H Commands

This chapter describes the Cisco NX-OS security commands that begin with H.

hardware access-list capture

To enable access control list (ACL) capture on all virtual device contexts (VDCs), use the **hardware access-list capture** command. To disable ACL capture, use the **no** form of the command.

hardware access-list capture

no hardware access-list capture

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
5.2(1)	This command was introduced.

Usage Guidelines

Only M1 Series modules not support ACL capture.

ACL capture is a hardware-assisted feature and is not supported for the management interface or for control packets originating in the supervisor. It is also not supported for software ACLs such as SNMP community ACLs and virtual teletype (VTY) ACLs.

Enabling ACL capture disables ACL logging for all VDCs and the rate limiter for ACL logging.

Only one ACL capture session can be active at any given time in the system across VDCs.

This command does not require a license.

Examples

This example shows how to enable ACL capture on all VDCs:

```
switch# configure terminal
switch(config)# hardware access-list capture
```

This example shows how to disable ACL capture on all VDCs:

```
switch # configure terminal
switch(config)# no hardware access-list capture
```

Related Commands

Command	Description
show hardware access-list status module	Displays the access control list (ACL) capture configuration.

hardware access-list resource pooling

To allow ACL-based features to use more than one TCAM bank on one or more I/O modules, use the **hardware access-list resource pooling** command. To restrict ACL-based features to using one TCAM bank on an I/O module, use the **no** form of this command.

hardware access-list resource pooling module *slot-number-list*

no hardware access-list resource pooling module *slot-number-list*

Syntax Description

module *slot-number-list*	Specifies the I/O module(s). The *slot-number-list* argument allows you to specify modules by the slot number that they occupy. You can specify a single I/O module, a range of slot numbers, or comma-separated slot numbers and ranges.

Defaults

None

Command Modes

Global configuration

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
4.2(1)	The hyphen was removed between the **resource** and **pooling** keywords.
4.1(2)	This command was introduced.

Usage Guidelines

By default, each ACL-based feature can use one TCAM bank on an I/O module. This default behavior limits each feature to 16,000 TCAM entries. If you have very large security ACLs, you may encounter this limit. The **hardware access-list resource pooling** command allows you to make more than 16,000 TCAM entries available to ACL-based features.

This command does not require a license.

Examples

This example shows how to enable ACL programming across TCAM banks on the I/O module in slot 1:

```
switch# config t
switch(config)# hardware access-list resource pooling module 1
```

Related Commands

Command	Description
hardware access-list update	Configures how a supervisor module updates an I/O module with changes to an ACL.
show running-config all	Displays the running configuration, including the default configuration.

hardware access-list update

To configure how a supervisor module updates an I/O module with changes to an access-control list (ACL), use the **hardware access-list update** command in the default virtual device context (VDC). To disable atomic updates, use the **no** form of this command.

hardware access-list update {**atomic** | **default-result permit**}

no hardware access-list update {**atomic** | **default-result permit**}

Syntax Description

atomic	Specifies that the device performs atomic updates, which do not disrupt traffic during the update. By default, a Cisco Nexus 7000 Series device performs atomic ACL updates.
default-result permit	Specifies that, during non-atomic updates, the device permits traffic that the updated ACL applies to.

Defaults

atomic

Command Modes

Global configuration

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
4.1(4)	This command is available only in the default VDC.
4.1(2)	This command was introduced to replace the **platform access-list update** command.

Usage Guidelines

In Cisco NX-OS Release 4.1(4) and later releases, the **hardware access-list update** command is available in the default VDC only and affects all VDCs.

By default, when a supervisor module of a Cisco Nexus 7000 Series device updates an I/O module with changes to an ACL, it performs an atomic ACL update. An atomic update does not disrupt traffic that the updated ACL applies to; however, an atomic update requires that an I/O module that receives an ACL update has enough available resources to store each updated ACL entry in addition to all preexisting entries in the affected ACL. After the update occurs, the additional resources used for the update are freed. If the I/O module lacks the required resources, the device generates an error message and the ACL update to the I/O module fails.

If an I/O module lacks the resources required for an atomic update, you can disable atomic updates by using the **no hardware access-list update atomic** command in the default VDC; however, during the brief time required for the device to remove the preexisting ACL and implement the updated ACL, traffic that the ACL applies to is dropped by default.

If you want to permit all traffic that an ACL applies to while it receives a nonatomic update, use the **hardware access-list update default-result permit** command in the default VDC.

This command does not require a license.

Examples

Note In Cisco NX-OS Release 4.1(4) and later releases, the **hardware access-list update** command is available in the default VDC only. To verify that the current VDC is the VDC 1 (the default VDC), use the **show vdc current-vdc** command.

This example shows how to disable atomic ACL updates:

```
switch# config t
switch(config)# no hardware access-list update atomic
```

This example shows how to permit affected traffic during a nonatomic ACL update:

```
switch# config t
switch(config)# hardware access-list update default-result permit
```

This example shows how to revert to the atomic update method:

```
switch# config t
switch(config)# no hardware access-list update default-result permit
switch(config)# hardware access-list update atomic
```

Related Commands

Command	Description
hardware access-list resource pooling	Allows ACL-based features to use more than one TCAM bank.
show running-config all	Displays the running configuration, including the default configuration.

hardware rate-limiter

To configure rate limits in packets per second on supervisor-bound traffic, use the **hardware rate-limiter** command. To revert to the default, use the **no** form of this command.

hardware rate-limiter {**access-list-log** {*packets* | **disable**} [**module** *module* [**port** *start end*]] | **copy** {*packets* | **disable**} [**module** *module* [**port** *start end*]] | **f1** {**rl-1** {*packets* | **disable**} [**module** *module* [**port** *start end*]] | **rl-2** {*packets* | **disable**} [**module** *module* [**port** *start end*]] | **rl-3** {*packets* | **disable**} [**module** *module* [**port** *start end*]] | **rl-4** {*packets* | **disable**} [**module** *module* [**port** *start end*]] | **rl-5** {*packets* | **disable**} [**module** *module* [**port** *start end*]]} | **layer-2** {**l2pt** {*packets* | **disable**} [**module** *module* [**port** *start end*]] | **mcast-snooping** {*packets* | **disable**} [**module** *module* [**port** *start end*]] | **port-security** {*packets* | **disable**} [**module** *module* [**port** *start end*]] | **storm-control** {*packets* | **disable**} [**module** *module* [**port** *start end*]] | **vpc-low** {*packets* | **disable**} [**module** *module* [**port** *start end*]]} | **layer-3** {**control**{*packets* | **disable**} [**module** *module* [**port** *start end*]] | **glean** {*packets* | **disable**} [**module** *module* [**port** *start end*]] | **mtu** {*packets* | **disable**} [**module** *module* [**port** *start end*]] | **multicast** {*packets* | **disable**} [**module** *module* [**port** *start end*]] | **ttl** {*packets* | **disable**} [**module** *module* [**port** *start end*]]} | **receive** {*packets* | **disable**} [**module** *module* [**port** *start end*]]

no hardware rate-limiter {**access-list-log** {*packets* | **disable**} [**module** *module* [**port** *start end*]] | **copy** {*packets* | **disable**} [**module** *module* [**port** *start end*]] | **f1** {**rl-1** {*packets* | **disable**} [**module** *module* [**port** *start end*]] | **rl-2** {*packets* | **disable**} [**module** *module* [**port** *start end*]] | **rl-3** {*packets* | **disable**} [**module** *module* [**port** *start end*]] | **rl-4** {*packets* | **disable**} [**module** *module* [**port** *start end*]] | **rl-5** {*packets* | **disable**} [**module** *module* [**port** *start end*]]} | **layer-2** {**l2pt** {*packets* | **disable**} [**module** *module* [**port** *start end*]] | **mcast-snooping** {*packets* | **disable**} [**module** *module* [**port** *start end*]] | **port-security** {*packets* | **disable**} [**module** *module* [**port** *start end*]] | **storm-control** {*packets* | **disable**} [**module** *module* [**port** *start end*]] | **vpc-low** {*packets* | **disable**} [**module** *module* [**port** *start end*]]} | **layer-3** {**control**{*packets* | **disable**} [**module** *module* [**port** *start end*]] | **glean** {*packets* | **disable**} [**module** *module* [**port** *start end*]] | **mtu** {*packets* | **disable**} [**module** *module* [**port** *start end*]] | **multicast** {*packets* | **disable**} [**module** *module* [**port** *start end*]] | **ttl** {*packets* | **disable**} [**module** *module* [**port** *start end*]]} | **receive** {*packets* | **disable**} [**module** *module* [**port** *start end*]]

Syntax Description

access-list-log	Specifies packets copied to the supervisor module for access list logging. The default rate is 100 packets per second.
disable	Disables the hardware rate limiter.
module *module*	(Optional) Specifies a module number. The range is from 1 to 18.
port *start end*	(Optional) Specifies a port start index. The range is from 1 to 32. You specify the start port and and end port with a space in between them.
copy	Specifies data and control packets copied to the supervisor module. The default rate is 30000 packets per second.
f1	Specifies the control packets from the F1 modules to the supervisor.
rl-1	Specifies the F1 rate-limiter 1.
rl-2	Specifies the F1 rate-limiter 2.
rl-3	Specifies the F1 rate-limiter 3.
rl-4	Specifies the F1 rate-limiter 4.
rl-5	Specifies the F1 rate-limiter 5.
layer-2	Specifies Layer 2 packet rate limits.

l2pt	Specifies Layer 2 Tunnel Protocol (L2TP) packets. The default rate is 4096 packets per second.
mcast-snooping	Specifies Layer 2 multicast-snooping packets. The default rate is 10000 packets per second.
port-security	Specifies port security packets. The default is disabled.
storm-control	Specifies broadcast, multicast, and unknown unicast storm-control packets. The default is disabled.
vpc-low	Specifies Layer 2 control packets over the VPC low queue. It synchronizes control-plane communication between VPC peer switches that are of a lower priority and protects the control plane when a vPC peer switch misbehaves or excessive traffic occurs between the two. The default rate is 4000 packets per second.
layer-3	Specifies Layer 3 packet rate limits.
control	Specifies Layer-3 control packets. The default rate is 10000 packets per second.
glean	Specifies Layer-3 glean packets. The default rate is 100 packets per second.
mtu	Specifies Layer-3 MTU failure redirected packets. The default rate is 500 packets per second.
multicast	Specifies Layer-3 multicast packets per second.
ttl	Specifies Layer-3 failed time-to-live redirected packets. The default rate is 500 packets per second.
receive	Specifies packets redirected to the supervisor module. The default rate is 30000 packets per second.
packets	Number of packets per second. The range is from 1 to 33554431.

Defaults

See the Syntax Description for the default rate limits.

Default rate limits for the F1 Series modules:

RL-1: 4500 packets per second

RL-2: 1000 packets per second

RL-3: 1000 packets per second

RL-4: 100 packets per second

RL-5: 1500 packets per second

Command Modes

Global configuration

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
5.1(1)	Added the **f1**, **rl-1**, **rl-2**, **rl-3**, **rl-4**, and **rl-5** keywords. Also, added the following keywords: **module**, **disable**, and **port**.
5.0(2)	Added the **l2pt** keyword.
4.1(2)	This command was introduced to replace the **platform rate-limit** command.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to configure a rate limit for control packets:

```
switch# config t
switch(config)# hardware rate-limiter layer-3 control 20000
```

This example shows how to revert to the default rate limit for control packets:

```
switch# config t
switch(config)# no hardware rate-limiter layer-3 control
```

Related Commands

Command	Description
clear hardware rate-limiter	Clears rate-limit statistics.
show hardware rate-limiter	Displays rate-limit information.
show running-config	Displays the running configuration.

host (IPv4)

To specify a host or a subnet as a member of an IPv4-address object group, use the **host** command. To remove a group member from an IPv4-address object group, use the **no** form of this command.

[*sequence-number*] **host** *IPv4-address*

no {*sequence-number* | **host** *IPv4-address*}

[*sequence-number*] *IPv4-address network-wildcard*

no *IPv4-address network-wildcard*

[*sequence-number*] *IPv4-address/prefix-len*

no *IPv4-address/prefix-len*

Syntax Description

sequence-number	(Optional) Sequence number for this group member. Sequence numbers maintain the order of group members within an object group. Valid sequence numbers are from 1 to 4294967295. If you do not specify a sequence number, the device assigns a number that is 10 greater than the largest sequence number in the current object group.
host *IPv4-address*	Specifies that the group member is a single IPv4 address. Enter *IPv4-address* in dotted-decimal format.
IPv4-address network-wildcard	IPv4 address and network wildcard. Enter *IPv4-address* and *network-wildcard* in dotted-decimal format. Use *network-wildcard* to specify which bits of *IPv4-address* are the network portion of the address, as follows: `switch(config-ipaddr-ogroup)# 10.23.176.0 0.0.0.255` A *network-wildcard* value of 0.0.0.0 indicates that the group member is a specific IPv4 address.
IPv4-address/prefix-len	IPv4 address and variable-length subnet mask. Enter *IPv4-address* in dotted-decimal format. Use *prefix-len* to specify how many bits of *IPv4-address* are the network portion of the address, as follows: `switch(config-ipaddr-ogroup)# 10.23.176.0/24` A *prefix-len* value of 32 indicates that the group member is a specific IP address.

Defaults

None

Command Modes

IPv4 address object group configuration

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

To specify a subnet as a group member, use either of the following forms of this command:

[*sequence-number*] *IPv4-address network-wildcard*

[*sequence-number*] *IPv4-address*/*prefix-len*

Regardless of the command form that you use to specify a subnet, the device shows the *IP-address*/*prefix-len* form of the group member when you use the **show object-group** command.

To specify a single IPv4 address as a group member, use any of the following forms of this command:

[*sequence-number*] **host** *IPv4-address*

[*sequence-number*] *IPv4-address* **0.0.0.0**

[*sequence-number*] *IPv4-address*/**32**

Regardless of the command form that you use to specify a single IPv4 address, the device shows the **host** *IP-address* form of the group member when you use the **show object-group** command.

This command does not require a license.

Examples

This example shows how to configure an IPv4-address object group named ipv4-addr-group-13 with two group members that are specific IPv4 addresses and one group member that is the 10.23.176.0 subnet:

```
switch# config t
switch(config)# object-group ip address ipv4-addr-group-13
switch(config-ipaddr-ogroup)# host 10.121.57.102
switch(config-ipaddr-ogroup)# 10.121.57.234/32
switch(config-ipaddr-ogroup)# 10.23.176.0 0.0.0.255
switch(config-ipaddr-ogroup)# show object-group ipv4-addr-group-13
        10 host 10.121.57.102
        20 host 10.121.57.234
        30 10.23.176.0/24
switch(config-ipaddr-ogroup)#
```

Related Commands

Command	Description
object-group ip address	Configures an IPv4 address group.
show object-group	Displays object groups.

host (IPv6)

To specify a host or a subnet as a member of an IPv6-address object group, use the **host** command. To remove a group member from an IPv6-address object group, use the **no** form of this command.

[*sequence-number*] **host** *IPv6-address*

no {*sequence-number* | **host** *IPv6-address*}

[*sequence-number*] *IPv6-address*/*network-prefix*

no *IPv6-address*/*network-prefix*

Syntax Description

sequence-number	(Optional) Sequence number for this group member. Sequence numbers maintain the order of group members within an object group. Valid sequence numbers are from 1 to 4294967295. If you do not specify a sequence number, the device assigns a number that is 10 greater than the largest sequence number in the current object group.
host *IPv6-address*	Specifies that the group member is a single IPv6 address. Enter *IPv6-address* in colon-separated, hexadecimal format.
IPv6-address/*network-prefix*	IPv6 address and a variable-length subnet mask. Enter *IPv6-address* in colon-separated, hexadecimal format. Use *network-prefix* to specify how many bits of *IPv6-address* are the network portion of the address, as follows: `switch(config-ipv6addr-ogroup)# 2001:db8:0:3ab7::/96` A *network-prefix* value of 128 indicates that the group member is a specific IPv6 address.

Defaults

None

Command Modes

IPv6 address object group configuration

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

To specify a subnet as a group member, use the following form of this command:

[*sequence-number*] *IPv6-address*/*network-prefix*

To specify a single IP address as a group member, use any of the following forms of this command:

[*sequence-number*] **host** *IPv6-address*

[*sequence-number*] *IPv6-address*/**128**

Regardless of the command form that you use to specify a single IPv6 address, the device shows the **host** *IPv6-address* form of the group member when you use the **show object-group** command.

This command does not require a license.

Examples

This example shows how to configure an IPv6-address object group named ipv6-addr-group-A7 with two group members that are specific IPv6 addresses and one group member that is the 2001:db8:0:3ab7:: subnet:

```
switch# config t
switch(config)# object-group ipv6 address ipv6-addr-group-A7
switch(config-ipv6addr-ogroup)# host 2001:db8:0:3ab0::1
switch(config-ipv6addr-ogroup)# 2001:db8:0:3ab0::2/128
switch(config-ipv6addr-ogroup)# 2001:db8:0:3ab7::/96
switch(config-ipv6addr-ogroup)# show object-group ipv6-addr-group-A7
        10 host 2001:db8:0:3ab0::1
        20 host 2001:db8:0:3ab0::2
        30 2001:db8:0:3ab7::/96
switch(config-ipv6addr-ogroup)#
```

Related Commands

Command	Description
object-group ipv6 address	Configures an IPv6 address group.
show object-group	Displays object groups.