仮想ルータ

仮想ルータを作成して、インターフェイスのサブセットのトラフィックを相互に分離することができます。

- 仮想ルータと Virtual Route Forwarding（VRF）について （1 ページ）
- 仮想ルータのガイドライン （5 ページ）
- 仮想ルータの管理 （7 ページ）
- 仮想ルータの例 （11 ページ）
- 仮想ルータのモニタリング （29 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のものになります。

仮想ルーター対応ポリシーの設定

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。

NAT などのセキュリティゾーンを使用しないポリシーでは、1つの仮想ルータに割り当てられたインターフェイスを送信元インターフェイスと宛先インターフェイスとして選択することによって、仮想ルータ固有のルールを作成できます。2つの個別の仮想ルータから送信元インターフェイスと宛先インターフェイスを選択する場合は、ルールが機能するよう、仮想ルータ間に適切なルートがあることを確認する必要があります。

仮想ルータ間のルーティング

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。

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	このモデルでは仮想ルータはサポートされていません。
Firepower 1120	5
Firepower 1140	10
Firepower 1150	10
Cisco Secure Firewall 1210CE	5
Cisco Secure Firewall 1210CP	5
Cisco Secure Firewall 1220CX	10
Cisco Secure Firewall 1230	10
Cisco Secure Firewall 1240	10
Cisco Secure Firewall 1250	15
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
Threat Defense Virtual、すべてのプラットフォーム	30
ISA 3000	10

仮想ルータのガイドライン

デバイスモデルのガイドライン

次を除くすべての対応デバイスモデルで、仮想ルータを設定できます。

- Firepower 1010

その他のガイドライン

- 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
  - BGPv6
  - マルチキャストルーティング
  - ポリシーベースのルーティング
  - [VPN]
- 次の機能は、仮想ルータごとに個別に設定できます。
  - スタティック ルートとその SLA モニタ。
  - OSPFv2
  - BGPv4
- 次の機能は、リモートシステムとクエリまたは通信するときに（ボックスからのトラフィック)、システムによって使用されます。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。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、システムが外部サーバに到達するためにルートを検索する必要がある場合は、グローバル仮想ルータでルートルックアップが行われます。
  - アクセス コントロール 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**コマンドの名前を解決する場合に使用されるDNSサーバ。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(Active Directoryなど)が、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。
- SNMP。

- NAT では、異なる仮想ルータに割り当てられた送信元インターフェイスと宛先インターフェイスを指定すると、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 ルール内のインターフェイスが意図せず混在していないことを確認します。通常は送信元と宛先のインターフェイスが使用され、ルーティングテーブルは無視され、手動 NAT での宛先変換も無視されます。ただし、NAT ルールでルートルックアップを実行する必要がある場合、インバウンド インターフェイスの VRF テーブルでのみルックアップが実行されます。必要に応じて、宛先インターフェイスの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ることに注意してください。仮想ルータを使用する場合は、NAT ルールを慎重にテストして、想定どおりに動作することを確認します。必要なルートリークを定義しておかないと、場合によっては、ルールが適合すると予想されるすべてのトラフィックにルールが適合せず、変換が適用されません。
- 仮想ルータ間のルートを設定する場合（ある仮想ルータから 2 番目の仮想ルータへのルートをリークする場合など）、システムは送信元の仮想ルータで宛先インターフェイス ルックアップを実行します。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。
- たとえば、仮想ルータ1から仮想ルータ2への仮想ルータ間ルート(リークルート)を使用する場合は、リターントラフィックを許可するために仮想ルータ2にミラー(リバース)ルートを設定する必要はありません。ただし、どちらの方向でも接続を開始できるようにする場合は、仮想ルータ1から2、および仮想ルータ2から1の両方の方向にルートがリークしていることを確認します。
- ある仮想ルータから別の仮想ルータにインターフェイスを移動すると、そのインターフェイスに設定されているすべての機能が保持されます。設定を調べて、スタティックルート、IP アドレス、およびその他のポリシーが新しい仮想ルータのコンテキスト内で有効なことを確認します。
- 複数の仮想ルータで重複するアドレス空間を使用する場合は、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ないことに注意してください。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アイデンティティレルムを設定します。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。
- 複数の仮想ルータで重複するアドレス空間を使用すると、ダッシュボードデータが紛らわしくなる可能性があります。同じ IP アドレスの接続は集約されます。そのため、同じ IP

アドレスが2つ以上のエンドポイントで共有されている場合は、そのアドレスで送受信されるトラフィックが増加したように見えます。個別のアイデンティティ レルムを使用してアイデンティティ ポリシーを慎重に作成する場合は、ユーザベースの統計情報の方が正確です。

- オーバーラップしているDHCPアドレスプールは、別の仮想ルータでは使用できません。
- DHCPサーバの自動設定は、グローバル仮想ルータのインターフェイスでのみ使用できます。自動設定は、ユーザ定義の仮想ルータに割り当てられているインターフェイスではサポートされていません。
- グローバル仮想ルータから新しいルータへの移動を含め、仮想ルータ間でインターフェイスを移動すると、そのインターフェイスを介した既存の接続はすべて切断されます。
- 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。

仮想ルータの管理

仮想ルータと呼ばれる複数の Virtual Routing and Forwarding（VRF）インスタンスを作成して、インターフェイスのグループに対して個別のルーティングテーブルを維持できます。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。

デフォルトでは、仮想ルーティングは無効になっています。すべてのデバイスで、データ（通過）および管理（ボックス間）トラフィック用に、1つのグローバルルーティングテーブルのセットが使用されます。

仮想ルーティングを有効にすると、最初のルーティングページは、システムで定義されている仮想ルータの一覧になります。仮想ルータを有効にしない場合、最初のルーティングページは、システムで定義されているスタティックルートの一覧になります。

グローバル仮想ルータは、常に存在します。グローバルルータは、個別の仮想ルータに割り当てられていないすべてのインターフェイスを保持します。

手順

ステップ1 [デバイス（Device）] をクリックしてから、[ルーティング（Routing）] サマリーにあるリンクをクリックします。

ステップ 2 まだ仮想ルータを有効にしていない場合は、[複数の仮想ルータの追加（Add Multiple Virtual Routers）] リンクをクリックし、次に [最初のカスタム仮想ルータの作成（Create First Custom Virtual Router）] をクリックします。

最初の仮想ルータの作成は、基本的に、追加の仮想ルータの作成と同じです。詳細については、仮想ルータの作成またはインターフェイス割り当ての編集 （9 ページ）を参照してください。

ステップ 3 次のいずれかを実行します。

- すべての仮想ルータに適用されるグローバル BGP を設定するには、[BGPグローバル設定（BGP Global Settings）] ボタンをクリックします。これらの設定は、スマート CLI を使用して行います。これについては、Smart CLI オブジェクトの設定で説明しています。1 つ以上の仮想ルータで BGP を設定する場合にのみ、グローバル BGP 設定を設定します。
- 新しいルータを作成するには、仮想ルータのリストの上にある [+] ボタンをクリックします。
- たとえば、スタティックルートを作成したり、ルーティングプロセスを定義したりするために、仮想ルータのルーティングプロパティを編集するには、仮想ルータの [アクション（Action）] セルの表示アイコン（  ）をクリックします。
- 仮想ルータの名前、説明、またはインターフェイスの割り当てを編集するには、仮想ルータの [アクション（Action）] セルの表示アイコン（  ）をクリックし、[仮想ルータのプロパティ（Virtual Router Properties）] タブを選択します。
- 仮想ルータの表示を切り替えるには、仮想ルータ名の横（ルーティングテーブルの上）にある下向き矢印をクリックし、目的の仮想ルータを選択します。[仮想ルータに戻る（Go Back To Virtual router）] 矢印（  ）をクリックすると、リストページに戻ることができます。
- 仮想ルータを削除するには、仮想ルータの [アクション（Action）] セルの削除アイコン（  ）をクリックするか、仮想ルータの内容を表示するときに仮想ルータ名の横に表示される削除アイコンをクリックします。最後の仮想ルータ（削除できないグローバルルータ以外）を削除すると、VRF は無効になります。
- 仮想ルータのルーティングをモニタするには、その仮想ルータのテーブル内のいずれかの **show** コマンドのリンクをクリックします。コマンドをクリックすると CLI コンソールが開き、CLI コマンドの出力を調べることができます。ルート、OSPF、および OSPF ネイバーに関する情報を表示できます。コマンド出力は展開された設定に基づいていることに注意してください。展開されていない編集内容は表示されません。

  これらのコマンドは、仮想ルータを表示するときに [コマンド（Commands）] ドロップダウン リストから選択して実行することもできます。

仮想ルータの作成またはインターフェイス割り当ての編集

仮想ルータでスタティック ルートまたはルーティング プロセスを設定するには、その前にルータを作成し、インターフェイスを割り当てる必要があります。

始める前に

[インターフェイス（Interface）] ページに移動し、仮想ルータに追加する各インターフェイスに名前が付いていることを確認します。仮想ルータに名前を付けるまでは、仮想ルータにインターフェイスを追加できません。

手順

ステップ 1 **[デバイス（Device）]** > **[ルーティング（Routing）]** をクリックします。

ステップ 2 次のいずれかを実行します。

- まだ仮想ルータを作成していない場合は、[複数の仮想ルータの追加（Add Multiple Virtual Routers）] リンクをクリックし、次に [最初のカスタム仮想ルータの作成（Create First Custom Virtual Router）] をクリックします。
- 仮想ルータのリストの上にある [+] ボタンをクリックして、新しいルータを作成します。
- 仮想ルータの編集アイコン（  ）をクリックして、そのプロパティとインターフェイスリストを編集します。
- 仮想ルータを表示している場合は、[仮想ルータのプロパティ（Virtual Router Properties）] タブをクリックして、表示している仮想ルータのプロパティを編集します。
- 仮想ルータを表示している場合は、仮想ルータ名の横にある下矢印をクリックし、[仮想ルータの新規作成（Create New Virtual Router）] をクリックします。

ステップ 3 仮想ルータのプロパティを設定します。

- [名前（Name）]：仮想ルータの名前。
- [説明（Description）]：仮想ルータの説明（任意）。
- [インターフェイス（Interfaces）]：[+] をクリックして、仮想ルータの一部となる各インターフェイスを選択します。インターフェイスを削除するには、インターフェイス上にカーソルを合わせ、インターフェイス カードの右側にある [X] をクリックします。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、ブリッジ グループ、および EtherChannel を割り当てられますが、VLAN は割り当てられません。

  他のインターフェイスへのルートを意図的に仮想ルーティング テーブルにリークしない限り、ルーティング テーブルはこれらのインターフェイスに制限されます。

ステップ 4 [OK] または [保存（Save）] をクリックします。

この仮想ルータのビューが表示されます。ここでスタティック ルートまたはルーティング プロセスを設定できます。

仮想ルータのスタティック ルートとルーティング プロセスの設定

各仮想ルータには、個別のスタティックルートとルーティングプロセスがあります。これは、他の仮想ルータに定義されているルートおよびルーティングプロセスとは別に動作します。

スタティック ルートを設定する場合は、仮想ルータの外部にある宛先インターフェイスを選択できます。これにより、宛先インターフェイスを含むルートが仮想ルータにリークされます。他の仮想ルータに必要以上のトラフィックを送信しないように、リークが必要なルートだけをリークするようにします。たとえば、インターネットへのパスが1つの場合、インターネット宛てのトラフィックについて、各仮想ルータからインターネットに接する仮想ルータへのルートをリークすることが理にかなっています。

手順

ステップ 1 **[デバイス（Device）] > [ルーティング（Routing）]** を選択します。

ステップ 2 仮想ルータを開くには、[アクション（Action）] セルの [表示（view）] アイコン（  ）をクリックします。

ステップ 3 次のいずれかを実行します。

- スタティックルートを設定するには、[スタティックルーティング（Static Routing）] タブをクリックしてから、ルートを作成または編集します。詳細については、スタティックルートの設定を参照してください。
- 等コストマルチパス（ECMP）トラフィックゾーンを設定するには、[ECMPトラフィックゾーン（ECMP Traffic Zones）] タブをクリックし、ゾーンを作成します。詳細については、ECMP トラフィックゾーンの設定を参照してください。
- BGPルーティングプロセスを設定するには、[BGP] タブをクリックし、プロセスを定義するために必要なスマートCLIオブジェクトを作成します。詳細については、Border Gateway Protocol（BGP）を参照してください。

  すべての仮想ルータに適用されるBGPのグローバル設定もあります。これらのプロパティを設定するには、仮想ルータのリストページに戻り、[BGPグローバル設定（BGP Global Settings）] ボタンをクリックします。
- OSPF ルーティングプロセスを設定するには、[OSPF] タブをクリックしてから、最大2つのプロセスを定義するために必要なスマートCLIオブジェクトを作成し、それらに関連付けられたインターフェイス設定を作成します。詳細については、Open Shortest Path First（OSPF）を参照してください。

- （グローバル仮想ルータのみ）EIGRP ルーティングプロセスを設定するには、[EIGRP] タブをクリックし、単一プロセスを定義するために必要な Smart CLI オブジェクトを作成します。詳細については、Enhanced Interior Gateway Routing Protocol（EIGRP）を参照してください。

仮想ルータの削除

仮想ルータが不要になった場合は、削除できます。グローバル仮想ルータを削除することはできません。

仮想ルータを削除すると、その仮想ルータ内で設定されているすべてのスタティックルートとルーティングプロセスも削除されます。

仮想ルータに割り当てられたすべてのインターフェイスは、グローバルルータに再割り当てされます。

手順

ステップ 1 **[デバイス（Device）] > [ルーティング（Routing）]** を選択します。

ステップ 2 次のいずれかを実行します。

- 仮想ルータのリストで、仮想ルータの[アクション（Action）]列にある削除アイコン（）をクリックします。
- 削除する仮想ルータを表示している場合、ルータ名の横にある削除アイコン（）をクリックします。

仮想ルータを削除することの確認を求められます。

ステップ 3 [OK] をクリックして、削除を実行します。

仮想ルータの例

次のトピックでは、仮想ルータの実装例を示します。

関連トピック

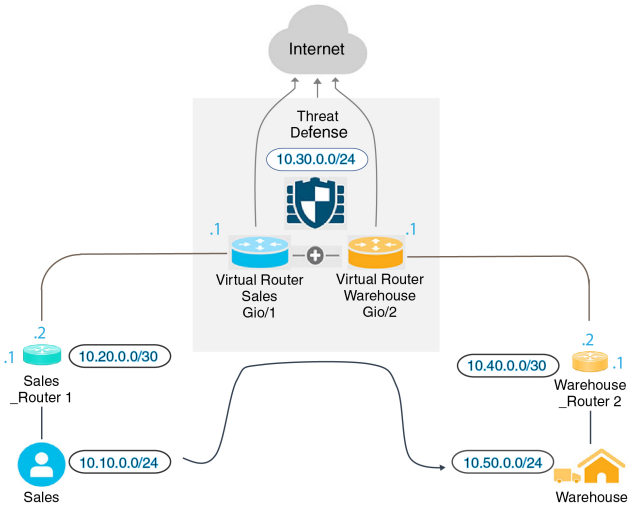
サイト間 VPN における複数の仮想ルータのネットワークからのトラフィックを保護する方法

異なる仮想ルータの内部ネットワークへの RA VPN アクセスを可能にする方法

複数の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

仮想ルータを使用する場合、1 つの仮想ルータのユーザが、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ある場合があります。

次の図を考えてみましょう。セールスチームのワークステーションは、Sales 仮想ルータに接続されています。ウェアハウスサーバは、Warehouse 仮想ルータを介して接続されます。販売チームが、IP アドレスが 10.50.0.5/24 であるウェアハウスサーバの情報を検索する必要がある場合は、Sales 仮想ルータからのルートを Warehouse 仮想ルータにリークする必要があります。また、Warehouse 仮想ルータは、Warehouse Router 2 から数ホップ離れたウェアハウスサーバへのルートも持っている必要があります。



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。

- Threat Defense デバイスの Sales と Warehouse の両方の仮想ルータで、GigabitEthernet 0/1 が Sales に割り当てられ、GigabitEthernet 0/2 が Warehouse に割り当てられています。
- Sales Router 1 には、10.20.0.1/30 インターフェイスから 10.50.0.5/24 にトラフィックを送信するスタティックルートまたはダイナミックルートのいずれかが含まれています。

手順

ステップ 1 10.50.0.5/24 または 10.50.0.0/24 のネットワークオブジェクトを作成します。また、ゲートウェイ（10.40.0.2/30）のオブジェクトを作成します。

ルートをウェアハウスサーバの単一の IP アドレスに制限する場合は、ホストオブジェクトを使用して10.50.0.5 を定義します。または、販売チームが倉庫内の他のシステムにアクセスできるようにするには、10.50.0.0/24 ネットワークのネットワークオブジェクトを作成します。この例では、ホスト IP アドレスのルートを作成します。

a) [オブジェクト（Objects）] を選択し、目次から [ネットワーク（Networks）] を選択します。
b) [+] をクリックし、次にウェアハウスサーバのオブジェクトプロパティを入力します。

c) [OK] をクリックします。
d) [+] をクリックし、次にウェアハウスネットワークへのルータゲートウェイのオブジェクトプロパティを入力します。

e) [OK] をクリックします。

ステップ 2 Warehouse 仮想ルータの Gi0/2 インターフェイスをポイントする、Sales でのルートリークを定義します。

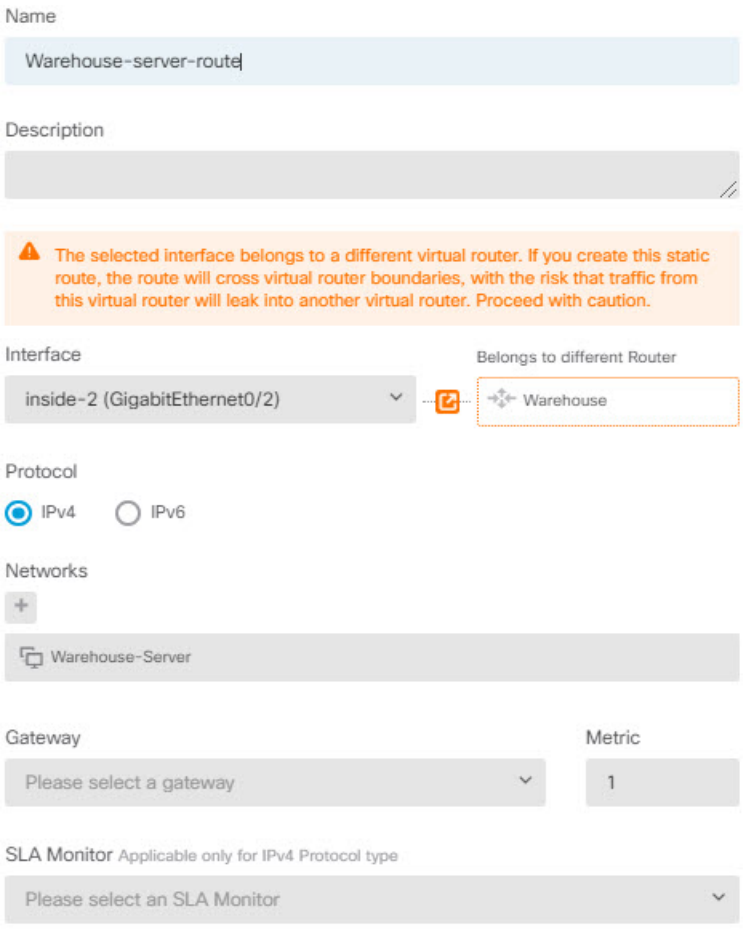
この例では、Gi0/1 に inside という名前が付けられており、Gi0/2 には inside-2 という名前が付けられています。

a) [デバイス（Device）] をクリックしてから、[ルーティング（Routing）] のサマリーで [設定の表示（View Configuration）] をクリックします。
b) 仮想ルータのリストで、Sales 仮想ルータの [アクション（Action）] 列にある [表示（view）] アイコン（  ）をクリックします。

c) [スタティックルーティング（Static Routing）] タブで、[+] をクリックしてルートを設定します。

- [名前（Name）]：Warehouse-server-route など、任意の名前が付けられます。
- [インターフェイス（Interface）]：**inside-2** を選択します。インターフェイスが別のルータにあり、ルートリークを作成しているという警告が表示されます。これを今から実行します。
- [プロトコル（Protocol）]：この例では、**IPv4** を使用します。または、IPv6 アドレスを使用してこの例を実装することもできます。
- [ネットワーク（Networks）]： Warehouse-Server オブジェクトを選択します。
- [ゲートウェイ（Gateway）]：この項目は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、ゲートウェイアドレスを選択しません。

次のようなダイアログが表示されるはずです。

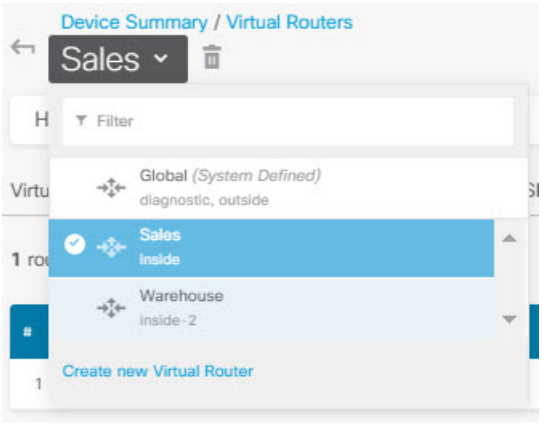


d) [OK] をクリックします。

ステップ 3 Warehouse 仮想ルータで、Warehouse Router 2 のゲートウェイを指すルートを定義します。

または、Warehouse Router 2 からルートを動的に検出するルーティングプロトコルを設定することで、これを行うことができます。この例では、スタティックルートを定義します。

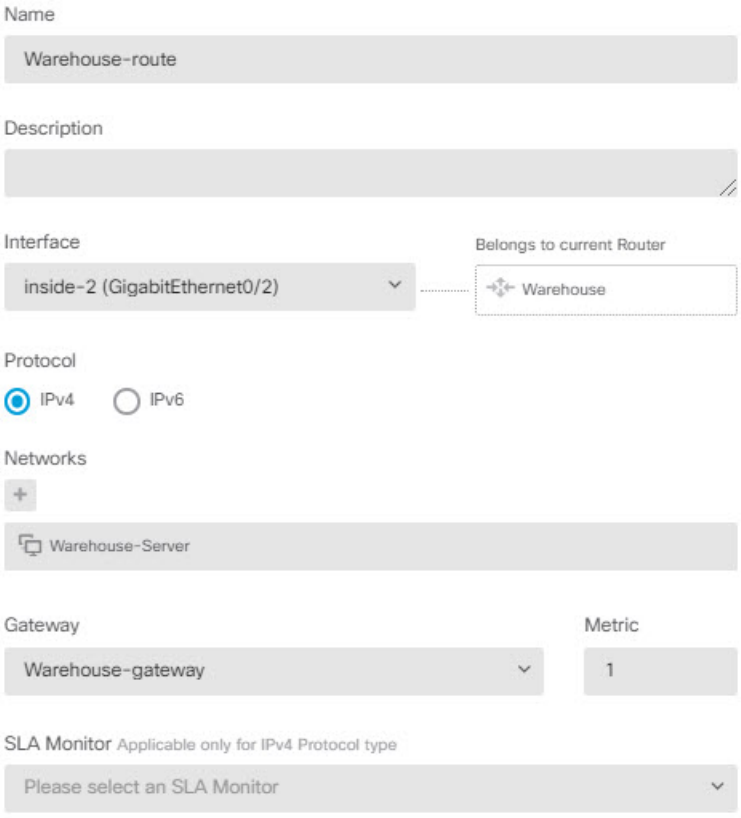
a) 現在 Sales と示されている仮想ルータのドロップダウンから、Warehouse 仮想ルータを選択してルータを切り替えます。



b) [スタティックルーティング（Static Routing）] タブで、[+] をクリックしてルートを設定します。

- [名前（Name）]：Warehouse-route など、任意の名前が付けられます。
- [インターフェイス（Interface）]：**inside-2** を選択します。
- [プロトコル（Protocol）]：**IPv4** を選択します。
- [ネットワーク（Networks）]： 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。

次のようなダイアログが表示されるはずです。

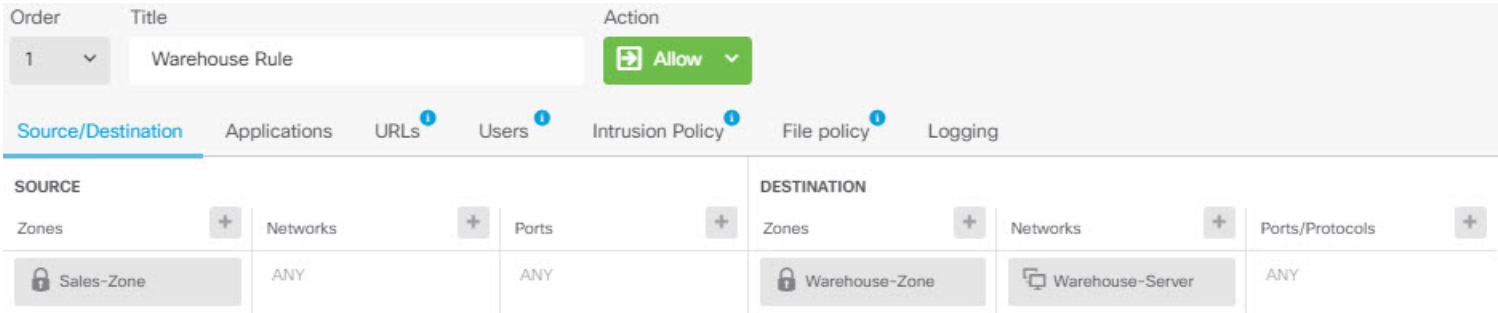


c) [OK] をクリックします。

ステップ 4 ウェアハウスサーバへのアクセスを許可するアクセス制御ルールがあることを確認します。

最も単純なルールは、Sales 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 Warehouse 仮想ルータ内の宛先インターフェイスへのトラフィックを許可するものです。適切な侵入インスペクションをトラフィックに適用できます。

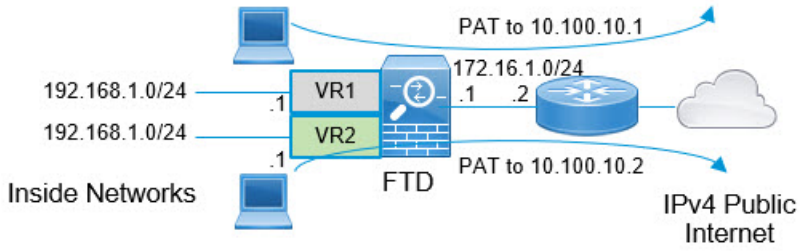
たとえば、Sales のインターフェイスが Sales-Zone セキュリティゾーンにあり、Warehouse のインターフェイスが Warehouse-Zone セキュリティゾーンにある場合、アクセス制御ルールは次のようになります。



重複するアドレス空間を持つ複数の仮想ルータへの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。たとえば、inside および inside-2 のインターフェイスをどちらも IP アドレス 192.168.1.1/24 を使用するように定義し、192.168.1.0/24 ネットワーク内のセグメント上のエンドポイントを管理することができます。ただし、これらの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、リターントラフィックが正しい宛先に到達するように、仮想ルータから発信されるトラフィックを慎重に処理する必要があります。

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。それぞれ別の NAT または PAT プールを使用することが理想的です。PAT を使用して、仮想ルータ 1 の送信元アドレスを 10.100.10.1 に変換し、仮想ルータ 2 の送信元アドレスを 10.100.10.2 に変換することができます。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を明示的に選択した NAT/PAT ルールを定義する必要があります。これは、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るからです。



（注） この例では、各仮想ルータに 1 つのインターフェイスが含まれています。「inside」仮想ルータに複数のインターフェイスがある場合は、「inside」インターフェイスごとに NAT ルールを作成する必要があります。重複するアドレス空間を使用しない仮想ルータ内にいくつかのインターフェイスがある場合でも、NAT ルールで送信元インターフェイスを明示的に特定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るようになります。

手順

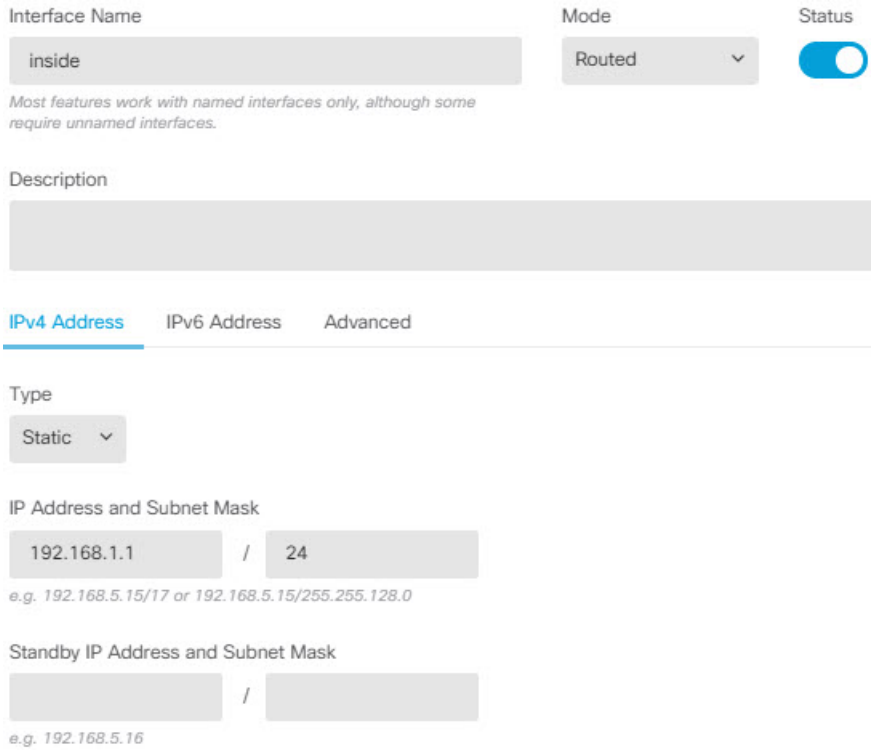
ステップ 1 仮想ルータ 1（VR 1）の内部インターフェイスを設定します。

a) [デバイス（Device）] をクリックしてから、[インターフェイス（Interfaces）] サマリーにある [すべてのインターフェイスを表示（View All Interfaces）] リンクをクリックします。

b) VR 1 に割り当てるインターフェイスの [アクション (Action)] 列にある編集アイコン（）をクリックします。

c) 少なくとも次のプロパティを設定します。

- [名前（Name）]：この例では **inside**。
- [モード（Mode）]：[ルーテッド（Routed）] を選択します。
- [ステータス（Status）]：インターフェイスを有効にします。
- [IPv4アドレスタイプ（IPv4 Address Type）]>：[スタティック（Static）] を選択します。
- [IPv4アドレスとサブネットマスク（IPv4 Address and Subnet Mask）]：192.168.1.1/24 と入力します。



d) [OK] をクリックします。

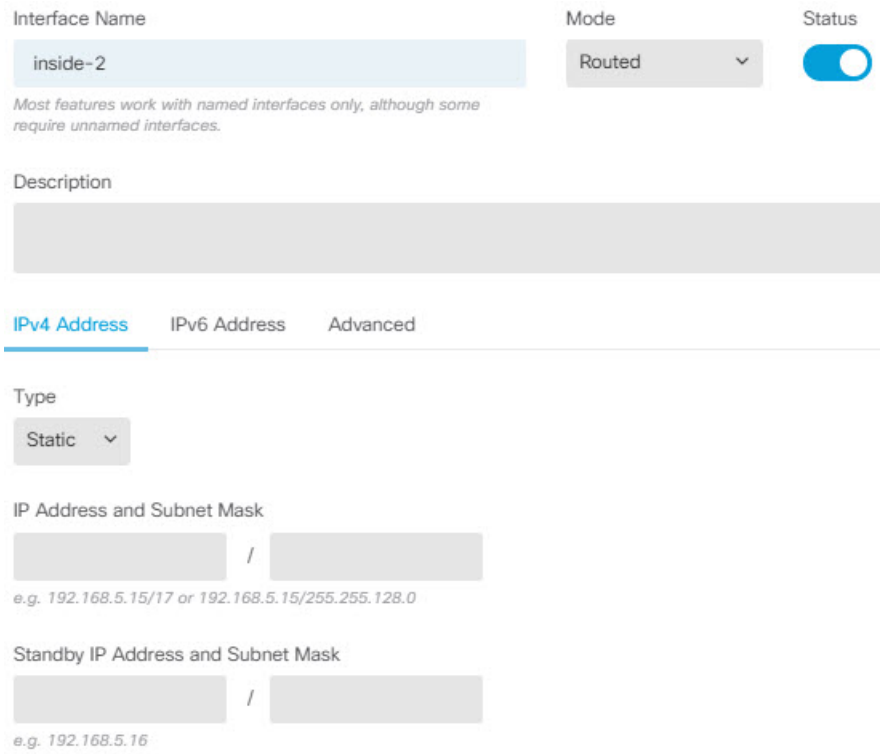
ステップ 2 仮想ルータ 2（VR2）の inside-2 インターフェイスを設定しますが、IP アドレスは指定しないでください。

a) [インターフェイス（Interface）] リストページで、VR2 に割り当てるインターフェイスの [アクション（Action）] 列にある編集アイコン（）をクリックします。

b) 少なくとも次のプロパティを設定します。

- [名前（Name）]：この例では **inside-2**。
- [モード（Mode）]：[ルーテッド（Routed）] を選択します。

- [ステータス（Status）]：インターフェイスを有効にします。
- [IPv4アドレスタイプ（IPv4 Address Type）]> ：[スタティック（Static）] を選択します。
- [IPv4アドレスとサブネットマスク（IPv4 Address and Subnet Mask）]：これらのフィールドは空欄のままにします。この時点で inside インターフェイスと同じアドレスを設定しようとすると、システムによってエラーメッセージが表示され、機能しない設定は作成できなくなります。同じルータ内の異なるインターフェイスを介して同じアドレス空間にルーティングすることはできません。



c) [OK] をクリックします。

ステップ 3 外部インターフェイスへのスタティック デフォルト ルート リークを含む、仮想ルータ VR1 を設定します。

a) [デバイス（Device）] をクリックしてから、[ルーティング（Routing）] のサマリーで [設定の表示（View Configuration）] をクリックします。
b) ルーティングページの上部にある [複数の仮想ルータの追加（Add Multiple Virtual Router）] をクリックします。
c) 説明パネルの右下にある [最初のカスタム仮想ルータの作成（Create First Custom Virtual Router）] をクリックします。
d) 仮想ルータ VR1 のプロパティを入力します。

- [名前（Name）]：VR1 または選択した別の名前を入力します。

- [インターフェイス（Interfaces）]：[+] をクリックし、**inside** を選択して [OK] をクリックします。

e) [OK] をクリックします。

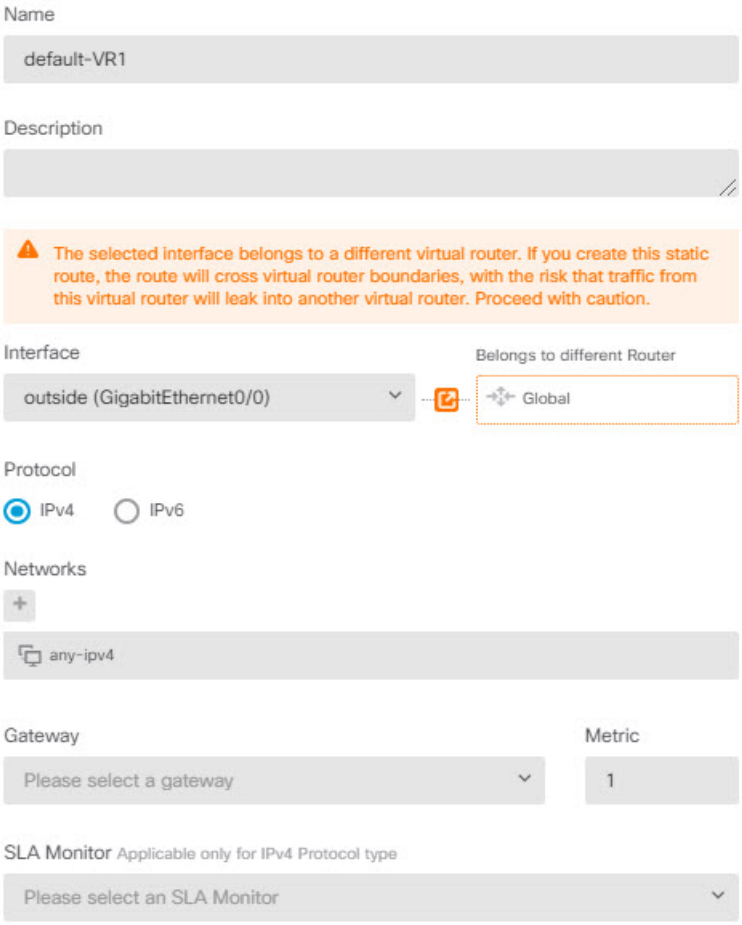
ダイアログボックスが閉じ、仮想ルータのリストが表示されます。

f) 仮想ルータのリストで、VR1 仮想ルータの [アクション（Action）] 列にある [表示（view）] アイコン（）をクリックします。

g) [スタティックルーティング（Static Routing）] タブで、[+] をクリックしてルートを設定します。

- [名前（Name）]：**default-VR1** などの任意の名前を指定します。
- [インターフェイス（Interface）]：**outside** を選択します。インターフェイスが別のルータにあり、ルートリークを作成しているという警告が表示されます。これを今から実行します。
- [プロトコル（Protocol）]：この例では、**IPv4** を使用します。
- [ネットワーク（Networks）]：**any-ipv4** オブジェクトを選択します。これは、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。
- [ゲートウェイ（Gateway）]：この項目は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、ゲートウェイアドレスを選択しません。

次のようなダイアログが表示されるはずです。



h) [OK] をクリックします。

ステップ 4 外部インターフェイスへのスタティック デフォルト ルート リークを含む、仮想ルータ VR2 を設定します。

a) VR1 を表示している場合は、戻るボタン（⮌）をクリックして仮想ルータのリストに戻ります。

b) リストの先頭にある [+] をクリックします。

c) 仮想ルータ VR2 のプロパティを入力します。

- [名前（Name）]：VR2 または選択した別の名前を入力します。
- [インターフェイス（Interfaces）]：[+] をクリックし、**inside-2** を選択して [OK] をクリックします。

d) [OK] をクリックします。

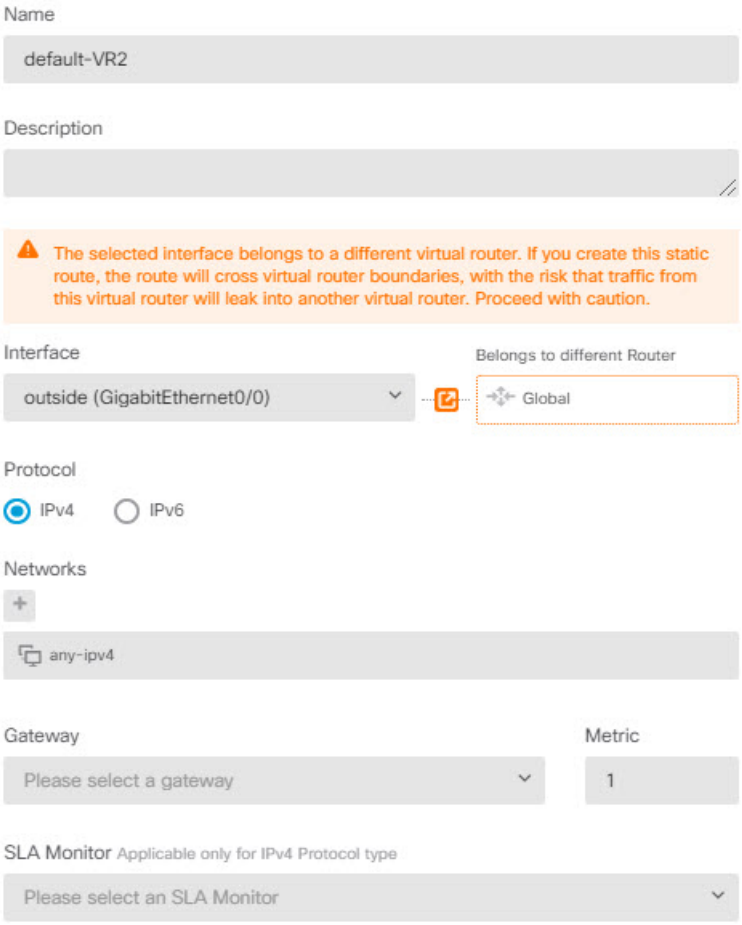
ダイアログボックスが閉じ、仮想ルータのリストが表示されます。

e) 仮想ルータのリストで、VR2 仮想ルータの [アクション（Action）] 列にある [表示（view）] アイコン（ ）をクリックします。

f) [スタティックルーティング（Static Routing）] タブで、[+] をクリックしてルートを設定します。

- [名前（Name）]：**default-VR2** などの任意の名前を指定します。
- [インターフェイス（Interface）]：**outside** を選択します。インターフェイスが別のルータにあり、ルートリークを作成しているという警告が表示されます。これを今から実行します。
- [プロトコル（Protocol）]：この例では、**IPv4** を使用します。
- [ネットワーク（Networks）]：**any-ipv4** オブジェクトを選択します。これは、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。
- [ゲートウェイ（Gateway）]：この項目は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、ゲートウェイアドレスを選択しません。

次のようなダイアログが表示されるはずです。

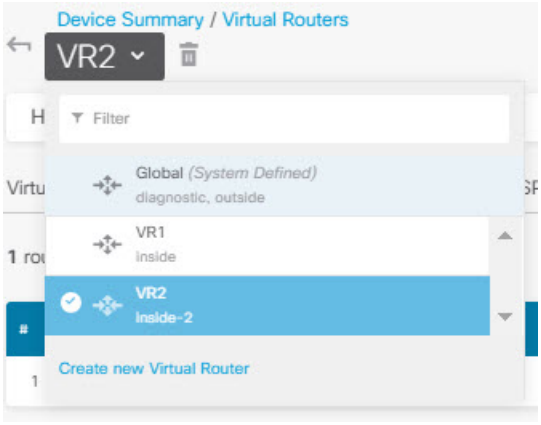


g) [OK] をクリックします。

ステップ 5 外部インターフェイスへのグローバルルータのデフォルトルートを作成します。

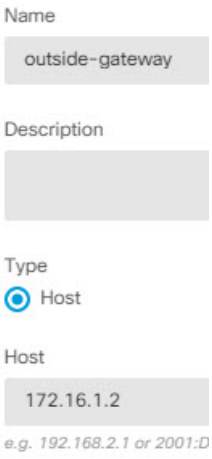
このルートの目的は、2 つの仮想ルータからグローバルルータの外部インターフェイスへのトラフィックリークに適切なゲートウェイを割り当てることです。

a) VR2 を表示している場合は、ページの上部にある VR2 の名前をクリックして仮想ルータのリストを開き、グローバルルータを選択します。

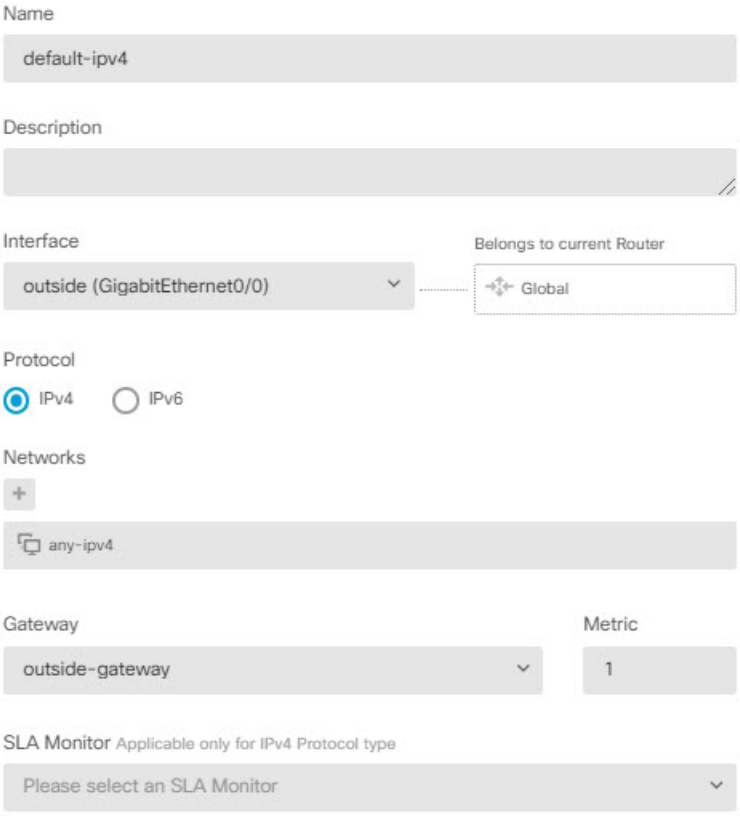


b) グローバルルータの [スタティックルーティング（Static Routing）] タブで、[+] をクリックしてルートを設定します。

- [名前（Name）]：default-ipv4 などの任意の名前を指定します。
- [インターフェイス（Interface）]：**outside** を選択します。
- [プロトコル（Protocol）]：この例では、**IPv4** を使用します。
- [ネットワーク（Networks）]：**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）]：オブジェクトがまだ存在していないと仮定して、[新規ネットワークオブジェクトの作成（Create New Network Object）] をクリックし、外部インターフェイス（この場合は 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、そのオブジェクトをスタティックルートの [ゲートウェイ（Gateway）] フィールドで選択します。



次のようなダイアログが表示されるはずです。



c) [OK] をクリックします。

ステップ 6 [インターフェイス（Interface）] ページに戻り、inside-2 に IP アドレスを追加します。

a) [デバイス（Device）] をクリックしてから、[インターフェイス（Interfaces）] サマリーにある [すべてのインターフェイスを表示（View All Interfaces）] リンクをクリックします。

b) VR2 に割り当てる inside-2 インターフェイスの [アクション（Action）] 列にある編集アイコン（）をクリックします。

c) [IPv4アドレス（IPv4 Address）] タブで、IP アドレスとサブネットマスクとして 192.168.1.1/24 と入力します。

d) [OK] をクリックします。

この時点では、inside および inside-2 インターフェイスが別の仮想ルータにあるため、重複する IP アドレスに対するエラーは発生しません。

ステップ 7 inside to outside 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。

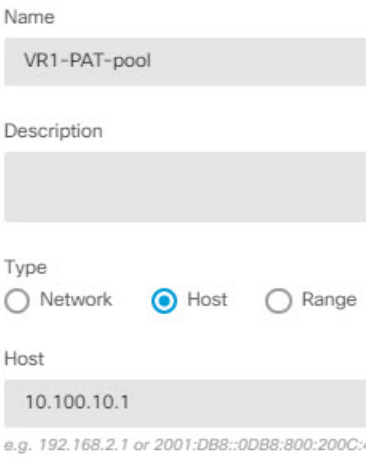
a) [ポリシー（Policies）] を選択し、[NAT] をクリックします。

b) 内部から外部インターフェイスに InsideOutsideNatRule という名前の手動 NAT ルールがすでに存在する場合、インターフェイス PAT を適用するには、ルールの編集アイコン（）をクリックします。そうでない場合は、[+] をクリックして新しいルールを作成します。

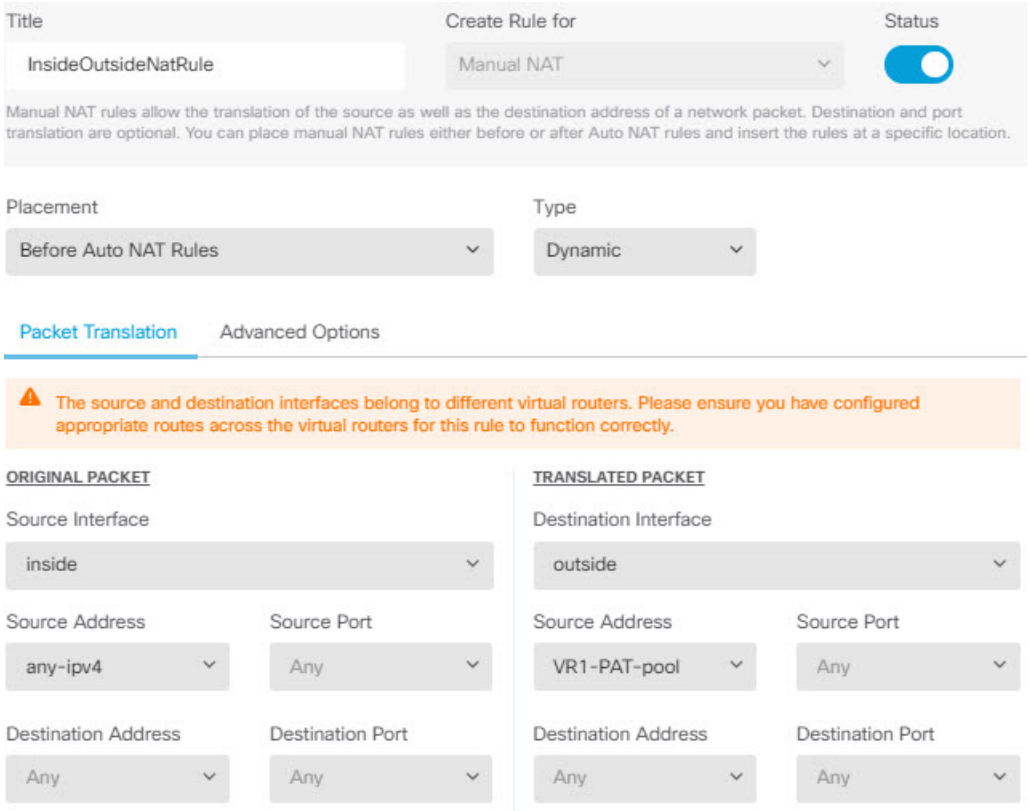
既存のルールを編集する場合は、送信元インターフェイスと宛先インターフェイスが異なる仮想ルータにあり、ルートを定義する必要があることを示す警告が表示されることに注意してください。これは、前の手順で行ったものです。

c) 既存のルールを編集する場合は、**[変換済みパケット（Translated Packet）]** > **[送信元アドレス（Source Address）]** のドロップダウン矢印をクリックし、[新規ネットワークの作成（Create New Network）] をクリックします（10.100.10.1 を定義しているホストオブジェクトがない場合）。

d) PAT アドレスのホスト ネットワーク オブジェクトを設定します。オブジェクトは次のようになります。



e) **[変換済みパケット（Translated Packet）]** > **[送信元アドレス（Source Address）]** として新しいオブジェクトを選択します。NAT ルールは次のようになります。



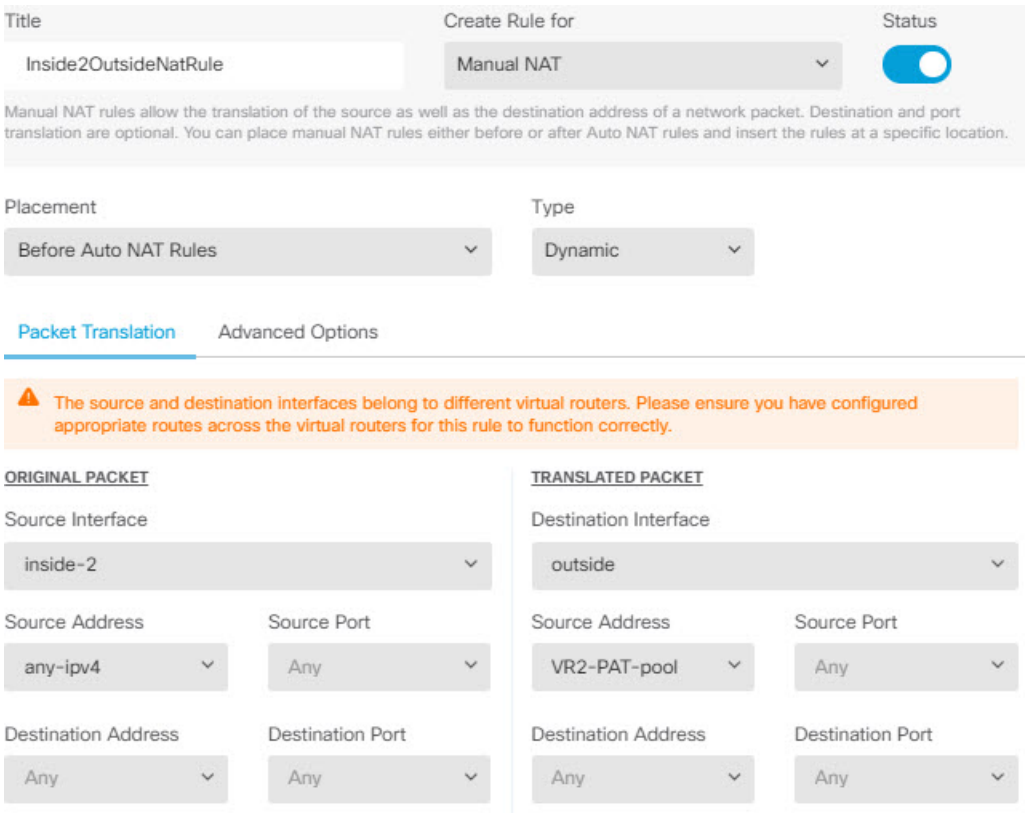
f) [OK] をクリックします。

ステップ 8 NAT ルールを作成して、inside-2 to outside トラフィックの 10.100.10.2 PAT を実行します。

このルールは、VR1 のルールとまったく同じように表示されますが、次の例外があります。

- [名前（Name）]：一意である必要があります（たとえば、Inside2OutsideNatRule）。
- **[元のパケット（Original Packet）]** > **[送信元インターフェイス（Source Interface）]**：inside-2 を選択します。
- **[変換済みパケット（Translated Packet）]** > **[送信元アドレス（Source Address）]**：10.100.10.2 の新しいホスト ネットワーク オブジェクトを作成します。

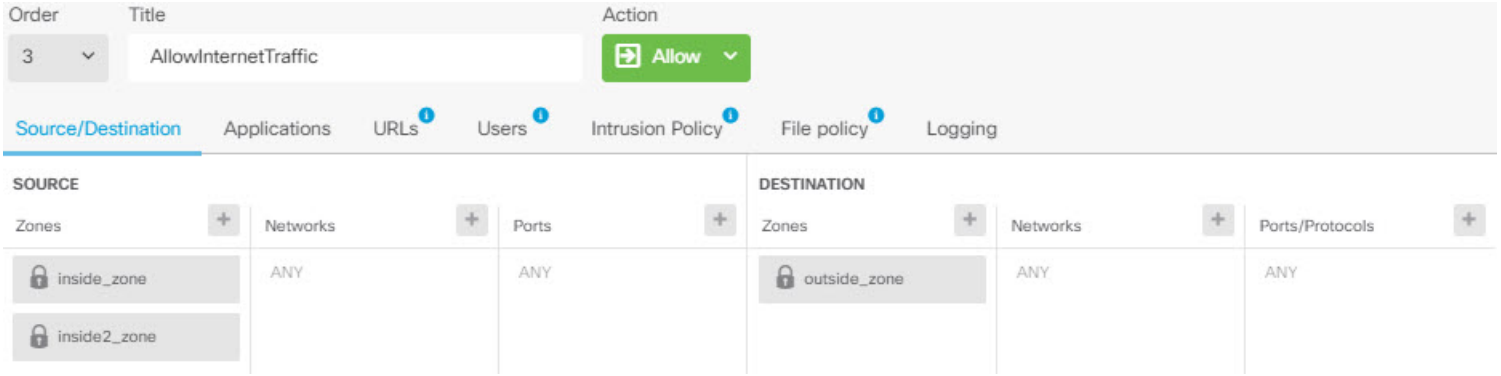
ルールは次のようになります。



ステップ 9 **[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** を選択し、inside_zone および inside2_zone からのトラフィックを outside_zone に許可するアクセス制御ルールを設定します。

最後に、inside インターフェイスと inside-2 インターフェイスから outside インターフェイスへのトラフィックを許可するようにアクセス コントロール ポリシーを設定する必要があります。アクセス制御ルールではセキュリティゾーンを使用する必要があるため、これらのインターフェイスごとにゾーンを作成する必要があります。または、inside と inside-2 の両方を保持する単一のゾーンを作成することもできますが、これらのルータでトラフィックがどのように処理されるかを区別するために、このポリシーまたは他のポリシーで追加のルールを作成することになるでしょう。

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。このルールには、適切な侵入ポリシーを適用できます。たとえば、URL フィルタリングを実装するために、不要なトラフィックをブロックする追加のルールを定義できます。



仮想ルータのモニタリング

仮想ルータをモニタし、トラブルシューティングを行うには、CLI コンソールを開くか、またはデバイスの CLI にログインして、次のコマンドを使用します。また、[ルーティング（Routing）] ページの [コマンド（Commands）] メニューから、これらのコマンドの一部を選択することもできます。

- **show vrf** システムで定義されている仮想ルータの情報を表示します。
- **show ospf** ［**vrf** *name* | **all**］

  仮想ルータの OSPF プロセスに関する情報を表示します。仮想ルータを指定して、その仮想ルータ内のプロセスに関する情報のみを表示するか、オプションを省略して、すべての仮想ルータにわたる VRF に関する情報を表示することができます。追加オプションを表示するには、**show ospf ?** を使用します。
- **show bgp** ［**vrf** *name* | **all**］

  仮想ルータの BGP プロセスに関する情報を表示します。仮想ルータを指定して、その仮想ルータ内のプロセスに関する情報のみを表示するか、オプションを省略して、すべての仮想ルータにわたる VRF に関する情報を表示することができます。追加オプションを表示するには、**show bgp ?** を使用します。
- **show eigrp** *option*

  EIGRP プロセスに関する情報を表示します。使用可能なオプションを表示するには、**show eigrp ?** を使用します。

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。