



仮想ルータ

この章では、仮想ルータおよびSecure Firewall Threat Defense 内での仮想ルーティングの仕組みに関する基本概念について説明します。

- [仮想ルータと Virtual Routing and Forwarding \(VRF\) について \(1 ページ\)](#)
- [デバイスモデルごとの仮想ルータの最大数 \(9 ページ\)](#)
- [仮想ルータの要件と前提条件 \(11 ページ\)](#)
- [仮想ルータに関する注意事項と制限事項 \(11 ページ\)](#)
- [Management Center Web インターフェイスの変更: \[ルーティング \(Routing\)\] ページ \(14 ページ\)](#)
- [仮想ルータの管理 \(14 ページ\)](#)
- [仮想ルータの作成 \(15 ページ\)](#)
- [仮想ルータのモニタリング \(19 ページ\)](#)
- [仮想ルータの設定例 \(19 ページ\)](#)
- [仮想ルータの履歴 \(65 ページ\)](#)

仮想ルータと Virtual Routing and Forwarding (VRF) について

複数の仮想ルータを作成して、インターフェイスグループの個別のルーティングテーブルを管理できます。各仮想ルータには独自のルーティングテーブルがあるため、デバイスを流れるトラフィックを明確に分離できます。

これにより、共通のネットワーク機器のセットを使用して、2 件以上のお客様にサポートを提供できます。また、仮想ルータを使用して、独自のネットワーク要素をより明確に分離することもできます。たとえば、開発ネットワークを汎用企業ネットワークから分離することができます。

仮想ルータは、Virtual Routing and Forwarding の「Light」バージョンである VRF-Lite を実装しますが、この VRF-Lite は Multiprotocol Extensions for BGP (MBGP) をサポートしていません。

仮想ルータを作成するときに、インターフェイスをルータに割り当てます。特定のインターフェイスを1つのみの仮想ルータに割り当てることができます。次に、スタティックルートを

定義し、各仮想ルータに OSPF や BGP などのルーティングプロトコルを設定します。また、ネットワーク全体で個別のルーティングプロセスを設定し、すべての参加デバイス上のルーティングテーブルが、仮想ルータごとの同じルーティングプロセスとテーブルを使用するようにします。仮想ルータを使用して、同じ物理ネットワーク上に論理的に分離されたネットワークを作成し、各仮想ルータを通過するトラフィックのプライバシーを確保します。

ルーティングテーブルは個別にあるため、仮想ルータ全体で同じ、または重複するアドレス空間を使用できます。たとえば、2つの別個の物理インターフェイスでサポートされている2つの別個の仮想ルータ用に、192.168.1.0/24 アドレス空間を使用できます。

仮想ルータごとに個別の管理およびデータのルーティングテーブルがあることに注意してください。たとえば、管理専用インターフェイスを仮想ルータに割り当てると、そのインターフェイスのルーティングテーブルは、仮想ルータに割り当てられたデータインターフェイスとは別なものになります。

仮想ルータとダイナミック VTI について

仮想ルータとダイナミック VTI

仮想ルータを作成し、作成した仮想ルータにダイナミック VTI を関連付けて、ネットワーク内のダイナミック VTI の機能を拡張できます。ダイナミック VTI は、グローバルまたはユーザー定義の仮想ルータに関連付けることができます。ダイナミック VTI は、1つの仮想ルータにのみ割り当てることができます。

以下と関連付けられた仮想ルータ：

- ダイナミック VTI は、屋内 VRF (IVRF) と呼ばれます。
- トンネル送信元インターフェイスは、Front Door VRF (FVRF) と呼ばれます。

ダイナミック VTI および対応する保護されたネットワーク インターフェイスは、同じ仮想ルータの一部である必要があり、借用 IP インターフェイスとダイナミック VTI を同じ仮想ルータにマッピングする必要があります。トンネル送信元インターフェイスは、複数の仮想ルータの一部にできます。

ルートベースのサイト間 VPN にダイナミック VTI を使用して仮想ルータを構成する場合は、[ダイナミック VTI を使用した仮想ルータの設定方法 \(2 ページ\)](#) を参照してください。

構成例の詳細については、[ダイナミック VTI を使用したサイト間 VPN における複数の仮想ルータのネットワークからのトラフィックを保護する方法 \(40 ページ\)](#) を参照してください。

ダイナミック VTI を使用した仮想ルータの設定方法

管理センターのルートベースのサイト間 VPN にダイナミック VTI を使用して仮想ルータを設定するには、次の手順を実行します。

手順	操作手順	詳細情報
1	ハブのダイナミック VTI インターフェイスとスポークのダイナミック VTI を使用する、ルートベースのサイト間 VPN を作成します。	ルートベースのサイト間 VPN の作成
2	仮想ルータを作成します。	仮想ルータの作成 (15 ページ)
3	インターフェイスを仮想ルータに割り当てます。	仮想ルータの設定 (15 ページ)
4	ハブとスポークのルーティングポリシーを設定します。	ハブアンドスポークトポロジのエンドポイントの設定
5	ハブとスポークのアクセス コントロール ポリシーを設定します。	ハブアンドスポークトポロジのエンドポイントの設定

仮想ルータの適用

仮想ルータにより、共有リソース上のネットワークを分離したり、共通セキュリティポリシーを使用してネットワークを分離したりすることができます。そのため、仮想ルータは、次のことを実現するために役立ちます。

- 顧客または部門ごとの専用ルーティングテーブルによって顧客のトラフィックを分離する。
- 異なる部門またはネットワークで共通セキュリティポリシーを管理する。
- 異なる部門またはネットワークでインターネットアクセスを共有する。

グローバルおよびユーザー定義の仮想ルータ

グローバル仮想ルータ

仮想ルーティング機能を備えたデバイスの場合、デフォルトでグローバル仮想ルータが作成され、ネットワーク内のすべてのインターフェイスがグローバル仮想ルータに割り当てられます。ルーテッドインターフェイスは、ユーザー定義の仮想ルータまたはグローバル仮想ルータのいずれかに属することができます。仮想ルータ機能を備えたバージョンに Threat Defense をアップグレードすると、既存のすべてのルーティング構成がグローバル仮想ルータの一部になります。

ユーザー定義の仮想ルータ

ユーザー定義の仮想ルータは、ユーザーが定義するルータです。1つのデバイス上に複数の仮想ルータを作成できます。ただし、1つのインターフェイスは常に1つのユーザー定義の仮想ルータにのみ割り当てることができます。一部のデバイス機能はユーザー定義の仮想ルータで

サポートされていますが、一部の機能はグローバル仮想ルータでのみサポートされています。ユーザー定義の仮想ルータは、ルートベースのサイト間VPN（スタティック VTI）（スタティックおよびダイナミック VTI）をサポートしています。

サポートされている機能とモニタリングポリシー

次の機能は、グローバル仮想ルータでのみ設定できます。

- OSPFv3
- RIP
- EIGRP
- IS-IS
- マルチキャストルーティング
- Policy Based Routing（PBR）

ISIS、および PBR は、Management Center の FlexConfig を介してサポートされます（[定義済みの FlexConfig オブジェクト](#)を参照）。これらの機能に対しては、グローバル仮想ルータのインターフェイスのみを設定します。

DHCP サーバーの自動設定では、インターフェイスから学習した WINS/DNS サーバーが使用されます。このインターフェイスに指定できるのは、グローバル仮想ルータインターフェイスだけです。

次の機能は、ユーザー定義の仮想ルータごとに個別に設定できます。

- スタティックルートとルートの SLA モニター
- OSPFv2
- BGPv4/v6
- Integrated Routing and Bridging（IRB）
- SNMP

次の機能は、リモートシステムに対してクエリまたは通信を行うときにシステムによって使用されます（ボックス内のトラフィック）。これらの機能は、グローバル仮想ルータのインターフェイスのみを使用します。つまり、この機能のインターフェイスを設定する場合、そのインターフェイスはグローバル仮想ルータに属する必要があります。一般的なルールとして、管理目的で外部サーバーに到達するためにルートを検索する必要があるシステムでは、グローバル仮想ルータでルートルックアップが実行されます。

- アクセス制御ルールで使用される完全修飾名を解決する場合、または ping コマンドの名前解決に使用される DNS サーバー。DNS サーバーのインターフェイスとして **any** を指定すると、グローバル仮想ルータのインターフェイスのみ考慮されます。
- AAA サーバーまたはアイデンティティレルム（VPN で使用する場合）。VPN は、グローバル仮想ルータのインターフェイスでのみ設定できるため、VPN に使用される外部 AAA

サーバー（Active Directory など）は、グローバル仮想ルータのインターフェイスを介して到達可能である必要があります。

ポリシーを仮想ルータ対応にするための設定

仮想ルータを作成する場合、その仮想ルータのルーティングテーブルは、グローバル仮想ルータまたは他の仮想ルータから自動的に分離されます。ただし、セキュリティポリシーは自動的に仮想ルータ対応にはなりません。

たとえば、「任意の」送信元または宛先のセキュリティゾーンに適用されるアクセス制御ルールを作成する場合、ルールはすべての仮想ルータのすべてのインターフェイスに適用されません。実はこれがまさに必要な機能かもしれません。たとえば、すべてのお客様が、同じリストの好ましくない URL カテゴリへのアクセスをブロックしたい場合があります。

ただし、いずれかの仮想ルータにのみポリシーを適用する必要がある場合は、その1つの仮想ルータからのインターフェイスのみを含むセキュリティゾーンを作成する必要があります。その後、セキュリティポリシーの送信元と宛先の条件に、仮想ルータが制約されたセキュリティゾーンを使用します。

メンバーシップが1つの仮想ルータに割り当てられたインターフェイスに制限されたセキュリティゾーンを使用することにより、次のポリシーで仮想ルータ対応ルールを作成できます。

- アクセス コントロール ポリシー
- 侵入およびファイルポリシー。
- SSL 復号ポリシー。
- アイデンティティポリシーと、ユーザーから IP アドレスへのマッピング。仮想ルータで重複するアドレス空間を使用する場合は、仮想ルータごとに個別のレームを作成し、アイデンティティ ポリシー ルールでそれらを正しく適用してください。

仮想ルータで重複するアドレス空間を使用する場合は、適切なポリシーが適用されるようにセキュリティゾーンを使用する必要があります。たとえば、2つの個別の仮想ルータで 192.168.1.0/24 アドレス空間を使用する場合、192.168.1.0/24 ネットワークを指定するだけのアクセスコントロールルールは、両方の仮想ルータのトラフィックに適用されます。これが求める結果ではない場合は、1つの仮想ルータのみに対して送信元/宛先セキュリティゾーンも指定することで、ルールの適用を制限できます。

仮想ルータの相互接続

スタティックおよびダイナミックルートリーク

仮想ルータ間でトラフィックをルーティングするようにデバイスを設定できます。このルートリークのプロセスは、スタティックルートを設定して手動で実行することも、BGP の設定を介して動的に実行することもできます。

スタティックルートリーク

仮想ルータ間でトラフィックをルーティングするようにスタティックルートを設定できます。

たとえば、グローバル仮想ルータに外部インターフェイスがある場合、外部インターフェイスにトラフィックを送信するために、他の各仮想ルータでスタティック デフォルト ルートを設定できます。その後、特定の仮想ルータ内でルーティングできないトラフィックは、その後のルーティングのためにグローバルルータに送信されます。

仮想ルータ間のスタティックルートは、別の仮想ルータにトラフィックをリークしているため、ルートリークと呼ばれます。ルートをリークしている場合（VR2 への VR1 ルートなど）、VR2 から VR1 のみへの接続を開始できます。トラフィックが VR1 から VR2 に流れるようにするには、逆ルートを設定する必要があります。別の仮想ルータのインターフェイスへのスタティックルートを作成する場合は、ゲートウェイアドレスを指定する必要はありません。単純に宛先インターフェイスを選択します。

仮想ルータ間ルートの場合、システムは送信元の仮想ルータ内で宛先インターフェイスルックアップを行います。次に、宛先の仮想ルータでネクストホップの MAC アドレスを検索します。したがって、宛先の仮想ルータには、宛先アドレスに対して選択されたインターフェイスのダイナミック（学習済み）ルートまたはスタティックルートのいずれかが設定されている必要があります。

異なる仮想ルータで送信元インターフェイスと宛先インターフェイスを使用する NAT ルールを設定すると、仮想ルータ間でトラフィックをルーティングすることもできます。ルートルックアップを実行するために NAT のオプションを選択しない場合、宛先の変換が発生するたびに、NAT 変換アドレスを使用して宛先インターフェイスからトラフィックが送信されます。ただし、宛先の仮想ルータには、ネクストホップルックアップが成功するように、変換後の宛先 IP アドレスのルートが設定されている必要があります。

NAT ルールは、ある仮想ルータから別の仮想ルータへのトラフィックをリークしますが、正しいルーティングを確保するため、変換されたトラフィック用に仮想ルータ間のスタティックルートリークを設定することを推奨します。ルートリークがないと、ルールが適合すると予想されるトラフィックにルールが適合しないことがあり、変換が適用されないおそれがあります。

仮想ルーティングは、ルートリークのカスケードリングまたはチェーンをサポートしません。たとえば、Threat Defense に VR1、VR2、および VR3 仮想ルータがあるとします。VR3 は、ネットワーク 10.1.1.0/24 に直接接続されています。ここで、VR2 のインターフェイス経由でネットワーク 10.1.1.0/24 の VR1 におけるルートリークを設定し、VR3 経由で 10.1.1.0/24 の VR2 におけるルートリークを定義するとします。このルートリークのチェーンは、VR1 から VR2 へのトラフィックのホップを許可せず、VR3 を終了します。ルートリークの場合、ルートルックアップでは、まず入力側の仮想ルータのルーティングテーブルで出力インターフェイスが決定され、仮想ルータのルーティングテーブルの出力でネクストホップルックアップが確認されます。両方のルックアップで、出力インターフェイスが一致している必要があります。この例では、出力インターフェイスが同じものにならないため、トラフィックは通過しません。

宛先ネットワークがアップストリーム（発信）VR の直接接続されたサブネットワークでない場合は、静的な VRF 間ルートを注意して使用してください。たとえば、VR1 と VR2 の 2 つの VR があるとします。VR1 は、BGP または任意の動的ルーティングプロトコルを介して外部のピアか

らデフォルトルートを取得する発信トラフィックを処理し、VR2は、VR1をネクストホップとして使用する静的なVRF間のデフォルトルートで構成された着信トラフィックを処理します。VR1がピアからのデフォルトルートを失ってもVR2はそのアップストリーム（発信）VRがデフォルトルートを失ったことを検出できず、トラフィックは引き続きVR1に送信され、最終的に通知なしでドロップされます。このシナリオでは、BGPを介した動的なルートリークを使用してVR2を構成することをお勧めします。

BGPを使用したダイナミックルートリーク

ルートターゲット拡張コミュニティを使用して送信元仮想ルータ（VR1など）から送信元BGPテーブルにルートをエクスポートし、同じルートターゲット拡張コミュニティを送信元BGPテーブルから宛先BGPテーブルにインポートすることで、仮想ルータ間ルートリークを実装できます。これは、その後、宛先仮想ルータ（VR2など）によって使用されます。ルートのフィルタリングにルートマップを使用できます。グローバル仮想ルータのルートは、ユーザ定義の仮想ルータにリークすることも、その逆も可能です。BGP仮想ルータ間ルートリークは、IPv4とIPv6の両方のプレフィックスをサポートします。

BGPルートリークの設定の詳細については、[BGPルートのインポート/エクスポート設定の設定](#)を参照してください。

BGPルートリークのガイドライン

- 再帰に必要なすべてのルートがインポートされ、入力仮想ルータのルーティングテーブルに存在することを確認します。
- ECMPは仮想ルータごとにサポートされます。したがって、異なる仮想ルータ間でECMPを設定しないでください。異なる仮想ルータからインポートされた重複するプレフィックスは、ECMPを形成できません。つまり、2つの異なる仮想ルータから他の仮想ルータ（グローバル仮想ルータまたはユーザ定義の仮想ルータ）に重複するアドレスを持つルートをインポートしようとする、1つのルート（BGPベストパスアルゴリズムに従って、アドバタイズされた最初のルート）がそれぞれの仮想ルーティングテーブルにインポートされます。たとえば、VR1に接続されたネットワーク10.10.0.0/24がBGPを介して最初にグローバル仮想ルータにアドバタイズされ、その後、VR2に接続された同じアドレス10.10.0.0/24を持つ別のネットワークもBGPを介してグローバル仮想ルータにアドバタイズされた場合、VR1ネットワークルートのみがグローバル仮想ルーティングテーブルにインポートされます。
- ユーザ定義の仮想ルータではOSPFv3はサポートされません。したがって、OSPFv3ユーザ定義の仮想ルータをグローバル仮想ルータにリークするようにBGPv6を設定しないでください。ただし、再配布によってOSPFv3グローバル仮想ルータのルートをユーザ定義の仮想ルータにリークするようにBGPv6を設定できます。
- ルートをリークしなくて済むように、VTIインターフェイスと保護されている内部インターフェイス（VTIでサポートされている場合はループバックインターフェイス）を同じ仮想ルータの一部にしておくことをお勧めします。

IP アドレスのオーバーラップ

仮想ルータは、独立したルーティングテーブルの複数のインスタンスを作成するため、同じ（重複する）IP アドレスを競合することなく使用できます。Threat Defense により、同じネットワークを2つ以上の仮想ルータの一部にすることができます。これには、インターフェイスまたは仮想ルータレベルで適用される複数のポリシーが含まれます。

いくつかの例外を除いて、ルーティング機能とほとんどの NGFW および IPS 機能は、重複する IP アドレスの影響を受けません。以下では、重複する IP アドレスによる制限がある機能と、それらに対処するための提案または推奨事項について説明します。

重複する IP アドレスによる制限

複数の仮想ルータで重複する IP アドレスを使用する場合、ポリシーを適切に適用するには、一部の機能のポリシーまたはルールを変更する必要があります。そのような機能では、既存のセキュリティゾーンを分割するか、必要に応じて新しいインターフェイスグループを使用して、より限定されたインターフェイスを使用する必要があります。

次の機能は、重複する IP アドレスで適切に動作させるために変更を加えてください。

- ネットワークマップ：ネットワーク検出ポリシーを変更して、一部の重複する IP セグメントを除外し、マッピングされる IP アドレスが重複しないようにします。
- アイデンティティポリシー：アイデンティティ フィールド ソースは仮想ルータ間で区別できません。この制限に対処するには、重複するアドレス空間または仮想ルータを異なるルームにマッピングします。

次の機能については、特定のインターフェイスにルールを適用して、重複する IP セグメントに異なるポリシーが適用されるようにする必要があります。

- アクセス ポリシー
- プレフィルタポリシー (Prefilter Policy)
- QoS/レート制限
- SSL ポリシー

重複した IP アドレスがあるとサポートされない機能

- AC ポリシーの ISE SGT ベースのルール：Cisco Identity Services Engine (ISE) からダウンロードした IP アドレスマッピングへのスタティック セキュリティ グループ タグ (SGT) は仮想ルータに対応していません。仮想ルータごとに異なる SGT マッピングを作成する必要がある場合は、仮想ルータごとに個別の ISE システムをセットアップします。これは、各仮想ルータで同じ IP アドレスを同じ SGT 番号にマッピングする場合には必要ありません。
- 仮想ルータ間での重複する DHCP サーバープールはサポートされていません。
- イベントと分析：Management Center 分析の多くは、同じ IP アドレスが2つの異なるエンドホストに属している場合に区別できないネットワークマップおよび ID マッピングに依

存しています。そのため、それらの分析は、同じデバイスであっても異なる仮想ルータに重複する IP セグメントが存在する場合、正確なものになりません。

ユーザー定義の仮想ルータでの SNMP の設定

管理インターフェイスおよびグローバル仮想ルータのデータインターフェイスでの SNMP のサポートに加えて、Secure Firewall Threat Defense ではユーザー定義の仮想ルータで SNMP ホストを設定できるようになりました。

ユーザー定義の仮想ルータでの SNMP ホストの設定には、次のプロセスが含まれます。

1. デバイスインターフェイスを設定します。
2. 仮想ルータの作成
3. 仮想ルータインターフェイスで SNMP ホストを設定します。



(注) SNMP は仮想ルータに対応していません。したがって、ユーザー定義の仮想ルータで SNMP サーバーを設定するときは、ネットワークアドレスが IP アドレスのオーバーラップでないことを確認してください。

4. 設定を Secure Firewall Threat Defense に展開します。展開が成功すると、SNMP ポーリングとトラップが仮想ルータインターフェイスを介してネットワーク管理ステーションに送信されます。

デバイスモデルごとの仮想ルータの最大数

作成できる仮想ルータの最大数は、デバイスモデルによって異なります。次の表に、上限を示します。show vrf counters コマンドを入力して、システムでダブルチェックできます。これにより、グローバル仮想ルータを含まない、そのプラットフォームのユーザー定義仮想ルータの最大数が表示されます。次の表の数字には、ユーザールータとグローバルルータが含まれています。Firepower 4100/9300 の場合、これらの数字はネイティブモードに適用されます。

Firepower 4100/9300 などのマルチインスタンス機能をサポートするプラットフォームでは、仮想ルータの最大数をデバイス上のコア数で割ってから、インスタンスに割り当てられたコア数を乗じて最も近い整数に丸めることにより、コンテナインスタンスごとの仮想ルータの最大数を決定します。たとえば、プラットフォームが最大 100 の仮想ルータをサポートする環境で、70 のコアが存在する場合、各コアは最大 1.43 (切り上げた数) の仮想ルータをサポートします。したがって、6 つのコアが割り当てられたインスタンスは、8.58 の仮想ルータをサポートします (この数は 8 に切り下げる)。10 のコアが割り当てられたインスタンスは、14.3 の仮想ルータをサポートします (この数は 14 に切り下げる)。

デバイス モデル	最大仮想ルータ数
Firepower 1010	5
Firepower 1120	5
Firepower 1140	10
Firepower 1150	10
Firepower 2110	10
Firepower 2120	20
Firepower 2130	30
Firepower 2140	40
Cisco Secure Firewall 3105	10
Secure Firewall 3110	15
Secure Firewall 3120	25
Secure Firewall 3130	50
Secure Firewall 3140	100
Firepower 4112	60
Firepower 4115	80
Firepower 4125	100
Firepower 4145	100
Cisco Secure Firewall 4215	100
Cisco Secure Firewall 4225	100
Cisco Secure Firewall 4245	100
Firepower 9300 appliance、すべてのモデル	100
Threat Defense Virtual、すべてのプラットフォーム	30
ISA 3000	10

関連トピック

[コンテナインスタンスの要件と前提条件](#)

仮想ルータの要件と前提条件

モデルのサポート

Threat Defense

サポートされるドメイン

任意

ユーザの役割

管理者

ネットワーク管理者

セキュリティ承認者

仮想ルータに関する注意事項と制限事項

ファイアウォールモードのガイドライン

仮想ルータは、ルーテッドファイアウォールモードでのみサポートされます。

インターフェイスのガイドライン

- インターフェイスは1つの仮想ルータにのみ割り当てることができます。
- 仮想ルータには、任意の数のインターフェイスを割り当てることができます。
- ユーザー定義の仮想ルータには、論理名とVTIを持つルーテッドインターフェイスのみを割り当てることができます。
- 仮想ルータインターフェイスを非ルーテッドモードに変更する場合は、仮想ルータからインターフェイスを削除してから、そのモードを変更します。
- グローバル仮想ルータまたは別のユーザー定義の仮想ルータから、インターフェイスを仮想ルータに割り当てることができます。
- 次のインターフェイスは、ユーザー定義の仮想ルータに割り当てることができません。
 - EtherChannel のメンバー。
 - 冗長インターフェイスのメンバー。
 - BVI のメンバー。
- VTI はルートベースのVPNです。したがって、トンネルが確立されたら、暗号化にVTIを使用するトラフィックはルーティングを通して制御される必要があります。スタティック

ルーティング、および BGP、OSPFv2/v3、または EIGRP を使用したダイナミックルーティングがサポートされています。

- ポリシーベースのサイト間 VPN またはリモートアクセス VPN では、ユーザー定義の仮想ルータに属するインターフェイスを使用できません。
- ダイナミック VTI および対応する保護されたネットワーク インターフェイスは、同じ仮想ルータの一部である必要があります。
- 借用 IP インターフェイスとダイナミック VTI を同じ仮想ルータにマッピングする必要があります。
- ユーザー定義の仮想ルータは、BGPv4/v6 および OSPFv2 ルーティングプロトコルのみをサポートします。
- トンネル送信元インターフェイスは、ダイナミック VTI に関連付けられているものとは異なるユーザー定義の仮想ルータにある可能性があります。
- 移行中のインターフェイスを使用している、またはその仮想ルータが削除されたルートが送信元または宛先の仮想ルータテーブルに存在する場合は、インターフェイスを移行または仮想ルータを削除する前に、そのルートを削除してください。
- 仮想ルータごとに個別のルーティングテーブルが維持されるため、インターフェイスが 1 つの仮想ルータから別の仮想ルータ（グローバルかユーザー定義かを問わず）に移行されると、インターフェイスで設定された IP アドレスは一時的に削除されます。インターフェイス上の既存の接続はすべて終了します。このように、仮想ルータ間でインターフェイスを移行すると、ネットワークトラフィックに大きな影響を与えます。インターフェイスを移行する前に予防措置を講じてください。

グローバル仮想ルータのガイドライン

- 名前が付けられていて、他の仮想ルータの一部ではないインターフェイスは、グローバル仮想ルータの一部です。
- グローバル仮想ルータからルーテッドインターフェイスを削除することはできません。
- グローバル仮想ルータを変更することはできません。
- 一般に、インターフェイスを設定した後、登録を解除して同じまたは別の Management Center に登録し直すと、インターフェイス設定がデバイスからインポートされます。仮想ルータのサポートには制限があります。つまり、グローバル仮想ルータインターフェイスの IP アドレスのみが保持されます。

クラスタリングのガイドライン

- コントロールユニットのリンクがそのインターフェイスの障害のために失敗すると、ユニットはそのインターフェイスのリークされたすべてのルートをグローバルルーティングテーブルから削除し、非アクティブな接続ルートとスタティックルートをクラスタの他のユニットに伝搬します。これにより、リークされたルートが他のユニットのルーティング

テーブルから削除されます。これらの削除は、別のユニットが新しいコントロールユニットになる前に実行され、約 500 ms かかります。別のユニットが新しいコントロールユニットになると、これらのルートが学習され、BGP コンバージェンスを介してルーティングテーブルに追加されます。したがって、コンバージェンスの時間になるまで（約 1 分間）、リークされたルートはルーティングイベントの発生のために利用できません。

- クラスタでコントロールロールの変更が発生すると、BGP を介して学習されたリークされたルートが最適な ECMP パスで更新されます。ただし、最適でない ECMP パスは、BGP 再コンバージェンスタイマー（210 秒）が経過しないと、クラスタのルーティングテーブルから削除されません。したがって、BGP 再コンバージェンスタイマーの期限切れるまで、古い最適ではない ECMP パスがルーティングイベントの優先ルートとして存続します。

その他のガイドライン

- 仮想ルータの BGP を設定するときに、同じ仮想ルータ内の異なるプロトコルに属するルートを再配布できます。たとえば、OSPF VR2 ルートは BGP VR1 にインポートできません。OSPF VR2 を BGP VR2 に再配布し、その後 BGP VR2 と BGP VR1 の間でルートリークを設定するのみ可能です。
- ルートマップ内のルートをフィルタリングするために IPv6 ACL を使用することはできません。プレフィックスリストのみがサポートされています。
- セキュリティインテリジェンスポリシー：セキュリティインテリジェンスポリシーは、仮想ルータに対応していません。IP アドレス、URL、または DNS 名をブロックリストに追加すると、すべての仮想ルータに対してブロックされます。この制限は、セキュリティゾーンを持つインターフェイスに適用されます。
- NAT ルール：NAT ルールにインターフェイスを混在させないでください。仮想ルーティングでは、指定された送信元インターフェイスと宛先インターフェイスオブジェクト（インターフェイスグループまたはセキュリティゾーン）に異なる仮想ルータに属するインターフェイスがある場合、NAT ルールにより、ある仮想ルータから別の仮想ルータにトラフィックが転送されます。NAT は、着信インターフェイスのみに対して仮想ルータテーブルでルートルックアップを行います。必要に応じて、宛先インターフェイスに対して送信元仮想ルータでスタティックルートを定義します。インターフェイスを [任意 (any)] のままにした場合は、仮想ルータのメンバーシップに関係なく、すべてのインターフェイスにルールが適用されます。
- DHCP リレー：DHCP リレーでは仮想ルータの相互接続はサポートされていません。たとえば、VR1 インターフェイスで DHCP リレークライアントが有効になっていて、VR2 インターフェイスで DHCP リレーサーバーが有効になっている場合、DHCP 要求は VR2 インターフェイスの外部に転送されません。
- 削除された仮想ルータの再作成：10 秒以内に削除された仮想ルータを再作成すると、仮想ルータの削除が進行中であることを示すエラーメッセージが表示されます。削除された仮想ルータを引き続き再作成する場合は、新しい仮想ルータに別の名前を使用します。

Management Center Web インターフェイスの変更 : [ルーティング (Routing)] ページ

Threat Defense 6.6 より前のデバイスと一部のデバイスモデルは、仮想ルーティング機能でサポートされていません。Management Center Web インターフェイスには、サポート対象外デバイスなどの Management Center 6.5 以前のバージョンと同じ [ルーティング (Routing)] ページが表示されます。仮想ルーティングでサポートされているデバイスとプラットフォームについては、「[デバイスモデルごとの仮想ルータの最大数](#)」を参照してください。

サポートされているデバイスの [ルーティング (Routing)] ページで仮想ルータを設定できます。

1. [デバイス (Devices)] > [デバイス管理 (Device Management)] に移動し、仮想ルータ対応デバイスを編集します。
2. [ルーティング (Routing)] をクリックして、[仮想ルータ (Virtual Routers)] ページを開きます。

仮想ルーティングを使用しているデバイスの場合、[ルーティング (Routing)] ページの左側のペインに次の項目が表示されます。

- [仮想ルータの管理 (Manage Virtual Routers)] : 仮想ルータを作成および管理できます。
- 仮想ルーティングプロトコルのリスト : 仮想ルータに設定できるルーティングプロトコルがリストされます。
- [一般設定 (General Settings)] : すべての仮想ルータに適用できる BGP の一般設定を設定できます。他の BGP 設定を定義するには、[BGPの有効化 (Enable BGP)] チェックボックスをオンにします。仮想ルータの他の BGP 設定を設定するには、仮想ルーティングプロトコルで [BGP] に移動します。

仮想ルータの管理

[仮想ルータ (Virtual Routers)] ペインで [仮想ルータの管理 (Manage Virtual Routers)] をクリックすると、[仮想ルータの管理 (Manage Virtual Routers)] ページが表示されます。このページには、デバイス上の既存の仮想ルータと関連するインターフェイスが表示されます。このページでは、デバイスに [仮想ルータの追加 (Add Virtual Router)] (+) できます。また、ユーザー定義の仮想ルータを [編集 (Edit)] (✎) または [削除 (Delete)] (🗑) できます。グローバル仮想ルータは編集も削除もできません。グローバル仮想ルータの詳細のみ [表示 (View)] (👁) できます。

仮想ルータの作成

手順

ステップ 1 [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択し、Threat Defense デバイスを編集します。

ステップ 2 [ルーティング (Routing)] をクリックします。

ステップ 3 [Manage Virtual Routers] をクリックします。

ステップ 4 [仮想ルータの追加 (Add Virtual Router)] (+) をクリックします。

ステップ 5 [Add Virtual Router] ボックスに、仮想ルータの名前と説明を入力します。

(注) 10秒以内に削除された仮想ルータを作成している場合は、仮想ルータの削除が進行中であることを示すエラーメッセージが表示されます。削除された仮想ルータを引き続き作成する場合は、新しい仮想ルータに別の名前を使用します。

ステップ 6 [OK] をクリックします。

[ルーティング (Routing)] ページが表示され、新しく作成された [仮想ルータ (Virtual Router)] ページが表示されます。

次のタスク

- [仮想ルータの設定](#)。

仮想ルータの設定

インターフェイスをユーザ定義の仮想ルータに割り当てて、デバイスのルーティングポリシーを設定できます。グローバル仮想ルータのインターフェイスは手動で追加または削除できませんが、デバイスインターフェイスのルーティングポリシーは設定できます。

始める前に

- ユーザ定義の仮想ルータのルーティングポリシーを設定するには、ルータを追加します。[仮想ルータの作成 \(15 ページ\)](#) を参照してください。
- 仮想ルーティング対応ではないデバイスのすべてのルーティング設定は、グローバル仮想ルータでも使用できます。設定の詳細については、「[Routing Settings](#)」を参照してください。
- ユーザ定義の仮想ルータでは、限定されたルーティングプロトコルのみがサポートされます。

手順

ステップ 1 [デバイス (Devices)] > [デバイス管理 (Device Management)] ページで、仮想ルータでサポートされているデバイスを編集します。[ルーティング (Routing)] に移動します。[ルーティング (Routing)] ページの変更の詳細については、[Management Center Web インターフェイスの変更 : \[ルーティング \(Routing\)\] ページ \(14 ページ\)](#) を参照してください。

ステップ 2 ドロップダウンリストから、目的の仮想ルータを選択します。

ステップ 3 [仮想ルータのプロパティ (Virtual Router Properties)] ページで、説明を変更できます。

ステップ 4 インターフェイスを追加するには、[Available Interfaces] ボックスでインターフェイスを選択し、[Add] をクリックします。

次の点を忘れないでください。

- 論理名を持つインターフェイスのみが [Available Interfaces] ボックスの下にリストされます。インターフェイスを編集し、[インターフェイス (Interfaces)] で論理名を指定できます。設定を有効にするには、必ず変更を保存してください。
- グローバル仮想ルータのインターフェイスのみを割り当てに使用できます。[使用可能なインターフェイス (Available Interfaces)] ボックスには、他のユーザ定義仮想ルータに割り当てられていないインターフェイスのみが表示されます。仮想ルータには物理インターフェイス、サブインターフェイス、冗長インターフェイス、ブリッジグループ、VTI、および EtherChannel を割り当てられますが、それらのメンバーインターフェイスは割り当てられません。メンバーインターフェイスに名前を付けることはできないため、仮想ルーティングでは使用できません。

診断インターフェイスは、グローバル仮想ルータにのみ割り当てることができます。

ステップ 5 設定を保存するには、[Save] をクリックします。

ステップ 6 仮想ルータのルーティングポリシーを設定するには、それぞれの名前をクリックして、対応する設定ページを開きます。

- [OSPF] : ユーザ定義の仮想ルータでは OSPFv2 のみがサポートされます。仮想ルータ対応ではないインターフェイスに関しては、OSPFv2 のその他すべての設定を適用できます。ただし、[インターフェイス (Interface)] では、設定している仮想ルータのインターフェイスのみ選択できます。グローバル仮想ルータの OSPFv3 および OSPFv2 ルーティングポリシーを定義できます。OSPF 設定の詳細については、[OSPF](#) を参照してください。
- [RIP] : グローバル仮想ルータに対してのみ RIP ルーティングポリシーを設定できます。RIP 設定の詳細については、[RIP](#) を参照してください。
- [BGP] : このページには、[設定 (Settings)] で設定した BGP の一般設定が表示されます。
 - このページでは、ルータ ID の設定を除き、BGP の一般設定は変更できません。[設定 (Settings)] ページで定義されているルータ ID の設定は、このページで編集することによりオーバーライドできます。
 - その他の BGP IPv4 または IPv6 設定を設定するには、[BGP] ページの [一般設定 (General Settings)] で [BGP] オプションを有効にする必要があります。

- IPv4 と IPv6 の両方のアドレスファミリの BGP 設定は、グローバルルータとユーザー定義の仮想ルータでサポートされます。

BGP の設定の詳細については、[BGP](#)を参照してください。

- [スタティックルート (Static Route)]: この設定を使用して、特定の宛先ネットワークに関するトラフィックの送信先を定義します。この設定を使用して、仮想ルータ間のスタティックルートも作成できます。ユーザー定義またはグローバル仮想ルータのインターフェイスを使用して、接続されたルートまたはスタティックルートのリークを作成できません。FMC は、別の仮想ルータに属し、ルートリークに使用できることを示すためにインターフェイスにプレフィックスを付けます。ルートリークを成功させるには、ネクストホップゲートウェイを指定しないでください。

スタティックルートテーブルの [仮想ルータからのリーク (Leaked from Virtual Router)] 列に、インターフェイスがルートリークに使用される仮想ルータが表示されます。ルートリークではない場合、この列には「該当なし」と表示されます。

スタティックルートが属している仮想ルータに関係なく、スタティックルートが属する同じ仮想ルータのインターフェイスとともに、Null0 インターフェイスがリストされます。

スタティックルートの設定の詳細については、[スタティックルートとデフォルトルート](#)を参照してください。

- [マルチキャスト (Multicast)]: グローバル仮想ルータにのみマルチキャストルーティングポリシーを設定できます。マルチキャスト設定の詳細については、[マルチキャスト](#)を参照してください。

ステップ 7 設定を保存するには、[Save] をクリックします。

次のタスク

- [仮想ルータの変更](#)。
- [仮想ルータの削除](#)。

仮想ルータの変更

仮想ルータの説明やその他のルーティングポリシーを変更できます。

手順

-
- ステップ 1** [デバイス (Devices)]>[デバイス管理 (Device Management)]を選択し、Threat Defense デバイスを編集します。
 - ステップ 2** [ルーティング (Routing)] をクリックします。
 - ステップ 3** [Manage Virtual Routers] をクリックします。

すべての仮想ルータと、割り当てられたインターフェイスが [Virtual Routers] ページに表示されます。

ステップ 4 仮想ルータを変更するには、目的の仮想ルータに対して **[編集 (Edit)]** (✎) をクリックします。

(注) グローバル仮想ルータの一般設定は変更できません。したがって、グローバルルータの編集はできません。代わりに、設定を表示する **[表示 (View)]** (👁) が用意されています。

ステップ 5 変更を保存するには、**[Save]** をクリックします。

次のタスク

- [仮想ルータの削除](#)。

仮想ルータの削除

始める前に

- グローバル仮想ルータを削除することはできません。したがって、グローバル仮想ルータには削除オプションは使用できません。
- 一度に複数の仮想ルータを削除できます。
- 削除された仮想ルータのすべてのルーティングポリシーも削除されます。
- 削除された仮想ルータのすべてのインターフェイスは、グローバル仮想ルータに移動します。
- IP の重複、ルート競合など、インターフェイスの移動に関する制限がある場合、競合を解決した後にのみルータを削除できます。

手順

ステップ 1 **[デバイス (Devices)]** > **[デバイス管理 (Device Management)]** を選択し、Threat Defense デバイスを編集します。

ステップ 2 **[ルーティング (Routing)]** をクリックします。

ステップ 3 **[Manage Virtual Routers]** をクリックします。

すべての仮想ルータと、マッピングされたインターフェイスが [Virtual Routers] ページに表示されます。

ステップ 4 仮想ルータを削除するには、目的の仮想ルータに対して **[削除 (Delete)]** (🗑) をクリックします。


ステップ5 複数のルータを削除するには、Ctrl キーを押しながら、削除する仮想ルータをクリックします。右クリックして、[削除 (Delete)] をクリックします。

ステップ6 変更を保存するには、[Save] をクリックします。

仮想ルータのモニタリング

仮想ルータをモニターし、トラブルシューティングを行うには、デバイスの CLI にログインして、次のコマンドを使用します。

- **show vrf** : 仮想ルータとその関連インターフェースの詳細情報が表示されます。
- **show route vrf <vrf_name>** : 仮想ルータのルーティング詳細情報が表示されます。
- **show run router bgp all** : すべての仮想ルータの BGP ルーティング詳細情報が表示されます。
- **show run router bgp vrf <vrf_name>** : 仮想ルータの BGP ルーティング詳細情報が表示されます。
- **show crypto ipsec sa/show crypto ikev2 sa** : トンネルと関連仮想ルータの詳細情報が表示されます。
- サイト間監視ダッシュボード ([概要 (Overview)] > [サイト間VPN (Site to Site VPN)]) でトンネルを監視できます。

[トンネルステータス (Tunnel Status)] ウィジェットで、トポロジにマウスのカーソルを合わせ、[表示 (View)]  をクリックし、[パケットトレーサ (Packet Tracer)] をクリックして、脅威防御 VPN トンネルを表示およびトラブルシューティングします。

仮想ルータの設定例

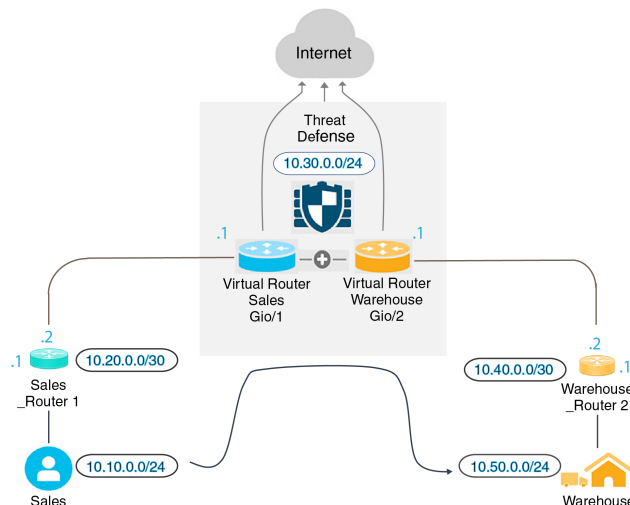
仮想ルータを介して遠隔サーバーにルーティングする方法

仮想ルーティングでは、複数の仮想ルータを作成して、インターフェースグループごとに個別のルーティングテーブルを用意することにより、ネットワークの分離を実現できます。場合によっては、個別の仮想ルータを介してのみ到達可能なサーバーにアクセスする必要があります。この例では、仮想ルータを相互接続して、複数のホップで隔てられているホストに到達する手順について説明します。

たとえば、衣料品会社の販売部門のメンバーが、工場単位の保管倉庫部門で保管されている在庫を検索するとします。仮想ルーティング環境では、宛先 (保管倉庫部門) が販売部門から複数ホップ離れている仮想ルータ間でルートをリークする必要があります。この操作は、マルチホップルートリークを追加することで実行されます。この場合、販売部門の仮想ルータ (送信元) で、保管倉庫の仮想ルータ (宛先) のインターフェースへのスタティックルートを設定す

する必要があります。宛先ネットワークが複数ホップ離れているため、宛先ネットワーク（10.50.0.0/24）へのルートを使用して、保管倉庫の仮想ルータを設定する必要があります。

図 1: 2つの仮想ルータの相互接続：例



始める前に

この例では、10.20.0.1/30 インターフェイスから 10.50.0.5/24 へトラフィックをルーティングするように Sales_Router1 がすでに設定されていることを前提としています。

手順

ステップ 1 販売部門の仮想ルータに割り当てられるデバイスの内部インターフェイス（Gi0/1）を設定します。

- a) **[Devices] > [Device Management] > [Interfaces]** の順に選択します。
- b) Gi0/1 インターフェイスを編集します。
 - [Name] : この例では、VR-Sales です。
 - [Enabled] チェックボックスをオンにします。
 - [IPv4] で、[IP Type] として [Use Static IP] を選択します。
 - [IP Address] : 「10.30.0.1/24」と入力します。
- c) [OK] をクリックします。
- d) **[保存 (Save)]** をクリックします。

ステップ 2 保管倉庫部門の仮想ルータに割り当てられるデバイスの内部インターフェイス（Gi0/2）を設定します。

- a) **[Devices] > [Device Management] > [Interfaces]** の順に選択します。
- b) Gi0/2 インターフェイスを編集します。

- [Name] : この例では、VR-Warehouse です。
- [Enabled] チェックボックスをオンにします。
- [IPv4] で、[IP Type] として [Use Static IP] を選択します。
- [IP Address] : 空白のままにします。ユーザー定義の仮想ルータをまだ作成していないため、システムは、同じ IP アドレス (10.30.0.1/24) を使用してインターフェイスを設定することをユーザーに許可しません。

- c) [OK] をクリックします。
- d) [保存 (Save)] をクリックします。

ステップ 3 販売部門および保管倉庫部門の仮想ルータを作成し、それぞれのインターフェイスを割り当てます。

- a) [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択し、Threat Defense デバイスを編集します。
- b) [ルーティング (Routing)] > [仮想ルータの管理 (Manage Virtual Routers)] の順に選択します。
- c) [Add Virtual Router] をクリックして、販売部門の仮想ルータを作成します。
- d) [Add Virtual Router] をクリックして、保管倉庫部門の仮想ルータを作成します。
- e) 仮想ルータのドロップダウンから [Sales] を選択し、[Virtual Router Properties] で、[Selected Interface] として [VR-Sales] を追加して保存します。
- f) 仮想ルータのドロップダウンから [Warehouse] を選択し、[Virtual Router Properties] で、[Selected Interface] として [VR-Warehouse] を追加して保存します。

ステップ 4 VR-Warehouse インターフェイスの設定を再確認します。

- a) [Devices] > [Device Management] > [Interfaces] の順に選択します。
- b) [VR-Warehouse] インターフェイスに対する [Edit] をクリックします。[IP Address] に「10.30.0.1/24」と入力します。インターフェイスが2つの異なる仮想ルータに個別に割り当てられたため、VR-Sales に同じ IP アドレスを設定できるようになりました。
- c) [OK] をクリックします。
- d) [保存 (Save)] をクリックします。

ステップ 5 保管倉庫部門のサーバー (10.50.0.0/24) のネットワークオブジェクトと、保管倉庫部門のゲートウェイ (10.40.0.2/30) のネットワークオブジェクトを作成します。

- a) [Objects] > [Object Management] の順に選択します。
- b) [Add Network] > [Add Object] の順に選択します。
 - [Name] : この例では、Warehouse-Server です。
 - [Network] : [Network] をクリックして「10.50.0.0/24」と入力します。
- c) [保存 (Save)] をクリックします。
- d) [Add Network] > [Add Object] の順に選択します。
 - [Name] : この例では、Warehouse-Gateway です。

- [Network] : [Host] をクリックして「10.40.0.2」と入力します。

e) [保存 (Save)] をクリックします。

ステップ6 VR-Warehouse インターフェイスをポイントする、販売部門でのルートリークを定義します。

- [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択し、Threat Defense デバイスを編集します。
- [ルーティング (Routing)] を選択します。
- ドロップダウンから販売部門の仮想ルータを選択して、[Static Route] をクリックします。
- [ルートを追加 (Add Route)] をクリックします。[Add Static Route Configuration] で、次の項目を指定します。

- [Interface] : [VR-Warehouse] を選択します。
- [Network] : Warehouse-Server オブジェクトを選択します。
- [Gateway] : 空白のままにします。別の仮想ルータにルートをリークする場合には、ゲートウェイを選択しません。

The screenshot shows the 'Add Static Route Configuration' dialog box. It has a title bar with a question mark icon. Below the title bar, there are several sections:

- Type:** Radio buttons for IPv4 (selected) and IPv6.
- Interface*:** A dropdown menu showing 'VR-Warehouse'.
- Available Network:** A search bar with a magnifying glass icon and a plus sign. Below it is a list of network objects: 'any-ipv4', 'IPv4-Benchmark-Tests', 'IPv4-Link-Local', 'IPv4-Multicast', 'IPv4-Private-10.0.0.0-8', and 'IPv4-Private-172.16.0.0-12'. An 'Add' button is to the right of the search bar.
- Selected Network:** A box containing 'Warehouse-Server' with a trash icon to its right.
- Gateway*:** An empty dropdown menu with a plus sign.
- Metric:** A text input field containing '1'. Below it is the text '(1 - 254)'.
- Tunneled:** A checkbox that is unchecked, followed by the text '(Used only for default Route)'.
- Route Tracking:** An empty dropdown menu with a plus sign.
- Buttons:** 'Cancel' and 'OK' buttons at the bottom right.

e) [OK] をクリックします。

f) [保存 (Save)] をクリックします。

ステップ7 保管倉庫部門の仮想ルータで、Warehouse Router 2 ゲートウェイをポイントするルートを定義します。

- a) ドロップダウンから保管倉庫部門の仮想ルータを選択して、[Static Route] をクリックします。
- b) [ルートを追加 (Add Route)] をクリックします。[Add Static Route Configuration] で、次の項目を指定します。

- [Interface] : [VR-Warehouse] を選択します。
- [Network] : Warehouse-Server オブジェクトを選択します。
- [Gateway] : Warehouse-Gateway オブジェクトを選択します。

Add Static Route Configuration

Type: IPv4 IPv6

Interface*
VR-Warehouse

Available Network +

- any-ipv4
- IPv4-Benchmark-Tests
- IPv4-Link-Local
- IPv4-Multicast
- IPv4-Private-10.0.0.0-8
- IPv4-Private-172.16.0.0-12

Selected Network
Warehouse-Server

Ensure that egress virtualrouter has route to that destination

Gateway
Warehouse-Gateway +

Metric:
1
(1 - 254)

Tunneled: (Used only for default Route)

Route Tracking:
+

Cancel OK

- c) [OK] をクリックします。
- d) [保存 (Save)] をクリックします。

ステップ 8 保管倉庫部門のサーバーへのアクセスを許可するアクセスコントロールルールを設定します。アクセスコントロールルールを作成するには、セキュリティゾーンを作成する必要があります。[Object] > [Object Management] > [Interface] を使用します。[Add] > [Security Zone] を選択して、VR-Sales および VR-Warehouse のセキュリティゾーンを作成します。Warehouse-Server のネットワークオブジェクト用に、Warehouse-Server インターフェイスグループを作成します ([Add] > [Interface Group] を選択)。

ステップ 9 [Policies] > [Access Control] を選択してアクセスコントロールルールを設定し、販売部門の仮想ルータの送信元インターフェイスから、宛先 Warehouse-Server ネットワークオブジェクトの保管倉庫部門用仮想ルータに含まれる宛先インターフェイスへのトラフィックを許可します。

たとえば、Sales のインターフェイスが Sales-Zone セキュリティゾーンにあり、Warehouse のインターフェイスが Warehouse-Zone セキュリティゾーンにある場合、アクセスコントロールルールは次のようになります。

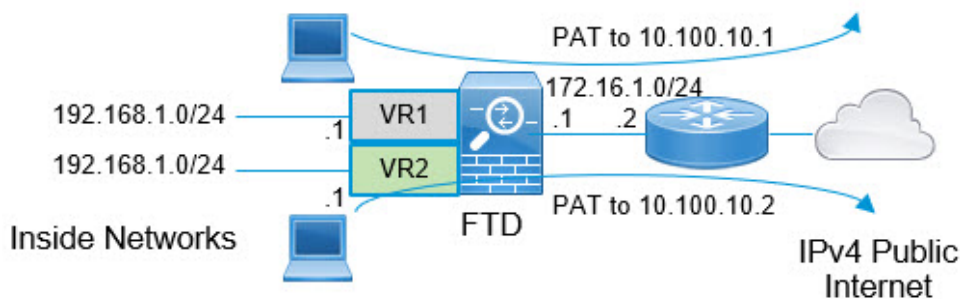
The screenshot shows the configuration page for 'SalesWarehouse'. The 'Rules' tab is active, displaying a table of rules. A search filter 'Warehouse-Rule' is applied. The table shows one rule with the following details:

Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applicat...	Source Ports	Dest Ports	URLs	Source SGT	Dest SGT	Action
Mandatory - SalesWarehouse (1-1)													
1	Warehouse-Rule	Sales-Zone	Warehouse-Zone	Any	10.50.0.5	Any	Any	Any	Any	Any	Any	Any	Allow

重複するアドレス空間を使用してインターネットアクセスを提供する方法

仮想ルータを使用する場合、別のルータに存在するインターフェイスに対して同じネットワークアドレスを設定できます。ただし、個別の仮想ルータでルーティングされる IP アドレスは同じであるため、個別の NAT/PAT プールを持つ各インターフェイスに NAT/PAT ルールを適用して、リターントラフィックが正しい宛先に送信されるようにします。この例では、仮想ルータと NAT/PAT ルールを設定して、重複するアドレス空間を管理する手順を示します。

たとえば、Threat Defense のインターフェイス vr1-inside および vr2-inside は、IP アドレス 192.168.1.1/24 を使用するように定義して、192.168.1.0/24 ネットワーク内の各セグメント上のエンドポイントを管理できます。たとえば、同じアドレス空間を使用する 2 つの仮想ルータからのインターネットアクセスを許可するには、NAT ルールを各仮想ルータ内のインターフェイスに個別に適用する必要があります。個別の NAT または PAT プールを使用するのが理想的です。PAT を使用して、VR1 の送信元アドレスを 10.100.10.1 に変換し、VR2 の送信元アドレスを 10.100.10.2 に変換できます。次の図は、インターネット側の外部インターフェイスがグローバルルータの一部である場合の設定を示しています。送信元インターフェイス (vr1-inside および vr2-inside) を明示的に選択して NAT/PAT ルールを定義する必要があります。送信元インターフェイスとして「any」を使用すると、同じ IP アドレスが 2 つの異なるインターフェイスに存在する可能性があるため、システムが正しい送信元を識別できなくなります。



- (注) 重複するアドレス空間を使用しない仮想ルータ内に一部のインターフェイスがある場合でも、送信元インターフェイスを指定して NAT ルールを定義することでトラブルシューティングが容易になり、インターネットにバインドされた仮想ルータからのトラフィックを確実に分離できます。

手順

ステップ 1 VR1 のデバイスの内部インターフェイスを設定します。

- a) **[Devices] > [Device Management] > [Interfaces]** の順に選択します。
- b) VR1 に割り当てるインターフェイスを編集します。
 - [名前 (Name)] : この例では、vr1-inside。
 - [Enabled] チェックボックスをオンにします。
 - [IPv4] で、[IP Type] として [Use Static IP] を選択します。
 - [IPアドレス (IP Address)] : 192.168.1.1/24 を入力します。
- c) [OK] をクリックします。
- d) **[保存 (Save)]** をクリックします。

ステップ 2 VR2 のデバイスの内部インターフェイスを設定します。

- a) **[Devices] > [Device Management] > [Interfaces]** の順に選択します。
- b) VR2 に割り当てるインターフェイスを編集します。
 - [名前 (Name)] : この例では、vr2-inside。
 - [Enabled] チェックボックスをオンにします。
 - [IPv4] で、[IP Type] として [Use Static IP] を選択します。
 - [IP Address] : 空白のままにします。ユーザー定義の仮想ルータをまだ作成していないため、ユーザーは同じ IP アドレスを使用してインターフェイスを設定できません。
- c) [OK] をクリックします。

d) [保存 (Save)] をクリックします。


ステップ 3 VR1 および外部インターフェイスへの静的デフォルトルートリンクを設定します。


- a) [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択し、Threat Defense デバイスを編集します。
- b) [ルーティング (Routing)] > [仮想ルータの管理 (Manage Virtual Routers)] の順に選択します。[仮想ルータの追加 (Add Virtual Router)] をクリックして、VR1 を作成します。
- c) VR1 の場合、[仮想ルータのプロパティ (Virtual Router Properties)] で、vr1-inside を割り当てて保存します。
- d) [Static Route] をクリックします。
- e) [ルートを追加 (Add Route)] をクリックします。[Add Static Route Configuration] で、次の項目を指定します。
 - [インターフェイス (Interface)] : グローバルルータの外部インターフェイスを選択します。
 - [ネットワーク (Network)] : any-ipv4 オブジェクトを選択します。このネットワークは、VR1 内でルーティングできないすべてのトラフィックのデフォルトルートになります。
 - [Gateway] : 空白のままにします。別の仮想ルータにルートをリンクする場合には、ゲートウェイを指定しません。

Add Static Route Configuration

Type: IPv4 IPv6

Interface*
outside

(Interface starting with this icon  signifies it is available for route leak)

Available Network  +

Selected Network

Q Search

- any-ipv4
- IPv4-Benchmark-Tests
- IPv4-Link-Local
- IPv4-Multicast
- IPv4-Private-10.0.0.0-8
- IPv4-Private-172.16.0.0-12

any-ipv4

Ensure that egress virtualrouter has route to that destination

Gateway
 +

Metric:
1
(1 - 254)

Tunneled: (Used only for default Route)

Route Tracking:
 +

- f) [OK] をクリックします。
- g) [保存 (Save)] をクリックします。

ステップ 4 VR2 および外部インターフェイスへの静的デフォルトルートトリックを設定します。

- a) [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択し、Threat Defense デバイスを編集します。
- b) [ルーティング (Routing)] > [仮想ルータの管理 (Manage Virtual Routers)] の順に選択します。[仮想ルータの追加 (Add Virtual Router)] をクリックして、VR2 を作成します。
- c) VR2 の場合、[仮想ルータのプロパティ (Virtual Router Properties)] で、vr2-inside を割り当てて保存します。
- d) [Static Route] をクリックします。
- e) [ルートを追加 (Add Route)] をクリックします。[Add Static Route Configuration] で、次の項目を指定します。

- [インターフェイス (Interface)] : グローバルルータの外部インターフェイスを選択します。
- [ネットワーク (Network)] : any-ipv4 オブジェクトを選択します。このネットワークは、VR2内でルーティングできないすべてのトラフィックのデフォルトルートになります。
- [Gateway] : 空白のままにします。別の仮想ルータにルートをリークする場合は、ゲートウェイを選択しません。

Add Static Route Configuration ?

Type: IPv4 IPv6

Interface*
 ▼
(Interface starting with this icon signifies it is available for route leak)

Available Network + Selected Network

Add

Available Network	Selected Network
any-ipv4	any-ipv4 🗑
IPv4-Benchmark-Tests	
IPv4-Link-Local	
IPv4-Multicast	
IPv4-Private-10.0.0.0-8	
IPv4-Private-172.16.0.0-12	

Ensure that egress virtualrouter has route to that destination

Gateway
 +

Metric:

(1 - 254)

Tunneled: (Used only for default Route)

Route Tracking:
 +

- f) [OK] をクリックします。
- g) [保存 (Save)] をクリックします。


ステップ 5 グローバルルータの外部インターフェイスで IPv4 スタティック デフォルトルート、つまり 172.16.1.2 を設定します。


- a) [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択し、Threat Defense デバイスを編集します。
- b) [ルーティング (Routing)] を選択し、グローバルルータのプロパティを編集します。
- c) [Static Route] をクリックします。
- d) [ルートを追加 (Add Route)] をクリックします。[Add Static Route Configuration] で、次の項目を指定します。
 - [インターフェイス (Interface)] : グローバルルータの外部インターフェイスを選択します。
 - [ネットワーク (Network)] : any-ipv4 オブジェクトを選択します。これは、任意の IPv4 トラフィックのデフォルトルートになります。
 - [ゲートウェイ (Gateway)] : 作成されている場合は、ドロップダウンからホスト名を選択します。オブジェクトがまだ作成されていない場合は、[追加 (Add)] をクリックして、外部インターフェイス (この例では 172.16.1.2) のネットワークリンクの反対側にあるゲートウェイの IP アドレスに対してホストオブジェクトを定義します。オブジェクトを作成したら、[ゲートウェイ (Gateway)] フィールドで選択します。

Add Static Route Configuration

Type: IPv4 IPv6

Interface*

(Interface starting with this icon  signifies it is available for route leak)

Available Network  +

- any-ipv4
- IPv4-Benchmark-Tests
- IPv4-Link-Local
- IPv4-Multicast
- IPv4-Private-10.0.0.0-8
- IPv4-Private-172.16.0.0-12

Selected Network

Gateway*
 +

Metric:

(1 - 254)

Tunneled: (Used only for default Route)

Route Tracking:
 +

- e) [OK] をクリックします。
- f) [保存 (Save)] をクリックします。

ステップ 6 vr2-inside インターフェイスの設定を再確認します。

- a) [Devices] > [Device Management] > [Interfaces] の順に選択します。
- b) vr2-inside インターフェイスに対して [編集 (Edit)] をクリックします。IP アドレスを 192.168.1.1/24 として指定します。インターフェイスが2つの異なる仮想ルータに個別に割り当てられたため、vr2-inside に同じ IP アドレスを設定できるようになりました。
- c) [OK] をクリックします。
- d) [保存 (Save)] をクリックします。

ステップ 7 VR1 の内部から外部へのトラフィックの 10.100.10.1 への PAT を実行する NAT ルールを作成します。

- a) [デバイス (Devices)] > [NAT] の順に選択します。
- b) [新しいポリシー (New Policy)] > [Threat Defense NAT] をクリックします。

- c) NAT ポリシー名として **InsideOutsideNATRule** を入力し、**Threat Defense** デバイスを選択します。[保存 (Save)] をクリックします。
- d) [InsideOutsideNATRule] ページで、[ルールを追加 (Add Rule)] をクリックして、以下を定義します。
- [NATルール (NAT Rule)] : [手動NATルール (Manual NAT Rule)] を選択します。
 - [タイプ (Type)] : [ダイナミック (Dynamic)] を選択します。
 - [挿入 (Insert)] : ダイナミック NAT ルールが存在する場合は [前述 (Above)] を選択します。
 - [Enabled] をクリックします。
 - [インターフェイスオブジェクト (Interface Objects)] で、**vr1-interface** オブジェクトを選択し、[ソースに追加 (Add to Source)] をクリックします (オブジェクトがない場合は、[オブジェクト (Object)] > [オブジェクト管理 (Object Management)] > [インターフェイス (Interface)] でオブジェクトを作成します)。次に、[宛先に追加 (Add to Destination)] で [外部 (Outside)] を選択します。
 - [変換 (Translation)] の [元の送信元 (Original Source)] で、[any-ipv4] を選択します。[変換済み送信元 (Translated Source)] で、[追加 (Add)] をクリックし、10.100.10.1 を指定してホストオブジェクト **VR1-PAT-Pool** を定義します。次の図に示されているように、**VR1-PAT-Pool** を選択します。

The screenshot shows the configuration for a NAT rule. The 'NAT Rule' dropdown is set to 'Manual NAT Rule'. The 'Insert' dropdown is set to 'In Category' and 'NAT Rules Before'. The 'Type' dropdown is set to 'Static'. The 'Enable' checkbox is checked. The 'Description' field is empty. The 'Translation' tab is selected, showing the 'Original Packet' and 'Translated Packet' sections. The 'Original Source' is 'any-ipv4' and the 'Original Destination' is 'Address'. The 'Translated Source' is 'VR1-PAT-Pool'. The 'Translated Destination' is empty. The 'Original Source Port', 'Original Destination Port', 'Translated Source Port', and 'Translated Destination Port' fields are all empty. The 'Cancel' and 'OK' buttons are at the bottom right.

- e) [OK] をクリックします。
- f) [保存 (Save)] をクリックします。

ステップ 8 VR2 の内部から外部へのトラフィックの 10.100.10.2 への PAT を実行する NAT ルールを追加します。

a) [デバイス (Devices)] > [NAT] の順に選択します。

b) InsideOutsideNATRule を編集して、VR2 NAT ルールを定義します。

- [NATルール (NAT Rule)] : [手動NATルール (Manual NAT Rule)] を選択します。
- [タイプ (Type)] : [ダイナミック (Dynamic)] を選択します。
- [挿入 (Insert)] : ダイナミック NAT ルールが存在する場合は [前述 (Above)] を選択します。
- [Enabled] をクリックします。
- [インターフェイスオブジェクト (Interface Objects)] で、vr2-interface オブジェクトを選択し、[ソースに追加 (Add to Source)] をクリックします (オブジェクトがない場合は、[オブジェクト (Object)] > [オブジェクト管理 (Object Management)] > [インターフェイス (Interface)] でオブジェクトを作成します)。次に、[宛先に追加 (Add to Destination)] で [外部 (Outside)] を選択します。
- [変換 (Translation)] の [元の送信元 (Original Source)] で、[any-ipv4] を選択します。[変換済み送信元 (Translated Source)] で、[追加 (Add)] をクリックし、10.100.10.2 を指定してホストオブジェクト VR2-PAT-Pool を定義します。次の図に示されているように、VR2-PAT-Pool を選択します。

NAT Rule:
Manual NAT Rule

Insert:
In Category: [] NAT Rules Before: []

Type:
Static

Enable
Description:
[]

Interface Objects Translation PAT Pool Advanced

Original Packet	Translated Packet
Original Source:* any-ipv4	Translated Source: Address
Original Destination: Address	Translated Destination: VR2-PAT-Pool
Original Source Port: []	Translated Source Port: []
Original Destination Port: []	Translated Destination Port: []

Cancel OK

c) [OK] をクリックします。

d) [保存 (Save)] をクリックします。

ステップ 9 vr1-inside および vr2-inside インターフェイスから外部インターフェイスへのトラフィックを許可するアクセスコントロールポリシーを設定するには、セキュリティゾーンを作成する必要があります。[Object] > [Object Management] > [Interface] を使用します。[追加 (Add)] > [セキュリティゾーン (Security Zone)] を選択し、vr1-inside、vr2-inside、および外部インターフェイスのセキュリティゾーンを作成します。

ステップ 10 [ポリシー (Policies)] > [アクセス制御 (Access Control)] を選択し、vr1-inside-zone および vr2-inside-zone から outside_zone へのトラフィックを許可するアクセス制御ルールを設定します。

インターフェイスの名前が付けられたゾーンを作成したとすると、すべてのトラフィックがインターネットに流れることを許可する基本ルールは、次のようになります。このアクセスコントロールポリシーに他のパラメータを適用できます。

Add Rule

Name: AllowInternetTraffic Enabled Insert: into Mandatory

Action: Allow Time Range: +

Zones Networks VLAN Tags **Users** Applications Ports URLs SGT/ISE Attributes

Available Zones

- outside-zone
- vr1-inside-zone
- vr2-inside-zone

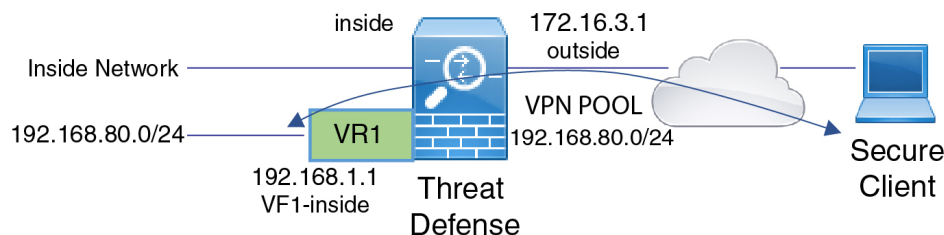
Source Zones (2)

- vr1-inside-zone
- vr2-inside-zone

仮想ルーティングで内部ネットワークへの RA VPN アクセスを許可する方法

仮想ルーティング対応デバイスでは、RA VPN は、グローバル仮想ルータインターフェイスでのみサポートされます。この例では、セキュアクライアントユーザーがユーザー定義の仮想ルータネットワークに接続できるようにする手順を示します。

次の例では、RA VPN (セキュアクライアント) ユーザーが、172.16.3.1 の Threat Defense の外部インターフェイスに接続します。このユーザーには 192.168.80.0/24 のプールに含まれる IP アドレスが割り当てられます。ユーザーは、グローバル仮想ルータのみの内部ネットワークにアクセスできます。ユーザー定義の仮想ルータ VR1 のネットワーク (つまり、192.168.1.0/24) を介したトラフィックフローを許可するには、グローバルと VR1 でスタティックルートを設定してルートをリークします。



始める前に

この例では、すでに RA VPN を設定し、仮想ルータを定義し、インターフェイスを設定して適切な仮想ルータに割り当てていることを前提としています。

手順

ステップ 1 グローバル仮想ルータからユーザー定義の VR1 へのルートリークを設定します。

- a) [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択し、Threat Defense デバイスを編集します。
- b) [ルーティング (Routing)] をクリックします。デフォルトでは、グローバルルーティングプロパティのページが表示されます。
- c) [Static Route] をクリックします。
- d) [ルートを追加 (Add Route)] をクリックします。[Add Static Route Configuration] で、次の項目を指定します。
 - [インターフェイス (Interface)] : VR1 内部インターフェイスを選択します。
 - [ネットワーク (Network)] : VR1 仮想ルータ ネットワーク オブジェクトを選択します。[オブジェクトの追加 (Add Object)] オプションを使用してオブジェクトを作成できます。
 - [Gateway] : 空白のままにします。別の仮想ルータにルートをリークする場合には、ゲートウェイを選択しません。

Add Static Route Configuration ?

Type: IPv4 IPv6

Interface*
vr1-inside

Available Network +

Q Search

- IPv4-Private-10.0.0.0-8
- IPv4-Private-172.16.0.0-12
- IPv4-Private-192.168.0.0-16
- IPv4-Private-All-RFC1918
- IPv6-to-IPv4-Relay-Anycast
- nw-192.168.1.0

Add

Selected Network

nw-192.168.1.0 ✕

Gateway* +

Metric:
1
(1 - 254)

Tunneled: (Used only for default Route)

Route Tracking: +

Cancel OK

ルートトリックにより、VPN プール内の IP アドレスが割り当てられたセキュアクライアントは、VR1 仮想ルータの 192.168.1.0/24 ネットワークにアクセスできるようになります。

e) [OK] をクリックします。

ステップ 2 VR1 からグローバル仮想ルータへのルートトリックを設定します。

- a) [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択し、Threat Defense デバイスを編集します。
- b) [ルーティング (Routing)] をクリックし、ドロップダウンから [VR1] を選択します。
- c) [Static Route] をクリックします。
- d) [ルートを追加 (Add Route)] をクリックします。[Add Static Route Configuration] で、次の項目を指定します。
 - [インターフェイス (Interface)] : グローバルルータの外部インターフェイスを選択します。
 - [ネットワーク (Network)] : グローバル仮想ルータ ネットワーク オブジェクトを選択します。
 - [Gateway] : 空白のままにします。別の仮想ルータにルートをリークする場合には、ゲートウェイを選択しません。

Add Static Route Configuration ?

Type: IPv4 IPv6

Interface*
outside

Available Network +
Q Search
outside-gateway
vpn-pool
vr1-inside
VR1-PAT-Pool
vr2-inside
VR2-PAT-Pool

Selected Network
vpn-pool

Gateway* +

Metric:
1
(1 - 254)

Tunneled: (Used only for default Route)

Route Tracking: +

Cancel OK

設定されたスタティックルートにより、192.168.1.0/24 ネットワーク（VR1）上のエンドポイントは、VPN プール内の IP アドレスが割り当てられたセキュアクライアントへの接続を開始できます。

e) [OK] をクリックします。

次のタスク

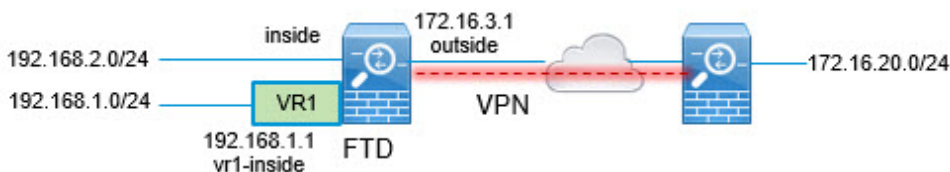
RA VPN アドレスプールとユーザー定義の仮想ルータの IP アドレスが重複している場合には、IP アドレスに対してスタティック NAT ルールを使用し、適切なルーティングを有効にする必要があります。または、重複しないように RA VPN アドレスプールを変更することもできます。

サイト間 VPN における複数の仮想ルータのネットワークからのトラフィックを保護する方法

仮想ルーティング対応デバイスでは、サイト間 VPN はグローバル仮想ルータインターフェイスでのみサポートされます。ユーザー定義の仮想ルータに属するインターフェイスでは設定できません。この例では、サイト間 VPN を介して、ユーザー定義の仮想ルータ内でホストされ

ているネットワークとの間の接続を保護する手順を示します。また、ユーザー定義の仮想ルーティングネットワークが含まれるように、サイト間 VPN 接続を更新する必要があります。

ブランチオフィス ネットワークと本社ネットワークの間にサイト間 VPN が設定されているシナリオを考えてみましょう。ブランチオフィスの Threat Defense に仮想ルータがあります。この例では、サイト間 VPN は 172.16.3.1 のブランチオフィスの外部インターフェイスで定義されます。この VPN には、内部インターフェイスがグローバル仮想ルータの一部でもあるため、追加の設定なしで内部ネットワーク 192.168.2.0/24 が含まれます。ただし、VR1 仮想ルータの一部である 192.168.1.0/24 ネットワークにサイト間 VPN サービスを提供するには、グローバルおよび VR1 でスタティックルートを設定して、VR1 ネットワークをサイト間 VPN 設定に追加して、ルートをリークする必要があります。



始める前に

この例では、すでに 192.168.2.0/24 ローカルネットワークと 172.16.20.0/24 外部ネットワークの間にサイト間 VPN を設定し、仮想ルータを定義し、インターフェイスを設定して適切な仮想ルータに割り当てていることを前提としています。

手順

ステップ 1 グローバル仮想ルータからユーザー定義の VR1 へのルートリークを設定します。

- a) [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択し、Threat Defense デバイスを編集します。
- b) [ルーティング (Routing)] をクリックします。デフォルトでは、グローバルルーティング プロパティのページが表示されます。
- c) [Static Route] をクリックします。
- d) [ルートを追加 (Add Route)] をクリックします。[Add Static Route Configuration] で、次の項目を指定します。
 - [インターフェイス (Interface)] : VR1 内部インターフェイスを選択します。
 - [ネットワーク (Network)] : VR1 仮想ルータ ネットワーク オブジェクトを選択します。[オブジェクトの追加 (Add Object)] オプションを使用してオブジェクトを作成できます。
 - [Gateway] : 空白のままにします。別の仮想ルータにルートをリークする場合には、ゲートウェイを選択しません。

Add Static Route Configuration

Type: IPv4 IPv6

Interface*
vr1-inside

Available Network +

Search

IPv4-Private-10.0.0.0-8
IPv4-Private-172.16.0.0-12
IPv4-Private-192.168.0.0-16
IPv4-Private-All-RFC1918
IPv6-to-IPv4-Relay-Anycast
nw-192.168.1.0

Add

Selected Network
nw-192.168.1.0

Gateway* +

Metric:
1
(1 - 254)

Tunneled: (Used only for default Route)

Route Tracking: +

Cancel OK

ルートリークにより、サイト間 VPN の外部（リモート）エンドによって保護されたエンドポイントは、VR1 仮想ルータの 192.168.1.0/24 ネットワークにアクセスできます。

e) [OK] をクリックします。

ステップ 2 VR1 からグローバル仮想ルータへのルートリークを設定します。

- [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択し、Threat Defense デバイスを編集します。
- [ルーティング (Routing)] をクリックし、ドロップダウンから [VR1] を選択します。
- [Static Route] をクリックします。
- [ルートを追加 (Add Route)] をクリックします。[Add Static Route Configuration] で、次の項目を指定します。
 - [インターフェイス (Interface)] : グローバルルータの外部インターフェイスを選択します。
 - [ネットワーク (Network)] : グローバル仮想ルータ ネットワーク オブジェクトを選択します。
 - [Gateway] : 空白のままにします。別の仮想ルータにルートを手動でリークする場合には、ゲートウェイを選択しません。

Add Static Route Configuration ?

Type: IPv4 IPv6

Interface*
outside

Available Network +
Q Search

- any-ipv4
- default-ipv4
- external-vpn-nw
- inside
- IPv4-Benchmark-Tests
- IPv4-Link-Local

Add

Selected Network
external-vpn-nw 🗑

Gateway* +

Metric:
1
(1 - 254)

Tunneled: (Used only for default Route)

Route Tracking: +

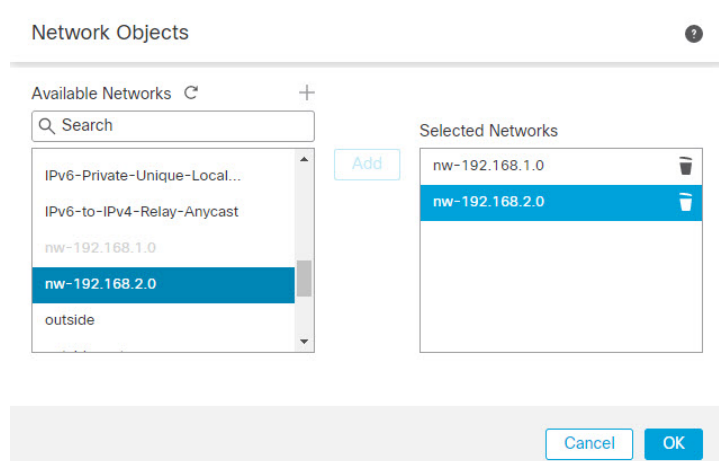
Cancel OK

このスタティックルートにより、192.168.1.0/24 ネットワーク（VR1）上のエンドポイントは、サイト間 VPN トンネルを通過する接続を開始できます。この例では、リモートエンドポイントが 172.16.20.0/24 ネットワークを保護しています。

e) [OK] をクリックします。

ステップ 3 192.168.1.0/24 ネットワークをサイト間 VPN 接続プロファイルに追加します。

- a) [デバイス (Devices)] > [VPN] > [サイト間 (Site To Site)] を選択し、VPN トポロジを編集します。
- b) [エンドポイント (Endpoints)] で、ノード A エンドポイントを編集します。
- c) [エンドポイントの編集 (Edit Endpoint)] の [保護されたネットワーク (Protected Networks)] フィールドで、[新しいネットワークオブジェクトの追加 (Add New Network Object)] をクリックします。
- d) 192.168.1.0 ネットワークで VR1 ネットワークオブジェクトを追加します。



e) [OK] をクリックして設定を保存します。

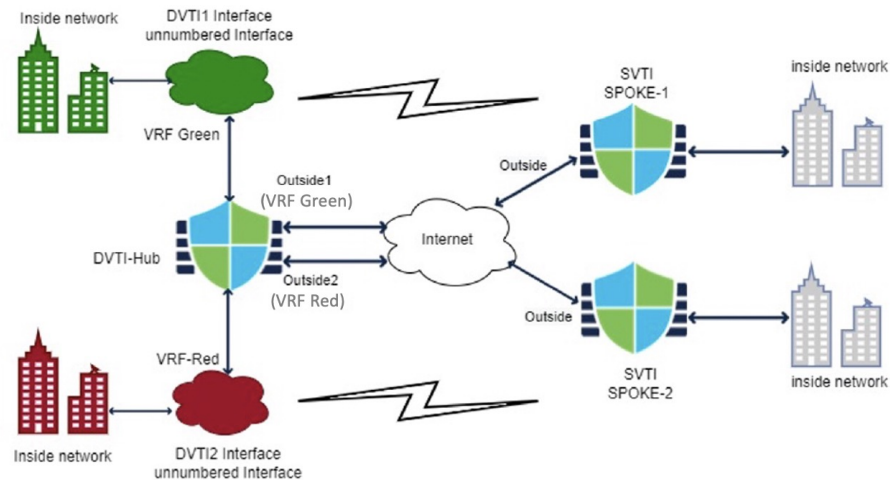
ダイナミック VTI を使用したサイト間 VPN における複数の仮想ルータのネットワークからのトラフィックを保護する方法

ISP は、お客様ごとに異なるセグメント化されたネットワークを持っています。仮想ルータを作成し、作成した仮想ルータにダイナミック VTI を関連付けて、ネットワーク内のダイナミック VTI の機能を拡張できます。ダイナミック VTI は、グローバルまたはユーザー定義の仮想ルータに関連付けることができます。単一の Threat Defense デバイスは、グローバルまたは 1 つ以上のユーザー定義の仮想ルータを備えたダイナミック VTI ハブとして機能できます。ユーザー定義の各仮想ルータを 1 つのカスタマーネットワークにすることができます。

ルートベースのサイト間 VPN が 2 つの会社の本社ネットワークと 2 つ会社の支社ネットワークの間に構成されている例を考えてみましょう。ISP の Threat Defense 機能であるダイナミック VTI ハブは、2 つのユーザー定義の仮想ルータ (VRF グリーンと VRF レッド) を使用して、2 つの企業本社ネットワークを管理します。ダイナミック VTI ハブは、以下の間でサイト間 VPN を確立します。

- お客様 1 (VRF グリーン) および支社 1 (SVTI スポーク 1)
- お客様 2 (VRF レッド) および支社 2 (SVT2 スポーク 2)

図 2: 複数の仮想ルータと動的 VTI を使用したサイト間 VPN



次の例は、動的 VTI を使用するサイト間 VPN を介し、複数の仮想ルータを使用してネットワークを設定する方法を示しています。

手順

ステップ 1 ハブに動的 VTI インターフェイスを設定します。

- [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択し、Threat Defense デバイスを編集します。
- [インターフェイスの追加 (Add Interfaces)] > [仮想トンネルインターフェイス (Virtual Tunnel Interface)] を選択します。
- [トンネルタイプ (Tunnel Type)] として [動的 (Dynamic)] を選択します。
- インターフェイス名として DVTI1 を指定し、動的 VTI のすべてのパラメータを設定します。
- [Save (保存)] をクリックします。
- ステップ 1a ~ e を繰り返して、ハブの 2 番目の動的 VTI (DVTI2) を設定します。

ステップ 2 スポーク 1 で静的 VTI を設定します。

- [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択し、Threat Defense デバイスを編集します。
- [インターフェイスの追加 (Add Interfaces)] > [仮想トンネルインターフェイス (Virtual Tunnel Interface)] を選択します。
- [トンネルタイプ (Tunnel Type)] として [静的 (Static)] を選択します。
- インターフェイス名として SVTI スポーク 1 を指定し、静的 VTI のすべてのパラメータを設定します。
- [Save (保存)] をクリックします。

- f) ステップ 2a ~ e を繰り返して、スポーク 2 (SVTI スポーク 2) にスタティック VTI を設定します。

ステップ 3 ハブと SVTI スポーク 1 の間にルートベースのサイト間 VPN を構成します。

- a) [デバイス (Devices)] > [サイト間 (Site To Site)] を選択し、 [+サイト間VPN (+ Site To Site VPN)] をクリックします。
- b) [トポロジ名 (Topology Name)] フィールドに、VPN トポロジの名前を入力します。
- c) [ルートベース (VTI) (Route Based (VTI))] を選択し、ネットワークトポロジとして [ハブアンドスポーク (Hub and Spoke)] を選択します。
- d) [エンドポイント (Endpoints)] タブをクリックします。
- e) ハブとスポーク (DVTI1 および SVTI スポーク 1) およびそれぞれのルーティングポリシーを設定します。
- f) 必要に応じて、VPN の [IKE]、[IPsec]、および [詳細 (Advanced)] オプションを設定します。
- g) [保存 (Save)] をクリックします。
- h) ステップ 3a ~ g を繰り返して、ハブ (DVTI2) と SVTI スポーク 2 の間に 2 番目のルートベースのサイト間 VPN トポロジを設定します。

ステップ 4 2 つの仮想ルータを設定します。

- a) [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択し、 Threat Defense デバイスを編集します。
- b) [ルーティング (Routing)] をクリックします。
- c) [Manage Virtual Routers] をクリックします。
- d) [仮想ルータの追加 (Add Virtual Router)] をクリックします。
名前を「VRF グリーン」として、仮想ルータの説明を入力します。
- e) ステップ 4a ~ d を繰り返して、VRF レッドを設定します。

ステップ 5 すべてのインターフェイスを仮想ルータに割り当てます。

- a) ドロップダウンリストから仮想ルータを選択します。
- b) [仮想ルータのプロパティ (Virtual Router Properties)] ページで、 [使用可能なインターフェイス (Available Interfaces)] ボックスに一覧表示されているインターフェイスを選択します。
他のインターフェイスとともにダイナミック VTI インターフェイスを割り当てます。
- c) [Add] をクリックします。

ステップ 6 VRF レッドに対してステップ 5a ~ c を繰り返します。

ステップ 7 仮想ルータのルーティングポリシーを設定します。

- a) ドロップダウンリストから仮想ルータを選択します。
- b) [スタティックルート (Static Route)] またはいずれかのダイナミックルーティングプロトコルをクリックします。
- c) ルーティングパラメータを設定します。

d) [保存 (Save)]をクリックします。

次のタスク

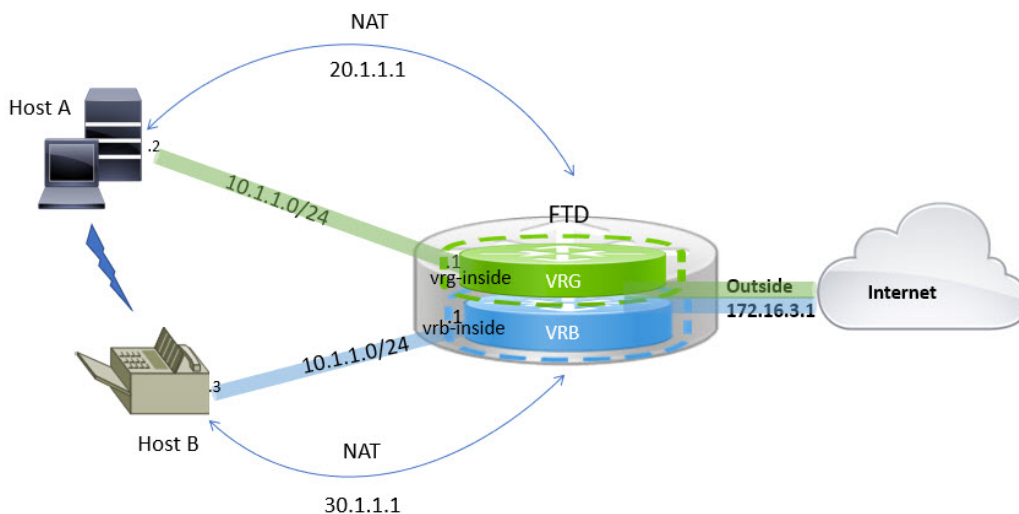
ハブアンドスポークデバイスを選択し、[展開 (Deploy)]をクリックします。展開すると、サイト間監視ダッシュボード ([概要 (Overview)]>[サイト間VPN (Site to Site VPN)]) でVPNトンネルを監視できます。

[仮想ルータのモニタリング \(19ページ\)](#) に一覧表示されているコマンドを使用して、仮想ルータを表示し、トラブルシューティングすることもできます。

仮想ルーティングにおいて2つの重複するネットワークホスト間でトラフィックをルーティングする方法

同じネットワークアドレスを持つ仮想ルータ上にホストを構成できます。ホストの通信には、Twice NATを設定できます。この例では、重複するネットワークホストを管理するためのNATルールの設定手順を示します。

次の例では、2つのホスト (ホストAとホストB) が異なる仮想ルータ (VRG (インターフェイス vrg-inside) 、VRB (インターフェイス vrb-inside)) にそれぞれ属しており、サブネットワーク (10.1.1.0/24) は同じです。両方のホストが通信するために、VRG-Host インターフェイスオブジェクトがマップされたNATアドレス (20.1.1.1) を使用し、VRB-Host インターフェイスオブジェクトがマップされたNATアドレス (30.1.1.1) を使用するNATポリシーを作成します。結果として、ホストAは30.1.1.1を使用してホストBと通信します。ホストBは20.1.1.1を使用してホストAに到達します。



始める前に

この例では、すでに以下の設定が実施されていることを前提としています。

- vrg-inside および vrb-inside インターフェイスは、仮想ルータ（VRG および VRB）にそれぞれ関連付けられており、どちらのインターフェイスも同じサブネットアドレス（10.1.1.0/24 など）を使用して設定されています。
- インターフェイスゾーン VRG-Inf、VRB-Inf は、それぞれ vrg-inside および vrb-inside インターフェイスを指定して作成されています。
- デフォルトゲートウェイとして vrg-inside を使用する VRG のホスト A。デフォルトゲートウェイとして vrb-inside を使用する VRB のホスト B。

手順

- ステップ 1** ホスト A からホスト B へのトラフィックを処理する NAT ルールを作成します。[**デバイス (Devices)**] > [**NAT**] を選択します。
- ステップ 2** [**新しいポリシー (New Policy)**] > [**Threat Defense NAT**] をクリックします。
- ステップ 3** NAT ポリシー名を入力し、Threat Defense デバイスを選択します。[**保存 (Save)**] をクリックします。
- ステップ 4** [NAT] ページで、[**ルールの追加 (Add Rule)**] をクリックして、以下の項目を定義します。
 - [NATルール (NAT Rule)] : [手動NATルール (Manual NAT Rule)] を選択します。
 - [タイプ (Type)] : [静的 (Static)] を選択します。
 - [挿入 (Insert)] : NAT ルールが存在する場合は [前述 (Above)] を選択します。
 - [Enabled] をクリックします。
 - [インターフェイス オブジェクト (Interface Objects)] で、VRB-Inf オブジェクトを選択し、[ソースに追加 (Add to Source)] をクリックします (オブジェクトがない場合は、[オブジェクト (Object)] > [オブジェクト管理 (Object Management)] > [インターフェイス (Interface)] でオブジェクトを作成します)。次に、VRB-Inf オブジェクトを選択して [宛先に追加 (Add to Destination)] をクリックします。
 - [変換 (Translation)] で、以下を選択します。
 - [元の送信元 (Original Source)] で vrg-inside を選択します。
 - [元の宛先 (Original Destination)] で [追加 (Add)] をクリックし、30.1.1.1 を指定してオブジェクト VRB-Mapped-Host を定義します。VRB-Mapped-Host を選択します。
 - [変換済み送信元 (Translated Source)] で [追加 (Add)] をクリックし、20.1.1.1 を指定してオブジェクト VRG-Mapped-Host を定義します。VRG-Mapped-Host を選択します。
 - [変換済みの宛先 (Translated Destination)] で、次の図に示されているように vrb-inside を選択します。

Add NAT Rule ?

NAT Rule:
Manual NAT Rule

Insert:
In Category NAT Rules Before

Type:
Static

Enable

Description:

Interface Objects Translation PAT Pool Advanced

Original Packet	Translated Packet
Original Source:* vrg-inside +	Translated Source: Address
Original Destination: Address	VRG-Mapped-Host +
VRB-Mapped-Host +	Translated Destination: vrb-inside +
Original Source Port: <input type="text"/> +	Translated Source Port: <input type="text"/> +
Original Destination Port: <input type="text"/> +	Translated Destination Port: <input type="text"/> +

Threat Defense デバイスで **show nat detail** コマンドを実行すると、次のような出力が表示されます。

```
firepower(config-service-object-group)# show nat detail
Manual NAT Policies (Section 1)
1 (2001) to (3001) source static vrg-inside VRG-MAPPED-HOST destination static
VRB-MAPPED-HOST vrb-inside
translate_hits = 0, untranslate_hits = 0
Source - Origin: 10.1.1.1/24, Translated: 20.1.1.1/24
Destination - Origin: 30.1.1.1/24, Translated: 10.1.1.1/24
```

ステップ 5 [OK] をクリックします。

ステップ 6 [保存 (Save)] をクリックします。

NAT ルールは次のようになります。

Host2Host Show Warning

Enter Description

Rules

[Filter by Device](#)

#	Direction	Type	Source Interface Objects	Destination Interface Objects	Original Packet			Translated Packet		
					Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	Translated Services
NAT Rules Before										
1		Static	VRG-Inf	VRB-Inf	vrg-inside	VRB-Mapped-Host		VRG-Mapped-Host	vrb-inside	
Auto NAT Rules										
NAT Rules After										

構成を展開すると、警告メッセージが表示されます。

Validation Messages: ×

1 total | 0 errors | 1 warning | 0 infos

ManualNat64Rule: Host2Host

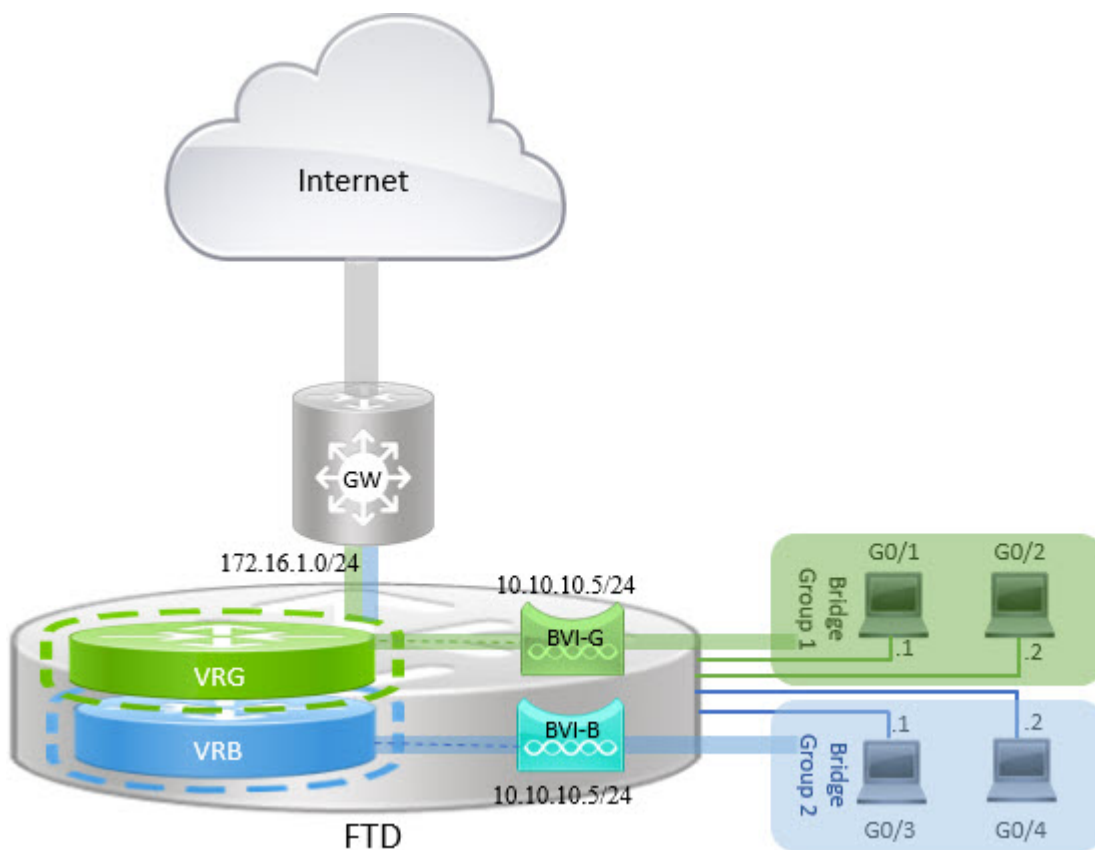
▼ Warning: [ManualNatRule 1] The NAT rule has source and destination interfaces belonging to different Virtual Routers, the traffic will be able to leak between Virtual Routers without explicit route leak configuration whenever destination translation happens. If you intent to apply this NAT rule even when destination translation is not happening, create a static route leak explicitly. The rule involves interfaces from [VRG] to [VRB]

BVI インターフェイスを使用したルーテッド ファイアウォールモードでの重複セグメントの管理方法

複数の重複ネットワーク間に単一の Threat Defense を透過的に展開したり、同じネットワークのホスト間にファイアウォールを展開することができます。この展開を実現するには、仮想ルータごとに BVI を設定します。ここでは、仮想ルータで BVI を設定する手順について説明します。

BVI は、通常のルーテッドインターフェイスのように動作する、ルータ内の仮想インターフェイスです。これはブリッジングをサポートしませんが、ルータ内のルーテッドインターフェイスに相当するブリッジグループを表します。これらのブリッジドインターフェイスで着信または発信するすべてのパケットは、BVI インターフェイスをパススルーします。BVI のインターフェイス番号は、仮想インターフェイスが代表するブリッジグループの番号です。

次の例では、BVI-G が VRG で設定されており、Bridge Group 1 がインターフェイス G0/1 および G0/2 のルーテッドインターフェイスです。同様に、BVI-B が VRB で設定されており、Bridge Group 2 がインターフェイス G0/3 および G0/4 のルーテッドインターフェイスです。両方の BVI が同じ IP サブネットアドレス (10.10.10.5/24) を持っていると考えてください。仮想ルータにより、ネットワークは共有リソース上で分離されます。



手順

ステップ 1 [デバイス (Devices)] > [デバイス管理 (Device Management)] の順に選択します。必要なデバイスを編集します。

ステップ 2 [インターフェイス (Interfaces)] で、[インターフェイスの追加 (Add Interfaces)] > [ブリッジグループインターフェイス (Bridge Group Interface)] を選択します。

a) BVI-G の次の詳細情報を入力します。

- [名前 (Name)] : この例では、「BVI-G」。
- [ブリッジグループID (Bridge Group ID)] : この例では、「1」。
- [利用可能なインターフェイス (Available Interface)] : インターフェイスを選択します。
- [IPv4] で、[IP Type] として [Use Static IP] を選択します。
- [IPアドレス (IP Address)] : 「10.10.10.5/24」と入力します。

Add Bridge Group Interface

Interfaces IPv4 IPv6

Name:
BVI-G

Description:

Bridge Group ID *:
1
(1 - 250)

Available Interfaces

- GigabitEthernet0/0
- GigabitEthernet0/1
- GigabitEthernet0/2**
- GigabitEthernet0/3
- GigabitEthernet0/4
- GigabitEthernet0/5

Add

Selected Interfaces

- GigabitEthernet0/1
- GigabitEthernet0/2

Cancel OK

- b) [OK] をクリックします。
- c) **【保存 (Save)** をクリックします。
- a) BVI-B の次の詳細情報を入力します。
- [名前 (Name)] : この例では、「BVI-B」。
 - [ブリッジグループID (Bridge Group ID)] : この例では、「2」。
 - [利用可能なインターフェイス (Available Interface)] : サブインターフェイスを選択します。
 - [IPv4] で、[IP Type] として [Use Static IP] を選択します。
 - [IPアドレス (IP Address)] : 2つのインターフェイスが重複する IP アドレスを持つことをシステムが許可しないため、このフィールドは空のままにします。仮想ルータで IP アドレスを調整した後に、ブリッジグループに再度アクセスし、同じ IP アドレスを指定することができます。

- b) [OK] をクリックします。
- c) [保存 (Save)] をクリックします。

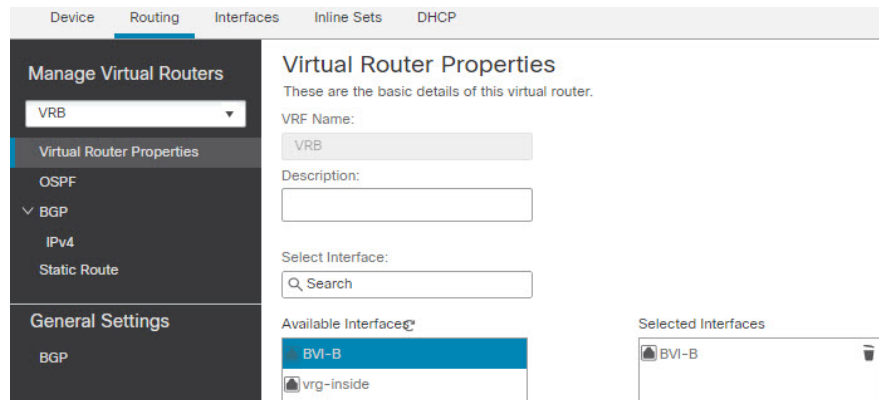
ステップ 3 仮想ルータ (VRG) を作成し、そのネットワークとして BVI-G を選択します。

- a) [デバイス (Devices)] > [デバイス管理 (Device Management)] の順に選択します。
- b) デバイスを編集し、[ルーティング (Routing)] > [仮想ルータの管理 (Manage Virtual Routers)] を選択します。
- c) [仮想ルータの追加 (Add Virtual Router)] をクリックします。仮想ルータの名前を入力し、[OK] をクリックします。
- d) [仮想ルーティングのプロパティ (Virtual Routing Properties)] で、[BVI-G] を選択し、[追加 (Add)] をクリックします。

- e) [保存 (Save)] をクリックします。

ステップ4 仮想ルータ（VRB）を作成し、そのネットワークとして BVI-B を選択します。

- [デバイス（Devices）]>[デバイス管理（Device Management）]の順に選択します。
- デバイスを編集し、[ルーティング（Routing）]>[仮想ルータの管理（Manage Virtual Routers）]を選択します。
- [仮想ルータの追加（Add Virtual Router）]をクリックします。仮想ルータの名前を入力し、[OK]をクリックします。
- [仮想ルーティングのプロパティ（Virtual Routing Properties）]で、[BVI-B]を選択し、[追加（Add）]をクリックします。



- [保存（Save）]をクリックします。

ステップ5 BVI-B の設定に再度アクセスします。

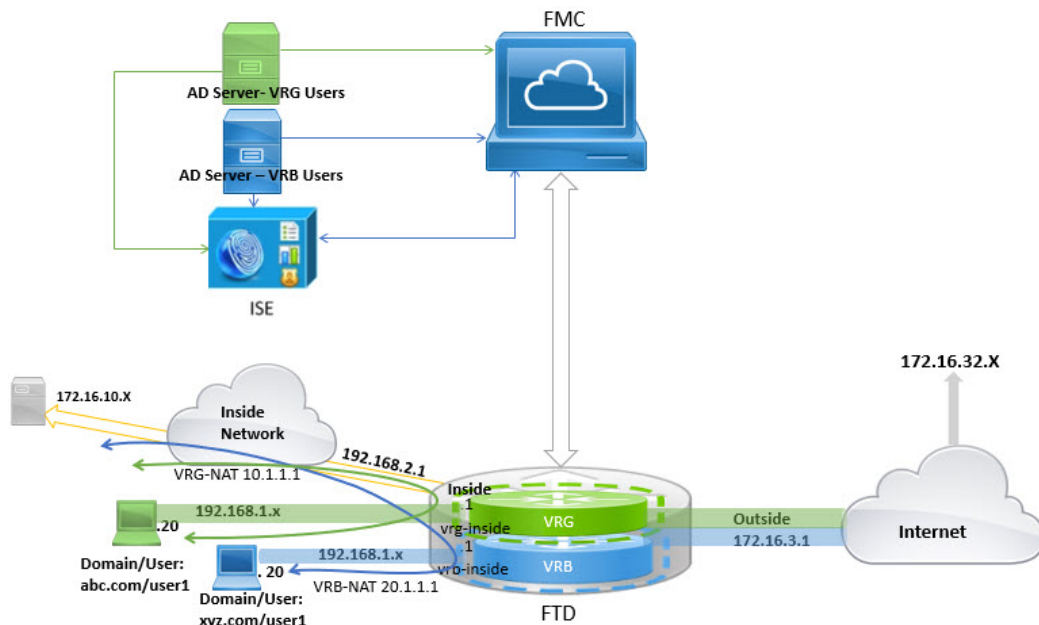
- [Devices]>[Device Management]>[Interfaces]の順に選択します。
- BVI-B インターフェイスに対して[編集（Edit）]をクリックします。IP アドレスを「10.10.10.5/24」と指定します。インターフェイスが2つの異なる仮想ルータに個別に割り当てられたため、BVI-G に同じ IP アドレスを設定できるようになりました。
- [OK]をクリックします。
- [保存（Save）]をクリックします。

BVI間通信を有効にする場合は、外部ルータをデフォルトゲートウェイとして使用します。この例のような重複 BVI のシナリオでは、Twice NAT 外部ルータをゲートウェイとして使用して、BVI 間トラフィックを確立します。ブリッジグループのメンバーに NAT を設定するには、メンバー インターフェイスを指定します。NAT をブリッジグループ インターフェイス（BVI）自体に設定することはできません。ブリッジグループメンバーのインターフェイス間で NAT を実行するときには、実際のおよびマッピングされたアドレスを指定する必要があります。インターフェイスとして「任意」を指定することはできません。

重複するネットワークを使用したユーザー認証の設定方法

仮想ルーティングでは、IP が重複し、ユーザーが重複する複数の仮想ルータを構成できます。この例では、VRG と VRB は、IP（192.168.1.1/24）が重複している仮想ルータです。2つの異なるドメインのユーザーは、重複するネットワーク IP（192.168.1.20）にも存在します。VRG

および VRB ユーザーが共有サーバー 172.16.10.X にアクセスする場合、ルートはグローバル仮想ルータにリークされます。送信元 NAT を使用して、重複する IP を処理します。VRG および VRB ユーザーからのアクセスを制御するには、Management Center でユーザー認証を設定する必要があります。Management Center では、レルム、Active Directory、アイデンティティソース、アイデンティティルールとポリシーを使用して、ユーザー ID が認証されます。Threat Defense にはユーザーの認証に関する直接的な役割がないため、ユーザーアクセスはアクセスコントロールポリシーを通じてのみ管理されます。重複するユーザーからのトラフィックを制御するには、ID ポリシーとルールを使用してアクセスコントロールポリシーを作成します。



始める前に

この例では、次のことを前提としています。

- VRG および VRB ユーザー用の 2 つの AD サーバーがある。
- ISE に 2 つの AD サーバーが追加されている。

手順

ステップ 1 VRG のデバイスの内部インターフェイスを設定します。

- [Devices] > [Device Management] > [Interfaces] の順に選択します。
- VRG に割り当てるインターフェイスを編集します。
 - [名前 (Name)] : この例では、VRG-inside。
 - [Enabled] チェックボックスをオンにします。
 - [IPv4] で、[IP Type] として [Use Static IP] を選択します。

- [IPアドレス (IP Address)] : 192.168.1.1/24 を入力します。

- c) [OK] をクリックします。
- d) [保存 (Save)] をクリックします。

ステップ 2 VRB のデバイスの内部インターフェイスを設定します。

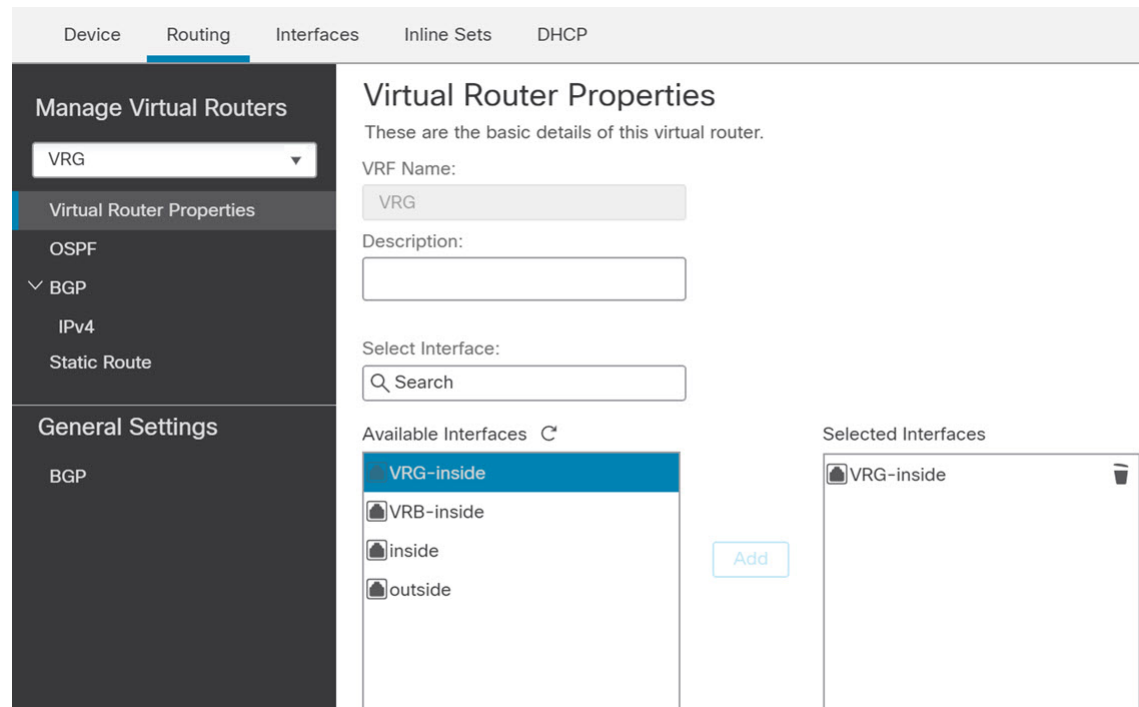
- a) [Devices] > [Device Management] > [Interfaces] の順に選択します。
- b) VRB に割り当てるインターフェイスを編集します。

- [名前 (Name)] : この例では、VRB-inside。
- [Enabled] チェックボックスをオンにします。
- [IPv4] で、[IP Type] として [Use Static IP] を選択します。
- [IP Address] : 空白のままにします。ユーザー定義の仮想ルータをまだ作成していないため、ユーザーは同じ IP アドレスを使用してインターフェイスを設定できません。

- c) [OK] をクリックします。
- d) [保存 (Save)] をクリックします。

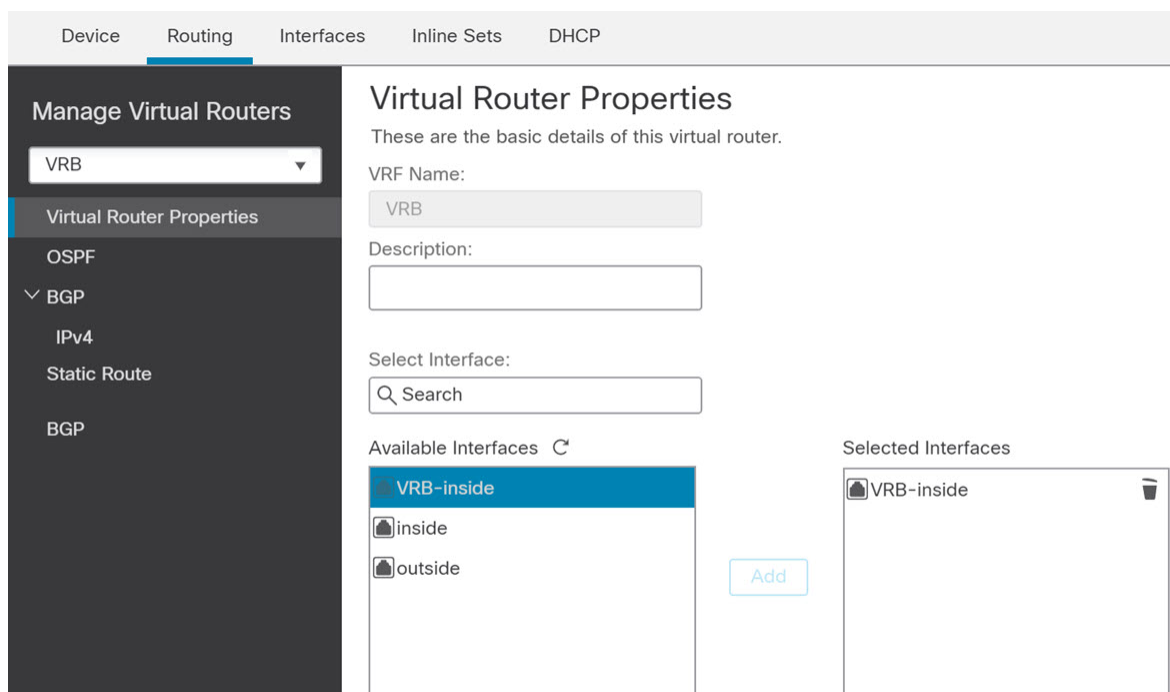
ステップ 3 VRG ユーザーが共通サーバー 172.16.10.1 にアクセスするためのグローバルルータの内部インターフェイスに対する VRG および静的デフォルトルートリークを設定します。

- a) [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択し、Threat Defense デバイスを編集します。
- b) [ルーティング (Routing)] > [仮想ルータの管理 (Manage Virtual Routers)] の順に選択します。[仮想ルータの追加 (Add Virtual Router)] をクリックして、VRG を作成します。
- c) VRG の場合、[仮想ルータのプロパティ (Virtual Router Properties)] で、VRG-inside を割り当てて保存します。



- d) [Static Route] をクリックします。
- e) [ルートを追加 (Add Route)] をクリックします。[Add Static Route Configuration] で、次の項目を指定します。
 - [インターフェイス (Interface)] : グローバルルータの内部インターフェイスを選択します。
 - [ネットワーク (Network)] : any-ipv4 オブジェクトを選択します。
 - [Gateway] : 空白のままにします。別の仮想ルータにルートをリークする場合は、ゲートウェイを選択しません。
- f) [OK] をクリックします。
- g) [保存 (Save)] をクリックします。

- ステップ 4** VRB ユーザーが共有サーバー 172.16.10.x にアクセスするためのグローバルルータの内部インターフェイスに対する VRB および静的デフォルトルートリークを設定します。
- a) [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択し、Threat Defense デバイスを編集します。
 - b) [ルーティング (Routing)] > [仮想ルータの管理 (Manage Virtual Routers)] の順に選択します。[仮想ルータの追加 (Add Virtual Router)] をクリックして、VRB を作成します。
 - c) VRB の場合、[仮想ルータのプロパティ (Virtual Router Properties)] で、VRB-inside を割り当てて保存します。



- d) [Static Route] をクリックします。
- e) [ルートを追加 (Add Route)] をクリックします。[Add Static Route Configuration] で、次の項目を指定します。
 - [インターフェイス (Interface)] : グローバルルータの内部インターフェイスを選択します。
 - [ネットワーク (Network)] : any-ipv4 オブジェクトを選択します。
 - [Gateway] : 空白のままにします。別の仮想ルータにルートをリークする場合は、ゲートウェイを選択しません。
- f) [OK] をクリックします。
- g) [保存 (Save)] をクリックします。

ステップ 5 VRB-inside インターフェイスの設定を再確認します。

- a) [Devices] > [Device Management] > [Interfaces] の順に選択します。
- b) VRB-inside インターフェイスに対して [編集 (Edit)] をクリックします。IP アドレスを 192.168.1.1/24 として指定します。インターフェイスが2つの異なる仮想ルータに個別に割り当てられたため、VR-inside に同じ IP アドレスを設定できるようになりました。
- c) [OK] をクリックします。
- d) [保存 (Save)] をクリックします。

ステップ 6 ソースオブジェクト VRG および VRB の NAT ルールを追加します。[デバイス (Devices)] > [NAT] をクリックします。

ステップ 7 [新しいポリシー (New Policy)] > [Threat Defense NAT] をクリックします。

- ステップ 8** NAT ポリシー名を入力し、Threat Defense デバイスを選択します。[保存 (Save)] をクリックします。
- ステップ 9** [NAT] ページで、[ルールを追加 (Add Rule)] をクリックし、VRG の次の送信元 NAT を定義します。
- [NATルール (NAT Rule)] : [手動NATルール (Manual NAT Rule)] を選択します。
 - [タイプ (Type)] : [静的 (Static)] を選択します。
 - [挿入 (Insert)] : NAT ルールが存在する場合は [前述 (Above)] を選択します。
 - [Enabled] をクリックします。
 - [インターフェイス オブジェクト (Interface Objects)] で、VRG-Inside オブジェクトを選択し、[ソースに追加 (Add to Source)] をクリックします (オブジェクトがない場合は、[オブジェクト (Object)] > [オブジェクト管理 (Object Management)] > [インターフェイス (Interface)] でオブジェクトを作成します)。次に、Global-Inside オブジェクトを選択して [宛先に追加 (Add to Destination)] をクリックします。
 - [変換 (Translation)] で、以下を選択します。
 - [元の送信元 (Original Source)] で VRG-Users を選択します。
 - [変換済み送信元 (Translated Source)] で、[追加 (Add)] をクリックし、10.1.1.1 を指定してオブジェクト VRG-NAT を定義します。次の図に示されているように、VRG-NAT を選択します。

Add NAT Rule

NAT Rule:
Manual NAT Rule

Insert:
In Category NAT Rules Before

Type:
Static

Enable

Description:

Interface Objects Translation PAT Pool Advanced

Original Packet	Translated Packet
Original Source:* VRG-Users +	Translated Source: Address
Original Destination: Address +	Translated Destination: VRG-NAT +
Original Source Port:	Translated Source Port:

Cancel OK

ステップ 10 [OK] をクリックします。

ステップ 11 [NAT] ページで、[ルールを追加 (Add Rule)] をクリックし、VRB の次の送信元 NAT を定義します。

- [NATルール (NAT Rule)] : [手動NATルール (Manual NAT Rule)] を選択します。
- [タイプ (Type)] : [静的 (Static)] を選択します。
- [挿入 (Insert)] : NAT ルールが存在する場合は [前述 (Above)] を選択します。
- [Enabled] をクリックします。
- [インターフェイス オブジェクト (Interface Objects)] で、VRB-Inside オブジェクトを選択し、[ソースに追加 (Add to Source)] をクリックします (オブジェクトがない場合は、[オブジェクト (Object)] > [オブジェクト管理 (Object Management)] > [インターフェイス (Interface)] でオブジェクトを作成します)。次に、Global-Inside オブジェクトを選択して [宛先に追加 (Add to Destination)] をクリックします。
- [変換 (Translation)] で、以下を選択します。
 - [元の送信元 (Original Source)] で VRG-Users を選択します。

- [変換済み送信元 (Translated Source)] で、[追加 (Add)] をクリックし、20.1.1.1 を指定してオブジェクト VRB-NAT を定義します。次の図に示されているように、VRB-NAT を選択します。

Add NAT Rule

NAT Rule:
Manual NAT Rule

Insert:
In Category NAT Rules Before

Type:
Static

Enable
Description:

Interface Objects Translation PAT Pool Advanced

Original Packet	Translated Packet
Original Source:* VRB-Users +	Translated Source: Address
Original Destination: Address +	VRB-NAT +
Original Source Port: 	Translated Destination: +
Translated Source Port: 	

Cancel OK

ステップ12 [保存 (Save)] をクリックします。

NAT ルールは次のようになります。

Rules						
Filter by Device						
#	Direction	Type	Source Interface	Destination Interface	Original Sources	Original Packet Destinations
NAT Rules Before						
1		St...	any	any	VRG-Users	
2		St...	any	any	VRB-Users	
Auto NAT Rules						

- ステップ 13** Management Center に 2 つの一意的 AD サーバー（VRG および VRB ユーザーごとに 1 つ）を追加します（[システム（System）]>[統合（Integration）]>[レルム（Realms）]を選択します）。
- ステップ 14** [新しいレルム（New Realm）]をクリックして、フィールドに入力します。各フィールドの詳細については、[レルム フィールド](#)を参照してください。
- ステップ 15** VRG および VRB ユーザーからのアクセスを制御するには、2 つの Active Directory を定義します。[\[レルムディレクトリ（Realm Directory）\]](#)および[\[同期（Synchronize）\]](#)フィールドを参照 [LDAP レルム](#)または[Active Directory レルム](#)および[レルムディレクトリの作成](#)を参照してください。
- ステップ 16** Management Center に ISE を追加します（[システム（System）]>[統合（Integration）]>[アイデンティティソース（Identity Sources）]を選択）。
- ステップ 17** [Identity Services Engine] をクリックして、フィールドに入力します。各フィールドの詳細については、[レルムを使用したユーザー制御用 ISE/ISE-PIC の設定方法](#)を参照してください。
- ステップ 18** ID ポリシーとルールを作成し、VRG および VRB からの重複するユーザーのアクセスを制御するためのアクセス コントロール ポリシーを定義します。

BGP を使用して仮想ルータを相互接続する方法

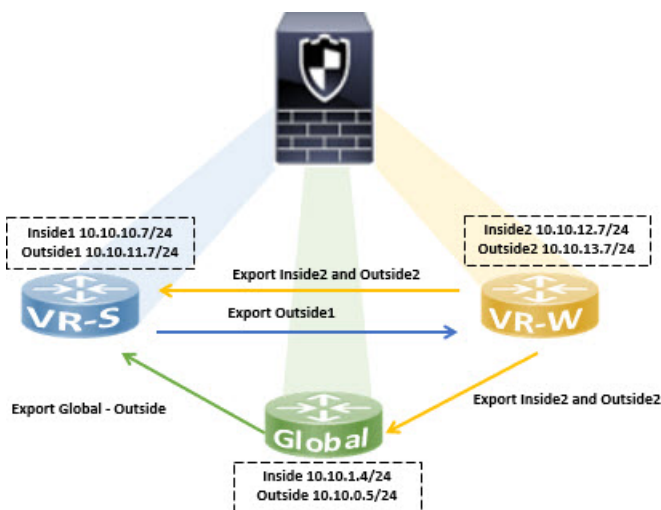
デバイスで BGP 設定を構成して、仮想ルータ（グローバルおよびユーザー定義の仮想ルータ）間のルートをリークできるようになりました。送信元仮想ルータのルートターゲットは BGP テーブルにエクスポートされ、次に宛先の仮想ルータにインポートされます。ルートマップは、グローバル仮想ルートをユーザー定義の仮想ルータと共有するために使用することも、その逆も可能です。BGP テーブルへのルートのインポートまたはエクスポートはすべて、グローバル仮想ルートを含む、ユーザー定義の仮想ルータで構成されることに注意してください。

工場のファイアウォールデバイスが次の仮想ルータとインターフェイスで構成されているとします。

- グローバル仮想ルータは Inside (10.10.1.4/24) および Outside (10.10.0.5/24) で構成されます。
- VR-S (営業) 仮想ルータは Inside1 (10.10.10.7/24) および Outside1 (10.10.11.7/24) で構成されます。
- VR-W (倉庫) 仮想ルータは Inside2 (10.10.12.7/24) および Outside2 (10.10.13.7/24) で構成されます。

倉庫 (VR-W) のルートを営業 (VR-S) とグローバルを使用してリークし、VR-S の外部インターフェイスルートを VR-W にリークするとします。同様に、グローバルルータの外部インターフェイスルートを営業 (VR-S) にリークする必要があります。この例では、ルータの相互接続を実現するための BGP 構成手順を示しています。

図 3: BGP を使用した仮想ルータの相互接続



始める前に

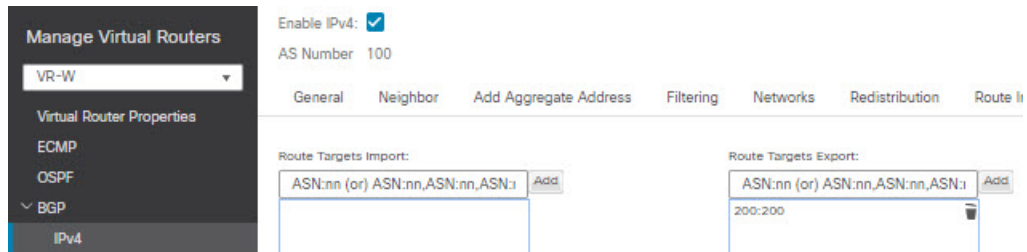
- **仮想ルータの作成** : VR-S および VR-W。
- BGP を有効にし、各仮想ルータで**接続されたルートの再配布用に BGP を構成**します。

手順

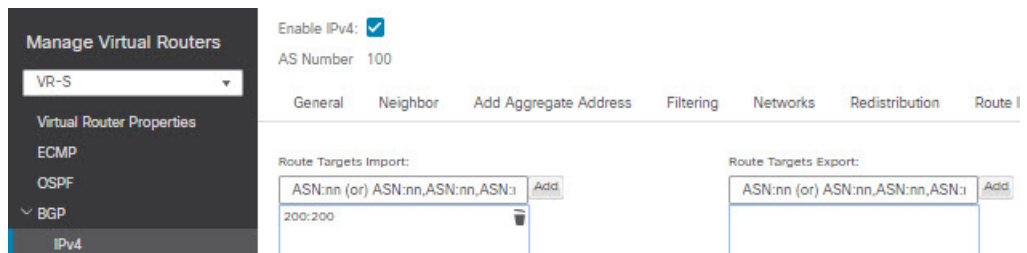
ステップ 1 ルートターゲットでタグ付けされたルートを VR-S にエクスポートするように VR-W を構成します。

- a) **[デバイス (Devices)] > [デバイス管理 (Device Management)]** を選択し、デバイスを編集して **[ルーティング (Routing)]** タブをクリックします。
- b) 仮想ルータのドロップダウンから、**VR-W** を選択します。
- c) **[BGP] > [IPv4] > [ルートのインポート/エクスポート (Route Import/Export)]** をクリックします。

- d) VR-W ルートを VR-S にリークするには、ルートにルートターゲットのタグを付けます。これにより、VR-W ルートは、ルートターゲットとマークされた BGP テーブルにエクスポートされます。[ルートターゲットのエクスポート (Route Targets Export)] フィールドに、200:200 などの値を入力します。[追加 (Add)] をクリックします。



- e) 仮想ルータのドロップダウンから、VR-S を選択します。
- f) [BGP] > [IPv4] > [ルートのインポート/エクスポート (Route Import/Export)] をクリックします。
- g) VR-W からリークされたルートを受け取るには、ルートターゲットのインポートを構成して、(ピアまたは再配布された) BGP テーブルから、ルートターゲットとマークされた VR-W ルートをインポートします。[ルートターゲットのインポート (Route Targets Import)] フィールドに、VR-W に設定したのと同じルートターゲット値 (200:200) を入力します。[Add] をクリックします。



- (注) VR-W からリークされるルートを条件付きにする場合は、ルートマップオブジェクトで一致基準を指定し、[ユーザー仮想ルータのエクスポートルートマップ (User Virtual Router Export Route Map)] でそれを選択できます。同様に、BGP テーブルから VR-S にインポートするルートを条件付きにする場合は、[ユーザー仮想ルータのインポートルートマップ (User Virtual Router Import Route Map)] を使用できます。この手順については、ステップ 3 で説明します。

ステップ 2 ルートをグローバル仮想ルータにエクスポートするように VR-W を構成します。

- a) VR-W ルートをグローバルルーティングテーブルにエクスポートできるようにするルートマップを作成する必要があります。[オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] > [ルートマップ (Route Map)] を選択します。
- b) [ルートマップの追加 (Add Route Map)] をクリックし、*Export-to-Global* などの名前を付けて、[追加 (Add)] をクリックします。
- c) [シーケンス番号 (Sequence Number)] (1 など) を指定し、[再配布 (Redistribution)] ドロップダウンリストから [許可 (Allow)] を選択します。

New Route Map Object

Name
Export-to-Global

Entries (1)

Sequence No ▲	Redistribution
1	Allow

Allow Overrides

Cancel Save

d) [保存 (Save)]をクリックします。

この例では、すべての VR-W ルートがグローバルルーティング テーブルにリークされます。したがって、ルートマップには一致基準が設定されません。

e) デバイスの [ルーティング (Routing)] タブに移動し、VR-W を選択します。[BGP]>[IPv4]>[ルートのインポート/エクスポート (Route Import/Export)] をクリックします。

f) [グローバル仮想ルータのエクスポートルートマップ (Global Virtual Router Export Route Map)] ドロップダウンリストから、[Export-to-Global] を選択します。

Enable IPv4:

AS Number: 100

General Neighbor Add Aggregate Address Filtering Networks Redistribution Rout

Route Targets Import:

ASN:nn (or) ASN:nn,ASN:nn,ASN:nn Add

Route Targets Export:

ASN:nn (or) ASN:nn,ASN:nn,ASN:nn Add

200:200

User Virtual Router

Import Route Map: --select--

Global Virtual Router

Import Route Map: --select--

User Virtual Router

Export Route Map: --select--

Global Virtual Router

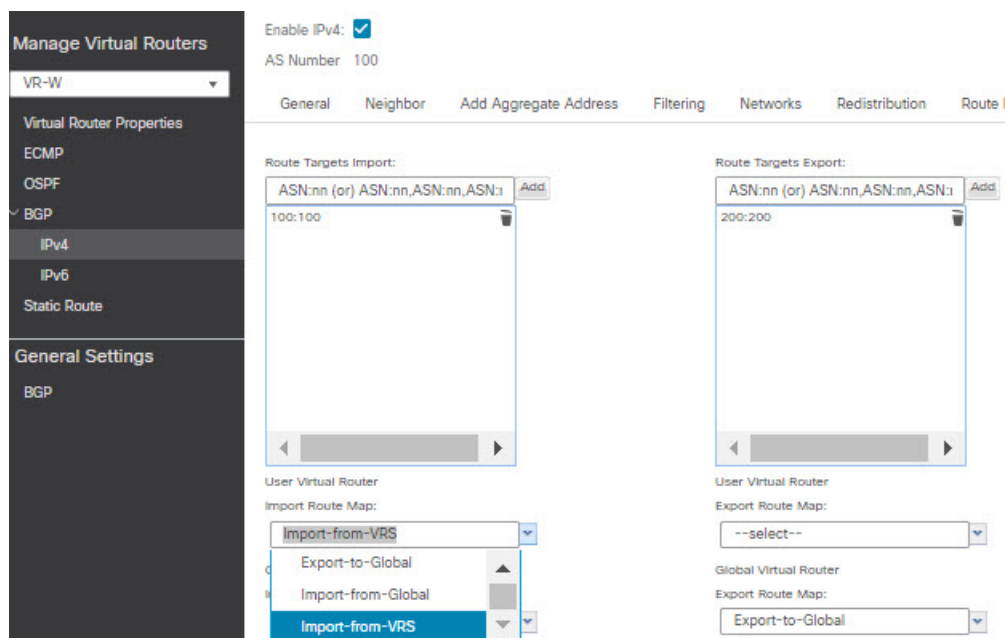
Export Route Map: Export-to-Global

Export-to-Global

ステップ 3 VR-S の Outside1 ルートのみを VR-W にリークするには :

a) 仮想ルータのドロップダウンから、VR-S を選択します。

- b) **[BGP]>[IPv4]>[ルートのインポート/エクスポート (Route Import/Export)]** をクリックします。
- c) VR-S ルートを VR-W にリークするには、ルートにルートターゲットのタグを付けます。これにより、VR-S ルートは、ルートターゲットとマークされた BGP テーブルにエクスポートされます。**[ルートターゲットのエクスポート (Route Targets Export)]** フィールドに、*100:100* などの値を入力します。**[Add]** をクリックします。
- d) 仮想ルータのドロップダウンから **[VR-W]** を選択し、**[BGP]>[IPv4]>[ルートのインポート/エクスポート (Route Import/Export)]** を選択します。
- e) VR-S からリークされたルートを受け取るには、ルートターゲットのインポートを構成して、(ピアまたは再配布された) BGP テーブルから、ルートターゲットとマークされた VR-S ルートをインポートします。**[ルートターゲットのエクスポート (Route Targets Export)]** フィールドに、VR-S のルートターゲットの値 (*100:100*) を入力します。**[Add]** をクリックします。
- f) ここで、VR-S の **Outside1** ルートのみが VR-W にリークされることを条件付ける必要があります。**[オブジェクト (Objects)]>[オブジェクト管理 (Object Management)]>[プレフィックスリスト (Prefix List)]>[IPv4プレフィックスリスト (IPv4 Prefix List)]** を選択します。
- g) **[IPv4プレフィックスリストの追加 (Add IPv4 Prefix List)]** をクリックし、**VRS-Outside1-Only** などの名前を付けて、**[追加 (Add)]** をクリックします。
- h) **[シーケンス番号 (Sequence Number)]** (1 など) を指定し、**[再配布 (Redistribution)]** ドロップダウンリストから **[許可 (Allow)]** を選択します。
- i) VR-S **Outside1** インターフェイスの IP アドレス (最初の 2 オクテット) を入力します。
- j) **[保存 (Save)]** をクリックします。
- k) プレフィックスリストを含む **match** 句を使用してルートマップを作成します。**[ルートマップ (Route Map)]** をクリックします。**[ルートマップの追加 (Add Route Map)]** をクリックし、**Import-from-VRS** などの名前を付けて、**[追加 (Add)]** をクリックします。
- l) **[シーケンス番号 (Sequence Number)]** (1 など) を指定し、**[再配布 (Redistribution)]** ドロップダウンリストから **[許可 (Allow)]** を選択します。
- m) **[match 句 (Match Clause)]** タブで **[IPv4]** をクリックします。**[アドレス (Address)]** タブで、**[プレフィックスリスト (Prefix List)]** をクリックします。
- n) **[利用可能な IPv4 プレフィックスリスト (Available IPv4 Prefix List)]** で、**[VRS-Outside1-Only]** を選択し、**[追加 (Add)]** をクリックします。
- o) **[保存 (Save)]** をクリックします。
- p) デバイスの **[ルーティング (Routing)]** タブに移動し、**VR-W** を選択します。**[BGP]>[IPv4]>[ルートのインポート/エクスポート (Route Import/Export)]** をクリックします。
- q) **[グローバル仮想ルータのインポートルートマップ (Global Virtual Router Import Route Map)]** ドロップダウンリストから、**[Import-from-VRS]** を選択します。



ステップ 4 グローバル仮想ルータの Outside ルートをインポートするように VR-S を構成します。

(注) グローバル仮想ルータとの間でルートをリークするには、送信元または宛先のユーザー定義仮想ルータをそれぞれ構成する必要があります。したがって、この例では、VR-S は、グローバル仮想ルータの Outside インターフェイスからルートをインポートする宛先ルータとなります。

- a) [オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] > [プレフィックスリスト (Prefix List)] > [IPv4プレフィックスリスト (IPv4 Prefix List)] を選択します。
- b) [IPv4プレフィックスリストの追加 (Add IPv4 Prefix List)] をクリックし、*Global-Outside-Only* などの名前を付けて、[追加 (Add)] をクリックします。
- c) [シーケンス番号 (Sequence Number)] (1 など) を指定し、[再配布 (Redistribution)] ドロップダウンリストから [許可 (Allow)] を選択します。
- d) グローバル Outside インターフェイスの IP アドレス (最初の 2 オクテット) を入力します。

Add Prefix List Entry

Action:

Sequence No:

Range: 1-4294967295

IP Addresses: (Limit 250) Address:

Format: ipaddr/len (len<=32)

Min Prefix Length:

Range: 1 - 32

Max Prefix Length:

Range: 1 - 32

- e) [保存 (Save)] をクリックします。
- f) [ルートマップ (Route Map)] をクリックします。[ルートマップの追加 (Add Route Map)] をクリックし、*Import-from-Global* などの名前を付けて、[追加 (Add)] をクリックします。
- g) [シーケンス番号 (Sequence Number)] (1 など) を指定し、[再配布 (Redistribution)] ドロップダウンリストから [許可 (Allow)] を選択します。
- h) [match 句 (Match Clause)] タブで [IPv4] をクリックします。[アドレス (Address)] タブで、[プレフィックスリスト (Prefix List)] をクリックします。
- i) [利用可能なIPv4プレフィックスリスト (Available IPv4 Prefix List)] で、[Global-Outside-Only] を選択し、[追加 (Add)] をクリックします。

Add Route Map Entry

Sequence No:

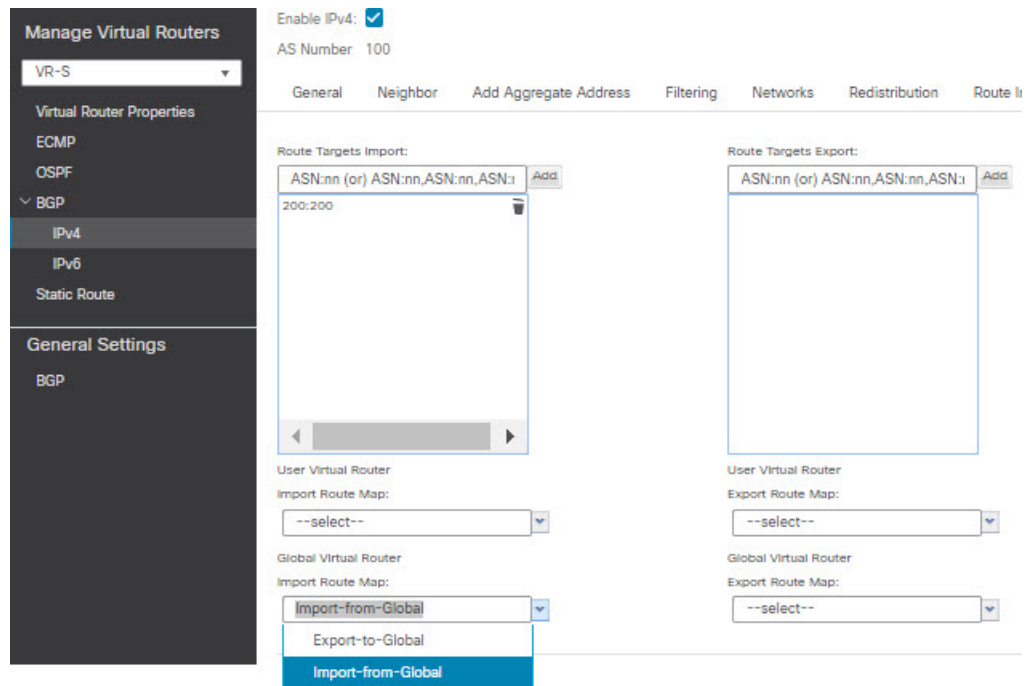
Redistribution:

Match Clauses Set Clauses

Security Zones	Address (2)	Next Hop (0)	Route Source (0)
IPv4	Select addresses to match as access list or prefix list addresses of route.		
IPv6	<input type="radio"/> Access List <input checked="" type="radio"/> Prefix List		
BGP	Available Access Lists:		
Others	<input type="text" value="Standard"/>		
	Available IPv4 Prefix List		Selected IPv4 Prefix List
	<input type="text" value="Q Search"/>		<input type="text" value="Global-Outside-Only"/>
	<input type="button" value="Add"/>		<input type="button" value="Add"/>

- j) [保存 (Save)] をクリックします。
- k) デバイスの [ルーティング (Routing)] タブに移動し、VR-S を選択します。[BGP] > [IPv4] > [ルートのインポート/エクスポート (Route Import/Export)] をクリックします。

- 1) [グローバル仮想ルータのインポートルートマップ (Global Virtual Router Import Route Map)] ドロップダウンリストから、[Import-from-Global] を選択します。



ステップ 5 [保存 (Save)]、[展開 (Deploy)] の順にクリックします。

仮想ルータの履歴

機能	最小 Management Center	最小 Threat Defense	詳細
ダイナミック VTI による仮想ルーティング	Management Center : 7.4 Threat Defense : 7.4	任意 (Any)	ルートベースのサイト間 VPN にダイナミック VTI を使用して仮想ルータを設定できるようになりました。 新規/変更された画面 : [使用可能なインターフェイス (Available Interfaces)] の下の [デバイス (Devices)] > [デバイス管理 (Device Management)] > [デバイスの編集 (Edit Device)] > [ルーティング (Routing)] > [仮想ルータのプロパティ (Virtual Router Properties)] > [ダイナミック VTI インターフェイス (Dynamic VTI interfaces)]。
ISA 3000 の仮想ルータサポート	7.0	任意 (Any)	ISA 3000 デバイスには最大 10 の仮想ルータを設定できます。 新規/変更された画面 : なし

機能	最小 Management Center	最小 Threat Defense	詳細
Snort 3 対応デバイスの仮想ルータ	7.0	任意 (Any)	Snort 3 対応デバイスで仮想ルータ機能がサポートされるようになりました。したがって、Snort 3 エンジンに切り替える前に、仮想ルータから Snort 2 デバイスを削除する必要はありません。 新規/変更された画面：なし
ユーザー定義の仮想ルータでの SNMP サポート	7.0	任意 (Any)	Secure Firewall Threat Defense は、ユーザー定義の仮想ルータでの SNMP の設定をサポートするようになりました。 新規/変更された画面：なし
仮想ルータの一括削除	6.7	任意 (Any)	一度に複数の仮想ルータを Secure Firewall Threat Defense から削除できます。 新規/変更された画面：[デバイス (Devices)]>[デバイス管理 (Device Management)]>[ルーティング (Routing)]>[仮想ルータの管理 (Manage Virtual Router)]ページ。
Secure Firewall Threat Defense の仮想ルータ	6.6	任意 (Any)	Secure Firewall Threat Defense の仮想ルータが導入されました。 新規/変更された画面：[デバイス (Devices)]>[デバイス管理 (Device Management)]>[ルーティング (Routing)]ページで仮想ルータを作成し、仮想ルータに Threat Defense インターフェイスを割り当てることができます。 サポートされているプラットフォーム：Secure Firewall Threat Defense

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。