WLCでのFlexconnect ACLの設定

内容

概要

このドキュメントでは、さまざまなFlexconnectアクセスコントロールリスト(ACL)タイプについて説明し、アクセスポイント(AP)で設定および検証する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- コード8.3以降を実行するCisco Wireless LAN Controller(WLC)
- WLCでのFlexconnectの設定

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- ソフトウェア リリース 8.3.133.0 を実行する Cisco 8540 シリーズ WLC.
- Flexconnectモードで動作する3802および3702 AP。

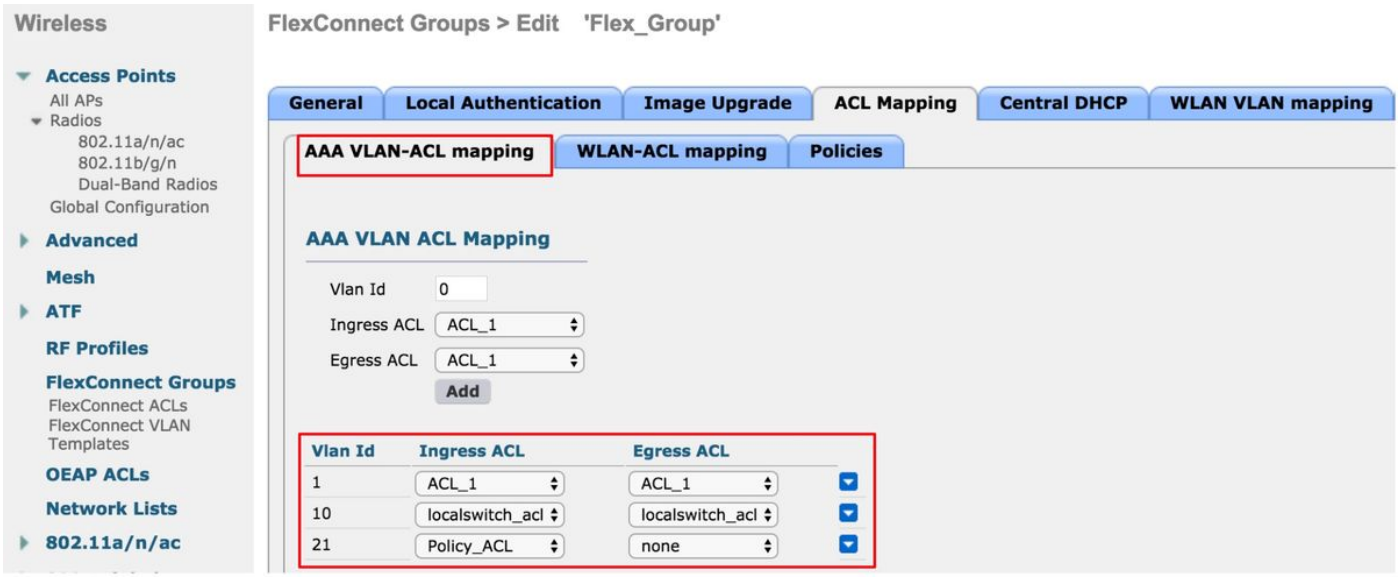
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

ACLタイプ

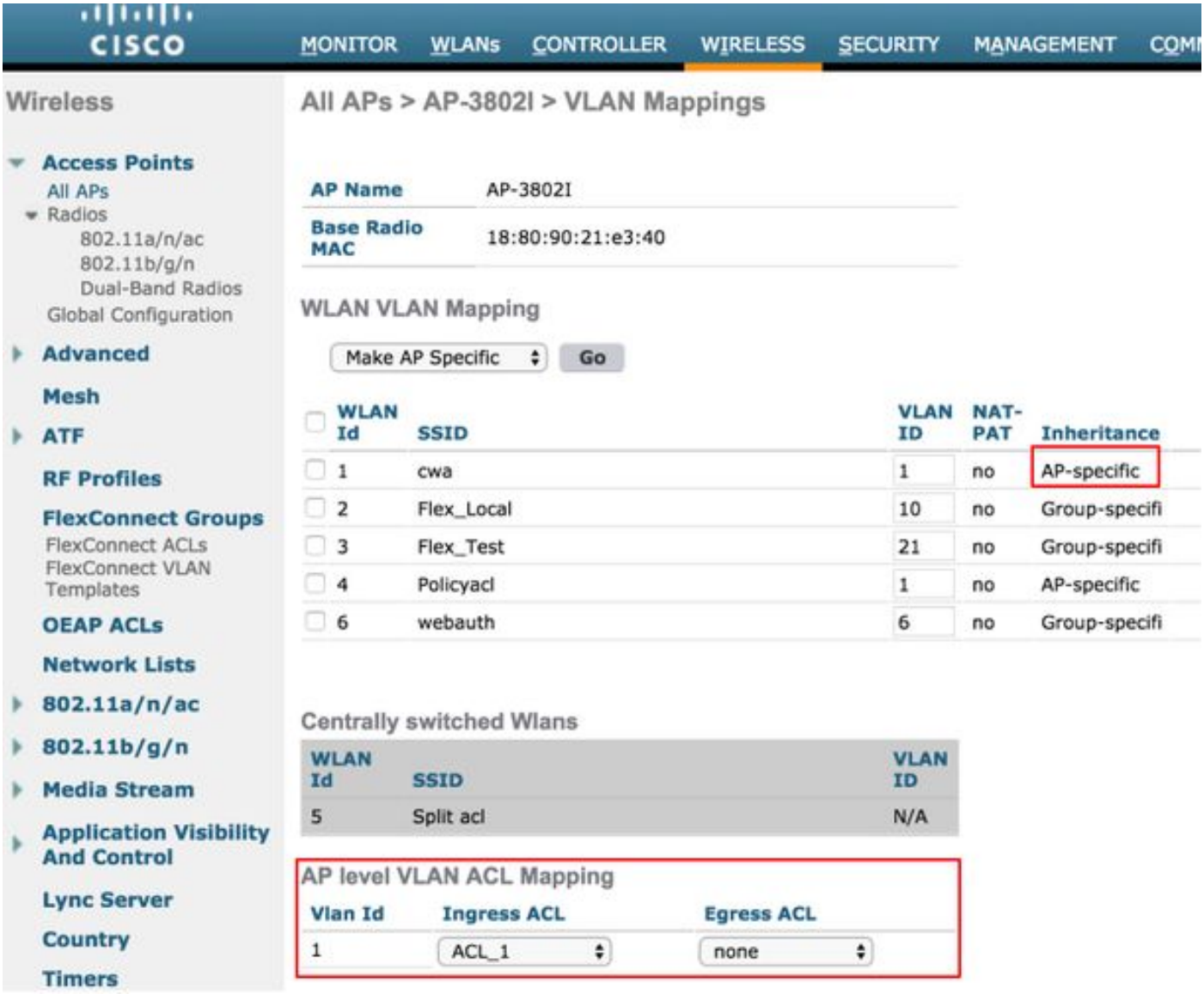
1. VLAN ACL

VLAN ACLは最も一般的に使用されるACLで、VLANに出入りするクライアントトラフィックを制御できます。

ACLは、図に示すように、[Wireless-Flexconnect Groups] > [ACL mapping] > [AAA VLAN-ACL mapping]の[AAA VLAN-ACL mapping]セクションを使用するflexconnectグループごとに設定できます。



APレベルに応じて設定することもできます。[Wireless] > [All AP's] > [AP name] > [Flexconnect]タブに移動し、[VLAN mappings]セクションをクリックします。ここで、最初にVLAN設定APを特定する必要があります。その後、図に示すように、APレベルのVLAN-ACLマッピングを指定できます。



ACLの方向

ACLを適用する方向を指定することもできます。

- 入力（入力はワイヤレスクライアントに対する意味）
- 出力（DSまたはLANに対して）、
- 両方またはなし

そのため、ワイヤレスクライアント宛てのトラフィックをブロックする場合は入力方向を使用でき、ワイヤレスクライアントから送信されたトラフィックをブロックする場合は出力方向を使用できます。

オプションnoneは、認証、許可、アカウンティング(AAA)オーバーライドを使用して別のACLをプッシュする場合に使用します。この場合、radiusサーバから送信されたACLはクライアントに動的に適用されます。

> **注**：ACLはFlexconnect ACLの下で事前に設定する必要があります。設定しないと適用されません。

ACLマッピングの考慮事項

VLAN ACLを使用する場合は、flexconnect APのVLANマッピングに関する次の考慮事項を理解することも重要です。

- VLANがFlexConnectグループを使用して設定されている場合、FlexConnectグループに設定されている対応するACLが適用されます。
- VLANがFlexConnectグループとAPの両方に設定されている場合（AP固有の設定として）、AP ACLの設定が優先されます。
- AP固有のACLがnoneに設定されている場合、ACLは適用されません。
- AAAから返されたVLANがAPに存在しない場合、クライアントはワイヤレスLAN(WLAN)に設定されたデフォルトVLANにフォールバックし、そのデフォルトVLANにマッピングされたACLが優先されます。

ACLがAPに適用されているかどうかを確認する

ここでは、設定が正常に機能しているかどうかを確認します。

1.ウェーブ2 AP

Wave 2 APでは、**show flexconnect vlan-acl**コマンドを使用して、ACLが実際にAPにプッシュされたかどうかを確認できます。ここでは、各ACLの通過パケットと廃棄パケットの数も確認できます。

```
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

APレベルでは、ACL設定が次の2つの方法でAPにプッシュされたかどうかを確認できます。

- **show access-lists**コマンドを使用します。このコマンドは、すべてのVLAN ACLがAPに設定されているかどうかを示します。

```
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
```

また、各ACLで発生するアクティビティを監視し、そのACLの詳細出力をチェックして、各行のヒットカウントを確認することもできます。

```
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)
```

- VLAN ACLはギガビットインターフェイスに適用されるため、ACLが正しく適用されているかどうかを確認できます。次に示すように、サブインターフェイスの出力を確認します。

```
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
```

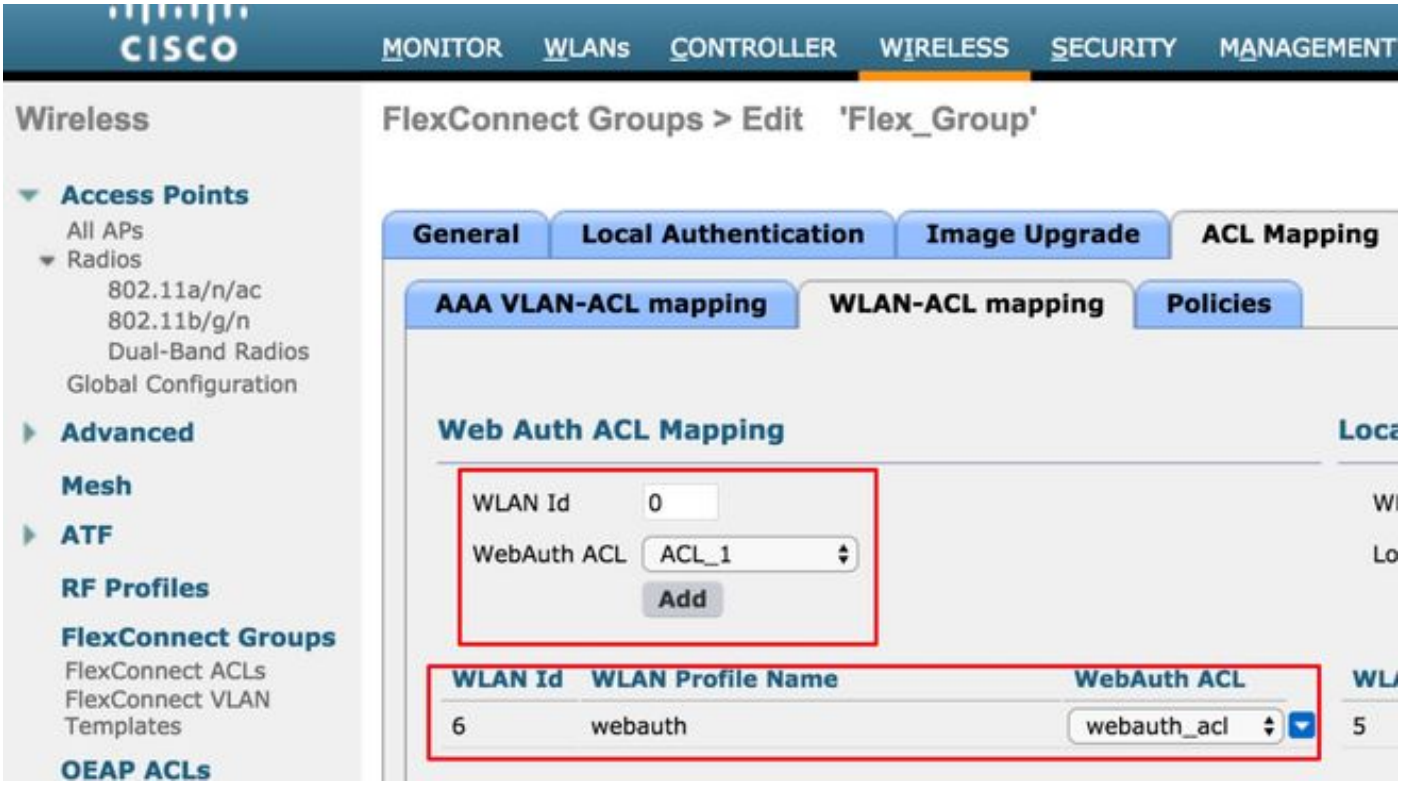
2. Webauth ACL

Webauth ACLは、Flexconnectローカルスイッチングが有効になっているWebauth/Webpassthrough Service Set Identifier(SSID)の場合に使用されます。これは事前認証ACLとして使用され、リダイレクトサーバへのクライアントトラフィックを許可します。リダイレクションが完了し、クライアントが**RUN状態**になると、ACLは停止して有効になります。

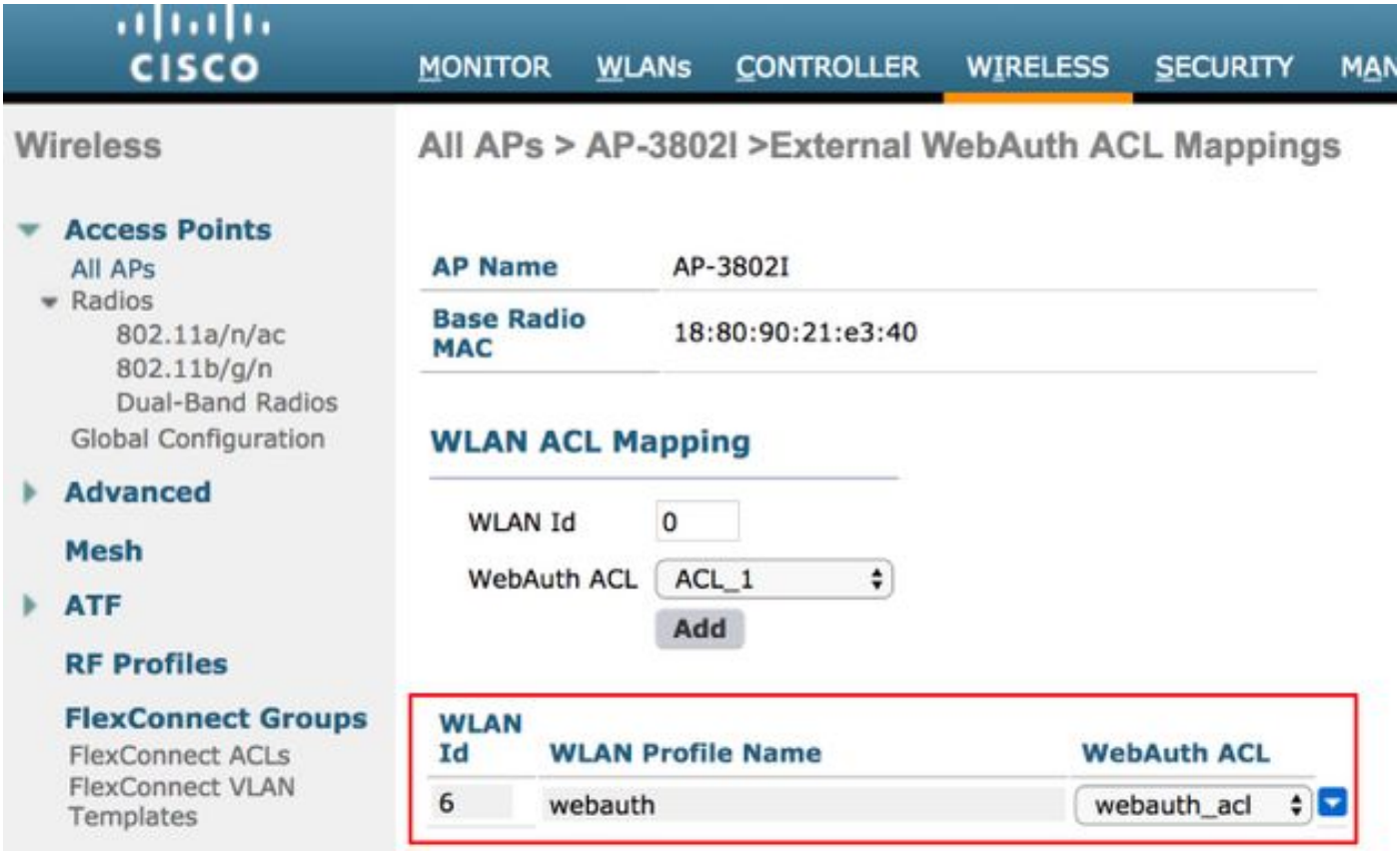
Webauth ACLは、WLANレベル、APレベル、またはflexconnectグループレベルで適用できます。AP固有のACLのプライオリティは最も高く、WLAN ACLのプライオリティは最も低くなります。3つすべてが適用されている場合、AP固有が優先され、その後にFlex ACLが続き、次にWLANグローバル固有ACLが続きます。

1つのAPに最大16のWeb認証ACLを設定できます。

図に示すように、Flexconnectグループレベルで適用でき、**[Wireless] > [Flexconnect Groups] > [Select the group you want configure] > [ACL mapping] > [WLAN-ACL mapping] > [Web Auth ACL Mapping]に移動します。**



ACLはAPレベルで適用できます。図に示すように、[Wireless] > [All AP's] > [AP name] > [Flexconnect]タブ> [External WebAuthentication ACLs] > [WLAN ACL]に移動します。



ACLはWLANレベルで適用できます。図に示すように、[WLAN] > [WLAN_ID] > [Layer 3] > [WebAuth FlexAcl]に移動します。

Cisco IOS® APでは、ACLがクライアントに適用されたかどうかを確認できます。次に示すように、**show controllers dot11radio 0 client**（クライアントがA無線に接続している場合は1）の出力を確認します。

```
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
```

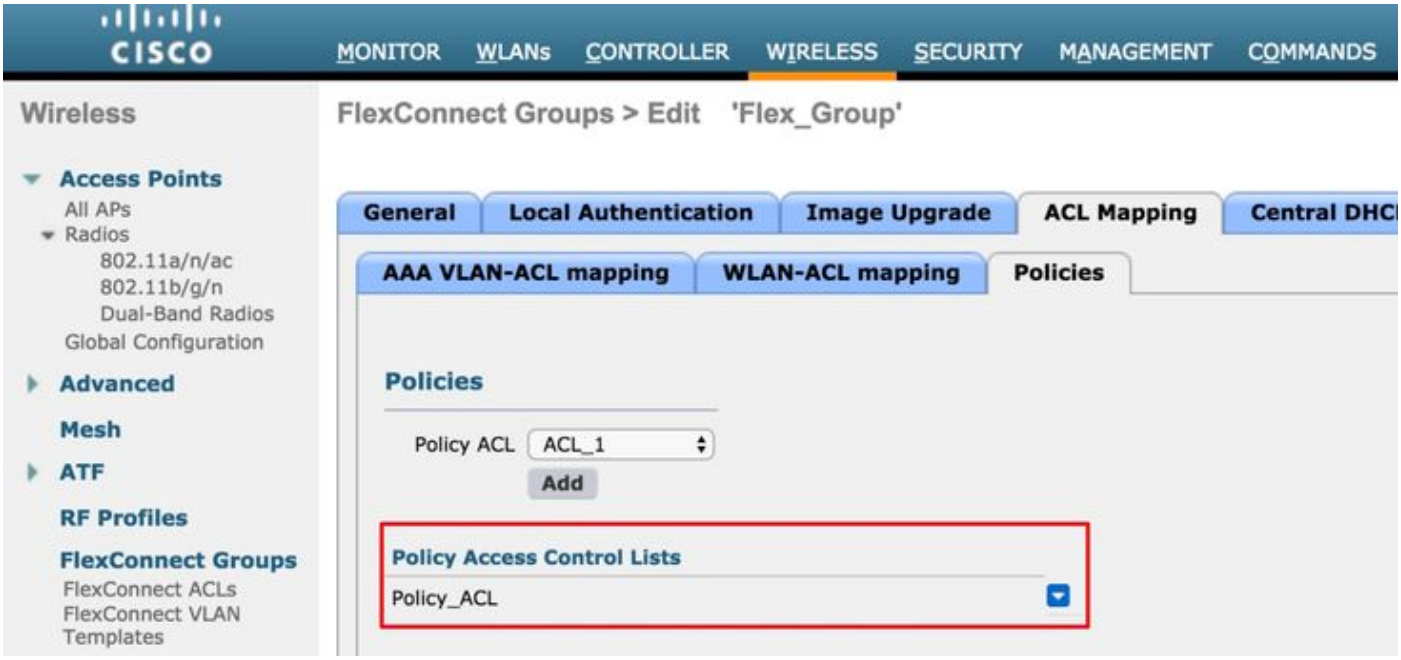
3. WebポリシーACL

WebPolicy ACLは、条件付きWebリダイレクト、スプラッシュページWebリダイレクト、および中央Web認証のシナリオに使用されます。

Flex ACLを使用したWebPolicy WLANでは、次の2つの設定モードを使用できます。

1. Flexconnectグループ

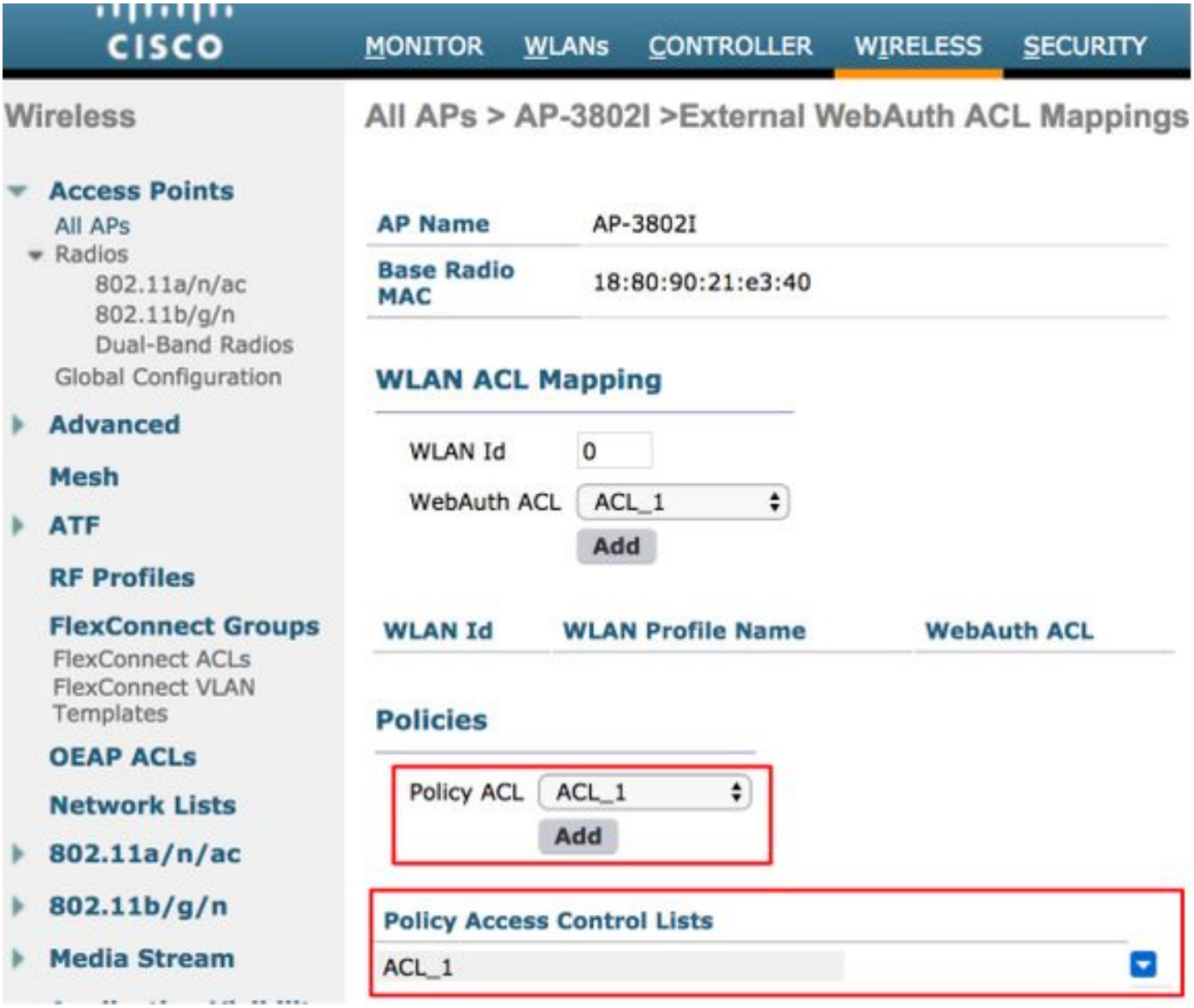
FlexConnectグループ内のすべてのAPは、設定されたACLを受信します。これは、[Wireless-Flexconnect Groups] > [Select the group you want configure] > [ACL mapping] > [Policies]に移動し、図に示すようにポリシーACLの名前を追加するときに設定できます。



2. AP固有

設定を行ったAPはACLを受信しますが、他のAPは影響を受けません。これは、**[Wireless] > [All APs] > [AP name] >**

図に示すように、[Flexconnect]タブ> [External WebAuthentication ACLs] > [Policies]を選択します。



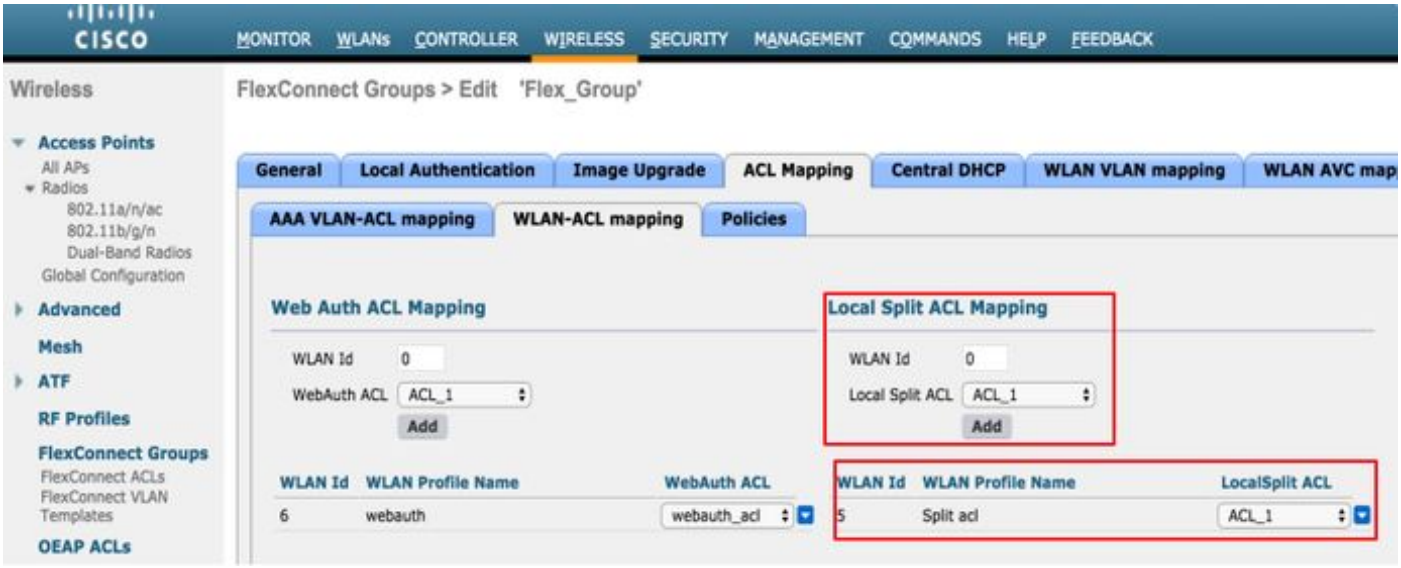
L2認証が成功した後、radiusサーバがredirect-acl AVペアでACL名を送信すると、これはAP上のクライアントに直接適用されます。クライアントが**RUN**状態になると、すべてのクライアントトラフィックがローカルにスイッチングされ、APはACLの適用を停止します。

1つのAPに最大または32個のWebPolicy ACLを設定できます。16個のAP固有および16個のFlexConnectグループ固有です。

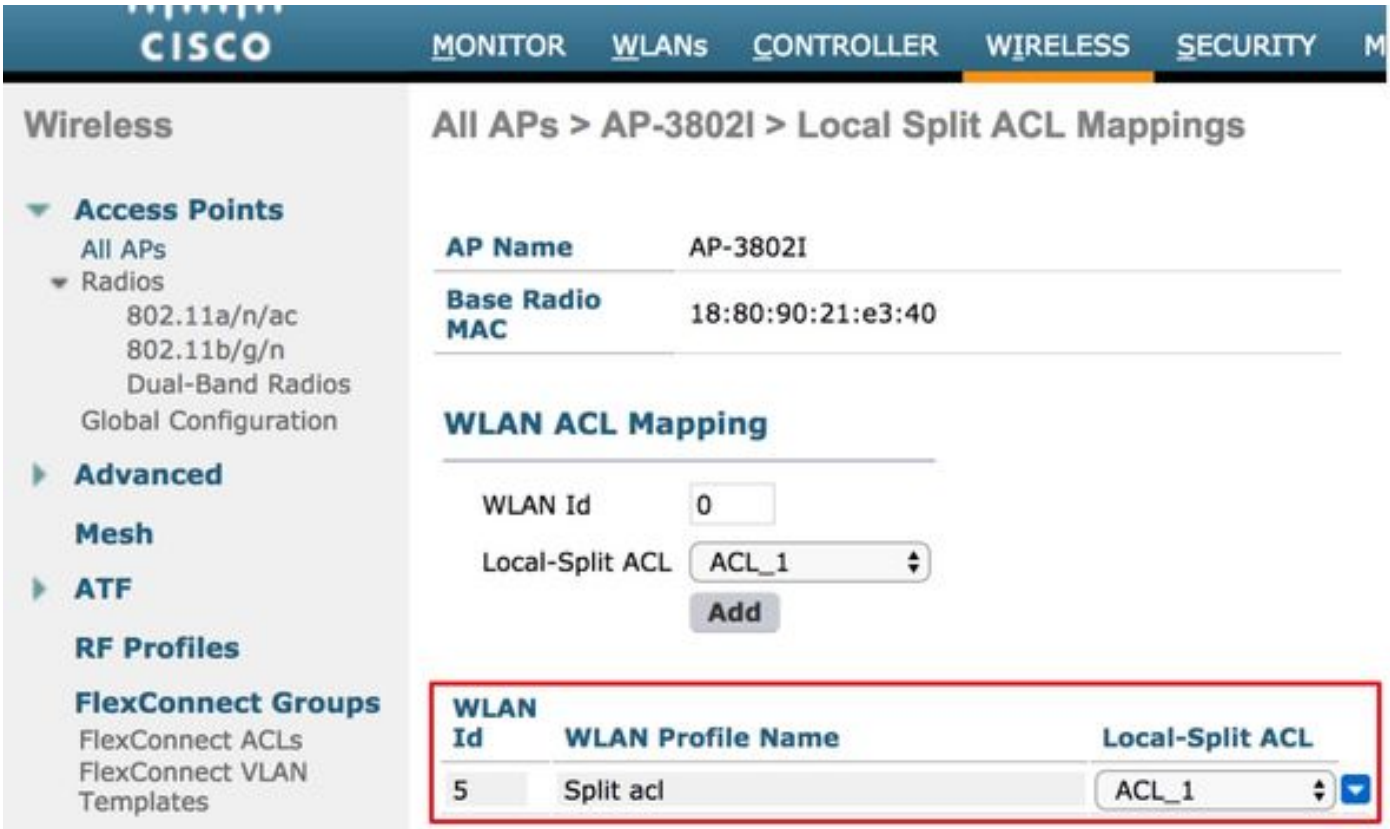
4.スプリットトンネルACL

スプリットトンネリングACLは、クライアントトラフィックの一部をローカルに送信する必要がある場合に、中央でスイッチングされるSSIDとともに使用されます。スプリットトンネリング機能は、スプリットトンネルACLの一部として指定された企業SSID上のクライアント（プリンタ、リモートLANポート上の有線マシン、またはパーソナルSSID上の無線デバイス）がローカルネットワーク上のデバイスと直接通信できるOffice Extend Access Point(OEAP)設定ののの機能です。

スプリットトンネリングACLは、Flexconnectグループレベルに従って設定できます。図に示すように、**Wireless-Flexconnect Groups > Select the group you want configure > ACL mapping > WLAN-ACL mapping > Local Split ACL Mappingに移動します。**



これらはAPレベルで設定することも可能で、**Wireless > All AP's > AP name > Flexconnect tab > Local Split ACLsに移動**して、図に示すようにflexconnect ACLの名前を追加します。



スプリットトンネリングACLでは、マルチキャスト/ブロードキャストトラフィックをローカルでブリッジすることはできません。マルチキャスト/ブロードキャストトラフィックは、FlexConnect ACLと一致する場合でも、中央でスイッチングされます。

トラブルシュート

現在、この設定に関する特定のトラブルシューティング情報はありません。