Command Reference BookMap

First Published: 2010-04-29

Last Modified: 2010-04-29

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

This is a command wrapper topic

This is a xref permit (IPv4), on page 2

permit (IPv4)

To create an IPv4 access control list(ACL) rule thta permits traffic matching its conditions, use the **permit**command. To remove a rule, use the **no** form of this command.

This is for test

CSCsy01403: Make sure there are no extra spaces in the syntax diagram block following

General Syntax:
[*sequence-number*]**permit** *protocol source destination QA Test: CSCsv22488 The following groupchose should appear with square brackets only* [{**dscp** *dscp* | **QA test CSCsz89741: check that a space appears after this** *precedence*}]
[*QA Test: CSCsx24477*] **This synblk must appear on a different line** *protocol source destination QA Test Sprint 9 CSCtc25038 and CSCsw43905 There should be a pipe separator between this sentence and this sentence. There should also be a single space before the pipe and after the pipe*
QA Test Sprint 9: Open this command in firefox and check that the fonts for the command syntax is the same size.
no deny *protocol* {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address*} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address*} [*operator* [*port-number*]][**dest-option-type** [{*doh-numberdoh-type*}]] [**dscp***value*] [**flow-label***value*] [**fragments**] [**log**] [**log-input**] [**mobility**] [**mobility-type**[{*mh-numbermh-type*}]] [**routing**] [**routing-type***routing-number*] [**sequence***value*] [**time-range***name*] [**undetermined-transport**]

Command Default

A Newly created IPv4 ACL contains no rules

If yo do not specify a sequence number, the device assigns to the rule a sequence number that is greater than 10 greater than the last rule in the ACL

Command Modes

IPv4 ACL configuration

Source and Destination

You can specify the *source*and *destination* arguments in one of several ways. In each rule, the method you use to specify one of these arguments does not affect how you specify the other. When you configure a rule, use the following methods to specify the *source* and *destination*arguments:

IP address group object—
You can use an IPv4 address group object to specify a source or destination argument. Use the **object-group ip address** command to create and change IPv4 address group objects. The syntax is as follows: QA: CSCsz86893. These sep elements after addrgroup should render with a space (2 spaces). This is outside of a syntaxdiagram.

addrgroup space *address-group-name*

The following example shows how to use an IPv4 address object group named lab-gateway-svrs to specify the destination argument:

```
switch(config-acl)# permit ip any addrgroup lab-gateway-svrs
```

Address and network wildcard
You can use an IPv4 address followed by a network wildcard to specify a host or a network as a source or destination. The syntax is as follows:*IPv4-addressnetwork-willdcard*

The following example shows how to specify the source argument with the IPv4 address and VLSM for the 192.168.67.0 subnet

```
switch(config-acl)#
```

ICMP Message Types

The icmp-message argument can be the ICMP message number, which is an integer from 0 to 255. It can also be one of the following keywords:

administratively-prohibited
Administratively-prohibited
alternate-address
Alternate-address

TCP Port Names

When you specify the protocol argument as tcp, the port argument can be a TCP port number, which is an integer from 0 to 65535. It can also be one of the following keywords:

bgp
Border Gateway Protocol
chargen
Character generator
cmd
Remote commands (rcmd,514)

create wwn-pool

To create a WWN (World Wide Name) pool, use the **create wwn-pool** command.

create wwn-pool *name*{**node-wwn-assignment** | **port-wwn-assignment**}

Syntax Description

name	WWN pool name. The range of valid values is 1 to 16.
node-wwn-assignment	Specifies world wide node name assignment.
port-wwn-assignment	Specifies world wide node port assignment.

Command Default

None

Command Modes

Organization (/org)

Command History

Release	Modification
1.0(1)	This command was introduced.

Usage Guidelines

Use this command to create a WWN pool with the specified name, and enters organization WWN pool mode.

A WWN pool can include only WWNNs or WWPNs in the 20:xx range. All other WWN ranges are reserved.

Examples

This example shows how to create a WWN pool:

```
switch-A# scope org org3
switch-A /org # create wwn-pool wwnp1 port-wwn-assignment
switch-A /org/wwn-pool* # commit-buffer
switch-A /org/wwn-pool #
```

create vsan-Sathish

QA Test Sprint 9 CSCta77961: Test that each Command appears in its own page. Karthik has changed it

To create a VSAN, use the **create vsan** command.

karthik included this after os patch

karthik has included this during sprint6-round1 build.

sprint-5 round1

sprint-5 round1 patch

create vsan *name id fcoe-vlan*

Syntax Description

name	VSAN name. The range of valid values is 1 to 16.
id	VSAN identification number. The range of valid values is 1 to 4093.
default-2	Specifies default 1.
fcoe-vlan	Fibre Channel over Ethernet VLAN. The range of valid values is 1 to 4093.
default-1	Specifies default 2.

Command Default

None

Command Modes

Fibre Channel uplink (/fc-uplink)

Switch (/fc-uplink/switch)

Command History

Release	Modification
1.0(1)	This command was introduced.

Usage Guidelines

Use this command to create a VSAN with the specified name, and enters organization VSAN mode.

You can create a named VSAN with IDs from 1 to 4093. VSANs configured on different FCoE VLANs cannot share the same ID.

Examples

This example shows how to create a VSAN:

```
switch-A# scope fc-uplink
switch-A /fc-uplink # create vsan vs2 6 10
switch-A /fc-uplink/vsan* # commit-buffer
switch-A /fc-uplink/vsan #
```

create vnic-egress-policy

To create a VNIC egress policy, use the **create vnic-egress-policy** command.

create vnic-egress-policy

This command has no arguments or keywords.

Command Default

None

Command Modes

Virtual NIC QoS (/org/vnic-qos)

Command History

Release	Modification
1.0(1)	This command was introduced.

Use this command to create a vNIC egress policy, and enter organization virtual NIC egress policy mode.

Examples

This example shows how to create a vNIC egress policy:

```
switch-A# scope org org3
switch-A /org # scope vnic-qos vnicq1
switch-A /org/vnic-qos # create vnic-egress-policy
switch-A /org/vnic-qos* # commit-buffer
switch-A /org/vnic-qos #
```

Profiling test

- This is for test

  This is for TESTING

-
-

Wrapper

create vnic

QA Test Sprint 9 CSCta77961: Test that each Command appears in its own page.

karthik added this to check wan bridge issue in sprint12

Syntax Description

name	VNIC template name. The range of valid values is 1 to 16.
fabric	Specifies the fabric switch identification number.
a	Specifies switch A.
a-b	Specifies redundant, with switch A as primary.
b	Specifies switch B.
b-a	Specifies redundant, with switch B as primary.
eth-if	Specifies a Ethernet interface.
eth-if	Ethernet interface name. The range of valid values is 1 to 16.

Command Default

None

Command Modes

Service profile (/org/service-profile)

Command History

Release	Modification
1.0(1)	This command was introduced.

Usage Guidelines

Use this command to create a vNIC with the specified name, and enters organization virtual NIC mode.

Examples

This example shows how to create a vNIC:

```
switch-A# scope org org3
switch-A /org # scope service-profile sp1
switch-A /org/service-profile # create vnic vnic110
switch-A /org/service-profile/vnic* # commit-buffer
switch-A /org/service-profile/vnic #
```

Related Commands

QA Test: CSCtd06182 Check that the shortdescriptions appear on the dfescription column below. Also click on the first cross chapter link and see that it works in html and pdf chapters

Command	Description
create vsan-Sathish, on page 5	This is short description for vsan command
create vnic-egress-policy, on page 6	This is short dfescription for create vnic-egress-policy command

Creating a Basic Access Control Policy

License: Any

Your access control policy must have a unique name and must specify a default action. At this point, the default action determines how the ASA FirePOWER module handles all unencrypted traffic; you will add other configurations that affect traffic flow later.

You can set the default policy action to block all traffic without further inspection, or to inspect traffic for intrusions, as shown in the following diagram.

Tip When you first create an access control policy, you cannot choose to trust traffic as the default action. If you want to trust all traffic by default, change the default action after you create the policy.

Use the **Access Control Policy** page (**Policies > Access Control**) to create new and manage existing access control policies.

Optionally, you can use and modify the initial system-provided policy named Default Trust All Traffic.

To create an access control policy:

Step 1 Select **Configuration** > **ASA FirePOWER Configuration** > **Policies** > **Access Control Policy**.

The **Access Control Policy** page appears.

Tip You can also copy an existing policy from this ASA FirePOWER module or import a policy from another ASA FirePOWER module. To copy a policy, click the **copy** icon. To import a policy, see .

Step 2 Give the policy a unique **Name** and, optionally, a **Description**.

You can use all printable characters, including spaces and special characters, except for the pound sign (#), a semi-colon (;), or either brace ({}). The name must include at least one non-space character.

Step 3 Specify the initial **Default Action**:

- **Block all traffic** creates a policy with the **Access Control: Block All Traffic** default action.
- **Intrusion Prevention** creates a policy with the **Intrusion Prevention: Balanced Security and Connectivity** default action.

For guidance on choosing an initial default action, as well as how to change it later, see .

Step 4 Click **Store ASA FirePOWER Changes**.

The access control policy editor appears. For information on configuring your new policy, see . Note that you must apply the policy for it to take effect; see .