Configurar ACLs do Flexconnect no WLC

Contents

Introduction

Este documento descreve os vários tipos de lista de controle de acesso (ACL) flexconnect e como eles podem ser configurados e validados no ponto de acesso (AP).

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco Wireless LAN Controller (WLC) que executa o código 8.3 e superior
- Configuração do Flexconnect na WLC

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- O Cisco 8540 Series WLC que executa o software versão 8.3.133.0.
- APs 3802 e 3702 executados no modo flexconnect.

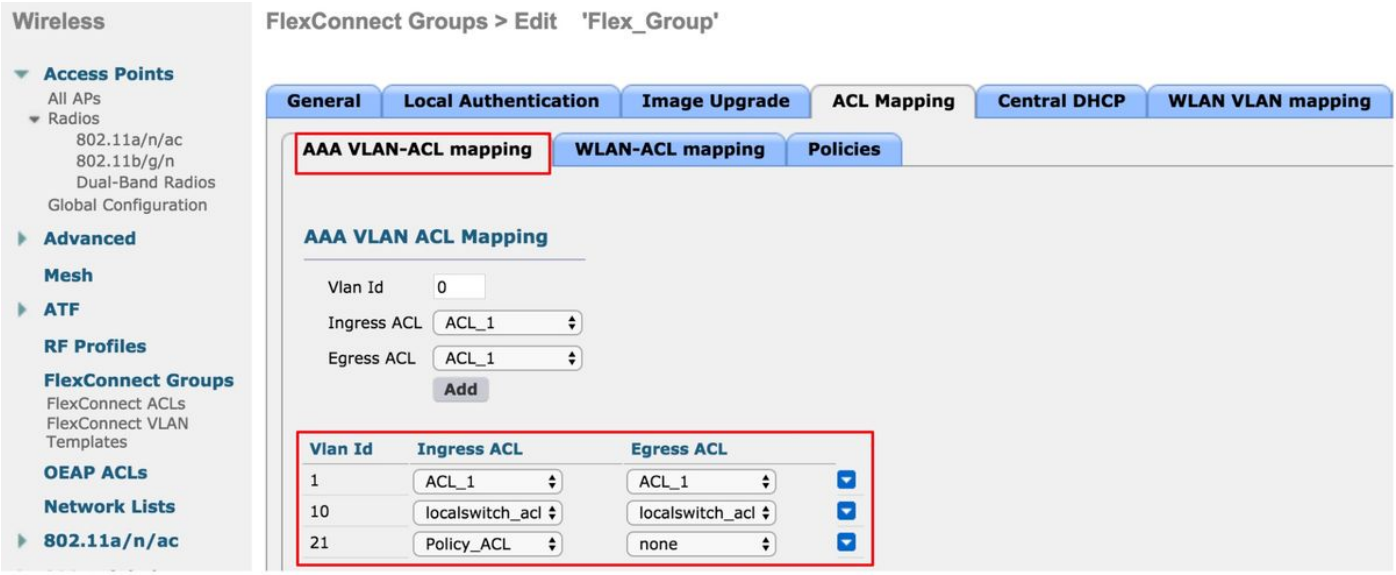
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Tipos de ACL

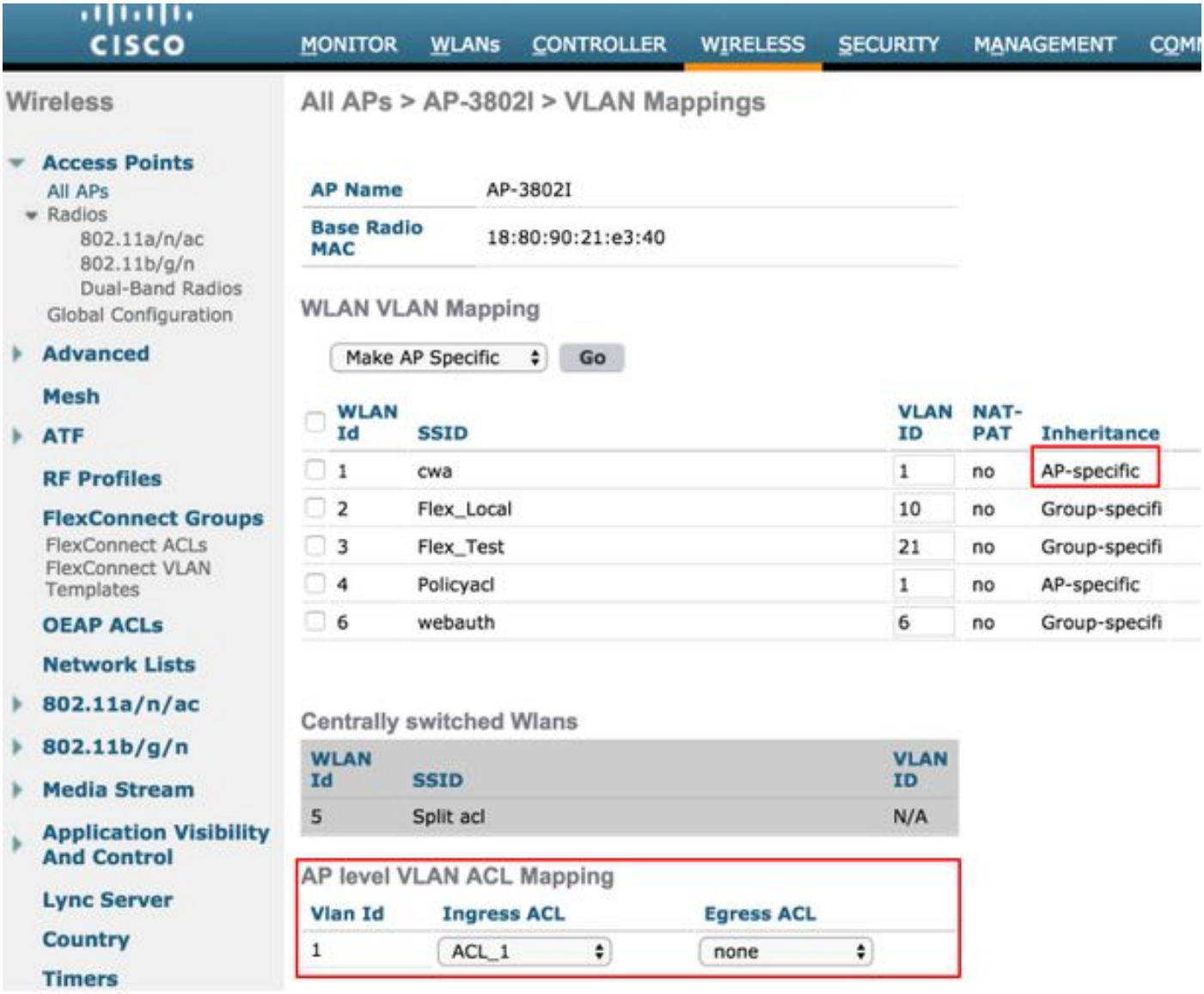
1. VLAN ACL

A ACL da VLAN é a ACL mais usada e permite controlar o tráfego do cliente que é enviado para dentro e para fora da VLAN.

A ACL pode ser configurada de acordo com o grupo flexconnect que usa a seção de mapeamento de **VLAN-ACL AAA** em **Grupos de Flexconnect sem fio > Mapeamento de ACL > Mapeamento de VLAN-ACL AAA** conforme mostrado na imagem.



Ele também pode ser configurado conforme o nível de AP, navegue para **Wireless > All APs > AP name > Flexconnect tab** e clique na seção **VLAN mappings**. Aqui, você precisa tornar o VLAN config AP específico primeiro, depois disso você pode especificar o mapeamento da VLAN-ACL no nível de AP como mostrado na imagem.



Instruções da ACL

Você também pode especificar a direção na qual a ACL é aplicada:

- Ingresso (entrada significa para o cliente sem fio)
- Saída (em direção ao DS ou LAN),
- ambos ou nenhum.

Assim, se você quiser bloquear o tráfego destinado ao cliente sem fio, poderá usar a direção de ingresso e, se quiser bloquear o tráfego originado pelo cliente sem fio, poderá usar a direção de saída.

A opção nenhum é usada quando você deseja enviar uma ACL separada com o uso da substituição de Autenticação, Autorização e Contabilidade (AAA). Nesse caso, a ACL enviada pelo servidor radius é aplicada dinamicamente ao cliente.

> **Note**: A ACL precisa ser configurada na ACL Flexconnect antes, caso contrário ela não será aplicada.

Considerações sobre o mapeamento de ACL

Ao usar ACLs de VLAN, também é importante entender estas considerações com relação aos mapeamentos de VLAN em APs do flexconnect:

- Se a VLAN estiver configurada com o uso do grupo FlexConnect, a ACL correspondente configurada no grupo FlexConnect será aplicada.
- Se uma VLAN for configurada no grupo FlexConnect e também no AP (como uma configuração específica do AP), a configuração da ACL do AP terá precedência.
- Se a ACL específica do AP estiver configurada como nenhuma, nenhuma ACL será aplicada.
- Se a VLAN retornada da AAA não estiver presente no AP, o cliente retorna à VLAN padrão configurada para a LAN sem fio (WLAN) e qualquer ACL mapeada para essa VLAN padrão tem precedência.

Verifique se a ACL está aplicada no AP

Use esta seção para confirmar se a sua configuração funciona corretamente.

1. APs da onda 2

Em um AP de onda 2, você pode verificar se a ACL realmente é enviada para o AP com o comando **show flexconnect vlan-acl**. Aqui, você também pode ver o número de pacotes transmitidos e descartados para cada 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. APs do Cisco IOS®

No nível do AP, você pode validar se a configuração da ACL foi enviada para o AP de duas maneiras:

- Use o comando **show access-lists** que mostra se todas as ACLs de VLAN estão configuradas no 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
```

Você também pode monitorar a atividade que acontece em cada ACL, verificar a saída detalhada dessa ACL e ver a contagem de ocorrências para cada linha:

```
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)
```

- Como as ACLs de VLAN são aplicadas na interface gigabit, você pode validar se a ACL está aplicada corretamente. Verifique a saída da subinterface como mostrado aqui:

```
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
```

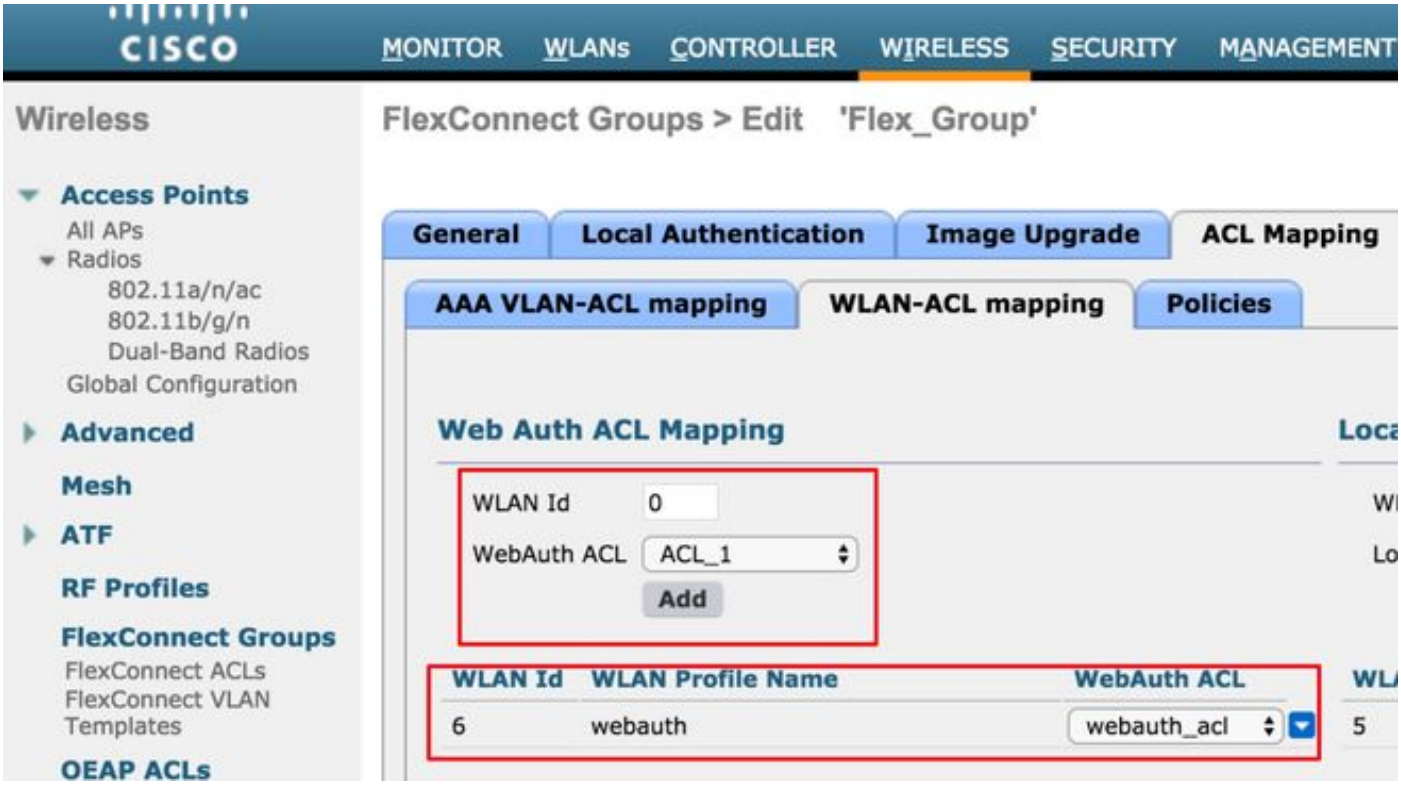
2. ACL de Webauth

A ACL da Web é usada no caso de um SSID (Service Set Identifier) da Webauth/Passthrough que foi ativado para switching local do flexconnect. Isso é usado como uma ACL de pré-autenticação e permite o tráfego do cliente para o servidor de redirecionamento. Quando o redirecionamento é concluído e o cliente está no estado **RUN**, a ACL para para de entrar em vigor.

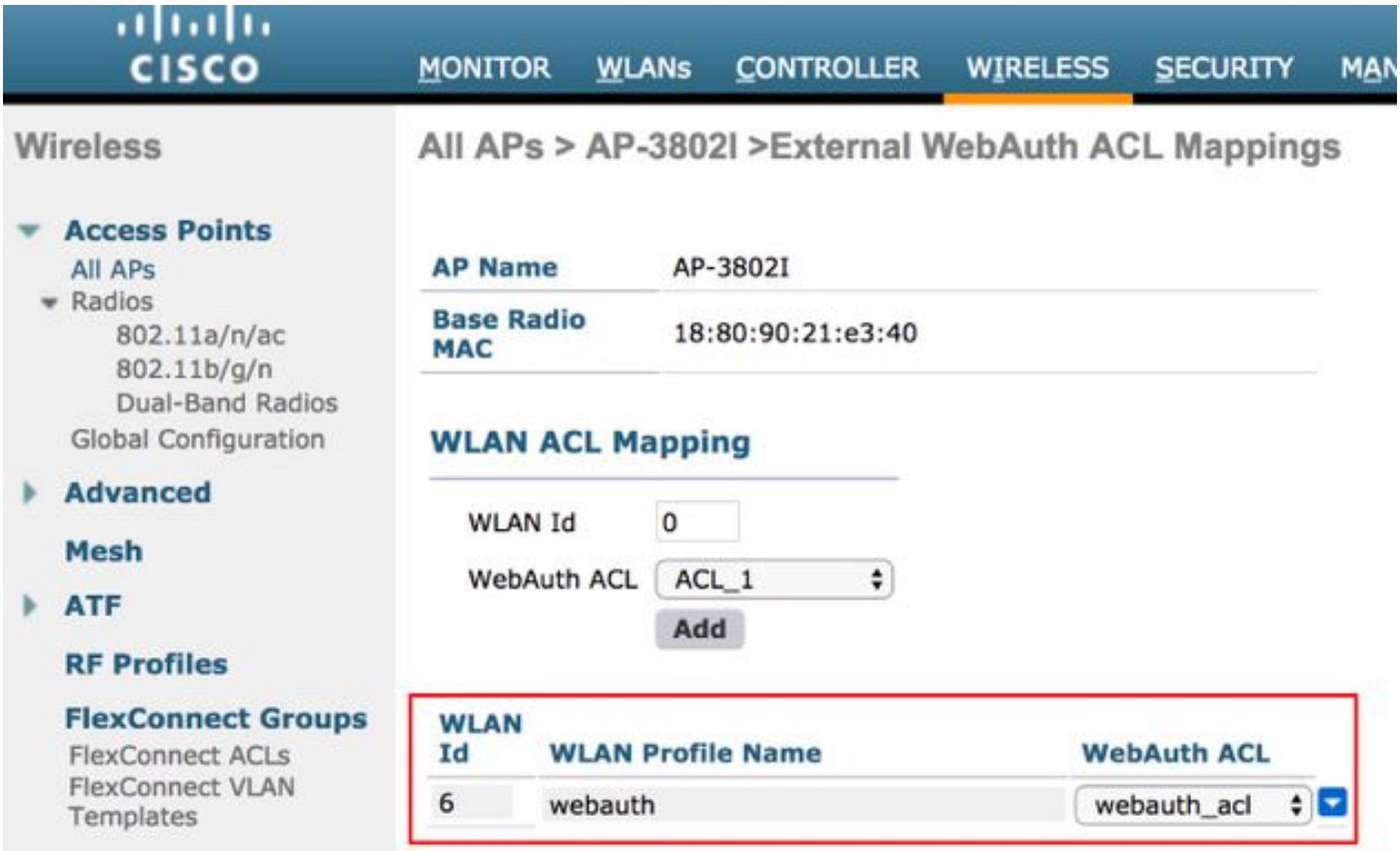
A ACL da Web pode ser aplicada no nível da WLAN, no nível do AP ou no nível do grupo flexconnect. Uma ACL específica do AP tem a prioridade mais alta, enquanto a ACL da WLAN tem a mais baixa. Se todos os três forem aplicados, o AP Specific tem precedência seguida de Flex ACL e depois de WLAN Global Specific ACL.

Pode haver um máximo de 16 ACLs Web-Auth configuradas em um AP.

Ele pode ser aplicado no nível do grupo flexconnect, navegue para **Wireless > Flexconnect Groups > Select the group you want configure > ACL mapping > WLAN-ACL mapping > Web Auth ACL Mapping** como mostrado na imagem.



A ACL pode ser aplicada no nível do AP, navegue para **Wireless >Todos os APs >Nome do AP >Guia Flexconnect > ACLs de autenticação da Web externa > ACL da WLAN** como mostrado na imagem.



A ACL pode ser aplicada no nível da WLAN, navegue para **WLAN > WLAN_ID > Layer 3 > WebAuth FlexAcl**, como mostrado na imagem.

No Cisco IOS® AP, você pode verificar se a ACL foi aplicada ao cliente. Verifique a saída de **show controllers dot11radio 0 client** (ou 1 se o cliente se conectar ao rádio A) como mostrado aqui:

```
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
```

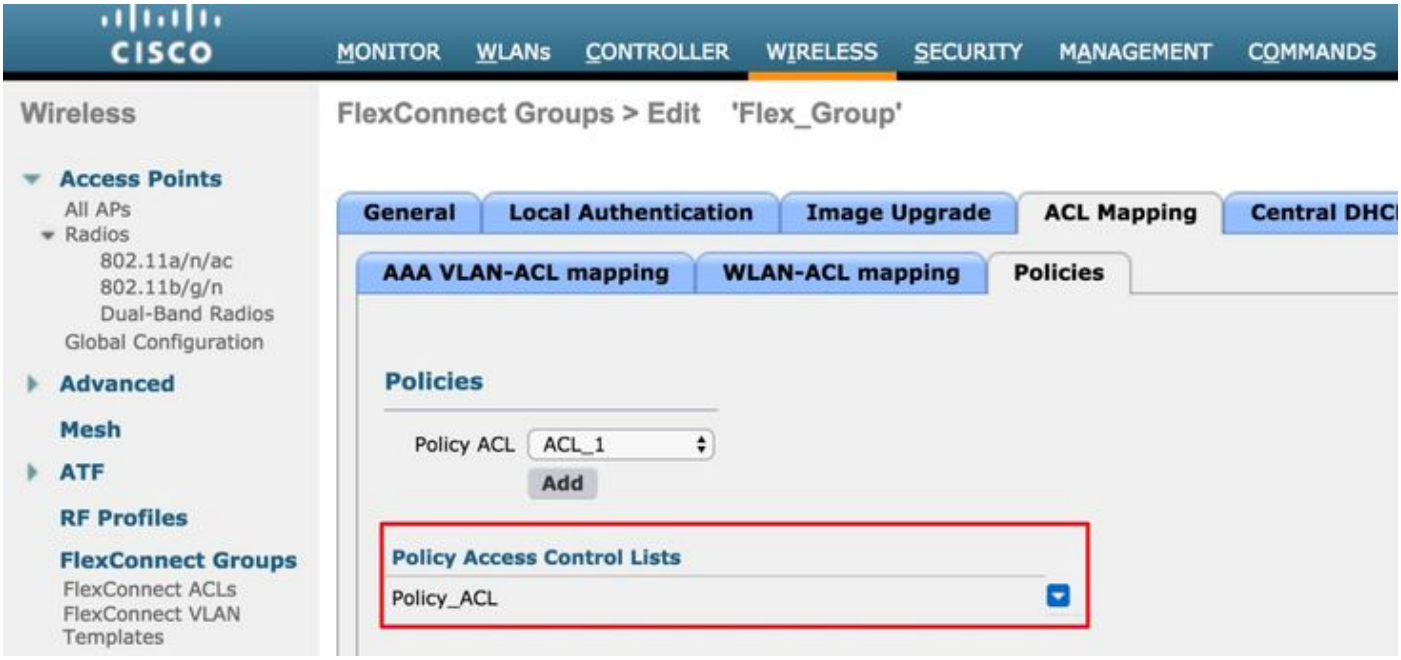
3. ACL de política da Web

A ACL da WebPolicy é usada para redirecionamento condicional da Web, redirecionamento da Web da página inicial e cenários da Web central.

Há dois modos de configuração disponíveis para WLANs WebPolicy com ACLs Flex:

1. Grupo Flexconnect

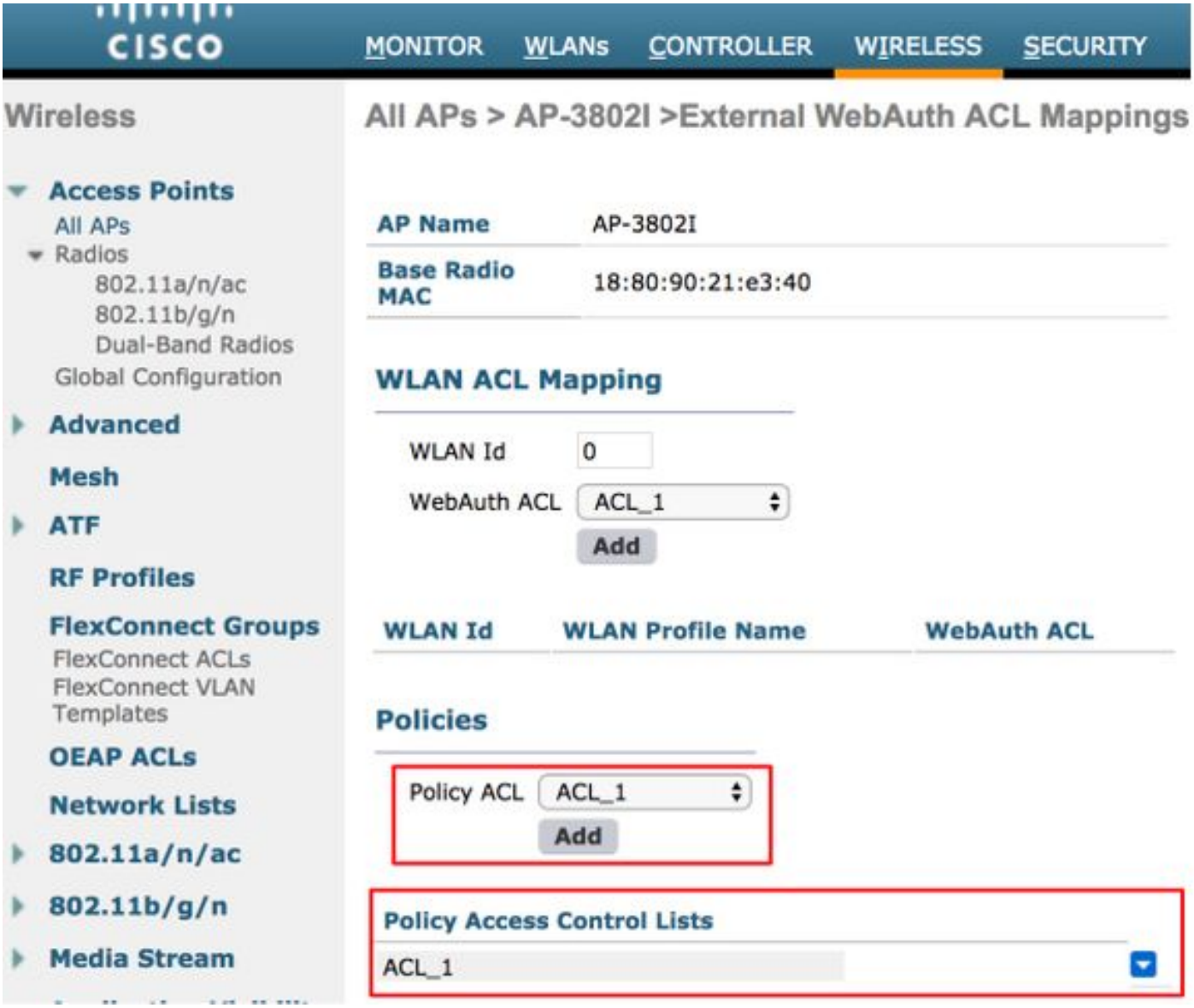
Todos os APs no grupo FlexConnect recebem a ACL configurada. Isso pode ser configurado à medida que você navega para **Wireless-Flexconnect Groups > Select the group you want configure > ACL mapping > Policies**, e adiciona o nome da ACL de política conforme mostrado na imagem:



2. Específico de AP

O AP para o qual a configuração é feita recebe a ACL, nenhum outro AP é afetado. Isso pode ser configurado à medida que você navega para **Sem fio > Todos os APs > Nome do AP >**

Guia Flexconnect > External WebAuthentication ACLs > Policies como mostrado na imagem.



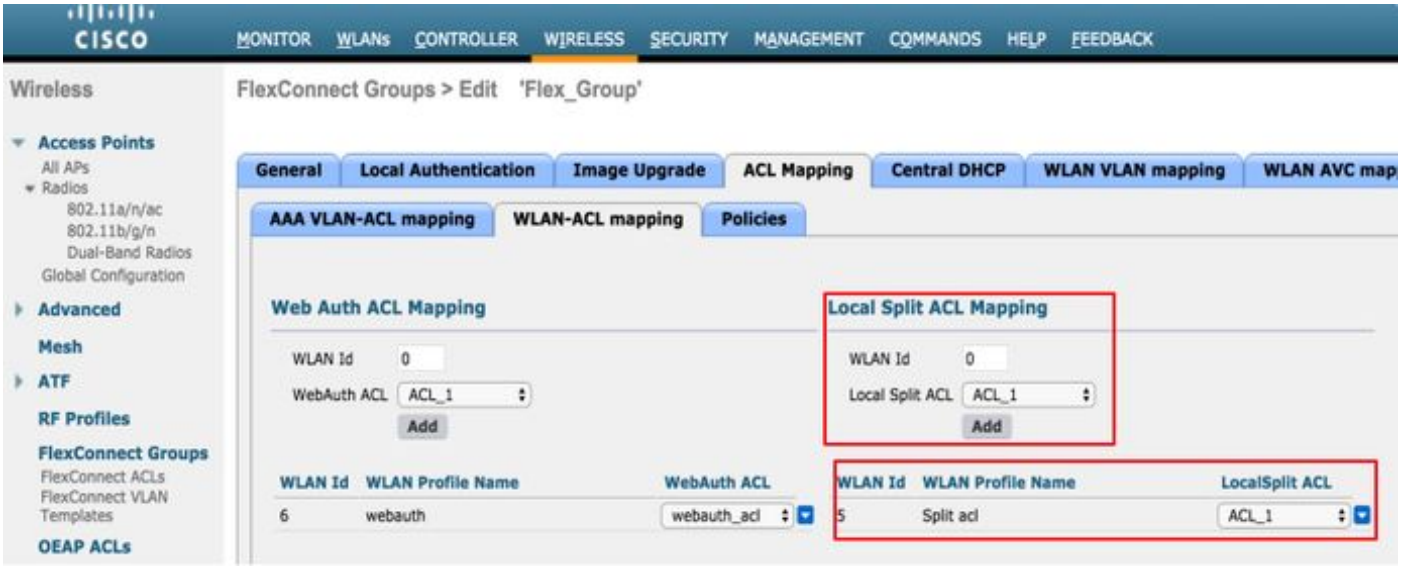
Após uma autenticação L2 bem-sucedida, quando o servidor radius envia o nome da ACL no par AV de ACL de redirecionamento, isso é aplicado diretamente ao cliente no AP. Quando o cliente entra no estado **RUN**, todo o tráfego do cliente é comutado localmente e o AP para de aplicar a ACL.

Pode haver um máximo ou 32 ACLs de política da Web configuradas em um AP. 16 AP específico e 16 grupo FlexConnect específico.

4. Dividir ACL do túnel

As ACLs de tunelamento dividido são usadas com SSIDs comutados centralmente quando parte do tráfego do cliente precisa ser enviado localmente. A funcionalidade Split Tunneling também é uma vantagem adicional para a configuração do OEAP (Office Extend Access Point), onde os clientes em um SSID corporativo podem se comunicar com dispositivos em uma rede local (impressoras, máquinas com fio em uma porta LAN remota ou dispositivos sem fio em um SSID pessoal) diretamente, assim que eles forem mencionados como parte da ACL do túnel dividido.

As ACLs de tunelamento dividido podem ser configuradas de acordo com o nível de grupo flexconnect, navegue para **Wireless-Flexconnect Groups > Select the group you want configure > ACL mapping > WLAN-ACL mapping > Local Split ACL Mapping** conforme mostrado na imagem.



Eles também podem ser configurados conforme o nível de AP, navegue para **Wireless > All APs > AP name > Flexconnect tab > Local Split ACLs** e adicione o nome do flexconnect ACL como mostrado na imagem.

As ACLs de tunelamento dividido não podem ligar localmente o tráfego Multicast/Broadcast. O tráfego multicast/broadcast é comutado centralmente mesmo que corresponda à ACL FlexConnect.

Troubleshoot

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.