



CHAPTER 8

Configuring a Simple Firewall

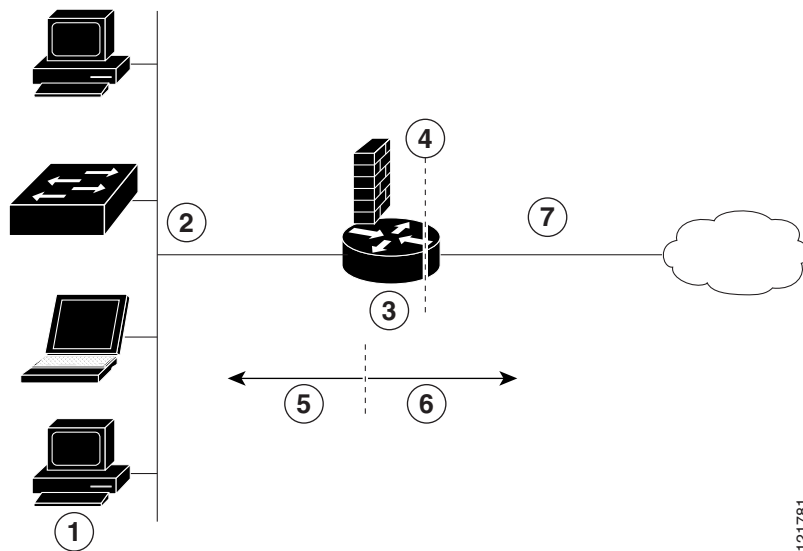
The Cisco Secure Router 520 Series routers support network traffic filtering by means of access lists. The routers also support packet inspection and dynamic temporary access lists by means of Context-Based Access Control (CBAC).

Basic traffic filtering is limited to configured access list implementations that examine packets at the network layer or, at most, the transport layer, permitting or denying the passage of each packet through the firewall. However, the use of inspection rules in CBAC allows the creation and use of dynamic temporary access lists. These dynamic lists allow temporary openings in the configured access lists at firewall interfaces. These openings are created when traffic for a specified user session exits the internal network through the firewall. The openings allow returning traffic for the specified session (that would normally be blocked) back through the firewall.

See the [Cisco IOS Security Configuration Guide, Release 12.3](#), for more detailed information on traffic filtering and firewalls.

Figure 8-1 shows a network deployment using PPPoE or PPPoA with NAT and a firewall.

Figure 8-1 Router with Firewall Configured



1	Multiple networked devices—Desktops, laptop PCs, switches
2	Fast Ethernet LAN interface (the inside interface for NAT)
3	PPPoE or PPPoA client and firewall implementation—Cisco Secure Router 520 Series router
4	Point at which NAT occurs
5	Protected network
6	Unprotected network
7	Fast Ethernet or ATM WAN interface (the outside interface for NAT)

In the configuration example that follows, the firewall is applied to the outside WAN interface (FE4) and protects the Fast Ethernet LAN on FE0 by filtering and inspecting all traffic entering the router on the Fast Ethernet WAN interface FE4. Note that in this example, the network traffic originating from the corporate network, network address 10.1.1.0, is considered safe traffic and is not filtered.

Configuration Tasks

Perform the following tasks to configure this network scenario:

- [Configure Access Lists](#)
- [Configure Inspection Rules](#)
- [Apply Access Lists and Inspection Rules to Interfaces](#)

A configuration example that shows the results of these configuration tasks is provided in the “Configuration Example” section on page 8-5.

**Note**

The procedures in this chapter assume that you have already configured basic router features as well as PPPoE or PPPoA with NAT. If you have not performed these configurations tasks, see [Chapter 1, “Basic Router Configuration,”](#) [Chapter 3, “Configuring PPP over Ethernet with NAT,”](#) and [Chapter 4, “Configuring PPP over ATM with NAT,”](#) as appropriate for your router. You may have also configured DHCP, VLANs, and secure tunnels.

Configure Access Lists

Perform these steps to create access lists for use by the firewall, beginning in global configuration mode:

	Command	Purpose
Step 1	<p>access-list <i>access-list-number</i> {deny permit} <i>protocol source source-wildcard [operator [port]] destination</i></p> <p>Example:</p> <pre>Router(config)# access-list 103 deny ip any any Router(config)# access-list 103 permit host 200.1.1.1 eq isakmp any Router(config)#</pre>	<p>Creates an access list which prevents Internet-initiated traffic from reaching the local (inside) network of the router, and which compares source and destination ports.</p> <p>See the Cisco IOS IP Command Reference, Volume 1 of 4: Addressing and Services for details about this command.</p>
Step 2	<p>access-list <i>access-list-number</i> {deny permit} <i>protocol source source-wildcard destination destination-wildcard</i></p> <p>Example:</p> <pre>Router(config)# access-list 105 permit ip 10.1.1.0 0.0.0.255 192.168.0.0 0.0.255.255 Router(config)#</pre>	<p>Creates an access list that allows network traffic to pass freely between the corporate network and the local networks through the configured VPN tunnel.</p>

Configure Inspection Rules

Perform these steps to configure firewall inspection rules for all TCP and UDP traffic, as well as specific application protocols as defined by the security policy, beginning in global configuration mode:

	Command or Action	Purpose
Step 1	<p>ip inspect name <i>inspection-name protocol</i></p> <p>Example:</p> <pre>Router(config)# ip inspect name firewall tcp Router(config)#</pre>	Defines an inspection rule for a particular protocol.
Step 2	<p>ip inspect name <i>inspection-name protocol</i></p> <p>Example:</p> <pre>Router(config)# ip inspect name firewall rtsp Router(config)# ip inspect name firewall h323 Router(config)# ip inspect name firewall netshow Router(config)# ip inspect name firewall ftp Router(config)# ip inspect name firewall sqlnet Router(config)#</pre>	Repeat this command for each inspection rule that you wish to use.

Apply Access Lists and Inspection Rules to Interfaces

Perform these steps to apply the ACLs and inspection rules to the network interfaces, beginning in global configuration mode:

	Command	Purpose
Step 1	<p>interface <i>type number</i></p> <p>Example:</p> <pre>Router(config)# interface vlan 1 Router(config-if)#</pre>	Enters interface configuration mode for the inside network interface on your router.
Step 2	<p>ip inspect <i>inspection-name {in out}</i></p> <p>Example:</p> <pre>Router(config-if)# ip inspect firewall in Router(config-if)#</pre>	Assigns the set of firewall inspection rules to the inside interface on the router.
Step 3	<p>exit</p> <p>Example:</p> <pre>Router(config-if)# exit Router(config)#</pre>	Returns to global configuration mode.

	Command	Purpose
Step 4	interface <i>type number</i> Example: Router(config)# interface fastethernet 4 Router(config-if)#	Enters interface configuration mode for the outside network interface on your router.
Step 5	ip access-group { <i>access-list-number</i> <i>access-list-name</i> } { in out } Example: Router(config-if)# ip access-group 103 in Router(config-if)#	Assigns the defined ACLs to the outside interface on the router.
Step 6	exit Example: Router(config-if)# exit Router(config)#	Returns to global configuration mode.

Configuration Example

A telecommuter is granted secure access to a corporate network, using IPsec tunneling. Security to the home network is accomplished through firewall inspection. The protocols that are allowed are all TCP, UDP, RTSP, H.323, NetShow, FTP, and SQLNet. There are no servers on the home network; therefore, no traffic is allowed that is initiated from outside. IPsec tunneling secures the connection from the home LAN to the corporate network.

Like the Internet Firewall Policy, HTTP need not be specified because Java blocking is not necessary. Specifying TCP inspection allows for single-channel protocols such as Telnet and HTTP. UDP is specified for DNS.

The following configuration example shows a portion of the configuration file for the simple firewall scenario described in the preceding sections.

```

!
! Firewall inspection is set up for all TCP and UDP traffic as well as
! specific application protocols as defined by the security policy.
ip inspect name firewall tcp
ip inspect name firewall udp
ip inspect name firewall rtsp
ip inspect name firewall h323
ip inspect name firewall netshow
ip inspect name firewall ftp
ip inspect name firewall sqlnet
!
interface vlan 1! This is the internal home network.
ip inspect firewall in ! Inspection examines outbound traffic.
no cdp enable
!
interface fastethernet 4! FE4 is the outside or Internet-exposed interface.
! acl 103 permits IPsec traffic from the corp. router
! as well as denies Internet-initiated traffic inbound.
ip access-group 103 in

```

```
ip nat outside
no cdp enable
!
! acl 103 defines traffic allowed from the peer for the IPsec tunnel.
access-list 103 permit udp host 200.1.1.1 any eq isakmp
access-list 103 permit udp host 200.1.1.1 eq isakmp any
access-list 103 permit esp host 200.1.1.1 any
! Allow ICMP for debugging but should be disabled because of security implications.
access-list 103 permit icmp any any
access-list 103 deny ip any any ! Prevents Internet-initiated traffic inbound.
! acl 105 matches addresses for the ipsec tunnel to or from the corporate network.
access-list 105 permit ip 10.1.1.0 0.0.0.255 192.168.0.0 0.0.255.255
no cdp run
!
```