

Внешняя веб-аутентификация с руководством по развертыванию локального коммутатора FlexConnect

Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Условные обозначения](#)

[Обзор функций](#)

[Дополнительные сведения](#)

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

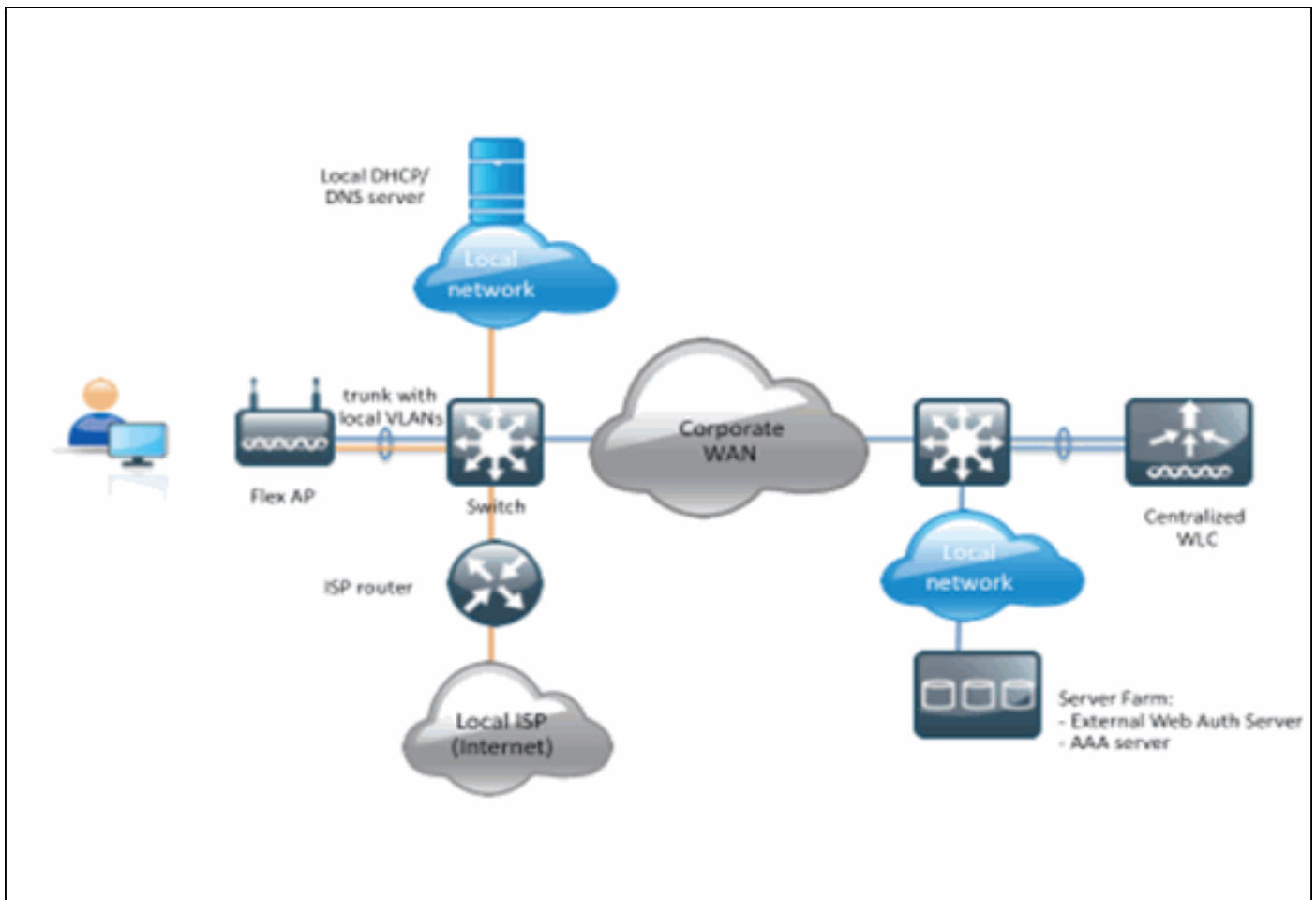
Эта функция расширяет возможность выполняющей Web-аутентификации к внешнему веб-серверу от AP в режиме FlexConnect для WLAN с локально коммутируемым трафиком (FlexConnect – Локальный коммутатор). Перед Выпуском 7.2.110.0 WLC Web-аутентификация к внешнему серверу поддерживалась для AP в режиме Автономного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



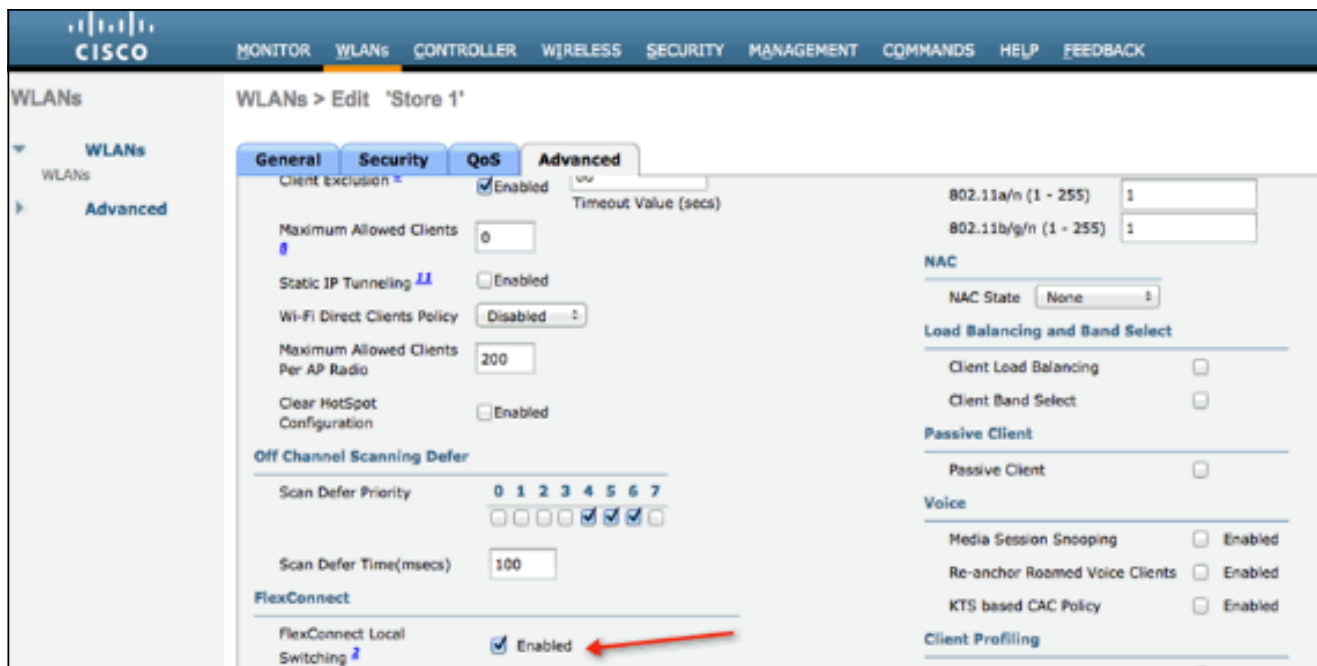
Сводка:

- 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

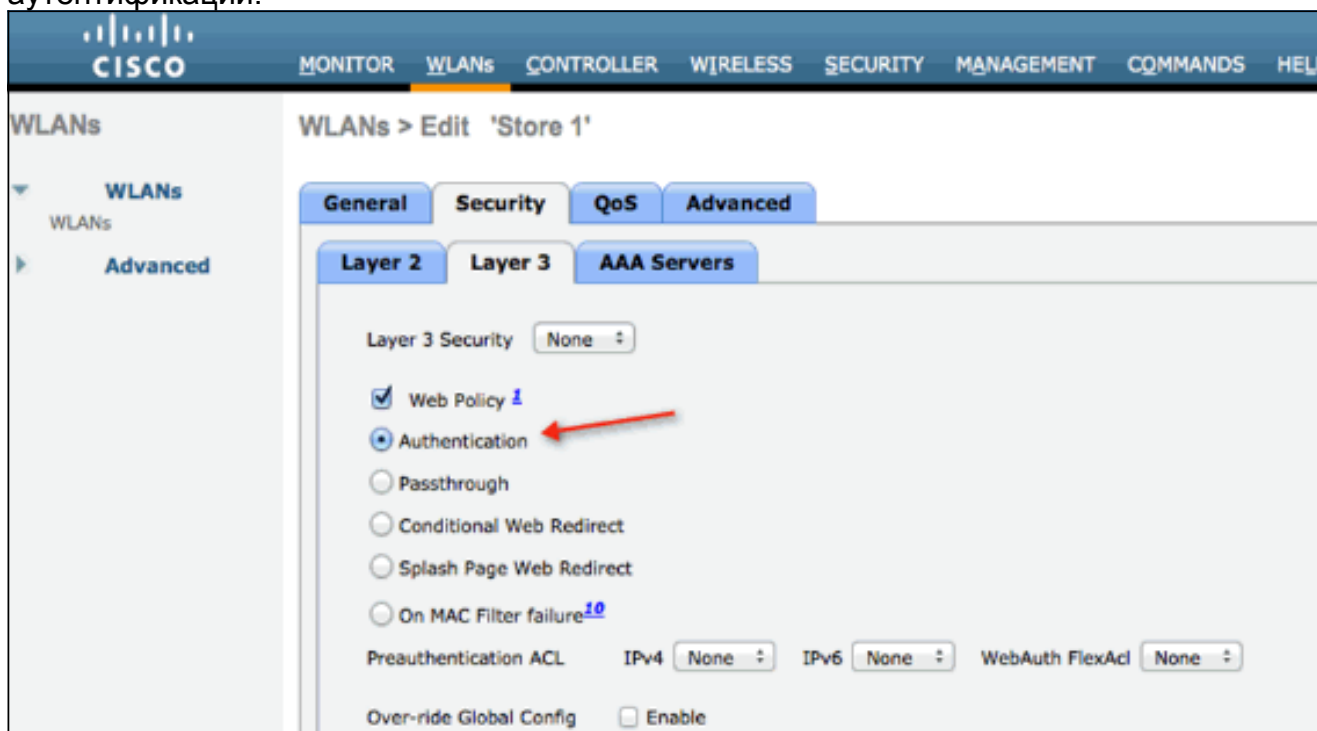
Процедура:

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: Authentication, Pass-through, Conditional Web Redirect, Splash Page Web Redirect. Этот 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 разрешены 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.

Access Control Lists > Edit

General

Access List Name: flex_pre_auth

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP
1	Permit	0.0.0.0 / 0.0.0.0	10.1.1.29 / 255.255.255.255	Any	Any	Any	Any

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:

All APs > Details for 3600i.0418


General | Credentials | Interfaces | High Availability | Inventory | **FlexConnect** | Advanced

VLAN Support

Native VLAN ID: **VLAN Mappings**

FlexConnect Group Name: Not Configured

PreAuthentication Access Control Lists

[External WebAuthentication ACLs](#) 

OfficeExtend AP

Enable OfficeExtend AP

Enable Least Latency Controller Join

Reset Personal SSID

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

The screenshot shows the Cisco Wireless LAN Controller configuration interface. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', and 'COMMANDS'. The main content area is titled 'All APs > 3600I.0418 > ACL Mappings'. On the left, a sidebar menu shows 'Wireless' with sub-items like 'Access Points', 'Radios', 'Advanced', 'Mesh', 'RF Profiles', 'FlexConnect Groups', and radio standards like '802.11a/n' and '802.11b/g/n'. The main configuration area shows 'AP Name' as 3600I.0418 and 'Base Radio MAC' as 64:d9:89:42:0e:20. Under 'WLAN ACL Mapping', there is a 'WLAN Id' field with '0' and a 'WebAuth ACL' dropdown menu set to 'AP-flex-ACL'. Below this is a table with columns 'WLAN Id', 'WLAN Profile Name', and 'WebAuth ACL'. The table contains one entry with '1' in the first column, 'flex' in the second, and 'AP-flex-ACL' in the third. A red arrow points to the 'WebAuth ACL' dropdown in the table. Below the table is a 'WebPolicies' section with a 'WebPolicy ACL' dropdown set to 'AP-flex-ACL' and an 'Add' button.

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:

The screenshot shows the Cisco Wireless configuration interface for an AP named 3600I.0418. The page is titled "All APs > 3600I.0418 > ACL Mappings". On the left, there is a navigation menu with sections like "Access Points", "Radios", "Advanced", "Mesh", "RF Profiles", "FlexConnect Groups", "802.11a/n", "802.11b/g/n", "Media Stream", "Country", "Timers", and "QoS". The main content area is divided into several sections:

- AP Information:** AP Name: 3600I.0418, Base Radio MAC: 64:d9:89:42:0e:20.
- WLAN ACL Mapping:** WLAN Id: 0, WebAuth ACL: AP-flex-ACL, with an "Add" button.
- WLAN Table:**

WLAN Id	WLAN Profile Name	WebAuth ACL
1	flex	AP-flex-ACL
- WebPolicies:** WebPolicy ACL: AP-flex-ACL, with an "Add" button. A red arrow points to this dropdown menu.

At the bottom, there is a link for "WebPolicy Access Control Lists".

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.

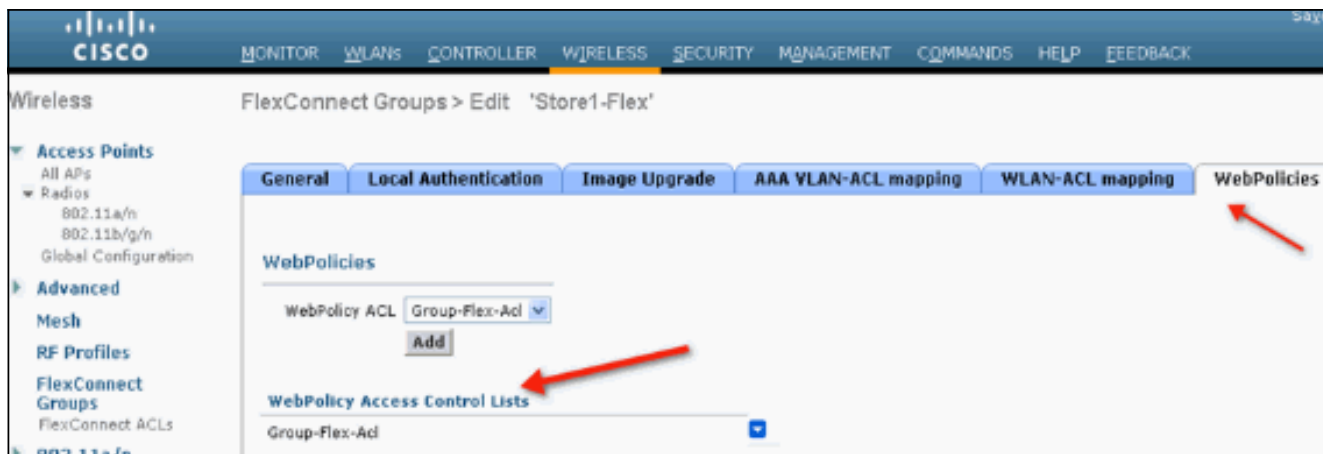
The screenshot shows the Cisco Wireless configuration interface for a FlexConnect Group named "Store1-Flex". The page is titled "FlexConnect Groups > Edit 'Store1-Flex'". The left navigation menu is similar to the previous screenshot. The main content area has several tabs: "General", "Local Authentication", "Image Upgrade", "VLAN-ACL mapping", "WLAN-ACL mapping", and "WebPolicies". The "WLAN-ACL mapping" tab is selected, and a red arrow points to it. The "WLAN ACL Mapping" section is visible:

- WLAN Id: 0
- WebAuth ACL: AP-flex-ACL, with an "Add" button.
- WLAN Table:**

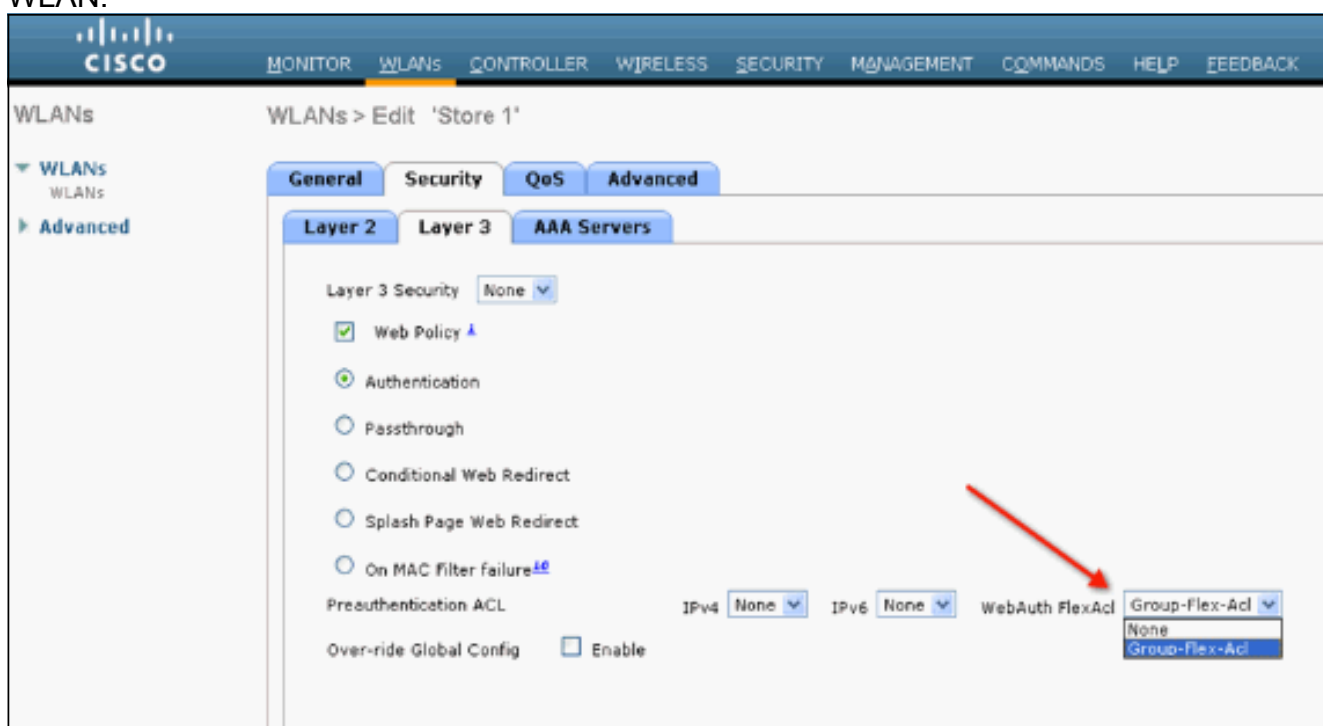
WLAN Id	WLAN Profile Name	WebAuth ACL
1	flex	Group-flex-ACL

A red arrow also points to the "Group-flex-ACL" dropdown menu in the table.

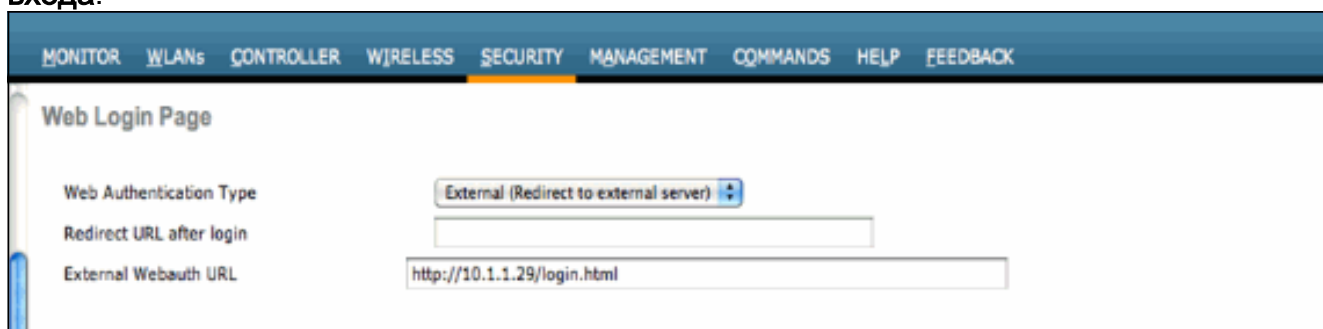
Точно так же для веб-ACL Политики (для веб-Перенаправления Условной и Страницы-заставки), необходимо выбрать вкладку **WebPolicies**.



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](#)