

Cisco IOS Firewall Overview

This chapter describes how you can configure your Cisco networking device to function as a firewall, using Cisco IOS security features.

This chapter has the following sections:

- Overview of Firewalls
- The Cisco IOS Firewall Solution
- Create a Customized Firewall
- Other Guidelines for Configuring a Firewall

Overview of Firewalls

Firewalls are networking devices that control access to your organization's network assets. Firewalls are positioned at the entrance points into your network. If your network has multiple entrance points, you must position a firewall at each point to provide effective network access control.

Firewalls are often placed in between the internal network and an external network such as the Internet. With a firewall between your network and the Internet, all traffic coming from the Internet must pass through the firewall before entering your network.

Firewalls can also be used to control access to a specific part of your network. For example, you can position firewalls at all the entry points into a research and development network to prevent unauthorized access to proprietary information.

The most basic function of a firewall is to monitor and filter traffic. Firewalls can be simple or elaborate, depending on your network requirements. Simple firewalls are usually easier to configure and manage. However, you might require the flexibility of a more elaborate firewall.

The Cisco IOS Firewall Solution

Cisco IOS software provides an extensive set of security features, allowing you to configure a simple or elaborate firewall, according to your particular requirements. You can configure a Cisco device as a firewall if the device is positioned appropriately at a network entry point. Security features that provide firewall functionality are listed in the section "Create a Customized Firewall."

In addition to the security features available in standard Cisco IOS feature sets, there is a Cisco IOS Firewall feature set that gives your router additional firewall capabilities.

The Cisco IOS Firewall Feature Set

The Cisco IOS Firewall feature set combines existing Cisco IOS firewall technology and the new context-based access control (CBAC) feature. When you configure the Cisco IOS Firewall feature set on your Cisco router, you turn your router into an effective, robust firewall.

The Cisco IOS Firewall feature set is designed to prevent unauthorized, external individuals from gaining access to your internal network, and to block attacks on your network, while at the same time allowing authorized users to access network resources.

You can use the Cisco IOS Firewall feature set to configure your Cisco IOS router as:

- An Internet firewall or part of an Internet firewall
- A firewall between groups in your internal network
- A firewall providing secure connections to or from branch offices
- A firewall between your company's network and your company's partners' networks

The Cisco IOS Firewall feature set provides the following benefits:

- Protects internal networks from intrusion
- Monitors traffic through network perimeters
- Enables network commerce via the World Wide Web

Create a Customized Firewall

To create a firewall customized to fit your organization's security policy, you should determine which Cisco IOS security features are appropriate, and configure those features. At a minimum, you must configure basic traffic filtering to provide a basic firewall. You can configure your Cisco networking device to function as a firewall by using the following Cisco IOS security features:

- Standard Access Lists and Static Extended Access Lists
- Lock-and-Key (Dynamic Access Lists)
- Reflexive Access Lists
- TCP Intercept
- Context-Based Access Control
- Security Server Support
- Network Address Translation
- Cisco Encryption Technology
- IPSec Network Security
- Neighbor Router Authentication
- Event Logging
- User Authentication and Authorization

As well as configuring these features, you should follow the guidelines listed in the section "Other Guidelines for Configuring Your Firewall." This section outlines important security practices to protect your firewall and network. Table 17 describes Cisco IOS security features.

Table 17 Cisco IOS Features for a Robust Firewall

Feature	Chapter	Comments
Standard Access Lists and Static Extended Access Lists	“Access Control Lists: Overview and Guidelines”	<p>Standard and static extended access lists provide basic traffic filtering capabilities. You configure criteria that describe which packets should be forwarded, and which packets should be dropped at an interface, based on each packet’s network layer information. For example, you can block all UDP packets from a specific source IP address or address range. Some extended access lists can also examine transport layer information to determine whether to block or forward packets.</p> <p>To configure a basic firewall, you should at a minimum configure basic traffic filtering. You should configure basic access lists for all network protocols that will be routed through your firewall, such as IP, IPX, AppleTalk, and so forth.</p>
Lock-and-Key (Dynamic Access Lists)	“Configuring Lock-and-Key Security (Dynamic Access Lists)”	<p>Lock-and-Key provides traffic filtering with the ability to allow temporary access through the firewall for certain individuals. These individuals must first be authenticated (by a username/password mechanism) before the firewall allows their traffic through the firewall. Afterwards, the firewall closes the temporary opening. This provides tighter control over traffic at the firewall than with standard or static extended access lists.</p>
Reflexive Access Lists	“Configuring IP Session Filtering (Reflexive Access Lists)”	<p>Reflexive access lists filter IP traffic so that TCP or UDP “session” traffic is only permitted through the firewall if the session originated from within the internal network.</p> <p>You would only configure Reflexive Access Lists when not using Context-Based Access Control.</p>
TCP Intercept	“Configuring TCP Intercept (Prevent Denial-of-Service Attacks)”	<p>TCP Intercept protects TCP servers within your network from TCP SYN-flooding attacks, a type of denial-of-service attack.</p> <p>You would only configure TCP Intercept when not using Context-Based Access Control.</p>
Context-Based Access Control	“Configuring Context-Based Access Control”	<p>Context-Based Access Control (CBAC) examines not only network layer and transport layer information, but also examines the application-layer protocol information (such as FTP information) to learn about the state of TCP and UDP connections. CBAC maintains connection state information for individual connections. This state information is used to make intelligent decisions about whether packets should be permitted or denied, and dynamically creates and deletes temporary openings in the firewall.</p> <p>CBAC is only available in the Cisco IOS Firewall Feature Set.</p>
Security Server Support	“Configuring TACACS+,” “Configuring TACACS and Extended TACACS,” “Configuring RADIUS,” and “Configuring Kerberos”	<p>The Cisco IOS Firewall feature set can be configured as a client of the following supported security servers:</p> <ul style="list-style-type: none"> • TACACS, TACACS+, and Extended TACACS • RADIUS • Kerberos <p>You can use any of these security servers to store a database of user profiles. To gain access into your firewall or to gain access through the firewall into another network, users must enter authentication information (such as a username and password), which is matched against the information on the security server. When users pass authentication, they are granted access according to their specified privileges.</p>

Table 17 Cisco IOS Features for a Robust Firewall (Continued)

Feature	Chapter	Comments
Network Address Translation	“Configuring IP Addressing” chapter in the <i>Network Protocols Configuration Guide, Part 1</i>	<p>You can use Network Address Translation (NAT) to hide internal IP network addresses from the world outside the firewall.</p> <p>NAT was designed to provide IP address conservation and for internal IP networks that have unregistered (not globally unique) IP addresses: NAT translates these unregistered IP addresses into legal addresses at the firewall. NAT can also be configured to advertise only one address for the entire internal network to the outside world. This provides security by effectively hiding the entire internal network from the world.</p> <p>NAT gives you limited spoof protection because internal addresses are hidden. Additionally, NAT removes all your internal services from the external name space.</p> <p>NAT does not work with the application-layer protocols RPC, VDOLive, or SQL*Net “Redirected.” (NAT does work with SQL*Net “Bequeathed.”) Do not configure NAT with networks that will carry traffic for these incompatible protocols.</p>
Cisco Encryption Technology	“Configuring Cisco Encryption Technology”	<p>Cisco Encryption Technology (CET) selectively encrypts IP packets that are transmitted across unprotected networks such as the Internet. You specify which traffic is considered sensitive and should be encrypted. This encryption prevents sensitive IP packets from being intercepted and read or tampered with.</p>
IPSec Network Security	“Configuring IPSec Network Security”	<p>IPSec is a framework of open standards developed by the Internet Engineering Task Force (IETF) that provides security for transmission of sensitive information over unprotected networks such as the Internet. IPSec acts at the network layer, protecting and authenticating IP packets between participating IPSec devices (“peers”) such as Cisco routers.</p> <p>IPSec services are similar to those provided by Cisco Encryption Technology, a proprietary security solution introduced in Cisco IOS Software Release 11.2. (The IPSec standard was not yet available at Release 11.2.) However, IPSec provides a more robust security solution, and is standards-based.</p>
Neighbor Router Authentication	“Neighbor Router Authentication: Overview and Guidelines”	<p>Neighbor router authentication requires the firewall to authenticate all neighbor routers before accepting any route updates from that neighbor. This ensures that the firewall receives legitimate route updates from a trusted source.</p>
Event Logging	“Troubleshooting the Router” chapter in the “System Management” part of the <i>Configuration Fundamentals Configuration Guide</i>	<p>Event logging automatically logs output from system error messages and other events to the console terminal. You can also redirect these messages to other destinations such as virtual terminals, internal buffers, or syslog servers. You can also specify the severity of the event to be logged, and you can configure the logged output to be timestamped. The logged output can be used to assist real-time debugging and management, and to track potential security breaches or other nonstandard activities throughout a network.</p>
User Authentication and Authorization	“Configuring Authentication” and “Configuring Authorization”	<p>Authentication and authorization help protect your network from access by unauthorized users.</p>

Other Guidelines for Configuring a Firewall

As with all networking devices, you should always protect access into the firewall by configuring passwords as described in the chapter “Configuring Passwords and Privileges.” You should also consider configuring user authentication, authorization, and accounting as described in the chapters in the “Authentication, Authorization, and Accounting (AAA)” part of this document.

You should also consider the following recommendations:

- When setting passwords for privileged access to the firewall, use the **enable secret** command rather than the **enable password** command, which does not have as strong an encryption algorithm.
- Put a password on the console port. In authentication, authorization, and accounting (AAA) environments, use the same authentication for the console as for elsewhere. In a non-AAA environment, at a minimum configure the **login** and **password password** commands.
- Think about access control *before* you connect a console port to the network in any way, including attaching a modem to the port. Be aware that a *break* on the console port might give total control of the firewall, even with access control configured.
- Apply access lists and password protection to all virtual terminal ports. Use access lists to limit who can Telnet into your router.
- Do not enable any local service (such as SNMP or NTP) that you do not use. Cisco Discovery Protocol (CDP) and Network Time Protocol (NTP) are on by default, and you should turn these off if you do not need them.

To turn off CDP, enter the **no cdp run** global configuration command. To turn off NTP, enter the **ntp disable** interface configuration command on each interface not using NTP.

If you must run NTP, configure NTP only on required interfaces, and configure NTP to listen only to certain peers.

Any enabled service could present a potential security risk. A determined, hostile party might be able to find creative ways to misuse the enabled services to access the firewall or the network.

For local services that are enabled, protect against misuse. Protect by configuring the services to communicate only with specific peers, and protect by configuring access lists to deny packets for the services at specific interfaces.

- Protect against spoofing: protect the networks on both sides of the firewall from being spoofed from the other side. You could protect against spoofing by configuring input access lists at all interfaces to pass only traffic from expected source addresses, and to deny all other traffic.

You should also disable source routing. For IP, enter the **no ip source-route** global configuration command. Disabling source routing at *all* routers can also help prevent spoofing.

You should also disable minor services. For IP, enter the **no service tcp-small-servers** and **no service udp-small-servers** global configuration commands.

- Prevent the firewall from being used as a relay by configuring access lists on any asynchronous Telnet ports.
- Normally, you should disable directed broadcasts for all applicable protocols on your firewall and on all your other routers. For IP, use the **no ip directed-broadcast** command. Rarely, some IP networks do require directed broadcasts; if this is the case, do not disable directed broadcasts.

Directed broadcasts can be misused to multiply the power of denial-of-service attacks, because every denial-of-service packet sent is broadcast to every host on a subnet. Furthermore, some hosts have other intrinsic security risks present when handling broadcasts.

Other Guidelines for Configuring a Firewall

- Configure the **no ip proxy-arp** command to prevent internal addresses from being revealed. (This is important to do if you do not already have NAT configured to prevent internal addresses from being revealed).
- Keep the firewall in a secured (locked) room.