CHAPTER 28

IP Access Control Lists

IP access control lists (IP-ACLs) provide basic network security to all switches in the Cisco MDS 9000 Family. IP-ACLs restrict IP-related traffic based on the configured IP filters. A filter contains the rules to match an IP packet, and if the packet matches, the rule also stipulates if the packet should be permitted or denied.

This chapter contains the following sections:

IP-ACL Configuration Guidelines

Each switch running Cisco MDS SAN-OS or Cisco FabricWare can have a maximum of 64 IP-ACLs, and each IP-ACL can have a maximum of 256 filters. IP-ACLs can be associated with the management interface or any Gigabit Ethernet interface on the IP services modules (IPS-4, IPS-8, and MPS-14/2).

Follow these guidelines when configuring IP-ACLs in any switch or director in the Cisco MDS 9000 Family:

- In Cisco MDS SAN-OS Release 1.3 and earlier, you could only apply IP-ACLs to VSAN interfaces and the management interface. As of Cisco MDS SAN-OS Release 2.0(1b), you can also apply IP-ACLs to Gigabit Ethernet interfaces (IP services modules, including MPS-14/2 modules) and Ethernet PortChannel interfaces.

Tip If IP-ACLs are already configured in a Gigabit Ethernet interface, you cannot add this interface to an Ethernet PortChannel group.

Caution Do not apply IP-ACLs to only one member of a PortChannel group. Apply IP-ACLs to the entire channel group.

- Configure the order of conditions accurately. As the IP-ACL filters are sequentially applied to the IP flows, only the first match determines the action taken. Subsequent matches are not considered. Be sure to configure the most important condition first. If no conditions match, the software drops the packet.

Filter Contents

An IP filter contains rules for matching an IP packet based on the protocol, address, port, ICMP type, and type of service (TOS).

Protocol Information

The protocol information is required in each filter. It identifies the name or number of an IP protocol. You can specify the IP protocol in one of two ways:

- Specify an integer ranging from 0 to 255. This number represents the IP protocol.
- Specify the name of a protocol including, but not restricted to, IP, Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Internet Control Message Protocol (ICMP).

Note When configuring IP-ACLs on Gigabit Ethernet interfaces, only use the TCP or ICMP options.

Address Information

The address information is required in each filter. It identifies the following details:

- Source—The address of the network or host from which the packet is being sent.
- Source-wildcard—The wildcard bits applied to the source.
- Destination—The number of the network or host to which the packet is being sent.
- Destination-wildcard—The wildcard bits applied to the destination.

Specify the source and source-wildcard or the destination and destination-wildcard in one of two ways:

- Using the 32-bit quantity in four-part, dotted decimal format (10.1.1.2/0.0.0.0 is the same as host 10.1.1.2).
  - Each wildcard bit set to zero indicates that the corresponding bit position in the packet's IP address must exactly match the bit value in the corresponding bit position in the source.
  - Each wildcard bit set to one indicates that both a zero bit and a one bit in the corresponding position of the packet's IP address will be considered a match to this access list entry. Place ones in the bit positions you want to ignore. For example, 0.0.255.255 to require an exact match of only the first 16 bits of the source. Wildcard bits set to one do not need to be contiguous in the source-wildcard. For example, a source-wildcard of 0.255.0.64 would be valid.
- Using the **any** option as an abbreviation for a source and source-wildcard or destination and destination-wildcard (0.0.0.0/255.255.255.255)

Port Information

The port information is optional. You can specify the port information in one of two ways:

- Specify the number of the port. Port numbers range from 0 to 65535. Table 28-1 displays the port numbers recognized by the Cisco MDS SAN-OS software for associated TCP and UDP ports.
- Specify the name of a TCP or UDP port as follows:
  - TCP port names can only be used when filtering TCP.
  - UDP port names can only be used when filtering UDP.

Table 28-1 TCP and UDP Port Numbers

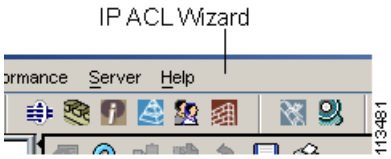
Protocol	Port	Number
UDP	dns	53
	tftp	69
	ntp	123
	radius accounting	1646 or 1813
	radius authentication	1645 or 1812
	snmp	161
	snmp-trap	162
	syslog	514
TCP	ftp	20
	ftp-data	21
	ssh	22
	telnet	23
	smtp	25
	tasacs-ds	65
	www	80
	sftp	115
	http	143
	wbem-http	5988
	wbem-https	5989

Using the IP-ACL Wizard

To use the IP-ACL Wizard to create an ordered list of IP filters in a named IP-ACL profile, follow these steps:

Step 1 In Fabric Manager, choose the **IP-ACL Wizard** icon from the Fabric Manager toolbar. You see the IP-ACL Wizard.

Figure 28-1 IP-ACL Wizard



Step 2 Enter a **Name** for the IP-ACL profile.

Step 3 Click the **Add** button to add a new rule to this IP-ACL profile. You see a new rule in the table with default values.

Step 4 Modify the **Source Ip** and **Source Mask** as necessary for your filter.

Note The IP-ACL Wizard only creates inbound IP filters.

Step 5 Choose the appropriate filter type from the Application column.

Step 6 Choose **permit** or **deny** from the Action column.

Step 7 Repeat Step 3 through Step 6 for additional IP filters.

Step 8 Click **Up** or **Down** to order the filters in this IP-ACL profile.

Tip Order the IP filters carefully. Traffic is compared to the IP filters in order. The first match is applied and the rest are ignored.

Step 9 Click **Next**. You see a list of switches that this IP-ACL profile can be applied to.

Step 10 Uncheck any switches that you do not want this IP-ACL profile applied to.

Step 11 Select the **Interface** you want this IP-ACL applied to.

Step 12 Click **Finish** to create this IP-ACL profile and apply it to the selected switches, or click **Cancel** to exit the IP-ACL Wizard without creating an IP-ACL profile.

Creating Complex IP-ACLs Using Device Manager

The IP-ACL Wizard in Fabric Manager provides tools to create an ordered list of simple IP filters and apply those filters to switches in the fabric.

To create more complex IP-ACLs using Device Manager, follow these steps:

Step 1 Choose **Security > IP ACLs**. You see the IP-ACL dialog box.

Step 2 Click **Create ...** to create an IP-ACL profile.

Step 3 Enter a profile name and click **Create**. This creates an empty, named IP-ACL profile.

Step 4 Click on the IP-ACL profile you created and click **Rules...**. You see the list of IP filters associated with this profile.

Step 5 Click **Create...** to create an IP filter. You see the Create IP Filter dialog box.

Step 6 Choose the **permit** or **deny** Action radio button and set the Internet Protocol Number in the Protocol field. The drop-down menu provides common filtered protocols.

Step 7 Set the source IP address you want this filter to match against and the wildcard mask, or check the **Any** check box to match this filter against any IP address. This creates an IP filter that will check the source IP address of frames.

Note The wildcard mask denotes a subset of the IP Address you want to match against. This allows a range of addresses to match against this filter.

Step 8 Set the transport layer source port range if the protocol chosen is TCP or UDP.

Step 9 Repeat Step 7 and Step 8 for the destination IP address and port range. This creates an IP filter that will check the destination IP address of frames.

Step 10 Set ToS, ICMPType, and ICMPCode as appropriate.

Step 11 Check the **TCPEstablished** check box if you want to match TCP connections with ACK,FIN,PSH,RST,SYN or URG control bits set.

Step 12 Check the **LogEnabled** check box if you want to log all frames that match this IP filter.

Step 13 Click **Create** to create this IP filter and add it to your IP-ACL profile or click **Close** to close the IP Filter dialog box without creating an IP filter.

Any existing IP filters for this IP-ACL profile can be modified from the IP-ACL profiles dialog box but the filters cannot be reordered.

Associating IP-ACL Profiles to Interfaces

To associate the IP-ACL profile to an interface, follow these steps.

Step 1 From Fabric Manager, choose **Switches > Security > IP ACL** from the Physical Attributes pane. You see the IP-ACL configuration in the Information pane.

From Device Manager, choose **Security > IP ACL**. You see the IP-ACL profiles dialog box.

Step 2 Click the **Interfaces** tab.

You see a list of interfaces and associated IP-ACL profiles.

Step 3 Click the **Create Row** icon in Fabric Manager or the **Create** button in Device Manager. You see the Create Interface dialog box.

Step 4 Optionally, select the switches you want to include in the IP-ACL profile by checking the check boxes next to the switch address in Fabric Manager.

Step 5 Set the interface you want associated with an IPA-CL profile in the Interface field.

Step 6 Choose the appropriate ProfileDirection radio button (either **inbound** or **outbound**).

Step 7 Enter the profile name in the Profile Name field.

Note This profile name must already have been created using the Create Profiles dialog box. If not, no filters will be enabled until you to go to the Create Profiles dialog box and create the profile.

Step 8 Click **Create** to associate the profile, or click **Close** to close the Create Interfaces dialog box without associating a profile.

You see the newly associated profile in the list of profiles.

Step 9 Repeat Step 8 to create additional associations, or click the **Close** button to close the Create Interfaces dialog box.

Removing Associations Between IP-ACL Profiles and Interfaces

To delete an IP-ACL profile, you must first delete all associations between that profile and the interfaces.

To remove associations between IP profiles and interfaces using Fabric Manager, follow these steps:

Step 1 Choose **Switches > Security > IP ACL** from the Physical Attributes pane.

You see the IP-ACL configuration in the Information pane.

Step 2 Click the **Interfaces** tab.

You see a list of switches, ACLs, and profile names.

Step 3 Select the row you want to delete. If you want to delete multiple rows, hold down the **Shift** key while selecting rows.

Step 4 Click the **Delete Row** icon.

The interfaces are disassociated from the profile.

Deleting IP Profiles

You must delete the association between IP profiles and interfaces before deleting the IP profile.

To delete an IP profile using Fabric Manager, follow these steps.

Step 1 Choose **Switches > Security > IP ACL** from the Physical Attributes pane.

You see the IP-ACL configuration in the Information pane.

Step 2 Click the **Profiles** tab.

You see a list of switches, ACLs, and profile names.

Step 3 Select the row you want to delete. If you want to delete multiple rows, hold down the Shift key while selecting rows.

Step 4 Click the **Delete Row** icon.

The profiles are deleted.