした Panorama のコンテンツ バージョンから、すばやくRevert Content(コンテンツを元に戻す)こ とができます。元に戻すコンテンツ バージョンは、現在ファイアウォールにインストールさ れているバージョンより古いバージョンである必要があります。コンテンツを元に戻す操作 は、Panorama 8.1 を実行することで利用できます。ファイアウォール上のコンテンツは、元に 戻す機能がファイアウォール上でローカルで使用可能な限り、元に戻すことができます。

項目	の意味
フィルタ	コンテンツを元に戻したいデバイスにフィル タを適用します。次のフィルタを使用できま す。 ・ デバイス状態 ・ プラットフォーム ・ デバイスグループ ・ テンプレート ・ tags ・ HA 状態 ・ ソフトウェアのバージョン (PAN-OS) ・ 現在のコンテンツのバージョン
機器	 元に戻すデバイスを1つ以上選択します。次のデバイス情報を表示します。 デバイス名-ファイアウォールの名前です。 現在のバージョン-デバイスにインストールされている現在のコンテンツバージョンです。コンテンツバージョンがインストールされていない場合、列に0が表示されます。

項目	の意味
	 以前のバージョン(コンテンツ)-PAN 8.1 以降を実行しているファイアウォール に以前にインストールされたコンテンツ バージョンです。コンテンツバージョン が以前にインストールされていない場合、 またはファイアウォールが 8.1 より前の PAN-OS バージョンを実行している場合 は、列は空白になります ソフトウェアのバージョン-デバイスに
	インストールされている現在の PAN-OS バージョンです。
	 HA ステータス– HA ペアの場合の HA ス テータスを表示します。デバイスが HA ペ アにない場合、列は空白になります。
グループ HA ペア	HA ピアをグループ化するにはこのボックス にチェックを入れます。

元に戻すデバイスを選択したら、OK をクリックします。

ファイアウォールのライセンス管理

• Panorama > Device Deployment > Licenses [Panorama > デバイスのデプロイ > ライセンス]

Panorama > Device Deployment(デバイスのデプロイ) **> Licenses**(ライセンス)を開き、以下のタスクを行ってください。

- インターネットに直接接続されていないファイアウォールのライセンスを更新します。Refresh(更新)をクリックしてください。
- ファイアウォールのライセンスをアクティベートします。ファイアウォールのライセンスを アクティベートする場合、Actibvate(アクティベート)をクリックし、ファイアウォールを 選択し、認証コードの列で Palo Alto Networks がファイアウォール用に配布した認証コード を入力します。
- VM-Series ファイアウォールにインストールされたすべてのライセンスやサブスクリプション/資格をディアクティベートします。Deactivate VMs(VMのディアクティベート)をクリックし、ファイアウォールを選択し(一覧には PAN-OS 7.0 以上のリリースを実行しているファイアウォールのみが表示されます)、次のうちいずれかをクリックします。
 - Continue[続行] ライセンスをディアクティベートして、変更をライセンス サーバーに自動的に登録します。ライセンスのクレジットがアカウントに戻されて、ライセンスが再利用可能になります。
 - Complete Manually[手動で実行] トークンファイルを生成します。Panorama からインターネットに直接アクセスできない場合、これを使用します。ディアクティベートの操作を完了する為には、サポートポータルにログインし、Assets (アセット)を選択し、Deactivate License(s) (ライセンスのディアクティベート)をクリックしてトークンファ

イルをアップロードし、Submit (送信)をクリックする必要があります。その後、ディアク ティベート プロセスを完了します。

管理対象ファイアウォールの現在のライセンス状態を表示することもできます。ファイアウォー ルがインターネットに直接接続されている場合、Panorama はライセンス サーバーに毎日自動的 にチェックインを行い、ライセンスの延長や更新を取得し、それらをファイアウォールにプッ シュします。チェックインは午前1時から2時の間に行われるようハードコードされており、こ の時間を変更することはできません。

ファイアウォール	のライセンス情報	
デバイス	ファイアウォール名	-
仮想システ ム(vsys)	ファイアウォールが複数の仮想システムをサポートす る しな い 冬 を示します。	かか
脅威防御	ライセンスが有	_
URLプロテク ションの	x)♥ 無 効⊗	```````````````````````````````````````
support	または期限切 れ [▲]	(有
GlobalProtectゲー トウェイ	_ 効期限日も表示されます)であることを示します。	
GlobalProtectポー タル		
WildFire		_
VM-Series 容量	これがVM-Seriesファイアウォールである か、 か	否 を

Panorama >デバイス登録認証キー

新しいファイアウォール、Log Collectors、および WildFire アプライアンスを Panorama[™] 管理 サーバーにオンボーディングする際のセキュリティポスチャを強化するには、新しいデバイス と最初の接続時の Panorama 管理サーバー間の相互認証のためのデバイス登録認証キーを作成 します。特定の値を使用して認証キーを設定できます: キーの有効期間、デバイス登録認証キー を使用して新しいファイアウォールをオンボードできる回数を決定する回数、デバイス登録認 証キーが有効な 1 つ以上のシリアル番号のリスト、認証キーが有効なデバイスの種類を指定し ます。Panorama で認証キーを作成したら、Panorama 管理へのオンボーディング中に、新しい ファイアウォール、ログ コレクタ、または WildFire アプライアンスに追加する必要がありま す。

デバイス登録認 証キー フィール ド	詳説
名前	デバイス登録認証キーの名前。この名前は、大文字と小文字が区別され、 デバイス グループ階層全体で一意でなければならず、文字、数字、スペー ス、ハイフン、アンダースコアのみで構成されます。
有効期間	キーの有効期間は、新しいファイアウォール、Log Collectors、および WildFire アプライアンスをオンボードするために、デバイス登録認証キー が有効な日数、時間数、および分数を表示します。
数	デバイス登録認証キーを使用して、新しいファイアウォール、Log Collectors、および WildFire アプライアンスをオンボードできる回数。
serial	デバイス登録認証キーが有効な1つ以上の新しいファイアウォール、Log Collectors、および WildFire アプライアンスのシリアル番号。
タイプ	認証キーが有効なデバイスの種類(、 ファイアウォール 、または Log Collector)。

デバイス登録認証キーの追加

新しいファイアウォール、Log Collectors、WildFire アプライアンスを Panorama に追加して、 デバイス登録認証キーを設定します。

デバイス登録認 証キーの設定	詳説
名前	デバイス登録認証キーを識別する名前を入力します。この名前は、大文字 と小文字が区別され、デバイス グループ階層全体で一意でなければなら
デバイス登録認 証キーの設定	詳説
-------------------	---
	ず、文字、数字、スペース、ハイフン、アンダースコアのみで構成されま す。
有効期間	デバイス登録認証キーを使用して新しいファイアウォール、Log Collectors、WildFire アライアンスをオンボードできる期間のキーの有効期 間を指定します。
数	認証キーを使用して新しいファイアウォール、Log Collector、および WildFire アプライアンスをオンボードできる回数を指定します。
デバイスタイプ	デバイス登録認証キーを使用できるデバイスを指定します。 ファイア ウォール 、ログ コレクタ 、または 任意の (デフォルト)。
デバイス	ファイアウォール、Log Collector、および WildFire アプライアンスのシ リアル番号を入力して、デバイス登録認証キーが有効なファイアウォー ル、Log Collectors、および WildFire アプライアンスを指定します。