TCP Intercept Commands

This chapter describes the function and displays the syntax for TCP Intercept commands. For more information about defaults and usage guidelines, see the corresponding chapter of the *Security Command Reference*.

ip tcp intercept connection-timeout

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

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

seconds	Time (in seconds) that the software will still manage the connection after no activity. The minimum value is 1 second. The default is 86400 seconds (24 hours).

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 value, use the **no** form of this command.

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

oldest	Software drops the oldest partial connection. This is the default.
random	Software drops a randomly selected partial connection.

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 value, use the **no** form of this command.

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

seconds	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.

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*

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

ip tcp intercept max-incomplete high

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

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

number	Defines the number of incomplete connections allowed, above which the software behaves aggressively. The range is 1 to 2147483647. The default is 1100.

ip tcp intercept max-incomplete low

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

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

number — Defines the number of incomplete connections below which the software stops behaving aggressively. The range is 1 to 2147483647. The default is 900.

ip tcp intercept mode

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

ip tcp intercept mode {**intercept** | **watch**}
no ip tcp intercept mode [**intercept** | **watch**]

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.

ip tcp intercept one-minute high

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

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

number — Specifies the number of connection requests that can be received in the last one-minute sample period before the software behaves aggressively. The range is 1 to 2147483647. The default is 1100.

ip tcp intercept one-minute low

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

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

number	Defines the number of connection requests in the last one-minute sample period below which the software stops behaving aggressively. The range is 1 to 2147483647. The default is 900.

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 value, use the **no** form of this command.

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

seconds	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.

show tcp intercept connections

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

show tcp intercept connections

show tcp intercept statistics

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

show tcp intercept statistics