Security Configuration Guide: Denial of Service Attack Prevention, Cisco IOS XE Gibraltar 16.12.X

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com go trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2019 Cisco Systems, Inc. All rights reserved.

CONTENTS

CHAPTER 1

Automatic Signature Extraction

The Automatic Signature Extraction (ASE) feature helps shorten the response time for identifying malware by dynamically extracting signatures of unknown viruses and worms traversing the network without the need for human intervention.

Before Cisco IOS Release 12.4(15)T, network protection from malware such as botnets, viruses, and worms was accomplished by deploying solutions that rely on manual signatures to identify the malware. Normally, security professionals require approximately 8 to 12 hours to generate a signature for a new piece of malware. This time interval had been acceptable for thwarting malware, but is no longer acceptable nor scalable due to the exponential increase in malware that is seen on networks.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and 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.

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.

Prerequisites for Automatic Signature Extraction

- The ASE collector runs on an x86-based Linux PC and must have IP connectivity to the network and ASE sensors. Threat Information Distribution Protocol (TIDP) is the communication protocol used between the Linux-based ASE collector and Cisco IOS-based ASE sensors.

- It is recommended that the ASE collector software image run on RedHat Enterprise Linux AS Release 3 or a later release.

Note Contact your Cisco representative for more information about installing the ASE collector functionality on your network.

Information About Automatic Signature Extraction

Automatic Signature Extraction Overview

The Automatic Signature Extraction feature is used to identify and define potential worms and viruses found in network traffic based on the following characteristics:

- Content invariance identifies that all worms have some code that remains unchanged through the infection.
- Content prevalence identifies if packet payloads were observed frequently in the network. Because worms are designed to spread, the unchanged portion of a worm's content appears frequently on a network as it spreads or attempts to spread.
- Address dispersion identifies whether the same payload is sent to and from a large number of source and destination IP address pairs.

Note The ASE feature can detect e-mail viruses but is disabled by default. This feature can be enabled on the ASE collector. Contact your Cisco representative for more information.

When the ASE sensor extracts a malware signature, the ASE sensor sends the signature to the collector using the TIDP Threat Mitigation Service (TMS) to contain and mitigate the malware outbreak among TMS consumers spread across the network. The TMS framework rapidly and efficiently distributes threat information to devices on the network and generates actions to TMS consumers to either drop or redirect the packets containing the malware signature.

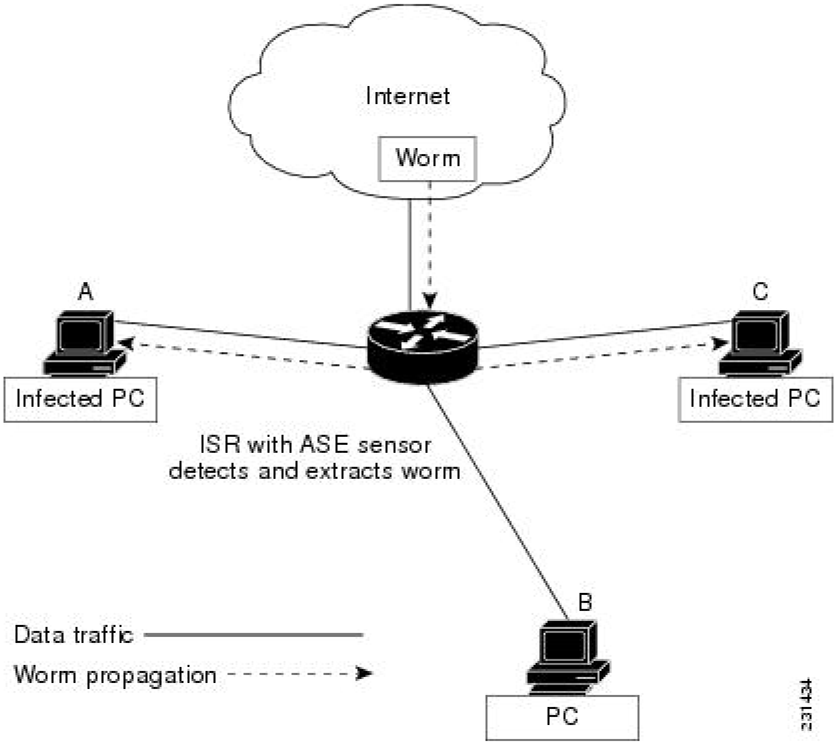
Note See the "Automatic Signature Extraction Sensor Operation" for more information on this feature.

Automatic Signature Extraction Sensor Operation

The ASE feature has two main components: a sensor and collector. The ASE sensor sifts through the contents of network traffic to reduce the number of different source and destination addresses seen in packets. To minimize the impact on the device, sensing can be enabled or disabled on a per-interface basis and traffic designated as ASE traffic can be specified. The ASE sensor observes the same traffic as the router can observe after an access list is applied.

Note The sensor is unable to extract signatures from within encrypted traffic passing through a router.

The figure below shows that devices A and C are infected with the same worm. As traffic crosses the Cisco IOS router running the ASE sensor, the router extracts the worm's signature based on its address dispersion and content prevalence. Then the router sends this information to the ASE collector for further processing.



Automatic Signature Extraction Collector Operation

The ASE collector, which runs on a Linux-based PC, performs the following functions:

- Processes signatures it receives from the ASE sensor.
- Initiates the mitigation of signatures.
- Coordinates detection between multiple ASE sensors.
- Manages and distributes entry information and files on the network.
- Collects signatures and packets sent by the sensor.
- Analyzes extracted signatures to determine what the best signature is for a malicious packet to correctly identify a threat.
- Performs post processing of signatures to reduce false alarms.
- Maintains a signature database.
- Reduces false positives in signatures through classification.
- Manages sensor configuration such as thresholds, scanning criteria, and other parameters.
- Generates a report or reports on collected signatures.

Note Contact your Cisco representative for more information about installing the ASE collector functionality on your network.

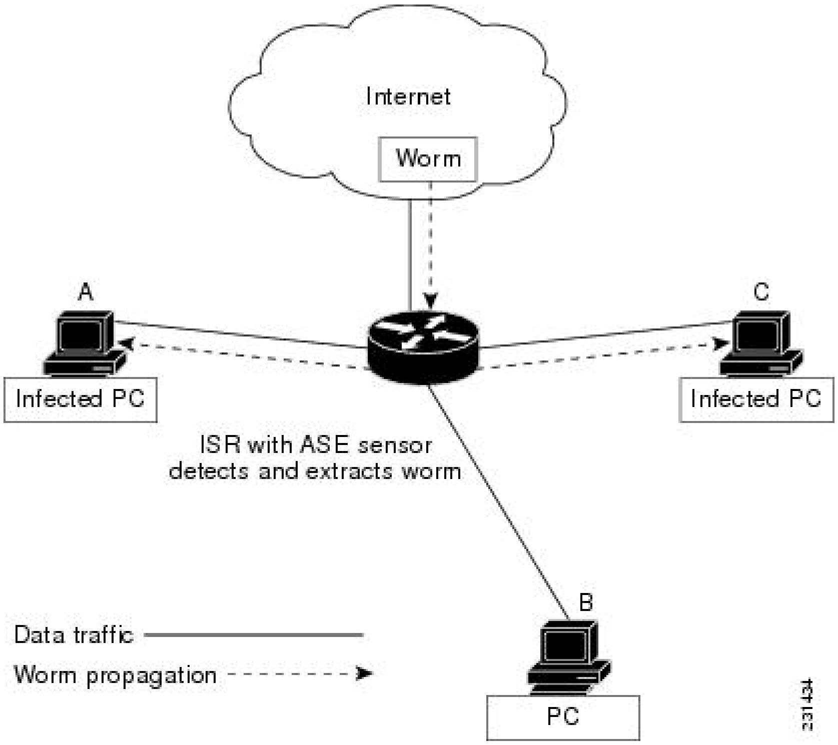
Automatic Signature Extraction Implementation on a Network

Self-propagating worms continue to grow and affect the security of hosts and networks. These malicious malware attacks often target specific victims or subnets within an enterprise organization. Specifically, a worm can affect and saturate the local network (including all hosts), the branch router, and the local WAN connection or both. The optimal location to detect, contain, and mitigate these worms is on the gateway network connection to prevent the worms from spreading to the entire network, including all connected branches.

Using the WAN Aggregation Model to Contain Malware

The ASE sensor is typically deployed on the Customer Premises Equipment (CPE) WAN so that worms closest to the source can be extracted and prevented from spreading to other areas of the enterprise network.

The WAN aggregation model refers to the traditional deployment scenario in which CPEs are terminated over WAN links to an aggregation HUB. In this model, the CPEs would serve as ASE sensors, and the aggregation HUB would provide ASE Collector functionality. The figure below shows how worm signatures are extracted at the CPEs and the HUB site with the ASE sensor and shows how the ASE sensor uses this signature information with the ASE collector to contain the outbreak.



How to Configure the Automatic Signature Extraction Sensor

Configuring Automatic Signature Extraction Sensor

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. ase group TIDP-group-number
4. ase collector ip-address
5. **ase signature extraction**
6. interface interface-type number
7. **ase enable**
8. **end**
9. **show ase**

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	ase group TIDP-group-number **Example:** `Router(config)# ase group 10`	The group number range is between 1 and 65535, which identifies the TIDP group number used for exchange between the ASE sensor and ASE collector.
Step 4	ase collector ip-address **Example:** `Router(config)# ase collector 10.10.10.3`	Enters the destination IP address of the ASE collector server so that the ASE sensor has IP connectivity to the ASE collector.
Step 5	**ase signature extraction** **Example:** `Router(config)# ase signature extraction`	Enables the ASE feature globally on the router.

	Command or Action	Purpose
Step 6	interface interface-type number **Example:** `Router(config)# interface GigabitEthernet0/1`	Enters the interface for the ASE feature, and enters interface configuration mode.
Step 7	**ase enable** **Example:** `Router(config-if)# ase enable`	Enables the ASE feature on this interface.

Step 8	**end**
	Example:
	`Router(config-if)# end`
		Returns to privileged EXEC mode.

Step 9	**show ase** **Example:** `Router# show ase`	Displays the ASE run-time status. The four states are: • **Not Enabled** --(Not displayed) The ASE feature is not enabled in global configuration mode. • **Enabled** --The ASE feature is enabled in global configuration mode, but the ASE sensor has not connected with the ASE collector. • **Connected** --The ASE sensor has connected with the ASE collector, but it has not completed initialization. • **Online** --The ASE is ready for inspecting traffic.

What to Do Next

Start the ASE collector. The ASE collector, which runs on a Linux-based PC, provides the ASE sensor software on the Cisco IOS with entries and analysis on extracted signatures.

Note Contact your Cisco representative for more information about installing the ASE collector on your network.

After the ASE collector is started, the ASE run-time status information can be displayed by using the **show ase** command, as shown below:

Note The ASE collector must be started in order for the ASE run-time status information to be displayed.

```
Router# show ase
ASE Information:
```

```
Collector IP: 10.10.10.3
TIDP Group  : 10
Status      : Online
Packets inspected: 1105071
Address Dispersion Threshold: 20
Prevalence Threshold: 10
Sampling set to: 1 in 64
Address Dispersion Inactivity Timer: 3600s
Prevalence Table Refresh Time: 60s
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases

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 Automatic Signature Extraction

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 Automatic Signature Extraction

Feature Name	Releases	Feature Information
Automatic Signature Extraction	12.4(15)T	The Automatic Signature Extraction feature helps shorten the response time for identifying malware by dynamically extracting signatures for unknown viruses and worms traversing the network without the need for human intervention. This feature was introduced on the Cisco 1800, 2800, and 7200 series routers, Cisco 7301 router, and Integrated Services Routers (ISRs) as ASE sensors. The following commands were introduced or modified: **ase collector , ase enable , ase group , ase signature extraction , clear ase signatures , debug ase , show ase**

Glossary

botnet --Slang term for a collection of software robots, or bots, which run autonomously or to a network of compromised “zombie” computers running distributed programs, which are usually referred to as worms, Trojan horses, or backdoors, under a common command and control infrastructure.

CPE --Customer Premises Equipment. Terminating equipment, such as a router installed at a customer site, and connected to a WAN.

ISR --Integrated Services Router. Router that supports integrated or multimedia services, including traffic management mechanisms.

malware --Detrimental software designed to infiltrate or damage a computer system without the owner's informed consent. Examples of malware include viruses, worms, botnets, spam, adware, etc.

signature --The 40 bytes of packet data that can be used to identify a piece of malware.

TIDP --Threat Information Distribution Protocol. Communication protocol used between the Linux-based Automatic Signature Extraction collector and Cisco IOS-based ASE sensors.

TMS --Threat Mitigation Service. TMS is used with the TIDP protocol to contain and mitigate the malware outbreak among TMS consumers on a network.

Virus --Hidden, self-replicating section of computer software, usually malicious logic, that propagates by infecting--that is, inserting a copy of itself into and becoming part of--another program. A virus cannot run by itself; it requires that its host program be run to make the virus active.

WAN --wide-area network. Data communications network that serves users across a broad geographic area and often uses transmission devices provided by common carriers. Frame Relay, SMDS, and X.25 are examples of WANs.

worm --Computer program that can run independently, can propagate a complete working version of itself onto other hosts on a network, and can consume computer resources destructively.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental. © 2011 Cisco Systems, Inc. All rights reserved.

CHAPTER 2

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 caveats and feature information, see Bug Search Tool and 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.

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

- Do not configure the TCP Intercept feature with either NAT and/or the zone-based firewall or Context-Based Access Control (CBAC) firewall.
- 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 Do not configure the TCP Intercept feature with either NAT and/or the zone-based firewall or Context-Based Access Control (CBAC) firewall.

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:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

Step 3	**access-list** *access-list-number* {**deny** | **permit** | **remark**} {*host-ip-address* | **any** | *host*}
	Example:
	`Device(config)# access-list 20 permit any`
		Defines an extended IP access list.

Step 4	**ip tcp intercept list** *access-list-number* **Example:** `Device(config)# ip tcp intercept list 20`	Enables TCP intercept.
Step 5	**ip tcp intercept mode** {**intercept** | **watch**} **Example:** `Device(config)# ip tcp intercept mode intercept`	Changes the TCP intercept mode.
Step 6	**ip tcp intercept drop-mode** {**oldest** | **random**} **Example:** `Device(config)# ip tcp intercept drop-mode random`	Sets the TCP intercept drop mode.
Step 7	**ip tcp intercept watch-timeout** *seconds* **Example:** `Device(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:**	Changes the time between receiving a reset or finish (FIN)-exchange and dropping the connection.

	Command or Action	Purpose
	`Device(config)# ip tcp intercept finrst-timeout 220`	
Step 9	**ip tcp intercept connection-timeout** *seconds* **Example:** `Device(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:** `Device(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.
Step 11	**ip tcp intercept one-minute low** *number* **high** *number* **Example:** `Device(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:** `Device(config)# exit`	Exits global configuration mode and enters privileged EXEC mode.
Step 13	**show tcp intercept connections** **Example:** `Device# show tcp intercept connections`	Displays incomplete and established TCP connections.
Step 14	**show tcp intercept statistics** **Example:** `Device# 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 2: 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**.