配置在WLC的Flexconnect ACL

目录

简介

本文描述多种flexconnect访问控制表(ACL)类型，并且他们如何在接入点(AP)可以配置和验证。

先决条件

要求

Cisco 建议您了解以下主题：

- Cisco无线LAN控制器(WLC)该运行编码8.3和更加高
- 在WLC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。
- 在flexconnect模式运行的3802和3702 AP的。

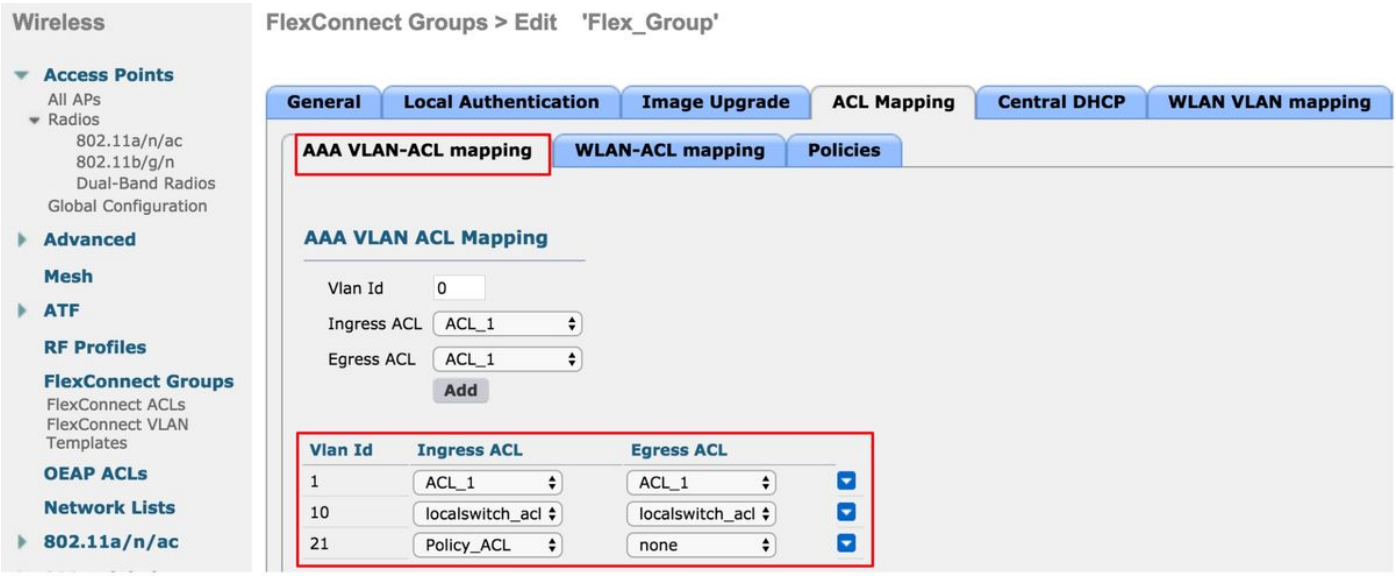
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

ACL类型

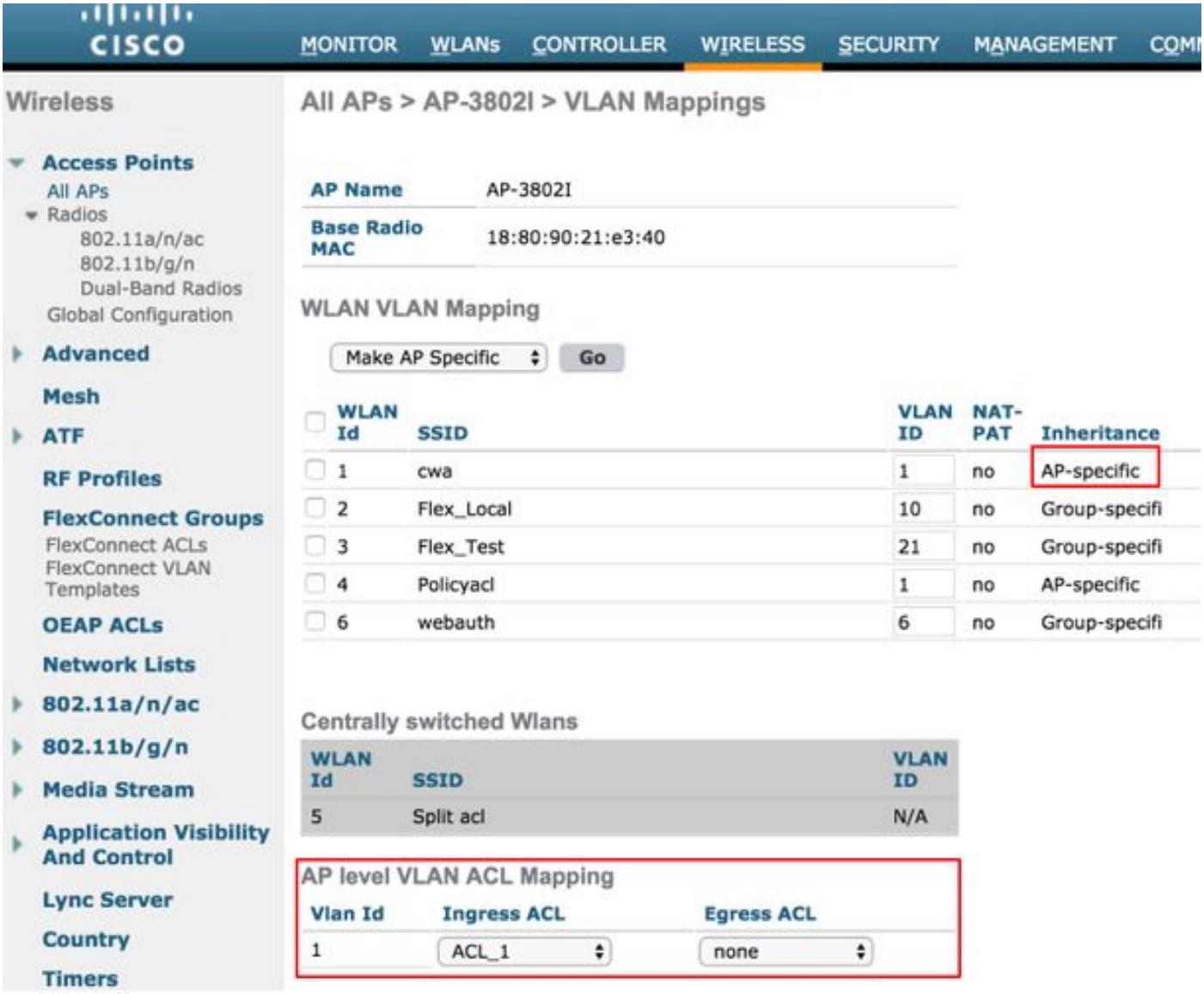
1. VLAN ACL

VLAN ACL是最常用的ACL，并且让发送进出VLAN的您控制客户端的流量。

ACL可以根据在**无线Flexconnect映射>AAA VLAN-ACL映射的Groups>** ACL使用AAA VLAN-ACL映射部分如镜像所显示的flexconnect组配置。



它能根据AP级别配置，也导航到**无线>所有AP > AP名称> Flexconnect选项卡**和单击**VLAN映射**部分。这里，您需要首先做VLAN设置AP特定，如镜像所显示，在后您能指定AP级别VLAN-ACL映射。



ACL方向

您能也指定ACL得到应用的方向：

- 入口(入口含义往无线客户端)
- 出口(往theDS或LAN)，
- 两或无。

因此，如果希望阻塞流量被注定往无线客户端您能然后使用入口方向，并且，如果希望阻塞无线客户端发出的流量，您能使用输出方向。

选项，当您希望推送与使用的分开的ACL验证、授权和统计(AAA)覆盖，无使用。在这种情况下，RADIUS服务器发送的ACL动态地应用给客户端。

Note:ACL需要予先配置在Flexconnect ACL下，否则不得到应用。

映射考虑事项的ACL

当您使用VLAN ACL时，了解这些考虑事项关于在flexconnect AP的VLAN映射也是重要的：

- 如果VLAN配置与使用FlexConnect组，在FlexConnect组配置的对应的ACL应用。
- 如果VLAN配置在两个FlexConnect组并且在AP (作为AP特定配置)，则AP ACL配置获得优先权。
- 如果AP特定ACL配置对无，则ACL没有应用。
- 如果从AAA返回的VLAN不是存在AP，客户端跌倒回到为无线局域网(WLAN)配置的默认VLAN，并且所有ACL被映射对该默认VLAN获得优先权。

如果ACL在AP，应用请验证

使用本部分可确认配置能否正常运行。

1. 波形2 AP

在波形2 AP，如果ACL实际上获得推送对与show命令**flexconnect VLAN ACL的**AP您能验证。这里，您能为每个ACL也看到编号合格和丢弃的数据包。

```
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

在AP级别，如果ACL配置推送对与两种方式的AP您能验证：

- 请使用显示的**show access-lists命令，**如果所有VLAN ACL在AP配置：

```
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
```

您能也监控在每个ACL发生的活动，检查该ACL详细的输出并且为每条线路看到命中数计数：

```
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)
```

- 因为VLAN ACL在千兆接口应用，您能验证，如果ACL正确地应用。检查子接口输出如显示此处：

```
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
```

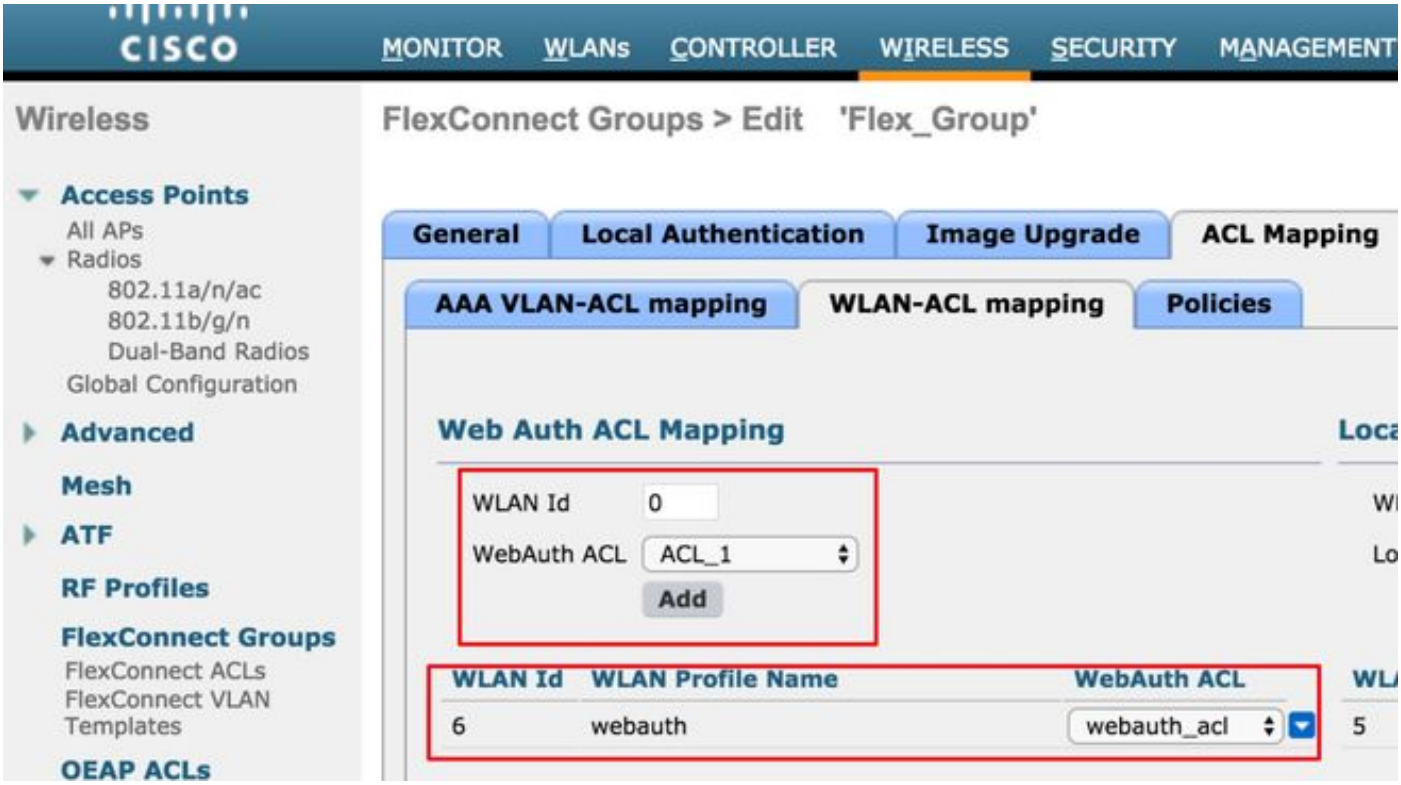
2. Webauth ACL

Webauth ACL使用一旦为flexconnect本地交换启用的Webauth/Webpassthrough服务集标识(SSID)。这使用作为预验证ACL并且允许客户端的流量到重定向服务器。一旦重定向完成，并且客户端是在运转状态， ACL停下来采取它到效果。

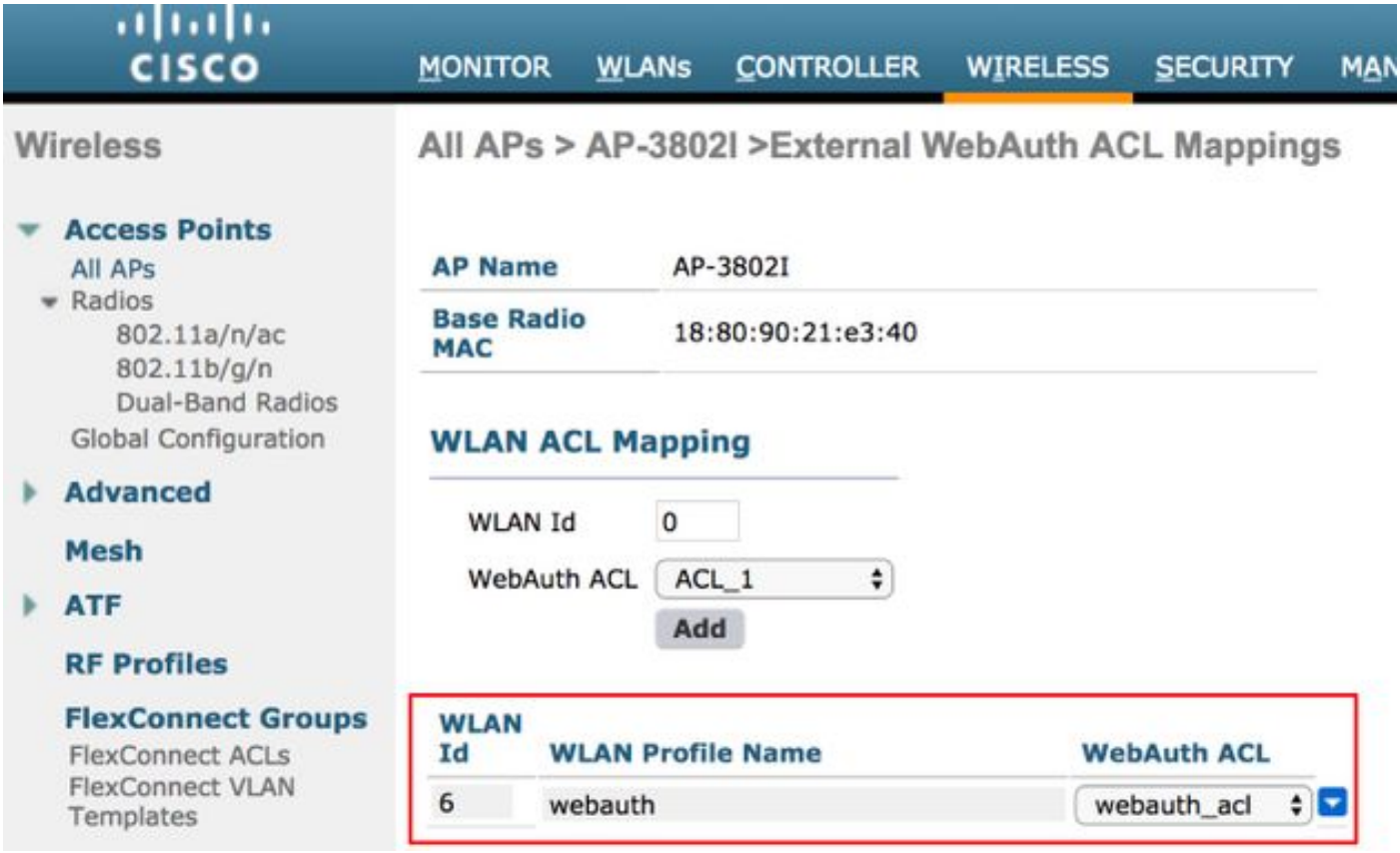
Webauth ACL可以应用二者之一在级的WLAN， AP级别或者flexconnect社团级别。AP特定ACL有最高优先级，而WLAN ACL有最低。如果全部三应用， AP特定获得弹性ACL然后WLAN全局特定跟随的优先权ACL。

可以有在AP配置的最多16个Web-auth ACL。

它可以应用在flexconnect社团级别，导航对**无线> Flexconnect Groups>选择您希望配置> ACL映射> WLAN-ACL映射> Web验证ACL映射**如镜像所显示的**组**。



如镜像所显示， ACL可以应用在AP级别，导航对**无线>All AP的>AP名称>Flexconnect选项卡>外部WebAuthentication ACL > WLAN ACL。**



如镜像所显示， ACL可以应用在级的WLAN，导航对**WLAN > WLAN_ID >第3层> Webauth FlexAcl。**

在Cisco IOS AP，如果ACL应用给客户端，您能验证。请检查**show controllers dot11radio 0客户端**输出(或1，如果客户端连接到A无线电)如显示此处：

```
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
```

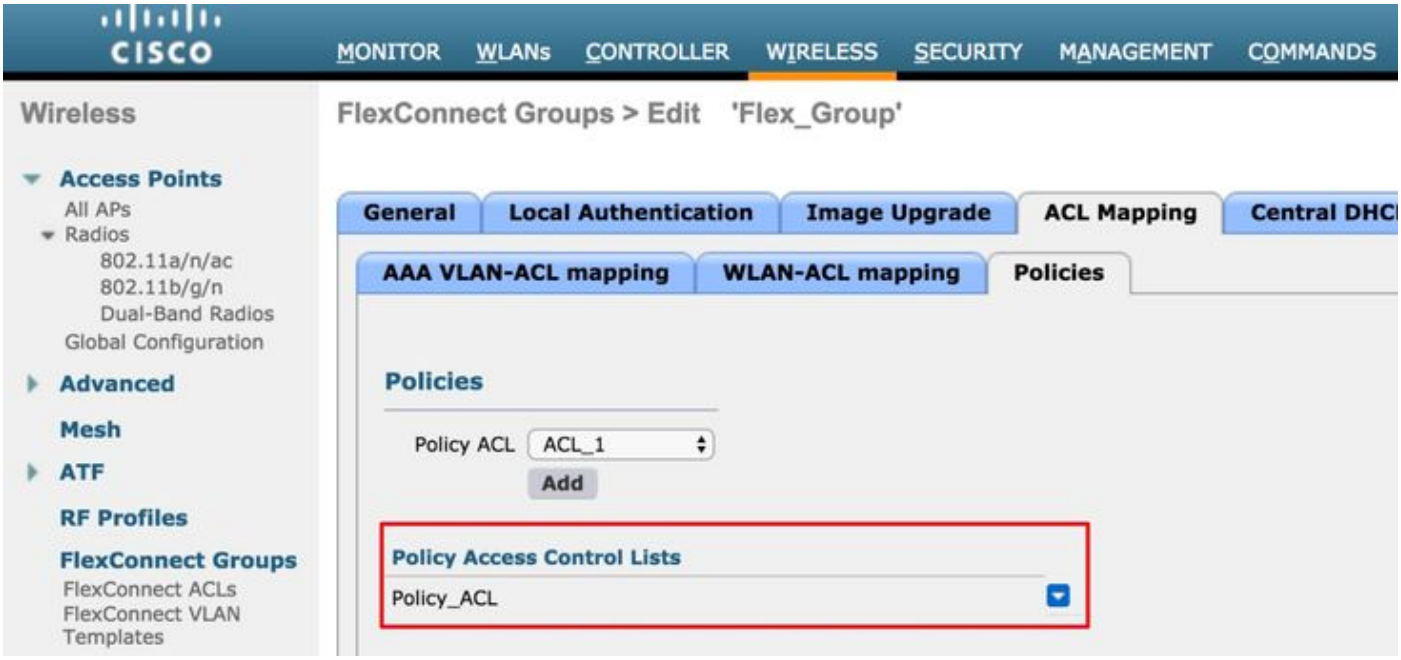
3. Web策略ACL

WebPolicy ACL使用有条件的Web重定向、飞溅页Web重定向和中央印制厂Webauth方案。

有配置联机两个模式WebPolicy WLAN的与弹性ACL ：

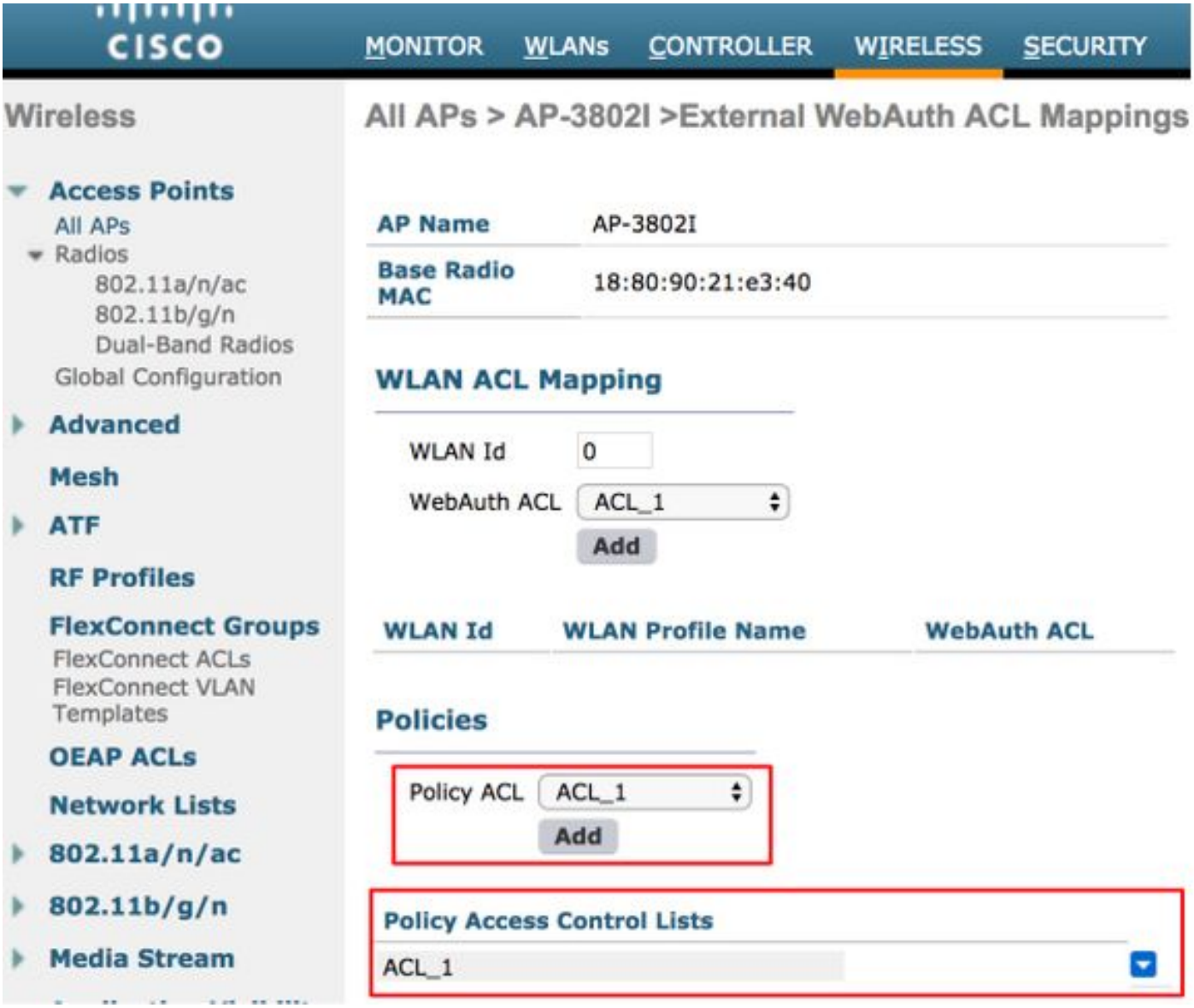
1. Flexconnect组

在配置的FlexConnect组接收的所有AP ACL。如镜像所显示，这可以配置作为您导航对**无线Flexconnect Groups>选择您希望配置> ACL映射>策略的组**，并且添加策略ACL的名称：



2. AP特定

配置是完成的AP接收ACL，没有其他AP被影响。这可以配置作为您导航到**无线>所有AP > AP名称> Flexconnect选项卡>外部WebAuthentication**如镜像所显示的**ACL >策略**。



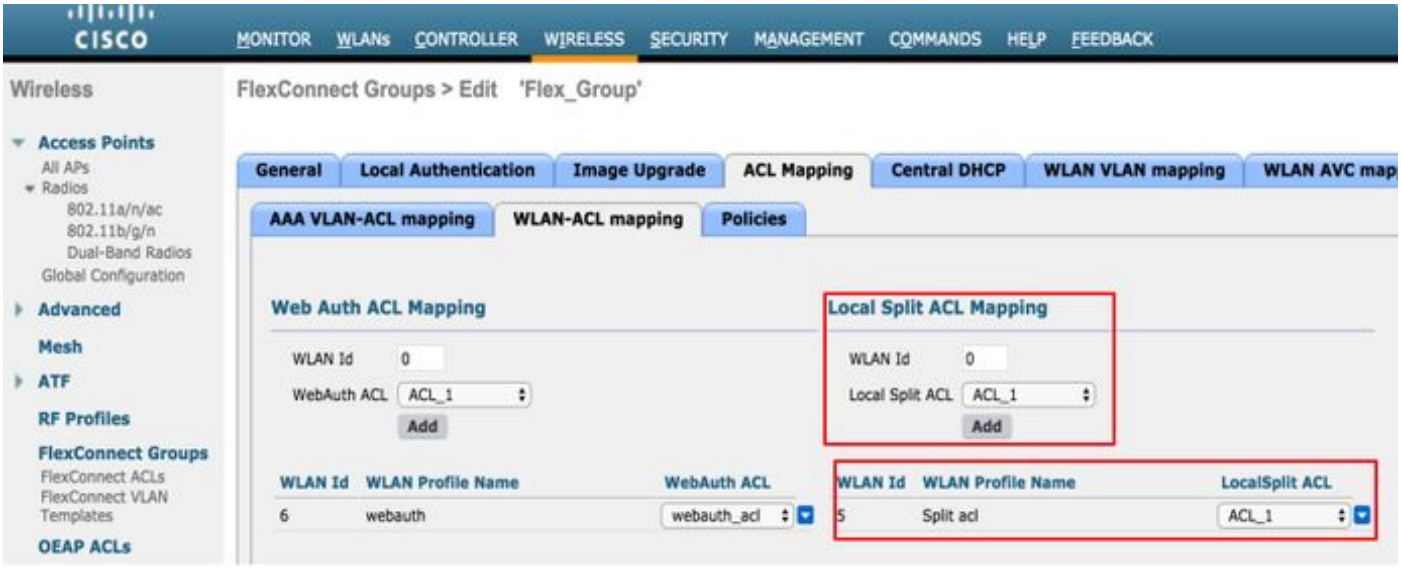
在一成功的L2验证以后，当RADIUS服务器发送在重定向ACL AV对时的ACL名称，这直接地为AP的客户端得到应用。当客户端搬入运转状态时，所有客户端的流量交换本地，并且AP停下来应用ACL。

可以有在AP或32个WebPolicy ACL配置的最大数量。16 AP特定和16基团特殊性的FlexConnect。

4. 分割隧道ACL

当某些客户端的流量需要发送本地时，分割隧道ACL与在中央交换的Ssid的一起使用。分割隧道功能也是办公室(OEAP)一个已添加优点设置的延伸接入点的一公司SSID的客户端能与在本地网络(打印机、有线的计算机在远程LAN波尔特或者无线设备的设备直接地谈在一个人SSID)的地方作为分割隧道ACL一部分，一旦他们被提及。

分割隧道ACL可以根据flexconnect社团级别配置，导航对**无线Flexconnect Groups>选择您希望配置> ACL映射> WLAN-ACL映射>本地已分解ACL映射**如镜像所显示的**组**。



如镜像所显示，他们能配置在根据AP级别，也导航到**无线>所有AP > AP名称> Flexconnect选项卡>本地已分解ACL**和添加flexconnect ACL的名称。

分割隧道ACL不能本地桥接组播/广播数据流。组播/广播数据流在中央交换，即使匹配FlexConnect ACL。

故障排除

目前没有针对此配置的故障排除信息。