



Reflexive Access List Commands

This chapter describes reflexive access list commands, which are used to configure IP session filtering. IP session filtering provides the ability to filter IP packets based on upper-layer protocol “session” information.

Refer to the *Command Reference Master Index* or search online to find complete descriptions of other commands used when configuring reflexive access lists.

For reflexive access list configuration information, refer to the “Configuring IP Session Filtering (Reflexive Access Lists)” chapter in the *Security Configuration Guide*.

evaluate

To nest a reflexive access list within an access list, use the **evaluate** access-list configuration command. Use the **no** form of this command to remove a nested reflexive access list from the access list.

```
evaluate name  
no evaluate name
```

Syntax Description

name The name of the reflexive access list that you want evaluated for IP traffic entering your internal network. This is the name defined in the **permit (reflexive)** command.

Default

Reflexive access lists are not evaluated.

Command Mode

Access-list configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.3.

This command is used to achieve reflexive filtering, a form of session filtering.

Before this command will work, you must define the reflexive access list using the **permit (reflexive)** command.

This command nests a reflexive access list within an extended named IP access list.

If you are configuring reflexive access lists for an external interface, the extended named IP access list should be one which is applied to inbound traffic. If you are configuring reflexive access lists for an internal interface, the extended named IP access list should be one which is applied to outbound traffic. (In other words, use the access list opposite of the one used to define the reflexive access list.)

This command allows IP traffic entering your internal network to be evaluated against the reflexive access list. Use this command as an entry (condition statement) in the IP access list; the entry “points” to the reflexive access list to be evaluated.

As with all access list entries, the order of entries is important. Normally, when a packet is evaluated against entries in an access list, the entries are evaluated in sequential order, and when a match occurs, no more entries are evaluated. With a reflexive access list nested in an extended access list, the extended access list entries are evaluated sequentially up to the nested entry, then the reflexive access list entries are evaluated sequentially, and then the remaining entries in the extended access list are evaluated sequentially. As usual, after a packet matches *any* of these entries, no more entries will be evaluated.

Example

This example is for reflexive filtering at an external interface. This example defines an extended named IP access list *inboundfilters*, and applies it to inbound traffic at the interface. The access list definition permits all BGP and Enhanced IGRP traffic, denies all ICMP traffic, and causes all TCP traffic to be evaluated against the reflexive access list *tcptraffic*.

If the reflexive access list *tcptraffic* has an entry that matches an inbound packet, the packet will be permitted into the network. *tcptraffic* only has entries that permit inbound traffic for existing TCP sessions.

```
interface Serial 1
  description Access to the Internet via this interface
  ip access-group inboundfilters in
  !
ip access-list extended inboundfilters
  permit bgp any any
  permit eigrp any any
  deny icmp any any
  evaluate tcptraffic
```

Related Commands

- ip access-list (extended)
- ip reflexive-list timeout
- permit (reflexive)

ip reflexive-list timeout

To specify the length of time that reflexive access list entries will continue to exist when no packets in the session are detected, use the **ip reflexive-list timeout** global configuration command. Use the **no** form to reset the timeout period to the default timeout. This command applies only to reflexive access lists that do not already have a specified timeout.

- ip reflexive-list timeout *seconds*
- no ip reflexive-list timeout

Syntax Description

seconds Specifies the number of seconds to wait (when no session traffic is being detected) before temporary access list entries expire. Use a positive integer from 0 to $2^{32}-1$.

Default

The reflexive access list entry is removed after no packets in the session are detected for 300 seconds.

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.3.

This command is used with reflexive filtering, a form of session filtering.

This command specifies when a reflexive access list entry will be removed after a period of no traffic for the session (the timeout period).

With reflexive filtering, when an IP upper-layer session begins from within your network, a temporary entry is created within the reflexive access list, and a timer is set. Whenever a packet belonging to this session is forwarded (inbound or outbound) the timer is reset. When this timer counts down to zero without being reset, the temporary reflexive access list entry is removed.

The timer is set to the *timeout period*. Individual timeout periods can be defined for specific reflexive access lists, but for reflexive access lists that do not have individually defined timeout periods, the global timeout period is used. The global timeout value is 300 seconds by default; however, you can change the global timeout to a different value at any time using this command.

This command does not take effect for reflexive access list entries that were already created when the command is entered; this command only changes the timeout period for entries created after the command is entered.

Examples

This example sets the global timeout period for reflexive access list entries to 120 seconds.

```
ip reflexive-list timeout 120
```

This example returns the global timeout period to the default of 300 seconds.

```
no ip reflexive-list timeout
```

Related Commands

evaluate
ip access-list (extended)
permit (reflexive)

permit (reflexive)

To create a reflexive access list and to enable its temporary entries to be automatically generated, use the **permit (reflexive)** access-list configuration command. Use the **no** form of this command to delete the reflexive access list (if only one protocol was defined) or to delete protocol entries from the reflexive access list (if multiple protocols are defined).

```
permit protocol any any reflect name [timeout seconds]  
no permit protocol any any reflect name
```

Syntax Description

<i>protocol</i>	Name or number of an IP protocol. It can be one of the keywords gre , icmp , ip , ipinip , nos , tcp , or udp , or an integer in the range 0 to 255 representing an IP protocol number. To match any Internet protocol (including ICMP, TCP, and UDP), use the keyword ip .
<i>name</i>	Specifies the name of the reflexive access list. Names cannot contain a space or quotation mark, and must begin with an alphabetic character to prevent ambiguity with numbered access lists. The name can be up to 64 characters long.
<i>timeout seconds</i>	(Optional) Specifies the number of seconds to wait (when no session traffic is being detected) before entries expire in this reflexive access list. Use a positive integer from 0 to $2^{32}-1$. If not specified, the number of seconds defaults to the global timeout value.

Default

If this command is not configured, no reflexive access lists will exist, and no session filtering will occur. If this command is configured without specifying a **timeout** value, entries in this reflexive access list will expire after the global timeout period.

Command Mode

Access-list configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.3.

This command is used to achieve reflexive filtering, a form of session filtering.

For this command to work, you must also nest the reflexive access list using the **evaluate** command.

This command creates a reflexive access list and triggers the creation of entries in the same reflexive access list. This command must be an entry (condition statement) in an extended named IP access list.

If you are configuring reflexive access lists for an external interface, the extended named IP access list should be one which is applied to outbound traffic.

If you are configuring reflexive access lists for an internal interface, the extended named IP access list should be one which is applied to inbound traffic.

IP sessions that originate from within your network are initiated with a packet exiting your network. When such packet is evaluated against the statements in the extended named IP access list, the packet is also evaluated against this reflexive **permit** entry.

As with all access list entries, the order of entries is important, because they are evaluated in sequential order. When an IP packet reaches the interface, it will be evaluated sequentially by each entry in the access list until a match occurs.

If the packet matches an entry prior to the reflexive **permit** entry, the packet will not be evaluated by the reflexive **permit** entry, and no temporary entry will be created for the reflexive access list (session filtering will not be triggered).

The packet will be evaluated by the reflexive **permit** entry if no other match occurs first. Then, if the packet matches the protocol specified in the reflexive **permit** entry, the packet is forwarded and a corresponding temporary entry is created in the reflexive access list (unless the corresponding entry already exists, indicating the packet belongs to a session in progress). The temporary entry specifies criteria that permits traffic into your network only for the same session.

Characteristics of Reflexive Access List Entries

This command enables the creation of temporary entries in the same reflexive access list that was defined by this command. The temporary entries are created when a packet exiting your network matches the protocol specified in this command. (The packet “triggers” the creation of a temporary entry.) These entries have the following characteristics:

- The entry is a **permit** entry.
- The entry specifies the same IP upper-layer protocol as the original triggering packet.
- The entry specifies the same source and destination addresses as the original triggering packet, except the addresses are swapped.
- If the original triggering packet is TCP or UDP, the entry specifies the same source and destination port numbers as the original packet, except the port numbers are swapped.

If the original triggering packet is a protocol other than TCP or UDP, port numbers do not apply, and other criteria are specified. For example, for ICMP, type numbers are used: the temporary entry specifies the same type number as the original packet (with only one exception: if the original ICMP packet is type 8, the returning ICMP packet must be type 0 to be matched).

- The entry inherits all the values of the original triggering packet, with exceptions only as noted in the previous four bullets.
- IP traffic entering your internal network will be evaluated against the entry, until the entry expires. If an IP packet matches the entry, the packet will be forwarded into your network.
- The entry will expire (be removed) after the last packet of the session is matched.
- If no packets belonging to the session are detected for a configurable length of time (the timeout period), the entry will expire.

Example

This example defines a reflexive access list *tcptraffic*, in an outbound access list that permits all BGP and Enhanced IGRP traffic and denies all ICMP traffic. This example is for an external interface (an interface connecting to an external network).

First, the interface is defined and the access list is applied to the interface for outbound traffic.

```
interface Serial 1
  description Access to the Internet via this interface
  ip access-group outboundfilters out
```

Next, the outbound access list is defined and the reflexive access list *tcptraffic* is created with a reflexive **permit** entry.

```
ip access-list extended outboundfilters
 permit tcp any any reflect tcptraffic
```

Related Commands

- evaluate
- ip access-list (extended)
- ip reflexive-list timeout