検証済みソリューション：Cisco SD-Access、Cisco SD-WAN、および Firepower との IPv6 の統合

改訂：2023 年 9 月 28 日

ソリューションの概要

このガイドでは、従来のネットワークよりもソフトウェア定義型ネットワークを好むお客様向けの IPv6 ソリューションについて説明します。ソリューション アーキテクチャは、キャンパスアーキテクチャ、WAN 用の Cisco SD-WAN、およびセキュアなインターネット接続用の Cisco Firepower 向けの Cisco Software-Defined Access に基づいています。その目的は、移行中にアンダーレイ インフラストラクチャのデュアルスタックを維持しながら、IPv6 専用クライアントを有効にすることです。オーバーレイとアンダーレイの両方のシングルスタック IPv6 アーキテクチャへの移行は、エンドツーエンドの IPv6 専用環境が完全にサポートされている場合に実行されます。

テクノロジーの概要

IPv6 ソリューションは、キャンパス、データセンター、ファイアウォール、WAN、インターネットなどの複数のドメインを含むクロスアーキテクチャ設計になっています。キャンパスサイト全体のエンドポイントは IPv6 専用クライアントであり、アンダーレイ インフラストラクチャは必要に応じてデュアルスタックになります。

Cisco SD-Access の IPv6

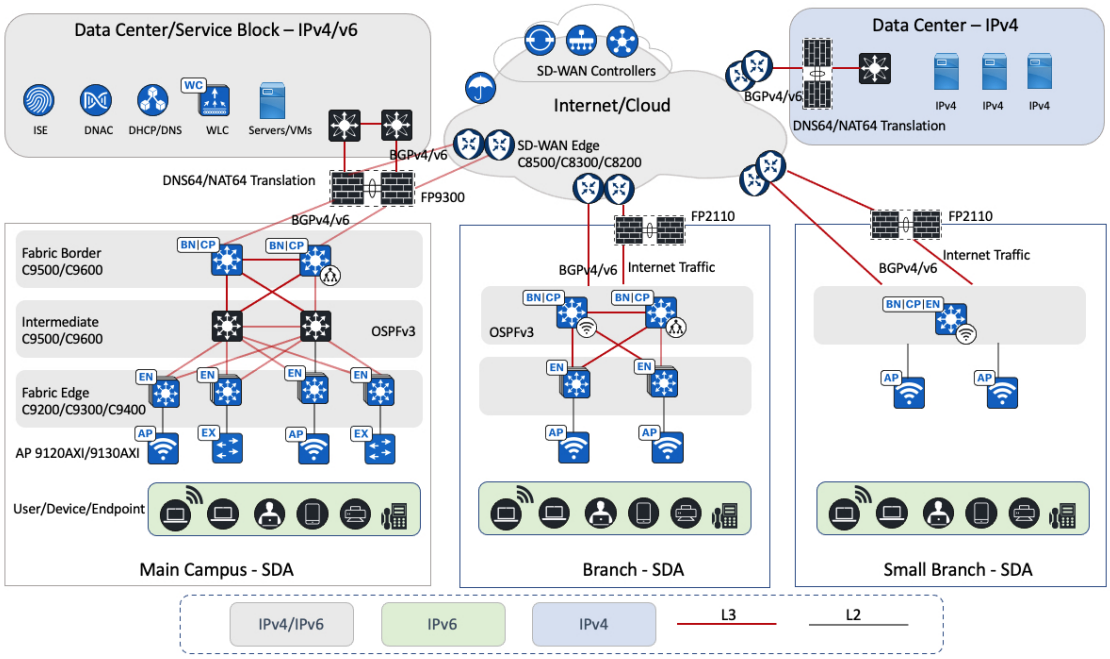
時間の経過とともに、Cisco DNA Center アーキテクチャは従来のキャンパス LAN 設計から Cisco SD-Access 設計アーキテクチャへと進化してきました。Cisco SD-Access は Cisco DNA Center を使用して、ポリシーの設計、プロビジョニング、および適用を実行し、インテリジェント キャンパス ネットワークの有線およびワイヤレス ネットワーク アシュアランスを提供します。このソリューションでは、Cisco SD-Access ファブリックアンダーレイは IPv4 アドレッシングを使用します。Cisco DNA Center は IPv4 を利用して、Cisco ISE との統合、デバイスの管理、および Cisco SD-Access ファブリックのプロビジョニングを実行します。Cisco SD-Access ファブリックでは、オーバーレイ IPv6 トラフィックは IPv4 Virtual Extensible LAN（VXLAN）トンネルで転送されます。

Cisco SD WAN の IPv6

Cisco SD WAN アーキテクチャは、個別のオーケストレーション、管理、コントロール、およびデータの各プレーンで構成されています。vBond コントローラを使用すると、Cisco SD WAN ルータを Cisco SD WAN オーバーレイに自動的にオンボードできます。vManage コントローラは、一元的な設定とモニタリングの役割を担います。vSmart コントローラは、Cisco SD WAN ネットワークの集中型コントロールプレーンの役割を担います。Cisco SD WAN エッジデバイスは、他の Cisco SD WAN エッジデバイスとのセキュアなデータプレーン接続を確立します。オーバーレイ IPv6 トラフィックは、ローカルおよびリモート Cisco SD WAN エッジデバイスの設定に基づいて、IPv4 または IPv6 トランスポートを介して確立された IP セキュリティ（IPsec）トンネルで転送できます。

Cisco SD-Access と Cisco SD WAN テクノロジードメインが統合され、Cisco SD WAN ファブリック全体の Cisco SD-Access サイト間の通信が可能になります。このソリューションテストでは、Cisco SD-Access と Cisco SD WAN テクノロジードメインの IPv6 統合と、メインキャンパスサイトで Cisco Firepower アプライアンスを Cisco SD-Access Fusion デバイスとして使用することを検証します。このテストでは、*Cisco SD-Access SD-WAN* 独立ドメインのペアワイズ統合ガイド [英語] に従って、デバイス間にボーダー ゲートウェイ プロトコル（BGP）および Virtual Routing and Forwarding（VRF）Lite を実装します。詳細については、*Cisco SD-Access SD-WAN* 独立ドメインのペアワイズ統合ガイド [英語] を参照してください。

図 *1*: ソリューションのテストベッドの論理トポロジ



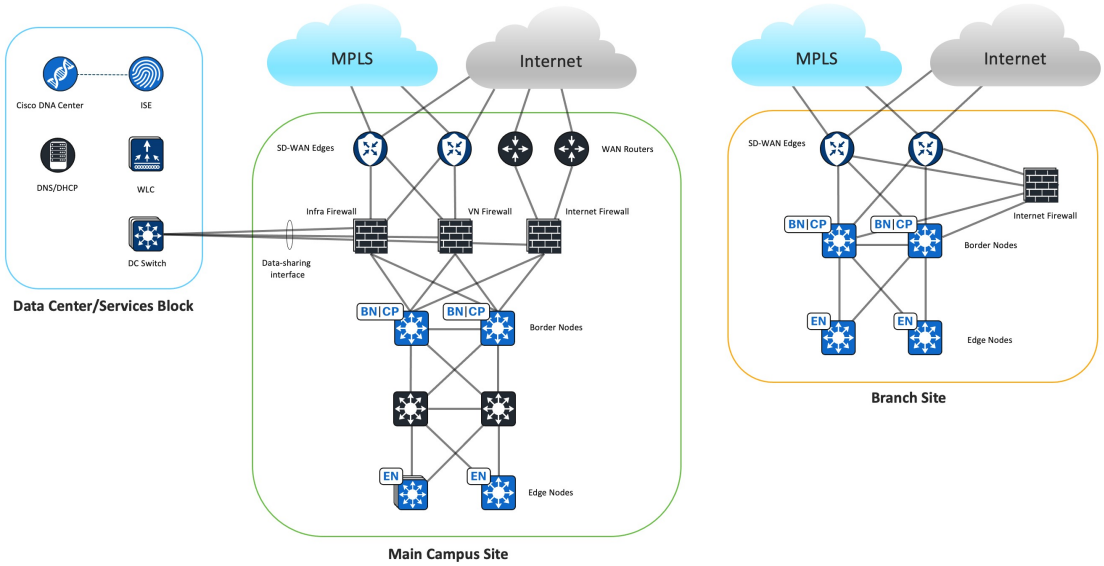
ソリューションのテストベッドの論理トポロジは、サイズが異なる複数 Cisco SD-Access のサイトを持つリファレンス カスタマー ネットワーク設計を表します。Cisco SD WAN ファブリックは、複数の Cisco SD-Access サイトとリモート データセンターを接続して、IPv4 および IPv6 トラフィックの転送を可能にします。キャンパスサイトとブランチサイトは、アップリンクの冗長性やノードの冗長性など、可能な限りの冗長性を備えて実装されています。このソリューションでは、Catalyst スイッチとルータが使用されます。メインキャンパスには、Cisco Catalyst 9000 スイッチと Cisco Catalyst 9800 ワイヤレスコントローラが導入されています。Cisco SD WAN エッジルータには、Cisco Catalyst 8000 および Cisco ASR 1000 シリーズ ルータが含まれます。

各サイトでは、Cisco Firepower アプライアンスにより、内部およびインターネットトラフィックのセキュリティ要件が実装されます。Cisco Firepower アプライアンスにより、DNS64 と連携して IPv4 サーバーへの IPv6 専用クライアントの到達可能性を提供するネットワークアドレス変換 64（NAT64）が有効になります。Cisco Firepower アプライアンスは、Firepower Management Center（FMC）によって一元管理されます。

このアーキテクチャでは、データセンターには、ドメインネームシステム（DNS）、Dynamic Host Configuration Protocol（DHCP）、その他のアプリケーションなどの集中型サービスが含まれています。Cisco DNA Center、ワイヤレスコントローラ、Cisco ISE、および Cisco FMC は、IPv4 と IPv6 の両方のサービスをサポートするメインサイトキャンパスと同じ場所にあるデータセンターに導入されます。このソリューションでは、Cisco DNA Center と Cisco ISE が設定され、IPv4 アドレスと統合されます。

メインキャンパスサイトの設計の概要

図 *2:* メインキャンパスとブランチサイトの論理図



メインキャンパスサイトの設計では、Cisco SD-Access Fusion デバイスとして Cisco Firepower 9300 を使用します。この設計は、データセンターとインターネットの共有リソースへのアクセスを許可しながら、Cisco SD-Access 仮想ネットワーク（VN）間のマクロセグメンテーションを実現することを目的としています。外部 BGP（eBGP）は、Cisco SD WAN エッジルータ、ファイアウォール、および Cisco SD-Access ファブリックボーダー間のプレフィックス到達可能性の交換を容易にするための優先ルーティングプロトコルです。このプロトコルは、Bidirectional Forwarding Detection（BFD）、きめ細かいプレフィックス フィルタリング、および最適パス選択に影響を与える BGP 属性による高速コンバージェンスを提供します。

コントロールプレーンとデータプレーンの統合

ファイアウォールは、Cisco SD-Access VN を Cisco SD WAN VPN に接続するために、Cisco SD-Access ファブリックボーダーと Cisco SD WAN エッジデバイスの間に配置されます。この配置により、異なるサイト間で同じ VN 通信が可能になります。この場所で、ファイアウォールはセキュリティポリシーを適用して、Cisco SD WAN 間の異なるサイトにある同じ Cisco SD-Access VN ホスト間のトラフィックを許可または拒否できます。ファイアウォールは、データセンターの共有サービスネットワークに向かうトラフィックも保護します。

このソリューションテストでは、コントロールプレーンの分離のために、Cisco SD-Access VN ごとに 1 つのファイアウォールインスタンスが作成されます。ファイアウォールインスタンスの観点からは、すべてのルーティングはグローバル ルーティング テーブルで行われます。Cisco SD-Access VN と Cisco SD WAN サービス VPN の間に 1 対 1 のマッピングを作成するために、1 つのファイアウォール サブインターフェイスがファブリックボーダー VN インターフェイスに接続され、別のファイアウォール サブインターフェイスが Cisco SD WAN エッジデバイスのサービス側インターフェイスに接続されます。ファイアウォール インスタンスは、Cisco SD-Access VN と Cisco SD WAN サービス VPN の間でルートを交換するために、Cisco SD-Access ボーダーおよび Cisco SD WAN エッジデバイスへの BGP ピアリングセッションを確立します。Cisco SD WAN エッジデバイスは、サービス VPN の相互 BGP からオーバーレイ管理プロトコル（OMP）へのルート再配布を実行します。

IPv6 パケットは、メインサイトのファブリックエッジに入ると、VXLAN でカプセル化され、Cisco SD-Access ファブリックを介してファブリックボーダーに送信されます。ファブリックボーダーはフレームのカプセル化を解除し、ファイアウォールに転送します。その後、ファイアウォールが Cisco SD WAN エッジデバイスのサービス側インターフェイスにフレームを転送します。その後、IPv6 パケットは IPsec でカプセル化され、Cisco SD WAN ファブリックを介して送信されます。受信側の Cisco SD WAN ブランチエッジはカプセル化解除を実行し、IPv6 パケットをブランチ ファブリック ボーダーに送信します。その後、ブランチ ファブリック ボーダーは VLXAN でカプセル化してブランチファブリックエッジに転送します。

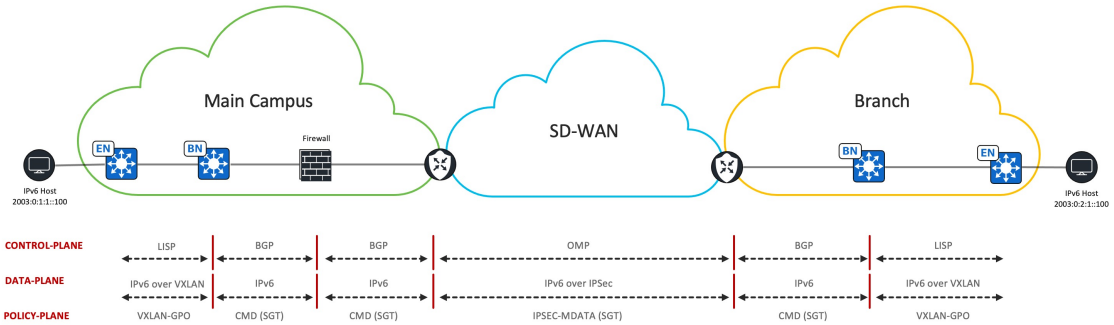
IPv6 Enterprise ワイヤレストラフィックと IPv4 ワイヤレストラフィックは、同じ方法を使用して Cisco SD-Access ファブリックを介して転送されます。IPv6 と IPv4 の両方のワイヤレストラフィックは、アクセスポイント（AP）から VXLAN トンネルを介してファブリックエッジに送信されます。

このセットアップでは、サイト間でエンドツーエンドのコントロールプレーンとデータプレーンの分離が維持されることに注意してください。

ポリシープレーンの統合

セキュリティグループタグ（SGT）インラインタギングは、Cisco SD WAN エッジデバイス、ファイアウォール、および Cisco SD-Access ファブリック ボーダー デバイス間のインターフェイスで有効になっています。SGT はファブリック VXLAN ヘッダーから転送され、メインサイトのファブリックボーダーによってイーサネットヘッダーの Cisco Meta Data（CMD）フィールドに配置され、ファイアウォールに送信されます。ファイアウォールから Cisco SD WAN エッジデバイスにフレームが送信され、SGT がイーサネット CMD フィールドから IPsec CMD フィールドにコピーされ、Cisco SD WAN ファブリック全体に伝送されます。受信側 Cisco SD WAN ブランチエッジでは、SGT が IPsec CMD フィールドからイーサネット CMD フィールドに転送されます。このイーサネットフレームはブランチ ファブリック ボーダーに送信されます。ボーダーで SGT がイーサネット CMD フィールドから VXLAN ヘッダーに転送され、ファブリックエッジに転送されます。このセットアップでは、サイト間でエンドツーエンドのポリシープレーンの分離が維持されることに注意してください。

図 *3 : IPv6*、*Cisco SD-Access*、および *Cisco SD WAN* のコントロールプレーン、データプレーン、およびポリシープレーンへの統合



Cisco SD WAN 間の Cisco SD-Access アンダーレイトラフィック

メインキャンパスサイトでは、Cisco DNA Center はデータセンター内にあります。デバイスの検出、管理、およびモニタリングのために、Cisco DNA Center と Cisco SD WAN 間のリモートサイトにあるすべての Cisco SD-Access ファブリックデバイス間の通信が必要です。この目的のために、Cisco SD WAN ファブリック全体で Cisco SD-Access アンダーレイトラフィックを伝送するために専用のサービス VPN が使用されます。インフラ ファイアウォール インスタンスは、この Cisco SD WAN サービス VPN インターフェイスに接続して、共有サービスネットワークと Cisco SD WAN 間のリモート Cisco SD-Access ファブリックデバイス間のパスを開きます。インフラ ファイアウォール インスタンスは、メイ

ンサイトのファブリック ボーダー グローバル インターフェイスにも接続し、メインサイトの Cisco SD-Access ファブリックデバイスへの到達可能性を有効にします。

Cisco SD-Access Fusion デバイスとしてのファイアウォール

Cisco SD-Access では、Fusion ルータはグローバル共有サービスルートと Cisco SD-Access VN ルートの間でルートリークを実行します。Cisco Firepower アプライアンスを Cisco SD-Access Fusion デバイスとして使用する場合、各ファイアウォール インスタンスにはグローバル ルーティング テーブルのみがあるため、ファイアウォール インスタンス間でルートがリークされることはありません。代わりに、ルートは Cisco Firepower アプライアンスのデータ共有インターフェイスを介して交換されます。各ファイアウォール インスタンスは、共有サービスネットワークにアクセスするために、データセンタースイッチに接続している同じデータ共有インターフェイスを共有します。各ファイアウォール インスタンスは、同じサブネット上に一意の IP アドレスを持ち、データセンタースイッチと eBGP ピアリングを形成して、ローカル Cisco SD-Access VN ルートをアドバタイズし、グローバル共有サービスルートを受信します。

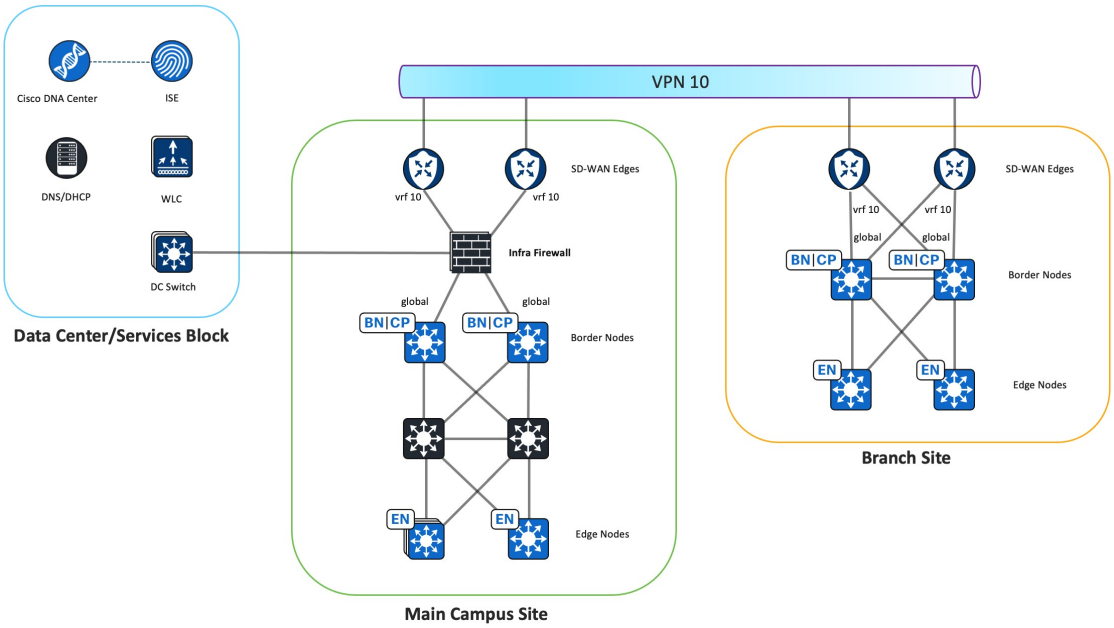
ファイアウォールでのステートフル インスペクションでは、戻りパケットが元のパケットと同じインターフェイスに到着する必要があります。ファブリックボーダーに接続された2つの内部ファイアウォールインターフェイスと、Cisco SD WAN エッジデバイスに接続された 2 つの外部ファイアウォール インターフェイスがあるため、ファイアウォールは別のインターフェイスに到着した戻りパケットをドロップします。冗長ファイアウォールリンクを使用するために、等コストマルチパス（ECMP）ルーティングゾーンが展開され、複数のインターフェイス間でのトラフィックの ECMP ルーティングとロードバランシングが可能になります。このソリューションテストでは、Cisco SD-Access ファブリックボーダーに接続された 2 つの内部ファイアウォール インターフェイスが 1 つの ECMP ゾーンに配置され、Cisco SD WAN エッジデバイスに接続された 2 つの外部ファイアウォール インターフェイスが別の ECMP ゾーンに配置されます。さらに、eBGP マルチパスは、宛先への 2 つの等コストパスを有効にするために、ファイアウォール BGP の設定で 2 に設定されます。

ファイアウォール インスタンスのタイプ

メインサイトでは、インフラファイアウォール、VN ファイアウォール、インターネット ファイアウォールの 3 種類のファイアウォールインスタンスが展開されます。次の図は、各ファイアウォールインスタンスの機能を示しています。

インフラ ファイアウォール インスタンス

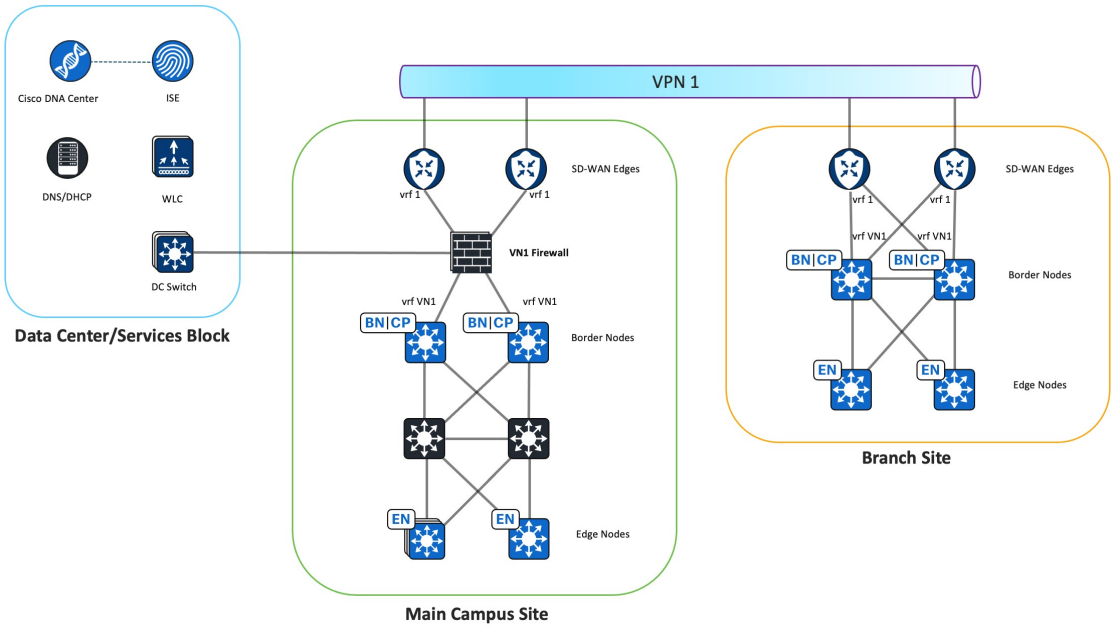
図 *4:*インフラ ファイアウォール インスタンス



- インフラ ファイアウォール インスタンスは、メインサイトとリモートブランチサイトで Cisco DNA Center が Cisco SD-Access ファブリックデバイスを検出するための Cisco SD-Access アンダーレイ接続を提供します。
- インフラ ファイアウォール インスタンスは、Cisco SD-Access ファブリック ボーダー グローバル インターフェイスと、共有サービスネットワークへのデータセンタースイッチに接続します。
- インフラ ファイアウォール インスタンスは、Cisco SD-Access アンダーレイトラフィック専用の Cisco SD WAN エッジサービス VPN にも接続し、リモートブランチサイトで Cisco DNA Center が Cisco SD-Access ファブリックデバイスを検出できるようにします。このソリューションの検証では、VPN 10 を使用して Cisco SD-Access アンダーレイトラフィックを転送します。
- インフラ ファイアウォール インスタンスは、データセンター内の Cisco SD-Access アンダーレイ ネットワークと共有サービスネットワーク間のトラフィックを許可します。
  - Cisco DNA Center、Cisco ISE、DNS、および DHCP への到達可能性をローカルおよびリモート Cisco SD-Access ファブリックデバイスに許可します。
  - AP からワイヤレスコントローラへの到達可能性を許可します。
  - AP から DHCP サーバーへの到達可能性を許可します。

VN ファイアウォール インスタンス

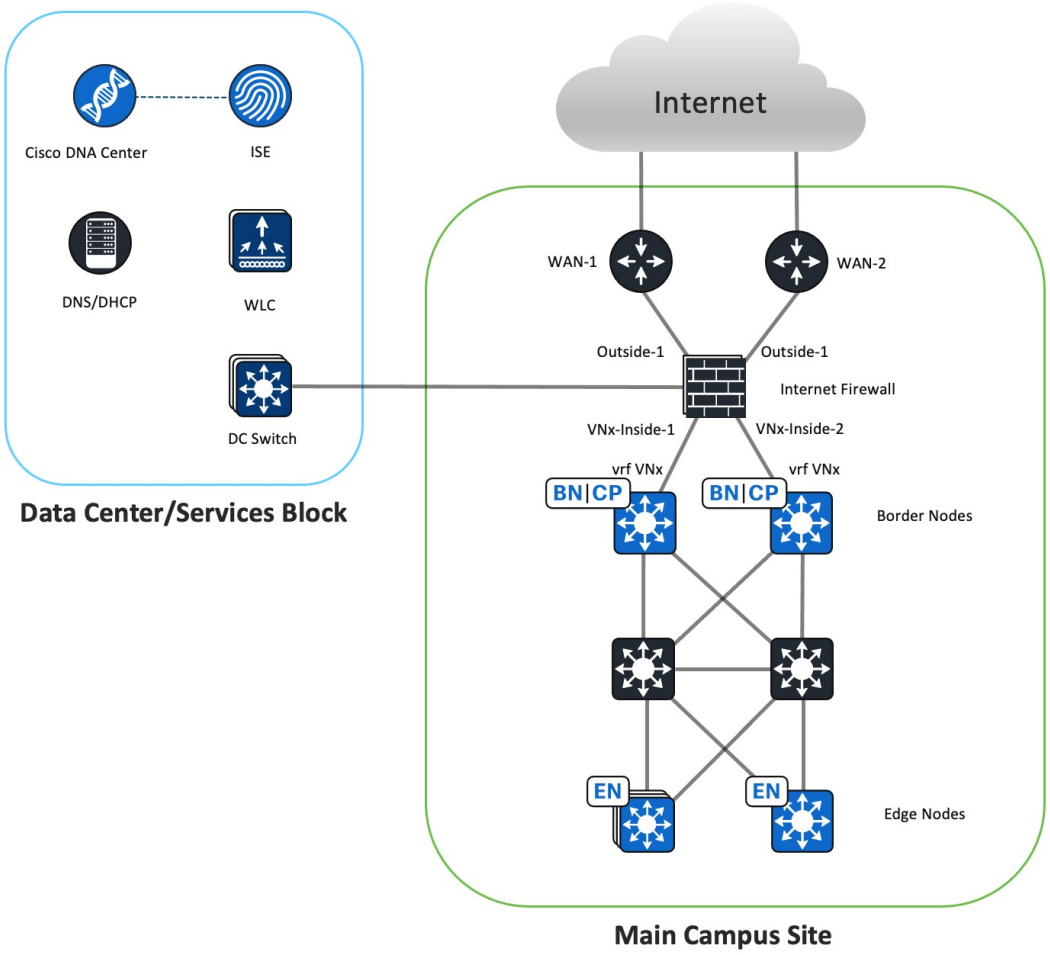
図 *5: VN* ファイアウォール インスタンス



- VN ファイアウォール インスタンスは、Cisco SD-Access VN を Cisco SD WAN VPN に接続し、データセンターの共有サービスネットワークへの VN 接続を提供します。
- Cisco SD-Access VN および関連する Cisco SD WAN VPN ごとに 1 つの VN ファイアウォール インスタンスがあります。この図は、Cisco SD-Access VN1 から Cisco SD WAN VPN 1 への関連付けを示しています。
- VN ファイアウォール インスタンスは、Cisco SD-Access ボーダー VN インターフェイスと Cisco SD WAN サービス側エッジインターフェイスに接続します。
- 各 VN ファイアウォール インスタンスは、データセンタースイッチに接続する同じデータ共有インターフェイスを共有します。eBGP ピアリングは、データセンタースイッチとファブリックボーダー VRF の間で形成され、Cisco SD-Access VN と共有サービスネットワークの間でルートを交換します。
- VN ファイアウォール インスタンスは、同じ VN 間のトラフィックを許可し、データセンター内の共有サービスネットワークへの到達可能性を提供します。
  - DHCP および DNS サーバーへの VN トラフィックを許可します。
  - 異なるサイト間で同じ VN トラフィックを許可します。
- デフォルトルートの送信元はインターネット ファイアウォール インスタンスから取得されるため、BGP デフォルトルートは Cisco SD-Access ファブリックボーダー VN からネイティブにフィルタリングされます。メインサイトのすべてのファイアウォール インスタンスで同じ BGP 自律システム（AS）番号が使用されるため、AS パス内にある同じローカル BGP AS 番号を持つ BGP プレフィックスはドロップされます。デフォルトルートは Cisco SD WAN エッジデバイスにアドバタイズされないため、インターネットベースのトラフィックがリモートサイトから送信されないことが重要です。インターネットベースのトラフィックは、各サイトでローカルに終了する必要があります。

インターネット ファイアウォール インスタンス

図 *6*: インターネット ファイアウォール インスタンス

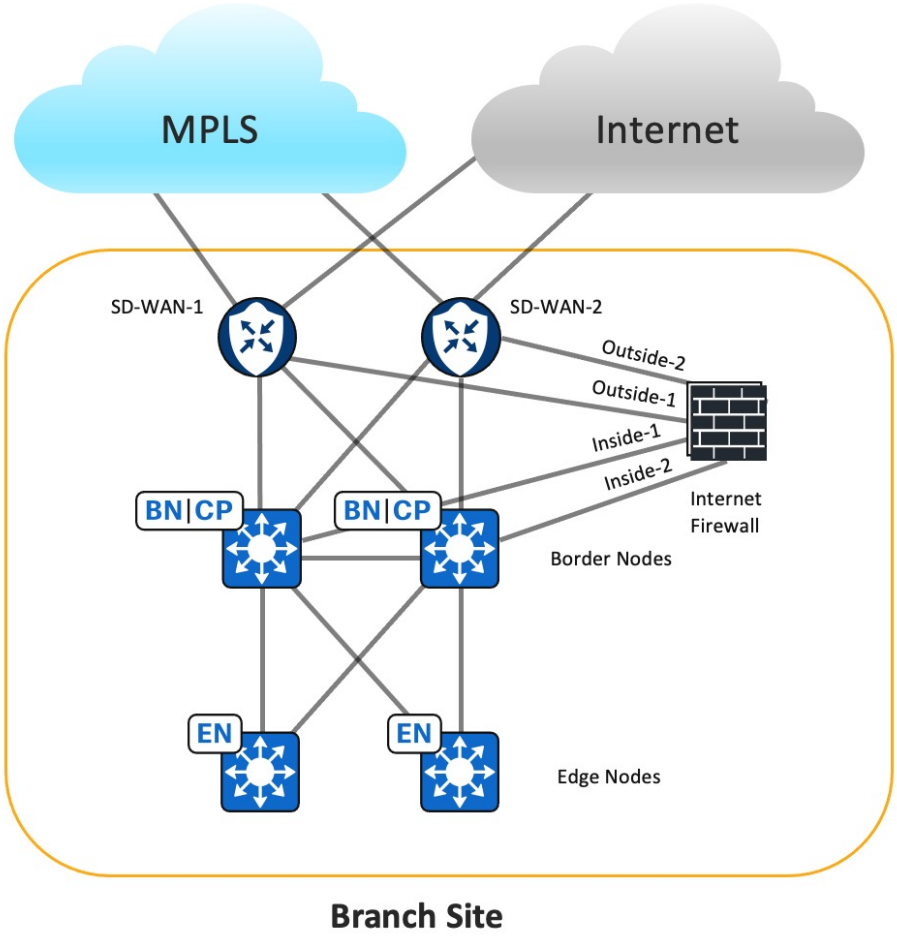


- インターネット ファイアウォール インスタンスは、Cisco SD-Access VN ホストへのインターネットアクセスを提供します。
- 1 つのインターネット ファイアウォール インスタンスがすべての Cisco SD-Access VN にサービスを提供します。
- メインサイトでは、インターネットファイアウォールインスタンスの外部インターフェイスはインターネットルータに直接接続し、内部インターフェイスは各ファブリックボーダー VN インターフェイスに接続します。
- インターネットファイアウォールインスタンスは、eBGP を介してインターネットルータにローカル Cisco SD-Access プレフィックスをアドバタイズします。
- インターネット ファイアウォール インスタンスは、eBGP を介してインターネットルータから IPv4 および IPv6 のデフォルトルートを受信します。
- インターネット ファイアウォール インスタンスは、IPv4 および IPv6 のデフォルトルートを eBGP を介してファブリックボーダーにアドバタイズします。

- インターネット ファイアウォール インスタンスは、マクロセグメンテーションを維持するために、異なる VN 間のトラフィックを拒否します。
  - インターネット ファイアウォール インスタンスはすべての VN へのルートを認識し、Cisco SD-Access ファブリックボーダーへのデフォルトルートをアドバタイズするため、ファイアウォールのアクセス コントロール ポリシーでこのオプションが許可されている場合は、VN 間でトラフィックをルーティングできます。
  - 暗黙的な拒否アクセス制御は、ある VN 内のホストが別の VN 内のホストと通信するのを防ぐために使用できます。また、明示的な拒否ルールを使用して、異なる VN 間の通信をブロックできます。
- インターネットファイアウォールインスタンスは、IPv4およびIPv6インターネットへのアウトバウンドトラフィックを許可します。
- ファイアウォールのステートフル インスペクションは、トラフィックのリターンを許可します。
- インターネット ファイアウォール インスタンスは NAT64 機能を実行し、IPv6 クライアントが IPv4 インターネットに到達できるようにします。
- データ共有ファイアウォール インターフェイスは、データセンターへのインターネットアクセスを提供します。

ブランチサイトの設計の概要

図 *7:* ブランチサイトの論理図



ブランチサイトの設計では、Cisco Firepower 2110 をインターネット ファイアウォールとして厳密に展開します。Cisco SD-Access では、ファブリックボーダーが外部ボーダーとして設定されます。2 つの Cisco SD WAN エッジデバイスがファブリックボーダーに接続してオーバーレイトラフィックを処理し、リモートサイトの Cisco SD-Access ネットワークとの通信を可能にします。トランスポートロケータ（TLOC）拡張は、IPv6 トランスポートではサポートされていないため、各 Cisco SD WAN ルータには 2 つの WAN インターフェイスが設定されています。

ファブリックボーダー VN インターフェイスは、内部ファイアウォールのサブインターフェイスに接続します。 eBGP ピアリングは、ファイアウォールと各ファブリックボーダー VN の間で形成されます。ファブリックボーダー VN は、デフォルトの IPv4 および IPv6 ルートを受信し、VN がインターネットに到達できるようにします。また、ファブリックボーダーには、対応する Cisco SD WAN サービス側エッジインターフェイスに接続する VN インターフェイスがあります。Cisco SD WAN エッジデバイスとの eBGP ピアリングを形成して、ローカル Cisco SD-Access ルートをアドバタイズし、同じ VN 内のリモート Cisco SD-Access ネットワーク、およびデータセンター内の共有サービスネットワークへの特定のルートを受信します。ブランチサイトが他のサイトからのインターネットトラフィックのトランジットサイトになるのを防ぐために、ファブリックボーダーは Cisco SD WAN エッジデバイスへの BGP デフォルトルートをフィルタリングします。

すべての VN ルートはファイアウォールのグローバル ルーティング テーブルに集まり、各ファブリックボーダー VN にはインターネット ファイアウォールへのデフォルトルートがあるため、異なる VN 間でトラフィックをルーティングできます。VN 間トラフィックが必要な場合を除き、異なる VN 間のトラフィックを拒否するようにアクセスポリシーを設定する必要があります。

ブランチファイアウォールのインターネットアクセス

通常、ISP からの 1 つのインターネットフィードは、ブランチサイトの Cisco SD WAN エッジデバイスに直接接続するため、ファイアウォールの外部インターフェイスを Cisco SD WAN エッジデバイスに接続してグローバルインターネットにアクセスすると、コスト効率が高くなります。現在、グローバルからサービスへの VPN ルートリークは IPv6 ではサポートされていないため、このソリューションはファイアウォールの外部インターフェイスを Cisco SD WAN エッジデバイスの VPN0 インターフェイスに接続します。

インターネット ファイアウォールの Outside-1 インターフェイスは、SD-WAN-1 エッジ VPN0 インターフェイスに接続します。インターネット ファイアウォールの Outside-2 インターフェイスは、SD-WAN-2 エッジ VPN0 インターフェイスに接続します。グローバルルーティングは、Cisco SD WAN インターネット トランスポート インターフェイスと VPN0 インターフェイスの間で発生し、インターネット ファイアウォールの外部インターフェイスに接続します。デフォルトでは、トンネルインターフェイスとして設定された WAN トランスポート インターフェイスから非 Cisco SD WAN インターフェイスへのトラフィックはドロップされます。2 つの VPN0 インターフェイス間でトラフィックを渡すために、ローカライズされたデータポリシーと明示的な Cisco SD WAN アクセス制御リスト（ACL）が Cisco SD WAN エッジデバイスに適用されます。

ハードウェアとソフトウェアの仕様

ソリューションは、次の表に示すハードウェアとソフトウェアで検証されています。サポートされているハードウェアの完全なリストについては、「Cisco Software-Defined Access Compatibility Matrix」を参照してください。

ロール	ハードウェア プラットフォーム	ソフトウェア バージョン
Cisco DNA Center コントローラ	DN2-HW-APL	2.3.3.7
Cisco Identity Service Management、RADIUS サーバー	仮想（ISE-VM-K9）プラットフォーム	3.1 パッチ 4
Cisco SD WAN NMS コントローラ	vManage	20.10
Cisco SD WAN エッジデバイス	ASR1002-X	17.9.2a
Cisco SD WAN エッジデバイス	C8300、C8500	17.10
Cisco SD-Access ファブリック ボーダー ノード	C9500H/C9600	17.9.3
Cisco SD-Access ファブリック コントロール プレーン ノード	C9500H/C9600	17.9.3
Cisco SD-Access ファブリックエッジ	C9200, C9300, C9400	17.9.3

ロール	ハードウェア プラットフォーム	ソフトウェア バージョン
Cisco Industrial Ethernet 4000 拡張ノード	IE4000	15.2(8)E1
Cisco ワイヤレス LAN コントローラ	C9800-40、C9800-CL	17.9.3
Cisco Firepower Threat Defense セキュリティアプライアンス	FPR9300、FPR2110	7.2
Cisco Secure Firewall Management Center	FMC 仮想	7.2

スケール

ソリューションのテストでは、次の表に示すスケールの数値について確認しました。ソフトウェアおよびハードウェアキャパシティについては、Cisco DNA Center のデータシート [英語] を参照してください。

カテゴリ	スケール番号
サイトごとの VN	5
サイトごとのワイヤレスコントローラ	HA あたり 2
ファブリックサイト	10
サイトごとの AP	200 ～ 1,000
IPv6 エンドポイント	20,000
サイトごとの SSID	4
SGT	100
トラフィックプロファイル	ユニキャストおよびマルチキャスト

ソリューションの導入例のシナリオ

次のユースケースは、 IPv6 業界プロファイルで検証されています。

- IPv4 および IPv6 トラフィックの自動でセキュアな Cisco SD WAN 転送
- IPv6 Enterprise ユーザー向けのファブリック対応ワイヤレス展開
- IPv6 デバイスとエンドポイントのネットワークの可視性、モニタリング、およびトラブルシューティング
- IPv6 アプリケーションの可視性と正常性
- IPv6 ネットワークのネットワークの堅牢性

- さまざまな IPv6 専用エンドポイントのセキュアなオンボーディング
- エンドツーエンドの IPv6 トラフィックとセキュアなインターネットアクセス
- Cisco SD WAN 間の Cisco SD-Access サイト間におけるエンドツーエンドのインライン SGT トラフィックの適用
- IPv6 専用クライアントは、IPv6 アプリケーションおよびレガシー IPv4 アプリケーションにアクセスします。
- Quality of Service（QoS）とパス選択による IPv6 アプリケーション パフォーマンスの最適化
- IPv6 エンドポイントとアドレスの拡張性
- 次の操作に関する n 日目の操作：イメージのアップグレード、設定管理、バックアップと復元、およびネットワーク拡張。

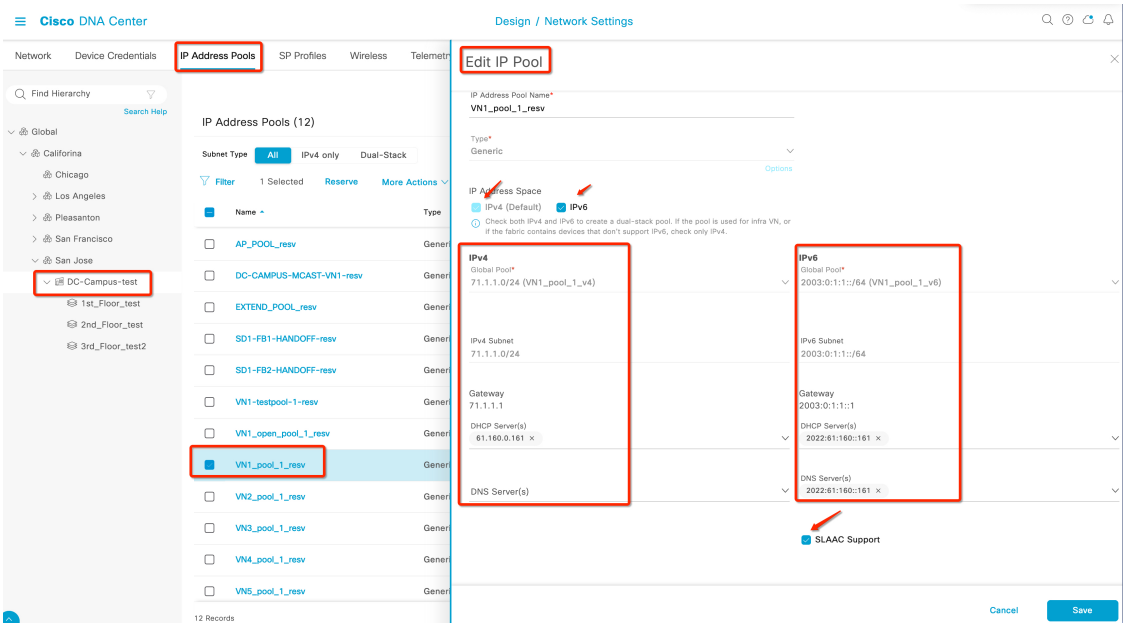
ソリューションの重要事項

ここでは、IPv6 ソリューションの展開に役立つ重要なテクニカルノートについて説明します。

IPv6 アドレスプールの設定

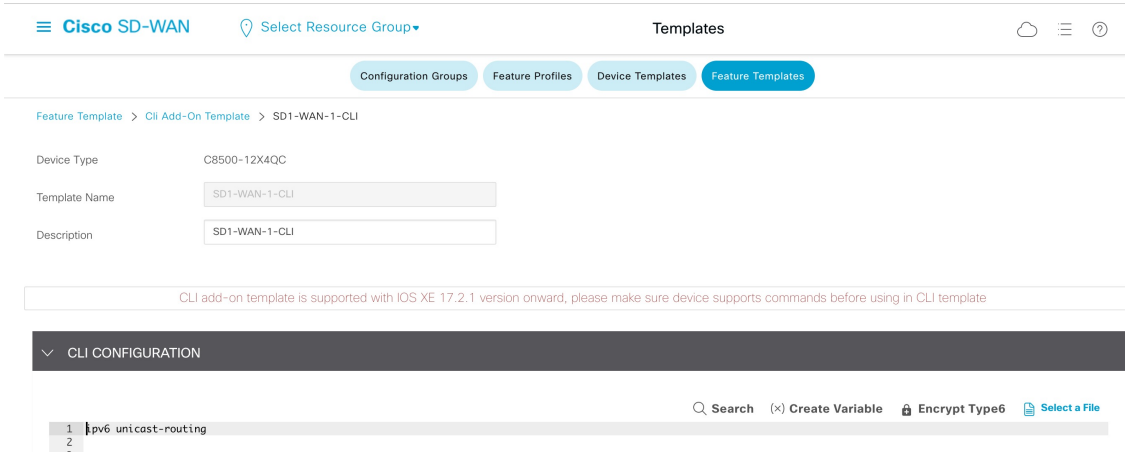
Cisco DNA Center リリース 2.3.3.x では、Cisco SD-Access サイトの IP プールを予約できます。この予約では、IPv4 プールと IPv6 プールの両方を指定する必要があり、指定することでデュアルスタック IP プールが作成されます。

クライアントが IPv6 アドレスのみを使用するように制限するには、クライアントで IPv4 アドレッシングを無効にするか、ダミーの IPv4 プールとダミーの DHCPv4 サーバーを設定します。ユーザーサブネットのステートレスアドレス自動設定（SLAAC）を有効にするには、[IPv6] エリアで、IPv6 プールの [SLAAC Support] チェックボックスをオンにします。



Cisco SD WAN エッジデバイスでの IPv6 ユニキャストルーティングの有効化

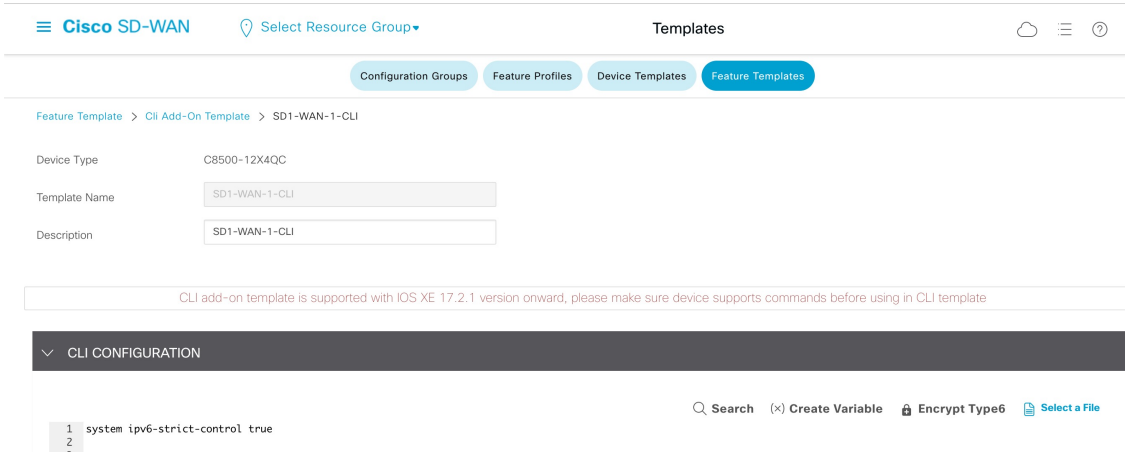
Cisco SD WAN エッジデバイスの場合は現在、IPv6 ユニキャストルーティングは、デバイス CLI、または [Cli Add-On Template] を使用した Cisco SD WAN GUI を介し、`ipv6 unicast-routing` コマンドを使用して有効にします。



Cisco SD WAN エッジデバイスでの IPv6 Strict Control の有効化

トランスポート VPN0 WAN インターフェイスでデュアルスタックが設定されている場合、制御接続とデータ接続の両方で IPv6 よりも IPv4 が優先されます。Cisco IOS XE SD-WAN デバイスのリリース 17.10 以降および Cisco SD WAN コントローラのリリース 20.10 以降では、IPv6 Strict Control 機能を介して制御接続を形成するために、IPv4 アドレッシングよりも IPv6 アドレッシングを優先するように Cisco SD WAN コントローラと Cisco SD WAN エッジデバイスを設定できます。IPv6 Strict Control が有効になっている場合、デュアルスタック Cisco SD WAN エッジデバイス間のデータプレーン接続は IPv6 トランスポートを使用して確立されます。

Cisco SD WAN エッジデバイスでは、デバイスの CLI を使用するか、 [Cli Add-On Template] を使用した Cisco SD WAN GUI を使用して、IPv6 Strict Control を有効にします。



Cisco SD WAN エッジデバイスの 2 つの VPN0 インターフェイス間におけるトラフィックのルーティング

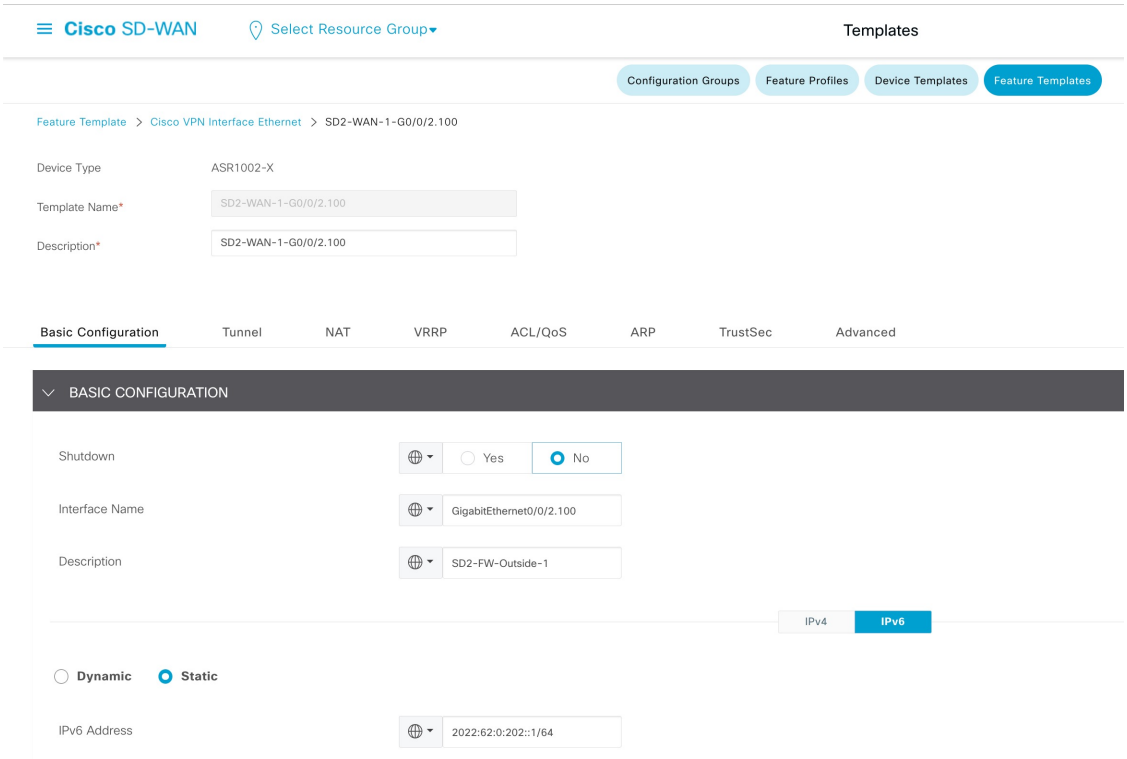
WAN トランスポート トンネル インターフェイスから非 Cisco SD WAN インターフェイスへのパケットのドロップは想定内の動作です。この動作を変更するには、ローカライズされたデータポリシーをデバイスに適用し、WAN トランスポート インターフェイスに明示的な Cisco SD WAN インバウンド ACL を適用します。この ACL により、ファイアウォールの外部インターフェイス サブネットおよび内部 IPv6 プレフィックスへのすべての IPv6 トラフィックが許可されます。

次の手順を使用して、ファイアウォールが Cisco SD WAN エッジデバイス VPN0 インターフェイスに接続し、Cisco SD WAN エッジインターネット WAN トランスポートを介して IPv6 インターネットにルーティングできるようにします。

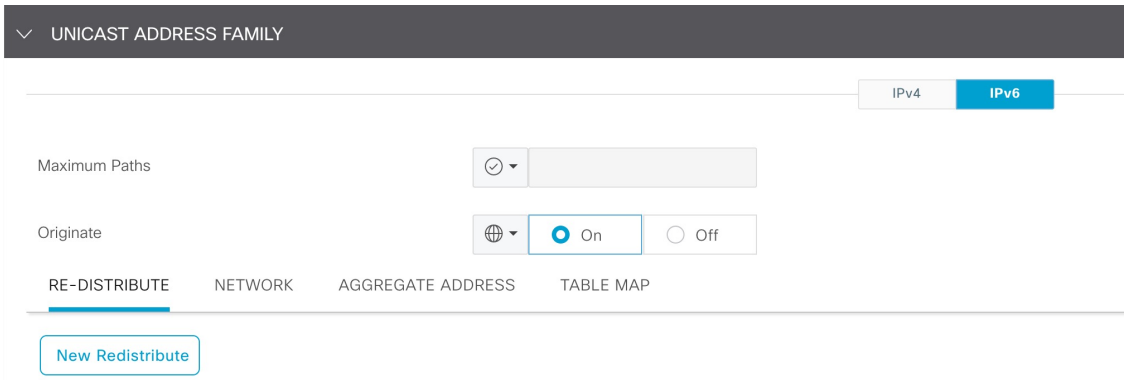
手順

ステップ 1 ファイアウォールの外部インターフェイス用の VPN インターフェイス イーサネット テンプレートと BGP テンプレートを作成し、デバイステンプレートの VPN0 トランスポートセクションに適用します。

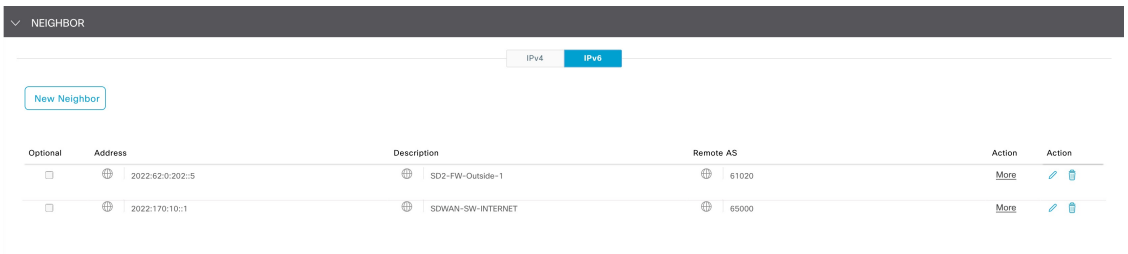
a) ファイアウォールの外部インターフェイスに接続するサブインターフェイスの VPN インターフェイス イーサネット テンプレートを作成します。



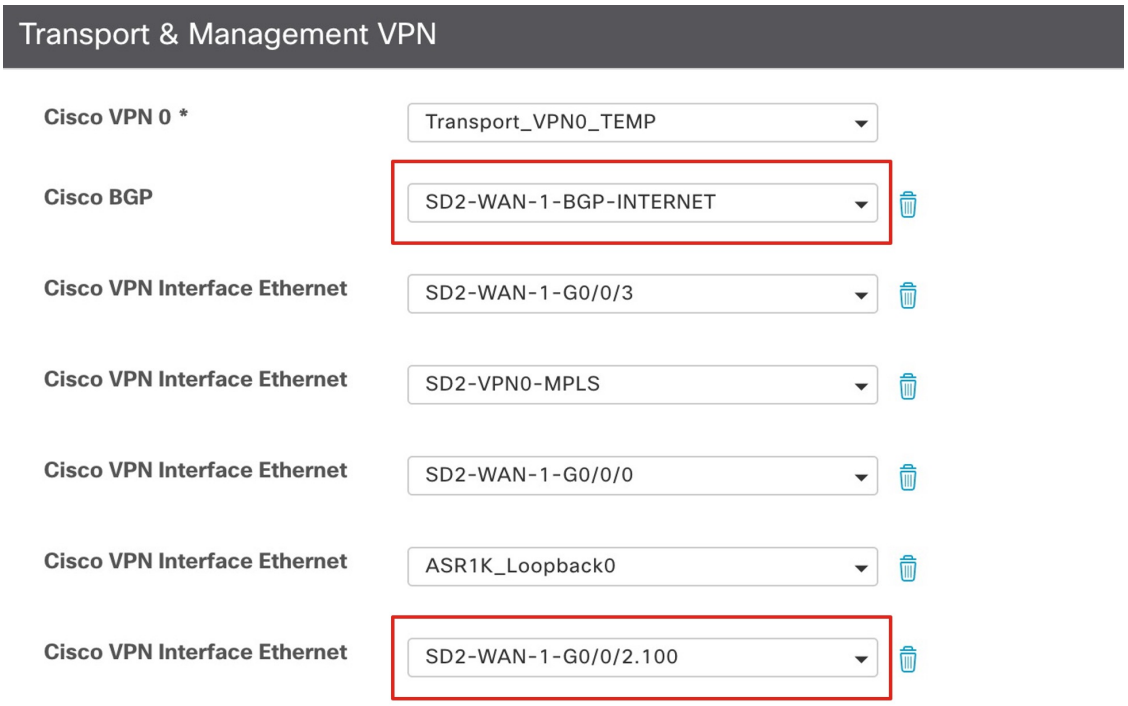
b) BGP テンプレートで、[BGP Default-Information Originate] を有効にして、Cisco SD WAN エッジデバイスがインターネットルータから学習したデフォルトルートをファイアウォールにアドバタイズできるようにします。



c) VPN0 インターフェイスの BGP テンプレートで、ファイアウォールとインターネットルータの BGP ネイバーを作成します。



d) [Transport & Management VPN] エリアで、VPN インターフェイス イーサネットおよび BGP テンプレートをデバイステンプレートの VPN0 トランスポートセクションに適用します。

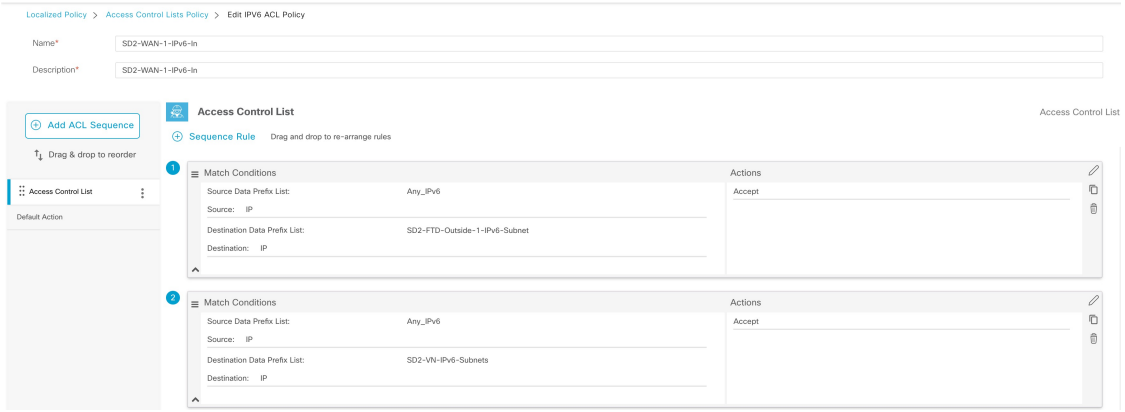


ステップ 2 ローカライズされたデータポリシーと明示的な Cisco SD WAN ACL を適用します。

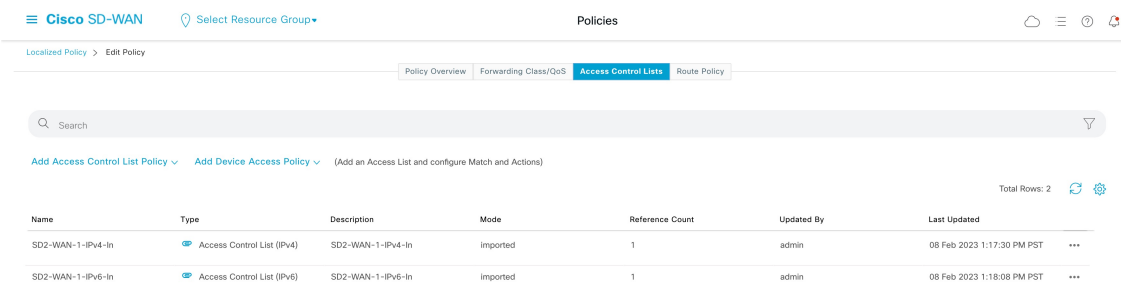
a) **[Configuration] > [Policies] > [Custom Options] > [Localized Policy] > [Lists]** ウィンドウで、次のデータプレフィックスを作成します。

- Any_IPv6 = ::/0
- SD2-FTD-Outside-1-IPv6-Subnet = 2022:62:0:202::/64
- SD2-VN-IPv6-Subnets = 2003:0:2::/48

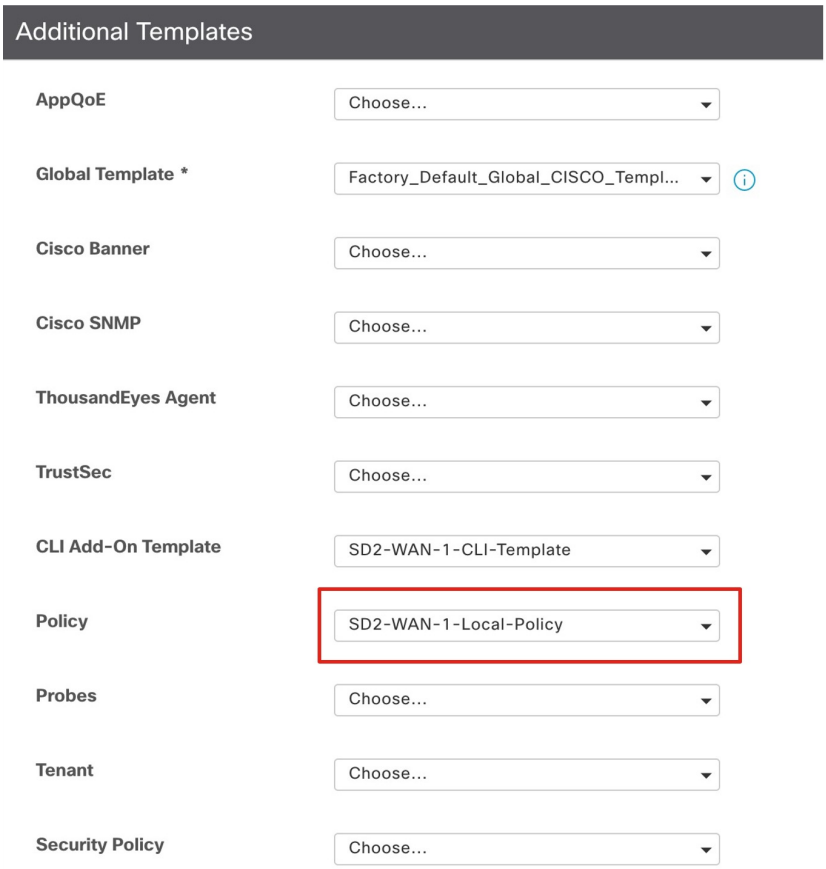
b) IPv6 ACL を作成して、ファイアウォールの外部インターフェイス、IPv6 サブネット、および内部 IPv6 サブネットに対する任意の IPv6 アドレスを許可します。



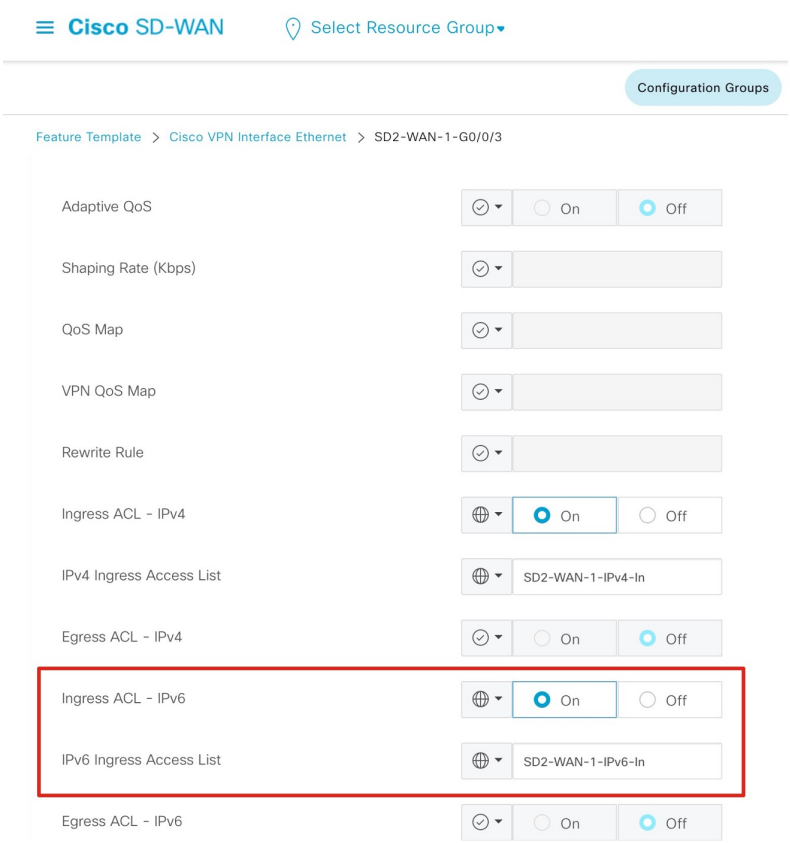
c) ローカライズされたデータポリシーに IPv6 ACL を適用します。



d) ローカライズされたデータポリシーをデバイステンプレートに適用します。



e) [Ingress ACL - IPv6] および [IPv6 Ingress Access List] をインターネット WAN トランスポート インターフェイス テンプレートに適用します。



Cisco Firepower アプライアンスでの NAT64 の設定

NAT64 は DNS64 サーバーと連携して、IPv6 専用クライアントがパブリック IPv4 インターネットに到達できるようにします。FMC を使用して Cisco Firepower アプライアンスの 1 つの内部インターフェイスと 2 つの外部インターフェイス間で NAT64 を設定するには、次の手順を使用します。

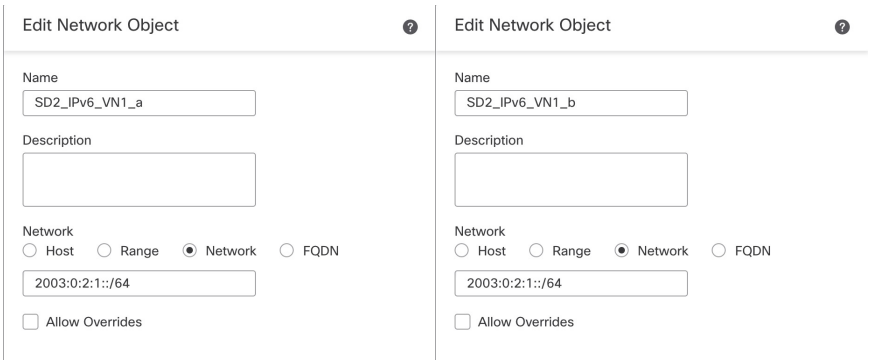
この手順では、NAT を実行して、DNS64/96 プレフィックス宛てのトラフィックの内部 Cisco SD-Access VN1 IPv6 アドレスを外部インターフェイスの IPv4 アドレスに変換します。逆方向の場合は、インターネットからの IPv4 アドレスを DNS64 /96 プレフィックスに変換するために NAT が適用されます。

手順

ステップ 1 **[Objects] > [Interface] > [Add Interface Group]** の順に選択し、Outside-1、Outside-2、および VN1-Inside インターフェイスを独自のインターフェイスグループに配置します。

ステップ 2 **[Objects] > [Network] > [Add Object]** の順に選択し、同じ内部 VN1 IPv6 サブネットの 2 つのネットワークオブジェクトを定義します。

自動NATで使用される各オブジェクトは、1つのNATステートメントのみを参照できるため、このステップが必要です。

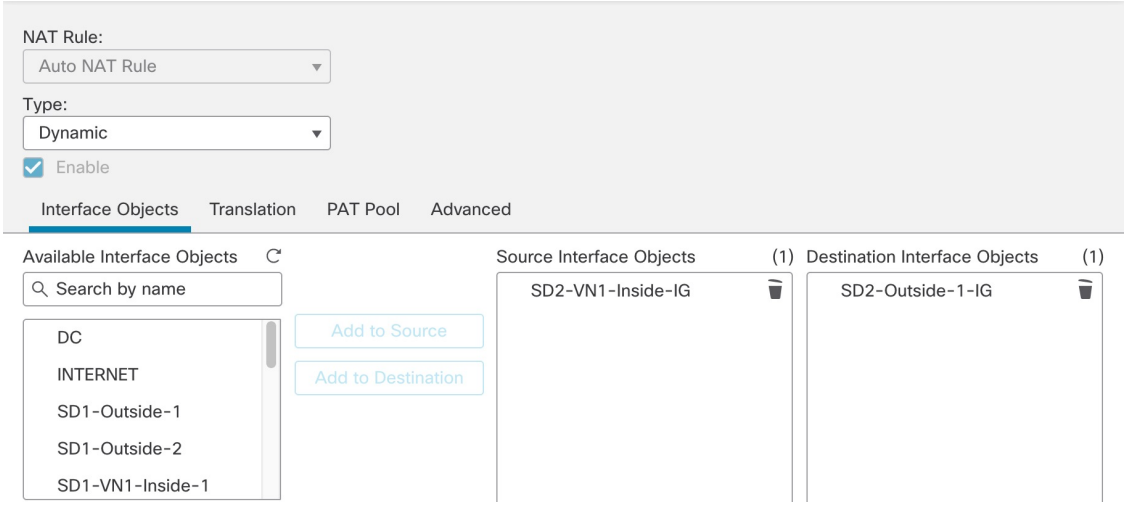


ステップ3 次の手順を実行して、内部 VN1 IPv6 サブネットの NAT を Outside-1 インターフェイス IP アドレスに設定する自動 NAT ダイナミックルールを作成します。

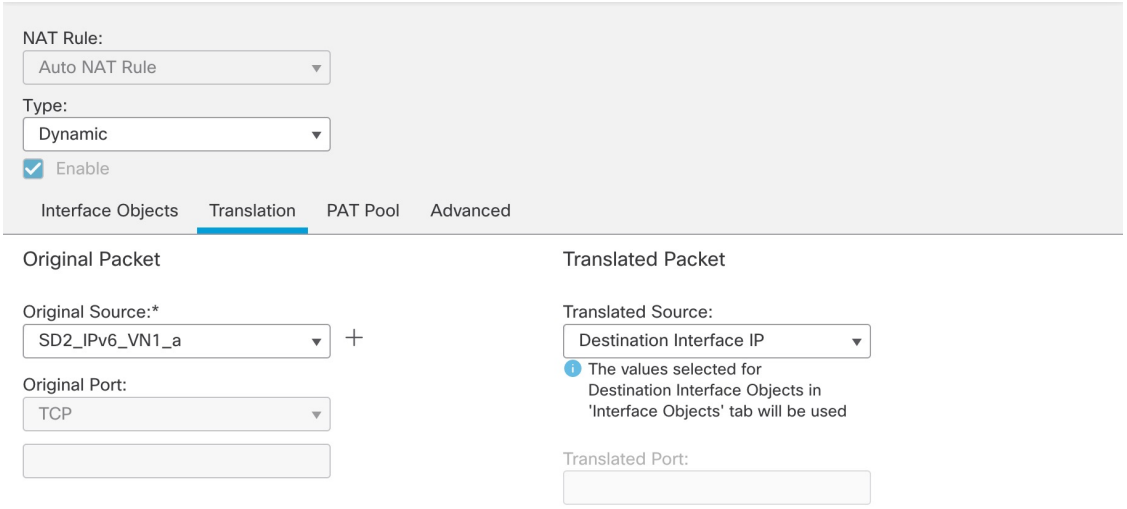
a) [NAT Rule] ドロップダウンリストから、[Auto NAT Rule] を選択します。

b) [Type] ドロップダウンリストから、[Dynamic] を選択します。

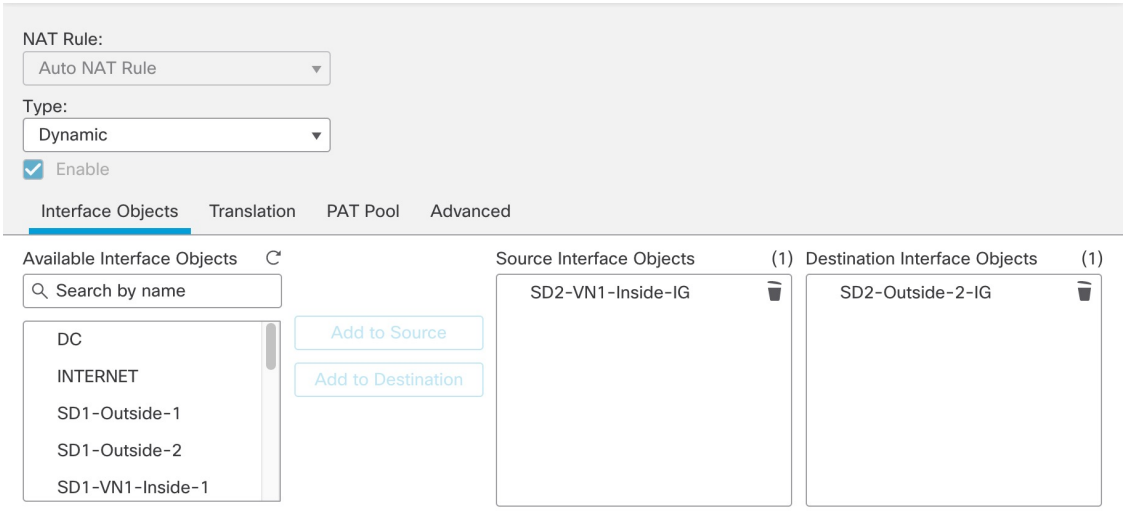
c) [Interface Objects] タブで、内部インターフェイスグループを [Source Interface Objects] に追加し、Outside-1 インターフェイスグループを [Destination Interface Objects] に追加します。



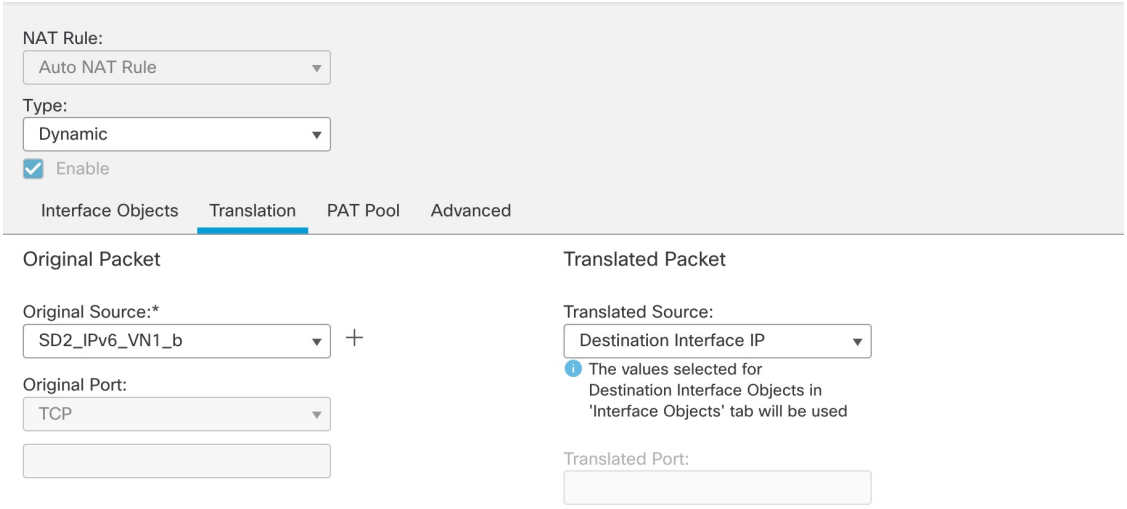
d) [Translation] タブの [Original Source] ドロップダウンリストから、内部 VN1 IPv6 サブネット用に作成された最初のネットワークオブジェクトを選択し、[Translated Source] ドロップダウンリストから [Destination Interface IP] を選択します。



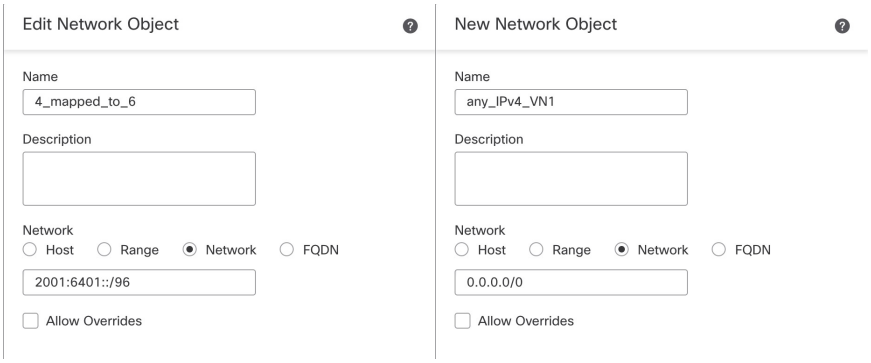
ステップ 4 ステップ 3 を繰り返して、内部 VN1 IPv6 サブネットの NAT を Outside-2 インターフェイス IP に設定するための 2 番目の自動 NAT ダイナミックルールを作成します。ただし、[Translation] タブでは、元の送信元に対して、同じ内部 IPv6 サブネットを参照する 2 番目のネットワークオブジェクトを使用します。



次の図は、元の送信元と同じ内部 IPv6 サブネットを参照する 2 番目のネットワークオブジェクトを示しています。



ステップ 5 NAT64 プレフィックス（2001:6401::/96）および任意の IPv4 アドレス（0.0.0.0/0）のオブジェクトを定義します。

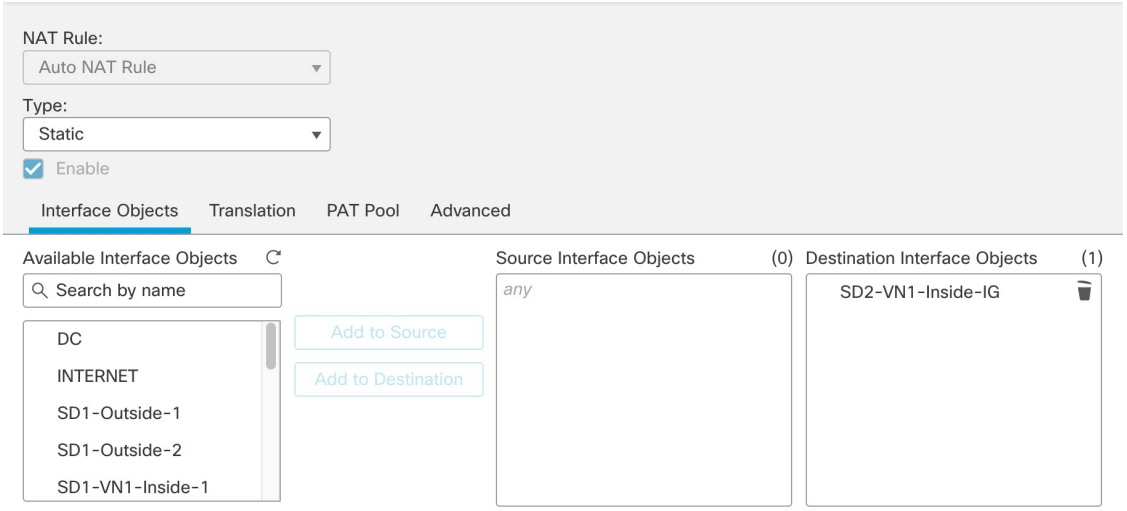


ステップ 6 次の手順を実行して、任意の IPv4 アドレスを NAT64 プレフィックスに変換する NAT を設定する自動 NAT スタティックルールを作成します。

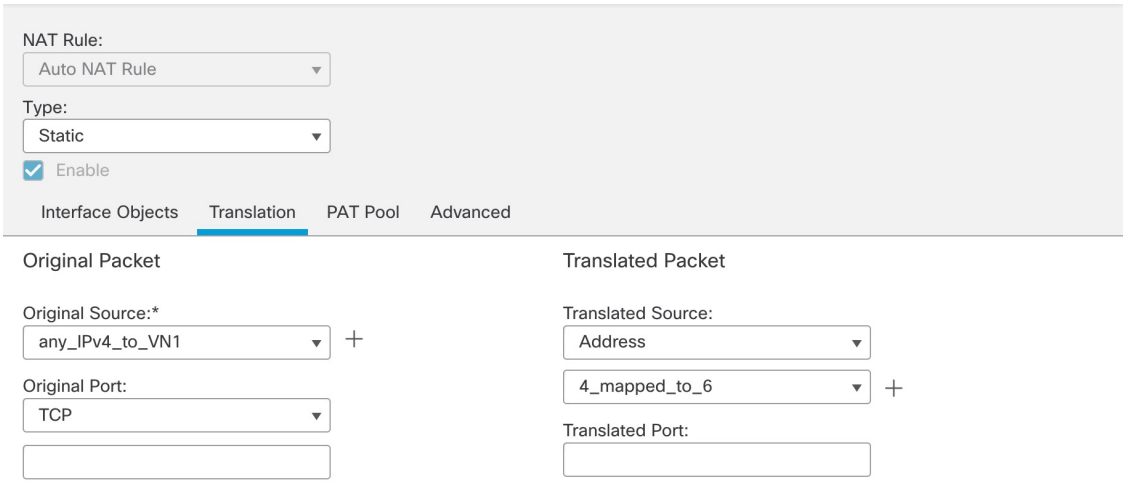
a) [NAT Rule] ドロップダウンリストから、[Auto NAT Rule] を選択します。

b) [Type] ドロップダウンリストから、[Static] を選択します。

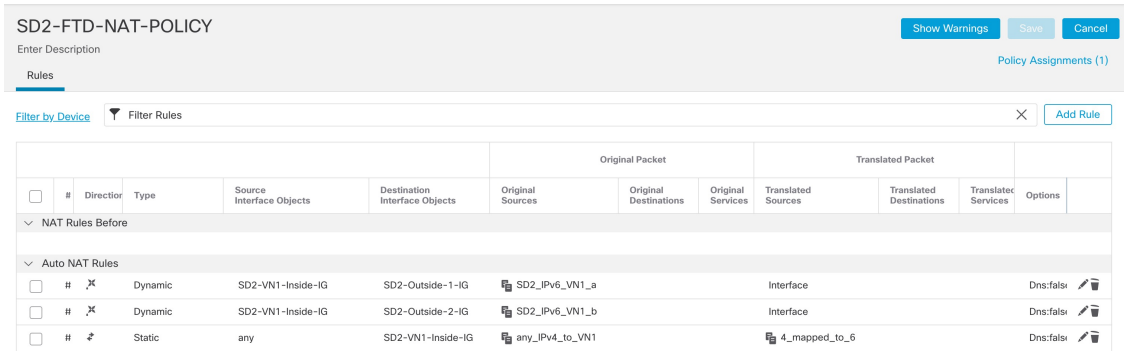
c) [Interface Objects] タブで、[Source Interface Objects] に「any」追加し、内部インターフェイスグループを [Destination Interface Objects] に追加します。



d) [Translation] タブの [Original Source] ドロップダウンリストから、任意の IPv4 ネットワーク オブジェクト オプションを選択し、[Translated Source] ドロップダウンリストから NAT64 プレフィックス オブジェクト オプションを選択します。



設定が完了すると、NAT64 ポリシーが表示されます。

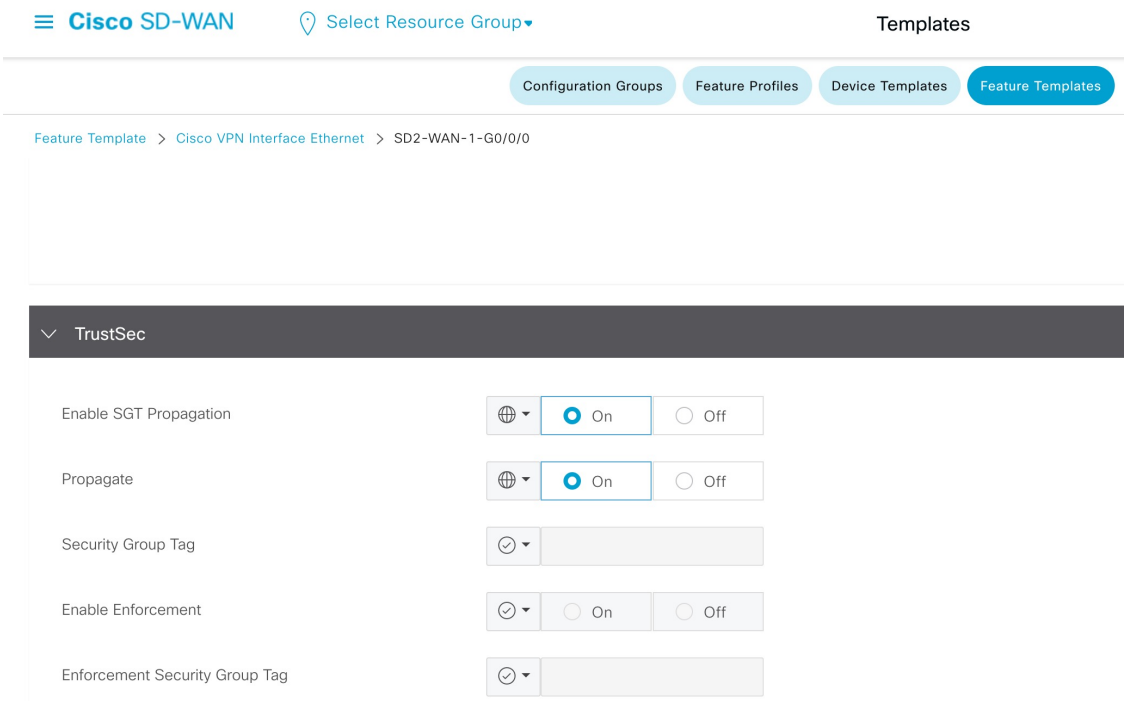


Cisco SD WAN エッジデバイスでの SGT 伝達の有効化

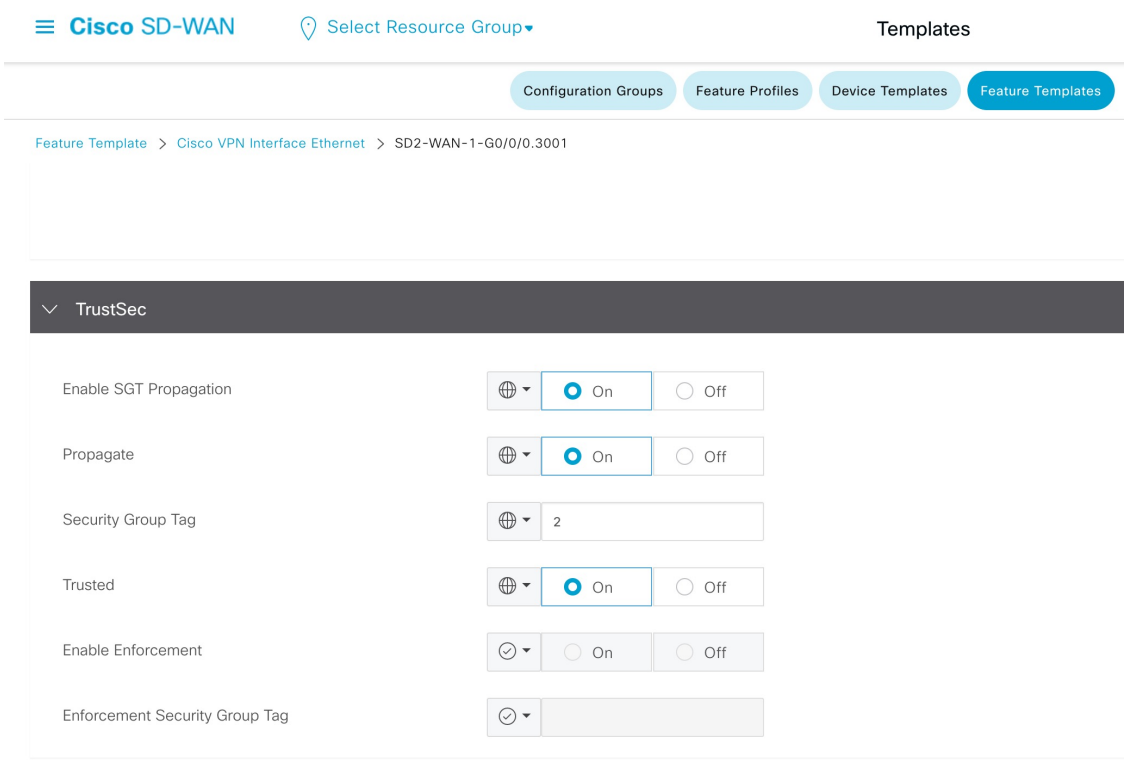
Cisco SD WANエッジデバイスとCisco SD-Accessファブリックボーダー間のSGTインラインタギングを設定するには、*SD-Access SD-WAN* 独立ドメイン統合ガイド [英語] の「Process 2: Configuring Cisco TrustSec Inline Tagging」の手順を使用します。20.6.1/17.6.1 以降、Cisco SD WAN トンネルインターフェイスでの SGT 伝達はデフォルトで無効になっているため、Cisco SD WAN間でSGT伝達を有効にするには追加の手順を実行する必要があります。次の手順に従い、WAN トランスポート トンネル インターフェイスで CTS SGT 伝達が有効になっていることを確認します。

手順

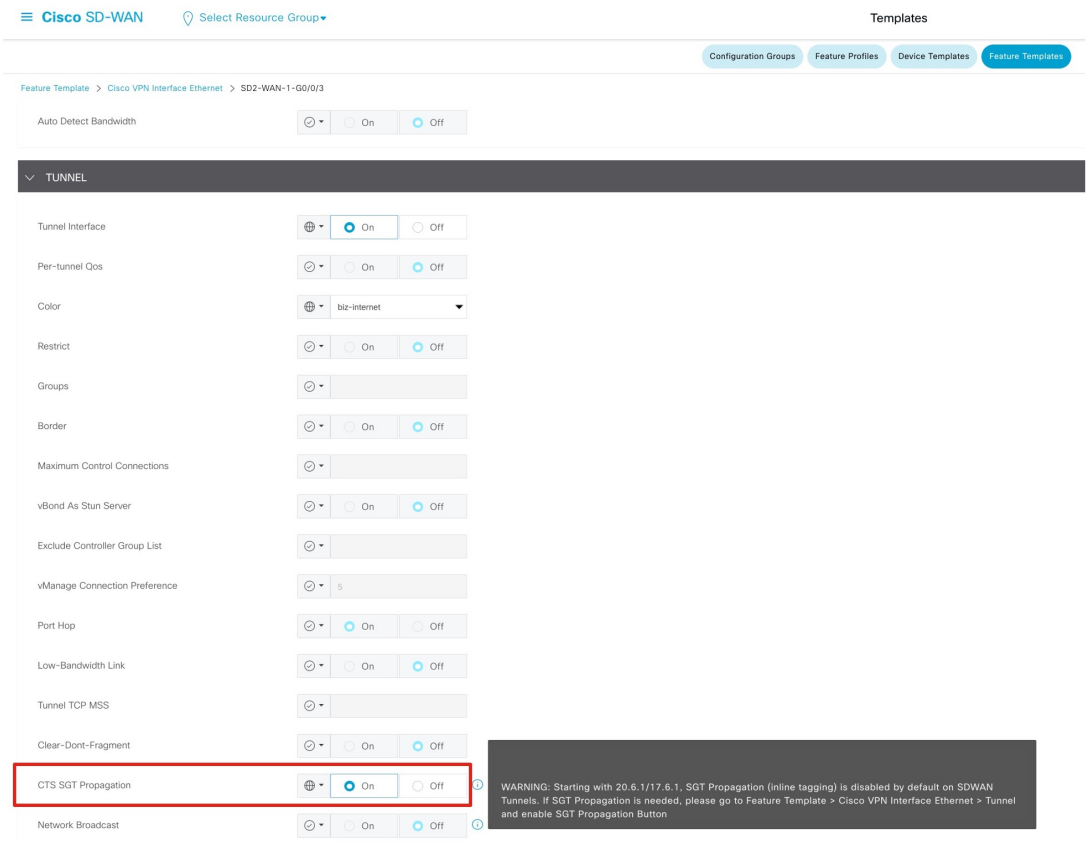
ステップ 1 Cisco SD WAN エッジデバイスの物理インターフェイスで、SGT インラインタギングを有効にします。このインターフェイスは、デバイステンプレートの VPN0 セクションに適用されます。



ステップ 2 Cisco SD WAN エッジデバイスのサービス VPN サブインターフェイスで、SGT インラインタギングを有効にします。

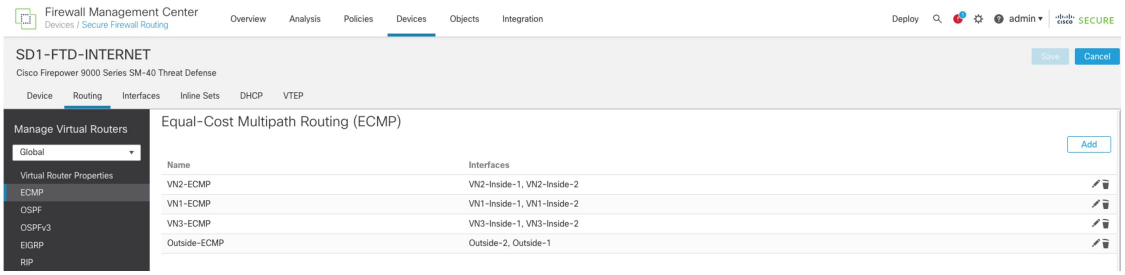


ステップ 3 各 WAN トランスポート トンネル インターフェイスで、[CTS SGT Propagation] を有効にします。

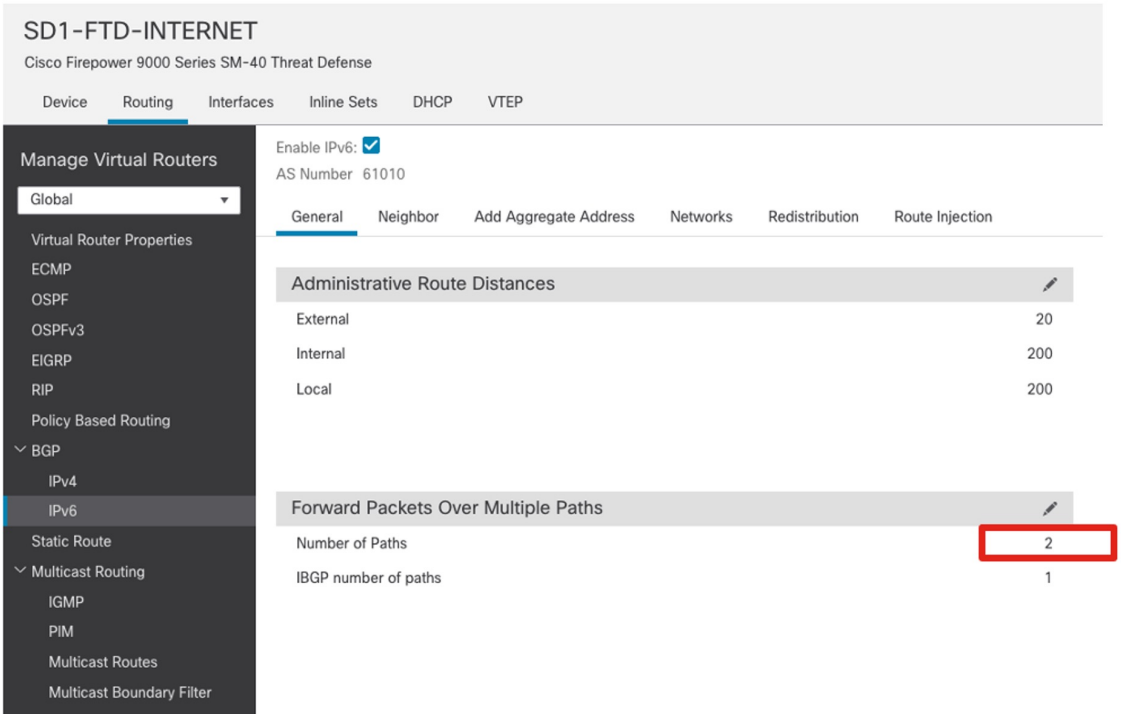


複数のインターフェイス間における ECMP ルーティングの有効化

次の ECMP 設定では、Outside-1 インターフェイスと Outside-2 インターフェイスの両方が Outside-ECMP ゾーンに割り当てられます。同様に、VN1-Inside-1 と VN1-Inside-2 の両方のインターフェイスが VN1-ECMP ゾーンに割り当てられます。



ECMP には等コストパスが必要です。ルーティングテーブルに 2 つの等コストルートをインストールするには、BGP を設定します。まず、BGP の [General] 設定に移動し、パスの数を 2 に設定します。



ファブリックボーダーとファイアウォール間の手動レイヤ 3 ハンドオフ

ファイアウォールがアクティブおよびスタンバイの高可用性（HA）モードに設定されている場合、モニタリングと管理のために各リンクでアクティブおよびスタンバイ IP アドレスを使用できます。ファブリックボーダーの IP アドレスまで考慮すると、リンク上の IP アドレスの数は 2 を超えます。Cisco DNA Center リリース 2.3.3.x 以前では、レイヤ 3 ハンドオフの自動化により、ポイントツーポイントリンクに IPv4 /30 および IPv6 /126 マスクが展開されます。より大きなアドレス空間に対応するために、手動レイヤ 3 ハンドオフを使用して、ファブリックボーダーとファイアウォール間のリンクを設定できます。このソリューションテストでは Cisco DNA Center リリース 2.3.3.7 を検証しているため、IPv4 には /24 マスクが使用され、IPv6 には /64 マスクが使用されます。この手順は、メインサイトとブランチサイトで使用できます。

（注） Cisco DNA Center リリース 2.3.4.x 以降では、各レイヤ 3 ハンドオフにカスタムサブネット（IPv4 の場合は /29、IPv6 の場合は /125 など）を展開できるため、Cisco DNA Center リリース 2.3.4.x 以降を実行している場合は、Cisco SD-Access GUI を使用して手動レイヤ 3 ハンドオフを展開できます。

手順

ステップ 1 ファブリックボーダーで、各 VN のレイヤ 3 SVI を定義し、ファブリックボーダーで BGP を設定します。

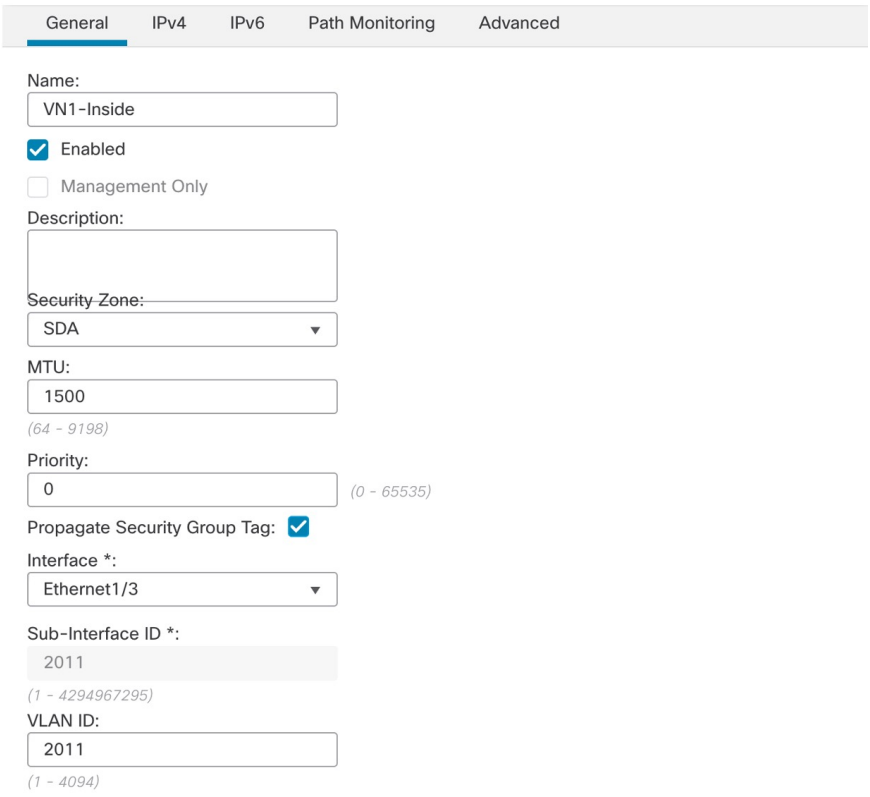
VLAN の範囲は 2000 です。この範囲は、範囲が 3000 の Cisco DNA Center 自動レイヤ 3 ハンドオフ VLAN とは異なります。

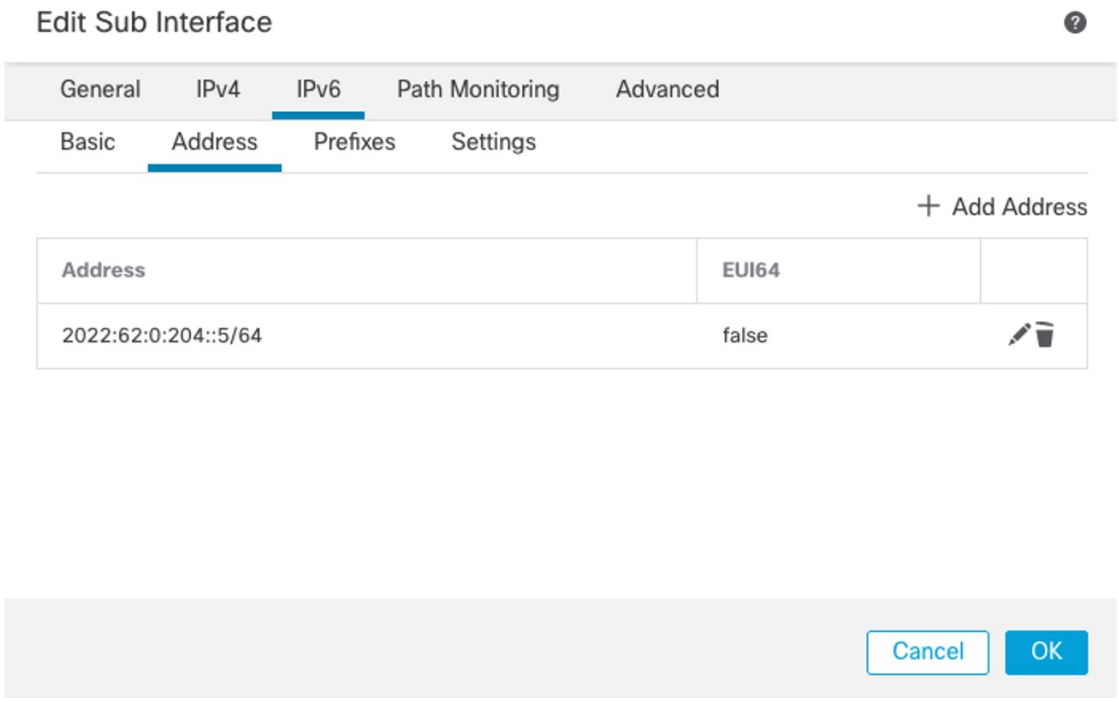
CLI または Cisco DNA Center テンプレートを使用して、この設定をファブリックボーダーに手動で適用できます。

Cisco SD-Access ファブリックボーダーの設定

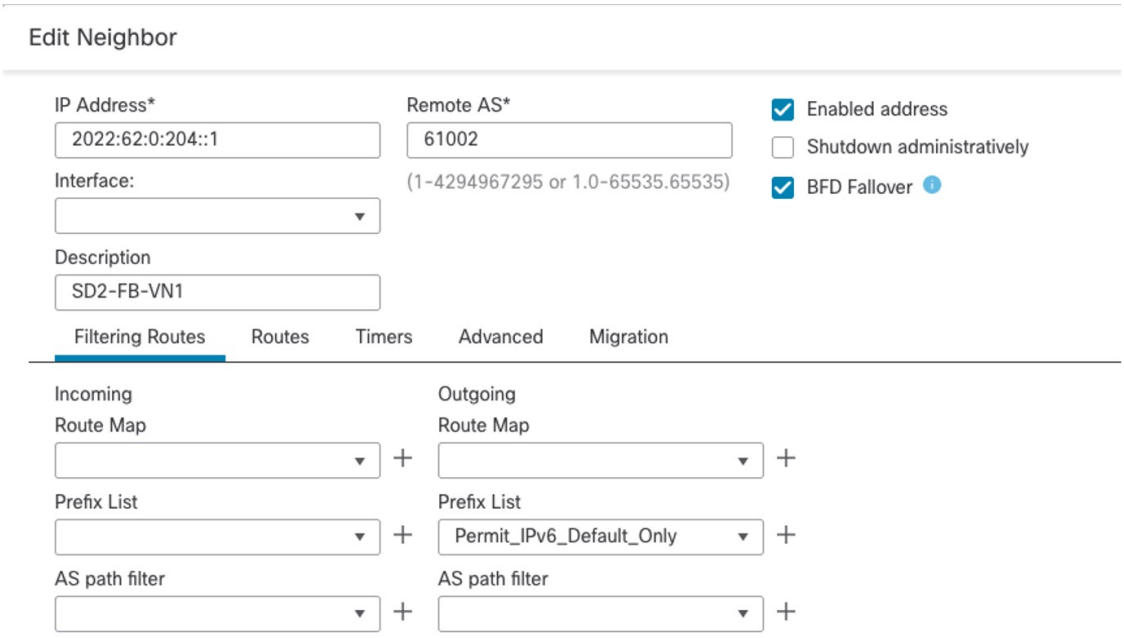
```
interface Vlan2011
 vrf forwarding VN1
 ip address 62.0.204.1 255.255.255.0
 ipv6 address 2022:62:0:204::1/64
 ipv6 enable
 bfd interval 300 min_rx 300 multiplier 3

router bgp 61002
  address-family ipv6 vrf VN1
  neighbor 2022:62:0:204::5 remote-as 61020
  neighbor 2022:62:0:204::5 update-source Vlan2011
  neighbor 2022:62:0:204::5 fall-over bfd
  neighbor 2022:62:0:204::5 activate
```

ステップ 2 Cisco SD-Access ファブリックボーダー VN に対してファイアウォール サブインターフェイスを設定します。





ステップ 3 ファイアウォールで、Cisco SD-Access ファブリックボーダー VN ネイバーの BGPv6 を設定します。



ブランチサイトのデフォルトルートフィルタ

Cisco SD-Access ファブリックボーダー VN は、インターネットファイアウォールからデフォルトルートを受信します。ブランチサイトがリモートサイトからのインターネットトラフィックのトランジットネットワークにならないようにするには、それらのデフォルトルートをフィルタリングして、Cisco SD WAN エッジデバイスにアドバタイズされないようにします。

次の例では、ファブリックボーダーは、Cisco SD WAN エッジデバイスの BGP ネイバーに向かう他のプレフィックスをすべて許可しながら、IPv6 デフォルトルートを拒否するフィルタを適用します。

Cisco SD-Access ファブリックボーダーの設定

```
ipv6 prefix-list no-ipv6-default-route seq 5 deny ::/0
ipv6 prefix-list no-ipv6-default-route seq 10 permit ::/0 le 128

router bgp 61002
 address-family ipv6 vrf VN1
  neighbor 2022:62:0:201::12 remote-as 61021
  neighbor 2022:62:0:201::12 update-source Vlan3002
  neighbor 2022:62:0:201::12 fall-over bfd
  neighbor 2022:62:0:201::12 activate
  neighbor 2022:62:0:201::12 weight 65535
  neighbor 2022:62:0:201::12 prefix-list no-ipv6-default-route out
```

MTU の一致

Cisco SD-Access スイッチの導入では、通常、VXLAN カプセル化に対応するために、システムの最大伝送ユニット（MTU）を 9,100 バイトに設定するため、レイヤ 3 インターフェイスでは、IPv4 および IPv6 MTU は 9,100 バイトになります。

接続された 2 つのデバイス間でレイヤ 3 の MTU を一致させると、Path Maximum Transmission Unit Discovery（PMTUD）が容易になり、受信デバイスが処理できるサイズを超えるパケットが一方のデバイスから送信されるのを防げます。このソリューションテストでは、ファイアウォールと Cisco SD WAN エッジデバイスに接続する SVI のファブリックボーダーレイヤ 3 IPv4 および IPv6 MTU を 1,500 バイトに調整します。

Cisco SD-Access ファブリックボーダーの設定

```
interface Vlan3001
 description vrf interface to External router
 vrf forwarding VN1
 ip address 61.0.201.129 255.255.255.252
 no ip redirects
 ip mtu 1500
 ip pim sparse-mode
 ip route-cache same-interface
 ipv6 address 2022:61:0:201::1/126
 ipv6 enable
 ipv6 mtu 1500
 ipv6 mld explicit-tracking
 bfd interval 300 min_rx 300 multiplier 3
```

Cisco Firepower アプライアンスでは、インターフェイス MTU はデフォルトで 1,500 バイトに設定されています。Cisco SD WAN エッジデバイスでは、`ip mtu` はデフォルトで 1,500 バイトに設定されますが、`ipv6 mtu` は物理インターフェイスの MTU のデフォルト値である 1,508 バイトから MTU 値が導出されます。IPv6 MTU は、デバイス CLI、または [Cli Add-On Template] を使用した Cisco SD WAN GUI を介して設定されます。

Cisco SD WAN エッジデバイスの設定

```
interface GigabitEthernet0/0/0.3001
 encapsulation dot1Q 3001
 vrf forwarding 1
 ip address 62.0.201.142 255.255.255.252
 no ip redirects
 ip mtu 1500
 ipv6 address 2022:62:0:201::E/126
 ipv6 mtu 1500
 no ipv6 redirects
 cts manual
  policy static sgt 2 trusted
 bfd template t1
 arp timeout 1200
```

IPv6 マルチキャスト

Cisco SD-Access の IPv6 マルチキャストは、ヘッドエンド レプリケーション モードの内部ランデブーポイント（RP）および外部 RP の Any Source Multicast（ASM）を使用して検証されます。次に、このソリューションにおける IPv6 マルチキャストの制限事項を示します。

- 現在、Cisco SD WAN は IPv6 マルチキャストをサポートしていません。
- IPv6 マルチキャストは、ECMP ゾーンに属するファイアウォール インターフェイスではサポートされません。
- IPv6 マルチキャストの内部 RP として設定できるファブリックボーダーは 1 つだけです。
- 現在、IPv6 のネイティブマルチキャストは Cisco SD-Access アンダーレイではサポートされていません。

参照

- *Cisco SD-Access Solution Design Guide (Cisco Validated Design)*
- *Cisco SD-Access SD-WAN* 独立ドメインのペアワイズ統合

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

この資料の記載内容は2008年10月現在のものです。
この資料に記載された仕様は予告なく変更する場合があります。

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255（フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。