DoS Commands

This chapter contains the following sections:

security-suite deny fragmented

To discard IP fragmented packets from a specific interface, use the **security-suite deny fragmented** Interface (Ethernet, Port Channel) Configuration mode command.

To permit IP fragmented packets, use the **no** form of this command.

Syntax

security-suite deny fragmented *{[***add** *{ip-address* | **any***} {mask* | */prefix-length}]* | *[***remove** *{ip-address* | **any***} {mask* | */prefix-length}]}*

no security-suite deny fragmented

Parameters

- **add** *ip-address* | *any*—Specifies the destination IP address. Use **any** to specify all IP addresses.
- **mask**—Specifies the network mask of the IP address.
- **prefix-length**—Specifies the number of bits that comprise the IP address prefix. The prefix length must be preceded by a forward slash (/).

Default Configuration

Fragmented packets are allowed from all interfaces.

If **mask** is unspecified, the default is 255.255.255.255.

If **prefix-length** is unspecified, the default is 32.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

For this command to work, show security-suite configuration, on page 15 must be enabled both globally and for interfaces.

Example

The following example attempts to discard IP fragmented packets from an interface.

```
switchxxxxxx(config)# security-suite enable global-rules-only
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# security-suite deny fragmented add any /32
To perform this command, DoS Prevention must be enabled in the per-interface mode.
```

security-suite deny icmp

To discard ICMP echo requests from a specific interface (to prevent attackers from knowing that the device is on the network), use the **security-suite deny icmp** Interface (Ethernet, Port Channel) Configuration mode command.

To permit echo requests, use the **no** form of this command.

Syntax

security-suite deny icmp *{[***add** *{ip-address* | **any***} {mask* | */prefix-length}]* | *[***remove** *{ip-address* | **any***} {mask* | */prefix-length}]}*

no security-suite deny icmp

Parameters

- **ip-address** | **any**—Specifies the destination IP address. Use **any** to specify all IP addresses.
- **mask**—Specifies the network mask of the IP address.
- **prefix-length**—Specifies the number of bits that comprise the IP address prefix. The prefix length must be preceded by a forward slash (/).

Default Configuration

Echo requests are allowed from all interfaces.

If **mask** is not specified, it defaults to 255.255.255.255.

If **prefix-length** is not specified, it defaults to 32.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

For this command to work, show security-suite configuration, on page 15 must be enabled both globally and for interfaces.

This command discards ICMP packets with "ICMP type= Echo request" that ingress the specified interface.

Example

The following example attempts to discard echo requests from an interface.

```
switchxxxxxx(config)# security-suite enable global-rules-only
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# security-suite deny icmp add any /32
To perform this command, DoS Prevention must be enabled in the per-interface mode.
```

security-suite deny martian-addresses

To deny packets containing system-reserved IP addresses or user-defined IP addresses, use the **security-suite deny martian-addresses** Global Configuration mode command.

To restore the default, use the **no** form of this command.

Syntax

security-suite deny martian-addresses *{***add** *{ip-address {mask | /prefix-length}}* | ***remove*** *{ip-address {mask | /prefix-length}} (*Add/remove user-specified IP addresses)

security-suite deny martian-addresses ***reserved*** *{***add** | **remove***} (*Add/remove system-reserved IP addresses, see tables below)

no security-suite deny martian-addresses (This command removes addresses reserved by **security-suite deny martian-addresses** *{***add** *{ip-address {mask | /prefix-length}}* | ***remove*** *{ip-address {mask | /prefix-length}},* and removes all entries added by the user. The user can remove a specific entry by using **remove** *ip-address {mask | /prefix-length}* parameter.

There is no **no** form of the **security-suite deny martian-addresses** ***reserved*** *{***add** | **remove***}* command. Use instead the **security-suite deny martian-addresses reserved** *remove* command to remove protection (and free up hardware resources).

Parameters

- **reserved add/remove**—Add or remove the table of reserved addresses below.
- **ip-address**—Adds/discards packets with the specified IP source or destination address.
- **mask**—Specifies the network mask of the IP address.
- **prefix-length**—Specifies the number of bits that comprise the IP address prefix. The prefix length must be preceded by a forward slash (/).
- **reserved**—Discards packets with the source or destination IP address in the block of the reserved (Martian) IP addresses. See the User Guidelines for a list of reserved addresses.

Default Configuration

Martian addresses are allowed.

Command Mode

Global Configuration mode

User Guidelines

For this command to work, show security-suite configuration, on page 15 must be enabled globally.

security-suite deny martian-addresses ***reserved*** adds or removes the addresses in the following table:

Address Block	Present Use
0.0.0.0/8 (except when 0.0.0.0/32 is the source address)	Addresses in this block refer to source hosts on "this" network.
127.0.0.0/8	This block is assigned for use as the Internet host loopback address.
192.0.2.0/24	This block is assigned as "TEST-NET" for use in documentation and example code.
224.0.0.0/4 as source	This block, formerly known as the Class D address space, is allocated for use in IPv4 multicast address assignments.
240.0.0.0/4 (except when 255.255.255.255/32 is the destination address)	This block, formerly known as the Class E address space, is reserved.

Note If the reserved addresses are included, individual reserved addresses cannot be removed.

Example

The following example discards all packets with a source or destination address in the block of the reserved IP addresses.

```
switchxxxxxx(config)# security-suite deny martian-addresses reserved add
```

security-suite deny syn

To block the creation of TCP connections from a specific interface, use the **security-suite deny syn** Interface (Ethernet, Port Channel) Configuration mode command. This a complete block of these connections.

To permit creation of TCP connections, use the **no** form of this command.

Syntax

security-suite deny syn {*[***add** *{tcp-port* | **any***} {ip-address* | **any***} {mask* | */prefix-length}]* | *[***remove** *{tcp-port* | **any***} {ip-address* | **any***} {mask* | */prefix-length}]}*

no security-suite deny syn

Parameters

- **ip-address** | **any**—Specifies the destination IP address. Use **any** to specify all IP addresses.
- **mask**— Specifies the network mask of the destination IP address.
- **prefix-length**—Specifies the number of bits that comprise the destination IP address prefix. The prefix length must be preceded by a forward slash (/).
- **tcp-port** | **any**—Specifies the destination TCP port. The possible values are: **http**, **ftp-control**, **ftp-data**, **ssh**, **telnet**, **smtp**, or **port number**. Use **any** to specify all ports.

Default Configuration

Creation of TCP connections is allowed from all interfaces.

If the **mask** is not specified, it defaults to 255.255.255.255.

If the ***prefix-length*** is not specified, it defaults to 32.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

For this command to work, show security-suite configuration, on page 15 must be enabled both globally and for interfaces.

The blocking of TCP connection creation from an interface is done by discarding ingress TCP packets with "SYN=1", "ACK=0" and "FIN=0" for the specified destination IP addresses and destination TCP ports.

Example

The following example attempts to block the creation of TCP connections from an interface. It fails because security suite is enabled globally and not per interface.

```
switchxxxxxx(config)# security-suite enable global-rules-only
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# security-suite deny syn add any /32 any
To perform this command, DoS Prevention must be enabled in the per-interface mode.
```

security-suite deny syn-fin

To drop all ingressing TCP packets in which both SYN and FIN are set, use the **security-suite deny syn-fin** Global Configuration mode command.

To permit TCP packets in which both SYN and FIN are set, use the **no** form of this command.

Syntax

security-suite deny syn-fin

no security-suite deny syn-fin

Parameters

This command has no arguments or keywords.

Default Configuration

The feature is enabled by default.

Command Mode

Global Configuration mode

Example

The following example blocks TCP packets in which both SYN and FIN flags are set.

```
switchxxxxxx(config)# security-suite deny syn-fin
```

security-suite dos protect

To protect the system from specific well-known Denial of Service (DoS) attacks, use the **security-suite dos protect** Global Configuration mode command. There are three types of attacks against which protection can be supplied (see parameters below).

To disable DoS protection, use the **no** form of this command.

Syntax

security-suite dos protect {**add** *attack* | **remove** *attack*}

no security-suite dos protect

Parameters

add/remove *attack*—Specifies the attack type to add/remove. To add an attack is to provide protection against it; to remove the attack is to remove protection.

The possible attack types are:

- **stacheldraht**—Discards TCP packets with source TCP port 16660.
- **invasor-trojan**—Discards TCP packets with destination TCP port 2140 and source TCP port 1024.
- **back-orifice-trojan**—Discards UDP packets with destination UDP port 31337 and source UDP port 1024.

Default Configuration

No protection is configured.

Command Mode

Global Configuration mode

User Guidelines

For this command to work, show security-suite configuration, on page 15 must be enabled globally.

Example

The following example protects the system from the Invasor Trojan DOS attack.

```
switchxxxxxx(config)# security-suite dos protect add invasor-trojan
```

security-suite dos syn-attack

To rate limit Denial of Service (DoS) SYN attacks, use the **security-suite dos syn-attack** Interface Configuration mode command. This provides partial blocking of SNY packets (up to the rate that the user specifies).

To disable rate limiting, use the **no** form of this command.

Syntax

security-suite dos syn-attack *syn-rate* {***any*** **|** *ip-address*} {*mask* | *prefix-length*}

no security-suite dos syn-attack {***any*** **|** *ip-address*} {*mask* | *prefix-length*}

Parameters

- **syn-rate**—Specifies the maximum number of connections per second. (Range: 199–1000)
- **any | ip-address**—Specifies the destination IP address. Use **any** to specify all IP addresses.
- **mask**—Specifies the network mask of the destination IP address.
- **prefix-length**—Specifies the number of bits that comprise the destination IP address prefix. The prefix length must be preceded by a forward slash (/).

Default Configuration

No rate limit is configured.

If **ip-address** is unspecified, the default is 255.255.255.255

If **prefix-length** is unspecified, the default is 32.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

For this command to work, show security-suite configuration, on page 15 must be enabled both globally and for interfaces. This command rate limits ingress TCP packets with "SYN=1", "ACK=0" and "FIN=0" for the specified destination IP addresses. SYN attack rate limiting is implemented after the security suite rules are applied to the packets. The ACL and QoS rules are not applied to those packets. Since the hardware rate limiting counts bytes, it is assumed that the size of “SYN” packets is short.

Example

The following example attempts to rate limit DoS SYN attacks on a port. It fails because security suite is enabled globally and not per interface.

```
switchxxxxxx(config)# security-suite enable global-rules-only
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# security-suite dos syn-attack 199 any /10
To perform this command, DoS Prevention must be enabled in the per-interface mode.
```

security-suite enable

To enable the security suite feature and setting, use the **security-suite enable** Global Configuration mode command. The security suite feature supports protection against various types of attacks. To restore the default configuration, use the **no** form of this command.

Syntax

security-suite enable [**global-rules-only | interface-rules-only**]

no security-suite enable

Parameters

- **global-rules-only**—(Optional) Specifies that device will support only global level (and not interface level) security suite commands). This setting saves space in the Ternary Content Addressable Memory (TCAM). If this keyword is not used, security-suite commands can be used both globally on per-interface.
- **interface-rules-only**—(Optional) Specifies that device will support only interface level security suite command (See details in user guidelines below). This mode cannot be enabled if an ACL is applied to any interface on device.
- **(none)** - If no keyword is used, security-suite commands can be used both globally and per-interface.This mode cannot be enabled if an ACL is applied to any interface on device.

Default Configuration

The security suite feature is disabled.

If neither **global-rules-only** or **interface-rules-only** are specified, the default is to enable security-suite globally and per interfaces.

Command Mode

Global Configuration mode

User Guidelines

Use this command to enable the ability to define security suite settings, and to determine the type of settings that can be enabled (only global level rules, only interface level rules or both types). When security-suite is enabled, the following commands can be used, depending on the mode set by user:

When this command is used, hardware resources are reserved. The number of resources reserved depends on the mode specified in command (**global-rules-only**, **interface-rules-only** or no mode (meaning both types)). Resources are released when the **no security-suite enable** command is entered.

MAC ACLs must be removed before the security-suite is enabled. The rules can be re-entered after the security-suite is enabled. If ACLs or policy maps are assigned on interfaces, per interface security-suite rules cannot be enabled.

Example 1—The following example enables the security suite feature and specifies that security suite commands are global commands only. When an attempt is made to configure security-suite on a port, it fails.

```
switchxxxxxx(config)# security-suite enable global-rules-only
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# security-suite dos syn-attack 199 any /10
To perform this command, DoS Prevention must be enabled in the per-interface mode.
```

Example 2—The following example enables the security suite feature globally and on interfaces. The security-suite command succeeds on the port.

```
switchxxxxxx(config)# security-suite enable
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# security-suite dos syn-attack 199 any /10
switchxxxxxx(config-if)#
```

security-suite syn protection mode

To set the TCP SYN protection mode, use the **security-suite syn protection mode** Global Configuration mode command.

To set the TCP SYN protection mode to default, use the **no** form of this command.

Syntax

security-suite syn protection mode {disabled | report | block}

no security-suite syn protection mode

Parameters

- **disabled**—Feature is disabled
- **report**—Feature reports about TCP SYN traffic per port (including rate-limited SYSLOG message when an attack is identified)
- **block**—TCP SYN traffic from attacking ports destined to the local system is blocked, and a rate-limited SYSLOG message (one per minute) is generated

Default Configuration

The default mode is block.

Command Mode

Global Configuration mode

User Guidelines

On ports in which an ACL is defined (user-defined ACL etc.), this feature cannot block TCP SYN packets. In case the protection mode is block but SYN Traffic cannot be blocked, a relevant SYSLOG message will be created, e.g.: “port gi1/0/1 is under TCP SYN attack. TCP SYN traffic cannot be blocked on this port since the port is bound to an ACL.”

Example 1: The following example sets the TCP SYN protection feature to report TCP SYN attack on ports in case an attack is identified from these ports.

```
switchxxxxxx(config)# security-suite syn protection mode report
```

Example 2: The following example sets the TCP SYN protection feature to block TCP SYN attack on ports in case an attack is identified from these ports.

```
switchxxxxxx(config)# security-suite syn protection mode block
```

security-suite syn protection recovery

To set the time period for the SYN Protection feature to block an attacked interface, use the **security-suite syn protection period** Global Configuration mode command.

To set the time period to its default value, use the **no** form of this command.

Syntax

security-suite syn protection recovery timeout

no security-suite syn protection recovery

Parameters

timeout—Defines the timeout (in seconds) by which an interface from which SYN packets are blocked gets unblocked. Note that if a SYN attack is still active on this interface it might become blocked again. (Range: 10-600)

Default Configuration

The default timeout is 60 seconds.

Command Mode

Global Configuration mode

User Guidelines

If the timeout is modified, the new value will be used only on interfaces which are not currently under attack.

Example

The following example sets the TCP SYN period to 100 seconds.

```
switchxxxxxx(config)# security-suite syn protection recovery 100
```

security-suite syn protection threshold

To set the threshold for the SYN protection feature, use the **security-suite syn protection threshold** Global Configuration mode command.

To set the threshold to its default value, use the **no** form of this command.

Syntax

security-suite syn protection threshold syn-packet-rate

no security-suite syn protection threshold

Parameters

syn-packet-rate—defines the rate (number of packets per second) from each specific port that triggers identification of TCP SYN attack. (Range: 20-200)

Default Configuration

The default threshold is 80pps (packets per second).

Command Mode

Global Configuration mode

Example

The following example sets the TCP SYN protection threshold to 40 pps.

```
switchxxxxxx(config)# security-suite syn protection threshold 40
```

show security-suite configuration

To display the security-suite configuration, use the **show security-suite configuration** switchxxxxxx> command.

Syntax

show security-suite configuration

Command Mode

User EXEC mode

Example

The following example displays the security-suite configuration.

```
switchxxxxxx# show security-suite configuration
Security suite is enabled (Per interface rules are enabled).
Denial Of Service Protect: stacheldraht, invasor-trojan, back-office-trojan.
Denial Of Service SYN-FIN Attack is enabled
Denial Of Service SYN Attack

Interface                IP Address               SYN Rate (pps)
-----------------        --------------           --------------
gi1/0/1                  176.16.23.0\24           100

Martian addresses filtering
Reserved addresses: enabled.
Configured addresses: 10.0.0.0/8, 192.168.0.0/16
SYN filtering

Interface                IP Address               TCP port
-----------------        --------------           --------------
gi1/0/2                  176.16.23.0\24           FTP

ICMP filtering

Interface                IP Address
---------------          --------------
gi1/0/2                  176.16.23.0\24

Fragmented packets filtering

Interface                IP Address
--------------           --------------
gi1/0/2                  176.16.23.0\24
```

show security-suite syn protection

To display the SYN Protection feature configuration and the operational status per interface-id, including the time of the last attack per interface, use the **show security-suite syn protection** switchxxxxxx> command.

Syntax

show security-suite syn protection [interface-id]

Parameters

interface-id—(Optional) Specifies an interface-ID. The interface-ID can be one of the following types: Ethernet port of Port-Channel.

Command Mode

User EXEC mode

User Guidelines

Use the Interface-ID to display information on a specific interface.

Example

The following example displays the TCP SYN protection feature configuration and current status on all interfaces. In this example, port gi1/0/2 is attacked but since there is a user-ACL on this port, it cannot become blocked so its status is Reported and not Blocked and Reported.

```
switchxxxxxx# show security-suite syn protection
Protection Mode: Block
Threshold: 40 Packets Per Second
Period: 100 Seconds
```

Interface Name	Current Status	Last Attack
gi1/0/1	Attacked	19:58:22.289 PDT Feb 19 2012 Blocked and Reported
gi1/0/2	Attacked	19:58:22.289 PDT Feb 19 2012 Reported
gi1/0/3	Attacked	19:58:22.289 PDT Feb 19 2012 Blocked and Reported