



# CHAPTER 15

## Configuring Multicast Routing

Multicast routing is supported in single, routed mode only. This section contains the following topics:

- [Multicast, page 15-1](#)—enable or disable multicast routing on the security appliance.
- [IGMP, page 15-2](#)—configure IGMP on the security appliance.
- [Multicast Route, page 15-7](#)—define static multicast routes.
- [MBoundary, page 15-8](#)—configure boundaries for administratively-scoped multicast addresses.
- [MForwarding, page 15-10](#)—enable or disable multicast forwarding on a per-interface basis.
- [PIM, page 15-11](#)—configure PIM on the security appliance.

## Multicast

The Multicast pane lets you enable multicast routing on the security appliance. Enabling multicast routing enables IGMP and PIM on all interfaces by default. 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.

### Fields

**Enable Multicast Routing**—Check this check box to enable IP multicast routing on the security appliance. Uncheck this check box to disable IP multicast routing. By default, multicast is disabled. Enabling multicast enables multicast on all interfaces. You can disable multicast on a per-interface basis.

### Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

# IGMP

IP hosts use IGMP to report their group memberships to directly connected multicast routers. 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.

For more information about configuring IGMP on the security appliance, see the following:

- [Access Group](#)
- [Join Group](#)
- [Protocol](#)
- [Static Group](#)

## Access Group

Access groups control the multicast groups that are allowed on an interface.

### Fields

- Access Groups—Displays the access groups defined for each interface.

The table entries are processed from the top down. Place more specific entries near the top of the table and more generic entries further down. For example, place an access group entry that permits a specific multicast group near the top of the table and an access group entry below that denies a range of multicast groups, including the group in the permit rule. The group is permitted because the permit rule is enforced before the deny rule.

Double-clicking an entry in the table opens the [Add/Edit Access Group](#) dialog box for the selected entry.

- Interface—Displays the interface the access group is associated with.
- Action—Displays “Permit” if the multicast group address is permitted by the access rule. Displays “Deny” if the multicast group address is denied by the access rule.
- Multicast Group Address—Displays the multicast group address that the access rule applies to.
- Netmask—Displays the network mask for the multicast group address.
- Insert Before—Opens the [Add/Edit Access Group](#) dialog box. Use this button to add a new access group entry before the selected entry in the table.
- Insert After—Opens the [Add/Edit Access Group](#) dialog box. Use this button to add a new access group entry after the selected entry in the table.
- Add—Opens the [Add/Edit Access Group](#) dialog box. Use this button to add a new access group entry at the bottom of the table.
- Edit—Opens the [Add/Edit Access Group](#) dialog box. Use this button to change the information for the selected access group entry.
- Delete—Removes the selected access group entry from the table.

### Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

## Add/Edit Access Group

The Add Access Group dialog box lets you add a new access group to the Access Group Table. The Edit Access Group dialog box lets you change information for an existing access group entry. Some fields may be locked when editing existing entries.

### Fields

- Interface—Choose the interface the access group is associated with. You cannot change the associated interface when you are editing an existing access group.
- Action—Choose “permit” to allow the multicast group on the selected interface. Choose “deny” to filter the multicast group from the selected interface.
- Multicast Group Address—Enter the address of the multicast group the access group applies to.
- Netmask—Enter the network mask for the multicast group address or choose one of the common network masks from the list.

### Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

## Join Group

You can configure the security appliance to be a member of a multicast group. The Join Group pane displays the multicast groups the security appliance is a member of.



### 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 [Static Group](#).

### Fields

- Join Group—Displays the multicast group membership for each interface.
  - Interface—Displays the name of the security appliance interface.
  - Multicast Group Address—Displays the address of a multicast group that the interface belongs to.

- Add—Opens the [Add/Edit IGMP Join Group](#) dialog box. Use this button to add a new multicast group membership to an interface.
- Edit—Opens the [Add/Edit IGMP Join Group](#) dialog box. Use this button to edit an existing multicast group membership entry.

### Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

## Add/Edit IGMP Join Group

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

### Fields

- Interface—Choose the name of the security appliance interface that you are configuring multicast group membership for. If you are editing an existing entry, you cannot change this value.
- Multicast Group Address—Enter the address of a multicast group in this field. The group address must be from 224.0.0.0 to 239.255.255.255.

### Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

## Protocol

The Protocol pane displays the IGMP parameters for each interface on the security appliance.

### Fields

- Protocol—Displays the IGMP parameters set on each interface. Double-clicking a row in the table opens the [Configure IGMP Parameters](#) dialog box for the selected interface.
  - Interface—Displays the name of the interface.
  - Enabled—Displays “Yes” if IGMP is enabled on the interface. Displays “No” if IGMP is disabled on the interface.
  - Version—Displays the version of IGMP enabled on the interface.

- Query Interval—Displays the interval, in seconds, at which the designated router sends IGMP host-query messages.
- Query Timeout—Displays the period of time before which the security appliance takes over as the querier for the interface after the previous querier has stopped doing so.
- Response Time—Displays the maximum response time, in seconds, advertised in IGMP queries. Changes to this setting are valid only for IGMP Version 2.
- Group Limit—Displays the maximum number of groups permitted on an interface.
- Forward Interface—Displays the name of the interface that the selected interface forwards IGMP host reports to.
- Edit—Opens the [Configure IGMP Parameters](#) dialog box for the selected interface.

### Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

## Configure IGMP Parameters

The Configure IGMP Parameters dialog box lets you disable IGMP and change IGMP parameters on the selected interface.

### Fields

- Interface—Displays the name of the interface being configured. You cannot change the information displayed in this field.
- Enable IGMP—Check this check box to enable IGMP on the interface. Uncheck the check box to disable IGMP on the interface. If you enabled multicast routing on the security appliance, then IGMP is enabled by default.
- Version—Choose the version of IGMP to enable on the interface. Choose 1 to enable IGMP Version 1, or 2 to enable IGMP Version 2. Some feature require IGMP Version 2. By default, the security appliance uses IGMP Version 2.
- Query Interval—Enter 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—Enter the period of time, in seconds, before which the security appliance takes over as the querier for the interface after the previous querier has stopped doing so. Valid values range from 60 to 300 seconds. The default value is 255 seconds.
- Response Time—Enter 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—Enter the maximum number of host that can join on an interface. Valid values range from 1 to 500. The default value is 500.

- Forward Interface—Choose the name of an interface to forward IGMP host reports to. Choose “None” to disable host report forwarding. By default, host reports are not forwarded.

### Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

## Static Group

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](#) pane 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 pane 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.

### Fields

- Static Group—Displays the statically assigned multicast groups for each interface.
  - Interface—Displays the name of the security appliance interface.
  - Multicast Group Address—Displays the address of a multicast group assigned to the interface.
- Add—Opens the [Add/Edit IGMP Static Group](#) dialog box. Use this button to assign a new static group to an interface.
- Edit—Opens the [Add/Edit IGMP Static Group](#) dialog box. Use this button to edit an existing static group membership.

### Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

## Add/Edit IGMP Static Group

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

### Fields

- **Interface**—Choose the name of the security appliance interface that you are configuring a multicast group for. If you are editing an existing entry, you cannot change this value.
- **Multicast Group Address**—Enter the address of a multicast group in this field. The group address must be from 224.0.0.0 to 239.255.255.255.

### Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

## Multicast Route

Defining static multicast routes lets 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 and to send the multicast packets over the tunnel.

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

### Fields

- **Multicast Route**—Displays the statically-defined multicast routes on the security appliance. Double-clicking an entry in the table opens the [Add/Edit Multicast Route](#) dialog box for that entry.
  - **Source Address**—Displays the IP address and mask, in CIDR notation, of the multicast source.
  - **Source Interface**—Displays the incoming interface for the multicast route.
  - **Destination Interface**—Displays the outgoing interface for the multicast route.
  - **Admin Distance**—Displays the administrative distance of the static multicast route.
- **Add**—Opens the [Add/Edit Multicast Route](#) dialog box. Use this button to add a new static route.
- **Edit**—Opens the [Add/Edit Multicast Route](#) dialog box. Use this button to change the selected static multicast route.
- **Delete**—Use this button to remove the selected static route.

### Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

## Add/Edit Multicast Route

Use the Add Multicast Route dialog box to add a new static multicast route to the security appliance. Use the Edit Multicast Route dialog box to change an existing static multicast route.

### Fields

- **Source Address**—Enter the IP address of the multicast source. You cannot change this value when editing an existing static multicast route.
- **Source Mask**—Enter the network mask for the IP address of the multicast source or chose a common mask from the list. You cannot change this value when editing an existing static multicast route.
- **Source Interface**—Choose the incoming interface for the multicast route.
- **Destination Interface**—(Optional) Choose 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 choose a destination interface, then RPF is used to forward the route.
- **Admin Distance**—Enter the administrative distance of the static multicast route. If the static multicast route has the same administrative distance as the unicast route, then the static multicast route takes precedence.

### Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

## MBoundary

The MBoundary pane lets you configure a multicast boundary for administratively-scoped multicast addresses. A multicast boundary restricts multicast data packet flows and enables reuse of the same multicast group address in different administrative domains. When a multicast boundary is defined on an interface, only the multicast traffic permitted by the filter ACL passes through the interface.

### Fields

The Multicast Boundary table contains the following information. Double-click a table entry to edit the multicast boundary filter settings.

- **Interface**—Lists the interfaces on the device.

- **Boundary Filter**—Lists the boundary filter entries for the specified interface. If a multicast boundary has not been defined for an interface, then this column displays “No Boundary Filters Configured” for the interface.
- **AutoFilter**—Shows if Auto-RP messages are denied by the boundary ACL. If the AutoFilter is enabled, the ACL also restricts the flow of Auto-RP messages. If the AutoFilter is disabled, all Auto-RP messages are passed by the interface. This setting is disabled by default.

You can perform the following actions on the entries of the Boundary table:

- **Edit**—Opens the Edit Boundary Filter dialog box.

### Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

## Edit Boundary Filter

The Edit Boundary Filter dialog box displays the multicast boundary filter ACL. You can add and remove boundary filter ACL entries using this dialog box.

When the boundary filter configuration is applied to the security appliance, the ACL appears in the running configuration with the name *interface-name\_multicast*, where the *interface-name* is the name of the interface the multicast boundary filter is applied to. If an ACL with that name already exists, a number is appended to the name, for example *inside\_multicast\_1*.

### Fields

- **Interface**—Displays the interface for which you are configuring the multicast boundary filter ACL.
- **Remove any Auto-RP group range**—Check this check box to filter Auto-RP messages from sources denied by the boundary ACL. If not checked, all Auto-RP messages are passed.

The Boundary Filter table contains the following information:

- **Action**—The action for the filter entry. Permit allows the specified traffic to pass. Deny prevents the specified traffic from passing through the interface. When a multicast boundary filter is configured on an interface, multicast traffic is denied by default.
- **Network Address**—The multicast group address of the group being permitted or denied.
- **Netmask**—The network mask applied to the multicast group address.

You can perform the following actions on the Boundary Filter table:

- **Insert**—Inserts a neighbor filter entry before the selected entry.
- **Add**—Adds a neighbor filter entry after the selected entry.
- **Edit**—Edits the selected boundary filter.
- **Delete**—Removes the selected neighbor filter entry.

**Modes**

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

## Add/Edit/Insert Neighbor Filter Entry

The Add/Edit/Insert Neighbor Filter Entry dialog box lets you create the ACL entries for the multicast boundary ACL.

**Fields**

- **Action**—Select Permit or Deny for the neighbor filter ACL entry. Selecting Permit allows the multicast group advertisements through the interface. Selecting Deny prevents the specified multicast group advertisements from passing through the interface. When a multicast boundary is configured on an interface, all multicast traffic is prevented from passing through the interface unless permitted with a neighbor filter entry.
- **Multicast Group Address**—Enter the address of the multicast group being permitted or denied. Valid group addresses are from 224.0.0.0 to 239.255.255.255.
- **Netmask**—Type or select the netmask for the multicast group address.

**Modes**

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

## MForwarding

The MForwarding pane lets you disable and reenable multicast forwarding on a per interface basis. By default, multicast forwarding is enabled on all interfaces.

When multicast forwarding is disabled on an interface, the interface does not accept any multicast packets unless specifically configured through other methods. IGMP packets are also prevented when multicast forwarding is disabled.

**Fields**

- The Multicast Forwarding table displays the following information:

- Interface—Displays the interfaces configured on the security appliance. Click an interface name to select the interface. Double-click an interface name to toggle the Multicast Forwarding Enabled status for the interface.
- Multicast Forwarding Enabled—Displays Yes if multicast forwarding is enabled on the specified interface. Displays No if multicast forwarding is disabled on the specified interface. Double-click this entry to toggle Yes/No for the selected interface.
- Enable—Enables multicast forwarding on the selected interface.
- Disable—Disables multicast forwarding on the selected interface.

### Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

### For More Information

- [Configuring Multicast Routing, page 15-1](#)

## PIM

Routers use PIM to maintaining forwarding tables for forwarding multicast datagrams.

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

For more information about configuring PIM, see the following:

- [Protocol](#)
- [Neighbor Filter, page 15-13](#)
- [Bidirectional Neighbor Filter, page 15-14](#)
- [Rendezvous Points](#)
- [Route Tree](#)
- [Request Filter](#)

## Protocol

The Protocol pane displays the interface-specific PIM properties.

### Fields

- Protocol—Displays the PIM settings for each interface. Double-clicking an entry in the table opens the [Edit PIM Protocol](#) dialog box for that entry.
  - Interface—Displays the name of the security appliance interfaces.

- PIM Enabled—Displays “Yes” if PIM is enabled on the interface, “No” if PIM is not enabled.
- DR Priority—Displays the interface priority.
- Hello Interval—Displays the frequency, in seconds, at which the interface sends PIM hello messages.
- Join-Prune Interval—Displays the frequency, in seconds, at which the interface sends PIM join and prune advertisements.
- Edit—Opens the [Edit PIM Protocol](#) dialog box for the selected entry.

### Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

## Edit PIM Protocol

The Edit PIM Protocol dialog box lets you change the PIM properties for the selected interface.

### Fields

- Interface—*Display only*. Displays the name of the selected interface. You cannot edit this value.
- PIM Enabled—Check this check box to enable PIM on the selected interface. Uncheck this check box to disable PIM on the selected interface.
- DR Priority—Sets the designated router priority for the selected 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 0 makes the security appliance interface ineligible to become the default router.
- Hello Interval—Enter 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.
- Join-Prune Interval—Enter 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.

### Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

## Neighbor Filter

The Neighbor Filter pane displays the PIM neighbor filters, if any, that are configured on the security appliance. A PIM neighbor filter is an 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.

When a PIM neighbor filter configuration is applied to the security appliance, an ACL appears in the running configuration with the name *interface-name\_multicast*, where the *interface-name* is the name of the interface the multicast boundary filter is applied to. If an ACL with that name already exists, a number is appended to the name, for example *inside\_multicast\_1*. This ACL defines which devices can become PIM neighbors of the security appliance.

### Fields

The PIM Neighbor Filter table displays the following information. Double-clicking an entry in the table opens the Edit Neighbor Filter Entry dialog box for the selected entry.

- **Interface**—Displays the name of the interface the PIM neighbor filter entry applies to.
- **Action**—Display “permit” if the specified neighbors are allowed to participate in PIM. Displays “deny” if the specified neighbors are prevented from participating in PIM.
- **Network Address**—The network address of the neighbor or neighbors being permitted or denied.
- **Netmask**—The network mask to use with the Network Address.

You can perform the following actions:

- **Insert**—Click to insert a neighbor filter entry before the selected entry.
- **Add**—Click to add a neighbor filter entry after the selected entry.
- **Edit**—Click to edit the selected neighbor filter entry.
- **Delete**—Click to remove the selected neighbor filter entry.

### Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

### For More Information

[Add/Edit/Insert Neighbor Filter Entry, page 15-13](#)

## Add/Edit/Insert Neighbor Filter Entry

The Add/Edit/Insert Neighbor Filter Entry lets you create ACL entries for the PIM neighbor filter ACL.

### Fields

- **Interface**—Select the name of the interface the PIM neighbor filter entry applies to from the list.

- Action—Select “permit” to allow the specified neighbors to participate in PIM. Select “deny” to prevent the specified neighbors from participating in PIM.
- Network Address—The network address of the neighbor or neighbors being permitted or denied.
- Netmask—The network mask to use with the Network Address.

### Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

## Bidirectional Neighbor Filter

The Bidirectional Neighbor Filter pane shows the PIM bidirectional neighbor filters, if any, that are configured on the security appliance. A PIM bidirectional neighbor filter is an ACL that defines the neighbor devices that can participate in the 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.

When a PIM bidirectional neighbor filter configuration is applied to the security appliance, an ACL appears in the running configuration with the name *interface-name\_multicast*, where the *interface-name* is the name of the interface the multicast boundary filter is applied to. If an ACL with that name already exists, a number is appended to the name, for example *inside\_multicast\_1*. This ACL defines which devices can become PIM neighbors of the security appliance.

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

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

When a PIM bidirectional neighbor filter is enabled, the routers 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.

### Fields

The PIM Bidirectional Neighbor Filter table contains the following entries. Double-click an entry to open the Edit Bidirectional Neighbor Filter Entry dialog box for that entry.

- Interface—Displays the interface the bidirectional neighbor filter applies to.

- **Action**—Displays “permit” if the bidirectional neighbor filter entry allows participation in the DF election process. Display “deny” if the entry prevents the specified addresses from participating in the DF election process.
- **Network Address**—The address being permitted or denied.
- **Netmask**—The network mask to apply to the Network Address.

You can perform the following actions:

- **Insert**—Click to insert a bidirectional neighbor filter entry before the selected entry.
- **Add**—Click to add a bidirectional neighbor filter entry after the selected entry.
- **Edit**—Click to edit the selected bidirectional neighbor filter entry.
- **Delete**—Click to remove the selected bidirectional neighbor filter entry.

### Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

### For More Information

[Add/Edit/Insert Bidirectional Neighbor Filter Entry, page 15-15](#)

## Add/Edit/Insert Bidirectional Neighbor Filter Entry

The Add/Edit/Insert Bidirectional Neighbor Filter Entry dialog box lets you create ACL entries for the PIM bidirectional neighbor filter ACL.

### Fields

- **Interface**—Select the interface for which you are configuring the PIM bidirectional neighbor filter ACL entry.
- **Action**—Select permit to allow the specified devices to participate in the DF election. Select deny to prevent the specified devices from participating in the DF election.
- **Network Address**—The network address of the neighbor or neighbors being permitted or denied.
- **Netmask**—The network mask to use with the Network Address.

### Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

## Rendezvous Points

When you configure PIM, you must choose one or more routers to operate as the RP. An RP is a single, common root of a shared distribution tree and is statically configured on each router. 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).

You can configure more than one RP, but you cannot have more than one entry with the same RP.

### Fields

- Generate IOS compatible register messages—Check this check box if your RP is a Cisco IOS router. The security appliance software accepts register messages with the checksum on the PIM header and only the next 4 bytes rather than using the Cisco IOS software method—accepting register messages with the checksum on the entire PIM message for all PIM message types.
- Rendezvous Points—Displays the RPs configured on the security appliance.
  - Rendezvous Point—Displays the IP address of the RP.
  - Multicast Groups—Displays the multicast groups associated with the RP. Displays “--All Groups--” if the RP is associated with all multicast groups on the interface.
  - Bi-directional—Displays “Yes” if the specified multicast groups are to operate in bidirectional mode. Displays “No” if the specified groups are to operate in sparse mode.
- Add—Opens the [Add/Edit Rendezvous Point](#) dialog box. Use this button to add a new RP entry.
- Edit—Opens the [Add/Edit Rendezvous Point](#) dialog box. Use this button to change an existing RP entry.
- Delete—Removes the selected RP entry from the Rendezvous Point table.

### Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

## Add/Edit Rendezvous Point

The Add Rendezvous Point dialog box lets you add a new entry to the Rendezvous Point table. The Edit Rendezvous Point dialog box lets you change an existing RP entry.

### Restrictions

- You cannot use the same RP address twice.
- You cannot specify All Groups for more than one RP.

### Fields

- Rendezvous Point IP Address—Enter the IP address of the RP. This is a unicast address. When editing an existing RP entry, you cannot change this value.

- Use bi-directional forwarding—Check this check box if you want the specified multicast groups to operation 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. Uncheck this check box if you want the specified multicast groups to operate in sparse mode.



**Note** The security appliance always advertises the bidir capability in the PIM hello messages regardless of the actual bidir configuration.

- Use this RP for All Multicast Groups—Choose this option to use the specified RP for all multicast groups on the interface.
- Use this RP for the Multicast Groups as specified below—Choose this option to designate the multicast groups to use with specified RP.
- Multicast Groups—Displays the multicast groups associated with the specified RP.

The table entries are processed from the top down. You can create an RP entry that includes a range of multicast groups but excludes specific groups within that range by placing deny rules for the specific groups at the top of the table and the permit rule for the range of multicast groups below the deny statements.

Double-click an entry to open the [Multicast Group](#) dialog box for the selected entry.

- Action—Displays “Permit” if the multicast group is included or “deny” if the multicast group is excluded.
- Multicast Group Address—Displays the address of the multicast group.
- Netmask—Displays the network mask of the multicast group address.
- Insert Before—Opens the [Multicast Group](#) dialog box. Use this button to add a new multicast group entry before the selected entry in the table.
- Insert After—Opens the [Multicast Group](#) dialog box. Use this button to add a new multicast group entry after the selected entry in the table.
- Add—Opens the [Multicast Group](#) dialog box. Use this button to add a new multicast group entry at the bottom of the table.
- Edit—Opens the [Multicast Group](#) dialog box. Use this button to change the information for the selected multicast group entry.
- Delete—Removes the selected multicast group entry from the table.

### Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

## Multicast Group

Multicast groups are lists of access rules that define which multicast addresses are part of the group. A multicast group can contain a single multicast address or a range of multicast addresses. Use the Add Multicast Group dialog box to create a new multicast group rule. Use the Edit Multicast Group dialog box to modify an existing multicast group rule.

### Fields

- Action—Choose “Permit” to create a group rule that allows the specified multicast addresses; choose “Deny” to create a group rule that filters the specified multicast addresses.
- Multicast Group Address—Enter the multicast address associated with the group.
- Netmask—Enter or choose the network mask for the multicast group address.

### Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

## Request Filter

When the security appliance is acting as an RP, you can restrict specific multicast sources from registering with it. This prevents unauthorized sources from registering with the RP. The Request Filter pane lets you define the multicast sources from which the security appliance will accept PIM register messages.

### Fields

- Multicast Groups—Displays the request filter access rules.

The table entries are processed from the top down. You can create an entry that includes a range of multicast groups but excludes specific groups within that range by placing deny rules for the specific groups at the top of the table and the permit rule for the range of multicast groups below the deny statements.

Double-click an entry to open the [Request Filter Entry](#) dialog box for the selected entry.

- Action—Displays “Permit” if the multicast source is allowed to register or “deny” if the multicast source is excluded.
- Source—Displays the address of the source of the register message.
- Destination—Displays the multicast destination address.
- Insert Before—Opens the [Request Filter Entry](#) dialog box. Use this button to add a new multicast group entry before the selected entry in the table.
- Insert After—Opens the [Request Filter Entry](#) dialog box. Use this button to add a new multicast group entry after the selected entry in the table.
- Add—Opens the [Request Filter Entry](#) dialog box. Use this button to add a new multicast group entry at the bottom of the table.

- Edit—Opens the [Request Filter Entry](#) dialog box. Use this button to change the information for the selected multicast group entry.
- Delete—Removes the selected multicast group entry from the table.

### Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

## Request Filter Entry

The Request Filter Entry dialog box lets you define the multicast sources that are allowed to register with the security appliance when the security appliance acts as an RP. You create the filter rules based on the source IP address and the destination multicast address.

### Fields

- Action—Choose “Permit” to create a rule that allows the specified source of the specified multicast traffic to register with the security appliance; choose “Deny” to create a rule that prevents the specified source of the specified multicast traffic from registering with the security appliance.
- Source IP Address—Enter the IP address for the source of the register message.
- Source Netmask—Enter or choose the network mask for the source of the register message.
- Destination IP Address—Enter the multicast destination address.
- Destination Netmask—Enter or choose the network mask for the multicast destination address.

### Modes

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

## Route Tree

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 shared tree, either for all multicast groups or only for specific multicast addresses.

### Fields

- Use Shortest Path Tree for All Groups—Choose this option to use shortest-path tree for all multicast groups.

- Use Shared Tree for All Groups—Choose this option to use shared tree for all multicast groups.
- Use Shared Tree for the Groups specified below—Choose this option to use shared tree for the groups specified in the Multicast Groups table. Shortest-path tree is used for any group not specified in the Multicast Groups table.
- Multicast Groups—Displays the multicast groups to use Shared Tree with.

The table entries are processed from the top down. You can create an entry that includes a range of multicast groups but excludes specific groups within that range by placing deny rules for the specific groups at the top of the table and the permit rule for the range of multicast groups below the deny statements.

Double-click an entry to open the **Multicast Group** dialog box for the selected entry.

- Action—Displays “Permit” if the multicast group is included or “deny” if the multicast group is excluded.
- Multicast Group Address—Displays the address of the multicast group.
- Netmask—Displays the network mask of the multicast group address.
- Insert Before—Opens the **Multicast Group** dialog box. Use this button to add a new multicast group entry before the selected entry in the table.
- Insert After—Opens the **Multicast Group** dialog box. Use this button to add a new multicast group entry after the selected entry in the table.
- Add—Opens the **Multicast Group** dialog box. Use this button to add a new multicast group entry at the bottom of the table.
- Edit—Opens the **Multicast Group** dialog box. Use this button to change the information for the selected multicast group entry.
- Delete—Removes the selected multicast group entry from the table.

### Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—