Authentification de Web externe avec le guide de déploiement de commutation locale de FlexConnect

Contenu

Introduction

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

Conditions préalables

Exigences

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

- Connaissance de base au sujet de l'architecture de FlexConnect et des Points d'accès (aps)
- La connaissance sur la façon dont installer et configurer un web server externe
- La connaissance sur la façon dont installer et configurer le DHCP et les serveurs DNS

Composants utilisés

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

- Le contrôleur LAN Sans fil de Cisco 7500 (WLC) ce exécute la version de microprogramme 7.2.110.0
- Point d'accès léger (LAP) de gamme Cisco 3500
- Web server externe qui héberge la page de connexion d'authentification Web
- DN et serveurs DHCP sur le site local pour l'address resolution et l'allocation d'adresse IP aux clients sans fil

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Bien qu'une gamme 7500 WLC soit utilisée pour ce guide de déploiement, cette caractéristique est prise en charge sur 2500, 5500, et WiSM-2 WLCs. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par

défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

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

Vue d'ensemble des fonctionnalités

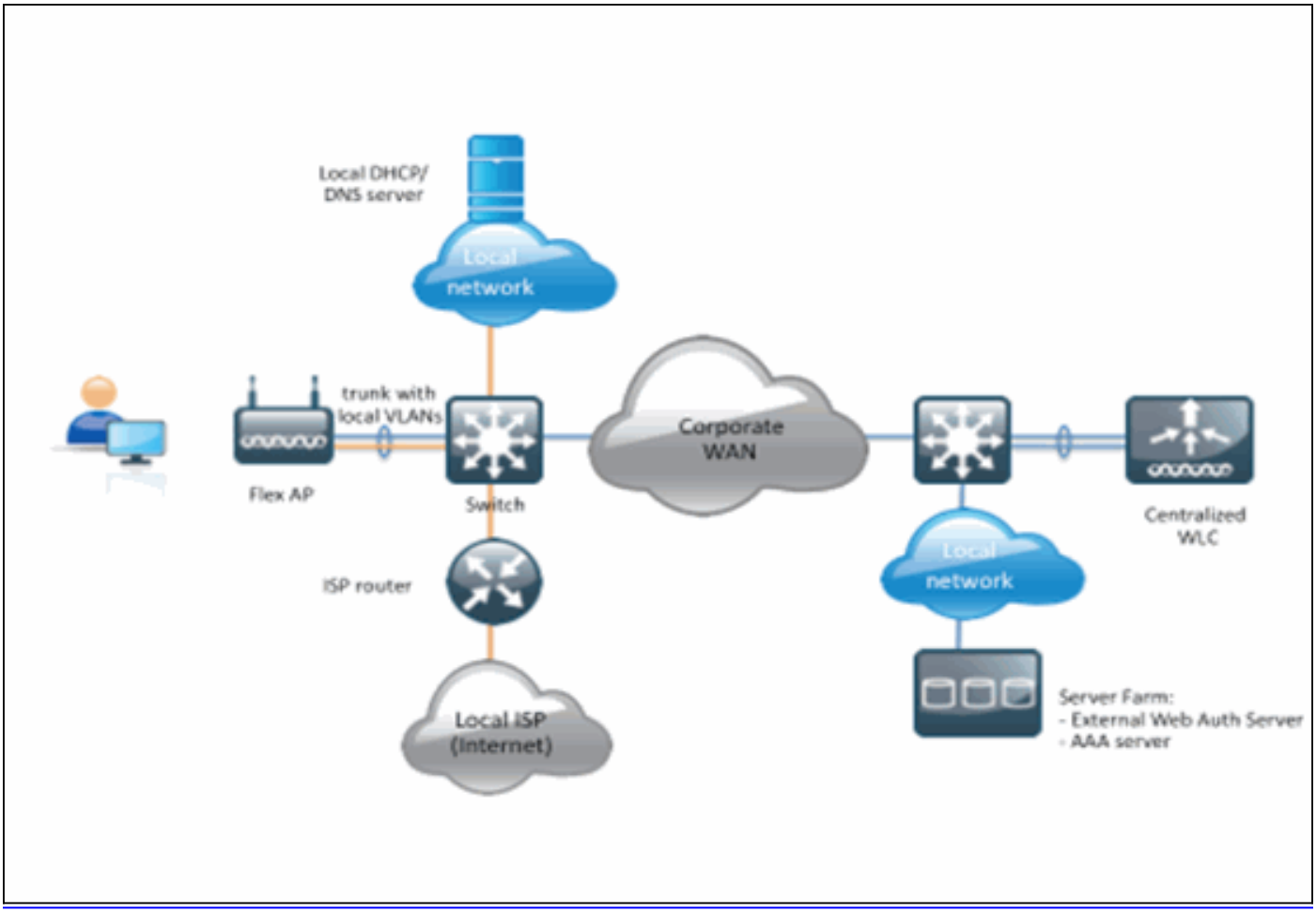
Cette caractéristique étend la capacité d'exécuter l'authentification Web à un web server externe d'AP en mode de FlexConnect, pour les WLAN avec le trafic localement commuté (FlexConnect – commutation locale). Avant que la release 7.2.110.0 WLC, l'authentification Web à un serveur externe ait été prise en charge pour des aps en mode local ou mode de FlexConnect pour des WLAN avec le trafic centralement commuté (FlexConnect – commutation centrale).

Souvent désigné sous le nom de l'authentification de Web externe, cette caractéristique étend la capacité pour la commutation locale WLAN de FlexConnect pour prendre en charge tout le Web de la couche 3 réorientent des types de Sécurité actuellement fournis par le contrôleur :

- Authentification Web
- Intercommunication de Web
- Le Web conditionnel réorientent
- La page de splash conditionnelle réorientent

Vu qu'un WLAN configuré pour l'authentification Web et pour la commutation locale, la logique derrière cette caractéristique est de distribuer et appliquer la liste de contrôle d'accès de FlexConnect de Pré-authentification (ACL) directement au niveau AP au lieu du niveau WLC. De cette façon, AP commutera les paquets provenant le client sans fil qui sont permis par l'ACL, localement. Les paquets non permis sont encore envoyés au-dessus du tunnel CAPWAP au WLC. D'autre part, quand AP reçoit le trafic au-dessus de l'interface de câble, si autorisé par l'ACL, l'expédiera au client sans fil. Autrement, le paquet est lâché. Une fois que le client est authentifié et autorisé, l'ACL de FlexConnect de Pré-authentification est retiré, et tout le trafic de données de client est permis et commuté localement.

Remarque: Cette caractéristique fonctionne dans la supposition que le client peut atteindre le serveur externe du VLAN localement commuté.



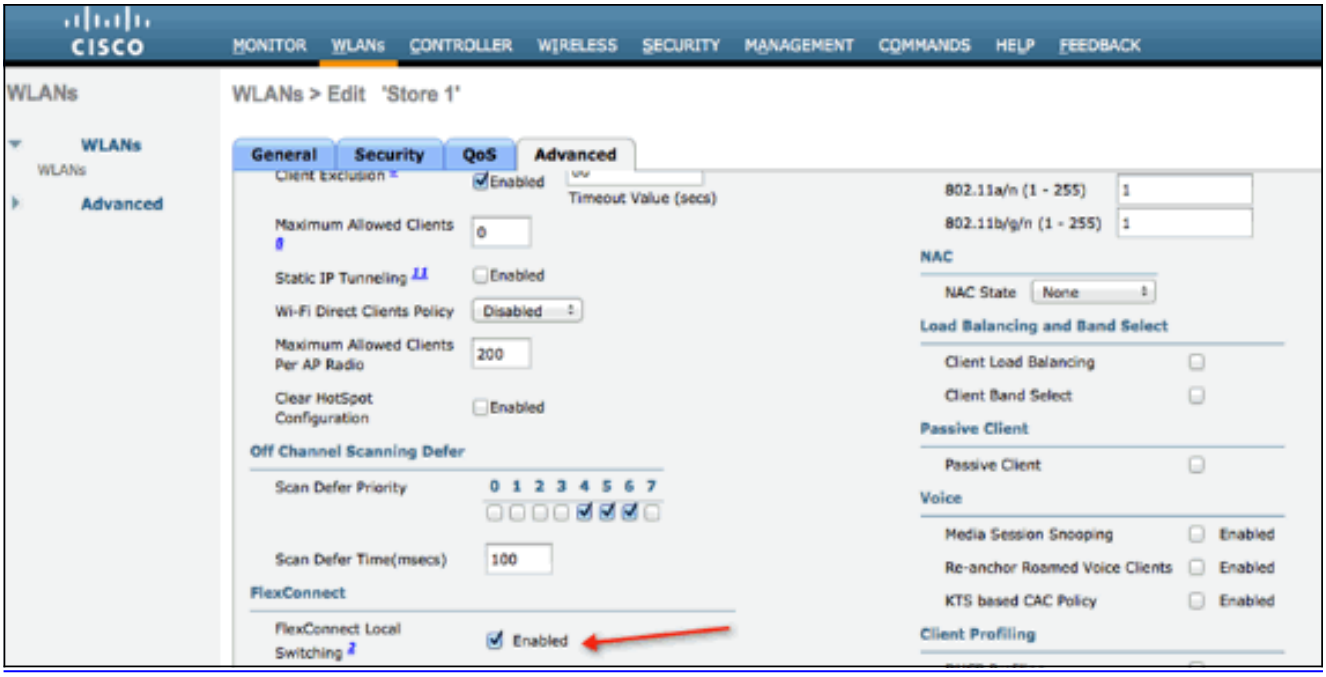
Résumé :

- WLAN configuré pour la commutation locale de FlexConnect et la Sécurité L3
- FlexConnect ACLs sera utilisé comme Pré-authentification ACLs
- FlexConnect ACLs une fois configuré doit être poussé à la base de données AP par l'intermédiaire du groupe de flexible ou par l'intermédiaire d'AP individuel, ou peut être appliqué sur le WLAN
- AP permet tout le trafic qui apparie l'ACL de Pré-authentification à commuter localement

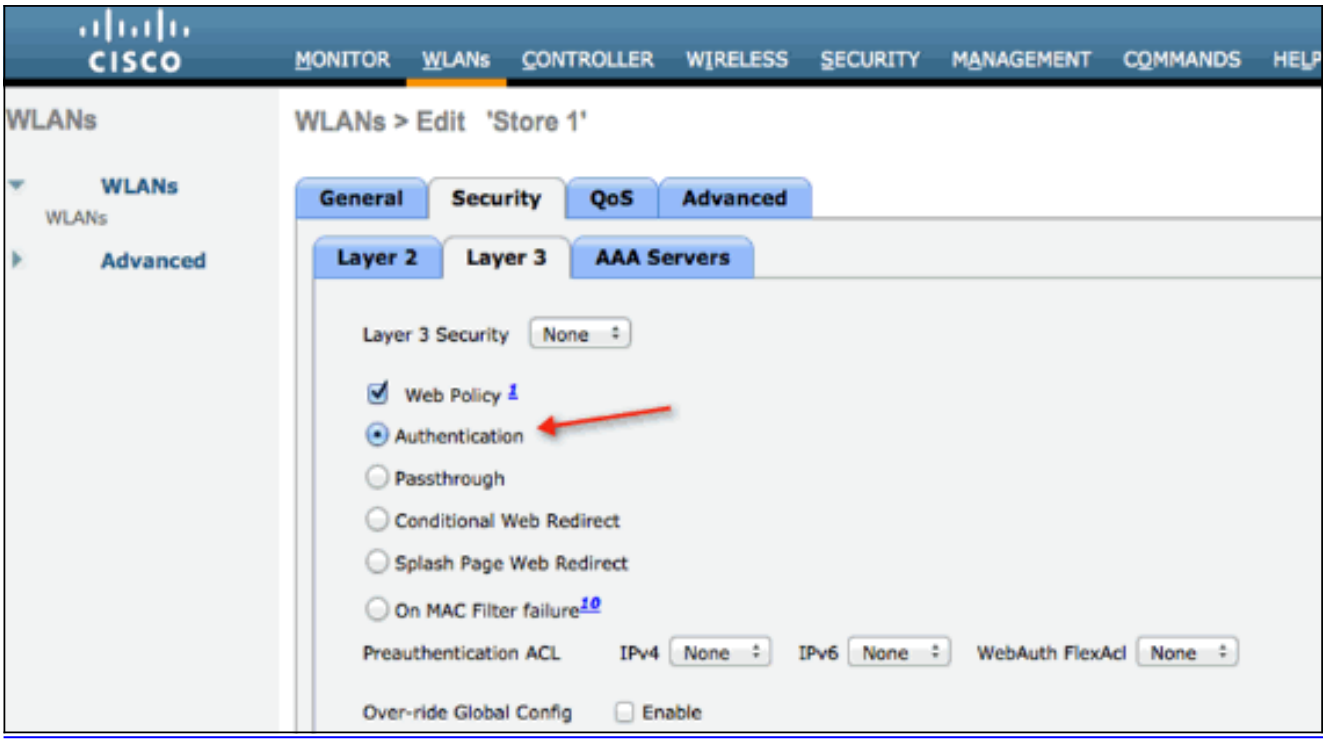
Procédure :

Terminez-vous ces étapes afin de configurer cette caractéristique :

1. Configurez un WLAN pour la commutation locale de FlexConnect.



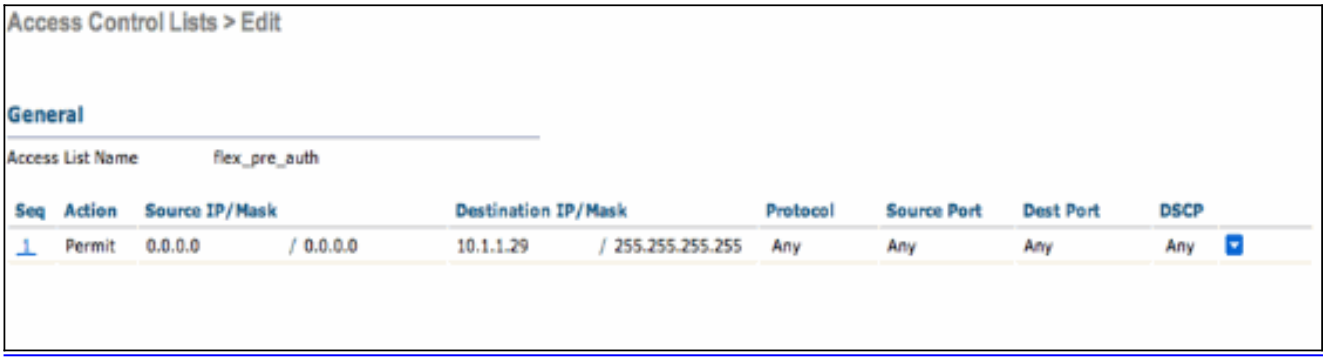
2. Afin d'activer l'authentification de Web externe, vous devez configurer la stratégie de Web comme stratégie de sécurité pour le WLAN localement commuté. Ceci inclut une de ces quatre options :AuthentificationIntercommunicationLe Web conditionnel réoriententLe Web de page de splash réoriententCaptures de ce document un exemple pour l'authentification Web
:



Les deux premières méthodes sont semblables et peuvent être groupées comme méthodes d'authentification Web d'un point de vue de configuration. Les deux deuxièmes (conditionnel réorientez et page de splash) sont des stratégies de Web et peuvent être groupés comme méthodes de Web-stratégie.

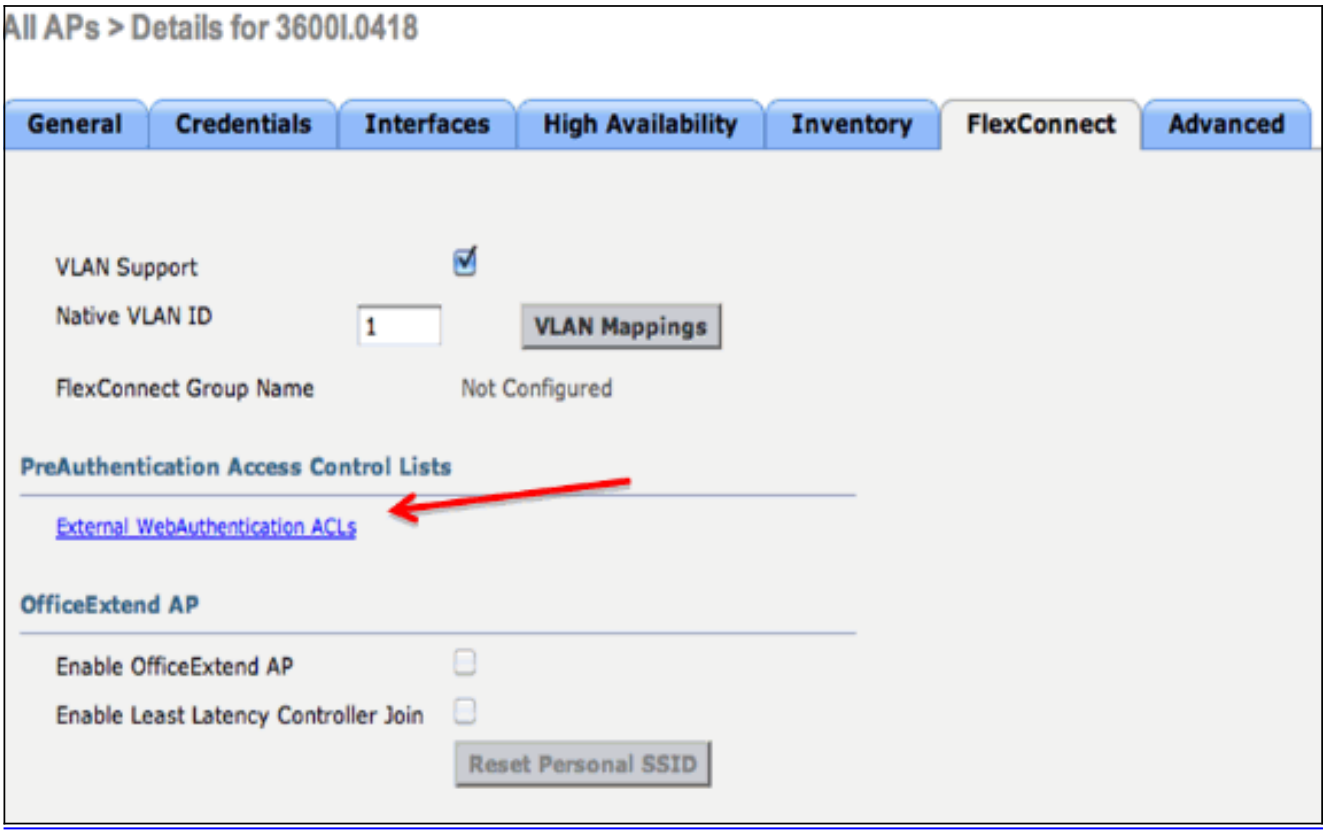
3. L'ACL de FlexConnect de Pré-authentification doit être configuré permettant aux clients sans fil pour atteindre l'adresse IP du serveur externe. L'ARP, le DHCP et le trafic DNS sont automatiquement permis et n'ont pas besoin d'être spécifiés. Sous la Sécurité > la liste de contrôle d'accès, choisissez **FlexConnect ACLs**. Puis, cliquez sur Add et définissez les noms et les règles comme ACL de contrôleur de

normale.

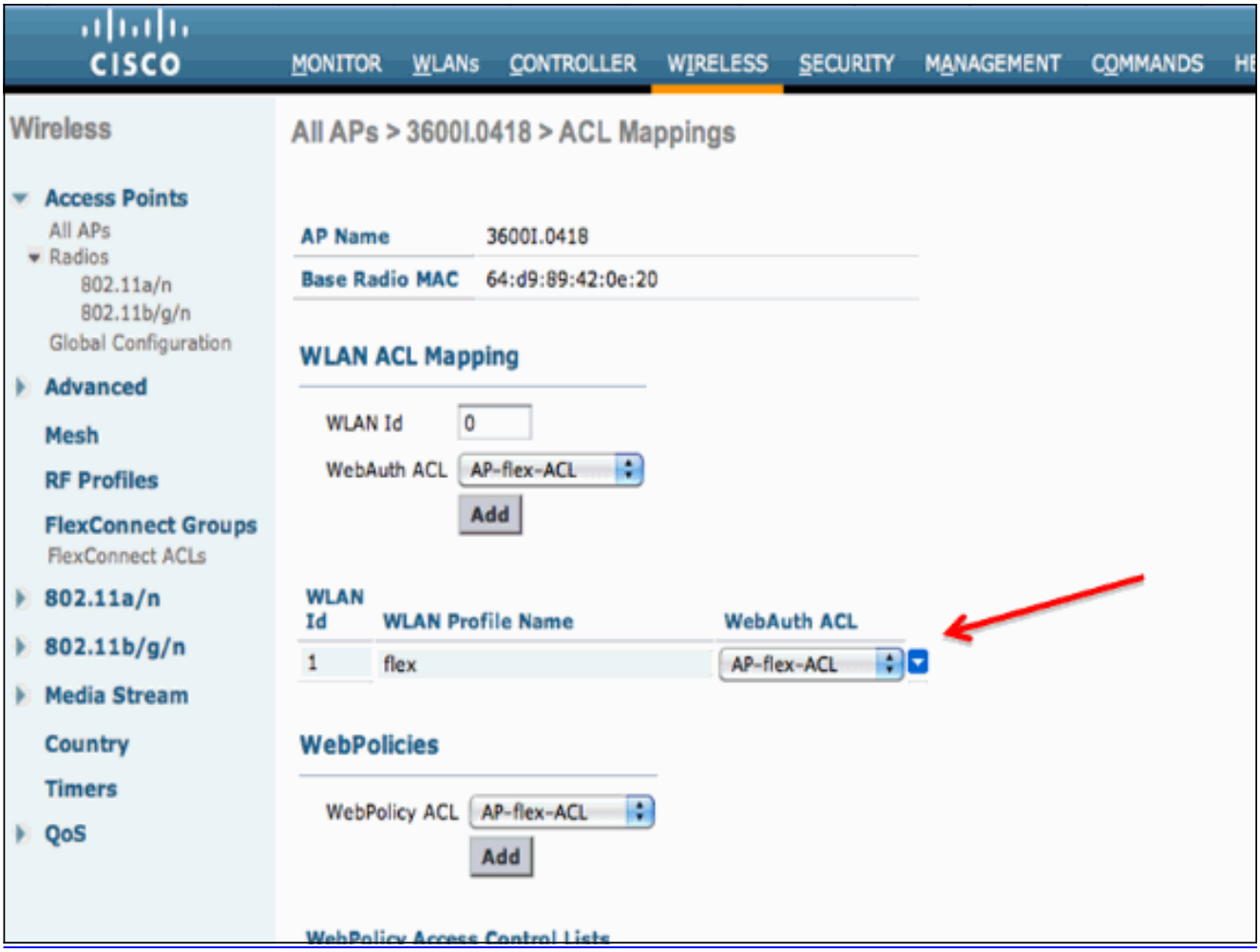


Remarque: Vous devrez créer des règles inverses pour le trafic chaque fois.

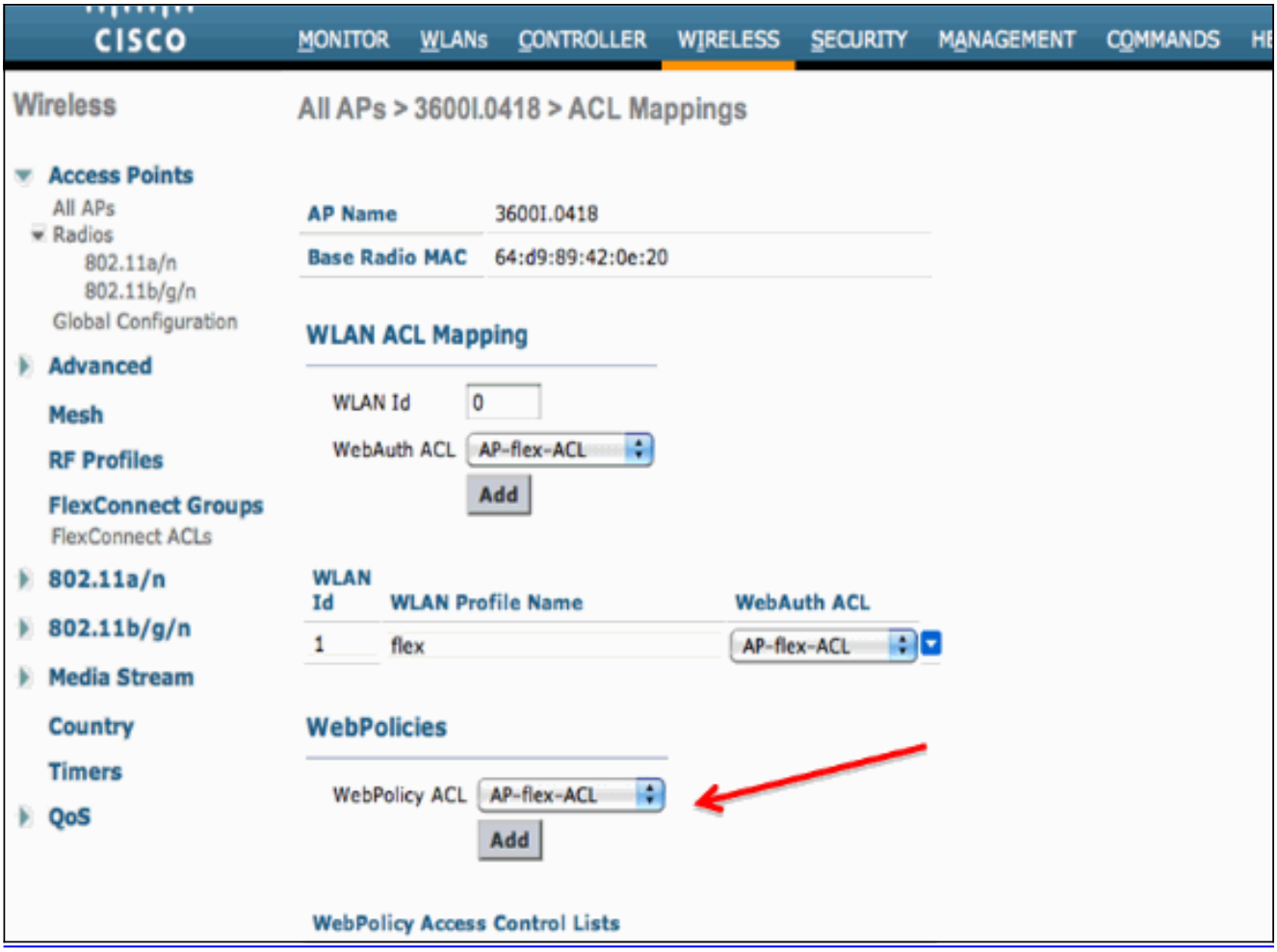
4. Une fois que FlexConnect ACLs sont créés il devrait être appliqué qui peut être fait aux différents niveaux : AP, groupe de FlexConnect et WLAN. Cette dernière option (ACL de flexible au WLAN) est seulement pour l'authentification Web et l'intercommunication de Web pour deux autres méthodes dans le cadre de stratégie de Web, telle que conditionnel et le splash réorientent. ACLs peut seulement être appliqué à AP ou fléchir le groupe. Voici un exemple d'un ACL assigné au niveau AP. Allez à la **radio > AP choisi**, puis cliquez sur l'onglet de **FlexConnect**
:



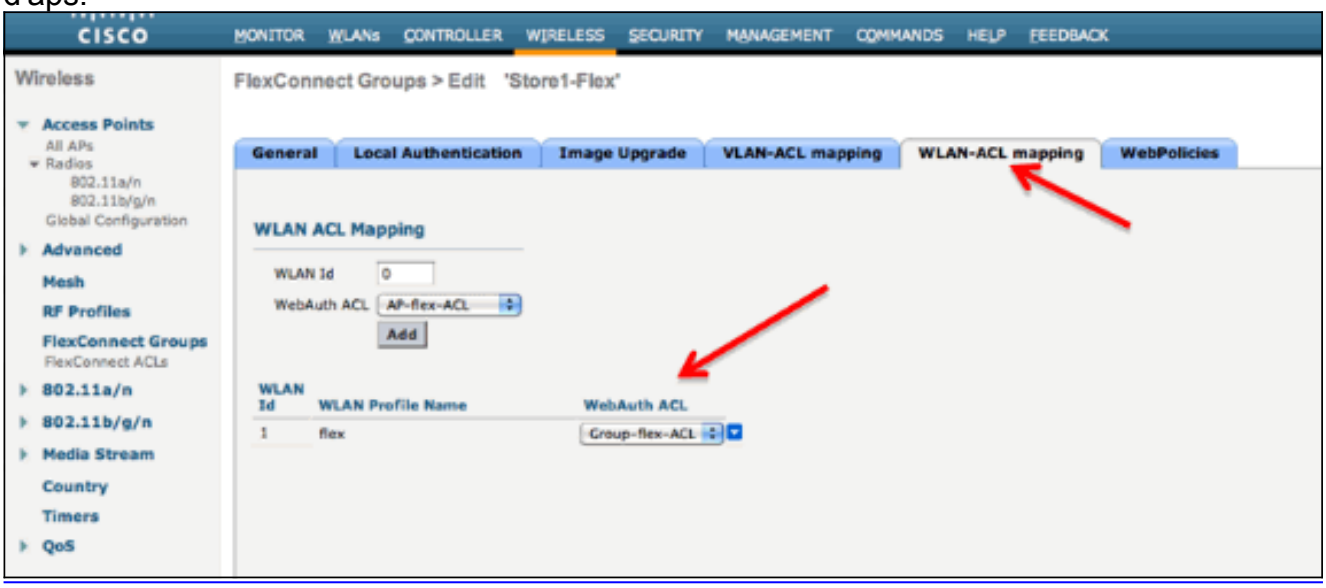
Cliquez sur le lien **externe de WebAuthentication ACLs**. Puis, choisissez l'ACL pour l'id particulier WLAN
:



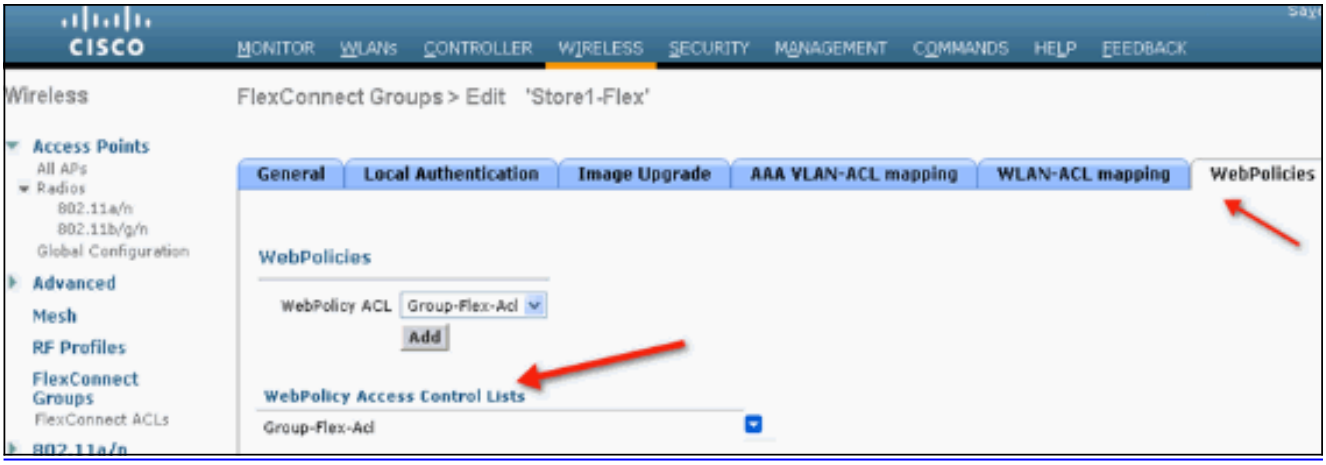
De même, pour l'ACL de stratégie de Web (par exemple, les conditionnels réorientent ou la page de splash réorientent), vous recevrez une option de sélectionner le flexible connectez l'ACL sous WebPolicies après que vous cliquiez sur le même lien externe de WebAuthentication ACLs. Ceci est affiché ici
:



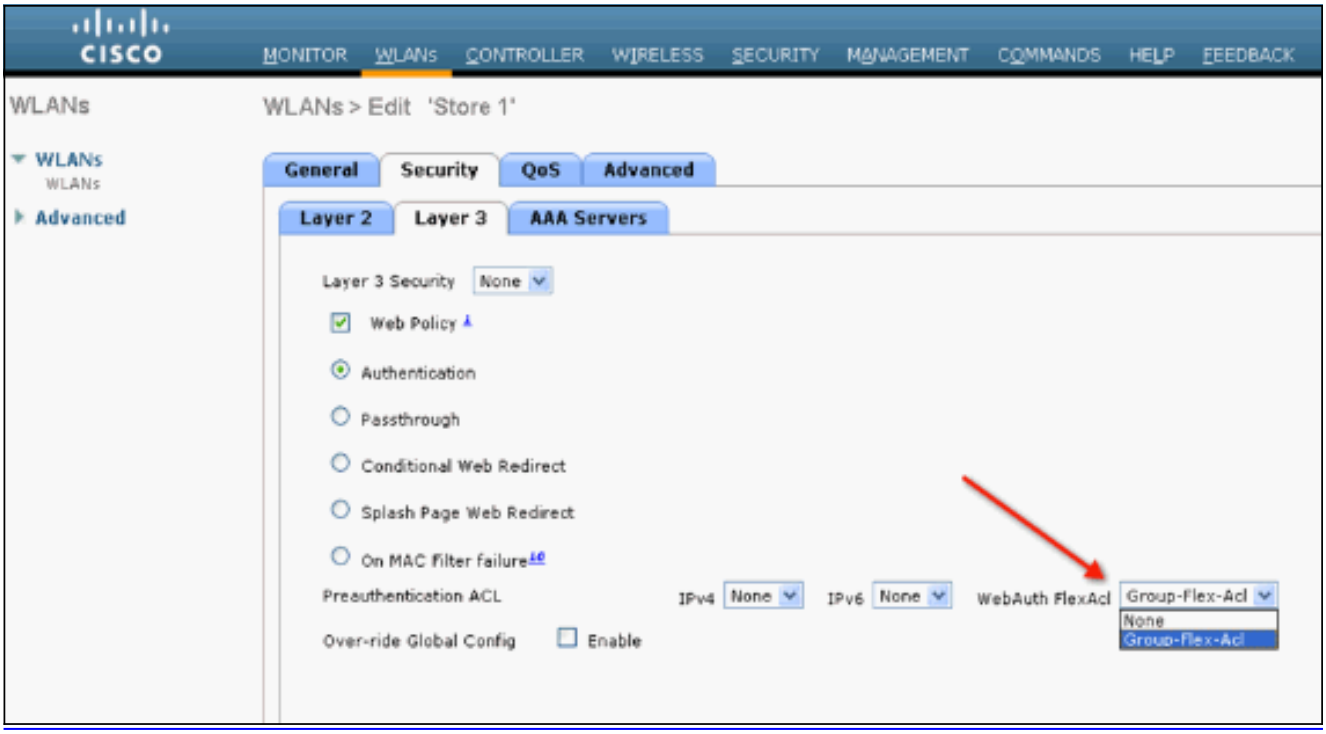
5. L'ACL peut également être appliqué au niveau du groupe de FlexConnect. Afin de faire ceci, allez à l'onglet de **mappage WLAN-ACL** dans la configuration de groupe de FlexConnect. Puis, choisissez l'id WLAN et l'ACL que vous voulez s'appliquer. Cliquez sur **Add**. C'est utile quand vous voulez définir un ACL pour un groupe d'aps.



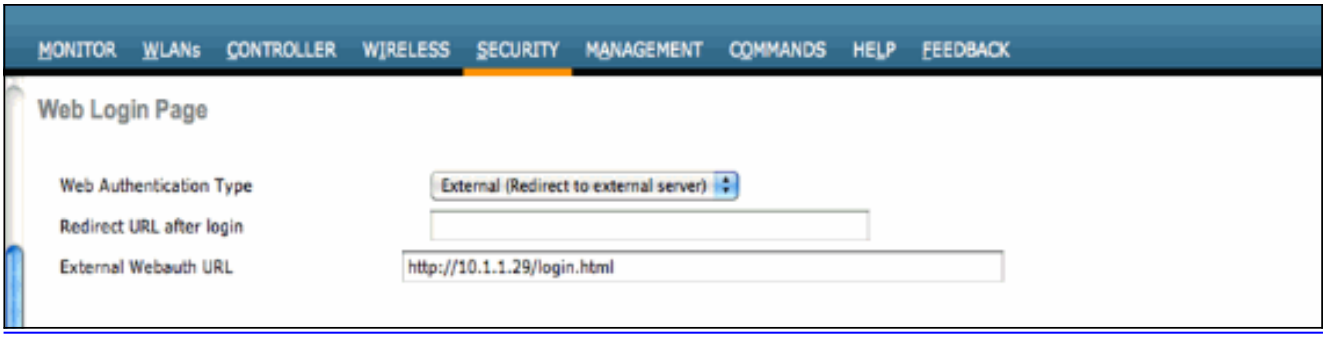
De même, parce que l'ACL de stratégie de Web (pour le Web conditionnel et de splash de page réorientez), vous devez sélectionner l'onglet de **WebPolicies**.



6. Le flexible ACLs d'authentification Web et d'intercommunication de Web peut également être appliqué sur le WLAN. Afin de faire ceci, choisissez l'ACL du déroulant de **WebAuth FlexACL** sous l'onglet de la couche 3 dans WLAN > Sécurité.



7. Pour l'authentification de Web externe, l'URL de réorientation doit être défini. Ceci peut être fait à un niveau global ou au niveau WLAN. Pour le niveau WLAN, cliquez sur le coche de **configuration globale de priorité** et insérez l'URL. Au niveau global, allez à la **Sécurité > au Web authentiques > page Web Login** :



Limites :L'authentification Web (interne ou à un serveur externe) exige du flexible AP d'être en mode connecté. L'authentification Web n'est pas prise en charge si le flexible AP est en mode autonome.L'authentification Web (interne ou à un serveur externe) est seulement 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 exécuter l'authentification Web.Toute la redirection de Web est exécutée au WLC et pas au niveau AP.

Informations connexes

- Support et documentation techniques - Cisco Systems