Security Configuration Guide: Denial of Service Attack Prevention, Cisco IOS Release 12.4

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

Configuring TCP Intercept (Preventing Denial-of-Service Attacks)

The TCP Intercept feature implements software to protect TCP servers from TCP SYN-flooding attacks, which are a type of denial-of-service attacks. The TCP Intercept feature helps prevent SYN-flooding attacks by intercepting and validating TCP connection requests.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for TCP Intercept

- You cannot configure the TCP Intercept feature on a device that has Network Address Translation (NAT) configured.
- TCP options that are negotiated on a handshake (such as RFC 1323 about window scaling) are not renegotiated because the TCP intercept software does not know what a server can negotiate.

Information About TCP Intercept

TCP Intercept

The TCP Intercept feature implements software to protect TCP servers from TCP SYN-flooding attacks, which are a type of denial-of-service attacks.

A SYN-flooding attack occurs when a hacker floods a server with a barrage of requests for connection. Because these messages have unreachable return addresses, these connections cannot be established. The resulting volume of unresolved open connections eventually overwhelms the server and causes it to deny service to valid requests, thereby preventing legitimate users from connecting to websites, accessing e-mails, using FTP service, and so on.

The TCP Intercept feature helps prevent SYN-flooding attacks by intercepting and validating TCP connection requests. In intercept mode, the TCP intercept software intercepts TCP synchronization (SYN) packets that match an extended access list from clients to servers. The software establishes a connection with the client on behalf of the destination server, and if successful, establishes a connection with the server on behalf of the client and knits the two half connections transparently. Because of the intercept of SYN packets, connection attempts from unreachable hosts never reach the server. The software continues to intercept and forward packets throughout the duration of the connection. The number of SYN packets per second and the number of concurrent connections that are proxied depends on the platform, memory, processor, and so on.

In case of illegitimate requests, the configured timeouts for half-opened connections and the configured thresholds for TCP connection requests protect destination servers while still allowing valid requests.

When establishing a security policy using TCP intercept, you can choose to intercept either all requests or only those coming from specific networks or destined for specific servers. You can also configure the connection rate and the threshold for outstanding connections.

You can choose to operate TCP intercept in watch mode, as opposed to intercept mode. In watch mode, the software passively watches the connection requests flowing through a router. If a connection fails to get established in a configured interval, the software intervenes and terminates the connection attempt.

TCP Intercept and Watch Modes

The TCP Intercept feature can operate in either active intercept mode or passive watch mode. The default is intercept mode.

In intercept mode, the software actively intercepts each incoming connection request (SYN) and responds on behalf of the server with a SYN-ACK, then waits for an acknowledge (ACK) from the client. When the ACK is received, the original SYN is sent to the server and the software performs a three-way handshake with the server. When the three-way handshake is complete, the two half connections are joined.

In watch mode, connection requests are allowed to pass through the router to the server but are watched until they become established. If connection requests fail to establish within 30 seconds (configurable by using the **ip tcp intercept watch-timeout** command), the software sends a reset request to the server to clear up its state.

TCP Intercept Timers and Aggressive Thresholds

In the TCP Intercept feature, two factors determine when the aggressive behavior begins and ends: total number of incomplete connections and connection requests during the last one-minute sample period. Both

these thresholds have default values that can be redefined. Use the **ip tcp intercept max-incomplete** and **ip tcp intercept one-minute** commands to configure aggressive thresholds.

When a threshold is exceeded, the TCP intercept assumes that the server is under attack and goes into aggressive mode. In aggressive mode, the following occurs:

- Each newly arriving connection causes the oldest partial connection to be deleted. (You can change this setting to a random drop mode.)
- The initial retransmission timeout is reduced by half to 0.5 seconds, which cuts the total time to establish a connection by half. (When not in aggressive mode, the initial retransmission timeout is 1 second. The subsequent timeouts are 2 seconds, 4 seconds, 8 seconds, and 16 seconds. The code retransmits four times before giving up, so it gives up after 31 seconds of no acknowledgment.)
- In watch mode, the watch timeout is reduced by half. (If the default is in place, the watch timeout becomes 15 seconds.)

The drop strategy can be changed from the oldest connection to a random connection by using the **ip tcp intercept drop-mode random** command.

Use the **ip tcp intercept max-incomplete** command to change the threshold for triggering aggressive mode based on the total number of incomplete connections. The default values for **low** and **high** are 900 and 1100 incomplete connections, respectively.

Use the **ip tcp intercept one-minute** command to change the threshold for triggering aggressive mode based on the number of connection requests received in the last one-minute sample period. The default values for **low** and **high** are 900 and 1100 connection requests, respectively. When the **high** value is exceeded, the aggressive behavior begins. When quantities fall below the **low** value, the aggressive behavior ends.

How to Configure TCP Intercept

Note You cannot configure the TCP Intercept feature on a device that has NAT configured.

- Enabling TCP Intercept, page 3

Enabling TCP Intercept

You can define an access list to intercept either all requests or only those coming from specific networks or destined for specific servers. Typically, the access list will define the source as **any** and define specific destination networks or servers. Do not filter source addresses because you may not know the source from which to intercept packets. You must identify the destination addresses to protect destination servers.

If no access list match is found, the router allows the request to pass with no further action.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **access-list** *access-list-number* {**deny** | **permit** | **remark**} {*host-ip-address* | **any** | *host*}
4. **ip tcp intercept list** *access-list-number*
5. **ip tcp intercept mode** {**intercept** | **watch**}
6. **ip tcp intercept drop-mode** {**oldest** | **random**}
7. **ip tcp intercept watch-timeout** *seconds*
8. **ip tcp intercept finrst-timeout** *seconds*
9. **ip tcp intercept connection-timeout** *seconds*
10. **ip tcp intercept max-incomplete low** *number* **high** *number*
11. **ip tcp intercept one-minute low** *number* **high** *number*
12. **exit**
13. **show tcp intercept connections**
14. **show tcp intercept statistics**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**access-list** *access-list-number* {**deny** | **permit** | **remark**} {*host-ip-address* | **any** | *host*} **Example:** `Router(config)# access-list 20 permit any`	Defines an extended IP access list.
Step 4	**ip tcp intercept list** *access-list-number* **Example:** `Router(config)# ip tcp intercept list 20`	Enables TCP intercept.

	Command or Action	Purpose
Step 5	**ip tcp intercept mode** {**intercept** | **watch**} **Example:** `Router(config)# ip tcp intercept mode intercept`	Changes the TCP intercept mode.
Step 6	**ip tcp intercept drop-mode** {**oldest** | **random**} **Example:** `Router(config)# ip tcp intercept drop-mode random`	Sets the TCP intercept drop mode.
Step 7	**ip tcp intercept watch-timeout** *seconds* **Example:** `Router(config)# ip tcp intercept watch-timeout 200`	Defines how long the software waits for a watched TCP intercept connection to reach the established state before sending a reset to the server.
Step 8	**ip tcp intercept finrst-timeout** *seconds* **Example:** `Router(config)# ip tcp intercept finrst-timeout 220`	Changes the time between receiving a reset or finish (FIN)-exchange and dropping the connection.
Step 9	**ip tcp intercept connection-timeout** *seconds* **Example:** `Router(config)# ip tcp intercept connection-timeout 180`	Changes the time a TCP connection is managed by TCP intercept after no activity.
Step 10	**ip tcp intercept max-incomplete low** *number* **high** *number* **Example:** `Router(config)# ip tcp intercept max-incomplete low 3220 high 4550`	Sets the threshold for the number of incomplete connections below which the software leaves aggressive mode or the maximum number of incomplete connections allowed before the software enters aggressive mode. • In Cisco IOS Release 12.4(15)T, the **ip tcp intercept max-incomplete high** and **ip tcp intercept max-incomplete low** commands were replaced by the **ip tcp intercept max-incomplete low** *number* **high** *number* command.

	Command or Action	Purpose
Step 11	**ip tcp intercept one-minute low** *number* **high** *number* **Example:** `Router(config)# ip tcp intercept one-minute low 234 high 456`	Sets the threshold for the number of connection requests received in the last one-minute below which the software leaves aggressive mode and the number of connection requests that can be received in the last one-minute before the software enters aggressive mode. • In Cisco IOS Release 12.4(15)T, the **ip tcp intercept one-minute high** and **ip tcp intercept one-minute low** commands were replaced by the **ip tcp intercept one-minute low** *number* **high** *number* command.
Step 12	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode and enters privileged EXEC mode.
Step 13	**show tcp intercept connections** **Example:** `Router# show tcp intercept connections`	Displays incomplete and established TCP connections.
Step 14	**show tcp intercept statistics** **Example:** `Router# show tcp intercept statistics`	Displays TCP intercept statistics.

Configuration Examples for TCP Intercept

Example: Enabling TCP Intercept

The following examples shows how to define the extended IP access list 101 and enable the intercept of packets for all TCP servers:

```
Router# configure terminal
Router(config)# access-list 101 permit any
Router(config)# ip tcp intercept list 101
Router(config)# ip tcp intercept mode intercept
Router(config)# ip tcp intercept drop-mode random
Router(config)# ip tcp intercept watch-timeout 200
Router(config)# ip tcp intercept finrst-timeout 220
Router(config)# ip tcp intercept connection-timeout 180
Router(config)# ip tcp intercept max-incomplete low 3220 high 4550
Router(config)# ip tcp intercept one-minute low 234 high 456
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	*Cisco IOS Master Commands List, All Releases*
Security commands	• *Cisco IOS Security Command Reference: Commands A to C* • *Cisco IOS Security Command Reference: Commands D to L* • *Cisco IOS Security Command Reference: Commands M to R* • *Cisco IOS Security Command Reference: Commands S to Z*

Standards and RFCs

Standard/RFC	Title
RFC 1323	*TCP Extensions for High Performance*

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for TCP Intercept

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1 Feature Information for TCP Intercept

Feature Name	Releases	Feature Information
TCP Intercept	11.3(1) 12.4(20)T	This chapter describes how to configure your router to protect TCP servers from TCP SYN-flooding attacks, a type of denial-of-service attacks. You must configure the TCP Intercept feature to protect against TCP SYN-flooding attacks. The following commands were introduced or modified: **ip tcp intercept connection-timeout**, **ip tcp intercept drop-mode**, **ip tcp intercept finrst-timeout**, **ip tcp intercept list**, **ip tcp intercept max-incomplete**, **ip tcp intercept mode**, **ip tcp intercept one-minute**, **ip tcp intercept watch-timeout**.