Cisco IOS Threat Defense Features

This chapter explores the advantages, concepts, and strategy behind the Cisco IOS Firewall offerings. Using a layered device as part of the overall security strategy allows the administrator great flexibility in access control. Using a demilitarized zone (DMZ) helps to isolate security breaches outside of the internal portion of the corporate network. If a security breach does occur, the rest of the network can remain intact. For example, "hacking" a web server that is positioned in a DMZ will not enable the hacker to penetrate into the internal portion of the network.

In this chapter, you will examine the differences between packet filters, application layer gateways (ALG), and stateful packet filters, learn about the Cisco IOS Firewall feature set, and discover how the Cisco IOS Firewall operates. Chapter 22, "Implementing Cisco IOS Firewall Features," covers how to implement the Cisco IOS Firewall.

"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 13-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 21-1 outlines the major topics discussed in this chapter and the "Do I Know This Already?" quiz questions that correspond to those topics.

Table 21-1 *"Do I Know This Already?" Foundation Topics Section-to-Question Mapping*

Foundation Topics Section	Questions Covered in This Section	Score
Layered Device Structure	1–2	
Firewall Technology Basics	3–8	
Cisco IOS Firewall Feature Set	9–10	
Cisco IOS Firewall Operation	11–12	
Cisco IOS Firewall Packet Inspection and Proxy Firewalls	13	
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. Why is it advised that each server be placed on a separate DMZ?
   a. It forces the administrator to deal with more ACLs, thereby ensuring that there is more security.
   b. It helps prevent one compromised server from becoming a launching platform for more security breaches.
   c. It helps the accounting department by tracking each server independently.
   d. It provides a way of tracking the use of each server.
2. When using multiple DMZs, what equipment is required (select all that apply)?
   a. A Cisco PIX Firewall must be used.
   b. A router with multiple interfaces must be used.
   c. A LAN switch must be used.
   d. A VPN Concentrator must be used.
   e. All these answers are correct.
3. What type of equipment would be employed to prevent the user from any direct access to a server?
   a. Packet filter
   b. Hybrid packet filter
   c. Stateful packet filter
   d. ALG
4. What type of firewall is best used when only UDP is used for access?
   a. Packet filter
   b. Authentication proxy
   c. ALG
   d. Stateful packet filter

5. Which type of equipment is used to provide data from a server while still preventing direct access to that server?

   a. Packet filter
   b. ALG
   c. Stateful packet filter
   d. Hybrid packet filter

6. How does a stateful packet filter's use of access control lists (ACL) differ from a packet filter's use of ACLs?

   a. ACLs are not required in a stateless filter.
   b. ACLs are not required in a stateful filter.
   c. ACLS require a separate database, such as SQL, in a stateful filter.
   d. ACLs are static in a stateless filter.
   e. ACLs are dynamically changed in a stateless filter.
   f. ACLs are dynamically changed in a stateful filter.

7. How does a stateful packet filter handle UDP packets?

   a. Defaults back to packet filter
   b. Allows only FTP UDP packets
   c. Defaults to a stateless firewall
   d. Blocks UDP traffic
   e. Allows UDP traffic

8. What does a stateful packet filter maintain?

   a. A connection database
   b. A session database
   c. A user database
   d. A connection table
   e. A session table
   f. A user table

9. What type of firewall is the Cisco IOS Firewall?

   a. Packet firewall
   b. Application layer gateway
   c. Stateful
   d. Hybrid

10. How does the Cisco IOS Firewall handle streaming video such as VDOLive or Streamworks?
    a. It ignores all streaming video, allowing it to pass.
    b. It ignores all streaming video, blocking it.
    c. It is fully aware of streaming video and blocks or passes as configured.
    d. Streaming video is allowed if the configuration is globally set.
11. What is unique about how the Cisco IOS Firewall handles ACLs?
    a. The Cisco IOS Firewall does not require ACLS.
    b. They are dynamically changed during operation.
    c. They are automatically generated.
    d. They must be applied before the inspection rule is applied.
12. How does the Cisco IOS Firewall handle UDP traffic (select all that apply)?
    a. It ignores all UDP traffic, allowing it to pass.
    b. It defaults to stateless modes.
    c. It uses timeouts for UDP traffic.
    d. It prevents all UDP traffic from passing.
13. Which of the following is not a benefit of the Cisco IOS Firewall?
    a. Allows combinations of proxy, stateless, and stateful firewall technologies
    b. Defaults to stateless when stateful is not practicable
    c. Ignores streaming video
    d. Can provide proxy services

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:

- **8 or fewer overall score**—Read the entire chapter. This includes the "Foundation Topics," "Foundation Summary," and "Q&A" sections.
- **9 to 12 overall score**—Begin with the "Foundation Summary" section, and then go to the "Q&A" section.
- **12 or more 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.

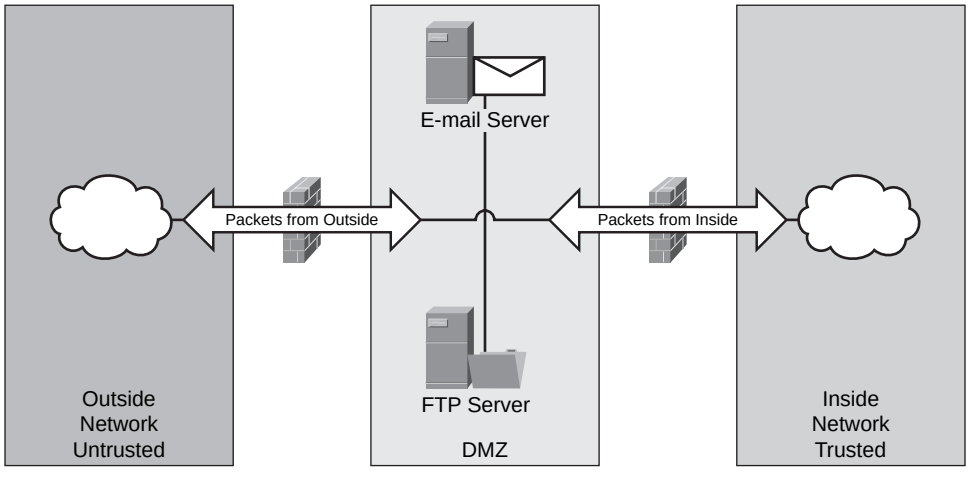
Foundation Topics

Layered Device Structure

The Cisco IOS Firewall uses DMZs as a way of isolating services from the internal network. By creating a buffer zone, these DMZs create networks that are neither entirely internal nor entirely external to the corporate network. Traditionally, the DMZ exists between the corporate network and the Internet. There is no requirement for a DMZ to allow access from either the internal network or the Internet. For example, a payroll server could be attached to a DMZ that allows access only from the internal network. This would allow the administrator to restrict access to certain machines or users on the corporate network while ensuring that users on the Internet never even see the server.

Take a moment to look at Figure 21-1. Notice that from an access viewpoint the DMZ is positioned between the corporate network and the Internet.

Figure 21-1 *Cisco DMZ*

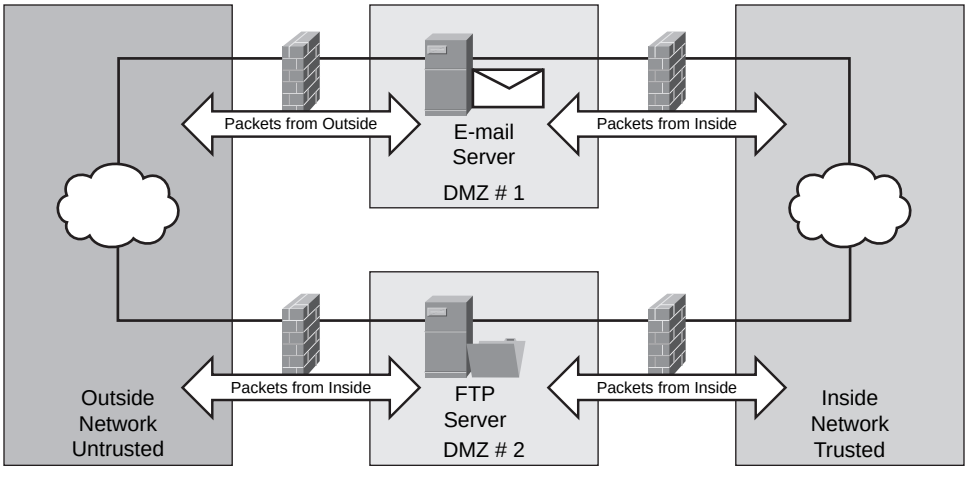


DMZ access is controlled by dedicated firewalls, such as the Cisco PIX Firewall, or by a router with multiple interfaces. Dedicated servers on the DMZ provide services such as web, FTP, or e-mail services. The DMZ may also host a gateway to applications that require outbound connectivity.

The primary advantage of a DMZ is that a security breach on one of the DMZ servers does not compromise the internal network. Using DMZs also encourages the administrator to compartmentalize the services onto dedicated servers, which may be extremely helpful in troubleshooting problems. When this compartmentalization is accomplished, it makes sense to place each server on its own DMZ.

Configuring a network to use multiple DMZs is considered by many to be both state-of-the-art architecture and the best security practice available. Instead of placing all servers requiring access from the Internet into a single DMZ, placing each server into a separate DMZ has important advantages. Having each server on a dedicated DMZ not only makes it is easier for the administrator to change who is allowed access to an individual server but, more importantly, also is one of the best ways to ensure that the compromise of any single server does not affect any other portion of the network. Figure 21-2 shows a conceptual example of a network with multiple DMZs.

Figure 21-2 *Multiple DMZs*



Firewall Technology Basics

Firewalls use three technologies: packet filtering, application layer gateway (ALG), and stateful packet filtering. Table 21-2 provides a short description of these technologies, which is followed by a deeper discussion of each.

Table 21-2 *Firewall Technologies*

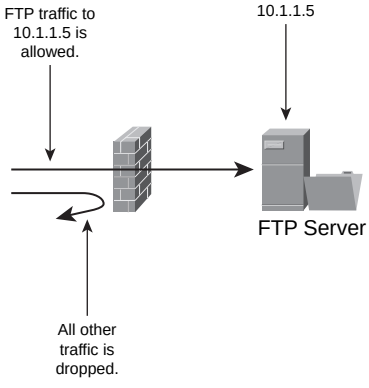
Technology	Description
Packet filtering	Uses IP addresses and/or port numbers with an ACL.
ALG	Works like a proxy server.
Stateful packet filtering	Uses ACLs. Also knows the connection state to determine access.

Packet Filtering

Packet filtering is the simplest technology used on the firewall. The difference between stateful and stateless is merely whether the filter tracks and responds to the context in which protocol requests are given. This technology limits traffic transiting the firewall by using an ACL. The ACL filters by IP address, port, or any other criterion within the assigned access list. Although packet filtering does allow great complexity and ease of use, it does not maintain a database of the current state of connections. Therefore, it is a less secure method than stateful packet filtering.

Figure 21-3 shows how FTP traffic is permitted to enter a single server while other traffic is denied access.

Figure 21-3 *Filtering FTP Traffic to a Specific Server*



Configuring the ACL can be simple or complex, depending on the requirements. Example 21-1 shows a simple ACL configuration that allows FTP traffic to enter a specific server, as shown in the example in Figure 21-3.

Example 21-1 *Packet Filtering ACL*

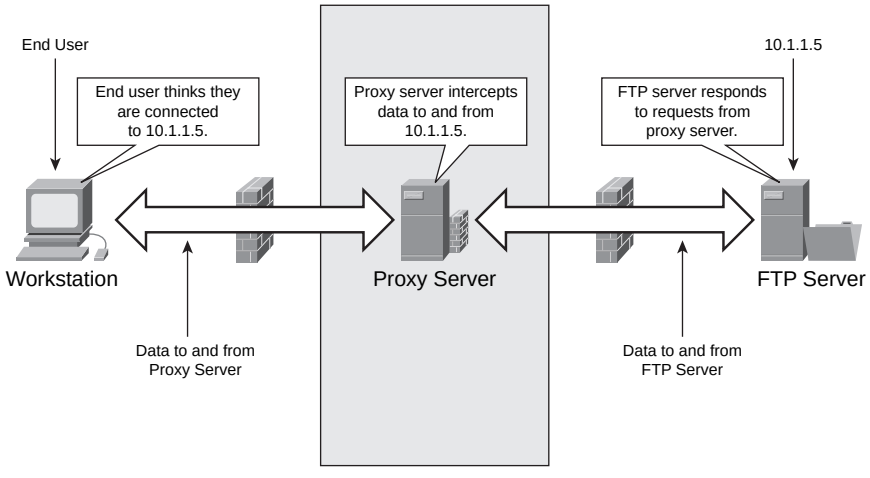
```
Router(config)#access-list 100 permit tcp any host 10.1.1.5
Router(config)#access-list 100 deny ip any any log
Router(config)#interface serial 1/1
Router(config-if)#ip access-group 100 in
Router(config-if)#^z
```

Application Layer Gateway

An application layer gateway (ALG) uses a server that provides proxy services. The outside user connects to the ALG. The ALG then makes a connection to the interior server and passes requests between the interior server and the user. This is a very effective method for services such as HTTP, HTTPS, FTP, and e-mail. This method provides a good deal of security because the user connects to the DMZ server and never actually sees the interior server.

Figure 21-4 shows an example of an ALG acting as a proxy server between a user and an internal FTP server.

Figure 21-4 *Application Layer Gateway*



Stateful Packet Filtering

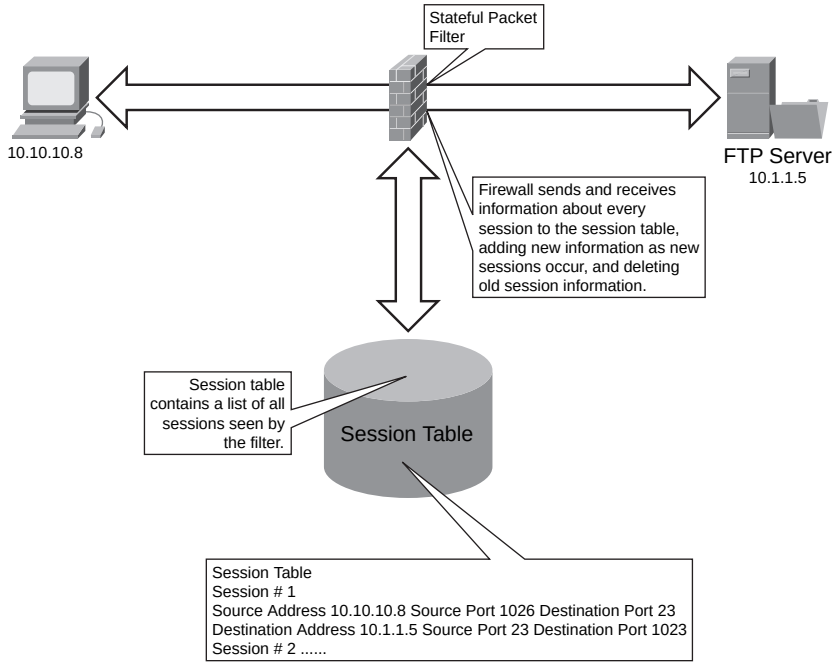
Stateful packet filtering is a refinement of the packet filtering technology that provides additional levels of security. The main advantage of stateful packet filtering is that the firewall understands the "state" of the connection. For example, a stateful packet filter will not allow an TCP ACK packet through unless there has already been a request from the same source to establish an TCP connection and a response from the server allowing the connection to proceed. Because the

firewall remembers the state of all connections and inspects every packet, it is able to filter out those packets that are inappropriate.

Additionally, a stateful packet filter understands Layer 7 protocols enough to allow new connections when they are required for the application. For example, FTP data transfers occur over a separate data channel that is negotiated over the original control connection. A stateful packet filter recognizes this negotiation and updates the session table accordingly to allow the traffic through.

Figure 21-5 shows a stateful packet filter in operation.

Figure 21-5 *Stateful Packet Filter Operation*



A stateful packet filter treats each protocol in a unique fashion. For example, TCP sequence numbers are checked to ensure they are arriving in a sequential manner. However, UDP does not have a sequence number, so this method cannot be used and the filter reverts to stateless mode for these UDP packets. Table 21-3 describes how a stateful packet filter handles different protocols.

Table 21-3 *Protocol Handling by a Stateful Packet Filter*

Applications	Features
TCP	Checks flow information Tracks sequence numbers
UDP	Hard to track UDP thoroughly No sequence numbers in UDP Checks timeouts Tracks source and destination IP addresses Tracks source and destination UDP ports
Applications	Watches application negotiations
Connectionless services (GRE, IPsec, and so on)	Usually defaults to stateless packet filtering operation

Cisco IOS Firewall Feature Set

The Cisco IOS Firewall feature set has the following three main features, each of which will be discussed briefly before you learn about how the Cisco IOS Firewall works:

- Cisco IOS Firewall
- Authentication Proxy
- Intrusion Prevention System (IPS)

Cisco IOS Firewall

The Cisco IOS Firewall is a stateful packet filter that has the following features:

- Permits or denies specified TCP and UDP traffic
- Maintains a state table
- Modifies ACLs dynamically
- Protects against DoS attacks
- Inspects packets passing through the interface

Authentication Proxy

The Authentication Proxy provides authentication and authorization on a per-user basis through either Remote Authentication Dial-In User Service (RADIUS) or Terminal Access Controller Access Control System Plus (TACACS+) for the following protocols:

- HTTP
- HTTPS
- FTP
- Telnet

Cisco IOS IPS

Cisco IOS IPS is an intrusion detection and response system that identifies and responds to over 700 forms of attack. Identification of an attack initiates one or more of the actions shown in Table 21-4.

Table 21-4 *Cisco IOS IPS Response to Attack*

Action	Description
Drop	Drops the packet
Block	Blocks the sending IP address for a specified period of time
Reset	Terminates a TCP session by sending a TCP reset
Alarm	Sends an alarm to the syslog server or SDM

Cisco IOS Firewall Operation

Before discussing how the Cisco IOS Firewall works, consider the following list of protocols that are fully recognized by the Cisco IOS Firewall:

- BGP
- FTP/FTPS
- HTTP/HTTPS
- ICMP
- Kazaa
- RTSP (Real Networks)
- RADIUS

- Signaling protocols
  - H.323
  - Skinny
  - SIP
- SMTP
- SNMP
- SQL*NET
- TACACS+
- Telnet
- TFTP
- TCP (single channel)
- UDP (single channel)
- UNIX R-commands (rlogin, rexec, and so on)
- Multimedia protocols
  - Microsoft NetShow
  - StreamWorks
  - VDOLive

As stated earlier, the Cisco IOS Firewall modifies ACLs dynamically as data passes through the interface. While this concept might seem strange at first, it is a relatively simple process. The firewall sees permitted traffic and adds a new line within the existing ACL. The Cisco IOS Firewall also allows you to configure real-time audit trails and alerts on a per-protocol basis, using syslog.

Figure 21-6 shows the steps in this process. Notice the state of the ACL before and during the Telnet session. The filter reverts to the original after the Telnet session has ended.

Cisco IOS Firewall Packet Inspection and Proxy Firewalls

The combination of services offered by the Cisco IOS Firewall, providing both power and flexibility, makes the Cisco security offerings an optimal security solution. The administrator has the option to log any or all protocols, and to allow or deny traffic by port, protocol, or IP address.

Figure 21-6 *Cisco IOS Firewall Process*

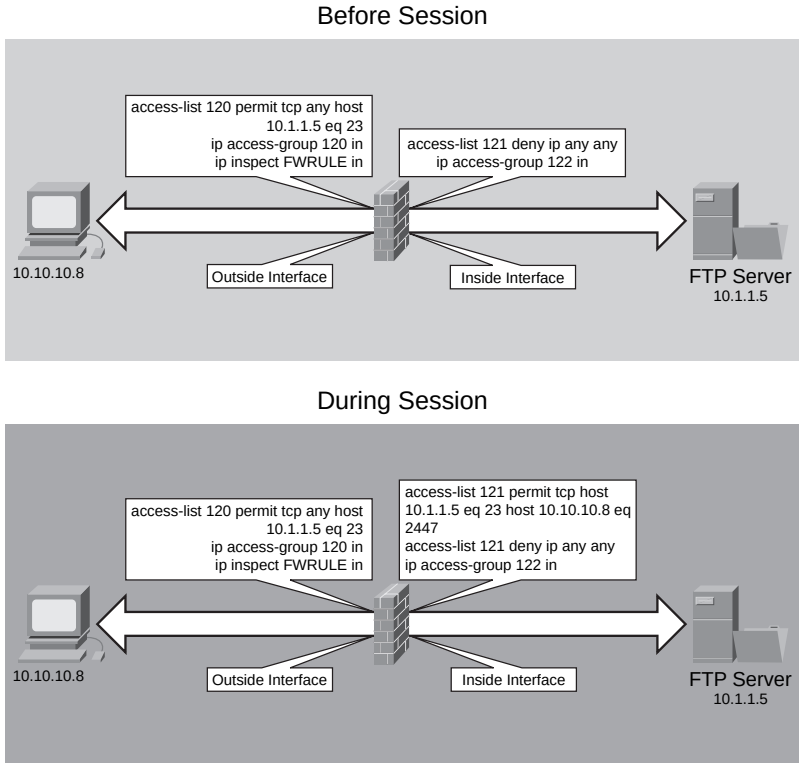


Table 21-5 summarizes the technologies available and the benefit of each to the administrator.

Table 21-5 *Capabilities of the Cisco IOS Firewall*

Capability	Benefit
Layered defense	A breach in one area does not compromise all of the network.
Packet filtering	May block specific types of packets.
ALG	The end user never connects directly to the resource.
Stateful packet filtering	Tracks the state of a connection and drops those packets that are not authorized.
Cisco IOS Firewall	Filters packets based on session and application.
Cisco IOS Authentication Proxy	Enables use of RADIUS or TACACS+.
Cisco IOS IPS	Identifies over 700 common attacks and refutes them.
Logging	Allows real-time logging of any or all events.

Foundation Summary

This chapter has given you an overview of the Cisco IOS defense features. The first area discussed was the three firewall technologies, as summarized in Table 21-6.

Table 21-6 *Firewall Technologies*

Technology	Description
Packet filtering	Uses IP addresses or port numbers with an ACL.
ALG	Works like a proxy server.
Stateful packet filtering	Uses ACLs. Also knows the connection state to determine access.

It is important to remember how protocols are handled within the stateful packet filter, as summarized in Table 21-7.

Table 21-7 *Protocol Handling by a Stateful Packet Filter*

Applications	Features
TCP	Checks flow information Tracks sequence numbers
UDP	Hard to track UDP thoroughly No sequence numbers in UDP Checks timeouts Tracks source and destination IP addresses Tracks source and destination UDP ports
Applications	Watches application negotiations
Connectionless services (GRE, IPsec, and so on)	Usually defaults to stateless packet filter operation

The Cisco IOS Firewall feature set consists of three systems:

- Cisco IOS Firewall
  - Permits or denies specified TCP and UDP traffic
  - Maintains a state table
  - Modifies ACLs dynamically
  - Protects against DoS attacks
  - Inspects packets passing through the interface
- Authentication Proxy
  - Provides AAA authentication
- IPS
  - Provides intrusion detection that allows four actions:
    - Drop the packet
    - Block the IP address
    - Terminate the TCP session
    - Send an alarm

The Cisco IOS Firewall modifies ACLs dynamically as data passes through the interface, editing the ACLs as data is permitted or denied.

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. You are designing a network that should have three servers available for access from the Internet, e-mail, FTP, and the web. How should this network be designed?
2. What are the three technologies used in firewalls and what are the main characteristics of each?
3. Which protocols does the Cisco IOS Firewall process recognize?
4. Why does the stateful packet filter not work with UDP?
5. What type of firewall monitors the applications and allows ports to be opened and closed in response to the application protocol negotiation?
6. You have a server that must service two different programs simultaneously. One of these programs contains your company's payroll records; the other program allows external users to browse a list of your employees. How should you design this access?
7. You are notified that a new security risk has been found in your version of BGP. What would you use to see all of the BGP packets on the network?
8. You are looking at an access list on your firewall. This access list has additional **permit** statements that you know, for a fact, are not in the configuration. How do you explain this?
9. What is the purpose of an authentication proxy server?

Exam Topic List

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

- **Configure a Cisco IOS Firewall Using the CLI**—Describes the five steps that enable you to configure a simple firewall using the CLI.

- **Configure a Basic Firewall Using SDM**—Explains how replacing the CLI with a graphical interface, the Basic Firewall Wizard, makes configurations quick, accurate, and intuitive.

- **Configure an Advanced Firewall Using SDM**—Describes how adding a DMZ or configuring multiple untrusted networks through the Advanced Firewall Wizard combines ease of use with multiple options to provide for all your configuration needs.