# Open Shortest Path First（OSPF）

この章では、Open Shortest Path First（OSPF）ルーティング プロトコルを使用してデータをルーティングし、認証を実行し、ルーティング情報を再配布するように Firewall Threat Defense を設定する方法について説明します。



# Open Shortest Path First（OSPF）

この章では、Open Shortest Path First（OSPF）ルーティング プロトコルを使用してデータをルーティングし、認証を実行し、ルーティング情報を再配布するように Firewall Threat Defense を設定する方法について説明します。

## About OSPF

OSPF is an interior gateway routing protocol that uses link states rather than distance vectors for path selection. OSPF propagates link-state advertisements rather than routing table updates. Because only LSAs are exchanged instead of the entire routing tables, OSPF networks converge more quickly than RIP networks.

OSPF uses a link-state algorithm to build and calculate the shortest path to all known destinations. Each router in an OSPF area contains an identical link-state database, which is a list of each of the router usable interfaces and reachable neighbors.

The advantages of OSPF over RIP include the following:

- OSPF link-state database updates are sent less frequently than RIP updates, and the link-state database is updated instantly, rather than gradually, as stale information is timed out.
- Routing decisions are based on cost, which is an indication of the overhead required to send packets across a certain interface. The Firewall Threat Defense device calculates the cost of an interface based

on link bandwidth rather than the number of hops to the destination. The cost can be configured to specify preferred paths.

The disadvantage of shortest path first algorithms is that they require a lot of CPU cycles and memory.

The Firewall Threat Defense device can run two processes of OSPF protocol simultaneously on different sets of interfaces. You might want to run two processes if you have interfaces that use the same IP addresses (NAT allows these interfaces to coexist, but OSPF does not allow overlapping addresses). Or you might want to run one process on the inside and another on the outside, and redistribute a subset of routes between the two processes. Similarly, you might need to segregate private addresses from public addresses.

You can redistribute routes into an OSPF routing process from another OSPF routing process, a RIP routing process, or from static and connected routes configured on OSPF-enabled interfaces.

The Firewall Threat Defense device supports the following OSPF features:

- Intra-area, inter-area, and external (Type I and Type II) routes.
- Virtual links.
- LSA flooding.
- Authentication to OSPF packets (both password and MD5 authentication).
- Configuring the Firewall Threat Defense device as a designated router or a designated backup router. The Firewall Threat Defense device also can be set up as an ABR.
- Stub areas and not-so-stubby areas.
- Area boundary router Type 3 LSA filtering.

OSPF supports MD5 and clear text neighbor authentication. Authentication should be used with all routing protocols when possible because route redistribution between OSPF and other protocols (such as RIP) can potentially be used by attackers to subvert routing information.

If NAT is used, if OSPF is operating on public and private areas, and if address filtering is required, then you need to run two OSPF processes—one process for the public areas and one for the private areas.

A router that has interfaces in multiple areas is called an Area Border Router (ABR). A router that acts as a gateway to redistribute traffic between routers using OSPF and routers using other routing protocols is called an Autonomous System Boundary Router (ASBR).

An ABR uses LSAs to send information about available routes to other OSPF routers. Using ABR Type 3 LSA filtering, you can have separate private and public areas with the ASA acting as an ABR. Type 3 LSAs (inter-area routes) can be filtered from one area to other, which allows you to use NAT and OSPF together without advertising private networks.

（注） Only Type 3 LSAs can be filtered. If you configure the Firewall Threat Defense device as an ASBR in a private network, it will send Type 5 LSAs describing private networks, which will get flooded to the entire AS, including public areas.

If NAT is employed but OSPF is only running in public areas, then routes to public networks can be redistributed inside the private network, either as default or Type 5 AS external LSAs. However, you need to configure static routes for the private networks protected by the Firewall Threat Defense device. Also, you should not mix public and private networks on the same Firewall Threat Defense device interface.

You can have two OSPF routing processes, one RIP routing process, and one EIGRP routing process running on the Firewall Threat Defense device at the same time.

# OSPF Support for Fast Hello Packets

The OSPF Support for Fast Hello Packets feature provides a way to configure the sending of hello packets in intervals less than one second. Such a configuration would result in faster convergence in an Open Shortest Path First (OSPF) network.

## Prerequisites for OSPF Support for Fast Hello Packets

OSPF must be configured in the network already or configured at the same time as the OSPF Support for Fast Hello Packets feature.

## OSPF Hello Interval and Dead Interval

OSPF hello packets are packets that an OSPF process sends to its OSPF neighbors to maintain connectivity with those neighbors. The hello packets are sent at a configurable interval (in seconds). The defaults are 10 seconds for an Ethernet link and 30 seconds for a non broadcast link. Hello packets include a list of all neighbors for which a hello packet has been received within the dead interval. The dead interval is also a configurable interval (in seconds), and defaults to four times the value of the hello interval. The value of all hello intervals must be the same within a network. Likewise, the value of all dead intervals must be the same within a network.

These two intervals work together to maintain connectivity by indicating that the link is operational. If a router does not receive a hello packet from a neighbor within the dead interval, it will declare that neighbor to be down.

## OSPF Fast Hello Packets

OSPF fast hello packets refer to hello packets being sent at intervals of less than 1 second. To understand fast hello packets, you should already understand the relationship between OSPF hello packets and the dead interval. See OSPF Hello Interval and Dead Interval （3 ページ） .

OSPF fast hello packets are achieved by using the ospf dead-interval command. The dead interval is set to 1 second, and the hello-multiplier value is set to the number of hello packets you want sent during that 1 second, thus providing subsecond or "fast" hello packets.

When fast hello packets are configured on the interface, the hello interval advertised in the hello packets that are sent out this interface is set to 0. The hello interval in the hello packets received over this interface is ignored.

The dead interval must be consistent on a segment, whether it is set to 1 second (for fast hello packets) or set to any other value. The hello multiplier need not be the same for the entire segment as long as at least one hello packet is sent within the dead interval.

## Benefits of OSPF Fast Hello Packets

The benefit of the OSPF Fast Hello Packets feature is that your OSPF network will experience faster convergence time than it would without fast hello packets. This feature allows you to detect lost neighbors within 1 second. It is especially useful in LAN segments, where neighbor loss might not be detected by the Open System Interconnection (OSI) physical layer and data-link layer.

# Implementation Differences Between OSPFv2 and OSPFv3

OSPFv3 is not backward compatible with OSPFv2. To use OSPF to route both IPv4 and IPv6 traffic, you must run both OSPFv2 and OSPFv3 at the same time. They coexist with each other, but do not interact with each other.

The additional features that OSPFv3 provides include the following:

- Protocol processing per link.
- Removal of addressing semantics.
- Addition of flooding scope.
- Support for multiple instances per link.
- Use of the IPv6 link-local address for neighbor discovery and other features.
- LSAs expressed as prefix and prefix length.
- Addition of two LSA types.
- Handling of unknown LSA types.
- Authentication support using the IPsec ESP standard for OSPFv3 routing protocol traffic, as specified by RFC-4552.

# OSPF の要件と前提条件

### Model support

Firewall Threat Defense

Firewall Threat Defense Virtual

### Supported domains

Any

### User roles

Admin

Network Admin

# Guidelines for OSPF

### Firewall Mode Guidelines

OSPF supports routed firewall mode only. OSPF does not support transparent firewall mode.

### High availability Guidelines

OSPFv2 and OSPFv3 support Stateful High availability.

### IPv6 Guidelines

- OSPFv2 does not support IPv6.
- OSPFv3 supports IPv6.
- OSPFv3 uses IPv6 for authentication.
- The Firewall Threat Defense device installs OSPFv3 routes into the IPv6 RIB, provided it is the best route.

### OSPFv3 Hello Packets and GRE

Typically, OSPF traffic does not pass through GRE tunnel. When OSPFv3 on IPv6 is encapsulated inside GRE, the IPv6 header validation for security check such as Multicast Destination fails. The packet is dropped due to the implicit security check validation, as this packet has destination IPv6 multicast.

You may define a pre-filter rule to bypass GRE traffic. However, with pre-filter rule, inner packets would not be interrogated by the inspection engine.

### Clustering Guidelines

- OSPFv3 encryption is not supported. An error message appears if you try to configure OSPFv3 encryption in a clustering environment.
- In Spanned interface mode, dynamic routing is not supported on management-only interfaces.
- In Individual interface mode, make sure that you establish the control and data units as either OSPFv2 or OSPFv3 neighbors.
- In Individual interface mode, OSPFv2 adjacencies can only be established between two contexts on a shared interface on the control unit. Configuring static neighbors is supported only on point-to point-links; therefore, only one neighbor statement is allowed on an interface.
- When a control role change occurs in the cluster, the following behavior occurs:
  - In spanned interface mode, the router process is active only on the control unit and is in a suspended state on the data units. Each cluster unit has the same router ID because the configuration has been synchronized from the control unit. As a result, a neighboring router does not notice any change in the router ID of the cluster during a role change.
  - In individual interface mode, the router process is active on all the individual cluster units. Each cluster unit chooses its own distinct router ID from the configured cluster pool. A control role change in the cluster does not change the routing topology in any way.

### Multiprotocol Label Switching (MPLS) and OSPF Guidelines

When a MPLS-configured router sends Link State (LS) update packets containing opaque Type-10 link-state advertisements (LSAs) that include an MPLS header, authentication fails and the appliance silently drops the update packets, rather than acknowledging them. Eventually the peer router will terminate the neighbor relationship because it has not received any acknowledgments.

Make sure that non-stop forwarding (NSF) is disabled on the appliance to ensure that the neighbor relationship remains stable:

- Navigate to the **Non Stop Forwarding** page in Firewall Management Center(**Devices** > **Device Management (select the desired device)** > **Routing** > **OSPF** > **Advanced** > **Non Stop Forwarding** ).

  Ensure the **Non Stop Forwarding Capability** boxes are not checked.

（注） The Firepower 4100/9300 models may have high latency when using MPLS because they lack load balancing across multiple receiving queues.

### Bidirectional and Forwarding Detection (BFD) and OSPF Guidelines

- You can enable BFD on OSPFv2 and OSPFv3 interfaces (Physical Interfaces, Sub-Interfaces, and Port-Channels).
- BFD is not supported on VTI Tunnels, DVTI Tunnels, Loopback, Switchport, VNI, VTEP, and IRB interfaces.

### Route Redistribution Guidelines

- Redistribution of route maps with IPv4 prefix list on OSPFv2 is supported. However, redistribution of route maps with IPv6 prefix list on OSPFv3 is not supported. Use an access list in the route map on OSPF for redistribution.
- When OSPF is configured on a device that is a part of EIGRP network or vice versa, ensure that OSPF-router is configured to tag the route (EIGRP does not support route tag yet).

  When redistributing OSPF into EIGRP and EIGRP into OSPF, a routing loop occurs when there is an outage on one of the links, interfaces, or even when the route originator is down. To prevent the redistribution of routes from one domain back into the same domain, a router can tag a route that belongs to a domain while it is redistributing, and those routes can be filtered on the remote router based on the same tag. Because the routes will not be installed into the routing table, they will not be redistributed back into the same domain.

### Additional Guidelines

- OSPFv2 and OSPFv3 support multiple instances on an interface.
- OSPFv3 supports encryption through ESP headers in a non-clustered environment.
- OSPFv3 supports Non-Payload Encryption.
- OSPFv2 supports Cisco NSF Graceful Restart and IETF NSF Graceful Restart mechanisms as defined in RFCs 4811, 4812 & 3623 respectively.
- OSPFv3 supports Graceful Restart mechanism as defined in RFC 5187.
- There is a limit to the number of intra area (type 1) routes that can be distributed. For these routes, a single type-1 LSA contains all prefixes. Because the system has a limit of 35 KB for packet size,

3000 routes result in a packet that exceeds the limit. Consider 2900 type 1 routes to be the maximum number supported.

- For a device using virtual routing, you can configure OSPFv2 and OSPFv3 for a global virtual router. However, you can configure only OSPFv2 for a user-defined virtual router.
- To avoid adjacency flaps due to route updates being dropped if the route update is larger than the minimum MTU on the link, ensure that you configure the same MTU on the interfaces on both sides of the link.
- OSPFv3 drops the LS update if the packet size exceeds 8190. As a result, the neighbourship is terminated. Hence, configure the switch with the "ospfv3 mtu-ignore" command to avoid neighbourship termination.

# OSPFv2 の設定

ここでは、OSPFv2 ルーティング プロセスの設定に関連するタスクについて説明します。仮想ルーティングを使用するデバイスでは、グローバルおよびユーザー定義の仮想ルータに対して OSPFv2 を設定できます。

## OSPF エリア、範囲、仮想リンクの設定

認証の設定、スタブエリアの定義、デフォルトの集約ルートへの特定コストの割り当てが含まれる複数の OSPF エリア パラメータを設定できます。最大 2 つの OSPF プロセス インスタンスを有効にできます。各 OSPF プロセスには、独自のエリアとネットワークが関連付けられます。認証では、エリアへの不正アクセスに対してパスワードベースで保護します。

スタブ エリアは、外部ルートの情報が送信されないエリアです。その代わりに、ABR で生成されるデフォルトの外部ルートがあり、このルートは自律システムの外部の宛先としてスタブ エリアに送信されます。OSPF スタブ エリアのサポートを活用するには、デフォルトのルーティングをスタブ エリアで使用する必要があります。

### 手順

**ステップ 1** [**Devices** > **Device Management**] を選択し、Firewall Threat Defense デバイスを編集します。

**ステップ 2** [ルーティング（Routing）] をクリックします。

**ステップ 3** （仮想ルータ対応デバイスの場合）[仮想ルータ（Virtual Routers）] ドロップダウンリストから、OSPF を設定する仮想ルータを選択します。

**ステップ 4** [OSPF] をクリックします。

**ステップ 5** [プロセス1（Process 1）] のチェックボックスをオンにします。それぞれのコンテキスト/仮想ルータで最大 2 つの OSPF プロセスインスタンスを有効にできます。エリアパラメータを設定するには、OSPF プロセスを選択する必要があります。

デバイスが仮想ルーティングを使用する場合、ID フィールドには選択された仮想ルータに対して生成された一意のプロセス ID が表示されます。

**ステップ 6** [OSPFロール（OSPF Role）] をドロップダウンリストから選択し、次のフィールドにそれぞれの説明を入力します。オプションは、[内部（Internal）]、[ABR]、[ASBR]、[ABRおよびASBR（ABR & ASBR）] です。OSPF の権限の説明については、About OSPF （1 ページ）を参照してください。

**ステップ 7** **[エリア（Area）]** > **[追加（Add）]** を選択します。

エリアを切り取り、コピー、貼り付け、挿入、削除するには、**Edit** (✎) をクリックするか、右クリックしてメニューを表示、選択します。

**ステップ 8** 以下のエリアのオプションを、それぞれの OSPF プロセスで設定します。

- [OSPF Process]：プロセス ID を選択します。仮想ルーティングを使用するデバイスの場合、選択した仮想ルータ用に生成された一意のプロセス ID がドロップダウンにリストされます。
- [エリア ID（Area ID）]：：ルートをサマライズするエリアの接続先。
- [エリア タイプ（Area Type）]：次のいずれかを選択します。
  - [Normal]：（デフォルト）標準 OSPF エリア。
  - [スタブ（Stub）]：スタブ エリアには、その向こう側にルータまたはエリアはありません。スタブ エリアは、自律システム（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します。スタブ エリアを作成すると、[サマリー スタブ（Summary Stub）] チェックボックスをオフにすることによって、集約 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るのを防ぐことができます。
  - [NSSA]：エリアを Not-So-Stubby Area にします。NSSA は、タイプ 7 LSA を受け入れます。[再配布（Redistribute）] チェックボックスをオフにし、[デフォルト情報起点（Default Information Originate）] チェックボックスをオンにすることで、ルートの再配布を無効化することができます。[集約 NSSA（Summary NSSA）] チェックボックスをオフにすることによって、集約 LSA でエリアへのフラッディングを防止できます。
- [メトリック値（Metric Value）]：デフォルト ルートの生成に使用するメトリックを指定します。デフォルト値は 10 です。有効なメトリック値の範囲は、0 ～ 16777214 です。
- [メトリック タイプ（Metric Type）]：メトリック タイプは、OSPF ルーティング ドメインにアドバタイズされるデフォルト ルートに関連付けられた外部リンク タイプです。使用可能なオプションは、タイプ 1 外部ルートの場合は 1、タイプ 2 外部ルートの場合は 2 です。
- [利用可能なネットワーク（Available Network）]：利用可能なネットワークの 1 つを選択して [追加（Add）] をクリックするか、**Add** (＋) をクリックして新しいネットワークオブジェクトを追加します。ネットワークの追加手順については、ネットワークを参照してください。
- [認証（Authentication）]：OSPF 認証を選択します。

- [なし（None）]：（デフォルト）OSPF エリアの認証を無効にします。
- [パスワード（Password）]：クリアテキストパスワードがエリア認証に使用されますが、セキュリティが懸念となっている場合は推奨しません。
- [MD5]：MD5 認証を許可します。

- [デフォルト コスト（Default Cost）]：接続先までの最短パスを割り出す OSPF エリアのデフォルトのコスト。有効値の範囲は、0 ～ 65535 です。デフォルト値は 1 です。

**ステップ 9** [OK] をクリックして、エリア設定を保存します。

**ステップ 10** **[範囲（Range）]** > **[追加（Add）]** を選択します。

- 使用可能なネットワークのいずれかを選択して、アドバタイズするかを決めます。
- **Add**(+)をクリックして、新しいネットワークオブジェクトを追加します。ネットワークの追加手順については、ネットワークを参照してください。

**ステップ 11** [OK] をクリックして、範囲設定を保存します。

**ステップ 12** [仮想リンク（Virtual Link）] を選択して、[追加（Add）](+) をクリックし、それぞれの OSPF プロセスに以下のオプションを設定します。

- [ピア ルータ（Peer Router）]：ピア ルータの IP アドレスを選択します。新しいピアルータを追加するには、**Add** (+) をクリックします。ネットワークの追加手順については、ネットワークを参照してください。
- [Hello 間隔（Hello Interval）]：hello パケットがインターフェイスで送信される秒単位の間隔です。hello 間隔は、hello パケットでアドバタイズされる符号なし整数です。この値は、特定のネットワーク上のすべてのルータおよびアクセス サーバーで同じである必要があります。有効値の範囲は 1 ～ 65535 です。デフォルトは 10 です。

  hello 間隔を小さくすると、トポロジ変更が検出されるまでの時間が短くなりますが、インターフェイス上で送信されるトラフィックは多くなります。
- [転送遅延（Transmit Delay）]：インターフェイス上で LSA パケットを送信するために必要と推定される時間（秒単位）。ゼロよりも大きい整数値を指定します。有効値の範囲は 1 ～ 8192 です。デフォルトは 1 です。

  アップデート パケット内の LSA 自体の経過時間は、転送前にこの値の分だけ増分されます。リンクでの送信前に遅延が加算されていない場合、LSA がリンクを介して伝播する時間は考慮されません。値は、インターフェイスの送信および伝播遅延を考慮して割り当てる必要があります。この設定は、非常に低速のリンクでより重要な意味を持ちます。
- [再転送間隔（Retransmit Interval）]：インターフェイスに属する隣接関係の LSA 再送信間の時間（秒単位）。再送信間隔は、接続されているネットワーク上の任意の 2 台のルータ間の予想されるラウンドトリップ遅延です。この値は、予想されるラウンドトリップ遅延より大きくなり、1 ～ 65535 の範囲で指定できます。デフォルトは 5 です。

ルータが自身のネイバーに LSA を送信する場合、ルータは確認応答メッセージを受信するまでその LSA を保持します。確認応答を受信しなかった場合、ルータでは LSA を再送します。この値は控えめに設定する必要があります。そうしないと、不要な再送信が発生する可能性があります。シリアル回線および仮想リンクの場合は、値を大きくする必要があります。

- [デッド間隔（Dead Interval）]：ルータがダウンしていることをネイバーが示す前に hello パケットを非表示にする秒単位の時間。Dead 間隔は符号なし整数です。デフォルトは hello 間隔の 4 倍または 40 秒です。この値は、共通のネットワークに接続されているすべてのルータおよびアクセス サーバーで同じであることが必要です。有効値の範囲は 1 ～ 65535 です。
- [認証（Authentication）]：以下から OSPF 仮想リンクの認証を選択します。
  - [なし（None）]：（デフォルト）仮想リンク エリアの認証を無効にします。
  - [エリア認証（Area Authentication）]：MD5 を使用して、エリア認証を有効にします。[追加（Add）] をクリックして、キー ID とキーを入力し、キーを確認し、[OK] をクリックします。
  - [パスワード（Password）]：クリアテキストパスワードが仮想リンクの認証に使用されますが、セキュリティが懸念となっている場合は推奨しません。
  - [MD5]：MD5 認証を許可します。[追加（Add）] をクリックして、キー ID とキーを入力し、キーを確認し、[OK] をクリックします。

    （注）
    MD5 キー ID として数字のみを入力してください。
  - [キー チェーン（Key Chain）]：キー チェーン認証を許可します。[追加（Add）] をクリックしてキーチェーンを作成した後、[保存（Save）] をクリックします。詳細な手順については、キーチェーンのオブジェクトの作成を参照してください。隣接関係を正常に確立するには、ピアに対して同じ認証タイプ（MD5 またはキー チェーン）とキー ID を使用します。

**ステップ 13** [OK] をクリックして、仮想リンクの設定を保存します。

**ステップ 14** ルーティング ページで [保存（Save）] をクリックして変更を保存します。

### 次のタスク

Configure OSPF Redistribution を続けます。

# OSPF 再配布の設定

Firewall Threat Defense デバイスは、OSPF ルーティング プロセス間のルート再配布を制御できます。1 つのルーティング プロセスから OSPF ルーティング プロセスへの再配布ルートのルールが表示されます。EIGRP、RIP および BGP で検出されたルートを、OSPF ルーティングプロ

セスに再配布することができます。スタティック ルートおよび接続されているルートも、OSPF ルーティング プロセスに再配布できます。

### 手順

**ステップ 1** [**Devices** > **Device Management**] を選択し、Firewall Threat Defense デバイスを編集します。

**ステップ 2** [ルーティング（Routing）] をクリックします。

**ステップ 3** （仮想ルータ対応デバイスの場合）[仮想ルータ（Virtual Routers）] ドロップダウンリストから、OSPF を設定する仮想ルータを選択します。

**ステップ 4** [OSPF] をクリックします。

**ステップ 5** [OSPFロール（OSPF Role）] ドロップダウンから、ロールを選択します。

**ステップ 6** **[再配布（Redistribution）]** > **[追加（Add）]** をクリックします。

エリアを切り取り、コピー、貼り付け、挿入、削除するには、**Edit** (✎) をクリックするか、右クリックしてメニューを表示、選択します。

**ステップ 7** OSPF プロセスごとに、次の再配布オプションを設定します。

- [OSPF Process]：プロセス ID を選択します。仮想ルーティングを使用するデバイスの場合、このドロップダウンリストに選択した仮想ルータ用に生成された一意のプロセス ID が表示されます。
- [ルート タイプ（Route Type）]：次のいずれかのタイプを選択します。
  - [スタティック（Static）]：スタティック ルートを OSPF ルーティング プロセスに再配布します。
  - [接続済み（Connected）]：接続されたルート（インターフェイス上で IP アドレスを有効にすることによって自動的に確立されるルート）を OSPF ルーティング プロセスに再配布します。接続済みルートは、デバイスの外部として再配布されます。[オプション（Optional）] リストのサブネットを使用するかどうかを選択できます。
  - [OSPF]：別の OSPF ルーティング プロセスからルートを再配布します（内部、外部 1 と 2、NSSA 外部 1 と 2、またはサブネットを使用するかどうか）。[オプション（Optional）] リストでこれらのオプションを選択できます。
  - [BGP]：BGP ルーティング プロセスからルートを再配布します。AS 番号およびサブネットを使用するかどうかを追加します。
  - [RIP]：RIP ルーティング プロセスからルートを再配布します。[オプション（Optional）] リストのサブネットを使用するかどうかを選択できます。

    （注）
    ユーザー定義の仮想ルータでは RIP がサポートされていないため、RIP からルートを再配布することはできません。

  - [EIGRP]：EIGRP ルーティング プロセスからルートを再配布します。AS 番号およびサブネットを使用するかどうかを追加します。

- [メトリック値（Metric Value）]：再配布するルートのメトリック値。デフォルト値は 10 です。有効な値の範囲は 0 ～ 16777214 です。

  同じデバイス上で 1 つの OSPF プロセスから別の OSPF プロセスに再配布する場合、メトリック値を指定しないと、メトリックは1つのプロセスから他のプロセスへ存続します。他のプロセスを OSPF プロセスに再配布するときに、メトリック値を指定しない場合、デフォルトのメトリックは 20 です。

- [メトリック タイプ（Metric Type）]：メトリック タイプは、OSPF ルーティング ドメインにアドバタイズされるデフォルト ルートに関連付けられた外部リンク タイプです。使用可能なオプションは、タイプ 1 外部ルートの場合は 1、タイプ 2 外部ルートの場合は 2 です。

- [タグ値（Tag Value）]：タグは 32 ビット 10 進数値を指定します。この値は、OSPF 自身では使用されないが ASBR 間の情報伝達に使用できる外部ルートのそれぞれに関連付けられます。何も指定しない場合、BGP および EGP からのルートにはリモート自律システムの番号が使用されます。その他のプロトコルについては、ゼロが使用されます。有効な値は 0 ～ 4294967295 です。

- [RouteMap]：送信元ルーティング プロトコルから現在のルーティング プロトコルへのルートのインポートのフィルタリングをチェックします。このパラメータを指定しない場合、すべてのルートが再配布されます。このパラメータを指定し、ルート マップ タグが表示されていない場合、ルートはインポートされません。または、**Add**(＋)をクリックして新しいルートマップを追加できます。新しいルートマップの追加については、「ルートマップ エントリの設定」を参照してください。

**ステップ 8** [OK] をクリックして、再配布設定を保存します。

**ステップ 9** [ルーティング（Routing）] ページで [保存（Save）] をクリックして変更を保存します。

### 次のタスク

OSPF エリア間フィルタリングの設定 （12 ページ）に進みます。

# OSPF エリア間フィルタリングの設定

ABR のタイプ 3 LSA フィルタリングは、OSPF を実行している ABR の機能を拡張して、異なる OSPF エリア間のタイプ 3 LSA をフィルタリングします。プレフィックス リストが設定されているときは、指定されたプレフィックスのみが OSPF エリア間で送信されます。その他のすべてのプレフィックスは、それぞれの OSPF エリアに制限されます。このタイプのエリア フィルタリングは、OSPF エリアを出入りするトラフィックに対して、またはそのエリアの着信と発信の両方のトラフィックに対して適用できます。

プレフィックス リストの複数のエントリが指定されたプレフィックスと一致する場合、シーケンス番号が最も小さいエントリが使用されます。効率性を高めるため、頻繁に一致するエントリまたは一致しないエントリに、小さいシーケンス番号を手動で割り当てることで、それらを

リストの上部に配置することもできます。デフォルトでは、シーケンス番号は自動的に生成され、開始値は 5 で 5 ずつ増えていきます。

### 手順

**ステップ 1** [**Devices** > **Device Management**] を選択し、Firewall Threat Defense デバイスを編集します。

**ステップ 2** [ルーティング（Routing）] をクリックします。

**ステップ 3** （仮想ルータ対応デバイスの場合）[仮想ルータ（Virtual Routers）] ドロップダウンリストから、OSPF を設定する仮想ルータを選択します。

**ステップ 4** [OSPF] をクリックします。

**ステップ 5** **[エリア間（InterArea）]** > **[追加（Add）]** を選択します。

エリア間を切り取り、コピー、貼り付け、挿入、削除するには、**Edit** (✎) をクリックするか、右クリックしてメニューを表示、選択します。

**ステップ 6** OSPF プロセスごとに、次のエリア間フィルタリング オプションを設定します。

- [OSPF Process]：仮想ルーティングを使用するデバイスの場合、選択した仮想ルータ用に生成された一意のプロセス ID がドロップダウンにリストされます。
- [エリア ID（Area ID）]：ルートを要約するエリア。
- [PrefixList]：プレフィックスの名前。新しいプレフィックス リスト オブジェクトを追加するには、ステップ 5 を参照してください。
- [トラフィックの方向（Traffic Direction）]：着信または発信。OSPF エリアへの LSA をフィルタリングするには [着信（Inbound）] を選択し、OSPF エリアからの LSA をフィルタリングするには [発信（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。

**ステップ 7** **Add** (＋) をクリックして、新しいプレフィックスリストの名前と、オーバーライドを許可するかどうかを入力します。

プレフィックス ルールを設定する前に、プレフィックス リストを設定する必要があります。

**ステップ 8** [追加（Add）] をクリックしてプレフィックス ルールを設定し、次のパラメータを設定します。

- [アクション（Action）]：再配布アクセスに対して [ブロック（Block）] または [許可（Allow）] を選択します。
- [シーケンス番号（Sequence No）]：ルーティング シーケンス番号。デフォルトでは、シーケンス番号は自動的に生成され、開始値は 5 で 5 ずつ増えていきます。
- [IP アドレス（IP Address）]：プレフィックス番号を IP アドレス/マスク長の形式で指定します。
- [最小プレフィックス長（Min Prefix Length）]：（オプション）最小のプレフィックス長。

- [最大プレフィックス長（Max Prefix Length）]：（オプション）最大のプレフィックス長。

**ステップ 9** [OK] をクリックして、エリア間フィルタリング設定を保存します。

**ステップ 10** [ルーティング（Routing）] ページで [保存（Save）] をクリックして変更を保存します。

### 次のタスク

OSPF フィルタルールの設定 （14 ページ）に進みます。

# OSPF フィルタルールの設定

OSPF プロセスごとに ABR タイプ 3 LSA フィルタを設定できます。ABR タイプ 3 LSA フィルタを設定すると、指定したプレフィックスだけが 1 つのエリアから別のエリアに送信され、その他のプレフィックスはすべて制限されます。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 エリアへ、または同じ OSPF エリアへ同時に適用できます。OSPF ABR タイプ 3 LSA フィルタリングによって、OSPF エリア間のルート再配布の制御が向上します。

### 手順

**ステップ 1** [**Devices** > **Device Management**] を選択し、Firewall Threat Defense デバイスを編集します。

**ステップ 2** [ルーティング（Routing）] をクリックします。

**ステップ 3** （仮想ルータ対応デバイスの場合）[仮想ルータ（Virtual Routers）] ドロップダウンリストから、OSPF を設定する仮想ルータを選択します。

**ステップ 4** [OSPF] をクリックします。

**ステップ 5** **[フィルタルール（Filter Rule）]** > **[追加（Add）]** を選択します。

**Edit** (✎) をクリックするか、右クリックメニューを使用して、フィルタルールの切り取り、コピー、貼り付け、挿入、および削除を行うことができます。

**ステップ 6** OSPF プロセスごとに、次のフィルタ ルール オプションを設定します。

- [OSPF Process]：仮想ルーティングを使用するデバイスの場合、選択した仮想ルータ用に生成された一意のプロセス ID がドロップダウンにリストされます。
- [アクセス リスト（Access List）]：この OSPF プロセスのアクセス リスト。新しい標準アクセスリストオブジェクトを追加するには、**Add** (＋) をクリックし、標準 ACL オブジェクトの設定を参照してください。
- [トラフィックの方向（Traffic Direction）]：フィルタリングするトラフィックの方向として [イン（In）] または [アウト（Out）] を選択します。OSPF エリアへの LSA をフィルタリングするには [イン（In）] を選択し、OSPF エリアからの LSA をフィルタリングするに

は [アウト（Out）] 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。

- [インターフェイス（Interface）]：このフィルタ ルールのインターフェイス。

**ステップ 7** [OK] をクリックしてルール設定を保存します。

**ステップ 8** [ルーティング（Routing）] ページで [保存（Save）] をクリックして変更を保存します。

### 次のタスク

OSPF サマリーアドレスの設定 （15 ページ）に進みます。

# OSPF サマリーアドレスの設定

他のプロトコルからのルートを OSPF に再配布する場合、各ルートは外部 LSA で個別にアドバタイズされます。ただし、再配布されるルートのうち、指定のネットワーク アドレスとマスクに含まれるすべてのものを 1 つのルートで表し、そのルートだけをアドバタイズするように Firewall Threat Defense デバイスを設定することができます。この設定によって OSPF リンクステート データベースのサイズが小さくなります。指定した IP アドレス マスク ペアと一致するルートは抑制できます。ルートマップで再配布を制御するために、タグ値を一致値として使用できます。

他のルーティング プロトコルから学習したルートをサマライズできます。サマリーのアドバタイズに使用されるメトリックは、具体的なルートすべての中で最小のメトリックです。サマリー ルートは、ルーティング テーブルのサイズを削減するのに役立ちます。

OSPF のサマリー ルートを使用すると、OSPF ASBR は、そのアドレスでカバーされるすべての再配布ルートの集約として、1 つの外部ルートをアドバタイズします。OSPF に再配布されている、他のルーティング プロトコルからのルートだけをサマライズできます。

### 手順

**ステップ 1** [**Devices** > **Device Management**] を選択し、Firewall Threat Defense デバイスを編集します。

**ステップ 2** [ルーティング（Routing）] をクリックします。

**ステップ 3** （仮想ルータ対応デバイスの場合）[仮想ルータ（Virtual Routers）] ドロップダウンリストから、OSPF を設定する仮想ルータを選択します。

**ステップ 4** [OSPF] をクリックします。

**ステップ 5** **[サマリーアドレス（Summary Address）]** > **[追加（Add）]** を選択します。

**Edit** ()をクリックして編集するか、右クリックメニューを使用して、サマリーアドレスの切り取り、コピー、貼り付け、挿入、および削除を行うことができます。

**ステップ 6** OSPF プロセスごとに、次のサマリー アドレス オプションを設定します。

- [OSPF Process]：仮想ルーティングを使用するデバイスの場合、選択した仮想ルータ用に生成された一意のプロセス ID がドロップダウンにリストされます。
- [利用可能なネットワーク（Available Networks）]：サマリーの IP アドレス。利用可能なネットワークリストから 1 つを選択して [追加（Add）] をクリックするか、**Add** (＋)をクリックして新しいネットワークを追加します。ネットワークを追加する手順については、ネットワークを参照してください。
- [タグ（Tag）]：各外部ルートに付加される 32 ビットの 10 進数値。この値は OSPF 自身には使用されませんが、ASBR 間の情報伝達に使用できます。
- [アドバタイズ（Advertise）]：集約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、このチェック ボックスはオンになっています。

**ステップ 7** [OK] をクリックしてサマリー アドレス設定を保存します。

**ステップ 8** [ルーティング（Routing）] ページで [保存（Save）] をクリックして変更を保存します。

### 次のタスク

OSPF インターフェイスとネイバーの設定 （16 ページ）に進みます。

# OSPF インターフェイスとネイバーの設定

必要に応じて一部のインターフェイス固有の OSPFv2 パラメータを変更できます。これらのパラメータを変更することは必須ではありませんが、hello インターバル、Dead 間隔、認証キーというインターフェイスパラメータは、接続されているネットワーク内のすべてのルータで一致している必要があります。これらのパラメータを設定する場合は、ネットワーク上のすべてのルータで、コンフィギュレーションの値が矛盾していないことを確認してください。

ポイントツーポイントの非ブロードキャスト ネットワークを介して OSPFv2 ルートをアドバタイズするには、スタティック OSPFv2 ネイバーを定義する必要があります。この機能により、OSPFv2 アドバタイズメントを GRE トンネルにカプセル化しなくても、既存の VPN 接続でブロードキャストすることができます。

### 手順

**ステップ 1** [**Devices** > **Device Management**] を選択し、Firewall Threat Defense デバイスを編集します。

**ステップ 2** [ルーティング（Routing）] をクリックします。

**ステップ 3** （仮想ルータ対応デバイスの場合）[仮想ルータ（Virtual Routers）] ドロップダウンリストから、OSPF を設定する仮想ルータを選択します。

**ステップ 4** [OSPF] をクリックします。

**ステップ 5** **[インターフェイス（Interface）]** > **[追加（Add）]** を選択します。

エリアを切り取り、コピー、貼り付け、挿入、削除するには、**Edit** (✎) をクリックするか、右クリックしてメニューを表示、選択します。

**ステップ 6** OSPF プロセスごとに、次のインターフェイス オプションを設定します。

- [インターフェイス（Interface）]：設定するインターフェイス。

  （注）
  デバイスが仮想ルーティングを使用している場合、このドロップダウンリストには、ルータに属するインターフェイスだけが表示されます。

- [デフォルトコスト（Default Cost）]：インターフェイスを介したパケット送信のコスト。デフォルト値は 10 です。

- [優先順位（Priority）]：ネットワークの代表ルータ。有効な値の範囲は 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指定ルータになったり、指定ルータのバックアップが行われたりします。

  2 つのルータがネットワークに接続している場合、両方が指定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指定ルータになります。ルータ優先順位が同じ場合は、ルータ ID が高い方が指定ルータになります。この設定は、ポイントツーポイントの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無視（MTU Ignore）]：OSPF は、共通のインターフェイス上でネイバーが同一の 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、ネイバーによる DBD パケットの交換時に行われます。DBD パケット内の受信した MTU が、受信インターフェイスに設定されている IP MTU より大きい場合は、OSPF 隣接関係は確立されません。

- [データベース フィルタ（Database Filter）]：この設定は、同期とフラッディングのときに発信 LSA インターフェイスをフィルタリングするのに使用します。デフォルトでは、OSPF は、LSA が到着したインターフェイスを除き、同じエリア内のすべてのインターフェイスで新しい LSA をフラッドします。完全メッシュ化トポロジでは、このフラッディングによって帯域幅が浪費されて、リンクおよび CPU の過剰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と、選択されているインターフェイスでは OSPF の LSA フラッディングが行われなくなります。

- [Hello 間隔（Hello Interval）]：インターフェイス上で送信される hello パケットの間隔を秒単位で指定します。有効な値の範囲は、1 ～ 8192 秒です。デフォルト値は 10 秒です。

  hello 間隔を小さくすると、トポロジ変更が検出されるまでの時間が短くなりますが、インターフェイス上で送信されるトラフィックは多くなります。この値は、特定のインターフェイス上のすべてのルータおよびアクセス サーバーで同じである必要があります。

- [伝送遅延（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（秒単位）。有効な値の範囲は 1 ～ 65535 秒です。デフォルト値は 1 秒です。

  更新パケット内の LSA には、送信前に、このフィールドで指定した値によって増分された経過時間が格納されます。リンクでの送信前に遅延が加算されていない場合、LSA がリンクを介して伝播する時間は考慮されません。値は、インターフェイスの送信および伝播遅延を考慮して割り当てる必要があります。この設定は、非常に低速のリンクでより重要な意味を持ちます。

- [再送信間隔（Retransmit Interval）]：インターフェイスに属する隣接関係の LSA 再送信間の時間（秒単位）。接続ネットワーク上の任意の2台のルータ間で想定される往復遅延より大きな値にする必要があります。有効な値の範囲は、1 ～ 65535 秒です。デフォルトは 5 秒です。

  ルータが自身のネイバーに LSA を送信する場合、ルータは確認応答メッセージを受信するまでその LSA を保持します。確認応答を受信しなかった場合、ルータでは LSA を再送します。この値は控えめに設定する必要があります。そうしないと、不要な再送信が発生する可能性があります。シリアル回線および仮想リンクの場合は、値を大きくする必要があります。

- [Dead 間隔（Dead Interval）]：hello パケットが確認されない場合に、ルータがダウンしたとネイバーが判断するまでの待ち時間（秒単位）。この値は、ネットワーク上のすべてのノードで同じである必要があり、1 ～ 65535 の範囲で指定できます。

- [Hello 乗数（Hello Multiplier）]：1 秒ごとに送信される hello パケットの数を指定します。有効な値は 3 ～ 20 です。

- [ポイント ツー ポイント（Point-to-Point）]：VPN トンネルで OSPF ルートを送信できます。

- [認証（Authentication）]： OSPF のインターフェイス認証を次から選択します。

  - [なし（None）]：（デフォルト）インターフェイス認証を無効にします。

  - [エリア認証（Area Authentication）]：MD5 を使用したインターフェイス認証を有効にします。[追加（Add）] をクリックして、キー ID とキーを入力し、キーを確認し、[OK] をクリックします。

  - [パスワード（Password）]：クリアテキストパスワードが仮想リンクの認証に使用されますが、セキュリティが懸念となっている場合は推奨しません。

  - [MD5]：MD5 認証を許可します。[追加（Add）] をクリックして、キー ID とキーを入力し、キーを確認し、[OK] をクリックします。

    （注）
    MD5 キー ID として数字のみを入力してください。

  - [キー チェーン（Key Chain）]：キー チェーン認証を許可します。[追加（Add）] をクリックしてキーチェーンを作成した後、[保存（Save）] をクリックします。詳細な手順については、キーチェーンのオブジェクトの作成を参照してください。隣接関係を正常に確立するには、ピアに対して同じ認証タイプ（MD5 またはキー チェーン）とキー ID を使用します。

- [BFDの有効化（Enable BFD）]：このインターフェイスで BFD を有効にできます。

- [パスワードの入力（Enter Password）]：認証のタイプとして [パスワード（Password）] を選択した場合に、設定するパスワード。

- [パスワードの確認（Confirm Password）]：選択したパスワードを確認します。

**ステップ 7** **[ネイバー（Neighbor）] > [追加（Add）]** を選択します。

エリアを切り取り、コピー、貼り付け、挿入、削除するには、**Edit** (✎) をクリックするか、右クリックしてメニューを表示、選択します。

**ステップ 8** OSPF プロセスごとに、次のパラメータを設定します。

- [OSPF プロセス（OSPF Process）] : 1 または 2 を選択します。
- [ネイバー（Neighbor）] : ドロップダウンリストでネイバーの 1 つを選択するか、**Add** (＋) をクリックして新しいネイバーを追加します。名前、説明、ネットワーク、およびオーバーライドを許可するかどうかを入力し、[保存（Save）] をクリックします。
- [インターフェイス（Interface）] : 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。

**ステップ 9** [OK] をクリックして、ネイバー設定を保存します。

**ステップ 10** [ルーティング（Routing）] ページで [保存（Save）] をクリックして変更を保存します。

# OSPF 詳細プロパティの設定

[高度なプロパティ（Advanced Properties）] を使用すると、syslog メッセージ生成、アドミニストレーティブ ルート ディスタンス、LSA タイマー、グレースフルリスタートなどのオプションを設定できます。

### グレースフル リスタート

Firewall Threat Defense デバイスでは、既知の障害状況が発生することがあります。これにより、スイッチング プラットフォーム全体でパケット転送に影響を与えることがあってはなりません。Non-Stop Forwarding（NSF）機能では、ルーティング プロトコル情報を復元している間に、既知のルートへのデータ転送が続行されます。この機能は、スケジュール済みヒットレス ソフトウェア アップグレードがあるときに便利です。NSF Cisco（RFC 4811 および RFC 4812）または NSF IETF（RFC 3623）のいずれかを使用して、OSPFv2 上でグレースフル リスタートを設定できます。

（注） NSF 機能は HA モードとクラスタリングでも役立ちます。

NSF グレースフル リスタート機能の設定には、機能の設定と NSF 対応または NSF 認識としてのデバイスの設定という 2 つのステップが伴います。NSF 対応デバイスは、ネイバーに対して独自のリスタート アクティビティを示すことができ、NSF 認識デバイスはネイバーのリスタートをサポートすることができます。

デバイスは、いくつかの条件に応じて、NSF 対応または NSF 認識として設定できます。

- デバイスは、現在のデバイスのモードに関係なく、NSF 認識デバイスとして設定できます。

- デバイスを NSF 対応として設定するには、デバイスはフェールオーバーまたはスパンド EtherChannel（L2）クラスタ モードのいずれかである必要があります。
- デバイスを NSF 認識または NSF 対応にするには、必要に応じて opaque リンク ステート アドバタイズメント（LSA）/リンク ローカル シグナリング（LLS）ブロックの機能を使って設定する必要があります。

## 手順

**ステップ 1** [**Devices** > **Device Management**] を選択し、Firewall Threat Defense デバイスを編集します。

**ステップ 2** [ルーティング（Routing）] をクリックします。

**ステップ 3** （仮想ルータ対応デバイスの場合）[仮想ルータ（Virtual Routers）] ドロップダウンリストから、OSPF を設定する仮想ルータを選択します。

**ステップ 4** [OSPF] > [詳細（Advanced）] をクリックします。 >

**ステップ 5** [一般（General）] を選択し、次のように設定します。

- [ルータID（Router ID）]：[自動（Automatic）] または [IP アドレス（IP Address）]（非クラスタおよびスパンド EtherChannel モードのクラスタの場合に表示）またはルータ ID の [クラスタプール（Cluster Pool）]（個別インターフェイスモードのクラスタの場合に表示）を選択します。[IPアドレス（IP address）] を選択する場合は、隣接するフィールドに IP アドレスを入力します。[クラスタプール（Cluster Pool）] を選択した場合は、隣接するドロップダウンフィールドで IPv4 クラスタプールの値を選択します。クラスタプールアドレスの作成については、アドレス プールを参照してください。
- [LSA MOSPF を無視（Ignore LSA MOSPF）]：ルートがサポートされていない LSA タイプ 6 マルチキャスト OSPF（MOSPF）パケットを受信した場合、syslog メッセージを抑制します。
- [RFC 1583 互換（RFC 1583 Compatible）]：集約ルートのコストを計算するための手段として RFC 1583 の互換性を設定します。RFC 1583 の互換性が有効な場合、ルーティング ループが発生することがあります。ルーティング ループを防止するには、これを無効にします。OSPF ルーティング ドメイン内のすべての OSPF ルータの RFC 互換設定が同じである必要があります。
- [隣接関係の変更（Adjacency Changes）]：syslog メッセージが送信される隣接関係の変更内容を定義します。

  デフォルトでは、OSPF ネイバーがアップ状態またはダウン状態になったときに、syslog メッセージが生成されます。OSPF ネイバーがダウンしたときに syslog メッセージを送信するようルータを設定することも、状態ごとに syslog を送信するように設定することもできます。

  - [隣接関係の変更のログ記録（Log Adjacency Changes）]：OSPF ネイバーが起動または停止したときに、Firewall Threat Defense デバイスによって syslog メッセージが送信されるようになります。この設定は、デフォルトでオンになっています。

- [隣接関係の変更の詳細のログ記録（Log Adjacency Change Details）]：ネイバーがアップ状態またはダウン状態になったときだけでなく、状態の変更が発生したときにも Firewall Threat Defense デバイスによって syslog メッセージが送信されるようになります。デフォルトでは、この設定はオフになっています。

- [アドミニストレーティブ ルート ディスタンス（Administrative Route Distance）]：**エリア間**、**エリア内**、および**外部** IPv6 ルートのアドミニストレーティブ ルート ディスタンスの設定に使用された設定を変更できます。アドミニストレーティブ ルート ディスタンスは 1 ～ 254 の整数です。デフォルトは 110 です。
- [LSA グループ ペーシング（LSA Group Pacing）]：LSA をグループにまとめてリフレッシュ、チェックサム計算、エージングする間隔を秒単位で指定します。有効な値の範囲は 10 ～ 1800 です。デフォルト値は 240 です。
- [デフォルト情報の発信を有効にする（Enable Default Information Originate）]：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には、[有効化（Enable）] チェックボックスをオンにして、次のオプションを設定します。
  - [デフォルト ルートを常にアドバタイズする（Always advertise the default route）]：デフォルト ルートが常にアドバタイズされるようにします。
  - [メトリック値（Metric Value）]：デフォルトルートの生成に使用するメトリックを指定します。有効なメトリック値の範囲は、0 ～ 16777214 です。デフォルト値は 10 です。
  - [メトリック タイプ（Metric Type）]：OSPFv3 ルーティング ドメインにアドバタイズされるデフォルトルートに関連付けられた外部リンク タイプ。有効な値は1（タイプ 1 の外部ルート）および 2（タイプ 2 の外部ルート）です。デフォルトはタイプ 2 外部ルートです。
  - [ルートマップ（RouteMap）]：ルートマップが満たされている場合にデフォルトルートを生成するルーティングプロセスを選択するか、**Add**(＋) をクリックして、新しいルーティングプロセスを追加します。新しいルートマップの追加については、「ルート マップ エントリの設定」を参照してください。

**ステップ 6** [OK] をクリックして、一般設定を保存します。

**ステップ 7** [ノンストップフォワーディング（Non Stop Forwarding）] を選択し、NSF 対応または NSF 認識デバイスに対して、OSPFv2 の Cisco NSF グレースフルリスタートを設定します。

（注）
OSPFv2 には、Cisco NSF と IETF NSF の 2 つのグレースフル リスタート メカニズムがあります。OSPF インスタンスに対しては、これらのグレースフル リスタート メカニズムのうち一度に設定できるのは 1 つだけです。NSF 認識デバイスは、Cisco NSF ヘルパーと IETF NSF ヘルパーの両方として設定できますが、NSF 対応デバイスは OSPF インスタンスに対して、Cisco NSF または IETF NSF モードのいずれかとして設定できます。

a) [Cisco Non Stop Forwarding 機能を有効にする（Enable Cisco Non Stop Forwarding Capability）] チェックボックスをオンにします。

b) （オプション）必要に応じて、[非 NSF 認識隣接ネットワーキング デバイスが検出されたときに NSF リスタートをキャンセルする（Cancel NSF restart when non-NSF-aware neighboring networking devices are detected）] チェックボックスをオンにします。

c) （オプション）[Cisco Non Stop Forwarding ヘルパー モードを有効にする（Enable Cisco Non Stop Forwarding Helper mode）] チェックボックスをオフにして、NSF 認識デバイスでのヘルパー モードを無効にします。

**ステップ 8** NSF 対応または NSF 認識デバイスに対して、OSPFv2 の IETF NSF グレースフル リスタートを設定します。

a) [IETF Non Stop Forwarding 機能を有効にする（Enable IETF Non Stop Forwarding Capability）] チェックボックスをオンにします。

b) [グレースフル リスタート間隔（秒）（Length of graceful restart interval (seconds)）] フィールドにリスタート間隔を秒単位で入力します。デフォルト値は 120 秒です。30 秒未満の再起動間隔では、グレースフル リスタートが中断します。

c) （オプション）[ヘルパー モードの IETF Nonstop Forwarding（NSF）を有効にする（Enable IETF nonstop forwarding (NSF) for helper mode）] チェックボックスをオフにして、NSF 認識デバイスでの IETF NSF ヘルパー モードを無効にします。

d) [厳密なリンク ステートのアドバタイズメント チェックを有効にする（Enable Strict Link State advertisement checking）]：有効にすると、再起動ルータにフラッディングされる可能性がある LSA への変更があることが検出された場合、またはグレースフル リスタート プロセスが開始されたときに再起動ルータの再送リスト内に変更された LSA があると検出された場合、ヘルパー ルータはルータの再起動プロセスを終了させます。

e) [IETF Non Stop Forwarding を有効にする（Enable IETF Non Stop Forwarding）]：スイッチオーバー後にルーティング プロトコル情報が復元される間、データのパケットの転送が既知のルートで続行される Non Stop Forwarding を有効にします。OSPF は OSPF プロトコルの拡張を使用して、隣接する OSPF デバイスからステートを回復します。リカバリが機能するためには、ネイバーが NSF プロトコル拡張をサポートし、再起動するデバイスの「ヘルパー」として積極的に動作する必要があります。ネイバーはまた、プロトコル ステートのリカバリが行われる間、再起動するデバイスにデータ トラフィックを転送し続ける必要もあります。

# OSPFv3 の設定

ここでは、OSPFv3 ルーティング プロセスの設定に関連するタスクについて説明します。仮想ルーティングを使用しているデバイスの場合、ユーザー定義の仮想ルータではなく、グローバル仮想ルータに対してのみ OSPFv3 を設定できます。

## OSPFv3 エリア、ルート集約、および仮想リンクの設定

OSPFv3 を有効にするには、OSPFv3 ルーティング プロセスを作成し、OSPFv3 用のエリアを作成して、OSPFv3 のインターフェイスを有効にする必要があります。その後、ターゲットの OSPFv3 ルーティング プロセスにルートを再配布する必要があります。

手順

**ステップ 1** [**Devices** > **Device Management**] を選択し、Firewall Threat Defense デバイスを編集します。

**ステップ 2** [ルーティング（Routing）] タブをクリックします。タブの左ペインで、 **[OSPFv3]** をクリックします。

**ステップ 3** デフォルトでは、[プロセス 1 を有効にする（Enable Process 1）] が選択されています。最大 2 つの OSPF プロセス インスタンスを有効にできます。

**ステップ 4** OSPFv3 ロールをドロップダウン リストから選択し、それに対応する説明を入力します。オプションは、[内部（Internal）]、[ABR]、[ASBR]、[ABR および ASBR（ABR and ASBR）] です。OSPFv3 ロールの説明については、About OSPF （1 ページ）を参照してください。

**ステップ 5** **[エリア（Area）] > [追加（Add）]** を選択します。

エリアを切り取り、コピー、貼り付け、挿入、削除するには、**Edit** (✎) をクリックするか、右クリックしてメニューを表示、選択します。

**ステップ 6** [一般（General）] を選択し、各 OSPF プロセスについて次のオプションを設定します。

- [エリア ID（Area ID）] : ルートを要約するエリア。
- [コスト（Cost）] : この集約ルートのメトリックまたはコスト。宛先への最短パスを決定するための OSPF SPF 計算で使用します。有効な値の範囲は 0 ～ 16777215 です。
- [タイプ（Type）] : [標準（Normal）]、[NSSA]、[スタブ（Stub）] を指定します。[標準（Normal）] を選択した場合、設定するその他のパラメータはありません。[スタブ（Stub）] を選択した場合、エリアでサマリー LSA を送信することができます。[NSSA] を選択した場合、次の 3 つのオプションを設定できます。
  - [このエリアへのサマリー LSA の送信を許可する（Allow Sending summary LSA into this area）] : エリアにサマリー LSA を送信することを許可します。
  - [標準およびNSSAエリアにルートをインポート（Imports routes to normal and NSSA area）] : 再配布でルートをスタブエリアでなく標準エリアにインポートできるようになります。
  - [デフォルト情報生成（Defaults information originate）] : OSPFv3 ルーティング ドメインへのデフォルト外部ルートを生成します。
- [メトリック（Metric）] : デフォルトルートを生成するために使用するメトリック。デフォルト値は 10 です。有効なメトリック値の範囲は、0 ～ 16777214 です。
- [メトリック タイプ（Metric Type）] : メトリック タイプは、OSPFv3 ルーティング ドメインにアドバタイズされるデフォルト ルートに関連付けられた外部リンク タイプです。使用可能なオプションは、タイプ 1 外部ルートの場合は 1、タイプ 2 外部ルートの場合は 2 です。

**ステップ 7** [OK] をクリックして、一般設定を保存します。

**ステップ 8** （内部 OSPFv3 ロールには適用されません）**[ルート集約（RouteSummary）]** > **[ルート集約の追加（Add Route Summary）]** を選択します。

**Edit**(✎)をクリックするか、右クリックメニューを使用して、ルート集約の切り取り、コピー、貼り付け、挿入、および削除を行うことができます。

**ステップ 9** OSPF プロセスごとに、次のルート集約オプションを設定します。

- [IPv6 プレフィックス/長さ（IPv6 Prefix/Length）]：IPv6 プレフィックス。新しいネットワークオブジェクトを追加するには、**Add**(＋)をクリックします。ネットワークを追加する手順については、ネットワークを参照してください。
- [コスト（Cost）]：この集約ルートのメトリックまたはコスト。宛先への最短パスを決定するための OSPF SPF 計算で使用します。有効な値の範囲は 0 ～ 16777215 です。
- [アドバタイズ（Advertise）]：集約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、このチェック ボックスはオンになっています。

**ステップ 10** [OK] をクリックして、ルート集約設定を保存します。

**ステップ 11** （内部 OSPFv3 ロールには適用されません）[仮想リンク（Virtual Link）] を選択し、[仮想リンクの追加（Add Virtual Link）] をクリックして、各 OSPF プロセスについて次のオプションを設定します。

- [ピア ルータ ID（Peer RouterID）]：ピア ルータの IP アドレスを選択します。新しいネットワークオブジェクトを追加するには、**Add**(＋)をクリックします。ネットワークを追加する手順については、ネットワークを参照してください。
- [TTL セキュリティ（TTL Security）]：TTL セキュリティ チェックを有効にします。このホップカウントの値は、1 ～ 254 の数値です。デフォルトは 1 です。

  OSPF は、IP ヘッダー存続可能時間（TTL）の値が 255 の発信パケットを送信し、設定可能なしきい値よりも低い TTL 値の入力パケットを廃棄します。IP パケットを転送する各デバイスは TTL が低下するため、直接（1 ホップ）接続により受信されたパケットの TTL 値は 255 になります。2 つのホップを通過するパケットの値は 254 というようになります。受信しきい値は、パケットが移動する可能性がある最大ホップ数で設定されます。
- [Dead 間隔（Dead Interval）]：hello パケットが届かなかった場合にネイバーがルータのダウンを示すまでの時間（秒単位）。デフォルトは hello 間隔の 4 倍または 40 秒です。有効な値の範囲は 1 ～ 65535 です。

  Dead 間隔は符号なし整数です。この値は、共通のネットワークに接続されているすべてのルータおよびアクセス サーバーで同じであることが必要です。
- [Hello 間隔（Hello Interval）]：hello パケットがインターフェイスで送信される間隔（秒単位）。有効な値の範囲は 1 ～ 65535 です。デフォルトは 10 です。

  hello 間隔は、hello パケットでアドバタイズされる符号なし整数です。この値は、特定のネットワーク上のすべてのルータおよびアクセス サーバーで同じである必要があります。

hello間隔を小さくすると、トポロジ変更が検出されるまでの時間が短くなりますが、インターフェイス上で送信されるトラフィックは多くなります。

- [再転送間隔（Retransmit Interval）]：インターフェイスに属する隣接関係の LSA 再送信間の時間（秒単位）。再送信間隔は、接続されているネットワーク上の任意の2台のルータ間の予想されるラウンドトリップ遅延です。この値は、予想されるラウンドトリップ遅延より大きくなり、1 ～ 65535 の範囲で指定できます。デフォルトは 5 です。

  ルータが自身のネイバーに LSA を送信する場合、ルータは確認応答メッセージを受信するまでその LSA を保持します。確認応答を受信しなかった場合、ルータでは LSA を再送します。この値は控えめに設定する必要があります。そうしないと、不要な再送信が発生する可能性があります。シリアル回線および仮想リンクの場合は、値を大きくする必要があります。

- [転送遅延（Transmit Delay）]：インターフェイス上で LSA パケットを送信するために必要と推定される時間（秒単位）。ゼロよりも大きい整数値を指定します。有効な値の範囲は 1 ～ 8192 です。デフォルトは 1 です。

  アップデート パケット内の LSA 自体の経過時間は、転送前にこの値の分だけ増分されます。リンクでの送信前に遅延が加算されていない場合、LSAがリンクを介して伝播する時間は考慮されません。値は、インターフェイスの送信および伝播遅延を考慮して割り当てる必要があります。この設定は、非常に低速のリンクでより重要な意味を持ちます。

**ステップ 12** [OK] をクリックして、仮想リンク設定を保存します。

**ステップ 13** [ルータ（Router）] ページで [保存（Save）] をクリックして変更を保存します。

### 次のタスク

OSPFv3 再配布の設定を続けます。

# OSPFv3 再配布の設定

Secure Firewall Threat Defense デバイスは、OSPF ルーティング プロセス間のルート再配布を制御できます。1 つのルーティング プロセスから OSPF ルーティング プロセスへの再配布ルートのルールが表示されます。EIGRP、RIP および BGP で検出されたルートを、OSPF ルーティングプロセスに再配布することができます。スタティック ルートおよび接続されているルートも、OSPF ルーティング プロセスに再配布できます。

### 手順

**ステップ 1** [**Devices** > **Device Management**] を選択し、Firewall Threat Defense デバイスを編集します。

**ステップ 2** [ルーティング（Routing）] > [OSPF] を選択します。

**ステップ 3** [再配布（Redistribution）] を選択し、[追加（Add）] をクリックします。

エリアを切り取り、コピー、貼り付け、挿入、削除するには、**Edit** (✎) をクリックするか、右クリックしてメニューを表示、選択します。

**ステップ 4** OSPF プロセスごとに、次の再配布オプションを設定します。

- [ソース プロトコル（Source Protocol）]：ルートの再配布元となるソース プロトコル。サポートされるプロトコルは、接続済み、OSPF、静的、EIGRP、BGP です。OSPF を選択した場合は、[プロセス ID（Process ID）] フィールドにプロセス ID を入力する必要があります。BGP を選択した場合は、[AS番号（AS Number）] フィールドに AS 番号を追加する必要があります。
- [メトリック（Metric）]：配布されるルートのメトリック値。 デフォルト値は 10 です。有効な値の範囲は 0 ～ 16777214 です。

  同じデバイス上で 1 つの OSPF プロセスから別の OSPF プロセスに再配布する場合、メトリック値を指定しないと、メトリックは 1 つのプロセスから他のプロセスへ存続します。他のプロセスを OSPF プロセスに再配布するときに、メトリック値を指定しない場合、デフォルトのメトリックは 20 です。
- [メトリック タイプ（Metric Type）]：メトリック タイプは、OSPF ルーティング ドメインにアドバタイズされるデフォルト ルートに関連付けられた外部リンク タイプです。使用可能なオプションは、タイプ 1 外部ルートの場合は 1、タイプ 2 外部ルートの場合は 2 です。
- [タグ（Tag）]：タグは 32 ビット 10 進数値を指定します。この値は、OSPF 自身では使用されないが ASBR 間の情報伝達に使用できる外部ルートのそれぞれに関連付けられます。何も指定しない場合、BGP および EGP からのルートにはリモート自律システムの番号が使用されます。その他のプロトコルについては、ゼロが使用されます。有効な値は 0 ～ 4294967295 です。
- [ルート マップ（Route Map）]：送信元ルーティング プロトコルから現在のルーティング プロトコルへのルートのインポートのフィルタリングをチェックします。このパラメータを指定しない場合、すべてのルートが再配布されます。このパラメータを指定し、ルート マップ タグが表示されていない場合、ルートはインポートされません。または、**Add** (＋) をクリックして新しいルートマップを追加できます。新しいルートマップを追加する手順については、ルート マップを参照してください。
- [プロセス ID（Process ID）]：OSPF プロセス ID。1 または 2。

  （注）
  プロセス ID が有効であると、OSPFv3 プロセスは別の OSPFv3 プロセスから認識したルートを再配布します。

- [一致（Match）]：OSPF ルートを他のルーティング ドメインに再配布できるようにします。
  - [内部（Internal）] は、特定の自律システムの内部にあるルートです。
  - [外部 1（External 1）] は、自律システムの外部であるが、OSPFv3 にタイプ 1 外部ルートとしてインポートされるルートです。

- [外部2（External2）]は、自律システムの外部であるが、OSPFv3にタイプ2外部ルートとしてインポートされるルートです。
- [NSSA外部1（NSSA External 1）]は、自律システムの外部であるが、IPv6用のNSSAのOSPFv3にタイプ1の外部ルートとしてインポートされるルートです。
- [NSSA外部2（NSSA External 2）]は、自律システムの外部であるが、IPv6用のNSSAのOSPFv3にタイプ2の外部ルートとしてインポートされるルートです。

**ステップ5** [OK] をクリックして、再配布設定を保存します。

**ステップ6** [ルーティング（Routing）] ページで [保存（Save）] をクリックして変更を保存します。

### 次のタスク

OSPFv3 サマリー プレフィックスの設定 （27 ページ）に進みます。

# OSPFv3 サマリー プレフィックスの設定

指定されたIPv6プレフィックスとマスクのペアに一致するルートをアドバタイズするようにFirewall Threat Defenseデバイスを設定できます。

### 手順

**ステップ1** [**Devices** > **Device Management**] を選択し、Firewall Threat Defenseデバイスを編集します。

**ステップ2** [ルーティング（Routing）] > [OSPFv3] を選択します。

**ステップ3** **[サマリープレフィックス（Summary Prefix）] > [追加（Add）]** を選択します。

**Edit** (✎) をクリックするか、右クリックメニューを使用して、サマリープレフィックスの切り取り、コピー、貼り付け、挿入、および削除を行うことができます。

**ステップ4** OSPFプロセスごとに、次のサマリー プレフィックス オプションを設定します。

- [IPv6プレフィックス/長さ（IPv6 Prefix/Length）]：IPv6プレフィックスとプレフィックス長のラベル。リストから1つを選択するか、**Add** (＋) をクリックして新しいネットワークオブジェクトを追加します。ネットワークを追加する手順については、ネットワークを参照してください。
- [アドバタイズ（Advertise）]：指定されたプレフィックスとマスクのペアに一致するルートをアドバタイズします。このチェックボックスをオフにすると、指定されたプレフィックスとマスク ペアと一致するルートが抑制されます。
- （オプション）[タグ（Tag）]：ルート マップで再配布を制御するための「match」値として使用できるタグ値。

**ステップ 5** [OK] をクリックして、サマリー プレフィックス設定を保存します。

**ステップ 6** [ルーティング（Routing）] ページで [保存（Save）] をクリックして変更を保存します。

### 次のタスク

OSPFv3 インターフェイス、認証、およびネイバーの設定 （28 ページ）に進みます。

# OSPFv3 インターフェイス、認証、およびネイバーの設定

必要に応じて特定のインターフェイス固有の OSPFv3 パラメータを変更できます。これらのパラメータを必ずしも変更する必要はありませんが、hello interval と dead interval というインターフェイスパラメータは、接続されているネットワーク内のすべてのルータで一致している必要があります。これらのパラメータを設定する場合は、ネットワーク上のすべてのルータで、コンフィギュレーションの値が矛盾していないことを確認してください。

Nexus スイッチで OSPFv3 認証を正常に実装するには、互換性のあるバージョンのスイッチ（Nexus 3000、7000、9000 シリーズ スイッチなど）があることを確認します。

### 手順

**ステップ 1** [**Devices** > **Device Management**] を選択し、Firewall Threat Defense デバイスを編集します。

**ステップ 2** [ルーティング（Routing）] > [OSPFv3] を選択します。

**ステップ 3** **[インターフェイス（Interface）] > [追加（Add）]** を選択します。

[編集（Edit）] をクリックしてエリアを編集するか、右クリックメニューを使用してエリアを切り取り、コピー、貼り付け、挿入、削除することができます。

**ステップ 4** 各 OSPFv3 プロセスについて、次のインターフェイス オプションを設定します。

- [インターフェイス（Interface）]：設定するインターフェイス。
- [OSPFv3 を有効にする（Enable OSPFv3）]：OSPFv3 を有効にします。
- [OSPF プロセス（OSPF Process）]：1 または 2 を選択します。
- [エリア（Area）]：このプロセスのエリア ID。
- [インスタンス（Instance）]：インターフェイスに割り当てるエリア インスタンス ID を指定します。インターフェイスは、OSPFv3 エリアを 1 つだけ保有できます。複数のインターフェイスで同じエリアを使用でき、各インターフェイスは異なるエリア インスタンス ID を使用できます。

**ステップ 5** [プロパティ（Properties）] を選択し、各 OSPFv3 プロセスについて次のオプションを設定します。

- [発信リンク ステート アドバタイズメントをフィルタ（Filter Outgoing Link Status Advertisements）]：OSPFv3インターフェイスへの発信LSAをフィルタ処理します。デフォルトでは、すべての発信 LSA がインターフェイスにフラッディングされます。
- [MTU 不一致検出を無効にする（Disable MTU mismatch detection）]：DBD パケットが受信された場合、OSPF MTU 不一致検出を無効にします。OSPF MTU 不一致検出は、デフォルトで有効になっています。
- [フラッドの削減（Flood Reduction）]：エリア全体で 3600 秒ごとにフラッディングしないように、標準の LSA を [LSA をエージングしない（Do Not Age LSAs）] に変更します。

  OSPF LSA は 3600 秒ごとに更新されます。大規模な OSPF ネットワークでは、これにより大量の不要な LSA フラッディングがエリアからエリアに発生する可能性があります。
- [ポイントツーポイント ネットワーク（Point-to-Point Network）]：OSPF ルートを VPN トンネル経由で送信できます。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はネイバーを 1 つだけ定義できます。
  - ネイバーは手動で設定する必要があります。
  - クリプト エンドポイントを指すスタティック ルートを定義する必要があります。
  - トンネル経由の OSPF がインターフェイスで実行中である場合は、アップストリームルータを使用する通常の OSPF を同じインターフェイス上で実行することはできません。
  - OSPF ネイバーを指定する前に、クリプト 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。これは、OSPF アップデートが VPN トンネルを通過できるようにするためです。OSPF ネイバーを指定した後でクリプト マップをインターフェイスにバインドした場合は、**clear local-host all** コマンドを使用して OSPF 接続をクリアします。これで、OSPF 隣接関係を VPN トンネル経由で確立できるようになります。
- [ブロードキャスト（Broadcast）]：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。デフォルトでは、イーサネットインターフェイスの場合はこのチェックボックスがオンになっています。このチェックボックスをオフにすると、インターフェイスをポイントツーポイントの非ブロードキャストインターフェイスとして指定したことになります。インターフェイスをポイントツーポイントの非ブロードキャストとして指定すると、OSPF ルートを VPN トンネル経由で送信できます。
- [コスト（Cost）]：インターフェイスでパケットを送信するコストを指定します。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指定ルータになったり、指定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の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。

  2 つのルータがネットワークに接続している場合、両方が指定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指定ルータになります。ルータ優先順位が同じ場合は、ルータ ID が高い方が指定ルータになります。

- [優先順位（Priority）]：ネットワークの代表ルータを指定します。有効な値の範囲は 0 ～ 255 です。
- [Dead 間隔（Dead Interval）]：hello パケットが確認されない場合に、ルータがダウンしたとネイバーが判断するまでの待ち時間（秒単位）。この値はネットワーク上のすべてのノードで同じにする必要があります。値の範囲は、1 ～ 65535 です。
- [Hello間隔（Hello Interval）]：ネイバーとの隣接関係が確立される前にルータが送信する OSPF パケット間の期間（秒単位）。ルーティング デバイスがアクティブなネイバーを検出すると、hello パケット間隔はポーリング間隔で指定された時間から Hello 間隔で指定された時間に変更されます。有効な値の範囲は、1 ～ 65535 秒です。
- [再送信間隔（Retransmit Interval）]：インターフェイスに属する隣接関係の LSA 再送信間の時間（秒単位）。接続ネットワーク上の任意の 2 台のルータ間で想定される往復遅延より大きな値にする必要があります。有効な値の範囲は、1 ～ 65535 秒です。デフォルトは 5 秒です。
- [転送遅延（Transmit Delay）]：インターフェイス上でリンクステート更新パケットを送信する予想時間（秒単位）。有効な値の範囲は、1 ～ 65535 秒です。デフォルト値は 1 秒です。
- [BFDの有効化（Enable BFD）]：このインターフェイスで BFD を有効にできます。

**ステップ 6** [OK] をクリックして、プロパティ設定を保存します。

**ステップ 7** [認証（Authentication）] を選択し、各 OSPFv3 プロセスについて次のオプションを設定します。

- [タイプ（Type）]：認証のタイプ。使用可能なオプションは、[エリア（Area）]、[インターフェイス（Interface）]、[なし（None）] です。[なし（None）] オプションを選択すると、認証が行われません。
- [セキュリティ パラメータ インデックス（Security Parameters Index）]：256 ～ 4294967295 の数値。タイプとして [インターフェイス（Interface）] を選択した場合、このオプションを設定します。
- [認証（Authentication）]：認証アルゴリズムのタイプ。サポートされる値は、[SHA-1] および [MD5] です。タイプとして [インターフェイス（Interface）] を選択した場合、このオプションを設定します。
- [認証キー（Authentication Key）]：MD5 認証を使用する場合、キーの長さは 32 桁の 16 進数（16 バイト）である必要があります。SHA-1 認証を使用する場合、キーの長さは 40 桁の 16 進数（20 バイト）である必要があります。
- [認証キーを暗号化する（Encrypt Authentication Key）]：認証キーの暗号化を有効にします。
- [暗号化を含める（Include Encryption）]：暗号化を有効にします。
- [暗号化アルゴリズム（Encryption Algorithm）]：暗号化アルゴリズムのタイプ。サポートされる値は DES です。ヌルのエントリは暗号化されません。[暗号化を含める（Include Encryption）] を選択した場合、このオプションを設定します。

- [暗号化キー（Encryption Key）]：暗号キーを入力します。キーは 16 進数の文字列である必要があります。AES-256-CBC 認証を使用する場合、キーは 130 桁の 16 進数である必要があります。[暗号化を含める（Include Encryption）] を選択した場合、このオプションを設定します。
- [キーを暗号化する（Encrypt Key）]：キーを暗号化できるようにします。

**ステップ 8** [OK] をクリックして、認証設定を保存します。

**ステップ 9** [ネイバー（Neighbor）] を選択し、[追加（Add）] をクリックして、各 OSPFv3 プロセスについて次のオプションを設定します。

- [リンク ローカル アドレス（Link Local Address）]：スタティック ネイバーの IPv6 アドレス。
- [コスト（Cost）]：コストを有効にします。アドバタイズする場合は、[コスト（Cost）] フィールドにコストを入力し、[発信リンク ステートアドバタイズメントをフィルタ（Filter Outgoing Link State Advertisements）] をオンにします。
- （オプション）[ポーリング間隔（Poll Interval）]：ポーリング間隔を有効にします。[優先順位（Priority）] レベルと [ポーリング間隔（Poll Interval）]（秒単位）を入力します。

**ステップ 10** [追加（Add）] をクリックして、ネイバーを追加します。

**ステップ 11** [OK] をクリックして、インターフェイス設定を保存します。

# OSPFv3 詳細プロパティの設定

[高度なプロパティ（Advanced Properties）] を使用すると、syslog メッセージ生成、アドミニストレーティブ ルート ディスタンス、パッシブ OSPFv3 ルーティング、LSA タイマー、グレースフルリスタートなどのオプションを設定できます。

### グレースフル リスタート

Firewall Threat Defense デバイスでは、既知の障害状況が発生することがあります。これにより、スイッチングプラットフォーム全体でパケット転送に影響を与えることがあってはなりません。Non-Stop Forwarding（NSF）機能では、ルーティング プロトコル情報を復元している間に、既知のルートへのデータ転送が続行されます。この機能は、スケジュール済みヒットレス ソフトウェア アップグレードがあるときに便利です。グレースフル リスタート（RFC 5187）を使用して、OSPFv3 上でグレースフル リスタートを設定できます。

（注） NSF 機能は HA モードとクラスタリングでも役立ちます。

NSF グレースフル リスタート機能の設定には、機能の設定と NSF 対応または NSF 認識としてのデバイスの設定という 2 つのステップが伴います。NSF 対応デバイスは、ネイバー

に対して独自のリスタート アクティビティを示すことができ、NSF 認識デバイスはネイバーのリスタートをサポートすることができます。

デバイスは、いくつかの条件に応じて、NSF 対応または NSF 認識として設定できます。

- デバイスは、現在のデバイスのモードに関係なく、NSF 認識デバイスとして設定できます。
- デバイスを NSF 対応として設定するには、デバイスはフェールオーバーまたはスパンド EtherChannel（L2）クラスタ モードのいずれかである必要があります。
- デバイスを NSF 認識または NSF 対応にするには、必要に応じて opaque リンク ステート アドバタイズメント（LSA）/リンク ローカル シグナリング（LLS）ブロックの機能を使って設定する必要があります。

## 手順

**ステップ 1** [**Devices** > **Device Management**] を選択し、Firewall Threat Defense デバイスを編集します。

**ステップ 2** **[ルーティング（Routing）]** > **[OSPFv3]** > **[高度（Advanced）]** を選択します。

**ステップ 3** [ルータID（Router ID）] で、[自動（Automatic）] または [IPアドレス（IP Address）]（非クラスタおよびスパンド EtherChannel モードのクラスタの場合に表示）または [クラスタプール（Cluster Pool）]（個別インターフェイスモードのクラスタの場合に表示）を選択します。[IPアドレス（IP address）] を選択する場合は、[IPアドレス（IP Address）] フィールドに IPv6 アドレスを入力します。[クラスタプール（Cluster Pool）] を選択した場合は、[クラスタプール（Cluster Pool）] ドロップダウンフィールドで IPv6 クラスタプール値を選択します。クラスタプールアドレスの作成については、アドレス プールを参照してください。

**ステップ 4** ルートがサポートされていない LSA タイプ 6 Multicast OSPF（MOSPF）パケットを受信する場合に syslog メッセージを抑制するには、[LSA MOSPF を無視（Ignore LSA MOSPF）] チェックボックスをオンにします。

**ステップ 5** [一般（General）] を選択し、次のように設定します。

- [隣接関係の変更（Adjacency Changes）]：syslog メッセージが送信される隣接関係の変更内容を定義します。

  デフォルトでは、OSPF ネイバーがアップ状態またはダウン状態になったときに、syslog メッセージが生成されます。OSPF ネイバーがダウンしたときに syslog メッセージを送信するようルータを設定することも、状態ごとに syslog を送信するように設定することもできます。

  - [隣接関係の変更（Adjacency Changes）]：OSPF ネイバーが起動または停止したときに、Firewall Threat Defense デバイスによって syslog メッセージが送信されるようになります。この設定は、デフォルトでオンになっています。
  - [詳細を含める（Include Details）]：ネイバーがアップ状態またはダウン状態になったときだけでなく、状態の変更が発生したときにも Firewall Threat Defense デバイスによって syslog メッセージが送信されるようになります。デフォルトでは、この設定はオフになっています。

- [アドミニストレーティブ ルート ディスタンス（Administrative Route Distances）]：エリア間、エリア内、および外部 IPv6 ルートのアドミニストレーティブ ルート ディスタンスの設定に使用された設定を変更できます。アドミニストレーティブ ルート ディスタンスは 1 ～ 254 の整数です。デフォルトは 110 です。
- [デフォルト情報の発信（Default Information Originate）]：デフォルトの外部ルートを OSPFv3 ルーティング ドメインに生成するには、[有効化（Enable）] チェックボックスをオンにして、次のオプションを設定します。
  - [常にアドバタイズする（Always Advertise）]：デフォルト ルートが存在するかどうかにかかわらず、常にアドバタイズします。
  - [メトリック（Metric）]：デフォルト ルートを生成するために使用するメトリック。有効なメトリック値の範囲は、0 ～ 16777214 です。デフォルト値は 10 です。
  - [メトリック タイプ（Metric Type）]：OSPFv3 ルーティング ドメインにアドバタイズされるデフォルト ルートに関連付けられた外部リンク タイプ。有効な値は 1（タイプ 1 の外部ルート）および 2（タイプ 2 の外部ルート）です。デフォルトはタイプ 2 外部ルートです。
  - [ルートマップ（Route Map）]：ルートマップが満たされている場合にデフォルトルートを生成するルーティングプロセスを選択するか、**Add**（＋）をクリックして、新しいルーティングプロセスを追加します。新しいルート マップを追加するには、ルートマップを参照してください。

**ステップ 6** [OK] をクリックして、一般設定を保存します。

**ステップ 7** [パッシブインターフェイス（Passive Interfaces）] を選択して、[使用可能なインターフェイス（Available Interfaces）] リストからパッシブ OSPFv3 ルーティングを有効にするインターフェイスを選択し、[追加（Add）] をクリックして [選択したインターフェイス（Selected Interfaces）] リストにこれらを移動します。

パッシブ ルーティングは、OSPFv3 ルーティング情報のアドバタイズメントの制御に有効であり、インターフェイスでの OSPFv3 ルーティング更新の送受信を無効にします。

**ステップ 8** [OK] をクリックしてパッシブ インターフェイス設定を保存します。

**ステップ 9** [タイマー（Timer）] を選択し、次の LSA ペーシングと SPF 計算タイマーを設定します。

- [到着（Arrival）]：ネイバーから到着する同一 LSA の最短受信間隔をミリ秒単位で指定します。有効な範囲は 0 ～ 6000,000 ミリ秒です。デフォルトは 1000 ミリ秒です。
- [フラッド ペーシング（Flood Pacing）]：フラッディング キュー内の LSA が更新間にペーシング処理される時間を指定します（ミリ秒単位）。設定できる範囲は 5 ～ 100 ミリ秒です。デフォルト値は、33 ミリ秒です。
- [グループ ペーシング（Group Pacing）]：LSA をグループにまとめてリフレッシュ、チェックサム計算、エージングする間隔を秒単位で指定します。有効な値の範囲は 10 ～ 1800 です。デフォルト値は 240 です。

- [再送信ペーシング（Retransmission Pacing）]：再送信キュー内の LSA がペースされる時間をミリ秒単位で指定します。設定できる範囲は 5 ～ 200 ミリ秒です。デフォルト値は 66 ミリ秒です。
- [LSA スロットル（LSA Throttle）]：LSA の最初のオカレンスを生成する遅延を指定します（ミリ秒単位）。デフォルト値は、0 ミリ秒です。最小値は、同じ LSA を送信する最小遅延をミリ秒単位で指定します。デフォルト値は、5000 ミリ秒です。最大値は、同じ LSA を送信する最大遅延をミリ秒単位で指定します。デフォルト値は、5000 ミリ秒です。

  （注）
  LSA スロットリングでは、最小時間または最大時間が最初のオカレンスの値よりも小さい場合、OSPFv3 が自動的に最初のオカレンス値に修正します。同様に、指定された最遅延が最小遅延よりも小さい場合、OSPFv3 が自動的に最小遅延値に修正します。

- [SPF スロットル（SPF Throttle）]：SPF 計算の変更を受信する遅延をミリ秒単位で指定します。デフォルト値は、5000 ミリ秒です。最小値は、最初と 2 番目の SPF 計算の間の遅延をミリ秒単位で指定します。デフォルト値は、10000 ミリ秒です。最大値は、SPF 計算の最大待機時間をミリ秒単位で指定します。デフォルト値は、10000 ミリ秒です。

  （注）
  SPF スロットリングでは、最小時間または最大時間が最初のオカレンスの値よりも小さい場合、OSPFv3 が自動的に最初のオカレンス値に修正します。同様に、指定された最遅延が最小遅延よりも小さい場合、OSPFv3 が自動的に最小遅延値に修正します。

**ステップ 10** [OK] をクリックして LSA タイマー設定を保存します。

**ステップ 11** [ノンストップフォワーディング（Non Stop Forwarding）] を選択し、[グレースフルリスタートヘルパーを有効にする（Enable graceful-restart helper）] 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は、デフォルトではオンになっています。NSF 認識デバイスでグレースフル リスタート ヘルパー モードを無効にするには、このチェックボックスをオフにします。

**ステップ 12** [リンク ステート アドバタイズメントを有効にする（Enable link state advertisement）] チェックボックスをオンにして、厳密なリンク ステート アドバタイズメント チェックを有効にします。

有効にすると、再起動ルータにフラッディングされる可能性がある LSA への変更があることが検出された場合、またはグレースフル リスタート プロセスが開始されたときに再起動ルータの再送リスト内に変更された LSA があると検出された場合、ヘルパー ルータはルータの再起動プロセスを終了させることを示します。

**ステップ 13** [グレースフル リスタートを有効にする（スパンド クラスタまたはフェールオーバーが設定されている場合に使用）（Enable graceful-restart (Use when Spanned Cluster or Failover Configured)）] をオンにして、グレースフル リスタート間隔を秒単位で入力します。範囲は 1 ～ 1800 です。デフォルト値は 120 秒です。30 秒未満の再起動間隔では、グレースフル リスタートが中断します。

**ステップ 14** [OK] をクリックしてグレースフル リスタート設定を保存します。

**ステップ 15** [ルーティング（Routing）] ページで [保存（Save）] をクリックして変更を保存します。

# OSPF の履歴

表 *1 : OSPF* の機能履歴

| 機能 | Minimum Firewall Management Center | Minimum Firewall Threat Defense | 詳細 |
|---|---|---|---|
| OSPF v2 および v3 に対する BFD サポート | 7.4 | 7.4 | OSPFv2 および OSPFv3 インターフェイスで BFD を有効にできます。<br>新規/変更された画面：<br>• **[設定（Configuration）] > [デバイスセットアップ（Device Setup）] > [ルーティング（Routing）] > [OSPFv2]**<br>• **[設定（Configuration）] > [デバイスセットアップ（Device Setup）] > [ルーティング（Routing）] > [OSPFv3]** |

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。