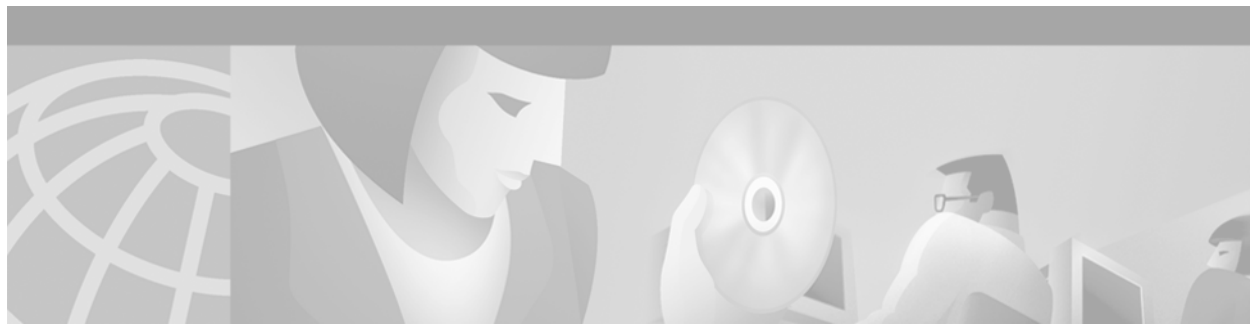




TCP Intercept Commands

This chapter describes TCP Intercept commands. TCP Intercept is a traffic filtering security feature that protects TCP servers from TCP SYN-flooding attacks, which are a type of denial-of-service attack. TCP Intercept is available for IP traffic only.

To find complete descriptions of other commands used when configuring TCP Intercept, refer to the *Cisco IOS Command Reference Master Index* or search online.

For TCP Intercept configuration information, refer to the chapter “Configuring TCP Intercept (Preventing Denial-of-Service Attacks)” in the *Cisco IOS Security Configuration Guide*.

ip tcp intercept connection-timeout

To change how long a TCP connection will be managed by the TCP intercept after no activity, use the **ip tcp intercept connection-timeout** global configuration command. To restore the default, use the **no** form of this command.

ip tcp intercept connection-timeout *seconds*

no ip tcp intercept connection-timeout [*seconds*]

Syntax Description

<i>seconds</i>	Time (in seconds) that the software will still manage the connection after no activity. The minimum value is 1 second. The default is 86,400 seconds (24 hours).
----------------	--

Defaults

86,400 seconds (24 hours)

Command Modes

Global configuration

Command History

Release	Modification
11.2 F	This command was introduced.

Usage Guidelines

Use the **ip tcp intercept connection-timeout** command to change how long a TCP connection will be managed by the TCP intercept after a period of inactivity.

Examples

The following example sets the software to manage the connection for 12 hours (43,200 seconds) after no activity:

```
ip tcp intercept connection-timeout 43200
```

ip tcp intercept drop-mode

To set the TCP intercept drop mode, use the **ip tcp intercept drop-mode** global configuration command. To restore the default, use the **no** form of this command.

ip tcp intercept drop-mode [**oldest** | **random**]

no ip tcp intercept drop-mode [**oldest** | **random**]

Syntax Description	oldest	(Optional) Software drops the oldest partial connection. This is the default.
	random	(Optional) Software drops a randomly selected partial connection.

Defaults	oldest
----------	--------

Command Modes	Global configuration
---------------	----------------------

Command History	Release	Modification
	11.2 F	This command was introduced.

Usage Guidelines	If the number of incomplete connections exceeds 1100 or the number of connections arriving in the last 1 minute exceeds 1100, the TCP intercept feature becomes more aggressive. When this happens, each new arriving connection causes the oldest partial connection to be deleted, and the initial retransmission timeout is reduced by half to 0.5 seconds (and so the total time trying to establish the connection will be cut in half).
------------------	---

Note that the 1100 thresholds can be configured with the **ip tcp intercept max-incomplete high** and **ip tcp intercept one-minute high** commands.

Use the **ip tcp intercept drop-mode** command to change the dropping strategy from oldest to a random drop.

Examples	The following example sets the drop mode to random:
----------	---

```
ip tcp intercept drop-mode random
```

Related Commands	Command	Description
	ip tcp intercept max-incomplete high	Defines the maximum number of incomplete connections allowed before the software enters aggressive mode.
	ip tcp intercept max-incomplete low	Defines the number of incomplete connections below which the software leaves aggressive mode.

Command	Description
ip tcp intercept one-minute high	Defines the number of connection requests received in the last one-minutes sample period before the software enters aggressive mode.
ip tcp intercept one-minute low	Defines the number of connection requests below which the software leaves aggressive mode.

ip tcp intercept finrst-timeout

To change how long after receipt of a reset or FIN-exchange the software ceases to manage the connection, use the **ip tcp intercept finrst-timeout** global configuration command. To restore the default, use the **no** form of this command.

ip tcp intercept finrst-timeout *seconds*

no ip tcp intercept finrst-timeout [*seconds*]

Syntax Description	<i>seconds</i>	Time (in seconds) after receiving a reset or FIN-exchange that the software ceases to manage the connection. The minimum value is 1 second. The default is 5 seconds.				
Defaults	5 seconds					
Command Modes	Global configuration					
Command History	<table><tr><th>Release</th><th>Modification</th></tr><tr><td>11.2 F</td><td>This command was introduced.</td></tr></table>	Release	Modification	11.2 F	This command was introduced.	
Release	Modification					
11.2 F	This command was introduced.					
Usage Guidelines	Even after the two ends of the connection are joined, the software intercepts packets being sent back and forth. Use this command if you need to adjust how soon after receiving a reset or FIN-exchange the software stops intercepting packets.					
Examples	The following example sets the software to wait for 10 seconds before it leaves intercept mode: <pre>ip tcp intercept finrst-timeout 10</pre>					

ip tcp intercept list

To enable TCP intercept, use the **ip tcp intercept list** global configuration command. To disable TCP intercept, use the **no** form of this command.

ip tcp intercept list *access-list-number*

no ip tcp intercept list *access-list-number*

Syntax Description

access-list-number Extended access list number in the range from 100 to 199.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
11.2 F	This command was introduced.

Usage Guidelines

The TCP intercept feature intercepts TCP connection attempts and shields servers from TCP SYN-flood attacks, also known as denial-of-service attacks.

TCP packets matching the access list are presented to the TCP intercept code for processing, as determined by the **ip tcp intercept mode** command. The TCP intercept code either intercepts or watches the connections.

To have all TCP connection attempts submitted to the TCP intercept code, have the access list match everything.

Examples

The following example configuration defines access list 101, causing the software to intercept packets for all TCP servers on the 192.168.1.0/24 subnet:

```
ip tcp intercept list 101
!
access-list 101 permit tcp any 192.168.1.0 0.0.0.255
```

Related Commands

Command	Description
access-list (IP extended)	Defines an extended IP access list.
ip tcp intercept mode	Changes the TCP intercept mode.
show tcp intercept connections	Displays TCP incomplete and established connections.
show tcp intercept statistics	Displays TCP intercept statistics.

ip tcp intercept max-incomplete high

To define the maximum number of incomplete connections allowed before the software enters aggressive mode, use the **ip tcp intercept max-incomplete high** global configuration command. To restore the default, use the **no** form of this command.

ip tcp intercept max-incomplete high *number*

no ip tcp intercept max-incomplete high [*number*]

Syntax Description

<i>number</i>	Defines the number of incomplete connections allowed, above which the software enters aggressive mode. The range is from 1 to 2147483647. The default is 1100.
---------------	--

Defaults

1100 incomplete connections

Command Modes

Global configuration

Command History

Release	Modification
11.2 F	This command was introduced.

Usage Guidelines

If the number of incomplete connections exceeds the *number* configured, the TCP intercept feature becomes aggressive. The following are the characteristics of aggressive mode:

- Each new arriving connection causes the oldest partial connection to be deleted.
- The initial retransmission timeout is reduced by half to 0.5 seconds (and so the total time trying to establish the connection is cut in half).
- The watch-timeout is cut in half (from 30 seconds to 15 seconds).

You can change the drop strategy from the oldest connection to a random connection with the **ip tcp intercept drop-mode** command.



Note

The two factors that determine aggressive mode (connection requests and incomplete connections) are related and work together. When the value of *either* **ip tcp intercept one-minute high** or **ip tcp intercept max-incomplete high** is exceeded, aggressive mode begins. When *both* connection requests and incomplete connections fall below the values of **ip tcp intercept one-minute low** and **ip tcp intercept max-incomplete low**, aggressive mode ends.

The software will back off from its aggressive mode when the number of incomplete connections falls below the number specified by the **ip tcp intercept max-incomplete low** command.

ip tcp intercept max-incomplete high**Examples**

The following example allows 1500 incomplete connections before the software enters aggressive mode:

```
ip tcp intercept max-incomplete high 1500
```

Related Commands

Command	Description
ip tcp intercept drop-mode	Sets the TCP intercept drop mode.
ip tcp intercept max-incomplete low	Defines the number of incomplete connections below which the software leaves aggressive mode.
ip tcp intercept one-minute high	Defines the number of connection requests received in the last one-minute sample period before the software enters aggressive mode.
ip tcp intercept one-minute low	Defines the number of connection requests below which the software leaves aggressive mode.

ip tcp intercept max-incomplete low

To define the number of incomplete connections below which the software leaves aggressive mode, use the **ip tcp intercept max-incomplete low** global configuration command. To restore the default, use the **no** form of this command.

ip tcp intercept max-incomplete low *number*

no ip tcp intercept max-incomplete low [*number*]

Syntax Description

<i>number</i>	Defines the number of incomplete connections below which the software leaves aggressive mode. The range is 1 to 2147483647. The default is 900.
---------------	---

Defaults

900 incomplete connections

Command Modes

Global configuration

Command History

Release	Modification
11.2 F	This command was introduced.

Usage Guidelines

When *both* connection requests and incomplete connections fall below the values of **ip tcp intercept one-minute low** and **ip tcp intercept max-incomplete low**, the TCP intercept feature leaves aggressive mode.



Note

The two factors that determine aggressive mode (connection requests and incomplete connections) are related and work together. When the value of *either* **ip tcp intercept one-minute high** or **ip tcp intercept max-incomplete high** is exceeded, aggressive mode begins. When *both* connection requests and incomplete connections fall below the values of **ip tcp intercept one-minute low** and **ip tcp intercept max-incomplete low**, aggressive mode ends.

See the **ip tcp intercept max-incomplete high** command for a description of aggressive mode.

Examples

The following example sets the software to leave aggressive mode when the number of incomplete connections falls below 1000:

```
ip tcp intercept max-incomplete low 1000
```

Related Commands

Command	Description
ip tcp intercept drop-mode	Sets the TCP intercept drop mode.
ip tcp intercept max-incomplete high	Defines the maximum number of incomplete connections allowed before the software enters aggressive mode.
ip tcp intercept one-minute high	Defines the number of connection requests received in the last one-minutes sample period before the software enters aggressive mode.
ip tcp intercept one-minute low	Defines the number of connection requests below which the software leaves aggressive mode.

ip tcp intercept mode

To change the TCP intercept mode, use the **ip tcp intercept mode** global configuration command. To restore the default, use the **no** form of this command.

ip tcp intercept mode {intercept | watch}

no ip tcp intercept mode [intercept | watch]

Syntax Description	intercept	Active mode in which the TCP intercept software intercepts TCP packets from clients to servers that match the configured access list and performs intercept duties. This is the default.
	watch	Monitoring mode in which the software allows connection attempts to pass through the router and watches them until they are established.

Defaults	intercept
----------	------------------

Command Modes	Global configuration
---------------	----------------------

Command History	Release	Modification
	11.2 F	This command was introduced.

Usage Guidelines

When TCP intercept is enabled, it operates in intercept mode by default. In intercept mode, the software actively intercepts TCP SYN packets from clients to servers that match the specified access list. For each SYN, the software responds on behalf of the server with an ACK and SYN, and waits for an ACK of the SYN from the client. When that ACK is received, the original SYN is sent to the server, and the code then performs a three-way handshake with the server. Then the two half-connections are joined.

In watch mode, the software allows connection attempts to pass through the router, but watches them until they become established. If they fail to become established in 30 seconds (or the value set by the **ip tcp intercept watch-timeout** command), a Reset is sent to the server to clear its state.

Examples

The following example sets the mode to watch mode:

```
ip tcp intercept mode watch
```

Related Commands	Command	Description
	ip tcp intercept watch-timeout	Defines how long the software will wait for a watched TCP intercept connection to reach established state before sending a reset to the server.

ip tcp intercept one-minute high

To define the number of connection requests received in the last one-minutes sample period before the software enters aggressive mode, use the **ip tcp intercept one-minute high** global configuration command. To restore the default, use the **no** form of this command.

ip tcp intercept one-minute high *number*

no ip tcp intercept one-minute high [*number*]

Syntax Description

<i>number</i>	Specifies the number of connection requests that can be received in the last one-minute sample period before the software enters aggressive mode. The range is 1 to 2147483647. The default is 1100.
---------------	--

Defaults

1100 connection requests

Command Modes

Global configuration

Command History

Release	Modification
11.2 F	This command was introduced.

Usage Guidelines

If the number of connection requests exceeds the *number* value configured, the TCP intercept feature becomes aggressive. The following are the characteristics of aggressive mode:

- Each new arriving connection causes the oldest partial connection to be deleted.
- The initial retransmission timeout is reduced by half to 0.5 seconds (and so the total time trying to establish the connection is cut in half).
- The watch-timeout is cut in half (from 30 seconds to 15 seconds).

You can change the drop strategy from the oldest connection to a random connection with the **ip tcp intercept drop-mode** command.



Note

The two factors that determine aggressive mode (connection requests and incomplete connections) are related and work together. When the value of *either* **ip tcp intercept one-minute high** or **ip tcp intercept max-incomplete high** is exceeded, aggressive mode begins. When *both* connection requests and incomplete connections fall below the values of **ip tcp intercept one-minute low** and **ip tcp intercept max-incomplete low**, aggressive mode ends.

Examples

The following example allows 1400 connection requests before the software enters aggressive mode:

```
ip tcp intercept one-minute high 1400
```

Related Commands	Command	Description
	ip tcp intercept drop-mode	Sets the TCP intercept drop mode.
	ip tcp intercept max-incomplete high	Defines the maximum number of incomplete connections allowed before the software enters aggressive mode.
	ip tcp intercept max-incomplete low	Defines the number of incomplete connections below which the software leaves aggressive mode.
	ip tcp intercept one-minute low	Defines the number of connection requests below which the software leaves aggressive mode.

ip tcp intercept one-minute low

To define the number of connection requests below which the software leaves aggressive mode, use the **ip tcp intercept one-minute low** global configuration command. To restore the default, use the **no** form of this command.

ip tcp intercept one-minute low *number*

no ip tcp intercept one-minute low [*number*]

Syntax Description

<i>number</i>	Defines the number of connection requests in the last one-minute sample period below which the software leaves aggressive mode. The range is from 1 to 2147483647. The default is 900.
---------------	--

Defaults

900 connection requests

Command Modes

Global configuration

Command History

Release	Modification
11.2 F	This command was introduced.

Usage Guidelines

When *both* connection requests and incomplete connections fall below the values of **ip tcp intercept one-minute low** and **ip tcp intercept max-incomplete low**, the TCP intercept feature leaves aggressive mode.



Note

The two factors that determine aggressive mode (connection requests and incomplete connections) are related and work together. When the value of *either* **ip tcp intercept one-minute high** or **ip tcp intercept max-incomplete high** is exceeded, aggressive mode begins. When *both* connection requests and incomplete connections fall below the values of **ip tcp intercept one-minute low** and **ip tcp intercept max-incomplete low**, aggressive mode ends.

See the **ip tcp intercept one-minute high** command for a description of aggressive mode.

Examples

The following example sets the software to leave aggressive mode when the number of connection requests falls below 1000:

```
ip tcp intercept one-minute low 1000
```

Related Commands	Command	Description
	ip tcp intercept drop-mode	Sets the TCP intercept drop mode.
	ip tcp intercept max-incomplete high	Defines the maximum number of incomplete connections allowed before the software enters aggressive mode.
	ip tcp intercept max-incomplete low	Defines the number of incomplete connections below which the software leaves aggressive mode.
	ip tcp intercept one-minute high	Defines the number of connection requests received in the last one-minutes sample period before the software enters aggressive mode.

ip tcp intercept watch-timeout

To define how long the software will wait for a watched TCP intercept connection to reach established state before sending a reset to the server, use the **ip tcp intercept watch-timeout** global configuration command. To restore the default, use the **no** form of this command.

ip tcp intercept watch-timeout *seconds*

no ip tcp intercept watch-timeout [*seconds*]

Syntax Description	<i>seconds</i> Time (in seconds) that the software waits for a watched connection to reach established state before sending a Reset to the server. The minimum value is 1 second. The default is 30 seconds.	
Defaults	30 seconds	
Command Modes	Global configuration	
Command History	Release	Modification
	11.2 F	This command was introduced.
Usage Guidelines	Use this command if you have set the TCP intercept to passive watch mode and you want to change the default time the connection is watched. During aggressive mode, the watch timeout time is cut in half.	
Examples	The following example sets the software to wait 60 seconds for a watched connection to reach established state before sending a Reset to the server: ip tcp intercept watch-timeout 60	
Related Commands	Command	Description
	ip tcp intercept mode	Changes the TCP intercept mode.

show tcp intercept connections

To display TCP incomplete and established connections, use the **show tcp intercept connections** EXEC command.

show tcp intercept connections

Syntax Description This command has no arguments or keywords.

Command Modes EXEC

Command History	Release	Modification
	11.2 F	This command was introduced.

Usage Guidelines Use the **show tcp intercept connections** command to display TCP incomplete and established connections.

Examples The following is sample output from the **show tcp intercept connections** command:

```
Router# show tcp intercept connections
```

```
Incomplete:
Client          Server          State    Create    Timeout  Mode
172.19.160.17:58190 10.1.1.30:23  SYNRCVD  00:00:09  00:00:05 I
172.19.160.17:57934 10.1.1.30:23  SYNRCVD  00:00:09  00:00:05 I

Established:
Client          Server          State    Create    Timeout  Mode
171.69.232.23:1045 10.1.1.30:23   ESTAB    00:00:08  23:59:54 I
```

Table 19 describes significant fields shown in the display.

Table 19 show tcp intercept connections Field Descriptions

Field	Description
Incomplete:	Rows of information under “Incomplete” indicate connections that are not yet established.
Client	IP address and port of the client.
Server	IP address and port of the server being protected by TCP intercept.
State	SYNRCVD—establishing with client. SYNSENT—establishing with server. ESTAB—established with both, passing data.
Create	Hours:minutes:seconds since the connection was created.
Timeout	Hours:minutes:seconds until the retransmission timeout.

Table 19 *show tcp intercept connections Field Descriptions (continued)*

Field	Description
Mode	I—intercept mode. W—watch mode.
Established:	Rows of information under “Established” indicate connections that are established. The fields are the same as those under “Incomplete” except for the Timeout field described below.
Timeout	Hours:minutes:seconds until the connection will timeout, unless the software sees a FIN exchange, in which case this indicates the hours:minutes:seconds until the FIN or RESET timeout.

Related Commands

Command	Description
ip tcp intercept connection-timeout	Changes how long a TCP connection will be managed by the TCP intercept after no activity.
ip tcp intercept finrst-timeout	Changes how long after receipt of a reset or FIN-exchange the software ceases to manage the connection.
ip tcp intercept list	Enables TCP intercept.
show tcp intercept statistics	Displays TCP intercept statistics.

show tcp intercept statistics

To display TCP intercept statistics, use the **show tcp intercept statistics** EXEC command.

show tcp intercept statistics

Syntax Description This command has no arguments or keywords.

Command Modes EXEC

Command History	Release	Modification
	11.2 F	This command was introduced.

Usage Guidelines Use the **show tcp intercept statistics** command to display TCP intercept statistics.

Examples The following is sample output from the **show tcp intercept statistics** command:

```
Router# show tcp intercept statistics

intercepting new connections using access-list 101
2 incomplete, 1 established connections (total 3)
1 minute connection request rate 2 requests/sec
```

Related Commands	Command	Description
	ip tcp intercept connection-timeout	Changes how long a TCP connection will be managed by the TCP intercept after no activity.
	ip tcp intercept finrst-timeout	Changes how long after receipt of a reset or FIN-exchange the software ceases to manage the connection.
	ip tcp intercept list	Enables TCP intercept.
	show tcp intercept connections	Displays TCP incomplete and established connections.

■ show tcp intercept statistics