Настройте ACL Flexconnect на WLC

Содержание

Введение

Этот документ описывает различные flexconnect типы Списка контроля доступа (ACL) и как они могут быть настроены и проверены на Точке доступа (AP).

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Контроллер беспроводной локальной сети Cisco (WLC), который выполняет код 8.3 и выше
- Конфигурация Flexconnect на WLC

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- WLC Серии Cisco 8540, который выполняет выпуск ПО 8.3.133.0.
- 3802 и 3702 AP, которые выполняются в flexconnect режиме.

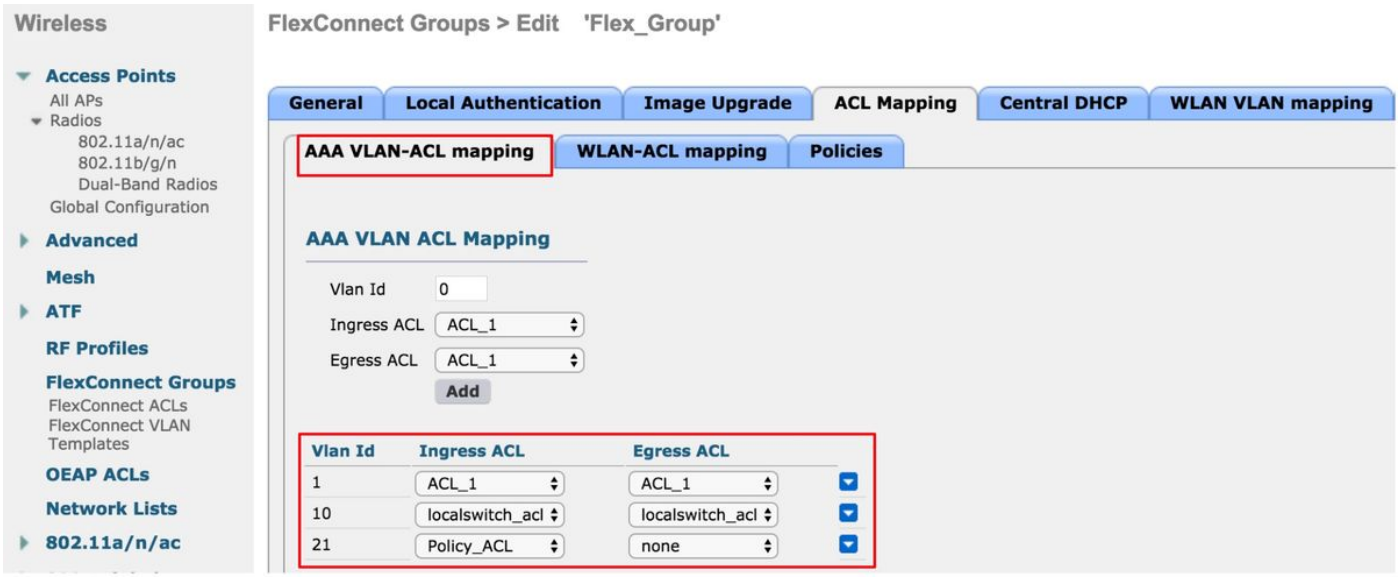
Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Типы ACL

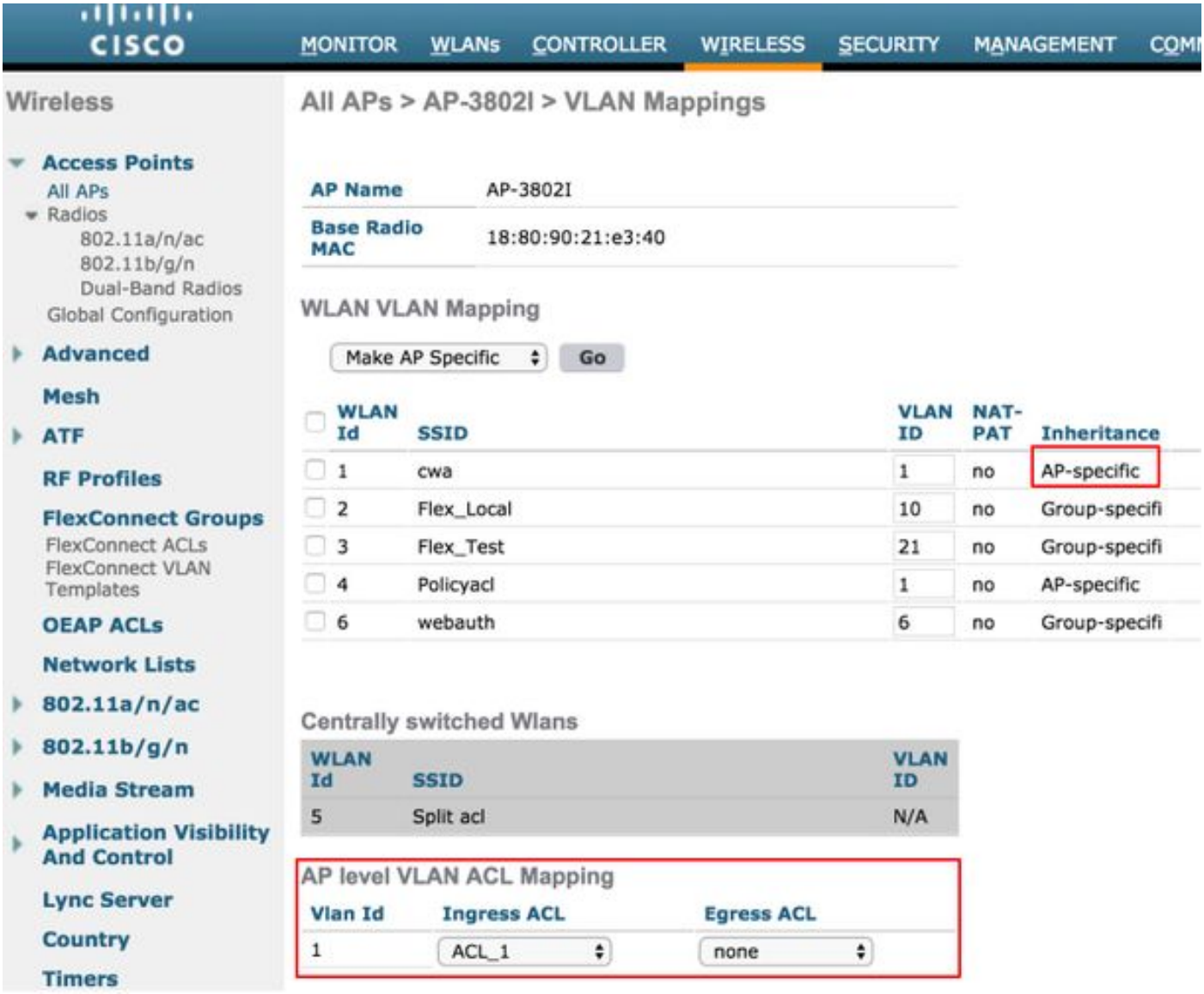
1. ACL VLAN

ACL VLAN является обычно используемым ACL, и это позволяет вам управлять трафиком клиента, который представлен и из VLAN.

ACL может быть настроен согласно flexconnect группе, которая использует раздел сопоставления **ACL VLAN AAA** в **Wireless-Flexconnect Groups> сопоставление ACL> ACL VLAN AAA, сопоставляющий** как показано в образе.



Это может также быть настроено согласно уровню AP, перейти к **беспроводным сетям> Весь AP> вкладка Flexconnect name> AP** и нажимать раздел **сопоставлений VLAN**. Здесь, необходимо заставить VLAN сконфигурировать AP, определенный первый, после которого можно задать ACL VLAN уровня AP, сопоставляющий как показано в образе.



Направления ACL

Можно также задать направление, в котором применен ACL:

- Вход (Вход означает к беспроводному клиенту),
- Выход (к theDS или LAN),
- оба или ни один.

Так, если бы требуется заблокировать трафик, предназначенный к беспроводному клиенту тогда, можно использовать направление доступа и если требуется заблокировать трафик, полученный беспроводным клиентом, можно использовать выходное направление.

Опция ни один не используется, когда требуется выдвинуть разделять ACL с использованием замены Аутентификации, авторизации и учета (AAA). В этом случае ACL, передаваемый сервером RADIUS, применен динамично к клиенту.

> **Примечание:** ACL должен быть настроен под ACL Flexconnect заранее, иначе это не становится прикладным.

Факторы сопоставления ACL

При использовании ACL VLAN также важно понять эти факторы относительно сопоставлений VLAN на flexconnect AP:

- Если VLAN настроена с использованием группы FlexConnect, соответствующий ACL, настроенный на группе FlexConnect, применен.
- Если VLAN настроена и на группе FlexConnect и на также на AP (как AP определенная конфигурация), то конфигурация списков управления доступом (ACL) AP имеет приоритет.
- Если AP, определенный ACL не настроен ни к одному, то никакой ACL не применен.
- Если VLAN, которая была возвращена из AAA, не присутствует на AP, клиент переключается на виртуальную локальную сеть (VLAN) по умолчанию, настроенную для Беспроводной локальной сети (WLAN), и любой ACL, сопоставленный с той виртуальной локальной сетью (VLAN) по умолчанию, имеет приоритет.

Проверьте, применен ли ACL на AP

Воспользуйтесь данным разделом для проверки правильности функционирования вашей конфигурации.

1. Волна 2 AP

На волне 2 AP можно проверить, выдвинут ли ACL фактически к AP с **командой show flexconnect acl vlan**. Здесь, можно также видеть количество переданных и отброшенных пакетов для каждого 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's

Если конфигурация списков управления доступом (ACL) была выдвинута к AP с двумя путями, на уровне AP можно проверить:

- Используйте **команду show access-lists**, которая показывает, настроен ли весь ACL VLAN на 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
```

Можно также контролировать действие, которое происходит на каждом ACL, проверьте подробные выходные данные того ACL и посмотрите, что соответствие значит каждую линию:

```
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)
```

- Начиная с ACL VLAN применены на гигабитный интерфейс, можно проверить, если ACL применен правильно. Проверьте sub выходную очередь удержания интерфейса как показано здесь:

```
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
```

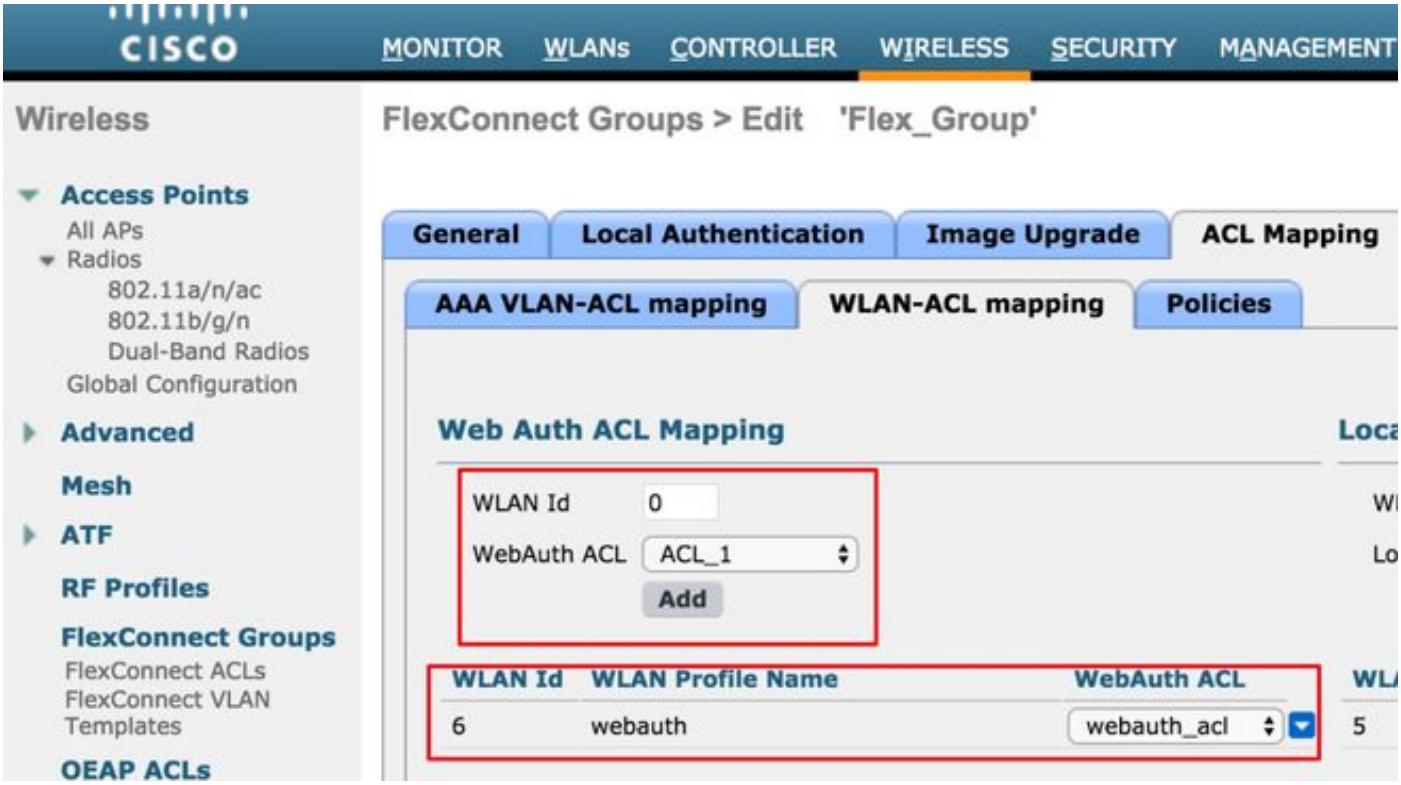
2. ACL Webauth

ACL Webauth используется в случае идентификаторов наборов сервисов (SSID) Webauth/Webpassthrough, которые были включены для flexconnect локального коммутатора. Это используется в качестве ACL процедур, предшествующих аутентификации и позволяет трафик клиента переадресации сервера. Как только перенаправление завершено, и клиент находится в **ВЫПОЛНЕННОМ** состоянии, ACL останавливается для взятия его в эффект.

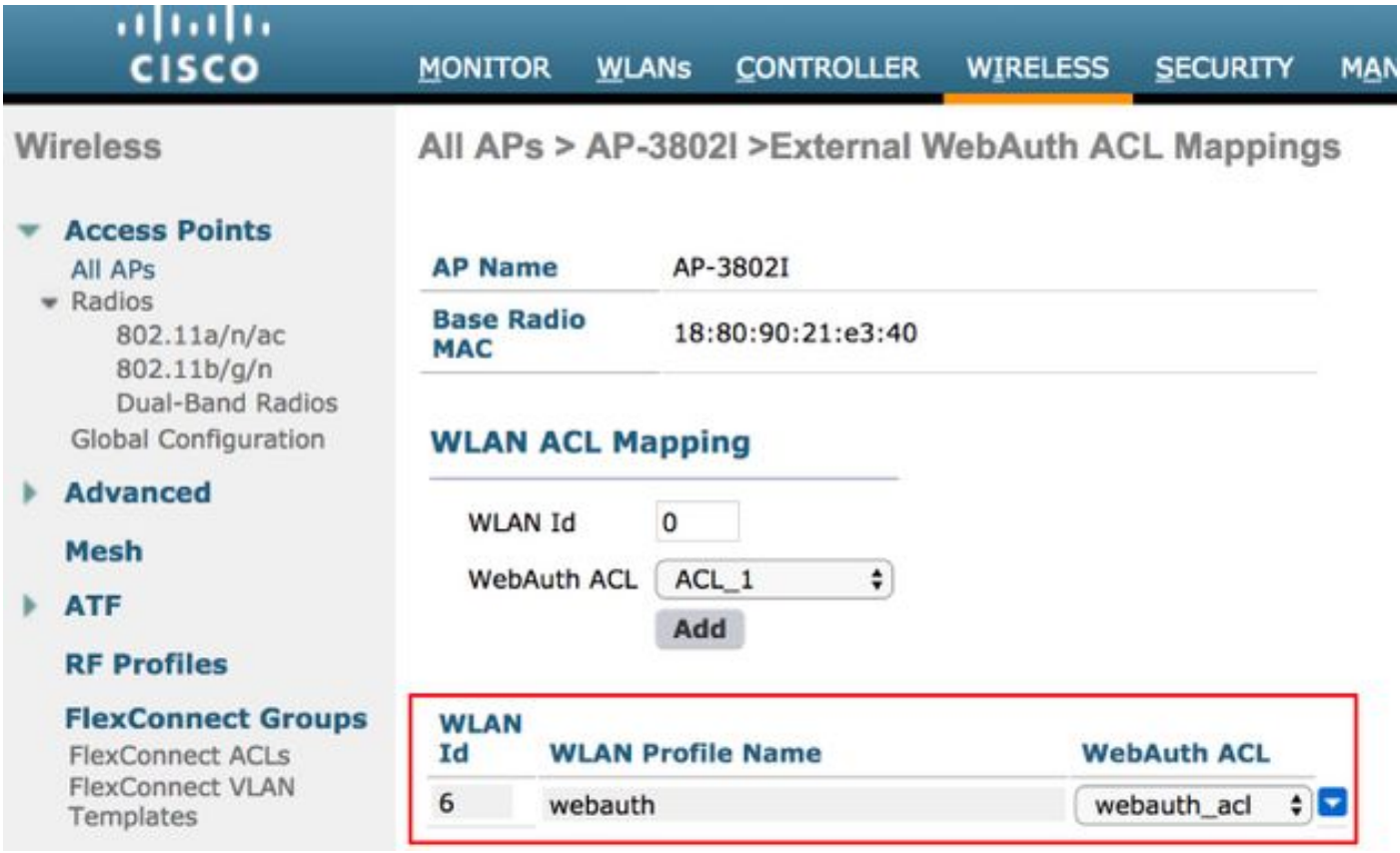
ACL Webauth может быть применен или на уровне WLAN, уровне AP или на flexconnect уровне группы. Определенный ACL AP имеет наивысший приоритет, тогда как ACL WLAN имеет самое низкое. Если все три применены, Определенный AP имеет приоритет придерживавшийся ACL Flex и затем Глобальным WLAN Определенный ACL.

Может быть максимум 16 Веб-Подлинных ACL, настроенных на AP.

Это может быть применено на flexconnect уровне группы, перейти к **беспроводным сетям>, Flexconnect Groups> Выбирает группу, которую вы хотите, настраивают> сопоставление ACL> сопоставление ACL WLAN> веб-Подлинный ACL, Сопоставляющий** как показано в образе.



ACL может быть применен на уровне AP, перейти к **беспроводным сетям> Весь AP> вкладка Flexconnect name> AP> Внешние ACL WebAuthentication> ACL WLAN** как показано в образе.



ACL может быть применен на уровне WLAN, перейти к **WLAN> WLAN_ID> Уровень 3> WebAuth FlexAcl** как показано в образе.

На Cisco IOS® AP можно проверить, был ли ACL применен к клиенту. Проверьте выходные данные **клиента show controllers dot11radio 0** (или 1, если клиент соединяется с радио), как показано здесь:

```
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
```

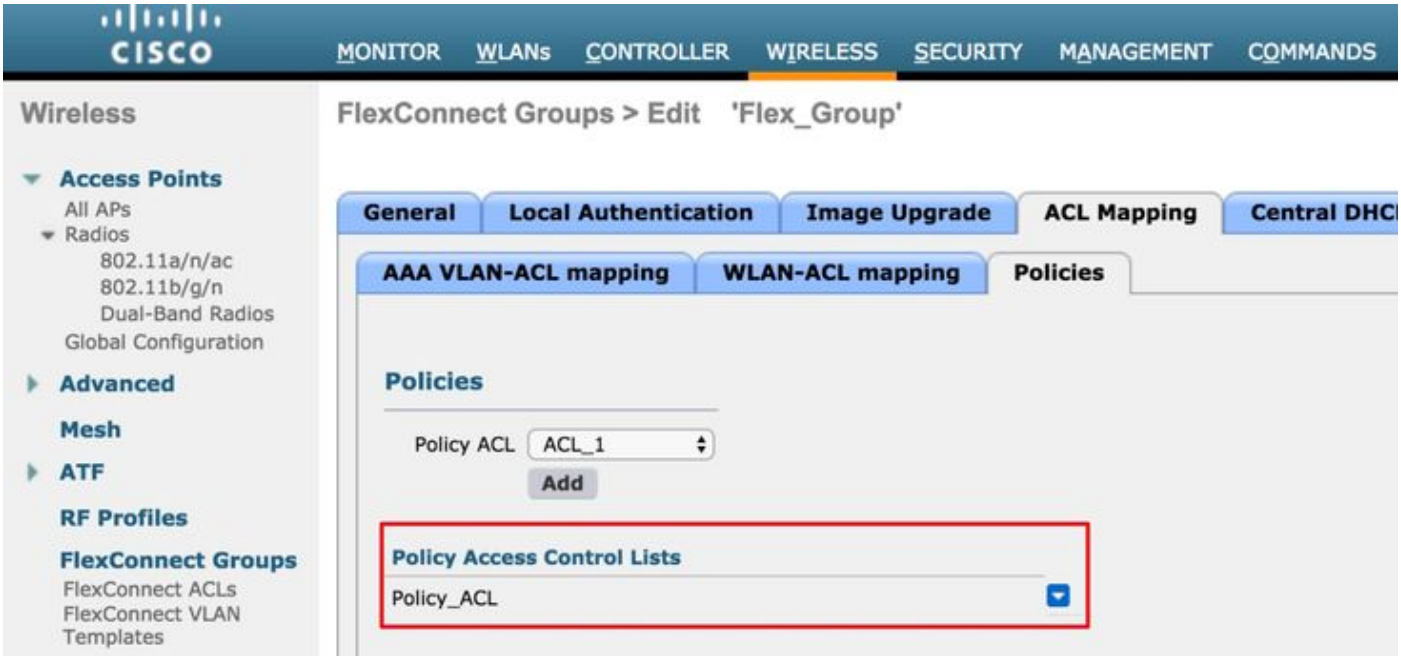
3. Веб-ACL политики

WebPolicy ACL используется для Условного веб-Перенаправления, веб-Перенаправления Страницы-заставки и Центральных сценариев Webauth.

Существует два режима конфигурации, доступной для WLAN WebPolicy с ACL Flex:

1. Flexconnect Group

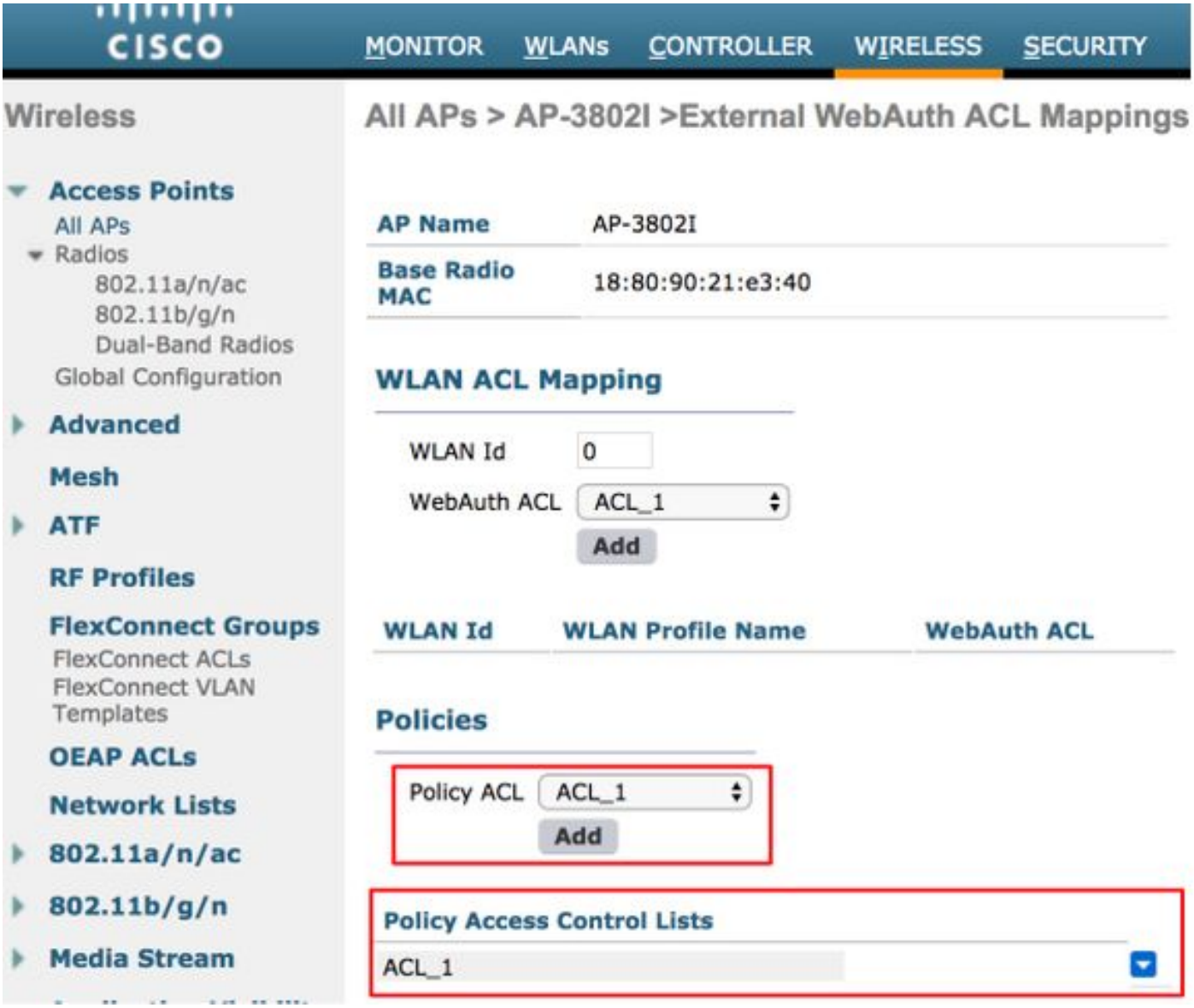
Все AP в group receive FlexConnect ACL, который настроен. Это может быть настроено, поскольку вы перешли к **Wireless-Flexconnect Groups>, Выбирают группу, которую вы хотите, настраивают> сопоставление ACL> Политика** и добавляют название ACL Политики как показано в образе:



2. Определенный AP

AP, для которого реализована конфигурация, получает ACL, ни на какие другие AP не влияют. Это может быть настроено, поскольку вы перешли к **беспроводным сетям> Все AP> name> AP**

Вкладка Flexconnect> Внешние ACL WebAuthentication> Политика как показано в образе.



После успешной аутентификации L2, когда сервер RADIUS передает название ACL в паре значение-атрибут acl перенаправления, это применено непосредственно для клиента на AP. Когда клиентские шаги в **ВЫПОЛНЕННОЕ** состояние, весь трафик клиента коммутирован локально, и AP останавливается для применения ACL.

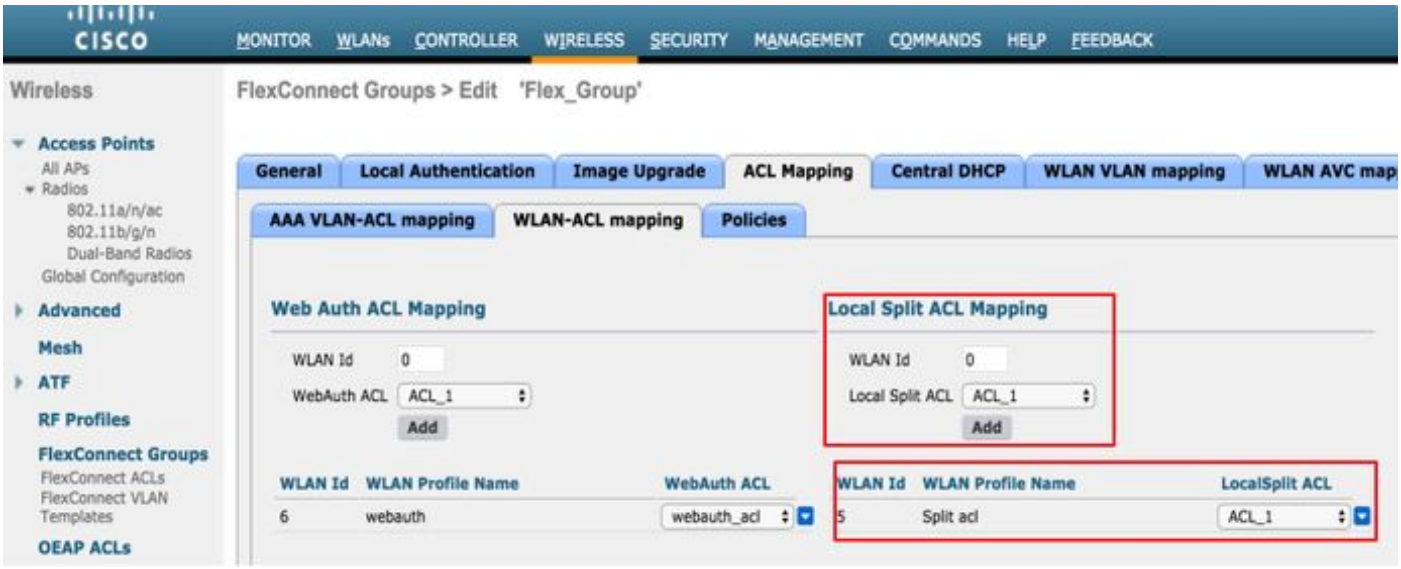
Может быть максимум или 32 ACL WebPolicy, настроенные на AP. 16 определенных AP и 16 определенных групп FlexConnect.

4. ACL разделения туннеля

Когда часть трафика клиента должна быть передана локально, ACL Разделенного туннелирования используется с централизованно коммутируемым SSID. Функциональность Разделенного туннелирования является также добавленным преимуществом для настройки Офиса расширяет точку доступа (OEAP), где клиенты на Корпоративном SSID могут говорить с устройствами на локальной сети (принтеры, соединенная проводом машина на Удаленном Порте LAN (локальной сети) или беспроводные устройства на Персональном SSID) непосредственно, как только они упомянуты как часть ACL разделения туннеля.

ACL Разделенного туннелирования может быть настроен на согласно flexconnect уровню группы, перейти к **Wireless-Flexconnect Groups>, Выбирают группу, которую вы хотите, настраивают> сопоставление ACL> сопоставление ACL WLAN> Локальный Раздельный**

ACL, Сопоставляющий как показано в образе.



Они могут также быть настроены в согласно уровню AP, перейти к **беспроводным сетям> Весь AP> вкладка Flexconnect name> AP> Локальные Раздельные ACL** и добавлять название flexconnect ACL как показано в образе.

ACL Разделенного туннелирования не может локально соединить Групповую адресацию/Широковещательный трафик. Групповая адресация/Широковещательный трафик коммутирована централизованно, даже если она совпадает с FlexConnect ACL.

Устранение неполадок

Для этой конфигурации в настоящее время нет сведений об устранении проблем.