CHAPTER 12

Configuring Traffic Filtering

The Cisco 10000 series router provides traffic filtering capabilities using access control lists (ACLs). Access lists filter network traffic by controlling whether routed packets are forwarded or blocked at the router's interfaces. Using ACLs, you can do such things as restrict the contents of routing updates, provide traffic flow control, and provide security for your network.

The Cisco 10000 series router supports the following ACL types and features:

- Standard and extended ACLs
- Named and numbered ACLs
- Turbo-ACLs
- Per-user ACLs
- IP receive ACLs
- Time-based ACLs

For more information about ACLs, see the following documents:

- *Turbo Access Control Lists, Release 12.1(5)T* feature module
- Part 3: Traffic Filtering and Firewalls in the *Cisco IOS Security Configuration Guide, Release 12.2*

This chapter describes the following features:

- IP Receive ACLs, page 12-1
- Time-Based ACLs, page 12-4

IP Receive ACLs

The IP Receive ACLs feature provides basic filtering capability for traffic that is destined for the router and protects the router from remote intrusions.

To restrict access to the router, you apply a numbered ACL to the ingress interface of the router. You can restrict access to the router to known and trusted sources, and to expected traffic profiles. The IP Receive ACLs feature supports both standard and extended ACLs. The rules for numbered ACLs also apply to the access control entries (ACEs) of the IP receive ACL.

The IP receive ACL filters traffic on the parallel express forwarding engine (PXF) before filtering the packets received by the route processor (RP). This feature protects the router from denial of service (DoS) floods, thereby preventing the flood from degrading the performance of the route processor (RP).

The IP Receive ACLs feature is described in the following topics:

- Feature History for IP Receive ACLs, page 12-2
- Restrictions for IP Receive ACLs, page 12-2
- Configuration Tasks for IP Receive ACLs, page 12-2
- Configuration Example for IP Receive ACLs, page 12-3

Feature History for IP Receive ACLs

Cisco IOS Release	Description	Required PRE
12.3(7)XI1	This feature was introduced on the Cisco 10000 series router.	PRE2

Restrictions for IP Receive ACLs

The IP receive ACLs feature has the following restrictions:

- A receive ACL must be a numbered ACL. You cannot use a named ACL as the receive ACL.
- The rules for numbered ACLs also apply to the access control entries (ACEs) of receive ACLs.
- Time-based and reflexive ACLs are not supported as receive ACLs.
- Only traffic processed by the RP is filtered. Traffic that is processed exclusively by the Forwarding Processor (FP) is not filtered. For example, GRE tunneled packets, L2TP tunneled packets, and some ICMP packets are not filtered.

Configuration Tasks for IP Receive ACLs

To configure the IP Receive ACLs feature, perform the following configuration tasks:

- Configuring Receive ACLs, page 12-3
- Verifying Receive ACLs, page 12-3

Configuring Receive ACLs

To configure receive ACLs, enter the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# ip receive acl 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.
		
		Defines an extended IP access list.
		
		Note The **timeout** argument and the **time-range** argument are not supported on Cisco IOS Release 12.3(7)XI1.

Verifying Receive ACLs

To verify the configuration of receive ACLs, enter any of the following commands in privileged EXEC mode:

Command	Purpose
`Router# show access-lists`	Displays the contents of all current standard and extended access lists. (Default)
`Router# show access-lists [access-list-number | access-list-name]`	Displays the contents of the access list you specify.
`Router# show ip access-list`	Displays the contents of all current standard and extended IP access lists. (Default)
`Router# show ip access-list [access-list-number | access-list-name]`	Displays the contents of the IP access list you specify.

Configuration Example for IP Receive ACLs

Example 12-1 shows how to configure an extended IP receive ACL. The ACEs of this numbered ACL (100) do the following:

- Deny fragmented ping operations
- Permit the router to respond to ping operations
- Permit FTP operations from network 192.168.1.0
- Permit OSPF routing updates
- Permit BGP routing updates from the host 10.0.0.1
- Deny any other IP traffic

Example 12-1 Receive ACL Configuration

```
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
```

Time-Based ACLs

The Time-based ACLs feature allows the network administrator to define a time range when certain resources may be accessed, thus providing greater control over resource usage.

While functionally similar to extended ACLs, time-based ACLs control access to the router for a specific time period. A time range, identified by a name, defines the specific times of the day and week that the ACL is active. The access control entries (ACEs) reference the time range name, which imposes the time restriction on the ACEs. The time range relies on router's system clock to activate or deactivate an ACE.

Previously, access list statements were always in effect after they were applied to an interface. However, using the time-range command, network administrators can now define when the permit and deny statements in the ACL are in effect. Both named and numbered access lists can reference a time range.

When you create a time range, you can specify both absolute and periodic time entries. The **periodic** command in time-range configuration mode allows you to specify the days of the week and the time of day that the access control entry (ACE) is active. The **absolute** command in time-range configuration mode allows you to specify a specific time and date to activate the ACE and a specific time and date to stop processing the ACE. You can specify only one absolute entry for each time range. During ACL processing, the router begins evaluating the time range entry attached to the ACE after it reaches the absolute start time. The router then evaluates the periodic values until the router reaches the absolute end entry. No further processing occurs after the router reaches the absolute end value.

The Tine-based ACLs feature is described in the following topics:

- Feature History for Time-Based ACLs, page 12-4
- Restrictions for Time-Based ACLs, page 12-5
- Configuration Tasks for Time-Based ACLs, page 12-5
- Monitoring and Maintaining Time-Based ACLs, page 12-8
- Configuration Examples for Time-Based ACLs, page 12-8

Feature History for Time-Based ACLs

Cisco IOS Release	Description	Required PRE
12.3(7)XI1	This feature was introduced on the Cisco 10000 series router.	PRE2
12.2(28)SB	This feature was integrated into Cisco IOS Release 12.2(28)SB.	PRE2

Restrictions for Time-Based ACLs

The Time-Based ACLs feature has the following restrictions:

- You can specify a time range for only IP extended access lists. Standard access lists are not supported.
- An ACE that refers to a non-existent time-range entry is considered active.
- You define time-based ACLs based on hours and minutes. You cannot specify seconds.

Configuration Tasks for Time-Based ACLs

To configure the Time-Based ACLs feature, perform the following configuration tasks:

- Creating a Time Range, page 12-5
- Applying a Time Range to a Numbered Access Control List, page 12-6
- Applying a Time Range to a Named Access Control List, page 12-7

Creating a Time Range

To create a time range, enter the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# time-range name`	Defines a named time range and enters time-range configuration mode.
Step 2	`Router(config-time-range)# periodic days-of-the-week hh:mm to [days-of-the-week] hh:mm`	(Optional) Defines the periodic times that the time range is active. Valid values for *days-of-the-week* are **Monday**, **Tuesday**, **Wednesday**, **Thursday**, **Friday**, **Saturday**, and **Sunday**. You can also specify **daily** for Monday through Sunday, **weekdays** for Monday through Friday, and **weekend** for Saturday and Sunday. The *hh:mm* argument specifies hours:minutes in a 24 hour format. For example, 8:00 is 8:00 a.m. and 20:00 is 8:00 p.m. The ending *days-of-the-week* argument defaults to the value you specify in the beginning *days-of-the-week* argument. Specify the ending *days-of-the-week* only if it is different from the beginning *days-of-the-week*.
Step 3	`Router(config-time-range)# absolute [start time date] [end time date]`	(Optional) Defines the absolute times that the time range is active. You specify the **start** and **end** arguments in the format of *hh:mm day month year*, using a 24 hour format. The minimum **start** value is **00:00 1 January 1993**. If you do not specify a start value, it defaults to **right now.** The maximum **end** value is **23:59 31 December 2035**. The **end** value must be greater than the **start** value; otherwise, an error occurs. If you do not specify an **end** value, it defaults to **forever after the starting time**. **Note** You can specify only one absolute entry for each time range you create.

Example 12-2 creates a periodic time range named *no-http* that specifies Monday through Friday from 8:00 a.m. to 6:00 p.m.

Example 12-2 Configuring a Time Range

```
Router(config)# time-range no-http
Router(config-time-range)# periodic weekdays 8:00 to 18:00
```

Example 12-3 creates a time range named *HTTP* that specifies both periodic and absolute values. During ACL processing, the router assumes that the time period begins right now because the **absolute** command does not specify a **start** value. The router then evaluates the **periodic** value, which indicates that the time period is restricted to Monday through Wednesday from 8:00 a.m. to 7:00 p.m. The time period ends on February 6 at 11:59 p.m.

Example 12-3 Configuring a Time Range with Periodic and Absolute Entries

```
Router(config)# time-range http
Router(config-t-range)# periodic monday 8:00 to wednesday 19:00
Router(config-t-range)# absolute end 23:59 6 February 2000
```

Applying a Time Range to a Numbered Access Control List

To apply a time range to the access control entries (ACEs) of a numbered extended access control list (ACL), enter the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`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* [**fragments**]	Defines a numbered extended IP access control list (ACL). The **time-range** *time-range-name* argument specifies the name of the time range to apply to the ACE. **Note** In Cisco IOS Release 12.3(7)XI1, the **time-range** argument is required. For more information about the access-list command, see the *Cisco IOS IP Command Reference, Volume 1 of 4: Addressing and Services, Release 12.3*.
Step 2	`Router(config)# interface` *type number slot/module/port.subinterface*	Configures an interface and enters interface configuration mode.
Step 3	`Router(config-if)# ip access-group` {*access-list-number* | *access-list-name*} {**in** | **out**}	Controls access to an interface.

Example 12-4 permits SMTP traffic to the access the mail host (128.88.1.2) on Monday through Sunday between the hours of 5:00 a.m. and 11:59 p.m, if the traffic belongs to an already established connection. The example creates the time range named *smtp* and applies it to the ACE of the extended access list numbered 102. The time-based ACL is then applied to the ingress serial 0 interface.

Example 12-4 Applying a Time Range to a Numbered ACL

```
Router(config)# time-range smtp
Router(config-time-range)# periodic daily 5:00 to 23:59
Router(config)# access-list 102 permit tcp 0.0.0.0 255.255.255.255 128.88.0.0 0.0.255.255
established
Router(config)# access-list 102 permit tcp 0.0.0.0 255.255.255.255 128.88.1.2 0.0.0.0 eq
25 time-range smtp
Router(config)# interface serial 0
Router(config-if)# ip access-group 102 in
```

Applying a Time Range to a Named Access Control List

To apply a time range to a named extended access control list (ACL), enter the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# ip access-list {standard | extended} access-list-name`	Defines an access list by name and enters named-access-control configuration mode. **Note** The time-based ACLs feature supports only extended access lists.
Step 2	`Router(config-ext-nacl)# {deny | permit} protocol source source-wildcard destination destination-wildcard [icmp-type [icmp-code] | icmp-message] [precedence precedence] [tos tos] [log] time-range time-range-name [fragments]`	Sets conditions in a named IP access list that will deny or permit packets. The **time-range** *time-range-name* option indicates the name of the time range that applies to this ACE. **Note** In Cisco IOS Release 12.3(7)XI1, the **time-range** argument is required.
Step 3	`Router(config)# interface type number slot/module/port.subinterface`	Configures an interface and enters interface configuration mode.
Step 4	`Router(config-if)# ip access-group {access-list-number | access-list-name} {in | out}`	Controls access to an interface.

Example 12-5 denies FTP traffic on Monday through Sunday between the hours of 9:00 a.m. and 3:00 p.m. The example creates the time range named *no-ftp* and applies it to the ACE of the extended IP access list named I. The time-based ACL is then applied to the ingress Ethernet 0 interface.

Example 12-5 Applying a Time Range to a Named ACL

```
Router(config)# time-range no-ftp
Router(config-time-range)# periodic daily 9:00 to 15:00
Router(config)# ip access-list extended strict
Router(config-ext-nacl)# deny tcp any any eq 21 time-range no-ftp
Router(config-ext-nacl)# exit
Router(config)# interface ethernet 0
Router(config-if)# ip access-group strict in
```

Monitoring and Maintaining Time-Based ACLs

To monitor and maintain time-based ACLs, enter any of the following commands in privileged EXEC mode:

Command	Purpose
Router# **show access-lists** [*access-list-number* | *access-list-name*]	Displays the contents of current access lists or the access list you specify.
Router# **show interface** *type number*	Displays information about the interface you specify and indicates if an access list is configured on the interface.
Router# **show time-range**	Displays the configured time ranges.

Configuration Examples for Time-Based ACLs

The following example permits Telnet connections from the 10.1.1.0 network to the 172.16.1.0 network on Monday, Wednesday, and Friday during the business hours.

```
time-range EVERYOTHERDAY
 periodic Monday Wednesday Friday 8:00 to 17:00
!
access-list 101 permit tcp 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255 eq telnet time-range
EVERYOTHERDAY
!
interface Ethernet0/0
 ip address 10.1.1.1 255.255.255.0
 ip access-group 101 in
```

The following example permits SMTP traffic from all networks to indefinitely access all networks beginning at 12:00 p.m. on January 1, 2001.

```
time-range forever
 absolute start 12:00 1 January 2001
!
ip access-list extended allusers
 permit tcp any any eq 25 time-range forever
```

The following example permits UDP traffic until noon on December 31, 2000. The ACL entry will no longer allow UDP traffic after that date and time.

```
time-range stop-udp
 absolute end 12:00 31 December 2000
!
ip access-list extended usa
 permit udp any any time-range stop-udp
```

The following configuration example permits telnet traffic on Monday, Tuesday, and Friday from 9:00 a.m. and 5:00 p.m.:

```
time-range telnet
  periodic Monday Tuesday Friday 9:00 to 17:00
!
ip access-list extended camden
  permit tcp any any eq telnet time-range telnet
```

The following configuration example permits UDP traffic on Saturday and Sunday from 8:00 a.m. on January 1, 1999 to 6:00 p.m. on December 31, 2001:

```
time-range udp
  absolute start 8:00 1 January 1999 end 18:00 31 December 2001
  periodic weekends 00:00 to 23:59
!
ip access-list extended boothbay
  permit udp any any time-range udp
```