仮想ルータのセットアップ

複数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レイヤ 3 の管理対象デバイスを設定できます。各インターフェイスに IP アドレスを割り当て、これらのインターフェイスを、トラフィックをルーティングする仮想ルータに割り当てる必要があります。シリーズ 3 管理対象デバイスでは、複数の物理インターフェイスを Link Aggregation Group（LAG）と呼ばれる単一の論理ルーテッド インターフェイスにグループ化できます。このように 1 つに集約された論理リンクは、帯域幅と冗長性の向上および、2 つのエンドポイント間でのロードバランシングを実現します。

宛先アドレスに従ってパケット転送の決定を行うことにより、パケットをルーティングするようにシステムを設定できます。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、転送基準に基づく発信インターフェイスからの宛先を取得します。適用するセキュリティ ポリシーは、アクセス制御ルールによって指定されます。

レイヤ 3 配置では、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 プロトコルを設定することができます。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 を組み合わせて設定することもできます。

注意 レイヤ 3 配置に何らかの理由で障害が発生した場合、デバイスはそれ以後トラフィックを転送しません。

注意 仮想ルータを追加すると、変更の適用時に Snort プロセスが再起動され、トラフィック インスペクションは一時的に中断されます。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、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、Snort の再開によるトラフィックへの影響（1-9 ページ）を参照してください。

レイヤ 3 配置の設定に関する詳細については、次の項を参照してください。

- ルーテッド インターフェイスの設定（7-2 ページ）
- 仮想ルータの設定（7-10 ページ）
- LAG の設定（8-2 ページ）

ルーテッド インターフェイスの設定

ライセンス: Control

Supported Defense Centers: シリーズ 3

ルーテッド インターフェイスのセットアップは物理設定または論理設定のいずれかで行うことができます。タグなし VLAN のトラフィックを処理するために物理ルーテッド インターフェイスを設定できます。指定の VLAN タグ付きトラフィックを処理する、論理ルーテッド インターフェイスを作成することもできます。

レイヤ 3 配置では、システムは待機するルーテッド インターフェイスがない外部物理インターフェイスで受信されるすべてのトラフィックをドロップします。システムが VLAN タグなしのパケットを受信した場合、該当するポートに物理ルーテッド インターフェイスが設定されていなければ、パケットはドロップされます。システムが VLAN タグ付きのパケットを受信した場合、論理ルーテッド インターフェイスが設定されていなければ、同じくパケットはドロップされます。

システムは、すべてのルール評価または転送決定の前に、入力の最も外側の VLAN タグを取り除くことによって、スイッチド 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を処理します。VLAN タグ付きの論理ルーテッド インターフェイスを通ってデバイスから離れるパケットは出力で関連付けられた VLAN タグによりカプセル化されます。システムは除去プロセスが完了した後、VLAN タグ付きで受信するすべてのトラフィックをドロップします。

親の物理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と、システムは関連するすべての論理インターフェイスを削除することに注意してください。

詳細については、次の各項を参照してください。

- 物理ルーテッド インターフェイスの設定（7-2 ページ）
- 論理ルーテッド インターフェイスの追加（7-5 ページ）
- 論理ルーテッド インターフェイスの削除（7-8 ページ）
- SFRP の設定（7-9 ページ）

物理ルーテッド インターフェイスの設定

ライセンス: Control

サポートされるデバイス: シリーズ 3

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　シリーズ 3 デバイスにルーテッド インターフェイス ペアを追加すると、変更の適用時に Snort プロセスが再起動され、トラフィック インスペクションは一時的に中断されます。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、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、Snort の再開によるトラフィックへの影響（1-9 ページ）を参照してください。

ルーテッド インターフェイスに Address Resolution Protocol（ARP）スタティック エントリを追加できます。外部ホストがトラフィックを送信する、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、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と、仮想ルータは IP アドレスおよび関連付けられている MAC アドレスで応答します。

ルーテッド 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 応答を防ぐことはできません。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 ポリシーにルールを追加できます。ネットワークベースのルールによるトラフィックの制御（15-1 ページ）を参照してください。

管理対象デバイスの [ローカル ルータ トラフィックの検査（Inspect Local Router Traffic）] オプションを有効にした場合、パケットはホストに到達する前にドロップされるため、すべての応答を防ぐことができます。ローカル ルータ トラフィックの検査の詳細については、高度なデバイス設定について（4-59 ページ）を参照してください。

注意　センシング インターフェイスまたはインライン セットの MTU の任意の値（シリーズ 2）または最高値（シリーズ 3）を変更すると、変更を適用する際、変更したインターフェイスだけではなく、デバイス上のすべてのセンシング インターフェイスに対するトラフィック インスペクションが一時的に中断されます。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、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。Snort の再開によるトラフィックへの影響（1-9 ページ）を参照してください。

物理ルーテッド インターフェイスの設定:

アクセス: Admin/Network Admin

手順 1　[デバイス（Devices）] > [デバイス管理（Device Management）] を選択します。

[デバイス管理（Device Management）] ページが表示されます。

手順 2　ルーテッド インターフェイスを設定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。

デバイスの [インターフェイス（Interfaces）] タブが表示されます。

手順 3　ルーテッド インターフェイスとして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。

[インターフェイスの編集（Edit Interface）] ポップアップ ウィンドウが表示されます。

手順 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。

手順 5　オプションで、[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 ゾーンを選択するか、または [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。

手順 6　オプションで、[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するか、または [新規（New）] を選択して新しい仮想ルータを追加します。

新しい仮想ルータを追加する場合、ルーテッド インターフェイスをセットアップした後で、[デバイス管理（Device Management）] ページ（[デバイス（Devices）] > [デバイス管理（Device Management）] > [仮想ルータ（Virtual Routers）]）の [仮想ルータ（Virtual Routers）] タブで設定する必要があることに注意してください。仮想ルータの追加（7-11 ページ）を参照してください。

手順 7　[有効化（Enabled）] チェック ボックスをオンにして、ルーテッド インターフェイスがトラフィックを処理することを許可します。

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。

手順 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(Autonegotiation)] 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。モード設定は銅インターフェイスでのみ使用可能であることに注意してください。

(注)　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。

手順 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 Auto-MDIX のいずれかを指定するオプションを選択します。MDI/MDIX 設定は銅線インターフェイス専用であることに注意してください。

通常、[MDI/MDIX] は [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。

手順 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 ではないことに注意してください。

設定可能な MTU の範囲は、FireSIGHT システムのデバイス モデルおよびインターフェイスのタイプによって異なる場合があります。詳細については、管理対象デバイスの MTU の範囲 (4-70 ページ)を参照してください。

手順 11　[ICMP] の横にある [応答を有効化(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。

手順 12　[IPv6 NDP] の横にある [ルータ アドバタイズメントを有効化(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。

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

[IP アドレスの追加(Add IP Address)] ポップアップ ウィンドウが表示されます。

手順 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。

手順 15　オプションで、IPv6 アドレスを使用している場合は、[IPv6(IPv6)] フィールドの横にある [アドレス自動設定(Address Autoconfiguration)] チェック ボックスをオンにして、インターフェイスの IP アドレスを自動的に設定します。

手順 16　[種類(Type)] には、[ノーマル(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(7-9 ページ)を参照してください。

手順 17　[OK] をクリックします。

IP アドレスが追加されます。

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。

(注)　IP アドレスをクラスタ 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、クラスタ 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。

手順 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。

[スタティック ARP エントリの追加（Add Static ARP Entry）] ポップアップ ウィンドウが表示されます。

手順 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。

手順 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形式を使用して、アドレスを入力します（たとえば、01:23:45:67:89:AB）。

手順 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。

ヒント　スタティック ARP エントリを編集するには、編集アイコン（ ）をクリックします。スタティック ARP エントリを削除するには、削除アイコン（ ）をクリックします。

手順 22　[保存（Save）] をクリックします。

物理ルーテッド インターフェイスが設定されます。デバイス設定を適用するまで、変更は有効になりません。デバイスへの変更の適用（4-27 ページ）を参照してください。

論理ルーテッド インターフェイスの追加

ライセンス：Control

サポートされるデバイス：シリーズ 3

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　シリーズ 3 デバイスにルーテッド インターフェイス ペアを追加すると、変更の適用時に Snort プロセスが再起動され、トラフィック インスペクションは一時的に中断されます。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、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、Snort の再開によるトラフィックへの影響（1-9 ページ）を参照してください。

ルーテッド 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 応答を防ぐことはできません。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 ポリシーにルールを追加できます。ネットワークベースのルールによるトラフィックの制御（15-1 ページ）を参照してください。

管理対象デバイスの [ローカル ルータ トラフィックの検査（Inspect Local Router Traffic）] オプションを有効にした場合、パケットはホストに到達する前にドロップされるため、すべての応答を防ぐことができます。ローカル ルータ トラフィックの検査の詳細については、高度なデバイス設定について（4-59 ページ）を参照してください。

注意　センシング インターフェイスまたはインライン セットの MTU の任意の値（シリーズ 2）または最高値（シリーズ 3）を変更すると、変更を適用する際、変更したインターフェイスだけではなく、デバイス上のすべてのセンシング インターフェイスに対するトラフィック インスペクションが一時的に中断されます。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、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。Snort の再開によるトラフィックへの影響（1-9 ページ）を参照してください。

既存のルーテッド インターフェイスを編集するには、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。

論理ルーテッド インターフェイスの追加:

アクセス: Admin/Network Admin

手順 1　[デバイス（Devices）] > [デバイス管理（Device Management）] を選択します。

[デバイス管理（Device Management）] ページが表示されます。

手順 2　ルーテッド 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。

デバイスの [インターフェイス（Interfaces）] タブが表示されます。

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

[インターフェイスの追加（Add Interface）] ポップアップ ウィンドウが表示されます。

手順 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。

手順 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。

手順 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。

手順 7　オプションで、[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 ゾーンを選択するか、または [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。

手順 8　オプションで、[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するか、または [新規（New）] を選択して新しい仮想ルータを追加します。

新しい仮想ルータを追加する場合、ルーテッド インターフェイスをセットアップした後で、[デバイス管理（Device Management）] ページ（[デバイス（Devices）] > [デバイス管理（Device Management）] > [仮想ルータ（Virtual Routers）]）で設定する必要があることに注意してください。仮想ルータの追加（7-11 ページ）を参照してください。

手順 9　[有効化（Enabled）] チェック ボックスをオンにして、ルーテッド インターフェイスがトラフィックを処理することを許可します。

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。

手順 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 ではないことに注意してください。

設定可能な MTU の範囲は、FireSIGHT システムのデバイス モデルおよびインターフェイスのタイプによって異なる場合があります。詳細については、管理対象デバイスの MTU の範囲（4-70 ページ）を参照してください。

手順 11　[ICMP（ICMP）] の横にある [応答の有効化（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。

手順 12　[IPv6 NDP] の横にある [ルータ アドバタイズメントを有効化（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。

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

[IP アドレスの追加（Add IP Address）] ポップアップ ウィンドウが表示されます。

手順 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。

手順 15　オプションで、IPv6 アドレスを使用している場合は、[IPv6（IPv6）] フィールドの横にある [アドレス自動設定（Address Autoconfiguration）] チェック ボックスをオンにして、インターフェイスの IP アドレスを自動的に設定します。

手順 16　[種類（Type）] には、[ノーマル（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（7-9 ページ）を参照してください。

手順 17　[OK] をクリックします。

IP アドレスが追加されます。

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。

（注）　IP アドレスをクラスタ 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、クラスタ 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。

手順 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。

[スタティック ARP エントリの追加（Add Static ARP Entry）] ポップアップ ウィンドウが表示されます。

手順 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。

手順 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形式を使用して、アドレスを入力します（たとえば、01:23:45:67:89:AB）。

手順 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。

ヒント　スタティック ARP エントリを編集するには、編集アイコン（  ）をクリックします。スタティック ARP エントリを削除するには、削除アイコン（  ）をクリックします。

手順 22　[保存(Save)] をクリックします。

論理ルーテッド インターフェイスが追加されます。デバイス設定を適用するまで、変更は有効になりません。デバイスへの変更の適用(4-27 ページ)を参照してください。

(注)　1 つの物理インターフェイスを無効化すると、その物理インターフェイスに関連付けられた論理インターフェイスも無効化されます。

論理ルーテッド インターフェイスの削除

ライセンス: Control

サポートされるデバイス: シリーズ 3

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。

注意　シリーズ 3 デバイスにルーテッド インターフェイス ペアを追加すると、変更の適用時に Snort プロセスが再起動され、トラフィック インスペクションは一時的に中断されます。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、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、Snort の再開によるトラフィックへの影響(1-9 ページ)を参照してください。

ルーテッド インターフェイスを削除する方法:

アクセス: Admin/Network Admin

手順 1　[デバイス(Devices)] > [デバイス管理(Device Management)] を選択します。

[デバイス管理(Device Management)] ページが表示されます。

手順 2　ルーテッド インターフェイスを削除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。

デバイスの [インターフェイス(Interfaces)] タブが表示されます。

手順 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。

手順 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。

インターフェイスが削除されます。デバイス設定を適用するまで、変更は有効になりません。デバイスへの変更の適用(4-27 ページ)を参照してください。

SFRP の設定

ライセンス: Control

サポートされるデバイス: シリーズ 3

Cisco 冗長プロトコル（SFRP）を設定して、デバイスのクラスタ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、同じ数のバックアップを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。

仮想ルータの SFRP の IP アドレスを有効にするには、少なくとも 1 つの非 SFRP IP アドレスを設定する必要があります。

クラスタ デバイスの場合、共有秘密を指定すると、SFRP の IP 設定とともにクラスタ 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） クラスタ化された シリーズ 3 デバイス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。

クラスタ デバイスの詳細については、デバイスのクラスタリング（4-31 ページ）を参照してください。

SFRP を設定する方法:

アクセス: Admin/Network Admin

手順 1　[デバイス（Devices）] > [デバイス管理（Device Management）] を選択します。

[デバイス管理（Device Management）] ページが表示されます。

手順 2　SFRP を設定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。

デバイスの [インターフェイス（Interfaces）] タブが表示されます。

手順 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。

[インターフェイスの編集（Edit Interface）] ポップアップ ウィンドウが表示されます。

手順 4　SFRP を設定するインターフェイスのタイプを選択します。

- [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。
- [ハイブリッド（Hybrid）] をクリックして、ハイブリッド インターフェイス オプションを表示します。

手順 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。

- IP アドレスを追加するには、[追加（Add）] 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 アドレスの追加（Add IP Address）] ポップアップ ウィンドウまたは [IP アドレスの編集（Edit IP Address）] ポップアップ ウィンドウが表示されます。

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

手順 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。

手順 8　[優先順位（Priority）] に [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。
- デバイスのクラスタの場合、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。

手順 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、デバイスのクラスタ内のグループに関するデータが自動的に入力されます。

手順 10　[アドバタイズメントの間隔:（Advertisement Interval:）] 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。

手順 11　[OK] をクリックします。

IP アドレスが追加または編集されます。

手順 12　[保存（Save）] をクリックします。

変更が保存されます。デバイス設定を適用するまで、変更は有効になりません。デバイスへの変更の適用（4-27 ページ）を参照してください。

仮想ルータの設定

ライセンス: Control

サポートされるデバイス: シリーズ 3

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。

仮想ルータの設定の詳細については、次の項を参照してください。

- 仮想ルータの表示（7-11 ページ）
- 仮想ルータの追加（7-11 ページ）
- 仮想ルータ統計情報の表示（7-35 ページ）
- 仮想ルータの削除（7-36 ページ）

仮想ルータの表示

ライセンス: Control

サポートされるデバイス:シリーズ 3

[デバイス管理(Device Management)] ページ([デバイス(Devices)] > [デバイス管理(Device Management)] > [仮想ルータ(Virtual Routers)])の [仮想ルータ(Virtual Routers)] タブには、デバイスに設定されているすべての仮想ルータのリストが表示されます。このテーブルには次の表に示すように、各ルータに関するサマリー情報が含まれます。

表 7-1　仮想ルータのテーブル ビュー フィールド

フィールド	説明
[名前(Name)]	仮想ルータの名前。
インターフェイス	仮想ルータに割り当てられたすべてのルーテッド インターフェイスのリスト。[インターフェイス(Interfaces)] タブからインターフェイスを無効にすると削除されます。
プロトコル(Protocols)	仮想ルータによって現在使用されているプロトコル。次のいずれかです。 • 静的 • スタティック、RIP • スタティック、OSPF

仮想ルータの追加

ライセンス: Control

サポートされるデバイス:シリーズ 3

[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。

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。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。

最大の TCP セキュリティを実現するには、厳密な適用(強制)を有効にできます。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
- レスポンダが SYN-ACK を送信する前に TCP 接続のイニシエータから送信された非 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
- イニシエータまたはレスポンダから確立された 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。既存の仮想ルータに対する変更により、デバイスのトラフィックが中断される可能性があります。

ヒント　既存の仮想ルータを編集するには、ルータの横にある編集アイコン（）をクリックします。

一般的なオプションに加え、いくつかの異なる方法で仮想ルータを設定できます。これらの設定の詳細については、次の項を参照してください。

- DHCP リレーのセットアップ（7-13 ページ）
- スタティック ルートのセットアップ（7-15 ページ）
- ダイナミック ルーティングのセットアップ（7-17 ページ）
- RIP 設定のセットアップ（7-18 ページ）
- OSPF 設定のセットアップ（7-23 ページ）
- 仮想ルータ フィルタのセットアップ（7-32 ページ）
- 仮想ルータ認証プロファイルの追加（7-34 ページ）

仮想ルータを追加する方法:

アクセス: Admin/Network Admin

手順 1　[デバイス（Devices）] > [デバイス管理（Device Management）] を選択します。

[デバイス管理（Device Management）] ページが表示されます。

手順 2　仮想ルータ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。

デバイスの [インターフェイス（Interfaces）] タブが表示されます。

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

[仮想ルータ（Virtual Routers）] タブが表示されます。

ヒント　デバイスがクラスタ スタック配置にある場合、[選択済み（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。

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

[仮想ルータの追加（Add Virtual Router）] ポップアップ ウィンドウが表示されます。

手順 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。

手順 6　仮想ルータで IPv6 スタティック ルーティング、OSPFv3、および RIPng を有効にするには、[IPv6 サポート（IPv6 Support）] チェック ボックスをオンにします。これらの機能を無効にするには、チェック ボックスをオフにします。

手順 7　オプションで、厳密な TCP 適用を有効にしない場合は、[厳格な TCP の強制（Strict TCP Enforcement）] 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。

手順 8　[インターフェイス（Interfaces）] の下の [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。仮想ルータに割り当てる 1 つ以上のインターフェイスを選択して、[追加（Add）] をクリックします。

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。

手順 9　[保存（Save）] をクリックします。

仮想ルータが追加されます。デバイス設定を適用するまで、変更は有効になりません。デバイスへの変更の適用（4-27 ページ）を参照してください。

DHCP リレーのセットアップ

ライセンス：Control

サポートされるデバイス：シリーズ 3

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。

詳細については、次の各項を参照してください。

- DHCPv4 リレーのセットアップ（7-13 ページ）
- DHCPv6 リレーのセットアップ（7-14 ページ）

DHCPv4 リレーのセットアップ

ライセンス：Control

サポートされるデバイス：シリーズ 3

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。

DHCPv4 リレーを設定する方法：

アクセス：Admin/Network Admin

手順 1　[デバイス（Devices）] > [デバイス管理（Device Management）] を選択します。

[デバイス管理（Device Management）] ページが表示されます。

手順 2　DHCP リレーを設定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。

デバイスの [インターフェイス（Interfaces）] タブが表示されます。

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

[仮想ルータ（Virtual Routers）] タブが表示されます。

手順 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。

[仮想ルータの編集（Edit Virtual Router）] ポップアップ ウィンドウが表示されます。

手順 5　DHCPv4 の DHCP リレーを設定するには、[DHCPv4（DHCPv4）] チェック ボックスをオンにします。

手順 6　[サーバ（Servers）] フィールドの下に、サーバの IP アドレスを入力します。

手順 7　[追加（Add）] をクリックします。

[サーバ（Servers）] フィールドに IP アドレスが追加されます。最大 4 台の DHCP サーバを追加できます。

ヒント　DHCP サーバを削除するには、サーバの IP アドレスの横にある削除アイコン（ ）をクリックします。

手順 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。

手順 9　[保存（Save）] をクリックします。

変更が保存されます。デバイス設定を適用するまで、変更は有効になりません。デバイスへの変更の適用（4-27 ページ）を参照してください。

DHCPv6 リレーのセットアップ

ライセンス：Control

サポートされるデバイス：シリーズ 3

次の手順は、仮想ルータで DHCPv6 リレーを設定する方法について説明します。

（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。

DHCPv6 リレーを設定する方法：

アクセス：Admin/Network Admin

手順 1　[デバイス（Devices）] > [デバイス管理（Device Management）] を選択します。

[デバイス管理（Device Management）] ページが表示されます。

手順 2　DHCP リレーを設定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。

デバイスの [インターフェイス（Interfaces）] タブが表示されます。

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

[仮想ルータ（Virtual Routers）] タブが表示されます。

手順 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。

[仮想ルータの編集（Edit Virtual Router）] ポップアップ ウィンドウが表示されます。

手順 5　DHCPv6 の DHCP リレーを設定するには、[DHCPv6(DHCPv6)] チェック ボックスをオンにします。

手順 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。

手順 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。

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ることに注意してください。両方を選択することは、インターフェイスはダウンストリームおよびアップストリームの両方であることを意味します。

手順 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。

手順 9　[保存(Save)] をクリックします。

変更が保存されます。デバイス設定を適用するまで、変更は有効になりません。デバイスへの変更の適用(4-27 ページ)を参照してください。

スタティック ルートのセットアップ

ライセンス: Control

サポートされるデバイス:シリーズ 3

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。

詳細については、次の各項を参照してください。

- スタティック ルート テーブル ビューについて(7-15 ページ)
- スタティック ルートの追加(7-16 ページ)

スタティック ルート テーブル ビューについて

ライセンス: Control

サポートされるデバイス:シリーズ 3

仮想ルータ エディタの [スタティック ルート(Static Routes)] タブには、仮想ルータに設定されているすべてのスタティック ルートのリストが表示されます。この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 7-2　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（Type）	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（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。 • [廃棄（Discard）]：スタティック ルートでパケットが廃棄され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。

スタティック ルートの追加

ライセンス：Control

サポートされるデバイス：シリーズ 3

次の手順は、スタティック ルートを追加する方法について説明します。

スタティック ルートを編集するには、編集アイコン（ ）をクリックします。スタティック ルートを削除するには、削除アイコン（ ）をクリックします。

スタティック ルートの追加：

アクセス：Admin/Network Admin

手順 1　[デバイス（Devices）] > [デバイス管理（Device Management）] を選択します。

[デバイス管理（Device Management）] ページが表示されます。

手順 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。

デバイスの [インターフェイス（Interfaces）] タブが表示されます。

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

[仮想ルータ（Virtual Routers）] タブが表示されます。

手順 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。

[仮想ルータの編集（Edit Virtual Router）] ポップアップ ウィンドウが表示されます。

手順 5　[スタティック（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。

手順 6　[スタティック ルートの追加(Add Static Route)] をクリックします。

[スタティック ルートの追加(Add Static Route)] ポップアップ ウィンドウが表示されます。

手順 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。

手順 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。

手順 9　[設定(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。

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。

手順 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。

手順 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。

手順 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(IP)] を選択した場合は、IP アドレスを入力します。
- 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。

手順 13　[OK] をクリックします。

スタティック ルートが追加されます。

手順 14　[保存(Save)] をクリックします。

変更が保存されます。デバイス設定を適用するまで、変更は有効になりません。デバイスへの変更の適用(4-27 ページ)を参照してください。

ダイナミック ルーティングのセットアップ

ライセンス: Control

サポートされるデバイス: シリーズ 3

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。

詳細については、次の各項を参照してください。

- RIP 設定のセットアップ(7-18 ページ)
- OSPF 設定のセットアップ(7-23 ページ)

RIP 設定のセットアップ

ライセンス：Control

サポートされるデバイス：シリーズ 3

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 設定の詳細については、次の項を参照してください。

- RIP 設定用インターフェイスの追加（7-18 ページ）
- RIP 設定の認証設定（7-19 ページ）
- RIP の高度な設定（7-20 ページ）
- RIP 設定のインポート フィルタの追加（7-21 ページ）
- RIP 設定へのエクスポート フィルタの追加（7-22 ページ）

RIP 設定用インターフェイスの追加

ライセンス：Control

サポートされるデバイス：シリーズ 3

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。

RIP 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。RIP 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。

RIP 設定でインターフェイスの追加：

アクセス：Admin/Network Admin

手順 1　[デバイス（Devices）] > [デバイス管理（Device Management）] を選択します。

[デバイス管理（Device Management）] ページが表示されます。

手順 2　RIP 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。

デバイスの [インターフェイス（Interfaces）] タブが表示されます。

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

[仮想ルータ（Virtual Routers）] タブが表示されます。

手順 4　RIP 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。

[仮想ルータの編集（Edit Virtual Router）] ポップアップ ウィンドウが表示されます。

手順 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。

手順 6　[RIP（RIP）] をクリックして、RIP オプションを表示します。

手順 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。

[インターフェイスの追加（Add an Interface）] ポップアップ ウィンドウが表示されます。

手順 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。

手順 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。

手順 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。

手順 11　[保存（Save）] をクリックします。

変更が保存されます。デバイス設定を適用するまで、変更は有効になりません。デバイスへの変更の適用（4-27 ページ）を参照してください。

RIP 設定の認証設定

ライセンス：Control

サポートされるデバイス：シリーズ 3

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。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（7-34 ページ）を参照してください。

RIP 設定の認証設定：

アクセス：Admin/Network Admin

手順 1　[デバイス（Devices）] > [デバイス管理（Device Management）] を選択します。

[デバイス管理（Device Management）] ページが表示されます。

手順 2　RIP 認証プロファイル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。

デバイスの [インターフェイス（Interfaces）] タブが表示されます。

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

[仮想ルータ（Virtual Routers）] タブが表示されます。

手順 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。

[仮想ルータの編集（Edit Virtual Router）] ポップアップ ウィンドウが表示されます。

手順 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。

手順 6　[RIP（RIP）] をクリックして、RIP オプションを表示します。

手順 7　[認証（Authentication）] の下の [プロファイル（Profile）] ドロップダウン リストを使用して、既存の仮想ルータ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。

手順 8　[保存（Save）] をクリックします。

変更が保存されます。デバイス設定を適用するまで、変更は有効になりません。デバイスへの変更の適用（4-27 ページ）を参照してください。

RIP の高度な設定

ライセンス：Control

サポートされるデバイス：シリーズ 3

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。

RIP の高度な設定：

アクセス：Admin/Network Admin

手順 1　[デバイス（Devices）] > [デバイス管理（Device Management）] を選択します。

[デバイス管理（Device Management）] ページが表示されます。

手順 2　RIP の詳細設定を編集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。

デバイスの [インターフェイス（Interfaces）] タブが表示されます。

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

[仮想ルータ（Virtual Routers）] タブが表示されます。

手順 4　RIP の詳細設定を編集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。

[仮想ルータの編集（Edit Virtual Router）] ポップアップ ウィンドウが表示されます。

手順 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。

手順 6　[RIP（RIP）] をクリックして、RIP オプションを表示します。

手順 7　[設定（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。

手順 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。

手順 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。

手順 10　[破棄時間（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。

手順 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。

手順 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

手順 13　[保存(Save)] をクリックします。

変更が保存されます。デバイス設定を適用するまで、変更は有効になりません。デバイスへの変更の適用(4-27 ページ)を参照してください。

RIP 設定のインポート フィルタの追加

ライセンス: Control

サポートされるデバイス: シリーズ 3

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。フィルタの設定の詳細については、仮想ルータ フィルタのセットアップ(7-32 ページ)を参照してください。

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。

RIP 設定へのインポート フィルタの追加:

アクセス: Admin/Network Admin

手順 1　[デバイス(Devices)] > [デバイス管理(Device Management)] を選択します。

[デバイス管理(Device Management)] ページが表示されます。

手順 2　RIP 仮想ルータ フィルタ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。

デバイスの [インターフェイス(Interfaces)] タブが表示されます。

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

[仮想ルータ(Virtual Routers)] タブが表示されます。

手順 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。

[仮想ルータの編集(Edit Virtual Router)] ポップアップ ウィンドウが表示されます。

手順 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。

手順 6　[RIP(RIP)] をクリックして、RIP オプションを表示します。

手順 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。

[インポート フィルタの追加(Add an Import Filter)] ポップアップ ウィンドウが表示されます。

手順 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。

手順 9　[アクション(Action)] の横にある [許可(Accept)] または [却下(Reject)] を選択します。

手順 10　[OK] をクリックします。

インポート フィルタが追加されます。

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。

手順 11　[保存(Save)] をクリックします。

変更が保存されます。デバイス設定を適用するまで、変更は有効になりません。デバイスへの変更の適用(4-27 ページ)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

ライセンス: Control

サポートされるデバイス: シリーズ 3

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。フィルタの設定の詳細については、仮想ルータ フィルタのセットアップ(7-32 ページ)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:

アクセス: Admin/Network Admin

手順 1　[デバイス(Devices)] > [デバイス管理(Device Management)] を選択します。

[デバイス管理(Device Management)] ページが表示されます。

手順 2　RIP 仮想ルータ フィルタ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。

デバイスの [インターフェイス(Interfaces)] タブが表示されます。

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

[仮想ルータ(Virtual Routers)] タブが表示されます。

手順 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。

[仮想ルータの編集(Edit Virtual Router)] ポップアップ ウィンドウが表示されます。

手順 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。

手順 6　[RIP(RIP)] をクリックして、RIP オプションを表示します。

手順 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。

[エクスポート フィルタの追加(Add an Export Filter)] ポップアップ ウィンドウが表示されます。

手順 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。

手順 9　[アクション(Action)] の横にある [許可(Accept)] または [却下(Reject)] を選択します。

手順 10　[OK] をクリックします。

エクスポート フィルタが追加されます。

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。

手順 11　[保存(Save)] をクリックします。

変更が保存されます。デバイス設定を適用するまで、変更は有効になりません。デバイスへの変更の適用(4-27 ページ)を参照してください。

OSPF 設定のセットアップ

ライセンス: Control

サポートされるデバイス:シリーズ 3

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。

詳細については、次の各項を参照してください。

- OSPF ルーティング エリアのセットアップ(7-23 ページ)
- OSPF 設定のインポート フィルタの追加(7-30 ページ)
- OSPF 設定へのエクスポート フィルタの追加(7-31 ページ)

OSPF ルーティング エリアのセットアップ

ライセンス: Control

サポートされるデバイス:シリーズ 3

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 エリアのセットアップの詳細については、次の項を参照してください。

- OSPF エリアの追加（7-24 ページ）
- OSPF エリア インターフェイスの追加（7-25 ページ）
- OSPF エリア vlink の追加（7-28 ページ）

OSPF エリアの追加

ライセンス：Control

サポートされるデバイス：シリーズ 3

次の手順は、OSPF エリアを追加し、一般設定を構成する方法について説明します。

OSPF エリアの追加：

アクセス：Admin/Network Admin

手順 1　[デバイス（Devices）] > [デバイス管理（Device Management）] を選択します。

[デバイス管理（Device Management）] ページが表示されます。

手順 2　OSPF の一般オプションを編集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。

デバイスの [インターフェイス（Interfaces）] タブが表示されます。

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

[仮想ルータ（Virtual Routers）] タブが表示されます。

手順 4　OSPF の一般オプションを編集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。

[仮想ルータの編集（Edit Virtual Router）] ポップアップ ウィンドウが表示されます。

手順 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。

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

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

[OSPF エリアの追加（Add OSPF Area）] ポップアップ ウィンドウが表示されます。

手順 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。

手順 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。

[デフォルト コスト（Default cost）] フィールドと [スタブネット（Stubnet）] フィールドが表示されます。

手順 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。

手順 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。

手順 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。

手順 13　[非表示（Hidden）] チェック ボックスをオンにして、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。

手順 14 [概要(Summary)] チェック ボックスをオンにして、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。

手順 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。

手順 16 [OK] をクリックします。

スタブネットが追加されます。

ヒント スタブネットを編集するには、編集アイコン( )をクリックします。スタブネットを削除するには、削除アイコン( )をクリックします。

手順 17 オプションで、[ネットワーク(Networks)] の下の追加アイコン( )をクリックします。

手順 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。

手順 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。

手順 20 [OK] をクリックします。

ネットワークが追加されます。

ヒント ネットワークを編集するには、編集アイコン( )をクリックします。ネットワークを削除するには、削除アイコン( )をクリックします。

手順 21 [保存(Save)] をクリックします。

変更が保存されます。デバイス設定を適用するまで、変更は有効になりません。デバイスへの変更の適用(4-27 ページ)を参照してください。

OSPF エリア インターフェイスの追加

ライセンス: Control

サポートされるデバイス: シリーズ 3

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。
- [非ブロードキャスト(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。

非ブロードキャスト

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(7-34 ページ)を参照してください。

Hello インターバル

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

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

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

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

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

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。

（注）　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。

OSPF エリア インターフェイスの追加:

アクセス: Admin/Network Admin

手順 1　[デバイス（Devices）] > [デバイス管理（Device Management）] を選択します。

[デバイス管理（Device Management）] ページが表示されます。

手順 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。

デバイスの [インターフェイス（Interfaces）] タブが表示されます。

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

[仮想ルータ（Virtual Routers）] タブが表示されます。

手順 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。

[仮想ルータの編集（Edit Virtual Router）] ポップアップ ウィンドウが表示されます。

手順 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。

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

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

[OSPF エリアの追加（Add OSPF Area）] ポップアップ ウィンドウが表示されます。

手順 8　[インターフェイス（Interfaces）] をクリックします。

[インターフェイス（Interfaces）] タブが表示されます。

手順 9　追加アイコン（ ）をクリックします。

[OSPF エリア インターフェイスの追加（Add OSPF Area Interface）] ポップアップ ウィンドウが表示されます。

手順 10　OSPF エリア インターフェイスの追加（7-25 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。

手順 11　オプションで、[ネイバー（Neighbors）] の下の追加アイコン（ ）をクリックします。

手順 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。

手順 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。

手順 14　[OK] をクリックします。

ネイバーが追加されます。

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。

手順 15　[OK] をクリックします。

OSPF エリア インターフェイスが追加されます。

手順 16　[保存（Save）] をクリックします。

OSPF エリアが保存されます。

手順 17　[保存（Save）] をクリックします。

変更が保存されます。デバイス設定を適用するまで、変更は有効になりません。デバイスへの変更の適用（4-27 ページ）を参照してください。

OSPF エリア vlink の追加

ライセンス：Control

サポートされるデバイス：シリーズ 3

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。

OSPF エリア vlink の追加:

アクセス: Admin/Network Admin

手順 1　[デバイス(Devices)] > [デバイス管理(Device Management)] を選択します。

[デバイス管理(Device Management)] ページが表示されます。

手順 2　OSPF vlink 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。

デバイスの [インターフェイス(Interfaces)] タブが表示されます。

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

[仮想ルータ(Virtual Routers)] タブが表示されます。

手順 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。

[仮想ルータの編集(Edit Virtual Router)] ポップアップ ウィンドウが表示されます。

手順 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。

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

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

[OSPF エリアの追加(Add OSPF Area)] ポップアップ ウィンドウが表示されます。

手順 8　[vlink(Vlinks)] をクリックします。

[vlink(Vlinks)] タブが表示されます。

手順 9　追加アイコン( )をクリックします。

[OSPF エリア vlink の追加(Add OSPF Area Vlink)] ポップアップ ウィンドウが表示されます。

手順 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。

手順 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。

手順 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。

手順 13　[再送間隔(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。

手順 14　[待ち時間(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。

手順 15　[デッド間隔(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。

手順 16　[無レスポンス カウント(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。

手順 17　[OK] をクリックします。

OSPF エリア vlink が追加されます。

手順 18　[保存(Save)] をクリックします。

OSPF エリアが保存されます。

手順 19　[保存(Save)] をクリックします。

変更が保存されます。デバイス設定を適用するまで、変更は有効になりません。デバイスへの変更の適用(4-27 ページ)を参照してください。

OSPF 設定のインポート フィルタの追加

ライセンス：Control

サポートされるデバイス：シリーズ 3

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。フィルタの設定の詳細については、仮想ルータ フィルタのセットアップ（7-32 ページ）を参照してください。

OSPF 設定のインポート フィルタの追加：

アクセス：Admin/Network Admin

手順 1　[デバイス（Devices）] > [デバイス管理（Device Management）] を選択します。

[デバイス管理（Device Management）] ページが表示されます。

手順 2　OSPF 仮想ルータ フィルタ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。

デバイスの [インターフェイス（Interfaces）] タブが表示されます。

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

[仮想ルータ（Virtual Routers）] タブが表示されます。

手順 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。

[仮想ルータの編集（Edit Virtual Router）] ポップアップ ウィンドウが表示されます。

手順 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。

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

手順 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。

[インポート フィルタの追加（Add Import Filter）] ポップアップ ウィンドウが表示されます。

手順 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。

手順 9　[アクション（Action）] の横にある [許可（Accept）] または [却下（Reject）] を選択します。

手順 10　[OK] をクリックします。

インポート フィルタが追加されます。

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。

手順 11　[保存（Save）] をクリックします。

変更が保存されます。デバイス設定を適用するまで、変更は有効になりません。デバイスへの変更の適用（4-27 ページ）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

ライセンス：Control

サポートされるデバイス：シリーズ 3

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。フィルタの設定の詳細については、仮想ルータ フィルタのセットアップ（7-32 ページ）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：

アクセス：Admin/Network Admin

手順 1　[デバイス（Devices）] > [デバイス管理（Device Management）] を選択します。

[デバイス管理（Device Management）] ページが表示されます。

手順 2　OSPF 仮想ルータ フィルタ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。

デバイスの [インターフェイス（Interfaces）] タブが表示されます。

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

[仮想ルータ（Virtual Routers）] タブが表示されます。

手順 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。

[仮想ルータの編集（Edit Virtual Router）] ポップアップ ウィンドウが表示されます。

手順 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。

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

手順 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。

[エクスポート フィルタの追加（Add an Export Filter）] ポップアップ ウィンドウが表示されます。

手順 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。

手順 9　[アクション（Action）] の横にある [許可（Accept）] または [却下（Reject）] を選択します。

手順 10　[OK] をクリックします。

エクスポート フィルタが追加されます。

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。

手順 11　[保存（Save）] をクリックします。

変更が保存されます。デバイス設定を適用するまで、変更は有効になりません。デバイスへの変更の適用（4-27 ページ）を参照してください。

仮想ルータ フィルタのセットアップ

ライセンス: Control

サポートされるデバイス:シリーズ 3

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。

ヒント　仮想ルータ 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。仮想ルータ 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。

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。このテーブルには次の表に示すように、各フィルタに関するサマリー情報が含まれます。

表 7-3　仮想ルータ フィルタ テーブル ビュー 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(RIP)]:ルートはダイナミックな RIP 設定から発生します。 • [OSPF(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。
ネクスト ホップ(Next Hop)	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 • Device • 廃棄
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。 • 外部 1(Ext-1) • 外部 2(Ext-2) • エリア間(Inter Area) • エリア内(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 フィルタの追加:

アクセス: Admin/Network Admin

手順 1　[デバイス(Devices)] > [デバイス管理(Device Management)] を選択します。

[デバイス管理(Device Management)] ページが表示されます。

手順 2　仮想フィルタ ルータ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。

デバイスの [インターフェイス(Interfaces)] タブが表示されます。

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

[仮想ルータ(Virtual Routers)] タブが表示されます。

手順 4　仮想フィルタ ルー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。

[仮想ルータの編集(Edit Virtual Router)] ポップアップ ウィンドウが表示されます。

手順 5　[フィルタ(Filter)] をクリックして、フィルタ オプションを表示します。

手順 6　[フィルタの追加(Add Filter)] をクリックします。

[フィルタの作成(Create Filter)] ポップアップ ウィンドウが表示されます。

手順 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。

手順 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。

手順 9　プロトコルとして [すべて(All)]、[スタティック(Static)]、または [RIP(RIP)] を選択した場合、[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。

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あることに注意してください。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。

手順 10　[追加(Add)] をクリックします。

[ルータから(From Router)] フィールドに値が入力されます。

手順 11　プロトコルとして [すべて(All)]、[スタティック(Static)]、または [RIP(RIP)] を選択した場合、[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。

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あることに注意してください。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。

手順 12　[追加(Add)] をクリックします。

[ネクスト ホップ(Next Hop)] フィールドに値が入力されます。

手順 13　[宛先タイプ(Destination Type)] で、フィルタに適用するオプションを選択します。

手順 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。

手順 15　[追加(Add)] をクリックします。

[宛先ネットワーク(Destination Network)] フィールドに値が入力されます。

手順 16　プロトコルとして [すべて(All)] または [OSPF(OSPF)] を選択した場合、[パス 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。

手順 17　プロトコルとして [OSPF(OSPF)] を選択した場合、[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。

手順 18　[追加(Add)] をクリックします。

[ルータ ID(Router ID)] フィールドに値が入力されます。

手順 19　[OK] をクリックします。

フィルタが追加されます。

手順 20　[保存(Save)] をクリックします。

変更が保存されます。デバイス設定を適用するまで、変更は有効になりません。デバイスへの変更の適用(4-27 ページ)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

ライセンス: Control

サポートされるデバイス:シリーズ 3

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。

ヒント　認証プロファイルを編集するには、編集アイコン( )をクリックします。認証プロファイルを削除するには、削除アイコン( )をクリックします。

仮想ルータ認証プロファイルの追加:

アクセス: Admin/Network Admin

手順 1　[デバイス(Devices)] > [デバイス管理(Device Management)] を選択します。

[デバイス管理(Device Management)] ページが表示されます。

手順 2　仮想ルータ認証プロファイル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。

デバイスの [インターフェイス(Interfaces)] タブが表示されます。

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

[仮想ルータ(Virtual Routers)] タブが表示されます。

手順 4　仮想ルータ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。

[仮想ルータの編集(Edit Virtual Router)] ポップアップ ウィンドウが表示されます。

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

[認証プロファイル(Authentication Profile)] タブが表示されます。

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

[認証プロファイルの追加（Add Authentication Profile）] ポップアップ ウィンドウが表示されます。

手順 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。

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

手順 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。

手順 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。

手順 11　[OK] をクリックします。

認証プロファイルが追加されます。

手順 12　[保存（Save）] をクリックします。

変更が保存されます。デバイス設定を適用するまで、変更は有効になりません。デバイスへの変更の適用（4-27 ページ）を参照してください。

仮想ルータ統計情報の表示

ライセンス：Control

サポートされるデバイス：シリーズ 3

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。

仮想ルータの統計情報の表示：

アクセス：Admin/Network Admin

手順 1　[デバイス（Devices）] > [デバイス管理（Device Management）] を選択します。

[デバイス管理（Device Management）] ページが表示されます。

手順 2　仮想ルータ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。

デバイスの [インターフェイス（Interfaces）] タブが表示されます。

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

[仮想ルータ（Virtual Routers）] タブが表示されます。

手順 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。

[統計情報（Statistics）] ポップアップ ウィンドウが表示されます。

手順 5　[OK] をクリックしてウィンドウを閉じます。

仮想ルータの削除

ライセンス：Control

サポートされるデバイス：シリーズ 3

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。

仮想ルータの削除：

アクセス：Admin/Network Admin

手順 1　[デバイス（Devices）] > [デバイス管理（Device Management）] を選択します。

[デバイス管理（Device Management）] ページが表示されます。

手順 2　仮想ルータを削除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。

デバイスの [インターフェイス（Interfaces）] タブが表示されます。

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

[仮想ルータ（Virtual Routers）] タブが表示されます。

手順 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。

手順 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。

仮想ルータが削除されます。デバイス設定を適用するまで、変更は有効になりません。デバイスへの変更の適用（4-27 ページ）を参照してください。
