Flexconnect ACL's op WLC configureren

Inhoud

Inleiding

In dit document worden de verschillende ACL-typen (Flexconnect Access Control List) beschreven en hoe deze op het access point (AP) kunnen worden geconfigureerd en gevalideerd.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco draadloze LAN-controller (WLC) met code 8.3 en hoger
- Flexconnect-configuratie op WLC

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco 8540 Series WLC-software met release 8.3.13.0
- 3802 en 3702 AP's die draaien in de flexconnectiviteitsmodus.

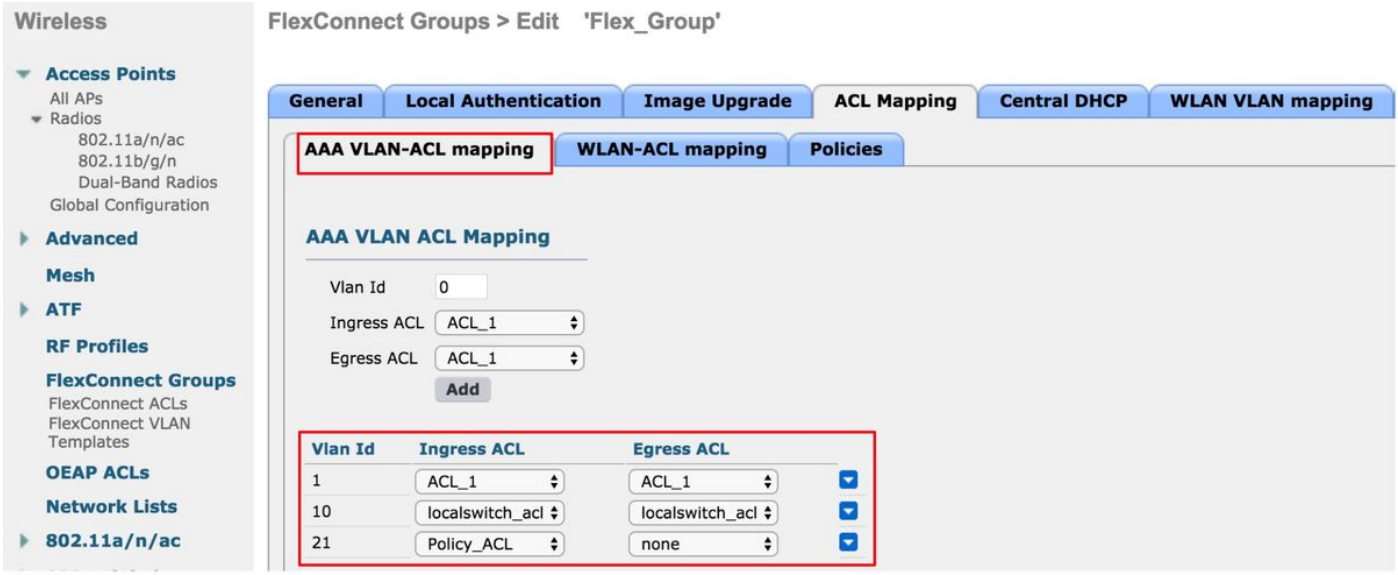
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

ACL-typen

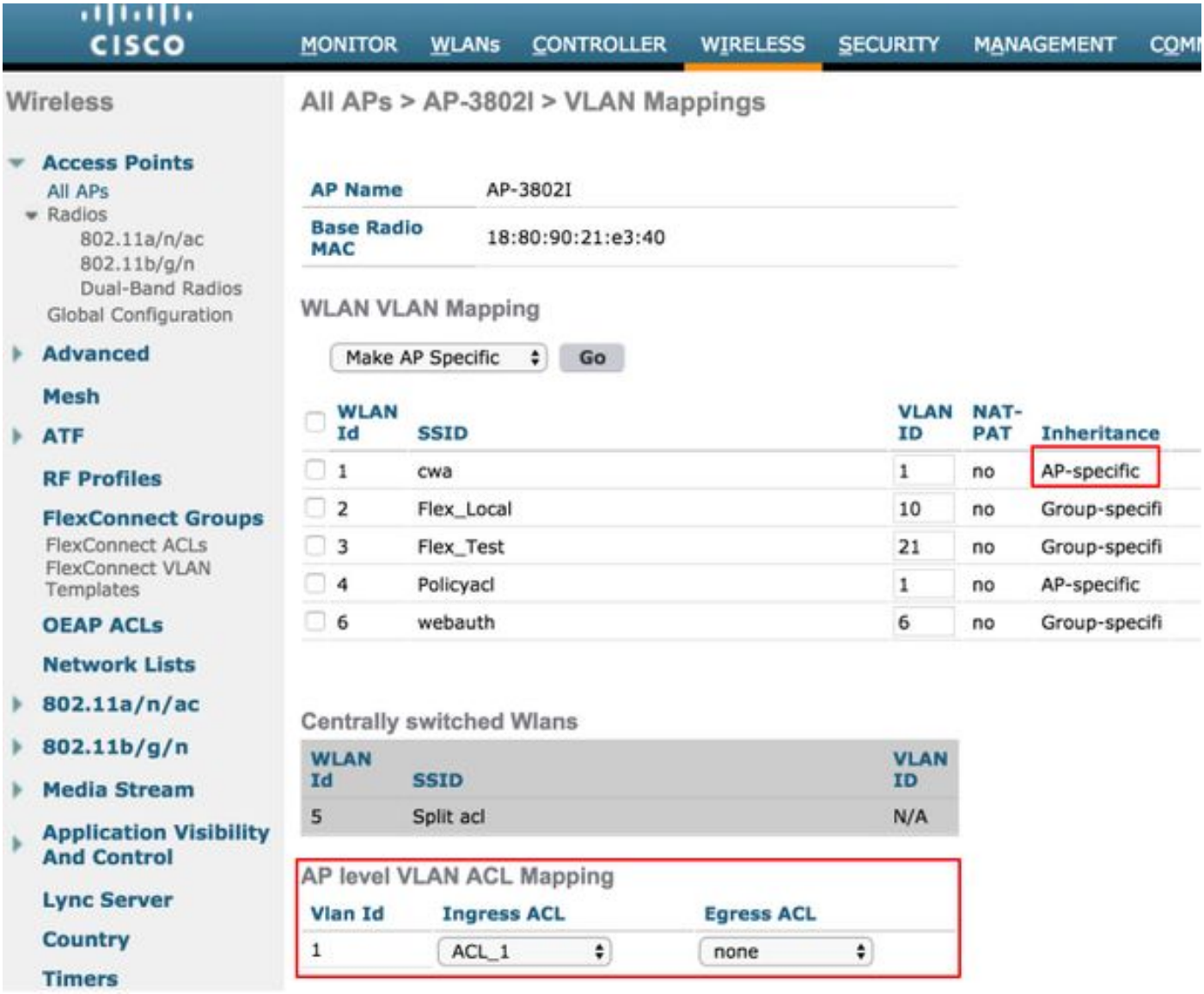
1. VLAN ACL

VLAN ACL is de meest gebruikte ACL en het laat u clientverkeer controleren dat in en uit het VLAN wordt verzonden.

ACL kan worden geconfigureerd zoals in de FlexConnect-groep die de sectie **AAA VLAN-**mapping gebruikt in **Wireless-Flexconnect groepen > ACL-**omzetting **> AAA VLAN-ACL** in de afbeelding.



Het kan ook worden ingesteld zoals op het AP-niveau, navigeer naar **Draadloos > Alle AP's > AP-naam > Flexconnect tab** en klik op **VLAN-mapping** sectie. Hier, moet u eerst de VLAN configuratie AP specifiek maken, waarna u het AP niveau VLAN-mapping zoals in het beeld kunt specificeren.



ACL-richting

U kunt ook de richting specificeren waarin ACL wordt toegepast:

- Ingoers (Ingoers betekent naar de draadloze client)
- uitgang (naar de DS of LAN),
- beide of geen.

Als je dus verkeer wil blokkeren dat bestemd is voor de draadloze client, dan kan je de ingangsrichting gebruiken en als je het verkeer wil blokkeren dat afkomstig is van de draadloze client, kan je de graafrichting gebruiken.

De optie geen wordt gebruikt wanneer u een afzonderlijke ACL wilt indrukken met het gebruik van Verificatie, autorisatie en accounting (AAA)-voorrang. In dit geval, wordt ACL die door de straal server wordt verzonden dynamisch op de client toegepast.

> Opmerking: ACL moet vooraf onder Flexconnect ACL worden ingesteld, anders wordt deze niet toegepast.

Toewijzing van ACL

Wanneer u VLAN ACL's gebruikt, is het ook belangrijk om deze overwegingen met betrekking tot VLAN-mappings op Flexconnect AP's te begrijpen:

- Als het VLAN is geconfigureerd met het gebruik van de FlexConnect-groep, wordt de corresponderende ACL die is geconfigureerd op de FlexConnect-groep toegepast.
- Als een VLAN op zowel de FlexConnect-groep als ook op AP (als een AP-specifieke configuratie) wordt geconfigureerd dan heeft de AP ACL-configuratie voorrang.
- Als AP-specifieke ACL op geen enkele, dan wordt geen ACL toegepast.
- Als het VLAN dat van de AAA is geretourneerd niet aanwezig is op de AP, valt de client terug naar de standaard VLAN dat is geconfigureerd voor het draadloze LAN (WLAN) en krijgt elke ACL die aan dat standaard VLAN is toegewezen voorrang.

Controleer of ACL op AP is toegepast

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

1. Wave 2 access points

Op een golf 2 AP, kunt u verifiëren of ACL daadwerkelijk naar AP wordt geduwd met de opdracht **tonen flexconnect VLAN-acl**. Hier, kunt u ook aantal van overgeslagen en geworpen pakketten voor elke ACL zien.

```
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's

Op het niveau van AP, kunt u bevestigen als de ACL configuratie met twee manieren naar AP is gedrukt:

- Gebruik de opdracht **Show access-lists** die toont als alle VLAN ACL's op AP zijn geconfigureerd:

```
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
```

U kunt ook de activiteit controleren die op elke ACL gebeurt, de gedetailleerde uitvoer van die ACL controleren en de slagtelling voor elke lijn zien:

```
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)
```

- Aangezien VLAN ACL's op de Gigabit-interface worden toegepast, kunt u bevestigen of ACL correct wordt toegepast. Controleer de subinterface-uitvoer zoals hieronder wordt getoond:

```
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
```

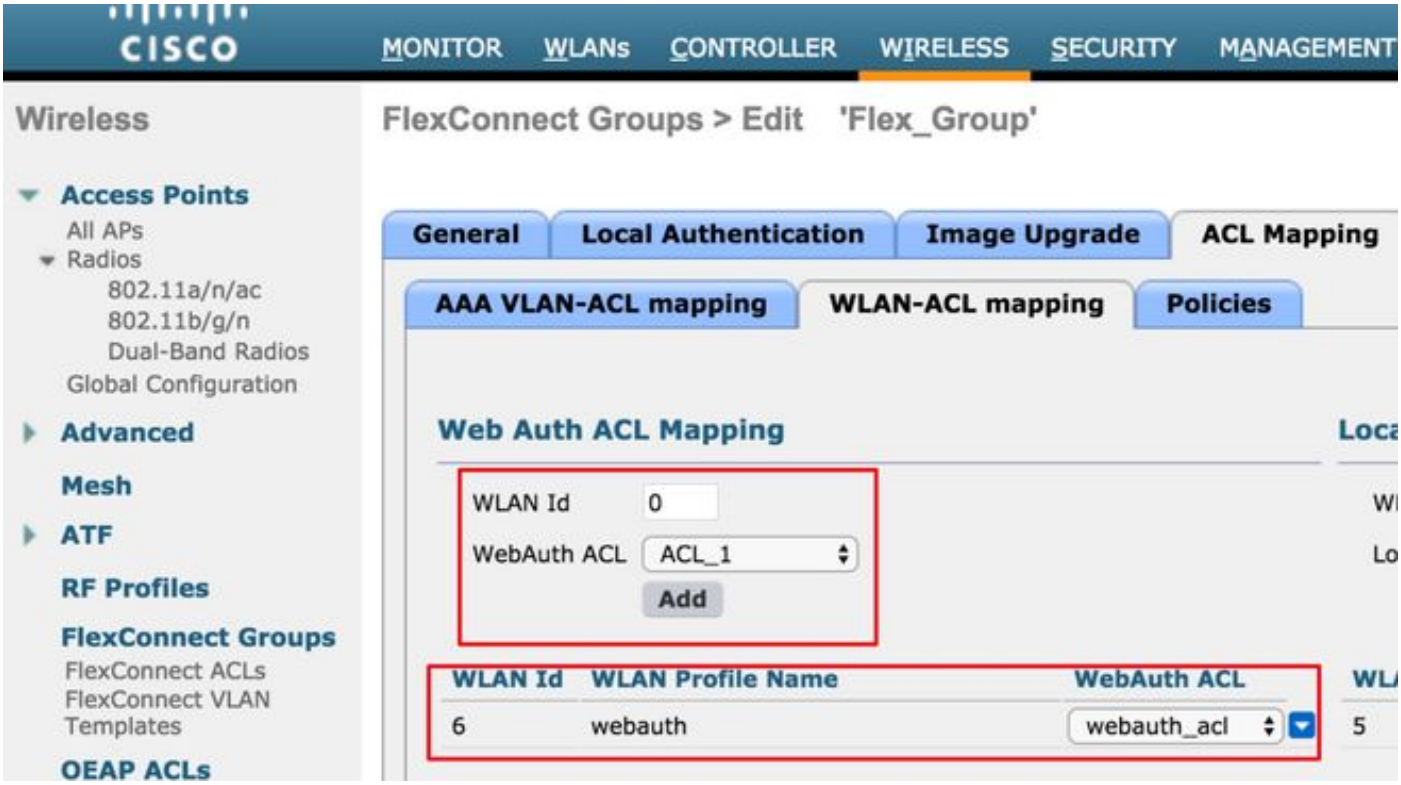
2. Webauth ACL

Webauth ACL wordt gebruikt in het geval van een WebEth/Webpassthrough Service Set Identifier (SSID) die is ingeschakeld voor flexconnect lokale switching. Dit wordt gebruikt als pre-authenticatie ACL en staat clientverkeer toe naar de redirect server. Zodra de omleiding is voltooid en de client **is** uitgerust met **RUN**, stopt ACL om deze uit te voeren.

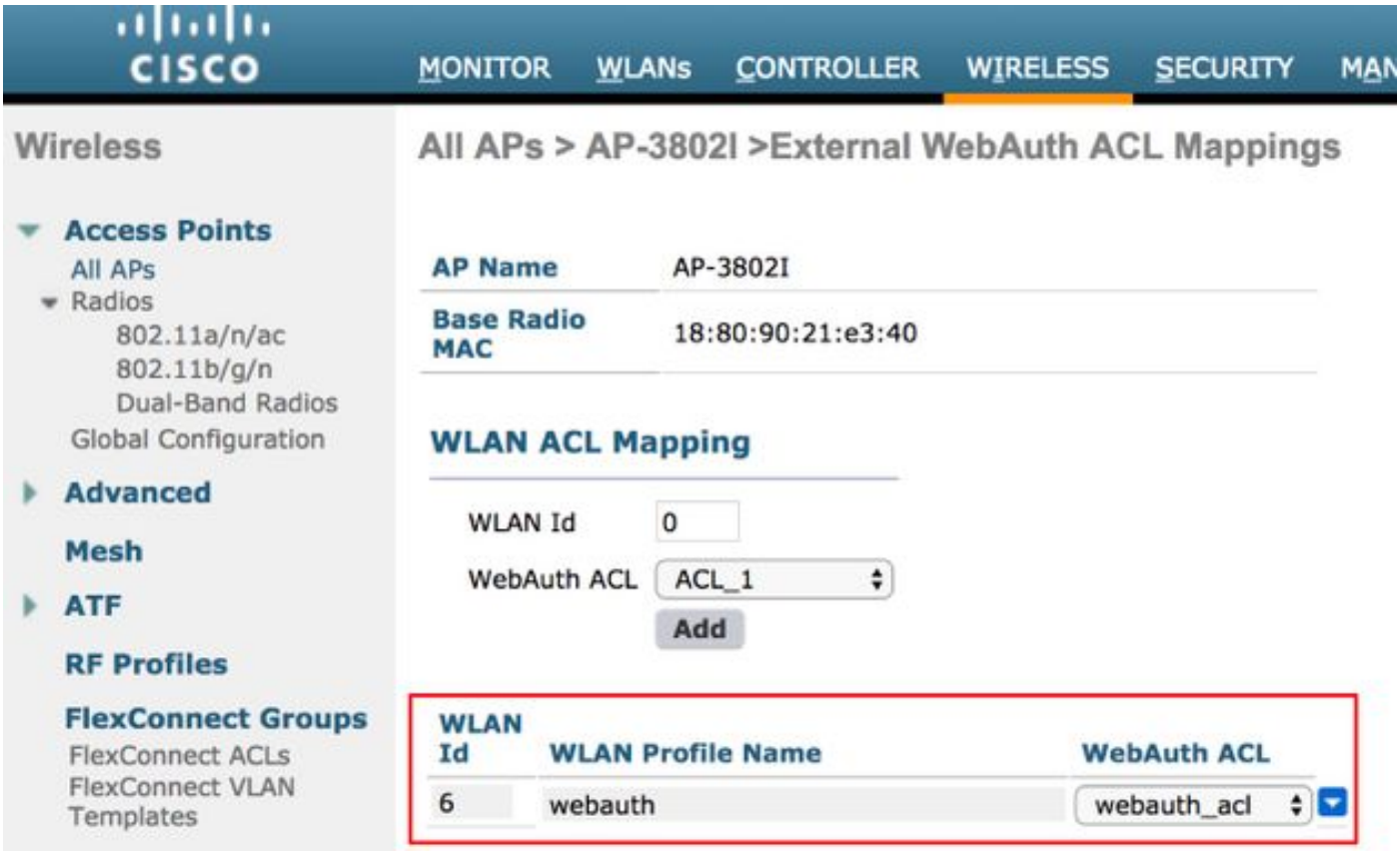
Webauth ACL kan worden toegepast op WLAN-niveau, AP-niveau of flexconnect-groepsniveau. Een AP-specifieke ACL heeft de hoogste prioriteit, terwijl WLAN ACL het laagste heeft. Als alle drie worden toegepast, wordt AP Specific gevolgd door Flex ACL en dan WLAN Global Specific ACL.

Er kunnen maximaal 16 Web-Auth ACL’s op een AP worden ingesteld.

Het kan op het niveau van de flexibele groep worden toegepast, navigeer naar **Draadloos > Flexconnect groepen > Selecteer de groep die u wilt configureren > ACL-mapping > WLAN-ACL** kaarten **> Toewijzing van Web AUth ACL** zoals in het beeld weergegeven wordt.



ACL kan op het niveau van AP worden toegepast, navigeer naar **Draadloos >Alle AP's >AP naam >Flexconnect tabblad > Externe WebAuthentication ACL's > WLAN ACL's** zoals in de afbeelding getoond.



ACL kan op WLAN-niveau worden toegepast, navigeer naar **WLAN > WLAN_ID > Layer 3 > Webex FlexAcl** zoals in de afbeelding.

Op Cisco IOS® AP, kunt u verifiëren of ACL op de client werd toegepast. Controleer de uitvoer van **showcontrollers dot11radio 0 client** (of 1 als de client verbinding maakt met de A-radio) zoals hier wordt getoond:

```
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
```

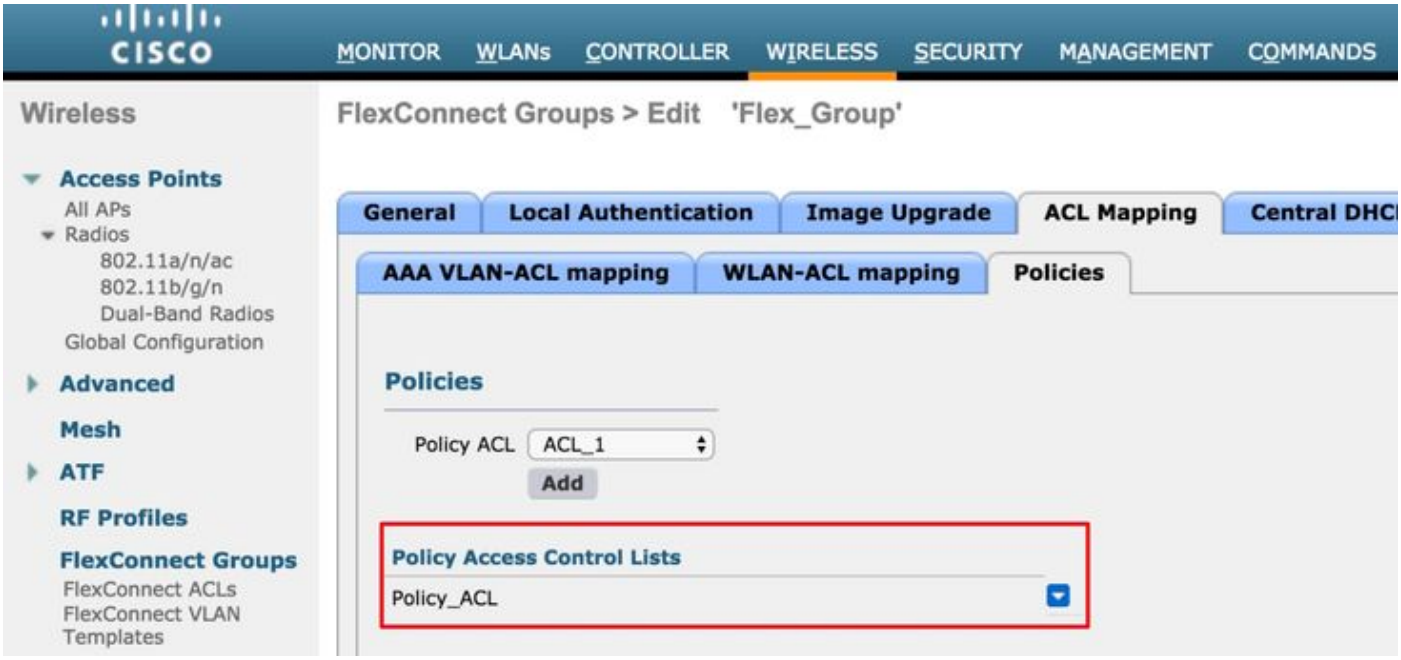
3. Web beleid ACL

WebexPolicy ACL wordt gebruikt voor scenario's voor voorwaardelijk Web redirect, Splash Page Web Redirect en Central WebEth.

Er zijn twee modi van configuratie beschikbaar voor WebPolicy WLAN's met Flex ACL's:

1. Flexconnect-groep

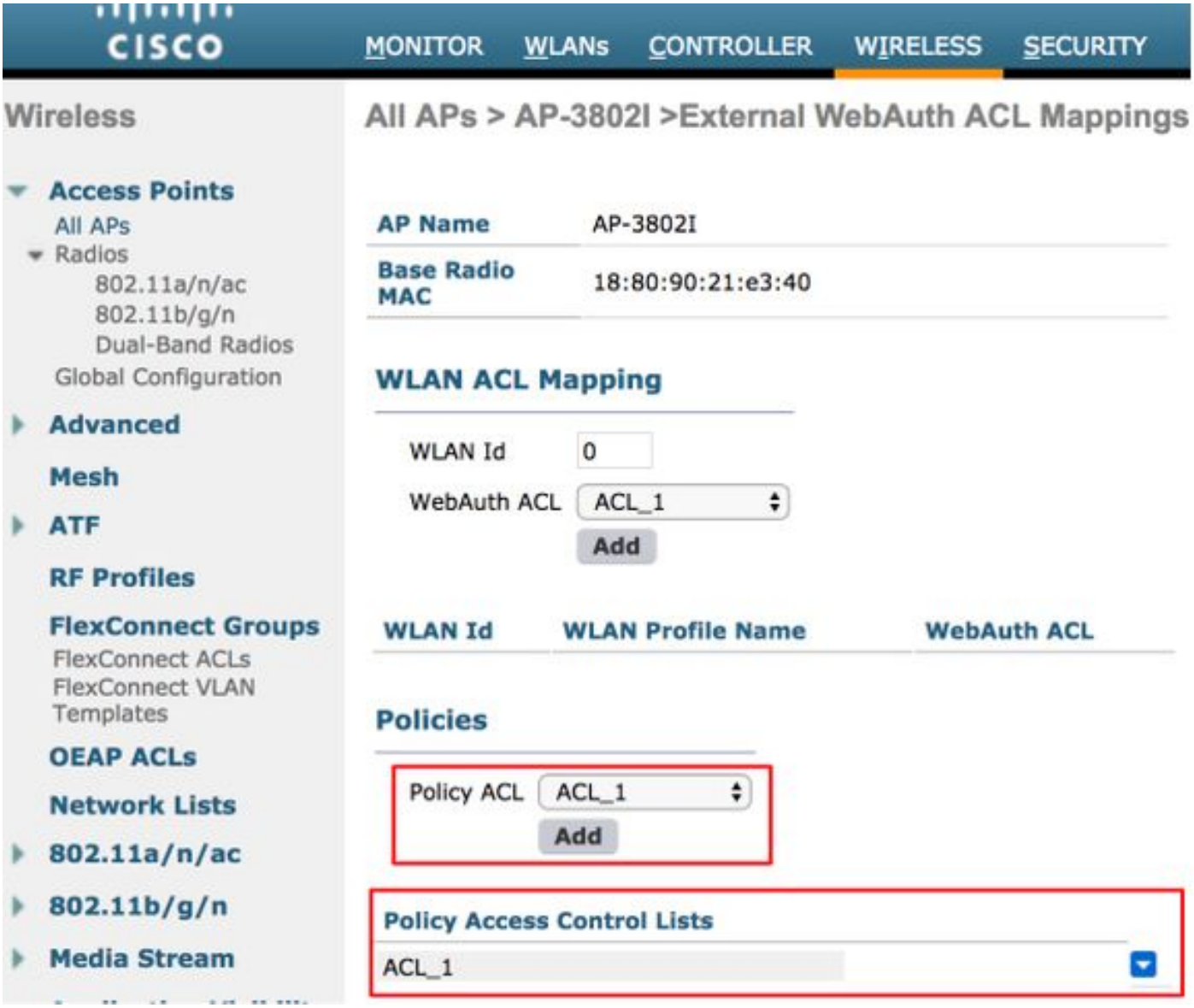
Alle APs in de groep FlexConnect ontvangen ACL die wordt gevormd. Dit kan worden ingesteld terwijl u naar **Wireless-Flexconnect groepen** navigeert **> Selecteer de groep die u wilt configureren > ACL-mapping > Beleid**, en voeg de naam van de Beleids-ACL toe zoals in de afbeelding:



2. Specifieke AP

AP waarvoor de configuratie wordt gedaan ontvangt ACL, geen andere APs worden beïnvloed. Dit kan worden ingesteld terwijl u naar **Draadloos** navigeert **> Alle AP's > AP-naam >**

Flexconnect tab > Externe WebVerificatie ACL's > Beleid zoals in de afbeelding weergegeven.



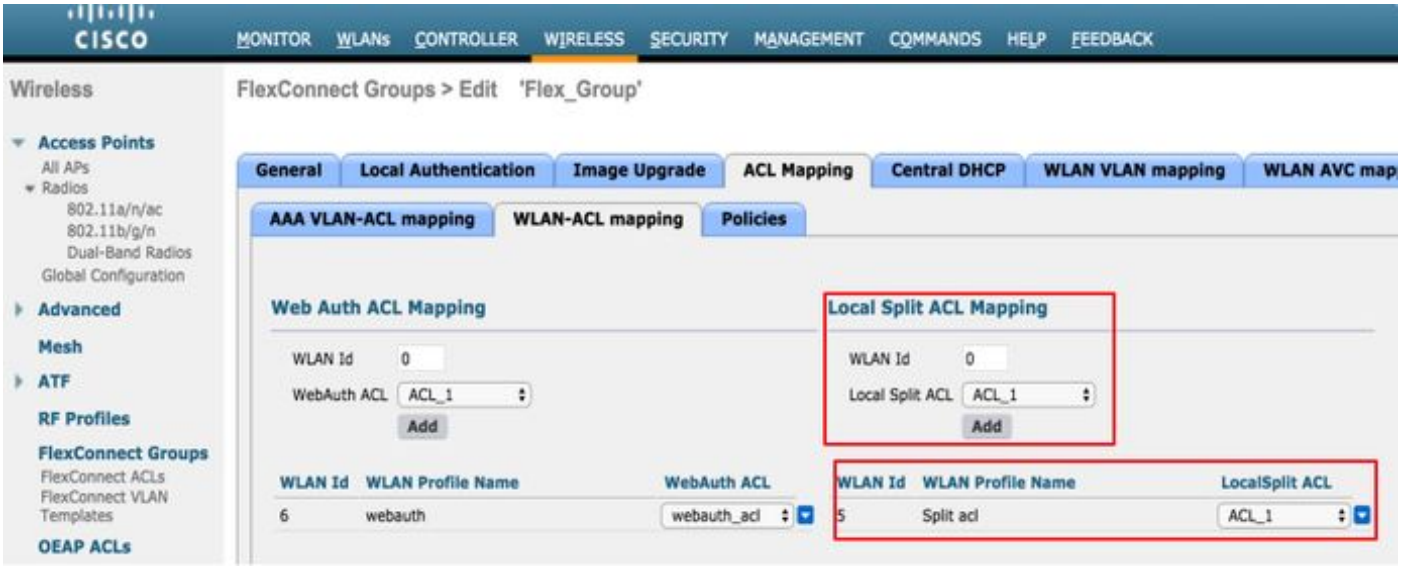
Na een succesvolle L2-verificatie, wanneer de Straalserver de ACL-naam in het AV-paar opnieuw direct opsturen, wordt dit direct toegepast op de client op AP. Wanneer de client naar **RUN**-status gaat, wordt al het clientverkeer lokaal geschakeld en de AP stopt om ACL toe te passen.

Er kunnen een maximum of 32 WebPolicy ACL's worden ingesteld op een AP. 16 AP-specifiek en 16 FlexConnect-groep.

4. Split Tunnel ACL

Split Tunneling ACL's wordt gebruikt met centraal geschakeld SSID's wanneer een deel van het clientverkeer lokaal moet worden verzonden. De functie Split Tunneling is ook een extra voordeel voor de instelling Office Extend access point (OEAP), waar klanten op een Corporate SSID direct met apparaten op een lokaal netwerk kunnen praten (printers, bekabelde machine op een Remote LAN-poort of draadloze apparaten op een persoonlijk SSID) zodra ze als deel van de gesplitste tunnelACL zijn vermeld.

Met de ACL's (splitter tunneling) van ACL's kan op het niveau van de flexibele groep worden ingesteld, navigeer naar **Wireless-Flexconnect groepen > Selecteer de groep die u wilt configureren > ACL-afbeelding > WLAN-ACL-omzetting > Toewijzing van lokale ACL-splitter** zoals in de afbeelding.



Ze kunnen ook worden geconfigureerd op het niveau van AP, navigeer naar **Draadloos > Alle AP > AP naam > Flexconnect tab > Local Split ACL's** en voeg de naam van de flexconnect ACL's toe zoals in de afbeelding.

Split-tunneling ACL's kunnen niet lokaal multicast/breedbandverkeer overbruggen. Multicast/broadcast-verkeer is centraal geschakeld, zelfs als dit overeenkomt met FlexConnect ACL.

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.