Configuration des listes de contrôle d'accès Flexconnect sur WLC

Contenu

Introduction

Ce document décrit les différents types de listes de contrôle d'accès flexconnect (ACL) et comment ils peuvent être configurés et validés sur le point d'accès (AP).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Contrôleur LAN sans fil Cisco (WLC) qui exécute le code 8.3 et supérieur
- Configuration de Flexconnect sur le WLC

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- WLC de la gamme Cisco 8540 qui exécute le logiciel version 8.3.133.0.
- AP 3802 et 3702 qui s'exécute en mode flexconnect.

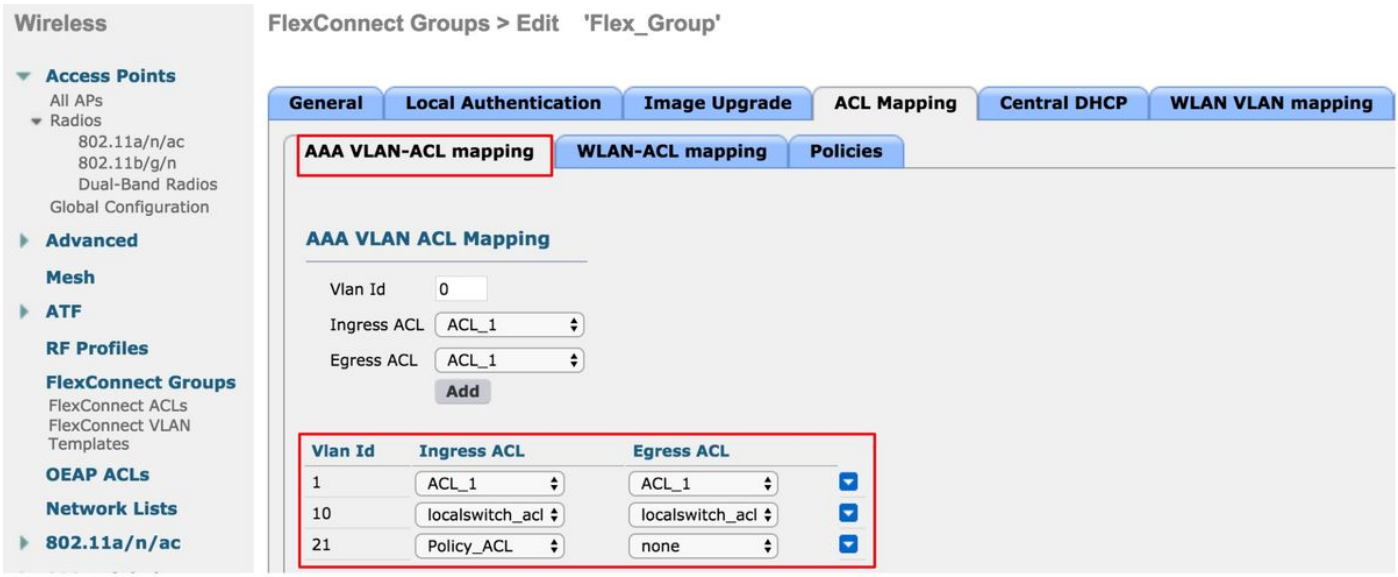
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Types ACL

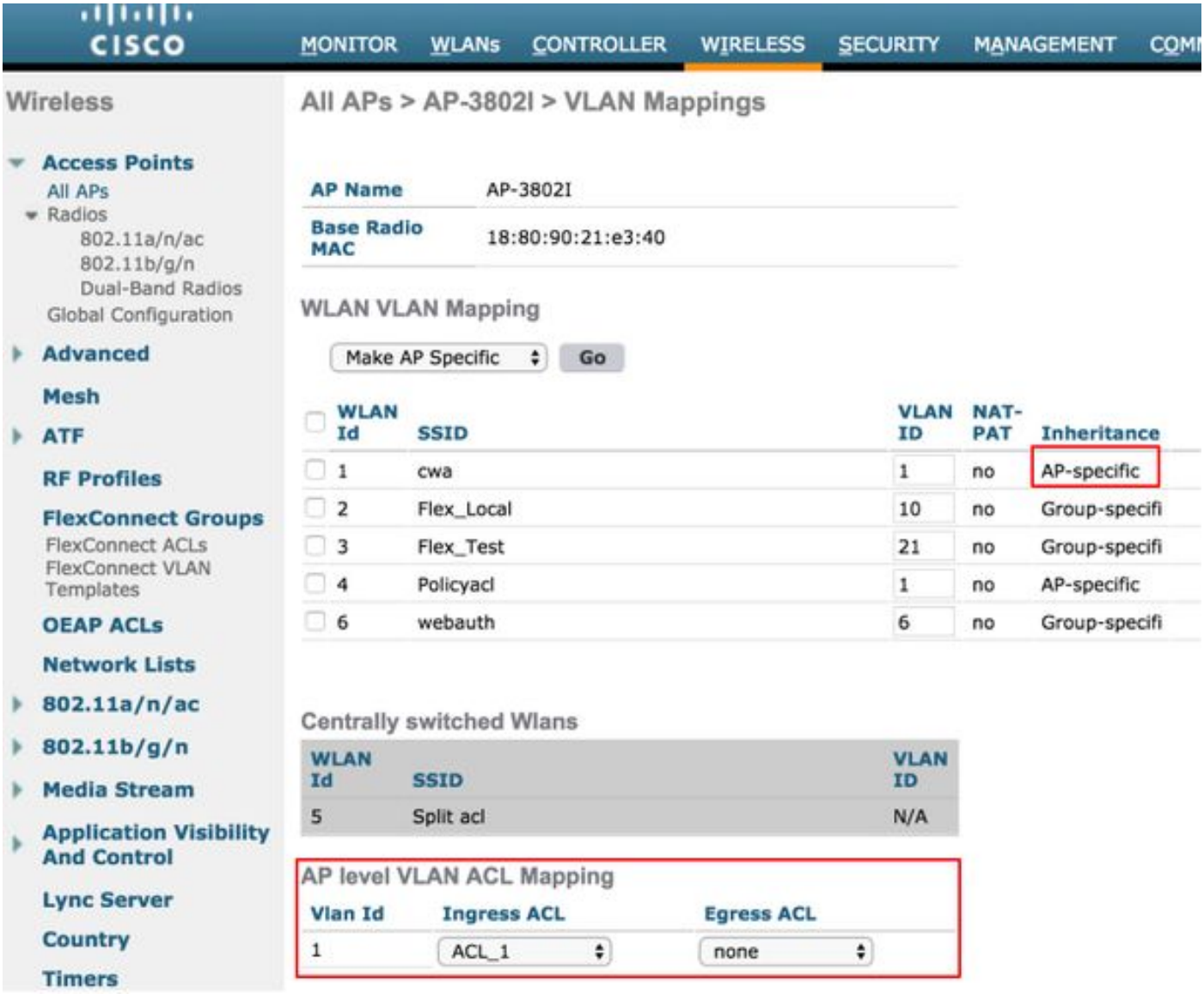
1. ACL VLAN

La liste de contrôle d'accès VLAN est la liste de contrôle d'accès la plus couramment utilisée et elle vous permet de contrôler le trafic client qui est envoyé à l'intérieur et à l'extérieur du VLAN.

La liste de contrôle d'accès peut être configurée conformément au groupe flexconnect qui utilise la section de mappage **AAA VLAN-ACL** dans **Groupes Wireless-Flexconnect > Mappage ACL > Mappage AAA VLAN-ACL** comme illustré dans l'image.



Il peut également être configuré en fonction du niveau AP, naviguez jusqu'à **Wireless > All AP's > AP name > Flexconnect tab** et cliquez sur **VLAN mappings** section. Ici, vous devez d'abord rendre l'AP de configuration VLAN spécifique, après quoi vous pouvez spécifier le mappage VLAN-ACL de niveau AP comme indiqué dans l'image.



Itinéraires des listes de contrôle d'accès

Vous pouvez également spécifier la direction dans laquelle la liste de contrôle d'accès est appliquée :

- Entrée (entrée signifie vers le client sans fil)
- Sortie (vers le DS ou le LAN),
- les deux ou aucun.

Ainsi, si vous souhaitez bloquer le trafic destiné au client sans fil, vous pouvez utiliser la direction d'entrée et si vous souhaitez bloquer le trafic provenant du client sans fil, vous pouvez utiliser la direction de sortie.

L'option no est utilisée lorsque vous souhaitez pousser une liste de contrôle d'accès distincte avec l'utilisation de la substitution AAA (Authentication, Authorization, and Accounting). Dans ce cas, la liste de contrôle d'accès envoyée par le serveur radius est appliquée de manière dynamique au client.

> **Note**: La liste de contrôle d'accès doit être configurée sous la liste de contrôle d'accès Flexconnect au préalable, sinon elle ne sera pas appliquée.

Considérations relatives au mappage des listes de contrôle d’accès

Lorsque vous utilisez des listes de contrôle d'accès VLAN, il est également important de comprendre ces considérations en ce qui concerne les mappages VLAN sur les points d'accès flexconnect :

- Si le VLAN est configuré avec l'utilisation du groupe FlexConnect, la liste de contrôle d'accès correspondante configurée sur le groupe FlexConnect est appliquée.
- Si un VLAN est configuré à la fois sur le groupe FlexConnect et aussi sur le point d'accès (en tant que configuration spécifique à un point d'accès), la configuration de la liste de contrôle d'accès AP a la priorité.
- Si la liste de contrôle d'accès spécifique au point d'accès est configurée sur no, aucune liste de contrôle d'accès n'est appliquée.
- Si le VLAN qui a été renvoyé de l'AAA n'est pas présent sur l'AP, le client revient au VLAN par défaut configuré pour le LAN sans fil (WLAN) et toute liste de contrôle d'accès mappée à ce VLAN par défaut est prioritaire.

Vérifier si la liste de contrôle d’accès est appliquée sur le point d’accès

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

1. Points d'accès Wave 2

Sur un point d'accès de vague 2, vous pouvez vérifier si la liste de contrôle d'accès est effectivement poussée vers le point d'accès à l'aide de la commande **show flexconnect vlan-acl**. Ici, vous pouvez également voir le nombre de paquets passés et abandonnés pour chaque liste de contrôle d’accès.

```
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. Points d'accès Cisco IOS®

Au niveau du point d'accès, vous pouvez valider si la configuration de la liste de contrôle d'accès a été poussée vers le point d'accès de deux manières :

- Utilisez la commande **show access-lists** qui indique si toutes les listes de contrôle d'accès VLAN sont configurées sur le point d'accès :

```
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
```

Vous pouvez également surveiller l'activité qui se produit sur chaque liste de contrôle d'accès, vérifier le résultat détaillé de cette liste et voir le nombre de résultats pour chaque ligne :

```
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)
```

- Puisque les listes de contrôle d'accès VLAN sont appliquées sur l'interface Gigabit, vous pouvez valider si la liste de contrôle d'accès est appliquée correctement. Vérifiez le résultat de la sous-interface comme indiqué ici :

```
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
```

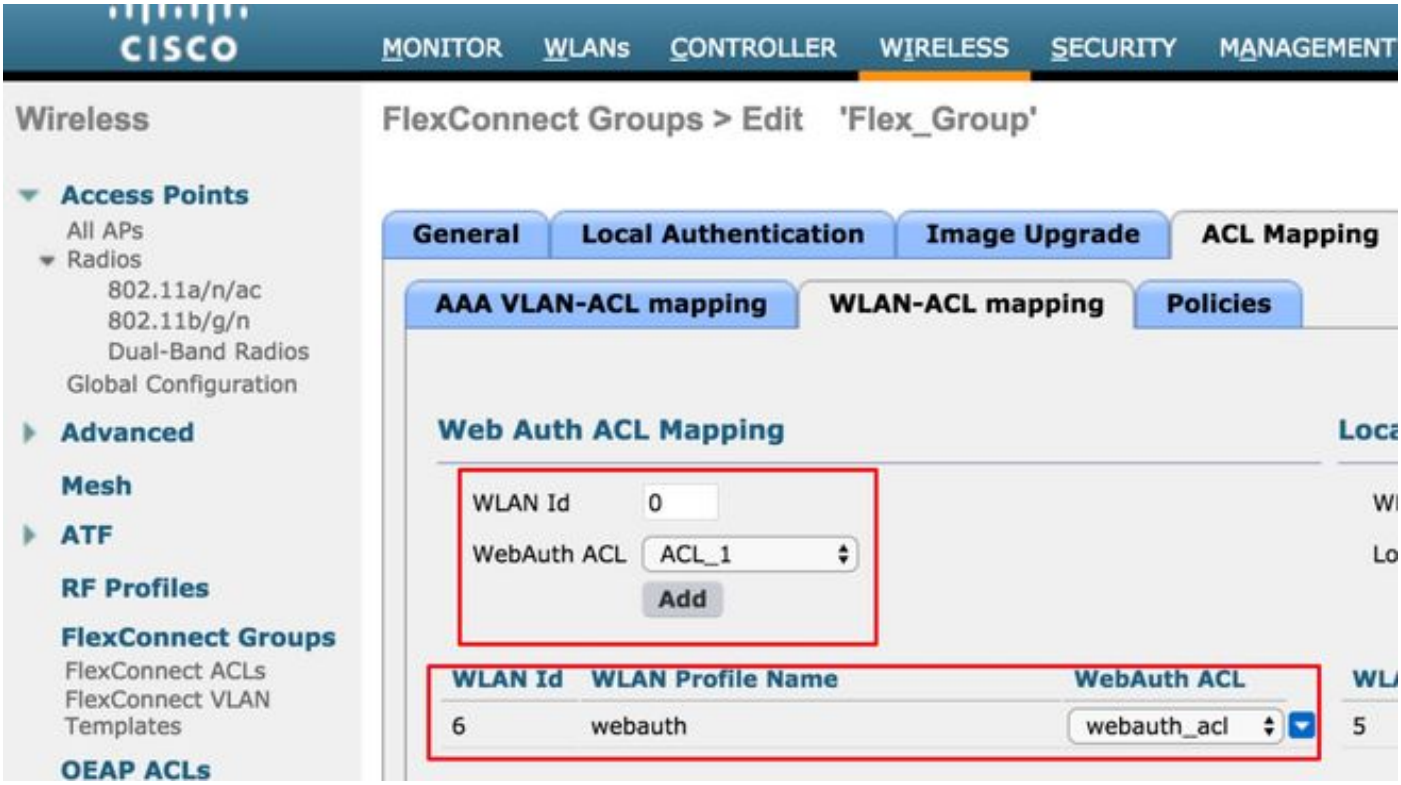
2. ACL Webauth

La liste de contrôle d'accès Webauth est utilisée dans le cas d'un SSID (Webauth/Webpassthrough Service Set Identifier) activé pour la commutation locale flexconnect. Il est utilisé comme liste de contrôle d'accès pré-authentification et autorise le trafic client vers le serveur de redirection. Une fois la redirection terminée et que le client est en état **EXÉCUTÉ**, la liste de contrôle d'accès s'arrête pour prendre effet.

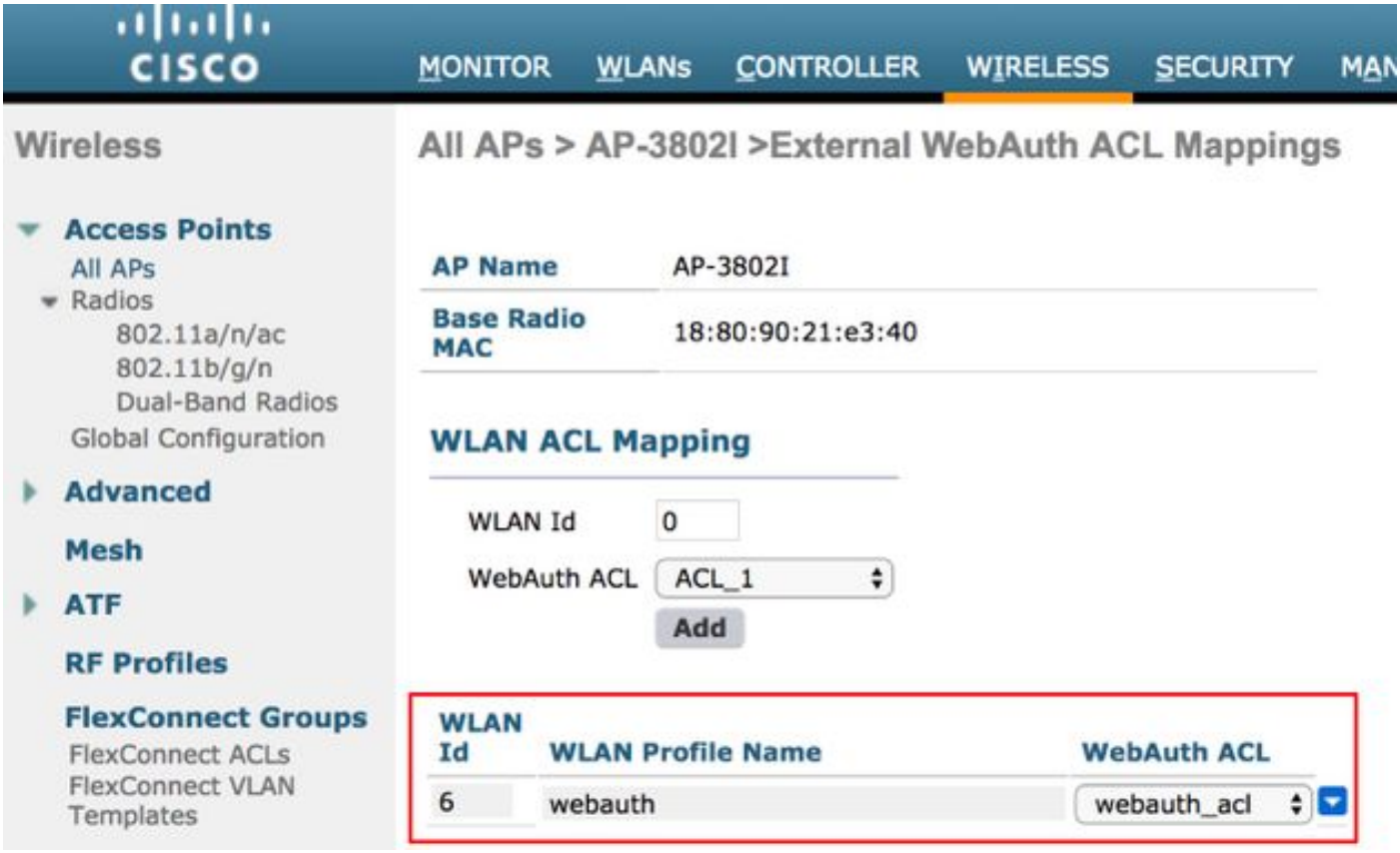
La liste de contrôle d'accès Webauth peut être appliquée au niveau WLAN, au niveau AP ou au niveau du groupe flexconnect. Une liste de contrôle d'accès spécifique au point d'accès a la priorité la plus élevée, tandis que la liste de contrôle d'accès WLAN est la plus basse. Si les trois sont appliquées, AP Specific a priorité suivie de Flex ACL, puis WLAN Global Specific ACL.

Il peut y avoir un maximum de 16 listes de contrôle d'accès d'authentification Web configurées sur un point d'accès.

Il peut être appliqué au niveau du groupe flexconnect, accédez à **Wireless > Flexconnect Groups > Select the group you want configure > ACL mapping > WLAN-ACL mapping > Web Auth ACL Mapping** tel qu'illustré dans l'image.



La liste de contrôle d'accès peut être appliquée au niveau du point d'accès, naviguez jusqu'à **Wireless >All AP's >AP name >Flexconnect tab > External WebAuthentication ACL > WLAN ACL** comme illustré dans l'image.



La liste de contrôle d'accès peut être appliquée au niveau WLAN, accédez à **WLAN > WLAN_ID > Layer 3 > WebAuth FlexAcl** comme indiqué dans l'image.

Sur le point d'accès Cisco IOS®, vous pouvez vérifier si la liste de contrôle d'accès a été appliquée au client. Vérifiez le résultat de **show controllers dot11radio 0 client** (ou 1 si le client se connecte à la radio A) comme indiqué ici :

```
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 stratégie Web

La liste de contrôle d'accès WebPolicy est utilisée pour les scénarios Conditional Web Redirect, Splash Page Web Redirect et Central Webauth.

Deux modes de configuration sont disponibles pour les WLAN WebPolicy avec des listes de contrôle d'accès Flex :

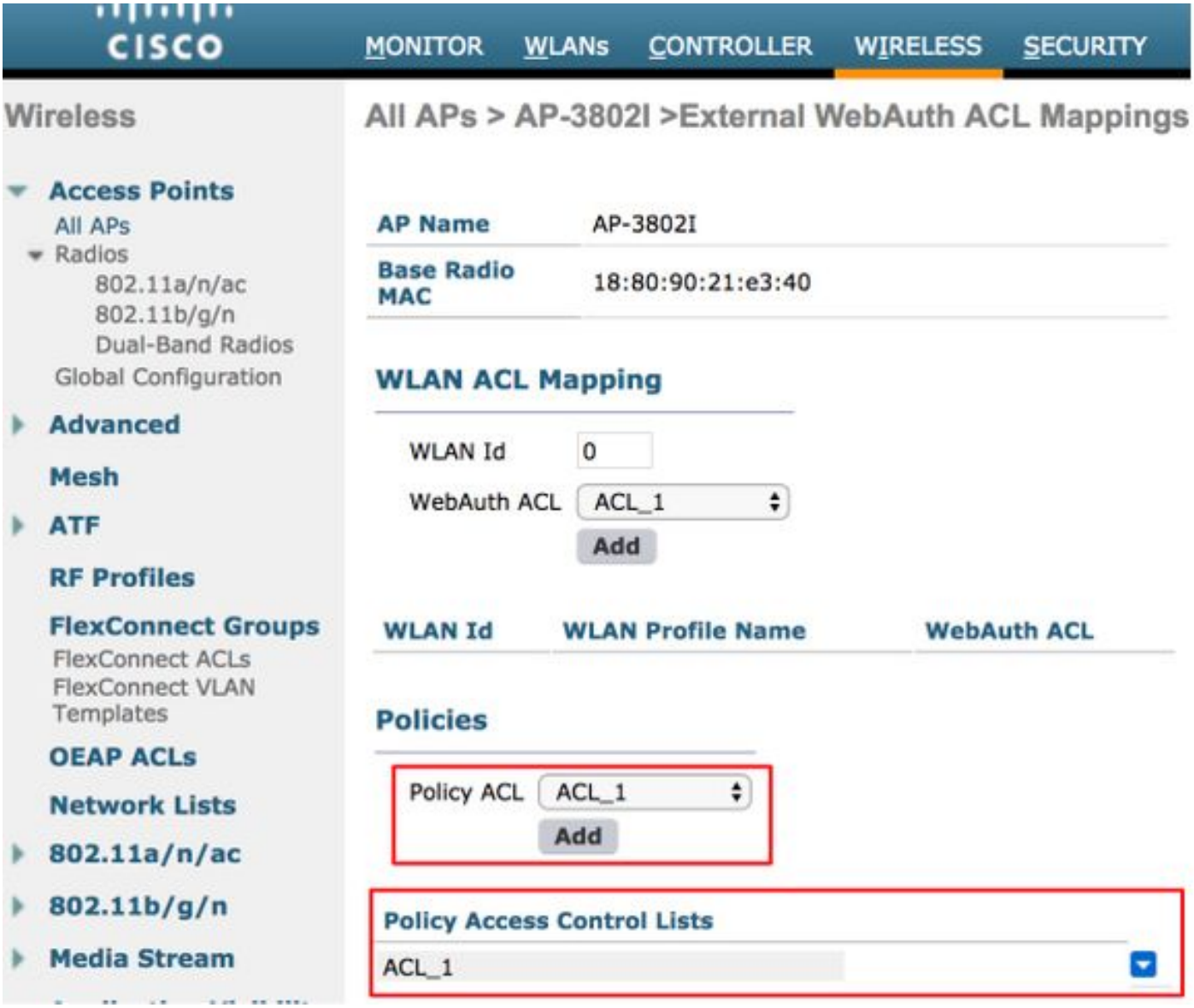
1. Groupe Flexconnect

Tous les points d'accès du groupe FlexConnect reçoivent la liste de contrôle d'accès configurée. Vous pouvez configurer ce paramètre lorsque vous naviguez vers **Groupes Wireless-Flexconnect > Sélectionnez le groupe que vous voulez configurer > Mappage ACL > Politiques**, et ajoutez le nom de la liste ACL de stratégie comme indiqué dans l'image :

2. Spécifique au point d'accès

Le point d'accès pour lequel la configuration est effectuée reçoit la liste de contrôle d'accès, aucun autre point d'accès n'est affecté. Ceci peut être configuré lorsque vous accédez à **Wireless > All APs > AP name >**

Onglet Flexconnect > ACL d'authentification Web externe > Stratégies comme illustré dans l'image.



Après une authentification L2 réussie, lorsque le serveur radius envoie le nom de la liste de contrôle d'accès dans la paire AV redirect-acl, ceci est appliqué directement au client sur l'AP. Lorsque le client passe à l'état **RUN**, tout le trafic client est commuté localement et le point d'accès s'arrête pour appliquer la liste de contrôle d'accès.

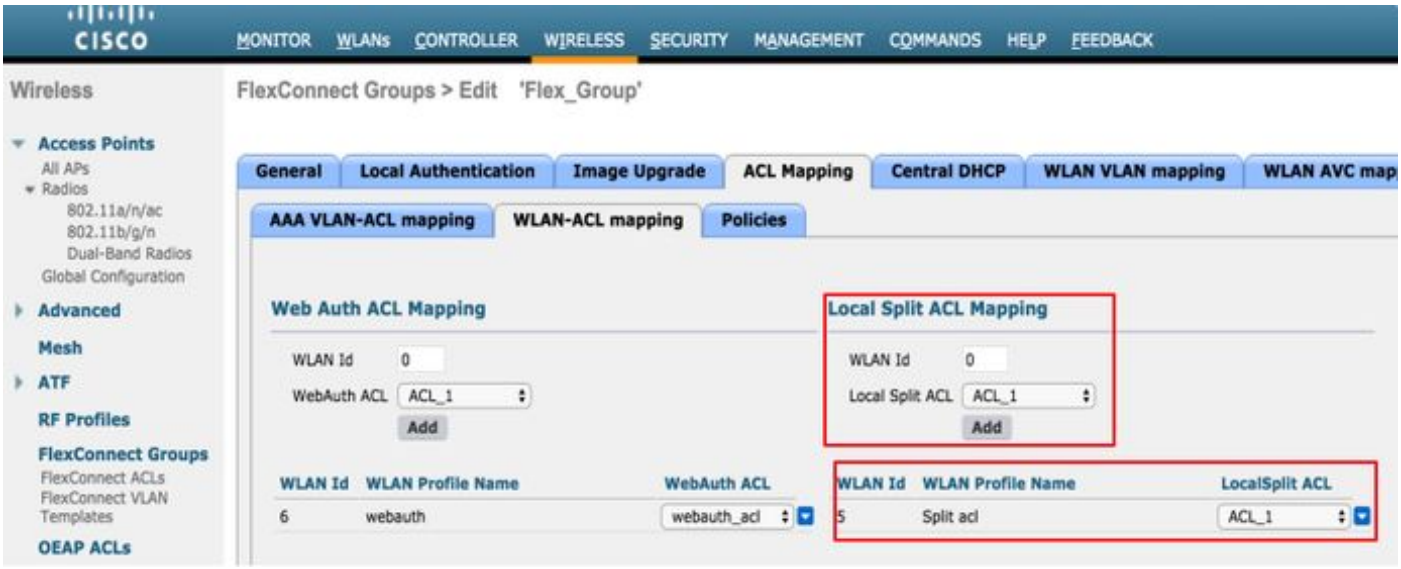
Il peut y avoir un maximum ou 32 listes de contrôle d'accès WebPolicy configurées sur un point d'accès. 16 points d'accès spécifiques et 16 groupes FlexConnect spécifiques.

4. Séparer la liste de contrôle d'accès du tunnel

Les listes de contrôle d'accès de tunnellisation fractionnée sont utilisées avec des SSID commutés de façon centralisée lorsque le trafic client doit être envoyé localement. La fonctionnalité de fractionnement en canaux est également un avantage supplémentaire pour la configuration d'Office Extend Access Point (OEAP), où les clients d'un SSID d'entreprise peuvent communiquer directement avec des périphériques d'un réseau local (imprimantes, machines filaires sur un port LAN distant ou périphériques sans fil sur un SSID personnel) une fois qu'ils sont mentionnés comme faisant partie de la liste de contrôle d'accès à tunnel partagé.

Les listes de contrôle d'accès de tunnellisation fractionnée peuvent être configurées en fonction du niveau du groupe flexconnect, accédez à **Groupes de connexion sans fil > Sélectionnez le groupe à configurer > Mappage ACL > Mappage WLAN-ACL > Mappage ACL fractionné local** comme

illustré dans l'image.



Ils peuvent également être configurés au niveau du point d'accès, naviguez jusqu'à **Wireless > All AP's > AP name > Flexconnect tab > Local Split ACL** et ajoutez le nom de la liste de contrôle d'accès flexconnect comme indiqué dans l'image.

Les listes de contrôle d'accès de fractionnement en canaux ne peuvent pas relier localement le trafic de multidiffusion/diffusion. Le trafic multidiffusion/diffusion est commuté de manière centralisée même s'il correspond à la liste de contrôle d'accès FlexConnect.

Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.