Externe webverificatie met FlexConnect Local Switching Deployment Guide

Inhoud

Inleiding

Dit document legt uit hoe u een externe webserver kunt gebruiken met FlexConnect Local Switching voor verschillende beleidsmaatregelen van het Web.

Voorwaarden

Vereisten

Zorg ervoor dat u aan deze vereisten voldoet voordat u deze configuratie probeert:

- Basiskennis van FlexConnect Architecture en Access Point (AP's)
- Kennis over het instellen en configureren van een externe webserver
- Kennis over het instellen en configureren van DHCP- en DNS-servers

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco 7500 draadloze LAN-controller (WLC) met firmware release 7.2.10.0
- Cisco 3500 Series lichtgewicht access point (LAP)
- Externe webserver waarop de logpagina voor de webverificatie wordt opgeslagen
- DNS en DHCP-servers op lokale site voor adresoplossing en IP-adrestoewijzing voor draadloze clients

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Hoewel een WLC van 7500 Series voor deze implementatiehandleiding wordt gebruikt, wordt deze functie ondersteund op WLC's van 2500, 5500 en WiSM-2. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Overzicht van functies

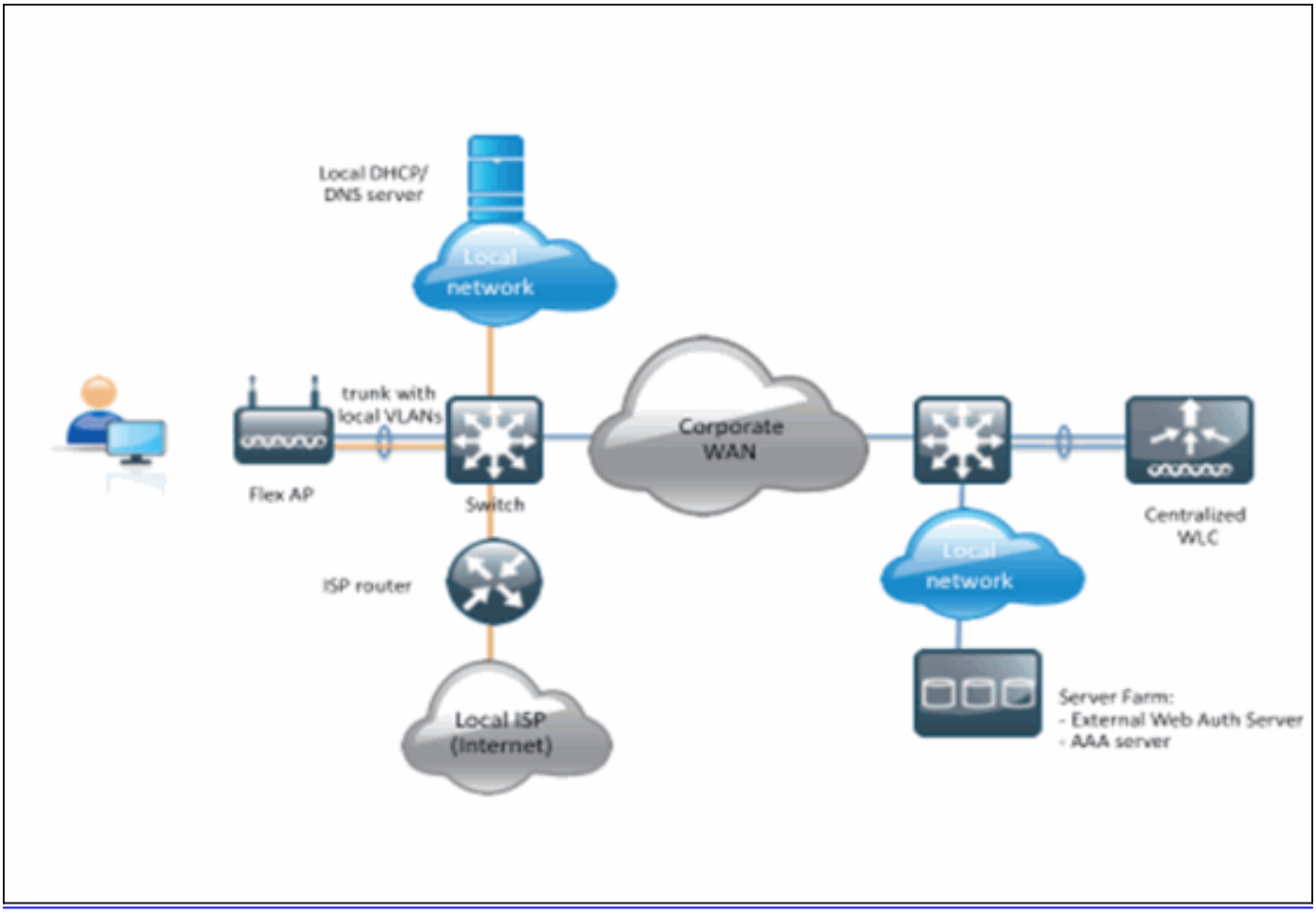
Deze functie breidt de mogelijkheid van het uitvoeren van Web Verificatie uit naar een externe webserver van AP in FlexConnect modus, voor de WLAN's met lokaal geschakeld verkeer (FlexConnect - Local Switching). Vóór WLC release 7.2.10.0 werd de webverificatie naar een externe server ondersteund voor AP's in lokale modus of FlexConnect-modus voor WLAN's met centraal switched verkeer (FlexConnect - Central Switching).

Deze functie, die vaak wordt aangeduid als Externe Webverificatie, breidt de mogelijkheid voor FlexConnect Local Switching WLAN uit om alle Layer 3 Web Redirect Security typen te ondersteunen die momenteel worden geleverd door de controller:

- Web verificatie
- Web Pass-Through
- Web voorwaardelijke omleiding
- plash-pagina conditionering voor omleiding

Gezien een WLAN-configuratie voor Web-verificatie en voor lokale switching, is de logica achter deze functie gelegen in het direct distribueren en toepassen van de Pre-Authentication FlexConnect Access Control List (ACL) op het AP-niveau in plaats van op het WLC-niveau. Op deze manier zal AP de pakketten van de draadloze client die door ACL, lokaal worden toegestaan veranderen. De niet toegestane pakketten worden nog steeds via de CAPWAP-tunnel naar de WLC verzonden. Aan de andere kant, wanneer AP het verkeer over de bekabelde interface ontvangt, indien toegestaan door ACL, zal het aan de draadloze client door sturen. Anders wordt het pakje ingetrokken. Zodra de client is geauthentiseerd en geautoriseerd, wordt Pre-Verificatie FlexConnect ACL verwijderd en wordt al het clientgegevensverkeer lokaal toegestaan en ingeschakeld.

Opmerking: Deze optie werkt onder de veronderstelling dat de client de externe server vanaf het lokaal geschakelde VLAN kan bereiken.



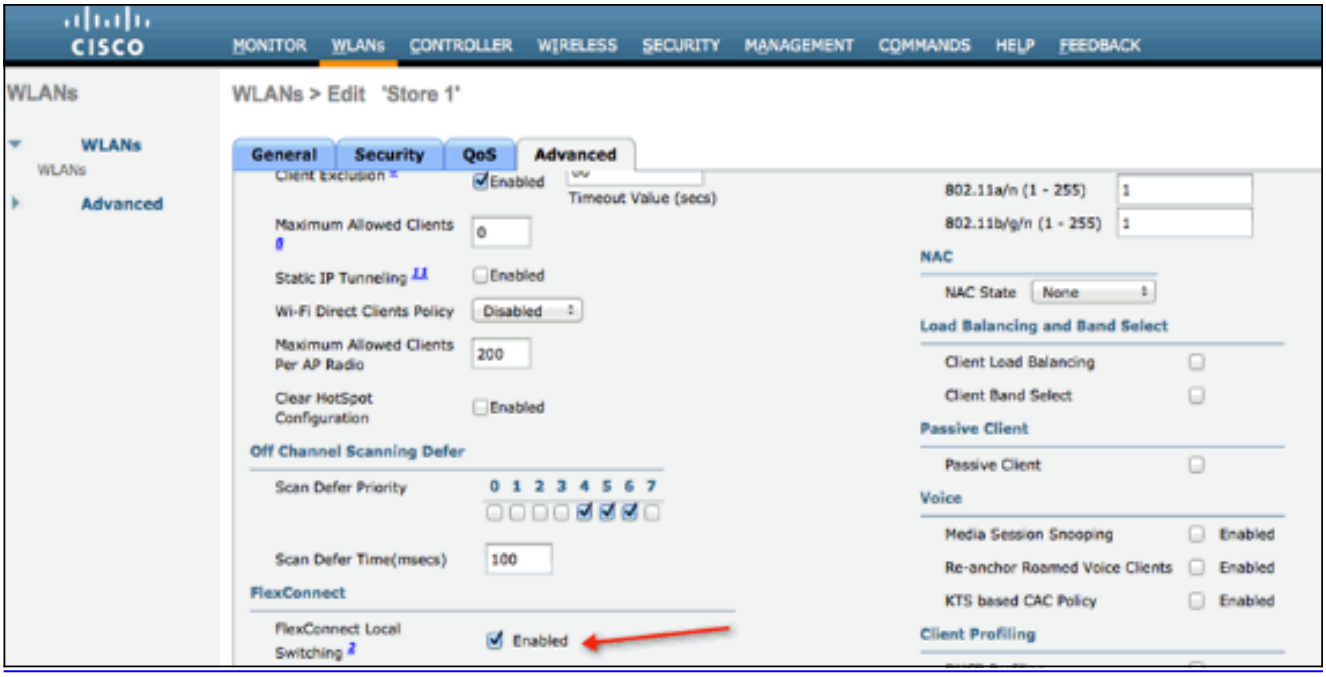
Samenvatting:

- WLAN's ingesteld voor FlexConnect Local Switching en L3 Security
- FlexConnect ACL's worden gebruikt als Pre-ACL's
- FlexConnect ACL's moeten eenmaal geconfigureerd naar de AP-database worden geduwd via Flex-groep of via afzonderlijke AP, of kunnen worden toegepast op WLAN
- AP staat al het verkeer toe dat met Pre-Verificatie ACL overeenkomt om lokaal te worden geschakeld

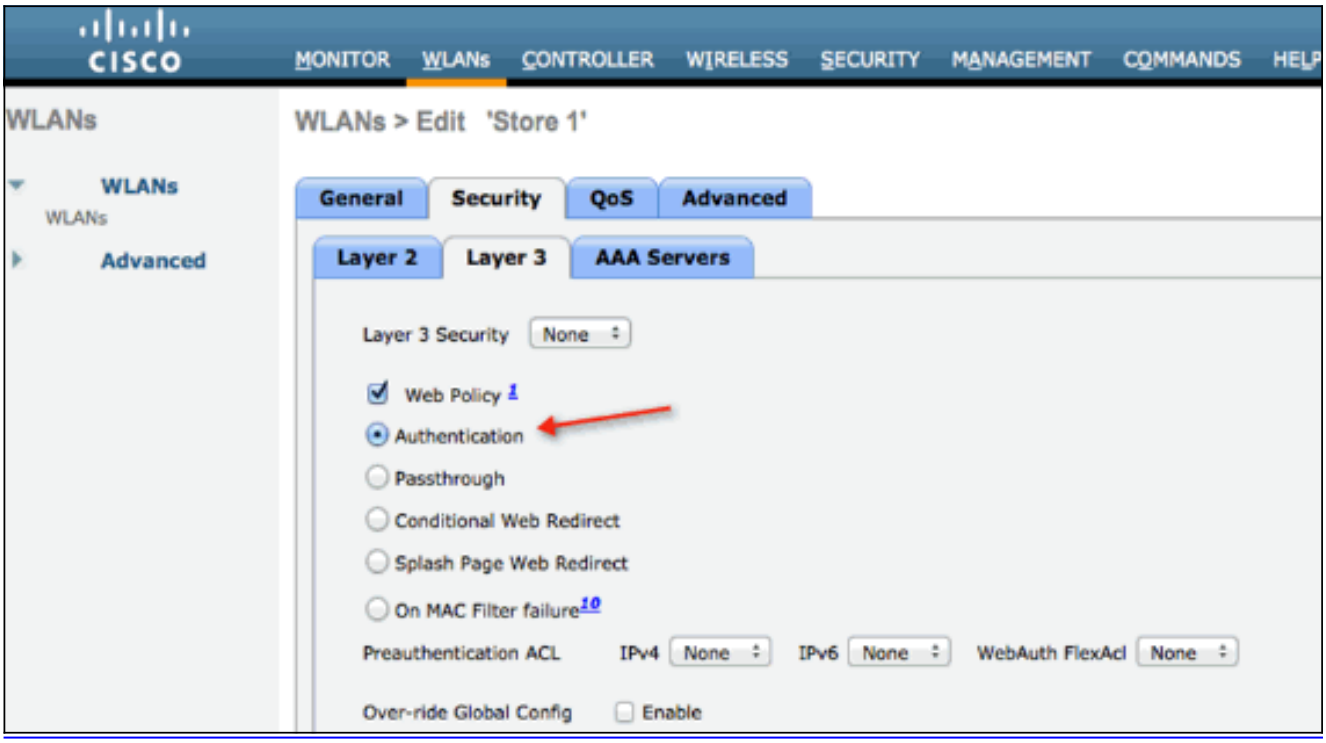
Procedure: Initiatief

Volg deze stappen om deze functie te configureren:

1. Configureer een WLAN voor FlexConnect lokale switching.

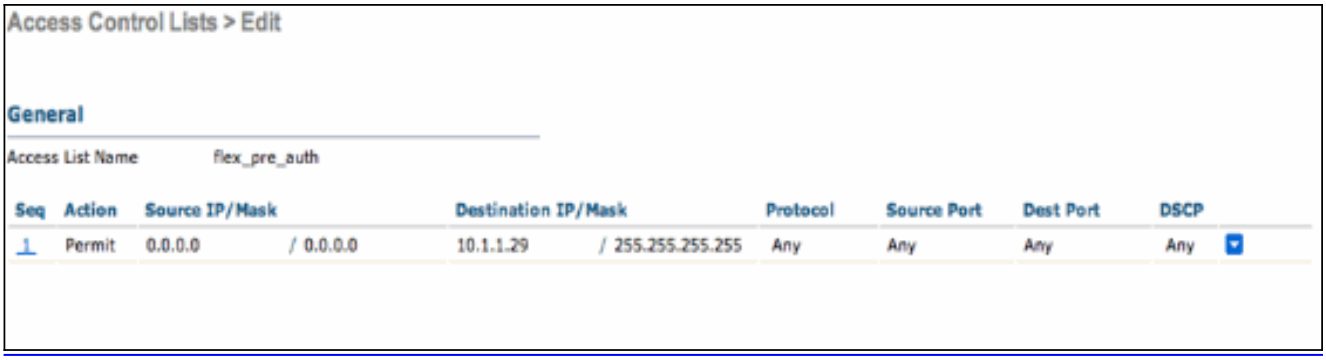


2. Om Externe Web Verificatie mogelijk te maken, moet u Web Policy configureren als het beveiligingsbeleid voor de lokaal switched WLAN. Dit omvat één van deze vier opties:VerificatieDoorlopenVoorwaardelijk web redirectspaander pagina Web redirectDit document neemt een voorbeeld voor webverificatie:



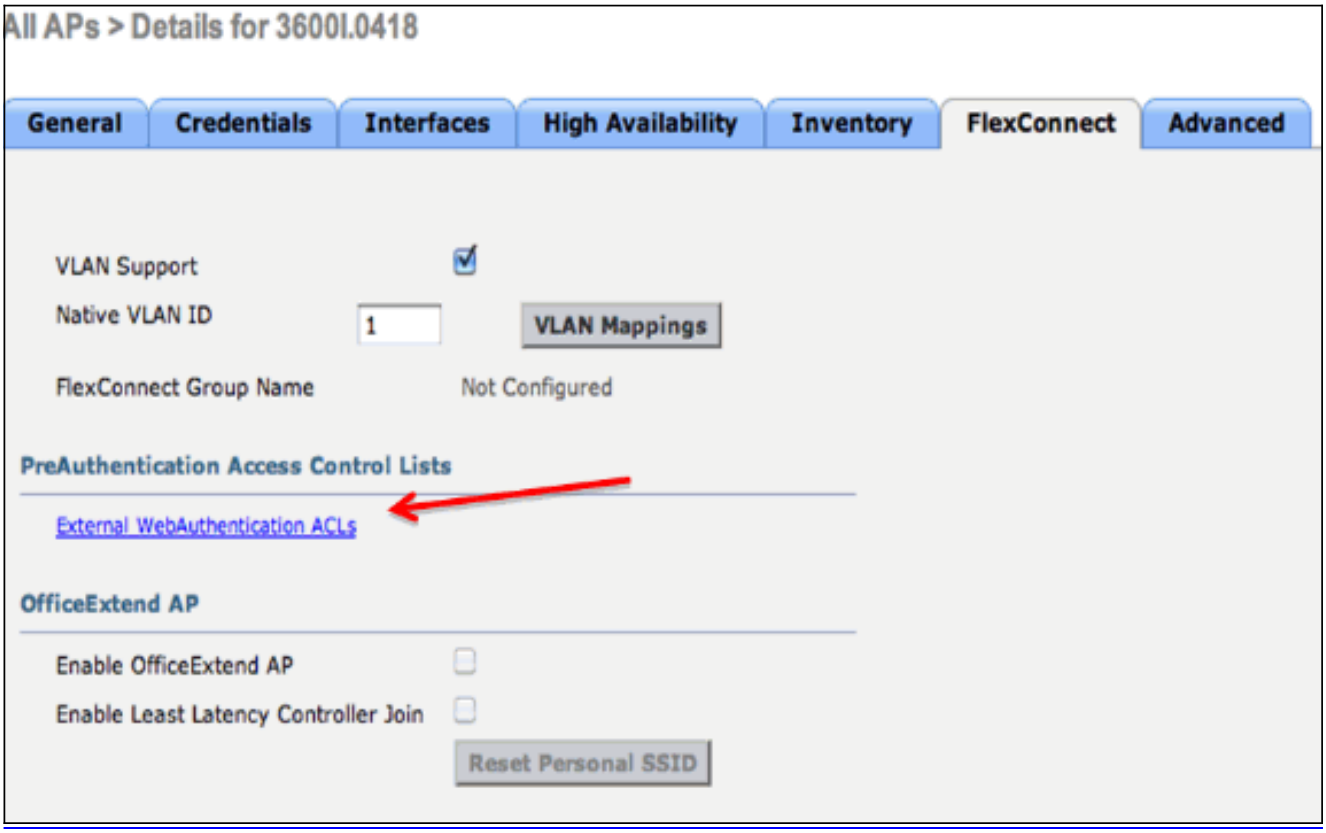
De eerste twee methoden zijn vergelijkbaar en kunnen worden gegroepeerd als Web-Verificatiemethoden uit een oogpunt van configuratie. De tweede twee (Conditional Redirect and Splash Page) zijn beleid op het web en kunnen worden gegroepeerd in Web-Policy methoden.

3. De Pre-Authentication FlexConnect ACL moet worden geconfigureerd zodat de draadloze client het IP-adres van de externe server kan bereiken. ARP-, DHCP- en DNS-verkeer is automatisch toegestaan en hoeft niet te worden gespecificeerd. Kies onder Security > Access Control List **FlexConnect ACL's**. Klik vervolgens op **Add** en definieer de namen en regels als een normale controller op ACL.

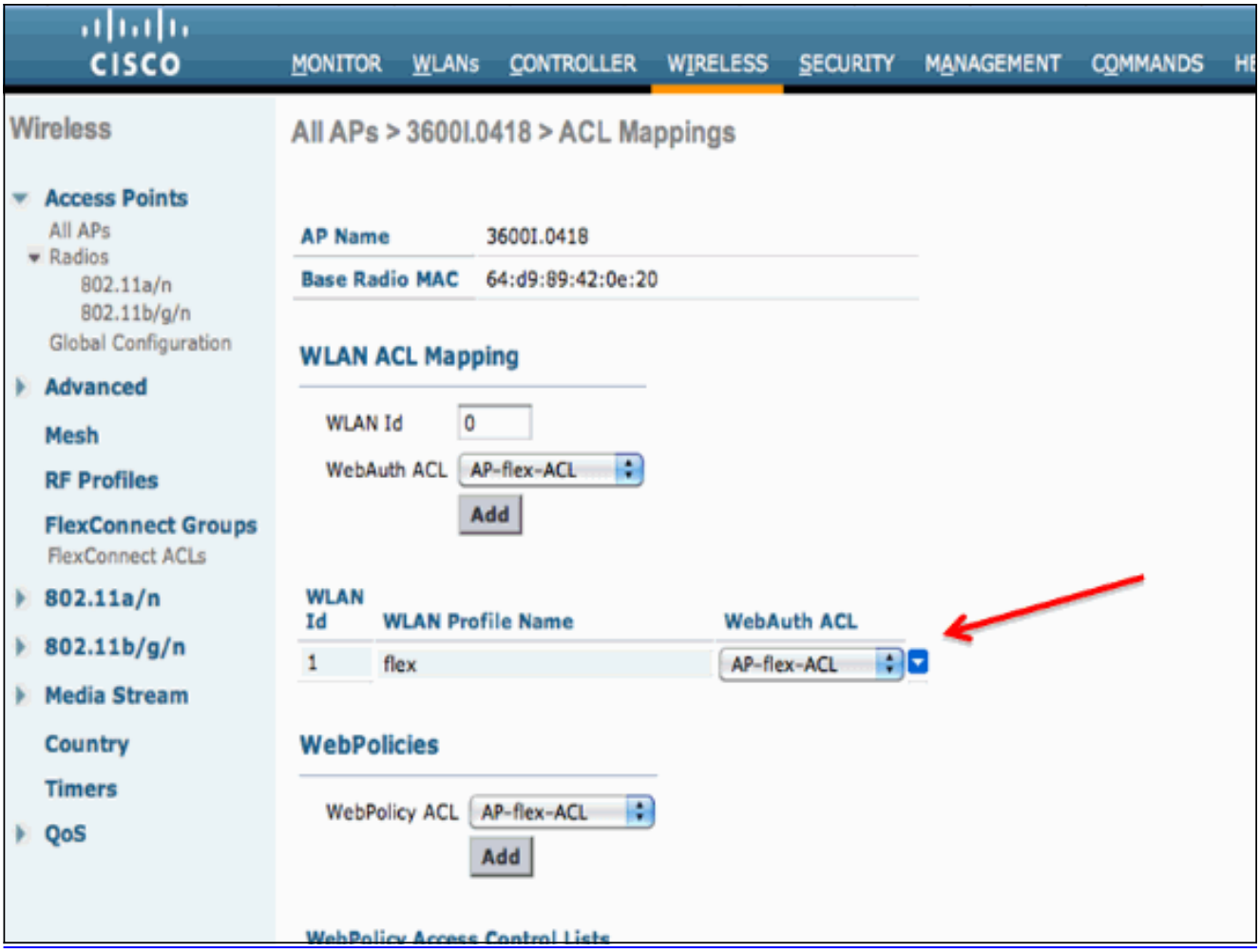


Opmerking: U moet telkens regels voor het verkeer omkeren.

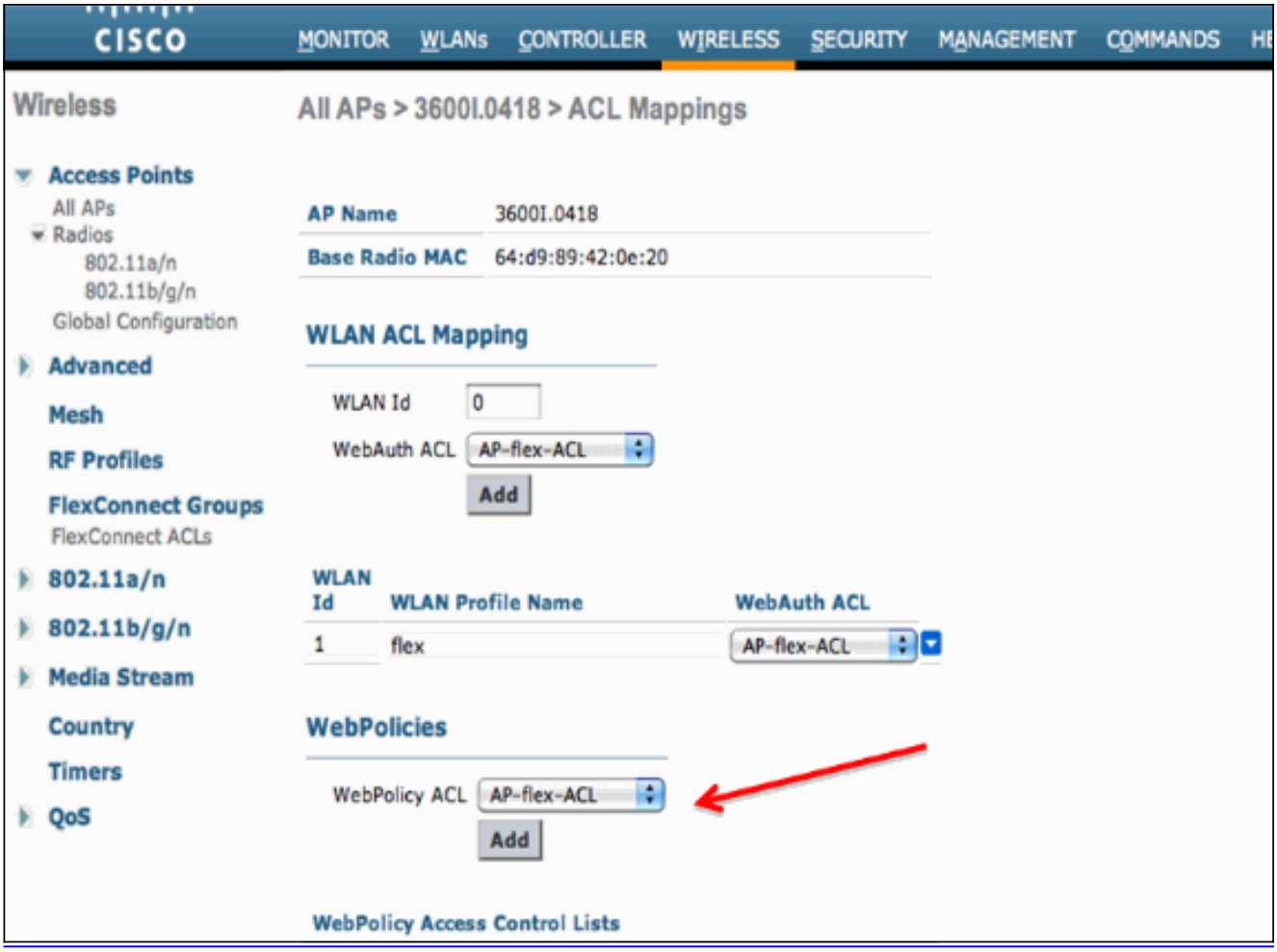
4. Zodra FlexConnect ACL's zijn gecreëerd, moet deze worden toegepast, wat op verschillende niveaus kan worden gedaan: AP, FlexConnect Group en WLAN. Deze laatste optie (Flex ACL bij WLAN) is alleen voor Web Verificatie en Web Pass-Through voor andere twee methoden onder Web Policy, zoals Conditional en Splash Redirect. ACL's kunnen alleen worden toegepast op AP of Flex Group. Hier is een voorbeeld van een ACL die op het niveau van AP wordt toegewezen. Ga naar **Draadloos > selecteer AP** en klik vervolgens op het **FlexConnect**
tabblad:



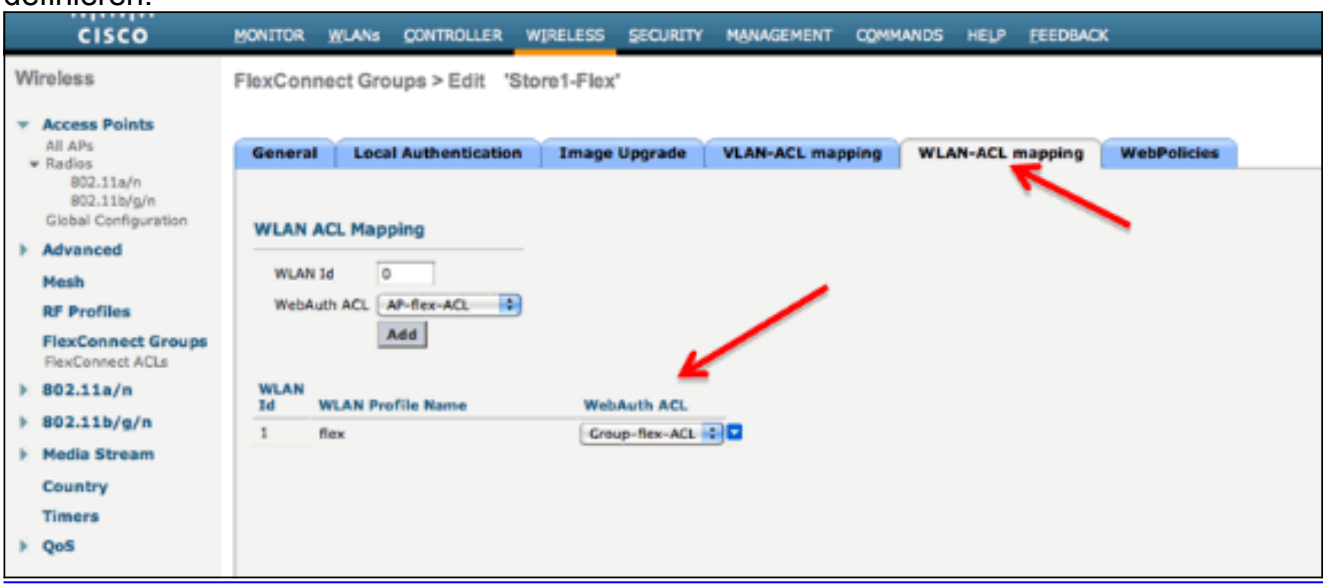
Klik op de link **Externe WebVerificatie ACL's**. Kies vervolgens de ACL voor de bepaalde WLAN-
id:



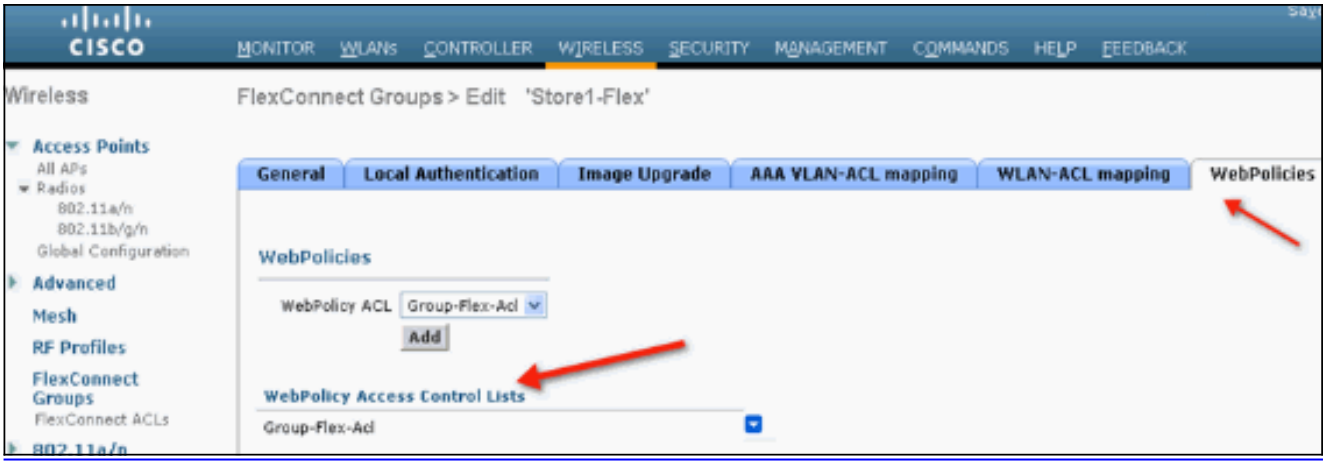
Op dezelfde manier zal u voor Web Policy ACL (bijvoorbeeld de voorwaardelijke omleiding of spaanpagina omleiding) een optie ontvangen om Flex Connect ACL onder WebPolicy te selecteren nadat u op dezelfde externe link van WebVerificatie ACL's klikt. Dit wordt hier getoond:



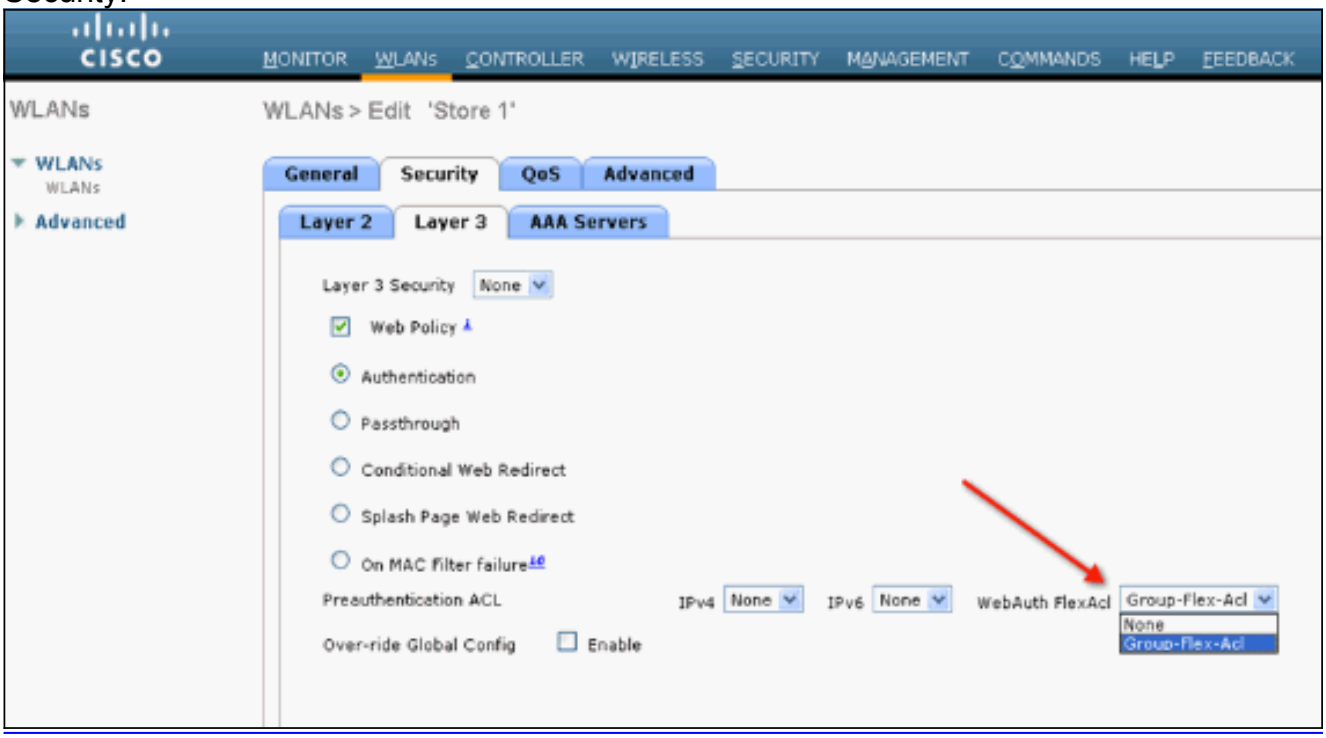
5. ACL kan ook op het niveau van FlexConnect worden toegepast. Ga om dit te doen naar het tabblad **WLAN-ACL-**mapping in de configuratie van de FlexConnect-groep. Kies vervolgens de WLAN-id en de ACL die u wilt toepassen. Klik op **Toevoegen**. Dit is nuttig wanneer u ACL voor een groep APs wilt definiëren.



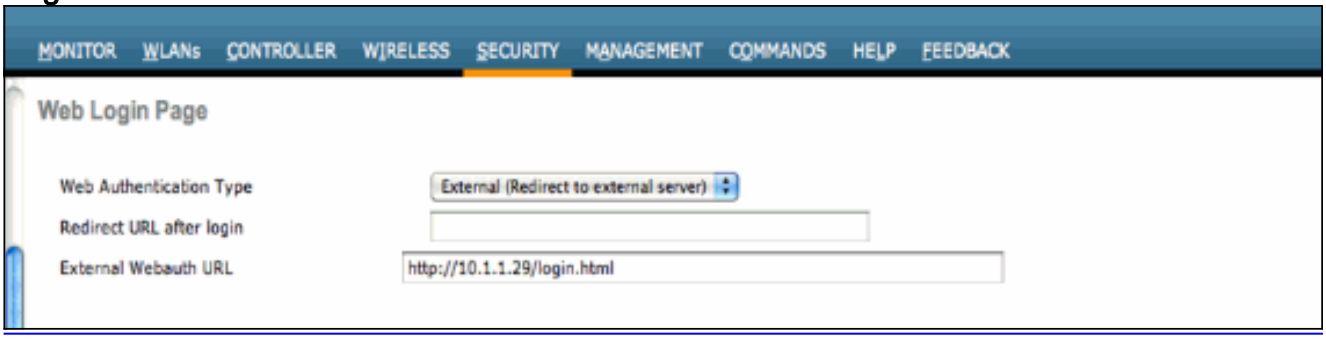
Op dezelfde manier moet u voor Web Policy ACL (voor voorwaardelijke en tijdelijke Web Redirect van de Pagina) het tabblad **Webebeleid** selecteren.



6. Web verificatie en Web Pass-Through Flex ACL's kunnen ook op het WLAN worden toegepast. Om dit te doen, kies ACL van de vervolgkeuzelijst **WebexACL** onder het tabblad Layer 3 in WLAN > Security.



7. Voor externe webverificatie moet de URL worden gedefinieerd. Dit kan worden gedaan op mondiaal niveau of op het WLAN-niveau. Klik voor het WLAN-niveau op het selectieteken van de **over-ride Global Config** en voer de URL in. Op mondiaal niveau gaat u naar **Security > Web Auth > Web Login Page**:



Beperkingen: Web verificatie (intern of op een externe server) vereist dat Flex AP in Connected Mode is. Web verificatie wordt niet ondersteund als Flex AP in Standalone modus is.Web verificatie (intern of naar een externe server) wordt alleen ondersteund door Central

Verificatie. Als een WLAN-instelling voor lokale switching is geconfigureerd voor lokale verificatie, kunt u geen Web-verificatie uitvoeren.Alle webomleiding wordt uitgevoerd op WLC en niet op AP-niveau.

Gerelateerde informatie

- Technische ondersteuning en documentatie – Cisco Systems