仮想ルータのセットアップ

以下のトピックでは、Firepower システムで仮想ルータをセットアップする方法について説明します。

- 仮想ルータ （1 ページ）
- ルーテッド インターフェイス （2 ページ）
- 物理ルーテッド インターフェイスの設定 （3 ページ）
- 論理ルーテッドインターフェイスの追加 （6 ページ）
- 論理ルーテッド インターフェイスの削除 （9 ページ）
- SFRP の設定 （10 ページ）
- 仮想ルータ設定 （12 ページ）
- 仮想ルータの追加 （13 ページ）
- DHCP リレー （14 ページ）
- スタティック ルート （16 ページ）
- ダイナミック ルーティング （19 ページ）
- 仮想ルータのフィルタ （34 ページ）
- 仮想ルータ認証プロファイルの追加 （37 ページ）
- 仮想ルータ統計情報の表示 （38 ページ）
- 仮想ルータの削除 （39 ページ）

仮想ルータ

レイヤ3展開の管理対象デバイスは、2つ以上のインターフェイス間のトラフィックをルーティングするように設定できます。トラフィックをルーティングするには、IP アドレスを各インターフェイスに割り当ててから、これらのインターフェイスを仮想ルータに割り当てる必要があります。仮想ルータに割り当てるインターフェイスは、物理インターフェイス、論理インターフェイス、または Link Aggregation Group（LAG）インターフェイスのいずれかにできます。

システムは、宛先アドレスに従ってパケット転送の決定を行うことで、パケットをルーティングするように設定できます。ルーテッドインターフェイスとして設定されたインターフェイスは、レイヤ3トラフィックを受信し、転送します。ルータは転送基準に基づいて発信インター

フェイスから宛先を取得し、アクセス コントロール ルールが、適用するセキュリティ ポリシーを指定します。

レイヤ 3 展開では、スタティック ルートを定義できます。また、Routing Information Protocol（RIP）および Open Shortest Path First（OSPF）のダイナミック ルーティング プロトコルを設定できます。さらに、スタティック ルートと RIP、またはスタティック ルートと OSPF の組み合わせを設定することもできます。

7000 または 8000 シリーズ デバイス上には、仮想ルータ、物理ルーテッド インターフェイス、または論理ルーテッド インターフェイスしか設定できないことに注意してください。

⚠

注意 レイヤ 3 展開に何らかの理由で障害が発生した場合、デバイスはトラフィックを転送しなくなります。

関連トピック

LAG 設定

ルーテッド インターフェイス

物理的設定または論理的設定のいずれかでルーテッド インターフェイスをセットアップできます。タグのない VLAN トラフィックを処理するために、物理的ルーテッド インターフェイスを設定できます。指定された VLAN タグのあるトラフィックを処理するために、論理的ルーテッド インターフェイスも作成できます。

レイヤ 3 の展開では、システムは待機しているルーテッド インターフェイスのない外部の物理的インターフェイスから受信したトラフィックをドロップします。このシステムでは、以下の場合パケットをドロップします。

- VLAN タブのないパケットを受信した場合、そのポート向けにルーテッド インターフェイスを設定したことがない場合。
- VLAN タグ付きパケットを受信した場合、そのポートの論理的ルーテッド インターフェイスを設定したことがない場合。

このシステムでは、ルールを評価するか、決定を転送する前にイングレスの最も外側の VLAN タグを削除して、スイッチ インターフェイス上で VLAN タグで受信したトラフィックを処理します。VLAN タグ付きの論理的ルーテッド インターフェイスを介してデバイスに残っているパケットは、イーグレスの関連付けられた VLAN タブによりカプセル化します。このシステムでは、削除プロセスの完了後、VLAN タブで受信したトラフィックをドロップします。

スタティック Address Resolution Protocol（ARP）エントリをルーテッド インターフェイスに追加できます。外部ホストは、トラフィックの送信先となるローカル ネットワーク上の宛先 IP アドレスの MAC アドレスを知る必要がある場合は、ARP 要求を送信します。スタティック ARP エントリを設定する場合、仮想ルータは IP アドレスや関連付けられた MAC アドレスに応答します。

論理ルーテッドLAGインターフェイスの[ICMP有効応答（ICMP Enable Responses）]オプションを無効にしても、すべてのシナリオでICMP応答が抑制されるわけではありません。宛先IPがルーテッド インターフェイスのIPで、プロトコルがICMPであるパケットをドロップするように、アクセス コントロール ポリシーにネットワークベースのルールを追加できます。

管理対象デバイスの[ローカル ルータ トラフィックを検査する（Inspect Local Router Traffic）]オプションを有効にすると、システムは、ホストに到着する前にパケットをドロップし、これによっていかなる応答も阻止できます。

MTU値の範囲は管理対象デバイスのモデルとインターフェイス タイプによって異なる場合があります。

注意 デバイス上のすべての非管理インターフェイスの中で最大MTU値を変更し、設定変更を展開すると、Snortプロセスが再起動され、トラフィック インスペクションが一時的に中断されます。インスペクションは、変更したインターフェイスだけでなく、すべての非管理インターフェイスで中断されます。この中断によってトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびインターフェイスのタイプに応じて異なります。詳細については、Snort® の再起動によるトラフィックの動作を参照してください。

上位の物理的インターフェイスをインラインまたはパッシブに変更する場合、システムでは、関連付けられた論理的インターフェイをすべて削除します。

関連トピック

- デバイスの詳細設定
- 7000 および 8000 シリーズ デバイスおよび NGIPSv の MTU 範囲
- Snort® の再起動シナリオ

物理ルーテッド インターフェイスの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
該当なし	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

ルーテッド インターフェイスとして管理対象デバイスの1つ以上の物理ポートを設定できます。トラフィックをルーティングする前に、物理ルーテッドインターフェイスを仮想ルータに割り当てる必要があります。

⚠

注意 ルーテッド インターフェイス ペアを 7000 または 8000 シリーズ デバイスに追加すると、設定の変更を展開する際に Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、ターゲットデバイスがトラフィックを処理する方法に応じて異なります。詳細はSnort® の再起動によるトラフィックの動作を参照してください。

手順

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 変更するデバイスの横にある編集アイコン（）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 変更するインターフェイスの横にある編集アイコン（）をクリックします。

ステップ 4 [ルーテッド（Routed）] をクリックして、ルーテッド インターフェイス オプションを表示します。

ステップ 5 セキュリティ ゾーンを適用するには、次のいずれかを実行します。

- [セキュリティ ゾーン（Security Zone）] ドロップダウン リストから既存のセキュリティ ゾーンを選択します。
- [新規（New）] を選択して新しいセキュリティ ゾーンを追加します。セキュリティ ゾーンおよびインターフェイス グループ オブジェクトの作成 を参照してください。

ステップ 6 仮想ルータを指定するには、次のいずれかを実行します。

- [仮想ルータ（Virtual Router）] ドロップダウン リストから既存の仮想ルータを選択します。
- [新規（New）] を選択して新しい仮想ルータ 仮想ルータの追加 （13 ページ）を追加します。

ステップ 7 ルーテッド インターフェイスにトラフィックを処理させるには、[有効（Enabled）] チェックボックスをオンにします。このチェックボックスをオフにすると、インターフェイスは無効になり、ユーザはセキュリティ上の理由によりアクセスできなくなります。

ステップ 8 [モード（Mode）] ドロップダウン リストからリンク モードを指定するオプションを選択するか、または[自動ネゴシエーション（Auto Negotiation）]を選択して、速度とデュプレックス設定を自動的にネゴシエートするようインターフェイスを設定します。

モード設定は銅線インターフェイスにのみ使用できます。

8000 シリーズアプライアンスのインターフェイスは、半二重オプションをサポートしません。

ステップ 9 [MDI/MDIX] ドロップダウン リストから、インターフェイスの設定対象として MDI（メディア依存型インターフェイス）、MDIX（メディア依存型インターフェイス クロスオーバー）、または自動 MDIX のいずれかを指定するオプションを選択します。

通常、[MDI/MDIX] は [自動 MDIX（Auto-MDIX）] に設定します。これにより、MDI と MDIX の間の切り替えが自動的に処理され、リンクが確立されます。

[MDI/MDIX] 設定は銅線インターフェイスでのみ使用できます。

ステップ 10 [MTU] フィールドに、最大伝送ユニット（MTU）を入力して、パケットの最大許容サイズを指定します。

MTU はレイヤ 2 MTU/MRU であり、レイヤ 3 MTU ではありません。

MTU 値の範囲は管理対象デバイスのモデルとインターフェイス タイプによって異なる場合があります。

注意 デバイス上のすべての非管理インターフェイスの中で最大 MTU 値を変更し、設定変更を展開すると、Snort プロセスが再起動され、トラフィック インスペクションが一時的に中断されます。インスペクションは、変更したインターフェイスだけでなく、すべての非管理インターフェイスで中断されます。この中断によってトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびインターフェイスのタイプに応じて異なります。詳細については、Snort® の再起動によるトラフィックの動作を参照してください。

ステップ 11 [ICMP] の横にある [応答を有効にする（Enable Responses）] チェックボックスをオンにして、インターフェイスを ping や traceroute などの ICMP トラフィックに応答可能にします。

ステップ 12 [IPv6 NDP] の横にある [ルータ アドバタイズメントを有効にする（Enable Router Advertisement）] チェックボックスをオンにして、インターフェイスがルータ アドバタイズメントを伝送できるようにします。

ステップ 13 IP アドレスを追加するには、[追加（Add）] をクリックします。

ステップ 14 [アドレス（Address）] フィールドに、ルーテッド インターフェイスの IP アドレスとサブネット マスクを CIDR 表記で入力します。

次の点に注意してください。

- ネットワークおよびブロードキャスト アドレス、またはスタティック MAC アドレス 00:00:00:00:00:00 および FF:FF:FF:FF:FF:FF は追加できません。
- サブネット マスクに関係なく、仮想ルータのインターフェイスに同じ IP アドレスを追加できません。

ステップ 15 組織が IPv6 アドレスを使用している場合、インターフェイスの IP アドレスを自動的に設定するには、[IPv6] フィールドの横の [アドレス自動設定（Address Autoconfiguration）] チェックボックスをオンにします。

ステップ 16 [タイプ（Type）] には、[普通（Normal）] または [SFRP] を選択します。

SFRP オプションの詳細についてはSFRP の設定 （10 ページ）を参照してください。

ステップ 17 [OK] をクリックします。

- IP アドレスを編集するには、編集アイコン（  ）をクリックします。
- IP アドレスを削除するには、削除アイコン（  ）をクリックします。

IP アドレスを 7000 または 8000 シリーズ デバイスのルーテッド インターフェイスに追加する場合、ハイアベイラビリティ ペア ピアのルーテッドインターフェイスに対応する IP アドレスを追加する必要があります。

ステップ 18 スタティック ARP エントリを追加するには、[追加（Add）] をクリックします。

ステップ 19 [IP アドレス（IP Address）] フィールドに、スタティック ARP エントリの IP アドレスを入力します。

ステップ 20 [MAC アドレス（MAC Address）] フィールドに、IP アドレスに関連付ける MAC アドレスを入力します。2 桁の 16 進数の 6 個のグループをコロンで区切る標準アドレス形式を使用します（たとえば、01:23:45:67:89:AB）。

ステップ 21 [OK] をクリックします。

ステップ 22 [保存（Save）] をクリックします。

次のタスク

設定変更を展開します。設定変更の展開を参照してください。

関連トピック

7000 および 8000 シリーズ デバイスおよび NGIPSv の MTU 範囲
Snort® の再起動シナリオ

論理ルーテッドインターフェイスの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
該当なし	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

各物理ルーテッド インターフェイスで、複数の論理ルーテッド インターフェイスを追加できます。物理インターフェイスで受信した VLAN タグ付きのトラフィックは、各論理インターフェイスにその特定のタグが関連付けられていなければ処理されません。トラフィックをルーティングするには、論理ルーテッドインターフェイスを仮想ルータに割り当てる必要があります。

⚠

注意 7000 または 8000 シリーズ デバイス 設定の変更を展開する際に Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、ターゲットデバイスがトラフィックを処理する方法に応じて異なります。詳細はSnort® の再起動によるトラフィックの動作を参照してください。 でのルーテッド インターフェイス ペアの追加

手順

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 変更するデバイスの横にある編集アイコン（  ）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [インターフェイスの追加（Add Interface）] をクリックします。

ステップ 4 [ルーテッド（Routed）] をクリックして、ルーテッド インターフェイス オプションを表示します。

ステップ 5 [インターフェイス（Interface）] ドロップダウン リストから、論理インターフェイスを追加する物理インターフェイスを選択します。

ステップ 6 [VLAN タグ（VLAN Tag）] フィールドで、このインターフェイス上のインバウンド/アウトバウンド トラフィックに割り当てるタグ値を入力します。この値には、1 ～ 4094 の任意の整数を指定できます。

ステップ 7 セキュリティ ゾーンを適用するには、次のいずれかを実行します。

- [セキュリティ ゾーン（Security Zone）] ドロップダウン リストから既存のセキュリティ ゾーンを選択します。
- [新規（New）] を選択して新しいセキュリティ ゾーンを追加します。セキュリティ ゾーンおよびインターフェイス グループ オブジェクトの作成 を参照してください。

ステップ 8 仮想ルータを指定するには、次のいずれかを実行します。

- [仮想ルータ（Virtual Router）] ドロップダウン リストから既存の仮想ルータを選択します。
- [新規（New）] を選択して新しい仮想ルータ 仮想ルータの追加 （13 ページ）を追加します。

ステップ 9 ルーテッド インターフェイスにトラフィックを処理させるには、[有効（Enabled）] チェックボックスをオンにします。

このチェックボックスをオフにすると、インターフェイスは無効になり、管理上はダウンした状態になります。物理インターフェイスを無効にする場合、それに関連付けられているすべての論理インターフェイスも無効にします。

ステップ 10 [MTU] フィールドに、最大伝送ユニット（MTU）を入力して、パケットの最大許容サイズを指定します。

MTU はレイヤ 2 MTU/MRU であり、レイヤ 3 MTU ではありません。

MTU 値の範囲は管理対象デバイスのモデルとインターフェイス タイプによって異なる場合があります。

注意 デバイス上のすべての非管理インターフェイスの中で最大 MTU 値を変更し、設定変更を展開すると、Snort プロセスが再起動され、トラフィック インスペクションが一時的に中断されます。インスペクションは、変更したインターフェイスだけでなく、すべての非管理インターフェイスで中断されます。この中断によってトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびインターフェイスのタイプに応じて異なります。詳細については、Snort® の再起動によるトラフィックの動作を参照してください。

ステップ 11 [ICMP] の横にある [応答を有効にする（Enable Responses）] チェックボックスをオンにして、他のルータ、中間デバイス、またはホストに更新またはエラー情報を伝送します。

ステップ 12 [IPv6 NDP] の横にある [ルータ アドバタイズメントを有効にする（Enable Router Advertisement）] チェックボックスをオンにして、インターフェイスがルータ アドバタイズメントを伝送できるようにします。

ステップ 13 IP アドレスを追加するには、[追加（Add）] をクリックします。

ステップ 14 [アドレス（Address）] フィールドに、IP アドレスを CIDR 表記で入力します。

次の点に注意してください。

- ネットワークおよびブロードキャスト アドレス、またはスタティック MAC アドレス 00:00:00:00:00:00 および FF:FF:FF:FF:FF:FF は追加できません。
- サブネット マスクに関係なく、仮想ルータのインターフェイスに同じ IP アドレスを追加できません。

ステップ 15 IPv6 を使用した環境で、インターフェイスの IP アドレスを自動設定するには、[IPv6] フィールドの横にある [アドレスの自動設定（Address Autoconfiguration）] チェックボックスを選択します。

ステップ 16 [タイプ（Type）] には、[普通（Normal）] または [SFRP] を選択します。

SFRP オプションの詳細についてはSFRP の設定 （10 ページ）を参照してください。

ステップ 17 [OK] をクリックします。

- IP アドレスを編集するには、編集アイコン（  ）をクリックします。
- IP アドレスを削除するには、削除アイコン（  ）をクリックします。

IP アドレスを 7000 または 8000 シリーズ デバイスの高可用性ペアのルーテッド インターフェイスに追加する場合、高可用性ペアピアのルーテッド インターフェイスに対応する IP アドレスを追加する必要があります。

ステップ 18 スタティック ARP エントリを追加するには、[追加（Add）] をクリックします。

ステップ 19 [IP アドレス（IP Address）] フィールドに、スタティック ARP エントリの IP アドレスを入力します。

ステップ 20 [MAC アドレス（MAC Address）] フィールドに、IP アドレスに関連付ける MAC アドレスを入力します。2 桁の 16 進数の 6 個のグループをコロンで区切る標準アドレス形式を使用します（たとえば、01:23:45:67:89:AB）。

ステップ 21 [OK] をクリックします。スタティック ARP エントリが追加されます。

ステップ 22 [保存（Save）] をクリックします。

次のタスク

設定変更を展開します。設定変更の展開を参照してください。

関連トピック

7000 および 8000 シリーズ デバイスおよび NGIPSv の MTU 範囲
Snort® の再起動シナリオ

論理ルーテッド インターフェイスの削除

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

論理ルーテッドインターフェイスを削除すると、帰属する物理インターフェイスのほか、割り当てられた仮想ルータおよびセキュリティ ゾーンからも削除されます。

手順

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 変更するデバイスの横にある編集アイコン（  ）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 削除する論理ルーテッドインターフェイスの横にある削除アイコン（  ）をクリックします。

ステップ 4 入力を求められた場合、インターフェイスを削除することを確認します。

次のタスク

- 設定変更を展開します。設定変更の展開を参照してください。

SFRP の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

Cisco 冗長プロトコル（SFRP）を設定して、7000 または 8000 シリーズ デバイスのハイ アベイラビリティ ペアまたは個別のデバイスのハイ アベイラビリティを得るためのネットワーク冗長性を実現できます。SFRP は IPv4 と IPv6 の両方のアドレスのゲートウェイ冗長性を提供します。ルーテッド インターフェイスおよびハイブリッド インターフェイスの SFRP を設定できます。

インターフェイスが個別のデバイスに設定される場合、同じブロードキャスト ドメインに存在する必要があります。インターフェイスのうち少なくとも 1 つをマスターに指定し、同じ数をバックアップとして指定する必要があります。システムは IP アドレスごとに 1 つのマスターと 1 つのバックアップのみをサポートします。ネットワーク接続が失われた場合、システムは自動的にバックアップをマスターに昇格し、接続を維持します。

SFRP に設定するオプションは、SFRP インターフェイス グループのすべてのインターフェイスで同じにする必要があります。グループ内の複数の IP アドレスのマスターとバックアップの状態は同じである必要があります。そのため、IP アドレスを追加または編集する場合、そのアドレスに設定する状態はグループ内のすべてのアドレスに適用されます。セキュリティのために、グループ内のインターフェイス間で共有される [グループ ID（Group ID）] と [共有秘密（Shared Secret）] の値を入力する必要があります。

仮想ルータで SFRP IP アドレスを有効にするには、1 つの非 SFRP IP アドレスを設定する必要もあります。インターフェイスごとに、非 SFRP アドレスを 1 つだけ設定する必要があることにご注意ください。

あるグループに含まれる SFRP はすべて一緒にフェールオーバーするので、同じ仮想ルータ上のすべての SFRP は同じ SFRP グループに属する必要があります。さらに、NAT、HA 状態共有、または VPN を使用している場合は、高可用性ペアの各デバイスに HA リンク インターフェイスを設定する必要もあります。HA リンク インターフェイスの詳細については、HA リンク インターフェイスの設定を参照してください。

高可用性ペアの 7000 または 8000 シリーズ デバイスの場合、共有秘密を指定すると、SFRP の IP 設定とともに高可用性ペアのピアにコピーされます。共有秘密は、ピアのデータを認証します。

（注） 7000 または 8000 シリーズ デバイスのハイ アベイラビリティ ペアのルーティングされたインターフェイスまたはハイブリッドインターフェイスで SFRP IP アドレスがすでに 1 つ構成されている場合、複数の非 SFRP IP アドレスを有効にすることは推奨しません。7000 または 8000 シリーズ デバイスのハイ アベイラビリティ ペアがスタンバイ モードでフェールオーバーした場合、NAT は実行されません。

手順

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 変更するデバイスの横にある編集アイコン（）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 SFRP を設定するインターフェイスの横にある編集アイコン（）をクリックします。

ステップ 4 SFRP を設定するインターフェイスのタイプ（[ルーテッド（Routed）] または [ハイブリッド（Hybrid）]）を選択します。

ステップ 5 IP アドレスを追加または編集するときに SFRP を設定できます。[追加（Add）] をクリックして、IP アドレスを追加します。IP アドレスを編集するには、編集アイコン（）をクリックします。

ステップ 6 [タイプ（Type）] に [SFRP] を選択して SFRP オプションを表示します。

ステップ 7 [グループ ID（Group ID）] フィールドに、SFRP 用に設定されたマスターまたはバックアップ インターフェイス グループを指定する値を入力します。

ステップ 8 [優先順位（Priority）] で、[マスター（Master）] または [バックアップ（Backup）] のどちらかを選択して、優先するインターフェイスを指定します。

- 個別のデバイスの場合、1 つのデバイスにマスターへのインターフェイスを 1 個設定し、2 番目のデバイスにバックアップへのインターフェイスを設定する必要があります。
- 7000 または 8000 シリーズ デバイスのハイ アベイラビリティ ペアの場合、マスターとして 1 個のインターフェイスを設定すると、もう 1 個のインターフェイスは自動的にバックアップになります。

ステップ 9 [共有秘密（Shared Secret）] フィールドに、共有秘密を入力します。

[共有秘密（Shared Secret）] フィールドには、7000 または 8000 シリーズ デバイスのハイ アベイラビリティ ペア内のグループに関するデータが自動的に入力されます。

ステップ 10 [**アドバタイズメント間隔（秒単位）（Adv. Interval (seconds)**] フィールドに、レイヤ 3 トラフィックのルート アドバタイズメントの間隔を入力します。

ステップ 11 [OK] をクリックします。

ステップ 12 [保存（Save）] をクリックします。

次のタスク

設定変更を展開します。設定変更の展開を参照してください。

関連トピック

7000 および 8000 シリーズ デバイスのハイ アベイラビリティについて

仮想ルータ設定

注意 7000 または 8000 シリーズ デバイスで仮想ルータを追加した場合 設定の変更を展開する際に Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、ターゲットデバイスがトラフィックを処理する方法に応じて異なります。詳細は Snort® の再起動によるトラフィックの動作を参照してください。

レイヤ3配置でルーテッドインターフェイスを使用する前に、仮想ルータを設定し、ルーテッドインターフェイスを割り当てる必要があります。仮想ルータは、レイヤ 3 トラフィックをルーティングするルーテッドインターフェイスのグループです。

1つの仮想ルータに割り当てることができるのは、ルーテッドインターフェイスとハイブリッドインターフェイスのみです。

最大限の TCP セキュリティを実現するため、厳格な強制を有効にすることができます。この機能は、3 ウェイ ハンドシェイクが完了していない接続をブロックします。厳密な適用では次のパケットもブロックされます。

- 3 ウェイ ハンドシェイクが完了していない接続の非 SYN TCP パケット
- 応答側が SYN-ACK を送信する前に TCP 接続の発信側から送信された非 SYN/RST パケット
- SYN の後、セッションの確立前に TCP 接続のレスポンダから送信された非 SYN-ACK/RST パケット
- 発信側または応答側のどちらかから送信された、確立された TCP 接続の SYN パケット

レイヤ3インターフェイスの設定を非レイヤ3インターフェイスに変更したり、仮想ルータからレイヤ3インターフェイスを削除したりすると、ルータは無効な状態になる場合があることに注意してください。たとえば、DHCPv6 で使用されている場合、アップストリームとダウンストリームの不一致が生じることがあります。

仮想ルータの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

[デバイス管理（Device Management）] ページの [仮想ルータ（Virtual Routers）] タブから仮想ルータを追加できます。ルーテッドインターフェイスを設定するときに、ルータを追加することもできます。

管理対象デバイスのインターフェイスを設定する前に仮想ルータを作成する場合は、空の仮想ルータを作成し、後でインターフェイスを追加できます。

⚠

注意 7000 または 8000 シリーズ デバイスで仮想ルータを追加した場合 設定の変更を展開する際に Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、ターゲットデバイスがトラフィックを処理する方法に応じて異なります。詳細は Snort® の再起動によるトラフィックの動作を参照してください。

手順

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 変更するデバイスの横にある編集アイコン（  ）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [仮想ルータ（Virtual Routers）] タブをクリックします。

ヒント デバイスが高可用性ペアのスタックにある場合、[選択済みデバイス（Selected Device）] ドロップダウン リストから、変更するスタックを選択します。

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 [名前（Name）] フィールドに仮想ルータの名前を入力します。英数字とスペースを使用できます。

ステップ 6 [IPv6 サポート（IPv6 Support）] チェックボックスをオンまたはオフにして、仮想ルータで IPv6 スタティック ルーティング、OSPFv3 と RIPng を設定します。

ステップ 7 TCP の厳密な適用をやめるには、[TCP の厳密な適用（Strict TCP Enforcement）] チェックボックスをオフにします。このオプションは、デフォルトで有効です。

ステップ 8 [インターフェイス（Interfaces）] の [使用可能（Available）] リストから 1 つまたは複数のインターフェイスを選択し、[追加（Add）] をクリックします。

[使用可能（Available）] リストには、仮想ルータに割り当てることが可能なデバイス上のすべての有効なレイヤ 3 インターフェイス（ルーテッドおよびハイブリッド）が含まれます。

ヒント 仮想ルータからルーテッドまたはハイブリッドインターフェイスを削除するには、削除アイコン（）をクリックします。[インターフェイス（Interfaces）] タブで、設定したインターフェイスを無効にすることによっても削除できます。

ステップ 9 [保存（Save）] をクリックします。

次のタスク

- 設定変更を展開します。設定変更の展開を参照してください。

DHCP リレー

DHCP はインターネット ホストに設定パラメータを提供します。IP アドレスを未取得の DHCP クライアントは、ブロードキャスト ドメインの外にある DHCP サーバと直接通信できません。DHCP クライアントが DHCP サーバと通信できるようにするには、クライアントがサーバと同じブロードキャスト ドメイン内にない状況に対応できるように DHCP リレー インスタンスを設定します。

ユーザは、設定するそれぞれの仮想ルータに対して DHCP リレーを設定できます。デフォルトでは、この機能は無効になっています。DHCPv4 リレーまたは DHCPv6 リレーのどちらかを有効にできます。

（注） 同じデバイスで実行中の複数の仮想ルータを介して DHCPv6 リレー チェーンを実行することはできません。

DHCPv4 リレーの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

次の手順は、仮想ルータで DHCPv4 リレーを設定する方法について説明します。

手順

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 変更するデバイスの横にある編集アイコン（  ）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [仮想ルータ（Virtual Routers）] タブをクリックします。

ステップ 4 変更する仮想ルータの横にある編集アイコン（  ）をクリックします。

ステップ 5 [DHCPv4（DHCPv6）] チェックボックスをオンにします。

ステップ 6 [サーバ（Servers）] フィールドに、サーバの IP アドレスを入力します。

ステップ 7 [追加（Add）] をクリックします。

最大 4 台の DHCP サーバを追加できます。

ステップ 8 [最大ホップ（Max Hops）] フィールドに 1 ～ 255 の最大ホップ カウントを入力します。

ステップ 9 [保存（Save）] をクリックします。

次のタスク

- 設定変更を展開します。設定変更の展開を参照してください。

DHCPv6 リレーの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

同じデバイスで実行中の複数の仮想ルータを介して DHCPv6 リレー チェーンを実行することはできません。

手順

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 変更するデバイスの横にある編集アイコン（  ）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [仮想ルータ（Virtual Routers）] タブをクリックします。

ステップ 4 DHCP リレーを設定する仮想ルータの横にある編集アイコン（  ）をクリックします。

ステップ 5 [DHCPv6] チェックボックスをオンにします。

ステップ 6 [インターフェイス（Interfaces）] フィールドで、仮想ルータに割り当てられている 1 つ以上のインターフェイスの横にあるチェックボックスをオンにします。

ヒント DHCPv6 リレー用に設定されているインターフェイスは、[インターフェイス（Interfaces）] タブから無効にできません。最初に [DHCPv6 リレー インターフェイス（DHCPv6 Relay interfaces）] チェックボックスをオフにして、設定を保存する必要があります。

ステップ 7 選択したインターフェイスの横にあるドロップダウンアイコンをクリックし、インターフェイスが DHCP 要求をリレーする方式として、[アップストリーム（Upstream）]、[ダウンストリーム（Downstream）] 、または [両方（Both）] を選択します。

（注） 少なくとも 1 つのダウンストリーム インターフェイスと 1 つのアップストリーム インターフェイスを含める必要があります。[両方（Both）] を選択することは、インターフェイスがダウンストリームとアップストリームの両方であることを意味します。

ステップ 8 [最大ホップ（Max Hops）] フィールドに 1 ～ 255 の最大ホップ カウントを入力します。

ステップ 9 [保存（Save）] をクリックします。

次のタスク

- 設定変更を展開します。設定変更の展開を参照してください。

スタティック ルート

スタティック ルーティングにより、ルータを通過するトラフィックの IP アドレスに関するルールを作成することができます。これはネットワークの現在のトポロジに関して他のルータとの通信がないため、仮想ルータのパス選択を設定する最も簡単な方法です。

割り当てられた仮想ルータがパケットをルーティングできない DHCPv4 サーバでは、IP インターフェイスへのルーティングを設定しないでください。これを行うと、以前に指定したルーティング可能な DHCP4 サーバがルーティングできなくなります。

スタティック ルート テーブルには次の表に示すように、各ルートに関するサマリー情報が含まれます。

表 *1:* スタティック ルート テーブル ビュー フィールド

フィールド	説明
有効（Enabled）	このルートが現在有効であるか、無効であるかを示します。
[名前（Name）]	スタティック ルートの名前。
[接続先（Destination）]	トラフィックがルーティングされる宛先ネットワーク。
タイプ	このルートに対して実行するアクションを指定します。次のいずれかです。 • [IP]：パケットが、隣接ルータのアドレスに転送されることを指定します。 • [インターフェイス（Interface）]：そのインターフェイスを介してトラフィックが直接接続されたネットワーク上のホストにルーティングされるインターフェイスにパケットが転送されることを指定します。 • [破棄（Discard）]：スタティック ルートでパケットをドロップすることを指定します。
ゲートウェイ（Gateway）	スタティック ルートのタイプとしてIPを選択した場合はターゲットIPアドレス、またはスタティック ルート タイプとしてインターフェイスを選択した場合はインターフェイス。
優先順位（Preference）	ルート選択を決定します。同じ宛先に対する複数のルートが存在する場合、より高い優先順位のルートが選択されます。

静的ルート テーブルの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	Control	7000 & 8000 シリーズ	任意（Any）	Admin/Network Admin

手順

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 表示するデバイスの横にある編集アイコン（）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [仮想ルータ（Virtual Routers）] タブをクリックします。

ステップ 4 静的ルートを表示する仮想ルータの横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は子孫ドメインに属しているか、設定を変更する権限がありません。

ステップ 5 [静的（Static）] タブをクリックします。

スタティック ルートの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

手順

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 スタティック ルートを追加するデバイスの横にある編集アイコン（）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [仮想ルータ（Virtual Routers）] タブをクリックします。

ステップ 4 スタティック ルートを追加する仮想ルータの横にある編集アイコン（）をクリックします。

ステップ 5 [静的（Static）] をクリックして、スタティック ルートのオプションを表示します。

ステップ 6 [静的ルートの追加（Add Static Route）] をクリックします。

ステップ 7 [ルート名（Route Name）] フィールドに、スタティック ルートの名前を入力します。英数字とスペースを使用できます。

ステップ 8 [有効（Enabled）] チェックボックスをオンにして、ルートが現在有効であることを指定します。

ステップ 9 [優先（Preference）] フィールドに、ルート選択を決定するための 1 ～ 65535 の数値を入力します。

（注） 同じ宛先に対する複数のルートが存在する場合、より高い優先順位のルートが使用されます。

ステップ 10 [タイプ（Type）] ドロップダウン リストから、設定するスタティック ルートのタイプを選択します。

ステップ 11 [宛先（Destination）] フィールドに、トラフィックがルーティングされる宛先ネットワークの IP アドレスを入力します。

ステップ 12 [ゲートウェイ（Gateway）] フィールドでは、次の 2 つの選択肢があります。

- スタティック ルート タイプとして [IP] を選択した場合は、IP アドレスを選択します。
- スタティック ルート タイプとして [インターフェイス（Interface）] を選択した場合は、ドロップダウン リストから有効なインターフェイスを選択します。

ヒント [インターフェイス（Interfaces）] タブから無効にしたインターフェイスは使用できません。追加したインターフェイスを無効にすると、設定から削除されます。

ステップ 13 [OK] をクリックします。

ステップ 14 [保存（Save）] をクリックします。

次のタスク

- 設定変更を展開します。設定変更の展開を参照してください。

ダイナミック ルーティング

ダイナミックつまり適応型のルーティングは、ルーティング プロトコルを使用して、ルートが取るパスをネットワーク条件の変化に応じて変更します。この適応は、できるだけ多くのルートの有効性を維持し、変更に応じて宛先に到達可能とすることを目的としたものです。このため、他のパスを選択できる限り、ネットワークはノードまたはノード間の接続の損失といった障害を「迂回」することができます。ダイナミック ルーティングなしでルータを設定することも、Routing Information Protocol（RIP）または Open Shortest Path First（OSPF）のルーティング プロトコルを設定することもできます。

RIP コンフィギュレーション

Routing Information Protocol（RIP）はホップ カウントを使用してルートを決定する、小規模な IP ネットワーク向けのダイナミック ルーティング プロトコルです。最適なルートは最小数のホップを使用します。RIP で許可されるホップの最大数は 15 です。このホップ制限により、RIP がサポートできるネットワークのサイズも制限されます。

RIP 設定のインターフェイスの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

RIP を設定する際、RIP を設定する仮想ルータにすでに含まれているインターフェイスを選択する必要があります。無効になっているインターフェイスを使用することはできません。

手順

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 変更するデバイスの横にある編集アイコン（）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [仮想ルータ（Virtual Routers）] タブをクリックします。

ステップ 4 変更する仮想ルータの横にある編集アイコン（）をクリックします。

ステップ 5 [ダイナミック ルーティング（Dynamic Routing）] をクリックして、ダイナミック ルーティングのオプションを表示します。

ステップ 6 [RIP] をクリックして、RIP オプションを表示します。

ステップ 7 [インターフェイス（Interfaces）] の下で、追加アイコン（）をクリックします。

ステップ 8 [名前（Name）] ドロップダウン リストから、RIP を設定するインターフェイスを選択します。

ヒント [インターフェイス（Interfaces）] タブから無効にしたインターフェイスは使用できません。追加したインターフェイスを無効にすると、設定から削除されます。

ステップ 9 [メトリック（Metric）] フィールドに、インターフェイスのメトリックを入力します。異なる RIP インスタンスからのルートを使用可能で、すべてが同じ設定である場合、メトリックが最小のルートが優先ルートになります。

ステップ 10 [モード（Mode）] ドロップダウン リストから、次のいずれかのオプションを選択します。

- [マルチキャスト（Multicast）]：RIP が指定されたアドレスですべての隣接ルータにルーティング テーブル全体をマルチキャストするデフォルトのモード。
- [ブロードキャスト（Broadcast）]：マルチキャスト モードが可能な場合でも、RIP にブロードキャスト（RIPv1 など）の使用を強制します。
- [待機（Quiet）]：RIP は、このインターフェイスに定期メッセージを送信しません。
- [リスナーなし（No Listen）]：RIP は、このインターフェイスに送信しますが、リッスンしません。

ステップ 11 [保存（Save）] をクリックします。

次のタスク

- 設定変更を展開します。設定変更の展開を参照してください。

RIP の認証設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

RIP 認証では、仮想ルータに設定した認証プロファイルの 1 つが使用されます。

手順

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 変更するデバイスの横にある編集アイコン（）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [仮想ルータ（Virtual Routers）] タブをクリックします。

ステップ 4 RIP 認証プロファイルを追加する仮想ルータの横にある編集アイコン（）をクリックします。

ステップ 5 [ダイナミック ルーティング（Dynamic Routing）] をクリックして、ダイナミック ルーティングのオプションを表示します。

ステップ 6 [RIP] をクリックして、RIP オプションを表示します。

ステップ 7 [認証（Authentication）] で、[プロファイル（Profile）] ドロップダウン リストから既存の仮想ルータの認証プロファイルを選択するか、[なし（None）] を選択します。

ステップ 8 [保存（Save）] をクリックします。

次のタスク

- 設定変更を展開します。設定変更の展開を参照してください。

高度な RIP の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

プロトコルの動作に影響するさまざまなタイムアウト値およびその他の機能に関していくつかの高度な RIP 設定を構成できます。

⚠

注意 不正な値に対する高度な RIP 設定を変更すると、ルータが他の RIP ルータと正常に通信することを妨げる場合があります。

手順

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 変更するデバイスの横にある編集アイコン（✎）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [仮想ルータ（Virtual Routers）] タブをクリックします。

ステップ 4 変更する仮想ルータの横にある編集アイコン（✎）をクリックします。

ステップ 5 [ダイナミック ルーティング（Dynamic Routing）] をクリックして、ダイナミック ルーティングのオプションを表示します。

ステップ 6 [RIP] をクリックして、RIP オプションを表示します。

ステップ 7 [優先順位（Preference）] フィールドに、ルーティング プロトコルの優先度の数値（高いほど優先される）を入力します。システムはスタティック ルートよりも RIP を使用して学習したルートを優先します。

ステップ 8 [期間（Period）] フィールドに、定期的な更新間隔（秒単位）を入力します。低い数値は高速なコンバージェンスを示しますが、ネットワーク負荷が大きくなります。

ステップ 9 [タイムアウト時間（Timeout Time）] フィールドに、到達不能とみなされるまでのルートの存続時間（秒単位）を指定する数値を入力します。

ステップ 10 [ガベージ時間（Garbage Time）] フィールドに、破棄されるまでのルートの存続時間（秒単位）を指定する数値を入力します。

ステップ 11 [無限（Infinity）] フィールドに、コンバージェンスの計算で無限間隔の値を指定する数値を入力します。値が大きいほど、プロトコル コンバージェンスが遅くなります。

ステップ 12 [実行（Honor）] ドロップダウン リストから、ルーティング テーブルをダンプする要求がいつ実行されるかを指定する、次のいずれかのオプションを選択します。

- [常時（Always）]：常に要求を実行する

- [ネイバー（Neighbor）]：直接接続されたネットワーク上のホストから送信された要求のみを実行する
- [なし（Never）]：要求を実行しない

ステップ 13 [保存（Save）] をクリックします。

次のタスク

- 設定変更を展開します。設定変更の展開を参照してください。

RIP 設定へのインポート フィルタの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

ルート テーブルに対して RIP からの受け入れまたは拒否を行うルートを指定するために、インポート フィルタを追加できます。インポート フィルタはテーブルに表示される順に適用されます。

インポートフィルタを追加するときは、仮想ルータに設定したフィルタの1つを使用します。

ヒント RIP インポート フィルタを編集するには、編集アイコン（）をクリックします。RIP インポート フィルタを削除するには、削除アイコン（）をクリックします。

始める前に

- 仮想ルータの追加 （13 ページ） の説明に従い、仮想ルータを追加します。
- 仮想ルータのフィルタの設定 （36 ページ） の説明に従い、仮想ルータにフィルタを設定します。

手順

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 変更するデバイスの横にある編集アイコン（）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [仮想ルータ（Virtual Routers）] タブをクリックします。

ステップ 4 RIP 仮想ルータ フィルタを追加する仮想ルータの横にある編集アイコン（）をクリックします。

ステップ 5 [ダイナミック ルーティング（Dynamic Routing）] をクリックして、ダイナミック ルーティングのオプションを表示します。

ステップ 6 [RIP] をクリックして、RIP オプションを表示します。

ステップ 7 [インポート フィルタ（Import Filters）] の下で、追加アイコン（）をクリックします。

ステップ 8 [名前（Name）] ドロップダウン リストから、インポート フィルタとして追加するフィルタを選択します。

ステップ 9 [アクション（Action）] の横にある [承認（Accept）] または [拒否（Reject）] を選択します。

ステップ 10 [OK] をクリックします。

ヒント インポート フィルタの順序を変更するには、必要に応じて、上へ移動するアイコン（）または下へ移動するアイコン（）をクリックします。リスト内でフィルタを上下にドラッグすることもできます。

ステップ 11 [保存（Save）] をクリックします。

次のタスク

- 設定変更を展開します。設定変更の展開を参照してください。

RIP 設定へのエクスポート フィルタの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

ルート テーブルから RIP に対しての受け入れまたは拒否を行うルートを定義するために、エクスポート フィルタを追加できます。エクスポート フィルタはテーブルに表示される順に適用されます。

エクスポート フィルタを追加するときは、仮想ルータに設定したフィルタの 1 つを使用します。

手順

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 変更するデバイスの横にある編集アイコン（）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [仮想ルータ（Virtual Routers）] タブをクリックします。

ステップ 4 RIP 仮想ルータ フィルタを追加する仮想ルータの横にある編集アイコン（  ）をクリックします。

ステップ 5 [ダイナミック ルーティング（Dynamic Routing）] をクリックして、ダイナミック ルーティングのオプションを表示します。

ステップ 6 [RIP] をクリックして、RIP オプションを表示します。

ステップ 7 [エクスポート フィルタ（Export Filters）] の下で、追加アイコン（  ）をクリックします。

ステップ 8 [名前（Name）] ドロップダウン リストから、エクスポート フィルタとして追加するフィルタを選択します。

ステップ 9 [アクション（Action）] の横にある [承認（Accept）] または [拒否（Reject）] を選択します。

ステップ 10 [OK] をクリックします。

ヒント エクスポート フィルタの順序を変更するには、必要に応じて、上へ移動するアイコン（  ）または下へ移動するアイコン（）をクリックします。リスト内でフィルタを上下にドラッグすることもできます。

ステップ 11 [保存（Save）] をクリックします。

次のタスク

- 設定変更を展開します。設定変更の展開を参照してください。

OSPF の設定

Open Shortest Path First（OSPF）は、他のルータから情報を取得し、リンク ステート アドバタイズメントを使用してルートを他のルータにアドバタイズすることで、ルートを動的に定義する適応型ルーティング プロトコルです。ルータは、それ自体と宛先との間のリンクに関する情報を維持し、ルーティングを決定します。OSPF は、各ルーテッド インターフェイスにコストを割り当て、コストが最低のルータを最適であるとみなします。

OSPF ルーティング エリア

OSPF ネットワークは、管理を簡略化し、トラフィックおよびリソースの使用を最適化するために、ルーティング エリアに構造化つまり分割することができます。エリアは、単純な 10 進数またはよく使用されるオクテットベースのドット付き 10 進数表記のいずれかで表現される 32 ビットの数字により識別されます。

慣習により、エリア ゼロつまり 0.0.0.0 は OSPF ネットワークのコアまたはバックボーン エリアを表します。他のエリアも指定できます。多くの場合、管理者はエリアのメイン ルータの IP アドレスをエリア ID として選択します。追加の各エリアはバックボーンの OSPF エリアに

直接または仮想接続できる必要があります。そうした接続は、エリア境界ルータ（ABR）と呼ばれる相互接続ルータによって保持されます。ABR は、管轄する各エリアの個々のリンクステートデータベースを管理し、ネットワーク内のすべてのエリアの集約ルートを保守します。

OSPF エリアの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

手順

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 変更するデバイスの横にある編集アイコン（）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [仮想ルータ（Virtual Routers）] タブをクリックします。

ステップ 4 変更する仮想ルータの横にある編集アイコン（）をクリックします。

ステップ 5 [ダイナミック ルーティング（Dynamic Routing）] をクリックして、ダイナミック ルーティングのオプションを表示します。

ステップ 6 [OSPF（OSPF）] をクリックして、OSPF オプションを表示します。

ステップ 7 [エリア（Areas）] の下で、追加アイコン（）をクリックします。

ステップ 8 [エリア ID（Area Id）] フィールドに、エリアを表す数値を入力します。この値には整数または IPv4 アドレスを指定できます。

ステップ 9 オプションで、[スタブネット（Stubnet）] チェックボックスをオンにし、エリアが自律システムの外部のルータ アドバタイズメントを受信せず、エリア内のルーティングは完全にデフォルトルートに基づくことを指定します。チェックボックスをオフにすると、このエリアはバックボーン エリアになります。それ以外の場合は、非スタブ エリアになります。

ステップ 10 [デフォルト コスト（Default cost）] フィールドに、エリアのデフォルト ルートに関連付けられたコストを入力します。

ステップ 11 [スタブネット（Stubnets）] の下で、追加アイコン（）をクリックします。

ステップ 12 [IP アドレス（IP Address）] フィールドに、IP アドレスを CIDR 表記で入力します。

ステップ 13 [非表示（Hidden）] チェックボックスを選択して、スタブネットが非表示であることを示します。

非表示のスタブネットは別のエリアに伝播されません。

ステップ 14 [サマリ（Summary）] チェックボックスを選択して、このスタブネットのサブネットワークであるデフォルトのスタブネットが非表示となるように指定します。

ステップ 15 [スタブ コスト（Stub cost）] フィールドに、このスタブ ネットワークへのルーティングに関連付けられたコストを定義する値を入力します。

ステップ 16 [OK] をクリックします。

ステップ 17 ネットワークを追加するには [ネットワーク（Networks）] の下の追加アイコン（  ）をクリックします。

ステップ 18 [IP アドレス（IP Address）] フィールドに、ネットワークの IP アドレスを CIDR 表記で入力します。

ステップ 19 [非表示（Hidden）] チェックボックスをオンにして、ネットワークが非表示であることを示します。非表示のネットワークは別のエリアに伝播されません。

ステップ 20 [OK] をクリックします。

ステップ 21 [保存（Save）] をクリックします。

次のタスク

- 設定変更を展開します。設定変更の展開を参照してください。

OSPF エリア インターフェイス

OSPF 用に仮想ルータに割り当てられたインターフェイスのサブセットを設定できます。次のリストに、各インターフェイスで指定できるオプションを示します。

インターフェイス

OSPF を設定するインターフェイスを選択します。[インターフェイス（Interfaces）] タブから無効にしたインターフェイスは使用できません。

タイプ（Type）

次のオプションから、OSPF インターフェイスのタイプを選択します。

- [ブロードキャスト（Broadcast）]：ブロードキャスト ネットワークでは、フラッディングおよび hello メッセージはマルチキャストを使用し、すべてのネイバーに対して 1 つのパケットで送信されます。このオプションは、ルータがリンク ステート データベースと同期し、ネットワーク リンク ステート アドバタイズメントを発信するように指定します。このネットワーク タイプは、物理的なノンブロードキャスト マルチプルアクセス（NBMP）ネットワークと適切な IP プレフィクスなしのアンナンバード ネットワークには使用できません。
- [ポイントツーポイント（PtP）（Point-to-Point (PtP)）]：ポイントツーポイント ネットワークでは、2 台のルータのみを接続します。選定は実行されず、ネットワーク リンク ステート アドバタイズメントは発生しないので、より単純かつ高速に確立されます。このネットワーク タイプは物理的な PtP インターフェイスだけでなく、PtP リンクとして使用されるブロードキャスト ネットワークにも役立ちます。このネットワーク タイプは物理的な NBMP ネットワークでは使用できません。

- [ノンブロードキャスト（Non-Broadcast）]：NBMP ネットワークで、パケットはマルチキャスト機能がないために各ネイバーに別々に送信されます。ブロードキャスト ネットワークと同様に、このオプションはリンク ステート アドバタイズメント伝播で中心的な役割を果たすルータを指定します。このネットワーク タイプはアンナンバードネットワークでは使用できません。
- [自動検出（Autodetect）]：システムは指定されたインターフェイスに基づいて正しいタイプを判別します。

コスト

インターフェイスの出力コストを指定します。

Stub

インターフェイスが OSPF トラフィックをリッスンし、独自のトラフィックを送信する必要があるかどうかを指定します。

[プライオリティ（Priority）]

指定ルータの選定に使用される優先度を示す数値を入力します。多重アクセス ネットワークごとに、システムはルータおよびバックアップ ルータを指定します。これらのルータには、フラッディング プロセスでの特別な機能があります。優先度を高くすると、この選定での優先順位が上がります。優先度 0 でルータを設定することはできません。

[ノンブロードキャスト（Nonbroadcast）]

hello パケットが任意の未定義のネイバーに送信されるかどうかを指定します。このスイッチは、任意の NBMA ネットワークでは無視されます。

認証

仮想ルータに設定した認証プロファイルの 1 つからこのインターフェイスが使用する OSPF 認証プロファイルを選択するか、または [なし（None）] を選択します。認証プロファイルの設定に関する詳細については、仮想ルータ認証プロファイルの追加 （37 ページ）を参照してください。

[Hello 間隔（Hello Interval）]

hello メッセージの送信間隔（秒単位）を入力します。

[ポーリング（Poll）]

NBMA ネットワーク上の一部のネイバーに対する hello メッセージの送信間隔（秒単位）を入力します。

[再送間隔（Retrans Interval）]

確認応答されていないアップデートの再送信間隔（秒単位）を入力します。

[再送遅延（Retrans Delay）]

インターフェイス経由でのリンクステート アップデート パケットの送信に要する推定秒数を入力します。

待ち時間（Wait Time）

ルータが選定の開始と隣接関係の構築の間で待機する秒数を入力します。

[デッド間隔（Dead Interval）]

ルータがネイバーからのメッセージを受信しない場合に、ネイバーの停止を宣言するまで待機する秒数を入力します。この値が定義されている場合、deadカウントから計算された値はオーバーライドされます。

[無レスポンス カウント（Dead Count）]

hello間隔と乗算されるときに、ルータがネイバーからのメッセージを受信しない場合に、ネイバーの停止を宣言するまで待機する秒数を指定する、数値を入力します。

OSPFエリアインターフェイスを編集するには、編集アイコン（）をクリックします。OSPFエリア インターフェイスを削除するには、削除アイコン（）をクリックします。[インターフェイス（Interfaces）] タブで設定されたインターフェイスを無効にすると削除されます。

OSPF エリア インターフェイスの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	Control	7000 & 8000 シリーズについて	リーフのみ	Admin/Network Admin

OSPF 用に仮想ルータに割り当てられたインターフェイスのサブセットを設定できます。

OSPF エリアで使用するインターフェイスは 1 つのみ選択できます。

手順

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 OSPF インターフェイスを追加するデバイスの横にある編集アイコン（）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [仮想ルータ（Virtual Routers）] タブをクリックします。

ステップ 4 OSPF インターフェイスを追加する仮想ルータの横にある編集アイコン（）をクリックします。

ステップ 5 [ダイナミック ルーティング（Dynamic Routing）] をクリックして、ダイナミック ルーティングのオプションを表示します。

ステップ 6 [OSPF（OSPF）] をクリックして、OSPF オプションを表示します。

ステップ 7 [エリア（Areas）] の下で、追加アイコン（）をクリックします。

ステップ 8 [インターフェイス（Interfaces）] をクリックします。

ステップ 9 追加アイコン（）をクリックします。

ステップ 10 OSPF エリア インターフェイス （27 ページ）で説明されているアクションのいずれかを実行します。

ステップ 11 ネットワークを追加するには[ネットワーク（Networks）]の下の追加アイコン（）をクリックします。

ステップ 12 [IP アドレス（IP address）] フィールドに、このインターフェイスから非ブロードキャスト ネットワークの hello メッセージを受信するネイバーの IP アドレスを入力します。

ステップ 13 [資格あり（Eligible）] チェックボックスをオンにして、ネイバーがメッセージを受け取る資格があることを示します。

ステップ 14 [OK] をクリックします。

ヒント ネイバーを編集するには、編集アイコン（）をクリックします。ネイバーを削除するには、削除アイコン（）をクリックします。

ステップ 15 [OK] をクリックします。

ステップ 16 [保存（Save）] をクリックします。

ステップ 17 [保存（Save）] をクリックします。

次のタスク

- 設定変更を展開します。設定変更の展開を参照してください。

OSPF エリア vlink の追加

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

OSPF 自律システムのすべてのエリアは、物理的にバックボーン エリアと接続されている必要があります。この物理接続が不可能である場合は、vlink を使用して、非バックボーン エリアを経由してバックボーンに接続できます。また vlink を使用して、非バックボーン エリアを経由し、分割されたバックボーンの 2 つの部分を接続することもできます。

vlink を追加するには、最低 2 つの OSPF エリアを追加しておく必要があります。

手順

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 変更するデバイスの横にある編集アイコン（）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [仮想ルータ（Virtual Routers）] タブをクリックします。

ステップ 4 変更する仮想ルータの横にある編集アイコン（）をクリックします。

ステップ 5 [ダイナミック ルーティング（Dynamic Routing）] をクリックして、ダイナミック ルーティングのオプションを表示します。

ステップ 6 [OSPF（OSPF）] をクリックして、OSPF オプションを表示します。

ステップ 7 [エリア（Areas）] の下で、追加アイコン（）をクリックします。

ステップ 8 [Vlinks] をクリックします。

ステップ 9 追加アイコン（）をクリックします。

ステップ 10 [ルータ ID（Router ID）] フィールドに、ルータの IP アドレスを入力します。

ステップ 11 [認証（Authentication）] ドロップダウン リストから、vlink が使用する認証プロファイルを選択します。

ステップ 12 [Hello インターバル（Hello Interval）] フィールドに、hello メッセージの送信間隔（秒単位）を入力します。

ステップ 13 [再送信間隔（Retrans Interval）] フィールドに、確認応答されていないアップデートの再送信間隔（秒単位）を入力します。

ステップ 14 [待機時間（Wait Time）] フィールドに、ルータが選定の開始と隣接関係の構築の間で待機する秒数を入力します。

ステップ 15 [Dead 間隔（Dead Interval）] フィールドに、ルータがネイバーからのメッセージを受信しない場合に、ネイバーの停止を宣言するまで待機する秒数を入力します。この値が定義されている場合、dead カウントから計算された値はオーバーライドされます。

ステップ 16 [Dead 回数（Dead Count）] フィールドに、hello 間隔と乗算されるときに、ルータがネイバーからのメッセージを受信しない場合に、ネイバーの停止を宣言するまで待機する秒数を指定する、数値を入力します。

ステップ 17 [OK] をクリックします。

ステップ 18 [保存（Save）] をクリックします。

ステップ 19 [保存（Save）] をクリックします。

次のタスク

- 設定変更を展開します。設定変更の展開を参照してください。

OSPF 設定へのインポート フィルタの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

ルートテーブルに対してOSPFからの受け入れまたは拒否を行うルートを定義するために、インポート フィルタを追加できます。インポート フィルタはテーブルに表示される順に適用されます。

インポートフィルタを追加するときは、仮想ルータに設定したフィルタの1つを使用します。

手順

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 変更するデバイスの横にある編集アイコン（  ）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [仮想ルータ（Virtual Routers）] をクリックします。

ステップ 4 変更する仮想ルータの横にある編集アイコン（  ）をクリックします。

ステップ 5 [ダイナミック ルーティング（Dynamic Routing）] をクリックして、ダイナミック ルーティングのオプションを表示します。

ステップ 6 [OSPF（OSPF）] をクリックして、OSPF オプションを表示します。

ステップ 7 [インポート フィルタ（Import Filters）] の下で、追加アイコン（  ）をクリックします。

ステップ 8 [名前（Name）] ドロップダウン リストから、インポート フィルタとして追加するフィルタを選択します。

ステップ 9 [アクション（Action）] の横にある [承認（Accept）] または [拒否（Reject）] を選択します。

ステップ 10 [OK] をクリックします。

ヒント インポート フィルタの順序を変更するには、必要に応じて、上へ移動するアイコン（  ）または下へ移動するアイコン（  ）をクリックします。リスト内でフィルタを上下にドラッグすることもできます。

ステップ 11 [保存（Save）] をクリックします。

次のタスク

- 設定変更を展開します。設定変更の展開を参照してください。

OSPF 設定へのエクスポート フィルタの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

ルート テーブルからOSPFに対しての受け入れまたは拒否を行うルートを定義するために、エクスポート フィルタを追加できます。エクスポート フィルタはテーブルに表示される順に適用されます。

エクスポート フィルタを追加するときは、仮想ルータに設定したフィルタの 1 つを使用します。

手順

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 変更するデバイスの横にある編集アイコン（）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [仮想ルータ（Virtual Routers）] タブをクリックします。

ステップ 4 OSPF 仮想ルータ フィルタを追加する仮想ルータの横にある編集アイコン（）をクリックします。

ステップ 5 [ダイナミック ルーティング（Dynamic Routing）] タブをクリックして、ダイナミック ルーティングのオプションを表示します。

ステップ 6 [OSPF] をクリックして、OSPF オプションを表示します。

ステップ 7 [エクスポート フィルタ（Export Filters）] の下で、追加アイコン（）をクリックします。

ステップ 8 [名前（Name）] ドロップダウン リストから、エクスポート フィルタとして追加するフィルタを選択します。

ステップ 9 [アクション（Action）] の横にある [承認（Accept）] または [拒否（Reject）] を選択します。

ステップ 10 [OK] をクリックします。

ヒント エクスポート フィルタの順序を変更するには、必要に応じて、上へ移動するアイコン（）または下へ移動するアイコン（）をクリックします。リスト内でフィルタを上下にドラッグすることもできます。

ステップ 11 [保存（Save）] をクリックします。

次のタスク

- 設定変更を展開します。設定変更の展開を参照してください。

仮想ルータのフィルタ

フィルタは、仮想ルータのルート テーブルへのインポートおよびルートのダイナミック プロトコルへのエクスポートを行うために、ルートを照合する方法を提供します。フィルタのリストを作成および管理できます。各フィルタは特定の基準を定義し、静的に定義されるか、またはダイナミック プロトコルから受信したルートを検索します。

仮想ルータ フィルタ テーブルには、仮想ルータに設定した各フィルタのサマリ情報が表示されます（次の表を参照してください）。

表 *2:* 仮想ルータ フィルタ テーブル ビューのフィールド

フィールド	説明
名前（Name）]	フィルタの名前。
プロトコル	ルートが発生するプロトコル。 • [スタティック（Static）]：ルートはローカル スタティック ルートとして発生します。 • [RIP]：ルートはダイナミックな RIP 設定から発生します。 • [OSPF]：ルートはダイナミックな OSPF 設定から発生します。
ルータから（From Router）	このフィルタがルートで一致を試みるルータの IP アドレス。スタティック フィルタおよび RIP フィルタに対してこの値を入力する必要があります。
Next Hop（ネクスト ホップ）	このルートを使用するパケットが転送されるネクストホップ。スタティック フィルタおよび RIP フィルタに対してこの値を入力する必要があります。
接続先タイプ（Destination Type）	パケットが送信される宛先のタイプ。 • ルータ（Router） • Device • 廃棄（Discard）

フィールド	説明
宛先ネットワーク（Destination Network）	このフィルタがルートで一致を試みるネットワーク。
OSPF パス タイプ（OSPF Path Type）	OSPF プロトコルにのみ適用されます。パスタイプは次のいずれかです。 • Ext-1 • Ext-2 • エリア間（Inter Area） • 内部エリア（Intra Area）
OSPF ルータ ID（OSPF Router ID）	OSPFプロトコルにのみ適用されます。ルート/ネットワークをアドバタイズするルータのルータ ID。

仮想ルータ フィルタの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	Control	7000 & 8000 シリーズ	任意（Any）	Admin/Network Admin

仮想ルータ エディタの [フィルタ（Filter）] タブには、仮想ルータに設定したすべてのフィルタを含むテーブルが表示されます。テーブルには、各フィルタに関するサマリー情報が含まれています。

手順

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 表示するデバイスの横にある編集アイコン（  ）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [仮想ルータ（Virtual Routers）] タブをクリックします。

ステップ 4 フィルタを表示する仮想ルータの横にある編集アイコン（）をクリックします。

ステップ 5 [フィルタ（Filter）] タブをクリックします。

仮想ルータのフィルタの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

手順

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 変更するデバイスの横にある編集アイコン（  ）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [仮想ルータ（Virtual Routers）] タブをクリックします。

ステップ 4 変更する仮想ルータの横にある編集アイコン（  ）をクリックします。

ステップ 5 [フィルタ処理（Filter）] タブをクリックします。

ステップ 6 [フィルタの追加（Add Filter）] をクリックします。

ステップ 7 [名前（Name）] フィールドにフィルタの名前を入力します。英数字のみを使用できます。

ステップ 8 [プロトコル（Protocol）] で、[すべて（All）] を選択するか、フィルタに適用するプロトコルを選択します。

ステップ 9 [プロトコル（Protocol）] として [すべて（All）]、[スタティック（Static）]、または [RIP] を選択した場合は、[ルータから（From Router）] で、このフィルタがルートで一致を試みるルータ IP アドレスを入力します。

（注） IPv4 アドレスに対する /32 の CIDR ブロックと IPv6 アドレスに対する /128 のプレフィクス長も入力可能です。他のすべてのアドレスブロックは、このフィールドでは無効です。

ステップ 10 [追加（Add）] をクリックします。

ステップ 11 [プロトコル（Protocol）] として [すべて（All）]、[スタティック（Static）]、または [RIP（RIP）] を選択した場合は、[ネクスト ホップ（Next Hop）] で、このフィルタがルートで一致を試みるゲートウェイの IP アドレスを入力します。

（注） IPv4 アドレスに対する /32 の CIDR ブロックと IPv6 アドレスに対する /128 のプレフィクス長も入力可能です。他のすべてのアドレスブロックは、このフィールドでは無効です。

ステップ 12 [追加（Add）] をクリックします。

ステップ 13 [送信先のタイプ（Destination Type）] で、フィルタに適用するオプションを選択します。

ステップ 14 [宛先ネットワーク（Destination Network）] で、このフィルタがルートで一致を試みるネットワークの IP アドレスを入力します。

ステップ 15 [追加（Add）] をクリックします。

ステップ 16 [プロトコル（Protocol）] として [すべて（All）] または [OSPF] を選択した場合は、[パスのタイプ（Path Type）] で、フィルタに適用するオプションを選択します。少なくとも 1 つのパスタイプを選択する必要があります。

ステップ 17 [プロトコル（Protocol）] として [OSPF] を選択した場合は、[ルータ ID（Router ID）] で、ルート/ネットワークをアドバタイズするルータのルータ ID の役割を持つ IP アドレスを入力します。

ステップ 18 [追加（Add）] をクリックします。

ステップ 19 [OK] をクリックします。

ステップ 20 [保存（Save）] をクリックします。

次のタスク

- 設定変更を展開します。設定変更の展開を参照してください。

仮想ルータ認証プロファイルの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

RIP および OSPF の設定で使用する認証プロファイルをセットアップできます。簡易パスワードを設定するか、共有暗号キーを指定できます。簡易パスワードでは、すべてのパケットが 8 バイトのパスワードを伝送できます。システムはこのパスワードが欠如している受信パケットを無視します。暗号キーでは検証が可能で、パスワードから生成される 16 バイト長のダイジェストがすべてのパケットに付加されます。

OSPF の場合、各エリアは異なる認証方式を使用できることに注意してください。そのため、多くのエリア間で共有できる認証プロファイルを作成します。OSPFv3 の認証は追加できません。

手順

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 変更するデバイスの横にある編集アイコン（  ）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [仮想ルータ（Virtual Routers）] タブをクリックします。

ステップ 4 変更する仮想ルータの横にある編集アイコン（）をクリックします。

ステップ 5 [認証プロファイル（Authentication Profile）] をクリックします。

ステップ 6 [認証プロファイルの追加（Add Authentication Profile）] をクリックします。

ステップ 7 [認証プロファイル名（Authentication Profile Name）] フィールドに、認証プロファイルの名前を入力します。

ステップ 8 [認証タイプ（Authentication Type）] ドロップダウン リストから、[単純（simple）] または [暗号化（cryptographic）] を選択します。

ステップ 9 [パスワード（Password）] フィールドに、安全なパスワードを入力します。

ステップ 10 確認のために [パスワードの確認（Confirm Password）] フィールドにもう一度パスワードを入力します。

ステップ 11 [OK] をクリックします。

ステップ 12 [保存（Save）] をクリックします。

次のタスク

- 設定変更を展開します。設定変更の展開を参照してください。

仮想ルータ統計情報の表示

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	Control	7000 & 8000 シリーズ	任意（Any）	Admin/Network Admin

各仮想ルータの実行時統計情報を表示できます。統計情報にはユニキャスト パケット、ドロップされたパケット、IPv4 および IPv6 アドレスの個別のルーティング テーブルが表示されます。

手順

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 統計情報を表示するデバイスの横にある編集アイコン（）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [仮想ルータ（Virtual Routers）] タブをクリックします。

ステップ 4 ルータ統計情報を表示する仮想ルータの横にある表示アイコン（）をクリックします。

仮想ルータの削除

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

仮想ルータを削除すると、ルータに割り当てられているすべてのルーテッドインターフェイスを他のルータに含めることができるようになります。

手順

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 変更するデバイスの横にある編集アイコン（）をクリックします。

マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [仮想ルータ（Virtual Routers）] タブをクリックします。

ステップ 4 削除する仮想ルータの横にある削除アイコン（）をクリックします。

ステップ 5 入力を求められた場合、仮想ルータを削除することを確認します。

次のタスク

- 設定変更を展開します。設定変更の展開を参照してください。