Loose Checking Option for TCP Window Scaling in Zone-Based Policy Firewall

The Loose Checking Option for TCP Window Scaling in Zone-Based Policy Firewall feature disables the strict checking of the TCP window-scaling option in a firewall.

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.

Information About Loose Checking Option for TCP Window Scaling in Zone-Based Policy Firewall

Loose Checking Option for TCP Window Scaling Overview

TCP provides various TCP extensions to improve performance over high-bandwidth and high-speed data paths. One such extension is the TCP window-scaling option. The loose-checking option for TCP window-scaling turns off strict checking of the window-scaling option described in RFC 1323.

A larger window size is recommended to improve TCP performance in network paths with large bandwidth-delay product characteristics that are called Long Fat Networks (LFNs). TCP window scaling expands the definition of the TCP window to 32 bits and then uses a scale factor to carry this 32-bit value in the 16-bit window field of the TCP header. The window size can increase to a scale factor of 14. Typical applications use a scale factor of 3 when deployed in LFNs.

A firewall implementation enforces strict checking of the TCP window-scaling option. A firewall drops SYN/ACK packets that have the TCP window-scaling option if it was not offered in the initial synchronization (SYN) packet for the TCP three-way handshake. The window-scale option is sent only in a SYN segment, which is a segment with the SYN bit on. Therefore, the window scale is fixed in each direction when a connection is opened.

Use the **tcp window-scale-enforcement loose** command to disable the strict checking of the TCP window-scaling option in TCP SYN segments.

How to Configure Loose Checking Option for TCP Window Scaling in Zone-Based Policy Firewall

Configuring the TCP Window-Scaling Option for a Firewall

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **parameter-map type inspect** {*parameter-map-name* | **global** | **default**}
4. **tcp window-scale-enforcement loose**
5. **exit**
6. **class-map type inspect** {**match-any** | **match-all**} *class-map-name*
7. **match protocol** [*parameter-map*] [**signature**]
8. **exit**
9. **policy-map type inspect** *policy-map-name*
10. **class type inspect** *class-map-name*
11. **inspect** [*parameter-map-name*]
12. **exit**
13. **class** *name*
14. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**parameter-map type inspect** {*parameter-map-name* | **global** | **default**} **Example:** `Device(config)# parameter-map type inspect pmap-fw`	Configures an inspect parameter map and enters profile configuration mode.
Step 4	**tcp window-scale-enforcement loose** **Example:** `Device(config-profile)# tcp window-scale-enforcement loose`	Disables the strict checking of the TCP window-scaling option in a firewall.
Step 5	**exit** **Example:** `Device(config-profile)# exit`	Exits profile configuration mode and returns to global configuration mode.
Step 6	**class-map type inspect** {**match-any** | **match-all**} *class-map-name* **Example:** `Device(config)# class-map type inspect match-any internet-traffic-class`	Creates an inspect-type class map and enters QoS class-map configuration mode.
Step 7	**match protocol** [*parameter-map*] [**signature**] **Example:** `Device(config-cmap)# match protocol tcp`	Configures a match criteria for a class map on the basis of the specified protocol.
Step 8	**exit** **Example:** `Device(config-cmap)# exit`	Exits the QoS class-map configuration mode and returns to global configuration mode.
Step 9	**policy-map type inspect** *policy-map-name* **Example:** `Device(config)# policy-map type inspect private-internet-policy`	Creates an inspect-type policy map and enters QoS policy-map configuration mode.
Step 10	**class type inspect** *class-map-name* **Example:** `Device(config-pmap)# class type inspect internet-traffic-class`	Specifies the traffic class on which an action is to be performed and enters policy-map class configuration mode.
Step 11	**inspect** [*parameter-map-name*] **Example:** `Device(config-pmap-c)# inspect pmap-fw`	Enables stateful packet inspection.

	Command or Action	Purpose
Step 12	**exit** **Example:** `Device(config-pmap-c)# exit`	Exits QoS policy-map class configuration mode and returns to QoS policy-map configuration mode.
Step 13	**class** *name* **Example:** `Device(config-pmap)# class class-default`	Associates the map class with a specified data-link connection identifier (DLCI).
Step 14	**end** **Example:** `Device(config-pmap)# end`	Exits QoS policy-map configuration mode and returns to privileged EXEC mode.

Configuring a Zone and Zone Pair for a TCP Window Scaling

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address*
5. **zone-member security** *security-zone-name*
6. **exit**
7. **interface** *type number*
8. **ip address** *ip-address*
9. **zone-member security** *security-zone-name*
10. **end**

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	**interface** *type number* **Example:** `Device(config)# interface GigabitEthernet 0/1/5`	Specifies an interface and enters interface configuration mode.

	Command or Action	Purpose
Step 4	**ip address** *ip-address* **Example:** `Device(config-if)# ip address 10.1.1.1 255.255.255.0`	Assigns an interface IP address.
Step 5	**zone-member security** *security-zone-name* **Example:** `Device(config-if)# zone-member security private`	Configures the interface as a zone member.
Step 6	**exit** **Example:** `Device(config-if)# exit`	Exits interface configuration mode and returns to global configuration mode.
Step 7	**interface** *type number* **Example:** `Device(config)# interface GigabitEthernet 0/1/6`	Specifies an interface and enters interface configuration mode.
Step 8	**ip address** *ip-address* **Example:** `Device(config-if)# ip address 209.165.200.225 255.255.255.0`	Assigns an IP address to an interface.
Step 9	**zone-member security** *security-zone-name* **Example:** `Device(config-if)# zone-member security internet`	Configures an interface as a zone member.
Step 10	**end** **Example:** `Device(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Configuration Examples for TCP Window-Scaling

Example: Configuring the TCP Window-Scaling Option for a Firewall

```
Device> enable
Device# configure terminal
Device(config)# parameter-map type inspect pmap-fw
Device(config-profile)# tcp window-scale-enforcement loose
Device(config-profile)# exit
Device(config)# class-map type inspect match-any internet-traffic-class
Device(config-cmap)# match protocol tcp
Device(config-cmap)# exit
Device(config)# policy-map type inspect private-internet-policy
Device(config-pmap)# class type inspect internet-traffic-class
Device(config-pmap-c)# inspect pmap-fw
```

```
Device(config-pmap-c)#exit
Device(config-pmap)# class class-default
Device(config-pmap)#end
```

Example: Configuring a Zone and Zone Pair for TCP Window Scaling

```
Device# enable
Device# configure terminal
Device(config)# interface GigabitEthernet 0/1/5
Device(config-if)# ip address 10.1.1.1 255.255.255.0
Device(config-if)# zone-member security private
Device(config-if)# exit
Device(config)# interface GigabitEthernet 0/1/6
Device(config-if)# ip address 209.165.200.225 255.255.255.0
Device(config-if)# zone-member security internet
Device(config-if)# end
```

Feature Information for Loose Checking Option for TCP Window Scaling in Zone-Based Policy Firewall

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 Loose Checking Option for TCP Window Scaling in Zone-Based Policy Firewall

Feature Name	Releases	Feature Information
Loose Checking Option for TCP Window Scaling in Zone-Based Policy Firewall	Cisco IOS XE Release 3.10S	Loose Checking Option for TCP Window Scaling in Zone-Based Policy Firewall feature disables the strict checking of the TCP Window Scaling option in an IOS-XE firewall. The following command was introduced or modified: **tcp window-scale-enforcement loose**. In Cisco IOS XE Release 3.10S, support was added for the Cisco CSR 1000V Series Routers.