CHAPTER **22**

Implementing Cisco IOS Firewalls

Using a router as a firewall is a viable solution for many networks. This chapter explores how to use Cisco IOS Software features to set up and monitor a firewall. Although this chapter does not go into the design concepts of security, it does show you how to quickly configure the Cisco IOS features to secure your network.

"Do I Know This Already?" Quiz

The purpose of the "Do I Know This Already?" quiz is to help you decide whether you really need to read the entire chapter. If you already intend to read the entire chapter, you do not necessarily need to answer these questions now.

The 9-question quiz, derived from the major sections in the "Foundation Topics" portion of the chapter, helps you to determine how to spend your limited study time.

Table 22-1 outlines the major topics discussed in this chapter and the "Do I Know This Already?" quiz questions that correspond to those topics.

Table 22-1	"Do I Know	This Already?"	Foundation Topics	Section-to-Question	Mapping
------------	------------	----------------	-------------------	---------------------	---------

Foundation Topics Section	Questions Covered in This Section	Score
Configure a Cisco IOS Firewall Using the CLI	1–4	
Configure a Basic Firewall Using SDM	5-6	
Configure an Advanced Firewall Using SDM	7–9	
Total Score		

CAUTION The goal of self-assessment is to gauge your mastery of the topics in this chapter. If you do not know the answer to a question or are only partially sure of the answer, you should mark this question wrong for purposes of self-assessment. Giving yourself credit for an answer that you correctly guess skews your self-assessment results and might provide you with a false sense of security.

- 1. Which of the following is the proper syntax to define an inspection rule named "myrule" that will inspect FTP packets?
 - a. ip inspect name inspection-name myrule protocol alert on timeout 30
 - b. ip inspect name myrule protocol ftp alert on timeout 30
 - c. ip inspect name myrule ftp alert on timeout 30
 - d. ip inspect name inspection-name myrule protocol ftp alert on timeout 30
- **2.** Which of the following is the correct command to apply the inspection rule named "myrule" to an interface to inspect packets traveling into the interface?
 - a. ip inspect myrule
 - b. ip inspect in myrule
 - c. ip inspect inbound myrule
 - d. ip inspect myrule in
- 3. Which of the following is the correct syntax used to enable real-time alerts?
 - a. ip-inspect alert
 - b. no ip-inspect alert-off
 - c. ip-inspect alert-on
 - d. ip-inspect alert-on
- 4. What is the default time between alert updates when using IP inspection?
 - a. 10 seconds
 - **b.** 20 seconds
 - c. 30 seconds
 - d. 60 seconds
- 5. Which of the following is true regarding the Basic Firewall Wizard used in SDM?
 - a. The Basic Firewall Wizard allows only two interfaces to be configured.
 - **b**. The Basic Firewall Wizard allows multiple trusted interfaces to be configured.
 - c. The Basic Firewall Wizard allows only one DMZ to be configured.
 - d. The Basic Firewall Wizard allows multiple untrusted interfaces to be configured.
- 6. Which of the following is not true regarding the Basic Firewall Wizard used in SDM?
 - **a.** You may edit policies for a specific protocol and interface within the Basic Firewall Wizard.
 - **b.** You must use the CLI or the Advanced Firewall Wizard to edit policies for a specific protocol on an interface.

- c. You may use the Basic Firewall Wizard on a router with more than two trusted interfaces.
- d. You may use the Basic Firewall Wizard on a router with more than one DMZ.
- 7. Which of the following is true regarding the Advanced Firewall Wizard?
 - **a.** You must already have defined a security policy in order to use it inside the Advanced Firewall Wizard.
 - **b.** There are four default application security policies built into SDM (None, Low, Medium, and High).
 - **c.** There are three default application security policies built into SDM (Low, Medium, and High).
 - **d**. Application security policies are not used in conjunction with the Advanced Firewall Wizard.
- 8. Which of the following is true regarding the Advanced Firewall Wizard?
 - a. Auditing is configured on a global level, affecting all protocols simultaneously.
 - **b**. Auditing is available only if logging is enabled.
 - c. Auditing is configured on a per-protocol level.
 - d. Logging is available only if auditing has been enabled.
- 9. Which is true regarding the Advanced Firewall Wizard?
 - a. Logging must be configured through the CLI before starting the wizard.
 - **b**. Logging may be configured through the wizard.
 - c. The logging hosts must be configured through the CLI before starting the wizard
 - d. The wizard allows a maximum of three logging hosts.

The answers to the "Do I Know This Already?" quiz are found in Appendix A, "Answers to the 'Do I Know This Already?' Quizzes and Q&A Sections." The suggested choices for your next step are as follows:

- **5 or fewer overall score**—Read the entire chapter. This includes the "Foundation Topics," "Foundation Summary," and "Q&A" sections.
- 6 or 7 overall score—Begin with the "Foundation Summary" section, and then go to the "Q&A" section.
- 8 or 9 overall score—If you want more review on these topics, skip to the "Foundation Summary" section, and then go to the "Q&A" section. Otherwise, move to the next chapter.

Foundation Topics

Configure a Cisco IOS Firewall Using the CLI

Configuring a Cisco IOS firewall using the CLI is simple. You already know how to make and access ACLs. A Cisco IOS firewall allows you to add inspection rules to the interface. An inspection rule is simply another method of ensuring the safety of that interface. The router drops packets that are unsafe in the context of the already established connections. For example, when a TCP inspection rule is added to an interface, a TCP reset (RST) packet is not allowed into the interface unless there has previously been a TCP connection established with the machine sending the reset.

When using inspection rules, you must apply an ACL to the interface. Any packet may be rejected by the inspection rule, the ACL, or both. The packet is first examined by the access list. If the packet passes the access list, then the inspection rule is checked next to determine whether that packet may transition the interface.

There are five simple steps to implementing inspection rules through the CLI:

Step 1	Choose the interface and packet direction to inspect.
Step 2	Configure an IP ACL for the interface.
Step 3	Define the inspection rules.
Step 4	Apply the inspection rules and the ACL to the interface.
Step 5	Verify the configuration.

Step 1: Choose an Interface and Packet Direction to Inspect

Choosing an interface is generally very easy. There are two general guidelines that will help you decide where to apply an ACL and inspection rule. Although every network is different, these two general guidelines will help you decide how and where to apply the ACL and inspection rule:

- On an interface where untrusted traffic originates:
 - Apply the ACL on the inbound direction of the interface so that only traffic allowed by the ACL is inspected.
 - Apply the inspection rule on the inbound direction of the interface so that only traffic considered safe transits the interface.

• For all other interfaces, apply the ACL on the outbound direction of the interface so that all unwanted traffic is dropped rather than sent over the network.

Step 2: Configure an IP ACL for the Interface

You must use extended access lists when you are also using inspection rules. If you are not familiar with extended access lists or need to review them, you are encouraged to do so now. A full explanation of extended access lists can be found at Cisco.com.

The access list in Example 22-1 would be applied to the outside interface. This access list allows users outside the network to connect to the SMTP server residing at 10.10.1.9 and the HTTP server residing at 10.10.1.15.

Example 22-1 Extended Access List

ip access-list extended acl_from_outside permit tcp any host 10.10.1.9 eq 25 permit tcp any host 10.10.1.15 eq 80 deny ip any any log

Step 3: Define the Inspection Rules

An inspection rule is defined through the **ip inspect** command, the syntax for which is as follows:

[no] ip inspect name inspection-name protocol [alert {on { off}] [timeout seconds] Table 22-2 lists the parameters available for this command.

 Parameter
 Description

 inspection-name
 Defines the name of the inspection rule.

 protocol
 Defines the protocol to be inspected. There are more than 170 supported protocols, some of which are as follows: TCP, UDP, ICMP, SMTP, ESMTP, SMTP, EMSTP, CUSEEME, FTP, FTPS, HTTP, H323, NETSHOW, RCMD, RealAudio, RPC, RTSP, SIP, SIP, SKINNY, SQLNET, TFTP, VDOLive.

 alert {on | off}
 Toggles alerts on or off.

 timeout seconds
 Defines the time interval in seconds between alert updates (default is 10 seconds).

 Table 22-2
 ip inspect Command Parameters

Example 22-2 shows how to define the inspection rules for this example.

Example 22-2 IP Inspection Rules

Router(config)#ip inspect name from_outside ftp alert off audit-trail on timeout 60 Router(config)#ip inspect name from_outside http alert on audit-trail on timeout 30

The preceding example sets the timeout for FTP to 60 seconds. No alerts are sent for FTP. The HTTP setting decreases the timeout to 30 seconds and sends alerts regarding HTTP. Both FTP and HTTP in this example use audit trails.

Step 4: Apply the Inspection Rules and the ACL to the Interface

Now that the ACL and inspection rules have been defined, you must apply these to the interface. Audit trails will be used, so your first task is to enable audit trails in the global configuration. Alerts have also been chosen. These are simple to set up with the global commands executed in Example 22-3.

Example 22-3 Global Configuration for Logging and Alerts

```
Router(config)#ip inspect audit-trail
! enables the delivery of audit trail messages using syslog
Router(config)#logging on
! turns on logging
Router(config)#logging host 10.10.1.20
! sets out logging server to 10.10.1.20
Router(config)#no ip inspect alert-off
! turns on real-time alerts
```

Now that the global configuration is established, you simply apply the previously defined inspection rules to the individual interface. While you are in the interface configuration mode, you will also apply the ACL to that interface as demonstrated in Example 22-4.

Example 22-4 Apply Inspection Rules to the Interface

```
Router(config)#int e0/0
Router(config-if)#ip inspect from_outside in
Router(config-if)#ip access-group acl_from_outside in
Router(config-if)#^z
```

The configuration is now complete. The next step is to verify your configuration.

Step 5: Verify the Configuration

Verification of the setup is very simple. The **show ip inspect** command displays how the inspection rules have been configured. The syntax for the **show ip inspect** command is as follows:

```
show ip inspect [name inspection-name | config | interface | session {detail} |
statistics | all]
```

A number of options are available with this command, as described in Table 22-3.

 Table 22-3
 show ip inspect Command Options

Parameter	Description
name inspection-name	Displays the configured inspection with the defined inspection name
config	Displays the entire IP inspection configuration
interface	Displays the configurations used within the interface mode
session	Displays sessions that are currently being tracked
detail	Displays additional details about current sessions
statistics	Displays statistical information
all	Displays all information

The output from this command is simple to understand, as demonstrated in Example 22-5.

Example 22-5 show ip inspect session Command Output

```
Router#show ip inspect session
Established Sessions
Session 70A64274 (172.16.1.12:32956)=>(10.10.1.5:25) tcp SIS_OPEN
Created 00:00:07, Last heard 00:00:03
Bytes sent (initiator:responder) [137:319] acl created 2
Inbound access-list acl_from_outside applied to interface Ethernet0/0
```

Example 22-6 shows the output from a **show ip inspect all** command.

Example 22-6 show ip inspect all Command Output

```
Router#show ip inspect all
Session audit trail is enabled
one-minute (sampling period) thresholds are [400:500] connections
max-incomplete sessions thresholds are [400:500]
max-incomplete tcp connections per host is 50. Block-time 0 minute.
tcp synwait-time is 30 sec -- tcp finwait-time is 5 sec
tcp idle-time is 3600 sec -- udp idle-time is 30 sec
dns-timeout is 5 sec
Inspection Rule Configuration
Inspection name inspect from outside
```

```
Example 22-6 show ip inspect all Command Output (Continued)
```

```
tcp timeout 3600
udp timeout 30
ftp timeout 3600
Interface Configuration
Interface Ethernet0
Inbound inspection rule is inspect_from_outside
tcp timeout 3600
udp timeout 30
ftp timeout 3600
Outgoing inspection rule is not set
Inbound access list is acl_from_outside
Outgoing access list is not set
Established Sessions
Session 25A6E1C (10.3.0.1:46065)=>(10.1.1.9:25) ftp SIS_OPEN
Session 25A34A0 (10.1.1.9:20)=>(10.3.0.1:46072) ftp-data SIS OPEN
```

Although debugging IP inspection is beyond the scope of this book, it can be helpful to know a few of the **debug** commands associated with inspection. Table 22-4 shows the most common **debug** commands associated with IP inspection and describes their purpose.

 Table 22-4
 debug ip inspect Commands

Command	Description
debug ip inspect function-trace	Debugs the functions used by ip inspect
debug ip inspect object-creation	Debugs the creation of objects used by ip inspect
debug ip inspect object-deletion	Debugs the deletion of objects used by ip inspect
debug ip inspect events	Debugs events within ip inspect
debug ip inspect timers	Debugs timers used in ip inspect
debug ip inspect detail	Provides detailed debugging of ip inspect

Configure a Basic Firewall Using SDM

SDM provides a graphical interface that allows you to configure security on Cisco routers quickly. The ease of use and automatic features of SDM can be a great benefit to the administrator. When using SDM to configure a basic firewall, you use the same five steps that you used with the CLI, as described in the previous section. However, because you are using a graphical interface, these steps are not easily distinguishable from each other.

This section describes how to use SDM to configure a basic firewall. If you have never used SDM before, you will be amazed by how quickly you can complete a simple configuration. The next section describes how to use SDM to configure an advanced firewall.

After you start SDM, click the **Configure** button at the top of the window. Next, click **Firewall and ACL** in the Tasks bar on the left. As Figure 22-1 shows, the default choice is Basic Firewall. Before you click the Launch the Selected Task button, notice the How do I pull-down menu at the bottom of the window. This menu provides help on the most common tasks when using SDM.

Figure 22-1 Basic Firewall Creation



Click the **Launch the selected task** button. You are taken to the Basic Firewall Interface Configuration window, shown in Figure 22-2, where you decide which interfaces are trusted and which are not trusted. Notice that this window also provides you with the option to allow SDM access through the untrusted interface. Assign the trust levels to the interfaces and click the **Next**> button.

Figure 22-2 Basic Firewall Interface Configuration

Firewall Wizard		×			
Firewall Wizard	Basic Firewall Interface Configuration				
	Select an outside(untrusted) interface from the drop down list. Out interface is the interface facing the Internet.	side(untrusted)			
	Outside(untrusted) Interface: Serial0	3			
	Allow secure SDM access from outside interfaces				
	Select inside(trusted) interfaces. SDM will apply access rules on the interfaces. Unselected interfaces are not affected.	ne selected			
	Inside(trusted) Interfaces: FastEthernet0 Serial0				
	< Back Next > Finish	Cancel Help			

Next, you see the Firewall Configuration Summary window, shown in Figure 22-3. Although this is one of the most basic configurations possible, you can see that many configuration options have been enabled with just a few mouse clicks. These options are converted into CLI commands to be saved in the configuration.

Figure 22-3 Firewall Configuration Summary

Firewall Wizard	X
Firewall Wizard Firewall Wizard	Firewall Configuration Summary Inside(trusted) Interfaces: Ethernet0 (192.168.101.15) Apply access rule to the inbound direction to deny spoofing traffic. Apply access rule to the inbound direction to deny traffic sourced from broadca Apply access rule to the inbound direction to permit all other traffic. Outside(untrusted) Interface: Serial0 (10.0.0.1) Apply application security policy SDM_LOW to the outbound direction. Turn on unicast reverse path forwarding check. Apply access rule to the inbound direction to permit IPSec tunnel traffic for interfic Apply access rule to the inbound direction to permit ICMP traffic. Apply access rule to the inbound direction to deny spoofing traffic. Apply access rule to the inbound direction to deny spoofing traffic. Apply access rule to the inbound direction to deny spoofing traffic. Apply access rule to the inbound direction to deny spoofing traffic. Apply access rule to the inbound direction to deny spoofing traffic. Apply access rule to the inbound direction to deny spoofing traffic. Apply access rule to the inbound direction to deny traffic sourced from broadca Apply access rule to the inbound direction to deny all other traffic.
	< Back Next> Finish Cancel Help

At this point, the basic configuration is complete. However, you might want to adjust some parameters to allow things such as HTTP or FTP access. You so this under the Edit Firewall Policy/ACL tab. As shown in Figure 22-4, this tab enables you to permit or deny access based on source or destination address, type of service, and application. Although this is still the basic firewall configuration, the flexibility provided is more than adequate for many users' needs. Take a few moments and review this short section before moving on to the advanced configuration using SDM.

ං ශී්ඩ Configu	re Monitor	Refresh Sav) Q e Search	? Help			cisco
🔒 Firewall :	and ACL						
Create Firewa	Edit Firewall Polic	y / ACL Application	n Security				
Select a dire	ction From: Ethe	rnet0	🕶 🕰 To: Seri	a10	▼ G 0		View Option
			hormot0			-	
		EU			enaio		
© Ori C Rei	ginating traffic			200	- uuu	*	
		108 5	irowall : Activo (from	n Ethornot0	to SocialO)		
		103 FI	irewaii. Active (iror	n Eulenielo	to Serialo)		
Firewall Fe	ature Availability: A	vailable	Cut Ba Conv 16	a Poste v	Sinspect	tion Rule: S	A Apply Firewall
Action	Rourse	Destination	Consiso	Log	Ontion	Description	and which the constitution
S Deny	= 10.0.0.0/0.0.0.255	* any	IP ip	LUg	Option	Description	_
O Denv	255.255.255.255	🛪 any	⊥r∕ip				
Dony	- 127 0 0 0/0 266 2	Mr any	TP. in				
O Deny ✓ Permit	➡ 127.0.0.0/0.255.2 ★ any	★ any ★ any	⊥₽∕ip ⊥₽∕ip				
O Deny ✓ Permit	+ 127.0.0.0/0.255.2 ★ any	★ any ★ any	_ı₽∕ip _ı₽∕ip				
O Deny ✓ Permit	∔ 127.0.0.0/0.255.2 ★ any	★ any ★ any	⊥e∕ip ⊥e∕ip				
Deny Permit Applications	+ 127.0.0.0/0.255.2 * any	★ any ★ any	⊥e∠ip ⊥e∠ip ⊈+Add • @ Edit	Delete	Global Settir	ngs 🛛 🗐 Su	mmary 🕰 Details
Deny Permit Applications Application	+ 127.0.0.0/0.255.2 * any s Protocol	* any * any Description	관·lp 관·lp � Add - 22 Edit	Delete	Global Settin	ngs 🛛 🗐 Sur	mmary 🕰 Details
Deny Permit Applications Application cuseeme	+ 127.0.0.0/0.255.2 * any Protocol	* any * any Description CUSeeMe Protoc	IP·ip IP·ip 오 Add ~ (김 Edit	Delete] 「및 Global Settin	ngs 🗐 Su	mmary 🕰 Details
Deny Permit Applications Application Cuseeme ftp h323	+ 127.0.0.0/0.255.2 * any Protocol	* any * any Description CUSeeMe Protoc File Transfer Prot H.323 Protocol (e	I I I I I I I I I I I I I I I I I I I	Delete	Global Settin	ngs 🛛 🗐 Su	mmary 🕰 Details
	+ 127.0.0.0/0.255.2 * any Protocol	* any * any Description CUSeeMe Protocol File Transfer Prot H.323 Protocol ICMP Protocol	I I I I I I I I I I I I I I I I I I I	Delete	Global Settin	ngs 📔 🖪 Su	mmary 🕰 Details
Deny Permit Applications Applications fip h323 icmp netshow	+ 127.0.0.070.255.2 * any Protocol	* any * any Description CUSeeMe Protoco File Transfer Proto H.323 Protocol (e ICMP Protocol Microsoft NetShow	I I P I P I P I P I P I P I P I P I P I	Delete	المعلق (Iobal Settin Phone)	ngs 🖪 Su	mmary 🕰 Details
Deny Permit Applications Applications Applications Inseries Applications Ap	+ 127.0.0.0/0.255.2 * any Protocol	* any * any Description CUSeeMe Protoc File Transfer Protoc H. 23P Protocol Microsoft NetShov	IE-ip IE-ip 로스ip Add ~ [2] Edit Col Cool G, MS NetMeeting, w Protocol	Delete	Clobal Settin	ngs 🖪 Su	mmary 🕰 Details

Figure 22-4 Edit Firewall Policy/ACL Tab

Configure an Advanced Firewall Using SDM

The Advanced Firewall Wizard provides easy access to some features that are not available under the Basic Firewall option. The Advanced Firewall Wizard works similarly to the Basic Firewall Wizard. As shown in Figure 22-5, simply choose **Advanced Firewall** instead of Basic Firewall on the Create Firewall tab of the Firewall and ACL window.

Figure 22-5 Advanced Firewall Creation



Click **Launch the selected task** and you are presented with the Advanced Firewall Interface Configuration window. The most noticeable differences on this window compared to the Basic Firewall Interface Configuration window (shown previously in Figure 22-2) are that you can choose multiple interfaces as either inside (trusted) or outside (untrusted) and can choose an interface for use as a DMZ. Figure 22-6 shows the Advanced Firewall Interface Configuration window. In this example, Ethernet0 is selected as a trusted (inside) network, Serial0 as an untrusted (outside) network, and FastEthernet0 as a DMZ.

Click the **Next>** button, and you are taken to the Advanced Firewall DMZ Service Configuration window, where you configure aspects of the DMZ. As Figure 22-7 shows, the wizard knows that FastEthernet0 was chosen as the DMZ. Click the **Add** button to continue.

Advanced Firewall Interface Configuration					
Select inside(trusted) and outs more inside(trusted) and outsid	ide(untrusted) interfaces. Yo de(untrusted) interfaces.	u can select one ol			
Note: Do not select the interface (untrusted) interface. If you do, y interface after you complete the	e through which you accesse you will not be able to launch Firewall Wizard.	ed SDM as the outs SDM from that			
interface	outside(untrusted)	inside(trusted)			
Ethernet0		v .			
FastEthernet0					
Serial0					
Select a DMZ interface if you have servers that you want to make accessible from the Internet. These are typically DNS, HTTP, FTP and SMTP servers. DMZ Interface (Optional): FastEthernet0					
Allow secure SDM access fr	om outside interfaces				
	Advanced Firewall Interface Coo Select inside(trusted) and outsi more inside(trusted) and outsi Note: Do not select the interface (untrusted) interface. If you do, y interface after you complete the interface Ethernet0 FastEthernet0 Serial0 Select a DMZ interface if you ha the Internet. These are typically DMZ Interface (Optional): Allow secure SDM access fr	Advanced Firewall Interface Configuration Select inside(trusted) and outside(untrusted) interfaces. Yo more inside(trusted) and outside(untrusted) interfaces. Note: Do not select the interface through which you accesses (untrusted) interface. If you do, you will not be able to launch interface after you complete the Firewall Wizard. interface outside(untrusted) Ethernet0			

Figure 22-6 Advanced Firewall Interface Configuration

Figure 22-7 Advanced Firewall DMZ Service Configuration

Firewall Wizard				2
Firewall Wizard	Advanced Firewall DM DMZ (demilitarized zon network. By default, tra	Z Service Configura e) is an area betwe ffic initiated by hosts	n tion en the Internet and : inside the DMZ is	your inside (trusted) blocked.
	DMZ Services: Int	erface (FastEtherne End IP Address	t0), IP Address (19	2.168.102.1)
	I			
	Add	Delete		
		<	Back Next > Fi	nish Cancel Help

Because you need to add services to the DMZ, you are prompted for the starting and ending IP addresses for a service. You then choose whether you will use IP or UDP and the service associated with the previously entered addresses. Figure 22-8 shows that UDP with port number 500 (IKE) was chosen. Alternatively, you can choose a service such as WWW or FTP.



Start IP Address:	192.168.0.3
nd IP Address:	192.168.0.3
Service:	
Service:	UDP

After you have added as many services as you wish to the DMZ, you see a list similar to that shown in Figure 22-9. If you have chosen more services than can be displayed in the window, you will see a scroll bar on the right side of the window.



	Advanced Firewall DM	Z Service Configura	ation	
rewall Wizard	DMZ (demilitarized zor	ne) is an area hetwe	en the Internet and	your inside (trusted)
	network. By default, tra	ffic initiated by hosts	inside the DMZ is	blocked.
	DMZ Services: In	terface (FastEtherne	et0), IP Address (19	2.168.102.1)
	Start IP Address	End IP Address	Service Type	Service
_	192.168.0.2	192.168.0.2	tcp	www
	192.168.0.3	192.168.0.3	udp	500
	Add	Delete	1	
	Aud	Delete	J	
	-			

After all the services are configured, click **Next>** to go to the Advanced Firewall Security Configuration window. In this window, you can choose to use one of the three built-in SDM security policies (High Security, Medium Security, or Low Security) or a custom security policy for applications. In Figure 22-10, the option to use a custom policy has been chosen. When you choose this option, you are presented with an additional pull-down menu that allows you to select an existing policy or create a new one.

Figure 22-10	Advanced	Firewall	Security	Configu	ration
--------------	----------	----------	----------	---------	--------

Firewall Wizard		x
Firewall Wizard	Advanced Firewall Security Config SDM provides preconfigured applic the security level or define a custor C Use a default SDM Application	uration ation security policies. Use the slider to select n application security policy. Security Policy
		Description:
	High Security	The router does not identify application. Specific traffic. Returns TCP and UDP traffic on sessions initiated inside the from all
L	Medium Security	 Choose this option if you do not need to track use of these applications on the network.
	Low Security	•
		Preview Commands
	Use a custom Application Secu	urity Policy
	Policy Name:	🗸
	1	Create a new policy Select an existing policy
		< Back None Help

When presented with the Application Security window, you can choose any of the predefined applications from the list on the left. In Figure 22-11, the general parameters for the TCP and UDP protocols have been set up. Clicking the **Next>** button brings up the Application Security Window.

Figure 22-11 Application Security

File Edit View	and Security Device Manager (SDI Tools Help	M): 192.168.101.15			
Home	Configure Moni	tor Refresh Save	Q ? Search Help		cisco
Tasks	🔒 Firewall and ACL				
	pplication Security				×
Interfaces an Connections	E-mail	Choose the items to inspect			Edit
97.	Neer-to-Peer (P2P)	Applications	Alerts	Audit Timeout	Options
Firewall and A	URL Filtering	₩ tcp			
<u>~</u>	URL Filter Servers	I udp			
VPN	Header Options				
En l	Content Options				
Security Rud	Applications / Protocols »				
Routing NRT	Root General Gene				
Intrusion Preven					
Quality of Servi					
Rdditional Tas		ОК	Cancel Hel	Ip	Go
Configuration (7 🗗

Even after you have configured all the protocols and applications that are required by the network, you can still go back to any given protocol and edit the inspection mode defaults for that protocol within the security policy. As Figure 22-12 shows, you can set alerts, auditing, and timeouts on a per-protocol basis. Clicking **OK** at the bottom of the dialog box takes you back to the Advanced Firewall Security Configuration window (see Figure 22-10), which allows you to save the policy.

File Edit View	and Security Device Manager (SD Tools Help	M): 192.168.101.15				_ _ ×
Home Home	Configure Mon	itor Refresh Save	Q 4 Search H	? lelp		cisco
Tasks	🔒 Firewall and ACL					
An Interfaces ar Connections	pplication Security E-mail Instant Messaging (IM)	General Choose the items to inspect				Edit
er.	Neer-to-Peer (P2P)	Applications	Alerts	Audit	Timeout	Options
Firewall and A	URL Filtering					
S						
VPN	B Header Options	Calit Inspection Rule			×	
Security Rud	Content Options Content Options Applications / Protocols Content Conte	Alert: Audit:	default			
Routing	M tcp C day of the transfer C day of the tr	ок С	L Cancel 1 H	ielo 1		
Ouality of Serv	⊞-⊡ ILl Multimedia					
Additional Tas		ОК	Cancel	Help		Go 7 fr

Figure 22-12 Editing the Inspection Mode

After you have finished configuring the security policy, you need to verify the policy. The Firewall Configuration Summary window shown in Figure 22-13 displays the security policies as configured by interface. Notice that numerous rules have been applied on the outside interface and that HTTP and IKE traffic is allowed to enter the interface bound for specific hosts. Several different protocols have also been filtered.

Figure 22-13 Firewall Configuration Summary

Firewall Wizard	Firewall Configuration Summary
Firewall Wizard	Outside(untrusted) Interface: Serial0 (10.0.0.1) Turn on unicast reverse path forwarding check for non-tunnel interfaces. Apply access rule to the inbound direction to permit IPSec tunnel traffic if neces Apply access rule to the inbound direction to permit ICMP traffic. Apply access rule to the inbound direction to permit ICMP traffic. Apply access rule to the inbound direction to permit INTP traffic if necessary. Apply access rule to the inbound direction to deny spoofing traffic. Apply access rule to the inbound direction to deny spoofing traffic. Apply access rule to the inbound direction to deny spoofing traffic. Apply access rule to the inbound direction to deny traffic sourced from broadca Apply access rule to the inbound direction to permit service traffic going to DMZ Service www at 192.168.0.2 to 192.168.0.3 Apply access rule to the inbound direction to deny all other traffic. DMZ Interface: FastEthernet0 (192.168.102.1)
	Apply CBAC inspection rule dmzinspect to the outbound direction Apply access rule to the inbound direction to deny all other traffic.

This completes the configuration of the policies, but you must still enable logging. To do so, click the **Configure** button at the top of the SDM window, click **Additional Tasks** in the Tasks bar on the left, expand **Router Properties**, and click **Logging**. Click **Edit** in the upper-right corner of the Logging pane to open the Logging dialog box. As Figure 22-14 shows, you can enable logging, set the logging levels, assign logging hosts, and set the logging buffer.

Cisco Router an File Edit View	d Security Device Manager (SDM): Tools Help	192.168.101.15					_ 🗆 🗵
Home	Configure Monitor	Q Refresh	Save Search	? Help			uluilu cisco
Tasks	l Additional Tasks						
Prevention Prevention Firewall and ACL WPN EXC Security Rudit Prevention NRT Intrusion Prevent	Router Properties Date/Time Date/Time Date/Time Date/Time Date/Time Date/Time Source Device Provisioning DHCP Port Eave Act_Editor Zones Local Pools Router Provisioning Dors Router Provisioning CapL Configuration Management	Logging Syslog Logging to I Buffer Size Logging Lex Host Loggir	Joging Logging Hostnam I♥ [Enable Logging Logging Level: IP Addre I♥ Logging Buffer Logging Level: Buffer Size: OK	e Level Informationa ss/Hostname: debuggi 4096	I (6) Value Disabled	id	Edit
Additional Tasks					1	1:53:58 UTC Wed A	pr 18 2007 📑

Figure 22-14 Setting Logging Options

At this point, the security policy configuration has been completed for this router. The final task is to monitor the router. Click the **Monitor** button at the top of the SDM window, and then click **Firewall Status** in the Tasks bar. As shown in Figure 22-15, this allows you to see what packets are flowing through the router.

Figure 22-15 Monitor Firewall Status

File Edit View	id Security Device Manager (SDM Tools Help	1): 192.168.101.15			_ 🗆 ×
Home	Configure Monit	r 🚱 🛄 Refresh Save	C ? Search Help		cisco
Tasks	🏽 Firewall Status				
-	Firewall Session Statistics				
R.	Number of Interface configured	for inspection: 2			
Overview	Number of TCP Packet(s) count	: 0			
	Number of UDP Packet(s) count	t 0			-
Interface Status	Total Number of active connection	ons O			Update
2	Source IP Address	Destination IP Address	Protocols	Match Count	
Firewall Status					
<u>41</u>					
VPN Status					
*					
name beaus					
QoS Status					
Sext					
NRC Status					
5					
Logging					
μ.					
IPS Status					
6th					
802.1x Status	4				
*	11				
Firewall Status				11:55:23 UT	C Wed Apr 18 2007

Foundation Summary

Configuring a router as a firewall using either the CLI or one of the wizards is not a difficult task. Take a few moments to review the highlights of this chapter. If you do not understand what is being presented, go back through the text and review.

There are five steps to implementing inspection rules:

- **Step 1** Choose the interface and packet direction to inspect.
- **Step 2** Configure an IP ACL for the interface.
- **Step 3** Define the inspection rules.
- **Step 4** Apply the inspection rules and the ACL to the interface.
- **Step 5** Verify the configuration.

To configure an extended access list, enter the following:

ip access-list extended acl_from_outside permit tcp any host 10.10.1.5 eq 25 permit tcp any host 10.10.1.10 eq 80 deny ip any any log

To create an inspection rule, enter the following:

ip inspect name *inspection-name protocol* [**alert** {**on** | **off**}] [**timeout** *seconds*] Table 22-5 lists and describes the parameters available for the preceding command.

 Table 22-5
 ip inspect name Parameters

Parameter	Description
inspection-name	Defines the name of the inspection rule.
protocol	Defines the protocol to be inspected. The list of supported protocols is as follows: TCP, UDP, ICMP, SMTP, ESMTP, SMTP, EMSTP, CUSEEME, FTP, FTPS, HTTP, H323, NETSHOW, RCMD, RealAudio, RPC, RTSP, SIP, SKINNY, SQLNET, TFTP, VDOLive.
alert {on off}	Toggles alerts on or off.
timeout seconds	Defines the time interval in seconds between alert updates (default is 10 seconds).

A sample IP inspection rule is as follows:

```
Router(config)#ip inspect name from_outside ftp alert off audit-trail on timeout 60
Router(config)#ip inspect name from_outside http alert on audit-trail on timeout 30
```

The **show ip inspect** command displays how the inspection rules have been configured. Table 22-6 describes the parameters for this command.

Parameter	Description
name inspection-name	Displays the configured inspection with the defined inspection name
config	Displays the entire IP inspection configuration
interface	Displays the configurations used within the interface mode
session	Displays sessions that are currently being tracked
detail	Displays additional details about current sessions
statistics	Displays statistical information
all	Displays all information

 Table 22-6
 show ip inspect Command Options

Table 22-7 shows the most common **debug** commands associated with the **ip inspection** command and their purpose.

 Table 22-7
 debug ip inspect Commands

Command	Description
debug ip inspect function-trace	Debugs the functions used by ip inspect
debug ip inspect object-creation	Debugs the creation of objects used by ip inspect
debug ip inspect object-deletion	Debugs the deletion of objects used by ip inspect
debug ip inspect events	Debugs events within ip inspect
debug ip inspect timers	Debugs timers used in ip inspect
debug ip inspect detail	Detailed debugging of ip inspect

There are many features available when using either the Basic Firewall Wizard or the Advanced Firewall Wizard. But, there are also a few major differences between the two wizards. Table 22-8 highlights the differences.

 Table 22-8
 Basic and Advanced Firewall Wizard Features

Feature	Basic	Advanced
Configure untrusted network	Yes	Yes
Configure multiple untrusted networks	No	Yes
Configure trusted network	Yes	Yes
Configure multiple trusted networks	Yes	Yes

Feature Basic Advanced Configure DMZ No Yes Configure protocol-specific alerts Yes Yes Configure protocol-specific logging Yes Yes Graphical interface Yes Yes Yes Monitoring capabilities Yes

 Table 22-8
 Basic and Advanced Firewall Wizard Features (Continued)

Q&A

The questions and scenarios in this book are designed to be challenging and to make sure that you know the answer. Rather than allowing you to derive the answers from clues hidden inside the questions themselves, the questions challenge your understanding and recall of the subject.

Hopefully, mastering these questions will help you limit the number of exam questions on which you narrow your choices to two options, and then guess.

You can find the answers to these questions in Appendix A. For more practice with exam-like question formats, use the exam engine on the CD-ROM.

- 1. Name some advantages of using the Advanced Firewall Wizard as opposed to using the CLI.
- **2.** When is it appropriate to use the Basic Firewall Wizard instead of the Advanced Firewall Wizard?
- 3. What are the steps to configure a firewall using the CLI?
- 4. Under what circumstances should the default timeouts for alerts be changed?



Exam Topic List

This chapter covers the following topics that you need to master for the CCNP ISCW exam:

- IDS and IPS Functions and Operations— Describes the functions and operations of intrusion detection systems (IDS) and intrusion prevention systems (IPS) and the difference between IDS and IPS
- Categories of IDS and IPS—Describes the categories of IDS and IPS
- **IDS and IPS Signatures**—Describes the four types of IDS and IPS signatures
- Signature Reaction—Describes what happens when a signature is matched
- IOS Configuration—Describes how to configure and verify Cisco IOS IPS using the CLI
- SDM Configuration—Describes the Cisco IOS IPS tasks that are completed with SDM