Внешняя веб-аутентификация с руководством по развертыванию локального коммутатора FlexConnect

Содержание

Введение

Этот документ объясняет, как использовать внешний web-сервер с локальным коммутатором FlexConnect для различных веб-политик.

Предварительные условия

Требования

Убедитесь, что вы обеспечили выполнение следующих требований, прежде чем попробовать эту конфигурацию:

- Базовые знания об Архитектуре FlexConnect и точках доступа (AP)
- Знание о том, как установить и настроить внешний веб-сервер
- Знание о том, как установить и настроить DHCP и серверы DNS

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Контроллер беспроводной локальной сети (WLC) Cisco 7500, который выполняет релиз микропрограммы 7.2.110.0
- Cisco облегченная точка доступа (LAP) серии 3500
- Внешний веб-сервер, который размещает страницу для входа в веб-аутентификацию
- DNS и Серверы DHCP на локальном узле для определения адресов и IP - адреса размещения беспроводным клиентам

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Несмотря на то, что WLC серии 7500 используется для этого руководства по развертыванию, эта функция поддерживается на 2500, 5500, и WLC WiSM2. Все устройства, описанные в данном документе, были запущены с конфигурацией по умолчанию. Если используемая сеть является действующей, убедитесь в понимании возможного влияния любой из применяемых команд.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.

Обзор функций

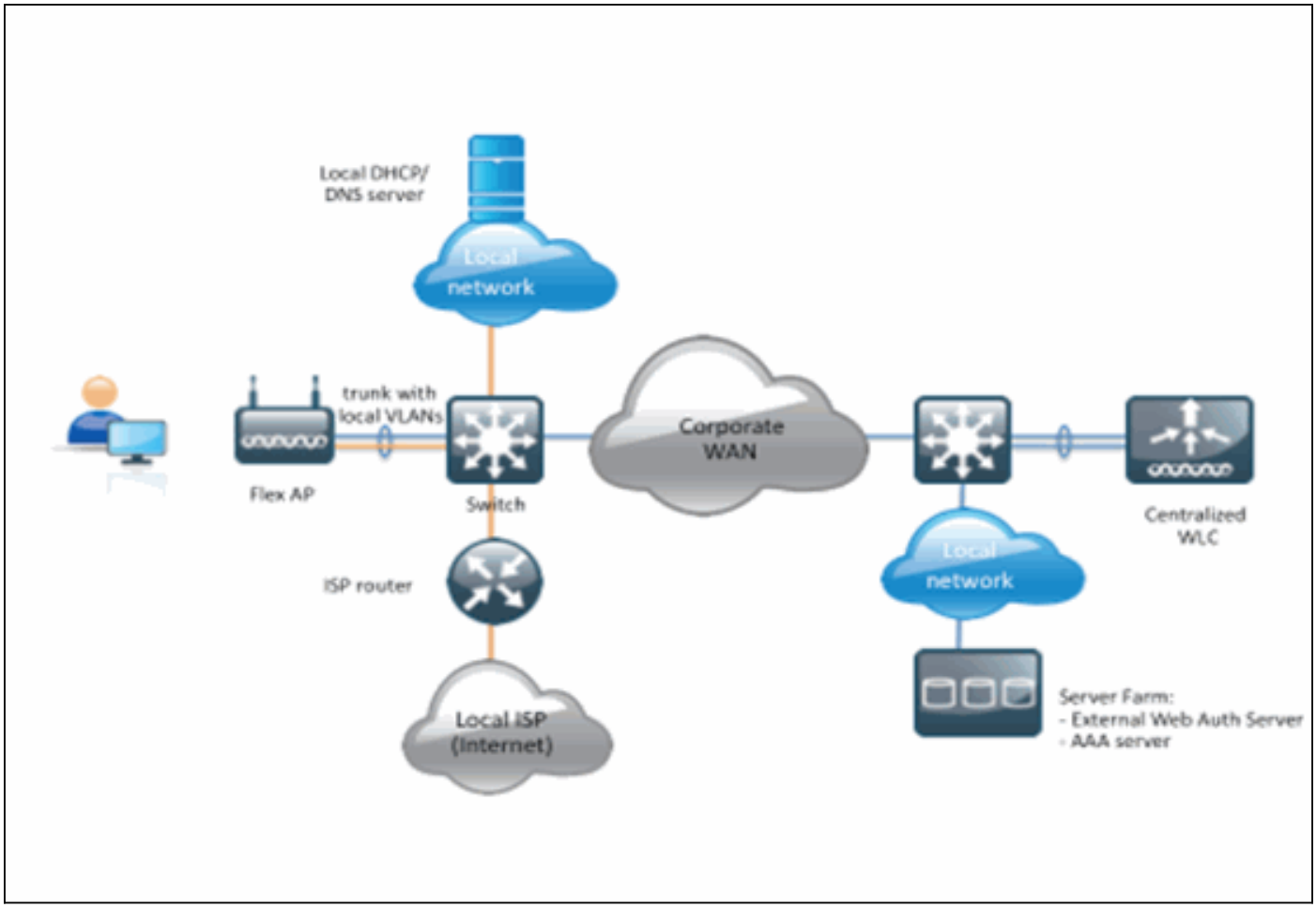
Эта функция расширяет возможность выполняющей Web-аутентификации к внешнему веб-серверу от AP в режиме FlexConnect для WLAN с локально коммутируемым трафиком (FlexConnect – Локальный коммутатор). Перед Выпуском 7.2.110.0 WLC Web-аутентификация к внешнему серверу поддерживалась для AP в режиме Автономного режима или FlexConnect для WLAN с централизованно коммутируемым трафиком (FlexConnect – Центральная Коммутация).

Часто называемый Внешней веб-аутентификацией, эта функция расширяет возможность WLAN Локального коммутатора FlexConnect для поддержки всех веб-Типов безопасности Перенаправления Уровня 3, в настоящее время предоставляемых контроллером:

- Web-аутентификация
- Веб-passthrough
- Веб-условное перенаправление
- Условное перенаправление страницы-заставки

Считая WLAN настроенным для Web-аутентификации и для локального коммутатора, логика позади этой функции должна распределить и применить предварительную проверку подлинности Список контроля доступа (ACL) FlexConnect непосредственно на уровне AP вместо уровня WLC. Таким образом AP коммутирует пакеты, прибывающие от беспроводного клиента, которые позволены ACL, локально. Пакеты, не позволенные, все еще переданы по туннелю CAPWAP к WLC. С другой стороны, когда AP получает трафик по проводному интерфейсу, если позволено ACL, передаст его беспроводному клиенту. В противном случае пакет отбрасывается. Как только клиент аутентифицируется и авторизуется, предварительная проверка подлинности FlexConnect ACL удалена, и весь трафик данных клиента позволен и коммутирован локально.

Примечание: Эта функция работает в предположении, что клиент может достигнуть внешнего сервера от локально коммутируемой VLAN.



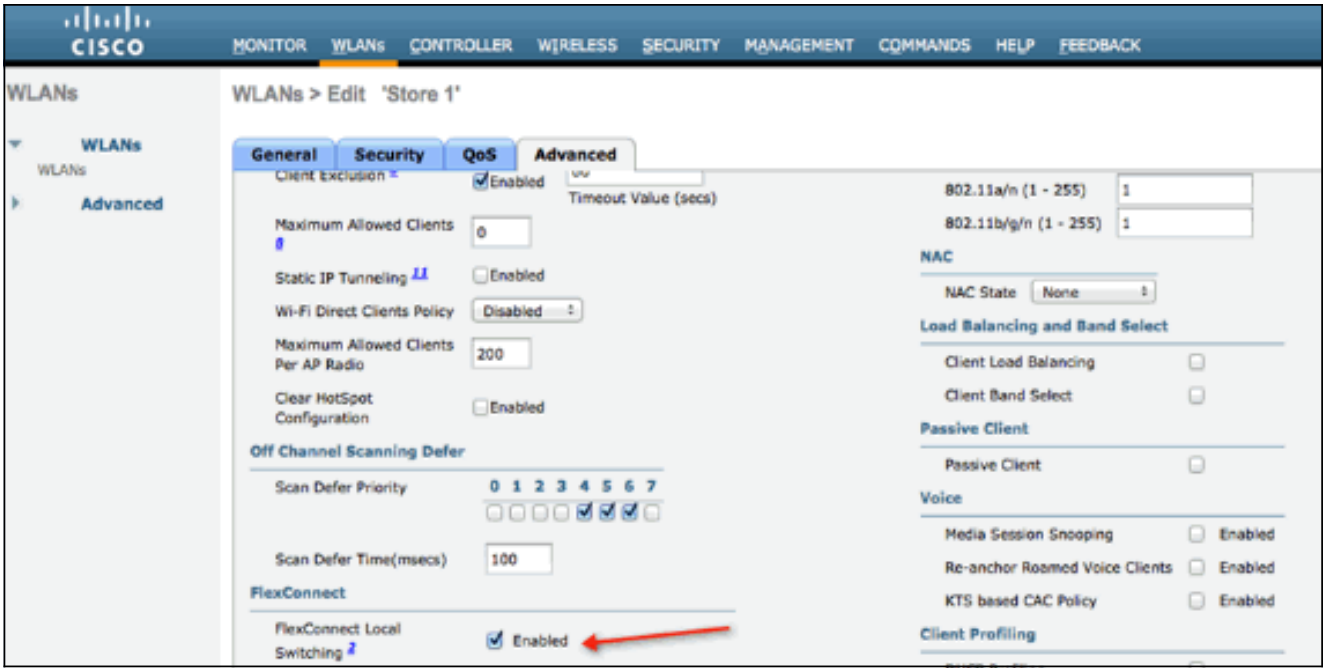
Сводка:

- WLAN, настроенный для Локального коммутатора FlexConnect и Безопасности L3
- ACL FlexConnect будут использоваться в качестве ACL предварительной проверки подлинности
- ACL FlexConnect, однажды настроенные, должны быть выдвинуты к базе данных AP через Flex Group или через Отдельный AP или могут быть применены на WLAN
- AP позволяет весь трафик, который совпадает с ACL предварительной проверки подлинности, который будет коммутирован локально

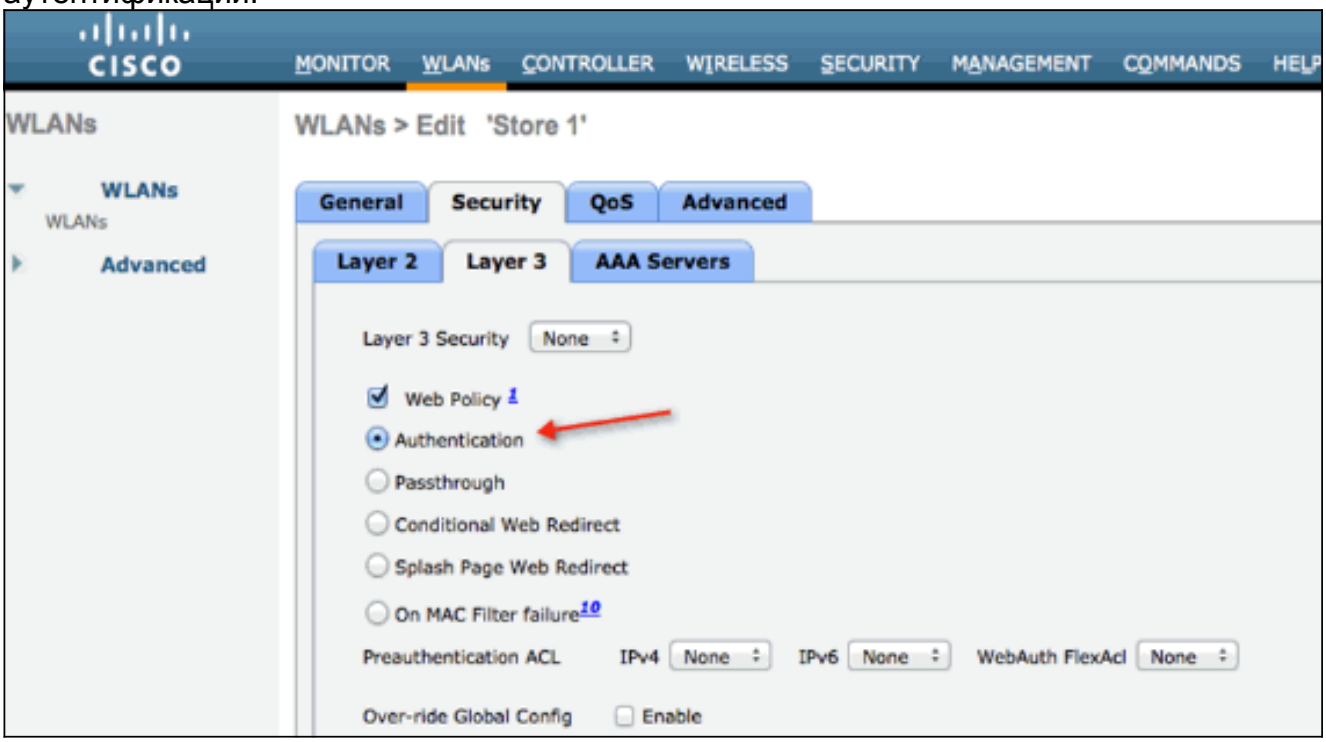
Процедура:

Выполните эти шаги для настройки этой функции:

1. Настройте WLAN для локального коммутатора FlexConnect.



2. Для включения Внешней веб-аутентификации необходимо настроить веб-Политику как политику безопасности для локально коммутируемого WLAN. Это включает одну из этих четырех опций:AuthenticationPass-throughУсловное веб-перенаправлениеВеб-перенаправление страницы-заставкиЭтот документ перехватывает пример для Web-аутентификации:

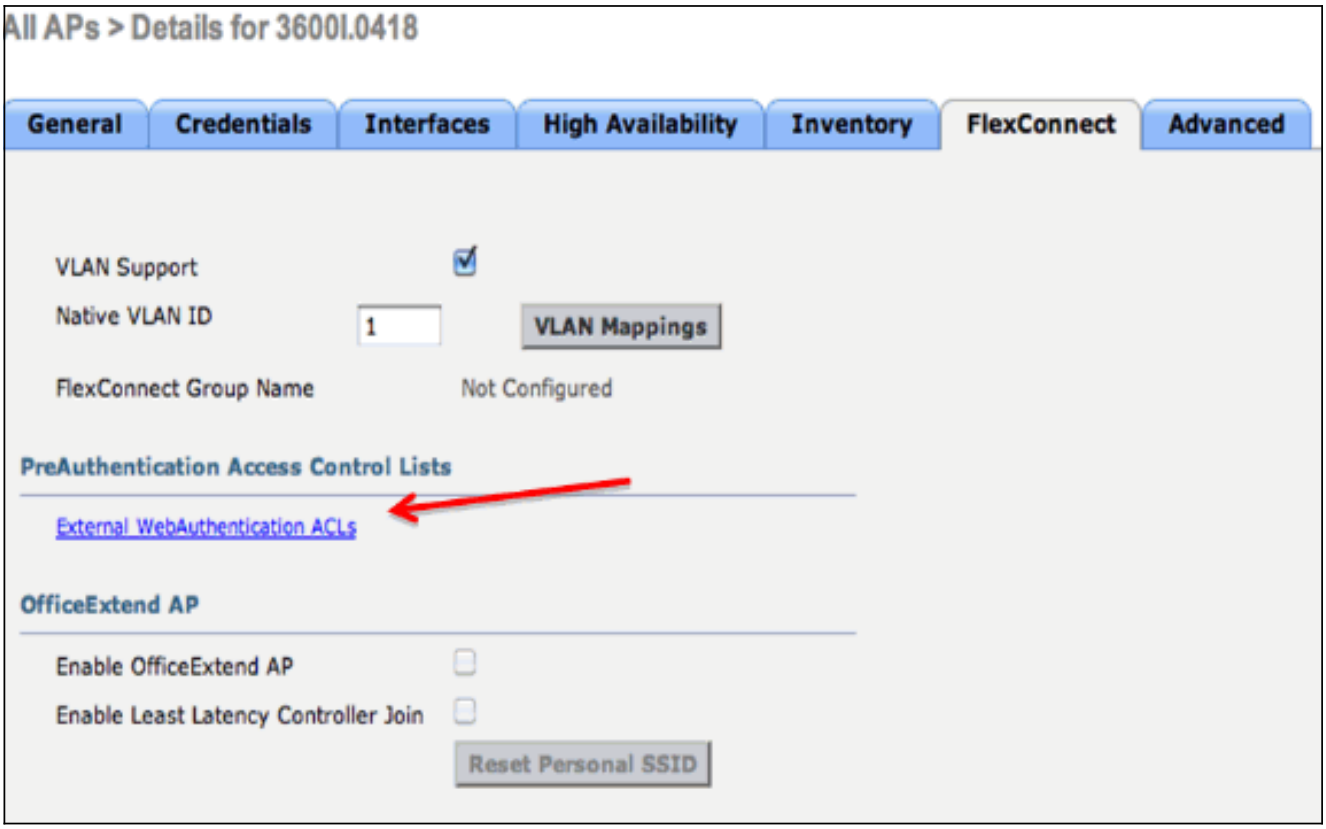


Первые два метода подобны и могут быть сгруппированы как методы Web-аутентификации с точки зрения конфигурации. Вторые два (Условное Перенаправление и Страница-заставка) являются веб-Политикой и могут быть сгруппированы как методы Веб-Политики.

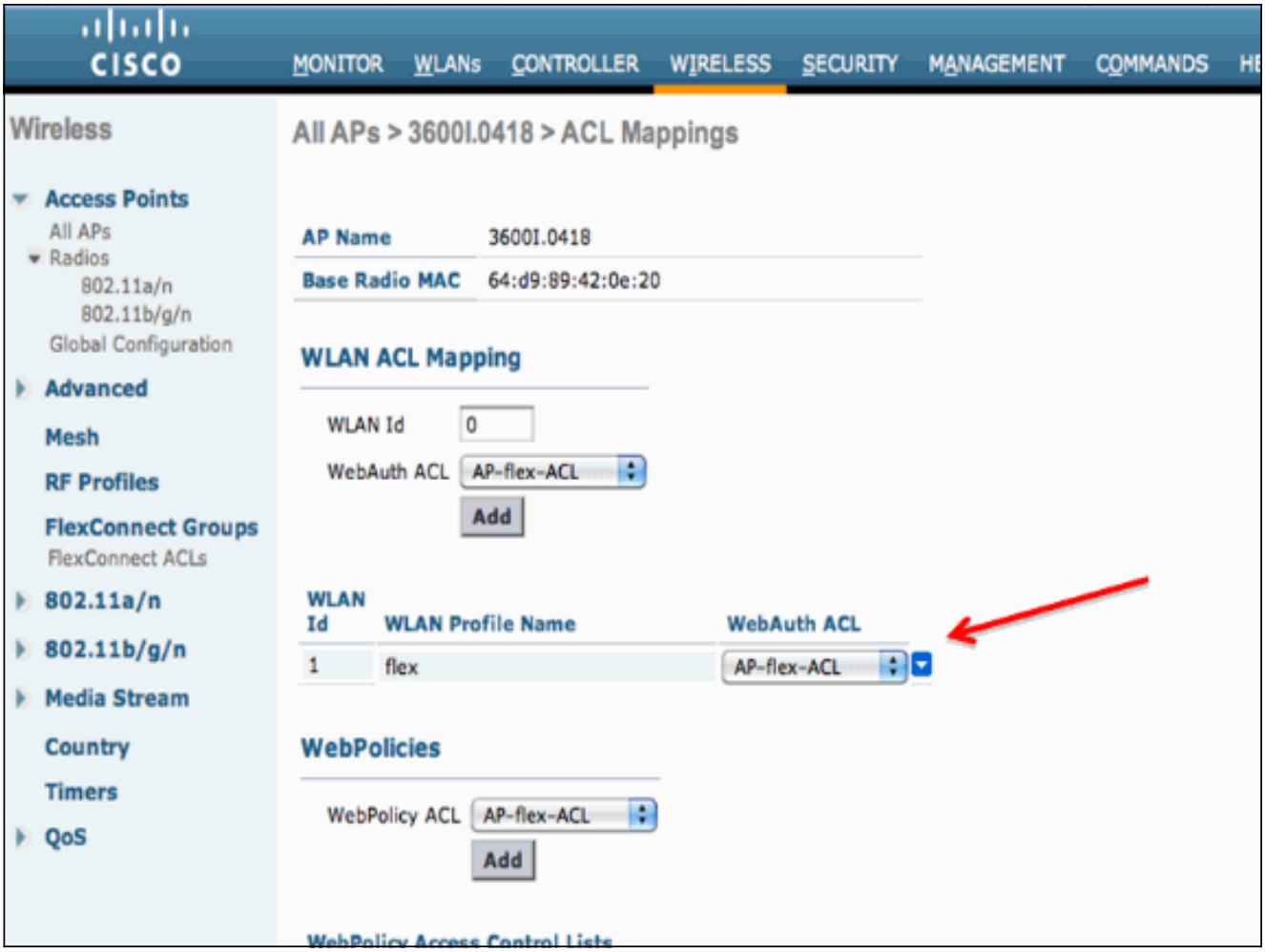
3. Предварительная проверка подлинности FlexConnect ACL должна быть настроена, позволив беспроводным клиентам достигнуть IP-адреса внешнего сервера. ARP, DHCP и трафик DNS автоматически позволены и не должны быть заданы. Под Безопасностью> Список контроля доступа, выберите **FlexConnect ACLs**. Затем **нажмите Add** и определите названия и правила как обычный ACL контроллера.

ACL **Примечание: FLEXCONNECT** отличаются от обычных ACL, потому что нет никакой потребности задать направление трафика. Каждое правило будет значить обоих входящих и исходящих трафика. Кроме того, если вы хотите настроить Web-аутентификацию для Централизованно Коммутируемых WLAN (или в Автономном режиме или в Flex), все еще необходимо использовать обычные ACL. Поэтому необходимо задать направление для трафика.

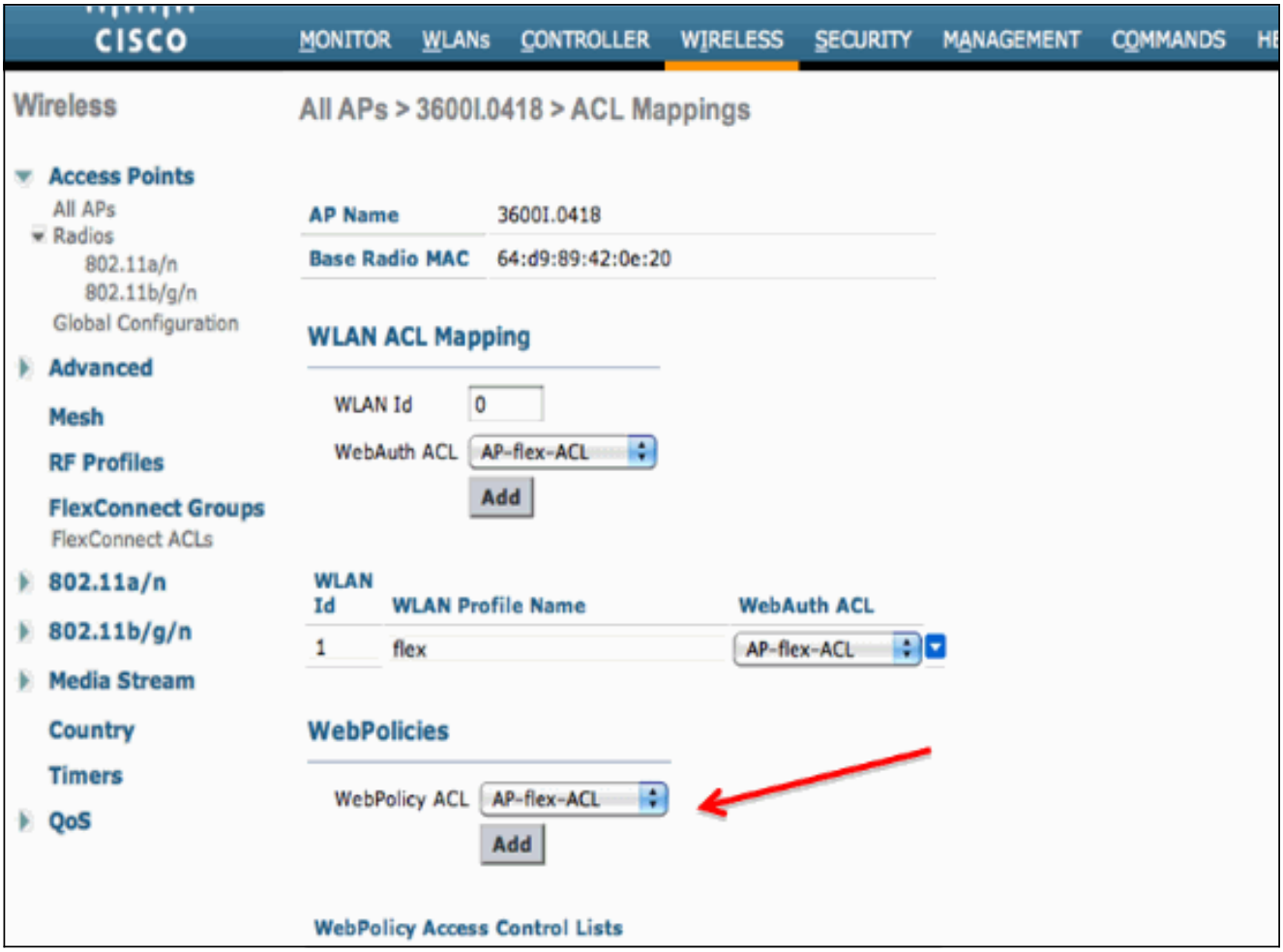
4. Как только ACL FlexConnect созданы, это должно быть применено, который может быть сделан на разных уровнях: AP, FlexConnect Group и WLAN. Этот последний параметр (ACL Flex в WLAN) только для Web-аутентификации и веб-Passthrough для других двух методов под веб-Политикой, таких как Перенаправление Всплеска и Условное выражение. ACL могут только быть применены в AP или Flex Group. Вот пример ACL, назначенного на уровне AP. Перейдите **к беспроводным сетям>, выбирают AP**, затем нажимают вкладку
FlexConnect:



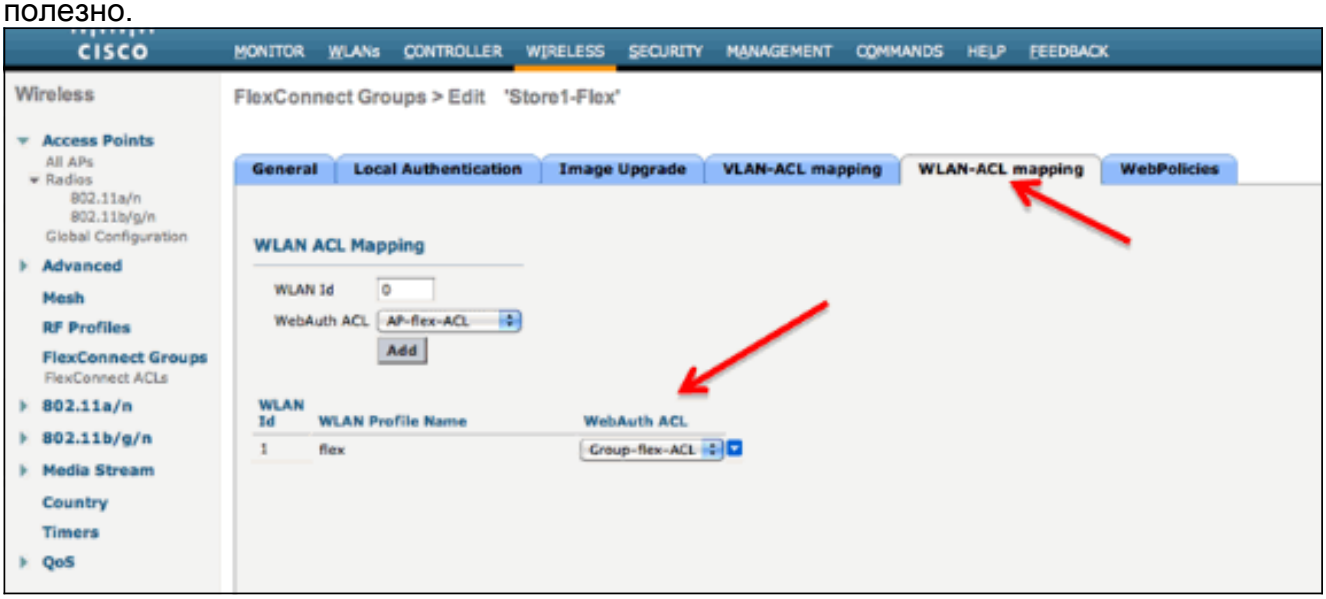
Щелкните **по Внешней** ссылке **ACL WebAuthentication**. Затем выберите ACL для определенного ИДЕНТИФИКАТОРА
WLAN:



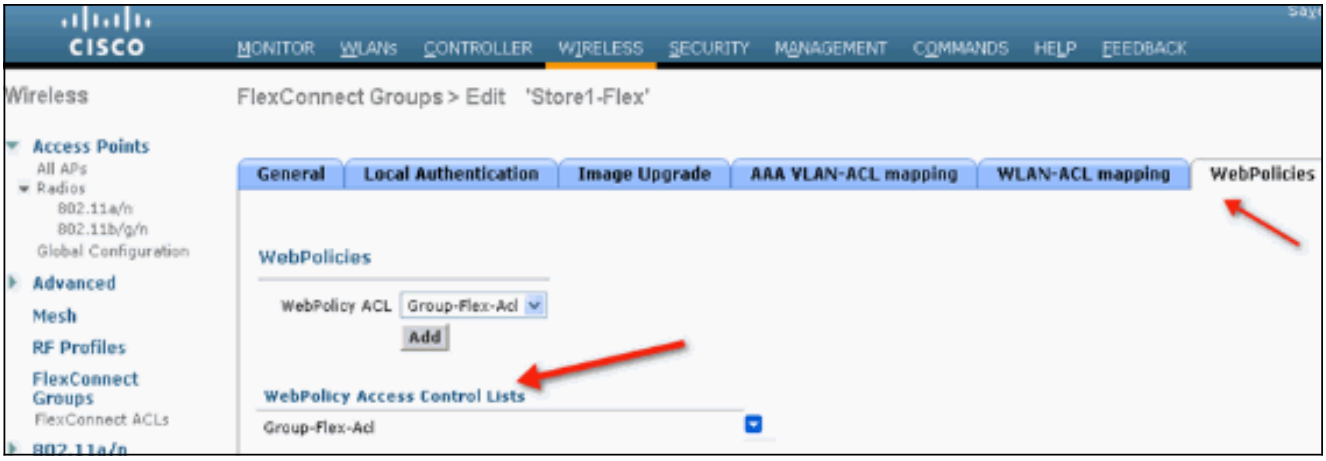
Точно так же для веб-ACL Политики (например, Условное Перенаправление Перенаправления или Страницы-заставки), вы получите опцию для выбора Flex Connect ACL под WebPolicies после щелчка на ту же Внешнюю ссылку ACL WebAuthentication. Это показывают
здесь:



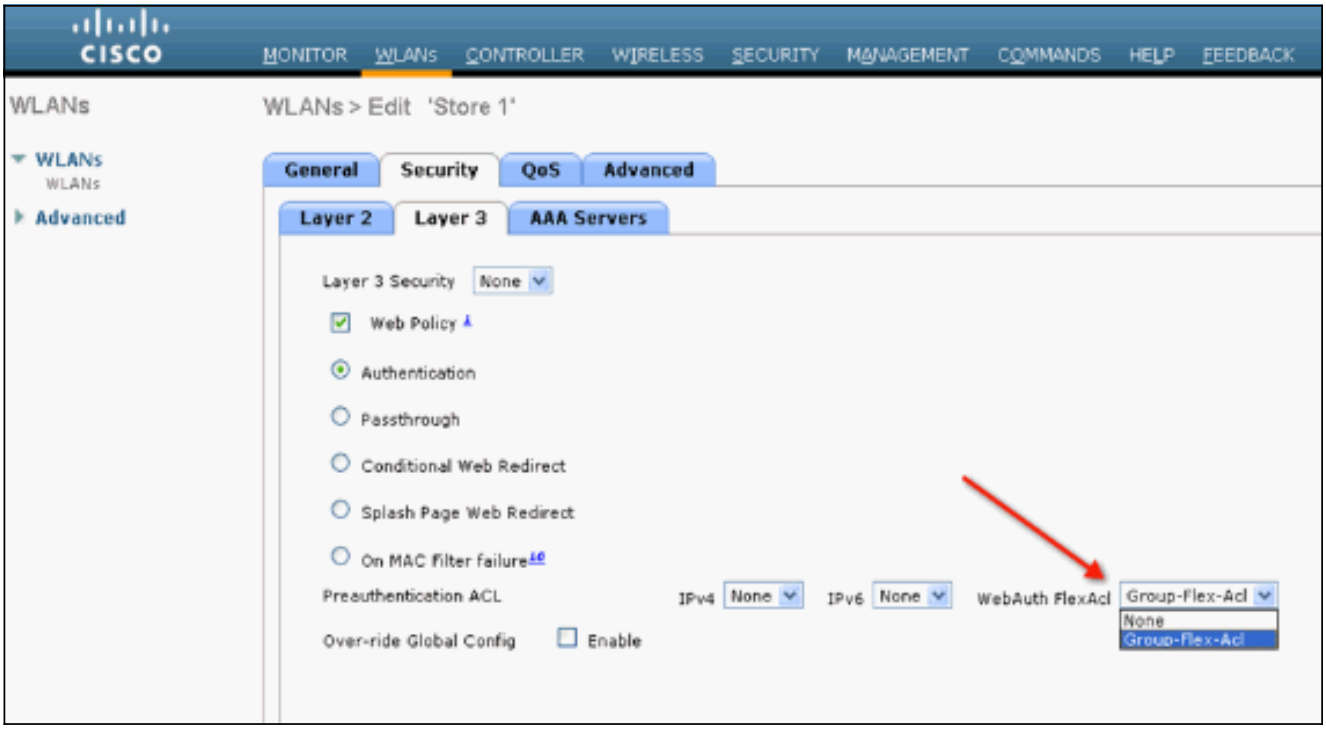
5. ACL может также быть применен на уровне FlexConnect Group. Чтобы сделать это, перейдите к вкладке **сопоставления ACL WLAN** в Конфигурации группы FlexConnect. Затем выберите WLAN Id и ACL, который вы хотите применить. **Нажмите Add**. Когда вы хотите определить ACL для группы AP, это полезно.



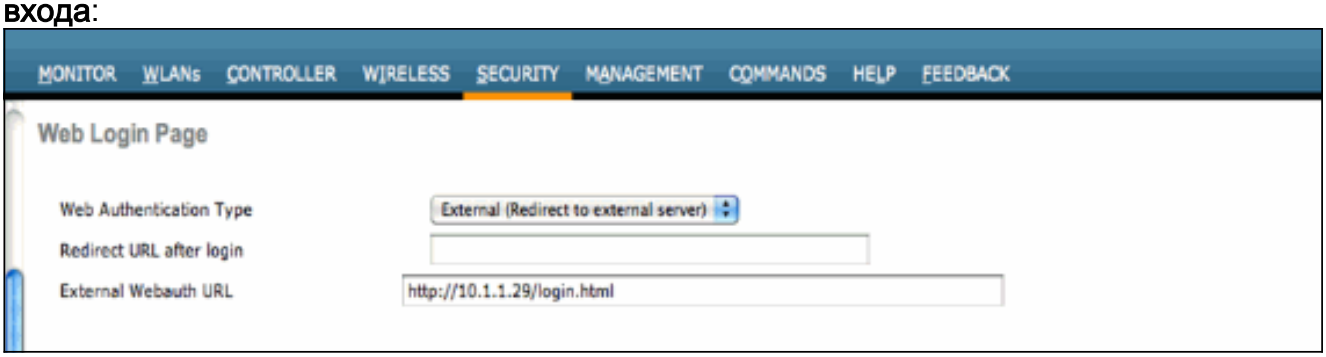
Точно так же для веб-ACL Политики (для веб-Перенаправления Условной и Страницы-заставки), необходимо выбрать вкладку **WebPolicies**.



6. Web-аутентификация и веб-Транзитные ACL Flex могут также быть применены на WLAN. Чтобы сделать это, выберите ACL из **WebAuth FlexACL**, выпадающего под вкладкой Уровня 3 в> Security
WLAN.



7. Для Внешней веб-аутентификации должен быть определен URL перенаправления. Это может быть сделано на глобальном уровне или на уровне WLAN. Для уровня WLAN нажмите **галочку Over-ride Global Config** и вставьте URL. На глобальном уровне перейдите **к Безопасности> веб-Аутентификация> Веб-страница для входа**:



Ограничения: Web-аутентификация (внутренний или к внешнему серверу) требует, чтобы AP Flex был в Связанном режиме. Если AP Flex находится в Автономном режиме, web-аутентификация не поддерживается.Web-аутентификация (внутренний

или к внешнему серверу) только поддерживается с Централизованной аутентификацией. Если WLAN, настроенный для локального коммутатора, настроен для Локальной проверки подлинности, вы не можете выполнить Web-аутентификацию.Все веб-Перенаправление выполнено в WLC а не на уровне AP.

Дополнительные сведения

- Cisco Systems – техническая поддержка и документация