外部Web验证用FlexConnect本地交换部署指南

目录

简介

本文解释如何以FlexConnect本地交换使用外部Web服务器不同的Web策略。

先决条件

要求

尝试进行此配置之前，请确保满足以下要求：

- 关于FlexConnect体系结构和接入点(AP)的基础知识
- 有关如何设置和配置外部 Web 服务器的知识
- 有关如何设置和配置 DHCP 和 DNS 服务器的知识

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco 7500该无线局域网的控制器(WLC)运行固件版本7.2.110.0
- Cisco 3500系列轻量级接入点(LAP)
- 托管 Web 身份验证登录页面的外部 Web 服务器
- 在本地站点的DNS和对无线客户端的DHCP服务器地址解析的和IP地址分配

本文档中的信息都是基于特定实验室环境中的设备编写的。虽然一7500系列WLC使用此部署指南，2500， 5500和WiSM-2 WLCs支持此功能。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

功能概述

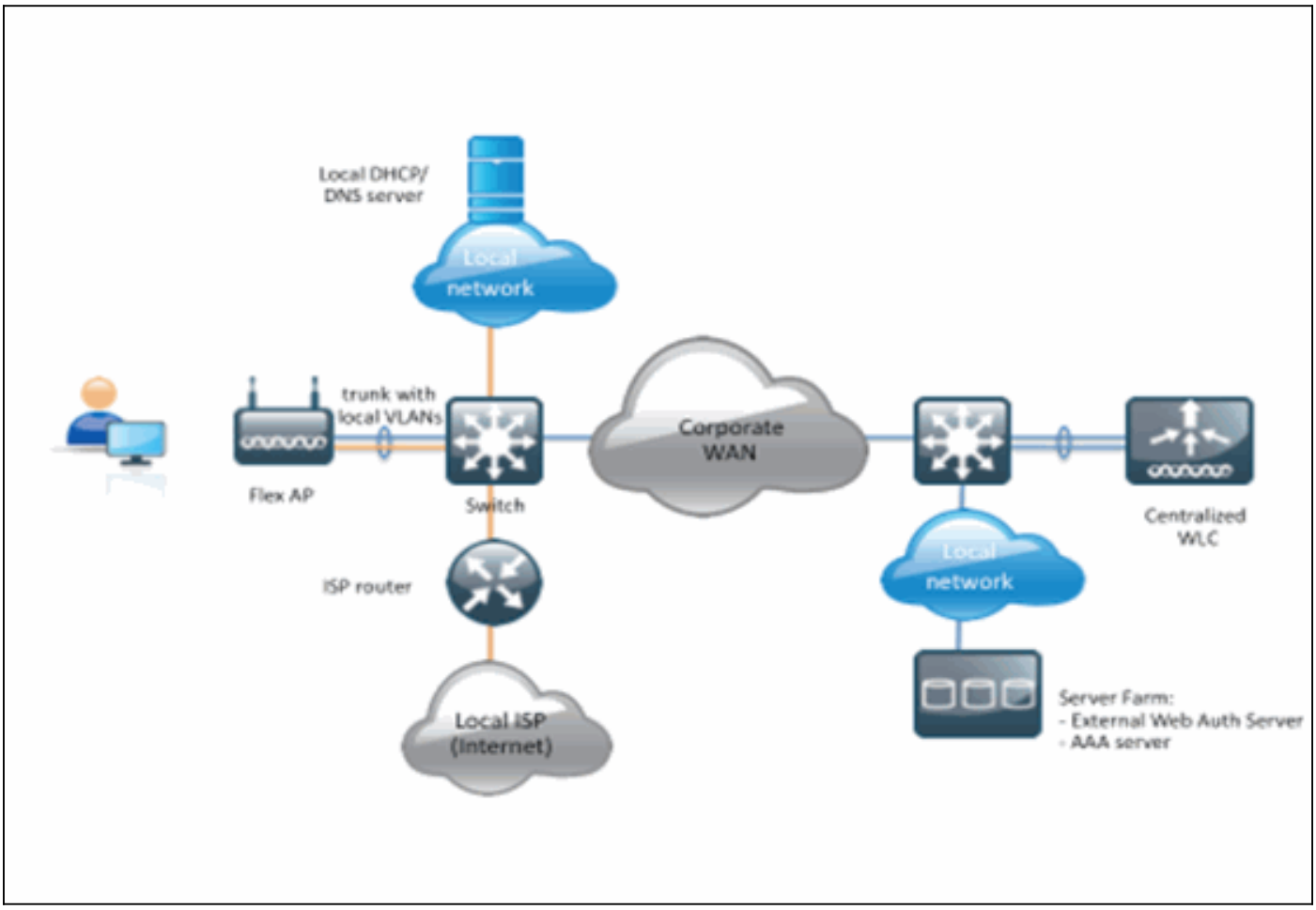
此功能对从AP的一外部Web服务器扩大执行的Web验证的功能在FlexConnect模式，与本地交换数据流(FlexConnect的WLAN的–本地交换)。在WLC版本7.2.110.0，对外部服务器的Web验证为在本地传送方式或FlexConnect模式的AP在中央支持与交换数据流前(FlexConnect的WLAN的–中央交换)。

通常指外部Web验证，此功能扩大FlexConnect本地交换WLAN的功能能支持控制器当前提供的所有第3层Web重定向安全类型：

- Web 身份验证
- Web转接
- Web有条件的重定向
- 飞溅页有条件的重定向

就为本地交换配置的为Web验证和WLAN而论，在此功能后的逻辑是分配和应用预验证FlexConnect访问控制表(ACL)直接地在AP级别而不是级的WLC。这样， AP将转换由ACL允许来自无线客户端的数据包，本地。没允许的数据包在CAPWAP通道仍然被发送对WLC。另一方面，当AP收到流量经过有线的接口，如果允许由ACL，将转发它给无线客户端。否则，将丢弃该数据包。一旦客户端验证并且授权，预验证FlexConnect ACL删除，并且所有客户端数据数据量允许并且交换本地。

注意： 以为客户端能到达从本地交换VLAN的外部服务器此功能运作。



摘要：

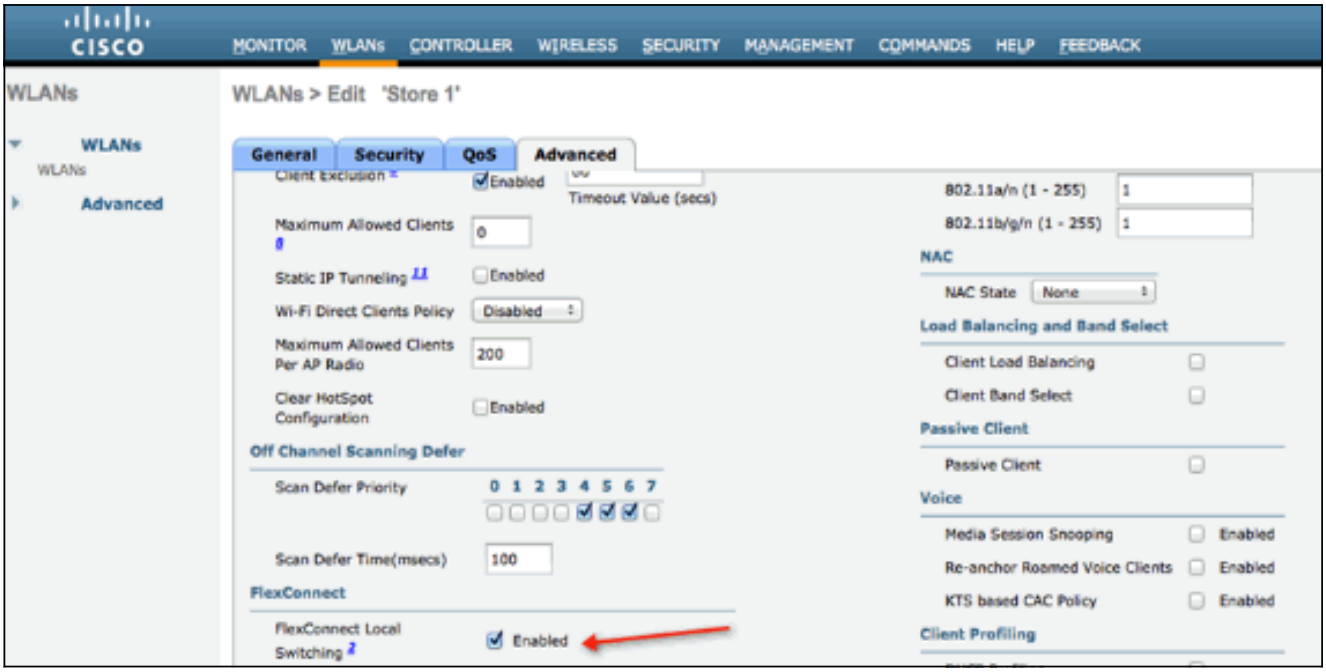
- 为FlexConnect本地交换和L3安全配置的WLAN

- FlexConnect ACL将使用作为预验证ACL
- 在WLAN必须推送一次配置的FlexConnect ACL到AP数据库通过弹性组或通过个人AP或者可以应用
- AP允许匹配将交换的预验证ACL本地的所有流量

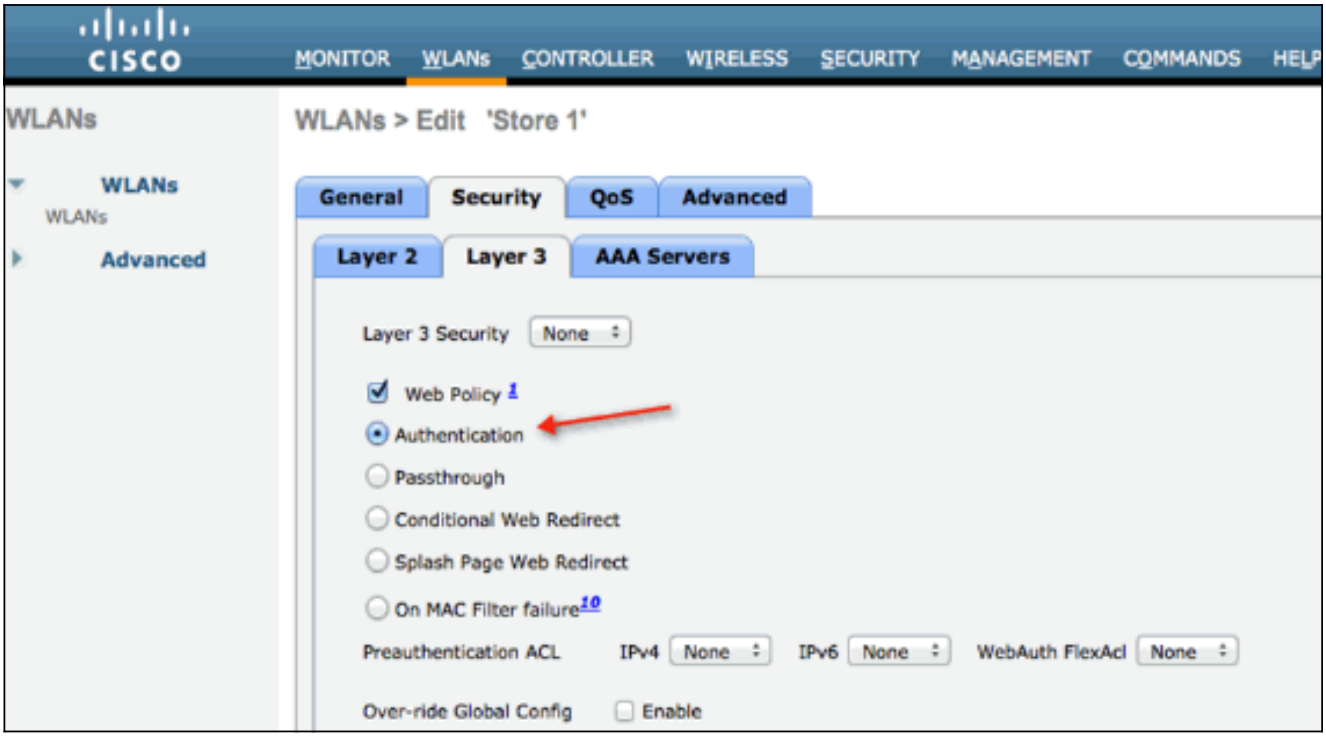
步骤：

完成这些步骤为了配置此功能：

1. 配置FlexConnect本地交换的一WLAN。



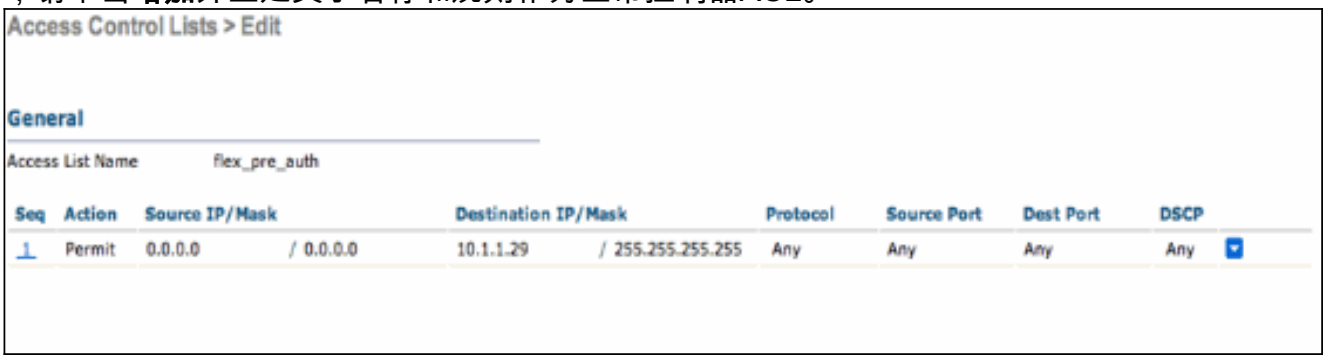
2. 为了启用外部Web验证，您需要配置Web策略作为本地交换的WLAN的安全策略。这包括这四个选项之一：验证转接有条件的Web重定向飞溅页Web重定向此文件收集Web验证的一示例：



前两个方法是类似的，并且可以分组作为Web验证方法从配置观点。第二两个(有条件的重定向和飞溅页)是Web策略，并且可以分组作为Web策略方法。

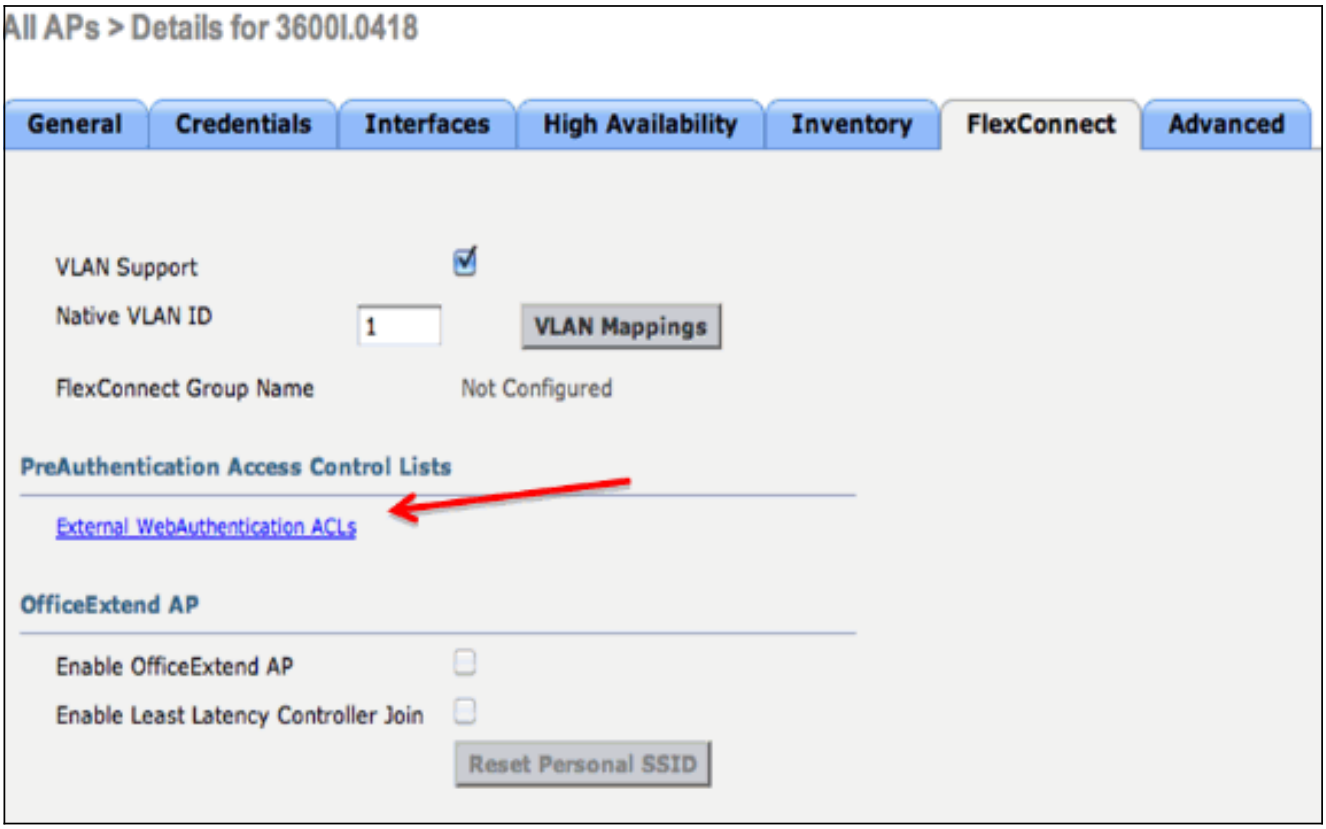
3. 预验证FlexConnect ACL需要配置允许无线客户端到达外部服务器的IP地址。ARP、DHCP和

DNS流量自动地允许和不需要指定。在安全下>访问控制表，请选择**FlexConnect ACL**。然后，请单击**增加**并且定义了名称和规则作为正常控制器ACL。

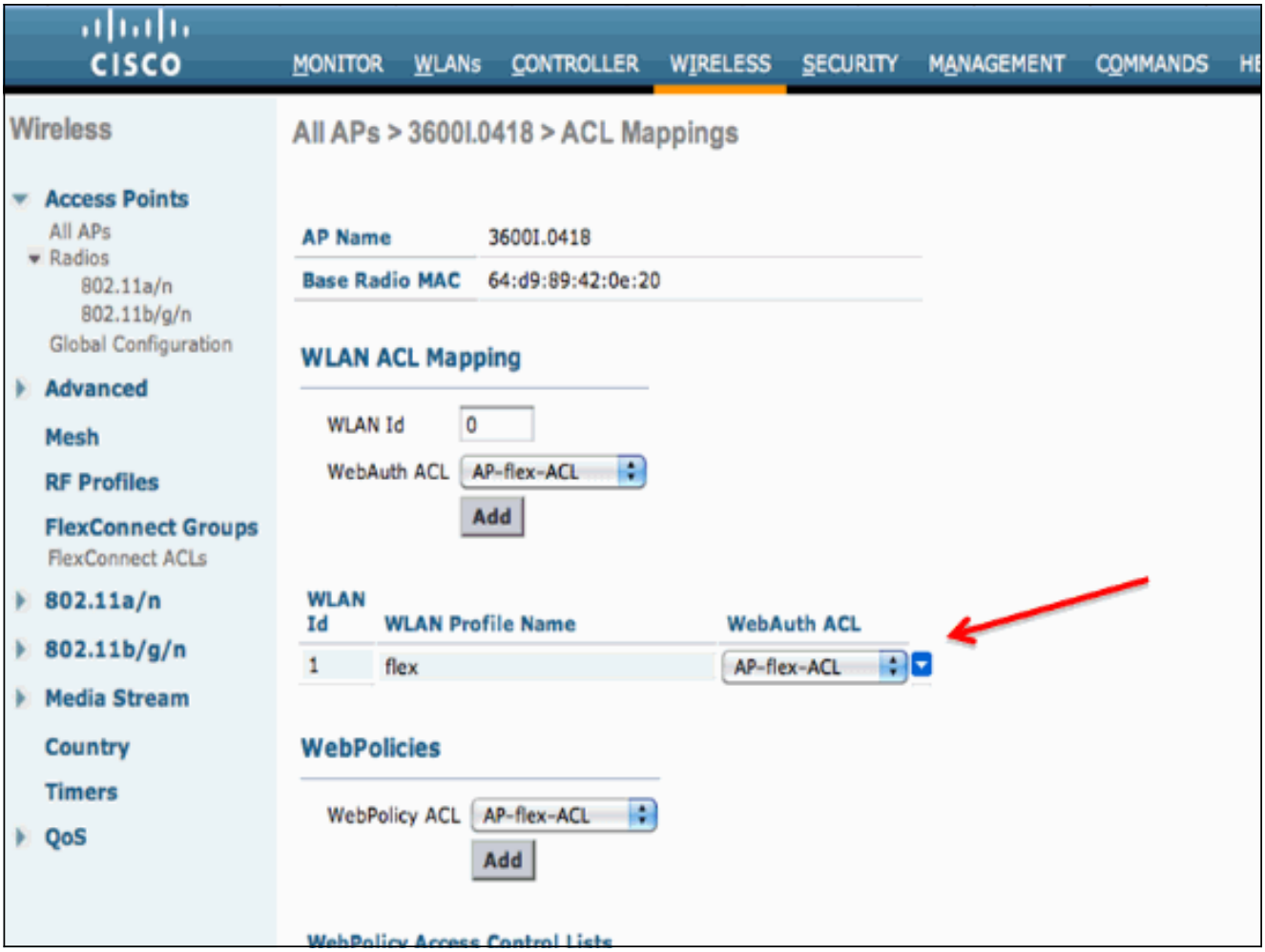


注意： 因为没有需要指定流量方向， FlexConnect ACL是与正常ACL不同。每个规则为流入和流出流量将计数。并且，如果要配置在中央交换的WLAN的Web验证(在本地传送方式或弹性)您仍然需要使用正常ACL。所以，您需要指定流量的方向。

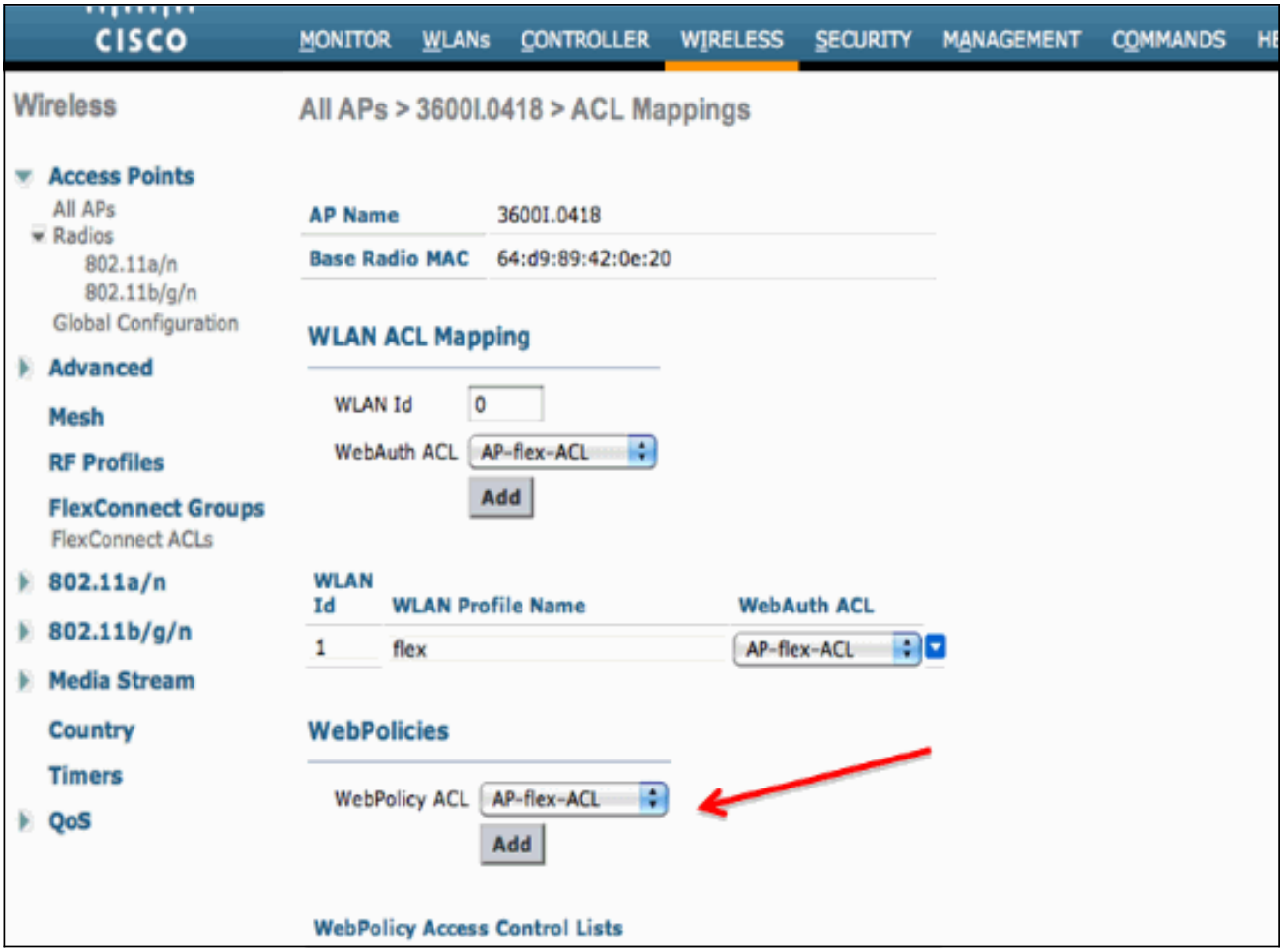
4. 一旦FlexConnect ACL创建的它可以执行在不同的级别应该应用：AP、FlexConnect组和WLAN。最后选项(在WLAN的弹性ACL)仅是为Web验证和Web转接另外两个方法的根据Web策略，例如有条件的和飞溅重定向。ACL可能只应用在AP或弹性组。这是ACL的示例分配在AP级别。去**无线>挑选AP**，然后点击**FlexConnect**选项卡：



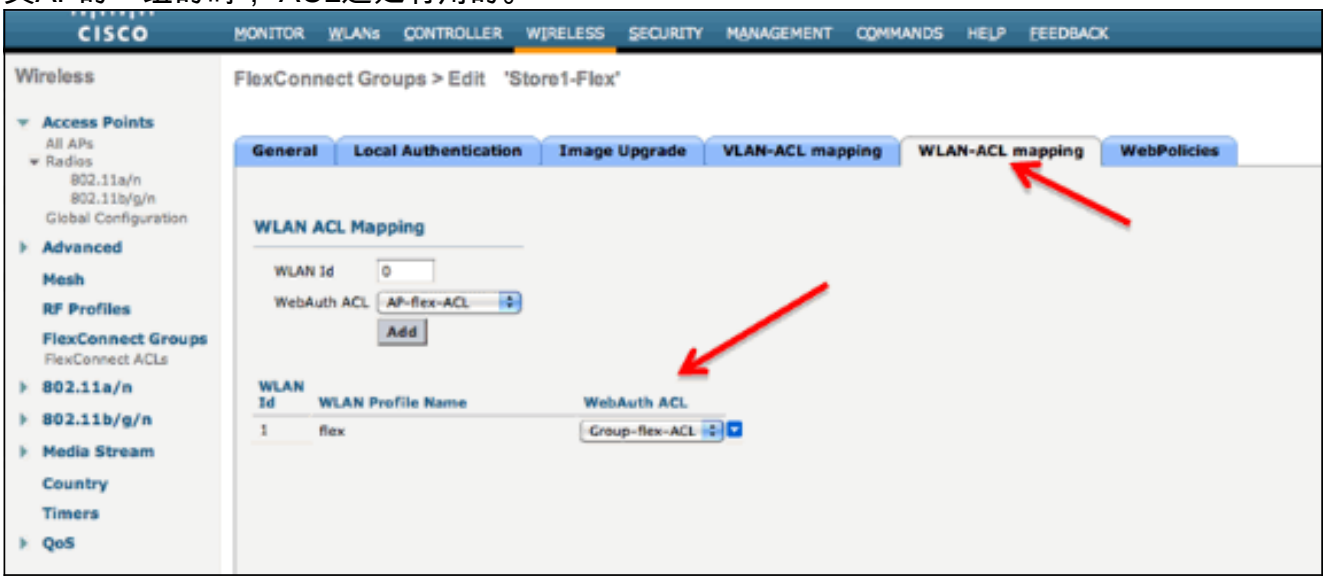
点击**外部WebAuthentication ACL**链路。然后，请选择特定的WLAN Id的ACL：



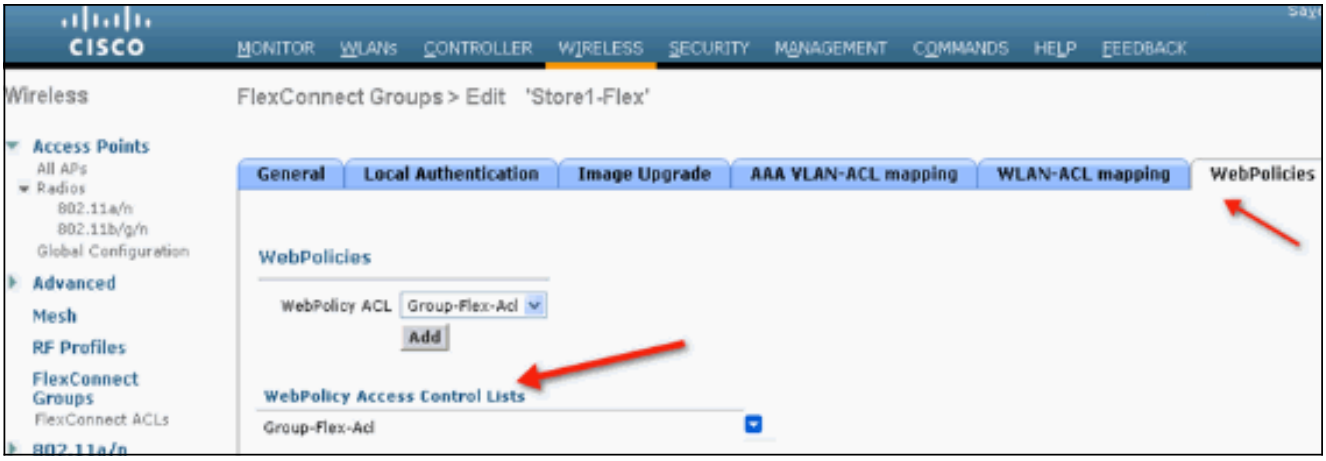
同样地，对于Web策略ACL (例如，有条件的重定向或飞溅页重定向)，您将接收中的选项弹性连接ACL在WebPolicies下，在您点击同一条外部WebAuthentication ACL链路后。这显示此处：



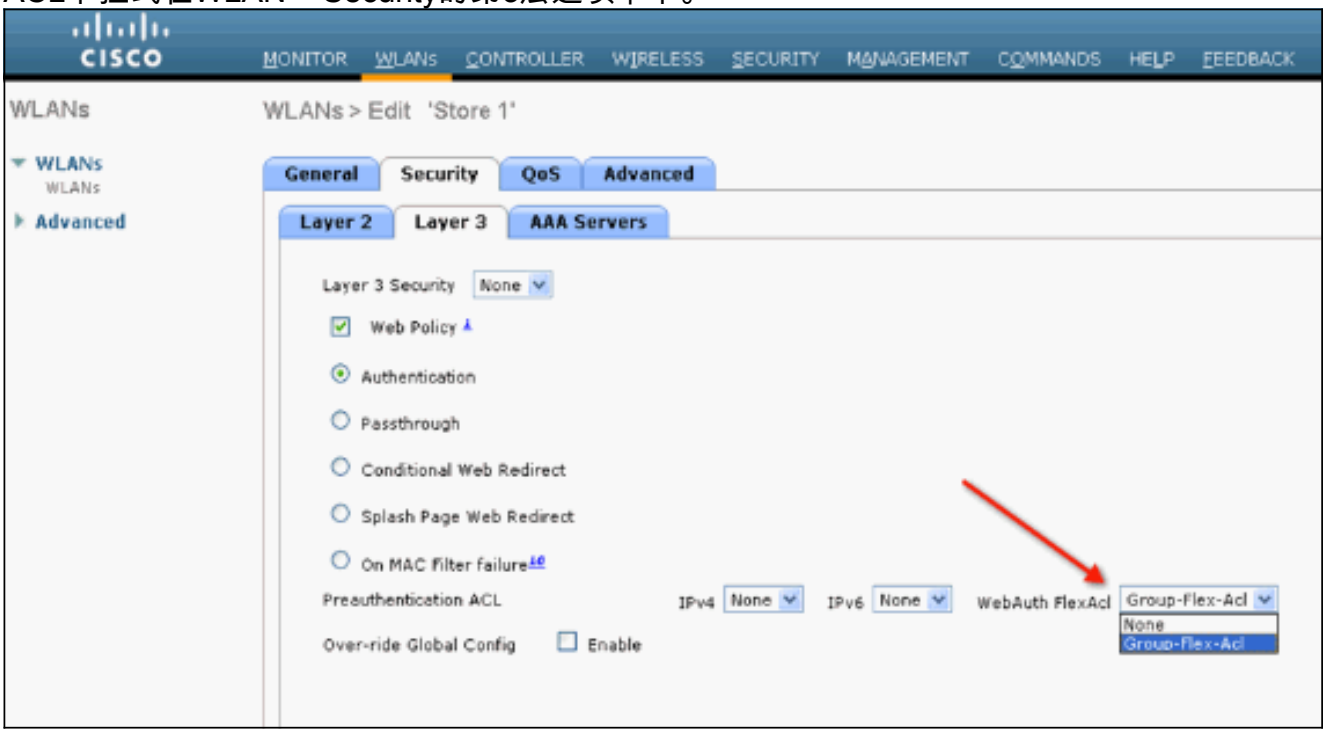
5. ACL可能也应用在FlexConnect社团级别。为了执行此，请去**WLAN-ACL映射**选项卡在FlexConnect组配置里。然后，请选择WLAN Id，并且您要应用的ACL。单击 **Add**。当您要定义AP的一组的时， ACL这是有用的。



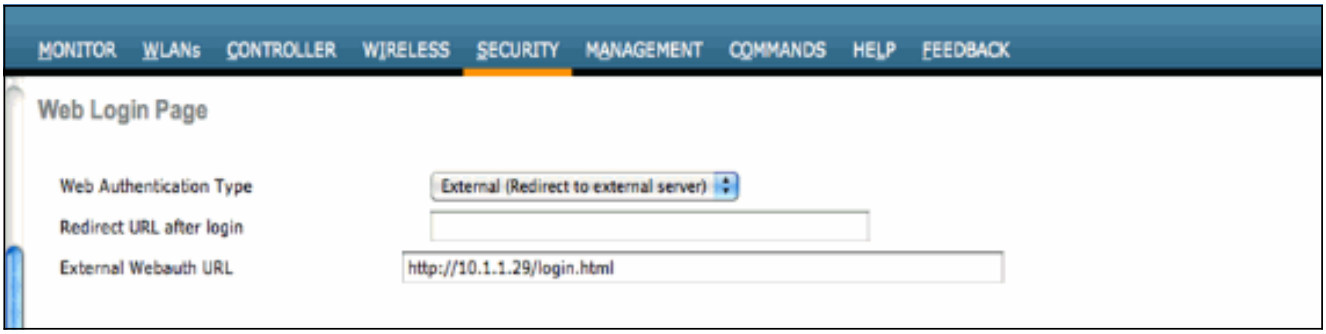
同样地，为了Web策略ACL (对于有条件的和请飞溅页Web重定向)，您需要选择**WebPolicies**选项卡。



6. Web验证和Web转接弹性ACL在WLAN可能也应用。为了执行此，请从**Webauth FlexACL**选择ACL下拉式在WLAN > Security的第3层选项卡下。



7. 对于外部Web验证，重定向URL需要定义。这可以执行在一个全局级别或在级的WLAN。对于级的WLAN，请点击**改写全局配置**复选标记并且插入URL。在全局级别，请去**安全> Web验证 > Web登录页**
：



限制：Web验证(内部或对外部服务器)要求弹性AP在已连接模式。Web验证，如果弹性AP在独立模式，不支持。Web验证(内部或对外部服务器)只支持与中央验证。如果为本地交换配置的WLAN为本地认证配置，您不可执行Web验证。所有Web重定向执行在WLC和不在AP级别
。

相关信息

- 技术支持和文档 - Cisco Systems