CHAPTER 54

Configuring Routing Policies on Firewall Devices

The Routing section in Security Manager contains pages for defining and managing routing settings for security appliances.

This chapter contains the following topics:

Configuring No Proxy ARP

When a host sends IP traffic to another device on the same Ethernet network, the host needs to know the MAC address of the device. Address Resolution Protocol (ARP) is a Layer 2 protocol that resolves an IP address to a MAC address: a host sends an ARP request asking "Who is this IP address?" The device owning the IP address replies, "I own that IP address; here is my MAC address."

With Proxy ARP, a device responds to an ARP request with its own MAC address, even though the device does not own the IP address. Serving as an ARP Proxy for another host effectively directs network traffic to the proxy, in this case your security appliance. Traffic that passes through the appliance is then routed to the appropriate destination.

For example, the security appliance uses proxy ARP when you configure NAT and specify a global address that is on the same network as the appliance interface. The only way traffic can reach the destination hosts is if the appliance claims and subsequently routes traffic to the destination global addresses.

By default, proxy ARP is enabled for all interfaces. Use the No Proxy ARP page to disable proxy ARP for global addresses:

- To disable proxy ARP for one or more interfaces, enter their names in the Interfaces field. Separate multiple interfaces with commas. You can click Select to choose the interfaces from a list of interfaces defined on the device, and interface roles defined in Security Manager.

Note On ASA 8.4.2 and later devices operating in routed mode, you can disable Proxy ARP on the egress interface for a Manual NAT rule. See Do not proxy ARP on Destination Interface for more information.

Navigation Path

- (Device view) Select **Platform > Routing > No Proxy ARP** from the Device Policy selector.
- (Policy view) Select **PIX/ASA/FWSM Platform > Routing > No Proxy ARP** from the Policy Type selector. Select an existing policy from the Shared Policy selector, or create a new one.

Related Topics

- Configuring Static Routes, page 54-48
- Configuring RIP, page 54-40
- Configuring OSPF, page 54-2

Configuring OSPF

The OSPF page provides nine tabbed panels for configuring OSPF (Open Shortest Path First) routing on a firewall device. The following topics provide detailed information about enabling and configuring OSPF:

- About OSPF, page 54-2
- General Tab, page 54-3
- Area Tab, page 54-6
- Range Tab, page 54-8
- Neighbors Tab, page 54-10
- Redistribution Tab, page 54-11
- Virtual Link Tab, page 54-13
- Filtering Tab, page 54-15
- Summary Address Tab, page 54-17
- Interface Tab, page 54-18

Navigation Path

- (Device view) Select **Platform > Routing > OSPF** from the Device Policy selector.
- (Policy view) Select **PIX/ASA/FWSM Platform > Routing > OSPF** from the Policy Type selector. Select an existing policy from the Shared Policy selector, or create a new one.

About OSPF

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

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

If NAT is used when OSPF is operating on public and private areas, and if address filtering is required, 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 security appliance acting as an ABR. Type 3 LSAs (inter-area routes) can be filtered from one area to other. This lets you use NAT and OSPF together without advertising private networks.

Note Only type 3 LSAs can be filtered. If you configure the security appliance as an ASBR in a private network, it will send type 5 LSAs describing private networks, which will be broadcast to the entire autonomous system (AS) including public areas.

If NAT is employed but OSPF is only running in public areas, 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 security appliance. Also, you should not mix public and private networks on the same security appliance interface.

Related Topics

- Configuring OSPF, page 54-2

General Tab

Use the General panel on the OSPF page to enable up to two OSPF process instances. Each OSPF process has its own associated areas and networks.

Note You cannot enable OSPF if you have RIP enabled.

Navigation Path

You can access the General panel from the OSPF Page; see Configuring OSPF, page 54-2 for more information.

Related Topics

- Area Tab, page 54-6
- Range Tab, page 54-8
- Neighbors Tab, page 54-10
- Redistribution Tab, page 54-11
- Virtual Link Tab, page 54-13
- Filtering Tab, page 54-15
- Summary Address Tab, page 54-17
- Interface Tab, page 54-18

Field Reference

Table 54-1 OSPF General Tab

Element	Description
The General tab provides two identical sections; each is used to enable one OSPF process. The following options are available in each section.	
Enable this OSPF Process	Check this box to enable an OSPF process. You cannot enable an OSPF process if you have RIP enabled on the security appliance. Deselect this option to remove the OSPF process.
OSPF Process ID	Enter a unique numeric identifier for the OSPF process. This process ID is used internally and does not need to match the OSPF process ID on any other OSPF devices. Valid values are from 1 to 65535.
Advanced button	Opens the OSPF Advanced Dialog Box, page 54-4, in which you can configure additional process-related parameters, such Router ID, Adjacency Changes, Administrative Route Distances, Timers, and Default Information Originate settings.

OSPF Advanced Dialog Box

Use the OSPF Advanced dialog box to configure settings such as the Router ID, Adjacency Changes, Administrative Route Distances, Timers, and Default Information Originate settings for an OSPF process.

Navigation Path

You can access the OSPF Advanced dialog box from the General Tab, page 54-3.

Related Topics

- Configuring OSPF, page 54-2

Field Reference

Table 54-2 OSPF Advanced Dialog Box

Element	Description
OSPF Process	Displays the ID of the OSPF process you are configuring. You cannot change this value in this dialog box.
Router ID	To use a fixed router ID, enter a router ID in IP address format in the Router ID field. If you leave this value blank, the highest-level IP address on the security appliance is used as the router ID.
Ignore LSA MOSPF	Select this option to suppress transmission of syslog messages when the security appliance receives Type 6 (MOSPF) LSA packets.
RFC 1583 Compatible	Select this option to calculate summary route costs per RFC 1583. Deselect this option to calculate summary route costs per RFC 2328. To minimize the chance of routing loops, all OSPF devices in an OSPF routing domain should have RFC compatibility set identically. This option is selected by default.

Table 54-2 OSPF Advanced Dialog Box (Continued)

Element	Description
Adjacency Changes	These options specify the syslog messages sent when adjacency changes occur. • Log Adjacency Changes – When selected, the security appliance sends a syslog message whenever an OSPF neighbor goes up or down. This option is selected by default. • Log Adjacency Changes Detail – When selected, the security appliance sends a syslog message whenever any state change occurs, not just when a neighbor goes up or down. This option is not selected by default.
Administrative Route Distances	Settings for the administrative route distances, according to the route type. • Inter Area – The administrative distance for all routes from one area to another. Valid values range from 1 to 255; the default value is 110. • Intra Area – The administrative distance for all routes within an area. Valid values range from 1 to 255; the default value is 110. • External – The administrative distance for all routes from other routing domains that are learned through redistribution. Valid values range from 1 to 255; the default value is 110.
Timers (in seconds)	Settings used to configure LSA pacing and SPF calculation timers. • SPF Delay – The time between receipt of a topology change and the start of shortest path first (SPF) calculations. Valid values range from 0 to 65535; the default value is 5 seconds. • SPF Hold – The hold time between consecutive SPF calculations. Valid values range from 1 to 65534; the default value is 10 seconds. • LSA Group Pacing – The interval at which LSAs are collected into a group and refreshed, checksummed, or aged. Valid values range from 10 to 1800; the default value is 240 seconds.

Table 54-2 OSPF Advanced Dialog Box (Continued)

Element	Description
Default Information Originate	Settings used by an ASBR to generate a default external route into an OSPF routing domain. • Enable Default Information Originate – Check this box to enable generation of a default route into the OSPF routing domain; the following options become available: – Always advertise the default route – Check this box to always advertise the default route. – Metric Value – Enter the OSPF metric for the default route. Valid values range from 0 to 16777214; the default value is 1. – Metric Type – Choose the external link type associated with the default route advertised into the OSPF routing domain. The choices are **1** or **2**, indicating a Type 1 or a Type 2 external route. The default value is 2. – Route Map – (Optional) The name of a route map to apply. The routing process generates the default route if the route map is satisfied. **Note** This field contains only the Route Map name. The Route Map is created and contained within a FlexConfig; see Chapter 7, "Managing FlexConfigs" for more information.

Area Tab

Use the Area tab on the OSPF page to configure OSPF areas and networks.

Navigation Path

You can access the Area tab from the OSPF page. For more information about the OSPF page, see Configuring OSPF, page 54-2.

Related Topics

- Add/Edit Area/Area Networks Dialog Box, page 54-7
- Configuring OSPF, page 54-2
- General Tab, page 54-3
- Range Tab, page 54-8
- Neighbors Tab, page 54-10
- Redistribution Tab, page 54-11
- Virtual Link Tab, page 54-13
- Filtering Tab, page 54-15
- Summary Address Tab, page 54-17
- Interface Tab, page 54-18

Field Reference

Table 54-3 Area Tab

Element	Description
OSPF Process	The OSPF process the area applies to.
Area ID	The area ID.
Area Type	The area type (Normal, Stub, or NSSA).
Networks	The area networks.
Options	The options, if any, set for the area type.
Authentication	The type of authentication set for the area (None, Password, or MD5).
Cost	The default cost for the area.

Add/Edit Area/Area Networks Dialog Box

Use the Add/Edit Area/Area Networks dialog box to define area parameters, the networks contained by the area, and the OSPF process associated with the area.

Navigation Path

You can access the Add/Edit Area/Area Networks dialog box from the Area Tab, page 54-6.

Related Topics

- Configuring OSPF, page 54-2

Field Reference

Table 54-4 Add/Edit Area/Area Networks Dialog Box

Element	Description
OSPF Process	When adding a new area, choose the OSPF process ID for the OSPF process for which the area is being added. If there is only one OSPF process enabled on the security appliance, that process is selected by default. When editing an existing area, you cannot change the OSPF process ID.
Area ID	When adding a new area, enter the area ID. You can specify the area ID as either a decimal number or an IP address. Valid decimal values range from 0 to 4294967295. You cannot change the area ID when editing an existing area.
Area Type	
Normal	Choose this option to make the area a standard OSPF area. This option is selected by default when you first create an area.
Stub	Choosing this option makes the area a stub area. Stub areas do not have any routers or areas beyond it. Stub areas prevent AS External LSAs (Type 5 LSAs) from being flooded into the stub area. When you create a stub area, you can prevent summary LSAs (Type 3 and 4) from being flooded into the area by deselecting the Summary check box.

Table 54-4 Add/Edit Area/Area Networks Dialog Box (Continued)

Element	Description
Summary (allows sending LSAs into the stub area)	When the area being defined is a stub area, deselecting this check box prevents LSAs from being sent into the stub area. This check box is selected by default for stub areas.
NSSA	Choose this option to make the area a not-so-stubby area. NSSAs accept Type 7 LSAs. When you create a NSSA, you can prevent summary LSAs from being flooded into the area by deselecting the Summary check box. You can also disable route redistribution by deselecting the Redistribute check box and enabling Default Information Originate.
Redistribute (imports routes to normal and NSSA areas)	Deselect this check box to prevent routes from being imported into the NSSA. This check box is selected by default.
Summary (allows sending LSAs into the NSSA area)	When the area being defined is a NSSA, deselecting this check box prevents LSAs from being sent into the stub area. This check box is selected by default for NSSAs.
Default Information Originate (generate a Type 7 default)	Select this check box to generate a Type 7 default into the NSSA. This check box is deselected by default.
Metric Value	Specifies the OSPF metric value for the default route. Valid values range from 0 to 16777214. The default value is 1.
Metric Type	The OSPF metric type for the default route. The choices are 1 (Type 1) or 2 (Type 2). The default value is 2.
Network	The IP address and network mask of the network or host to be added to the area. Use 0.0.0.0 with a netmask of 0.0.0.0 to create the default area. You can only use 0.0.0.0 in one area. **Tip** You can click **Select** to select the interfaces from a list of interface objects.
Authentication	Contains the settings for OSPF area authentication. • None—Choose this option to disable OSPF area authentication. This is the default setting. • Password—Choose this option to use a clear text password for area authentication. This option is not recommended where security is a concern. • MD5—Choose this option to use MD5 authentication.
Default Cost	Specify a default cost for the area. Valid values range from 0 to 65535. The default value is 1.

Range Tab

Use the Range tab to summarize routes between areas.

Navigation Path

You can access the Range tab from the OSPF page. For more information about the OSPF page, see Configuring OSPF, page 54-2.

Related Topics

- Add/Edit Area Range Network Dialog Box, page 54-9

Field Reference

Table 54-5 Range Tab

Element	Description
Process ID	The ID of the OSPF process associated with the route summary.
Area ID	The ID of the area associated with the route summary.
Network	The summary IP address and network mask.
Advertise	Displays “true” if the route summaries are advertised when they match the address/mask pair or “false” if the route summaries are suppressed when they match the address/mask pair.

Add/Edit Area Range Network Dialog Box

Use the Add/Edit Area Range Network dialog box to add a new entry to the Route Summarization table or to change an existing entry.

Navigation Path

You can access the Add/Edit Area Range Network dialog box from the Range Tab, page 54-8.

Related Topics

- Configuring OSPF, page 54-2

Field Reference

Table 54-6 Add/Edit Area Range Network Dialog Box

Element	Description
OSPF Process	Select the OSPF process to which the route summary applies. You cannot change this value when editing an existing route summary entry.
Area	Select the area ID of the area to which the route summary applies. You cannot change this value when editing an existing route summary entry.
Network	The IP address and mask of the network for the routes being summarized. **Tip** You can click **Select** to select the networks from a list of network objects.
Advertise	Select this check box to set the address range status to “advertise”. This causes Type 3 summary LSAs to be generated. Deselect this check box to suppress the Type 3 summary LSA for the specified networks.

Neighbors Tab

Use the Neighbors tab to define static neighbors. You need to define a static neighbor for each point-to-point, non-broadcast interface. You also need to define a static route for each static neighbor in the Neighbors table.

Navigation Path

You can access the Neighbors tab from the OSPF page. For more information about the OSPF page, see Configuring OSPF, page 54-2.

Related Topics

- Add/Edit Static Neighbor Dialog Box, page 54-10

Field Reference

Table 54-7 Neighbors Tab

Element	Description
OSPF Process	The OSPF process associated with the static neighbor.
Neighbor	The IP address of the static neighbor.
Interface	The interface associated with the static neighbor.

Add/Edit Static Neighbor Dialog Box

Use the Add/Edit Static Neighbor dialog box to define a static neighbor or change information for an existing static neighbor. You must define a static neighbor for each point-to-point, non-broadcast interface.

Navigation Path

You can access the Add/Edit Static Neighbor dialog box from the Neighbors Tab, page 54-10.

Related Topics

- Configuring OSPF, page 54-2

Field Reference

Table 54-8 Add/Edit Static Neighbor Dialog Box

Element	Description
OSPF Process	The OSPF process associated with the static neighbor.
Neighbor	The IP address of the static neighbor. **Tip** You can click **Select** to select the neighbor from a list of host objects.
Interface	The interface associated with the static neighbor. **Tip** You can click **Select** to select the interface from a list of interface objects.

Redistribution Tab

Use the Redistribution tab to define the rules for redistributing routes from one routing domain to another.

Navigation Path

You can access the Redistribution tab from the OSPF page. For more information about the OSPF page, see Configuring OSPF, page 54-2.

Related Topics

- Redistribution Dialog Box, page 54-11

Field Reference

Table 54-9 Redistribution Tab

Element	Description
OSPF Process	The OSPF process associated with the route redistribution entry.
Route Type	The source protocol the routes are being redistributed from. Valid entries are the following: • Static—The route is a static route. • Connected—The route was established automatically by virtue of having IP enabled on the interface. • OSPF—The route is an OSPF route from another process.
Match	The conditions used for redistributing routes from one routing protocol to another.
Subnets	Displays “true” if subnetted routes are redistributed. Does not display anything if only routes that are not subnetted are redistributed.
Metric Value	The metric that is used for the route. This column is blank for redistribution entries if the default metric is used.
Metric Type	Displays “1” if the metric is a Type 1 external route, “2” if the metric is Type 2 external route.
Tag Value	A 32-bit decimal value attached to each external route. This value is not used by OSPF itself. It may be used to communicate information between ASBRs. Valid values range from 0 to 4294967295.
Route Map	The name of the route map to apply to the redistribution entry.

Redistribution Dialog Box

Use the Redistribution dialog box to add a redistribution rule or to edit an existing redistribution rule in the Redistribution table.

Navigation Path

You can access the Redistribution dialog box from the Redistribution Tab, page 54-11.

Related Topics

- Configuring OSPF, page 54-2

Field Reference

Table 54-10 OSPF Redistribution Settings Dialog Box

Element	Description
OSPF Process	Select the OSPF process associated with the route redistribution entry.
Route Type	Select the source protocol from which the routes are being redistributed. You can choose one of the following options: • Static—The route is a static route. • Connected—The route was established automatically by virtue of having IP enabled on the interface. • OSPF—The route is an OSPF route from another process.
Match	The conditions used for redistributing routes from one routing protocol to another. The routes must match the selected condition to be redistributed. You can choose one or more of the following match conditions: • Internal—The route is internal to a specific AS. • External 1—Routes that are external to the autonomous system, but are imported into OSPF as Type 1 external routes. • External 2—Routes that are external to the autonomous system, but are imported into OSPF as Type 2 external routes. • NSSA External 1—Routes that are external to the autonomous system, but are imported into OSPF as Type 2 NSSA routes. • NSSA External 2—Routes that are external to the autonomous system, but are imported into OSPF as Type 2 NSSA routes.
Metric Value	The metric value for the routes being redistributed. Valid values range from 1 to 16777214. When redistributing from one OSPF process to another OSPF process on the same device, the metric will be carried through from one process to the other if no metric value is specified. When redistributing other processes to an OSPF process, the default metric is 20 when no metric value is specified.
Metric Type	Select “1” if the metric is a Type 1 external route, “2” if the metric is a Type 2 external route.
Tag Value	The tag value is a 32-bit decimal value attached to each external route. This is not used by OSPF itself. It may be used to communicate information between ASBRs. Valid values range from 0 to 4294967295.
Use Subnets	When selected, redistribution of subnetted routes is enabled. Deselect this check box to cause only routes that are not subnetted to be redistributed.
Route Map	The name of the route map to apply to the redistribution entry.

Virtual Link Tab

Use the Virtual Link tab to create virtual links. If you add an area to an OSPF network, and it is not possible to connect the area directly to the backbone area, you need to create a virtual link. A virtual link connects two OSPF devices that have a common area, called the transit area. One of the OSPF devices must be connected to the backbone area.

Navigation Path

You can access the Virtual Link tab from the OSPF page. For more information about the OSPF page, see Configuring OSPF, page 54-2.

Related Topics

- Add/Edit OSPF Virtual Link Configuration Dialog Box, page 54-13

Field Reference

Table 54-11 Virtual Link Tab

Element	Description
OSPF Process	The OSPF process associated with the virtual link.
Area ID	The ID of the transit area.
Peer Router	The IP address of the virtual link neighbor.
Authentication	Displays the type of authentication used by the virtual link: • None—No authentication is used. • Password—Clear text password authentication is used. • MD5—MD5 authentication is used.

Add/Edit OSPF Virtual Link Configuration Dialog Box

Use the Add/Edit OSPF Virtual Link Configuration dialog box to define virtual links or change the properties of existing virtual links.

Navigation Path

You can access the Add/Edit OSPF Virtual Link Configuration dialog box from the Virtual Link Tab, page 54-13.

Related Topics

- Add/Edit OSPF Virtual Link MD5 Configuration Dialog Box, page 54-15
- Configuring OSPF, page 54-2

Field Reference

Table 54-12 Add/Edit OSPF Virtual Link Configuration Dialog Box

Element	Description
OSPF Process	Select the OSPF process associated with the virtual link.

Table 54-12 Add/Edit OSPF Virtual Link Configuration Dialog Box (Continued)

Element	Description
Area ID	Select the area shared by the neighbor OSPF devices. The selected area cannot be an NSSA or a stub area.
Peer Router	Enter the IP address of the virtual link neighbor.
Hello Interval	The interval, in seconds, between hello packets sent on an interface. The smaller the hello interval, the faster topological changes are detected but the more traffic is sent on the interface. This value must be the same for all routers and access servers on a specific interface. Valid values range from 1 to 65535 seconds. The default value is 10 seconds.
Retransmit Interval	The time, in seconds, between LSA retransmissions for adjacencies belonging to the interface. When a router sends an LSA to its neighbor, it keeps the LSA until it receives the acknowledgement message. If the router receives no acknowledgement, it will resend the LSA. Be conservative when setting this value, or needless retransmission can result. The value should be larger for serial lines and virtual links. Valid values range from 1 to 65535 seconds. The default value is 5 seconds.
Transmit Delay	The estimated time, in seconds, required to send an LSA packet on the interface. LSAs in the update packet have their ages increased by the amount specified by this field before transmission. If the delay is not added before transmission over a link, the time in which the LSA propagates over the link is not considered. The value assigned should take into account the transmission and propagation delays for the interface. This setting has more significance on very low-speed links. Valid values range from 1 to 65535 seconds. The default value is 1 second.
Dead Interval	The interval, in seconds, in which no hello packets are received, causing neighbors to declare a router down. Valid values range from 1 to 65535. The default value of this field is four times the interval set by the Hello Interval field.
Authentication	Contains the OSPF authentication options. • None—Choose this option to disable OSPF authentication. • Password—Choose this option to use clear text password authentication. This is not recommended where security is a concern. • MD5—Choose this option to use MD5 authentication (recommended).
Authentication Password	Contains the settings for entering the password when password authentication is enabled. • Password—Enter a text string of up to 8 characters. • Confirm—Re-enter the password.

Table 54-12 Add/Edit OSPF Virtual Link Configuration Dialog Box (Continued)

Element	Description
MD5 IDs and Keys	Contains the settings for entering the MD5 keys and parameters when MD5 authentication is enabled. All devices on the interface using OSPF authentication must use the same MD5 key and ID. • MD5 Key ID and MD5 Key Table – MD5 Key ID—A numerical key identifier. Valid values range from 1 to 255. – MD5 Key—An alphanumeric character string of up to 16 bytes.

Add/Edit OSPF Virtual Link MD5 Configuration Dialog Box

Use the Add/Edit OSPF Virtual Link MD5 Configuration dialog box to define MD5 keys for authentication of virtual links.

Navigation Path

You can access the Add/Edit OSPF Virtual Link MD5 Configuration dialog box from the Add/Edit OSPF Virtual Link Configuration Dialog Box, page 54-13.

Related Topics

- Add/Edit OSPF Virtual Link Configuration Dialog Box, page 54-13
- Virtual Link Tab, page 54-13
- Configuring OSPF, page 54-2

Field Reference

Table 54-13 Add/Edit OSPF Virtual Link MD5 Configuration Dialog Box

Element	Description
MD5 Key ID	A numerical key identifier. Valid values range from 1 to 255.
MD5 Key	An alphanumeric character string of up to 16 bytes.
Confirm	Re-enter the MD5 key.

Filtering Tab

Use the Filtering tab to configure the ABR Type 3 LSA filters for each OSPF process. ABR Type 3 LSA filters allow only specified prefixes to be sent from one area to another area and restricts all other prefixes. This type of area filtering can be applied out of a specific OSPF area, into a specific OSPF area, or into and out of the same OSPF areas at the same time.

Benefits

OSPF ABR Type 3 LSA filtering improves your control of route distribution between OSPF areas.

Restrictions

Only type-3 LSAs that originate from an ABR are filtered.

Navigation Path

You can access the Filtering tab from the OSPF page. For more information about the OSPF page, see Configuring OSPF, page 54-2.

Related Topics

- Add/Edit Filtering Dialog Box, page 54-16

Field Reference

Table 54-14 Filtering Tab

Element	Description
OSPF Process	The OSPF process associated with the filter entry.
Area ID	The ID of the area associated with the filter entry.
Prefix List Name	The name of the prefix list.
Filtered Network	The IP address and mask of the network being filtered.
Traffic Direction	Displays “Inbound” if the filter entry applies to LSAs coming in to an OSPF area or “Outbound” if it applies to LSAs going out of an OSPF area.
Sequence #	The sequence number for the filter entry. When multiple filters apply to an LSA, the filter with the lowest sequence number is used.
Action	Displays “Permit” if LSAs matching the filter are allowed or “Deny” if LSAs matching the filter are denied.
Lower Range	The minimum prefix length to be matched.
Upper Range	The maximum prefix length to be matched.

Add/Edit Filtering Dialog Box

Use the Add/Edit Filtering dialog box to add new filters to the Filter table or to modify an existing filter.

Navigation Path

You can access the Add/Edit Filtering dialog box from the Filtering Tab, page 54-15.

Related Topics

- Configuring OSPF, page 54-2

Field Reference

Table 54-15 Add/Edit Filtering Dialog Box

Element	Description
OSPF Process	Select the OSPF process associated with the filter entry.
Area ID	Select the ID of the area associated with the filter entry.
Prefix List Name	Enter the prefix name.
Filtered Network	Enter the IP address and mask of the network being filtered.

Table 54-15 Add/Edit Filtering Dialog Box (Continued)

Element	Description
Traffic Direction	Select the traffic direction to filter. Choose “Inbound” to filter LSAs coming into an OSPF area or “Outbound” to filter LSAs going out of an OSPF area.
Sequence Number	Enter a sequence number for the filter. Valid values range from 1 to 4294967294. When multiple filters apply to an LSA, the filter with the lowest sequence number is used.
Action	Select “Permit” to allow the LSA traffic or “Deny” to block the LSA traffic.
Lower Range	Specify the minimum prefix length to be matched. The value of this setting must be greater than the length of the network mask entered in the Filtered Network field and less than or equal to the value, if present, entered in the Upper Range field.
Upper Range	Enter the maximum prefix length to be matched. The value of this setting must be greater than or equal to the value, if present, entered in the Lower Range field, or, if the Lower Range field is left blank, greater than the length of the network mask length entered in the Filtered Network field.

Summary Address Tab

Use the Summary Address tab to configure summary addresses for each OSPF routing process.

Routes learned from other routing protocols can be summarized. The metric used to advertise the summary is the smallest metric of all the more specific routes. Summary routes help reduce the size of the routing table.

Using summary routes for OSPF causes an OSPF ASBR to advertise one external route as an aggregate for all redistributed routes that are covered by the address. Only routes from other routing protocols that are being redistributed into OSPF can be summarized.

Navigation Path

You can access the Summary Address tab from the OSPF page. For more information about the OSPF page, see Configuring OSPF, page 54-2.

Related Topics

- Table 54-17 on page 54-18

Field Reference

Table 54-16 Summary Address Tab

Element	Description
OSPF Process	The OSPF process associated with the summary address.
Network	The IP address and network mask of the summary address.

Table 54-16 Summary Address Tab (Continued)

Element	Description
Tag	A 32-bit decimal value attached to each external route. This value is not used by OSPF itself. It may be used to communicate information between ASBRs.
Advertise	Displays “true” if the summary routes are advertised. Displays “false” if the summary route is not advertised.

Add/Edit Summary Address Dialog Box

Use the Add/Edit Summary Address dialog box to add new entries or to modify existing entries in the Summary Address table.

Navigation Path

You can access the Add/Edit Summary Address dialog box from the Summary Address Tab, page 54-17.

Related Topics

- Configuring OSPF, page 54-2

Field Reference

Table 54-17 Add/Edit Summary Address Dialog Box

Element	Description
OSPF Process	Choose the OSPF process associated with the summary address. You cannot change this information when editing an existing entry.
Network	The IP address and network mask of the summary address.
Tag	The tag value is a 32-bit decimal value attached to each external route. This is not used by OSPF itself. It may be used to communicate information between ASBRs. Valid values range from 0 to 4294967295.
Advertise	When selected, summary routes are advertised. Deselect this check box to suppress routes that fall under the summary address. By default, this check box is selected.

Interface Tab

Use the Interface tab to configure interface-specific OSPF authentication routing properties.

Navigation Path

You can access the Interface tab from the OSPF page. For more information about the OSPF page, see Configuring OSPF, page 54-2.

Related Topics

- Table 54-19 on page 54-20

Field Reference

Table 54-18 Interface Tab

Element	Description
Interface	The name of the interface to which the configuration applies.
Authentication	The type of OSPF authentication enabled on the interface. The authentication type can be one of the following values: • None—OSPF authentication is disabled. • Password—Clear text password authentication is enabled. • MD5—MD5 authentication is enabled. • Area—The authentication type specified for the area is enabled on the interface. Area authentication is the default value for interfaces. However, area authentication is disabled by default. So, unless you previously specified an area authentication type, interfaces showing Area authentication have authentication disabled.
Point-to-Point	Displays “true” if the interface is set to non-broadcast (point-to-point). Displays “false” if the interface is set to broadcast.
Cost	The cost of sending a packet through the interface.
Priority	The OSPF priority assigned to the interface.
MTU Ignore	Displays “false” if MTU mismatch detection is enabled. Displays “true” if the MTU mismatch detection is disabled.
Database Filter	Displays “true” if outgoing LSAs are filtered during synchronization and flooding. Displays “false” if filtering is not enabled.
Hello Interval	The interval, in seconds, between hello packets sent on an interface. The smaller the hello interval, the faster topological changes are detected but the more traffic is sent on the interface. This value must be the same for all routers and access servers on a specific interface. Valid values range from 1 to 65535 seconds. The default value is 10 seconds.
Transmit Delay	The estimated time, in seconds, required to send an LSA packet on the interface. LSAs in the update packet have their ages increased by the amount specified by this field before transmission. If the delay is not added before transmission over a link, the time in which the LSA propagates over the link is not considered. The value assigned should take into account the transmission and propagation delays for the interface. This setting has more significance on very low-speed links. Valid values range from 1 to 65535 seconds. The default value is 1 second.
Retransmit Interval	The time, in seconds, between LSA retransmissions for adjacencies belonging to the interface. When a router sends an LSA to its neighbor, it keeps the LSA until it receives the acknowledgement message. If the router receives no acknowledgement, it resends the LSA. Be conservative when setting this value, or needless retransmission can result. The value should be larger for serial lines and virtual links. Valid values range from 1 to 65535 seconds. The default value is 5 seconds.

Table 54-18 Interface Tab (Continued)

Element	Description
Dead Interval	The interval, in seconds, in which no hello packets are received, causing neighbors to declare a router down. Valid values range from 1 to 65535. The default value of this setting is four times the interval set by the Hello Interval field.

Add/Edit Interface Dialog Box

Use the Add/Edit Interface dialog box to add OSPF authentication routing properties for an interface or to change an existing entry.

Navigation Path

You can access the Add/Edit Interface dialog box from the Interface Tab, page 54-18.

Related Topics

- Configuring OSPF, page 54-2

Field Reference

Table 54-19 Add/Edit Interface Dialog Box

Element	Description
Interface	The name of the interface to which the configuration applies.
Authentication	The type of OSPF authentication enabled on the interface. The authentication type can be one of the following values: • No Authentication—OSPF authentication is disabled. • Area Authentication—The authentication type specified for the area is enabled on the interface. Area authentication is the default value for interfaces. However, area authentication is disabled by default. So, unless you previously specified an area authentication type, interfaces showing Area authentication have authentication disabled. • Password Authentication—Clear text password authentication is enabled. • MD5 Authentication—MD5 authentication is enabled.
Authentication Password	Contains the settings for entering the password when password authentication is enabled. • Enter Password—Enter a text string of up to 8 characters. • Confirm—Re-enter the password.

Table 54-19 Add/Edit Interface Dialog Box (Continued)

Element	Description
MD5 Key IDs and Keys	Contains the settings for entering the MD5 keys and parameters when MD5 authentication is enabled. All devices on the interface using OSPF authentication must use the same MD5 key and ID. • Key ID—Enter a numerical key identifier. Valid values range from 1 to 255. • Key—An alphanumeric character string of up to 16 bytes. • Confirm—Re-enter the MD5 key.
Cost	The cost of sending a packet through the interface.
Priority	The OSPF priority assigned to the interface.
MTU Ignore	When selected, MTU mismatch detection is disabled. Deselect this check box to enable MTU mismatch detection.
Database Filter All Out	When selected, outgoing LSAs are filtered during synchronization and flooding. Deselect this check box to disable filtering.
Hello Interval (sec)	The interval, in seconds, between hello packets sent on an interface. The smaller the hello interval, the faster topological changes are detected but the more traffic is sent on the interface. This value must be the same for all routers and access servers on a specific interface. Valid values range from 1 to 65535 seconds. The default value is 10 seconds.
Transmit Delay (sec)	The estimated time, in seconds, required to send an LSA packet on the interface. LSAs in the update packet have their ages increased by the amount specified by this field before transmission. If the delay is not added before transmission over a link, the time in which the LSA propagates over the link is not considered. The value assigned should take into account the transmission and propagation delays for the interface. This setting has more significance on very low-speed links. Valid values range from 1 to 65535 seconds. The default value is 1 second.
Retransmit Interval (sec)	The time, in seconds, between LSA retransmissions for adjacencies belonging to the interface. When a router sends an LSA to its neighbor, it keeps the LSA until it receives the acknowledgment message. If the router receives no acknowledgment, it will resend the LSA. Be conservative when setting this value, or needless retransmission can result. The value should be larger for serial lines and virtual links. Valid values range from 1 to 65535 seconds. The default value is 5 seconds.
Dead Interval (sec)	The interval, in seconds, in which no hello packets are received, causing neighbors to declare a router down. Valid values range from 1 to 65535. The default value of this setting is four times the interval set by the Hello Interval field.
Point-to-Point	Displays “true” if the interface is set to non-broadcast (point-to-point). Displays “false” if the interface is set to broadcast.

Configuring OSPFv3

The OSPFv3 page provides two tabbed panels for configuring OSPF (Open Shortest Path First) version 3 routing on a firewall device.

Navigation Path

- (Device view) Select **Platform > Routing > OSPFv3** from the Device Policy selector.
- (Policy view) Select **PIX/ASA/FWSM Platform > Routing > OSPFv3** from the Policy Type selector. Select an existing policy from the Shared Policy selector, or create a new one.

This is the basic procedure for configuring an OSPFv3 process and assigning it to an interface on the OSPFv3 page:

1. On the Process Tab, page 54-24:
   - Specify which of the two processes you are configuring by choosing **Process 1** or **Process 2** from the OSPFv3 Process drop-down list.
   - Check **Enable OSPFv3 Process**.
   - Assign a **Process ID**; any positive integer between 1 and 65535.
   - Use the following features as needed to define the process:
   - **Advanced** button, opening the OSPFv3 Advanced Properties Dialog Box, page 54-25.
   - Area Tab (OSPFv3), page 54-28, for managing area, range, and virtual-link definitions, by means of the Add/Edit Area Dialog Box (OSPFv3), page 54-29, Add/Edit Range Dialog Box (OSPFv3), page 54-30, and Add/Edit Virtual Link Dialog Box (OSPFv3), page 54-31.
   - **Redistribution** panel, for managing route redistribution definitions by means of the Add/Edit Redistribution Dialog Box (OSPFv3), page 54-32.
   - **Summary Prefix** panel, for managing summary-prefix definitions by means of the Add/Edit Summary Prefix Dialog Box (OSPFv3), page 54-34.
2. On the OSPFv3 Interface Tab, page 54-34:
   a. Use the Interface and Neighbor panels to assign the process to a specific interface, using the Add/Edit Interface Dialog Box (OSPFv3), page 54-35 and the Add/Edit Neighbor Dialog Box (OSPFv3), page 54-38.

Related Topics

- About OSPFv3, page 54-22

About OSPFv3

Open Shortest Path First (OSPF) is an interior gateway routing protocol that uses link states rather than distance vectors for path selection. Version 3 is basically OSPFv2 enhanced for IPv6. It is similar to OSPFv2 (see About OSPF, page 54-2), but it is not backward compatible. To use OSPF to route both IPv4 and IPv6v packets, it will be necessary to run both OSPFv2 and OSPFv3 concurrently. They co-exist with each other, but do not interact.

Note OSPFv3 is supported on ASA 9.0+ devices operating in single-context, routed mode only. That is, multiple contexts and transparent mode are not supported.

Think of a link as being an interface on a networking device. A link-state protocol makes its routing decisions based on the states of the links that connect source and destination devices. The state of a link is a description of that interface and its relationship to its neighboring networking devices. This interface information includes the IPv6 prefix/length of the interface, the type of network it is connected to, the devices connected to that network, and so on. This information is propagated in various type of link-state advertisements (LSAs). Because only LSAs are exchanged, rather than entire routing tables, OSPF networks converge more quickly than RIP networks.

The ASA can run two processes of the OSPFv3 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 co-exist, but OSPFv3 does not allow overlapping addresses). Or you might want to run one process on the inside interface and another on the outside, redistributing 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 OSPFv3 routing process from another OSPFv3 routing process, a RIP routing process, or from static and connected routes configured on OSPFv3-enabled interfaces.

If NAT is employed but OSPFv3 is only running in public areas, 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 security appliance. Also, you should not mix public and private networks on the same security appliance interface.

Differences Between OSPFv2 and OSPFv3

The additional features provided by OSPFv3 over OSPFv2 include the following:

- 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.
- Protocol processing per link.
- Removal of addressing semantics.
- Addition of flooding scope.
- Support for multiple instances per link.
- Authentication support using the IPSec ESP standard for OSPFv3 routing protocol traffic, as specified by RFC-4552.

Configuration Restrictions

The following are ASA OSPFv3 configuration restrictions:

- To enable OSPFv3 on a specific interface, IPv6 should be enabled on the interface and it must be named.
- Only one OSPFv3 process, with one area and one instance, can be assigned to an interface.
- The Interface neighbor entries take effect only when the OSPFv3 is enabled, and network type should be point-to-point on the specified interface.
- Interface neighbor address must be a link-local address.
- Range value in area Range table should be unique across the area.
- If the area is set to NSSA or stub, the same area cannot be set for virtual-link.
- OSPFv3 redistribution not applicable on the same OSPFv3 process.

- If used in an ASA cluster, OSPFv3 encryption should be disabled.
- The Layer 3 cluster pool is not shared between OSPFv3 and the interface.

Related Topics

- Configuring OSPFv3, page 54-22
- Process Tab, page 54-24
- OSPFv3 Interface Tab, page 54-34

Process Tab

Use the Process tab on the OSPFv3 page to enable and configure up to two OSPFv3 routing processes. Each OSPF process has its own associated areas and networks. For each, at minimum, create an area for OSPFv3, enable an interface for OSPFv3, then redistribute the route into the targeted OSPFv3 routing processes. Note that only single-context mode is supported.

Navigation Path

The Process tab is on the OSPFv3 page.

- (Device view) Select **Platform > Routing > OSPFv3** from the Device Policy selector.
- (Policy view) Select **PIX/ASA/FWSM Platform > Routing > OSPFv3** from the Policy Type selector. Select an existing policy from the Shared Policy selector, or create a new one.

Related Topics

- Configuring OSPFv3, page 54-22
- About OSPFv3, page 54-22
- Area Tab (OSPFv3), page 54-28
- OSPFv3 Interface Tab, page 54-34

Field Reference

Table 54-20 Process Tab

Element	Description
OSPFv3 Process	Identify which OSPFv3 process you are configuring: choose **Process 1** or **Process 2**. You can enable one or both.
Enable OSPFv3 Process	Check this box to enable the chosen OSPFv3 process. Deselect this option to disable the OSPFv3 process; the process configuration information is retained should you wish to re-enable it later.
Process ID	Enter a unique numeric identifier for this process. The ID can be any positive integer between 1 and 65535. This process ID is used internally and does not need to match the OSPFv3 process ID on any other OSPFv3 devices.
Advanced	Opens the OSPFv3 Advanced Properties Dialog Box, page 54-25, in which you can configure additional process-related parameters, such Router ID, Adjacency Changes, Administrative Route Distances, Timers, Default Information Originate, and Passive Interface settings.

Table 54-20 Process Tab (Continued)

Element	Description
Area	Use the tabs and tables in this panel to manage area, range and virtual-link definitions. See Area Tab (OSPFv3), page 54-28 for more about these definitions.
Redistribution	Use this panel to manage redistribution definitions. See Add/Edit Redistribution Dialog Box (OSPFv3), page 54-32 for more about these definitions.
Summary Prefix	Use this panel to manage summary prefix definitions. See Add/Edit Summary Prefix Dialog Box (OSPFv3), page 54-34 for more about these definitions.

OSPFv3 Advanced Properties Dialog Box

Use the OSPF Advanced dialog box to configure settings such as the Router ID, Adjacency Changes, Administrative Route Distances, Timers, and Default Information Originate settings for an OSPF process.

Navigation Path

You can access the OSPF Advanced dialog box from the Process Tab, page 54-24.

Related Topics

- Configuring OSPFv3, page 54-22
- About OSPFv3, page 54-22

Field Reference

Table 54-21 OSPF Advanced Dialog Box

Element	Description
OSPF Process	This read-only field displays the ID of the OSPF process you are configuring.
Router ID	On a single device, choose **Automatic** or **IP Address**. (An address field appears when you choose IP Address.) If you choose Automatic, the highest-level IP address on the security appliance is used as the router ID. To use a fixed router ID, choose IP Address and enter an IPv4 address in the Router ID field. On a device cluster, choose **Automatic** or **Cluster Pool**. (An IPv4 Pool object ID field appears when you choose Cluster Pool.) If you choose Cluster Pool, enter or Select the name of the IPv4 Pool object that is to supply the Router ID address. For more information, see Add or Edit IPv4 Pool Dialog Box, page 6-84.
Ignore LSA MOSPF	Select this option to suppress transmission of syslog messages when the security appliance receives Type 6 (MOSPF) LSA packets.

Table 54-21 OSPF Advanced Dialog Box (Continued)

Element	Description
Adjacency Changes	These options specify the syslog messages sent when adjacency changes occur: • Log Adjacency Changes – When selected, the security appliance sends a syslog message whenever an OSPF neighbor goes up or down. Checking this box enables the Include Details option. • Include Details – When selected, the security appliance sends a syslog message whenever any state change occurs, not just when a neighbor goes up or down. This option is available only when Log Adjacency Changes is checked.
Administrative Route Distances	Settings for the administrative route distances, according to the route type. • Inter Area – The administrative distance for all routes from one area to another. Valid values range from 1 to 254; the default value is 110. • Intra Area – The administrative distance for all routes within an area. Valid values range from 1 to 254; the default value is 110. • External – The administrative distance for all routes from other routing domains that are learned through redistribution. Valid values range from 1 to 254; the default value is 110.

Table 54-21 OSPF Advanced Dialog Box (Continued)

Element	Description
Timers (in milliseconds)	LSA and SPF throttling provide a dynamic mechanism to slow LSA updates in OSPFv3 during times of network instability, and allow faster OSPFv3 convergence by providing LSA rate limiting. The settings used to configure LSA pacing and SPF calculation timers are: • LSA Arrival – The minimum delay between acceptance of the same LSA arriving from neighbors. Valid values range from 0 to 6000000 milliseconds. The default is 1000. • LSA Flood Pacing – The amount of time LSAs in the flooding queue are paced in between updates. Valid values range from 5 to 100 milliseconds. The default value is 33. • LSA Group Pacing – The interval at which LSAs are collected into a group and refreshed, check summed, or aged. Valid values range from 10 to 1800; the default value is 240 milliseconds. • LSA Retransmission Pacing – The length of time at which LSAs in the retransmission queue are paced. Valid values range from 5 to 200 milliseconds. The default value is 66. • LSA Throttle – The delay in milliseconds to generate the first occurrence of the LSA. Valid values range from 0 to 600000 milliseconds. When you enter a value in this field, the min and max fields are enabled: – min – The minimum delay for originating the same LSA. Valid values range from 1 to 600000 milliseconds. – max – The maximum delay for originating the same LSA. Valid values range from 1 to 600000 milliseconds. • SPF Throttle – The delay to receive a change to the SPF calculation. Valid values range from 1 to 600000 milliseconds. When you enter a value in this field, the min and max fields are enabled: – min – The delay between the first and second SPF calculations. Valid values range from 1 to 600000 milliseconds. – max – The maximum wait time for SPF calculations. Valid values range from 1 to 600000 milliseconds. **Note** Note For LSA throttling, if the minimum or maximum time is less than the first occurrence value, then OSPFv3 automatically corrects to the first occurrence value. Similarly, if the maximum delay specified is less than the minimum delay, then OSPFv3 automatically corrects to the minimum delay value.

Table 54-21 OSPF Advanced Dialog Box (Continued)

Element	Description
Default Information Originate	Settings used by an ASBR to generate a default external route into an OSPFv3 routing domain: • Enable Default Information Originate – Check this box to enable generation of a default route into the OSPFv3 routing domain; the following options become available: – Always advertise the default route – Check this box to always advertise the default route. – Metric Value – The OSPFv3 metric used to generate the default route. Valid values range from 0 to 16777214. – Metric Type – The external link type associated with the default route advertised into the OSPFv3 routing domain. Choose **1** or **2**, indicating a Type 1 or a Type 2 external route. The default value is 1. – Route Map – (Optional) The name of a route map to apply. The routing process generates the default route if the route map is satisfied. **Note** This field contains only the Route Map name. The Route Map is created and contained within a FlexConfig; see Chapter 7, "Managing FlexConfigs" for more information.
Passive Interface	Passive routing helps control the advertisement of OSPFv3 routing information, and disables sending and receiving OSPFv3 routing updates on an interface. Enter or Select one or more interfaces, or interface objects, to enable passive OSPFv3 routing on those interfaces. IPv4 and IPv6 addresses are supported.

Area Tab (OSPFv3)

Use the Area panel on the Process Tab, page 54-24 of the OSPFv3 page to configure OSPFv3 areas, ranges and virtual links. The Area panel consists of three definition tables—Area, Range, and Virtual Link:

- Refer to Add/Edit Area Dialog Box (OSPFv3), page 54-29 for information about adding and editing Area table entries.
- Refer to Add/Edit Range Dialog Box (OSPFv3), page 54-30 for information about adding and editing Range table entries.
- Refer to Add/Edit Virtual Link Dialog Box (OSPFv3), page 54-31 for information about adding and editing Virtual Link table entries.

Refer to Using Tables, page 1-47 for basic information about working with Security Manager tables.

Navigation Path

You can access the Area tab from the Process Tab, page 54-24 of the OSPFv3 page. For more information about the OSPFv3 page, see Configuring OSPFv3, page 54-22.

Related Topics

- About OSPFv3, page 54-22
- OSPFv3 Interface Tab, page 54-34

Add/Edit Area Dialog Box (OSPFv3)

Use the Add/Edit Area dialog box to define parameters for the area.

Navigation Path

You can access the Add/Edit Area dialog box from the Area Tab (OSPFv3), page 54-28.

Related Topics

- Configuring OSPFv3, page 54-22
- About OSPFv3, page 54-22
- Process Tab, page 54-24

Field Reference

Table 54-22 Add/Edit Area Dialog Box

Element	Description
Area ID	Enter an identifier for the area as either a decimal number or an IP address. Valid decimal values range from 0 to 4294967295.
Cost	The cost of sending a packet on an interface. Valid values are 0 to 65535. Routing decisions are based on cost, which is an indication of the overhead required to send packets across a certain interface. The ASA 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.

Table 54-22 Add/Edit Area Dialog Box (Continued)

Element	Description
Type	Define the area type by choosing one of the following: • Normal – Make the area a standard OSPFv3 area. This option is selected by default when you first create an area. • NSSA – Make the area a "not-so-stubby area." NSSAs accept Type 7 LSAs. When you choose this option, the Default Information Originate options are enabled. When you create a NSSA, you can prevent summary LSAs from being flooded into the area by deselecting *Allow sending summary LSA into this area*. You can also disable route redistribution by deselecting *Redistribute*, and enabling *Default information originate*. • Stub – Make the area a stub area. Stub areas do not have any routers or areas beyond it. Stub areas prevent AS External LSAs (Type 5 LSAs) from being flooded into the stub area. When you choose this option, *Allow sending summary LSA into this area* is enabled. When you create a stub area, you can prevent summary LSAs (Type 3 and 4) from being flooded into the area by deselecting *Allow sending summary LSA into this area*.
Default Information Originate These options are enabled when you choose NSSA as the area Type. The first option is enabled when you choose Stub as the area Type.	
Allow sending summary LSA into this area	Select to allow flooding of summary LSAs into the area.
Redistribute (imports routes to normal and NSSA areas)	Select to allow route redistribution.
Default information originate	Check this box to generate a Type 7 default into the NSSA. Selecting this option enables the following metric options: • Metric – The OSPF metric value for the default route. Valid values range from 1 to 16777214. The default is 1. • Metric Type – The OSPF metric type for the default route. Choose 1 (Type 1) or 2 (Type 2). The default is 1.

Add/Edit Range Dialog Box (OSPFv3)

Use the Add/Edit Area Range Network dialog box to add a new range to the area selected in the Area table, or to change an existing entry.

Navigation Path

You can access the Add/Edit Range dialog box from the Range panel under the Area Tab (OSPFv3), page 54-28.

Related Topics

- Configuring OSPFv3, page 54-22

- About OSPFv3, page 54-22
- Process Tab, page 54-24

Field Reference

Table 54-23 Add/Edit Range Dialog Box

Element	Description
Area ID	This read-only entry is the ID of the area to which this range applies.
IPv6 Prefix/Length	The IPv6 address(es) for the routes being summarized. **Tip** You can click **Select** to select the networks from a list of network objects.
Cost	The cost for the summary route, which is used during OSPF SPF calculations to determine the shortest paths to the destination. Valid values are 0 to 16777215. Routing decisions are based on cost, which is an indication of the overhead required to send packets across a certain interface. The ASA 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.
Advertise	Select this option to set the address range status to advertise. This causes Type 3 summary LSAs to be generated (this is the default). Deselect this option to suppress the Type 3 summary LSAs for the specified networks.

Add/Edit Virtual Link Dialog Box (OSPFv3)

Use the Add/Edit Virtual Link dialog box to define virtual links for the area selected in the Area table, or change the properties of existing virtual links.

Navigation Path

You can access the Add/Edit Virtual Link dialog box from the Virtual Link panel under the Area Tab (OSPFv3), page 54-28.

Related Topics

- Configuring OSPFv3, page 54-22
- About OSPFv3, page 54-22
- Process Tab, page 54-24

Field Reference

Table 54-24 Add/Edit Virtual Link Dialog Box

Element	Description
Area ID	This read-only entry is the ID of the area to which this virtual link applies.

Table 54-24 Add/Edit Virtual Link Dialog Box (Continued)

Element	Description
Peer Router ID	Enter the IP address of the virtual link neighbor. **Tip** You can click **Select** to select from a list of network objects.
TTL Security	The time-to-live (TTL) security hop count on a virtual link. The hop count value can range from 1 to 254.
Dead Interval	The interval, in seconds, if no hello packets are received, neighbors declare the device down. Valid values range from 1 to 8192. The default value of this field is four times the Hello Interval.
Hello Interval	The interval, in seconds, between hello packets sent on an interface. The smaller the hello interval, the faster topological changes are detected but the more traffic is sent on the interface. This value must be the same for all routers and access servers on a specific interface. Valid values range from 1 to 8192 seconds. The default value is 10 seconds.
Transmit Interval	The time, in seconds, between LSA retransmissions for adjacencies belonging to the interface. When a device sends an LSA to its neighbor, it keeps the LSA until it receives the acknowledgment message. If the device does not receive an acknowledgment, it will resend the LSA. Be conservative when setting this value, or needless retransmission can result. The value should be larger for serial lines and virtual links. Valid values range from 1 to 8192 seconds. The default value is 5 seconds.
Transmit Delay	The estimated time, in seconds, required to send an LSA packet on the interface. LSAs in the update packet have their ages increased by the amount specified by this field before transmission. If the delay is not added before transmission over a link, the time in which the LSA propagates over the link is not considered. The value assigned should take into account the transmission and propagation delays for the interface. This setting has more significance on very low-speed links. Valid values range from 1 to 8192 seconds. The default value is 1 second.

Add/Edit Redistribution Dialog Box (OSPFv3)

Use the Add/Edit Redistribution dialog box to add a redistribution rule to this process, or to edit an existing redistribution rule.

Navigation Path

You can access the Redistribution dialog box from the Redistribution panel under the Process Tab, page 54-24.

Related Topics

- Configuring OSPFv3, page 54-22
- About OSPFv3, page 54-22

Field Reference

Table 54-25 Add/Edit Redistribution Dialog Box

Element	Description
Source Protocol	Choose the source protocol for route redistribution: • Connected – Redistributes connected routes (routes established automatically by virtue of having an IP address enabled on the interface) to the OSPFv3 routing process. Connected routes are redistributed as external to the autonomous system. • OSPF – Redistributes routes from another OSPF routing process. The Routing PID and the Match options are enabled when you choose this option. • Static – Redistributes static routes to the OSPFv3 routing process.
Metric	The metric value for the routes being redistributed. Valid values range from 1 to 16777214; the default is 20. When redistributing from one OSPF process to another OSPF process on the same device, the metric will be carried through from one process to the other if no metric value is specified.
Metric Type	The metric type is the external link type associated with the default route that is advertised into the OSPFv3 routing domain. Choose None, 1, or 2, where None indicates there is no default route, 1 indicates the metric is a Type 1 external route, and 2 is a Type 2 external route.
Tag (optional)	The tag is a 32-bit decimal value attached to each external route. This is not used by OSPF itself. It may be used to communicate information between other border devices. Valid values range from 0 to 4294967295.
Route Map	The name of the route map to apply to the redistribution entry. **Note** This field contains only the Route Map name. The Route Map is created and contained within a FlexConfig; see Chapter 7, "Managing FlexConfigs" for more information.
Routing PID	The ID of the process to which redistribution is directed. (The Process ID is defined on the Process Tab, page 54-24.) This option is enabled only when OSPF is chosen as the Source Protocol.
Include Connected	Check this box to include connected routes in the redistribution.
Match	
The conditions used for redistributing routes from one routing protocol to another. The routes must match the selected condition to be redistributed. You can choose one or more of the following match conditions. These options are enabled only when OSPF is chosen as the Source Protocol.	
Internal	The route is internal to a specific autonomous system.
External 1	Routes that are external to the autonomous system, but are imported into OSPF as Type 1 external routes.
External 2	Routes that are external to the autonomous system, but are imported into OSPF as Type 2 external routes.

Table 54-25 Add/Edit Redistribution Dialog Box (Continued)

Element	Description
NSSA External 1	Routes that are external to the autonomous system, but are imported into OSPF as Type 2 NSSA routes.
NSSA External 2	Routes that are external to the autonomous system, but are imported into OSPF as Type 2 NSSA routes.

Add/Edit Summary Prefix Dialog Box (OSPFv3)

Use the Add/Edit Summary Prefix dialog box to add new route-summarization entries to the selected process, or to modify existing entries.

Navigation Path

You can access the Add/Edit Summary Prefix dialog box from the Summary Prefix panel under the Process Tab, page 54-24.

Related Topics

- Configuring OSPFv3, page 54-22
- About OSPFv3, page 54-22

Field Reference

Table 54-26 Add/Edit Summary Prefix Dialog Box

Element	Description
Process ID	This read-only value identifies the process to which this rule applies.
IPv6 Prefix/Length	Enter an IPv6 prefix/length for external route summarization. **Tip** You can click **Select** to select from a list of network objects.
Advertise	When selected, summary routes that match the specified prefix and mask pair are advertised. When deselected, routes that match the specified prefix and mask pair are suppressed. By default, this check box is selected.
Tag (optional)	The tag is a 32-bit decimal value attached to each external route. This is not used by OSPF itself. It may be used to communicate information between border devices. Valid values range from 0 to 4294967295. This field is enabled when you check Advertise.

OSPFv3 Interface Tab

Use the Interface panel to configure interface-and neighbor-specific OSPFv3 routing properties. The Interface panel consists of two definition tables, Interface and Neighbor:

- Refer to Add/Edit Interface Dialog Box (OSPFv3), page 54-35 for information about adding and editing Interface table entries.
- Refer to Add/Edit Neighbor Dialog Box (OSPFv3), page 54-38 for information about adding and editing Neighbor table entries.

Refer to Using Tables, page 1-47 for basic information about working with Security Manager tables.

Navigation Path

Click the Interface tab on the OSPFv3 page to display this panel. For more information about the OSPFv3 page, see Configuring OSPFv3, page 54-22.

Related Topics

- About OSPFv3, page 54-22
- Process Tab, page 54-24

Add/Edit Interface Dialog Box (OSPFv3)

Use the Add/Edit Interface dialog box to define OSPFv3 routing properties for an individual interface, or to change an existing entry.

Navigation Path

You can access the Add/Edit Interface dialog box from the Interface panel under the OSPFv3 Interface Tab, page 54-34.

Related Topics

- Configuring OSPFv3, page 54-22
- About OSPFv3, page 54-22
- Process Tab, page 54-24

Field Reference

Table 54-27 Add/Edit Interface Dialog Box

Element	Description
Interface	The name of the interface to which this routing configuration applies. **Tip** You can click **Select** to select from a list of interface objects.
Enable OSPFv3 on this interface	Check this box to enable OSPFv3 on the specified interface, and activate the following fields: • Process ID – Choose the process to apply to this interface; defined on the OSPFv3 Process Tab, page 54-24. • Area ID – Identify the area to be assigned; areas are also defined on the OSPFv3 Process Tab, page 54-24. • Instance ID – (Optional) Specify an ID for this process instance. Valid values for this setting range from 0 to 255. This feature lets you have multiple OSPFv3 processes on a single link. Received packets with other instance IDs are then ignored by this process.
Properties	
Filter outgoing link-state advertisements	Check this box to filter outgoing LSAs. All outgoing LSAs are flooded to the interface by default.

Table 54-27 Add/Edit Interface Dialog Box (Continued)

Element	Description
Disable MTU mismatch detection	Check this box to disable the OSPFv3 MTU mismatch detection when database description (DBD) packets are received.
Flood Reduction	Check this box to suppress unnecessary flooding of LSAs in stable topologies.
Point-to-point Network	Check this box to define this as a link to a point-to-point network; that is, a network between two routing devices. All neighbors on a point-to-point network establish adjacency and there is no designated router. This option is unavailable when the Broadcast option is selected.
Broadcast	Check this box to define this as a link to a network with multiple routing devices. Such networks establish a designated router (DR), as well as a backup designated router (BDR), that controls LSA flooding on the network. This option is unavailable when the Point-to-point Network option is selected.
Cost	The cost of sending a packet through the interface. Link cost is an arbitrary number used in shortest path first calculations. If you do not assign a value, the configured reference bandwidth divided by the interface port speed is used. (The default reference bandwidth is 40 Gb/sec.)
Priority	Assign an OSPFv3 priority to this interface. Valid values for this setting range from 0 to 255. Entering 0 for this setting makes the device ineligible to become the designated router or backup designated router. This setting does not apply to interfaces that are configured as point-to-point, non-broadcast interfaces. When two routing devices connect to a network, both attempt to become the designated router. The device with the higher priority becomes the designated router. If there is a tie, the router with the higher router ID becomes the designated router.
Dead Interval	If no hello packets are received from a neighbor within this interval, that device is designated as inactive. Valid values range from 1 to 65535. The default value for this setting is four times the hello interval.
Poll Interval	If a neighboring device is inactive, it may be necessary to continue sending hello packets to that neighbor. The hello packets are sent at this reduced interval, which should be larger than the hello interval.
Retransmit Interval	The time, in seconds, between LSA retransmissions for adjacent neighbors. When a router sends an LSA to a neighbor, it keeps the LSA until it receives an acknowledgment. If an acknowledgment is not received within this interval, it will resend the LSA. Be conservative when setting this value, or needless retransmission can result. The value should be larger for serial lines and virtual links. Valid values range from 1 to 65535 seconds.

Table 54-27 Add/Edit Interface Dialog Box (Continued)

Element	Description
Transmit Delay	The estimated time, in seconds, required to send an LSA packet on the interface. LSAs in the update packet have their ages increased by the amount specified by this field before transmission. If the delay is not added before transmission over a link, the time in which the LSA propagates over the link is not considered. The value assigned should take into account the transmission and propagation delays for the interface. This setting has more significance on very low-speed links. Valid values range from 1 to 65535 seconds.
Authentication	
Type	The type of authentication enabled on this interface. Choose one of the following: • Area – OSPFv3 does not provide "built-in" authentication, instead relying on IPv6/IPSec protocols. Choose this option to use those protocols to authenticate OSPFv3 traffic on all interfaces in the area; this means all routing devices in the area must use this option. This is the default. • Interface – Choose this option to secure this interface and protect OSPFv3 virtual links. The additional parameters in this section are enabled when you choose this option. • None – OSPFv3 authentication is disabled.
Security Parameter Index	Enter an IPSec identification tag used to distinguish this particular OSPFv3 interface; used in conjunction with the specified authentication and encryption rules. Valid values range from 256 to 4294967295.
Authentication Algorithm	Choose the type of authentication algorithm to use: • md5 – Message Digest 5; produces a 128-bit hash value. • sha1 – Secure Hash Algorithm version 1; produces a 160-bit hash value.
Authentication Key	Enter an authentication key. The length of the key entered depends on the type of authentication chosen as the Authentication Algorithm, and whether the key is to be encrypted (when you check the Encrypt Authentication Key box): • md5 – 32 characters. • md5 (encrypted) – 66 characters. • sha1 – 40 characters. • sha1 (encrypted) – 82 characters.
Encrypt Authentication Key	Check this box to require encryption of the specified Authentication Key for transmission.
Include Encryption	Check this box to require encryption of OSPFv3 packets. The following options are enabled.

Table 54-27 Add/Edit Interface Dialog Box (Continued)

Element	Description
Encryption Algorithm	Choose the type of encryption to use: • 3des – Triple DES; the Data Encryption Standard cipher algorithm is applied three times to each packet. • aes-cbc – Encryption is based on the Advanced Encryption Standard with Cipher Block Chaining, to produce a key of the size chosen with the Key Type parameter. The Key Type list is enabled only when you choose this encryption option. Choose one of these options: – 128 – For 128-bit keys. – 192 – For 192-bit keys. – 256 – For 256-bit keys. • des – Encryption is based on the Data Encryption Standard, using 56-bit keys.
Encryption Key	Enter an encryption key. The length of the key entered depends on the type of encryption chosen as the Encryption Algorithm, and whether the key is to be encrypted (when you check the Encrypt Key box): • 3des – 48 characters (192 bits). • 3des (encrypted) – 98 characters (192 bits). • aes-cbc/128 – 32 characters (128 bits). • aes-cbc/128 (encrypted) – 66 characters (128 bits). • aes-cbc/192 – 48 characters (192 bits). • aes-cbc/192 (encrypted) – 98 characters (192 bits). • aes-cbc/256 – 64 characters (256 bits). • aes-cbc/256 (encrypted) – 130 characters (256 bits). • des – 16 characters (64 bits). • des (encrypted) – 34 characters (64 bits).
Encrypt Key	Check this box to require encryption of the specified Encryption Key for transmission.

Add/Edit Neighbor Dialog Box (OSPFv3)

You must define a static neighbor for each point-to-point, non-broadcast interface. This feature lets you broadcast OSPFv3 advertisements across an existing VPN connection without having to encapsulate the advertisements in a GRE tunnel. Note the following restrictions:

- You cannot define the same static neighbor for two different OSPFv3 processes.
- You must define a static route for each static neighbor.

Use the Add/Edit Neighbor dialog box to define a static neighbor for the interface selected in the Interface table, or to change information for an existing static neighbor.

Navigation Path

You can access the Add/Edit Neighbor dialog box from the Neighbor panel under the OSPFv3 Interface Tab, page 54-34.

Related Topics

- Configuring OSPFv3, page 54-22
- About OSPFv3, page 54-22
- Process Tab, page 54-24

Field Reference

Table 54-28 Add/Edit Neighbor Dialog Box

Element	Description
Interface	The interface associated with this neighbor definition (read-only).
Link-local Address	Enter the IPv6 address of the static neighbor.
Cost and Database Filter	Check this box to enable filtering of the outgoing LSAs on the interface during synchronization and flooding. The following options are enabled: • Cost – Use this field to assign an arbitrary cost to this neighbor. If a value is not assigned, the cost of the interface is used (this value is based on the port speed of the interface, and is calculated as reference bandwith divided by interface speed). Valid values range from 1 to 65535. • Filter outgoing link-state advertisements – Check this box to disable forwarding of outgoing LSAs to this neighbor. **Note** The Cost and Database Filter options and the Poll-Interval options are mutually exclusive.
Poll-Interval	Check this box to enable the following options: • Poll Interval – Time interval in seconds between transmission of hello packets to a “dead” neighbor. The default is 120. If a neighboring device becomes inactive (hello packets have not been received for the dead interval period), it may be necessary to continue sending hello packets to the dead neighbor at a reduced rate. Thus this value should be larger than the interface hello interval. • Priority – The router priority value of this neighbor. The default is 0; valid values range from 1 to 255. The priority value helps determine the designated router for an OSPFv3 link. A value of zero means the device is ineligible to become the designated router, or backup designated router. **Note** The Poll-Interval options and the Cost and Database Filter options are mutually exclusive. Also, these values do not apply to point-to-multipoint interfaces.

Configuring RIP

Routing Information Protocol (RIP) is a dynamic routing protocol, or more precisely, an interior gateway protocol that is based on distance vectors. RIP uses hop count as the metric for path selection. When RIP is enabled on an interface, the interface exchanges RIP broadcast packets with neighboring devices to dynamically learn about and advertise routes. These RIP packets contain information about the destination networks that the gateways can reach, and the number of gateways that a packet must travel through to reach those destinations.

Cisco Security Manager supports both RIP version 1 and RIP version 2. Version 1 does not send the subnet mask with the routing update; RIP version 2 sends the subnet mask with the routing update, and supports variable-length subnet masks. Additionally, RIP version 2 supports neighbor authentication when routing updates are exchanged. This authentication ensures that the security appliance receives reliable routing information from a trusted source.

Note You cannot enable RIP if you have OSPF processes running.

Limitations

RIP has the following limitations:

- Cisco Security Manager cannot pass RIP updates between interfaces.
- RIP Version 1 does not support variable-length subnet masks.
- RIP has a maximum hop count of 15. A route with a hop count greater than 15 is considered unreachable.
- RIP convergence is relatively slow compared to other routing protocols.

RIP Version 2 Notes

The following information applies to RIP Version 2 only:

- If using neighbor authentication, the authentication key and key ID must be the same on all neighbor devices that provide RIP version 2 updates to the interface.
- With RIP version 2, the security appliance transmits and receives default route updates using the multicast address 224.0.0.9. In passive mode, it receives route updates at that address.
- When RIP version 2 is configured on an interface, the multicast address 224.0.0.9 is registered on that interface. When a RIP version 2 configuration is removed from an interface, that multicast address is unregistered.

Using Security Manager to Configure RIP on Security Appliances

Use the RIP page to enable the Routing Information Protocol on an interface. The settings and features available when configuring RIP depend on the type of device and OS version that you are configuring:

- To configure RIP on a PIX Firewall or ASA running an OS version earlier than 7.2, or on any FWSM, see RIP Page for PIX/ASA 6.3–7.1 and FWSM, page 54-41.
- To configure RIP on a PIX Firewall or ASA running OS version 7.2 or later, see RIP Page for PIX/ASA 7.2 and Later, page 54-43.

Related Topics

- Configuring Static Routes, page 54-48
- Configuring OSPF, page 54-2

- Configuring No Proxy ARP, page 54-1
- Configuring Routing Information Protocol – a chapter from the "Cisco IOS IP Configuration Guide, Release 12.2," providing additional detailed information about RIP

RIP Page for PIX/ASA 6.3–7.1 and FWSM

Use this RIP page to enable the Routing Information Protocol (RIP) on an interface in any FWSM, or in a PIX/ASA running a pre-7.2 version operating system.

The RIP table on this page lists all interfaces on which RIP is currently defined. Use the Add RIP Configuration and Edit RIP Configuration dialog boxes to create and maintain these entries. See RIP Page for PIX/ASA 6.3–7.1 and FWSM, page 54-41 for more information.

Navigation Path

- (Device view) Select **Platform > Routing > RIP** from the Device Policy selector.
- (Policy view) Select **PIX/ASA/FWSM Platform > Routing > RIP** from the Policy Type selector. Select an existing policy from the Shared Policy selector, or create a new one.

  When creating a shared RIP policy, you must choose a Version in the Create a Policy dialog box, as follows:

  - **PIX/ASA 6.3-7.1 and FWSM**
  - **PIX/ASA 7.2 and Later**

  When assigning a shared RIP policy, be sure to assign the appropriate RIP policy for the device. For example, you cannot assign a PIX/ASA 7.2+ RIP policy to an FWSM.

Related Topics

- Configuring Static Routes, page 54-48
- Configuring OSPF, page 54-2
- Configuring No Proxy ARP, page 54-1
- RIP Page for PIX/ASA 7.2 and Later, page 54-43
- Standard rules table topics:
  - Using Rules Tables, page 12-7
  - Table Columns and Column Heading Features, page 1-48

Add/Edit RIP Configuration (PIX/ASA 6.3–7.1 and FWSM) Dialog Boxes

Use the Add RIP Configuration and Edit RIP Configuration dialog boxes to add a RIP configuration to the security appliance, or to make changes to an existing RIP configuration. By adding a RIP configuration, you enable RIP on the specified interface. Except for their titles, the two dialog boxes are identical.

Navigation Path

You can access the Add and Edit RIP Configuration dialog boxes from the RIP Page for PIX/ASA 6.3–7.1 and FWSM, page 54-41.

Field Reference

Table 54-29 Add/Edit RIP Configuration (PIX/ASA 6.3-7.1 and FWSM) Dialog Boxes

Element	Description
Interface	Enter or Select the interface for the RIP configuration. You cannot configure two different RIP configurations on the same interface.
Mode	Select the interface behavior regarding RIP updates: • **Send default routes** – The interface will transmit RIP routing updates only. • **Receive routes** – The interface will listen for RIP routing broadcasts and use that information to populate its routing table, but it will not send RIP routing updates. • **Send default routes and receive routes** – The interface will send and receive RIP routing updates.
Version	Select the RIP version to enable on the interface: • **RIP Version 1** – Enables RIP Version 1 on the interface. • **RIP Version 2** – Enables RIP Version 2 on the interface. Configuring RIP Version 2 registers the multicast address 224.0.0.9 on the interface.
Version 2 Authentication	These options let you enable and select the type of authentication used with RIP Version 2. • **Enable Authentication** – This option is available when you select RIP Version 2 above. When this box is checked, RIP neighbor authentication is enabled and the following options become available: – **Type** – Select **MD5** to use the MD5 hash algorithm for authentication (recommended), or select **Clear text** to use clear text for authentication. – **Key ID** – The identification number of the authentication key. This number must be shared with all other devices sending updates to and receiving updates from the security appliance. Valid values range from 1 to 255. – **Key** – The shared key used for authentication. This key must be shared with all other devices sending updates to and receiving updates from the security appliance. The key can be up to 16 characters.

RIP Page for PIX/ASA 7.2 and Later

Use this RIP page to enable and configure the Routing Information Protocol (RIP) on PIX and ASA devices running operating system 7.2 or later. The RIP page consists of these tabbed panels:

- RIP - Setup Tab, page 54-43
- RIP - Redistribution Tab, page 54-45
- RIP - Filtering Tab, page 54-46
- RIP - Interface Tab, page 54-47

Navigation Path

- (Device view) Select **Platform > Routing > RIP** from the Device Policy selector.
- (Policy view) Select **PIX/ASA/FWSM Platform > Routing > RIP** from the Policy Type selector. Select an existing policy from the Shared Policy selector, or create a new one.

  When creating a shared RIP policy, you must choose a Version in the Create a Policy dialog box, as follows:

  - **PIX/ASA 6.3-7.1 and FWSM**
  - **PIX/ASA 7.2 and Later**

  When assigning a shared RIP policy, be sure to assign the appropriate RIP policy for the device. For example, you cannot assign a PIX/ASA 7.2+ RIP policy to an FWSM.

Related Topics

- Configuring Static Routes, page 54-48
- Configuring OSPF, page 54-2
- Configuring No Proxy ARP, page 54-1
- RIP Page for PIX/ASA 6.3–7.1 and FWSM, page 54-41

RIP - Setup Tab

Use the Setup panel to define RIP on the security appliance, and to configure global RIP protocol parameters. You can only enable a single RIP process on the security appliance.

Navigation Path

You can access the Setup tab from the RIP Page for PIX/ASA 7.2 and Later, page 54-43.

Related Topics

- RIP - Redistribution Tab, page 54-45
- RIP - Filtering Tab, page 54-46
- RIP - Interface Tab, page 54-47
- Chapter 54, “Configuring Routing Policies on Firewall Devices”

Field Reference

Table 54-30 Setup Tab

Element	Description
Networks	Define one or more networks for RIP routing. Enter IP address(es), or enter or Select the desired Network/Hosts objects (see Understanding Networks/Hosts Objects, page 6-75); IP addresses must not contain any subnet information. There is no limit to the number of networks you can add to the security appliance configuration. The RIP routing updates will be sent and received only through interfaces on the specified networks. Also, if the network of an interface is not specified, the interface will not be advertised in any RIP updates.
Passive Interface	Use this option to specify passive interfaces on the security appliance, and by extension the active interfaces. The device listens for RIP routing broadcasts on passive interfaces, using that information to populate its routing tables, but does not broadcast routing updates on passive interfaces. Interfaces that are not designated as passive, receive and send updates. Choose one of these options: 1. **None** – No interfaces are designated as passive. 2. **All Interfaces** – All interfaces on the device are designated as passive, except those entered the Excluded Interfaces field below. 3. **Specified Interfaces** – Only those interfaces explicitly specified in the Interfaces field below are designated as passive.
Interfaces/Excluded Interfaces	Use this field to specify the interfaces excluded from the passive list, or those explicitly designated as passive, depending on your choice from the Passive Interface list above: • If you chose All Interfaces, this field is labeled **Excluded Interfaces**: enter or Select only those interfaces to be excluded (that is, those that are to be active not passive). • If you chose Specified Interfaces in the Passive Interface list, enter or Select those interfaces that are to be designated as passive. **Note** You cannot specify two different RIP configurations for the same interface.
RIP Version	Choose the RIP versions for sending and receiving RIP updates: • Receive Version 1 and 2, Send Version 1 • Send and Receive Version 1 • Send and Receive Version 2
Generate Default Route	When selected, a default route is generated for distribution, based on the Route Map you specify.
Route Map	Specify the route map to use for generating default routes. **Note** This field contains only the Route Map name. The Route Map is created and contained within a FlexConfig; see Chapter 7, "Managing FlexConfigs" for more information.

Table 54-30 Setup Tab (Continued)

Element	Description
Enable Auto-Summary	When Send and Receive Version 2 is the chosen RIP Version, this option is available. When checked, automatic route summarization is enabled. Disable automatic summarization if you must perform routing between disconnected subnets. When automatic summarization is disabled, subnets are advertised. **Note** RIP Version 1 always uses automatic summarization—you cannot disable it.

RIP - Redistribution Tab

Use the Redistribution panel to manage redistribution routes. These are the routes that are being redistributed from other routing processes into the RIP routing process. See Add/Edit Redistribution Dialog Box, page 54-45 for more information.

Navigation Path

You can access the Redistribution tab from the RIP Page for PIX/ASA 7.2 and Later, page 54-43.

Related Topics

- RIP - Setup Tab, page 54-43
- RIP - Filtering Tab, page 54-46
- RIP - Interface Tab, page 54-47
- Chapter 54, “Configuring Routing Policies on Firewall Devices”

Add/Edit Redistribution Dialog Box

Use the Add Redistribution and Edit Redistribution dialog boxes to add and edit redistribution routes on the RIP - Redistribution Tab, page 54-45. These are the routes that are being redistributed from other routing processes into the RIP routing process. Except for their titles, these two dialog boxes are identical.

Navigation Path

You can access the Add and Edit Redistribution dialog boxes from the Redistribution tab on the RIP Page for PIX/ASA 7.2 and Later, page 54-43.

Field Reference

Table 54-31 Add/Edit Redistribution Dialog Box

Element	Description
Protocol to Redistribute	Choose the routing protocol to redistribute into the RIP routing process: • **Static** – Static routes. • **Connected** – Directly connected networks. • **OSPF** – Routes discovered by the OSPF routing process. If you choose OSPF, you must also enter the OSPF Process ID and, optionally, Match criteria.

Table 54-31 Add/Edit Redistribution Dialog Box (Continued)

Element	Description
Process ID	Enter the process ID when the OSPF protocol is chosen.
Match	If you are redistributing OSPF routes into the RIP routing process, you can select specific types of OSPF routes to redistribute. Ctrl-click to select multiple types: • Internal – Routes internal to the autonomous system (AS) are redistributed. • External 1 – Type 1 routes external to the AS are redistributed. • External 2 – Type 2 routes external to the AS are redistributed. • NSSA External 1 – Type 1 routes external to a not-so-stubby area (NSSA) are redistributed. • NSSA External 2 – Type 2 routes external to an NSSA are redistributed. Match criteria are optional. The default is match Internal, External 1, and External 2.
Metric	The RIP metric type to apply to the redistributed routes. The two choices are: • **Transparent** – Use the current route metric. • **Specified Value** – Assign a specific metric value.
Metric Value	The metric value to be assigned; enter a value from 0 to 16.
Route Map	The name of a route map that must be satisfied before the route can be redistributed into the RIP routing process. **Note** This field contains only the route Map name. The contents of the route map are created and contained within a FlexConfig. See Chapter 7, "Managing FlexConfigs" for more information.

RIP - Filtering Tab

Use the Filtering panel to manage filters for the RIP policy. Filters are used to limit network information in incoming and outgoing RIP advertisements. See Add/Edit Filter Dialog Box, page 54-47 for more information.

Navigation Path

You can access the Filtering tab from the RIP Page for PIX/ASA 7.2 and Later, page 54-43.

Related Topics

- RIP - Setup Tab, page 54-43
- RIP - Redistribution Tab, page 54-45
- RIP - Interface Tab, page 54-47
- Chapter 54, "Configuring Routing Policies on Firewall Devices"

Add/Edit Filter Dialog Box

Use the Add Filter and Edit Filter dialog boxes to add and edit RIP filters on the RIP - Filtering Tab, page 54-46. Filters are used to limit network information in incoming and outgoing RIP advertisements. Except for their titles, these two dialog boxes are identical.

Navigation Path

You can access the Add and Edit Filter dialog boxes from the Filtering tab on the RIP Page for PIX/ASA 7.2 and Later, page 54-43.

Field Reference

Table 54-32 Add/Edit Filter Dialog Box

Element	Description
Traffic Direction	Choose the type of traffic to be filtered: **Inbound** or **Outbound**. **Note** If Traffic Direction is Inbound, you can define an Interface filter only.
Filter On	Specify whether the filter is based on an **Interface** or a **Route**. If you select Interface, enter or Select the name of the interface on which routing updates are to be filtered. If you select Route, choose the route type: • **Static** – Only static routes are filtered. • **Connected** – Only connected routes are filtered. • **OSPF** – Only OSPF routes discovered by the specified OSPF process are filtered. Enter the Process ID of the OSPF process to be filtered.
Filter ACLs	Enter or Select the name of one or more access control lists (ACLs) that define the networks to be allowed or removed from RIP route advertisements.

RIP - Interface Tab

Use the Interface panel to manage the interfaces configured to send and receive RIP broadcasts. See Add/Edit Interface Dialog Box, page 54-48 for more information.

Navigation Path

You can access the Interface tab from the RIP Page for PIX/ASA 7.2 and Later, page 54-43.

Related Topics

- RIP - Setup Tab, page 54-43
- RIP - Redistribution Tab, page 54-45
- RIP - Filtering Tab, page 54-46
- Chapter 54, “Configuring Routing Policies on Firewall Devices”

Add/Edit Interface Dialog Box

Use the Add Interface and Edit Interface dialog boxes to add and edit RIP interface configurations on the RIP - Interface Tab, page 54-47. Except for their titles, these two dialog boxes are identical.

Navigation Path

You can access the Add and Edit Interface dialog boxes from the Interface tab on the RIP Page for PIX/ASA 7.2 and Later, page 54-43.

Field Reference

Table 54-33 Add/Edit Interface Dialog Box

Element	Description
Interface	Enter or Select an interface defined on this appliance.
Send (Version)	These options let you override, for this interface, the global Send versions specified on the RIP - Setup Tab, page 54-43. Select the appropriate boxes to specify sending updates using RIP Version 1, Version 2, or both.
Receive (Version)	These options let you override the global Receive versions. Select the appropriate boxes to specify accepting updates using RIP Version 1 only, Version 2 only, or both.
Authentication type	Choose the authentication used on this interface for RIP broadcasts: • **None** – No authentication. • **MD5** – Employ MD5. • **Clear Text** – Employ clear-text authentication. If you choose MD5 or Clear Text, you must also provide the following authentication parameters: • **Key ID** – The ID of the authentication key. Valid values are from 0 to 255. • **Key** – The key used by the chosen authentication method. Can contain up to 16 characters. • **Confirm** – Enter the authentication key again, to confirm.

Configuring Static Routes

A static route is a specific path to a particular destination network that is manually defined on the current device. Static routes are used in a variety of situations, and can be a quick and effective way to route data from one network to another when there is no dynamic route to the destination, or when use of a dynamic routing protocol is not feasible.

All routes have a value or “metric” that represents its priority of use. (This metric is also referred to as “administrative distance.”) When two or more routes to the same destination are available, devices use administrative distance to decide which route to use.

For static routes, the default metric value is one, which gives them precedence over routes from dynamic routing protocols. If you increase the metric to a value greater than that of a dynamic route, the static route operates as a back-up in the event that dynamic routing fails. For example, Open Shortest Path First

(OSPF)-derived routes have a default administrative distance of 100. To configure a back-up static route that is overridden by an OSPF route, specify a metric value for the static route that is greater than 100. This is referred to as a "floating" static route.

There is a special kind of static route known as a default route, or a "zero-zero" route because all zeroes are used for both the destination address and subnet mask. The default static route serves as a catch-all gateway: if there are no matches for a particular destination in the device's routing table, the default route is used. The default route generally includes a next-hop IP address or local exit interface.

Use the Static Route page to maintain manually defined static routes. The Static Route table on this page lists all currently defined static routes, showing for each, the name of the interface or interface role for which the route is defined, the destination network(s), the next hop gateway, the route metric, whether the route is tunneled, and whether there is service-level agreement tracking for the route. For a detailed explanation of these fields, see Add/Edit Static Route Dialog Box, page 54-49 or Add/Edit IPv6 Static Route Dialog Box, page 54-50.

Navigation Path

- (Device view) Select **Platform > Routing > Static Route** or **Platform > Routing > IPv6 Static Route** from the Device Policy selector.
- (Policy view) Select **PIX/ASA/FWSM Platform > Routing > Static Route** or **PIX/ASA/FWSM Platform > Routing > IPv6 Static Route** from the Policy Type selector. Select an existing policy from the Shared Policy selector, or create a new one.

Related Topics

- Chapter 54, "Configuring Routing Policies on Firewall Devices"
- Add/Edit Static Route Dialog Box, page 54-49
- Add/Edit IPv6 Static Route Dialog Box, page 54-50
- Monitoring Service Level Agreements (SLAs) To Maintain Connectivity, page 50-8
- Standard rules table topics:
  - Using Rules Tables, page 12-7
  - Table Columns and Column Heading Features, page 1-48

Add/Edit Static Route Dialog Box

The Add/Edit Static Route dialog box lets you add or edit a static route.

Navigation Path

You can access the Add/Edit Static Route dialog box from the Static Routes page. Click the Add Row button to add a new static route; select an existing static route and click the Edit Row button to edit that route.

Related Topics

- Configuring Static Routes, page 54-48
- Chapter 54, "Configuring Routing Policies on Firewall Devices"

Field Reference

Table 54-34 Add/Edit Static Route Dialog Box

Element	Description
Interface	Enter or Select the interface to which this static route applies.
Network	Enter or Select the destination network(s). You can provide one or more IP address/netmask entries, one or more Networks/Hosts objects, or a combination of both; separate the entries with commas. Enter "0.0.0.0/0" or "any" to specify a default route.
Gateway	Enter or Select the gateway router which is the next hop for this route. You can provide an IP address, or a Networks/Hosts object. **Note** If an IP address from one of the security appliance's interfaces is used as the Gateway IP address, the security appliance will resolve the designated IP address in the packet instead of resolving the Gateway IP address.
Metric	The Metric is a measurement of the "expense" of a route, based on the number of hops (hop count) to the network on which a specific host resides. Hop count is the number of networks that a network packet must traverse, including the destination network, before it reaches its final destination. Because the hop count includes the destination network, all directly connected networks have a metric of 1. Enter the number of hops to the destination network. Valid values range from 1 to 255; the default value is 1. The maximum number of equal-cost (equal-metric) routes that can be defined per interface is three. You cannot add a route with the same metric on different interfaces that are on the same network.
Tunneled	Select this option to make this a tunnel route; can be used only for a default route. You can configure only one default tunneled gateway per device. The Tunneled option is not supported in transparent mode. Available only on PIX/ASA 7.0+ devices.
Route Tracking	To monitor route availability, enter or Select name of an SLA (service level agreement) object that defines the monitoring policy. Available only on PIX/ASA 7.2+ devices. For more information on route tracking, see Monitoring Service Level Agreements (SLAs) To Maintain Connectivity, page 50-8.

Add/Edit IPv6 Static Route Dialog Box

The Add/Edit IPv6 Static Route dialog box lets you add or edit an IPv6 static route. IPv6 static routes are only supported on the following devices:

- ASA 7.0 and later (Routed mode)
- ASA 8.2 and later (Transparent mode)
- FWSM 3.1 and later (Routed mode)

Navigation Path

You can access the Add/Edit IPv6 Static Route dialog box from the IPv6 Static Route page. Click the **Add Row** button to add a new static route; select an existing static route and click the **Edit Row** button to edit that route.

Related Topics

- Configuring Static Routes, page 54-48
- Chapter 54, "Configuring Routing Policies on Firewall Devices"

Field Reference

Table 54-35 Add/Edit IPv6 Static Route Dialog Box

Element	Description
Interface	Enter or Select the interface to which this static route applies.
IPv6 Network	Enter or Select the destination network(s). You can provide one or more IP address entries, one or more Networks/Hosts objects, or a combination of both; separate the entries with commas. Enter two colons (::) to specify a default route.
IPv6 Gateway	Enter or Select the gateway router which is the next hop for this route. You can provide an IP address, or a Networks/Hosts object. **Note** If an IP address from one of the security appliance's interfaces is used as the Gateway IP address, the security appliance will resolve the designated IP address in the packet instead of resolving the Gateway IP address.
Metric	The Metric is a measurement of the "expense" of a route, based on the number of hops (hop count) to the network on which a specific host resides. Hop count is the number of networks that a network packet must traverse, including the destination network, before it reaches its final destination. Because the hop count includes the destination network, all directly connected networks have a metric of 1. Enter the number of hops to the destination network. Valid values range from 1 to 255; the default value is 1. The maximum number of equal-cost (equal-metric) routes that can be defined per interface is three. You cannot add a route with the same metric on different interfaces that are on the same network.
Tunneled	Select this option to specify the route as the default tunnel gateway for VPN traffic. You can configure only one default tunneled gateway per device. Available only on ASA 7.0+ devices in routed mode.