*Panorama*でファイアウォールを管理するためのベストプラクティス

10.0 (EoL)

techDOCS paloalto NETWORKS

Contact Information

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

About the Documentation

- To ensure you are viewing the most current version of this document, or to access 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

December 3, 2020

Table of Contents

*Panorama*にファイアウォールを追加するためのベストプラクティス

Panorama™管理サーバーは、次世代ファイアウォールの集中管理と可視性を提供する、Palo Alto Networksのネットワークセキュリティ管理ソリューションです。このドキュメントは、Panoramaに新しいファイアウォールをオンボーディングする、または既存のファイアウォールを移行して、操作を簡素化および合理化するためのベストプラクティスを提供しています。

- ユースケース - Panoramaへの新たな次世代ファイアウォールのオンボーディング
- ユースケース - 次世代ファイアウォールのPanoramaへの移行

ユースケース - Panoramaへの新たな次世代ファイアウォールのオンボーディング

Panorama™管理サーバーの利用を開始するための最初のユースケースは、Panoramaに新たにデプロイしたファイアウォールを管理対象デバイスとして追加することです。

STEP 1 | **Associate Devices**（デバイスを関連付ける）、または複数のファイアウォールを**Import**（インポート）して、オンボーディングプロセスを合理化してください。

- ファイアウォールをPanoramaに正常に追加した後に手動で関連付けるのではなく、1ヶ所からPanoramaにファイアウォールを追加する際に、ファイアウォールをデバイスグループ、テンプレートスタック、コレクタグループ、およびLog Collector（ログコレクタ）に関連付けます。
- 多数のファイアウォールを追加する場合は、CSVファイルを使って新しいファイアウォールをPanoramaにインポートします。CSVファイルにより、手動でファイアウォールを関連付ける代わりに、すべてのファイアウォールをデバイスグループ、テンプレートスタック、コレクタグループ、およびLog Collectorと関連付けることができます。このオプションは、手動によるファイアウォールの関連付けに時間がかかるような、大量のファイアウォールを追加する場合に特に役立ちます。

STEP 2 | **Auto Push on 1st Connect**（最初の接続時に自動プッシュ）を有効にして、**To SW Version**（次の**SW**バージョン）を、最初にPanoramaに正常に接続した時に管理対象ファイアウォールにデバイスグループとテンプレートスタック設定を自動的にプッシュ配信するように設定し、指定したPAN-OSのバージョンに管理対象ファイアウォールをアップグレードします。これには、PAN-OSアップグレードパス内の各PAN-OSバージョンに対して、必要なすべてのコンテンツアップデートを自動インストールすることも含まれています。

- 新しいファイアウォールすべてをCSVファイルでPanoramaにインポートする場合、**Auto Push on 1st Connect**（最初の接続時に自動的にプッシュ配信）を有効にして、CSVファイル内の**To SW Version**（**SW**バージョン）を設定してインポートプロセスを合理化してください。
- ロールベースのアクセス制御を実装する場合、すべてのPanorama管理者に対してスーパーユーザー権限を有効にするのではなく、デバイスグループとテンプレート管理者を活用して、アクセスドメイン内のデバイスグループとテンプレートにファイアウォールを追加します。

STEP 3 | ファイアウォールをPanoramaに正常に追加したら、管理対象ファイアウォールの検索とフィルタリングを簡単に行えるように、タグを作成して適用します。これにより、Panoramaを使用して管理するファイアウォール数が増加しても、管理対象ファイアウォールを整理しておくことができます。

STEP 4 | ITスタッフが少数または存在していないリモートサイトにファイアウォールをデプロイする場合は、Zero Touch Provisioning（ゼロタッチプロビジョニング）（ZTP）を設定して、リモートサイトにネットワークまたはIT管理者を必要とせず、新しい管理対象ファイアウォールのオンボーディングを自動化することで、ファイアウォールの初期デプロイを合理化できます。

ユースケース - 次世代ファイアウォールのPanoramaへの移行

Panorama™管理サーバーの利用を開始するための2番目のユースケースが、既存のファイアウォールをPanoramaに移行することです。可能な場合は、移行時にPalo Alto Networksのセールスエンジニアまたはプロフェッショナルサービスエンジニアと協力して、ファイアウォール設定が正しくPanoramaに移行されていることを確認してください。

STEP 1 | 作業の鍵となるのがプランニングです。移行作業を開始する前に、次の事項を理解していることを確認してください。

- Palo Alto Networks互換性マトリックスを参照して、Panoramaとファイアウォール、ログコレクタ、およびコンテンツバージョン間の互換性を理解し、移行時に互換性に関する問題が発生しないようにしてください。
- 無駄を減らし、ファイアウォールのセット内のすべてのファイアウォール間で共有される設定の管理を合理化するようにデバイスグループとテンプレートのプランニングを行います。
- ファイアウォールをPanoramaに正常に移行した後に、重要なトラフィックやアプリケーショントラフィックを検証するために、移行後のテストプランを用意します。

STEP 2 | ファイアウォールをPanorama管理に移行する場合、同一の設定オブジェクトの重複を避けるために、デバイスの共有オブジェクトを**Panorama**の共有コンテキストにインポートしてください。

STEP 3 | 正常に移行が完了したら、ポリシーを参照して、重複したルールがないかどうかを確認します。コミットエラーを防止するために、Panoramaにコミットする前に重複しているルールのいずれかを削除するようにしてください。

STEP 4 | 管理対象ファイアウォールに**Export or push device config bundle**（デバイス設定バンドルのエクスポートまたはプッシュ配信）を行う場合、**Merge with Candidate Config**（候補設定と結合）、**Include Device and Network Templates**（デバイスおよびネットワークテンプレートを含める）、および**Force Template Values**（テンプレート値を強制）を有効にして、プッシュ内のすべてのデバイスグループとテンプレートを含めて、ファイアウォール上のローカルな保留中の変更を強制的にコミットし、Panorama上のデバイスグループまたはテンプレートに存在していない任意のローカル設定を削除するようにしてください。これにより、Panoramaが管理するベースライン設定が、Panoramaに移行されるすべてのファイアウォールにプッシュ配信されます。

STEP 5 | 移行後テストを実行して、移行が正常に完了し、すべてが予定通りに動作していることを確認します。時間の経過とともに、必要に応じて構成を最適化します。Expeditionのような移行ツールを使用して定期的に設定の状態を評価して、未使用のオブジェクトや重複したオブジェクトを削除します。また、Policy Optimizerを利用して、セキュリティポリシールールベースを最適化します。

*Panorama*でファイアウォール設定を管理するためのベストプラクティス

ファイアウォールには、セキュリティとネットワークの2種類の設定が存在しています。Panoramaはデバイスグループを使ってオブジェクトおよびポリシールールなどのセキュリティ設定を管理し、テンプレートおよびテンプレートスタックを使ってネットワーク設定を管理します。

- Panoramaでのデバイスグループ設定の管理
- Panoramaでのテンプレートとテンプレートスタックの設定の管理
- Panoramaでのテンプレートとテンプレートスタックの変数の管理

Panoramaでのデバイスグループ設定の管理

デバイスグループは、継承の原則を適用して、適切に定義されたデバイスグループ階層を実装することで、ポリシーを整理して再利用する方法を提供します。Panoramaでは、階層内の複数のデバイスグループにまたがって、同じデバイスグループ設定を再利用できる一方で、ローカル設定をカスタマイズして、継承された設定に上書きする事もできます。

- デバイスグループ階層を設計する際に、機能または地域的なニーズを考慮して、事前ルールと事後ルール間の違いについて理解するようにしてください。

  たとえば、管理対象ファイアウォールに例外なく適用するセキュリティ事前ルールを作成し、セキュリティ事前ルールに該当しなかったトラフィックをクリーンアップするためのセキュリティ事後ルールを作成します。
- 小規模な管理対象ファイアウォールの容量制限を超えないように、**Shared**（共有）デバイスグループの過度の使用は避けるようにしてください。単一の共有設定オブジェクトが変更された場合、すべてのファイアウォールが`Out of Sync`（非同期）になるため、適切なデバイスグループレベルで設定オブジェクトを管理することで、`Out of Sync`（非同期）状態のファイアウォール数を効率的に最小限に抑えることができます。
- カスタムアドレスオブジェクトを使ってカスタムリージョンを設定し、アドレス範囲または地域を指定します。

  企業はRFC 1918のアドレス空間を使用していますが、10.0.0xネットワーク全体を管理するポリシーは役に立ちません。代わりに、カスタムアドレスオブジェクトを使ってカスタムリージョンを定義して、アドレス範囲またはジオロケーションを指定します。これにより、よりきめ細かく関連性の高いポリシーを作成して、攻撃対象領域を減らすことができます。
- 各デバイスグループに対して**Master Device**（マスターデバイス）を設定し、Panoramaがユーザーグループマッピングを収集できる様にします。デバイスグループにマスターデバイスを設定することで、ポリシールールの作成時にユーザーグループを利用することができます。さらに、Panoramaによって収集されたユーザーグループマッピングを使用して、ACCとMonitor（監視）タブをフィルタリングできます。
- セキュリティ設定を完了するには、管理対象ファイアウォールが所属していないテンプレートに含まれている、ネットワーク設定オブジェクトを参照するように、**Reference Templates**（リファレンステンプレート）を関連付けます。そうすることによって、**Shared**（共有）デバイスグループを過度に使用したり、同一のネットワーク設定オブジェクトを再作成したりすることなく、デバイスグループとテンプレートにまたがって共通の設定オブジェクトを有効活用することができます。

Panoramaでのテンプレートとテンプレートスタックの設定の管理

テンプレートとテンプレートスタックを使用して、ロギングや高可用性（HA）など一般的な設定のため、管理対象ファイアウォール全体でネットワークとファイアウォールの構成オブジェクトを再利用します。 また、異なるテンプレートスタック内の複数のマネージドファイアウォールで必要に応じて組み合わせることができるモジュラーテンプレートを構成できます。

- 設定が不完全な場合でも、設定の論理グループを使ってテンプレートを作成し、モジュール構成を実現します。設定が完了しており、すべての参照がテンプレートスタックレベル（各テンプレートではない）で解決されている必要があります。テンプレートスタック設定を完了するために、異なるテンプレートからオブジェクトを再利用、参照、および上書きすることができます。
- モデル固有のテンプレート（例:ネットワークインターフェイス設定）およびユースケース固有のテンプレート（例:管理者、ロールベースのアクセス制御セット）を作成します。これにより、テンプレートをテンプレートスタックに追加する際に、適切なテンプレートを混合、照合することができます。
- テンプレート内、または管理対象ファイアウォール上でローカルに優先させるネットワーク設定を使用して、テンプレートスタックを設定します。

Panoramaでのテンプレートとテンプレートスタックの変数の管理

テンプレートとテンプレートスタック変数を作成して、管理対象ファイアウォール全体でのネットワークおよびデバイス設定のオブジェクトの設定共有と再利用を最大化します。

- 必要に応じてテンプレートおよびテンプレートスタック変数を使用することで、より少ないテンプレートで管理対象ファイアウォール構成を管理し、構成を合理化します。

  たとえば、一般的にファイアウォール間でIPアドレスは異なっています。テンプレート変数を使用して、IPアドレスの代わりに変数を指定することで、必要な設定を作成することができます。設定を管理対象ファイアウォールにプッシュ配信する際に、Panoramaは管理対象ファイアウォールごとに設定された値に基づいて、ファイアウォール単位に正しいIPアドレスを設定できます。
- 管理対象ファイアウォールに間違った設定をプッシュ配信されないように、デフォルト値**None**（なし）で変数を作成してください。

  ここで注意する例外となるのが、DNSのIPアドレスです。最悪の場合でも、管理対象ファイアウォールがDNSクエリを解決できる可能性があります。

設定変更管理のベストプラクティス

ロールベースのアクセス制御（RBAC）を活用し、管理対象ファイアウォールへのアクセスをセグメント化することで、管理者が行える設定の変更を管理します。外部ダイナミックリスト（EDL）やダイナミックユーザーグループ（DAG）などの動的な構造を活用してポリシールールを最新の状態に保ち、管理者がコミットして管理対象ファイアウォールにプッシュ配信できる設定の変更内容をきめ細かく制御することができます。

- Panoramaからの管理ロールとアクセスドメインの管理
- Panoramaが管理するセキュリティルールの簡素化
- 大規模チームの設定変更管理
- Panorama の設定変更のコミット
- Panorama の設定変更のプッシュ配信

Panoramaからの管理ロールとアクセスドメインの管理

動的な環境で設定管理を正常に行うための鍵となるのが、チームメンバーに適切な権限を割り当てることができるようにすることです。Panoramaは、きめ細かく役割の定義を行うための、拡張されたロールベースのアクセス制御（RBAC）を提供しています。RBACをアクセスドメインと組み合わせて、管理対象ファイアウォールへのアクセスのセグメント化を簡単に行うことができます。これにより攻撃対象領域が現象し、偶発的な、または悪意のある管理者権限の誤用を防止することができます。

パノラマおよびマネージドファイアウォール構成へのアクセスを適切に制御する方法の詳細については、「セキュリティ管理アクセスのベストプラクティス」を参照してください。

- 管理者がアクセスを過剰にプロビジョニングすることなく、ファイアウォールを正常に管理できるように、管理者の役割を定義します。
- 異なる目的に対応するファイアウォールのサブセットが複数ある場合は、Panorama管理者用のアクセスドメインを作成します。。たとえば、データセンターファイアウォール、境界ファイアウォール、およびブランチファイアウォールが異なるパノラマ管理者によって管理されている場合、管理するファイアウォールのみへのアクセスを制限するアクセスドメインを構成および割り当てます。
- アクセスドメインおよび管理の役割の内の管理対象ファイアウォールへの管理アクセスをより適切に制御するには、デバイスグループとテンプレート管理者を作成します。これにより、チームが運用上の問題を引き起こすことなく仕事を行えるようにする、最もきめ細かいアクセスが提供されます。

Panoramaが管理するセキュリティルールの簡素化

ポリシールールベースを管理する場合にもっとも重要な作業の1つが、セキュリティポリシーを管理することです。

- Policy OptimizerおよびPolicy Rule Usage（ポリシールール使用状況）を組み合わせて使用して、App-ID（アプリケーションID）およびUser-ID（ユーザーID）ベースのセキュリティポリシールールに移行して、ルールベースをアプリケーションが認識するようにしてください。

  より効果的で分かりやすくなるように、セキュリティポリシールール内に使用グループを作成します。また、Expedition（調査）およびBest Practice Asessment（ベストプラクティス評価）（BPA）ツールを活用して、ルールベースの各リビジョンを反復処理し、セキュリティ体制を強化することができます。
- ポリシールールベースを評価して、すでに存在している可能性があるオブジェクトやルールを識別する際には、Global Find（グローバル検索）を活用してください。これは、Panoramaでのコミットを遅らせる原因となる、設定内の無駄な項目を減らすために役立ちます。
- 提案するポリシールール設定の変更が、変更のみが必要な既存のルールによってすでに処理されているかどうかをテストするために、ポリシールールのトラブルシューティングを行います。これにより、重複するポリシールールを減らして、ポリシールールベースの肥大化を防止することができます。
- ルールの目的、機能、ライフサイクル、またはその他の特性を識別して、似たようなルールを素早くソートしてグループ化するには、タグベースのルールグループを使用します。タグベースのルールグループにより、ルールベース内の各ルールセットを視覚的に区別して、グループとして管理したり、グループ内の単一のルールを個別に変更したりすることができます。
- サポートされているセキュリティ監査の重要な運用機能に対応するために、ポリシールールの作成と変更に対して監査コメントを適用します。適切にドキュメントに記録された、一連の監査コメントを持つルールにより、ルールの説明や外部ツールに依存することなく、監査リクエストに対応することができます。また、設定の変更をPanoramaにコミットする際に説明を入力することで、監査コメントを補足することができます。
- 外部ダイナミックリスト、ダイナミックアドレスグループ、およびダイナミックユーザーグループなどの動的な構成物を利用して、設定作業を能率化して、セキュリティポリシールールベースのメンテナンスを簡素化してください。環境が変化するにつれて、必要に応じてコミットすることなく、これらを変更することができます。
- セキュリティポリシールールを作成する場合、**Target**（ターゲット）タブで1つまたは複数の管理対象ファイアウォールを選択することは避けるようにしてください。表示される管理対象ファイアウォールの設定同期ステータスが信頼できない情報になってしまいます。

  一般的にこのことは、ポリシーターゲッティングと呼ばれています。ポリシーターゲッティングは、Panoramaではなくファイアウォール上で評価されます。その結果、ポリシールールがプッシュ配信されない管理対象ファイアウォールには、誤って`Out of Sync`（非同期）と表示されることがあります。ポリシーターゲッティングが必要になることを防止する、または最低限に抑えるように、デバイスグループ階層をデザインしてください。

大規模チームの設定変更管理

大規模チームが設定の集中管理にPanoramaを使用する際に、設定エラーが発生します。Panoramaは、設定を元に戻す、インポート、エクスポート、ロード、結合、および置換など、きめ細かい操作をすることが可能です。これらの操作は、デバイスグループまたはテンプレートレベルで行われます。

- Panoramaの設定を以前の状態に素早く戻す場合、Panorama設定全体ではなく、影響を受けたデバイスグループまたはテンプレートのみを元に戻すことを検討してください。

  これにより、影響を受けるデバイスグループまたはテンプレートで設定を変更しなかった、他の管理者からの変更内容を保持することができます。さらに、設定をエクスポートして、それをオフラインで変更し、作業が完了したらそれをPanoramaにインポートして戻すことができます。
- 緊急の設定変更を管理対象ファイアウォールにプッシュ配信するために、作業途中のデバイスグループやテンプレート設定の変更をエクスポートします。エクスポートを行ったら、Panoramaの設定を元に戻して、緊急の変更を行います。変更内容が管理対象ファイアウォールに正常にプッシュ配信されたら、作業途中の設定変更を含むPanorama設定をインポートすることができます。
- 複数のPanorama設定を統合する場合は、デバイスグループやテンプレートの設定を結合して、単一のPanorama設定に統一します。

Panorama の設定変更のコミット

Panoramaには、コミットプロセスを制御するためのさまざまな方法が用意されています。これを理解して、日常業務に役立てることをお勧めします。

- Panorama設定変更をコミットする場合は、**Commit Changes Made by**（担当者による変更のみをコミット）を選択して、自分が変更した内容のみをコミットし、他の管理者が行った設定の変更はコミットしないようにしてください。そうすることで、進行中または承認されていない他の設定変更が誤ってPanoramaにコミットすることを防げます。
- 設定の変更をコミットする場合、管理者に対して**Preview Changes**（変更内容をプレビュー）して、変更サマリーを確認を要求します。多くの場合、設定の変更を視覚的に確認することで、間違いを見つけ、後の運用メンテナンスの時間を節約できます。

Panorama の設定変更のプッシュ配信

Panoramaは、設定の変更を管理対象ファイアウォールにプッシュ配信するための、さまざまな手段を提供しています。これを理解して、日常業務に役立てることをお勧めします。

- 設定の変更を管理対象ファイアウォールにプッシュ配信する前に、プッシュ配信する範囲を確認して（**Commit**（コミット）> **Push to Devices**（デバイスにプシュ配信）> **Edit Selections**（選択項目の編集））、ターゲットファイアウォールの一覧が正しいことを確認するようにしてください。

  デバイスグループ階層が正しくデザインされており、設定の変更が適切である場合でも、メンテナンス期間が異なるため、一度にすべてのファイアウォールに設定の変更をプッシュ配信する必要がないこともあります。ベストプラクティスとして、常にターゲットファイアウォールの一覧を確認して、必要な管理対象ファイアウォールにのみ設定の変更がプッシュ配信されることを確認するようにしてください。
- **Force Template Values**（テンプレート値の強制）（**Commit**（コミット）> **Push to Devices**（デバイスにプッシュ配信）> **Edit Selections**（選択項目の編集））設定は、慎重に使用してください。この設定のプッシュ配信では、ローカルファイアウォール設定を含めて、管理対象ファイアウォール設定全体の上書きが有効になります。

*Panorama*でのモニタリングと可視性のベストプラクティス

組織の要件に基づいてログの取り込みと保管を最適に行えるように、ロギングインフラを設計してください。その後、Application Command Center（ACC）、PDF Summary（PDFサマリー）レポート、およびカスタムレポートを活用して、調査と解決が必要なネットワークアクティビティや脅威を識別します。

- ロギングインフラの設計
- PanoramaでのApplication Command Center（ACC）とログのモニタリング
- Panoramaでの標準およびカスタムレポートの生成

ロギングインフラの設計

新しい管理対象ファイアウォールをデプロイする前に、ロギングインフラを計画、及び設計することをお勧めします。Panorama管理サーバーには、デバイス管理とログ収集のために、複数のモードを提供しますPanoramaモードでは、ファイアウォール設定の管理と、ログの取り込みと保管の両方を行えます。Panoramaを単一機能目的で動作させたい場合向、Log Collector（ログコレクタ）モードが用意されています。このモードは、ログの取り込みと保管のみを目的に設計されています。また、Management Only（管理専用）モードは、ファイアウォール設定の管理のみを目的設計されています。

- ロギングレートの計算と、ログストレージ要件については、『Panoramaサイジングおよびデザインガイド』を参照してください。これは、ログコレクターのログストレージ容量を決定するときに重要であり、規制要件などのさまざまな要因に基づくことがあります。

  ロギングインフラのサイジングをする際には、セールスエンジニア（SE）にご相談ください。ニーズに合わせてデプロイを理解し、カスタマイズするために必要な技術的専門知識を提供いたします。
- レガシー（従来）モードに関連するロギング上の制限事項が多いため、Panorama仮想アプライアンスをデプロイする場合は、レガシーモードを使用しないでください。Panoramaのレガシーモードはラボまたはデモ環境には適していますが、実働環境ではこのモードを使用しないでください。
- 管理対象ファイアウォールのログ収集には、個別のインターフェイスを使用してください。これにより、Panoramaと通信する管理インターフェイスのパフォーマンスを維持することができます。セキュリティ上のベストプラクティスとして、すべてのインターフェイスに対する、許可するIPリストを設定してください。

PanoramaでのApplication Command Center（ACC）とログのモニタリング

Application Command Center（ACC）は、ネットワーク内のイベントを素早く理解することを目的に設計された、インタラクティブな視覚化ツールです。ACCは、管理対象ファイアウォールログを分かりやすく表示することで、トラフィックパターンに関する洞察と、調査で使用できる脅威に関する実用的な情報を取得できるようにします。

- ACCでは、利用できる全てのデータとの対話の使用方法について学習してください。
  - ACCフィルタを使用して、アドレスやユーザーなどの特定の情報にドリルダウンすることができます。
  - グローバルフィルタを適用して、注目している情報の詳細のACC表示をピボットし、不要な情報を除外することができます。
  - GlobalProtectを利用している場合、**GlobalProtect Activity**ウィジェットからHIP一致ログに基づいたHIPレポートを参照し、ネットワークにアクセスするエンドデバイスのセキュリティステータスを理解することができます。
  - 目的の情報を絞り込んだら、ACCデータをCSV形式、またはウィジェットをPDF形式でエクスポートして、さらなる調査や修正を行いたいチームと情報を共有することができます。
- ACCをカスタマイズして、監視したい特定のネットワークアクティビティ向けに表示内容を調整することができます。

  そうすることにより、特定のユーザーまたはホストの調査効率を改善することができます。タブを切り替えたり、延々とスクロールしたりしないでも、目的の情報や状況を完全に把握することができます。

  - ACCに新しいウィジェットを追加して、**Content Activity**（コンテンツアクティビティ）を選択します。
  - ACCに新しいウィジェットを追加して、**URL Filtering**（URLフィルタリング）を選択します。
  - デフォルトでは、**Threat Activity**（脅威アクティビティ）ウィジェットが表示されます。表示されない場合は、新しいウィジェットを追加して、**Threat Activity**（脅威アクティビティ）を選択します。
- **Objects**（オブジェクト）> > **Regions**（リージョン）を選択し、IPアドレス範囲を使用して、セキュリティポリシールールで使用するカスタムリージョンを作成します。カスタムリージョンを使用することで、ACCのネットワークイベントをより深く相関させることができます。

  たとえば、指定オフィス用のカスタムリージョンを設定した後、特定のIPアドレスが不審な大量のトラフィックに関与していることに気が付いた場合を考えてみましょう。カスタムリージョンを活用することで、この不審なネットワークアクティビティを特定のオフィスと関連付け、調査を行い是正措置を取ることができます。

Panoramaでの標準およびカスタムレポートの生成

Panorama™管理サーバーは、ファイアウォール デプロイ環境全体の情報を一元化および集約して、PDFレポートやカスタムレポートを作成するための方法を提供しています。

- 組織で使用されているすべてのSaaSアプリケーションを、**Sanctioned**（許可）または**Unsanctioned**（不許可）として識別して分類します。

  Panoramaおよび管理対象ファイアウォールは、許可されたタグを持たない任意のアプリケーションを、ネットワークでの使用が許可されていないと見なします。許可されていないSaaSアプリケーションは、脅威にさらされたり、プライベートデータや機密データが失われたりする可能性があります。ネットワークアクティビティを詳細に調査するために、SaaSアプリケーションを分類することが重要になります。

  1. **Objects (オブジェクト) >** > **Applications (アプリケーション)** を選択します。
  2. 必要に応じて、カスタムSaaSアプリケーションを作成します。
  3. 1つまたは複数のSaaSアプリケーションを選択して、**Edit Tags**（タグの編集）を選択します。
  4. Add Tags（タグの追加）ドロップダウンから、**Sanctioned**（許可）または**Unsanctioned**（不許可）を選択します。
  5. 必要に応じてSaaSアプリケーションにタグが設定されるまで、ステップ1～4を繰り返します。
  6. **Commit**（コミット）> > **Commit and Push**（コミットおよびプッシュ配信）を選択して、設定内容を**Commit and Push**（コミットしてプッシュ配信）します。
- ユーザーグループに基づいてユーザーアクティビティレポートとSaaSアプリケーションの使用状況レポートを構成し、レポートの粒度を高めます。

  たとえば、財務部門がGitHubに大量のデータを保存しているとします。ユーザーアクティビティおよびSaaSアプリケーション使用状況レポートでユーザーグループを活用することにより、不審な行動をより簡単に識別することができます。そうしない場合、組織全体に対してレポートが実行され、この不審な行動が見過ごされてしまう可能性があります。
- 目的に応じた固有のカスタムレポートを設定して、必要な項目にのみに数を制限してください。

  レポートのパラメータを簡潔にすることで、調査が必要なネットワークアクティビティをより簡単に識別できるようになります。

カスタムレポートを作成する場合、可能な限りQuery Builderを利用して、結果を素早く絞り込むようにしてください。

たとえば、1つのオフィスをターゲットにしたレポートは、すべてのオフィスをターゲットにしたレポートに比べて遥かに効率的で実用的です。複数のオフィスを含むレポートが必要な場合、各オフィス固有のクエリを使用して、いくつかの異なるレポートを実行することをお勧めします。