



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 Route 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 (8 ページ)
- 仮想ルータの要件と前提条件 (9 ページ)
- 仮想ルータに関する注意事項と制限事項 (10 ページ)
- Firewall Management Center Web インターフェイスの変更 : [ルーティング (Routing)] ページ (12 ページ)
- 仮想ルータの管理 (13 ページ)
- 仮想ルータの作成 (13 ページ)
- 仮想ルータのモニタリング (17 ページ)
- 仮想ルータの設定例 (18 ページ)
- 仮想ルータの履歴 (60 ページ)

仮想ルータと Virtual Route 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、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によって、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。

仮想ルータは、Virtual Routing and Forwarding の「軽量」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することができます。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

■ 仮想ルータの適用

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なります。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き、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のものになります。

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 Firewall 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）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、Firewall 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きます。

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（ボックス内のトライフィック）。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している必要があります。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サーバのインターフェイスとして**any**を指定すると、システムはグローバル仮想ルータのインターフェイスだけを考慮します。
- AAAサーバまたはアイデンティティレム（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。
- SYSLOGサーバ。

仮想ルーター対応ポリシーの設定

仮想ルーターを作成する場合、その仮想ルーターのルーティングテーブルは、グローバル仮想ルーターまたは他の仮想ルーター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ー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ーのすべてのインターフェイスに適用されます。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ーにのみポリシーを適用する必要がある場合は、その1つの仮想ルーター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、仮想ルーター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つの仮想ルーター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ー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、ユーザから IP アドレスへのマッピング。仮想ルーターで重複するアドレス空間を使用する場合は、仮想ルーターごとに個別のレルムを作成し、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。

仮想ルーター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ーで 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、両方の仮想ルーター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つの仮想ルーター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。

仮想ルーターの相互接続

スタティックおよびダイナミックルートリーク

仮想ルーター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

仮想ルーター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に流れるようになりますには、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ます、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ディングまたはチェーンをサポートしません。たとえば、Firewall 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

仮想ルータの相互接続

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、トライ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と、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）と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。Firewall 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
- 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 : Firewall 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

■ ユーザー定義の仮想ルータでの SNMP の設定

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. インターフェイスで仮想ルータを設定します。
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重複する IP アドレス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、デバイスマodel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にユーザが定義した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
Firepower 9300 appliance、すべてのモデル	100
Firewall 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

■ 仮想ルータに関する注意事項と制限事項

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することができます。
- 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することができます。
- 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することができます。
- 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ることはできません。
 - 診断インターフェイス。
 - 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。

- ・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、ネットワークトライ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ィング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 Firewall 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500ms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 再コンバージエンスタイマー（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 再コンバージエ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。

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

Firewall Threat Defense 6.6 より前のデバイスと一部のデバイスマネジメント機能でサポートされていません。Firewall 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 Firewall 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、「[サポートされているデバイスマネジメント](#)」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)] (edit icon) または [削除 (Delete)] (trash icon) 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 (search icon) 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、Firewall Threat Defense デバイスを編集します。

ステップ2 [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)

仮想ルータの設定

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

- [仮想ルータを設定します。](#)

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 \(13 ページ\)](#) 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、[Firewall Management Center Web インターフェイスの変更 : \[ルーティング \(Routing\) \] ページ \(12 ページ\)](#) 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て使用できます。[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、[Open Shortest Path First \(OSPF\)](#) 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す。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。

仮想ルータの変更

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

- [仮想ルータを変更します。](#)
- [仮想ルータを削除します。](#)

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、Firewall Threat Defense デバイスを編集します。

ステップ2 [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)] (edit icon) 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](#) (magnifying glass icon) 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

- [仮想ルータを削除します。](#)

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インターフェイスはすべて、グローバル仮想ルータに移動します。
- IPの重複、ルートの競合など、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、Firewall Threat Defense デバイスを編集します。

ステップ2 [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)] (trash bin icon) 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イスの詳細情報が表示されます。

■ 仮想ルータの設定例

- **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。

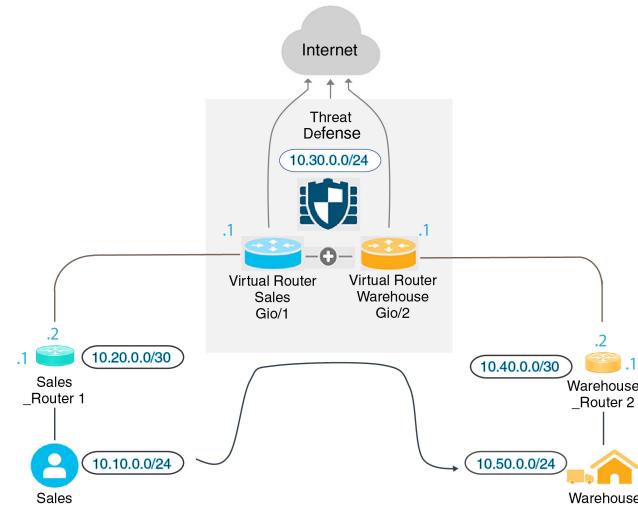
仮想ルータの設定例

仮想ルータを介して遠隔サーバ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、インターフェイ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にアクセスする必要が生じことがあります。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）のインターフェイスへのスタティックルートを設定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) [デバイス (Devices)] > [デバイス管理 (Device Management)] > [インターフェイス (Interfaces)] を選択します。
- b) Gi0/1 インターフェイスを編集します。
 - ・[名前 (Name)] : この例では、VR-Sales です。
 - ・[有効 (Enabled)] チェックボックスをオンにします。
 - ・[IPv4] で、[IPタイプ (IP Type)] として [静的IPを使用する (Use Static IP)] を選択します。
 - ・[IPアドレス (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) [デバイス (Devices)] > [デバイス管理 (Device Management)] > [インターフェイス (Interfaces)] を選択します。
- b) Gi0/2 インターフェイスを編集します。
 - ・[名前 (Name)] : この例では、VR-Warehouse です。
 - ・[有効 (Enabled)] チェックボックスをオンにします。
 - ・[IPv4] で、[IPタイプ (IP Type)] として [静的IPを使用する (Use Static IP)] を選択します。
 - ・[IPアドレス (IP Address)] : 空白のままにします。ユーザ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。

■ 仮想ルータを介して遠隔サーバにルーティングする方法

- a) [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択し、Firewall 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)] を選択します。
- c) [仮想ルータの追加 (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) [仮想ルータの追加 (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 [販売部門 (Sales)] を選択し、[仮想ルータのプロパティ (Virtual Router Properties)] で、[選択したインターフェイス (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 [保管倉庫部門 (Warehouse)] を選択し、[仮想ルータのプロパティ (Virtual Router Properties)] で、[選択したインターフェイス (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) [デバイス (Devices)] > [デバイス管理 (Device Management)] > [インターフェイス (Interfaces)] を選択します。
- b) [VR-Warehouse] インターフェイスに対する [編集 (Edit)] をクリックします。[IPアドレス (IP Address)] に「10.30.0.1/24」を入力します。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 (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) [オブジェクト (Object)] > [オブジェクト管理 (Object Management)] を選択します。
- b) [ネットワークの追加 (Add Network)] > [オブジェクトの追加 (Add Object)] の順に選択します。
 - [名前 (Name)] : この例では、Warehouse-Server です。
 - [ネットワーク (Network)] : [ネットワーク (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) [ネットワークの追加 (Add Network)] > [オブジェクトの追加 (Add Object)] の順に選択します。
 - [名前 (Name)] : この例では、Warehouse-Gateway です。
 - [ネットワーク (Network)] : [ホスト (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、Firewall 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、[スタティックルート (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。[スタティックルート設定の追加 (Add Static Route Configuration)]で、次の項目を指定します。
 - ・[インターフェイス (Interface)] : [VR-Warehouse]を選択します。
 - ・[ネットワーク (Network)] : Warehouse-Server オブジェクトを選択します。
 - ・[ゲートウェイ (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*: VR-Warehouse

Available Network	Selected Network
+ 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	Warehouse-Server

Gateway*: +

Metric: 1
(1 - 254)

Tunneled: (Used only for default Route)

Route Tracking: +

Cancel OK

- [OK]をクリックします。
- [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。

- 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、[スタティックルート (Static Route)]をクリックします。

仮想ルータを介して遠隔サーバにルーティングする方法

- b) [ルートを追加 (Add Route)] をクリックします。[スタティックルート設定の追加 (Add Static Route Configuration)] で、次の項目を指定します。

- ・[インターフェイス (Interface)] : [VR-Warehouse] を選択します。
- ・[ネットワーク (Network)] : Warehouse-Server オブジェクトを選択します。
- ・[ゲートウェイ (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	Selected Network
+ 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	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。
[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)]を使用します。[追加 (Add)]>[セキュリティゾーン (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 ([追加 (Add)]>[インターフェイスグループ (Interface Group)]を選択)。

ステップ9 [ポリシー (Policies)]>[アクセス制御 (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。

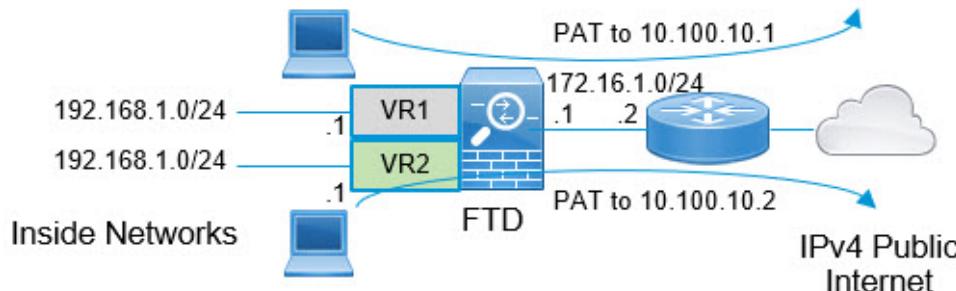
たとえば、Sales のインターフェイスが Sales-Zone セキュリティゾーンにあり、Warehouse のインターフェイスが Warehouse-Zone セキュリティゾーンにある場合、アクセス制御ルールは次のようにになります。

Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applicat...	Source Ports	Dest Ports	URLs	Source SGT	Dest SGT	Action
Warehouse-Rule	Sales-Zone	Warehouse-Zone	Any	10.50.0.5	Any	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、Firewall 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。



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



(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。

- [Devices] > [Device Management] > [Interfaces] の順に選択します。
- 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。
 - [有効 (Enabled)] チェックボックスをオンにします。
 - [IPv4] で、[IP タイプ (IP Type)] として [静的IPを使用する (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。
- [OK] をクリックします。
- [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。

- [Devices] > [Device Management] > [Interfaces] の順に選択します。
- 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。
 - [有効 (Enabled)] チェックボックスをオンにします。
 - [IPv4] で、[IP タイプ (IP Type)] として [静的IPを使用する (Use Static IP)] を選択します。
 - [IP アドレス (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。
- [OK] をクリックします。
- [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、Firewall 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。[スタティックルート設定の追加 (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イ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には、ゲートウェイを指定しません。

■ 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

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
+ <input type="text" value="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	<input type="button" value="Add"/> any-ipv4 

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、Firewall 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。[スタティックルート設定の追加 (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イ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*

Available Network +

Selected Network

Gateway

Metric: 1

Tunneled:

Route Tracking:

Cancel OK

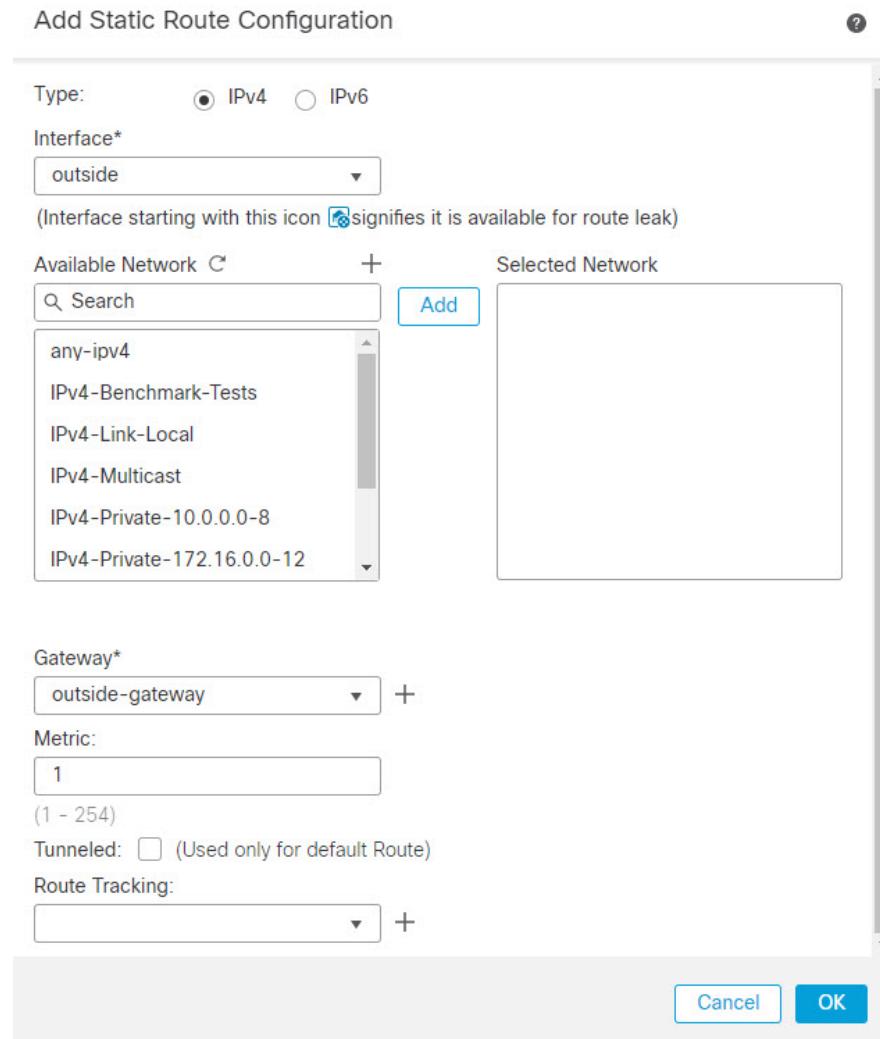
f) [OK] をクリックします。

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。

■ 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

- a) [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択し、Firewall 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。[スタティックルート設定の追加 (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。



- 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。

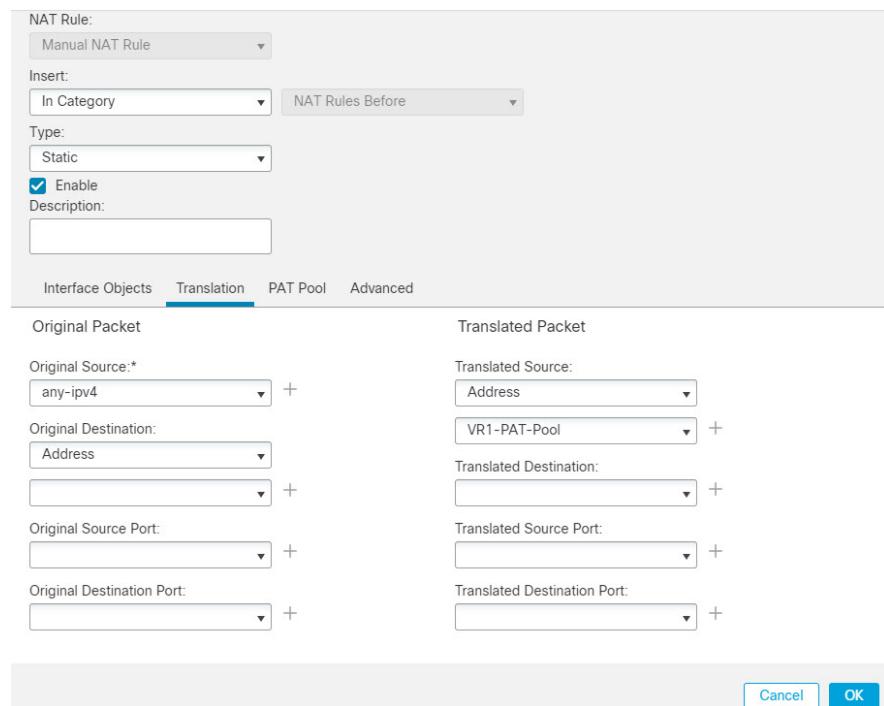
- a) [Devices] > [Device Management] > [Interfaces] の順に選択します。
- b) vr2-inside インターフェイスに対して [編集 (Edit)] をクリックします。IP アドレスを 192.168.1.1/24 として指定します。インターフェイスが 2 つの異なる仮想ルータに個別に割り当てられたため、vr2-inside に同じ IP アドレスを設定できるようになりました。
- c) [OK] をクリックします。
- d) [保存 (Save)] をクリックします。

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。

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

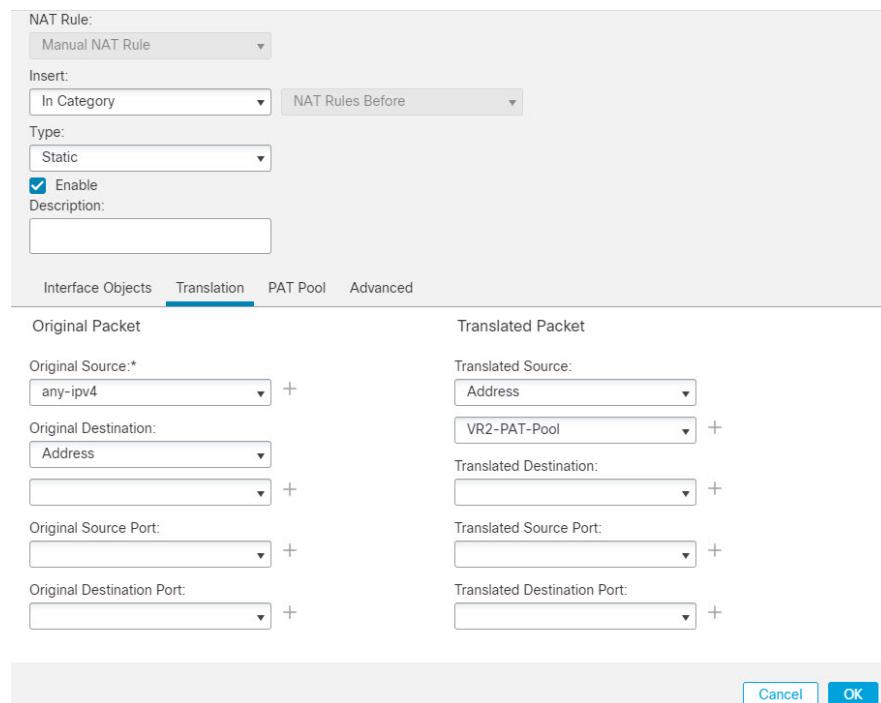
- c) NAT ポリシー名として InsideOutsideNATRule を入力し、Firewall Threat Defense デバイスを選択します。[保存 (Save)] をクリックします。
- d) [InsideOutsideNATRule] ページで、[ルールの追加 (Add Rule)] をクリックして、以下を定義します。
 - [NATルール (NAT Rule)] : [手動NATルール (Manual NAT Rule)] を選択します。
 - [タイプ (Type)] : [ダイナミック (Dynamic)] を選択します。
 - [挿入 (Insert)] : ダイナミック 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。



- 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イフィックの 10.100.10.2 への PAT を実行する NAT ルールを追加します。

- [デバイス (Devices)] > [NAT] の順に選択します。
- 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。



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

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

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イ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 へのトライ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、すべてのトライ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

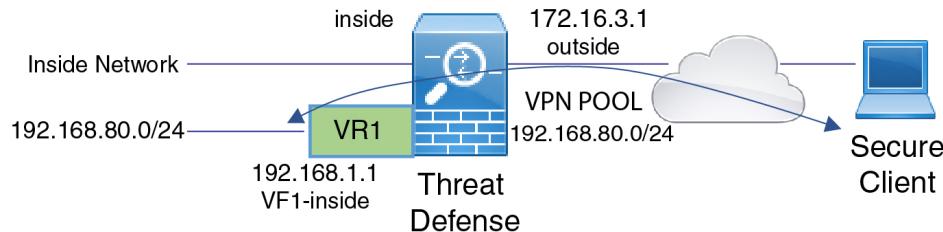
The screenshot shows the 'Add Rule' configuration page. The rule is named 'AllowInternetTraffic', is enabled, and is inserted into the 'Mandatory' list. The action is set to 'Allow'. The source zones selected are 'vr1-inside-zone' and 'vr2-inside-zone', and the destination zone is 'outside-zone'. The 'Time Range' dropdown is empty.

Available Zones		Source Zones (2)	
<input type="text"/> Search by name		vr1-inside-zone vr2-inside-zone <small>outside-zone</small>	
		Add to Source	Add to Destination
<small>outside-zone</small>			

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 Firewall 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。

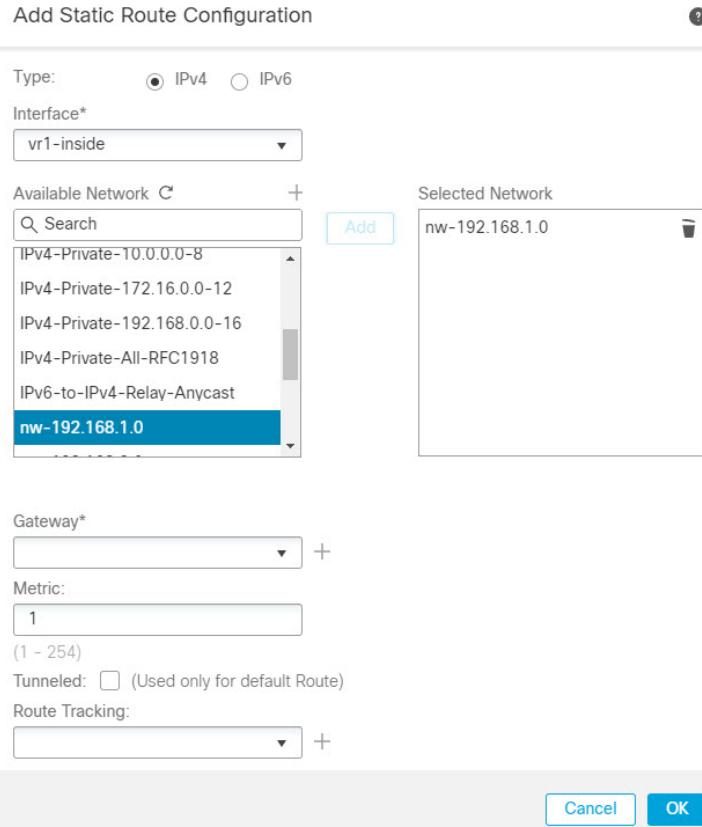
手順

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。

- [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択し、Firewall 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。
- [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。[スタティックルート設定の追加 (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。

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

- [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。



ルートリークにより、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。

- [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、Firewall 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。[スタティックルート設定の追加 (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 C +
 Search
 outside-gateway
vpn-pool
 vr1-inside
 VR1-PAT-Pool
 vr2-inside
 VR2-PAT-Pool

Add 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。

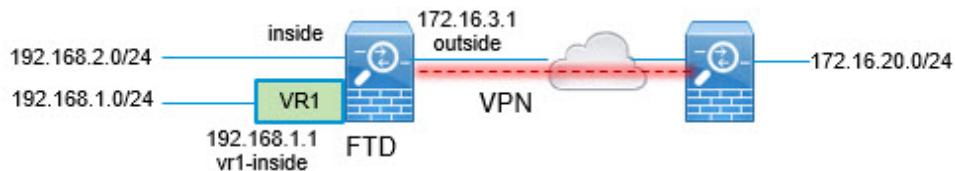
サイト間 VPN における複数の仮想ルータのネットワークからのトラフィックを保護する方法

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

■ 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

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。

プ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。プランチオフィスの Firewall 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 のプ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。

- [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択し、Firewall 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。
- [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。[スタティックルート設定の追加 (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。
 - [ゲートウェイ (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 C +
 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

Selected Network
 nw-192.168.1.0

Gateway*:

Metric: 1
(1 - 254)

Tunneled: (Used only for default Route)

Route Tracking:

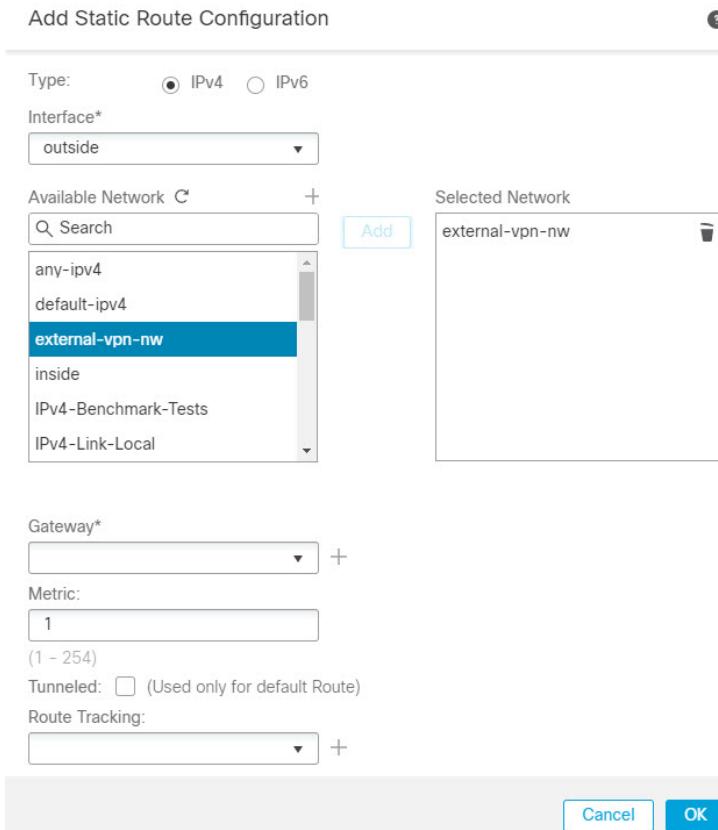
ルートリークにより、サイト間 VPN の外部（リモート）エンドによって保護されたエンドポイントは、VR1 仮想ルータの 192.168.1.0/24 ネットワークにアクセスできます。

- 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、Firewall 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。[スタティックルート設定の追加 (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。
 - [ゲートウェイ (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。

■ 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

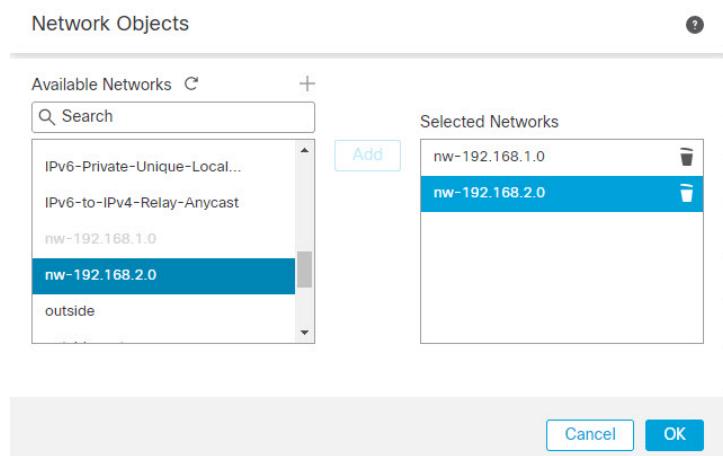


この静态ルートにより、192.168.1.0/24 ネットワーク (VR1) 上のエンドポイントは、サイト間 VPN トンネルを通過する接続を開始できます。この例では、リモートエンドポイントが 172.16.20.0/24 ネットワークを保護しています。

- 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。



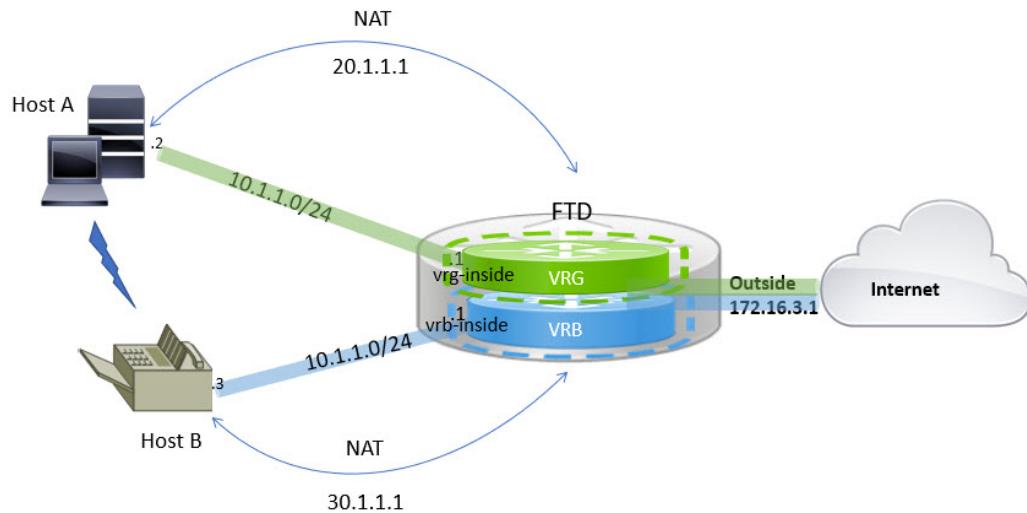
- e) [OK] をクリックして設定を保存します。

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イ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 vrbe-inside））にそれぞれ属しており、サブネット（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。

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



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。

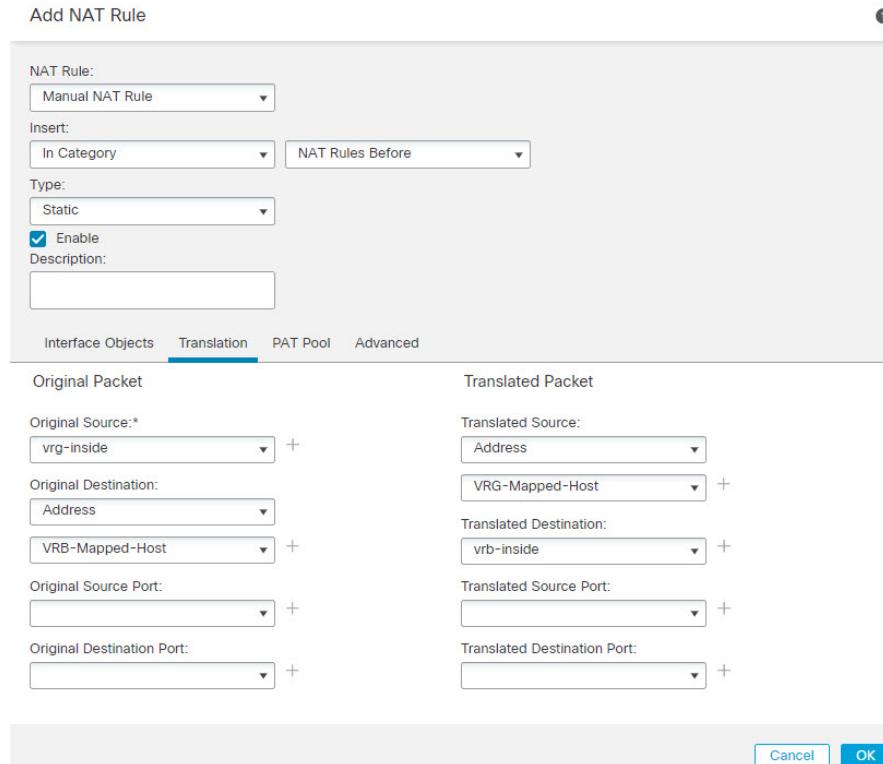
ステップ2 [新しいポリシー (New Policy)] > [Threat Defense NAT] をクリックします。

ステップ3 NAT ポリシーネームを入力し、Firewall 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。



Firewall 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
```

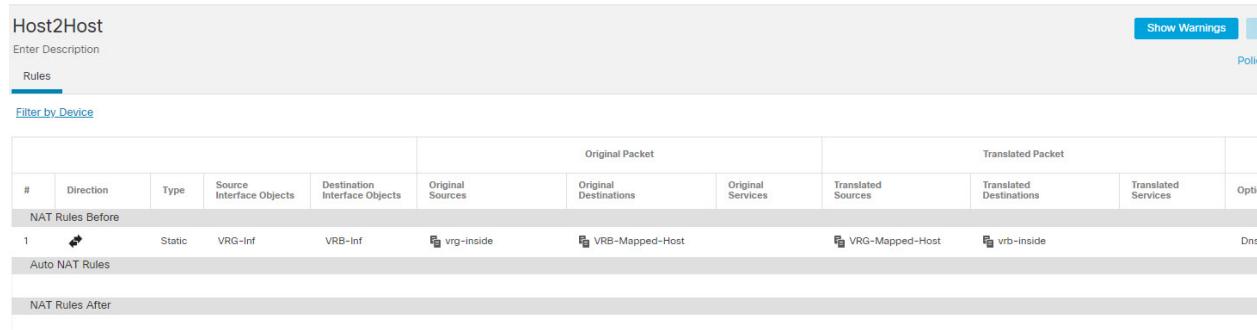
BVI インターフェイスを使用したルーテッドファイアウォール モードでの重複セグメントの管理方法

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。

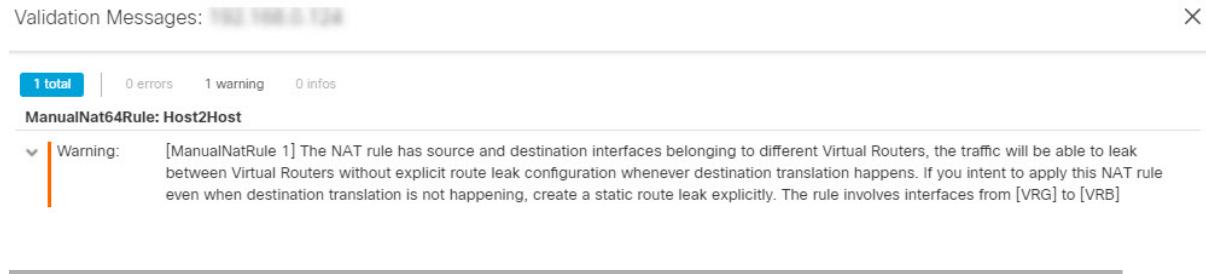
ステップ6 [保存 (Save)] をクリックします。

NAT ルールは次のようにになります。



Original Packet							Translated Packet			
#	Direction	Type	Source Interface Objects	Destination Interface Objects	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。

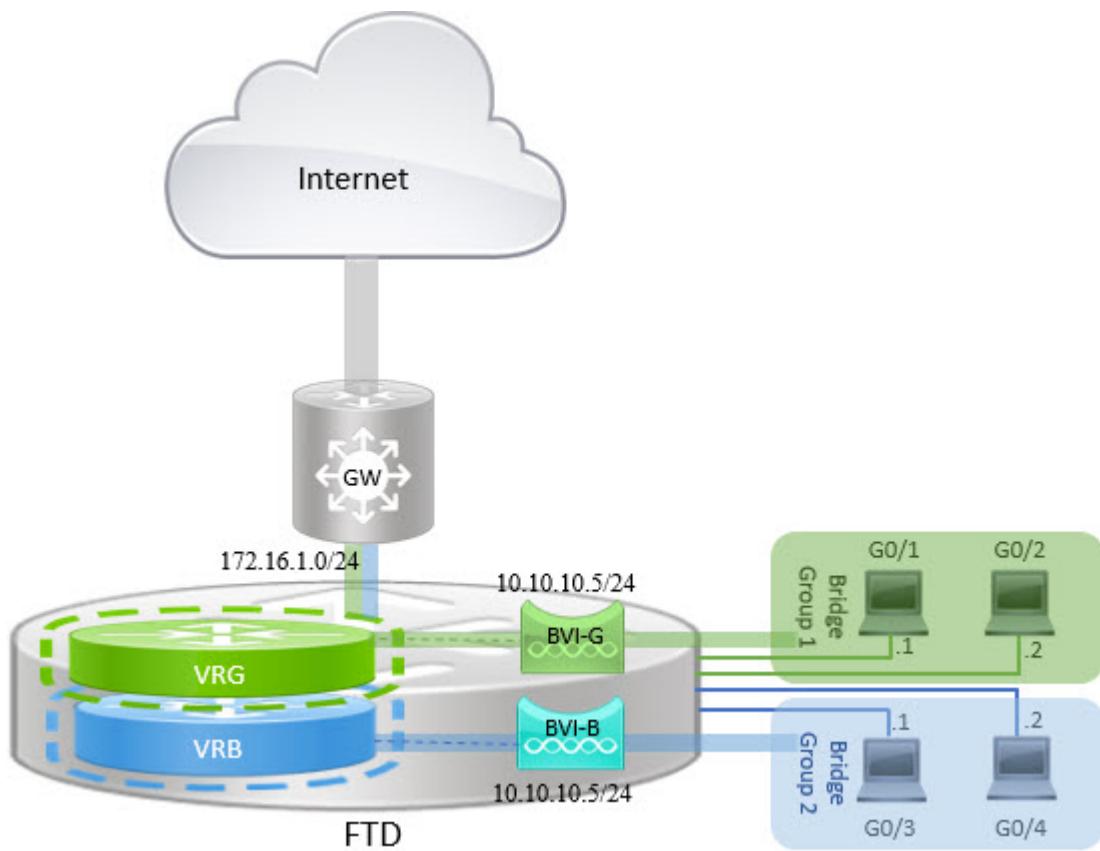


BVI インターフェイスを使用したルーテッドファイアウォール モードでの重複セグメントの管理方法

複数の重複ネットワーク間に単一の Firewall 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

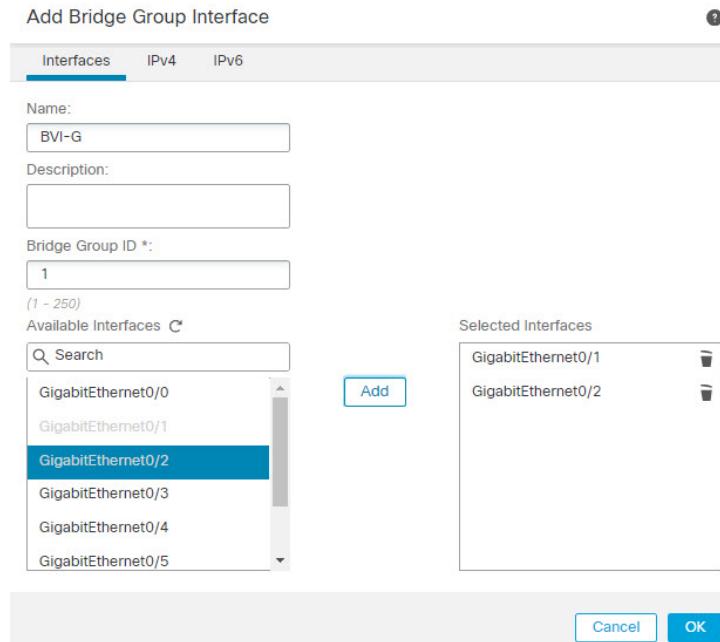
ステップ1 [デバイス (Devices)] > [デバイス管理 (Device Management)] の順に選択します。必要なデバイスを編集します。

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。

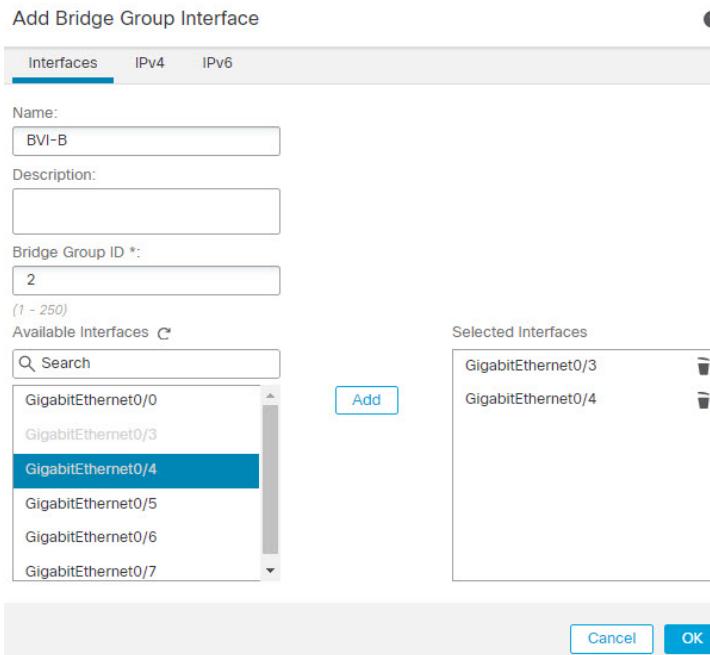
a) BVI-G の次の詳細情報を入力します。

- [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。

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



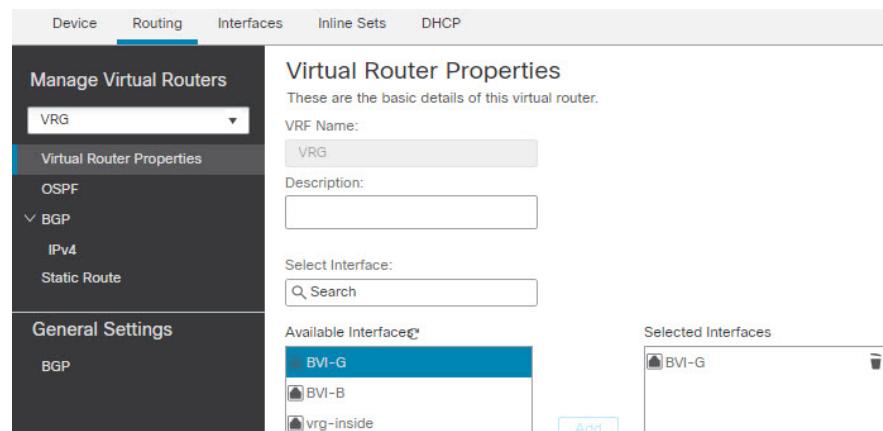
- b) [OK] をクリックします。
- c) [保存 (Save)] をクリックします。
- a) BVI-B の次の詳細情報を入力します。
 - ・[名前 (Name)] : この例では、「BVI-B」。
 - ・[ブリッジグループID (Bridge Group ID)] : この例では、「2」。
 - ・[利用可能なインターフェイス (Available Interface)] : サブインターフェイスを選択します。
 - ・[IPv4] で、[IP Type] として [Use Static IP] を選択します。
 - ・[IPアドレス (IP Address)] : 2つのイン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なります。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。

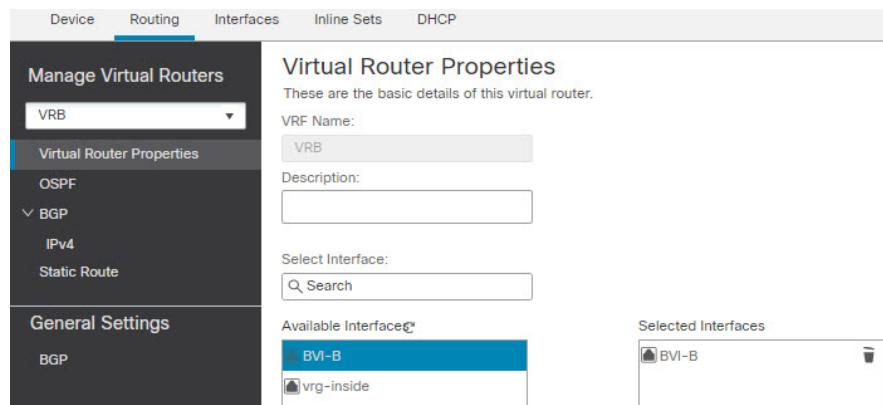


- e) [保存 (Save)] をクリックします。

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

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。

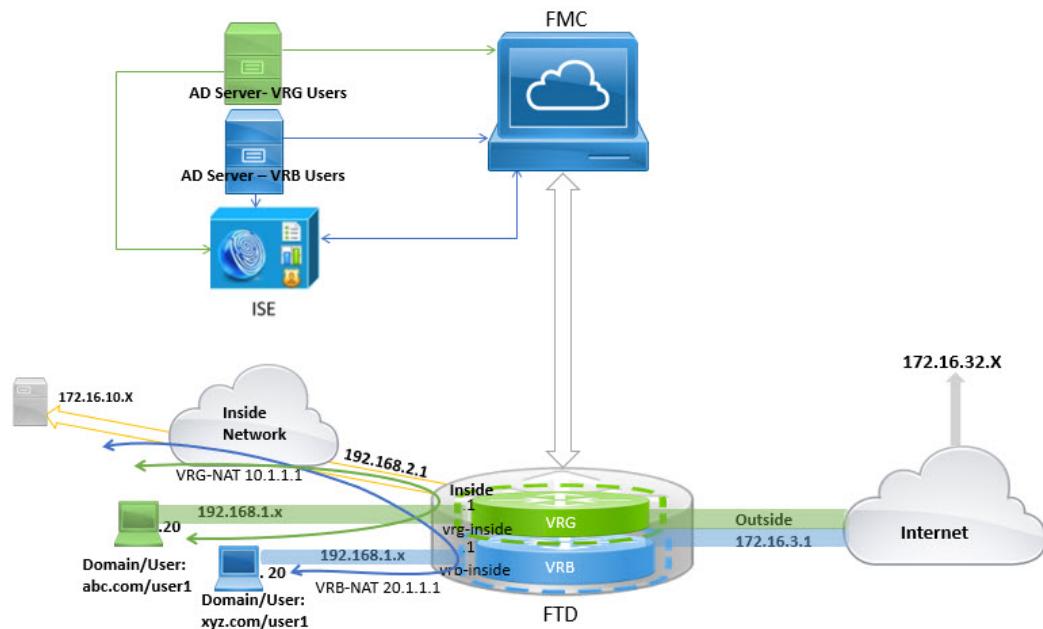
- [Devices]>[Device Management]>[Interfaces]の順に選択します。
- BVI-Bインターフェイスに対して[編集 (Edit)]をクリックします。IPアドレスを「10.10.10.5/24」と指定します。インターフェイスが2つの異なる仮想ルータに個別に割り当てられたため、BVI-Gと同じIPアドレスを設定できるようになりました。
- [OK]をクリックします。
- [保存 (Save)]をクリックします。

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のNATを設定するときは、メンバーインターフェイスを指定します。ブリッジグループインターフェイス(BVI)自体にNATを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、Firewall Management Center でユーザー認証を設定する必要があります。Firewall 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。Firewall 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。

- a) [Devices] > [Device Management] > [Interfaces] の順に選択します。
- b) 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。
- [有効 (Enabled)] チェックボックスをオンにします。

■ 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

- [IPv4] で、[IP タイプ (IP Type)] として [静的IPを使用する (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。

• [有効 (Enabled)] チェックボックスをオンにします。

• [IPv4] で、[IP タイプ (IP Type)] として [静的IPを使用する (Use Static IP)] を選択します。

• [IP アドレス (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。

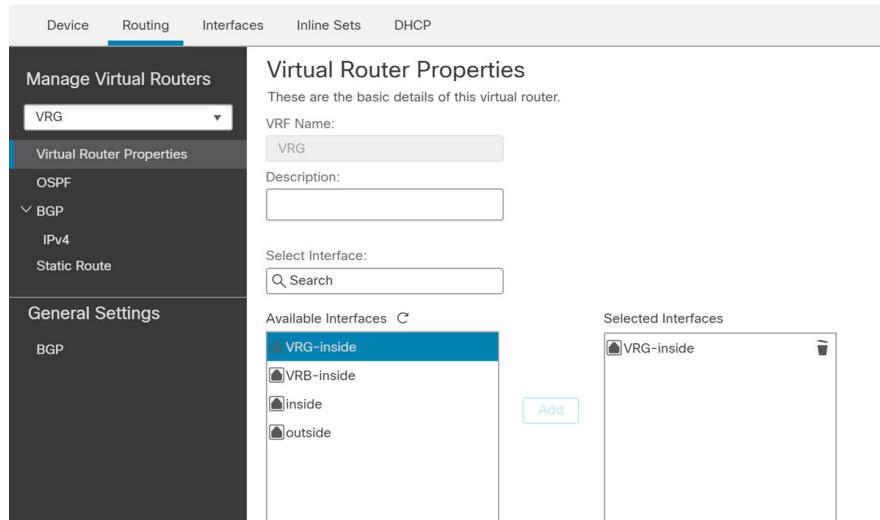
- c) [OK] をクリックします。
- d) [保存 (Save)] をクリックします。

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、Firewall 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。

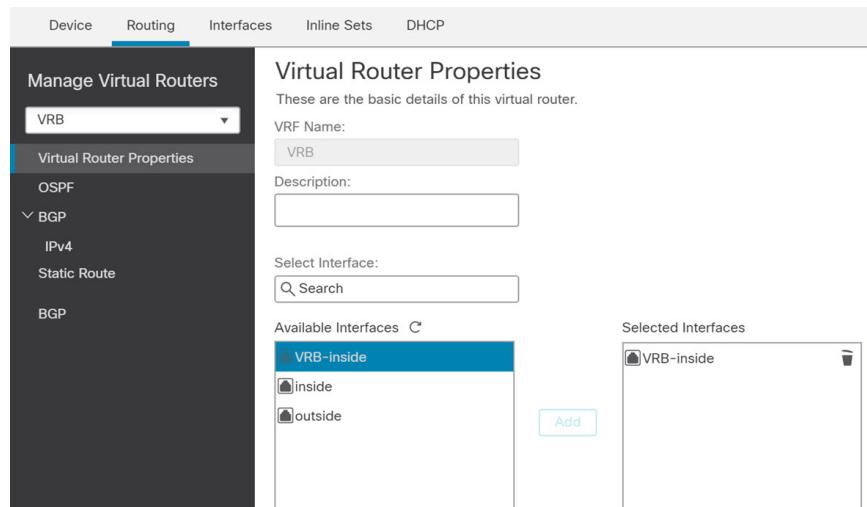
c) VRG の場合、[仮想ルータのプロパティ (Virtual Router Properties)] で、VRG-inside を割り当てて保存します。



- 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。[スタティックルート設定の追加 (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、Firewall 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。

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



- 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。[スタティックルート設定の追加 (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。

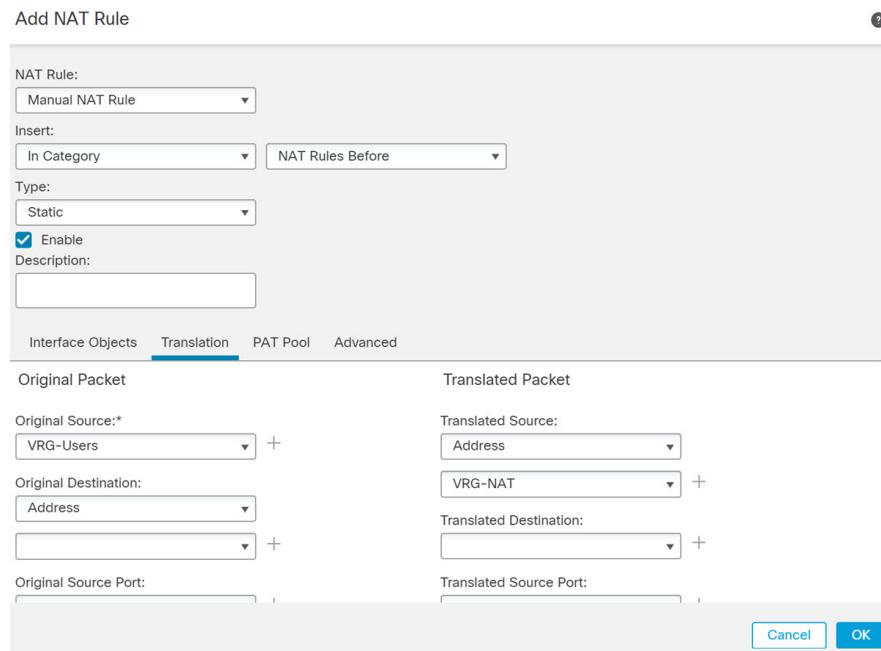
ステップ7 [新しいポリシー (New Policy)] > [Threat Defense NAT] をクリックします。

ステップ8 NAT ポリシーネームを入力し、Firewall 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、[ルールの追加 (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。



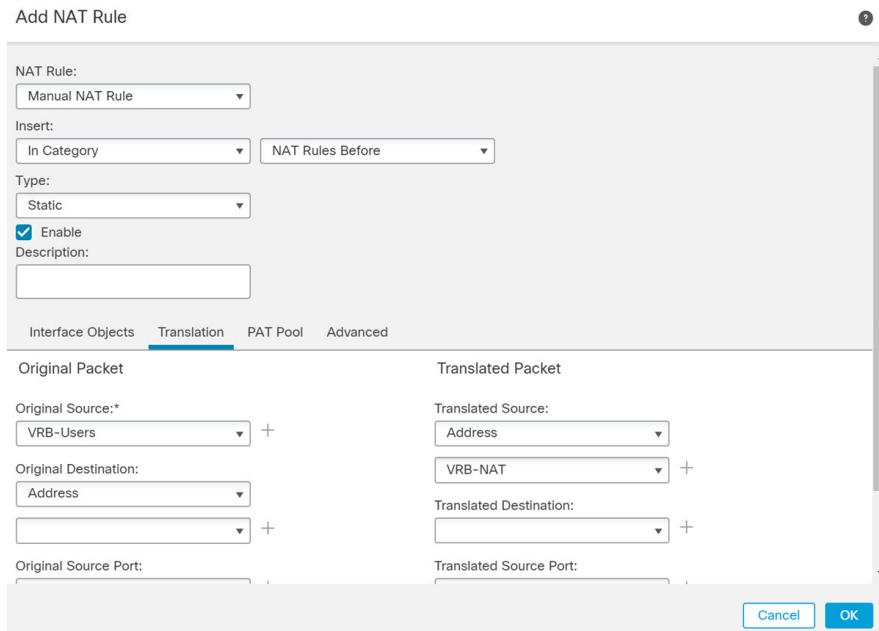
ステップ 10 [OK] をクリックします。

ステップ 11 [NAT] ページで、[ルールの追加 (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。

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

- [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。



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になります。

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

ステップ 13 Firewall Management Center に 2 つの一意の 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realm (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、[realm 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。[realmディレクトリ (Realm Directory)] および [同期 (Synchronize)] フィールドを参照 [LDAP realm または Active Directory realm および realm ディレクトリの作成](#)を参照してください。
- ステップ 16** Firewall 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、[realm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。

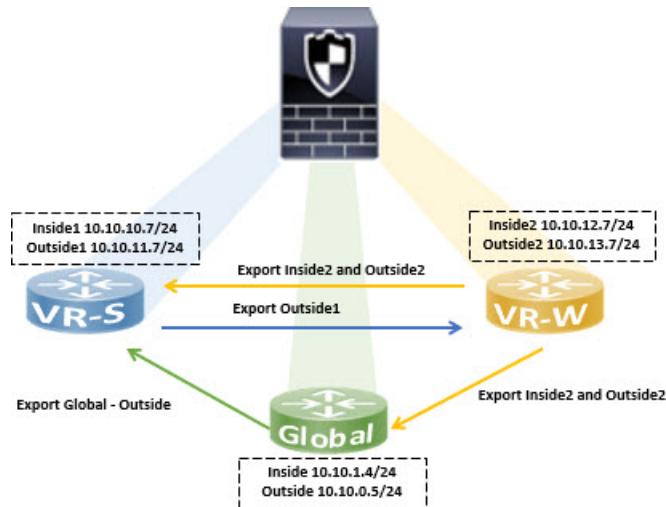
工場のファイアウォールデバイスが次の仮想ルータとインターフェイスで構成されているとします。

- 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。

BGP を使用して仮想ルータを相互接続する方法

図 2:BGP を使用した仮想ルータの相互接続



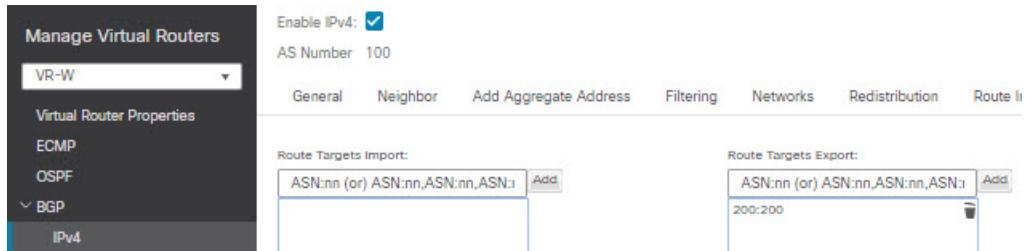
始める前に

- 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。

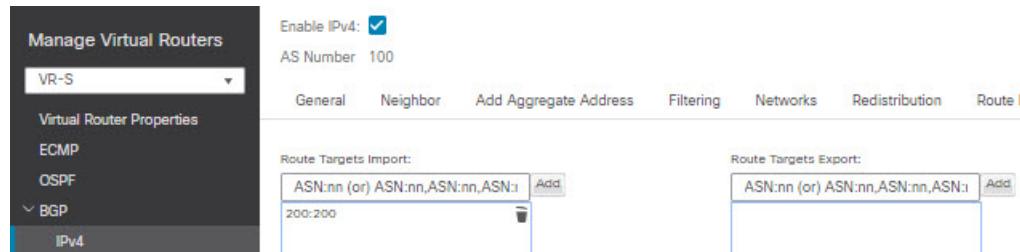
手順

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。

- [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。
- 仮想ルータのドロップダウンから、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。
- 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。



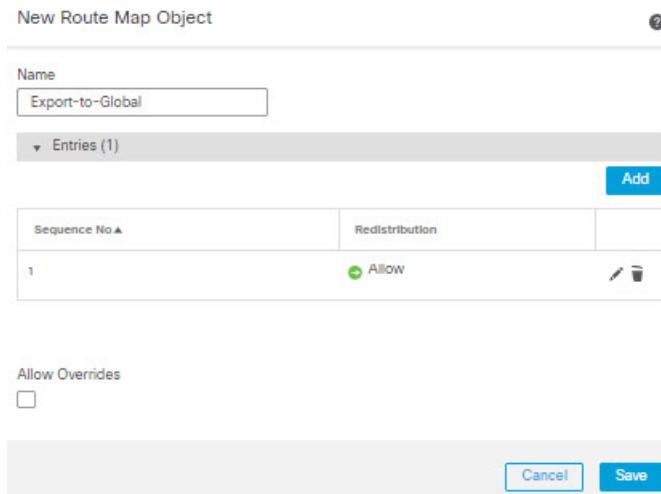
(注)

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トマッピ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。

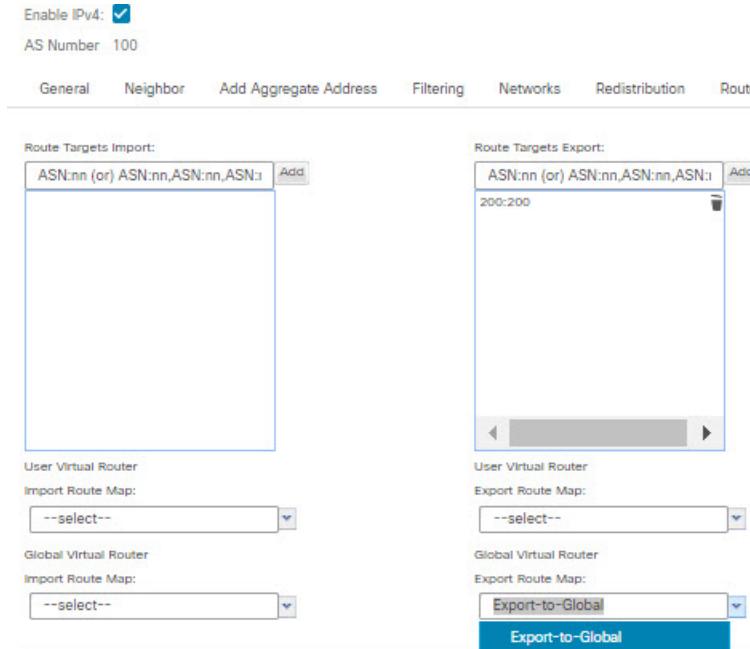
BGP を使用して仮想ルータを相互接続する方法



- 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。

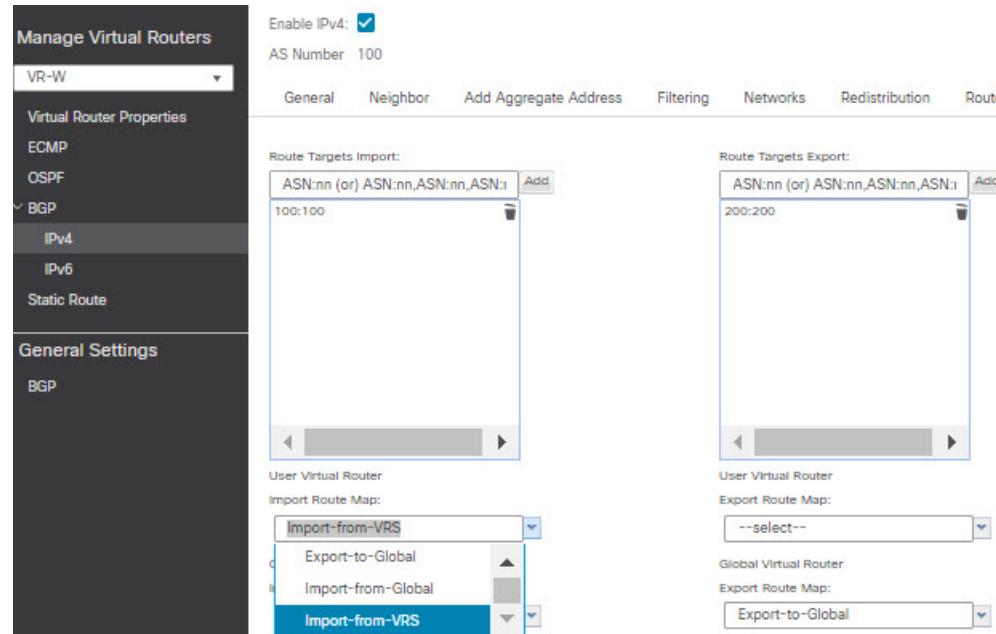


ステップ3 VR-S の Outside1 ルートのみを VR-W にリークするには：

- 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。

BGP を使用して仮想ルータを相互接続する方法



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一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。

- [オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] > [プレフィックリスト (Prefix List)] > [IPv4 プレフィックリスト (IPv4 Prefix List)] を選択します。
- [IPv4 プレフィックリストの追加 (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。
- [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。
- 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: 1

IP Addresses: (Limit 250) Address: 10.10.0.0/24

Min Prefix Length:

Max Prefix Length:

- 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: 1

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			
BGP			
Others			

Available Access Lists : Standard

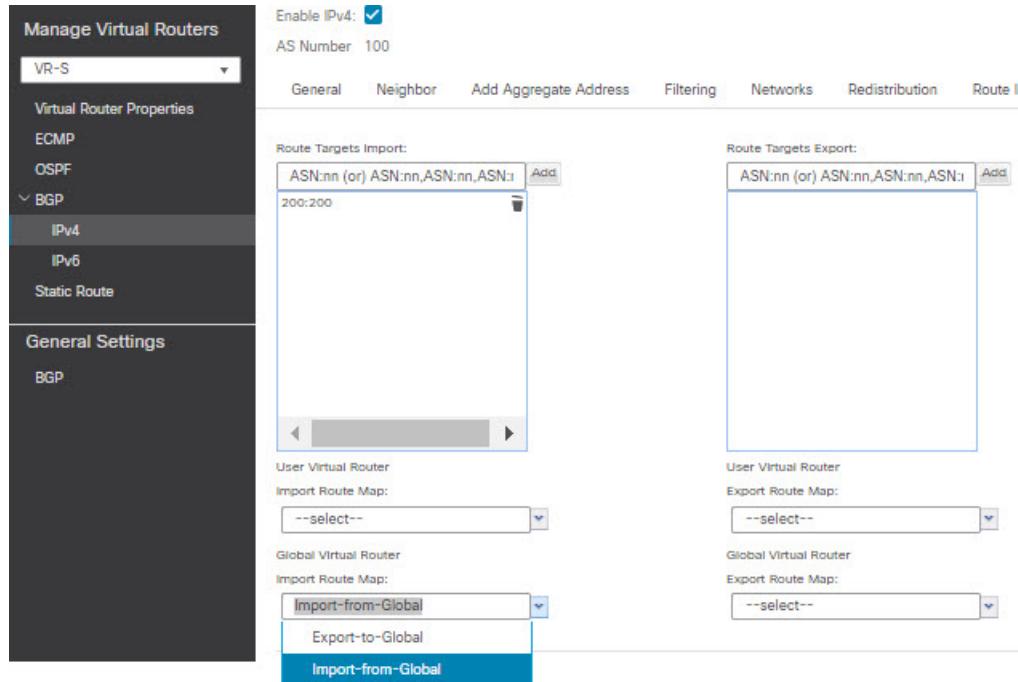
Available IPv4 Prefix List Global-Outside-Only

Selected IPv4 Prefix List Global-Outside-Only

- 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。

仮想ルータの履歴

- 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 Firewall Management Center	最小 Firewall Threat Defense	詳細
ISA 3000 の仮想ルータサポート。	7.0	7.0	ISA 3000 には最大 10 の仮想ルータを設定できます。
ユーザ一定義の仮想ルータでの SNMP サポート	7.0	7.0	ユーザ一定義の仮想ルータで SNMP を設定できるようになりました。
仮想ルータの一括削除。	6.7	6.6	一度に複数の仮想ルータを 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 Routers)]

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
Threat Defense の仮想ルータと VRF-Lite。	6.6	6.6	<p>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るようになりました。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。仮想ルータは、Virtual Routing and Forwarding の「軽量」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。作成できる仮想ルータの最大数は 5 ~ 100 の範囲で、デバイスのモデルによって異なります。</p> <p>新規/変更された画面 : [デバイス (Devices)]>[デバイス管理 (Device Management)]のデバイスの編集の [ルーティング (Routing)] タブ 新規/変更された CLI コマンド :</p> <ul style="list-style-type: none"> • show vrf • [vrf name all] キーワードセットを CLI コマンド clear ospf、clear route、ping、show asp table routing、show bgp、show ipv6 route、show ospf、show route、show snort counters に追加し、必要に応じて出力が仮想ルータ情報を表示するように変更 <p>プラットフォームの制限 : Firepower 1010 および ISA 3000 ではサポートされていません。</p>

■ 仮想ルータの履歴

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。