Guide de déploiement de l'authentification Web externe avec la commutation locale FlexConnect

Contenu

Introduction

Ce document explique comment utiliser un serveur Web externe avec la commutation locale FlexConnect pour différentes politiques Web.

Conditions préalables

Conditions requises

Assurez-vous que vous répondez à ces exigences avant d'essayer cette configuration :

- Connaissances de base sur l'architecture et les points d'accès FlexConnect
- Connaissances sur la configuration et la configuration d'un serveur Web externe
- Connaissances sur la configuration et la configuration des serveurs DHCP et DNS

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Contrôleur LAN sans fil (WLC) Cisco 7500 qui exécute la version 7.2.110.0 du micrologiciel
- Point d'accès allégé (LAP) Cisco, série 3500
- Serveur Web externe qui héberge la page de connexion d'authentification Web
- Serveurs DNS et DHCP sur le site local pour la résolution d'adresses et l'allocation d'adresses IP aux clients sans fil

The information in this document was created from the devices in a specific lab environment. Bien qu'un WLC de la gamme 7500 soit utilisé pour ce guide de déploiement, cette fonctionnalité est prise en charge sur les WLC 2500, 5500 et WiSM-2. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Présentation des fonctionnalités

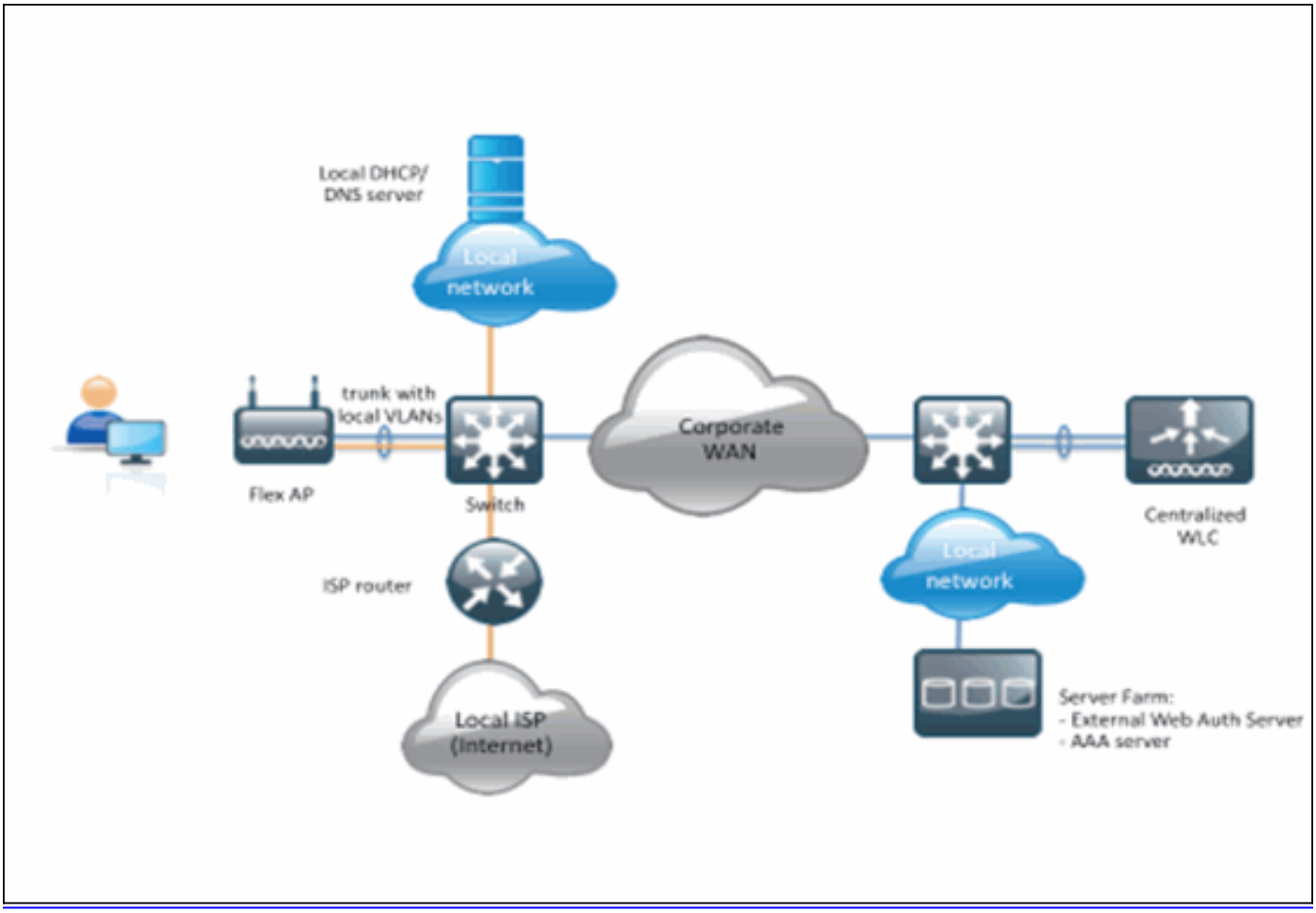
Cette fonctionnalité étend la capacité d'exécution de l'authentification Web à un serveur Web externe à partir de l'AP en mode FlexConnect, pour les WLAN avec trafic commuté localement (FlexConnect - Commutation locale). Avant la version 7.2.110.0 du WLC, l'authentification Web à un serveur externe était prise en charge pour les points d'accès en mode local ou FlexConnect pour les WLAN avec trafic commuté centralisé (FlexConnect - Commutation centrale).

Souvent appelée Authentification Web externe, cette fonctionnalité étend la capacité du WLAN de commutation locale FlexConnect pour prendre en charge tous les types de sécurité de redirection Web de couche 3 actuellement fournis par le contrôleur :

- Authentification Web
- Accès Web
- Redirection conditionnelle Web
- Redirection conditionnelle de la page de démarrage

En considérant un WLAN configuré pour l'authentification Web et la commutation locale, la logique derrière cette fonctionnalité est de distribuer et d'appliquer la liste de contrôle d'accès (ACL) FlexConnect de préauthentification directement au niveau du point d'accès au lieu du niveau du WLC. De cette manière, le point d’accès commute localement les paquets provenant du client sans fil qui sont autorisés par la liste de contrôle d’accès. Les paquets non autorisés sont toujours envoyés par le tunnel CAPWAP au WLC. D'autre part, lorsque le point d'accès reçoit le trafic sur l'interface câblée, si la liste de contrôle d'accès l'autorise, le transfère au client sans fil. Sinon, le paquet est abandonné. Une fois le client authentifié et autorisé, la liste de contrôle d'accès Pre-Authentication FlexConnect est supprimée et tout le trafic de données client est autorisé et commuté localement.

Remarque : cette fonctionnalité fonctionne en partant du principe que le client peut atteindre le serveur externe à partir du VLAN commuté localement.



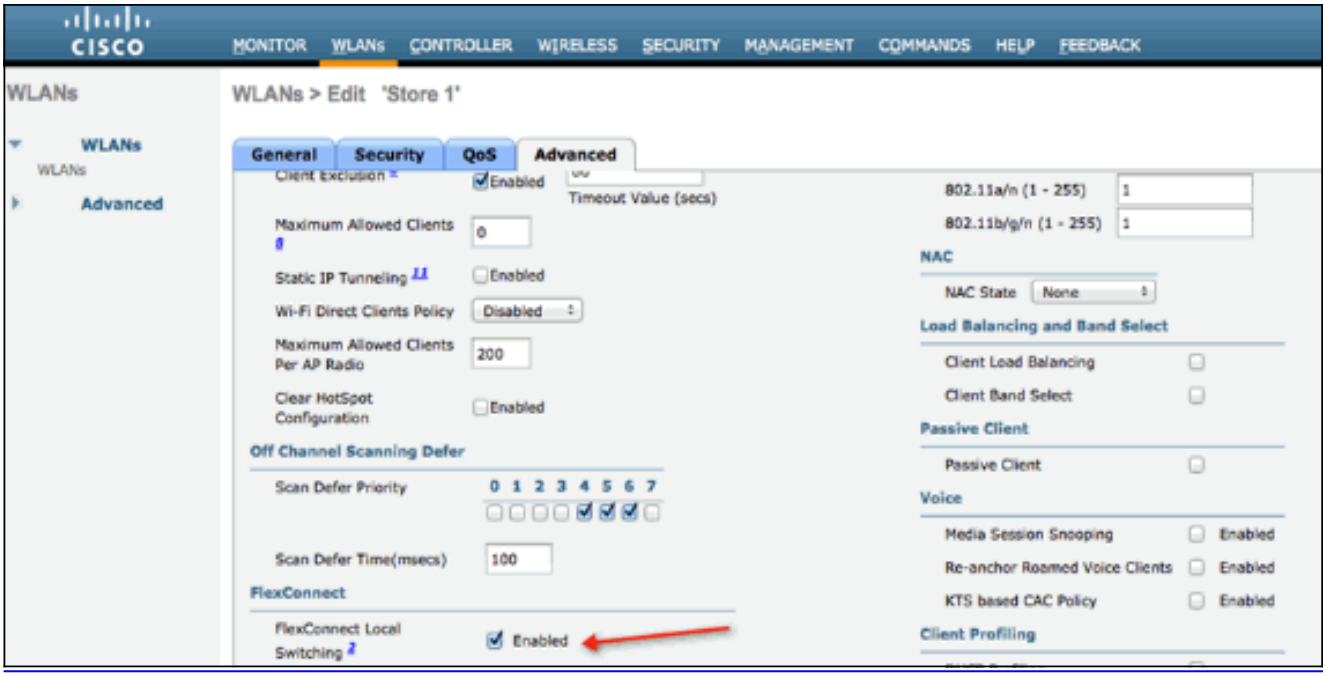
Résumé:

- WLAN configuré pour la commutation locale FlexConnect et la sécurité de couche 3
- Les listes de contrôle d'accès FlexConnect seront utilisées comme listes de contrôle d'accès pré-authentification
- Une fois configurées, les listes de contrôle d'accès FlexConnect doivent être transmises à la base de données des points d'accès via Flex Group ou via un point d'accès individuel, ou peuvent être appliquées sur le WLAN
- Le point d’accès permet à tout le trafic correspondant à la liste de contrôle d’accès de pré-authentification d’être commuté localement

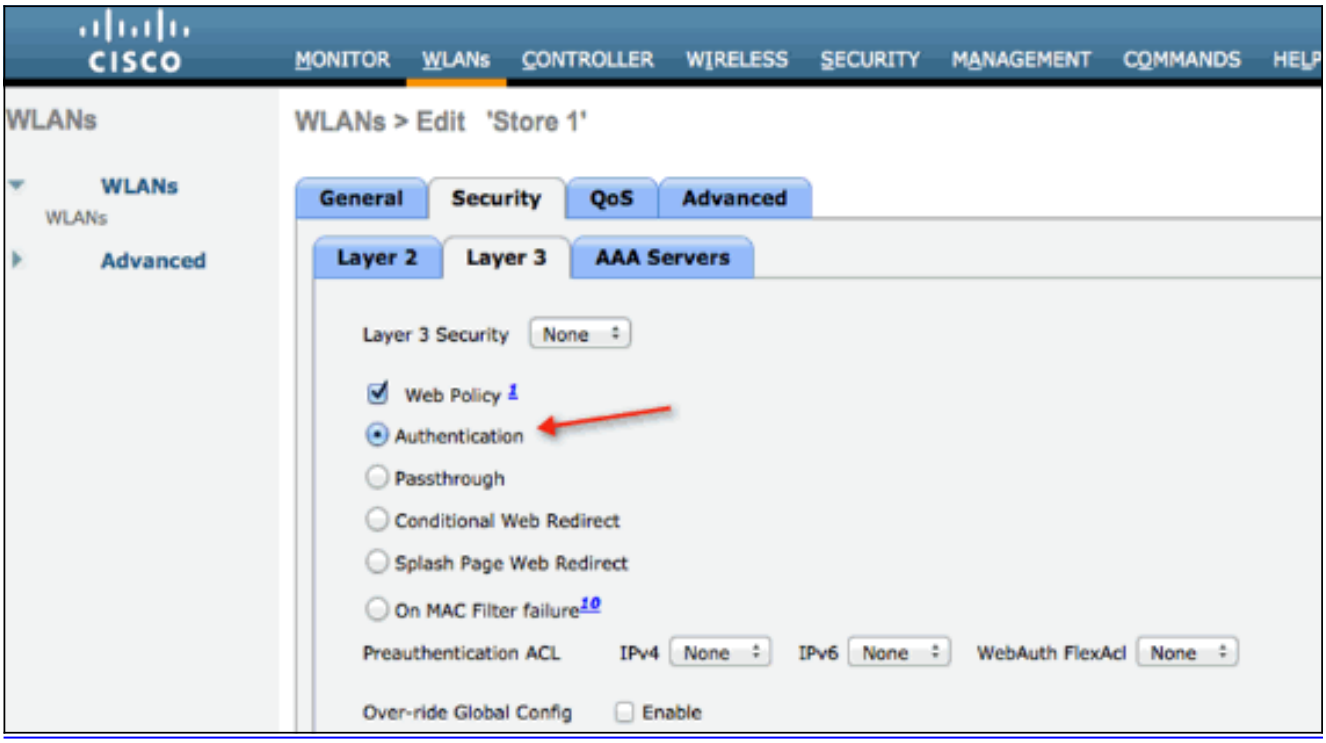
Procédure:

Complétez ces étapes afin de configurer cette fonctionnalité :

1. Configurez un WLAN pour la commutation locale FlexConnect.

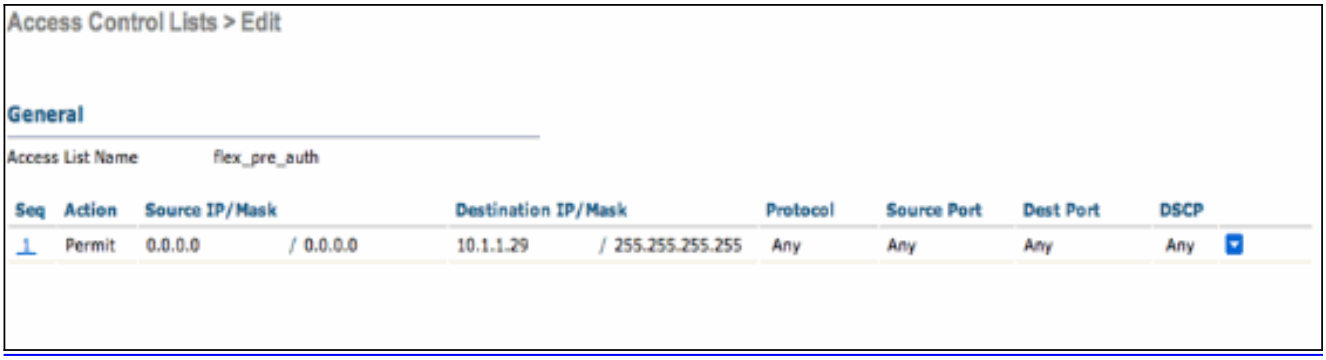


2. Afin d'activer l'authentification Web externe, vous devez configurer la stratégie Web comme stratégie de sécurité pour le WLAN commuté localement. Ceci inclut l'une des quatre options suivantes :AuthentificationPassthroughRedirection Web conditionnelleRedirection Web de la page de démarrageCe document capture un exemple d'authentification Web
:



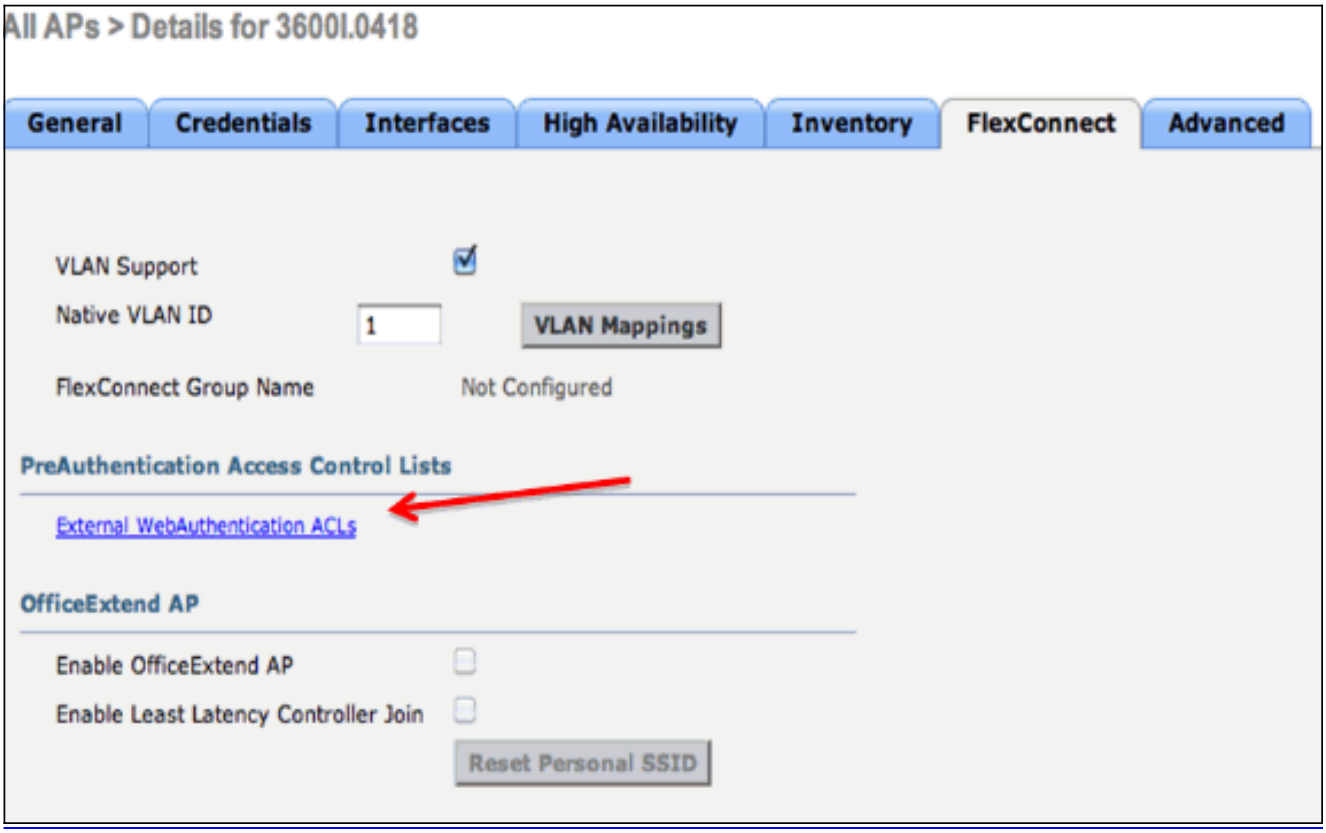
Les deux premières méthodes sont similaires et peuvent être regroupées en méthodes d'authentification Web d'un point de vue de configuration. Les deux autres (Redirection conditionnelle et Page de démarrage) sont des stratégies Web et peuvent être regroupées en méthodes de stratégie Web.

3. La liste de contrôle d'accès Pre-Authentication FlexConnect doit être configurée pour permettre aux clients sans fil d'atteindre l'adresse IP du serveur externe. Le trafic ARP, DHCP et DNS est automatiquement autorisé et n'a pas besoin d'être spécifié. Sous Security > Access Control List, sélectionnez **FlexConnect ACL**. Ensuite, cliquez sur **Ajouter** et définissez les noms et les règles en tant que liste de contrôle d'accès de contrôleur normale.

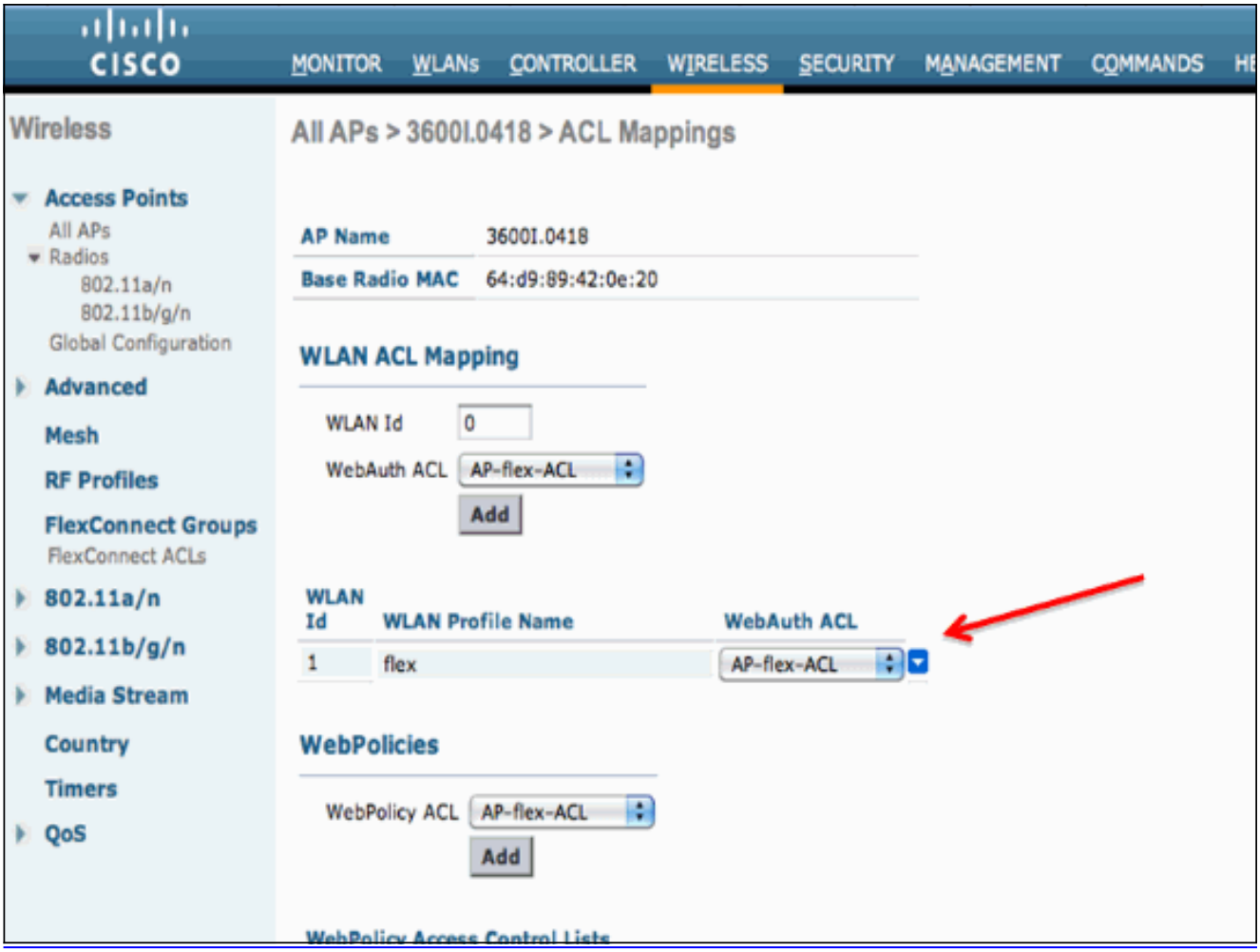


Note: Vous devez créer des règles inverses pour le trafic à chaque fois.

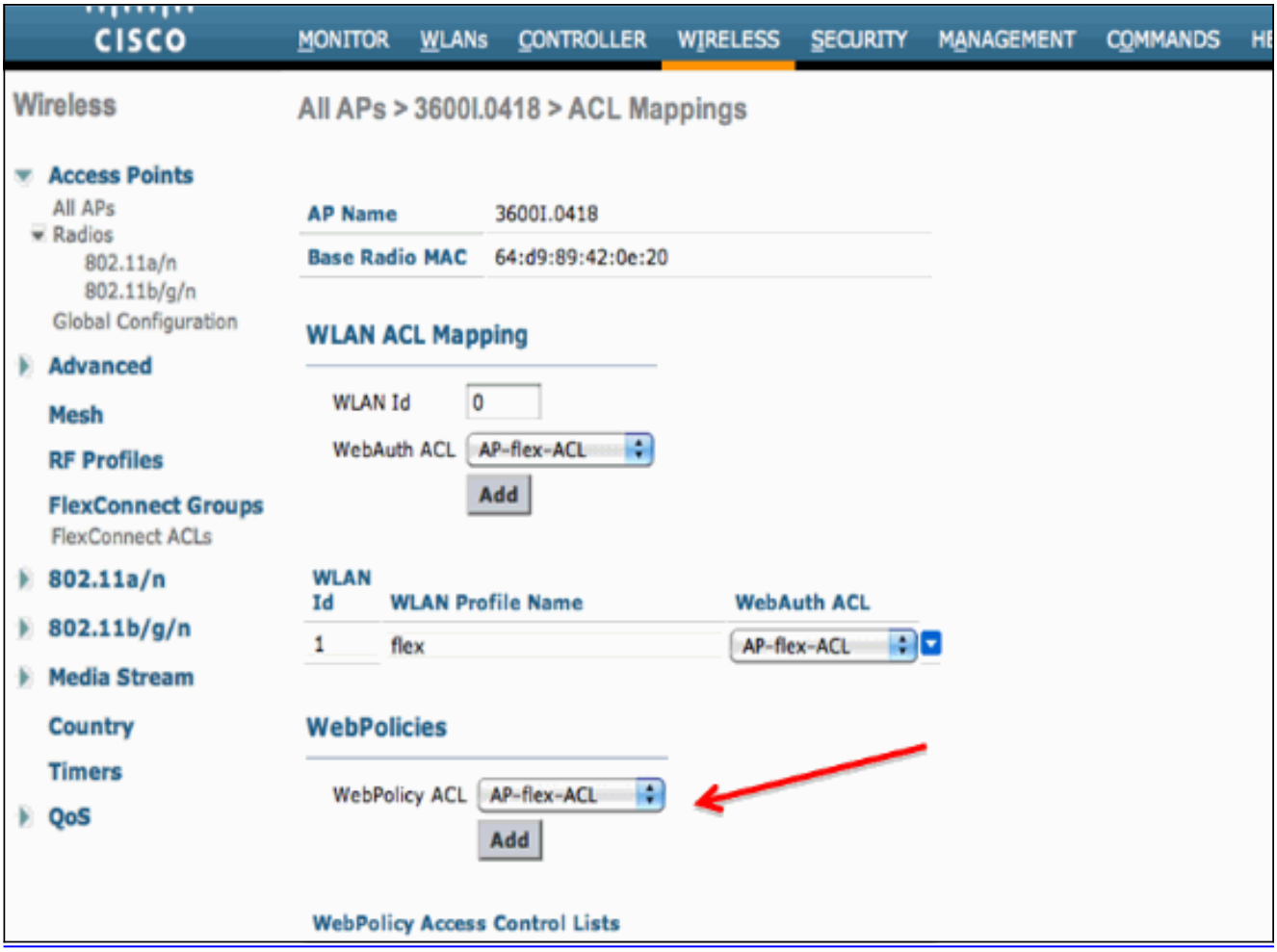
4. Une fois les listes de contrôle d'accès FlexConnect créées, elles doivent être appliquées à différents niveaux : AP, FlexConnect Group et WLAN. Cette dernière option (Flex ACL at WLAN) est uniquement destinée à l'authentification Web et au transfert Web pour deux autres méthodes sous Politique Web, telles que Conditional et Splash Redirect. Les listes de contrôle d'accès ne peuvent être appliquées qu'au niveau du groupe AP ou Flex. Voici un exemple de liste de contrôle d'accès affectée au niveau du point d'accès. Accédez à **Wireless > select AP**, puis cliquez sur l'onglet **FlexConnect** :



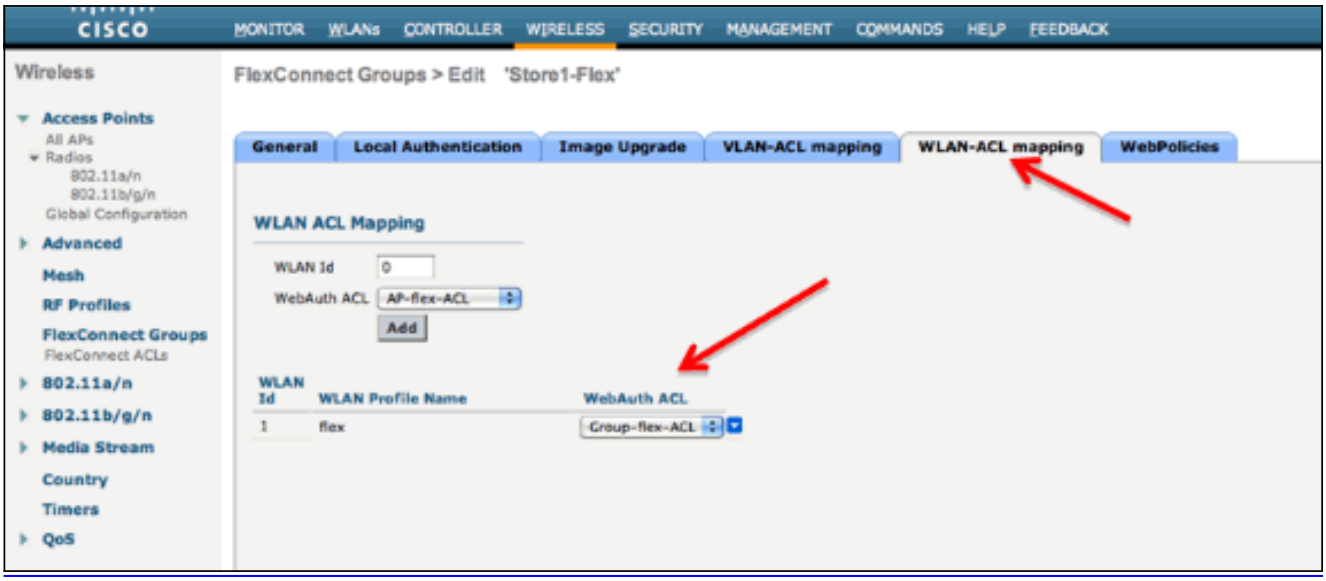
Cliquez sur le lien **ACL d'authentification Web externe**. Choisissez ensuite la liste de contrôle d'accès correspondant à l'ID WLAN spécifique :



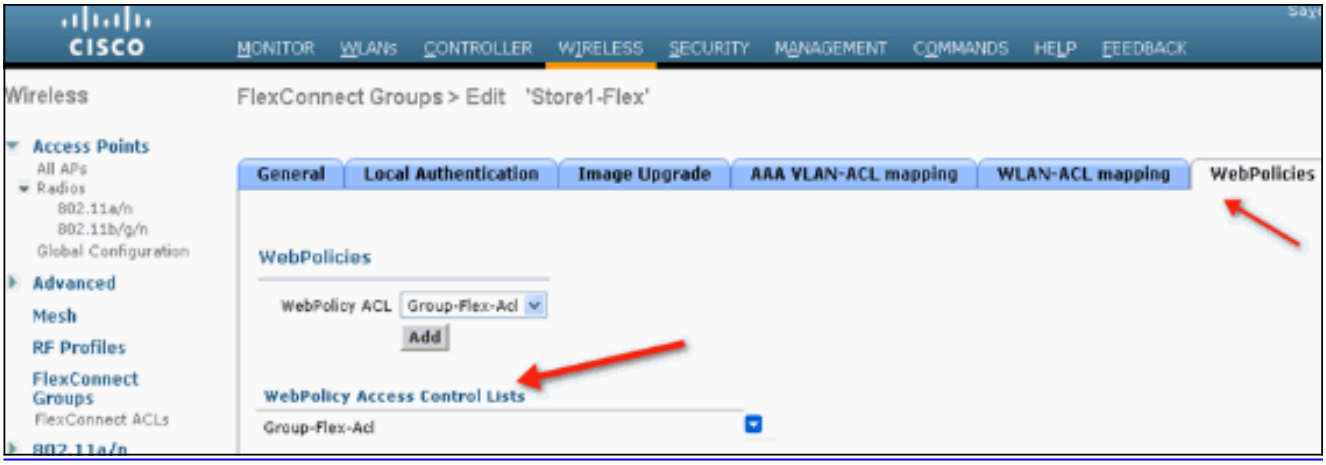
De même, pour la liste de contrôle d'accès de stratégie Web (par exemple, la redirection conditionnelle ou la redirection de page de démarrage), vous recevrez une option pour sélectionner la liste de contrôle d'accès Flex Connect sous WebPolicies après avoir cliqué sur le même lien ACL d'authentification Web externe. Ceci est illustré ici
:



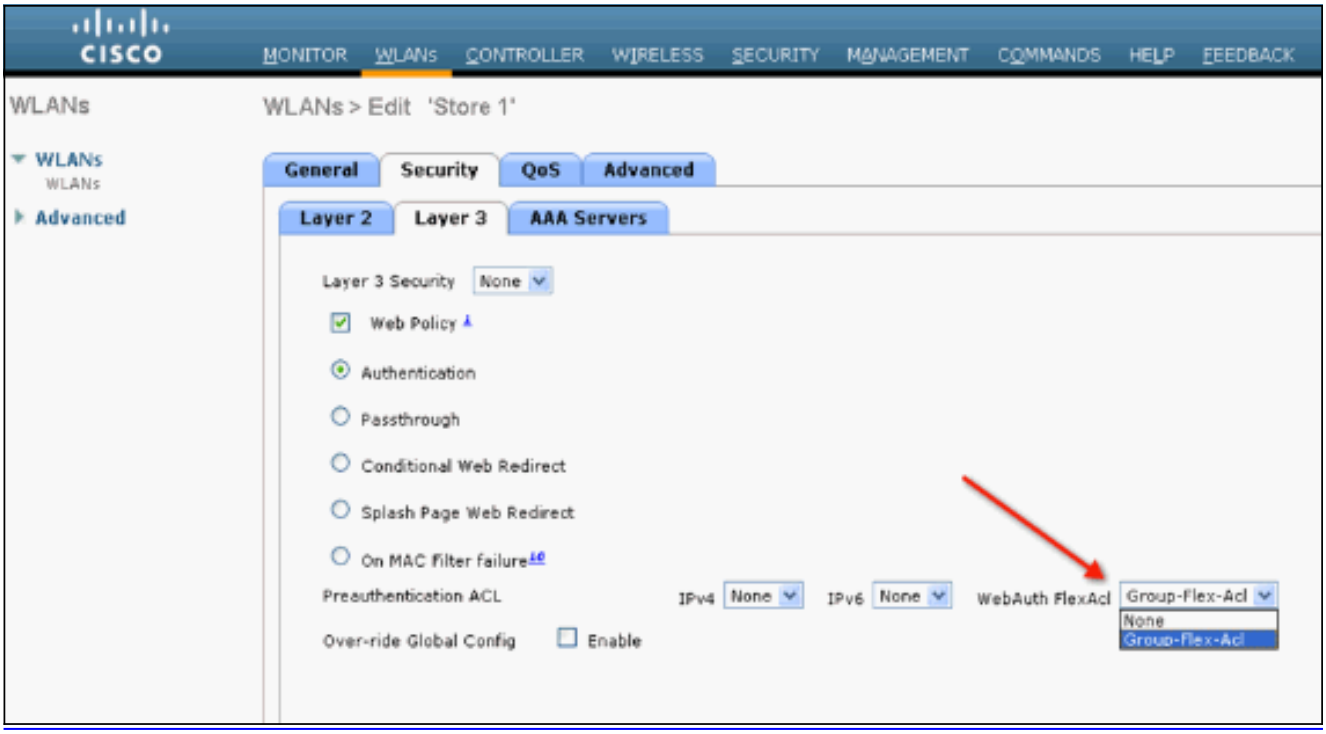
5. La liste de contrôle d'accès peut également être appliquée au niveau du groupe FlexConnect. Pour ce faire, accédez à l'onglet **WLAN-ACL mapping** dans la configuration FlexConnect Group. Choisissez ensuite l'ID WLAN et la liste de contrôle d'accès que vous voulez appliquer. Cliquez sur **Add**. Ceci est utile lorsque vous voulez définir une liste de contrôle d'accès pour un groupe de points d'accès.



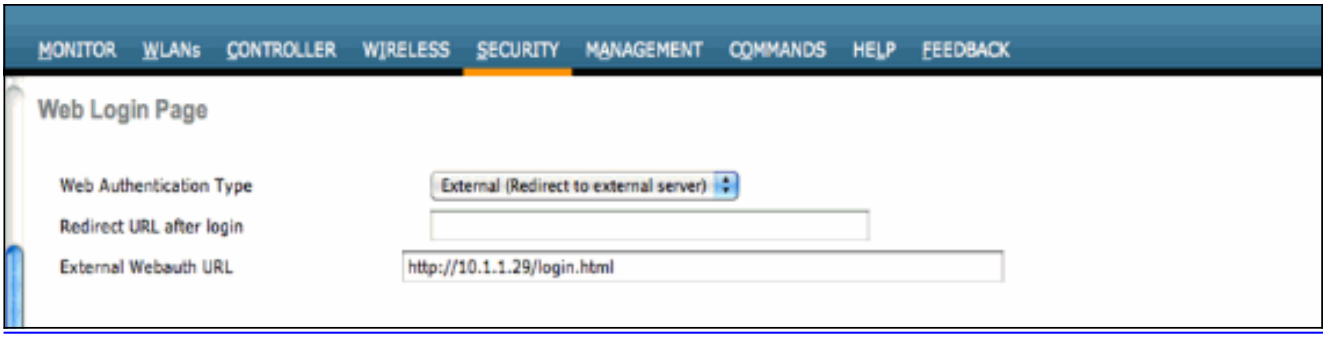
De même, pour la liste de contrôle d'accès de stratégie Web (pour Redirection Web conditionnelle et Page de démarrage), vous devez sélectionner l'onglet **WebPolicies**.



6. L'authentification Web et les listes de contrôle d'accès Flex Web Pass-through peuvent également être appliquées sur le WLAN. Pour ce faire, choisissez la liste de contrôle d'accès dans la liste déroulante **WebAuth FlexACL** sous l'onglet Couche 3 dans WLAN > Sécurité.



7. Pour l'authentification Web externe, l'URL de redirection doit être définie. Cela peut se faire au niveau mondial ou au niveau des réseaux locaux sans fil. Pour le niveau WLAN, cliquez sur la coche **Remplacer la configuration globale** et insérez l'URL. Au niveau mondial, accédez à **Security > Web Auth > Web Login Page**
:



Limites:L'authentification Web (interne ou externe) nécessite que le point d'accès Flex soit en mode Connecté. L'authentification Web n'est pas prise en charge si Flex AP est en mode autonome.L'authentification Web (interne ou externe) est uniquement prise en charge avec

l'authentification centrale. Si un WLAN configuré pour la commutation locale est configuré pour l'authentification locale, vous ne pouvez pas effectuer l'authentification Web.Toute redirection Web est effectuée au niveau du WLC et non au niveau du point d'accès.

Informations connexes

- Support et documentation techniques - Cisco Systems