在WLC上配置Flexconnect ACL

目录

简介

本文档介绍各种flexconnect访问控制列表(ACL)类型，以及如何在接入点(AP)上配置和验证这些类型。

先决条件

要求

Cisco 建议您了解以下主题：

- 运行代码8.3及更高版本的思科无线局域网控制器(WLC)
- WLC上的FlexConnect配置

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行软件版本8.3.133.0的Cisco 8540系列WLC。
- 以flexconnect模式运行的3802和3702 AP。

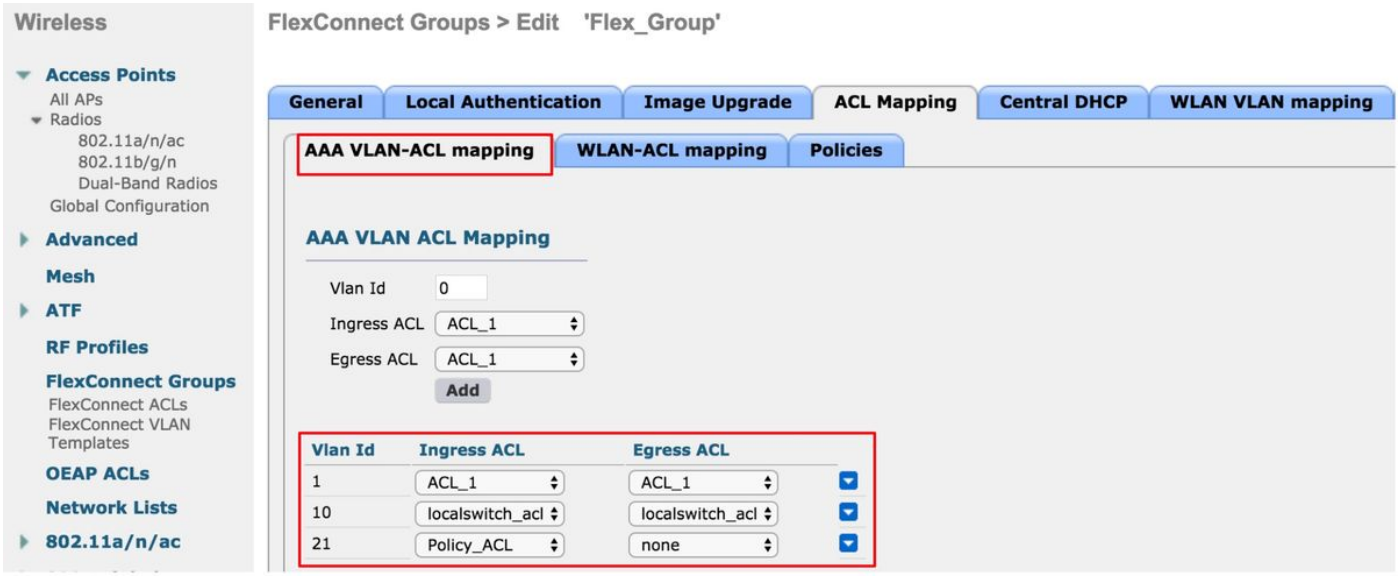
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

ACL类型

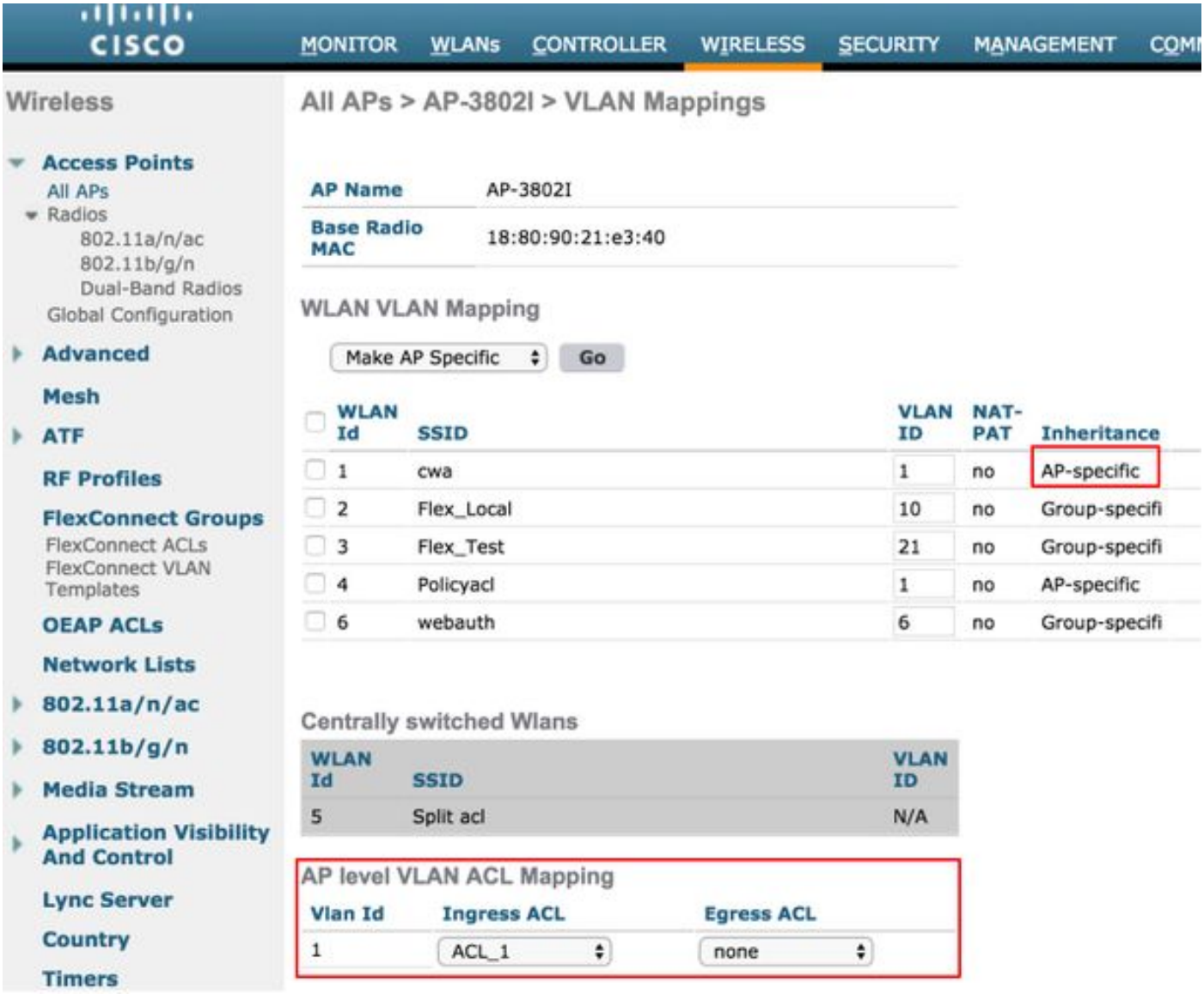
1. VLAN ACL

VLAN ACL是最常用的ACL，它允许您控制进出VLAN的客户端流量。

ACL可以按照使用**Wireless-Flexconnect Groups > ACL mapping > AAA VLAN-ACL映射(**如图所示)中AAA VLAN-ACL映射部分的Flexconnect组进行配置。



也可以根据AP级别进行配置，导航至**Wireless > All AP's > AP name > Flexconnect选项卡，然**后单击**VLAN映射**部分。在此，您需要先将VLAN配置AP设置为特定AP，然后您可以指定AP级VLAN-ACL映射，如图所示。



ACL方向

您还可以指定应用ACL的方向：

- 入口（入口指向无线客户端）
- 出口（面向DS或LAN），
- 两者都不行。

因此，如果您希望阻止发往无线客户端的流量，则可以使用入口方向；如果您希望阻止来自无线客户端的流量，则可以使用出口方向。

当您要使用身份验证、授权和记帐(AAA)覆盖推送单独的ACL时，将使用无选项。在这种情况下，RADIUS服务器发送的ACL将动态应用到客户端。

注意：ACL需要预先在Flexconnect ACL下配置，否则不会应用。

ACL映射注意事项

使用VLAN ACL时，了解FlexConnect AP上VLAN映射的以下注意事项也很重要：

- 如果VLAN配置为使用FlexConnect组，则应用在FlexConnect组上配置的相应ACL。
- 如果VLAN在FlexConnect组和AP上都配置（作为AP特定配置），则AP ACL配置优先。
- 如果将AP特定ACL配置为无，则不应用ACL。
- 如果AP上不存在从AAA返回的VLAN，客户端将回退到为无线LAN(WLAN)配置的默认VLAN，并且映射到该默认VLAN的任何ACL都优先。

检验AP上是否应用了ACL

使用本部分可确认配置能否正常运行。

1.第2波AP

在第2波AP上，您可以使用命令show flexconnect vlan-acl检验ACL是否实际被**推送到AP**。在此，您还可以看到每个ACL的已传递和已丢弃数据包的数量。

```
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的

在AP级别，您可以通过两种方式验证ACL配置是否已推送到AP:

- 使用**show access-lists**命令，该命令显示AP上是否配置了所有VLAN ACL:

```
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
```

您还可以监控每个ACL上发生的活动，检查该ACL的详细输出，并查看每行的命中计数：

```
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)
```

- 由于VLAN ACL应用于千兆接口，因此您可以验证ACL是否应用正确。检查子接口输出，如下所示：

```
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
```

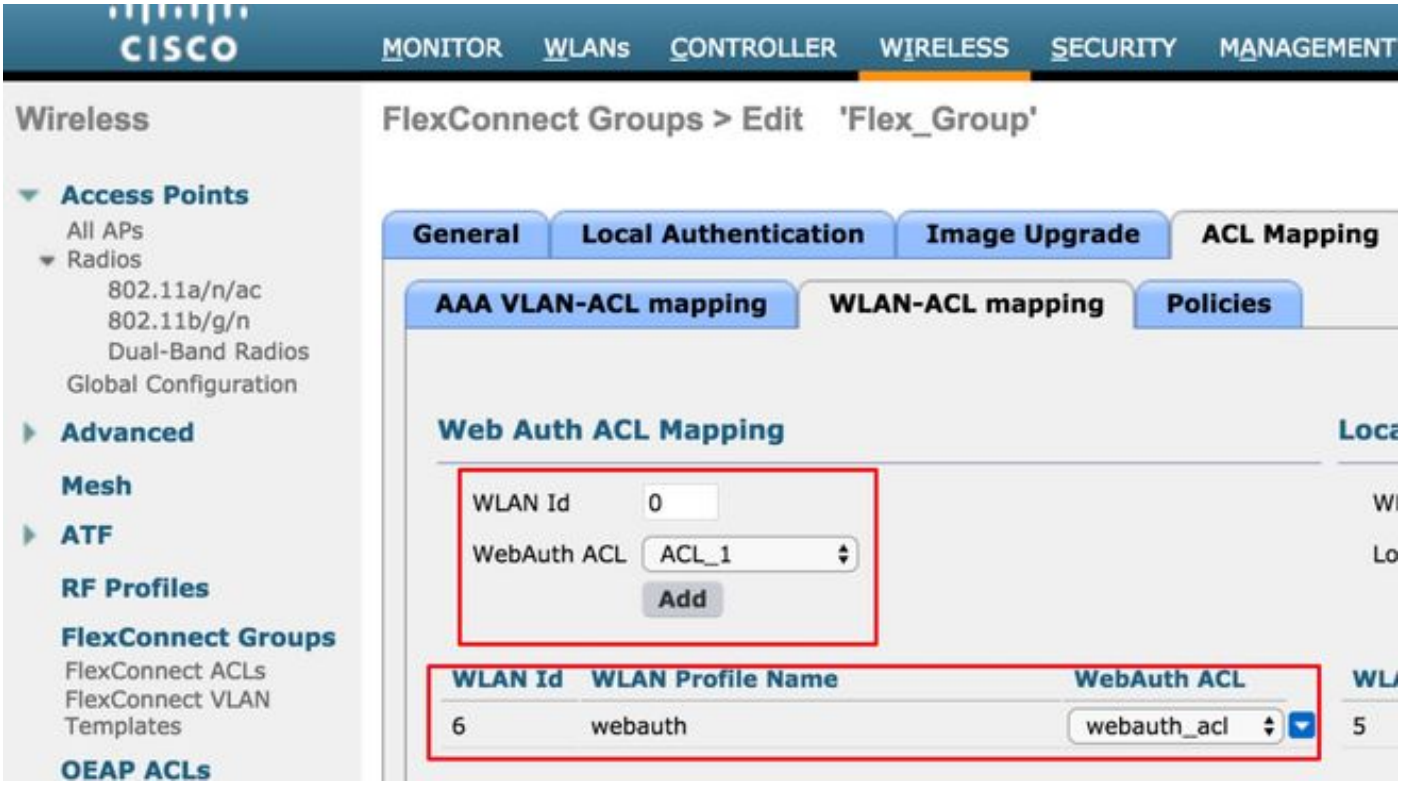
2. Webauth ACL

Webauth ACL用于Webauth/Webpassthrough服务集标识符(SSID)，该标识符已启用用于FlexConnect本地交换。这用作预身份验证ACL，允许客户端流量到重定向服务器。当重定向完成且客户端处于**RUN**状态时，ACL将停止，使其生效。

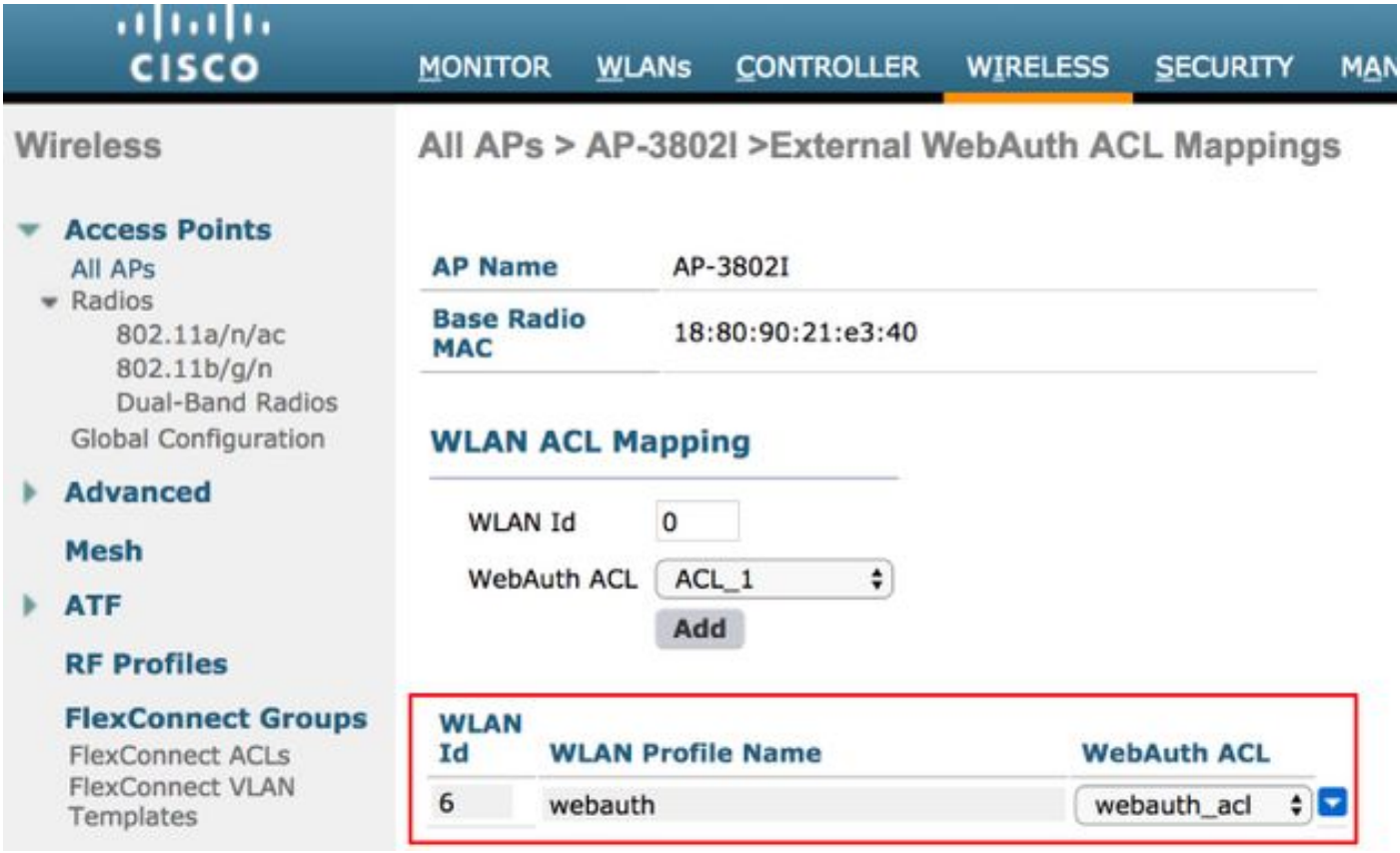
Webauth ACL可以在WLAN级别、AP级别或flexconnect组级别应用。AP特定ACL的优先级最高，而WLAN ACL的优先级最低。如果全部应用了这三个AP，则AP特定优先于Flex ACL，然后是WLAN全局特定ACL。

AP上最多可配置16个Web身份验证ACL。

可以在flexconnect组级别应用它，导航至**Wireless > Flexconnect Groups > Select the group you want configure > ACL mapping > WLAN-ACL mapping > Web Auth ACL Mapping**，如图所示。



ACL可以在AP级别应用，导航至**Wireless >All APs >AP name >Flexconnect选项卡> External WebAuthentication ACLs > WLAN ACL，如**图所示。



ACL可以在WLAN级别应用，导航至**WLAN > WLAN_ID > Layer 3 > WebAuth FlexAcl**，如图所示。

在Cisco IOS® AP上，您可以验证ACL是否已应用到客户端。如下所示，检**查show controllers dot11radio 0 client(或**1，如果客户端连接到A无线电)的输出：

```
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
```

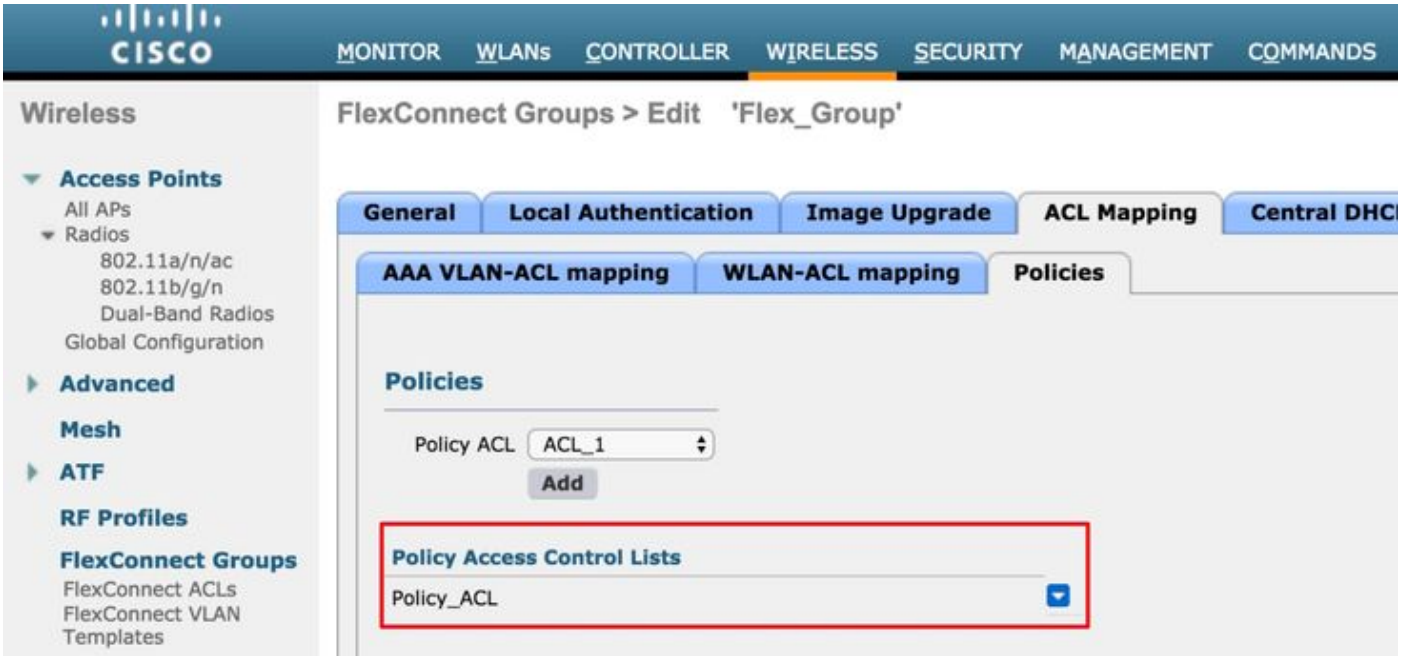
3. Web策略ACL

WebPolicy ACL用于条件Web重定向、启动页Web重定向和中心Webauth场景。

有两种配置模式可用于具有Flex ACL的WebPolicy WLAN:

1. Flexconnect组

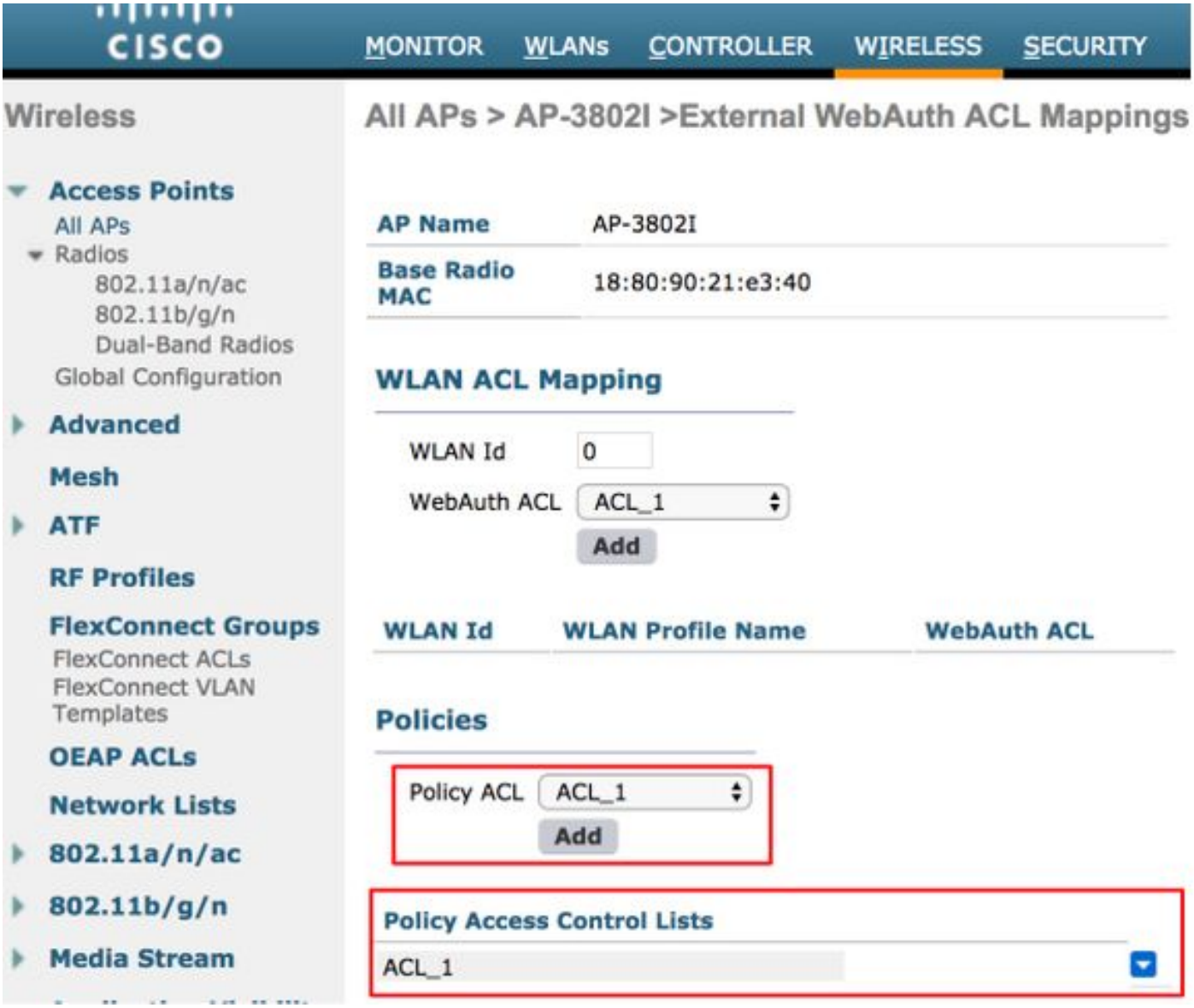
FlexConnect组中的所有AP都会收到配置的ACL。当您导航至**Wireless-Flexconnect Groups > Select the group you want configure > ACL mapping > Policies**，并添加策略ACL的名称时，可以进行配置，如图所示：



2. AP特定

完成配置的AP接收ACL，其他AP不受影响。当您导航至Wireless > All APs > AP name >时，可以配置此配置

Flexconnect选项卡>外部Web身份验证ACL >策略，如图所示。



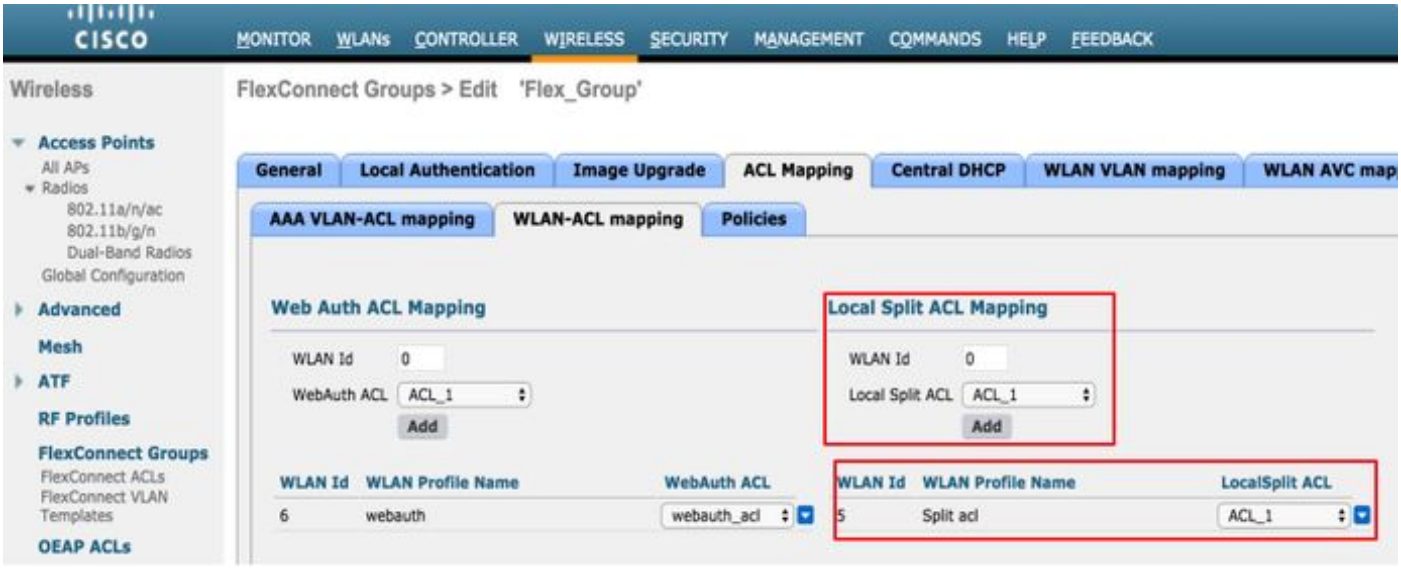
成功进行L2身份验证后，当RADIUS服务器在redirect-acl AV对中发送ACL名称时，该名称将直接应用于AP上的客户端。当客户端进入**RUN**状态时，所有客户端流量都在本地交换，AP停止应用ACL。

在AP上可以配置最多或32个WebPolicy ACL。16个AP特定和16个FlexConnect组特定。

4.拆分隧道ACL

当某些客户端流量需要在本地发送时，拆分隧道ACL与集中交换SSID一起使用。分割隧道功能也是Office扩展接入点(OEAP)设置的一个额外优势，在此设置中，企业SSID上的客户端可以直接与本地网络上的设备（打印机、远程LAN端口上的有线计算机或个人SSID上的无线设备）通信，一旦将其作为分割隧道ACL的一部分。

可以根据flexconnect组级别在上配置分割隧道ACL，导航至**Wireless-Flexconnect Groups > Select the group you want configure > ACL mapping > WLAN-ACL mapping > Local Split ACL Mapping**，如图所示。



也可以根据AP级别配置这些ACL，导航至**Wireless > All AP's > AP name > Flexconnect选项卡> Local Split ACLs**，然后添加Flexconnect ACL的名称，如图所示。

分割隧道ACL无法在本地桥接组播/广播流量。即使组播/广播流量与FlexConnect ACL匹配，也会集中交换。

故障排除

目前没有针对此配置的故障排除信息。