paloalto TECHDOCS

SD-WAN 管理者ガイド

3.2

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

May 20, 2024

Table of Contents

SD-WAN の概要 5
- SD-WAN 情報 6
- SD-WAN のシステム要件 10
- SD-WAN の設定要素 15
- SD-WAN 設定計画 17

SD-WAN の設定 21
- SD-WAN プラグインのインストール 22
  - Panorama のインターネット接続時のSD-WAN プラグインのインストール 22
  - Panorama のインターネット非接続時のSD-WAN プラグインのインストール 23
- SD-WANに対応する Panorama とファイアウォールのセットアップ 26
  - SD-WAN ファイアウォールの管理対象デバイスとしての追加 26
  - SD-WAN ネットワークテンプレートの作成 29
  - Panorama の事前定義ゾーンの作成 30
  - SD-WAN デバイス グループの作成 32
- リンクタグの作成 36
- SD-WAN インターフェース プロファイルの設定 37
- SD-WAN に対応する物理イーサネット インターフェースの設定 43
- SD-WAN 用の集約イーサネット インターフェイスとサブインターフェイスの設定 51
- SD-WAN 用のレイヤ 3 サブインターフェイスの設定 58
- 仮想 SD-WAN インターフェースの設定 64
- SD-WAN インターフェースへのデフォルト ルートの作成 67
- SD-WAN リンク管理プロファイルの設定 68
  - パス品質プロファイルの作成 68
  - SaaS モニタリングの設定 70
  - SD-WAN トラフィック分散プロファイル 82
  - トラフィック分散プロファイルの作成 88
  - エラー訂正プロファイルの作成 91
- SD-WAN ポリシー ルールの設定 96
- MPLS リンクへのダイレクト インターネット アクセスのトラフィック フェイル オーバーを許可する 102
- DIA AnyPath の設定 103
- 合致しないセッションの分散 110
- Panorama への SD-WAN デバイスの追加 112

SD-WANデバイスの証明書ベース認証の設定 112
SD-WAN デバイスの追加 116
複数の SD-WAN デバイスの一括インポート 128
オンボードPAN-OS ファイアウォールからPrisma Accessへ 132
SD-WANハブで複数の仮想ルーターを構成する 147
SD-WANブランチで複数の仮想ルーターを設定する 151
SD-WAN 対応 HA デバイスの設定 156
VPN クラスタの作成 157
DDNS サービスを含むフルメッシュ VPN クラスタの作成 172
SD-WAN のスタティック ルートの作成 178
SD-WAN の高度なルーティングの設定 180
モニタリングおよびレポート 187
SD-WAN タスクの監視 188
SD-WAN アプリケーションおよびリンクパフォーマンスの監視 190
Prisma Access Hubの監視 197
Prisma Access Hubアプリケーションとリンクのパフォーマンスをベースライン化 197
Prisma Access Hub アプリケーションとリンクのパフォーマンスを監視する 199
SD-WAN レポートの生成 204
トラブルシューティング 207
SD-WAN タスクでの CLI コマンドの使用 208
SD-WAN デバイスの交換 212
アプリケーションパフォーマンスのトラブルシューティング 214
リンクパフォーマンスのトラブルシューティング 219
SD-WAN ファイアウォールのアップグレード 224
SD-WAN プラグインのインストール 225
SD-WAN プラグインのアンインストール 226

SD-WAN の概要

SD-WAN について学習し、デプロイメントを確実に成功させる設定計画を策定します。

- SD-WAN 情報
- SD-WAN のシステム要件
- SD-WAN の設定要素
- SD-WAN 設定計画

SD-WAN 情報

Software-Defined Wide Area Network (SD-WAN) は、複数のインターネットサービスおよびプライベートサービスを使用し、インテリジェントかつ動的な WAN を構築することができるテクノロジーであり、コスト削減とアプリケーションの品質および使いやすさの最大化に役立ちます。PAN-OS® 9.1 以降、Palo Alto Networks® は、単一の管理システムで SD-WAN オーバーレイを採用したパワフルなセキュリティ機能を提供しています。ルーター、ファイアウォール、WAN パスコントローラー、WAN オプティマイザーなどのコンポーネントを使用して WAN をインターネットに接続する高価で時間のかかる MPLSの代わりにPalo Alto Networksのファイアウォールで SD-WAN を使用することにより、より低コストでインターネットサービスが利用でき、機器の数も減少します。その他の WAN コンポーネントを購入し、維持する必要はありません。

- SD-WAN 機能を備えた PAN-OS セキュリティ
- SD-WAN リンクとファイアウォールのサポート
- プリズマアクセスハブのサポート
- 集中管理

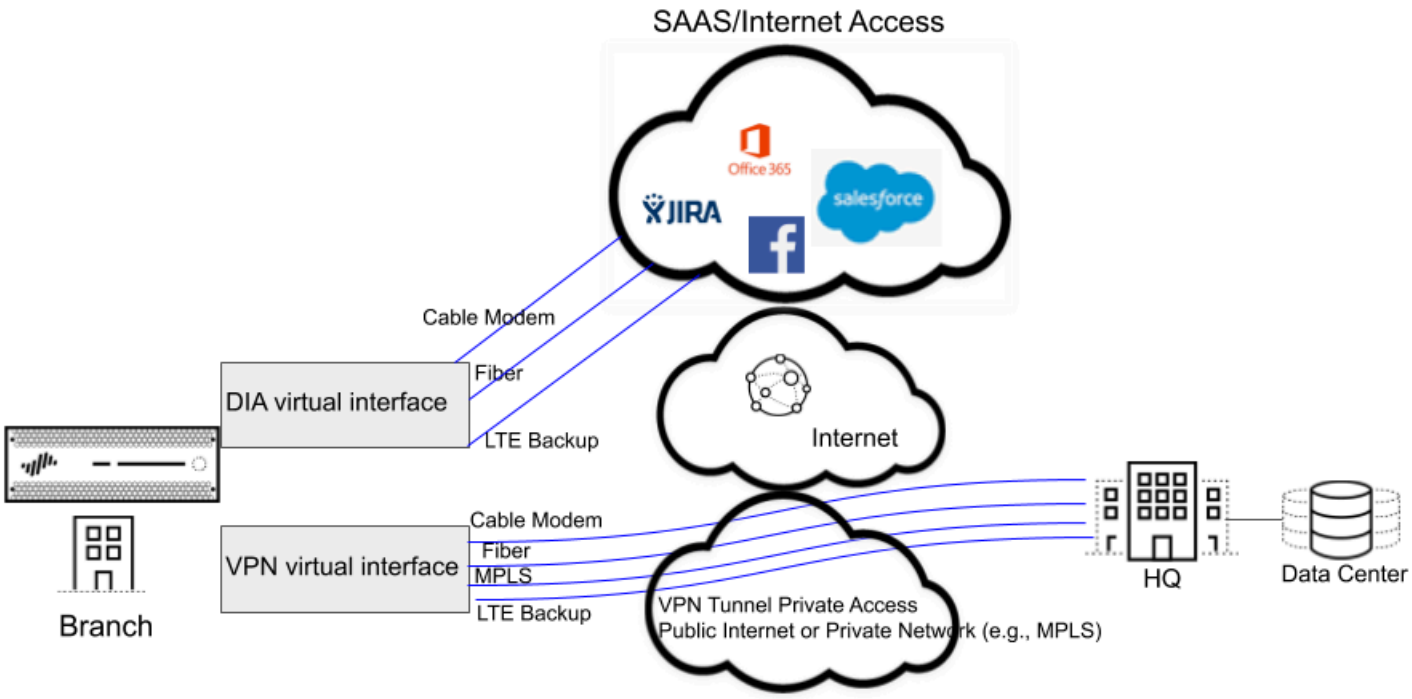
SD-WAN 機能を備えた PAN-OS セキュリティ

SD-WAN プラグインは PAN-OS と統合されているため、単一のベンダーから PAN-OS ファイアウォールのセキュリティ機能と SD-WAN 機能を入手することができます。SD-WAN オーバーレイは、アプリケーションとサービス、そして各アプリケーションまたはサービスが使用を許可されているリンクの条件に基づき、動的でインテリジェントなパス選択を提供します。各リンクのパスヘルスモニタリングの対象には、遅延、ジッター、およびパケット損失が含まれます。アプリケーションおよびサービスをきめ細かく制御し、アプリケーションに関して、ミッションクリティカルであるかどうか、遅延が許されないかどうか、あるいは特定の正常性基準を満たすかどうか、等の条件に基づき、アプリケーションに優先順位を付けることができます。動的パス選択により、セッションが 1 秒未満でより優れたパフォーマンスを発揮するパスにフェイルオーバーするため、電圧低下やノード障害の問題を回避します。

The SD-WAN オーバーレイは、 User-ID™ および App-ID™ 等の PAN-OS のすべてのセキュリティ機能と連携し、ブランチオフィスにも完全なセキュリティ制御を提供します。すべての App-ID 機能の優れた機能 (App-ID デコーダー、App-ID キャッシュ、および送信元 / 宛先の外部動的リスト [EDL] IP アドレスリスト) により、SD-WAN トラフィックのアプリケーションベースの制御向けのアプリケーションを識別します。トラフィックのゼロトラストセグメンテーションを使用してファイアウォールを展開することが可能です。SD-WAN は、Panorama Web インターフェースまたは Panorama REST API から一元的に設定および管理することができます。

クラウドベースのサービスを採用している場合でも、インターネットトラフィックがブランチからハブそしてクラウドに流れるのではなく、直接接続した ISP を使用してインターネットトラフィックがブランチからクラウドに直接流れるようにしたい場合があります。このようなブランチからインターネットへのアクセスは、ダイレクト インターネット アクセス (DIA) となります。インターネットトラフィックに自社ハブの帯域幅と資金を費やす必要はなくなります。ブランチのファイアウォールは既にセキュリティを実行しているため、ハブのファイアウォールでインターネットトラフィックにセキュリティを適用する必要はありません。ハブにバックホールするべきでない SaaS、Web ブラウジング、または帯域幅を多く使用するアプリケーションに対応

するためにブランチで DIA を使用します。以下の図では、ブランチからクラウドへの 3 つのリンクから構成される DIA 仮想インターフェースが説明されています。この図では、ブランチを本社のハブに接続する4つのリンクから構成される VPN トンネル仮想インターフェースも示されています。



SD-WAN リンクとファイアウォールのサポート

(異種 ISP が同じ宛先と通信するために使用される) 複数の物理リンクは、リンクバンドリングにより、仮想 SD-WAN インターフェースへとグループ化することができます。アプリケーションとサービスに基づき、ファイアウォールは、セッションロードシェアリング向けのリンクを選択して (パスの選択) 、電圧低下または停電時にフェイルオーバー保護を提供します。これにより、アプリケーションに最高品質のパフォーマンスが提供されます。ファイアウォールは、仮想 SD-WAN インターフェースのリンクに関してセッションロードシェアリングを自動的に実行し、利用可能な帯域幅を有利に使用します。SD-WAN インターフェースへの接続の種類は、すべて同じ (DIA またはVPN のいずれか) でなければなりません。VPN リンクは、ハブアンドスポーク型トポロジをサポートしています。

SD-WAN は、以下のタイプの WAN 接続をサポートしています。ADSL/DSL、ケーブルモデム、イーサネット、ファイバ、LTE/3G/4G/5G、MPLS、マイクロ波 / ラジオ波、衛星、WiFi、およびファイアウォールのインターフェースへのイーサネットとして終端するものすべて。リンクの使用方法に関する適切な戦略は御社が決定することになります。高価な MPLS や LTE 接続を導入する以前に、低コストのブロードバンド接続を使用することができます。あるいは、特定の VPN トンネルを使用して、地域の特定のハブにアクセスすることもできます。

SD-WAN ソフトウェア機能をサポートするファイアウォールモデルの完全なリストについては、SD-WANのシステム要件」を参照してください。

Palo Alto Networks の次世代ファイアウォールを購入する新規のお客様は、デフォルトの Virtual Router (仮想ルーター - VR) をSD-WAN に使用することになります。既存のお客様は、PAN-OS に既存の Virtual Router (仮想ルーター - VR) を上書きさせるか、SD-WAN の新しい Virtual Router (仮想ルーター - VR) と新しいゾーンを使用して、SD-WAN のコンテンツを既存の設定から分けることができます。

PAN-OS 11.0 以降、SD-WAN プラグイン 3.1 は、業界標準の設定方法を使用して管理者タスクを容易にする 高度なルーティングエンジン をサポートします。概念的には同等ですが、高度なルーティング エンジンは、ルーティング ドメインをインスタンス化するために 仮想ルーター ではなく論理ルーターを使用します。高度なルーティングを有効にすると、論理ルーターが作成され、ルーティングに高度なルーティング エンジンが使用されます。高度なルーティングを無効にすると、仮想ルーターが作成され、ルーティングにレガシーエンジンが使用されます。

プリズマアクセスハブのサポート

SD-WAN プラグイン 2.2 以降のリリースでは、PAN-OS セキュア SD-WAN は Prisma Access ハブをサポートし、アプリケーションのセキュリティ保護方法と場所を完全に制御できます。プリズマアクセスハブのサポートにより、PAN-OSファイアウォールはプリズマアクセスコンピューティングノード(CN)に接続して、SD-WANハブアンドスポークトポロジでクラウドベースのセキュリティを実現できます。このサポートにより、オンプレミスのセキュリティからPrisma Accessへのシームレスなリンクフェイルオーバーが可能になり、セキュリティのニーズを満たすために両方を組み合わせることができます。

SD-WAN ファイアウォールと Prisma Access ハブの両方を持つ混合トポロジでは、SD-WAN ハブはプリズマ アクセス CN(IPSec ターミネーション ノード)であり、SD-WAN ブランチは PAN-OS ファイアウォールです。SD-WAN は、ブランチをハブに接続する IKE および IPSec トンネルを自動的に作成します。トラフィック分散プロファイルを使用すると、特定のインターネットアプリケーションに一致する SD-WAN ポリシーを作成し、選択した PAN-OS ファイアウォールまたは Prisma Access 展開にリダイレクトできます。Prisma Accessハブのサポートにより、オンプレミスとクラウドのセキュリティプラットフォームが連携して、Panoramaによって管理される一貫したセキュリティポリシーを備えた完全なソリューションを提供します。

Prisma Access ハブのサポートに必要な最小 PAN-OS および SD-WAN プラグインのバージョンについては、SD-WANのシステム要件を参照してください。

Prisma Accessハブのサポートには、次の制限があります。

- Prisma Accessに関連するSD-WAN設定のインポートとエクスポートはサポートされていません。
- Prisma Access 設定のロード、部分ロード、リバート、および部分リバートはサポートされていません。
- 既存の Prisma Access リモート ネットワーク セキュリティ プロセス ノード (RN-SPN) へのオンボードはサポートされていません。Prisma Access に接続されている既存のブランチの場合は、ブランチを削除してから再度オンボードする必要があります。
- SD-WAN CLI コマンドは、Prisma Accessファイアウォールでは使用できません。
- CN では、CN で発信されるトラフィックのパス選択はありません。

- プリズマアクセス統計は、SD-WAN レポートおよび統計では提供されません。

集中管理

Panorama™ は、SD-WAN を設定および管理する手段を提供します。これにより、地理的に分散した多数のファイアウォールの複数のオプションの設定が、ファイアウォールを個別に設定するよりも格段に迅速かつ容易になります。各ファイアウォールを個別に設定するのではなく、単一の場所からネットワークの設定を変更することができます。自動 VPN 設定により、Panorama では安全な IKE/IPSec 接続でブランチとハブを設定することができます。VPN クラスタにより、地理的領域で相互に通信するハブとブランチが定義されます。ファイアウォールは、ブランチとハブとの間のパスのヘルスモニタリングに VPN トンネルを使用し、1 秒未満で電圧低下状態の検出を提供します。

Panorama ダッシュボードでは、SD-WAN リンクとパフォーマンスの可視性が提供されるため、SD-WAN のパス品質のしきい値やその他の側面の調整が可能となり、パフォーマンスの向上を図ることができます。集中管理された統計およびレポートでは、アプリケーションとリンクのパフォーマンス統計、パスヘルス測定および傾向分析、さらにアプリケーションとリンクの問題に焦点を当てたビューが提供されます。

SD-WAN のユースケースの把握から始め、SD-WAN 設定要素、トラフィック分散方法を確認し、SD-WAN 設定を計画します。空の SD-WAN デバイスの CSV をエクスポートし、ブランチオフィスの IP アドレス、使用する Virtual Router (仮想ルーター - VR) 、ファイアウォールのサイト名、ファイアウォールが属するゾーン、BGP ルート情報等の情報を入力することが、設定の大幅な高速化につながるベストプラクティスです。Panorama では、CSV ファイルを使用して SD-WAN ハブとブランチを設定し、ハブとブランチ間の VPN トンネルを自動的にプロビジョニングします。SD-WAN では eBGP を介したダイナミックルーティングをサポートし、Panorama の SD-WAN プラグインを使用して、すべてのブランチがハブのみ、あるいはハブとその他のブランチと通信できるように設定することができます。

パノラマが マルチ vsys ファイアウォール を管理している場合は、すべての *SD-WAN* 対応インターフェイスおよび設定を *vsys1* で設定する必要があります。

SD-WAN は、マルチ *VSYS* ファイアウォールの複数の仮想システムにまたがる *SD-WAN* 構成をサポートしません。

SD-WAN インターフェイスは、同じ仮想ルータで設定する必要があります。仮想ルータ間で分割することはできません。

SD-WAN のシステム要件

SD-WAN 用 Panorama™ プラグインの最小ソフトウェアバージョン、プラグインバージョン、およびリソース要件を確認します。

PAN-OS 11.0 以降では、プラグイン バージョン *3.1* で SD-WANの高度なルーティングを構成できます。

次の表に、各プラグインと互換性のあるバージョンを示します。対応バージョンには新機能やバグフィックス、機能拡張が含まれているため、Prisma Accessのクラウド設定プラグイン版と、表に記載されている対応するSD-WANプラグイン版を併用することが推奨されています。

プラットフォーム	PAN-OS	システム要件	Prisma Access Cloud Configuration Plugin	SD-WAN プラグイン
Panorama	11.2.3	• (Panorama Virtual Appliance) システム ディスク—224GB システム ディスク • **CPU**—16 CPUs • メモリ—64GB メモリ • システム モード—Panorama モードと管理専用モード • (M-Series アプライアンスの管理専用モードのみ)8TB RAID ロギング ディスクペアが有効	—	3.3.1
	11.2.0		5.0.0-h22	3.3.0
	11.1.5		—	3.2.2
	11.1.3		5.0.0-h31	3.2.1
	11.1.0		4.0.0 および 5.0.0	3.2.0
	11.0.4		5.0.0-h21	3.1.3
	11.0.3		4.0.0 および 5.0.0	3.1.2
	11.0.2		4.0.0	3.1.2

プラットフォーム	PAN-OS	システム要件	Prisma Access Cloud Configuration Plugin	SD-WAN プラグイン
	11.0.2	上記の情報は、最大*500*台の管理対象デバイスに適用されます。最大*1,000*の管理対象デバイスの使用については、「Panorama仮想アプライアンスのシステム要件」を参照してください。	4.0.0	3.1.1
	11.0.1 *11.0.1*は*11.0.x*の推奨リリースです。		3.2.1.h21	3.0.1-h6
	11.0.0		3.2.1-h3	3.1.0-h6
	10.2.8		4.0.0-h80、4.1.0-h49、および5.0.0-h9	3.0.7
	10.2.7		4.0.0 および5.0.0	3.0.6
	10.2.6		4.0.0	3.0.6
	10.2.5		4.0.0	3.0.5
	10.2.4 *10.2.4*は*10.2.x*の推奨リリースです。		3.2.1-h21	3.0.4
	10.2.3		3.2.1-h5	3.0.4

プラットフォーム	PAN-OS	システム要件	Prisma Access Cloud Configuration Plugin	SD-WAN プラグイン
	10.2.1		このリリースではサポートされていません。今後のリリースで予定されています。Prisma Access Cloud Configuration PluginでSD-WANを使用している場合は、PAN-OS 11.1にアップグレードしないでください。	3.0.1
	10.2.0			3.0.0
	10.1.11		4.0.0 および 5.0.0	2.2.6
	10.1.11		4.0.0	2.2.5
	10.1.10 *10.1.10*は*10.1.x*の推奨リリースです。		4.0.0	2.2.4
	10.1.9		3.2.1-h5	2.2.4

プラットフォーム	PAN-OS	システム要件	Prisma Access Cloud Configuration Plugin	SD-WAN プラグイン
	*10.1.9*は*10.1.x*の推奨リリースです。			
	10.1.8		3.2.1-h5	2.2.2
	10.1.5-h1		2.1	2.2.1
	10.1.0		2.1	2.2
次世代 Firewall	• **PAN-OS 11.1**—11.1.0 • **PAN-OS 11.0**—11.0.0 • **PAN-OS 10.2**—10.2.0 • **PAN-OS 10.1**—10.1.4 • **PAN-OS 10.0**—10.0.8	該当なし		
Prisma Access Compute Node	10.0.7*	* Prisma Access Compute Nodes(IPSec 終端ノード)は、PAN-OS 10.0.7 またはそれ以降の 10.0 リリースを実行する必要があります。必要に応じて、ブランチ オフィスを Prisma Access ハブにオンボードする前に、営業チームと協力してアップグレードを要求します。		

以下のファイアウォールモデルが、SD-WAN ソフトウェア機能をサポートしています。

- PA-220 および PA-220R
- PA-400シリーズ
- PA-820およびPA-850
- PA-1400 シリーズ
- PA-3200シリーズ

- PA-3400シリーズ
- PA-5200シリーズ
- PA-5400シリーズ
- PA-7000シリーズ
- VM-シリーズ ファイアウォール

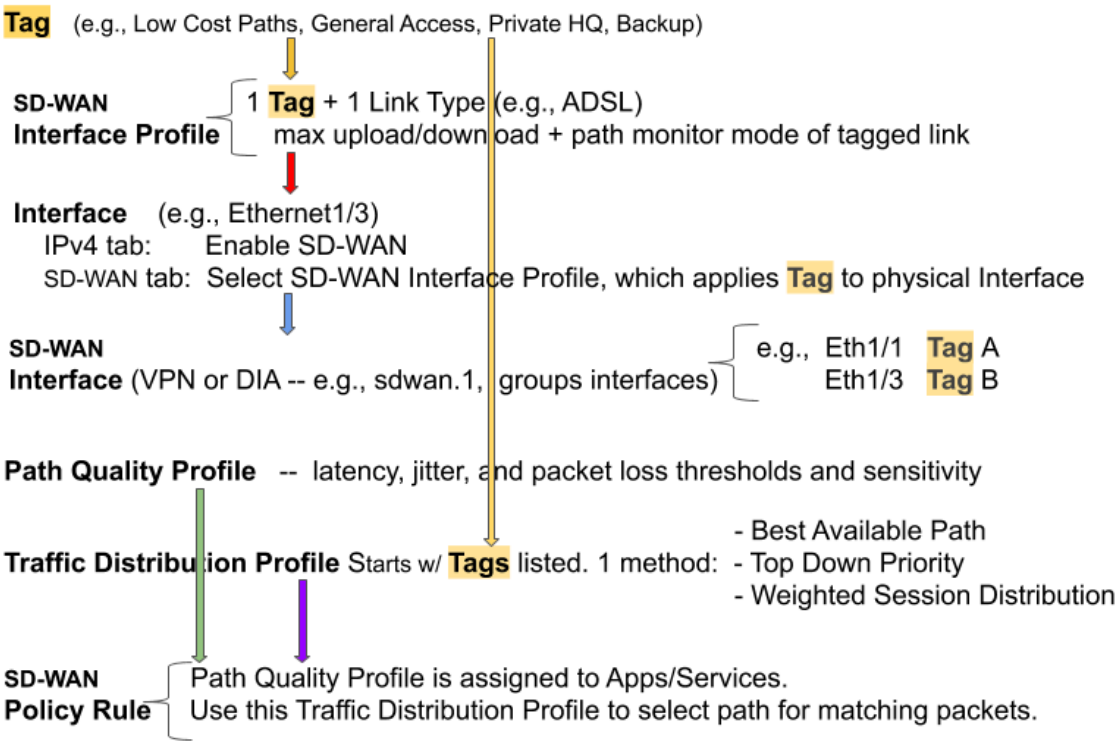
特定のハードウェアの可用性の詳細については、互換性マトリックスを参照してください。

SD-WAN の設定要素

SD-WAN 設定の要素が連携すると、以下が可能となります。

- 共通の宛先を共有する物理イーサネット インターフェースを論理 SD-WAN インターフェイスにグループ化します。
- リンク速度を指定します。
- SD-WAN への劣化したパス (または電圧低下または停電) が新たな最適パスの選択を迫られるしきい値を指定します。
- この新たな最適パスを選択する方法を指定します。

このビューでは、要素間の関係が一目で説明されます。



特定のアプリケーションまたはサービスがブランチからハブに、あるいはブランチからインターネットでとる VPN トンネルまたはダイレクト インターネット アクセス (DIA) を指定することにより、トラフィックがとるリンクを制御することが、SD-WAN 設定の目的です。あるパスが劣化した場合にファイアウォールが新たな最適なパスを選択できるようにパスをグループ化します。

- 選択した **Tag** (タグ) 名により、リンクは識別されます。赤い矢印が示す通り、インターフェースにインターフェース プロファイルを適用することによりリンク (インターフェース) にタグを適用します。リンクが持てるタグは、1 つだけです。2 つの黄色の矢印は、タグがインターフェース プロファイルおよびトラフィック分散プロファイルで参照されていることを示しています。タグの使用により、インターフェースがトラフィック分散に使用される順序

を制御することができます。Panorama ではタグを使用して、SD-WAN 機能を備えた数多くのファイアウォール インターフェースを体系的に設定することができます。

- **SD-WAN Interface Profile(SD-WAN** インターフェース プロファイル**)** は、物理インターフェースに適用するタグを指定し、そのインターフェースのリンクのタイプも指定します。(タイプには、ADSL/DSL、ケーブルモデム、イーサネット、ファイバ、LTE/3G/4G/5G、MPLS、マイクロ波 / ラジオ波、衛星、WiFi、その他があります)。インターフェース プロファイルでは、ISP 接続の最大アップロード速度およびダウンロード速度 (Mbps単位) を指定することもできます。ファイアウォールがパスを頻繁に監視するかどうかを変更することもできます。デフォルトで、ファイアウォールはリンクタイプの適切な監視を行います。
- IPv4 または IPv6 アドレスを持つレイヤ 3 イーサネット **Interface** は、SD-WAN 機能をサポートできます。このインターフェース (赤い矢印) にSD-WAN インターフェース プロファイルを適用し、インターフェースを特徴づけます。青い矢印は、物理インターフェースが参照され、仮想 SD-WAN インターフェースにグループ化されていることを示しています。
- 仮想 **SD-WAN Interface (SD-WAN** インターフェース**)** は、トラフィックのルーティングが可能な番号がつけられた仮想 SD-WAN インターフェースを構成する 1つまたは複数のインターフェースの VPN トンネルまたは DIA グループです。SD-WAN インターフェースのパスはすべて同じ宛先 WAN に向かい、すべて同じタイプ (DIAまたはVPNトンネル) となります。(タグ A とタグ B は、仮想インターフェースの物理インターフェースに別々のタグ付けが可能であることを示しています。)
- **Path Quality Profile (**パス品質プロファイル**)** では、遅延、ジッター、およびパケット損失の最大しきい値を指定します。しきい値の超過は、パスが劣化し、ファイアウォールが対象への新しいパスを選択する必要があることを示します。高、中、低の感度設定により、プロファイルが適用されるアプリケーションにとってより重要なパス モニタリング パラメータをファイアウォールに示すことができます。緑の矢印は、1 つまたは複数の SD-WAN ポリシー ルールでパス品質プロファイルが参照されていることを示しています。従って、アプリケーション、サービス、送信元、宛先、ゾーン、およびユーザーが異なるパケットで適用されるルールに、異なるしきい値を指定することができます。
- **Traffic Distribution Profile (**トラフィック分散プロファイル**)** では、現在の優先パスがパス品質しきい値を超えた場合にファイアウォールが新しい最適パスを決定する方法を指定します。新しいパスの選択の絞り込みのためにこの分散方法が使用するタグを指定します。ですから、黄色の矢印はタグからトラフィック分散プロファイルを指しています。トラフィック分散プロファイルでは、ルールの分散方法が指定されます。
- 上記の要素が **SD-WAN Policy Rules (SD-WAN** ポリシー ルール**)** でまとめられます。紫色の矢印は、ファイアウォールがセッションに属さないパケットに対してアプリケーションベースの SD-WAN パス選択を実行する時期および方法を具体的に示すために、パケット アプリケーション / サービス、送信元、宛先、およびユーザー、そしてパス修飾プロファイルおよびトラフィック分散プロファイルがルールで参照されることを説明しています。(SD-WAN ポリシー ルール内で **SaaS Quality Profile (SaaS** 品質プロファイル**)** および **Error Correction Profile (**エラー訂正プロファイル**)** を参照することもできます。)

要素間の関係を理解したので、トラフィック分散方法を確認してからSD-WAN 設定計画を確認します。

SD-WAN 設定計画

SD-WAN 対応のブランチおよびハブのファイアウォール インターフェースの全体トポロジーを計画し、CSV ファイルで Panorama™ テンプレートを作成し、設定をファイアウォールにプッシュします。

STEP 1 | ブランチおよびハブの場所、リンク要件、および IP アドレスを計画します。Panorama から 空の SD-WAN デバイス CSV をエクスポートして、ブランチとハブの情報を入力します。

1. (ブランチまたはハブの) 各ファイアウォールのロールを決定します。
2. どのブランチがどのハブと通信するかを決定します。相互通信するブランチ ファイアウォールとハブ ファイアウォールの各機能グループは、VPN クラスタとなります。例えば、VPN クラスタは、地理的あるいは機能別に編成される場合があります。
3. 各ブランチおよびハブがサポートする ISP リンクタイプを決定します。ADSL/DSL、ケーブルモデム、イーサネット、ファイバ、LTE/3G/4G/5G、MPLS、マイクロ波 / ラジオ波、衛星、および WiFi があります。
4. ステップ 2 で説明される通り、リンクタイプがサポートする最大ダウンロードおよびアップロード帯域幅 (Mbps) および、速度制御をリンクに適用する方法を決定します。ISP リンクの最大ダウンロードおよびアップロード帯域幅 (Mbps) を記録します。アプリケーションの帯域幅を制御する QoS を設定する必要がある場合には、この情報が参照用最大出力として機能します。
5. スタティックあるいは動的な割り当てかどうかに関わらず、ブランチ ファイアウォールのパブリック IP アドレスを収集します。ファイアウォールが IPSec トンネルを開始および終了し、アプリケーショントラフィックをインターネットとの間でルーティン

グできるには、インターネットでルーティング可能なパブリック IP アドレスが必要です。

ISP の社内向け機器は、ファイアウォールのイーサネット インターフェースに直接接続する必要があります。

ブランチ ファイアウォールとハブの間に *NAT* を実行するデバイスがある場合、*NAT* デバイスはファイアウォールの *IKE* ピアリングおよび *IPSec* トンネルの起動を妨げる場合があります。トンネルが失敗した場合は、リモート *NAT* デバイスの管理者の協力を得て問題を解決してください。

6. ブランチ ファイアウォールおよびハブ ファイアウォールのプライベート ネットワーク プレフィックスとシリアルナンバーを収集します。
7. 各ファイアウォール インターフェースのリンクタイプを決定します。

   ブランチ ファイアウォールにわたり同じイーサネット インターフェースに同じリンクタイプを割り当てると、設定が容易となります。例えば、イーサネット *1/1* は常にケーブルモデムとします。
8. サイトおよび SD-WAN デバイスの命名規則を決定します。

   自動 *VPN* 設定はこのキーワードを使用して多様な設定要素を生成するため、「ハブ」または「ブランチ」といった単純なホスト名は使用しないでください。
9. SD-WAN の設定以前に既にゾーンが設定されている場合は、SD-WAN がパスの選択に使用する事前定義済みゾーンにそれらのゾーンをマップする方法を決定します。既存のゾーンを、zone-internal、zone-to-hub、zone-to-branch、zone-internet と名付けられた事前定義済みゾーンにマッピングします。

   *(*複数の *SD-WAN* デバイスを一括追加できるように*) CSV* に入力する情報には、以下が含まれます。シリアルナンバー、デバイスのタイプ *(*ブランチまたはハブ*)*、事前定義済みゾーン *(*製品導入済みの場合*)* にマップするゾーン名、ループバック アドレス、再配信するプレフィックス、*AS* 番号、ルーター *ID*、および *Virtual Router (* 仮想ルーター - *VR)*名。

STEP 2 | プライベート リンクのリンク バンドルと VPN セキュリティ計画を策定します。

リンク バンドルを使用すると、パスの選択およびフェイルオーバー保護のために、複数の物理リンクを 1 つの仮想 SD-WAN インターフェースに結合することができます。複数の物理リンクをバンドル化することにより、物理リンクが劣化した場合にもアプリケーションの品質を最大化できます。(SD-WAN インターフェース プロファイルで) 複数のリンクに同じリンクタグを適用してバンドルを作成します。リンクタグは、同様のタイプのアクセスと同様のタイプの SD-WAN ポリシー処理がなされるリンク バンドルを識別します。例えば、**`low cost broadband (`**低コストブロードバンド**`)`** と名付けられたリンクを作成し、ケーブルモデムおよびファイバブロードバンドサービスを含めることができます。

STEP 3 | SD-WAN および QoS 最適化を利用するアプリケーションを特定します。

1. SD-WAN の制御およびポリシーを提供する重要かつ遅延の影響を受けやすいビジネス アプリケーションを特定します。そのようなアプリケーションは、優れたユーザー エ

クスペリエンスを必要とするアプリケーションであり、リンク状態が劣悪の場合、正常に機能しない恐れがあります。

最も重要かつ遅延に敏感なアプリケーションから開始します。*SD-WAN*がスムーズに機能した後でアプリケーションを追加することができます。

2. 帯域幅の優先に向けて、QoS ポリシーを必要とするアプリケーションを特定します。これは、重要あるいは遅延の影響を受けやすいと特定されたアプリケーションと同じであるはずです。

最も重要かつ遅延に敏感なアプリケーションから開始します。*SD-WAN*がスムーズに機能した後でアプリケーションを追加することができます。

STEP 4 | 元のリンクが劣化あるいは失敗した場合に、リンクを別のリンクにフェイルオーバーするタイミングおよび方法を決定します。

1. リンクのパス モニタリング モードを決定します。ただし、リンクタイプのデフォルト設定を保持することがベストプラクティスです。

   - **Aggressive (アグレッシブ)**- ファイアウォールが、一定の頻度でプローブ パケットを SD-WAN リンクの反対側に送信します (デフォルトでは 毎秒 5 プローブ)。アグレッシブ モードは、パス品質のモニタリングが重要となるリンクに最適です。この場合、電圧低下および停電時の高速検出とフェイルオーバーが必要となります。アグレッシブ モードでは、1 秒未満の検出およびフェイルオーバーが提供されます。
   - **Relaxed (緩やか)**-ファイアウォールは、プローブパケット送信間の設定可能なアイドル時間を7秒間 (設定したプローブ頻度) 保持します。これにより、アグレッシブ モードよりもパス モニタリング頻度が低減します。緩やかなモードは、非常に低い帯域幅のリンク、衛星や LTE などの操作コストが高いリンク、または高速検出がコストおよび帯域幅の維持と比べてさほど重要でない場合に適しています。

2. ファイアウォールが新たなセッションの最初のリンクを選択する順序および、複数の候補がある場合にフェイルオーバーしているリンクを置き換えるリンクが候補となる優先順序を決定します。

   例えば、コスト高のバックアップ LTE リンクを最後に使用するリンクにする場合 (コスト安のブロードバンド リンクがオーバーサブスクライブされているか、完全にダウンしている場合のみ)、トップダウン優先トラフィック分散方式を使用して、LTE リンクのタグをトラフィック分散プロファイルのタグのリストの最後に配置します。

3. アプリケーションおよびサービスについて、パスの品質が低下していると見なされ、ファイアウォールが新しいパスを選択する (フェイルオーバー) ことになるパスヘルスのしきい値を決定します。品質特性は、遅延 (10～2,000 ミリ秒)、ジッター (10～1,000 ミリ秒の範囲)、およびパケット損失率です。

   上記のしきい値は、SD-WAN ポリシー ルールで参照されるパス品質プロファイルを構成します。いずれかのしきい値 (パケット損失、ジッター、または遅延) を超えた場合 (および残りのルール基準が満たされた場合)、ファイアウォールは、一致するトラフィックの新たな優先パスを選択します。例えば、ゾーン XYZ からの FTP パケットが届く場合にはルール 1 で使用するために、遅延 / ジッター / パケット損失のしきい値、それぞれ1000/800/10 でパス品質プロファイル AAA を作成し、送信元の IP アドレス 10.1.2.3 からの FTP パケットが届く場合にはルール 2 で使用するために、(しきい値が 50/200/5 である) パス品質プロファイル BBB を作成します。高いしきい値から始

め、アプリケーションの許容度をテストすることが、ベストプラクティスです。値を低く設定しすぎると、アプリケーションのパスの切り替えが頻繁に発生する恐れがあります。

使用しているアプリケーションおよびサービスが、待機時間、ジッター、またはパケット損失の影響を格別受けやすいかどうかを検討します。例えば、ビデオ アプリケーションは、遅延およびジッターを軽減する優れたバッファリング機能を備えている場合がありますが、パケット損失の影響を受けやすく、これがユーザーエクスペリエンスに影響を与えます。プロファイルのパス品質パラメータの感度は、高、中、または低に設定することができます。遅延、ジッター、およびパケット損失の感度設定が同じ場合、ファイアウォールはパケット損失、遅延、ジッターの順でパラメータを調査します。

4. アプリケーションまたはサービスの新たなセッションをロード シェアリングするリンクを持つかどうかを決定します。

STEP 5 | Panorama がブランチとハブにプッシュし、この間のトラフィックを動的にルーティングする BGP 設定の計画を策定します。

1. 4byte (バイト) の自律システム番号 (ASN) を含む BGP ルート情報の計画をたてます。各ファイアウォール サイトは個別の AS にあるため、一意の ASNが必要です。各ファイアウォールには、一意のルーター ID も必要です。
2. BGP が既に使用されている環境で BGP ルーティングを使用して SD-WAN を実装する前に、SD-WAN プラグインによって生成された BGP 設定が既存の BGP 設定と競合していないことを確認します。たとえば、既存の BGP AS 番号とルータ ID 値を、対応する SD-WAN デバイス値に使用する必要があります。
3. BGP 動的ルーティングを使用しない場合は、Panorama のネットワーク 設定機能を使用してその他のルーティング設定をプッシュする計画を策定します。ブランチとハブの間では、スタティック ルーティングすることが可能です。Panorama プラグインの BGP 情報をすべて抜かし、通常の Virtual Router (仮想ルーター - VR) のスタティック ルートを使用してスタティック ルーティングを実行します。

STEP 6 | 仮想 SD-WANインターフェースのファイアウォール モデルの容量、SD-WAN ポリシー ルール、ログサイズ、IPSec トンネル (プロキシ ID を含む)、IKE ピア、BGP およびスタティック ルートテーブル、BGP ルーティング ピア、およびファイアウォール モード (App-ID™、脅威、IPSec、復号化) のパフォーマンスを検討します。使用するブランチおよびハブのファイアウォール モデルが、必要な容量をサポートしていることを確認します。

SD-WAN の設定

SD-WAN 設定計画したら、SD-WAN プラグインをインストールし、Panorama™ 管理サーバーをセットアップして、ハブとブランチのファイアウォール の SD-WAN 構成を一元管理します。Panorama を活用することで、SD-WAN デプロイメントを管理する上での管理要件および運用オーバーヘッドが削減され、リンクの状態の監視および問題発生時のトラブルシューティングがより容易となります。

パノラマがマルチ *vsys* ファイアウォール を管理している場合は、すべての *SD-WAN* 対応インターフェイスおよび設定を *vsys1* で設定する必要があります。

SD-WAN は、マルチ *VSYS* ファイアウォールの複数の仮想システムにまたがる *SD-WAN* 構成をサポートしません。

- SD-WAN プラグインのインストール
- SD-WANに対応する Panorama とファイアウォールのセットアップ
- リンクタグの作成
- SD-WAN インターフェース プロファイルの設定
- SD-WAN に対応する物理イーサネット インターフェースの設定
- (任意)SD-WAN 用の集約イーサネット インターフェイスとサブインターフェイスの設定
- (任意)SD-WAN 用のレイヤ 3 サブインターフェイスの設定
- 仮想 SD-WAN インターフェースの設定
- SD-WAN インターフェースへのデフォルト ルートの作成
- SD-WAN リンク管理プロファイルの設定
- SD-WAN ポリシー ルールの設定
- MPLS リンクへのダイレクト インターネット アクセスのトラフィック フェイルオーバーを許可する
- DIA AnyPath の設定
- 合致しないセッションの分散
- Panorama への SD-WAN デバイスの追加
- (任意)SD-WANハブで複数の仮想ルーターを構成する
- (任意)SD-WANブランチで複数の仮想ルーターを設定する
- (任意)SD-WAN 対応 HA デバイスの設定
- VPN クラスタの作成
- DDNS サービスを含むフルメッシュ VPN クラスタの作成
- (任意)SD-WAN のスタティック ルートの作成
- (Optional) SD-WAN用のAdvanced Routingの設定

SD-WAN プラグインのインストール

SD-WAN デプロイメントの設定および管理には、SD-WAN プラグインを備えた Panorama™ 管理サーバが必要となります。Panorama がインターネットに接続されている場合は、SD-WAN プラグインを Panorama から直接ダウンロードして、Panorama 管理サーバにインストールします。Panorama がインターネットに接続されていない場合は、SD-WAN プラグインを Palo Alto Networks® のカスタマーサポート ポータルからダウンロードして、Panorama 管理サーバにインストールします。

- Panorama のインターネット接続時のSD-WAN プラグインのインストール
- Panorama のインターネット非接続時のSD-WAN プラグインのインストール

Panorama のインターネット接続時のSD-WAN プラグインのインストール

SD-WAN デプロイメントを設定および管理するには、SD-WAN プラグインがインストールされた Panorama™ 管理サーバが必要です。Panorama がインターネットに接続されている場合、SD-WAN プラグインを Panorama ウェブ インターフェースから直接ダウンロードしてインストールします。プラグインのインストールが必要なのは、SD-WAN ファイアウォールを管理する Panorama のみです。個々のハブ ファイアウォールやブランチ ファイアウォールにインストールする必要はありません。

STEP 1 | Panorama Web インターフェイスへのログイン。

STEP 2 | **Panorama**、 > **Plugins (**プラグイン**)** と選択し、**sd_wan** プラグインの最新バージョンを **Check Now(**今すぐチェック**)** します。

STEP 3 | SD-WAN プラグインを**Download (**ダウンロード**)** および**Install (**インストール**)** します。

STEP 4 | SD-WAN プラグインのインストールが正常に完了した後、**Commit (**コミット**)** および **Commit to Panorama (Panorama** へのコミット**)** します。

この手順は、いずれの設定の変更を Panorama にコミットする前に必要となります。

STEP 5 | (Management Only mode only)SD-WAN 監視データの保存に必要なログディスクを有効にします。

- **M-Series Appliances**:すべてのMシリーズアプライアンスには、デフォルトでRAID 1に2組の8TBロギングディスクが付属しています。管理専用モードで Panorama から SD-WAN

を使用して firewall を管理する場合は、SD-WAN モニタリングデータを保存するために、ロギングディスクペアの最初のペアを有効にする必要があります。

1. Panorama CLI へのログインを行います。
2. M-Seriesアプライアンスにデフォルトで含まれているロギングディスクペアの最初のペアを有効にします。

```
>show system raid add A1
```

3. Logging Disk Pair A が 利用可能 であることを確認します。

```
> show system raid detail
```

RAID のセットアップが完了すると、以下の応答が表示されます。

```
Disk Pair A       Available Status         clean Disk id
 A1     Present model :ST91000640NS size :953869 MB status:
 active sync
```

4. ログ ディスクのペアをログに使用できるようにします。
   1. **Panorama** > **Managed Collectors** を選択し、Log Collector を編集します。
   2. **Disks**（ディスク）を選択し、各アレイを **Add**（追加）します。
   3. **OK** をクリックして変更内容を保存します。
   4. **Commit** > **Commit to Panorama**および **Commit** を選択し、変更をコミットします。
   5. **Commit** > **Push to Devices** を選択し、Collector Group と **Push** を選択します。

- **Panorama Virtual Appliances**:Panorama 仮想アプライアンスを管理専用モードで展開した場合、SD-WAN 監視データを保存するには、システム ディスクを 224 GB に増やす必要があります。

STEP 6 | SD-WANに対応する Panorama とファイアウォールのセットアップ に進み、SD-WAN 展開の構成を開始します。

Panorama のインターネット非接続時のSD-WAN プラグインのインストール

SD-WAN デプロイメントの設定および管理には、SD-WAN プラグインを備えた Panorama™ 管理サーバが必要となります。Panorama がインターネットに接続されていない場合は、SD-WAN プラグインを Palo Alto Networks のカスタマーサポート ポータルからダウンロードして、Panorama 管理サーバにアップロードします。プラグインのインストールが必要なのは、SD-WAN ファイアウォールを管理する Panorama のみです。個々のハブ ファイアウォールやブランチ ファイアウォールにインストールする必要はありません。

STEP 1 | Palo Alto Networksカスタマーサポートポータルにログインします。

STEP 2 | **Updates (**更新**)** 、 **> Software Updates (**ソフトウェアの更新**)** を選択して、Filter By (フィルタ条件) のドロップダウンで **Panorama Integration Plug In (Panorama** 統合プラグイン**)** を選択します。

STEP 3 | **SD-WAN Plug-in**を検索してダウンロードします。

STEP 4 | Panorama Web インターフェイスへのログイン。

STEP 5 | **Panorama** 、 **> Plugins (**プラグイン**)** を選択し、SD-WAN プラグインを **Upload (**アップロード**)** します。

STEP 6 | **Browse (**参照**)** して、カスタマーサポート プラグインからダウンロードしたSD-WAN プラグインを検索し、**OK** をクリックします。

STEP 7 | SD-WAN プラグインを **Install (**インストール**)** します。

STEP 8 | SD-WAN プラグインのインストールが正常に完了した後、**Commit (**コミット**)** および **Commit to Panorama (Panorama** へのコミット**)** します。

この手順は、いずれの設定の変更を Panorama にコミットする前に必要となります。

STEP 9 | (Management Only mode only)SD-WAN 監視データの保存に必要なログディスクを有効にします。

- **M-Series Appliances**:すべてのMシリーズアプライアンスには、デフォルトでRAID 1に2組の8TBロギングディスクが付属しています。管理専用モードで Panorama から SD-WAN

を使用して firewall を管理する場合は、SD-WAN モニタリングデータを保存するために、ロギングディスクペアの最初のペアを有効にする必要があります。

1. Panorama CLI へのログインを行います。
2. M-Seriesアプライアンスにデフォルトで含まれているロギングディスクペアの最初のペアを有効にします。

   ```
   >show system raid add A1
   ```

3. `Logging Disk Pair A` が 利用可能 であることを確認します。

   ```
   > show system raid detail
   ```

   RAID のセットアップが完了すると、以下の応答が表示されます。

   ```
   Disk Pair A       Available Status         clean Disk id
    A1     Present model :ST91000640NS size :953869 MB status:
    active sync
   ```

4. ログ ディスクのペアをログに使用できるようにします。
   1. **Panorama** > **Managed Collectors** を選択し、Log Collector を編集します。
   2. **Disks**（ディスク）を選択し、各アレイを **Add**（追加）します。
   3. **OK** をクリックして変更内容を保存します。
   4. **Commit** > **Commit to Panorama**および **Commit** を選択し、変更をコミットします。
   5. **Commit** > **Push to Devices** を選択し、Collector Group と **Push** を選択します。

- **Panorama Virtual Appliances**:Panorama 仮想アプライアンスを管理専用モードで展開した場合、SD-WAN 監視データを保存するには、システム ディスクを 224 GB に増やす必要があります。

STEP 10 | SD-WANに対応する Panorama とファイアウォールのセットアップ に進み、SD-WAN 展開の構成を開始します。

SD-WANに対応する Panorama とファイアウォールのセットアップ

SD-WAN デプロイメントの設定を開始する前に、ハブ ファイアウォールおよびブランチ ファイアウォールを管理対象デバイスとして追加し、SD-WAN の設定を SD-WAN ファイアウォールへのプッシュを正常に実行するために必要なテンプレートおよびデバイス グループの設定を作成する必要があります。

- SD-WAN ファイアウォールの管理対象デバイスとしての追加
- SD-WAN ネットワークテンプレートの作成
- Panorama の事前定義ゾーンの作成
- SD-WAN デバイス グループの作成

SD-WAN ファイアウォールの管理対象デバイスとしての追加

SD-WAN 展開の構成を開始する前に、まずハブとブランチファイアウォールを管理対象デバイスとして Panorama™ 管理サーバーSD-WAN プラグインのインストールに追加する必要があります。SD-WAN ファイアウォールを Panorama ™ 管理サーバーの管理対象デバイスとして追加する作業の一環として、SD-WAN ライセンスをアクティベートして、ファイアウォールの SD-WAN 機能を有効にする必要があります。

SD-WAN ファイアウォールを管理対象デバイスとして追加する作業の一環として、ログを Panorama に転送するように管理対象ファイアウォールを設定する必要があります。Panorama は、設定ログ、トラフィック ログ、リンク特性測定値等の複数の送信元から情報を収集し、SD-WAN アプリケーションの可視性を生成し、ヘルス情報をリンクします。

*SD-WAN*オーバーレイにのみ依存するよう*Panorama*管理サーバー接続を用意しないでください。*Panorama*が常に*PAN-OS*ファイアウォールに到達可能な信頼性の高い接続を維持するためには、*PAN-OS*ファイアウォールから*Panorama*（*Panorama*があるハブ/ブランチ間の*SD-WAN*オーバーレイの外側）に到達する専用の*IPSec*トンネルを作成することをお勧めします。このアプローチにより、*SD-WAN*オーバーレイに何らかの影響があったとしても、*Panorama*管理サーバーに常に到達できるようにすることができます。

STEP 1 | ファイアウォール Webインターフェースを起動します。

STEP 2 | SD-WAN ライセンスをアクティベート して、ファイアウォールでの SD-WAN 機能を有効にします。

SD-WAN デプロイメントで使用する各ファイアウォールには、それぞれライセンスをアクティベートする一意の認証コードが必要です。例えば、100 台のファイアウォールがある場合、100 個の SD-WAN ライセンスを購入し、各ファイアウォールで 100 個の一意の認証

コードの中の 1 つを使用して、各SD-WAN ライセンスをアクティベートする必要があります。

VM-Series のファイアウォールの場合は、特定の *VM-Series* ファイアウォールに対して*SD-WAN* 認証コードを適用します。VM-Series ファイアウォールをディアクティベートする場合、*SD-WAN* 認証コードは、同じモデルの別の *VM-Series* ファイアウォールでアクティベートすることができます。

引き続き *SD-WAN* を利用するには、*SD-WAN* ライセンスが有効であることを確認してください。*SD-WAN* ライセンスの有効期限が切れると、以下の事象が発生します。

- 設定の変更を ***Commit (***コミットすると、警告が表示されます。コミットのエラーは発生しません。
- *SD-WAN* の設定は機能しませんが、削除はされません。
- ファイアウォールはリンクのヘルスメトリックの監視および収集を実行せず、モニタリング プローブの送信を停止します。
- ファイアウォールは、アプリケーションおよびリンクのヘルスメトリックを *Panorama* に送信しなくなります。
- *SD-WAN* パス選択ロジックが無効になります。
- 新しいセッションは、仮想 SD-WAN インターフェースでラウンドロビン方式で処理されます。
- 既存のセッションは、ライセンスの有効期限が切れた時点での特定のリンクに残留します。
- インターネットの停止が発生した場合、トラフィックは標準のルーティングと、設定済の場合は ECMP を使用します。

STEP 3 | Panorama の IP アドレスをファイアウォールに追加します。

1. **[Device]** > [セットアップ] > [管理] の順に選択し、[Panorama 設定] を編集します。
2. 先頭のフィールドに Panorama の IP アドレスを入力します。

   Panorama FQDN は、*SD-WAN* ではサポートされません。

3. (任意) Panorama で高可用性 (HA) ペアをセットアップした場合は、2 番目のフィールドにセカンダリ Panorama の IP アドレスを入力します。
4. **Enable pushing device monitoring data to Panorama(**デバイス監視データの **Panorama** へのプッシュを有効にする**)**が選択されていることを確認します。
5. **OK** をクリックします。
6. 変更を **Commit (**コミット**)**します。

STEP 4 | Panorama へのログ転送の設定を行います。

モニタリングおよびレポートデータを表示するには、SD-WANファイアウォールからPanoramaにログを転送する必要があります。

デフォルトでは、アプリケーション トラフィックの復号化が有効になっている場合、*HTTP/2* インスペクションは自動的に有効になります。*HTTP/2*接続を使用する親セッションは、アプリケーション トラフィックを伝送しないため、トラフィック ログを生成しません。ただし、*HTTP/2* 親セッション内のストリームで生成された子セッションは、引き続きトラフィック ログを生成します。*HTTP/2* 接続のログの閲覧に関する詳細については、Palo Alto Networks Knowledgebase (Palo Alto Networks ナレッジベース)を参照してください。

STEP 5 | Panorama に 1 つ以上のインターフェイスを追加します。

ファイアウォールの Panorama への追加方法の詳細については、 管理対象デバイスとしてのファイアウォールの追加をご参照ください。

1. Panorama Web インターフェイスへのログイン。
2. **Panorama** > **Managed Devices(Panorama**管理対象デバイス**)** > **Summary (**概要**)** を選択して、ファイアウォールを **Add(**追加**)** します。
3. ファイアウォールのシリアルナンバーを入力します。
4. 必要なデバイス グループおよびテンプレートが既に作成されている場合にファイアウォールを追加するには、**Associate Devices (**デバイスの関連付け**)** を有効にして (オンにして) 適切なデバイス グループとテンプレート スタックに新しいファイアウォールを割り当てます。
5. CSV を使用して複数のファイアウォールを追加するには、**Import(**インポート**)** を選択して、**Download Sample CSV(**サンプル **CSV** のダウンロード**)** を選択し、ファイアウォールの情報を入力し、**Browse (**参照**)** を選んでファイアウォールをインポートします。
6. **OK** をクリックします。

STEP 6 | **Commit (**コミット**)** を選択して、設定を **Commit and Push (**コミットしてプッシュ**)** します。

STEP 7 | SD-WAN 展開で使用する各ファイアウォールで、ステップ 2 から 5 を繰り返します。

SD-WAN ネットワークテンプレートの作成

SD-WAN ハブおよびブランチのすべてのネットワーク設定 オブジェクトを含むテンプレートを作成します。ハブのファイアウォール向けには個別のテンプレートおよびテンプレート スタックを作成し、ブランチのファイアウォール向けに個別のテンプレートおよびテンプレート スタックを作成する必要があります。SD-WAN デバイス 設定の管理に使用するテンプレートおよびテンプレートスタックの数は制限しておくことが推奨されます。すべてのハブとブランチで使用されるテンプレートおよびテンプレート スタックの数を制限することにより、複数の SD-WAN ハブとブランチの設定管理の運用上のオーバーヘッドが大幅に削減されます。使用するテンプレート数を減らすには、template or template stack variables(テンプレートまたはテンプレートスタック変数) を使用します。

STEP 1 | Panorama Web インターフェイスへのログイン。

STEP 2 | SD-WAN ハブのネットワーク テンプレートを作成します。

1. **Panorama**、 > **Templates** (テンプレート) と選択し、**Add** (追加) します。
2. **Name** (名前) フィールドにわかりやすいテンプレート名を入力します。
3. （任意）テンプレートの**Description**（説明）入力します。
4. **OK** をクリックして、設定の変更を保存します。

STEP 3 | ハブのテンプレート スタックを作成します。

1. 新しいテンプレート スタックを追加するには、**Panorama** 、 > **Templates** (テンプレート) と選択し、**Add Stack**(スタックを追加)します。
2. **Name** (名前) フィールドにわかりやすいテンプレート スタック名を入力します。
3. （任意）テンプレートの**Description**（説明）入力します。
4. ステップ 2 で作成した SD-WAN ネットワーク テンプレートを **Add** (追加) します。
5. **Devices** (デバイス) セクションで、すべての SD-WAN ハブのファイアウォールのチェックボックスをオンにします。
6. **OK** をクリックして、設定の変更を保存します。

STEP 4 | SD-WAN ブランチのネットワーク テンプレートを作成します。

1. 新しいテンプレートを **Add** (追加) します。
2. **Name** (名前) フィールドにわかりやすいテンプレート名を入力します。
3. （任意）テンプレートの**Description**（説明）入力します。
4. **OK** をクリックして、設定の変更を保存します。

STEP 5 | ブランチのテンプレート スタックを作成します。

1. 新しいテンプレート スタックを追加するには、**Add Stack (**スタックの追加**)** をクリックします。
2. **Name (**名前**)** フィールドにわかりやすいテンプレート スタック名を入力します。
3. （任意）テンプレートの**Description**（説明）入力します。
4. ステップ 4 で作成した SD-WAN ネットワーク テンプレートを **Add** (追加) します。
5. **Devices (**デバイス**)** セクションで、すべての SD-WAN ブランチのファイアウォールのチェックボックスをオンにします。
6. **OK** をクリックして、設定の変更を保存します。

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

Panorama の事前定義ゾーンの作成

SD-WAN ポリシールールでは、内部パスの選択およびトラフィック転送に事前定義済みゾーンを使用します。ユースケースは 2 つあります。既存のセキュリティポリシーがある現在使用中の PAN-OS® ファイアウォールで SD-WAN を有効にしている場合、そして、それまでセキュリティ ポリシー ルールがなく、まったく新たに PAN-OS を展開する場合には別々のユースケースを採用します。現在使用中のファイアウォールにセキュリティ ポリシー ルールが設定されている場合は、SD-WAN ポリシーが使用する事前定義済みゾーンに既存のゾーンをマッピングします。

SD-WAN エンジンは、トラフィックを転送にこの事前定義済みゾーンを利用します。また、Panorama ™ テンプレートで事前定義済みゾーンを作成すると、マネージド ファイアウォールと Panorama 間で、一貫した可視性が提供されます。

- **Zone Internet (**ゾーン インターネット**)** -信頼されていないインターネットとの間で送受信されるトラフィック向け。
- **Zone to Hub (**ハブへのゾーン**)**- ブランチ ファイアウォールからハブ ファイアウォールへのトラフィック、およびハブ ファイアウォール間でのトラフィック向け。
- **Zone to Branch (**ブランチへのゾーン**)**-ハブ ファイアウォールからブランチ ファイアウォールへのトラフィック、およびブランチ ファイアウォール間のトラフィック向け。
- **Zone Internal(**内部ゾーン**)**- 特定の場所の内部トラフィック向け。
- **Zone to PA Hub (PA**ハブへのゾーン**)** – 内部トラフィックがプリズマアクセスハブに到達する場合。

事前定義済みゾーンを作成しない場合、*SD-WAN* プラグインはブランチおよびハブのファイアウォールに事前定義済みゾーンを自動的に作成します。これは、*Panorama* では表示されません。

事前定義済みゾーンの 2つの ユースケース。

- **Existing Zones (**既存のゾーン**)**- User-ID™ および多様なポリシー (セキュリティ ポリシー ルール、QoSポリシールール、ゾーン保護、およびパケットバッファー保護) が採用されている既存のゾーンがある場合。ファイアウォールの適切なトラフィック転送のために、既存のゾーンをSD-WAN が使用する事前定義済みのゾーンにマップする必要があります。新しい事前定

義済みゾーンは SD-WAN 転送にのみ利用されるため、全ポリシーで既存のゾーンを継続して使用する必要があります。CSV ファイルを作成して、Panorama への SD-WAN デバイスの追加するときにゾーンをマップします。(CSV ファイルを使用しない場合、**Panorama** の > **SD-WAN** > **Devices(**デバイス**)** の設定の際、そして **Zone Internet (**ゾーン インターネット**)**、**Zone to Hub (**ハブへのゾーン**)**、**Zone to Branch (**ブランチへのゾーン**)**、**Zone Internal (**内部ゾーン**)** に既存のゾーンを追加する際にマップします。)

マッピングを行うと、ブランチ ファイアウォールまたはハブ ファイアウォールが転送検索を実行して、出口 SD-WAN インターフェース、つまり出力ゾーンを決定することができます。既存のゾーンを事前定義済みのゾーンにマッピングしない場合は、許可されたセッションが SD-WAN を使用しません。現在使用中の場合、さまざまなゾーン名が設定されています。ファイアウォールはこのようなゾーン名をすべて事前定義済みのゾーンに絞り込む必要があるため、マッピングが必要となります。必ずしもすべての定義済みゾーンにゾーンをマップする必要はありませんが、既存のゾーンを少なくとも **Zone** から **Hub** ゾーンおよび **Zone to Branch** ゾーンにマップする必要があります。

- **No Existing Zones (**既存のゾーンなし**)**-今回初めてPalo Alto Networks® ファイアウォールおよび SD-WAN を新たにデプロイする場合。この場合、マップするゾーンが存在しないため、デプロイメントを簡素化するために、PAN-OS ポリシーで事前定義済みゾーンおよびユーザー ID の使用が推奨されます。

SD-WAN デプロイメントの設定を開始する前に、両方のユースケースで、**zone-internet(**ゾーン インターネット**)**、**zone-internal (**内部ゾーン**)**、**zone-to-hub(**ハブへのゾーン**)**、**zone-to-branch(**ブランチへのゾーン**)** および**zone-to-pa-hub (PA**ハブへのゾーン**)** と名付ける必須の事前定義済みゾーンを Panorama で作成します。ブランチとハブのファイアウォールをオンボードすると、Panorama への SD-WAN デバイスの追加します。既に製品をご使用の場合、SD-WAN プラグインは、SD-WAN ポリシー ルール、QoS ポリシー ルール、ゾーン保護、ユーザー ID、およびパケット バッファー保護を実行する際、SD-WANプラグインは既存のゾーンを上記の事前定義済みゾーンに内部的にマッピングし、事前定義済みゾーンを使用して、Panorama でゾーンのログ記録と表示を行います。新たに使用する場合、事前定義済みのゾーンにより適切なセットアップが提供されています。

事前定義済みゾーンは、設定を Panorama から管理対象の SD-WAN デバイスにプッシュする際にお使いのSD-WAN ハブとブランチ間に VPN トンネルを自動的にセットアップする上でも必要です。

ゾーン名では大文字と小文字が区別されるため、この手順で提供する名前は大文字と小文字の違いに注意する必要があります。ゾーン名がこの手順で設定する名前と一致しない場合、ファイアウォール上のコミットは失敗します。

この例は、**zone-internet (**ゾーン インターネット**)** という名前のゾーンを作成しています。

STEP 1 | Panorama Web インターフェイスへのログイン。

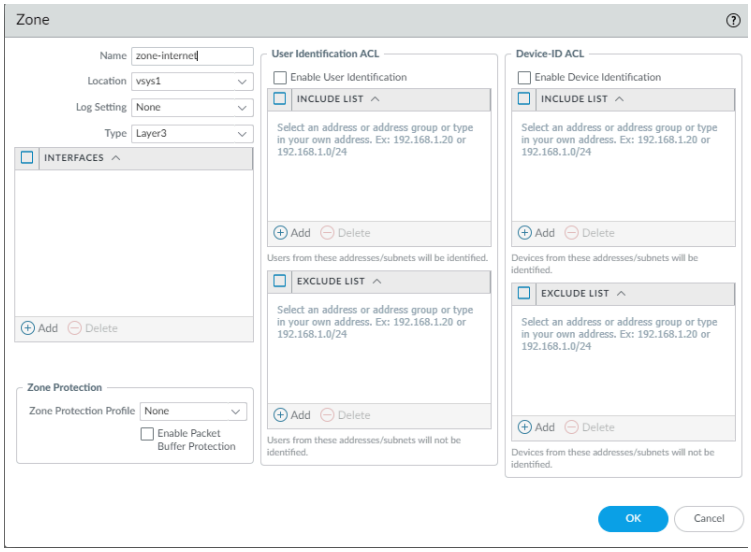
STEP 2 | **Network (**ネットワーク**)**、 > **Zones (**ゾーン**)** を選択し、**Template (**テンプレート**)** コンテクスト ドロップダウンで以前に作成した network template (ネットワーク テンプレート) を選択します。

STEP 3 | 新しいゾーンを **Add (**追加**)** します。

STEP 4 | ゾーンの **Name** (名前) に、例えば、**`zone-internet`** (ゾーン インターネット) と入力します。

STEP 5 | ゾーン**Type** (タイプ) には、**Layer3** (レイヤー 3) を選択します。

STEP 6 | **OK** をクリックします。



STEP 7 | 残りのゾーンについても、この手順を繰り返します。全体で以下のゾーンを作成する必要があります。

- **`zone-to-branch`** (ブランチへのゾーン)
- **`zone-to-hub`** (ハブへのゾーン)
- **`zone-internal`** (内部ゾーン)
- **`zone-internal`** (ゾーン インターネット)
- **`zone-to-pa-hub`** (**PA**ハブへのゾーン)

STEP 8 | 設定の変更を **Commit** (コミット) および**Commit and Push** (コミットしてプッシュ) します。

STEP 9 | 変更を **Commit** (コミット)します。

SD-WAN デバイス グループの作成

SD-WAN ハブとブランチのすべてのポリシー ルールおよび設定 オブジェクトを含むデバイス グループをハブととブランチ向けに作成します。ハブとブランチのデバイス グループの作成後、ハブとブランチ ゾーン間のトラフィックを許可する各デバイス グループにセキュリティ ポリシー ルールを作成する必要があります。このセキュリティ ポリシーを作成しておくと、SD-WAN プラグインが create a VPN cluster (VPN クラスタの作成) をする際、SD-WAN デバイス ゾーン間のトラフィックが許可されます。

ハブ ファイアウォール全体の設定は同一に、ブランチ ファイアウォール全体の設定も同一に構成します。これにより、複数の *SD-WAN* ハブおよびブランチの設定管理の運用オーバーヘッドが大幅に削減され、設定の問題のトラブルシューティング、分離、更新をより迅速に実行することができます。

STEP 1 | Panorama Web インターフェイスへのログイン。

STEP 2 | 「Panorama の事前定義ゾーンの作成」を行います。

STEP 3 | SD-WAN ハブ デバイスグループを作成します。

1. **Panorama** > **Device Groups** (デバイス グループ)と選択し、デバイス グループを **Add** (追加) します。
2. デバイス グループの **Name** (名前) として、**SD-WAN_Hub** を入力します。
3. （任意）テンプレートの**Description**（説明）入力します。
4. **Devices** (デバイス) セクションで、チェックボックスをオンにしてSD-WAN ハブをグループに割り当てます。
5. **Parent Device Group** (親デバイス グループ) は**Shared** (共有) のままにします。
6. **OK** をクリックします。

STEP 4 | SD-WAN ブランチ デバイスグループを作成します。

1. **Panorama** > **Device Groups** (デバイス グループ)と選択し、デバイス グループを **Add** (追加) します。
2. デバイス グループの **Name**(名前) は、**SD-WAN_Branch** と入力します。
3. （任意）テンプレートの**Description**（説明）入力します。
4. **Devices**(デバイス)セクションでチェックボックスをオンにして、SD-WAN ブランチをグループに割り当てます。
5. **Parent Device Group** (親デバイス グループ) は**Shared** (共有) のままにします。
6. **OK** をクリックします。

STEP 5 | ブランチ オフィスからハブの内部ゾーン、そしてハブの内部ゾーンからブランチ オフィスへのトラフィック フローを制御するセキュリティ ポリシー ルールを作成します。

1. **Policies (ポリシー)**、 > **Security (セキュリティ)** を選択し、**Device Group (デバイス グループ)** コンテクスト ドロップダウンで **SD-WAN_Hub** デバイスグループを選択します。
2. 新しいポリシールールを**Add(追加)** します。
3. ポリシールールの**Name (名前)** を、例えば、**`SD-WAN access--hub DG`** と入力します。
4. **Source (送信元)** > **Source Zone (送信元ゾーン)** を選択し、**zone-internal (内部ゾーン)** および **zone-to-branch (ブランチへのゾーン)** を **Add (追加)** します。
5. **Destination (宛先)** > **Destination Zone(宛先ゾーン)** と選択し、**zone-internal (内部ゾーン)** および**zone-to-branch(ブランチへのゾーン)** を**Add (追加)** します。
6. 許可する **Application (アプリケーション)** を選択して **Add (追加)** します。

   BGP ルーティングを使用している場合は、*BGP* を許可する必要があります。
7. **Actions (アクション)** を選択して、選択したアプリケーションを **Allow (許可)** します。
8. **Target (対象)** を選択して、Panorama™ がルールをプッシュする対象デバイスを指定します。

STEP 6 | ブランチ オフィスからハブの内部ゾーン、そしてハブの内部ゾーンからブランチ オフィスへのトラフィック発信を制御するセキュリティ ポリシー ルールを作成します。

1. **Policies (ポリシー)**、 > **Security (セキュリティ)** を選択し、**Device Group (デバイス グループ)** コンテクスト ドロップダウンで **SD-WAN_Branch** デバイス グループを選択します。
2. 新しいポリシールールを**Add(追加)** します。
3. ポリシールールの**Name (名前)** を、例えば、**`SD-WAN access--branch DG`** と入力します。
4. **Source(送信元)** > **Source Zone (送信元ゾーン)** を選択し、**zone-internal (内部ゾーン)**および**zone-to-hub (ハブへのゾーン)** を **Add(追加)** します。
5. **Destination (宛先)** > **Destination Zone (宛先ゾーン)** と選択し、**zone-internal(内部ゾーン)**および**zone-to-hub(ハブへのゾーン)** を **Add (追加)** します。
6. 許可する **Application (アプリケーション)** を選択して **Add (追加)** します。

   BGP ルーティングを使用している場合は、*BGP* を許可する必要があります。
7. **Actions (アクション)** を選択して、選択したアプリケーションを **Allow (許可)** します。
8. **Target (対象)** を選択して、Panorama がルールをプッシュする対象デバイスを指定します。

STEP 7 | 構成した設定をコミットおよびプッシュします。

1. 設定の変更を **Commit (コミット)** および**Commit and Push (コミットしてプッシュ)** します。
2. [Push Scope] (プッシュの範囲) セクションで、**Edit Selections (選択内容の編集)** をクリックします。
3. **Include Device and Network Templates (デバイスおよびネットワークのテンプレートを含める)** を有効 (チェックをオン) にして **OK** をクリックします。
4. 設定変更を **Commit and Push(コミットおよびプッシュ)** します。

> デバイス グループとテンプレートの設定をコミットしてプッシュする場合、*2* つのコミット操作が自動的に実行されます。*2* つ目のコミットが正常に終了したことを確認するには、***Tasks (タスク)*** を表示します。この *2*回のコミット操作では、*1* 回目の操作は常に失敗します。

リンクタグの作成

リンクタグを作成して、SD-WAN トラフィック分散およびフェイルオーバー保護中にアプリケーションとサービスが特定の順序で使用する 1 つまたは複数の物理リンクを識別します。複数の物理リンクをグループ化すると、物理リンクの状態が悪化した場合に、アプリケーションとサービスの品質を最大化することができます。

リンクをグループ化する方法を計画する際は、リンクの使用または目的を考慮して、適切にグループ化を行います。例えば、低コストあるいはビジネスクリティカル以外のトラフィックを対象とするリンクを設定している場合、リンクタグを作成してインターフェースをグループ化し、トラフィックがビジネスに不可欠なアプリケーションあるいはサービスに影響を与える可能性がある高コストのリンクではなく、主にこの低コストリンクを通過させることができます。

STEP 1 | Panorama Web インターフェイスへのログイン。

STEP 2 | **Objects(オブジェクト)**、 > **Tags (タグ)** と選択し、**Device Group(デバイス グループ)**コンテクスト ドロップダウンでデバイス グループを選択します。

STEP 3 | 新しいタグを **Add (追加)** します。

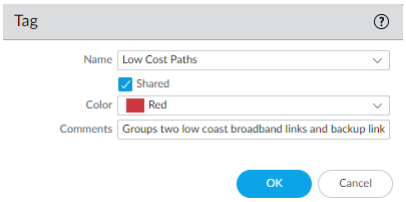
STEP 4 | タグには、わかりやすい**Name (名前)** を入力します。例えば、低コストパス、高コストパス、一般アクセス、プライベート HQ、またはバックアップ等が考えられます。

STEP 5 | **Shared** を有効にして、Panorama™ 管理サーバー上のすべてのデバイス グループと、単一の vsys ハブまたはブランチ上のデフォルトの vsys、またはプッシュ先の複数の vsys ハブまたはブランチ上の vsys1 でリンク タグを使用できるようにします。

共有リンクタグの設定により、Panorama はファイアウォールの設定検証でリンクタグを参照して、設定を正常にコミットし、ブランチとハブにプッシュすることができます。Panorama がリンクタグを参照できないと、コミットは正常に完了しません。

STEP 6 | (任意) タグの**Color(色)** を選択します。

STEP 7 | タグに関する役に立つ **Comments (コメント)** を入力します。例えば、一般的なインターネット アクセス用の **2** つの低コスト ブロードバンド リンクとバックアップ リンクのグループ化 とします。



STEP 8 | **OK** をクリックして、設定の変更を保存します。

STEP 9 | 設定の変更を **Commit (コミット)** および**Commit and Push (コミットしてプッシュ)** します。

STEP 10 | 「SD-WAN インターフェース プロファイルの設定」を行います。

SD-WAN インターフェース プロファイルの設定

SD-WAN インターフェース プロファイルを作成して ISP 接続の特性を定義し、リンクの速度およびファイアウォールのリンク監視頻度を指定し、リンクのリンクタグを指定します。複数のリンクで同じリンクタグを指定すると、物理リンクがリンクバンドルあるいはファットパイプにグループ化 (バンドル化) されます。イーサネット インターフェースを保存する前に、SD-WAN インターフェース プロファイルを設定し、SD-WAN 対応イーサネット インターフェースで SD-WAN インターフェースを指定する必要があります。

リンクのグループ化は、共通の基準に基づいて定義します。例えば、優先度別に優先度が最も高いパスから優先度が最も低いパスという順でリンクをグループ化したり、リンクをコスト別にグループ化したりすることができます。

STEP 1 | Panorama Web インターフェイスへのログイン。

STEP 2 | **Network (ネットワーク)**、 > **Network Profiles (ネットワーク プロファイル)**、 > **Interface Profile (インターフェース プロファイル)** と選択し、**Template(テンプレート)** コンテクストドロップダウンで適切なテンプレートを選択します。

STEP 3 | SD-WAN インターフェース プロファイルを**Add (追加)** します。

STEP 4 | SD-WAN インターフェース プロファイルには、レポート、トラブルシューティング、統計情報に表示された場合にわかりやすい **Name (名前)** を入力します。

STEP 5 | マルチvsys Panorama™ 管理サーバを使用している場合は、vsys の **Location(場所)** を選択します。デフォルトでは、vsys1 が選択されています。

STEP 6 | このプロファイルがインターフェースに割り当てる **Link Tag (リンクタグ)** を選択します。

STEP 7 | プロファイルの **Description (説明)** を入力します。

STEP 8 | 事前定義済みリストから物理 **Link Type (リンクのタイプ)** を選択します。(リンク タイプには、**ADSL/DSL**、**Cable modem (ケーブルモデム)**、**Ethernet(イーサネット)** 、**Fiber (ファイバ)**、**LTE/3G/4G/5G**、**MPLS**、**Microwave/Radio (マイクロ波 / ラジオ波)**、**Satellite (衛星)**、**WiFi**、**Private Link1**、**Private Link2**、**Private Link3**、**Private Link4** もしくは その他).が提供されています)。PAN-OS 11.1.3では、SD-WANプラグイン3.2.1以降のリリースで、**Private Link1**、**Private Link2**、**Private Link3**、**Private Link4**などの追加のポイントツーポイントPrivate Linkタイプがサポートされます。**Private Link1**、**Private Link2**、**Private Link3**、**Private Link4**のリンクタイプでは、SD-WANブランチファイアウォールからSD-WANハブファイアウォールへのプレーンテキストトラフィックはサポートされていません。新しいPrivate Linkタイプのいずれかを構成するときは、パブリックリンクタイプのみで構成されたSD-WANポリシールールがハブにあることを確認してください。インターネット経由のトラフィックがブランチからハブにバックホールまたは失敗した場合、このSD-WANポリシールールと一致する必要があるためです。そうしないと、これらのPrivate Link（**Private Link1**、**Private Link2**、**Private Link3** 、**Private Link4**）がダイレ

クトインターネットアクセス（DIA）SD-WANインターフェイスの一部であるため、トラフィックはドロップされます。

（*PAN-OS 11.1.3*以降のリリース、*SD-WAN*プラグイン*3.2.1*以降のリリースの場合）追加のポイントツーポイント*Private Link*タイプを有効にするには、次のことを確認する必要があります。

- *Panorama*管理サーバーは *PAN-OS 11.1.3* で実行されている必要があります
- *Panorama*管理対象デバイスは *PAN-OS 11.1.3* で実行されている必要があります
- *SD-WAN* プラグインのバージョンは *3.2.1* である必要があります

（*PAN-OS 11.2.0*以降のリリース、*SD-WAN*プラグイン*3.3.0*以降のリリースの場合）追加のポイントツーポイント*Private Link*タイプを有効にするには、次のことを確認する必要があります。

- *Panorama*管理サーバーは *PAN-OS 11.2.0* で実行されている必要があります
- *Panorama*管理対象デバイスは *PAN-OS 11.2.0* で実行されている必要があります
- *SD-WAN* プラグインのバージョンは *3.3.0* である必要があります

ファイアウォールは、終端し、イーサネット接続としてファイアウォールに引き渡すすべての CPE デバイスをサポートすることが可能です。例えば、WiFi アクセスポイント、LTE モデム、レーザー / マイクロ波 CPE はすべて、イーサネット ハンドオフで終端可能です。

次のリンクタイプは、同じリンクタイプのみのトンネルを形成します。

- パブリック（またはその他）リンクタイプ：イーサネット、***ASDL/DSL***、ケーブルモデム、ファイバー、***LTE/3G/4G/5G*** 、***WiFi***、その他。

  他のパブリックリンクタイプへのパブリックリンクタイプであれば、トンネルは正常に作成されます。たとえば、イーサネットと他者のリンクタイプと他者間のリンクタイプでは、トンネルが正常に作成されます。

- *Private Link*タイプとポイントツーポイントリンクタイプ：***MPLS***、サテライト、***Private Link1***、***Private Link2***、***Private Link3*** 、***Private Link4***、およびマイクロ波/無線。

  *Private Link*タイプは、同じ*Private Link*タイプでのみトンネルを作成できます。たとえば、*MPLS-MPLS* リンクタイプおよび衛星-衛星リンクタイプは有効であるため、トンネルは正常に作成されますが、*MPLS*-衛星間ではトンネルは作成されません。

SD-WAN をサポートするために使用されるインターフェイスにゾーンが定義されている既存の *PAN-OS* 展開の場合、*Panorama* は、次の条件下でインターフェイスのゾーン名を事前定義された *SD-WAN* ゾーンの *1* つに自動的に構成する場合があります。

1. *SD-WAN*インターフェイスは、インターフェイスプロファイルでポイントツーポイントの*Private Link*タイプ（***MPLS***、サテライト、***Private Link1***、***Private Link2***、***Private Link3*** 、***Private Link4***、またはマイクロ波）として構成されています。
2. ***VPN*** データトンネルサポート チェックボックスは、*SD-WAN* インターフェイスプロファイルで無効 *(*オフ*)* になっています。これにより、*SD-WAN VPN* トンネルの外部にクリアテキストでトラフィックを転送するように *PAN-OS* に指示します。***Private Link1***、***Private Link2***、***Private Link3*** 、***Private Link4*** のリンクタイプは、*SD-WAN* ブランチファイアウォールから *SD-WAN* ハブファイアウォールへのプレーンテキストトラフィックをサポートしていないため、これらの*Private Link*タイプを設定するときは ***VPN*** データトンネルサポートオプションを有効のままにしておく必要があります。

ハブファイアウォールでは、条件 a) が満たされると、ゾーン名は "`zone-to-branch`" として構成されます。ブランチファイアウォールでは、条件 a) と条件 b) の両方が満たされている

場合、ゾーン名は "zone-to-hub" として構成されます。Panorama は、このステップを自動化して構成を簡素化し、ハブとブランチファイアウォール間の適切な通信を確保します。古いゾーン名を参照する既存のファイアウォールポリシーがある場合は、新しい事前定義された SD-WAN ゾーン名を反映するようにポリシーを更新する必要があります。

STEP 9 | ISP からの **Maximum Download (Mbps)** (最大ダウンロード **(Mbps)**) 速度をメガビット毎秒 (メガビット - Mb)単位で指定します (0～100,000 の範囲、デフォルトなし)。小数点以下 3 桁までの範囲を入力できます (例: 10.456)。ISP にリンク速度を問い合わせるか、speedtest.net 等のツールを使用してリンクの最大速度をサンプリングし、十分に時間をかけて最大値の平均を取ります。

STEP 10 | ISP への **Maximum Upload (Mbps)** (最大アップロード **(Mbps)**) 速度をメガビット毎秒 (メガビット - Mb)単位で指定します (0～100,000 の範囲、デフォルトなし)。小数点以下 3 桁までの範囲を入力できます (例: 10.456)。ISP にリンク速度を問い合わせるか、speedtest.net 等のツールを使用してリンクの最大速度をサンプリングし、十分に時間をかけて最大値の平均を取ります。

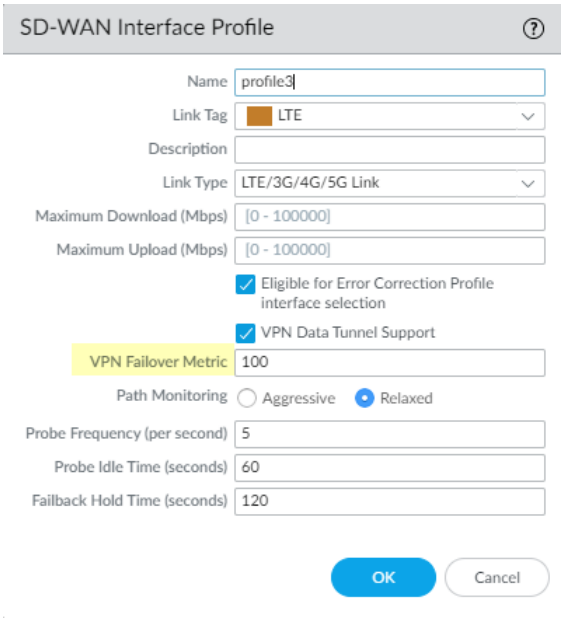
STEP 11 | **Eligible for Error Correction Profile interface selection** (エラー訂正プロファイル インターフェイスの選択対象) を選択して、Forward Error Correction (FEC) (前方誤り訂正) またはインターフェースのパケットの複製を有効化します。エンコード ファイアウォールとデコード ファイアウォールの両方でこれを有効にする必要があります。また、特定のアプリケーションの SD-WAN ポリシー ルールに適用するには、エラー訂正プロファイルを作成する必要があります。

STEP 12 | **VPN Data Tunnel Support**(**VPN** データ トンネルのサポート) が、ブランチからハブへのトラフィックと、リターントラフィックがVPN トンネルを通過してセキュリティを強化するかどうか (デフォルトの方法)、あるいは、暗号化のオーバーヘッドを回避して VPN トンネル外に通過させるかを決定します。

- 直接インターネット接続またはケーブルモデム、ADSL、その他のインターネット接続などのインターネット ブレイクアウト機能を備えたパブリック リンク タイプでは、 **VPN Data Tunnel Support (VPN** データ トンネル サポート) を有効のままにします。
- Private Linkタイプ（MPLS、サテライト、マイクロ波など）で、Private Linkタイプ（**Private Link1**、**Private Link2**、**Private Link3**、**Private Link4** 以外はインターネットブレークアウト機能なし）の **VPN** データトンネルサポートを無効にできます。ただし、この場合、トラフィックが VPNトンネル外に送信されるため、トラフィック傍受をされないようにする必要があります。
- （SD-WAN Plugin 3.2.1以降のリリース）**Private Link1**、**Private Link2**、**Private Link3**、**Private Link4**のリンクタイプは、SD-WANブランチファイアウォールからSD-WANハブファイアウォールへのプレーンテキストトラフィックをサポートしていないため、これらのPrivate Linkタイプを設定するときは、**VPN**データトンネルサポートを有効にしたままにする必要があります。
- ブランチには、ハブに接続するプライベート MPLS リンクにフェイルオーバーし、ハブからインターネットにアクセスする必要がある DIA トラフィックがある場合があります。**VPN Data Tunnel Support (VPN** データ トンネル サポート) の設定は、プライベートデータが VPN トンネルを通過するか、あるいはトンネル外を通過するかを決定し、フェイルオーバー トラフィックはその他の接続を使用します(プライベートデータフローは使

用しません)。ファイアウォールはゾーンを使用して、プライベート MPLS トラフィックからの DIA フェイルオーバー トラフィックをセグメント化します。

STEP 13 | DIA AnyPath の設定する場合、プリンシパル仮想インターフェイスは複数のハブ仮想インターフェイスを持つことができるため、フェールオーバー用に特定のハブを選択する順序に優先順位を付ける必要があります。このプロファイルが適用されるハブ仮想インターフェースにバンドルされている VPN トンネルに**VPN Failover Metric (VPN** フェイルオーバーメトリック**)** を設定して、このような優先度を指定します。メトリックが低いほど、フェールオーバー中に選択されるインターフェイスの優先順位が高くなります。複数のハブ仮想インターフェースに同じメトリック値がある場合、SD-WAN はラウンドロビン方式で新しいセッション トラフィックを送信します。



STEP 14 | (任意) SD-WAN インターフェース プロファイルを適用するインターフェースをファイアウォールが監視する **Path Monitoring (**パス モニタリング**)** モードを選択します。

ファイアウォールは、***Link Type (***リンク タイプ**)** に基づき、最適なモニタリング方法と考えられるものを選択します。(このプロファイルを適用する) インターフェースに、よりアグレッシブあるいははより緩やかなパス モニタリングが求められる問題がない限り、リンク タイプのデフォルト設定はこのまま変更しません。

- **Aggressive (**アグレッシブ**)**- (LTE および衛星を除くすべてのリンク タイプのデフォルト) ファイアウォールが、一定の頻度でプローブ パケットを SD-WAN リンクの反対側に送信します。このモードは、電圧低下およびブラックアウト時の高速検出およびフェイルオーバーが必要な場合に使用します。
- **Relaxed (**リラックスド**)**-(LTE およびサテライト リンク タイプのデフォルト) ファイアウォールのプローブパケットセットを送信する間隔が数秒空くため、**(Probe Idle Time (**プローブ アイドル時間**))** パス モニタリングの頻度が低下します。プローブ アイドル時間が経過すると、ファイアウォールは設定済の **Probe Frequency (**プローブ頻度**)** で 7 秒間プローブを送信します。このモードは、低帯域幅リンク、使用量に応じて課金されるリンク

(LTE等) を使用している場合、あるいはコストおよび帯域幅の維持と比べて高速検出が重要ではない場合に使用します。

STEP 15 | **Probe Frequency (per second) (**プローブ頻度 (秒)**)** を設定します。これは、SD-WAN リンクの反対側の端にファイアウォールがプローブパケットを 1 秒あたりに送信する回数です (1〜5 の範囲、デフォルトは 5)。デフォルト設定では、電圧低下および停電時に 1 秒未満での検出が提供されます。

Panorama テンプレートのプローブ頻度を変更する場合は、*Panorama* デバイスグループの *Path Quality profile* (パス品質プロファイル) の ***Packet Loss(***パケット損失**)** の割合のしきい値も調整する必要があります。

STEP 16 | **Relaxed (**リラックスド**)** パス モニタリングを選択した場合、ファイアウォールがプローブパケットセット間で待機する時間である **Probe Idle Time (seconds)(**プローブ アイドル時間 (秒)**)** を設定することができます 1〜60 の範囲、デフォルトは 60)。

STEP 17 | **Failback Hold Time (seconds) (**フェールバック待機時間 (秒)**)** を入力します。ファイアウォールは、フェイルオーバー後にリンクを優先リンクとして復元する前に、指定された時間分、回復したリンクが限定されたままで待機します (20〜120 の範囲、デフォルトは 120)。

STEP 18 | **OK** をクリックしてプロファイルを保存します。

STEP 19 | 設定の変更を **Commit (**コミット**)** および**Commit and Push (**コミットしてプッシュ**)** します。

STEP 20 | アプリケーションおよびリンクパスのヘルス メトリックを監視し、アプリケーションおよびリンクのヘルス パフォーマンスのレポートを生成します。詳細については、モニタリングおよびレポートを参照してください。

SD-WAN に対応する物理イーサネット インターフェースの設定

Panoramaで、物理的なレイヤー 3 イーサネット インターフェースを設定して、SD-WAN 機能を有効にします。物理インターフェイスを設定するには、IPv4またはIPv6アドレス、あるいはその両方を割り当てる必要があります。また、インターフェイスに完全修飾ネクストホップゲートウェイを割り当て、SD-WAN インターフェイスプロファイルをインターフェイスに割り当てる必要があります。(SD-WAN はレイヤ 3 インターフェイス タイプのみをサポートしますが、VPLS などのレイヤ 2 ネットワークはサポートしていません)。

Panorama を使用してVPN クラスタを作成し、ハブおよびブランチ情報を CSV にエクスポートすると、SD-WAN プラグインの自動 VPN 設定はその情報を使用して、事前定義済みの SD-WAN ゾーンを含め、関連するブランチおよびハブの設定を生成します。また、SD-WAN ブランチとハブの間には、セキュアな VPN トンネルが作成されます。自動 VPN 構成では、SD-WAN ブランチまたはハブを追加するときに CSV または Panorama に BGP 情報を入力すると、BGP 構成も生成されます。

STEP 1 | Panorama Web インターフェイスへのログイン。

STEP 2 | **Network(ネットワーク)**、 > **Interfaces (インターフェース)**、 > **Ethernet (イーサネット)** と選択します、**Template (テンプレート)** コンテクスト ドロップダウンで適切なテンプレートを選択して、スロット番号を選択し(Slot1など)、それからインターフェースを選択します(例えば、ethernet1/1 等)。

STEP 3 | **Interface Type (インターフェース タイプ)** は **Layer3** と選択します。

STEP 4 | [**Config (設定)**]タブで、レガシールーティングエンジンの場合、仮想ルータを選択するか、新しい仮想ルータを作成します。Advanced Routing Engine の場合は、**Logical Router** を選択するか、新しい論理ルーターを作成します。

STEP 5 | 設定中のインターフェースに適した **Security Zone** (セキュリティ ゾーン) を割り当てます。

例えば、ISP へのアップリンクを作成する場合、選択したイーサネット インターフェースが信頼されていないゾーンに面することを理解しておく必要があります。

STEP 6 | IPv4インターフェイスでSD-WANを有効にするには、[**IPv4**]タブを選択し、[**Enable SD-WAN (SD-WAN**を有効化)]を選択します。

SD-WANプラグイン3.2.0以降のリリースでは、SD-WAN対応インターフェイスに最大4つのIPアドレスを設定できます。SD-WANプラグインは、設定されたIPアドレスリストの最初のIPアドレスのみを使用してSD-WANトンネルを作成します。

SD-WANはネクストホップゲートウェイの最初の**IP**アドレスのみを考慮し、リスト内の残りの**IP**アドレスは無視します。

（HAデプロイメントのみ）SD-WANプラグインバージョン3.2.0から3.1.0以前のバージョンにダウングレードする場合は、PAN-OSおよびSD-WANプラグインバージョンのダウングレードなどのダウングレード手順を実行する前に、両方のファイアウォールのHAアクティブ/パッシブ構成を削除してください。

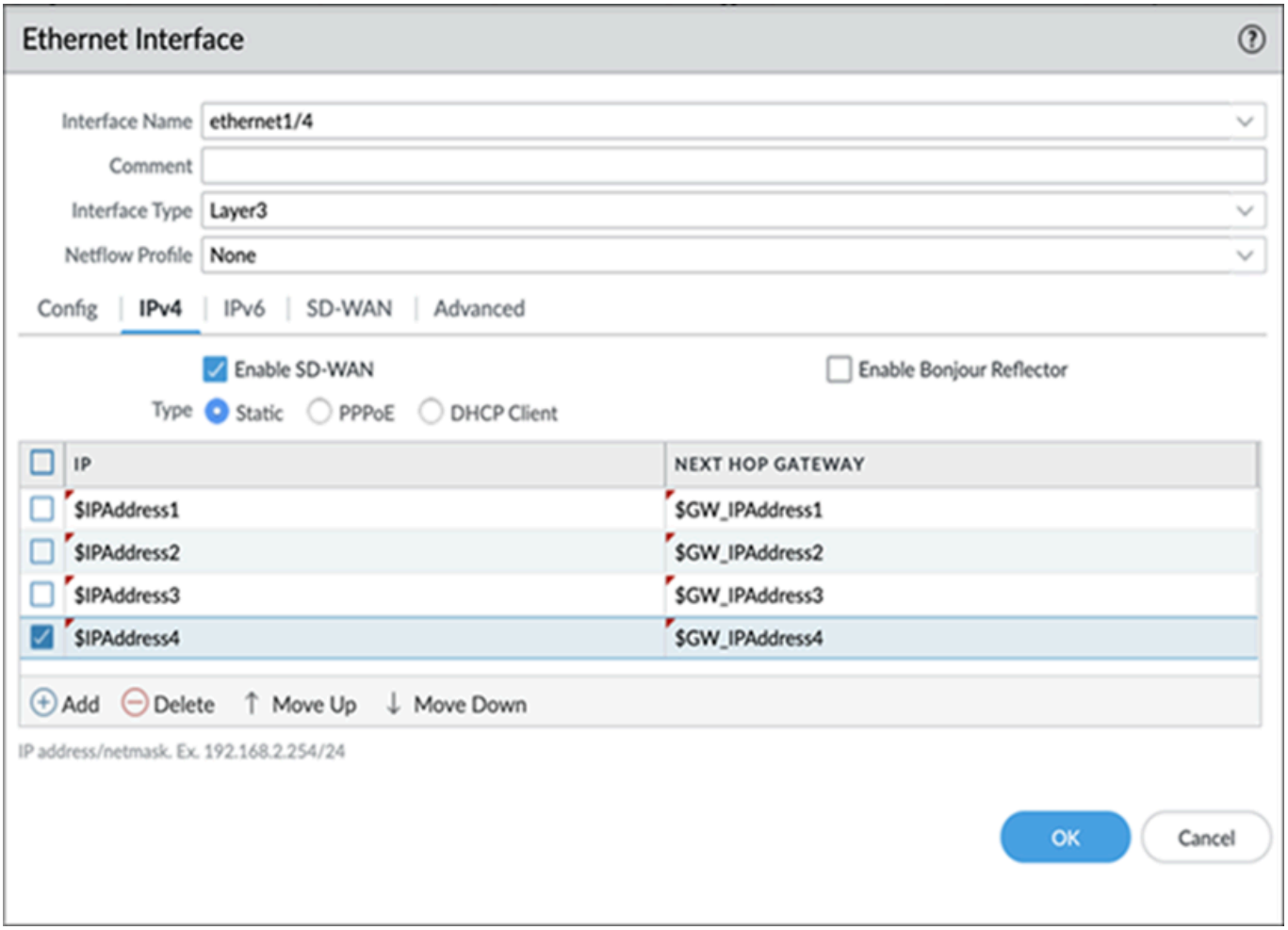
STEP 7 | IPv4インターフェイスの場合、アドレスの種類を以下から選択します。

- スタティック **-IP** フィールドで、インターフェースの IPv4 アドレスとプレフィックスの長さを **Add (**追加**)** します。アドレスの範囲には、 $uplink 等の定義済み変数が利用できます。の完全修飾 IPv4 アドレスを入力してください。ザ **Next Hop Gateway**(入力した IPv4 アドレスからの次ホップ)。ネクストホップ ゲートウェイは、IP v4 アドレスと同じサブネット上にある必要があります。ネクストホップ ゲートウェイは、サービス購入時に ISP から提供された ISP のデフォルト ルーターの IP アドレスです。この IP アドレスは、ISP のネットワーク、そして最終的にインターネットおよびハブにアクセスするためにファイアウォールがトラフィックを次に送信すべき IP アドレスです。
- **PPPoE**—DSL リンクの PPPoE 認証を **Enable (**有効化**)** し、**Username (**ユーザー名**)** と **Password (**パスワード**)** と **Confirm Password (**パスワードの確認**)** を入力します。
- **DHCP Client (DHCP** クライアント**)**-DHCP が、ISP 接続のネクストホップ接続とも呼ばれるデフォルト デートウェイを割り当てることが重要となります。動的IP アドレス、DNS

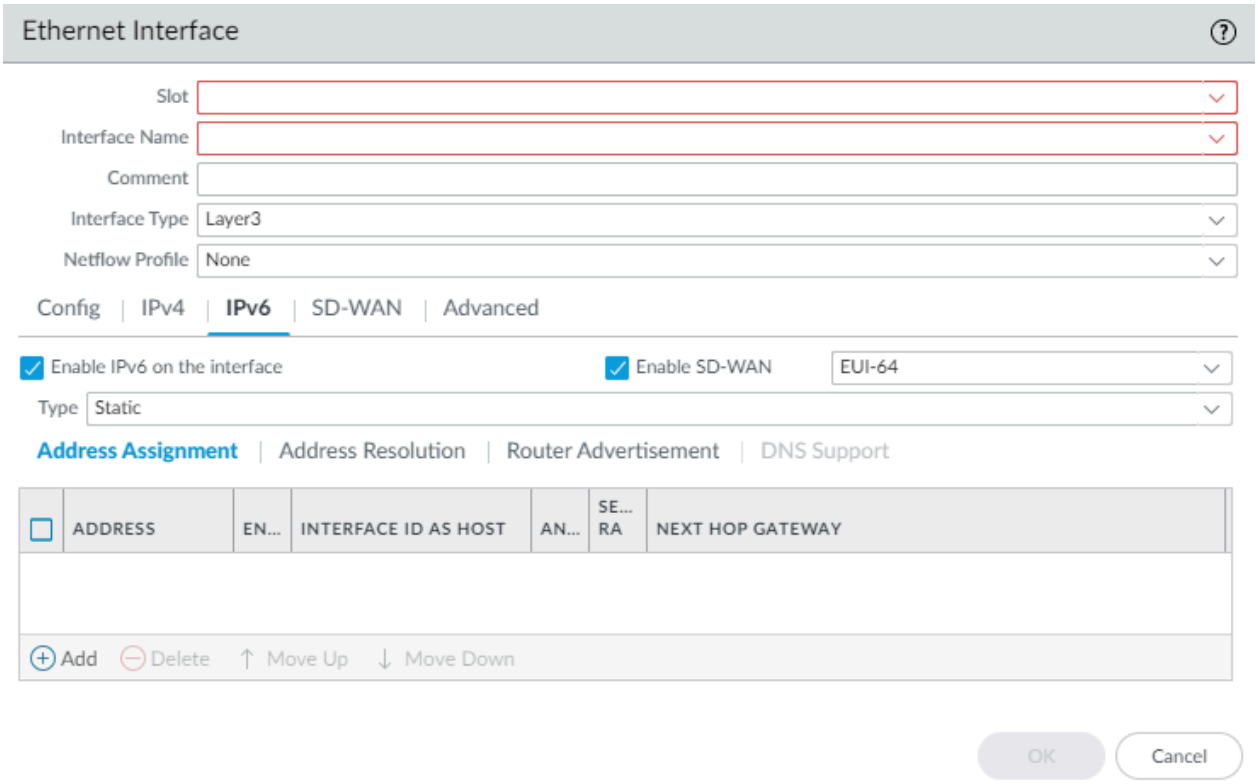
サーバー、デフォルト ゲートウェイ等、必要とされるすべての接続に関する情報は、ISP から提供されます。

DHCP クライアントはハブ インターフェイスまたはブランチ インターフェイスでサポートされていますが、ハブ インターフェイスでは、*DHCP* クライアントではなく ***Static (***静的*)* アドレスを割り当てることをお勧めします。ハブで*DHCP*を使用するには、*Palo Alto Networks DDNS*サービスが必要です。*DDNS* サービスが変更されたときに新しい *IP* アドレスを登録するのに数分かかる場合がありますが、ハブ サイトで静的アドレスを使用すると、*DHCP IP* アドレスの変更の解決に *DDNS* が関与せず、より安定した環境が作成されます。複数のブランチ サイトがハブ サイトに接続している場合、ネットワークを稼動し続けるには安定性が不可欠です。

DHCP クライアントを選択する場合は、デフォルトで有効にされている ***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する*)* オプションは、必ず無効にしてください。



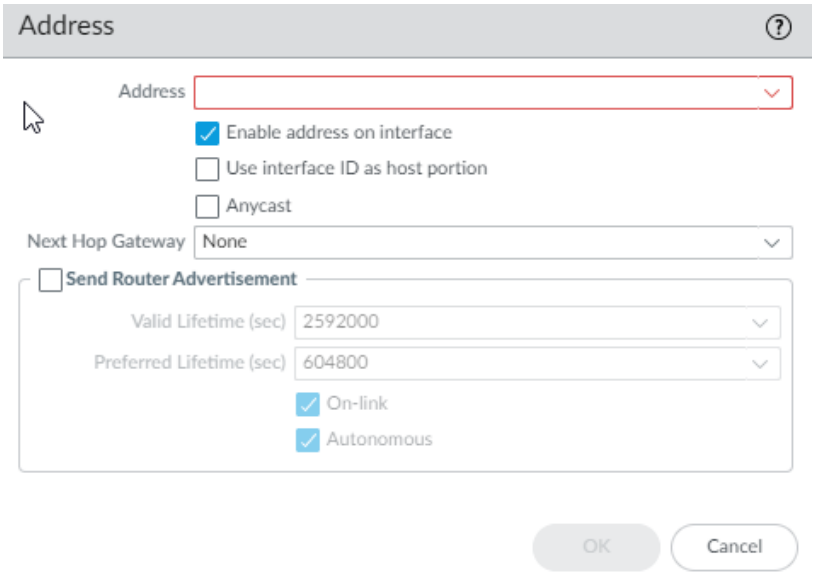
STEP 8 | IPv6インターフェイスでSD-WANを有効にするには、［**IPv6**］タブ、［**Enable IPv6 on the interface (**インターフェイスで**IPv6**を有効にする**)**］、［**Enable SD-WAN (SD-WAN**を有効にする**)**］を選択します。



STEP 9 | ［**EUI-64**（デフォルト**64**ビット拡張固有識別子）］フィールドに、64ビットEUIを16進数形式で入力します。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。

STEP 10 | IPv6インターフェイスの場合は、アドレスの種類を**[Static (静的)]**として選択します。**[アドレス割り当て]**タブを選択します。

1. インターフェイスのIPv6アドレスを追加するか、**[New Variable (新しい変数)]**を選択して変数を作成します。SD-WANは物理インターフェイスごとに1つのIPv6アドレスをサポートします。
2. インターフェイス上のアドレスを有効にします。



3. インターフェイス**ID**をホスト部分として使用する – 説明については、前の手順を参照してください。
4. **Anycast** – IPv6 アドレス（ルート）を Anycast アドレス（ルート）にする場合に選択します。つまり、複数のロケーションが同じプレフィックスをアドバタイズ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。
5. **Next Hop Gateway (**ネクスト ホップゲートウェイ**)** – Next Hop Gateway (入力した IPv4 アドレスからのネクスト ホップ) のIPv6 アドレスを入力します。ネクストホップ ゲートウェイは、IP v6 アドレスと同じサブネット上にある必要があります。ネクスト ホップ ゲートウェイは、サービス購入時に ISP から提供された ISP のデフォルト ルーターの IP アドレスです。ファイアウォールがISPのネットワーク、最終的にはインターネットとハブに到達するためにトラフィックを送信するネクストホップIPアドレスです。
6. **Send Router Advertisement (**ルーターのアドバタイジングを送信**)**–ファイアウォールがルーター アドバタイズメント(RA)でこのアドレスを送信できるように選択します。この場合、インターフェイス上 **(Router Advertisement (**ルーターアドバタイズメント**)**タブ) 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。
7. **Valid Lifetime (**有効な有効期間**) (**秒**)** – ファイアウォールがアドレスを有効とみなす有効期間（秒単位）を入力します。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）。

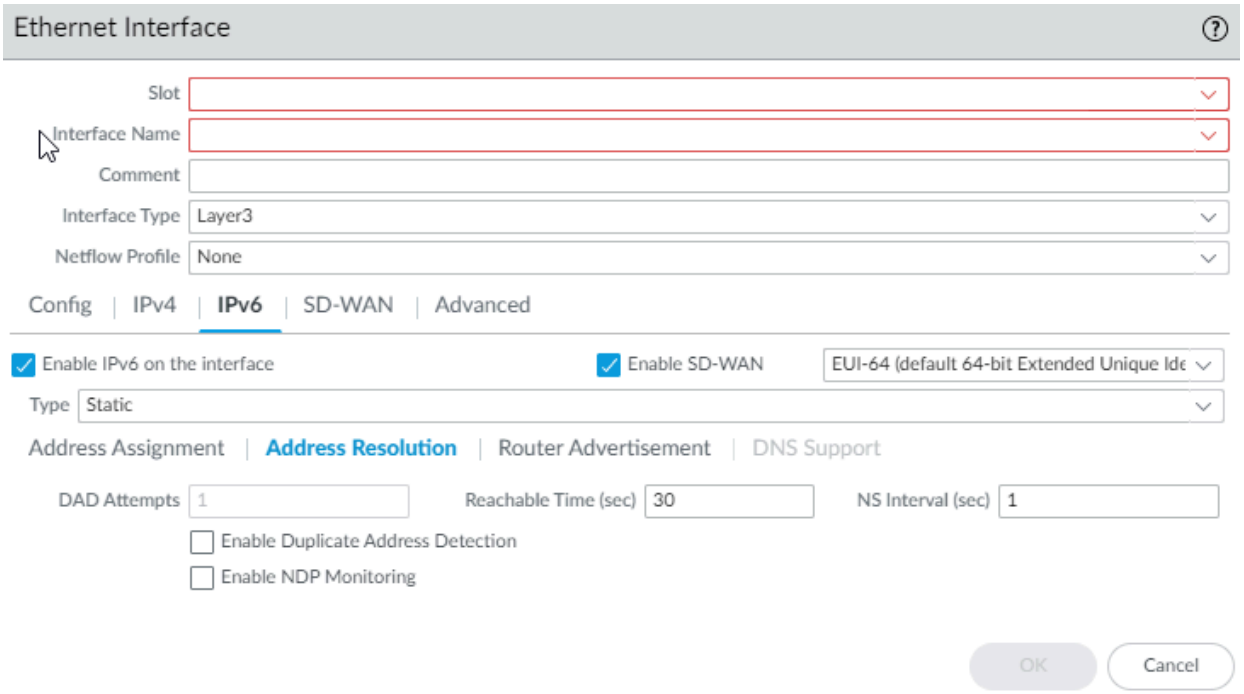
8. **Preferred Lifetime (優先ライフタイム) (秒)**:有効なアドレスが優先される時間の長さ (秒単位) (ファイアウォールがそのアドレスを使用してトラフィックを送受信できることを意味します)を入力します。優先ライフタイムの期限後は、ファイアウォールがこのアドレスを使用して新しい接続を確立することはできませんが、既存の接続は[Valid Lifetime（有効なライフタイム）]の期限まで有効です（デフォルトは 604,800）。
9. **On-link**（オンリンク） – プレフィックス内にアドレスがあるシステムにルーターなしで到達可能である場合に選択します。
10. **Autonomous**（自律型） – 通知されたプレフィックスとインターフェイス ID を組み合わせて、システムが IP アドレスを独自に作成できる場合に選択します。
11. **OK** をクリックします。

STEP 11 | 静的 IPv6 インターフェースの場合、アドレス解決を構成します。

1. **Address Resolution (アドレス解決)** を選択します。
2. 重複アドレス検出を有効にする(DAD) インターフェイスに割り当てる前に、潜在的な IPv6 アドレスの一意性を検証する場合 (デフォルトは有効)。
3. 重複アドレス検出を有効にするを選択した場合は、ネイバー識別の試行が失敗するまでのネイバー要請(NS)間隔内の**DAD**試行回数を指定します。範囲は1～10、デフォルトは1です。
4. **Reachable Time (sec)**、到達可能性確認メッセージを受信した後にクライアントがネイバーが到達可能であると想定する時間の長さを入力します。範囲は 10 から 36,000 です。デフォルトは 30 です。
5. **NS 間隔(秒)** (ネイバー要請間隔)、ネイバー要請間の時間の長さを入力します。範囲は 1 から 3,600 です。デフォルトは 1 です。
6. **Enable NDP Monitoring** は、ネイバー探索プロトコルのモニタリングを有効にします。有効にすると、NDP アイコン([機能] 列)を選択し、ファイアウォールが検出したネイ

バーの IPv6 アドレス、対応する MAC アドレス、User-ID、ステータス(最良の場合)などの情報を表示できます。

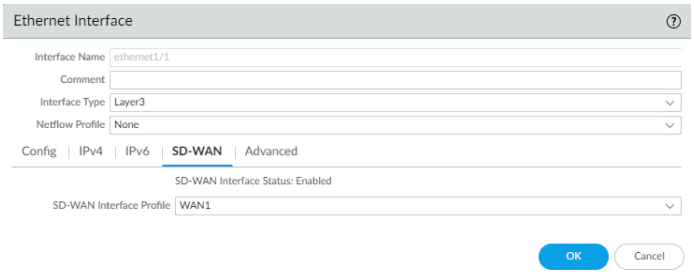
7. **OK** をクリックします。



STEP 12 | インターフェイスで IPv6 Router Advertisement（RA:ルータ アドバタイズメント）を送信できるようにし、オプションで RA パラメータを調整する場合は、「PAN-OS Networking Administrator ` s Guide (PAN-OS ネットワーキング管理者ガイド)」の「Configure Layer 3 Interfaces (レイヤー3インタフェースの設定)」 の説明に従ってルータ アドバタイズメントを設定します。

STEP 13 | **SD-WAN** タブで、作成済みの **SD-WAN Interface Profile (SD-WAN** インターフェース プロファイル) を選択し、(あるいは新規の SD-WAN Interface Profile (SD-WAN インターフェース プロファイル) を作成し、) このインターフェースに適用します。SD-WAN インターフェイス プロファイルには関連するリンクタグがあり、このプロファイルが適用されるインターフェイスには、この関連リンクタグが付与されます。各インターフェイスが持つことができるリンクタグは1つのみです。

STEP 14 | **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。

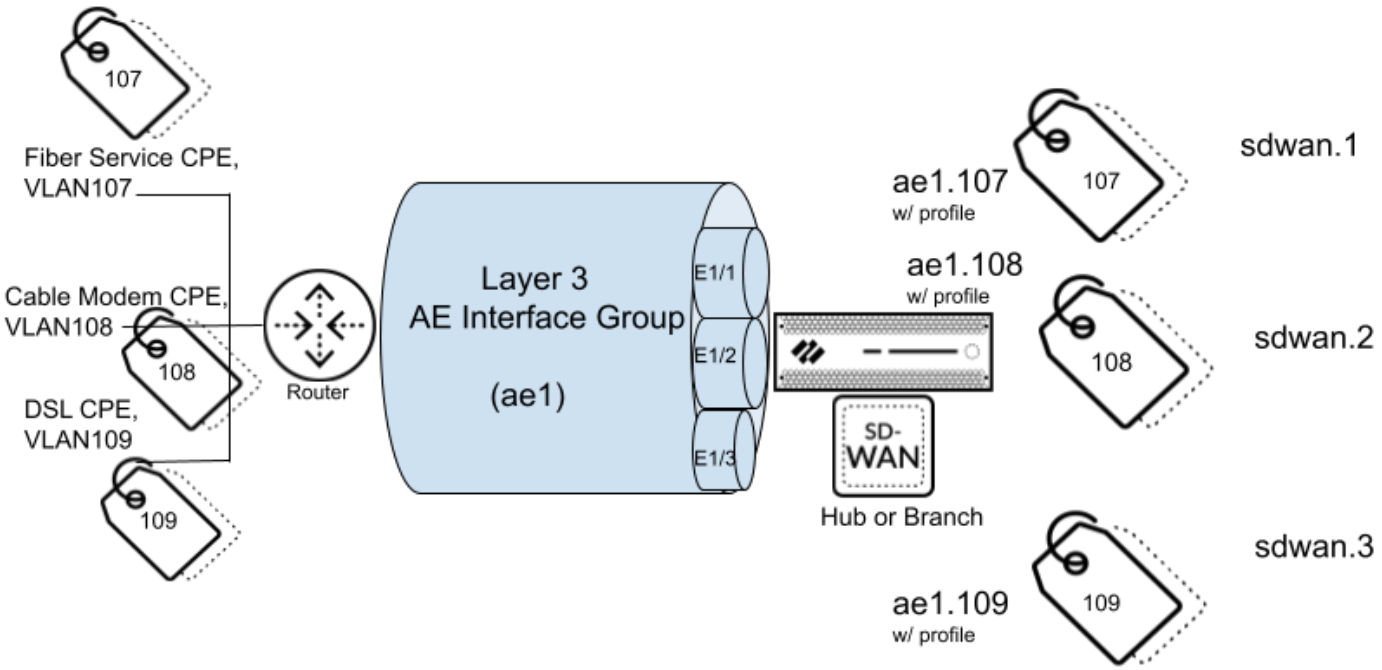


STEP 15 | 設定の変更を **Commit (**コミット) および**Commit and Push (**コミットしてプッシュ) します。

STEP 16 | (SD-WAN 手動設定のみ)仮想 SD-WAN インターフェースの設定.自動 VPN を使用している場合、このタスクは自動 VPN 設定が実行します。

SD-WAN 用の集約イーサネット インターフェイスとサブインターフェイスの設定

PAN-OS 11.0 および SD-WAN プラグイン 2.1.0 を実行している物理ファイアウォールは、アグリゲート型イーサネット (AE) インターフェイス上の SD-WAN をサポートしているため、たとえば、データセンター内の SD-WANファイアウォールは、リンク冗長性を提供する物理イーサネットインターフェイスの集約インターフェイスグループ (バンドル) を持つことができます。SD-WAN は、サブインターフェイスの有無にかかわらず AE インターフェイスをサポートします。エンドツーエンドトラフィックセグメンテーションを提供するために、異なるISPサービスにタグを付けることができるサブインターフェイスを持つ AE インターフェイスを作成できます。したがって、ISP サービスは、接続ごとに専用のファイバーを使用しなくても、複数のラボや建物にアクセスできます。レイヤ 3 AE インターフェイス グループは、次の図に示すようにルータに接続します。



VM シリーズ ファイアウォールは *AE* インターフェイスをサポートしません。*AE* インターフェイスは *VM* シリーズ のファイアウォールではサポートされていないため、*AE* インターフェイスを持つ *SD-WAN* ハブまたはブランチ ファイアウォールは、*VM* シリーズ *SD-WAN* ハブまたはブランチ ファイアウォールと同じ *VPN* クラスタに属してはなりません。

PPPoE はサブインターフェイスではサポートされていません。

STEP 1 | Panorama Web インターフェイスへのログイン。

STEP 2 | AE インターフェイス グループ内の各 ISP 接続(サブインターフェイス)に対してSD-WAN インターフェース プロファイルの設定して、そのリンク属性を定義します。

STEP 3 | AE インターフェイス グループを作成します。

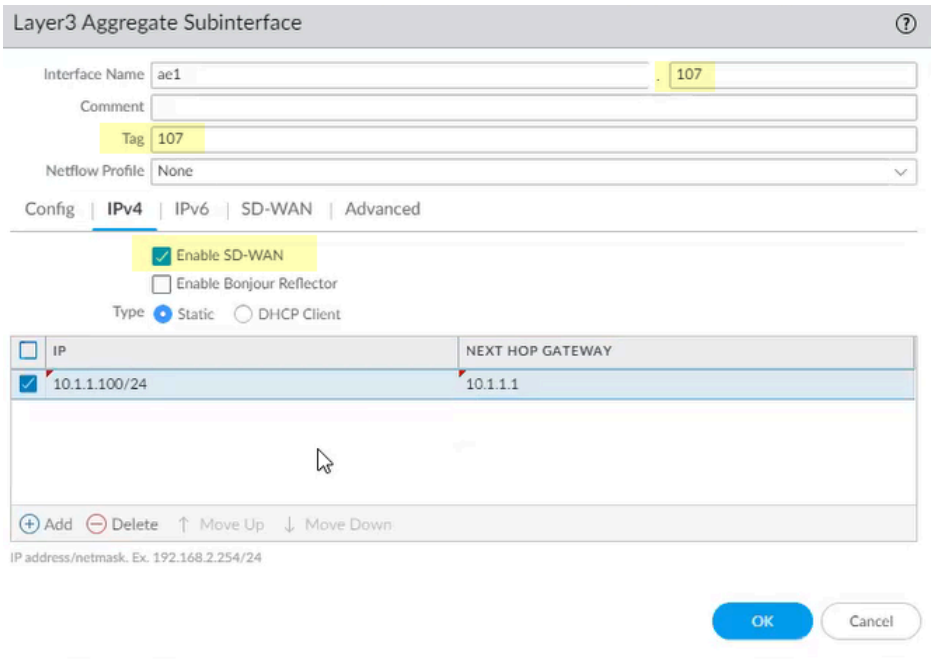
1. [ネットワーク > インターフェイス, イーサネット] を選択し、[パノラマ テンプレート,] を選択し、[集合グループの追加]をクリックします。
2. [インターフェイス名,] に、集計グループを識別する番号を入力します。
3. **Interface Type (**インターフェイス タイプ**)** については、**Layer3** を選択します。
4. **OK** をクリックします。

STEP 4 | 物理インターフェイスを集約グループに割り当てます。

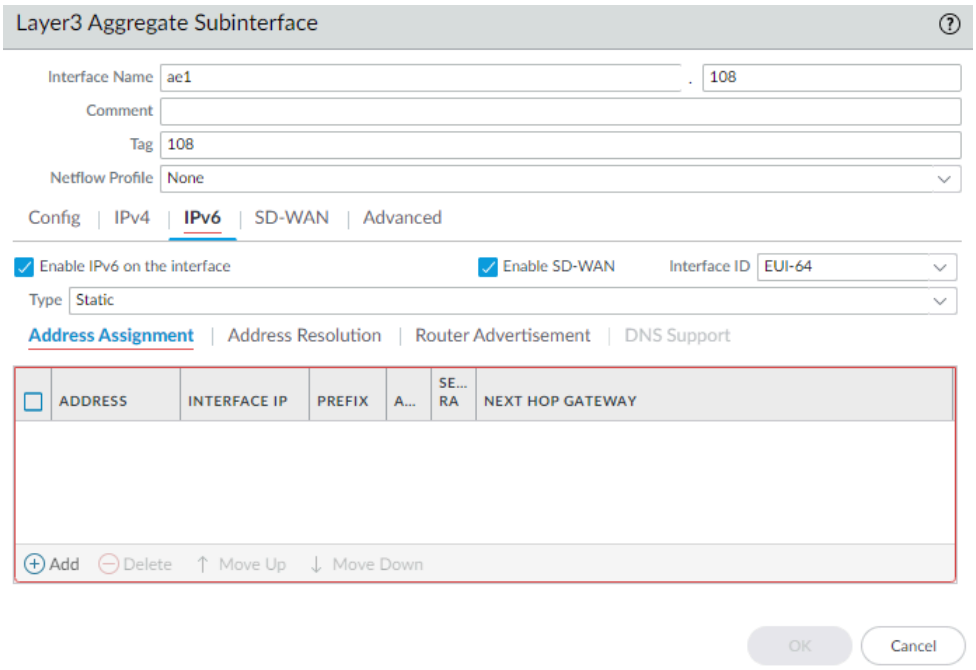
1. ネットワーク インターフェイス イーサネットを選択し、集約グループに割り当てるインターフェイスを選択します。
2. [インターフェイスの種類] を [集約イーサネット] として選択します。
3. 作成した 集計グループ (ae1 など) を選択します。
4. [詳細設定] タブで、[リンク速度,]、[リンクデュ, プレックス]、[リンク状態] を選択します。
5. **OK** をクリックします。
6. 集約グループに割り当てる各インターフェイスに対して、この手順を繰り返します。

STEP 5 | 集約グループの場合は、静的 IP アドレスを使用するサブインターフェイスを作成します。

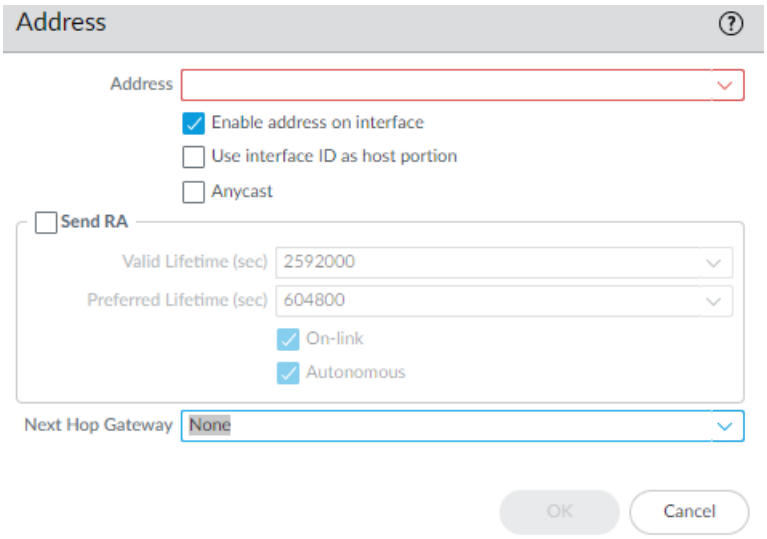
1. [ネットワーク > インターフェイス, イーサネット] を選択し、ae1 などの集約インターフェイスをハイライト表示して、画面下部の [サブインターフェイス の追加] をクリックします。
2. [インターフェイス名,] に、ピリオドの後の数値 (107 など) を入力します。
3. サブインターフェイスを区別するために VLAN タグ を入力します。使いやすさを高めるには、タグをサブインターフェイス ID と同じ番号にします。
4. サブインターフェイスに静的IPv4アドレスを設定するには、**[IPv4]**タブを選択し、[**Enable SD-WAN (SD-WAN**の有効化**)]**を選択します。



5. アドレスの種類を選択します。静的.
6. サブインターフェイスの **IP** アドレス (およびサブネット マスク) を追加 します。
7. 次ホップ ゲートウェイの IP アドレスを入力します。
8. サブインターフェイスに固定IPv6アドレスを設定するには、**[IPv6]**タブ、**[Enable IPv6 on the interface (**インターフェイス上で**IPv6**を有効にする**)]**、**[Enable SD-WAN (SD-WAN**の有効化**)]**を選択します。



9. ［**EUI-64**（デフォルト**64**ビット拡張固有識別子）］フィールドに、64ビットEUIを16進数形式で入力します。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。
10. [**Address Assignment (**アドレス割り当て**)**]を選択してインターフェイスの[IPv6 **Address**]を追加するか、[**New Variable (**新しい変数**)**]を選択して変数を作成します。



11. インターフェイス **ID** をホスト部分として使用します。**EUI-64** については、前のサブステップを参照してください。
12. **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

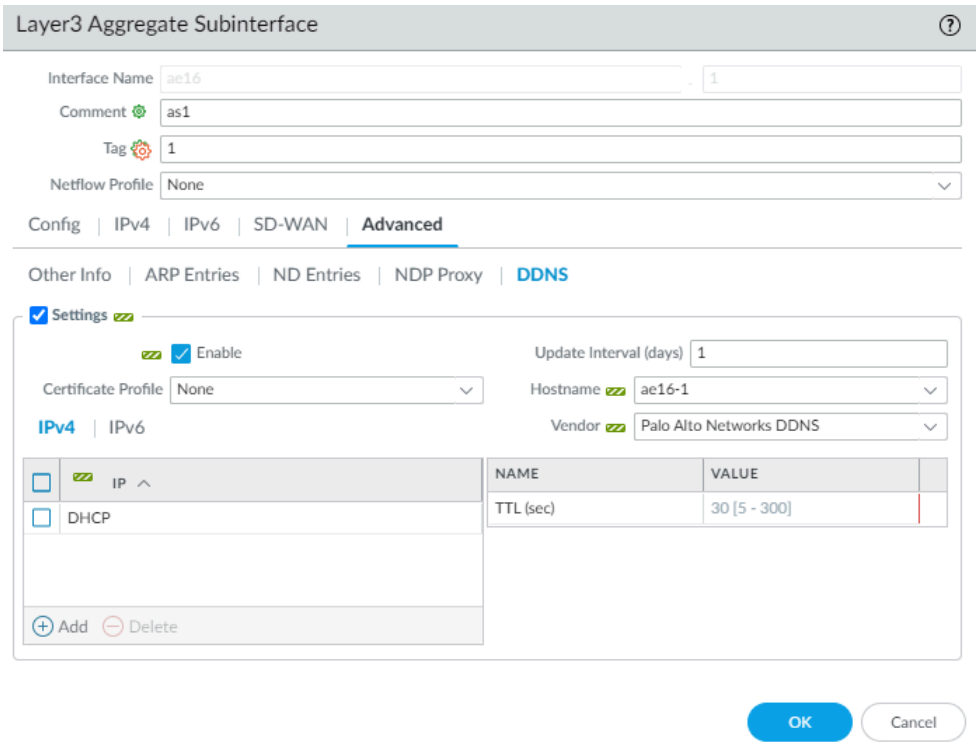
にし、ルーティング プロトコルのコストや他の要素に基づいて IPv6 が最も近いと判断したノードに Anycast トラフィックを送信できるようにします。

13. **Next Hop Gateway (**ネクスト ホップゲートウェイ**)** の IPv6 アドレス (入力した IPv6 アドレスからのネクスト ホップ) を入力します。ネクストホップ ゲートウェイは、IP v6 アドレスと同じサブネット上にある必要があります。ネクストホップ ゲートウェイは、サービス購入時に ISP から提供された ISP のデフォルト ルーターの IP アドレスです。ファイアウォールがISPのネットワーク、最終的にはインターネットとハブに到達するためにトラフィックを送信するネクストホップIPアドレスです。。
14. **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（ルーター広告タブ上）。
15. 有効な有効期間 **(**秒**)**を入力します。これはファイアウォールがそのアドレスを有効と見なす時間の長さ (秒単位)を示します。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）。
16. 有効なアドレスが優先される**Preferred Lifetime (**優先されるライフタイム**) (**秒**)** (秒単位) (ファイアウォールがそのアドレスを使用してトラフィックを送受信できることを意味します)を入力します。優先ライフタイムの期限後は、ファイアウォールがこのアドレスを使用して新しい接続を確立することはできませんが、既存の接続は[Valid Lifetime（有効なライフタイム）]の期限まで有効です（デフォルトは 604,800）。
17. プレフィックス内にアドレスを持つシステムがルーターなしで到達可能な場合は、**On-Link** を選択します。
18. システムがアドバタイズされたプレフィックスと Interface ID を組み合わせて IPアドレスを個別に作成できる場合は、**Autonomous (**自律型**)** を選択します。
19. **OK** をクリックします。

STEP 6 | スタティック アドレスの代わりに、集約グループに対して、アドレスを取得するために DHCP を使用するサブインターフェイスを作成します。

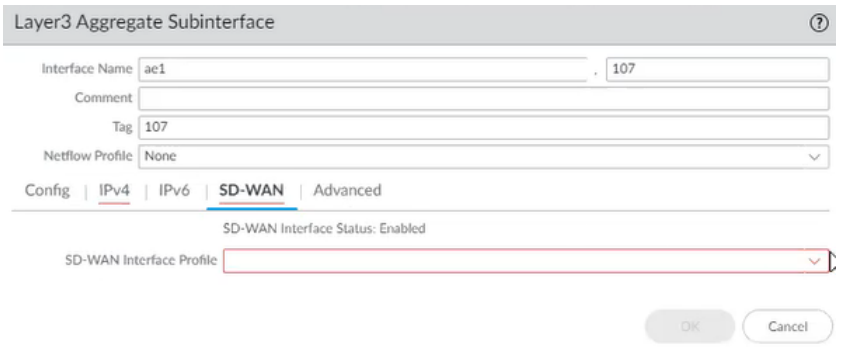
1. **[Network**（ネットワーク）**] > [Interfaces**（インターフェース）**] > [Ethernet**（イーサネット）**]**の順に選択し、**[Template**（テンプレート）**]** フィールドでハブのテンプレート スタックを選択します。
2. ae1 などの集約インターフェイスをハイライト表示し、画面下部の [サブインターフェイス の追加] をクリックします。
3. サブインターフェイスをハイライト表示し、画面下部の [上書き] をクリックします。
4. サブインターフェイスをハイライト表示し、[インターフェイス, 名]にピリオドの後の数値 (1 など) を入力します。
5. サブインターフェイスを区別するために VLAN タグ を入力します。使いやすさを高めるには、タグをサブインターフェイス ID と同じ番号にします。
6. **[IPv4]** タブと **[SD-WAN**の有効化]を選択します。

   集約インターフェイス グループのサブインターフェイスは、*DHCP* クライアントとして *IPv4* アドレスだけをサポートし、*IPv6* アドレスはサポートしません。
7. アドレスの種類を選択します。**DHCP** クライアント.
8. **Enable**[有効] を選択します。
9. サーバー **111** によって提供されるデフォルト ゲートウェイを指す既定のルートを自動的に作成する場合は、オフにします **(**選択しない**)**。
10. [詳細設定] タブと **[DDNS]** タブを選択します。
11. [設定] および [有効] を選択します。ホスト名 は、パノラマ SD-WAN プラグインによって自動的に生成されます。
12. **[**ベンダー] を [パロ アルトネットワーク DDNS]として選択します。
13. **OK** をクリックします。



STEP 7 | サブインターフェイスに SD-WAN インターフェイス プロファイルを適用します。

1. 作成したサブインターフェイスをハイライト表示し 、**[SD-WAN]** タブを選択します。
2. このリンク用に作成した **SD-WAN** インターフェイス プロファイル を選択するか、新しいプロファイルを作成します。



3. **OK** をクリックします。

STEP 8 | 前の手順を繰り返して、集約インターフェイス グループに対して追加のレイヤ 3 サブインターフェイスを作成し、各サブインターフェイスに SD-WAN インターフェイス プロファイルを適用します。

STEP 9 | **[コミット]** します。

SD-WAN 用のレイヤ 3 サブインターフェイスの設定

PAN-OS 11.0 および SD-WAN プラグイン 2.1.0 を実行しているファイアウォールは、レイヤ 3 サブインターフェイスで SD-WAN をサポートしているため、ファイアウォールは VLAN タグを使用してトラフィックをセグメント化できます。次のタスクでは、静的 IP アドレスを使用する Layer3 サブインターフェイスを作成する方法と、DHCP を使用してアドレスを取得するレイヤを作成する方法を示します。サブインターフェイスに VLAN タグを割り当て、サブインターフェイスで SD-WAN をイネーブルにする方法を示します。各 ISP 接続を定義し、対応するサブインターフェイス(仮想 SD-WAN インターフェイス)にプロファイルを割り当てる SD-WAN インターフェイス プロファイルを作成します。

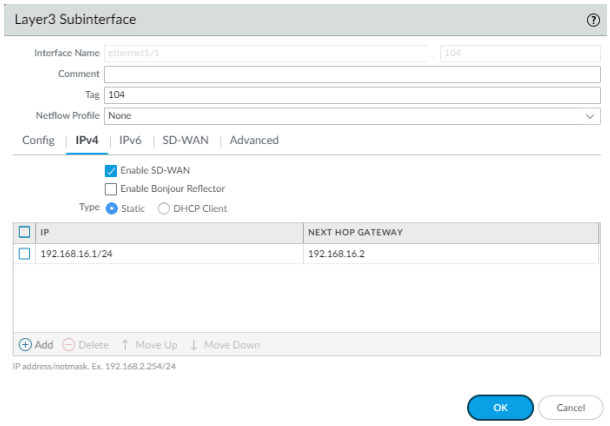
VM シリーズ のファイアウォールで *SD-WAN* レイヤ *3* サブインターフェイスを設定する場合、*VMware* 構成では、すべての *VLAN* を許可する各インターフェイスに接続された各ポートグループが必要です。

PPPoE はサブインターフェイスではサポートされていません。

STEP 1 | 各 ISP 接続 (サブインターフェイス) のリンク属性を定義するSD-WAN インターフェース プロファイルの設定。

STEP 2 | 静的 IPv4 アドレスを使用するレイヤ 3 サブインターフェイスを作成します。

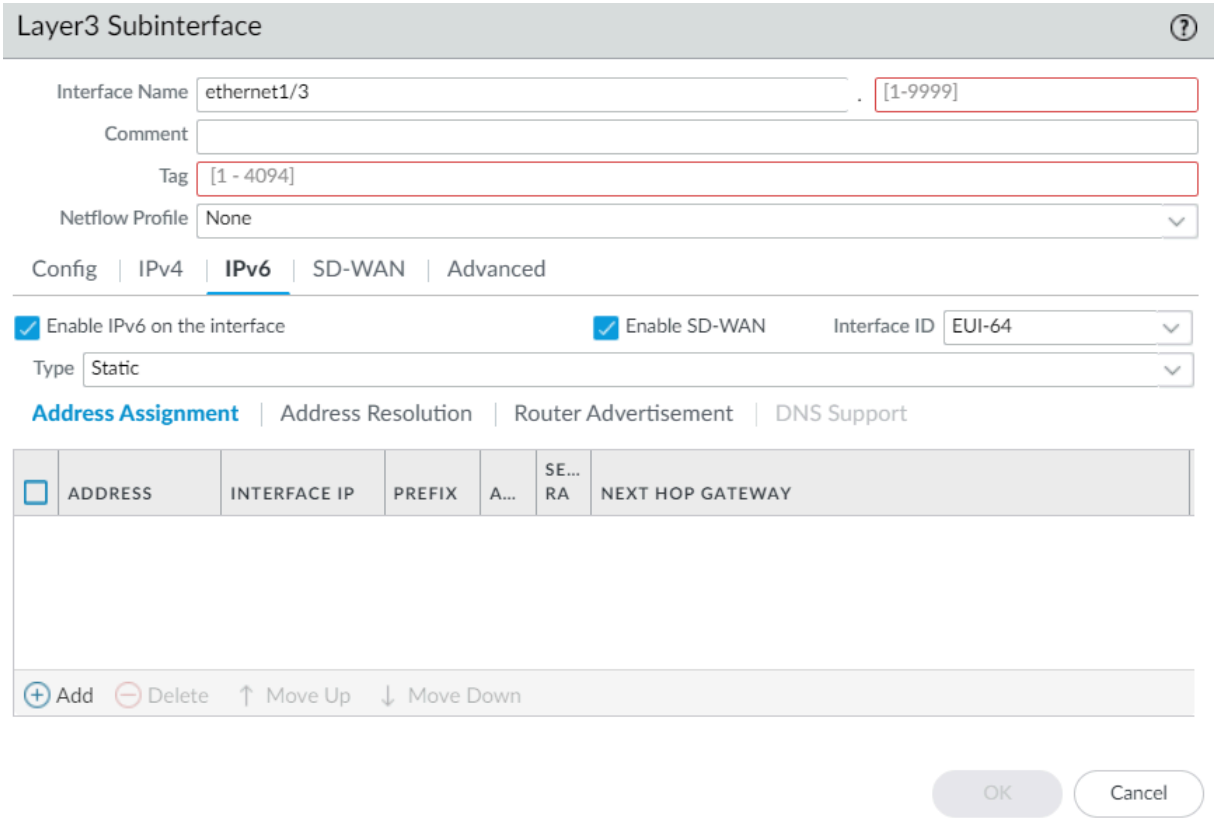
1. **[Network**（ネットワーク）**] > [Interfaces**（インターフェース）**] > [Ethernet**（イーサネット）**]**の順に選択し、**[Template**（テンプレート）**]** フィールドでハブのテンプレートを選択します。
2. インターフェイスを選択します。
3. [インターフェイスの種類] で [レイヤ 3] を選択し、[OK] をクリックします。
4. インターフェイスをハイライト表示し、画面の下部にある [サブインターフェイスの追加] をクリックします。
5. インターフェイス名とピリオドの後に、サブインターフェイス番号を入力します。
6. サブインターフェイスのタグを入力します（範囲は1～4,094）。使いやすさを高めるには、タグをサブインターフェイス ID と同じ番号にします。
7. **IPv4** タブで、**Enable SD-WAN(SD-WAN** を有効にする**)** を選択します。
8. アドレスの種類を選択します。静的.
9. IP アドレスとサブネット マスクを追加します。
10. 次ホップ ゲートウェイの IP アドレスを入力します。
11. **OK** をクリックします。



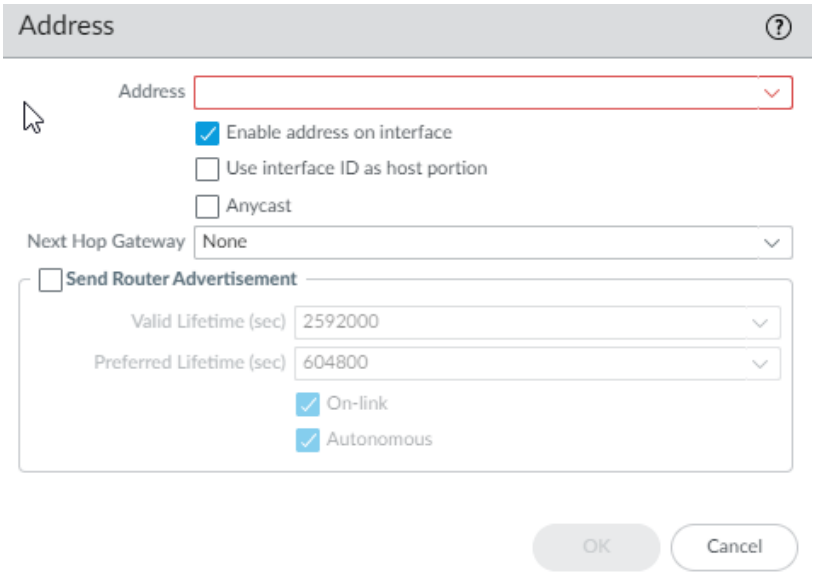
STEP 3 | 静的 IPv6 アドレスを使用するレイヤ 3 サブインターフェイスを作成します。

1. スタティック IPv4 アドレスを使用するレイヤ 3 サブインターフェイスを作成するには、ステップの最初の 6 つのサブステップを実行します。これらは IPv6 アドレスで同じであるためです。
2. **IPv6** タブで **Enable IPv6 on the interface (**インターフェイスでの **IPv6** の有効化**)** と**Enable SD-WAN (SD-WAN**の有効化**)**を行います。
3. ［**EUI-64**（デフォルト**64**ビット拡張固有識別子）］フィールドに、64ビットEUIを16進数形式で入力します。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。
4. アドレスの種類を選択します。静的.

5. [アドレス割り当て]を選択します。



6. インターフェイスのIPv6アドレスを追加するか、**[New Variable (新しい変数)]**を選択して変数を作成します。SD-WANは物理インターフェイスごとに1つのIPv6アドレスをサポートします。
7. インターフェイス上のアドレスを有効にします。

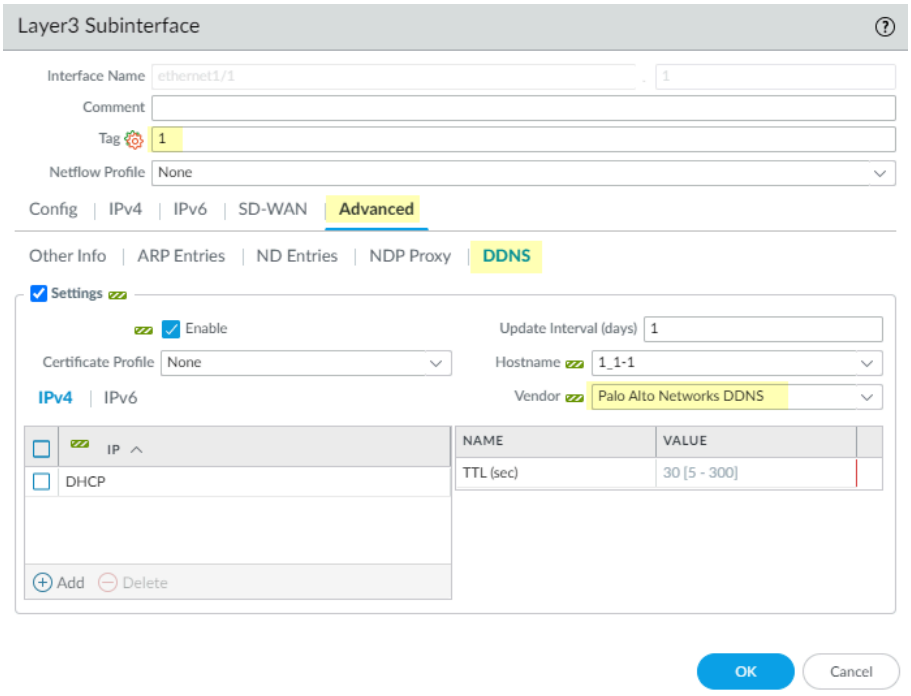


8. インターフェイス**ID**をホスト部分として使用する – 説明については、上記の３番目のサブステップを参照してください。

9. **Anycast** – IPv6 アドレス（ルート）を Anycast アドレス（ルート）にする場合に選択します。つまり、複数のロケーションが同じプレフィックスをアドバタイズ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。
10. **Next Hop Gateway (**ネクスト ホップゲートウェイ**)** – Next Hop Gateway (入力した IPv4 アドレスからのネクスト ホップ) のIPv6 アドレスを入力します。ネクストホップ ゲートウェイは、IP v6 アドレスと同じサブネット上にある必要があります。ネクスト ホップ ゲートウェイは、サービス購入時に ISP から提供された ISP のデフォルト ルーターの IP アドレスです。ファイアウォールがISPのネットワーク、最終的にはインターネットとハブに到達するためにトラフィックを送信するネクストホップIPアドレスです。
11. **Send Router Advertisement (**ルーターのアドバタイジングを送信**)**–ファイアウォールがルーター アドバタイズメント(RA)でこのアドレスを送信できるように選択します。この場合、インターフェイス上 (**Router Advertisement (**ルーターアドバタイズメント**)**タブ) 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。
12. **Valid Lifetime (**有効な有効期間**) (**秒**)** – ファイアウォールがアドレスを有効とみなす有効期間（秒単位）を入力します。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）。
13. **Preferred Lifetime (**優先ライフタイム**) (**秒**)** – 有効なアドレスが優先される時間の長さ (秒単位) (ファイアウォールがそのアドレスを使用してトラフィックを送受信できることを意味します)を入力します。優先ライフタイムの期限後は、ファイアウォールがこのアドレスを使用して新しい接続を確立することはできませんが、既存の接続は[Valid Lifetime（有効なライフタイム）]の期限まで有効です（デフォルトは 604,800）。
14. **On-link**（オンリンク） – プレフィックス内にアドレスがあるシステムにルーターなしで到達可能である場合に選択します。
15. **Autonomous**（自律型） – 通知されたプレフィックスとインターフェイス ID を組み合わせて、システムが IP アドレスを独自に作成できる場合に選択します。
16. **OK** をクリックします。

STEP 4 | 静的アドレスの代わりに、DHCP を使用して IPv4 アドレスを取得するレイヤ 3 サブインターフェイスを作成します。

1. **[Network**（ネットワーク）**] > [Interfaces**（インターフェース）**] > [Ethernet**（イーサネット）**]**の順に選択し、**[Template**（テンプレート）**]** フィールドでハブのテンプレート スタック (テンプレートではない) を選択します。
2. インターフェイスを選択します。
3. [インターフェイスの種類] で [レイヤ 3] を選択し、[OK] をクリックします。
4. インターフェイスをハイライト表示し、画面下部の [サブインターフェイスの追加] をクリックします。
5. サブインターフェイスをハイライト表示し、[上書き] をクリックします。
6. サブインターフェイスをハイライト表示し、インターフェイス名とピリオドの後にサブインターフェイス番号を入力します。
7. サブインターフェイスのタグを入力します（範囲は1～4,094）。使いやすさを高めるには、タグをサブインターフェイス ID と同じ番号にします。
8. **IPv4** タブで、**Enable SD-WAN(SD-WAN** を有効にする**)** を選択します。
9. 以下のアドレスの **Type(**タイプ**)** を選択します。DHCPクライアントと有効化。
10. [(選択しない)] [既定のルートを自動的に作成] をオフにして、既定のゲートウェイを指し示す [サーバー] をクリックします。
11. [詳細設定] タブを選択し、[DDNS] タブを選択します。
12. [設定] および [有効] を選択します。ホスト名 は、パノラマ SD-WAN プラグインによって自動的に生成されます。
13. **[**ベンダー **]** を **[**パロ アルトネットワーク DDNS**]**として選択します。
14. **OK** をクリックします。



STEP 5 | サブインターフェイスに SD-WAN インターフェイス プロファイルを適用します。

1. 作成したサブインターフェイスをハイライト表示し 、**[SD-WAN]** タブを選択します。
2. このリンク用に作成した **SD-WAN** インターフェイス プロファイル を選択するか、新しいプロファイルを作成します。
3. **OK** をクリックします。

STEP 6 | インターフェイスにサブインターフェイスを追加するには、前の手順を繰り返します。

STEP 7 | [コミット] します。

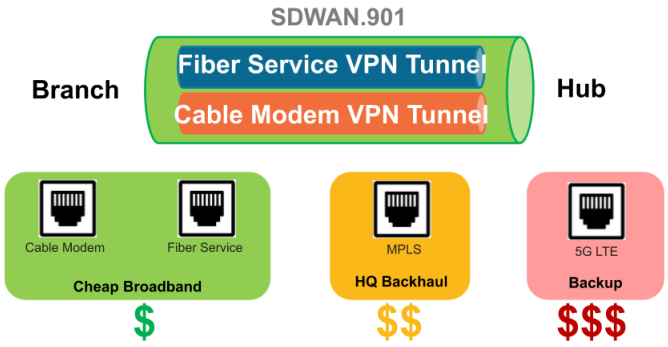
仮想 SD-WAN インターフェースの設定

Panorama で自動 VPN 設定を使用している場合、Panorama がSD-WAN インターフェースを作成します。この場合、仮想 SD-WAN インターフェースを作成および設定する必要はありません。

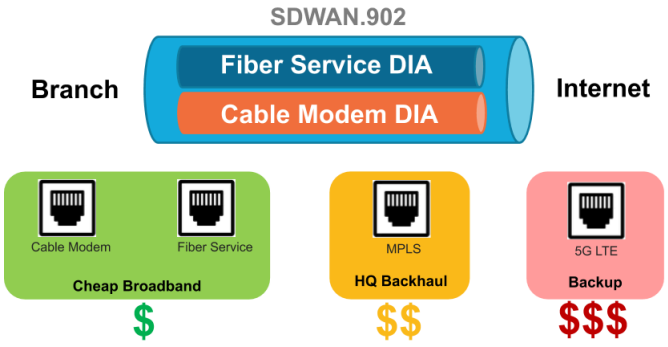
Panorama で自動 VPN 設定を使用していない場合は、仮想 SD-WAN インターフェースを作成および設定して、特定のハブあるいはインターネット等の同じ宛先に接続する 1 つまたは複数の物理 SD-WAN 対応の ethernet interfaces (イーサネット インターフェース) を指定します。実際、仮想 SD-WAN インターフェースのすべてのリンクは同じタイプとする必要があります。すべて VPN トンネル リンクにするか、すべてダイレクト インターネットアクセス (DIA) リンクとします。

以下の最初の図は、異種キャリアを使用する 2 台の物理インターフェースをバンドルする SDWAN.901 という名前のSD-WAN インターフェースの例を示しています。Ethernet1/1 (ケーブルモデム リンク) と Ethernet1/2 (ファイバ回線リンク)。この 2 つのリンクは共に、ブランチからハブへの VPN トンネルです。

この図では、*SD-WAN* インターフェースの両方のリンクが同じリンクタグ (格安ブロードバンド) を使用していますが、*SD-WAN* インターフェースのリンクは異なるリンクタグとすることも可能です。



以下の図では、ブランチからインターネットへの DIA リンクである Ethernet1/1 および Ethernet1/2 リンクが SDWAN.902 にバンドルされています。



STEP 1 | Panorama Web インターフェイスへのログイン。

STEP 2 | **Network** (ネットワーク)、 > **Interfaces** (インターフェース)、 > **SD-WAN** と選択し、**Template** (テンプレート) コンテクスト ドロップダウンで適切なテンプレートを選択します。

STEP 3 | 追加ボタンをクリックして、**sdwan.** のプレフィックスに続けて、番号 (1 ～ 9,999 の範囲) を入力し、論理 SD-WAN インターフェースを **Add** (追加)します。

自動 *VPN* 設定では、*.901*、*.902*、等の番号の *SD-WAN* インターフェースが作成されます。したがって、*SD-WAN*インターフェイスを手動で作成する場合は、*SD-WAN*インターフェイス名に*sdwan.90x*形式を使用しないでください。同様に、*Auto VPN*の設定では、*IPv6*インターフェイス用に*.9016*という番号の*SD-WAN*インターフェイスが作成されます。

STEP 4 | わかりやすい **Comment** (説明) を入力します。

ブランチのテンプレートの場合は、***Branch to internet(***ブランチからインターネットへ***)*** や ***Branch to western USA hub(***ブランチから西部米国ハブへ***)*** 等の役に立つ説明を追加します。説明を追加することにより、自動生成された名前をログやレポートで解読するよりも、トラブルシューティングが容易になります。

STEP 5 | 仮想SD-WANインターフェイスの種類を示す**Protocol** (プロトコル)を選択します。

- **ipv4** は IPv4 DIA 仮想インターフェイスを示します。
- **ipv6** は IPv6 DIA 仮想インターフェイスを示します。
- **none** は VPN トンネル仮想インターフェイスを示します。

STEP 6 | **Config**(設定) タブで、SD-WAN インターフェースを**Virtual Router** (仮想ルーター) に割り当てます。

STEP 7 | SD-WAN インターフェースを **Security Zone** (セキュリティ ゾーン) に割り当てます。

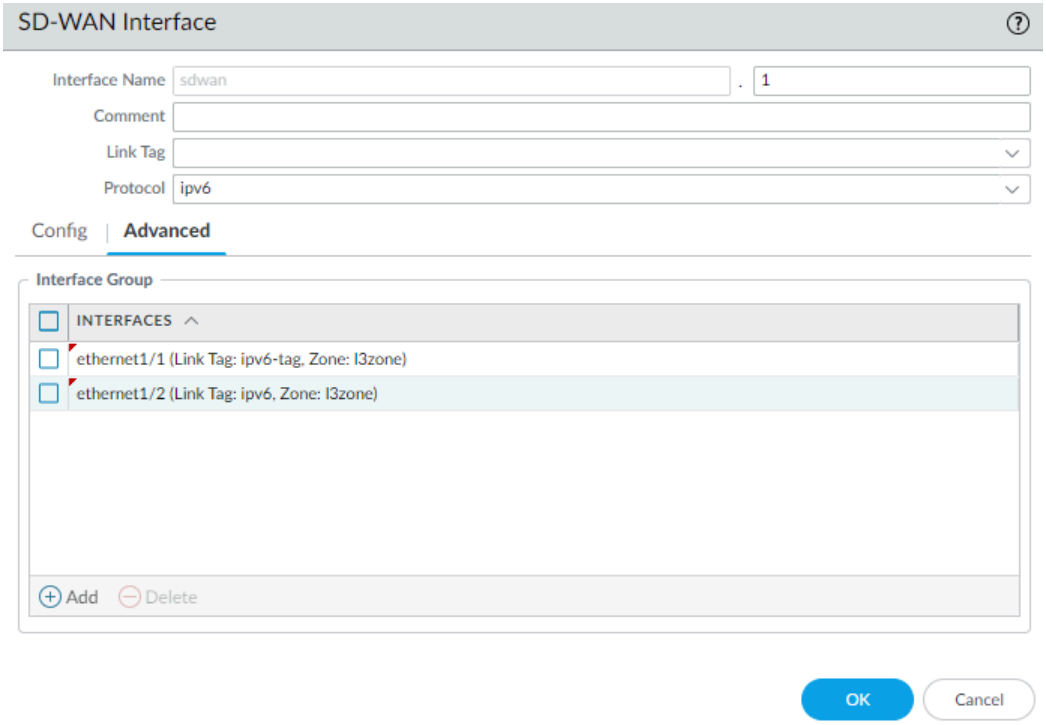
仮想 SD-WAN インターフェースおよび仮想 SD-WAN のすべてのインターフェースメンバーは、同じセキュリティ ゾーン内にある必要があります。このため、ブランチから同じ宛先へのすべてのパスに同じセキュリティ ポリシー ルールが適用されます。

STEP 8 | **Advanced** (詳細) タブで、1 つまたは複数のレイヤー 3 イーサネット インターフェース (DIA 向け) あるいは 1 つまたは複数の 仮想 VPN トンネル インターフェース (ハブ用) を選択して、同じ宛先に送信するメンバーである **Interfaces** (インターフェース) を **Add** (追加)

します。複数のインターフェースを入力する場合は、すべて同じタイプ (VPN トンネルまたは DIA) を選択します。

ファイアウォールの *Virtual Router (* 仮想ルーター - *VR)* は、この仮想 *SD-WAN* インターフェースを使用して、*SD-WAN* トラフィックを *DIA* あるいはハブの場所にルーティングします。ルーティング中に、ルートテーブルが、パケットの宛先 *IP* アドレスに基づき、パケットがどの仮想 *SD-WAN* インターフェース *(*出口インターフェース*)* を使用するかを決定します。次に、パケットが合致する *SD-WAN*ポリシールールの *SD-WAN* パスヘルスおよびトラフィック分散プロファイルにより、使用するパス (およびパスが劣化した場合に新しいパスを検討する順序) が決定されます。

STEP 9 | **OK** をクリックして、設定の変更を保存します。



STEP 10 | 設定の変更を **Commit (**コミット**)** および**Commit and Push (**コミットしてプッシュ**)** します。

SD-WAN インターフェースへのデフォルト ルートの作成

Panorama™にアクセスするサービスルートを使用している場合、ファイアウォールを起動するには、作成したSD-WANインターフェイスを指すデフォルトルートを作成する必要があります。

Auto VPN は、IPv6 DIA 用に sdWAN.901 と名付けられた仮想 SD-WAN インターフェースを作成し、VPN トンネル用には sdWAN.902 と名付けられた仮想 SD-WAN インターフェースを作成します。VPNトンネル用にsdwan.902という名前の仮想SD-WANインターフェイスを作成します。Auto VPN はまた、sdwan.901 (IPv4) インターフェースと sdwan.9016 (IPv6) インターフェースをイグレスインターフェースとして使用し、低いメトリックを使用する独自のデフォルトルートを作成します。そのため、sdwan.901 (IPv4) インターフェースと sdwan.9016 (IPv6) インターフェースは、作成したデフォルトルートよりも優先されます。

STEP 1 | Panorama Web インターフェイスへのログイン。

STEP 2 | 作業中の **Template (テンプレート)** を選択します。

STEP 3 | **Network (ネットワーク)**、 > **Virtual Routers (仮想ルーター)**と選択し、**sd-wan** 等の仮想ルーターを 1 つ選択します。

STEP 4 | **[Static Routes (スタティックルート)]**を選択します。

STEP 5 | [**IPv4**]または[**IPv6**]を選択し、[名前でスタティックルートを追加]を選択します。

STEP 6 | IPv4の**Destination (宛先)**には、「0.0.0.0/0」を入力します。IPv6の**Destination (宛先)**には、「::/0」を入力します。

STEP 7 | 出口**Interface(インターフェース)**の場合、ファイアウォールの構築で作成した論理 SD-WAN インターフェースの 1 つ を選択します 。

> *sdWAN.901* あるいは*sdWAN.902*または*sdwan.9016*以外の任意の論理 *SD-WAN* インターフェースを出口インターフェースとして選択することが可能です。

STEP 8 | **Next Hop (ネクストホップ)** には、**None (なし)** を選択します。

STEP 9 | **Metric (メトリック)** には、自動 VPN が低メトリックで作成するデフォルト ルートよりもこのデフォルト ルートが優先されないため、50 以上の値を入力します。

STEP 10 | **OK** をクリックします。

STEP 11 | **Commit (コミット)** を選択し、設定の変更を **Commit and Push (コミットおよびプッシュ)** します。

STEP 12 | 変更を **Commit (コミット)** します。

STEP 13 | Panorama にアクセスするサービス ルートを使用するファイアウォール上の他のテンプレートに対して、このタスクを繰り返します。

SD-WAN リンク管理プロファイルの設定

パス品質、SaaS 品質、トラフィック分散、およびエラー訂正プロファイルを作成して設定し、SD-WAN リンクフェイルオーバーを管理します。

- パス品質プロファイルの作成
- SaaS モニタリングの設定
- SD-WAN トラフィック分散プロファイル
- トラフィック分散プロファイルの作成
- エラー訂正プロファイルの作成

パス品質プロファイルの作成

ビジネスクリティカルで遅延の影響を受けやすいアプリケーション、アプリケーション フィルタ、アプリケーション グループ、サービス、サービス オブジェクト、およびサービスグループオブジェクトのセット毎に、遅延、ジッター、およびパケット損失率に基づく固有のネットワーク品質 (ヘルス) 要件を持つパス品質プロファイルを作成します。アプリケーションとサービスは、パス品質プロファイルを共有することができます。各パラメータに最大しきい値を指定します。このしきい値を超えると、ファイアウォールは、より優れたパスを選択すべき劣化したパスであると見なします。

パス品質プロファイルを作成する代わりに、いずれかの事前定義済みパス品質プロファイルを使用することも可能です。事前定義済みパス品質プロファイルには、**general-business (**業務全般)、**voip-video (VoIP** 動画)、**file-sharing (**ファイル共有)、**audio-streaming(**音声ストリーミング)、**photo-video(**画像動画)、**remote-access (**リモート アクセス)等があります。事前定義済みプロファイルは、プロファイル名で示されるアプリケーションおよびサービスのタイプに対して、遅延、ジッター、およびパケット損失のしきい値を最適化するように設定されています。

Panorama デバイス グループの事前定義済みパス品質プロファイルは、*Panorama* テンプレートの *SD-WAN* インターフェース プロファイルのデフォルトの ***Probe Frequency (***プローブ頻度*)* 設定に依拠しています。デフォルトのプローブ頻度設定を変更する場合、インターフェース プロファイルを変更した *Panorama* テンプレートの影響を受けるデバイス グループ内のファイアウォールのパス品質プロファイルで、***Packet Loss(***パケット損失率*)* のしきい値を調整する必要があります。

ファイアウォールでは、遅延、ジッター、およびパケット損失のしきい値を OR 条件として扱います。つまり、しきい値のいずれか 1 つが超過した場合、ファイアウォールは新たな最適な (優先) パスを選択します。遅延、ジッター、およびパケット損失 が 3 つのしきい値と同じか下回るパスはすべて適格とされ、ファイアウォールは関連するトラフィック分散プロファイルに基づいてパスを選択します。

デフォルトでは、ファイアウォールは200 ミリ秒毎に 遅延 および ジッター を測定し、直近の3つの測定値の平均を取り、スライディング ウィンドウ方式でパス品質を測定します。この動作を変更するには、SD-WAN インターフェース プロファイルの設定時に積極的なパス監視または緩和されたパス監視を選択します。

設定された **packet loss** (パケット損失) のしきい値を超過したため、パスがフェイルオーバーした場合でも、ファイアウォールは失敗したパスにプローブパケットを送信し、パスの回復に伴いパケット損失率を計算します。回復したパスのパケット損失率が、パス品質プロファイルで設定されたパケット損失のしきい値を下回るまで、3 分ほどかかる場合もあります。例えば、アプリケーションの SD-WAN ポリシー ルールに、1 %のパケット損失しきい値を指定するパス品質プロファイルと、まずはタグ 1 (tunnel.1に適用)、次にタグ 2 (tunnel.2 に適用)をリストに指定するトップダウン方式のトラフィック分配プロファイルがあるとします。tunnel.1で 1 %のパケット損失率が超過すると、データパケットは tunnel.2にフェイルオーバーします。tunnel.1が (プローブパケットに基づき) 0%のパケット損失率に回復した後、tunnel.1の監視パケット損失率が 1 %以下となるのに最大 3 分かかることがあります。この際、ファイアウォールは再び tunnel.1の最良のパスを選択します。

感度設定では、プロファイルが適用されるアプリケーションで、どのパラメータ (遅延、ジッター、またはパケット損失) がより重要 (推奨される) かを指定します。ファイアウォールのリンク品質評価の際には、**high** (高) 設定のパラメータが最初に検討されます。例えば、ファイアウォールが 2 つのリンクを比較する際、一方のリンクの遅延が 100 ミリ秒でジッターが 20 ミリ秒、もう一方のリンクの遅延が 300 ミリ秒、ジッターが 10 ミリ秒であるとします。遅延の感度が高と設定されている場合、ファイアウォールは最初のリンクを選択します。ジッターの感度が高と設定されている場合、ファイアウォールは 2 つ目のリンクを選択します。パラメータの感度が同じ設定の場合 (デフォルトでは、パラメータは **medium** (中) と設定されています)、ファイアウォールはまずパケット損失率を評価し、次に遅延、最後にジッターを評価します。

SD-WAN トラフィック分散プロファイルの概念にあるように、Path Monitoring と Probe Frequency をデフォルト設定のままにすると、新しいパス選択は 1 秒未満で行われます。そうしないと、新しいパスの選択に 1 秒以上かかる可能性があります。パケット損失に基づいて秒未満のフェールオーバーを実現するには、遅延の感度を **high** に設定し、遅延のしきい値を 250 ミリ秒以下に設定する必要があります。

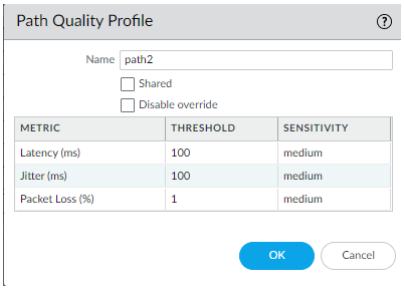
ファイアウォールは、SD-WAN policy rule(SD-WAN ポリシールール)を参照して、劣化したパスを一致するアプリケーション パケットの新しいパスに置き換えるしきい値を制御します。

STEP 1 | Panorama Web インターフェイスへのログイン。

STEP 2 | **Device Group**(デバイス グループ) を選択します。

STEP 3 | **Objects** (オブジェクト)、 > **SD-WAN Link Management** (SD-WAN リンク管理)、 > **Path Quality Profile** (パス品質プロファイル) と選択します。

STEP 4 | 最大 31 文字までの英数字を使用して、**Name**(名前)でパス品質プロファイルを **Add**(追加) します。



STEP 5 | **Latency (遅延)** については、**Threshold (しきい値)** をダブルクリックして、パケットがファイアウォールを出て SD-WAN トンネルの反対側の端に到着するまで、また、しきい値を超える前にファイアウォールに戻る応答パケットをミリ秒で入力します (10～2,000 の範囲、デフォルトは 100)。

STEP 6 | **Latency (遅延)** について、**Sensitivity(感度)** を選択します (**low (低)**、**medium (中)**、**high (高)**)。デフォルト設定は **medium** (中) です。

しきい値を昇順または降順で並べ替えるには、*Threshold (しきい値)* 列の端の矢印をクリックします。

STEP 7 | **Jitter (ジッター)** は、**Threshold (しきい値)** をダブルクリックして、ミリ秒で入力します (10～1,000 の範囲、デフォルトは 100)。

STEP 8 | **Jitter(ジッター)** について、**Sensitivity (感度)** を選択します (**low (低)**、**medium (中)**、**high (高)**)。デフォルト設定は **medium** (中) です。

STEP 9 | **Packet Loss (パケット損失)** は、**Threshold (しきい値)** をダブルクリックして、しきい値を超えるまでのリンクのパケット損失率を入力します (1～100.0 の範囲、デフォルトは 1)。

Packet Loss (パケット損失) の ***Sensitivity (感度)*** 設定は無効のため、デフォルト設定のままにします。

SD-WAN インターフェース プロファイルの ***Probe Frequency***（プローブ頻度） を変更する場合は、*Panorama* デバイス グループの パケット損失の割合のしきい値も調整する必要があります。

STEP 10 | **OK** をクリックします。

STEP 11 | 設定の変更を **Commit (コミット)** および**Commit and Push (コミットしてプッシュ)** します。

STEP 12 | 変更を **Commit (コミット)**します。

STEP 13 | すべてのデバイス グループについて、これを繰り返します。

SaaS モニタリングの設定

SaaS アプリケーションとブランチ ファイアウォール間のダイレクト インターネットアクセス (DIA; Direct Internet Access) リンクを監視するように、SaaS 品質プロファイルを設定します。

SaaS アプリケーション パス モニタリングは、*SD-WAN* 対応の *PAN-OS* ファイアウォールでのみサポートされます。*SaaS* アプリケーション パスの監視は、プリズマ アクセス ハブではサポートされていません。

- SaaS 品質プロファイルの作成
- ユース ケース：ブランチ ファイアウォール用 SaaS モニタリングの設定
- ユース ケース：ブランチファイアウォールから同じ SaaS アプリケーション宛先への SaaS モニタリング用のハブファイアウォール フェイルオーバーを設定する

- ユース ケース：ブランチファイアウォールから異なる SaaS アプリケーション宛先への SaaS モニタリング用のハブファイアウォール フェイルオーバーを設定する

SaaS 品質プロファイルの作成

ブランチ ファイアウォールにソフトウェア アズ ア サービス (SaaS) アプリケーションへのダイレクト インターネット アクセス (DIA) リンクがある場合は、SaaS 品質プロファイルを作成して、1 つ以上の SaaS アプリケーションを監視する方法を指定します。SaaS 品質プロファイルは SD-WAN ポリシー ルールに関連付けられており、ブランチファイアウォールが遅延、ジッター、およびパケット損失のパス品質しきい値を決定し、発信パケットの優先パスを選択する方法を決定します。

SaaS 品質プロファイルは、最大 4 つの静的 IP アドレス、または SaaS 品質プロファイルごとに 1 つの完全修飾ドメイン名 (FQDN)または URL をサポートします。複数の静的 IP アドレスが設定されている場合、ブランチ ファイアウォールは、SaaS 品質プロファイルでの IP アドレスの順序に基づいて、カスケード順序で一度に1つの IP アドレスを監視します。たとえば、IP1、IP2、IP3、および IP4 を追加すると、ブランチファイアウォールは IP1 を監視して、パス品質のしきい値を超えているかどうかを判断し、IP2 に進みます。

> *SD-WAN* モニタリングおよびレポート作成 データには、*SD-WAN* 監視データを表示するときに適用される時間フィルタに関係なく、*SD-WAN* ポリシー ルールに関連する *SaaS Quality (SaaS* 品質*)* プロファイルで現在設定されている通りの *SaaS* アプリケーションと *SaaS* アプリケーション *IP*、*FQDN*、または *URL* が表示されます。
>
> たとえば、*3* 日前に、*SaaS* アプリケーションの *IP* アドレスを *SaaS* 品質プロファイルで ***192.168.10.50*** として最初に設定し、トラフィックを *SaaS* 品質プロファイルが関連付けられている *SD-WAN* ポリシー ルールと一致させたとします。そして今日、この既存の *SaaS* 品質プロファイルを再設定し、*SaaS* アプリケーションの *IP*アドレスを ***192.168.10.20*** に変更しました。*SD-WAN* 監視データを確認すると、この *SaaS* アプリケーションの既存のすべての監視データに *IP* アドレス ***192.168.10.20*** が表示されます。

STEP 1 | Panorama Web インターフェースにログインします。

STEP 2 | **Objects (**オブジェクト**) > SD-WAN Link Management (SD-WAN** リンク管理**) > SaaS Quality Profile (SaaS** 品質プロファイル**)** の順に選択し、SD-WAN 設定を含む **Device Group (**デバイス グループ**)** を指定します。

STEP 3 | 新しい SaaS 品質プロファイルを **Add (**追加**)** します。

STEP 4 | SaaS 品質プロファイルの分かりやすい **Name**（名前） を入力します。

STEP 5 | (任意) **Shared (**共有**)** を有効化（チェック）すると、SaaS 品質プロファイルをすべてのデバイスグループ間で共有します。

STEP 6 | (任意) **Disable override (**オーバーライドを無効化**)** をオン (チェック) にすると、ローカルファイアウォールでの SaaS 品質プロファイル設定のオーバーライドを無効にします。

> ***Disable override (***オーバーライドを無効化***)*** は、***Shared (***共有***)*** が前のステップで無効な場合にのみ有効にすることができます。

STEP 7 | SaaS 監視モードを設定します。

- SaaS アプリケーション パスの正常度を自動で監視します。

  デフォルトで有効になっている、 **Adaptive (**アダプティブ**)** モニタリングにより、ブランチファイアウォールは SaaS アプリケーション セッションの送受信アクティビティをパッシブにモニタリングして、パス品質のしきい値を超えているかどうかを判定できます。SaaS

アプリケーション パスの正常度の品質は、SD-WAN インターフェースで追加のヘルス チェックを行わなくても自動的に判定されます。

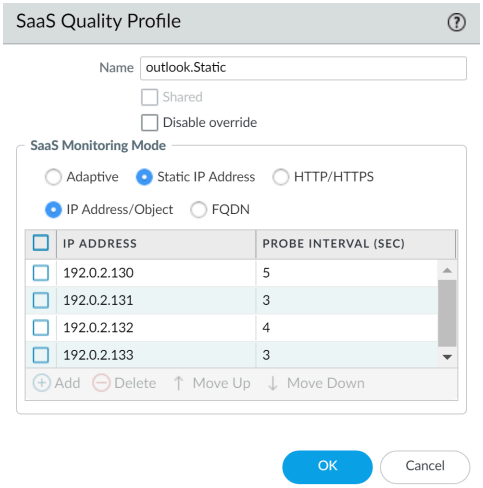
アダプティブ *SaaS* モニタリングは、*TCP SaaS* アプリケーションでのみサポートされます。

- SaaS アプリケーションの静的 IP アドレスを設定します。

  監視が必要な、重要な *SaaS* アプリケーションごとに *SaaS* 品質プロファイルを作成します。*SaaS* アプリケーションに複数の *IP* アドレスがある場合は、その *SaaS* アプリケーションの複数の静的 *IP* アドレスを使用して *SaaS* 品質プロファイルを設定します。

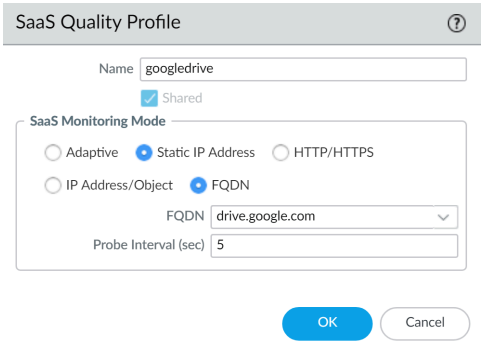
  SaaS モニタリングはリソースを大量に消費するため、多数の *SaaS* アプリケーションを監視すると、ファイアウォールのパフォーマンスに影響を与える可能性があります。優れたユーザビリティを必要とするビジネスクリティカルな *SaaS* アプリケーションのみを監視することを推奨します。

  1. **IP Address/Object (IP** アドレス/オブジェクト) > **Static IP Address (**静的 **IP** ドレス) の順に選択して、IP アドレスを **Add (**追加) します。
  2. SaaS アプリケーションの IP アドレスを入力するか、設定済みの アドレス オブジェクトを選択します。
  3. ブランチ ファイアウォールが SaaS アプリケーション パスで正常性情報をプローブするための **Probe Interval (**プローブ間隔**)** を入力します。
  4. **OK** をクリックして、設定の変更を保存します。



- SaaS アプリケーションの完全修飾ドメイン名 (FQDN) を設定します。
  1. SaaS アプリケーションの FQDN アドレス オブジェクト を設定します。
  2. **IP Address/Object (IP** アドレス/オブジェクト) > **FQDN** を選択して、FQDN を **Add (**追加**)** します。
  3. SaaS アプリケーションの FQDN アドレス オブジェクト を選択します。

4. ブランチ ファイアウォールが SaaS アプリケーション パスで正常性情報をプローブするための **Probe Interval (プローブ間隔)** を入力します。
5. **OK** をクリックして、設定の変更を保存します。

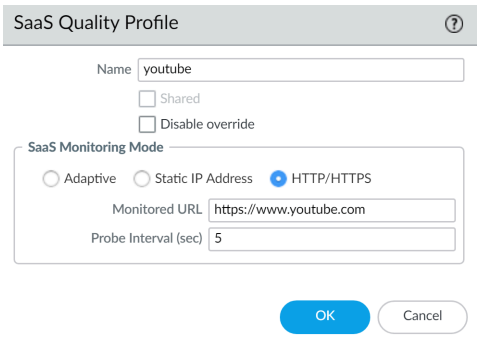


- SaaS アプリケーションの URL を設定します。

  URL モニタリングは、ポート *80*、*443*、*8080*、*8081*、および *143* 上のトラフィックのみに対応します。

  1. **HTTP/HTTPS** を選択します。
  2. SaaS アプリケーションの **Monitored URL**（監視対象 **URL**） を入力します。
  3. ブランチ ファイアウォールが SaaS アプリケーション パスで正常性情報をプローブするための **Probe Interval (プローブ間隔)** を入力します。

     SaaS アプリケーションの HTTP/HTTPS でサポートされる最小プローブ間隔は 3 秒です。
  4. **OK** をクリックして、設定の変更を保存します。



STEP 8 | **Commit (コミット)** を選択し、設定の変更を **Commit and Push (コミットおよびプッシュ)** します。

ユース ケース：ブランチ ファイアウォール用 SaaS モニタリングの設定

あなたの組織がブランチ ファイアウォールのロケーションでのビジネス クリティカルな SaaS アプリケーションを活用している場合、SaaS 品質プロファイルを設定し、それを SD-WAN ポリシー ルールに関連付けることで、重要な SaaS アプリケーションの遅延、ジッタ、およびパケット損失の正常度メトリックをモニターすることが可能であり、また、SD-WAN ブランチ ファイ

アウォールからダイレクト インターネット アクセス (DIA) リンク上の SaaS アプリケーションにリンクを切り替えて、アプリケーションの使いやすさを向上させることができます。

ビジネスクリティカルな SaaS アプリケーションの DIA リンクの正常度メトリックがしきい値を超えると、すべての新しいセッションはトラフィック分散プロファイルで設定されている次の DIA リンクにスワップされます。劣化した DIA リンク上の既存のセッションは、次の DIA リンクにスワップオーバーされません。

STEP 1 | SD-WAN デプロイメントを設定します。

1. 「SD-WAN プラグインのインストール」を行います。
2. 「SD-WANに対応する Panorama とファイアウォールのセットアップ」を行います。
3. 「Panorama への SD-WAN デバイスの追加」を行います。
4. (高可用性構成のみ)SD-WAN 対応 HA デバイスの設定.
5. 「VPN クラスタの作成」を行います。

STEP 2 | リンクタグの作成、SaaS アプリケーションの DIA リンクをグループ化します。

リンク タイプに基づいて各 SaaS アプリケーション DIA リンクに異なる SD-WAN モニタリング設定を適用するために、DIA リンクに複数のリンク タグを作成します。

さらに、複数の DIA リンクに対して単一のリンク タグを作成して、リンクを単一のリンク バンドルにグループ化できます。複数の DIA リンクに対して単一のリンク タグを作成すると、バンドルされたリンク間の帯域幅を集約し、ファイアウォールが複数のリンク間でセッションを分散できるようになります。

STEP 3 | SD-WAN インターフェース プロファイルを設定して ISP 接続の特性を定義し、DIA リンクの速度、ブランチ ファイアウォールがリンクをモニターする頻度を指定し、リンク タグを選択して、SD-WAN インターフェース プロファイルが適用されるリンクを指定します。

複数のリンク タグを作成した場合は、リンク タグごとに SD-WAN インターフェース プロファイルを設定する必要があります。

複数の DIA リンクを単一の リンク タグに割り当てることによってリンク バンドルを作成した場合、リンク タグを指定すると、バンドル内のすべての DIA リンクに SD-WAN インターフェース プロファイル設定が適用されます。

STEP 4 | 各 SaaS アプリケーションの DIA リンクの 物理イーサネット インターフェースを設定します。

DIA リンクのすべての物理イーサネット インターフェースは *Layer3* である必要があります。

STEP 5 | SaaS アプリケーション DIA リンクのすべての物理イーサネット インターフェイスを 1 つのインターフェイス グループにグループ化します仮想 SD-WAN インターフェースの設定。

ファイアウォールの仮想 ルーターは、この仮想 SD-WAN インターフェイスを使用して、SD-WAN トラフィックを DIA の場所にルーティングします。SD-WAN ポリシールールの SD-WAN パスヘルスおよびトラフィック分散プロファイルにより、使用するパス (およびパスの正常性が劣化した場合に新しいパスを検討する順序) が決定されます。

STEP 6 | パス品質プロファイルを作成 して、ブランチ ファイアウォールが次の DIA リンクにスワップするタイミングを指定するために、遅延、ジッター、パケット損失のしきい値と感度を設定します。

STEP 7 | SaaS品質プロファイルを作成 して、SaaS アプリケーションと DIA リンクがモニターされる頻度を指定します。

STEP 8 | トラフィック分散プロファイルを作成 して、リンクの状態が劣化した場合に、ブランチ ファイアウォールが DIA リンクにスワップする順序を指定します。

STEP 9 | SD-WAN ポリシールールを設定 して、SaaS アプリケーションとリンク正常度メトリックを指定し、ファイアウォールが重要な SaaS アプリケーション トラフィックの優先リンクを選択する方法を決定します。

Application *(アプリケーション) タブで、監視している SaaS アプリケーションを SD-WAN ポリシー ルールに追加して、SaaS モニタリング設定が目的の SaaS アプリケーションにのみ適用されるようにします。*

ユース ケース：ブランチファイアウォールから同じ SaaS アプリケーション宛先への SaaS モニタリング用のハブファイアウォール フェイルオーバーを設定する

あなたの組織がブランチ ファイアウォールの場所で SaaS アプリケーションを活用しているが、ブランチ ファイアウォールにスワップ先の正常な DIA リンクがない場合、SaaS アプリケーションへの正常な接続を維持するためのフェイルオーバーの代替手段としてハブファイアウォールを設定できます。

SaaS アプリケーションの DIA リンクヘルス メトリックのしきい値を超え、ブランチ ファイアウォールで使用可能な正常な DIA リンクがない場合、すべての新しいセッションは次のハブ ファイアウォールにスワップされます。劣化した DIA リンク上の既存のセッションは、ハブ ファイアウォールにスワップオーバーされません。

たとえば、ブランチ ファイアウォールとハブ ファイアウォールが同じリージョンにあり、同じ宛先 IP を使用して SaaS アプリケーションにアクセスするとします。ブランチファイアウォールから SaaS アプリケーションへの正常な DIA リンクがない場合に、ブランチ ファイアウォールから利用可能な正常な DIA リンクがなければ、ブランチ ファイアウォールとハブ ファイアウォールの両方で同じ名前の SaaS 品質プロファイルを設定して、ハブ ファイアウォールに自動的にフェイルオーバーすることにより、フェイルオーバーとして機能するようにハブ ファイアウォールを設定できます。これにより、SaaS アプリケーションの正常なパスを維持し、ネットワーク帯域幅を輻輳させることなく、正確なエンドツーエンドの SaaS アプリケーションのモニタリング データを維持できます。

STEP 1 | SD-WAN デプロイメントを設定します。

1. 「SD-WAN プラグインのインストール」を行います。
2. 「SD-WANに対応する Panorama とファイアウォールのセットアップ」を行います。
3. 「Panorama への SD-WAN デバイスの追加」を行います。
4. (高可用性構成のみ)SD-WAN 対応 HA デバイスの設定.
5. 「VPN クラスタの作成」を行います。

STEP 2 | リンクタグの作成、SaaS アプリケーションの DIA リンクをグループ化します。

リンク タイプに基づいて各 SaaS アプリケーション DIA リンクに異なる SD-WAN モニタリング設定を適用するために、DIA リンクに複数のリンク タグを作成します。

さらに、複数の DIA リンクに対して単一のリンク タグを作成して、リンクを単一のリンク バンドルにグループ化できます。

STEP 3 | SD-WAN インターフェース プロファイルを設定して ISP 接続の特性を定義し、DIA リンクの速度、ブランチ ファイアウォールがリンクを監視する頻度を指定し、リンク タグを選択して、WAN インターフェース プロファイルが適用されるリンクを指定します。

複数のリンク タグを作成した場合は、リンク タグごとに SD-WAN インターフェース プロファイルを設定する必要があります。

複数の DIA リンクを単一の リンク タグに割り当てることによってリンク バンドルを作成した場合、リンク タグを指定すると、バンドル内のすべての DIA リンクに SD-WAN インターフェース プロファイル設定が適用されます。

STEP 4 | 各 SaaS アプリケーションの DIA リンクの 物理イーサネット インターフェースを設定します。

DIA リンクのすべての物理イーサネット インターフェースは *Layer3* である必要があります。

STEP 5 | SaaS アプリケーション DIA リンクのすべての物理イーサネット インターフェイスを 1 つのインターフェイス グループにグループ化します仮想 SD-WAN インターフェースの設定。

ファイアウォールの仮想 ルーターは、この仮想 SD-WAN インターフェイスを使用して、SD-WAN トラフィックを DIA の場所にルーティングします。SD-WAN ポリシールールの SD-WAN パスヘルスおよびトラフィック分散プロファイルにより、使用するパス (およびパスの正常性が劣化した場合に新しいパスを検討する順序) が決定されます。

STEP 6 | ハブ ファイアウォールとブランチ ファイアウォールの両方に対して、同じ名前の SaaS 品質プロファイルを作成します。

代替フェイルオーバーとしてハブ ファイアウォールを正常に活用するには、2 つの同じ名前の SaaS 品質プロファイルをハブ ファイアウォールとブランチ ファイアウォールに設定する必要があります。これを実現する最も簡単な方法は、共有デバイス グループに単一の SaaS 品質プロファイルを作成することです。あるいは、異なるデバイス グループに同じ名前の 2 つの SaaS 品質プロファイルを作成し、それらをハブ ファイアウォールおよびブランチ ファイアウォールにプッシュすることもできます。

1. **Objects (オブジェクト) > SD-WAN Link Management (SD-WAN リンク管理) > SaaS Quality Profile (SaaS 品質プロファイル)** の順に選択し、デバイス グループのドロップダウンから、**Shared (共有)** を選択します。
2. 新しい SaaS 品質プロファイルを 追加 します。
3. SaaS 品質プロファイルの分かりやすい 名前を入力します。

4. **Shared (**共有**)** をオン（チェック）にすると、SaaS 品質プロファイルをすべてのデバイス グループ間で共有します。

   これは、ブランチ ファイアウォールとハブ ファイアウォールが属するすべてのデバイス グループで SaaS 品質プロファイルを利用できるようにするために必要です。
5. **Disable override (**オーバーライドを無効化**)** をオン (チェック) にすると、ローカル ファイアウォールでの SaaS 品質プロファイル設定のオーバーライドを無効にします。
6. 次のいずれかの方法を使用して、 SaaS モニタリング モードを設定します。
   - SaaS アプリケーションの静的 IP アドレスを設定します。

     SaaS アプリケーションごとに *SaaS* 品質プロファイルを作成します。*SaaS* アプリケーションに複数の *IP* アドレスがある場合は、その *SaaS* アプリケーションの複数の静的 *IP* アドレスを使用して *SaaS* 品質プロファイルを設定します。

     1. **IP Address/Object (IP** アドレス/オブジェクト**) > Static IP Address (**静的 **IP** ドレス**)** の順に選択して、IP アドレスを **Add (**追加**)** します。
     2. SaaS アプリケーションの IP アドレスを入力するか、設定済みの アドレス オブジェクトを選択します。
     3. ブランチ ファイアウォールが SaaS アプリケーション パスで正常性情報をプローブするための **Probe Interval (**プローブ間隔**)** を入力します。
     4. **OK** をクリックして、設定の変更を保存します。
   - SaaS アプリケーションの完全修飾ドメイン名 (FQDN) を設定します。
     1. SaaS アプリケーションの FQDN アドレス オブジェクト を設定します。
     2. **IP Address/Object (IP** アドレス/オブジェクト**) > FQDN** を選択して、FQDN を **Add (**追加**)** します。
     3. SaaS アプリケーションの FQDN アドレス オブジェクト を選択します。
     4. ブランチ ファイアウォールが SaaS アプリケーション パスで正常性情報をプローブするための **Probe Interval (**プローブ間隔**)** を入力します。
     5. **OK** をクリックして、設定の変更を保存します。
   - SaaS アプリケーションの URL を設定します。

     URL モニタリングは、ポート *80*、*443*、*8080*、*8081*、および *143* 上のトラフィックのみに対応します。

     1. **HTTP/HTTPS** を選択します。
     2. SaaS アプリケーションの **Monitored URL**（監視対象 **URL**） を入力します。
     3. ブランチ ファイアウォールが SaaS アプリケーション パスで正常性情報をプローブするための **Probe Interval (**プローブ間隔**)** を入力します。
     4. **OK** をクリックして、設定の変更を保存します。

STEP 7 | トラフィック分散プロファイルを作成 して、リンクの状態が劣化した場合に、ブランチ ファイアウォールが DIA リンクから VPN リンク、ハブ ファイアウォールにスワップする順序を指定します。

STEP 8 | SD-WAN ポリシールールを設定 して、SaaS アプリケーションとリンク正常度メトリックを指定し、ファイアウォールが重要な SaaS アプリケーション トラフィックの優先リンクを選択する方法を決定します。

> ***Application*** *(アプリケーション)* タブで、監視している *SaaS* アプリケーションを *SD-WAN* ポリシー ルールに追加して、*SaaS* モニタリング設定が目的の *SaaS* アプリケーションにのみ適用されるようにします。

ユース ケース：ブランチファイアウォールから異なる SaaS アプリケーション宛先への SaaS モニタリング用のハブファイアウォール フェイルオーバーを設定する

組織がブランチ ファイアウォールの場所で SaaS アプリケーションを活用しているが、ブランチ ファイアウォールにスワップ先の正常な DIA リンクがない場合、別の SaaS アプリケーションの宛先を指す SaaS 品質プロファイルを使用して、SaaS アプリケーションへの正常な接続を維持するためのフェイルオーバーの代替手段としてハブファイアウォールを設定できます。

SaaS アプリケーションの DIA リンクヘルス メトリックのしきい値を超え、ブランチ ファイアウォールで使用可能な正常な DIA リンクがない場合、すべての新しいセッションのリンクは次のハブ ファイアウォールにスワップされます。劣化した DIA リンク上の既存のセッションは、ハブ ファイアウォールにスワップオーバーされません。

たとえば、ブランチ ファイアウォールとハブ ファイアウォールが該当する国の反対側にあり、GCP などのクラウド プロバイダにデプロイされている SaaS クラウド アプリケーションにアクセスするとします。ブランチ ファイアウォールから SaaS アプリケーションへの正常な DIA リンクがない場合に、フェイルオーバーとして機能するようにハブ ファイアウォールを設定できます。これを達成するには、ブランチ ファイアウォールとハブ ファイアウォールの両方で同じ名前の SaaS 品質プロファイルを設定し、ブランチ ファイアウォールから正常な DIA リンクが利用できない場合にハブ ファイアウォールに自動的にフェイルオーバーします。ハブ ファイアウォールで設定された SaaS 品質プロファイルは、ハブに最も近いローカル リソースを利用するために、ハブに最も近いランプ上の場所を指します。これにより、正常なフェイルオーバー パスを柔軟に指定でき、ネットワーク帯域幅を輻輳させることなく、正確なエンドツーエンドの SaaS アプリケーションのモニタリング データを維持できます。

STEP 1 | SD-WAN デプロイメントを設定します。

1. 「SD-WAN プラグインのインストール」を行います。
2. 「SD-WANに対応する Panorama とファイアウォールのセットアップ」を行います。
3. 「Panorama への SD-WAN デバイスの追加」を行います。
4. (高可用性構成のみ)SD-WAN 対応 HA デバイスの設定.
5. 「VPN クラスタの作成」を行います。

STEP 2 | リンクタグの作成、SaaS アプリケーションの DIA リンクをグループ化します。

リンク タイプに基づいて各 SaaS アプリケーション DIA リンクに異なる SD-WAN モニタリング設定を適用するために、DIA リンクに複数のリンク タグを作成します。

さらに、複数の DIA リンクに対して単一のリンク タグを作成して、リンクを単一のリンク バンドルにグループ化できます。

STEP 3 | SD-WAN インターフェース プロファイルを設定して ISP 接続の特性を定義し、DIA リンクの速度、ブランチ ファイアウォールがリンクを監視する頻度を指定し、リンク タグを選択して、WAN インターフェース プロファイルが適用されるリンクを指定します。

複数のリンク タグを作成した場合は、リンク タグごとに SD-WAN インターフェース プロファイルを設定する必要があります。

複数の DIA リンクを単一の リンク タグに割り当てることによってリンク バンドルを作成した場合、リンク タグを指定すると、バンドル内のすべての DIA リンクに SD-WAN インターフェース プロファイル設定が適用されます。

STEP 4 | 各 SaaS アプリケーションの DIA リンクの 物理イーサネット インターフェースを設定します。

DIA リンクのすべての物理イーサネット インターフェースは *Layer3* である必要があります。

STEP 5 | SaaS アプリケーション DIA リンクのすべての物理イーサネット インターフェイスを 1 つのインターフェイス グループにグループ化します仮想 SD-WAN インターフェースの設定。

ファイアウォールの仮想 ルーターは、この仮想 SD-WAN インターフェイスを使用して、SD-WAN トラフィックを DIA の場所にルーティングします。SD-WAN ポリシールールの SD-WAN パスヘルスおよびトラフィック分散プロファイルにより、使用するパス (およびパスの正常性が劣化した場合に新しいパスを検討する順序) が決定されます。

STEP 6 | ハブ ファイアウォールとブランチ ファイアウォールの両方に対して、同じ名前の SaaS 品質プロファイルを作成します。

代替フェイルオーバーとしてハブ ファイアウォールを正常に活用するには、2 つの同じ名前の SaaS 品質プロファイルをハブ ファイアウォールとブランチ ファイアウォールに設定する必要があります。それぞれが異なるデバイス グループ内の異なる SaaS アプリケーションの宛先を指す同じ名前の 2 つの SaaS 品質プロファイルを作成し、それらをハブ ファイアウォールおよびブランチ ファイアウォールにプッシュします。

1. **Objects (オブジェクト) > SD-WAN Link Management (SD-WAN リンク管理) > SaaS Quality Profile (SaaS 品質プロファイル)** の順に選択し、Device Group (デバイス グループ) ドロップダウンリストからブランチ ファイアウォールを含むターゲットのデバイス グループを選択します。
2. 新しい SaaS 品質プロファイルを 追加 します。
3. SaaS 品質プロファイルの分かりやすい 名前を入力します。
4. **Disable override (オーバーライドを無効化)** をオン (チェック) にすると、ローカル ファイアウォールでの SaaS 品質プロファイル設定のオーバーライドを無効にします。

5. 次のいずれかの方法を使用して、 SaaS モニタリング モードを設定します。
   - SaaS アプリケーションの静的 IP アドレスを設定します。

     SaaS アプリケーションごとに *SaaS* 品質プロファイルを作成します。*SaaS* アプリケーションに複数の *IP* アドレスがある場合は、その *SaaS* アプリケーションの複数の静的 *IP* アドレスを使用して *SaaS* 品質プロファイルを設定します。

     1. **IP Address/Object (IP** アドレス/オブジェクト**) > Static IP Address (**静的 **IP** アドレス**)** の順に選択して、IP アドレスを **Add (**追加**)** します。
     2. SaaS アプリケーションの IP アドレスを入力するか、設定済みの アドレス オブジェクトを選択します。
     3. ブランチ ファイアウォールが SaaS アプリケーション パスで正常性情報をプローブするための **Probe Interval (**プローブ間隔**)** を入力します。
     4. **OK** をクリックして、設定の変更を保存します。
   - SaaS アプリケーションの完全修飾ドメイン名 (FQDN) を設定します。
     1. SaaS アプリケーションの FQDN アドレス オブジェクト を設定します。
     2. **IP Address/Object (IP** アドレス/オブジェクト**) > FQDN** を選択して、FQDN を **Add (**追加**)** します。
     3. SaaS アプリケーションの FQDN アドレス オブジェクト を選択します。
     4. ブランチ ファイアウォールが SaaS アプリケーション パスで正常性情報をプローブするための **Probe Interval (**プローブ間隔**)** を入力します。
     5. **OK** をクリックして、設定の変更を保存します。
   - SaaS アプリケーションの URL を設定します。

     URL モニタリングは、ポート *80*、*443*、*8080*、*8081*、および *143* 上のトラフィックのみに対応します。

     1. **HTTP/HTTPS** を選択します。
     2. SaaS アプリケーションの **Monitored URL**（監視対象 **URL**） を入力します。
     3. ブランチ ファイアウォールが SaaS アプリケーション パスで正常性情報をプローブするための **Probe Interval (**プローブ間隔**)** を入力します。
     4. **OK** をクリックして、設定の変更を保存します。
6. **Objects (**オブジェクト**) > SD-WAN Link Management (SD-WAN** リンク管理**) > SaaS Quality Profile (SaaS** 品質プロファイル**)** の順に選択し、Device Group (デバイス グループ) ドロップダウンリストからハブ ファイアウォールを含むターゲットのデバイス グループを選択します。
7. ステップ 6.2～6.5 を繰り返して、別の宛先にある SaaS アプリケーション用に同じ名前の SaaS 品質プロファイルを作成します。

   このステップは、ハブ ファイアウォールが属するデバイス グループに同じ名前の SaaS 品質プロファイルを作成するために必要です。

STEP 7 | トラフィック分散プロファイルを作成 して、リンクの状態が低下した場合に、ブランチ ファイアウォールが DIA リンクから VPN リンク、ハブ ファイアウォールにスワップする順序を指定します。

STEP 8 | SD-WAN ポリシールールを設定 して、SaaS アプリケーションとリンク正常度メトリックを指定し、ファイアウォールが重要な SaaS アプリケーション トラフィックの優先リンクを選択する方法を決定します。

> ***Application*** *(アプリケーション)* タブで、監視している *SaaS* アプリケーションを *SD-WAN* ポリシー ルールに追加して、*SaaS* モニタリング設定が目的の *SaaS* アプリケーションにのみ適用されるようにします。

SD-WAN トラフィック分散プロファイル

SD-WAN のトポロジーでは、ファイアウォールは、重要なビジネスアプリケーションで最高のパフォーマンスが得られるように、*per application (アプリケーション毎)* に電圧低下、停電、およびパスの劣化を検出し、新たなパスを選択します。複数の ISP リンクを使用すると、トラフィック容量が拡大され、コストを削減することができます。Path Monitoring and Probe Frequency (パス モニタリングおよびプローブ頻度) をデフォルト設定のままにしておくと、新たなパスの選択は 1 秒未満で実行されます。それ以外の場合は、新たなパスの選択に 1 秒以上かかる場合があります。

このようなパス選択の実装に、ファイアウォールは SD-WAN ポリシールールを使用します。SD-WAN ポリシー ルールは、アプリケーション用のパス品質の低下時にセッションロード分散およびより良いパスへのフェイルオーバーのためのパスの選択方法を指定するトラフィック分散プロファイルを参照します。

(SD-WAN ポリシー ルールに合致する) アプリケーションまたはサービスが使用するべきトラフィック分散方法を決定します。

- **Best Available Path (最適なパス)**-コストが要因ではなく、アプリケーションがブランチからの任意のパスを使用して良い場合は、この方法を選択します。ファイアウォールはパス品質メトリックに基づいてトラフィックを分散し、リスト内のすべてのリンク タグに属するリンクの中から特定のリンクにフェイルオーバーすることで、ユーザーに最高のアプリケーション エクスペリエンスを提供します。
- **Top-Down Priority (トップダウン優先)**-最後の手段として、あるいはバックアップ用リンクとしてのみ使用する高コストあるいは低容量のリンクがある場合、トップダウン優先方式を使用し、それらのリンクを含むタグをプロファイルのリンクタグのリストの末尾に配置します。ファイアウォールは、まずリストの先頭のリンクタグを使用してセッションのトラフィックをロードするリンクおよびフェイルオーバーするリンクを決定します。トップ リンク タグのどのリンクもパス品質プロファイルに基づいて修飾されていない場合、ファイアウォールはリストの 2 番目のリンク タグからリンクを選択します。2 番目のリンク タグ内のどのリンクも修飾されていない場合、ファイアウォールが最後のリンクタグで修飾されたリンクを見つけるまで、このプロセスが必要に応じて続行されます。関連付けられているすべてのリンクが過負荷であり、品質のしきい値を満たすリンクがない場合、ファイアウォールは Best Available Path (最適なパス) 方法を使用して、トラフィックを転送するリンクを選択します。ファイアウォールは、フェイルオーバー イベント開始時に、リンクタグのトップダウン 優先順位リストの先頭から開始して、フェイルオーバー先のリンクを検索します。

- **Weighted Session Distribution** (加重セッション分散)-(ルールに一致する) ISP および WAN リンクに手動でトラフィックをロードし、電圧低下時にフェイルオーバーを必要としない場合は、この方法を選択します。1 つのリンクタグでグループ化されたインターフェースが取得する新規セッションのスタティックな割合を適用する際に、リンクロードを手動で指定します。ファイアウォールは、最も低い割合が割り当てられているリンクがそのセッションの割合に達するまで、指定されたリンクタグを備えたリンク間でラウンドロビン方式で新たなセッションを分散します。次に、ファイアウォールは残りのリンクを同じ方法で使用します。この方法は、待機時間の影響を受けず、大規模なブランチ バックアップや大きなファイル転送など、リンクの帯域幅容量を大量に必要とするアプリケーションに選択できます。

  リンクでブラウンアウトが発生した場合、ファイアウォールは一致するトラフィックを別のリンクにリダイレクトしません。

パスの悪状態が発生した場合、SD-WAN ポリシールールでアプリケーション向けに選択したトラフィック分散方法と、リンクのグループのリンクタグにより、ファイアウォールは以下の通り、新しいパスを選択する (リンク フェイルオーバーを実行する) かどうか、そして選択方法を決定します。

Path Condition (パスの状況)	Top-Down Priority (トップダウン優先)	Best Available Path (最適なパス)	Weighted Session Distribution (加重セッション分散)
Session on existing path failed a path health threshold (brownout) (既存のパスのセッションがパス ヘルスのしきい値を満たさない(電圧低下))	Affected session fails over to better path (if available) (影響を受けたセッションが (可能な場合)、より適切なパスにフェイルオーバーする)	Affected session fails over to better path (if available) (影響を受けたセッションが (可能な場合)、より適切なパスにフェイルオーバーする)	Affected sessions don't fail over (影響を受けたセッションがフェイルオーバーしない)
Top-Down or Best Available Path recovered: existing path is still qualified (good) (トップダウンまたは最適なパスが回復し、既存のパスが依然修飾される(良好))	Affected session fails back to previous path (影響を受けたセッションが以前のパスにフェイルバックする)	Affected session stays on existing path, doesn't fail back (影響を受けたセッションが既存のパスにとどまり、フェイルバックしない)	Affected sessions don't fail over (影響を受けたセッションがフェイルオーバーしない)
Top-Down or Best Available Path recovered: existing path is still qualified (good) (トップダウンまたは最適なパスが回復し、既存のパス	All sessions fail back to previous path (全セッションが以前のパスにフェイルバックする)	Selective sessions fail back to previous path until affected existing path recovers (影響を受けた既存のパスが回復するまで、選択されたセッションが	Affected sessions don't fail over (影響を受けたセッションがフェイルオーバーしない)

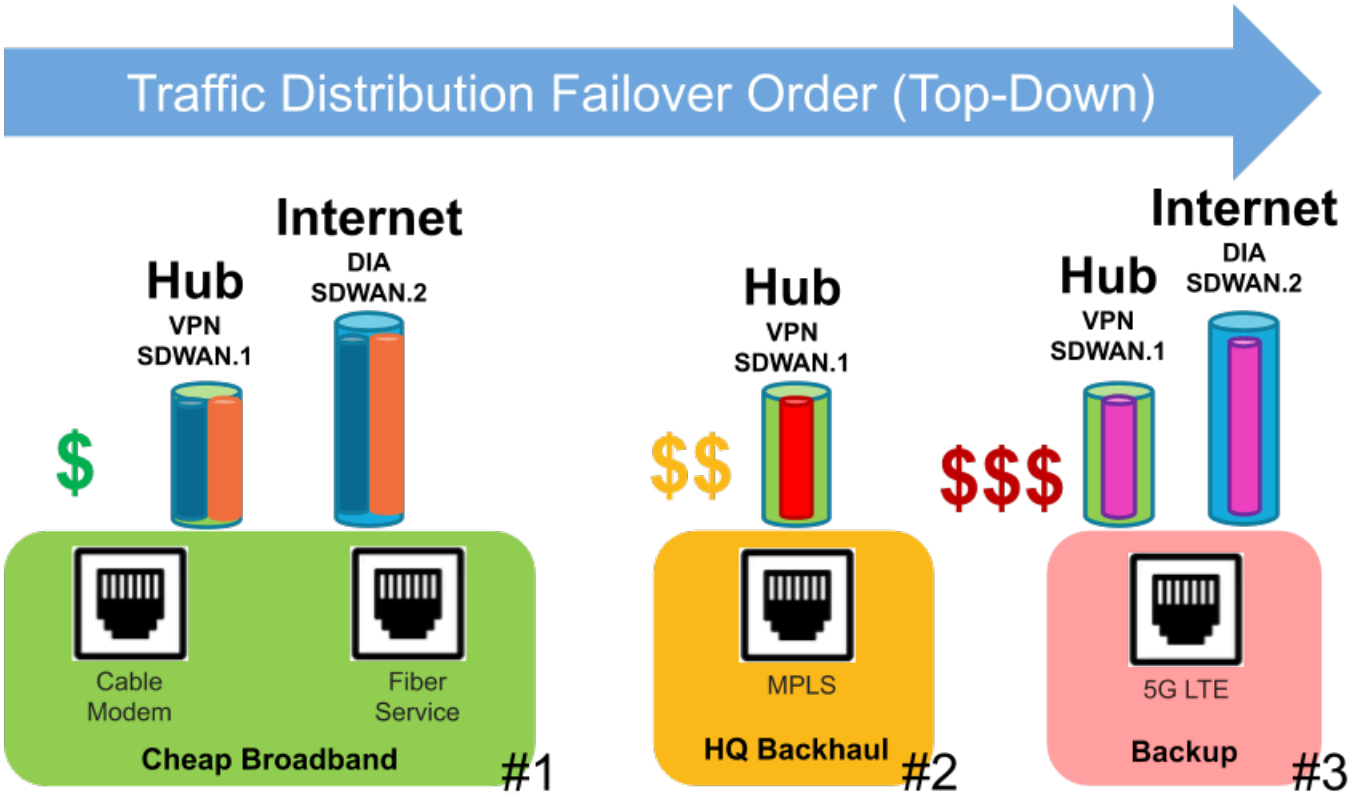
Path Condition (パスの状況)	Top-Down Priority (トップダウン優先)	Best Available Path (最適なパス)	Weighted Session Distribution (加重セッション分散)
のヘルス チェックを満たさない)		以前のパスにフェイルバックする)	
Existing path is down (blackout) (既存のパスがダウンする(blackout))	All sessions fail over to next path on list (全セッションがリストの次のパスにフェイルオーバーする)	All sessions fail over to next best path (全セッションが次の最適なパスにフェイルオーバーする)	All sessions fail over to other tags based on weight settings (全セッションが、重み付けされた設定に基づき、その他のタグにフェイルオーバーする)
Brownout with no qualified (better) path (Brownout時に修飾パス（より良好なパス）が存在しない)	Take best available path (最適なパスを取る)	Take best available path (最適なパスを取る)	Take best available path (最適なパスを取る)

また、ファイアウォールは、単一のリンクタグのインターフェース メンバー間でのセッション ロードの共有機能を自動的に実行します。インターフェースが最大 Mbps 近くになると、優れたインターフェースのヘルス メトリックがある場合、新たなセッションは、(トラフィック分散方式に基づき) 別のリンクタグを持つインターフェースに流れます。

Path Condition (パスの状況)	Top-Down Priority (トップダウン優先)	Best Available Path (最適なパス)	Weighted Session Distribution (加重セッション分散)
Multiple links with the same SD-WAN Tag (同じ SD-WAN タグを備える複数のリンク)	Share session load equally among links within SD-WAN Tag (SD-WAN タグのリンク間でセッション ロードを均等に共有する)	Share session load based on best path within SD-WAN Tag (SD-WAN タグ内の最適パスに基づき、セッションロードを共有する)	Share session load based on % weight assigned to SD-WAN Tag (SD-WAN タグに割り当てられた割合の重みに基づき、セッションロードを共有する)
Multiple links with different SD-WAN Tags (SD-WAN タグが異なる複数リンク)	Share session load based on list priority, load link(s) in first SD-WAN Tag first. (リストの優先度に基づき、セッションロードを共有し、SD-WAN タグの最初の	Share session load based on best path from all SD-WAN Tags (全 SD-WAN タグからの最適パスに基づいてセッションロードを共有する)	Share session load based on % weight assigned to SD-WAN Tags (SD-WAN タグに割り当てられ割合の重みに基づき、

Path Condition (パスの状況)	Top-Down Priority (トップダウン優先)	Best Available Path (最適なパス)	Weighted Session Distribution (加重セッション分散)
	リンクをまずロードする。)		セッションロードを共有する)

以下の図は、トップダウン方式の優先順位を使用するトラフィック分布プロファイルの例を説明しています。#1、#2、#3 は、アプリケーション セッションのフェイルオーバーを完了するために高ヘルスのパスを検索する上でファイアウォールが必要に応じて検査するリンクのリンクタグの順序を示します。ファイアウォールは、発生した個別のフェイルオーバーイベント毎にリンクタグのトップダウン方式のリストの先頭から開始します。

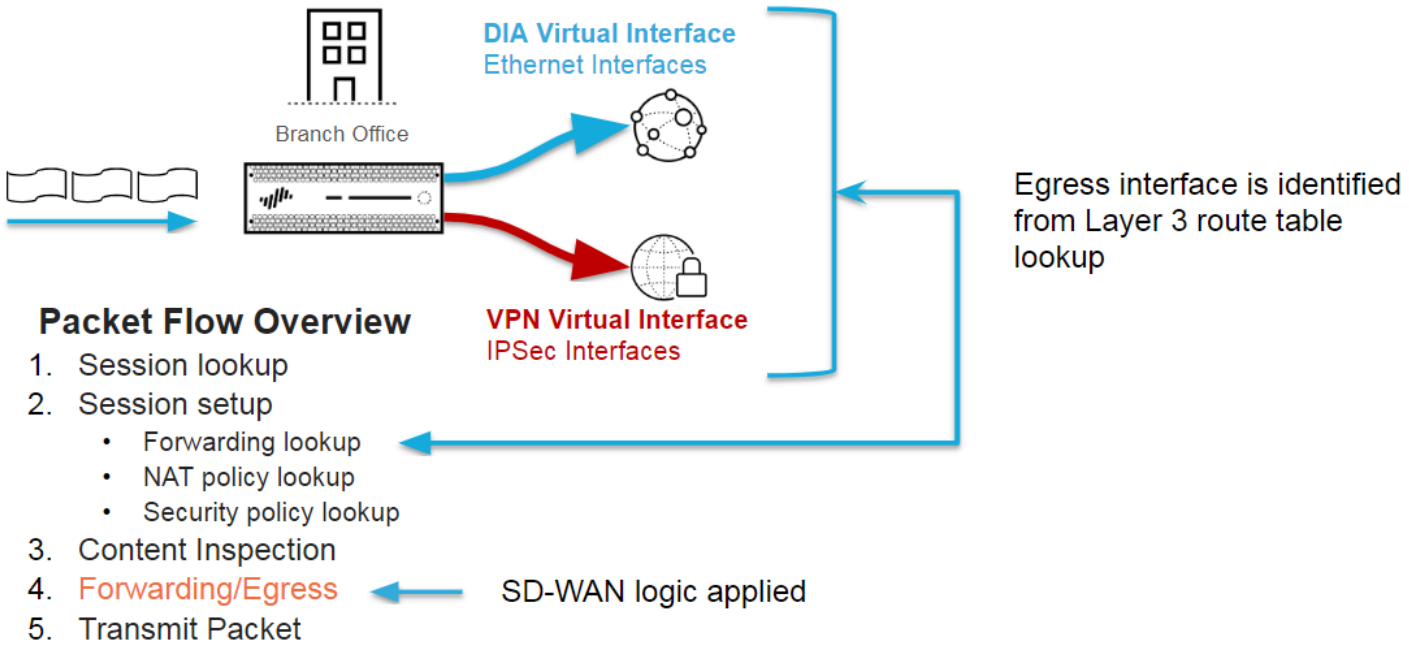


1. このトップダウン優先の例では、ブランチからの特定のアプリケーション (office365-enterprise-access 等) の内容を含むパケットがファイアウォールに届きます。ファイアウォールは、ルートテーブルを使用して、宛先へのネクストホップおよび、sdwan.901 と名付けられた仮想 SD-WAN インターフェース トンネルである発信インターフェースを決定します。セキュリティ ポリシー ルールではこのパケットは許可されます。次に、パケットは、ハブの宛先ゾーンを指定する (Office365 to Hub1 と名付けられた) SD-WAN ポリシー ルールと合致することになります。ファイアウォールは、SD-WAN ポリシールールのパス品質プロファイル、トラフィック分散プロファイル、および上記プロファイルのリンクタグを使用して、sdwan.901 のどのインターフェースメンバー (リンク) を使用するかを決定します。トラフィック分散プロファイルには、3 つのリンクタグが以下の順序でリストされています。#1

コスト安のブロードバンド、#2 本社のバックホール、#3 バックアップ (ファイアウォールがリンクを調べてフェイルオーバー可能なリンクを検出するリンクタグの順序)。

2. すべてのパスが パス品質プロファイルにより) 修飾されていると仮定する場合、ファイアウォールは、トラフィック分散プロファイルリストの最初のリンクタグでタグ付けされた物理リンクの 1 つにパケットを分散します。つまり、コスト安のブロードバンドです。sdwan.901 トンネルには、ケーブルモデムの VPN トンネルとファイバサービスの VPN トンネルの 2 つのメンバーインターフェース (2 つのキャリア) があります。ファイアウォールは、まずラウンドロビン方式でリンクを検査し、最初に見つかった修飾リンク (ケーブルモデムリンク等) を選択します。例えば、ケーブルモデムリンクです。
3. 最初のコスト安ブロードバンドリンク (ケーブルモデム) が修飾リンクでない場合、ファイアウォールは 2 番目のコスト安ブロードバンドリンク (ファイバサービス) を選択します。
4. 2 番目のコスト安ブロードバンドリンク (ファイバサービス) が修飾リンクでない場合、ファイアウォールは #2 リンクタグである 本社のバックホールとタグ付けされたリンクを選択します。これは、同じハブに向かうよりコスト高の MPLS リンクです。
5. MPLS リンクが修飾リンクでない場合、ファイアウォールは #3 リンクタグとタグ付けされたバックアップを選択します。これは、同じハブに向かうさらにコスト高の 5G LTE リンクです。
6. ファイアウォールは、フェイルオーバーする適切なリンクを検出できない場合、最適な方法を使用してリンクを選択します。
7. ファイアウォールは、新たなフェイルオーバー イベント開始時に、リンクタグのトップダウン リストの先頭から開始して、フェイルオーバー先のリンクを検索します。

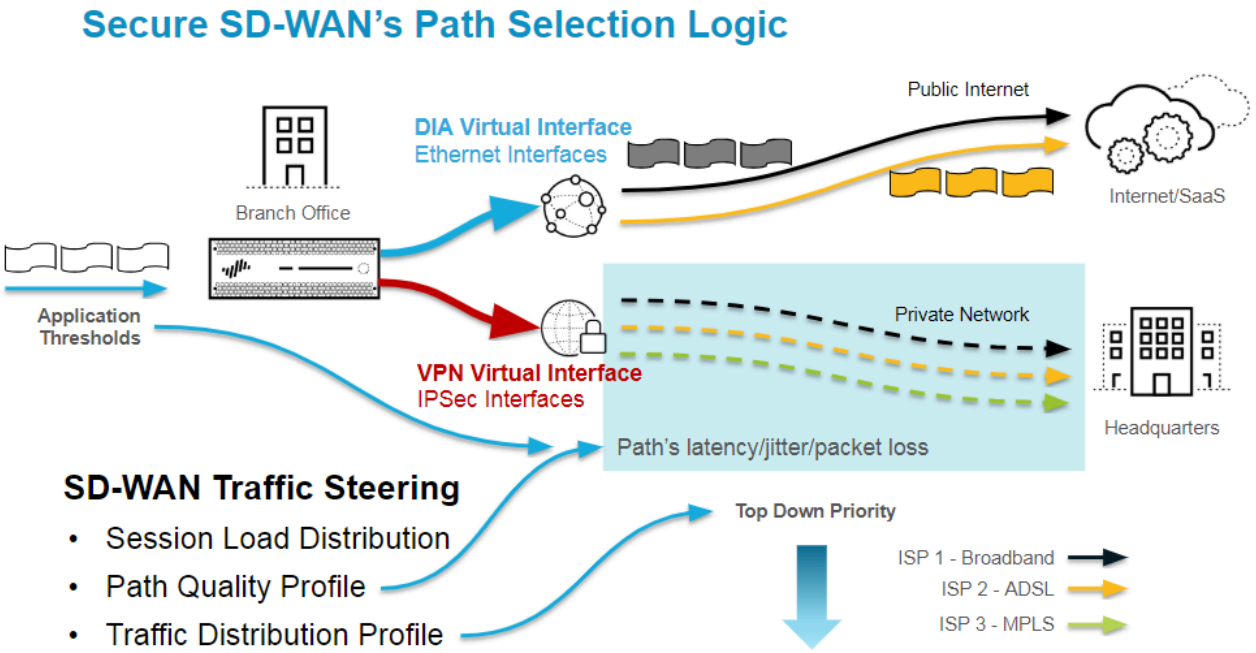
SD-WAN トラフィック分散は、パケットフロー ロジックの後半のステップの 1 つであることに留意してください。ここで、パケットフローの全体像を俯瞰してみましょう。



図のパケットフローの詳細は以下の通りです。

1. アプリケーションのセッションがファイアウォールに届くと、ファイアウォールはセッション検索を実行して、このセッションが既存のセッションであるか、それとも新しいセッションかを判断します。
2. 新しいセッションの場合は、セッションセットアッププロセスを通ります。
    1. Forwarding lookup (転送検索)-ファイアウォールは、レイヤー3 ルートテーブルあるいはレイヤー2 転送データベース検索等で出口ゾーン、出口インターフェース、および仮想システムを取得します。SD-WAN ポリシールールに合致するアプリケーションの場合、ファイアウォールは仮想 SD-WAN インターフェースを出口インターフェースとして使用します。
    2. NAT Policy lookup (NAT ポリシー検索) -セッションが NAT ルールに合致する場合、ファイアウォールは別の転送ルックアップを実行し、最終的な (トランスレートされた) 出力インターフェースおよびゾーンを決定します。
    3. Security Policy lookup (セキュリティ ポリシー検索)-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には、セッションが作成され、セッションテーブルにインストールされます。次に、ファイアウォールは App-ID™ および User-ID™ を使用し、追加の分類を実行します。
3. Content Inspection (コンテンツの検査)-ファイアウォールは、必要に応じてペイロードおよびヘッダに対して脅威検査 (IPS のアンチスパイウェア [脆弱性防御]、アンチウイルス、URL フィルタリング、WildFire®、その他) を実行します。
4. 転送 / 出口段階は、パス選択を実行し、パケットを転送します。この段階では、SD-WAN パス選択が行われます。
    1. Packet Forwarding Process (パケット転送プロセス)- ファイアウォールは、入口インターフェースを使用して転送ドメインを決定します。ルーティング、スイッチング、またはバーチャル ワイヤ転送が実行されます。
    2. SD-WAN パスの選択は、アプリケーションが SD-WAN ポリシー ルールに合致した際に実行されます。パス品質プロファイルはパス修飾を定義し、トラフィック分散プロファイルは、パスの選択方法および選択中に考慮されるパスの順序を定義します。
    3. 必要に応じて、IPSec/SSL-VPN トンネル暗号化が実行されます。
    4. Packet Egress Process (パケット出力プロセス)-(必要な場合)QoS シェーピング、DSCP リライト、および IP フラグメンテーションが適用されます。
5. Transmit Packet (パケットの送信)-ファイアウォールが、選択された出口インターフェース経由でパケットを転送します。

ここで視点を変えて、SD-WAN パス選択ロジックをさらに詳しく説明します。



1. ファイアウォールは、転送検索中にルートテーブルを参照します。ファイアウォールは、レイヤー3 プレフィックスと一致する宛先 IP アドレスに基づき、出口 SD-WAN 仮想インターフェースを決定します。パケットは直接公開されたインターネットに送信される、セキュアな VPN リンク経由でハブに戻されます。
2. ファイアウォールは、VPN トンネル経由で実行されるヘルスチェックを実行することにより、各パスを監視します。各 DIA 回線には、ヘルス情報を監視する VPN トンネルが備わっています。
3. SD-WAN ポリシー ルールのアプリケーションはパス品質プロファイルに関連付けられており、ファイアウォールは実際のパスの平均遅延、ジッター、およびパケット損失の値をしきい値と比較します。
4. 遅延、ジッター、またはパケット損失の値がしきい値よりも高いパスは選択されません。
5. 次に、仮想 SD-WAN インターフェースの全修飾パスが、トラフィック分散プロファイル方法およびパスの優先度 (順序付け) ロジックの対象となります。SD-WAN リンクタグは ISP サービスをグループ化し、トラフィック分散プロファイルにおける上記タグの順序により、パスの選択中にパスの優先順位が付けられます。
6. つまり、Path Quality Profile (パス品質プロファイル) および Traffic Distribution profile (トラフィック分散プロファイル) が共に使用すべき次の最善のパスを決定し、ファイアウォールがそのリンクを使用してトラフィックを転送します。

トラフィック分散プロファイルの作成

SD-WAN 構成計画に基づいて、SD-WAN ポリシールール内のアプリケーションのセッションロードとフェイルオーバーの方法に基づいて、必要なSD-WAN トラフィック分散プロファイルを作成します。

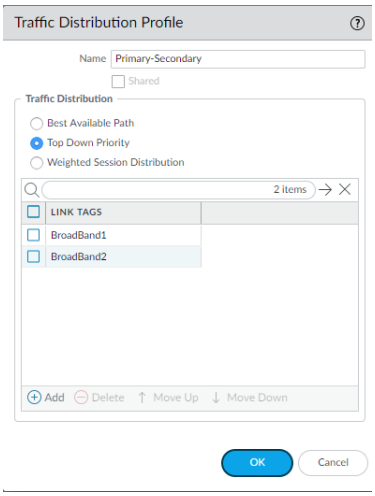
STEP 1 | Panorama Web インターフェイスへのログイン。

STEP 2 | SD-WAN interface profile (SD-WAN インターフェース プロファイル) でリンクタグが既に設定され、コミットおよびプッシュされていることを確認します。Panorama™ がこのトラフィック分配プロファイルで指定されたリンクタグを SD-WAN インターフェース プロファイルに正常に関連付けることができるように、リンクタグをハブとブランチにプッシュする必要があります。

STEP 3 | **Device Group(デバイス グループ)** を選択します。

STEP 4 | トラフィック分配プロファイルを作成します。

1. **Objects (オブジェクト)**、 > **SD-WAN Link Management(SD-WAN リンク管理)**、 > **Traffic Distribution Profile (トラフィック分配プロファイル)** と選択します。
2. 最大 31 文字までの英数字を使用して、**Name (名前)** でトラフィック分配プロファイルを **Add (追加)** します。



3. すべてのデバイスグループ (ハブとブランチの両方) でこのトラフィック分配プロファイルを使用する場合にのみ、 **Shared (共有)** を選択します。
4. トラフィック分配方法から 1 つを選択して、このプロファイルにこの方法を使用する最大 4 つのリンクタグを追加します。

   - **Best Available Path (利用できる最適なパス)**- 1 つまたは複数の **Link Tags (リンク タグ)** を **Add (追加)** します。最初にパケットが交換される際、App-ID がアプリケーションをパケットに分類する前に、ファイアウォールは (タグの順序に基づき) タグ内の最良のヘルスメトリックのパスを使用します。ファイアウォールはアプリケーションを識別した後、使用していたパスのヘルス (パス品質) を最初のリンクタグの最初のパス (インターフェース) のヘルスと比較します。元のパスのヘルスが良い場合は、選択されたパスは引き続き使用されます。それ以外の場合、ファイアウォールは元のパスを置き換えます。ファイアウォールは、リンクタグ内のすべてのパス

が評価されるまでこのプロセスを繰り返します。最後のパスは、一致基準を満たすパケットが到着したときにファイアウォールが選択するパスです。

リンクが非修飾になり、次善パスにフェイルオーバーする必要がある場合、ファイアウォールは非修飾リンクから次善パスに毎分最大 *1,000* セッションを移行できます。例えば、*tunnel.901* に *3,000* のセッションがあるとします。このうち *2,000* セッションが *SD-WAN* ポリシー ルール*A* に合致し、*1,000* セッションが *SD-WAN* ポリシー ルール *B* に合致します *(*どちらのルールも ***Best Path Available*** *(*利用できる最適なパス*)* で設定したトラフィック分配ポリシーを備えています*)*。*tunnel.901* が非修飾になった場合、*3,000* セッションを非修飾リンクから次善パスに移行するのに *3* 分かかります。

- **Top Down Priority (**トップダウン優先度**)**-1 つまたは複数の **Link Tags (**リンクタグ**)** を **Add(**追加**)** します。ファイアウォールは、追加した **Link Tags (**リンクタグ**)** のトップダウン順序を使用して(一致基準を満たす) 新しいセッションをリンクに分配します。ファイアウォールは、このプロファイル向けに設定された最初のタグを調べ、そのタグを使用するパスを調べて、適格な (このルールのパス品質のしきい値以下の) 最初のパスを選択します。そのリンクタグで適格なパスが見つからない場合、ファイアウォールは次のリンクタグを使用するパスを調べます。全リンクタグで全パスを調べてもパスが見つからない場合、ファイアウォールは **Best Available Path (**利用可能な最適なパス**)** の手法を使用します。選択された最初のパスは、そのパスのパス品質しきい値の 1 つを超えるまで優先パスです。超えた時点で、ファイアウォールはリンク タグ リストの先頭から再び開始して、新しい優先パスを見つけます。

  ハブにリンクが *1* つしかない場合、そのリンクはすべての仮想インターフェイスと *DIA* トラフィックをサポートします。特定の順序でリンクの種類を使用する場合は、トラフィック配信プロファイルを *[*上位の優先度*]* を指定するハブに適用し、*[*リンク タグ*]* に優先順序を指定する必要があります。代わりに *[*利用可能な最適パス*]* を指定するトラフィック配布プロファイルを適用すると、ファイアウォールはコストに関係なくリンクを使用して、ブランチへの最適なパスを選択します。要約すると、トラフィック分散プロファイルのリンク タグ、ハブ仮想インターフェイスに適用されるリンク タグ、*SD-WAN* インターフェイス プロファイルの ***VPN*** フェールオーバー メトリックは、トラフィック分散プロファイルが 最高ダウン優先順位を指定した場合にのみ機能します。

- **Weighted Session Distribution (**重み付きセッション分散**)**-1 つまたは複数の **Link Tags(**リンクタグ**)**を**Add (**追加**)**して、各 **Link Tag (**リンクタグ**)**に対して**Weight (**重み**)** の割合を合計 100% となるように入力します。ファイアウォールはリンクタグ間のセッション負荷分散を、この割合が最大値に達するまで、実行します。リンクタグに複数のパスがある場合、ファイアウォールはパスのヘルスメトリックに達する

までラウンドロビンで均等に分配した後、制限に達していないその他のメンバーにセッションを分配します。

複数の物理インターフェースに同じタグが付いている場合、ファイアウォールは一致するセッションをそのインターフェイス間で均等に分配します。すべてのパスがヘルス (パス品質) のしきい値未満の場合、ファイアウォールは、ヘルス統計値が最も良好なパスを選択します。*SD-WAN* リンクが使用できない場合 (停電時等)、ファイアウォールはスタティックあるいはダイナミックルーティングを使用して、合致するパケットをルーティングします。

パケットが仮想 *SD-WAN* インターフェースにルーティングされても *SD-WAN* ポリシーのトラフィック分配プロファイルに基づいてセッションの優先パスを見つけられない場合、ファイアウォールは暗黙のうちに利用できる最適なパスの手法を使用して優先パスを見つけます。ファイアウォールは、*SD-WAN* ポリシールールに合致しないアプリケーション セッションをファイアウォールの暗黙の最終ルールに基づき分散します。これにより、トラフィック分配プロファイルに関わらず、利用可能なすべてのリンク間でセッションがラウンドロビンで分配されます。

ファイアウォールが一致しないセッションを配布する方法を制御する場合は、指定した順序で特定のリンクに合致しないセッションの分散する最終的な包括的ルールを作成します。

5. (任意) リンクタグを追加した後、**Move Up** (上へ) or **Move Down** (下へ) の矢印を使用して、ファイアウォールがこのプロファイルと SD-WAN ポリシールールで選択したアプリケーションのリンクを使用します。
6. **OK** をクリックします。

STEP 5 | 設定の変更を **Commit** (コミット) および**Commit and Push** (コミットしてプッシュ) します。

STEP 6 | 変更を **Commit** (コミット)します。

エラー訂正プロファイルの作成

前方誤り訂正 (FEC) は、ノイズの多い通信回線で発生する特定のデータ伝送エラーを訂正する方法であり、これにより、再送信を必要とせずにデータの信頼性が向上します。FEC は、音声、VoIP、ビデオ会議など、パケットの損失や破損に敏感なアプリケーションに役立ちます。FEC を使用すると、受信ファイアウォールは、送信エンコーダがアプリケーション フローに埋め込むパリティ ビットを使用することにより、損失したパケットや破損したパケットを回復することができます。フローを修復すると、SD-WAN データを別のパスにフェイルオーバーしたり、TCP がパケットを再送信したりする必要がなくなります。また、UDP はパケットを再送信しないため、FEC は、失われたパケットまたは破損したパケットを回復することにより、UDP アプリケーションを支援できます。

SD-WAN FEC は、エンコーダーおよびデコーダーとして機能するブランチ ファイアウォールとハブ ファイアウォールをサポートします。FEC メカニズムでは、エンコーダが冗長ビットをビットストリームに追加し、デコーダはその情報を使用して、必要に応じて受信データを修正してから、宛先に送信します。

SD-WAN は、エラー訂正の代替方法としてパケット複製もサポートしています。パケット複製は、1 番目のトンネルから 2 番目のトンネルへのアプリケーション セッションの完全な複製を実行します。パケットの複製には FEC よりも多くのリソースが必要であり、ドロップされたパケットに対する許容度が低い重要なアプリケーションにのみ使用する必要があります。

独自の復旧メカニズムを内蔵した最新のアプリケーションでは、*FEC* やパケットの複製が不要な場合があります。*FEC* またはパケット複製は、そのようなメカニズムから実際に利益を得ることができるアプリケーションにのみ適用してください。そうしないと、多くの追加の帯域幅と *CPU* オーバーヘッドが何のメリットもなく導入されます。*SD-WAN* の問題が輻輳である場合、*FEC* もパケットの複製も有用ではありません。

FEC およびパケット複製機能を使用するには、Panorama が PAN-OS 10.0.2 以降のリリースと、PAN-OS リリースと互換性のある SD-WAN プラグイン 2.0 以降のリリースを実行する必要があります。エンコーダとデコーダは両方ともPAN-OS 10.0.2 以降のリリースで実行している必要があります。1 つのブランチまたはハブが必要条件よりも旧式のソフトウェア リリースを実行している場合、FEC またはパケット複製ヘッダーのあるトラフィックはそのファイアウォールでドロップされます。

PAN-OS 10.0.3 以降、FEC とパケットの複製は、既にサポートされているハブスポーク トポロジに加えて、フル メッシュ トポロジでサポートされています。

FEC とパケットの重複は、DIA リンクでは使用しないでください。ブランチとハブ間の VPN トンネル リンク専用です。

FEC およびパケットの複製は、*SD-WAN* 対応の *PAN-OS*ファイアウォールでのみサポートされます。*FEC* とパケットの重複は、プリズマ アクセス ハブではサポートされていません。

エンコーダ (FEC またはパケット複製を開始する側) で FEC またはパケット複製を設定するには、Panorama を使用して次の操作を行います。

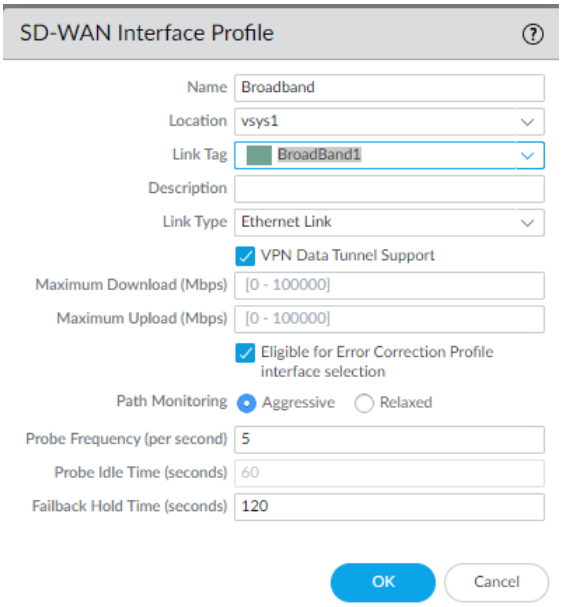
- **Eligible for Error Correction Profile interface selection (**エラー訂正プロファイル インターフェイスの選択対象**)** を指定する SD-WAN インターフェースを作成して、プロファイルを 1 つ以上のインターフェースに適用します。
- エラー訂正プロファイルを作成して、FEC またはパケットの複製を実装します。
- エラー訂正プロファイルを SD-WAN ポリシー ルールに適用し、ルールを適用する単一のアプリケーションを指定します。
- 設定をエンコーダにプッシュします。(デコーダ [受信側] は、FEC またはパケット複製のための特定の設定を必要としません。エンコーダがエラー訂正を開始する限り、メカニズムはデコーダでデフォルトで有効になっています)

FEC とパケットの複製は、*1,340 byte* の *MTU* をサポートします。これより大きいパケットは、*FEC* またはパケット複製プロセスを通過しません。

STEP 1 | Panorama Web インターフェイスへのログイン。

STEP 2 | SD-WAN インターフェース プロファイルの設定、エラー訂正プロファイルインターフェイス選択の対象 を選択して、ファイアウォールがエラー訂正のためにインターフェイス (SD-WAN インターフェイスプロファイルが適用される場所) を自動的に使用できることを示します。このオプションがデフォルトで選択されているかどうかは、プロファイルに選択した **Link Type** (リンク タイプ) によって異なります。

たとえば、プロファイルで***Eligible for Error Correction Profile interface selection*** (エラー修正プロファイル インターフェイスの選択対象) のチェックを外し、プロファイルを高価な *5G LTE* リンクに適用して、そのリンクでコストのかかるエラー訂正が実行されないようにすることができます。



STEP 3 | 作成した SD-WAN インターフェイスプロファイルをイーサネットインターフェイスにSD-WAN に対応する物理イーサネット インターフェースの設定して適用します。

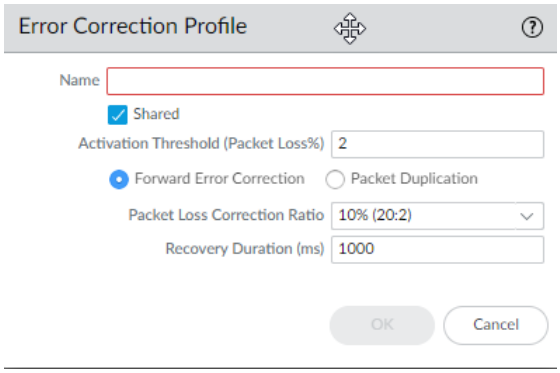
STEP 4 | FEC またはパケットの複製用にエラー訂正プロファイルを作成します。

1. **Objects** (オブジェクト) > **SD-WAN Link Management** (SD-WAN リンク管理) > **Error Correction Profile** (エラー訂正プロファイル) の順に選択します。
2. エラー訂正プロファイルを **Add** (追加) し、分かりやすい **Name** (名前) を 31 文字以内で入力します (例: EC_VOIP)。
3. **Shared** を選択すると、Panorama 上のすべてのデバイス グループと、単一 vsys ハブまたはブランチ上のデフォルトの vsys、またはこの設定をプッシュするマルチ vsys ハブまたはブランチ上の vsys1 でエラー訂正プロファイルを使用できるようになります。
4. **Activate when packet loss exceeds** (パケット損失が設定値を超えたらアクティブ化) **(%)** 設定を指定します–パケット損失がこの割合を超えると、この Error Correction Profile（エラー訂正プロファイル）が適用される SD-WAN ポリシールールで設定され

たアプリケーションに対して FEC またはパケット複製がアクティブ化されます。範囲は 1 ～ 99、デフォルトは 2 です。

5. **Forward Error Correction (**前方誤り訂正**)** または **Packet Duplication (**パケット複製**)** を選択して、SD-WAN ポリシー ルールがこの SD-WAN インターフェース プロファイルを参照するときにファイアウォールが使用するエラー訂正方法を示します。デフォルトは前方誤り訂正です。パケット複製を選択した場合、SD-WAN は複製パケットを送信するためのインターフェースを選択します。(SD-WAN は、前の手順の**Eligible for Error Correction Profile interface selection (**エラー訂正プロファイル インターフェースの選択対象**)** で設定したインターフェースの 1 つを選択します）
6. (前方誤り訂正のみ) **Packet Loss Correction Ratio (**パケット損失の修正率**)** を選択します。**10% (20:2)**、**20% (20:4)**、**30% (20:6)**、**40% (20:8)**、または **50% (20:10)**–データ パケットに対するパリティ ビットの比率。デフォルトは 10% (20:2) です。送信ファイアウォール (エンコーダ) が送信するデータ パケットに対するパリティ ビットの比率が高いほど、受信ファイアウォール (デコーダ) がパケット損失を修復できる可能性が高まります。ただし、比率が上がるほど冗長性も増大するため、帯域幅のオーバーヘッドが高まります。これは、エラー訂正を実現上のトレードオフとなります。パリティの割合は、エンコーディング ファイアウォールの発信トラフィックに適用されます。例えば、ハブ ファイアウォールのパリティ比率が 50%、ブランチ ファイアウォールのパリティ比率が 20%の場合、ハブ ファイアウォールは 20%、ブランチ ファイアウォールは 50% を受け取ります。
7. **Recovery Duration (**復旧期間**) (**ミリ秒**)** の指定–受信ファイアウォール（デコーダ）が受信したパリティ パケットを使用して、損失したデータ パケットのパケット回復を実行する際の最大時間（ミリ秒）。範囲は 1～5,000、デフォルトは 1,000 です。ファイアウォールは、受信したデータ パケットを直ちに宛先に送信します。復旧期間中、デコーダは失われたデータ パケットのパケット回復を実行します。復旧期間が終了すると、すべてのパリティ パケットがリリースされます。エンコーダのエラー訂正プロファイルで復旧期間を設定します。これにより、復旧期間の値がデコーダに送信されます。デコーダの復旧期間の設定は影響しません。

   デフォルトの復旧期間設定を使用することから始め、通常および断続的な電圧低下でのテストに基づいて、必要に応じて調整を行ってください。



8. **OK** をクリックします。

STEP 5 | SD-WAN ポリシー ルールの設定、ルールで作成した **Error Correction Profile** を参照し、ルールを適用する重要なアプリケーションを指定します。

FEC またはパケットの複製を設定する場合は、*SD-WAN* ポリシー ルールで *1* つのアプリケーションのみを指定します。*FEC* またはパケットの重複に対して、複数のアプリケーションを *1* つのポリシー ルールに組み合わせないようにしてください。。

STEP 6 | **Commit (コミット)** を実行し、エンコーディング ファイアウォール (ブランチおよびハブ) への設定の変更を **Commit and Push (コミットしてプッシュ)** します。

SD-WAN ポリシー ルールの設定

SD-WAN ポリシー ルールは、アプリケーションおよび/またはサービス、またトラフィック分散プロファイルを指定し、ファイアウォールが既存のセッションに属さず、その他のすべての基準に合致する着信パケットの優先パスを選択する方法を決定します。この基準には、送信元と宛先のゾーン、送信元と宛先の IP アドレス、送信元ユーザー等があります。SD-WAN ポリシー ルールは、遅延、ジッター、およびパケット損失のしきい値のパス品質プロファイルも指定します。いずれかのしきい値の超過があると、ファイアウォールはアプリケーションおよび/またはサービスに新たなパスを選択します。

SD-WAN トラフィックの モニタリング に関しては、ハブデバイスの後ろ側から発信されたトラフィックは、ハブデバイスに入る際にハブデバイスにプッシュされる SD-WAN ポリシーに照らして評価されます。パス選択は既に決定されているため、ブランチデバイスを通過して最終的なターゲットデバイスに到達する際には、ブランチデバイスは SD-WAN ポリシーに照らしたトラフィックの評価は行いません。逆に、ブランチデバイスの後ろの送信元から発信されるトラフィックは、ハブデバイスではなく、ブランチデバイスにプッシュされる SD-WAN ポリシーに照らして評価されます。Panorama™ 管理サーバは、ハブおよびブランチ両方からログを集約します。同じトラフィックの場合、セッション エントリが2 回表示されますが、最初にトラフィックを評価した SD-WAN デバイスのみに SD-WAN の詳細が表示されます。

SD-WAN ポリシー ルールでは、ドロップまたは破損したパケットに対する許容度が低い特定の重要なアプリケーションに、前方誤り訂正 (FEC) またはパケット複製を適用できるように、エラー訂正プロファイルの参照が可能です。

SD-WAN ポリシー ルールでは、Panorama がルールをプッシュする先のデバイスも指定します。

STEP 1 | Panorama Web インターフェイスへのログイン。

STEP 2 | **Policies (ポリシー)**、 > **SD-WAN** を選択し、**Device Group (デバイス グループ)** コンテクストドロップダウンで適切なデバイス グループを選択します。

STEP 3 | SD-WAN ポリシー ルールを **Add(追加)** します。

STEP 4 | **General(全般)** タブで、わかりやすいルールの **Name (名前)** を入力します。

STEP 5 | **Source(送信元)** タブでポリシー ルールの送信元のパラメータを設定します。

1. **Source Zone (送信元ゾーン)** を追加するか、**Any (任意の)** 送信元ゾーンを選択します。
2. 1 つまたは複数の送信元アドレスを **Add (追加)** するか、external dynamic list (外部ダイナミックリスト)(EDL) あるいは **Any (任意の)** 送信元アドレスを選択します。
3. 1 人または複数の送信元ユーザーを **Add (追加)** するか、**any (任意の)** 送信元ユーザーを選択します。

STEP 6 | **Destination** (宛先) タブで、ポリシー ルールの宛先パラメータを設定します。

1. **Destination Zone** (宛先ゾーン) を **Add**(追加) するか、**Any** (任意の) 宛先ゾーンを選択します。
2. 1 つまたは複数の宛先アドレスを **Add** (追加) するか、EDL を設定するか、**Any** (任意の) 宛先アドレスを選択します。

STEP 7 | **Application/Service** (アプリケーション/サービス) タブで、SD-WAN リンク管理プロファイルをアタッチし、アプリケーションとサービスを指定します。

PAN-OS 10.0.2 は、*SaaS* 品質プロファイルまたはエラー訂正の関連付けのみをサポートしますが、両方の関連付けはサポートしません。これらのプロファイルの *1* つを *SD-WAN* ポリシー ルールに関連付ける場合、他のプロファイルを関連付けることはできません。

たとえば、*SaaS* 品質プロファイルを *SD-WAN* ポリシー ルールに関連付ける場合、エラー訂正プロファイルを同じ *SD-WAN* ポリシー ルールに関連付けることはできません。

1. **Path Quality** またはパス品質プロファイルの作成を選択します。
2. **SaaS Quality Profile** を選択するか、ブランチファイアウォールに SaaS アプリケーションへのダイレクト インターネット アクセス (DIA) リンクがある場合はSaaS 品質プロファイルの作成します。デフォルト設定は **None** (なし) です。
3. **Error Correction Profile** または エラー訂正プロファイルの作成 を選択して、SD-WAN ポリシールールに一致するアプリケーションに前方誤り訂正(FEC)またはパケット重複を適用します。デフォルト設定は **None** (なし) です。
4. **Add Applications**(アプリケーションを追加) し、リストから 1 つまたは複数のアプリケーションを選択するか、 **Any** (任意の) アプリケーションを選択します。選択したパス品質プロファイルで指定されたヘルスしきい値が、選択したアプリケーションすべてに適用されます。パケットがこのアプリケーションのいずれかに合致し、そのアプリケーションがパス品質プロファイルのヘルスしきい値のいずれかを超過する (またこの

パケットが残りのルール基準に合致する) 場合に、ファイアウォールは新しい優先パスを選択します。

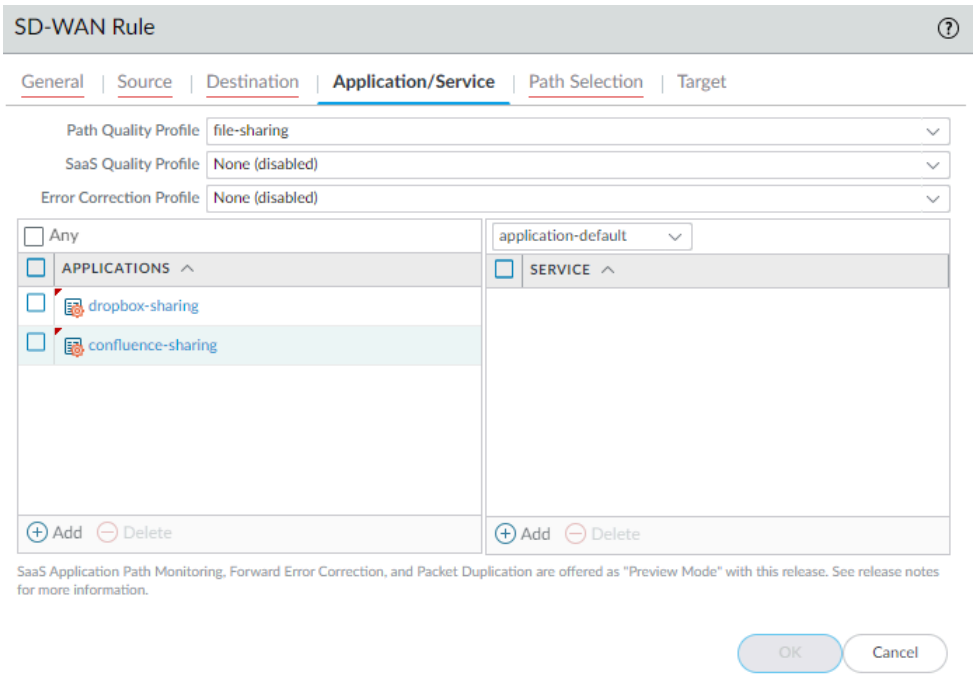
ビジネス クリティカル アプリケーションおよびユーザビリティの面でパス状況に依存するアプリケーションのみを追加します。

***Adaptive* (アダプティブ) モードの SaaS Quality profile (SaaS 品質プロファイル) を *SD-WAN* ポリシーに関連付ける場合は、監視したい特定の *SaaS* アプリケーションを追加します。*SD-WAN* ポリシー ルールに一致するすべてのアプリケーションにアダプティブ監視を使用すると、*SD-WAN* ファイアウォールのパフォーマンスに影響を与える可能性があります。**

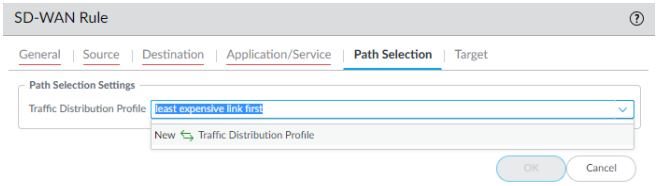
SaaS Quality profile (SaaS 品質プロファイル) を指定の *SaaS* アプリケーションと関連付ける場合は、*SaaS* アプリケーションを *SD-WAN* ルールに追加して、*SaaS* 監視設定が目的の *SaaS* アプリケーションにのみ適用されるようにします。

5. **Add Services** (サービスを追加) して、リストから 1 つまたは複数のサービスを選択するか、**Any** (任意の) サービスを選択します。選択したパス品質プロファイルで指定されたヘルスしきい値が選択したサービスすべてに適用されます。パケットがこのサービスのいずれかに合致し、そのサービスがパス品質プロファイルのヘルスしきい値のいずれかを超過する (またこのパケットが残りのルール基準に合致する) 場合に、ファイアウォールは新しい優先パスを選択します。

   ビジネス クリティカル サービスおよびユーザビリティの面でパス状況に依存するサービスのみを追加します。

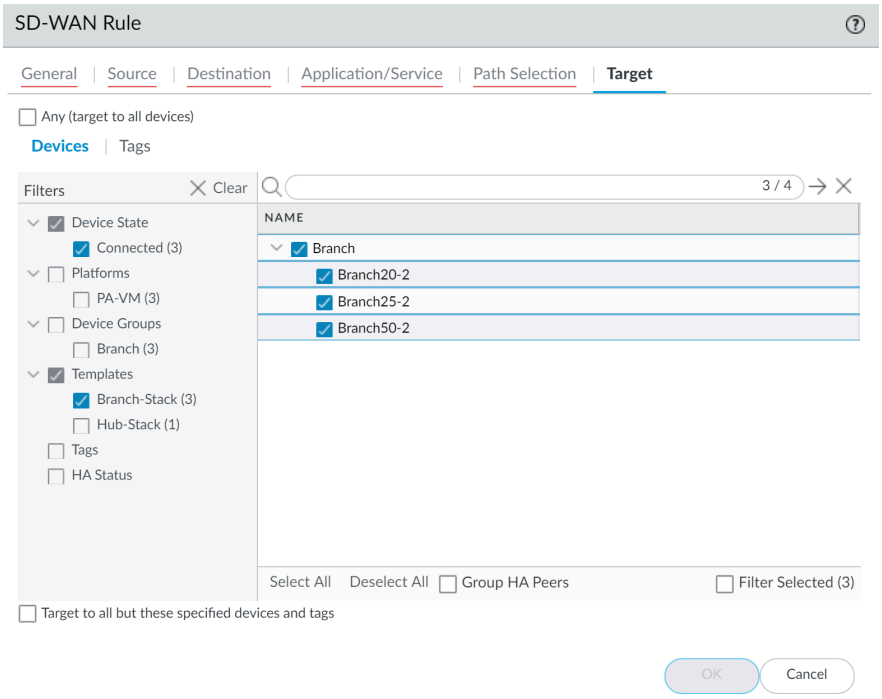


STEP 8 | **Path Selection** タブで、**Traffic Distribution** プロファイルまたはトラフィック分散プロファイルの作成を選択します。(セッションに関連付けられていない) 着信パケットがルールのすべての一致条件に合致する場合、ファイアウォールはこのトラフィック分散プロファイルを使用して、新しい優先パスを選択します。

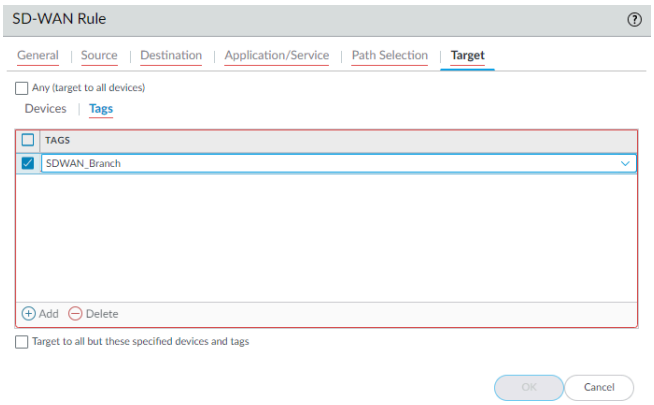


STEP 9 | **Target (**ターゲット**)** タブで、以下のいずれかの方法で、Panorama が SD-WAN ポリシー ルールをプッシュするデバイスグループ内のターゲットファイアウォールを指定します。

- ルールをすべてのデバイスにプッシュするには、**Any (target to all devices) (**任意 **(**すべてのデバイスをターゲットに設定**))** を選択します。または、**Devices(**デバイス**)** または **Tags(**タグ**)** を選択して、Panorama が SD-WAN ポリシー ルールをプッシュするデバイスを指定します。
- **Devices** タブで、1 つ以上のフィルターを選択して、[名前] フィールドに表示される選択を制限します。次に、次の例のように、Panorama がルールをプッシュする 1 つ以上のデバイスを選択します



- **Tags** タブの 1 つ以上の **Tags** の追加をクリックし、次の例のように、選択したタグでタグ付けされたデバイスに Panorama がルールをプッシュするように指定するタグを選択します



- デバイスもしくはタグを指定した場合、**Target to all but these specified devices and tags** (これらの指定されたデバイスおよびタグのみをターゲットに設定する) を選択すると、Panorama に SD-WAN ポリシー ルール を指定したデバイスまたはタグがつけられたデバイスを除くすべてのデバイスにプッシュさせることができます。

STEP 10 | **OK** をクリックします。

STEP 11 | 設定の変更を **Commit** (コミット) および**Commit and Push** (コミットしてプッシュ) します。

STEP 12 | (ベスト プラクティス)一致しないセッションが使用するリンクを制御し、SD-WAN プラグインのロギングとレポートで一致しないセッションを表示できるように、合致しないセッションの分散包含的な SD-WAN ポリシールールを作成します。

合致しないセッションを分配するキャッチオールのルールを作成しない場合は、合致しないセッション向けのトラフィック分配プロファイルがないため、ファイアウォールは使用可能なすべてのリンクにラウンドロビンで分配します。合致しないセッションをラウンドロビンで分配する場合、コストが予想外に増加し、アプリケーションの可視性が失われる恐れがあります。

STEP 13 | SD-WAN ポリシー ルールの設定後、Create a Security Policy Rule (セキュリティ ポリシー ルールを作成) して、トラフィックを (例えば、**bgp** を **Application** (アプリケーション) として) ブランチからインターネットへ、ブランチからハブへ、そしてハブからブランチへと流れることを許可します。

STEP 14 | (任意) 重要なアプリケーションに対して Configure QoS(QoS を設定) します。

SD-WAN アプリケーションが帯域幅保証を必要とする場合、あるいはその他のアプリケーションが重要なビジネスアプリケーションの帯域幅を奪わないようにする場合は、適切に帯域幅を制御する *QoS* ルールを作成します。

STEP 15 | VPN クラスタ メンバー間の BGP ルーティングを自動的に設定するには、SD-WAN プラグインで、ブランチとハブ間の Configure BGP routing (BGP ルーティングを設定) して、SD-

WAN フェイルオーバーおよび負荷分散の対象となるトラフィックを動的にルーティングします。

あるいは、BGP ルーティングを各ファイアウォールで手動で設定する場合、あるいは (制御の強化のために) 個別の Panorama テンプレートを使用してBGP ルーティングを設定する場合は、プラグインの BGP 情報は入力しません。代わりに、BGP ルーティングを設定します。

STEP 16 | パブリックの仮想 SD-WAN インターフェース向けに Configure NAT (NATを設定) します。

MPLS リンクへのダイレクト インターネット アクセスのトラフィック フェイルオーバーを許可する

SD-WAN ブランチオフィスでは、ファイアウォールがスプリット トンネリングを実行します。パブリック IP アドレスを持つアプリケーションはすべてインターネットへのダイレクト インターネット アクセス (DIA) インターフェースを使用し、ハブに属するプライベート IP アドレスを持つアプリケーションは、VPN インターフェースを使用します。必要に応じてファイアウォールが DIA アプリケーションをハブへの MPLS プライベート接続に自動的にフェイルオーバーするため、インターネット宛てのトラフィックは、インターネットへのアクセスにハブ経由での代替パスを使用します。これが機能するには、以下を実行する必要があります。

STEP 1 | ブランチとハブの間に MPLS リンクを作成します。インターフェース プロファイルを作成する際のリンク タイプは、ハブとブランチの両方で **MPLS** を指定する必要があります。

STEP 2 | プライベート トラフィックを VPN トンネルを経由させるには、**SD-WAN Interface profile (SD-WAN** インターフェース プロファイル**)** の VPN Data Tunnel Support (VPN データ トンネルのサポート) を有効にします。**VPN Data Tunnel Support (VPN** データ トンネルのサポート**)** を無効にすると、プライベート データが VPN トンネルの外に送信されてしまいます。

STEP 3 | **Top Down Priority** メソッドを指定する特定のアプリケーション、パス品質プロファイルの作成、およびトラフィック分散プロファイルの作成SD-WAN ポリシー ルールの設定。トラフィック分散プロファイルは、フェイルオーバーの (タグで識別される) オプションの 1 つとして **MPLS** リンクも指定する必要があります。SD-WAN ポリシー ルールのアプリケーションがパス品質とトラフィック分散プロファイルを正しく参照していること、およびトラフィック分散プロファイルがトップダウン優先順位を指定していることを確認します。

ハブおよびブランチの双方で VPN データ トンネルのサポートが有効となり、MPLS リンクが動作可能になると、ファイアウォールは自動的に MPLS 接続を使用し、必要に応じて DIA トラフィックをフェイルオーバーします。

STEP 4 | ハブの設定で、ハブにインターネットへのパスが存在し、ハブ トラフィックがインターネットにアクセスするためのルーティングが正しく設定されていることを確認します。

ファイアウォールは、DIA 仮想インターフェースと VPN 仮想インターフェースを使用して、パブリック インターネット トラフィックが同じパス内のプライベート トラフィックと確実に分離させます。つまり、インターネット トラフィックとプライベート トラフィックが同じ VPN トンネルを通過することはありません。適切なゾーニングによる完全なセグメンテーションが実行されます。

DIA AnyPath の設定

ISP からの SD-WAN ダイレクト インターネット アクセス (DIA; direct internet access) リンクに停電または電圧降下が発生する時は、ビジネス継続性を確保するために、これらのリンクを別のリンクにフェイルオーバーする必要があります。DIA リンクは MPLS リンクへのフェイルオーバーが可能ですが、MPLS リンクがない場合があります。DIA リンクは、インターネットへの直接パスまたは間接パス（ハブまたはブランチを介して）を持つ別のリンクにフェイルオーバーできる必要があります。DIA トラフィックは、インターネットに到達するために利用可能な任意のパスをとることができ、DIA に限定されません。DIA AnyPath は、ハブ ファイアウォールに接続してインターネットに到達するプライベート VPN トンネルにフェイルオーバーする DIA リンクをサポートします。さらに、トポロジがフルメッシュ (ブランチ間) でハブがない場合、DIA トラフィックはブランチ ファイアウォールにフェイルオーバーしてインターネットに到達する可能性があります。

DIA AnyPath には、PAN-OS 10.0.3 以降の PAN-OS リリースと、互換性マトリックスのPanorama プラグインセクションの SD-WAN テーブルに示されている互換性のある SD-WAN プラグイン リリースが必要です。

インターネットリンクをVPNトンネルにフェイルオーバーさせたい場合のいくつかの使用例があります (DIA AnyPath):

- 高価な MPLS リンクから、通常はさまざまなベンダーの 1 つ以上のパブリックインターネット接続に移行したいと考えているとします。
- VPN クラスターには複数のハブがあり、プライマリ ハブから一連のバックアップ ハブへのウォーターフォール タイプのフェイルオーバーを可能にします。
- スプリット トンネリングのシナリオでは、VPN トンネルを介してデータセンター ハブに戻る代わりに、帯域幅を大量に消費する特定のアプリケーションのみを、ブランチの DIA リンクを介してインターネットに直接接続することで、WANの帯域幅コストを節約できます。DIA のブラウンアウトまたは停電が発生した場合、このアプリケーション トラフィックは、インターネットに到達するためにデータセンター ハブにフェールオーバーします。必要に応じて、インターネットに到達するために、2番目のハブにフェールオーバーすることができます。
- 他のスプリット トンネリングのシナリオでは、インターネット ブレイクアウトのためにトラフィックをデータセンターにバックホールするのではなく、大半のインターネット トラフィックを DIA リンクから送信します。そして、特定のアプリケーション (別のセキュリティ デバイスによる追加のスキャンまたはロギングが必要になる場合があります) をデータセンターに戻すことを検討します。ファイアウォールのルート テーブルのデフォルト ルートによって決定される通常の DIA リンクではなく、SD-WAN ポリシー ルールを作成して、これらのアプリケーションをハブへのプライマリ パスに転送します。電圧低下または停電が発生した場合、これらのアプリケーションはフェイルオーバーしてブランチの DIA インターフェースを取得します。

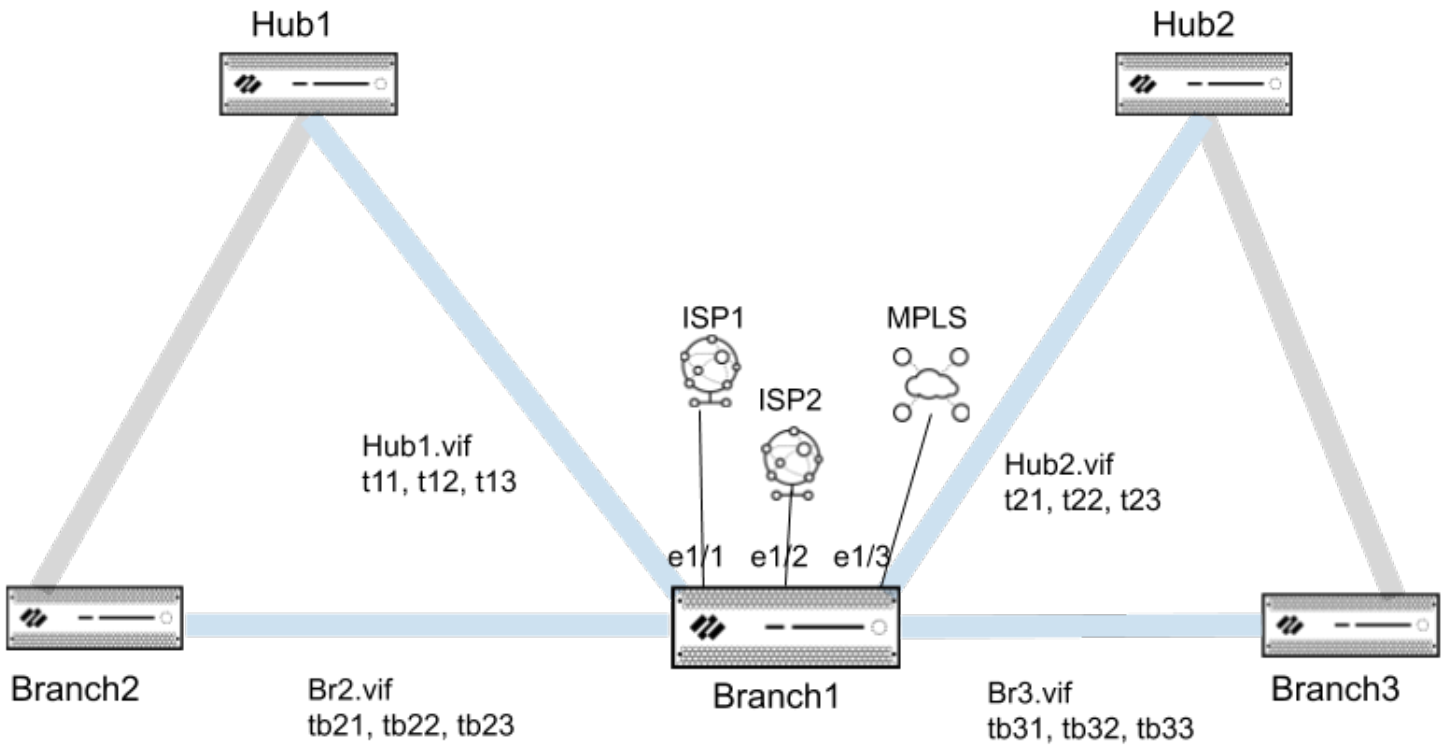
DIA AnyPath はプリンシパル仮想インターフェースのコンセプトを導入しています。これは DIA リンクとネスト型ハブ仮想インターフェースとそれぞれに独自のリンクが含まれるブランチ仮想インターフェース (VPN トンネル) の両方に追加することができます。プリンシパル仮想インターフェースには、最大 9 つの DIA (イーサネット) インターフェース、ハブ仮想インターフェイス、およびブランチ仮想インターフェースを含めることができます。ハブ デバイスを

Panorama に追加するときに、リンク タグをハブに割り当てます。SD-WAN プラグインの使用を前提に、Auto VPN はそのリンク タグをハブ仮想インターフェースに割り当てます。これにより、トラフィック分散プロファイルでタグを指定して、仮想インターフェース間のフェイルオーバー順序を制御できます。

プリンシパル仮想インターフェースは *CLI* コマンド内で *DIA-VIF* と称されます。

プリンシパル仮想インターフェイスは、異なるセキュリティ ゾーンに属するインターフェイス メンバを持つことができます。ただし、プリンシパル仮想インターフェイスのすべてのメンバ インターフェイスが同じセキュリティ ゾーンに属するようにすることをお勧めします。もう *1* つのベスト プラクティスは、リンク タイプイーサネット、ケーブル モード、*ADSL*、ファイバ、*LTE*、*WiFi* のメンバ インターフェイスを主体仮想インターフェイスに *1* つ以上設定することです。

次のトポロジの例では 2 つの ISP 接続と 1 つの MPLS リンクを持つ Branch1 を示しています。Branch1 には、Hub1 に接続する 3 つの VPN トンネルを備えた Hub1 仮想インターフェースと、Hub2 に接続する 3 つの VPN トンネルを備えた Hub2 仮想インターフェースもあります。Branch1 には、Branch2 に接続する 3 つの VPN トンネルを備えた branch2 仮想インターフェースと、Branch3 に接続する 3 つの VPN トンネルを備えた branch3 仮想インターフェースもあります。DIA AnyPath の目標は、DIA が VPN トンネルにフェイルオーバーしてインターネットに直接または間接的に到達し、ビジネス継続性を維持できる順序を選択することです。



プリンシパル仮想インターフェースを設定すると、その設定は、インターネットトラフィックがプリンシパル仮想インターフェースのメンバー (DIA リンクと VPN トンネルの両方) のいずれかに適切にルーティングされるように、自動的にデフォルトのルートとなります。パス選択は SD-WAN Path Quality プロファイルとトラフィック分配プロファイルを基準にしており、これは、フェイルオーバーの順序を制御するためにトップダウン優先度の配信方法を使用するように設定します。トポロジの例では、Traffic Distribution (トラフィックの配信) プロファイルは、最初にプリンシパル仮想インターフェースのタグ、次に Hub1仮想インターフェースのタグ、次に Hub2 仮想インターフェースのタグを一覧表示できます。

より深いレベルのフェールオーバー優先度にズームインすると、ハブ仮想インターフェイスには複数のトンネルメンバーがあるため、LTE VPNトンネルの前にブロードバンドVPNトンネルを使用することを優先するなど、メンバーのフェールオーバー順序を優先する方法が必要です。イーサネット インターフェースをに適用する SD-WAN インターフェース プロファイル内の **VPN Failover Metric (VPN** フェイルオーバー メトリック**)** を使用して優先度を指定します。メトリック値が低いほど、フェイルオーバー時に選択されるトンネルの優先度が高くなります。トポロジの例では、Hub1 仮想インターフェースで、t12 よりも t11 の VPN フェイルオーバー メトリックが低いと、インターネット トラフィックは t12 の前に t11 にフェイルオーバーします。仮想インターフェース内の複数のトンネルのメトリックが同じである場合、SD-WAN はラウンドロビン方式で新しいセッション トラフィックをトンネルに送信します。

STEP 1 | Panorama Web インターフェイスへのログイン。

STEP 2 | ハブ仮想インターフェースまたはブランチ仮想インターフェースにバンドルされている VPN トンネルのフェイルオーバー優先度を指定します。

1. 選択またはSD-WAN インターフェース プロファイルの設定。

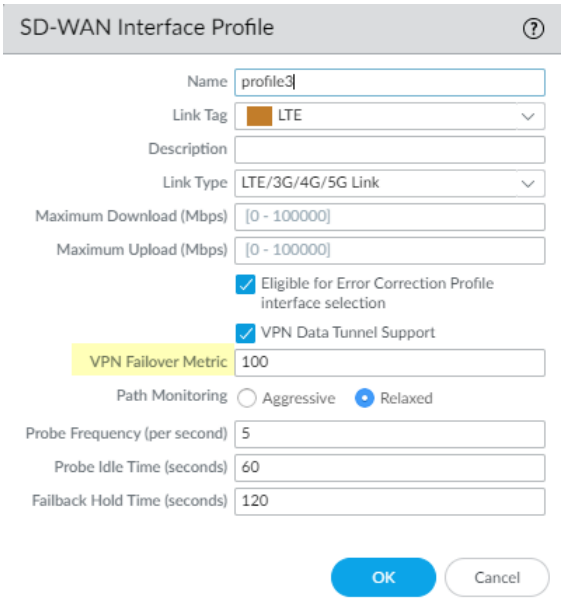
   ベスト プラクティスは、イーサネット、ケーブル モデム、*ADSL*、ファイバ、*LTE*、または *WiFi* のリンク タイプを持つインターフェイスを少なくとも *1* つ設定することです。

2. **VPN Data Tunnel Support (VPN** データ トンネルのサポート**)** を有効化する必要があります。
3. VPN トンネル用に **VPN Failover Metric (VPN** フェイルオーバー メトリック**)** を指定します。範囲は 1～65,535、デフォルトは 10 です。メトリック値が低いほど、このプロファイルを適用するリンクの VPN トンネル (リンク) 優先度は高くなります。

   例えば、メトリックを低い値に設定して、プロファイルをブロードバンド インターフェースに適用します。次に、ブロードバンドがフェイルオーバーした後にのみ使用さ

れるように、高コストの LTE インターフェースに適用させる高メトリック設定の別のプロファイルを作成します。

ハブにリンクが *1* つしかない場合、そのリンクはすべての仮想インターフェイスと *DIA* トラフィックをサポートします。特定の順序でリンクの種類を使用する場合は、トラフィック配信プロファイルを *[*上位の優先度*]* を指定するハブに適用し、*[*リンク タグ*]* に優先順序を指定する必要があります。代わりに *[*利用可能な最適パス*]* を指定するトラフィック配布プロファイルを適用すると、ファイアウォールはコストに関係なくリンクを使用して、ブランチへの最適なパスを選択します。要約すると、トラフィック配信プロファイルのリンク タグです。ハブ仮想インターフェイスに適用されるリンク タグ *(*このタスクの手順 *6)*、および *VPN* フェールオーバー メトリックは、*[*トラフィック分布*]* プロファイルで *[*上位ダウン優先順位*]* を指定した場合にのみ機能します。



4. **OK** をクリックします。

STEP 3 | SD-WAN に対応する物理イーサネット インターフェースの設定 [SD-WAN] タブで、前の手順で作成した SD-WAN インターフェイスプロファイルを適用します。

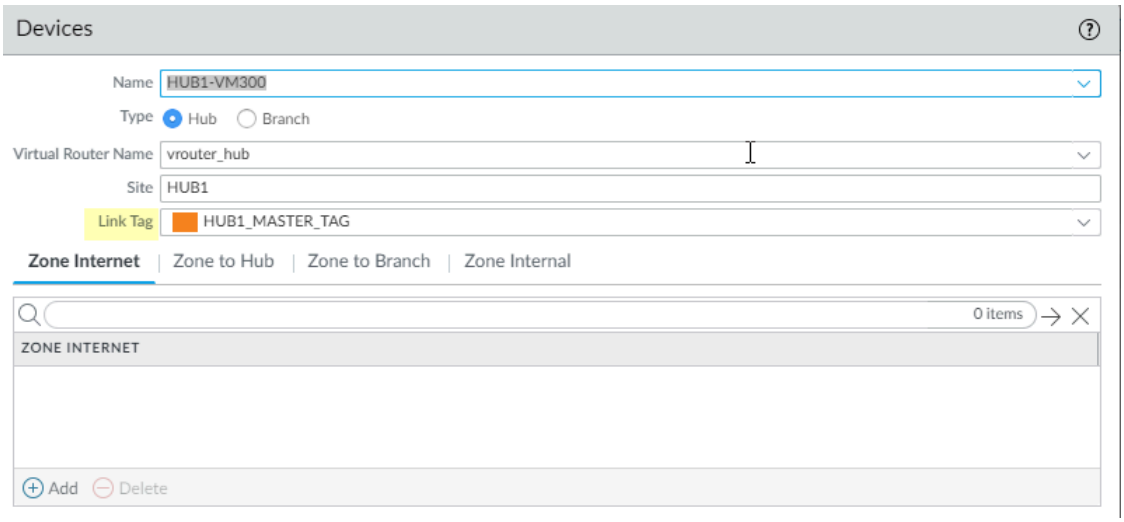
ベスト プラクティスは、プリンシパル仮想インターフェイスのすべてのインターフェイスが同じセキュリティ ゾーンに属するようにすることです。

STEP 4 | ステップ 2 と 3 を繰り返して、異なる VPN フェイルオーバー メトリックで追加の SD-WAN インターフェース プロファイルを設定し、プロファイルを異なるイーサネット インターフェースに適用して、リンクに対してフェイルオーバーが発生する順序を決定します。

STEP 5 | ハブ仮想インターフェイスのリンクタグの作成。

STEP 6 | DIA AnyPath 内に追加したいハブにリンク タグを追加します。

1. **Panorama**で > **SD-WAN** > **Devices**, SD-WAN デバイスの追加 をクリックして、パノラマで管理するハブを追加します。
2. ハブを選択します。
3. 前のステップで作成した**Link Tag (**リンク タグ**)** を選択します。これは、Auto VPN が個々のリンクではなく、ハブ仮想インターフェース全体に適用されます。したがって、トラフィック分散プロファイルでこのリンク タグを参照して、DIA AnyPathの フェイルオーバー順序のハブ仮想インターフェースを示すことができます。ブランチ デバイスでは、Auto VPN はこのタグを使用し、ハブ デバイスで終端する SD-WAN 仮想インターフェースの Link Tag（リンク タグ）フィールドにデータを入力します。



4. **OK** をクリックします。

STEP 7 | ステップ 5 と 6 を繰り返して、ハブ仮想インターフェースごとにリンク タグを作成し、DIA AnyPath に参加する各ハブにタグを追加します。ブランチ仮想インターフェースについても同様の手順を実行します。

STEP 8 | DIA AnyPath を実装するためのトラフィック分散プロファイルを作成します。

1. 「トラフィック分散プロファイルの作成」を行います。
2. **Top Down Priority (**トップダウン優先**)** を選択します。
3. リンク タグを追加して、関連付けられたリンクをフェイルオーバーに使用する順序で表示されるようにします。

   たとえば、特定のアプリケーションで最初に DIA を使用するユースケースの場合、最初に DIA タグをリストし、次にハブ仮想インターフェース タグ、さらに 2 番目のハブ仮想インターフェースタグをリストします。特定のアプリケーションが最初にハブに移動し、次にインターネットに移動する場合は、最初にハブ仮想インターフェースをリストし、次に 2 番目のハブ仮想インターフェースをリストし、最後に DIA タグをリストします。ハブのないフルメッシュがある場合は、DIA タグとブランチ仮想インターフェースタグをを目的の順序で使います。

STEP 9 | ハブ ファイアウォールとブランチ ファイアウォールの両方に対して、同じ名前のSaaS Quality profiles (SaaS 品質プロファイル) を作成します。

代替フェイルオーバーとしてハブ ファイアウォールを正常に活用するには、2 つの同じ名前の SaaS 品質プロファイルをハブ ファイアウォールとブランチ ファイアウォールに設定する必要があります。

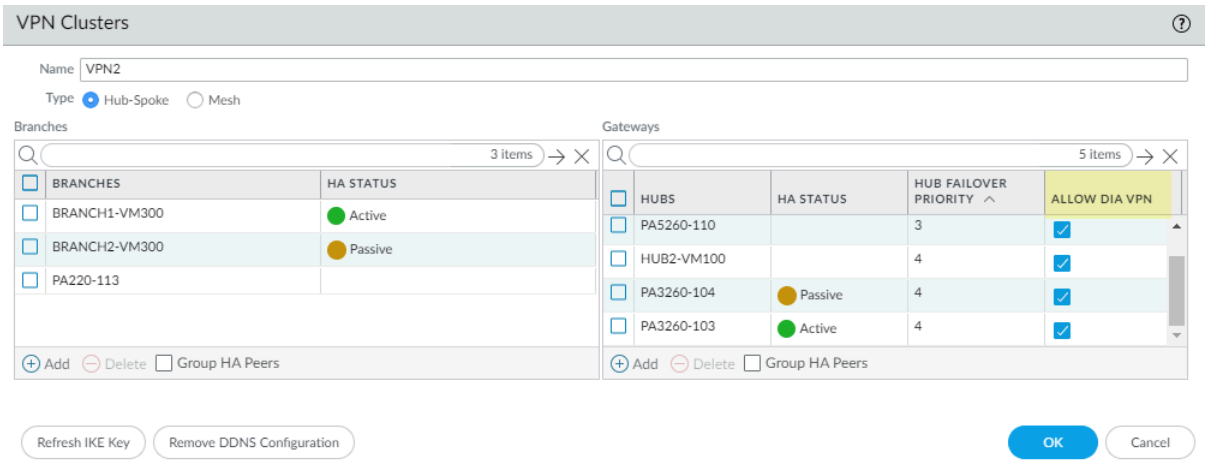
同じ SaaS アプリケーションの宛先を持つハブファイアウォールへのフェイルオーバーを設定する最も簡単な方法は、共有デバイス グループに単一の SaaS 品質プロファイルを作成することです。あるいは、異なるデバイス グループに同じ名前の 2 つの SaaS 品質プロファイルを作成し、それらをハブ ファイアウォールおよびブランチ ファイアウォールにプッシュすることもできます。

異なる SaaS アプリケーション宛先を含むハブ ファイアウォールにフェイルオーバーするためには、それぞれが異なるデバイス グループ内の異なる SaaS アプリケーションの宛先を指す同じ名前の 2 つの SaaS 品質プロファイルを作成し、それらをハブ ファイアウォールおよびブランチ ファイアウォールにプッシュします。

また、ハブが *SaaS* 品質プロファイルのリンク品質統計をブランチにアドバタイズできるようにするには、この *SaaS* 品質プロファイルを参照する *SD-WAN* ポリシールールを作成する必要があります。そうすることで、ハブを介したエンドツーエンドの *SaaS* 監視が実現します。この *SD-WAN* ポリシー ルールがなければ、ブランチからハブへのリンク測定値のみがあり、ハブから *SaaS* アプリケーションへのリンク測定値はありません。

STEP 10 | ハブが DIA AnyPth に参加することを許可します。

1. VPN クラスタの作成およびハブを選択します。
2. ハブに対して **Allow DIA VPN (DIA VPN** の許可) を選択します。最大 4 つのハブ(DIA AnyPath および Prisma Access ハブに参加している PAN-OS ハブの任意の組み合わせ)がサポートされます。HA ハブの場合、合計 8 つのハブがサポートされます。ペアの一方の HA ピアに対して **DIA VPN** を許可する場合は、もう一方の HA ピアに対しても有効にする必要があります。



STEP 11 | DIA AnyPath を使用する特定のアプリケーションの SD-WAN ポリシー ルールを作成します。

1. 「SD-WAN ポリシー ルールの設定」を行います。
2. **Application/Service (**アプリケーション/サービス**)** タブでDIA AnyPath に実装したいアプリケーションとサービスを指定します。
3. 前のステップで作成した **SaaS Quality Profile (SaaS** 品質プロファイル**)** を関連付けます。

   SaaS 品質プロファイルを他の SaaS アプリケーション宛先で設定している場合、SaaS 品質プロファイルを各ブランチおよびハブ デバイス グループの SD-WAN ポリシー ルールに関連付ける必要があります。
4. **Path Selection (**パスの選択**)** タブで、アプリケーション用に作成した **Traffic Distribution (**トラフィック分配**)** プロファイルを選択します。

STEP 12 | SD-WAN ポリシールールに一致しない新しいセッションと、Panorama またはファイアウォールの設定変更中に到着するセッションをルーティングします。

1. このようなセッションを処理するために、適切なパス品質プロファイルとトラフィック分散プロファイルを作成します。
2. SD-WAN ポリシー ルールの設定、これはこれらのセッションを包括するルールです。
3. ルールをリストの最後に配置します。

STEP 13 | **Commit (**コミット**)** および **Push to Devices(**デバイスにプッシュ**)** を実行します。

STEP 14 | Create a Security Policy Rule (セキュリティ ポリシーの追加) を実行し、DIA が `zone-internet` と `zone-to-hub` という名の **Destination Zones (**宛先ゾーン**)** をトラフィックし、**Applications (**アプリケーション**)** サブジェクトをルールに指定できるようにします。ブランチにコミットとプッシュします。

STEP 15 | DIA 情報を監視するには、次の CLI コマンドを実行します。

1. **SDWAN** 接続**<dia-vif-name>**を表示する
2. **`show sdwan path-monitor stats dia-vif all`**
3. **`show sdwan path-monitor dia-anypath`**
4. **`show sdwan path-monitor dia-anypath packet-buffer all`**
5. **`show sdwan path-monitor stats conn-idx <IDX>`**

合致しないセッションの分散

ファイアウォールは、SD-WAN 仮想インターフェースに届いたセッションを SD-WAN ポリシー ルールに合致させようとします。セキュリティ ポリシー ルールの場合と同様、ファイアウォールは SD-WAN ポリシー ルールを上から順に検査します。

- 合致するSD-WAN ルールがある場合、ファイアウォールはその SD-WAN ポリシールールのパスモニタリングおよびトラフィック分配を実行します。
- リスト内のどの SD-WAN ポリシー ルールにも合致しない場合、セッションは、リストの最後の暗黙の SD-WAN ポリシールールとの合致となり、ラウンドロビン方式で1つの SD-WAN インターフェース 内のすべてのリンク間で合致しないセッションを分配します。これは、ルート検索に基づきます。

さらに、特定のアプリケーションに SD-WAN ポリシー ルールがない場合、ファイアウォールは、SD-WAN プラグインでのロギングやレポート等の SD-WAN 独自の視覚化ツールでのそのアプリケーションのパフォーマンスは追跡しません。

暗黙のポリシー ルールの説明:

- 3 つの SD-WAN ポリシー ルールがファイアウォールにあるとします。1 つ目のルールは、5 つの音声アプリケーションを指定し、2 つ目のルールは 6 つのビデオ会議アプリケーションを指定し、3 つ目のルールは 10 の SaaS アプリケーションを指定しています。
- 例えば、ビデオ アプリケーション セッション等のセッションがファイアウォールに届き、SD-WAN ポリシー ルールのいずれにも合致しないとします。このセッションがルールに合致しないため、ファイアウォールには、セッションに適用するパス品質プロファイルまたはトラフィック分配プロファイルがありません。
- このため、ファイアウォールはビデオ アプリケーションを暗黙のルールに合致させ、使用可能なすべての SD-WAN リンクタグと、ファイアウォール上の 2 つのブロードバンド リンク、MPLS リンク、LTE リンク等の関連リンクに各ビデオ セッションを分配します。セッション 1 はブロードバンド インターフェースの 1 つのメンバーに、セッション 2 はブロードバンド インターフェースの別のメンバーに、セッション 3 は MPLS に、セッション 4 は LTE に、セッション 5 はブロードバンド インターフェースの最初のメンバーに、セッション 6 はブロードバンド インターフェースの 2 番目のメンバーに渡され、ラウンドロビン方式の分散が続きます。

セッションの分配が制御できないため、合致しないセッションを暗黙の SD-WAN ルールに合致させることを使用者が望まない場合もあります。この場合は、代わりに、キャッチオールの SD-WAN ポリシー ルールを作成し、SD-WAN ポリシー ルールのリストの最後に配置することが推奨されます。キャッチオールSD-WAN ポリシー ルールでは、以下が可能です:

- 合致しないセッションが使用するリンクの制御。
- SD-WAN プラグインのログとレポートでの、ファイアウォール上のすべてのアプリケーション (合致しないアプリケーションセッションを含む) の表示。

STEP 1 | Panorama Web インターフェイスへのログイン。

STEP 2 | パス品質プロファイルの作成、非常に高い遅延、ジッター、およびパケット損失のしきい値を設定し、決して超えることはありません。例えば、2,000 ミリ秒の遅延、1,000 ミリ秒のジッター、そして 99%のパケット損失とします。

STEP 3 | トラフィック分散プロファイルの作成、使用する SD-WAN リンクタグを、それらのリンクタグに関連付けられたリンクが一致しないセッションで使用される順序で指定します。

合致しないアプリケーションに特定のパス (物理インターフェース) を全く使用させない場合は、トラフィック分配プロファイルのリンクタグのリストから、そのリンクを含むタグを除外します。例えば、動画ストリーミング等の合致しないアプリケーションでコスト高の *LTE* リンクを使用させない場合は、トラフィック分配プロファイルのリンクタグのリストから *LTE* リンクのリンクタグを除外します。

STEP 4 | キャッチオールの SD-WAN policy rule (SD-WAN ポリシー ルール) を **Add** (追加) し、**Application/Service** (アプリケーション / サービス) タブで、作成した **Path Quality Profile** (パス品質プロファイル) を指定します。

STEP 5 | **Applications**(アプリケーション)および **Service** (サービス) は、**Any** (すべて) を選択します。

STEP 6 | **Path Selection** (パスの選択) タブで、作成した **Traffic Distribution** (トラフィック分配) プロファイルを選択します。

STEP 7 | SD-WAN ポリシー ルールのリストをの最後の位置に **Move** (移動) します。

STEP 8 | 設定の変更を **Commit** (コミット) および**Commit and Push** (コミットしてプッシュ) します。

STEP 9 | 変更を **Commit** (コミット)します。

Panorama への SD-WAN デバイスの追加

単一のSD-WANハブまたはブランチファイアウォールを追加するか、CSVを使用して、複数のSD-WANハブおよびブランチファイアウォールを事前共有キーまたは証明書認証タイプで一括インポートします。

- SD-WANデバイスの証明書ベース認証の設定
- SD-WAN デバイスの追加
- 複数の SD-WAN デバイスの一括インポート
- オンボードPAN-OS ファイアウォールからPrisma Accessへ

SD-WANデバイスの証明書ベース認証の設定

どこで使用できますか?	何が必要ですか?
• PAN-OS • SD-WAN	❑ SD-WAN plugin license

次の 2 つの認証タイプのいずれかを使用して SD-WAN デバイスを認証できます。

- 事前共有鍵（デフォルトの認証タイプ）
- 証明書 (SD-WAN プラグイン 3.2.0 以降のリリース)

新しい SD-WAN クラスターを作成するか、3.2.0 より前のバージョンの SD-WAN プラグインを使用してキーを更新すると、SD-WAN プラグインによって事前共有鍵が自動的に生成されます。事前共有鍵認証タイプに加えて、次世代ファイアウォール向けの SD-WAN プラグイン 3.2.0 以降のリリースでは、セキュリティ ニーズを満たす証明書ベースの認証も提供しています。証明書ベースの認証を使用してすべての SD-WAN サイトの認証と検証を強化し、セキュリティを次のレベルに引き上げます。

当社は、SD-WAN をサポートするレガシーまたは高度なルーティング エンジンを実行するすべてのソフトウェアおよびハードウェア デバイスで証明書ベースの認証をサポートしています。

現在の SD-WAN プラグインをアップグレードまたはダウングレードする前に、「Upgrade and Downgrade Considerations (アップグレードとダウングレードの考慮事項)」 に記載されている手順に従ってください。

SD-WAN デバイスの証明書ベースの認証を構成するには、次のワークフローを使用します。

STEP 1 | Panorama Web インターフェイスへのログイン。

STEP 2 | Panorama 上の SD-WAN デバイスの証明書を生成します。

1. **[Panorama] > [Certificate Management (**証明書管理**)] > [Certificates (**証明書**)]**を順に選択します。
2. 自己署名ルート CA 証明書を作成するかエンタープライズ CA から証明書をインポートします。ルート CA に基づいて、SD-WAN デバイスの デバイス証明書を生成します。SCEPで生成された証明書はサポートしていません。

   生成された証明書は、SD-WANデバイスごとに一意である必要があります。つまり、証明書を生成して複数の SD-WAN デバイス間で共有することはできません。

   SD-WAN トンネル認証に使用されるブランチおよびハブのファイアウォール証明書を生成するときは、次の点に注意してください。

   - 2つの異なるハブデバイスが同じハブ証明書を使用できます。
   - 次の条件を満たす場合、2つの異なるブランチデバイスが同じブランチ証明書を使用できます。
     - ブランチ デバイスは同じ VPN クラスターの一部ではありません。
     - これらのブランチ デバイスが属する VPN クラスター間には共通のハブ デバイスがありません。
   - (HA 展開のみ) 2 つの異なるブランチ デバイスが HA メンバーとして構成されている場合は、同じブランチ証明書を持つこともできます。
   - ハブデバイスがVPNクラスタ間で共通である場合、これらのVPNクラスタの一部のブランチデバイスの証明書は、すべての属性が一意の値を持つ一意の証明書を持つ必要があります。証明書とその値の一意性を確保しないと、ハブデバイスでコミットに失敗します(Panoramaではコミットに失敗します)。

   また、*SD-WAN*トンネル認証に使用されるリーフ証明書（ブランチおよびハブファイアウォール証明書）が、次の基準を満たして生成されることを確認してください。

   - キーの使用にはデジタル署名が必要です。
   - すべての証明書は同じルート *CA* によって署名されている必要があり
   - 。デバイス証明書はルート *CA* によって直接署名されている必要があります。
   - 証明書形式は*PKCS12*とします

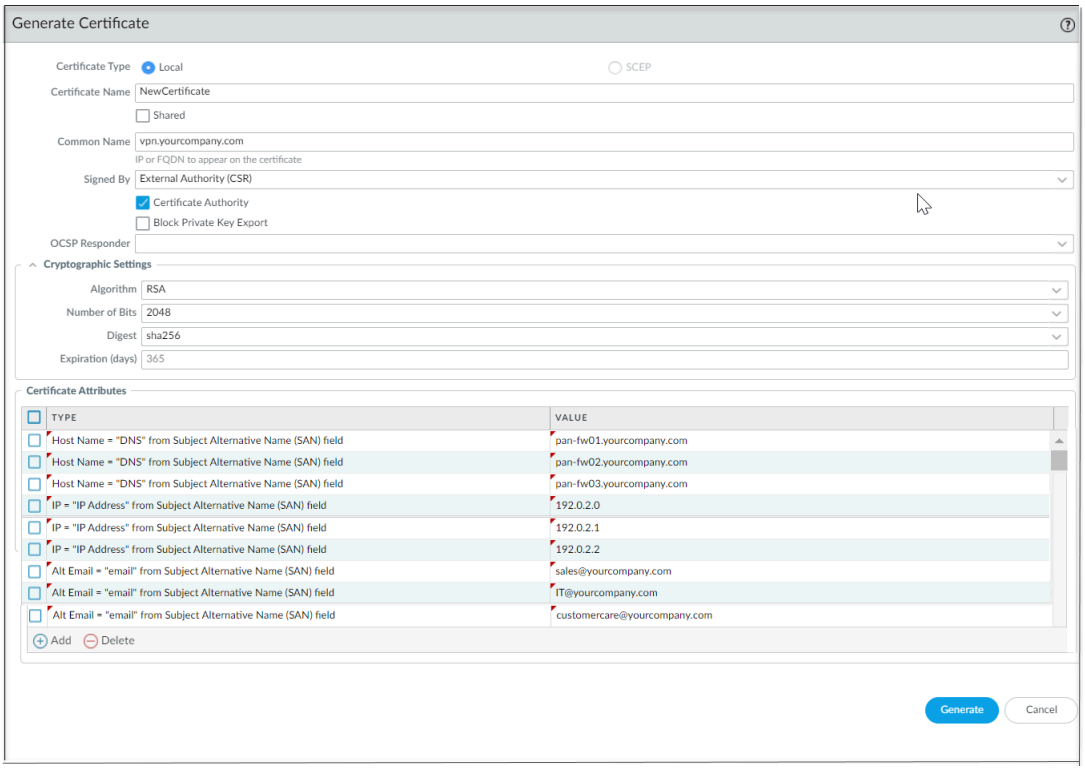
   証明書属性は、IKE ゲートウェイのローカル ID とピア ID を決定するために使用されます。したがって、リーフ証明書、つまりSD-WANトンネル認証に使用されるブランチおよびハブファイアウォール証明書は、以下の3つの証明書属性で生成し、各証明書

属性に3つの一意の属性値を割り当てる必要があります。そうでない場合、コミットエラーがスローされます。

- FQDN (ホスト名)
- IPアドレス (**IP**)
- ユーザーFQDN (代替メールアドレス)

すべての証明書間で、 ホスト名、***IP***、 代替メールの証明書属性が一意であることが必須です。つまり、どの証明書にもこれらの属性値が共通であってはなりません。

以下の例では、合計 9 つの必須証明書属性を持つ NewCertificate が生成されます。ホスト名証明書属性には、pan-fw01.yourcompany.com、pan-fw02.yourcompany.com、pan-fw03.yourcompany.comの3つの一意の属性値が設定されます。属性付きの**IP**証明書は、次の3つの固有の属性値で設定されます。192.0.2.0、192.0.2.1および192.0.2.2.代替電子メール証明書属性には、sales@yourcompany.com、IT@yourcompany.com、customercare@yourcompany.comの3つの固有の属性値が設定されます。



STEP 3 | (任意)セキュア サーバー通信用のルート CA および中間 CA が含まれる証明書プロファイルを設定します。

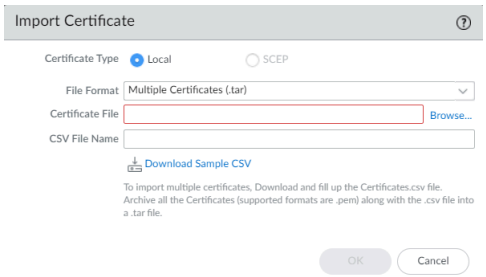
1. **[Panorama]** > **[**証明書管理 **(Certificate Management)]** > **[**証明書プロファイル **(Certificate Profile)]**を順に選択します。
2. 証明書プロファイルの設定を行います。

   証明書プロファイルの一部として中間 CA を設定する場合、ルート CA も含める必要があります。

   この証明書プロファイルは、SD-WAN ハブとブランチが相互に認証する方法を定義します。

STEP 4 | CA 証明書をインポートして、SD-WAN デバイスの ID を検証します。

1. **Panorama** > 証明書の管理 > 証明書
2. クラスタ内の各 SD-WAN デバイスのCA 証明書とキー ペアを Panorama にインポートする か、 複数の証明書 **(.tar)**を使用して複数の証明書をインポートします。CSVを使用して証明書をPanorama管理サーバーに一括インポートします。CSV を使用すると、各証明書を手動で追加するのではなく、複数の証明書を一度にインポートできます。



3. 変更を **Commit (**コミット**)** します。インポートした証明書をさらに構成できるようにするには、証明書をインポートした後にコミットすることが重要です。

STEP 5 | Panorama 管理サーバーによって管理される SD-WAN ハブまたはブランチ ファイアウォールを追加するときに、証明書ベースの認証タイプを構成します。デバイスを追加するときは、デバイスの種類 (ブランチまたはハブ) とデバイスの認証タイプを指定し、各デバイスにサイト名を付けて簡単に識別できるようにします。

1. **[Panorama]** > **[SD-WAN]** > **[Devices (**デバイス**)]**を順に選択し、 Panorama 管理サーバーによって管理される SD-WANデバイス(SD-WAN ハブまたはブランチファイアウォール) を追加します。
2. **VPN** トンネル タブを選択し、 認証 タイプを構成します。証明書ベースの認証の場合は、**[Certificate (**証明書**)]** を選択し、証明書関連のフィールドを構成します。SD-WAN デバイスを追加する際には、認証タイプを選択することが必須です。

STEP 6 | PAN-OS ファイアウォールを Prisma Access にオンボードするときに、証明書ベースの認証を構成します。

1. **[Panorama]** > **[SD-WAN]** > **[Devices (**デバイス**)]** を順に選択して、SD-WAN ブランチ ファイアウォールを選択し、Prisma Access ハブに接続して接続を構成します。
2. **[Prisma Access Onboarding (Prisma Access**オンボーディング**)]** を選択し、コンピューティング ノードを **[Region (**リージョン**)]**に 追加します 。**VPN** トンネルでは、CN

(Prisma Access ハブ) を認証するための認証タイプを選択することが必須です。証明書ベースの認証の場合は、 **[Authentication (認証)]** タイプとして **[Certificate (証明書)]** を選択し、証明書関連のフィールドを構成します。PAN-OS ファイアウォールを Prisma Access にオンボードする際には、認証タイプを選択することが必須です。

すべてのブランチ デバイスと追加される *Prisma Access* ハブに対して同じ認証タイプを選択していることを確認します。ブランチと *Prisma* ハブに異なる認証タイプを使用しようとすると、*Panorama* でコミット エラーが発生します。

STEP 7 | VPN クラスターを作成するときに、証明書ベースの認証を構成します。

1. **[Panorama]** > **[SD-WAN]** > **[VPN Clusters (VPN クラスター)]**を順に選択します。
2. VPN クラスタの **Type (タイプ)** を選択します。
3. **[Authentication Type (認証タイプ)]** として **[Certificate (証明書)]**を選択します。VPN クラスターにデバイスを追加するには、認証タイプを指定することが必須です。VPN クラスターでは、すべてのデバイスに対して同じ認証タイプを選択する必要があります。すでに VPN クラスターに追加されている SD-WAN デバイスの認証タイプを変更することはできません。変更する場合は、VPN クラスターとその SD-WAN デバイスを削除し、選択した認証タイプで再度構成します。デフォルトでは、VPN クラスター内のデバイスに対して事前共有鍵認証タイプがサポートされます (証明書タイプを手動で選択していない場合)。

STEP 8 | 設定の変更を **Commit (コミット)** します。

STEP 9 | **Push to Devices (デバイスにプッシュ)** を選択して、設定の変更を管理対象ファイアウォールにプッシュします。

SD-WAN デバイスの追加

Panorama ™ 管理サーバーが管理する SD-WAN ハブまたはブランチ ファイアウォールを追加します。デバイスを追加する際、デバイスの種類 (ブランチまたはハブ) を指定して、容易に識別できるように各デバイスにサイト名を付けます。デバイスを追加する前に、SD-WAN 設定計画 を策定し、必要な IP アドレスがすべてあること、SD-WAN トポロジが確実に把握されていることを確認します。これにより、設定エラーを低減することができます。

2 台のブランチ ファイアウォールあるいは *2* 台のハブファイアウォールで *Active/Passive HA*を稼働させる場合は、この時点ではそのファイアウォールを *SD-WAN* デバイスとして追加しないでください。SD-WAN 対応 HA デバイスの設定時に *HA* ピアとして個別に追加します。

BGP ルーティングを使用している場合は、内部ゾーンからハブゾーンへ、そしてハブゾーンから内部ゾーンへの *BGP* を許可するセキュリティ ポリシー ルールを追加する必要があります。*4 byte (バイト)*の *AS* 番号を使用する場合は、まず *Virtual Router (仮想ルーター - VR)* に対して *4 byte (バイト)*の *ASN* を有効にする必要があります。

SD-WAN デバイスを表示しているときに、データが存在しない場合、または *SD-WAN* が未定義であることを示す画面が表示されている場合は、互換性マトリックス使用しているパノラマリリースは、使用しようとしている*SD-WAN*プラグインリリースをサポートしています。

STEP 1 | Panorama Web インターフェイスへのログイン。

STEP 2 | **[Panorama]** > **[SD-WAN]** > **[Devices (デバイス)]** を順に選択し、新しい SD-WAN ファイアウォールを **Add**追加 します。

STEP 3 | SD-WAN デバイスとして追加する管理ファイアウォールの **Name (名前)**を選択します。SD-WAN デバイスとして追加する前に、SD-WAN ファイアウォールを管理対象デバイスとして追加する 必要があります。

STEP 4 | SD-WAN デバイスの**Type (タイプ)**を選択します。

- ハブ-すべてのブランチデバイスが VPN 接続を使用して接続するプライマリオフィスまたは場所に配置された集中型ファイアウォール。ブランチ間のトラフィックはハブを通過してから対象ブランチに進み、ブランチをハブの場所にある集中リソースに接続します。ハブデバイスは、トラフィックを処理し、ポリシー ルールを適用し、プライマリオフィスまたは場所でのリンクスワッピングを管理します。
- ブランチ- VPN 接続を使用してハブを接続し、ブランチレベルでセキュリティを提供する物理的なブランチの場所に配置されたファイアウォール。ブランチデバイスは、トラフィックを処理し、ポリシー ルールを適用し、ブランチロケーションでのリンクスワッピングを管理します。

STEP 5 | （任意） （PAN-OS 11.1.3以降のリリース、およびSD-WANプラグイン3.2.1以降のリリース）SD-WANハブに複数の仮想ルーターを設定します。

［**Enable Multi-VR Support (複数の仮想ルーターを有効)**］を選択すると、SD-WANハブに複数の仮想ルータを設定できます。

SD-WANハブの複数の仮想ルータのサポートを導入し、同じSD-WANハブに接続するブランチデバイスでIPサブネットアドレスを重複させることができます。［SD-WANの種類］を［ハブ］として選択すると 、 ［ **Enable Multi-VR Support (複数のVRサポートを有効にする)**］オプションを選択して複数の仮想ルーターを設定できるようになります。

STEP 6 | SD-WAN ハブとブランチ間のルーティングに使用する ルーター名 を選択します。デフォルトでは、`sdwan-default` （sdwan-デフォルト） Virtual Router (仮想ルーター - VR) が作成され、Panorama によるルーター設定の自動プッシュが可能となります。

(高度なルーティング が有効な場合) 高度なルーティングを構成し、論理ルーターが正常に作成された場合、ルータ名 は仮想ルーター名と論理ルーター名の両方を表示します。

- 仮想ルータ名と論理ルータ名が同じ場合、［**Router Name (ルーター名)**］ には同じ名前が表示されます。これは、拡張ルーティングによって仮想ルータと同じ名前の論理ルータがデフォルトで作成されるためです。高度なルーティングエンジンを使用する場合は、論理ルーター名と仮想ルーター名が同じテンプレートで同一であることが重要です。
- 仮想ルータ名と論理ルータ名が異なる場合(論理ルータ名を手動で更新した場合にのみ発生します)、ルータ名には仮想ルータ名と論理ルータ名の両方が表示されます。要件に基づい

て、仮想ルーター (レガシー エンジンの場合) または論理ルーター (高度なルーティング エンジンの場合) のいずれかを選択できます。高度なルーティング を有効にしていない場合は、ルータ名 (レガシー エンジン用) から選択できる仮想ルーターのみがあります。

（PAN-OS 11.1.3以降のリリース、およびSD-WANプラグイン3.2.1以降のリリース） 複数の仮想ルーター（**Enable Multi-VR Support (**複数の**VR**サポートを有効**)**）が有効になっている場合 、 ［仮想ルーター名］に［DIA仮想ルーター］を選択します。

STEP 7 | SD-WAN **Site(**サイト**)**名を入力して、デバイスの地理的な場所または目的を識別できるようにします。

SD-WAN サイト名は、大文字と小文字のすべての英数字と特殊文字が使用できます。スペースはサイト名でサポートされていないため、そのサイトのモニタリング *(**Panorama** >* モニタリング*)* データは表示されません。

高可用性 *(HA)* 構成の *SD-WAN* デバイスを含むすべての *SD-WAN* デバイスには、一意のサイト名が必要です。

STEP 8 | 自動 VPN が仮想インターフェイスに割り当てるハブ仮想インターフェイス(またはブランチ仮想インターフェイス)用に作成した リンク タグ を選択します。トラフィック分散プロファイルでこのリンク タグを使用して、ハブ (またはブランチ) がDIA AnyPath に参加できるようにします。

STEP 9 | ハブに対して NAT を実行するデバイスの後方にハブを追加する場合は、自動 VPN 設定がそのアドレスをハブのトンネルエンドポイントとして使用できるように、アップストリーム NAT を実行するデバイスでパブリック側のインターフェースの IP アドレスまたは FQDN を指定します。この IP アドレスには、ブランチオフィスの IKE および IP Sec フローが到達可能である必要があります。(既に SD-WAN に対応する物理イーサーネットインターフェースが設定されている必要があります。)

1. **Upstream NAT (**アップストリーム **NAT)** タブで、**Upstream NAT (**アップストリーム **NAT)**を有効にします。
2. **SD-WAN interface (SD-WAN** インターフェース**)**を **Add(**追加**)** します。既に設定した SD-WAN 対応インターフェースを選択します。
3. **IP Address([IP** アドレス**)** または **FQDN** を選択し、サブネットマスクなしの IP v4 アドレス (例えば、192.168.3.4) あるいはアップストリームデバイスの FQDN をそれぞれ入力します。

4. **OK** をクリックします。

   また、*NAT* を実行するアップストリーム デバイスで *1* 対 *1* の *NAT* ポリシーで*Destination NAT (*宛先 *NAT - DNAT)* をセットアップする必要があります。*IKE* または*IP Sec* トラフィックフローへのポート変換は設定してはいけません。

   アップストリームデバイスの *IP* アドレスが変更された場合、新しい *IP* アドレスを再設定して、*VPN* クラスタにプッシュする必要があります。ブランチとハブの両方で、*CLI* コマンド ***clear ipsec-sa***、***clear vpn ike-sa***、***clear session all***を使用します。また、*IP* アドレスの *NAT* ポリシーを設定した *Virtual Router (* 仮想ルーター - *VR)* でも、***clear session all(***すべてのセッションをクリア***)*** を実行します。

   アップストリーム *NAT* はレイヤ *2* インターフェイスではサポートされていません。

STEP 10 | (新規デプロイメント時のみ）ブランチの NAT を実行するデバイスの背後にあるブランチを追加する場合は、そのアップストリーム NAT 実行デバイスの公開インターフェイスの IP アドレスまたは FQDN を指定するか、[DDNS] を選択して、NAT デバイスのインターフェイスの IP アドレスが Palo Alto Networks DDNS サービスから取得されることを示す必要があります。したがって、自動 VPN 設定は、そのパブリック IP アドレスをブランチのトンネル エンドポイントとして使用します。この IP アドレスには、ブランチオフィスの IKE および IP Sec フローが到達可能である必要があります。(既に SD-WAN に対応する物理イーサーネットインターフェースが設定されている必要があります。)

1. **Upstream NAT (**アップストリーム **NAT)** タブで、**Upstream NAT (**アップストリーム **NAT)**を有効にします。
2. **SD-WAN interface (SD-WAN** インターフェース)を **Add(**追加**)** します。既に設定した SD-WAN 対応インターフェースを選択します。
3. **NAT IP Address Type (NAT IP** アドレス タイプ**)** を **Static IP (**静的 **IP)** を使用する場合は、**IP Address (IP** アドレス**)** または **FQDN** を選択し、サブネットマスクなしの IP v4 アドレス (例えば、192.168.3.4) あるいはアップストリームデバイスの FQDN をそれぞれ入力します。
4. あるいは、**NAT IP Address Type (NAT IP** アドレス タイプ**)** を **DDNS** を選択します。

5. **OK** をクリックします。

   また、*NAT* を実行するアップストリーム デバイスで *1* 対 *1* の *NAT* ポリシーで*Destination NAT (*宛先 *NAT - DNAT)* をセットアップする必要があります。*IKE* または*IP Sec* トラフィックフローへのポート変換は設定してはいけません。

   アップストリームデバイスの *IP* アドレスが変更された場合、新しい *IP* アドレスを再設定して、*VPN* クラスタにプッシュする必要があります。ブランチとハブの両方で、*CLI* コマンド ***clear ipsec(***クリア ***ispec)***、***clear ike-sa(***クリア ***ike-sa)***、***clear session all (***すべてのセッションをクリア*)*を使用します。また、*IP* アドレスの *NAT* ポリシーを設定した *Virtual Router (* 仮想ルーター - *VR)* でも、***clear session all(***すべてのセッションをクリア***)*** を実行します。

   *Web*インターフェース には、ブランチのアップストリーム *NAT* を設定できる *2* 番目の場所がありますが、次の場所は推奨されないため、両方の場所でブランチのアップストリーム *NAT* を設定しないでください。アップストリーム *NAT* を設定するためのセカンダリの非優先ロケーションは *Panorama* の***Network (***ネットワーク***) > Interfaces (***インターフェース***) > Ethernet (***イーサネット***)*** にあります。 ***Template (***テンプレート***)*** フィールドでテンプレートを選択し、イーサネット インターフェースを選択し、***SD-WAN*** タブを選択します。この時点でアップストリーム *NAT* を、***Enable (***有効化***)*** し、***NAT IP Address Type (NAT IP*** アドレス タイプ***)*** を選択できます。この *2* 番目の方法が優先されます。テンプレートスタックを介して *Panorama* 上のイーサネット インターフェースにアップストリーム *NAT* が最初に設定されている場合、プラグイン デバイス設定ページで別の設定を使用しても、*SD-WAN* プラグインは設定を変更しません。テンプレートスタックを介して *Panorama* にアップストリーム *NAT* が設定されていない場合にのみ、アップストリーム *NAT* のプラグイン設定が有効になります。

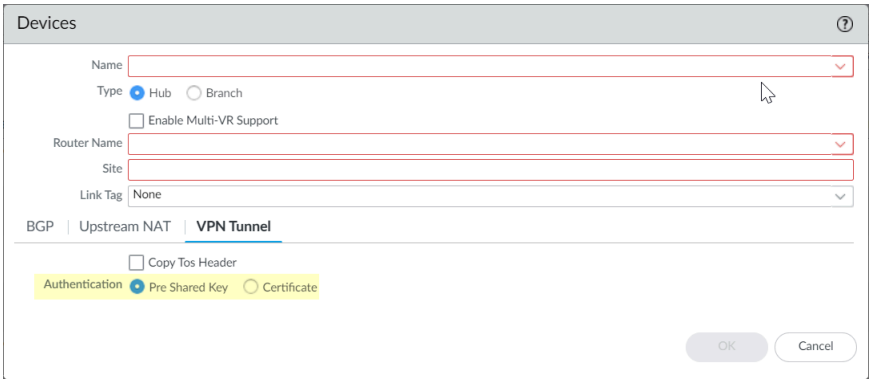
   アップストリーム *NAT* はレイヤ *2* インターフェイスではサポートされていません。

STEP 11 | アプリケーション トラフィックがタイプ オブ サービス(ToS)ビットまたは Differentiated Services Code Point (DSCP) マーキングでタグ付けされている場合は、QoS 情報を保持するために、VPN トンネルを通過するカプセル化されたパケットの内部 IPv4 ヘッダーから外部 VPN ヘッダーに ToS フィールドをコピーします。

1. **VPN Tunnel** タブを選択します。
2. **Copy ToS Header** を選択します。
3. **OK** をクリックします。

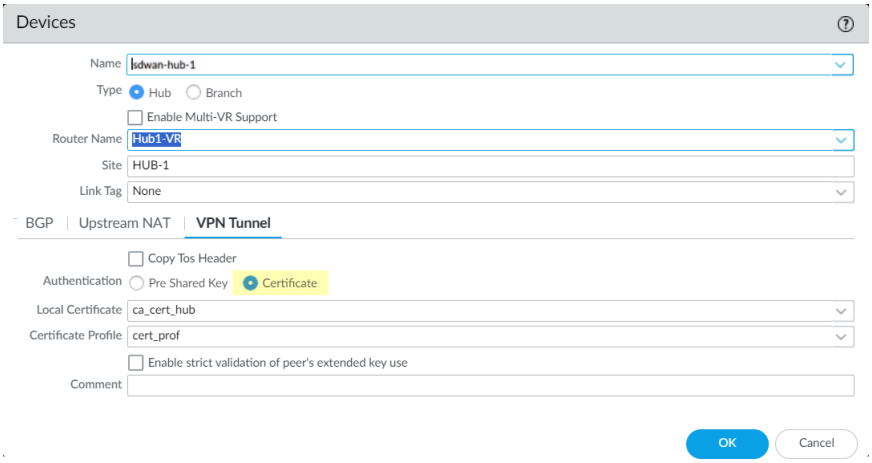
STEP 12 | （必須）（SD-WANプラグイン3.2.0以降）ピアの認証方法を指定します。

認証タイプを選択してください**[Pre-Shared Key (事前共有鍵)]** あるいは**[Certificate (証明書)]** です。事前共有鍵を選択すると、事前共有鍵が自動的に生成されます。



- *SD-WAN*クラスタ内のデバイスごとに固有の証明書を使用する必要があります。
- *VPN*クラスタに*SD-WAN*デバイスを追加した後は、認証タイプを変更することはできません。
- *(HA*デプロイメントのみ*)Panorama*で高可用性*(HA)*ペアを設定している場合は、アクティブファイアウォールとパッシブファイアウォールの両方で同じ証明書を使用する必要があります。*RMA*プロセス中に、アクティブなファイアウォールと同じ証明書で代替ファイアウォールを設定する必要があります。アクティブファイアウォールの証明書が無効になり、新しい証明書がプッシュされた場合、パッシブファイアウォールも新しい証明書で更新する必要があります。つまり、高可用性構成では、アクティブファイアウォールとパッシブファイアウォールの両方に同じ証明書が設定されている必要があります。

STEP 13 | （証明書認証タイプをイネーブルにする場合のみ）証明書ベースの認証を設定します。



1. すでにPanoramaにある **Local Certificate (**ローカル証明書**)** を選択するか、証明書を **Import (**インポート**)** するか、新しい証明書を **Generate (**生成**)** します。

   - 証明書を **Import (**インポート**)** する必要がある場合は、はじめに IKEv2 ゲートウェイ認証の証明書のインポート を行ってから、このタスクに戻ってください。SCEPで生成された証明書はサポートしていません。
   - 新しい証明書を **Generate**（生成）する場合は、はじめにPanoramaでの証明書の生成を行ってから、このタスクに戻ります。生成された証明書は、SD-WANデバイスごとに一意である必要があります。つまり、証明書を生成して複数のSD-WANデバイス間で共有することはできません。

     SD-WANトンネル認証に使用されるブランチおよびハブファイアウォール証明書を生成する際には、次の点に注意してください。

     - 2つの異なるハブデバイスが同じハブ証明書を使用できます。
     - 次の条件を満たす場合、2つの異なるブランチデバイスが同じブランチ証明書を使用できます。
       - ブランチ デバイスは、同じ VPN クラスタの一部ではありません。
       - これらのブランチ デバイスが属する VPN クラスタ間に共通のハブ デバイスはありません。
     - （HAデプロイメントのみ）2 つの異なるブランチ デバイスが HA メンバーとして設定されている場合は、同じブランチ証明書を持つこともできます。
     - ハブデバイスがVPNクラスタ間で共通である場合、これらのVPNクラスタの一部のブランチデバイスの証明書は、すべての属性が一意の値を持つ一意の証明書を

持つ必要があります。証明書とその値の一意性を確保しないと、ハブデバイスでコミットに失敗します(Panoramaではコミットに失敗します)。

また、*SD-WAN*トンネル認証に使用されるリーフ証明書（ブランチおよびハブファイアウォール証明書）が、次の基準を満たして生成されることを確認してください。

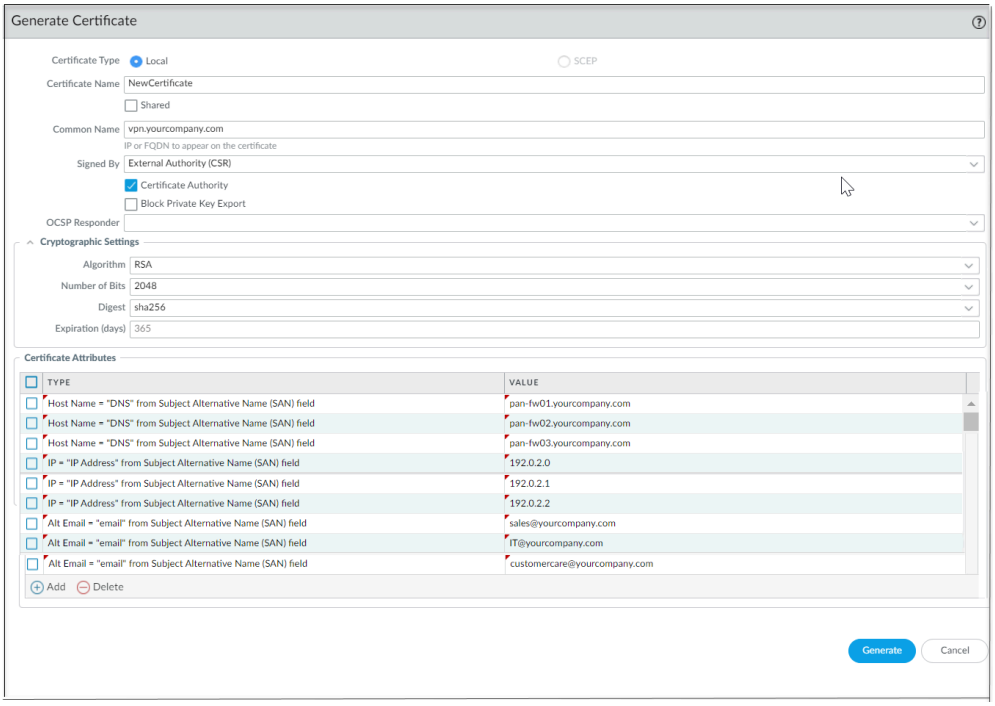
- キーの使用にはデジタル署名が必要です。
- すべての証明書は、同じルート*CA*によって署名されている必要があります。
- デバイス証明書は、ルート*CA*によって直接署名されている必要があります。
- 証明書形式は*PKCS12*とします。

- 証明書アトリビュートは、IKE ゲートウェイのローカル ID およびピア ID を決定するために使用されます。したがって、リーフ証明書、つまりSD-WANトンネル認証に使用されるブランチおよびハブファイアウォール証明書は、以下の3つの証明書属性で生成し、各証明書属性に3つの一意の属性値を割り当てる必要があります。そうでない場合、コミットエラーがスローされます。
  - FQDN（ホスト名）I
  - Pアドレス（**IP**）
  - ユーザーFQDN（代替電子メール）

  すべての証明書の中で一意の ホスト名、***IP***、 代替電子メール 証明書属性を持つことが必須です。つまり、どの証明書にも共通してこれらの属性値を持つことはできません。

  次の例では、NewCertificateは合計9つの必須証明書属性を使用して生成されます。ホスト名証明書属性には、pan-fw01.yourcompany.com、pan-fw02.yourcompany.com、pan-fw03.yourcompany.comの3つの一意の属性値が設定されます。属性付きの**IP**証明書は、次の3つの固有の属性値で設定されます。192.0.2.0、192.0.2.1および192.0.2.2.代替電子メール証明書属性に

は、sales@yourcompany.com、IT@yourcompany.com、customercare@yourcompany.comの3つの固有の属性値が設定されます。



2. (任意)証明書プロファイルを選択します。証明書プロファイルには、ピア ゲートウェイの認証方法に関する情報が含まれています。
3. （任意）鍵の使用方法を厳密に制御する場合は、**Enable strict validation of peer's extended key use**（ピアの拡張鍵使用の厳密な検証を有効にする）をクリックします。

STEP 14 | （任意）BGP ルーティングを設定します。

BGP ルーティングを VPN クラスタ メンバー間で自動的に設定するには、以下の BGP 情報を入力します。BGP ルーティングを各ファイアウォールで手動で設定する場合、あるいは制御

の強化に向けて個別の Panorama テンプレートを使用して BGP ルーティングを設定する場合は、以下の BGP 情報は入力しません。

BGP がすでに使用されている環境で *BGP* ルーティングを使用して *SD-WAN* を実装する前に、*SD-WAN* プラグインによって生成された *BGP* 設定が既存の *BGP* 設定と競合していないことを確認してください。たとえば、既存の *BGP AS* 番号とルータ *ID* 値を、対応する *SD-WAN* デバイス値に使用する必要があります。プラグインによって生成された *BGP* 設定が既存の *BGP* 設定と競合する場合は、既存の *BGP* 設定が優先されます。プッシュされた構成を優先する場合は、パノラマプッシュを実行するときに強制テンプレート値を有効にする必要があります。

1. **BGP** タブを選択し、**BGP** を有効にして、SD-WAN トラフィックの BGP ルーティングを設定します。
2. BGP の **Router ID (**ルーター**ID)**を入力します。この ID は、全ルーターで一意である必要があります。
3. **AS** 番号を入力します。autonomous system number(自律システム番号(AS 番号))は、一般的に定義されたインターネットへのルーティングポリシーを指定します。AS 番号は、ハブとブランチの場所毎で一意である必要があります。

STEP 15 | IPv4を使用するようにBGPを設定するには、**IPv4 BGP**を選択します。BGP環境がIPv4のみの場合も、デュアルスタック（IPv4とIPv6）の場合も、IPv4 BGPを有効にする必要があります。

1. **IPv4 BGP** サポートの有効化.

   アップグレードされた構成（既存の*SD-WAN IPv4*構成）では、デフォルトで［***Enable IPv4 BGP support (IPv4 BGP***サポートを有効にする**)***］が選択されています。それ以外の場合は、明示的に ***IPv4 BGP*** サポートを有効にします。

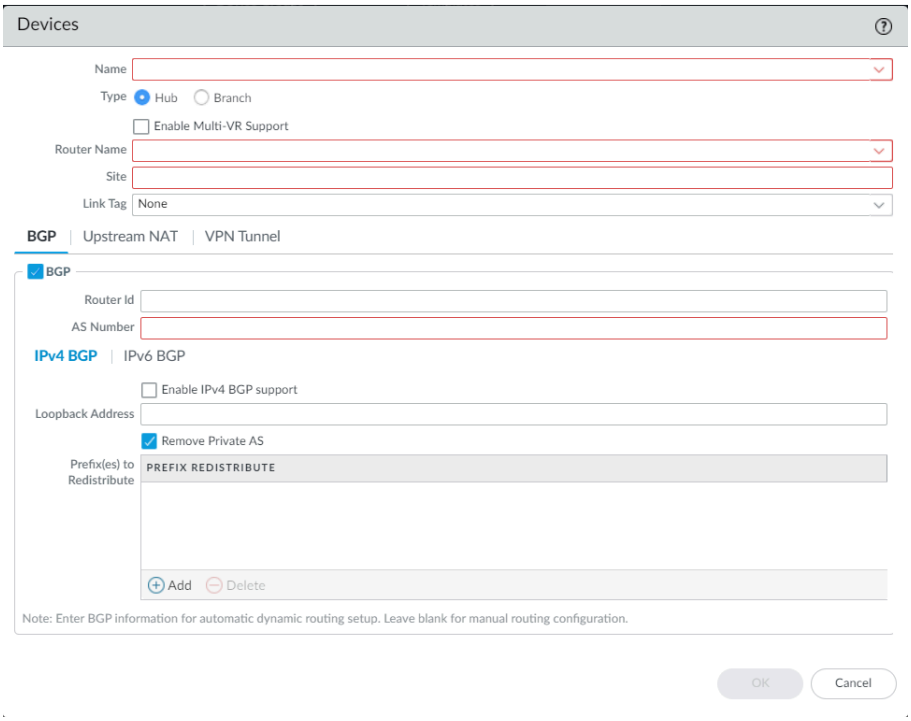
2. BGP ピアリングのスタティック IPv4 **Loopback Address (**ループバック アドレス**)** を指定します。自動 VPN 設定では、指定した IP v4 アドレスと同じループバックインターフェースが自動的に作成されます。既存のループバックアドレスを指定すると、コミットは正常に完了しません。既にループバックアドレスに使用されていない IP v4 アドレスを指定する必要があります。
3. SD-WAN BGP トポロジでハブまたはブランチ ファイアウォールとルートを交換する必要があるエンドポイントがあり、BGP アップデートのAS_PATH属性からプライベート AS 番号(64512 ~ 65534)を削除しないエンドポイントがある場合は、プライベート AS

の削除オプション(デフォルトは有効)を無効にします。この場合、プライベート AS 番号が BGP アップデートの SD-WAN プライベート AS から残ることを許可します。

プライベート ***AS*** の削除設定は、ブランチまたはハブ ファイアウォール上のすべての *BGP* ピア グループに適用されます。*BGP* ピア グループまたはピア間でこの設定を異なる場合は、*SD-WAN* プラグインの外部で設定を構成する必要があります。

プライベート ***AS*** の削除設定を変更し、すべての *SD-WAN* クラスタ ノードにコミットし、その後 *2.0.2* より前の *SD-WAN* プラグイン バージョンにダウングレードする場合は、プライベート ***AS*** に関連するすべての設定を *SD-WAN* プラグインの外部またはファイアウォールで直接行う必要があります。

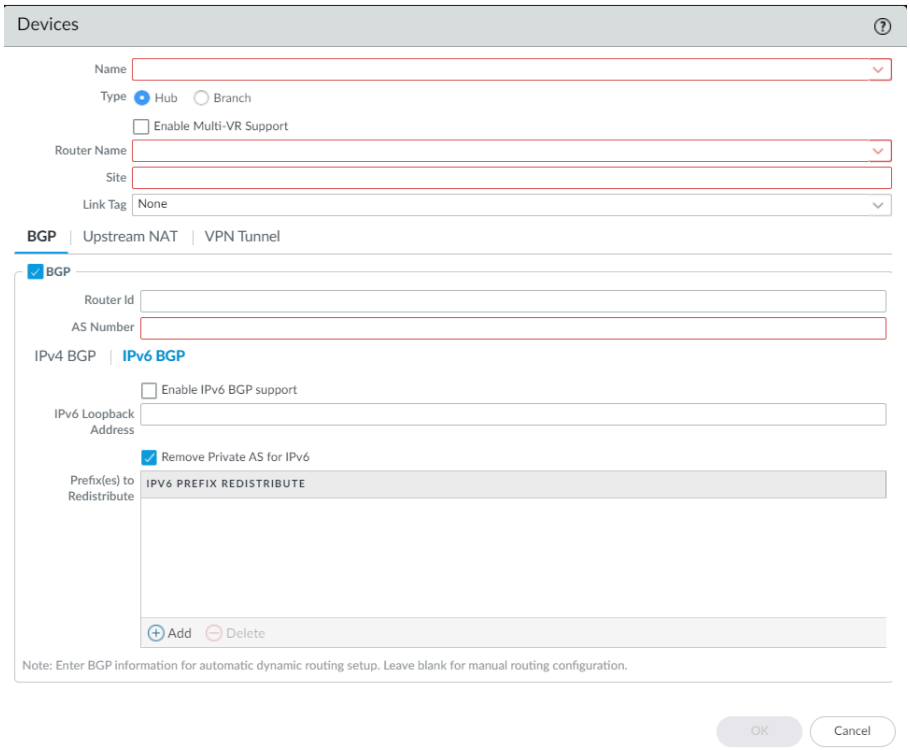
4. 再配信用プレフィックスの追加。ハブデバイスでは、SD-WANトンネル経由で再配信するために少なくとも1つのプレフィックスを入力する必要があります。ブランチ デバイスでは、ブランチ ロケーションに接続されたサブネットがデフォルトで再配布されるため、この必須の設定要件はありません。



STEP 16 | IPv6を使用するようにBGPを設定するには、**IPv6 BGP**を選択します。

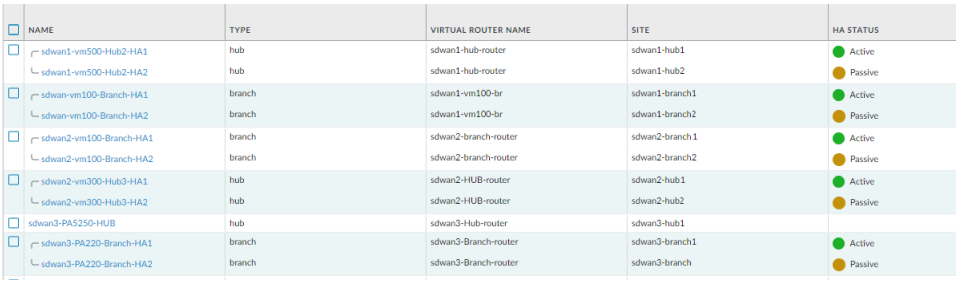
1. **IPv6 BGP** サポートの有効化.
2. BGP ピアリングの静的 **IPv6** ループバック アドレス を指定します。自動 VPN 設定では、指定したのと同じ IPv6 アドレスを持つループバック インターフェイスが自動的に作成されます。既存のループバックアドレスを指定するとコミットが失敗するため、まだループバックアドレスではない IPv6 アドレスを指定する必要があります。
3. SD-WANトンネル経由で再配布するプレフィックスを追加します。ハブデバイスでは、SD-WANトンネル経由で再配信するために少なくとも1つのプレフィックスを入力

する必要があります。ブランチ デバイスでは、ブランチ ロケーションに接続されたサブネットがデフォルトで再配布されるため、この必須の設定要件はありません。



STEP 17 | **OK** をクリックします。

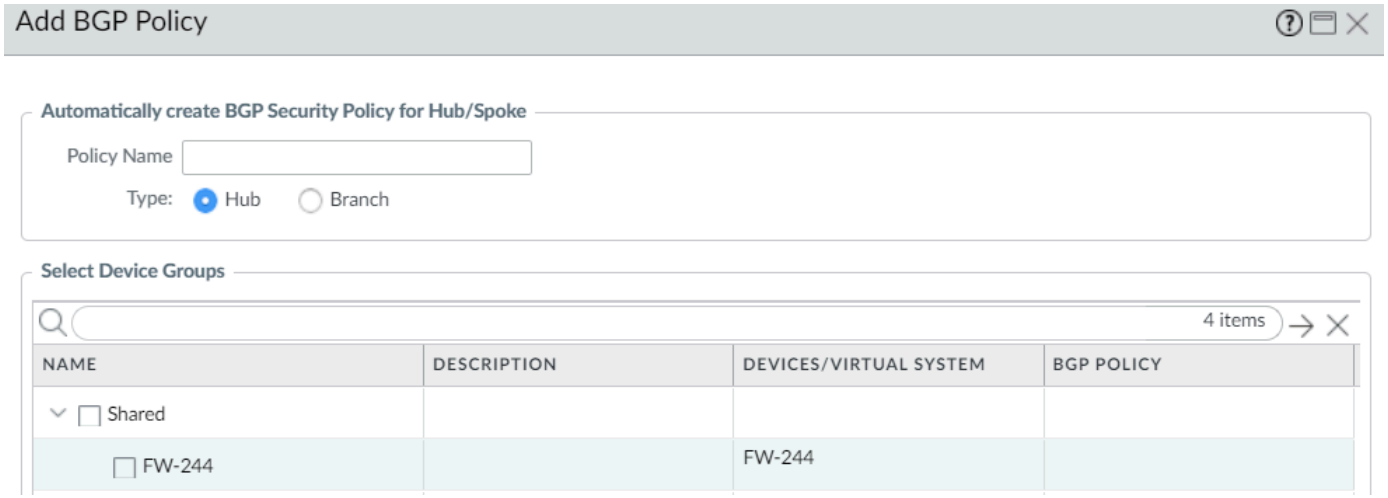
STEP 18 | 画面の下部にある **Group HA Peers (HA** ピアのグループ化**)** を選択して、HA ピアであるブランチ (あるいはハブ) を共に表示します。



NAME	TYPE	VIRTUAL ROUTER NAME	SITE	HA STATUS
sdwan1-vm500-Hub2-HA1	hub	sdwan1-hub-router	sdwan1-hub1	Active
sdwan1-vm500-Hub2-HA2	hub	sdwan1-hub-router	sdwan1-hub2	Passive
sdwan-vm100-Branch-HA1	branch	sdwan1-vm100-br	sdwan1-branch1	Active
sdwan-vm100-Branch-HA2	branch	sdwan1-vm100-br	sdwan1-branch2	Passive
sdwan2-vm100-Branch-HA1	branch	sdwan2-branch-router	sdwan2-branch 1	Active
sdwan2-vm100-Branch-HA2	branch	sdwan2-branch-router	sdwan2-branch2	Passive
sdwan2-vm300-Hub3-HA1	hub	sdwan2-HUB-router	sdwan2-hub1	Active
sdwan2-vm300-Hub3-HA2	hub	sdwan2-HUB-router	sdwan2-hub2	Passive
sdwan3-PA5250-HUB	hub	sdwan3-Hub-router	sdwan3-hub1	
sdwan3-PA220-Branch-HA1	branch	sdwan3-Branch-router	sdwan3-branch1	Active
sdwan3-PA220-Branch-HA2	branch	sdwan3-Branch-router	sdwan3-branch	Passive

STEP 19 | Panorama で、BGP がブランチとハブの間で実行できるセキュリティ ポリシー ルールを作成し、ファイアウォールにプッシュします。

1. 画面下部の[**IPv4 BGP**ポリシー]または[**IPv6 BGP**ポリシー]を選択し、ポリシールールを追加します。
2. Panorama が自動的に作成するセキュリティ ポリシー ルールの **Policy Name (**ポリシー名**)** を入力します。
3. **Type** を **Hub** または **Branch** として選択します。
4. **Select Device Groups (**デバイス グループを選択**)** して、Panorama がセキュリティ ポリシー ルールをプッシュするデバイス グループを指定します。
5. **OK** をクリックします。



STEP 20 | **Push to Devices (**デバイスにプッシュ**)** を選択して、設定の変更を管理対象ファイアウォールにプッシュします。

複数の SD-WAN デバイスの一括インポート

各デバイスを 1 台ずつ手動で追加するのではなく、複数の SD-WAN デバイスを追加して、ブランチとハブのファイアウォールを即座にオンボーディングします。デバイスを追加する際、デバイスの種類 (ブランチまたはハブ) を指定して、容易に識別できるように各デバイスにサイト名を付けます。デバイスを追加する前に、 SD-WAN構成を計画するうえで必要なすべての IP アドレスがあり、SD-WAN トポロジを理解していることを確認します。これが、設定 エラーの低減につながります。

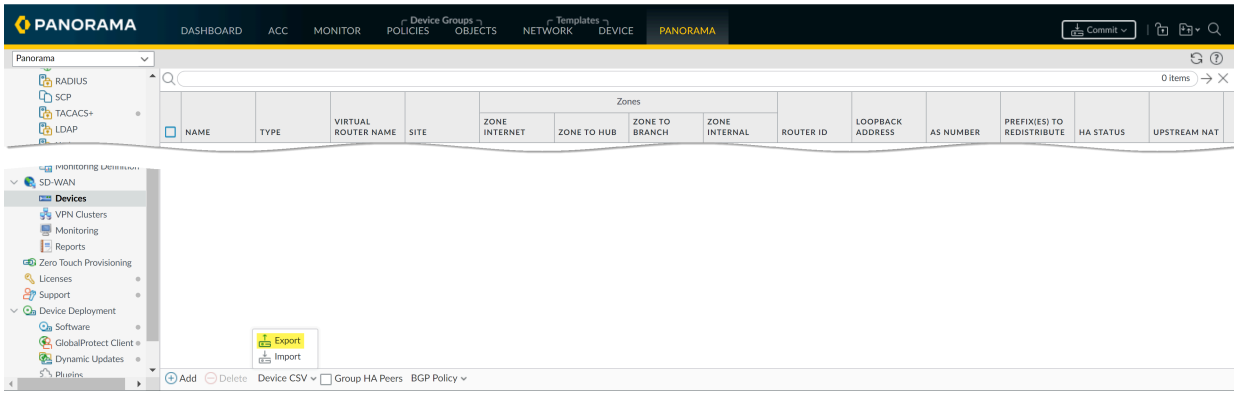
2 台のブランチ ファイアウォールあるいは *2* 台のハブファイアウォールで アクティブ/パッシブ *HA*を稼働させる場合は、そのファイアウォールを *CSV* ファイルで *SD-WAN* デバイスとして追加しないでください。SD-WAN 対応 HA デバイスの設定時に *HA* ピアとして個別に追加します。

BGP ルーティングを使用している場合は、内部ゾーンからハブゾーンへ、そしてハブゾーンから内部ゾーンへの *BGP* を許可するセキュリティ ポリシー ルールを追加する必要があります。*4-byte* (バイト)の 自律システム番号*(autonomous system numbers (ASN))*を使用する場合は、まず *Virtual Router* (仮想ルーター - *VR*) に対して *4-byte* (バイト)の *ASN* を有効にする必要があります。

Palo Alto Networks ファイアウォール用の既存のゾーンがある場合、SD-WAN で使用される事前定義済みのゾーンにマッピングします。

STEP 1 | Panorama Web インターフェイスへのログイン。

STEP 2 | **Panorama**、 > **SD-WAN** 、 > **Devices(**デバイス**)**、 > **Device CSV (**デバイス **CSV)** を選択し、空のSD-WAN デバイス CSV を **Export(**エクスポート**)** します。CSV を使用すると、それぞれのデバイスを手動で追加せずに、複数のブランチ デバイスおよびハブ デバイスを一度にインポートできます。



STEP 3 | SD-WAN デバイス CSV にブランチとハブの情報を入力して、CSV を保存します。特に明記されていない限り、すべてのフィールドへの入力が必須です。ハブとブランチごとに次のように入力します。

- **device-serial (**デバイス シリアル**):** ブランチまたはハブのファイアウォールのシリアル番号。
- **type (**タイプ**)**-デバイスが **`branch`** **(**ブランチ**)** であるか、あるいは **hub(**ハブ**)** であるかを指定します。
- **site SD-WAN** -デバイスのサイト名を入力して、デバイスの地理的な場所や目的を識別できるようにします。

  SD-WAN サイト名は、大文字と小文字のすべての英数字と特殊文字が使用できます。サイト名では空白文字は使用できません。空白文字を使用すると、そのサイトのモニタリング *(**Panorama** > **SD-WAN** > **Monitoring(**モニタリング**)**)* モニタリング データが表示されません。

  高可用性 *(HA)* 構成の *SD-WAN* デバイスを含むすべての *SD-WAN* デバイスには、一意のサイト名が必要です。
- **vr-name (VR**名**)**- SD-WAN ハブとブランチ間のルーティングに使用する Virtual Router (仮想ルーター - VR) を入力します。デフォルトでは、**sdwan-default (sdwan-**デフォルト**)**

Virtual Router (仮想ルーター - VR) がPanoramaによって作成され、Panorama によるルーター設定の自動プッシュが可能となります。

- **vif-link-tag (vif**リンクタグ**)**- リンクタグを指定して、SD-WANトラフィックの分散およびフェイルオーバー中にアプリケーションやサービスがこのリンクを使用するときにハブを識別します。
- (任意) **router-id (**ルーター**ID)**- BGP ルーター ID を指定します。ルーターID は、すべての Virtual Router (仮想ルーター - VR) と論理ルーター全体で一意である必要があります。

  ルーター *ID* としてループバック アドレスを入力します。

  BGP が既に使用されている環境で *BGP* ルーティングを使用して *SD-WAN* を実装する前に、*SD-WAN* プラグインによって生成された *BGP* 設定が既存の *BGP* 設定と競合していないことを確認します。たとえば、既存の *BGP AS* 番号とルータ *ID* 値を、対応する *SD-WAN* デバイス値に使用する必要があります。
- (任意) **as-number**-ハブまたはブランチの Virtual Router (仮想ルーター - VR) が属するプライベート AS の ASN を入力します。SD-WAN プラグインは、プライベートの自律システムのみをサポートします。ASNは、全ハブおよびブランチで一意である必要があります。4-byte (バイト) の ASNの範囲は、4,200,000,000 から 4,294,967,294、あるいは、64512.64512 から 65535.65534 までです。2-byte (バイト) の ASNの範囲は、64512 から 65534 までです。

  *4-byte (*バイト*)* のプライベート *ASN*を使用します。

  BGP が既に使用されている環境で *BGP* ルーティングを使用して *SD-WAN* を実装する前に、*SD-WAN* プラグインによって生成された *BGP* 設定が既存の *BGP* 設定と競合していないことを確認します。たとえば、既存の *BGP AS* 番号とルータ *ID* 値を、対応する *SD-WAN* デバイス値に使用する必要があります。
- (任意) **ipv4-bgp-enable (IPv4-BGP**を有効にする**)** – IPv4 アドレスの BGP を有効または無効にするには、[yes]または[no]を指定します。
- (任意) **loopback-address (**ループバック アドレス**)** - Border Gateway Protocol (ボーダ ゲートウェイ プロトコル -BGP) ピアリングのスタティック ループバック IPv4 アドレスを指定します。SD-WAN プラグイン 3.1.1 以降の 3.1 リリースでは、BGP ピアリング用の IPv6 ループバックアドレスがサポートされています。
- (任意) **remove-private-as (**としてプライベートを消去**)** – SD-WAN BGPトポロジーでハブまたはブランチファイアウォールとルートを交換する必要があるエンドポイントがあり、BGP UpdatesのAS_PATH属性からプライベートAS番号（64512～65534）を削除したくない場合は、[no]を指定してプライベートASの削除オプションを無効にします（デフォルトは有効）。

  この設定は、ブランチまたはハブ ファイアウォール上のすべての BGP ピア グループに適用されます。BGP ピア グループまたはピア間でこの設定を異なる場合は、SD-WAN プラグインの外部で設定を構成する必要があります。
- (任意) **prefix-redistribute(**プレフィックスの再配信**)**- ブランチがアクセスできるハブにブランチが通知する IP プレフィックスを入力します。複数のプレフィックスを追加する場合

は、プレフィックスを空白文字、アンパサンド (&)、そして空白文字で区切ります。例えば、192.2.10.0/24 & 192.168.40.0/24 と入力します。デフォルトでは、ブランチ ファイアウォールはローカルに接続されたすべてのインターネット プレフィックスをハブにアドバタイズします。

Palo Alto Networks では、*ISP* から取得したブランチ オフィスのデフォルト ルートは再配信しません。

- (任意) **ipv6-bgp-enable (IPv6-BGPを有効にする)** – IPv6 アドレスの BGP を有効/無効にするには、yes/no を指定します。
- (任意) **ipv6-loopback-address (IPv6ループバックアドレス)** – BGP ピアリングのスタティック ループバック IPv6 アドレスを指定します。
- (任意) **ipv6-prefix-redistribute (IPv6 プレフィックスの再配布)**–ブランチからハブ ルータに再配布する IPv6 プレフィックスを入力します。デフォルトでは、ローカルに接続されるすべてのインターネットIPv6プレフィックスがハブの場所にアドバタイズされます。
- (任意) **copy-tos-header (TOSヘッダーのコピー)** – 元のTOS情報を保持するために、カプセル化されたパケットの内側のIPヘッダーから外側のIPヘッダーにTOS（Type of Service）ヘッダーをコピーするこのオプションを有効/無効にするには、yes/noを指定します。
- **authentication-type (認証タイプ)**–デバイス(ハブまたはブランチ)がサポートする認証タイプ(事前共有キーまたは証明書認証)を指定します。
- (証明書 認証の種類のみ) **certificate-name (証明書名)** - 証明書名を入力します。名前は大文字小文字を区別し、ファイアウォールでは最大 63 文字、Panorama では最大 31 文字を使用できます。英字、数字、ハイフン、およびアンダースコアのみを使用し、一意である必要があります。

  事前共有鍵認証の種類の場合、このフィールドは空のままにする必要があります。

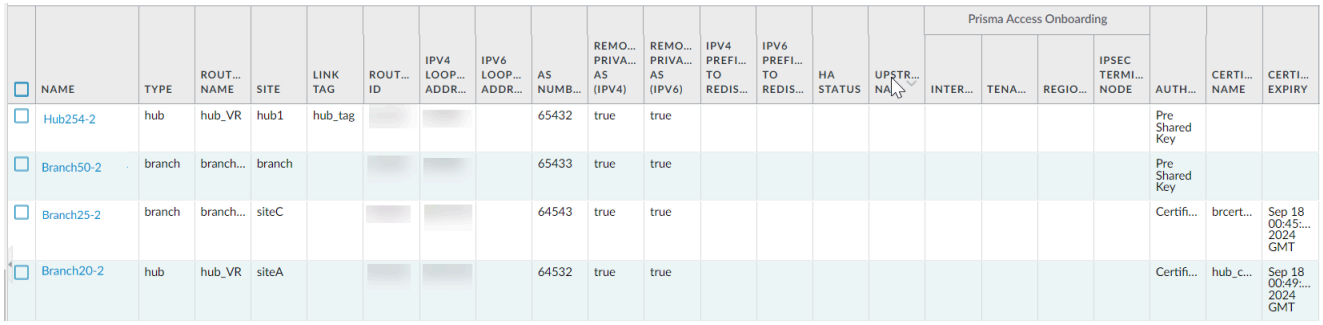
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
1	device-serial	type	site	router-name	vif-link-tag	router-id	as-number	ipv4-bgp-enable	loopback-addres	remove-private-a	prefix-redistribut	ipv6-bgp-enable	ipv6-loopback-a	ipv6-prefix-redist	copy-tos-he	authentication-ty	certificate-name
2		hub	hub1	hub_VR			65520			yes						pre-shared-key	
3		branch	branch	branch_VR			65501			yes						pre-shared-key	
4		branch	siteC	branch_VR			65502			yes						certificate	brcert1_cacert
5		hub	siteA	hub_VR			65525			yes						certificate	hub_cacert
6																	

STEP 4 | SD-WAN デバイス CSV を Panorama にインポートします。

Panorama で保留中のコミットがないことを確認します。そうでなければ、インポート エラーが発生します。

1. Panoramaで、**Panorama** 、 > **SD-WAN** 、 > **Devices (デバイス)**、 > **Device CSV(デバイス CSV)** を選択し、前のステップで編集した CSV を **Import (インポート)** します。
2. **Browse (参照)** して、SD-WAN デバイス CSV を選択します。
3. **OK** をクリックして SD-WAN デバイスをインポートします。

STEP 5 | SD-WAN デバイスが正常に追加されたことを確認します。



NAME	TYPE	ROUT... NAME	SITE	LINK TAG	ROUT... ID	IPV4 LOOP... ADDR...	IPV6 LOOP... ADDR...	AS NUMB...	REMO... PRIVA... AS (IPV4)	REMO... PRIVA... AS (IPV6)	IPV4 PREFI... TO REDIS...	IPV6 PREFI... TO REDIS...	HA STATUS	UPSTR... NA...	Prisma Access Onboarding				AUTH...	CERTI... NAME	CERTI... EXPIRY
															INTER...	TENA...	REGIO...	IPSEC TERMI... NODE			
Hub254-2	hub	hub_VR	hub1	hub_tag				65432	true	true									Pre Shared Key		
Branch50-2	branch	branch...	branch					65433	true	true									Pre Shared Key		
Branch25-2	branch	branch...	siteC					64543	true	true									Certifi...	brcert...	Sep 18 00:45:... 2024 GMT
Branch20-2	hub	hub_VR	siteA					64532	true	true									Certifi...	hub_c...	Sep 18 00:49:... 2024 GMT

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

STEP 7 | **Push to Devices** (デバイスにプッシュ) を選択して、設定の変更を管理対象ファイアウォールにプッシュします。

オンボードPAN-OS ファイアウォールからPrisma Accessへ

SD-WAN プラグイン 2.2 は Prisma Access ハブサポート を提供し、Prisma Access コンピューティングノード(CN)に接続する PAN-OSファイアウォールが SD-WAN ハブアンドスポークトポロジでクラウドベースのセキュリティを実現します。このトポロジでは、SD-WAN ハブは Prisma Access CN(IPSec Termination Nodes)であり、SD-WAN ブランチは PAN-OS ファイアウォールです。最大 4 つのハブ(DIA AnyPath および Prisma Access ハブに参加している PAN-OS ハブの任意の組み合わせ)がサポートされます。SD-WAN は、ブランチをハブに接続する IKE および IPSec トンネルを自動的に作成します。SD-WAN および Prisma Accessのシステム要件を確認します。

最初に *Prisma Access* を設定してから、*SD-WAN* を設定することが重要です。

- 新しい*Prisma Access*構成を開始する場合は、Prisma Access Administrator's Guide (Prisma Access管理者ガイド)を読み、フェーズ*1*、次にフェーズ*2*の構成手順を完了してください。
- すでに*Prisma Access*を実行している場合は、フェーズ*1*が完了していることを確認してから、フェーズ*2*を完了します。

次のフローチャートは、2 つの構成フェーズの順序と、各フェーズ内の基本的な手順を示しています。リンクを含む完全なPrisma Accessの前提条件とSD-WANの設定手順は、フローチャートに従います。

フェーズ 1—PRISMA ACCESS	フェーズ 2:SD-WAN
(最初にフェーズ**1**を完了する)	(フェーズ **1** を完了した後にのみ開始)
1. テナントのインフラストラクチャ サブネット、インフラストラクチャ BGP AS、テンプレート スタック、およびデバイス グループを設定します。	1. SD-WAN が有効になっているインターフェイスを使用してブランチファイアウォールを設定します。 2. Panorama Web インターフェイスにログインします。

フェーズ 1—PRISMA ACCESS (最初にフェーズ1を完了する)	フェーズ 2:SD-WAN (フェーズ 1 を完了した後にのみ開始)
2. テンプレートスタック、テンプレート、デバイスグループ、信頼ゾーンと非信頼ゾーン、および特定のリージョンの帯域幅割り当てを設定します。 3. Prisma Access の展開がリモート ネットワーク用にライセンスされていることを確認します。 4. デプロイで、場所ごとではなく、コンピューティング場所ごとに帯域幅が割り当てられていることを確認します。 5. オンボードする場所に対応するコンピューティング場所に帯域幅が割り当てられていることを確認します。 6. ローカル コミットを実行し、Prisma Access クラウドにプッシュします。	3. ループバック アドレスの BGP ローカル アドレス プールを指定します。 4. SD-WAN ブランチファイアウォールを選択して Prisma Access ハブに接続し、接続を設定します。 5. 構成をコミットしてクラウドにプッシュします。 6. オンボーディングが完了していることを確認します。 7. ブランチファイアウォール を Prisma Access に同期します。 8. Panorama にコミットします。 9. デバイスにプッシュします。 10. 作成された新しいインターフェイスを表示します。 11. IPSec トンネルが稼働していることを確認します。 12. IKE ゲートウェイが稼働していることを確認します。 13. 監視データを生成する SD-WAN ポリシー ルールを作成します。 14. ブランチファイアウォールにコミットおよびコミットとプッシュを行います。 15. Prisma Accessハブアプリケーションとリンクのパフォーマンスを監視します。

SD-WAN を Prisma Access に接続する前に、SD-WAN が有効になっているインターフェイスを持つブランチファイアウォールが必要です。さらに、1 つ以上のテナントに対して次の Prisma Access 前提条件を実行していることを確認します。フェーズ 1 の手順は次のとおりです。

1. **Panorama** > **Cloud Services** > **Configuration** については、**Service Setup** ページでテナントのインフラストラクチャ サブネット、インフラストラクチャ BGP AS、テンプレート スタック、およびデバイス グループを設定します。
2. **Remote Networks** ページで、テンプレート スタック、テンプレート、デバイス グループ、信頼ゾーンと非信頼ゾーン、および特定のリージョンの帯域幅割り当てを設定します。

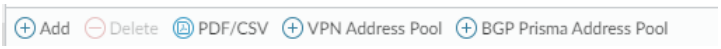
3. **[Panorama] > [Licenses (ライセンス)]**を順に選択してライセンス情報を確認し、Prisma Accessのデプロイメントがリモートネットワーク用にライセンスされていることを確認します。
   - 2020 年 11 月 17 日以降に利用可能なライセンスには、 **Net Capacity (ネット容量)** 領域のリモート ネットワークにライセンスされている帯域幅の量が表示されます。
   - 2020 年 11 月 17 日より前に利用可能なライセンスは、**Total Mbps** の下の **GlobalProtect Cloud Service for Remote Networks** エリアで使用可能なリモート ネットワーク帯域幅を示しています
4. ロケーションごとではなく、コンピュートロケーション ごとに帯域幅が割り当てられていることを確認します。
5. オンボードするロケーション https://docs.paloaltonetworks.com/prisma/prisma-access/prisma-access-panorama-admin/prepare-the-prisma-access-infrastructure/list-of-prisma-access-locations.html に対応するコンピュートロケーションに帯域幅が割り当てられていることを確認します。Prisma Access は、リージョンに割り当てる帯域幅の 500 Mbps ごとに 1 つの IPSec 終端ノードを割り当てます。
6. ローカル コミットを実行し、Prisma Access クラウドにプッシュします。

Prisma Access を使用してフェーズ 1 の前述の手順を実行した後、SD-WAN に対して次のフェーズ 2 の手順を実行します。

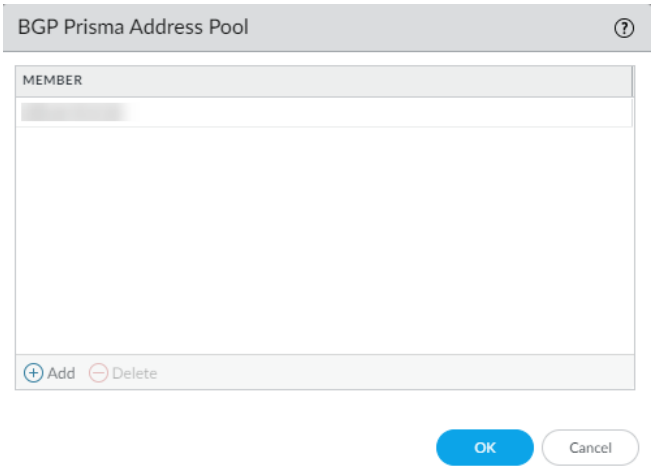
STEP 1 | Panorama Web インターフェイスへのログイン。

STEP 2 | ループバック アドレスの BGP ローカル アドレス プールを指定します。

1. **Panorama** 、 **> SD-WAN > VPN Clusters (VPN** クラスタ**)** と選択します。
2. 画面の下部で、**BGP Prisma Address Pool** を選択します。



3. Prisma Access のローカル BGP アドレスの未使用のプライベート サブネット (プレフィックスとネットマスク)を追加します。



4. **OK** をクリックします。
5. **[**コミット**]** します。

Prisma Access が既にオンボードされている場合は、既存のアドレス プールを単純に変更しないでください。アドレスプールを変更する必要がある場合は、メンテナンス期間中に次の手順を実行して、アドレスプールの変更で *SD-WAN* ブランチと *Prisma Access CN* を更新します。

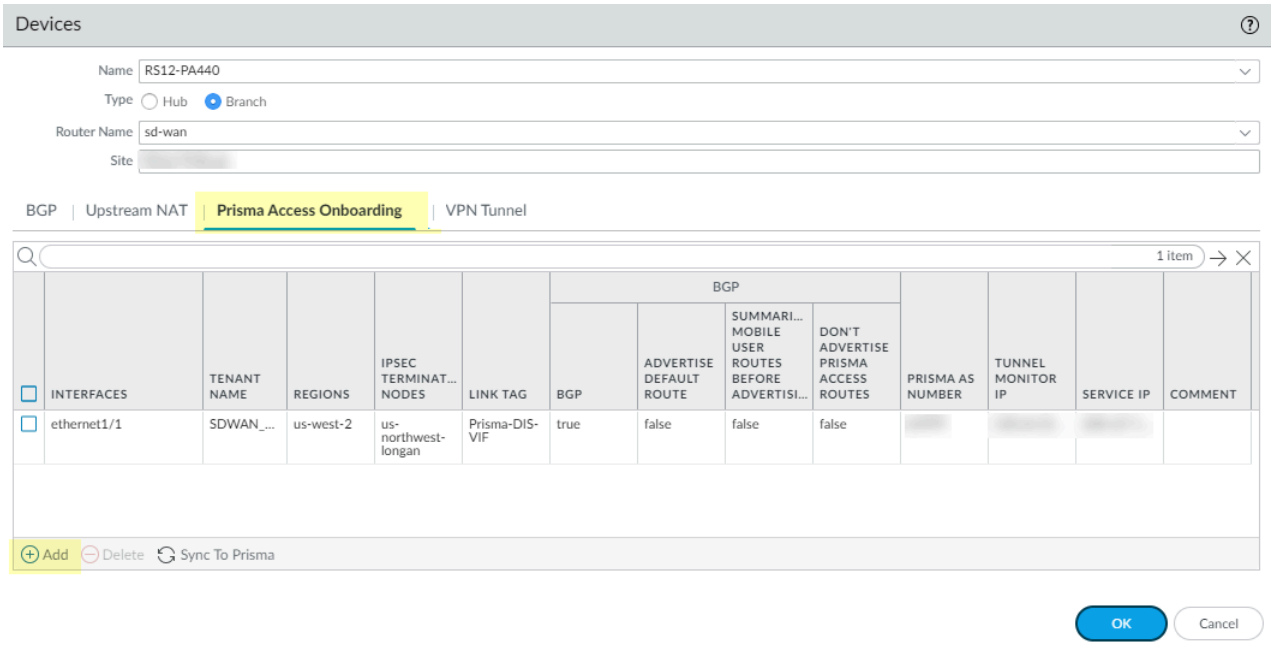
1. *Panorama* を使用して *SD-WAN* ブランチにアクセスし、アドレスプールの変更が影響する既存のオンボーディングを削除します。次に、ローカルコミットを実行します。
2. *VPN* アドレス プールを更新してから、ローカル コミットを実行します。
3. *Prisma Access*のオンボーディングを再度実行してから、ローカルのコミットとプッシュを実行します。

STEP 3 | SD-WAN ブランチファイアウォールを選択して Prisma Access ハブに接続し、接続を設定します。

1. **[Panorama]** > **[SD-WAN]** > [デバイス]を順に選択します。
2. SD-WAN を有効にしたブランチファイアウォールを選択し、その名前が **Name** フィールドに入力されます。
3. **Type** of device as **Branch**を選択します。
4. **Router Name** を選択します。
5. **Site** を入力します。

   すべての *SD-WAN* デバイスには、一意のサイト名が必要です。

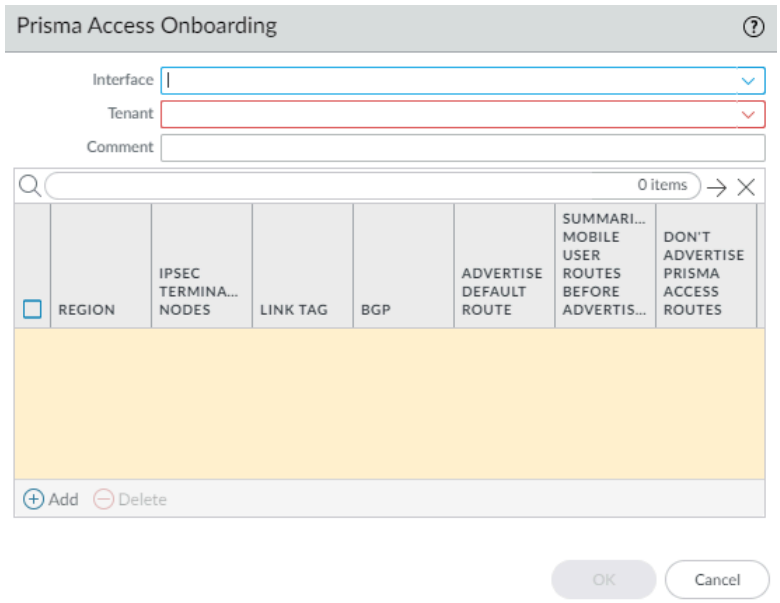
6. **Prisma Access Onboarding** と **Add** を選択します。



7. ファイアウォールでローカルの SD-WAN 対応 **Interface** を選択して、Prisma Access ハブに接続します。
8. Prisma Access **Tenant** を選択します (シングル テナント環境の場合は **default** を選択します)。

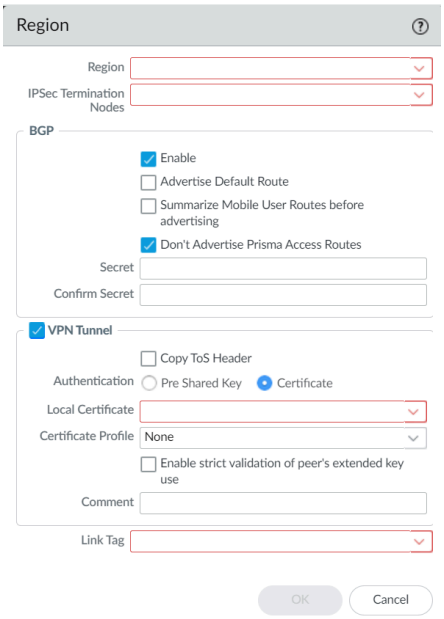
   ブランチファイアウォール 上のすべての SD-WAN インターフェイスは、同じ Prisma Access テナントを使用する必要があります。

9. 役に立つ コメント を入力してください。



10. CN (Prisma Access ハブ) が配置されているリージョンを選択して、**Region** にコンピューティング ノードを追加します。

    インターフェイスごとに複数のリージョンが存在する可能性があります。



11. ノードの一覧から **IPSec** 終端ノード (GP ゲートウェイ) を選択します。このリストは、Prisma Accessが以前にその地域のために起動したノードに基づいています。この

ブランチが接続するハブを選択しています。SD-WAN 自動 VPN 構成は、このノードとの IKE および IPSec 関係とトンネリングを構築します。

12. ブランチとハブ間の通信用の BGP(デフォルトは [有効] です)を有効化します。
13. **Advertise Default Route** を使用して、Prisma Access ハブのデフォルト ルートをブランチファイアウォール にアドバタイズできるようにします。
14. アドバタイズの前にモバイルユーザールートを要約すると、Prisma Accessハブに要約されたモバイルユーザーのIPサブネットルートをアドバタイズさせ、それによってブランチへのアドバタイズの数を減らします。
15. **Don't Advertise Prisma Access Routes** を使用して、IPSec Terminate Node/Hub が Prisma Access ルートを SD-WAN ブランチにアドバタイズしないようにします。
16. BGP 通信の認証用の **Secret** と **ConfirmSecret** を入力します。
17. (SD-WAN プラグイン 3.2.0 以降のリリース) PAN-OS ファイアウォールと Prisma Access ハブを認証するには、VPN トンネル パラメータと認証タイプを構成します。
    1. （任意）カプセル化されたパケット内のサービスタイプ（ToS）情報を保持する場合は、**[TOS**ヘッダーのコピー**]**を選択します。

       トンネル内に複数のセッション（それぞれ異なる *ToS* 値）、コピー *ToS* ヘッダーにより、*IPSec* パケットが順序どおりに到着しない可能性があります。
    2. 認証を以下より選択してください。**[Pre-Shared Key (**事前共有鍵**)]** あるいは**[Certificate (**証明書**)]** 。

       すべてのブランチ デバイスと追加される *Prisma Access* デバイスに対して同じ認証タイプを選択していることを確認してください。

    リージョンの認証タイプとして選択すると、事前共有鍵が自動的に生成されます。
18. 証明書ベースの認証を構成するには、**[Certificate (**証明書**)]** を選択します。
19. (証明書 認証タイプを有効にしている場合のみ) SD-WAN ブランチ ファイアウォールの Prisma Access オンボーディングを実行する前に、証明書が Panorama に存在し

ている必要があります。SCEPで生成された証明書はサポートしていません。すでに Panorama 上にある **[Local Certificate (**ローカル証明書**)]**を選択します。

Prisma Access オンボーディング プロセスを正常に実行するには、Panorama にある証明書について次の点を確認してください。

- 証明書は SD-WAN デバイスごとに一意である必要があります。複数のSD-WANデバイス間で証明書を共有することはできません。

  SD-WAN トンネル認証に使用されるブランチおよびハブのファイアウォール証明書を生成するときは、次の点に注意してください。

  - 2つの異なるハブデバイスが同じハブ証明書を使用できます。
  - 次の条件を満たす場合、2つの異なるブランチデバイスが同じブランチ証明書を使用できます。
    - ブランチ デバイスは同じ VPN クラスターの一部ではありません。
    - これらのブランチ デバイスが属する VPN クラスター間には共通のハブ デバイスがありません。
  - （HAデプロイメントのみ）2つの異なるブランチデバイスがHAメンバーとして構成されている場合、同じブランチ証明書を持つことができます。
  - ハブ デバイスが VPN クラスター間で共通である場合、これらの VPN クラスターの一部であるブランチ デバイスの証明書には、すべての属性が一意の値を持つ一意の証明書が必要です。一意性を確保しないと、 証明書 およびその値が異なる場合、ハブ デバイスでのコミットは失敗します (Panorama ではコミットは失敗しません)。

  また、*SD-WAN*トンネルの認証に使用されるリーフ証明書（ブランチおよびハブのファイアウォール証明書）が、以下の基準を満たすように生成されていることを確認してください：

  - キーの使用にはデジタル署名が必要です。
  - すべての証明書は同一のルート *CA* によって署名されている必要があります。
  - デバイス証明書はルート *CA* によって直接署名されている必要があります。
  - 証明書の形式は *PKCS12* である必要があります

- 証明書の属性は、IKE ゲートウェイのローカル ID とピア ID を決定するために使用されます。従って リーフ証明書、つまり SD-WAN トンネル認証に使用される ブランチおよびハブ ファイアウォール証明書は、次の 3 つの証明書属性を使用して生成する必要があり、各証明書属性には 3 つの一意の属性値を割り当てる必要があります。そうでない場合、コミット エラーがスローされます。

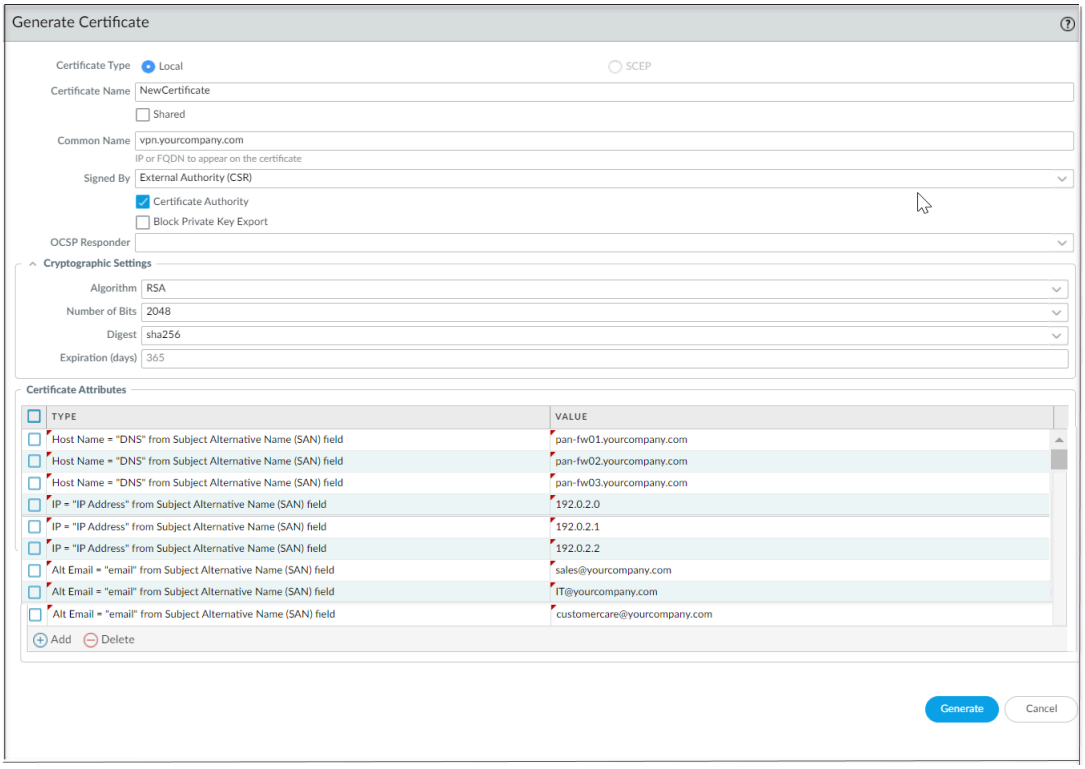
  - FQDN (ホスト名)

- IPアドレス (**IP**)
- ユーザーFQDN (代替メールアドレス)

すべての証明書において、一意のホスト名、***IP***、および 代替電子メール 証明書属性を持つことが必須とされています。つまり、どの証明書にも共通してこれらの属性値を持つことはできません。

次の例では、NewCertificateは合計9つの必須証明書属性を使用して生成されます。ホスト名証明書属性には、pan-fw01.yourcompany.com、pan-fw02.yourcompany.com、pan-fw03.yourcompany.comの3つの一意の属性値が設定されます。**IP**証明書属性は、次の3つの固有の属性値で設定されます。192.0.2.0, 192.0.2.1, and 192.0.2.2.代替電子メール証明書属性に

は、sales@yourcompany.com、IT@yourcompany.com、customercare@yourcompany.comの3つの固有の属性値が設定されます。

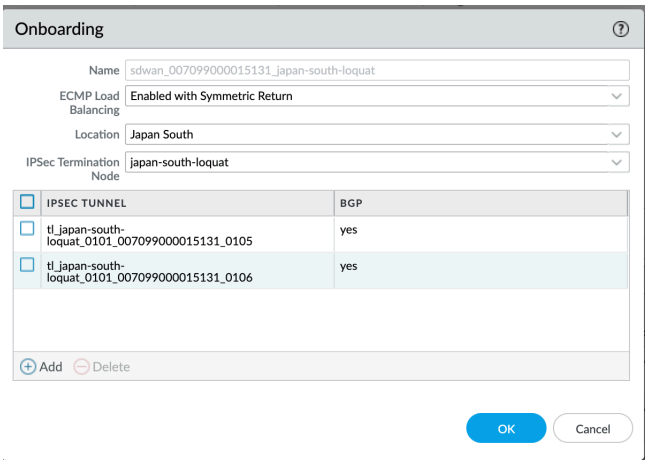


20. (オプション) (証明書 認証タイプを有効にする場合のみ) 証明書プロファイルを選択します。証明書プロファイルには、ピア ゲートウェイの認証方法に関する情報が含まれています。
21. （任意）鍵の使用方法を厳密に制御する場合は、**Enable strict validation of peer's extended key use**（ピアの拡張鍵使用の厳密な検証を有効にする）をクリックします。
22. ハブの **Link** タグ を選択します。

    Prisma Access ハブの *ECMP* を有効にする場合は、複数のブランチ インターフェイスを同じコンピューティング ノード*(CN)*にオンボードし、それらのブランチ インターフェイスで同じリンク タグを使用します。
23. **OK** をクリックします。ディスプレイには、ピアAS番号とPrisma Accessによって提供されるトンネルモニターIPアドレスが含まれます。

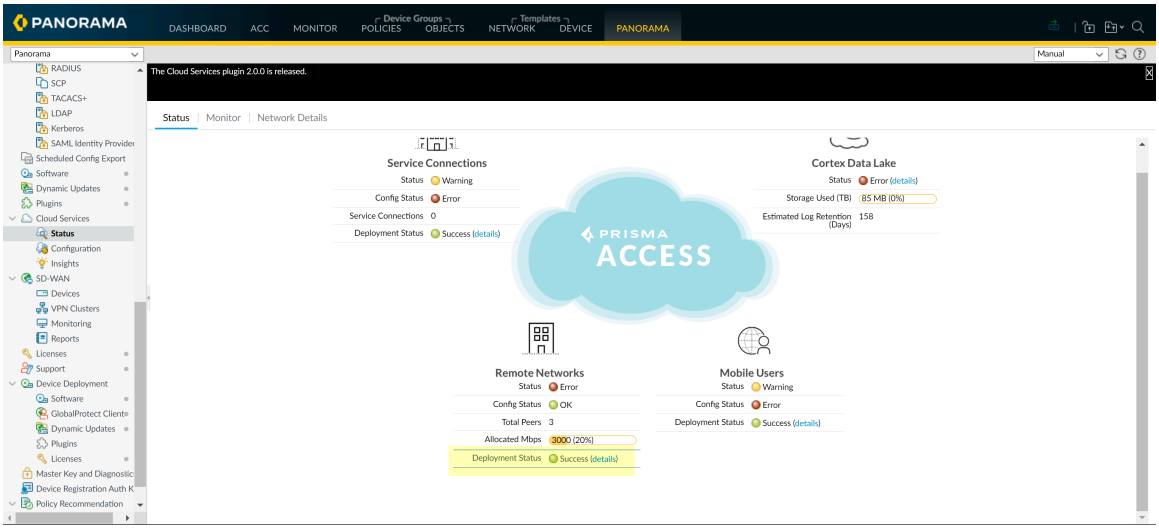
STEP 4 | **Commit and Push** で構成をクラウドに送信し、Prisma Access は要求された帯域幅に基づいて正しい数の IPSec ターミネーション ノードを起動します。

複数の *IPSec* トンネルが同じ *CN* に向かう場合、次の *Prisma Access* の例に示すように、*Prisma Access* 設定では対称リターンで *ECMP* が有効になっています。

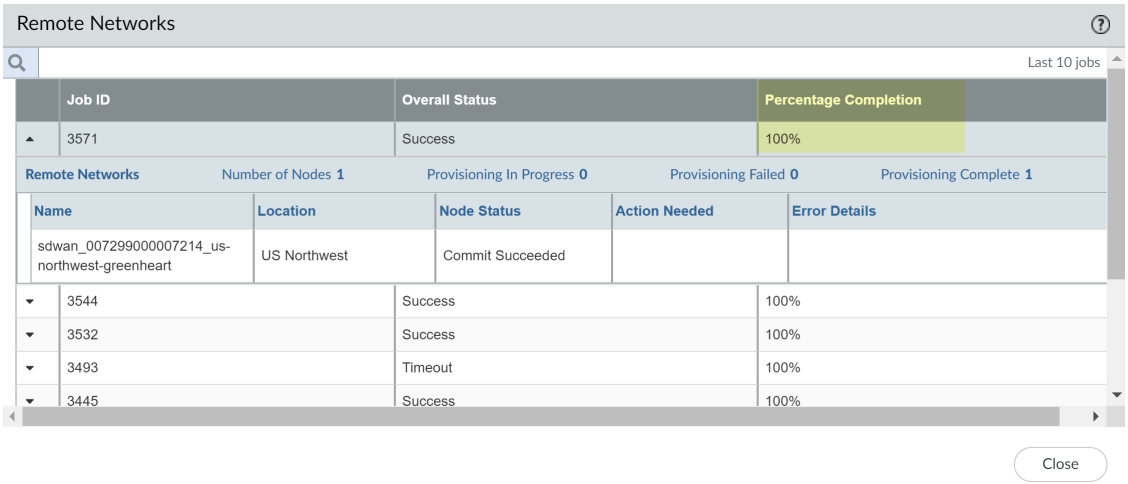


STEP 5 | オンボーディングが完了していることを確認します。

1. **Panorama** > **Cloud Services** > **Status** を選択し、[リモート ネットワークの展開状態] に success と表示されていることを確認します。



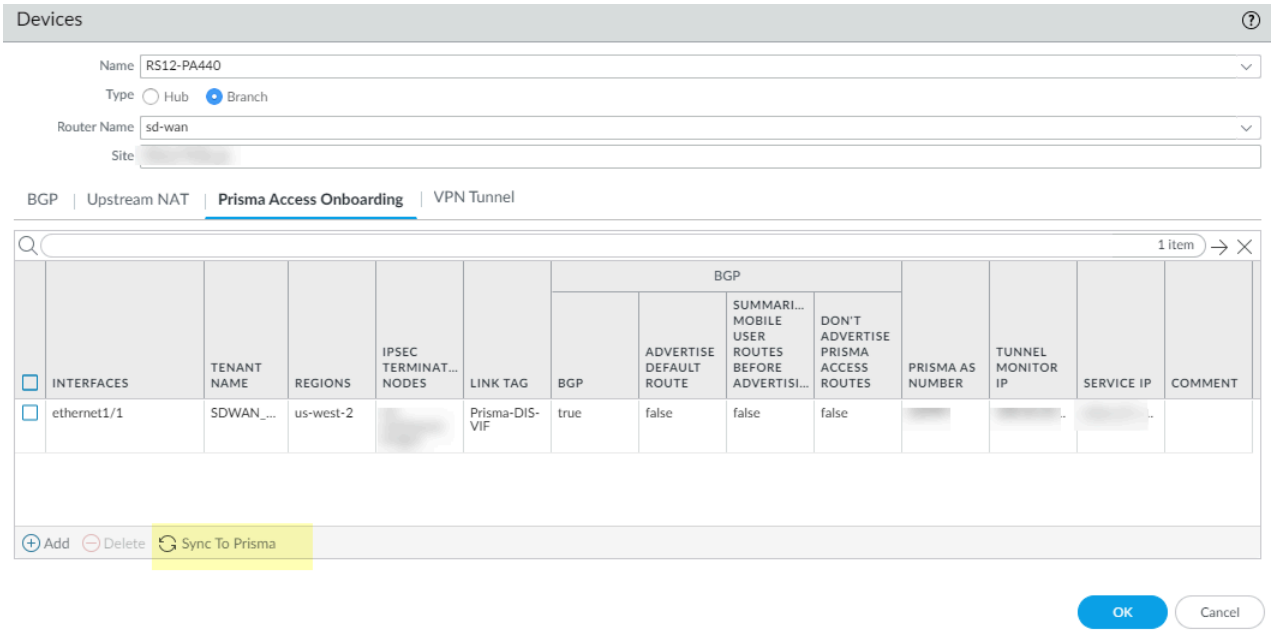
2. Remote Networks Deployment Status **details** を選択します。
3. Prisma Access ノードの完了に 100% と表示されていることを確認します。



STEP 6 | ブランチファイアウォールを Prisma Access に同期して、CN のサービス IP アドレスを取得します。

1. **Panorama** > **SD-WAN** > **Devices**を選択します。
2. SD-WAN ブランチ デバイスを選択します。
3. **Prisma Access Onboarding** と **Sync To Prisma** を選択します (メッセージに応答して続行します)。ブランチ デバイスごとに繰り返します。

> *Prisma* への同期が成功すると、*SD-WAN* ブランチファイアウォールに *Prisma Access* 設定パラメータが表示されます。そうでない場合は、約*15*分待ってから、*Prisma*への同期を繰り返します。必要に応じて、*Prisma Access* プラグインに移動し、*CN* のオンボーディングが完了していることを確認します *(*帯域幅と *IP* アドレスが割り当てられた *CN* を確認できます*)*。その検証の後、*Sync To Prisma* を再試行します。



STEP 7 | Panorama にコミットします。

STEP 8 | **Push to Devices**で、ローカルブランチファイアウォールにプッシュします。**Edit Selections** をクリックして、プッシュ範囲を選択します。正しい **Template** と **Device Group** を選択してください。

STEP 9 | ブランチファイアウォール で、**Network** > **Interfaces** > **SD-WAN** を選択し、作成したリンク タグで作成され、**zone-to-pa-hub** という名前のセキュリティ ゾーンに割り当てられ、CN に接続する IPSec トンネルを使用して作成された新しいインターフェイスを確認します。

STEP 10 | **Network** > **IPSec Tunnels** を選択し、IPSec トンネルが稼働していることを確認します。

STEP 11 | **Network** > **Network Profiles** > **IKE Gateways** を選択し、IKE ゲートウェイが稼働していることを確認します。

STEP 12 | 監視データを生成する SD-WAN ポリシールールを作成します。

この手順は、正確なトラフィック分散のために Prisma Access Hub の遅延、ジッター、およびパケット損失データのベースラインを作成するために必要です。SD-WAN モニタリングデータは、SD-WAN ポリシールールに一致するトラフィックから生成されます。

1. 「トラフィック分散プロファイルの作成」を行います。
2. パス品質プロファイルの作成、高遅延、ジッター、およびパケット損失のしきい値があります。

   SD-WAN ポリシー ルールを作成するには、パス品質プロファイルが必要です。高いしきい値を持つパス品質プロファイルを作成すると、アプリが別のリンクにスワップすることなく、Prisma Access Hub の遅延、ジッター、およびパケット損失のベースラインを作成できます。
3. 「SD-WAN ポリシー ルールの設定」を行います。

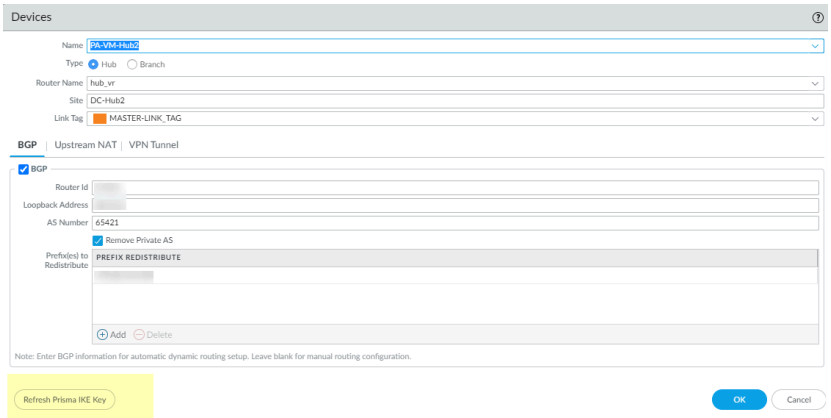
STEP 13 | **Commit** および **Commit and Push** をブランチファイアウォールに行います。

STEP 14 | (事前共有鍵 認証タイプを有効にしている場合のみ) Prisma IKE 事前共有鍵を更新します。

ブランチと*Prisma*ハブ間の*IPSec*接続を保護するために使用されている現在の*Prisma IKE*キーを変更する必要がある場合は、この手順を実行して、トンネルの新しいキーをランダムに生成し、トンネルの両側を更新します。この手順は、ハブとブランチがビジー状態でない場合に実行します。

「*gw_*」で始まる名前の*IKE*ゲートウェイは、オンボーディング中の*Prisma IKE*作成用に予約されているため、手動で作成しないでください。*Prisma IKE* 事前共有鍵を更新するこの手順では、*Prisma Access* によって作成されたゲートウェイ以外の名前付き *IKE* ゲートウェイがある場合は、すべての名前付き *IKE* ゲートウェイが更新されます。

1. **[Panorama]** > **[SD-WAN]** > **[Devices (**デバイス**)** を順に選択し、デバイスを選択します。
2. 画面の下部で、**Refresh Prisma IKE Key** を選択します。



3. IKE キーを更新すると、ブランチと Prisma Access ハブ間のすべての SD-WAN トンネルが更新され、すべてのブランチと Prisma Access ハブデバイスへの同時

設定プッシュが必要になることを通知するメッセージが表示されます。ベストプラクティスの推奨事項は、トラフィックが影響を受ける可能性があるため、メンテナンス期間中に更新を実行することです。`Do you wish to continue?` 続行しますか? 続行する場合は `Yes` を選択します。

STEP 15 | **Commit** および **Commit and Push** をブランチファイアウォールに行います。

STEP 16 | Prisma Access Hub アプリケーションとリンクのパフォーマンスを監視する、Prisma Access へのリンクのベースライン遅延、ジッター、およびパケット損失を理解する必要があります。

この手順は、正確な遅延、ジッター、およびパケット損失データを収集して、Prisma Access Hub Path Quality プロファイル を微調整するために必要です。

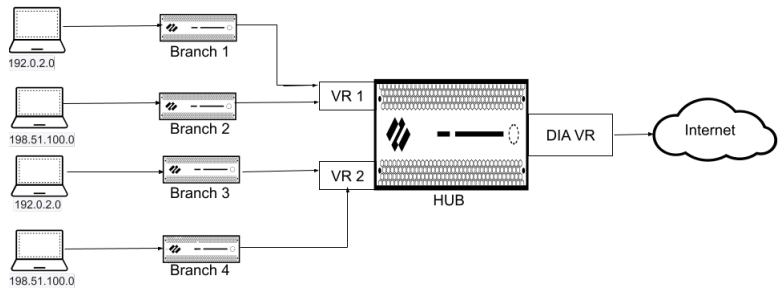
SD-WANハブで複数の仮想ルーターを構成する

どこで使用できますか?	何が必要ですか?
• PAN-OS • SD-WAN	❑ SD-WAN plugin license

（PAN-OS 11.1.3以降のリリース、およびSD-WANプラグイン3.2.1以降のリリース） 同じSD-WANハブに接続するブランチデバイス上でIPサブネットアドレスの重複を可能にするSD-WANハブ上の複数の仮想ルーターの サポート を 導入しました。この機能を使用すると、サブネットが重複する複数の論理ルーティングドメインを持つことができます。この機能を有効にすると、SD-WANハブは重複するサブネットが異なる仮想ルータにある場合にのみ重複するサブネットをサポートします。

デフォルトでは、SD-WANハブ上の複数の仮想ルーターは無効になっています。

次の図は、2つの仮想ルーターを備えたSD-WANハブを示しています。SD-WANハブで**multiple virtual routers support (**複数の仮想ルーターをサポート)を有効にすることで、同じSD-WANハブに接続する4つのブランチは、IPサブネットが重複したり、トラフィックが異なる仮想ルータに送信されるため、異なるエンティティに属して独立して機能したりできます。



複数の仮想ルーター機能は、SD-WANハブファイアウォールとPrisma Accessハブの両方でサポートされています。複数の仮想ルーター機能が有効になっているオンプレミスのハブにブランチが接続されている場合は、ブランチからハブとしてPrisma Accessをオンボードできます。

SD-WANハブファイアウォールを追加しながら、複数の仮想ルーターを構成します（**Panorama** > **SD-WAN** > デバイス ） 。

SD-WANデバイスのインポート中にCSVファイルを使用して複数の仮想ルーター関連設定をインポートすることはできません。

SD-WANハブ上の複数の仮想ルーターが有効になっている場合、高度なルーティングをサポートします。

STEP 1 | Panorama Web インターフェイスへのログイン。

STEP 2 | **[Panorama] > [SD-WAN] > [Devices (デバイス)]** を順に選択し、新しい SD-WAN ファイアウォールを 追加 します。

ハブテンプレートを作成中に、複数の仮想ルーターが有効になるSD-WANハブに参加しているすべての仮想ルーターを追加します。SD-WANプラグインを使用してSD-WANデバイスを追加する前に、この作業を行う必要があります。ハブテンプレートの作成中に、ブランチ上の仮想ルーター名がハブ上の仮想ルーターのいずれかと一致することを確認します。

STEP 3 | SD-WANハブで複数の仮想ルーターを構成する方法

- SD-WAN デバイスの**Type (タイプ)**を**Hub (ハブ)**として選択します。
- **[Enable Multi-VR Support (マルチVRサポートの有効化)]**を選択します。

仮想ルーター名に選択された仮想ルータは、ハブ ダイレクト インターネット アクセス（DIA）仮想ルータとして使用され、デフォルトの仮想ルータと見なされます。**[BGP]** タブで指定する設定は、DIA 仮想ルータに固有である必要があります。

- *SD-WAN*ハブで複数の仮想ルーター機能が有効になっている場合、*FEC*とパケットの二重化には対応していません。
- *SD-WAN*ハブの複数仮想ルーター機能は、ハブスポークトポロジでのみサポートされています（フルメッシュトポロジではサポートされていません）。
- *SD-WAN*ハブでインターネットトラフィックを処理するには、*SD-WAN*ポリシーにより、*MPLS*リンクにインターネットアクセスと*NAT*がある場合にのみ*MPLS*タグが選択されるようにする必要があります。
- 複数の仮想ルーターによる *SD-WAN*ハブ機能のサポートがイネーブルの場合、*PAN-OS* は *SD-WAN VPN* トンネルの外部でのトラフィックのクリアテキスト転送（***SD-WAN Interface Profile (SD-WAN** インターフェイス プロファイル)*で ***VPN*** データトンネルサポートが無効となっている場合）をサポートしません。

パロアルトネットワークスのファイアウォールでサポートされている仮想ルーターの数は次のとおりです。

Palo Alto Networks ファイアウォール	最大仮想ルーターに対応	最大SD-WANハブ仮想ルーターに対応
PA-3400	11	10
10 PA-5220およびPA-5410	20	20

Palo Alto Networks ファイアウォール	最大仮想ルーターに対応	最大SD-WANハブ仮想ルーターに対応
20 PA-5250およびPA-5430	125	50
PA-5420	50	20
20 PA-5260、PA-5280、PA-5400、PA-5440、PA-5445、PA-7000	225	50

STEP 4 | （任意）仮想ルーターを設定します。

1. ［**Virtual Routers (**仮想ルーター**)**］タブを選択すると、SD-WANハブに複数の仮想ルーターを設定できます。
2. BGPルーティングはデフォルトでIPv4を使用するため、[**Enable IPv4 BGP Support (IPv4 BGP**サポートの有効化**)**]が有効になり、この構成を変更することはできません。
3. 仮想ルーターの名前を入力します。
4. ハブテンプレート（**Network** > **Zones**）で、設定している仮想ルータに適した作成済みの **Zone (**ゾーン**)** を選択します。

   Multi-VR Configuration (マルチ***VR***設定***)***で複数の仮想ルータに同じゾーンを設定する場合は、仮想ルータが重複するサブネットで設定されていないことを確認してください。
5. （任意）仮想ルーター**ID**を入力します。このIDは、全ルーターで一意である必要があります。
6. BGP ピアリングのスタティック IPv4 **Loopback Address (**ループバック アドレス**)** を指定します。自動 VPN 設定では、指定した IP v4 アドレスと同じループバックインターフェースが自動的に作成されます。既存のループバックアドレスを指定すると、コミットは正常に完了しません。既にループバックアドレスに使用されていない IP v4 アドレスを指定する必要があります。
7. **AS** 番号を入力します。autonomous system number(自律システム番号(AS 番号))は、一般的に定義されたインターネットへのルーティングポリシーを指定します。AS 番号は、ハブとブランチの場所毎で一意である必要があります。
8. SD-WAN BGP トポロジでハブまたはブランチ ファイアウォールとルートを交換する必要があるエンドポイントがあり、BGP アップデートのAS_PATH属性からプライベート AS 番号(64512 ~ 65534)を削除しないエンドポイントがある場合は、プライベート AS

の削除オプション(デフォルトは有効)を無効にします。この場合、プライベート AS 番号が BGP アップデートの SD-WAN プライベート AS から残ることを許可します。

プライベート ***AS*** の削除設定は、ブランチまたはハブ ファイアウォール上のすべての *BGP* ピア グループに適用されます。*BGP* ピア グループまたはピア間でこの設定を異なる場合は、*SD-WAN* プラグインの外部で設定を構成する必要があります。

Remove Private AS (プライベート ***AS*** の削除**)**設定を変更し、すべての *SD-WAN* クラスタ ノードにコミットし、その後 *2.0.2* より前の *SD-WAN* プラグイン バージョンにダウングレードする場合は、 ***Remove Private AS (***プライベート ***AS****)* に関連するすべての設定を *SD-WAN* プラグインの外部またはファイアウォールで直接行う必要があります。

9. **Prefix(es) to Redistribute (**再配信プレフィックス**)**を入力します。ハブデバイスでは、再配信用に少なくとも 1 つのプレフィックスを入力します。
10. **[OK]** をクリックします。
11. ［**Virtual Routers (**仮想ルーター**)**］タブの下部にある［追加］をクリックして、仮想ルーターをさらに追加します。

SD-WANブランチで複数の仮想ルーターを設定する

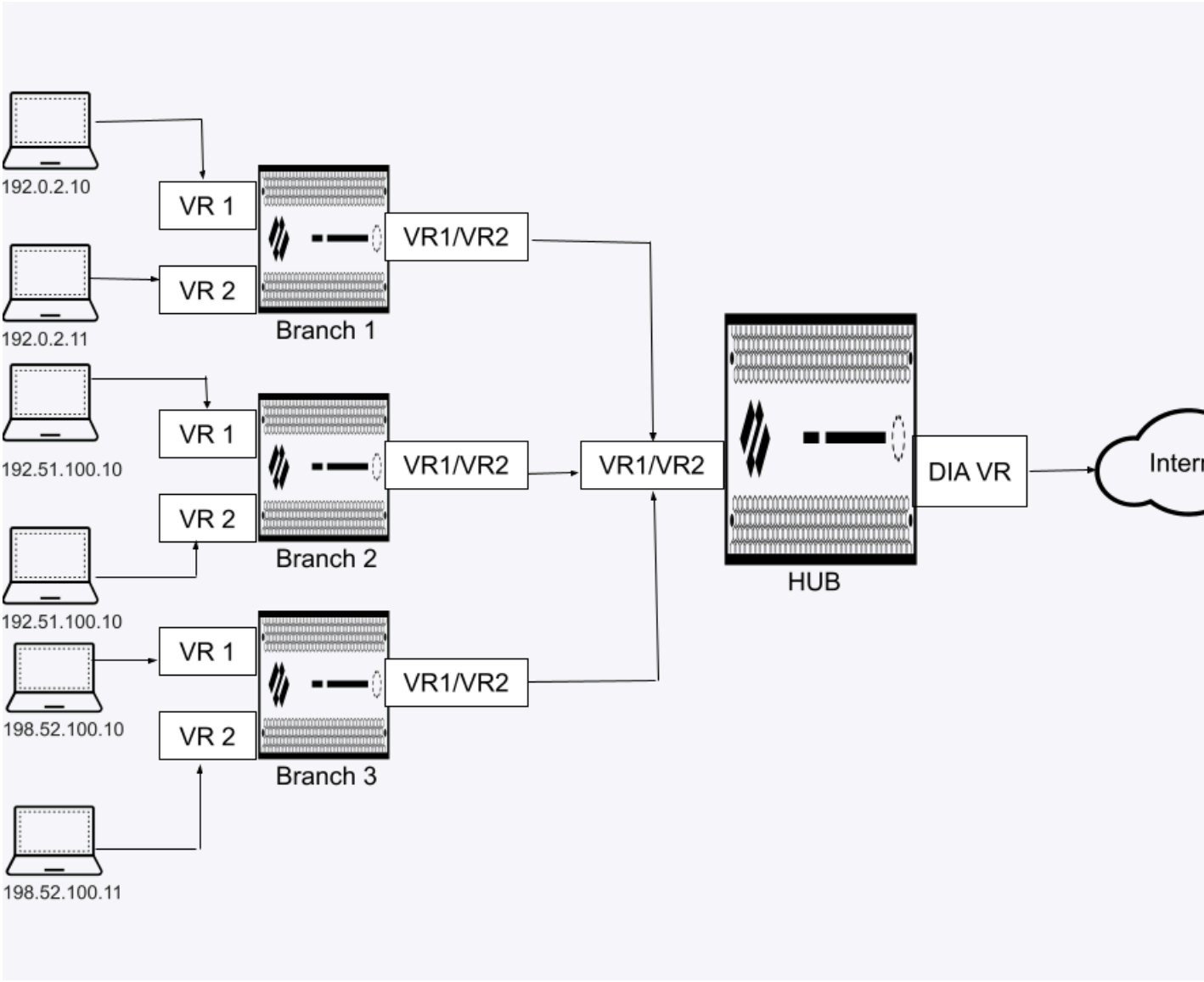
どこで使用できますか?	何が必要ですか?
• PAN-OS • SD-WAN	❑ SD-WAN plugin license

（PAN-OS 11.2.3 以降の 11.2 リリース、および SD-WAN プラグイン 3.3.1 以降の 3.3 リリース）SD-WAN ブランチの複数の仮想ルーターで、ハブデバイスとブランチデバイスの両方で IP サブネットアドレスが重複するサポートを導入しました。この機能を使用すると、サブネットが重複する複数の論理ルーティングドメインを持つことができます。

SD-WANブランチデバイスで複数の仮想ルーターを有効にする前に、次のことを確認してください。

- ブランチが接続されているハブデバイスは、複数の仮想ルーターをサポートしている必要があります。 ブランチ デバイスが接続されているハブ デバイスには、ブランチ デバイスに存在するすべての仮想ルーターが必要です。
- VPN クラスタで、ブランチが複数の仮想ルーターをサポートするようにするには、最初にすべてのハブで複数の仮想ルーターのサポートを有効にする必要があります。

次の図は、3つのSD-WANブランチを示しており、それぞれが1つ以上の仮想ルーターで構成されています。SD-WANブランチで複数の仮想ルーターサポートを有効にすることで、同じSD-WANハブに接続する3つのブランチは、IPサブネットが重複したり、トラフィックが異なる仮想ルータに送信されるため、異なるエンティティに属して独立して機能したりできます。



STEP 1 | Panorama Web インターフェイスへのログイン。

STEP 2 | **[Panorama]** > **[SD-WAN]** > **[Devices (デバイス)]** を順に選択し、新しい SD-WAN ファイアウォールを 追加 します。

STEP 3 | SD-WANブランチデバイスに複数の仮想ルーターを設定するには、次の手順を実行します。

- SD-WAN デバイスの**Type (**タイプ)を**[Branch (**ブランチ)**]**として選択します。
- **[Enable Multi-VR Support (**マルチ**VR**サポートの有効化**)]**を選択します。

仮想ルーター名に選択された仮想ルータは、ブランチ ダイレクト インターネット アクセス（DIA）仮想ルータとして使用され、デフォルトの仮想ルータと見なされます。［**BGP**］ タブで指定する設定は、DIA 仮想ルーターに固有である必要があります。

- *SD-WAN*ブランチで複数の仮想ルーター機能が有効になっている場合、*FEC*とパケットの二重化には対応していません。
- *SD-WAN*ブランチの複数仮想ルーター機能は、ハブスポークトポロジでのみサポートされています（フルメッシュトポロジではサポートされていません）。
- *SD-WAN*ブランチでインターネットトラフィックを処理するには、*SD-WAN*ポリシーにより、*MPLS*リンクにインターネットアクセスと*NAT*がある場合にのみ*MPLS*タグが選択されるようにする必要があります。
- 複数の仮想ルーターによる *SD-WAN* ブランチ機能のサポートがイネーブルの場合、*PAN-OS* は *SD-WAN VPN* トンネルの外部でのトラフィックのクリアテキスト転送（***SD-WAN Interface Profile (SD-WAN*** インターフェイス プロファイル*)*で ***VPN*** データトンネルサポートが無効となっている場合）をサポートしません。

SD-WANブランチデバイスでは、最大20台まで仮想ルーターをサポートできます。ただし、SD-WANブランチでサポートされている仮想ルーターの数は、プラットフォームによって異なります。

Palo Alto Networks ファイアウォール	サポートされる仮想ルーターの最大数	サポートされる**SD-WAN**ブランチ仮想ルーターの最大数
PA-460	5	5
PA-450	5	5
PA-445	3	3
PA-440	3	3
PA-415	3	3

Palo Alto Networks ファイアウォール	サポートされる仮想ルーターの最大数	サポートされるSD-WANブランチ仮想ルーターの最大数
PA-1420	10	10
PA-1410	10	10
PA-850	5	5
PA-820	5	5
PA-3200	10	10

STEP 4 | （任意）仮想ルーターを設定します。

1. ［**Virtual Routers**］タブを選択すると、SD-WANブランチに複数の仮想ルーターを設定できます。
2. BGPルーティングはデフォルトでIPv4を使用するため、[**Enable IPv4 BGP Support (IPv4 BGP**サポートの有効化**)**]が有効になり、この構成を変更することはできません。
3. 仮想ルーターの名前を入力します。
4. 仮想ルーターの一意のゾーンを選択します。

   複数の仮想ルーター構成の VPN クラスタでは、複数の仮想ルータ構成に参加している仮想ルーターを持つ各デバイス（ブランチまたはハブ）に一意のゾーンが必要です。
5. （任意）仮想ルーター**ID**を入力します。このIDは、全ルーターで一意である必要があります。
6. BGP ピアリングのスタティック IPv4 **Loopback Address (**ループバック アドレス**)** を指定します。自動 VPN 設定では、指定した IP v4 アドレスと同じループバックインターフェースが自動的に作成されます。既存のループバックアドレスを指定すると、コミットは正常に完了しません。既にループバックアドレスに使用されていない IP v4 アドレスを指定する必要があります。
7. **AS** 番号を入力します。autonomous system number(自律システム番号(AS 番号))は、一般的に定義されたインターネットへのルーティングポリシーを指定します。AS 番号は、ハブとブランチの場所毎で一意である必要があります。
8. SD-WAN BGP トポロジでハブまたはブランチ ファイアウォールとルートを交換する必要があるエンドポイントがあり、BGP アップデートのAS_PATH属性からプライベート AS 番号(64512 ~ 65534)を削除しないエンドポイントがある場合は、プライベート AS

の削除オプション(デフォルトは有効)を無効にします。この場合、プライベート AS 番号が BGP アップデートの SD-WAN プライベート AS から残ることを許可します。

プライベート ***AS*** の削除設定は、ブランチまたはハブ ファイアウォール上のすべての *BGP* ピア グループに適用されます。*BGP* ピア グループまたはピア間でこの設定を異なる場合は、*SD-WAN* プラグインの外部で設定を構成する必要があります。

Remove Private AS (プライベート ***AS*** の削除**)**設定を変更し、すべての *SD-WAN* クラスタ ノードにコミットし、その後 *2.0.2* より前の *SD-WAN* プラグイン バージョンにダウングレードする場合は、 ***Remove Private AS (***プライベート ***AS****)* に関連するすべての設定を *SD-WAN* プラグインの外部またはファイアウォールで直接行う必要があります。

9. **Prefix(es) to Redistribute (**再配信プレフィックス**)**を入力します。ハブデバイスでは、再配信用に少なくとも 1 つのプレフィックスを入力します。
10. **[OK]** をクリックします。
11. ［仮想ルーター］タブの下部にある［追加］をクリックして、仮想ルーターをさらに追加します。

SD-WAN 対応 HA デバイスの設定

SD-WAN 環境の一部として、アクティブ/パッシブ HA モードのブランチとして 2 つのファイアウォール (またはアクティブ/パッシブ HA モードのハブとして 2 つの ファイアウォール) を設定できます。この場合、Panorama ™ は 2 台のファイアウォールを個別に対処するのではなく、同じ設定をアクティブピアとパッシブピアにプッシュする必要があります。これには、SD-WAN 用のデバイスを追加する前にアクティブ / パッシブ HA を設定して、Panorama がこのデバイスが HA ピアであることを認識し、同じ設定をプッシュできるようにする必要があります。(HA アクティブ/パッシブ モードのみがサポートされます。)

HA ピアを *SD-WAN* デバイスとして追加した後でコミットしてしまうことがないよう、作業を開始する前に以下の手順を必ずお読みください。

HA では、ファイアウォールは *SD-WAN* セッション分散統計を同期しません。*HA* フェールオーバー後、セッション分散統計情報には新しいセッションの統計情報のみが表示されます。既存のセッションの統計は失われます。

STEP 1 | HA ピアで SD-WAN を有効にする前に、SD-WAN をサポートする 2 台のファイアウォール モデルで、configure Active/Passive HA (アクティブ / パッシブHAの設定) を行います。

STEP 2 | HA ピアを SD-WAN devices (SD-WAN デバイス) として追加します。ただし、コミットする最後の手順は実行しません。

STEP 3 | Panorama で、**Panorama** 、 > **Managed Devices** (管理対象デバイス) > **Summary**(サマリー)と選択します。

STEP 4 | 画面の下部で、**Group HA Peers** (**HA** ピアのグループ化) を選択します。Status (ステータス) 表示の下のHA Status (HAステータス) 列に、アクティブおよびパッシブの 2 台のファイアウォールが含まれていることを確認します。Panorama が HA ステータスを認識しているので、コミットすると、同じ SD-WAN 設定が 2 つの HA ピアにプッシュされます。

STEP 5 | **Commit** (コミット) および **Commit and Push** (コミットしてプッシュ) を選択します。

VPN クラスタの作成

SD-WAN 設定では、 1 つまたは複数の VPN クラスタを設定して、どのブランチがどのハブと通信するかを決定し、ブランチとハブのデバイス間にセキュアな接続を作成する必要があります。VPN クラスタはデバイスの論理的なグループであり、デバイスを論理的にグループ化する際は、地理的な場所あるいは機能等を考慮します。

PAN-OS® は、ハブスポークトポロジとフルメッシュ SD-WAN VPN トポロジの両方をサポートします。ハブスポーク トポロジでは、プライマリ オフィスまたは場所にある中央集中型ファイアウォール ハブが、ブランチ デバイス間のゲートウェイとして機能します。ハブからブランチへの接続は VPN トンネルです。この設定では、ブランチ間のトラフィックはハブを通過することになります。

SD-WAN ハブまたはブランチファイアウォールの直接インターネットアクセス (DIA) リンクを初めて仮想 SD-WAN インターフェースの設定すると、`autogen_hubs_cluster` という VPN クラスターが自動的に作成され、SD-WAN ファイアウォールが VPN クラスターに自動的に追加されます。これにより、Panorama™ 管理サーバーは、SD-WANファイアウォールによって保護されているデバイスをSD-WAN アプリケーションおよびリンクパフォーマンスの監視し、企業ネットワーク外のリソースにアクセスできます。さらに、将来 DIA リンクを使用して設定するいずれの SD-WAN ファイアウォールは、自動的に `autogen_hubs_cluster` VPN クラスタに追加されます。このクラスタには、DIA リンクを備えたすべてのハブおよびブランチが含まれており、Panorama はアプリケーションとリンクのパフォーマンスを監視することができます。`autogen_hubs_cluster` は、純粋にアプリケーションとリンクの状態を監視するものであり、DIA リンクを使用してハブとブランチの間に VPN トンネルを作成するものではありません。ハブとブランチを VPN トンネルで接続する場合は、新しい VPN クラスタを作成して、必要となるすべてのハブおよびブランチをその VPN クラスタに追加する必要があります。

認証タイプとして事前共有鍵を選択すると、VPN トンネル保護目的で、VPN クラスタ内のすべてのハブとブランチに強力かつランダムな IKE 事前共有キーが作成されます。また各ファイアウォールは事前共有キーを暗号化するマスターキーを保持します。本システムでは、管理者からも事前共有キーを保護します。Panorama がクラスタのすべてのメンバーに送信する IKE 事前共有キーを更新することができます。

クラスタ メンバーが混雑状態以外の時に事前共有キーを更新します。

［**Authentication Type (認証タイプ)**］で［**Certificate (証明書)**］を選択すると、SD-WAN VPNクラスタ内のハブとブランチはcertificate-based authentication (証明書ベース認証)に基づきます。

SD-WAN プラグインを 2.1.0 にアップグレードした後、1 つの VPN クラスター内のハブとブランチ ファイアウォールはすべて PAN-OS 10.0.4 (または後の 10.0 リリース) または 10.1.0 を実行する必要があります。

VPN クラスタを表示しているときに、データが存在しないか、*SD-WAN* が未定義であることが画面に表示されている場合は、使用している*Panorama*リリースが使用しようとしている *SD-WAN* プラグインリリースをサポートしていることを *[*Compatibility Matrix (互換性マトリックス)*]* で確認してください。

2つのイーサネットポート（またはサブインターフェイスまたはAEインターフェイス）（DIAリンク）間にIPv4またはIPv6のIPSecトンネルが形成されるかどうかは、イーサネットインターフェイス（またはサブインターフェイスまたはAEインターフェイス）のアドレスがIPv4かIPv6かによって異なります。両方のインターフェイスに IPv4 アドレスがある場合、IPv4 トンネルが起動します。両方のインターフェイスに IPv6 アドレスがある場合、IPv6 トンネルが起動します。デュアルスタックの場合、IPv4トンネルが起動します。

トンネルインターフェイスの IP アドレスは VPN プールから取得されます。IPv4アドレスプールとは無関係にIPv6アドレスプールを作成できます。IPv4アドレスとIPv6アドレスの両方が設定されている場合、次の表に示すように、トンネルインターフェイスにはIPv4アドレスのみが割り当てられます。IPv4 VPN アドレス プールが使い果たされ、IPv6 アドレス プールが存在する場合、トンネル インターフェイスには IPv6 アドレスが割り当てられます。IPv4のみが設定されている場合、トンネルはIPv4アドレスを使用します。IPv6のみが設定されている場合、トンネルはIPv6アドレスを使用します。

VPNプール	設定済み		
IPv4	あり	あり	いいえ
IPv6	あり	なし	あり
トンネル インターフェイスIP	IPv4 のみ	IPv4 のみ	IPv6 のみ

STEP 1 | ブランチとハブの VPN トポロジ計画を策定して、それぞれのハブと通信するブランチを決定します。詳細については、SD-WAN 設定計画を参照してください。

STEP 2 | Panorama Web インターフェイスへのログイン。

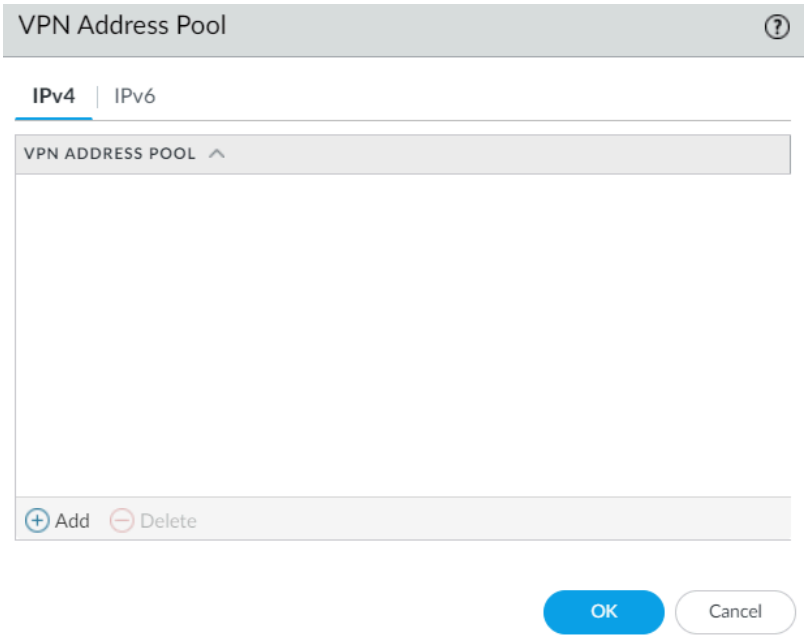
STEP 3 | 自動 VPN 設定が作成する IPSec VPN トンネルの IP アドレス範囲を指定します。

自動 *VPN* 設定は、ハブとブランチの間に *VPN* トンネルを作成し、*IP* アドレスをトンネル エンドポイントに割り当てます。*Auto VPN* が *VPN* トンネル アドレスとして使用するサブネットの範囲を入力します。最大 *20* の *IP* プレフィックスまたはネットマスク範囲を入力することができます。*Auto VPN* は、このプールの、まず範囲が最大のものから *VPN* トンネルのアドレスを取得します(アドレスファミリーの場合)。次に、必要に応じて次に大きい範囲のアドレスから取得します。このプールには少なくとも *1* つの範囲を設定する必要があります。設定をハブまたはブランチにプッシュする前にこの手順を実行しないと、コミットおよびプッシュは正常に完了しません。

以前の *SD-WAN* プラグイン リリースからアップグレードする場合は、設定済の範囲が正しいことを確認する必要があります。そうでない場合は、新しい範囲を入力します。***Commit* (コミット)** した後、すべてのトンネルは破棄され、新たなトンネルが使用されることになるので、この作業は、低トラフィックの時間帯に実行します。

1. **[Panorama] > [SD-WAN] > [VPN Clusters (VPN クラスター)]**を順に選択します。
2. 画面の下部の **VPN Address Pool (VPN アドレス プール)** を選択します。

3. 「**IPv4**」または「**IPv6**」を選択し、「192.168.0.0/16」または「2001：：/16」のように、1つ以上（最大2）のメンバーIPアドレスとネットマスク範囲のアドレスプールを追加します。
4. **OK** をクリックします。



Prisma Access がオンボードされている場合は、既存のアドレスプールを単純に変更しないでください。アドレスプールを変更する必要がある場合は、メンテナンス期間中に次の手順を実行して、アドレスプールの変更でブランチと*Prisma Access CN*を更新します。

1. *Panorama* を使用して *SD-WAN* ブランチにアクセスし、アドレスプールの変更が影響する既存のオンボーディングを削除します。次に、ローカルコミットを実行します。
2. *VPN* アドレス プールを更新してから、ローカル コミットを実行します。
3. *Prisma Access*のオンボーディングを再度実行してから、ローカルのコミットとプッシュを実行します。

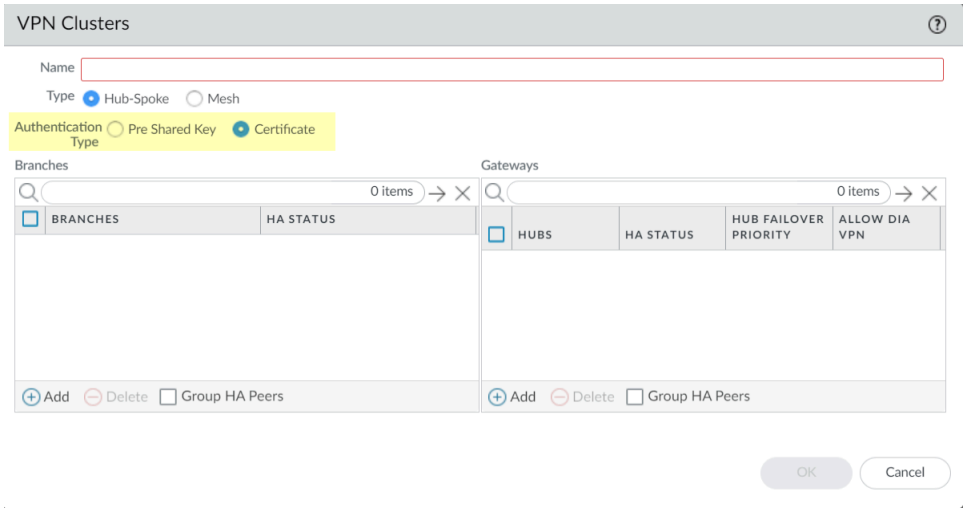
STEP 4 | VPN クラスタ の設定を行います。必要に応じて、この手順を繰り返し、VPN クラスタを作成します。

1. **[Panorama] > [SD-WAN] > [VPN Clusters(VPN** クラスタ**)]** と順に選択し、VPN クラスタを 追加します。
2. 名前にわかりやすい VPN クラスタ名を入力します。

   VPN クラスタ名ではアンダースコアおよび空白文字は使用できません。使用すると、そのクラスタのモニタリング *(**Panorama** > **SD-WAN** > **Monitoring (*モニタリング*))* データが表示されません。後で変更が必要にならないように、*VPN* クラスタ名は、慎重に選択します。*SD-WAN* monitoring (モニタリング) データは古いクラスタ名に基づいて生成され、新しいクラスタ名に一致させることができないため、*VPN* クラスタの監視またはレポートの生成時に、報告されるクラスタの数の面で問題が発生します。
3. VPN クラスタの **Type (**タイプ**)** を選択します。

   PAN-OS 10.0.2 以前の *11.0* リリースでは、***Hub-Spoke** VPN* クラスタ タイプのみがサポートされています。*PAN-OS 10.0.3* 以降では、DDNS サービスを含むフルメッシュ VPN クラスタの作成できます。
4. （SD-WANプラグイン3.2.0以降）以下の認証タイプを選択します。**[Pre-Shared Key (**事前共有鍵**)]** あるいは**[Certificate (**証明書**)]** 。VPN クラスターにデバイスを追加するに

は、認証タイプを指定することが必須です。VPN クラスターでは、すべてのデバイスに対して同じ認証タイプを選択する必要があります。



VPN クラスタの認証タイプを選択すると、VPN クラスタに追加できるのは（VPN クラスタと同じ）同じ認証タイプで設定されているブランチとハブだけです。たとえば、VPNクラスタの認証タイプとして証明書を選択した場合、クラスタに追加されるすべてのハブとブランチは、認証タイプとして証明書を使用して設定する必要があります。

すでに設定されているVPNクラスターの認証タイプやVPNクラスター名は変更できません。変更を行うには、VPNクラスタとそのSD-WANデバイスを削除し、新しい認証タイプまたはVPNクラスタ名を使用して再設定します。デフォルトでは、VPNクラス

タ内のデバイスの事前共有認証タイプをサポートしています（証明書方式が手動で選択されていない場合）。

- *VPN*クラスタを設定したら、クラスタ名やその認証タイプ（クラスタとデバイスレベルの両方）を変更することはできません。
- *1*つの*VPN*クラスタ内で異なる認証タイプを持つことはできません。つまり、*VPN*クラスタ認証タイプは、*VPN*クラスタ内のすべての*SD-WAN*デバイスと一致している必要があります。違いがあればコミット失敗となります。
- 異なる認証タイプの異なる*VPN*クラスタを設定できます。
- *VPN*クラスタでは、異なる認証タイプの*SD-WAN*デバイスを選択することはできません。*SD-WAN*ハブが*2*つの*VPN*クラスタの一部である場合、*2*つのクラスタは同じ認証タイプで構成する必要があります。

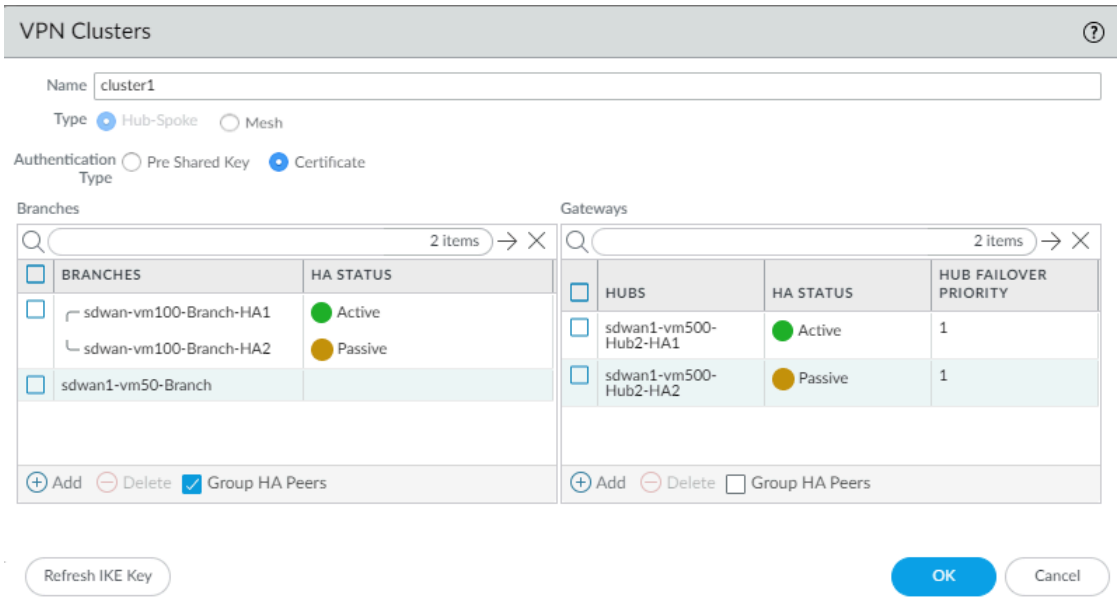
既存のVPNクラスタの認証タイプを証明書に変更する場合は、VPNクラスタを削除し、任意の認証タイプで作成し直します。

証明書認証タイプでVPNクラスタを作成した後、証明書認証タイプをサポートしていないPAN-OSまたはSD-WANプラグインバージョンにダウングレードする場合は、次の手順を実行します。

- 既存のVPNクラスタを削除します。SD-WANデバイス認証はダウングレード時に自動的に事前共有鍵に変更されます。
- 好みのPAN-OSまたはSD-WANプラグインバージョンにダウングレードします。証明書認証タイプの構成に必要な最小PAN-OSおよびSD-WANプラグインのバージョンについては、「SD-WANのシステム要件」を参照してください。

現在のSD-WANプラグインをアップグレードまたはダウングレードする前に 、「アップグレードとダウングレードの考慮事項」に記載されている手順に従ってください。

5. 相互通信の必要がある 1 つまたは複数のブランチ デバイスを **Add(追加)** します。
   - **Group HA Peers** を選択して、HA ピアであるブランチ デバイスをまとめて表示します。



- クラスタに追加するブランチ デバイスを選択します。
- **OK** をクリックします。

6. ブランチ デバイスとの通信が必要であると判断された 1 つまたは複数のハブ デバイスを **Add (**追加**)** します。

   HA 設定の SD-WAN ハブは、単一の SD-WAN ハブ ファイアウォールと見なされます。

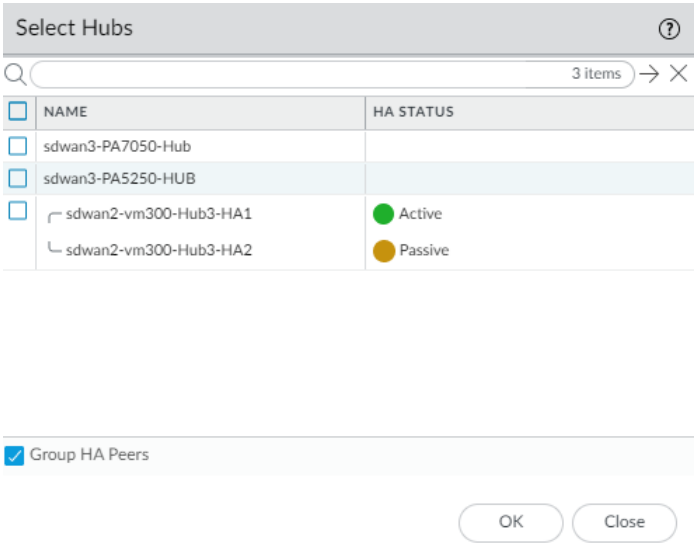
   MPLS および衛星リンク タイプは、同じリンク タイプのみでトンネルを形成します。これには、例えば、*MPLS*と*MPLS* および衛星と衛星間があります。例えば、*MPLS* リンクとイーサネット リンクの間にトンネルは作成されません。

   3.1.3より前のバージョンのSD-WANでは、VPNクラスターに最大4つのSD-WANハブファイアウォールを追加できます。

   （SD-WANプラグイン3.2.1以降）VPNクラスタに最大16台のSD-WANハブファイアウォールを追加できます。ECMP により、VPN クラスタ内で同じハブ優先順位を持つ

ことができるのは、16 のハブのうち 4 つだけです。4台以上のSD-WANハブに同じ優先度を設定しようとすると、コミットエラーが発生します。

- **Group HA Peers** (グループ **HA** ピア) を選択して、HA ピアであるブハブ デバイスを一緒に表示します。
- クラスターに追加するハブを選択し、**OK** をクリックします。



- 複数のハブを持つ新規または既存の VPN クラスタの場合、ハブに優先順位を付けて、a) トラフィックを特定のハブに送信し、b) 後続のハブ フェイルオーバーの順序を決定する必要があります。ハブ フェイルオーバーの優先度範囲は 1 ～ 4 です。アップグレードする場合、デフォルトの優先度は 4 に設定されます。次の表に示すように、プラグインはハブ フェイルオーバーの優先度を BGP ローカルプリファレンス番号に内部的に変換します。優先度の値が低いほど、優先度とローカルプリファレンスが高くなります。クラスタは、3.1.3以前のSD-WANバージョンで最大4つのハブをサポートします。SD-WANプラグイン3.2.1以降では、VPNクラスタに最大16台のSD-WANハブファイアウォールを追加できます。1 組のアクティブ/パッシブ HA ペアは 1 つのハブとしてカウントされます。複数のハブに同じ優先度を設定できます。HA ペアの優先度は同じである必要があります。Panorama は、ブランチの BGP テンプレートを使用して、ハブのローカル設定をクラスター内のブランチにプッシュします。

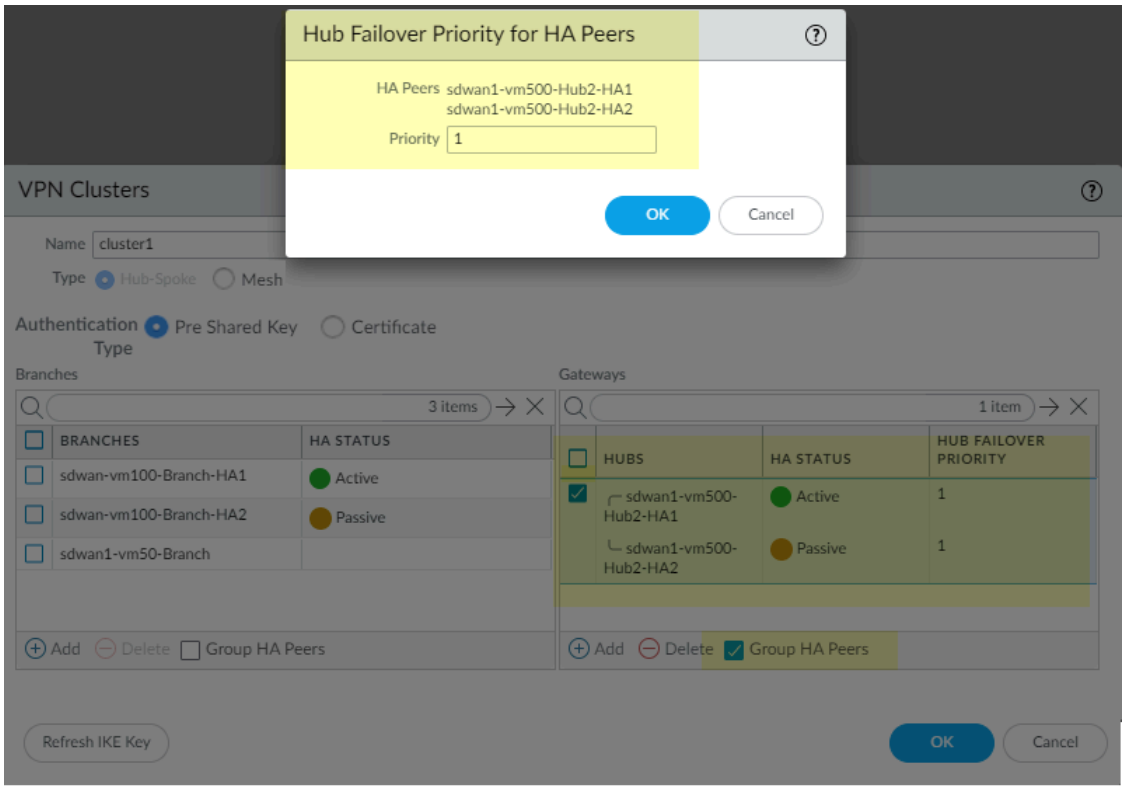
Hub Failover Priority (ハブフェイルオーバーの優先順位)	**Local Preference** (ローカル優先)
1	250
2	200
3	150

Hub Failover Priority (ハブフェイルオーバーの優先順位)	Local Preference (ローカル優先)
4	100

複数のハブの優先順位が同じ場合、*Panorama* は各ブランチ ファイアウォールの *2* か所で *ECMP* を有効にして、ブランチがパスを選択する方法を決定します。*ECMP* は仮想ルーターに対して有効になっており (***Network*** (ネットワーク) > ***Virtual Routers*** (仮想ルーター) > ***ECMP***)、***ECMP Multiple AS Support*** (***ECMP*** 複数 ***AS*** サポート) は *BGP* に対して有効になっています (***Network*** (ネットワーク) > ***Virtual Routers*** (仮想ルーター) > ***BGP*** > ***Advanced*** (高度機能))。クラスタ内のすべてのハブに一意の優先度がある場合、*ECMP* はブランチで無効になります。ハブの優先度の設定が変更された場合、*Panorama* は *ECMP* を有効にするか無効にするかを再評価します。

- **Group HA Peers** (グループ **HA** ピア) を選択した場合は、ペアを選択し、**Hub Failover Priority** (ハブ フェイルオーバー優先度) フィールドをクリックしま

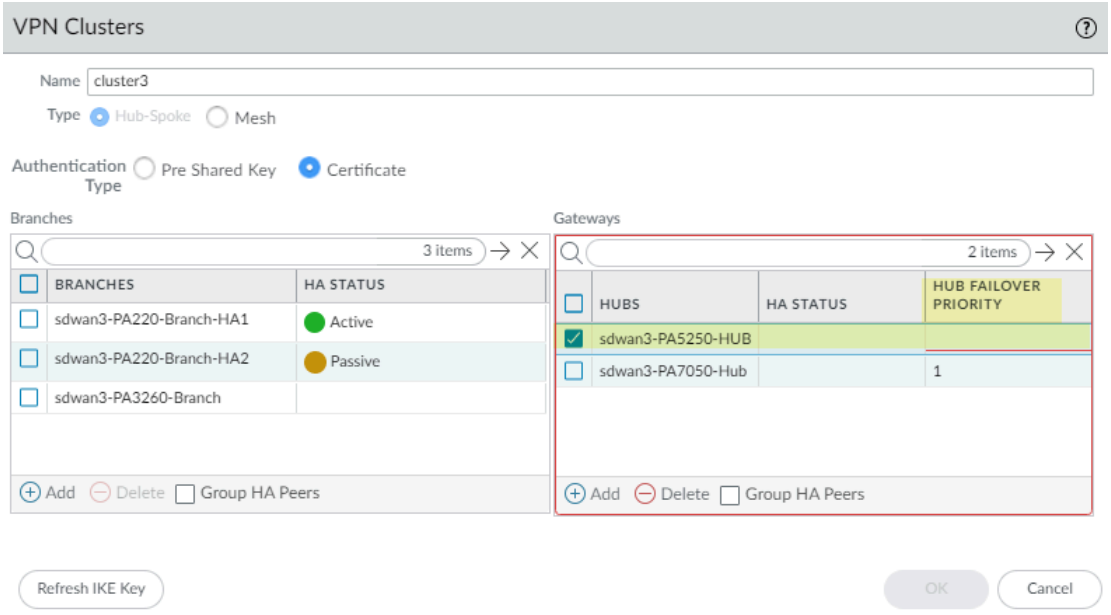
す。HA ペアの両方のハブに適用される単一の **Priority (優先度)** (範囲は1～4)を入力し、**OK** をクリックします。



[HA ピアのハブ フェールオーバー プライオリティ] ウィンドウは、設定された *HA* ペアに対してのみ表示されます。新しい *HA* ペアを追加する場合は、*2* つの新しいピアのそれぞれにハブ フェールオーバー プライオリティを個別に設定する必要があります。

グループ化されていない *HA* ピアであるハブに異なる優先順位を割り当ててから、***Group HA Peers*** および 送信を選択すると、エラーメッセージが表示されます。

- HA ペアではないハブの場合は、ハブを選択し、**[Hub Failover Priority (Hub フェールオーバー優先度)]** フィールドをクリックし、優先度を入力します (範囲は 1 から 4)。



7. **OK** をクリックすると VPN クラスタを保存します。

STEP 5 | ブランチの追加のプレフィクスをハブにアドバタイズします。

ファイアウォールがブランチからハブへのすべての非公開の接続ルートを自動的に再配信 (アドバタイズ) します。ブランチからハブに任意の追加のプレフィックスを再配信することもできます。***Prefix(es) to Redistribute*** **(**再配信するプレフィックス**)** フィールドでは、単一のプレフィックスのみでなく、複数のプレフィックスのリストを指定することができます。

1. **[Panorama] > [SD-WAN] > [Devices (デバイス)]** を順に選択し、ブランチ ファイアウォールを選択します。
2. **BGP** および **Add(追加)** を選択して、ネットマスクと共に1 つまたは複数の IP アドレスを **Prefix(es) to Redistribute (**再配信するプレフィックス**)** に追加します。
3. **OK** をクリックします。

STEP 6 | **Commit (コミット)** および**Commit to Panorama (Panorama** へのコミット**)** を選択します。

STEP 7 | (SD-WAN プラグイン 2.0.1 および以降の 2.0 リリース) ハブ スポーク VPN クラスタ内のハブ ファイアウォールに DHCP またはPPPoE インターフェースがある場合は、DDNS を使用する必要があります。**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、**Template**（テンプレート） フィールドでハブのテンプレート スタックを選択します。

STEP 8 | (SD-WAN プラグイン 2.0.1 および以降の 2.0 リリース) `Dynamic-DHCP Client` (ダイナミック DHCP クライアント) または PPPOE を示す IP アドレス 、画面底部の **Override** (オーバーライド) をクリックし、**OK** をクリックして閉じます。

STEP 9 | (SD-WAN Plugin 2.0.1 および以降の 2.0 リリース) DDNS 設定が設定されたことを Panorama 上で確認します。

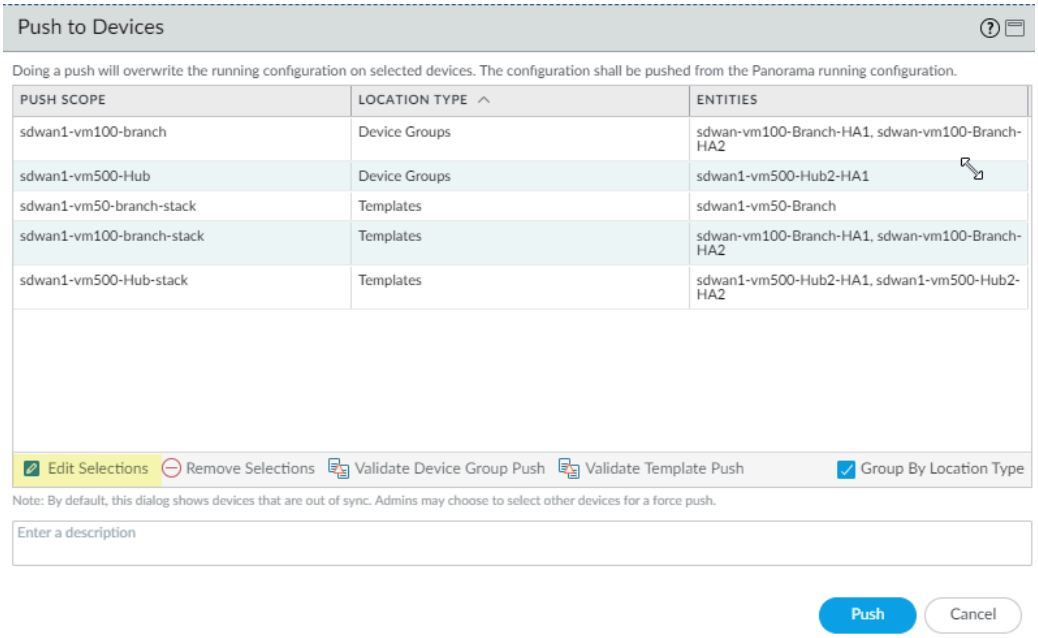
1. **Network** (ネットワーク) > **Interfaces** (インターフェース) > **Ethernet** (イーサネット) の順に選択し、同じインターフェースを再度選択します。
2. **Advanced** > **DDNS** の順に選択します。
3. DDNS 設定が **Hostname** (ホスト名) で自動的に設定されたことと、**Vendor** (ベンダー) が `Palo Alto Networks DDNS` に自動的に設定されたことを確認します。
4. **OK** をクリックします。

STEP 10 | (SD-WAN プラグイン 2.0.1 および以降の 2.0 リリース) **Commit** (コミット) および **Commit to Panorama** (**Panorama** にコミット) を実行します。

STEP 11 | 設定をハブにプッシュします。

Panorama は、ハブの仮想 *SD-WAN* インターフェース作成時に、必ずしも連続したインターフェース番号を使用してインターフェースを作成するわけではありません。例えば、*sdwan.921*、*sdwan.922*、*sdwan.924*、*sdwan.925* の通り、インターフェース番号をランダムにスキップする場合もあります。連続性に欠ける番号付けであったとしても、*Panorama* は、*SD-WAN* インターフェースの数に相当する数を作成します。*SD-WAN* インターフェースを表示するには、利用可能な *CLI* コマンド ***show interface sdwan?*** を使用します。

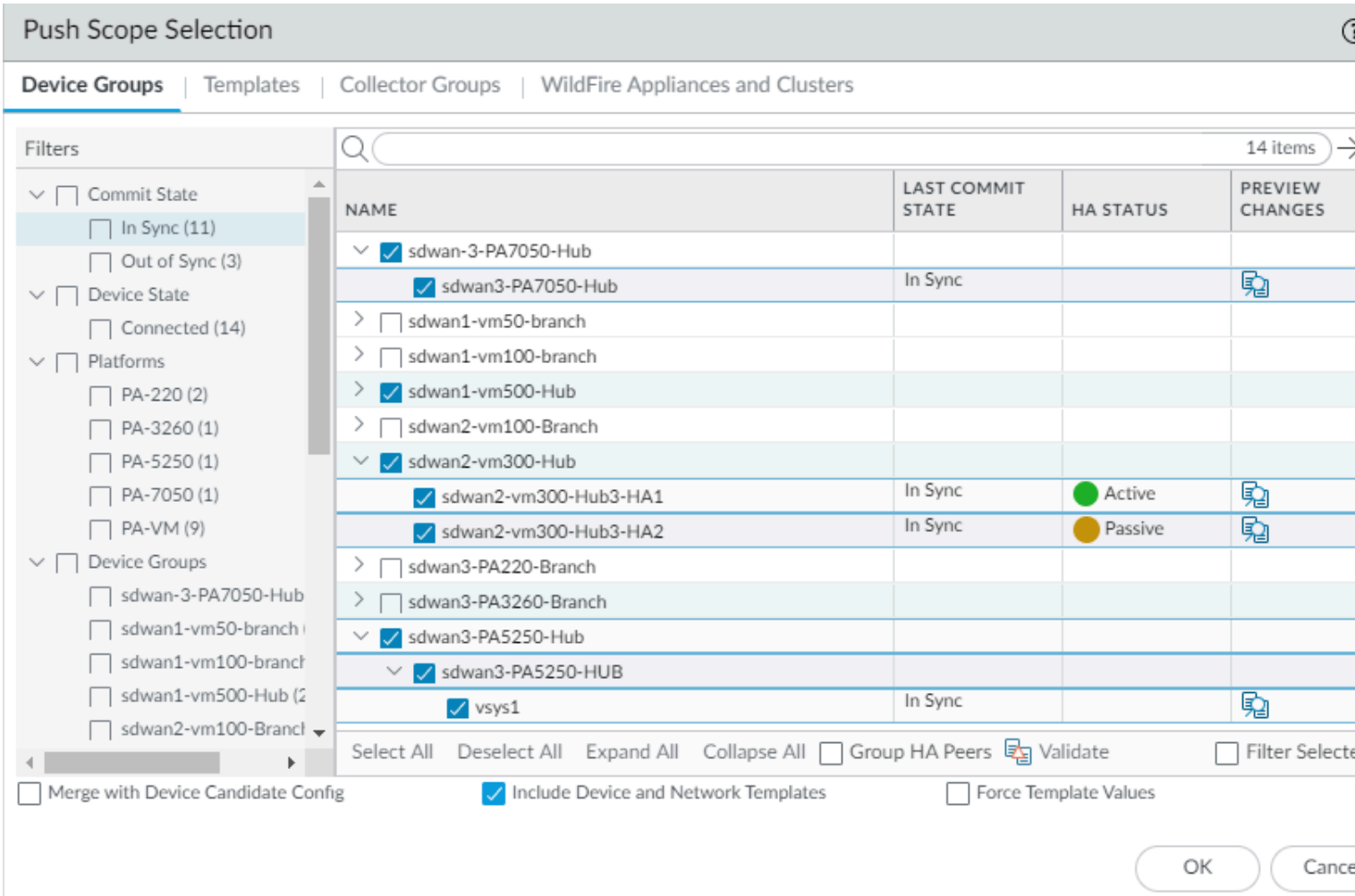
1. **Commit (コミット)** および **Push to Devices(デバイスにプッシュ)** を選択します。
2. 画面の左下の **Edit Selections (選択内容の編集)** を選択します。



3. **Filter Selected (選択したフィルタ)** の選択を解除します。
4. **Deselect All(すべての選択を解除)** をクリックします。
5. 使用するハブのデバイス グループを選択します。画面の下の **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)** を選択します。ブランチへのプッシュの前にハブへのプッシュを実行する必要があります。

   ほとんどのブランチでは、サービスプロバイダーを介して動的 IP アドレスを取得し、ハブにはブランチの IP アドレスの情報がないため、ブランチが IKE/IP Sec 接続を開始する必要があります。ハブが IKE/IP Sec 接続を受信できるには、ブランチの設定の前

にハブの設定をコミットおよびプッシュする必要があります。これにより、ブランチの設定がプッシュされ、ブランチがハブへの接続を開始すると、ハブの準備が整います。



6. **Templates (**テンプレート**)** タブを選択し、**Deselect All(**すべて選択解除**)**をクリックします。
7. **Push Scope (**プッシュのスコープ**)** はデバイス グループです。設定をハブに **Push(**プッシュ**)** します。

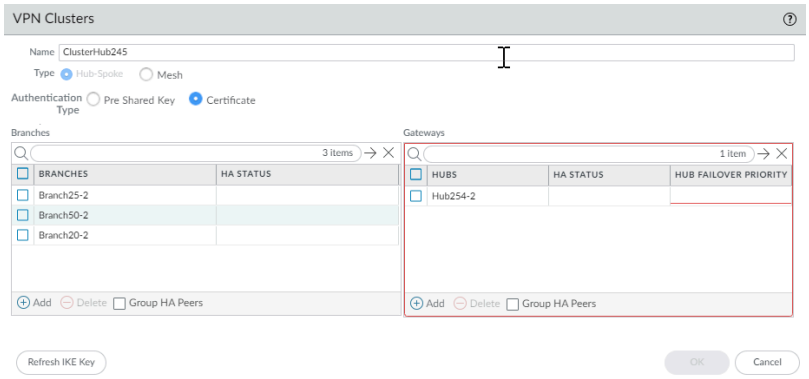
STEP 12 | 前の手順を繰り返してブランチのデバイス グループを選択し、設定をブランチにプッシュします。

STEP 13 | IKE 事前共有キーを更新します。

VPN クラスタ デバイス間の *IP Sec* 接続の保護目的で、使用されている現在の *IKE* キーを変更する必要がある場合は、この手順を実行し、クラスタの新しいキーのランダム生成を実行します。

この手順は、クラスタ メンバーが混雑状態でない時間に実行します。

1. **[Panorama] > [SD-WAN] > [VPN Clusters (VPN** クラスタ**)]** と順に選択し、クラスタを選択します。
2. 画面の下部で、**Refresh IKE Key (IKE** キーの更新**)** を選択します。



3. IKE キーを更新すると、VPN クラスタ内のすべての SD-WAN ファイアウォールに対して新しいセキュリティアソシエーション（SA）が生成されることを通知するメッセージが表示されます。これにより、サービスが中断する可能性があります。Do you wish to continue? 続行しますか?はい | いいえ続行する場合は [はい] を選択します。
4. **[**コミット**]** します。

   IKE Key を更新したら、クラスタ全体にコミットする必要があります。部分コミットを行うと、トンネルがダウンします。
5. **Push to Devices (**デバイスにプッシュ**)** します。

DDNS サービスを含むフルメッシュ VPN クラスタの作成

PAN-OS 10.0.3 以降のバージョンで、SD-WAN は、ハブスポーク トポロジに加えてフル メッシュ トポロジをサポートします。メッシュは、ハブの有無にかかわらずブランチで設定できます。ブランチが相互に直接通信を要求する場合は、フル メッシュを使用します。フル メッシュのユースケースの例には、ブランチとハブを持つ小売業者、ハブの有無にかかわらず運営するエンタープライズが含まれます。

一部のファイアウォール インターフェースは、DHCP を使用して IP アドレスを取得します。ブランチ オフィスは、多くの場合、消費者向けのインターネット サービスを使用し、動的 IP アドレスを受け取りますが、これはもちろん変更される可能性があります。このため、ファイアウォールにはダイナミック DNS (DDNS) が必要であり、DDNS サービスは SD-WAN を実行しているファイアウォール インターフェースの公開 IP アドレスを検出できます。DDNS 設定をすべてのファイアウォールにプッシュすると、各ファイアウォールに、外部インターフェースの IP アドレスを Palo Alto Networks DDNS クラウド サービスに登録して、IP アドレスが FQDN に変換されるように通知します。

また、ISP の CPE デバイスが送信元 NAT を実行している可能性があるため、DDNS も必要です。(ダイナミック IP アドレスは送信元 NAT 変換される場合とされない場合があります)。DDNS サービスを使用すると、ファイアウォールは公開 IP アドレスを DDNS サーバーに登録できます。デバイスをブランチ間メッシュに接続すると、Auto VPN はそれらのファイアウォールの DDNS サービスに接続して、DDNS クラウドに登録されているパブリック IP アドレスをプルし、それらのパブリック IP アドレスを使用して IKE ピアリングと VPN トンネルを作成します。CPE デバイスが送信元 NAT を実行している場合、Panorama によって管理される SD-WAN ブランチ デバイスを追加すると、**Upstream NAT (**アップストリーム**NAT)** が有効になり、NAT IP アドレスタイプは **DDNS** になります。

> 送信元 *NAT* を使用する *CPE* デバイスまたはアップストリーム ルーティング デバイスの場合、そのデバイスで *1* 対 *1* の宛先 *NAT* ルール *(*ポート変換なし*)* を作成して、外部 *IP* アドレスを、ファイアウォールのインターフェースに割り当てたプライベート *IP* アドレスに変換し直す必要があります。この変換により、*IKE* および *IPSec* プロトコルをファイアウォールに戻すことができます。*(Palo Alto Networks* には送信元 *NAT* を実行しているアップストリーム *CPE* またはアップストリーム ルーターへのアクセス権がありません*)*

DDNS サービスを備えた SD-WAN フル メッシュには、以下が必要です。

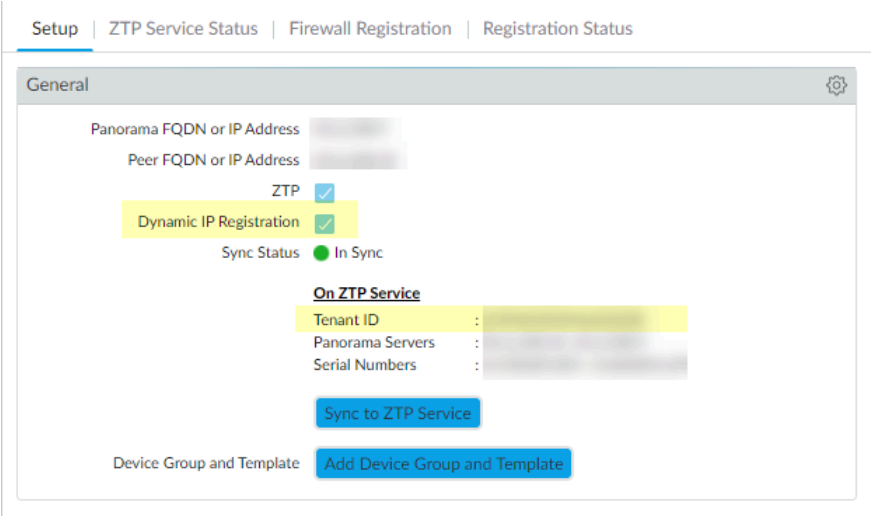
- PAN-OS 10.0.3 以降もしくは 11.1 リリース
- SD-WAN プラグイン 2.0.1 または以降の 2.0 リリース
- ZTP プラグイン 1.0.1 または以降の 1.0 リリースをダウンロード、インストールし、ZTP に関連する DDNS 用に設定します。Panorama が ZTP に登録済みであり、 ZTP サービスと通信している必要があります。
- アプリケーションと脅威コンテンツ リリース バージョン 8354 またはそれ以降のバージョン

- フル メッシュ DDNS に参加しているすべてのファイアウォールは、同じカスタマー サポート ポータル (CSP) アカウントで登録する必要があります。
- フル メッシュ DDNS に参加しているすべてのファイアウォールには、最新のデバイス証明書がインストールされている必要があります。ファイアウォール、Panorama、およびクラウド サービスを適切に認証することは、デバイス証明書、および CSP および ZTP サービスを必要とする重要なセキュリティ手順となります。
- Palo Alto Networksファイアウォールの前に発信トラフィックを制御するファイアウォールまたはその他のネットワーク デバイスがある場合は、DDNS 対応インターフェイスから次の FQDN へのトラフィックを許可するように、そのデバイスの設定を変更する必要があります:
  - https://myip.ngfw-ztp.paloaltonetworks.com/ (whatsmyIP サービスに到達するため)
  - https://ngfw-ztp.paloaltonetworks.com/ (DDNS 登録サービスに到達するため)

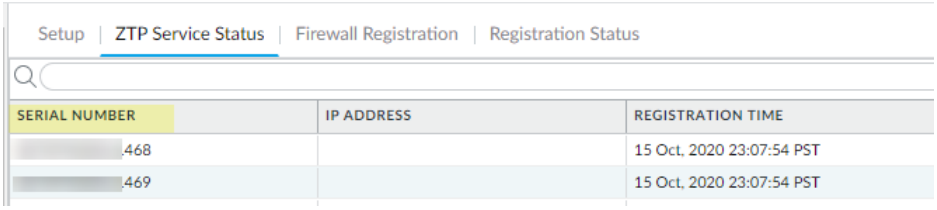
STEP 1 | Panorama およびハブまたはブランチであるすべてのマネージドファイアウォール用に最新のデバイス証明書をインストールします。

STEP 2 | ZTP プラグイン 1.0.1 をインストールして、ゼロタッチプロビジョニングをセットアップします。

1. Panorama 管理者ガイドで、ZTP Overview (ZTP の概要) をお読みください。
2. Install the ZTP Plugin (ZTP プラグインのインストール) を実行します。
3. Configure the ZTP Installer Administrator Account (ZTP インストーラ管理者アカウントの設定) を実行します。
4. **Panorama** > **Zero Touch Provisioning**（ゼロタッチプロビジョニング） > **Setup**（設定）の順に選択し、一般設定を編集して **Dynamic IP Registration (**ダイナミック **IP)** を有効化します。
5. **OK** をクリックします。一般設定は、テナント ID 番号を持つ On ZTP サービスを示します。



6. **ZTP Service Status (ZTP** サービスのステータス**)** を選択し、ファイアウォールのシリアル番号がリストに入っていることを確認します。



STEP 3 | これが未完了である場合は、SD-WAN プラグイン 2.0.1 または以降の 2.0 リリースをインストールします。

STEP 4 | Panorama で **Commit (**コミット**)** を実行します。

STEP 5 | Panorama Web インターフェイスへのログイン。

STEP 6 | VPN クラスタの作成に示すように、VPN アドレス プールを作成します。

STEP 7 | フル メッシュ VPN クラスタを作成します。

1. **Panorama** 、 > **SD-WAN** > **VPN Clusters (VPN** クラスタ**)** と選択します。
2. サーバーの**Mesh (**メッシュ**)** 対象の **Type**(タイプ) を選択します。
3. 相互に通信する必要のある **Branches (**ブランチ**)** を **Add (**追加**)** します。
4. (任意) メッシュ内のハブも希望する場合は、1 つ以上の **Hubs (**ハブ**)** を **Add (**追加**)** します。
5. **OK** をクリックします。

STEP 8 | **Commit (**コミット**)** および**Commit to Panorama (Panorama** へのコミット**)** を選択します。ファイアウォールに静的 IP アドレスがある場合、手順は完了しています。VPN メッシュのブランチ ファイアウォールまたはハブ ファイアウォールに DHCP または PPPoE インターフェースがある場合は、DDNS を使用する必要があるため、次の手順を続行してください。

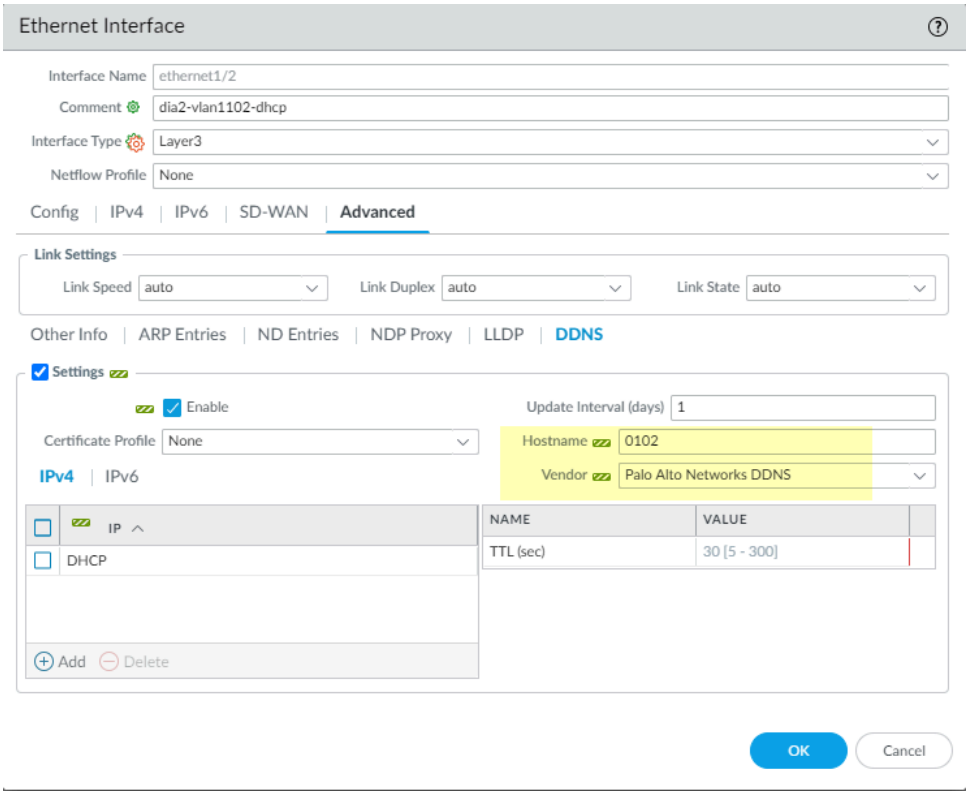
STEP 9 | **Network**（ネットワーク） > **Interfaces**（インターフェース） > **Ethernet**（イーサネット）の順に選択し、**Template**（テンプレート） フィールドで特定のブランチのテンプレート スタックを選択します。

STEP 10 | `Dynamic-DHCP Client` (ダイナミック DHCP クライアント) または PPPOE を示す IP アドレス インターフェースを選択し、画面最下部の **Override (**オーバーライド**)** をクリックし、**OK** をクリックして閉じます。

STEP 11 | DDNS 設定が設定されたことを Panorama 上で確認します。

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、同じインターフェースを再度選択します。
2. **Advanced** > **DDNS** の順に選択します。
3. DDNS 設定がインターフェース名に基づいた **Hostname (**ホスト名**)** で自動的に設定されたことと、**Vendor (**ベンダー**)** が `Palo Alto Networks DDNS` に自動的に設定された

ことを確認します。たとえば、Ethernet1/2 インターフェース上で、結果として生じるホスト名は「0102」です。



4. **OK** をクリックします。

STEP 12 | VPN クラスタに DHCP または PPPoE インターフェースを持つハブが含まれている場合は、ステップ 9～11 を繰り返しますが、**Template (テンプレート)** フィールドでは、特定のハブのテンプレートスタックを選択します。

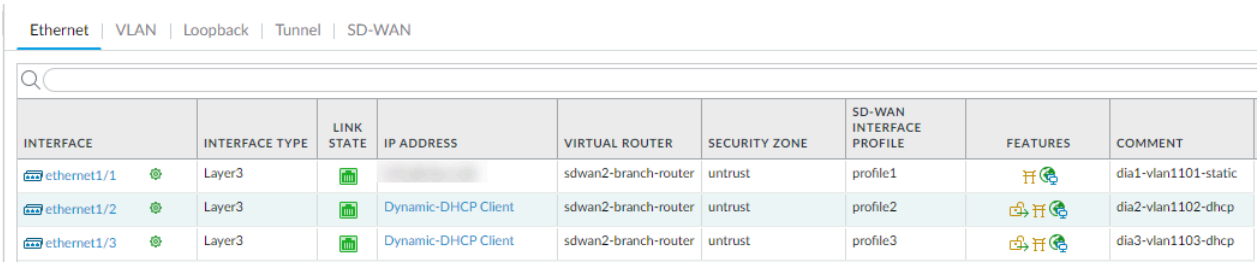
ハブがフル メッシュ クラスタになく、ハブ スポーク クラスタにある場合でも、ハブが *DHCP* または *PPPOE* を使用して *SD-WAN* インターフェースの *IP* アドレスを取得する場合は、オーバーライド手順を実行して *DDNS* を有効にする必要があります。

STEP 13 | Panorama に **Commit (コミット)** を実行し、**Push to Devices (デバイスにプッシュ)** します。

STEP 14 | ブランチ ファイアウォールで、ブランチが DDNS で設定されることを検証します。

1. ブランチ ファイアウォールにログインします。
2. **Network (ネットワーク)** > **Interfaces (イーサネット)** > **Ethernet (イーサネット)** の順に選択し、設定したイーサネット インターフェースを対象に、Features (機能) 列の

DDNS 情報アイコンをスクロールして、ベンダー、ホスト名、IP アドレス、およびその他のDDNS 情報を確認します。



STEP 15 | クラスタ内の別のブランチで、インターフェースのピア アドレスが DDNS 登録用にシステムで生成された FQDN であることを確認します。

1. 別のブランチにログオンして、**Network (**ネットワーク**) > Network Profiles (**ネットワークのプロファイル**) > IKE Gateways (IKE** ゲートウェイ**)** の順に選択します。
2. ピア アドレスが安全な名前であり、簡単に参照されず、会社情報が表示されないことを確認します。例えば0101.8ced8460fcc5177cd3665ce41b634533a15a612b8e52ec1d9ec057a582cb4.t13855f6c9a92

STEP 16 | ブランチとハブの FQDN を表示し、DDNS 情報を更新します。

1. CLI へのアクセスを行います。
2. その他のブランチおよびハブの FQDN (DDNS により生成されたもの) を表示する: **`show dns-proxy fqdn all`**
3. DDNS アドレスを更新する: **`request system fqdn refresh`**

SD-WAN のスタティック ルートの作成

BGP ルーティングに加え (または代わりとして) 、スタティック ルートを作成して SD-WAN トラフィックをルーティングすることができます。

スタティック ルートは、Panorama™ を使用するか、ファイアウォール ハブまたはブランチで直接設定することができます。Panorama を使用する場合、Configure a Template or Template Stack Variable (テンプレートまたはテンプレート スタック変数の設定) 手順を把握しておく必要があります。以下の手順の通り、スタティック ルートの宛先として使用する変数を作成します。（ネクストホップ用の変数を作成することもできます）。(ハブに向かう) スタティック ルートをブランチにプッシュします。(ブランチに向かう) スタティック ルートをハブにプッシュします。

STEP 1 | Panorama Web インターフェイスへのログイン。

STEP 2 | Configure a Template or Template Stack Variable (テンプレートまたはテンプレート スタック変数を設定) し、以下の形式で変数の **Name(名前)** を入力します。*$peerhostname_clustername.customname*。例えば、$branchsanjose_clusterca.10 or $DIA_cluster2.location3 と指定します。ドル記号 ($) 以降の要素は以下の通りです。

- *peerhostname*-スタティック ルートの宛先となる宛先ハブまたはブランチのホスト名。インターネットへのスタティック ルートの場合、peerhostname は、**DIA** と指定する必要があります。ピアのホスト名の代わりに、ピアのシリアル番号を使用することも可能です。ピアが HA ペアの一部である場合、2 台の HA ファイアウォールのいずれかのホスト名またはシリアル番号を使用することができます。
- *clustername*- 宛先ハブまたはブランチが属する VPN クラスタ名。
- *customname*-任意のテキスト文字列。カスタム名にピリオド (.) は使用できません。

同じピアに向かうスタティック ルートは、複数指定することができます。つまり、変数は同じ peerhostname や clustername を持つことが可能です。変数は、異なるカスタム名を使用して区別します。

STEP 3 | 変数 **Type** を **IP Netmask** に選択して、/でネットマスク長を表記した宛先 IP アドレスを入力します(例: 192.168.2.1/24)。IPv6の場合は、2001:DB8::/32のように、IPv6アドレスをスラッシュとプレフィックスの長さで入力します。

STEP 4 | **OK** をクリックして変数を保存します。

STEP 5 | **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。

STEP 6 | **[Static Routes (スタティックルート{]**を選択します。

STEP 7 | **IPv4**または**IPv6**を選択し、スタティックルートの名前を追加します。

STEP 8 | **Destination (宛先)** には、作成した変数を選択します。

STEP 9 | **Interface (インターフェース)** へ、テンプレートの中からインターフェースのみを含むものをドロップダウン リストから選択します (例: Ethernet1/1、Tunnel.x、または sdwan.xx)。

STEP 10 | **Next Hop**(ネクストホップ)には、**IP Address**(**IP** アドレス)または**IPv6 Address**(**IPv6** アドレス)を選択し、スタティックルートのネクストホップ (スタティックルートが向かうハブまたはブランチ) の IP アドレスまたは変数を入力します。

STEP 11 | **OK** をクリックします。

STEP 12 | 変更内容を、**Commit** (コミット)および**Commit and Push** (コミットおよびプッシュ) します。

Auto VPN 設定により、スタティック ルートの [Interface](インターフェース) フィールドの **sdwan** キーワードは、宛先変数に基づいて決定する出口仮想 SD-WAN インターフェースに置き換えられます。そのため、ルーティング テーブルのスタティック ルートでは、識別される VPN クラスタのピアホストに向かうトラフィックが仮想 SD-WAN インターフェースを出て、指定された以下のホップに到達することが示されます。

STEP 13 | リターン トラフィックのスタティック ルートを設定します。

SD-WAN の高度なルーティングの設定

高度なルーティングエンジンにより、ファイアウォールは拡張し、大規模なデータセンター、ISP、企業、およびクラウドユーザーに安定した高性能で可用性の高いルーティング機能を提供できます。高度なルーティングエンジン は業界標準の構成方法に依存しているため、管理者のタスクが容易になります。これにより、さまざまな機能(フィルタリング、再配布、メトリックの変更など)に使用されるプロファイルを作成でき、すべての論理ルーターで使用できます。これらのプロファイルは、各ダイナミック ルーティング プロトコルのルートをフィルタリングするためのより細かい粒度を提供し、複数のプロトコル間でのルートの再配布を改善します。

概念的には同等ですが、高度なルーティング エンジンは、仮想ルーターではなく論理ルーターを使用してルーティング ドメインをインスタンス化します。

仮想ルーターとは異なり、論理ルーターはデフォルトでは作成されません。ルーティング機能を設定する前に作成する必要があります。

ネットワーク要件に基づいて、高度なルーティング エンジンまたはレガシー エンジンを使用できます。

- 高度なルーティングを有効にすると、論理ルーターが作成され、高度なルーティング エンジンがルーティングに使用されます。
- 高度なルーティング を無効にすると、仮想ルーターが作成され、ルーティングにレガシ エンジンが使用されます。

高度なルート エンジンは、複数の論理ルータ(レガシー ルート エンジンでは仮想ルータと呼ばれます)をサポートします。高度なルート エンジンには、より便利なメニュー オプションがあり、BGP ピア グループやピアなどに適用されるプロファイル(認証、タイマー、アドレス ファミリ、または再配布プロファイル)で簡単に設定できる BGP 設定がさらにあります。

高度なルーティングエンジンは、スタティック ルート、MP-BGP、OSPFv2、OSPFv3、RIPv2、プロトコル独立マルチキャスト スパース モード(PIM-SM)、PIM 送信元固有マルチキャスト(SSM)、BFD、再配布、RIB へのルート フィルタリング、アクセス リスト、プレフィックス リスト、およびルート マップをサポートします。

SD-WAN で高度なルーティングエンジンを設定するには、次のものが必要です。

プラットフォーム	PAN-OS リリースを実行しているファイアウォール	SD-WAN プラグイン
Panorama™	11.1 以降	3.1.0 以降

SD-WAN プラグインは、高度なルーティングオプションの値に基づいて論理ルーターまたは仮想ルーターを作成します。高度なルーティングを有効にすると、論理ルーターが作成されます。それ以外の場合は、仮想ルータが作成されます。

テンプレートスタックで高度なルーティングを有効にし、Panorama コミットを実行して firewall にプッシュすると、SD-WAN プラグインは移行スクリプトを実行して、論理ルーターに

SD-WAN 関連オブジェクト(スタティック、インターフェイス、再配布プロファイル、BGP)を作成します。移行スクリプトは、同じテンプレートの仮想ルーター名と同じ論理ルーター名を作成します。したがって、ハブとブランチは常に同じルーター名を持ちます。

移行後、*Panorama* では移行された仮想ルーターを削除することはできません。

Panorama SD-WAN プラグイン 3.1.0 は、高度なルーティングエンジンを使用して firewall を同時に管理し、レガシールーティングエンジンを使用してファイアウォールを同時に管理できます。この利点は、選択した管理対象ファイアウォールを新しい高度なルーティング エンジンに移行しながら、他のルート エンジンの現在の従来のルーティング エンジン構成を維持できることです。

SD-WAN プラグイン 3.1.0 はルーティングエンジンに関係なくファイアウォールを管理しますが、管理対象のファイアウォールで一度に有効にできるルーティングエンジン設定は 1 つだけです。**Advanced Routing** オプションを使用して、アドバンスド ルーティング エンジンを有効または無効にすることができます。ファイアウォールが使用するエンジンを変更するたびに (アドバンスト エンジンまたはレガシー エンジンにアクセスするためにアドバンスト ルーティングをそれぞれ有効または無効にします)、変更を有効にするには、設定をコミットし、ファイアウォールを再起動する必要があります。

高度なルート エンジンに切り替える前に、現在の構成のバックアップを作成してください。同様に、アドバンストルーティングを有効または無効にするテンプレートスタックを使用して *Panorama* を設定した場合、テンプレートスタックをコミットしてデバイスにプッシュした後、変更を有効にするためにテンプレートスタック内のデバイスを再起動する必要があります。

Panorama を設定するときは、すべて同じ詳細ルーティング設定(すべて有効またはすべて無効)を使用するデバイスのデバイスグループとテンプレートスタックを作成します。*Panorama* は、アドバンストルーティングが有効になっている構成を、アドバンストルーティングをサポートしていない小さな ファイアウォールにプッシュしません。これらの ファイアウォールでレガシーな構成が存在する場合、*Panorama* は古い設定をプッシュします。

適切な SD-WAN プラグインと PAN-OS バージョンにダウングレードし、仮想ルータを使用する場合は **Advanced Routing** を無効にしてください。SD-WAN プラグインをダウングレードするときに、**Advanced Routing** が無効になっている (この場合は仮想ルーターが作成されている) 別のテンプレートを使用します。

Advanced Routing を構成していて、仮想ルーターに切り替える場合は、Advanced Routing を無効にして、以前に保存した仮想ルーター構成に戻します。PAN-OS および SD-WAN プラグイン バージョンのダウングレードなどのダウングレード手順を実行する前に、高度なルーティングを無効にした後、ファイアウォールに加えられた変更をコミットしてプッシュします。

高度なルーティングを有効にする場合は、SD-WAN インターフェイスを同じ論理ルーターに設定する必要があります。論理ルーター間で分割することはできません。

STEP 1 | Panorama Web インターフェイスへのログイン。

STEP 2 | Panorama を 11.1 へとアップグレードし and SD-WAN plugin 3.1.0.をインストールします。

STEP 3 | ハブおよびブランチファイアウォールを管理デバイスとして Panorama™ 管理サーバーに追加します。

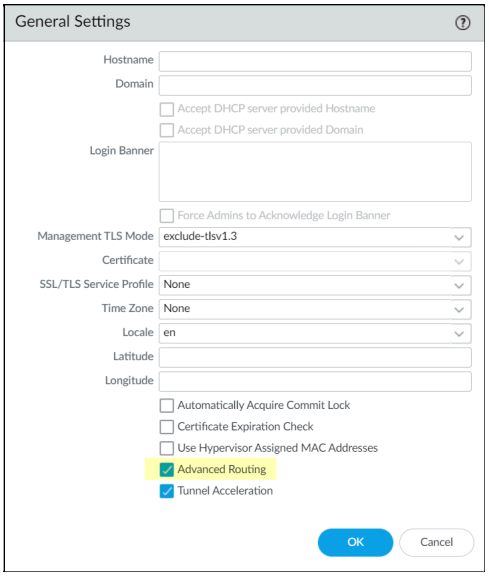
STEP 4 | アドバンスドルーティングを有効にする前に、現在の構成のバックアップを作成してください。

STEP 5 | **Device** セクションで、**Template** コンテキスト ドロップダウンから適切なテンプレート スタックを選択します。

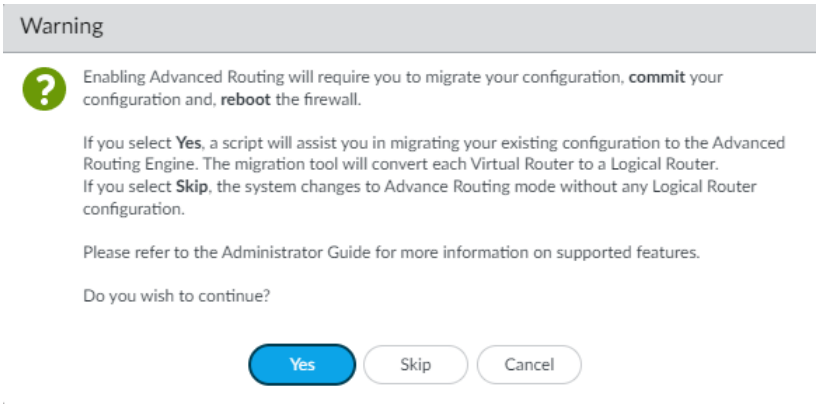
STEP 6 | アドバンストルーティングエンジンの有効化.

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. **Advanced Routing** を有効にします。SD-WAN プラグインは、高度なルーティングオプションの値に基づいて論理ルーターまたは仮想ルーターを作成します。高度なルーティ

ングを有効にすると、論理ルーターが作成されます。それ以外の場合は、仮想ルーターが作成されます。

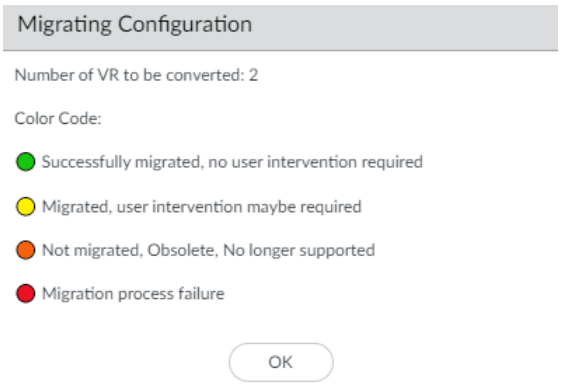


3. **OK** をクリックします。
4. 移行に関する警告メッセージが表示されます。続行するには **Yes** をクリックします。

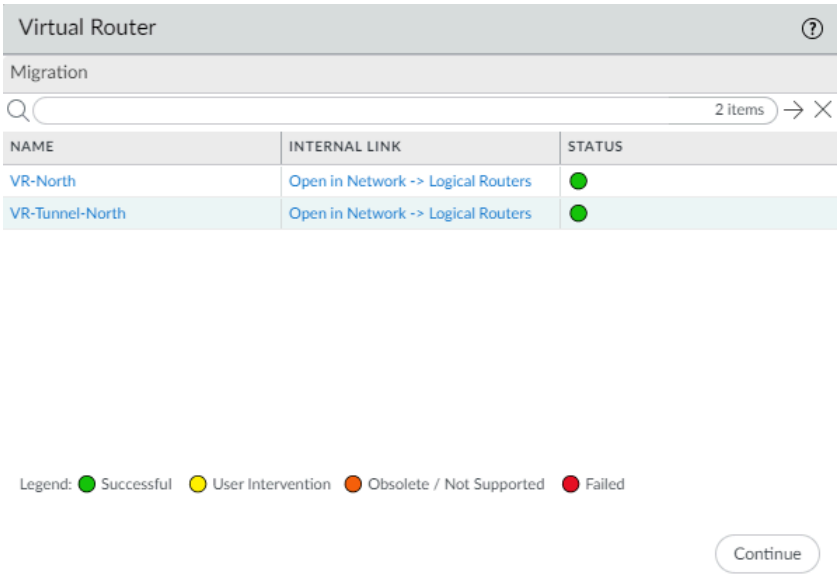


Yes をクリックすると、組み込みの移行スクリプトによって既存の構成が高度なルーティング エンジンに移行されます。**Skip** を選択すると、高度なルーティング エンジン用に空の構成が作成されます。

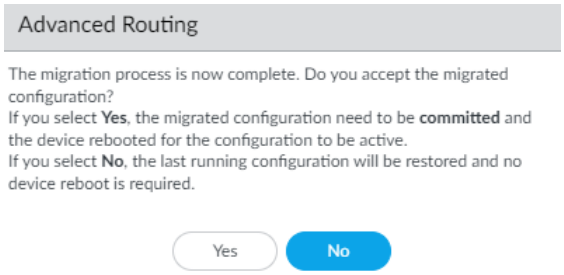
移行構成 には、移行状態を示すカラー コードが表示されます。



Virtual Router で、テンプレート スタック内のテンプレートの **STATUS** を確認します。移行を成功させるには、**STATUS** が緑色になっている必要があります。それ以外の場合は、移行に成功しなかったテンプレートに対して必要なアクションを実行します。



移行が成功すると、各仮想ルーターが対応する論理ルーターに自動的に変換されます。変更を有効にするには、構成をコミットし、ファイアウォールを再起動する必要があります。



5. [コミット] します。
6. **Device** > **Setup** > **Operations** を選択し、 **Reboot Device** を実行します。

STEP 7 | **Commit** > **Commit to Panorama** and **commit** を選択します。

STEP 8 | 構成の変更をコミットし、管理対象のファイアウォールにプッシュします。デバイスにプッシュ を選択して、選択した SD-WAN firewall に追加された論理ルーターを表示します。

1. **Commit**（コミット） > **Push to Devices**（デバイスへのプッシュ）の順に選択し、**Edit Selections**（選択内容の編集）を行います。
2. **Templates** を選択し、リストからテンプレート スタックとテンプレートを選択します。
3. **Force Template Values** を有効にして、更新されたテンプレート値でローカル構成を上書きします。このオプションを使用する前にファイアウォールのオーバーライドされた値をチェックし、コミットによって予期せぬネットワークの障害が発生したり、これらのオーバーライドされた値によって問題が生じたりしないことを確認してください。
4. **OK** および **Push** をクリックしてデバイスに接続します。

STEP 9 | その後、ファイアウォールに再度ログインします。

STEP 10 | **Network** を選択します。

従来のメニューの1つの項目 (Virtual Routers) よりも業界標準的で、より詳細なメニュー項目に注目してください。**Routing** には、**Logical Routers** と **Routing Profiles** が含まれ、これには **BGP**、**BFD**、**OSPF**、**OSPFv3**、**RIPv2**、**Filters**、**Multicast** が含まれます。

STEP 11 | 設定に複数のテンプレートスタックがある場合は、テンプレートスタックごとに **Advanced Routing** を個別に有効にする必要があります。アドバンストルーティング用に更新する予定のファイアウォール上の他のテンプレート スタックに対して、手順 5 から 10 を繰り返します。

設計要件に従って、高度なルーティング エンジンを使用する場合、論理ルーター名は同じテンプレートの仮想ルーター名と同じである必要があります。つまり、ハブとブランチのルーター名は常に同じです。移行スクリプトを使用せずに論理ルーターを手動で作成する場合は、論理ルーター名と仮想ルーター名が同じであることを確認する必要があります。

STEP 12 | SD-WAN 展開で仮想ルーターまたは論理ルーターを選択します。

Panorama > **SD-WAN** > **Devices**を選択し、 Panorama 管理サーバーによって管理される SD-WANデバイス(SD-WAN ハブまたはブランチファイアウォール) を追加します。

SD-WAN デバイスを追加するための既存の構成オプションに加えて、**Router Name** の論理ルーター (高度なルーティングエンジンの場合) または仮想ルーター (レガシーエンジンの場合) を選択できるようになりました。高度なルーティング エンジンを使用する場合は、論理ルーター名と仮想ルーター名が同じテンプレートで同じであることが重要です。

SD-WAN ハブとブランチ間のルーティングに使用する **Router Name** (論理ルーターまたは仮想ルーター) を選択します。

- 仮想ルーター名と論理ルーター名が同じ場合、**Router Name** には 1 つの名前が表示されます。
- 仮想ルーター名と論理ルーター名が異なる場合、**Router Name** には仮想ルーター名と論理ルーター名の両方が表示されます。要件に基づいて、仮想ルーター (レガシー エンジンの

場合) または論理ルーター (高度なルーティング エンジンの場合) のいずれかを選択できます。

モニタリングおよびレポート

VPN クラスタのアプリケーションおよびリンクのヘルス ステータスレポートを監視および生成し、問題を特定し、解決します。Panorama 管理サーバーが SD-WAN アプリケーションとリンクの正常性情報を表示するには、SD-WAN ファイアウォールがデバイス監視データを Panorama™ にプッシュし、SD-WAN ファイアウォールの管理対象デバイスとしての追加時に Configure ログ転送を Panorama にプッシュできるようにする必要があります。ログの Panorama 転送を SD-WAN ファイアウォールで設定していない場合、SD-WAN **Monitoring (**モニタリング**)** は、アプリケーションまたはリンクのヘルス情報は表示しません。

Panoroma が *SD-WAN* モニタリング データを収集するには、*SD-WAN* 設定を *Panorama* から *SD-WAN* ファイアウォールにプッシュする必要があります。*SD-WAN* モニタリング データが表示されない場合は、*SD-WAN* 設定が正常にプッシュされたことを確認してください。

- SD-WAN タスクの監視
- SD-WAN アプリケーションおよびリンクパフォーマンスの監視
- Prisma Access Hubの監視
- SD-WAN レポートの生成

SD-WAN タスクの監視

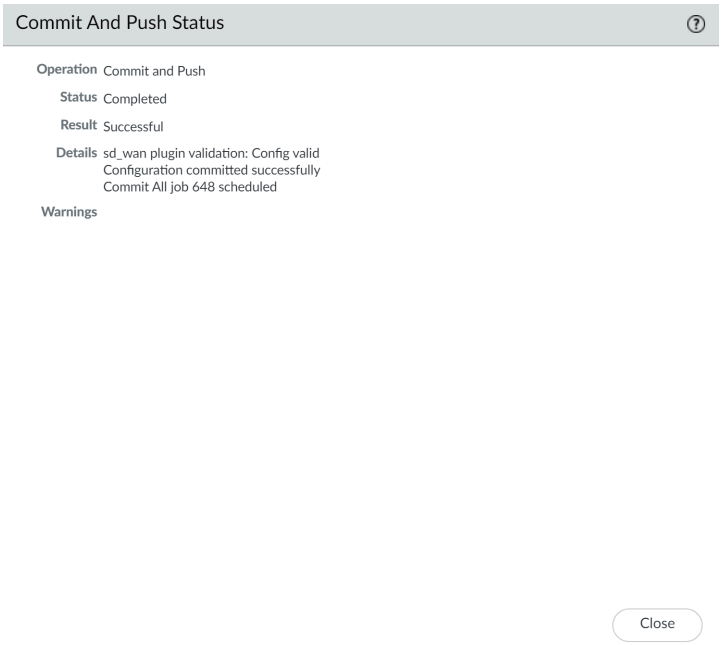
Panorama™ 管理サーバーから実行されたコミット、プッシュ、その他の SD-WAN タスクを監視し、特定のタスクに関する分析情報および詳細情報を取得します。

タスクが警告付きで正常に完了または失敗した場合は、詳細な警告および説明を表示させて、設定ミスの解決方法をよりよく把握することができます。さらに、最新のプッシュ状態の詳細を表示させ、タスクの警告またはエラーの原因に関する詳細情報を確認することができます。

STEP 1 | Panorama Web インターフェースにログインします。

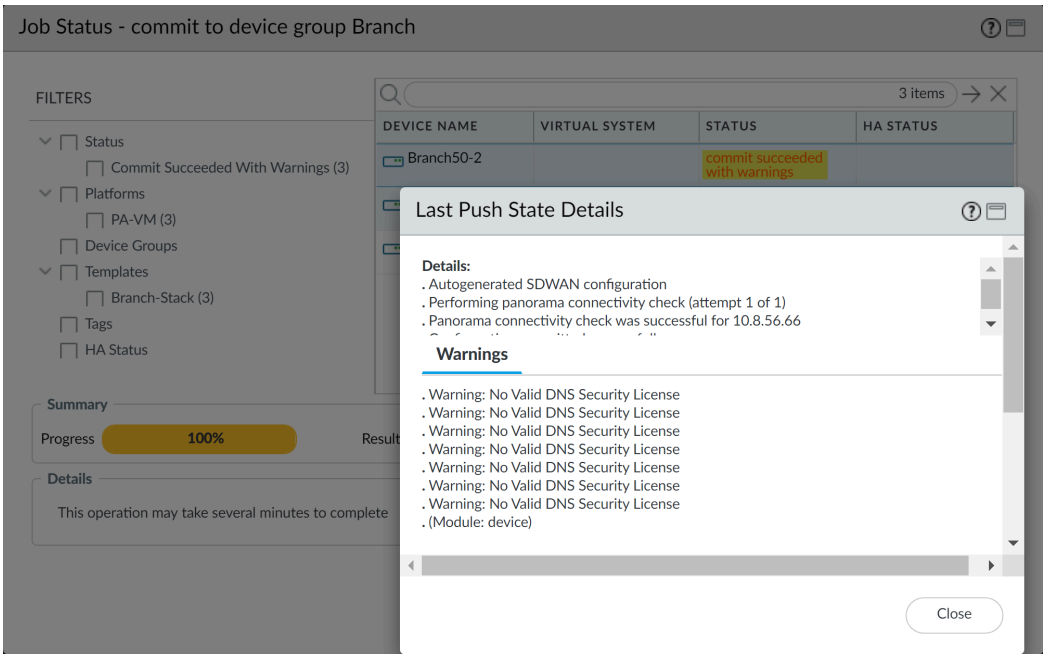
STEP 2 | SD-WAN 設定の編集後、変更内容を **Commit (コミット)** してジョブのステータスを表示させます。

ジョブ ステータス ウィンドウには、実行された操作、結果、およびジョブ ステータスに関する詳細および警告が表示されます。



STEP 3 | 警告付きで完了したジョブまたは失敗したジョブの最新のプッシュ詳細を表示させます。

1. Web インターフェースの下部にある **Tasks(**タスク）(Tasks) をクリックして、Task Manager (タスク マネージャ) を開きます。
2. SD-WAN タスクのジョブ **Type (**タイプ**)** をクリックします。
3. タスクの最新のプッシュ状態の詳細を表示するには、ジョブ **Status (**ステータス**)** をクリックします。
4. 最新のプッシュ状態の詳細を確認して設定の問題を特定し、解決します。



SD-WAN アプリケーションおよびリンクパフォーマンスの監視

VPN クラスタ内のアプリケーションおよびリンクのパフォーマンスを監視して、すべての VPN クラスタ全体のサマリー情報を表示し、引き続きドリルダウンして、影響を受けるサイト、アプリケーション、リンクへの問題を特定し、問題のトラブルシューティングを行います。SD-WAN トラフィックの可視性は、トラフィックを受信する SD-WAN ファイアウォールに表示されます。たとえば、ハブ ファイアウォールからブランチ ファイアウォールへのトラフィックの場合、SD-WAN モニタリング データはブランチ ファイアウォールに反映されます。ランディング ダッシュボードには以下が表示されます。

- App Performance (アプリのパフォーマンス)
  - **Impacted (影響あり)**-ファイアウォールが選択可能なパスのリストのパス品質プロファイルで指定されたしきい値を満たす、ジッター、遅延、またはパケット損失のパフォーマンスがパスにない VPN クラスタ内の 1 つまたは複数のアプリケーション。
  - **OK**-ジッター、遅延、またはパケット損失のパフォーマンスの問題が発生していない VPN クラスタ、ハブ、およびブランチの数。
- Link Performance (リンクのパフォーマンス)
  - **Error (エラー)**-VPN クラスタ内の 1 つまたは複数のサイトに、トンネルまたは仮想インターフェース (VIF) のダウン等の接続の問題があります。
  - 警告–帯域幅（SD-WAN プラグイン 3.3.0 以降のリリースの PAN-OS 11.2.0 でサポート）、帯域幅（SD-WAN プラグイン 3.2.2 以降のリリースの PAN-OS 11.1.5 でサポート）、ジッタ、遅延、またはパケット損失のパフォーマンス測定値がメトリックの移動 7 日間の平均値を超えるリンクを持つ VPN クラスタ、ハブ、ブランチの数。
  - **OK**–帯域幅（SD-WAN プラグイン 3.3.0 以降のリリースの PAN-OS 11.2.0 でサポート）、帯域幅（SD-WAN プラグイン 3.2.2 以降のリリースの PAN-OS 11.1.5 でサポート）、ジッタ、遅延、またはパケット損失のパフォーマンス測定値がない VPN クラスタ、ハブ、ブランチの数。

  PAN-OS 11.2.0以降、SD-WANプラグイン3.3.0以降のリリースでは、リンクパフォーマンスの主要な測定基準である「帯域幅」をサポートしています。PAN-OS 11.1.5以降、SD-WANプラグイン3.2.2以降のリリースでは、リンクパフォーマンスの主要な測定基準である「帯域幅」をサポートしています。

ハブ ファイアウォールまたはブランチ ファイアウォールに、前方誤り訂正で設定された SD-WAN ポリシー ルールがある場合は、 `Error Correction Initiated (エラー訂正を開始しました)` というメッセージが表示され、ハブ ファイアウォールまたはブランチ ファイアウォールがアプリケーションの送信データのエラーを検出して修正したことを通知します。

SD-WAN ハブは、トラフィックが SD-WAN ハブから SD-WAN ブランチに発信され、エラー訂正プロファイルがアタッチされた SD-WAN ポリシールールと一致した場合にのみ、`Error Correction Initiated (エラー修正を開始しました)` というメッセージを表示します。

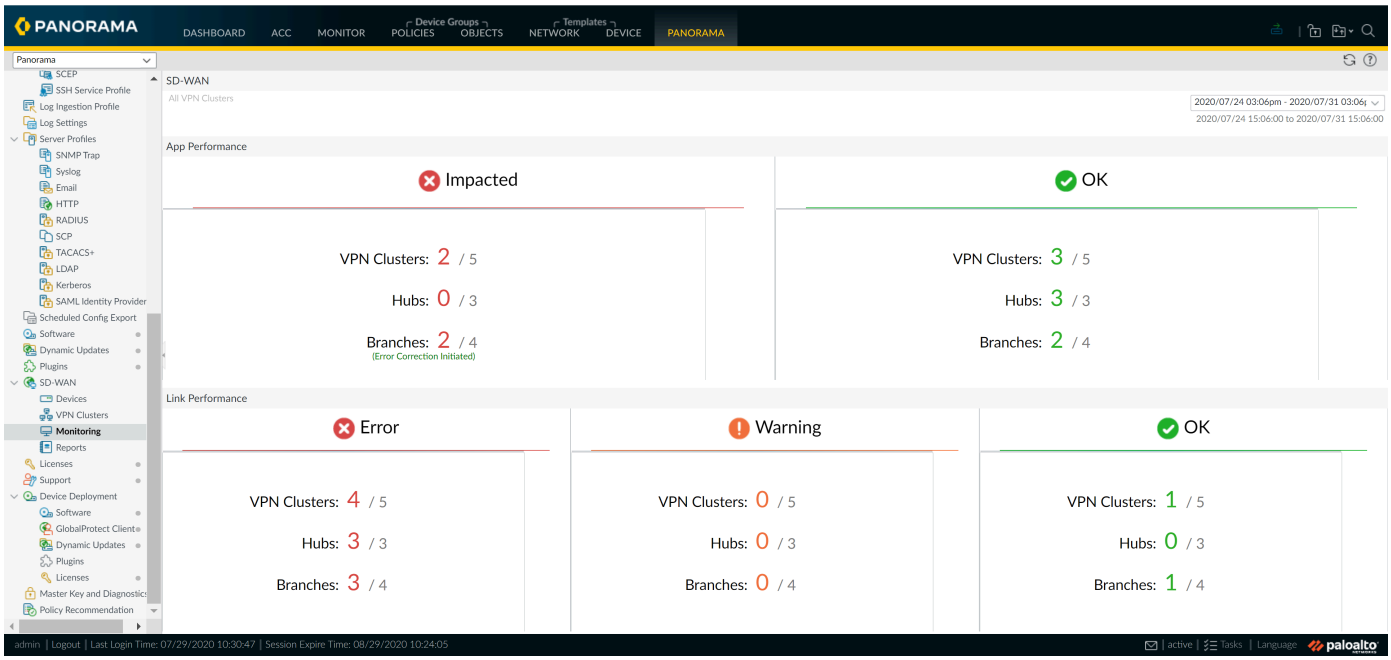
ランディング ダッシュボードから、エラーまたは警告ステータスのある、影響を受けたアプリケーションまたはリンクへとビューを絞り込みます。次に、影響を受けたサイトを選択し、サイト レベルの詳細を表示します。サイトから、アプリケーション レベルまたはリンク レベルの詳細を表示します。

Prisma Access Hub アプリケーションとリンクのパフォーマンスを監視するPrisma Accessハブのアプリケーションとリンクのパフォーマンスを監視するにはを参照してください。

データが存在しない場合、または *SD-WAN* が未定義であることを示す画面が表示される場合は、使用している *Panorama* リリースが使用しようとしている *SD-WAN* プラグインリリースをサポートしていることを、互換性マトリックスで確認してください。

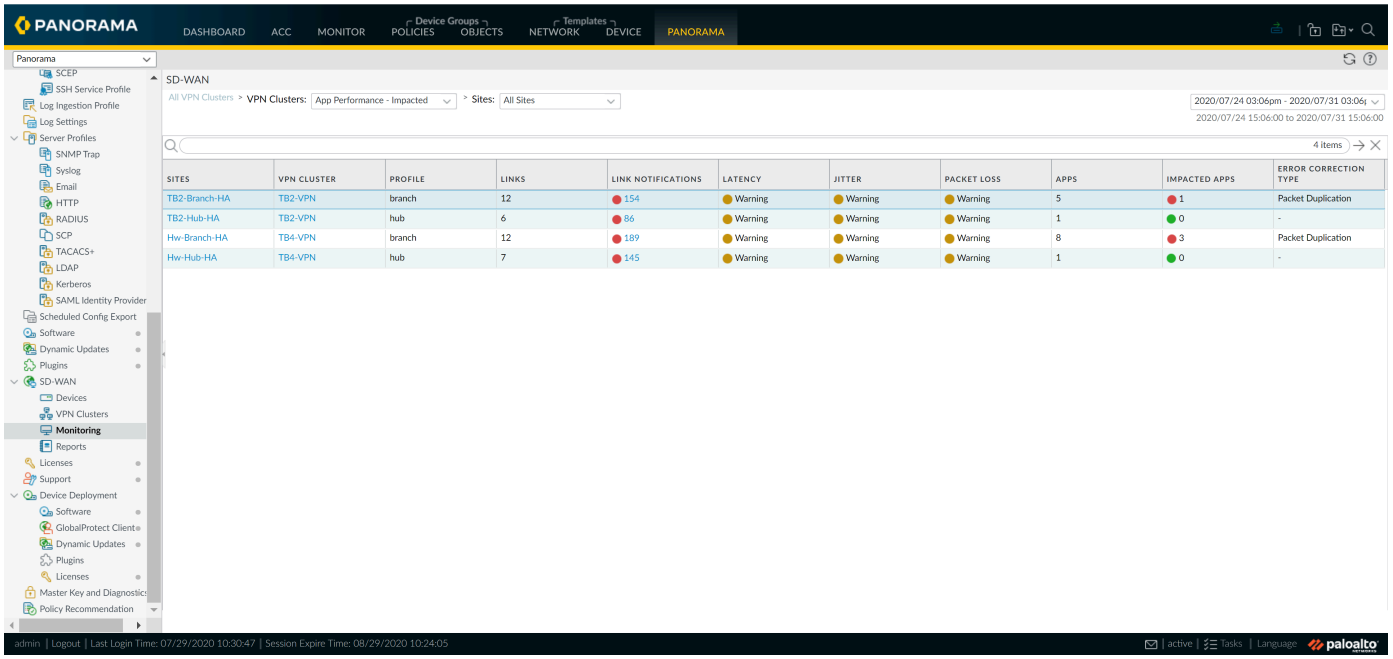
STEP 1 | Panorama Web インターフェイスへのログイン。

STEP 2 | **Panorama** 、 **> SD-WAN** 、 **> Monitoring(モニタリング)** と選択し、VPN クラスタ、ハブ、およびブランチのヘルス ステータスの概要を確認します。



STEP 3 | ［App Performance］または［Link Performance］の概要をクリックすると、［Impacted］、［Error］、［Warning］のカウントが表示され、帯域幅（リンクパフォーマンスについてはSD-WANプラグイン3.3.0以降のリリースのPAN-OS 11.2.0でサポート）、帯域幅（SD-WANプラグイン3.2.2以降のリリースのPAN-OS 11.1.5以降でサポート）、遅

延、ジッター、パケット損失に基づくサイトとそのステータスの詳細なリストが表示されます。



STEP 4 | Warning (警告) または Error (エラー) が表示されたサイトをクリックして、個々の VPN クラスタを表示させます。サイトデータには、影響を受けたアプリケーションを含め、App Performance (アプリのパフォーマンス) および Link Performance (リンクのパフォーマンス) が表示されます。さらに、サイト フィルタを使用して、リンク通知、遅延偏差、ジッター偏差、パケット損失偏差、あるいは影響を受けたアプリケーションに基づき VPN クラスタを表示させます。

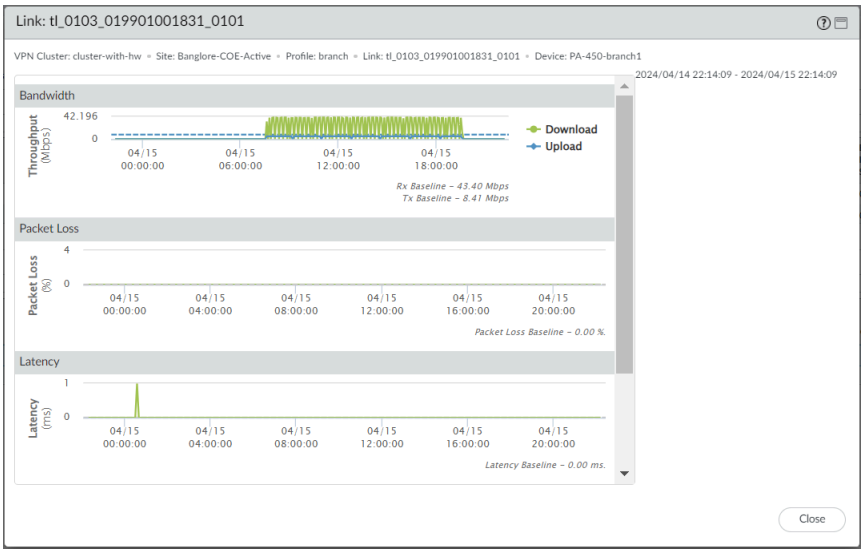
（SD-WANプラグイン3.3.0以降のPAN-OS 11.2.0 ） （ PAN-OS 11.1.5以降のSD-WANプラグイン3.2.2以降のリリース） VPNクラスタ内の選択したサイトの新しいリンクパフォーマンスパラメータ、最大アップロード/ダウンロード速度を表示できるようになりました。

各リンクをクリックすると、トンネルで測定されたベースライン帯域幅（SD-WANプラグイン3.3.0以降のリリースのPAN-OS 11.2.0でサポート）、帯域幅（SD-WANプラグイン3.2.2以降のリリースのPAN-OS 11.1.5でサポート）、ジッタ、パケット損失、および遅延が表示されます。

（SD-WANプラグイン3.3.0以降のPAN-OS 11.2.0 ） （ PAN-OS 11.1.5以降のSD-WANプラグイン3.2.2以降のリリース） 帯域幅グラフは、物理リンクとトンネルリンクのローリング最大アップロードおよびダウンロード速度を示します。

- 物理リンクの場合、グラフにはSD-WANインターフェイスプロファイルの設定（設定されている場合）が最大値として表示されます。それ以外の場合は、物理リンクがこれまでに確認した Tx と Rx の最大値が最大値としてグラフに表示されます。

- トンネルリンクの場合、グラフにはトンネルがこれまでに確認した Tx と Rx の最大値が最大値として表示されます。



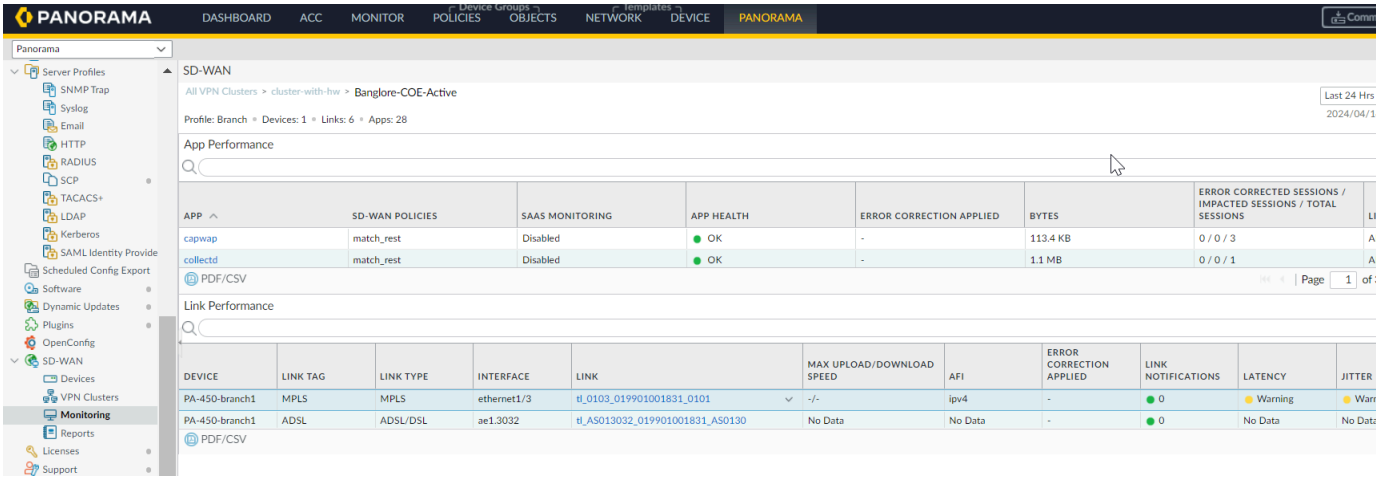
ダイレクト インターネット アクセス (DIA) リンク上の SaaS アプリケーション用に、**SaaS Monitoring (SaaS** モニタリング**)** 列は、アプリが SaaS Quality (SaaS 品質) プロファイルで作成され、1 つ以上の SD-WAN ポリシー ルールに関連付けられているかどうかを示します。

- `Disabled` (無効)–アプリは SaaS 品質プロファイルで設定された SaaS アプリケーションではありません。
- `Enabled`–アプリは SaaS 品質プロファイルで構成された SaaS アプリケーションであり、1 つ以上の SD-WAN ポリシーに関連付けられています。

アプリケーション用にエラー訂正プロファイルを SD-WAN ポリシー ルール と関連付けた場合、**Error Correction Applied (**エラー訂正適用済み**)** 列には、エラー訂正が適用されたことと、エラー修正の種類が表示されます。また、指定された時間枠のセッションの総数のうち、ブランチ ファイアウォールまたはハブ ファイアウォールによってエラー修正されたセッションの数を理解するために、**Error Corrected Sessions (**エラー訂正済みのセッション**)/**

Impacted Sessions (影響を受けたセッション)/**Total Sessions** (セッション合計) を閲覧することができます。

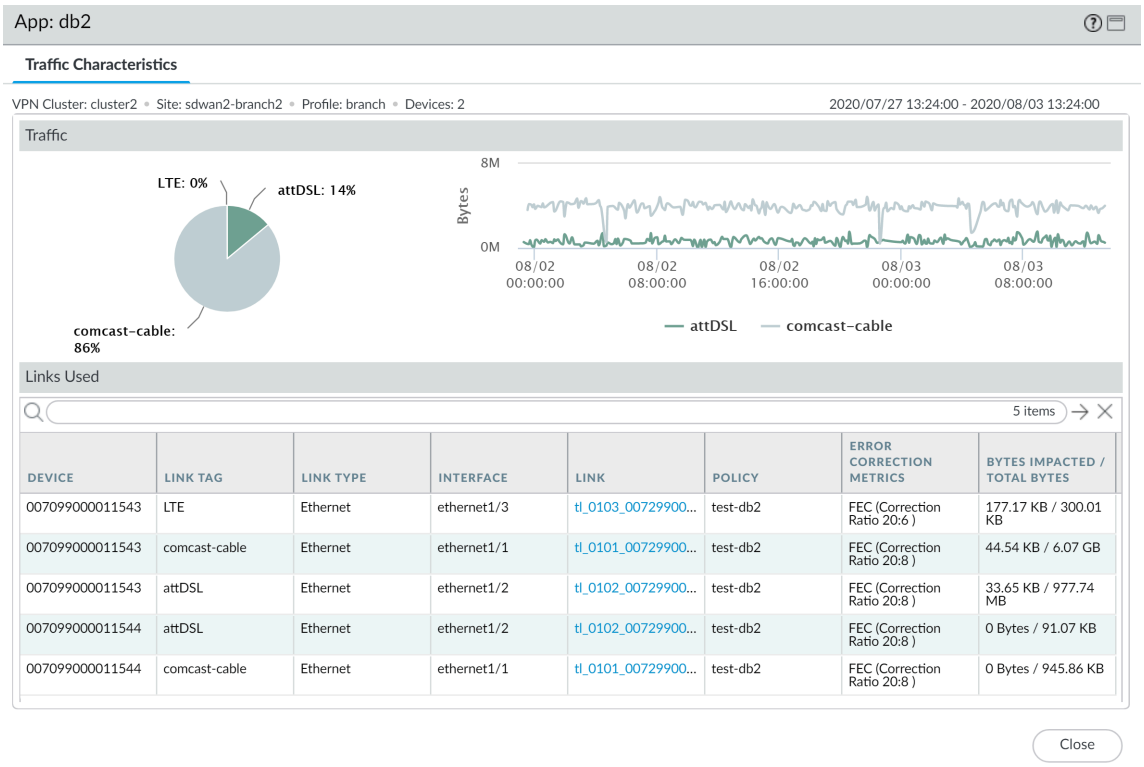
サイトのアプリケーションおよびリンクの詳細なヘルス情報を PDF または CSV 形式でエクスポートするには、**PDF/CSV** をクリックします。

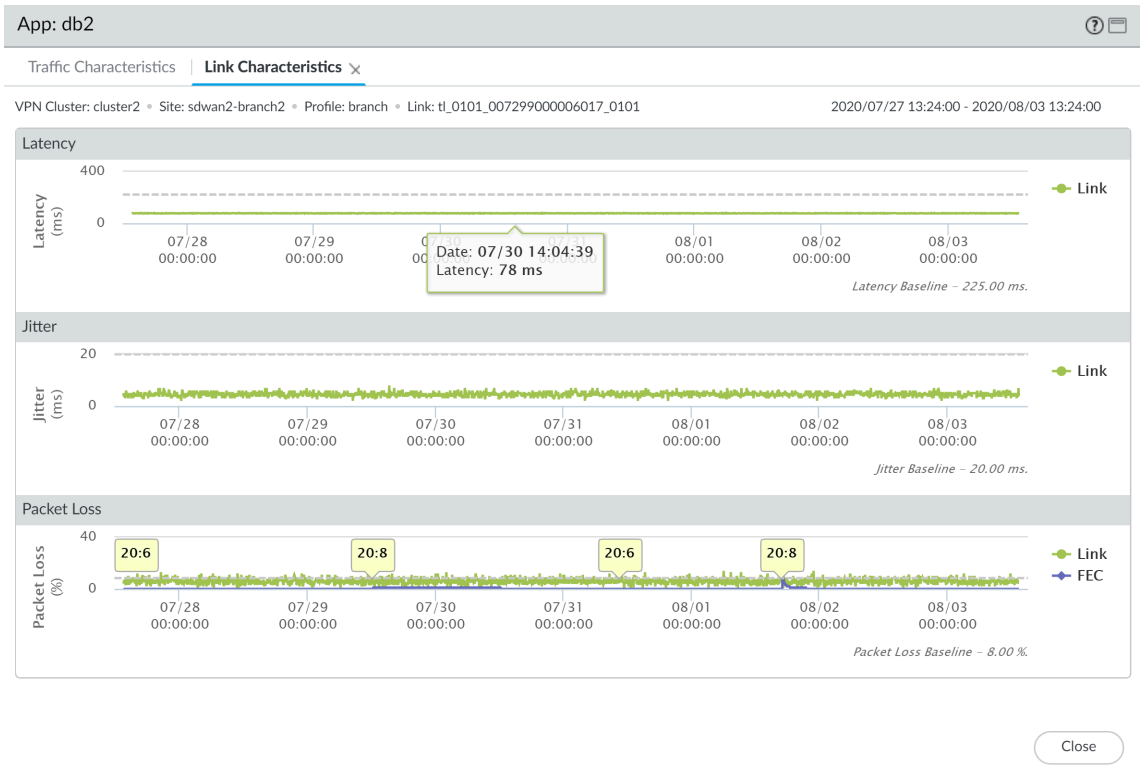


STEP 5 | 注意が必要なアプリケーションがあるブランチまたはハブをクリックします。

STEP 6 | アプリケーション レベルまたはリンク レベルの詳細を表示するには、影響を受けたアプリケーションをクリックします。

たとえば、アプリケーションのリンク特性を表示して、指定されたリンクでのアプリケーションの遅延、ジッタ、およびパケット損失を理解します。また、該当のリンクに対してエラー訂正が適用されたかを閲覧できます。





Prisma Access Hubの監視

Prisma Access Hub アプリケーションとリンクのパフォーマンスをベースライン化および監視して、SD-WAN リンク管理プロファイルを構成および変更する方法を理解します。

- Prisma Access Hubアプリケーションとリンクのパフォーマンスをベースライン化
- Prisma Access Hub アプリケーションとリンクのパフォーマンスを監視する

Prisma Access Hubアプリケーションとリンクのパフォーマンスをベースライン化

SD-WAN リンク管理プロファイルの設定する前に、P1alo Alto Networksは、Prisma Access Hubアプリケーションとリンクパフォーマンスのベースラインを設定して、Prisma Access Hubの通常のペイロードアクティビティをよりよく理解し、不要なアプリケーションとトラフィックの不要なリンクスワッピングを回避することをお勧めします。

STEP 1 | Panorama Web インターフェイスへのログイン。

STEP 2 | 「オンボードPAN-OS ファイアウォールからPrisma Accessへ」を行います。

STEP 3 | **Panorama** > **SD-WAN** > **Monitoring** を選択し、SD-WAN モニタリングの時間範囲を変更します。

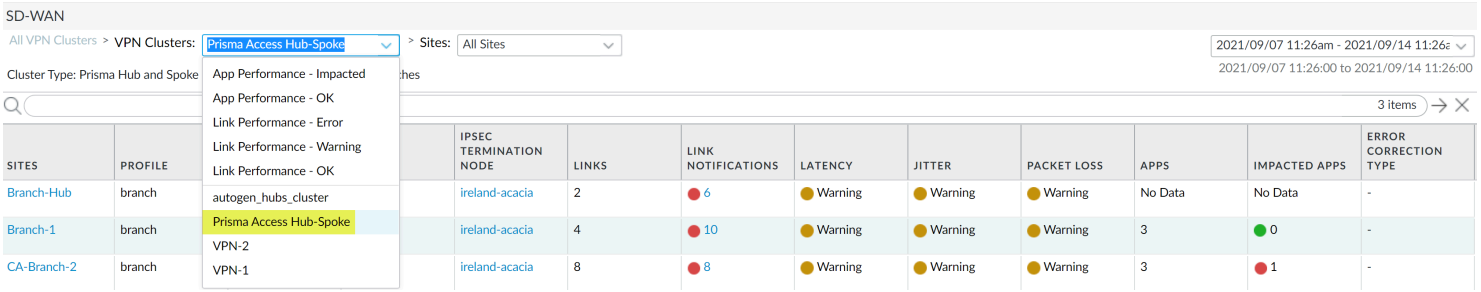
Prisma Access Hub アプリとリンクのパフォーマンスのベースラインに使用する期間が長いほど、ベースラインはより正確になります。少なくとも 3 日分のアプリとリンクのパフォーマンスを使用して、SD-WAN リンク管理プロファイルの作成に使用するレイテンシー、ジッター、パケット損失のデータをベースライン化します。

*Palo Alto Networks*は、*Prisma Access Hub*のレイテンシー、ジッター、パケット損失をベースライン化するために、7日間のアプリとリンクのパフォーマンスデータを評価することを推奨しています。

STEP 4 | SD-WAN モニタリングをフィルタリングして、プリズマアクセスハブスポーク VPN クラスターのみを表示します。

1. Impacted (影響あり)、Error (エラー)、または Warning (警告) の数を示す App Performance (アプリのパフォーマンス) または Link Performance (リンクのパフォーマンス) のサマリーをクリックして、遅延、ジッター、およびパケット損失に関するサイトおよびそのステータスの詳細なリストを表示します。
2. VPN クラスター フィルターで、**Prisma Access Hub-Spoke** を選択します。

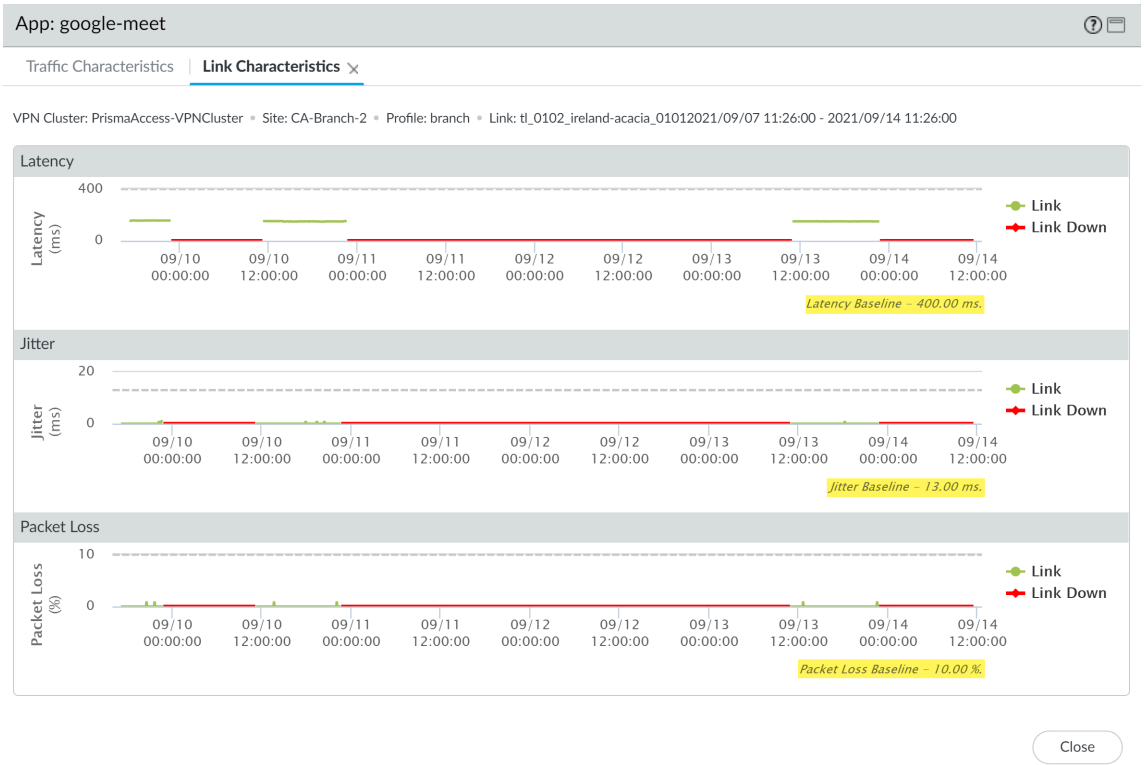
3. サイトをクリックすると、Prisma Access Hubの正常性の詳細が表示されます。



STEP 5 | Prisma Access Hub アプリケーションのリンク特性を確認します。

1. App Performance セクションでアプリケーションをクリックして、トラフィック特性とアプリケーション トラフィックに使用されるリンクを表示します。
2. 各リンクをクリックすると、リンク全体で測定されたアプリケーションのベースライン遅延、ジッター、およびパケット損失が表示されます。

   Prisma Access Hub パス品質プロファイルを変更するのに十分なベースライン データを収集するまで、すべてのリンクに対してこの手順を繰り返します。



STEP 6 | 収集した待機時間、ジッター、およびパケット損失のベースラインに基づいて、Prisma Access Hub Path Quality profile を変更します。

STEP 7 | 必要に応じて SD-WAN の設定を続行します。

STEP 8 | SD-WAN リンク管理プロファイルをさらに微調整Prisma Access Hub アプリケーションとリンクのパフォーマンスを監視する。

Prisma Access Hub アプリケーションとリンクのパフォーマンスを監視する

Prisma Access Hubのアプリケーションとリンクのパフォーマンスを監視し、すべてのVPNクラスターの概要情報を表示し、順番にドリルダウンして影響を受けるサイト、アプリケーション、およびリンクに問題を分離することで、問題のトラブルシューティングを行います。SD-WANトラフィックの可視性は、トラフィックを受信する Prisma Access 展開または SD-WANファイアウォールに表示されます。たとえば、ハブ ファイアウォールからブランチ ファイアウォールへのトラフィックの場合、SD-WAN モニタリング データはブランチ ファイアウォールに反映されます。ランディング ダッシュボードには以下が表示されます。

- App Performance (アプリのパフォーマンス)
  - **Impacted (影響あり)**-ファイアウォールが選択可能なパスのリストのパス品質プロファイルで指定されたしきい値を満たす、ジッター、遅延、またはパケット損失のパフォーマンスがパスにない VPN クラスタ内の 1 つまたは複数のアプリケーション。
  - **OK**-ジッター、遅延、またはパケット損失のパフォーマンスの問題が発生していない VPN クラスタ、ハブ、およびブランチの数。
- Link Performance (リンクのパフォーマンス)
  - **Error (エラー)**-VPN クラスタ内の 1 つまたは複数のサイトに、トンネルまたは仮想インターフェース (VIF) のダウン等の接続の問題があります。
  - **Warning (警告)**- メトリックの7 日間の移動平均値を超過するジッター、遅延、またはパケット損失のパフォーマンス測定値を持つリンクがある VPN クラスタ、ハブ、およびブランチの数。
  - **OK**-ジッター、遅延、またはパケット損失のパフォーマンスの問題が発生していない VPN クラスタ、ハブ、およびブランチの数。

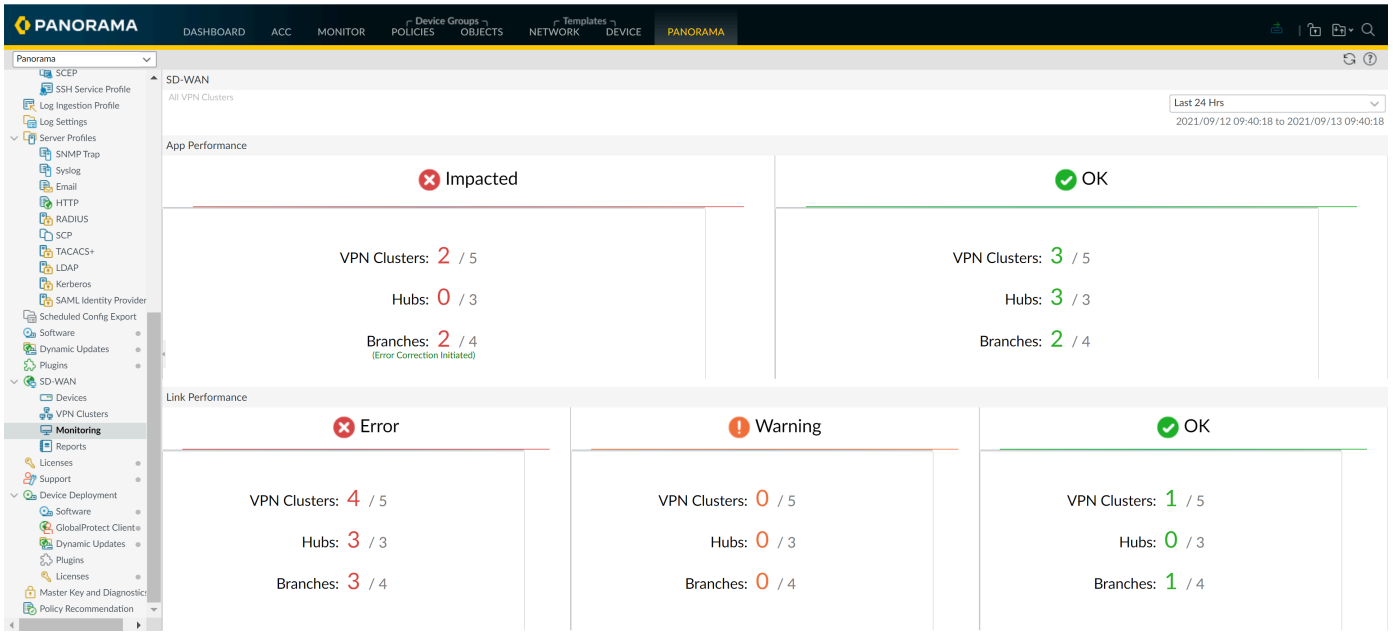
ランディング ダッシュボードから、エラーまたは警告ステータスのある、影響を受けたアプリケーションまたはリンクへとビューを絞り込みます。次に、影響を受けたサイトを選択し、サイト レベルの詳細を表示します。サイトから、アプリケーション レベルまたはリンク レベルの詳細を表示します。

すべての SD-WAN サイトでアプリケーションとリンクのパフォーマンスを監視するSD-WAN アプリケーションおよびリンクパフォーマンスの監視を参照してください。

データが存在しない場合、または *SD-WAN* が未定義であることを示す画面が表示される場合は、使用している *Panorama* リリースが使用しようとしている *SD-WAN* プラグインリリースをサポートしていることを、互換性マトリックスで確認してください。

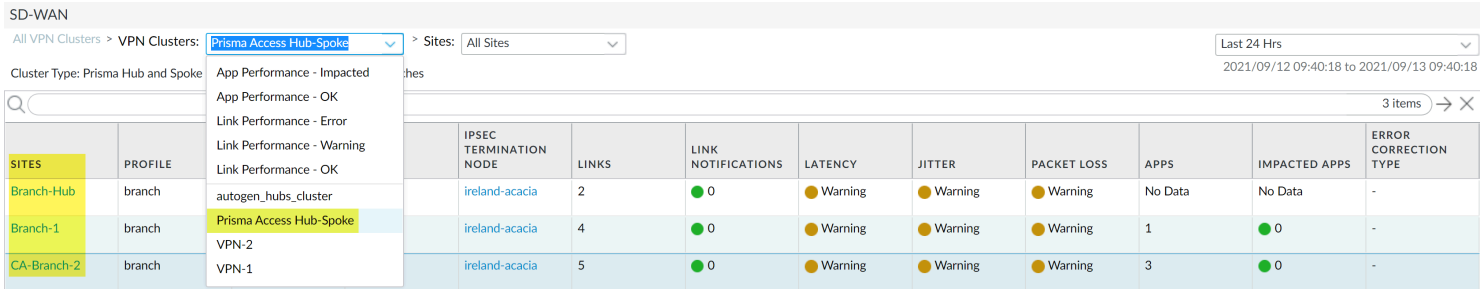
STEP 1 | Panorama Web インターフェイスへのログイン。

STEP 2 | **Panorama** 、 **> SD-WAN** 、 **> Monitoring(モニタリング)** と選択し、VPN クラスタ、ハブ、およびブランチのヘルス ステータスの概要を確認します。



STEP 3 | SD-WAN モニタリングをフィルタリングして、Prisma Accessハブスポーク VPN クラスターのみを表示します。

1. Impacted (影響あり)、Error (エラー)、または Warning (警告) の数を示す App Performance (アプリのパフォーマンス) または Link Performance (リンクのパフォーマンス) のサマリーをクリックして、遅延、ジッター、およびパケット損失に関するサイトおよびそのステータスの詳細なリストを表示します。
2. VPN クラスター フィルターで、**Prisma Access Hub-Spoke** を選択します。
3. サイトをクリックすると、Prisma Access Hubの正常性の詳細が表示されます。



STEP 4 | Prisma Access Hubの正常性の詳細を確認します。

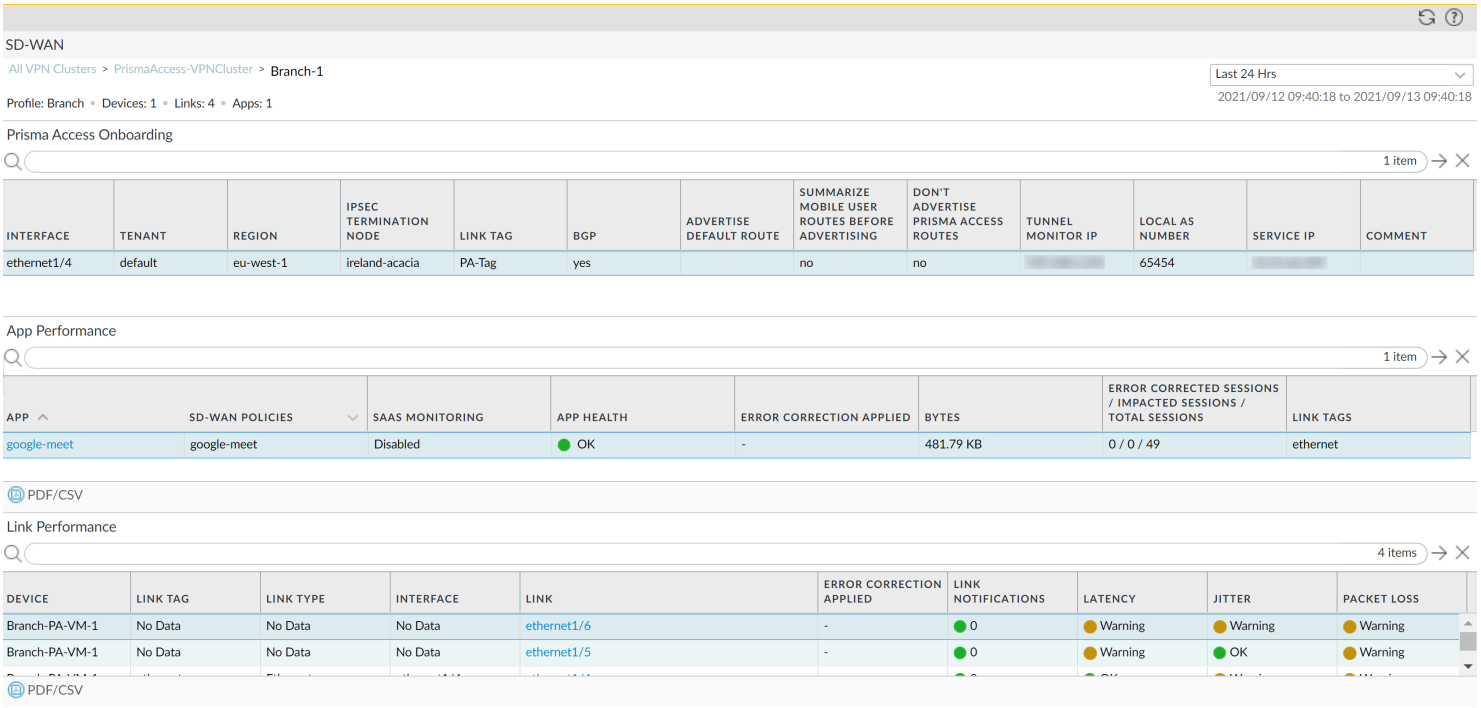
サイトデータには、Prisma Accessオンボーディングの詳細、影響を受けるアプリケーションを含むアプリのパフォーマンスとリンクパフォーマンスが表示されます。

ダイレクト インターネット アクセス (DIA) リンク上の SaaS アプリケーション用に、**SaaS Monitoring (SaaS** モニタリング**)** 列は、アプリが SaaS Quality (SaaS 品質) プロファイルで作成され、1 つ以上の SD-WAN ポリシー ルールに関連付けられているかどうかを示します。

- `Disabled` (無効)–アプリは SaaS 品質プロファイルで設定された SaaS アプリケーションではありません。
- `Enabled`–アプリは SaaS 品質プロファイルで構成された SaaS アプリケーションであり、1 つ以上の SD-WAN ポリシーに関連付けられています。

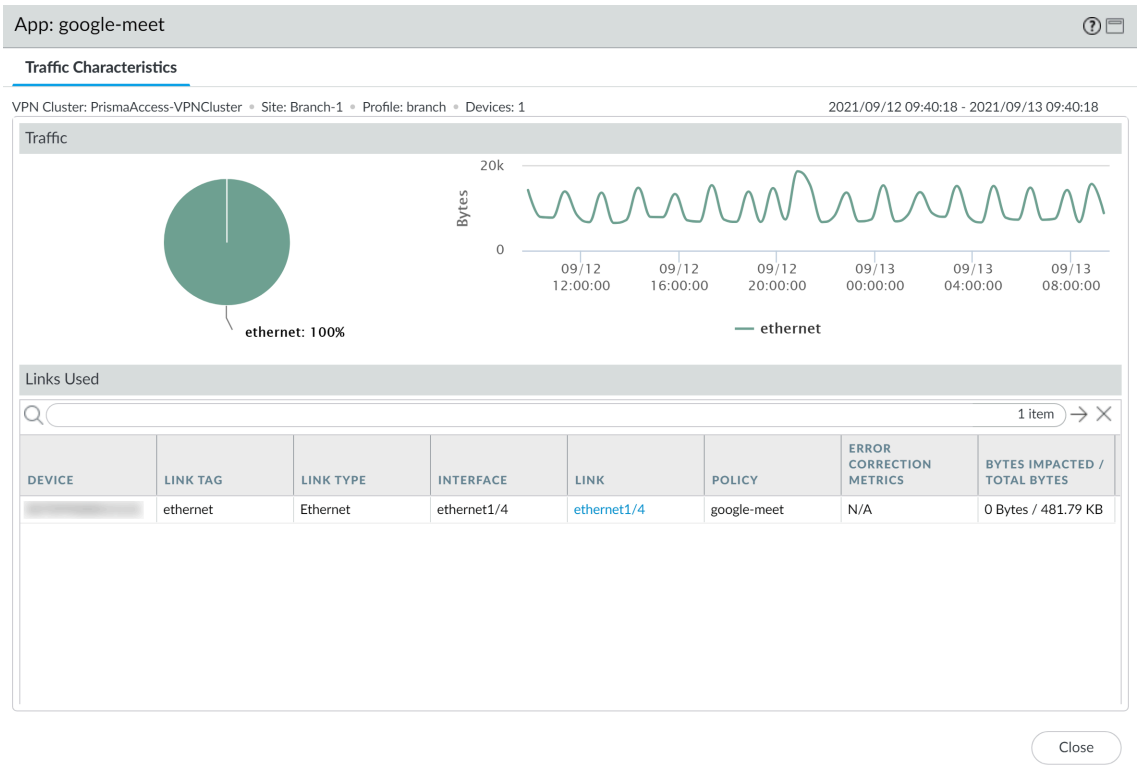
アプリケーション用にエラー訂正プロファイルを SD-WAN ポリシー ルール と関連付けた場合、**Error Correction Applied (**エラー訂正適用済み**)** 列には、エラー訂正が適用されたことと、エラー修正の種類が表示されます。また、指定された時間枠のセッションの総数のうち、ブランチ ファイアウォールまたはハブ ファイアウォールによってエラー修正されたセッションの数を理解するために、**Error Corrected Sessions (**エラー訂正済みのセッション**)/ Impacted Sessions (**影響を受けたセッション**)/Total Sessions (**セッション合計**)** を閲覧することができます。

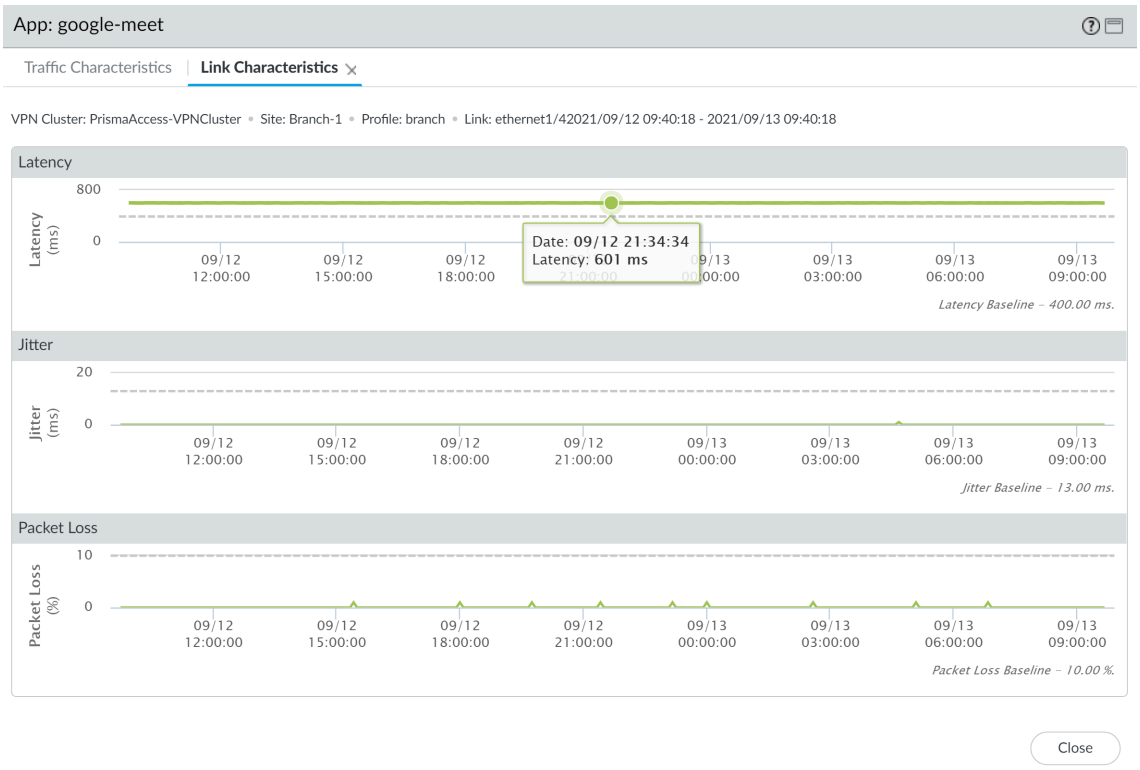
サイトのアプリケーションおよびリンクの詳細なヘルス情報を PDF または CSV 形式でエクスポートするには、**PDF/CSV** をクリックします。



STEP 5 | アプリケーション レベルまたはリンク レベルの詳細を表示するには、影響を受けたアプリケーションをクリックします。

たとえば、アプリケーションのリンク特性を表示して、指定されたリンクでのアプリケーションの遅延、ジッタ、およびパケット損失を理解します。また、該当のリンクに対してエラー訂正が適用されたかを閲覧できます。





SD-WAN レポートの生成

パス品質低下の頻度が最も高い上位のアプリケーションまたはリンクの詳細を表示する SD-WAN レポートを設定および生成します。アプリケーションまたはリンクがレポートに表示される順番は、それにより影響を受けるデータの量に基づいています。アプリケーションまたはリンクは、影響を受けるデータが多い順にレポートに表示されます。SD-WAN レポートは必要に応じて生成され、スケジュール生成はできません。SD-WAN レポートを使用して、アプリケーションまたはリンクの正確なスループットを確認したり、アプリケーションまたはリンクの影響がユーザーにインパクトを与えないようにします。例えば、ISP が一定量のスループットをリンクで保証している場合、そのリンクの Link Performance (リンクパフォーマンス) レポートを生成して、保証された帯域幅が遵守されていることを確認することができます。

Panorama™ 管理サーバからは、SD-WAN 対応ファイアウォールを通過するアプリケーションまたはリンクのレポートのみ生成可能です。個々のファイアウォールで処理されたアプリケーションまたはリンクのレポートを生成するには、ファイアウォールでローカル レポートを作成します。

データが存在しない場合、または *SD-WAN* が未定義であることを示す画面が表示される場合は、使用している *Panorama* リリースが使用しようとしている *SD-WAN* プラグインリリースをサポートしていることを、互換性マトリックスで確認してください。

STEP 1 | Panorama Web インターフェースにログインします。

STEP 2 | **Panorama** 、 > **SD-WAN** 、 > **Reports(**レポート**)** と選択し、新規レポート を **Add (**追加**)** します。

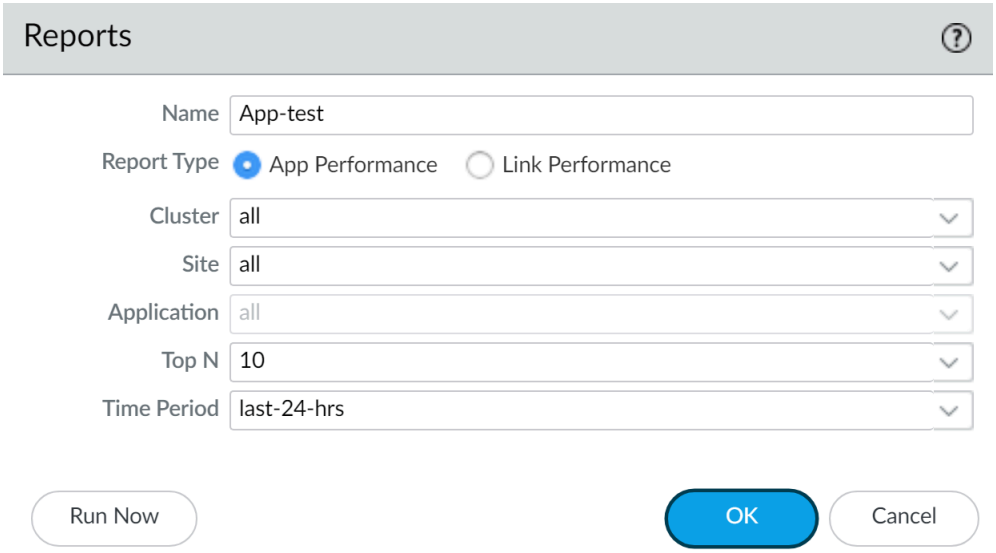
STEP 3 | SD-WAN レポートのパラメータを設定します。

1. **Name**（名前）フィールドに分かりやすいレポート名を入力します。
2. **Report Type(**レポートタイプ**)**を選択します。
   - アプリケーション ヘルスパフォーマンスのみの詳細レポートを生成するには、**App Performance (**アプリケーション パフォーマンス**)** を選択します。
   - リンク ヘルスパフォーマンスのみの詳細レポートを生成するには、**Link Performance (**リンク パフォーマンス**)** を選択します。
3. レポートを生成する対象の VPN **Cluster (**クラスタ**)** を選択します。デフォルトでは、**all (**すべて**)** が選択されています。
4. レポートを生成する対象の VPN クラスタ内の **Site (**サイト**)** を選択します。デフォルトでは、**all (**すべて**)** が選択されています。

   All (すべて**)** のクラスタを選択した場合、このフィールドはグレー表示されており、サイトは選択できません。
5. (App Performance only (アプリケーション パフォーマンスのみ) の場合) レポートを生成する対象の **Application (**アプリケーション**)** を選択します。

   All (すべて**)** のクラスタおよびサイトを選択した場合、このフィールドはグレー表示されており、個々のアプリケーションは選択できません。
6. (Link Performance only (リンク パフォーマンスのみ) の場合) レポートを生成する **Link Tag (**リンクタグ**)** を選択します。リンクタグを選択した場合、クラスタまたはサイトのタグでグループ化されたすべてのリンクのレポートが生成されます。デフォルトでは、**all (**すべて**)** が選択されています。
7. (Link Performance(リンク パフォーマンス) の場合のみ) レポートを生成する **Link Type (**リンクタイプ**)** を選択します。リンクタイプを選択した場合、クラスタまたはサイトの指定されたタイプのリンクのレポートが生成されます。デフォルトでは、**all (**すべて**)** が選択されています。
8. **Top N (**上位**N)** アプリケーションまたはリンクを選択します。この設定により、ヘルスの低下が発生しているアプリケーションまたはリンクのレポートに含める数が決定します。デフォルトでは、レポートにはヘルスの低下が発生している上位 **5** つのアプリケーションまたはリンクが含まれます。
9. レポートを生成する **Time Period (**期間**)** を指定します。デフォルトでは、**None (**なし**)** が選択されており、アプリケーションまたはリンクのヘルス ステータスの全履歴に対してクエリが実行されます。

STEP 4 | **Run Now (**今すぐ実行**)**をクリックしてレポートを生成します。



STEP 5 | 生成されたレポートを表示させて、**Export XML (XML**をエクスポート**)** して、ローカル デバイスにレポートを XML 形式でエクスポートします。準備が整ったら、**Close (**閉じる**)** をクリックします。

App Performance Report by application - top 10 apps across all clusters and all sites

Time period 2020-09-15 14:14:24 to 2020-09-16 14:14:24

CLUSTER	SITE	APP	SAAS MONITORING	AVG FLAP/SESSION	IMPACTED/TOT... BYTES PER APP	ERROR CORRECTED/IM... SESSIONS PER APP	POLICIES	Link Info			
								LINK TAG	LINK TYPE	ERROR CORRECTED METRICS	IMPACTED/... BYTES PER LINK TAG
ClusterHub245	Branch20	ssh	Disabled	175	9.08GB/339.08...	0/4/12	Tunnel_SCP	BroadBand2	ADSL/DSL		4.45GB/23....
							Tunnel_SCP	BroadBand1	Cablemodem		4.62GB/51....
ClusterHub245	Hub254	bgp	Disabled	16	904.35KB/19.4...	0/1/1		BroadBand2			904.24KB/9...
								BroadBand1	Ethernet		117.00b/11...
ClusterHub245	Branch50	ftp	Disabled	0	900.00b/1.64KB	0/1/2	Tunnel_FTP	BroadBand1	Cablemodem		900.00b/1.6...
ClusterHub245	Branch20	bgp	Disabled	15	380.00b/18.68...	0/1/1		BroadBand2	ADSL/DSL		170.00b/17...
								BroadBand1	Cablemodem		210.00b/21...
autogen_hubs_cl...	Hub254	dropbox-base	Disabled	0	0/38.41KB	0/0/33	DIA	BroadBand1	Ethernet		0/27.47KB
							DIA	BroadBand2	Ethernet		0/10.94KB
ClusterHub245	Branch20	taobao	Disabled	0	0/1.65MB	0/0/1.4k	DIA	BroadBand2	ADSL/DSL		0/729.81KB
							DIA,test-rule	BroadBand1	Cablemodem		0/962.53KB
ClusterHub245	Branch25	netbios-dg	Disabled	0	0/3.56KB	0/0/15	test-rule	BroadBand1	Cablemodem		0/3.56KB
ClusterHub245	Branch25	youku-base	Disabled	0	0/167.28KB	0/0/115	DIA	BroadBand2	ADSL/DSL		0/20.36KB
							DIA,test-rule	BroadBand1	Cablemodem		0/146.92KB
ClusterHub245	Hub254	insufficient-data	Disabled	0	0/24.92KB	0/0/105	BranchToBranch...	BroadBand1	Ethernet		0/13.05KB
							BranchToBranch...	BroadBand2	Ethernet		0/11.87KB
autogen_hubs_cl...	Hub254	apt-get	Disabled	0	0/62.36KB	0/0/2	DIA	BroadBand1	Ethernet		0/62.36KB

Export XML Close

STEP 6 | 設定したレポートを保存するには、Reports (レポート) のポップアップ画面で、**OK** をクリックします。

STEP 7 | **Commit(**コミット**)v** 、 **> Commit to Panorama(Panorama** へのコミット**)** を実行し、変更内容を **Commit (**コミット**)**します。

トラブルシューティング

Panorama™ 管理サーバのcommand line interface (コマンド ライン インターフェース - CLI) を使用して、SD-WAN 情報を表示し、操作を実行します。

- SD-WAN タスクでの CLI コマンドの使用
- SD-WAN デバイスの交換
- アプリケーションパフォーマンスのトラブルシューティング
- リンクパフォーマンスのトラブルシューティング
- SD-WAN ファイアウォールのアップグレード
- SD-WAN プラグインのインストール
- SD-WAN プラグインのアンインストール

SD-WAN タスクでの CLI コマンドの使用

以下の CLI コマンドを使用して、SD-WAN 情報の表示および消去、SD-WAN グローバル カウンターを表示します。VPN トンネル情報、BGP 情報、SD-WAN インターフェース情報を表示することもできます。

実行したい内容	以下を使用
SD-WAN 情報の表示または消去	
• SD-WAN インターフェースのパス名およびID、ステータス、ローカルおよびピア IP アドレス、トンネル インターフェース番号を表示します。	`> SDWAN 接続をすべて表示 |<sdwan-interface>`
• 仮想 SD-WAN インターフェースの各トンネルメンバーに分散されたセッション数および割合を表示します。	`> show sdwan session distribution policy-name <sdwan-policy-name>`
• 指定した仮想 SD-WAN インターフェースにトラフィックを送信する SD-WAN ポリシー ルール名、トラフィック分散方法、設定された遅延、ジッター、パケット損失のしきい値、ルールで識別されたリンクタグ、メンバー トンネル インターフェースを表示します。	`> show sdwan rule vif sdwan.x`
• パス選択やパス品質測定等の SD-WAN イベントを表示します。 *PAN-OS 10.0.0* および *10.0.1* の場合、*SD-WAN* 設定を変更(パス品質プロファイルの変更など)した結果 、別の *SD-WAN* パスが選択された場合、トラフィック ログはパス変更をカウントまたはロギングしません。	`> show sdwan event`
• SD-WAN イベントを消去します。	`> clear sdwan event`

実行したい内容	以下を使用

• 仮想 SD-WAN インターフェースの遅延、ジッター、およびパケット損失を表示します (インターフェース番号または名前を指定します)。
 	
遅延、ジッター、およびパケット損失の測定が実施され、3 種類の期間にわたり平均化されます。各期間にはヘルスバージョンが表示されており、(しきい値を超過する) ヘルス パラメータ値が変更されると増分します。リアルタイム測定に加え、リアルタイムの使用測定が提供されます。ここでは、リアルタイム値の変化がしきい値を最後に超えた時のパラメータ値が表示されます。
	`> show sdwan path-monitor stats vif <sdwan.x>`
	
	`> show sdwan path-monitor stats vif <sdwan-interface-name>`

• 指定されたセッションが合致する SD-WAN ポリシールール名、送信元および宛先のトンネル インターフェース、ルールに設定された遅延、ジッター、パケット損失の割合、およびトラフィック分散方法が表示されます。 *PAN-OS 10.0.0* および *10.0.1* の場合、*SD-WAN* 設定を変更(パス品質プロファイルの変更など)した結果 、別の *SD-WAN* パスが選択された場合、トラフィック ログはパス変更をカウントまたはロギングしません。	`> show sdwan session path-select session-id <session-id>`
• 仮想 SD-WAN リンクのモニタリング モード(アグレッシブまたは緩やか) および更新間隔が表示されます。	`> show sdwan path-monitor parameter path-name <sdwan-path-name>`
• 仮想 SD-WAN インターフェースのモニタリング モード(アグレッシブまたは緩やか)、更新間隔、およびプローブ統計が表示されます。	`> show sdwan path-monitor parameter vif <sdwan.x>`
SD-WAN のトラブルシューティング用のグローバル カウンターの表示	

実行したい内容	以下を使用
• ブランチ側で、送信される SD-WAN プローブ要求パケット数が受信されるプローブ応答パケット数とが同数であることを確認します。 ブランチ ファイアウォールでは、ほとんどの SD-WAN トンネルがイニシエータとなります。つまり、トンネルでは SD-WAN パスモニター プローブが有効化されています。	**> show counter global filter delta yes** flow_sdwan_prob_req_tx flow_sdwan_prob_reply_rx
• ハブ側で、受信した SD-WAN プローブ要求パケット数が、送信したプローブ応答パケット数と同数であることを確認します。 ハブ ファイアウォールでは、ほとんどの SD-WAN トンネルがレスポンダとなります。つまり、トンネルでは SD-WAN パスモニター プローブが無効となっています。	**> show counter global filter delta yes** flow_sdwan_prob_req_rx flow_sdwan_prob_reply_tx
VPN トンネル情報の表示	
• ファイアウォールで作成されたすべてのトンネルを表示します。	**> show vpn flow**
• 名前で識別される個々のトンネルの詳細を表示します。	**> show vpn flow name <name>**
• ID で識別される個々のトンネルの詳細を表示します。	**> show vpn flow tunnel-id <tunnel-id>**
• 全トンネルのインターネットキー交換 (IKE) フェーズ 1 およびフェーズ 2 の詳細を表示します。	**> show vpn ike-sa**
• 特定のゲートウェイの IKEv2 security associations(セキュリティ アソシエーション (SA))および IKEv2 IPSec の子SA を表示します。	**> show vpn ike-sa gateway <gateway>**
• トンネルの詳細を表示します。	**> show vpn tunnel**

実行したい内容	以下を使用
BGP 情報の表示	
• Virtual Router (仮想ルーター - VR)の BGP 概要を表示します。	`> show routing protocol bgp summary virtual-router <virtual-router>`
• BGP ピア概要を表示します。	`> show routing protocol bgp peer peer-name virtual-router`
• ローカルRouting Information Base (ルーティング情報ベース - RIB) の概要を表示します。	`> show routing protocol bgp loc-rib`
RIB と **FIB** 間の **SD-WAN** インターフェース情報の表示	
• 新たな SD-WAN 出口インターフェースを表示します。	`> show routing route`
• forwarding information base (転送情報ベース - FIB)で SD-WAN インターフェースを表示します。	`> show routing fib`

SD-WAN デバイスの交換

返品認証（RMA）プロセスをご利用いただくことで、支店やデータセンターサイトで、故障または誤作動したSD-WANデバイスを新品または再利用可能な機能SD-WANデバイスと交換できます。SD-WANデバイスは、デバイスチップの故障、デバイスの設定ミス、日常的な消耗など、さまざまな理由で故障や誤動作を起こす可能性があります。SD-WANデバイスが誤動作や全体的な障害で使用できない場合は、RMAプロセスを使用して、故障または誤動作しているデバイスを交換します。

適切なRMAプロセスに従わずに既存のデプロイメントからSD-WANファイアウォールを置き換えようとすると、Panorama™および管理対象デバイスでコミット障害が発生します。

RMAプロセスを開始する前に、次の手順を実行します。

- [Before Starting RMA Firewall Replacement (RMA ファイアウォールの交換を開始する前に)]を確認します。
- SD-WANは、デバイスのシリアル番号に基づいて、IPSecゲートウェイやkeyIDなどの設定を生成します。そのため、SD-WANの代替ファイアウォールのシリアル番号を更新して、新しいファイアウォールを認識し、コミットの失敗を回避する必要があります。SD-WAN構成に古いファイアウォールへのIPSecまたはVPNオブジェクト参照があるかどうかを調べます。
  - 高可用性（HA）デプロイメントでブランチファイアウォールを置き換えるには、ハブファイアウォールにログインし 、 **[Network (**ネットワーク**)]** > **[Network Profiles (**ネットワークプロファイル**)]** > **[IKE Gateways (IKE**ゲートウェイ**)]**を順に選択します。古いファイアウォールのシリアル番号（空白を含まない）を検索します。検索結果が1つ以上表示された場合は、SD-WANがゲートウェイ構成で古いファイアウォールシリアル番号を参照していることを示しています。この場合、PanoramaとHAデプロイメント入から古いブランチファイアウォールを切断することをお勧めします。
  - ハブを使用しないフルメッシュ デプロイメントでファイアウォールを置き換えるには、ブランチファイアウォールのいずれかで古いファイアウォールシリアル番号を検索します。検索結果が1つ以上表示された場合は、SD-WANがゲートウェイ構成で古いファイアウォールシリアル番号を参照していることを示しています。この場合、Panoramaおよびメッシュデプロイメントから古いブランチファイアウォールを切断することをお勧めします。
  - スタンドアロン ファイアウォールを交換する場合、シリアル番号を検索する必要はありません。

RMAがある場合に管理対象ファイアウォールの設定を復元するには、次のワークフローを使用します。

STEP 1 | **[Panorama]** > **[SD-WAN]** > **[VPN Clusters (VPN**クラスタ**)]**を選択し、古いファイアウォールを削除します。

STEP 2 | **[Panorama]** > **[SD-WAN]** > **[Devices (**デバイス**)]**を順に選択し、古いファイアウォールを削除します。

STEP 3 | 変更を Panorama にコミットします。

STEP 4 | （HAデプロイメントのみ）すべてのハブと他のHAピア（交換が必要な古いファイアウォールを除く）に変更をプッシュします。先に進む前に、ハブとスタンドアロンファイアウォールの両方でコミットが成功することを確認してください。古いファイアウォールシリアル番号を検索してもゲートウェイ設定が返されない場合は、この手順を省略できます。

STEP 5 | RMA代替ファイアウォールを設定します。

STEP 6 | （HA デプロイメントのみ）代替ファイアウォールとスタンドアロンファイアウォールの間に HA 接続を確立します。数値が小さい方のファイアウォール(つまり優先順位が高もの)が、アクティブに指定されます。代替ファイアウォールがアクティブHAピアとして引き継がれないようにするには、デバイスの優先度を高くして割り当てられないようにします。

STEP 7 | **[Panorama] > [SD-WAN] > [Devices (デバイス)]**を順に選択し、新しいブランチファイアウォールを追加します。

STEP 8 | **[Panorama] > [SD-WAN] > [VPN Clusters (VPN**クラスタ**)]**を順に選択し、新しいブランチファイアウォールを追加します。

STEP 9 | 変更を Panorama にコミットします。

STEP 10 | ［**Commit (コミット)] > [Push to Devices (デバイスにプッシュ)]** を順に選択し、Panoramaで管理されている設定全体をハブとブランチの両方のHAピアにプッシュします。

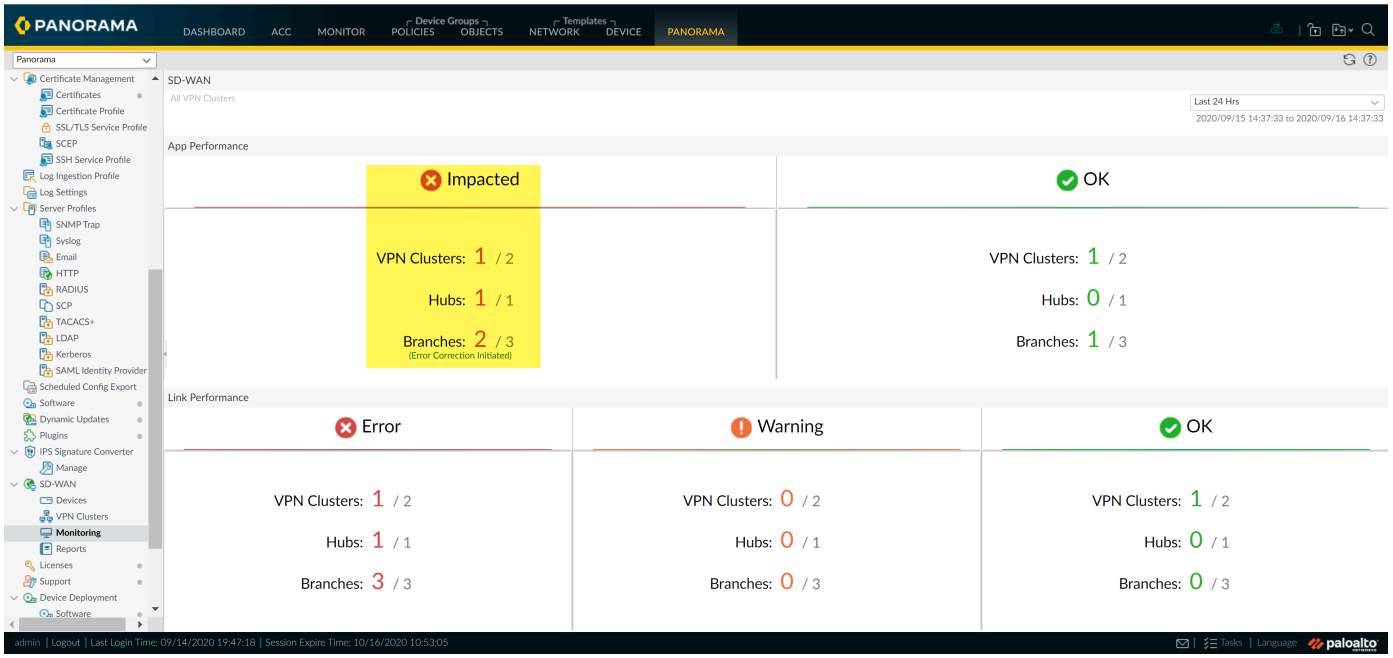
> ***[Push to Devices (デバイスにプッシュ)***］ を選択すると、*Panorama* は *HA*デプロイメントとハブ アンド スポーク デプロイメントの両方で、クラスタ内のすべてのデバイスに変更をプッシュしようとします。変更をすべてのデバイスにプッシュしないようにするには、［*Push Scope (プッシュスコープ)*］で［***Edit Selections (選択を編集)***］を選択し、［***Device Groups (デバイスグループ)***］のデバイスと［***Templates (テンプレート)***］で他のすべてのデバイスを無効にします。
>
> - ハブ アンド スポーク デプロイメントでは、設定をプッシュするブランチシステムのハブ ファイアウォールと*HA*テンプレートスタックを選択します。その結果、選択されていないサイトは同期しなくなる可能性があります。
> - フルメッシュデプロイメントでは、クラスタ内のすべてのデバイスに変更をプッシュすることが必須です。

アプリケーションパフォーマンスのトラブルシューティング

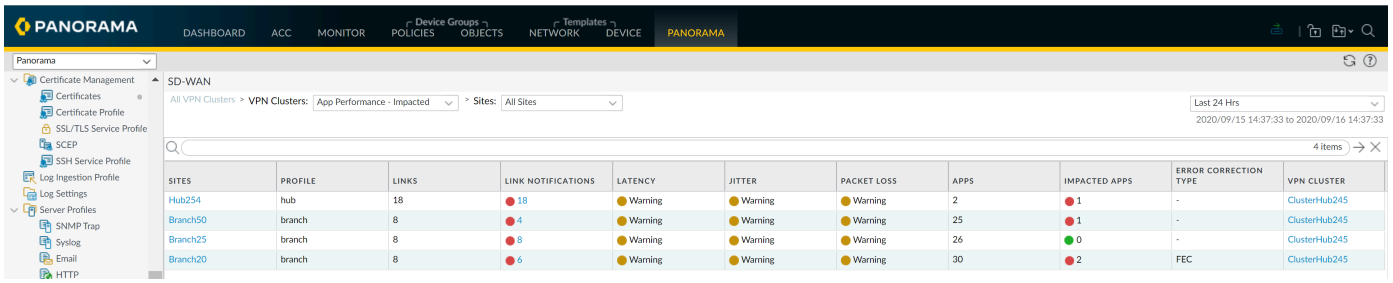
アプリケーションやサービスのパフォーマンス低下の原因の把握は、ユーザーエクスペリエンスに影響を与えないためには不可欠です。VPN クラスタが影響を受け、アプリケーションのトラフィックが別のリンクにフェールオーバーする理由を理解しておくと、SD-WAN 設定の微調整に役立ちます。

STEP 1 | Panorama Web インターフェイスへのログイン。

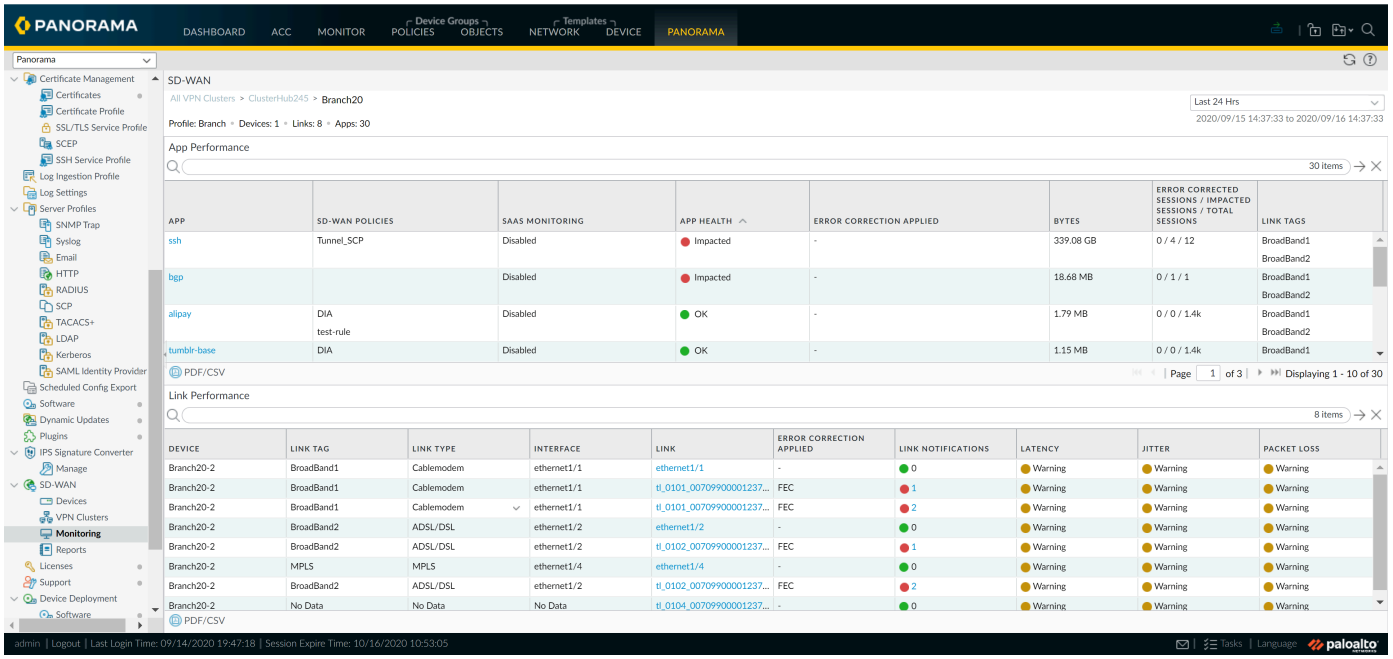
STEP 2 | **Panorama** 、 **> SD-WAN** 、 **> Monitoring (**モニタリング**)** と選択し、**Impacted (**影響を受けた**)** VPN クラスタを表示します。



STEP 3 | **Site(**サイト**)** ドロップダウンの優先メトリックに基づき VPN クラスタを絞り込み、期間を選択します。この例では、過去 12 時間で影響を受けた VPN クラスタを含む **All Sites (**全サイト**)** が表示されています。

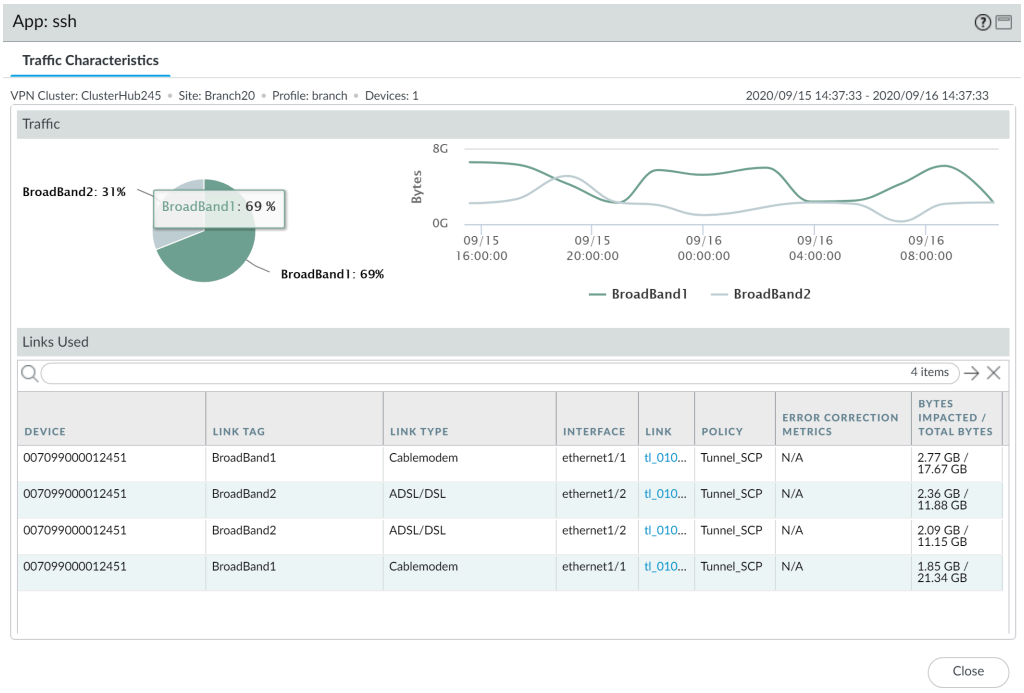


STEP 4 | Sites (サイト) 列で、影響を受けたハブまたはブランチ ファイアウォールを選択し、影響を受けたアプリケーションと対応するリンクのパフォーマンスを表示します。



STEP 5 | App Performance (アプリケーションのパフォーマンス) セクションでアプリケーションをクリックして、インターネット サービスや使用されるリンク等、アプリケーションのトラフィックに関する詳細なトラフィック特性情報を表示します。

- インターネット サービス全体でのアプリケーション トラフィックの内訳を把握するには、円グラフを確認します。
- 各インターネットサービス経由で転送されたデータのbyte (バイト)数を把握するには、折れ線グラフを確認します。
- 使用されたアプリケーショントラフィックのリンクを把握し、選択した期間の合計バイトのうち、影響を受けたバイトの数を理解するには、Links Used (使用されたリンク) セクションを確認します。

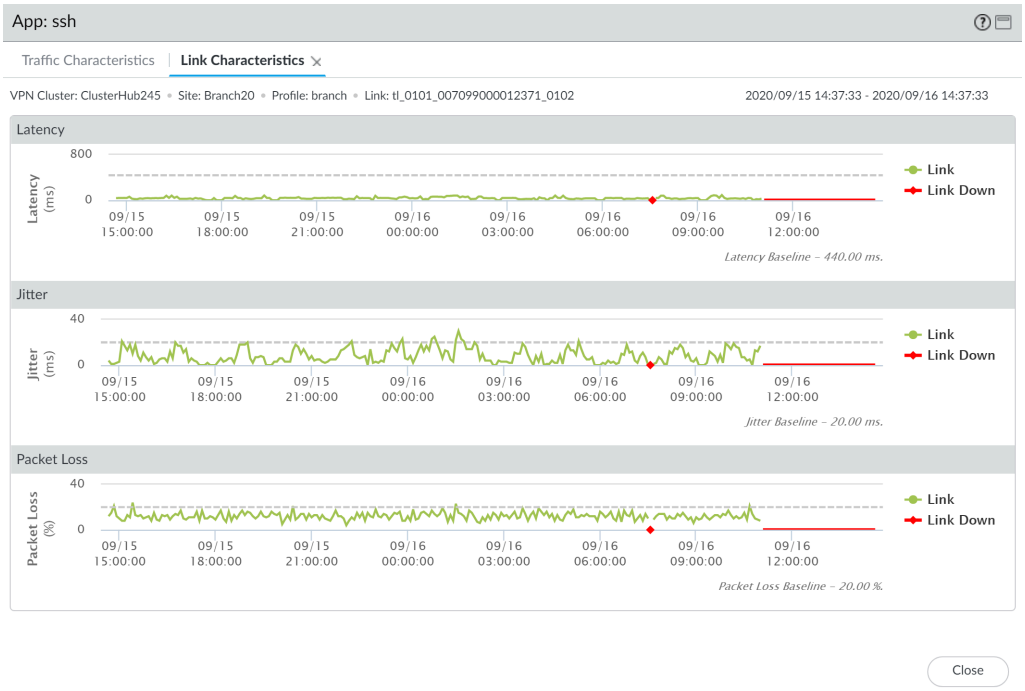


STEP 6 | アプリケーションがリンクを変える原因となったヘルス メトリックを調査します。

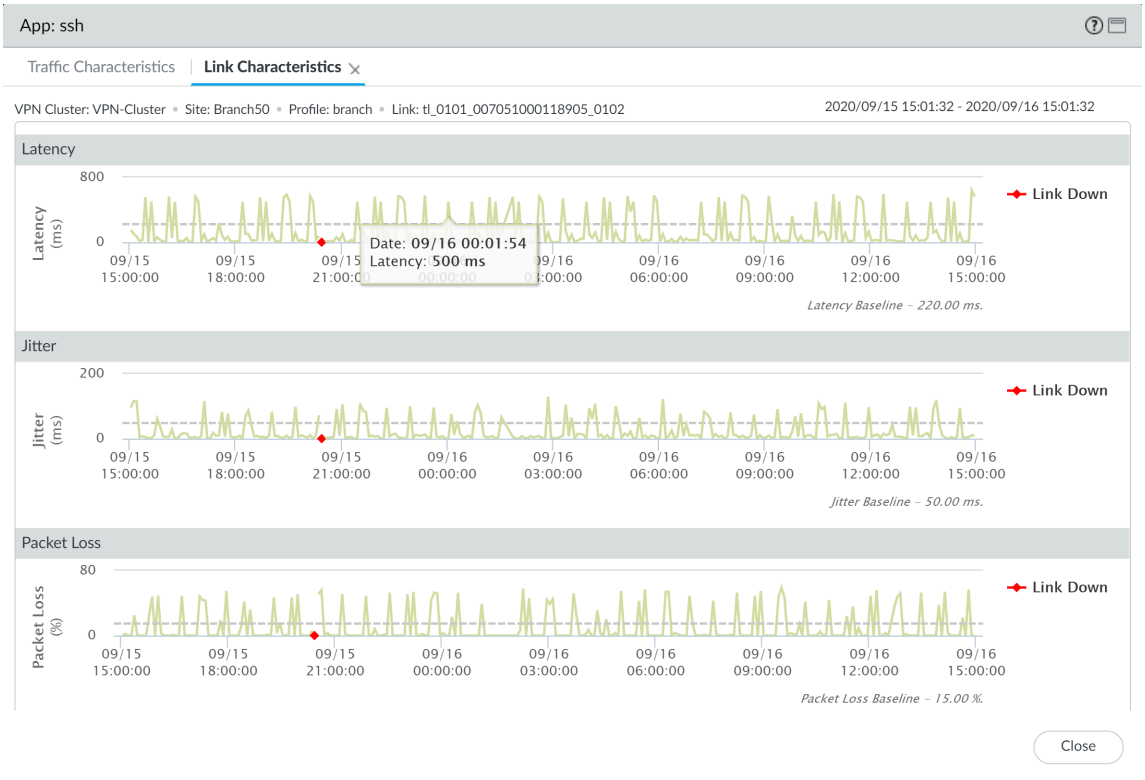
点線は、7日間のヘルス メトリックの平均を示しています。

1. Traffic Characteristics (トラフィック特性) タブの Links Used (使用されたリンク) セクションで、イーサネットリンクをクリックして、ステップ 2 で指定された期間の詳細

なリンク特性 (遅延、ジッター、およびパケット損失) を表示し、どのヘルスメトリックが原因でアプリケーションがリンクを変更したかを調査します。。



2. **Traffic Characteristics (**トラフィック特性**)** タブで、別のリンクを選択してセカンダリアプリ リンクのリンク特性を表示し、VPN クラスタが影響を受ける原因をよりよく理解します。



STEP 7 | アプリケーションのトラフィックが影響を受けた理由を特定した後、以下の点を検討して問題を解決します。

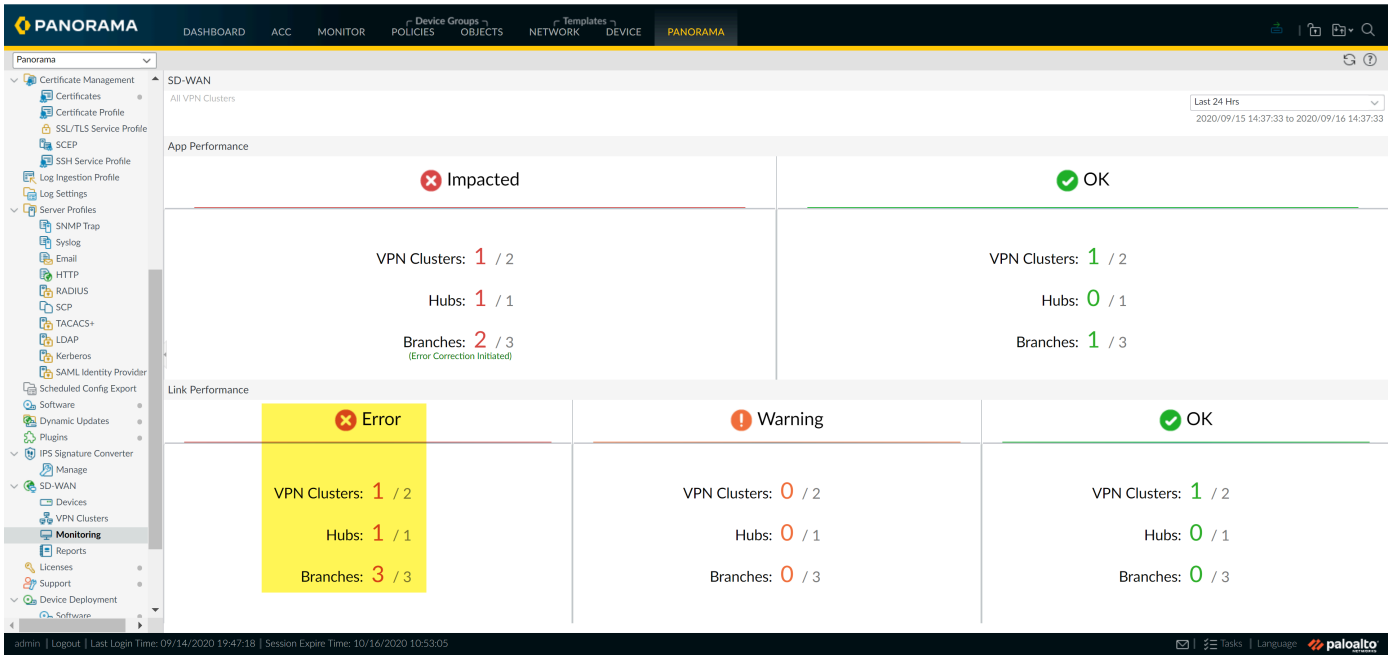
- Traffic Distribution Profile (トラフィック分散プロファイル) へのリンクの追加を検討します。アプリケーションのトラフィックのフェールオーバー先のリンクを追加することで、アプリケーションのトラフィックとユーザー エクスペリエンスが、ヘルスが劣化したリンクの影響を受けないようにすることができます。
- Path Quality Profile (パス品質プロファイル) でヘルスしきい値を再設定します。正常性のしきい値が厳しすぎるため、不要なリンク フェールオーバーが発生する可能性があります。例えば、ユーザー エクスペリエンスが影響を受けるまでに最大 18% のパケット損失の発生を許容するアプリケーションがある場合、10% のパケット損失のしきい値が設定されていると、必要がない場合でもアプリケーションが別のリンクにフェイルオーバーされます。
- インターネット サービス プロバイダー (ISP) に問い合わせて、ネットワークに制御できない影響があり、解決できる可能性があるかどうかを確認します。

リンクパフォーマンスのトラブルシューティング

リンクのパフォーマンス低下の原因の把握は、アプリケーションやサービスを使用する際のユーザーエクスペリエンスに影響を与えないためには不可欠です。VPN クラスタでの影響を受けたリンクの理由を理解すると、SD-WAN 設定を微調整して、アプリケーションやサービスの使用の際のユーザー エクスペリエンスが、劣化したヘルスのリンクの影響を受けないようにすることができます。

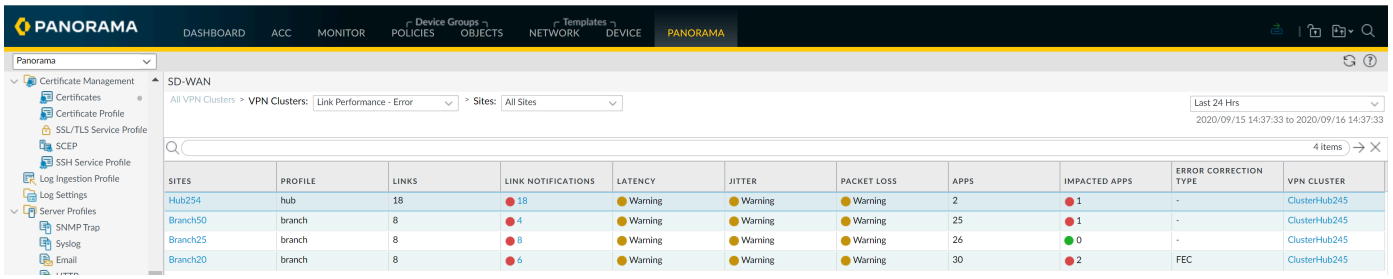
STEP 1 | Panorama Web インターフェイスへのログイン。

STEP 2 | **Panorama** 、 **> SD-WAN** 、 **> Monitoring (**モニタリング**)** と選択し、**Impacted (**影響を受けた**)** VPN クラスタを表示します。

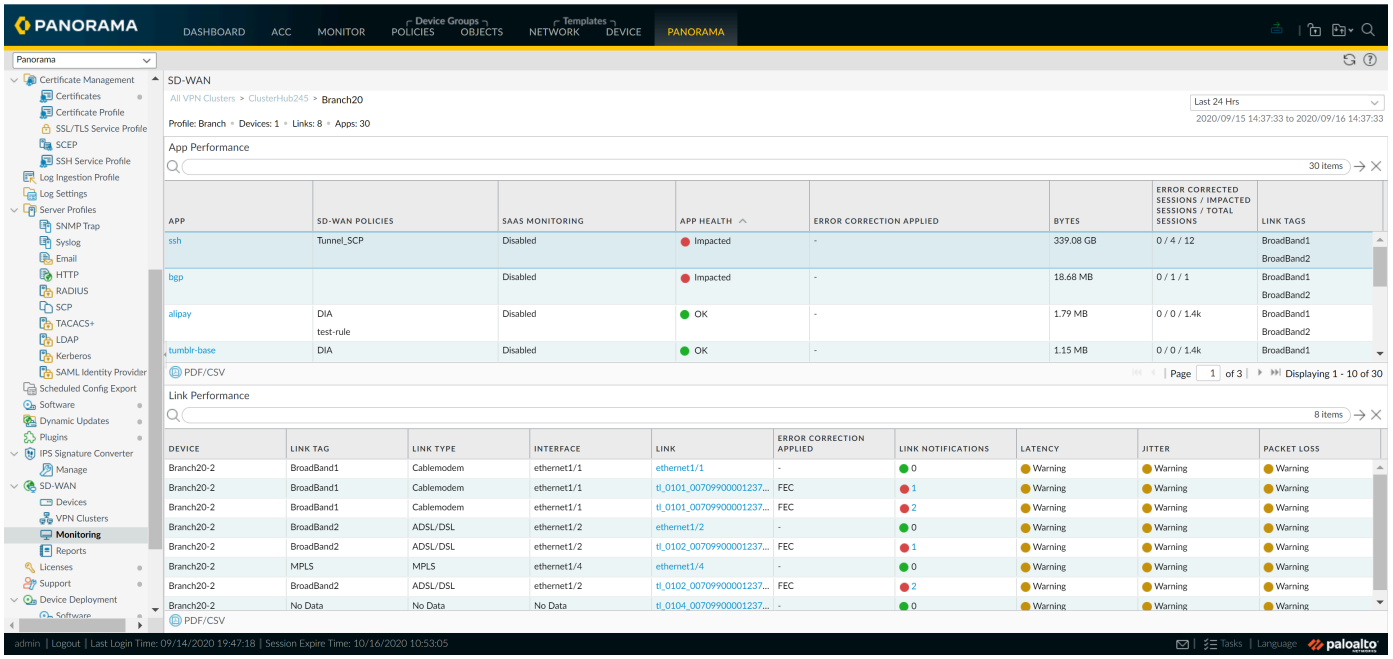


STEP 3 | **Site(**サイト**)** ドロップダウンの優先メトリックに基づき VPN クラスタを絞り込み、期間を選択します。Sites (サイト) 列で、影響を受けたハブまたはブランチ ファイアウォールを選択し、影響を受けたアプリケーションと対応するリンクのパフォーマンスを表示します。

この例では、過去 24 時間で影響を受けた VPN クラスタを含む **All Sites** (全サイト) が表示されています。

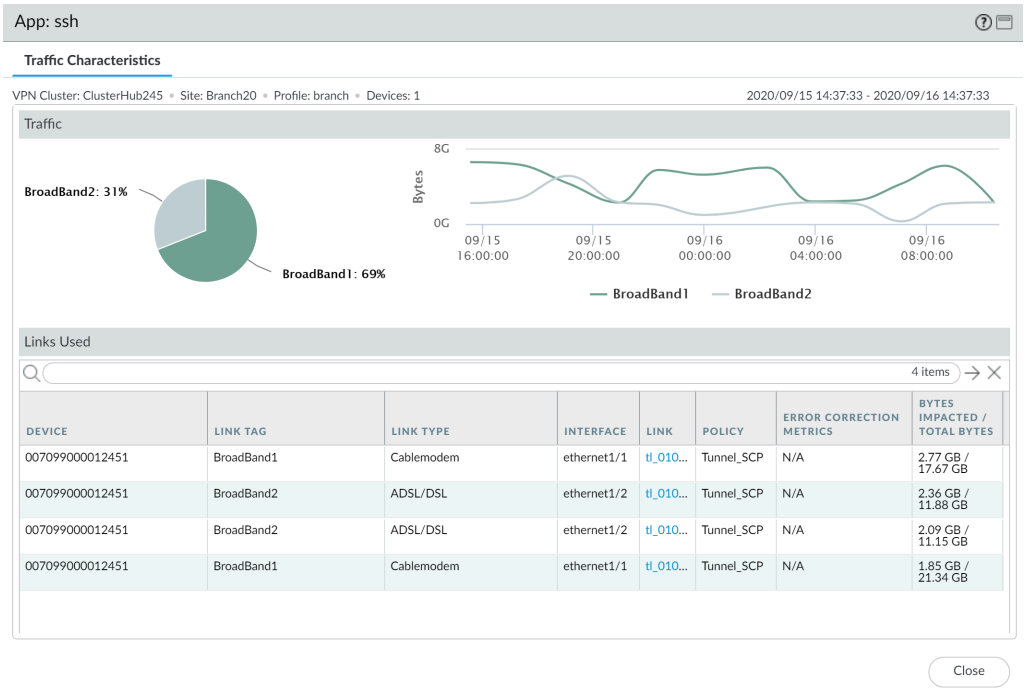


STEP 4 | Sites (サイト) 列で、影響を受けたハブまたはブランチ ファイアウォールを選択し、影響を受けたアプリケーションと対応するリンクのパフォーマンスを表示します。



STEP 5 | App Performance (アプリケーションのパフォーマンス) セクションでアプリケーションをクリックして、インターネット サービスや使用されるリンク等、アプリケーションのトラフィックに関する詳細なトラフィック特性情報を表示します。

- インターネット サービス全体でのアプリケーション トラフィックの内訳を把握するには、円グラフを確認します。
- 各インターネットサービス経由で転送されたデータのbyte (バイト)数を把握するには、折れ線グラフを確認します。
- 使用されたアプリケーショントラフィックのリンクを把握し、選択した期間の合計バイトのうち、影響を受けたバイトの数を理解するには、Links Used (使用されたリンク) セクションを確認します。

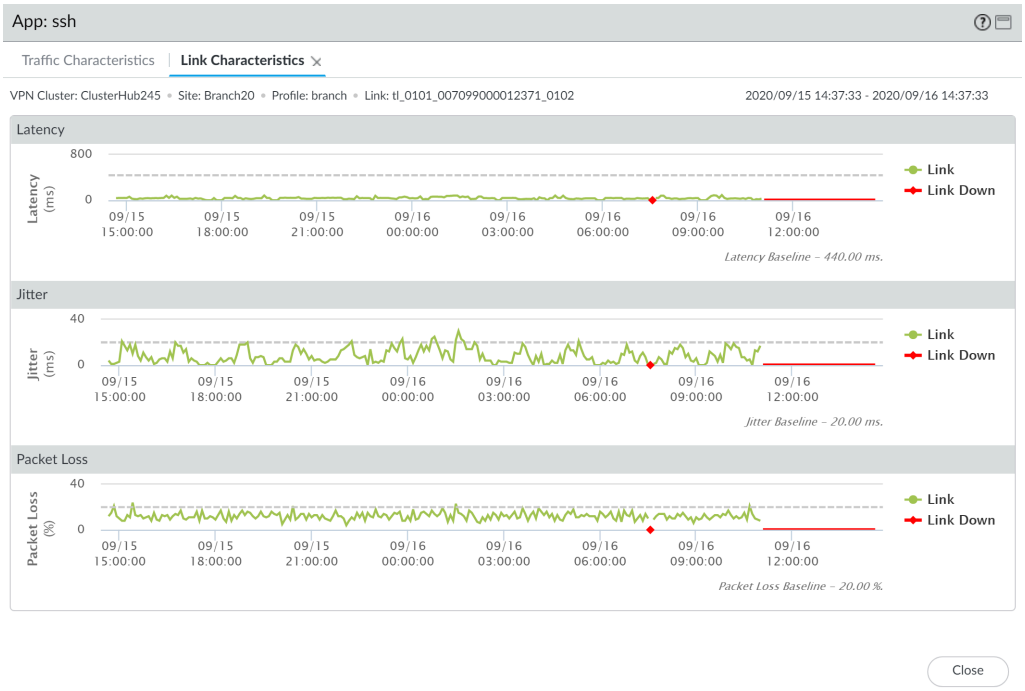


STEP 6 | アプリケーションがリンクを変える原因となったヘルス メトリックを調査します。

点線は、パス品質プロファイルの作成時に設定するしきい値を示します。

1. Traffic Characteristics (トラフィック特性) タブの Links Used (使用されたリンク) セクションで、イーサネットリンクをクリックして、ステップ 2 で指定された期間の詳細なリンク特性 (遅延、ジッター、およびパケット損失) を表示し、どのヘルスメトリックが原因でアプリケーションがリンクを変更したかを調査します。。この例では、イーサネット 1/1を表示しており、損失したパケットの割合が定期的にアプリケーションのパス品質プロファイルで設定したしきい値を超過していることが確認できるため、これ

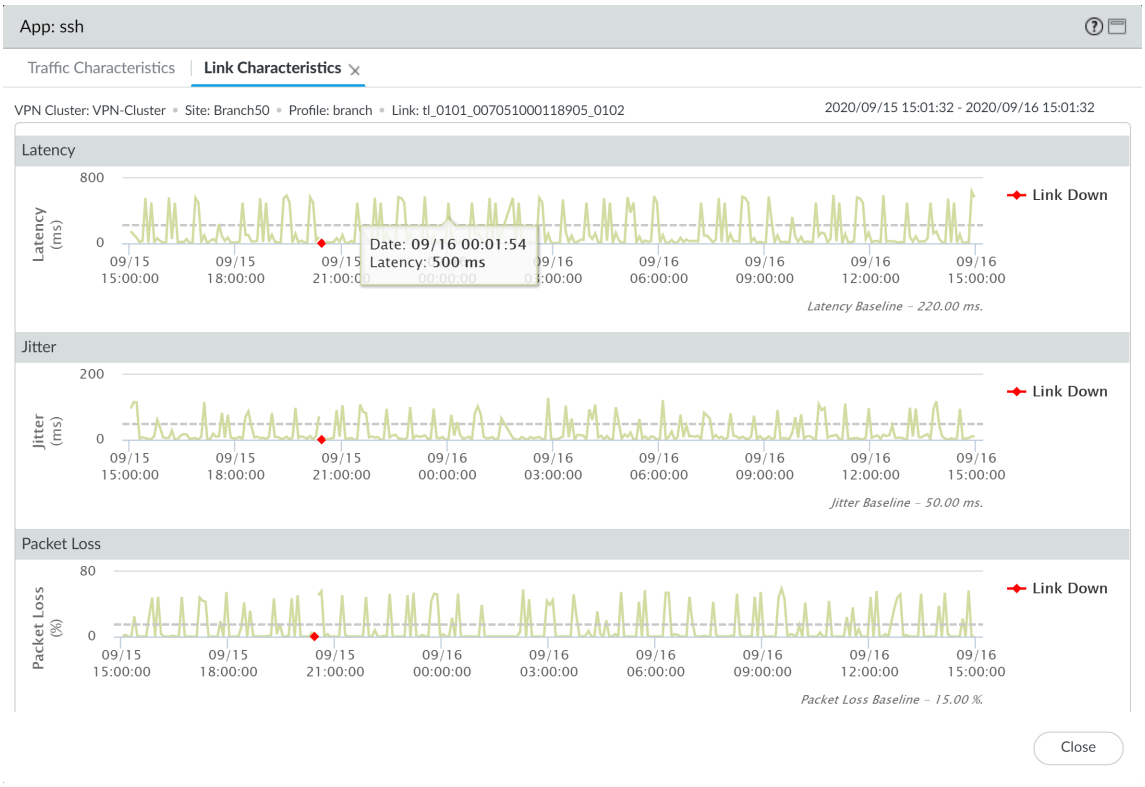
が、アプリケーションのトラフィックが次善のリンクにフェイルオーバーした理由であると結論付けることができます。



2. **Traffic Characteristics (**トラフィック特性**)** タブで、別のリンクを選択して、リンク特性を表示させます。この例では、イーサネット1/4 が表示されています。アプリケーションのトラフィックのフェイルオーバー後、イーサネット 1/4ではアプリケーションのジッターが設定したしきい値を超過していることが確認できます。これが原因で、アプ

リケーションのトラフィックはイーサネット 1/1 にフェイルオーバーする必要があったわけです。

VPN クラスタが影響を受けたのは、両方のリンクでヘルス メトリックが超過したため、アプリケーションのトラフィックにはフェイルオーバー先となる健全なリンクがなかったからです。



STEP 7 | アプリケーションのトラフィックが影響を受けた理由を特定した後、以下の点を検討して問題を解決します。

- Traffic Distribution Profile (トラフィック分散プロファイル) へのリンクの追加を検討します。アプリケーションのトラフィックのフェールオーバー先のリンクを追加することで、アプリケーションのトラフィックとユーザー エクスペリエンスが、ヘルスが劣化したリンクの影響を受けないようにすることができます。
- Path Quality Profile (パス品質プロファイル) でヘルスしきい値を再設定します。ヘルスしきい値が厳密過ぎて不要なリンクフェイル オーバーが発生している場合もあります。例えば、ユーザー エクスペリエンスが影響を受けるまでに最大 18% のパケット損失の発生を許容するアプリケーションがある場合、10% のパケット損失のしきい値が設定されていると、必要がない場合でもアプリケーションが別のリンクにフェイルオーバーされます。
- インターネット サービス プロバイダー (ISP) に問い合わせ、ユーザー側では制御不能なネットワークの影響を解決することができるかどうかを判断します。

SD-WAN ファイアウォールのアップグレード

Panorama Plugin for SD-WAN 2.0 Release Notes (SD-WAN 2.0 用 Panorama プラグインに関するリリースノート) を確認してから、次のステップに従い、Panorama ファイアウォールとマネージド SD-WAN ファイアウォールをアップグレードします。

STEP 1 | Panorama のコンテンツ更新とソフトウェア更新のインストールを行います。

STEP 2 | マネージド ログ コレクタをアップグレードします。

- Panorama がインターネットに接続されている状態でログ コレクタをアップグレードします。
- Panorama がインターネットに接続されていない状態でログ コレクタをアップグレードします。

STEP 3 | SD-WAN ハブ ファイアウォールをアップグレードします。

ブランチ ファイアウォールをアップグレードする前にハブ ファイアウォールを *PAN-OS 10.0.0* から *PAN-OS 10.0.1* 以降のリリースにアップグレードする必要があります。ハブファイアウォールの前にブランチ ファイアウォールをアップグレードすると、モニタリングのデータ (***Panorama*** > ***SD-WAN*** > ***Monitoring*** (モニタリング)) が不正確になり、また、*SD-WAN* リンクが間違って *down* と表示される可能性があります。

- Panorama がインターネットに接続されている状態でファイアウォールをアップグレードします。
- Panorama がインターネットに接続されていない状態でファイアウォールをアップグレードします。

STEP 4 | SD-WAN ブランチ ファイアウォールをアップグレードします。

- Panorama がインターネットに接続されている状態でファイアウォールをアップグレードします。
- Panorama がインターネットに接続されていない状態でファイアウォールをアップグレードします。

SD-WAN プラグインのインストール

ご利用のPanorama™管理サーバーとSD-WANを利用するファイアウォールにSD-WANプラグインバージョンをインストールします。

Palo Alto Networks Panorama プラグイン互換性マトリックス を参照し、ターゲット SD-WAN プラグインバージョンに必要な最小 PAN-OS バージョンを確認してください。SD-WAN プラグイン リリースと互換性のある Panorama管理サーバーおよび Palo Alto Networks ファイアウォールをアップグレードするには、「互換性のある PAN-OS リリース での SD-WAN プラグインのアップグレード」を参照してください。

STEP 1 | Panorama Web インターフェースにログインします。

STEP 2 | PanoramaにSD-WANプラグインのバージョンをインストールします。

Panorama が高可用性 (HA) 設定の場合、Panorama HA ピアでこのステップを繰り返します。

1. 最新の **Panorama** > **Plugins** および **Check Now** を選択して、最新の **sd_wan** プラグイン バージョンを入手してください。
2. 最新バージョンの SD-WAN プラグインを **Download** (ダウンロード) して **Install** (インストール) します。
3. SD-WAN プラグインのインストールが正常に完了した後、**Commit** (コミット) および **Commit to Panorama** (**Panorama** へのコミット) します。

   この手順は、いずれの設定の変更を Panorama にコミットする前に必要となります。

STEP 3 | 新しいプラグインバージョンが正常にインストールされたら、Panorama **Dashboard** (ダッシュボード) を表示し、一般情報ウィジェットで SD-WAN プラグイン にインストールした SD-WAN プラグインのバージョンが表示されていることを確認します。

SD-WAN プラグインのアンインストール

Panorama 管理サーバから SD-WAN プラグインをアンインストールするには、SD-WAN プラグインのアンインストールを完了する前に、Panorama から SD-WAN プラグインの設定を削除する必要があります。

STEP 1 | Panorama Web インターフェースにログインします。

STEP 2 | SD-WAN ハブおよびブランチの間で BGP を実行することを許可するセキュリティ ポリシー ルールをすべて削除します。

1. **Panorama** 、 > **SD-WAN**、 > **Devices (**デバイス**)** 、 > **BGP Policy (BGP** ポリシー**)** と選択して、セキュリティ ポリシー ルールを **Remove (**削除**)**します。
2. **OK** をクリックして、設定の変更を保存します。

STEP 3 | **Panorama** 、 > **Plugins (**プラグイン**)** と選択し、SD-WAN の**Remove Config (**設定の削除**)** を選択します。

STEP 4 | **Commit (**コミット**)** を選択し、マネージド ファイアウォールへの設定の変更を **Commit and Push (**コミットしてプッシュ**)** します。

STEP 5 | SD-WAN プラグインを **Uninstall** (アンインストール) します。

SD-WAN プラグインのアンインストールの続行を求められたら、**OK** をクリックします。

