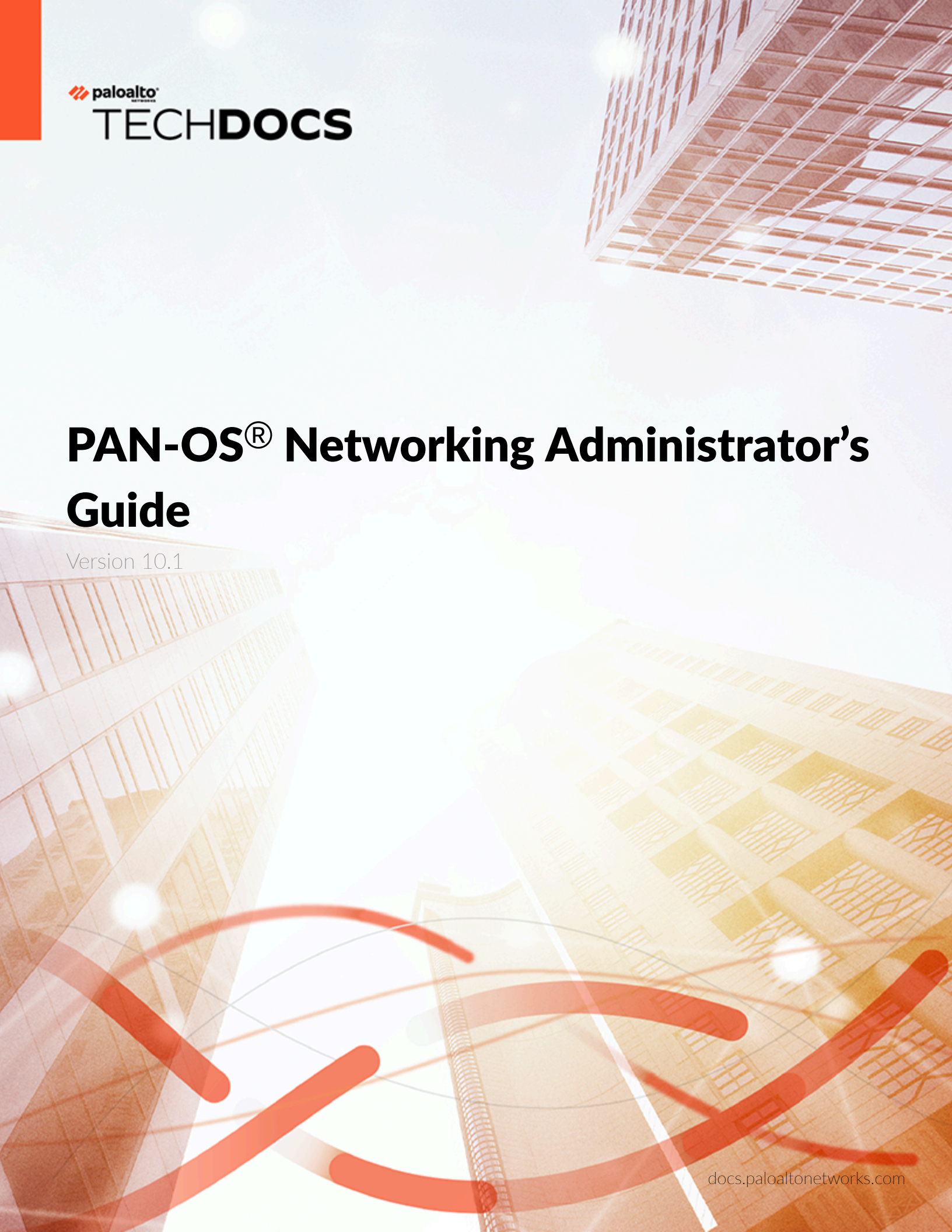
paloalto TECHDOCS

PAN-OS® Networking Administrator's Guide

Version 10.1



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

Last Revised

August 9, 2021

Table of Contents

ネットワーキング

Palo Alto Networks® の次世代ファイアウォールでは、ダイナミック ルーティング、スイッチング、および VPN 接続のサポートなど、柔軟なネットワーク アーキテクチャを提供し、さまざまなネットワーク環境でファイアウォールのデプロイを可能にします。

> ネットワークの概要

ネットワークの概要

ネットワークは、データを受信し、処理し、転送できる必要があるため、ファイアウォールの基本的な構成要素です。ファイアウォールで Ethernet ポートを設定する場合、タップ、仮想ワイヤ、レイヤ 2、レイヤ 3、または AE インターフェイスの展開を選択できます。さらに、さまざまなネットワーク セグメントに統合できるように、異なるポートでさまざまなインターフェイス タイプを設定できます。

ネットワーキングを開始するには、まずPAN-OS ® AdministratorのGuideのGetting Startedトピックにアクセスする必要があります。ここでは、ネットワークのセグメント化と の設定インターフェイスとゾーン について学習します。この初期タスクは、インターネット、内部ネットワーク、およびデータセンター アプリケーションに接続するようにレイヤ 3 インターフェイスを設定する方法を示しています。

この PAN-OS Net!作業 Administrator の Guide は、タップ、仮想ワイヤ、レイヤ 2、レイヤ 3、および AE インターフェイスの設定方法に関するトピックを含む、その情報について詳しく説明します。ネットワークインターフェイスを設定した後、Export Configuration Table Data を PDF または CSV として内部レビューまたは監査を行うことができます。

また、ファイアウォールが複数の仮想ルータをサポートして、他のサブネットへのレイヤ 3 ルートを取得し、個別のルート セットを維持する方法についても説明します。残りの章では、静的ルート、動的ルーティング 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主要な機能について説明します。

- インターフェイスの設定
- 仮想ルーター
- サービス ルート
- 静的ルート
- RIP
- OSPF
- BGP
- IP マルチキャスト
- ルート再配信
- GRE トンネル
- DHCP
- DNS
- DDNS
- NAT
- NPTv6
- NAT64
- ECMP
- LLDP

- BFD
- セッション設定とセッション タイムアウト
- Tunnel Content Inspection（トンネル コンテンツ検査）
- ネットワークパケットブローカー

インターフェイスの設定

Palo Alto Networks ®次世代ファイアウォールは、インターフェイス レベルで展開が行われるため、複数の展開で一度に動作できます。例えば、レイヤー 3 インターフェイス用のいくつかのインターフェイスを設定してファイアウォールを動的なルーティング環境に統合しつつ、他のインターフェイスはレイヤー 2 の切り替えネットワークに統合するよう設定することができます。次のトピックでは、インターフェイスの展開の種類と設定方法、Bonjour Reflector の設定方法、およびインターフェイス管理プロファイルの使用方法について説明します。

タップ インターフェイス

ネットワーク タップは、コンピュータ ネットワーク間を流れるデータにアクセスするためのデバイスです。タップ モード導入では、スイッチの SPAN またはミラー ポートを介してネットワーク内のトラフィック フローをパッシブにモニターできます。

SPAN ポートまたはミラー ポートでは、スイッチの他のポートからトラフィックをコピーすることが許可されています。ファイアウォールの 1 つのインターフェイスをタップ モード専用インターフェイスとして割り当て、スイッチの SPAN ポートに接続すると、スイッチの SPAN ポートからファイアウォールにミラーリングされたトラフィックが提供されます。これにより、ネットワーク トラフィック フローが通過しないネットワーク内でアプリケーションを可視化できます。

ファイアウォールをタップモードで展開することで、ネットワーク設計を変更することなく、ネットワーク上で実行されているアプリケーションを確認できます。さらに、タップモードでは、ファイアウォールはネットワーク上の脅威も識別できます。ただし、タップモードではトラフィックがファイアウォールを通過しないため、トラフィックを脅威でブロックしたり、QoS トラフィック制御を適用したりするなど、トラフィックに対するアクションを実行できません。

タップインターフェイスを設定し、ネットワーク上のアプリケーションと脅威の監視を開始するには：

STEP 1 | タップインターフェイスとして使用するポートを決定し、それを SPAN/RSPAN またはポートミラーリングで設定されたスイッチに接続します。

SPAN の宛先ポートからファイアウォールを通過してネットワークトラフィックを送信するので、ネットワーク上のアプリケーションや脅威を把握できます。

STEP 2 | ファイアウォールのウェブインターフェイスから、ネットワークタップとして使用するインターフェイスを設定します。

1. **Network (ネットワーク)** > **Interfaces (インターフェイス)**を選択し、ケーブルを接続したばかりのポートに対応するインターフェイスを選択します。
2. **Interface Type (インターフェイス タイプ)** として **Tap (タップ)** を選択します。
3. **Config (設定)** タブで、**Security Zone (セキュリティ ゾーン)** を展開して **New Zone (新規ゾーン)** を選択します。
4. ゾーンダイアログで、新しいゾーンの **Name (名前)** (例：TapZone) を入力してから、**OK** をクリックします。

STEP 3 | (任意) 使用する転送プロファイルを作成します。

- Configure Log Forwarding.
- Configure Syslog Monitoring.

STEP 4 | Security Profiles を作成して、ネットワークトラフィックの脅威をスキャンします。

1. **Objects (オブジェクト)** > **Security Profile (セキュリティプロファイル)**の順に選択します。
2. セキュリティプロファイルの種類ごとに、新しいプロファイルを **Add (追加)** して、アクションを **Alert (アラート)** に設定します。

   ファイアウォールはトラフィックとインラインになっていないため、ブロックまたはリセットアクションを使用することはできません。アクションをアラートに設定することで、ファイアウォールがログと ACC で検出した脅威を確認できます。

STEP 5 | タップインターフェイスを通過するトラフィックを許可するセキュリティポリシールールを作成します。

タップモードのセキュリティポリシールールを作成する際は、送信元ゾーンと宛先ゾーンの両方が同じである必要があります。

1. **Policies**（ポリシー） > **Security**（セキュリティ） を選択してルールをクリックします。.
2. **Source (送信元)** タブで、**Source Zone (送信元ゾーン)** を作成したばかりの TapZone に設定します。
3. **Destination (宛先)** タブで **Destination Zone (宛先ゾーン)** を TapZone にも設定します。
4. すべてのルール一致条件 (**Applications (アプリケーション)**、**User (ユーザー)**、**Service (サービス)**、**Address (アドレス)**)を **any (いずれか)** に設定します。
5. **Actions**（アクション）タブで、**Action Setting**（アクション設定）を**Allow**（許可）に設定します。
6. **Profile Type (プロファイルの種類)** を **Profiles (プロファイル)** に設定し、作成した各セキュリティプロファイルを選択して脅威を警告します。
7. **Log at Session End**[セッション終了時にログを記録]が有効になっていることを確認します。
8. **OK** をクリックします。
9. ルールベースの一番上にルールを配置します。

STEP 6 | 設定を **Commit**（コミット）します。

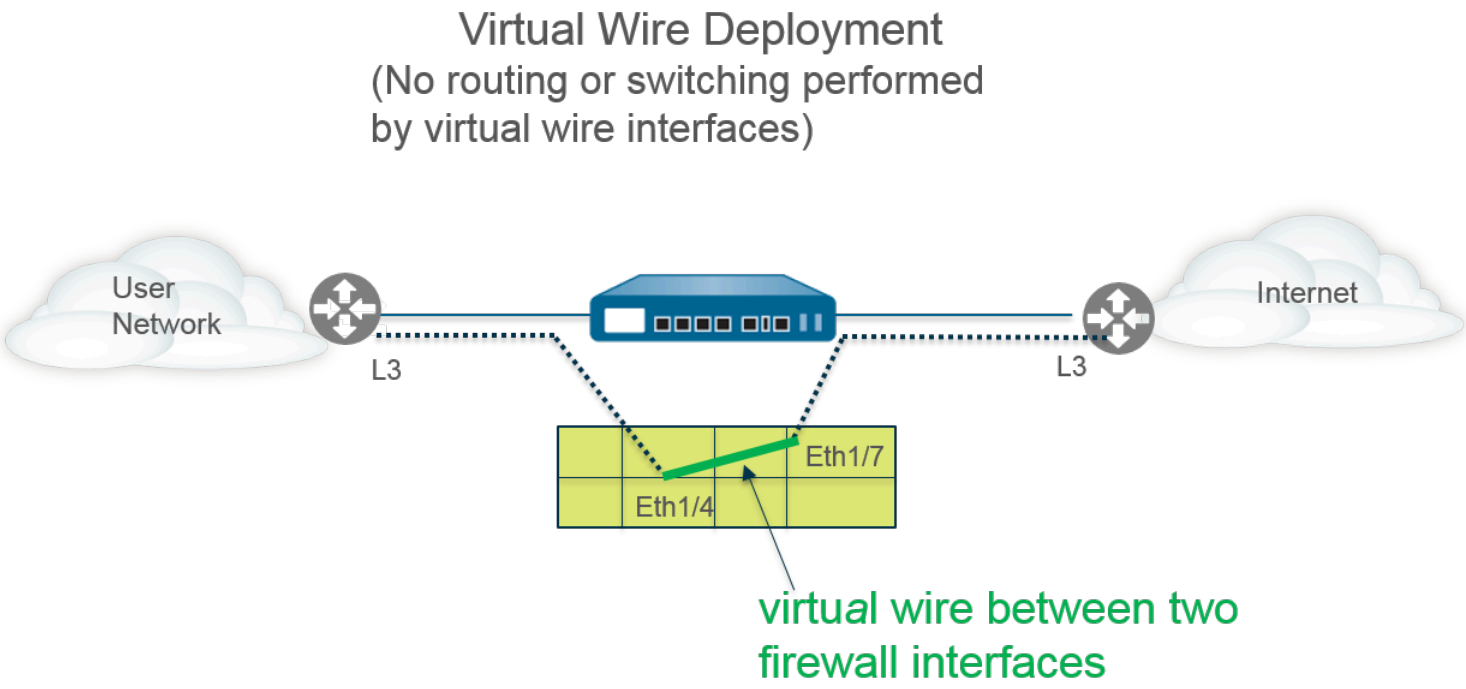
STEP 7 | ファイアウォールログ (**Monitor (モニター)** > **Logs (ログ)**) および **ACC** を監視して、ネットワーク上のアプリケーションと脅威を把握します。

バーチャル ワイヤー インターフェイス

バーチャル ワイヤー導入の場合、ファイアウォールを、2 つのファイアウォール ポート（インターフェイス）を結合することによってネットワーク セグメント上に透過的にインストールします。バーチャル ワイヤは 2 つのインターフェイスを論理的に接続します。つまり、バーチャル ワイヤはファイアウォールの内部にあります。

ファイアウォールをトポロジーにシームレスに統合したい場合で、かつファイアウォール上で接続された 2 つのインターフェイスがスイッチングやルーティングを必要としない場合にのみ、バーチャル ワイヤのデプロイメントを利用します。これら 2 つのインターフェイスについては、ファイアウォールが *Bump In The Wire* とみなされます。

インターフェイスに MAC あるいは IP アドレスを割り当てたり、ネットワークを再設計したり、周辺のネットワーク機器を再構成したりすることなく、既存のトポロジーにファイアウォールを挿入できるため、バーチャル ワイヤのデプロイメントは、ファイアウォールのインストールや設定を簡略化します。バーチャル ワイヤは、セキュリティポリシールール、App-ID、コンテンツ ID、User-ID、復号化、LLDP、アクティブ/パッシブおよびアクティブ/アクティブ HA、QoS、ゾーン プロテクション（一部例外あり）、非 IP プロトコル保護、DoS 保護、パケット バッファ保護、トンネル コンテンツ検査、および NAT のサポートに加え、仮想 LAN（VLAN）タグに基づいてトラフィックをブロックあるいは許可する機能をサポートしています。



各バーチャル ワイヤ インターフェイスは、レイヤー 2 あるいはレイヤー 3 ネットワーク機器あるいはホストに直に接続します。バーチャル ワイヤ インターフェイスはレイヤー 2 や レイヤー 3 アドレスを持っていません。いずれかのバーチャル ワイヤ インターフェイスがフレームあるいはパケットを受信すると、スイッチングやルーティングのためにレイヤー 2 あるいはレイヤー 3 アドレスを無視しますが、許可されるフレームあるいはパケットをバーチャル ワイヤ

を通して 2 つ目のインターフェイスへと通過させ、それに接続されたネットワーク機器に送る前に、セキュリティあるいは NAT ポリシー ルールを適用します。

スイッチング、VPN トンネル、あるいはルーティングのサポートが必要なインターフェイスについては、レイヤー 2 あるいはレイヤー 3 アドレスが必要になるため、バーチャル ワイヤのデプロイメントを利用しません。バーチャル ワイヤ インターフェイスは、HTTP や ping などのサービスを制御するためにインターフェイスに IP アドレスを求めるインターフェイス管理プロファイルを使用しません。

工場出荷時のすべてのファイアウォールには、バーチャル ワイヤ インターフェイスとして事前に設定された 2 つのイーサネット ポート（ポート 1 および 2）が備わっており、これらのインターフェイスはタグなしのトラフィックをすべて許可します。

Cisco Trustsec ネットワークで *security group tags (*セキュリティグループ タグ; *SGT)* を使用している場合は、ファイアウォールをレイヤー*2* モード、またはバーチャル ワイヤ モードのインライン構成で展開することが、ベストプラクティスになります。レイヤー *2* モードまたはバーチャル ワイヤー モードのファイアウォールは、タグ付けされたトラフィックを検査して脅威防止機能を提供することができます。

事前設定されたバーチャル ワイヤを使う気がない場合は、設定を削除し、ファイアウォール上で構成した他の設定にそれが干渉しないようにします。外部サービスへのネットワーク アクセスのセットアップを参照してください。

- バーチャル ワイヤを介したレイヤー 2 およびレイヤー 3 パケット
- バーチャル ワイヤ インターフェイスのポート速度
- バーチャル ワイヤを通した LLDP
- バーチャル ワイヤ用の集約インターフェイス
- 高可用性のバーチャル ワイヤ サポート
- バーチャル ワイヤ インターフェイスのゾーン プロテクション
- VLAN タグの付いたトラフィック
- バーチャル ワイヤー サブインターフェイス
- バーチャル ワイヤの設定

バーチャル ワイヤを介したレイヤー 2 およびレイヤー 3 パケット

バーチャル ワイヤ インターフェイスは、そのゾーンあるいはインターフェイスに適用されたポリシーがトラフィックを許す限り、接続されたデバイスから来るレイヤー 2 およびレイヤー 3 パケットが透過的に通過するのを許可します。バーチャル ワイヤ インターフェイス自身はルーティングあるいはスイッチングに参加しません。

例えば、リンクは透過的でありホップとしてカウントされないため、ファイアウォールは、仮想リンクを通過するトレースルート パケット内の TTL を減少させません。例えば Operations、Administration and Maintenance（OAM）プロトコル データ ユニット（PDU）などのパケットは、ファイアウォールを目的地にしません。そのため、バーチャル ワイヤはファイ

アウォールがセキュリティ、NAT、および QoS サービスを提供しつつも、パススルー リンクとして見えない形で存在を維持できるようにします。

bridge protocol data unit（BPDU）およびその他のレイヤー 2 制御パケット（通常はタグなし）がバーチャル ワイヤを通過できるようにするために、タグなしのトラフィックを許可するバーチャル ワイヤ オブジェクトにインターフェイスをアタッチする必要があり、デフォルト設定でそのようになっています。バーチャル ワイヤ オブジェクトの **Tag Allowed (**タグを許可**)** フィールドが空の場合、バーチャル ワイヤはタグなしのトラフィックを許可します。（セキュリティ ポリシールールは レイヤー 2 パケットに適用されません）

ルーティング（レイヤー 3）制御パケットがバーチャル ワイヤを通過できるようにするために、トラフィックが通過するのを許可するセキュリティポリシー ルールを適用する必要があります。例えば、BGP や OSPF といったアプリケーションを許可するセキュリティポリシー ルールを適用します。

ファイアウォール上のバーチャル ワイヤ インターフェイスに到達する IPv6 トラフィック用のゾーンにセキュリティポリシールールを適用できるようにする場合は、IPv6 ファイアウォーリングを有効化します。そうでない場合は、ワイヤ全体にかけて IPv6 トラフィックが透過的に転送されます

バーチャル ワイヤ オブジェクト用のマルチキャスト ファイアウォーリングを有効にしてバーチャル ワイヤ インターフェイスに適用すると、ファイアウォールはマルチキャスト トラフィックを検査し、セキュリティポリシールールに基づいてそれを転送するかかどうかを判断します。マルチキャスト ファイアウォーリングを有効化しない場合、ファイアウォールは単純にマルチキャスト トラフィックを透過的に転送します。

他のインターフェイスのデプロイモードと同様に、バーチャル ワイヤのフラグメンテーションが発生します。

バーチャル ワイヤ インターフェイスのポート速度

各ファイアウォール モデルは、異なる速度で動作する様々な数の銅ポートおよび光ファイバー ポートを提供します。バーチャル ワイヤーは、同じタイプ（両方とも銅、あるいは両方とも光ファイバー）のイーサネット ポートを 2 つ、あるいは光ファイバー ポートと銅ポートを結束できます。デフォルトでは、ファイアウォールの銅ポートの **Link Speed**（リンク速度）が **auto** に設定されており、ファイアウォールは速度と送信モードを自動的にネゴシエーションします（**Link Duplex**（リンク デュプレックス））。また、バーチャル ワイヤーを設定する時に、特定の**Link Speed**（リンク速度）と **Link Duplex**（リンク デュプレックス）を選択できますが、これらの設定の値は単一のバーチャル ワイヤー内の両ポートに対して同一である必要があります。

バーチャル ワイヤを通した LLDP

バーチャル ワイヤ インターフェイスは LLDP を使用して隣接するデバイスとその機能を発見でき、LLDP は隣接するデバイスがネットワーク内のファイアウォールの存在を検知できるようにします。LLDP により、特にバーチャル ワイヤ上（バーチャル ワイヤを通過する ping またはトレースルートでファイアウォールが通常検出されない状況）でのトラブルシューティングが一層容易になります。LLDP は、他のデバイスがネットワーク内のファイアウォールを検知できる方法を提供します。LLDP がなければ、ネットワーク管理システムが仮想リンクを通してファイアウォールの存在を検知することが実質不可能になります。

バーチャル ワイヤ用の集約インターフェイス

バーチャル ワイヤー インターフェイスの集約インターフェイス グループの設定を行うことができますが、バーチャル ワイヤーは LACP を使用しません。ファイアウォールを他のネットワークに接続するデバイスに LACP を設定すると、バーチャル ワイヤーは LACP 機能を実行せずに透過的に LACP パケットを通過させます。

集約インターフェイス グループが正常に機能するためには、バーチャル ワイヤーの同じ側の同一 ***LACP*** グループに属するすべてのリンクが同じゾーンに割り当てられていることを確認してください。

高可用性のバーチャル ワイヤ サポート

ファイアウォールがバーチャル ワイヤ パス グループを使用して高可用性用のパス モニタリングを実行するように設定する場合、ファイアウォールは両方のバーチャル ワイヤ インターフェイスから ARP パケットを送信することで、設定済みの宛先 IP アドレス用に ARP を解決しようと試みます。監視中の宛先 IP アドレスは、バーチャル ワイヤ周辺のいずれかのデバイスと同じサブネットワーク上になければなりません。

バーチャル ワイヤ インターフェイスはアクティブ/パッシブおよびアクティブ/アクティブ HA の両方をサポートしています。バーチャル ワイヤを伴うアクティブ/アクティブ HA の場合、スキャンされたパケットを受信ファイアウォールに戻して転送パスを維持する必要があります。そのため、ピア HA ファイアウォールが所有するセッションに属すパケットを受け取ると、ファイアウォールはパケットを HA3 を通してピアに送信します。

HA ペアでパッシブ ファイアウォールを設定して、HA フェールオーバーが発生する前に、ファイアウォールの両側にあるピア デバイスが仮想ワイヤを介して LLDP と LACP を事前にネゴシエートできるように設定できます。そのような アクティブ/パッシブ HA のための LACP および LLDP プレネゴシエーションの設定により、HA フェイルオーバーが高速になります。

バーチャル ワイヤ インターフェイスのゾーン プロテクション

仮想ワイヤ インターフェイスにゾーン保護を適用することはできますが、仮想ワイヤ インターフェイスはルーティングを実行しないため、スプーフィングされた IP アドレスを持つパケットに パケット ベースの攻撃保護 を適用したり、ICMP TTL 期限切れエラー パケットや ICMP Frag 必要パケットを抑制したりすることはできません。

デフォルトでは、バーチャル ワイヤー インターフェイスは受信したすべての非 IP トラフィックを転送します。ただし、 プロトコル保護を使用してゾーン保護プロファイルを適用し、バーチャル ワイヤー上のセキュリティ ゾーン間で特定の非 IP プロトコル パケットをブロックまたは許可することができます。

VLAN タグの付いたトラフィック

バーチャル ワイヤ インターフェイスはデフォルトでタグなしのトラフィックをすべて許可するようになっています。ただし、バーチャル ワイヤーを使用して 2 つのインターフェイスに接続し、仮想 LAN （VLAN）タグに基づいてトラフィックをブロックまたは許可するインターフェイスのいずれかを設定できます。VLAN タグ 0 はタグなしのトラフィックを示します。

また、複数のサブインターフェイスを作成して異なるゾーンに追加し、VLAN タグ、または VLAN タグと IP 分類子（アドレス、範囲、またはサブネット）の組み合わせに基づいてトラフィックを分類して、特定の VLAN タグまたは特定の IP アドレス、範囲、またはサブネットからの VLAN タグにきめ細かいポリシー制御を適用することもできます。

バーチャル ワイヤー サブインターフェイス

バーチャル ワイヤのデプロイメントでは、バーチャル ワイヤ サブインターフェイスを使用してトラフィックを複数のゾーンに別けることができます。複数顧客のネットワークからのトラフィックを管理する必要がある場合、バーチャル ワイヤー サブインターフェイスを使用すると、個別のポリシーを適用するときの柔軟性が高まります。サブインターフェイスでは、以下の基準を使用してトラフィックを異なるゾーン（必要に応じて別々の仮想システムに属することができる）に区別して分類できます。

- **VLAN** タグ – サブインターフェイスを持つバーチャル ワイヤー デプロイメント（VLAN タグのみ）の例は、バーチャル ワイヤー サブインターフェイスを使用して、VLAN タグで 2 つの異なる顧客のトラフィックを区別する ISP を示しています。
- **VLAN** タグと **IP** 分類子（アドレス、範囲、またはサブネット）との組み合わせ – 以下の例は、2 つの異なる顧客のトラフィックを管理する 1 つのファイアウォール上に、2 つの異なる仮想システムを持つ ISP を示しています。この例では、各仮想システムで、VLAN タグおよび IP 分類子を持つバーチャル ワイヤー サブネットを使用してトラフィックを個別のゾーンに分類し、各ネットワークの顧客に関連するポリシーを適用する方法を示しています。

バーチャル ワイヤー サブインターフェイスのワークフロー

- 2 つの Ethernet インターフェイスをバーチャル ワイヤー タイプとして設定し、これらのインターフェイスを 1 つのバーチャル ワイヤーに割り当てます。

- 親バーチャル ワイヤーにサブインターフェイスを作成し、CustomerA と CustomerB のトラフィックを区別します。バーチャル ワイヤーとして設定されたサブインターフェイスの各ペアに定義する VLAN タグは同一にします。バーチャル ワイヤーは VLAN タグを切り替えないため、このようにする必要があります。

- 新しいサブインターフェイスを作成して IP による分類を定義します。このタスクは任意であり、VLAN タグと特定のソース IP アドレス、範囲、またはサブネットの組み合わせに基づいて顧客からのトラフィックをさらに管理するために追加のサブインターフェイスと IP 分類子を追加する場合のみ必要です。

タグのないトラフィックを管理するために IP 分類子を使用することもできます。そのためには、VLAN タグ「0」を持つサブインターフェイスを作成し、IP 分類子を使用してタグのないトラフィックを管理するために IP 分類子を持つサブインターフェイスを定義する必要があります。

IP による分類は、片側のバーチャル ワイヤーに関連付けられているサブインターフェイスでのみ使用できます。対応する側のバーチャル ワイヤーで定義されたサブインターフェイスは同じ *VLAN* タグを使用する必要がありますが、*IP* による分類を含めることはできません。

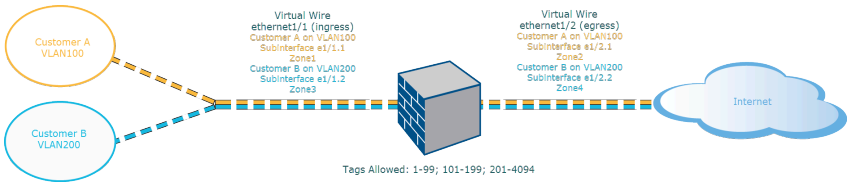


図 **1 :** サブインターフェイスを持つバーチャル ワイヤー デプロイメント（**VLAN** タグのみ）

サブインターフェイスを持つバーチャル ワイヤー デプロイメント（VLAN タグのみ）は、バーチャル ワイヤーとして設定された入力インターフェイスである物理インターフェイス ethernet1/1 経由でファイアウォールに接続された CustomerA と CustomerB を示しています。2 つ目の物理インターフェイス ethernet1/2 もバーチャル ワイヤーの一部であり、インターネットへのアクセスを提供する出力インターフェイスです。

CustomerA には、サブインターフェイス ethernet1/1.（入力）と ethernet1/2.（出力）もあります。CustomerB には、サブインターフェイス ethernet1/1.（入力）と ethernet1/2.（出力）があります。顧客ごとにポリシーを適用するため、サブインターフェイスの設定時に適切な VLAN タグとゾーンを割り当てる必要があります。この例の場合、CustomerA のポリシーは Zone1 と Zone2 の間で作成され、CustomerB のポリシーは Zone3 と Zone4 の間で作成されます。

トラフィックが CustomerA または CustomerB からファイアウォールに入ると、受信パケットの VLAN タグは最初に、入力サブインターフェイスで定義された VLAN タグに対して照合されます。この例では、1 つのサブインターフェイスが受信パケットの VLAN タグに一致するため、そのサブインターフェイスが選択されます。ゾーンに定義されたポリシーは、パケットが対応するサブインターフェイスから出る前に評価され、適用されます。

親バーチャル ワイヤー インターフェイスとサブインターフェイスで同じ *VLAN* タグを定義しないでください。親バーチャル ワイヤー インターフェイスの *Tag Allowed*（タグを許可）リストで定義される *VLAN* タグ（***Network (***ネットワーク***) > Virtual Wires (***バーチャル ワイヤ***)***）がサブインターフェイスに含まれていないことを確認します。

サブインターフェイスを持つバーチャル ワイヤー デプロイメント（VLAN タグおよび IP 分類子）は、デフォルトの仮想システム（vsys1）に加えて 2 つの仮想システム（vsys）を持つ 1 つの物理ファイアウォールに接続された CustomerA および CustomerB を示しています。各仮想システムは、各顧客について個別に管理される独立した仮想ファイアウォールです。各 vsys にはインターフェイス/サブインターフェイスが接続されており、独立して管理されるセキュリティ ゾーンがあります。

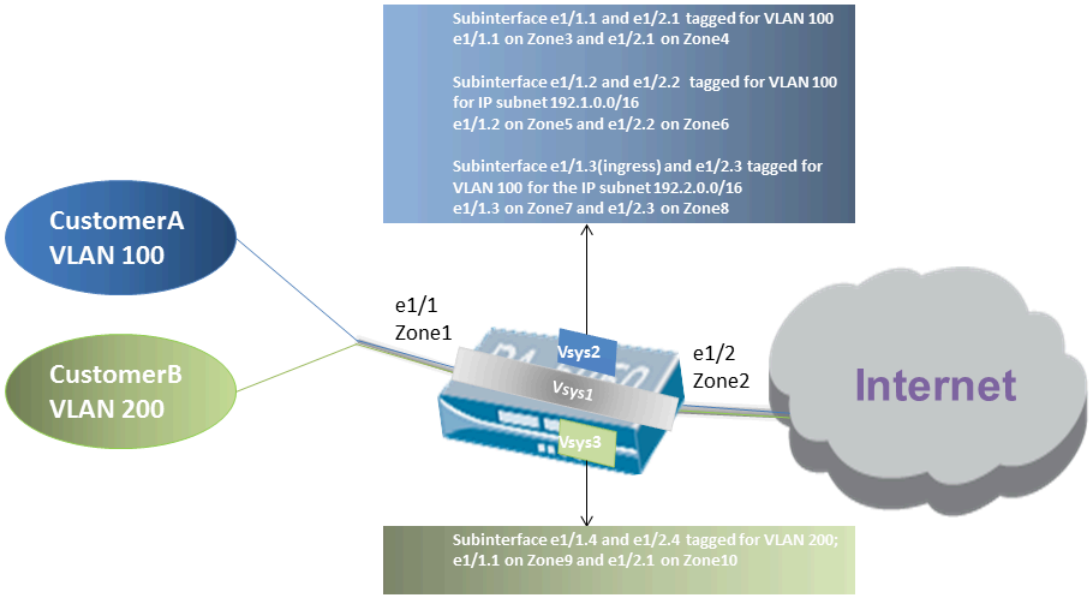


図 **2 :** サブインターフェイスを持つバーチャル ワイヤー デプロイメント（**VLAN** タグおよび **IP** 分類子）

vsys1 は物理インターフェイス ethernet1/1 および ethernet1/2 をバーチャル ワイヤーとして使用するようにセットアップされます。ethernet1/1 は入力インターフェイスで、ethernet1/2 はインターネットへのアクセスを提供する出力インターフェイスです。このバーチャル ワイヤーは、サブインターフェイスに割り当てられた VLAN タグ 100 および 200 を除いてすべてのタグありおよびタグなしのトラフィックを受け入れるように設定されています。

CustomerA は vsys2 で管理され、CustomerB は vsys3 で管理されます。vsys2 および vsys3 で、以下の vwire サブインターフェイスが適切な VLAN タグおよびゾーンを使用して作成され、ポリシー指定を適用します。

導入	vsys	vwire サブインターフェイス	ゾーン	VLAN タグ	IP による分類
A	2	e1/1.1 （入力） e1/2.1 （出力）	Zone3IPv6 Zone4IPv6	100 100	無し
	2	e1/1.2 （入力） e1/2.2 （出力）	Zone5IPv6 Zone6IPv6	100 100	IP サブネット 192.1.0.0/16

導入	vsys	vwire サブインターフェイス	ゾーン	VLAN タグ	IP による分類
	2	e1/1.3（入力） e1/2.3 （出力）	Zone7IPv6 Zone8IPv6	100 100	IP サブネット 192.2.0.0/16
B	3	e1/1.4 （入力） e1/2.4 （出力）	Zone9IPv6 Zone10IPv6	200 200	無し

トラフィックが CustomerA または CustomerB からファイアウォールに入ると、受信パケットの VLAN タグは最初に、入力サブインターフェイスで定義された VLAN タグに対して照合されます。この場合、CustomerA には、同じ VLAN タグを使用するサブインターフェイスが複数存在します。そのため、ファイアウォールは最初にパケット内のソース IP アドレスに基づいて 1 つのサブインターフェイスに分類を制限します。ゾーンに定義されたポリシーは、パケットが対応するサブインターフェイスから出る前に評価され、適用されます。

return-path トラフィックでは、ファイアウォールは顧客側サブインターフェイスの IP 分類子で定義されているように宛先 IP アドレスを比較し、適切なバーチャル ワイヤーを選択して正確なサブインターフェイス経由でトラフィックをルーティングします。

親バーチャル ワイヤー インターフェイスとサブインターフェイスで同じ *VLAN* タグを定義しないでください。親バーチャル ワイヤー インターフェイスの *Tag Allowed*（タグを許可）リストで定義される *VLAN* タグ（***Network (***ネットワーク***) > Virtual Wires (***バーチャル ワイヤ***)***）がサブインターフェイスに含まれていないことを確認します。

バーチャル ワイヤの設定

次の作業は、2 つの バーチャルワイヤインターフェース （この例では Ethernet 1/3 および Ethernet 1/4）を設定してバーチャル ワイヤを作成する方法を示しています。2 つのインターフェイスは、同じ **Link Speed**（リンク速度）と転送モード（**Link Duplex**（リンク デュプレックス）を有するようにします）。例えば、full-duplex 1000 Mbps の銅ポートは、1 Gbps の full-duplex 光ファイバーポートに一致します。

STEP 1 | 最初のバーチャル ワイヤ インターフェイスを作成します。

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、配線したインターフェイスを選択します（この例では **ethernet1/3**）。
2. **Interface Type**（インターフェイス タイプ）を **Virtual Wire**（バーチャル ワイヤ）に設定します。

STEP 2 | インターフェイスをバーチャル ワイヤ オブジェクトにアタッチします。

1. 同じイーサネット インターフェイスにいる間に、**Config (設定)**タブで、**Virtual Wire (バーチャル ワイヤ)**を選択して、 **New Virtual Wire (新規バーチャル ワイヤ)**をクリックします。
2. バーチャル ワイヤの **Name**（名前） を入力します。
3. **Interface1 (インターフェイス1)**の場合、先ほど設定したインターフェイス（**ethernet1/3**）を選択します。(バーチャル ワイヤ インターフェイスとして設定されたインターフェイスだけがリストに表示されます。)
4. **Tag Allowed (タグの許可)** については、**0** を入力することで、タグを持たないトラフィック（BPDU や他のレイヤー 2 制御トラフィックなど）を許可するよう指定します。タグがない場合は暗黙的にタグ 0 を示します。許可される追加のタグ インテグレータあるいはタグ範囲を入力し、コンマで区切ります（デフォルトは 0 で、範囲は 0～4,094）。
5. バーチャル ワイヤを通過するマルチキャスト トラフィックにセキュリティ ルールを適用できるようにする場合は、**Multicast Firewalling (マルチキャスト ファイアウォール)**を選択します。そうでない場合、マルチキャスト トラフィックは透過的にバーチャル ワイヤ中で転送されます。
6. ファイアウォールが透過的に機能できるよう、**Link State Pass Through (リンク状態パス スルー)** を選択します。バーチャル ワイヤのリンクがリンク ダウン状態であることをファイアウォールが検知すると、バーチャル ワイヤ ペアのもう一方のインターフェイスを停止させます。これにより、あたかもデバイス間にファイアウォールが存在しないかのように、ファイアウォールの両側のデバイスが一貫したリンク状態になります。このオプションを選択しない場合、リンク状態はバーチャルワイヤーを通じて反映されません。
7. **OK** をクリックしてバーチャル ワイヤ オブジェクトを保存します。

STEP 3 | バーチャル ワイヤ インターフェイスのリンク速度を決定します。

1. 同じイーサネット インターフェイスにいる間に、**Advanced (詳細)** タブを選択して、**Link Speed (リンク速度)** を控えておくか変更します。ポート タイプにより、リストで利用できる速度設定が決まります。デフォルト設定では、銅ポートは **auto (自動)** ネゴシエート リンク速度に設定されています。どちらのバーチャル ワイヤ インターフェイスも同じリンク速度である必要があります。
2. **OK** をクリックして Ethernet (イーサネット) インターフェイスを保存します。

STEP 4 | 前のステップを繰り返して、2 番目のバーチャル ワイヤ インターフェイス（この例では **ethernet1/4** ）を設定します。

作成した**Virtual Wire**（バーチャル ワイヤ）オブジェクトを選択すると、ファイアウォールは自動的に 2 番目のバーチャル ワイヤ インターフェイスを **Interface2** として追加します。

STEP 5 | バーチャル ワイヤ インターフェイスのそれぞれについて別個のセキュリティ ゾーンを作成します。

1. **Network (ネットワーク)** > **Zones (ゾーン)** を選択してゾーンを **Add (追加)** します。
2. ゾーンの **Name (名前)**（**Internet** など）を入力します。
3. **Location (場所)** については、ゾーンを適用する仮想システムを選択します。
4. **Type (タイプ)** については **Virtual Wire (バーチャル ワイヤ)** を選択します。
5. このゾーンに属する **Interface (インターフェイス)** を **Add (追加)** します。
6. **OK** をクリックします。

STEP 6 | （任意）レイヤー 3 トラフィックに対してパススルーを許可するセキュリティポリシー ルールを作成します。

バーチャル ワイヤ全体でレイヤー 3 トラフィックを許可するためには、ユーザーのゾーンからインターネットのゾーンへのトラフィックを許可するセキュリティ ポリシー ルールを作成し、さらにインターネットのゾーンからユーザーのゾーンへのトラフィックを許可するポリシーを作成し、許可するアプリケーション（BGP や OSPF など）を選択します。

STEP 7 | （Optional）IPv6 ファイアウォーリングを有効化します。

バーチャル ワイヤ インターフェイスに到達する IPv6 トラフィックにセキュリティポリシー ルールを適用できるようにする場合は、IPv6 ファイアウォーリングを有効化します。そうでない場合は、IPv6 トラフィックが透過的に転送されます。

1. **Device (デバイス)** > **Setup (セットアップ)** > **Session (セッション)** を選択して Session Settings (セッション設定) を編集します。
2. **Enable IPv6 Firewalling (IPv6 ファイアウォールの有効化)** を選択します。
3. **OK** をクリックします。

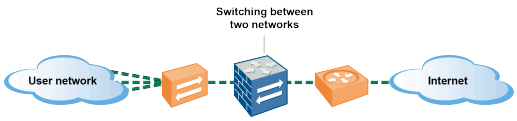
STEP 8 | 変更を **Commit (コミット)**します。

STEP 9 | （任意）LLDP プロファイルを設定し、それをバーチャル ワイヤ インターフェイスに適用します（ LLDPの設定 を参照）。

STEP 10 | (オプション)非 IP プロトコル制御を仮想ワイヤ ゾーンに適用します (プロトコル保護の構成)。そうしない場合は、すべての非 IP トラフィックがバーチャル ワイヤにまたがって転送されます。

レイヤー 2 インターフェイス

レイヤー 2 デプロイメントの場合、ファイアウォールは複数ネットワーク間のスイッチングを行います。デバイスはレイヤー 2 セグメントに接続されており、ファイアウォールはフレームで識別された MAC アドレスに関連する適切なポートにフレームを転送します。スイッチングが必要な場合はレイヤー 2 インターフェイスの設定を行います。



Cisco Trustsec ネットワークで *security group tags (*セキュリティグループ タグ; *SGT)* を使用している場合は、ファイアウォールをレイヤー*2* モード、またはバーチャル ワイヤ モードのインライン構成で展開することが、ベストプラクティスになります。レイヤー *2* モードまたはバーチャル ワイヤー モードのファイアウォールは、タグ付けされたトラフィックを検査して脅威防止機能を提供することができます。

次のトピックでは、複数のグループ間でトラフィックおよびポリシーを分離する仮想 LAN（VLAN）の詳細な使用方法などを含め、必要な各種のデプロイ環境用に設定できる異なるタイプのレイヤー 2 インターフェイスを説明します。別のトピックでは、ファイアウォールがシスコの VLAN 単位のスパニングツリー（PVST +）または Rapid PVST + ブリッジ プロトコル データユニット（BPDU）の受信ポート VLAN ID 番号を書き換える方法について説明します。

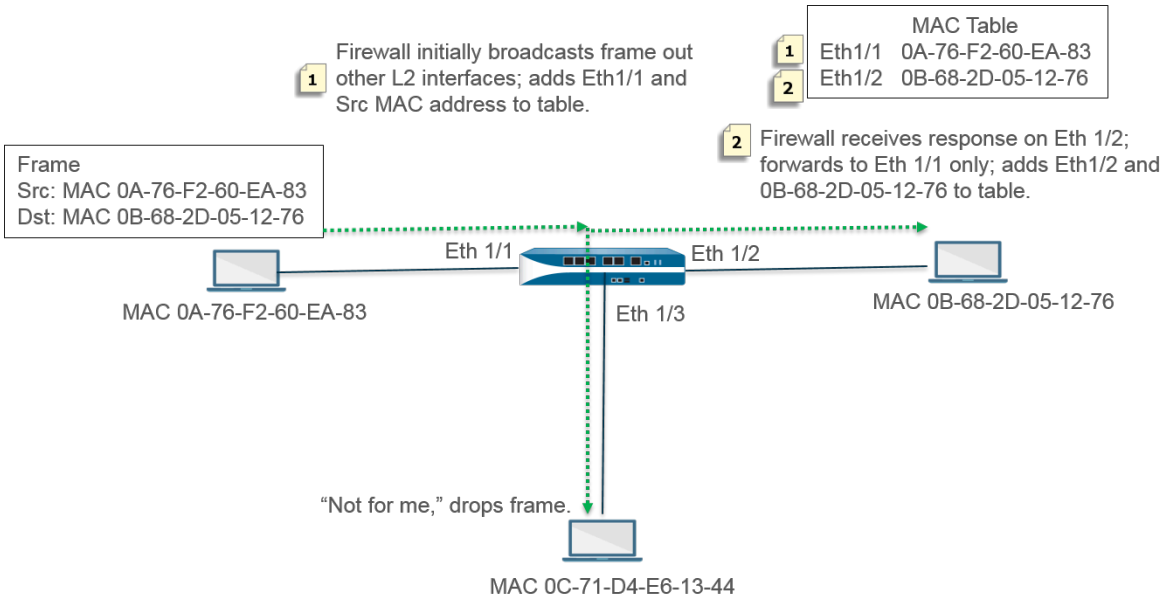
- VLAN を使用しないレイヤー 2 インターフェイス
- VLAN を使用するレイヤー 2 インターフェイス
- レイヤー 2 インターフェイスの設定
- レイヤー 2 インターフェイス、サブインターフェイス、VLANの設定
- VLAN 単位のスパニング ツリー（PVST +）BPDU 書き換えの管理

VLAN を使用しないレイヤー 2 インターフェイス

ファイアウォール上のレイヤー 2 インターフェイスの設定を行い、レイヤー 2 ネットワーク内（ネットワークの末端ではなく）におけるスイッチとして機能するようにします。レイヤー 2 ホストはおそらく地理的にお互い近い位置にあり、同じブロードキャスト ドメインに属しています。インターフェイスをセキュリティ ゾーンに割り当て、セキュリティルールをゾーンに適用する際に、ファイアウォールはレイヤー 2 ホスト間でセキュリティを提供します。

各ホストはフレームを交換することで、OSI モデルのレイヤー 2 にてファイアウォールおよびお互いの間で通信を行います。フレームには、送信元および宛先 Media Access Control（MAC）アドレス（ハードウェアの物理アドレス）を含むイーサネット ヘッダが含まれています。MAC アドレスは、6 つの 8 ビット数をコロンあるいはハイフンで区切った 48 ビットの 16 進数です（例：00-85-7E-46-F1-B2）。

次の図は、各々がレイヤー 2 ホストに一対一のマッピングで接続された 3 つのレイヤー 2 インターフェイスを持つファイアウォールを示しています。



このファイアウォールの MAC テーブルは空の状態で始まります。送信元アドレス 0A-76-F2-60-EA-83 を持つホストがフレームをファイアウォールに送る際、ファイアウォールの MAC テーブルには宛先アドレス 0B-68-2D-05-12-76 がないため、ファイアウォールはどのインターフェイスにフレームを転送すべきか判断できず、フレームをすべてのレイヤー 2 インターフェイスにブロードキャストします。ファイアウォールは送信元アドレス 0A-76-F2-60-EA-83 および関連した Eth1/1 を自身の MAC テーブルに追加します。

0C-71-D4-E6-13-44 のホストはブロードキャストを受信しますが、自身の MAC アドレスに宛先 MAC アドレスがないため、フレームをドロップします。

受信インターフェイスである Ethernet 1/2 はフレームをそのホストに転送します。ホスト 0B-68-2D-05-12-76 は応答時に宛先アドレス 0A-76-F2-60-EA-83 を使用し、ファイアウォールが Ethernet 1/2 を 0B-68-2D-05-12-76 に到達するためのインターフェイスとして自身の MAC テーブルに追加します。

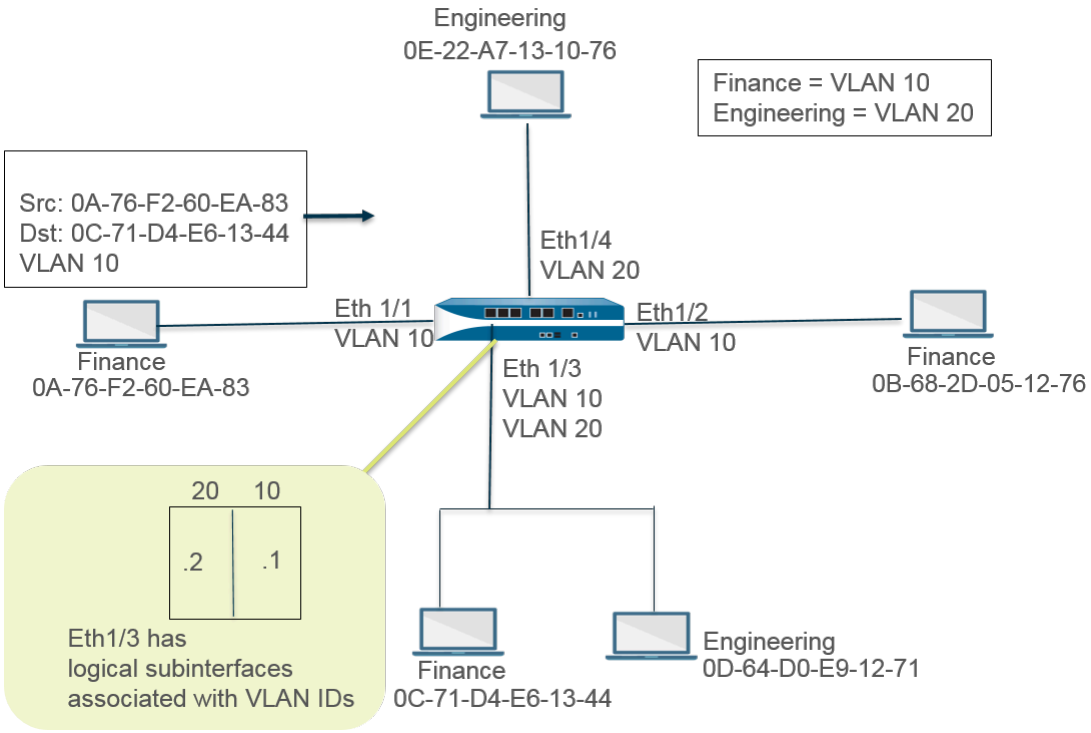
VLAN を使用するレイヤー 2 インターフェイス

組織で LAN を別々の仮想 LAN（VLAN）に分けて各部門のトラフィックおよびポリシーを分離した状態を保ちたい場合、複数のレイヤー 2 ホストを論理的に VLAN としてグループ化することで、レイヤー 2 ネットワーク セグメントを分離してブロードキャスト ドメインにすることができます。例えば、会計やエンジニアリング部門のために VLAN を作成できます。そのためには、レイヤー 2 インターフェイス、サブインターフェイス、VLAN の設定を行います。

ファイアウォールは、VLAN ID を含むイーサネット ヘッダを持つフレームを転送するスイッチとして機能します。そのフレームを受け取ってホストに転送するためには、宛先インターフェイスにその VLAN ID を持つサブインターフェイスがなければなりません。ファイアウォール上でレイヤー 2 インターフェイスを設定し、そのインターフェイス用に、それぞれが VLAN タグ（ID）を持つ論理的サブインターフェイスを一つあるいは複数設定します。

次の図では、組織内の異なる部門に属すレイヤー 2 ホストに接続する 4 つのレイヤー 2 インターフェイスがファイアウォール上にあります。イーサネット インターフェイス 1/3 はサブインターフェイス .1（VLAN 10 のタグ付き）およびサブインターフェイス .2（VLAN 20 のタグ付

き）を持つよう設定されているため、そのセグメントには 2 つのブロードキャスト ドメインが存在しています。VLAN 10 内のホストは財務に、VLAN 20 内のホストはエンジニアリングに所属しています。



この例では、MAC アドレス 0A-76-F2-60-EA-83 のホストが VLAN ID 10 を持つフレームを送信し、それをファイアウォールが他の L2 インターフェイスにブロードキャストします。イーサネット インターフェイス 1/3 は宛先 0C-71-D4-E6-13-44 を持つホストに接続されており、そのサブインターフェイス .1 に VLAN 10 が割り当てられているため、フレームを受け取ります。イーサネット インターフェイス 1/3 はフレームを財務のホストに転送します。

レイヤー 2 インターフェイスの設定

レイヤー 2 切り替えが必要であり、VLAN 毎にトラフィックを別ける必要がない場合は、VLAN なしのレイヤー 2 インターフェイスを設定します。

STEP 1 | レイヤー 2 インターフェイスの設定

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、さらにインターフェイスを選択します。**Interface Name (インターフェイス名)** は固定されています（ethernet1/1 など）。
2. **Interface Type (インターフェイス タイプ)** については **Layer2** を選択します。
3. **Config (設定)** タブを選択し、**Security Zone (セキュリティ ゾーン)** にインターフェイスを割り当てるか、**New Zone (新規ゾーン)** を作成します。
4. 他のレイヤー 2 ホストに接続するファイアウォール上でさらにレイヤー 2 インターフェイスを設定します。

STEP 2 | コミットします。

OK、**Commit (コミット)** の順にクリックします。

レイヤー 2 インターフェイス、サブインターフェイス、VLANの設定

レイヤー 2 切り替えが必要であり、VLAN 毎にトラフィックを別ける必要がある場合は、VLAN ありのレイヤー 2 インターフェイスを設定します。任意で、レイヤー 2 インターフェイス上のセキュリティ ゾーン間で、あるいはレイヤー 2 VLAN 上の単一のゾーン内で非 IP プロトコルを制御できます。

STEP 1 | 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を設定し、VLAN を割り当てます。

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、さらにインターフェイスを選択します。**Interface Name (インターフェイス名)** は固定されています（ethernet1/1 など）。
2. **Interface Type (インターフェイス タイプ)** については **Layer2** を選択します。
3. **Config (設定)** タブを選択します。
4. **VLAN** については **None (なし)** の設定のままにします。
5. インターフェイスを **Security Zone (セキュリティ ゾーン)** に割り当てるか、**New Zone (新規ゾーン)** を作成します。
6. **OK** をクリックします。
7. Ethernet (イーサネット) インターフェイスをハイライト表示させた状態で **Add Subinterface (サブインターフェイスの追加)** をクリックします。
8. **Interface Name (インターフェイス名)** は固定されています。ピリオドの後に、サブインターフェイス番号を 1 から 9,999 の範囲で入力します。
9. VLAN タグ ID を 1 から 4,094 の範囲で入力します。
10. サブインターフェイスを **Security Zone (セキュリティ ゾーン)** に割り当てます。
11. **OK** をクリックします。

STEP 2 | コミットします。

Commit（コミット）をクリックします。

STEP 3 | （任意）プロトコル保護を伴うゾーン プロテクション プロファイルを適用し、レイヤー 2 ゾーン間（あるいは単一のレイヤー 2 ゾーン内のインターフェイス間）の非 IP プロトコル パケットを制御します。

偵察行為防御の設定を行います。

VLAN 単位のスパニング ツリー（PVST +）BPDU 書き換えの管理

ファイアウォール上のインターフェースがレイヤー 2 デプロイメント用に設定されている場合、ファイアウォールはシスコの VLAN 単位のスパニングツリー（PVST +）または Rapid PVST + ブリッジ プロトコル データユニットのインバウンドポート VLAN ID（PVID）番号を書き換

え、（BPDU）を適切なアウトバウンドVLAN ID番号に変換し、BPDUを転送します。PAN-OS 7.1 で搭載されたこのデフォルトの動作により、ファイアウォールは、ファイアウォールの両側にある VLAN 内のシスコスイッチ間で、シスコ占有の PVST + および Rapid PVST + フレームに正しくタグを付けることができるため、Cisco PVST + および Rapid PVST + を使用したスパニングツリー ループ検出を適切に機能させることができます。ファイアウォールはSpanning Tree Protocol (スパニング ツリー プロトコル - STP)の選定プロセスに参加していないため、他のタイプのスパニングツリーの動作に変更はありません。

Cisco スイッチのループガードを無効にし、*PVST+* あるいは *Rapid PVST+ BPDU* の書き換え機能がファイアウォール上で正しく機能するようにしなければなりません。

この機能はレイヤー 2 イーサネットおよびAggregate Ethernet (AE) interfaces (集約イーサネット (AE)インターフェース)上でのみ上でサポートされます。ファイアウォールは、ネイティブ VLAN ID が 1 の PVID 範囲 1 ～ 4,094 をサポートし、シスコのネイティブ VLAN 実装と互換性があります。

PVST + BPDU 書き換え機能をサポートするために、PAN-OS は PVST + ネイティブ VLAN の概念をサポートしています。ネイティブ VLAN との間で送受信されるフレームには、ネイティブ VLAN と同じ PVID がタグ付けされていません。PVST + が正しく機能するためには、同じレイヤ 2 配置のすべてのスイッチとファイアウォールに同じネイティブ VLAN が必要です。シスコのネイティブ VLAN のデフォルトは vlan1 ですが、VLAN ID は 1 以外の番号にすることもできます。

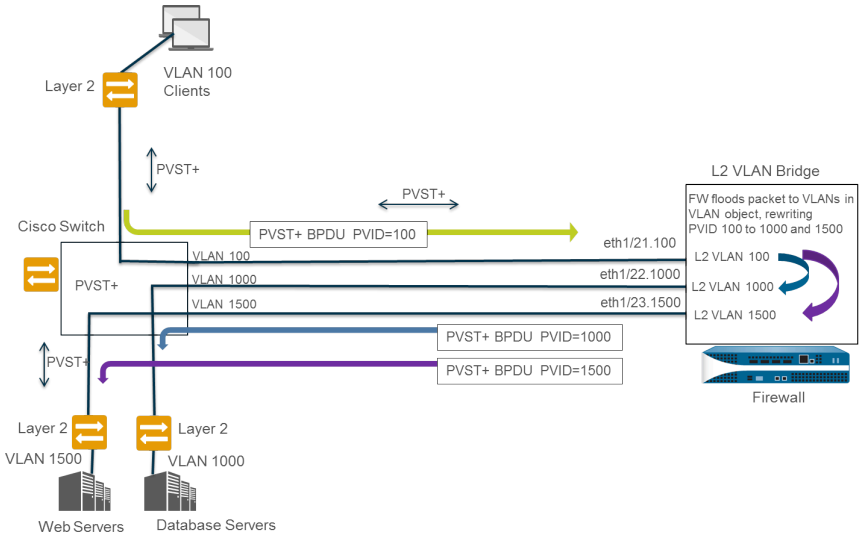
たとえば、ファイアウォールは VLAN オブジェクト（VLAN_BRIDGE という名前）で設定され、スイッチまたはブロードキャスト ドメインに属するインターフェースとサブインターフェースを記述します。この例では、VLAN には 3 つのサブインターフェースが含まれています。100 でタグ付けされたethernet1/21.100、1000でタグ付けされたethernet1/22.1000、および1500でタグ付けされたethernet1/23.1500です。

VLAN_BRIDGE に属するサブインターフェースは次のようになります

Ethernet | VLAN | Loopback | Tunnel | SD-WAN

INTERFACE	INTERFACE TYPE	LINK STATE	TAG	VLAN / VIRTUAL-WIRE	SECURITY ZONE	SD-WAN INTERFACE PROFILE	UPSTREAM NAT
ethernet1/21	Layer2		Untagged	none	none		Disabled
ethernet1/21.100	Layer2		100	VLAN_BRIDGE	Zone_Trust		Disabled
ethernet1/22	Layer2		Untagged	none	none		Disabled
ethernet1/22.1000	Layer2		1000	VLAN_BRIDGE	Zone_Untrust		Disabled
ethernet1/23	Layer2		Untagged	none	none		Disabled
ethernet1/23.1500	Layer2		1500	VLAN_BRIDGE	Zone_Management		Disabled

ファイアウォールが PVST + BPDU を自動的に書き換えるシーケンスを次の図と説明に示します。



1. VLAN 100 に属する Cisco スイッチポートは、PVID および 802.1Q VLAN タグが 100 に設定された PVST + BPDU をファイアウォールに送信します。
2. ファイアウォール インターフェースとサブインターフェースは、レイヤ 2 インターフェースタイプとして設定されています。ファイアウォールの入力サブインターフェースは VLAN 100 でタグ付けされます。これは、受信 BPDU の PVID および VLAN タグと一致するため、ファイアウォールは BPDU を受け取ります。ファイアウォールは PVST + BPDU を、同じ VLAN オブジェクト（この例では、ethernet1/22.1000およびethernet1/23.1500）に属する他のすべてのインターフェースにフラッディングします。VLAN タグが一致しない場合、ファイアウォールは代わりに BPDU をドロップします。
3. ファイアウォールが（同じ VLAN オブジェクトに属する）他のインターフェースを介して BPDU をフラッディングすると、ファイアウォールは PVID とすべての 802.1Q VLAN タグを書き換えて、出口インターフェースの VLAN タグと一致させます。この例では、BPDU がファイアウォールのレイヤ 2 ブリッジを通過するときに、ファイアウォールが 1 つのサブインターフェースの BPDU PVID を 100 から 1000 に、2 番目のサブインターフェースを 100 から 1500 に書き換えます。
4. 各シスコスイッチは、受信 BPDU で正しい PVID と VLAN タグを受信し、PVST + パケットを処理して、ネットワーク内のループの可能性を検出します。

以下の CLI 操作コマンドを使用すると、PVST + および Rapid PVST + BPDU を管理できます。

PVID の PVST + および Rapid PVST + BPDU の書き換えをグローバルに無効または再度有効にします（デフォルトは有効です）。

```
set session rewrite-pvst-pvid <yes|no>
```

ファイアウォールのネイティブ VLAN ID を設定します（範囲は 1 ～ 4,094 で、デフォルトは 1 です）。

スイッチのネイティブ *VLAN ID* が *1* 以外の値である場合は、ファイアウォールのネイティブ *VLAN ID* を同じ番号に設定する必要があります。 そうでない場合、ファイアウォールはその *VLAN ID* のパケットをドロップします。これは、トランクインターフェイスと非トランクインターフェースに適用されます。

set session pvst-native-vlan-id <*vid*>

すべての STP BPDU パケットをドロップします。

set session drop-stp-packet <yes|no>

すべての STP BPDU パケットをドロップする必要がある場合：

- ファイアウォールの両側にスイッチが 1 つだけあり、ループを引き起こす可能性のあるスイッチ間の他の接続がない場合、STP は不要であり、スイッチで無効にするか、ファイアウォールでブロックできます。
- 不適切に動作する STP スイッチが BPDU を不適切にフラッディングする場合、ファイアウォールで STP パケットを停止して、BPDU フラッディングを停止できます。

PVST + BPDU の書き換えが有効になっているかどうかを確認し、PVST ネイティブ VLAN ID を表示して、ファイアウォールがすべての STP BPDU パケットをドロップしているかどうかを確認します。

show vlan all

```
pvst+ tag rewrite: 無効
pvst native vlan id:    5
drop stp:                無効
total vlans shown:      1
名前       インターフェース              仮想インターフェース
ブリッジ    ethernet1/1
           ethernet1/2
           ethernet1/1.1
           ethernet1/2.1
```

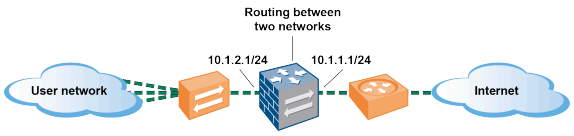
PVST + BPDU エラーのトラブルシューティングを行います。

show counter global

flow_pvid_inconsistent カウンターを見てください。これは、PVST + BPDU パケット内の 802.1Q タグと PVID フィールドが一致しない回数をカウントします。

レイヤー 3 インターフェイス

レイヤー 3 デプロイメントの場合、ファイアウォールは複数のポート間でトラフィックをルーティングします。レイヤ 3 インターフェイス を設定する前に、各レイヤ 3 インターフェイスのトラフィックをルーティングするためにファイアウォールで使用する 仮想ルータ を設定する必要があります。



Cisco Trustsec ネットワークで *security group tags (*セキュリティグループ タグ; *SGT)* を使用している場合は、ファイアウォールをレイヤー*2* モード、またはバーチャル ワイヤ モードのインライン構成で展開することが、ベストプラクティスになります。しかし、*Cisco TrustSec* ネットワークでレイヤー*3* ファイアウォールを使用する必要がある場合、レイヤー*3*ファイアウォールを*2* つの *SGT* 交換プロトコル *(SXP)* ピアの間に展開し、*SXP* ピア間のトラフィックをファイアウォールが許可するように設定する必要があります。

次のトピックでは、レイヤー 3 インターフェイスを設定する方法、Neighbor Discovery Protocol（NDP）を使用して IPv6 ホストを準備する方法、リンク ローカル ネットワーク上のデバイスの IPv6 アドレスを表示して素早くデバイスを探す方法を説明します。

- レイヤー 3 インターフェイスの設定
- NDP を使用して IPv6 ホストを管理

レイヤー 3 インターフェイスの設定

次の作業は、IPv4 あるいは IPv6 アドレスを持つレイヤー 3 インターフェイス（イーサネット、VLAN、ループバック、トンネル インターフェイス）を設定し、ファイアウォールがそれらのインターフェイス上でルーティングを行えるようにするために必要になります。ルーティングでトンネルを使用する場合、あるいはトンネル モニタリングがオンになっている場合、トンネルには IP アドレスが必要になります。次のタスクを実行する前に、1 つ以上の virtual routers を定義します。

通常は次の作業を行い、インターネットおよび内部ネットワークのインターフェイスに接続する外部インターフェイスを設定します。同じインターフェイスに IPv4 と IPv6 の両方のアドレスを設定できます。

PAN-OS ファイアウォール モデルでは、物理的あるいは仮想的なレイヤー *3* インターフェイスに最大 *16,000* 件の *IP* アドレスを割り当てることができますが、この数には *IPv4* および *IPv6* アドレスの両方が含まれています。

IPv6 ルートを使用している場合、DNS 設定用に IPv6 ルーター アドバタイズメントを提供するよう、ファイアウォールを設定することができます。ファイアウォールは再帰的な DNS サーバー（RDNS）アドレスおよび DNS 検索リストを持つ IPv6 DNS クライアントを準備し、そのク

ライアントが IPv6 DNS リクエストを解決できるようにします。これにより、ファイアウォールが DHCPv6 サーバーのように機能するようになります。

STEP 1 | インターフェイスを選択してセキュリティ ゾーンを使って設定します。

1. **Network (ネットワーク)** > **Interfaces (インターフェイス)** の順に選択し、さらに希望するインターフェイスの種類に応じて **Ethernet (イーサネット)**、**VLAN**、**loopback (ループバック)**、あるいは **Tunnel (トンネル)** のいずれかを選択します。
2. 設定するインターフェイスを選択します。
3. **Layer3 (レイヤー 3)** の **Interface Type (インターフェイス タイプ)** を選択します。
4. **Config (設定)** タブの **Virtual Router (仮想ルーター)** で、**default (デフォルト)** など、設定中の仮想ルーターを選択します。
5. マルチ仮想システム ファイアウォールの場合、**Virtual System (仮想システム)** は設定中の仮想システムを選択します。
6. **Security Zone (セキュリティ ゾーン)** については、インターフェイスが属するゾーンを選択するか、**New Zone (新規ゾーン)** を作成します。
7. **OK** をクリックします。

STEP 2 | IPv4 アドレスを持つインターフェイスを設定します。

次の 3 つのいずれかの方法で、IPv4 アドレスをレイヤー 3 インターフェイスに割り当てることができます。

- スタティック
- DHCP クライアント—ファイアウォール インターフェイスが DHCP クライアントとして機能し、動的に割り当てられた IP アドレスを受信します。ファイアウォールには、DHCP クライアント インターフェイスから受信した設定をファイアウォールで稼働中の DHCP サーバーに配信する機能も備えられています。これは一般的に、インターネット サービス プロバイダから提供される DNS サーバー設定を、ファイアウォールで保護されているネットワークで稼働中のクライアント マシンに配信する場合に使用されます。
- PPPoE—インターフェイスを PPPoE（Point-to-Point Protocol over Ethernet）終端点として設定し、デジタル加入者線（DSL）モデムはあるが、それ以外に接続を終端する PPPoE デバイスがない DSL 環境をサポートすることができます。

1. **Network (ネットワーク)** > **Interfaces (インターフェイス)** の順に選択し、さらに希望するインターフェイスの種類に応じて **Ethernet (イーサネット)**、**VLAN**、**loopback (ループバック)**、あるいは **Tunnel (トンネル)** のいずれかを選択します。
2. 設定するインターフェイスを選択します。
3. 静的 IPv4 アドレスを使ってインターフェイスを設定するには、**IPv4** タブで **Type (タイプ)** を **Static (静的)** に設定します。
4. アドレスの **Name (名前)** および任意で **Description (説明)** を **Add (追加)** します。

5. **Type (タイプ)** については次のいずれかを選択します。
   - **IP Netmask (IP** ネットマスク**)**—インターフェイスに割り当てる IP アドレスとネットワーク マスク（例：208.80.56.100/24）を入力します。

     レイヤー *3* インターフェイス アドレスに */31* サブネットマスクを使用している場合は、*ping* などのユーティリティが正しく機能するためには、インターフェイスを *.1/31* アドレスで設定する必要があります。

     IPv4 アドレスでループバック インターフェースを設定する場合は、*/32* サブネットマスクが必要です。 たとえば、*192.168.2.1/32* です。
   - **IP Range (IP** 範囲**)**—IP アドレス範囲を入力します（例：192.168.2.1-192.168.2.4）。
   - **FQDN**—完全修飾ドメイン名を入力します。
6. アドレスを適用する **Tags (タグ)** を選択します。
7. **OK** をクリックします。

STEP 3 | Point-to-Point Protocol over Ethernet（PPPoE）を持つインターフェイスを設定します。レイヤー 3 インターフェイスを参照してください。

HA アクティブ/アクティブ モードでは、*PPPoE* はサポートされていません。

1. **Network (ネットワーク)** > **Interfaces (インターフェイス)**を選択し、さらに **Ethernet (イーサネット)**、**VLAN**、**loopback (ループバック)**、あるいは **Tunnel (トンネル)** のいずれかを選択します。
2. 設定するインターフェイスを選択します。
3. **IPv4** タブで **Type (タイプ)** を **PPPoE** に設定します。
4. **General (全般)** タブで **Enable (有効)** を選択し、PPPoE 終端点用のインターフェイスを有効化します。
5. 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。
6. そのユーザー名用の **Password (パスワード)** と **Confirm Password (パスワードの確認)** を入力します。
7. **OK** をクリックします。

STEP 4 | DHCP クライアントとしてインターフェイスを設定する動的に割り当てられた IPv4 アドレスを受け取れるようになります。

HA アクティブ/アクティブ モードでは、*DHCP* クライアントはサポートされていません。

STEP 5 | 静的 IPv6 アドレスを持つインターフェイスを設定します。

1. **Network (ネットワーク)** > **Interfaces (インターフェイス)**を選択し、さらに **Ethernet (イーサネット)**、**VLAN**、**loopback (ループバック)**、あるいは **Tunnel (トンネル)** のいずれかを選択します。
2. 設定するインターフェイスを選択します。
3. **IPv6** タブで **Enable IPv6 on the interface (インターフェイスでの IPv6 の有効化)** を選択し、インターフェイス上の IPv6 アドレスを有効化します。
4. **Interface ID (インターフェイス ID)**については、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（たとえば、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。
5. IPv6 **Address (アドレス)** を **Add (追加)** するか、アドレスグループを選択します。
6. **Enable address on interface**（インターフェイス上のアドレスを有効にする） を選択し、インターフェイス上のこの IPv6 アドレスを有効にします。
7. **Use interface ID as host portion** （ホスト部分にインターフェイス **ID** を使用） を選択し、IPv6 アドレスのホスト部分に Interface ID（インターフェイス ID）を使用します。
8. （任意）**Anycast** を選択し、IPv6 アドレス（ルート）を Anycast アドレス（ルート）にします。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することを可能にし、ルーティング プロトコルのコストや他の要素に基づいて IPv6 が最も近いと判断したノードに Anycast トラフィックを送信できるようにします。
9. （イーサネット インターフェイスのみ）**Send Router Advertisement (ルーターのアドバタイジングを送信)**（RA）を選択し、ファイアウォールがルーター アドバタイズメントでこのアドレスを送信できるようにします。この場合、インターフェイス上でグローバル **Enable Router Advertisement (ルーターのアドバタイジングを有効化)** オプションも有効化する必要があります（次のステップ）。
10. （イーサネット インターフェイスのみ）ファイアウォールがアドレスを有効だとみなす **Valid Lifetime (sec) (有効期間（秒）)** を秒単位で入力します。有効期間は、**Preferred Lifetime (sec)**（優先ライフタイム（秒）） 以上でなければなりません（デフォルトは 2,592,000）。
11. （イーサネット インターフェイスのみ）有効なアドレスが優先される時間（秒）として、**Preferred Lifetime (sec)**（優先ライフタイム（秒）） を入力します。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）。
12. （イーサネット インターフェイスのみ）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は、**On-link (オン リンク)** を選択します。
13. （イーサネット インターフェイスのみ）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は、**Autonomous (自律型)** を選択します。
14. **OK** をクリックします。

STEP 6 | （IPv6 アドレスのみを使用する VLAN あるいはイーサネットのみ）ファイアウォールがインターフェイスから IPv6 ルーター アドバタイズメント（RA）を送信できるようにし、任意で RA パラメータを調整します。

次のいずれかを目的として *RA* パラメータを調整します。異なる値を使用するルーター/ホストを同時に使用するため。複数のゲートウェイが提示された場合に収束を高速化するため。例えば、プライマリ ゲートウェイが失敗した後で *IPv6* クライアント/ホストが素早くデフォルトゲートウェイを切り替え、ネットワーク内の別のデフォルトゲートウェイに向けて転送を開始できるよう、***Min Interval* (**最小間隔**)**、***Max Interval* (**最大間隔**)**、および ***Router Lifetime* (**ルーターの有効期間**)** の値を小さく設定します。

1. **Network (**ネットワーク**)** > **Interfaces (**インターフェイス**)** の順に選択し、さらに **Ethernet (**イーサネット**)** あるいは **VLAN** を選択します。
2. 設定するインターフェイスを選択します。
3. **[IPv6]** を選択します。
4. **Enable IPv6 on the interface (**インターフェイスでの **IPv6** の有効化**)** を選択します。
5. **Router Advertisement (**ルーター通知**)** タブで **Enable Router Advertisement (**ルーターのアドバタイジングを有効化**)**を選択します（デフォルトは disabled）。
6. （任意）ファイアウォールが送信する RA 間の最小間隔（秒）として **Min Interval (sec) (**最小間隔 **(**秒**))** を設定します（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。
7. （任意）ファイアウォールが送信する RA 間の最大間隔（秒）として **Max Interval (sec) (**最大間隔（秒）**)** を設定します（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。
8. （任意）クライアントに適用する、送信パケットの **Hop Limit (**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。
9. （任意）クライアントに適用するリンク最大送信ユニット（MTU）として **Link MTU (**リンク **MTU)** を設定します（範囲は 1,280～9,192、デフォルトは **unspecified (**未指定**)**）。リンク MTUがない場合は **unspecified (**未指定**)** を選択します。
10. （任意）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 **Reachable Time (ms) (**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 ～ 3600000、デフォルトは**unspecified**)。
11. （任意）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 **Retrans Time (ms) (**リトランスミッション タイマー（ミリ秒）**)** を設定します。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 ～ 4294967295、デフォルトは**unspecified**)。
12. （任意）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（秒）を **Router Lifetime (**ルーターの有効期間**) (sec)** で設定します（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。

13. 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に、優先するルーターを選択するためにクライアントが使用する **Router Preference (優先するルーター)** を設定します。**High (高)**、**Medium (中)**（デフォルト）、**Low (低)** は、RA がアドバタイズメントを行う際の優先順位であり、セグメント上の他のルーターに対するファイアウォールの仮想ルーターの相対的な優先順位を示します。
14. 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は、**Managed Configuration (管理された設定)** を選択します。
15. 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は、**Other Configuration (その他の設定)** を選択します。
16. 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は、**Consistency Check (一貫性チェック)** を選択します。一貫していない場合はファイアウォールがログに記録します。
17. **OK** をクリックします。

STEP 7 | （IPv6 アドレスのみを使用する VLAN あるいはイーサネットのみ）ファイアウォールがこのインターフェイスから ND ルーター アドバタイズメントでアドバタイズを行う 再帰的な DNS サーバーアドレスおよび DNS 検索リストを指定します。

クライアントが IPv6 DNS リクエストを解決できるよう、RDNS サーバーおよび DNS 検索リストは、DNS クライアント用の DNS 設定の一部になっています。

1. **Network (ネットワーク)** > **Interfaces (インターフェイス)** の順に選択し、さらに **Ethernet (イーサネット)** あるいは **VLAN** を選択します。
2. 設定中のインターフェイスを選択します。
3. **IPv6** > **DNS Support (サポート)** を選択します。
4. **Include DNS information in Router Advertisement (ルーター アドバタイズメントに DNS 情報を含める)** を選択し、ファイアウォールが IPv6 DNS 情報を送信できるようにします。
5. DNS **Server (サーバー)** については再帰的な DNS サーバーの IPv6 アドレスを **Add (追加)** します。再帰的な DNS サーバーを 最大 8 件 **Add (追加)** します。ファイアウォールは ICMPv6 ルーター アドバタイズメント内でサーバー アドレスを上から順に送信します。
6. ドメイン名を解決するためにクライアントが特定の RDNS サーバーを使用できる最大期間として、**Lifetime (有効期間)** を秒単位で指定します。
   - **Lifetime (有効期間)** 範囲は、**Max Interval (最大間隔)**（**Router Advertisement (ルーター通知)** タブで設定したもの）および **Max Interval (最大間隔)** の 2 倍の値と同じかその中間の値です。例えば、Max Interval (最大間隔) が 600 秒の場合、Lifetime (有効期間) の範囲は 600～1,200 秒です。
   - デフォルトの **Lifetime (有効期間)** は 1,200 秒です。
7. DNS Suffix (DNS サフィックス) については、**DNS Suffix (DNS サフィックス)**（最大 255 バイトのドメイン名）を **Add (追加)** します。DNS サフィックスを 最大 8 件 **Add (追加)**

します。ファイアウォールは ICMPv6 ルーター アドバタイズメント内でサフィックスを上から順に送信します。

8. クライアントがサフィックスを使用できる最大期間として、**Lifetime (**有効期間**)** を秒単位で指定します。この有効期間の範囲およびデフォルトの値は、**Server (**サーバー**)** のものと同じです。
9. **OK** をクリックします。

STEP 8 | （イーサネットまたは VLAN インターフェイス）静的 ARP エントリを指定します。静的 ARP エントリが ARP プロセシングを減少させます。

1. **Network (**ネットワーク**)** > **Interfaces (**インターフェイス**)** の順に選択し、さらに **Ethernet (**イーサネット**)** あるいは **VLAN** を選択します。
2. 設定中のインターフェイスを選択します。
3. **Advanced**（詳細） > **ARP Entries**（**ARP** エントリ）を選択します。
4. **IP Address**（**IP** アドレス）と対応する **MAC Address**（**MAC** アドレス）を **Add**（追加）します（ハードウェアまたはメディア アクセス制御アドレス）。VLAN インターフェイスの場合は、**Interface**（インターフェイス）も選択する必要があります。

   静的 *ARP* エントリはタイムアウトしません。自動学習されたキャッシュ内の *ARP* エントリは、デフォルトで *1,800* 秒でタイムアウトします。 *ARP* キャッシュ タイムアウトはカスタマイズできます。 「セッション タイムアウトの設定」を参照してください。
5. **OK** をクリックします。

STEP 9 | （イーサネットまたは VLAN インターフェイス）静的近隣探索プロトコル (NDP) エントリを指定します。IPv6 の NDP では、IPv4 の ARP と同じような機能が実行されます。

1. **Network (**ネットワーク**)** > **Interfaces (**インターフェイス**)** の順に選択し、さらに **Ethernet (**イーサネット**)** あるいは **VLAN** を選択します。
2. 設定中のインターフェイスを選択します。
3. **Advanced**（詳細） > **ND Entries**（**ND** エントリ）を選択します。
4. **IPv6 Address**（**IPv6** アドレス）とその対応する **MAC Address**（**MAC** アドレス）を **Add**（追加）します。
5. **OK** をクリックします。

STEP 10 | （任意）インターフェイスでサービスを有効化します。

1. インターフェイスでサービスを有効化するには、**Network (ネットワーク)** > **Interfaces (インターフェイス)** を選択し、さらに **Ethernet (イーサネット)** あるいは **VLAN** を選択します。
2. 設定中のインターフェイスを選択します。
3. **Advanced**（詳細） > **Other Info**（その他の情報）を選択します。
4. **Management Profile (管理プロファイル)** リストを拡張し、プロファイルまたは **New Management Profile (新規管理プロファイル)** を選択します。
5. プロファイルの**Name**（名前）を入力します。
6. **Permitted Services (許可するサービス)** については **Ping** などのサービスを選択し、**OK** をクリックします。

STEP 11 | 変更をコミットします。

STEP 12 | インターフェイスにケーブルを接続します。

ストレート ケーブルを使用して、設定したインターフェイスから対応するスイッチまたはルーターにネットワーク セグメントごとに接続します。

STEP 13 | インターフェイスがアクティブであることを確認します。

Web インターフェイスから、**Network (ネットワーク)** > **Interfaces (インターフェイス)** の順に選択し、Link State (リンク状態) 列のアイコンが緑になっていることを確認します。また、**[Dashboard]** の **[インターフェイス]** ウィジェットからリンク状態をモニタリングすることもできます。

STEP 14 | 仮想ルーターがトラフィックをルーティングできるよう、スタティック ルートかつ/または動的ルーティング プロトコル（RIP、OSPF、BGP）を設定します。

- スタティック ルートの設定
- RIP
- OSPF
- BGP

STEP 15 | デフォルト ルートを設定します。

スタティック ルートの設定を行い、それをデフォルトに設定します。

NDP を使用して IPv6 ホストを管理

このトピックは、NDP を使って IPv6 ホストを準備する方法を説明します。そのため、この目的で DHCPv6 サーバーを分離する必要はありません。また、これは NDP を使って IPv6 アドレスを監視し、セキュリティルールに違反した関連するユーザーおよびデバイスの IPv6 アドレスと MAC アドレスを素早く追跡できるようにする方法も説明します。

- DNS 設定用の IPv6 ルーター アドバタイズメント
- IPv6 ルーター アドバタイズメント用に RDNS サーバーおよび DNS 検索リストを設定

- NDP モニタリング
- NDP モニタリングの有効化

DNS 設定用の IPv6 ルーター アドバタイズメント

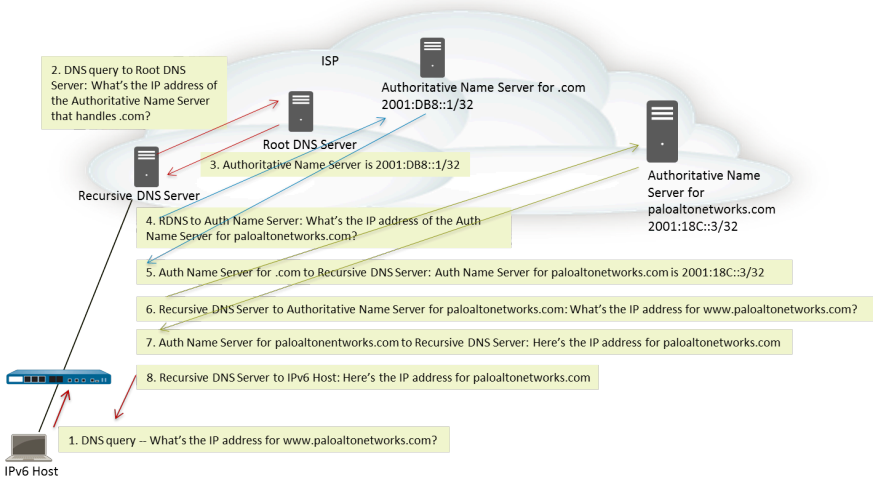
ファイアウォールにおけるネイバー検出（ND）の実装は強化されており、RFC 6106、IDNS 設定用の IPv6 ルーター アドバタイズメントに準拠した再帰的な DNS サーバー（RDNSS）オプションおよび DNS 検索リスト（DNSSL）を持つ IPv6 ホストを準備できます。レイヤー 3 インターフェイスの設定を行う際、ファイアウォール上でこれらの DNS オプションを設定し、ファイアウォールが IPv6 ホストを準備できるようにします。そのため、ホストを用意するために別途 DHCPv6 サーバーが必要になることはありません。ファイアウォールは DNS 設定の一部として、これらのオプションを含む IPv6 ルーター アドバタイズメント（RA）を IPv6 ホストに送信し、それらがインターネット サービスに到達できるよう、準備を完了させます。そのため、IPv6 ホストは次と共に設定されています。

- DNS クエリを解決できるRDNS サーバーのアドレス。
- ドメイン名を DNS クエリに入力する前に DNS クライアントが非修飾ドメイン名に付与（一度に一つ）するドメイン名（サフィックス）のリスト。

DNS 設定用の IPv6 ルーター アドバタイズメントは、すべての PAN-OS プラットフォームのイーサネット インターフェイス、サブインターフェイス、集約イーサネット インターフェイス、およびレイヤー 3 VLAN インターフェイスでサポートされています。

ファイアウォールは *DNS* 設定用に *IPv6 RA* を送信できるため、*DNS* プロキシ、*DNS* クライアントあるいは *DNS* サーバーであるファイアウォールとは無関係に、*DHCP* と同様の役割を果たすことができます。

RDNS サーバーのアドレスを使ってファイアウォールを設定したら、ファイアウォールはそれらのアドレスを使って IPv6 ホスト（DNS クライアント）を用意します。IPv6 ホストは、それらのアドレスの一つあるいは複数を使って RDNS サーバーに到達します。次の図でクエリおよびレスポンスの 3 つのペアとして示されている通り、再帰的な DNS は RDNS サーバーによる一連の DNS リクエストを参照します。例えば、ユーザーが www.paloaltonetworks.com にアクセスしようと試みる際、ローカルのブラウザが、自らのキャッシュにそのドメイン名に対応する IP アドレスが存在せず、クライアントのオペレーティングシステムにも存在しないことを知ります。クライアントのオペレーティングシステムは、ローカル ISP に属す再帰的な DNS サーバーに対して DNS クエリをローンチします。



IPv6 ルーター アドバタイズメントには、複数の DNS 再帰的なサーバーアドレス オプション（それぞれの有効期限は同じでも異なっていても良い）を含めることができます。単一の DNS 再帰的な DNS サーバーアドレス オプションには、各アドレスの有効期限が同じであれば、再帰的な DNS サーバーアドレスを複数含めることができます。

DNS 検索リストは、ファイアウォールが DNS クライアントにアドバタイズするドメイン名（サフィックス）のリストです。これによりファイアウォールは、非修飾 DNS クエリ内のサフィックスを使用する DNS クライアントを準備します。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、DNS 検索クライアントは非修飾ドメイン名に 1 つずつサフィックスを付与します。これにより、DNS クエリで完全修飾ドメイン名（FQDN）が使用されます。たとえば、（DNS クライアントを設定中の）ユーザーの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 FQDN になります。

DNS クエリに失敗すると、クライアントはリストの 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。クライアントは、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して）、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 サフィックスを順番に使用します。

ND 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。DNS 検索リスト オプションを受信する DNS クライアントが用意され、非修飾 DNS クエリでそのサフィックスを使用します。

RDNS サーバーおよび DNS 検索リストを指定するには、IPv6 ルーター アドバタイズメント用に RDNS サーバーおよび DNS 検索リストを設定します。

IPv6 ルーター アドバタイズメント用に RDNS サーバーおよび DNS 検索リストを設定

このタスクを実行し、IPv6 ホストの DNS 設定用の IPv6 ルーター アドバタイズメントを設定します。

STEP 1 | ファイアウォールがインターフェイスから IPv6 ルーター アドバタイズメントを送信できるようにします。

1. **Network (ネットワーク)** > **Interfaces (インターフェイス)** の順に選択し、さらに **Ethernet (イーサネット)** あるいは **VLAN** を選択します。
2. 設定するインターフェイスを選択します。
3. **IPv6** タブで **Enable IPv6 on the interface (インターフェイスでの IPv6 の有効化)** を選択します。
4. **Router Advertisement (ルーター通知)** タブで **Enable Router Advertisement (ルーターのアドバタイジングを有効化)**を選択します。
5. **OK** をクリックします。

STEP 2 | ファイアウォールがこのインターフェイスから ND ルーター アドバタイズメントでアドバタイズを行う 再帰的な DNS サーバーアドレスおよび DNS 検索リストを指定します。

クライアントが IPv6 DNS リクエストを解決できるよう、RDNS サーバーおよび DNS 検索リストは、DNS クライアント用の DNS 設定の一部になっています。

1. **Network (ネットワーク)** > **Interfaces (インターフェイス)** の順に選択し、さらに **Ethernet (イーサネット)** あるいは **VLAN** を選択します。
2. 設定中のインターフェイスを選択します。
3. **IPv6** > **DNS Support (サポート)** を選択します。
4. **Include DNS information in Router Advertisement (ルーター アドバタイズメントに DNS 情報を含める)** を選択し、ファイアウォールが IPv6 DNS 情報を送信できるようにします。
5. DNS **Server (サーバー)** については再帰的な DNS サーバーの IPv6 アドレスを **Add (追加)** します。再帰的な DNS サーバーを 最大 8 件 **Add (追加)** します。ファイアウォールは ICMPv6 ルーター アドバタイズメント内でサーバー アドレスを上から順に送信します。
6. ドメイン名を解決するためにクライアントが特定の RDNS サーバーを使用できる最大期間として、**Lifetime (有効期間)** を秒単位で指定します。
   - **Lifetime (有効期間)** 範囲は、**Max Interval (最大間隔)**（**Router Advertisement (ルーター通知)** タブで設定したもの）および **Max Interval (最大間隔)** の 2 倍の値と同じかその中間の値です。例えば、Max Interval (最大間隔) が 600 秒の場合、Lifetime (有効期間) の範囲は 600～1,200 秒です。
   - デフォルトの **Lifetime (有効期間)** は 1,200 秒です。
7. DNS Suffix (DNS サフィックス) については、**DNS Suffix (DNS サフィックス)**（最大 255 バイトのドメイン名）を **Add (追加)** します。DNS サフィックスを 最大 8 件 **Add (追加)** します。ファイアウォールは ICMPv6 ルーター アドバタイズメント内でサフィックスを上から順に送信します。
8. クライアントがサフィックスを使用できる最大期間として、**Lifetime (有効期間)** を秒単位で指定します。この有効期間の範囲およびデフォルトの値は、**Server (サーバー)** のものと同じです。
9. **OK** をクリックします。

STEP 3 | 変更をコミットします。

Commit（コミット）をクリックします。

NDP モニタリング

IPv6 用の Neighbor Discovery Protocol（NDP）（RFC 4861）は、IPv4 用の ARP と同様の機能を果たします。ファイアウォールはデフォルトで、リンク層アドレスおよび接続リンク上のネイバーの状態を発見して追跡するために ICMPv6 パケットを使用する NDP を実行します。

NDP モニタリングの有効化そのため、リンク ローカル ネットワーク上のデバイスの IPv6 アドレス、その MAC アドレス、User-IDからの関連するユーザー名（そのデバイスの使用者がディレクトリ サービスを使ってログインした場合）、アドレスの到達可能性ステータス、NDP モニターが IPv6 アドレスからルーター アドバタイズメントを受信して最後に報告された日時を表示できます。ユーザー名はベストケースに基づきます。プリンター、ファックス装置、サーバーなど、ユーザー名を持たない IPv6 デバイスがネットワークに多く存在する可能性があります。

セキュリティルールに違反したデバイスやユーザーを素早く追跡したい際、IPv6 アドレス、MAC アドレス、ユーザー名が一箇所に表示されるため非常に便利です。MAC アドレスを物理スイッチあるいはアクセスポイントまでトレースバックするためには、IPv6 アドレスに対応する MAC アドレスが必要です。

NDP あるいは重複アドレス検出（*DAD*）メッセージをフィルタで除外するファイアウォールおよびクライアント間に別のネットワーク デバイスが存在する可能性があるため、*NDP* モニタリングでは、すべてのデバイスを検出できるという保証はありません。ファイアウォールは、インターフェイス上で学習したデバイスのみを監視できます。

また、NDP モニタリングはクライアントおよびネイバーから来る重複アドレス検出（DAD）パケットも監視します。さらに、IPv6 ND ログを監視してトラブルシューティングを行いやすくすることもできます。

NDP モニタリングは、すべての PAN-OS モデルのイーサネット インターフェイス、サブインターフェイス、集約イーサネット インターフェイス、および VLAN インターフェイスでサポートされています。

NDP モニタリングの有効化

このタスクを実行してインターフェイスの NDP モニタリング を有効化します。

STEP 1 | NDP モニタリングを有効化します。

1. **Network (ネットワーク)** > **Interfaces (インターフェイス)** の順に選択し、さらに **Ethernet (イーサネット)** あるいは **VLAN** を選択します。
2. 設定中のインターフェイスを選択します。
3. **[IPv6]** を選択します。
4. **Address Resolution (アドレス解決)** を選択します。
5. **Enable NDP Monitoring (NDP モニタリングの有効化)** を選択します。

   NDP モニタリングを有効化した後で ***Commit (コミット)*** を行わなければ、*NDP* モニタリングを開始・終了することができません。
6. **OK** をクリックします。

STEP 2 | 変更をコミットします。

Commit（コミット）をクリックします。

STEP 3 | クライアントおよびネイバーからの NDP および DAD パケットを監視します。

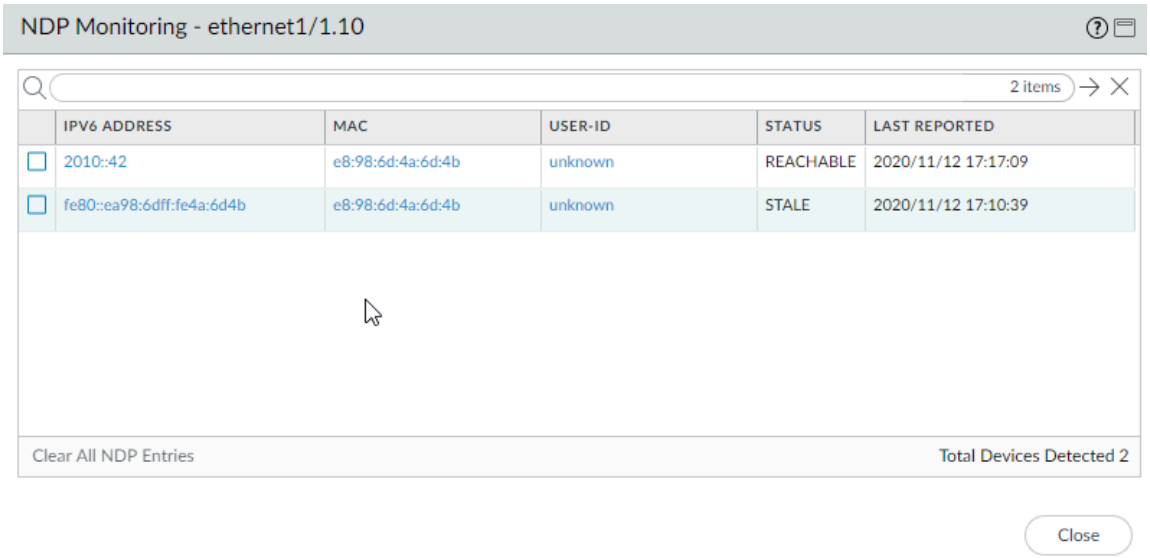
1. **Network (ネットワーク)** > **Interfaces (インターフェイス)** の順に選択し、さらに **Ethernet (イーサネット)** あるいは **VLAN** を選択します。
2. NDP モニタリングを有効にしたインターフェイスの [機能] 列で、[NDP モニタリング] アイコンの上にカーソルを置きます。

   インターフェイス用の NDP モニタリングのサマリーでは、RA が有効な場合にこのインターフェイスがルーター アドバタイズメント（RA）内で送信する IPv6 **Prefixes (プレフィックス)** のリストが表示されます。

   またこのサマリーは、DAD、ルーター アドバタイズメント、および DNS サポートが有効かどうか、いずれかの再帰的な DNS サーバーの IP アドレスが設定されているか

どうか、DNS 検索リストで設定されている DNS サフィックスがあづかどうかも示します。

3. NDP モニタリング アイコンをクリックして詳細を表示します。



インターフェイス用の詳細な NDP モニタリングの表の各行には、ファイアウォールが発見したネイバーの IPv6 アドレス、対応する MAC アドレス、対応する User-ID（最高の条件下で）、アドレスに到達可能かどうかという状態、この IP アドレスからこの NDP モニターが RA を受信して西郷に報告された日時が表示されます。プリンターや他のユーザーベースでないホストの場合、User-ID は表示されません。IP アドレスのステータスが Stale の場合、そのネイバーは到達可能なものであるということがまだ既知になっていません（RFC 4861 に基づく）。

右下の数字は、リンク ローカル ネットワーク上で **Total Devices Detected (**検知されたデバイス合計数**)** です。

- フィルタ フィールドに IPv6 アドレスを入力してアドレスを検索して表示します。
- チェックボックスを切り替え、IPv6 アドレスを表示する、あるいは非表示にします。
- 数字あるいは左右の矢印をクリックするか、縦のスクロールバーを使えば多くの項目を表示できます。
- **Clear All NDP Entries (NDP** エントリをすべてクリア**)** をクリックして表全体をクリアします。

STEP 4 | レポートを行うために ND ログを監視します。

1. **Monitor (**監視**)** > **Logs (**ログ**)** > を選択します。
2. Type (タイプ) 列で、**ipv6nd** ログおよびその説明を確認します。

   例えば `inconsistent router advertisementreceived` は、送信しようとしている RA とは異なる RA を、ファイアウォールが受信したことを示します。

集約インターフェイス グループの設定

集約インターフェースグループはIEEE 802.1AXリンク集約を用い、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を別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ースにまとめます。集約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。

デフォルト設定では、LACPを使用しない場合、直接接続されたピア間の物理レイヤーのみにおいてインターフェイス障害が自動的に検出されます。しかし、LACP（Link Aggregation Control Protocol）を有効化した場合、ピアが直接接続されているかどうかに関わらず、物理層およびデータリンク層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。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。VM シリーズ モデルを除くすべての Palo Alto Networks ®ファイアウォールは、集合グループをサポートします。Product Selection tool (製品選択ツール) は、各ファイアウォールがサポートする集約グループの数を示します。各集約グループには最大 8 つのインターフェースを設定できます。

PAN-OS ®ファイアウォール モデルでは、物理または仮想レイヤ *3* インターフェイスに割り当てられる最大 *16,000* 個の *IP* アドレスがサポートされます。この最大数には、*IPv4* アドレスと *IPv6* アドレスの両方が含まれます。

QoS は、最初の8つの集約グループでのみサポートされます。

集約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。いずれか特定の集約グループに割り当てられた各インターフェイスに対して、別のハードウェア メディアを使用できます（例：光ファイバーおよび銅を混在させられます）が、帯域幅およびインターフェイス タイプは同一でなければなりません。帯域幅およびインターフェイス タイプのオプション：

- 帯域幅—1Gbps、10Gbps、40Gbps、あるいは 100Gbps。
- **Interface type** [インターフェイス タイプ]—HA3、バーチャル ワイヤ、Layer 2、あるいはLayer 3。

ここでは、*Palo Alto Networks*のファイアウォールにのみ該当する設定の流れをご説明します。また、ピア デバイス上でも集約グループを設定する必要があります。説明についてはそのデバイスのドキュメントをご覧ください。

STEP 1 | 一般的なインターフェイス グループのパラメーターを設定します。

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、**Add Aggregate Group (集約グループの追加)** を行います。
2. 読み取り専用の **Interface Name**[インターフェイス名] に隣接したフィールドで、集約グループを識別する数値（1 ～ 8）を入力します。
3. **Interface Type** [インターフェイス タイプ]として**HA**、**Virtual Wire** [バーチャル ワイヤ]、**Layer2**、あるいは**Layer3**を選択します。
4. 選択した**Interface Type** [インターフェイス タイプ]に関する残りのパラメーターを設定します。

STEP 2 | LACP の設定を行います。

その集約グループでLACPを有効にしたい場合のみ、このステップを実行してください。

バーチャル ワイヤー インターフェイスでは *LACP* を有効にできません。

1. **LACP** タブを選択し、さらに[LACP を有効化] を選択します。
2. LACPステータス クエリの**Mode** [モード]を**Passive** [パッシブ]（デフォルト設定。ファイアウォールは応答のみ行います）あるいは**Active** [アクティブ]（ファイアウォールはピア デバイスのクエリを送信します）に設定します。

   片方の*LACP*ピアをアクティブにし、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。ファイアウォールは自身のピア デバイスのモードを検出することができません。
3. LACPクエリおよびレスポンス交換の**Transmission Rate** [送信頻度]を**Slow** [低]（デフォルト設定。30秒ごと）あるいは**Fast** [高]（毎秒）に設定します。ネットワークがサポートしているLACP処理量、および必要なLACPピアの検知速度とインターフェイス エラーの解決速度に応じて選択を行います。
4. 待機中のインターフェイスへのフェイルオーバーを1秒未満で行う機能を有効化する場合は**Fast Failover** [高速フェイルオーバー]を選択します。デフォルト設定ではこのオプションは無効になっており、ファイアウォールはIEEE 802.1ax規格を使用してフェイルオーバー処理を行うため、3秒以上の時間を要します。

   ***Fast Failover** [高速フェイルオーバー]*は、標準的なフェイルオーバー間隔では重要なデータを失うおそれがあるようなデプロイ環境で使用することが推奨されます。
5. 集約グループでアクティブ（1～8）になっている**[最大ポート]**（インターフェース数）を入力します。グループに割り当てるインターフェイス数が **[最大ポート]** を超えると、残りのインターフェイスはスタンバイ モードになります。ファイアウォールは、割り当てた (ステップ3) 各インターフェースの **LACP Port Priority (LACP** ポート優先順位**)** を使用して、最初にアクティブになるインターフェースとフェイルオーバー時にスタンバイ インターフェースがアクティブになる順序を決定します。LACPピアが非一致ポートの優先度値を持っている場合、**System Priority**（システム優先） 番号（デフォ

ルトは32,768。範囲は1～65,535）が低いピアの値で他のピアがオーバーライドされます。

6. （任意）アクティブ/パッシブ ファイアウォールの場合についてのみ、パッシブ ファイアウォール用のLACPプレ ネゴシエーションを有効にしたい場合は**Enable in HA Passive State** [HAパッシブ状態で有効]を選択します。LACP プレ ネゴシエーションにより、パッシブ ファイアウォールに素早くフェイルオーバーできるようになります（詳細についてはアクティブ/パッシブ HA のための LACP および LLDP プレネゴシエーションを参照）。

   このオプションを選択すると***Same System MAC Address for Active-Passive HA*** *[アクティブ/パッシブHAと同じシステムMACアドレス]* は選択できません。プレ ネゴシエーションでは、各*HA*ファイアウォールが固有のインターフェイス*MAC*アドレスを持っていなければならないためです。

7. （任意）アクティブ/パッシブ ファイアウォールの場合のみ、**Same System MAC Address for Active-Passive HA** [アクティブ/パッシブHAと同じシステムMACアドレス]を選択し、両方のHAファイアウォールに対して単一の**MAC Address** [MACアドレス]を指定します。このオプションにより、LACPピアが仮想化されている場合（単一のデバイスとしてネットワークに出現）、フェイルオーバーの待機時間が最短化されます。このオプションはデフォルトで無効になっています。HA ペアの各ファイアウォールは一意の MAC アドレスを持っています。

   *LACP*ピアが仮想化されていない場合は、一意の*MAC*アドレスを使用してフェイルオーバーの待機時間を最小限に抑えます。

STEP 3 | **OK** をクリックします。

STEP 4 | インターフェイスを集約グループに割り当てます。

集約グループのメンバーになるインターフェイス（1 ～ 8）ごとに以下の手順を実行します。

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、インターフェイス名をクリックして編集します。
2. **Interface Type** [インターフェイス タイプ]を **Aggregate Ethernet** [集約イーサネット]に設定します。
3. 定義した **[集約グループ]** を選択します。
4. **[リンク速度]**、**[リンク デュプレックス]**、および **[リンク状態]** を選択します。

   グループの各インターフェイスに同じリンク速度とデュプレックスの値を設定することをお勧めします。値が一致していない場合、ファイアウォールはデフォルトのより速い速度およびフル デュプレックスを設定します。

5. （任意）集約グループ用のLACPを有効にした場合、**LACP Port Priority**（**LACP**ポート優先度）（デフォルトは32,768。範囲は1～65,535）を入力します。割り当てるインターフェイス数が、グループの **Max Ports** [最大ポート]の値を超える場合、ポート優先順位により、どのインターフェイスがアクティブまたはスタンバイになるのかが決まります。数値がより低い（優先度が高い）インターフェイスがアクティブになります。
6. **OK** をクリックします。

STEP 5 | ファイアウォールがアクティブ/アクティブ構成であり、さらにHA3インターフェイスを集約している場合、その集約グループのパケット転送を有効にします。

1. **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)** の順に選択し、Packet Forwarding (パケット転送) セクションを編集します。
2. **HA3 Interface** [HA3インターフェイス]用に設定した集約グループを選択し、**OK**をクリックします。

STEP 6 | 変更を **Commit (コミット)** します。

STEP 7 | 集約グループの状態を確認します。

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. Link State （リンク状態）列に、集約グループの緑色のアイコンが表示されていることを確認します。緑色のアイコンは、すべてのメンバー インターフェイスがアップになっていることを示します。アイコンが黄色だと、少なくとも 1 つのメンバー（すべてのメンバーではない）がダウンしています。アイコンが赤色だと、すべてのメンバーがダウンしています。
3. LACPを構成した場合、Features （機能）列に、集約グループの LACPが有効になっていることを示すアイコン  が表示されていることを確認します。

STEP 8 | (PA-7050 および PA-7080 ファイアウォールのみ)異なるラインカード上に配置されたインターフェイスを持つ集約インターフェイス グループがある場合は、ファイアウォールを有効にして、複数のカードに分散している AE グループの複数のインターフェイスで受信したフラグメント化された IP パケットを処理できるようにすることがベスト プラクティスです。これを行うには、**hash** キーワードを指定して次の CLI 操作コマンドを使用します。(他の 2 つのキーワードも、完全性のために示されています。

1. CLI へのアクセスを行います。
2. 次の操作可能な CLI コマンドを使用してください: 設定 **ae-frag** 再配布ポリシー < 自己 | 固定 **sXdpX** | ハッシュ >
   - **self** – (デフォルト) このキーワードはレガシー動作用です。AE インターフェイス グループの複数のインターフェイスで受信したフラグメント化パケットをファイアウォールで処理することはできません。
   - 固定 **s** < *slot-number* >**dp** <データプレーン *cpu-number* >: スロット番号 変数を置き換え、 データプレーン *CPU* 番号 変数を、すべての AE インターフェイスのすべてのメンバーが受信するすべての IP フラグメントを処理するデータプレーンのデータプレーン番号に置き換えます。**fixed** キーワードは主にトラブルシューティングを目的としており、運用環境では使用しないでください。
   - **hash** –ファイアウォールが、複数のラインカード上にある AE インターフェイス グループの複数のインターフェイスで受信したフラグメント化パケットを処理できるようにするために使用します。

ネットワークセグメンテーションのためのConfigure Bonjourリフレクター

Apple Bonjour (ゼロ設定ネットワークとしても知られる) では、ローカル ネットワーク上のデバイスとサービスを自動検出できます。たとえば、Bonjour により、プリンタのIPアドレスを手動設定することなくプリンタに接続できます。名前をローカル ネットワーク上のアドレスへ変換するのに、Bonjour はMulticast DNS (マルチキャスト DNS; mDNS) を使用します。Bonjour ではトラフィックにプライベート マルチキャスト範囲を使用しています。これにより、トラフィック ルーティングが許可されず、セキュリティ目的または管理目的でネットワーク セグメンテーションを使用する環境 (サーバーとクライアントが異なるサブネットにある場合など) での使用が妨げられます。

セグメント化を使用してトラフィックをルーティングするネットワーク環境で Apple Bonjour をサポートするには、指定した レイヤー 3 インターフェイス(L3) Ethernet または Aggregate Ethernet (AE) インターフェイスまたはサブインターフェイス間で Bonjour IPv4 トラフィックを転送できます。Bonjour Reflector オプションを使用すると、マルチキャスト Bonjour アドバタイズメントとクエリを、L3 イーサネット、および AE インターフェースまたはサブインターフェースに転送でき、Time To Live (セッションの有効期間; TTL) 値やホップ制限に関係なく、ユーザーのサービスへのアクセスと、デバイスの検出可能性を確保します。

Bonjour トラフィック転送は、*PA-220*、*PA-400*、*PA-800*、および *PA-3200* シリーズでサポートされています。

このオプションを有効にすると、ファイアウォールは Bonjour トラフィックを、このオプションを有効にした L3、AE インターフェース、サブインターフェースにリダイレクトします。Bonjour トラフィックを管理したいインターフェース (サポートされているもの) すべてで、このオプションを有効にする必要があります。たとえば、特定の L3 インターフェースで、Bonjour トラフィックを AE インターフェースに転送したい場合、両方のインターフェースでこのオプションを有効にする必要があります。このオプションは最大16のインターフェースで有効にできます。

ループ防止のため、ファイアウォールは送信元 *MAC* アドレスを、ファイアウォールの出口インターフェース *MAC* アドレスに変更します。フラッド攻撃を防ぐために、以下の表に指定されている秒毎パケット数を超えるパケットをファイアウォールが受信すると、ファイアウォールはパケットを廃棄して、ファイアウォールとネットワークを保護します。

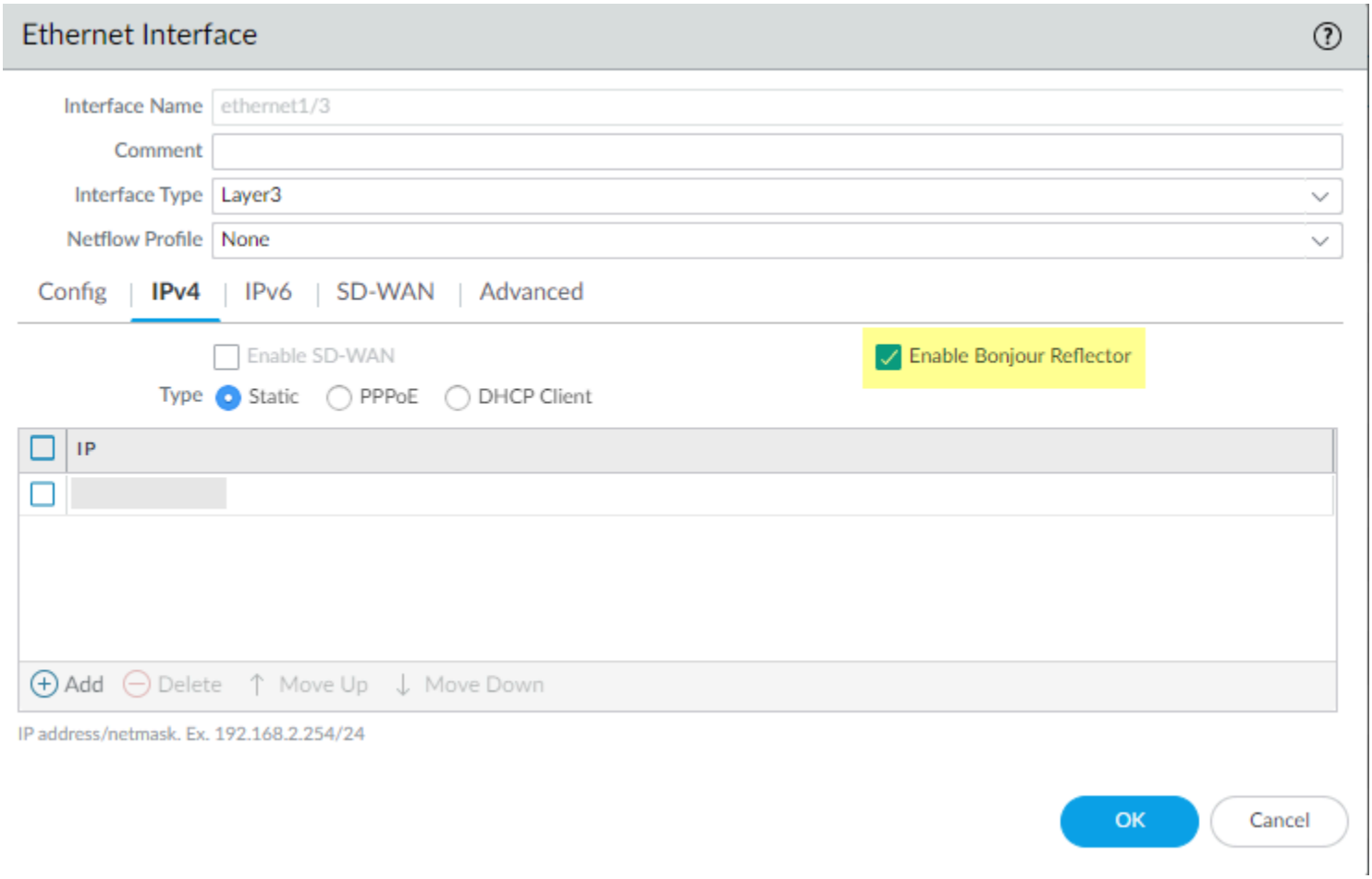
シリーズ	更新制限 *(*毎秒*)*
PA-220	*100*
PA-400	該当なし
PA-800	*200*
PA-3200	*500*

STEP 1 | **Network**（ネットワーク） > **Interfaces**（インターフェース）を選択します。

STEP 2 | L3 イーサネット、サブ インターフェース、AE インターフェースのいずれかを選択または **Add** (追加) します。

サブ インターフェースを追加する場合、そのサブ インターフェースは *0* ではなく ***Tag*** *(*タグ*)*を使用する必要があります。

STEP 3 | **IPv4** を選択してから、**Enable Bonjour Reflector (Bonjour Reflector** 有効化**)** オプションを選択します。



STEP 4 | **OK**をクリックします。

STEP 5 | Bonjour トラフィックを転送したい、L3、AE インターフェース、サブインターフェースの全てに対して、ステップ 1～4 を繰り返します。

このオプションは、最大*16*の別個のインターフェースまたはサブインターフェースで有効にできます。

STEP 6 | 変更を **Commit (**コミット**)**します。

STEP 7 | Bonjour Reflector オプションを有効にした各インターフェースの **Features (**機能**)** 列に、`Bonjour Reflector:yes` （ ）が表示されていることを確認します。

STEP 8 | `show bonjour interface` **(Bonjour**インターフェース表示**)** CLIコマンドを使用して、ファイアウォールが Bonjour トラフィックを転送するすべてのインターフェース、とカウンタのリストを表示します。`rx` はインターフェースが受信する Bonjour パケットの総数

を表し、tx はインターフェースが送信する Bonjour パケットの総数を表し、drop はインターフェースが廃棄するパケットの数を表します。

```
admin> show bonjour interface

name                    rx          tx          drop
-----------------------------------------------------------
ethernet1/4             1           1           0
ethernet1/7             0           0           0
ethernet1/7.10          0           0           0
ethernet1/7.20          4           4           0
ae15                    0           0           0
ae16                    0           0           0
ae16.30                 0           2           0
ae16.40                 0           0           0
```

インターフェイス管理プロファイルを使用してアクセスを制限

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管理トラフィックのアクセスを許可するプロトコル、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。例えば、ユーザーがethernet1/1インターフェイスを介して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のを拒否し、しかしそのインターフェイスがネットワーク監視システムからSNMPクエリを受信するのは許可したいという状況があり得ます。この場合、インターフェイス管理プロファイルでSNMPを有効化してHTTP/HTTPSを無効化し、そのプロファイルをethernet1/1に割り当てることになるでしょう。

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、および論理インターフェイス（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インターフェイス管理プロファイルをインターフェイスに割り当てない場合、デフォルト設定ではすべてのIPアドレス、プロトコル、サービスからのアクセスが拒否されます。

管理（*MGT*）インターフェイスではインターフェイス管理プロファイルが必須ではありません。がファイアウォールの初期構成 を実行する場合、*MGT* インターフェイスのプロトコル、サービス、および *IP* アドレスを制限します。*MGT*インターフェイスがダウンした場合でも、他のインターフェイスへの管理アクセスを許可しておくことでファイアウォールの管理を継続して行うことができます。

インターフェイス管理プロファイルを使用してファイアウォール インターフェイスへのアクセスを有効にする場合は、インターネットまたはエンタープライズ セキュリティ境界内の他の信頼されないゾーンからの管理アクセス *(HTTP、HTTPS、SSH、*または *Telnet)* を有効にしないように注意してください。これらのプロトコルは平文で送信されます。ファイアウォールへの管理アクセスを保護するためのベストプラクティスに従い、ファイアウォールが適切に保護されることを確認してください。

STEP 1 | インターフェイス管理プロファイルを設定します。

1. **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)** の順に選択し、**Add (追加)** をクリックします。
2. インターフェイスが管理トラフィックに対して許可するプロトコルを選択します。**Ping**、**Telnet**、**SSH**、**HTTP**、**HTTP OCSP**、**HTTPS**、あるいは**SNMP**のいずれかです。

   これらのプロトコルは平文で送信を行い、安全ではないため ***HTTP*** または ***Telnet*** を有効にしないでください。
3. インターフェイスが管理トラフィックに対して許可するサービスを選択します。
   - **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。
     - キャプティブ ポータル –キャプティブ ポータル応答ページを提供するために、ファイアウォールはレイヤ 3 インターフェイスでポートを開いたままにします。トランスペアレント モードのキャプティブ ポータルの 6081、リダイレクト モードのキャプティブ ポータルの場合は 6082。詳細については、認証ポリシーおよび認証ポータル 00 を参照してください。
     - **URL** 管理オーバーライド–詳細については特定のサイトへのパスワード アクセスを許可するを参照してください。
   - ユーザ **ID** - に使用して、データと認証のタイムスタンプ を再配分します。
   - **User-ID Syslog Listener-SSL** あるいは **User-ID Syslog Listener-UDP**–SSL あるいは UDP を介して、User-ID を設定してユーザーマッピング用に Syslog 送信者を監視するために使用します。
4. 任意）インターフェイスへのアクセスを許可するIPアドレスを**Add** [追加]します。リストに項目を加えない場合、インターフェイスのIPアドレス制限はありません。
5. **OK** をクリックします。

STEP 2 | インターフェイス管理プロファイルをインターフェイスに割り当てます。

1. **Network (ネットワーク)** > **Interfaces (インターフェイス)** を選択し、インターフェイスのタイプ（**Ethernet (イーサネット)**、**VLAN**、**Loopback (ループバック)**、あるいは **Tunnel (トンネル)**）を選択し、さらにインターフェイスを選択します。
2. **Advanced (詳細)** > **Other info (その他の情報)** を選択し、先ほど追加した Interface (インターフェイス) **Management Profile (管理プロファイル)** を選択します。
3. **OK**、**Commit (コミット)** の順にクリックします。

仮想ルーター

ファイアウォール上の仮想ルーターがレイヤ 3 ルーティングに参加し、仮想ルータを構成する方法について説明します。

仮想ルータの概要

ファイアウォールは、手動で静的ルートを定義するか、1 つ以上のレイヤ 3 ルーティング プロトコル(動的ルート)への参加を通じて、他のサブネットへのレイヤ 3 ルートを取得するために仮想ルータを使用します。これらの方式を通じてファイアウォールが取得するルートは、ファイアウォール上で IP ルーティング情報ベース（RIB）を自動作成します。パケットの目的地が到達した場所とは異なるサブネットである場合、仮想ルーターは RIB から最適なルートを取得し、それを転送情報ベース（FIB）に配置し、パケットを FIB で定義されているネクストホップのルーターに転送します。ファイアウォールは Ethernet スイッチングを使用して同じ IP サブネット上の他のデバイスにアクセスします。(FIB で行われる 1 つの最適ルートに対する例外は、ECMP を使用している場合に発生します。

ファイアウォールで定義されたイーサネット、VLAN、トンネル インターフェイスでは、レイヤー 3 パケットが送受信されます。宛先ゾーンは転送基準に基づいた発信インターフェイスによって決定され、ファイアウォールがポリシールールに問い合わせて各パケットに適用するセキュリティ ポリシーを識別します。仮想ルーターでは、他のネットワーク デバイスにルーティングする以外に、同じファイアウォール内にある他の仮想ルーターにルーティングすることもできます（ネクスト ホップが別の仮想ルーターを指すように指定されている場合）。

は、動的ルーティング プロトコル (BGP、OSPF、OSPFv3、または RIP) に参加し、スタティック ルートを追加するように、仮想ルータ のレイヤ 3 インターフェイスを設定できます。また、複数の仮想ルーターを作成し、各ルーターが他のルーターと共有しない独立したルートを保持することにより、インターフェイス間で異なるルーティングの動作を設定できます。

各仮想ルータでループバック インターフェイスを設定し、2 つのループバック インターフェイス間にスタティック ルートを作成し、これらの 2 つのインターフェイス間をピアリングするようにダイナミック ルーティング プロトコルを設定することにより、1 つの仮想ルータから別の仮想ルータへの動的ルーティングを設定できます。

ファイアウォールに定義されたレイヤー 3 イーサネット、ループバック、VLAN、およびトンネル 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しか属すことができませんが、単一の仮想ルーターに対して複数のルーティング プロトコルおよびスタティック ルートを設定できます。仮想ルータに対して設定するスタティック ルートとダイナミック ルーティング プロトコルに関係なく、1 つの一般的な設定が必要です。

仮想ルーターの構成

レイヤ 3 ルーティングに参加する 仮想ルータ をファイアウォール上に作成します。

STEP 1 | ネットワーク管理者から必要な情報を入手します。

- ルーティングを行いたいファイアウォール上のインターフェイス。
- スタティック、OSPF 内部、OSPF 外部、IBGP、EBGP、RIP の管理距離

STEP 2 | 仮想ルーターを作成してインターフェイスをそれに割り当てます。

ファイアウォールには、**default (**デフォルト**)** という名前の仮想ルーターが備わっています。**default (**デフォルト**)** の仮想ルーターを編集するか、新しい仮想ルーターを追加できます。

1. **Network (**ネットワーク**)** > **Virtual Routers (**仮想ルーター**)**の順に選択します。
2. 仮想ルーター（**default (**デフォルト**)** という名前のもの、あるいは別の仮想ルーター）を選択するか、新しい仮想ルーターの **Name (**名前**)** を **Add (**追加**)** します。
3. **Router Settings (**ルーター設定**)** > **General** （全般） を選択します。
4. **Interfaces (**インターフェイス**)**ボックスで **Add (**追加**)** をクリックし、定義済みのインターフェイスを選択します。

   仮想ルーターに追加するすべてのインターフェイスについてこのステップを繰り返します。
5. **OK** をクリックします。

STEP 3 | スタティックおよびダイナミック ルーティングの管理距離を設定します。

ネットワークの要件に合わせて、ルートの各タイプの管理距離を設定します。宛先が同じルートを複数持っている場合、仮想ルーターは管理距離を使用して、異なるルーティング プロトコルおよびスタティック ルートから、距離が短いものを優先しつつ最適なパスを選択します。

- 静的 :範囲は 10 ~ 240 です。デフォルトは 10 です。
- **OSPF** 外部 –範囲は 10 から 240 です。デフォルトは 110 です。
- **OSPF** 外部 :範囲は 10 ~ 240 です。デフォルトは 110 です。
- **IBGP** :範囲は10~240です。デフォルトは 200 です。
- **EBGP** –範囲は10~240です。デフォルトは 20 です。
- **RIP** –範囲は 10 から 240 です。デフォルトは 120 です。

転送のために同コストのパスを複数活用したい場合は、ECMP を参照してください。

STEP 4 | 仮想ルーターの全般的な設定をコミットします。

OK、**Commit (**コミット**)** の順にクリックします。

STEP 5 | イーサネット、VLAN、ループバック、およびトンネル インターフェイスを必要に応じて設定します。

レイヤー 3 インターフェイスの設定を行います。

サービス ルート

ファイアウォールがサービス ルートを使用して外部サービスに要求を送信し、サービス ルートを構成する方法について説明します。

サービス ルートの概要

ファイアウォールは、デフォルトで管理 (MGT) インターフェイスを使用して、DNS サーバー、外部認証サーバー、Palo Alto Networks® サービス (ソフトウェア、URL 更新、ライセンス、オートフォーカスなど) などの外部サービスにアクセスします。MGT インターフェイスの使用に代わる方法は、これらのサービスにアクセスするデータ ポート（通常のインターフェイス）を設定することです。インターフェイスからサーバー上のサービスへのパスをサービス ルートといいます。サービス パケットは外部サービスに割り当てられているポートからファイアウォールを出て、サーバーはその応答を、設定されている送信元インターフェイスおよび送信元 IP アドレスに送信します。

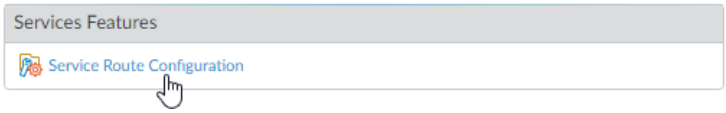
ファイアウォールに対してグローバルに サービス ルートの設定 個、または複数の仮想システムに対応するファイアウォール上の仮想システム のサービス ルートを カスタマイズして、仮想システムに関連付けられたインターフェイスを柔軟に使用できます。特定のサービスに対してサービス ルートを設定していない仮想システムでは、そのサービスに対してグローバルに設定されているインターフェイスと IP アドレスが継承されます。

サービス ルートの設定

次の手順では、サービス ルート を設定して、ファイアウォールが外部サービスに要求を送信するために使用するインターフェイスを変更できます。

STEP 1 | サービスルートをカスタマイズします。

1. **Device (デバイス)** > **Setup (セットアップ)** > **Services (サービス)** > **Global (グローバル)** を選択（複数仮想システムの能力を持たないファイアウォールの場合は Global (グローバル) を省略）し、Services Features (サービス機能) セクションで **Service Route Configuration (サービスルート設定)** をクリックします。



2. **Customize (カスタマイズ)** を選択し、次のいずれかを選択してサービスルートを作成します。

   - 事前定義済みのサービスの場合：
     - **IPv4** あるいは **IPv6** を選択し、サービスルートをカスタマイズしたいサービスのリンクをクリックします。

       複数のサービスで同じ送信元アドレスを使用しやすくするためには、***Set Selected Routes (選択したルートを設定)*** をクリックし、次のステップに進みます。

     - 送信元アドレスのリストを制限するためには、**Source Interface (送信元インターフェイス)** を選択し、(インターフェイスから) **Source Address (送信元アドレス)** をサービスルートとして選択します。アドレス オブジェクトは、選択したインターフェイスで既に設定されている場合は、送信元アドレスとして参照することもできます。**Any (すべての)** Source Interface (ソース インターフェイス) を選択すると、アドレスを選択する Source Address (送信元アドレス) リストで、あらゆるインターフェイスのすべての IP アドレスを利用できるようになります。**Use default (ユーザーデフォルト)** を選択すると、パケットの宛先 IP アドレスが設定済みの宛先 IP アドレスにマッチしない限り、ファイアウォールがサービスルート用の管理インターフェイスを使用するようになり、ソース IP アドレスがその **Destination (宛先)** 用に設定された **Source Address (送信元アドレス)** に設定されることになります。**MGT** を選択すると、宛先サービスルートに関わらず、ファイアウォールがサービスルート用の MGT インターフェイスを使用するようになります。

       サービス ルートの送信元アドレスは、参照先インターフェイスから構成の変更を継承しません。別の ***IP*** アドレスまたはアドレス オブジェクトにインターフェイス ***IP*** アドレスを変更しても、対応するサービス ルート 送信元アドレスは更新されません。これにより、コミットエラーが発生し、サービス ルートを有効な送信元アドレス値に更新する必要があります。

     - **OK** をクリックして設定を保存します。

- サービス用に IPv4 および IPv6 アドレスの両方を指定したい場合はこのステップを繰り返します。
- 宛先サービスルートの場合：
  - **Destination (宛先)** を選択し、**Destination (宛先)** IP アドレス を **Add (追加)** します。このケースでは、この設定済みの **Destination (宛先)** アドレスにマッチする宛先 IP アドレスと共にパケットが到達した場合、そのパケットの送信元 IP アドレスが、次のステップで設定する **Source Address (送信元アドレス)** にセットされます。
  - 送信元アドレスのリストを制限するためには、**Source Interface (送信元インターフェイス)** を選択し、(インターフェイスから) **Source Address (送信元アドレス)** をサービスルートとして選択します。**Any (すべての)** Source Interface (ソース インターフェイス) を選択すると、アドレスを選択する Source Address (送信元アドレス) リストで、あらゆるインターフェイスのすべての IP アドレスを利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。
  - **OK** をクリックして設定を保存します。

3. カスタマイズする各サービス ルートについて、前のステップを繰り返します。
4. **OK** をクリックしてサービスルートの設定を保存します。

STEP 2 | **[コミット]** します。

静的ルート

スタティック ルートは通常、動的ルーティング プロトコルと組み合わせて使用されます。動的ルーティング プロトコルが到達できないロケーション用にこのスタティックルートを設定する場合があります。ファイアウォールが動的ルートを自身のルートテーブルに入力するのと異なり、スタティック ルートでは、ネットワーク内のすべてのルーターで手動の設定を行う必要があります。スタティック ルートはその設定をすべてのルーターに対して求めますが、小さなネットワークにおいては、ルーティング プロトコルを設定するよりも適している場合があります。

スタティック ルートの概要

特定のレイヤー 3 トラフィックが IP ルーティング プロトコルに参加することなく特定のルートを取るようにさせる場合、IPv4 および IPv6 ルートを使用してスタティック ルートの設定を行うことができます。

特定のスタティックルートがデフォルト ルートになります。仮想ルーターのデフォルト ルートを取得するために動的ルーティングを使用しない場合、静的なデフォルト ルートを設定する必要があります。仮想ルーターがインバウンド パケットを持ち、ルートテーブルでそのパケットの宛先に対するマッチを見つけられない場合、仮想ルーターはそのパケットをデフォルト ルートに送信します。デフォルトの IPv4 ルートは 0.0.0.0/0、デフォルトの IPv6 ルートは ::/0 です。IPv4 および IPv6 両方のデフォルト ルートを設定できます。

スタティック ルートはネットワーク環境の変化に合わせて自己調整を行わないため、通常、静的に定義されたエンドポイントまでのルートでエラーが生じた場合、トラフィックは再ルーティングされません。しかし、次のような問題に備えてスタティック ルートのバックアップを取るオプションが用意されています。

- ファイアウォールおよび BFD ピア間の BFD セッションが失敗した場合、ファイアウォールが失敗したスタティックルートを RIB および FIB テーブルから取り除き、優先順位が低い別のルートを使用できるよう、双方向送信検出 (BFD) プロファイルを使ってスタティックルートを定義できます。
- ファイアウォールが別のルートを使用できるよう、スタティックルート用のパス モニタリングを設定を行えます。

デフォルト設定では、スタティック ルートの管理距離は 10 になっています。ファイアウォールが同じ宛先までのルートを複数持っている場合、管理距離が最も小さいルートを使用します。スタティックルートの管理距離をダイナミック ルートよりも大きい値に増やすことで、ダイナミック ルートを利用できない場合のバックアップ ルートとしてスタティックルートを使用できます。

スタティックルートを設定する際、ファイアウォールが IPv4 スタティックルートをユニキャストあるいはマルチキャスト ルート テーブル（RIB）、あるいは両方のテーブルにインストールするか、ルートを一切インストールしないかを指定できます。例えば、マルチキャスト トラフィックのみがルートを使用するようにするために、IPv4 スタティックルートをマルチキャスト ルート テーブルにインストールできます。このオプションにより、トラフィックが取るルートをより細かく指定できます。また、ファイアウォールが IPv6 スタティックルートをユニキャスト ルートテーブルにインストールするかどうかを指定できます。

パス モニタリングに基づくスタティックルートの削除

スタティックルート用のパス モニタリングを設定する際、ファイアウォールはパス モニタリングを使用して、一つあるいは複数の監視対象の宛先がダウンしたことを検知します。その後ファイアウォールは、別のルートを使用してトラフィックを再ルーティングします。次のように、ファイアウォールは HA あるいは ポリシーベース フォワーディング（PBF）用のパス モニタリングとほぼ同じように、スタティック ルートのパス モニタリングを使用します。

- ファイアウォールは、堅牢でスタティックルートのアベイラビリティを反映していると判断した監視対象の宛先の一つあるいは複数に対して ICMP ping メッセージを送信します。
- 監視対象の宛先に対する ping のいずれかあるいはすべてが失敗した場合、ファイアウォールはスタティックルートもダウンしているとみなし、それをルーティング情報ベース（RIB）および転送情報ベース（FIB）から取り除きます。RIB は、ファイアウォール用に設定されたスタティック ルート、およびルーティング プロトコルから学習したダイナミック ルートのテーブルです。FIB は、ファイアウォールがパケットを転送するために使用するルートの転送テーブルです。ファイアウォールは RIB から得た同じ宛先までの代替スタティックルートを選択（最も小さいメトリックを持つルートに基づいて）し、それを FIB に配置します。
- ファイアウォールは失敗したルートの監視を継続します。ルートがバックアップから来ており、さらに（失敗条件が **Any (**いずれか**)** あるいは **All (**すべて**)** であるかに基づいて）パスモニターが Up 状態に戻る際、プリエンプション待機時間が開始されます。ホールドタイマーの期間中、パスモニターが稼働状態を保つ必要があります。そうするとファイアウォールはスタティックルートが安定しているとみなし、RIB に戻します。次にファイアウォールはルートのメトリックを同じ宛先と比較し、どのルートを FIB に加えるのか判断します。

パス モニタリングは、以下のトラフィックのサイレント破棄を防ぐ最適なメカニズムです:

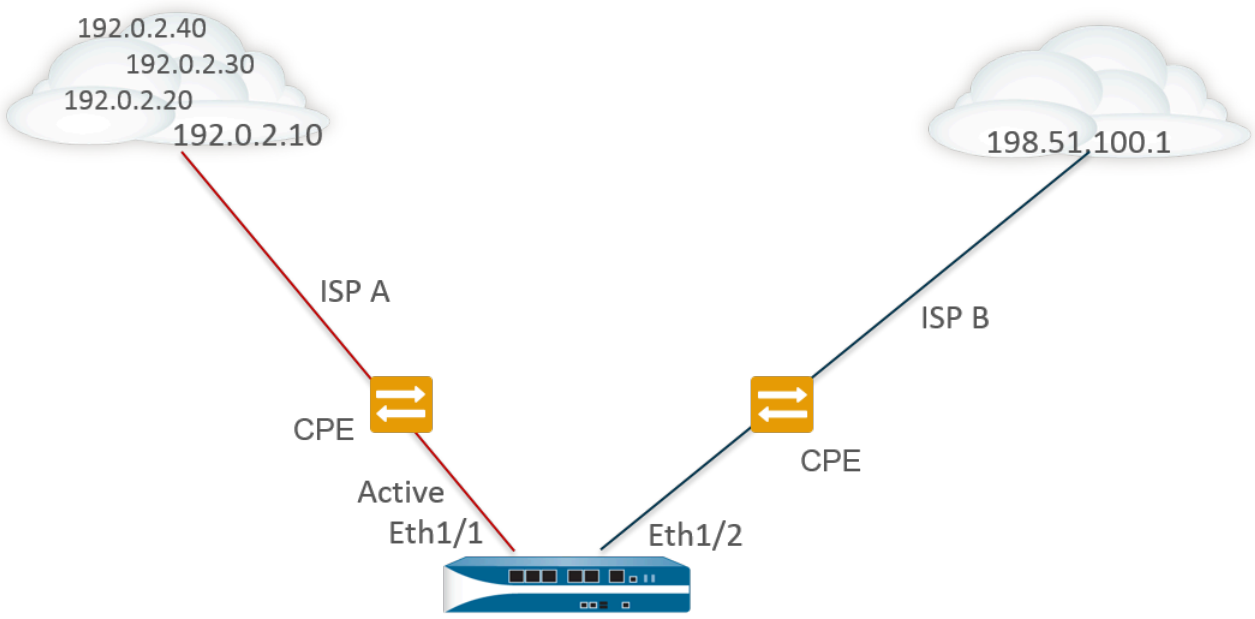
- スタティックあるいはデフォルト ルート。
- ルーティング プロトコルに再配信されるスタティックあるいはデフォルト ルート。
- 一つのピアが BFD をサポートしていない場合、スタティックあるいはデフォルト ルート。（単一のインターフェイス上で BFD およびパス モニタリングの両方を有効化しないことがベストプラクティスになります）
- 失敗したスタティックルートを RIB、FIB、あるいは再配信ポリシーから取り除かない、PBF パス モニタリングを使用する代わりとして、スタティックあるいはデフォルト ルート。

> パス モニタリングは、仮想ルーター間で設定されたスタティック ルートには適用されません。

次の図では、インターネットへのルートを冗長化するために、ファイアウォールが 2 つの ISP に接続されています。プライマリ デフォルト ルート 0.0.0.0（メトリック 10）はネクストホップ 192.0.2.10 を、セカンダリ デフォルト ルート 0.0.0.0（メトリック 50）はネクストホップ 198.51.100.1 を使用します。ISP A 用のクラスタ プレミス装置（CPE）が、インターネット接続がダウンした後でも、プライマリ物理層をアクティブに保ちます。リンクが人為的にアクティブになっている状態では、ファイアウォールはリンクがダウンしていることや、失敗したルートを RIB のセカンダリ ルートと置き換えなければならないということを検知しません。

失敗したリンクに向かうトラフィックのサイレント破棄を回避するために、192.0.2.20、192.0.2.30、192.0.2.40 のパス モニタリングを設定し、これらの宛先へのパス

のすべて（あるいはいずれか）が失敗した場合、ファイアウォールがネクストホップ 192.0.2.10 へのパスもダウンしていると仮定し、（ネクストホップ 192.0.2.10 を使う）スタティック ルート 0.0.0.0 を RIB から取り除き、それを、インターネットにアクセスする（ネクストホップ 198.51.100.1 を使う）同じ宛先 0.0.0.0 へのセカンダリ ルートと置き換えます。



Route Table

Destination	Next Hop	Metric	Interface	
0.0.0.0/0	192.0.2.10	10	ethernet1/1	X Pings to 192.0.2.20, 192.0.2.30, and 192.0.2.40 fail, so static route remove
0.0.0.0/0	198.51.100.1	50	ethernet1/2	

スタティック ルートの設定を行う際の必須フィールドの一つが、その宛先に向かうネクストホップです。次のように、設定するネクストホップのタイプによって、ファイアウォールがパスモニタリングを行う間に実行するアクションが決まります。

スタティックルートの **Next Hop Type (**ネクストホップ タイプ**)** が次の場合：	**ICMP ping** 用のファイアウォールのアクション
IP アドレス	ファイアウォールはスタティックルートの送信元 IP アドレスおよび出力インターフェイスを ICMP ping の送信元アドレスおよび出力インターフェイスとして使用します。これは監視対象の宛先の設定済みの宛先 IP アドレスを ping の宛先アドレスとして使用します。これはスタティックルートのネクストホップ アドレスを ping のネクストホップ アドレスとして使用します。
次の **VR**	ファイアウォールはスタティックルートの送信元 IP アドレスを ICMP ping の送信元アドレスとして使用します。出力インターフェイスは、ネ

スタティックルートの **Next Hop Type (**ネクストホップ タイプ**)** が次の場合：	**ICMP ping** 用のファイアウォールのアクション
	クストホップの仮想ルーターから得られる検索結果に基づいています。これは監視対象の宛先の設定済みの宛先 IP アドレスが ping の宛先アドレスになります。
無し	ファイアウォールはパスモニターの宛先 IP アドレスをネクストホップとして使用し、スタティックルートで指定されたインターフェイスに ICMP ping を送信します。

スタティックあるいはデフォルト ルートのパス モニタリングが失敗すると、ファイアウォールは critical (重要) なイベント（path-monitor-failure）をログに記録します。スタティックあるいはデフォルト ルートが回復すると、ファイアウォールはもう一度 critical (重要) なイベント（path-monitor-recovery）をログに記録します。

ファイアウォールはアクティブ/パッシブ HA デプロイメント用のパス モニタリング設定を同期しますが、パッシブ HA ピアの出力 ICMP ping パケットについては、これがアクティブにトラフィックを処理していないため、ブロックします。ファイアウォールはアクティブ/アクティブ HA デプロイメントのパス モニタリング設定を同期しません。

スタティック ルートの設定

次のタスクを実行し、ファイアウォール上のVirtual Router (仮想ルーター - VR) 用にスタティックルートあるいはデフォルト ルートを設定します。

STEP 1 | スタティック ルートを設定します。

1. **Network (**ネットワーク**)** > **Virtual Router (**仮想ルーター**)** を選択し、**default (**デフォルト**)** など、設定中の仮想ルーターを選択します。
2. **Static Routes** [スタティックルート]タブを選択します。
3. 設定したいスタティックルートの種類に応じて **IPv4** あるいは **IPv6** を選択します。
4. ルートの **Name (**名前**)** を **Add (**追加**)** します。
5. **Destination (**宛先**)** については、ルートおよびネットマスクを入力します（例えば、IPv4 アドレスの場合は 192.168.2.2/24、あるいは IPv6 アドレスの場合は 2001:db8:123:1::1/64 ）。デフォルト ルートを作成している場合は、デフォルト ルートを入力します（IPv4 アドレスの場合は 0.0.0.0/0、IPv6 アドレスの場合は ::/0）。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。
6. （任意）**Interface (**インターフェイス**)** については、パケットがネクストホップに進むために使用するアウトバウンド インターフェイスを指定します。これを使用し、このルートのネクストホップで使用するルートテーブルに含まれるインターフェイスではなく、どのインターフェイスをファイアウォールが使用するのか厳密に制御します。
7. **Next Hop (**ネクストホップ**)** については次のいずれかを選択します。
   - **IP Address (IP** アドレス**)**—特定のネクストホップにルーティングしたい際は、IP アドレス（例えば、192.168.56.1 や 2001:db8:49e:1::1）を入力します。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**（インターフェースでの **IPv6** 有効化）を実行する必要があります。デフォルト ルートを作成している場合は、**Next Hop (**ネクストホップ**)** で **IP Address (IP** アドレス**)** を選択し、インターネット ゲートウェイの IP アドレスを入力する必要があります（例えば、192.168.56.1 あるいは 2001:db8:49e:1::1）。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。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。
   - **Next VR (**次の **VR)**—ファイアウォール上の別の仮想ルーターへと内部でルーティングを行いたい場合は、このオプションを選択してから仮想ルーターを選択します。

- **FQDN**—FQDN を入力するか、FQDN を使用するアドレス オブジェクトを選択するか、あるいは FQDN 型のアドレス オブジェクトを新たに作成します。

  スタティックルートのネクストホップとして *FQDN* を使用する場合、その *FQDN* はスタティックルート用に設定したインターフェ-スと同じサブネットに属する *IP* アドレスに解決される必要があります。そうでない場合、ファイアウォールは解決を拒否して *FQDN* は未解決のままになります。

  ファイアウォールは *FQDN* の *DNS* 解決から得られた一つの *IP* アドレス *(IPv4* あるいは *IPv6* 系統それぞれ*)* のみを使用します。*DNS* 解決が複数のアドレスを返すと、ファイアウォールはネクストホップ用に設定された *IP* 系統 *(IPv4* あるいは *IPv6)* にマッチする、優先される *IP* アドレスを使用します。優先される *IP* アドレスは、*DNS* サーバーが初回の応答で返す最初のアドレスです。ファイアウォールは、順序に関わらずアドレスが後の応答に現れる限り、このアドレスを優先的に保持します。

- **Discard**（破棄） – この宛先に向かうパケットをドロップする場合に選択します。
- **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。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。

8. このVirtual Router (仮想ルーター - VR)について、静的ルート用に設定されたデフォルトの管理距離をルートが上書きする際の **Admin Distance (**管理距離**)**を入力します（範囲は 10～240、デフォルトは 10）。
9. ルートの **Metric**（メトリック） を入力します（範囲は 1～65,535）。

STEP 2 | ルートをインストールする場所を選択します。

ファイアウォールにスタティックルートをインストールさせたい **Route Table (**ルート テーブル**)**（RIB）を選択します。

- **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。ユニキャスト トラフィックでのみルートを使用したい場合はこのオプションを選択します。
- **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（IPv4 ルートでのみ利用可能）。マルチキャスト トラフィックでのみルートを使用したい場合はこのオプションを選択します。
- **Both (**両方**)**—ユニキャストおよびマルチキャスト ルート テーブルにルートをインストールします（IPv4 ルートでのみ利用可能）。ユニキャストあるいはマルチキャスト トラフィックでルートを使用したい場合はこのオプションを選択します。
- **No Install (**インストールしない**)**—いずれのルートテーブルにもルートをインストールしません。

STEP 3 | （任意）ファイアウォールのモデルがBFDをサポートしている場合、スタティックルートが失敗した際、ファイアウォールが RIB および FIB からそのルートを削除し、代わりのルートを選択できるよう、**BFD Profile**（**BFD** プロファイル）をスタティックルートに適用することができます。デフォルト設定は **None (**なし**)** です。

STEP 4 | **OK** を 2 回クリックします。

STEP 5 | 設定を **Commit**（コミット）します。

スタティックルート用のパス モニタリングを設定

次の各作業を行い、パス モニタリングに基づくスタティックルートの除去を設定します。

STEP 1 | スタティックルート用のパス モニタリングを有効化します。

1. **Network (ネットワーク)** > **Virtual Routers (仮想ルーター)** の順に選択し、さらに仮想ルーターを選択します。
2. **Static Routes (静的ルート)** を選択し、さらに **IPv4** あるいは **IPv6** を選択し、監視したいスタティックルートを選択します。最大 128 個のスタティック ルートを監視できます。
3. そのルールを対象にしてパス モニタリングを有効化するには、**Path Monitoring (パス モニタリング)** を選択します。

STEP 2 | スタティックルート用の監視対象の宛先を設定します。

1. 監視する宛先を **Name (名前)** 毎に **Add (追加)** します。スタティックルート毎に、監視対象の宛先を最大 8 件まで追加できます。
2. 宛先を監視するには、**Enable (有効)** を選択します。
3. **Source (送信元) IP** については、監視対象の宛先に ICMP ping を行う際に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。
4. **Destination IP (宛先 IP)** については、ファイアウォールがパスを監視する IP アドレスあるいはアドレス 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。

   宛先 *IP* アドレスは、信頼できるエンドポイントに属していなければなりません。パス モニタリングの基準を不安定あるいは信頼できないデバイスにするのは好ましくありません。
5. （任意）ファイアウォールがパスを監視する頻度を定める ICMP **Ping Interval (sec) (ping 間隔（秒）)** を秒数で指定します（範囲は 1 ～ 60、デフォルトは 3）。
6. （任意）スタティックルートがダウンしているとファイアウォールが判断してそれを RIB および FIB から取り除くまでの間、宛先から返されないパケットの ICMP **Ping Count (ping 数)** を指定します。
7. **OK** をクリックします。

STEP 3 | スタティックルート用のパス モニタリングの基準を単一あるいはすべての監視対象の宛先にするかを判断し、プリエンプション待機時間を設定します。

1. **Failure Condition (失敗条件)** を選択します。ファイアウォールはスタティック ルートを RIB および FIB から削除して、メトリックが次に小さく、同じ宛先に向かうスタティック ルートを FIB に追加するために、スタティック ルートの監視対象宛先の **Any (いずれか)** あるいは **All (すべて)**）がすべて ICMP から到達不能でなければなりません。

   All (すべて)を選択すると、たとえばいずれか *1* つの宛先がメンテナンスのためにオフラインになっていることで、ルート エラーとなってしまうような可能性を避けられます。

2. （任意）ファイアウォールがスタティックルートを RIB に再インストールするまでの間、ダウンしたパス モニタリングが Up 状態を維持しなければならない分数として、**Preemptive Hold Time (min) (プリエンプション待機時間（分）)** を指定します。パスモニターがスタティックルート用にすべての監視対象の宛先を評価し、**Any (すべて)** あるいは **All (すべて)** の失敗条件に基づいて動作します。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、リンクがダウン状態から復帰する際、パス モニターがダウン状態から復帰する場合があります。タイマーはパス 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ルートを RIB に再インストールします。範囲は 0 ～ 1,440、デフォルトは 2 です。

3. **OK** をクリックします。

STEP 4 | コミットします。

Commit（コミット）をクリックします。

STEP 5 | スタティック ルート上のパス モニタリングを検証します。

1. **Network**（ネットワーク） > **Virtual Routers**（仮想ルーター）を選択し、関心のある仮想ルーターの行で **More Runtime Stats**（ランタイム状態の詳細）を選択します。
2. **Routing (ルーティング)** タブで **Static Route Monitoring (静的ルート モニタリング)** を選択します。
3. スタティックルートの場合、パス モニタリングが Enabled (有効) か Disabled (無効) かを確認します。Status (状態) の列には、ルートが Up (アップ)、Down (ダウン)、Disabled (無効) であるかどうかが示されます。スタティックルートのフラグ：A—active (アクティブ)、S—static (スタティック)、E—ECMP。
4. 定期的に **Refresh (更新)** を選択し、パス モニタリングの最新の状態を確認します（安全状態チェック）。
5. ルートのステータスにカーソルを合わせ、監視対象の IP アドレス、およびそのルート用に監視対象の宛先に送信された ping の結果を表示します。例えば、3/5は ping 間隔が 3 秒であり、5 回連続して ping が失敗した（ファイアウォールが 15 秒間 ping を受信しなかった）ことを示し、パス モニタリングがリンクのエラーを検知したことが分かります。失敗条件が **Any (すべて)** あるいは **All (すべて)** であるかに応じて、パス モニタリングが失敗状態でファイアウォールが 15 秒後に ping を受け取った場合、パスが

有効だとみなされて **Preemptive Hold Time (**プリエンプティブ ホールド タイム**)** が開始されることがあります。

State (状態) は、最後に監視された ping の結果（成功あるいは失敗）を示します。Failed は、一連の ping パケット（ping 間隔 x ping 数）が成功しなかったことを示します。単一の ping パケットが失敗しても、ping 状態の失敗には反映されません。

STEP 6 | RIB および FIB を表示し、スタティックルートが除去されていることを確認します。

1. **Network**（ネットワーク） > **Virtual Routers**（仮想ルーター）を選択し、関心のある仮想ルーターの行で **More Runtime Stats**（ランタイム状態の詳細）を選択します。
2. **Routing (**ルーティング**)** タブで **Route Table (**ルート テーブル**)**（RIB）を選択し、さらに **Forwarding Table (**転送テーブル**)**（FIB）を選択してそれぞれを表示します。
3. 適切なルートテーブルを表示するには、**Unicast (**ユニキャスト**)** あるいは **Multicast (**マルチキャスト**)** を選択します。
4. **Display Address Family (**アドレス ファミリーの表示**)** については、**IPv4 and IPv6 (IPv4** および **IPv6)**、**IPv4 Only (IPv4** のみ**)**、あるいは **IPv6 Only (IPv6** のみ**)** を選択します。
5. （任意）フィルタ フィールドに検索対象のルートを入力し、矢印を選択するか、スクロールバーを使って各ルートのページを移動します。
6. ルートが削除されたか、まだ残っているかを確認します。
7. 定期的に **Refresh (**更新**)** を選択し、パス モニタリングの最新の状態を確認します（安全状態チェック）。

パス モニタリング用にロギングされたイベントを確認するには、***Monitor (***監視***) > Logs (***ログ***) > System (***システム***)*** を選択します。スタティックルート宛先用のパス モニタリングが失敗し、ルートが削除されたことを示す、***path-monitor-failure*** の項目を確認します。スタティックルート宛先用のパス モニタリングが回復し、ルートが復元されたことを示す、***path-monitor-recovery*** の項目を確認します。

RIP

RIP がネットワークに適したルーティング プロトコルであるかどうかを検討し、その場合は RIP を構成します。

RIP の概要

Routing Information Protocol （RIP）は、小規模 IP ネットワーク用に設計された内部ゲートウェイ プロトコル（IGP）です。RIP は、ホップ カウントに基づいてルートを決定します。ホップ数が最も少ないルートが最適ルートになります。RIP は UDP 上で動作し、ルートの更新にポート 520 を使用します。ルートを最大 15 ホップに制限すると、プロトコルによりルーティング ループの発生が回避されますが、サポートされるネットワーク サイズも制限されます。RIP を 設定する前に、15 ホップを超えるホップが必要な場合はトラフィックがルーティングされないことを考慮してください。RIP は、OSPF やその他のルーティング プロトコルよりも収束に時間がかかる場合があります。

ファイアウォールでは RIP v2 がサポートされています。

RIP の設定

RIPを構成するには、次の手順を実行します。

STEP 1 | 一般的な 仮想ルータ 設定を構成します。

STEP 2 | 全般的な RIP の設定を設定します。

1. 仮想ルーター (ネットワーク > 仮想ルーター) を選択し、仮想ルーターの場合は **RIP** を選択します。
2. RIPプロトコルを有効化する場合は、**Enable** [有効化]を選択します。
3. RIP 経由でデフォルト ルートを学習しない場合は、**Reject Default Route** [デフォルト ルートの拒否] を選択します。これが推奨されるデフォルトの設定です。

   RIP経由でデフォルト ルートを再配信するのを許可する場合は、**Reject Default Route** [デフォルト ルートの拒否] の選択を解除します。

STEP 3 | RIP 用のインターフェイスを設定します。

1. **Interfaces (インターフェイス)**タブで、Interface (インターフェイス) 設定セクションからインターフェイスを選択します。
2. 定義済みのインターフェイスを選択します。
3. **Enable**[有効] を選択します。
4. 指定したメトリック値を持つ RIP ピアにデフォルト ルートをアドバタイズするには、[アドバタイズ デフォルト ルート] を選択します。
5. (任意) **Auth Profile (認証プロファイル)** リストからプロファイルを選択することもできます。
6. **Mode (モード)** リストから normal、passive、または send-only を選択します。
7. (オプション)仮想ルータの RIP に対して BFDをグローバルに有効にするには、**BFD** プロファイルを選択します。
8. **OK** をクリックします。

STEP 4 | RIP タイマーを設定します。

1. **Timers**[タイマー] タブで、**Interval Seconds (sec)**[間隔 (秒)] ボックスに値を入力します。この設定では、次の RIP タイマー間隔の長さを秒単位で定義します (範囲は 1 ~ 60、デフォルトは 1)。
2. 更新間隔 を指定して、ルート更新アナウンスの間隔の数を定義します (範囲は 1 ~ 3,600、デフォルトは 30)。
3. の期限間隔 を指定して、ルートが最後に更新されてからその有効期限までの間隔の数を定義します (範囲は 1 から 3600、デフォルトは 120)。
4. 削除間隔 を指定して、ルートの有効期限が切れる間隔から削除までの間隔の数を定義します (範囲は 1 から 3,600、デフォルトは 180)。

STEP 5 | （任意）認証プロファイルを設定します。

デフォルトでは、ファイアウォールは RIP ネイバー間の交換に RIP 認証を使用しません。必要に応じて、簡易パスワードまたは MD5 認証を使用して RIP ネイバー間の RIP 認証を設定できます。単純なパスワードよりもセキュリティが優れているため、MD5 認証が推奨されます。

簡易パスワード **RIP** 認証

1. **Auth Profiles (**認証プロファイル**)** を選択し、RIP メッセージを認証する認証プロファイルの名前を **Add (**追加**)** します。
2. **Password Type**（パスワード タイプ） として **Simple Password**（簡易パスワード）を選択します。
3. 簡易パスワードを入力してから確認します。

MD5 RIP 認証

1. **Auth Profiles (**認証プロファイル**)** を選択し、RIP メッセージを認証する認証プロファイルの名前を **Add (**追加**)** します。
2. **Password Type**（パスワード タイプ） として **MD5** を選択します。
3. 次のような、単一あるいは複数のパスワード項目を **Add (**追加**)** します。
   - キー ID (範囲は 0 から 255)
   - 鍵
4. （任意）**Preferred (**優先**)** ステータスを選択します。
5. **[OK]** をクリックし、発信するメッセージを認証するために使用するキーを指定します。
6. [仮想ルーター - RIP - 認証プロファイル] ダイアログ ボックスで再び **[OK]** をクリックします。

STEP 6 | 変更を **Commit (**コミット**)** します。

OSPF

Open Shortest Path First (OSPF) は、大規模なエンタープライズ ネットワークでネットワーク ルートを動的に管理するために最も頻繁に使用される内部ゲートウェイ プロトコル (IGP) です。OSPF は、Link State Advertisement （LSA）を経由して別のルーターから情報を取得し、他のルーターにルートを通知することにより、動的にルートを決定します。LSA から収集される情報は、ネットワークのトポロジ マップを作成するために使用されます。このトポロジ マップはネットワーク内のルーター間で共有され、使用可能なルートで IP ルーティング テーブルを入力するために使用されます。

ネットワーク トポロジの変更は動的に検出され、数秒以内に新しいトポロジ マップを生成するために使用されます。最短経路のツリーが各ルートについて計算されます。各ルーティング インターフェイスに関連付けられたメトリックが最適なルートを計算するために使用されます。これらには距離、ネットワーク スループット、リンク可用性などが含まれます。さらに、これらのメトリックを静的に設定して、OSPF トポロジ マップの結果を誘導することができます。

Palo Alto Networks® OSPF の実装は、次の RFC を完全にサポートしています。

- RFC 2328（IPv4 用）
- RFC 5340（IPv6用）

以下のトピックでは、OSPF の詳細と、ファイアウォールで OSPF を設定する手順を説明します。

- OSPF の概念
- OSPF の設定
- OSPFv3 の設定
- OSPF グレースフル リスタートの設定
- OSPF 動作の確認

OSPF の概念

以下のトピックでは、ファイアウォールを OSPF ネットワークに参加するように設定するために理解しておく必要のある OSPF の概念を紹介します。

- OSPFv3IPv6
- OSPF ネイバー
- OSPF エリア
- OSPF ルーターのタイプ

OSPFv3IPv6

OSPFv3 は、IPv6 ネットワーク内で OSPF ルーティング プロトコルをサポートします。これにより、IPv6 アドレスおよびプレフィックスをサポートします。OSPFv （IPv4 用）の構造および機能はほとんど保持されますが、わずかながら変更点があります。以下は、OSPFv3 での追加および変更点の一部です。

- リンクごとに複数のインスタンスのサポート – OSPFv3 では、1 つのリンクで OSPF プロトコルの複数のインスタンスを実行できます。これは、OSPFv3 インスタンス ID 番号を割り当てることで実現されます。インスタンス ID に割り当てられたインターフェイスは、異なる ID を持つパケットをドロップします。
- リンクごとのプロトコル処理 – OSPFv3 は、IP サブネット単位だった OSPFv2 とは異なり、リンク単位で動作します。
- アドレス処理の変更 – リンク状態更新パケット内の LSA ペイロードを除き、IPv6 アドレスは OSPFv3 パケットに存在しません。隣接するルートはルーター ID によって識別されます。
- 認証の変更 – OSPFv3 には認証機能が含まれていません。ファイアウォールで OSPFv3 を設定するには、Encapsulating Security Payload（ESP）または IPv6 Authentication Header（AH）を指定する認証プロファイルが必要です。RFC 4552 で指定されているキーの再生成手順はこのリリースではサポートされません。
- リンクごとに複数のインスタンスをサポート – 各インスタンスは、OSPFv3 パケット ヘッダーに含まれるインスタンス ID に対応します。
- 新規**LSA**タイプ–OSPFv3は次の2つの新しいLSAタイプをサポートしています。Link LSAおよびIntra Area Prefix LSA。

すべての追加の変更点は、RFC 5340 に詳しく記述されています。

OSPF ネイバー

共通のネットワークで接続され、同じ OSPF エリアに存在する 2 つの OSPF が有効なルーターが関係を築いている場合、これらは OSPF ネイバーです。これらのルーター間の接続は、共通のブロードキャスト ドメインを経由する場合もあれば、ポイントツーポイント接続による場合もあります。この接続は、hello OSPF プロトコル パケットの交換を通じて確立されます。これらのネイバー関係は、ルーター間でルーティング更新を交換するために使用されます。

OSPF エリア

OSPF は、1 つの AS （Autonomous System）内で動作します。ただし、この 1 つの AS 内のネットワークは、多数のエリアに分割できます。デフォルトでは、エリア 0 が作成されます。エリア 0 は、単独で機能することも、多数のエリアの OSPF バックボーンとして機能することもできます。各 OSPF エリアは、ほとんどの場合、IP4 アドレスと同じドット区切りの表記法で記述される 32 ビット識別子を使用して名前が付けられます。たとえば、エリア 0 は通常 0.0.0.0 と記述されます。

エリアのトポロジは独自のリンク状態データベースでメンテナンスされ、他のエリアからは非表示になるため、OSPF によって必要なトラフィック ルーティングが削減されます。トポロジは、ルーターを接続することによってエリア間の要約された形式で共有されます。

OSPF エリアのタイプ	説明
バックボーン エリア	バックボーン エリア（エリア 0）とは、OSPF ネットワークの中心です。その他のすべてのエリアはこのエリアに接続され、エリア間のすべてのトラフィックはこのエリアを通過する必要があります。エリア間のすべてのルーティングは、バックボーン エリアを通じて分配されます。その他のすべての OSPF エリアはバックボーン エリアに接続する必要がありますが、この接続は直接的である必要はなく、仮想リンクを通じて行うこともできます。
通常の OSPF エリア	通常の OSPF エリアには制限はありません。エリアではすべてのタイプのルートを使用できます。
スタブ OSPF エリア	スタブ エリアは他の AS からのルートを受信しません。デフォルト ルートを通じてバックボーン エリアまでのスタブ エリアからのルーティングが可能です。
NSSA エリア	Not So Stubby Area （NSSA）とは、いくつかの例外はあるものの、外部ルートをインポートできるスタブ エリアの一種です。

OSPF ルーターのタイプ

OSPF エリア内で、ルーターは以下のカテゴリに分割できます。

- 内部ルーター – 同じエリアのデバイスのみと OSPF ネイバー関係を持つルーター。
- **Area Border Router（ABR）** – 複数の OSPF エリアのデバイスと OSPF ネイバー関係を持つルーター。ABR は接続されたエリアからトポロジ情報を収集し、バックボーン エリアに分配します。
- **Backbone Router**–バックボーン ルーターは、OSPF を実行するルーターであり、OSPF バックボーン エリアに接続されたインターフェイスを少なくとも 1 つ持っています。ABR は必ずバックボーンに接続されているため、必ずバックボーン ルーターとして分類されます。

- **Autonomous System Boundary Router （ASBR）** — ASBR とは、複数のルーティング プロトコルに接続され、その間でルーティング情報を交換するルーターです。

OSPF の設定

OSPF は、Link State Advertisement （LSA）を経由して別のルーターから情報を取得し、他のルーターにルートを通知することにより、動的にルートを決定します。ルーターには宛先との間のリンク情報が保存されているため、より効率的なルート決定を行うことができます。各ルーター インターフェイスには 1 つのコストが割り当てられます。経由するすべてのルーターの出力インターフェイスと LSA を受信したインターフェイスを総和したときコストが最低のルートとなるよう、最適なルートは決定されます。

階層手法を使用して、通知する必要があるルートおよび関連付けられる LSA の数を制限します。OSPF ではかなりの量のルート情報が動的に処理されるため、RIP の場合より大規模なプロセッサとメモリが必要になります。

STEP 1 | 一般的な virtual router 設定を構成します。

STEP 2 | OSPFを有効にします。

1. **OSPF** タブを選択します。
2. OSPFプロトコルを有効化する場合は、**Enable** [有効化]を選択します。
3. **Router ID**（ルーター **ID**）を入力します。
4. OSPF 経由でデフォルト ルートを学習しない場合は、**Reject Default Route** [デフォルトルートの拒否] を選択します。これが推奨されるデフォルトの設定です。

   OSPF経由でデフォルト ルートを再配信するのを許可する場合は、**Reject Default Route**（デフォルト ルートの拒否）の選択を解除します。

STEP 3 | OSPFプロトコルの Areas [エリア] - Type [タイプ]を設定します。

1. **Areas (エリア)** タブで、**Area ID (エリア ID)** を *x.x.x.x* の形式で **Add (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。
2. **Type (タイプ)** タブで、エリアの **Type (タイプ)** リストから以下のいずれかを選択します。
   - **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する場合、以下を設定します。
     - サマリーの受け入れ – Link State Advertisement（LSA）は他のエリアから受け入れられます。スタブ エリアのエリア ボーダー ルーター（ABR）インターフェイスでこのオプションが無効になっていると、OSPF エリアは Totally Stubby Area（TSA）として動作し、ABR はサマリー LSA を配信しません。
     - **Advertise Default Route** [デフォルト ルートの通知]– デフォルト ルート LSA は、設定された範囲（1 ～ 255）の設定されたメトリック値とともにスタブ エリアへの通知に含まれます。
   - **NSSA**（Not-So-Stubby Area） – ファイアウォールは、OSPF ルート以外のルートでのみエリアを出ることができます。NSSA を選択する場合、**Stub (スタブ)** につい

て説明したように **Accept Summary (**サマリーの受け入れ**)** および **Advertise Default Route (**デフォルト ルートのアドバタイズメント**)** を設定します。このオプションを選択する場合、以下を設定します。

- **Type**（タイプ） – デフォルト LSA を通知する **Ext 1** または **Ext 2** ルート タイプを選択します。
- **Ext Ranges (**外部範囲**)**–**Advertise (**アドバタイズメント**)** したい、あるいはアドバタイズメントを **Suppress (**抑制**)** したい外部ルートの範囲を **Add (**追加**)** します。

3. **OK** をクリックします。

STEP 4 | OSPFプロトコルの Areas [エリア] - Range [範囲]を設定します。

1. **Range (**範囲**)** タブで、エリア内の集約 LSA 宛先アドレスをサブネットに **Add (**追加**)** します。
2. サブネットと一致する LSA の通知を **Advertise**[通知] または **Suppress**[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。

STEP 5 | OSPFプロトコルの Areas [エリア] - Interfaces [インターフェイス]を設定します。

1. **Interface (**インターフェイス**)** タブで、エリアに含める各インターフェイス毎に次の情報を **Add (**追加**)** 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。
   - 有効化 – OSPF インターフェイス設定を有効にするにはこのオプションをオンにします。
   - **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しなければならない場合は **p2mp**（point-to-multipoint）を選択し、このインターフェイスを通じて到達できるすべてのネイバーの IP アドレスを **Add (**追加**)** します。
   - **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（範囲は 0 ～ 65535、デフォルトは 10）。
   - 優先順位 – このインターフェイスの OSPF 優先順位を入力します。この優先順位に基づいて、ルーターが指名ルーター（DR）またはバックアップ DR （BDR）として選択されます（範囲は 0 ～ 255、デフォルトは 1）。0 に設定すると、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。
   - **Timing (**タイミング**)**–必要な場合はタイミング設定を変更します（非推奨）。これらの設定の詳細については、オンライン ヘルプを参照してください。
2. **OK** をクリックします。

STEP 6 | Areas（エリア） - Virtual Links（仮想リンク）を設定します。

1. **Virtual Link (**仮想リンク**)** タブで、バックボーン エリアに含める各仮想リンク毎に次の情報を **Add (**追加**)** します。
   - **Name**（名前） – 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するには、オンにします。
   - **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。
   - **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。
2. **OK** をクリックして仮想リンクを保存します。
3. **OK** をクリックして、エリアを保存します。

STEP 7 | （任意）認証プロファイルを設定します。

デフォルトでは、ファイアウォールは OSPF ネイバー間の交換に OSPF 認証を使用しません。任意で、簡易パスワードまたは MD5 認証を使用して OSPF ネイバー間の OSPF 認証を設定できます。単純なパスワードよりもセキュリティが優れているため、MD5 認証が推奨されます。

簡易パスワード **OSPF** 認証

1. **Auth Profiles (**認証プロファイル**)** タブを選択し、OSPF メッセージを認証する認証プロファイルの名前を **Add (**追加**)** します。
2. **Password Type**（パスワード タイプ） として **Simple Password**（簡易パスワード）を選択します。
3. 簡易パスワードを入力してから確認します。

MD5 OSPF 認証

1. **Auth Profiles (**認証プロファイル**)** タブを選択し、OSPF メッセージを認証する認証プロファイルの名前を **Add (**追加**)** します。
2. **MD5** を **Password Type (**パスワード タイプ**)** として選択し、次のような単一あるいは複数のパスワード項目を **Add (**追加**)** します。
   - 鍵 ID （範囲は 0 ～ 255）
   - 鍵
   - **Preferred**（優先） オプションを選択して、発信メッセージの認証に使用するキーを指定します。
3. **OK** をクリックします。

STEP 8 | 詳細な OSPF オプションを設定します。

1. RFC 1583 への準拠を確保するには、**Advanced (詳細)** タブで、**RFC 1583 Compatibility (RFC 1583 の互換性)** を選択します。
2. 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タイマー（秒単位）として **SPF Calculation Delay (sec)**（**SPF** 計算遅延（秒）） の値を指定します。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、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。
3. **LSA Interval (sec) (LSA** 間隔 **(秒))** タイマーの値を設定します。このタイマーは、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。
4. **OK** をクリックします。

STEP 9 | 変更を **Commit (コミット)** します。

OSPFv3 の設定

OSPF では、IPv4 および IPv6 の両方がサポートされています。IPv6 を使用する場合は OSPFv3IPv6を使用する必要があります。

STEP 1 | 一般的な 仮想ルータ 設定を構成します。

STEP 2 | 全般的な OSPFv3 の設定を設定します。

1. **OSPFv3** タブを選択します。
2. OSPFプロトコルを有効化する場合は、**Enable** [有効化]を選択します。
3. **Router ID**（ルーター **ID**）を入力します。
4. OSPFv3 経由でデフォルト ルートを学習しない場合は、**Reject Default Route** （デフォルト ルートの拒否） を選択します。これが推奨されるデフォルトの設定です。

   OSPFv3 経由でデフォルト ルートを再配信するのを許可する場合は、**Reject Default Route (**デフォルト ルートの拒否**)** の選択を解除します。

STEP 3 | OSPFv3プロトコルの認証プロファイルを設定します。

OSPFv3 には独自の認証機能が含まれていませんが、ネイバー間の通信を安全にするために全面的に IPSec に依存します。

認証プロファイルを設定する場合、Encapsulating Security Payload （ESP）（推奨）または IPv6 Authentication Header （AH）を使用する必要があります。

ESP OSPFv3 認証

1. **Auth Profiles (認証プロファイル)** タブで、OSPFv3 メッセージを認証する認証プロファイルの名前を **Add (追加)** します。
2. セキュリティポリシー インデックス（**SPI**）を指定します（00000000～FFFFFFFF の範囲の 16 進数）。SPI の値が、OSPFv3 隣接の両端間で一致する必要があります。
3. **[プロトコル]** に **[ESP]** を選択します。
4. **Crypto Algorithm (暗号化アルゴリズム)** を選択します。

   None (なし) あるいは以下のアルゴリズムを一つ選択できます。**SHA1**、**SHA256**、**SHA384**、**SHA512**、あるいは**MD5**。
5. 「なし」以外の **Crypto Algorithm (暗号化アルゴリズム)** を選択した場合、**Key (キー)** の値を入力して確認します。

AH OSPFv3 認証

1. **Auth Profiles (認証プロファイル)** タブで、OSPFv3 メッセージを認証する認証プロファイルの名前を **Add (追加)** します。
2. Security Policy Index（**[SPI]**）を指定します。SPI は、OSPFv3 隣接の両端間で一致する必要があります。SPI 番号は 00000000 から FFFFFFFF までの 16 進数である必要があります。
3. **[プロトコル]** に **[AH]** を選択します。
4. **Crypto Algorithm (暗号化アルゴリズム)** を選択します。

   以下のアルゴリズムのいずれかを入力する必要があります。**SHA1**、**SHA256**、**SHA384**、**SHA512**、あるいは**MD5**。
5. **[キー]** の値を入力して確認します。
6. **OK** をクリックします。
7. Virtual Router - OSPF Auth Profile [仮想ルーター - OSPF - 認証プロファイル]ダイアログで再び **OK** をクリックします。

STEP 4 | OSPFv3 プロトコルの Areas (エリア) - Type (タイプ) を設定します。

1. **Areas (エリア)** タブで **Area ID (エリア ID)** を **Add (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。
2. **General (全般)** タブで、エリアの **Type (タイプ)** リストから以下のいずれかを選択します。
   - **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する場合、以下を設定します。
     - サマリーの受け入れ – Link State Advertisement（LSA）は他のエリアから受け入れられます。スタブ エリアのエリア ボーダー ルーター（ABR）インターフェイスでこのオプションが無効になっていると、OSPF エリアは Totally Stubby Area（TSA）として動作し、ABR はサマリー LSA を配信しません。
     - **Advertise Default Route** [デフォルト ルートの通知]– デフォルト ルート LSA は、設定された範囲（1 ～ 255）の設定されたメトリック値とともにスタブ エリアへの通知に含まれます。
   - **NSSA**（Not-So-Stubby Area） – ファイアウォールは、OSPF ルート以外のルートでのみエリアを出ることができます。選択した場合、**Stub**（スタブ） について説明したように **Accept Summary**（サマリーの受け入れ） および **Advertise Default Route**（デフォルト ルートの通知） を設定します。このオプションを選択する場合、以下を設定します。
     - **Type**（タイプ） – デフォルト LSA を通知する **Ext 1** または **Ext 2** ルート タイプを選択します。
     - **Ext Ranges (Ext 範囲)**–アドバタイズメントを有効化あるいは抑制したい外部ルートの範囲を **Add (追加)** します。

STEP 5 | OSPFv3 認証プロファイルをエリアまたはインターフェイスに関連付けます。

エリアに関連付けるには、以下の手順を実行します。

1. **Arias**（エリア） タブで、表から既存のエリアを選択します。
2. **General (全般)** タブで、**Authentication (認証)** リストから、以前に定義した **Authentication Profile (認証プロファイル)** を選択します。
3. **OK** をクリックします。

インターフェイスに関連付けるには、以下の手順を実行します。

1. **Arias**（エリア） タブで、表から既存のエリアを選択します。
2. **Interface (インターフェイス)** タブを選択し、OSPF インターフェイスに関連付ける認証プロファイルを **Auth Profile (認証プロファイル)** リストから **Add (追加)** します。
3. **OK** をクリックします。

STEP 6 | 再び **OK** をクリックしてエリア設定を保存します。

STEP 7 | （任意）エクスポート ルールを設定します。

1. OSPFv3 経由でデフォルト ルートを再配信するのを許可する場合は、**Export Rules (ルールのエクスポート)** タブで **Allow Redistribute Default Route (デフォルト ルートの再配信を許可)** を選択します。
2. **Add**（追加）をクリックします。
3. **Name (名前)** を入力します。値は、有効な IPv6 サブネットあるいは有効な再配信プロファイルの名前でなければなりませ。
4. **New Path Type (新規パス タイプ)**、**Ext 1** あるいは **Ext 2** を選択します。
5. 32 ビット値を持つ一致したルートの **New Tag (新規タグ)** を、ドット付きの 10 進表記で指定します。
6. 新しいルールに **Metric (メトリック)** を割り当てます（範囲は 1～16,777,215）。
7. **OK** をクリックします。

STEP 8 | 詳細な OSPFv3 オプションを設定します。

1. トランジット トラフィックの送受信に使用せずにファイアウォールを OSPF トポロジ配信に参加させる場合は、**Advanced**（詳細）タブで、**Disable Transit Routing for SPF Calculation**（SPF 計算用トランジット ルーティングを無効にする）を選択します。
2. 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タイマー（秒単位）として **SPF Calculation Delay (sec)**（**SPF** 計算遅延（秒）） の値を指定します。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、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。
3. **LSA Interval (sec) (LSA** 間隔 **(秒))** タイマーの値（秒単位）を設定します。このタイマーは、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。
4. （任意）OSPF グレースフル リスタートの設定を行います。
5. **OK** をクリックします。

STEP 9 | 変更を **Commit (コミット)** します。

OSPF グレースフル リスタートの設定

OSPF グレースフル リスタートにより、OSPF ネイバーは障害が発生した場合の短い移行中にファイアウォールを経由してルートを使用し続けます。この動作により、短期間のダウンタイム中に発生するおそれのあるルーティング テーブルの再設定および関連するルート フラッピングが少なくなるため、ネットワークの安定性が高まります。

Palo Alto Networks® ファイアウォールの OSPF グレースフル リスタートには、次の操作が含まれます。

- ファイアウォールがリスタートするデバイスの場合 – ファイアウォールが短期間ダウンする場合や短期間使用できなくなる場合は、グレース LSA をその OSPF ネイバーに送信します。ネイバーは、グレースフル リスタート ヘルパー モードで実行するように設定する必要があります。ヘルパー モードでは、ネイバーはファイアウォールが **Grace Period (**グレース ピリオド**)** として定義した指定された期間内にグレースフル リスタートを実行することを通知するグレース LSA を受信します。グレース ピリオド中、ネイバーはファイアウォール経由でルートを送受信し続け、ファイアウォール経由でルートを通知する LSA を送信し続けます。グレース ピリオドの失効前にファイアウォールが動作を再開すると、トラフィックの送受信はネットワーク障害が発生する前と同じように行われます。グレース ピリオドが失効した後もファイアウォールが動作を再開しない場合、ネイバーはヘルパー モードを終了し、ファイアウォールをバイパスするルーティング テーブルの再設定を伴う通常の動作を再開します。
- ファイアウォールがグレースフル リスタート ヘルパーになる場合–ファイアウォールがグレースフル リスタート ヘルパーになる場合 – 隣接するルートが短期間ダウンするおそれがある場合、ファイアウォールはグレースフル リスタート ヘルパー モードで動作するように設定できます。その場合、ファイアウォールは **Max Neighbor Restart Time (**ネイバー再起動の最大時間**)** を採用します。ファイアウォールがグレース LSA をその OSPF ネイバーから受信すると、グレース ピリオドまたはネイバー再起動の最大時間が経過するまで、トラフィックをネイバーにルーティングし続け、ネイバーを経由したルートを通知し続けます。ネイバーが復帰する前にどちら時間も経過しなければ、トラフィックの送受信はネットワーク障害が発生する前と同じように行われます。ネイバーが復帰する前にどちらかの期間が経過すると、ファイアウォールはヘルパー モードを終了し、ネイバーをバイパスするルーティング テーブルの再設定を伴う通常の動作を再開します。

STEP 1 | **Network (**ネットワーク**)** > **Virtual Routers (**仮想ルーター**)** の順に選択し、設定したい仮想ルーターを選択します。

STEP 2 | **OSPF** > **Advanced (**詳細**)** あるいは **OSPFv3** > **Advanced (**詳細**)** を選択します。

STEP 3 | 以下を選択していることを確認します（デフォルトでは有効になっています）。

- グレースフル リスタートを有効にする
- ヘルパー モードを有効にする
- 厳密な **LSA** チェックを有効化する

トポロジで必要がない限り、これらをオンのままにしておく必要があります。

STEP 4 | **[**グレース ピリオド**]** を秒単位で設定します。

STEP 5 | **Max Neighbor Restart Time**（ネイバー再起動の最大時間） を秒単位で設定します。

OSPF 動作の確認

OSPF 設定をコミットしたら、その OSPF が動作することを確認するために以下の操作を実行できます。

- ルーティング テーブルの表示
- OSPF 隣接の確認
- OSPF 接続の確立の確認

ルーティング テーブルの表示

ルーティング テーブルを表示することで、OSPF ルートが確立されたかどうかを確認できます。ルーティング テーブルは、Web インターフェイスまたは CLI からアクセスできます。CLI を使用する場合、以下のコマンドを使用します。

- **`show routing route`**
- **`show routing fib`**

Web インターフェイスを使用してルーティングテーブルを表示している場合、次の作業を行います。

STEP 1 | **Network (ネットワーク)** > **Virtual Routers (仮想ルーター)**More Runtime Stats (ランタイム状態の詳細) リンクをクリックします。

STEP 2 | **Routing (ルーティング)** > **Route Table (ルート テーブル)**タブを選択し、OSPF によって学習されたルートのルーティング テーブルの **Flags (フラグ** 列を調べます。

OSPF 隣接の確認

次の流れで、OSPFv3 隣接が構築されていることを確認します。

STEP 1 | **Network (ネットワーク)** > **Virtual Routers (仮想ルーター) More Runtime Stats (ランタイム状態の詳細)** リンクをクリックします。

STEP 2 | **OSPF** > **Neighbor (ネイバー)** の順に選択し、**Status (ステータス)** 列を調べて OSPF 隣接が確立されたかどうかを判断します。

OSPF 接続の確立の確認

システム ログを表示し、ファイアウォールが OSPF 接続を確立したことを確認します。

STEP 1 | **Monitor (監視)** > **System (システム)** の順に選択し、OSPF 隣接が確立されたことを確認するメッセージを探します。

STEP 2 | **OSPF** > **Neighbor (ネイバー)** の順に選択し、**Status (ステータス)** 列を調べて OSPF 隣接が確立された（フル）かどうかを判断します。

BGP

Border Gateway Protocol （BGP）は、インターネット ルーティング プロトコルの主流となっています。BGP は、AS （Autonomous System）内で使用可能な IP プレフィックスに基づいてネットワークが到達可能かどうかを判断します。AS とは、ネットワーク プロバイダによって指定された、同じルーティング ポリシーに属する IP プレフィックスのセットです。

BGP

BGP は AS 間（外部 BGP あるいは eBGP）または単一の AS（内部 BGP あるいは iBGP）内で機能し、BGP スピーカーとルーティングおよび到達可能情報を交換します。このファイアウォールでは、以下の機能を含む、完全な BGP 実装が可能です。

- 仮想ルーター毎に 1 つの BGP ルーティング インスタンスを指定
- 仮想ルーター毎の BGP 設定。これには、ローカル ルート ID やローカル AS などの基本パラメータと、パス選択、ルート リフレクタ、BGP コンフェデレーション、ルート フラップ、ダンペニングのプロファイルなどの詳細オプションがあります。
- ピア グループおよびネイバー設定。ネイバー アドレスやリモート AS に加え、ネイバー属性やネイバー接続などの高度なオプションが含まれます。
- ポリシーをルーティングしてルートのインポート、エクスポート、およびアドバタイズメントの制御、プレフィックスに基づいたフィルタリング、アドレス集約
- IGP と BGP の相互作用による、再配信プロファイルを使用した BGP へのルートの注入
- 認証プロファイル。BGP 接続のための MD5 認証キーを指定します。認証により、ルートのリークや DoS 攻撃が成功する可能性が低くなります。
- BGP ピアが更新パケット内で IPv6 ユニキャスト ルートおよび IPv4 マルチキャスト ルートを配送できるようにし、ファイアウォールおよび BGP ピアが IPv6 アドレスを使って互いに通信できるようにするマルチプロトコル BGP（MP-BGP）。
- BGP は、プレフィックスのAS_PATH リストで最大 255 個の AS 番号をサポートします。

MP-BGP

BGP は IPv4 ユニキャスト プレフィックスをサポートしていますが、IPv4 マルチキャスト ルートあるいは IPv6 ユニキャスト プレフィックスを使用する BGP ネットワークでは、IPv4 ユニキャスト以外のアドレス タイプのルートを交換するために、マルチプロトコル BGP（MP-BGP）が必要になります。MP-BGP は、MP-BGPが有効になっていなくても BGP ピアが運ぶことができる IPv4 ユニキャスト ルートに加え、BGP ピアが更新パケット内で IPv4 マルチキャスト ルートおよび IPv6 ユニキャスト ルートを運ぶことを許可します。

これにより、ネイティブ IPv6 あるいはデュアル スタック IPv4 および IPv6 を使用する BGP ネットワークに IPv6 で接続できるようになります。サービスプロバイダは顧客に IPv6 サービスを提供することができ、企業はサービスプロバイダの IPv6 サービスを使用できます。ファイアウォールおよび BGP ピアは IPv6 アドレスを使用して互いに通信できます。

BGP にマルチネットワーク レイヤー プロトコル（IPv4 用 BGP-4 を除く）をサポートさせるために、BGP-4 用のマルチプロトコル エクステンション（RFC 4760）はファイアウォールがBGP 更新パケットで送受信する Multiprotocol Reachable NLRI 属性内で Network Layer Reachability Information（NLRI）を使用します。この属性には、次の 2 つの識別子を含む、宛先プレフィックスに関する情報が含まれています。

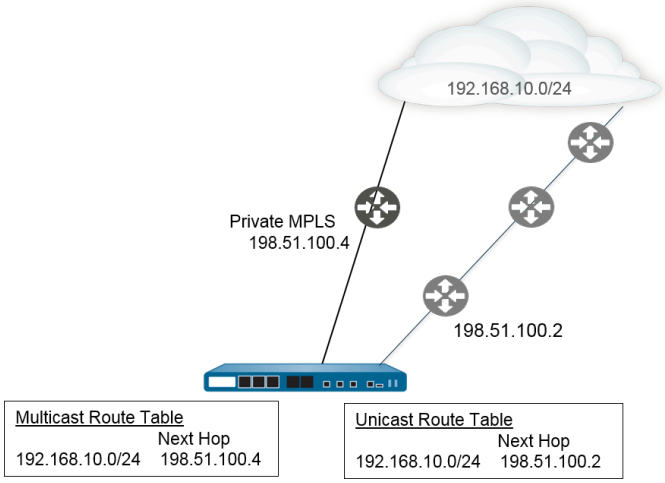
- アドレス ファミリー番号の IANA で定義されている通りの Address Family Identifier（AFI）、宛先プレフィックスが IPv4 あるいは IPv6 アドレスであることを示します。（PAN-OS は IPv4 および IPv6 AFIをサポートしています）
- PAN-OS の Subsequent Address Family Identifier（SAFI）は、宛先プレフィックスがユニキャストあるいはマルチキャスト アドレスである（AFI が IPv4 の場合）、あるいは宛先プレフィックスがユニキャスト アドレスである（AFI が IPv6 の場合）ことを示します。PAN-OS は IPv6 マルチキャストをサポートしていません。

IPv4 マルチキャスト用の MP-BGP を有効化する、あるいはマルチキャスト スタティックルートを設定する場合、ファイアウォールは静的ルート用に別々のユニキャストおよびマルチキャスト ルート テーブルをサポートします。同じ宛先に向かうユニキャストおよびマルチキャスト トラフィックを分離したい場合があります。例えばマルチキャスト トラフィックが重要であるため、マルチキャスト トラフィックはユニキャスト トラフィックとは別のパスを選択できます。そのため、ホップ数を減らしたり、遅延を少なくさせることで、それをもっと効率良くする必要があります。

また、BGP がルートのインポートおよびエクスポートを行う際、条件付きアドバタイズメントを送信する際、ルートの再配信あるいは集約を行う際に BGP がユニキャストあるいはマルチキャスト ルート テーブルのみ（あるいは両方）のルートを使用するように設定することで、BGP の機能の仕方をさらに制御できるようにすることもできます。

MP-BGP を有効化し、アドレス ファミリーとして IPv4 を、後続のアドレス ファミリーとしてマルチキャストを選択する、あるいはマルチキャスト ルート テーブルに IPv4 スタティックルートをインストールすることで、専用のマルチキャスト RIB（ルートテーブル）を使用するかどうか指定できます。マルチキャスト RIB を使用するためにこれらの方法のいずれかを実施した後、ファイアウォールはすべてのマルチキャスト ルーティングおよび reverse path forwarding（RPF）でマルチキャスト RIB を使用します。すべてのルーティング（ユニキャストおよびマルチキャスト）でユニキャスト RIB を使用したい場合、いずれの方法でもマルチキャスト RIB を有効化しないでください。

次の図はでは、192.168.10.0 へのスタティックルートがユニキャスト ルートテーブルにインストールされており、そのネクストホップが 198.51.100.2 です。しかし、マルチキャスト トラフィックはプライベート MPLS クラウドまでの別のパスを取ることができます。パスが異なるように、別のネクストホップ（198.51.100.4）を持つマルチキャスト ルート テーブルに同じスタティックルートがインストールされています。



別々のユニキャストおよびマルチキャスト ルート テーブルを使用することで、次の BGP 機能を設定する際の柔軟性および管理性が高まります。

- 前の例で示したとおりに、IPv4 スタティックルートをユニキャストあるいはマルチキャスト ルート テーブルに、あるいは両方にインストールします。（IPv6 スタティックルートはユニキャスト ルートテーブルにのみインストールできます）
- 一致基準にマッチするプレフィックスがすべてユニキャストあるいはマルチキャスト ルート テーブルに、あるいは両方にインポートされるよう、インポート ルールを作成します。
- 一致基準にマッチするプレフィックスがユニキャストあるいはマルチキャスト ルート テーブルから、あるいは両方からエクスポートされるよう、エクスポート ルールを作成します。
- 非存在フィルタを持つ条件付きアドバタイズメントを設定し、ファイアウォールがユニキャストあるいはマルチキャスト ルート テーブル（あるいは両方）を検索し、必ずルートがテーブル内に存在せず、ファイアウォールが別のルートをアドバタイズできるようにします。
- アドバタイズ フィルタを持つ条件付きアドバタイズメントを設定し、ファイアウォールがユニキャストあるいはマルチキャスト ルート テーブル、あるいは両方から一致基準にマッチするルートをアドバタイズするようにします。
- ユニキャストあるいはマルチキャスト ルート テーブル、あるいは両方にあるルートを再配信します。
- アドバタイズ フィルタを持つルート集約を設定し、アドバタイズする集約ルートがユニキャストあるいはマルチキャスト ルート テーブル、あるいは両方から来るようにします。
- 反対に、抑制フィルタを持つルート集約を設定し、抑制（アドバタイズしない）すべき集約ルートがユニキャストあるいはマルチキャスト ルート テーブル、あるいは両方から来るようにします。

IPv6 のアドレス ファミリーを使って MP-BGP を持つピアを設定する際、インポート ルール、エクスポート ルール、条件付きアドバタイズメント（アドバタイズ フィルタおよび非存在フィル

タ）および集約ルール（アドバタイズ フィルタ、抑制フィルタ、集約ルート属性）のネクスト ホップ フィールドおよびアドレス プレフィックスにある IPv6 アドレスを使用できます。

BGP の設定

BGP を設定するには、以下のタスクを実行します。

STEP 1 | 一般的な virtual router 設定を構成します。

STEP 2 | 仮想ルーター用の BGP を有効化し、ルーター IDを割り当て、仮想ルーターを AS に割り当てます。

1. **Network (ネットワーク)** > **Virtual Routers (仮想ルーター)** の順に選択し、さらに仮想ルーターを選択します。
2. **BGP** を選択します。
3. このVirtual Router (仮想ルーター - VR)用に BGP を **Enable**（有効化）する。
4. **Router ID (ルーター ID)** を仮想ルーター用の BGP に割り当てます（通常、ルーター ID が一意になるよう、IPv4 アドレスにします）。
5. **AS** 番号—ルーター ID に基づいて、Virtual Router (仮想ルーター - VR)が属する AS の番号を割り当てます（範囲は 1 ～ 4294967295 です）。
6. **OK** をクリックします。

STEP 3 | 全般的な BGP 設定を設定します。

1. **Network (ネットワーク)** > **Virtual Routers (仮想ルーター)** の順に選択し、さらに仮想ルーターを選択します。
2. **BGP** > **General** （全般） を選択します。
3. BGP ピアから通知されるデフォルト ルートを無視するには、**Reject Default Route**（デフォルト ルートの拒否）を選択します。
4. 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は、**Install Route**（ルートをインストール）を選択します。
5. 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、**Aggregate MED (集約 MED)** を選択します。
6. 異なるパスで設定を決定するために使用できる **Default Local Preference (デフォルトのローカル設定)** を指定します。
7. 相互運用性を確保するために **AS Format (AS 形式)** を選択します。
   - **2** バイト（デフォルト）
   - **4** バイト

   ランタイム統計は、RFC 5396 に従って *asplain* 表記を使用して *BGP 4*バイトの *AS* 番号を表示します。
8. **Path Selection (パス選択)** の以下のそれぞれの設定を有効化または無効化します。
   - 常に **MED** を比較 – 別の AS 内のネイバーから受け取ったパスを選択するには、この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には、この比較を有効にします。
9. **Auth Profiles (認証プロファイル)** については、認証プロファイルを **Add (追加)** 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。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。
10. **OK** を 2 回クリックします。

STEP 4 | （任意）BGP を設定します。

1. **Network (ネットワーク)** > **Virtual Routers (仮想ルーター)** の順に選択し、さらに仮想ルーターを選択します。
2. **BGP** > **Advanced (詳細)** を選択します。
3. 複数の BGP AS で ECMP を実行できるようにする場合は、**ECMP Multiple AS Support (ECMP マルチ AS サポート)** を選択します。
4. **Enforce First AS for EBGP**（最初の **AS** を **EBGP** に適用）（デフォルトで有効）により、AS_PATH 属性の最初の AS番号 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ファイアウォールがドロップするようにします。

5. **Graceful Restart (グレースフル リスタート)** を選択して次のタイマーを設定します。
   - **Stale Route Time (sec)**（接続期限切れルート時間（秒））—ルートが接続期限切れ状態を維持できる時間の長さを秒単位で指定します（範囲は 1 ～ 3,600、デフォルトは 120）。
   - ローカル再起動時間 **(秒)**—ローカル デバイスが再起動するために待機する時間の長さを秒単位で指定します。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 (sec)**（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受け入れ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）。
6. **Reflector Cluster ID**（リフレクタ クラスタ **ID**）の場合は、リフレクタ クラスタを示す IPv4 識別子を指定します。
7. **Confederation Member AS**（コンフェデレーション メンバー **AS**）の場合は、自律システム番号のID（サブ AS 番号とも呼ばれます）を指定します。これは BGP コンフェデレーション内でのみ表示されます。詳細は、「BGP コンフェデレーション」を参照してください。
8. 設定したいダンプ プロファイル毎に次の情報を **Add (追加)** し、**Enable (有効)** を選択して **OK** をクリックします。
   - **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。
   - **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)。この値を下回ると停止になったルートは再度使用されます。
   - **Max Hold Time (sec)**（最大ホールド タイム（秒））—どれだけ不安定であったかに関係なく、ルートを停止できる時間の最大長を秒単位で指定します（範囲は 0 ～ 3600、デフォルトは 900）。
   - **Decay Half Life Reachable (sec)**（**Decay Half Life** 到達可能（秒））—ルートが到達可能とみなされた場合、ルートの安定性メトリックを 1/2 にするまでの時間を秒単位で指定します（範囲は 0 ～ 3600、デフォルトは 300）。
   - **Decay Half Life Unreachable (sec)**（**Decay Half Life** 到達不可能（秒））—ルートが到達不可能とみなされた場合、ルートの安定性メトリックを 1/2 にするまでの時間を秒単位で指定します（範囲は 0 ～ 3600、デフォルトは 300）。
9. **OK** を 2 回クリックします。

STEP 5 | BGP ピア グループを設定します。

1. **Network (ネットワーク)** > **Virtual Routers (仮想ルーター)** の順に選択し、さらに仮想ルーターを選択します。
2. **BGP** > **Peer Group (ピア グループ)** を選択し、ピア グループの **Name (名前)** を **Add (追加)** して **Enable (有効)** を選択します。
3. 設定した集約済みコンフェデレーション AS へのパスを含めるには、**Aggregated Confed AS Path** [集約済みコンフェデレーション AS パス]を選択します。
4. 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には、**Soft Reset with Stored Info**[保存した情報を使用したソフト リセット] を選択します。
5. ピア グループの **Type (タイプ)** を選択します。
   - **IBGP** – **Export Next Hop (ネクスト ホップのエクスポート)**：**Original (元)** あるいは **Use self (自己使用)** を選択します。
   - **EBGP Confed (EBGP コンフェデレーション)** – **Export Next Hop (ネクスト ホップのエクスポート)**：**Original (元)** あるいは **Use self (自己使用)** を選択します。
   - **EBGP Confed (EBGP コンフェデレーション)** – **Export Next Hop (ネクスト ホップのエクスポート)**：**Original (元)** あるいは **Use self (自己使用)** を選択します。
   - **EBGP** – **Import Next Hop (ネクスト ホップのインポート)**：**Original (元)** あるいは **Use self (自己使用)**そして**Export Next Hop (ネクストホップのエクスポート)**を選択します。**[解決]** または **[自己の使用]** を指定します。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、**Remove Private AS (プライベート AS の削除)** を選択します。
6. **OK** をクリックします。

STEP 6 | ピア グループに属する BGP ピアを設定し、アドレス処理を指定します。

1. **Network (ネットワーク)** > **Virtual Routers (仮想ルーター)** の順に選択し、さらに仮想ルーターを選択します。
2. **BGP** > **Peer Group (ピア グループ)** を選択し、さらに作成したピア グループを選択します。
3. Peer (ピア) については、ピアを **Name (名前)** 毎に **Add (追加)** します。
4. ピアを **Enable**（有効）にします。
5. ピアの所属先となる **Peer AS (ピア AS)** を入力します。
6. **Addressing (アドレス処理)** を選択します。
7. **Local Address (ローカル アドレス)** については、BGP を設定している **Interface (インターフェイス)** 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、そのインターフェイスの BGP ピアになる IP アドレスを入力します。
8. **Peer Address (ピアのアドレス)** については、いずれかの **IP** を選択して IP アドレスを入力するか、アドレス オブジェクトを選択あるいは作成するか、**FQDN** を選択して FQDN 型のアドレス オブジェクトあるいは FQDN を入力します。

   ファイアウォールは *FQDN* の *DNS* 解決から得られた一つの *IP* アドレス *(IPv4* あるいは *IPv6* 系統それぞれ*)* のみを使用します。*DNS* 解決が複数のアドレスを返すと、ファイアウォールは *BGP* ピア用に設定された *IP* 系統 *(IPv4* あるいは *IPv6)* にマッチする、優先される *IP* アドレスを使用します。優先される *IP* アドレスは、*DNS* サーバーが初回の応答で返す最初のアドレスです。ファイアウォールは、順序に関わらずアドレスが後の応答に現れる限り、このアドレスを優先的に保持します。
9. **OK** をクリックします。

STEP 7 | BGP ピア用の接続設定を行います。

1. **Network (ネットワーク)** > **Virtual Routers (仮想ルーター)** の順に選択し、さらに仮想ルーターを選択します。
2. **BGP** > **Peer Group (ピア グループ)** を選択し、さらに作成したピア グループを選択します。
3. 設定した **Peer (ピア)** を選択します。
4. **Connection Options (接続オプション)** を選択します。
5. ピアノ **Auth Profile (認証プロファイル)** を選択します。
6. **Keep Alive Interval**（**sec**）（キープアライブ間隔（秒））– 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間隔（秒単位）を設定します（範囲は 0 ～ 1,200、デフォルトは 30）。
7. **Multi Hop (マルチホップ)**–IP ヘッダーのtime-to-live (Time-To-Live- TTL)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。

8. **Open Delay Time（sec）**（オープン遅延時間 **(秒)**）—TCPハンドシェイクと、ファイアウォールが最初に BGP Open メッセージを送信して BGP 接続を確立するまでの遅延時間（秒単位）を指定します（範囲は 0 ～ 240、デフォルトは 0）。
9. **Hold Time（sec）**（待機時間（秒））—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）。
10. **Idle Hold Time (sec)**（待機継続時間（秒））—ピアへの接続を再試行するまでの待機時間（秒単位）を指定します（範囲は 1 ～ 3,600、デフォルトは 15）。
11. **Min Route Advertisement Interval (sec)**（ルート アドバタイズメント最小間隔 **(秒)**）—ルートをアドバタイズしたりルートを撤回したりする BGP ピアに BGP スピーカー (ファイアウォール) が送信する、一続きの 2 つの更新メッセージ間の最小時間(秒単位)を指定します（範囲は 1 ～ 600、デフォルトは 30）。
12. **Incoming Connections (**インバウンド接続**)** については、**Remote Port (**リモート ポート**)** を入力し、**Allow (**許可**)** を選択してこのポートに向かうインバウンド トラフィックを許可します。
13. **Outgoing Connections (**アウトバウンド接続**)** については、**Local Port (**ポート**)** を入力し、**Allow (**許可**)** を選択してこのポートから出るアウトバウンド トラフィックを許可します。
14. **OK** をクリックします。

STEP 8 | ルート リフレクター クライアント、ピアリング タイプ、最大プレフィックス、双方向送信検出（BFD）の設定を持つ BGP ピアを設定します。

1. **Network (ネットワーク)** > **Virtual Routers (仮想ルーター)** の順に選択し、さらに仮想ルーターを選択します。
2. **BGP** > **Peer Group (ピア グループ)** を選択し、さらに作成したピア グループを選択します。
3. 設定した **Peer (ピア)** を選択します。
4. **Advanced** [詳細]を選択します。
5. **Reflector Client (リフレクタ クライアント)** については次のいずれかを選択します。
   - **non-client (非クライアント)**（デフォルト）—ピアはルート リフレクター クライアントではありません。
   - **client (クライアント)**—ピアはルート リフレクター クライアントです。
   - **meshed-client (メッシュ クライアント)**
6. **Peering Type (ピアリング タイプ)** については次のいずれかを選択します。
   - **Bilateral (双方向)**— 2 つの BGP ピアがピア接続を確立します。
   - **Unspecified (未指定)**（デフォルト）。
7. **Max Prefixes (最大プレフィックス)** については、サポートする IP プレフィックスの最大数（範囲は 1～100,000）を入力するか、**unlimited (無制限)** を選択します。
8. の **BFD** を有効化する場合は（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）、以下のうち一つを選択します。
   - **default (デフォルト)**—ピアはデフォルトの BFD 設定のみを使用します。
   - **Inherit-vr-global-setting (vr グローバル設定を継承)**（デフォルト）—仮想ルーター用の BGP のためにグローバルに選択してある BFD プロファイルをピアが継承します。
   - 設定したBFD プロファイル—BFD プロファイルの作成を参照してください。

   Disable BFD (BFD** 無効**) を選択し、*BGP* ピアの *BFD* を無効にします。
9. **OK** をクリックします。

STEP 9 | インポートおよびエクスポートのルールを設定します。

インポートおよびエクスポート ルールは、他のルーター間でルートをインポートおよびエクスポートするために使用されます（たとえば、Internet Service Provider (インターネット サービス プロバイダ - ISP)からのデフォルト ルートのインポート）。

1. **Import (インポート)** を選択し、**Rules (ルール)** フィールドに名前を **Add (追加)** し、インポート ルールを**Enable (有効化)** します。
2. ルートのインポート元になる **Peer Group (ピア グループ)** を **Add (追加)** します。
3. **Match**（一致）を選択し、ルーティング情報をフィルタリングするために使用するオプションを定義します。ルート フィルタリングのためにルーターまたはサブネットへ

の MED （Multi-Exit Discriminator）値とネクスト ホップ値を定義することもできます。MED オプションは、ネイバーに AS への優先パスを知らせるための外部メトリックです。低い値が高い値に優先されます。

4. **Action**（アクション）を選択し、**Match**（一致）タブで定義したフィルタリング オプションに基づいて行うべきアクション（許可/拒否）を定義します。**Deny**（拒否）を選択した場合、追加のオプションを定義する必要はありません。**Allow**（許可）を選択した場合、他の属性を定義します。
5. **Export**（エクスポート）を選択してエクスポート属性を定義します。これは **Import**（インポート）設定に似ていますが、ファイアウォールからネイバーにエクスポートされるルート情報を制御するために使用されます。
6. **OK** をクリックします。

STEP 10 | 条件付き通知機能を設定します。これにより、ピアリングまたは到達の失敗を示し、ローカル BGP ルーティング テーブル（LocRIB）で異なる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。

1. **Conditional Adv**（条件付き通知）を選択し、**Policy**（ポリシー）名を**Add**（追加）します。
2. 条件付き通知を**Enable**（有効化）します。
3. **Used By (**使用者**)** セクションにおいて、条件付き通知ポリシーを使用するピア グループを **Add (**追加**)** します。
4. **Non Exist Filter**（非存在フィルタ）を選択し、優先ルートのネットワーク プレフィックスを定義します。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、通知が抑制されます。
5. **Advertise Filters**（フィルタの通知）を選択し、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定義します。プレフィックスが通知されようとするときに非存在フィルタと一致しないと、通知が行われます。
6. **OK** をクリックします。

STEP 11 | BGP 設定にルートを集約するために集約オプションを設定します。

BGP ルート集約は、BGP がアドレスを集約する方法を制御するために使用されます。テーブルの各エントリにより、1つの集約アドレスが作成されます。これにより、指定したアドレス

に一致する少なくとも 1 つの特定のルートが学習された場合に、ルーティング テーブルの集約エントリになります。

1. **Aggregate (**集約**)**を選択し、集約アドレスの名前を **Add (**追加**)** します。
2. 集約されたプレフィックスのプライマリ プレフィックスになるネットワーク **Prefix**（プレフィックス）を入力します。
3. **Suppress Filters**（フィルタの抑制）を選択し、一致したルートを抑制する属性を定義します。
4. **Advertise Filters**（フィルタの通知）を選択し、一致したルートを必ずピアに通知する属性を定義します。
5. **OK** をクリックします。

STEP 12 | 再配信ルールを設定します。

このルールは、ホスト ルートおよびローカル RIB にない不明なルートをピア ルーターに再配信するために使用されます。

1. **Redist Rules**（ルールの再配信）を選択し、新しい再配信ルールを**Add**（追加）します。
2. IP サブネットの**Name**（名前）を入力するか、再配信プロファイルを選択します。また、必要に応じて新しい再配信プロファイルを設定することもできます。
3. ルールを **Enable (**有効**)** にします。
4. ルールに使用されるルート **Metric**（メトリック）を入力します。
5. **Set Origin (**発信元の設定**)** リストから **incomplete (**不完全**)**、**igp**、または **egp** を選択します。
6. （任意）MED、ローカル設定、AS パス制限、コミュニティの値を指定します。
7. **OK** をクリックします。

STEP 13 | 変更を **Commit (**コミット**)** します。

IPv4 あるいは IPv6 ユニキャスト用に MP-BGP を持つ BGP ピアを設定

BGP の設定を行った後、次のいずれかの状況においては、IPv4 あるいは IPv6 ユニキャスト用に MP-BGP を持つ BGP ピア を設定します。

- BGP ピアに IPv6 ユニキャスト ルートを持たせるために、Address Family Type (アドレス ファミリー タイプ) が **IPv6** であり、Subsequent Address Family (サブネット アドレス ファミリー) が **Unicast (ユニキャスト)** である MP-BGPを設定し、IPv6 ユニキャスト ルートを含む BGP 更新をピアが送信できるようにします。BGP ピアリング（Local Address (ローカル アドレス) および Peer Address (ピアのアドレス)）は、どちらも IPv4 アドレスのままにするか、どちらも IPv6 アドレスにすることができます。
- IPv6 アドレスを介して BGP ピアリングを行うため（**Local Address (ローカル アドレス)** および **Peer Address (ピアのアドレス)** が IPv6 アドレスを使用）。

次のタスクは、MP-BGP を持つ BGP ピアを有効化し、ピアが IPv6 ユニキャスト ルートを持ち、IPv6 アドレスを使ってピアリングできるようにする方法を示しています。

また、このタスクは、ユニキャストあるいはマルチキャスト ルート テーブルを表示する方法、転送テーブル、BGP ローカル RIB、BGP RIB Out（ネイバーに送信されるルート）を表示し、ユニキャストあるいはマルチキャスト ルート テーブルあるいは特定のアドレス ファミリー（IPv4 あるいは IPv6）からのルートを確認する方法も示しています。

STEP 1 | ピア用の MP-BGP 拡張を有効化します。

次の設定を行い、BGP ピアが更新パケット内の IPv4 あるいは IPv6 ユニキャスト ルートを持ち、ファイアウォールが IPv4 あるいは IPv6 アドレスを使用して自身のピアと通信できるようにします。

1. **Network (**ネットワーク**)** > **Virtual Routers (**仮想ルーター**)** の順に選択し、設定中の仮想ルーターを選択します。
2. **BGP** を選択します。
3. **Peer Group (**ピア グループ**)** を選択し、ピア グループを一つ選びます。
4. BGP ピア（ルーター）を選択します。
5. **Addressing (**アドレス処理**)** を選択します。
6. そのピアが対象となる **Enable MP-BGP Extensions (MP-BGP** 拡張の有効化**)** を選択します。
7. **Address Family Type (**アドレス ファミリーの種類**)** については **IPv4** あるいは **IPv6** を選択します。例えば、IPv6 を選択します。
8. **Subsequent Address Family (**後続のアドレス ファミリー**)** については、**Unicast (**ユニキャスト**)** が選択されています。Address Family (アドレス ファミリー) で **IPv4** を選んだ場合、**Multicast (**マルチキャスト**)** も選択できます。
9. **Local Address (**ローカル アドレス**)** については **Interface (**インターフェイス**)** を選択し、任意で **IP** アドレスを選択します（2001:DB8:55::/32 など）。
10. **Peer Address (**ピアのアドレス**)** については、Local Address (ローカル アドレス) と同じアドレス ファミリー（IPv4 あるいは IPv6）を使用し、ピアの **IP** アドレスを入力します（例えば 2001:DB8:58::/32）。
11. **Advanced** [詳細]を選択します。
12. （任意）**Enable Sender Side Loop Detection (**送信側ループ検出の有効化**)** を行います。送信側ループ検出を有効化すると、ファイアウォールで更新でルートを送信する前に FIB のルートの AS_PATH 属性をチェックし、ピア AS 番号が AS_PATH リストにないことを確認できます。リストにある場合、ファイアウォールで削除してループを回避できます。
13. **OK** をクリックします。

STEP 2 | （任意）ルートはユニキャストの用途でしか使用しないため、スタティックルートを作成し、ユニキャスト ルートテーブルにインストールします。

1. **Network (ネットワーク)** > **Virtual Routers (仮想ルーター)** の順に選択し、設定中の仮想ルーターを選択します。
2. **Static Routes (静的ルート)** を選択し、**IPv4** あるいは **IPv6** を選択してルートを **Add (追加)** 追加します。
3. スタティックルートの **Name (名前)** を入力します。
4. IPv4 と IPv6 のどちらを選択するかに応じて、IPv4 あるいは IPv6 の **Destination (宛先)** プレフィックスおよびネットマスクを入力します。
5. 出力 **Interface (インターフェイス)** を選択します。
6. **Next Hop (ネクストホップ)** で **IPv6 Address (IPv6 アドレス)**（あるいは IPv4 を選ぶ場合は **IP Address (IP アドレス)**）を選択し、このスタティックルートにおいてユニキャスト トラフィックの宛先にしたいネクストホップのアドレスを入力します。
7. **Admin Distance (管理距離)** を入力します。
8. **Metric (メトリック)** を入力します。
9. **Route Table (ルート テーブル)** については **Unicast (ユニキャスト)** を選択します。
10. **OK** をクリックします。

STEP 3 | 設定をコミットします。

Commit（コミット）をクリックします。

STEP 4 | ユニキャストあるいはマルチキャスト ルート テーブルを表示します。

1. Select **Network (ネットワーク)** > **Virtual Routers (仮想ルーター)**。
2. 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。
3. **Routing (ルーティング)** > **Route Table (ルート テーブル)** を選択します。
4. **Route Table (ルート テーブル)** については **Unicast (ユニキャスト)** あるいは **Multicast (マルチキャスト)** を選択し、これらのルートだけを表示します。
5. **Display Address Family (アドレス ファミリーの表示)** については、**IPv4 Only (IPv4 のみ)**、**IPv6 Only (IPv6 のみ)**、あるいは **IPv4 and IPv6 (IPv4 および IPv6)** を選択し、そのアドレス ファミリーに対してこれらのルートだけを表示します。

   IPv6 Only (IPv6 のみ) と共に ***Multicast (マルチキャスト)*** を選択することはできません。

STEP 5 | 転送テーブルを表示します。

1. Select **Network (ネットワーク)** > **Virtual Routers (仮想ルーター)**。
2. 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。
3. **Routing (ルーティング)** > **Forwarding Table (転送テーブル)** を選択します。
4. **Display Address Family (アドレス ファミリーの表示)** については、**IPv4 Only (IPv4 のみ)**、**IPv6 Only (IPv6 のみ)**、あるいは **IPv4 and IPv6 (IPv4 および IPv6)** を選択し、そのアドレス ファミリーに対してこれらのルートだけを表示します。

STEP 6 | BGP RIB テーブルを表示します。

1. BGP パケットをルーティングするためにファイアウォールが使用する BGP ルートを確認できる、BGP ローカル RIB を表示します。
   1. Select **Network (ネットワーク)** > **Virtual Routers (仮想ルーター)**。
   2. 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。
   3. **BGP** > **Local RIB (ローカル RIB)** を選択します。
   4. **Route Table (ルート テーブル)** については **Unicast (ユニキャスト)** あるいは **Multicast (マルチキャスト)** を選択し、これらのルートだけを表示します。
   5. **Display Address Family (アドレス ファミリーの表示)** については、**IPv4 Only (IPv4 のみ)**、**IPv6 Only (IPv6 のみ)**、あるいは **IPv4 and IPv6 (IPv4 および IPv6)** を選択し、そのアドレス ファミリーに対してこれらのルートだけを表示します。

      IPv6 Only (IPv6 のみ) と共に ***Multicast (マルチキャスト)*** を選択することはできません。
2. ファイアウォールが BGP ネイバーに送信するルートを確認できる、BGP RIB Out テーブルを表示します。
   1. Select **Network (ネットワーク)** > **Virtual Routers (仮想ルーター)**。
   2. 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。
   3. **BGP** > **RIB Out (RIB アウト)** を選択します。
   4. **Route Table (ルート テーブル)** については **Unicast (ユニキャスト)** あるいは **Multicast (マルチキャスト)** を選択し、これらのルートだけを表示します。
   5. **Display Address Family (アドレス ファミリーの表示)** については、**IPv4 Only (IPv4 のみ)**、**IPv6 Only (IPv6 のみ)**、あるいは **IPv4 and IPv6 (IPv4 および IPv6)** を選択し、そのアドレス ファミリーに対してこれらのルートだけを表示します。

      IPv6 Only (IPv6 のみ) と共に ***Multicast (マルチキャスト)*** を選択することはできません。

IPv4 マルチキャスト用に MP-BGP を持つ BGP ピアを設定

BGP ピアに BGP 更新に含まれる IPv4 マルチキャスト ルートを学習・引き渡しさせたい場合、BGP の設定を行った後、IPv4 マルチキャスト用に MP-BGP を持つ BGP ピアを設定します。マルチキャスト トラフィックからユニキャストを分離する、あるいはMP-BGP に列挙されている各機能を採用することで、ユニキャストあるいはマルチキャスト ルート テーブル、あるいは両方のテーブルのルートのみを使用することができます。

マルチキャスト トラフィックのみをサポートしたい場合、フィルターを使用してユニキャスト トラフィックを取り除く必要があります。

ファイアウォールはマルチキャスト トラフィック用の ECMP をサポートしていません。

STEP 1 | BGP ピアが IPv4 マルチキャスト ルートを交換できるよう、MP-BGP 拡張を有効化します。

1. **Network (ネットワーク)** > **Virtual Routers (仮想ルーター)** の順に選択し、設定中の仮想ルーターを選択します。
2. **BGP** を選択します。
3. **Peer Group (ピア グループ)** を選択し、ピア グループおよび BGP ピアを選択します。
4. **Addressing (アドレス処理)** を選択します。
5. **Enable MP-BGP Extensions (MP-BGP 拡張の有効化)** を選択します。
6. **Address Family Type (アドレス ファミリーの種類)** については **IPv4** を選択します。
7. For **Subsequent Address Family (後続のアドレス ファミリー)** については、**Unicast (ユニキャスト)** を選択してから **Multicast (マルチキャスト)** を選択します。
8. **OK** をクリックします。

STEP 2 | （任意）IPv4 スタティックルートを作成し、それをマルチキャスト ルート テーブルのみにインストールします。

MP-BGP のトポロジーに記載されているように、BGP ピア用のマルチキャスト トラフィックを特定のネクストホップに向けたい場合にこれを行うことになります。

1. **Network (ネットワーク)** > **Virtual Routers (仮想ルーター)** の順に選択し、設定中の仮想ルーターを選択します。
2. **Static Routes (静的ルート)** > **IPv4** を選択し、ルートの **Name (名前)** を **Add (追加)** します。
3. IPv4 **Destination (宛先)** プレフィックスおよびネットマスクを入力します。
4. 出力 **Interface (インターフェイス)** を選択します。
5. **IP Address (IP アドレス)** として **Next Hop (ネクストホップ)** を選択し、このスタティックルートにおいてマルチキャスト トラフィックの宛先にしたいネクストホップの IP アドレスを入力します。
6. **Admin Distance (管理距離)** を入力します。
7. **Metric (メトリック)** を入力します。
8. **Route Table (ルート テーブル)** については **Multicast (マルチキャスト)** を選択します。
9. **OK** をクリックします。

STEP 3 | 設定をコミットします。

Commit（コミット）をクリックします。

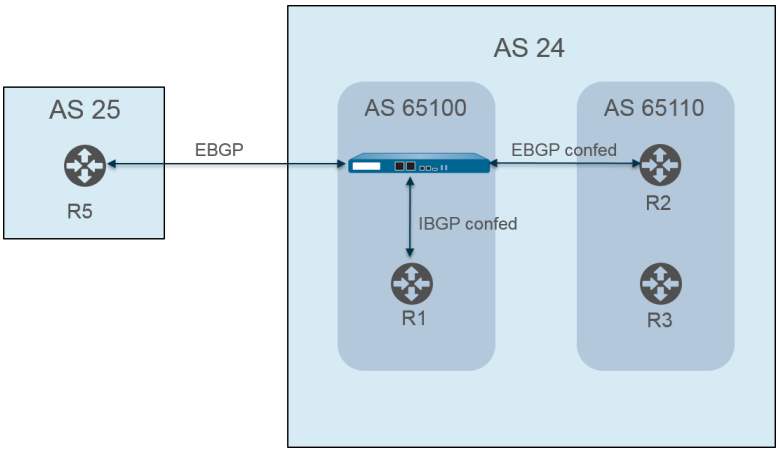
STEP 4 | ルートテーブルを表示します。

1. Select **Network (ネットワーク)** > **Virtual Routers (仮想ルーター)**。
2. 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。
3. **Routing (ルーティング)** > **Route Table (ルート テーブル)** を選択します。
4. **Route Table (ルート テーブル)** については **Unicast (ユニキャスト)** あるいは **Multicast (マルチキャスト)** を選択し、これらのルートだけを表示します。
5. **Display Address Family (アドレス ファミリーの表示)** については、**IPv4 Only (IPv4 のみ)**、**IPv6 Only (IPv6 のみ)**、あるいは **IPv4 and IPv6 (IPv4 および IPv6)** を選択し、そのアドレス ファミリーに対してこれらのルートだけを表示します。

STEP 5 | 転送テーブル、BGP ローカル RIB、あるいは BGP RIB Out テーブルを表示するには、IPv4 あるいは IPv6 ユニキャスト用 MP-BGP を使って BGP ピアを設定を参照してください。

BGP コンフェデレーション

BGP コンフェデレーションは、自律システム（AS）を 2 つ以上の副自律システム（サブ AS）に分割して、IBGP のフル メッシュ要件が引き起こす負担を軽減する方法を提供します。サブ AS 内のファイアウォール（または他のルーティング デバイス）は、同じサブ AS 内の他のファイアウォールと完全な iBGP メッシュもなければなりません。メイン AS 内で完全に接続するには、サブ自律システム間で BGP ピアリングが必要です。サブ AS 内で相互にピアリングするファイアウォールは、IBGP コンフェデレーション ピアリングを形成します。あるサブ AS 内のファイアウォールが、異なるサブ AS 内のファイアウォールを使用してピアリングし、EBGP コンフェデレーション ピアリングを形成します。接続する異なる自律システムからの 2 つのファイアウォールは、EBGP ピアです。

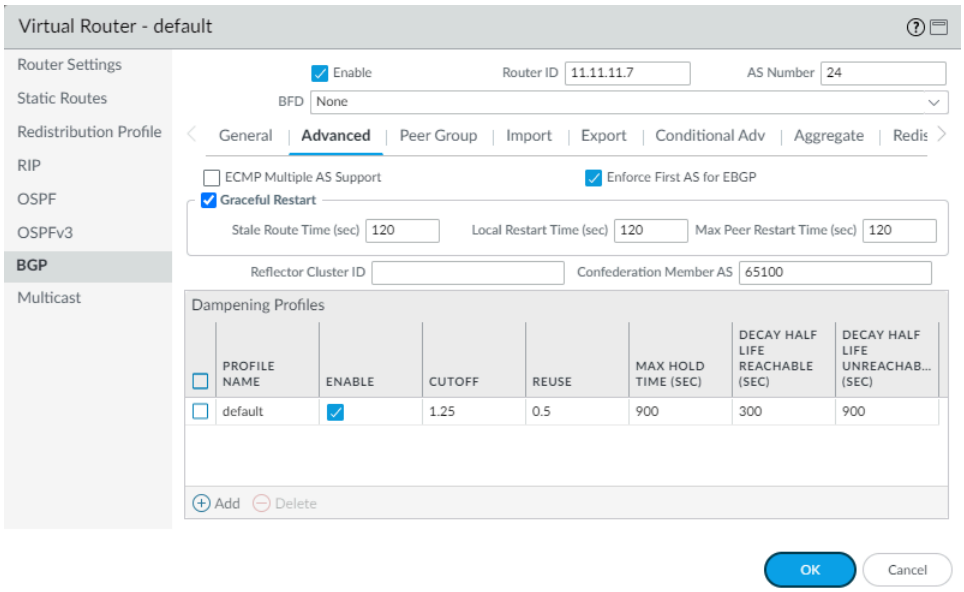


自律システムは、前の図の AS 24とAS 25 などのパブリック（グローバルに割り当てられる）AS 番号で識別されます。PAN-OS 環境では、各サブ AS に固有のコンフェデレーション メンバー AS 番号を割り当てます。これは、AS 内でのみ表示されるプライベート番号です。この図では、コンフェデレーションは AS 65100 と AS 65110 です。（RFC6996、私的使用のための自律システム（AS）予約）は、IANA が私的使用のために AS 番号 64512-65534 を予約していることを示しています。

サブ AS コンフェデレーションは、AS 内の互いに完全な自律システムのように見えます。ただし、ファイアウォールが AS パスを EBGP ピアに送信すると、パブリック AS 番号だけが AS パスに表示されます。プライベートサブ AS（連盟メンバー AS）番号は含まれません。

BGP ピアリングは、ファイアウォールと R2 の間で行われます。図のファイアウォールには、次の関連する設定があります。

- AS 番号—24
- コンフェデレーション メンバー AS—65100
- ピアリング タイプ—EBGP コンフェデレーション
- ピア AS—65110



AS 65110 のルータ 2（R2）は、次のように設定されています：

- AS 番号—24
- コンフェデレーション メンバー AS—65110
- ピアリング タイプ—EBGP コンフェデレーション
- ピア AS—6500

ファイアウォールと R1 の間で BGP ピアリングも発生します。ファイアウォールには次の追加設定があります：

- AS 番号—24
- コンフェデレーション メンバー AS—65100
- ピアリング タイプ—IBGP コンフェデレーション
- ピア AS—65110

R1 は次のように設定されています。

- AS 番号—24
- コンフェデレーション メンバー AS—65110
- ピアリング タイプ—IBGP コンフェデレーション
- ピア AS—6500

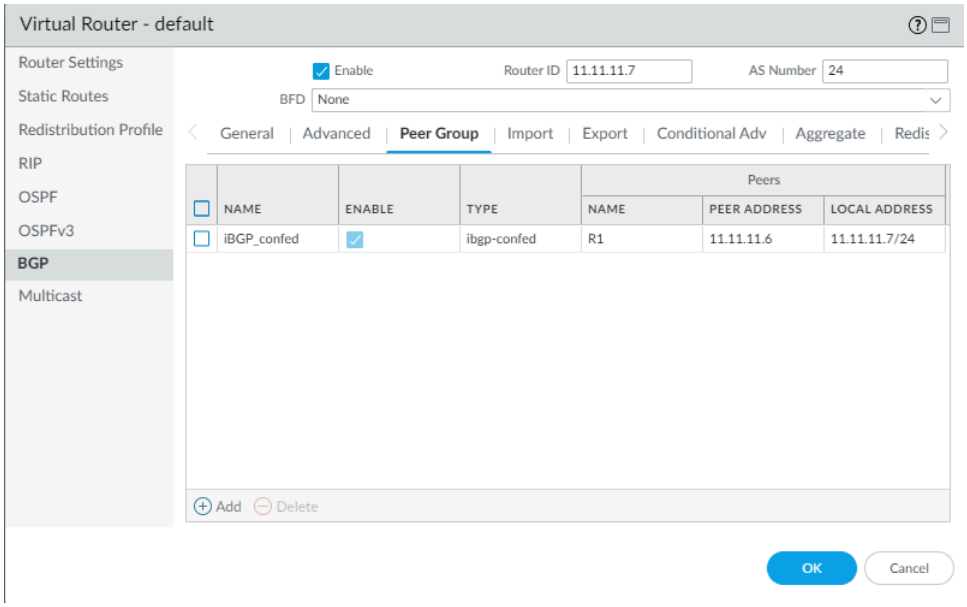
ファイアウォールと R5 の間で BGP ピアリングが発生します。ファイアウォールには次の追加設定があります：

- AS 番号—24
- コンフェデレーション メンバー AS—65100
- ピアリング タイプ—EBGP
- ピア AS—25

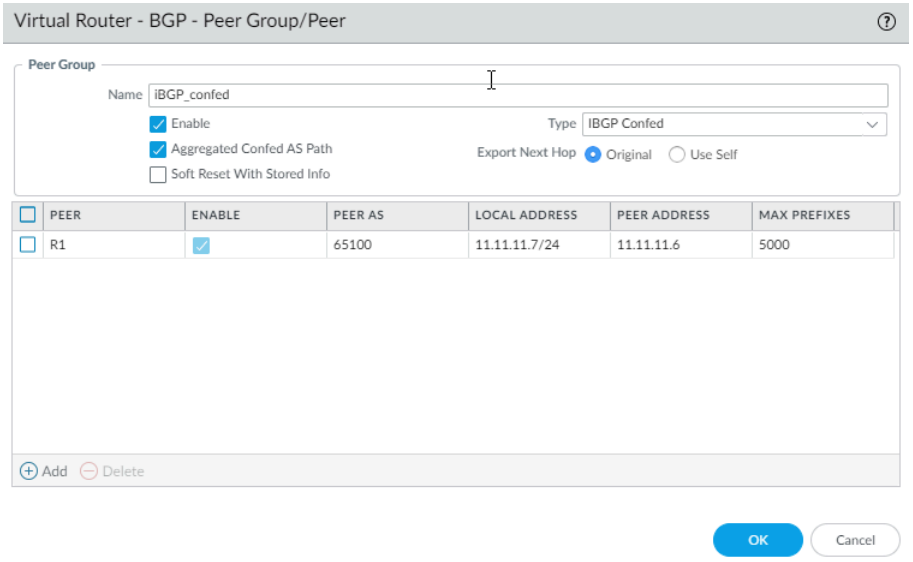
R5 は次のように設定されています。

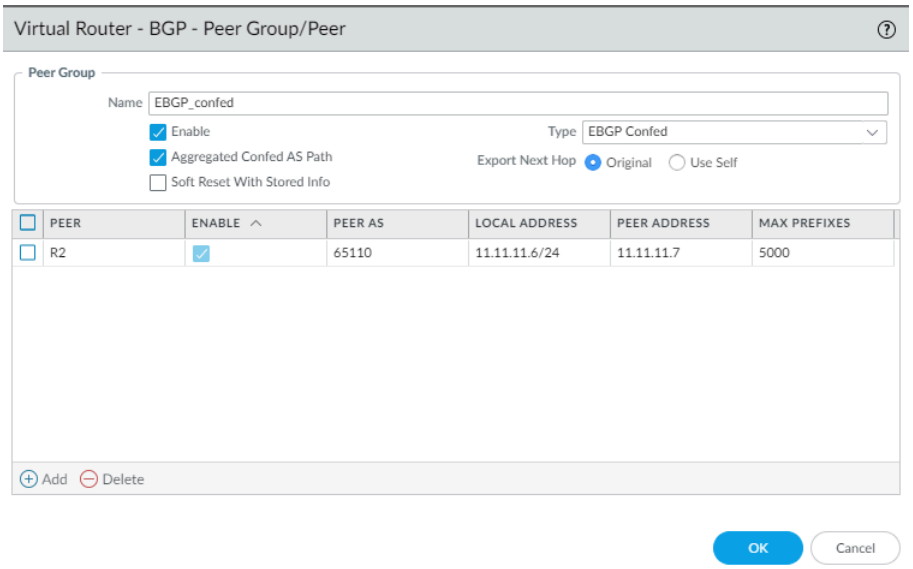
- AS—25
- ピアリング タイプ—EBGP
- ピア AS—24

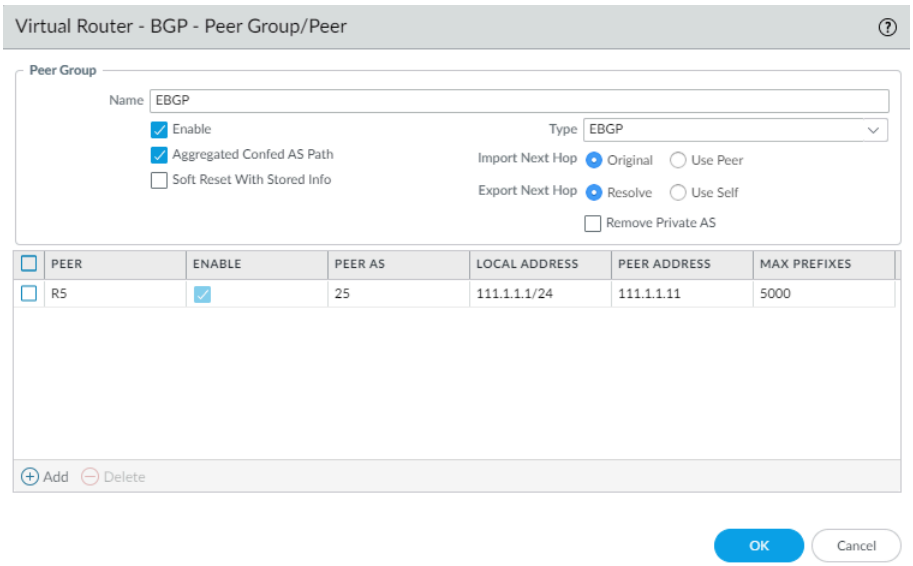
ファイアウォールが R1、R2、および R5 とピアツーピアするように設定された後、そのピアは**Peer Group**（ピア グループ）タブに表示されます。



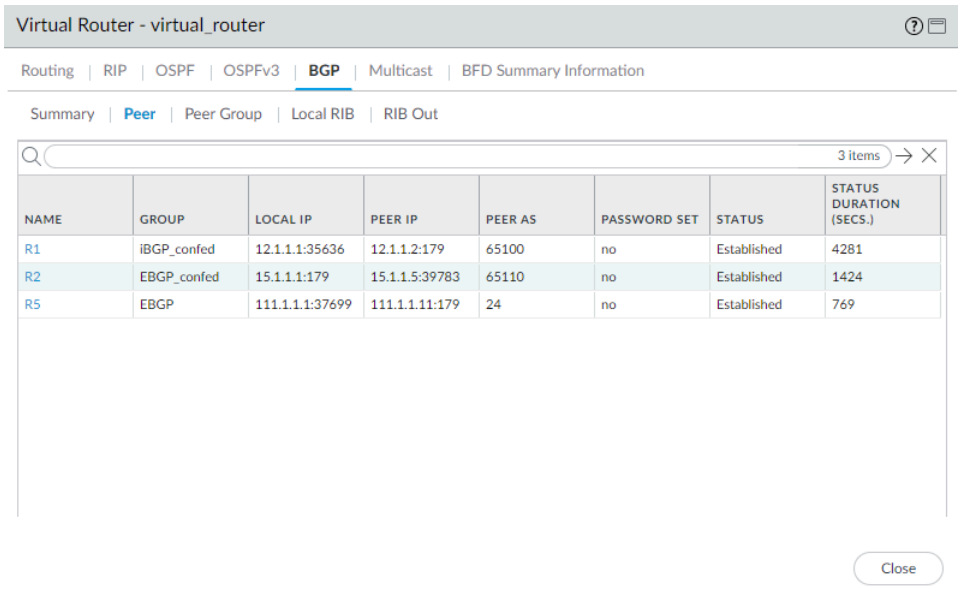
ファイアウォールには、R1、R2、および R5 ピアが表示されます。



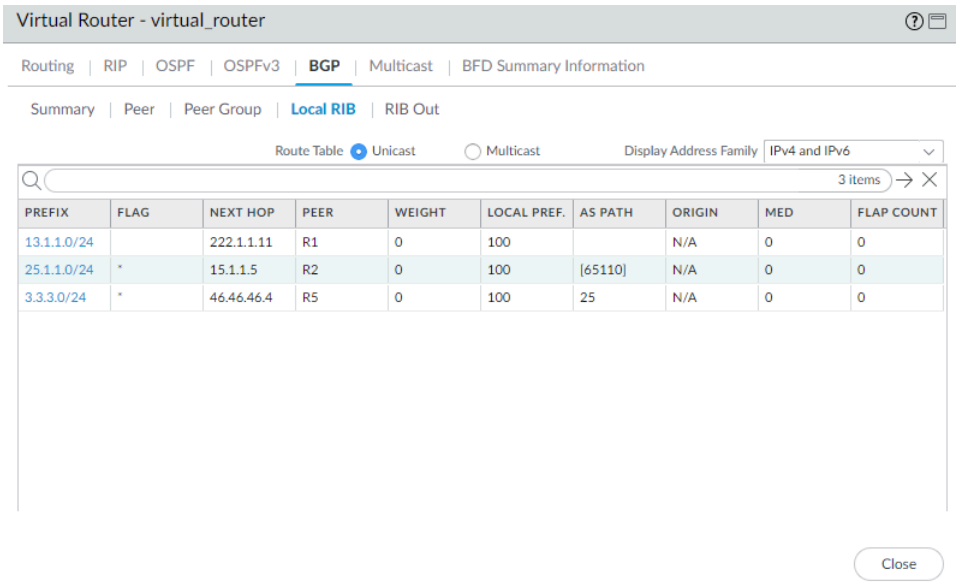




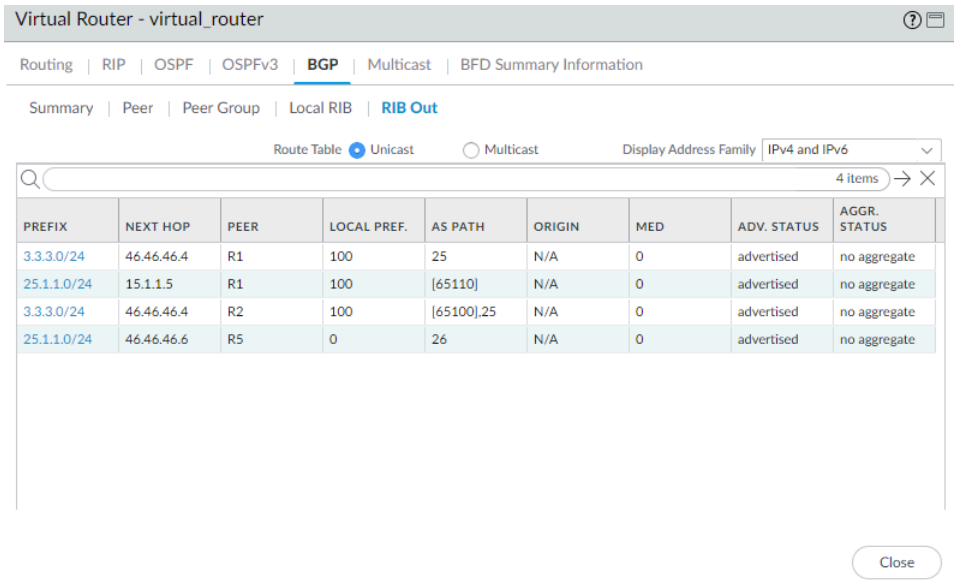
ファイアウォールからピアへのルートが確立されていることを確認するには、仮想ルータの画面で**More Runtime Stats**（その他のランタイム統計）を選択し、 **Peer**（ピア）タブを選択します。



ルート情報ベース（RIB）に保存されているルートに関する情報を表示するには、 **Local RIB**（ローカル **RIB**）タブを選択します。



次に、 **RIB Out**（**RIB** アウト）タブを選択します。



IP マルチキャスト

IP マルチキャストは、マルチキャスト IP データグラムを関連する受信者のグループに送信するためにネットワーク アプライアンスが使用する一連のプロトコルです。トラフィックを複数の受信者にユニキャストするのではなく、一度の送信で行うため、帯域幅を節約できます。単一のソース（あるいは多くのソース）から多くの受信者に通信する IP マルチキャストは、音声、動画、ストリーミング、IPTV、ビデオ会議、そしてニュースや経済データのような他の情報を配信するのに適しています。

マルチキャスト アドレスは、対象のアドレスに向かうトラフィックを受信したい受信者のグループを識別します。範囲 224.0.0.0～224.0.0.255、239.0.0.0～239.255.255.255 など、特別な用途のために予約されているマルチキャスト アドレスは使用しないでください。マルチキャスト トラフィックは UDP を使用するため、紛失したパケットを再送信しません。

Palo Alto Networks® のファイアウォールは、ファイアウォール上の仮想ルーター用に構成する、レイヤー 3 インターフェイス上の Protocol Independent Multicast（PIM）および IP マルチキャストをサポートしています。

マルチキャスト ルーティングの場合、レイヤー 3 インターフェイスのタイプはイーサネット、集約イーサネット（AE）、VLAN、ループバック、あるいはトンネルになります。インターフェイス グループを使えば、同じ Internet Group Management Protocol（IGMP）および PIM パラメーター、同じグループ権限（任意のソースから、あるいは特定のソースからのみトラフィックを許可するマルチキャスト グループ）を持つ複数のファイアウォールのインターフェイスを一度に構成できます。インターフェイスは、1 つのインターフェイス グループにのみ属することができます。

ファイアウォールは IPv4 マルチキャストをサポートしています。IPv6 マルチキャストはサポートしていません。また、ファイアウォールは PIM Dense Mode（PIM-DM）、IGMP プロキシ、IGMP 静的ジョイン、Anycast RP、GRE、レイヤー 2 上のマルチキャスト構成、バーチャル ワイヤ インターフェイス タイプもサポートしていません。しかし、バーチャル ワイヤ インターフェイスはマルチキャスト パケットを通過させることができます。また、レイヤー 2 インターフェイスは異なる VLAN 間でレイヤー 3 IPv4 マルチキャストを切り替えられます。ファイアウォールは出力インターフェイスの VLAN ID を使って VLAN ID をタグ付けし直します。

インターフェイスがマルチキャスト パケットを受信あるいは転送できるようにするために、仮想ルーターについてはマルチキャストを、入力および出力インターフェイスについては PIM を有効化する必要があります。PIM に加え、受信者に面した出力インターフェイス上で IGMP を有効化する必要もあります。**multicast (**マルチキャスト**)**という名前の事前定義済みのレイヤー 3 宛先ゾーンあるいは**any (**すべて**)**の宛先ゾーンに向かう IP マルチキャスト トラフィックを許可するために、セキュリティポリシー ルールを設定する必要があります。

IGMP

インターネット グループ管理プロトコル（IGMP）とは、Palo Alto Networks® のファイアウォール上のインターフェイスと通信するためにマルチキャスト レシーバーが使用する、またマルチキャスト グループのメンバーを追跡するためにファイアウォールが使用する、IPv4 プロトコルのことです。ホストがマルチキャスト トラフィックを受信したい際、IGMP の実装が IGMP メンバーシップ レポート メッセージを送信し、それを受信したルーターが次に、ホストが参加したいグループのマルチキャスト グループのアドレスに PIM ジョイン メッセージを送信します。その後、同じ物理ネットワーク（イーサネット セグメントなど）上にある IGMP が有効なルーターが PIM を使用して他の PIM が有効なルーターと通信士、ソースから対象のレシーバーへのパスを判断します。

IGMP はマルチキャスト レシーバーに面しているインターフェイス上でのみ有効化してください。レシーバーにできるのは、仮想ルーターから離れる単一のレイヤー 3 ホップだけです。IGMP メッセージは 1 の値の TTL 値を持つレイヤー 2 メッセージであるため、LAN の外に出ることはできません。

IP マルチキャストの設定を行う際、インターフェイスがIGMP バージョン 1、IGMP バージョン 2、IGMP バージョン 3のいずれを使用するのか指定します。IP ルーター アラート オプション、RFC 2113を適用し、IGMPv2 あるいは IGMPv3 を使用するインバウンドの IGMP パケットに IP ルーター アラート オプションを持たせることができます。

デフォルト設定では、インターフェイスはすべてのマルチキャスト グループについて IGMP メンバーシップ レポートを受け取ります。マルチキャスト グループの権限を設定し、仮想ルーターが任意のソース（Any-Source Multicast、つまり ASM）からメンバーシップ レポートを受け取るグループを制御することができます。通常、これは PIM スパース モード（PIM-SM）になります。また、仮想ルーターが特定のソース（PIM Source-Specific Multicast [PIM-SSM]）からメンバーシップ レポートを受け取るグループを指定することもできます。ASM あるいは SSM グループのいずれかの権限を指定すると、仮想ルーターは他のグループからのメンバーシップ レポートを拒否するようになります。インターフェイスは IGMPv3 を使って PIM-SSM トラフィックを通過させる必要があります。

単一のインターフェイスで IGMP が同時に処理できるソースの最大数およびマルチキャスト グループの最大数を指定できます。

仮想ルーターは定期的にマルチキャスト グループのすべてのレシーバーに対して IGMP クエリをマルチキャストします。レシーバーは、対象のグループのマルチキャストをまだ受信したいということを知らせる IGMP メンバーシップ レポートで、IGMP クエリに応答します。仮想ルーターはレシーバーを持つマルチキャスト グループのテーブルを管理します。仮想ルーターは、マルチキャスト配信ツリーがグループに参加しているレシーバーがまだ存在する場合のみ、マルチキャスト パケットをインターフェイス外部、ネクストホップに転送します。仮想ルーターは、厳密にどのレシーバーがグループに参加しているのか追跡しません。サブネット上の単一のルーター、つまり IGMP Querier（最も小さい IP アドレスを持つルーター）だけが IGMP クエリに応答します。

IGMP クエリの間隔、レシーバーがクエリに応答するまでに許される時間（Max Query Response Time (最大クエリ応答時間)）をインターフェイスに対して設定できます。グループを離れるレシーバーから IGMP リーブ メッセージを受け取る際、仮想ルーターは、リーブ メッセージを受信したインターフェイスに即時脱退オプションが設定されていないことを確認します。即時脱退

オプションがない状態で、仮想ルーターが対象のグループにまだレシーバーのメンバーがあるかどうか判断するためのクエリを送信します。Last Member Query Interval (最終メンバー クエリ間隔) は、対象のグループに残されているレシーバーが、グループのマルチキャスト トラフィックをまだ受け取りたいということを確認するための応答を行うまでに許される秒数を指定します。

インターフェイスは IGMP ロバストネス変数をサポートしています。これを調整すると、次にファイアウォールが Group Membership Interval (グループ メンバーシップ間隔)、Other Querier Present Interval (その他のクエリ送信者存在間隔)、Startup Query Count (スタートアップ クエリ数)、Last Member Query Count9 (最終メンバー クエリ数) を調整します。ロバストネス変数を大きくすると、パケットをドロップしそうなサブネットに対応できます。

IP マルチキャスト情報を表示し、IGMP が有効なインターフェイス、IGMP のバージョン、Querier のアドレス、堅牢性設定、マルチキャスト グループおよびソースの上限数、インターフェイスに対して即時脱退が設定されているかどうかを確認します。また、インターフェイスが属すマルチキャスト グループ、および他の IGMP メンバーシップ情報も確認できます。

PIM

IP マルチキャストはルーター間で Protocol Independent Multicast（PIM）を使用し、マルチキャスト パケットが送信元から受信者（マルチキャスト グループのメンバー）に至るまでに通る配信ツリー上のパスを判断します。Palo Alto Networks® のファイアウォールは PIM スパースモード（PIM-SM）（RFC 4601）、PIM Any-Source Multicast（ASM）（PIM スパースモードと呼ばれることもあります）、PIM Source-Specific Multicast（SSM）をサポートしています。PIM-SM では、マルチキャスト グループに属す受信者（ユーザー）が送信元にトラフィックを送るよう求めるまで、送信元はマルチキャスト トラフィックを転送しません。ホストがマルチキャスト トラフィックを受信したい際、IGMP の実装が IGMP メンバーシップ レポート メッセージを送信し、それを受信したルーターが次に、参加したいグループのマルチキャスト グループのアドレスに PIM ジョイン メッセージを送信します。

- **ASM**では、受信者が IGMP を使ってトラフィックにマルチキャスト グループ アドレスを求めます。そのトラフィックを起源とするソースに制約はありません。その結果、受信者は送信者を知る必要がなく、また不要なマルチキャスト トラフィックを受信する可能性があります。
- **SSM**（RFC 4607）では、受信者が IGMP を使って、特定の一つあるいは複数のソースからマルチキャスト グループ アドレスに向かうトラフィックをリクエストします。受信者は送信者の IP アドレスを知っており、必要なマルチキャスト トラフィックのみを受信します。SSM では IGMPv3 が必要です。デフォルトの SSM アドレス空間（232.0.0.0/8）はオーバーライドできます。

Palo Alto Networks ファイアウォールで IP Multicast を設定すると、受信者向けのインターフェイスでもマルチキャスト トラフィックを転送するインターフェイスの PIM を有効にする必要があります。これは、受信者に面したインターフェイス上でのみ有効化する IGMP とは異なります。

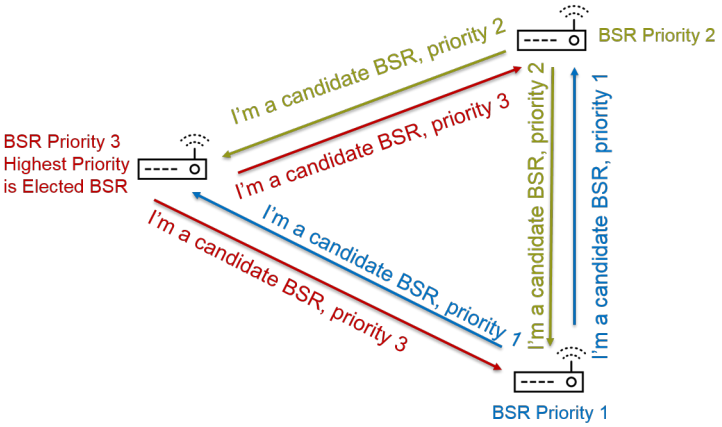
ASM は、共有配信ツリーの連結点あるいはルートに位置するルーターであるランデブーポイント（RP）を必要とします。マルチキャスト ドメイン用の RP は、すべてのマルチキャスト グループがジョイン メッセージの送信先にする単一のポイントとして機能します。この動作により、グループのメンバーが複数のルーターにジョイン メッセージを送信した場合に起こり得るルーティング ループの発生を回避できます。（ソース固有マルチキャストは最短パスツリーを使い、RP が不要であるため、SSM は RP を必要としません）

ASM 環境では、どのルーターがマルチキャスト グループの RP であるのか仮想ルーターが判断する方法が 2 つあります：

- 静的 **RP** 対グループ マッピング—ファイアウォール上の仮想ルーターがマルチキャスト グループの RP として機能するように構成します。静的 RP アドレスを設定する、あるいはローカル RP を候補 RPと指定して動的に選択させる（優先順位の値が最も小さいもの）ことで、ローカル RP を構成します。また、ローカル RP がカバーしないグループ アドレス範囲の外部 RP を一つあるいは複数静的に構成でき、それによりマルチキャスト トラフィックの負荷分散を行い、単一の RP の負荷が大きくなり過ぎるのを防ぐことができます。

- ブートストラップ ルーター（**BSR**）—（RFC 5059）—BSR のロールを定義します。次の図のように、まずは BSR の候補が優先順位をお互いにアドバタイズし、その後で優先順位が最大である候補が BSR として選出されます。

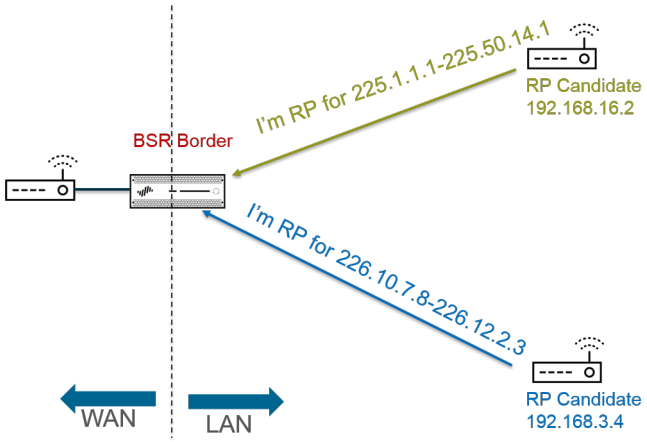
RPs Advertise Their BSR Candidacy; Highest Priority Wins



次に、候補 RP が 自身の IP アドレスおよび自身が RP になるマルチキャスト グループ範囲を含む BSR メッセージを BSR に定期的にユニキャストする際、BSR が RP を探査します。ローカル仮想ルーターを候補 RP として構成することが可能です。この場合、自身が RP であることを仮想ルーターが特定のマルチキャスト グループあるいは複数のグループに伝えます。BSR は、PIM ドメイン内の他の RP に RP 情報を送信します。

インターフェイスの PIM を構成する際、ファイアウォールのインターフェイスがエンタープライズの境界に位置し、エンタープライズ ネットワークの外側を向いている場合、BSR を選択できます。BSR ボーダー設定は、ファイアウォールが RP キャンディダシー BSR メッセージを LAN の外部に送信するのを防止します。次の図は、LAN に面したインターフェイスで BSR ボーダーが有効であり、そのインターフェイスが最も高い優先順位を持っている状態です。仮想ルーターが静的 RP および動的 RP（BSR から学習）の両方を持っている場合、ローカルの静的 RP を構成する際に、あるグループについて学習した RP を静的 RP でオーバーライドするかどうかを指定できます。

BSR Border Router Discovers RPs;
Keeps PIM RP Candidacy Messages Within LAN



PIM スパースモードが共有ツリーの下方に送信するトラフィックがあるということを RP に通知するためには、RP が送信元を知る必要があります。宛先ルーター（DR）が PIM レジスターメッセージ内のホストの最初のパケットをカプセル化し、そのパケットをローカル ネットワーク上の RP にユニキャストする際、ホストはトラフィックをマルチキャスト グループ アドレスに送信していることを RP に通知します。また、DR は受信者から RP にプルーン メッセージも転送します。RP は、マルチキャスト グループへと送信している送信元の IP アドレスのリストを維持し、RP は送信元から来たマルチキャスト パケットを転送できます。

PIM ドメイン内のルーターが DR を必要とする理由とは？ルーターがスイッチに PIM ジョイン メッセージを送信する際、2 つのルーターがそれを受信して同じ RP に送信し、冗長なトラフィックと帯域幅の無駄が生じるおそれがあります。不要なトラフィックをなくすために、PIM ルーターは DR（最大の IP アドレスを持つルーター）を選出し、DR だけがジョイン メッセージをRP に転送します。あるいは、IP アドレスの比較よりも優先される DR 優先順位をインターフェイス グループに割り当てることもできます。DR は PIM メッセージを転送（ユニキャスト）しており、IP マルチキャスト パケットをマルチキャストしているわけではないということにご注意ください。

インターフェイス グループが仮想ルーターのピアになることを許可する PIM ネイバー（ルーター）の IP アドレスを指定できます。デフォルト設定では、すべての PIM が有効なルーターが PIM ネイバーになることができますが、ネイバーを制限するオプションにより、PIM 環境の仮想ルーターのセキュリティをさらに向上させることができます。

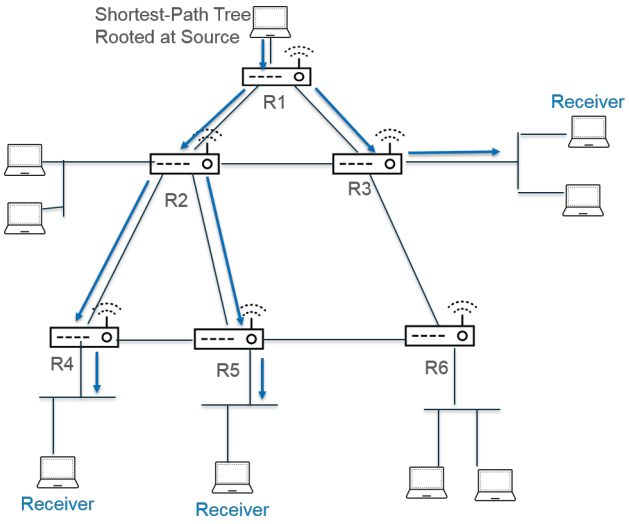
- 最短パスツリー（SPT）および共有ツリー
- PIM アサート メカニズム
- リバースパス フォワーディング

最短パスツリー（SPT）および共有ツリー

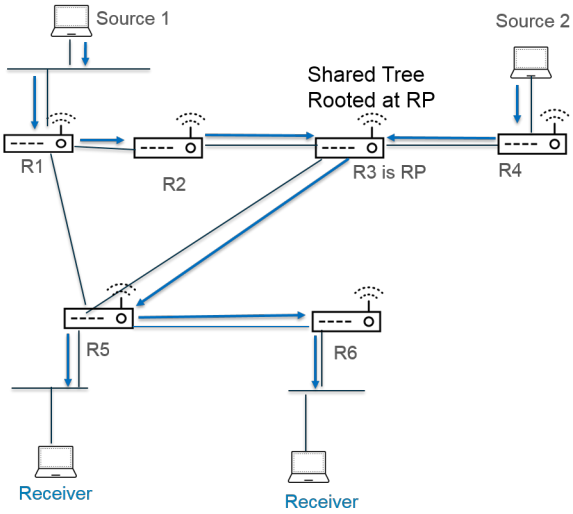
受信者がマルチキャスト グループに参加した後、グループ内の各受信者にデータを送るために必要となるルーティング パスをマルチアクセス ネットワークのルーターが構築します。マルチキャスト グループに送信された各 IP データグラムはすべてのメンバーに配信（転送）されます。ルーティング パスは、マルチキャスト パケットの配信ツリーのタイプを構成します。マルチキャスト配信ツリーの目的は、パケットがパスの分岐点に達し、ルーターがパケットをさらに複数のパス経由ですべてのグループのメンバーへと送信する必要がある際に、ルーターにマルチキャスト パケットを複製させることですが、配信ツリーは適切な受信者が存在しないパスにパケットを送信するのを避けます。配信ツリーは次のいずれかです：

- ソース ツリー—複数の送信元（ツリーのルート）からネットワークを通りマルチキャスト グループの受信者へと至るパスです。ソース ツリーはマルチキャスト パケットが送信元から受信者に至るまでの最短のパスであるため、最短パスツリー（**SPT**）とも呼ばれます。送信者と受信者はソースおよびマルチキャスト グループのペア、それを短縮して (S, G) とラベリング

されます（例：(192.168.1.1, 225.9.2.6)）。次の図は、送信元から 3 つの受信者までの、3 つの最短パスツリーを示しています。



- 共有ツリー—マルチキャスト ソースではなく、RP をルートに持つパスです。共有ツリーは RP ツリーあるいは RPT とも呼ばれます。ルーターは様々なソースからのマルチキャスト パケットを RP に転送し、その RP がパケットを共有ツリーの中でさらに進めます。共有ツリーは (*, G) とラベリングされます。マルチキャスト グループに属すすべてのソースが RP からの同じ配信ツリーを共有するため、ソースとしてワイルドカードを使用します。共有ツリーのラベリングの例は、(*, 226.3.1.5) です。次の図は、RP のルートから受信者に至る共有ツリーを示しています。



Source-Specific Multicast（SSM）は、ソース ツリー配信を使用します。Any-Source Multicast（ASM）を使うためにIP マルチキャストを設定する際、グループの SPT しきい値を設定することで、マルチキャスト パケットをグループに届けるために Palo Alto Networks® のファイアウォール上の仮想ルーターがどの配信ツリーを使用するのか指定できます。

- デフォルト設定では、仮想ルーターがグループあるいはプレフィックス（**SPT Threshold (SPT しきい値)**を 0 に設定）の最初のマルチキャスト パケットを受け取る際に、マルチキャスト ルーティングを共有ツリーから SPT に切り替えます。

- 指定されたマルチキャスト グループあるいはプレフィックス用の、任意のインターフェイス上で任意の期間に受信するパケットの合計キロビット数が設定済みの値に達したとき、SPT に切り替えるように仮想ルーターを設定できます。
- グループあるいはプレフィックスに対し、SPT に切り替えないように仮想ルーターを設定することもできます（継続して共有ツリーを使用）。

SPT はより多くのメモリを必要とするため、グループに向かうマルチキャスト トラフィックのレベルに応じて設定を選択してください。仮想ルーターが SPT に切り替わる場合、ソース（RP ではなく）からパケットを受信し、仮想ルーターはプルーン メッセージを RP に送信します。ソースは、グループの後続のマルチキャスト パケットを最短パスツリーに沿って送信します。

PIM アサート メカニズム

マルチアクセス ネットワーク上のルーターが同じマルチキャスト トラフィックを同じネクストホップに転送（冗長なトラフィックや帯域幅の無駄につながるおそれがある）しないようにするために、PIM はアサート メカニズムを使用してマルチアクセス ネットワークの単一の PIM フォワーダーを選出します。

仮想ルーターがパケット内で同じ (S,G) ペアと識別された外向きのインターフェイスとしてすでに関連付けているインターフェイス上の送信元から仮想ルーターがマルチキャスト パケットを受信する場合、それは冗長なパケットになります。その結果、仮想ルーターはそのメトリックを含むアサート メッセージをマルチアクセス ネットワーク上の他のルーターに送信します。その後、ルーターは次の方法で PIM フォワーダーを選出します。

1. PIM フォワーダーは、マルチキャスト ソースまでの管理距離が最短であるルーターです。
2. 管理距離が最短であるものが複数ある場合、ソースまでのユニキャスト ルーティングメトリックが最適なルーターが PIM フォワーダーになります。
3. 最適なメトリックが複数ある場合、IP アドレスが最も大きいルーターが PIM フォワーダーになります。

PIM フォワーダーとして選出されなかったルーターは、(S,G) ペアで識別されたマルチキャスト グループにトラフィックを転送するのを停止します。

IP マルチキャストを設定する際、仮想ルーターがインターフェイス外に PIM アサート メッセージを送信する間隔（アサート間隔）を設定できます。IP マルチキャスト情報を表示する際、**PIM Interface (PIM** インターフェイス**)**タブにインターフェイスのアサート間隔が表示されます。

リバースパス フォワーディング

PIMはリバースパス フォワーディング（RPF）を使用し、仮想ルーター上のユニキャスト ルーティングテーブルを利用することで、マルチキャスト ルーティング ループを回避します。仮想ルーターはマルチキャスト パケットを受信する際、そのユニキャスト ルーティングテーブル内でマルチキャスト パケットの送信元を探し、その送信元 IP アドレスに関連する外向きのインターフェイスが、パケットが到達するインターフェイスであるか確認します。インターフェイスがマッチする場合、仮想ルーターはパケットを複製してそれをインターフェイス外部、グループ内のマルチキャスト レシーバーに向けて転送します。インターフェイスがマッチしない場合、仮想ルーターはパケットをドロップします。ユニキャスト ルーティングテーブルは、OSPF など、ネットワークが使用する背後の内部ゲートウェイ プロトコル（IGP）あるいは静的ルートに基づきます。

また、PIM は RPF を使用して、一度に PIM ルーター ホップを一つずつ、ソースまでの最短パスツリーを構築します。仮想ルーターはマルチキャスト ソースのアドレスを持っているため、ソースに遡るそのネクストホップとして、仮想ルーターがソースにユニキャスト パケットを転送するために使用する上流の PIM ネイバーを選びます。ネクストホップ ルーターが同じことを行います。

RPF が成功し、仮想ルーターがそのマルチキャスト ルーティング情報ベース（mRIB）にルートエントリを確保した後、仮想ルーターはそのマルチキャスト転送情報ベース（マルチキャスト転送テーブルあるいは mFIB）内にソースベースのツリーのエントリ (S,G) および共有ツリーのエントリ (*,G) を維持します。各エントリには、送信元 IP アドレス、マルチキャスト グループ、内向きInterface (インターフェイス)（RPF インターフェイス）、外向きインターフェイスのリストが含まれています。最短パスツリーはルーターで分岐することがあり、ルーターは異なるパスの先にあるグループの受信者へと到達させるためにパケットを複数のインターフェイスから転送しなければならないため、外向きのインターフェイスが複数ある場合があります。仮想ルーターが mFIB を使ってマルチキャスト パケットを転送する際、(*,G) エントリにマッチさせようと試みる前に (S,G) にマッチさせます。

マルチキャスト ソース プレフィックスを BGP へとアドバタイズしている場合（IPv4 アドレス ファミリーおよびマルチキャスト下位アドレス ファミリーと共にMP-BGPを設定）、ファイアウォールはマルチキャスト下位アドレス ファミリーの元で受信した BGP ルート上で RPF チェックを実行します。

IP マルチキャスト情報を表示し、mFIB および mRIB エントリの確認方法を把握します。マルチキャスト ルート テーブル（mRIB）はユニキャスト ルートテーブル（RIB）とは別のテーブルですので、ご注意ください。

IP マルチキャストを設定します

IP マルチキャスト パケットを受信・転送するよう、Palo Alto Networks® ファイアウォールのVirtual Router (仮想ルーター - VR)上のインターフェースを設定します。仮想ルーターの IP マルチキャストを有効化し、入力および出力インターフェイス上で Protocol Independent Multicast（PIM）を設定し、レシーバーに面したインターフェイス上で Internet Group Management Protocol（IGMP）を設定する必要があります。

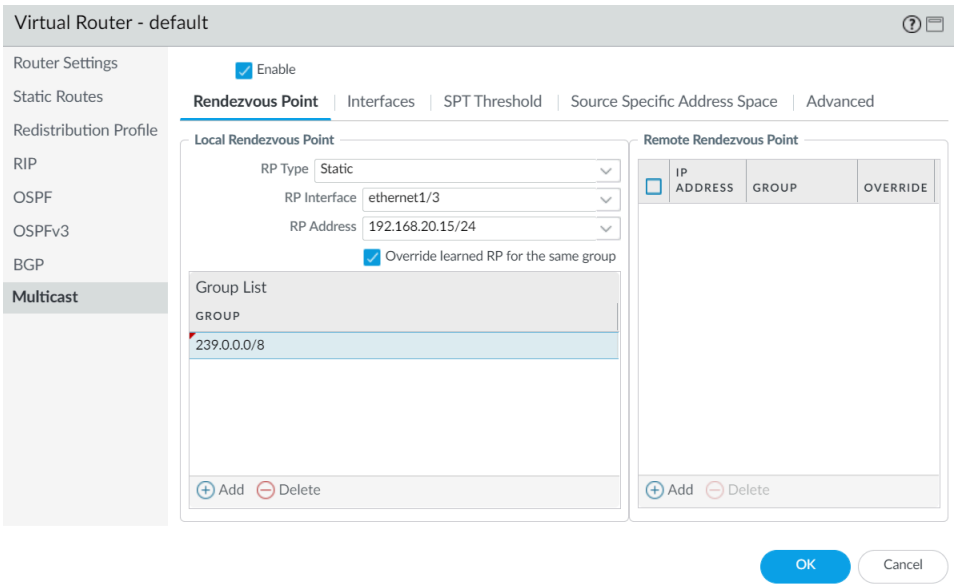
STEP 1 | 仮想ルーターの IP マルチキャストを有効にします。

1. **Network (ネットワーク)** > **Virtual Routers (仮想ルーター)** の順に選択し、さらに仮想ルーターを選択します。
2. **Multicast (マルチキャスト)**を選択して IP マルチキャストを**Enable (有効化)**します。

STEP 2 | （ASM のみ）仮想ルーターが位置するマルチキャスト ドメインが Any-Source Multicast（ASM）を使用する場合、マルチキャスト グループ用のローカルおよびリモート ランデブーポイント（RP）を識別・設定します。

1. **Rendezvous Point (**ランデブーポイント**)**を選択します。
2. RP の選択基準を定めるローカル**RP Type (RP** タイプ**)**を選択します（オプションは**Static (**静的**)**、**Candidate (**候補**)**あるいは**None (**なし**)**）：

   - **Static (**静的**)**—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。静的 RP の設定では、PIM ドメイン内の他の PIM ルーターと同じ RP を明示的に構成する必要があります。
     - **RP Interface**（**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、Layer3、バーチャル ワイヤ、ループバック、VLAN、集約イーサネット（AE）、およびトンネルです。
     - **RP Address**（**RP** アドレス）を選択します。選択した RP インターフェイスの IP アドレスがリストを作成します。
     - **Override learned RP for the same group (**同じグループで学習した **RP** をオーバーライド**)**を選択し、グループ リストで対象のグループ用の候補に挙げられた RP ではなく、この静的 RP サーバーを RP として機能させます。
     - RP を RP として動作させるマルチキャスト**Groups (**グループ**)**を一つあるいは複数**Add (**追加**)**します。



   - **Candidate (**候補**)**—優先順位に基づいてマルチキャスト グループへの RP の動的マッピングを確立し、PIM ドメイン内の各ルーターが自動的に同じ RP を選別できるようにします。
     - 候補の RP の**RP Interface (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、レイヤー 3、ループバック、VLAN、集約イーサネット（AE）、およびトンネルです。
     - 候補の RP の**RP Address(RP** アドレス**)**を選択します。選択した RP インターフェイスの IP アドレスがリストを作成します。

- （任意）候補 RP の**Priority (優先順位)**を変更します。ファイアウォールは候補 RP の優先順位を他の候補 RP の優先順位と比較し、対象のグループでどれが RP として動作するのか決定します。ファイアウォールは優先順位の値が最も低い候補 RP を選択します（範囲は 0～255、デフォルトは 192）。
- （任意）**Advertisement Interval (sec) (**アドバタイズメント間隔 （秒）**)**を変更します（範囲は 1～26,214、デフォルトは 60）。
- RP と通信するマルチキャスト グループの**Group List (**グループ リスト**)**を入力します。

- **None (**なし**)**–この仮想ルーターが RP でない場合はこれを選択します。

3. Remote Rendezvous Point (リモート ランデブーポイント) を**Add (**追加**)**し、そのリモート（外部）RP の**IP Address (IP** アドレス**)**を入力します。
4. 指定したリモート RP アドレスを RP として動作させるマルチキャスト**Group Addresses (**グループのアドレス**)**を**Add (**追加**)**します。
5. **Override learned RP for the same group (**同じグループで学習した **RP** をオーバーライド**)**を選択し、グループアドレス リストで対象のグループ用に動的に学習した（候補に挙げられた）RP ではなく、この静的に構成した外部 RP サーバーを RP として機能させます。
6. **OK** をクリックします。

STEP 3 | マルチキャスト設定（IGMP、PIM、およびグループ権限）を共有するインターフェイスのグループを指定します。

1. **Interfaces (**インターフェイス**)**タブでインターフェイス グループの**Name (**名前**)**を**Add (**追加**)**します。
2. **Description (**説明**)** を入力します。
3. **Interface (**インターフェイス**)**を**Add (**追加**)**し、対象のインターフェイス グループに属すレイヤー 3 インターフェイスを一つあるいは複数選択します。

STEP 4 | （任意）インターフェイス グループのマルチキャスト グループ権限を設定します。デフォルト設定では、インターフェイス グループはすべてのグループから IGMP メンバーシップ レポートおよび PIM ジョイン メッセージを受け取ります。

1. **Group Permissions (**グループ権限**)**を選択します。
2. このインターフェイス グループに使用する Any-Source Multicast（ASM）グループを構成するには、Any Source (任意のソース) ウィンドウで、任意のソースからの PIM ジョ

イン メッセージおよび IGMP メンバーシップ レポートを許可するマルチキャスト グループを識別する**Name (名前)**を**Add (追加)**します。

3. マルチキャスト**Group (グループ)**のアドレスあるいはアドレスグループおよび任意のソースからインターフェイス上でマルチキャスト パケットを受け取ることができる / prefix を入力します。
4. **Included (含有)**を選択し、インターフェイス グループに ASM **Group (グループ)**を含めます（デフォルト）。**Included (含有)**の選択を解除すれば、テストを行う際などに、簡単に ASM グループをインターフェイス グループから除外できます。
5. 任意のソースからマルチキャスト パケットを受け取らせたい他のマルチキャスト**Groups (グループ)**（インターフェイス グループ用）を**Add (追加)**します。
6. このインターフェイス グループで Source-Specific Multicast（SSM）を構成するには、Source Specific (ソース固有) ウィンドウで、マルチキャスト グループとソース アドレスのペアを識別する**Name (名前)**を**Add (追加)**します。Any-Source Multicast で使

用した名前を使わないでください。（IGMPv3 を使って SSM を設定する必要があります）

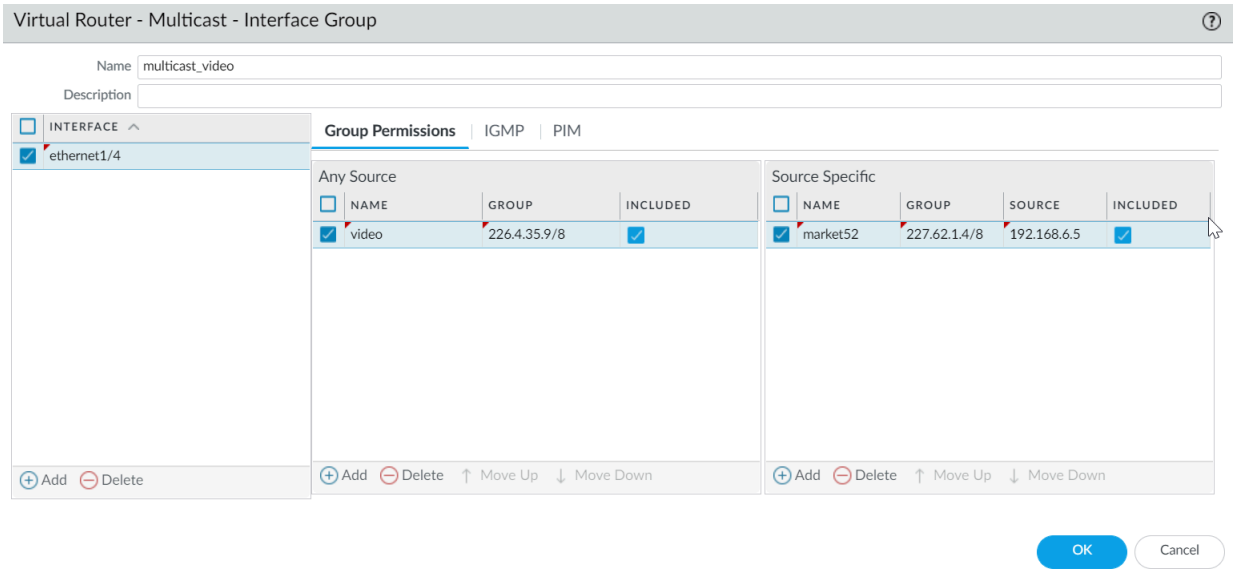
7. マルチキャスト**Group (**グループ**)**のアドレスあるいはアドレスグループおよび特定のソースのみからマルチキャスト パケットを受け取りたい（そしてインターフェイス上でパケットを受け取ることができる）グループの /prefix を入力します。

   権限を指定するソース固有のグループは、仮想ルーターが *source-specific*（ソース固有）として扱わなければならないグループになります。権限を設定するソース固有のグループ含む***Source Specific Address Space*** **(**ソース固有のアドレス空間**)**（ステップ 9）を設定します。

8. このマルチキャスト グループがマルチキャスト パケットの受信元にする**Source (**送信元**)** IP アドレスを入力します。

9. **Included (**含有**)**を選択し、インターフェイス グループに SSM グループおよび送信元アドレス ペアを含めます（デフォルト）。**Included (**含有**)**の選択を解除すれば、テストを行う際などに、簡単にペアをインターフェイス グループから除外できます。

10. 特定のソースからのマルチキャスト パケットのみを受信させるマルチキャスト**Groups (**グループ**)**（インターフェイス グループ用）を**Add**（追加）します。



STEP 5 | インターフェイスがマルチキャスト レシーバーに面している場合、グループに参加するために IGMP を使用しなければならないインターフェイス グループの IGMP を設定します。

1. **IGMP**タブで IGMP を**Enable (**有効化**)**（デフォルト）します。
2. インターフェイス グループ内のインターフェイスのIGMPパラメーターを指定します：
   - **IGMP Version (IGMP** バージョン**)**—**1**、**2**、あるいは**3**（デフォルト）。
   - **Enforce Router-Alert IP Option (**ルーターアラート **IP** オプションを適用**)**（デフォルトで無効）—IGMPv2 あるいは IGMPv3 を使用するインバウンド IGMP パケットにIP

ルーターアラート オプション、RFC 2113 を求める場合はこのオプションを選択します。

- **Robustness (堅牢性)**—ファイアウォールがグループ メンバーシップ間隔、その他のクエリ送信者存在間隔、スタートアップ クエリ数、最終メンバー クエリ数を調整するために使用する変数です（範囲は 1～7、デフォルトは 2）。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。
- **Max Sources (最大ソース数)**—単一のインターフェイスについて IGMP が同時に処理できるソースの最大数です（範囲は 1～65,535、デフォルトは**unlimited (無制限)**）。
- **Max Groups (最大グループ数)**—単一のインターフェイスについて IGMP が同時に処理できるグループの最大数です（範囲は 1～65,535、デフォルトは**unlimited (無制限)**）。
- **Query Interval (クエリ間隔)**—レシーバーがまだ対象のグループのマルチキャスト パケットを受信したいかどうか判断するために仮想ルーターがレシーバーに送信する、IGMP メンバーシップ クエリ メッセージの間隔を秒数で示します（範囲は 1～31,744、デフォルトは 125）。
- **Max Query Response Time (sec) (最大クエリ応答時間（秒）)**—対象のグループについてレシーバーがもうマルチキャスト パケットを受信しなくて良いと仮想ルーターが判断する前に、レシーバーが IGMP メンバーシップ クエリ メッセージに応答するまでに許される最大秒数です（範囲は 0～3,174.4、デフォルトは 10）。
- **Last Member Query Interval (sec) (最終メンバー クエリ間隔（秒）)**—レシーバーがリーブ グループ メッセージを送信した後、仮想ルーターが送信するグループ固有クエリにレシーバーが応答するまでに許される秒数です（範囲は 0.1～3,174.4、デフォルトは 1）。
- **Immediate Leave (即時脱退)**（デフォルトで無効）—マルチキャスト グループのメンバーが一つだけであり、仮想ルーターがそのグループを対象にした IGMP リーブ メッセージを受け取る際、最終メンバー クエリ間隔が失効するのを待たずに、即時脱退設定が、仮想ルーターにそのグループ、multicast routing information base（mRIB）からの外向きインターフェイス、multicast forwarding information base（mFIB）を即座に削除させます。即時脱退設定はネットワークリソースを保存します。インターフェイス グループが IGMPv1 を使用する場合は Immediate Leave (即時脱退) を選択できません。

STEP 6 | そのインターフェイス グループの PIM スパースモード（PIM-SM）を設定します。

1. **PIM**タブで PIM を**Enable (有効化)**（デフォルトで有効）します。
2. インターフェイス グループの PIM パラメーターを指定します：

- **Assert Interval (アサート間隔)**—マルチアクセス ネットワーク上の他の PIM ルーターが PIM 転送者を選出する際に、仮想ルーターが他の PIM ルーターに送信するPIM アサート メッセージの間隔を秒数で示します（範囲は 0～65,534、デフォルトは 177）。
- **Hello Interval (Hello 間隔)**—仮想ルーター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その PIM ネイバーに送信する PIM Hello メッセージの間隔を秒数で示します（範囲は 0～18,000、デフォルトは 30）。

- **Join Prune Interval (**ジョイン プルーン間隔**)**—仮想ルーターが上流のマルチキャスト ソースに送信する PIM ジョイン メッセージの間隔（および PIM プルーン メッセージの間隔）を秒数で示します（範囲は 0～18,000、デフォルトは 60）。
- **DR Priority (DR** 優先順位**)**—マルチアクセス ネットワーク内のどのルーターが PIM ジョインおよびプルーン メッセージを RP に転送するのか制御する宛先ルーター（DR）の優先順位です（範囲は 0～429,467,295、デフォルトは 1）。DR を選出する際、DR 優先順位は IP アドレスの比較よりも優先されます。
- **BSR Border (BSR** ボーダー**)**—インターフェイス グループのインターフェイスが、エンタープライズ LAN の境界に位置する BSR であり、仮想ルーター上にある場合は、このオプションを選択します。これは、RP キャンディダシー BSR メッセージが LAN を出るのを阻止します。

3. 仮想ルーターがマルチキャスト パケットを許可する各ルーターの**IP Address (IP** アドレス**)**を指定し、一つあるいは複数の**Permitted PIM Neighbors (**許可する **PIM** ネイバー**)**を**Add (**追加**)**します。

STEP 7 | **OK** をクリックして、インターフェイス グループ設定を保存します。

STEP 8 | （任意）最短パスツリー（SPT）および共有ツリーに記載されているように、Shortest-Path Tree（SPT）を変更します。

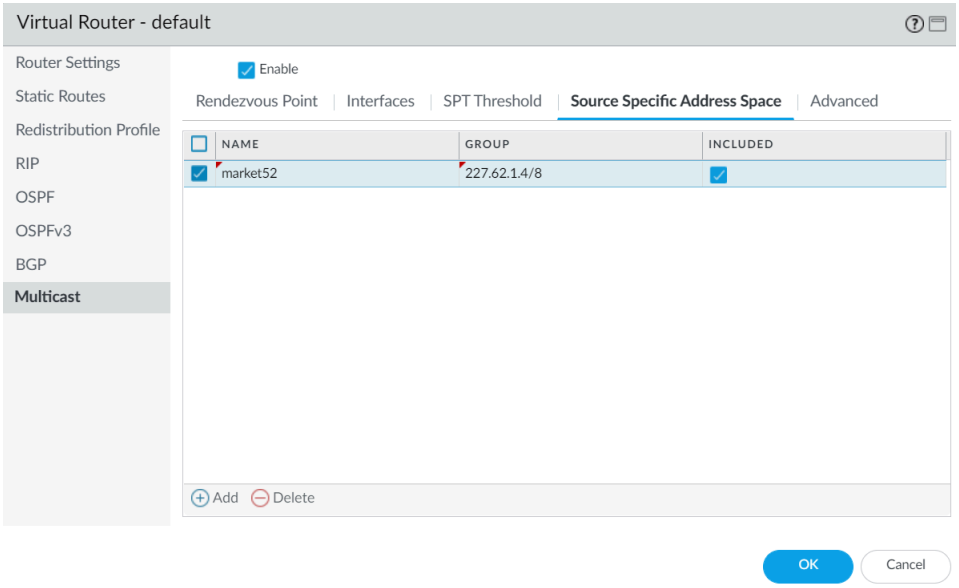
1. **SPT Threshold (SPT** しきい値**)**を選択し、**Multicast Group/Prefix (**マルチキャスト グループ**/**プレフィックス**)**（配信ツリーの指定対象であるマルチキャスト グループあるいはプレフィックス）を**Add (**追加**)**します。
2. **Threshold (kb) (**しきい値（**kb**）**)**を指定します—特定のマルチキャスト グループへのルーティングあるいはプレフィックスが共有ツリー（RP がソース）から SPT 配信に切り替わるポイントです：
   - **0 (switch on first data packet) (0**（最初のデータパケット時に切り替え）**)**（デフォルト）—仮想ルーターが対象のグループあるいはプレフィックスの最初のデータパケットを受け取る際、仮想ルーターが共有ツリーからグループあるいはプレフィックスの SPT に切り替えます。
   - **never (do not switch to spt) (**なし（**spt** に切り替えない）**)**—仮想ルーターは継続して共有ツリーを使ってパケットをグループあるいはプレフィックスに転送します。
   - 任意のインターフェイスおよび任意の期間で（仮想ルーターがそのマルチキャスト グループあるいはプレフィックスのために SPT 配信に切り替わるタイミング）、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。

STEP 9 | 特定のソースからのマルチキャスト パケットのみを受け取るグループおよびプレフィックスあるいはマルチキャスト グループを特定します。

1. **Source Specific Address Space (**ソース固有のアドレス空間**)**を選択し、その空間の**Name (**名前**)**を**Add (**追加**)**します。
2. 特定のソースからマルチキャスト パケットを受け取るアドレス空間を識別する、プレフィックス長を持つマルチキャスト**Group (**グループ**)**を入力します。仮想ルーターが SSM グループからマルチキャスト パケットを受信し、そのグループが**Source Specific**

Address Space (ソース固有のアドレス空間)でカバーされていない場合は、仮想ルーターがパケットをドロップします。

3. **Included** (含有)を選択し、ソース固有のアドレス空間をマルチキャスト グループのアドレス範囲として含めます。仮想ルーターは、この許可された特定のソースから来るマルチキャスト パケットを許可します。**Included** (含有)の選択を解除すれば、簡単にグループのアドレス空間を除外してテストを行えます。
4. 他のソース固有のアドレス空間を追加し、SSM グループ権限を指定したすべてのグループを含めます。



STEP 10 | （任意）マルチキャスト グループおよびソース間でセッションが修了した後、マルチキャスト ルートが mRIB に残る時間を変更します。

1. **Advanced**（詳細）タブを選択します。
2. **Multicast Route Age Out Time (sec)** (マルチキャスト ルート存続期間（秒）)（範囲は 210～7,200、デフォルトは 210）。

STEP 11 | **OK** をクリックして、マルチキャスト設定を保存します。

STEP 12 | 宛先ゾーンへのマルチキャスト トラフィックを許可するセキュリティポリシールールを作成します。

1. セキュリティ ポリシー ルールを作成し、**Destination** (宛先)タブの**Destination Zone** (宛先ゾーン)で**multicast** (マルチキャスト)あるいは**any** (すべて)を選択します。**multicast** (マルチキャスト)ゾーンは、すべてのマルチキャスト トラフィックにマッチする事前定義済みのレイヤー 3 ゾーンです。**Destination Address** (宛先アドレス)をマルチキャスト グループのアドレスにすることができます。
2. 残りのセキュリティポリシー ルールの設定を行います。

STEP 13 | （任意）ルートがセットアップされる前にマルチキャスト パケットのバッファリングを有効化します。

1. **Device (デバイス)** > **Setup (セットアップ)** > **Session (セッション)** を選択して Session Settings (セッション設定) を編集します。
2. **Multicast Route Setup Buffering (**マルチキャストルートの設定バッファ**)**を有効化します（デフォルトで無効）。対応するマルチキャスト グループのエントリがマルチキャスト転送テーブル（mFIB）にまだ存在しない場合、ファイアウォールはマルチキャスト フローからの最初のパケットを保持できます。**Buffer Size (**バッファサイズ**)**は、ファイアウォールがフローからのパケットをどれだけバッファリングするのかを制御します。ルートが mFIB にインストールされた後、ファイアウォールはバッファリングされた最初のパケットを自動的にレシーバーに転送します。（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、使用しているマルチキャスト アプリケーションがフロー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）
3. （任意）**Buffer Size (**バッファサイズ**)**を変更します。バッファサイズは、mFIB エントリがセットアップされるまでに、ファイアウォールがバッファリングできるマルチキャスト フロー毎のパケット数です（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合計 5,000 パケット（すべてのフローが対象）をバッファリングすることができます。
4. **OK** をクリックします。

STEP 14 | 変更をコミットします。

STEP 15 | IP マルチキャスト情報を表示して、mRIB および mFIB エントリ、IGMP インターフェイス設定、IGMP グループ メンバーシップ、PIM ASM および SSM モード、RP に対するグループ マッピング、DR アドレス、PIM 設定、PIM ネイバーなどを閲覧します。

STEP 16 | マルチキャスト トラフィック用にスタティック ルートの設定を行う場合、ルートがマルチキャスト トラフィックにのみ使用されるよう、マルチキャスト ルーティングテーブルにのみ（ユニキャスト ルーティングテーブルではなく）ルートをインストールできます。

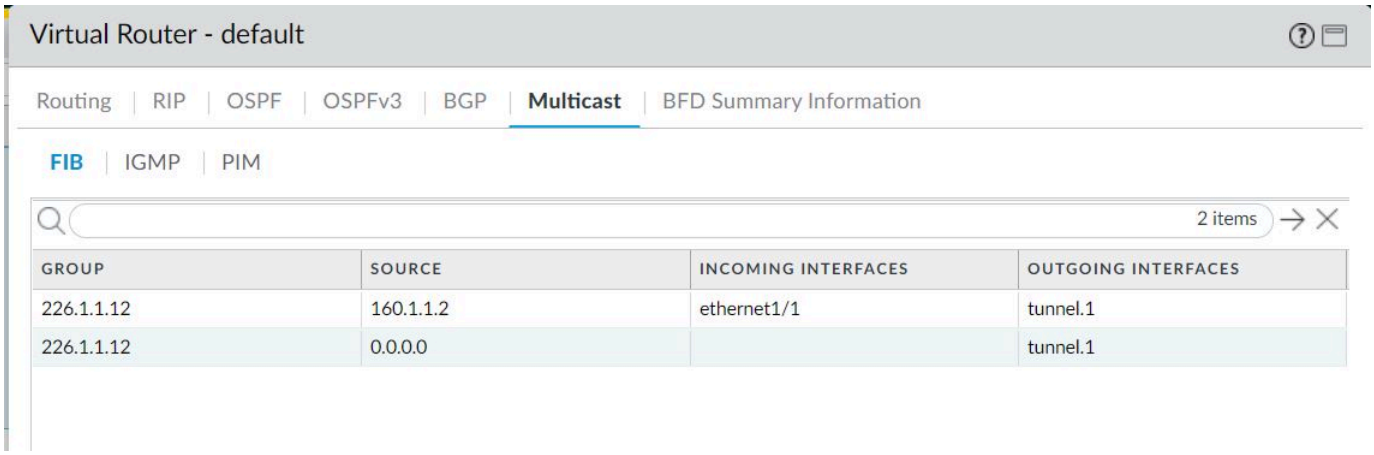
STEP 17 | IP マルチキャストを有効化する場合、論理的マルチキャスト トポロジーを論理的ユニキャスト トポロジーと別けていなければ、IPv4 マルチキャスト用に MP-BGP を伴う BGP を設定する必要はありません。マルチキャスト下位アドレス ファミリーに属す BGP にマルチキャスト ソース プレフィックスをアドバタイズしたい際、IPv4 アドレス ファミリーおよびマルチキャスト下位アドレス ファミリーと共に MP-BGP 拡張を構成します。

IP マルチキャスト情報の表示

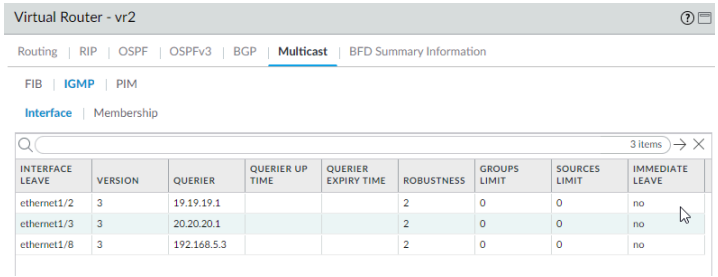
IP マルチキャスト ルーティングの設定を行った後、マルチキャスト ルート、転送するエントリー、IGMP および PIM インターフェイスの情報を表示します。

Network （ネットワーク） > **Virtual Routers** （仮想ルーター）を選択し、構成した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。

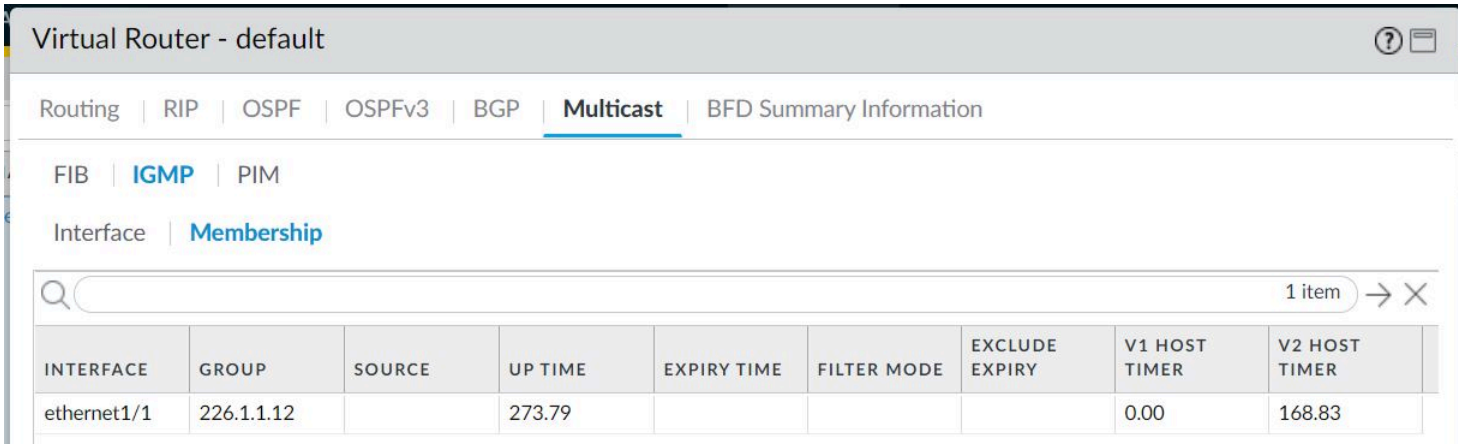
1. **Routing (ルーティング)** > **Route Table (ルート テーブル)**を選択してからさらに**Multicast (マルチキャスト)**のラジオボタンを選択し、マルチキャスト ルートだけを表示します（宛先 IP マルチキャスト グループ、そのグループへのネクストホップ、出力インターフェイス）。これは mRIB から得る情報です。
2. **Multicast (マルチキャスト)** > **FIB**を選択し、mFIB のマルチキャスト ルート情報を表示します（仮想ルーターが属すマルチキャスト グループ、対応するソース、入力インターフェイス、レシーバーへの出力インターフェイス）。



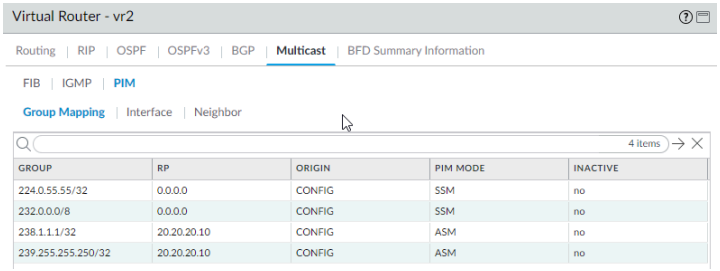
3. **Multicast (マルチキャスト)** > **IGMP** > **Interface (インターフェイス)**を選択し、IGMP が有効なインターフェイス、関連する IGMP バージョン、IGMP Querier の IP アドレス、Querier の起動時間と失効時間、堅牢さ設定、マルチキャスト グループおよびソースの制限数、そしてインターフェイスの即時脱退用の設定が行われているかどうかを表示します。



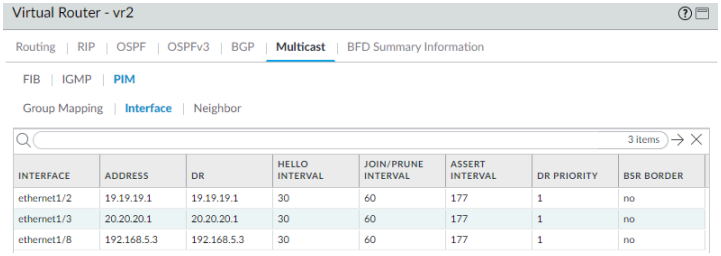
4. **Multicast (マルチキャスト)** > **IGMP** > **Membership (メンバーシップ)**を選択し、IGMP が有効なインターフェイス、それが属すマルチキャスト グループ、ソース、その他の IGMP 情報を表示します。



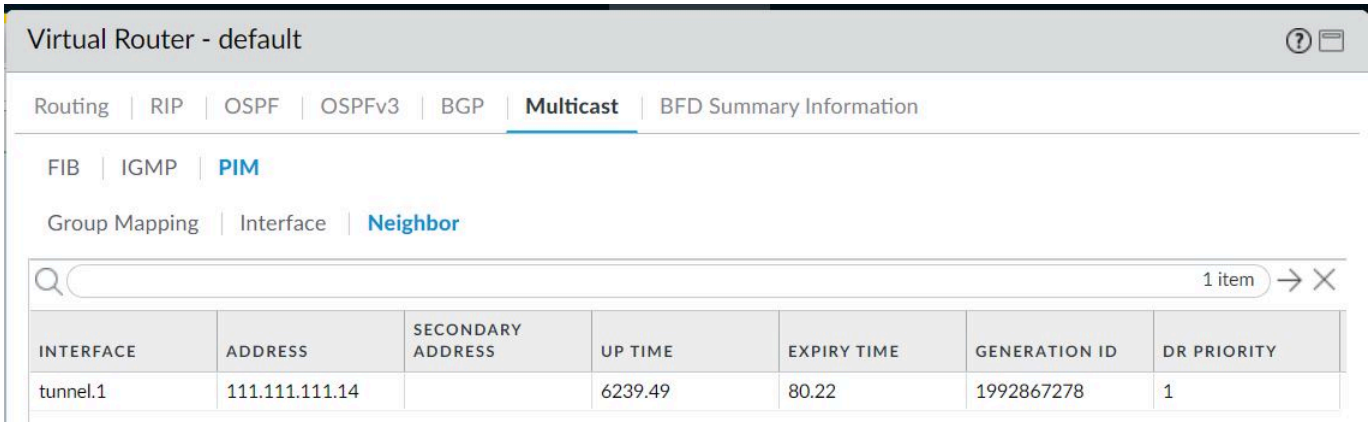
5. **Multicast (マルチキャスト)** > **PIM** > **Group Mapping (グループ マッピング)**を選択し、RP にマッピングされているマルチキャスト グループ、RP マッピングのソース、グループの PIM モード（ASM あるいは SSM）、そしてグループが無効な状態であるかどうかを表示します。SSM モードの各グループは RP を使用しないため、 RP アドレスは 0.0.0.0 として表示されます。デフォルトの SSM グループは 232.0.0.0/8 です。



6. **Multicast (マルチキャスト)** > **PIM** > **Interface (インターフェイス)**を選択し、インターフェイス用の DR の IP アドレス、DR の優先順位、Hello、Join/Prune、Assert の間隔、そしてインターフェイスがブートストラップ ルーター（BSR）であるかどうかを表示します。



7. **Multicast (マルチキャスト)** > **PIM** > **Neighbor (ネイバー)**を選択し、仮想ルーターに対して PIM ネイバーであるルーターの情報を表示します。



ルート再配信

ネットワーク トラフィックのアクセシビリティを高めるために、ルートの再配布について説明し、構成します。

ルート再配布の概要

ファイアウォールのルート再配信は、ファイアウォールがルーティング プロトコル（あるいはスタティックあるいは接続済みルート）から学習したルートを別のルーティング プロトコルで利用できるようにすることで、ネットワーク トラフィックのアクセシビリティを向上させます。ルート再配信がない場合、ルーターあるいは仮想ルーターは、同じルーティング プロトコルを実行する他のルーターとのみ、ルートのアドバタイズメントと共有を行います。IPv4 あるいは IPv6 BGP、接続済み、スタティック ルートは OSPF RIB に、OSPFv3、接続済み、スタティック ルートは BGP RIB に再配信できます。

つまり、例えば特定のルーター上の手動スタティックルート設定によってのみ利用できた特定のネットワークを、BGP AS や OSPF エリアで利用できるようにすることが可能です。また、例えばプライベート ラボ ネットワークなど、ローカルで接続されたルートを BGP AS や OSPF エリアにアドバタイズすることもできます。

内部 OSPFv3 ネットワークのユーザーがインターネット上のデバイスにアクセスできるようにするために、ユーザーを BGP にアクセス可能にしたい場合があります。このケースでは、BGP ルートを OSPFv3 RIB に再配信することになります。

逆に、OSPFv3 ルートを BGP RIB に再配信することで BGP を通して内部 OSPFv3 ネットワークを利用できるようにするために、外部ユーザーが内部ネットワークの一部にアクセスできるようにしたい場合があります。

ルート再配布の構成に再配布プロファイルを作成します。

ルート再配布の構成

ルート再配布 を設定するには、次の手順を実行します。

STEP 1 | 再配信プロファイルを作成します。

1. **Network (ネットワーク)** > **Virtual Routers (仮想ルーター)** の順に選択し、さらに仮想ルーターを選択します。
2. **Redistribution Profile (再配信プロファイル)**および**IPv4**あるいは**IPv6**を選択し、プロファイルを**Add (追加)**します。
3. プロファイルの**Name (名前)**を入力します。これは英数字で始める必要があり、アンダーバー（_）、ハイフン（-）、ドット（.）、スペースを含められます（16 文字まで）。
4. 1～255 の範囲でプロファイルの **Priority (優先順位)** を入力します。ファイアウォールは、優先順位が一番高い（優先順位の値が一番低い）プロファイルを最初に使用する形で、ルートを順にプロファイルにマッチさせます。優先順位が高いルールが、優先順位が低いルールよりも優先されます。
5. **Redistribute (再配信)** については次のいずれかを選択します。
   - **Redist (再配信)**—このフィルタにマッチするルートを再配信する場合に選択します。
   - **No Redist (再配信なし)**—このフィルタにマッチするルートを除き、再配信プロファイルにマッチするルートを再配信する場合に選択します。これを選択すると、再配信から除外するルートを指定するブロックリストのようにプロファイルが扱われます。例えば、BGP 用の複数の再配信プロファイルがある場合、**No Redist (再配信なし)** プロファイルを作成して一部のプレフィックスを除外し、その後で低い優先順位（高い優先順位の値）を持つ一般的な再配信プロファイルを作成することができます。2 つのプロファイルが一緒になり、優先順位が高いプロファイルが優先されます。**No Redist (再配信なし)** のプロファイルだけにすることはできません。ルートを再配信する **Redist (再配信)** プロファイルを必ず 1 つ以上用意する必要があります。

6. **General Filter (**一般フィルタ**)** タブの Source Type (送信元タイプ) で、再配信するルートのタイプを一つあるいは複数選択します。
   - **bgp**—プロファイルにマッチする BGP ルートを再配信します。
   - **connect (**接続**)**—プロファイルにマッチする接続済みルートを再配信します。
   - **ospf**（IPv4 のみ）—プロファイルにマッチする BGP ルートを再配信します。
   - **rip**（IPv4 のみ）—プロファイルにマッチする BGP ルートを再配信します。
   - **ospfv3**（IPv6 のみ）—プロファイルにマッチする OSPFv3 ルートを再配信します。
   - **static (**スタティック**)**—プロファイルにマッチするスタティック ルートを再配信します。
7. （任意）**Interface (**インターフェイス**)** については、再配信のためにマッチさせる関連ルートの出力インターフェイスを一つあるいは複数 **Add (**追加**)** します。エントリを削除するには、**Delete (**削除**)** をクリックします。
8. （任意）**Destination (**宛先**)** については、再配信のためにマッチさせる IPv4 または IPv6 宛先を一つあるいは複数 **Add (**追加**)** します。エントリを削除するには、**Delete (**削除**)** をクリックします。
9. （任意）**Next Hop (**ネクストホップ**)** については、再配信のためにマッチさせるルートのネクストホップ IPv4 あるいは IPv6 アドレスを一つあるいは複数 **Add (**追加**)** します。エントリを削除するには、**Delete (**削除**)** をクリックします。
10. **OK** をクリックします。

STEP 2 | （任意—一般フィルタに ospf あるいは ospfv3 が含まれる場合）OSPF フィルタを作成し、どの OSPF あるいは OSPFv3 ルートを再配信するのか詳細に指定します。

1. **Network (**ネットワーク**)** > **Virtual Routers (**仮想ルーター**)** を選択し、さらに仮想ルーターを選択します。
2. **Redistribution Profile (**再配信プロファイル**)**および**IPv4**あるいは**IPv6**を選択し、さらに作成したプロファイルを選択します。
3. **OSPF Filter (OSPF** フィルタ**)** を選択します。
4. Path Type (パス タイプ) については、次のうち、再配信する単一あるいは複数の OSPF パスを選択します。**ext-1**、**ext-2**、**inter-area**、あるいは **intra-area**。
5. OSPF あるいは OSPFv3 ルートの再配信元になる **Area (**エリア**)** を指定するためには、エリアを IP アドレスの形式で **Add (**追加**)** します。
6. **Tag (**タグ**)** を指定するためには、タグを IP アドレスの形式で **Add (**追加**)** します。
7. **OK** をクリックします。

STEP 3 | （任意—一般フィルタに bgp が含まれる場合）BGP フィルタを作成し、どの BGP ルートを再配信するのか詳細に指定します。

1. **Network (ネットワーク)** > **Virtual Routers (仮想ルーター)** を選択し、さらに仮想ルーターを選択します。
2. **Redistribution Profile (再配信プロファイル)**および**IPv4**あるいは**IPv6**を選択し、さらに作成したプロファイルを選択します。
3. **BGP Filter (OSPF フィルタ)** を選択します。
4. **Community (コミュニティ)** については、コミュニティのリストから **Add (追加)** します（well-known コミュニティなど）。 **local-as**, **no-advertise**, **no-export**, あるいは **nopeer**.また、10 進数または 16 進数、あるいは AS:VAL のフォーマットで 32 ビットの値を入力することもできます。AS と VAL はそれぞれ 0〜65,535 までの範囲の値です。最大 10 個のエントリを入力します。
5. **Extended Community (拡張コミュニティ)** については、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 **Add (追加)** 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 個のエントリを入力します。
6. **OK** をクリックします。

STEP 4 | ルートを再配信するプロトコルを選択し、それらのルートの属性を設定します。

このタスクは、ルートを BGP に再配信する方法を示しています。

1. **Network (ネットワーク)** > **Virtual Routers (仮想ルーター)** を選択し、さらに仮想ルーターを選択します。
2. **BGP** > **Redist Rules (再配信ルール)** を選択します。
3. ファイアウォールがデフォルト ルートを再配信できるようにするには、**Allow Redistribute Default Route (デフォルト ルートの再配信を許可)** を選択します。
4. **Add**（追加）をクリックします。
5. **Address Family Type (アドレス ファミリーの種類)** を選択します。**IPv4** あるいは **IPv6**。再配信されたルートをどのルートテーブルに追加するのかを指定します。
6. 作成した再配信プロファイルの **Name (名前)** を選択（再配信するルートを選択）します。
7. 再配信ルールを **Enable (有効化)** します。
8. （任意）再配信されるルートにファイアウォールが適用する、次の値を入力します。
   - 範囲 1〜65,535 の **Metric (メトリック)**。
   - **Set Origin (発信元の設定)**—ルートの発信元： **igp**、**egp**、または**incomplete**。
   - **Set MED (MED の設定)**—MED の値、範囲は 0〜4,294,967,295 です。
   - **Set Local Preference (ローカル優先項目の設定)**—ローカル優先値、範囲は 0〜4,294,967,295 です。
   - **Set AS Path Limit (AS パス制限の設定)**—AS_PATH 内の AS の最大数、範囲は 1〜255 です。
   - **Set Community (コミュニティの設定)**—10 進数または 16 進数で 32 ビットの値を選択あるいは入力するか、AS:VAL のフォーマットで値を入力します。AS と VAL はそれぞれ 0 から 65,525 までの範囲の値です。最大 10 個のエントリを入力します。
   - **Set Extended Community (拡張コミュニティの設定)**—拡張コミュニティとして、16 進数、TYPE:AS:VAL または TYPE:IP:VAL のフォーマットで 64 ビットの値を入力あるいは選択します。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 個のエントリを入力します。
9. **OK** をクリックします。

STEP 5 | 変更を **Commit (コミット)** します。

GRE トンネル

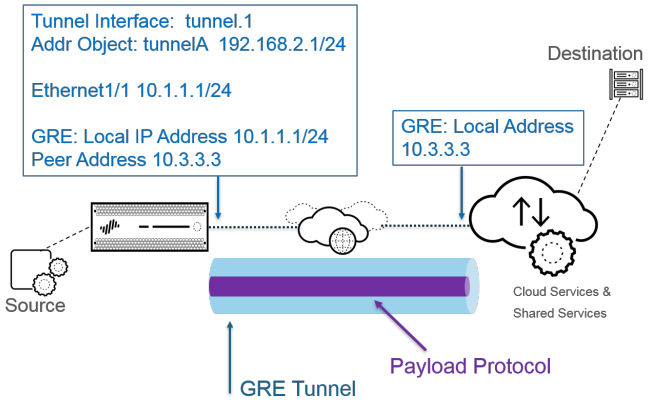
Generic Routing Encapsulation(ジェネリックルーティングカプセル化（GRE）)トンネル プロトコルは、ペイロードのプロトコルをカプセル化するキャリア プロトコルです。GRE パケット自体が転送プロトコル（IPv4 あるいは IPv6）内でカプセル化されます。

GRE トンネルの概要

Generic Routing Encapsulation (GRE) トンネルは、ポイントツーポイントの論理リンクで 2 つのエンドポイント（ファイアウォールと他のアプリケーション）に接続します。ファイアウォールは GRE トンネルを終了できます。ユーザーはパケットを GRE トンネルにルーティングあるいは転送できます。使用しやすい GRE トンネルは、特にクラウド上のサービスやパートナーのネットワークにポイントツーポイントで接続する際によく選ばれるトンネル プロトコルです。

例えばクラウドベースのプロキシあるいはパートナーのネットワークなど、IP アドレスが特定のポイントツーポイントのパスを取ることができるよう、パケットを宛先に向かわせる際にGRE トンネルを作成します。パケットは宛先アドレスに向かう途中にクラウドサービスに向かって GRE トンネルを介して移動します (インターネットなどのトランジット ネットワークを介して)。これにより、クラウドサービスはそのサービスやポリシーをパケットに適用できます。

次の図は、インターネットを介してファイアウォールをクラウドサービスに接続する GRE トンネルの例です。



最高のパフォーマンスを確保し、単一点におけるエラーを回避するために、単一のトンネルを使用するのではなく、ファイアウォールへの複数の接続を複数の *GRE* トンネルに分散させます。各 *GRE* トンネルでトンネル インターフェイスが必要になります。

ファイアウォールがパケットが通過することを許可 (ポリシー マッチに基づき) し、パケットが GRE トンネル インターフェースに向かって離れる際、ファイアウォールは GRE カプセル化を追加します。セッションは生成しません。ファイアウォールは GRE でカプセル化されたトラフィックに対してセキュリティポリシー ルールの検索を行わないため、ファイアウォールがカプセル化する GRE トラフィックではセキュリティポリシー ルールが不要です。しかし、GRE トラフィックを受け取る際、ファイアウォールはセッションを生成してカプセル化されたトラフィックに加えてすべてのポリシーを GRE IP ヘッダーに付与します。ファイアウォールは受信した GRE パケットを他のパケットと同様に扱います。そのため：

- GRE トンネルに紐付けられたトンネル インターフェイスと同じゾーンを持つインターフェイス上で (例：tunnel.1) ファイアウォールが GRE パケットを受信する場合、送信元ゾーンは宛先ゾーンと同じになります。デフォルト設定ではゾーン内 (イントラゾーン トラフィック) でトラフィックが許可されるため、入口 GRE トラフィックはデフォルトで許可されます。

- しかし、独自のイントラゾーンのセキュリティポリシー ルールを設定してそのようなトラフィックを拒否する場合、明示的に GRE トラフィックを許可する必要があります。
- 同様に、GRE トンネルに紐付けられたトンネル インターフェイスのゾーン (例：tunnel.1) が入力インターフェイスのゾーンと異なる場合、セキュリティポリシー ルールを設定して GRE トラフィックを許可する必要があります。

ファイアウォールは GRE パケット内にトンネル パケットをカプセル化するため、GRE ヘッダーに 24 byte (バイト)を加えることで、自動的に最大転送単位 (MTU) で最大セグメント サイズ (MSS：Maximum Segment Size)が小さくなります。インターフェースの IPv4 MSS 調整サイズを変更しない場合、ファイアウォールはデフォルトで MTU を 64 byte (バイト)分減らします (IP ヘッダー 40 byte (バイト) + GRE ヘッダー 24 byte (バイト))。つまり、デフォルトの MTU が 1,500 byte (バイト)の場合、MSS は 1,436 byte (バイト)になります (1,500 - 40 - 24 = 1,436)。例えば、MSS 調整サイズを 300 byte (バイト)に設定する場合、は MSS はたった 1,176 byte (バイト)になります (1,500 - 300 - 24 = 1,176)。

ファイアウォールは GRE または IPSec トンネルを GRE トンネルにルーティングすることをサポートしていませんが、GRE トンネルを IPSec トンネルにルーティングできます。補足：

- GRE トンネルは QoS をサポートしていません。
- ファイアウォールは GRE トンネル エンドポイントおよび復号化ブローカーの両方として機能する単一のインターフェイスをサポートしていません。
- GRE トンネルは GRE トンネル エンドポイント間の NAT をサポートしていません。

他のベンダーのネットワークに接続する必要がある場合は、*GRE* トンネルではなく、IPSec トンネル を設定することをお勧めします。*GRE* トンネルは、ベンダーがサポートする唯一のポイントツーポイント トンネル メカニズムである場合にのみ使用してください。また、リモート エンドポイントによって求められる場合（***Add GRE Encapsulation***（***GRE*** カプセル化を追加））は、*GRE over IPSec* を有効化することもできます。*IPSec* がトラフィックを暗号化する前に、リモートエンドポイントでトラフィックを *GRE* トンネル内にカプセル化する必要がある場合は、*GRE* カプセル化を追加します。例えば、一部の実装では、*IPSec* が暗号化する前にマルチキャストトラフィックをカプセル化する必要があります。これが必須の環境であり、*GRE* トンネルおよび *IPSec* トンネルが同じ *IP* アドレスを共有する場合は、*IPSec* トンネルをセットアップする際に ***Add GRE Encapsulation (GRE*** カプセル化を追加***)*** を行います。

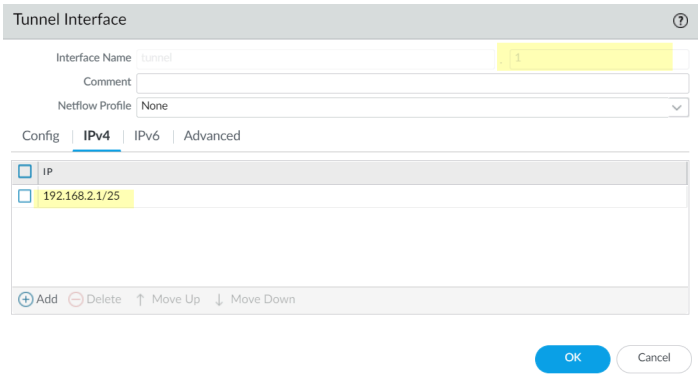
ファイアウォールを *GRE* トンネルの終着点にする予定はなく、*GRE* トンネル内でファイアウォールを通過するトラフィックを検査・制御したい場合は、*GRE* トンネルを作成しないでください。その代わりに、*GRE* トラフィックのTunnel Content Inspection（トンネル コンテンツ検査）を行います。トンネル コンテンツ検査では、トラフィックを転送するためのポイントツーポイントの論理リンクを作成するのではなく、ファイアウォールを通過する *GRE* トラフィックを検査してポリシーを適用します。

GRE トンネルの作成

Generic Routing Encapsulation (GRE) トンネルを作成し、ポイントツーポイントの論理リンクで 2 つのエンドポイントを接続します。

STEP 1 | トンネル インターフェイスを作成します。

1. **Network**（ネットワーク） > **Interfaces**（インターフェイス） > **Tunnel (トンネル)**を選択します。
2. トンネルを **Add (追加)** し、トンネル **Interface Name (インターフェース名)** にピリオドと数字を入力します (範囲は 1 ～ 9999)。例：**`tunnel.1`**
3. **Config (設定)** タブで、**Virtual Router (仮想ルーター)** にインターフェイスを割り当てます。
4. 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場合、トンネルインターフェイスを **Virtual System (仮想システム)** に割り当てます。
5. トンネルインターフェイスを **Security Zone (セキュリティ ゾーン)** に割り当てます。



6. IP アドレスをトンネルインターフェイスに割り当てます。(このトンネルにルーティングするか、トンネルエンドポイントを監視する場合は、IP アドレスを割り当てる必要があります。) **IPv4** または **IPv6** を選択するか、あるいは両方を設定します。

   このアドレスとピアのトンネルインターフェイスの対応するアドレスは、ポイント ツー ポイントの論理リンクであるため、同じサブネット上にある必要があります。

   - （IPv4 のみ）**IPv4** タブで、IPv4 アドレスを **Add**（追加）するか、アドレスオブジェクトを選択するか、**New Address**（新しいアドレス）をクリックしてアドレスの **Type**（タイプ）を指定し、入力します。例えば、**`192.168.2.1`** と入力します。
   - （IPv6 のみ）**IPv6** タブで **Enable IPv6 on the interface (インターフェイスでの IPv6 の有効化)** を選択します。
     1. **Interface ID (インターフェイス ID)** の場合、**EUI-64 (default 64-bit Extended Unique Identifier) (EUI-64 (デフォルトの 64 ビット拡張一意識別子))** を選択します。
     2. 新しい **Address (アドレス)** を **Add (追加)** するか、IPv6 アドレスオブジェクトを選択するか、または **New Address (新しいアドレス)** をクリックしてアドレスの

Name (名前) を指定します。**Enable address on interface** (インターフェイス上でアドレスを有効化) を選択して **OK** をクリックします。

3. アドレスの **Type**（タイプ）を選択し、IPv6 アドレスまたは FQDN を入力し、**OK** をクリックし新しいアドレスを保存します。
4. **Enable address on interface** (インターフェイス上でアドレスを有効化) を選択して**OK** をクリックします。

7. **OK** をクリックします。

STEP 2 | GRE トンネルを作成して、パケットが特定のポイントツーポイントパスを通るようにします。

1. **Network** (ネットワーク) > **GRE Tunnels** (GRE トンネル) を選択してトンネルを **Name** (名前) で **Add** (追加) します。
2. ローカル GRE トンネル エンドポイント（ソース インターフェース）（イーサネット インターフェースあるいはサブインターフェース）、集約イーサネット（AE）インターフェース、ループバック インターフェース、あるいは VLAN インターフェースとして使用する**Interface**（インターフェース）を選択します。
3. **IP** にする **Local Address** (ローカルアドレス) を選択し、選択したインターフェイスの IP アドレスを選択します。
4. **Peer Address** (ピアアドレス) を入力します。これは GRE トンネルの反対側にあるエンドポイントの IP アドレスです。
5. ステップ 1 で作成した **Tunnel Interface** (トンネルインターフェイス) を選択します。(これは、トンネルがルーティングの出力 **Interface** (インターフェイス) である場合に特定します。)
6. 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）。
7. **Copy ToS Header** (**ToS** ヘッダーのコピー) を選択して、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。ネットワークで QoS を使用し、QoS ポリシーを適用するために ToS ビットに依存している場合は、このオプションを選択します。

STEP 3 | (ベストプラクティス) GRE トンネルのキープアライブ機能を有効にします。

> 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 (再試行) を受け取り、*GRE* トンネルが復帰する際は *10* 秒間隔で *5* つのホールドタイマー間隔を受け取ります。

1. **Keep Alive (**キープアライブ**)** を選択して、GRE トンネルのキープアライブ機能を有効にします (デフォルトは無効です)。
2. (任意) GRE トンネルのローカルエンド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 **Interval (sec) (**間隔 **(**秒**))** (秒単位) を設定します。これは、**Hold Timer (**ホールドタイマー**)** を掛けたときに、GRE トンネルが回復するまでにファイアウォールが正常なキープアライブパケットを確認しなければならない時間の長さでもあります (範囲は 1 ～ 50、デフォルトは 10)。設定する間隔が小さすぎると、環境では不要なキープアライブパケットが多数発生し、追加の帯域幅と処理が必要になります。間隔を大きくしすぎると、エラー状態がすぐに識別されない可能性があるため、フェイルオーバーが遅れる可能性があります。
3. (任意) **Retry (**再試行**)** 設定を入力します。これは、ファイアウォールがトンネルピアのダウンを考慮するまでにキープアライブパケットが返されないIntervals (間隔)の数です (範囲は 1 ～ 255、デフォルトは 3)。トンネルがダウンすると、ファイアウォールはトンネルに関連付けられたルートを転送テーブルから削除します。再試行設定を構成すると、実際にダウンしていないトンネルでの対策を回避できます。
4. (任意) **Hold Timer (**ホールドタイマー**)** を設定します。これはキープアライブパケットが成功する **Intervals (**間隔**)** の数です。その後、ファイアウォールはトンネルピアとの通信を再確立します (範囲は 1 ～ 64、デフォルトは 5)。

STEP 4 | **OK** をクリックします。

STEP 5 | GRE トンネル経由で宛先にトラフィックをルーティングするために、ルーティングプロトコルまたは静的ルートを設定します。例えば、 スタティック ルートの設定宛先サーバーのネットワークに、出口 **Interface (**インターフェース**)** をローカルトンネルエンドポイント (tunnel.1) に指定します。ネクストホップを、反対側のトンネルの IP アドレスに設定します。例：192.168.2.3

STEP 6 | 変更をコミットします。

STEP 7 | パブリック IP アドレス、ローカル IP アドレスとピア IP アドレス (ファイアウォール上の GRE トンネルのピア IP アドレスとローカル IP アドレスにそれぞれ対応します)、およびルーティングプロトコルまたは静的ルートを使用して、トンネルの反対側を設定します。

STEP 8 | ファイアウォールが GRE トンネルを介してトンネルピアと通信できることを確認します。

1. CLI へのアクセスを行います。
2. > **ping source192.168.2.1 host192.168.2.3**

DHCP

このセクションでは、Dynamic Host Configuration Protocol (DHCP) と、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する Palo Alto Networks® ファイアウォール上のインターフェイスを構成するために必要なタスクについて説明します。これらのロールを異なるインターフェイスに割り当てることで、ファイアウォールで複数の役割を実行できます。

DHCP の概要

DHCP は、RFC 2131、 Dynamic Host Configuration Protocol（英語）で定義されている、標準化プロトコルです。DHCP の主な目的は 2 つあります。1 つは、TCP/IP およびリンク層の設定パラメータを提供することで、もう 1 つは、TCP/IP ネットワーク上に動的に設定されるホストにネットワーク アドレスを提供することです。

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。このモデルにはデバイス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）として機能するデバイスは、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 デバイスのユーザーは、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デバイスは、クライアントにサービスを提供できます。3 つのDHCP アドレスメカニズムのいずれかを使用することで、ネットワーク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 アドレスや多くの DHCP オプションを多数のクライアントに配信できます。
- DHCP リレー エージェントとして機能するデバイスは、DHCP クライアントと DHCP サーバー間で DHCP メッセージを送信できます。

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 67 （UDP – ブートストラップ プロトコルおよび DHCP）DHCP メッセージに送信されます。

Palo Alto Networks ®ファイアウォール上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 エージェントの役割を果たすことができます。DHCP サーバーまたはリレー エージェントのインターフェイスは、レイヤー 3 Ethernet、集約された Ethernet、レイヤー 3 VLAN インターフェイスである必要があります。ロールの組み合わせに合った適切な設定で、ファイアウォールのインターフェイスを設定します。各ロールの動作の要約は、「DHCP サーバーおよびクライアントとしてのファイアウォール」を参照してください。

ファイアウォールでは、DHCPv4 サーバーと DHCPv6 リレーがサポートされています。

Palo Alto Networks の DHCP サーバーおよび DHCP クライアントの実装では、IPv4 アドレスのみをサポートしています。DHCP リレーの実装では、IPv4 と IPv6 をサポートしています。高可用性アクティブ/アクティブ モードでは、DHCP クライアントはサポートされていません。

DHCP サーバーおよびクライアントとしてのファイアウォール

ファイアウォールは、DHCP サーバーおよび DHCP クライアントとして機能することができます。Dynamic Host Configuration Protocol、RFC 2131 は、IPv4 および IPv6 アドレスをサポートするように設計されています。PAlo Alto Networks® DHCP サーバーの実装では、IPv4 アドレスのみがサポートされています。

ファイアウォール DHCP サーバーは、以下のように動作します。

- DHCP サーバーがクライアントから DHCPDISCOVER メッセージを受信すると、サーバーは、設定に表示される順序ですべての事前定義済みオプションおよびユーザー定義のオプションが含まれる DHCPOFFER メッセージで応答します。クライアントは、必要なオプションを選択し、DHCPREQUEST メッセージで応答します。
- サーバーがクライアントから DHCPREQUEST メッセージを受信すると、サーバーは、要求で指定されたオプションのみが含まれる DHCPACK メッセージで応答します。

ファイアウォール DHCP クライアントは、以下のように動作します。

- DHCP クライアントがサーバーから DHCPOFFER を受信すると、DHCPREQUEST で送信されたオプションかどうかに関係なく、クライアントは後で使用できるように、提供されたすべてのオプションを自動的にキャッシュします。
- デフォルトでは、コードの複数の値を受信した場合、クライアントはメモリ消費量を抑えるために各オプション コードの最初の値のみをキャッシュします。
- DHCP クライアントが DHCPDISCOVER または DHCPREQUEST メッセージのオプション 57 で最大値を指定していない限り、DHCP メッセージに最大長はありません。

DHCP メッセージ

DHCP では、DHCP メッセージのオプション タイプ番号で識別される 8 個の標準メッセージ タイプが使用されます。たとえば、クライアントが DHCP サーバーを検索する場合、そのローカル物理サブネットワークで DHCPDISCOVER メッセージをブロードキャストします。そのサブネットに DHCP サーバーがない場合、DHCP ヘルパーや DHCP リレーが適切に設定されていれば、メッセージが別の物理サブネットの DHCP サーバーに転送されます。そうでない場合、メッセージは送信元のサブネットまでしか進みません。1 つ以上の DHCP サーバーが DHCPOFFER メッセージで応答します。このメッセージには、使用可能なネットワーク アドレスとその他の設定パラメータが含まれています。

クライアントで IP アドレスが必要になると、DHCPREQUEST を 1 つ以上のサーバーに送信します。クライアントが IP アドレスを要求する場合、まだ IP アドレスは割り当てられていないため、RFC 2131 では、クライアントが送信するブロードキャスト メッセージに、IP ヘッダーが 0 の送信元アドレスを設定することが求められています。

クライアントがサーバーに設定パラメータを要求する場合、複数のサーバーから応答を受信する可能性があります。クライアントがその IP アドレスを受信すると、少なくとも IP アドレスが（場合によってはその他の設定パラメータも）クライアントにバインドされます。DHCP サーバーは、このようなクライアントへの設定パラメータのバインドを管理します。

以下の表に、DHCP メッセージを示します。

DHCP メッセージ	説明
DHCPDISCOVER	使用可能な DHCP サーバーを検索するクライアント ブロードキャスト。
DHCPOFFER	クライアントの DHCPDISCOVER へのサーバー応答。設定パラメータを提供します。
DHCPREQUEST	1 つ以上のサーバーへのクライアント メッセージで、以下のいずれかを実行します。 • 1 つのサーバーにパラメータを要求し、暗黙的にその他のサーバーからのオファーを拒否します。 • システムの再起動後などに、以前に割り当てられたアドレスが正しいことを確認します。 • ネットワーク アドレスのリースを延長します。
DHCPACK	確認済みのネットワーク アドレスなどの設定パラメータが含まれている、サーバーからクライアントへの肯定応答メッセージ。
DHCPNAK	クライアントのネットワーク アドレスの認識が正しくない（クライアントが新しいサブネットに移動した場合など）、またはクラ

DHCP メッセージ	説明
	イアントのリースの有効期限が切れていることを示す、サーバーからクライアントへの否定応答。
DHCPDECLINE	ネットワーク アドレスがすでに使用されていることを示す、クライアントからサーバーへのメッセージ。
DHCPRELEASE	ネットワーク アドレスのユーザーを放棄し、リースの残り時間をキャンセルする、クライアントからサーバーへのメッセージ。
DHCPINFORM	ローカル設定パラメータのみを要求する、クライアントからサーバーへのメッセージ。クライアントには、外部で設定されたネットワーク アドレスが割り当てられます。

DHCP アドレス

DHCP アドレスの割り当て方法

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。DHCP のリースセクションを参照してください。
- **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 割り当ては永久的です。これを行うには、DHCP サーバーを設定し、クライアント デバイスの **[MAC** アドレス**]** に対応するように **[**予約済みアドレス**]** を選択します。DHCP の割り当ては、クライアントがログオフまたは再起動したり、停電が発生したりしても、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 デバイスが何か重要な用途で使用されていて、デバイスがオフになったり、再起動したり、プラグが抜かれたり、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。

  [予約済みアドレス**]** を設定する場合、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、どのデバイスにも **[**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 のリース

リースは、DHCP サーバーがネットワーク アドレスをクライアントに割り当てる期間として定義されます。リースは、後続の要求で延長（更新）できます。クライアントでアドレスが不要になった場合、リース期間が終了する前にアドレスをサーバーにリリースすることができます。その後、サーバーは、未割り当てアドレスがなくなった場合に、別のクライアントにそのアドレスを自由に割り当てることができます。

DHCP サーバーに設定されたリース期間は、単一の DHCP サーバー（インターフェイス）がクライアントに動的に割り当てるすべてのアドレスに適用されます。つまり、動的に割り当てられるすべてのインターフェイスのアドレスは、**[無制限]** の期間または同じ **[タイムアウト]** 値になります。ファイアウォールに設定された別の DHCP サーバーに、異なるクライアント リース期間を割り当てることができます。**[予約済みアドレス]** は、静的なアドレス割り当てで、リース期間は適用されません。

DHCP 標準、RFC 2131 に準拠して、DHCP クライアントはリースの有効期限が切れるまで待機しません。これは、新しいアドレスが割り当てられるリスクがあるためです。代わりに、DHCP クライアントがリース期間の半分に達すると、同じ IP アドレスを保持できるようにそのリースを延長しようとします。そのため、リース期間はスライディング ウィンドウのようになります。

通常、IP アドレスがデバイスに割り当てられた後に、デバイスがネットワークから切断された場合、そのリースが延長されていないと、DHCP サーバーはそのリースを使い切ります。クライアントがネットワークから切断されて、そのアドレスが不要になるため、サーバーのリース期間に達すると、リースは Expired （失効）状態になります。

ファイアウォールには、有効期限の切れた IP アドレスがすぐに再割り当てされないようにする保留タイマーがあります。この動作では、デバイスがネットワークに戻った場合に備えてデバイスのアドレスが一時的に予約されます。ただし、アドレス プールのアドレスがなくなると、保留タイマーの有効期限が切れる前に、サーバーはこの有効期限の切れたアドレスを再割り当てします。有効期限の切れたアドレスは、システムで追加のアドレスが必要になったときや、保留タイマーでリリースされたときに自動的にクリアされます。

割り当てられた IP アドレスに関するリース情報を表示するには、CLI で **show dhcp server lease** 操作コマンドを使用します。有効期限の切れたリースが自動的にリリースされるまで待機しないようにする場合は、**clear dhcp lease interface *<interface>* expired-only** コマンドを使用して、有効期限の切れたリースをクリアします。これにより、それらのアドレスがプールで再度使用できるようになります。特定の IP アドレスをリリースするには、**clear dhcp lease interface *<interface>* ip *<ip_address>*** コマンドを使用します。特定の MAC アドレスをリリースするには、**clear dhcp lease interface *<interface>* mac *<mac_address>*** コマンドを使用します。

DHCP オプション

DHCP および DHCP の歴史は、ブートストラップ プロトコル（BOOTP）まで遡ります。BOOTP は、ホストの起動手順でホスト自体を動的に設定するために使用されていました。ホストは、サーバーから起動プログラムをダウンロードするための IP アドレスとファイル、およびサーバーのアドレスとインターネット ゲートウェイのアドレスを受信できました。

BOOTP パケットには、ベンダー情報フィールドがあり、さまざまなタイプの情報（サブネット マスク、BOOTP ファイル サイズ、およびその他の多くの値など）が含まれる、タグ付けされた多数のフィールドを格納することができました。RFC 1497 には、BOOTP Vendor Information Extensions（英語）が記載されています。BOOTP は DHCP に置き換わっているため、BOOTP はファイアウォールではサポートされません。

これらの拡張は拡大していき、最終的には DHCP および DHCP ホスト設定パラメータ（オプションとも呼ばれる）が使用されるようになりました。ベンダー拡張と同じように、DHCP オプションは、DHCP クライアントに情報を提供する、タグ付けされたデータ項目です。オプションは、DHCP メッセージの最後に可変長フィールドで送信されます。たとえば、DHCP メッセージ タイプがオプション 53 で、値が 1 の場合、DHCPDISCOVER メッセージを示します。DHCP オプションは、RFC 2132、DHCP Options and BOOTP Vendor Extensions（英語）で定義されています。

DHCP クライアントは、サーバーとネゴシエートし、クライアントが要求するオプションのみをサーバーが送信するように制限できます。

- 事前定義済み DHCP オプション
- DHCP オプションの複数の値
- DHCP オプション 43、55、60 およびその他のカスタム オプション

事前定義済み DHCP オプション

Palo Alto Networks ® ファイアウォールは、DHCP サーバー実装でユーザー定義および定義済みの DHCP オプションをサポートします。このようなオプションは、DHCP サーバーで設定され、DHCPREQUEST をサーバーに送信したクライアントに送信されます。クライアントは、受け入れるようにプログラムされたオプションを継承して実装します。

ファイアウォールは、DHCP サーバーの以下の事前定義済みオプションをサポートしています。（**[DHCP** サーバー**]** 設定画面に表示される順序で記載）。

DHCP オプション	DHCP オプション名
51	リース期間
3	ゲートウェイ
1	IP プール サブネット（マスク）

DHCP オプション	DHCP オプション名
6	Domain Name System （DNS）サーバー アドレス（プライマリおよびセカンダリ）
44	Windows Internet Name Service （WINS）サーバー アドレス（プライマリおよびセカンダリ）
41	Network Information Service （NIS）サーバー アドレス（プライマリおよびセカンダリ）
42	Network Time Protocol （NTP）サーバー アドレス（プライマリおよびセカンダリ）
70	Post Office Protocol Version （POP3）サーバー アドレス
69	Simple Mail Transfer Protocol （SMTP）サーバー アドレス
15	DNS サフィックス

前述したように、ベンダー固有のオプションやカスタム オプションを設定することもできるため、IP 電話やワイヤレス インフラストラクチャ デバイスなどのさまざまなオフィス機器に対応できます。各オプション コードでは、複数の値（IP アドレス、ASCII、または 16 進数形式）がサポートされています。ファイアウォールの拡張 DCHP オプションがサポートされているため、ベンダー固有のオプションやカスタム オプションを DHCP クライアントに提供するために支社で独自の DHCP サーバーを購入して管理する必要はありません。

DHCP オプションの複数の値

同じ **Option Name** [オプション名]の **Option Code** [オプション コード]に複数のオプション値を入力できますが、特定のコードと名前の組み合わせの値はすべて同じタイプ（IP アドレス、ASCII、または 16 進数）にする必要があります。コードと名前の組み合わせが同じ場合、あるタイプが継承または入力されてから別のタイプが入力されると、2 番目のタイプで最初のタイプが上書きされます。

異なる **Option Name** [オプション名]を使用して、同じ **Option Code** [オプション コード]を複数回入力できます。この場合、Option Code [オプション コード]の **Option Type** [オプション タイプ]は、各オプションで異なっていても問題ありません。たとえば、オプション Coastal Server （オプション コード 6）が IP アドレス タイプで設定されている場合、ASCII タイプのオプション Server XYZ （オプション コード 6）も使用できます。

ファイアウォールは、オプションの複数の値を上から下の順序で（数珠つなぎに）クライアントに送信します。そのため、オプションに複数の値を入力する場合、優先順に値を入力するか、優先順になるようにリストのオプションを移動します。ファイアウォール設定のオプションの順序により、DHCPOFFER および DHCPACK メッセージに表示されるオプションの順序が決まります。

事前定義済みオプション コードとしてすでに存在するオプション コードを入力できます。カスタム オプション コードを使用すると、事前定義済み DHCP オプションがオーバーライドされます。このとき、ファイアウォールでは警告が表示されます。

DHCP オプション 43、55、60 およびその他のカスタム オプション

以下の表に、RFC 2132 で説明されているいくつかのオプションの動作を示します。

オプション コード	オプション名	オプションの説明 / 動作
43	ベンダー固有の情報	サーバーからクライアントに送信されます。DHCP サーバーからクライアントに提供するように設定されたベンダー固有の情報です。この情報は、サーバーのテーブルにあるベンダー クラス識別子（VCI）がクライアントの DHCPREQUEST の VCI と一致する場合にのみクライアントに送信されます。 オプション 43 パケットには、複数のベンダー固有の情報を含めることができます。また、カプセル化されたベンダー固有のデータ拡張子を含めることもできます。
55	パラメータ要求リスト	クライアントからサーバーに送信されます。DHCP クライアントが要求する設定パラメータ（オプション コード）のリストです。このリストは、クライアントの優先順になっている可能性があります。サーバーは、同じの順序でオプションに応答しようとします。
60	ベンダー クラス識別子（VCI）	クライアントからサーバーに送信されます。DHCP クライアントのベンダー タイプおよび設定です。DHCP クライアントは、DHCPREQUEST でオプション コード 60 を DHCP サーバーに送信します。サーバーがオプション 60 を受信すると、VCI を確認して、各自のテーブルで一致する VCI を検索し、その値（VCI に対応する値）と共にオプション 43 を返します。これにより、ベンダー固有の情報が正しいクライアントにリレーされます。クライアントとサーバーの両方で VCI が認識されます。

RFC 2132 で定義されていないベンダー固有のカスタム オプション コードを送信できます。オプション コードは、範囲が 1 ～ 254 で、固定長または可変長にすることができます。

カスタム *DHCP* オプションは *DHCP* サーバーによって検証されません。作成したオプションに正しい値が入力されていることを確認する必要があります。

ASCII および 16 進数の DHCP オプション タイプの場合、オプション値は最大 255 オクテットです。

DHCP サーバーとしてインターフェイスを設定する

このタスクの前提条件は以下のようになります。

- 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する。
- インターフェイスを仮想ルーターおよびゾーンに割り当てる。
- 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 プールを決定する。
- 設定する DHCP オプション、値、およびベンダー クラス識別子を収集する。

キャパシティは次の通りです：

- PA-5200 Series および PA-7000 Series ファイアウォール以外のファイアウォールモデルについては、Product Selection tool（製品選択ツール）を参照してください。
- PA-5220 Series のファイアウォールでは、最大 500 台の DHCP サーバーと、最大 2,048 台の DHCP リレー エージェントから設定された DHCP サーバーの数を差し引くことができます。たとえば、500 台の DHCP サーバーを設定する場合は、 1,548 台の DHCP リレーエージェントを設定できます。
- PA-5250、PA-5260 および PA-7000 Series のファイアウォールでは、最大 500 台の DHCP サーバーと、最大 4,096 台の DHCP リレー エージェントから設定された DHCP サーバーの数を差し引くことができます。たとえば、500 台の DHCP サーバーを設定する場合は、3,596 台の DHCP リレーエージェントを設定できます。

DHCP サーバーとして機能するようにファイアウォールのインターフェイスを設定するには、以下のタスクを実行します。

STEP 1 | DHCP サーバーにするインターフェイスを選択します。

1. **Network (ネットワーク)** > **DHCP** > **DHCP Server (サーバー)** を選択し、**Interface (インターフェイス)** の名前を **Add (追加)** するか、一つを選びます。
2. **[モード]** で、**[有効]** または **[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。
3. （任意）サーバーがクライアントに IP アドレスを割り当てる前に IP アドレスを ping する場合、**Ping IP when allocating new IP** [新しい IP を割り当てるときに IP に Ping する]を選択します。

   ping が応答を受信した場合は、すでに別のデバイスにそのアドレスが設定されているため、使用できないことを意味します。サーバーがプールから次のアドレスを割り当てます。この動作は、Optimistic Duplicate Address Detection (DAD) for IPv6、RFC 4429（英語）に似ています。

   オプションを設定して *DHCP Server [DHCP* サーバー*]*タブに戻ると、インターフェイスの ***Probe IP*** （プローブ *IP*）列に、***Ping IP when allocating new IP*** *[新しい IP* を割り当てるときに *IP* に *Ping* する*]*が選択されたかどうかが表示されます。

STEP 2 | サーバーがクライアントに送信する事前定義済み <95>DHCP オプション</95>を設定します。

- [オプション] セクションで、<100>[リース]</100> タイプを選択します。
- **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。
- <112>Timeout（タイムアウト）</112>により、リースの継続時間が決まります。**[日]** および **[時間]** の数値を入力し、必要に応じて **[分]** の数値を入力します。
- 継承ソース – **[なし]** のままにするか、各種サーバーの設定を DHCP サーバーに配信するソースの 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と、ファイアウォールはアップストリーム サーバーから DHCP クライアントで受信される DHCP オプションをすばやく追加できます。また、ソースでオプションが変更されても、クライアントのオプションを最新の状態にしておくこともできます。たとえば、ソースで NTP サーバー（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。

> 複数の *IP* アドレスが含まれる *DHCP* オプションを継承する場合、ファイアウォールは、オプションに含まれる最初の *IP* アドレスのみを使用して、キャッシュ メモリを節約します。*1* つのオプションに複数の *IP* アドレスが必要な場合、継承を設定する代わりにそのファイアウォールで直接 *DHCP* オプションを設定します。

- **Check inheritance source status** [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、このリンクをクリックすると、**Dynamic IP Interface Status** [ダイナミック IP インターフェイス状態]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 – 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。
- **Subnet Mask** [サブネット マスク] – **IP Pools** [IP プール]のアドレスと共に使用されるネットワーク マスク。

以下のフィールドの下向き矢印をクリックし、**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。<152>inherited（継承済み）</152>を選択する

と、DHCP サーバーはソース DHCP クライアントから、<153>Inheritance Source（継承ソース）</153>として指定された値を継承します。

- **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 Network Time Protocol サーバーの IP アドレス。
- **POP3 Server (POP3 サーバー)**—Post Office Protocol（POP3）サーバーの IP アドレス。
- **SMTP Server**（**SMTP** サーバー） — Simple Mail Transfer Protocol（SMTP）サーバーの IP アドレス。
- **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。

STEP 3 | （任意）DHCP サーバーがクライアントに送信するベンダー固有の DHCP オプションまたはカスタム DHCP オプションを設定します。

1. Custom DHCP Options (カスタム DHCP オプション) セクションで、DHCP オプションを識別する分かりやすい **Name (名前)** を **Add (追加)** します。
2. サーバーから提供されるように設定する **Option Code (オプション コード)** を入力します（範囲は 1 ～254）。（オプション コードについては、RFC 2132 を参照してください）
3. <203>Option Code</203> [オプション コード]が <204>43</204> の場合、<205>Vendor Class Identifier</205> [ベンダー クラス識別子]フィールドが表示されます。文字列または 16 進数値（0x のプレフィックスが付いている）の VCI を入力します。この値は、オプション 60 が含まれるクライアント要求の値と照合されます。サーバーは、テーブルで受信 VCI を探して見つけ、オプション 43 および対応するオプション値を返します。
4. **Inherit from DHCP server inheritance source (DHCP サーバーの継承ソースから継承)**—DHCP サーバーの事前定義済みオプションの **Inheritance Source (継承ソース)** を指定しており、ベンダー固有のオプションまたはカスタム オプションもこのソースから **inherited (継承済み)** する場合にのみ選択します。
5. **Check inheritance source status** [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、このリンクをクリックすると、**Dynamic IP Interface Status** [ダイナミック IP インターフェイス状態]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。
6. **Inherit from DHCP server inheritance source** [DHCP サーバーの継承ソースから継承]を選択しなかった場合、**Option Type** [オプション タイプ]を次のいずれかから選択します。**IP Address** [IPアドレス]、**ASCII**、あるいは**Hexadecimal** [16進数]。16 進数値は、0x のプレフィックスで始まる必要があります。

7. その **Option Code** [オプション コード]に対して DHCP サーバーから提供される **Option Value** [オプション値]を入力します。複数の値を 1 行ずつ入力できます。
8. **OK** をクリックします。

STEP 4 | （任意）別のベンダー固有の DHCP オプションまたはカスタム DHCP オプションを追加します。

1. 前のステップを繰り返し、もう一つのカスタム DHCP オプションを入力します。
   - 同じ **Option Name** [オプション名]の **Option Code** [オプション コード]に複数のオプション値を入力できますが、**Option Code** [オプション コード]の値はすべて同じタイプ（**IP Address** [IP アドレス]、**ASCII**、または **Hexadecimal** [16 進数]）にする必要があります。**Option Code** （オプション コード）と **Option Name** [オプション名]が同じ場合、あるタイプが継承または入力されてから別のタイプが入力されると、2 番目のタイプで最初のタイプが上書きされます。

     オプションに複数の値を入力する場合、優先順に値を入力するか、優先順になるようにリストのカスタム DHCP オプションを移動します。オプションを選択して <266>Move Up (上へ)</266> または <267>Move Down (下へ)</267> をクリックします。
   - 異なる **Option Name** [オプション名]を使用して、同じ **Option Code** [オプション コード]を複数回入力できます。この場合、Option Code [オプション コード]の **Option Type** [オプション タイプ]は、各オプションで異なっていても問題ありません。
2. **OK** をクリックします。

STEP 5 | DHCP サーバーがアドレスを選択するために使用する IP アドレスのステートフル プールを特定し、DHCP クライアントに割り当てます。

該当のネットワークのネットワーク管理者でない場合、*DHCP* サーバーで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 プールをネットワーク管理者に問い合わせてください。

1. **IP Pools (IP プール)** フィールドで、このサーバーがクライアントに割り当てる IP アドレスの範囲を **Add (追加)** します。IP サブネットとサブネット マスク（たとえば、192.168.1.0/24）、または IP アドレスの範囲（たとえば、192.168.1.10-192.168.1.20）を入力します。
   - 動的IPアドレスの割り当ての場合はIP プールあるいは<306>Reserved Address</306> [予約済みアドレス]が必須です。
   - 割り当てる静的IPアドレスが、ファイアウォールのインターフェイスが運転するサブネット内にある場合は、静的IPアドレス用のIP プールは必須項目ではありません。
2. （任意）このステップを繰り返し、別の IP アドレス プールを指定します。

STEP 6 | （任意）動的に割り当てない、IP プールの IP アドレスを指定します。**[MAC** アドレス**]** も指定すると、デバイスが DHCP を使用して IP アドレスを要求したときに **[**予約済みアドレス**]** がそのデバイスに割り当てられます。

> ***Reserved Address (***予約済みアドレス**)** の割り当ての説明は、DHCP アドレスセクションを参照してください。

1. **Reserved Address (**予約済みアドレス**)** フィールドで **Add (**追加**)** をクリックします。
2. **[IP** プール**]** から、DHCP サーバーに動的に割り当てない IP アドレス（*x.x.x.x* の形式）を入力します。
3. （任意）先ほど指定した IP アドレスを永久的に割り当てるデバイスの **MAC Address (MAC** アドレス**)**（*xx:xx:xx:xx:xx:xx* の形式）を入力します。
4. （任意）前の 2 つのステップを繰り返し、別のアドレスを予約します。

STEP 7 | 変更をコミットします。

OK、**Commit (**コミット**)** の順にクリックします。

DHCP クライアントとしてインターフェイスを設定する

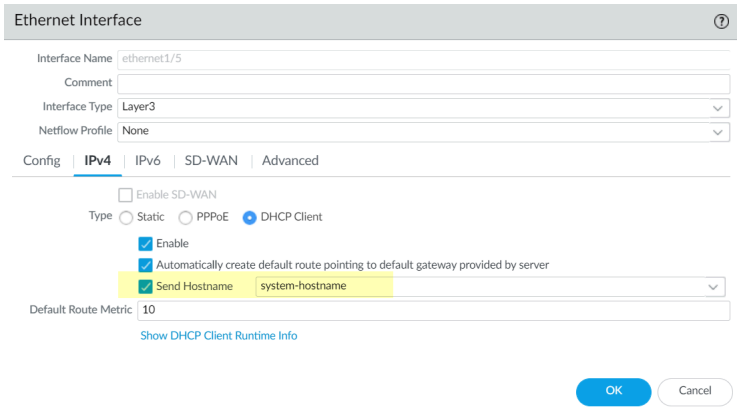
DHCP クライアントとしてファイアウォール インターフェースを設定する前に、レイヤー 3 インターフェース (イーサネット、イーサネット サブインターフェース、VLAN、VLAN サブインターフェース、集約、あるいは集約サブインターフェース) が設定されていることと、インターフェースが仮想ルーターおよびゾーンに割り当てられていることを確認します。DHCP を使用してインターフェースの IPv4 アドレスを要求する必要がある場合、DHCP クライアントとしてインターフェースを設定します。

また、DHCP クライアントとして管理インターフェイスを設定することもできます。

STEP 1 | DHCP クライアントとしてインターフェイスを設定します。

1. **Network (ネットワーク)** > **Zones (ゾーン)** の順に選択します。
2. **Ethernet (イーサネット)** タブあるいは **VLAN** タブで、DHCP クライアントにしたい設定済みのレイヤー 3 インターフェースを選択、あるいはレイヤー 3 インターフェースを **Add (追加)** します。
3. **IPv4**タブを選択し、**Type**（タイプ）で**DHCP** クライアントを選択します。
4. **Enable**[有効] を選択します。
5. （任意）**Automatically create default route pointing to default gateway provided by server(サーバーが提供するデフォルト ゲートウェイを指すデフォルト ルートを自動的に作成)**のオプションを有効にします(デフォルトで有効)。 このオプションを有効にすると、ファイアウォールはデフォルト 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 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。
6. (任意)**Send Hostname (ホスト名を送信)**のオプションを有効にして DHCP クライアント インターフェー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 サーバーに送信し、それからホスト名を DNS サーバーに登録させます。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ファ

イアウォールのホスト名です。あるいは、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 文字でホスト名を入力することができます。



7. （任意）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（範囲は 1 ～ 65535、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。

   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）は、デフォルトで*10*です。スタティック デフォルト ルート *0.0.0.0/0* が出力インターフェースとして *DHCP* インターフェースを使用する場合、そのルートのデフォルト ***Metric***（メトリック） も*10*です。したがって、*10* のメトリックを持つ *2* つのルートがあり、ファイアウォールは一方のルートをランダムに選択し、もう一方のルートは別のタイミングで選択できます。

   サーバーが提供するデフォルト ゲートウェイを指すデフォルト ルートを自動的に作成のオプションを有効にし、*Virtual Router (* 仮想ルーター *- VR)*を選択し、レイヤー *3* インターフェースのスタティック ルートを追加し、***Metric***（メトリック）（デフォルトは *10*）を *10* より大きい値（この例では *100*）に変更し、変更をコミットします。ルート テーブルでは、ルートのメトリックは *100* を示しません。代わりに、設定値 *100* よりも *10* が優先されるため、期待どおりにデフォルト値の *10* を示します。ただし、スタティック ルートの ***Metric***（メトリック）を *10* 未満の値（*6* など）に変更する場合、ルート テーブルのルートが更新され、設定されたメトリック *6* を示します。

8. （任意）**Show DHCP Client Runtime Info**（**DHCP** クライアント ランタイム情報の表示）のオプションを有効にし、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確認します。

STEP 2 | 変更をコミットします。

OK、**Commit (**コミット**)** の順にクリックします。

Ethernet インターフェースは、**Ethernet**（イーサネット） タブにある **IP Address**（**IP** アドレス）としてダイナミック **- DHCP** クライアントを表示します。

STEP 3 | （任意）ファイアウォールのどのインターフェイスが DHCP クライアントとして設定されているのかを確認します。

1. **Network (**ネットワーク**)** > **Interfaces (**インターフェース**)** > **Ethernet (**イーサネット**)** の順に選択し、**IP** アドレスを確認して、どのインターフェースが DHCP クライアントとして表示されているのかを確認します。
2. **Network (**ネットワーク**)** > **Interfaces (**インターフェース**)** > **VLAN** を選択し、**IP** アドレスを確認して、どのインターフェイスが DHCP クライアントを表示しているかを確認します。

DHCP クライアントとして管理インターフェイスを設定する

ファイアウォールの管理インターフェイスはIPv4用のDHCPクライアントをサポートしているため、管理インターフェイスはDHCPサーバーから自身のIPv4アドレスを受信できます。また、管理インターフェイスはDHCP Option 12およびOption 61もサポートしているため、ファイアウォールは自身のホスト名およびクライアントIDをそれぞれDHCPサーバーに送信することができます。

デフォルト設定ではAWSおよびAzure™にデプロイされたVM-Seriesファイアウォールは管理インターフェイスをDHCPクライアントとして使用し、静的IPアドレスではなく自身のIPアドレスを取得します。これは、クラウドのデプロイ環境ではこの機能によって自動化を行う必要があるからです。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。WildFire および Panorama モデル上の管理インターフェイスはこの DHCP 機能をサポートしていません。

- ハードウェアベースのファイアウォール モデル（*VM-Series*ではない）の場合、可能な限り管理インターフェイスを静的*IP*アドレスを使用して設定します。
- ファイアウォールが管理インターフェイスのアドレスを*DHCP*を介して取得する場合、そのファイアウォールを扱う*DHCP*サーバー上の*MAC*アドレスの予約を割り当てます。この予約により、ファイアウォールが再起動後も管理*IP*アドレスを確実に維持できるようになります。*DHCP* サーバーが *Palo Alto Networks* ® ファイアウォールである場合は、手順 *6/* アドレスを予約するための DHCP サーバー としてインターフェイスを構成するを参照してください。

管理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、次の制限がかかってきます。

- 制御リンク（HA1あるいはHA1バックアップ）、データリンク（HA2あるいはHA2バックアップ）、あるいはパケット転送（HA3）通信では、HA構成の管理インターフェイスを使用できません。
- サービスルートをカスタマイズする際（**Device (**デバイス**)** > **Setup (**セットアップ**)** > **Services (**サービス**)** > **Service Route Configuration (**サービスルート設定**)** > **Customize (**カスタマイズ**)**）は Source Interface (ソース インターフェイス) として **MGT** を選択できません。しかし、**Use default** [デフォルトを使用]を選択し、管理インターフェイスを介してパケットのルーティングを行うことができます。
- 管理インターフェイスの動的 IP アドレスを使用してハードウェア セキュリティ モジュール（HSM）に接続することはできません。HSM は IP アドレスを使用してファイアウォールを認証し、実行中に IP アドレスが変更されると HSM は停止してしまうため、HSM クライアント ファイアウォールの IP アドレスは静的 IP アドレスでなければなりません。

管理インターフェイスがDHCPサーバーにアクセスできることがこの作業の前提条件となります。

STEP 1 | 管理インターフェイスをDHCPクライアントとして設定し、管理インターフェイスが自身のIPアドレス（IPv4）、ネットマスク（IPv4）、およびデフォルトゲートウェイをDHCPサーバーから受信できるようにします。

また任意で、使用するオーケストレーション システムが管理インターフェイスのホスト名およびクライアント識別子を承認する場合は、この情報をDHCPサーバーに送信することもできます。

1. **Device (デバイス)** > **Setup (セットアップ)** > **Management (管理)** を選択して Management Interface Settings (管理インターフェイス設定) を編集します。
2. **IP Type** [IPタイプ]で**DHCP Client** [DHCPクライアント]を選択します。
3. （任意）ファイアウォールがDHCP DiscoverあるいはRequestメッセージでDHCPサーバーに送る項目のオプションについて、次のいずれかあるいは両方を選択します。
   - **Send Hostname (ホスト名を送信)** —DHCP Option 12の一部として **Hostname (ホスト名)**（**Device (デバイス)** > **Setup (セットアップ)** > **Management (管理)** にて定義）を送信します。
   - **Send Client ID** [クライアントIDを送信] - DHCP Option 61の一部としてクライアント識別子を送信します。クライアント識別子はDHCPクライアントを一意に識別し、DHCPサーバーは自身の設定パラメーターデータベースのインデックス フィールドでこれを使用します。
4. **OK** をクリックします。

STEP 2 | （任意）DHCPサーバーから送信されたホスト名およびドメインをファイアウォールが承認するように設定します。

1. **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) を編集します。
2. 次のオプションのいずれかあるいは両方を選択します。
   - **Accept DHCP server provided Hostname** [DHCPサーバーが提供したホスト名を承認]—DHCPサーバーから送られたホスト名をファイアウォールが承認する（正当な場合）ことを許可します。これを有効化すると、**Device** > **Setup** > **Management** で定義されている既存の **Hostname (ホスト名)** がすべてDHCPサーバーからのホスト名で上書きされます。ホスト名を手動で設定したい場合はこのオプションを選択しないでください。
   - **Accept DHCP server provided Domain** [DHCPサーバーが提供したドメインを承認]—DHCPサーバーから送られたドメインをファイアウォールが承認することを許可します。**Device (デバイス)** > **Setup (セットアップ)** > **Management (管理)** で定義されている既存の **Domain (ドメイン)** がすべてDHCPサーバーからのドメイン（末尾がDNS）で上書きされます。ドメインを手動で設定したい場合はこのオプションを選択しないでください。
3. **OK** をクリックします。

STEP 3 | 変更をコミットします。

Commit（コミット）をクリックします。

STEP 4 | DHCP クライアント情報を表示します。

1. **Device (デバイス)** > **Setup (セットアップ)** > **Management (管理)** を選択し、さらに Management Interface Settings (管理インターフェイス設定) を選択します。
2. **Show DHCP Client Runtime Info** [DHCP クライアント ランタイム情報の表示]をクリックします。

STEP 5 | （任意）リース期間に関わらず、DHCPサーバーでDHCPリースを更新します。

このオプションは、ネットワークの問題をテストあるいはトラブルシュートする際に役立ちます。

1. **Device (デバイス)** > **Setup (セットアップ)** > **Management (管理)** を選択して Management Interface Settings (管理インターフェイス設定) を編集します。
2. **Show DHCP Client Runtime Info** [DHCP クライアント ランタイム情報の表示]をクリックします。
3. **Renew** [更新]をクリックします。

STEP 6 | （任意）DHCPサーバーから送られた次のDHCPオプションを解除します。

- IP アドレス
- ネットマスク
- デフォルトゲートウェイ
- DNSサーバー（プライマリおよびセカンダリ）
- NTPサーバー（プライマリおよびセカンダリ）
- ドメイン（末尾がDNS）

これを解除すると*IP*アドレスが開放されるため、管理アクセス用に他のインターフェイスが設定されていない場合はネットワーク接続が途切れてファイアウォールを管理できなくなります。

CLI操作コマンド**`request dhcp client management-interface release`**を使用します。

DHCP リレー エージェントとしてインターフェイスを設定する

クライアントとサーバー間のDHCPメッセージをファイアウォールのインターフェイスが送信できるようにするには、ファイアウォールをDHCPリレーエージェントとして設定する必要があります。こ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、最初に応答したサーバーの DHCPOFFER メッセージは、要求したクライアントにリレーされます。

キャパシティは次の通りです：

- PA-5200 Series および PA-7000 Series 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で、合計 500 台の DHCP サーバー (IPv4) と DHCP リレーエージェント (IPv4 および IPv6) を設定できます
- PA-5220 Series のファイアウォールでは、最大 500 台の DHCP サーバーと、最大 2,048 台の DHCP リレー エージェントから設定された DHCP サーバーの数を差し引くことができます。たとえば、500 台の DHCP サーバーを設定する場合は、 1,548 台の DHCP リレーエージェントを設定できます。
- PA-5250、PA-5260 および PA-7000 Series のファイアウォールでは、最大 500 台の DHCP サーバーと、最大 4,096 台の DHCP リレー エージェントから設定された DHCP サーバーの数を差し引くことができます。たとえば、500 台の DHCP サーバーを設定する場合は、3,596 台の DHCP リレーエージェントを設定できます。

DHCP リレー エージェントを設定する前に、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。

STEP 1 | DHCP リレーを選択します。

Network (ネットワーク) > **DHCP** > **DHCP Relay (DHCP リレー)** を選択します。

STEP 2 | DHCP リレー エージェントと通信する各 DHCP サーバーの IP アドレスを指定します。

1. **Interface (インターフェイス)** フィールドで、DHCP リレー エージェントにするインターフェイスを選択します。
2. **IPv4** または **IPv6** のいずれかを選択し、指定する DHCP サーバー アドレスのタイプを示します。
3. **IPv4** にチェックを入れている場合、**DHCP Server IP Address (DHCP** サーバーの **IP** アドレス**)** フィールドで、DHCP メッセージをリレーする DHCP サーバーのアドレスを **Add (追加)** します。
4. **IPv6** にチェックを入れている場合、**DHCP Server IPv6 Address (DHCP** サーバーの **IPv6** アドレス**)** フィールドで、DHCP メッセージをリレーする DHCP サーバーのアドレスを **Add (追加)** します。マルチキャスト アドレスを指定した場合、発信インターフェイスも指定します。
5. （任意）前の 3 つのステップを繰り返し、IPアドレス ファミリーごとに最大 8 個の DHCP サーバー アドレスを入力します。

STEP 3 | 設定をコミットします。

OK、**Commit (**コミット**)** の順にクリックします。

DHCP のモニターおよびトラブルシューティング

CLI からコマンドを発行して、DHCP サーバーが割り当てた、または DHCP クライアントに割り当てられた動的なアドレス リースの状態を表示できます。また、タイムアウトして自動的にリリースされる前にリースをクリアすることもできます。

- DHCP サーバー情報の表示
- DHCP リースのクリア
- DHCP クライアント情報の表示
- DHCP に関するデバッグ出力の収集

DHCP サーバー情報の表示

このタスクを実行し、DHCP プールの統計情報、DHCP サーバーが割り当てた IP アドレス、対応する MAC アドレス、リースの状態や期間、リースの開始時間を表示します。アドレスが **Reserved Address**（予約済みアドレス） として設定されている場合、`state` 列には `reserved` と表示され、`duration` または `lease_time` は表示されません。リースが **[無制限]** として設定されている場合、`duration` 列には、`0` の値が表示されます。

DHCP プールの統計情報、DHCP サーバーが割り当てられた IP アドレス、MAC アドレス、リースの状態と期間、リースの開始時間を表示します。

```
admin@PA-220> show dhcp server lease interface all
```

```
interface: "ethernet1/2"
Allocated IPs: 1, Total number of IPs in pool: 5. 20.0000% used
ip              mac                state      duration
 lease_time
192.168.3.11    f0:2f:af:42:70:cf  committed  0           Wed Jul
 2 08:10:56 2014
admin@PA-220>
```

DHCP サーバーがクライアントに割り当てたオプションを表示します。

```
admin@PA-220> show dhcp server settings all
```

```
Interface    GW           DNS1        DNS2       DNS-Suffix Inherit
 source
------------------------------------------------------------------------------
ethernet1/2  192.168.3.1  10.43.2.10  10.44.2.10
             ethernet1/3
admin@PA-220>
```

DHCP リースのクリア

DHCP リースをクリアする方法は複数あります。

ホールドタイマーによって自動的にリリースされる前に、ethernet1/2 など、インターフェイス（サーバー）の失効した DHCP リース をリリースします。これらのアドレスは、IP プールで再度使用できるようになります。

```
admin@PA-220> clear dhcp lease interface ethernet1/2 expired-only
```

特定の IP アドレス（例：192.168.3.1）のリースをリリースします。

```
admin@PA-220> clear dhcp lease interface ethernet1/2 ip 192.168.3.1
```

特定の MAC アドレス（例：f0:2c:ae:29:71:34）のリースをリリースします。

```
admin@PA-220> clear dhcp lease interface ethernet1/2 mac
 f0:2c:ae:29:71:34
```

DHCP クライアント情報の表示

ファイアウォールが DHCP クライアントとして機能している場合、ファイアウォールに送信された IP アドレスのリースの状態を表示するには、これらのうちいずれかの CLI コマンドを使用します。

```
admin@PA-220>show dhcp client state <interface_name>
```

```
admin@PA-220> show dhcp client state all
```

```
Interface       State        IP              Gateway
 Leased-until
--------------------------------------------------------------------------------
ethernet1/1     Bound        10.43.14.80     10.43.14.1
 70315
admin@PA-220>
```

DHCP に関するデバッグ出力の収集

DHCP に関するデバッグ出力を収集するには、以下のいずれかのコマンドを使用します。

```
admin@PA-220> debug dhcpd
```

```
admin@PA-220> debug management-server dhcpd
```


DNS

Domain Name System（DNS）は、www.paloaltonetworks.com などのユーザーにとって分かりやすいドメイン名を IP アドレスに変換（解決）し、インターネットあるいはプライベート ネットワーク上のコンピューター、ウェブサイト、サービス、あるいは他のリソースにユーザーがアクセスできるようにするプロトコルです。

DNS の概要

DNS は、ユーザーが IP アドレスを記憶する必要をなくし、各コンピューターがドメイン名と IP アドレスとのマッピングを大量に保存する必要性をなくすことで、ユーザーがネットワークリソースにアクセスする上で非常に重要な役割を果たします。DNS はクライアント/サーバー モデルを採用しています。DNS サーバーは自身のキャッシュを検索して DNS クライアントのためにクエリを解決します。また必要に応じて、対応する IP アドレスをクライアントに返せるようになるまで、他のサーバーにクエリを送信します。

ドメイン名の DNS のストラクチャは階層的なものです。ドメイン名のトップレベル ドメイン（TLD）には、com、edu、gov、int、mil、net、あるいは org（gov および mil は米国のみ）といったジェネリック TLD（gTLD）、あるいは us （米国）などの国コード（ccTLD）があります。通常、ccTLD は国や属領のために予約されています。

完全修飾ドメイン名（FQDN）には最低でもホスト名、セカンドレベル ドメイン、および TLD が含まれており、DNS のストラクチャに属すホストの位置を完璧に特定できます。例えば、www.paloaltonetworks.com は FQDN です。

Palo Alto Networks®ファイアウォールがユーザー インターフェイスまたは CLI で FQDN を使用する場合、ファイアウォールは DNS を使用してその FQDN を解決する必要があります。® FQDN クエリの発信元に応じて、ファイアウォールは、クエリの解決に使用する DNS 設定を決定します。

FQDN の DNS レコードには、time-to-live (TTL) の値が含まれており、ファイアウォールはデフォルトで、TTL がファイアウォールで設定したMinimum FQDN Refresh Time (最低 FQDN 更新時間)以上である、あるいは最低時間を設定していない場合はデフォルト設定の 30 秒である場合、DNS サーバーであれば個々の TTL に基づいてキャッシュ内の各 FQDN を更新します。TTL の値に基づいて FQDN を更新することは、サービスの非常に高い可用性を確保するために頻繁に FQDN を更新することが多く求められるクラウドプラットフォームのサービスへのアクセスを保護する際に特に役立ちます。例えば、自動スケーリングをサポートしているクラウド環境は自動的にサービスをスケールアップ、スケールダウンするために FQDN 解決に依存しており、そのような時間が重要である環境では迅速な FQDN 解決が不可欠になります。

最低 FQDN 更新時間を設定することで、ファイアウォールがどれだけ小さい TTL の値を尊重するのか、制限することができます。IP アドレスがあまり頻繁に変わらない場合、最低 FQDN 更新時間を大きく設定し、ファイアウォールが無駄にエントリを更新しないようにすると良いでしょう。ファイアウォールは大きい方の DNS TTL 時間と、設定された最低 FQDN 更新時間を使用します。

例えば、2 つの FQDN が次の TTL の値を持っています。最低 FQDN 更新時間は、より小さい TTL (早い) の値をオーバーライドします。

	TTL	最低 **FQDN** 更新 **= 26** の場合	実際の更新時間
FQDN A	20		26
FQDN B	30		30

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、FQDN 更新タイマーが開始されます。

さらに、stale timeout (ステール タイムアウト) を設定し、DNS サーバーに到達できない場合にファイアウォールが古い (失効した) FQDN 解決を使用し続ける時間を指定することができます。ステール タイムアウトの期間が終了する時点でまだ DNS サーバーに到達できない場合、古い FQDN のエントリは解決不能になります (ファイアウォールは古い FQDN のエントリを削除します)。

次のファイアウォールのタスクは、DNS に関するものです。

- ホスト名を解決できるよう、ファイアウォールに DNS サーバーを少なくとも 1 つ設定します。ユース ケース1：ファイアウォールには DNS 解決が必要にある通り、プライマリおよびセカンダリ DNS サーバー、あるいはそのようなサーバーを指定する DNS プロキシ オブジェクトを設定します。
- ファイアウォールが各仮想システムについて、セキュリティポリシールール、レポート、管理サービス（email、Kerberos、SNMP Syslog など）によって開始される DNS 解決を行う方法をカスタマイズします。参照：ユース ケース 2：ISP テナントが DNS プロキシを使用して、仮想システム内のセキュリティ ポリシー、レポート、サービスの DNS 解決を処理する場合。
- ファイアウォールがクライアント用の DNS サーバーとして機能するよう設定を行います。参照：ユース ケース 3：ファイアウォールがクライアントとサーバー間の DNS プロキシとして機能する場合。
- アンチスパイウェア プロファイルを設定してDNS クエリを使用してネットワーク上の感染ホストを特定します。
- 回避シグネチャを有効化し、脅威防止用の回避シグネチャを有効化します。
- DHCP サーバーとしてインターフェイスを設定する。これにより、ファイアウォールが DHCP サーバーとして機能して DNS 情報を DHCP クライアントに送信することで、用意された DHCP クライアントが対応する DNS サーバーに到達できるようにします。

DNS プロキシ オブジェクト

DNS プロキシとして設定されたファイアウォールは、DNS クライアントとサーバーの仲介役になることで、DNS プロキシ キャッシュからクエリを解決して DNS サーバー自体として機能します。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、（DNS クエリが到達するインターフェイス上の）特定の DNS プロキシ オブジェクトのエントリの中からドメイン名が一致するものを検索します。ファイアウォールは一致結果に基づき、適切な DNS サーバーにクエリを転送します。いずれもマッチしない場合、ファイアウォールはデフォルトの DNS サーバーを使用します。

DNS プロキシ オブジェクトは、ファイアウォールが DNS プロキシとしてどのように機能するかを設定する場所です。DNS プロキシ オブジェクトは、1 つの仮想システムに割り当てることも、すべての仮想システムで共有することもできます。

- DNS プロキシ オブジェクトを 1 つの仮想システムで使用する場合は、DNSサーバ プロファイルを指定できます。このプロファイルには、プライマリおよびセカンダリ DNS サーバーアドレスをはじめとする情報を指定します。DNS サーバー プロファイルを使用すると、設定が簡便になります。
- DNS プロキシ オブジェクトを共有する場合は、DNS サーバーの少なくともプライマリ アドレスを指定する必要があります。

> 複数のテナント（*ISP* 加入者）に *DNS* サービスを設定する場合は、各テナントに独自の *DNS* プロキシを定義します。この定義により、テナントの *DNS* サービスが他のテナントのサービスとは分離された状態で維持されます。

プロキシ オブジェクトには、ファイアウォールが DNS プロキシとして機能するインターフェイスを指定します。インターフェイスの DNS プロキシはサービス ルートを使用しません。DNS 要求への応答は常に、DNS 要求が到着した仮想ルーターに割り当てられたインターフェイスに送信されます。

DNS プロキシ オブジェクトの設定 を行う際、DNS プロキシに FQDN からアドレスへのスタティック マッピングを指定できます。また、ドメイン名のクエリをどの DNS サーバーに送信するかを制御する DNS プロキシ ルールも作成できます。最大 256 個の DNS プロキシ オブジェクトをファイアウォールに設定できます。この DNS プロキシ オブジェクトが**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） > **vsys** > **General**（全般） > **DNS Proxy**（**DNS** プロキシ）に割り当てられている場合、（**Network**（ネットワーク） > **DNS Proxy**（**DNS** プロキシ） > **Advanced**（詳細）の下で ）**Cache**（キャッシュ）および**Cache EDNS Responses**（キャッシュ **EDNS** 応答）を有効にする必要があります。さらに、この DNS プロキシ オブジェクトに **DNS proxy rules**（**DNS** プロキシ ルール）が設定されている場合、それらのルールでもキャッシュを有効にする必要があります（このマッピングによって解決されるドメインのキャッシングをオンにする）。

ファイアウォールが FQDN クエリを受信する際（そしてドメイン名が DNS プロキシ キャッシュに存在しない場合）、ファイアウォールは FQDN クエリに含まれるドメイン名を、DNS プロキシ オブジェクトの DNS プロキシ ルールにあるドメイン名と比較します。単一の DNS プロキシ ルールで複数のドメイン名を指定する場合、ルールに含まれるドメイン名のいずれか一つにクエリがマッチすれば、クエリがルールにマッチしたことになります。 DNS プロキシ ルール

および FQDN マッチングファイアウォールが FQDN を DNS プロキシ ルール内のドメイン名にマッチさせるかどうか判断する方法を示しています。ルールにマッチする DNS クエリは、プロキシ オブジェクトを解決するよう設定されたプライマリ DNS サーバーに送信されます。

DNSサーバ プロファイル

仮想システムの設定を簡便にするために、DNS サーバー プロファイルを使用すると、設定中の仮想システム、DNS サーバーの継承ソースまたはプライマリ/セカンダリ IP 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は、ルート テーブルが設定された仮想ルーターを決定します。送信元インターフェイスが割り当てられている仮想ルーターのルート テーブルで宛先 IP アドレスが検索されます。宛先 IP 出力インターフェイスの結果が送信元インターフェイスとは異なることがあります。パケットは、ルート テーブル検索によって決定された宛先 IP 出力インターフェイスを通過しますが、送信元 IP アドレスが設定されたアドレスである場合もあります。送信元アドレスは、DNS サーバーからの応答で宛先アドレスとして使用されます。

仮想システム レポートおよび仮想システム サーバー プロファイルは、そのクエリを、仮想システムに対して指定された DNS サーバー（ある場合）に送信します（使用される DNS サーバーは、**Device (**デバイス**)** > **Virtual Systems (**仮想システム**)** > **General (**全般**)** > **DNS Proxy (DNS** プロキシ**)** で定義します） 仮想システムに DNS サーバーが 1 つも指定されていない場合は、ファイアウォールに対して指定されている DNS サーバーがクエリされます。

仮想システムに対してのみDNS サーバー プロファイルの設定 が可能です。グローバルな共有領域には使用できません。

マルチテナント DNS のデプロイメント

ファイアウォールは、要求がどこから発信されたかに基づいて DNS 要求の処理方法を決定します。単一のファイアウォール上に複数のテナントを持つ ISP の環境は、マルチテナントとして知られています。マルチテナント DNS のデプロイメントの 3 つのユース ケースを紹介します。

- グローバル管理の **DNS** 解決 – ファイアウォールには独自の目的の DNS 解決が必要です。たとえば、ソフトウェア更新サービスなどの管理イベントのために、FQDN を解決するための要求が管理プレーンから送信される場合などです。ファイアウォールは、DNS リクエストが特定の仮想ルーターにやって来ないために、サービス ルートを使用して DNS サーバーに到達します。
- 仮想システムのポリシーおよびレポートの **FQDN** 解決 – セキュリティ ポリシー、レポート、あるいはサービスからの DNS クエリについては、仮想システム（テナント）に固有の DNS サーバー セットを指定することも、デフォルトのグローバル DNS サーバーを指定することもできます。仮想システム毎に異なる DNS サーバーのセットが必要なユースケースでは、DNS プロキシ オブジェクトを設定する必要があります。解決は、DNS プロキシが割り当てられている仮想システムに固有です。この仮想システムに適用可能な特定の DNS サーバーがない場合は、ガイドラインはグローバル DNS 設定を使用します。
- 仮想システムのデータプレーンの **DNS** 解決 – この方法は、DNS 解決のネットワーク要求ともいいます。ネットワーク内のテナントの DNS サーバーで、指定したドメイン名が解決されるように、テナントの仮想システムを設定できます。この方法はスプリット ***DNS*** をサポートします。つまり、テナントは、独自のサーバーで解決されずに残っている DNS クエリに独自の ISP DNS サーバーを使用できます。DNS プロキシ オブジェクト ルールは、スプリット DNS を制御します。具体的には、テナントのドメインが DNS 要求を、DNS サーバー プロファイルで設定されたその DNS サーバーにリダイレクトします。DNS サーバー プロファイルには、プライマリおよびセカンダリ DNS サーバーと、デフォルトの DNS 設定をオーバーライドする IPv4 および IPv6 の DNS サービス ルートが指定されています。

以下の表は、各 DNS 解決のタイプの要約です。バインド場所は、解決にどの DNS プロキシ オブジェクトを使用するかを決定します。ユース ケースでは、わかりやすく説明する目的で、ファイアウォール上およびテナント（加入者）の仮想システムに必要な DNS クエリを解決する DNS サービスを提供するために、サービス プロバイダが DNS をどのように設定していると考えられるかを示します。

解決タイプ	場所:共有	場所:特定の**Vsys**
ファイアウォールの DNS 解決 – 管理プレーンが実行	バインド：Global ユース ケース 1 で説明	N/A
セキュリティ プロファイル、サポート、サーバー プロファイルの解決 – 管理プレーンが実行	バインド：Global ユース ケース 1 と同じ動作	バインド：特定のVsys ユース ケース 2 で説明
ファイアウォールを通過して DNS サーバーに到達する、ファ	バインド：interface インターフェイス	

解決タイプ	場所:共有	場所:特定のVsys
イアウォールのインターフェイスに接続された DNS クライアント ホストの DNS プロキシの解決 –データプレーンで実行	サービス ルート：DNS 要求を受信したインターフェイスおよび IP アドレス。 ユース ケース3 で説明	

- ユース ケース1：ファイアウォールには DNS 解決が必要
- ユース ケース2：ISP テナントが DNS プロキシを使用して、仮想システム内のセキュリティ ポリシー、レポート、サービスの DNS 解決を処理する場合。
- ユース ケース3：ファイアウォールがクライアントとサーバー間の DNS プロキシとして機能する場合。

DNS プロキシ オブジェクトの設定

ファイアウォールを DNS プロキシとして機能させる場合は、このタスクを実行してDNS プロキシ オブジェクトの設定を行います。プロキシ オブジェクトは、すべての仮想システムで共有することも、特定の仮想システムに適用することもできます。

ファイアウォールが *DNS* プロキシとして動作する機能が有効な場合、偽装された *HTTP* あるいは *TLS* リクエストを検知する回避シグネチャが、元の *DNS* リクエストで指定されているもの以外のドメインにクライアントが接続する際にアラートを生成できます。ベストプラクティスとして、*DNS* プロキシを設定してから回避シグネチャを有効化し、改ざんされたリクエストが検出された場合にアラートを発生させます。

STEP 1 | DNS プロキシ オブジェクトの基本設定を行います。

1. **Network (**ネットワーク**)** > **DNS Proxy (DNS** プロキシ**)** を選択して新しいオブジェクトを **Add (**追加**)** します。
2. **Enable** [有効化]が選択されていることを確認します。
3. オブジェクトの **Name [**名前**]** を入力します。
4. **Location**（場所）には、オブジェクトを適用する仮想システムを選択します。**Shared (**共有**)** を選択する場合は、少なくとも **Primary (**プライマリ**)** DNS サーバー アドレスを指定する必要があります。必要に応じて **Secondary (**セカンダリ**)** アドレスも指定します。
5. 仮想システムを選択した場合は、**Server Profile (**サーバープロファイル**)** に DNS サーバー プロファイルを選択するか、 **DNS Server Profile (DNS** サーバープロファイル**)** をクリックして新しいプロファイルを設定します。DNS サーバー プロファイルの設定を参照してください。
6. Inheritance Source (継承ソース) については、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。デフォルト設定は**None**（なし）です。
7. **Interface** [インターフェイス]で **Add** [追加]をクリックし、DNS プロキシ オブジェクトを適用するインターフェイスを指定します。
   - DNS 検索の実行に DNS プロキシ オブジェクトを使用する場合は、インターフェイスが必要です。ファイアウォールはこのインターフェイスで DNS 要求をリッスンし、プロキシとして機能します。
   - サービス ルートに DNS プロキシ オブジェクトを使用する場合、インターフェイスは任意です。

STEP 2 | （任意）DNS プロキシ ルールを指定します。

1. **DNS Proxy Rules (DNS** プロキシ ルール**)** タブでルールの **Name (**名前**)** を **Add (**追加**)** します。
2. ファイアウォールで解決されたドメインをキャッシュする場合は、**Turn on caching of domains resolved by this mapping** [このマッピングによって解決されるドメインのキャッシングをオンにする]チェック ボックスをオンにします。
3. **Domain Name (**ドメイン名**)** については、ファイアウォールが FQDN クエリを比較する対象となる単一あるいは複数のドメインを、各行に一つずつ **Add (**追加**)** します。ルールに含まれるいずれかのドメインにクエリが一致すると、（前のステップで設定した内容に応じて）クエリが次のいずれかのサーバーに送信され、解決されます。
   - このプロキシ オブジェクト用に直に指定された **Primary (**プライマリ**)** あるいは **Secondary (**セカンダリ**)** DNS サーバー。
   - このプロキシ オブジェクト用の DNS サーバープロファイルで指定された **Primary (**プライマリ**)** あるいは **Secondary (**セカンダリ**)** DNS サーバー。

   DNS プロキシ ルールおよび FQDN マッチングは、ファイアウォールが FQDN 内のドメイン名をどのように DNS プロキシ ルールとマッチさせるのかを指定します。マッチしない場合、デフォルトの DNS サーバーがクエリを解決します。
4. **Location (**場所**)** の設定に応じて、次のいずれかを行います。
   - 仮想システムを選択した場合は **DNS Server profile (DNS** サーバー プロファイル**)** を選択します。
   - **Shared (**共有**)** を選択した場合、**Primary (**プライマリ**)** および任意で **Secondary (**セカンダリ**)** アドレスを入力します。
5. **OK** をクリックします。

STEP 3 | （任意）DNS プロキシに FQDN からアドレスへのスタティック エントリを指定します。スタティック DNS エントリを指定すると、ファイアウォールが DNS サーバーにクエリを送信することなく、FQDN から IP アドレスを解決できます。

1. **Static Entries (**スタティック エントリ**)** タブで **Name (**名前**)** を **Add (**追加**)** します。
2. 完全修飾ドメイン名（**FQDN**）を入力します。
3. **Address (**アドレス**)** については、FQDN をマッピングさせなければならない IP アドレスを **Add (**追加**)** します。

   項目の IP アドレスを追加することができます。ファイアウォールはこれらのすべての IP アドレスを DNS 応答で提供し、クライアントは使用する IP アドレスを選択します。
4. **OK** をクリックします。

STEP 4 | キャッシュを有効にして、DNS プロキシのその他の詳細設定を行います。

1. TCP を使用する DNS クエリを有効にするには、**Advanced (詳細)** タブで **TCP Queries (TCP クエリ)** を選択します。
   - **Max Pending Requests** [最大保留要求] – ファイアウォールでサポートされる同時未解決 TCP DNS 要求の最大数を入力します（範囲は 64 ～ 256、デフォルトは 64）。
2. **UDP Queries Retries (UDP クエリの再試行)** は次のように入力します。
   - **Interval (sec) (間隔（秒）)**–応答を受信しなかった場合に別の要求が送信されるまでの時間（秒）を指定します（範囲は1～ 30 、デフォルトは 2 ）。
   - **Attempts (試行回数)** –次 DNS サーバーをクエリするまでの UDP クエリの最大試行回数（最初の思考は除く）（範囲は 1 ～ 30、デフォルトは 5。）
3. FQDN からアドレスへのマッピングを学習させてファイアウォールがキャッシュできるようにするには、**Cache (キャッシュ)** を選択します。この DNS プロキシ オブジェクトが、ファイアウォールによって生成されるクエリに使用される場合 (つまり、**Device** セットアップ **Services** > **DNS** > 、または > **Device** 仮想システム 以下)、仮想システムと > **General** DNS Proxy を選択する場合は、 > **Cache** (既定で有効) を有効にする必要があります。
   - ファイアウォールがプロキシ オブジェクトの DNS 解決エントリをキャッシュする時間の長さを制限するには、**Enable TTL (TTL の有効化)** を選択します。デフォルトで無効になっています。
     - プロキシ オブジェクト用にキャッシュされたエントリがすべて削除されるまでの秒数として **Time to Live (sec)** を入力します。エントリの削除後は、新しい DNS 要求を解決してキャッシュし直す必要があります。範囲は 60 ～ 86,400。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）–この DNS プロキシ オブジェクトをファイアウォールが生成するクエリに使用する場合、この設定を有効にする必要があります。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**-vsys**）の下で、virtual system (仮想システム - vsys)と**General**（全般） > **DNS Proxy**（**DNS** プロキシ)を選択します。

STEP 5 | 変更をコミットします。

OK、**Commit (コミット)** の順にクリックします。

DNS サーバー プロファイルの設定

仮想システムの構成をシンプルにするDNS サーバープロファイルを設定します。**Primary DNS** [プライマリ DNS]または **Secondary DNS** [セカンダリ DNS]アドレスを使用して、仮想システムが DNS サーバーに送信する DNS 要求を作成します。

STEP 1 | DNS サーバー プロファイルに名前を付けて、適用する仮想システムを選択し、プライマリおよびセカンダリ DNS サーバー アドレスを指定します。

1. **Device (デバイス)** > **Server Profiles (サーバープロファイル)** > **DNS** を選択し、DNS サーバープロファイルの **Name (名前)** を **Add (追加)** します。
2. **Location** [場所]には、プロファイルを適用する仮想システムを選択します。
3. DNS サーバー アドレスを継承しない場合は、**Inheritance Source (継承ソース)** で **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。DNS サーバーを選択する場合は、**Check inheritance source status** [継承ソース状態のチェック]をクリックしてその情報を確認します。
4. **Primary DNS** [プライマリ DNS]サーバーの IP アドレスを指定します。**Inheritance Source** [継承ソース]を選択した場合は、**inherited** [継承済み]のままにします。

   *IP アドレスではなく FQDN を指定する場合、その FQDN の DNS は **Device (デバイス) > Virtual Systems (仮想システム) > DNS Proxy (DNS プロキシ)** で解決されます。*
5. **Secondary DNS** [セカンダリ DNS]サーバーの IP アドレスを指定します。**Inheritance Source** [継承ソース]を選択した場合は、**inherited** [継承済み]のままにします。

STEP 2 | ターゲット DNS サーバーに指定されている IP アドレスのファミリ タイプが IPv4 か IPv6 かに応じて、ファイアウォールが自動的に使用するサービス ルートを設定します。

1. ターゲット DNS のアドレスが IPv4 アドレスの場合は、**Service Route IPv4** [サービス ルート IPv4]をクリックして、サービス ルートとして使用する後続のインターフェイスと IPv6 アドレスを有効にします。
2. **Source Interface** [送信元インターフェイス]を指定して、サービス ルートが使用する DNS サーバーの 送信元 IP アドレスを選択します。ファイアウォールは、そのインターフェイスにどの仮想ルーターが割り当てられているかを判断したうえで、仮想ルーターのルーティング テーブルでルート検索を行い、（**Primary DNS** [プライマリ DNS]アドレスに基づいて）宛先ネットワークに到達します。
3. DNS サーバーに送信されるパケットの **Source Address** [送信元アドレス]（IPv4）を指定します。
4. ターゲット DNS のアドレスが IPv4 アドレスの場合は、**Service Route IPv4** [サービス ルート IPv4]をクリックして、サービス ルートとして使用する後続のインターフェイスと IPv6 アドレスを有効にします。
5. **Source Interface** [送信元インターフェイス]を指定して、サービス ルートが使用する DNS サーバーの 送信元 IP アドレスを選択します。ファイアウォールは、そのインターフェイスにどの仮想ルーターが割り当てられているかを判断したうえで、仮想ルーターのルーティング テーブルでルート検索を行い、（**Primary DNS** [プライマリ DNS]アドレスに基づいて）宛先ネットワークに到達します。

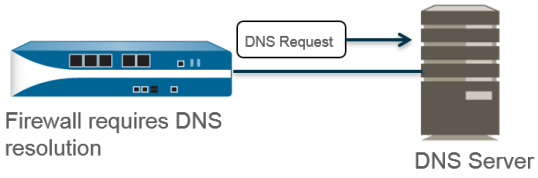
6. DNS サーバーに送信されるパケットの **Source Address** [送信元アドレス]（IPv4）を指定します。
7. **OK** をクリックします。

STEP 3 | 設定をコミットします。

OK、**Commit (コミット)** の順にクリックします。

ユース ケース1：ファイアウォールには DNS 解決が必要

この使用事例では、ファイアウォールは、セキュリティポリシールール、レポート、管理サービス (電子メール、Kerberos、SNMP、syslog など)、およびソフトウェア更新サービス、動的ソフトウェア更新、WildFire などの管理イベントに関する FQDN の DNS 解決を要求するクライアントです。動的環境では、FQDN はより頻繁に変更されます。 正確な DNS 解決により、ファイアウォールは正確なポリシングを実施し、レポートおよび管理サービスを提供し、管理イベントを処理できます。共有されるグローバル DNS サービスが、管理プレーン機能の DNS 解決を実行します。



STEP 1 | ファイアウォールが管理上の DNS 解決に使用する、プライマリおよびセカンダリ DNS サーバーを設定します。

ファイアウォールで少なくとも *1* つの *DNS* サーバーを手動で設定する必要があり、設定しないとホスト名を解決することができなくなります。そのファイアウォールは、*ISP* などの別のソースからの *DNS* サーバー設定を使用できません。

1. 複数の仮想システムをサポートするファイアウォールのサービス設定を編集します。**Device**（デバイス） > **Setup**（セットアップ） > **Services**（サービス） > **Global**（グローバル）。それ以外の場合は**Device**（デバイス） > **Setup**（セットアップ） > **Services**（サービス）です。.
2. **Services (**サービス**)** タブの **DNS** で、**Servers (**サーバー**)** を選択し、**Primary DNS Server (**プライマリ **DNS** サーバー**)** のアドレスと **Secondary DNS Server (**セカンダリ **DNS** サーバー**)** のアドレスを入力します。
3. ステップ 3 に進みます。

STEP 2 | または、スプリット DNS、DNS プロキシ オーバーライド、DNS プロキシ ルール、スタティック エントリ、DNS 継承など高度な DNS 機能を設定する場合は、DNS プロキシ オブジェクトを設定できます。

1. 複数の仮想システムをサポートするファイアウォールのサービス設定を編集します。**Device**（デバイス） > **Setup**（セットアップ） > **Services**（サービス） > **Global**（グローバル）。それ以外の場合は**Device**（デバイス） > **Setup**（セットアップ） > **Services**（サービス）です。.
2. **Services (**サービス**)** タブの **DNS** で **DNS Proxy Object (DNS** プロキシ オブジェクト**)** を選択します。

3. **DNS Proxy (DNS** プロキシ**)** のリストで、グローバル DNS サービスの設定で使用したい DNS プロキシを選択するか、次のように **DNS Proxy (DNS** プロキシ**)** をクリックし、新しい DNS プロキシ オブジェクトを設定します。
   1. **Enable (**有効**)** をクリックし、DNS プロキシ オブジェクトの **Name (**名前**)** を入力します。
   2. 複数の仮想システムをサポートするファイアウォール上で、**Location**（ロケーション）用にグローバル、ファイアウォール全体の DNS プロキシ サービスに対して **Shared**（共有中）を選択します。

      共有される *DNS* プロキシ オブジェクトは、テナントの仮想システムに属する特定のサービス ルートを必要としないため、*DNS* サーバー プロファイルを使用しません。
   3. **Primary (**プライマリ**)** DNS サーバーの IP アドレスを入力します。必要に応じて、**Secondary** [セカンダリ] DNS サーバーの IP アドレスも入力します。
4. **Advanced**（詳細）タブを選択します。**Cache**（キャッシュ）が有効で、**Cache EDNS Responses**（キャッシュ **EDNS** 応答）が有効であることを確認します（どちらもデフォルトで有効です）。
5. **OK** をクリックして、DNS プロキシ オブジェクトを保存します。

STEP 3 | (任意)**Minimum FQDN Refresh Time (sec) (**最小 **FQDN** 更新時間 **(**秒**))** を設定し、ファイアウォールが FQDN キャッシュエントリを更新する頻度を制限します。

デフォルトでは、ファイアウォールは、DNS レコード内の FQDN の個々の TTL に基づいて、更新設定以上である限り (または、最小 FQDN 更新時間を設定しない場合は、TTL がデフォルト設定の 30 秒以上である限り) キャッシュ内の各 FQDN を更新します。最小 FQDN 更新時間を設定するには、値を秒単位で入力します (範囲は 0～14,400、デフォルトは 30 です)。0 に設定すると、ファイアウォールは DNS レコードの TTL 値に基づいて FQDN を更新します。ファイアウォールは、最低 FQDN 更新時間を適用しなくなります。ファイアウォールは、DNS TTL 時間と最小 FQDN 更新時間のうち長い方を使用します。

DNS の *FQDN* の *TTL* が短くても、*FQDN* の解像度が *TTL* の時間枠ほど頻繁に変更されないため、より高速な更新を必要としない場合には、*FQDN* の更新を必要以上に頻繁に行わないように最低 *FQDN* 更新時間を設定する必要があります。

STEP 4 | (任意) **FQDN Stale Entry Timeout (min) (FQDN** 失効エントリタイムアウト **(**分**))** を指定します。これは、到達不能な DNS サーバがあった場合に、ファイアウォールが古い FQDN 解決を引き続き使用する分数です (範囲は 0～10,080、デフォルトは 1,440)。

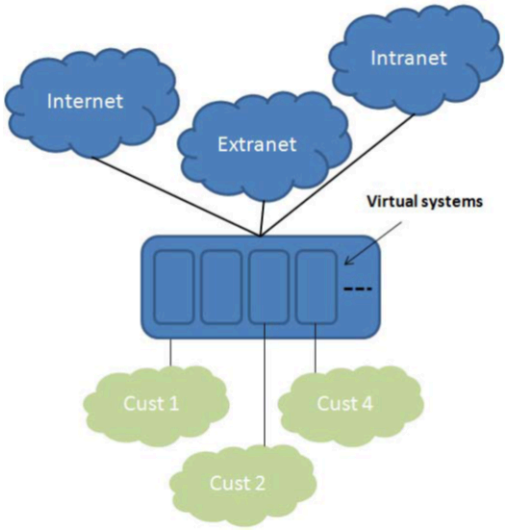
0 に設定すると、ファイアウォールは古い FQDN エントリを使用し続けなくなります。

誤ったトラフィックの転送 (セキュリティリスクが発生する場合があります) を許さないよう *FQDN Stale Entry Timeout* (古い *FQDN* エントリのタイムアウト)の値を十分短くしつつ、かつ意図せずネットワークをダウンさせないよう、トラフィックの継続性を維持できるよう十分長くします。

STEP 5 | **OK**、**Commit (**コミット**)** の順にクリックします。

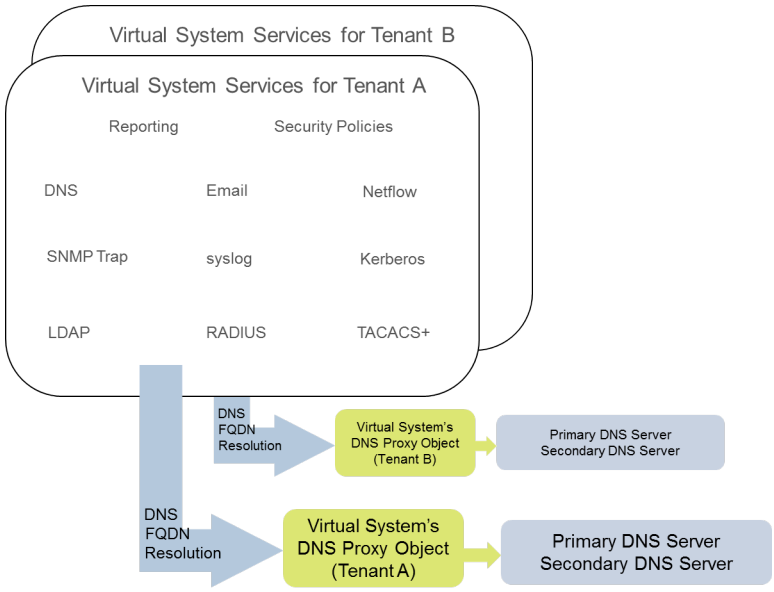
「ユース ケース2：ISP テナントが DNS プロキシを使用して、仮想システム内のセキュリティ ポリシー、レポート、サービスの DNS 解決を処理する場合

このユース ケースでは、ファイアウォールに複数のテナント（ISP 加入者）が定義され、各テナントのサービスや管理ドメインをセグメント化する目的で、テナントごとに個別の仮想システム（vsys）と仮想ルーターが割り当てられています。以下の図は、ファイアウォール内のいくつかの仮想システムを示しています。



テナントごとに、セキュリティポリシー ルール、レポート、および管理サービス（電子メール、Kerberos、SNMP、syslog など）の独自のサーバー プロファイルが独自のネットワークに定義されています。

これらのサービスによって開始される DNS 解決の場合、各仮想システムが独自の DNS プロキシ オブジェクトを使用して設定されるため、仮想システム内で DNS 解決がどのように処理されるかを各テナントがカスタマイズできます。**Location** [場所]が設定されたサービスはすべて、仮想システム用に設定された DNS プロキシ オブジェクトを使用して、FQDN を解決するプライマリ（またはセカンダリ）DNS サーバーを判断します（下図を参照）。



STEP 1 | 仮想システムごとに、使用する DNS プロキシを指定します。

1. **Device (デバイス)** > **Virtual Systems (仮想システム)** を選択して仮想システムの **ID** を **Add (追加)**（範囲は 1～255）し、任意で **Name (名前)** を追加します（この例では Corp1 Corporation）。
2. **General** [全般]タブで、**DNS Proxy** [DNS プロキシ]を選択するか、新しい DNS プロキシを作成します。この例では、Corp1 Corporation の仮想システムのプロキシに、Corp1 という DNS プロキシが選択されています
3. **Interfaces** [インターフェイス]で **Add** [追加]をクリックします。この例では、Ethernet1/20 がこのテナント専用のインターフェイスです。
4. **Virtual Routers** [仮想ルーター]で **Add** [追加]をクリックします。ルーティング機能を分離するために、Corp1 VR という名前の仮想ルーターがこの仮想システムに割り当てられています。
5. **OK** をクリックします。

STEP 2 | 仮想システムの DNS 解決をサポートするために、DNS プロキシとサーバー プロファイルを設定します。

1. **Network (ネットワーク)** > **DNS Proxy (DNS プロキシ)** を選択して **Add (追加)** をクリックします。
2. **Enable** [有効化]をクリックして、DNS プロキシの **Name** [名前]を入力します。
3. **Location** [場所]には、テナントの仮想システムを選択します。この例では、Corp1 Corporation （vsys6）です（代わりに、**Shared** [共有] DNS プロキシ リソースを選択することもできます）。
4. **Server Profile** [サーバー プロファイル]では、プロファイルを選択または作成して、このテナントのセキュリティ ポリシー、レポート、およびサーバー プロファイル サービスの DNS 解決に使用する DNS サーバーをカスタマイズします。

   プロファイルがまだ設定されていない場合は、**Server Profile** [サーバー プロファイル]フィールドで、**DNS Server Profile** [DNS サーバー プロファイル]をクリックしてDNS サーバー プロファイルの設定を行います。

   DNS サーバー プロファイルは、この仮想システムの管理上の DNS 解決に使用するプライマリおよびセカンダリ DNS サーバーの IP アドレスを識別します。
5. また、必要に応じてこのサーバー プロファイルに **Service Route Ipv4 (サービス ルート IPv4)** や **Service Route Ipv6 (サービス ルート IPv6)** を設定し、DNS 要求でどの **Source Interface (ソース インターフェイス)** を使用するかをファイアウォールに指示します。そのインターフェイスに IP アドレスが複数ある場合は、**Source Address** [ソース アドレス]も設定します。
6. **Advanced**（詳細）タブを選択します。**Cache**（キャッシュ）が有効で、**Cache EDNS Responses**（キャッシュ **EDNS** 応答）が有効であることを確認します（どちらもデフォルトで有効です）。これは、DNS プロキシ オブジェクトが**Device**（デバイス） > **Virtual Systems**（仮想システム） > **vsys** > **General**（全般） > **DNS Proxy**（**DNS** プロキシ）で使用される場合に必要です。
7. **OK** をクリックします。
8. **OK**、**Commit (コミット)** の順にクリックします。

   スプリット *DNS* などの高度な機能は、必要に応じて、***DNS Proxy Rules*** *[DNS* プロキシ ルール*]*を使用して設定できます。個別の *DNS* サーバー プロファイルを使用すると、***DNS Proxy Rule*** *[DNS* プロキシ ルール*]*の ***Domain Name*** *[*ドメイン名*]*と一致する *DNS* 解決を別の *DNS* サーバー セットにリダイレクトできます。スプリット *DNS* については、ユース ケース *3* で説明します。

   同じ DNS プロキシ オブジェクトに 2 つの別個の DNS サーバー プロファイルがあり、1 つが DNS プロキシ用で、もう 1 つが DNS プロキシ ルール用の場合は以下の動作が生じます。

   - サービス ルートが、DNS プロキシに使用される DNS サーバー プロファイルで定義されている場合は、このルートが優先して使用されます。
   - サービス ルートが、DNS プロキシ ルールに使用される DNS サーバー プロファイルで定義されている場合は、このルートは使用されません。サービス ルート

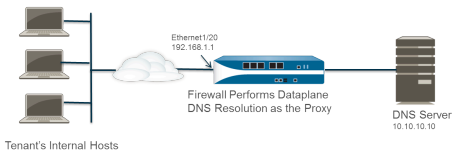
が、DNS プロキシに使用される DNS サーバー プロファイルで定義されるものと異なる場合は、**Commit** [コミット]プロセス時に以下の警告メッセージが表示されます。

```
Warning: The DNS service route defined in the DNS proxy object
 is different from the DNS proxy rule’s service route. Using
 the DNS proxy object’s service route.
```

- どの DNS サーバー プロファイルにもサービス ルートが定義されていない場合は、必要に応じてグローバル サービス ルートが使用されます。

「ユース ケース3：ファイアウォールがクライアントとサーバー間の DNS プロキシとして機能する場合

このユース ケースでは、ファイアウォールが DNS クライアントと DNS サーバーの間に位置します。ファイアウォール上の DNS プロキシは、ファイアウォール インターフェイスに接続されたテナントのネットワーク上に存在するホストの DNS サーバーとして機能します。こうしたシナリオでは、ファイアウォールはデータプレーン上で DNS 解決を実行します。



このシナリオでは、スプリット *DNS* を使用しており、ドメイン名の一致に基づいて、DNS 要求を DNS サーバー セットにリダイレクトするように DNS プロキシ ルールが設定されています。一致がない場合はサーバー プロファイルが、要求の送信先となる DNS サーバーを決定します。そのため、2 つのスプリットされた DNS 解決方法が存在します。

データプレーンの *DNS* 解決の場合、*PAN-OS* の *DNS* プロキシから外部の *DNS* サーバーに送信される *IP* アドレスは通常、プロキシのアドレス（元の要求の宛先 *IP*）です。*DNS* サーバー プロファイルで定義されているサービス ルートは使用されません。たとえば、要求がホスト *172.16.1.1* から *192.168.1.1* の *DNS* プロキシに送信される場合、（*10.10.10.10* の）*DNS* サーバーへの要求は、送信元に *192.168.1.1*、宛先に *10.10.10.10* を使用します。

STEP 1 | **Network (**ネットワーク**)** > **DNS Proxy (DNS** プロキシ**)** を選択して **Add (**追加**)** をクリックします。

STEP 2 | **Enable** [有効化]をクリックして、DNS プロキシの **Name** [名前]を入力します。

STEP 3 | **Location** [場所]には、テナントの仮想システムを選択します。この例では、Corp1 Corporation （vsys6）です

STEP 4 | **Interface** [インターフェイス]では、テナントのホストから DNS 要求を受信するインターフェイスを選択します。この例では、Ethernet1/20 です。

STEP 5 | **Server Profile** [サーバー プロファイル]を選択または作成して、このテナントの DNS 要求を解決する DNS サーバーをカスタマイズします。

STEP 6 | **DNS Proxy Rules (DNS** プロキシ ルール**)** タブでルールの **Name (**名前**)** を **Add (**追加**)** します。

STEP 7 | （任意）**Turn on caching of domains resolved by this mapping** （このマッピングによって解決されるドメインのキャッシングをオンにする） を選択します。

STEP 8 | 各行に 1 項目ずつ **Domain Name (**ドメイン名**)** を **Add (**追加**)** します。DNS プロキシ ルールおよび FQDN マッチングは、ファイアウォールが FQDN をどのように DNS プロキシ ルール内のドメイン名とマッチさせるのかを指定します。

STEP 9 | **DNS Server profile (DNS** サーバー プロファイル**)** については、プロファイルを選択します。ファイアウォールが、DNS 要求のドメイン名を、**DNS Proxy Rules** [DNS プロキシ ルール]で定義されたドメイン名と比較します。一致がある場合は、このルールで定義された **DNS Server profile** [DNS サーバー プロファイル]を使用して DNS サーバーが決定されます。

STEP 10 | この例では、要求のドメインが myweb.corp1.com と一致した場合に、myweb DNS サーバー プロファイルで定義された DNS サーバーが使用されます。一致がない場合は、**Server Profile** [サーバー プロファイル]で定義された DNS サーバー（Corp1 DNS サーバー プロファイル）が使用されます。

STEP 11 | **OK** を 2 回クリックします。

DNS プロキシ ルールおよび FQDN マッチング

DNS プロキシ ルールを使用する DNS プロキシ オブジェクトをファイアウォールに設定する際、ファイアウォールは DNS クエリに含まれる FQDN を、DNS プロキシ ルールにあるドメイン名と比較します。ファイアウォールによる比較は、以下のように動作します。

DNS プロキシ ルールに対して **FQDN** を比較	例
ファイアウォールはまず DNS プロキシ ルール内のドメイン名および FQDN をトークン化します。ドメイン名の中で、ピリオド（.）で区切られた文字列がトークンになります。	***.boat.fish.com** consists of four tokens: **[*] [boat][fish][com]**
マッチ プロセスは、ルール内のドメイン名と FQDN のトークンを完全に一致させる作業です。部分文字列はマッチされません。	ルール： **fishing** **fish** – マッチなし
完全一致の条件の例外になるのが、ワイルドカード（アスタリスク（*））の使用です。* は、一つあるいは複数のトークンにマッチします。 つまり、ワイルドカード（*）だけで構成されたルールは、トークンを持つすべての FQDN にマッチします。	ルール：***.boat.com** **www.boat.com** – マッチ **www.blue.boat.com** – マッチ **boat.com** – マッチなし
	ルール ： ***** **boat** – マッチ **www.boat.com** – マッチ **www.boat.com** – マッチ
* はトークンの前、間、後ろなど、どの位置でも使用できます（ただし、一つのトークン内で別の文字と併用することはできません）。	ルール： **www.*.com** **www.boat.com** – マッチ **www.blue.boat.com** – マッチ
	ルール： **www.*.com** **www.boat.com** – マッチ **www.boat.fish.com** – マッチ
	www.boat*.com – 不正

DNS プロキシ ルールに対して FQDN を比較	例
トークンの前、間、後ろなど、ドメイン名のどの位置でも複数のワイルドカード（*）を挿入できます。連続しない * は、それぞれ一つあるいは複数のトークンにマッチします。	ルール： **a.*.d.*.com** **a.b.d.e.com** – マッチ **a.b.c.d.e.f.com** – マッチ **a.d.d.e.f.com** – マッチ（最初の * が **d** にマッチ、2 つ目の * が **e** および **f** にマッチ） **a.d.e.f.com** – マッチなし（最初の * が **d** にマッチ、ルールの 後続の **d** はマッチなし）
連続したトークン内でワイルドカードを使用すると、最初の * が一つあるいは複数のトークンにマッチし、2 つ目の * が一つのトークンにマッチします。 つまり、* だけで構成されたルールは、2 つ以上のトークンを持つすべての FQDN にマッチします。	トークンの前に来る連続したワイルドカード： ルール： ***.*.boat.com** **www.blue.boat.com** – マッチ **www.blue.sail.boat.com** – マッチ
	トークンの間にある連続したワイルドカード： ルール： **www.*.com** **www.blue.sail.boat.com** – マッチ **www.big.blue.sail.boat.com** – マッチ
	トークンの後ろに来る連続したワイルドカード： ルール： **www.*.com** **www.boat.fish.com** – マッチ **www.boat.fish.ocean.com** – マッチ
	連続したワイルドカードのみ： ルール： *.* **boat** – マッチなし **www.boat.com** – マッチ **www.boat.com** – マッチ

DNS プロキシ ルールに対して FQDN を比較	例
連続したワイルドカードと連続していないワイルドカードを一つのルールで使用できます。	ルール： **a.*.d.*.com** **a.b.c.d.e.f.com** – マッチ（最初の * が **b** および **c** にマッチ、2 つ目の * が **e** にマッチ、3 つ目の * が **f** にマッチ） **a.b.c.d.e.com** – マッチなし（最初の * が **b** および **c** にマッチ、2 つ目の * が **e** にマッチ、3 つ目の * はマッチなし）
暗黙的な後方一致の挙動により、さらに表現が簡潔になります。 ルールの最後のトークンが * でない限り、ルールにない末尾のトークンが FQDN に追加で存在する場合でも、ルール内のすべてのトークンが FQDN にマッチするのであれば、比較結果がマッチになります。	ルール： **www.*.com** **www.boat.fish.com** – マッチ **www.boat.fish.ocean.com** – マッチ **www.boat.fish** – マッチ
このルールは * で終わっているため、暗黙的な後方一致ルールの動作は適用されません。* が前述の通りの動作をし、一つあるいは複数のトークンにマッチします。	ルール： **www.*.com** **www.boat.fish.com** – マッチ **www.boat.fish.ocean.com** – マッチ **www.boat.fish** – マッチなし（この FQDN には、ルールの * にマッチするトークンがありません）
FQDN が複数のルールにマッチする場合、タイブレーカーアルゴリズムによって最も具体的な（長い）ルールが選択されます。つまり、トークンの数が多く、ワイルドカード（*）の数が少ないルールを優先するアルゴリズムになっています。	ルール1： ***.fish.com** – マッチ ルール2： ***.com** – マッチ ルール3： **boat.fish.com** – マッチおよびタイブレーカー FQDN: **boat.fish.com** FQDN が 3 つのルールすべてにマッチしますが、ファイアウォールは最も具体的なルール 3 を使用します。
	ルール1：***.fish.com** – マッチなし ルール2： ***.com** – マッチ ルール3：**boat.fish.com** – マッチなし **fish.com**

DNS プロキシ ルールに対して FQDN を比較	例
	* がマッチするトークンがないため、FQDN はルール 1 にマッチしません。
	ルール1：***.fish.com** – マッチおよびタイブレーカー ルール2： ***.com** – マッチ ルール3：**boat.fish.com** – マッチなし FQDN: **blue.boat.fish.com** FQDN はルール 1 およびルール 2 にマッチします（* は一つあるいは複数のトークンにマッチするため）。ファイアウォールは最も具体的なルール 1 を使用します。
ワイルドカード（*）および暗黙的な後方一致ルールを使用する際、FQDN が複数のルールにマッチし、タイブレーカーアルゴリズムが各ルールを同等に重み付けする場合があります。 曖昧さを回避するために、暗黙的な後方一致あるいはワイルドカード（*）を持つルールが重複する場合は、末尾のトークンを明示して暗黙的な後方一致ルールをなくしてください。	変更元： ルール:**www.boat** 変更後： ルール: **www.boat.com**
DNS プロキシ ルールを作成して曖昧さおよび予期せぬ結果を回避するためのベストプラクティス	
ドメイン名にトップレベル ドメインを含めて、FQDN を複数のルールにマッチさせる可能性がある暗黙的な後方一致の発生を防ぎます。	**boat.com**
ワイルドカード（*）を使用する場合は、左端のトークンとしてのみ使用してください。 この練習は、ワイルドカード DNS レコードおよび DNS の階層的性質の常識に従っています。	***.boat.com**
ルール内で * を複数使用しないでください。	

DNS プロキシ ルールに対して FQDN を比較	例
* を使用して DNS サーバーと関連付けられたベース ルールを構築し、より多くのトークンを持つルールを使用してルールの除外項目を増やし、異なるサーバーに関連付けます。 タイブレーカーアルゴリズムはマッチしたトークンの数に基づき、最も具体的なマッチを選択します。	ルール:***.corporation.com** – DNS サーバー A ルール:**www.corporation.com** – DNS サーバー B ルール:***.internal.corporation.com** – DNS サーバー C ルール:**www.internal.corporation.com** – DNS サーバー D **mail.internal.corporation.com** – DNS サーバー C にマッチ **mail.corporation.com** – DNS サーバー A にマッチ

DDNS

動的 DNS (DDNS) サービスがドメイン名と IP アドレスのマッピングを更新して、DNS クライアントに正確な IP アドレスを提供する方法について説明します。

ダイナミック DNS の概要

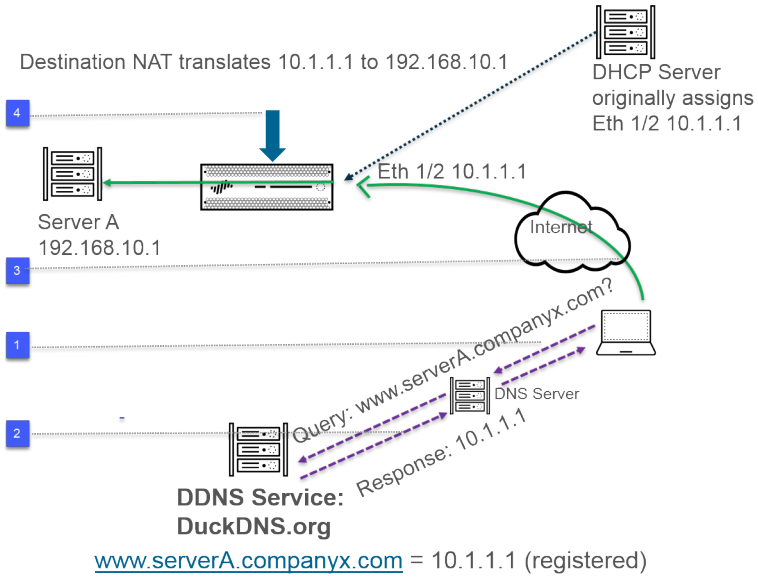
ファイアウォールの後ろでホストされているサービスがあり、ファイアウォール上で宛先 NAT ポリシーを使用してそれらのサービスに接続する、あるいはファイアウォールへのリモート アクセスを可能にする必要がある場合、インターフェイスの IPv4 アドレス変更 (インターフェイスが動的アドレスを受信する、あるいは固定アドレスを持つ DHCP クライアントかどうかによる) あるいは IPv6 アドレス変更 (固定アドレスのみ) をダイナミック DNS (DDNS) サービスプロバイダに登録できます。DDNS サービスは自動的にドメイン名対 IP アドレスのマッピングを更新して DNS クライアントに正確な IP アドレスを提供し、それによってファイアウォールの後ろにあるサービスおよびファイアウォールにアクセスできるようになります。DDNS は、サービスをホストしているブランチ デプロイメントでよく使用されます。ファイアウォールのインターフェイスで DDNS がサポートされていない場合は、クライアントに正確な IP アドレスを提供するために外部コンポーネントが必要になります。

ファイアウォールでは、次のDDNS サービスプロバイダがサポートされています：DuckDNS、DynDNS、FreeDNS Afraid.org Dynamic API、FreeDNS Afraid.org、および No-IP。ホスト名に対してサポートする IP アドレスの数、IPv6 アドレスをサポートするかどうかなど、提供するサービスは各 DDNS サービスプロバイダが決定します。Palo Alto Networks®はコンテンツの更新を使用して、新しいDDNSサービスプロバイダを追加し、そのサービスにアップデートを提供します。

ファイアウォールは現行の *Palo Alto Networks* コンテンツ リリース バージョンに基づいて *DDNS* 設定を維持するため、高可用性 *(HA)* 構成の場合、*HA* ファイアウォール ピア *(*アクティブ*/*パッシブあるいはアクティブ*/*アクティブ*)* のコンテンツ バージョンが同期されていることを確認してください。*Palo Alto Networks* はコンテンツ リリースを通じて既存の *DDNS* サービスを変更したり、非推奨にしたりすることができます。さらに、*DDNS* サービスプロバイダは提供するサービスを変更できます。*HA* ピア間でコンテンツ リリース バージョンが異なると、*DDNS* サービスを使用する機能に問題が生じるおそれがあります。

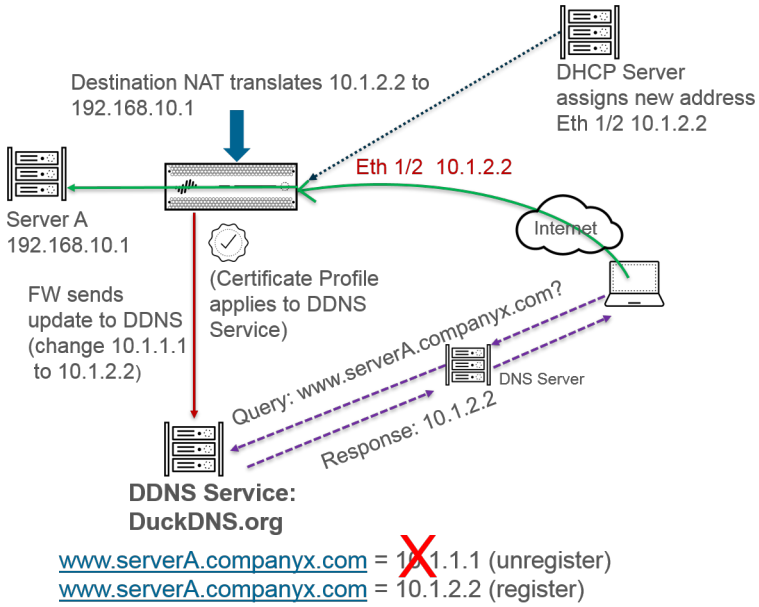
ファイアウォールは *Point-to-Point Protocol over Ethernet (PPPoE)* 終着点であるインターフェイスを介した *DDNS* をサポートしていません。

次の例では、ファイアウォールは DDNS サービスプロバイダの DDNS クライアントです。最初に、DHCP サーバーが IP アドレス 10.1.1.1 を Ethernet 1/2 インターフェイスに割り当てます。宛先 NAT ポリシーがパブリックな 10.1.1.1 をファイアウォールの後ろにあるサーバー A の実際のアドレス (192.168.10.1) に変換します。



1. ユーザーが www.serverA.companyx.com とやり取りしようとする際、ユーザーはそのローカル DNS サーバーに IP アドレスを求めます。www.serverA.companyx.com (例えば、duckdns.org レコード serverA.companyx.duckdns.org への CNAME として設定) は DDNS プロバイダー (この例では DuckDNS) に属すドメインです。DNS サーバーは DDNS プロバイダーにレコードを問い合わせてクエリを解決します。
2. DNS サーバーは、www.serverA.companyx.com の IP アドレスである 10.1.1.1 を使ってユーザーに応答します。
3. 宛先が 10.1.1.1 であるユーザーのパケットがファイアウォールのインターフェイス、Ethernet 1/2 に向かいます。
4. この例では、パケットを宛先に送信する前にファイアウォールが宛先 NAT を実行して 10.1.1.1 を 192.168.10.1 に変換します。

ある程度時間が経過したら、DHCP が新しい IP アドレスをファイアウォールのインターフェイスに割り当て、それによって次のように DDNS 更新が行われます：



1. DHCP サーバーが新しい IP アドレス (10.1.2.2) を Ethernet 1/2 に割り当てます。
2. 新しいアドレスを受信すると、ファイアウォールは www.serverA.companyx.com の新しいアドレスを伴う更新を DDNS サービスに送信し、それを DDNS サービスが登録します。(また、ファイアウォールは設定された更新間隔に基づいて通常の更新も送信します。ファイアウォールは HTTPS ポート 443 を介して DDNS 更新を送信します)。

結果として、次に www.serverA.companyx.com の IP アドレスをクライアントが DNS サーバーに求める、DNS サーバーが DDNS サービスをチェックする際、DDNS サービスは更新されたアドレス (10.1.2.2) を送信します。そのため、ユーザーは更新されたインターフェイスのアドレスを使ってファイアウォールのインターフェイスを介してサービスあるいはアプリケーションに正しくアクセスできます。

ファイアウォールが *HA* アクティブ/パッシブ モードで構成されている場合、*2* つの *HA* ファイアウォールの状態が決定する間に必ずファイアウォールが *DDNS* 更新を *DDNS* サービスに送信するようにしてください。*HA* 状態が決定した後、パッシブ ファイアウォール上で *DDNS* が無効になります。例えば、*2* つの *HA* ファイアウォールが最初に起動する際、*HA* アクティブとパッシブ モードのどちらの状態なのか判断できるまで、両方が *DDNS* 更新を送信します。この間、まだシステム ログに *DDNS* 更新が記録されます。*HA* 状態が決定し、各ファイアウォールがそのクライアントにアクティブあるいはパッシブな状態であると通知した後、パッシブ ファイアウォールは *DDNS* 更新を送信しなくなります。*(HA* アクティブ/アクティブ モードでは、各ファイアウォールが独立した *DDNS* 設定を持ち、*DDNS* 設定を同期しません*)*。

ファイアウォールインターフェイスのダイナミック DNS を構成する

ファイアウォールインターフェイスの DDNS を構成する前に：

- DDNS プロバイダーに登録したホスト名を決定します。
- DDNS サービスからパブリック SSL 証明書を取得し、ファイアウォールにインポートします。
- (FreeDNS Afraid.org v1 または FreeDNS Afraid.org Dynamic API v1 を使用する場合) DDNS サーバーでは、Dynamic DNS service タブには次のオプションが含まれます。**Link updates of the same IP together? (**同じ **IP** の更新をリンクしますか？**)**このオプションを有効にすると、DDNS サービスは、単一のホスト名と IP アドレスの DNS レコードだけでなく、変更中の古い IP アドレスを含む DNS レコードのすべてのホスト名を更新します。更新する予定のないホストの DNS レコードが更新されないようにするには、DDNS サーバーが、DDNS 更新に含まれる新しい IP アドレスで特定のホスト名を含む DNS レコードのみを更新するようにするため、 **Link updates of the same IP together? (**同じ **IP** の更新をリンクしますか？**)** オプションを無効にする必要があります。

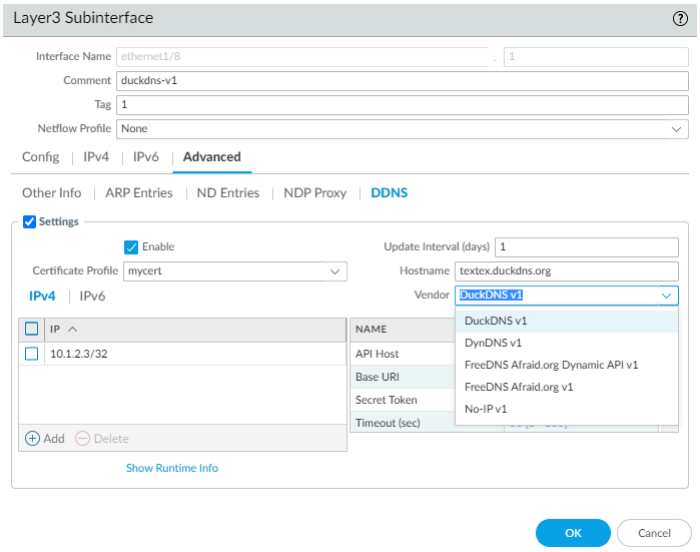
STEP 1 | DDNS を設定する。

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、レイヤー 3 インターフェイス、サブインターフェイス、または集約イーサネット (AE) インターフェイスを選択します。または、**Network (**ネットワーク**)** > **Interfaces (**インターフェイス**)** > **VLAN** を選択して、インターフェイスまたはサブインターフェイスを選択します。
2. **Advanced (**詳細**)** > **DDNS** を選択し、**Settings (**設定**)** を選択します。
3. DDNS を **Enable (**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て部分的な設定を失わないようにすることができます。)
4. 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 **Update Interval (days) (**更新間隔 **(**日数**))** を入力します (範囲は 1～30、デフォルトは 1)。IP アドレスの変更頻度に基づいて間隔を選択します。(ファイアウォールが定期的に送信する更新は、アドレス変更の受信時にファイアウォールが送信する更新に追加されます。定期的に送信される更新は、アドレスの変更ごとに送信される更新が失われないようにするためです。)
5. DDNS サービスに既に登録されているインターフェイスの **Hostname (**ホスト名**)** (例：www.serverA.companyx.com または serverA) を入力します。

   このホスト名が、*DDNS* サービスに登録したホスト名と一致することを確認してください。ホスト名に *FQDN* を入力する必要があります。*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。
6. **IPv4** を選択し、インターフェイスに割り当てられた 1 つ以上の IPv4 アドレスを選択するか、ホスト名に関連付ける IPv4 アドレスを **Add (**追加**)** します (例：10.1.1.1)。IPv4 アドレスは DDNS サービス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 IPv4 アドレスは DDNS サービスに登録されています。少なくとも 1 つの IPv4 または 1 つの IPv6 アドレスを選択します。

7. **IPv6** を選択し、インターフェースに割り当てられた 1 つ以上の IPv6 アドレスを選択するか、ホスト名に関連付ける IPv6 アドレスを **Add (追加)** します。IPv6 アドレスは DDNS サービス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 IPv6 アドレスは DDNS サービスに登録されています。少なくとも 1 つの IPv4 または 1 つの IPv6 アドレスを選択します。
8. DDNS サービスからインポートされた SSL 証明書を使用して 新しい証明書プロファイル (**Certificate Profile (証明書プロファイル)**) を選択または作成し、ファイアウォールが最初に DDNS サービスに接続して IP アドレスを登録するたびに、DDNS サービスの SSL 証明書を検証します。ファイアウォールが DDNS サービスに接続して更新を送信すると、DDNS サービスは、認証局 (CA) によって署名された SSL 証明書をファイアウォールに提示し、ファイアウォールが DDNS サービスを認証できるようにします。
9. DDNS サービスに使用している **Vendor (ベンダー)** (およびバージョン番号) を選択します。



Palo Alto Networks®は、コンテンツの更新を通じてサポートされている *DDNS* サービス プロバイダーを変更する可能性があります。

[仕入先] フィールドの *Palo Alto Network DDNS* の選択は、*SD-WAN* や *ZTP* などの *Palo Alto Networks* 機能用の予約済み *DDNS* サービスであり、この現在のタスクには選択しないでください。対応するサポート機能が有効になっていないときに誤って *Palo Alto Networks DDNS* を選択すると、エラーメッセージが表示されます。

10. ベンダーの選択により、Vendor (ベンダー) フィールドにある **Name (名前)** および **Value (値)** フィールドが決まります。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の値フィールドもあります。DDNS サービスが提供するパスワードや、DDNS サービスから更新を受信し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、残りの値フィールドを構成します。
11. **OK** をクリックします。

STEP 2 | (任意) 管理インターフェース以外のインターフェースを使用してファイアウォールが DDNS サービスと通信するようにする場合は、DDNS のサービスルートを設定します (外部サービスのネットワークアクセスの設定)。

STEP 3 | 変更をコミットします。

STEP 4 | インターフェイスの DDNS 情報を表示します。

1. **Network (ネットワーク)** > **Interfaces (インターフェイス)** > **Ethernet (イーサネット)** または **Network (ネットワーク)** > **Interfaces (インターフェイス)** > **VLAN** を選択し、設定したインターフェイスを選択します。(DDNS が設定されたインターフェイスでは、Features (機能) フィールドに DDNS アイコン が表示されます。)
2. **Advanced (詳細)** > **DDNS** および **Settings (設定)** を選択します。
3. ランタイム情報を表示 **(Show Runtime Info)** して、最後のリターンコード (最終の FQDN 更新の結果) や DDNS サービスが FQDN 更新を受信した最終時刻 (日付と時刻) など、インターフェイスの DDNS 情報を確認します。

NAT

このセクションでは、ネットワーク アドレス変換（NAT）と、NAT用のファイアウォールの設定方法について説明します。NAT では、ルーティングできないプライベート IPv4 アドレスをグローバルにルーティングできる 1 つ以上の IPv4 アドレスに変換するため、組織のルーティング可能な IP アドレスを節約できます。NATを使用すれば、公開アドレスにアクセスする必要があるホストの真のIPアドレスを非公開にし、ポート転送によってトラフィックを管理できるようになります。また、NATにより同一の IP サブネットのネットワークが相互通信できるようにして、ネットワーク設計の課題を解決できます。ファイアウォールはレイヤー3およびバーチャル ワイヤ インターフェイス上でNATをサポートしています。

NAT64オプションでは、異種 IP アドレス スキームを使用して、ネットワーク間の接続（IPv6 アドレスへの移行パス）を提供し、IPv6 アドレスと IPv4 アドレスを変換します。IPv6 間ネットワーク接頭辞変換（NPTv6）は、IPv6 プレフィックスを別の IPv6 プレフィックスに変換します。PAN-OS では、これらのすべての機能をサポートしています。

内部ネットワークでプライベート IP アドレスを使用する場合、プライベート アドレスを外部ネットワークにルーティングできるパブリック アドレスに変換するために、NAT を使用する必要があります。PAN-OS では、変換が必要なパケット アドレスとポート、および変換後のアドレスとポートについてファイアウォールに指示する NAT ポリシー ルールを作成します。

NAT ポリシー ルール

- NAT ポリシーの概要
- アドレス オブジェクトとして識別される NAT アドレス プール
- NAT アドレス プールのプロキシ ARP

NAT ポリシーの概要

少なくとも、パケットの送信元ゾーンと宛先ゾーンを照合する NAT ルールを設定します。ゾーンの他に、パケットの宛先インターフェイス、送信元アドレス、宛先アドレス、およびサービスに基づいて、照合基準を設定できます。複数の NAT ルールを設定できます。ファイアウォールは、上から下にルールを評価します。パケットが 1 つの NAT ルールの基準に一致すると、そのパケットにはその他の NAT ルールは適用されません。そのため、NAT ルールのリストは、最も具体的なルールから最も抽象的なルールの順序になっている必要があります。こうすることで、作成した中で最も具体的なルールがパケットに適用されます。

スタティック NAT ルールは、他の形式の NAT よりも優先されません。そのため、スタティック NAT が機能するには、ファイアウォールのリストでスタティック NAT ルールが他のすべての NAT ルールよりも上になるようにする必要があります。

NAT ルールでは、パケットを許可または拒否するセキュリティ ポリシー ルールとは異なり、アドレス変換が提供されます。ファイアウォールで NAT ルールおよびセキュリティ ポリシー ルールを適用する場合、定義したゾーンに応じて必要なルールを決定できるように、ファイアウォールのフロー ロジックを理解することが重要です。セキュリティポリシー ルールがNATトラフィックを許可するように設定する必要があります。

ファイアウォールは、入力時にパケットを調査して、ルート検索を行い、出力インターフェイスおよびゾーンを決定します。その後、ファイアウォールは、送信元ゾーンや宛先ゾーンに基づいて、そのパケットが定義済みの NAT ルールのいずれかと一致するかどうかを検査します。次に、NAT 後のゾーンではなく、元の（NAT 前の）送信元アドレスと宛先アドレスに基づいて、パケットと一致するセキュリティ ポリシーを評価および適用します。最後に、ファイアウォールは、一致する NAT ルールで出力時に送信元アドレスや宛先アドレスおよびポート番号を変換します。

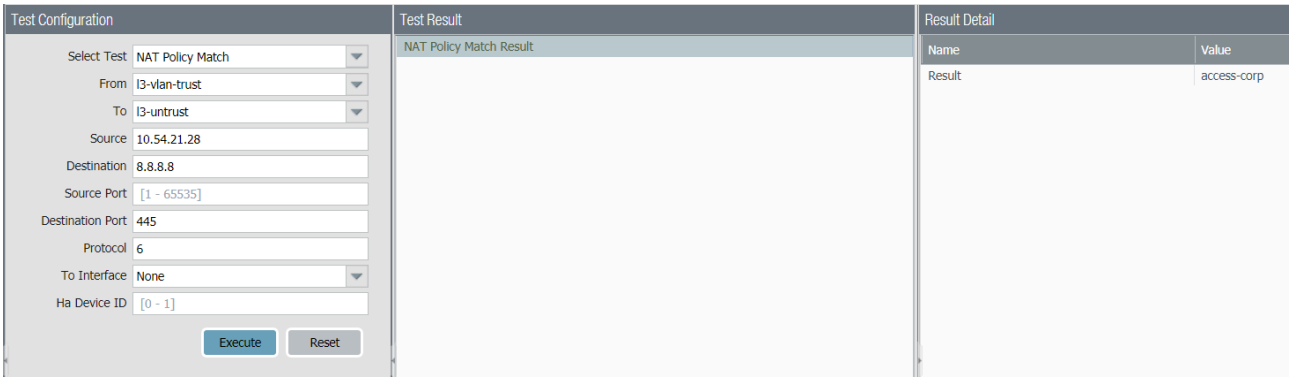
IP アドレスおよびポートの変換は、パケットがファイアウォールから送信されるまで行われません。NAT ルールおよびセキュリティ ポリシーは、元の IP アドレス（NAT 前の IP アドレス）に適用されます。NAT ルールは、NAT 前の IP アドレスに関連付けられたゾーンに基づいて設定されます。

セキュリティ ポリシーは、NAT 後のゾーンを調査して、パケットを許可するかどうかを決定するため、NAT ルールとは異なります。NAT の本質は、送信元 IP アドレスまたは宛先 IP アドレスを変更することにあります。そのため、パケットの発信インターフェイスおよびゾーンが変更される可能性があるので、セキュリティ ポリシーは NAT 後のゾーンに適用されます。

コール マネージャーが電話の代わりに*SIP*メッセージを送信して接続をセットアップするため、*SIP*コールはファイアウォールを通過する際に一方向音声になる時があります。コール マネージャーからのメッセージがファイアウォールに達すると、*SIP ALG*が*NAT*を介して電話の*IP*アドレスをプットしなければなりません。コール マネージャーおよび電話が別のセキュリティ ゾーンにある場合、コール マネージャーのゾーンを使用して電話の*IP*アドレスの*NAT*ルックアップが行われます。*NAT* ポリシーではこのことを考慮する必要があります。

非 NAT ルールを設定して、後の NAT ポリシーで定義される NAT ルールの範囲から除外する IP アドレスを設定できます。非 NAT ポリシーを定義するには、すべての一致条件を指定し、送信元変換列のNo Source Translation（送信元変換なし）を選択します。

処理された NAT ルールは、**Device (デバイス)** > **Troubleshooting (トラブルシューティング)**を選択し、NAT ルールのトラフィック マッチをテストすることで確認できます。以下に例を示します。



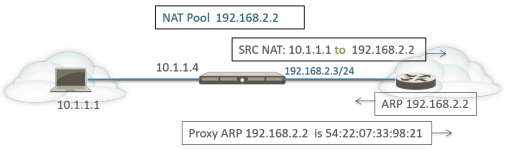
アドレス オブジェクトとして識別される NAT アドレス プール

通常、NAT ポリシー ルールで **Dynamic IP** [ダイナミック IP] または **Dynamic IP and Port** [ダイナミック IP およびポート] NAT アドレス プールを設定する場合、アドレス オブジェクトを使用して、変換後アドレスのプールを設定します。各アドレス オブジェクトは、ホスト IP アドレス、IP アドレス範囲、または IP サブネットになります。

アドレス オブジェクトは、*NAT* ルールとセキュリティ ポリシールールの両方で使用されるため、*NAT* で使用されるアドレス オブジェクトの名前に「*NAT-name*」などのプレフィックスを付けて、これらを区別することをお勧めします。

NAT アドレス プールのプロキシ ARP

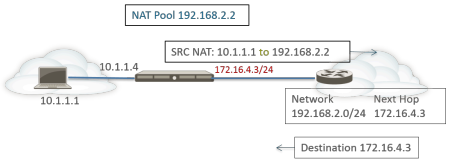
NAT アドレス プールは、どのインターフェイスにもバインドされません。以下の図は、NAT アドレス プールのアドレスに対してプロキシ ARP を実行するときのファイアウォールの動作を示しています。



ファイアウォールは、クライアントの送信元 NAT を実行し、送信元アドレス 10.1.1.1 を NAT プールのアドレス 192.168.2.2 に変換します。変換されたパケットはルーターに送信されます。

リターン トラフィックでは、ルーターは 192.168.2.2 に到達する方法がわからないため（IP アドレスは、NAT アドレス プールのアドレスであるため）、ARP 要求パケットをファイアウォールに送信します。

- アドレス プール（192.168.2.2）が出力/入力インターフェイスの IP アドレス（192.168.2.3/24）と同じサブネットにある場合、ファイアウォールは、IP アドレスのレイヤー 2 MAC アドレスを示すプロキシ ARP 応答をルーターに送信できます（上の図を参照）。
- アドレス プール（192.168.2.2）がファイアウォールのインターフェイスのサブネットでない場合、ファイアウォールはプロキシ ARP 応答をルーターに送信しません。つまり、リターン トラフィックがファイアウォールに戻されるようにするには、192.168.2.2 宛てのパケットの送信先を知るために必要なルートがルーターに設定されている必要があります（下の図を参照）。



送信元 NAT と宛先 NAT

ファイアウォールでは、送信元アドレスとポートの変換、宛先アドレスとポートの変換のどちらにも対応します。

- 送信元NAT
- 宛先NAT (DNAT)

送信元NAT

通常、送信元 NAT は内部ユーザーがインターネットに接続するために使用します。送信元アドレスは変換されるため、非公開にしておくことができます。送信元 NAT のタイプは 3 つあります。

- ダイナミック **IP** およびポート**(DIPP)** – 複数のホストの送信元 IP アドレスを同じパブリック IP アドレス（ポート番号は異なる）に変換できます。**[**変換後アドレス**]** プール（IP アドレス、アドレスの範囲、サブネット、またはこれらの組み合わせ）として設定した NAT アドレス プールの次に使用可能なアドレスに動的に変換されます。

  DIPP では、NAT アドレス プールの次のアドレスを使用する代わりに **Interface** [インターフェイス]自体のアドレスを指定できます。NAT ルールでインターフェイスを指定することの利点は、インターフェイスで取得されるアドレスを使用するように NAT ルールが自動的に更新されることです。DIPP は、インターフェイス ベースの NAT やネットワーク アドレス ポート変換（NAPT）と呼ばれることもあります。

  DIPP には、デフォルトの NAT オーバーサブスクリプション率があります。これは、同じ変換後 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。詳細は、ダイナミック IP およびポート NAT オーバーサブスクリプションおよびDIPP NAT のオーバーサブスクリプション率の変更をご参照ください。

  （第 *2* 世代の *PA-7050-SMC-B* または *PA-7080-SMC-B Switch Management Card (*スイッチ マネジメント カード*- SMC)* を使用しない *PA-7000 Series* のファイアウォールのみに影響）*DIPP NAT* でポイントツーポイント トンネル プロトコル（*PPTP*）を使用する場合 、ファイアウォールは、変換された *IP* アドレスとポートのペアを *1* つの接続のみに使用するように制限されます。（ファイアウォールは *DIPP NAT* をサポートしていません。）回避策は、*PA-7000 Series* のファイアウォールを第 *2* 世代の *SMC-B* カードにアップグレードすることです。

- ダイナミック **IP** – 送信元 IP アドレスのみ（ポート番号なし）を NAT アドレス プールの次に使用可能なアドレスに 1 対 1 で動的に変換できます。NAT プールのサイズは、アドレス変換を必要とする内部ホストの数と同じにする必要があります。デフォルトでは、送信元アドレス プールが NAT アドレス プールよりも大きく、最終的にすべての NAT アドレスが割り当てられると、アドレス変換を必要とする新しい接続はドロップされます。このデフォルトの動作をオーバーライドするには、**Advanced (Dynamic IP/Port Fallback)** [詳細 (ダイナミック IP ポートのフォールバック)]を使用して、必要なときに DIPP アドレスを使用できるようにしま

す。セッションが停止するか、プールのアドレスが使用可能になると、新しい接続を変換するためにアドレスを割り当てることができます。

ダイナミック IP NAT では、ダイナミック IP NAT アドレスの予約を行うためのオプションがサポートされています。

- スタティック **IP** – 送信元 IP アドレスを 1 対 1 で静的に変換できます。ただし、送信元ポートはそのまま変わりません。スタティック IP 変換の一般的なシナリオは、インターネットで使用可能にする必要がある内部サーバーです。

宛先NAT (DNAT)

ファイアウォールが宛先アドレスを別の宛先アドレスに変換する際、インバウンド パケット上で宛先 NAT が実行されます。例えば、公開宛先アドレスをプライベートな宛先アドレスに変換します。また、宛先 NAT は、ポート転送やポート変換を実行するオプションも提供します。

宛先 NAT により、静的および動的変換が可能です：

- 静的 **IP**– 1 対 1 の静的な変換であり、いくつかのフォーマットで設定することができます。変換済みパケットの形式が同じであり、同じ数の IP アドレスを指定している場合、元のパケットが単一の宛先 IP アドレス、IP アドレスの範囲、または IP ネットマスクのどれを持つのか指定できます。ファイアウォールは静的に元の宛先アドレスを毎回同じ宛先アドレスへと変換します。つまり、宛先アドレスが複数ある場合、ファイアウォールは常に同じ変換を行い、元のパケット用に設定された最初の宛先アドレスを、変換済みパケット用に設定された最初の宛先アドレスへと変換し、設定済みの 2 つ目の元のパケットを、設定済みの 2 つ目の変換済みパケットへと変換し、それ以降も同様に変換していきます。

  宛先 NAT を使用して静的 IPv4 アドレスを変換する場合、ファイアウォールの片側で DNS サービスを使用して別の側のクライアントのために FQDN を解決することもできます。IPv4 アドレスを含む DNS 応答がファイアウォールを通過する際、DNS サーバーは外部デバイスに内部 IP アドレスを提供するか、その逆を行います。PAN-OS 9.0.2 およびそれ以降の 9.0 リリースから、ファイアウォールを設定して (ルールにマッチする) DNS 応答の IP アドレスを書き換え、クライアントが適切なアドレスを受信して宛先サービスに到達することができるようになっています。対象のDNS の書き換えのユースケースは、書き換えを設定する方法を示しています。

- 動的 **IP (セッション配布を伴う)** –宛先 NAT を使用すると、元の宛先アドレスを、の動的 IP アドレス を持つ宛先ホストまたはサーバーに変換できます。動的 IP (セッション分散を伴う) は IPv4 アドレスのみをサポートしています。動的 IP アドレスを使用する宛先 NAT は、通常は動的 IP アドレス指定を使用するクラウド デプロイメントで特に有用です。

  変換済みの宛先アドレスが複数のアドレスに解決される場合、ファイアウォールはインバウンドの NAT セッションを複数のアドレスに配信し、セッションの配信を強化します。ラウンドロビン (デフォルトの方式)、ソース IP ハッシュ、IP モジュロ、IP ハッシュ、最小セッションのいずれかに基づいて分散が行われます。DNS サーバーが FQDN に 32 を超える IPv4 ア

ドレスを返した場合、ファイアウォールはパケット内の最初の 32 個のアドレスを使用します。

変換後アドレスが *IPv6* アドレスにしか解決されないタイプの *FQDN* アドレス オブジェクトである場合、宛先 *NAT* ポリシールールは *FQDN* を未解決として扱います。

Dynamic IP (with session distribution)（動的 **IP**（セッション分散）） を使用すると、複数の NAT 前の宛先 IP アドレス（ *M* ）を複数のNAT 後の宛先 IP アドレス（ *N* ）に変換できます。多対多の変換は、単一の NAT ルールを使用した *M* x *N* 個の宛先 NAT 変換であることを意味します。

宛先 *NAT* の場合、ベストプラクティスは次のとおりです。

- スタティック *IP* アドレスには***Static IP***（スタティック ***IP***）アドレス変換を使用します。これにより、ファイアウォールは元の宛先 *IP* アドレスの数が変換された宛先 *IP* アドレスの数と等しいことを確認し、保証できます。
- *FQDN* ベースのダイナミック アドレスに対してのみ、***Dynamic IP (with session distribution)***（ダイナミック ***IP***（セッション分散））アドレス変換を使用します（ファイアウォールは *IP* アドレス番号のチェックを実行しません）。

以下はファイアウォールが許可する宛先 NAT 変換の一般的例です：

変換タイプ	元のパケットの宛先アドレス	変換済みパケットの宛先アドレスにマッピング	メモ
スタティック **IP**	192.168.1.1	2.2.2.2	元のパケットおよび変換済みパケットは、宛先アドレスの候補をそれぞれ 1 つ持ちます。
	192.168.1.1-192.168.1.4	2.2.2.1-2.2.2.4	元のパケットおよび変換済みパケットは、宛先アドレスの候補をそれぞれ 4 つ持ちます。 192.168.1.1 は必ず 2.2.2.1 にマッピングします。 192.168.1.2 は必ず 2.2.2.2 にマッピングします。 192.168.1.3 は必ず 2.2.2.3 にマッピングします。 192.168.1.4は必ず 2.2.2.4 にマッピングします。

変換タイプ	元のパケットの宛先アドレス	変換済みパケットの宛先アドレスにマッピング	メモ
	192.168.1.1/30	2.2.2.1/30	元のパケットおよび変換済みパケットは、宛先アドレスの候補をそれぞれ 4 つ持ちます。 192.168.1.1 は必ず 2.2.2.1 にマッピングします。 192.168.1.2 は必ず 2.2.2.2 にマッピングします。 192.168.1.3 は必ず 2.2.2.3 にマッピングします。 192.168.1.4は必ず 2.2.2.4 にマッピングします。
動的 **IP**（セッション分散）	192.168.1.1/30	domainname.com	元のパケットには 4 つの宛先アドレスがあり、たとえば、変換された宛先アドレスの FQDN が 5 つの IP アドレスに解決された場合、1つの NAT ルールに 20 の宛先 NAT 変換が可能です。

宛先 NAT の一般的な用途の 1 つは、いくつかの NAT ルールを設定し、単一のパブリック宛先アドレスを、サーバーまたはサービスに割り当てられているいくつかのプライベート宛先ホストアドレスにマッピングすることです。この場合、宛先ポート番号を使用して宛先ホストが識別されます。以下に例を示します。

- ポート転送 – パブリック宛先アドレスとポート番号をプライベート宛先アドレスに変換できます。ただし、ポート番号はそのまま変わりません。
- ポート変換 – パブリック宛先アドレスとポート番号をプライベート宛先アドレスと別のポート番号に変換できます。したがって、実際のポート番号を非公開にしておくことができます。ポート転送を設定するには、NAT ポリシー ルールの **Translated Packet (**変換済みパケット**)** タブで、**Translated Port (**変換済みポート**)** を入力します。ポート変換を使用した宛先 NAT の例を参照してください。

DNS 書き換えを伴う宛先 NAT のユースケース

宛先 NAT を使用して IPv4 アドレスを別の IPv4 アドレスに静的に変換する際、クライアントの FQDN を解決するためにファイアウォールの片側で DNS サービスも使用することになります。IP アドレスを伴う DNS 応答がファイアウォールを介してクライアントに向かう際、ファイアウォールはその IP アドレスに対して NAT を実行しないため、DNS サーバーは内部 IP アドレ

スを外部デバイスに提供、あるいはその逆を行い、結果として DNS クライアントが宛先サービスに接続できなくなります。

こうした問題を避けるため、NATポリシー ルール用に設定した変換済み IPアドレスに基づいて (A レコードから) ファイアウォールを設定して DNS 応答の IPアドレスを書き換えることができるようになっています。ファイアウォールは、クライアントに応答する前に DNS 応答内の IPv4 アドレスに対して NAT を実行します (FQDN 解決)。そのため、クライアントは適切なアドレスを受信して宛先サービスに到達できます。単一の NAT ポリシー ルールにより、ファイアウォールがルールにマッチするパケットに NAT を実行するようになり、また元の宛先アドレスあるいはルール内の変換済み宛先アドレスにマッチする DNS 応答内の IP アドレスに対して NAT を実行するようになります。

DNSの書き換えはグローバル レベルで行われます。ファイアウォールは、元のパケット タブの宛先アドレスを変換されたパケット タブの宛先アドレスにマップします。Original Packet (元のパケット) タブ上のその他すべてのフィールドは無視されます。DNS 応答パケットが到着すると、ファイアウォールは、次のように、方向に基づいて、マップされた宛先アドレスのいずれかに一致する A レコードが応答に含まれているかどうかを確認します。

ファイアウォールが NAT ルールに対する DNS 応答の IP アドレスに対して NAT を実行する方法を指定する必要があります逆方向または 転送 :

- **reverse(逆)**—DNS 応答がルールの**Translated (変換された)** 宛先アドレスと一致する場合、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 IPアドレスを **1.1.1.10** から **192.168.1.10** に変換する場合、ファイアウォールは DNS 応答を **192.168.1.10** から **1.1.1.10**に書き換えます。
- **forward(順)**—DNS 応答がルールの**Original (元の)** 宛先アドレスと一致する場合、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 IPアドレスを **1.1.1.10** から **192.168.1.10** に変換する場合、ファイアウォールは DNS 応答を **1.1.1.10** から **192.168.1.10** に書き換えます。

> *DNS* 書き換えが無効化されている、オーバーラップした *NAT* ルールがあり、その下に *DNS* 書き換えが有効でオーバーラップに含まれている *NAT* ルールがある場合、ファイアウォールはオーバーラップした *NAT* ルールに従って *DNS* 応答を書き換えます (***reverse* (逆)** あるいは ***forward* (順)** 設定のいずれか)。書き換えが優先され、*NAT* ルールの順序は無視されます。

DNS 書き換えを設定するユースケースを検討してください :

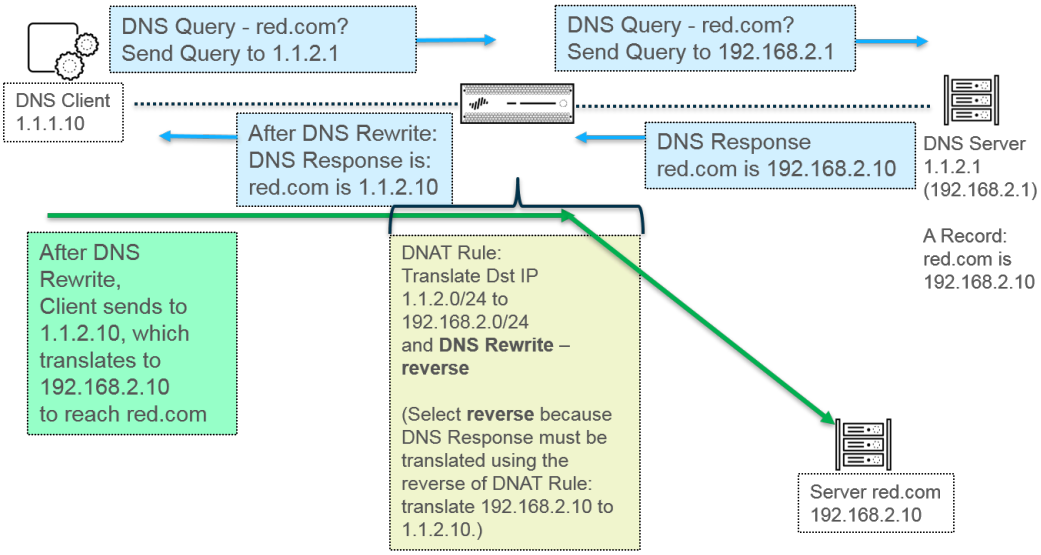
- 逆方向の DNS 書き換えを伴う宛先 NAT のユースケース
- 順方向の DNS 書き換えを伴う宛先 NAT のユースケース

逆方向の DNS 書き換えを伴う宛先 NAT のユースケース

次のユースケースでは、**reverse (逆)** 方向のDNS 書き換えを伴う宛先 NAT を示します。これら 2 つのユースケースの違いは、単に DNS クライアント、DNS サーバー、宛先サーバーがパブリックな場所にあるか、ファイアウォールに隔てられた内部にあるかどうかです。どちらのケースでも、DNS クライアントはファイアウォールを隔てて最終宛先サーバーと逆の側にあります。(DNS クライアントと最終宛先サーバーがファイアウォールを隔てて同じ側にある場合、順方向の DNS 書き換えを伴う宛先 NAT のユースケース 3 および 4 を検討してください。)

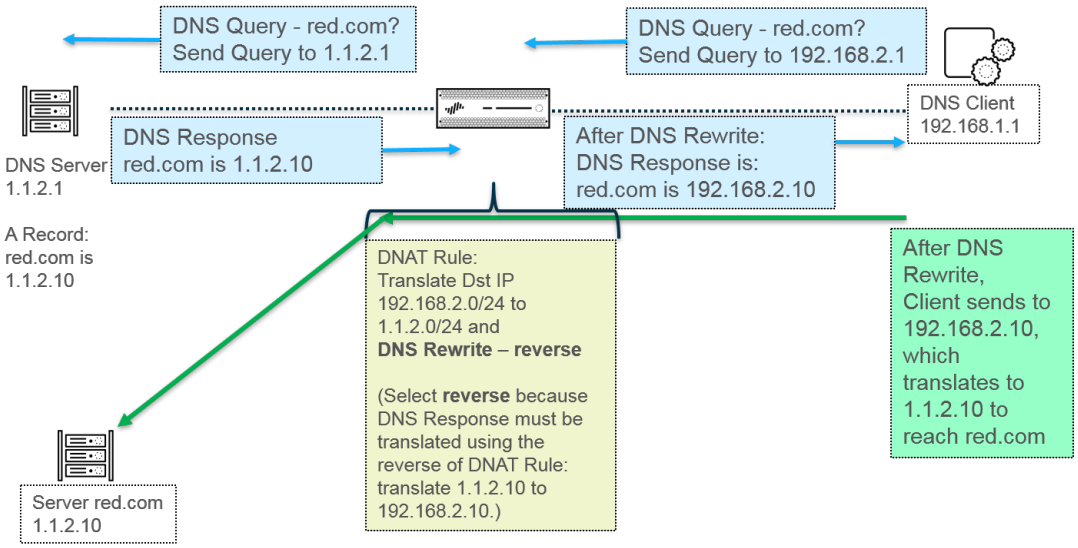
ユースケース 1 では、ファイアウォールのパブリックな側に DNS クライアントがあり、DNS サーバーおよび最終宛先サーバーがどちらも内側にある場合を示します。このケースでは逆方向の DNS 書き換えが必要になります。DNS クライアントは red.com の IP アドレスを求めます。ファイアウォールは NAT ルールに基づいて (元はパブリック アドレス 1.1.2.1 に向かう) クエリを内部アドレス 192.168.2.1 に変換します。DNS サーバーは red.com の IP アドレスが 192.168.2.10. であると応答します。ルールには **DNS** 書き換え - 逆方向を有効化が含まれており、192.168.2.10 の DNS 応答はルールの 192.168.2.0/24 の宛先変換アドレスにマッチするため、ファイアウォールはルールが使用する **reverse (逆)** 変換を使って DNS 応答を変換します。ルールは 1.1.2.0/24 を 192.168.2.0/24 に変換するよう指定しているため、ファイアウォールは 192.168.2.10 の DNS 応答を 1.1.2.10 に書き換えます。DNS クライアントが応答を受信して 1.1.2.10 に送信し、それをルールが 192.168.2.10 に変換してサーバー red.com に到達できるようにします。

ユース ケース1 のまとめ：DNS クライアントと宛先サーバーがファイアウォールを隔てて別の側にあります。DNS サーバーが NAT ルールの変換済み宛先アドレスにマッチするアドレスを提供するため、NAT ルールの **reverse (逆)** 変換を使用して DNS 応答を変換します。



ユースケース 2 では、ファイアウォールの内部に DNS クライアントがあり、DNS サーバーおよび最終宛先サーバーがどちらもパブリックな側にある場合を示します。このケースでは逆方向の DNS 書き換えが必要になります。DNS クライアントは red.com の IP アドレスを求めます。ファイアウォールは NAT ルールに基づいて (元は内部アドレス 192.168.2.1 に向かう) クエリをパブリック アドレス 1.1.2.1 に変換します。DNS サーバーは red.com の IP アドレスが 1.1.2.10 であると応答します。ルールには **DNS** 書き換え - 逆方向を有効化が含まれており、 1.1.2.10 の DNS 応答はルールの 1.1.2.0/24 の宛先変換アドレスにマッチするため、ファイアウォールはルールが使用する **reverse (逆)** 変換を使って DNS 応答を変換します。ルールは 192.168.2.0/24 を 1.1.2.0/24 に変換するよう指定しているため、ファイアウォールは 1.1.2.10 の DNS 応答を 192.168.2.10 に書き換えます。DNS クライアントが応答を受信して 1.1.2.10 に送信し、それをルールが 192.168.2.10 に変換してサーバー red.com に到達できるようにします。

ユースケース2 のまとめはユースケース 1 のまとめと同じです。DNS クライアントと宛先サーバーがファイアウォールを隔てて別の側にあります。DNS サーバーが NAT ルールの変換済み宛先アドレスにマッチするアドレスを提供するため、NAT ルールの **reverse (逆)** 変換を使用して DNS 応答を変換します。



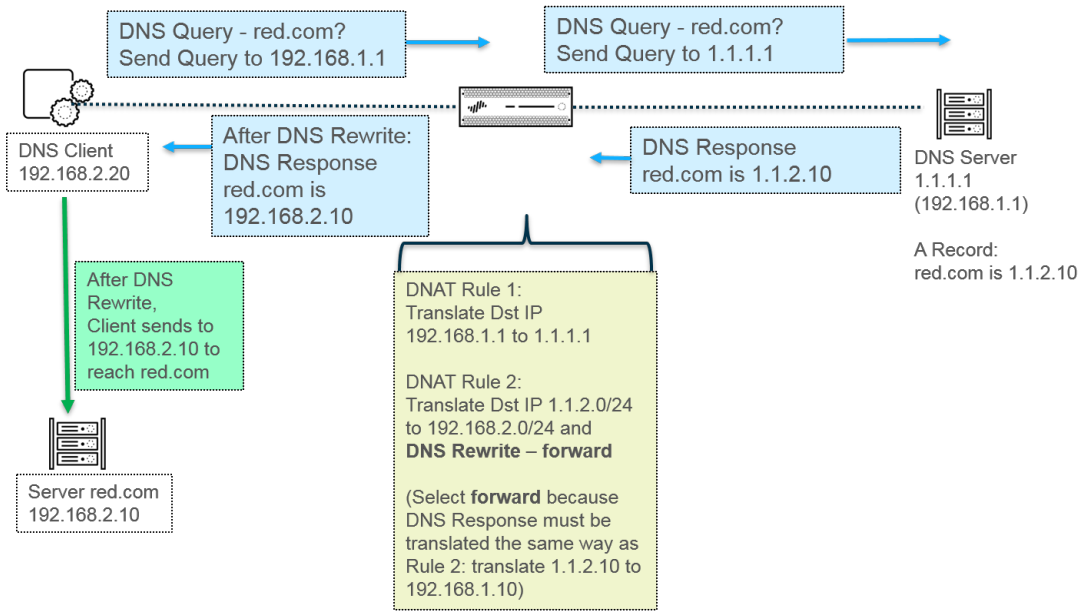
DNS 書き換えを実装するには、DNS 書き換えを伴う宛先 NAT の設定を行います。

順方向の DNS 書き換えを伴う宛先 NAT のユースケース

次のユースケースでは、**forward (順)** 方向のDNS 書き換えを伴う宛先 NAT を示します。これら 2 つのユースケースの違いは、単に DNS クライアント、DNS サーバー、宛先サーバーがパブリックな場所にあるか、ファイアウォールに隔てられた内部にあるかどうかです。どちらのケースでも、DNS クライアントはファイアウォールを隔てて最終宛先サーバーと同じ側にあります。(DNS クライアントと最終宛先サーバーがファイアウォールを隔てて逆の側にある場合、逆方向の DNS 書き換えを伴う宛先 NAT のユースケース 1 および 2 を検討してください。)

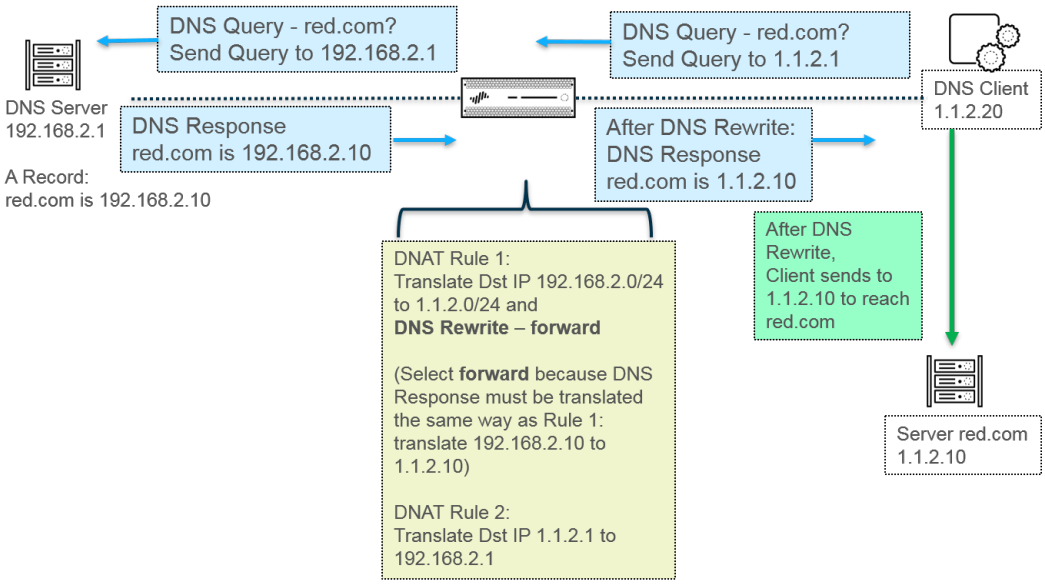
ユースケース 3 では、ファイアウォールの内側に DNS クライアントおよび最終宛先サーバーが両方あり、DNS サーバーがパブリックな側にある場合を示します。このケースでは順方向の DNS 書き換えが必要になります。DNS クライアントは red.com の IP アドレスを求めます。ファイアウォールはルール 1 に基づいて (元は内部アドレス 192.168.1.1 に向かう) クエリを 1.1.1.1 に変換します。DNS サーバーは red.com の IP アドレスが 1.1.2.10 であると応答します。ルール 2 は、**DNS** 書き換え - 順方向を有効化が含まれており、1.1.2.10 の DNS 応答はルール 2 の 1.1.2.0/24 の元の宛先アドレスにマッチするため、ファイアウォールはルールが使用する同じ変換を使って DNS 応答を変換します。ルール 2 は 1.1.2.0/24 を 192.168.2.0/24 に変換するよう指定しているため、ファイアウォールは 1.1.2.10 の DNS 応答を 192.168.2.10 に書き換えます。DNS クライアントが応答を受信してそれを 192.168.2.10 に送信し、サーバー red.com に到達できるようにします。

ユース ケース 3 のまとめ：DNS クライアントと宛先サーバーがファイアウォールを隔てて同じ側にあります。DNS サーバーが NAT ルールの同じ宛先アドレスにマッチするアドレスを提供するため、NAT ルールと同じ **forward (順)** 変換を使用して DNS 応答を変換します。



ユースケース 4 では、ファイアウォールのパブリックな側に DNS クライアントおよび最終宛先サーバーが両方あり、DNS サーバーが内側にある場合を示します。このケースでは順方向の DNS 書き換えが必要になります。DNS クライアントは red.com の IP アドレスを求めます。ファイアウォールはルール 2 に基づいて (元はパブリックな宛先 1.1.2.1 に向かう) クエリを 192.168.2.1 に変換します。DNS サーバーは red.com の IP アドレスが 192.168.2.10. であると応答します。ルール 1 は、**DNS** 書き換え - 順方向を有効化が含まれており、192.168.2.10 の DNS 応答はルール1 の192.168.2.0/24 の元の宛先アドレスにマッチするため、ファイアウォールはルールが使用する同じ変換を使って DNS 応答を変換します。ルール1 は 1.1.2.0/24 を 192.168.2.0/24 に変換するよう指定しているため、ファイアウォールは 1.1.2.10 の DNS 応答を 192.168.2.10 に書き換えます。DNS クライアントが応答を受信してそれを 1.1.2.10 に送信し、サーバー red.com に到達できるようにします。

ユースケース 4 のまとめはユースケース 3 のまとめと同じです。DNS クライアントと宛先サーバーがファイアウォールを隔てて同じ側にあります。DNS サーバーが NAT ルールの同じ宛先アドレスにマッチするアドレスを提供するため、NAT ルールと同じ **forward (順)** 変換を使用して DNS 応答を変換します。



DNS 書き換えを実装するには、DNS 書き換えを伴う宛先 NAT の設定を行います。

NAT ルールのキャパシティ

許可される NAT ルールの数は、ファイアウォール モデルに基づいています。個々のルールの制限は、スタティック、ダイナミック IP （DIP）、ダイナミック IP およびポート（DIPP）NAT で設定されます。これらの NAT タイプで使用されるルールの合計数は、NAT ルールの合計キャパシティを超えることはできません。DIPP の場合、ルールの制限は、ファイアウォールのオーバーサブスクリプション設定（8、4、2、1）と、ルールごとに 1 つの変換後 IP アドレスという前提に基づいています。モデル固有の NAT ルールの制限および変換後 IP アドレスの制限を確認するには、ファイアウォールの比較ツールを使用します。

NAT ルールを処理する場合、以下の事項を考慮します。

- プールのリソースがなくなった場合、モデルの最大ルール数に達していなくても、それ以上 NAT ルールを作成することはできません。
- NAT ルールを統合すると、ログとレポートも統合されます。統計情報は、ルール内のすべてのアドレスごとではなく、ルールごとに提供されます。詳細なログおよびレポートが必要な場合は、ルールを統合しないでください。

ダイナミック IP およびポート NAT オーバーサブスクリプション

ダイナミック IP およびポート（DIPP）NAT では、変換後 IP アドレスとポートの各ペアを同時セッションで複数回（8、4、2）使用できます。この IP アドレスおよびポートの再利用可能性（オーバーサブスクリプションと呼ばれる）により、パブリック IP アドレスが少なすぎる顧客に拡張性を提供できます。この設計は、異なる宛先にホストが接続されていて、セッションを一意に識別でき、競合がほとんど発生しないという前提に基づいています。実際には、オーバーサブスクリプション率でアドレス/ポート プールの元のサイズを乗算して、8、4、2 倍のサイズにします。たとえば、許可される同時セッション数のデフォルトの制限が 64,000 の場合、オーバーサブスクリプション率 8 で乗算すると、許可される同時セッション数は 512,000 になります。

許可されるオーバーサブスクリプション率は、モデルによって異なります。オーバーサブスクリプション率は、グローバルにファイアウォールに適用されます。このオーバーサブスクリプション率は、デフォルトで設定されていて、オーバーサブスクリプションが必要ないほど十分なパブリック IP アドレスがあってもメモリを消費します。オーバーサブスクリプション率をデフォルト設定からより低い設定または（オーバーサブスクリプションなし）に減らすことができます。オーバーサブスクリプション率を減らすと、送信元デバイスの変換可能数は減少しますが、DIP および DIPP NAT ルール キャパシティは増加します。デフォルトのオーバーサブスクリプション率を変更する方法については、「DIPP NAT のオーバーサブスクリプション率の変更」を参照してください。

Platform Default (プラットフォームのデフォルト**)** を選択すると、オーバーサブスクリプションの明示的な設定はオフになり、以下の表に示すように、プラットフォーム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。**[**プラットフォームのデフォルト**]** 設定では、ソフトウェア リリースのアップグレードまたはダウングレードを行うことができます。

以下の表に、各モデルのデフォルト（最高）のオーバーサブスクリプション率を示します。

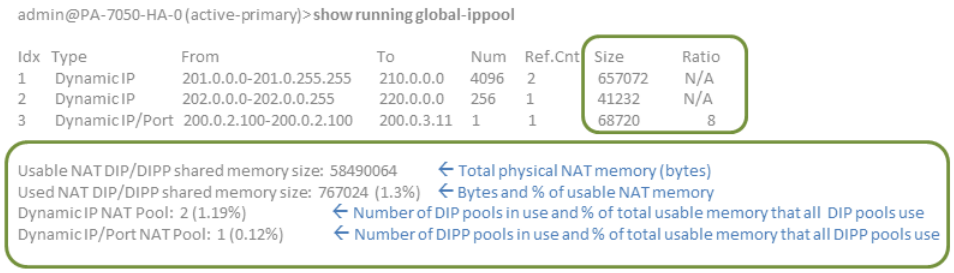
モデル	デフォルトのオーバーサブスクリプション率
PA-220	2
PA-820IPv6	2
PA-850	2
PA-3220	4
PA-3250	4
PA-3260	4
PA-5220IPv6	8

モデル	デフォルトのオーバーサブスクリプション率
PA-5250IPv6	8
PA-5260IPv6	8
PA-5280	8
PA-7050IPv6	8
PA-7080IPv6	8
VM-50	2
VM-100	2
VM-200	2
VM-300	2
VM-500	8
VM-700IPv6	8
VM-1000-HVIPv6	2

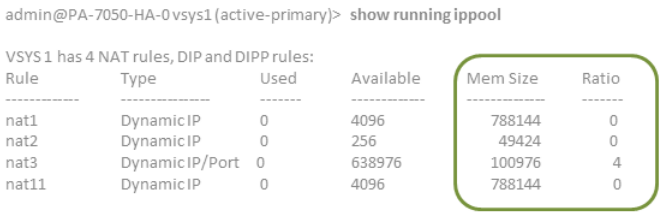
ファイアウォールでは、NAT ルールごとに最大 256 個の変換後 IP アドレスがサポートされています。また、各モデルでは、（統合されたすべての NAT ルールの）変換後 IP アドレスの最大数がサポートされています。オーバーサブスクリプションが原因で、ルールごとの変換後 IP アドレスの最大数（256）を超える場合、ファイアウォールは、コミットが成功するように自動的にオーバーサブスクリプション率を下げます。ただし、NAT ルールによる変換で、モデルの変換後アドレスの最大数を超える場合、コミットは失敗します。

データ プレーンの NAT メモリの統計情報

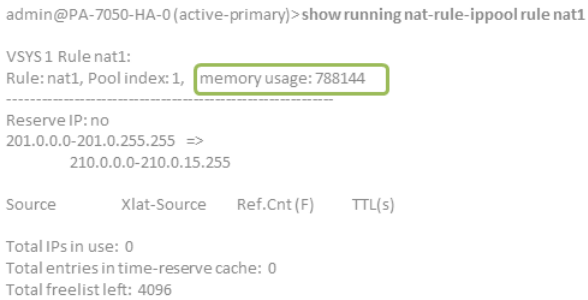
show running global-ippool コマンドを実行すると、プールの NAT メモリ消費量に関する統計情報が表示されます。Size 列には、リソース プールで使用しているメモリのバイト数が表示されます。Ratio 列には、オーバーサブスクリプション率が表示されます（DIPP プールのみ）。プールおよびメモリの統計情報の行については、以下のサンプル出力で説明します。



仮想システムの NAT プールの統計情報の場合、**show running ippool** コマンドの列には、使用されている NAT ルールごとのメモリ サイズとオーバーサブスクリプション率（DIPP ルールの場合）が表示されます。以下は、このコマンドのサンプル出力です。



show running nat-rule-ippool rule コマンドの出力のフィールドには、使用されている NAT ルールごとのメモリ（バイト）が表示されます。以下は、このコマンドのサンプル出力です（囲まれた部分がルールのメモリ使用量です）。

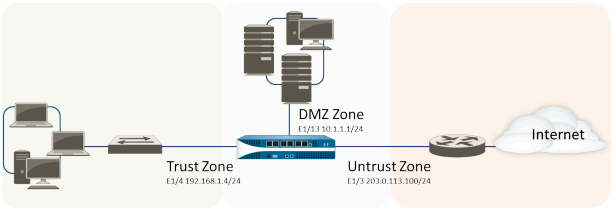


NAT の設定

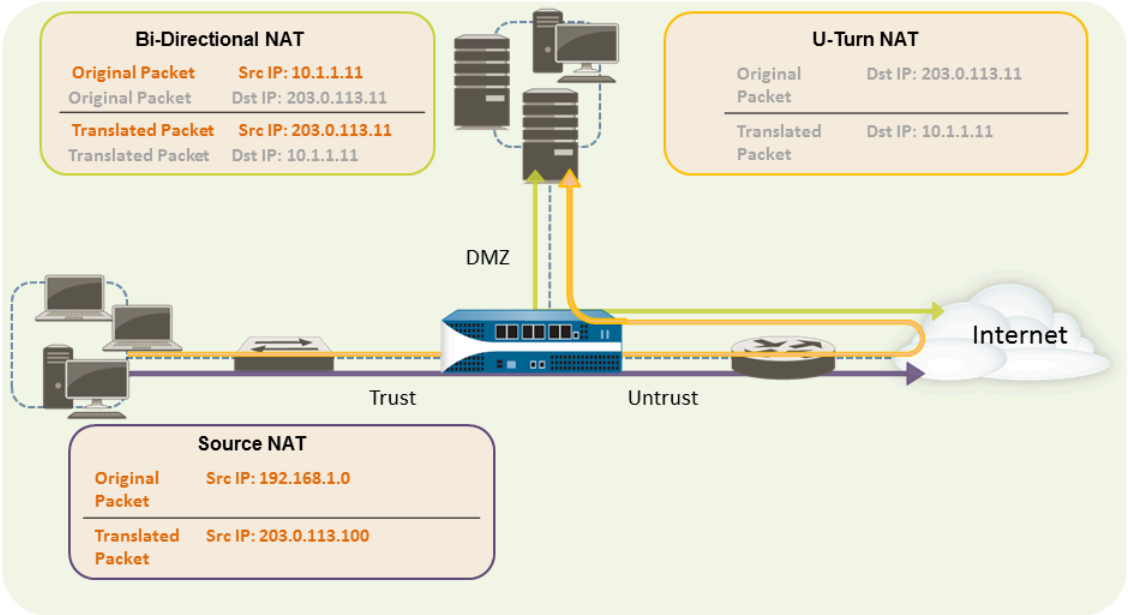
NAT のさまざまな機能を設定するには、以下の手順を実行します。下記以外の例については、NAT 設定の例セクションを参照してください。

- 内部クライアントの IP アドレスからパブリック IP アドレスへの変換（送信元 DIPP NAT）
- 内部ネットワークのクライアントからパブリック サーバーへのアクセスの有効化（宛先 U ターン NAT）
- パブリックフェイシング サーバーの双方向アドレス変換の有効化（送信元スタティック NAT）
- DNS 書き換えを伴う宛先 NAT の設定
- 動的 IP アドレスを使用した宛先 NAT の設定
- DIPP NAT のオーバーサブスクリプション率の変更
- ダイナミック IP NAT アドレスの予約
- 特定のホストまたはインターフェイスの NAT の無効化

このセクションの最初の 3 つの NAT の例は、次のトポロジーに基づいています。



次のように、このトポロジーに基づいて 3 つの NAT ポリシーを作成する必要があります。



- 内部ネットワークのクライアントからインターネット上のリソースにアクセスできるようにするには、内部アドレス 192.168.1.0 をルーティング可能なパブリック アドレスに変換する

必要があります。この場合、出力インターフェイス アドレス 203.0.113.100 を使用して、内部ゾーンからファイアウォールを通過するすべてのパケットの送信元アドレスとして、送信元 NAT （上記の紫色の囲いおよび矢印）を設定します。流れについては内部クライアントの IP アドレスからパブリック IP アドレスへの変換（送信元 DIPP NAT）を参照してください。

- 内部ネットワークのクライアントから DMZ ゾーンのパブリック Web サーバーにアクセスできるようにするには、外部ネットワークからのパケットをリダイレクトする NAT ルールを設定する必要があります。この場合、元のルーティング テーブルを検索することにより、パケット内の宛先アドレス 203.0.113.11 に基づき、DMZ ネットワーク上の Web サーバーが持つ実際のアドレス 10.1.1.11 に移動する必要があると判断します。このような変換を行うには、宛先アドレスを DMZ ゾーンのアドレスに変換するための、Trust ゾーン (パケットの送信元アドレスが存在する場所) から Untrust ゾーン (元の宛先アドレスが存在する場所) への NAT ルールを作成する必要があります。このタイプの宛先 NAT （上記の黄色の囲いおよび矢印）を「*U ターン NAT*」といいます。流れについては内部ネットワークのクライアントからパブリック サーバーへのアクセスの有効化（宛先 U ターン NAT）を参照してください。
- DMZ ネットワークのプライベート IP アドレスと、外部ユーザーがアクセスするパブリック フェイシング アドレスの両方を持つ Web サーバーで、要求を送受信できるようにするには、ファイアウォールでパブリック IP アドレスからプライベート IP アドレスに着信するパケットを、プライベート IP アドレスからパブリック IP アドレスに発信するパケットに変換する必要があります。ファイアウォールで双方向の送信元スタティック NAT のポリシー（上記の緑色の囲いおよび矢印）を 1 つ作成すれば、このような変換を実現できます。流れについてはパブリック フェイシング サーバーの双方向アドレス変換の有効化（送信元スタティック NAT）を参照してください。

内部クライアントの IP アドレスからパブリック IP アドレスへの変換（送信元 DIPP NAT）

内部ネットワークのクライアントから要求を送信する場合、パケットの送信元アドレスにその内部ネットワーク クライアントの IP アドレスが含まれます。プライベート IP アドレスの範囲を内部で使用している場合、ネットワークから発信されるパケットの送信元 IP アドレスをルーティング可能なパブリック アドレスに変換しない限り、クライアントのパケットをインターネットにルーティングできません。

送信元アドレスと送信元ポート（任意）とをパブリック アドレスに変換する送信元 NAT のポリシーをファイアウォールで設定すれば、このような変換を実現できます。その方法の 1 つとして、以下の手順に示すように、すべてのパケットの送信元アドレスをファイアウォールの出力インターフェイスに変換する方法があります。

STEP 1 | 使用する外部 IP アドレスのオブジェクトを作成します。

1. **Objects (オブジェクト)** > **Addresses (アドレス)** を選択し、オブジェクトの **Name (名前)** および任意で **Description (説明)** を **Add (追加)** します。
2. **Type (タイプ)** から **IP Netmask (IP ネットマスク)** を選択し、ファイアウォールの外部インターフェイスの IP アドレス (この例では 203.0.113.100) を入力します。
3. **OK** をクリックします。

ポリシーでアドレス オブジェクトを使用する必要がない場合でも、アドレス オブジェクトを作成しておけば、アドレスの参照基準となるポリシーを個別ではなく一括で更新できるなど、管理者の負担が軽減されるため、作成しておくのがベスト プラクティスです。

STEP 2 | NAT ポリシーを作成します。

1. **Policies (ポリシー)** > **NAT** の順に選択して **Add (追加)** をクリックします。
2. **[全般]** タブの **[名前]** にポリシーの分かりやすい名前を入力します。
3. （任意）タグを入力します。タグは、ポリシーをソートまたはフィルタリングできるようにするキーワードまたはフレーズです。
4. **NAT Type**[NAT タイプ] で **ipv4**（デフォルト）を選択します。
5. **Original Packet (元のパケット)** タブの **Source Zone (送信元ゾーン)**セクションで内部ネットワーク用に作成したゾーンを選択し (**Add (追加)** をクリックしてからゾーンを選択します)、**Destination Zone (宛先ゾーン)**リストでは外部ネットワーク用に作成したゾーンを選択します。
6. **Translated Packet (変換済みパケット)** タブで、画面の Source Address Translation (送信元アドレスの変換) セクションの **Translation Type (変換タイプ)** リストから **Dynamic IP And Port (ダイナミック IP およびポート)** を選択します。
7. **Address Type** [アドレス タイプ] には、2 つの選択肢があります。**Translated Address** [変換後アドレス] を選択して**Add** [追加] できたはずです。作成したアドレス オブジェクトを選択します。

   もう 1 つの **Address Type** [アドレス タイプ] は **Interface Address** [インターフェイス アドレス] です。この場合、変換後アドレスはインターフェイスの IP アドレスになります。これを選択した場合、**Interface** [インターフェイス]を選択し、インターフェイスに複数の IP アドレスがある場合は必要に応じて**IP Address** [IP アドレス] を選択します。
8. **OK** をクリックします。

STEP 3 | 変更をコミットします。

Commit（コミット）をクリックします。

STEP 4 | （任意）CLI にアクセスして、変換を確認します。

1. **show session all** コマンドを使用して、セッション テーブルを表示します。ここでは、送信元 IP アドレスとポートおよび対応する変換後 IP アドレスとポートを確認できます。
2. *show session id <id_number>* を使用して、セッションに関する詳細を表示します。
3. ダイナミック IP NAT を設定している場合、**show counter global filter aspect session severity drop | match nat** コマンドを使用して、NAT IP 割り当てが原因でセッションが失敗していないかどうかを確認します。新しい接続の変換時にダイナミック IP NAT プールのすべてのアドレスが割り当てられていると、そのパケットはドロップされます。

内部ネットワークのクライアントからパブリック サーバーへのアクセスの有効化（宛先 U ターン NAT）

内部ネットワークのユーザーが、DMZ にある企業 Web サーバーへのアクセス要求を送信する場合、DNS サーバーがパブリック IP アドレスを解決します。要求を処理する際に、ファイアウォールではパケットの元の宛先 (パブリック IP アドレス) を使用して、Untrust ゾーンの出力インターフェイスにパケットをルーティングします。Trust ゾーンのユーザーから要求を受信したときに、ファイアウォールで Web サーバーのパブリック IP アドレスを DMZ ネットワークのアドレスに変換する必要があると判断するには、以下のように、ファイアウォールから DMZ ゾーンの出力インターフェイスに要求を送信できるようにするための、宛先 NAT のルールを作成する必要があります。

STEP 1 | Web サーバーのアドレス オブジェクトを作成します。

1. **Objects (オブジェクト)** > **Addresses (アドレス)** を選択し、アドレス オブジェクトの **Name (名前)** および任意で **Description (説明)** を **Add (追加)** します。
2. **Type (タイプ)** については **IP Netmask (IP ネットマスク)** を選択し、Web サーバーのパブリック IPv4 アドレスを入力します（この例では 203.0.113.11）。

   Resolve（解決）をクリックすることで アドレス オブジェクトのタイプを **IP Netmask**（**IP** ネットマスク）から **FQDN** に切り替えることができ、また、FQDN が表示されたら、**Use this FQDN**（この **FQDN** を使用する）をクリックします。あるいは、**Type**（タイプ）の場合は、**FQDN** を選択してアドレス オブジェクトに使用するための FQDN を入力します。FQDNを入力して **Resolve**（解決） をクリックすると、FQDN が解決する IP アドレスがフィールドに表示されます。この IP アドレスを使用してアドレス オブジェクトの **Type**（タイプ）を FQDN から IP ネットマスクに切り替えるには、**Use this address**（このアドレスを使用）をクリックします。すると、**Type**（タイプ）がそのIP アドレスを含む **IP Netmask**（**IP** ネットマスク）に切り替わり、フィールドに表示されます。
3. **OK** をクリックします。

STEP 2 | NAT ポリシーを作成します。

1. **Policies (ポリシー)** > **NAT** の順に選択して **Add (追加)** をクリックします。
2. **[全般]** タブの **[名前]** に NAT ルールの分かりやすい名前を入力します。
3. **Original Packet (元のパケット)** タブの **Source Zone (送信元ゾーン)**セクションで内部ネットワーク用に作成したゾーンを選択し (**Add (追加)** をクリックしてからゾーンを選択します)、**Destination Zone (宛先ゾーン)**リストでは外部ネットワーク用に作成したゾーンを選択します。
4. **Destination Address (宛先アドレス)** セクションで、パブリック WEB サーバー用に作成したアドレス オブジェクトを **Add (追加)** します。
5. **Translated Packet (変換済みパケット)** タブで、宛先アドレスの返還、 **DTranslation Type**（変換タイプ）用に、**Static IP**（静的 **IP**） を選択し、DMZ ネットワーク上の Web サーバー インターフェイスに割り当てられた IP アドレス (この例では 10.1.1.11) を入力します。あるいは、**Translation Type (変換タイプ)** を **Dynamic IP (with session distribution) (動的 IP (セッション分散あり))** に選択し、**Translated Address (変換されたアドレス)** を IP ネットマスク、IP 範囲、あるいは FQDN を使用するアドレス オブジェクトまたはアドレスグループに入力することもできます。これらはいずれも DNS から複数のアドレスを返す可能性があります。変換済みの宛先アドレスが複数のアドレスに解決される場合、ファイアウォールは次の方法のいずれかに基づき、インバウンドの NAT セッションを複数のアドレスに配信します：**Round Robin (ラウンドロビン)** (デフォルトの方法)、**Source IP Hash (送信元 IP ハッシュ)**、**IP Modulo (IP モジュロ)**、**IP Hash (IP ハッシュ)**、あるいは **Least Sessions (最小セッション)**。
6. **OK** をクリックします。

STEP 3 | **Commit**（コミット）をクリックします。

パブリックフェイシング サーバーの双方向アドレス変換の有効化（送信元スタティック NAT）

パブリックフェイシング サーバーで、そのサーバーが実際に存在するネットワーク セグメントのプライベート IP アドレスが割り当てられている場合、出力時にサーバーの送信元アドレスを外部アドレスに変換する送信元 NAT のルールが必要となります。内部の送信元アドレス 10.1.1.11 を外部 Web サーバーのアドレス（この例では 203.0.113.11）に変換するスタティック NAT ルールを作成します。

ただし、パブリックフェイシング サーバーはパケットを送受信できる必要があります。パブリック アドレス（インターネット ユーザーからの着信パケットの宛先 IP アドレス）をプライベート アドレスに変換し、ファイアウォールから DMZ ネットワークへパケットをルーティングできるようにするための、相互ポリシーが必要となります。以下の手順に示すとおり、双方向のスタティック NAT ルールを作成します。双方向変換は、スタティック NAT のみのオプションです。

STEP 1 | Web サーバーの内部 IP アドレスのオブジェクトを作成します。

1. **Objects (オブジェクト)** > **Addresses (アドレス)** を選択し、オブジェクトの **Name (名前)** および任意で **Description (説明)** を **Add (追加)** します。
2. **Type (タイプ)**リストから **IP Netmask (IP** ネットマスク)を選択し、DMZ ネットワークのウェブサーバーの IP アドレス (この例では 10.1.1.11) を入力します。
3. **OK** をクリックします。

Web サーバーのパブリック アドレスに対するアドレス オブジェクトを作成していない場合は、そのオブジェクトも今すぐ作成する必要があります。

STEP 2 | NAT ポリシーを作成します。

1. **Policies (ポリシー)** > **NAT** の順に選択して **Add (追加)** をクリックします。
2. **[全般]** タブの **[名前]** に NAT ルールの分かりやすい名前を入力します。
3. s**Original Packet (元のパケット)**タブの **Source Zone (送信元ゾーン)** セクションで DMZ 用に作成したゾーンを選択し、(**Add (追加)** をクリックしてゾーンを選択します)、**Destination Zone (宛先ゾーン)**リストでは外部ネットワーク用に作成したゾーンを選択します。
4. **Source Address (送信元アドレス)** セクションで、内部 WEB サーバーのアドレス用に作成したアドレス オブジェクトを **Add (追加)** します。
5. **Translated Packet (変換済みパケット)**タブの **Source Address Translation (送信元アドレスの変換)**セクションで、**Translation Type (変換タイプ)**リストから **Static IP (静的 IP)**を選択し、**Translated Address (変換後アドレス)**リストから、外部 Web サーバーのアドレス用に作成したアドレス オブジェクトを選択します。
6. **Bi-directional**[双方向] フィールドで **Yes**[はい] を選択します。
7. **OK** をクリックします。

STEP 3 | コミットします。

Commit（コミット）をクリックします。

DNS 書き換えを伴う宛先 NAT の設定

IPv4 アドレスの静的変換を実行する宛先 NAT ポリシー ルールを設定する場合、ルールに設定された元の IP アドレスまたは変換された IP アドレスに基づいて、ファイアウォールが DNS 応答の IPv4 アドレスを書き換えることができるようにルールを構成することもできます。ファイアウォールは、レスポンスをクライアントに返す前に (ルールにマッチする) DNS 応答内の IPv4 アドレスに対して NAT を実行 (FQDN 解決) します。そのため、クライアントが適切なアドレスを受信して宛先サービスに到達できます。

書き換えを **reverse (逆方向)** で行うべきか **forward (順方向)** で行うべきか判断するのに役立つDNS 書き換えのユースケースを表示します。

DNS 書き換えを有効化する同じ *NAT* ルールで ***Bi-directional (双方向)*** 送信元アドレス変換を有効化することはできません。

STEP 1 | ルールにマッチする IPv4 アドレスの静的変換をファイアウォールが実行すること、および IPv4 アドレス (A レコードから) が NAT ルールの元の、あるいは変換後の宛先アドレスにマッチする際に DNS 応答内の IP アドレスをファイアウォールが書き換えること指定する宛先 NAT ポリシールールを作成します。

1. **Policies (ポリシー)** > **NAT** を選択して NATポリシー ルールを **Add (追加)** します。
2. (任意) **General (全般)** タブで、ルールの分かりやすい **Name (名前)** を入力します。
3. **NAT Type** [NAT タイプ]として、**ipv4** を選択します。
4. **Original Packet (元のパケット)** タブで、**Destination Address (宛先アドレス)** を**Add (追加)** します。

   また、送信元ゾーンまたは任意の 送信元ゾーンを選択する必要がありますが、*DNS*の書き換えはグローバルレベルで行われます。*[Original Packet(元のパケット)]* タブの宛先アドレスのみが一致します。*DNS* 書き換えは、*Original Package (元のパケット)* タブ上のその他すべてのフィールドを無視します。
5. **Translated Packet (変換済みパケット)** タブの Destination Address Translation (宛先アドレス変換) については、**Translation Type (変換タイプ)** を **Static IP (静的 IP)** にします。
6. **Translated Address (変換後アドレス)** を選択するか、新しいアドレスを入力します。
7. **Enable DNS Rewrite (DNS 書き換えを有効化)** して **Direction (方向)** を選択します：
   - NAT ルールが指定するのとは逆の変換が DNS 応答内の IPアドレスで求められる場合は **reverse (逆)** (デフォルト) を選択します。ルールの**Translated(変換後)**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 IPアドレス 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。
   - NAT ルールが指定するのと同じ変換が DNS 応答内の IPアドレスで求められる場合は **forward (順)** を選択します。ルールの**Original**（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 IPアドレス 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。
8. **OK** をクリックします。

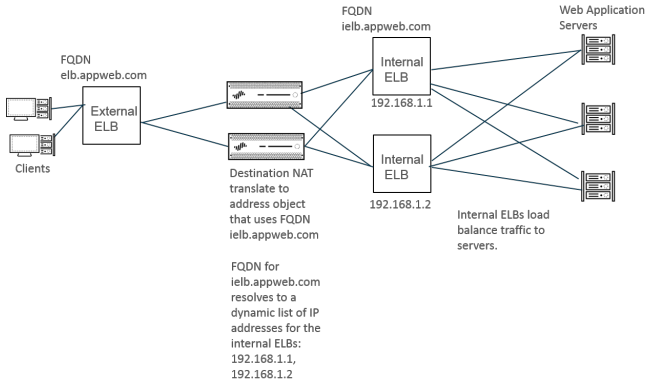
STEP 2 | 変更を **Commit (コミット)**します。

動的 IP アドレスを使用した宛先 NAT の設定

Destination NAT (宛先 NAT) を使用して、元の宛先アドレスを、ダイナミック IP アドレスを持ち FQDN を使用する宛先ホストまたはサーバーに変換します。動的 IP アドレスを使用する宛先 NAT は、通常は動的 IP アドレス指定を使用するクラウド デプロイメントで特に有用です。クラウド内のホストまたはサーバーに新しい（動的な）IP アドレスがある場合、DNS サーバーに継続的に問い合わせることによって NAT ポリシールールを手動で更新する必要はなく、DNS サーバーを更新するために別個の外部コンポーネントを使用して最新の FQDN-to-IP アドレスマッピングを使用する必要もありません。

動的 IP アドレスを使用して宛先 NAT を構成する場合は、FQDN のみを使用する必要があります (IP ネットマスクまたは IP 範囲は使用しないでください)。

次のトポロジ例では、クライアントはクラウド内の Web アプリケーションをホストしているサーバーにアクセスしたいと考えています。外部 Elastic Load Balancer（ELB）はファイアウォールに接続し、ファイアウォールはサーバーに接続する内部 ELB に接続します。たとえば、Amazon Web Services（AWS）は、サービスの需要に基づいて内部 ELB に割り当てられた FQDN の IP アドレスを追加（および削除）します。内部 ELB に NAT 用の FQDN を使用する柔軟性があることで、ポリシーが異なる時間に異なる IP アドレスを解決しやすくなり、更新が動的なので宛先 NAT の使用を容易化します。



STEP 1 | アドレスを変換するサーバーの FQDN を使用してアドレス オブジェクトを作成します。

1. **Objects**（オブジェクト） > **Addresses**（アドレス）を選択し、**post-NAT-Internal-ELB** などの**Name**（名前）ごとにアドレス オブジェクトを **Add**（追加）します。
2. **FQDN** を **Type**（タイプ）として選択し、FQDN を入力します。この例では FQDN は **ielb.appweb.com** です。
3. **OK** をクリックします。

STEP 2 | 宛先 NAT ポリシーを作成します。

1. **Policies**（ポリシー） > **NAT** を選択して、**General**（全般）タブの **Name**（名前）ごとの NAT ポリシー ルールを**Add**（追加）します。
2. **NAT Type**（**NAT** タイプ）として **ipv4** を選択します。
3. **Original Packet**（元のパケット）タブで、**Source Zone**（送信元ゾーン）と **Destination Zone**（宛先ゾーン）を **Add**（追加）します。
4. 宛先アドレス変換セクションの、**Translated Packet**（変換済みパケット）タブで、**Dynamic IP (with session distribution)**（動的 **IP**（セッション配信あり））を **Translation Type**（変換タイプ）に選択します。
5. [変換アドレス] の場合は、FQDN 用に作成したアドレス オブジェクトを選択します。この例では FQDN は **`post-NAT-Internal-ELB`** です。
6. **Session Distribution Method (**セッション分散方法**)** で、以下のいずれかを選択します。
   - **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。分散方法を変更する理由がない限り、ラウンドロビンが適切な分散方法になるでしょう。
   - **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 アドレスから来るトラフィックがある場合、送信元 IP ハッシュを選択せず、他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に基づい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。

     ファイアウォールは、複数の *IP* アドレスにセッションを分散する前に宛先 *IP* アドレスのリストから重複した *IP* アドレスを削除しません。ファイアウォールは、重複していないアドレスにセッションを分配するのと同じ方法で、重複したアドレスにセッションを分配します。(例えば、変換後アドレスがアドレス オブジェクトのアドレスグループであり、*1*つのアドレス オブジェクトが *IP* アドレスに解決される *FQDN* であり、一方もう*1*つのアドレス オブジェクトが同じ *IP* アドレスを含む範囲である場合には、変換プール内でアドレスの重複が発生します)。
7. **OK** をクリックします。

STEP 3 | 変更を **Commit (**コミット**)** します。

STEP 4 | (任意) ファイアウォールが FQDN をリフレッシュする頻度を設定できます(ユース ケース1：ファイアウォールには DNS 解決が必要)。

DIPP NAT のオーバーサブスクリプション率の変更

DIPP NAT のオーバーサブスクリプションを使用する必要のない十分なパブリック IP アドレスがある場合、オーバーサブスクリプション率を減らして、許可される DIP および DIPP NAT ルールを増やすことができます。

STEP 1 | DIPP NAT オーバーサブスクリプション率を表示します。

1. **Device (デバイス)** > **Setup (セットアップ)** > **Session (セッション)** > **Session Settings (セッション設定)** を選択します。**[NAT オーバーサブスクリプション率]** 設定を表示します。

STEP 2 | DIPP NAT オーバーサブスクリプション率を設定します。

1. Session Settings [セッション設定]セクションを編集します。
2. **NAT Oversubscription Rate (NAT オーバーサブスクリプション率)** リストで、目的のオーバーサブスクリプション率に応じて、**1x**、**2x**、**4x**、または **8x** を選択します。

   Platform Default (プラットフォームのデフォルト) 設定がモデルのデフォルトのオーバーサブスクリプション設定に適用されます。オーバーサブスクリプションが不要な場合は、***[1x]*** を選択します。
3. **[OK]** をクリックし、変更を **[コミット]** します。

ダイナミック IP NAT アドレスの予約

ダイナミック IP NAT アドレスを予約し（期間は設定可能）、変換が必要な別の送信元 IP アドレスに変換後アドレスとして割り当てられないようにすることができます。設定した予約は、進行中の変換と新しい変換のすべての変換後ダイナミック IP アドレスに適用されます。

進行中の変換と新しい変換のどちらも、送信元 IP アドレスが使用可能な変換後 IP アドレスに変換されると、その固有の送信元 IP に関連するすべてのセッションの有効期限が切れた後でもそのペアリングが保持されます。各送信元 IP アドレスの予約タイマーは、その送信元 IP アドレス変換を使用するすべてのセッションの有効期限が切れた後に開始されます。ダイナミック IP NAT は 1 対 1 の変換です。1 つの送信元 IP アドレスは、設定したプールで使用できるアドレスから動的に選択された 1 つの変換後 IP アドレスに変換されます。そのため、予約されている変換後 IP アドレスは、新しいセッションが開始されずに予約の有効期限が切れるまで、他の送信元 IP アドレスで使用することはできません。タイマーは、セッションが一定期間アクティブにならなかった後、送信元 IP/変換後 IP のマッピングの新しいセッションが開始されるたびにリセットされます。

デフォルトでは、どのアドレスも予約されていません。ファイアウォールまたは仮想システムのダイナミック IP NAT アドレスを予約できます。

ファイアウォールのダイナミック IP NAT アドレスを予約します。

以下のコマンドを入力します。

```
admin@PA-3250# set setting nat reserve-ip yes
```

```
admin@PA-3250# set setting nat reserve-time <1-604800 secs>
```

仮想システムのダイナミック IP NAT アドレスを予約します。

以下のコマンドを入力します。

```
admin@PA-3250# set vsys <vsysid>  setting nat reserve-ip yes
```

```
admin@PA-3250# set vsys <vsysid> setting nat reserve-time <1-604800
 secs>
```

たとえば、**nat reserve-time** が 28800 秒（8 時間）が設定されている場合に、30 個のアドレスが含まれるダイナミック IP NAT プールと、20 個の進行中の変換があるとします。現在、これらの 20 個の変換が予約されています。そのため、各送信元 IP/変換後 IP のマッピングを使用する（アプリケーションの）最後のセッションの有効期限が切れると、送信元 IP アドレスを再度変換する必要がある場合に備えて、変換後 IP アドレスがその送信元 IP アドレス専用に 8 時間予約されます。また、残りの 10 個の変換後アドレスが割り当てられると、各変換後アドレスが送信元 IP アドレス用に予約されます。各変換後アドレスのタイマーは、その送信元 IP アドレスの最後のセッションの有効期限が切れたときに開始されます。

このように、各送信元 IP アドレスをプールの同じ NAT アドレスに繰り返し変換することができます。その変換後アドレスにアクティブなセッションがない場合でも、プールの予約済み変換後 IP アドレスは別のホストに割り当てられません。

送信元 IP/変換後 IP のマッピングのすべてのセッションの有効期限が切れ、8 時間の予約タイマーが開始されるとします。その変換の新しいセッションが開始されると、タイマーが停止し、セッションはすべて終了するまで継続されます。すべて終了すると予約タイマーが再び開始され、変換後アドレスが予約されます。

ダイナミック IP NAT プールの予約タイマーは、**set setting nat reserve-ip no** コマンドを入力するか、**nat reserve-time** を別の値に変更して無効にするまで有効なままです。

予約用の CLI コマンドは、ダイナミック IP およびポート（DIPP）またはスタティック IP NAT プールには影響しません。

特定のホストまたはインターフェイスの NAT の無効化

送信元 NAT と宛先 NAT の両方のルールを設定して、アドレス変換を無効にできます。サブネットの特定のホスト、または特定のインターフェイスから送信されるトラフィックで NAT が実行されないようにする例外を設定できます。以下の手順は、ホストの送信元 NAT を無効にする方法を示しています。

STEP 1 | NAT ポリシーを作成します。

1. **Policies (ポリシー)** > **NAT** を選択し、ポリシーの分かりやすい **Name (名前)** を **Add (追加)** します。
2. **Original Packet (元のパケット)** タブの **Source Zone (送信元ゾーン)**セクションで内部ネットワーク用に作成したゾーンを選択し (**Add (追加)** をクリックしてからゾーンを選択します)、**Destination Zone (宛先ゾーン)**リストでは外部ネットワーク用に作成したゾーンを選択します。
3. [送信元アドレス] で、[追加] をクリックして、ホストのアドレスを入力します。**OK** をクリックします。
4. **Translated Packet (変換済みパケット)** タブで、画面の Source Address Translation (送信元アドレスの変換) セクションの **Translation Type (変換タイプ)** リストから **None (なし)** を選択します。
5. **OK** をクリックします。

STEP 2 | 変更をコミットします。

Commit（コミット）をクリックします。

NAT ルールは上から下の順序で処理されるため、*NAT* 適用除外ポリシーは、他の *NAT* ポリシーの前に配置して、適用除外する送信元のアドレス変換が発生する前に処理されるようにします。

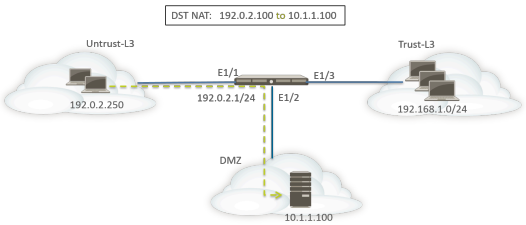
NAT 設定の例

宛先 NAT の例 – 1 対 1 のマッピング

NAT およびセキュリティ ルールの設定時の最も一般的なミスは、ゾーンおよびアドレス オブジェクトへの参照です。宛先 NAT ルールに使用されるアドレスは、パケットの元の IP アドレス（変換前アドレス）を常に参照します。NAT ルールの宛先ゾーンは、元のパケットの宛先 IP アドレス（NAT 前の宛先 IP アドレス）のルート検索後に決まります。

セキュリティ ポリシーのアドレスも、元のパケットの IP アドレス（NAT 前のアドレス）を参照します。ただし、宛先ゾーンは、エンド ホストが物理的に接続されているゾーンです。つまり、セキュリティ ルールの宛先ゾーンは、NAT 後の宛先 IP アドレスのルート検索後に決まります。

以下の 1 対 1 の宛先 NAT マッピングの例では、Untrust-L3 という名前のゾーンのユーザーが、DMZ という名前のゾーンのサーバー 10.1.1.100 に IP アドレス 192.0.2.100 を使用してアクセスしています。



NAT ルールを設定する前に、このシナリオのイベント シーケンスを考えます。

- ホスト 192.0.2.250 は、アドレス 192.0.2.100 （宛先サーバーのパブリック アドレス）の ARP 要求を送信します。
- ファイアウォールは、Ethernet1/1 インターフェイスで宛先 192.0.2.100 の ARP 要求パケットを受信し、要求を処理します。宛先 NAT ルールの設定により、ファイアウォールは、その MAC アドレスで ARP 要求に応答します。
- NAT ルールが評価されて照合が行われます。宛先 IP アドレスを変換する場合、宛先 IP 192.0.2.100 を 10.1.1.100 に変換するには、ゾーン untrust-l3 からゾーン untrust-l3 への宛先 NAT ルールが作成されている必要があります。

- 変換後アドレスが決まったら、ファイアウォールは宛先 10.1.1.100 のルート検索を実行して、出力インターフェイスを決定します。この例の場合、出力インターフェイスは、ゾーン DMZ の Ethernet1/2 になります。
- ファイアウォールはセキュリティ ポリシー検索を実行して、ゾーン Untrust-L3 から DMZ へのトラフィックが許可されているかどうかを確認します。

  ポリシーの方向は、入力ゾーン、およびサーバーが物理的に配置されているゾーンに一致します。

  セキュリティ ポリシーは、（宛先アドレスが *192.0.2.100* の）元のパケットの *IP* アドレスを参照します。
- ファイアウォールは、出力インターフェイス Ethernet1/2 からパケットをサーバーに転送します。パケットがファイアウォールから出ると宛先アドレスが 10.1.1.100 に変わります。

この例では、アドレス オブジェクトはwebserver-private（10.1.1.100）およびWebserver-public（192.0.2.100）用に設定されています。設定された NAT ルールは以下のようになります。

NAME	TAGS	Original Packet						Translated Packet	
		SOURCE ZONE	DESTINATION ZONE	DESTINATION INTERFACE	SOURCE ADDRESS	DESTINATION ADDRESS	SERVICE	SOURCE TRANSLATION	DESTINATION TRANSLATION
Dst NAT-webserver	none	Untrust-L3	Untrust-L3	any	any	Webserver-public	any	none	destination-translation address: webserver-private

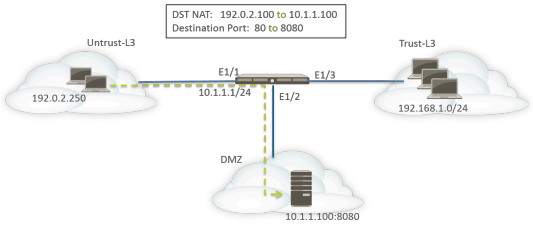
NAT ルールの方向は、ルート検索の結果に基づいています。

untrust-l3 ゾーンからサーバーにアクセスするために設定されたセキュリティ ポリシーは以下のようになります。

NAME	Source		Destination		APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
	ZONE	ADDRESS	ZONE	ADDRESS					
Webserver access	Untrust-L3	any	DMZ	Webserver-pu...	web-browsing	any	Allow	none	

ポート変換を使用した宛先 NAT の例

この例では、ポート 8080 の HTTP トラフィックをリッスンするように Web サーバーが設定されています。クライアントは、IP アドレス 192.0.2.100 および TCP ポート 80 を使用して、Web サーバーにアクセスします。IP アドレスを 10.1.1.100、ポートを TCP ポート 8080 に変換するように宛先 NAT ルールが設定されています。アドレス オブジェクトはwebserver-private（10.1.1.100）およびServers-public（192.0.2.100）用に設定されています。



以下の NAT およびセキュリティ ルールがファイアウォールで設定されている必要があります。

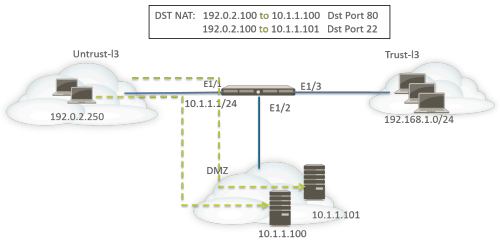
NAME	TAGS	Original Packet						Translated Packet	
		SOURCE ZONE	DESTINATION ZONE	DESTINATION INTERFACE	SOURCE ADDRESS	DESTINATION ADDRESS	SERVICE	SOURCE TRANSLATION	DESTINATION TRANSLATION
Dst NAT-webserver	none	Untrust-L3	Untrust-L3	any	any	Servers-public	any	none	destination-translation address: webserver-private port: 8080

NAME	TAGS	TYPE	Source				Destination			APPLICATION	SERVICE	ACTION
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE			
Webserver access	none	universal	Untrust-L3	any	any	any	DMZ	Servers-public	any	web-browsing	any	Allow

show session all CLI コマンドを使用して、変換を確認します。

宛先 NAT の例 – 1 対多のマッピング

この例では、1 つの IP アドレスが 2 つの異なる内部ホストにマッピングされています。ファイアウォールは、アプリケーションを使用して、ファイアウォールがトラフィックを転送する内部ホストを識別します。



すべての HTTP トラフィックは、ホスト 10.1.1.100 に送信され、SSH トラフィックはサーバー 10.1.1.101 に送信されます。以下のアドレス オブジェクトが必要です。

- サーバーの変換前 IP アドレスのアドレス オブジェクト
- SSH サーバーの実際の IP アドレスのアドレス オブジェクト
- Web サーバーの実際の IP アドレスのアドレス オブジェクト

対応するアドレス オブジェクトが作成されます。

- Servers-public：192.0.2.100
- SSH-server：10.1.1.101
- webserver-private：10.1.1.100

NAT ルールは以下のようになります。

NAME	TAGS	Original Packet						Translated Packet	
		SOURCE ZONE	DESTINATION ZONE	DESTINATION INTERFACE	SOURCE ADDRESS	DESTINATION ADDRESS	SERVICE	SOURCE TRANSLATION	DESTINATION TRANSLATION
Dst NAT-webserver	none	Untrust-L3	Untrust-L3	any	any	Servers-public	service-http	none	destination-translation address: webserver-private
Dst NAT-SSH	none	Untrust-L3	Untrust-L3	any	any	Servers-public	custom-ssh	none	destination-translation address: SSH-server

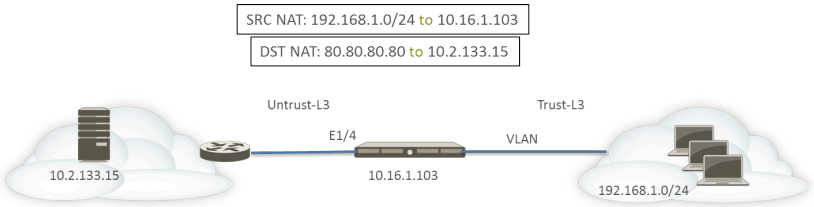
セキュリティ ルールは以下のようになります。

NAME	TAGS	TYPE	Source				Destination			APPLICATION	SERVICE	ACTION
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE			
Webserver access	none	universal	Untrust-L3	any	any	any	DMZ	Servers-public	any	web-browsing	any	Allow
SSH access	none	universal	Untrust-L3	any	any	any	DMZ	Servers-public	any	ssh	any	Allow

送信元 NAT と宛先 NAT の例

この例では、NAT ルールにより、クライアントとサーバー間でパケットの送信元 IP アドレスと宛先 IP アドレスの両方が変換されます。

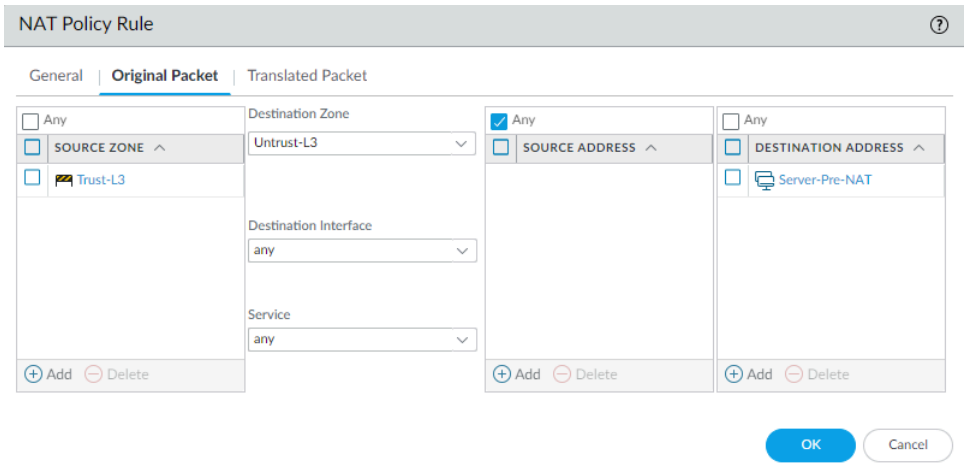
- 送信元 NAT – Trust-L3 ゾーンのクライアントから Untrust-L3 ゾーンのサーバーへのパケットの送信元アドレスは、ネットワーク 192.168.1.0/24 のプライベート アドレスからファイアウォールの出力インターフェイスの IP アドレス（10.16.1.103）に変換されます。ダイナミック IP およびポート変換により、ポート番号も変換されます。
- 宛先 NAT – クライアントからサーバーへのパケットの宛先アドレスは、サーバーのパブリック アドレス（80.80.80.80）からサーバーのプライベート アドレス（10.2.133.15）に変換されます。

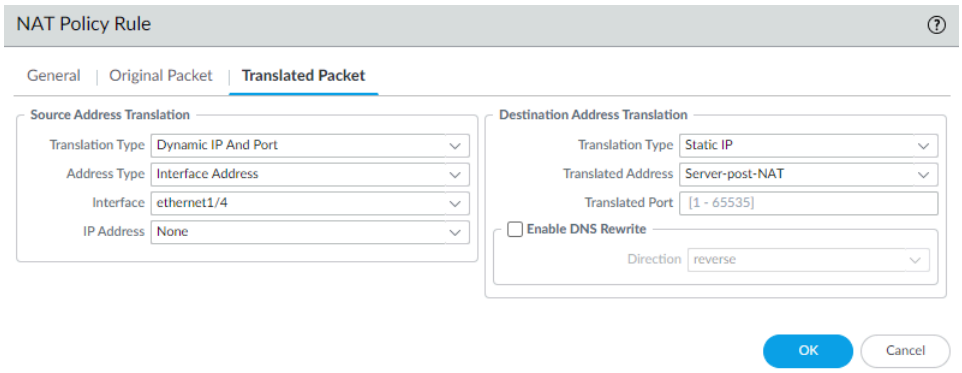


宛先 NAT 用に以下のアドレス オブジェクトが作成されます。

- Server-Pre-NAT：80.80.80.80
- Server-post-NAT：10.2.133.15

以下のスクリーン ショットは、この例の送信元 NAT ポリシーと宛先 NAT ポリシーの設定方法を示しています。





変換を確認するには、CLI コマンド **show session all filter destination 80.80.80.80** を使用します。クライアントのアドレス 192.168.1.11 は 10.16.1.103、クライアントのポート番号は特定のポート番号に変換されます。宛先アドレス 80.80.80.80 は 10.2.133.15 に変換されます。

バーチャル ワイヤーの送信元 NAT の例

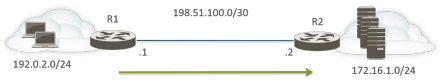
パロアルトネットワーク®ファイアウォールの仮想ワイヤ展開には、エンドデバイスに透過的にセキュリティを提供するという利点が含まれています。バーチャル ワイヤーで設定されたインターフェイスに NAT を設定することができます。すべての NAT タイプ（送信元 NAT （ダイナミック IP、ダイナミック IP およびポート、スタティック）と宛先 NAT）を使用できます。

バーチャル ワイヤーのインターフェイスには IP アドレスが割り当てられていないため、IP アドレスをインターフェイスの IP アドレスに変換することはできません。IP アドレス プールを設定する必要があります。

バーチャル ワイヤー インターフェイスで NAT を実行する場合、隣接するデバイスが通信するサブネットとは異なるサブネットに送信元アドレスを変換することをお勧めします。ファイアウォールは、NAT アドレスの ARP をプロキシしません。バーチャル ワイヤー モードでパケットを変換するには、アップストリームおよびダウンストリーム ルーターで適切なルーティングが設定されている必要があります。隣接するデバイスは、バーチャル ワイヤーのもう一方の終端のデバイスのインターフェイスに存在する IP アドレスの ARP リクエストのみを解決できます。プロキシ ARP の詳細な説明については、NAT アドレス プールのプロキシ ARP を参照してください。

以下の送信元 NAT の例では、vw-trust という名前のバーチャル ワイヤー ゾーンから vw-untrust という名前のゾーンにセキュリティ ポリシー（記載なし）が設定されています。

以下のトポロジでは、サブネット 192.0.2.0/24 と 172.16.1.0/24 間の接続を提供する 2 つのルーターが設定されています。ルーター間のリンクは、サブネット 198.51.100.0/30 で設定されています。ネットワーク間の接続を確立するスタティック ルーティングが両方のルーターで設定されています。ファイアウォールがこの環境にデプロイされる前の各ルーターのトポロジおよびルーティング テーブルは以下のようになっています。



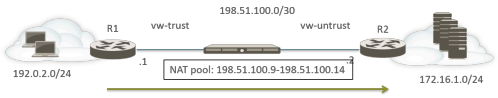
R1のルート:

宛先	ネクストホップ
172.16.1.0/24	198.51.100.2

R2 のルート:

宛先	ネクストホップ
192.0.2.0/24	198.51.100.1

今度は、ファイアウォールが 2 つのレイヤー 3 デバイス間にバーチャル ワイヤー モードでデプロイされています。198.51.100.9〜198.51.100.14 の範囲の NAT IP アドレス プールがファイアウォールに設定されています。ネットワーク 172.16.1.0/24 のサブネット 192.0.2.0/24 にあるクライアントからのすべての通信は、198.51.100.9〜198.51.100.14 の範囲の変換元アドレスで R2 に到達します。サーバーからの応答の宛先はこれらのアドレスになります。



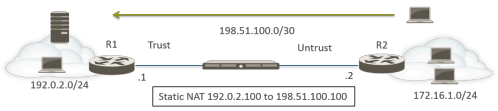
送信元 NAT が機能するには、他のアドレス宛てのパケットがドロップされないように、R2 で適切なルーティングを設定する必要があります。以下のルーティング テーブルは、R2 の変更されたルーティング テーブルを示しています。 ルートは、宛先 198.51.100.9-198.51.100.14（つまり、サブネット 198.51.100.8/29 上のホスト）へのトラフィックがファイアウォールを介して R1 に戻されるようにします。

R2 のルート:

宛先	ネクストホップ
198.51.100.8/29	198.51.100.1

バーチャル ワイヤーのスタティック NAT の例

この例では、Trust という名前のバーチャル ワイヤー ゾーンから Untrust という名前のバーチャル ワイヤー ゾーンにセキュリティ ポリシーが設定されています。ホスト 192.0.2.100 は、アドレス 198.51.100.100 に静的に変換されます。**Bi-directional** [双方向] オプションが有効になっていると、ファイアウォールは Untrust ゾーンから Trust ゾーンへの NAT ポリシーを生成します。Untrust ゾーンのクライアントは、IP アドレス 198.51.100.100 を使用してサーバーにアクセスし、ファイアウォールがこの IP アドレスを 198.0.2.100 に変換します。192.0.2.100 のサーバーが開始した接続は、すべて送信元 IP アドレス 198.51.100.100 に変換されます。



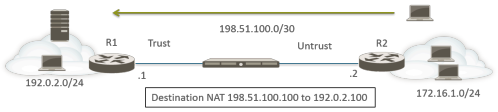
R2 のルート:

宛先	ネクストホップ
198.51.100.100/32	198.51.100.1

	Original Packet						Translated Packet	
NAME	SOURCE ZONE	DESTINATION ZONE	DESTINATION INTERFACE	SOURCE ADDRESS	DESTINATION ADDRESS	SERVICE	SOURCE TRANSLATION	DESTINATION TRANSLATION
Static NAT	Trust	Untrust	any	webserver-private	any	any	static-ip webserver-public bi-directional: yes	none

バーチャル ワイヤーの宛先 NAT の例

Untrust ゾーンのクライアントは、IP アドレス 198.51.100.100 を使用してサーバーにアクセスし、ファイアウォールがこの IP アドレスを 192.0.2.100 に変換します。Untrust ゾーンから Trust ゾーンに NAT およびセキュリティ ポリシーを設定する必要があります。



R2 のルート:

宛先	ネクストホップ
198.51.100.100/32	198.51.100.1

	Original Packet						Translated Packet	
NAME	SOURCE ZONE	DESTINATION ZONE	DESTINATION INTERFACE	SOURCE ADDRESS	DESTINATION ADDRESS	SERVICE	SOURCE TRANSLATION	DESTINATION TRANSLATION
DST NAT	Untrust	Trust	any	any	webserver-public	any	none	destination-translation address: webserver-private

NPTv6

IPv6 間ネットワーク接頭辞変換（NPTv6）は、IPv6 プレフィックスを別の IPv6 プレフィックスにステートレスかつ静的に変換します（ポート番号はそのまま）。NPTv6 には、主に 4 つの利点があります。

- 複数のデータセンターからプロバイダ非依存アドレスが通知されることによって生じる非対称ルーティングの問題を回避できます。
- NPTv6 では、トラフィックを送信したファイアウォールにリターン トラフィックが到達するように、より具体的なルートを通知できます。
- プライベート アドレスとパブリック アドレスが独立しています。一方のアドレスを他方のアドレスに影響を与えることなく変更できます。
- ユニーク ローカル アドレスをグローバルにルーティングできるアドレスに変換できます。

このトピックは、NAT の基本を理解していることを前提としてます。NPTv6 を設定する前に、 NAT の概念を理解していることを確認してください。

NPTv6 の概要

このセクションでは、IPv6 間ネットワーク接頭辞変換（NPTv6）とその設定方法について説明します。NPTv6 は RFC 6296 で定義されています。Palo Alto Networks® は RFC で定義されているすべての機能を実装するわけではありませんが、実装した機能では RFC に準拠しています。

NPTv6 は、IPv6 プレフィックスを別の IPv6 プレフィックスにステートレスに変換します。ステートレスな変換であるため、変換後アドレスにポートやセッションは記録されません。NPTv6 は、ストートフルな NAT66 とは異なります。Palo Alto Networks では、NPTv6 RFC 6296 プレフィックス変換はサポートされていますが、NAT66 はサポートされていません。

IPv4 スペースのアドレスには限りがあるため、NATを使用して、ルーティングできないプライベート IPv4 アドレスをグローバルにルーティングできる 1 つ以上の IPv4 アドレスに変換する必要がありました。IPv6 アドレスは豊富にあるため、IPv6 アドレスを使用する組織は IPv6 アドレスを IPv6 アドレスに変換する必要はありません。ただし、ファイアウォールで IPv6 プレフィックスを変換するためにNPTv6 を使用する理由があります。

> ***NPTv6*** ではセキュリティが提供されないことを理解することが重要です。一般的なステートレスなネットワーク アドレス変換では、セキュリティは提供されません。アドレス変換機能を提供します。***NPTv6*** では、ポート番号の隠蔽や変換は行われません。トラフィックを意図したとおりに制御するには、各方向でファイアウォール セキュリティ ポリシーを正しくセットアップする必要があります。

NPTv6 は、IPv6 アドレスのプレフィックス部分を変換しますが、ホスト部分やアプリケーション ポート番号は変換しません。ホスト部分はコピーされるだけなので、ファイアウォールの各側で変わりません。また、ホスト部分は、パケット ヘッダー内で参照できる状態のままです。

NPTv6 は、次のファイアウォール モデルでサポートされています (NPTv6 ハードウェア検索が、パケットは CPU を経由します)。

- PA-7000 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-3200 シリーズ ファイアウォール
- PA-800 ファイアウォール
- PA-220 ファイアウォール

VM-Series ファイアウォールは NPTv6 をサポートしますが、ハードウェアでセッションルックアップを実行する機能はありません。

- ユニーク ローカル アドレス
- NPTv6 を使用する理由

ユニーク ローカル アドレス

RFC 4193、Unique Local IPv6 Unicast Addresses（英語）では、IPv6 ユニキャスト アドレスであるユニーク ローカル アドレス（ULA）が定義されています。このアドレスは、RFC

1918、Address Allocation for Private Internets（英語）で特定されている、グローバルにルーティングできないプライベート IPv4 アドレスの IPv6 版と考えることができます。

ULA は、グローバルに一意ですが、グローバルにルーティングできるアドレスとして想定されていません。これは、ローカル通信を目的としており、1 つのサイトや少数のサイト間などの限定的なエリアでルーティングできるようになっています。Palo Alto Networks® は ULA の割り当てを推奨しませんが、NPTv6 で構成されたファイアウォールは、ULA を含む送信されたプレフィックスを変換します。

NPTv6 を使用する理由

グローバルにルーティングできるパブリック IPv6 アドレスは不足していませんが、IPv6 アドレスを変換することが必要になる理由があります。NPTv6：

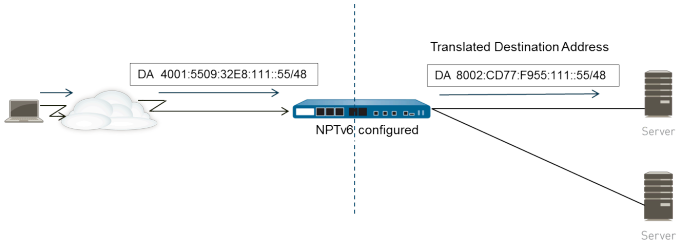
- 非対称ルーティングの防止 – 複数のデータ センターによって非依存アドレス スペース（/48 など）がグローバル インターネットに通知される場合、非対称ルーティングが発生することがあります。NPTv6 を使用すると、各地域のファイアウォールからより具体的なルートを通知できます。これにより、トランスレータが送信元 IP アドレスを変換したファイアウォールにリターン トラフィックが到達します。
- アドレスの非依存性の確保 – （たとえば、ISP によって、または組織統合の結果）グローバル プレフィックスが変更されても、ローカル ネットワーク内で使用する IPv6 プレフィックスを変更する必要はありません。反対に、インターネットからプライベート ネットワークのサービスにアクセスするときに使用されるアドレスを妨げることなく、自由に内部アドレスを変更できます。いずれの場合も、ネットワーク アドレスの再割り当てを行うのではなく、NAT ルールを更新します。
- ルーティングのための **ULA** の変換 – プライベート ネットワーク内でユニーク ローカル アドレス を割り当て、ファイアウォールでそのアドレスをグローバルにルーティングできるアドレスに変換できます。そのため、プライベート アドレスの利便性と、ルーティング可能な変換後アドレスの機能を得ることができます。
- **IPv6** プレフィックスの漏洩の削減 – IPv6 プレフィックスでは、ネットワーク プレフィックスを変換しない場合よりも漏洩の危険性は低くなりますが、NPTv6 はセキュリティ対策ではありません。各 IPv6 アドレスのインターフェイス識別子部分は変換されません。ファイアウォールの各側で同じままで、パケット ヘッダーを表示できれば誰でも参照できます。また、プレフィックスも安全ではなく、第三者に特定される可能性があります。

NPTv6 の仕組み

NPTv6 のポリシーを構成すると、Palo Alto Networks® ファイアウォールは、両方向で静的な 1 対 1 の IPv6 変換を実行します。変換は、RFC 6296 に記載されているアルゴリズムに基づいて行われます。

あるユース ケースでは、NPTv6 を実行するファイアウォールが内部ネットワークと、グローバルにルーティングできるプレフィックスを使用する外部ネットワーク（インターネットなど）の間に配置されています。データグラムがアウトバウンド方向に送信される場合、内部送信元プレフィックスが外部プレフィックスに置き換えられます。これは、送信元変換と呼ばれます。

別のユース ケースでは、データグラムがインバウンド方向に送信される場合、宛先プレフィックスが内部プレフィックスに置き換えられます。これは、宛先変換と呼ばれます。以下の図は、NPTv6 の宛先変換とその特徴を示しています。IPv6 アドレスのプレフィックス部分のみが変換されています。アドレスのホスト部分は変換されず、ファイアウォールの各側で変わりません。以下の図では、ファイアウォールのどちらの側のホスト識別子も 111::55 になっています。



NPTv6 ではセキュリティが提供されないことを理解することが重要です。NPTv6 NAT ポリシーを計画する場合、各方向のセキュリティ ポリシーも設定してください。

NAT または NPTv6 ポリシー ルールでは、Source Address （送信元アドレス）と Translated Address （変換後アドレス）の両方を Any （いずれか）に設定することはできません。

IPv6 プレフィックスの変換が必要な環境では次の3 つのファイアウォール機能が連携します。NPTv6 NAT ポリシー、セキュリティポリシー、および NDP プロキシ。

以下に、ファイアウォールで変換されないアドレスおよびサブネットを示します。

- ファイアウォールのネイバー検出（ND）キャッシュにあるアドレス。
- サブネット 0xFFFF （RFC 6296、Appendix B （英語）に準拠）。
- IP マルチキャスト アドレス。
- プレフィックス長が /31 以下の IPv6 アドレス。
- リンク ローカル アドレス。ファイアウォールがバーチャル ワイヤー モードで動作している場合、変換する IP アドレスがないため、リンク ローカル アドレスはファイアウォールで変換されません。
- TCP Authentication Option （RFC 5925）を使用してピアを認証する TCP セッションのアドレス。

NPTv6 は低速パスで実行されるため、NPTv6 を使用する場合は高速パス トラフィックのパフォーマンスに影響します。

NPTv6 は、ファイアウォールがトンネルを開始および終了する場合にのみ IPSec IPv6 と連携します。送信元/宛先 IPv6 アドレスが変更されるため、トランジット IPSec トラフィックが失敗します。パケットをカプセル化する NAT トラバーサル方式では、IPSec IPv6 と NPTv6 を連携できます。

- チェックサム ニュートラルなマッピング
- 双方向変換
- 特定のサービスへの NPTv6 の適用

チェックサム ニュートラルなマッピング

ファイアウォールが実行する NPTv6 マッピングの変換はチェックサム ニュートラルです。つまり、この IPv6 IP ヘッダーでは、標準のインターネット チェックサム アルゴリズム（RFC 1071）を使用して計算されたチェックサムと同じ擬似ヘッダー チェックサムが生成されます。チェックサム ニュートラルなマッピングの詳細は、RFC 6296、Section 2.6（英語）を参照してください。

NPTv6 を使用して宛先 NAT を実行する場合、**`test nptv6`** CLI コマンドの構文で、ファイアウォール インターフェイスの内部 IPv6 アドレスと外部プレフィックス/プレフィックス長を指定できます。この CLI は、その宛先に到達するために NPTv6 設定で使用されるチェックサム ニュートラルなパブリック IPv6 アドレスで応答します。

双方向変換

NPTv6 ポリシーの作成を行う場合、**Translated Packet** [変換済みパケット]タブの **Bi-directional** [双方向]オプションが便利です。このチェック ボックスを使用すると、対応する NAT または NPTv6 変換を、設定した変換の反対方向にも作成できます。デフォルトでは、**Bi-directional** [双方向]変換は無効になっています。

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確認しておく必要があります。そのようなポリシーが設定されていないと、***Bi-directional*** *[双方向]*機能によってパケットが双方向に自動的に変換されるようになります。これは意図する動作とは異なります。

特定のサービスへの NPTv6 の適用

Palo Alto Networks の NPTv6 の実装では、パケットをフィルタリングして、変換が適用されるパケットを制限できます。NPTv6 ではポート変換が実行されないことに注意してください。NPTv6 では IPv6 プレフィックスしか変換されないため、ダイナミック IP およびポート（DIPP）変換の概念はありません。ただし、特定のサービス ポートのパケットのみが NPTv6 変換の対象となるように指定することはできます。このためには、 NPTv6 ポリシーの作成を行い、元のパケットの**Service** [サービス]を指定します。

NDP プロキシ

IPv6 のネイバー検出プロトコル（NDP）では、IPv4 のアドレス解決プロトコル（ARP）と同じような機能が実行されます。RFC 4861 では、Neighbor Discovery for IP version 6 (IPv6) が定義されています。ホスト、ルーター、およびファイアウォールは、NDP を使用して接続リンクのネイバーのリンク層アドレスを判断したり、到達可能なネイバーを記録したり、変更されたネイバーのリンク層アドレスを更新したりします。ピアは、各自の MAC アドレスと IPv6 アドレスを通知したり、ピアのアドレスを要請したりします。

ノードに隣接するデバイスがあり、そのデバイスでそのノードの代わりにパケットを転送できる場合、NDP でプロキシの概念もサポートされます。デバイス（ファイアウォール）は、NDP プロキシの役割を果たします。

Palo Alto Networks ®ファイアウォールは、インタフェース上でNDPとNDPプロキシをサポートします。アドレスの NDP プロキシとして動作するようにファイアウォールを設定すると、ファイアウォールはネイバー検出（ND）通知を送信し、ピアからの ND 要請（ファイアウォールの背後にあるデバイスに割り当てられた IPv6 プレフィックスの MAC アドレスの要求）に応答します。また、ファイアウォールがプロキシ要求に応答しないアドレス（除外されたアドレス）を設定することもできます。

実際、NDP はデフォルトで有効になっており、NPTv6 を設定する場合は以下の理由で NDP プロキシを設定する必要があります。

- NPTv6 はステートレスであるため、指定した NDP プロキシ アドレスに送信される ND パケットには応答するが、除外された NDP プロキシ アドレスには応答しないようにファイアウォールに指示する方法が必要です。

  NDP プロキシでは、ファイアウォールがファイアウォールの背後にあるアドレスに到達することが示されますが、ネイバーはファイアウォールの背後にないため、*NDP* プロキシ設定でネイバーのアドレスを除外することをお勧めします。

- NDP により、ファイアウォールの ND キャッシュのネイバーの MAC アドレスと IPv6 アドレスを節約できます（「NPTv6 および NDP プロキシの例」の図を参照してください）。 ファイアウォールは、競合を避けるために ND キャッシュにあるアドレスの NPTv6 変換は実行しません。キャッシュのアドレスのホスト部分が偶然ネイバーのアドレスのホスト部分と重複していて、（ファイアウォールの出力インターフェイスがネイバーと同じサブネットに属しているために）キャッシュのプレフィックスがネイバーと同じプレフィックスに変換される場合、変換後アドレスはネイバーの正当な IPv6 アドレスとまったく同じになり、競合が発生します（ND キャッシュのアドレスで NPTv6 変換を実行しようとすると、informational の Syslog メッセージで次のイベントが記録されます：**NPTv6 Translation Failed**）

NDP プロキシが有効になっているインターフェイスで、IPv6 アドレスの MAC アドレスを要求する ND 要請を受信する場合、以下のようなシーケンスが発生します。

- ファイアウォールは、ND キャッシュを検索して、要請の IPv6 アドレスがキャッシュにないことを確認します。アドレスがキャッシュにある場合、ファイアウォールは ND 要請を無視します。
- 送信元 IPv6 アドレスが 0 の場合、重複アドレス検出パケットであるため、ファイアウォールは ND 要請を無視します。

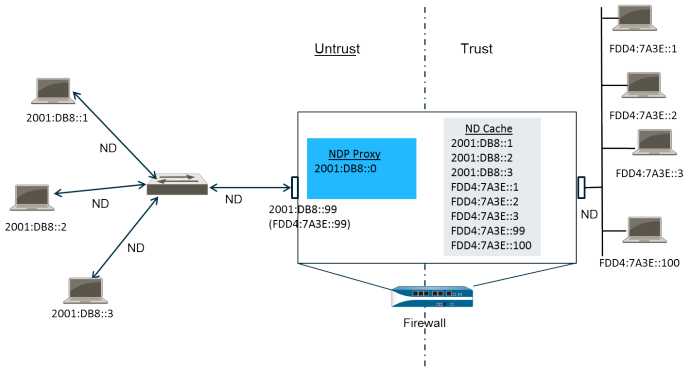
- ファイアウォールは、NDP プロキシ アドレスの最長プレフィックス一致検索を実行し、要請のアドレスに最も一致するアドレスを検索します。一致したアドレスの Negate フィールド（NDP Proxy （NDP プロキシ）リスト）がオンになっている場合、ファイアウォールは ND 要請をドロップします。
- 最長プレフィックス一致検索に一致し、一致したアドレスが除外されていない場合にのみ、NDP プロキシは ND 要請に応答します。ファイアウォールは ND パケットで応答し、該当の宛先へのネクスト ホップの MAC アドレスとしてその MAC アドレスを提供します。

NDP を正常にサポートするために、ファイアウォールは以下の NDP プロキシを実行しません。

- 重複アドレス検出（DAD）。
- ND キャッシュのアドレス（キャッシュのアドレスは、ファイアウォールではなく検出されたネイバーに属しているため）。

NPTv6 および NDP プロキシの例

以下の図は、NPTv6 と NDP プロキシの連携方法を示しています。



- NPTv6 の ND キャッシュの例
- NPTv6 の NDP プロキシの例
- NPTv6 の NPTv6 変換の例
- ND キャッシュのネイバーは変換されない

NPTv6 の ND キャッシュの例

上の例では、複数のピアがスイッチを経由してファイアウォールに接続されており、ピアとスイッチ間、スイッチとファイアウォール間、ファイアウォールと trust 側のデバイス間で ND が発生します。

ファイアウォールがピアを学習すると、ピアのアドレスがファイアウォールの ND キャッシュに保存されます。信頼されているピア FDDA:7A3E::1、FDDA:7A3E::2、および FDDA:7A3E::3 は、trust 側のファイアウォールに接続されています。FDDA:7A3E::99 は、ファイアウォール自体の変換前アドレスで、そのパブリックフェイシング アドレスは 2001:DB8::99 です。untrust 側のピアのアドレスは検出されており、ND キャッシュに表示されています：2001:DB8::1、2001:DB8::2、および2001:DB8::3。

NPTv6 の NDP プロキシの例

このシナリオでは、ファイアウォールの背後にあるデバイスのプレフィックスの NDP プロキシとしてファイアウォールを動作させます。ファイアウォールが指定した一連のアドレス/範囲/プレフィックスの NDP プロキシであり ND 要請または通知でこの範囲のアドレスを検出した場合、その特定のアドレスのデバイスが最初に応答することなく、そのアドレスが NDP プロキシ設定で除外されておらず ND キャッシュにもなければ、ファイアウォールが応答します。ファイアウォールはプレフィックス変換（下記参照）を行い、trust 側にパケットを送信します。そのアドレスは trust 側のデバイスに割り当てられている場合もありますが、割り当てられていない場合もあります。

この例では、ND プロキシ テーブルにネットワーク アドレス 2001:DB8::0 が含まれています。2001:DB8::100 の ND がインターフェイスで検出されると L2 スイッチの他のデバイスからパケットが要求されなくなるため、ファイアウォールはプロキシ範囲に基づいてパケットを要求

します。FDD4:7A3E::100 への変換が完了したら、ファイアウォールはパケットを trust 側に送信します。

NPTv6 の NPTv6 変換の例

この例では、**Original Packet** [元のパケット]の **Source Address** [送信元アドレス]が FDD4:7A3E::0、**Destination** [宛先]が **Any** [いずれか]に設定されています。**Translated Packet** [変換済みパケット]の **Translated Address** [変換後アドレス]は 2001:DB8::0 に設定されています。

そのため、送信元が FDD4:7A3E::0 の送信パケットは 2001:DB8::0 に変換されます。ネットワークの宛先プレフィックスが 2001:DB8::0 の受信パケットは、FDD4:7A3E::0 に変換されます。

ND キャッシュのネイバーは変換されない

この例では、ファイアウォールの背後にホスト識別子が :1、:2、:3 のホストがあります。これらのホストのプレフィックスがファイアウォールの背後にあるプレフィックスに変換され、アドレスのホスト識別子部分は変わらないため、それらのデバイスのホスト識別子も :1、:2、:3 になる場合、変換後アドレスが既存のデバイスに属し、アドレスの競合が発生します。重複するホスト識別子の競合を回避するために、NPTv6 では ND キャッシュにあるアドレスは変換されません。

NPTv6 ポリシーの作成

1 つの IPv6 プレフィックスを別の IPv6 プレフィックスに変換するように NAT NPTv6ポリシーを設定する場合は、このタスクを実行します。このタスクの前提条件は以下のようになります。

- IPv6 を有効にします。[デバイス > セットアップ > セッション] を選択します。**Edit** [編集]をクリックし、**IPv6 Firewalling** [IPv6 ファイアウォール設定]を選択します。
- 有効な IPv6 アドレスがあり、IPv6 が有効になっているレイヤー 3 Ethernet 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)** > **Ethernet (イーサネット)** の順に選択してインターフェイスを選択し、**IPv6** タブで、**Enable IPv6 on the interface (インターフェイスでの IPv6 の有効化)** を選択します。
- NPTv6 ではセキュリティが提供されないため、ネットワーク セキュリティ ポリシーを作成します。
- 送信元変換、宛先変換、またはその両方を行うかどうかを決定します。
- NPTv6 ポリシーを適用するゾーンを指定します。
- 元の IPv6 プレフィックスと変換後 IPv6 プレフィックスを指定します。

STEP 1 | 新しい NPTv6 ポリシーを作成します。

1. **Policies (ポリシー)** > **NAT** の順に選択して **Add (追加)** をクリックします。
2. **General** [全般]タブの **Name** [名前]に NPTv6 ポリシー ルールの分かりやすい名前を入力します。
3. （任意）**Description** [内容]と **Tag** [タグ]を入力します。
4. **NAT Type** [NAT タイプ]として、**NPTv6** を選択します。

STEP 2 | 受信パケットの一致基準を指定します。すべての基準を満たすパケットに NPTv6 変換が適用されます。

ゾーンは、両方のタイプの変換に必要です。

1. **Original Packet (元のパケット)** タブで、**Source Zone (送信元ゾーン)** を **Any (すべて)** のままにするか、**Add (追加)** をクリックして、ポリシーを適用する送信元ゾーンを入力します。
2. ポリシーを適用する **Destination Zone** [宛先ゾーン]を入力します。
3. （任意）**Destination Interface** [宛先インターフェイス]を選択します。
4. （任意）**Service (サービス)** を選択して、変換するパケット タイプを制限します。
5. 送信元変換を行う場合、**Source Address**（送信元アドレス）を入力するか、**Any**（いずれか） を選択します。このアドレスは、アドレス オブジェクトになる可能性があります。**Source Address (送信元アドレス)** と **Destination Address (宛先アドレス)** には、以下の制約が適用されます。
   - **Original Packet (元のパケット)** と **Translated Packet (変換済みパケット)** の **Source Address (送信元アドレス)** と **Destination Address (宛先アドレス)** の プレフィックスは、xxxx:xxxx::/yy の形式にする必要があります。ただし、プレフィックスの先頭のゼロはドロップされます。

- IPv6 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 ～ /64 です。
- **Source Address** [送信元アドレス]と **Destination Address** [宛先アドレス]の両方を **Any** [いずれか]に設定することはできません。

6. 送信元変換を行う場合、必要に応じて **Destination Address** [宛先アドレス]を入力できます。宛先変換を行う場合、**Destination Address** [宛先アドレス]は必須です。（アドレス オブジェクトが許可される）宛先アドレスは、ただの IPv6 アドレスや範囲ではなく、ネットマスクでなければなりません。プレフィックス長は /32～/64 のいずれかの値である必要があります。例：2001:db8::/32。

STEP 3 | 変換済みパケットを指定します。

1. **Translated Packet** [変換済みパケット]タブで、送信元変換を行う場合は Source Address Translation [送信元アドレスの変換]セクションの **Translation Type** [変換タイプ]に **Static IP** [スタティック IP]を選択します。送信元変換を行わない場合は、**None** [なし]を選択します。
2. **Static IP** [スタティック IP]を選択した場合、**Translated Address** [変換後アドレス]フィールドが表示されます。変換後 IPv6 プレフィックスまたはアドレス オブジェクトを入力します。前の手順に記載されている制約を参照してください。

   ファイアウォールの *untrust* インターフェイス アドレスのプレフィックスになる ***Translated Address*** *[変換後アドレス]*を設定することをお勧めします。たとえば、*untrust* インターフェイスのアドレスが *2001:1a:1b:1::99/64* の場合、***Translated Address*** **(**変換後アドレス**)** を *2001:1a:1b:1::0/64* にします。

3. （任意）対応する NPTv6 変換を設定する変換の反対方向にも作成する場合、**Bi-directional (**双方向**)** を選択します。

   Bi-directional *[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 ポリシールールが設定されていることを確認しておく必要があります。そのようなポリシールールが設定されていないと、***Bi-directional*** *[双方向]*変換によってパケットが双方向に自動的に変換されるようになります。これは意図する動作とは異なります。

4. 宛先変換を行う場合、**Destination Address Translation** [宛先アドレス変換]を選択します。**Translated Address (**変換後アドレス**)**フィールドでアドレス オブジェクトを選択するか、内部宛先アドレスを入力します。
5. **OK** をクリックします。

STEP 4 | NDP プロキシを設定します。

アドレスの NDP プロキシとして動作するようにファイアウォールを設定すると、ファイアウォールはネイバー検出（ND）通知を送信し、ピアからの ND 要請（ファイアウォールの背

後にあるデバイスに割り当てられた IPv6 プレフィックスの MAC アドレスの要求）に応答します。

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、さらにインターフェイスを選択します。
2. **Advanced (詳細)** > **NDP Proxy (NDP プロキシ)** タブで、**Enable NDP Proxy (NDP プロキシの有効化)** を選択し、**Add (追加)** をクリックします。
3. NDP プロキシを有効にする **IP Address(es)** [IP アドレス]を入力します。これにはアドレス、アドレス範囲、またはプレフィックスとプレフィックス長を入力します。IP アドレスの順序は関係ありません。これらのアドレスは NPTv6 ポリシーで設定した変換後アドレスと同じになっていることが理想的です。

   アドレスがサブネットの場合、*NDP* プロキシはサブネットのすべてのアドレスに応答するため、次の手順で説明されているようにそのサブネットで ***Negate** [拒否]*が選択されているネイバーをリストする必要があります。
4. （任意）NDP プロキシを有効にしない 1 つ以上のアドレスを入力し、**Negate** [拒否]を選択します。たとえば、前の手順で設定した IP アドレス範囲またはプレフィックス範囲のアドレスのより小さなサブセットを除外できます。ファイアウォールのネイバーのアドレスを除外することをお勧めします。

STEP 5 | 設定を Commit（コミット）します。

OK、**Commit (コミット)** の順にクリックします。

NAT64

NAT64 は、IPv4 ネットワークとの通信を維持しつつも、IPv6 に移行できる方法を提供します。IPv6 専用のネットワークから IPv4 ネットワークと通信を行う必要がある場合、NAT64 を使用して送信元および宛先アドレスを IPv6 から IPv4 に、あるいはその逆に変換します。NAT64 では、IPv6 クライアントから IPv4 サーバーへのアクセスと、IPv4 クライアントから IPv6 サーバーへのアクセスが許可されます。NAT64 を設定する前に、NAT を理解しておく必要があります。

NAT64の概要

パロアルトネットワーク®のファイアウォール上で2種類のNAT64変換を設定できます。各グループは、2 つの IP アドレス ファミリ間で双方向変換を行います。

- ファイアウォールは、複数の IPv6 アドレスを単一の IPv4 アドレスにマッピングすることで IPv4 アドレスを保持する、IPv6 から開始される通信用のステートフル NAT64 をサポートしています。（これは、単一の IPv6 アドレスを単一の IPv4 アドレスにマッピングすることで IPv4 アドレスを保持するステートレス NAT64 はサポートしていません）IPv6 から開始される通信に NAT64 を設定.
- ファイアウォールは、IPv4 アドレスおよびポート番号を IPv6 アドレスにマッピングする静的バインディングを伴う、IPv4 から開始される通信をサポートしています。IPv4 から開始される通信に NAT64 を設定。またこれは、IPv4 アドレスおよびポート番号を複数のポート番号を持つ IPv6 アドレスに変換することでより多くの IPv4 アドレスを保持するポート リライトもサポートしています。ポート変換を伴う IPv4 から開始される通信用に NAT64 を設定。

単一の IPv4 アドレスを NAT44 および NAT64 で使用できます。NAT64 のみの場合は IPv4 アドレスのプールを保持しません。

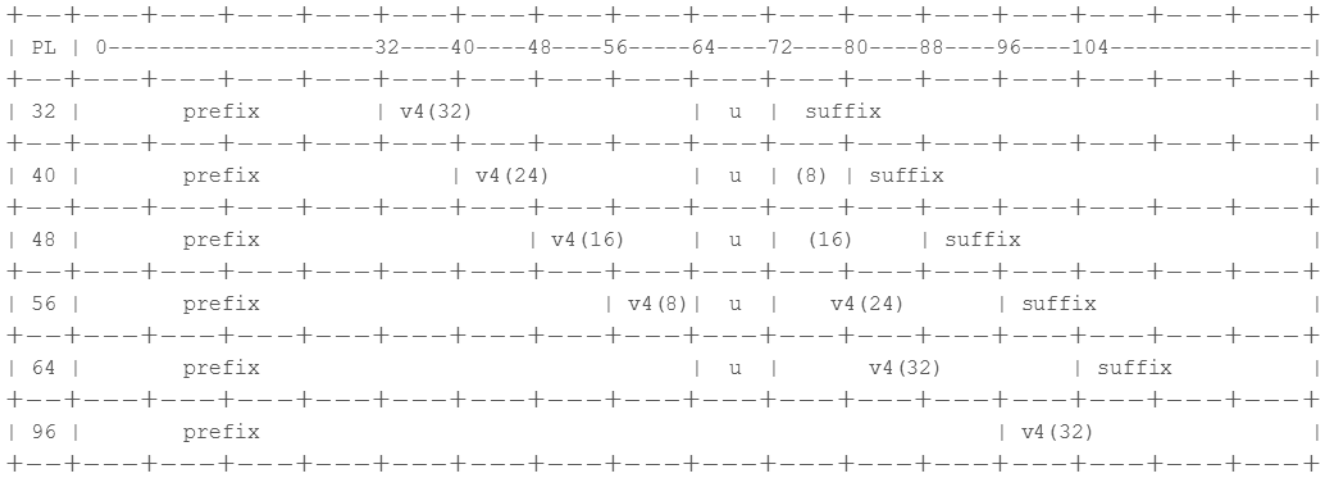
NAT64 は、レイヤー 3 インターフェイス、サブインターフェイス、トンネル インターフェイス上で稼働します。Palo Alto Networks ファイアウォールで IPv6 から開始される通信を行うために NAT64 を使用するには、サードパーティ DNS64 サーバー あるいは製品を持っており、DNS クエリ機能を NAT 機能から切り離す必要があります。DNS64 サーバーは、公開 DNS サーバーから受信した IPv4 アドレスを IPv6 ホストの IPv6 アドレスにエンコードすることで、IPv6 ホストおよび IPv4 DNS サーバーを変換します。

Palo Alto Networks は、次の NAT64 機能をサポートしています。

- ヘアピン（NAT U ターン）。さらに、送信元プレフィックス 64::/n を持つインバウンド IPv6 パケットをすべてドロップすることで、NAT64 がヘアピン ループ攻撃を防ぎます。
- RFC 6146 に従う TCP/UDP/ICMP パケット変換およびファイアウォールにより、アプリケーション レベル ゲートウェイ（ALG）を使用しない他のプロトコルを最善の形で変換します。例えば、ファイアウォールは GRE パケットを変換できます。この変換には、NAT44 と同じ制限があります。別の制御およびデータ チャネルを使うプロトコル用の ALG がない場合、リターン トラフィックのフローをファイアウォールが理解しない可能性があります。
- RFC 4884 に従う、元のデータグラム フィールドの ICMP 長属性の IPv4 および IPv6 間の変換。

IPv4 が埋め込まれた IPv6 アドレス

RFC 6052、IPv4/IPv6 トランスレータの IPv6 アドレシングに記載されているとおり、NAT64 は IPv4 が埋め込まれた IPv6 アドレスを使用します。IPv4 が埋め込まれた IPv6 アドレスは、エンコードされた 32 ビットの IPv4 アドレスを含む IPv6 アドレスです。IPv6 プレフィックス長（図では PL）は、次のように、IPv6 アドレス内のどこに IPv4 アドレスがエンコードされているのか判断します。



ファイアウォールは、/32、/40、/48、/56、/64、および /96 サブネット用に、これらのプレフィックスを使用する変換をサポートしています。単一のファイアウォールは複数のプレフィックスをサポートしています。各 NAT64 ルールは一つのプレフィックスを使用します。プレフィックスは、アドレス トランスレータ（DNS64 デバイス）を制御する組織に対して一意なネットワーク固有のプレフィックス（NSP）あるいは既知のプレフィックス（64:FF9B::/96）にすることができます。通常、NSP は組織の IPv6 プレフィックス内のネットワークになります。DNS64 デバイスは通常、u フィールドおよびサフィックスをゼロに設定します。ファイアウォールはこれらのフィールドを無視します。

DNS64 サーバー

DNS を使用する必要があり、IPv6 から開始される通信を使用して NAT64 変換を行いたい場合は、既知のプレフィックスあるいは NSP を使ってセットアップされたサードパーティの DNS64 サーバーあるいはその他の DNS64 製品を使用する必要があります。IPv6 ホストがインターネット上の IPv4 ホストあるいはドメインへのアクセスを試みる際、DNS64 サーバーが管理用の DNS サーバーにクエリを送信し、ホスト名にマッピングされた IPv4 アドレスを求めます。DNS サーバーは、そのホスト名用の IPv4 アドレスを含む DNS64 サーバーにアドレス レコード（A レコード）を返します。

それに応じて DNS64 サーバーは IPv4 アドレスを 16 進数に変換し、プレフィックス長に基づいて使用するようセットアップされた適切な 8 ビット の IPv6 プレフィックス（既知のプレフィックスあるいは NSP）へとエンコードし、その結果、IPv4 が埋め込まれた IPv6 アドレスとなります。DNS64 サーバーは、IPv4 が埋め込まれた IPv6 アドレスを IPv4 ホスト名へとマッピングする IPv6 ホストに AAAA レコードを送信します。

Path MTU Discovery

IPv6 はフラグメント化されたパケットをサポートしていないため、ファイアウォールは 2 つの方式を使用し、パケットをフラグメント化するニーズを減らします。

- DF（don't fragment）ビットがゼロの IPv4 パケットをファイアウォールが変換するということは、送信者が大きすぎるパケットをファイアウォールにフラグメント化してもらいたいが、IPv6 はパケットをフラグメント化しないため、ファイアウォールが IPv6 ネットワーク用にパケットをフラグメント化しないことを意味します（変換後）。その代わりに、ファイアウォールが変換を行う前に IPv4 パケットをフラグメント化する際の最小サイズを設定できます。**NAT64 IPv6 Minimum Network MTU (NAT64 IPv6** 最小ネットワーク **MTU)** の値がその設定であり、RFC 6145、IP/ICMP 変換アルゴリズムに準拠しています。**NAT64 IPv6 Minimum Network MTU (NAT64 IPv6** 最小ネットワーク **MTU)**を最大値に設定（**Device (**デバイス**)** > **Setup (**セットアップ**)** > **Session (**セッション**)**）することで、ファイアウォールが IPv4 パケットを IPv6 に変換する前に、それを IPv6 の最小サイズにフラグメント化できるようになります。（**NAT64 IPv6 Minimum Network MTU (NAT64 IPv6** 最小ネットワーク **MTU)** はインターフェイス MTU を変更しません）
- ファイアウォールがフラグメンテーションを減らすために使うもう一つの方法は、Path MTU Discovery（PMTUD）です。IPv4 から開始される通信では、変換対象の IPv4 パケットが DF ビットを設定しており、その出力インターフェイス用の MTU がパケットよりも小さい場合、ファイアウォールは PMTUD を使用してパケットをドロップし、ICMP 「Destination Unreachable - fragmentation needed」メッセージを送信元に返します。送信元はその宛先用のパス MTU を減らし、パス MTU を減らしていくことでパケットを配信できるようになるまで、パケットを再送信します。

IPv6 から開始される通信

ファイアウォールに向けて IPv6 から開始される通信は、IPv4 トポロジーにおけるソース NAT と同様です。IPv6 ホストが IPv4 サーバーと通信する必要がある場合はIPv6 から開始される通信用に NAT64 を設定します。

NAT64 ポリシールールにて、元のソースを IPv6 ホスト アドレスあるいは Any (すべて) として設定します。宛先 IPv6 アドレスを、DNS64 サーバーが使用する NSP あるいは 既知のプレフィックスのいずれかに設定します。（ルールでは完全な IPv6 宛先アドレスを設定しません）

DNS を使用する必要がある場合は、 DNS64 サーバーを使用して、IPv4 DNSの「A」結果を NAT64 プレフィックスとマージされた「AAAA」結果に変換する必要があります。DNS を使用しない場合は、 RFC 6052 のルールに従って、ファイアウォールに設定された IPv4 宛先アドレスと NAT64 プレフィックスを使用してアドレスを作成する必要があります。

DNS を使用する環境では、下のトポロジ例は DNS64 サーバーとの通信を示しています。DNS64 サーバーが RFC 6052 に準拠する既知のプレフィックス 64:FF9B::/96 あるいはネットワーク固有のプレフィックスを使用するように設定する必要があります（/32、/40、/48、/56、/64、あるいは /96）。

ステートフル NAT64 を実装するためには、ファイアウォールの変換後の側で変換タイプが Dynamic IP および Port でなければなりません。変換後の送信元アドレスをファイアウォール上の出力インターフェイスの IPv4 アドレスとして設定します。宛先変換フィールドは設定しません。ファイアウォールは、まずルールの元の宛先アドレスに含まれるプレフィックス長を見つけて、次にそのプレフィックスに基づき、エンコードされた IPv4 アドレスをインバウンド パケット内の元の宛先 IPv6 アドレスから抽出することで、アドレスを変換します。

ファイアウォールは NAT64 ルールを見る前に、ルートのルックアップを実行してインバウンド パケットの宛先セキュリティ ゾーンを見つける必要があります。ファイアウォールが NAT64 プレフィックスをルーティングできるようにしてはならないため、必ず宛先ゾーンの割り当てを通じて NAT64 プレフィックスに到達できるようにしなければなりません。ファイアウォールは NAT64 プレフィックスをデフォルト ルートに割り当てるか、それ用のルートが存在しないために NAT64 プレフィックスをドロップすることが多くあります。出力インターフェイスおよびゾーンに関連付けられたルーティングテーブルの中に NAT64 プレフィックスがないため、ファイアウォールは宛先ゾーンを探しません。

また、トンネル インターフェイス（終端点のないもの）も設定する必要があります。NAT64 プレフィックスを使用する IPv6 トラフィックが正しい宛先ゾーンに割り当てられるように、トンネルに NAT64 プレフィックスを適用し、適切なゾーンを適用します。トンネルには、トラフィックが NAT64 ルールと一致しない場合、NAT64 接頭辞を使用して IPv6 トラフィックをドロップする利点もあります。ファイアウォール上に設定されたルーティング プロトコルは、ルーティング テーブル内の IPv6 プレフィックスを参照して宛先ゾーンを見つけ、NAT64 ルールを調べます。

次の図は、名前解決プロセスで DNS64 サーバーが果たす役割を示しています。この例では、DNS64 サーバーは既知のプレフィックス（64:FF9B::/96）を使用するように設定されています。

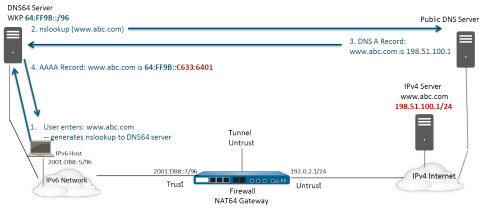
1.IPv6 ホストにいるユーザーが www.abc.com という URL を入力すると、DNS64 サーバーに対してネームサーバーのルックアップ（nslookup）が発生します。

2.DNS64 サーバーが www.abc.com を扱う 公開 DNS サーバーに対して nslookup を送信し、IPv4 アドレスをリクエストします。

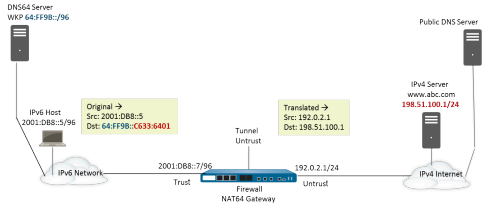
3.DNS サーバーは DNS64 サーバーに A レコードを返して IPv4 アドレスを提供します。

4.DNS64 サーバーは IPv6 ユーザーに AAAA レコードを送信し、ドット付きの 10 進数の IPv4 198.51.100.1 を C633:6401 の 16 進数に変換し、それを自身の IPv6 プレフィックス 64:FF9B::/96 に埋め込みます。（198 = C6 hex、51 = 33 hex、100 = 64 hex、1 = 01 hex）その結果、IPv4 が埋め込まれた IPv6 アドレス 64:FF9B::C633:6401 になります。

/96 プレフィックスでは、IPv4 アドレスが IPv6 アドレス内でエンコードされた最後の4つの 8 ビットになりますのでご注意ください。DNS64 サーバーが /32、/40、/48、/56 あるいは /64 プレフィックスを使用する場合、IPv4 アドレスは RFC 6052 で示されている通りにエンコードされます。



透過的に名前解決を行う際、IPv6 ホストは自身の IPv6 送信元アドレスおよび宛先 IPv6 アドレス 64:FF9B::C633:6401（DNS64 サーバーが判断したもの）を含むパケットをファイアウォールに送信します。ファイアウォールは NAT64 ルールに基づいて NAT64 変換を行います。



IPv6 から開始される通信に NAT64 を設定

この設定作業および各アドレスは、IPv6 から開始される通信の図に対応しています。

STEP 1 | IPv6 を有効化し、ファイアウォール上で稼働させます。

1. **Device (デバイス)** > **Setup (セットアップ)** > **Session (セッション)** を選択して Session Settings (セッション設定) を編集します。
2. **Enable IPv6 Firewalling (IPv6** ファイアウォールの有効化**)** を選択します。
3. **OK** をクリックします。

STEP 2 | IPv6 宛先アドレス用のアドレス オブジェクトを作成します（変換前）。

1. **Objects (オブジェクト)** > **Addresses (アドレス)** を選択して **Add (追加)** をクリックします。
2. オブジェクトの **Name (名前)** を入力します（例：nat64-IPv4 Server）。
3. **Type (タイプ)** については **IP Netmask (IP** ネットマスク**)** を選択し、RFC 6052 に準拠したネットマスクを伴う IPv6 プレフィックスを入力します（/32、/40、/48、/56、/64、あるいは /96）。これは、DNS64 サーバーで設定したネットワーク固有のプレフィックスあるいは既知のプレフィックスのいずれかになります。

   例えば、64:FF9B::/96 と入力します。

   送信元および宛先のネットマスク（プレフィックス長）が同じである必要があります。

   （ファイアウォールはプレフィックス長に基づき、インバウンド パケットに含まれる元の宛先 IPv6 アドレスからエンコードされた IPv4 アドレスを抽出するため、完全な宛先アドレスを入力することはありません。この例では、インバウンド パケットのプレフィックスが C633:6401 の 16 進数（IPv4 宛先アドレス 198.51.100.1）でエンコードされます。
4. **OK** をクリックします。

STEP 3 | （任意）IPv6 送信元アドレス用のアドレス オブジェクトを作成します（変換前）。

1. **Objects (オブジェクト)** > **Addresses (アドレス)** を選択して **Add (追加)** をクリックします。
2. オブジェクトの **Name [名前]** を入力します。
3. **Type (タイプ)** については **IP Netmask (IP** ネットマスク**)** を選択し、IPv6 ホストのアドレスを入力します（この例では 2001:DB8::5/96）。
4. **OK** をクリックします。

STEP 4 | （任意）IPv4 送信元アドレス用のアドレス オブジェクトを作成します（変換後）。

1. **Objects (オブジェクト)** > **Addresses (アドレス)** を選択して **Add (追加)** をクリックします。
2. オブジェクトの **Name [名前]** を入力します。
3. **Type (タイプ)** については **IP Netmask (IP ネットマスク)** を選択し、ファイアウォールの出力インターフェイスの IPv4 アドレスを入力します（この例では 192.0.2.1）。
4. **OK** をクリックします。

STEP 5 | NAT64 ルールを作成します。

1. **Policies (ポリシー)** > **NAT** の順に選択して **Add (追加)** をクリックします。
2. **General** （全般） タブで NAT64 ルールの **Name (名前)** を入力します（例えば、nat64_ipv6_init）。
3. （任意）**Description (内容)** を入力します。
4. **NAT Type** [NAT タイプ]として、**nat64** を選択します。

STEP 6 | 元の送信元および宛先情報を指定します。

1. **Original Packet (元のパケット)** については、**Source Zone (送信元ゾーン)** を **Add (追加)** しmふぁす（trusted ゾーンの場合が多い）。
2. **Destination Zone (宛先ゾーン)**を選択します（この例では Untrust ゾーン）。
3. （任意） a **Destination Interface (宛先インターフェイス)** あるいはデフォルト（**any (すべて)**）を選択します。
4. **Source Address (送信元アドレス)** については、**Any (すべて)** を選択、あるいは IPv6 ホスト用に作成したアドレス オブジェクトを **Add (追加)** します。
5. **Destination Address (宛先アドレス)** については、IPv6 宛先アドレス用に作成したアドレス オブジェクトを **Add (追加)** します（この例では nat64-IPv4 サーバー）。
6. （任意）**Service (サービス)** で **any (すべて)** を選択します。

STEP 7 | 変換済みパケット情報を指定します。

1. **Translated Packet (変換済みパケット)** については、**Source Address Translation (送信元アドレスの変換)** の **Translation Type (変換タイプ)** で **Dynamic IP and Port (動的 IP およびポート)** を選択します。
2. **Address Type (アドレス タイプ)** については、次のいずれかを実行します。
   - **Translated Address (変換後アドレス)** を選択し、IPv4 送信元アドレス用に作成したアドレス オブジェクトを **Add (追加)** します。
   - 変換後の送信元アドレスが IP アドレスであり、ファイアウォールのネットマスクが出力インターフェイスである場合の、**Interface Address (インターフェイス アドレス)** を選択します。これを選択した場合、**Interface (インターフェイス)** を選択し、インターフェイスに複数の IP アドレスがある場合は必要に応じて **IP Address (IP アドレス)** を選択します。
3. **Destination Address Translation (宛先アドレスの変換)** は未選択のままにします。（ファイアウォールは、NAT64 ルールの元の宛先で指定されているプレフィックス長

に基づき、インバウンド パケット内の IPv6 プレフィックスから IPv4 アドレスを抽出します）

4. **OK** をクリックして NAT64 ポリシー ルールを保存します。

STEP 8 | トンネル インターフェイスを設定し、128 以外のネットマスクを持つループバック インターフェイスをエミュレートします。

1. **Network (ネットワーク)** > **Interfaces (インターフェイス)** > **Tunnel (トンネル)** を選択してトンネルを **Add (追加)** します。
2. **Interface Name (インターフェイス名)** については、.2 などの数値の添え字を入力します。
3. **Config (設定)** タブで、NAT64 を設定している **Virtual Router (仮想ルーター)** を選択します。
4. **Security Zone (セキュリティ ゾーン)** については、IPv4 サーバーの宛先に関連する宛先ゾーンを選択します（Trust ゾーン）。
5. **IPv6** タブで **Enable IPv6 on the interface (インターフェイスでの IPv6 の有効化)** を選択します。
6. **Add (追加)** をクリックし、**Address (アドレス)** で **New Address (新規アドレス)** を選択します。
7. アドレスの **Name (名前)** を入力します。
8. （任意）トンネル アドレスの **Description (説明)** を入力します。
9. **Type (タイプ)** については **IP Netmask (IP ネットマスク)** を選択しIPv6 プレフィックスおよびプレフィックス長を入力します（この例では 64:FF9B::/96）。
10. **OK** をクリックします。
11. **Enable address on interface (インターフェイス上でアドレスを有効化)** を選択して**OK** をクリックします。
12. **OK** をクリックします。
13. **[OK]** をクリックしてトンネルを保存します。

STEP 9 | 信頼できるゾーンからの NAT トラフィックを許可するセキュリティポリシーを作成します。

1. **Policies (ポリシー)** > **Security (セキュリティ)** を選択してルールの **Name (名前)** を **Add (追加)** します。
2. **Source (送信元)** を選択して **Source Zone (送信元ゾーン)** を **Add (追加)** します（**Trust** を選択）。
3. **Source Address (送信元アドレス)** については **Any (すべて)** を選択します。
4. **Destination (宛先)** を選択して **Destination Zone (宛先ゾーン)** を **Add (追加)** します（**Untrust** を選択）。
5. **Application (アプリケーション)** については **Any (すべて)** を選択します。
6. **Actions （アクション）** については **Allow (許可)** を選択します。
7. **OK** をクリックします。

STEP 10 | 変更をコミットします。

Commit（コミット）をクリックします。

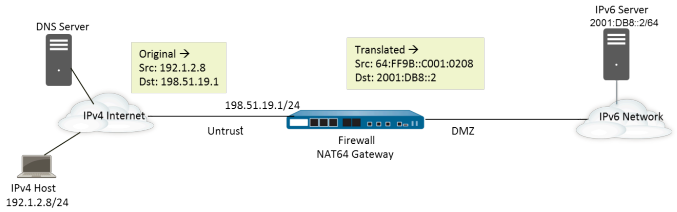
STEP 11 | NAT64 セッションのトラブルシューティングあるいは確認を行います。

```
> show session id <session-id>
```


IPv4 から開始される通信に NAT64 を設定

IPv6 サーバーに対して IPv4 から開始される通信は、IPv4 トポロジーにおける宛先 NAT と同様です。宛先IPv4 アドレスは、一対一の静的 IP 変換（複数対一の変換ではない）によって宛先 IPv6 アドレスにマッピングします。

ファイアウォールは、送信元 IPv4 アドレスを RFC 6052 で定義されている既知のプレフィックス 64:FF9B::/96 にエンコードします。変換された宛先アドレスは実際の IPv6 アドレスになります。IPv4 から開始される通信の典型的なユースケースは、組織がパブリックな信頼できないゾーンから組織の DMZ ゾーン内にある IPv6 サーバーへのアクセスを提供する場合です。このトポロジーは DNS64 サーバーを使用しません。



STEP 1 | IPv6 を有効化し、ファイアウォール上で稼働させます。

1. **Device (デバイス)** > **Setup (セットアップ)** > **Session (セッション)** を選択して Session Settings (セッション設定) を編集します。
2. **Enable IPv6 Firewalling (IPv6** ファイアウォールの有効化**)** を選択します。
3. **OK** をクリックします。

STEP 2 | （任意）IPv4 パケットの DF ビットがゼロに設定されている場合（かつ、IPv6 がパケットをフラグメント化しないために）、必ず変換後の IPv6 パケットが宛先 IPv6 ネットワーク用のパス MTU を超過しないようにしてください。

1. **Device (デバイス)** > **Setup (セットアップ)** > **Session (セッション)** を選択して Session Settings (セッション設定) を編集します。
2. For **NAT64 IPv6 Minimum Network MTU (NAT64 IPv6** 最小ネットワーク **MTU)**、ファイアウォールが IPv6 に変換するために IPv4 パケットをフラグメント化する最小バイト数を入力します（範囲は 1280～9216、デフォルトは 1280）。

   ファイアウォールが変換前に *IPv4* パケットをフラグメント化しないようにするためには、*MTU* を *9216* に設定します。変換後の *IPv6* パケットがまだこの値を超過している場合、ファイアウォールはパケットをドロップし、宛先に到達できないためにフラグメント化が必要であることを示す *ICMP* パケットを発行します。
3. **OK** をクリックします。

STEP 3 | IPv4 宛先アドレス用のアドレス オブジェクトを作成します（変換前）。

1. **Objects (オブジェクト)** > **Addresses (アドレス)** を選択して **Add (追加)** をクリックします。
2. オブジェクトの **Name (名前)** を入力します（例：nat64_ip4server）。
3. **Type (タイプ)** については **IP Netmask (IP** ネットマスク**)** を選択し、Untrust ゾーン内のファイアウォールのインターフェイスの IPv4 アドレスを入力します。アドレスは、ネットマスクを使用しないか、/32 のネットマスクのみを使用する必要があります。この例では 198.51.19.1/32 を使用します。
4. **OK** をクリックします。

STEP 4 | IPv6 送信元アドレス用のアドレス オブジェクトを作成します（変換後）。

1. **Objects (オブジェクト)** > **Addresses (アドレス)** を選択して **Add (追加)** をクリックします。
2. オブジェクトの **Name (名前)** を入力します（例：nat64_ip6server）。
3. **Type (タイプ)** については **IP Netmask (IP** ネットマスク**)** を選択し、RFC 6052 に準拠したネットマスクを伴うNAT64 IPv6 アドレスを入力します（/32、/40、/48、/56、/64、あるいは /96）。

   例えば、64:FF9B::/96 と入力します。

   （ファイアウォールは IPv4 送信元アドレス 192.1.2.8（C001:0208 の 16 進数）でプレフィックスをエンコードします）
4. **OK** をクリックします。

STEP 5 | IPv6 宛先アドレス用のアドレス オブジェクトを作成します（変換後）。

1. **Objects (オブジェクト)** > **Addresses (アドレス)** を選択して **Add (追加)** をクリックします。
2. オブジェクトの **Name (名前)** を入力します（例：nat64_server_2）。
3. **Type (タイプ)** については **IP Netmask (IP** ネットマスク**)** を入力し、IPv6 サーバー（宛先）の IPv6 アドレスを入力します。アドレスには、ネットマスクを使用しないか、/128 のネットマスクのみを使用する必要があります。この例では 2001:DB8::2/128 を使用します。
4. **OK** をクリックします。

STEP 6 | NAT64 ルールを作成します。

1. **Policies (ポリシー)** > **NAT** の順に選択して **Add (追加)** をクリックします。
2. **General** （全般） タブで NAT64 ルールの **Name (名前)** を入力します（例えば、nat64_ipv4_init）。
3. **NAT Type** [NAT タイプ]として、**nat64** を選択します。

STEP 7 | 元の送信元および宛先情報を指定します。

1. **Original Packet (**元のパケット**)** については、**Source Zone (**送信元ゾーン**)** を **Add (**追加**)** します（untrustゾーンの場合が多い）。
2. **Destination Zone (**宛先ゾーン**)** を選択します（trust あるいは DMZ ゾーンの場合が多い）。
3. **Source Address (**送信元アドレス**)** については、**Any (**すべて**)** を選択、あるいは IPv4 ホスト用のアドレス オブジェクトを **Add (**追加**)** します。
4. **Destination Address (**宛先アドレス**)** については、IPv4 宛先のアドレス オブジェクトを **Add (**追加**)** します（この例では nat64_ip4server）。
5. **Service (**サービス**)** については **any (**すべて**)** を選択します。

STEP 8 | 変換済みパケット情報を指定します。

1. **Translated Packet (**変換済みパケット**)** については、**Source Address Translation (**送信元アドレスの変換**)**、**Translation Type (**変換タイプ**)** にて **Static IP (**静的 **IP)** を選択します。
2. **Translated Address (**変換後アドレス**)** については、作成した送信元の変換後アドレス オブジェクト「nat64_ip6source」を選択します。
3. **Destination Address Translation (**宛先アドレスの変換**)** については、**Translated Address (**変換後アドレス**)** で単一の IPv6 アドレス（アドレス オブジェクト（この例では nat64_server_2）あるいはサーバーの IPv6 アドレス）を選択します。
4. **OK** をクリックします。

STEP 9 | Untrust ゾーンからの NAT トラフィックを許可するセキュリティポリシーを作成します。

1. **Policies (**ポリシー**)** > **Security (**セキュリティ**)** を選択してルールの **Name (**名前**)** を **Add (**追加**)** します。
2. **Source (**送信元**)** を選択して **Source Zone (**送信元ゾーン**)** を **Add (**追加**)** します（**Untrust** を選択）。
3. **Source Address (**送信元アドレス**)** については **Any (**すべて**)** を選択します。
4. **Destination (**宛先**)** を選択して **Destination Zone (**宛先ゾーン**)** を **Add (**追加**)** します（**DMZ** を選択）。
5. **Actions** （アクション） については **Allow (**許可**)** を選択します。
6. **OK** をクリックします。

STEP 10 | 変更をコミットします。

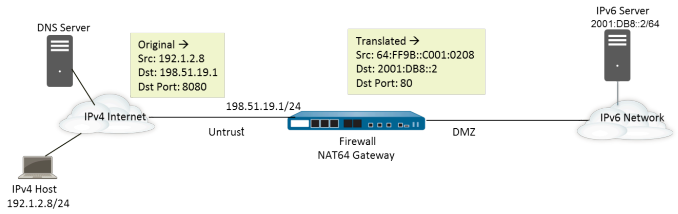
Commit（コミット）をクリックします。

STEP 11 | NAT64 セッションのトラブルシューティングあるいは確認を行います。

```
> show session id <session-id>
```


ポート変換を伴う IPv4 から開始される通信用に NAT64 を設定

IPv4 から開始される通信用に NAT64 を設定するタスクがこのタスクの前提になりますが、IPv6 ネットワークを制御する組織は、パブリックな宛先ポート番号を内部のポート番号に変換することで、ファイアウォールの信頼できない IPv4 側のユーザーから隠蔽することを好みます。この例では、ポート 8080 がポート 80 に変換されます。そのために、NAT64 ポリシールールの Original Packet (元のパケット) にて、宛先ポートを 8080 として指定する新しいサービスを作成します。Translated Packet (変換済みパケット) の場合、変換後のポートは80 です。



STEP 1 | IPv6 を有効化し、ファイアウォール上で稼働させます。

1. **Device (デバイス)** > **Setup (セットアップ)** > **Session (セッション)** を選択して Session Settings (セッション設定) を編集します。
2. **Enable IPv6 Firewalling (IPv6** ファイアウォールの有効化**)** を選択します。
3. **OK** をクリックします。

STEP 2 | （任意）IPv4 パケットの DF ビットがゼロに設定されている場合（かつ、IPv6 がパケットをフラグメント化しないために）、必ず変換後の IPv6 パケットが宛先 IPv6 ネットワーク用のパス MTU を超過しないようにしてください。

1. **Device (デバイス)** > **Setup (セットアップ)** > **Session (セッション)** を選択して Session Settings (セッション設定) を編集します。
2. **NAT64 IPv6 Minimum Network MTU (NAT64 IPv6** 最小ネットワーク **MTU)**、ファイアウォールが IPv6 に変換するために IPv4 パケットをフラグメント化する最小バイト数を入力します（範囲は 1280～9216、デフォルトは 1280）。

   ファイアウォールが変換前に *IPv4* パケットをフラグメント化しないようにするためには、*MTU* を *9216* に設定します。変換後の *IPv6* パケットがまだこの値を超過している場合、ファイアウォールはパケットをドロップし、宛先に到達できないためにフラグメント化が必要であることを示す *ICMP* パケットを発行します。
3. **OK** をクリックします。

STEP 3 | IPv4 宛先アドレス用のアドレス オブジェクトを作成します（変換前）。

1. **Objects (オブジェクト)** > **Addresses (アドレス)** を選択して **Add (追加)** をクリックします。
2. オブジェクトの **Name (名前)** を入力します（例：nat64_ip4server）。
3. **Type (タイプ)** については **IP Netmask (IP** ネットマスク**)** を選択し、Untrust ゾーン内のファイアウォールのインターフェイスのネットマスクおよび IPv4 アドレスを入力します。この例では 198.51.19.1/24 を使用します。
4. **OK** をクリックします。

STEP 4 | IPv6 送信元アドレス用のアドレス オブジェクトを作成します（変換後）。

1. **Objects (オブジェクト)** > **Addresses (アドレス)** を選択して **Add (追加)** をクリックします。
2. オブジェクトの **Name (名前)** を入力します（例：nat64_ip6server）。
3. **Type (タイプ)** については **IP Netmask (IP** ネットマスク**)** を選択し、RFC 6052 に準拠したネットマスクを伴うNAT64 IPv6 アドレスを入力します（/32、/40、/48、/56、/64、あるいは /96）。

   例えば、64:FF9B::/96 と入力します。

   （ファイアウォールは IPv4 送信元アドレス 192.1.2.8（C001:0208 の 16 進数）でプレフィックスをエンコードします）
4. **OK** をクリックします。

STEP 5 | IPv6 宛先アドレス用のアドレス オブジェクトを作成します（変換後）。

1. **Objects (オブジェクト)** > **Addresses (アドレス)** を選択して **Add (追加)** をクリックします。
2. オブジェクトの **Name (名前)** を入力します（例：nat64_server_2）。
3. **Type (タイプ)** については **IP Netmask (IP** ネットマスク**)** を入力し、IPv6 サーバー（宛先）の IPv6 アドレスを入力します。この例では 2001:DB8::2/64 を使用します。

   送信元および宛先のネットマスク（プレフィックス長）が同じである必要があります。
4. **OK** をクリックします。

STEP 6 | NAT64 ルールを作成します。

1. **Policies (ポリシー)** > **NAT** の順に選択して **Add (追加)** をクリックします。
2. **General** （全般） タブで NAT64 ルールの **Name (名前)** を入力します（例えば、nat64_ipv4_init）。
3. **NAT Type** [NAT タイプ]として、**nat64** を選択します。

STEP 7 | 元の送信元および宛先情報を指定し、サービスを作成して変換を単体の入力ポート番号に限定します。

1. **Original Packet (**元のパケット**)** については、**Source Zone (**送信元ゾーン**)** を **Add (**追加**)** します（untrustゾーンの場合が多い）。
2. **Destination Zone (**宛先ゾーン**)** を選択します（trust あるいは DMZ ゾーンの場合が多い）。
3. **Service (**サービス**)** については新規の **Service (**サービス**)** を選択します。
4. サービスの **Name (**名前**)**（Port_8080 など）を入力します。
5. **TCP** を **Protocol (**プロトコル**)** として選択します。
6. **Destination Port (**宛先ポート**)** については 8080 を入力します。
7. **OK** をクリックして Service (サービス) を保存します。
8. **Source Address (**送信元アドレス**)** については、**Any (**すべて**)** を選択、あるいは IPv4 ホスト用のアドレス オブジェクトを **Add (**追加**)** します。
9. **Destination Address (**宛先アドレス**)** については、IPv4 宛先のアドレス オブジェクトを **Add (**追加**)** します（この例では nat64_ip4server）。

STEP 8 | 変換済みパケット情報を指定します。

1. **Translated Packet (**変換済みパケット**)** については、**Source Address Translation (**送信元アドレスの変換**)**、**Translation Type (**変換タイプ**)** にて **Static IP (**静的 **IP)** を選択します。
2. **Translated Address (**変換後アドレス**)** については、作成した送信元の変換後アドレス オブジェクト「nat64_ip6source」を選択します。
3. **Destination Address Translation (**宛先アドレスの変換**)** については、**Translated Address (**変換後アドレス**)** で単一の IPv6 アドレス（アドレス オブジェクト（この例では nat64_server_2）あるいはサーバーの IPv6 アドレス）を選択します。
4. ファイアウォールがパブリックな宛先ポート番号の変換先にするプライベートな宛先 **Translated Port (**変換済みポート**)** 番号を指定します。
5. **OK** をクリックします。

STEP 9 | Untrust ゾーンからの NAT トラフィックを許可するセキュリティポリシーを作成します。

1. **Policies (**ポリシー**)** > **Security (**セキュリティ**)** を選択してルールの **Name (**名前**)** を **Add (**追加**)** します。
2. **Source (**送信元**)** を選択して **Source Zone (**送信元ゾーン**)** を **Add (**追加**)** します（**Untrust** を選択）。
3. **Source Address (**送信元アドレス**)** については **Any (**すべて**)** を選択します。
4. **Destination (**宛先**)** を選択して **Destination Zone (**宛先ゾーン**)** を **Add (**追加**)** します（**DMZ** を選択）。
5. **Actions** （アクション） については **Allow (**許可**)** を選択します。
6. **OK** をクリックします。

STEP 10 | 変更をコミットします。

Commit（コミット）をクリックします。

STEP 11 | NAT64 セッションのトラブルシューティングあるいは確認を行います。

```
> show session id <session-id>
```


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。

- 同じ宛先に対するフロー（セッション）を複数の等コストのリンクで負荷分散する。
- 一部のリンクを未使用のままにせず、同じ宛先に対する複数のリンクで使用可能なすべての帯域幅を効率的に使用する。
- 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ます。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。これは、リンクに障害が発生したときにダウンタイムを削減するのに役立ちます。

ECMPは、PA-7000シリーズ、PA-5200シリーズ、PA-3200シリーズでハードウェアフォワーディングサポートを提供し、すべてのPalo Alto Networks®ファイアウォールモデルでサポートされています。VM-Series ファイアウォールでは、ソフトウェアを介してのみ ECMP がサポートされます。セッションをハードウェア オフロードできない場合、パフォーマンスに影響します。

ECMP は、レイヤー 3、レイヤー 3 サブインターフェイス、VLAN、トンネル、および集約された Ethernet インターフェイスでサポートされます。

ECMP は、スタティック ルートや、ファイアウォールでサポートされているダイナミック ルーティング プロトコル用に設定できます。

容量はパス数に基づいているため、ECMP はルート テーブル容量に影響します。そのため、4 つのパスがある ECMP ルートでは、ルート テーブル容量の 4 つのエントリが消費されます。トラフィック フローを特定のインターフェイスにマッピングするためにセッション ベースのタグでより多くメモリが使用されているため、ECMP の実装でルート テーブル容量が若干減少する場合があります。

スタティック ルートを使用する仮想ルーター間ルーティングでは、ECMP はサポートされません。

HAピアが失敗した際のECMPパスを選択する方法についてはアクティブ/アクティブHAモードにおけるECMPを参照してください。

以下のセクションでは、ECMP とその設定方法について説明します。

- ECMP 負荷分散アルゴリズム
- 仮想ルーターでの ECMP の設定
- 複数の BGP AS （Autonomous System）の ECMP の有効化
- ECMP の確認

ECMP 負荷分散アルゴリズム

ファイアウォールのルーティング情報ベース（RIB）に、1 つの宛先への等コストのパスが複数あるとします。等コストのパスの最大数はデフォルトの 2 になっています。ECMP は、RIB から最適な 2 つの等コストのパスを選択し、転送情報ベース（FIB）にコピーします。次に、ECMP は負荷分散方式に基づいて、このセッション中にファイアウォールが宛先として使用するパスを FIB のいずれかのパスから選択します。

ECMP 負荷分散は、パケット レベルではなくセッション レベルで行われるため、ファイアウォール（ECMP）が等コストのパスを選択したときに新しいセッションが開始されます。1 つの宛先への等コストのパスは、ECMP パス メンバーまたは ECMP グループ メンバーとみなされます。FIB には 1 つの宛先へのパスが複数ありますが、ECMP は、設定した負荷分散アルゴリズムに基づいて、その中から ECMP フローで使用するパスを決定します。仮想ルーターで使用できる負荷分散アルゴリズムは 1 つのみです。

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。

4 つの各アルゴリズムでは、以下のように優先する内容が異なります。

- **Hash-based algorithms prioritize session stickiness** [セッション持続性を優先するハッシュ ベース アルゴリズム] – **IP Modulo** [IP モジュロ]および **IP Hash** [IP ハッシュ]アルゴリズムでは、パケット ヘッダーの情報（送信元アドレスや宛先アドレスなど）に基づくハッシュを使用します。特定のセッションの各フローのヘッダーには、同じ送信元および宛先情報が含まれているため、これらのオプションではセッション持続性が優先されます。**IP Hash** アルゴリズムを選択した場合、ハッシュは送信元アドレスと宛先アドレスに基づくか、または送信元アドレスのみに基づいてハッシュを使用できます。送信元アドレスのみを基準にして IP ハッシュを使用すると、同じ送信元 IP アドレスに属すすべてのセッションが、複数の利用できるパスの中から常に同じパスを選ぶようになります。そのためパスの固定性が増し、必要な場合にトラブルシューティングを行いやすくなります。同じ宛先のセッションが大量にあり、ECMP リンク間で均等に分散されない場合に、必要に応じて **Hash Seed (**ハッシュ シード**)** の値を設定し、さらに負荷分散をランダム化できます。
- [負荷分散を優先する均等アルゴリズム] – **Balanced Round Robin** [均等ラウンド ロビン]アルゴリズムでは、受信セッションをリンク間で均等に分散し、セッション持続性よりも負荷分散を優先します（ラウンド ロビンは、最も長い間選択されていない項目が選択されるシーケンスを示します）。 また、新しいルートが ECMP グループに追加されたり、ECMP グループから削除されたりした場合（グループのパスがダウンした場合など）、仮想ルーターがグループのリンク間でセッションを再調整します。また、機能停止により、セッションのフローのルートを切り替える必要がある場合、セッションに関連付けられている元のルートが再度使用可能になると、仮想ルーターがもう一度負荷を再調整するときに、セッションのフローが元のルートに戻ります。
- 加重アルゴリズムはリンク容量および/または速度 を優先する – ECMP プロトコル規格の拡張として、パロアルトネットワークス® 実装は、ファイアウォールの出力の出力の異なるリンク容量と速度を考慮した 重み付きラウンドロビン ロードバランシング オプションを提供します。このオプションを使用すると、リンクのキャパシティ、速度、待機時間などの要素

を使用して、リンクパフォーマンスに基づいてインターフェイスに **ECMP Weights** (範囲は 1 ~ 255、デフォルトは 100) を割り当て、使用可能なリンクを完全に活用するために負荷のバランスを取ることができます。

たとえば、ファイアウォールに、ISP への冗長性リンク ethernet1/ （100 Mbps）および ethernet1/ （200 Mbps）があるとします。これらは等コストのパスですが、ethernet1/8 経由のリンクの帯域幅の方が大きいため、ethernet1/1 リンクよりも大きな負荷を処理できます。そのため、負荷分散機能でリンク容量およびリンク速度が考慮されるように、ethernet1/8 に 200 の重み、ethernet1/1 に 100 の重みを割り当てることができます。重みの割合が 2:1 であるため、仮想ルーターは ethernet1/1 の 2 倍のセッションを ethernet1/8 に送信します。ただし、ECMP プロトコルは本質的にはセッション ベースであるため、**Weighted Round Robin** [重み付きラウンド ロビン]アルゴリズムを使用する場合、ファイアウォールは、ベスト エフォート ベースでのみ ECMP リンク間で負荷を分散できます。

ECMP の重みをインターフェイスに割り当てる目的は、（コストが異なる可能性のある各ルートから）ルートを選択することではなく、（等コストのパスの選択に影響する）負荷分散を決定することです。

速度の遅いまたは容量の小さいリンクを割り当てる場合、重みを小さくします。速度の速いまたは容量の大きいリンクを割り当てる場合、重みを大きくします。このようにして、ファイアウォールは、いずれかの等コストのパスの容量の小さいリンクを過度に使用することなく、これらの割合に基づいてセッションを分散できます。

仮想ルーターでの ECMP の設定

仮想ルーターで ECMP を有効にするには、以下の手順を実行します。以下の操作を実行していることが前提条件となります。

- 仮想ルーターに属するインターフェイスを指定します（**Network (ネットワーク)** > **Virtual Routers (仮想ルーター)** > **Router Settings (ルーター設定)** > **General (全般)**）。
- IP ルーティング プロトコルを指定する。

既存の仮想ルーターで ECMP の有効化、無効化、または変更を行うと、仮想ルーターが再起動します。これにより、セッションが終了する場合があります。

STEP 1 | 仮想ルーターの ECMP を有効にします。

1. **Network (ネットワーク)** > **Virtual Routers (仮想ルーター)** の順に選択し、ECMP を有効にする仮想ルーターを選択します。
2. **Router Settings (ルーター設定)** > **ECMP** の順に選択し、さらに **Enable (有効)** を選択します。

STEP 2 | （任意）サーバーからクライアントへのパケットの対称リターンを有効にします。

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。**Symmetric Return** [対称リターン]設定は、負荷分散よりも優先されます。この動作は、トラフィック フローがサーバーからクライアントに移動する場合にのみ実行されます。

STEP 3 | **Strict Source Path (厳密な送信元パス)** を有効にして、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、IPSec トンネルの送信元 IPアドレスが属する物理インターフェースから確実に出力されるようにします。

ECMP を有効にすると、ファイアウォールで発信される 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。または、厳密な送信元パスを有効にすることで、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、IPSec トンネルの送信元 IPアドレスが属する物理インターフェースから常に出力されるようにすることができます。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、この機能を有効にします。ISP は通常、リバース パス フォワーディング (RPF) チェック (または IPアドレス スプーフィングを防ぐための別のチェック) を実行して、そのトラフィックが到着したのと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 (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、それはISP が期待するものではないことがあり、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。この場合、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、RPF チェックが成功し、ISP がリターン トラフィックを許可するように、厳密な送信元パスを有効にします。

STEP 4 | ルーティング情報ベース（RIB）から転送情報ベース（FIB）にコピーできる（宛先ネットワークへの）等コストのパスの最大数を指定します。

許容される **Max Path** [最大パス]に、**2**、**3**、または **4** を入力します。デフォルト：2.

STEP 5 | 仮想ルーターの負荷分散アルゴリズムを選択します。各負荷分散方式とそれらの違いの詳細は、ECMP 負荷分散アルゴリズムを参照してください。

Load Balance (負荷分散**)** については、**Method (**メソッド**)** リストから以下のいずれかのオプションを選択します。

- **IP Modulo (IP** モジュロ**)**（デフォルト） — 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。
- **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 メソッドは 2 つあります（ステップ 5 でハッシュ オプションを選択）。
  - 送信元アドレスのハッシュを使用します（PAN-OS 8.0.3 以降のリリースで利用可能）。
  - 送信元および宛先 IP アドレスのハッシュを使用します（デフォルトの IP ハッシュ メソッド）。
- **Balanced Round Robin** [均等ラウンド ロビン] — ECMP パス間でラウンド ロビンを使用し、パス数が変更されたときにパスを再調整します。
- **Weighted Round Robin** [重み付きラウンド ロビン] — ラウンド ロビンと相対的な重みを使用して、ECMP パスを選択します。以下のステップ 6 で重みを指定します。

STEP 6 | （IP Hash only (IP ハッシュのみ)）IP ハッシュ オプションを設定します。

Method [メソッド]として **IP Hash** [IP ハッシュ]を選択した場合、以下の手順を実行します。

1. 同じソース IP アドレスに属するすべてのセッションが必ず、利用可能な複数のパスの中から同じパスを取得するようにしたい場合は、**Use Source Address Only (**送信元アドレスのみを使用**)**（PAN-OS 8.0.3 以降のリリースで利用可能）を選択します。この IP ハッシュ オプションによりパスの固定性が増し、トラブルシューティングを行いやすくなります。このオプションを選択しない、あるいはPAN-OS 8.0.3 より前のリリースを使用している場合、IP ハッシュは送信元および宛先 IP アドレスに基づきます（デフォルトの IP ハッシュ メソッド）。

   > ***Use Source Address Only (***送信元アドレスのみを使用***)*** を選択する場合、*PAN-OS 8.0.2*、*8.0.1*、あるいは *8.0.0* を実行しているファイアウォールに *Panorama* から設定をプッシュしてはなりません。

2. **IP Hash** [IP ハッシュ]の計算に送信元または宛先ポート番号を使用する場合、**Use Source/Destination Ports** [送信元/宛先ポートの使用]を選択します。

   > ***Use Source Address Only (***送信元アドレスのみを使用***)*** と併せてこのオプションを有効化すると、同じソース *IP* アドレスに属すセッションであっても、パスがランダムに選択されるようになります。

3. **Hash Seed (**ハッシュ シード**)** の値を入力します（最大 9 桁の整数）。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]の値を指定します。同じタプル情報のセッションが多数存在する場合、ハッシュ シード値を指定すると便利です。

STEP 7 | （Weighted Round Robin only (重み付きラウンド ロビンのみ)）ECMP グループの各インターフェイスの重みを定義します。

Method [メソッド]として **Weighted Round Robin** [重み付きラウンド ロビン]を選択した場合、同じ宛先にルーティングされるトラフィックの出力点となる各インターフェイス（ISP に冗長性リンクを提供するインターフェイスや企業ネットワークのコア ビジネス アプリケーションへのインターフェイスなど、ECMP グループに含まれるインターフェイス）の重みを定義します。

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。

1. **Add (追加)** をクリックして、**Interface (インターフェイス)** を選択し、ECMP グループを作成します。
2. ECMP グループに他のインターフェイスを**Add** [追加]します。
3. **Weight** [重み]をクリックし、各インターフェイスの相対的な重みを指定します（範囲は 1 ～ 255、デフォルトは 100）。

STEP 8 | 設定を保存します。

1. **OK** をクリックします。
2. ECMP Configuration Change [ECMP設定変更]のプロンプトで**Yes** [はい]をクリックして仮想ルーターを再起動します。仮想ルーターを再起動すると、既存のセッションが終了する可能性があります。

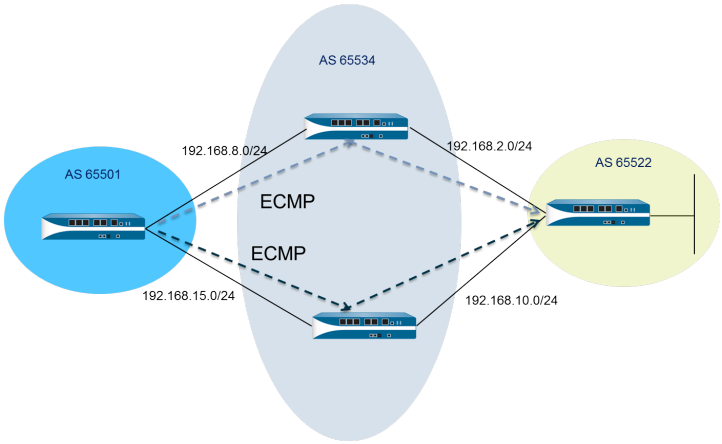
   このメッセージは、*ECMP* を使用する既存の仮想ルーターを変更する場合にのみ表示されます。

STEP 9 | 変更をコミットします。

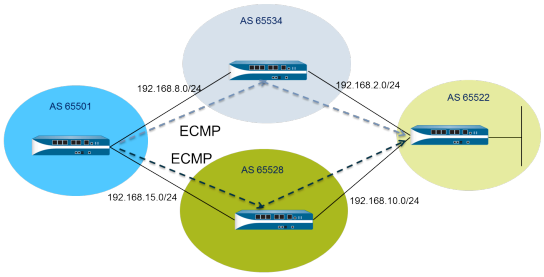
設定を **Commit**（コミット）します。

複数の BGP AS （Autonomous System）の ECMP の有効化

BGP を設定していて、複数の AS で ECMP を有効にする場合、以下のタスクを実行します。このタスクは、BGP がすでに設定されていることを想定しています。以下の図では、1 つの宛先への 2 つの ECMP パスが 1 つの BGP AS の 1 つの ISP に属している 2 つのファイアウォールを通過しています。



以下の図では、1 つの宛先への 2 つの ECMP パスが異なる BGP AS の 2 つの異なる ISP に属している 2 つのファイアウォールを通過しています。



STEP 1 | ECMP を設定します。

仮想ルーターでの ECMP の設定を参照してください。

STEP 2 | BGP ルーティングの場合、複数の AS で ECMP を有効にします。

1. **Network (ネットワーク)** > **Virtual Routers (仮想ルーター)** の順に選択し、複数の BGP AS の ECMP を有効にする仮想ルーターを選択します。
2. **BGP** > **Advanced (詳細)** を選択し、さらに **ECMP Multiple AS Support (ECMP マルチ AS サポート)** を選択します。

STEP 3 | 変更をコミットします。

OK、**Commit (コミット)** の順にクリックします。

ECMP の確認

ECMP 用に設定された仮想ルーターは、転送情報ベース（FIB）テーブルで ECMP ルートとなるルートを示します。ルートの ECMP フラグ（E）は、ルートがそのネクスト ホップへ出力インターフェイスの ECMP に参加していることを示します。ECMP を検証するために、次の作業を行って FIB を調べ、一部のルートが等コストの複数のパスであることを確認します。

STEP 1 | Select **Network (ネットワーク)** > **Virtual Routers (仮想ルーター)**。

STEP 2 | ECMP を有効にした仮想ルーターの行で、**More Runtime Stats** [詳細ランライム状態]をクリックします。

STEP 3 | **Routing (ルーティング)** > **Forwarding Table (転送テーブル)** を選択して FIB を確認します。

テーブルでは、（異なるインターフェイスから）同じ宛先への複数のルートに「*E*」フラグが設定されています。アスタリスク（*）は、*ECMP* グループの優先パスを示します。

LLDP

Palo Alto Networks ファイアウォールは、Link Layer Discovery Protocol (LLDP) をサポート®、隣接するデバイスとその機能を検出するためにリンクレイヤーで機能します。LLDP を使用すると、ファイアウォールおよび他のネットワーク デバイスは、LLDP データ ユニット（LLDPDU）をネイバーとの間で送受信できます。受信デバイスは、Simple Network Management Protocol （SNMP）がアクセスできる MIB に情報を保存します。LLDP により、トラブルシューティングが一層容易になります。特に、ping または traceroute でファイアウォールが通常検出されないバーチャル ワイヤー デプロイメントにおいて、トラブルシューティングがより簡単に行えるようになります。

LLDP の概要

Link Layer Discovery Protocol (LLDP) は、MAC アドレスを使用して OSI モデルのレイヤ 2 で動作します。LLDPDU は、Ethernet フレームのカプセル化された type-length-value （TLV）要素のシーケンスです。IEEE 802.1AB 標準では、LLDPDU の 3 つの MAC アドレスが定義されています。01-80-C2-00-00-0E、01-80-C2-00-00-03、および01-80-C2-00-00-00。

Palo Alto Networks ®ファイアウォールは、LLDP データユニットの送受信に 1 つの MAC アドレスのみをサポートします。01-80-C2-00-00-0E。送信する場合、ファイアウォールは宛先 MAC アドレスとして 01-80-C2-00-00-0E を使用します。受信する場合、ファイアウォールは宛先 MAC アドレスとして 01-80-C2-00-00-0E を使用して、データグラムを処理します。ファイアウォールのインターフェイスで LLDPDU のその他の 2 つのいずれかの MAC アドレスを受信する場合、ファイアウォールは、以下のように、この機能の前に実行した転送アクションを実行します。

- インターフェイス タイプが vwire の場合、ファイアウォールはデータグラムをもう一方のポートに転送します。
- インターフェイス タイプが L2 の場合、ファイアウォールは残りの VLAN にデータグラムをフラッディングします。
- インターフェイス タイプが L3 の場合、ファイアウォールはデータグラムをドロップします。

Panorama および WildFire アプライアンスはサポートされていません。

LLDP をサポートしないインターフェイスの種類は、タップ、高可用性 (HA)、Decrypt Mirror、仮想ワイヤ/vlan/L3 サブインターフェイス、および PA-7000 シリーズ Log Prog の Processing Card (LPC) インターフェイスです。

LLDP Ethernet フレームの形式は、以下のとおりです。

Preamble	Destination MAC	Source MAC	Ethertype	Chassis ID TLV	Port ID TLV	Time To Live TLV	Optional TLVs	End of LLDPDU TLV	Frame Check Sequence
	01:80:C2:00:00:0E or 01:80:C2:00:00:03 or 01:80:C2:00:00:00	Station's Address	0x88CC	Type=1	Type=2	Type=3	Zero or more complete TLVs	Type=0, Length=0	

LLDP Ethernet フレーム内の TLV 構造の形式は以下のとおりです。

TLV Type	TLV Information String Length	TLV Information String
7 bits	9 bits	0-511 octets

LLDP のサポートされている TLV

LLDPDU には、必須および任意の TLV があります。以下の表に、ファイアウォールでサポートされている必須 TLV を示します。

必須 TLV	TLV タイプ	説明
シャーシ ID	1	ファイアウォールのシャーシを識別します。各ファイアウォールには、1 つの一意のシャーシ ID が必要です。Chassis ID サブタイプは、Palo Alto Networks® モデルでは、一意性を確保するために Eth0 の MAC アドレスを使用します。
ポート ID	2	LLDPDU の送信元ポートを識別します。各ファイアウォールは、送信される LLDPDU メッセージごとに 1 つのポート ID を使用します。ポート ID サブタイプは（インターフェイス名）で、送信ポートを一意に識別します。ファイアウォールは、ポート ID としてインターフェイスの ifname を使用します。
Time-to-live（TTL）	3	ピアから受信した LLDPDU 情報が有効な状態でローカル ファイアウォールに保持される秒数（範囲は 0 ～ 65535）を指定します。値は、LLDP ホールド タイム乗数の倍数になります。TTL の値が 0 になると、デバイスに関連付けられている情報が無効になり、ファイアウォールはそのエントリを MIB から削除します。
LLDPDU の終了	0	LLDP Ethernet フレームの TLV の終了を示します。

以下の表に、Palo Alto Networks ファイアウォールでサポートされている任意の TLV を示します。

任意の TLV	TLV タイプ	ファイアウォールの実装の目的およびメモ
ポートの説明	4	ファイアウォールのポート（英数字形式）を説明します。ifAlias オブジェクトが使用されます。
システム名	5	設定されているファイアウォールの名前（英数字形式）。sysName オブジェクトが使用されます。
システムの説明	6	ファイアウォール（英数字形式）を説明します。sysDescr オブジェクトが使用されます。

任意の **TLV**	**TLV** タイプ	ファイアウォールの実装の目的およびメモ
システムの機能	7	以下のようなインターフェイスのデプロイメント モードを説明します。 • L3 インターフェイスは、ルーター（ビット 6）の機能と「他の」ビット（ビット 1）を使用して通知されます。 • L2 インターフェイスは、MAC ブリッジ（ビット 3）の機能と「他の」ビット（ビット 1）を使用して通知されます。 • バーチャル ワイヤー インターフェイスは、リピータ（ビット 2）の機能と「他の」ビット（ビット 1）を使用して通知されます。
管理アドレス	8	ファイアウォールの管理に使用される以下のような 1 つ以上の IP アドレス。 • 管理（MGT）インターフェイスの IP アドレス • インターフェイス IPv4 および/または IPv6 アドレス • ループバック アドレス • 管理アドレス フィールドに入力されたユーザー定義アドレス 管理 IP アドレスを指定しない場合、デフォルトは送信インターフェイスの MAC アドレスです。 指定した管理アドレスのインターフェイス番号が含まれます。また、指定した管理アドレスのハードウェア インターフェイスの OID も含まれます（該当する場合）。 複数の管理アドレスを指定した場合、指定した順に（リストの上から）送信されます。最大 4 個の管理アドレスがサポートされています。 これは任意のパラメータであるため、無効のままにすることができます。

LLDP Syslog メッセージおよび SNMP トラップ

ファイアウォールは、MIB に LLDP 情報を保存し、SNMP マネージャがそれをモニターできます。LLDP イベントに関する SNMP トラップ通知および Syslog メッセージをファイアウォールから送信する場合、LLDP プロファイルで **SNMP Syslog Notification** [SNMP Syslog 通知]を有効にする必要があります。

MIB が変更されると、LLDP は RFC 5424、Syslog Protocol や RFC 1157、Simple Network Management Protocol を使用して、Syslog および SNMP トラップ メッセージを送信します。これらのメッセージの頻度は LLDP グローバル設定の **Notification Interval** [通知間隔]によって制限されています。この設定はデフォルトの 5 秒になっていますが、変更可能です。

LLDP Syslog および SNMP トラップ メッセージの頻度が制限されているため、これらのプロセスに提供される LLDP 情報の一部は、LLDP 状態情報を表示するときに表示される最新の LLDP 統計と一致しない可能性があります。これは、想定どおりの正常な動作です。

インターフェイス（Ethernet または AE）ごとに最大 5 個の MIB を受信できます。異なる送信元ごとに 1 つの MIB があります。この制限を超えると、エラー メッセージ `tooManyNeighbors` がトリガーされます。

LLDP の設定

LLDP を設定して LLDP プロファイルを作成するには、スーパーユーザーかデバイス管理者（deviceadmin）である必要があります。ファイアウォール インターフェイスでは、最大 5 個の LLDP ピアがサポートされています。

STEP 1 | ファイアウォールで LLDP を有効にします。

Network (ネットワーク) > **LLDP** の順に選択してLLDP General (LLDP 一般) セクションを編集し、**Enable (有効)** を選択します。

STEP 2 | （任意）LLDP グローバル設定を変更します。

1. **Transmit Interval (sec)** [送信間隔 (秒)]で、LLDPDU が送信される間隔（秒）を指定します。範囲は 1 から 3600 までです。デフォルトは 30 です。
2. **Transmit Delay (sec)** [送信遅延 (秒)]で、TLV 要素が変更された後に送信される LLDP 伝送間の遅延時間（秒）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。**[送信遅延]** の値は、**[送信間隔]** よりも小さくする必要があります。範囲は 1 から 600 です。デフォルトは 2 です。
3. **Hold Time Multiple** [ホールド タイムの間隔数]で、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 から 100 までです。デフォルトは 4 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。
4. **Notification Interval (通知間隔)** で、MIB の変更時にLLDP Syslog メッセージおよび SNMP トラップが送信される間隔（秒）を指定します。範囲は 1 から 3600 までです。デフォルトは 5 です。
5. **OK** をクリックします。

STEP 3 | LLDP プロファイルを作成します。

任意の TLV の詳細は、LLDP のサポートされている TLV を参照してください。

1. **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)** を選択し、その BFD プロファイルの **Name (名前)** を **Add (追加)** します。
2. **Mode** [モード]で、**transmit-receive** [送受信]（デフォルト）、**transmit-only** [送信のみ]、または **receive-only** [受信のみ]を選択します。
3. **SNMP Syslog Notification (SNMP Syslog 通知)** を選択して、SNMP 通知および Syslog メッセージを有効にします。有効にした場合、グローバル **Notification Interval** [通知間隔]が使用されます。ファイアウォールは **Device (デバイス)** > **Log Settings (ログ設定)** > **System (システム)** > **SNMP Trap Profile (SNMP トラップ プロファイル)** and **Syslog**

Profile (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。

4. 任意の TLV の場合、送信する TLV を選択します。
   - ポートの説明
   - システム名
   - システムの説明
   - システムの機能
5. （任意）**Management Address** [管理アドレス]を選択し、管理アドレスを追加（複数可）して**Name** [名前]を**Add** [追加]します。
6. 管理アドレスを取得する **Interface** [インターフェイス]を選択します。**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、管理アドレスの TLV 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。
7. **IPv4** または **IPv6** を選択した後、隣のフィールドのリスト (選択したインターフェイスに設定されているアドレスがリストされる) から IP アドレスを選択するか、アドレスを入力します。
8. **OK** をクリックします。
9. 最大 4 個の管理アドレスを使用できます。複数の **Management Address** [管理アドレス]を指定した場合、指定した順に（リストの上から）送信されます。アドレスの順番を変更するには、アドレスを選択して **Move Up** [上へ]ボタンまたは **Move Down** [下へ]ボタンを使用します。
10. **OK** をクリックします。

STEP 4 | LLDP プロファイルをインターフェイスに割り当てます。

1. **Network (ネットワーク)** > **Interfaces (インターフェイス)** の順に選択し、LLDP プロファイルを割り当てるインターフェイスを選択します。
2. **Advanced[詳細]** > **LLDP** を選択します。
3. **Enable LLDP** [LLDP の有効化]を選択して、LLDP プロファイルをインターフェイスに割り当てます。
4. **Profile**（プロファイル）で作成したプロファイルを選択します。**None** [なし]を選択すると、基本的な機能（3 つの必須 TLV の送信および **transmit-receive** [送受信]モードの有効化）で LLDP が有効になります。

   新しいプロファイルを作成する場合は **LLDP Profile (LLDP プロファイル)** をクリックし、上記の流れに従って作業を行います。
5. **OK** をクリックします。

STEP 5 | 変更を **Commit (コミット)** します。

LLDP 設定および状態の表示

LLDP 設定および状態を表示するには、以下の手順を実行します。

STEP 1 | LLDP グローバル設定を表示します。

Network (ネットワーク) > **LLDP** を選択します。

LLDP General [LLDP一般]画面の **Enable** [有効化]は、LLDP が有効になっているかどうかを示します。

- LLDP が有効になっている場合、設定されたグローバル設定（Transmit Interval （送信間隔）、Transmit Delay （送信遅延）、Hold Time Multiple （ホールド タイムの間隔数）、および Notification Interval （通知間隔））が表示されます。
- LLDP が有効になっていない場合、グローバル設定のデフォルト値が表示されます。

これらの値の説明については、LLDP の設定の 2 番目のステップを参照してください。

STEP 2 | LLDP 状態情報を表示します。

1. **Status** [状態]タブを選択します。
2. （任意）表示される情報を制限するフィルタを入力します。

   インターフェイス情報:

   - **Interface** [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。
   - **LLDP** – LLDP の状態で、enabled [有効]または disabled [無効]のいずれかです。
   - **Mode** [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。
   - **Profile** [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。

   送信情報:

   - **Total Transmitted** [送信合計] – インターフェイスから送信された LLDPDU の数。
   - **Dropped Transmit** [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。

   受信情報:

   - **Total Received** [受信合計] – インターフェイスで受信した LLDP フレームの数。
   - **Dropped TLV** [ドロップされた TLV] – 受信時に破棄された LLDP フレームの数。
   - **Errors** [エラー] – インターフェイスで受信した TLV 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。

- **Unrecognized** [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。たとえば、TLV のタイプが予約済みの TLV の範囲内にある TLV などが挙げられます。
- **Aged Out** [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。

STEP 3 | インターフェイスで検出された各ネイバーの LLDP サマリー情報を表示します。

1. **Peers** [ピア]タブを選択します。
2. （任意）表示される情報を制限するフィルタを入力します。

   Local Interface [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 [リモート シャーシ ID] — ピアのシャーシ ID。MAC アドレスが使用されます。

   Port ID [ポート ID] — ピアのポート ID。

   Name [名前]—ピアの名前。

   More info [その他の情報] — 必須および任意の TLV に基づく以下のリモート ピアの詳細が表示されます。

   - シャーシのタイプ:MAC アドレス:
   - 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。

LLDP 統計のクリア

特定のインターフェイスの LLDP 統計をクリアできます。

特定のインターフェイスの LLDP 統計をクリアします。

1. **Network (**ネットワーク**)** > **LLDP** > **Status (**ステータス**)** の順に選択し、左側の列で、LLDP 統計をクリアするインターフェイスを 1 つ以上選択します。
2. 画面の下部にある **Clear LLDP Statistics (LLDP** 統計のクリア**)** をクリックします。

BFD

ファイアウォールは、2つのルーティング ピア間の双方向パスに関するエラーを認識するプロトコル「双方向送信検出 （BFD）（RFC 5880）」をサポートしています。BFD障害検知は極めて高速なため、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。高可用性が求められるミッションクリティカルなデータセンターやネットワーク、および極めて高速なフェイルオーバーを達成しようとすると、BFDによる極めて高速なエラー検知が必要になってきます。

- BFD の概要
- BFDの設定
- リファレンス：BFDの詳細。

BFD の概要

BFDを有効化する際、BFDは3方向ハンドシェイクを使用し、あるエンドポイント（ファイアウォール）からリンクのエンドポイントにあるそのBFDピアへのセッションを確立します。制御パケットがハンドシェイクを行い、ピアが制御パケットを送受信できる最少間隔など、BFDプロファイルで設定されているパラメーターをネゴシエートします。IPv4およびIPv6用のBFD制御パケットは、UDPポート3784を介して送信されます。マルチホップをサポートするためのBFD制御パケットは、UDPポート4784を介して送信されます。いずれかのポートを介して送信されたBFD制御パケットは、UDPパケットにカプセル化されます。

BFD セッションが確立されると、BFD の Palo Alto Networks® 実装は非同期モードで動作し、両方のエンドポイントがネゴシエートされた間隔で互いに制御パケット (Hello パケットのように機能) を送信します。あるピアが検知時間（ネゴシエート済みの送信間隔に検知時間乗数を掛けた値）内に制御パケットを受信しない場合、そのピアはセッション切れと判断します。（ファイアウォールは、制御パケットを定期的に送信する代わりに必要なときのみ送信するデマンド モードをサポートしていません）

スタティックルート、およびファイアウォール間のBFDセッション用のBFDを有効化しており、さらにBFDピアが失敗した場合、ファイアウォールはRIBおよびFIBテーブルからその失敗したルートを削除し、優先度が低い別のパスを代わりに使用することを許可します。ルーティング プロトコル用のBFDを有効化する場合、BFDはそのルーティング 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。そのため、ファイアウォールおよびBFDピアが新しいパス上で再変換されます。

BFD プロファイルにより、BFDの設定を行い、それをファイアウォール上の単体あるいは複数のルーティング プロトコルやスタティックルートに割り当てることができます。プロファイルを設定せずにBFDを有効化した場合、ファイアウォールはデフォルトのBFDプロファイル（デフォルト設定をすべて）を使用します。このデフォルトのBFDプロファイルに変更を加えることはできません。

インターフェイスが異なるBFDプロファイルを使用する複数のプロトコルを実行している場合、BFDは**Desired Minimum Tx Interval** [目標の最低Tx間隔]が最も小さいプロファイルを使用します。動的ルーティング プロトコル用のBFDを参照してください。

アクティブ/パッシブHAピアはBFD設定およびセッションを同期しますが、アクティブ/アクティブHAピアはこれを行いません。

BFDは RFC 5880 で標準化されています。PAN-OSはRFC 5880のすべてのコンポーネントをサポートしているわけではありません（サポートされていないBFDのRFCコンポーネントを参照）。

PAN-OS は、RFC 5881, www.rfc-editor.org/rfc/rfc5881.txt もサポートしています。この場合、BFDはIPv4あるいはIPv6を使用する2つのシステム間のシングル ホップを追跡するため、2つのシステムは直接相互接続されることになります。また、BFDはBGPによって接続されているピアからの複数ホップも追跡します。PAN-OS は、 RFC 5883 , www.rfc-editor.org/rfc/rfc5883.txt で説明されているように BFD カプセル化に従います。ただし、PAN-OSは認証をサポートしていません。

- BFD モデル、インターフェイス、クライアント サポート
- サポートされていないBFDのRFCコンポーネント

- スタティックルート用のBFD
- 動的ルーティング プロトコル用のBFD

BFD モデル、インターフェイス、クライアント サポート

次のファイアウォール モデルは BFD をサポートしていません。PA-800 Series、PA-220、および VM-50 ファイアウォール。BFD をサポートする各モデルは、製品選択ツールにリストアップされているBFDセッションの最大数をサポートしています。

BFDは、物理イーサネット、集約イーサネット（AE）、VLAN、およびトンネル インターフェイス（サイト間VPNおよびLSVPN）、およびレイヤー3 サブインターフェイス上で稼働します。

サポートされているBFDクライアント：

- シングル ホップから成るスタティックルート（IPv4およびIPv6）
- OSPFv2およびOSPFv3（インターフェイス タイプにはブロードキャスト、ポイント トゥ ポイント、ポイント トゥ マルチポイントが含まれます）
- シングル ホップあるいはマルチ ホップから成るBGP IPv4 と IPv6（IBGP、EBGP）
- RIP（シングル ホップ）

サポートされていないBFDのRFCコンポーネント

- デマンド モード
- 認証
- Echoパケットの送受信（ただし、ファイアウォールはバーチャル ワイヤあるいはタップ インターフェイスに到達したEchoパケットを通過させます）。（BFD Echoパケットの送信元および宛先用のIPアドレスは同じです）
- ポール シーケンス
- ふくそう制御

スタティックルート用のBFD

スタティックルートでBFDを使用するには、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。**Next Hop** [ネクストホップ]のタイプが**IP Address** [IPアドレス]であるバアのみ、スタティックルートがBFDプロファイルを持つことができます。

ピアへのスタティックルートが複数設定されているインターフェイスの場合（BFDセッションの送信元IPアドレスと宛先IPアドレスは同じです）、単一のBFDセッションが自動的に複数のスタティックルートに対処します。この挙動により、BFDセッション数が削減されます。各スタティックルートが異なるBFDプロファイルを持っている場合、**Desired Minimum Tx Interval** [目標の最低Tx間隔]が最も小さいプロファイルが有効になります。

DHCPあるいはPPPoEクライアント インターフェイス上でスタティックルート用のBFDを設定したいデプロイ環境については、コミットを2度行う必要があります。スタティックルート用のBFDを有効化する場合、**Next Hop** [ネクストホップ]のタイプが**IP Address** [IPアドレス]でなければなりません。しかし、DHCPあるいはPPPoEインターフェイスをコミットする時点では、イ

ンターフェイスのIPアドレスおよびネクストホップのIPアドレス（デフォルトゲートウェイ）が分かっていません。

まずはそのインターフェイス用のDHCPあるいはPPPoEクライアントを有効化し、コミットを実行し、DHCPあるいはPPPoEサーバーがファイアウォールにクライアントのIPアドレスおよびデフォルトゲートウェイのIPアドレスを送信するまで待機する必要があります。その後、スタティックルート（ネクストホップとしてDHCPあるいはPPPoEクライアントのデフォルトゲートウェイ アドレスを使用）を設定し、BFDを有効化し、2度目のコミットを行います。

動的ルーティング プロトコル用のBFD

スタティックルート用のBFDに加え、ファイアウォールはBGP、OSPF、およびRIPルーティング プロトコル用のBFDをサポートしています。

Palo Alto Networks® マルチホップ BFD の実装は、マルチホップ パス の RFC 5883 、双方向転送検出(BFD)のカプセル化部分に従いますが、認証はサポートしていません。代替策として、BGP用のVPNトンネルにおけるBFDを設定できます。VPNトンネルでは、BFD認証が重複することなく認証を行えます。

OSPFv2あるいはOSPFv3ブロードキャスト インターフェイス用のBFDを有効化する際、OSPFはDR（宛先ルーター）およびBDR（バックアップ宛先ルーター）とのみBFDセッションを確立します。ポイント トゥ ポイント インターフェイス上でOSPFは直接のネイバーとBFDセッションを確立します。ポイント トゥ マルチポイント インターフェイス上でOSPFは各ピアとBFDセッションを確立します。

OSPFあるいはOSPFv3仮想リンク上のBFDはファイアウォールでサポートされていません。

各ルーティング プロトコルは、インターフェイス上で独立したBFDセッションを持つことができます。あるいは、2つ以上のルーティング プロトコル（BGP、OSPF、およびRIP）がいずれかのインターフェイス用の共通BFDセッションを共有することができます。

同じインターフェイス上で複数プロトコル用のBFDを有効化し、かつそのプロトコルの送信元IPアドレスおよび宛先IPアドレスが同じである場合、プロトコルは単一のBFDセッションを共有するため、データプレーンのオーバーヘッド（CPU）およびインターフェイス上のトラフィック負荷が削減されます。これらのプロトコルに対して異なるBFDプロファイルを設定する場合、**Desired Minimum Tx Interval**[目標の最低Tx間隔]が最も小さいBFDプロファイルが一つだけ使用されます。各プロファイルの**Desired Minimum Tx Interval** [目標の最低Tx間隔]が同じである場合、最初に生成されたセッションで使われたプロファイルが有効になります。スタティックルートおよびOSPFが同じセッションを共有するこのケースでは、静的セッションがコミットの直後に生成されるため、OSPFは隣接物が立ち上がるまで待機しますが、そのスタティックルートのプロファイルが有効になります。

こういったケースで単一のBFDセッションを使用することには、リソースを効率よく使えるというメリットがあります。ファイアウォールは保存済みのリソースを使用し、異なるインターフェイス上のBFDセッションをさらに多くサポートしたり、送信元IPおよび宛先IPアドレスのペアが異なる場合のBFDをサポートすることができます。

同じインターフェイス上のIPv4およびIPv6は同じBFDプロファイルを使用できますが、必ず異なるBFDセッションが生成されます。

HA パス モニタリングおよび *BGP* 用の *BFD* をどちらも実装する場合、*Palo Alto Networks* は、*BGP* グレースフル リスタートを実装することは推奨しません。*BFD* ピアのインターフェイスが失敗し、パス モニタリングが失敗すると、*BFD* はルーティングテーブルに与えられたルートを取り除き、グレースフル リスタートが有効になる前にこの変更をパッシブ *HA* ファイアウォールと同期する場合があります。*BGP* 用の *BFD*、*BGP* 用のグレースフル リスタート、および *HA* パス モニタリングを実装することにした場合、*BFD* の目標の最低 *Tx* 間隔、検知時間乗数をデフォルトの値よりも大きめに設定する必要があります。

BFDの設定

サポートされているファイアウォール モデルとインターフェースを含むBFD の概要を読み終えたら、 BFD を設定する前に以下の手順を実行します:

- 1 つまたは複数の virtual routers を設定します。
- BFDをスタティックルートに適用する場合は単体あるいは複数のスタティックルートを設定する。
- BFD をルーティング プロトコルに適用する場合は、ルーティング プロトコル (BGP 、OSPF、OSPFv3 、または RIP) を設定します。

*BFD*を効率よく実装できるかどうかは、トラフィック負荷、ネットワーク条件、どの程度積極的な*BFD*設定を行うか、データプレーンがどの程度ビジー状態になるかといった様々な要素に左右されます。

STEP 1 | BFDプロファイルを作成します。

既存の*BFD*セッションが使用している*BFD*プロファイルの設定を変更して変更をコミットする場合、ファイアウォールはその*BFD*セッションを検知して新しい設定のものを再生成する前に、ローカル状態が*admin down [*アドミン ダウン*]*に設定された*BFD*パケットを送信します。ピア デバイスがルーティング プロトコルあるいはスタティックルートをフラップするかどうかは、RFC 5882のセクション*3.2*のピアの実装に基づきます。

1. **Network (**ネットワーク**)** > **Network Profiles (**ネットワーク プロファイル**)** > **BFD Profile (BFD** プロファイル**)** を選択し、その BFD プロファイルの **Name (**名前**)** を **Add (**追加**)** します。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。
2. BFDの運転 **Mode (**モード**)** を選択します。
   - **Active**[アクティブ] - BFDがピアに対してコントロールパケットを送信開始します（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。

STEP 2 | BFD 間隔を設定します。

1. **Desired Minimum Tx Interval (ms)** [目標の最低Tx間隔（ミリ秒）]を入力します。これはBFDプロトコル（BFDと呼ぶ）にBFD制御パケットを送信させる最低間隔（ミリ秒）であり、これにより送信間隔についてピアとネゴシエートを行います。PA-7000、およ

び PA-5200 Series のファイアウォールでは最低 50、VM-Series ファイアウォールでは最低 200 です。最大は2,000で、デフォルトは1,000です。

推奨は、*PA-7000 Series* ファイアウォールの ***Desired Minimum Tx Interval*** *(*目標の最低 ***Tx*** 間隔*)* を *100* 以上に設定することです。 *100* 未満の値は *BFD* フラップを引き起こす危険性があります。

*1*つのインターフェイスにおいて複数のルーティング 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****[*目標の最低*Tx*間隔*]*を設定してください。

2. **Required Minimum Tx Interval (ms)** [必須の最低Tx間隔（ミリ秒）]を入力します。これは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（ミリ秒）です。PA-7000、および PA-5200 Series のファイアウォールでは最低 50、VM-Series ファイアウォールでは最低 200 です。最大は2,000で、デフォルトは1,000です。

   推奨は、*PA-7000 Series* ファイアウォールの ***Required Minimum Rx Interval*** *(*必須の最低 ***Tx*** 間隔*)* を *100* 以上に設定することです。 *100* 未満の値は *BFD* フラップを引き起こす危険性があります。

STEP 3 | BFD 検知時間乗数を設定します。

Detection Time Multiplier [検知時間乗数]を入力します。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。範囲は 2 ～ 50、デフォルトは 3 です。

例えば、送信間隔300 ms x 3（検知時間乗数） = 900 msの検知時間になります。

*BFD*プロファイルを設定する際、ファイアウォールが通常はネットワークの末端あるいはデータセンターに配置されるセッション ベースのデバイスであり、専用のルーターよりもリンクが遅いことを考慮してください。そのため、ファイアウォールでは設定できる最短のものよりも比較的長い間隔および大きい乗数が必要になるのが普通です。検知時間が短すぎると、トラフィックが多く混雑しているだけの場面で誤ってエラーを検出してしまうおそれがあります。

STEP 4 | BFD 待機時間を設定します。

Hold Time (ms) [待機時間（ミリ秒）] を入力します。これは、リンクが確立されてからBFD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。BFDが**Hold Time** [待機時間] 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 です。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、BFDは直ちにBFDコントロールパケットの送受信を行います。

STEP 5 | （任意—BGP IPv4を実装する場合のみ）BFDプロファイルのホップ関連の設定を行います。

1. **Multihop** [マルチホップ]を選択してBGPマルチホップを介したBFDを有効にします。
2. **Minimum Rx TTL** [最低Rx TTL]を入力します。これは、BGPがマルチホップBFDをサポートしている場合にBFDが受け入れる（受信する）BFD制御パケット内のTime-to-Live値（ホップ数）の最低値です。（範囲は1～254。デフォルト値はありません）

   設定済みの**Minimum Rx TTL (**最低 **Rx TTL)** よりも小さい TTL を受信すると、ファイアウォールはパケットをドロップします。例えば、5ホップ先にあるピアがTTLが100であるBFDパケットをファイアウォールに送信し、かつそのファイアウォールの**Minimum Rx TTL (**最低 **Rx TTL)** が96以上に設定されている場合、ファイアウォールはパケットをドロップします。

STEP 6 | BFD プロファイルを保存します。

OK をクリックします。

STEP 7 | （任意）スタティックルート用のBFDを有効にします。

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。

1. **Network (**ネットワーク**)** > **Virtual Routers (**仮想ルーター**)** の順に選択し、スタティックルートを設定した仮想ルーターを選択します。
2. **Static Routes** [スタティックルート]タブを選択します。
3. **IPv4** または **IPv6** タブを選択します。
4. BFDを適用するスタティックルートを選択します。
5. **Interface** [インターフェイス]を選択します（DHCPアドレスを使用している場合でも）。**Interface** [インターフェイス]設定は**None** [なし]以外です。
6. **Next Hop** [ネクストホップ]で**IP Address** [IPアドレス]を選択し、まだ指定していない場合はIPアドレスを入力します。
7. **BFD Profile**[BFDプロファイル]で、以下のいずれかを選択します。
   - **default** [デフォルト]—デフォルト設定のみを使用します。
   - 設定したBFD プロファイル—BFD プロファイルの作成を参照してください。
   - **New BFD Profile (**新規 **BFD** プロファイル**)**—BFD プロファイルを作成できます。

     None (Disable BFD) (なし（***BFD***無効）**)** を選択すると、このスタティックルートで*BFD*が無効になります。
8. **OK** をクリックします。

IPv4あるいは**IPv6**タブのBFD列は、スタティックルート用に設定されたBFDプロファイルを表示しています。

STEP 8 | （任意）すべてのBGPインターフェイスあるいは単体のBGPピア用のBFDを有効にします。

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、再収斂を行う可能性があります。*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。

HA パス モニタリングおよび *BGP* 用の *BFD* をどちらも実装する場合、*Palo Alto Networks* は、*BGP* グレースフル リスタートを実装することは推奨しません。*BFD* ピアのインターフェイスが失敗し、パス モニタリングが失敗すると、*BFD* はルーティングテーブルに与えられたルートを取り除き、グレースフル リスタートが有効になる前にこの変更をパッシブ *HA* ファイアウォールと同期する場合があります。*BGP* 用の *BFD*、*BGP* 用のグレースフル リスタート、および *HA* パス モニタリングを実装することにした場合、*BFD* の目標の最低 *Tx* 間隔、検知時間乗数をデフォルトの値よりも大きめに設定する必要があります。

1. **Network (**ネットワーク**)** > **Virtual Routers (**仮想ルーター**)** の順に選択し、BGPを設定した仮想ルーターを選択します。
2. **BGP** タブを選択します。
3. (任意) BFD を仮想ルーター上のすべての BGP インターフェイスに割り当てるには、**BFD** リストで次のいずれかを選択して **OK** をクリックします。
   - **default** [デフォルト]–デフォルト設定のみを使用します。
   - 設定したBFD プロファイル–BFD プロファイルの作成を参照してください。
   - **New BFD Profile (**新規 **BFD** プロファイル**)**–BFD プロファイルを作成できます。

   None (Disable BFD) (なし（***BFD***無効）***)*** を選択すると、すべての*BGP*インターフェイスで*BFD*を無効化されます。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。
4. （任意）単体のBGPピア インターフェイス用のBFDを有効化する（それにより、無効化されていない場合はBGP用の**BFD**設定がオーバーライドされます）場合は、次の作業を行います。
   1. **Peer Group (**ピア グループ**)** タブを選択します。
   2. ピア グループを選択します。
   3. ピアを選択します。
   4. **BFD** リストで次のいずれかを選択します。

      default [デフォルト]–デフォルト設定のみを使用します。

      Inherit-vr-global-setting [vrグローバル設定を継承]（デフォルト）–仮想ルーター用のBGPのためにグローバルに選択してあるBFDプロファイルをBGPピアが継承します。

設定したBFD プロファイル—BFD プロファイルの作成を参照してください。

***Disable BFD (BFD** 無効**)** を選択すると、*BGP*ピアの*BFD*が無効化されます。

5. **OK** をクリックします。
6. **OK** をクリックします。

BGP - Peer Group/Peer [BGP - ピア グループ/ピア]リストのBFD列は、そのインターフェイス用に設定されたBFDプロファイルを表示します。

STEP 9 | （任意）OSPFあるいはOSPFv3用のBFDをグローバルに有効化するか、OSPFインターフェイス用のBFDを有効化します。

1. **Network (**ネットワーク**)** > **Virtual Routers (**仮想ルーター**)** の順に選択し、OSPFあるいはOSPFv3を設定した仮想ルーターを選択します。
2. **OSPF** あるいは **OSPFv3** タブを選択します。
3. (任意) **BFD** リストで次のいずれかを選択し、すべての OSPF あるいは OSPFv3 インターフェイス用の BFD を有効化して **OK** をクリックします。
   - **default** [デフォルト]—デフォルト設定のみを使用します。
   - 設定したBFD プロファイル—BFD プロファイルの作成を参照してください。
   - **New BFD Profile (**新規 **BFD** プロファイル**)**—BFD プロファイルを作成できます。

   ***None (Disable BFD) (**なし（*BFD*無効）**)** を選択すると、すべての*OSPF*インターフェイスで*BFD*を無効化されます。単一の*OSPF*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。
4. （任意）単体のOSPFピア インターフェイスのBFDを有効化する（それにより、無効化されていない場合はOSPF用の**BFD**設定がオーバーライドされます）場合は、次の作業を行います。
   1. **Areas** [エリア]タブを選択し、エリアを一つ選択します。
   2. **Interface** [インターフェイス] タブでインターフェイスを一つ選択します。
   3. **BFD** リストで次のいずれかを選択し、指定した OSPF ピア用の BFD を設定します。

      default [デフォルト]—デフォルト設定のみを使用します。

      Inherit-vr-global-setting [vrグローバル設定を継承]（デフォルト）—仮想ルーター用のOSPFあるいはOSPFv3の**BFD**設定をOSPFピアが継承します。

      設定したBFD プロファイル—BFD プロファイルの作成を参照してください。

      ***None (Disable BFD)[**なし（*BFD*無効）*]* を選択すると、*OSPF*あるいは*OSPFv3*インターフェイス用の*BFD*が無効化されます。
   4. **OK** をクリックします。
5. **OK** をクリックします。

OSPF **Interface** [インターフェイス]タブのBFD列は、そのインターフェイス用に設定されたBFDプロファイルを表示します。

STEP 10 | （任意）RIP 用のBFDをグローバルに有効化するか、単体のRIPインターフェイス用のBFDを有効にします。

1. **Network (**ネットワーク**)** > **Virtual Routers (**仮想ルーター**)** の順に選択し、RIPを設定した仮想ルーターを選択します。
2. **RIP** タブを選択します。
3. (任意) **BFD** リストで次のいずれかを選択し、仮想ルーター上のすべての RIP インターフェイス用の BFD を有効化して **OK** をクリックします。
   - **default** [デフォルト]–デフォルト設定のみを使用します。
   - 設定したBFD プロファイル–BFD プロファイルの作成を参照してください。
   - **New BFD Profile (**新規 **BFD** プロファイル**)**–BFD プロファイルを作成できます。

   None (Disable BFD) (なし（***BFD***無効）**)** を選択すると、すべての*RIP*インターフェイスで*BFD*を無効化されます。単一の*RIP*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。
4. （任意）単体のRIPインターフェイスのBFDを有効化する（それにより、無効化されていない場合はRIP用の**BFD**設定がオーバーライドされます）場合は、次の作業を行います。
   1. **Interfaces** [インターフェイス]タブを選択し、インターフェイスを一つ選択します。
   2. **BFD** リストで次のいずれかを選択します。

      default [デフォルト]–デフォルト設定のみを使用します）。

      Inherit-vr-global-setting [vrグローバル設定を継承]（デフォルト）–仮想ルーター用のRIPのためにグローバルに選択してあるBFDプロファイルをRIPインターフェイスが継承します。

      設定したBFD プロファイル–BFD プロファイルの作成を参照してください。

      None (Disable BFD)[なし（*BFD*無効）*]* を選択すると、*RIP*インターフェイス用の*BFD*が無効化されます。
   3. **OK** をクリックします。
5. **OK** をクリックします。

Interface [インターフェイス]タブのBFD列は、そのインターフェイス用に設定されたBFDプロファイルを表示します。

STEP 11 | 設定をコミットします。

Commit（コミット）をクリックします。

STEP 12 | BFD のサマリーと詳細を確認します。

1. **Network (**ネットワーク**)** > **Virtual Routers (**仮想ルーター**)** を開き、詳細を確認したい仮想ルーターを探し、**More Runtime Stats (**ランタイム状態の詳細**)** をクリックします。
2. **BFD Summary Information (BFD** サマリー情報**)** タブを選択し、BFDの状態やランタイム統計といった概要を表示します。
3. （任意）任意のインターフェイスの行で **details (**詳細**)** を選択し、参照：BFDの詳細。

STEP 13 | ルーティング設定が参照しているBFDプロファイルを監視します（BFD統計、ステータス、状態を監視します）。

以下のCLI操作コマンドを使用します。

- show routing bfd active-profile [<name>]
- **show routing bfd details [interface** *<name>***][local-ip** *<ip>***][multihop] [peer-ip** *<ip>***][session-id][virtual-router** *<name>***]**
- show routing bfd drop-counters session-id <session-id>
- **show counter global | match bfd**

STEP 14 | （任意）BFD僧院、受信、およびドロップのカウンターをクリアします。

```
clear routing bfd counters session-id all | <1-1024>
```

STEP 15 | （任意）デバッグ用にBFDセッションをクリアします。

```
clear routing bfd session-state session-id all | <1-1024>
```


リファレンス：BFDの詳細

仮想ルーターのための次の BFD 情報を確認する方法は、BFDのサマリーと詳細を表示するのステップを参照してください。

名前	値（例）	説明
Session Id セッション ID	1	BFDセッションのID番号。
interface インターフェイス	Ethernet1/12	選択した、BFDが実行されているインターフェイス。
PROTOCOL	STATIC(IPV4) OSPF	インターフェイス上で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）かつ/または動的ルーティング プロトコル。
Local IP Address	10.55.55.2	インターフェイスの IP アドレス。
隣接 IP アドレス	10.55.55.1	BFD ネイバーの IP アドレス。
BFDプロファイル	デフォルト*（このBFDセッションには複数のBFDプロファイルがあります。有効なプロファイルは最も小さいDesired Minimum Tx Interval (ms) [目標の最低Tx間隔（ミリ秒）]を使用して選択されます）	インターフェイスに割り当てられたBFDプロファイルの名前。 サンプル インターフェイスには、異なるプロファイルを持つBFDを実行しているOSPFおよびスタティックルートの両方があるため、ファイアウォールは最も小さい **Desired Minimum Tx Interval (目標の最低Tx間隔)** を持つプロファイルを使用します。この例で使用するプロファイルは、デフォルトのプロファイルです。
状態（ローカル/リモート）	up/up	ローカルおよびリモートBFDピアのBFDの状態。状態にはadmin down、down、init、およびupがあります。
アップ タイム	2h 36m 21s 419ms	BFD のアップタイム（時間、分、秒、ミリ秒）。

名前	値（例）	説明
弁別子（ローカル/リモート）	1391591427/1	ローカルおよびリモートBFDピアの弁別子。
モード	アクティブ	インターフェイス上で設定されているBFDのモード。アクティブあるいはパッシブ。
デマンド モード	無効	PAN-OSはBFDデマンド モードをサポートしていないため、これは常にDisabled [無効]な状態になります。
マルチ ホップ	無効	BFDマルチホップ：有効あるいは無効。
マルチホップTTL		マルチホップのTTL。範囲は1～254。マルチホップが無効な場合は空欄になります。
ローカル診断コード	0（診断なし）	診断コードは、ローカルシステムの状態が前回変更された理由を示します。 0–診断なし 1–制御検知時間切れ 2–Echo機能失敗 3–ネイバーがセッション切れを報告 4–転送プレーン リセット 5–パス ダウン 6–連結パス ダウン 7–管理関連のダウン 8–反転連結パス ダウン
前回受信したリモート診断コード	0（診断なし）	BFDピアから前回受信した診断コード。
送信待機時間	0 ms	リンクが確立されてからBFD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（ミリ秒単位）。待機時間が0msの場合、転送が即座に行われます。範囲は 0 ～ 120000ms です。
受信した最小Rx間隔	1000ms	ピアから受信した最小Rx間隔（BFDピアが制御パケットを受信できる間隔）。最低2000msです。

名前	値（例）	説明
ネゴシエート済みの送信間隔	1000ms	BFDピアがお互いにBFD制御パケットを送信することに関して同意した送信間隔（ミリ秒）。最低2000msです。
受信した乗数	3	BFDピアから受信した検知時間乗数の値。送信時間にこの乗数を掛けたものが検知時間になります。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 です。
検知時間（超過）	3000ms (0)	算出された検知時間（ネゴシエート済みの送信間隔に乗数を掛けたもの）、および検知時間が超過したミリ秒数。
Tx制御パケット（前回）	9383（420ms前）	送信されたBFD制御パケット数（およびBFDが最後の制御パケットを送信してからの時間）。
Rx制御パケット（前回）	9384（407ms前）	受信したBFD制御パケット数（およびBFDが最後の制御パケットを受信してからの時間）。
エージェント データプレーン	スロット1 - DP 0	PA-7000 Seriesファイアウォールでは、このBFDセッション用のパケットを処理するために割り当てられたデータプレーンのCPU。
エラー	0	BFD エラーの数。
状態変更の原因となった最後のパケット		
Version（バージョン）	1	BFDバージョン。
ポールビット	0	BFDポールビット。0は未設定であることを示します。
目標の最小 Tx 間隔	1000ms	状態変更の原因となった最後のパケットの目標最低送信間隔。
必須の最小Rx間隔	1000ms	状態変更の原因となった最後のパケットの必須の最低受信間隔。
検知乗数	3	状態変更の原因となった最後のパケットの検知乗数。

名前	値（例）	説明
マイ弁別子	1	リモート弁別子。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。
ユア弁別子	1391591427	ローカル弁別子。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。
診断コード	0（診断なし）	状態変更の原因となった最後のパケットの診断コード。
長さ	24	BFD制御パケットの長さ（バイト）。
デマンド ビット	0	PAN-OSはBFDデマンド モードをサポートしていないため、デマンド ビットは常に0（無効）になります。
最終ビット	0	PAN-OSはポール シーケンスをサポートしていないため、最終ビットは常に0（無効）になります。
マルチポイント ビット	0	このビットは、今後ポイント トゥ マルチポイントをBFDに拡張するために予約されています。これは送受信の両方が0でなければなりません。
制御プレーン独立ビット	1	• 1に設定されている場合、送信システムのBFD実装はその制御プレーンと結果を共有しません（つまり、BFDは転送プレーンに実装され、制御プレーンがダウンしても機能し続けることができます）。PAN-OSでは、このビットは常に1です。 • 0に設定されている場合、送信システムのBFD実装はその制御プレーンと結果を共有します。
認証プレゼント ビット	0	PAN-OSはBFD認証をサポートしていないため、プレゼント ビットは常に0になります。
必須の最小Echo Rx間隔	0 ms	PAN-OSはBFD Echo機能をサポートしていないため、これは常に0msになります。

セッション設定とセッション タイムアウト

このセクションでは、TCP、UDP、ICMPv6 セッション、および IPv6、NAT64、NAT オーバーサブスクリプション、ジャンボ フレーム サイズ、MTU、セッション保持時間短縮、キャプティブ ポータル認証に影響するグローバル設定について説明します。また、新しく設定されたセキュリティ ポリシーをすでに進行中のセッションに適用できるようにする設定（Rematch Sessions （セッションの再マッチング））もあります。

以下の最初のいくつかのトピックでは、OSI モデル、TCP、UDP、および ICMP のトランスポート層の概要について説明します。プロトコルの詳細は、それぞれの RFC を参照してください。残りのトピックでは、セッションのタイムアウトおよび設定について説明します。

トランスポート層のセッション

ネットワーク セッションとは、複数の通信デバイス間で発生し、一定期間継続するメッセージの交換です。確立されたセッションは、セッションが終了すると削除されます。OSI モデルの 3 つの層（トランスポート層、セッション層、アプリケーション層）では、異なるタイプのセッションが発生します。

トランスポート層は、OSI モデルのレイヤー 4 で動作し、信頼性の高いまたは信頼性の低い、エンドツーエンドのデータ配信およびデータ フロー制御を提供します。トランスポート層でセッションを実装するインターネット プロトコルには、Transmission Control Protocol （TCP）や User Datagram Protocol （UDP）などがあります。

TCP

Transmission Control Protocol （TCP）（RFC 793）は、Internet Protocol （IP）スイートの主要プロトコルの 1 つです。このプロトコルは広く普及しており、IP と一緒に ***TCP/IP*** と呼ばれることが一般的です。TCP は、セグメントの送受信中にエラーをチェックして、受信したセグメントの肯定応答を行い、誤った順序で到着するセグメントの順序を並べ替えることができるため、信頼性の高いトランスポート プロトコルだと考えられています。また、TCP では、ドロップされたセグメントの再送信を要求および提供できます。TCP はステートフルな接続指向プロトコルです。つまり、セッションの期間中に送信者と受信者間の接続が確立されます。TCP では、パケットのフロー制御が行われるため、ネットワークの輻輳を処理できます。

TCP では、セッションのセットアップ時にハンドシェークが実行され、セッションの開始および確認応答が行われます。データの転送後、セッションは正しい手順（各側で FIN パケットを送信し、ACK パケットで肯定応答する）で終了します。通常、TCP セッションを開始するハンドシェークは、イニシエータとリスナー間の 3 ウェイ ハンドシェーク（3 つのメッセージの交換）になります。あるいは、4 ウェイまたは 5 ウェイ スプリット ハンドシェークや同時オープンなどのバリエーションもあります。TCP スプリット ハンドシェーク セッションの確立の防止を行う方法については、「TCP スプリット ハンドシェークのドロップ」を参照してください。

TCP をトランスポート プロトコルとして使用するアプリケーションには、Hypertext Transfer Protocol （HTTP）、HTTP Secure （HTTPS）、File Transfer Protocol （FTP）、Simple Mail Transfer Protocol （SMTP）、Telnet、Post Office Protocol version （POP3）、Internet Message Access Protocol （IMAP）、Secure Shell （SSH）などがあります。

以下のトピックでは、PAN-OS の TCP の実装の詳細ついて説明します。

- TCP Half Closed および TCP Time Wait タイマー
- Unverified RST タイマー
- TCP スプリット ハンドシェークのドロップ
- 最大セグメント サイズ (MSS：Maximum Segment Size)

パケットベースの攻撃保護 を設定し、望ましくない特性を持つ IP、TCP、および IPv6 パケットをドロップしたり、パケットから望ましくないオプションを取り除いてからゾーンに入ることができます。また、フラッド防御を設定し、アラームを発生させ、ファイアウォールが SYN パケットをランダムにドロップするか SYN Cookie を使用するようトリガーし、最大レートを超える SYN パケットをファイアウォールにドロップさせ始める SYN の 1 秒あたりの接続数（既存のセッションにマッチしないもの）を指定します。

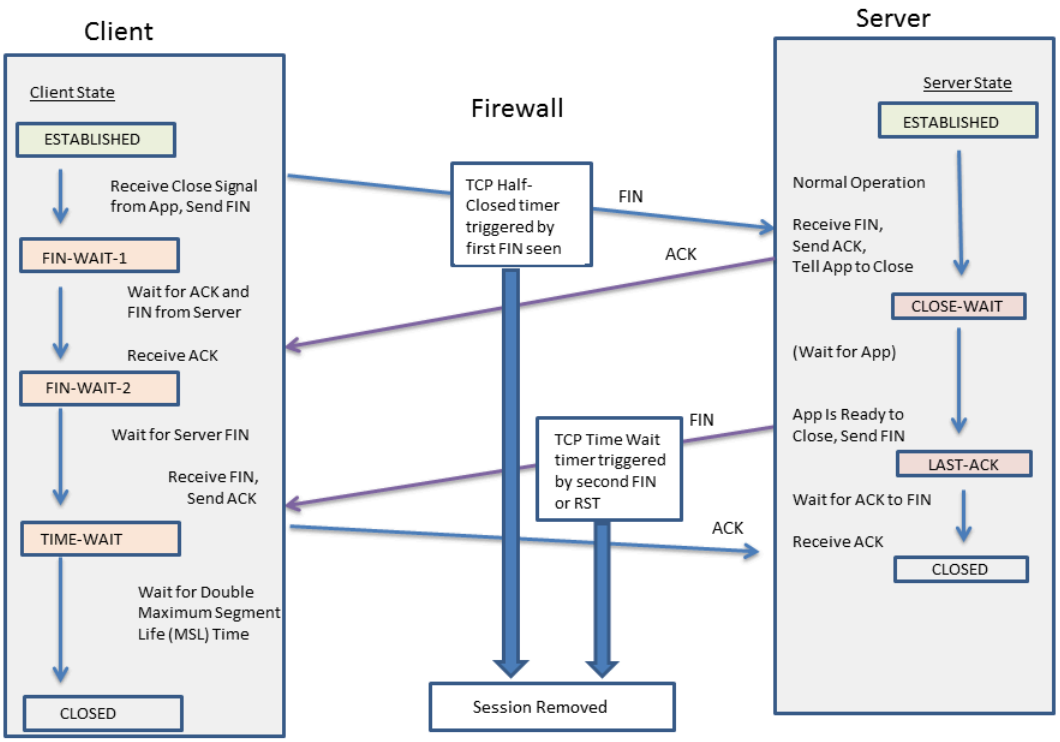
TCP Half Closed および TCP Time Wait タイマー

TCP 接続の終了手順では、TCP Half Closed タイマーが使用されます。このタイマーは、セッション中にファイアウォールで最初に確認される FIN によってトリガーされます。接続の一方でのみ FIN が送信されているため、このタイマーは TCP Half Closed という名前になっています。2 番目のタイマー TCP Time Wait は、2 番目の FIN または RST でトリガーされます。

最初の FIN で 1 つのタイマーのみがトリガーされるファイアウォールの場合、設定が短すぎると、half-closed セッションの終了が早くなりすぎる可能性があります。反対に、設定が長すぎ

ると、セッション テーブルが大きくなりすぎて、すべてのセッションを使い果たしてしまう可能性があります。タイマーが 2 つあることで、比較的長い TCP Half Closed タイマーと短い TCP Time Wait タイマーを設定できます。これにより、完全に終了したセッションの保持時間短縮を迅速に行い、セッション テーブルのサイズを制御できます。

以下の図は、TCP 接続の終了手順でファイアウォールの 2 つのタイマーがトリガーされるときの様子を示しています。



TCP Time Wait タイマーには、TCP Half Closed タイマーよりも小さい値を設定する必要があります。この理由は以下のとおりです。

- 最初の FIN が確認されてからの許容時間が長いほど、接続の反対側でセッションを完全に終了できる時間を確保できます。
- Time Wait 時間が短いのは、2 番目の FIN または RST が確認されてから長時間セッションを開いたままにしておく必要がないためです。Time Wait 時間を短くすればそれだけ早くリソースを解放できます。ただし、ファイアウォールで最後の ACK を確認する時間と、他のデータグラムの再送信のための時間は確保しておきます。

TCP Time Wait タイマーに TCP Half Closed タイマーよりも大きな値を設定しても、コミットは受け入れられます。ただし、実際には TCP Time Wait タイマーは TCP Half Closed の値を超えることはありません。

タイマーは、グローバルまたはアプリケーション単位で設定できます。デフォルトでは、すべてのアプリケーションを対象にグローバル設定が使用されます。アプリケーション レベルで TCP Time Wait タイマーを設定すると、グローバル設定がオーバーライドされます。

Unverified RST タイマー

（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、非対称パスから送信されていることが原因で）検証できない Reset （RST）パケットをファイアウォールで受信する場合、Unverified RST タイマーでセッション保持時間を制御します。デフォルトは 30 秒で、範囲は 1 ～ 600 秒です。Unverified RST タイマーには、以下の 2 番目の箇条書きで説明されている追加のセキュリティ対策があります。

RST パケットの結果は、以下の 3 つのいずれかになります。

- TCP ウィンドウ外の RST パケットはドロップされます。
- TCP ウィンドウ内にあるが、期待されるシーケンス番号がない RST パケットは、検証されず、Unverified RST タイマー設定が適用されます。この動作により、ランダムな RST パケットをファイアウォールに送信して、既存のセッションを中断させようとするサービス拒否（DoS）攻撃を回避できます。
- TCP ウィンドウ内あり、期待されるシーケンス番号がある RST パケットは、TCP Time Wait タイマー設定が適用されます。

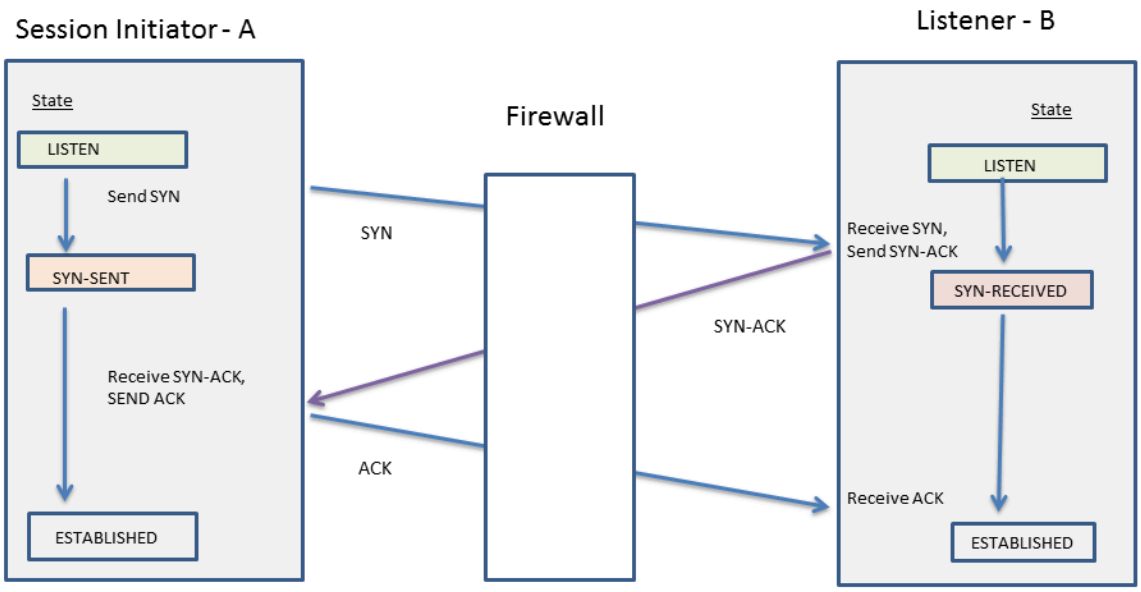
TCP スプリット ハンドシェークのドロップ

ゾーン プロテクション プロファイルの **Split Handshake (**スプリット ハンドシェイク**)** オプションでは、セッション確立手順で一般的な 3 ウェイ ハンドシェークではなく、4 ウェイまたは 5 ウェイ スプリット ハンドシェークや同時オープンなどのバリエーションが使用される場合に、TCP セッションが確立されないようにすることができます。

Palo Alto Networks® 次世代ファイアウォールは、**Split Handshake** オプションを有効にすることなく、スプリット ハンドシェイクと同時オープン セッション確立のためのセッションとすべてのレイヤ 7 プロセスを正しく処理します。それでも、**Split Handshake (**スプリット ハンドシェイク**)** オプション（TCP スプリット ハンドシェークがドロップされる）を使用できるようにします。**Split Handshake (**スプリット ハンドシェイク**)** オプションをゾーン プロテクション プロファイルに対して設定し、そのプロファイルをゾーンに適用するときは、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。

Split Handshake (スプリット ハンドシェイク**)** オプションはデフォルトで無効になっています。

以下に、イニシエータ（通常はクライアント）とリスナー（通常はサーバー）間に PAN-OS ファイアウォールがある状態で TCP セッションを確立するために使用される標準的な 3 ウェイ ハンドシェークを示します。



Split Handshake [スプリット ハンドシェイク]オプションは、ゾーンに割り当てられているゾーン プロテクション プロファイルに対して設定されます。ゾーンのメンバーであるインターフェイスは、サーバーから送信される同期（SYN）パケットをドロップします。これにより、ハンドシェークの以下のバリエーションを防止します。図中の文字 A はセッション イニシエータ、B はリスナーを示します。ハンドシェークの番号付きの各セグメントには、送信者から受信者へのセグメントの方向を示す矢印があります。各セグメントは制御ビットの設定を示します。

4-Way Split Handshake (Version 1)	4-Way Split Handshake (Version 2)	Simultaneous Open	5-Way Split Handshake
1. A → B SYN 2. A ← B ACK 3. A ← B SYN 4. A → B ACK	1. A → B SYN 2. A ← B SYN 3. A → B SYN-ACK 4. A ← B ACK	1. A → B SYN 2. A ← B SYN 3. A → B SYN-ACK 4. A ← B SYN-ACK	1. A → B SYN 2. A ← B ACK 3. A ← B SYN 4. A → B SYN-ACK 5. A ← B ACK

TCP スプリット ハンドシェーク セッションの確立の防止を行えます。

最大セグメント サイズ (MSS：Maximum Segment Size)

最大送信単位（MTU：maximum transmission unit）とは、単一のTCPパケットで送信できる最大バイト数を表す値のことです。MTUにはヘッダーの長さも含まれるため、MTUからヘッダーのバイト数を引いたものが最大セグメント サイズ（MSS）になり、これは単一のパケットで送信できる最大データ バイト数を示します。

MSS調整サイズ（以下を参照）を設定すれば、デフォルト設定で許可されているものよりも長いヘッダーをファイアウォールに許可させることができます。カプセル化によりヘッダーが延

長されるので、例えばMPLSヘッダーやVLANタグを持つトンネルトラフィックに対応できるよう、MSS調整サイズをそれらよりも大きく設定することになるでしょう。

パケットにDF（フラグメント化なし）ビットが設定されている場合、長いヘッダーのパケットが許可されているMTUを超える長さにならないようにする上で、特にMSS調整サイズを大きくしてMSSを小さくすることが役立ちます。DFビットが設定されており、MTUが超過した場合、より大きいパケットがドロップされます。

パケットに*DF*ビットが設定されている場合でも、出力インターフェイスの*MTU*を超える*IPv4*パケットをフラグメントを行う様、ファイアウォールの基本(グローバル)動作を構成できます。*CLI* コマンド ***debug dataplane set ip4-df-ignore yes*** を使用して、レイヤー *3* 物理インターフェースと *IPSec* トンネル インターフェースに対してこれを有効にします。*CLI* コマンド ***debug dataplane set ipv4-df-ignore no*** を使用して、ファイアウォールをデフォルトの動作に戻します。

ファイアウォールは、次のレイヤー3インターフェイス タイプにおけるIPv4およびIPv6アドレスに対して設定可能なMSS調整サイズをサポートしています。イーサネット、サブインターフェイス、集約イーサネット（AE）、VLAN、およびループバック。IPv6 MSS調整サイズは、インターフェイスでIPv6が有効になっている場合のみ適用されます。

*IPv4*および*IPv6*がインターフェイス上で有効になっており、*MSS*調整サイズが*2*つの*IP*アドレスフォーマット間で異なる場合、*TCP*トラフィックに対して*IP*タイプに対応する適切な*MSS*値が使用されます。

IPv4およびIPv6アドレスについては、ファイアウォールはlarger-than-expected（予想よりも大きい）TCPヘッダー長に対応します。ヘッダー長が予定よりも長いTCPパケットに対しては、ファイアウォールは次の2つの値のうちいずれか大きい方をMSS調整サイズとして選択します。

- 設定済みのMSS調整サイズ
- TCPヘッダー長（20） + TCP SYN内のIPヘッダーの長さの合計値

このように動作するため、ファイアウォールは必要に応じて設定済みのMSS調整サイズをオーバーライドすることになります。例えば、MSS調整サイズを42に設定した場合、MSSは1458に等しい（デフォルトのMTUサイズ引く調整サイズ[1500 - 42]）と予想しています。しかし、TCPパケットのヘッダーには4バイトのIPオプションが追加されているため、MSS調整サイズは44（20+20+4）になり、設定済みのMSS調整サイズ（42）より大きくなってしまいます。最終的なMSSは1500-44=1456バイトであり、予想よりも小さくなっています。

MSSサイズを調整する場合は、Configure Session Settings（セッション設定）項目を参照してください。

UDP

User Datagram Protocol （UDP）（RFC 768）は、IP スイートの別の主要プロトコルで、TCP の代替手段です。セッションをセットアップするためのハンドシェークや、送信者と受信者間の接続がないという点で、UDP はステートレスなコネクションレス型プロトコルです。各パケットは異なるルートを経由して 1 つの宛先に到達する場合があります。UDP は、データグラムの応答確認、エラーチェック、再送信、並べ替えを行わないため、信頼性の低いプロトコルだと考えられています。UDP では、これらの機能を提供するために必要な負担がなくなるため、遅延が減少し、TCP よりも高速になります。UDP は、データが宛先に到達するためのメカニズムや保証がないため、ベストエフォート プロトコルと呼ばれます。

UDP データグラムは IP パケット内にカプセル化されています。UDP では、チェックサムを使用してデータの整合性が確保されますが、ネットワーク インターフェイス レベルでエラー チェックは実行されません。エラー チェックは、UDP 自体ではなくアプリケーションで実行されるか、不要であるということを前提としています。UDP には、パケットのフロー制御を処理するメカニズムがありません。

UDP は、Voice over IP （VoIP）、ストリーミング オーディオおよびビデオ、オンライン ゲームなど、時間的制約のある高速なリアルタイム配信を必要とするアプリケーションで主に使用されます。UDP は、トランザクション指向のプロトコルであるため、Domain Name System （DNS）や Trivial File Transfer Protocol （TFTP）など、多数のクライアントからの小さなクエリに応答するアプリケーションでも使用されます。

ファイアウォールのゾーン保護プロファイルを使用して フラッド保護 を設定し、アラームをトリガーし、ファイアウォールをトリガーして UDP パケットをランダムにドロップし、最大レートを超える UDP パケットをドロップする 1 秒あたりの UDP 接続の速度を指定できます(既存のセッションには一致しません)。（UDP はコネクションレスですが、ファイアウォールはセッションベースで IP パケット内の UDP データグラムを追跡するため、UDP パケットが既存のセッションとマッチしない場合は新しいセッションとみなされ、接続がカウントされてしきい値に加味されます）

ICMP

Internet Control Message Protocol （ICMP）（RFC 792）も Internet Protocol スイートの主要プロトコルの 1 つで、OSI モデルのネットワーク層で動作します。ICMP は、診断および制御のために使用され、IP 操作に関するエラー メッセージや、ホストまたはルーターの要求されたサービスや到達可能性に関するメッセージを送信します。traceroute や ping などのネットワーク ユーティリティは、さまざまな ICMP メッセージを使用して実装されます。

ICMP は、実際のセッションを開いたり、管理したりしないコネクションレス型プロトコルです。ただし、2 つのデバイス間の ICMP メッセージをセッションとして考えることもできます。

Palo Alto Networks® ファイアウォールは ICMPv4 および ICMPv6 をサポートしています。ICMPv4 および ICMPv6 パケットを制御する方法はいくつかあります。

- ICMP および ICMPv6 パケットに基づくセキュリティポリシールール を作成し、ルール内の **icmp** あるいは **ipv6-icmp** アプリケーションを選択します。
- セッション設定の指定 を行う際に ICMPv6 レート制限 を制御します。
- Flood Protection を設定し、アラームをトリガーし、ファイアウォールをトリガーして ICMP または ICMPv6 パケットをランダムにドロップし、最大レートを超える ICMP パケットまたは ICMPv6 パケットをドロップする ICMP または ICMPv6 接続の速度を指定します (既存のセッションに一致しません)。
- Packet-Based Attack Protection パケットベースの攻撃保護を設定します。
  - ICMP の場合、特定のタイプのパケットをドロップするか、特定のパケットの送信を抑制することができます。
  - ICMPv6 パケット（タイプ 1、2、3、4、および 137）の場合、ICMPv6 パケットが許可されているかどうかを判断するために、ファイアウォールが ICMP セッション キーを使用してセキュリティポリシー ルールをマッチさせるかどうかを指定できます。（ファイアウォールはセキュリティポリシー ルールを使用し、埋め込まれたパケットを使用するデフォルトの動作をオーバーライドすることで、セッション マッチを判断します） ファイアウォールがセキュリティポリシー ルールにマッチする ICMPv6 パケットをドロップする際、ファイアウォールはトラフィックログに詳細を記録します。

ICMP および ICMPv6 パケットに基づくセキュリティポリシールール

ファイアウォールは、セキュリティポリシー ルールがセッションを許可する場合のみ、ICMP あるいは ICMPv6 を転送します（ファイアウォールが他のパケット タイプに対して行うのと同様）。ファイアウォールは、パケットが ICMP あるいは ICMPv6 エラー パケットのどちらであるかに基づいて、2 つのうちのいずれかの方向でセッション マッチを判断するか、ICMP あるいは ICMPv6 情報パケットとは反対にパケットをリダイレクトします。

- **ICMP** タイプ **3**、**5**、**11**、および **12** および **ICMPv6** タイプ **1**、**2**、**3**、**4**、および **137**—ファイアウォールはデフォルトで、エラーを発生させた元のデータグラムから情報の埋め込まれた IP パケット バイトを探します（invoking packet）。埋め込まれたパケットが既存のセッションにマッチする場合、ファイアウォールは、その同じセッションにマッチするセキュリティポリシー ルールで指定されているアクションに従って ICMP あるいは ICMPv6 パケットを転

送あるいはドロップします。(Packet-Based Attack Protection を使用して、ICMPv6 タイプのこのデフォルトの動作を上書きすることができます。

- 残りの **ICMP** あるいは **ICMPv6** パケット タイプ—ファイアウォールは ICMP あるいは ICMPv6 パケットを、それらが新規セッションに属しているかのように扱います。セキュリティポリシー ルールがパケット（ファイアウォールが **icmp** あるいは **ipv6-icmp** セッションとして認識するもの）にマッチする場合、ファイアウォールはセキュリティポリシー ルールのアクションに基づいてそのパケットを転送あるいはドロップします。セキュリティポリシー カウンターおよびトラフィックログがアクションを反映します。

  パケットにマッチするセキュリティポリシー ルールがない場合、ファイアウォールは、ゾーン内トラフィックを許可してゾーン間トラフィックをブロックするデフォルトのセキュリティポリシールールを適用します（これらのルールでは、ロギングがデフォルトで無効になっています）。

  デフォルトルールをオーバーライドしてロギングを有効化したり、デフォルトのアクションを変更したりできますが、デフォルトルールが関与するトラフィックがすべて影響を受けるため、デフォルトの動作を変更することが推奨されない特定のケースもあります。代わりに、*ICMP* あるいは *ICMPv6* パケットを明示的に制御およびロギングするセキュリティポリシールールを作成してください。

  エラーあるいはリダイレクト パケットではない ICMP あるいは ICMPv6 パケットを扱う明示的なセキュリティポリシールールを作成する方法は、次の 2 つです。

  - すべての **ICMP** あるいは **ICMPv6** パケットを許可（あるいは拒否）するセキュリティポリシー ルールを作成—このセキュリティポリシー ルールでアプリケーション **icmp** あるいは **ipv6-icmp** を指定します。ファイアウォールは、ICMP プロトコル番号（1）あるいは ICMPv6 プロトコル番号（58）のそれぞれにファイアウォールを通してマッチする IP パケットをすべて許可（あるいは拒否）します。
  - アプリケーションを出入りするパケットを許可（あるいは拒否）するセキュリティポリシー ルールおよびカスタム アプリケーションを作成—このより詳細なアプローチにより、特定の ICMP あるいは ICMPv6 タイプおよびコードの制御 を行えるようになります。

ICMPv6 レート制限

ICMPv6 レート制限は、フラッド攻撃や DDoS 攻撃を回避するためのスロットリング メカニズムです。この実装では、エラー パケット速度とトークン バケットが使用されます。これらが連携することで、スロットリングが有効になり、ファイアウォールによって保護されているネットワーク セグメントに ICMP パケットが大量に送信されることを回避できます。

まず、グローバル **ICMPv6 Error Packet Rate (per sec) (ICMPv6** エラー パケット速度（毎秒）**)**を使用して、ファイアウォールで許可される ICMPv6 エラー パケット速度を制御します。デフォルトは 100 パケット/秒で、範囲は 10 ～ 65535 パケット/秒です。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、以下のように、トークン バケットが始動して、スロットリングが発生します。

論理トークン バケットの概念で、ICMP メッセージを送信できる速度を制御します。バケットのトークン数は設定可能で、各トークンは、送信できる ICMPv6 メッセージを表しています。トークン数は ICMPv6 メッセージが送信されるたびに減少し、バケットのトークンがゼロになると、別のトークンがバケットに追加されるまで ICMPv6 メッセージを送信できなくなります。トーク

ン バケットのデフォルト サイズは 100 トークン（パケット）で、範囲は 10 ～ 65535 トークンです。

デフォルトのトークン バケット サイズまたはエラー パケット速度を変更する方法については、「 セッション設定の指定」セクションを参照してください。

特定の ICMP あるいは ICMPv6 タイプおよびコードの制御

このタスクを実行してカスタム ICMP あるいは ICMPv6 アプリケーションを作成し、次にそのアプリケーションを許可あるいは拒否するセキュリティポリシー ルールを作成します。

STEP 1 | ICMP あるいは ICMPv6 メッセージ タイプおよびコード用のカスタム アプリケーションを作成します。

1. **Object (オブジェクト)** > **Applications (アプリケーション)** を選択してカスタム アプリケーションを **Add (追加)** します。
2. **Configuration (構成)** タブでカスタム アプリケーションの **Name (名前)** および **Description (説明)** を入力します。例えば、ping6 という名前を入力します。
3. **Category (カテゴリ)** については **networking (ネットワーキング)** を選択します。
4. **Subcategory (サブカテゴリ)** については **ip-protocol (IP プロトコル)** を選択します。
5. **Technology (テクノロジー)** については **network-protocol (ネットワーク プロトコル)** を選択します。
6. **OK** をクリックします。
7. **Advanced (詳細)** タブで **ICMP Type (ICMP タイプ)** あるいは **ICMPv6 Type (ICMPv6 タイプ)** を選択します。
8. **Type (タイプ)** については、許可あるいは拒否したい ICMP あるいは ICMPv6 メッセージのタイプを表す数値（範囲は 0～255）を入力します。例えば、エコーリクエストのメッセージ（ping）は 128 です。
9. Type (タイプ) にコードが含まれる場合、許可あるいは拒否したい **Type (タイプ)** の値に適用される **Code (コード)** 番号（範囲は 0～255）を入力します。**Type (タイプ)** の値が Code 0 のみのものもあります。
10. **OK** をクリックします。

STEP 2 | 作成したカスタム アプリケーションを許可あるいは拒否するセキュリティポリシー ルールを作成します。

セキュリティ ポリシー ルールを作成します。**Application (アプリケーション)** タブで、先ほど作成したカスタム アプリケーションの名前を指定します。

STEP 3 | 変更をコミットします。

Commit（コミット）をクリックします。

セッション タイムアウトの設定

セッション タイムアウトには、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。特に TCP、UDP、および ICMP 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、デフォルトのタイムアウトが適用されます。タイムアウトはグローバルです。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。

ファイアウォールがキャッシュに ARP エントリ（IP アドレスとハードウェア アドレスのマッピング）を保持する期間を制御するグローバル ARP キャッシュ タイムアウト設定を構成することもできます。

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定義できます。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 または UDP セッション タイムアウトがオーバーライドされます。

アプリケーション レベルで *TCP* または *UDP* タイマーを変更すると、事前定義されたアプリケーションと共有カスタム アプリケーションのタイマーは、すべての仮想システム全体で実装されます。仮想システムでアプリケーションの複数のタイマーをそれぞれ違うものにする必要がある場合は、カスタム アプリケーションを作成し、固有のタイマーを割り当てて、独自の仮想システムにカスタム アプリケーションを割り当てる必要があります。

TCP、UDP、ICMP、キャプティブ ポータル認証、または他のタイプのセッションのグローバル セッション タイムアウト設定のデフォルト値を変更する必要がある場合、以下のタスクを実行します。すべての値は秒単位です。

デフォルトは、最適値です。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。

STEP 1 | セッションのタイムアウトにアクセスします。

Device (デバイス) > **Setup (セットアップ)** > **Session (セッション)** を選択して Session Timeouts (セッション タイムアウト) を編集します。

STEP 2 | （任意）その他のタイムアウトを変更します。

- **Default (デフォルト)** – TCP / UDP 以外、または ICMP 以外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時間（範囲は 1 ～ 15,999,999、デフォルトは 30）。
- **Discard Default (デフォルトの破棄)** – ファイアウォールに設定されたセキュリティ ポリシーに基づいて PAN-OS でセッションが拒否されてから、TCP / UDP 以外のセッションが開いた状態を維持する最大時間（範囲は 1 ～ 15,999,999、デフォルトは 60）。
- **Scan**（スキャン）– 非アクティブだと判断されてから、セッションが開いた状態を維持する最大時間。アプリケーションは、そのアプリケーションに定義されたアプリケーション トリクルしきい値を超えたときに非アクティブと見なされます（範囲は 5 ～ 30、デフォルトは 10）。
- 認証ポータル –キャプティブ ポータル Web フォームの認証セッション タイムアウト。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（範囲は 1 ～ 15,999,999、デフォルトは 30）。
- アイドル タイマー、ユーザーの再認証が必要になるまでの有効期限など、その他の認証ポータル タイムアウトを定義するには、**Device (デバイス)** > **User Identification (ユーザー ID)** > **Authentication Portal Settings (認証ポータル設定)** を選択します。Configure Authentication Portal (認証ポータルの設定)を参照してください。

STEP 3 | （任意）TCP タイムアウトを変更します。

- **TCP** の破棄 – ファイアウォールに設定されたセキュリティ ポリシーに基づいて TCP セッションが拒否されてから、TCP セッションが開いた状態を維持する最大時間。範囲は 1 から 15,999,999 です。デフォルトは 90 です。
- **TCP** – TCP セッションが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が送信されてから）応答なしで開いた状態を維持する最大時間。範囲は 1 ～ 15,999,999、デフォルトは 3,600 です。
- **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に許可された最大時間。範囲は 1 から 60 です。デフォルトは 10 です。
- **TCP init** – SYN を受信してから、TCP ハンドシェーク タイマーの開始前に SYN-ACK を送信するまでに許可された最大時間。範囲は 1 から 60 です。デフォルトは 5 です。
- **TCP Half Closed** – 最初の FIN を受信してから、2 つ目の FIN または RST を受信するまでの最大時間。範囲は 1 から 604,800 です。デフォルトは 120 です。
- **TCP Time Wait** – 2 つ目の FIN または RST を受信してからの最大時間。範囲は 1 から 600 です。デフォルトは 15 です。
- **Unverified 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時間。範囲は 1 から 600 です。デフォルトは 30 です。
- （任意）その他のタイムアウトを変更セクションの **Scan (スキャン)** のタイムアウトも参照してください。

STEP 4 | （任意）UDP タイムアウトを変更します。

- **UDP** の破棄 – ファイアウォールに設定されたセキュリティ ポリシーに基づいて UDP セッションが拒否されてから、UDP セッションが開いた状態を維持する最大時間。範囲は 1 から 15,999,999 です。デフォルトは 60 です。
- **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時間。範囲は 1 から 15,999,999 です。デフォルトは 30 です。
- （任意）その他のタイムアウトを変更セクションの **Scan (**スキャン**)** のタイムアウトも参照してください。

STEP 5 | （任意）ICMP タイムアウトを変更します。

- **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。範囲は 1 から 15,999,999 です。デフォルトは 6 です。
- 「(任意) その他のタイムアウトを変更する」セクションの **Discard Default (**デフォルトの破棄**)** および **Scan (**スキャン**)** のタイムアウトも参照してください。

STEP 6 | **OK**、**Commit (**コミット**)** の順にクリックします。

STEP 7 | （ 任意 ）ARP キャッシュ タイムアウトを変更します。

1. CLI にアクセスし、ファイアウォールが ARP エントリをキャッシュに保持する秒数を指定します。操作コマンド **`set system setting arp-cache-timeout`** <*value*> を使用します。範囲は 60～65,535 です。デフォルトは 1,800 です。

   タイムアウトを減らし、キャッシュ内の既存のエントリの TTL が新しいタイムアウトより大きい場合、ファイアウォールはこれらのエントリを削除し、ARP キャッシュを更新します。タイムアウトを増加して、既存のエントリの TTL が新しいタイムアウトよりも短くなる場合は、TTL に従ってファイアウォールが期限切れになり、ファイアウォールは新しいタイムアウト値を持つ新しいエンティティをキャッシュします。
2. 操作 CLI コマンド **`show system setting arp-cache-timeout`** を含む ARP キャッシュ タイムアウト設定を表示します。

セッション設定の指定

このトピックでは、タイムアウト値以外のセッションのさまざまな設定について説明します。デフォルト設定を変更する必要がある場合、以下のタスクを実行します。

STEP 1 | セッション設定を変更します。

Device (デバイス) > **Setup (セットアップ)** > **Session (セッション)** を選択して Session Settings (セッション設定) を編集します。

STEP 2 | 新しく設定したセキュリティポリシー ルールを進行中のセッションに対して割り当てるかどうかを指定します。

Rematch all sessions on config policy change（設定ポリシーの変更についてすべてのセッションに再マッチング）を選択し、新しく設定し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対して割り当てます。この機能はデフォルトで有効になっています。このチェックボックスをオフにすると、ポリシールールの変更内容はすべて、ポリシーの変更をコミットした後に発生し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を現在のセッションに適用してブロックします。

STEP 3 | IPv6の設定を行います。

- **ICMPv6 Token Bucket Size** [ICMPv6 トークン バケット サイズ]–デフォルト：100トークン。ICMPv6 レート制限のセクションを参照してください。
- **ICMPv6 Error Packet Rate (per sec)** [ICMPv6 エラー パケット速度（秒あたり）] – デフォルト：100ICMPv6 レート制限のセクションを参照してください。
- **IPv6** ファイアウォールの有効化 – IPv6 のファイアウォール機能を有効にします。IPv6 が有効になっていないと、IPv6 ベースの設定はすべて無視されます。インターフェイスで IPv6 が有効な場合でも、IPv6 が機能するためには **[IPv6** ファイアウォール設定] 設定も有効にする必要があります。

STEP 4 | ジャンボフレームを有効化し、MTUを設定します。

1. **Enable Jumbo Frame** [Jumbo Frame を有効にする]を選択し、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します。Jumbo Frame の最大伝送単位（MTU）は 9,216 バイトで、特定のモデルで使用できます。
2. ジャンボフレームを有効にしたかどうかに応じて**Global MTU** [グローバルMTU]を設定します。
   - ジャンボフレームを有効化しなかった場合、**Global MTU**[グローバル MTU] はデフォルトの 1,500 バイトになり、範囲は 576 ～ 1,500 バイトになります。
   - ジャンボフレームを有効化した場合、**Global MTU** [グローバル MTU]はデフォルトの 9,192 バイトになり、範囲は 9,192 ～ 9,216 バイトになります。

   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 フレームを使用しないインターフェイスがある場合、その MTU を 1500 バイトか別の値に設定する必要があります。

インポートする場合 (デバイス > セットアップ > オペレーション > インポート) とジャンボフレームが有効になっている構成をロードし、まだジャンボフレームが有効になっていないファイアウォールにコミットすると、ジャンボフレーム の設定はコミットされません。最初に ***Jumbo Frame*** を有効にして再起動してから、設定をインポート、ロード、コミットします。

STEP 5 | NATセッション設定を調整します。

- **NAT64 IPv6** 最小 **MTU** – IPv6 変換済みトラフィックのグローバル MTU を設定します。デフォルトの 1,280 バイトは、IPv6 トラフィックの標準の最小 MTU に基づきます。
- **NAT** オーバーサブスクリプション率 – NAT がダイナミック IP およびポート（DIPP）変換として設定されている場合、オーバーサブスクリプション率を設定し、同じ変換後 IP アドレスとポートのペアを同時に使用できる回数を乗算できます。オーバーサブスクリプ

ション率は、1、2、4、または 8 です。デフォルト設定は、ファイアウォール モデルに基づいています。

- オーバーサブスクリプション率が 1 の場合、オーバーサブスクリプションは行われず、変換後の IP アドレスとポートのペアは、それぞれ一時点に 1 回のみ使用できます。
- 設定が **Platform Default (**プラットフォームのデフォルト**)** の場合、オーバーサブスクリプション率のユーザー設定は無効になり、プラットフォーム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。

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。

STEP 6 | 保持時間短縮設定を調整します。

Accelerated Aging (保持時間短縮**)** を選択し、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。しきい値（%）および倍率を変更することもできます。

- セッション保持時間短縮の開始しきい値 — セッション テーブルのパーセント。このパーセントに達すると、セッション保持時間短縮が開始されます。デフォルトは 80% です。セッション テーブルがこのしきい値（% 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保持時間の計算に適用されます。
- セッション保持時間短縮倍率 — セッション保持時間短縮の計算に使用される倍率。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。

たとえば、短縮倍率が10の場合、通常は3600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。

STEP 7 | パケット バッファ保護を有効にします。

1. **Packet Buffer Protection (**パケット バッファ保護**)** を選択し、ファイアウォールのパケット バッファを超過させることで正当なトラフィックをドロップさせてしまうおそれがあるセッションに対してファイアウォールが取るアクションを有効化します。これはデフォルトで有効になっています。
2. パケット バッファ保護を有効にすると、ファイアウォールがパケット バッファの悪用に対処する方法を決めるしきい値およびタイマーを調整できます。
   - **Alert (%) (**アラート（%）**)**：パケット バッファの使用率がこのしきい値を超えると、ファイアウォールがログ イベントを生成します。デフォルトのしきい値は 50% で、範囲は 0～99% です。値を 0% に指定すると、ファイアウォールはログ イベントを作成しません。
   - **Activate (%) (**アクティベート（%）**)**：パケット バッファの使用率がこのしきい値を超えると、ファイアウォールが悪用されているセッションにランダム早期ドロップ

（RED）を適用します。デフォルトのしきい値は 80% で、範囲は 0～99% です。値を 0% に設定すると、ファイアウォールは RED を適用しません。

アラート イベントはシステム ログに記録されます。トラフィックのドロップ、破棄されたセッション、ブロックされた *IP* アドレスの各イベントは脅威ログに記録されます。

- **Block Hold Time (sec) (**ブロック ホールド タイム（秒）**)**：破棄するまでの間に、ファイアウォールが RED が軽減されたセッションが継続するのを許可する期間です。デフォルトでは、ブロック ホールド タイムは 60 秒です。範囲は 0 ～ 65,535 秒です。値を 0 に設定すると、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。
- **Block Duration (sec) (**ブロック期間（秒）**)**：この設定は、セッションが破棄される期間あるいは IP アドレスがブロックされる期間を定義します。デフォルトは 3,600 秒で、範囲は 0 ～ 15,999,999 秒です。値を 0 に設定すると、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または IP アドレス ブロックを実施しません。

STEP 8 | マルチキャスト ルートの設定パケットのバッファリングを有効化します。

1. **Multicast Route Setup Buffering** [マルチキャストルートの設定バッファ]を選択すると、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なります。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。このオプションはデフォルトでは無効になっています。
2. バッファリングを有効化した場合、フローごとのバッファサイズを指定する**Buffer Size** [バッファサイズ]の調整も行えます。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。

仮想ルーターを操作するマルチキャスト設定を仮想ルーター上で行うことで、セッション終了後にファイアウォール上のルーティングテーブルでマルチキャスト ルートが保持される時間（秒）を調整することもできます（仮想ルーター設定の ***Multicast (***マルチキャスト***) > Advanced (***詳細***)*** タブにある ***Multicast Route Age Out Time (sec) (***マルチキャスト ルートのエイジアウト秒数***)*** を設定）。

STEP 9 | セッション設定を保存します。

OK をクリックします。

STEP 10 | レイヤー 3 インターフェイス用の最大セグメント サイズ（MSS）調整サイズを調整します。

1. **Network (ネットワーク)** > **Interfaces (インターフェイス)** を選択し、**Ethernet (イーサネット)**、**VLAN**、あるいは **Loopback (ループバック)** を選択し、さらに Layer 3 (レイヤー 3) インターフェイスを選択します。
2. **Advanced**（詳細） > **Other Info**（その他の情報）を選択します。
3. **Adjust TCP MSS (TCP MSS** の調整**)** を選択し、次のうちいずれかあるいは両方の値を入力します。
   - **IPv4 MSS Adjustment Size (IPv4 MSS** 調整サイズ**)** (範囲は 40〜300 バイト、デフォルトは 40 バイト)。
   - **IPv6 MSS Adjustment Size (IPv6 MSS** 調整サイズ**)** (範囲は 60〜300 バイト、デフォルトは 60 バイト)。
4. **OK** をクリックします。

STEP 11 | 変更をコミットします。

Commit（コミット）をクリックします。

STEP 12 | ジャンボフレームの設定を変更した後、ファイアウォールを再起動します。

1. **Device**（デバイス） > **Setup**（セットアップ） > **Operations**（操作）を選択します。
2. **Reboot Device**（デバイスの再起動） をクリックします。

セッション配信ポリシー

セッション配信ポリシーは、PA-5200 および PA-7000 Series ファイアウォールが、ファイアウォール上のデータプレーン プロセッサ（DP）にセキュリティ処理（App-ID、Content-ID、URL フィルタリング、SSL 復号化、および IPSec）を配信する方法を定義します。ファイアウォールがセッションを配信する際の効率を最大化するよう、各ポリシーは特定の種類のネットワーク環境およびファイアウォール構成専用に設計されています。例えば、Hash セッション配布ポリシーは、大規模なソース NAT を使用する環境に最適です。

許可されるファイアウォール上の DP の数は、ファイアウォール モデルに基づいています：

Firewall Model（ファイアウォール モデル）	データプレーン プロセッサ
PA-7000シリーズ	インストール済みの Network Processing Cards（NPC）の数によります。各 NPC は複数のデータプレーン プロセッサ（DP）を持っており、ファイアウォールに複数の NPC をインストールできます。
PA-5220 ファイアウォール	1 *PA-5220* ファイアウォールには *DP* が一つしかないため、セッション配信ポリシーは効果がありません。ポリシーはデフォルト（*round-robin*）のままにします。
PA-5250 ファイアウォール	2
PA-5260 および PA-5280 ファイアウォール	3
PA-5450 ファイアウォール	インストールされているData Processing Cards(DPC)の数によって異なります。

次の各トピックは、利用できるセッション配信ポリシーについての情報、アクティブ ポリシーを変更する方法、セッション配信統計情報を表示する方法を説明します。

- セッション分配ポリシーについて
- セッション配信ポリシーの変更および統計の閲覧

セッション分配ポリシーについて

次の表は、自身の環境およびファイアウォールの設定に最適なポリシーを決定する際に役立つ、セッション配信ポリシーについての情報を示しています。

セッション配信ポリシー	の意味
固定	ファイアウォールがセキュリティ処理を行うために使用するデータプレーン プロセッサ（DP）を指定することができるようになります。 このポリシーはデバッグを行うために使用します。
ハッシュ	ファイアウォールは、ソースアドレスまたは宛先アドレスのハッシュに基づいてセッションを分配します。ハッシュ ベースの配信により、IP アドレスあるいはポートが衝突するリスクをなくすことで、NAT アドレス リソース管理の効率が向上し、NAT セッション セットアップの遅延が減ります。 このポリシーは、ダイナミック IP 変換またはダイナミック IP およびポート変換またはその両方で大規模ソース NAT を使用する環境で使用します。動的 IP 変換を使用する際、**source（送信元）**アドレスのオプションを選択します。動的 IP およびポート変換を使用する際、**destination（宛先）**アドレスのオプションを選択します。
入力スロット（PA-7000 Series ファイアウォールではデフォルト）	（PA-7000 Series ファイアウォールのみ）新規セッションは同じ NPC 上の DP に割り当てられ、そこにセッションの最初のパケットが到達します。DP の選択はセッション ロード アルゴリズムに基づいて行いますが、このケースでは、セッションが入力 NPC 上の DP に制限されています。 トラフィックおよびネットワークのトポロジーに応じて、このポリシーはトラフィックがスイッチ構造を通過する可能性を全体的に減らします。 このポリシーを使用し、入力および出力がどちらも同じ NPC 上にある場合の遅延を減らします。ファイアウォールに NPC が混在する（例えば PA-7000 20G および PA-7000 20GXM）場合、このポリシーは増加した能力を対応する NPC に隔離できるため、NPC のエラー時の影響が隔離されやすくなります。
Random ランダム	ファイアウォールはセッション処理のために DP をランダムに選択します。
ラウンドロビン（PA-5200 Series ファイアウォールではデフォルト）	ファイアウォールは、入力、出力とセキュリティ処理機能が、すべてのアクティブ データプレーンで共有されるように、ラウンドロビン アルゴリズムに基づき、データプレーンから、データプレーン プロセッサを選択します。

セッション配信ポリシー	の意味
	シンプルかつ予想可能な負荷分散アルゴリズムで十分な、要求が小～中程度の環境でこのポリシーを使用します。 要求が大きい環境では、セッションロード アルゴリズムを使うことが推奨されます。
セッションロード	このポリシーはラウンドロビン ポリシーと似ていますが、DP 間のバランスを保つためにセッションを配信する方法を決定する際、ウェイト ベースのアルゴリズムを使用します。セッションの有効期間は多様であるため、DP の負荷が必ずしも同じになるとは限りません。例えば、ファイアウォールが 3 つの DP を持っており、DP0 の容量が 25%、 DP1 が 25%、 DP2 が 50% の場合、新規セッションの割り当ては、容量が低い DP を優先して行われます。持続的に負荷分散を改善するためにこれが役立ちます。 スロット間の集約インターフェイス グループのような、セッションが複数の NPC スロットにわたって配信される環境、あるいは非対称転送を行う環境では、このポリシーを使用します。また、セッション能力が異なる NPC（PA-7000 20G および PA-7000 20GXM NPC など）がファイアウォールに混在している場合も、このポリシーあるいは入力スロット ポリシーを使用できます。
対称ハッシュ	（PAN-OS 8.0 以降を実行している PA-7000 Series および PA-5200 Series ファイアウォール）ファイアウォールは、ソートされた送信元および宛先 IP アドレスのハッシュによって DP を選択します。このポリシーでは、サーバー対クライアント（s2c）およびクライアント対サーバー（c2s）トラフィックで同じ結果が得られます（ファイアウォールが NAT を使用していないと仮定）。 要求の大きい IPSec あるいは GTP デプロイ環境でこのポリシーを使用します。 これらのプロトコルの場合はどちらの方向も、フロータプルを互いに送付できない一方通行のフローとして扱われます。このポリシーはどちらの方向も同じ DP に割り当て、DP 間の通信を不要にすることで、パフォーマンスを向上させて遅延を少なくします。

セッション配信ポリシーの変更および統計の閲覧

次の表は、アクティブなセッション配信ポリシーを表示・変更する方法、ファイアウォール内の各データプレーン プロセッサ（DP）に関するセッション統計情報を閲覧する方法を示しています。

タスク	コマンド
アクティブ セッション配信ポリシーを表示します。	アクティブ セッション配信ポリシーを表示するには、**show session distribution policy** コマンドを使用します。 以下の出力は、入口スロット配信ポリシーが有効であり、NPC 4 枚を設置した PA-7080 ファイアウォールを示しています（スロット 2、10、11、12）。 **> show session distribution policy** Ownership Distribution Policy: ingress-slot Flow Enabled Line Cards: [2, 10, 11, 12]Packet Processing Enabled Line Cards: [2, 10, 11, 12]
アクティブ セッション配信ポリシーを変更します。	アクティブ セッション配布ポリシーを変更するには、**set session distribution-policy *<policy>*** コマンドを使用します。 例えば、セッションロード ポリシーを選択する場合、以下のコマンドを入力します。 **> set session distribution-policy session-load**
セッション配信統計を表示します。	**show session distribution statistics** コマンドを使用し、ファイアウォール上のデータプレーン プロセッサ（DP）および各アクティブ DP 上のセッション数を表示します。 次の出力は PA-7080 ファイアウォールのものです。 **> show session distribution statistics** DP Active Dispatched Dispatched/sec --- s1dp0 78698 7829818 1473 s1dp1 78775 7831384 1535 s3dp0 7796 736639 1488 s3dp1 7707 737026 1442

タスク	コマンド
	DP Active column (DP アクティブ列) には、インストール済みの NPC 上にある各データプレーンが列挙されています。最初の 2 文字はスロット番号を、最後の 3 文字はデータプレーン番号を示します。例えば s1dp0 はスロット 1 内の NPC 上のデータプレーン 0 を示し、s1dp1 はスロット 1 内の NPC 上のデータプレーン 1 を示します。 **Dispatched (発信)** 列は、前回ファイアウォールが再起動されてから、データプレーンが処理した合計セッション数を表示しています。 **Dispatched/sec (発信/秒)** 列は、発信速度を示します。**Dispatched (発信)** 列の数値を足すと、合計の値はファイアウォール上のアクティブなセッションの数と一致します。また、**show session info CLI (セッション情報 CLI を表示)** コマンドを実行して、有効セッションの合計数を確認することもできます。 *PA-5200 Series* ファイアウォールの出力は、*DP* の数がモデルによって異なるのと、*NPC* スロットが一つ（*s1*）しかないという点以外は同様です。

TCP スプリット ハンドシェーク セッションの確立の防止

ゾーン プロテクション プロファイルで TCP スプリット ハンドシェークのドロップを設定して、標準的な 3 ウェイ ハンドシェークが使用されていない場合に TCP セッションが確立されないようにすることができます。この作業では、TCPスプリット ハンドシェイクにセッションを確立させたくないインターフェイス用のセキュリティ ゾーンを割り当て済みであるという前提で説明していきます。

STEP 1 | ゾーン プロテクション プロファイルを設定して、3 ウェイ ハンドシェーク以外を使用する TCP セッションでセッションが確立されないようにします。

1. **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)** を選択し、新しいプロファイルを **Add (追加)**（あるいは既存のプロファイルを選択）します。
2. 新しいプロファイルを選択する場合、プロファイルの **Name** [名前]、および必要に応じて **Description** [内容]を入力します。
3. **Packet Based Attack Protection (パケット ベースの攻撃防御)** > **TCP Drop (TCP ドロップ)** の順に選択し、**Split Handshake (スプリット ハンドシェイク)** を選択します。
4. **OK** をクリックします。

STEP 2 | プロファイルを 1 つ以上のセキュリティ ゾーンに適用します。

1. **Network (ネットワーク)** > **Zones (ゾーン)** の順に選択し、ゾーン プロテクション プロファイルを割り当てるゾーンを選択します。
2. Zone (ゾーン) ウィンドウの **Zone Protection Profile (ゾーン プロテクション プロファイル)**リストから、前のステップで設定したプロファイルを選択します。

   または、ここで **Zone Protection Profile** [ゾーン プロテクション プロファイル]をクリックして新しいプロファイルの作成を開始することもできます。その場合、その結果に基づいて続行されます。
3. **OK** をクリックします。
4. （任意）手順 1 ～ 3 を繰り返して、プロファイルを他のゾーンに適用します。

STEP 3 | 変更をコミットします。

OK、**Commit (コミット)** の順にクリックします。

Tunnel Content Inspection（トンネル コンテンツ検査）

ファイアウォールは、トンネルを終端させずに平文トンネル プロトコルのトラフィック内容を検査できます。

- Generic Routing Encapsulation（GRE））RFC 2784）
- 非暗号 IPSec トラフィック [IPSec 用の NULL 暗号化アルゴリズム（RFC 2410）および転送モードの AH IPSec]
- ユーザー データ (GTP-U) 用の General Packet Radio Service (GPRS) トンネリング プロトコル
- 仮想拡張ローカルエリアネットワーク (VXLAN) (RFC 7348)

トンネル コンテンツ検査はクリアテキスト トンネル用であり、暗号化されたトラフィックを運ぶ *VPN* あるいは *LSVPN* トンネルには使いません。

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 IPSec トンネル）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。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。

すべてのファイアウォール モデルが GRE、非暗号化 IPSec、VXLAN プロトコルのトンネル コンテンツ検査をサポートしています。GTP セキュリティをサポートするファイアウォールのみが GTP-U トンネルコンテンツインスペクションをサポートします。互換性マトリックスの GTP および SCTP セキュリティをサポートするモデル別の PAN-OS リリースを参照してください。

デフォルトでは、サポートされているファイアウォールはトンネル アクセラレーションを実行して、GRE トンネル、VXLAN トンネル、および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とスループットを向上させます。トンネル アクセラレーションは、ハードウェア オフロードを提供して、フロー ルックアップの実行にかかる時間を短縮し、内部トラフィックに基づいてトンネル トラフィックをより効率的に分散できるようにします。ただし、トンネル アクセラレーションを無効化によりトラブルシューティングを実行できます。

- トンネル コンテンツ検査の概要
- トンネル コンテンツ検査の設定
- 検査済みのトンネル アクティビティを表示
- ログでトンネル情報を閲覧
- タグ付けされたトンネル トラフィックに基づいてカスタム レポートを作成
- トンネル アクセラレーションを無効化

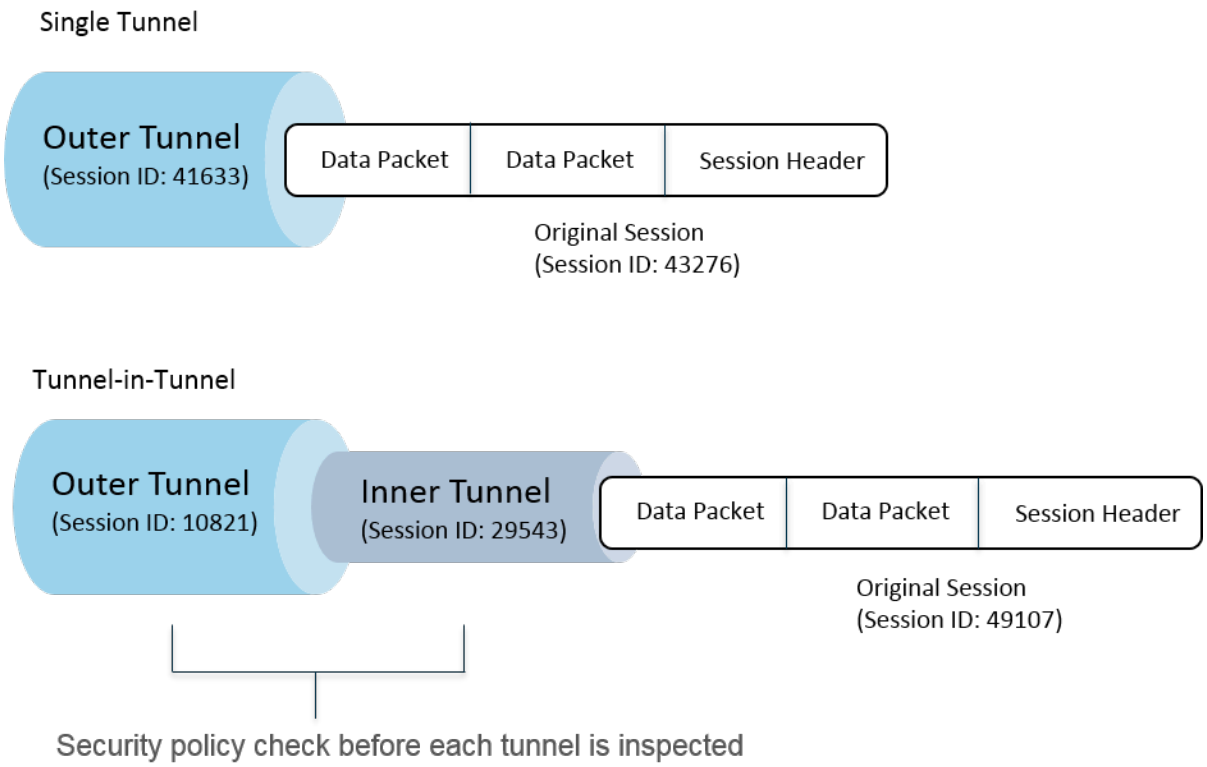
トンネル コンテンツ検査の概要

ファイアウォールは、事前にトンネルを終了する機会がないネットワークのどこでも、トンネル コンテンツを検査できます。GRE、非暗号化 IPSec、GTP-U、あるいは VXLAN トンネルのパス上にある限り、ファイアウォールはトンネル コンテンツを検査できます。

- トンネル コンテンツ検査が必要な企業のお客様は、GRE、VXLAN、あるいは非暗号化 IPSec を使用してファイアウォール上のトンネルの一部あるいはすべてにトンネルを適用することができます。セキュリティ、QoS、レポート関連の目的で、トンネル内のトラフィックを検査します。
- サービスプロバイダのお客様は GTP-U を使用して、モバイル デバイスからのデータトラフィックにトンネルを適用することができます。トンネル プロトコルを終了させることなく内部コンテンツを検査し、ユーザーからのデータを記録することになるでしょう。

ファイアウォールは、イーサネット インターフェイス、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 インターフェイスでのトンネル コンテンツ検査をサポートします。（ファイアウォールが検査するクリアテキスト トンネルは、ファイアウォールを終端とする VPN あるいは LSVPN トンネル内に入れることが可能です。つまり、VPN あるいは LSVPN トンネル インターフェイスにすることができます。言い換えると、ファイアウォールが VPN あるいは LSVPN エンドポイントである際、ファイアウォールはトンネル コンテンツ検査をサポートする暗号化されていないあらゆるトンネルのトラフィックを検査できます。

トンネル コンテンツ検査は、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。



次の図は、ファイアウォールが実行できる 2 つのレベルのトンネル検査を示しています。トンネル検査ポリシー ルールが設定されているファイアウォールがパケットを受信する際：

- ファイアウォールはまずセキュリティポリシーチェックを実行し、パケット内のトンネル プロトコル（アプリケーション）が許可されるか拒否されるかを判断します。（IPv4 および IPv6 パケットはトンネル内でサポートされているプロトコルです）
- セキュリティポリシーがパケットを許可する場合、ファイアウォールは送信元ゾーン、送信元アドレス、送信元ユーザー、宛先ゾーン、および宛先アドレスに基づいてパケットをトンネル検査ポリシー ルールにマッチさせます。トンネル検査ポリシー ルールは、ファイアウォールが検査するトンネル プロトコル、許可されるカプセル化の最大レベル（単一のトンネル、あるいはトンネルに含まれたトンネル）、RFC 2780 に従う厳密なヘッダー検査をパスしないトンネル プロトコルを含むkパケットを許可するかどうか、未知のプロトコルを含むパケットを許可するかどうかを判断します。
- パケットがトンネル検査ポリシー ルールの一致条件にパスすると、ファイアウォールは内部コンテンツを検査します。その際、これはセキュリティポリシー（必須）および任意で指定できるポリシーの影響を受けます。（元のセッション用にサポートされているポリシータイプを、次の表にリストアップしています）
- ファイアウォールが代わりに別のトンネルを見つける場合、ファイアウォールは 2 つ目のヘッダのパケットを再帰的にパースし、カプセル化のレベル 2 になります。そのため、ファイアウォールがパケットの処理を継続するためには、トンネル ゾーンにマッチする 2 つ目のトンネル検査ポリシー ルールが、トンネル検査の最大レベル 2 を許可する必要があります。
  - ルールが検査レベル 2 を許可すると、ファイアウォールはこの内側のトンネルに対してセキュリティポリシーチェックを実施し、次にトンネル検査ポリシーチェックを行います。

内側のトンネルで使用するトンネル プロトコルは、外側のトンネルで使用するトンネル プロトコルと異なっていても構いません。

- ルールが検査レベル 2 を許可しない場合、設定した最大トンネル検査レベルよりも高いレベルでカプセル化されているパケットをドロップする設定を行っているかどうかに基づき、ファイアウォールがアクションを決定します。

デフォルト設定では、トンネルにカプセル化されたコンテンツはトンネルと同じセキュリティ ゾーンに属し、そのゾーンを保護するセキュリティ ポリシー ルールの適用対象になります。ただし、トンネル ゾーンを設定すれば、トンネル用のセキュリティ ポリシー ルールと異なるセキュリティ ポリシー ルールを柔軟に内部コンテンツに設定できるようになります。そのトンネル ゾーンに対して異なるトンネル検査ポリシーを使用する場合、定義によってファイアウォールがカプセル化の 2 つ目のレベルを見るため、必ず最大トンネル検査レベルが 2 レベルでなければなりません。

ファイアウォールは、ファイアウォールを終端とするトンネルについては、トラフィックにマッチするトンネル検査ポリシー ルールをサポートしていません。ファイアウォールは内側のトンネル セッションにマッチするパケットを破棄します。例えば、IPSec トンネルがファイアウォール上で終了する際に、終了させるトンネルにマッチするトンネル検査ポリシー ルールを作成してはなりません。ファイアウォールはすでに内側のトンネル トラフィックを検査しているため、トンネル検査ポリシー ルールは不要です。

トンネル コンテンツ検査は共通ゲートウェイでも仮想システム間の通信でも動作しますが、トンネル ゾーンを共通ゲートウェイあるいは仮想システム間の通信に割り当てることはできません。それらには、所属先のゾーンと同じセキュリティ ポリシー ルールが適用されます。

内側のトンネル セッションおよび外側のトンネル セッションは両方とも、そのファイアウォール モデルの最大セッション容量に加味されます。

次の表では、外側のトンネル セッション、内側のトンネル セッション、内部、元のセッションのそれぞれに適用できるポリシーの種類をチェックマークで示しています。

ポリシーのタイプ	外側のトンネル セッション	内側のトンネル セッション	内部、元のセッション
アプリケーション オーバーライド	✓ VXLAN 専用	–	✓
DoS プロテクション	✓	✓	✓
NAT	✓	–	–
ポリシーベース フォワーディング（PBF）および対称リターン	✓	–	–

ポリシーのタイプ	外側のトンネル セッション	内側のトンネル セッション	内部、元のセッション
QoS	–	–	✓
セキュリティ（必須）	✓	✓	✓
User-ID	✓	✓	✓
ゾーン プロテクション	✓	✓	✓

VXLAN は他のプロトコルと異なります。ファイアウォールは、2 つの異なるセッション鍵セットのいずれかを使用して VXLAN 用の外部トンネルセッションを作成することができます。

- VXLAN UDP セッション–6 タプルキー (ゾーン、送信元 IP、宛先 IP、プロトコル、送信元ポート、および宛先ポート) は、VXLAN UDP セッションを作成します。
- VNI セッション–トンネル ID (VXLAN ネットワーク識別子、または VNI) を組み込み、ゾーン、送信元 IP、宛先 IP、プロトコル、およびトンネル ID (VNI) を使用して VNI セッションを作成する 5 タプルのキー。

ACC 上で検査済みのトンネル アクティビティを表示するか、ログでトンネル情報を閲覧できます。素早く表示を確認するためには、監視タグを設定し、タグに基づいてトンネル アクティビティを監視したりログの結果をフィルタリングしたりできるようにします。

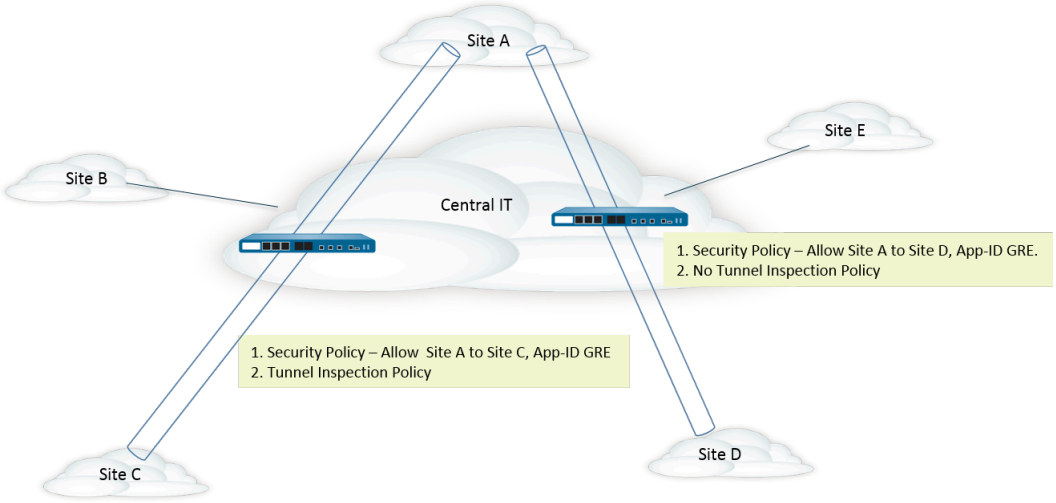
ACC トンネル アクティビティは、様々な表示形式でデータを提供します。Tunnel ID Usage (トンネル ID の使用状況)、Tunnel Monitor Tag (トンネル監視タグ)、および Tunnel Application Usage (トンネル アプリケーション使用状況) については、**bytes (バイト)**、**sessions (セッション)**、**threats (脅威)**、**content (コンテンツ)**、および **URLs** のデータがトラフィック サマリー データベースから取得されます。Tunnel User (トンネル ユーザー)、Tunneled Source IP (トンネル送信元 IP) および Tunneled Destination IP Activity (トンネル宛先 IP アクティビティ) については、**bytes (バイト)** および **sessions (セッション)** のデータはトラフィック サマリー データベースから、**threats (脅威)** のデータは脅威サマリーから、**URLs** のデータは URL サマリーから、**contents (コンテンツ)** のデータは、脅威ログのサブネットである Data データベースから取得されます。

インターフェイス上で NetFlow を有効化すると、重複カウント（外側および内側のフローのバイト数を両方カウント）を避けるために、NetFlow が外側のトンネルの統計情報のみをキャプチャするようになります。

お使いのファイアウォール モデルのトンネル検査ポリシールールおよびトンネル ゾーンの能力については、製品選択ツールを参照してください。

次の図は、複数の部門を運用し、異なるセキュリティ ポリシーおよびトンネル検査ポリシーを使用する企業を示しています。Central IT チームがリージョン間の接続を提供します。Site A から Site C に接続するトンネルがあります。別のトンネルは Site A から Site D に接続します。Central IT が各トンネルのパスにファイアウォールを 1 つ配置し、Sites A および C 間のトンネル内のファイアウォールが、トンネル検査を実施します。トラフィックが非常にセンシティ

ブであるため、Sites A および D 間のトンネル内のファイアウォールはトンネル検査ポリシーを持っていません。



トンネル コンテンツ検査の設定

このタスクを実行し、トンネル経由で許可するトンネル プロトコルに対するトンネル コンテンツ検査を設定します。

STEP 1 | 特定のアプリケーション（GRE アプリケーションなど）を使用するパケットを、送信元ゾーンから送信先ゾーンへのトンネル経由で許可するセキュリティ ポリシー ルールを作成します。

セキュリティ ポリシー ルールを作成する

ファイアウォールは、セッションの開始時、セッションの終了時、またはその両方でトンネル検査ログを作成できます。セキュリティポリシー ルールの***Actions***（アクション） を指定する際、*GRE* セッションなど、長期間継続するトンネル用に***Log at Session Start (***セッション開始時にログ**)** を選択します。

STEP 2 | トンネル検査ポリシー ルールを作成します。

1. **Policies (**ポリシー**)** > **Tunnel Inspection (**トンネル検査**)** を選択してポリシールールを**Add (**追加**)** します。
2. **General (**全般**)** タブで Tunnel Inspection (トンネル検査) ポリシールールの**Name (**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 (-)、ドット (.)、スペースを含めることができます。
3. 任意**Description (**内容**)** を入力します。
4. 任意）レポートおよびロギングを目的として、トンネル検査ポリシー ルールの対象になるパケットを特定する**Tag (**タグ**)** を指定します。

STEP 3 | トンネル検査ポリシー ルールを適用するパケットの送信元を判断する基準を指定します。

1. **Source (**送信元**)** タブを選択します。
2. ゾーンのリストから**Source Zone (**送信元ゾーン**)** を**Add (**追加**)** します（デフォルト**Any**（任意））。
3. 任意**Source Address (**送信元アドレス**)** を**Add (**追加**)** します。IPv4 あるいは IPv6 アドレス、アドレスグループ、あるいは Geo Region アドレス オブジェクトを入力できます（**Any**（任意））。
4. 任意）これらの指定する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。
5. Optional（任意）**Source User**（送信元ユーザー）を**Add**（追加）します（デフォルトは**any**（任意））です**Known-user (**既知のユーザー**)** は認証したことがあるユーザーです**Unknown (**未知**)** のユーザーは認証したことがありません。

STEP 4 | トンネル検査ポリシー ルールを適用するパケットの宛先を判断する基準を指定します。

1. **Destination (宛先)** タブを選択します。
2. ゾーンのリストから**Destination Zone (宛先ゾーン)** を**Add (追加)** します（デフォルト**Any**（任意））。
3. 任意**Destination Address (宛先アドレス)** を**Add (追加)** します。IPv4 あるいは IPv6 アドレス、アドレスグループ、あるいは Geo Region アドレス オブジェクトを入力できます（デフォルトは**Any**（任意）です）。

   新しいアドレスあるいはアドレスグループを設定することもできます。
4. 任意）これらの指定する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。

STEP 5 | このルールでファイアウォールが検査するトンネル プロトコルを指定します。

1. **Inspection (検査)** タブを選択します。
2. 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（GRE） 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）Tunneling Protocol for User Data（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、トンネルで仮想拡張ローカルエリアネットワーク (VXLAN) トンネリングプロトコルを使用するパケットを検査します。

STEP 6 | ファイアウォールが検査するカプセル化のレベル数、ファイアウォールがパケットをドロップする条件を指定します。

1. **Inspect Options (**検査オプション**)** を選択します。
2. ファイアウォールが検証を行う**Maximum Tunnel Inspection Levels (**最大トンネル検査レベル**)** を選択します。

   - **One Level (1** レベル**)**（デフォルト）–ファイアウォールは外側のトンネルのコンテンツのみを検査します。

     VXLAN の場合、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。検査は外部トンネルでのみ行われるため**One Level (1** レベル**)** を選択しなければなりません。

   - **Two Levels (Tunnel In Tunnel) (2** レベル（トンネル イン トンネル）**)**–ファイアウォールは外側のトンネルのコンテンツおよび内側のトンネルのコンテンツを検査します。
3. 次のいずれか、すべて、またはどれも選択しないで、各条件でファイアウォールがパケットをドロップするかどうかを指定します。

   - **Drop packet if over maximum tunnel inspection level (**最大トンネル検査レベルを超過したらパケットをドロップ**)**–ファイアウォールが**Maximum Tunnel Inspection Levels (**最大トンネル検査レベル**)** で設定されているよりも多いカプセル化のレベルを含むパケットをドロップします。
   - **Drop packet if tunnel protocol fails strict header check (**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にパケットをドロップ**)**–ファイアウォールがプロトコルの 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ている可能性があります。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。

     ファイアウォールがRFC 2890 よりも古いバージョンの *GRE* を実装したデバイスを使って *GRE* のトンネリングを行う場合***Drop packet if tunnel protocol fails strict header check (***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にパケットをドロップ**)** するオプションを有効化しないでください。

   - **Drop packet if unknown protocol inside tunnel (**トンネル内に未知のプロトコルがある場合にパケットをドロップ**)**–ファイアウォールが特定できないプロトコルをトンネル内に含むパケットをドロップします。

     例えば、このオプションを選択すると、ファイアウォールは暗号化された IPSec パケットを読み取ることができないため、トンネル検査ポリシールールにマッチしたそのパケットをドロップします。これにより IPSec パケットを許可できるようになり、ファイアウォールが null-encrypted IPSec および AH IPSec パケットのみを許可するようになります。

   - **Return scanned VXLAN tunnel to source (**スキャンされた **VXLAN** トンネルをソースに戻す**)**–トラフィックがファイアウォールにリダイレクト (ステアリング) されると、VXLAN はパケットをカプセル化します。トラフィックステアリングは、パブリッククラウド環境で最も一般的なものです**Return scanned VXLAN tunnel to**

source (スキャンされた **VXLAN** トンネルをソースに返す**)** を有効にして、カプセル化されたパケットを発信元の VXLAN トンネルエンドポイント (VTEP) に返します。このオプションは、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。

4. **OK** をクリックします。

STEP 7 | トンネル検査ポリシー ルールを管理します。

次を使用してトンネル検査ポリシー ルールを管理します。

- （フィルタ フィールド）–フィルタ フィールドで名前が指定されているトンネル ポリシールールのみを表示します。
- **Delete (**削除**)**–選択したトンネル ポリシールールを削除します。
- **Clone (**コピー**)Add (**追加**)** ボタンの代わりに使用でき、選択したルールに新しい名前（後で変更可能）を付けてコピーできます。
- **Enable (**有効**)**–選択したトンネル ポリシールールを有効化します。
- **Disable (**無効化**)**–選択したトンネル ポリシールールを無効化します。
- **Move (**移動**)**–選択したトンネル ポリシールールをリストの上下に移動させます。パケットは上から順にルールと照らし合わせて評価されます。
- **Highlight Unused Rules (**未使用のルールをハイライト表示**)**–ファイアウォールが前回再起動してから、パケットが一度もマッチしていないトンネル ポリシールールをハイライト表示します。

STEP 8 | 任意）トンネル コンテンツ用にトンネル送信元ゾーンおよびトンネル宛先ゾーンを作成し、ゾーン毎にセキュリティポリシー ルールを設定します。

トンネル トラフィック用にトンネル ゾーンを作成するのがベストプラクティスになります。そうすることで、同じ *5* タプル（送信元 *IP* アドレスおよびポート、宛先 *IP* アドレスおよびポート、プロトコル）を持つトンネル化されたパケットおよびトンネル化されていないパケットに対し、ファイアウォールが別々のセッションを作るようになります。

PA-5200 Series ファイアウォールでトンネル ゾーンをトンネル トラフィックに割り当てると、ファイアウォールがソフトウェア内でトンネル検査を行うようになります。ハードウェア トンネル検査によって負荷を減らすことはありません。

1. トンネル コンテンツに、外部トンネル（以前に設定済み）のゾーンのセキュリティ ポリシー ルールとは異なるセキュリティ ポリシー ルールを適用させたい場合**Network**

(ネットワーク) > **Zones (ゾーン)** を選択し、その Tunnel Source Zone (トンネル送信元ゾーン) の**Name (名前)** を**Add (追加)** します。

2. **Location (場所)** については仮想システムを選択します。
3. **Type (タイプ)** については**Tunnel (トンネル)** を選択します。
4. **OK** をクリックします。
5. これらのサブステップを繰り返し、トンネル宛先ゾーンを作成します。
6. トンネル送信元ゾーン用セキュリティポリシー ルールの設定を行います。

   トンネル トラフィックの発信者あるいはトラフィック フローの行き先が分からない場合があり、あるアプリケーションについてトンネルを通るトラフィックを不意に禁止したくない場合があるため、両方のトンネル ゾーンを***Source Zone*** **(送信元ゾーン)** として指定し、かつセキュリティポリシー ルールで両方のトンネル ゾーンを***Destination Zone*** **(宛先ゾーン)** として指定するか、両方の送信元および宛先ゾーンに対して***Any*** **(すべて)** を選択します。次に***Applications*** **(アプリケーション)** を指定してください。
7. トンネル宛先ゾーン用セキュリティポリシー ルールの設定を行います。トンネル送信元ゾーン用のセキュリティポリシー ルールを設定するため以前のステップ で紹介したヒントが、トンネル宛先ゾーンにも当てはまります。

STEP 9 | 任意）内側のコンテンツ用にトンネル送信元ゾーンおよびトンネル宛先ゾーンを指定します。

1. 先ほど内部コンテンツ用のゾーンとして追加したトンネル送信元ゾーンおよびトンネル宛先ゾーンを指定します**Policies (ポリシー)** > **Tunnel Inspection (トンネル検査)** を選択し、作成した Tunnel Inspection (トンネル検査) ポリシールールの**Name (名前)** を**General** （全般） タブで選択します。
2. **Inspection (検査)** を選択します。
3. **Security Options (セキュリティ オプション)** を選択します。
4. 内部コンテンツの送信元が指定した**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が指定した**Tunnel Destination Zone**（トンネル宛先ゾーン） に属すようにするために**Enable Security Options (セキュリティ オプションの有効化)** （デフォルトでは無効）を行います。

   Enable Security Options (セキュリティ オプションの有効化)を行わない場合、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送信元ゾーンに属し、内部コンテンツの宛先は外部トンネルの宛先と同じ宛先ゾーンに属します。つまり、それらの外部ゾーンに同じセキュリティポリシールールが適用されます。
5. **Tunnel Source Zone**（トンネル送信元ゾーン）の場合、トンネル送信元ゾーンに適用されるそのゾーンにポリシーを適用させるために前のステップで作成した、適切なトンネル ゾーンを選択します。上記以外の場合、デフォルトでは、内部コンテンツは外部トンネルで使用されているのと同じ送信元ゾーンを使用し、外部トンネル ソース ゾーンのポリシーは内部コンテンツ ソース ゾーンにも適用されます。
6. **Tunnel Destination Zone**（トンネル宛先ゾーン）の場合、トンネル宛先ゾーンに適用されるそのゾーンにポリシーを適用させるために前のステップで作成した、適切なトンネル ゾーンを選択します。上記以外の場合、デフォルトでは、内部コンテンツは外部ト

ンネルで使用されているのと同じ宛先ゾーンを使用し、外部トンネル ソース ゾーンのポリシーは内部コンテンツ ソース ゾーンにも適用されます。

トンネル検査ポリシー ルール用に***Tunnel Source Zone*** **(**トンネル送信元ゾーン**)** および***Tunnel Destination Zone*** **(**トンネル宛先ゾーン**)** を設定する場合***Any*** **(**すべて**)** の***Source Zone*** **(**送信元ゾーン**)** および***Any*** **(**すべて**)** の***Destination Zone*** **(**宛先ゾーン**)** を指定する代わりに、トンネル検査ポリシー ルールの一致条件にて特定の***Source Zone*** **(**送信元ゾーン**)** (ステッ3 にて)および特定の***Destination Zone*** **(**宛先ゾーン**)** (ステッ4 にて) を設定する必要があります。これにより、必ずゾーン再割り当ての方向が適切に親ゾーンと対応するようになります。

PA-5200 Series または *PA-7080* ファイアウォールでは、*VXLAN* の検査中にマルチキャストアンダーレイを使用すると、内部セッションが複数のデータプレーンで複製され、競合状態が発生する可能性があります。一部のパケットのドロップを回避するには、次の要件が適用されます。

- 各 *VXLAN* トンネルエンドポイント *(VTEP)* に向かう外部 *VXLAN* パケットと一致するように、個別のトンネルコンテンツ検査ルールを構成する必要があります。
- 別のルールでは、トンネルゾーンを割り当てます。異なるトンネルゾーンを使用すると、エンドポイントごとに内部セッションが異なります。競合状態は発生せず、パケットのドロップは見られません。

7. **OK** をクリックします。

STEP 10 | トンネル検査ポリシー ルールに一致するトラフィックの監視オプションを設定します。

1. **Policies (**ポリシー**)** > **Tunnel Inspection (**トンネル検査**)** を選択し、作成した Tunnel Inspection (トンネル検査) ポリシールールを選択します。
2. **Inspection (**検査**)** > **Monitor Options (**監視オプション**)** を選択します。
3. ロギングおよびレポートを目的として**Monitor Name (**モニター名**)** を入力し、類似のトラフィックをグループ化します。
4. 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**Monitor Tag (number) (**監視タグ（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。

   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、*VXLAN* ヘッダーの *VNI ID* を自動的に使用します。

   トンネル トラフィックをタグ付けする場合、後でトンネル検査ログ内の *Monitor Tag* (監視タグ) でフィルタリングし、*ACC* を使用して監視タグに基づいてトンネル アクティビティを確認することができます。
5. 選択したトンネル検査ポリシー ルールに一致するセッションのロギングおよびログ転送オプションを有効にするには**Override Security Rule Log Setting**（セキュリティ ルールのログ設定のオーバーライド）を行います。この設定を選択しない場合、トンネルログの生成とログ転送は、トンネルのトラフィックに適用されるセキュリティ ポリ

シー ルールのログ設定によって決定されます。トンネル ログをトラフィック ログとは別に保存するようにトンネル検査ログ設定を構成することにより、トラフィック ログを制御するセキュリティ ポリシー ルールのログ転送設定をオーバーライドできます。トンネル検査ログには、外部トンネル (GRE、非暗号化 IPSec、VXLAN、または GTP-U) セッションが保存され、トラフィック ログには内部トラフィック フローが保存されます。

6. **Log at Session Start (**セッション開始時にログ**)**を選択すると、セッションの開始時にトラフィックをログに記録します。

   セッション開始時とセッション終了時の両方にログを記録しておくのがトンネル ログのベストプラクティスです。これは、トンネルが長時間にわたって滞留す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記録しないと、*ACC* では、アクティブな *GRE* トンネルが存在しません。

7. **Log at Session End(**セッション終了時にログ**)**を選択すると、セッションの終了時にトラフィックをログに記録します。
8. ファイアウォールがトンネル検査ルールに適合するセッションのトンネルログを転送する場所を決定す**Log Forwarding**（ログ転送）プロファイルを選択します。あるいログ転送を設定する場合は、新しいログ転送プロファイルを作成することもできます。
9. **OK** をクリックします。

STEP 11 | 任意、VXLAN のみ**)VXLAN ID (VNI)** を設定します。デフォルトでは、すべての VXLAN ネットワークインターフェイス (VNI) が検査されます。1 つ以上の VXLAN ID を設定すると、ポリシーはそれらの VNI のみを検査します。

VXLAN プロトコルのみがトンネル *ID* タブを使用して *VNI* を指定します。

1. **Tunnel Id (**トンネル **ID)** タブを選択し**Add (**追加**)** をクリックします。
2. **Name (**名前**)** を割り当てます。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。
3. **VXLAN ID (VNI)** フィールドで、単一の VNI、コンマ区切りの VNI のリスト、 VNI の範囲 (ハイフンを区切り文字として使用)、あるいはこれらを組み合わせて入力します。例えば、次の項目の指定が可能です：

   1677002、1677003、1677011-1677038、1024

STEP 12 | 任意**Rematch Sessions (**セッションの再マッチング**)** を有効化**Device (**デバイス**)** > **Setup (**セットアップ**)** > **Session (**セッション**)**）した場合は、トンネル検査ポリシーを有効化したり編集したりする際にファイアウォールが既存のセッションをドロップしないよう、トンネルのセキュリティ ポリシー ルールを制御するゾーンの**Reject Non-SYN TCP (**非 **SYN TCP** の拒否**)** を無効化します。

以下の場合、ファイアウォールが次の警告を表示します。

- トンネル検査ポリシー ルールを作成します。

- **Protocol (**プロトコル**)** を追加する、あるいは**Maximum Tunnel Inspection Levels (**最大トンネル検査レベル**)** を**One Level (1** レベル**)** から**Two Levels (2** レベル**)** に増やすことで、トンネル検査ポリシーを編集します。
- **Security Options (**セキュリティ オプション**)** タブで、新しいゾーンを追加するか、あるゾーンを別のゾーンに変更し**Enable Security Options (**セキュリティ オプションの有効化**)** を行います。

警告:既存のトンネル セッションでトンネル検査ポリシーを有効化すると、トンネル内の既存の *TCP* セッションが *non-syn-tcp* フローとして扱われるようになります。トンネル検査ポリシーが有効化される際に既存のセッションがドロップされないよう、ゾーン プロテクション プロファイルを使用してゾーンの***Reject Non-SYN TCP (***非 ***SYN TCP*** の拒否**)** 設定を***no*** にし、トンネルのセキュリティ ポリシーを制御するゾーンにそれを割り当てます。既存のセッションがファイアウォールで認識されると***Reject Non-SYN TCP (***非 ***SYN TCP*** の拒否**)** 設定を***yes (***はい**)** または***global (***グローバル**)** に設定して再有効化できます。

1. **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**)** を選択してプロファイルを**Add (**追加**)** します。
2. プロファイル**Name**（名前）を入力します。
3. **Packet Based Attack Protection (**パケット ベースの攻撃防御**)** > **TCP Drop (TCP** ドロップ**)** を選択します。
4. **Reject Non-SYN TCP (**非 **SYN TCP** の拒否**)** については**no (**いいえ**)** を選択します。
5. **OK** をクリックします。
6. **Network (**ネットワーク**)** > **Zones (**ゾーン**)** を選択し、トンネルのセキュリティ ポリシー ルールを制御するゾーンを選択します。
7. **Zone Protection Profile (**ゾーン プロテクション プロファイル**)** については、先ほど作成したゾーン プロテクション プロファイルを選択します。
8. **OK** をクリックします。
9. 前の 3 つのサブステップ (12f、 12g、 12h) を繰り返し、トンネルのセキュリティ ポリシー ルールを制御する追加のゾーンにゾーン保護プロファイルを適用します。
10. ファイアウォールが既存のセッションを認識した後**Reject Non-SYN TCP (**非 **SYN TCP** の拒否**)** を**yes (**はい**)** または**global (**グローバル**)** に設定して再有効化できます。

STEP 13 | 任意）トンネル内のトラフィックのフラグメンテーションを制限します。

1. **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**)** を選択し**Name (**名前**)** でプロファイルを**Add (**追加**)** します。
2. **Description (**説明**)** を入力します。
3. **Packet Based Attack Protection (**パケット ベースの攻撃防御**)** > **IP Drop (IP**ドロップ**)** > **Fragmented traffic (**フラグメント化されたトラフィック**)** を選択します。
4. **OK** をクリックします。
5. **Network (**ネットワーク**)** > **Zones (**ゾーン**)** を選択し、フラグメンテーションを制限したいトンネル ゾーンを選択します。
6. **Zone Protection Profile (**ゾーン プロテクション プロファイル**)** については、先ほど作成したプロファイルを選択し、そのゾーン プロテクション プロファイルをトンネル ゾーンに適用します。
7. **OK** をクリックします。

STEP 14 | 変更を**Commit (**コミット**)** します。

検査済みのトンネル アクティビティを表示

次の各作業を行い、検査済みのトンネルのアクティビティを表示します。

STEP 1 | **ACC** を選択し、さらに単体の **Virtual System (**仮想システム**)** あるいは **All (**すべて**)** の仮想システムを選択します。

STEP 2 | Tunnel Activity (トンネル アクティビティ) を選択します。

STEP 3 | Last 24 Hrs (直近の 24 時間) や Last 30 Days (直近の 30 日) など、表示する Time period (期間) を選択します。

STEP 4 | グローバルフィルターの場合は + あるいは - ボタンをクリックして、トンネル アクティビティで ACC フィルタを使用できます。

STEP 5 | 検査済みのトンネル アクティビティを表示します。各ウィンドウのデータは、**bytes (**バイト**)**、**sessions (**セッション**)**、**threats (**脅威**)**、**content (**コンテンツ**)**、あるいは **URLs** に基づいて表示・並び替えできます。各ウィンドウに、トンネル データの異なる側面がグラフと表形式で表示されます。

- **Tunnel ID Usage (**トンネル **ID** 使用状況**)**—トンネル プロトコル毎に、そのプロトコルを使用しているトンネルのトンネル ID が一覧表示されます。表にはそのプロトコルの合計バイト数、セッション、脅威、コンテンツ、および URL が表示されます。トンネル ID にカーソルを合わせると、トンネル ID 毎の内訳が表示されます。
- **Tunnel Monitor Tag (**トンネル監視タグ**)**—トンネル プロトコル毎に、タグを使用しているトンネルのトンネル監視タグが一覧表示されます。表にはそのタグおよびプロトコルの合計バイト数、セッション、脅威、コンテンツ、および URL が表示されます。トンネル監視タグにカーソルを合わせると、タグ毎の内訳が表示されます。
- **Tunneled Application Usage (**トンネルを使用するアプリケーションの使用状況**)**—アプリケーション カテゴリ毎に、メディアにグループ化されたアプリケーションのタイプ、一般利益、コラボレーション、ネットワーキングが、リスクに基づいて色分けしてグラフィカルに表示されます。アプリケーション表には、アプリケーション毎のユーザー数も含まれます。
- **Tunneled User Activity (**トンネルを使用するユーザーアクティビティ**)**—日時をX軸にするなどの形式で送信バイト数、受信バイト数がグラフで表示されます。グラフのポイントにカーソルを合わせると、そのポイントのデータが表示されます。送信元ユーザーおよび宛先ユーザーの表は、ユーザー毎のデータを提供します。
- **Tunneled Source IP Activity (**トンネルを使用する送信元 **IP** アクティビティ**)**—ある IP アドレスの攻撃者からなどの、バイト数、セッション、脅威がグラフと表形式で表示されます。グラフのポイントにカーソルを合わせると、そのポイントのデータが表示されます。
- **Tunneled Destination IP Activity (**トンネルを使用する宛先 **IP** アクティビティ**)**—宛先 IP アドレスに基づいてグラフと表が表示されます。例えば、ある IP アドレスの被害者に関する脅威を表示します。グラフのポイントにカーソルを合わせると、そのポイントのデータが表示されます。

ログでトンネル情報を閲覧

トンネル検査ログ自身、あるいは他の種類のログのトンネル検査情報を表示できます。

GRE、非暗号化 **IPSec**、**GTP-U** プロトコル

- TCI トラフィックルールが一致すると、GRE、IPSec、および GTP-U プロトコルは、トンネル ログタイプ、一致したプロトコル、および設定されたモニタ名とモニタタグ (番号) とともにトンネル検査ログに記録されます。
- TCI ルールが一致しない場合、すべてのプロトコルはトラフィックログに記録されます。

VXLAN プロトコル

- TCI トラフィックルールが一致すると、VXLAN プロトコルは、トンネル (VXLAN) ログタイプ、設定されたモニタ名、およびトンネル ID (VNI) とともにトンネル検査ログに記録されます。

  内部セッションのトラフィックログでは、トンネル検査済みフラグは VNI セッションを示します。親セッションは、内部セッションが作成時にアクティブだったセッションであるため、ID は現在のセッション ID と一致しない可能性があります。
- TCI ルールが一致しない場合、VNI セッションは UDP プロトコル、送信元ポート 0、および送信先ポート 4789 (デフォルト) でトラフィックログに記録されます。

トンネル検査ログの表示

1. **Monitor (監視)** > **Logs (ログ)** > **Tunnel Inspection (トンネル検査)** を選択してログデータを表示し、トラフィックで使用されたトンネル **Applications (アプリケーション)**や、ヘッダの厳密なチェックに失敗した大量のパケット数などの懸念事項を特定します。
2. Detailed Log View (ログの詳細ビュー) をクリックして、ログの詳細を表示します。

他のログのトンネル検査情報を表示します。

1. **Monitor (監視)** > **Logs (ログ)**を選択します。
2. **Traffic (トラフィック)**、**Threat (脅威)**、**URL Filtering (URL フィルタリング)**、**WildFire Submissions (WildFire 送信)**、**Data Filtering (データ フィルタリング)**、あるいは **Unified (未定義)** を選択します。
3. ログ エントリについては、Detailed Log View (ログの詳細ビュー) () をクリックします。
4. Flags (フラグ) ウィンドウで、**Tunnel Inspected (トンネル検査済み)** フラグにチェックが入っているかどうか確認します。トンネル検査済みフラグは、ファイアウォールがトンネル検査ポリシー ルールを使用して内部コンテンツあるいは内側のトンネルを検査したことを示します。親セッション情報は、外側のトンネル（内側のトンネルと比較）あるいは内側のトンネル（内部コンテンツと比較）についてのものです。

   Traffic (トラフィック)、**Threat (脅威)**、**URL Filtering (URL フィルタリング)**、**WildFire Submissions (WildFire 送信)**、**Data Filtering (データ フィルタリング)** ログでは、内部セッション ログの Detailed Log View (ログの詳細ビュー) に直接の親の情報のみが表示され、トンネル ログ情報は表示されません。2 レベルのトンネル検査を設定した場合、この直接の親の親セッションを選択して 2 つ目の親のログを表示できます。（前

のステップで示した通り、**Tunnel Inspection (**トンネル検査**)** ログを監視してトンネルログ情報を表示する必要があります）

5. トンネル点検が行われている内部セッションのログを表示している場合は、General (全般) セクションの **View Parent Session (**親セッションを表示**)** をクリックすることで、外部セッションの情報を閲覧できます。

タグ付けされたトンネル トラフィックに基づいてカスタム レポートを作成

トンネル トラフィックに適用したタグに基づいて情報を収集するレポートを作成できます。

STEP 1 | **Monitor (監視)** > **Manage Custom Reports** を選択して、**Add (追加)** をクリックします。

STEP 2 | Database (データベース) については、Traffic (トラフィック)、Threat (脅威)、URL、Data Filtering (データ フィルタリング)、あるいは WildFire Submissions (WildFire 送信) ログを選択します。

STEP 3 | Available Columns (利用可能列) については Flags (フラグ) および Monitor Tag (監視タグ) を、レポートに必要な他のデータと共に選択します。

カスタムレポートを生成することもできます。

トンネル アクセラレーションを無効化

デフォルトでは、サポートされているファイアウォールはトンネル アクセラレーションを実行して、GRE トンネル、VXLAN トンネル、および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とスループットを向上させます。トンネル アクセラレーションは、ハードウェアオフロードを提供して、フロー ルックアップの実行にかかる時間を短縮し、内部トラフィックに基づいてトンネル トラフィックをより効率的に分散できるようにします。

GRE および VXLAN トンネル アクセラレーションは、PA-3200シリーズ ファイアウォールおよび PA-7000-100G-NPC-A および PA-7050-SMC-B または PA-7080-SMC-B を備えたPA-7000 シリーズ ファイアウォールでサポートされています。トラブルシューティングのためにトンネル アクセラレーションを無効にすることができます。トンネルアクセラレーションを無効にすると、GRE、VXLAN、および GTP-U トンネルに対して同時に無効になります。

STEP 1 | **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) を編集します。

STEP 2 | 無効にするには、**Tunnel Acceleration (トンネル アクセラレーション)** を選択解除します。

STEP 3 | **OK** をクリックします。

STEP 4 | **[コミット]** します。

STEP 5 | ファイアウォールを再起動します。

STEP 6 | (オプション) トンネル アクセラレーションのステータスを検証します。

1. CLI へのアクセスを行います。
2. **> show tunnel-acceleration**

   システム出力は `Enabled (有効)` または `Disabled (無効)` です。GTP-U 限定の追加のステータスと理由は次の通りです:

   - `Disabled (無効)`—GTP-U トンネル アクセラレーションがファイアウォールのモデルでサポートされていないか、GTP セキュリティが無効です。
   - エラー(`GTP-U が予期せず設定された TCI`) -GTP-U プロトコルを使用した TCI はトンネル アクセラレーションが有効になっているときに設定されます。
   - `Enabled (有効)`—トンネル アクセラレーションが有効になっています。GTP-U トンネル アクセラレーションは未実行です。GTP セキュリティは有効ですが、まだ再起動していません。
   - `Installed (インストール済み)`—GTP-U トンネル アクセラレーションは実行中です。

ネットワークパケットブローカー

Network Packet Broker は、ネットワークトラフィックをフィルタリングして、1 つ以上のサードパーティ製セキュリティアプライアンスの外部セキュリティチェーンに転送します。Network Packet Broker は、PAN-OS 8.1 で導入された Decryption Broker 機能を置き換え、転送の非復号化 TLS トラフィックと非 TLS トラフィック (クリアテキスト) と TLS トラフィックの暗号化解除を含むように機能を拡張します。あらゆる種類のトラフィックを処理する機能は、金融や政府機関などの非常に高いセキュリティ環境で特に価値があります。

Net!work P!acket B!rokerはPA-7000シリーズ、PA-5400シリーズ、PA-5200シリーズ、PA-3200シリーズの装置およびVM-300およびVM-700モデルのために支えられている。ファイアウォールが信頼できるサードパーティ（または中間者）としてセッション トラフィックに確立されている場合は、SSL 転送プロキシの復号化を有効にする必要があります。

ファイアウォールのインターフェイスを復号化ブローカーと *GRE* トンネル エンドポイントの両方にすることはできません。

Network Packet Broker 概要

セキュリティ スイート全体の一部として 1 つ以上のサードパーティ製セキュリティ アプライアンス (セキュリティ チェーン) を使用する場合は、Network Packet Broker を使用して、ネットワーク トラフィックをフィルタリングし、それらのセキュリティ アプライアンスに転送できます。Network Packet Broker は PAN-OS 8.1 で導入された復号化ブローカー機能を置き換えます。

Decryption B!ローカーのように、Network Packet Brokerは復号化機能とセキュリティチェーン管理を提供します。これにより、これらの機能に専用デバイスをサポートする複雑さを排除し、資本コストと運用コストを削減することで、ネットワークを簡素化できます。また、Decryption Broker、Network Packet Brokerのように、セキュリティチェーンへのパスが正常であることを確認するためのヘルスチェックと、チェーンがダウンした場合のトラフィックを処理するためのオプションを提供します。

Network Packet Broker はファイアウォールのセキュリティ チェーン転送機能を拡張し、暗号化解除された TLS トラフィックだけでなく、非復号された TLS および非 TLS (クリアテキスト) トラフィックをアプリケーション、ユーザー、デバイス、IP アドレス、およびゾーンに基づいて 1 つ以上のセキュリティ チェーンにフィルタリングおよび転送できるようにします。これらの機能は、金融や政府機関などの非常に高いセキュリティ環境で特に価値があります。

アップグレードとダウングレード:

- Decryption Broker ライセンスを持つファイアウォールで PAN-OS 10.1 にアップグレードする場合:
  - ファイアウォールを再起動すると、ライセンス名が自動的に Network Packet Broker に変更されます。

    ファイアウォールがスタンドアロン ファイアウォールであるか、*HA* ペアの一部であるか、または *Network Packet Broker* ライセンスをパノラマからファイアウォールにプッシュした場合でも、ファイアウォールを再起動してライセンスを有効にし、ユーザー インターフェイスを更新する必要があります。
  - PAN-OSは、既存のDecryption Broker Forwardingプロファイル(プロファイル > **Decryption** > **Forwarding Profile**)をPacket Brokerプロファイルに変換します。
  - PAN-OS は、セキュリティチェーンへのトラフィックを Network Packet Broker ポリシールールに転送するための既存の Decryption P!オリシールールを変換します。
  - PAN-OSは、ユーザーインターフェイスからDecryption Brokerプロファイルを削除し、Packet Brokerプロファイル(プロファイル > **Packet Broker**)に置き換え、Network Packet Brokerポリシー(**Policies** > **Network Packet Broker**)を追加します。

- PAN-OS 10.1 から PAN-OS 10.0 にダウングレードすると、次のようになります。
  - PAN-OS は、既存の Packet Broker プロファイルを Decryption Broker Forwarding プロファイルに変換します。
  - PAN-OS は、Network Packet Broker ルールベースを削除し、警告メッセージを出力します。Network Packet Broker ポリシールールをDecryption ForwardingのDecryptionポリシールールとして再構成する必要があります。
  - ライセンス名はNetwork Packet Brokerのままです(ライセンス名は再起動後のすべてのPAN-OSバージョンでDecryption BrokerからNetworkパケットブローカーに変更され、Decryption Brokerの動作には影響しません)。ただし、機能は Decryption Broker 機能であり、Network Packet Broker 機能ではありません。
  - PAN-OS は、ユーザー インターフェイスから Network Packet Broker プロファイルを削除し、Decryption Forwarding プロファイルに置き換え、ユーザー インターフェイスから Network Packet Broker ポリシーを削除します (置換はありません。

Network Packet Broker を使用するための要件:

- ファイアウォールに無料の Packet Broker ライセンスをインストールする必要があります。無料ライセンスがないと、インターフェイスの Packet Broker ポリシーとプロファイルにアクセスできません。
- ファイアウォールには、パケット ブローカ転送インターフェイスの専用ペアとして使用するために、少なくとも 2 つの使用可能なレイヤ 3 Ethernet インターフェイスが必要です。
  - 複数のペアの専用の Network Packet Broker 転送インターフェイスを設定して、異なるセキュリティ チェーンに接続できます。
  - 各セキュリティ チェーンに対して、専用の Network Packet Broker インターフェイスのペアは、同じセキュリティ ゾーン内になければなりません。
  - 専用インターフェイスのペアは、セキュリティ チェーン内の最初のデバイスと最後のデバイスに接続します。

  Network Packet ブローカーは、ルーティングされたレイヤ *3* セキュリティ チェーンと *Transparent Bridge Layer 1* セキュリティ チェーンをサポートしています。ルーティングされたレイヤ *3* チェインの場合、*1* 組のパケット ブローカ転送インターフェイスは、適切に設定されたスイッチ、ルータ、またはその他のデバイスを使用して、ファイアウォールとセキュリティ チェーンの間で必要なレイヤ *3* ルーティングを実行することで、複数のレイヤ *3* セキュリティ チェーンに接続できます。
- 専用 Network Packet Broker 転送インターフェイスは、動的ルーティング プロトコルを使用できません。
- ファイアウォールは変更されたセッションを元のセッションと一致させることができないため、トラフィックをドロップするため、セキュリティ チェーン内のデバイスはいずれも元のセッションの送信元または宛先 IP アドレス、送信元または宛先ポート、またはプロトコルを変更できません。

Network Packet Broker は次をサポートしています。

- TLS の復号、非復号 TLS、および TLS 以外のトラフィック。

- SSL Forward Proxy、SSL インバウンドインスペクション、および暗号化された SSH トラフィック。
- ルーティングされたレイヤ 3 セキュリティ チェーン。
- Transparent Bridge レイヤ 1 セキュリティ チェーン。

  ルーティング レイヤ *3* とレイヤ *1 Transparent Bridge* セキュリティ チェインを同じファイアウォール上に設定できますが、タイプごとに異なるペアのフォワーディング インターフェイスを使用する必要があります。

- チェーンを通る単方向トラフィック フロー: チェーンへのすべてのトラフィックは、1 つの専用インターフェイスでファイアウォールを送信し、別の専用インターフェイスのファイアウォールに戻るので、すべてのトラフィックは専用の Network Packet Broker インターフェイスのペアを通って同じ方向に流れます。

  ファイアウォール転送インターフェイスは、どちらも同じゾーンになければなりません。

- セキュリティ チェーンを通る双方向トラフィック フロー:
  - Client-to-server(c2s)トラフィックは、1 つの専用ファイアウォール ブローカ インターフェイスでファイアウォールを送信し、別の専用ファイアウォール ブローカ インターフェイスのファイアウォールに戻ります。
  - Server-to-client(s2c)トラフィックは、c2sトラフィックと同じ2つの専用ファイアウォールブローカーインターフェイスを使用しますが、トラフィックはセキュリティチェーンを通して反対方向に流れます。s2c トラフィックがチェーンに送信されるファイアウォール ブローカ インターフェイスは、c2s トラフィックがチェーンからファイアウォールに戻るインターフェイスと同じです。s2c トラフィックがファイアウォールに戻るファイアウォール ブローカ インターフェイスは、c2s トラフィックがチェーンに送信されるインターフェイスと同じです。

    ファイアウォール転送インターフェイスは、どちらも同じゾーンになければなりません。

Network Packet Broker はマルチキャスト、ブロードキャスト、または復号化された *SSH* トラフィックをサポートしていません。

ネットワーク パケット ブローカーのしくみ

サードパーティ製のセキュリティ デバイスのチェーンにファイアウォールを接続するための高度なワークフローは次のとおりです。

1. 転送する非復号化 TLS、復号化された TLS、および TLS (TCP および UDP) 以外のトラフィックを識別します。
2. セキュリティ チェーン トポロジを識別します。各セキュリティ チェーンのデバイスがトラフィックを透過的に転送するか (ブリッジング)するか、デバイスがレイヤ 3 情報に基づいてトラフィックをルーティングするかを決定します。複数のセキュリティ チェーンを使用すると、トラフィックの負荷分散に役立ちます。さらに、セキュリティ チェーンをバイパスするか (トラフィックはファイアウォールで通常の処理を通過し、それに応じて転送またはブロックされます)、またはセキュリティ チェーンがヘルスチェックに失敗した場合にトラフィックをブロックするかどうかを決定します。
3. セキュリティ チェーンにトラフィックを転送するファイアウォールに、空きネットワーク パケット ブローカー ライセンスをインストールします。
4. 1 つ以上のファイアウォール インターフェイスのペアを識別して、トラフィックを 1 つ以上のセキュリティ チェーンに転送し、それらのインターフェイスでネットワーク パケット ブローカを有効にします。
5. 少なくとも 1 つのパケット ブローカ プロファイルを設定します。
6. 少なくとも 1 つのネットワーク パケット ブローカ ポリシーを設定します。

サードパーティ製のセキュリティ デバイスのチェーンを使用してトラフィックを検査するには、ファイアウォール上に次の 3 つのオブジェクトを設定します。

- インターフェイス :ファイアウォールからセキュリティ チェーンにトラフィックを転送し、処理されたトラフィックをセキュリティ チェーンから受信するためのレイヤ 3 イーサネット ファイアウォール インターフェイスの 1 つまたは複数のペア。プロファイルにインターフェイス ペアを指定する必要があるため、プロファイルとポリシー ルールを設定する前に、ネットワーク パケット ブローカ インターフェイス ペアを設定します。
- パケット ブローカー プロファイル :プロファイルは、ポリシーで定義したトラフィックをセキュリティ チェーンに転送する方法を制御します。各ネットワーク パケット ブローカ ポリシー ルールには、関連付けられたパケット ブローカ プロファイルがあります。プロファイルは、セキュリティ チェーンがルーティング レイヤ 3 チェーンかレイヤ 1 トランスペアレント ブリッジ チェーンか、チェーンを通過するトラフィックの方向(単方向または双方向)、専用のネットワーク パケット ブローカ ファイアウォール インターフェイス、およびファイアウォールとセキュリティ チェーン間の接続のヘルスを監視する方法を定義します。複数のルーティングされたレイヤ 3 セキュリティ チェーンの場合、各チェーンの最初と最後のデバイスと、関連付けられたトラフィックに対してセッション配信(ロード バランシング)方法を指定できます。
- ネットワーク パケット ブローカ ポリシー ルール –ポリシー ルールは、各セキュリティ チェーンに転送するアプリケーション トラフィックを定義するか、または複数のルーティングされた(レイヤ 3)チェーンのロード バランシングを行います。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の送信元と宛先、ユーザー、アプリケーション、およびサービスを定義します。ポリシー ルールは、セキュリティ チェーンに転送する

トラフィックの種類も定義します。復号化された TLS トラフィック、非復号 TLS トラフィック、TLS 以外のトラフィック、またはトラフィックタイプの任意の組み合わせを選択できます。また、各ポリシー ルールにパケット ブローカ プロファイルを追加して、トラフィックを転送するセキュリティ チェーン (およびその他すべてのプロファイル特性) を指定します。

ポリシー オプティマイザー を使用して、ネットワーク パケット ブローカ ポリシー ルールを確認および強化します。

ネットワーク パケット ブローカー ポリシー ルールにアプリケーション トラフィックを一致させるために、ネットワーク パケット ブローカーはファイアウォールの App-ID キャッシュ内のアプリケーションを参照します。アプリケーションが App-ID キャッシュにない場合、ファイアウォールはセキュリティ チェーンをバイパスし、セキュリティ ポリシーで構成されている脅威検査をトラフィックに適用します。アプリケーションが App-ID キャッシュ内にある場合、ファイアウォールは、ネットワーク パケット ブローカ ポリシー ルールと関連付けられたパケット ブローカ プロファイルで指定された方法で、セキュリティ チェーンにトラフィックを転送します。

非復号された TLS および TLS 以外のトラフィックの場合、ファイアウォールは最初のセッションで App-ID キャッシュにアプリケーションをインストールするため、ファイアウォールはネットワーク パケット ブローカー ポリシーとプロファイルで指定されたトラフィックを処理します。

TLS トラフィックの復号の場合、アプリケーションの の最初のセッション では、ネットワーク パケット ブローカーはセッションが復号化されていることを認識せず、"ssl" をアプリケーションとして認識します。基になる特定のアプリケーションはまだ認識されていないか、App-ID キャッシュにインストールされていないので、ブローカーの検索が失敗し、トラフィックはセキュリティ チェーンをバイパスします。トラフィックは、セキュリティ ポリシー許可ルールで設定された脅威インスペクションの対象となります。ファイアウォールがトラフィックを復号化すると、ファイアウォールは特定のアプリケーションを学習し、App-ID キャッシュにインストールします。同じアプリケーションの 2 番目以降の復号されたセッションでは、特定のアプリケーションが App-ID キャッシュに入り、ファイアウォールが想定どおりにトラフィックをセキュリティ チェーンに転送するため、ネットワーク パケット ブローカの検索は成功します。

Network Packet Broker を展開する準備をする

ネットワーク パケット ブローカーを展開する準備をするには、次の操作を実行します。

1. 無料の Network Packet Broker ライセンスを取得してアクティブ化します。
   1. カスタマーサポート ポータルにログインします。
   2. 左側のナビゲーション ペインで**Assets (アセット)** > **Devices (デバイス)**を選択します。
   3. 復号化ブローカーあるいは復号ポート ミラーリングを有効化するデバイスを探し、**Actions (アクション)**（鉛筆のアイコン）を選択します。
   4. ライセンスのアクティブ化で、**Activate Feature License** を選択します。
   5. **Network Packet Broker** 無料ライセンスを選択します。
   6. **Agree and Submit (同意して送信)** をクリックします。
2. ファイアウォールにライセンスをインストールします。
   1. **Device** > **Licenses** を選択します。
   2. **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）をクリックします。
   3. **Device** > **Licenses** ページに、**Network Packet Broker** ライセンスがファイアウォールでアクティブになったことを確認します。
   4. ファイアウォールを再起動します（**Device (デバイス)** > **Setup (セットアップ)** > **Operations (操作)**）。Network Packet Broker は、ファイアウォールが再起動するまで構成に使用できません。

      *Network PacketBroker*ライセンスを*Panorama*からマネージドファイアウォールにプッシュできます。ライセンスを有効にしてユーザー インターフェイスを更新するには、ファイアウォールを再起動する必要があります。
3. Network Packet Broker のアプリケーション ID キャッシュを有効にします。
   1. App-ID キャッシュは、既定では無効になっています。コンフィギュレーション モード CLI コマンドを使用して有効にします。

      ```
      admin@PA-3260# set deviceconfig setting application cache yes
      ```
   2. ファイアウォールで App-ID キャッシュを使用してアプリケーションを識別できるようにします。

      ```
      admin@PA-3260# set deviceconfig setting application use-cache-
      for-identification yes
      ```

   設定を確認すると、アプリケーション キャッシュ が はい に設定され、appid のキャッシュの使用が はい に設定されていることを確認します。

   ```
   admin@PA-3260> show running application setting
   Application setting:
   ```

```
Application cache              : yes
Supernode                      : yes
Heuristics                     : yes
Cache Threshold                : 1
Bypass when exceeds queue limit: no
Traceroute appid               : yes
Traceroute TTL threshold       : 30
Use cache for appid            : yes
Use simple appsigs for ident   : yes
Use AppID cache on SSL/SNI     : no
Unknown capture                : on
Max. unknown sessions          : 5000
Current unknown sessions       : 33
Application capture            : off
```

```
Current APPID Signature
   Memory Usage                : 16768  KB (Actual 16461  KB)
      TCP 1 C2S                : regex 11898  states
      TCP 1 S2C                : regex 4549   states
      UDP 1 C2S                : regex 4263   states
      UDP 1 S2C                : regex 1605   states
```

4. 1 つまたは複数のセキュリティ チェーンに転送するトラフィックを特定します。
5. 各セキュリティ チェーンのトポロジを特定し、ファイアウォールで設定するセキュリティ チェーンの種類を決定するレイヤ 1 Transparent Bridge 転送またはルーティング レイヤ 3 転送を使用するかどうかを決定します。考慮事項は次のとおりです。
   - 複数のチェーン間でトラフィックをロードバランスする場合(ルータ、スイッチ、またはその他のルーティング デバイスを介して複数のチェーン間でセッションを分散するためにルーティングレイヤ 3 セキュリティ チェーンを使用する)、単一のチェーンを使用するか、異なるタイプのトラフィックに異なるセキュリティ チェーンを使用します。複数レイヤ 1 Transparent Bridge チェーンの場合、レイヤ 1 接続はルーティングされないため、セキュリティ チェーンごとに専用のファイアウォール インターフェイスのペアが必要です。
   - セキュリティ チェーンを通じて単方向トラフィックフローと双方向トラフィック フローのどちらを使用するか。
6. 専用 Network Packet Broker 転送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ペアを決定します。。
   - レイヤ 1 Transparent Bridge チェーンの場合、各レイヤ 1 セキュリティ チェーンに専用のファイアウォール インターフェイスのペアが必要です。特定のトラフィックを異なるセキュリティ チェーンに送信するようにポリシー ルールを設定できます。
   - ルーティングされたレイヤ 3 チェインの場合、ファイアウォール インターフェイスの 1 つの専用ペアは、スイッチ、ルータ、またはその他のルーティング可能なデバイスを介して、複数のレイヤ 3 セキュリティ チェーン間のトラフィックをロード バランシングできます。
   - ルーティングされたレイヤ 3 チェーンの場合、複数のペアの専用ファイアウォール インターフェイスを使用して、異なるポリシー ルールを使用して特定のトラフィックを異なるセキュリティ チェーンに送信できます。

トランスペアレント ブリッジ セキュリティ チェーンの設定

レイヤ 1 トランスペアレント ブリッジ セキュリティ チェーンは、1 つのファイアウォール インターフェイスから、直接接続された一連のデータ検査およびセキュリティ デバイスの処理を介してトラフィックを転送し、トラフィックをルーティングすることなく別のファイアウォール インターフェイスを介して転送します。

レイヤ 1 トランスペアレント ブリッジ セキュリティ チェーンを設定する前に、Network Packet Broker を展開する準備をするに手順を実行し、ファイアウォールとセキュリティ チェーン デバイス間の物理的な接続が正しいことを確認します。

複数のトランスペアレント ブリッジ セキュリティ チェーンにセッションを分散するには、トラフィックの負荷分散に使用するセキュリティ チェーンごとに、ファイアウォール上に 1 つのレイヤ 1 トランスペアレント ブリッジ セキュリティ チェーンを作成します。ファイアウォール上の各トランスペアレント ブリッジ セキュリティ チェーンには、2 つの専用レイヤ 3 イーサネット インターフェイスが必要です。設定するトポロジーに十分な空きイーサネット・インターフェースがあることを確認します。

レイヤ 1 トランスペアレント ブリッジ セキュリティ チェーンはルーティングされないため、別のセキュリティ チェーンにフェールオーバーできません。

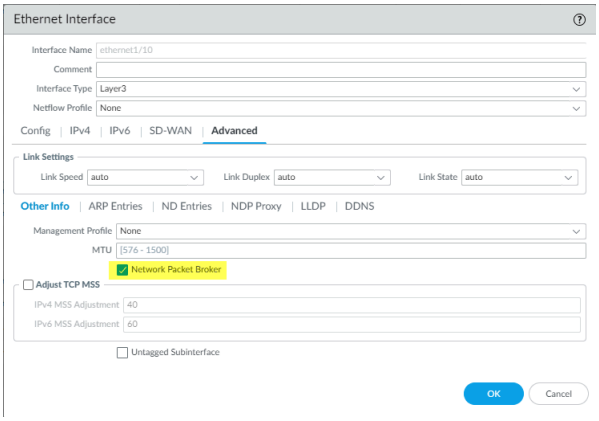
STEP 1 | ネットワーク パケット ブローカ転送インターフェイスとして 2 つのレイヤ 3 イーサネット インターフェイスを有効にします。

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. 2 つのネットワーク パケット ブローカ転送インターフェイスの 1 つとして使用する未使用のイーサネット 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. [**Config**] タブで、インターフェイスを割り当てるゾーンを選択します。

   同じゾーン内の両方のセキュリティ チェーン インターフェイスを設定する必要があります。
5. [**Config**] タブでは、ベスト プラクティスとして、インターフェイスを割り当てる専用の仮想ルータを使用するか、作成します。専用の仮想ルータを使用すると、ネットワーク パ

ケット ブローカ インターフェイス トラフィックが他のトラフィックから分離された状態に保たれます。

6. **Advanced** を選択し、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。



7. **OK** をクリックして、インターフェイス設定を保存します。
8. 別の未使用のイーサネット インターフェイスでこの手順を繰り返して、他のネットワーク パケット ブローカ転送インターフェイスを設定します。

STEP 2 | パケット ブローカ プロファイルを設定して、トラフィックをレイヤ 1 透過ブリッジ セキュリティ チェーンに転送する方法を制御します。

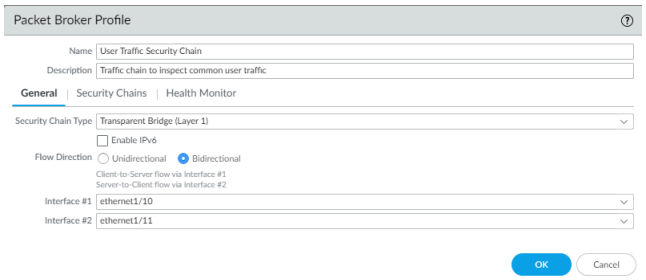
1. オブジェクト > パケット ブローカ プロファイル および 追加 新しいプロファイルを選択するか、既存のプロファイルを変更します。
2. プロファイルに 名前 と 説明 を指定して、目的を簡単に識別できるようにします。
3. 一般 タブで、次の手順を実行します。
   - セキュリティ チェーン タイプ として 透過ブリッジ**(**レイヤ **1)**を選択します。
   - トラフィックが **IPv6** トラフィックの場合は、**IPv6** を有効にします。
   - 流れ方向 を選択します。

     ネットワーク トポロジは、単方向フローと双方向フローのどちらを使用するかを決定します。どちらの方法でも、パフォーマンスはほぼ同じです。

     1 つのファイアウォール インターフェイスを使用して c2 と s2c の両方のセッション フローをセキュリティ チェーンに転送し、もう一方のファイアウォール インターフェイスを使用して両方のセッション フローをセキュリティ チェーンから受信するには、[単方向] を選択します。

     インターフェイス **#1** を使用してセキュリティ チェーンに c2s フローを転送し、セキュリティ チェーンから s2c フローを受信し、 インターフェイス **#2** を使用して s2c フローをセキュリティ チェーンに転送し、セキュリティ チェーンから c2s フローを受信するには、[双方向] を選択します。
   - インターフェイス **#1** および インターフェイス **#2** でネットワーク パケット ブローカ転送インターフェイス ペアを指定します。両方のインターフェイスを使用できるようにするには、ネットワーク パケット ブローカー (Network Packet Broker を展開する準

備をするを参照) を有効にしておく必要があります。どのインターフェイスが インターフェイス **#1**で、どのインターフェイスが インターフェイス **#2** を設定する場合は、フローの方向に注意してください。



4. セキュリティ チェーン タブは、トランスペアレント ブリッジには使用されません。
5. ヘルス モニタ タブで、次の手順を実行します。
   - 実行するヘルスモニタリングの種類を選択して、セキュリティ チェーンで障害が発生した場合の動作を制御できるようにします。パス監視 、**HTTP** モニタリング 、および **HTTP** モニタリング遅延 から 1 つ、2 つ、またはすべてを選択できます。

     パスモニタリング :ping を使用してデバイスの接続をチェックします。

     HTTP モニタリング :デバイスの可用性と応答時間をチェックします。

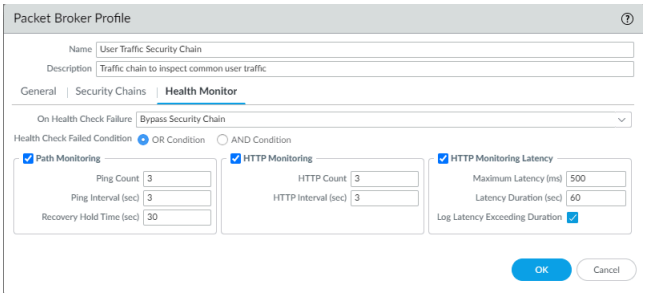
     HTTP モニタリング遅延 :デバイスの処理速度と効率をチェックします。このオプションを選択すると、**HTTP** モニタリング も自動的に有効になります。
   - 1 つ以上の種類の正常性監視を有効にすると、状態チェックの失敗 オプションがアクティブになり、セキュリティ チェーンのヘルス障害が発生した場合にファイアウォールがセキュリティ チェーン トラフィックを処理する方法が決まります。オプションは、バイパスセキュリティチェーンとブロックセッションです。

     バイパスセキュリティチェーン:ファイアウォールは、トラフィックをセキュリティ チェーンではなく宛先に転送し、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。

     選択する方法は、セキュリティ チェーンを通じてトラフィックを実行できない場合に、トラフィックをどのように処理するかによって異なります。
   - 複数のヘルスチェックオプションを選択する場合は、ファイアウォールでヘルスチェックが失敗したと見なす (ヘルスチェック失敗条件) が失敗条件 (**OR** 条件) を記録している場合、または選択したすべての監視オプションに失敗条件 (**AND** 条件) を記録する場合に選択します。たとえば、3 つのヘルスチェック オプションをすべて有効にし、そのうちの 1 つが失敗した条件を記録した場合、**OR** 条件 を選択した場合、ファイアウォールはセキュリティ チェーン接続が失敗したと見なし、**On Health Check Fail** で指

定したアクションを実行します。[**AND** 条件] を選択した場合、2 つの正常性メトリックは依然として問題ないので、ファイアウォールは接続が正常であると見なします。



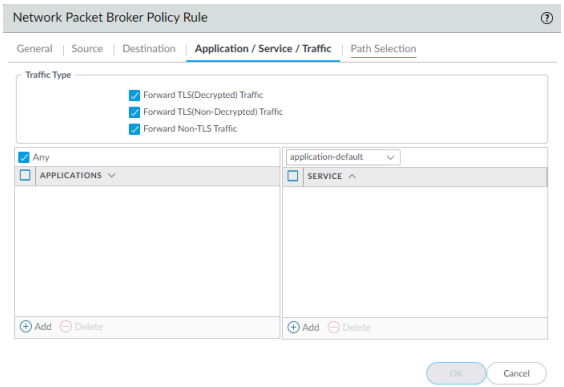
6. **OK** をクリックしてプロファイルを保存します。

STEP 3 | レイヤ 1 トランスペアレント ブリッジ セキュリティ チェーンに転送するトラフィックを定義するパケット ブローカ ポリシーを設定します。

1. ポリシー > ネットワーク パケット ブローカー と 追加 新しいポリシー ルールを選択するか、既存のポリシー ルールを変更します。
2. [**General**] タブで、ポリシー ルールに 名 と 説明 を指定して、目的を簡単に特定し、監査コメント を追加し、使用する場合はタグを適用します。
3. [**Source**] タブで、ルールをセキュリティ 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、およびデバイスを指定します。
4. [宛先] タブで、ルールをセキュリティ チェーンに転送するトラフィックの宛先ゾーン、IP アドレス、およびデバイスを指定します。
5. [アプリケーション/サービス/トラフィック] タブで、ルールをセキュリティ チェーンに転送するアプリケーションとサービスを指定します。内部カスタム アプリケーションなどの非標準ポートを使用することが予期されるルール制御アプリケーションを使用しない限り、ベスト プラクティスは、非標準ポートを使用して回避動作を示すアプリケーションがブロックされるように、**Service** を アプリケーションの既定の に設定することです。

   [トラフィック タイプ] で、ルールをセキュリティ チェーンに転送するトラフィックのタイプをすべて選択します。転送 **TLS(**復号された**)** トラフィック がデフォルトの選択で

す。転送 **TLS**(復号された) トラフィック 、 転送 **TLS**(非復号) 、および 転送非 **TLS** トラフィック の任意の組み合わせを選択して、セキュリティ チェーンに転送できます。



6. [**Path Selection**] タブで、ステップ 2 で作成したパケット ブローカ プロファイルを選択するか、ポリシールールがセキュリティ チェーンに制御するトラフィックの送信方法を制御する新しいプロファイルを作成します。

STEP 4 | ステップ 1 ~ ステップ 3 を繰り返して、より多くのレイヤー 1 のトランスペアレント ブリッジ セキュリティ チェーンを作成します。

各レイヤ 1 の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 パケット ブローカフォワーディング インターフェイスとして使用される 2 つのイーサネット インターフェイスは、各セキュリティ チェーン専用にする必要があります。トランスペアレント ブリッジ セキュリティ チェーンに使用されるイーサネット インターフェイスは、他の目的に使用したり、他のトラフィックを伝送したりすることはできません。
- ネットワーク パケット ブローカフォワーディング インターフェイスの各ペアは、1 つのレイヤ 1 トランスペア ブリッジ セキュリティ チェーンに接続します。

透過的なブリッジ セキュリティ チェーン間で比較的均等にトラフィックを分割するネットワーク パケット ブローカ ポリシー ルールを作成することで、トラフィックのロード バランシングを行うことができます。ポリシー ルールを使用して、特定のセキュリティ チェーンを通じて特定のトラフィックとトラフィックの種類を指示することもできます。

レイヤ *1* トランスペアレント ブリッジ セキュリティ チェーンはルーティングされないため、別のセキュリティ チェーンにフェールオーバーできません。トランスペアレント ブリッジ セキュリティ チェーンが失敗した場合のトラフィックの処理方法を設定するには、パケット ブローカ プロファイルの *[* ヘルス モニタ *]* タブを使用します。

ルーティングレイヤ 3 セキュリティ チェーンの設定

ルーティングされたレイヤ 3 セキュリティ チェーンは、トラフィックを一連のデータ検査および処理セキュリティ デバイスに転送し、ファイアウォール上の 2 つの専用転送インターフェイスを使用してファイアウォールに戻します。

ルーティングレイヤ 3 セキュリティ チェーンを設定する前に、Network Packet Broker を展開する準備をする に手順を実行し、ファイアウォールとセキュリティ チェーン デバイス間の物理的な接続が正しいことを確認します。構成するトポロジーに十分な空きイーサネット・インターフェースがファイアウォール上にあることを確認します。

ファイアウォール上に設定する各ルーティング レイヤ 3 セキュリティ チェーンには、2 つの専用レイヤ 3 イーサネット インターフェイスが必要であり、1 つのレイヤ 3 セキュリティ チェーンに接続したり、ファイアウォールとセキュリティ チェーンの間に適切に設定されたルータ、スイッチ、または類似のデバイスを使用して最大 64 のレイヤ 3 セキュリティ チェーンにセッションを分散 (ロード バランス) することができます。

ネットワーク パケット ブローカーは、ルーティングされたレイヤ *3* セキュリティ チェーン上の *IPv6* トラフィックを転送できません。*IPv6* トラフィックを転送するには、トランスペアレント ブリッジ*(*レイヤ *1)*セキュリティ チェーンを使用します。

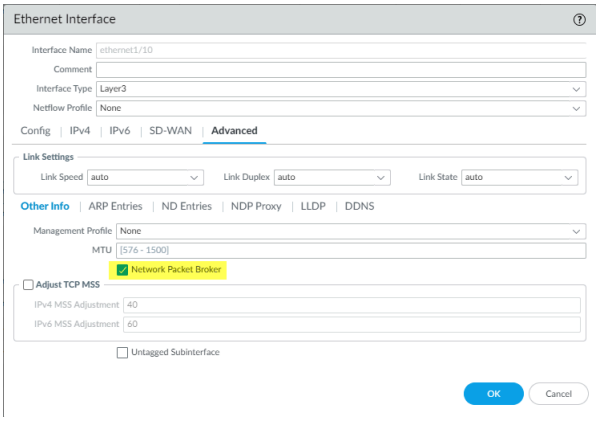
STEP 1 | ネットワーク パケット ブローカ転送インターフェイスとして 2 つのレイヤ 3 イーサネット インターフェイスを有効にします。

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. 2 つのネットワーク パケット ブローカ転送インターフェイスの 1 つとして使用する未使用のイーサネット 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. [**Config**] タブで、インターフェイスを割り当てるゾーンを選択します。

   同じゾーン内の両方のセキュリティ チェーン インターフェイスを設定する必要があります。
5. [**Config**] タブでは、ベスト プラクティスとして、インターフェイスを割り当てる専用の仮想ルータを使用するか、作成します。専用の仮想ルータを使用すると、ネットワーク パ

ケット ブローカ インターフェイス トラフィックが他のトラフィックから分離された状態に保たれます。

6. **Advanced** を選択し、 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。



7. **OK** をクリックして、インターフェイス設定を保存します。
8. 別の未使用のイーサネット インターフェイスでこの手順を繰り返して、他のネットワーク パケット ブローカ転送インターフェイスを設定します。

STEP 2 | ルーティングされたレイヤ 3 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制御するためにパケット ブローカ プロファイルを設定します。

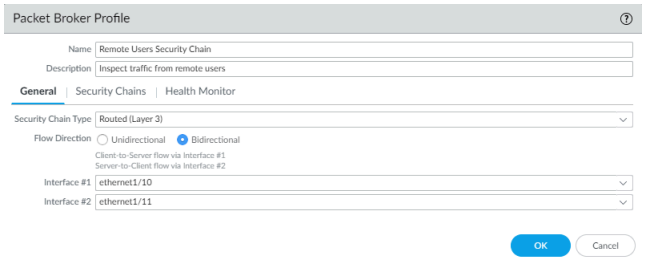
1. オブジェクト > パケット ブローカ プロファイル および 追加 新しいプロファイルを選択するか、既存のプロファイルを変更します。
2. プロファイルに 名前 と 説明 を指定して、目的を簡単に識別できるようにします。
3. 一般 タブで、次の手順を実行します。
   - セキュリティ チェーン タイプ として [ルーテッド **(レイヤ 3)]** を選択します。
   - 流れ方向 を選択します。

     ネットワーク トポロジは、単方向フローと双方向フローのどちらを使用するかを決定します。どちらの方法でも、パフォーマンスはほぼ同じです。

     1 つのファイアウォール インターフェイスを使用して c2 と s2c の両方のセッション フローをセキュリティ チェーンに転送し、もう一方のファイアウォール インターフェイスを使用してセキュリティ チェーンから両方のセッション フローを受信するには、[単方向] を選択します。

     インターフェイス **#1** を使用してセキュリティ チェーンに c2s フローを転送し、セキュリティ チェーンから s2c フローを受信し、インターフェイス **#2** を使用して s2c フローをセキュリティ チェーンに転送し、セキュリティ チェーンから c2s フローを受信するには、[双方向] を選択します。
   - インターフェイス **#1** および インターフェイス **#2** でネットワーク パケット ブローカ転送インターフェイス ペアを指定します。両方のインターフェイスを使用できるようにするには、ネットワーク パケット ブローカー (ステップ 1 を参照) を有効にしておく

必要があります。どのインターフェイスが インターフェイス **#1**で、どのインターフェイスが インターフェイス **#2** を設定する場合は、フローの方向に注意してください。

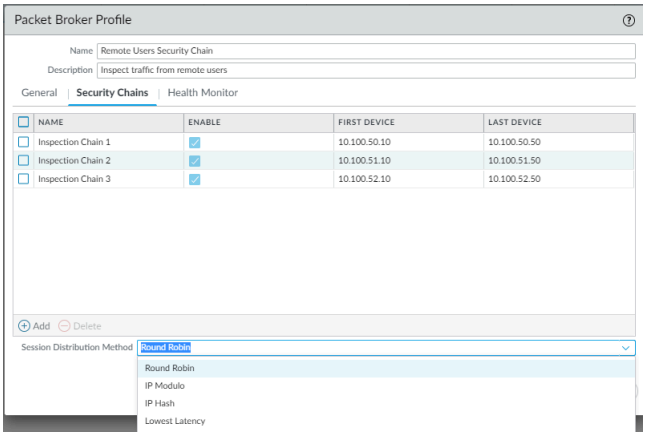


セッション配布 (負荷分散) は、新しいセッションにのみ適用されます。ファイアウォールは、セッションの途中でトラフィックの再調整を行いません。ファイアウォールは、ステータスが「*up*」(アクティブ、正常) になっているセキュリティ チェーンにのみセッションを配布します。

4. [セキュリティ チェーン] タブで、接続するルーティングされた各レイヤ **3** セキュリティ チェーンの最初と最後のデバイスの **IP** アドレスを 追加します。少なくとも 1 つのセキュリティ チェーンを指定する必要がありますまたは、ファイアウォールがトラフィックをチェーンにルーティングできないので、プロファイルを保存できません。

   複数のルーティングレイヤ 3 セキュリティ チェーンを指定する場合は、ファイアウォールとセキュリティ チェーンの間に正しく設定されたルータ、スイッチ、または類似のデバイ

スを配置して、適切なルーティングを実行する必要があります。さらに、セッション配布方法 を指定して、セキュリティ チェーン間でトラフィックを負荷分散します。



5. ヘルス モニタ タブで、次の手順を実行します。

   - 実行するヘルスモニタリングの種類を選択して、セキュリティ チェーンで障害が発生した場合の動作を制御できるようにします。

     パス監視 、 **HTTP** モニタリング 、および **HTTP** モニタリング遅延 から 1 つ、2 つ、またはすべてを選択できます。

     パスモニタリング –ping を使用してデバイスの接続をチェックします。

     HTTP モニタリング –デバイスの可用性と応答時間をチェックします。

     HTTP モニタリング遅延 :デバイスの処理速度と効率をチェックします。このオプションを選択すると、**HTTP** モニタリング も自動的に有効になります。

   - 1 つ以上の種類の正常性監視を有効にすると、状態チェックの失敗 オプションがアクティブになり、セキュリティ チェーンのヘルス障害が発生した場合にファイアウォールがセキュリティ チェーン トラフィックを処理する方法が決まります。

     ルーティングされたレイヤ 3 ネットワーク パケット ブローカ インターフェイスの 1 つのセットに複数のセキュリティ チェーンを設定した場合、セキュリティ チェーンの障害時に、トラフィックは残りの健全なセキュリティ チェーンにフェールオーバーします。フェールオーバー トラフィックを処理するために使用できるセキュリティ チェーンがない場合、ファイアウォールは の設定された [状態チェック失敗] を実行します。オプションは、バイパスセキュリティチェーンとブロックセッションです。

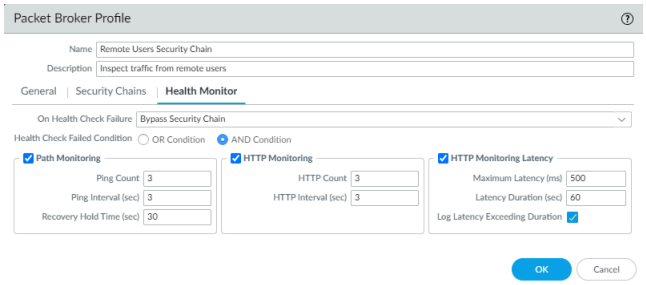
     バイパスセキュリティチェーン:ファイアウォールは、トラフィックをセキュリティ チェーンではなく宛先に転送し、設定済みのセキュリティプロファイルと保護をトラフィックに適用します。

     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。

     選択する方法は、セキュリティ チェーンを通じてトラフィックを実行できない場合に、トラフィックをどのように処理するかによって異なります。

   - 複数のヘルスチェックオプションを選択する場合、監視オプションのいずれかが失敗条件(**OR**条件)を記録している場合、または選択したすべての監視オプションに失敗条件(**AND**条件)を記録する場合に、ファイアウォールでヘルスチェックが失敗したと見

なす (ヘルスチェック失敗条件) を選択します。たとえば、3 つの正常性チェック オプションをすべて有効にし、そのうちの 1 つが失敗した条件を記録した場合、**OR** 条件 を選択した場合、ファイアウォールはセキュリティ チェーン接続が失敗したと見なし、**On Health Check Fail** で指定したアクションを実行します。[**AND** 条件] を選択した場合、2 つの正常性メトリックは依然として問題ないので、ファイアウォールは接続が正常であると見なします。



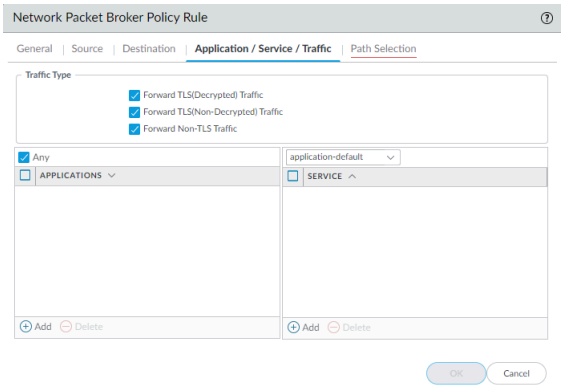
6. **OK** をクリックしてプロファイルを保存します。

STEP 3 | ルーティングされたレイヤ 3 セキュリティ チェーンに転送するトラフィックを定義するパケット ブローカ ポリシーを設定します。

1. ポリシー > ネットワーク パケット ブローカー と 追加 新しいポリシー ルールを選択するか、既存のポリシー ルールを変更します。
2. [全般] タブで、ポリシールールに [名前] と [説明] を指定して、その目的を簡単に識別し、監査コメントを追加し、使用する場合はタグを適用します。
3. [**Source**] タブで、ルールをセキュリティ 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、およびデバイスを指定します。
4. [宛先] タブで、ルールをセキュリティ チェーンに転送するトラフィックの宛先ゾーン、IP アドレス、およびデバイスを指定します。
5. [アプリケーション/サービス/トラフィック] タブで、ルールをセキュリティ チェーンに転送するアプリケーションとサービスを指定します。内部カスタム アプリケーションなどの非標準ポートを使用することが予期されるルール制御アプリケーションを使用しない限り、ベスト プラクティスは、非標準ポートを使用して回避動作を示すアプリケーションがブロックされるように、 **Service** を アプリケーションの既定の に設定することです。

   [トラフィック タイプ] で、ルールをセキュリティ チェーンに転送するトラフィックのタイプをすべて選択します。 転送 **TLS(**復号された**)** トラフィック がデフォルトの選択で

す。転送 **TLS**(復号された) トラフィック 、転送 **TLS**(非復号) 、および 転送非 **TLS** トラフィック の任意の組み合わせを選択して、セキュリティ チェーンに転送できます。



6. [**Path Selection**] タブで、 ステップ 2 で作成したパケット ブローカ プロファイルを選択するか、ポリシールールがセキュリティ チェーンに制御するトラフィックの送信方法を制御する新しいプロファイルを作成します。

STEP 4 | 異なる専用のファイアウォール インターフェイスを使用する個別のルーティング レイヤ 3 セキュリティ チェーンを作成する場合は、ステップ 1 ~ Step 3 を繰り返して、ネットワーク パケット ブローカ セキュリティ チェーンを作成します。ネットワーク パケット ブローカフォワーディング インターフェイスとして使用される 2 つのレイヤ 3 イーサネット インターフェイスは、セキュリティ チェーン専用にする必要があり、他の目的に使用したり、他のトラフィックを伝送したりすることはできません。

Network Packet Broker HA Support

セキュリティ チェーンの障害から保護するために Packet Broker プロファイルで使用できるパスと遅延ヘルスモニタリングに加えて、ファイアウォールの障害から保護するために、Network Packet Broker インターフェイスの転送を行うファイアウォール上で High Availability (HA) を設定することもできます。パス監視と HA の両方を構成することで、セキュリティ チェーンの障害だけでなく、ファイアウォールの障害にも対して保護されます。

ネ!トワークPacket BrokerはActive /Passive HAペアをサポートしています。専用のブローカー転送インターフェイスは Packet Broker プロファイルで指定する必要があるため、Active/Active HA ペアはサポートされません。

フェールオーバー後、SSL 状態が HA ノード間で同期されないため、復号された SSL トラフィックはリセットされます。セッションが正しく同期され、TCP シーケンスが正しく再学習されると、クリアテキスト トラフィックが再開されます。

ネットワーク パケット ブローカーのユーザー インターフェイスの変更

ネットワーク パケット ブローカーは、PAN-OS 8.1 で導入された復号化ブローカー機能を置き換え、非復号化 TLS および非 TLS トラフィックの転送、および復号化された TLS トラフィックをセキュリティ チェーンに含める機能を拡張します。ネットワーク パケット ブローカをサポートするために、PAN-OS 10.1 のユーザ インターフェイスは次の変更を行います。

- 新しいポリシー (ポリシー > ネットワーク パケット ブローカー) を使用すると、特定のトラフィックをセキュリティ チェーンに転送するように設定し、パケット ブローカ プロファイルをアタッチして、指定したトラフィックをセキュリティ チェーンに転送する方法を制御できます。

  復号化ブローカーは、復号化された *TLS* トラフィックのみをセキュリティ チェーンに転送するために、復号化ポリシー ルールを使用しました。新しいネットワーク パケット ブローカ ポリシー ルールを使用すると、復号化された *TLS* トラフィックだけでなく、暗号化された *TLS* トラフィックと *TLS* 以外のトラフィックも選択できます。

- 新しいプロファイル (**Object** > **Packet Broker Profile**) は、古い オブジェクト > 復号化 > 復号化ブローカ プロファイル に置き換え、トラフィックをセキュリティ チェーンに転送する方法と、パスと遅延のヘルスを監視する方法を正確に構成できるようにします。[**General**] タブで、専用のファイアウォール ネットワーク パケット ブローカフォワーディング インターフェイス ペアを入力するフィールドの名前が、それぞれ インターフェイス **#1** および インターフェイス **#2** に変更されました。
- ポリシー > ネットワーク パケット ブローカー を選択すると、ポリシー オプティマイザー のルール使用 オプションのいずれかを選択して、ネットワーク パケット ブローカ ポリシーの使用状況情報を表示できます。ルールの使用の 統計は、未使用のネットワーク パケット ブローカ ルールを保持する必要があるかどうか、またはそれらを削除してルールベースを強化して攻撃の可能性を減らすかどうかを評価するのに役立ちます。
- ネットワーク パケット ブローカーは復号化ブローカーに取って代わるために、復号化ポリシーはセキュリティ チェーンへのトラフィックの仲介を処理しなくなりました。そのため、オプション タブで、復号化と転送 オプションは、ポリシーが取ることができる アクション ではなく、復号化プロファイルのみが復号化ポリシーで有効であるため、転送プロファイル フィールドも削除されました。
- ネットワーク > インターフェイス > イーサネット で、インターフェイス タイプ をレイヤ 3 に設定し、[**Advanced**] タブを選択すると、ネットワーク パケット ブローカの転送インターフェイスとしてインターフェイスを有効にするチェックボックスの名前が"Decrypt Forward"から ネットワーク パケット ブローカ **00** に変更されました。
- デバイス > 管理者ロール の場合は、[**Web UI**] タブで、2 つの変更があります。
  - ポリシー で、ネットワーク パケット ブローカー 管理者ロールのアクセス許可を設定できるようになりました。
  - オブジェクト の下で、復号化 > 転送プロファイル オプションが削除され、管理ロールのアクセス許可の パケット ブローカ プロファイル オプションに置き換えられます。

- ファイアウォールの場合、 **Monitor** > のカスタム レポートの管理 で、[データベース の詳細ログ] から [の利用可能な列] ボックスの一覧で [トラフィック ログ] を選択すると、[セキュリティ チェーン に転送] を選択できるようになりました。

  パノラマでは、[モニタ > カスタムレポートの管理] で、[詳細ログ] から [パノラマトラフィックログ] を [データベース] として選択すると、[使用可能な列] リストで、セキュリティチェーンに転送されます。
- トラフィック ログの [転送の復号] 列は、に転送されたセキュリティ チェーン に変更されます。トラフィックログの詳細ビューの フラグ セクションで、「転送を復号」のチェックボックスは に変更されてセキュリティチェーン に転送されます。
- この機能の無料ライセンスは、"復号化ブローカー" から パケット ブローカー に変更されます。ファイアウォールに無料の復号化ブローカーライセンスがある場合、PAN-OS 10.1 にアップグレードすると名前が自動的に変更されます。変更は名前にだけ存在し、フィーチャーには影響しません。

Network Packet Brokerの制限

ほとんどの Palo Alto Networks platforms support Network Packet Broker, が、いくつかは、いくつかの制限があります。

- サポートは、Prisma Access または NSX ではご利用いただけません。
- AWS、Azure、および GCP は、ルーティングされたレイヤ 3 セキュリティ チェーンのみをサポートします。

Network Packet Broker には、管理対象ファイアウォール用の Panorama にはいくつかの制限があり、いくつかの使用制限があります。Panorama:

- N!etwork P!acket B!roker ライセンスを管理対象ファイアウォールにプッシュする場合は、インストールするライセンスと関連するユーザーインターフェイス要素のファイアウォールを再起動する必要があります。
- パケットブローカプロファイルで特定のインターフェイスを設定するため、**Shared** コンテキストで Packet Broker プロファイルを作成することはできません。
- Different Device Groups は同じ Packet Broker プロファイルを共有できません。
- Panoramaは、10.1より古いPAN-OSバージョンを実行するファイアウォールを含むDevice Groupを含むDevice GroupにNetwork Packet Broker構成(Network Packet Brokerポリシールールとプロファイル)をプッシュすることはできません。

  複数の PAN-OS バージョンのファイアウォールを含む Device Group で Network Packet Broker を使用し、それらのファイアウォールの一部が 10.1 より古い PAN-OS バージョンを実行する場合は、10.1 より前のファイアウォールを PAN-OS 10.1 にアップグレードするか、10.1 より前のファイアウォールを Device Group から削除してから、パケット ネットワークをプッシュする前に

  > ***Panorama*** を使用して、復号ポリシールールにアタッチされている ***Packet Broker*** プロファイルを、***Decryption Broker*** ライセンスがインストールされている ***10.1*** より前のファイアウォールにプッシュできます。ルールの アクション (オプション タブ) は 復号化および転送 である必要があり、パケット ブローカ プロファイルをルールにアタッチする必要があります(オプション タブの 復号化プロファイル 設定)。***10.1*** より前のファイアウォールでは、***Decryption Broker*** の ***Decryption Forwarding*** プロファイルとして ***Packet Broker*** プロファイルを使用します。***Decryption*** ポリシールールは、ファイアウォールがプロファイルを適用するトラフィックを決定します。
  >
  > 復号化ポリシー ルールで制御されるトラフィックは、***SSL*** トラフィックの復号が必要です (復号化ブローカーは暗号化 ***SSL*** トラフィックまたはクリアテキスト トラフィックをサポートしていません)。

- PAN-OS 10.0 から PAN-OS 10.1 にアップグレードする場合、復号化ブローカーに使用されるローカル復号化ポリシー ルールのみが Network Packet Broker 規則に移行されます。パノラマからファイアウォールにプッシュされた復号化ブローカーポリシールールは、Panorama上で自動的に移行されますが、ファイアウォール上で自動的に移行されません。ファイアウォー

ル上でローカルに設定された暗号化解除ブローカーポリシールールは、そのファイアウォール上でのみNetwork Packet Brokerルールに移行されます。Panorama で設定されたルールの場合、Panorama は、パノラマで Network Packet Broker ルールに移行された復号化ブローカールールを同期するために、ファイアウォールに対してもう一度コミット プッシュを行う必要があります。

- PAN-OS 10.1 から PAN-OS 10.0 にダウングレードすると、Network Packet Broker ルールは自動的に削除されます。

Network Packet Broker には、いくつかの使用制限があります。

- Network Packet Broker ファイアウォールも送信元ネットワーク アドレス変換 (SNAT) を実行し、トラフィックがクリアテキスト トラフィックである場合、ファイアウォールはトラフィックに対して NAT を実行し、セキュリティ チェーンにトラフィックを転送します。セキュリティ チェーン アプライアンスには、元の送信元アドレスではなく、NAT アドレスのみが表示されます。

  1. ファイアウォールは、クライアントのトラフィックに対して NAT を実行します。
  2. ファイアウォールはトラフィックをセキュリティ チェーンに転送し、ルーティングは NAT アドレスに基づいている必要があります。
  3. パケットの送信元アドレスが NAT アドレスになったため、セキュリティ チェーン アプライアンスには NAT アドレスのみが表示されます。実際のクライアントソースアドレスは表示されません。
  4. セキュリティ チェーンがファイアウォールにトラフィックを返すと、ファイアウォールはユーザーが誰であるかを認識しません。

  送信元ユーザがセッションに対して誰であるかを調べるには、そのセッションのトラフィック ログをチェックし、パケットをそれらのログと関連付けます。トラフィック ログには、元の送信元アドレスと、送信元ユーザーを特定できる SNAT アドレスの両方が含まれます。

  このシナリオは、ファイアウォール以外のデバイスで *NAT* を実行することで回避できます。

- 復号化された SSH、マルチキャスト、およびブロードキャスト トラフィックはサポートされていません。
- RSA 証明書を使用する場合、SSL インバウンド検査ではクライアント認証はサポートされません。
- レイヤ 1 トランスペア ブリッジ モードでは、トランスペア ブリッジ接続を使用する場合、専用のネットワーク 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各ペアが 1 つのセキュリティ チェーンにのみ接続するため、セキュリティ チェーンに障害が発生してもフェールオーバーは発生しません。(レイヤ 1 ではトラフィックをル(レイヤ 1 ではトラフィックをルーティングできません。ーティングできません。
- IPv6 トラフィックは、レイヤ 1 トランスペアレント ブリッジ モードでのみ転送できます。IPv6 トラフィックをルーテッド(レイヤ 3)モードでは転送できません。
- 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トンネルインターフェイスまたはループバック インターフェイスを使用することはできません。
- ネットワーク パケット ブローカ インターフェイスは、動的ルーティング プロトコルを使用できません。

- 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。
- セキュリティ チェーン内のデバイスは、元のセッションの送信元 IP アドレス、宛先 IP アドレス、送信元ポート、宛先ポート、またはプロトコルを変更できません。
- ネットワーク パケット ブローカーの高可用性は、アクティブ/パッシブ HA ファイアウォール ペアでのみサポートされます。ネットワーク パケット ブローカーの高可用性は、アクティブ/アクティブ ファイアウォール ペアではサポートされていません。
- SSL トラフィックでは高可用性はサポートされていません。SSL セッションはフェールオーバー時にリセットされます。
- PAN-OS 10.0 から PAN-OS 10.1 にアップグレードすると、復号化ブローカーに使用されるローカル復号化ポリシー ルールがネットワーク パケット ブローカ ルールに移行されます。
- PAN-OS 10.1 から PAN-OS 10.0 にダウングレードすると、ネットワーク パケット ブローカのルールは自動的に削除されます。

ネットワーク パケット ブローカーのトラブルシューティング

ネットワーク パケット ブローカの設定で問題が発生した場合は、次の項目を確認してください。

- ファイアウォールの構成:
  - 転送インターフェイス のペアでネクストホップ ルートをチェックして、正しいデバイス インターフェイスを指定していることを確認します。
  - チェーン デバイスとファイアウォール インターフェイスの IP アドレスを使用し、パケット ブローカ プロファイルに正しく入力されていることを確認します。
  - HA が有効になっている場合は、プロファイルに正しいインターフェースが指定されていることを確認してください。
  - チェーンを通過するトラフィックのフロー方向を確認します。
  - プロファイルが適切なセキュリティ チェーンの種類を示していることを確認します。
- セキュリティ チェーンの設定。小切手：
  - セキュリティ チェーン内の各アプライアンスの IP アドレス、次ホップ アドレス、およびデフォルト ゲートウェイ。
  - IP アドレス指定、次ホップ、およびデフォルト ゲートウェイの構成ミスのためのファイアウォールとセキュリティ チェーン (ルーター、スイッチなど) の間のデバイスの構成。
  - ファイアウォールとチェーン間のパス。
- ファイアウォールのトラフィック ログをチェックして、仲介トラフィックに対して予期したとおりに設定された "転送" フラグが表示されることを確認します。
- 有用な CLI コマンドには、次のものがあります。
  - ルールベースネットワークパケットブローカーを表示する
  - ネットワーク パケット ブローカの状態を表示する
  - ネットワーク パケット ブローカの統計情報を表示する
  - 実行中のアプリケーション キャッシュをすべて表示する
  - `show` アプリケーション設定 — App-ID キャッシュが有効になっていること、およびキャッシュが App-ID に使用されていることを確認し、キャッシュのしきい値の設定を確認します。