Configuring FlexConnect ACLs

- FlexConnect Access Control Lists, on page 1
- Restrictions for FlexConnect Access Control Lists, on page 1
- Configuring FlexConnect Access Control Lists (GUI), on page 3
- Configuring FlexConnect Access Control Lists (CLI), on page 4
- Viewing and Debugging FlexConnect Access Control Lists (CLI), on page 6

FlexConnect Access Control Lists

An access control list (ACL) is a set of rules used to limit access to a particular interface (for example, if you want to restrict a wireless client from pinging the management interface of the controller). ACLs enable access control of network traffic. After ACLs are configured on the controller, you can apply them to the management interface, the AP-Manager interface, any of the dynamic interfaces, or a WLAN. ACLs enable you to control data traffic to and from wireless clients or to the controller CPU. You can configure ACLs on FlexConnect access points to enable effective usage and access control of locally switched data traffic on an access point.

The FlexConnect ACLs can be applied to VLAN interfaces on access points in both the Ingress and Egress mode.

Existing interfaces on an access point can be mapped to ACLs. The interfaces can be created by configuring a WLAN-VLAN mapping on a FlexConnect access point.

The FlexConnect ACLs can be applied to an access point's VLAN only if VLAN support is enabled on the FlexConnect access point.

Related Information

- To set up location authentication, see the FlexConnect chapter of the *Enterprise Mobility Design Guide*.
- Wireless BYOD for FlexConnect Deployment Guide

This section contains the following subsections:

Restrictions for FlexConnect Access Control Lists

- FlexConnect ACLs can be applied only to FlexConnect access points. The configurations applied are per AP and per VLAN.

- FlexConnect ACLs are supported on the native VLAN.

  Note FlexConnect ACLs are not supported on native VLAN when setting comes from FlexConnect Group.

- You can configure up to 512 ACLs on a Cisco Wireless Controller. Each rule has parameters that affect its action. When a packet matches all the parameters pertaining to a rule, the action set pertaining to that rule is applied to the packet.
  - You can define 64 IPv4 address based rules in each ACL.
- Non-FlexConnect ACLs that are configured on the controller cannot be applied to a FlexConnect AP.
- FlexConnect ACLs do not support direction per rule. Unlike normal ACLs, Flexconnect ACLs cannot be configured with a direction. An ACL as a whole needs to be applied to an interface as ingress or egress.
- ACLs in your network might have to be modified because Control and Provisioning of Wireless Access Points (CAPWAP) use ports that are different from the ones used by the Lightweight Access Point Protocol (LWAPP).
- All ACLs have an implicit *deny all rule* as the last rule. If a packet does not match any of the rules, it is dropped by the corresponding access point.
- ACLs mapping on the VLANs that are created on an AP using WLAN-VLAN mapping, should be performed on a per-AP basis only. VLANs can be created on a FlexConnect group for AAA override. These VLANs will not have any mapping for a WLAN.
- ACLs for VLANs that are created on a FlexConnect group should be mapped only on the FlexConnect group. If the same VLAN is present on the corresponding AP as well as the FlexConnect group, AP VLAN will take priority. This means that if no ACL is mapped on the AP, the VLAN will not have any ACL, even if the ACL is mapped to the VLAN on the FlexConnect group.
- Ensure the FlexConnect ACL and the regular ACL names are not the same while configuring a WLAN for FlexConnect local switching.
- AAA client ACL support:
  - Before the AAA sends the client ACL, ensure that the ACL is created on a FlexConnect group or an AP. The ACL is not downloaded to the AP dynamically when the client gets associated with the AP.
  - A maximum of 96 ACLs can be configured on an AP. Each ACL can have a maximum of 64 rules.
  - FlexConnect ACLs do not have directions. The entire ACL is applied as ingress or egress.
  - The ACL returned by the AAA is applied on both ingress and egress on the 802.11 side of the client.

Note A Local Switching WLAN is configured and ACL is mapped to a FlexConnect group with an ACL. The ACL has set of 'deny and permit' rules. When you associate a client to the WLAN, the client needs to have DHCP permit rule added for getting the IP address.

Configuring FlexConnect Access Control Lists (GUI)

Step 1 Choose **Security** > **Access Control Lists** > **FlexConnect Access Control Lists**.

The **FlexConnect ACL** page is displayed.

This page lists all the FlexConnect ACLs configured on the controller. This page also shows the FlexConnect ACLs created on the corresponding controller. To remove an ACL, hover your mouse over the blue drop-down arrow that is next to the corresponding ACL name and choose **Remove**.

Step 2 Add a new ACL by clicking **New**.

The **Access Control Lists** > **New** page is displayed.

Step 3 In the **Access Control List Name** field, enter a name for the new ACL. You can enter up to 32 alphanumeric characters.

Step 4 Click **Apply**.

Step 5 Click the name of the new ACL after the **Access Control Lists** page is displayed again.

When the **Access Control Lists > Edit** page appears, click **Add New Rule**.

The **Access Control Lists** > **Rules** > **New** page is displayed.

Step 6 Configure an IP address based rule for a given FlexConnect ACL as follows:

a) Choose **IP Rule** to create an IP address based rule.

The **Access Control Lists** > **Rules** > **New** page is displayed.

b) The controller supports up to 64 rules for each IP address-based ACL. These rules are listed in order from 1 to 64. In the **Sequence** field, enter a value (between 1 and 64) to determine the order of this rule in relation to any other rules defined for this ACL.

Note If rules 1 to 4 are already defined and you add rule 29, it is added as rule 5. If you add or change a sequence number of a rule, the sequence numbers of the other rules are automatically adjusted to maintain a continuous sequence. For instance, if you change a rule's sequence number from 7 to 5, the rules with sequence numbers 5 and 6 are automatically reassigned as 6 and 7, respectively.

c) From the **Source** drop-down list, choose one of these options to specify the source of the packets to which this ACL is applicable:

- **Any**—Any source (This is the default value.).
- **IP Address**—A specific source. If you choose this option, enter the IP address and netmask of the source in the corresponding fields.

d) From the **Destination** drop-down list, choose one of these options to specify the destination of the packets to which this ACL applies:

- **Any**—Any destination (This is the default value.).
- **IP Address**—A specific destination. If you choose this option, enter the IP address and the details of the destination in the relevant fields.

e) From the **Protocol** drop-down list, choose the protocol ID of the IP packets to be used for this ACL. The protocol options that you can use are the following:

- **Any**—Any protocol (This is the default value.).
- **TCP**
- **UDP**
- **ICMP**—Internet Control Message Protocol
- **ESP**—IP Encapsulating Security Payload
- **AH**—Authentication Header
- **GRE**—Generic Routing Encapsulation
- **IP in IP**—Permits or denies IP-in-IP packets
- **Eth Over IP**—Ethernet-over-Internet Protocol
- **OSPF**—Open Shortest Path First
- **Other**—Any other Internet-Assigned Numbers Authority (IANA) protocol

Note If you choose Other, enter the number of the desired protocol in the **Protocol** field. You can find the list of available protocols in the INAI website.

The controller can permit or deny only the IP packets in an ACL. Other types of packets (such as Address Resolution Protocol (ARP) packets) cannot be specified.

If you choose TCP or UDP, two more parameters—Source Port and Destination Port, are displayed. These parameters enable you to choose a specific source port and destination port or port range. The port options are used by applications that send and receive data to and from the networking stack. Some ports are designated for certain applications, such as Telnet, SSH, HTTP, and so on.

f) From the **DSCP** drop-down list, choose one of these options to specify the differentiated services code point (DSCP) value of this ACL. DSCP is an IP header field that can be used to define the quality of service across the Internet.

- **Any**—Any DSCP (This is the default value.).
- **Specific**—A specific DSCP from 0 to 63, which you enter in the **DSCP** field.

g) From the **Action** drop-down list, choose **Deny** to cause this ACL to block packets, or **Permit** to cause this ACL to allow packets. The default value is **Deny**.

h) Click **Apply**.

The **Access Control Lists > Edit** page is displayed on which the rules for this ACL are shown.

i) Repeat this procedure to add more rules, if required, for this ACL.

Configuring FlexConnect Access Control Lists (CLI)

Use the following commands on the controller to configure FlexConnect ACLs:

Procedure

- Create or delete an ACL on a FlexConnect access point by entering this command:

  config flexconnect acl {**create | delete** } *name*

  The IPv4 ACL name of up to 32 characters is supported.

- Associate a FlexConnect ACL to a WLAN.

  a) Enable web authentication by entering this command:

  config wlan security web-auth enable *wlan_id*

  b) Configure the FlexConnect ACL to a WLAN by entering this command:

  config wlan security web-auth flexacl *wlan_id acl_name*

- Configure an IP address based rule for an ACL

  a) Add an IP address based rule to the FlexConnect ACL by entering this command:

  config flexconnect acl rule add *acl-name rule-index*

  b) Configure a rule's source IP address and netmask by entering this command:

  config flexconnect acl rule source address *acl-name rule-index ipv4-addr subnet-mask*

  c) Configure a rule’s source port range by entering this command:

  config flexconnect acl rule source port range *acl-name rule-index start-port end-port*

  d) Configure a rule's destination IP address and netmask by entering this command:

  IPv4—**config flexconnect acl rule destination address** *acl-name rule-index ipv4-addr subnet-mask*

  e) Configure a rule’s destination port range by entering this command:

  config flexconnect acl rule destination port range*acl-name rule-index start-port end-port*

  f) Configure the rule's IP protocol by entering this command:

  config flexconnect acl rule protocol *acl-name rule-index* **protocol**

  Specify an index value between 0 and 64. Specify the protocol value between 0 and 255 or ‘any’. The default is ‘any.’

  g) Specify the differentiated services code point (DSCP) value of the rule index by entering this command:

  config flexconnectacl rule dscp *acl-name rule-index dscp-value*

  DSCP is an IP header that can be used to define the quality of service across the Internet. Enter a value between 0 and 63 or the value **any**. The default value is **any**.

  h) Set the Permit or deny action to the rule by entering this command:

  config flexconnect acl rule actionacl-name *rule-index* **{permit |deny}**

  i) Change the index value for an ACL rule by entering this command:

  config flexconnectacl rule change index *acl-name old-index new-index*

  j) Swap the index values between two rules by entering this command:

config flexconnect acl rule swap *acl-name index-1 index-2*

k) Delete a rule from the FlexConnect ACL by entering this command:

config flexconnect acl rule delete *name*

l) Apply an ACL to the FlexConnect access point by entering this command:

config flexconnect acl apply *acl-name*

- [Optional] Add a VLAN on a FlexConnect access point by entering this command:

  config ap flexconnect vlan add *acl vlan-id ingress-aclname egress-acl-name ap-name*

Viewing and Debugging FlexConnect Access Control Lists (CLI)

Use the following commands on the controller to view information related to FlexConnect ACLs:

Procedure

- **show flexconnect acl summary**—Displays a summary of the ACLs.
- **show client detail** *mac-address*—Displays AAA override ACL.
- **show flexconnect acl detailed acl-name**—Displays the detailed information about the ACL.
- **debug flexconnect acl {enable | disable}**—Enables or disables the debugging of FlexConnect ACL.
- **debug capwap reap**—Enables debugging of CAPWAP.