Configurazione degli ACL Flexconnect sul WLC

Sommario

Introduzione

In questo documento vengono descritti i vari tipi di elenchi di controllo di accesso (ACL, Access Control List) di flexconnect e viene spiegato come configurarli e convalidarli sul punto di accesso.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Wireless LAN Controller (WLC) con codice 8.3 e versioni successive
- Configurazione Flexconnect sul WLC

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Il Cisco serie 8540 WLC con software versione 8.3.13.0.
- 3802 e 3702 AP in modalità flexconnect.

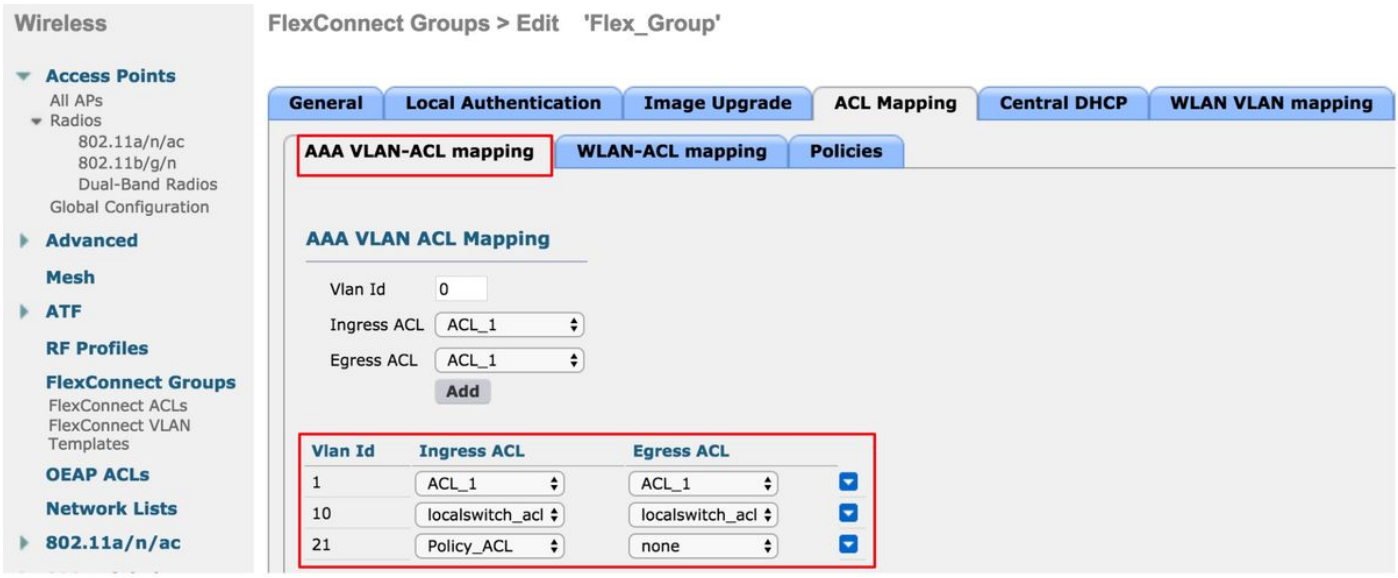
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Tipi di ACL

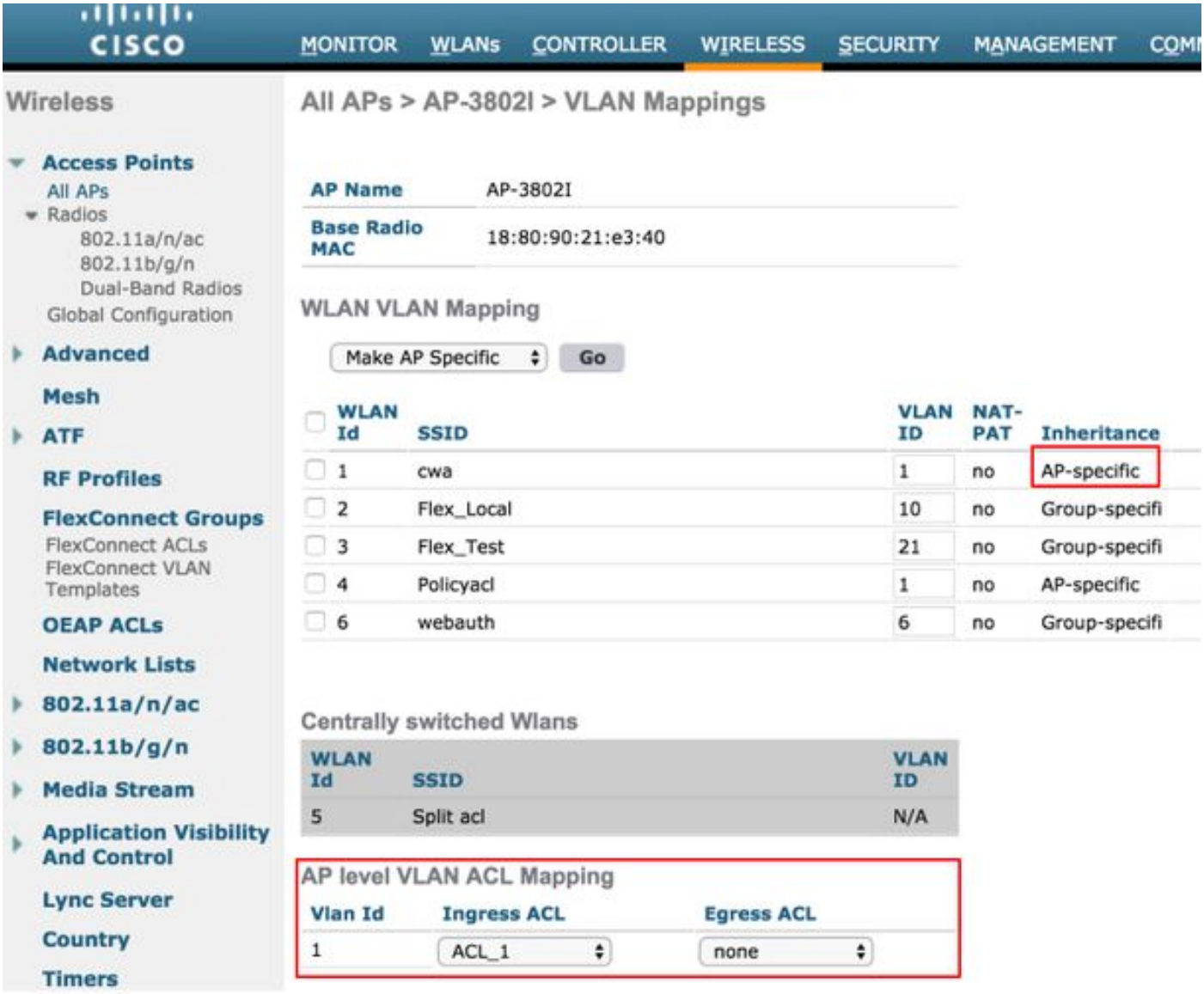
1. ACL VLAN

Gli ACL VLAN sono gli ACL più utilizzati e consentono di controllare il traffico dei client in entrata e in uscita dalla VLAN.

Èpossibile configurare l'ACL come per il gruppo flexconnect che usa la sezione di mappatura **AAA VLAN-ACL** in **Gruppi Wireless-Flexconnect > mappatura ACL > mappatura AAA VLAN-ACL** come mostrato nell'immagine.



Può anche essere configurato in base al livello dell'access point, selezionare **Wireless > Tutti gli access point > Nome access point > Scheda Flexconnect** e fare clic sulla sezione **Mapping delle VLAN**. Qui è necessario specificare prima la configurazione VLAN AP, quindi è possibile specificare il mapping VLAN-ACL del livello AP, come mostrato nell'immagine.



Direzioni ACL

Èinoltre possibile specificare la direzione in cui applicare l'ACL:

- In ingresso (in ingresso significa verso il client wireless)
- in uscita (verso il DS o la LAN),
- entrambi o nessuno.

Pertanto, se si desidera bloccare il traffico destinato al client wireless, è possibile utilizzare la direzione in entrata e, se si desidera bloccare il traffico proveniente dal client wireless, è possibile utilizzare la direzione in uscita.

L'opzione none (nessuno) viene usata quando si desidera eseguire il push di un ACL separato con l'uso dell'override Authentication, Authorization, and Accounting (AAA). In questo caso, l'ACL inviato dal server radius viene applicato dinamicamente al client.

> **Nota:** Prima di usare il comando Flexconnect, l'ACL deve essere configurato nell'ACL di connessione, altrimenti non viene applicato.

Considerazioni sul mapping degli ACL

Quando si usano gli ACL VLAN, è importante conoscere anche queste considerazioni rispetto ai mapping VLAN sugli access point flexconnect:

- Se la VLAN è configurata con l'uso del gruppo FlexConnect, viene applicato l'ACL corrispondente configurato sul gruppo FlexConnect.
- Se una VLAN è configurata sia sul gruppo FlexConnect che sull'access point (come configurazione specifica dell'access point), la configurazione dell'access point ha la precedenza.
- Se l'ACL specifico dell'access point è configurato su nessuno, non viene applicato alcun ACL.
- Se la VLAN restituita dal server AAA non è presente nell'access point, il client torna alla VLAN predefinita configurata per la LAN wireless (WLAN) e ha la priorità qualsiasi ACL mappato a tale VLAN predefinita.

Verifica dell'applicazione dell'ACL all'access point

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

1. Punti di accesso Wave 2

Su un access point wave 2, è possibile verificare se l'ACL viene effettivamente spinto all'access point con il comando **show flexconnect vlan-acl**. Qui è possibile anche vedere il numero di pacchetti passati e scartati per ciascun 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

A livello di access point, è possibile verificare se la configurazione dell'ACL è stata sottoposta a push nell'access point in due modi:

- Usare il comando **show access-lists** per verificare se tutti gli ACL VLAN sono configurati sull'access point:

```
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
```

Èpossibile anche monitorare l'attività che avviene su ciascun ACL, controllare l'output dettagliato dell'ACL e verificare il numero di accessi per ciascuna riga:

```
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)
```

- Poiché gli ACL VLAN sono applicati all'interfaccia Gigabit, è possibile verificare se l'ACL è applicato correttamente. Controllare l'uscita dell'interfaccia secondaria come mostrato di seguito:

```
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
```

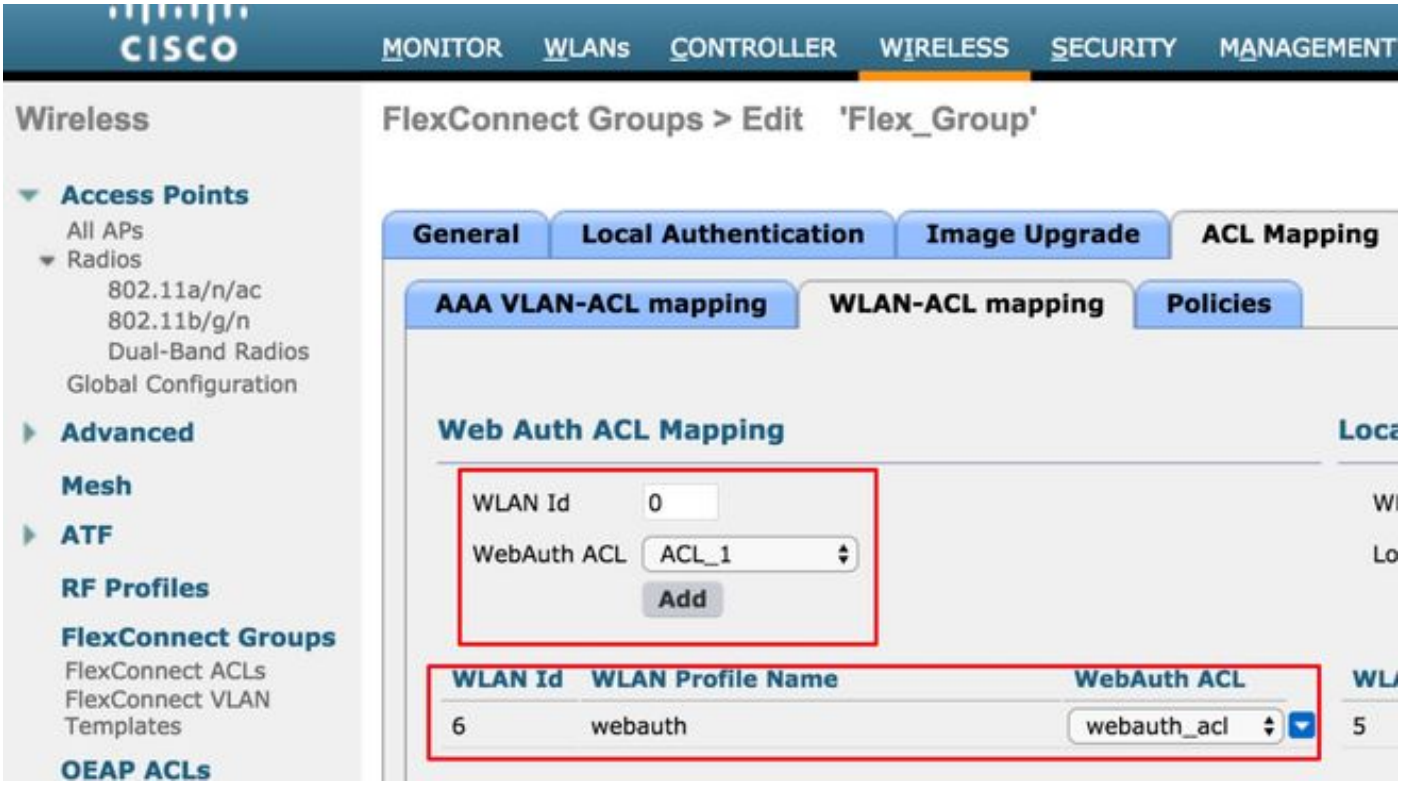
2. ACL Webauth

L'ACL Webauth viene usato nel caso di un SSID (Service Set Identifier) Webauth/Webpassthrough abilitato per la commutazione locale flexconnect. Viene usato come ACL di preautenticazione e consente il traffico del client verso il server di reindirizzamento. Una volta completato il reindirizzamento e impostato lo stato **RUN** per il client, l'ACL si interrompe per renderlo effettivo.

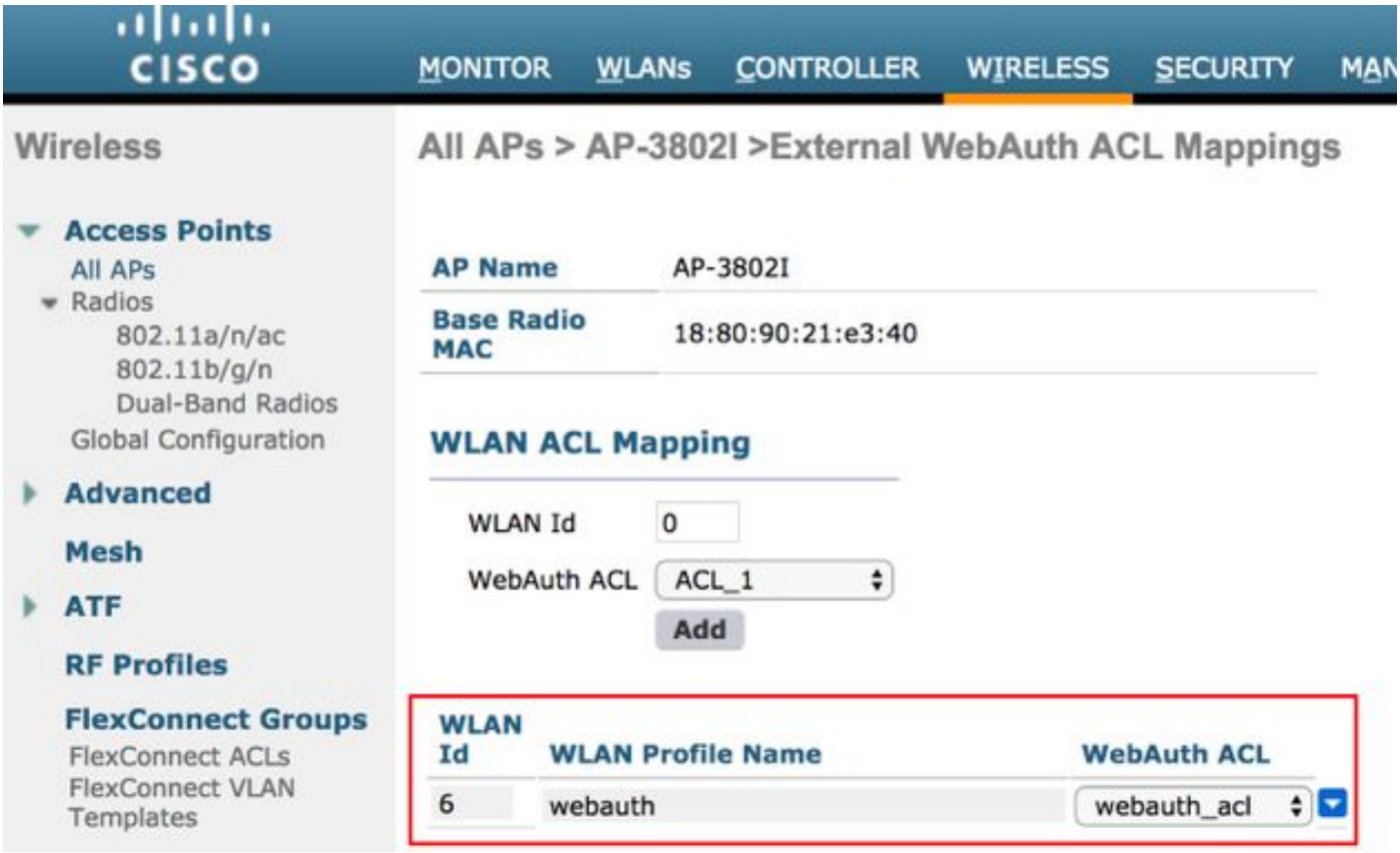
L'ACL Webauth può essere applicato a livello di WLAN, AP o gruppo flexconnect. Un ACL specifico dell'access point ha la priorità più alta, mentre l'ACL della WLAN ha la priorità più bassa. Se vengono applicati tutti e tre gli ACL, quello specifico dell'access point ha la precedenza, seguito dall'ACL Flex e quindi dall'ACL specifico globale della WLAN.

In un access point possono essere configurati un massimo di 16 ACL Web-Auth.

Può essere applicato a livello di gruppo flexconnect, selezionare **Wireless > Gruppi Flexconnect > Selezionare il gruppo che si desidera configurare > Mappatura ACL > Mappatura WLAN-ACL > Mappatura ACL Web Auth**, come mostrato nell'immagine.



L'ACL può essere applicato al livello dell'access point. Selezionare **Wireless >All AP's >AP name >Flexconnect tab > External Web Authentication ACLs > WLAN ACL** (Tutti gli access point > Nome access point > Scheda Flexconnect > ACL di autenticazione Web esterna > ACL WLAN), come mostrato nell'immagine.



L'ACL può essere applicato a livello di WLAN. Selezionare **WLAN > WLAN_ID > Layer 3 > WebAuth FlexAcl**, come mostrato nell'immagine.

Sull'access point Cisco IOS®, è possibile verificare se l'ACL è stato applicato al client. Controllare l'output del **client show controller dot11radio 0** (o 1 se il client si connette alla radio A) come mostrato di seguito:

```
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
```

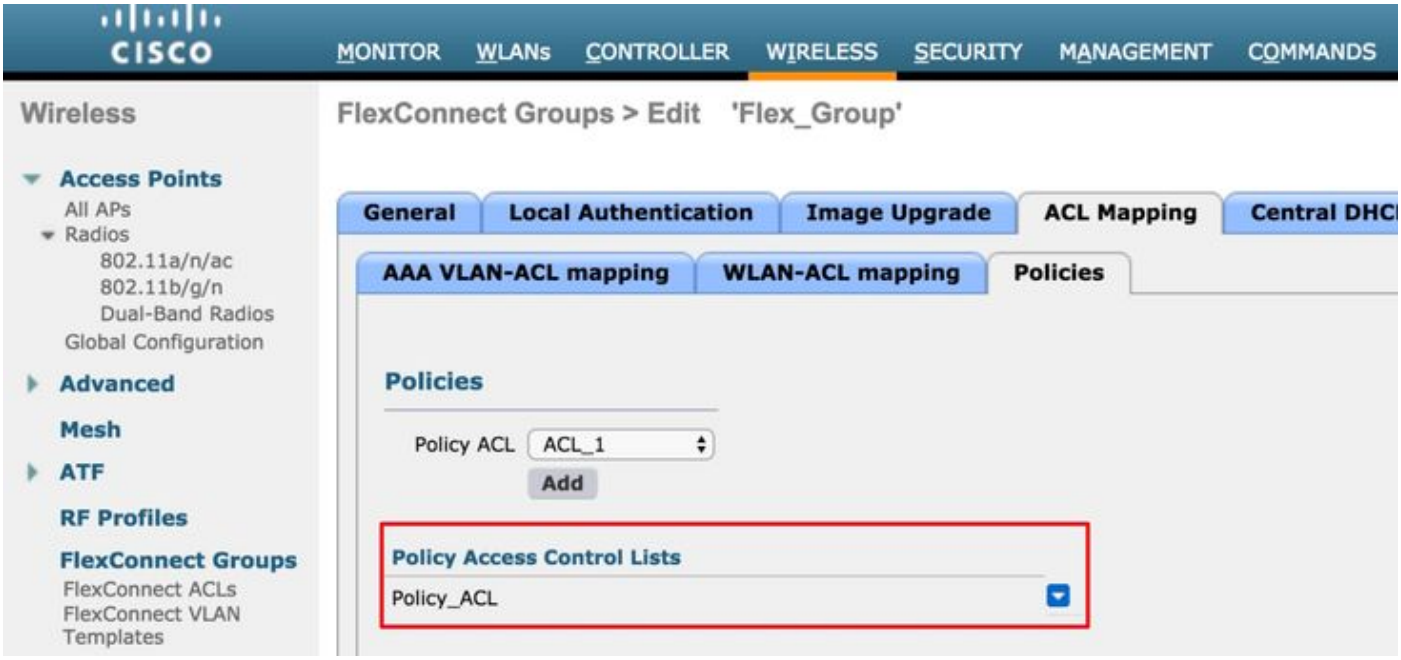
3. ACL del criterio Web

L'ACL WebPolicy viene utilizzato per gli scenari Web Redirect condizionale, Web Redirect pagina iniziale e WebAuth centrale.

Per le WLAN WebPolicy con ACL Flex, sono disponibili due modalità di configurazione:

1. Gruppo Flexconnect

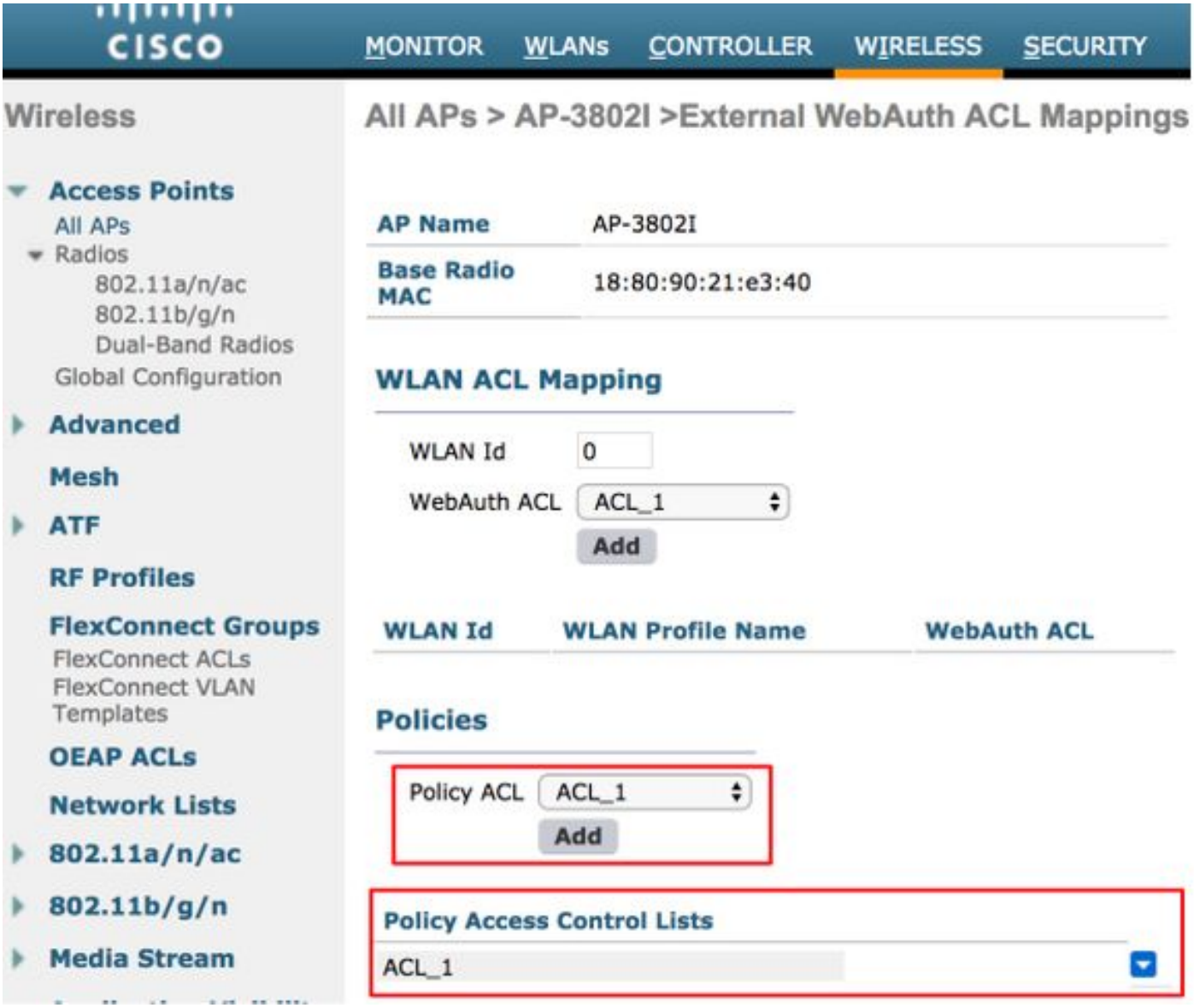
Tutti gli access point nel gruppo FlexConnect ricevono l'ACL configurato. È possibile configurare questa impostazione mentre si passa a **Gruppi Wireless-Flexconnect > Selezionare il gruppo che si desidera configurare > Mapping ACL > Criteri**, quindi aggiungere il nome dell'ACL del criterio come mostrato nell'immagine:



2. Specifiche del punto di accesso

L'ACL viene ricevuto dall'access point per cui è stata eseguita la configurazione, non vi sono problemi per gli altri access point. È possibile configurare questa opzione mentre si passa a **Wireless > Tutti gli access point > Nome access point >**

Scheda Flexconnect > ACL WebAuthentication esterni > Criteri come mostrato nell'immagine.



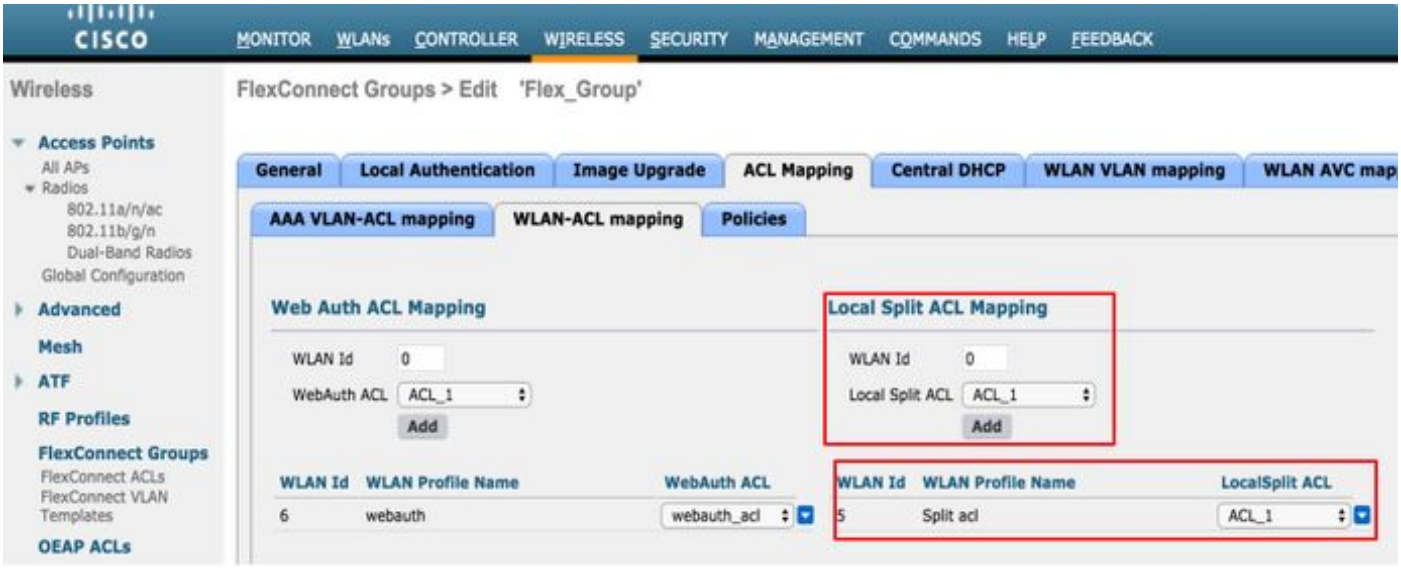
Se l'autenticazione L2 ha esito positivo, quando il server RADIUS invia il nome ACL nella coppia AV reindirizzamento-ACL, il nome viene applicato direttamente al client nell'access point. Quando il client passa allo stato **RUN**, tutto il traffico viene commutato localmente e l'access point si arresta per applicare l'ACL.

Èpossibile configurare un massimo di 32 ACL WebPolicy su un punto di accesso. 16 ACL specifici per ogni punto di accesso e 16 ACL specifici per ogni gruppo FlexConnect.

4. ACL con tunnel suddiviso

Gli ACL di tunneling ripartito vengono usati con gli SSID commutati centralmente quando parte del traffico del client deve essere inviato localmente. La funzionalità di tunneling ripartito è un ulteriore vantaggio della configurazione di Office Extend Access Point (OEAP), in cui i client di un SSID aziendale possono comunicare direttamente con i dispositivi di una rete locale (stampanti, computer cablati su una porta LAN remota o dispositivi wireless su un SSID personale) una volta menzionati come parte dell'ACL del tunnel ripartito.

Èpossibile configurare gli ACL di tunneling suddivisi in base al livello di gruppo della connessione flessibile, selezionare **Gruppi Wireless-Flexconnect > Selezionare il gruppo da configurare > Mapping ACL > Mapping WLAN-ACL > Mapping ACL suddiviso locale**, come mostrato nell'immagine.



Possono anche essere configurati a livello di access point, selezionare **Wireless > Tutti gli access point > Nome access point > scheda Flexconnect > ACL suddivisi in locale** e aggiungere il nome dell'ACL flexconnect come mostrato nell'immagine.

Gli ACL di tunneling ripartito non possono unire localmente il traffico multicast/broadcast. Il traffico multicast/broadcast viene commutato centralmente anche se corrisponde all'ACL FlexConnect.

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.