Configure las ACL de Flexconnect en el WLC

Contenido

Introducción

Este documento describe los diversos tipos de la lista de control de acceso (ACL) flexconnect y cómo se pueden configurar y validar en el punto de acceso (AP).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Controlador de LAN inalámbrica de Cisco (WLC) que ejecuta código 8.3 y superior
- Configuración de Flexconnect en el WLC

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- El WLC de la serie 8540 de Cisco que ejecuta la versión de software 8.3.133.0.
- 3802 y 3702 AP que se ejecutan en el modo flexconnect.

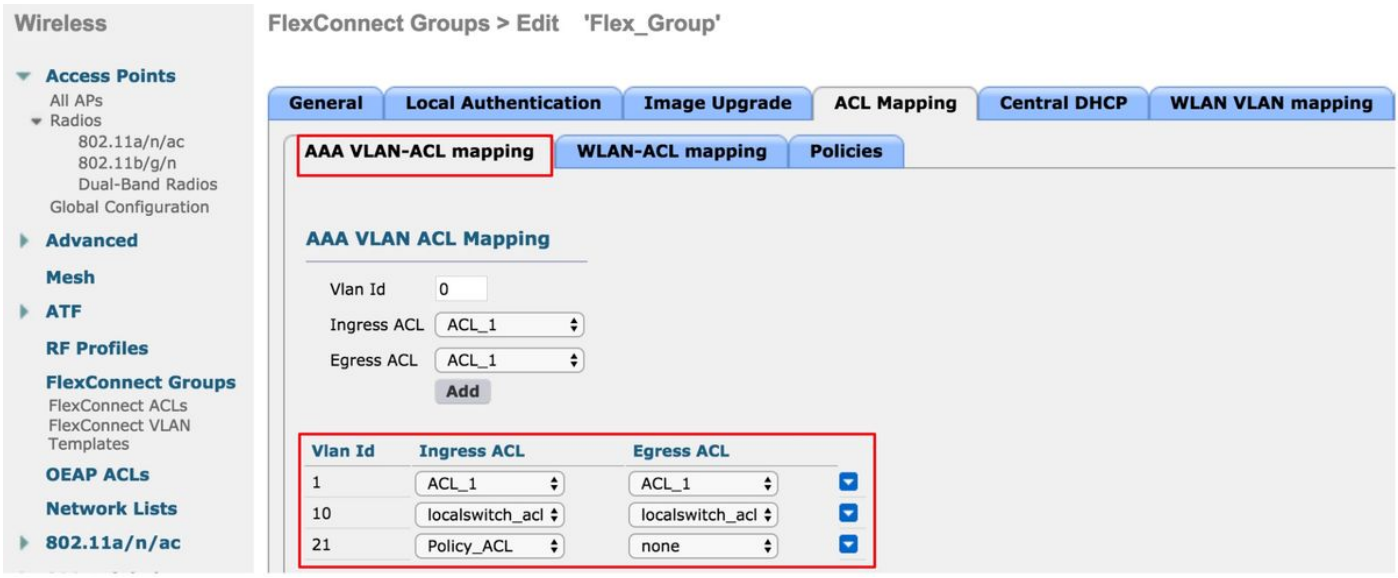
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Tipos de ACL

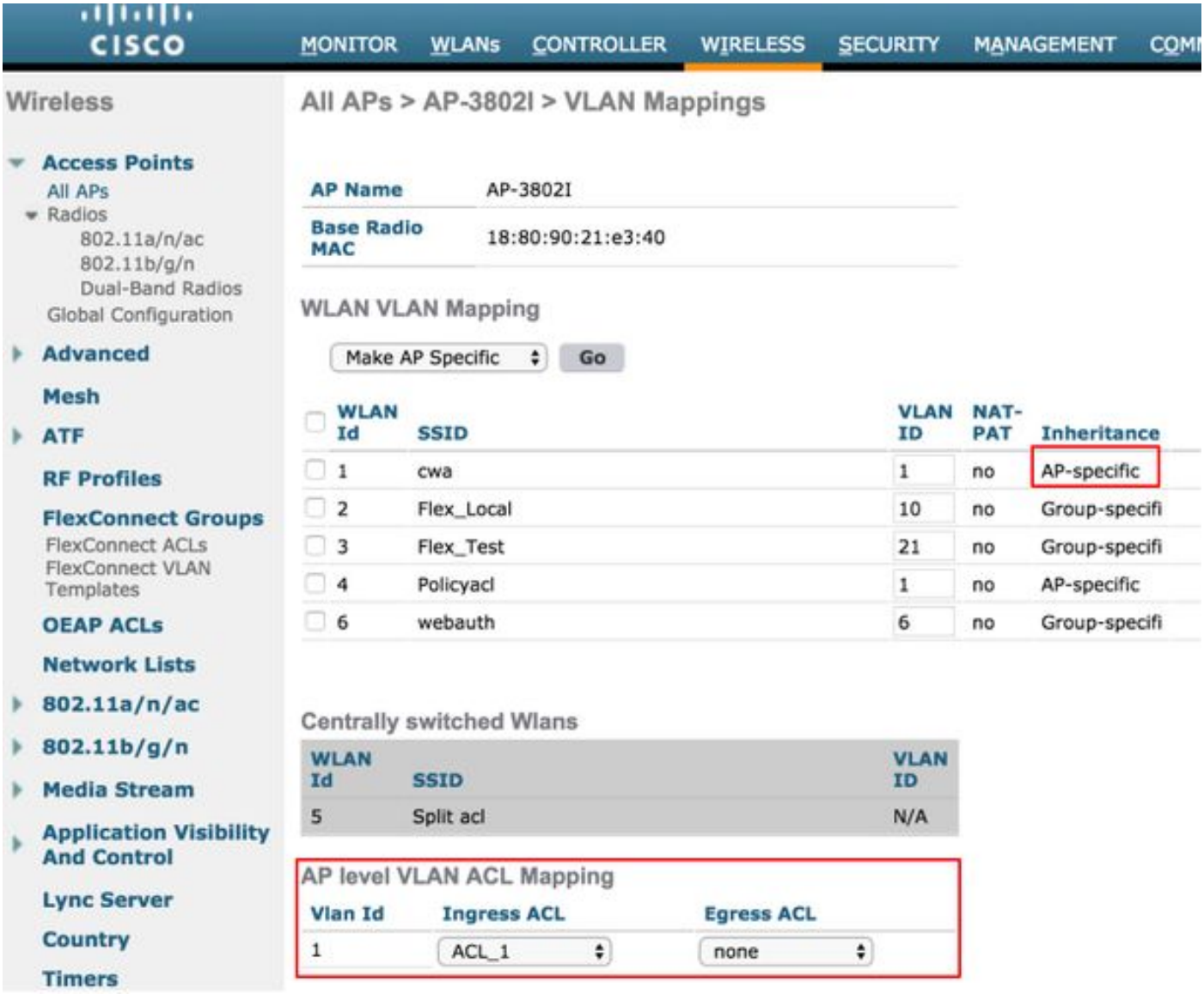
1. ACL de VLAN

VLAN ACL son las ACL más utilizadas y le permite controlar el tráfico de cliente que se envía dentro y fuera de la VLAN.

La ACL se puede configurar según el grupo flexconnect que utiliza la sección de mapeo **AAA VLAN-ACL** en **Grupos de Flexconnect Inalámbricos > mapping ACL > mapeo AAA VLAN-ACL** como se muestra en la imagen.



También se puede configurar según el nivel AP, navegue a **Inalámbrico > Todos los AP > Nombre AP > Ficha Flexconnect** y haga clic en la sección **Asignaciones VLAN**. Aquí, debe hacer que el AP de configuración de VLAN sea específico primero, después de lo cual puede especificar el mapping de VLAN-ACL de nivel AP como se muestra en la imagen.



Direcciones ACL

También puede especificar la dirección en la que se aplica la ACL:

- Entrada (entrada significa hacia el cliente inalámbrico)
- Salida (hacia DS o LAN),
- ambos o ninguno.

Por lo tanto, si desea bloquear el tráfico destinado al cliente inalámbrico, puede utilizar la dirección de ingreso y si desea bloquear el tráfico originado por el cliente inalámbrico, puede utilizar la dirección de salida.

La opción none se utiliza cuando desea presionar una ACL independiente con el uso de la autenticación, autorización y control (AAA). En este caso, la ACL enviada por el servidor RADIUS se aplica dinámicamente al cliente.

> **Nota:** La ACL debe configurarse de antemano en Flexconnect ACL; de lo contrario, no se aplica.

Consideraciones de Mapping de ACL

Cuando utiliza ACL de VLAN, también es importante entender estas consideraciones con respecto a los mapeos de VLAN en los AP de flexconnect:

- Si la VLAN se configura con el uso del grupo FlexConnect, se aplica la ACL correspondiente configurada en el grupo FlexConnect.
- Si se configura una VLAN en el grupo FlexConnect y también en el AP (como configuración específica de AP), la configuración de ACL de AP tiene prioridad.
- Si la ACL específica del AP se configura en ninguno, no se aplica ninguna ACL.
- Si la VLAN que se devolvió desde el AAA no está presente en el AP, el cliente vuelve a la VLAN predeterminada configurada para la LAN inalámbrica (WLAN) y cualquier ACL asignada a esa VLAN predeterminada tiene prioridad.

Verifique si la ACL se aplica en el AP

Utilize esta sección para confirmar que su configuración funcione correctamente.

1. Puntos de acceso Wave 2

En un AP de onda 2, puede verificar si la ACL se envía realmente al AP con el comando **show flexconnect vlan-acl**. Aquí, también puede ver el número de paquetes pasados y perdidos para cada ACL.

```
AP-3802I#show flexconnect vlan-acl
Flexconnect VLAN-ACL mapping-- ingress vlan     -----Listing ACL's in ingress direction
ACL enabled on ingress vlan

vlan_id: 10
ACL rules:
0: deny true and dst 10.1.1.0 mask 255.255.255.0,
1: deny true and dst 10.1.10.1 mask 255.255.255.255,
2: allow true,
the number of passed packets: 4
the number of dropped packets: 0

Flexconnect VLAN-ACL mapping-- egress vlan      -----Listing ACL's in egress direction
ACL enabled on egress vlan

vlan_id: 21
ACL rules:
0: allow true and dst 10.106.34.13 mask 255.255.255.255,
1: allow true and src 10.106.34.13 mask 255.255.255.255,
2: deny true,
the number of passed packets: 1
the number of dropped packets: 4
```

2. AP del IOS® de Cisco

En el nivel AP, puede validar si la configuración ACL se ha enviado al AP de dos maneras:

- Utilice el comando **show access-lists** que muestra si todas las VLAN ACL están configuradas en el AP:

```
AP-3702#sh access-lists
Extended IP access list Policy_ACL
    10 permit ip any host 10.106.34.13
    20 permit ip host 10.106.34.13 any
    30 permit udp any range 0 65535 any eq bootpc
    40 permit udp any eq bootps any range 0 65535
    50 deny ip any any
```

También puede monitorear la actividad que ocurre en cada ACL, verificar el resultado detallado de esa ACL y ver el recuento de aciertos para cada línea:

```
AP-3702#sh access-lists Policy_ACL
Extended IP access list Policy_ACL
    10 permit ip any host 10.106.34.13
    20 permit ip host 10.106.34.13 any
    30 permit udp any range 0 65535 any eq bootpc (6 matches)  -------------Shows the hit count
    40 permit udp any eq bootpc any range 0 65535
    50 deny ip any any (78 matches)
```

- Dado que las ACL de VLAN se aplican en la interfaz gigabit, puede validar si la ACL se aplica correctamente. Verifique el resultado de la subinterfaz como se muestra aquí:

```
AP-3702#sh run interface GigabitEthernet0.10
Building configuration...

Current configuration : 219 bytes
!
interface GigabitEthernet0.10
 encapsulation dot1Q 10
 ip access-group localswitch_acl in --------Specifies that localswitch_acl has been applied in
ingress direction
 ip access-group localswitch_acl out -------Specifies that localswitch_acl has been applied in
egress direction
 bridge-group 6
 bridge-group 6 spanning-disabled
 no bridge-group 6 source-learning
```

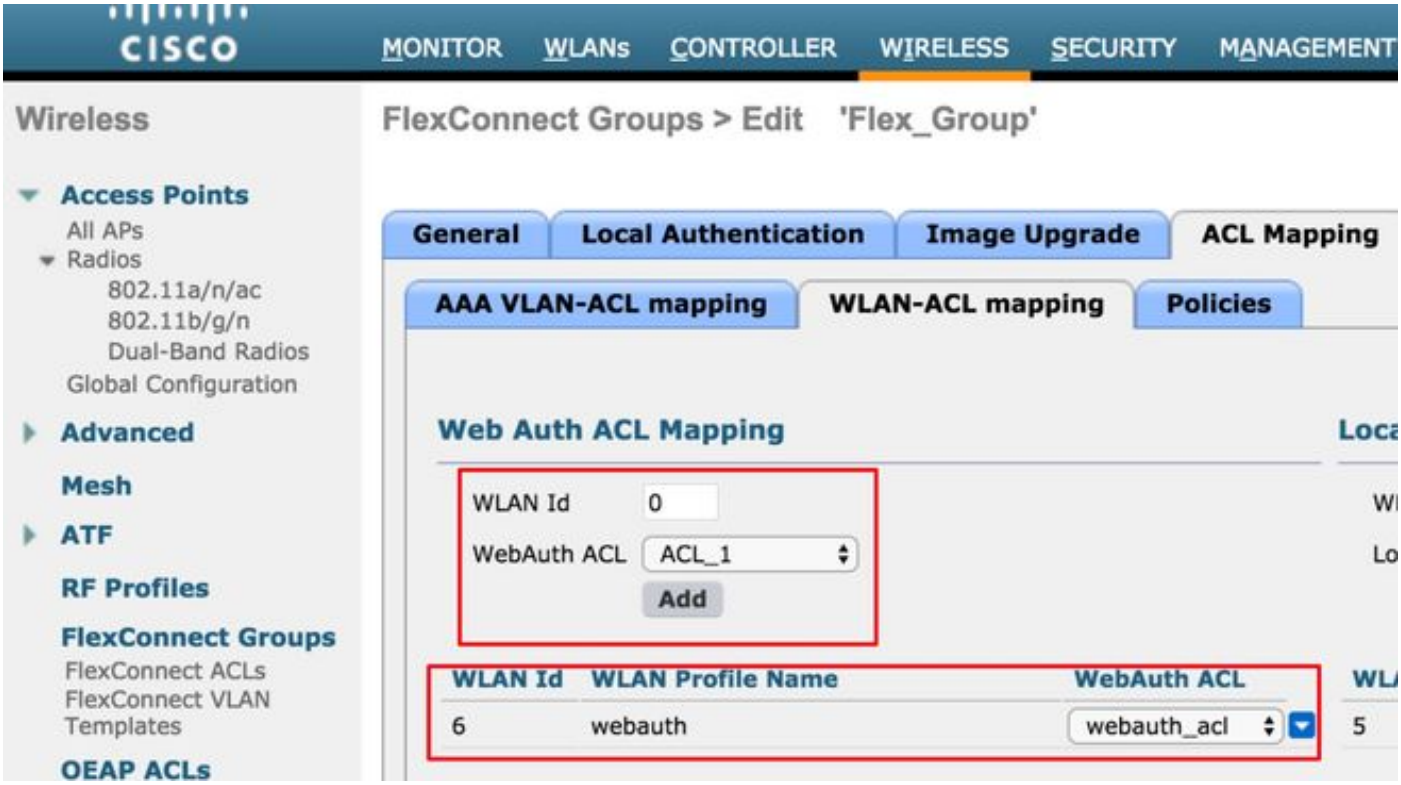
2. ACL de Webauth

Webauth ACL se utiliza en el caso de un identificador de conjunto de servicios (SSID) Webauth/Webpassthrough que se ha habilitado para el switching local flexconnect. Esto se utiliza como ACL de autenticación previa y permite el tráfico del cliente al servidor de redirección. Una vez que se completa el redireccionamiento y el cliente está en el estado **RUN**, la ACL se detiene para tenerlo en efecto.

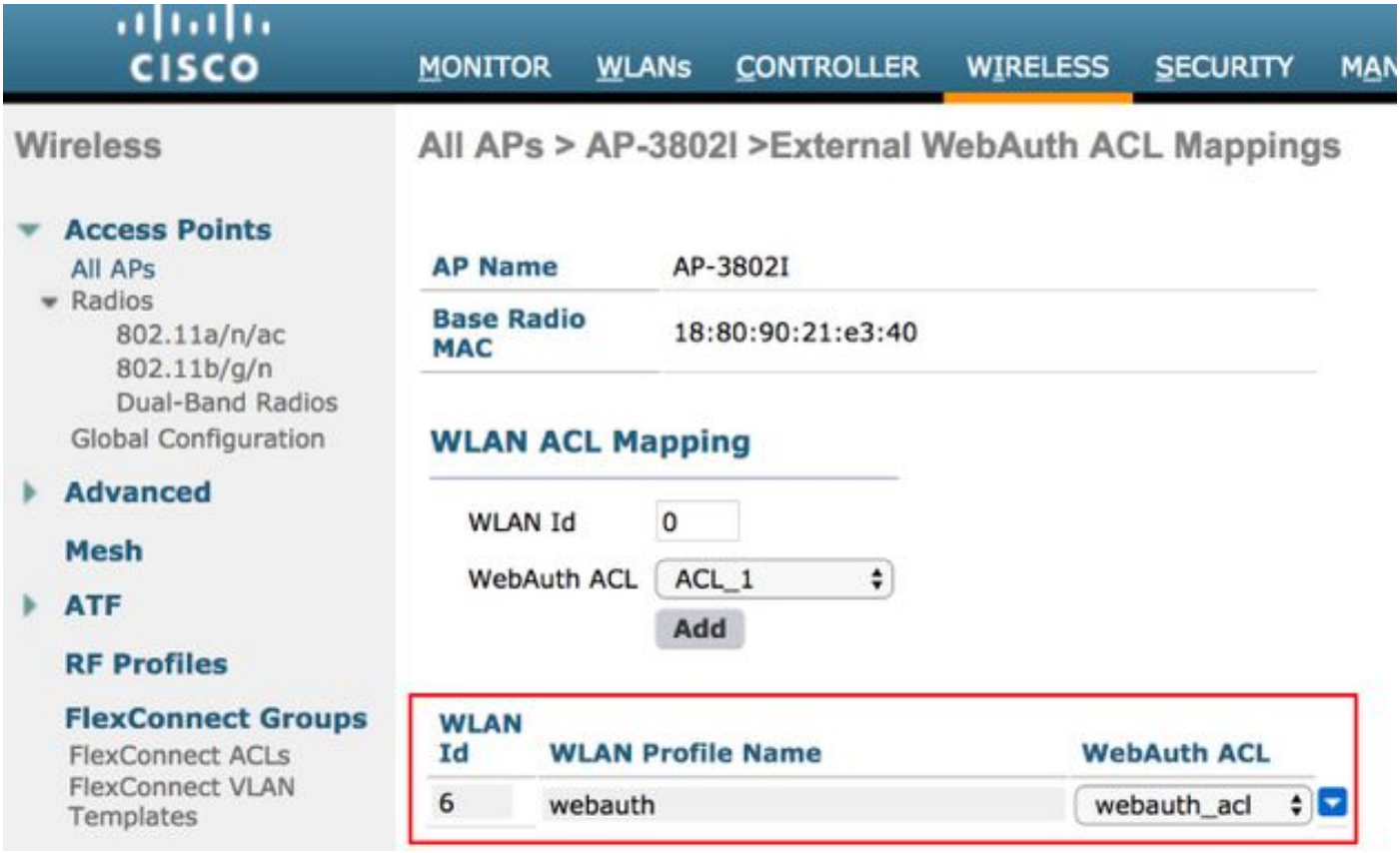
La ACL de Webauth se puede aplicar en el nivel de WLAN, el nivel de AP o el nivel de grupo de flexconnect. Una ACL específica de AP tiene la prioridad más alta, mientras que la ACL de WLAN tiene la más baja. Si se aplican las tres, AP Specific tiene prioridad seguida de Flex ACL y luego WLAN Global Specific ACL.

Puede haber un máximo de 16 ACL de autenticación web configuradas en un AP.

Se puede aplicar en el nivel del grupo flexconnect, navegue hasta **Wireless > Flexconnect Groups > Seleccione el grupo que desea configurar > ACL mapping > WLAN-ACL mapping > Web Auth ACL Mapping** como se muestra en la imagen.



La ACL se puede aplicar en el nivel AP, navegue a **Wireless >All AP's >AP name >Flexconnect tab > External WebAuthentication ACL > WLAN ACL** como se muestra en la imagen.



La ACL se puede aplicar en el nivel WLAN, navegue a **WLAN > WLAN_ID > Capa 3 > WebAuth FlexAcl** como se muestra en la imagen.

En el Cisco IOS® AP, puede verificar si la ACL se aplicó al cliente. Verifique la salida del **cliente show controllers dot11radio 0** (o 1 si el cliente se conecta a la radio A) como se muestra aquí:

```
AP-3702#show controller dot11radio0 client
---Clients 0  AID VLAN Status:S/I/B/A Age TxQ-R(A) Mode Enc Key  Rate  Mask Tx   Rx
BVI   Split-ACL Client-ACL WebAuth-ACL L2-ACL
e850.8b64.4f45    1    4 30 40064 000 0FE 299  0-0 (0) 13B0 200 0-10 1EFFFFFF00000000000  020F
030 - - - webauth_acl       -     --------Specifies the name of the ACL that was applied
```

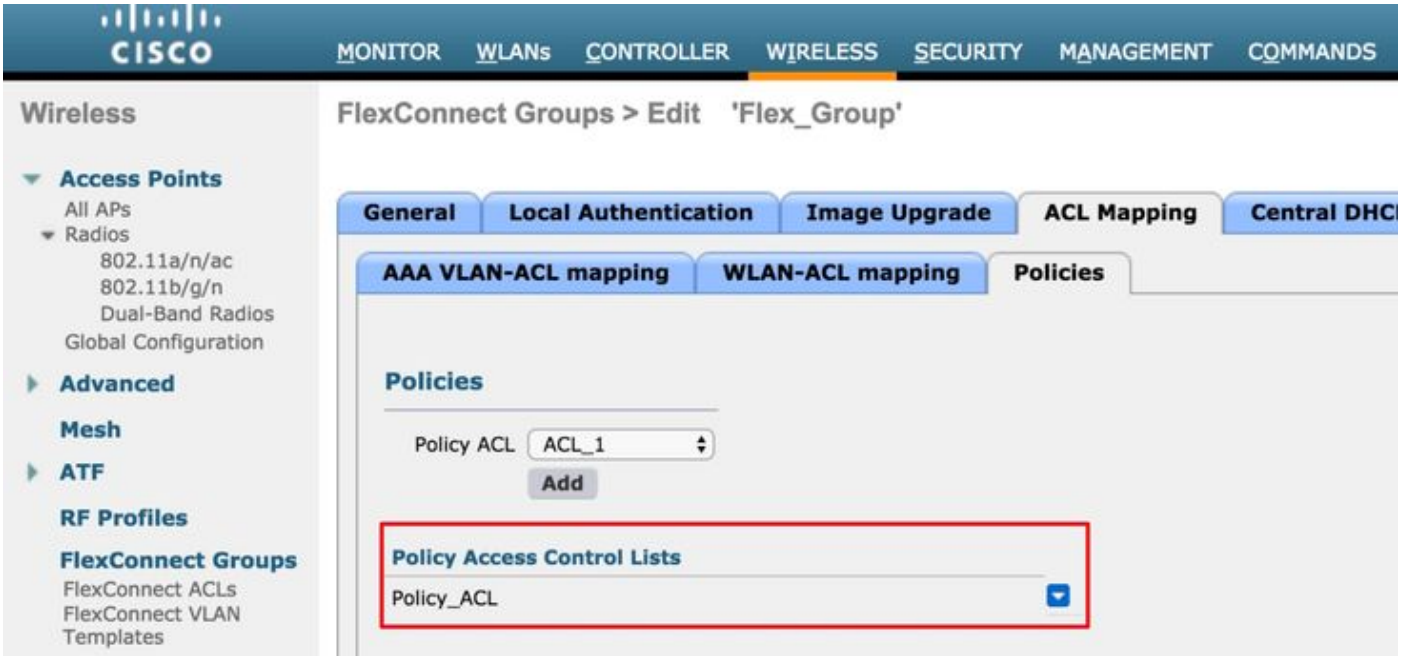
3. ACL de política web

WebPolicy ACL se utiliza para los escenarios de redirección web condicional, redirección web de la página de inicio y Webauth central.

Hay dos modos de configuración disponibles para las WLANs WebPolicy con ACLs Flex:

1. Grupo Flexconnect

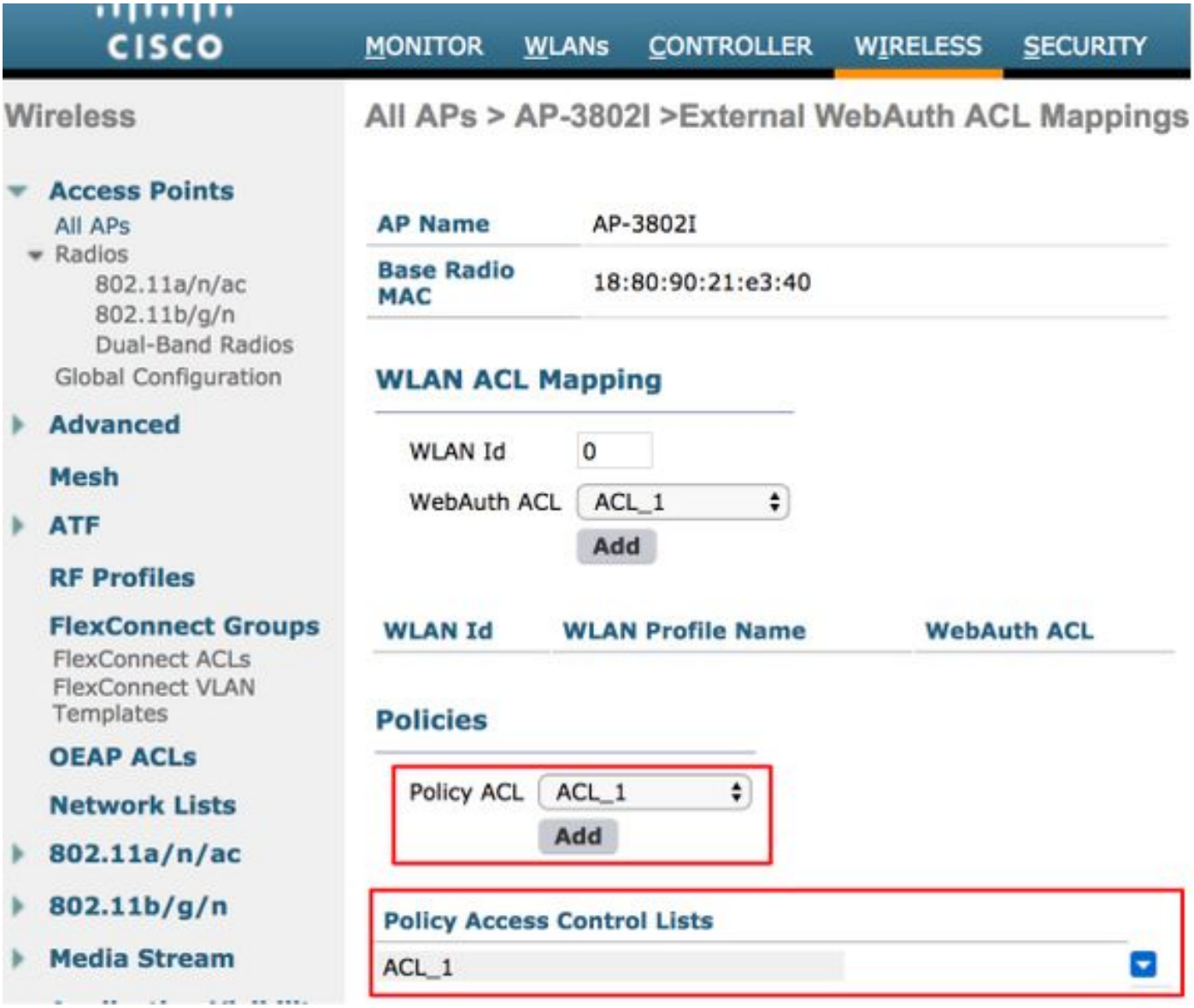
Todos los AP del grupo FlexConnect reciben la ACL configurada. Esto se puede configurar mientras navega a **Wireless-Flexconnect Groups > Seleccione el grupo que desea configurar > ACL mapping > Policies**, y agregue el nombre de la política ACL como se muestra en la imagen:



2. AP específico

El AP para el cual se realiza la configuración recibe la ACL, no se impactan otros AP. Esto se puede configurar a medida que navega a **Wireless > All APs > AP name >**

Ficha Flexconnect > ACL de WebAuthentication externas > Políticas como se muestra en la imagen.



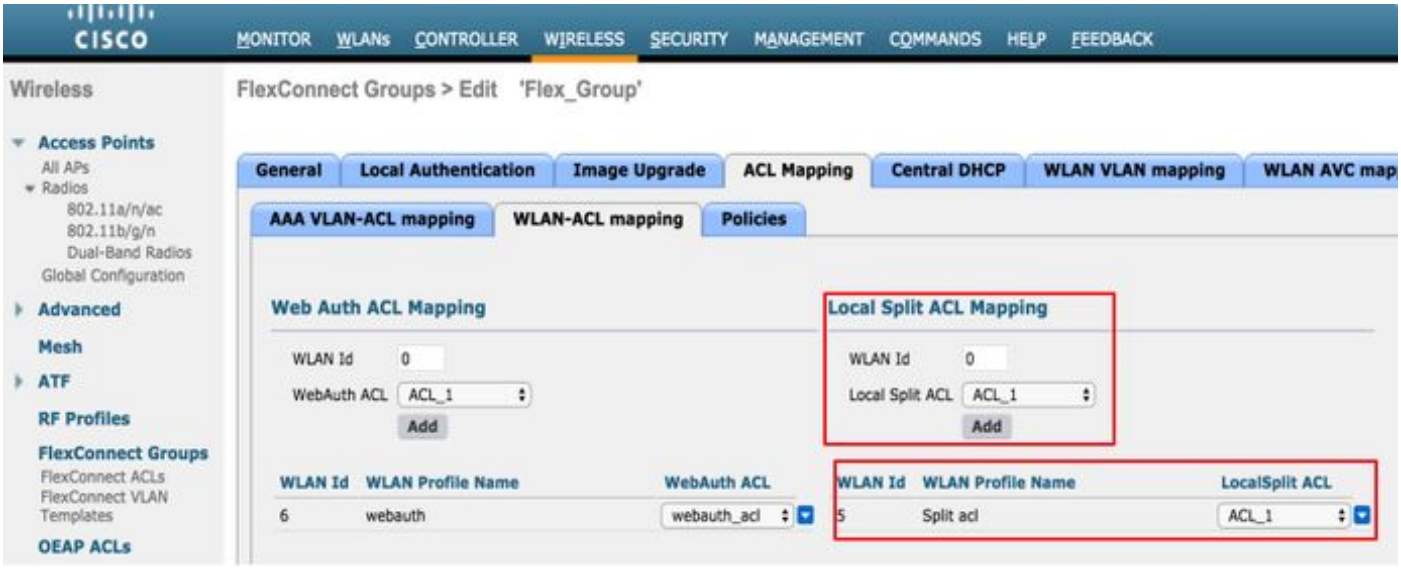
Después de una autenticación L2 exitosa, cuando el servidor radius envía el nombre ACL en el par AV redirect-acl, esto se aplica directamente para el cliente en el AP. Cuando el cliente pasa al estado **RUN**, todo el tráfico del cliente se conmuta localmente y el AP se detiene para aplicar ACL.

Puede haber un máximo de 32 ACL de WebPolicy configuradas en un AP. 16 AP específicos y 16 FlexConnect específicos del grupo.

4. ACL de túnel dividido

Las ACL de tunelización dividida se utilizan con los SSID conmutados centralmente cuando parte del tráfico del cliente debe enviarse localmente. La función de tunelación dividida también es una ventaja añadida para la configuración de punto de acceso de Office Extend (OEAP), en la que los clientes de un SSID corporativo pueden comunicarse con los dispositivos de una red local (impresoras, máquinas con cables en un puerto LAN remoto o dispositivos inalámbricos en un SSID personal) directamente una vez que se mencionan como parte de la ACL de túnel dividido.

Las ACL de Tunelización Dividida se pueden configurar en según el nivel de grupo flexconnect, navegue hasta **Grupos de FlexConexión Inalámbrica > Seleccione el grupo que desea configurar > mapeo ACL > mapeo de ACL WLAN-ACL > Mapping de ACL Dividida Local** como se muestra en la imagen.



También se pueden configurar según el nivel AP, navegue a **Inalámbrico > Todos los AP > Nombre AP > Ficha Flexconnect > ACL Divididas Locales** y agregue el nombre de la ACL flexconnect como se muestra en la imagen.

Las ACL de tunelización dividida no pueden puentear localmente el tráfico de multidifusión/difusión. El tráfico de multidifusión/difusión se conmuta de forma centralizada aunque coincida con la ACL de FlexConnect.

Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.