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

Last Updated: January 19, 2012

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

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.

Americas 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

- How TCP Out-of-Order Packet Support Works, page 2

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

- Changing Default TCP Out-of-Order Packet Parameters, page 3

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

Example Verifying TCP Out-of-Order Packets

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

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
IPS configuration	"IPS 5.x Signature Format Support and Usability Enhancements"
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 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 Out-of-Order Packet Support for Cisco IOS Firewall and IPS

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 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. The following command was introduced by this feature: **ip inspect tcp reassembly**.