



IP Receive ACL

Part Number OL-8697-01 (Rev A0), January 19, 2006

The IP Receive ACL feature provides basic filtering capability for IPv4 and IPv6 traffic that is received on a router with the following benefits:

- The router can protect high-priority routing protocol traffic from an attack because filtering occurs after an input access control list (ACL) is applied on the ingress interface.
- You can implement this feature in a security solution to protect a router from remote intrusions and to limit access to Cisco IOS services if unwanted services are inadvertently left enabled. Access to the router can be restricted to known, trusted sources and expected traffic profiles.
- 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.

Feature History

Release	Modification
12.0(22)S	This feature was introduced on the Cisco 12000 series Internet router.
12.0(24)S	This feature was implemented on the Cisco 7500 series.
12.0(31)S	This feature was implemented on the Cisco 10720 Internet Router.
12.0(31)S3 12.0(32)S	This feature was enhanced to filter IPv6 traffic on the Cisco 12000 series Internet router.

Contents

- [Prerequisites for IP Receive ACL, page 2](#)
- [Restrictions for IP Receive ACL, page 2](#)
- [Information About IP Receive ACL, page 2](#)
- [Configuring an IP Receive ACL, page 4](#)
- [Monitoring and Maintaining IP Receive ACL, page 6](#)
- [Configuration Examples for IP Receive ACL, page 6](#)



Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Copyright © 2006 Cisco Systems, Inc. All rights reserved.

- [Additional References, page 7](#)
- [Command Reference, page 8](#)

Prerequisites for IP Receive ACL

Before you configure the IP Receive ACL feature, you must first create the ACL that you want to use to pass or deny traffic, using the **access-list** (for IPv4 traffic) or **ipv6 access-list** (for IPv6 traffic) command.

Restrictions for IP Receive ACL

Named ACLs

A named ACL for IPv4 traffic is not supported as the receive ACL.

IPv6 ACLs

When you create a receive ACL using an IPv6 ACL, you must define a unique ACL name (IPv6 does not support numbered ACLs). An IPv4 ACL and an IPv6 ACL cannot share the same name.

Link Bundling

Link-bundling isn't supported for any IPv6 feature, including IPv6 ACLs.

Cisco 10720 Specific Restrictions

On the Cisco 10720 Internet Router, the IP Receive ACL feature is implemented with the following restrictions:

- The IP Receive ACL feature is applied only to IPv4 traffic destined for the Route Processor (RP), with the exception of IPv4 options.
- The IP Receive ACL feature supports only standard and extended access lists. You cannot use a named ACL as the receive ACL.
- Because ICMP ping replies are implemented in PXF (not in the Route Processor as on other platforms), you must configure ICMP filtering separately on each 10720 input interface (not on the RP interface).

Information About IP Receive ACL

To configure the IP Receive ACL feature, you should understand the following concepts:

- [Using Access Control Lists, page 2](#)
- [Using an IP Receive ACL, page 3](#)

Using Access Control Lists

Packet filtering helps control packet movement through the network. Such control can help limit network traffic and restrict network use by certain users or devices. To permit or deny packets from crossing specified interfaces, use *access control lists* (also referred to as *access lists*).

An access list is a sequential collection of permit and deny conditions that apply to IP addresses. The Cisco IOS software tests addresses against the conditions in an access list one by one. The first match determines whether the software accepts or rejects the address. Because the software stops testing conditions after the first match, the order of the conditions is critical. If no conditions match, the software rejects the address.

The two main tasks involved in using access lists are as follows:

1. Create an access list by specifying an access list number or name and access conditions.
2. Apply the access list to interfaces or terminal lines.

Cisco IOS software supports the following types of access lists for IP packet filtering:

- Standard IP access lists that use source addresses for matching operations.
- Extended IP access lists that use source and destination addresses for matching operations, and optional protocol type information for finer filtering.
- Dynamic extended IP access lists that grant access per user to a specific source or destination host basis through a user authentication process. You can allow user access through a firewall dynamically, without compromising security restrictions. Dynamic access lists and lock-and-key access are described in “[Configuring Lock-and-Key Security \(Dynamic Access Lists\)](#)” in the *Cisco IOS Security Configuration Guide*.
- 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 “[Configuring IP Session Filtering \(Reflexive Access Lists\)](#)” chapter in the *Cisco IOS Security Configuration Guide* and the “[Reflexive Access List Commands](#)” chapter in the *Cisco IOS Security Command Reference*.

For detailed information on how to create and use different types of access lists, refer to:

- “[Configuring IP Services](#)” chapter in *Cisco IOS IP Configuration Guide*, Release 12.3
- “[Access Control Lists: Overview and Guidelines](#)” chapter in *Cisco IOS Security Configuration Guide*, Release 12.3

The following example shows how to create a numbered access list. In this example, network 36.0.0.0 is a Class A network whose second octet specifies a subnet; that is, its subnet mask is 255.255.0.0. The third and fourth octets of a network 36.0.0.0 address specify a particular host. Using access list 2, the Cisco IOS software accepts one address on subnet 48 and rejects all others on that subnet. The last line of the list shows that the software accepts addresses on all other network 36.0.0.0 subnets.

```
access-list 2 permit 36.48.0.3
access-list 2 deny 36.48.0.0 0.0.255.255
access-list 2 permit 36.0.0.0 0.255.255.255
interface ethernet 0
 ip access-group 2 in
```

Using an IP Receive ACL

You can configure an ACL that you have created to filter IPv4 or IPv6 traffic to process receive IP packets and reduce the CPU load on the route processor of unwanted traffic. In this way, you mitigate the adverse effects of denial-of-service attacks against the router. On a distributed platform, such as the Cisco 12000 series, the IP receive ACL filters traffic on the distributed line cards before IP packets are punted to the route processor, including:

- Local addresses configured on router interfaces
- Multicast groups of which the router is a member

- Link-local unicast and multicast addresses

The following counters are updated for packets processed by the IP Receive ACL feature:

- Access control entry (ACE) counters—Displayed with the **show access-lists** and **show ipv6 access-list** commands or, on a Cisco 12000 series ISE line card, with the **show access-lists hardware interface interface-type slot:port [in | out]** command, after you connect to the Cisco IOS image running on the line card using the **attach slot-number** command:
- "Receive policy deny" counter for dropped packets—Displayed with the **execute-on slot show controller events** command on a Cisco 12000 series Internet router.

The IP Receive ACL feature is designed to be used in any of the following ways, depending on your network configuration and security goals:

- Always-on configuration—After you determine the amount of control-plane traffic to be handled by the router, configure an ACL with the set of rules that explicitly permits desired IP packets. At the end of the ACL configuration, include a final **deny** statement to block all other traffic: **deny ip any any** (for IPv4 traffic) or **deny ipv6 any any** (for IPv6 traffic).
- Reactive configuration—Either you do not configure a receive ACL to be used by default, or you configure a very permissive receive ACL. You can include an explicit rule to block a denial-of-service attack for when the routers detects an attack.
- Traffic analysis —You can configure a receive ACL with **permit** statements to collect counters for the various types of traffic received on the router.

Configuring an IP Receive ACL

This section describes the procedure for configuring the IP Receive ACL feature.

PREREQUISITES

Before you configure the IP Receive ACL feature, you must create a numbered ACL for IPv4 traffic or a named ACL for IPv6 traffic as follows:

- For IPv4 traffic:
 - To define a standard IP access list, enter the following command:
access-list access-list-number {deny | permit} source [source-wildcard] [log]
 - To define an extended IP access list, enter the following command:
**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]**

For information about the configuration procedure for IPv4 ACLs and command syntax, refer to the “[Filtering IP Packets Using Access Lists](#)” section in the “[Configuring IP Services](#)” chapter of the *Cisco IP Configuration Guide*, Release 12.3.

- For IPv6 traffic, enter the following commands:
**ipv6 access-list access-list-name
permit {protocol} {source-ipv6-prefix/prefix-length | any | host source-ipv6-address}
[operator [port-number]] {destination-ipv6-prefix/prefix-length | any | host
destination-ipv6-address} [operator [port-number]] [dscp value] [flow-label value]
[fragments] [log] [log-input] [reflect name [timeout value]] [routing] [time-range name]
[sequence value]**

Or

```
deny {protocol} {source-ipv6-prefix/prefix-length | any | host source-ipv6-address} [operator
[port-number]] {destination-ipv6-prefix/prefix-length | any | host destination-ipv6-address}
[operator [port-number]] [dscp value] [flow-label value] [fragments] [log] [log-input]
[routing] [time-range name] [undetermined-transport] [sequence value]
```

For information about the configuration procedure for IPv6 ACLs and command syntax, refer to the [Implementing Security for IPv6](#)

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip receive access-list** *number*

Or

```
ipv6 receive access-list name
```

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	ip receive access-list <i>number</i> Example: Router(config)# ip receive access-list 2 Or ipv6 receive access-list <i>name</i> Example: Router(config)# ipv6 receive access-list deny-telnet	Enables a a numbered ACL for IPv4 traffic or a named ACL for IPv6 traffic as the receive ACL that filters packets destined for the router.

Monitoring and Maintaining IP Receive ACL

To display information about the configured receive ACL, use the following **show** commands in privileged EXEC mode:

Command	Purpose
Router# show access-lists	Displays the contents of all IPv4 access lists, including counters for permit and deny statements.
Router# execute-on slot slot-number show controller events	Displays the number of packets denied on a specified line card by the receive ACL.
Router# show ip access-list	Displays the contents of one access list. Note The show ip access-list command provides output identical to the show access-lists command, except that it is IP-specific and allows you to specify a particular access list.
Router# show ipv6 access-list	Displays the contents of all current IPv6 access lists, including counters for permit and deny statements.

Configuration Examples for IP Receive ACL

This section contains the following configuration examples for IP Receive ACL:

- [Configuring a Receive ACL for IPv4 Traffic, page 6](#)
- [Configuring a Receive ACL for IPv6 Traffic, page 6](#)
- [Displaying the Number of Packets Denied on a Line Card by a Receive ACL, page 7](#)

Configuring a Receive ACL for IPv4 Traffic

The following example shows how to enable a receive ACL for IPv4 traffic that permits OSPF and BGP packets from one host, and allows 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
```

Configuring a Receive ACL for IPv6 Traffic

The following example shows how to enable a receive ACL for IPv6 traffic that blocks all attempts to establish a Telnet connection to the router while permitting all other IPv6 traffic:

```
ipv6 receive access-list deny-telnet
deny tcp any any eq telnet
permit ipv6 any any
```

Displaying the Number of Packets Denied on a Line Card by a Receive ACL

The following example shows how to display the number of packets denied on a specified line card by the receive ACL. The number of denied packets is displayed for the “Receive policy deny” counter:

```
execute-on slot 5 show controller events

===== Line Card (Slot 5) =====
Drop Counters
Packets punt to RP: 8
HW engine punt: 12889
HW engine reject: 8
Receive policy deny: 12889
Gen4 Packet Sanity Check (Warning): 8

RX HW Engine Reject Counters
MAC ID unrecognized: 8
```

Additional References

The following sections provide references related to the IP Receive ACL feature.

Related Documents

Related Topic	Document Title
General information about how to use and configure access control lists	“Access Control Lists: Overview and Guidelines” chapter in <i>Cisco IOS Security Configuration Guide</i> , Release 12.3 Configuring IP Access Lists
Information about how to use and configure an IPv4 ACL for traffic filtering	“Filtering IP Packets Using Access Lists” section in the “Configuring IP Services” chapter of the <i>Cisco IP Configuration Guide</i> , Release 12.3
Information about how to use and configure an IPv6 ACL for traffic filtering	Implementing Security for IPv6
Command syntax and usage guidelines for IPv4 ACL configuration commands	“IP Addressing and Services Commands” in the <i>Cisco IOS IP Command Reference, Volume 1 of 4: Addressing and Services</i> , Release 12.3
Command syntax and usage guidelines for IPv6 ACL configuration commands	Cisco IOS IPv6 Command Reference

Standards

Standards	Title
No new or modified standards are supported by this feature.	—

MIBs

MIBs	MIBs Link
<ul style="list-style-type: none"> No new or modified MIBs are supported by this feature. 	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
No new or modified RFCs are supported by this feature.	—

Technical Assistance

Description	Link
The Cisco Technical Support website, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access more content.	http://www.cisco.com/public/support/tac/home.shtml

Command Reference

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

- [ip receive access-list, page 9](#)
- [ipv6 receive access-list, page 10](#)

ip receive access-list

To activate a receive access control list (ACL) for IPv4 traffic, use the **ip receive access-list** command in global configuration mode. To deactivate the ACL and allow the router to receive all IPv4 traffic, use the **no** form of this command.

ip receive access-list *number*

no ip receive access-list *number*

Syntax Description

<i>number</i>	Number of IPv4 ACL.
Note	Named IPv4 ACLs are not supported as the receive ACL.

Defaults

Receive ACLs are not activated, and all IPv4 traffic is permitted.

Command Modes

Global configuration

Command History

Release	Modification
12.0(22)S	This command was introduced on the Cisco 12000 series.
12.0(24)S	This command was implemented on the Cisco 7500 series.
12.0(31)S	This command was implemented on the Cisco 10720 Internet router.

Usage Guidelines

Use the **ip receive access-list** command to configure a receive ACL that filters IPv4 packets sent to the router.

Examples

The following example shows how to permit Open Shortest Path First (OSPF) and Border Gateway Protocol (BGP) packets 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.

ipv6 receive access-list

To activate a receive access control list for IPv6 traffic, use the **ipv6 receive access-list** command in global configuration mode. To deactivate the ACL and allow the router to receive all IPv6 traffic, use the **no** form of this command.

ipv6 receive access-list *name*

no ipv6 receive access-list *name*

Syntax Description

<i>name</i>	Name of IPv6 ACL.
Note	Numbered IPv6 ACLs are not supported as the receive ACL.

Defaults

Receive ACLs are not activated, and all IPv6 traffic is permitted.

Command Modes

Global configuration

Command History

Release	Modification
12.0(32)S	This command was introduced on the Cisco 12000 series.

Usage Guidelines

Use the **ipv6 receive access-list** command to configure a receive ACL that filters IPv6 packets sent to the router.

Examples

The following example shows how to enable a receive ACL for IPv6 traffic that blocks all attempts to establish a Telnet connection to the router, while permitting all other IPv6 traffic:

```
ipv6 receive access-list deny-telnet
deny tcp any any eq telnet
permit ipv6 any any
```

Related Commands

Command	Description
ipv6 access-list	Defines an IPv6 access list.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership. Copyright © 2006 Cisco Systems, Inc. All rights reserved.