TCP Out-of-Order Packet Support for Cisco IOS Firewall and Cisco IOS IPS

First Published: November 17, 2006
Last Updated: November 17, 2006

This feature allows out-of-order packets in TCP streams to be cached and reassembled before they are inspected by Cisco IOS Intrusion Prevention System (IPS) or Cisco IOS Firewall.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the "Feature Information for TCP Out-of-Order Packet Support for Cisco IOS Firewall and IPS" section on page 9.

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

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

Contents

CISCO SYSTEMS

Corporate Headquarters
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Prerequisites for TCP Out-of-Order Packet Support for Cisco IOS Firewall and Cisco IOS IPS

Cisco IOS IPS or Cisco IOS Firewall must be configured on your router.

Restrictions for TCP Out-of-Order Packet Support for Cisco IOS Firewall and Cisco IOS IPS

- The feature is enabled by default. The user must explicitly disable it. To disable TCP out-of-order packet buffering and reassembly, issue the **ip inspect tcp reassembly queue length 0** command.
- Zone-based policy firewall is not supported. Only Cisco IOS IPS and Cisco IOS Firewall application inspection can support out-of-order TCP packets.

Information About TCP Out-of-Order Packet Support for Cisco IOS Firewall and Cisco IOS IPS

Before reassembling TCP out-of-order packets, you should understand the following concept:

How TCP Out-of-Order Packet Support Works

Cisco IOS Firewall and IPS track packets in TCP connections. If configured to look into the application data of the packets, Cisco IOS Firewall and IPS expect the TCP packets to arrive in the correct order because some data items are split across segments. When packets arrive out of order, they are dropped by the firewall or IPS. Dropping out-of-order packets can cause significant delays in end applications because packets are dropped only after the retransmission timer expires (on behalf of the sender).

Out-of-order TCP packet support enables Cisco IOS Firewall and IPS to hold a copy of the out-of-order packet in a buffer (whose size is configurable with a maximum of 1024 packets per session). The original packet passes through the router and reaches its destination, but the firewall or IPS do not execute on the packet. When the next packet arrives, the firewall or IPS look for that packet to “fill the hole,” providing a consecutive sequence of segments. If this packet does not fulfill that requirement, it is processed as an out-of-order packet; when another packet arrives and provides a consecutive sequence of segments, it is processed by the firewall or IPS.

How to Configure Cisco IOS Firewall or IPS to Handle TCP Out-of-Order Packets

This section contains the following procedure:

Changing Default TCP Out-of-Order Packet Parameters

Use this task to change any of the predefined parameters that instruct Cisco IOS Firewall application inspection or Cisco IOS IPS how to handle out-of-order TCP packets.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip inspect tcp reassembly** {[**queue length** *packet-number*] [**timeout** *seconds*] [**memory limit** *size-in-kb*] [**alarm** {**on** | **off**}]}

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	**ip inspect tcp reassembly** {[**queue length** *packet-number*] [**timeout** *seconds*] [**memory limit** *size-in-kb*] [**alarm** {**on** | **off**}]} **Example:** `Router(config)# ip inspect tcp reassembly queue length 10 timeout 8`	Sets parameters that define how a Cisco IOS IPS handles out-of-order TCP packets. • **queue length** *packet-number*—Maximum number of out-of-order packets that can be held per queue (buffer). Note that there are 2 queues per session. Available value range: 0 to 1024. Default value: 16. If the queue length is set to 0, all out-of-order packets are dropped. • **timeout** *seconds*—Number of seconds the TCP reassembly module will hold out-of-order segments waiting for the first segment missing in the sequence. After the timeout timer has expired, a retry timer is started. The value for the retry timer is four times the configured timeout value. • **memory limit** *size-in-kb*—Maximum allowed memory use by the TCP reassembly module. • **alarm** {**on** | **off**}—If enabled, a syslog message is generated when an out-of-order packet is dropped. Default value: **on**

Configuration Examples for TCP Out-of-Order Packet Parameters

This sections contains the following configuration example:

- Verifying TCP Out-of-Order Packets: Example, page 4

Verifying TCP Out-of-Order Packets: Example

The following example shows how to instruct Cisco IOS IPS how to handle out of order packets for TCP connections:

```
Router(config)# ip inspect tcp reassembly queue length 18
Router(config)# ip inspect tcp reassembly memory limit 200
```

The following sample output displays the configured out-of-order packet parameters:

```
Router# show ip ips statistics

Signature Statistics [process switch:fast switch]
Signature 1000: 324 packets checked: [124:200]
Signature 1024: 100 packets checked: [0:100]
Interfaces configured for ips 0
Session creations since subsystem startup or last reset 0
Current session counts (estab/half-open/terminating) [0:0:0]
Maxever session counts (estab/half-open/terminating) [0:0:0]
Last session created never
Last statistic reset never
TCP reassembly statistics
received 200 packets out-of-order; dropped 25
peak memory usage; 200 KB; current usage: 154 KB
peak queue length 18
```

Additional References

The following sections provide references related to the TCP Out-of-Order Packet Support for Cisco IOS Firewall and Cisco IOS IPS feature.

Related Documents

Related Topic	Document Title
IPS configuration	*IPS 5.x Signature Format Support and Usability Enhancements*, Cisco IOS Release 12.4(11)T feature module
Firewall configuration	*Cisco IOS Security Configuration Guide*
Firewall IPS commands	*Cisco IOS Security Command Reference*

Standards

Standard	Title
None	—

MIBs

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

RFCs

RFC	Title
None	—

Technical Assistance

Description	Link
The Cisco Technical Support & Documentation website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, tools, and technical documentation. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Command Reference

This section documents the following new command:

- **ip inspect tcp reassembly**

ip inspect tcp reassembly

To set parameters that define how Cisco IOS Firewall application inspection and Cisco IOS Intrusion Prevention System (IPS) will handle out-of-order TCP packets, use the **ip inspect tcp reassembly** command in global configuration mode. To disable at least one defined parameter, use the **no** form of this command.

ip inspect tcp reassembly {[**queue length** *packet-number*] [**timeout** *seconds*] [**memory limit** *size-in-kb*] [**alarm** {**on** | **off**}]}

no ip inspect tcp reassembly {[**queue length**] [**timeout**] [**memory limit**]}

Syntax Description

queue length *packet-number*	Maximum number of out-of-order packets that can be held per queue (buffer). (There are two queues per session.) Available value range: 0 to 1024. Default value: 16. **Note** If the queue length is set to 0, all out-of-order packets are dropped; that is, TCP out-of-order packet buffering and reassembly is disabled.
timeout *seconds*	Number of seconds the TCP reassembly module will hold out-of-order segments that are waiting for the first segment missing in the sequence. After the timeout timer has expired, a retry timer is started. The value for the retry timer is four times the configured timeout value.
memory limit *size-in-kb*	Maximum memory use allowed by the TCP reassembly module.
alarm {**on** | **off**}	If enabled, a syslog message is generated when an out-of-order packet is dropped. Default value: **on**

Command Default

Queue length: 16

Timeout value:

Memory Limit: 1024 kilobytes

Alarm: on

Command Modes

Global configuration

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

The queue length Value

The value specified for the queue length is applicable for two queues per session: one queue is for the initiator traffic and the other queue is for the responder traffic. For example, the default queue size is 16. Thus, up to 16 packets can be held per queue, so 16 packets per queue results in a maximum of 32 packets per session.

When the maximum queue length value is reached, the packet being switched is dropped unless it is the packet that will be processed by a firewall or IPS. If the packet is dropped, a syslog message, which explains why the packet was dropped, will be generated. (To generate syslog messages, you must have the alarm option set to "on.")

The timeout Value

When a timer expires for the first time, the packets in the queue are not deleted. However, after the retry timer expires, the session is deleted, a syslog message is generated, and all unprocessed, out-of-order packets still in the queue are deleted.

The memory limit Value

When the limit for TCP reassembly memory is reached, packets from the reassembly queue of the current session are released so incoming packets can be accepted. Packets from the end of the queue are released to ensure that they are farthest away from the hole that is to be filled. However, if the queue is empty and the maximum memory has been reached, the incoming packet is dropped.

The alarm Value

If an alarm value is not configured, the value is set to "on," unless the **ip inspect alarm** command is enabled and set to off; thus, syslog messages related to TCP connections will not be generated. However, if the alarm value for this command is set to "on" and the **ip inspect alarm** command is set to "off," the value of the **ip inspect alarm** command is ignored and syslog messages are generated.

The alarm value is independent of and in addition to the syslog messages that can be enabled for a Cisco IOS Firewall or Cisco IOS IPS.

Examples

The following example shows how to instruct Cisco IOS IPS how to handle out-of-order packets for TCP connections:

```
Router(config)# ip inspect tcp reassembly queue length 18
Router(config)# ip inspect tcp reassembly memory limit 200
```

Feature Information for TCP Out-of-Order Packet Support for Cisco IOS Firewall and IPS

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 1 Feature Information for TCP Out-of-Order Support

Feature Name	Releases	Feature Information
TCP Out-of-Order Packet Support for Cisco IOS Firewall and Cisco IOS IPS	12.4(11)T	This feature allows out-of-order packets in TCP streams to be cached and reassembled before they are inspected by Cisco IOS Intrusion Prevention System (IPS) or Cisco IOS Firewall.