CHAPTER 14

ダイナミック ルーティングおよびスタティック ルーティングの設定

Routing 領域では、スタティック ルートを編集し、セキュリティ アプライアンスがホストまたはネットワークを宛先としたネットワーク パケットを正しく転送できるようにします。また、スタティック ルートを使用して、ダイナミック ルートで検出されたメトリックより低いメトリックでスタティック ルートを指定することで、このホストまたはネットワークに対して検出されたダイナミック ルートを上書きできます。ホストまたはネットワークにスタティック ルートを作成するには、選択したホストまたはネットワークを宛先としたパケットをセキュリティ アプライアンスが転送する先の、ホップ ゲートウェイの IP アドレスおよびメトリックを定義する必要があります。また、1 つのホストまたはネットワークに対して複数のスタティック ルートを定義できます。

ここでは、次の項目について説明します。

Dynamic Routing

Dynamic Routing 領域には、次の項目があります。

- OSPF
- RIP

OSPF

OSPF は、パスの選択に距離ベクトルではなくリンク状態を使用する内部ゲートウェイ ルーティング プロトコルです。OSPF は、ルーティング テーブル更新ではなくリンクステート アドバタイズメントをプロパゲートします。ルーティング テーブル全体ではなく、LSA だけが変更されるため、OSPF ネットワークは、RIP ネットワークよりすばやく集約できます。

OSPF は、MD5 およびクリア テキスト ネイバー認証をサポートします。OSPF と他のプロトコル（RIP など）の間でのルート再配布は、攻撃者によるルーティング情報の悪用に使用される可能性があるため、すべてのルーティング プロトコルに可能な限り認証を使用する必要があります。

NAT が使用されている場合、パブリック エリアおよびプライベート エリアで OSPF が実行されている場合、およびアドレス フィルタリングが必須である場合、2 つの OSPF プロセスを実行する必要があります。このとき、1 つはパブリック エリアのプロセス用、もう 1 つはプライベート エリアのプロセス用になります。

複数のエリアにインターフェイスを持つルータは、Area Border Router（ABR; エリア境界ルータ）と呼ばれます。ゲートウェイとして動作し、OSPF を使用しているルータとルーティング プロトコルを使用している他のルータとの間にトラフィックを再配布するルータは、Autonomous System Boundary Router（ASBR; 自律システム境界ルータ）と呼ばれます。

ABR は LSA を使用して、使用可能なルートに関する情報を他の OSPF ルータに送信します。ABR タイプ 3 LSA フィルタリングを使用すれば、セキュリティ アプライアンスが ABR として動作するプライベート エリアおよびパブリック エリアを分けることができます。タイプ 3 LSA（エリア間ルート）は、あるエリアから別のエリアにフィルタリングできます。このフィルタリングにより、プライベート ネットワークをアドバタイズすることなく NAT と OSPF を一緒に使用できます。

（注）　フィルタリングできるのは、タイプ 3 LSA だけです。セキュリティ アプライアンスを ASBR としてプライベート ネットワークで設定している場合、プライベート ネットワークを説明するタイプ 5 LSA が送信され、パブリック エリアを含む AS 全体に対してフラッディングされます。

NAT は使用されているが、OSPF がパブリック エリアでのみ実行されている場合、パブリック ネットワークへのルートは、プライベート ネットワーク内でデフォルトまたはタイプ 5 AS External LSA として再配布できます。ただし、セキュリティ アプライアンスで保護されているプライベート ネットワークにスタティック ルートを設定する必要があります。また、同一セキュリティ アプライアンス インターフェイス上にパブリック ネットワークとプライベート ネットワークを混在させないでください。

2 つの OSPF ルーティング プロセスと 1 つの RIP ルーティング プロセスをセキュリティ アプライアンスで同時に保持できます。

OSPF のイネーブル化および設定の詳細については、次の項目を参照してください。

- Setup
- Interface

- Static Neighbor
- Virtual Link
- Filtering
- Redistribution
- Summary Address

Setup

Configuration > Routing > Dynamic Routing > OSPF > Setup

Setup ペインでは、OSPF プロセスをイネーブルにし、OSPF エリアおよびネットワークを設定して、OSPF ルート集約を定義できます。

これらのエリアの設定の詳細については、次の項目を参照してください。

- Setup > Process Instances タブ
- Setup > Area/Networks タブ
- Setup > Route Summarization タブ

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Setup > Process Instances タブ

Configuration > Routing > Dynamic Routing > OSPF > Setup > Process Instances タブ

OSPF プロセス インスタンスを 2 つまでイネーブルにできます。各 OSPF プロセスは、独自の関連エリアおよびネットワークを持ちます。

フィールド

- OSPF Process 1 エリアおよび OSPF Process 2 エリア：各エリアには、特定の OSPF プロセスのための設定が含まれます。
- Enable this OSPF Process：チェックボックスをオンにすると、OSPF プロセスをイネーブルにします。OSPF プロセスを削除するには、チェックボックスをオフにします。
- OSPF Process ID：OSPF プロセスの一意の数値 ID を入力します。このプロセス ID は内部的に使用され、他の OSPF デバイス上の OSPF プロセス ID に一致している必要はありません。有効値の範囲は、1 ～ 65535 です。
- Advanced：Edit OSPF Process Advanced Properties ダイアログボックスが開きます。このダイアログボックスでは、Router ID、djacency Changes、Administrative Route Distances、Timers、および Default Information Originate の各種設定を実行できます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Edit OSPF Process Advanced Properties

Configuration > Routing > Dynamic Routing > OSPF > Setup > Process Instances > Edit OSPF Process Advanced Properties

Edit OSPF Process Advanced Properties ダイアログボックスでは、Router ID、Adjacency Changes、Administrative Route Distances、Timers、および Default Information Originate 設定など、プロセス固有の設定を編集できます。

フィールド

- OSPF Process：設定している OSPF プロセスを表示します。この値は変更できません。
- Router ID：固定ルータ ID を使用するには、Router ID フィールドに IP アドレス形式でルータ ID を入力します。この値を空白にすると、セキュリティ アプライアンスで最高レベルの IP アドレスがルータ ID として使用されます。
- Ignore LSA MOSPF：このチェックボックスをオンにすると、セキュリティ アプライアンスがタイプ 6（MOSPF）LSA パケットを受信したときのシステム ログ メッセージの送信を抑止します。デフォルトでは、この設定はオフになっています。
- RFC 1583 Compatible：このチェックボックスをオンにすると、RFC 1583 あたりのサマリー ルート コストを計算します。このチェックボックスをオフにすると、RFC 2328 あたりのサマリー ルート コストが計算されます。ルーティング ループが発生する可能性を最小限にするため、OSPF ルーティング ドメインのすべての OSPF デバイスには、同じように RFC 互換性が設定されている必要があります。この設定は、デフォルトでオンになっています。
- Adjacency Changes：隣接関係の変更を定義する設定が含まれます。隣接関係が変更されると、システム ログ メッセージが送信されます。
  - Log Adjacency Changes：このチェックボックスをオンにすると、OSPF ネイバーが起動またはダウンするたびにセキュリティ アプライアンスがシステム ログ メッセージを送信します。この設定は、デフォルトでオンになっています。
  - Log Adjacency Changes Detail：このチェックボックスをオンにすると、ネイバーが起動またはダウンしたときだけでなく、状態の変更が発生するたびにセキュリティ アプライアンスがシステム ログ メッセージを送信します。デフォルトでは、この設定はオフになっています。
- Administrative Route Distances：ルート タイプに基づくルートの管理ディスタンスの設定を含みます。
  - Inter Area：1 つのエリアから別のエリアへのすべてのルートの管理ディスタンスを設定します。有効値の範囲は 1 ～ 255 です。デフォルト値は 100 です。
  - Intra Area：エリア内のすべてのルートの管理ディスタンスを設定します。有効値の範囲は 1 ～ 255 です。デフォルト値は 100 です。
  - External：再配布を通じて取得される他のルーティング ドメインからのすべてのルートの管理ディスタンスを設定します。有効値の範囲は 1 ～ 255 です。デフォルト値は 100 です。
- Timers：LSA ペーシングおよび SPF 計算タイマーの設定に使用する設定が含まれます。
  - SPF Delay Time：OSPF がトポロジーの変更を受信してから SPF の計算が開始されるまでの時間を指定します。有効値の範囲は 0 ～ 65535 です。デフォルト値は 5 です。

- SPF Hold Time：連続する SPF 計算の間の保持時間を指定します。有効値の範囲は 1 ～ 65534 です。デフォルト値は 10 です。
- LSA Group Pacing：LSA がグループに収集され、更新、チェックサム、または時間経過する間隔を指定します。有効値の範囲は 10 ～ 1800 です。デフォルト値は 240 です。

- Default Information Originate：ASBR がデフォルトの外部ルートを OSPF ルーティング ドメインに生成するときに使用する設定を含みます。
  - Enable Default Information Originate：このチェックボックスをオンにすると、OSPF ルーティング ドメインへのデフォルト ルートの生成をイネーブルにします。
  - Always advertise the default route：このチェックボックスをオンにすると、デフォルト ルートを常にアドバタイズします。デフォルトではオフになっています。
  - Metric Value：OSPF デフォルト メトリックを指定します。有効値の範囲は 0 ～ 16777214 です。デフォルト値は 1 です。
  - Metric Type：OSPF ルーティング ドメインにアドバタイズされたデフォルト ルートに関連付けられた外部リンク タイプを指定します。有効値は 1 または 2 です。それぞれタイプ 1 またはタイプ 2 外部ルートを示します。デフォルト値は 2 です。
  - Route Map：（オプション）適用するルート マップの名前です。ルート マップが確認された場合、ルーティング プロセスではデフォルト ルートが生成されます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Setup > Area/Networks タブ

Configuration > Routing > Dynamic Routing > OSPF > Setup > Area/Networks タブ

Area/Networks タブでは、セキュリティ アプライアンス上の各 OSPF プロセスのエリア、およびそこに含まれるネットワークが表示されます。

フィールド

- Area/Networks：各 OSPF プロセスに対して設定されたエリアおよびエリア ネットワークに関する情報を表示します。このテーブルの行をダブルクリックすると、選択したエリアを対象とした Add/Edit OSPF Area ダイアログボックスが開きます。
  - OSPF Process：エリアの適用先である OSPF プロセスを表示します。
  - Area ID：エリア ID を表示します。
  - Area Type：エリア タイプを表示します。エリア タイプは、通常、スタブ、NSSA のいずれかです。
  - Networks：エリア ネットワークを表示します。
  - Authentication：そのエリアに設定された認証タイプを表示します。 認証タイプは、None、Password、MD5 のいずれかです。
  - Options：そのエリア タイプに設定されたオプションを表示します。
  - Cost：そのエリアのデフォルト コストを表示します。
- Add：Add/Edit OSPF Area ダイアログボックスが開きます。新しいエリア設定を追加する場合は、このボタンを使用します。

- Edit : Add/Edit OSPF Area ダイアログボックスが開きます。選択したエリアのパラメータを変更する場合は、このボタンを使用します。
- Delete：選択したエリアを設定から削除します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Add/Edit OSPF Area

Configuration > Routing > Dynamic Routing > OSPF > Setup > Area/Networks > Add/Edit OSPF Area

Add/Edit OSPF Area ダイアログボックスでは、エリア パラメータ、そのエリアに含まれるネットワーク、およびエリアに関連付けられた OSPF プロセスを定義します。

フィールド

- OSPF Process：新しいエリアを追加するときに、そのエリアが追加される OSPF プロセスの OSPF プロセス ID を選択します。セキュリティ アプライアンスでイネーブルになっている OSPF プロセスが 1 つのみの場合は、デフォルトでそのプロセスが選択されています。既存のエリアを編集する場合、OSPF プロセス ID は変更できません。
- Area ID：新しいエリアを追加するときに、エリア ID を入力します。エリア ID は、10 進数または IP アドレスのいずれかで指定できます。有効な 10 進数値の範囲は、0 ～ 4294967295 です。既存のエリアを編集する場合、エリア ID は変更できません。
- Area Type：設定しているエリアのタイプに対する設定を含みます。
  - Normal：エリアを標準 OSPF エリアとする場合に、このオプションを選択します。最初にエリアを設定するときは、デフォルトでこのオプションが選択されています。
  - Stub：このオプションを選択すると、エリアがスタブ エリアになります。スタブ エリアは、範囲外のルータまたはエリアを持つことができません。スタブ エリアでは、AS External LSA（タイプ 5 LSA）がスタブ エリアにフラッディングされないようになっています。スタブ エリアを作成するとき、Summary チェックボックスをオフにすることでサマリー LSA（タイプ 3 および 4）がそのエリアにフラッディングされないようにするオプションがあります。
  - Summary：定義しているエリアがスタブ エリアのときにこのチェックボックスをオフにすると、LSA がスタブ エリアに送信されません。このチェックボックスは、スタブ エリアのデフォルトでオンになっています。
  - NSSA：エリアを not so stubby エリアにするには、このオプションを選択します。NSSA はタイプ 7 LSA を受け入れます。NSSA エリアを作成するときに、Summary チェックボックスをオフにすることでサマリー LSA がそのエリアにフラッディングされないようにするオプションがあります。また、Redistribute チェックボックスをオフにして Default Information Originate をイネーブルにすることで、ルートの再配布をディセーブルにもできます。
  - Redistribute：このチェックボックスをオフにすると、ルートは NSSA にインポートされません。このチェックボックスは、デフォルトでオンになっています。
  - Summary：定義しているエリアが NSSA のとき、このチェックボックスをオフにすると、LSA がスタブ エリアに送信されません。このチェックボックスは、NSSA のデフォルトでオンになっています。

- Default Information Originate：このチェックボックスをオンにすると、タイプ 7 デフォルトを NSSA に生成します。このチェックボックスは、デフォルトでオフになっています。
- Metric Value：デフォルト ルートの OSPF メトリック値を指定します。有効値の範囲は 0 ～ 16777214 です。デフォルト値は 1 です。
- Metric Type：デフォルト ルートの OSPF メトリック タイプです。選択肢は 1（タイプ 1）または 2（タイプ 2）です。デフォルト値は 2 です。

• Area Networks：OSPF エリアを定義するための設定を含みます。
- Enter IP Address and Mask：そのエリア内のネットワークを定義するのに使用する設定を含みます。

  IP Address：そのエリアに追加するネットワークまたはホストの IP アドレスを入力します。デフォルト エリアの作成には、0.0.0.0 およびネットマスク 0.0.0.0 を使用します。0.0.0.0 は 1 つのエリアでのみ使用できます。

  Netmask：エリアに追加する IP アドレスまたはホストのネットワーク マスクを選択します。ホストを追加する場合、255.255.255.255 マスクを選択します。
- Add：Enter IP Address and Mask 領域で定義したネットワークをエリアに追加します。追加されたネットワークは、Area Networks テーブルに表示されます。
- Delete：選択したネットワークを Area Networks テーブルから削除します。
- Area Networks：そのエリアに対して定義されたネットワークを表示します。

  IP Address：ネットワークの IP アドレスを表示します。

  Netmask：ネットワークのネットワーク マスクを表示します。

• Authentication：OSPF エリア認証の設定を含みます。
- None：このオプションを選択すると、OSPF エリア認証をディセーブルにします。これはデフォルトの設定です。
- Password：このオプションを選択すると、エリア認証にクリア テキスト パスワードを使用します。セキュリティが重要な場合、このオプションはお勧めできません。
- MD5：MD5 認証を使用するには、このオプションを選択します。

• Default Cost：エリアのデフォルト コストを指定します。有効値の範囲は 0 ～ 65535 です。デフォルト値は 1 です。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Setup > Route Summarization タブ

Configuration > Routing > Dynamic Routing > OSPF > Setup > Route Summarization タブ

OSPF では、ABR が 1 つのエリアから別のエリアにネットワークをアドバタイズします。あるエリアにおいて連続する複数のネットワーク番号が割り当てられている場合、指定された範囲に含まれるエリア内の個別のネットワークをすべてカバーするサマリー ルートをアドバタイズするように ABR を設定できます。OSPF エリアに再配布されている外部ルートのサマリー アドレスを定義するには、「Summary Address」を参照してください。

フィールド

- Route Summarization：セキュリティ アプライアンスで定義されたルート集約についての情報を表示します。このテーブルの行をダブルクリックすると、選択したルート集約を対象とした Add/Edit Route Summarization ダイアログボックスが開きます。
  - OSPF Process：ルート集約に関連付けられた OSPF プロセスの OSPF プロセス ID を表示します。
  - Area ID：ルート集約に関連付けられたエリアを表示します。
  - IP Address：サマリー アドレスを表示します。
  - Network Mask：サマリー マスクを表示します。
  - Advertise：アドレスとマスクのペアに一致するときにルート集約がアドバタイズされる場合は「yes」、アドレスとマスクのペアに一致するときにルート集約が抑止される場合は「no」を表示します。
- Add：Add/Edit Route Summarization ダイアログボックスが開きます。新しいルート集約を定義するには、このボタンを使用します。
- Edit：Add/Edit Route Summarization ダイアログボックスが開きます。選択したルート集約のパラメータを変更するには、このボタンを使用します。
- Delete：選択したルート集約を設定から削除します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Add/Edit Route Summarization

Configuration > Routing > Dynamic Routing > OSPF > Setup > Route Summarization > Add/Edit Route Summarization

新しいエントリを Route Summarization テーブルに追加するには、Add Route Summarization ダイアログボックスを使用します。既存のエントリを変更するには、Edit Route Summarization ダイアログボックスを使用します。

フィールド

- OSPF Process：ルート集約を適用する OSPF プロセスを選択します。既存のルート集約エントリを編集するときは、この値を変更できません。
- Area ID：ルート集約を適用するエリア ID を選択します。既存のルート集約エントリを編集するときは、この値を変更できません。
- IP Address：集約するルートのネットワーク アドレスを入力します。
- Network Mask：リストから共通ネットワーク マスクの 1 つを選択するか、フィールドにマスクを入力します。
- Advertise：このチェックボックスをオンにすると、アドレス範囲ステータスを「アドバタイズ」に設定します。これによって、タイプ 3 サマリー LSA が生成されます。指定したネットワークのタイプ 3 サマリー LSA を抑止するには、このチェックボックスをオフにします。このチェックボックスは、デフォルトでオンになっています。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Filtering

Configuration > Routing > Dynamic Routing > OSPF > Filtering

Filtering ペインでは、各 OSPF プロセスに設定された ABR タイプ 3 LSA フィルタを表示します。

ABR タイプ 3 LSA フィルタにより、指定したプレフィックスのみを 1 つのエリアから別のエリアに送信し、その他すべてのプレフィックスを制限できます。このタイプのエリア フィルタリングは、特定の OSPF エリアから特定の OSPF エリアに、または OSPF エリアから同一の OSPF エリアに同時に適用できます。

利点

OSPF ABR タイプ 3 LSA フィルタリングにより、OSPF エリア間のルート配布を詳細に制御できます。

制約事項

ABR から発信されたタイプ 3 LSA のみがフィルタリングされます。

フィールド

Filtering テーブルには、次の情報が表示されます。テーブル エントリをダブルクリックすると、選択したエントリを対象とした Add/Edit Filtering Entry ダイアログボックスが開きます。

- OSPF Process：フィルタ エントリに関連付けられた OSPF プロセスを表示します。
- Area ID：フィルタ エントリに関連付けられたエリアの ID を表示します。
- Filtered Network：フィルタリングされているネットワーク アドレスを表示します。
- Traffic Direction：OSPF エリアに着信する LSA にフィルタ エントリが適用される場合「Inbound」を、OSPF エリアから発信される LSA に適用される場合は「Outbound」を表示します。
- Sequence #：フィルタ エントリのシーケンス番号を表示します。複数のフィルタが LSA に適用されているとき、最も低いシーケンス番号のフィルタが使用されます。
- Action：フィルタに一致する LSA が許可される場合は「Permit」を、フィルタに一致する LSA が拒否される場合は「Deny」を表示します。
- Lower Range：照合される最小プレフィックス長を表示します。
- Upper Range：照合される最大プレフィックス長を表示します。

Filtering テーブルのエントリでは、次のアクションを実行できます。

- Add：新しいエントリを Filter テーブルに追加するための Add/Edit Filtering Entry ダイアログボックスが開きます。
- Edit：選択したフィルタを変更するための Add/Edit Filtering Entry ダイアログボックスが開きます。
- Delete：選択したフィルタを Filter テーブルから削除します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Add/Edit Filtering Entry

Configuration > Routing > Dynamic Routing > OSPF > Filtering > Add/Edit Filtering Entry

Add/Edit Filtering Entry ダイアログボックスでは、新しいフィルタを Filter テーブルに追加するか、既存のフィルタを変更できます。既存のフィルタを編集するとき、一部のフィルタ情報は変更できません。

フィールド

- OSPF Process：フィルタ エントリに関連付けられた OSPF プロセスを選択します。既存のフィルタ エントリを編集している場合、この設定は変更できません。
- Area ID：フィルタ エントリに関連付けられたエリアの ID を選択します。既存のフィルタ エントリを編集している場合、この設定は変更できません。
- Filtered Network：CIDR 表記（a.b.c.d/m）を使用して、フィルタリングしているネットワークのアドレスおよびマスクを入力します。
- Traffic Direction：フィルタリングされているトラフィックの方向を選択します。OSPF エリアに着信する LSA をフィルタリングするには「Inbound」を、OSPF エリアから発信される LSA をフィルタリングするには「Outbound」を選択します。既存のフィルタ エントリを編集している場合、この設定は変更できません。
- Sequence #：フィルタのシーケンス番号を入力します。有効値の範囲は 1 ～ 4294967294 です。複数のフィルタが LSA に適用されているとき、最も低いシーケンス番号のフィルタが使用されます。
- Action：LSA トラフィックを許可する場合は「Permit」を、LSA トラフィックをブロックする場合は「Deny」を選択します。
- Optional：フィルタのオプション設定を含みます。
  - Lower Range：照合される最小プレフィックス長を指定します。この設定の値は、Filtered Network フィールドに入力したネットワーク マスクの長さより大きく、Upper Range フィールドに入力した値がある場合は、その値と同じか小さい必要があります。
  - Upper Range：照合される最大プレフィックス長を入力します。この設定の値は、Lower Range フィールドに入力した値がある場合は、その値と同じかより大きい必要があります。Lower Range フィールドを空白のままにした場合は、Filtered Network フィールドに入力したネットワーク マスク長の長さより大きい必要があります。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Interface

Configuration > Routing > Dynamic Routing > OSPF > Interface

Interface ペインでは、インターフェイス固有の OSPF 認証ルーティング プロパティを設定できます。これらのプロパティの設定の詳細については、次の項目を参照してください。

- Interface > Authentication タブ
- Interface > Properties タブ

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Interface > Authentication タブ

Configuration > Routing > Dynamic Routing > OSPF > Interface > Authentication タブ

Authentication タブでは、セキュリティ アプライアンス インターフェイスの OSPF 認証情報が表示されます。

フィールド

- Authentication Properties：セキュリティ アプライアンス インターフェイスの認証情報を表示します。このテーブルの行をダブルクリックすると、選択したインターフェイスを対象とした Edit OSPF Interface Properties ダイアログボックスが開きます。
  - Interface：インターフェイス名を表示します。
  - Authentication Type：インターフェイスでイネーブルになっている OSPF 認証のタイプを表示します。認証タイプは、次のいずれかです。

    None：OSPF 認証はディセーブルです。

    Password：クリア テキスト パスワード認証がイネーブルです。

    MD5：MD5 認証がイネーブルです。

    Area：エリアに指定した認証タイプがインターフェイス上でイネーブルです。インターフェイスでは、エリア認証がデフォルト値です。ただし、エリア認証はデフォルトでディセーブルです。したがって、それ以前にエリア認証タイプを指定していない限り、エリア認証が表示されているインターフェイスでは、認証がディセーブルになっています。
- Edit：選択したインターフェイスを対象とした Edit OSPF Interface Properties ダイアログボックスが開きます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Edit OSPF Interface Authentication

Configuration > Routing > Dynamic Routing > OSPF > Interface > Authentication > Edit OSPF Interface Authentication

Edit OSPF Interface Authentication ダイアログボックスでは、選択したインターフェイスの OSPF 認証タイプおよびパラメータを設定できます。

フィールド

- Interface : 認証を設定するインターフェイスの名前を表示します。このフィールドは編集できません。
- Authentication：OSPF 認証オプションを含みます。
  - None：このオプションを選択すると、OSPF 認証をディセーブルにします。
  - Password：クリア テキスト パスワード認証を使用するには、このオプションを選択します。セキュリティが重要な場合、このオプションはお勧めできません。
  - MD5：MD5 認証を使用するには、このオプションを選択します（推奨）。
  - Area :（デフォルト）エリアに指定された認証タイプを使用するには、このオプションを選択します（エリア認証の設定の詳細については、「Add/Edit OSPF Area」を参照してください）。エリア認証はデフォルトでディセーブルになっています。したがって、それ以前にエリア認証タイプを指定していない限り、エリア認証を設定するインターフェイスでは、設定するまで認証がディセーブルになっています。
- Authentication Password：パスワード認証がイネーブルになっているとき、パスワードの入力のための設定が含まれます。
  - Enter Password：8 文字までのテキスト文字列を入力します。
  - Re-enter Password：パスワードを再入力します。
- MD5 IDs and Keys：MD5 認証がイネーブルになっているとき、MD5 キーおよびパラメータの入力のための設定が含まれます。OSPF 認証を使用しているインターフェイス上のすべてのデバイスが、同じ MD5 キーおよび ID を使用する必要があります。
  - Enter MD5 ID and Key：MD5 キー情報を入力するための設定が含まれます。

    Key ID：数字キー ID を入力します。有効値の範囲は 1 ～ 255 です。

    Key：16 バイトまでの英数字の文字列です。
  - Add：指定した MD5 キーを MD5 ID および Key テーブルに追加します。
  - Delete：選択した MD5 キーおよび ID を MD5 ID および Key テーブルから削除します。
  - MD5 ID and Key：設定済みの MD5 キーおよびキー ID を表示します。

    Key ID：選択したキーのキー ID を表示します。

    Key：選択したキー ID のキーを表示します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Interface > Properties タブ

Configuration > Routing > Dynamic Routing > OSPF > Interface > Properties タブ

Properties タブでは、テーブル形式で各インターフェイスに定義された OSPF プロパティが表示されます。

フィールド

- OSPF Interface Properties：インターフェイス固有の OSPF プロパティを表示します。このテーブルの行をダブルクリックすると、選択したインターフェイスを対象とした Edit OSPF Interface Properties ダイアログボックスが開きます。
  - Interface：OSPF 設定が適用されるインターフェイスの名前を表示します。
  - Broadcast：インターフェイスが非ブロードキャスト（ポイントツーポイント）に設定されている場合、「No」を表示します。インターフェイスがブロードキャストに設定されている場合は「Yes」を表示します。「Yes」は、イーサネット インターフェイスのデフォルト設定です。
  - Cost：インターフェイスを介したパケットの送信のコストを表示します。
  - Priority：インターフェイスに割り当てられた OSPF 優先順位を表示します。
  - MTU Ignore：MTU ミスマッチ検出がイネーブルになっている場合、「No」を表示します。MTU ミスマッチ検出がディセーブルになっている場合は「Yes」を表示します。
  - Database Filter：同期化およびフラッディングの間に発信 LSA がフィルタリングされる場合、「Yes」を表示します。フィルタリングがイネーブルでない場合は「No」を表示します。
- Edit：選択したインターフェイスを対象とした Edit OSPF Interface Properties ダイアログボックスを開きます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Edit OSPF Interface Properties

Configuration > Routing > Dynamic Routing > OSPF > Interface > Properties > Edit OSPF Interface Properties

フィールド

- Interface：OSPF プロパティを設定するインターフェイスの名前を表示します。このフィールドは編集できません。
- Broadcast：このチェックボックスをオンにすると、インターフェイスがブロードキャスト インターフェイスであることを指定します。このチェックボックスは、イーサネット インターフェイスのデフォルトでオンになっています。インターフェイスをポイントツーポイント、非ブロードキャスト インターフェイスとして指定するには、このチェックボックスをオフにします。インターフェイスをポイントツーポイント、非ブロードキャストとして指定すると、OSPF ルートが VPN トンネルで送信されます。

  インターフェイスをポイントツーポイント、非ブロードキャストとして設定すると、次の制限が適用されます。
  - インターフェイスに定義できるネイバーは 1 つのみです。
  - ネイバーは手動で設定する必要があります（「Static Neighbor」を参照）。

- 暗号化エンドポイントを指定しているスタティック ルートを定義する必要があります（「Static Routes」を参照）。
- トンネル経由の OSPF がインターフェイス上で実行されている場合、アップストリーム ルータを使用した通常の OSPF は、同一インターフェイス上で実行できません。
- OSPF の更新が VPN トンネルを通過するように OSPF ネイバーを指定する前に、暗号マップをインターフェイスにバインドする必要があります。OSPF ネイバーを指定した後で暗号マップをインターフェイスにバインドする場合は、**clear local-host all** コマンドを使用して OSPF 接続をクリアし、OSPF の隣接関係が VPN トンネル経由で確立されるようにします。

- Cost：インターフェイスを介したパケット送信のコストを指定します。デフォルト値は 10 です。
- Priority：OSPF ルータの優先順位を指定します。2 つのルータがネットワークに接続している場合、両方が代表ルータになろうとします。ルータ優先順位の高いデバイスが代表ルータになります。ルータ優先順位が同じ場合は、ルータ ID が高い方が代表ルータになります。

  この設定の有効値の範囲は、0 ～ 255 です。デフォルト値は 1 です。この設定に 0 を入力すると、適切でないルータが代表ルータになったり、代表ルータのバックアップが行われたりします。この設定は、ポイントツーポイント、非ブロードキャスト インターフェイスとして設定されているインターフェイスには適用されません。
- MTU Ignore：OSPF は、ネイバーが共通インターフェイスで同じ MTU を使用しているかどうかをチェックします。このチェックは、ネイバーが DBD パケットを交換したときに実行されます。DBD パケットで受信される MTU が受信インターフェイスで設定された IP MTU より高い場合、OSPF 隣接関係は確立されません。
- Database Filter：このチェックボックスをオンにすると、同期化およびフラッディングの間に発信 LSA インターフェイスをフィルタリングします。デフォルトでは、OSPF は、LSA が到達するインターフェイスを除き、同一エリア内のすべてのインターフェイスで新しい LSA をフラッディングします。完全メッシュ化トポロジでは、この設定が帯域幅を無駄にして、過剰なリンクおよび CPU の使用につながることがあります。このチェックボックスをオンにすることで、選択したインターフェイスでの OSPF LSA のフラッディングを防ぎます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Edit OSPF Interface Advanced Properties

Configuration > Routing > Dynamic Routing > OSPF > Interface > Properties > Edit OSPF Interface Properties > Edit OSPF Interface Advanced Properties

Edit OSPF Interface Advanced Properties ダイアログボックスでは、OSPF の hello 間隔、再送信間隔、送信遅延、dead 間隔の値を変更できます。通常は、ネットワーク上で OSPF の問題が発生した場合にのみ、これらの値をデフォルトから変更する必要があります。

フィールド

- Hello Interval：hello パケットがインターフェイスで送信される間隔を秒数で指定します。hello 間隔が小さいほど、トポロジの変更が速く検出されますが、インターフェイス上にはより多くのトラフィックが送信されることになります。この値は、すべてのルータに対して同じで、特定のインターフェイス上でサーバにアクセスする必要があります。有効値の範囲は 1 ～ 65535 秒です。デフォルト値は、10 秒です。

- Retransmit Interval：インターフェイスに属する隣接関係の LSA 再送信の間隔を秒数で指定します。ルータが LSA をネイバーに送信するとき、確認応答メッセージを受信するまで LSA を保持します。ルータが確認応答を受信しない場合、LSA を再送信します。この値の設定は慎重に行ってください。不要な再送信につながることがあります。値は、シリアル回線と仮想リンクに対して十分な大きさにしてください。有効値の範囲は 1 ～ 65535 秒です。デフォルト値は、5 秒です。
- Transmit Delay：インターフェイス上で LSA パケットを送信するのに必要な予想時間を秒数で指定します。更新パケットの LSA は、送信前にこのフィールドで指定された時間により、有効期限が長くなります。リンクでの送信前に遅延が追加されない場合、LSA がリンクでプロパゲートする時間は考慮されません。割り当てられた値では、インターフェイスの送信およびプロパゲート遅延を考慮に入れる必要があります。この設定は、超低速リンクで顕著に現れます。有効値の範囲は 1 ～ 65535 秒です。デフォルト値は、1 秒です。
- Dead Interval：hello パケットが受信されず、ネイバーがルータのダウンを宣言する間隔を秒数で指定します。有効値の範囲は、1 ～ 65535 です。この設定のデフォルト値は、Hello Interval フィールドで設定した間隔の 4 倍です。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Redistribution

Configuration > Routing > Dynamic Routing > OSPF > Redistribution

Redistribution ペインでは、あるルーティング ドメインから別のルーティング ドメインへルートが再配布されるときのルールを表示します。

フィールド

Redistribution テーブルには、次の情報が表示されます。テーブル エントリをダブルクリックすると、選択したエントリを対象とした Add/Edit OSPF Redistribution Entry ダイアログボックスが開きます。

- OSPF Process：ルート再配布エントリに関連付けられた OSPF プロセスを表示します。
- Protocol：ルートの再配布元であるソース プロトコルを表示します。有効なエントリは次のとおりです。
  - Static：ルートはスタティック ルートです。
  - Connected：インターフェイス上で IP をイネーブルにしたことで、ルートが自動的に確立されました。これらのルートは、AS の外部として再配布されます。
  - OSPF：ルートは、別のプロセスからの OSPF ルートです。
- Match：あるルーティング プロトコルから別のルーティング プロトコルにルートが再配布されるときに使用する条件を表示します。
- Subnets：サブネットされたルートが再配布される場合、「Yes」を表示します。サブネットされていないルートだけが再配布される場合は何も表示しません。
- Metric Value：ルートに使用されるメトリックを表示します。デフォルトのメトリックを使用する場合、再配布エントリに対してこのカラムは空白です。
- Metric Type：メトリックがタイプ 1 外部ルートの場合は「1」を、メトリックがタイプ 2 外部ルートの場合は「2」を表示します。

- Tag Value：各外部ルートに付加される 32 ビットの 10 進数値です。この値を OSPF 自身が使用することはありません。ASBR 間の情報の通信に使用されます。有効値の範囲は 0 ～ 4294967295 です。
- Route Map：再配布エントリに適用されるルート マップの名前を表示します。

Redistribution テーブル エントリでは次のアクションを実行できます。

- Add：新しい再配布エントリを追加するための Add/Edit OSPF Redistribution Entry ダイアログボックスが開きます。
- Edit：選択した再配布エントリを変更するための Add/Edit OSPF Redistribution Entry ダイアログボックスが開きます。
- Delete：選択した再配布エントリを Redistribution テーブルから削除します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Add/Edit OSPF Redistribution Entry

Configuration > Routing > Dynamic Routing > OSPF > Redistribution > Add/Edit OSPF Redistribution Entry

Add/Edit OSPF Redistribution Entry ダイアログボックスでは、Redistribution テーブルに新しい再配布ルールを追加したり、既存の再配布ルールを編集したりできます。既存の再配布ルールを編集するとき、一部の再配布ルール情報は変更できません。

フィールド

- OSPF Process：ルート再配布エントリに関連付けられた OSPF プロセスを選択します。既存の再配布ルールを編集している場合、この設定は変更できません。
- Protocol：ルートの再配布元であるソース プロトコルを選択します。次のいずれかのオプションを選択できます。
  - Static：ルートはスタティック ルートです。
  - Connected：インターフェイス上で IP をイネーブルにしたことで、ルートが自動的に確立されました。接続済みルートは、AS の外部として再配布されます。
  - OSPF：ルートは、別のプロセスからの OSPF ルートです。

    OSPF：再配布されるルートの OSPF プロセス ID を選択します。
- Match：あるルーティング プロトコルから別のルーティング プロトコルにルートが再配布されるときに使用する条件を表示します。ルートが再配布されるには、選択した条件に一致する必要があります。次の一致条件から 1 つまたは複数を選択できます。
  - Internal：特定の AS に対してルートは内部的です。
  - External 1：ルートは自律システムに対して外部的ですが、タイプ 1 外部ルートとして OSPF にインポートされます。
  - External 2：ルートは自律システムに対して外部的ですが、タイプ 2 外部ルートとして OSPF にインポートされます。
  - NSSA External 1：ルートは自律システムに対して外部的ですが、タイプ 1 NSSA ルートとして OSPF にインポートされます。

- NSSA External 2：ルートは自律システムに対して外部的ですが、タイプ 2 NSSA ルートとして OSPF にインポートされます。

- Metric Value：再配布するルートのメトリック値を指定します。有効値の範囲は 1 ～ 16777214 です。同じデバイス上で、ある OSPF プロセスから別の OSPF プロセスに再配布を行うとき、メトリック値が指定されていない場合は、あるプロセスから別のプロセスにメトリック値が引き継がれます。別のプロセスから 1 つの OSPF プロセスに再配布するとき、メトリック値が指定されていない場合のデフォルト値は 20 です。
- Metric Type：メトリックがタイプ 1 外部ルートである場合は「1」を、メトリックがタイプ 2 外部ルートである場合は「2」を選択します。
- Tag Value：タグ値は、各外部ルートに付加される 32 ビットの 10 進数値です。この値を OSPF 自身が使用することはありません。ASBR 間の情報の通信に使用されます。有効値の範囲は 0 ～ 4294967295 です。
- Use Subnets：このチェックボックスをオンにして、サブネットされたルートの再配布をイネーブルにします。サブネットされていないルートのみを再配布するには、このチェックボックスをオフにします。
- Route Map：再配布エントリに適用されるルート マップの名前を入力します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Static Neighbor

Configuration > Routing > Dynamic Routing > OSPF > Static Neighbor

Static Neighbor ペインでは、手動で定義されたネイバーが表示されます。検出されたネイバーは表示されません。

ポイントツーポイント、非ブロードキャスト インターフェイスのそれぞれに、スタティック ネイバーを定義する必要があります。また、Static Neighbor テーブルにある各スタティック ネイバーに対してスタティック ルートを定義する必要もあります。

フィールド

- Static Neighbor：各 OSPF プロセスに定義されたスタティック ネイバーの情報を表示します。このテーブルの行をダブルクリックすると、Add/Edit OSPF Neighbor Entry ダイアログボックスが開きます。
  - OSPF Process：スタティック ネイバーに関連付けられた OSPF プロセスを表示します。
  - Neighbor：スタティック ネイバーの IP アドレスを表示します。
  - Interface：スタティック ネイバーに関連付けられたインターフェイスを表示します。
- Add：Add/Edit OSPF Neighbor Entry ダイアログボックスが開きます。このボタンを使用して、新しいスタティック ネイバーを定義します。
- Edit：Add/Edit OSPF Neighbor Entry ダイアログボックスが開きます。このボタンを使用して、スタティック ネイバーの設定を変更します。
- Delete：選択したエントリを Static Neighbor テーブルから削除します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Add/Edit OSPF Neighbor Entry

Configuration > Routing > Dynamic Routing > OSPF > Static Neighbor > Add/Edit OSPF Neighbor Entry

Add/Edit OSPF Neighbor Entry ダイアログボックスでは、新しいスタティック ネイバーを定義するか、既存のスタティック ネイバーの情報を変更できます。

ポイントツーポイント、非ブロードキャスト インターフェイスのそれぞれに、スタティック ネイバーを定義する必要があります。

制約事項

- 異なる 2 つの OSPF プロセスに対して同じスタティック ネイバーを定義できません。
- 各スタティック ネイバーにスタティック ルートを定義する必要があります（「Static Routes」を参照）。

フィールド

- OSPF Process：スタティック ネイバーに関連付けられた OSPF プロセスを選択します。既存のスタティック ネイバーを編集している場合、この値は変更できません。
- Neighbor：スタティック ネイバーの IP アドレスを入力します。
- Interface：スタティック ネイバーに関連付けられたインターフェイスを選択します。既存のスタティック ネイバーを編集している場合、この値は変更できません。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Summary Address

Configuration > Routing > Dynamic Routing > OSPF > Summary Address

Summary Address ペインでは、各 OSPF ルーティング プロセスに設定されたサマリー アドレスに関する情報を表示します。

他のルーティング プロトコルから取得したルートは、集約が可能です。サマリーのアドバタイズに使用されるメトリックは、すべての特定ルートの中で最も小さいメトリックです。サマリー ルートは、ルーティング テーブルのサイズを減らすのに役立ちます。

OSPF でサマリー ルートを使用すると、このアドレスでカバーされる再配布ルートすべての集約として、1 つの外部ルートが OSPF ASBR からアドバタイズされます。OSPF に再配布される他のルーティング プロトコルからのルートのみ集約可能です。

フィールド

Summary Address テーブルには、次の情報が表示されます。テーブルのエントリをダブルクリックすると、選択したエントリを対象とした Add/Edit OSPF Summary Address Entry ダイアログボックスが開きます。

- OSPF Process：サマリー アドレスに関連付けられた OSPF プロセスを表示します。
- IP Address：サマリー アドレスの IP アドレスを表示します。
- Netmask：サマリー アドレスのネットワーク マスクを表示します。
- Advertise：サマリー ルートがアドバタイズされる場合は「Yes」を表示します。サマリー ルートがアドバタイズされない場合は「No」を表示します。
- Tag：各外部ルートに付加される 32 ビットの 10 進数値を表示します。この値を OSPF 自身が使用することはありません。ASBR 間の情報の通信に使用されます。

Summary Address テーブルのエントリでは、次のアクションを実行できます。

- Add：新しいサマリー アドレス エントリを追加するための Add/Edit OSPF Summary Address Entry ダイアログボックスが開きます。
- Edit：選択したエントリを対象とした Add/Edit OSPF Summary Address Entry ダイアログボックスが開きます。
- Delete：選択したサマリー アドレス エントリを Summary Address テーブルから削除します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Add/Edit OSPF Summary Address Entry

Configuration > Routing > Dynamic Routing > OSPF > Summary Address > Add/Edit OSPF Summary Address Entry

Add/Edit OSPF Summary Address Entry ダイアログボックスでは、Summary Address テーブルに新しいエントリを追加したり、Summary Address テーブルの既存のエントリを変更したりできます。既存のエントリを編集するとき、一部のサマリー アドレス情報は変更できません。

フィールド

- OSPF Process：サマリー アドレスに関連付けられた OSPF プロセスを選択します。既存のエントリを編集するときは、この情報を変更できません。
- IP Address：サマリー アドレスの IP アドレスを入力します。既存のエントリを編集するときは、この情報を変更できません。
- Netmask：サマリー　アドレスのネットワーク　マスクを入力するか、共通マスクのリストからネットワーク マスクを選択します。既存のエントリを編集するときは、この情報を変更できません。

- Advertise：このチェックボックスをオンにすると、サマリー ルートをアドバタイズします。サマリー アドレスになるルートを抑止するには、このチェックボックスをオフにします。デフォルトでは、チェックボックスがオンになっています。
- Tag：（オプション）タグ値は、各外部ルートに付加される 32 ビットの 10 進数値です。この値を OSPF 自身が使用することはありません。ASBR 間の情報の通信に使用されます。有効値の範囲は 0 ～ 4294967295 です。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Virtual Link

Configuration > Routing > Dynamic Routing > OSPF > Virtual Link

OSPF ネットワークにエリアを追加し、そのエリアをバックボーン エリアに直接接続することができない場合、仮想リンクを作成する必要があります。仮想リンクは、通過エリアと呼ばれる共通エリアを持つ 2 つの OSPF デバイスを接続します。いずれかの OSPF デバイスがバックボーン エリアに接続されている必要があります。

フィールド

Virtual Link テーブルには、次の情報が表示されます。テーブルのエントリをダブルクリックすると、選択したエントリを対象とした Add/Edit Virtual Link ダイアログボックスが開きます。

- OSPF Process：仮想リンクに関連付けられた OSPF プロセスを表示します。
- Area ID：通過エリアの ID を表示します。
- Peer Router ID：仮想リンク ネイバーのルータ ID を表示します。
- Authentication：仮想リンクが使用する認証のタイプを表示します。
  - None：認証は使用されません。
  - Password：クリア テキスト パスワード認証が使用されます。
  - MD5：MD5 認証が使用されます。

Virtual Link テーブルのエントリでは、次のアクションを実行できます。

- Add：新しいエントリを Virtual Link テーブルに追加するための Add/Edit Virtual Link ダイアログボックスが開きます。
- Edit：選択したエントリを対象とした Add/Edit Virtual Link ダイアログボックスが開きます。
- Delete：選択したエントリを Virtual Link テーブルから削除します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Add/Edit Virtual Link

Configuration > Routing > Dynamic Routing > OSPF > Virtual Link > Add/Edit Virtual Link

Add/Edit Virtual Link ダイアログボックスでは、新しい仮想リンクの定義や、既存の仮想リンクのプロパティの変更が実行できます。

フィールド

- OSPF Process : 仮想リンクに関連付けられた OSPF プロセスを選択します。既存の仮想リンクを編集している場合、この値は変更できません。
- Area ID：ネイバー OSPF デバイスと共有するエリアを選択します。NSSA エリアまたはスタブ エリアを選択することはできません。既存の仮想リンクを編集している場合、この値は変更できません。
- Peer Router ID：仮想リンク ネイバーのルータ ID を入力します。既存の仮想リンクを編集している場合、この値は変更できません。
- Advanced : Advanced OSPF Virtual Link Properties ダイアログボックスが開きます。このエリアにある仮想リンクに対して、OSPF プロパティを設定できます。プロパティには、認証およびパケット間隔設定が含まれます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Advanced OSPF Virtual Link Properties

Configuration > Routing > Dynamic Routing > OSPF > Virtual Link > Add/Edit Virtual Link > Advanced OSPF Virtual Link Properties

Advanced OSPF Virtual Link Properties ダイアログボックスでは、OSPF 認証およびパケット間隔を設定できます。

フィールド

- Authentication：OSPF 認証オプションを含みます。
  - None：OSPF 認証をディセーブルにするには、このオプションを選択します。
  - Password：クリア テキスト パスワード認証を使用するには、このオプションを選択します。セキュリティが重要な場合、このオプションはお勧めできません。
  - MD5：MD5 認証を使用するには、このオプションを選択します（推奨）。

- Authentication Password：パスワード認証がイネーブルになっているとき、パスワードの入力のための設定が含まれます。
  - Enter Password：8 文字までのテキスト文字列を入力します。
  - Re-enter Password：パスワードを再入力します。
- MD5 IDs and Keys：MD5 認証がイネーブルになっているとき、MD5 キーおよびパラメータの入力のための設定が含まれます。OSPF 認証を使用しているインターフェイス上のすべてのデバイスが、同じ MD5 キーおよび ID を使用する必要があります。
  - Enter MD5 ID and Key：MD5 キー情報を入力するための設定が含まれます。

    Key ID：数字キー ID を入力します。有効値の範囲は 1 ～ 255 です。

    Key：16 バイトまでの英数字の文字列です。
  - Add：指定した MD5 キーを MD5 ID および Key テーブルに追加します。
  - Delete：選択した MD5 キーおよび ID を MD5 ID および Key テーブルから削除します。
  - MD5 ID and Key：設定済みの MD5 キーおよびキー ID を表示します。

    Key ID：選択したキーのキー ID を表示します。

    Key：選択したキー ID のキーを表示します。
- Intervals：パケット間隔のタイミングを変更するための設定を含みます。
  - Hello Interval：hello パケットがインターフェイスで送信される間隔を秒数で指定します。hello 間隔が小さいほど、トポロジの変更が速く検出されますが、インターフェイス上にはより多くのトラフィックが送信されることになります。この値は、すべてのルータに対して同じで、特定のインターフェイス上でサーバにアクセスする必要があります。有効値の範囲は 1 ～ 65535 秒です。デフォルト値は、10 秒です。
  - Retransmit Interval：インターフェイスに属する隣接関係の LSA 再送信の間隔を秒数で指定します。ルータが LSA をネイバーに送信するとき、確認応答メッセージを受信するまで LSA を保持します。ルータが確認応答を受信しない場合、LSA を再送信します。この値の設定は慎重に行ってください。不要な再送信につながることがあります。値は、シリアル回線と仮想リンクに対して十分な大きさにしてください。有効値の範囲は 1 ～ 65535 秒です。デフォルト値は、5 秒です。
  - Transmit Delay：インターフェイス上で LSA パケットを送信するのに必要な予想時間を秒数で指定します。更新パケットの LSA は、送信前にこのフィールドで指定された時間により、有効期限が長くなります。リンクでの送信前に遅延が追加されない場合、LSA がリンクでプロパゲートする時間は考慮されません。割り当てられた値では、インターフェイスの送信およびプロパゲート遅延を考慮に入れる必要があります。この設定は、超低速リンクで顕著に現れます。有効値の範囲は 1 ～ 65535 秒です。デフォルト値は、1 秒です。
  - Dead Interval：hello パケットが受信されず、ネイバーがルータのダウンを宣言する間隔を秒数で指定します。有効値の範囲は、1 ～ 65535 です。このフィールドのデフォルト値は、Hello Interval フィールドで設定した間隔の 4 倍です。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

RIP

Configuration > Routing > Dynamic Routing > RIP

RIP とは、パスの選択のためのメトリックとしてホップ カウントを使用する、距離ベクトル ルーティング プロトコルです。インターフェイス上で RIP がイネーブルになっているとき、インターフェイスはネイバーのデバイスと RIP ブロードキャストを交換し、ダイナミックにルートを取得してアドバタイズします。

セキュリティ アプライアンスは、RIP バージョン 1 と RIP バージョン 2 の両方をサポートします。RIP バージョン 1 は、ルーティング更新でサブネット マスクを送信しません。RIP バージョン 2 は、ルーティング更新でサブネット マスクを送信し、変数長サブネット マスクをサポートします。さらに、RIP バージョン 2 は、ルーティング更新が交換されるときのネイバー認証をサポートします。認証により、セキュリティ アプライアンスは信頼できるルーティング情報を信頼の置けるソースから受け取ることができます。

2 つの OSPF ルーティング プロセスと 1 つの RIP ルーティング プロセスをセキュリティ アプライアンスで同時に保持できます。

制限事項

RIP には次の制限事項があります。

- セキュリティ アプライアンスは、インターフェイス間に RIP 更新を渡すことができません。
- RIP バージョン 1 は、変数長サブネット マスクをサポートしません。
- RIP の最大ホップ カウントは 15 です。ホップ カウントが 15 以上のルートは、到達不能と見なされます。
- RIP コンバージェンスは、他のルーティング プロトコルに比べ、低速です。
- セキュリティ アプライアンスでは、1 つの RIP プロセスだけをイネーブルにできます。

RIP バージョン 2 の注意点

次の情報は、RIP バージョン 2 にのみ該当します。

- ネイバー認証を使用する場合、認証キーおよびキー ID は、RIP バージョン 2 更新をインターフェイスに提供するすべてのネイバー デバイスで同じになっている必要があります。
- RIP バージョン 2 では、セキュリティ アプライアンスがマルチキャスト アドレス 224.0.0.9 を使用してデフォルト ルートの更新を送信および受信します。パッシブ モードでは、そのアドレスでルート更新を受信します。
- RIP バージョン 2 がインターフェイス上に設定されているとき、マルチキャスト アドレス 224.0.0.9 がそのインターフェイス上で登録されます。RIP バージョン 2 のコンフィギュレーションがインターフェイスから移動されると、マルチキャスト アドレスの登録は解除されます。

Global Setup

Configuration > Routing > Dynamic Routing > RIP >Global Setup

Global Setup ペインを使用して、セキュリティ アプライアンスで RIP をイネーブルにし、グローバル RIP プロトコル パラメータを設定します。セキュリティ アプライアンスでは、1 つの RIP プロセスだけをイネーブルにできます。

フィールド

- Enable RIP Routing : このチェックボックスをオンにすると、セキュリティ アプライアンスでの RIP ルーティングをイネーブルにします。RIP をイネーブルにすると、すべてのインターフェイス上でイネーブルになります。また、このチェックボックスをオンにすると、このペインの他

のフィールドもイネーブルになります。セキュリティ アプライアンスでの RIP ルーティングをディセーブルにするには、このチェックボックスをオフにします。

- Enable Auto-summarization：このチェックボックスをオフにすると、自動ルート集約をディセーブルにします。自動ルート集約を再度イネーブルにするには、このチェックボックスをオンにします。RIP バージョン 1 は常に自動集約を使用します。RIP バージョン 1 の自動集約をディセーブルにすることはできません。RIP バージョン 2 を使用している場合は、このチェックボックスをオフにすれば自動集約をオフにできます。切断されたサブネット間でルーティングを実行する必要がある場合、自動集約はディセーブルにします。自動集約がディセーブルになっているとき、サブネットがアドバタイズされます。
- Enable RIP version：セキュリティ アプライアンスが使用する RIP のバージョンを指定するには、この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がオフになっている場合、セキュリティ アプライアンスは RIP バージョン 1 更新を送信し、RIP バージョン 1 およびバージョン 2 更新を受信します。この設定は、Interface ペインでインターフェイスごとに上書きできます。
  - Version 1：セキュリティ アプライアンスが RIP バージョン 1 更新のみを送信および受信するように指定します。受信されたバージョン 2 更新はドロップされます。
  - Version 2：セキュリティ アプライアンスが RIP バージョン 2 更新のみを送信および受信するように指定します。受信されたバージョン 1 更新はドロップされます。
- Enable default information originate：このチェックボックスをオンにすると、RIP ルーティング プロセスにデフォルト ルートを生成します。デフォルト ルートの生成前に満たす必要のあるルート マップを設定できます。
  - Route-map：適用するルート マップの名前を入力します。ルート マップが確認された場合、ルーティング プロセスではデフォルト ルートが生成されます。
- IP Network to Add：RIP ルーティング プロセスのネットワークを定義します。指定するネットワーク数に、サブネット情報を含めることはできません。セキュリティ アプライアンスの設定に追加できるネットワーク数に制限はありません。RIP ルーティング更新は、指定したネットワーク上のインターフェイスを介してのみ送信および受信されます。また、インターフェイスのネットワークが指定されていない場合、そのインターフェイスは RIP 更新でアドバタイズされません。
  - Add：指定したネットワークをネットワークのリストに追加するには、このボタンをクリックします。
  - Delete：選択したネットワークをネットワークのリストから削除するには、このボタンをクリックします。
- Configure interfaces as passive globally：セキュリティ アプライアンス上のすべてのインターフェイスをパッシブ RIP モードに設定するには、このチェックボックスをオンにします。セキュリティ アプライアンスはすべてのインターフェイス上の RIP ルーティング ブロードキャストを受信し、その情報を使用してルーティング テーブルを取り込みますが、ルーティング更新をブロードキャストすることはありません。特定のインターフェイスをパッシブ RIP に設定するには、Passive Interfaces テーブルを使用します。
- Passive Interfaces テーブル：セキュリティ アプライアンスでの設定済みインターフェイスを一覧表示します。パッシブ モードで操作するインターフェイスの Passive カラムにあるチェックボックスをオンにします。他のインターフェイスは、引き続き RIP ブロードキャストを送信および受信します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Interface

Configuration > Routing > Dynamic Routing > RIP > Interface

Interface ペインでは、インターフェイスが送受信する RIP のバージョン、また使用する場合は RIP ブロードキャストの認証方式など、インターフェイス固有の RIP 設定を行えます。

フィールド

- Interface テーブル：（表示のみ）各行には、インターフェイスのインターフェイス固有 RIP 設定が表示されます。エントリの行をダブルクリックすると、そのインターフェイスを対象とした Edit RIP Interface Entry ダイアログボックスが開きます。
- Edit：Interface テーブルで選択したインターフェイスを対象とした Edit RIP Interface Entry ダイアログボックスが開きます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Edit RIP Interface Entry

Configuration > Routing > Dynamic Routing > RIP > Interface > Edit RIP Interface Entry

Edit RIP Interface Entry ダイアログボックスでは、インターフェイス固有 RIP 設定を設定できます。

フィールド

- Override Global Send Version：このチェックボックスをオンにして、インターフェイスが送信する RIP バージョンを指定します。次のオプションを選択できます。
  - バージョン 1
  - バージョン 2
  - バージョン 1 および 2

  このチェックボックスをオフにすると、グローバル設定が復元されます。
- Override Global Receive Version：このチェックボックスをオンにして、インターフェイスが受け入れる RIP バージョンを指定します。未サポートのバージョンの RIP から更新された RIP をインターフェイスが受信した場合、ドロップされます。次のオプションを選択できます。
  - バージョン 1
  - バージョン 2
  - バージョン 1 および 2

  このチェックボックスをオフにすると、グローバル設定が復元されます。
- Enable Authentication：このチェックボックスをオンにすると、RIP 認証をイネーブルにします。RIP ブロードキャスト認証をディセーブルにするには、このチェックボックスをオフにします。
  - Key：認証方式で使用するキーです。16 文字までで指定できます。
  - Key ID：キー ID です。有効値の範囲は 0 ～ 255 です。
  - Authentication Mode：次の認証モードを選択できます。

    MD5：RIP メッセージ認証に MD5 を使用します。

    Text：RIP メッセージ認証にクリア テキストを使用します（お勧めしません）。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Filter Rules

Configuration > Routing > Dynamic Routing > RIP > Filter Rules

フィルタ ルールにより、RIP ルーティング更新で受信したネットワーク、または RIP ルーティング更新で送信したネットワークをフィルタリングできます。各フィルタ ルールは、1 つ以上のネットワーク ルールで構成されます。

フィールド

- Filter Rules テーブル：設定済み RIP フィルタ ルールを表示します。
- Add：このボタンをクリックすると、Add/Edit Filter Rule ダイアログボックスが開きます。新しいフィルタ ルールは、リストの最下部に追加されます。
- Edit：このボタンをクリックすると、選択したフィルタ ルールを対象とした Add/Edit Filter Rule ダイアログボックスが開きます。
- Delete：このボタンをクリックすると、選択したフィルタ ルールが削除されます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Add/Edit Filter Rule

Configuration > Routing > Dynamic Routing > RIP > Filter Rules > Add/Edit Fitler Rule

フィルタ ルールを作成するには、Add/Edit Filter Rule ペインを使用します。すべてのインターフェイスに適用されるフィルタ ルール、または特定のインターフェイスに適用されるフィルタ ルールを作成できます。

フィールド

- Direction：フィルタが動作する方向を次の中から 1 つ選択します。
  - In：受信 RIP 更新でネットワークをフィルタリングします。
  - Out：送信 RIP 更新からのネットワークをフィルタリングします。
- Interface：フィルタ ルールに対して特定のインターフェイスを選択することも、All Interfaces オプションを選択してフィルタをすべてのインターフェイスに適用することもできます。
- Action：（表示のみ）受信または送信 RIP アドバタイズメントから指定されたネットワークがフィルタリングされない場合、Permit を表示します。受信または送信 RIP アドバタイズメントから指定されたネットワークがフィルタリングされる場合、Deny を表示します。

- IP Address：（表示のみ）フィルタリングするネットワークの IP アドレスを表示します。
- Netmask：（表示のみ）IP アドレスに適用されるネットワーク マスクを表示します。
- Insert：リストで選択したルールの上にネットワーク　ルールを追加するには、このボタンをクリックします。このボタンをクリックすると、Network Rule ダイアログボックスが開きます。
- Edit : 選択したルールを編集するには、このボタンをクリックします。このボタンをクリックすると、Network Rule ダイアログボックスが開きます。
- Add：リストで選択したルールの下にネットワーク　ルールを追加するには、このボタンをクリックします。このボタンをクリックすると、Network Rule ダイアログボックスが開きます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Network Rule

Configuration > Routing > Dynamic Routing > RIP > Filter Rules > Add/Edit Fitler Rule > Network Rule

Network Rule ペインを使用して、フィルタ ルールにある特定ネットワークのルールの Permit および Deny を設定できます。

フィールド

- Action：RIP 更新で指定ネットワークがアドバタイズされる、または RIP ルーティング プロセスに受け入れられるのを許可するには、Permit を選択します。指定ネットワークが RIP 更新でアドバタイズされる、または RIP ルーティング プロセスに受け入れられるのを防ぐには、Deny を選択します。
- IP Address：許可されるまたは拒否されるネットワークの IP アドレスを入力します。
- Netmask：ネットワーク　IP　アドレスに適用されるネットワーク　マスクを指定します。 このフィールドにネットワーク マスクを入力するか、リストから共通マスクの 1 つを選択します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Route Redistribution

Configuration > Routing > Dynamic Routing > RIP > Route Redistribution

Route Redistribution ペインでは、他のルーティング プロセスから RIP ルーティング プロセスに再配布されるルートを表示します。

フィールド

- Protocol：（表示のみ）RIP ルーティング プロセスに再配布されるルーティング プロトコルを表示します。
  - Static：スタティック ルートです。
  - Connected：ネットワークに直接接続されています。
  - OSPF：指定した OSPF ルーティング プロセスで検出されたネットワークです。
- Metric：再配布されたルートに適用される RIP メトリックです。
- Match：（表示のみ）RIP ルーティング プロセスに再配布される OSPF ルートのタイプを表示します。OSPF 再配布ルールに対して Match カラムが空白の場合、内部、外部 1、および外部 2 ルートは、RIP ルーティング プロセスに再配布されます。
- Route Map：（表示のみ）再配布に適用されるルート マップの名前がある場合は、その名前を表示します。ルート マップは、どのルートが指定したルーティング プロセスから RIP に再配布されるかといった非常に詳細な内容を指定するのに使用されます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Add/Edit Route Redistribution

Configuration > Routing > Dynamic Routing > RIP > Route Redistribution > Add/Edit Route Redistribution

新しい再配布ルールを追加するには、Add Route Redistribution ダイアログボックスを使用します。既存のルールを変更するには、Edit Route Redistribution ダイアログボックスを使用します。

フィールド

- Protocol：RIP ルーティング プロセスに再配布するルーティング プロトコルを選択します。
  - Static：スタティック ルートです。
  - Connected：ネットワークに直接接続されています。
  - OSPF and OSPF ID : OSPF ルーティング プロセスで検出されたルートです。OSPF を選択する場合、OSPF プロセス ID を入力する必要もあります。さらに、Match 領域から再配布する OSPF ルートの特定タイプを選択できます。
- Route Map：ルートが RIP ルーティング プロセスに再配布される前に満たす必要のあるルートマップの名前を指定します。
- Configure Metric Type : このチェックボックスをオンにして、再配布されるルートのメトリックを指定します。指定しない場合、ルートにはメトリック 0 が割り当てられます。
  - Transparent：このオプションを選択します。
  - Value：特定のメトリック値を割り当てるには、このオプションを選択します。入力できる値は、0 ～ 16 です。
- Match：OSPF ルートを RIP ルーティング プロセスに再配布する場合、ルート タイプの隣にあるチェックボックスをオンにすれば、再配布する OSPF ルートの特定タイプを選択できます。いずれのルート タイプもオンにしない場合、デフォルトでは、内部、外部 1、および外部 2 ルートが再配布されます。
  - Internal：AS に対して内部のルートが再配布されます。
  - External 1：AS に対して外部のタイプ 1 ルートが再配布されます。
  - External 2：AS に対して外部のタイプ 2 ルートが再配布されます。
  - NSSA External 1：NSSA に対して外部のタイプ 1 ルートが再配布されます。
  - NSSA External ：NSSA に対して外部のタイプ 2 ルートが再配布されます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

スタティック ルート

マルチコンテキスト モードは、ダイナミック ルーティングをサポートしていません。したがって、セキュリティ アプライアンスが直接接続されないネットワークに対してスタティック ルートを定義する必要があります。

透過ファイアウォール モードでは、セキュリティ アプライアンスから直接接続されていないネットワークに宛てたトラフィック用にデフォルト ルートまたはスタティック ルートを設定して、セキュリティ アプライアンスがトラフィックの送信先インターフェイスを認識できるようにする必要があります。セキュリティ アプライアンスから発信されるトラフィックには、syslog サーバ、Websense サーバまたは N2H2 サーバ、あるいは AAA サーバとの通信もあります。1 つのデフォルト ルートで到達できないサーバがある場合、スタティック ルートを設定する必要があります。

最も単純なオプションは、すべてのトラフィックをアップストリーム ルータに送信するようにデフォルト ルートを設定して、トラフィックのルーティングをルータに委せることです。しかし、デフォルトのゲートウェイでは宛先ネットワークに到達できない場合があるため、スタティック ルートをさらに詳しく設定する必要があります。たとえば、デフォルトのゲートウェイが外部インターフェイス上にある場合、デフォルト ルートは、セキュリティ アプライアンスに直接接続されていない内部ネットワークにはまったくトラフィックを転送できません。

また、スタティック ルートをダイナミック ルーティング プロトコルと共に使用し、ダイナミックに検出されたルートがダウンしたときに使用されるフローティング スタティック ルートを提供できます。ダイナミック ルーティング プロトコルの管理ディスタンスよりも長い管理ディスタンスを指定してスタティック ルートを作成すると、ルーティング プロトコルで検出される指定の宛先へのルートがスタティック ルートより優先されます。スタティック ルートは、ダイナミックに検出されたルートがルーティング テーブルから削除された場合に限り使用されます。

指定したゲートウェイが使用できなくなっても、スタティック ルートはルーティング テーブルに残ります（例外があるので P.14-31 の「スタティック ルート トラッキング」を参照してください）。指定されたゲートウェイが利用できなくなった場合は、スタティック ルートをルーティング テーブルから手動で削除する必要があります。ただし、スタティック ルートは、セキュリティ アプライアンスの関連インターフェイスがダウンした場合にルーティング テーブルから削除されます。これらのルートは、インターフェイスが復旧すると再適用されます。

インターフェイスあたり最大 3 つの等コスト ルートが同じ宛先に定義できます。複数のインターフェイス間を通る Equal Cost Multi-Path routing（ECMP; 等コスト マルチパス ルーティング）はサポートされていません。ECMP では、トラフィックはルート間で必ずしも均等に分割されません。トラフィックは、送信元と宛先の IP アドレスをハッシュするアルゴリズムに従って指定のゲートウェイ間に分散されます。

デフォルト ルートは、既知のルートもスタティック ルートも指定されていない IP パケットすべてをセキュリティ アプライアンスが送信する、ゲートウェイの IP アドレスを特定するルートです。デフォルト ルートは、宛先の IP アドレスとして 0.0.0.0/0 が指定された単なるスタティック ルートです。特定の宛先が特定されたルートはデフォルト ルートより優先されます。

デバイスあたり最大 3 つの等コスト デフォルト ルート エントリを定義することができます。複数の等コスト デフォルト ルート エントリを定義すると、デフォルト ルートに送信されるトラフィックは、指定されたゲートウェイの間に分散されます。複数のデフォルト ルートを定義する場合は、各エントリに同じインターフェイスを指定する必要があります。

4 つ以上の等コスト デフォルト ルートを定義しようとした場合、またはすでに定義されているデフォルト ルートとは別のインターフェイスでデフォルト ルートを定義しようとした場合は、エラー メッセージが表示されます。

トンネル トラフィックには、標準のデフォルト ルートの他に別のデフォルト ルートを 1 つ定義することができます。tunneled オプションを使用してデフォルト ルートを作成すると、セキュリティ アプライアンスに着信し、既知のルートでもスタティック ルートでもルーティングできない暗号化されたトラフィックはすべて、このルートに送信されます。これ以外の暗号化されていないトラフィックには、標準のデフォルト ルート エントリが使用されます。***tunneled*** オプションでは、複数のデフォルト ルートを定義することはできません。トンネル トラフィックでは ECMP がサポートされていないためです。

ASDM を使用したスタティック ルートおよびデフォルト ルートの表示と設定の詳細については、P.14-32 の「スタティック ルートのフィールド情報」を参照してください。

スタティック ルート トラッキング

セキュリティ アプライアンスがマルチコンテキスト モードや透過モードの場合など、必ずしもセキュリティ アプライアンスでダイナミック ルーティング プロトコルを使用できるとは限りません。この場合、スタティック ルートを使用する必要があります。

スタティック ルートの問題の 1 つは、ルートがアップ状態なのかダウン状態なのかを判定する固有のメカニズムがないことです。スタティック ルートは、ネクストホップ ゲートウェイがダウンしても、ルーティング テーブルに保持されています。スタティック ルートは、セキュリティ アプライアンスの関連インターフェイスがダウンした場合にのみルーティング テーブルから削除されます。

スタティック ルート トラッキング機能には、スタティック ルートの可用性を追跡し、プライマリ ルートがダウンした場合のバックアップ ルートをインストールするための方式が用意されています。これを利用すると、デフォルト ルートを ISP ゲートウェイに定義し、プライマリ ISP が使用できない場合に備えて、バックアップ用のデフォルト ルートをセカンダリ ISP に定義することができます。

セキュリティ アプライアンスでは、定義するモニタリング対象にスタティック ルートを関連付けることにより、これを行います。対象のモニタリングは、ICMP エコー要求を使用して行います。指定された時間内にエコー応答がない場合は、そのオブジェクトがダウンしているとみなされ、関連ルートがルーティング テーブルから削除されます。削除されたルートに代わって、すでに定義されているバックアップ ルートが使用されます。

モニタリング対象の選択時には、その対象が ICPM エコー要求に応答できることを確認してください。対象には、ICMP エコー要求に応答する任意のネットワーク オブジェクトを選択できます。選択肢として考えられるのは次のとおりです。

- ISP ゲートウェイ アドレス（デュアル ISP サポート用）。
- ネクストホップ ゲートウェイ アドレス（ゲートウェイの可用性を考慮する場合）。
- AAA サーバなど、セキュリティ アプライアンスが通信を行う必要のあるサーバ。
- 宛先ネットワーク上の永続的なネットワーク オブジェクト（夜間にシャットダウンするデスクトップ PC やノートブック PC は適しません）。

スタティック ルート トラッキングの設定の詳細については、P.14-32 の「スタティック ルート トラッキングの設定」を参照してください。スタティック ルート トラッキング プロセスの監視方法については、P.40-10 の「interface connection」を参照してください。

スタティック ルート トラッキングの設定

ここで説明する手順では、スタティック ルート トラッキングの設定の概要を示します。この機能の設定に使用するさまざまなフィールドの詳細については、P.14-32 の「スタティック ルートのフィールド情報」を参照してください。

スタティック ルートのトラッキングを設定するには、次の手順を実行します。

ステップ 1　対象を選択します。対象がエコー要求に応答することを確認してください。

ステップ 2　Static Routes ページを開きます。**Configuration > Routing > Static Routes** の順に移動します。

ステップ 3　**Add** をクリックし、選択した対象の使用可能状況に基づいて使用されるスタティック ルートを設定します。このルートのインターフェイス、IP アドレス、マスク、ゲートウェイ、およびメトリックを入力する必要があります。これらのフィールドの詳細については、P.14-34 の「Add/Edit Static Route」を参照してください。

ステップ 4　このルートには、Options 領域で **Tracked** を選択します。

ステップ 5　トラッキング プロパティを設定します。一意のトラック ID、一意の SLA ID、および対象の IP アドレスを入力する必要があります。これらのフィールドの詳細については、P.14-34 の「Add/Edit Static Route」を参照してください。

ステップ 6　（オプション）監視プロパティを設定するには、Add Static Route ダイアログボックスの **Monitoring Options** をクリックします。監視プロパティの詳細については、P.14-35 の「Route Monitoring Options」を参照してください。

ステップ 7　**OK** をクリックして変更内容を保存します。

追跡するルートを保存するとすぐに、モニタリング プロセスが開始されます。

ステップ 8　セカンダリ　ルートを作成します。 セカンダリ　ルートは、追跡されたルートと同じ宛先へのスタティック ルートですが、異なるインターフェイスまたはゲートウェイを経由します。このルートは、追跡されたルートより長い管理ディスタンス（メトリック）に割り当てる必要があります。

スタティック ルートのフィールド情報

特定のペインの詳細については、次の項目を参照してください。

- Static Routes（P.14-33）
- Add/Edit Static Route（P.14-34）
- Route Monitoring Options（P.14-35）

Static Routes

Configuration > Routing > Dynamic Routing > Static Routes

Static Route ペインでは、任意のインターフェイス上のルータに接続されたネットワークにアクセスするスタティック ルートを作成できます。デフォルト ルートを入力するには、IP アドレスおよびマスクを 0.0.0.0、または短縮形式の 0 を設定します。

1 つのセキュリティ アプライアンス インターフェイスの IP アドレスがゲートウェイの IP アドレスとして使用される場合、セキュリティ アプライアンスは、ゲートウェイ IP アドレスに ARP を実行するのではなく、パケットの指定 IP アドレスに ARP を実行します。

ゲートウェイ ルータのホップ数が明確でない場合は、Metric をデフォルトの 1 のままにしておきます。

フィールド

Static Route ペインには、Static Route テーブルが表示されます。

- Interface：（表示のみ）インターフェイスでイネーブルになっている内部または外部ネットワーク インターフェイス名を一覧表示します。
- IP Address：（表示のみ）内部または外部ネットワーク IP アドレスを一覧表示します。デフォルト ルートを指定するには、**0.0.0.0** を使用します。IP アドレス **0.0.0.0** は、**0** に短縮できます。
- Netmask：（表示のみ）IP アドレスに適用されるネットワーク マスク アドレスを一覧表示します。デフォルト ルートを指定するには、**0.0.0.0** を使用します。ネットマスク **0.0.0.0** は、**0** に短縮できます。
- Gateway IP：（表示のみ）このルートの次のホップ アドレスであるゲートウェイ ルータの IP アドレスを一覧表示します。
- Metric：（表示のみ）ルートの管理ディスタンスを一覧表示します。メトリックが指定されない場合、デフォルトは 1 です。
- Options：（表示のみ）スタティック ルートに指定されたオプションを表示します。
  - None：スタティック ルートにはオプションが指定されていません。
  - Tunneled：ルートを VPN トラフィックのデフォルト トンネル ゲートウェイとして指定します。デフォルト ルートにのみ使用されます。1 つのデバイスに設定できるのは 1 つのトンネル ルートのみです。透過モードではトンネル オプションがサポートされていません。
  - Tracked：ルートを追跡することを指定します。追跡するオブジェクトの ID および追跡対象のアドレスも表示されます。追跡オプションは、シングルモードおよびルーテッド モードでのみサポートされます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit Static Route

Configuration >Routing > Static Routes > Add/Edit Static Route

Startup Wizard > Static Routes >Add/Edit Static Route

スタティック ルート プロパティを設定するには、Add/Edit Static Route ダイアログボックスを使用します。このダイアログボックスは、Startup ウィザードの Static Routes 画面および Configuration > Routing > Static Route ペインで使用できます。

フィールド

- Interface Name：ルートの出力インターフェイスを選択します。
- IP Address：内部または外部ネットワーク IP アドレスを指定します。デフォルト ルートを指定するには、**0.0.0.0** を使用します。IP アドレス **0.0.0.0** は、**0** に短縮できます。
- Mask：IP アドレスに適用されるネットワーク マスク アドレスを指定します。デフォルト ルートを指定するには、**0.0.0.0** を使用します。ネットマスク **0.0.0.0** は、**0** に短縮できます。
- Gateway IP：このルータの次のホップ アドレスであるゲートウェイ ルータの IP アドレスを指定します。
- Metric：ルートの管理ディスタンスを指定できます。メトリックが指定されない場合、デフォルトは **1** です。

スタティック ルートには次のオプションを使用できます。1 つのスタティック ルートには、これらのオプションから 1 つのみ選択できます。デフォルトでは、オプションなし（None）が選択されています。

- None：スタティック ルートにはオプションが指定されていません。
- Tunneled：デフォルト ルートにのみ使用されます。セキュリティ アプライアンスごとに、デフォルト トンネル ゲートウェイが 1 つだけ許可されます。透過モードではトンネル オプションがサポートされていません。
- Tracked：ルートを追跡するように指定するには、このオプションを選択します。このオプションを指定すると、ルート トラッキング プロセスが開始されます。
  - Track ID：ルート トラッキング プロセスの一意の ID です。
  - Track IP Address/DNS Name：追跡される対象の IP アドレスまたはホスト名を入力します。通常は、ルートの次のホップ ゲートウェイの IP アドレスですが、そのインターフェイスで使用可能な任意のネットワーク オブジェクトの IP アドレスを指定することもできます。
  - SLA ID：SLA モニタリング プロセスの一意の ID です。
  - Monitor Options：このボタンをクリックして、Route Monitoring Options ダイアログボックスを開きます。Route Monitoring Options ダイアログボックスでは、追跡されるオブジェクトのモニタリング プロセスのパラメータを設定できます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Route Monitoring Options

Configuration > Routing > Static Routes > Add/Edit Static Route > Route Monitoring Options

追跡するオブジェクトの監視プロパティを変更するには、Route Monitoring Options ダイアログボックスを使用します。

フィールド

- Frequency：追跡対象の存在をセキュリティ アプライアンスがテストする頻度を秒数で入力します。デフォルト値は、60 秒です。有効値の範囲は 1 ～ 604800 秒です。
- Threshold：しきい値を超えたイベントを示す時間をミリ秒数で入力します。この値に、タイムアウト値より大きい値を指定することはできません。
- Timeout：ルート監視操作が要求パケットからの応答を待つ時間をミリ秒数で入力します。デフォルト値は 5000 ミリ秒です。有効値の範囲は、0 ～ 604800000 ミリ秒です。
- Data Size：エコー要求パケットで使用するデータ ペイロードのサイズを入力します。デフォルト値は 28 です。有効値の範囲は 0 ～ 16384 です。

（注） この設定では、ペイロードのサイズのみが指定されます。パケット全体のサイズは指定されません。

- ToS：エコー要求の IP ヘッダーにあるサービス バイトのタイプの値を入力します。デフォルト値は 0 です。有効値の範囲は 0 ～ 255 です。
- Number of Packets：各テストに送信されるエコー要求の数です。デフォルト値は 1 です。有効値の範囲は 1 ～ 100 です。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

ASR Group

Configuration > Routing > ASR Group

非同期ルーティング グループ ID 番号をインターフェイスに割り当てるには、ASR Group 画面を使用します。

一部の場合では、セッションのリターン トラフィックが送信元とは異なるインターフェイスを経由してルート指定されることがあります。フェールオーバー コンフィギュレーションでは、1 つの装置で送信元となった接続のリターン トラフィックが、ピア装置を経由して戻る場合があります。これが最もよく発生するのは、1 つのセキュリティ アプライアンス上の 2 つのインターフェイス、またはフェールオーバー ペアの 2 つのセキュリティ アプライアンスが、異なるサービス プロバイダーに接続されており、発信接続で NAT アドレスが使用されていない場合です。デフォルトでは、セキュリティ アプライアンスはリターン トラフィックをドロップします。これは、トラフィックの接続情報がないためです。

リターン トラフィックのドロップは、ドロップが発生する可能性のあるインターフェイスで ASR Group を使用することで防止できます。ASR Group で設定されたインターフェイスがセッション情報を持たないパケットを受信すると、同じグループにある他のインターフェイスのセッション情報をチェックします。

（注） セッション情報の Stateful Failover がスタンバイ フェールオーバー グループからアクティブ フェールオーバー グループに渡されるようにイネーブルにする必要があります。

一致する情報が見つからないと、パケットはドロップされます。一致する情報が見つかると、次の動作のうちいずれかが開始します。

- 着信トラフィックがフェールオーバー コンフィギュレーションのピア装置で発信すると、レイヤ 2 ヘッダーの一部またはすべてが書き直され、パケットは他の装置にリダイレクトされます。このリダイレクトは、セッションがアクティブである限り続行されます。
- 着信トラフィックが同じ装置の別のインターフェイスで発信すると、レイヤ 2 ヘッダーの一部またはすべてが書き直され、パケットはストリームにリダイレクトされます。

フィールド

ASR Group テーブルには、セキュリティ アプライアンスの各インターフェイスの次の情報が表示されます。

- **Interface**：セキュリティ アプライアンスのインターフェイスの名前を表示します。
- **ASR Group ID**：インターフェイスが属する ASR Group の数を表示します。インターフェイスに ASR Group 番号が割り当てられていない場合、このカラムには「-- None --」が表示されます。有効値の範囲は 1 ～ 32 です。

  ASR Group 番号をインターフェイスに割り当てるには、割り当てるインターフェイスの行の **ASR Group ID** セルをクリックします。有効な ASR Group 番号のリストが表示されます。希望の ASR Group 番号をリストから選択します。1 つの ASR Group には最高 8 つのインターフェイスを割り当てることができます。他のコンテキストに ASR Group に割り当てられたインターフェイスがある場合、これらのインターフェイスは、現在設定されているコンテキストに対しても合計 8 つにカウントされます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	—	•	—

Proxy ARPs

Configuration > Routing > Proxy ARPs

状況によっては、グローバル アドレスのプロキシ ARP をディセーブルにする場合があります。

ホストが同じイーサネット ネットワーク上の別のデバイスに IP トラフィックを送信するとき、ホストはそのデバイスの MAC アドレスを知っている必要があります。ARP は、MAC アドレスに対して IP アドレスを解決するレイヤ 2 プロトコルです。ホストは、「この IP アドレスはだれのものか」と尋ねる ARP 要求を送信します。その IP アドレスを持つデバイスは「その IP アドレスは自分のもので、これが MAC アドレスである」と応答します。

プロキシ ARP は、デバイスが自身の IP アドレスを持たなくても、ARP 要求に自身の MAC アドレスで応答する場合に使用されます。NAT を設定し、セキュリティ アプライアンス インターフェイスと同じネットワーク上にあるグローバル アドレスを指定するとき、セキュリティ アプライアンスはプロキシ ARP を使用します。セキュリティ アプライアンスがプロキシ ARP を使用する場合、トラフィックがホストに到達するためには、セキュリティ アプライアンスの MAC アドレスが宛先グローバル アドレスに割り当てられている必要があります。

フィールド

- Interface：インターフェイス名を一覧表示します。
- Proxy ARP Enabled：プロキシ ARP が NAT グローバル アドレスに対してイネーブルになっているか、ディセーブルになっているかを Yes または No で表示します。
- Enable：選択したインターフェイスのプロキシ ARP をイネーブルにします。デフォルトでは、すべてのインターフェイスでプロキシ ARP がイネーブルになっています。
- Disable：選択したインターフェイスのプロキシ ARP をディセーブルにします。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—