CHAPTER 53

Configuring Multicast Policies on Firewall Devices

The Multicast section contains pages for defining IP multicast routing on security devices. Multicast routing is supported in single-context, routed mode only.

Enabling multicast routing enables IGMP and PIM on all interfaces by default. Internet Group Management Protocol (IGMP) is used to learn whether members of a group are present on directly attached subnets. Hosts join multicast groups by sending IGMP report messages. Protocol Independent Multicast (PIM) is used to maintain forwarding tables for multicast datagrams.

Note Only the UDP transport layer is supported for multicast routing.

This chapter contains the following topics:

Enabling PIM and IGMP

The Enable PIM and IGMP page lets you enable or disable Internet Group Management Protocol (IGMP) and Protocol Independent Multicast (PIM) on all interfaces on the security appliance. IGMP is used to learn whether members of a group are present on directly attached subnets. Hosts join multicast groups by sending IGMP report messages. PIM is used to maintain forwarding tables to forward multicast datagrams.

When **Enable PIM and IGMP** is checked on this page, PIM and IGMP are enabled on all interfaces on the security appliance. Deselect the option to disable PIM and IGMP on all interfaces.

Note You can disable PIM and IGMP on a per-interface basis; see IGMP Page - Protocol Tab, page 53-3 and PIM Page - Protocol Tab, page 53-12 for more information.

Navigation Path

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

Related Topics

- Configuring IGMP, page 53-2
- Configuring Multicast Routes, page 53-8
- Configuring Multicast Boundary Filters, page 53-9
- Configuring PIM, page 53-11

Configuring IGMP

Internet Protocol hosts use IGMP to report their group memberships to directly connected multicast routers. Internet Group Management Protocol (IGMP) uses group-address (Class D) IP addresses.

Host group addresses can be in the range 224.0.0.0 to 239.255.255.255. The address 224.0.0.0 is never assigned to any group. The address 224.0.0.1 is assigned to all systems on a subnet. The address 224.0.0.2 is assigned to all routers on a subnet.

The IGMP page provides four tabbed panels, used to configure and manage IGMP in Security Manager:

- IGMP Page - Protocol Tab, page 53-3 – This panel displays interface-specific IGMP parameters; you can disable IGMP and change IGMP parameters.
- IGMP Page - Access Group Tab, page 53-5 – Lets you manage access groups that restrict the multicast sources allowed on an interface.
- IGMP Page - Static Group Tab, page 53-6 – Sometimes, hosts on a network may have a configuration that prevents them from answering IGMP queries; however, you still want multicast traffic to be forwarded to that network segment. There are two methods to pull multicast traffic down to a network segment:
  - Use the Join Group tab to configure the interface as a member of the multicast group. With this method, the security appliance accepts the multicast packets in addition to forwarding them to the specified interface.
  - Use the Static Group tab to configure the security appliance to be a statically connected member of a group. With this method, the security appliance does not accept the packets itself, but only forwards them. Therefore, this method allows fast switching. The outgoing interface appears in the IGMP cache, but itself is not a member of the multicast group.

  Use this tab to statically assign a multicast group to an interface, or change existing static group assignments.
- IGMP Page - Join Group Tab, page 53-7 – Use this tab to manage the multicast groups to which the security appliance belongs.

Note If you simply want to forward multicast packets for a specific group to an interface without the security appliance accepting those packets as part of the group, see IGMP Page - Static Group Tab, page 53-6.

Navigation Path

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

IGMP Page - Protocol Tab

Use the Protocol tab to configure IGMP parameters for an interface on the security appliance.

Navigation Path

You can access the Protocol tab from the IGMP page. For more information about the IGMP page, see Configuring IGMP, page 53-2.

Related Topics

- Configure IGMP Parameters Dialog Box, page 53-4
- Enabling PIM and IGMP, page 53-1
- Configuring PIM, page 53-11
- Configuring Multicast Routes, page 53-8

Field Reference

Table 53-1 Protocol Tab

Element	Description
Protocol Table	
Interface	The name of the interface to which the IGMP settings apply.
Enabled	Indicates whether IGMP is enabled on the interface.
Version	The version of IGMP enabled on the interface.
Query Interval	The interval, in seconds, at which the designated router sends IGMP host-query messages. Valid values range from 1 to 3600 seconds. The default value is 125 seconds.
Query Timeout	The period of time, in seconds, before the security appliance takes over querying the interface, after the previous appliance has stopped doing so. Valid values range from 60 to 300 seconds. The default value is 255 seconds.
Response Time	The maximum response time, in seconds, advertised in IGMP queries. If the security appliance does not receive any host reports within the designated response time, the IGMP group is pruned. Decreasing this value lets the security appliance prune groups faster. Valid values range from 1 to 12 seconds. The default value is 10 seconds. Changing this value is only valid only for IGMP Version 2.
Group Limit	The maximum number of hosts that can join on an interface. Valid values range from 1 to 500. The default value is 500.
Maximum Groups (PIX 6.3)	The maximum number of groups enabled for multicast. Valid values range from 0 to 2000.

Table 53-1 Protocol Tab (Continued)

Element	Description
Forward Interface	The name of the interface to which the selected interface forwards IGMP host reports if IGMP forwarding is enabled.

Configure IGMP Parameters Dialog Box

Use the Configure IGMP Parameters dialog box to configure IGMP parameters for an interface on the security appliance.

Navigation Path

You can access the Configure IGMP Parameters dialog box from the IGMP Page - Protocol tab. For more information, see IGMP Page - Protocol Tab, page 53-3.

Related Topics

- IGMP Page - Protocol Tab, page 53-3
- Configuring IGMP, page 53-2

Field Reference

Table 53-2 Configure IGMP Parameters Dialog Box

Element	Description
Interface	The name of the interface to which the IGMP settings apply.
Forward Interface	The name of the interface to which IGMP host reports are forwarded if IGMP forwarding is enabled.
Version	The version of IGMP to enable on the interface. Choose 1 to enable IGMP Version 1, or 2 to enable IGMP Version 2. Some features require IGMP Version 2. By default, the security appliance uses IGMP Version 2.
Query Interval	The interval, in seconds, at which the designated router sends IGMP host-query messages. Valid values range from 1 to 3600 seconds. The default value is 125 seconds.
Response Time	The maximum response time, in seconds, advertised in IGMP queries. If the security appliance does not receive any host reports within the designated response time, the IGMP group is pruned. Decreasing this value lets the security appliance prune groups faster. Valid values range from 1 to 12 seconds. The default value is 10 seconds. Changing this value is valid only for IGMP Version 2.
Maximum Groups (PIX 6.3)	The maximum number of groups enabled for multicast. Valid values range from 0 to 2000.
PIX 7.x and ASA Only	
Enable IGMP	When selected, IGMP is enabled on the specified interface.
Group Limit	The maximum number of hosts that can join on an interface. Valid values range from 1 to 500. The default value is 500.

Table 53-2 Configure IGMP Parameters Dialog Box (Continued)

Element	Description
Query Timeout	The period of time, in seconds, before the security appliance takes over querying the interface, after the previous appliance has stopped doing so. Valid values range from 60 to 300 seconds. The default value is 255 seconds.

IGMP Page - Access Group Tab

Use the Access Group tab to control the multicast groups that are allowed on an interface.

The table on this page lists all currently defined multicast access groups, showing for each, the name of the interface or interface role for which the group is defined, the group network(s), and whether this group is permitted or denied. For a detailed explanation of these fields, see Configure IGMP Access Group Parameters Dialog Box, page 53-5.

- To add a multicast access group to the table, click the Add Row button.
- To edit the settings for a group, select it and click the Edit Row button.
- To delete a group, select it and click the Delete Row button.

Navigation Path

You can access the Access Group tab from the Configuring IGMP, page 53-2.

Related Topics

- Enabling PIM and IGMP, page 53-1
- Configuring Multicast Routes, page 53-8

Configure IGMP Access Group Parameters Dialog Box

Use the Configure IGMP Access Group Parameters dialog box to add or modify an access group entry.

Navigation Path

You can access the Configure IGMP Access Group Parameters dialog box from the IGMP Page - Access Group Tab, page 53-5.

Related Topics

- IGMP Page - Access Group Tab, page 53-5
- Configuring IGMP, page 53-2

Field Reference

Table 53-3 Configure IGMP Access Group Parameters Dialog Box

Element	Description
Interface	Enter or Select the name of the interface to which the access group is assigned.

Table 53-3 Configure IGMP Access Group Parameters Dialog Box (Continued)

Element	Description
Multicast Group Network	Enter or Select the multicast group address(es) assigned to the specified interface. 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. Group network addresses can range from 224.0.0.0 to 239.255.255.255.
Action	Choose **permit** if the multicast group is permitted on the interface. Choose **deny** if the multicast group is not permitted.

IGMP Page - Static Group Tab

Use the Static Group tab to statically assign a multicast group to an interface.

Navigation Path

You can access the Static Group tab from the IGMP page. For more information about the IGMP page, see Configuring IGMP, page 53-2.

Related Topics

- Enabling PIM and IGMP, page 53-1
- Configuring Multicast Routes, page 53-8
- Configuring PIM, page 53-11

Field Reference

Table 53-4 Static Group Tab

Element	Description
Interface	The name of the interface with which the static group is associated.
Multicast Group Address	The multicast group address to which this rule applies.

Configure IGMP Static Group Parameters Dialog Box

Use the Configure IGMP Static Group Parameters dialog box to statically assign a multicast group to an interface or to change existing static group assignments.

Navigation Path

You can access the Configure IGMP Static Group Parameters dialog box from the IGMP Page - Static Group tab. For more information, see IGMP Page - Static Group Tab, page 53-6.

Related Topics

- IGMP Page - Static Group Tab, page 53-6
- Configuring IGMP, page 53-2

Field Reference

Table 53-5 Configure IGMP Static Group Parameters Dialog Box

Element	Description
Interface	The name of the interface with which the static group is associated.
Multicast Group	The multicast group address to which this rule applies. The group address must be from 224.0.0.0 to 239.255.255.255.

IGMP Page - Join Group Tab

Use the Join Group tab to configure an interface to be a member of a multicast group.

Navigation Path

You can access the Join Group tab from the IGMP page. For more information about the IGMP page, see Configuring IGMP, page 53-2.

Related Topics

- Enabling PIM and IGMP, page 53-1
- Configuring PIM, page 53-11
- Configuring Multicast Routes, page 53-8

Field Reference

Table 53-6 Join Group Tab

Element	Description
Interface	The name of the interface for which you are configuring multicast group membership.
Multicast Group Address	The multicast group address to which this rule applies.

Configure IGMP Join Group Parameters Dialog Box

Use the Configure IGMP Join Group Parameters dialog box to configure an interface to be a member of a multicast group or to change existing membership information.

Navigation Path

You can access the Configure IGMP Join Group Parameters dialog box from the IGMP Page - Join Group tab. For more information, see IGMP Page - Join Group Tab, page 53-7.

Related Topics

- IGMP Page - Join Group Tab, page 53-7
- Configuring IGMP, page 53-2

Field Reference

Table 53-7 Configure IGMP Join Group Parameters Dialog Box

Element	Description
Interface	The name of the interface for which you are configuring multicast group membership.
Join Group	The multicast group address to which this rule applies. The group address must be from 224.0.0.0 to 239.255.255.255.

Configuring Multicast Routes

Static multicast routes let you separate multicast traffic from unicast traffic. For example, when a path between a source and destination does not support multicast routing, the solution is to configure two multicast devices with a GRE tunnel between them, sending the multicast packets over the tunnel.

Static multicast routes are local to the security appliance and are not advertised or redistributed.

Use the Multicast Routes page to manage static multicast routes—currently defined routes are listed, and you can add, edit and delete static multicast routes.

See Add/Edit MRoute Configuration Dialog Box, page 53-8 for more information about the fields displayed in the table on this page.

Navigation Path

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

Related Topics

- Chapter 53, “Configuring Multicast Policies on Firewall Devices”
- Enabling PIM and IGMP, page 53-1
- Configuring IGMP, page 53-2
- Configuring PIM, page 53-11

Add/Edit MRoute Configuration Dialog Box

Use the Add/Edit MRoute Configuration dialog box to add a static multicast route to the security appliance, or to change an existing route.

Navigation Path

You can access the Add/Edit MRoute Configuration dialog box from the Multicast Routing page. See Configuring Multicast Routes, page 53-8 for more information.

Field Reference

Table 53-8 Add/Edit MRoute Configuration Dialog Box

Element	Description
Source Interface	Enter or Select the incoming interface for the multicast route.
Source Network	Enter the IP address and mask of the multicast source, or select a Networks/Hosts object.
Output Interface/Dense	(Optional) Enter or Select the outgoing interface for the multicast route. If you specify the destination interface, the route is forwarded through the selected interface. If you do not specify a destination interface, then RPF is used to forward the route. You can specify the interface, or the RPF neighbor, but not both at the same time.
Multicast Network (PIX 6.3)	Enter or Select the group that is to receive the multicast packets. This must be a multicast IP address in the range of 224.0.1.0 to 239.255.255.255.
Distance (PIX 7.x, ASA and FWSM)	Enter an administrative distance for the static multicast route. If the static multicast route has the same administrative distance as the unicast route, the static multicast route takes precedence.

Configuring Multicast Boundary Filters

On an ASA running version 7.2(1) or later, you can use the Multicast Boundary Filter page to configure the appliance to act as a boundary between multicast domains. The ASA compares multicast group addresses to an access list, blocking all multicast traffic except that specifically permitted by the list.

The Multicast Boundary Filter page lists all currently defined per-interface boundary filter lists; you can add, edit and delete filter lists from this page.

Refer to Add/Edit MBoundary Configuration Dialog Box, page 53-10 for a description of the fields on this page.

Navigation Path

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

Related Topics

- Add/Edit MBoundary Interface Configuration Dialog Box, page 53-10

Add/Edit MBoundary Configuration Dialog Box

Use the Add/Edit MBoundary Configuration dialog box to add, edit and delete multicast boundary filter lists for individual interfaces.

Navigation Path

You can access the Add/Edit MBoundary Configuration dialog box from the Configuring Multicast Boundary Filters, page 53-9.

Related Topics

- Add/Edit MBoundary Interface Configuration Dialog Box, page 53-10
- Configuring Multicast Boundary Filters, page 53-9

Field Reference

Table 53-9 Add/Edit MBoundary Configuration Dialog Box

Element	Description
Interface	Enter or Select an interface for this multicast boundary.
Remove any Auto_RP group range announcements	If you check this box, Auto-RP messages denied by the boundary access control list for this interface are dropped. This is referred to as AutoFiltering.
Multicast boundary filter configuration list	Lists the multicast group addresses specifically permitted or denied for the specified interface. This list is managed with the Add/Edit MBoundary Interface Configuration Dialog Box, page 53-10 (click Add Row or Edit Row).

Add/Edit MBoundary Interface Configuration Dialog Box

Use this dialog box to define permit or deny multicast group entries for the list in the Add/Edit MBoundary Configuration dialog box.

Navigation Path

You can access the Add/Edit MBoundary Interface Configuration dialog box from the Add/Edit MBoundary Configuration Dialog Box, page 53-10.

Related Topics

- Configuring Multicast Boundary Filters, page 53-9

Field Reference

Table 53-10 Add/Edit MBoundary Interface Configuration Dialog Box

Element	Description
Action	Choose **permit** or **deny** to specify the action taken for this multicast group.

Table 53-10 Add/Edit MBoundary Interface Configuration Dialog Box (Continued)

Element	Description
Multicast Group	Enter a single multicast address, or a multicast group address, to which this action applies. The address must be 0.0.0.0, or from 224.0.0.0 to 239.255.255.255. A group address range can be entered using either a standard subnet mask (e.g., 239.0.0.0 255.0.0.0), or using CIDR prefix notation (e.g., 239.0.0.0/8). You also can Select a named network/host object.

Configuring PIM

Protocol independent multicast (PIM) provides a scalable method for determining the best paths in a network for distributing a specific multicast transmission to each host that has registered using IGMP to receive the transmission. Routers and security devices use PIM to maintain tables for forwarding multicast datagrams.

With PIM sparse mode (PIM SM), which is the default for Cisco routers, when the source of a multicast transmission begins broadcasting, the traffic is forwarded from one multicast router to the next until the packets reach every registered host. If a more direct path to the traffic source exists, the last-hop router sends a join message to the source that causes the traffic to be rerouted along the better path.

Note PIM is not supported with PAT—the PIM protocol does not use ports and PAT only works with protocols that use ports.

When you enable multicast routing on a security appliance, PIM and IGMP are enabled on all interfaces by default. You can disable PIM on a per-interface basis.

The PIM page provides up to six tabbed panels:

- PIM Page - Protocol Tab, page 53-12 – Lets you manage interface-specific PIM properties.
- PIM Page - Neighbor Filter Tab, page 53-13 – Lets you manage neighbor filters for individual interfaces; available only on ASA 7.2(1)+ devices.
- PIM Page - Bidirectional Neighbor Filter Tab, page 53-14 – Lets you manage bidirectional neighbor filters for individual interfaces; available only on ASA 7.2(1)+ devices.
- PIM Page - Rendezvous Points Tab, page 53-15 – When you configure PIM, you must choose one or more devices to operate as the rendezvous point (RP). An RP is a single, common root of a shared distribution tree and is statically configured on each device. First-hop routers use the RP to send registration packets on behalf of the source multicast hosts.
- PIM Page - Route Tree Tab, page 53-17 – By default, PIM leaf routers join the shortest-path tree immediately after the first packet arrives from a new source. This reduces delay, but requires more memory than shared tree. You can configure whether the security appliance should join shortest-path tree, or use a shared tree, either for all multicast groups or only for specific multicast addresses.
- PIM Page - Request Filter Tab, page 53-18 – When the security appliance is acting as an RP, you can restrict specific multicast sources from registering. This prevents unauthorized sources from registering with the RP. The Request Filter panel lets you define the multicast sources from which the security appliance will accept PIM registration messages.

PIM Page - Protocol Tab

Use the Protocol tab to configure PIM properties for the interfaces on a security appliance (not available on PIX 6.3 devices). All currently configured interfaces are listed; you can add, edit and delete entries on this panel.

Refer to Add/Edit PIM Protocol Dialog Box, page 53-12 for a description of the fields on this panel.

Navigation Path

You access the Protocol tab from the PIM page. For more information, see Configuring PIM, page 53-11.

Related Topics

- PIM Page - Rendezvous Points Tab, page 53-15
- PIM Page - Route Tree Tab, page 53-17
- PIM Page - Request Filter Tab, page 53-18

Add/Edit PIM Protocol Dialog Box

Use the Add/Edit PIM Protocol dialog box to configure PIM properties for an interface on a security appliance running PIX 7.x or later.

About the Designated Router

The DR is responsible for sending PIM register, join, and prune messaged to the Rendezvous Point (RP). When there is more than one multicast routing device on a network segment, there is an election process to select the Designated Router based on DR priority. If multiple devices have the same DR priority, then the device with the highest IP address becomes the DR. By default, security appliances have a DR priority of 1.

Navigation Path

You can access the Add/Edit PIM Protocol dialog box from the PIM Page - Protocol Tab, page 53-12.

Field Reference

Table 53-11 Add/Edit PIM Protocol Dialog Box

Element	Description
Interface	Enter or Select the interface on which you are configuring PIM.
Enable PIM	When checked, PIM is enabled on the selected interface. You can deselect this option to disable PIM on the interface without deleting this PIM Protocol entry from the table.
DR Priority	The designated router (DR) priority for this interface. The router with the highest DR priority on subnet becomes the designated router. Valid values range from 0 to 4294967294. The default DR priority is 1. Setting this value to zero makes the security appliance interface ineligible to become the default router.
Hello Interval (seconds)	The frequency, in seconds, at which the interface sends PIM hello messages. Valid values range from 1 to 3600 seconds; the default value is 30 seconds.

Table 53-11 Add/Edit PIM Protocol Dialog Box (Continued)

Element	Description
Join-Prune Interval (seconds)	The frequency, in seconds, at which the interface sends PIM join and prune advertisements. Valid values range from 10 to 600 seconds; the default value is 60 seconds.

PIM Page - Neighbor Filter Tab

A PIM neighbor filter is an access control list (ACL) that defines the neighbor devices that can participate in PIM. If a neighbor filter is not configured for an interface, then there are no restrictions. If a PIM neighbor filter is configured, only those neighbors permitted by the filter list can participate in PIM with the security appliance.

On an ASA running version 7.2(1) or later, you can use the Neighbor Filter tab to control the devices that can become PIM neighbors. This panel is used to define and manage the per-interface neighbor filter list. Refer to Add/Edit PIM Neighbor Filter Dialog Box, page 53-13 for a description of the fields on this panel.

Navigation Path

You access the Protocol tab from the PIM page. For more information, see Configuring PIM, page 53-11.

Related Topics

- PIM Page - Protocol Tab, page 53-12
- PIM Page - Bidirectional Neighbor Filter Tab, page 53-14
- PIM Page - Rendezvous Points Tab, page 53-15
- PIM Page - Route Tree Tab, page 53-17
- PIM Page - Request Filter Tab, page 53-18

Add/Edit PIM Neighbor Filter Dialog Box

Use the Add/Edit PIM Neighbor Filter dialog box to add and edit entries in the PIM neighbor filter ACL displayed on the Neighbor Filter panel of the PIM page.

Navigation Path

You can access the Add/Edit PIM Neighbor Filter dialog box from the PIM Page - Neighbor Filter Tab, page 53-13.

Field Reference

Table 53-12 Add/Edit PIM Neighbor Filter Dialog Box

Element	Description
Interface	Enter or Select the interface to which this PIM Neighbor filter entry will be applied.

Table 53-12 Add/Edit PIM Neighbor Filter Dialog Box (Continued)

Element	Description
Neighbor Filter Group	Enter a single multicast address, or a multicast group address, to which the chosen Action applies. A group address range can be entered using either a standard subnet mask (e.g., 239.0.0.0 255.0.0.0), or using CIDR prefix notation (e.g., 239.0.0.0/8). You also can Select a named network/host object.
Action	Choose **permit** to allow the specified neighbors to participate in PIM, or **deny** to prevent the specified neighbors from participating in PIM.

PIM Page - Bidirectional Neighbor Filter Tab

A PIM bidirectional neighbor filter is an access control list (ACL) that defines the neighbor devices that can participate in the bidirectional trees and designated forwarder (DF) election. If a PIM bidirectional neighbor filter is not configured for an interface, then there are no restrictions. If a PIM bidirectional neighbor filter is configured, only those neighbors permitted by the ACL can participate in DF election process.

The PIM bidirectional neighbor filters enable the transition from a sparse-mode-only network to a "bidir" network by letting you specify the devices that should participate in DF election, while still allowing all devices to participate in the sparse-mode domain. The bidir-enabled devices can elect a DF from among themselves, even when there are non-bidir devices on the segment. Multicast boundaries on the non-bidir devices prevent PIM messages and data from the bidir groups from leaking in or out of the bidir subset cloud.

Bidirectional PIM allows multicast devices to maintain reduced state information. All of the multicast devices in a segment must be bidirectionally enabled for bidir to elect a DF.

When a PIM bidirectional neighbor filter is enabled, the routers and other devices that are permitted by the ACL are considered to be bidir-capable. Therefore:

- If a permitted neighbor does not support bidir, the DF election does not occur.
- If a denied neighbor supports bidir, then DF election does not occur.
- If a denied neighbor does not support bidir, the DF election can occur.

Managing the Bidirectional Neighbor Filter List

On an ASA running version 7.2(1) or later, you can use this panel to define and manage the per-interface bidirectional neighbor filter list, permitting or denying multicast source addresses for specific interfaces. Refer to Add/Edit PIM Bidirectional Neighbor Filter Dialog Box, page 53-15 for a description of the fields on this panel.

Navigation Path

You access the Bidirectional Neighbor Filter tab from the PIM page. For more information, see Configuring PIM, page 53-11.

Related Topics

- PIM Page - Protocol Tab, page 53-12
- PIM Page - Neighbor Filter Tab, page 53-13
- PIM Page - Rendezvous Points Tab, page 53-15

- PIM Page - Route Tree Tab, page 53-17
- PIM Page - Request Filter Tab, page 53-18

Add/Edit PIM Bidirectional Neighbor Filter Dialog Box

Use the Add/Edit PIM Bidirectional Neighbor Filter dialog box to add or edit an entry in the bidirectional neighbor access control list displayed on the PIM Page - Bidirectional Neighbor Filter Tab, page 53-14.

Navigation Path

You can access the Add/Edit PIM Bidirectional Neighbor Filter dialog box from the PIM Page - Bidirectional Neighbor Filter Tab, page 53-14.

Field Reference

Table 53-13 Add/Edit PIM Bidirectional Neighbor Filter Dialog Box

Element	Description
Interface	Enter or Select the interface to which this PIM Bidirectional Neighbor filter entry will be applied.
Neighbor Filter Group	Enter a single multicast address, or a multicast group address, to which the chosen Action applies. A group address range can be entered using either a standard subnet mask (e.g., 239.0.0.0 255.0.0.0), or using CIDR prefix notation (e.g., 239.0.0.0/8). You also can Select a named network/host object.
Action	Choose **permit** to allow the specified neighbors to participate in the DF election process, or **deny** to prevent the specified neighbors from participating in the process.

PIM Page - Rendezvous Points Tab

When you configure PIM, you must choose one or more routers or routing devices to operate as the RP. An RP is a single, common root of a shared distribution tree and is statically configured on each device. First hop routers use the RP to send register packets on behalf of the source multicast hosts.

You can configure a single RP to serve more than one group. If a specific group is not specified, the RP for the group is applied to the entire IP multicast group range (224.0.0.0/4).

Use the Rendezvous Points panel to define rendezvous points. You can configure more than one RP, but you cannot have more than one entry with the same RP.

Navigation Path

You access the Rendezvous Points tab from the PIM page. For more information, see Configuring PIM, page 53-11.

Related Topics

- PIM Page - Protocol Tab, page 53-12
- PIM Page - Route Tree Tab, page 53-17
- PIM Page - Request Filter Tab, page 53-18

Field Reference

Table 53-14 Rendezvous Points Tab

Element	Description
Generate older IOS compatible register messages	Check this box if your rendezvous point is a Cisco IOS router. The security appliance software accepts register messages with the checksum calculated on the PIM header and only the next 4 bytes, while Cisco IOS software accepts register messages with the checksum calculated on the entire PIM message for all PIM message types.
Rendezvous Points table	Lists the rendezvous points currently configured on the security appliance. Use the Add Row, Edit Row and Delete Row buttons to manage this list; the Add Row and Edit Row buttons open the Add/Edit Rendezvous Point Dialog Box, page 53-16.

Add/Edit Rendezvous Point Dialog Box

Use the Add/Edit Rendezvous Point dialog box to add an entry to the Rendezvous Points table, or to edit an existing rendezvous point entry. Please note the following:

- You cannot use the same rendezvous point address twice.
- You cannot specify “All Groups” for more than one rendezvous point.

Navigation Path

You can access the Add/Edit Rendezvous Point dialog box from the PIM Page - Rendezvous Points Tab, page 53-15.

Field Reference

Table 53-15 Add/Edit Rendezvous Point Dialog Box

Element	Description
Rendezvous Point IP Address	Enter the IP address of the rendezvous point. This is a unicast address. You also can click Select to select a Networks/Hosts object. When editing a rendezvous point entry, you cannot change this value.
Use bi-directional forwarding	Check this box if you want the specified Multicast Groups to operate in bidirectional mode. In bidirectional mode, if the security appliance receives a multicast packet and has no directly connected members or PIM neighbors present, it sends a Prune message back to the source. Deselect this option if you want the specified Multicast Groups to operate in Sparse Mode. **Note** The security appliance always advertises bidirectional capability in PIM hello messages regardless of the actual bidir configuration.
Use this RP for All Multicast Groups	Select this option to use the specified Rendezvous Point for all multicast groups on the interface.
Use this RP for the Multicast Groups as specified below	Select this option to define the multicast groups that are to use the specified Rendezvous Point; the Multicast Groups table is activated.

Table 53-15 Add/Edit Rendezvous Point Dialog Box (Continued)

Element	Description
Multicast Groups table	The multicast groups currently associated with the specified Rendezvous Point are listed. Table entries are processed from the top down. For example, you can create an entry that includes a range of multicast groups, and then exclude specific groups within that range by placing deny rules for those specific groups at the top of the table. That is, the permit rule for the range of multicast groups follows the individual deny statements. Use the buttons at the bottom of the table to open the Add/Edit Multicast Group Rules Dialog Box, page 53-17 to add or edit an entry; to delete an entry; and to move entries up or down in the table.

Add/Edit Multicast Group Rules Dialog Box

Use the Add/Edit Multicast Group Rules dialog box to create a multicast group rule, or modify a multicast group rule, for the Multicast Groups table in the Add/Edit Rendezvous Point dialog box. This dialog box is also used to specify individual multicast groups that use Shared Tree route filtering on the Route Tree tab

Navigation Path

When defining Rendezvous Points, you access the Add/Edit Multicast Group Rules dialog box from the Add/Edit Rendezvous Point Dialog Box, page 53-16. See PIM Page - Rendezvous Points Tab, page 53-15 for more information.

When specifying how PIM register messages are filtered, you open this dialog box by clicking Add Row or Edit row buttons below the Multicast Groups table on the PIM Page - Route Tree Tab, page 53-17.

Field Reference

Table 53-16 Add/Edit Multicast Group Rules Dialog Box

Element	Description
Action	Choose **permit** to create a group rule that allows the specified multicast addresses; choose **deny** to create a group rule that denies the specified multicast addresses.
Multicast Group Network	Enter the multicast address and network mask associated with the group, or Select the desired Networks/Hosts object.

PIM Page - Route Tree Tab

If the security appliance is acting as a Rendezvous Point, use the Route Tree tab to specify how the PIM register messages from various sources are filtered: shortest-path tree or shared tree, either for all multicast groups or only for specific multicast addresses.

Navigation Path

You can access the Route Tree tab from the PIM page. For more information, see Configuring PIM, page 53-11.

Related Topics

- PIM Page - Protocol Tab, page 53-12
- PIM Page - Rendezvous Points Tab, page 53-15
- PIM Page - Request Filter Tab, page 53-18

Field Reference

Table 53-17 Route Tree Tab

Element	Description
If.., specify how the PIM register messages from various sources are filtered	Select a tree/groups option: • **Use Shortest Path Tree for All Groups** – The security appliance uses shortest-path tree for all multicast groups. • **Use Shared Tree for All Groups** – The security appliance uses shared tree for all multicast groups. • **Use Shared Tree for the Groups specified below** – The security appliance uses shared tree for those groups specified below in the Multicast Groups table. Shortest-path tree is used for any group not listed in the Multicast Groups table.
Multicast Groups table	The multicast groups using Shared Tree are listed. Table entries are processed from the top down. For example, you can create an entry that includes a range of multicast groups, and then exclude specific groups within that range by placing deny rules for those specific groups at the top of the table. That is, the permit rule for the range of multicast groups follows the individual deny statements. Use the buttons at the bottom of the table to open the Add/Edit Multicast Group Rules Dialog Box, page 53-17 to add or edit an entry; to delete an entry; and to move entries up or down in the table.

PIM Page - Request Filter Tab

When the security appliance acts as a rendezvous point, you can restrict specific multicast sources from registering with it. This prevents unauthorized sources from registering with the rendezvous point. You can use the Request Filter tab to define the multicast sources from which the security appliance accepts and denies PIM register messages.

Navigation Path

You can access the Request Filter tab from the PIM page. For more information, see Configuring PIM, page 53-11.

Related Topics

- PIM Page - Protocol Tab, page 53-12
- PIM Page - Rendezvous Points Tab, page 53-15
- PIM Page - Route Tree Tab, page 53-17

Field Reference

Table 53-18 Request Filter Tab

Element	Description
Filter PIM register messages using	Choose how PIM register messages are filtered for different multicast groups: • **None** – Do not filter PIM register messages. • **route-map** – Filter PIM register messages using a specified route map; the Route Map field is activated. Only PIM register messages that are permitted by the route map are allowed to reach the rendezvous point. • **access-list** – Filter PIM register messages using an access list; the Multicast Groups table is activated. Only PIM register messages that are permitted by the access list are allowed to reach the rendezvous point.
Route Map	When **route-map** is the chosen filter, enter a route-map name. Use standard host ACLs in the referenced route map; extended ACLs are not supported. **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.
Multicast Groups table	Lists the currently defined multicast group Request Filter rules. Table entries are processed from the top down. For example, you can create an entry that includes a range of multicast groups, and then exclude specific groups within that range by placing deny rules for those specific groups at the top of the table. That is, the permit rule for the range of multicast groups follows the individual deny statements. Use the buttons at the bottom of the table to open the Add/Edit Multicast Group Rules Dialog Box, page 53-19 to add or edit an entry; to delete an entry; and to move entries up or down in the table.

Add/Edit Multicast Group Rules Dialog Box

Use the Add/Edit Multicast Group Rules dialog box to define the multicast sources that are denied or permitted to register with the security appliance when the appliance acts as a rendezvous point. You create the filter rules based on the source IP address and the destination multicast address.

Navigation Path

You can access the Add/Edit Multicast Group Rules dialog box from the PIM Page - Request Filter Tab, page 53-18.

Field Reference

Table 53-19 Add/Edit Multicast Group Rules Dialog Box

Element	Description
Action	Choose **permit** to create a rule that allows the specified Source of the specified Destination multicast traffic to register with the security appliance; choose **deny** to create a rule that denies registration to the specified Source/Destination multicast traffic.
Source Network	Enter the IP address and network mask for the source of the register message, or Select the appropriate Networks/Hosts object.
Destination Network	Enter the IP address and network mask for the multicast destination, or Select the appropriate Networks/Hosts object.