Configurar Flexconnect ACL no WLC

Índice

Introdução

Este documento descreve os vários tipos do Access Control List do flexconnect (ACL) e como podem ser configurados e validado no Access Point (AP).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- O controlador de LAN do Cisco Wireless (WLC) esse executa o código 8.3 e mais alto
- Configuração de Flexconnect no WLC

Componentes Utilizados

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

- O Cisco 8540 Series WLC que executa o software release 8.3.133.0.
- 3802 e 3702 AP que são executado no modo do flexconnect.

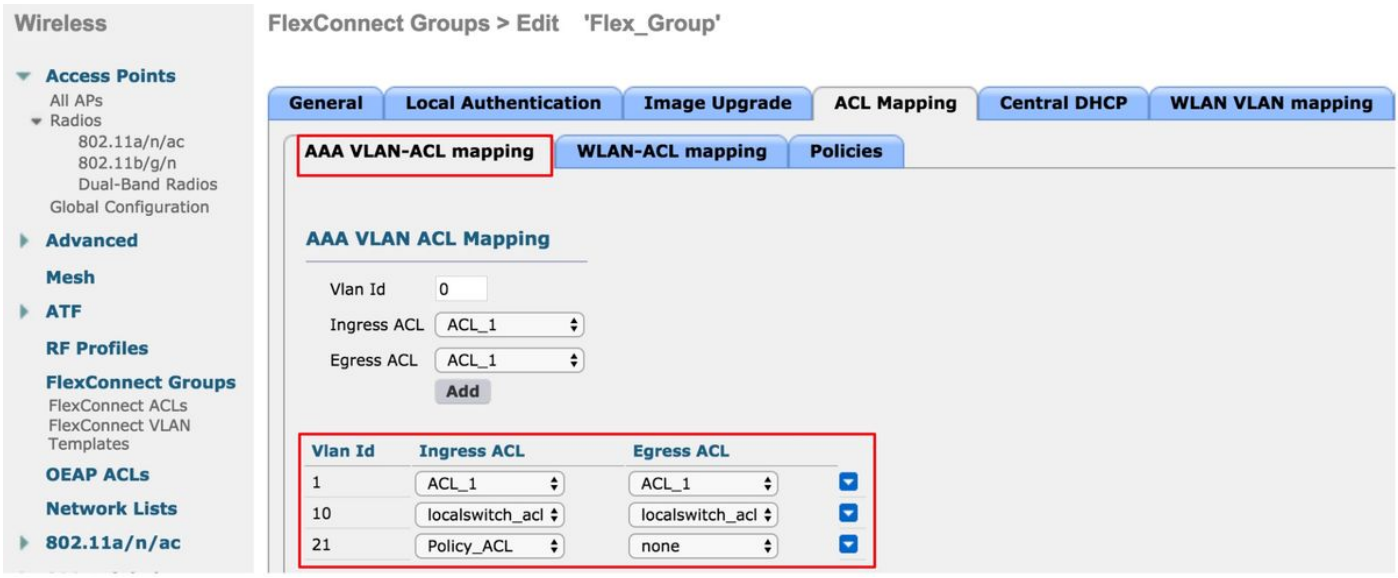
As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Tipos ACL

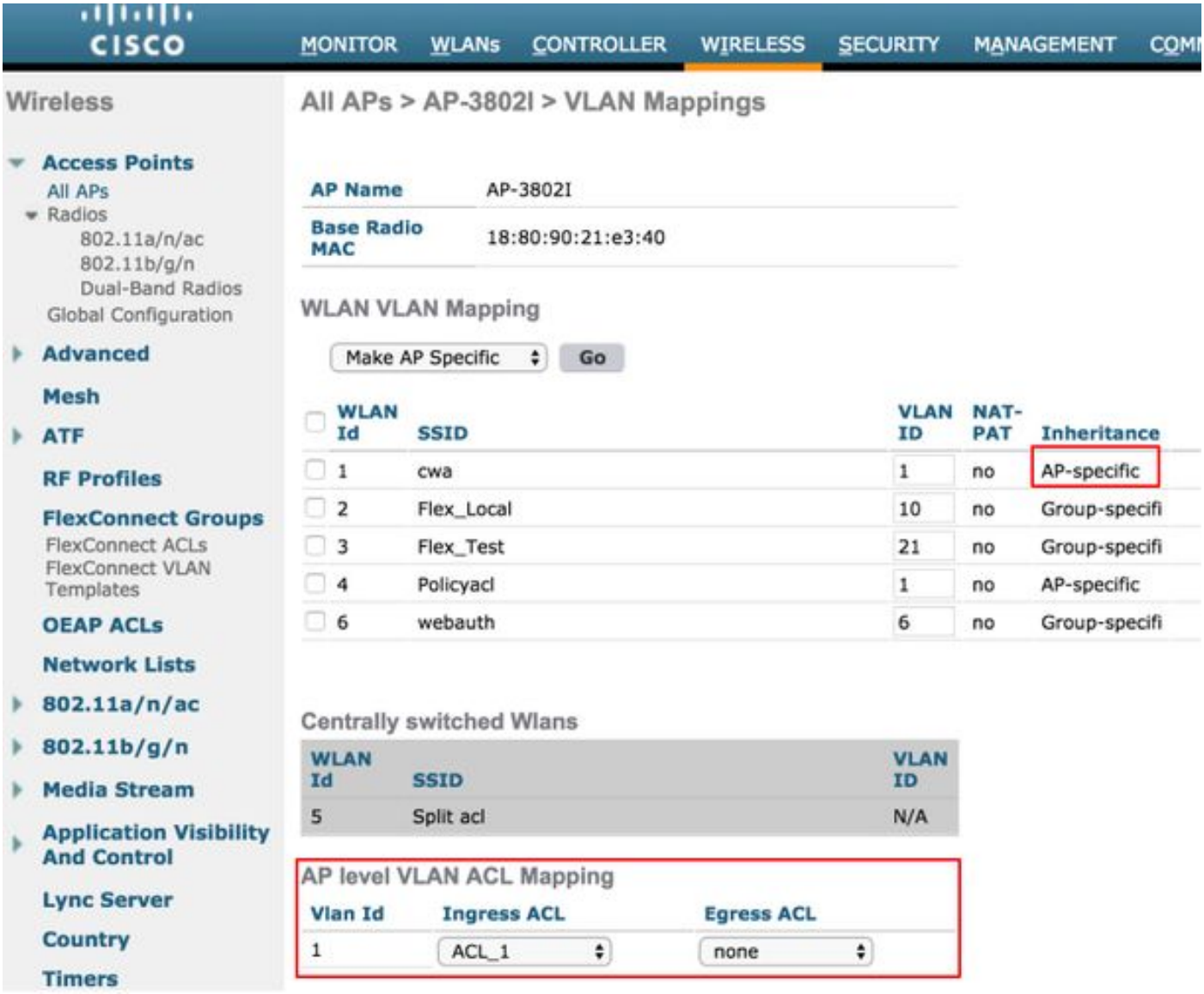
1. VLAN ACL

O VLAN ACL é o ACL o mais de uso geral e deixa-o controlar o tráfego do cliente que é enviado dentro e fora do VLAN.

O ACL pode ser configurado conforme o grupo do flexconnect que usa a seção do mapeamento **AAA VLAN-ACL no Sem fio-Flexconnect agrupa > mapeamento ACL > mapeamento AAA VLAN-ACL** segundo as indicações da imagem.



Pode igualmente ser configurado conforme o nível AP, navegar ao **Sem fio > todo o nome AP > AP > aba de Flexconnect** e clicar a seção dos **mapeamentos VLAN**. Aqui, você precisa de fazer primeiramente o específico da configuração AP VLAN, depois do qual você pode especificar o mapeamento do nível VLAN-ACL AP segundo as indicações da imagem.



Sentidos ACL

Você pode igualmente especificar o sentido em que o ACL obtém aplicado:

- Ingresso (o ingresso significa para o cliente Wireless)
- Saída (para o theDS ou o LAN),
- ambo ou nenhuns.

Assim, se você gostaria de obstruir o tráfego destinado para o cliente Wireless então que você pode usar a direção de ingresso e se você gostaria de obstruir o tráfego originado pelo cliente Wireless, você pode usar a direção de saída.

A opção nenhuns é usada quando você gostaria de empurrar um ACL separado com o uso da ultrapassagem do Authentication, Authorization, and Accounting (AAA). Neste caso, o ACL enviado pelo servidor Radius é aplicado dinamicamente ao cliente.

> **Note**: O ACL precisa de ser configurado de antemão sob Flexconnect ACL, se não não obtém aplicado.

Considerações do mapeamento ACL

Quando você usa VLAN ACL, é igualmente importante compreender estas considerações no que diz respeito aos mapeamentos VLAN no flexconnect AP:

- Se o VLAN é configurado com o uso do grupo de FlexConnect, o ACL correspondente configurado no grupo de FlexConnect é aplicado.
- Se um VLAN está configurado no grupo de FlexConnect e igualmente no AP (como uma configuração específica AP), a seguir a configuração ACL AP toma a precedência.
- Se o AP ACL específico é configurado a nenhuns, a seguir nenhum ACL é aplicado.
- Se o VLAN que esteve retornado do AAA não está atual no AP, o cliente cai de volta ao VLAN padrão configurado para o Wireless LAN (WLAN) e todo o ACL traçado a esse VLAN padrão toma a precedência.

Verifique se o ACL é aplicado no AP

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

1. Onda 2 AP

Em uma onda 2 AP, você pode verificar se o ACL obtém realmente empurrado para o AP com o **flexconnect VLAN-ACL do** comando show. Aqui, você pode igualmente ver o número de passado e pacotes descartado 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. Cisco IOS® AP

A nível AP, você pode validar se a configuração ACL foi empurrada para o AP com duas maneiras:

- Use o **comando show access-lists** que mostra se todo o VLAN ACL é configurado 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 pode igualmente monitora a atividade que acontece em cada ACL, verifica a saída detalhada desse ACL e vê a contagem da batida 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)
```

- Desde que o VLAN ACL é aplicado na interface de gigabit, você pode validar se o ACL é aplicado corretamente. Verifique as saídas de interface secundárias 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
```

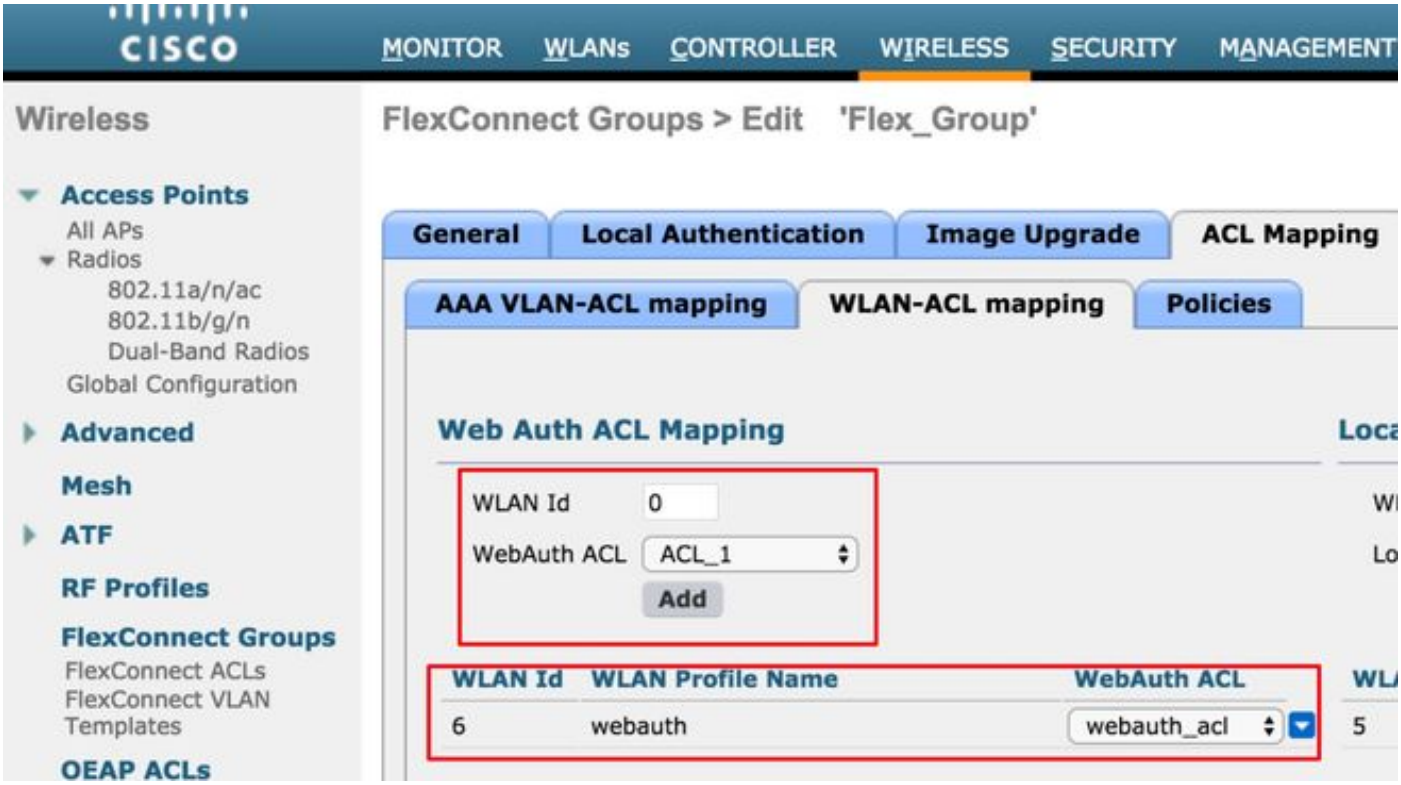
2. Webauth ACL

Webauth ACL é usado no caso de um Service Set Identifier (SSID) Webauth/Webpassthrough que foi permitido para o switching local do flexconnect. Isto é usado como uma PRE-autenticação ACL e permite o tráfego do cliente à redirecionar servidor. Uma vez que a reorientação está completa e o cliente está no estado de **CORRIDA**, as paradas ACL para tomá-lo no efeito.

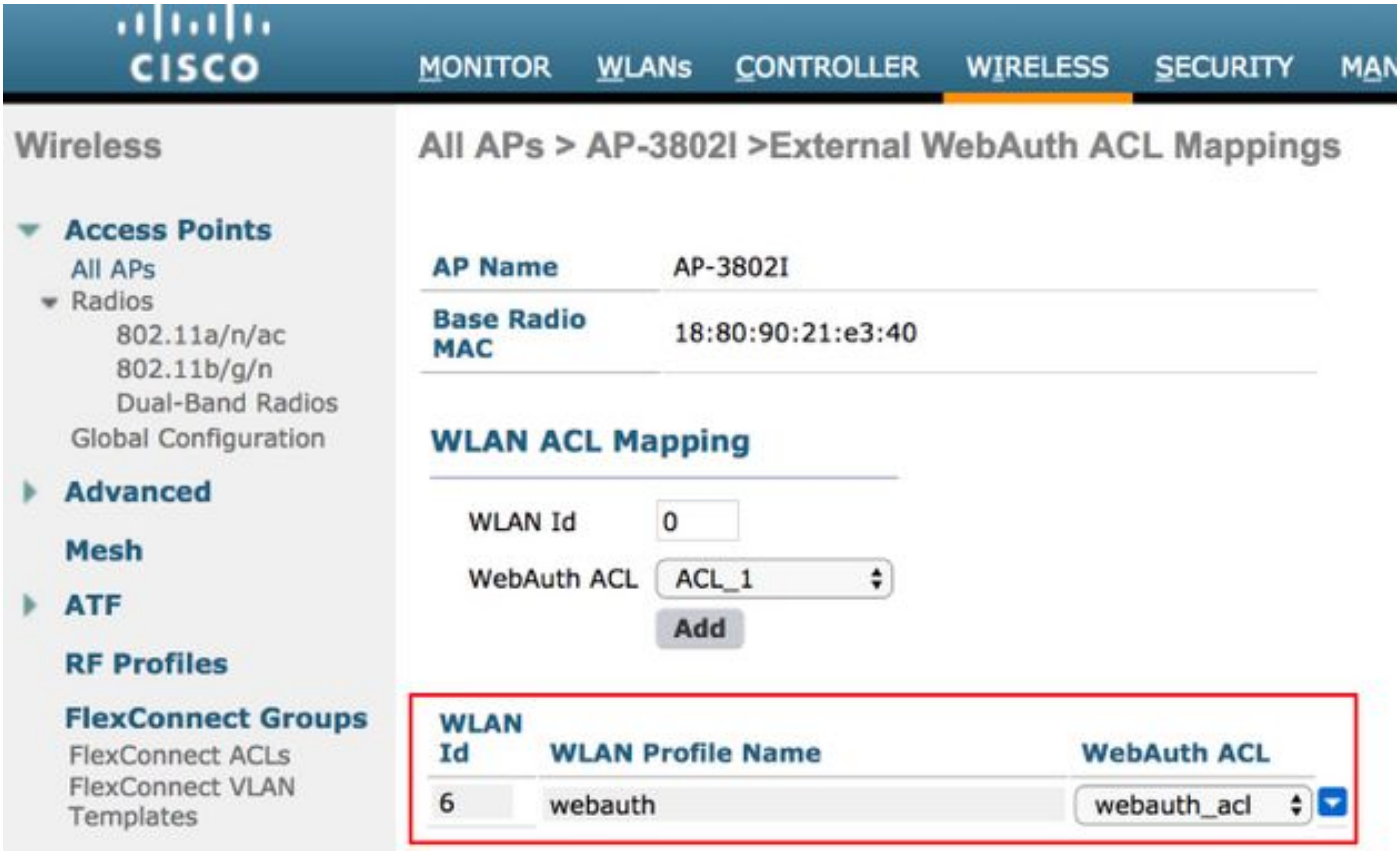
Webauth ACL pode ser aplicado a nível WLAN, nível AP ou nível do grupo do flexconnect. Um AP ACL específico tem a prioridade mais alta, visto que o WLAN ACL tem o mais baixo. Se todos os três são aplicados, o específico AP toma a precedência seguida pelo cabo flexível ACL e então pelo específico global ACL WLAN.

Pode haver um máximo de 16 Web-AUTH ACL configurados em um AP.

Pode ser aplicado a nível do grupo do flexconnect, navega ao **Sem fio > aos grupos de Flexconnect > seleciona o grupo que você quer configura > mapeamento ACL > mapeamento WLAN-ACL > mapeamento do AUTH ACL da Web** segundo as indicações da imagem.



O ACL pode ser aplicado a nível AP, navega à **aba wireless do >Flexconnect do nome >AP do >All AP > WebAuthentication externo ACL > WLAN ACL** segundo as indicações da imagem.



O ACL pode ser aplicado a nível WLAN, navega a **WLAN > WLAN_ID > camada 3 > WebAuth FlexAcl** segundo as indicações da imagem.

Em Cisco IOS® AP, você pode verificar se o ACL foi aplicado ao cliente. Verifique a saída do **cliente dos controladores dot11radio 0** (ou 1 da **mostra** se o cliente conecta 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
```

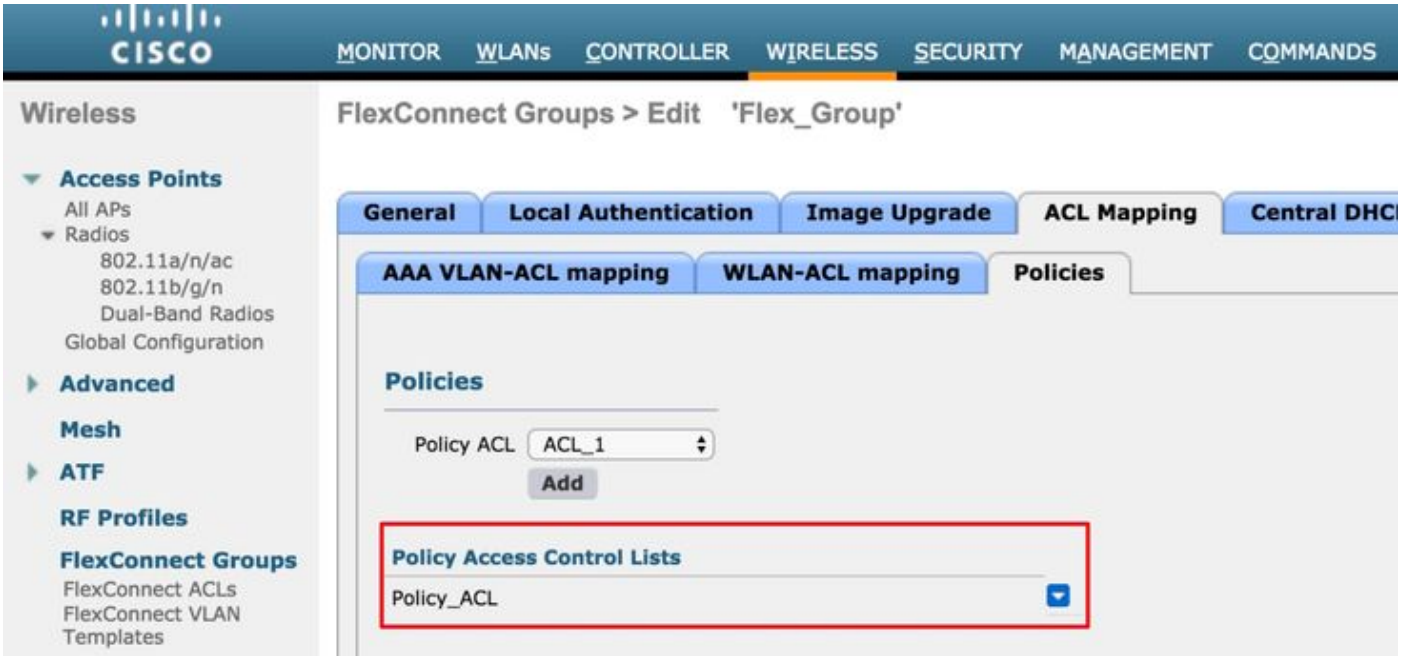
3. Política ACL da Web

WebPolicy ACL é usado para a Web condicional reorienta, a Web da página do respingo reorienta e encenações centrais de Webauth.

Há dois modos de configuração disponíveis para WebPolicy WLAN com cabo flexível ACL:

1. Grupo de Flexconnect

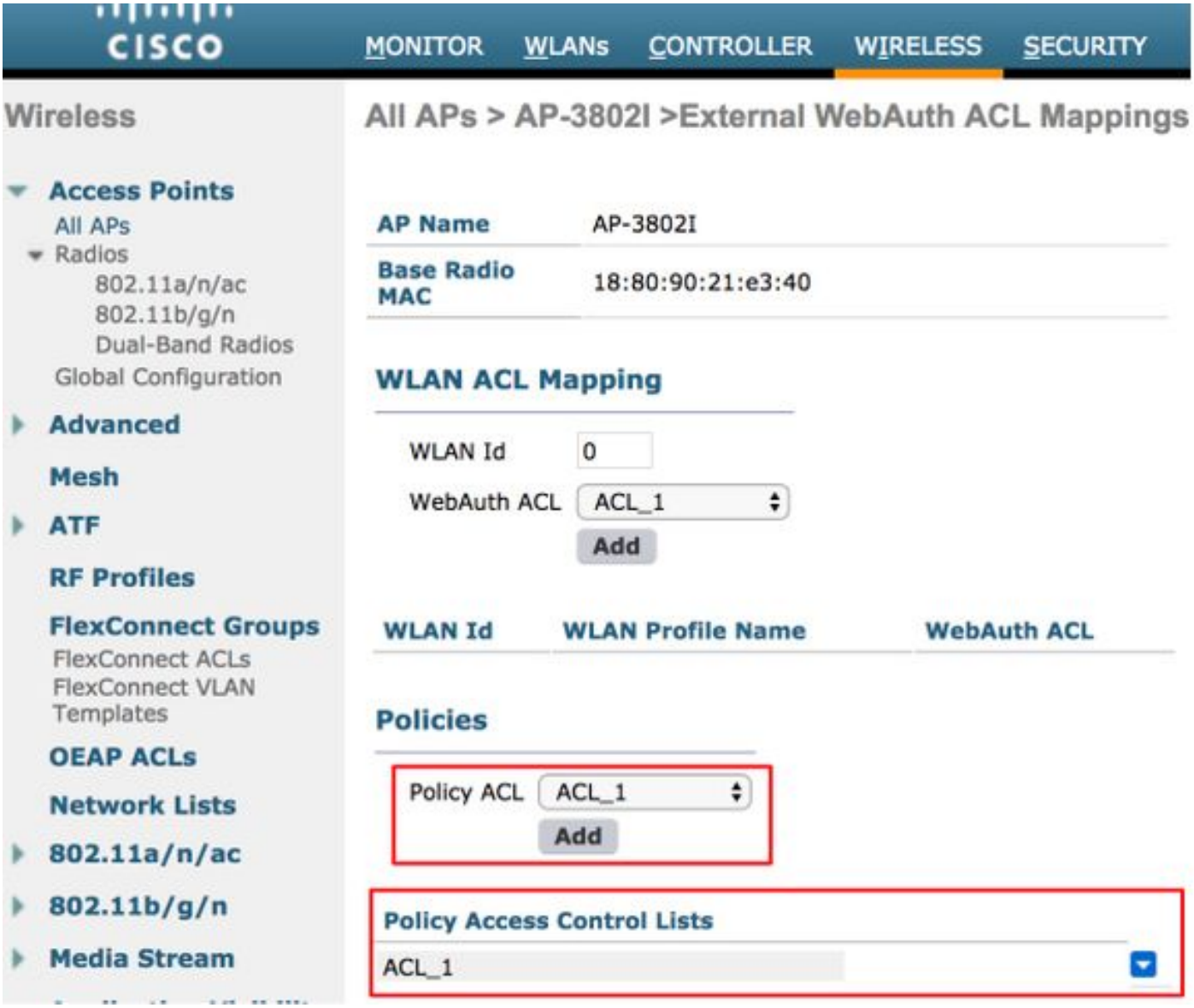
Todos os AP no grupo de FlexConnect recebem o ACL que é configurado. Isto pode ser configurado como você navega aos **grupos do Sem fio-Flexconnect > seleciona o grupo que você quer configura > mapeamento > políticas ACL**, e adiciona o nome da política ACL segundo as indicações da imagem:



2. Específico AP

O AP para que a configuração é feita recebe o ACL, nenhuns outros AP é impactado. Isto pode ser configurado como você navega ao **Sem fio > todo o AP > nome AP >**

Aba de Flexconnect > WebAuthentication externo ACL > políticas segundo as indicações da imagem.



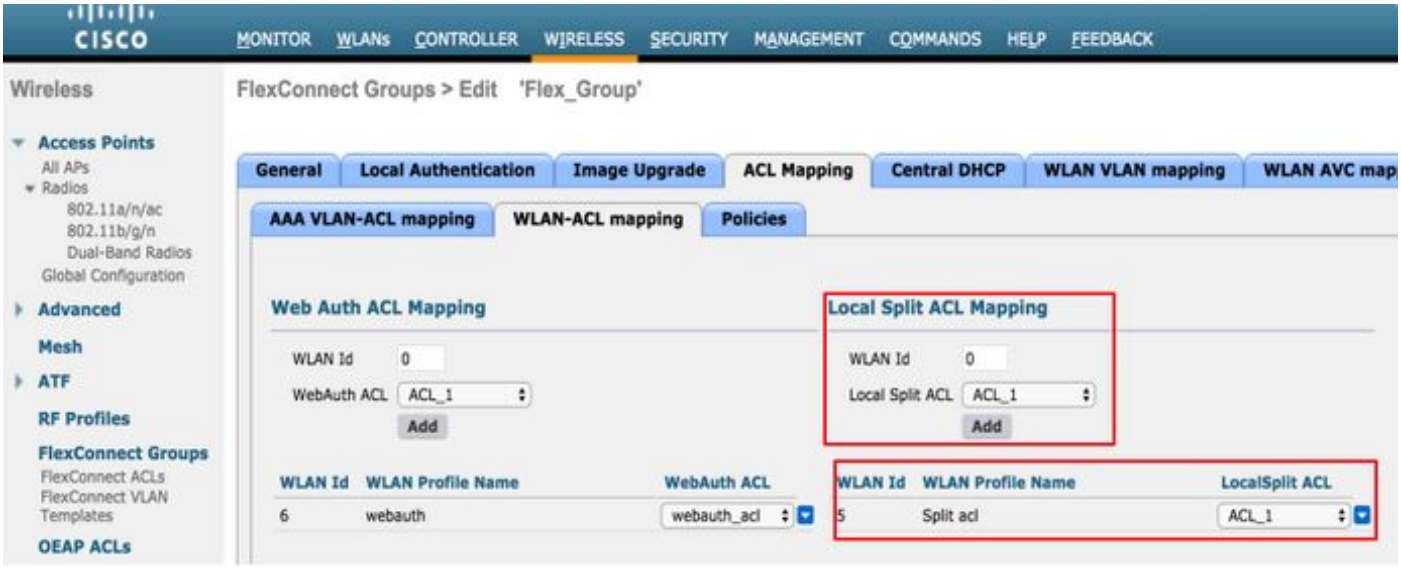
Após uma autenticação L2 bem sucedida, quando o servidor Radius envia o nome ACL no par AV reorientar-ACL, isto obtém aplicado diretamente para o cliente no AP. Quando o cliente se move no estado de **CORRIDA**, todo o tráfego do cliente está comutado localmente e o AP para para aplicar o ACL.

Pode haver um máximo ou 32 WebPolicy ACL configurado em um AP. 16 AP específicos e específico do grupo de 16 FlexConnect.

4. Túnel em divisão ACL

O Split Tunneling ACL está usado com os SSID centralmente comutados quando algum do tráfego do cliente precisa de ser enviado sobre localmente. A funcionalidade do Split Tunneling é igualmente uma vantagem adicionada para o escritório estende o Access point (OEAP) setup onde os clientes em um SSID corporativo podem falar aos dispositivos em uma rede local (impressoras, máquina prendida em uma porta do LAN remota, ou dispositivos Wireless em um SSID pessoal) diretamente uma vez que são mencionados como parte do túnel em divisão ACL.

O Split Tunneling ACL pode ser configurado sobre conforme o nível de grupo do flexconnect, navega aos **grupos do Sem fio-Flexconnect > seleciona o grupo que você quer configura > mapeamento ACL > mapeamento WLAN-ACL > mapeamento local da separação ACL** segundo as indicações da imagem.



Podem igualmente ser configurados a conforme nível AP, navegar ao **Sem fio > todo o nome AP > AP > aba de Flexconnect > a separação local ACL** e adicionar o nome do flexconnect ACL segundo as indicações da imagem.

O Split Tunneling ACL não pode localmente construir uma ponte sobre o Multicast/tráfego de broadcast. O Multicast/tráfego de broadcast é comutado centralmente mesmo se combina o FlexConnect ACL.

Troubleshooting

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