



CHAPTER 11

Configuring Security Features

This chapter gives an overview of authentication, authorization, and accounting (AAA), the primary Cisco framework for implementing selected security features that can be configured on the Cisco Secure Router 520 Series routers.



Note

Individual router models may not support every feature described throughout this guide. Features not supported by a particular router are indicated whenever possible.

This chapter contains the following sections:

- [Authentication, Authorization, and Accounting](#)
- [Configuring AutoSecure](#)
- [Configuring Access Lists](#)
- [Configuring a CBAC Firewall](#)
- [Configuring Cisco IOS Firewall IDS](#)
- [Configuring VPNs](#)

Each section includes a configuration example and verification steps, where available.

Authentication, Authorization, and Accounting

AAA network security services provide the primary framework through which you set up access control on your router. Authentication provides the method of identifying users, including login and password dialog, challenge and response, messaging support, and, depending on the security protocol you choose, encryption. Authorization provides the method for remote access control, including one-time authorization or authorization for each service, per-user account list and profile, user group support, and support of IP, Internetwork Packet Exchange (IPX), AppleTalk Remote Access (ARA), and Telnet. Accounting provides the method for collecting and sending security server information used for billing, auditing, and reporting, such as user identities, start and stop times, executed commands (such as PPP), number of packets, and number of bytes.

AAA uses protocols such as RADIUS, TACACS+, or Kerberos to administer its security functions. If your router is acting as a network access server, AAA is the means through which you establish communication between your network access server and your RADIUS, TACACS+, or Kerberos security server.

For information about configuring AAA services and supported security protocols, see the following sections of the *Cisco IOS Security Configuration Guide*:

- [Configuring Authentication](#)
- [Configuring Authorization](#)
- [Configuring Accounting](#)
- [Configuring RADIUS](#)
- [Configuring TACACS+](#)
- [Configuring Kerberos](#)

Configuring AutoSecure

The AutoSecure feature disables common IP services that can be exploited for network attacks and enables IP services and features that can aid in the defense of a network when under attack. These IP services are all disabled and enabled simultaneously with a single command, greatly simplifying security configuration on your router. For a complete description of the AutoSecure feature, see the *AutoSecure* feature document.

Configuring Access Lists

Access lists (ACLs) permit or deny network traffic over an interface based on source IP address, destination IP address, or protocol. Access lists are configured as standard or extended. A standard access list either permits or denies passage of packets from a designated source. An extended access list allows designation of both the destination and the source, and it allows designation of individual protocols to be permitted or denied passage. An access list is a series of commands with a common tag to bind them together. The tag is either a number or a name. [Table 11-1](#) lists the commands used to configure access lists.

Table 11-1 Access List Configuration Commands

ACL Type	Configuration Commands
Numbered	
Standard	access-list { 1-99 } { permit deny } source-addr [source-mask]
Extended	access-list { 100-199 } { permit deny } protocol source-addr [source-mask] destination-addr [destination-mask]
Named	
Standard	ip access-list standard name followed by deny {source source-wildcard any}
Extended	ip access-list extended name followed by {permit deny} protocol {source-addr[source-mask] any} {destination-addr [destination-mask] any}

Access Groups

A sequence of access list definitions bound together with a common name or number is called an access group. An access group is enabled for an interface during interface configuration with the following command:

```
ip access-group {access-list-number | access-list-name} {in | out}
```

where **in** | **out** refers to the direction of travel of the packets being filtered.

Guidelines for Creating Access Groups

Use the following guidelines when creating access groups.

- The order of access list definitions is significant. A packet is compared against the first access list in the sequence. If there is no match (that is, if neither a permit nor a deny occurs), the packet is compared with the next access list, and so on.
- All parameters must match the access list before the packet is permitted or denied.
- There is an implicit “deny all” at the end of all sequences.

For more complete information on creating access lists, see the “[Access Control Lists: Overview and Guidelines](#)” section of the *Cisco IOS Release 12.3 Security Configuration Guide*.

Configuring a CBAC Firewall

Context-Based Access Control (CBAC) lets you configure a stateful firewall where packets are inspected internally and the state of network connections is monitored. This is superior to static access lists, because access lists can only permit or deny traffic based on individual packets, not streams of packets. Also, because CBAC inspects the packets, decisions to permit or deny traffic can be made by examining application layer data, something static access lists cannot do.

To configure a CBAC firewall, specify which protocols to examine by using the following command in interface configuration mode:

```
ip inspect name inspection-name protocol timeout seconds
```

When inspection detects that the specified protocol is passing through the firewall, a dynamic access list is created to allow the passage of return traffic. The **timeout** parameter specifies the length of time the dynamic access list remains active without return traffic passing through the router. When the timeout value is reached, the dynamic access list is removed, and subsequent packets (possibly valid ones) are not permitted.

Use the same inspection name in multiple statements to group them into one set of rules. This set of rules can be activated elsewhere in the configuration by using the **ip inspect *inspection-name* in | out** command when you configure an interface at the firewall.

See [Chapter 8, “Configuring a Simple Firewall,”](#) for a sample configuration. For additional information about configuring a CBAC firewall, see the “[Configuring Context-Based Access Control](#)” section of the *Cisco IOS Release 12.3 Security Configuration Guide*.

Configuring Cisco IOS Firewall IDS

Cisco IOS Firewall Intrusion Detection System (IDS) technology enhances perimeter firewall protection by taking appropriate action on packets and flows that violate the security policy or represent malicious network activity.

Cisco IOS Firewall IDS identifies 59 of the most common attacks using “signatures” to detect patterns of misuse in network traffic. It acts as an in-line intrusion detection sensor, watching packets and sessions as they flow through the router, scanning each to match any of the IDS signatures. When it detects suspicious activity, it responds before network security can be compromised, logs the event, and, depending on configuration, sends an alarm, drops suspicious packets, or resets the TCP connection.

For additional information about configuring Cisco IOS Firewall IDS, see the “[Configuring Cisco IOS Firewall Intrusion Detection System](#)” section of the *Cisco IOS Release 12.3 Security Configuration Guide*.

Configuring VPNs

A virtual private network (VPN) connection provides a secure connection between two networks over a public network such as the Internet. Cisco Secure Router 520 Series routers support site-to-site VPNs using IP security (IPsec) tunnels and generic routing encapsulation (GRE). Permanent VPN connections between two peers, or dynamic VPNs using EZVPN which create and tear down VPN connections as needed, can be configured. [Chapter 6, “Configuring a VPN Using Easy VPN and an IPsec Tunnel,”](#) and [Chapter 7, “Configuring VPNs Using an IPsec Tunnel and Generic Routing Encapsulation,”](#) show examples of how to configure your router with these features. For more information about IPsec and GRE configuration, see the “[Configuring IPsec Network Security](#)” chapter of the *Cisco IOS Release 12.3 Security Configuration Guide*.

For information about additional VPN configurations supported by Cisco Secure Router 520 Series routers, see the [EZVPN Server](#) feature document. Cisco Secure Router 520 Series routers can be configured to act as EZVPN servers, letting authorized EZVPN clients establish dynamic VPN tunnels to the connected network.