Configuración Flexconnect ACL en el WLC

Contenido

Introducción

Este documento describe los diversos tipos de la lista de control de acceso (ACL) del flexconnect y cómo pueden ser configurados y ser validados en el punto de acceso.

Prerequisites

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- El controlador LAN de la tecnología inalámbrica de Cisco (WLC) ese funciona con el código 8.3 y más alto
- 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 las Cisco 8540 Series que funciona con la versión de software 8.3.133.0.
- 3802 y 3702 AP que se ejecutan en el modo del flexconnect.

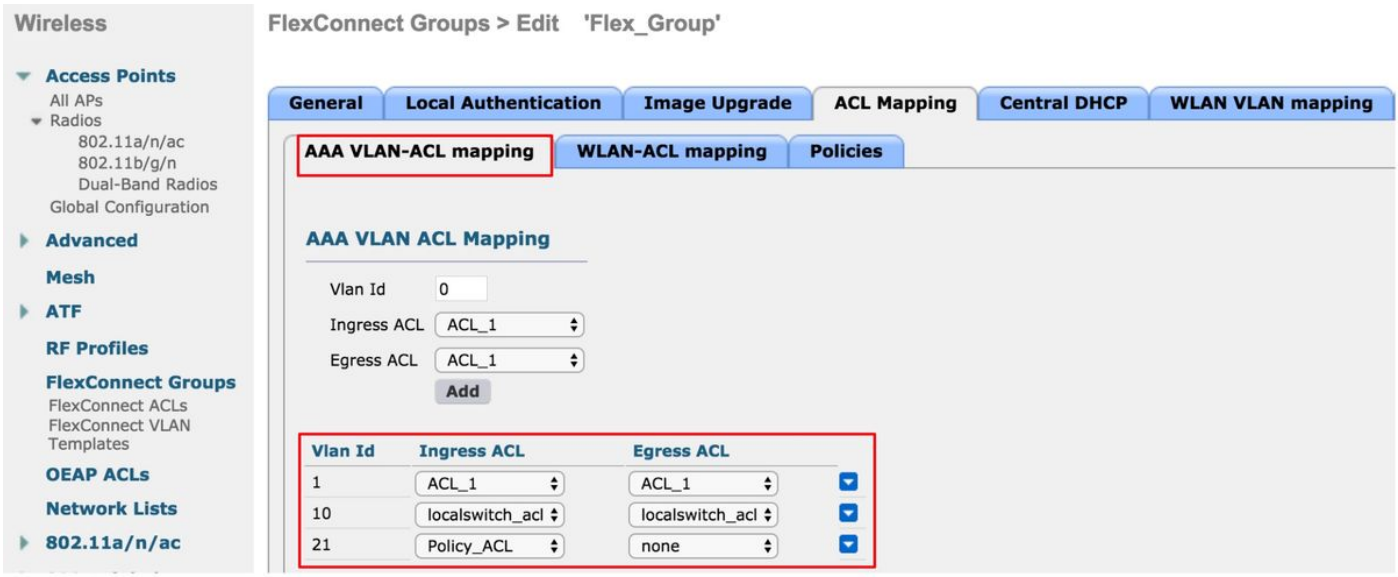
La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Tipos ACL

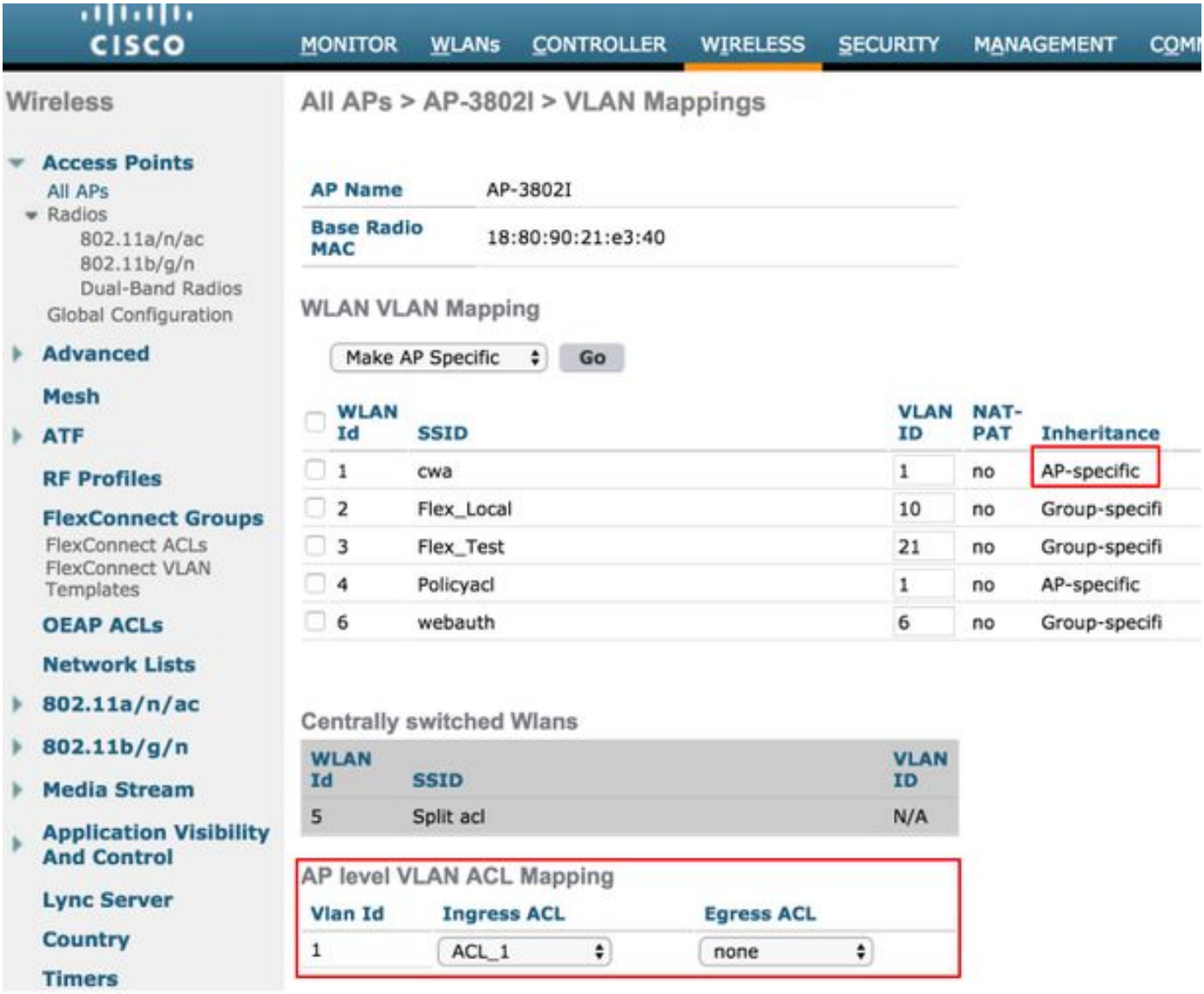
1. VLA N ACL

El VLA N ACL es el ACL más de uso general y le deja controlar el tráfico del cliente que se envía dentro y fuera del VLA N.

El ACL se puede configurar según el grupo del flexconnect que utiliza la sección de la asignación **AAA VLAN-ACL** en **Tecnología inalámbrica-Flexconnect agrupa > ACL que asocia >AAA la asignación VLAN-ACL** tal y como se muestra en de la imagen.



Puede también ser configurado según el nivel AP, navegar a la **Tecnología inalámbrica > toda la lengueta de Flexconnect del name> AP > AP** y hacer clic la sección de las **asignaciones del VLA N**. Aquí, usted necesita hacer el específico de los config AP del VLA N primero, después de lo cual usted puede especificar la asignación del nivel VLAN-ACL AP tal y como se muestra en de la imagen.



Direcciones ACL

Usted puede también especificar la dirección en la cual el ACL consigue aplicado:

- Ingreso (el ingreso significa hacia el cliente de red inalámbrica)
- Salida (hacia el theDS o el LAN),
- ambo o ninguno.

Así pues, si usted quisiera bloquear el tráfico destinado hacia el cliente de red inalámbrica entonces que usted puede utilizar a la dirección de ingreso y si usted quisiera bloquear el tráfico originado por el cliente de red inalámbrica, usted puede utilizar a la dirección de salida.

Se utiliza la opción ningunos cuando usted quisiera avanzar un ACL separado con el uso de la invalidación del Authentication, Authorization, and Accounting (AAA). En este caso, el ACL enviado por el servidor de RADIUS se aplica dinámicamente al cliente.

> **Note**: El ACL necesita ser configurado bajo Flexconnect ACL de antemano, si no no consigue aplicado.

Consideraciones de la asignación ACL

Cuando usted utiliza el VLA N ACL, es también importante entender estas consideraciones en cuanto a las asignaciones del VLA N en el flexconnect AP:

- Si el VLA N se configura con el uso del grupo de FlexConnect, el ACL correspondiente configurado en el grupo de FlexConnect es aplicado.
- Si un VLA N se configura en el grupo de FlexConnect y también en el AP (como configuración específica AP), después la configuración ACL AP toma la precedencia.
- Si el AP ACL específico se configura a ningunos, después no hay ACL aplicado.
- Si el VLA N que fue vuelto del AAA no está presente en el AP, el cliente recurre al VLAN predeterminado configurado para el Wireless LAN (red inalámbrica (WLAN)) y cualquier ACL asociado a ese VLAN predeterminado toma la precedencia.

Verifique si el ACL se aplica en el AP

Utilize esta sección para confirmar que su configuración funcione correctamente.

1. Onda 2 AP

En una onda 2 AP, usted puede verificar si el ACL consigue realmente avanzado al AP con el **flexconnect VLAN-ACL del** comando show. Aquí, usted puede también ver el número de pasado y los paquetes 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. Cisco IOS® AP

En el nivel AP, usted puede validar si la configuración ACL se ha avanzado al AP con dos maneras:

- Utilice el **comando show access-lists** que muestra si todo el VLA N ACL se configura 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
```

Usted puede también monitorea la actividad que sucede en cada ACL, marca la salida detallada de ese ACL y ve la cuenta del golpe 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)
```

- Puesto que el VLA N ACL se aplica en la interfaz Gigabit, usted puede validar si el ACL se aplica correctamente. Marque la salida de la interfaz sub 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. Webauth ACL

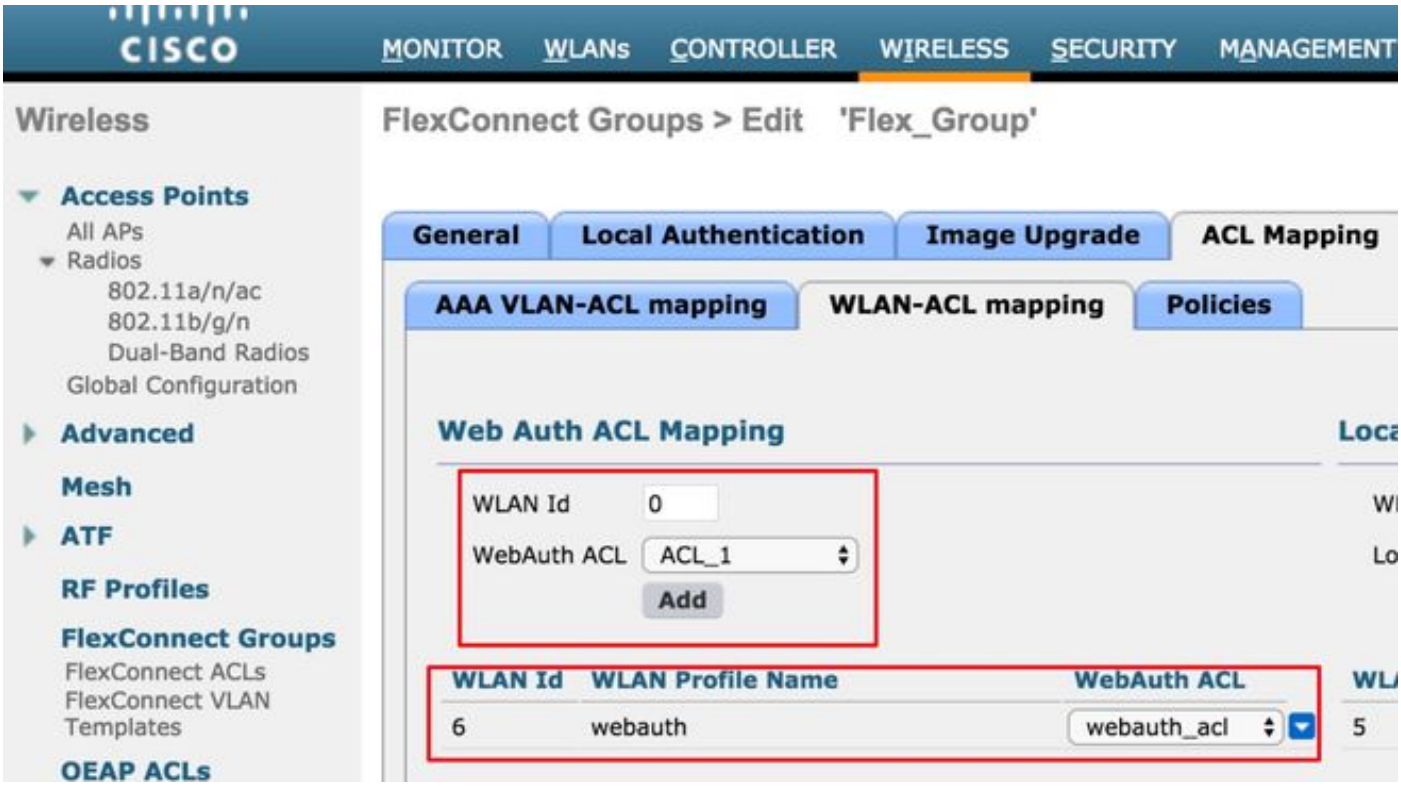
Webauth ACL se utiliza en el caso de un Service Set Identifier (SSID) Webauth/Webpassthrough que se ha habilitado para el Local Switching del flexconnect. Esto se utiliza como PRE-autenticación ACL y permite el tráfico del cliente al servidor de redirección. Una vez que el cambio de dirección es completo y el cliente está en el estado de **FUNCIONAMIENTO**, las paradas ACL para tomarlo en el efecto.

Webauth ACL se puede aplicar cualquiera en el nivel de la red inalámbrica (WLAN), el nivel AP o el nivel de grupo del flexconnect. Un AP ACL específico tiene la prioridad más alta, mientras que la red inalámbrica (WLAN) ACL tiene el más bajo. Si los tres son aplicados, el específico AP toma la precedencia seguida por la flexión ACL y entonces el específico global ACL de la red inalámbrica (WLAN).

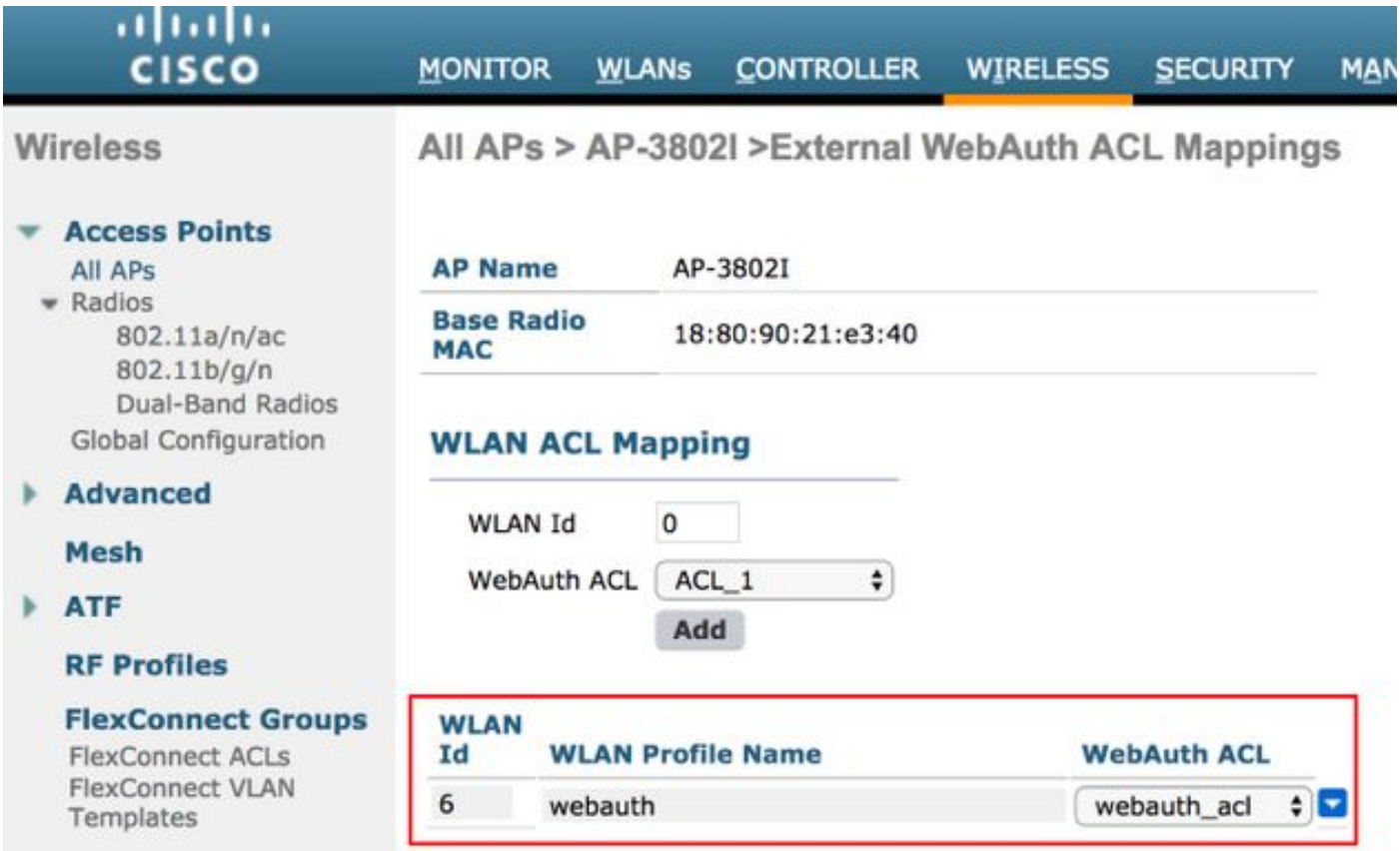
Puede haber un máximo de 16 Red-auth ACL configurados en un AP.

Puede ser aplicado en el nivel de grupo del flexconnect, navega a la **Tecnología inalámbrica > a los grupos de Flexconnect > selecciona al grupo que usted quiere la configuración > la asignación ACL > la asignación WLAN-ACL > la asignación del auth ACL de la red** tal y como se muestra en

de la imagen.



El ACL puede ser aplicado en el nivel AP, navega a la **lengueta inalámbrica del >Flexconnect del nombre >AP del >All AP > WebAuthentication externo los ACL > la red inalámbrica (WLAN) ACL** tal y como se muestra en de la imagen.



El ACL puede ser aplicado en el nivel de la red inalámbrica (WLAN), navega a la **red inalámbrica (WLAN) > a WLAN_ID > a la capa 3 > WebAuth FlexAcl** tal y como se muestra en de la imagen.

En Cisco IOS® AP, usted puede verificar si el ACL fue aplicado al cliente. Marque la salida del **cliente de los reguladores dot11radio 0** (o 1 de la **demostración** si el cliente conecta con 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
```

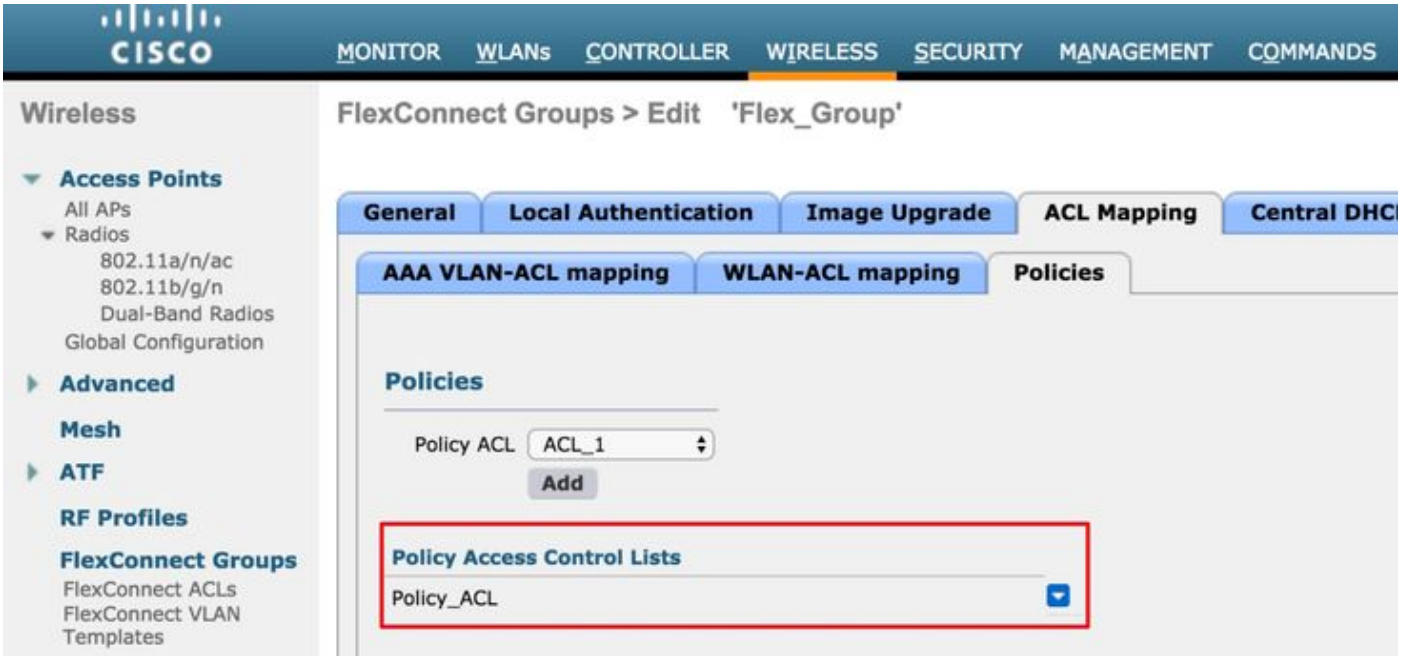
3. Directiva ACL de la red

WebPolicy ACL se utiliza para la red condicional reorienta, la red de la página del chapoteo reorienta y los escenarios centrales de Webauth.

Hay dos modos de configuración disponibles para WebPolicy WLAN con la flexión ACL:

1. Grupo de Flexconnect

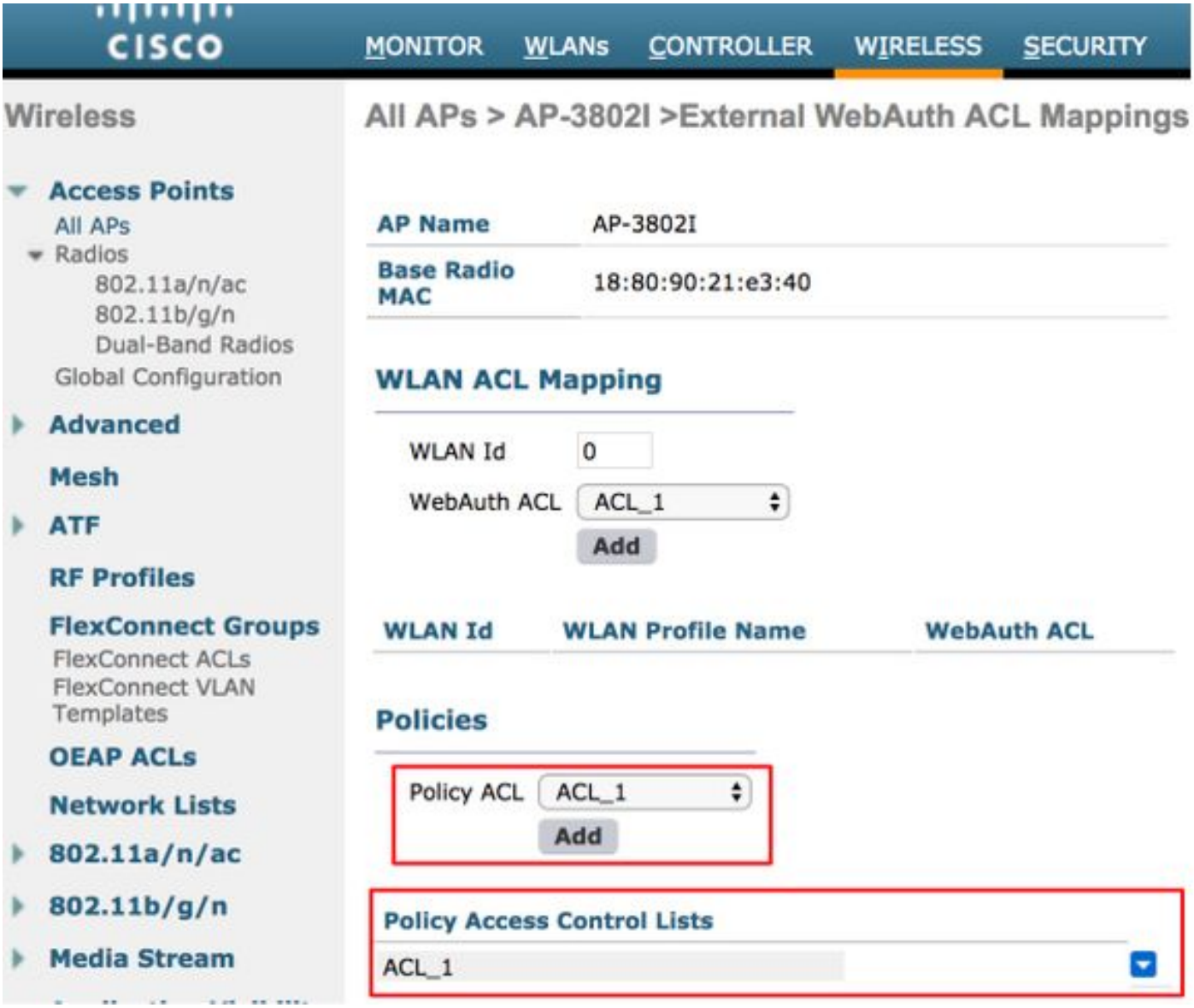
Todos los AP en el grupo de FlexConnect reciben el ACL se configura que. Esto se puede configurar como usted navega a los **grupos de la Tecnología inalámbrica-Flexconnect > selecciona al grupo que usted quiere la configuración > la asignación > las directivas ACL**, y agrega el nombre de la directiva ACL tal y como se muestra en de la imagen:



2. Específico AP

Se afecta El AP para el cual se hace la configuración recibe el ACL, ningunos otros AP. Esto se puede configurar como usted navega a la **Tecnología inalámbrica > todo el los AP > name> AP**

Lengueta de Flexconnect > WebAuthentication externo ACL > directivas tal y como se muestra en de la imagen.



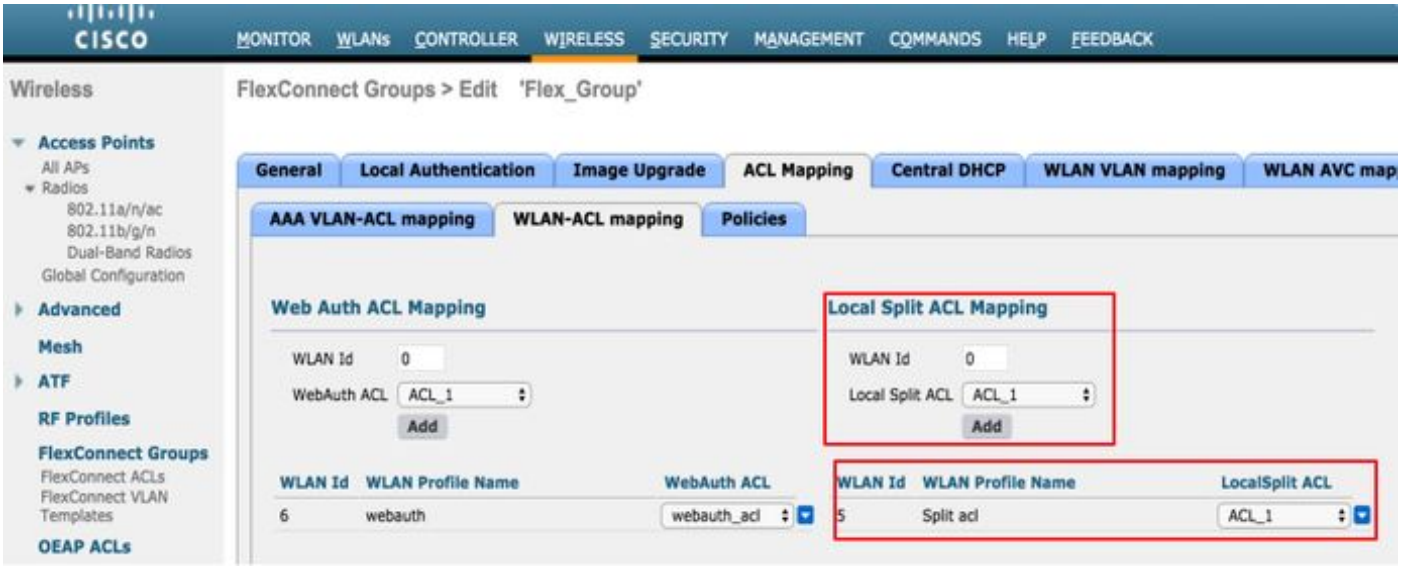
Después de una autenticación acertada L2, cuando el servidor de RADIUS envía el nombre ACL en el par AV reorientar-ACL, éste consigue solicitado directamente el cliente en el AP. Cuando el cliente se traslada al estado de **FUNCIONAMIENTO**, todo el tráfico del cliente se conmuta localmente y el AP para aplicar el ACL.

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

4. Túnel dividido ACL

El Túnel dividido ACL se utiliza con los SSID centralmente conmutados cuando algo del tráfico del cliente necesita ser enviado localmente. Las funciones del Túnel dividido son también una ventaja agregada para la oficina amplían el Punto de acceso (OEAP) puesto donde los clientes en un SSID corporativo pueden hablar con los dispositivos en una red local (impresoras, máquina atada con alambre en un puerto del LAN remoto, o dispositivos de red inalámbrica en un SSID personal) directamente una vez que les mencionan como parte del túnel dividido ACL.

El Túnel dividido ACL se puede configurar encendido según el nivel de grupo del flexconnect, navega a los **grupos de la Tecnología inalámbrica-Flexconnect > selecciona al grupo que usted quiere la configuración > la asignación ACL > la asignación WLAN-ACL > la asignación partida del Local ACL** tal y como se muestra en de la imagen.



Pueden también ser configuradas en según el nivel AP, navegar a la **Tecnología inalámbrica > toda la lengueta de Flexconnect del name> AP > AP > el Local ACL partidos** y agregar el nombre del flexconnect ACL tal y como se muestra en de la imagen.

El Túnel dividido ACL no puede localmente interligar el Multicast/el tráfico de broadcast. El Multicast/el tráfico de broadcast se conmuta centralmente incluso si hace juego el FlexConnect ACL.

Troubleshooting

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