

Traffic Protection Commands

This module describes the commands used to configure traffic protection.

Note All commands applicable for the Cisco NCS 5500 Series Router are also supported on the Cisco NCS 540 Series Router that is introduced from Cisco IOS XR Release 6.3.2. References to earlier releases in Command History tables apply to only the Cisco NCS 5500 Series Router.

Note

- Starting with Cisco IOS XR Release 6.6.25, all commands applicable for the Cisco NCS 5500 Series Router are also supported on the Cisco NCS 560 Series Routers.
- Starting with Cisco IOS XR Release 6.3.2, all commands applicable for the Cisco NCS 5500 Series Router are also supported on the Cisco NCS 540 Series Router.
- References to releases before Cisco IOS XR Release 6.3.2 apply to only the Cisco NCS 5500 Series Router.
- Cisco IOS XR Software Release 7.0.1 specific updates are not applicable for the following variants of Cisco NCS 540 Series Routers:
  - N540-28Z4C-SYS-A
  - N540-28Z4C-SYS-D
  - N540X-16Z4G8Q2C-A
  - N540X-16Z4G8Q2C-D
  - N540X-16Z8Q2C-D
  - N540-12Z20G-SYS-A
  - N540-12Z20G-SYS-D
  - N540X-12Z16G-SYS-A
  - N540X-12Z16G-SYS-D

For detailed information about traffic protection concepts, configuration tasks, and examples, see the *Traffic Protection for Third-Party Applications* chapter in the *System Security Configuration Guide for Cisco NCS 5500 Series Routers*.

- allow, on page 3
- tpa, on page 5

allow

To configure a local port and third-party application protocols for traffic protection, use the **allow** command in protection mode. To disallow a protocol on an interface, use the **no**form of this command.

allow protocol {**tcp** | **udp**}**local-port** *port-number* [**interface** *interface-name* | **local-address** *local IP address* | **remote-address***remote IP address*

no allow protocol {**tcp** | **udp**}**local-port** *port-number* [**interface** *interface-name* | **local-address** *local IP address* | **remote-address***remote IP address*

Syntax Description

protocol	Specifies the L4 protocol to be configured for traffic protection. The supported protocols are TCP and UDP.
local-port	Specifies local L4 port.
Port-number	Specifies a port number in the range of 1 to 65535.
interface	Specifies the interface on which the protocol has to be configured.
local-address	Specifies the local IP address of the host or client.
remote-address	Specifies the remote IP address of the host or client.

Command Default

Not Applicable

Command Modes

Protection

Command History

Release	Modification
Release 6.5.2	This command was introduced.

Usage Guidelines

If no allow command is used for a given local port and protocol, then by default, any ingress traffic is delivered to Third Party Applications. If one or more allow entries are added, only the ingress traffic matching an allow entry is delivered for that protocol and port. It is possible to configure multiple allow entries for the same protocol and port, for example, to allow traffic from multiple remote addresses.

Note If multiple allow entries are configured for the same protocol and port, the entries are expected to be non-overlapping. If overlapping entries are present, for example, multiple remote addresses in overlapping subnets, then the behaviour is platform-dependent.

Task ID

Task ID	Operation
system	read, write

Example

The following example shows how to configure a local port and third-party application protocols for traffic protection:

```
Router# configure
Router(config)# tpa
Router(config-tpa)# vrf default
Router(config-tpa-vrf)# address-family ipv4
Router(config-tpa-vrf-afi)# protection
Router(config-tpa-vrf-afi-prot)# allow protocol tcp local-port 6 remote-address 192.0.2.3
interface MgmtEth0 local-address 192.0.2.125
```

tpa

To configure a third-party application protocol for traffic protection, use the **tpa**command in global configuration mode. To disable all configurations that are related to the third-party application, use the **no**form of this command.

tpa vrf *vrf-name* **address-family** [**ipv4** | **ipv6**] **update-source dataports** { **bvi** *bviname* | **Bundle-Ether** *bundleetherval* | **Bundle-POS** *bundlePosvalue* | **EightHundredGigE** *eighthundredGigEifname* | **FiftyGigE** *fiftygigEifname* | **FortyGigE** *fortyGigEifname* | **FourHundredGigE** *fourHundredGigEifname* | **GigabitEthernet** *gigabitEthernetifname* | **HundredGigE** *hundredGigEifname* | **Loopback** *loopbackval* | **MgmtEth** *mgmtEthifname* | **Multilink** *multilinkifname* | **Null 0 SRP** *srpifname* | **Serial** *serialifname* | **TenGigE** *tenGigEifname* | **TwentyFiveGigE** *twentyFiveGigEifname* | **TwoHundredGigE** *twoHundredGigEifname* | **active-management lpts 0 | nve** *nvevalue* | **tunnel-ip** *tunnelipvalue* | **tunnel-ipsec** *tunnel-ipsecvalue* } | **protection**

no tpa vrf *vrf-name* **address-family** [**ipv4** | **ipv6**] **protection**

Syntax Description

vrf	Configures a VPN routing and forwarding (VRF) reference.
address-family	Enables support for various address family configuration modes while configuring TPA.
ipv4	Specifies IPv4 address prefixes.
ipv6	Specifies IPv6 address prefixes.
protection	Enters the Traffic Protection submode.
update-source dataports	Specifies the command to define the potential sources for the data ports.
BVI	A vrtual bridge group interface that allows Layer 2 and Layer 3 connectivity.
Bundle-Ether	A group of Ethernet interfaces combined to act as a single logical interface for increased bandwidth and redundancy. Its value ranges 1–65535.
Bundle-POS	A logical interface that is created by bundling multiple Packets over SONET/SDH interfaces for improved performance. Its value ranges 1–65535.
EightHundredGigE	Ethernet interfaces supporting 800 Gbps. It must be specified in Rack/Slot/Instance/Port/Breakout format or R/S/I/P format.
FiftyGigE	Ethernet interfaces supporting 50 Gbps. It must be specified in Rack/Slot/Instance/Port/Breakout format or R/S/I/P format.
FortyGigE	Ethernet interfaces supporting 40 Gbps. It must be specified in Rack/Slot/Instance/Port/Breakout format or R/S/I/P format.
FourHundredGigE	Ethernet interfaces supporting 400 Gbps. It must be specified in Rack/Slot/Instance/Port or R/S/I/P format.

GigabitEthernet	Ethernet interfaces supporting 1 Gbps. It must be specified in Rack/Slot/Instance/Port or R/S/I/P format.
HundredGigE	Ethernet interfaces supporting 100 Gbps. It must be specified in Rack/Slot/Instance/Port or R/S/I/P format.
Loopback	A virtual interface that is primarily used for network testing and management. Its value ranges 0–2147483647.
MgmtEth	Managements Ethernet interface used for device management tasks.
Multilink	Combines multiple network links into a single logical link for increased throughput.
Null 0	A virtual interface that discards all incoming traffic, often used for testing.
SRP	Interfaces used for Spatial Reuse Protocol, which enhances bandwidth utilization.
Serial	Interfaces used for serial communication over network connections.
TenGigE	serial interface that support 10-Gbps Ethernet connections. It must be specified in Rack/Slot/Instance/Port or R/S/I/P format.
TwentyFiveGigE	Ethernet interfaces supporting 25 Gbps. It must be specified in Rack/Slot/Instance/Port or R/S/I/P format.
TwoHundredGigE	Ethernet interfaces supporting 200 Gbps. It must be specified in Rack/Slot/Instance/Port or R/S/I/P format.
active-management	Utilizes the management port on the Active Route Processor (RP) for managing network devices.
lpts 0	Low-priority traffic management.
nve	Network virtualization endpoints, facilitating network overlays. Its value ranges 0–65535.
tunnel-ip	Interfaces supporting Generic Routing Encapsulation (GRE) or IP-in-IP tunneling protocols for encapsulating packets. Its value ranges 0–131070.
tunnel-ipsec	Interfaces used for creating secure IPsec tunnels for encrypted communication. Its value ranges 0–4294967295.

Command Default

Not Applicable

Command Modes

Global configuration

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

Some platforms do not support non-management traffic in any VRFs apart from default VRF.

Example

This example shows how to configure a third-party application protocol for traffic protection.

```
Router# configure
Router(config)# tpa
Router(config-tpa)# vrf vrf-name
Router(config-tpa-vrf)# address-family [ipv4 | ipv6]
Router(config-tpa-vrf-afi)# protection
```

This example shows how to configure the updating of source data ports for a third-party application using the **TwoHundredGig** cli.

```
Router(config)# tpa
Router(config-tpa)#vrf green
Router(config-tpa-vrf)# address-family ipv4
Router(config-tpa-vrf-afi)# update-source dataports TwoHundredGigE 0/0/0/12
```

This example shows how to configure the updating of source data ports for a third-party application using the **active-management** cli.

```
Router(config)# tpa
Router(config-tpa)#vrf green
Router(config-tpa-vrf)# address-family ipv4
Router(config-tpa-vrf-afi)# update-source dataports active-management
/*Utilizes the management port on the Active Route Processor (RP) for managing network
devices.*/
```