



## CHAPTER 6

# Create Firewall

---

A firewall is a set of rules used to protect the resources of your **LAN**. These rules filter the packets arriving at the router. If a packet does not meet the criteria specified in the rule, it is dropped. If it does meet the criteria, it is allowed to pass through the interface that the rule is applied to. This wizard enables you to create a firewall for your LAN by answering prompts in a set of screens.

In this window, select the type of firewall that you want to create.



### Note

- The router that you are configuring must be using a Cisco IOS image that supports the Firewall feature set in order for you to be able to use Cisco Router and Security Device Manager (Cisco SDM) to configure a firewall on the router.
- The LAN and WAN configurations must be complete before you can configure a firewall.

### Basic Firewall

Click this if you want Cisco SDM to create a firewall using default rules. The use case scenario shows a typical network configuration in which this kind of firewall is used.

Advanced Firewall

Click this if you want Cisco SDM to lead you through the steps of configuring a firewall. You have the option to create a [DMZ](#) network, and to specify an [inspection rule](#). The use case scenario shown when you select this option shows you a typical configuration for an Internet of firewall.

What Do You Want to Do?

If you want to:	Do this:
Have Cisco SDM create a firewall for me. You might want to select this option if you do not want to configure a DMZ network, or if there is only one outside interface.	Click <b>Basic Firewall</b> . Then, click <b>Launch the Selected Task</b> . Cisco SDM asks you to identify the interfaces on your router, and then it uses Cisco SDM default access rules and inspection rules to create the firewall.

If you want to:	Do this:
<p>Have Cisco SDM help me create an Advanced Firewall.</p> <p>If your router has multiple inside and outside interfaces, and you want to configure a DMZ, you should select this option.</p>	<p>Select <b>Advanced Firewall</b>. Then, click <b>Launch the Selected Task</b>.</p> <p>Cisco SDM will show you the default inspection rule and allow you to use it in the firewall. Or, you can create your own inspection rule. Cisco SDM will use a default access rule in the firewall</p>
<p>Get information about a task that this wizard does not help me complete.</p>	<p>Select a topic from the following list:</p> <ul style="list-style-type: none"> <li>• <a href="#">How Do I View Activity on My Firewall?</a></li> <li>• <a href="#">How Do I Configure a Firewall on an Unsupported Interface?</a></li> <li>• <a href="#">How Do I Configure a Firewall After I Have Configured a VPN?</a></li> <li>• <a href="#">How Do I Permit Specific Traffic Through a DMZ Interface?</a></li> <li>• <a href="#">How Do I Modify an Existing Firewall to Permit Traffic from a New Network or Host?</a></li> <li>• <a href="#">How Do I Configure NAT on an Unsupported Interface?</a></li> <li>• <a href="#">How Do I Configure NAT Passthrough for a Firewall?</a></li> <li>• <a href="#">How Do I Permit Traffic Through a Firewall to My Easy VPN Concentrator?</a></li> <li>• <a href="#">How Do I Associate a Rule with an Interface?</a></li> <li>• <a href="#">How Do I Disassociate an Access Rule from an Interface</a></li> <li>• <a href="#">How Do I Delete a Rule That Is Associated with an Interface?</a></li> <li>• <a href="#">How Do I Create an Access Rule for a Java List?</a></li> <li>• <a href="#">How Do I View the IOS Commands I Am Sending to the Router?</a></li> <li>• <a href="#">How Do I Permit Specific Traffic onto My Network if I Don't Have a DMZ Network?</a></li> </ul>

# Basic Firewall Configuration Wizard

Cisco SDM will protect the LAN with a default firewall when you select this option. For Cisco SDM to do this, you must specify the inside and outside interfaces in the next window. Click **Next** to begin configuration.

## Basic Firewall Interface Configuration

Identify the interfaces on the router so that the firewall will be applied to the correct interface.

### Outside (untrusted) Interface

Select the router interface that is connected to the Internet or to your organization's WAN.

**Note**

Do not select the interface through which you accessed Cisco SDM as the outside (untrusted) interface. Doing so will cause you to lose your connection to Cisco SDM. Because it will be protected by a firewall, you will not be able to launch Cisco SDM from the outside (untrusted) interface after the Firewall Wizard completes.

### Allow secure Cisco SDM access from outside interfaces checkbox

Check this box if you want users outside the firewall to be able to access the router using Cisco SDM. The wizard will display a screen that allows you to specify a host IP address or a network address. The firewall will be modified to allow access to the address you specify. If you specify a network address, all hosts on that network will be allowed through the firewall.

### Inside (trusted) Interfaces

Check the physical and logical interfaces connecting to the LAN. You can select multiple interfaces.

## Configuring Firewall for Remote Access

Creating a firewall can block access to the router that remote administrators may need. You can specify the router interfaces to use for remote management access and the hosts from which administrators can log on to Cisco SDM to manage the router. The firewall will be modified to allow secure remote access from the host or network that you specify.

### Select the outside interface

If you are using the Advanced Firewall wizard, select the interface through which users are to launch Cisco SDM. This field does not appear in the Basic Firewall wizard.

### Source Host/Network

If you want to allow a single host access through the firewall, choose **Host Address** and enter the IP address of a host. Choose **Network Address** and enter the address of a network and a subnet mask to allow hosts on that network access through the firewall. The host or network must be accessible from the interface that you specified. Choose **Any** to allow any host connected to the specified interfaces secure access to the network.

## Advanced Firewall Configuration Wizard

Cisco SDM will help you create an [Internet](#) firewall by asking you for information about the interfaces on the router, whether you want to configure a DMZ network, and what rules you want to use in the firewall.

Click **Next** to begin configuration.

## Advanced Firewall Interface Configuration

Identify the router's inside and outside interfaces and the interface that connects to the DMZ network.

Check **outside** or **inside** to identify each interface as an outside or an inside interface. Outside interfaces connect to your organizations's **WAN** or to the Internet. Inside interfaces connect to your **LAN**.

### Allow secure Cisco SDM access from outside interfaces checkbox

Check this box if you want users outside the firewall to be able to access the router using Cisco SDM. The wizard will display a screen that allows you to specify a host IP address or a network address. The firewall will be modified to allow access to the address you specify. If you specify a network address, all hosts on that network will be allowed through the firewall.

### DMZ Interface

Select the router interface that connects to a DMZ network, if one exists. A DMZ network is a buffer zone used to isolate traffic that comes from an untrusted network. If you have a DMZ network, select the interface that connects to it.

## Advanced Firewall DMZ Service Configuration

This window allows you to view rule entries that specify which services available inside the DMZ you want to make available through the router's outside interfaces. Traffic of the specified service types will be allowed through the outside interfaces into the DMZ network.

### DMZ Service Configuration

This area shows the DMZ service entries configured on the router.

#### Start IP Address

The first IP address in the range that specifies the hosts in the DMZ network.

#### End IP Address

The last IP address in the range that specifies the hosts in the DMZ network. If there is no value listed in this column, the IP address in the Start IP address column is presumed to be the only host in the DMZ network. The range can specify a maximum of 254 hosts.

**Service Type**

The type of service, either Transmission Control Protocol (TCP) or User Datagram Protocol (UDP).

**Service**

The name of the service, such as Telnet, or FTP, or a protocol number.

**To configure a DMZ service entry:**

Click **Add**, and create the entry in the DMZ Service Configuration window.

**To edit a DMZ service entry:**

Select the service entry, and click **Edit**. Then, edit the entry in the DMZ Service Configuration window.

## DMZ Service Configuration

Create or edit a DMZ service entry in this window.

**Host IP Address**

Enter the address range that will specify the hosts in the DMZ that this entry applies to. The firewall will allow traffic for the specified TCP or UDP service to reach these hosts.

**Start IP Address**

Enter the first IP address in the range; for example, 172.20.1.1. If Network Address Translation (**NAT**) is enabled, you must enter the NAT-translated address, known as the *inside global address*.

**End IP Address**

Enter the last IP address in the range; for example, 172.20.1.254. If NAT is enabled, you must enter the NAT-translated address.

## Service

### TCP

Click this option if you want to allow traffic for a TCP service.

### UDP

Click this option if you want to allow traffic for a UDP service.

### Service

Enter the service name or number in this field. If you do not know the name or number, click the button and select the service from the list displayed.

## Application Security Configuration

Cisco SDM provides preconfigured application security policies that you can use to protect the network. Use the slider bar to select the security level that you want and to view a description of the security it provides. The wizard summary screen displays the policy name, SDM\_HIGH, SDM\_MEDIUM, or SDM\_LOW and the configuration statements in the policy. You can also view the details of the policy by clicking the Application Security tab and choosing the name of the policy.

### Preview Commands Button

Click to view the IOS commands that make up this policy.

### Custom Application Security Policy Button

This button and the Policy Name field are visible if you are completing the Advanced Firewall wizard. Choose this option if you want to create your own application security policy. If the policy already exists, enter the name in the field, or click the button on the right, choose **Select an existing policy**, and select the policy. To create a policy, click the button, choose **Create a New Policy**, and create the policy in the dialog displayed.



## Domain Name Server Configuration

The router must be configured with the IP address of at least one DNS server for application security to work. Click **Enable DNS-based hostname-to-address** translation, and provide the IP address of the primary DNS server. If a secondary DNS server is available, enter its IP address in the **Secondary DNS Server** field.

The IP addresses that you enter will be visible in the DNS Properties window under Additional Tasks.

## URL Filter Server Configuration

URL filter servers are capable of storing and maintaining much more URL filtering information than a router configuration file can contain. If there are URL filter servers on the network, you can configure the router use them. You can configure additional URL filter server parameters by going to **Configure > Additional Tasks > URL Filtering**. See [URL Filtering](#) for more information.

### Filter HTTP Request through URL Filter Server

Check the **Filter HTTP Request through URL Filter Server** box to enable URL filtering by URL filter servers.

### URL Filter Server Type

Cisco SDM supports the Secure Computing and Websense URL filter servers. Choose either **Secure Computing** or **Websense** to specify the type of URL filter server on the network.

### IP Address/Hostname

Enter the IP address or the hostname of the URL filter server.

## Select Interface Zone

This window appears if a router interface other than the one you are configuring is a member of a Zone-Based Policy Firewall [security zone](#). For more information about this topic, see [Zone-Based Policy Firewall](#).

## Select Zone

Select the security zone that you want the interface to be a member of. If you choose not to assign the interface to a zone, there is a strong possibility that traffic will not pass through the interface.

## ZPF Inside Zones

Zones that include interfaces used in generic routing encapsulation ([GRE](#)) tunnels must be designated as inside (trusted) zones in order for GRE traffic to pass through the firewall.

This window lists the configured zones and their member interfaces. To designate a zone as inside, check the **inside (trusted)** column in the row for that zone.

## Summary

This screen summarizes the firewall information. You can review the information in this screen and use the Back button to return to screens in the wizard to make changes.

The summary screen uses plain-language to describe the configuration. You can view the CLI commands that Cisco SDM delivers to the router by going to Edit > Preferences, and checking **Preview commands before delivering to router**.

## Inside (trusted) Interface(s)

Cisco SDM lists the router's logical and physical interfaces that you designated as the inside interfaces in this wizard session, along with their IP addresses. Underneath, plain-language descriptions are given for each configuration statement applied to the inside interfaces. The following are examples:

```
Inside(trusted) Interfaces:
FastEthernet0/0 (10.28.54.205)
Apply access rule to the inbound direction to deny spoofing traffic.
Apply access rule to the inbound direction to deny traffic sourced
from broadcast, local loopback address.
Apply access rule to the inbound direction to permit all other
traffic.
Apply application security policy SDM_HIGH to the inbound direction.
```

This example shows the Cisco SDM Application Security policy SDM\_HIGH applied to inbound traffic on this interface.

## Outside (untrusted) Interface(s)

Cisco SDM lists the router logical and physical interfaces that you designated as outside interfaces in this wizard session, along with their IP addresses.

Underneath, plain-language descriptions are given for each configuration statement applied to the outside interfaces. The following are examples:

```
FastEthernet0/1 (142.120.12.1)
Turn on unicast reverse path forwarding check for non-tunnel
interfaces.
Apply access rule to the inbound direction to permit IPSec tunnel
traffic if necessary.
Apply access rule to the inbound direction to permit GRE tunnel
traffic for interfaces if necessary.
Apply access rule to the inbound direction to permit ICMP traffic.
Apply access rule to the inbound direction to permit NTP traffic if
necessary.
Apply access rule to the inbound direction to deny spoofing traffic.
Apply access rule to the inbound direction to deny traffic sourced
from broadcast, local loopback and private address.
Apply access rule to the inbound direction to permit service traffic
going to DMZ interface.
Service ftp at 10.10.10.1 to 10.10.10.20
Apply access rule to the inbound direction to permit secure SDM access
from 140.44.3.0 255.255.255.0 host/network
Apply access rule to the inbound direction to deny all other traffic.
```

Note that this configuration turns on reverse path forwarding, a feature that allows the router to discard packets that lack a verifiable source IP address, and permits ftp traffic to the DMZ addresses 10.10.10.1 through 10.10.10.20.

## DMZ Interface

If you configured an Advanced firewall, this area shows you the DMZ interface you designated, along with its IP address. Underneath, Cisco SDM describes what access and inspection rules were associated with this interface. The following are examples:

```
FastEthernet (10.10.10.1)
Apply CBAC inspection rule to the outbound direction
Apply access rule to the inbound direction to deny all other traffic.
```

## To save this configuration to the router's running configuration and leave this wizard:

Click **Finish**. Cisco SDM saves the configuration changes to the router's running configuration. The changes will take effect immediately, but will be lost if the router is turned off.

If you checked **Preview commands before delivering to router** in the User Preferences window, the Deliver configuration to router window appears. In this window, you can view the CLI commands you that are delivering to the router.

## SDM Warning: SDM Access

This window appears when you have indicated that Cisco SDM should be able to access the router from outside interfaces. It informs you that you must ensure that SSH and HTTPS are configured, and that at least one of the interfaces designated as outside be configured with a static IP address. To do this, you must ensure that an outside interface is configured with a static IP address, and then associate a management policy with that interface.

## Determining if an Outside Interface is Configured with a Static IP Address

Complete the following steps to determine if an outside interface is configured with a static IP address.


- 
- Step 1** Click **Configure > Interfaces and Connections > Edit Interface/Connection**.
  - Step 2** Review the IP column in the Interface list table to determine if an outside interface has a static IP addresses.
  - Step 3** If no outside interface has a static IP address, select one and click **Edit** to display a dialog that allows you to reconfigure the IP address information for the interface.

If there is an outside interface with a static IP address, note that interface name and complete the next procedure.

---

## Configuring SSH and HTTPS

Complete the following steps to configure a management policy for SSH and HTTPS on the router.

- 
- Step 1** Click **Configure > Additional Tasks > Router Access > Management Access**.
- Step 2** If there is no management policy, click **Add**. If you want to edit an existing management policy, select the policy and click **Edit**.
-  **Note** If you are editing a management policy it must be associated with an interface that has a static IP address.
- 
- Step 3** In the displayed dialog, enter the address information in the Source Host/Network box. The IP address information that you enter must include the IP address of the PC you will use to manage the router.
- Step 4** Choose an outside interface with a static IP address in the Management Interface box. This interface must have a route to the IP address you specified in the Source Host/Network box.
- Step 5** In the Management Protocols box, check **Allow SDM**.
- Step 6** Check **HTTPS** and **SSH** to allow those protocols.
- Step 7** Click OK to close the dialog.
- Step 8** Click **Apply Changes** in the window that displays management access policies.
- 

## How Do I...

This section contains procedures for tasks that the wizard does not help you complete.

## How Do I View Activity on My Firewall?

Activity on your [firewall](#) is monitored through the creation of log entries. If logging is enabled on the router, whenever an access [rule](#) that is configured to generate log entries is invoked—for example, if a connection were attempted from a denied IP address—then a log entry is generated and can be viewed in Monitor mode.

## Enable Logging

The first step to viewing firewall activity is to enable logging on the router. To enable logging:

- 
- Step 1** From the left frame, select **Additional Tasks**.
  - Step 2** In the Additional Tasks tree, click **Logging** and then click the **Edit** button.
  - Step 3** In the Syslog screen, check **Logging to Buffer**.
  - Step 4** In the Buffer Size field, enter the amount of router memory that you want to use for a logging buffer. The default value is 4096 bytes. A larger buffer will store more log entries but you must balance your need for a larger logging buffer against potential router performance issues.
  - Step 5** Click **OK**.
- 

## Identify the Access Rules for Which You Want to Generate Log Entries

In addition to enabling logging, you must identify the access rules that you want to generate log entries. To configure access rules for generating log entries:

- 
- Step 1** From the left frame, select **Additional Tasks**.
  - Step 2** In the Additional Tasks tree, click **ACL Editor**, and then click **Access Rules**.  
Each access rule appears in the upper table on the right side of the screen. The lower table shows the specific source and destination IP addresses and the services that are permitted or denied by the rule.
  - Step 3** In the upper table, click the rule that you want to modify.
  - Step 4** Click **Edit**.  
The Edit a Rule dialog box appears.
  - Step 5** The Rule Entry field shows each of the source IP/destination IP/service combinations that are permitted or denied by the rule. Click the rule entry that you want to configure to generate log entries.
  - Step 6** Click **Edit**.
  - Step 7** In the rule entry dialog box, check the **Log Matches Against this Entry** check box.

- Step 8** Click **OK** to close the dialog boxes you have displayed.
- The rule entry that you just modified will now generate log entries whenever a connection is attempted from the IP address range and services that the define the rule entry.
- Step 9** Repeat Step 4 through Step 8 for each rule entry that you want to configure to generate log entries.
- 

Once your logging configuration is complete, follow the steps below to view your firewall activity:

---

- Step 1** From the toolbar, select **Monitor Mode**.
- Step 2** From the left frame, select **Firewall Status**.
- In the Firewall statistics, you can verify that your firewall is configured and view how many connection attempts have been denied.
- The table shows each router log entry generated by the firewall, including the time and the reason that the log entry was generated.
- 

## How Do I Configure a Firewall on an Unsupported Interface?

Cisco SDM can configure a [firewall](#) on an interface type unsupported by Cisco SDM. Before you can configure the firewall, you must first use the router [CLI](#) to configure the interface. The interface must have, at a minimum, an IP address configured, and it must be working. For more information on how to configure an interface using the CLI, refer to the Software Configuration Guide for your router.

To verify that the connection is working, verify that the interface status is “Up” in the Interfaces and Connections window.

The following is an excerpt showing the configuration for an ISDN interface on a Cisco 3620 router:

```
!  
isdn switch-type basic-5ess  
!  
interface BRI0/0
```

```

! This is the data BRI WIC
ip unnumbered Ethernet0/0
no ip directed-broadcast
encapsulation ppp
no ip mroute-cache
dialer map ip 100.100.100.100 name junky 883531601
dialer hold-queue 10
isdn switch-type basic-5ess
isdn tei-negotiation first-call
isdn twait-disable
isdn spid1 80568541630101 6854163
isdn incoming-voice modem

```

Other configurations are available in the Software Configuration Guide for your router.

After you have configured the unsupported interface using the CLI, you can use Cisco SDM to configure the firewall. The unsupported interface will appear as “Other” in the fields listing the router interfaces.

## How Do I Configure a Firewall After I Have Configured a VPN?

If a [firewall](#) is placed on an interface used in a VPN, the firewall must permit traffic between the local and remote VPN peers. If you use the Basic or Advanced Firewall wizard, Cisco SDM will automatically permit traffic to flow between VPN peers.

If you create an access rule in the ACL Editor available in Additional Tasks, you have complete control over the permit and deny statements in the rule, and you must ensure that traffic is permitted between VPN peers. The following statements are examples of the types of statements that should be included in the configuration to permit VPN traffic:

```

access-list 105 permit ahp host 123.3.4.5 host 192.168.0.1
access-list 105 permit esp host 123.3.4.5 host 192.168.0.1
access-list 105 permit udp host 123.3.4.5 host 192.168.0.1 eq isakmp
access-list 105 permit udp host 123.3.4.5 host 192.168.0.1 eq
non500-isakmp

```



## How Do I Permit Specific Traffic Through a DMZ Interface?

Follow the steps below to configure access through your firewall to a web server on a [DMZ](#) network:

- 
- Step 1** From the left frame, select **Firewall and ACL**.
  - Step 2** Select **Advanced Firewall**.
  - Step 3** Click **Launch the Selected Task**.
  - Step 4** Click **Next**.  
The Advanced Firewall Interface Configuration screen appears.
  - Step 5** In the Interface table, select which interfaces connect to networks inside your firewall and which interfaces connect to networks outside the firewall.
  - Step 6** From the DMZ Interface field, select the interface that connects to your DMZ network.
  - Step 7** Click **Next>**.
  - Step 8** In the IP Address field, enter the IP address or range of IP addresses of your web server(s).
  - Step 9** From the Service field, select TCP.
  - Step 10** In the Port field, enter **80** or **www**.
  - Step 11** Click **Next>**.
  - Step 12** Click **Finish**.
- 

## How Do I Modify an Existing Firewall to Permit Traffic from a New Network or Host?

You can use the Edit Firewall Policy tab to modify your firewall configuration to permit traffic from a new network or host.

- 
- Step 1** From the left frame, select **Firewall and ACL**.
  - Step 2** Click the **Edit Firewall Policy** tab.

- Step 3 In the traffic selection panel select a From interface and a To interface to specify the traffic flow to which the firewall has been applied, and click **Go**. A firewall icon will appear in the router graphic if a firewall has been applied to the traffic flow. If the traffic flow you select does not display the access rule you need to modify, select a different From interface or a different To interface.
  - Step 4 Examine the access rule in the Service area. Use the **Add** button to display a dialog for a new access rule entry.
  - Step 5 Enter a permit statement for the network or host you want to allow access to the network. Click **OK** in the rule entry dialog.
  - Step 6 The new entry appears in the service area..
  - Step 7 Use the **Cut** and **Paste** buttons to reorder the entry to a different position in the list if you need to do so.
- 

## How Do I Configure NAT on an Unsupported Interface?

Cisco SDM can configure Network Address Translation ([NAT](#)) on an interface type unsupported by Cisco SDM. Before you can configure the firewall, you must first use the router [CLI](#) to configure the interface. The interface must have, at a minimum, an IP address configured, and it must be working. To verify that the connection is working, verify that the interface status is “Up.”

After you have configured the unsupported interface using the CLI, you can configure NAT . The unsupported interface will appear as “Other” on the router interface list.

## How Do I Configure NAT Passthrough for a Firewall?

If you have configured [NAT](#) and are now configuring your firewall, you must configure the [firewall](#) so that it permits traffic from your public IP address. To do this you must configure an [ACL](#). To configure an ACL permitting traffic from your public IP address:

- 
- Step 1 From the left frame, select **Additional Tasks**.
  - Step 2 In the Rules tree, select **ACL Editor** and then **Access Rules**.

- Step 3** Click **Add**.  
The Add a Rule dialog box appears.
- Step 4** In the Name/Number field, enter a unique name or number for the new rule.
- Step 5** From the Type field, choose **Standard Rule**.
- Step 6** In the Description field, enter a short description of the new rule, such as “Permit NAT Passthrough.”
- Step 7** Click **Add**.  
The Add a Standard Rule Entry dialog box appears.
- Step 8** In the Action field, choose **Permit**.
- Step 9** In the Type field, choose **Host**.
- Step 10** In the IP Address field, enter your public IP address.
- Step 11** In the Description field, enter a short description, such as “Public IP Address.”
- Step 12** Click **OK**.
- Step 13** Click **OK**.  
The new rule now appears in the Access Rules table.
- 

## How Do I Permit Traffic Through a Firewall to My Easy VPN Concentrator?

In order to permit traffic through your firewall to a VPN concentrator, you must create or modify access [rules](#) that permit the [VPN](#) traffic. To create these rules:

- 
- Step 1** From the left frame, select **Additional Tasks**.
- Step 2** In the Rules tree, select **ACL Editor** and then **Access Rules**.
- Step 3** Click **Add**.  
The Add a Rule dialog box appears.
- Step 4** In the Name/Number field, enter a unique name or number for this rule.
- Step 5** In the Description field, enter a description of the rule, such as “VPN Concentrator Traffic.”

- Step 6** Click **Add**.  
The Add an Extended Rule Entry dialog box appears.
- Step 7** In the Source Host/Network group, from the Type field, select **A Network**.
- Step 8** In the IP Address and Wildcard Mask fields, enter the IP address and network mask of the VPN source peer.
- Step 9** In the Destination Host/Network group, from the Type field, select **A Network**.
- Step 10** In the IP Address and Wildcard Mask fields, enter the IP address and network mask of the VPN destination peer.
- Step 11** In the Protocol and Service group, select **TCP**.
- Step 12** In the Source port fields, select =, and enter the port number **1023**.
- Step 13** In the Destination port fields, select =, and enter the port number **1723**.
- Step 14** Click **OK**.  
The new rule entry appears in the Rule Entry list.
- Step 15** Repeat Step 7 through Step 15, creating rule entries for the following protocols and, where required, port numbers:
- Protocol **IP**, IP protocol **GRE**
  - Protocol **UDP**, Source Port **500**, Destination Port **500**
  - Protocol **IP**, IP Protocol **ESP**
  - Protocol **UDP**, Source Port **10000**, Destination Port **10000**
- Step 16** Click **OK**.
- 

## How Do I Associate a Rule with an Interface?

If you use the Cisco SDM Firewall wizard, the access and inspection rules that you create are automatically associated with the interface for which you created the firewall. If you are creating a rule in Additional Tasks/ACL Editor, you can associate it with an interface from the [Add or Edit a Rule](#) window. If you do not associate it with an interface at that time, you can still do so later.

- 
- Step 1** Click **Interfaces and Connections** in the left panel and click the **Edit Interfaces and Connections** tab.
  - Step 2** Select the interface that you want to associate a rule with, and click **Edit**.
  - Step 3** In the Association tab, enter the rule name or number in the Inbound or Outbound field in the Access Rule or Inspection Rule boxes. If you want the rule to filter traffic before it enters the interface, use the Inbound field. If you want the rule to filter traffic that has already entered the router, but may exit the router through the selected interface, use the Outbound field.
  - Step 4** Click **OK** in the Association tab.
  - Step 5** In the Access Rules or the Inspection Rules window, examine the Used By column to verify that the rule has been associated with the interface.
- 

## How Do I Disassociate an Access Rule from an Interface

You may need to remove the association between an access rule and an interface. Removing the association does not delete the access rule. You can associate it with other interfaces if you want. To remove the association between an access rule and an interface, perform the following steps.

- 
- Step 1** Click **Interfaces and Connections** in the left panel and click the **Edit Interfaces and Connections** tab.
  - Step 2** Select the interface that you want to disassociate the access rule from.
  - Step 3** Click **Edit**.
  - Step 4** In the Association tab, find the access rule in the inbound or outbound field in the Access Rule box. The access rule may have a name, or a number.
  - Step 5** Click in the inbound or outbound field, and then click the button to the right.
  - Step 6** Click **None (clear rule association)**.
  - Step 7** Click **OK**.
-

## How Do I Delete a Rule That Is Associated with an Interface?

Cisco SDM does not allow you to delete a rule that is associated with an interface; you must first remove the association between the rule and the interface, and then delete the access rule.

- 
- Step 1** Click **Interfaces and Connections** in the left panel and click the **Edit Interfaces and Connections** tab.
  - Step 2** Select the interface that you want to disassociate the rule from.
  - Step 3** Click **Edit..**
  - Step 4** In the Association tab, find the rule in the Access Rule box or the Inspection Rule box. The rule may have a name or a number.
  - Step 5** Find the rule in the association tab. **If it is an access rule, click None (clear rule association). If it is an Inspection rule, click None.**
  - Step 6** Click **OK**.
  - Step 7** Click **Rules** in the left frame. Use the Rules tree to go to the Access Rule or the Inspection Rule window.
  - Step 8** Select the rule that you want to remove, and click **Delete**.

## How Do I Create an Access Rule for a Java List?

Inspection rules allow you to specify Java lists. A Java list is used to permit Java applet traffic from trusted sources. These sources are defined in an access rule that the Java List references. To create this kind of access rule, and use it in a Java list, do the following:

- 
- Step 1** If you are at the Inspection Rules window, and you have clicked **Java List**, click the button to the right of the Number field and click **Create a new rule (ACL) and select**. The Add a Rule window opens.  
If you are at the Access Rules window, click **Add** to open the Add a Rule window.
  - Step 2** From the Add a Rule window, create a standard access rule that permits traffic from the addresses you trust. For example, if you wanted to permit Java applets from hosts 10.22.55.3, and 172.55.66.1, you could create the following access rule entries in the Add a Rule window:

```
permit host 10.22.55.3
permit host 172.55.66.1
```

You can provide descriptions for the entries and a description for the rule.

You do not need to associate the rule with the interface to which you are applying the inspection rule.

- Step 3** Click **OK** in the Add a Rule window.
  - Step 4** If you started this procedure from the Inspection Rules window, then click **OK** in the Java List window. You do not need to complete Step 5 and Step 6.
  - Step 5** If you started this procedure in the Access Rules window, go to the Inspection Rules window and select the inspection rule you want to create a Java list for, and click **Edit**.
  - Step 6** Check **http** in the Protocols column, and click **Java List**.
  - Step 7** In the Java List Number field, enter the number of the access list that you created. Click **OK**.
- 

## How Do I Permit Specific Traffic onto My Network if I Don't Have a DMZ Network?

The Firewall wizard, lets you specify the traffic that you want to allow onto the DMZ. If you do not have a DMZ network, you can still permit specified types of outside traffic onto your network, using the Firewall Policy feature.

- 
- Step 1** Configure a firewall using the Firewall wizard.
  - Step 2** Click **Edit Firewall Policy/ACL**.
  - Step 3** To display the access rule you need to modify, select the outside (untrusted) interface as the From interface, and the inside (trusted) interface as the To interface. The access rule applied to inbound traffic on the untrusted interface is displayed.
  - Step 4** To allow a particular type of traffic onto the network that is not already allowed, click **Add** in the Service area.
  - Step 5** Create the entries you need in the rule entry dialog. You must click **Add** for each entry you want to create.

**Step 6** The entries you create will appear in the entry list in the Service area.

---