P Commands

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

permit

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

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

no permit {**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.

Defaults

None

Command Modes

role-based access control list (RBACL)

Command History

Release	Modification
5.1(3)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 permit action to an SGACL and enable RBACL logging:

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

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

```
switch# configure terminal
switch(config)# cts role-based access-list MySGACL
switch(config-rbacl)# no permit 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.
deny	Configures deny actions in an SGACL.
feature cts	Enables the Cisco TrustSec feature.
feature dot1x	Enables the 802.1X feature on the switch.
show cts role-based access-list	Displays the Cisco TrustSec SGACL configuration.

policy

To manually configure a Cisco TrustSec authentication policy on an interface with either a Cisco TrustSec device identifier or security group tag (SGT), use the **policy** command. To revert to the default, use the **no** form of this command.

policy {**dynamic identity** *device-id* | **static sgt** *sgt-value* [**trusted**]}

no policy {**dynamic** | **static**}

Syntax Description

dynamic identity	Specifies a dynamic policy using a Cisco TrustSec device identifier.
device-id	Cisco TrustSec device identifier. The device identifier is case sensitive.
static sgt	Specifies a static policy using an SGT.
sgt-value	Cisco TrustSec SGT. The format is **0x***hhhh*. The range is 0x2 to 0xffef.
trusted	(Optional) Specifies that traffic coming on the interface with the SGT should not have its tag overridden.

Command Default

None

Command Modes

Cisco TrustSec manual configuration mode

Command History

Release	Modification
5.1(3)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.

After using this command, you must enable and disable the interface using the **shutdown** and **no shutdown** command sequence for the configuration to take effect.

This command does not require a license.

Examples

This example shows how to manually configure a dynamic Cisco TrustSec policy on an interface:

```
switch# configure terminal
switch(config)# interface ethernet 2/3
switch(config-if)# cts manual
switch(config-if-cts-manual)# policy dynamic identity DeviceB
switch(config-if-cts-manual)# exit
switch(config-if)# shutdown
switch(config-if)# no shutdown
switch(config-if)#
```

This example shows how to remove a manually configured dynamic Cisco TrustSec policy from an interface:

```
switch# configure terminal
switch(config)# interface ethernet 2/3
switch(config-if)# cts manual
switch(config-if-cts-manual)# no policy dynamic
switch(config-if-cts-manual)# exit
switch(config-if)# shutdown
switch(config-if)# no shutdown
switch(config-if)#
```

This example shows how to manually configure a static Cisco TrustSec policy on an interface:

```
switch# configure terminal
switch(config)# interface ethernet 2/4
switch(config-if)# cts manual
switch(config-if-cts-manual)# policy static sgt 0x100
switch(config-if-cts-manual)# exit
switch(config-if)# shutdown
switch(config-if)# no shutdown
switch(config-if)#
```

This example shows how to remove a manually configured static Cisco TrustSec policy on an interface:

```
switch# configure terminal
switch(config)# interface ethernet 2/4
switch(config-if)# cts manual
switch(config-if-cts-manual)# no policy static
switch(config-if-cts-manual)# exit
switch(config-if)# shutdown
switch(config-if)# no shutdown
switch(config-if)#
```

Related Commands

Command	Description
cts manual	Enters Cisco TrustSec manual configuration mode for an interface.
feature cts	Enables the Cisco TrustSec feature.
feature dot1x	Enables the 802.1X feature on the switch.
show cts interface	Displays the Cisco TrustSec configuration for interfaces.

propagate-sgt

To enable security group tag (SGT) propagation on Layer 2 Cisco TrustSec interfaces, use the **propagate-sgt** command. To disable SGT propagation, use the **no** form of this command.

propagate-sgt

no propagate-sgt

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled if manual configuration is enabled on the interface.

Disabled if manual configuration is disabled on the interface.

Command Modes

Global configuration mode

Command History

Release	Modification
5.1(3)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.

You can disable the SGT propagation feature on an interface if the peer device connected to the interface can not handle Cisco TrustSec packets tagged with an SGT.

After using this command, you must enable and disable the interface using the **shutdown** and **no shutdown** command sequence for the configuration to take effect.

This command does not require a license.

Examples

This example shows how to disable SGT propagation:

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# cts manual
switch(config-if-cts-manual)# no propagate-sgt
switch(config-if-cts-manual)# exit
switch(config-if)# shutdown
switch(config-if)# no shutdown
switch(config-if)#
```

This example shows how to enable SGT propagation:

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# cts manual
switch(config-if-cts-manual)# propagate-sgt
switch(config-if-cts-manual)# exit
```

```
switch(config-if)# shutdown
switch(config-if)# no shutdown
switch(config-if)#
```

Related Commands

Command	Description
cts manual	Enables Cisco TrustSec manual configuration on an interface.
feature cts	Enables the Cisco TrustSec feature.
feature dot1x	Enables the 802.1X feature on the switch.
show cts interface	Displays the Cisco TrustSec configuration for interfaces.