IP Receive ACL

Feature History

Release	Modification
12.0(22)S	This feature was introduced on the Cisco 12000 platform.
12.0(24)S	Support was added for the Cisco 7500 series.

This document describes the IP Receive ACL feature in Cisco IOS Release 12.0(24)S. It includes the following sections:

- Feature Overview, page 1
- Supported Platforms, page 2
- Supported Standards, MIBs, and RFCs, page 3
- Configuration Tasks, page 3
- Configuration Examples, page 4
- Command Reference, page 4

Feature Overview

The IP Receive ACL feature provides basic filtering capability for traffic that is destined for the router; that is, the router can protect high-priority routing protocol traffic from an attack because the filtering occurs after any input access control list (ACL) on the ingress interface.

This feature may be implemented in a security solution to protect a router from remote intrusions. Access to the router can be restricted to known, trusted sources and expected traffic profiles.

Benefits

On distributed platforms, such as the Cisco 12000 series, the IP receive ACL filters traffic on the distributed line cards before packets are received by the route processor. This feature allows the users to filter denial of service (DoS) floods against the router, thereby preventing the flood from degrading the performance of the route processor.

Restrictions

A named ACL cannot be used as the receive ACL.

Related Features and Technologies

- Dynamic extended IP access lists that grant access per user to a specific source or destination host basis through a user authentication process. In essence, you can allow user access through a firewall dynamically, without compromising security restrictions. For more information, refer to the chapter "Configuring Lock-and-Key Security (Dynamic Access Lists)" of the *Cisco IOS Security Configuration Guide*, Release 12.0.
- Reflexive access lists that allow IP packets to be filtered based on session information. Reflexive access lists contain temporary entries and are nested within an extended, named IP access list. For information on reflexive access lists, refer to the chapter "Configuring IP Session Filtering (Reflexive Access Lists)" in the *Cisco IOS Security Configuration Guide*, Release 12.0.

Related Documents

- The chapter "Access Control Lists: Overview and Guidelines" in the *Cisco IOS Security Configuration Guide*, Release 12.0
- The chapter "Configuring IP Services" in the *Cisco IOS Release 12.0 Network Protocols Configuration Guide, Part 1*
- The chapter "IP Services Commands" in the *Cisco IOS Release 12.0 Network Protocols Command Reference, Part 1*

Supported Platforms

Cisco IOS Release 12.0(22)S Only

- Cisco 12000 series

This feature is available in all Internet router images.

Cisco IOS Release 12.0(24)S Only

- Cisco 7500 series

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Supported Standards, MIBs, and RFCs

Standards

None

MIBs

None

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

http://www.cisco.com/go/mibs

RFCs

None

Configuration Tasks

See the following sections for configuration tasks for the IP Receive ACL feature. Each task in the list is identified as either required or optional.

- Configuring IP Receive ACLs (required)
- Verifying IP Receive ACLs (optional)

Configuring IP Receive ACLs

To enable receive ACLs, use the following command in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# ip receive access-list number`	Activates receive ACLs and begins filtering packets destined for the router.

Step 2	`Router(config)# access-list access-list-number {deny | permit} source [source-wildcard] [log]`
	
	OR
	
	`Router (config)# access-list access-list-number [dynamic dynamic-name [timeout minutes]] {deny | permit} protocol source source-wildcard destination destination-wildcard [precedence precedence] [tos tos] [log | log-input] [time-range time-range-name]`
		Defines a standard IP access list or an extended IP access list, respectively.

Verifying IP Receive ACLs

To verify ACL configurations, use at least one of the following EXEC commands:

Command	Purpose
Router# **show access-lists**	Displays the contents of all access lists.
Router# **show ip access-list**	Displays the contents of one access list.

Configuration Examples

This section provides the following configuration example:

- IP Receive ACL Configuration Example

IP Receive ACL Configuration Example

The following example shows how to permit ospf, bgp from one host, and allow the router to respond to pings (excluding fragmented pings):

```
ip receive access-list 100
access-list 100 deny icmp any any fragments
access-list 100 permit icmp any any echo
access-list 100 permit tcp 192.168.1.0 0.0.0.255 any eq 22
access-list 100 permit ospf any any precedence internet
access-list 100 permit tcp host 10.0.0.1 any eq bgp precedence internet
access-list 100 deny ip any any
```

Command Reference

This section documents a new command. All other commands used with this feature are documented in the Cisco IOS Release 12.0 command reference publications.

- **ip receive access-list**

ip receive access-list

To activate a receive access control list (ACL), use the **ip receive access-list** command in global configuration mode. To deactivate an ACL and allow the router to receive all traffic, use the **no** form of this command.

ip receive access-list *number*

no ip receive access-list *number*

Syntax Description

number	The receive ACL. **Note** A named ACL cannot be used as the receive ACL.

Defaults

Receive ACLs are not activated, and all traffic is permitted.

Command Modes

Global configuration

Command History

Release	Modification
12.0(22)S	This command was introduced on the Cisco 12000 series platform.
12.0(24)S	Support for the Cisco 7500 series platform was added.

Usage Guidelines

Use the **ip receive access-list** command to configure a receive ACL that will filter packets destined to the router.

Examples

The following example shows how to permit ospf, bgp from one host, and allow the router to respond to pings (excluding fragmented pings):

```
ip receive access-list 100
access-list 100 deny icmp any any fragments
access-list 100 permit icmp any any echo
access-list 100 permit tcp 192.168.1.0 0.0.0.255 any eq 22
access-list 100 permit ospf any any precedence internet
access-list 100 permit tcp host 10.0.0.1 any eq bgp precedence internet
access-list 100 deny ip any any
```

Related Commands

Command	Description
access-list (IP extended)	Defines an extended IP access list.
access-list (IP standard)	Defines a standard IP access list.