D Commands

This chapter describes the Cisco NX-OS TrustSec commands that begin with D.

deny

To configure a deny action in the security group access control list (SGACL), use the **deny** command. To remove the action, use the **no** form of this command.

deny {**all** | **icmp** | **igmp** | **ip** | {{**tcp** | **udp**} [{**dest** | **dst** | **src**} {{**eq** | **gt** | **lt** | **neq**} *port-number*} | **range** *port-number1 port-number2*}]} [**log**]

no deny {**all** | **icmp** | **igmp** | **ip** | {{**tcp** | **udp**} [{**dest** | **dst** | **src**} {{**eq** | **gt** | **lt** | **neq**} *port-number*} | **range** *port-number1 port-number2*}]} [**log**]

Syntax Description

all	Specifies all traffic.
icmp	Specifies Internet Control Message Protocol (ICMP) traffic.
igmp	Specifies Internet Group Management Protocol (IGMP) traffic.
ip	Specifies IP traffic.
tcp	Specifies TCP traffic.
udp	Specifies User Datagram Protocol (UDP) traffic.
dest	Specifies the destination port number.
dst	Specifies the destination port number.
src	Specifies the source port number.
eq	Specifies equal to the port number.
gt	Specifies greater than the port number.
lt	Specifies less than the port number.
neq	Specifies not equal to the port number.
port-number	Port number for TCP or UDP. The range is from 0 to 65535.
range	Specifies a port range for TCP or UDP.
port-number1	First port in the range. The range is from 0 to 65535.
port-number2	Last port in the range. The range is from 0 to 65535.
log	(Optional) Specifies that packets matching this configuration be logged.

Command Default

None

Command Modes

role-based access control list (RBACL)

Command History

Release	Modification
5.2(1)N1(1)	This command was introduced.

Usage Guidelines

To use this command, you must first enable the 802.1X feature by using the **feature dot1x** command and then enable the Cisco TrustSec feature using the **feature cts** command.

To enable RBACL logging, you must enable RBACL policy enforcement on the VLAN. You must also enable Cisco TrustSec counters using the **cts role-based counters enable** command.

This command does not require a license.

Examples

This example shows how to add a deny action to an SGACL and enable RBACL logging:

```
switch# configure terminal
switch(config)# cts role-based access-list MySGACL
switch(config-rbacl)# deny icmp log
switch(config-rbacl)#
```

This example shows how to remove a deny action from an SGACL:

```
switch# configure terminal
switch(config)# cts role-based access-list MySGACL
switch(config-rbacl)# no deny icmp log
switch(config-rbacl)#
```

Related Commands

Command	Description
cts role-based access-list	Configures Cisco TrustSec SGACLs.
cts role-based counters	Enables RBACL counters.
feature cts	Enables the Cisco TrustSec feature.
feature dot1x	Enables the 802.1X feature on the switch.
permit	Configures permit actions in an SGACL.
show cts role-based access-list	Displays the Cisco TrustSec SGACL configuration.