



CHAPTER 7

Firewall Services

This chapter contains the following topic:

- [FAQs About Firewall Services, page 7-1](#)



Note

For more detailed information on working with firewall services, see the “Managing Firewall Services” chapter in the [User Guide for Cisco Security Manager](#) for your release.

FAQs About Firewall Services

This section answers the following questions about firewall services:

- [Q. Why doesn't the Hit Count report show all ACEs that are discovered for my FWSM devices?](#)
- [Q. Why do I lose my connection after I deploy my firewall rules to an IOS device?](#)
- [Q. Why doesn't the Hit Count report show standard ACLs for my IOS device?](#)
- [Q. Why does the CLI supporting HTTP for authentication proxy remain on the device after I unassign the policy?](#)
- [Q. Why can't I deploy my policies with the BGP routing protocol to IOS devices?](#)
- [Q. Why is an ACE removed from the ACL even though it is bound to the interface?, page 7-2](#)
- [Q. Why am I getting a validation error during the discovery of my transparent firewall rules?, page 7-2](#)
- [Q. How do I create an ACL that permits a range of addresses, as defined in a network/host object, but negates selected addresses within that range?](#)
- [Q. How do I configure the management IP of a security context without going to the device to configure it?](#)
- [Q. Why is the OK button missing on the Combined Rules Results Summary page?](#)
- [Q. Why do I get an error when I try to create a service group from the cell contents of an access rule or AAA rule?](#)

Q. Why doesn't the Hit Count report show all ACEs that are discovered for my FWSM devices?

A. When you run a **show access-list** command in PIX 6.3 and 7.0 devices, all object groups in the ACE are expanded; however, FWSM does not expand object groups when listing access rules if the Object Group Search feature is enabled. If you discover the device, then request a Hit Count report, the report results are not accurate.

- Q.** Why do I lose my connection after I deploy my firewall rules to an IOS device?
- A.** Security Manager does not check whether the firewall rules that you configured in Security Manager permit management traffic (SSH and HTTPS) to the IOS device being managed. As a result, after you deploy firewall rules to the device, connection to the device might be lost. Therefore, we strongly recommend that your ACLs contain a global rule that permits Security Manager to access the device.
- Q.** Why doesn't the Hit Count report show standard ACLs for my IOS device?
- A.** IOS devices use standard ACLs for filtering, which are not recognized when Hit Count reports are generated. After you deploy to the device, standard ACLs are replaced by extended ACLs and the results are displayed in the Hit Count report.
- Q.** Why does the CLI supporting HTTP for authentication proxy remain on the device after I unassign the policy?
- A.** IOS devices require that HTTP be used as the traffic type for authentication proxy, which generates the command **ip http server**. Security Manager does not remove the CLI after you unassign authentication proxy from the device in Security Manager. If you do not plan to run the web server on the IOS device, you can manually remove the CLI or create a FlexConfig object to remove the CLI from the devices.
- Q.** Why can't I deploy my policies with the BGP routing protocol to IOS devices?
- A.** IOS 87x ISR routers do not support BGP as a routing protocol or as a service in ACLs if the device has only 24 MB of memory; however, BGP is supported if the device has more than 24 MB of memory. Security Manager does not detect the amount of memory available on the device and cannot enforce any restrictions. As a result, deploying a job containing an ACL with ACEs having BGP fails. If you create an ACL with a single ACE containing BGP, an empty ACL is created on the device, which you can remove manually.
- Q.** Why is an ACE removed from the ACL even though it is bound to the interface?
- A.** If you import or discover a PIX 6.3 device that has an ACE with the "interface" keyword, then you deploy to the same device without making any changes, the ACE might be removed from the ACL even though it is bound to the interface by the **access-group** command. This can occur if the ACL has other ACEs, or the ACL contains only the ACEs using the "interface" keyword. The **access-group** command for the ACL is removed from the device.
- Q.** Why am I getting a validation error during the discovery of my transparent firewall rules?
- A.** When you configure transparent firewall on IOS devices, only one bridge group is supported. Bridge Group 1 is dedicated to transparent firewall. If you use Bridge Group 1 for something else, and only one interface exists for that group, a validation error results upon discovery.
- Q.** How do I create an ACL that permits a range of addresses, as defined in a network/host object, but negates selected addresses within that range?
- A.** It is not possible to create a network object that includes a range but excludes certain addresses within that range. Instead, create two ACLs. The first ACL should define those addresses that you want to deny. You can create a network/host object for that purpose. The second ACL, which should immediately follow the first, should define the range of permitted addresses, as defined in the other network/host object.
- Q.** How do I configure the management IP of a security context without going to the device to configure it?

- A.** This requires a two-step process. First, you must configure and deploy a management IP policy to the security context. You can then configure the device properties of the security context so that Security Manager uses the management IP to communicate directly with the security context.

-
- Step 1** In the Device selector, select the security context, then select **Platform > Bridging > Management IP** in the Policy selector.
- Step 2** Enter the management IP address and network mask, then click **Save**.
- Step 3** Submit and deploy your changes. Deployment to the security context is performed via the system context. The management IP is now configured on the device.
- Step 4** In the Device selector, right-click the security context, then select **Device Properties**.
- Step 5** On the General page, enter the management IP address in the IP Address field.
- Step 6** Click **Credentials** to display the Credentials page.
- Step 7** Enter the credentials for the security context, then click **Save**. Security Manager can now communicate directly with the security context.
-

- Q.** Why is the OK button missing on the Combined Rules Results Summary page?

- A.** The OK button is not displayed under the following circumstances:
- If you have read-only permissions.
 - If you selected an inherited policy in Device view.

In both cases, the Combined Rules Results Summary displays a preview of what the rules would look like after they are combined, but without the OK button you cannot implement the changes.

To save the changes displayed on the Combine Rules page, you must use an account that has the necessary permissions for modifying policies. For more information, see “Setting Up User Permissions” in the *User Guide for Cisco Security Manager*. When you are working with an inherited policy, run the Combine Rules option from Policy view instead of from Device view.

- Q.** Why do I get an error when I try to create a service group from the cell contents of an access rule or AAA rule?
- A.** You cannot create a service group from a cell that contains a nameless service (that is, a service that you defined directly in the cell, such as tcp/10 or udp/20/30, rather than selecting a service object). First, you must create a service object from each nameless service. Then you can create a service group from the individual services.

