Managing Access Control Lists

This chapter contains the following sections:

About Access Control Lists

Packet filtering allows you to limit network traffic and restrict network use by certain users or devices. Access control list (ACL), filters traffic as it passes through a switch and permit or deny packets crossing specified interfaces. An ACL is a sequential collection of permit and deny conditions that apply to packets. When a packet is received on an interface, the switch compares the fields in the packet against any applied ACLs to verify that the packet has the required permissions to be forwarded.

You can use ACLs to protect networks and specific hosts from unnecessary or unwanted traffic. For example, you could use ACLs to disallow HTTP traffic from a high-security network to the Internet. You could also use ACLs to allow HTTP traffic but only to specific sites, using the IP address of the site to identify it in an IP ACL.

In Cisco UCS Director, you can configure ACLs on the following Cisco network devices:

- Cisco Nexus 9300 and 9500 Series switches firewall
- Cisco IOS Devices

In Cisco UCS Director, you can configure context ACLs on the following Cisco network devices:

- Cisco ASA 5500 Series firewall
- Cisco Adaptive Security Virtual Appliance (ASAv)

Creating an ACL Entry

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the pod.

Step 3 Select the device for which you want to create an ACL.

Step 4 From the **More Actions** drop-down list, choose **Create ACL Entry**.

Step 5 In the **Create ACL Entry** screen, complete the following fields:

Name	Description
ACL Name field	The name of the ACL.
Type drop-down list	Choose one of the following as the ACL type: • **IP** • **MAC** • **IPV6**
Description field	The description of the ACL.
Per ACL Entry stats collection check box	Check the check box to collect the statistics details of the ACL entry.
Apply ACL to Interface check box	Check the check box to apply the ACL to an interface. The **Interface Name** field appears. Click **Select** and choose an interface to which you want to apply the ACL.
Copy Running configuration to Startup configuration check box	Check the check box to copy the running configuration to the startup configuration.

Step 6 Click **Submit**.

Configuring ACL

To create an ACL for a context, you can either use this procedure, or you can use the **Configure ACL** workflow task.

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the pod.

Step 3 Select the device for which you want to configure context ACL and click **View Details**.

Step 4 Click the **ACL** tab.

Step 5 Click **Configure ACL**.

Step 6 In the **Configure ACL** screen, complete the following fields:

Name	Description
ACL Name field	The name of the context ACL. This field is mandatory.
Interface Name drop-down list	Choose the interface name on which you want to configure the context ACL. This field is mandatory.
Permit check box	Check the check box to forward the packets.
InBound Traffic check box	Check the check box to apply the ACL to inbound packets on an interface.
Protocol drop-down list	Choose one of the following to filter by Application layer protocol: • **ip** • **tcp** • **udp** • **icmp** This field is mandatory.
Source IP Address/IPv6 Prefix field	The IP address of the source host name that you want to apply to the ACL so that the packets from host are permitted or denied as per ACL.
Source Net Mask field	The subnet mask of a source network that you want to apply to the ACL so that the packets from the network are permitted or denied as per ACL.
Source Port Range field	The range of ports that you want to apply to the ACL so that the packets from the port range are permitted or denied as per ACL.
Destination IP Address/IPv6 Prefix field	The IP address of the destination host name that you want to apply to the ACL so that the packets to the destination host are forwarded or denied as per ACL.

Name	Description
Destination Net Mask field	The subnet mask of a destination network that you want to apply to the ACL so that the packets to the network are permitted or denied as per ACL.
Destination Port Range field	The range of ports that you want to apply to the ACL so that the packets to the port range are permitted or denied as per ACL.
Copy Running configuration to Startup configuration check box	Check the check box to copy the running configuration to the startup configuration.

Step 7 Click **Submit**.
The ACL is created in the device. After it is created, an inventory collection process runs automatically, after which the ACL is listed in the **ACL** tab.

Adding a MAC ACL Rule or an IP ACL Rule

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the pod.

Step 3 Select the Cisco Nexus 1000 Series switch for HyperV.

Step 4 Click **ACL**.

Step 5 Choose the ACL entry for which you want to add a MAC or an IP ACL rule.
The actions appear according to the type of the ACL. When you choose MAC type ACL, the **Add MAC ACL Rule** and **Delete MAC ACL Rule** actions appear. When you choose IP type ACL, the **Add IP ACL Rule** and **Delete IP ACL Rule** actions appear.

Step 6 To add a MAC ACL rule, click **Add MAC ACL Rule** and complete the following fields:

Name	Description
ACL Name drop-down list	Displays the name of the ACL.
Action drop-down list	Choose **permit** or **deny** as the action for the MAC ACL rule.
Source Type field	Choose one of the following as the source type: • **any—**To permit or deny any source host or network. • **source MAC address—**To permit or deny packets from a specific source MAC address. In the **Source MAC address** and **Source Wildcard bits** fields, enter the MAC address and wildcard bits to specify the source host.

Name	Description
Destination Type field	Choose one of the following as the destination type: • **any—**To permit or deny any destination host or network. • **Destination MAC address—**To permit or deny packets to a specific destination MAC address. In the **Destination MAC address** and **Destination Wildcard bits** fields, enter the MAC address and wildcard bits to specify the destination host.
VLAN ID drop-down list	Choose a VLAN ID to which you to need to apply the ACL entry.
Copy Running configuration to Startup configuration check box	Check the check box to copy the running configuration to the startup configuration.

Step 7 To add an IP ACL rule, click **Add IP ACL Rule** and complete the following fields:

Name	Description
ACL Name drop-down list	Displays the name of the ACL.
Action drop-down list	Choose **permit** or **deny** as the action for the IP ACL rule.
Protocol drop-down list	Choose a protocol for communication.
Source Type field	Choose one of the following as the source type: • **any—**To permit or deny any source host or network. • **network prefix—**To specify the source network prefix. In the **Source Network Prefix** field, enter the source network prefix. • **network address—**To permit or deny packets from a specific source network address. In the **Source Network address** and **Source Wildcard Bits** fields, enter the source network address and wildcard bits to specify the source network address range. • **host—**To specify the source network prefix. In the **Source Host Address** field, enter the source host address.

Name	Description
Destination Type field	Choose one of the following as the destination type: • **any—**To permit or deny any source host or network. • **network prefix—**To specify the source network prefix. In the **Destination Network Prefix** field, enter the source network prefix. • **network address—**To permit or deny packets from a specific source network address. In the **Destination Network address** and **Destination Wildcard Bits** fields, enter the source network address and wildcard bits to specify the destination network address range. • **host—**To specify the source network prefix. In the **Destination Host Address** field, enter the destination host address.
Copy Running configuration to Startup configuration check box	Check the check box to copy the running configuration to the startup configuration.

Step 8 Click **Submit**.