Configuration des listes de contrôle d'accès Flexconnect sur WLC

Contenu

Introduction Conditions préalables Conditions requises Components Used Types ACL 1. ACL VLAN Itinéraires des listes de contrôle d'accès Considérations relatives au mappage des listes de contrôle d'accès Vérifier si la liste de contrôle d'accès est appliquée sur le point d'accès 2. ACL Webauth 3. ACL de stratégie Web 4. Séparer la liste de contrôle d'accès du tunnel Dépannage

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.

| Wireless | FlexConnect Groups > Edit 'F | lex_Group' | | |
|---|------------------------------|--|--------------|-------------------|
| Access Points All APs Radios 802.11a/n/ac 802.11b/g/n Dual-Band Radios Global Configuration | General Local Authentication | Image Upgrade ACL Mapping AN-ACL mapping Policies | Central DHCP | WLAN VLAN mapping |
| Advanced | AAA VLAN ACL Mapping | | | |
| Mesh | Vlan Id 0 | | | |
| ▶ ATF | Ingress ACL ACL 1 + | | | |
| RF Profiles | | | | |
| FlexConnect Groups FlexConnect ACLs FlexConnect VLAN | Add | | | |
| Templates | Vlan Id Ingress ACL | Egress ACL | | |
| OEAP ACLs | 1 ACL_1 \$ | ACL_1 💠 🔽 | | |
| Network Lists | 10 localswitch_acl \$ | localswitch_acl 🖨 🔽 | | |
| 802.11a/n/ac | 21 Policy_ACL \$ | none 💠 🔽 | | |

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.

| Wireless All APs > AP-3802l > VLAN Mappings • Access Points All APs AP Name AP-3802l All APs AP Name All APs AP Name All APs AP-3802l B02.11a/n/ac Bose Radio B02.11b/g/n Base Radio Dual-Band Radios Make AP Specific Global Configuration Make AP Specific AttF Make AP Specific Atters AP-specific Atters AP olicyacl Atters AP olicyacl Application Vis | cisco | | <u>W</u> LANs | CONTROLLER | WIRELESS | SECURITY | MANA | GEMENT COM |
|--|--|-----------------|---------------|-----------------|------------|------------|-------------|---------------|
| Access Points All APs Radios 802.11a/n/ac 802.11b/g/n Dual-Band Radios Giobal Configuration Advanced Mesh ATF RF Profiles FlexConnect Groups FlexConnect Groups FlexConnect VLAN Templates OEAP ACLs Network Lists 802.11a/n/ac 802.11a/n/ac S02.11a/n/ac S02.11a/n/ac S02.11a/n/ac S02.11a/n/ac S02.11a/n/ac S02.11a/n/ac S02.11b/g/n Media Stream Application Visibility And Control VLAN ACL Mapping All APS AP Ievel VLAN ACL Mapping AP Ievel VLAN ACL Mapping Application Visibility And Control AP Ievel VLAN ACL Mapping AP Ievel VLAN ACL Mapping Apping Action Application Visibility And Control Application Visibility And Control AP Ievel VLAN ACL Mapping Apping All APS AC AP Ievel VLAN ACL Mapping Apping Action Application Visibility And Control Application Visibility Application Visibility And Control Application Visibility And Control Application Visibility And Control Application Visibility Application Visibility And Control Application Visibility And Control Application Visibility And Control Application Visibility Application Visibility And Control Application Visibility Application Visibility Application Visibility Application Visibility Applicatidi Visibility Applicatidi Vis | Wireless | All APs | > AP-380 | 2I > VLAN Ma | ppings | | | |
| Base Radio 18:80:90:21:e3:40 MAC 18:80:90:21:e3:40 WLAN VLAN Mapping WLAN VLAN Mapping Advanced Make AP Specific ‡ Go Mesh VLAN Mapping ATF Id RF Profiles 1 cwa FlexConnect Groups 2 FlexConnect ACLs 1 no AP-specific 2 Second VLAN 2 VLAN 1 no AP-specific 1 no AP-specific 3 FlexConnect VLAN 5 Second VLAN 6 Metia Stream VLAN Application Visibility Make AP Specific Application Visibility AP level VLAN ACL Mapping | Access Points All APs Radios | AP Name | AP | -38021 | | | | |
| S02.11b/g/n WLAN VLAN Mapping Make AP Specific () Go Make AP Specific () Go Mesh Make AP Specific () Go A Atr Make AP Specific () Go RF Profiles 1 cwa 1 no FlexConnect Groups 2 Flex_Local 10 no Group-specific StexConnect VLAN 3 Flex_Test 21 no Group-specific OEAP ACLs 6 webauth 6 no Group-specific Network Lists S02.11a/n/ac Centrally switched Wlans VLAN Media Stream Id SSID ID Application Visibility Application Visibility AP level VLAN ACL Mapping | 802.11a/n/ac | Base Rad MAC | lio 18 | :80:90:21:e3:40 | | | | |
| Advanced Mesh ATF Id SSID SSID Id SSID S | Dual-Band Radios Global Configuration | WLAN VL | AN Mappi | ing | | | | |
| Mesh VLAN VLAN NAT- ATF Id SSID ID PAT Inheritance RF Profiles 1 cwa 1 no AP-specific FlexConnect Groups 2 Flex_Local 10 no Group-specific Seconnect ACLs 3 Flex_Test 21 no Group-specific GEAP ACLs 4 Policyacl 1 no AP-specific Network Lists 6 webauth 6 no Group-specific 802.11a/n/ac Centrally switched Wlans VLAN MLAN SSID 5 Split acl N/A Media Stream VLAN SSID Split acl N/A N/A APplication Visibility AP level/LAN ACL Mapping VLAN N/A | Advanced | Make | AP Specific | \$ Go | | | | |
| RF Profiles 1 cwa 1 no AP-specific PlexConnect Groups Flex_Local 10 no Group-specific FlexConnect ACLs 3 Flex_Test 21 no Group-specific 3 Flex_Test 21 no Group-specific 3 Flex_Test 21 no AP-specific 0EAP ACLs 6 webauth 6 no Group-specific Network Lists 6 webauth 6 no Group-specific 802.11a/n/ac Centrally switched Wlans 6 no Group-specific Media Stream MLAN SSID ID ID 5 Split acl N/A AP level VLAN ACL Mapping AP level VLAN ACL Mapping ID ID ID ID | Mesh ATF | | SSID | | | VLAN ID | NAT- PAT | Inheritance |
| FlexConnect Groups 2 Flex_Local 10 no Group-specifie Bit 3 Flex_Test 21 no Group-specifie CEAP ACLs 4 Policyacl 1 no AP-specifie Media Stream 6 webauth 6 no Group-specifie Media Stream VLAN SSID Split acl VLAN VLAN Application Visibility And Control N/A AP level VLAN ACL Mapping N/A | RF Profiles | 1 | cwa | | | 1 | no | AP-specific |
| FlexConnect ACLs 3 Flex_Test 21 no Group-specific FlexConnect VLAN 4 Policyacl 1 no AP-specific OEAP ACLs 6 webauth 6 no Group-specific Network Lists 6 webauth 6 no Group-specific 802.11a/n/ac Centrally switched Wlans 6 no Group-specific 802.11b/g/n Media Stream Id SSID Split acl N/A Application Visibility AP level VLAN ACL Mapping N/A N/A | FlexConnect Groups | 2 | Flex_Local | I. | | 10 | no | Group-specifi |
| Image: Prexconnect VLAN 4 Policyacl 1 no AP-specific Image: OEAP ACLs 6 webauth 6 no Group-specific Image: OEAP ACLs 6 webauth 6 no Group-specific Network Lists Image: OEAP ACLs Image: OEAP ACLs Image: OEAP ACLs 6 no Group-specific Network Lists Image: OEAP ACLs | FlexConnect ACLs | 3 | Flex_Test | | | 21 | no | Group-specifi |
| OEAP ACLs 6 no Group-specifi Network Lists 802.11a/n/ac Centrally switched Wlans VLAN 802.11b/g/n WLAN Centrally switched Wlans VLAN Media Stream Id SSID ID Application Visibility Split acl N/A AP level VLAN ACL Mapping AP level VLAN ACL Mapping | Templates | 4 | Policyacl | | | 1 | no | AP-specific |
| Network Lists Ketwork Lists 802.11a/n/ac Centrally switched Wlans 802.11b/g/n WLAN Media Stream MLAN Application Visibility SSID And Control AP level VLAN ACL Mapping | OEAP ACLs | 6 | webauth | | | 6 | no | Group-specifi |
| 802.11a/n/ac Centrally switched Wlans 802.11b/g/n WLAN Id SSID Media Stream Id Application Visibility And Control Split acl | Network Lists | | | | | | | |
| > 802.11b/g/n WLAN VLAN > Media Stream Id SSID ID > Application Visibility 5 Split acl N/A | 802.11a/n/ac | Controlly | switched | Wlane | | | | |
| Media Stream Id SSID ID Application Visibility And Control 5 Split acl N/A | 802.11b/g/n | WLAN | Switched | WIGIIS | | VLAN | | |
| Application Visibility And Control AP level VLAN ACL Mapping | Media Stream | Id | SSID | | | ID | | |
| AP level VLAN ACL Mapping | Application Visibility And Control | 5 | Split acl | | | N/A | | |
| LVDC Server | Lync Server | AP level | VLAN ACL | . Mapping | | | | |
| Vian Id Ingress ACL Egress ACL | Country | Vlan Id | Ingres | S ACL | Egress ACL | | | |
| 1 (ACL_1 +) (none +) | Timore | 1 | ACL_1 | ÷] | none | • | | |

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
```

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.

| cisco | MONITOR | WLANS CONTRO | OLLER V | WIRELESS SEC | CURITY MANA | GEMENT |
|---|-----------|---------------------------|----------|---------------|---------------|--------|
| Wireless | FlexConne | ect Groups > E | dit 'Fle | ex_Group' | | |
| Access Points All APs Radios | General | Local Authent | ication | Image Upgra | ade ACL M | apping |
| 802.11a/n/ac 802.11b/g/n Dual-Band Radios Global Configuration | AAA VL | AN-ACL mapping | WLA | N-ACL mapping | Policies | 1 |
| Advanced Mesh | Web Au | Ith ACL Mappin | g | | | W |
| ATF RF Profiles | WebAu | Act_1 | • | | | Lo |
| FlexConnect Groups FlexConnect ACLs FlexConnect VLAN Templates | WLAN 3 | d WLAN Profile webauth | Name | W | vebauth_acl 🛟 | WL/ |
| OFAP ACLS | | | | | | _ |

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.

| cisco | MONITOR | WLANs | CONTROLLER | WIRELESS | <u>S</u> ECURITY | MAN | | |
|---|-----------------------|-------------|-------------------------------|-----------|------------------|-----|--|--|
| Wireless | All APs > | AP-380 | 2I >External V | VebAuth A | CL Mapping | gs | | |
| Access Points All APs Radios | AP Name Base Radio | AP 9 18 | AP-3802I 18:80:90:21:e3:40 | | | | | |
| 802.11b/g/n Dual-Band Radios Global Configuration | WLAN AC | CL Mappi | ing | | | | | |
| Advanced Mesh ATF RF Profiles | WLAN Id WebAuth | 0 ACL AC | CL_1 \$ | | | | | |
| FlexConnect Groups FlexConnect ACLs FlexConnect VLAN Templates | Id WLAN 6 we | LAN Profi | le Name | We | bAuth ACL | | | |

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.

| cisco | | LANS <u>C</u> ON | TROLLER | WIRELES | is <u>s</u> ecur | | ENT COMMANDS | HELP |
|----------|--|---|--------------------------------------|----------|------------------|-----------------------|-----------------|------|
| WLANs | WLANs > E | dit 'webau | uth' | | | | | |
| WLANS | General | Security | QoS | Policy-M | apping | Advanced | | |
| Advanced | Layer 2 | Layer 3 | AAA S | ervers | | | | |
| | Layer 3 Auth Passi Cond Splas On M Preauth Sleeping Over-rid | Security We entication through litional Web Re sh Page Web R IAC Filter failur entication ACL g Client Er le Global Confi | edirect tedirect IPv4 nable | None 🕏 | IPv6 None | • WebAuth Flex | xAcl Policy_ACL | ÷ |

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 :

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 :

| cisco | MONITOR WL | Ns <u>C</u> ontroli | LER WIRELESS | SECURITY M | 1 <u>A</u> NAGEMENT | C <u>O</u> MMANDS |
|---|--------------|---------------------|---------------|-------------|---------------------|-------------------|
| Wireless | FlexConnect | Groups > Edi | t 'Flex_Group |) ' | | |
| Access Points All APs Radios | General | ocal Authentic | ation Image | Upgrade AC | CL Mapping | Central DHC |
| 802.11a/n/ac 802.11b/g/n Dual-Band Radios Global Configuration | AAA VLAN- | ACL mapping | WLAN-ACL ma | pping Polic | ies | |
| Advanced | Policies | | | | | |
| Mesh | Policy ACL | ACL_1 | • | | | |
| ATF RF Profiles | | Add | | | - | |
| FlexConnect Groups | Policy Acces | ss Control Lists | | | | |
| FlexConnect ACLs FlexConnect VLAN Templates | Policy_ACL | | | | | |

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.

| | CISCO | MONITOR W | (LANs | | WIRELESS | <u>S</u> ECURITY |
|----|---|------------------------------|--------------|-------------------------|-----------|------------------|
| Wi | Access Points | All APs > A | P-380 | 2I >External \ | WebAuth A | CL Mappings |
| | All APs Radios 802.11a/n/ac 802.11b/g/n | AP Name Base Radio MAC | AP- 18: | 3802I 80:90:21:e3:40 | | |
| | Global Configuration | WLAN ACL | Mappi | ng | | |
| * | Advanced Mesh | WLAN Id WebAuth AC | 0 CL AC | L_1 ‡ | | |
| | RF Profiles | | Ad | d | | |
| | FlexConnect Groups FlexConnect ACLs FlexConnect VLAN Templates | WLAN Id Policies | WLAN | Profile Name | WebA | uth ACL |
| | OEAP ACLs Network Lists | Policy ACL | ACL_1 Add | \$ | | |
| • | 802.11a/n/ac 802.11b/g/n | Policy Access | Contr | ol Lists | | |
| * | Media Stream | ACL_1 | | | _ | |

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.

| cisco | MONITOR WLANS CONTROLLER WIR | ELESS SECURITY MANAGEM | ient commands help | FEEDBACK |
|---|---|------------------------|-------------------------------------|-------------------------------|
| Wireless | FlexConnect Groups > Edit 'Flex_ | Group' | | |
| Access Points All APs Radios | General Local Authentication | Image Upgrade ACL Mapp | ing Central DHCP W | LAN VLAN mapping WLAN AVC map |
| 802.11a/n/ac 802.11b/g/n Dual-Band Radios Global Configuration | AAA VLAN-ACL mapping WLAN-A | ACL mapping Policies | | |
| Advanced | Web Auth ACL Mapping | | Local Split ACL Mapping | |
| Mesh ATF RF Profiles Electropect Groups | WLAN Id 0 WebAuth ACL ACL_1 0 Add | | WLAN Id 0 Local Split ACL ACL_1 Add | • |
| FlexConnect ACLs | WLAN Id WLAN Profile Name | WebAuth ACL | WLAN Id WLAN Profile Nam | e LocalSplit ACL |
| Templates OEAP ACLs | 6 webauth | webauth_acl 🕴 🖬 | 5 Split acl | ACL_1 + |

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.

| cisco | MONITOR | WLANs | CONTROL | LER | WIRELESS | SECURITY | м |
|--|------------------------------|----------|---------------|-------|--------------|----------|---|
| Wireless | All APs > | AP-38 | 02I > Loca | l Spl | it ACL Map | pings | |
| Access Points All APs Radios | AP Name AP-3802I | | | | | | |
| 802.11a/n/ac 802.11b/g/n Dual-Band Radios | Base Radi MAC | • 1 | 8:80:90:21:e3 | | | | |
| Global Configuration | WLAN A | CL Map | ping | | | | |
| Advanced | WLAN Id | |) | | | | |
| ▶ ATF | Local-Sp | olit ACL | ACL_1 | \$ | | | |
| RF Profiles | | | Add | | | | |
| FlexConnect Groups FlexConnect ACLs | WLAN Id WLAN Profile Name | | | Loc | al-Split ACL | | |
| FlexConnect VLAN Templates | 5 Split acl | | | | AC | L_1 | • |

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.