Configurez Flexconnect ACL sur WLC

Contenu

Introduction

Ce document décrit les divers types de liste de contrôle d'accès de 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 :

- Le contrôleur LAN Sans fil de Cisco (WLC) ce exécute le code 8.3 et plus élevé
- Configuration de Flexconnect sur le WLC

Composants utilisés

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

- La gamme Cisco 8540 WLC qui exécute la version logicielle 8.3.133.0.
- 3802 et 3702 AP qui fonctionnent en mode de flexconnect.

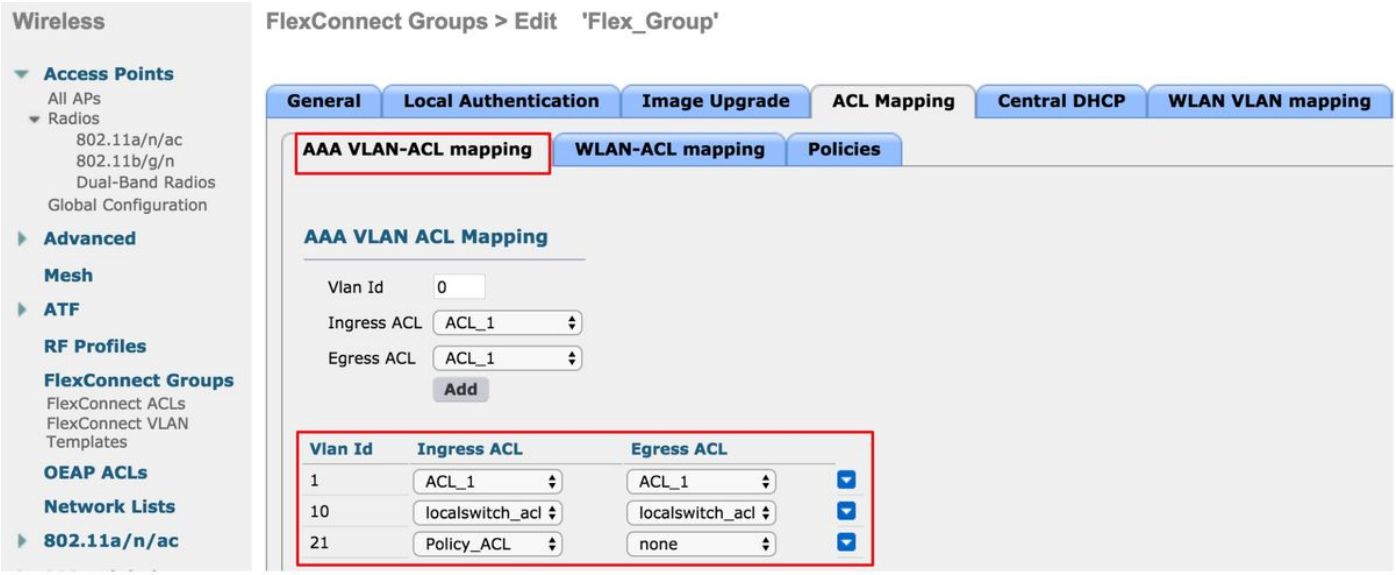
Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Types d'ACL

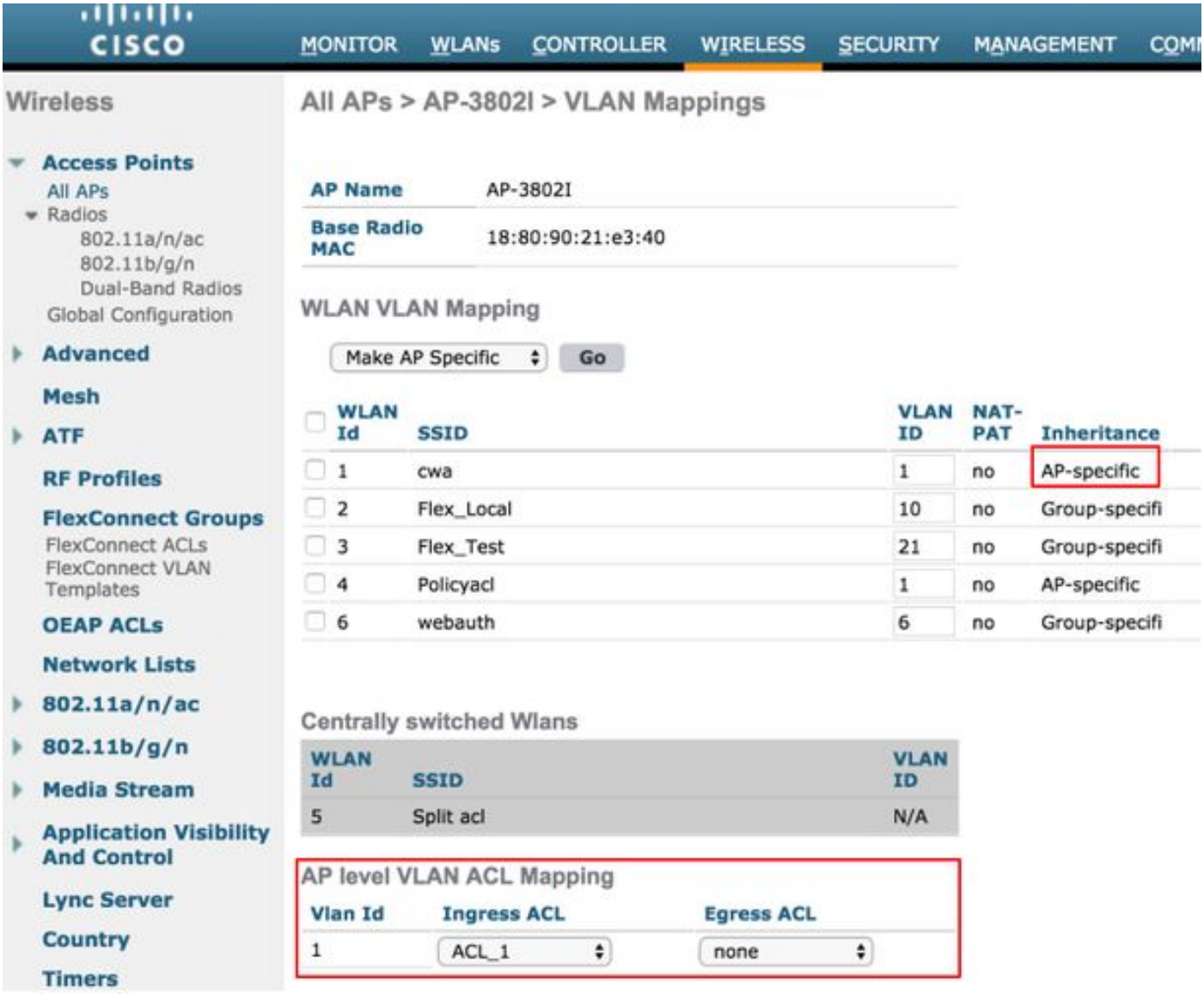
1. ACL VLAN

L'ACL VLAN sont l'ACL le plus utilisé généralement et il vous permet de contrôler le trafic de client qui est envoyé dans et hors du VLAN.

L'ACL peut être configuré selon le groupe de flexconnect qui utilise la section de mappage de l'**AAA VLAN-ACL** dans la **radio-Flexconnect groupe > ACL traçant > mappage de l'AAA VLAN-ACL** suivant les indications de l'image.



Il peut également être configuré selon le niveau AP, naviguer vers la **radio > tout le nom AP > AP > onglet de Flexconnect** et cliquer sur la section de **mappages VLAN**. Ici, vous devez faire la particularité du config AP VLAN d'abord, après quoi vous pouvez spécifier le mappage du niveau VLAN-ACL AP suivant les indications de l'image.



Directions d'ACL

Vous pouvez également spécifier la direction dans laquelle l'ACL obtient appliqué :

- D'entrée (le d'entrée signifie vers le client sans fil)
- De sortie (vers le theDS ou le RÉSEAU LOCAL),
- les deux ou aucun.

Ainsi, si vous voudriez bloquer le trafic destiné vers le client sans fil alors que vous pouvez utiliser la direction d'entrée et si vous voudriez bloquer le trafic originaire par le client sans fil, vous pouvez utiliser la direction de sortie.

L'option aucun est utilisée quand vous voudriez pousser un ACL distinct avec l'utilisation du dépassement d'Authentification, autorisation et comptabilité (AAA). Dans ce cas, l'ACL envoyé par le serveur de rayon est appliqué dynamiquement au client.

> **Note**: L'ACL doit être configuré sous l'ACL de Flexconnect à l'avance, autrement il n'obtient pas appliqué.

ACL traçant des considérations

Quand vous utilisez VLAN ACL, il est également important de comprendre ces considérations en ce qui concerne des mappages VLAN sur le flexconnect AP :

- Si le VLAN est configuré avec l'utilisation du groupe de FlexConnect, l'ACL correspondant configuré sur le groupe de FlexConnect est appliqué.
- Si un VLAN est configuré sur le groupe de FlexConnect et également sur AP (comme configuration spécifique AP), alors la configuration d'ACL AP a la priorité.
- Si l'ACL spécifique AP est configuré à aucun, alors aucun ACL n'est appliqué.
- Si le VLAN qui a été retourné de l'AAA n'est pas présent sur AP, le client retombe au par défaut VLAN configuré pour le RÉSEAU LOCAL Sans fil (WLAN) et tout ACL tracé à ce par défaut VLAN a la priorité.

Vérifiez si l'ACL est appliqué sur AP

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

1. Onde 2 AP

Sur une onde 2 AP, vous pouvez vérifier si l'ACL obtient réellement poussé à AP avec le VLAN-**acl de flexconnect d'exposition de** commande. Ici, vous pouvez également voir le nombre de paquets passés et lâchés pour chaque 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

Au niveau AP, vous pouvez valider si la configuration d'ACL a été poussée à AP avec deux manières :

- Utilisez le **show access-lists** commandent ce qui affiche si tout le VLAN ACL sont configurés sur 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
```

Vous pouvez surveillez également l'activité qui se produit sur chaque ACL, vérifiez la sortie détaillée de cet ACL et voyez le nombre de hits 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 le VLAN ACL sont appliqués sur l'interface de gigabit, vous pouvez valider si l'ACL est appliqué correctement. Vérifiez la sous sortie d'interface comme affiché 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
```

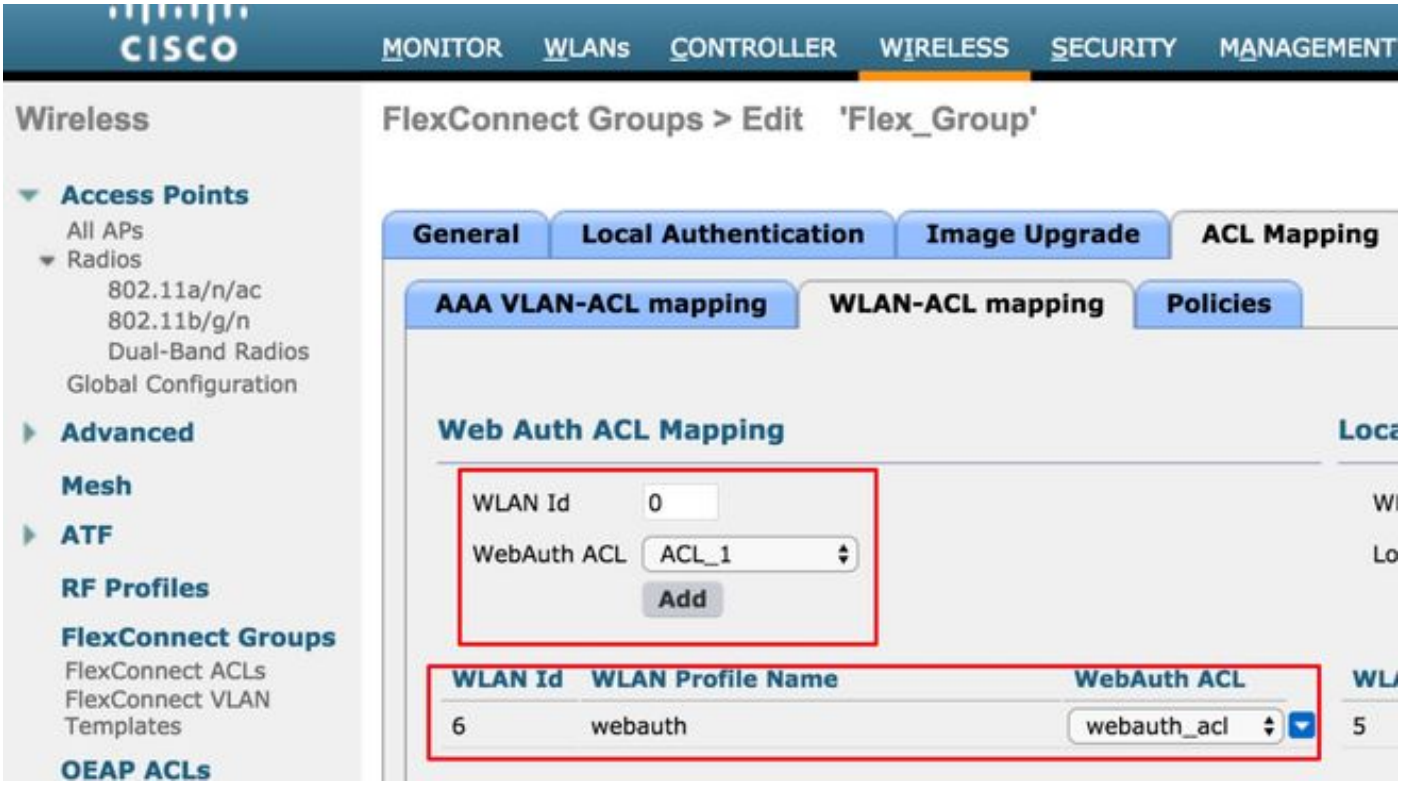
2. ACL de Webauth

L'ACL de Webauth est utilisé dans le cas d'un Identifiant SSID (Service Set Identifier) Webauth/Webpassthrough qui a été activé pour la commutation locale de flexconnect. Ceci est utilisé comme ACL de pré-authentification et permet le trafic de client au serveur de réorientation. Une fois que la redirection est complète et le client est dans l'état de **PASSAGE**, les arrêts d'ACL pour le prendre dans l'effet.

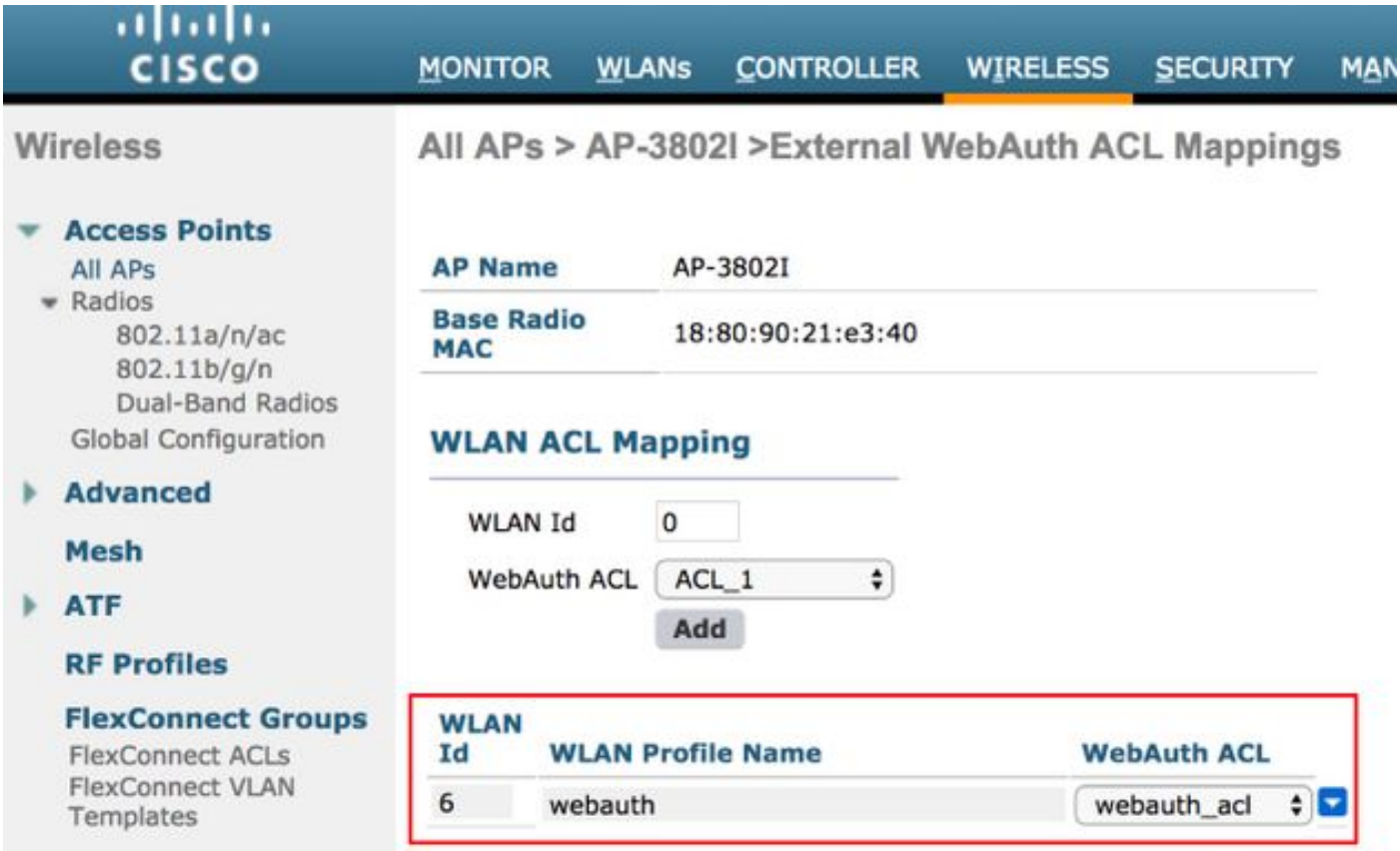
L'ACL de Webauth peut être appliqué au niveau WLAN, au niveau AP ou au niveau du groupe de flexconnect. Un ACL spécifique AP a le plus prioritaire, tandis que l'ACL WLAN a le plus bas. Si chacun des trois est appliqué, la particularité AP a la priorité suivie d'ACL de flexible et puis d'ACL spécifique global WLAN.

Il peut y a un maximum 16 du Web-Auth ACLs configuré sur AP.

Il peut être appliqué au niveau du groupe de flexconnect, naviguent vers la **radio > les groupes de Flexconnect > sélectionnent le groupe que vous voulez configurez > ACL traçant > mappage WLAN-ACL > ACL authentique de Web traçant** suivant les indications de l'image.



L'ACL peut être appliqué au niveau AP, naviguent vers l'**onglet Sans fil de >Flexconnect de nom >AP du >All AP > WebAuthentication externe ACLs > ACL WLAN** suivant les indications de l'image.



L'ACL peut être appliqué au niveau WLAN, naviguent vers **WLAN > WLAN_ID > couche 3 > WebAuth FlexAcl** suivant les indications de l'image.

Sur le Cisco IOS® AP, vous pouvez vérifier si l'ACL était appliqué au client. Vérifiez la sortie du **client des shows controllers dot11radio 0** (ou 1 si le client se connecte à la radio A) comme affiché 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
```

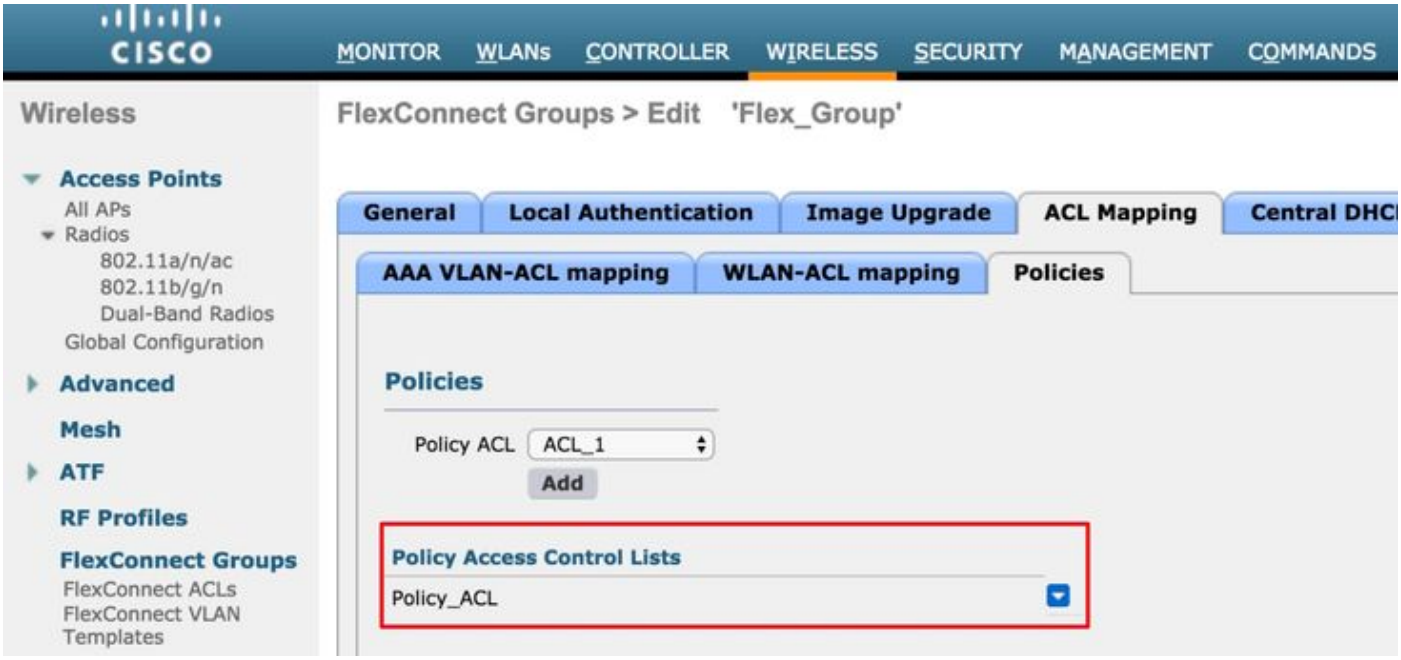
3. ACL de stratégie de Web

L'ACL de WebPolicy est utilisé pour le Web conditionnel réorientent, le Web de page de splash réorientent et les scénarios centraux de Webauth.

Il y a deux modes de configuration disponibles pour WebPolicy WLAN avec le flexible ACLs :

1. Groupe de Flexconnect

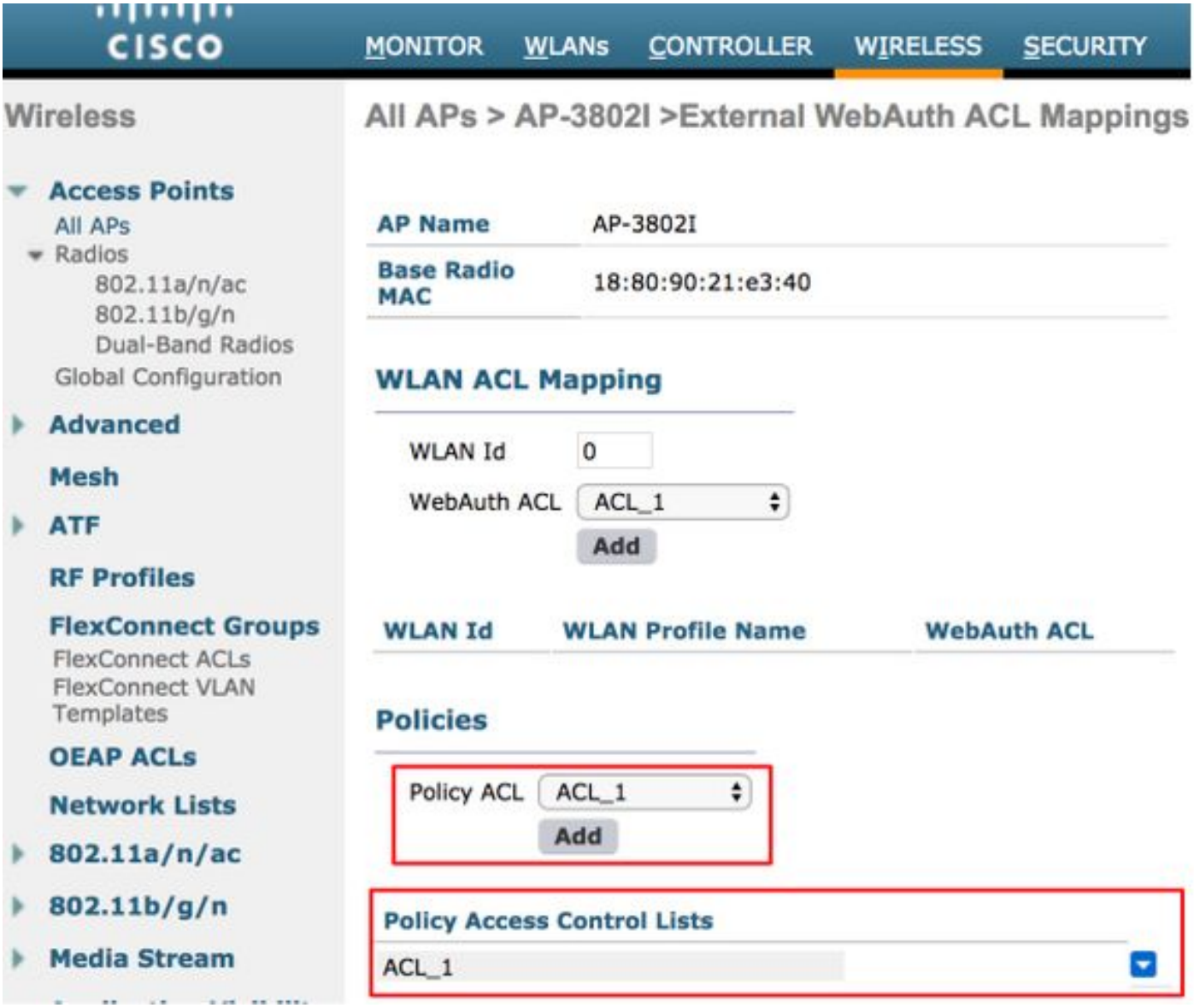
Tous les aps dans le group receive de FlexConnect l'ACL qui est configuré. Ceci peut être configuré en tant que vous naviguent vers des **groupes de radio-Flexconnect > sélectionnent le groupe que vous voulez configurez > ACL traçant > des stratégies**, et ajoutent le nom de l'ACL de stratégie suivant les indications de l'image :



2. Particularité AP

AP pour lequel la configuration est faite reçoit l'ACL, aucun autres aps sont affectés. Ceci peut être configuré en tant que vous naviguent vers la **radio > tout des aps > nom AP >**

Onglet de Flexconnect > WebAuthentication externe ACLs > stratégies suivant les indications de l'image.



Après une authentification L2 réussie, quand le serveur de rayon envoie le nom d'ACL dans la paire AV de réorienter-acl, ceci obtient appliqué directement pour le client sur AP. Quand le client entre dans l'état de **PASSAGE**, tout le trafic de client est commuté localement et AP cesse d'appliquer l'ACL.

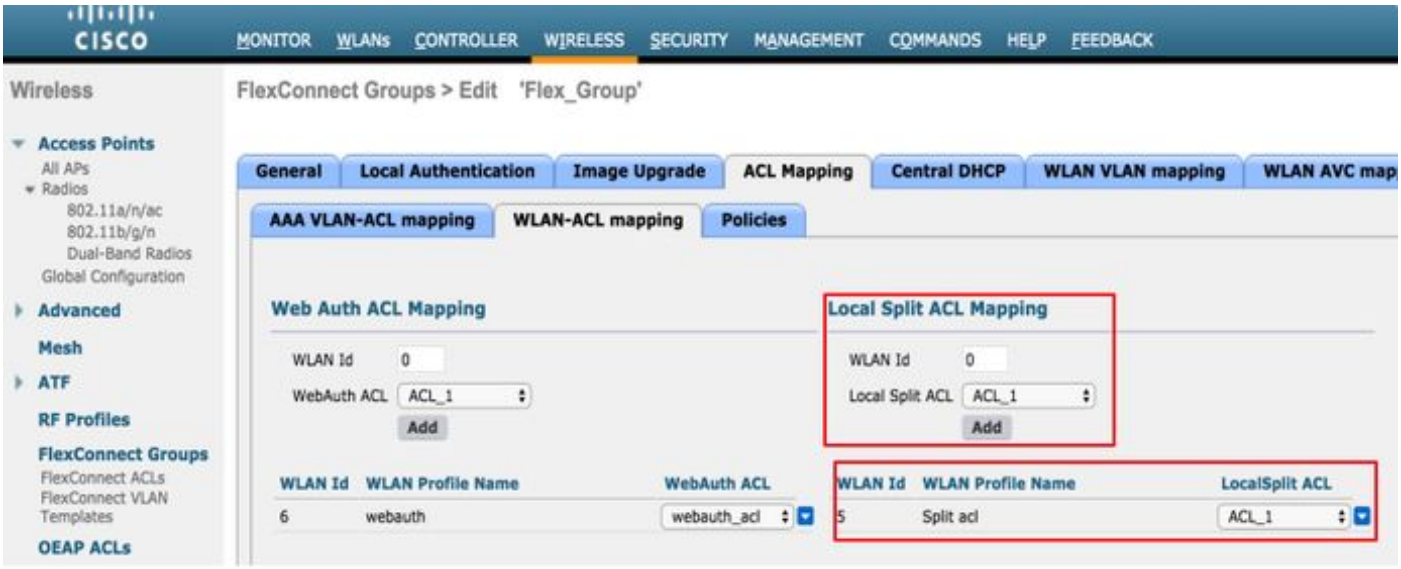
Il peut y avoir un maximum ou de 32 WebPolicy ACLs configuré sur AP. Particularité de 16 AP et particularité de groupe de 16 FlexConnect.

4. ACL de tunnel partagé

La Segmentation de tunnel ACL sont utilisées avec des SSID centralement commutés quand une partie du trafic de client doit être envoyée plus de localement. La fonctionnalité de Segmentation de tunnel est également un avantage ajouté pour le bureau étendent le Point d'accès (OEAP) installé où les clients sur un SSID entreprise peuvent parler aux périphériques sur un réseau local (imprimantes, ordinateur de câble sur un port LAN distant, ou périphériques sans fil sur un SSID personnel) directement une fois qu'ils sont mentionnés en tant qu'élément de l'ACL de tunnel partagé.

La Segmentation de tunnel ACL peut être configurée en fonction selon le niveau du groupe de flexconnect, naviguent vers des **groupes de radio-Flexconnect > sélectionnent le groupe que vous voulez configurez > ACL traçant > mappage WLAN-ACL > ACL fendu local traçant** suivant les

indications de l'image.



Ils peuvent également être configurés à selon le niveau AP, naviguer vers la **radio > tout le nom AP > AP > onglet de Flexconnect > ACLs fendu local** et ajouter le nom de l'ACL de flexconnect suivant les indications de l'image.

La Segmentation de tunnel ACL ne peut pas localement jeter un pont sur le trafic de Multidiffusion/émission. Le trafic de Multidiffusion/émission est commuté centralement même si il apparie l'ACL de FlexConnect.

Dépannez

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