FlexConnect ローカル スイッチングを使用した外部 Web 認証の導入ガイド

目次

概要

このドキュメントでは、さまざまな Web ポリシーに対して、外部 Web サーバと FlexConnect ローカル スイッチングを使用する方法について説明します。

前提条件

要件

この設定を行う前に、次の要件が満たされていることを確認します。

- FlexConnect アーキテクチャとアクセス ポイント（AP）に関する基本的な知識
- 外部 Web サーバのセットアップ方法および設定方法に関する知識
- DHCP サーバと DNS サーバのセットアップ方法および設定方法に関する知識

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くものです。

- ファームウェア リリース 7.2.110.0 が稼働する Cisco 7500 シリーズ ワイヤレス LAN コントローラ（WLC）
- Cisco 3500 シリーズ Lightweight アクセス ポイント（LAP）
- Web 認証ログイン ページをホストする外部 Web サーバ
- ワイヤレス クライアントに対するアドレス解決と IP アドレス割り当てに使用する、ローカル側の DNS サーバおよび DHCP サーバ

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 この導入ガイドでは 7500 シリーズ WLC が使用されますが、この機能は 2500、5500、WiSM-2 の各 WLC でサポートされています。 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。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

機能の概要

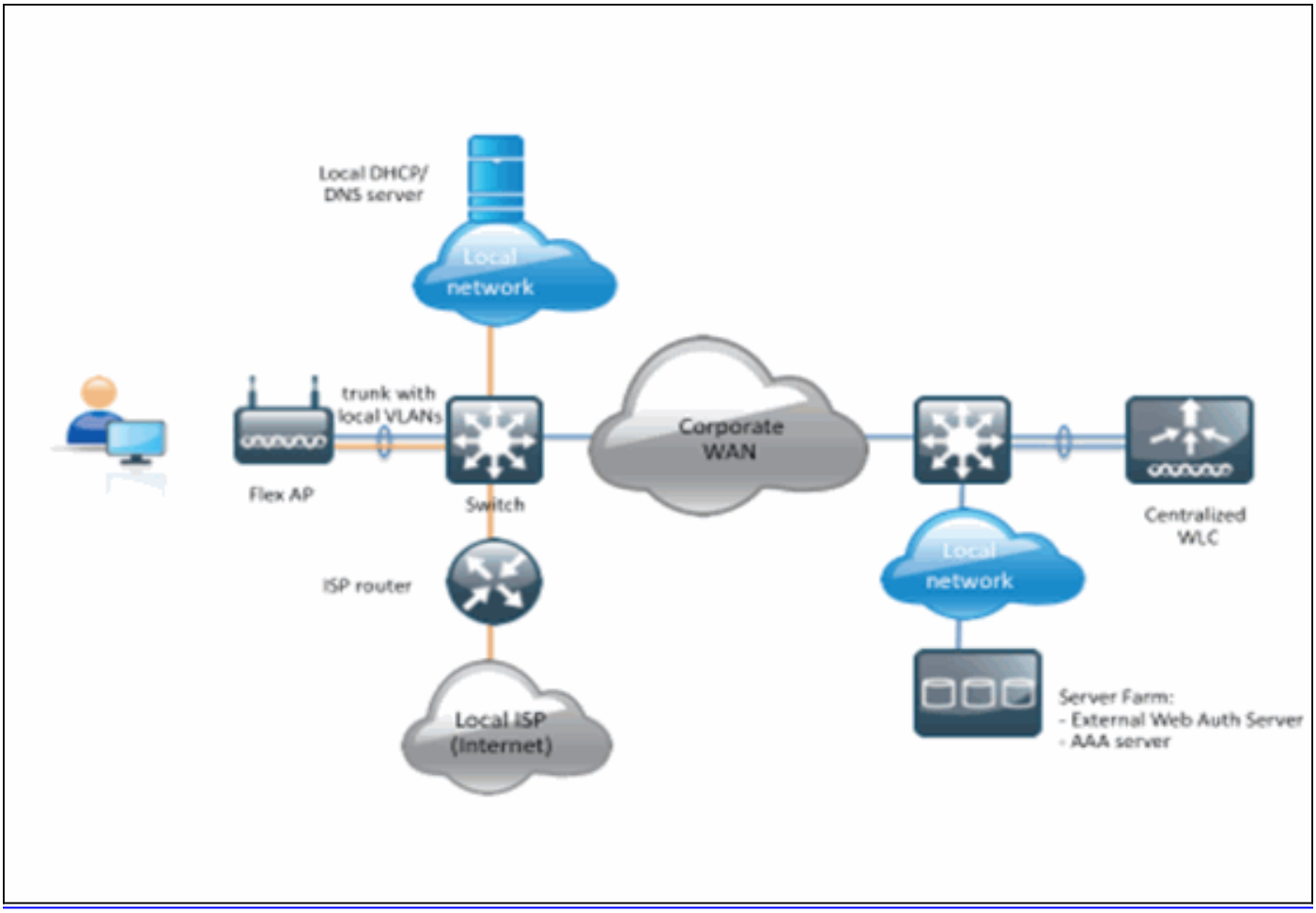
この機能は、FlexConnect モードの AP から外部 Web サーバへの Web 認証を、ローカルにスイッチングされるトラフィック（FlexConnect – ローカル スイッチング）の WLAN に対して実行する機能を拡張します。 WLC リリース 7.2.110.0 より前では、外部サーバへの Web 認証が、ローカル モードまたは FlexConnect モードの AP で、中央でスイッチングされるトラフィック（FlexConnect – 中央スイッチング）の WLAN に対してサポートされていました。

この機能は、外部 Web 認証と呼ばれることも多く、FlexConnect ローカル スイッチング WLAN の機能を拡張して、現在コントローラによって提供されているすべてのレイヤ 3 Web リダイレクト セキュリティ タイプをサポートしています。

- Web 認証
- Web パススルー
- Web 条件付きリダイレクト
- スプラッシュ ページ条件付きリダイレクト

Web 認証おおびローカル スイッチング用に設定された WLAN を考慮した、この機能の背後の論理は、事前認証 FlexConnect アクセス コントロール リスト（ACL）を、WLC レベルではなく、AP レベルに直接配布および適用することです。 このようにして、AP は、ワイヤレス クライアントから送信された、ACL でローカルに許可されているパケットをスイッチングします。 許可されていないパケットは、CAPWAP トンネル上で WLC に送信されます。 一方、AP は、有線インターフェイス上でトラフィックを受信すると、ACL で許されている場合は、ワイヤレス クライアントに転送します。 それ以外の場合、パケットはドロップされます。 クライアントが認証および許可されると、事前認証 FlexConnect ACL が削除され、すべてのクライアント データ トラフィックがローカルに許可され、スイッチングされます。

注: このメカニズムは、ローカルにスイッチングされる VLAN から外部サーバにクライアントが到達可能であることを前提として機能します。



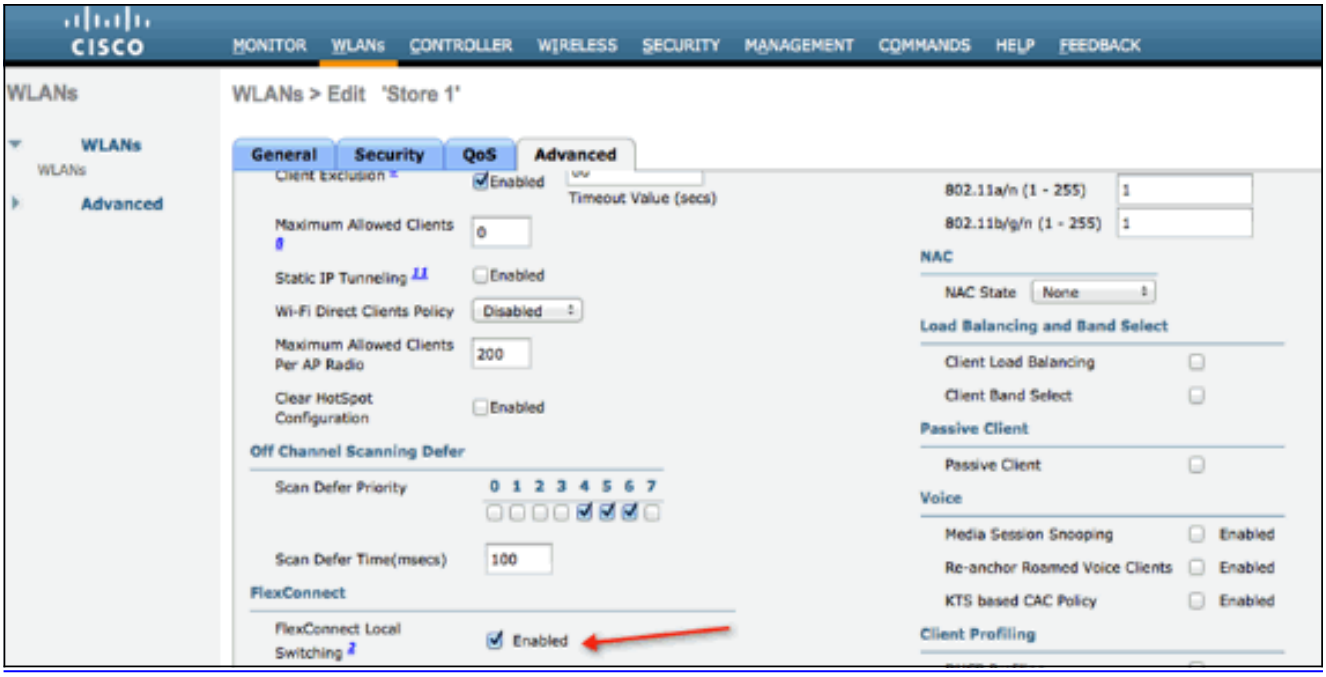
要約：

- FlexConnect ローカル スイッチングおよび L3 セキュリティ用に設定された WLAN
- FlexConnect ACL は事前認証 ACL として使用される
- 一度設定された FlexConnect ACL は、FlexConnect グループまたは個々の AP 経由で AP データベースにプッシュされる必要があるか、WLAN に適用できる
- AP では、事前認証 ACL に一致するすべてのトラフィックにローカル スイッチングが許可される

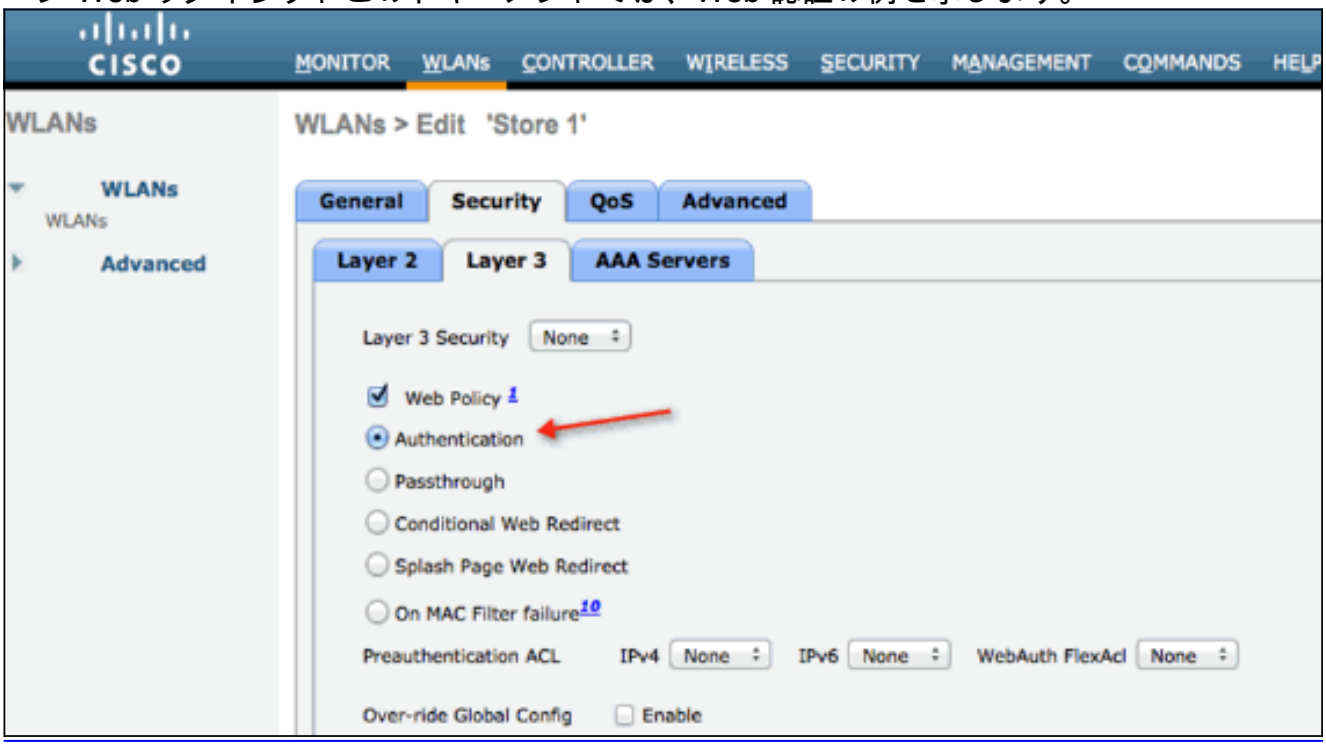
手順：

この機能を設定するには、次の手順を実行します。

1. FlexConnect ローカル スイッチング用に WLAN を設定します。

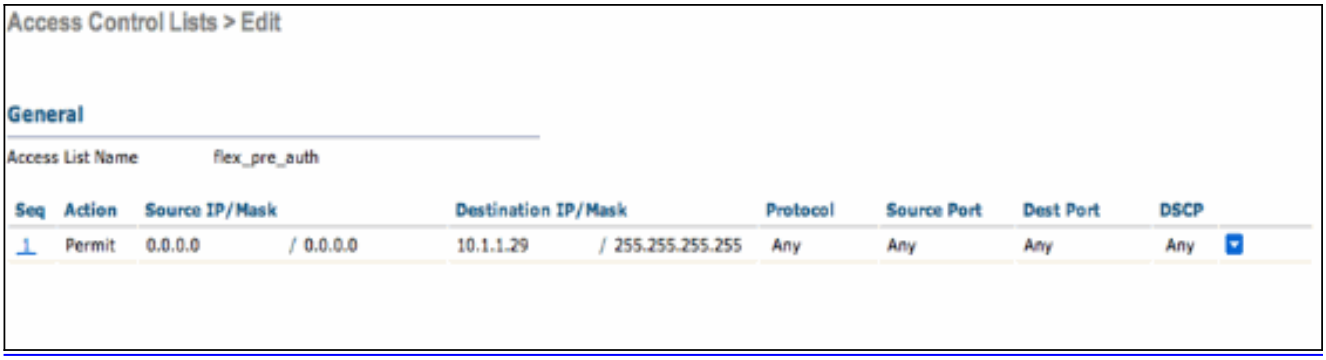


2. 外部 Web 認証を有効にするには、ローカルにスイッチングされる WLAN のセキュリティ ポリシーとして Web ポリシーを設定する必要があります。 これには、次の 4 種類のオプションのいずれかが含まれます。認証パススルー条件付き Web リダイレクトスプラッシュ ページ Web リダイレクトこのドキュメントでは、Web 認証の例を示します。



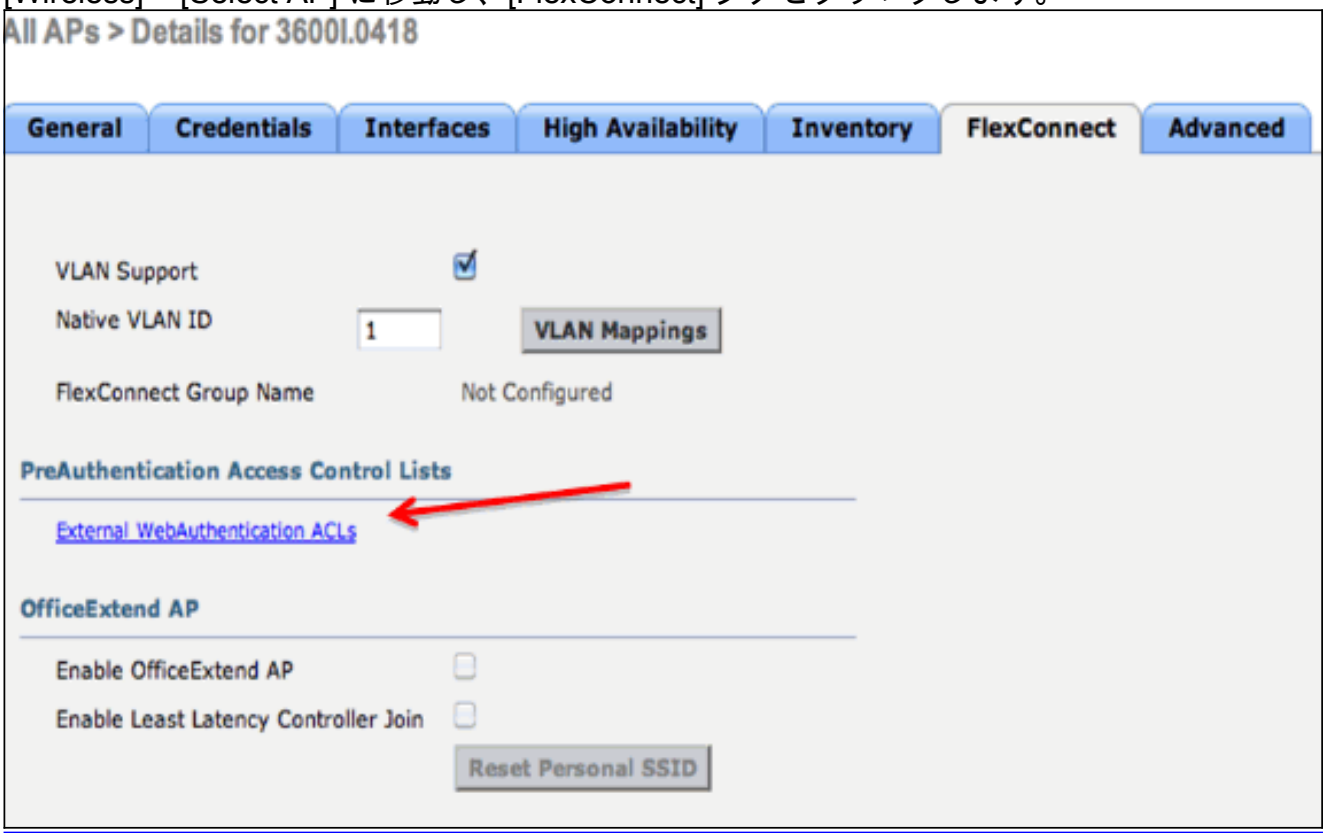
最初の 2 つの方法は似ており、設定の観点からは、Web 認証方式としてグループ化できます。 その次の 2 つ (条件付きリダイレクトとスプラッシュ ページ) は Web ポリシーであり、Web ポリシー方式としてグループ化できます。

3. 事前認証 FlexConnect ACL を、ワイヤレス クライアントが外部サーバの IP アドレスに到達することが許可されるように設定する必要があります。 ARP、DHCP、および DNS のトラフィックは自動的に許可されるため、指定する必要はありません。 [Security] > [Access Control List] で [FlexConnect ACLs] を選択します。 次に、[Add] をクリックし、通常のコントローラ ACL として名前とルールを定義します。

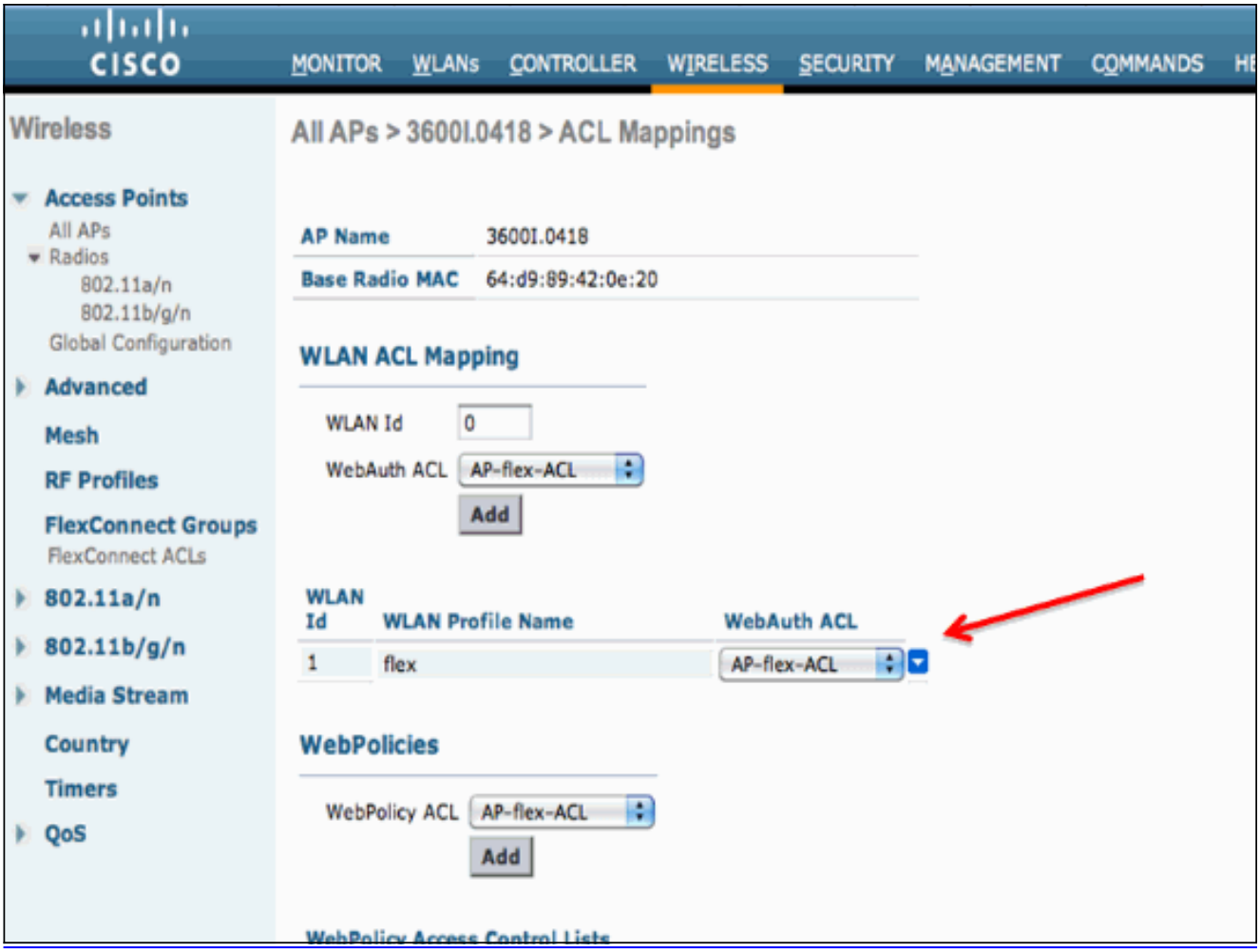


注: トラフィックのための逆ルールをいつも作成する必要があります。

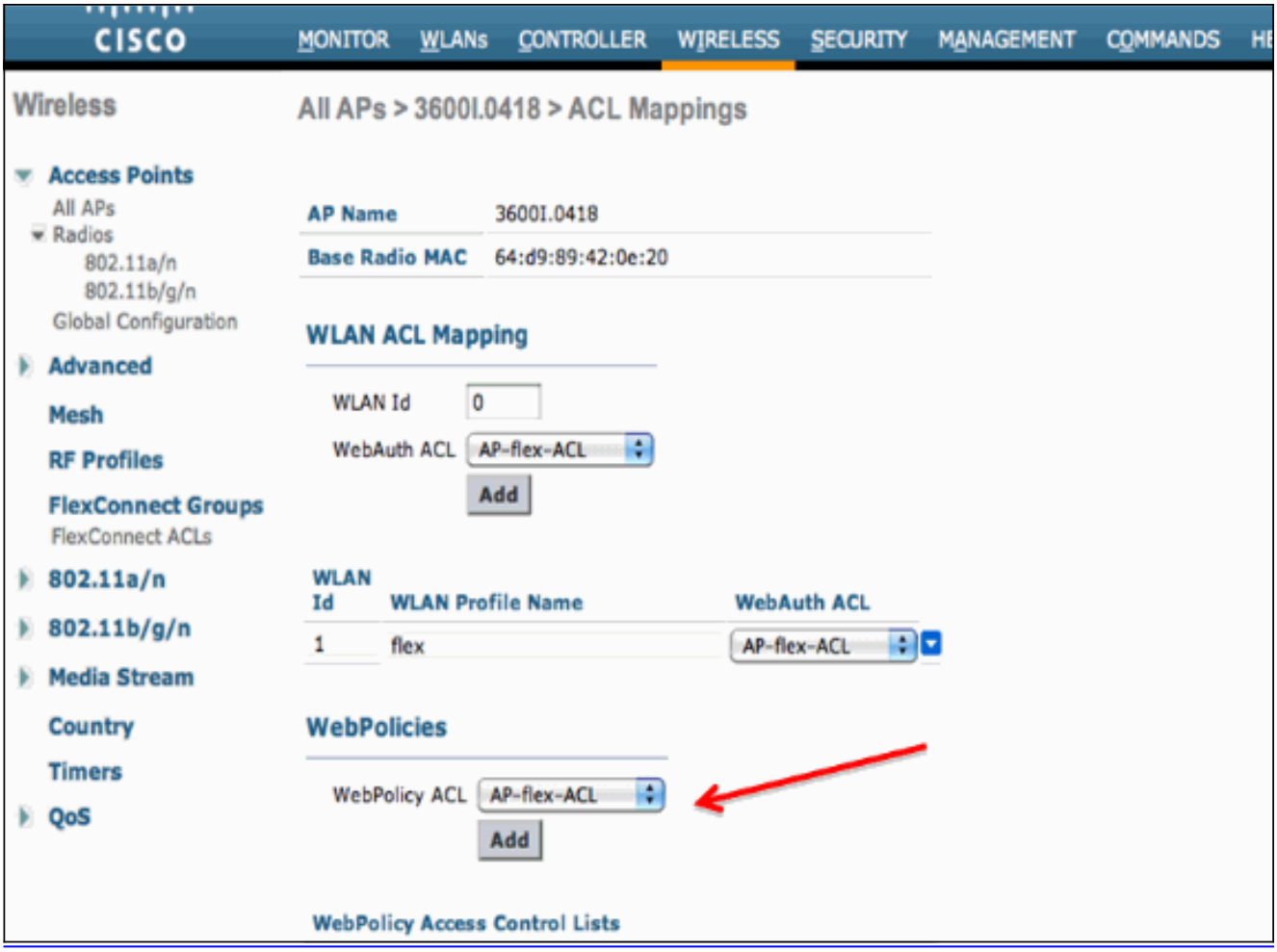
4. FlexConnect ACL が作成されたら、適用する必要があります。これは、 AP、FlexConnect グループ、WLAN の各レベルで実行できます。 この最後のオプション（WLAN での Flex ACL）は、条件付きリダイレクトとスプラッシュ リダイレクトなど、Web ポリシーでの他の 2 つの方法の Web 認証および Web パススルー専用です。 ACL は、AP または Flex グループでだけ適用できできます。 AP レベルで割り当てられた ACL の例を次に示します。 [Wireless] > [Select AP] に移動し、[FlexConnect] タブをクリックします。



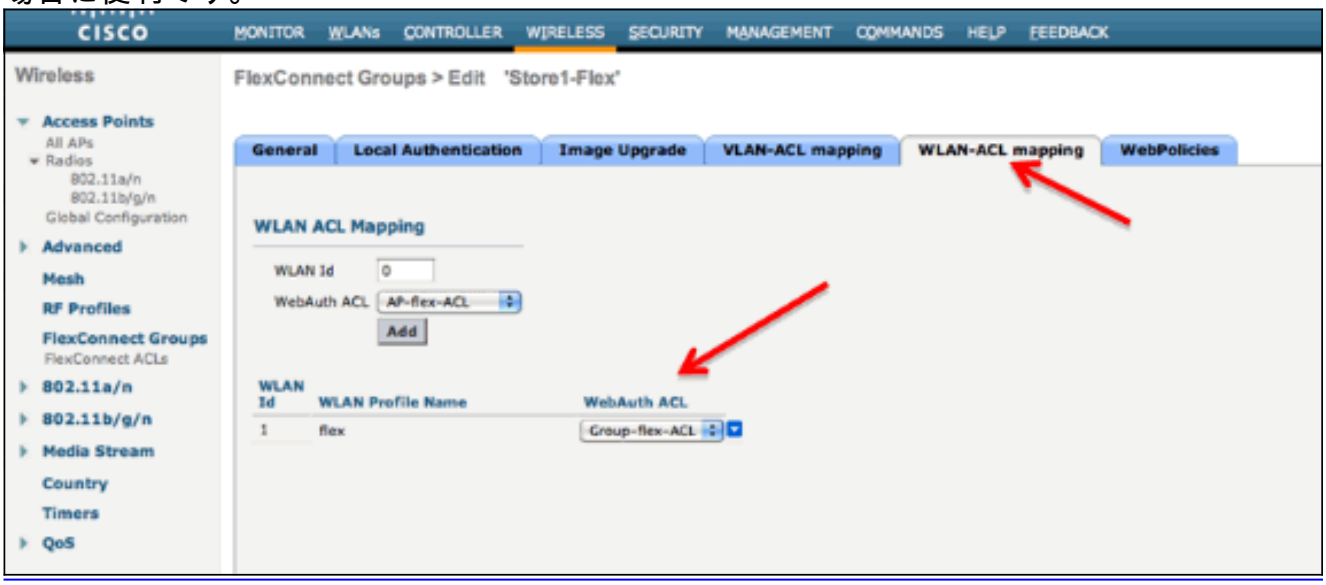
[External WebAuthentication ACLs] リングをクリックします。 次に、特定の WLAN ID の ACL を選択します。



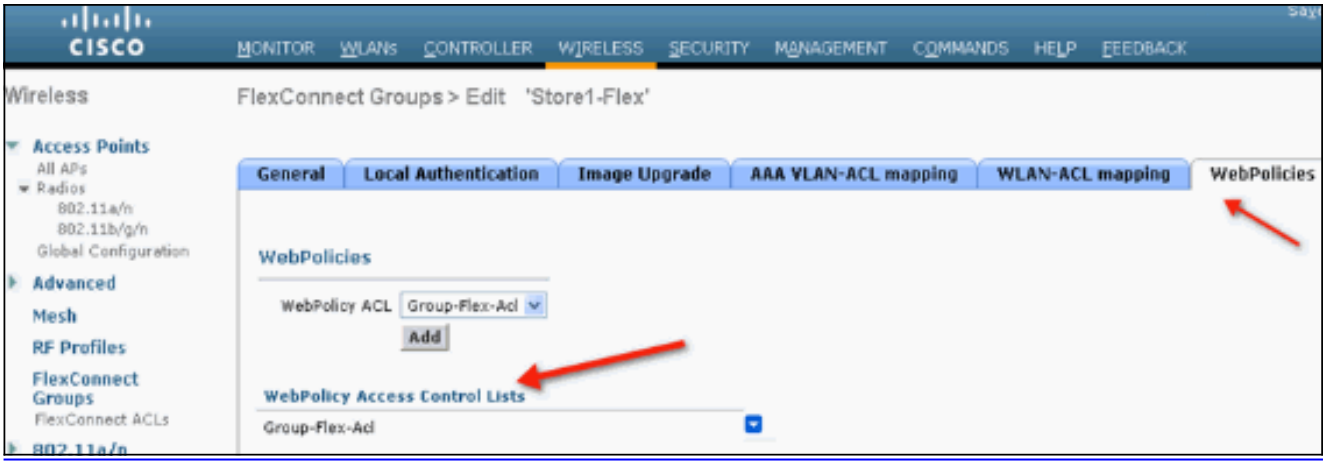
同様に、同じ [External WebAuthentication ACLs] リンクをクリックした後、Web ポリシー ACL（条件付きリダイレクト、スプラッシュ ページ リダイレクトなど）用に、Web ポリシーの Flex Connect ACL を選択できるようになります。 これは、次の図に示されています。



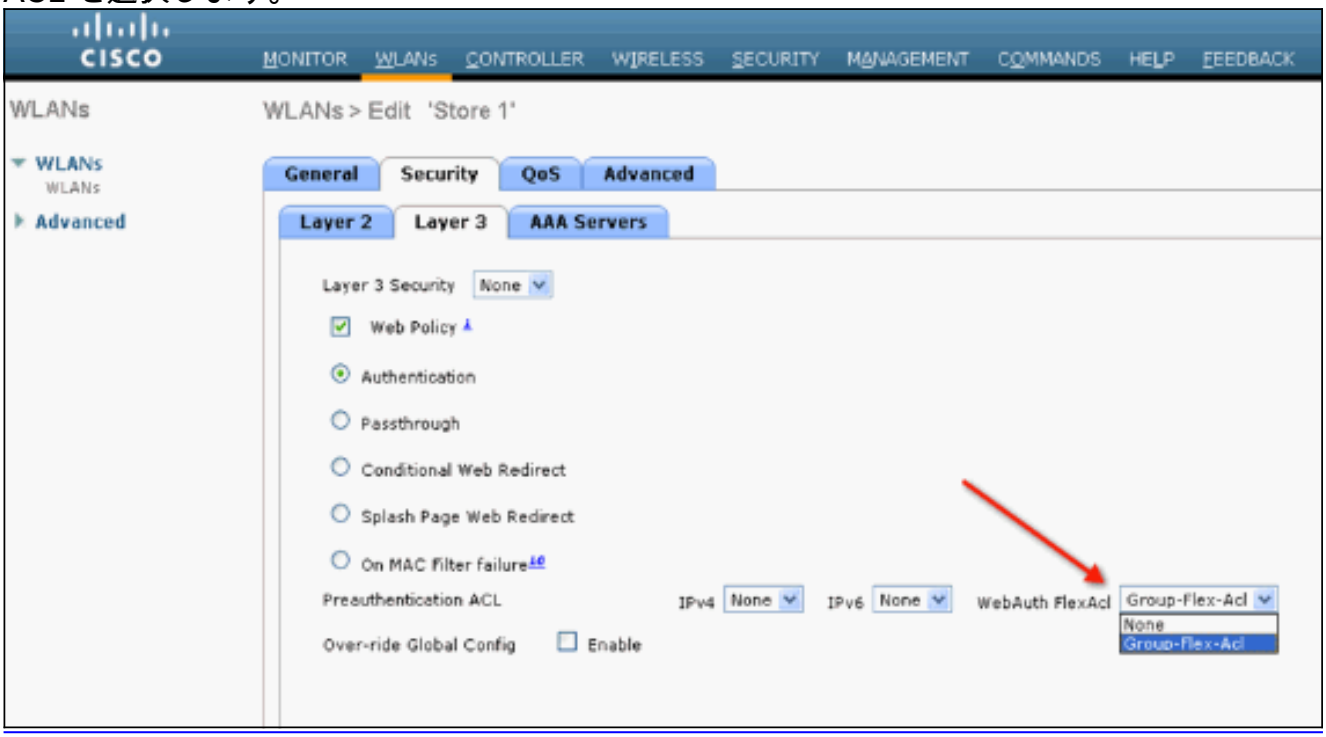
5. ACL は、FlexConnect グループ レベルでも適用できます。 これを行うには、FlexConnect グループ設定で [WLAN-ACL mapping] タブに移動します。 次に、WLAN ID と、適用する ACL を選択します。 [Add] をクリックします。 これは、AP のグループに ACL を定義する場合に便利です。



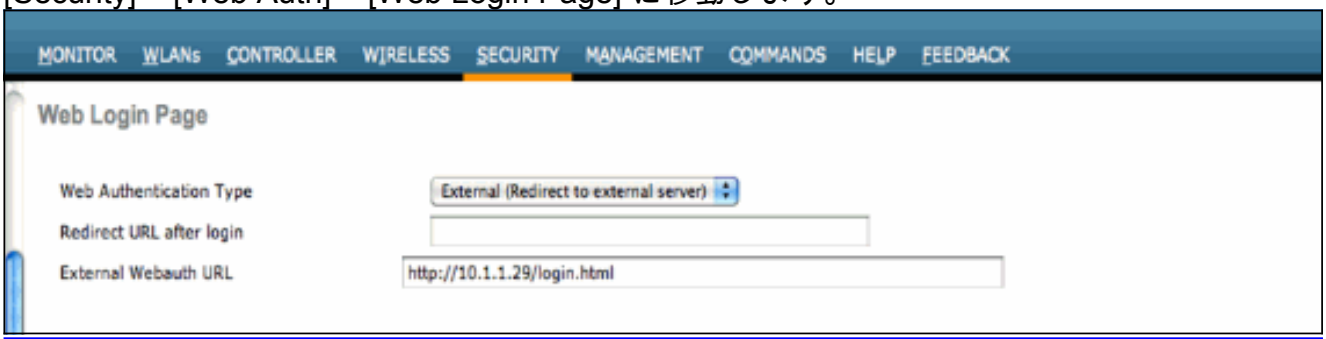
同様に、Web ポリシー ACL (条件リダイレクトとスプラッシュ ページ Web リダイレクトの場合) に対して [WebPolicies] タブを選択する必要があります。



6. Web 認証と Web パススルーの Flex ACL も、WLAN で適用できます。 これを行うには、[WLAN] > [Security] の [Layer 3] タブで [WebAuth FlexACL] ドロップダウン リストから ACL を選択します。



7. 外部 Web 認証用のために、リダイレクト URL を定義する必要があります。 これは、グローバル レベルまたは WLAN レベルで実行できます。 WLAN レベルに対して、[Over-ride Global Config] チェックマークをクリックし、URL を挿入します。 グローバル レベルで [Security] > [Web Auth] > [Web Login Page] に移動します。



制限事項：Web 認証（内部の、または外部サーバへの）では、FlexConnect AP が接続モードであることが必要です。 Web 認証は、FlexConnect AP がスタンドアロン モードの場合はサポートされません。Web 認証（内部の、または外部サーバへの）は、中央認証の場合にのみサポートされます。 ローカル スイッチング用に設定された WLAN がローカル認証用に設定されている場合は、Web 認証を実行できません。すべての Web リダイレクトは、

AP レベルではなく、WLC で実行されます。

関連情報

- テクニカル サポートとドキュメント – Cisco Systems