Web-аутентификация на контроллере беспроводной локальной сети

Содержание

Введение

Этот документ объясняет процессы для Web-аутентификации на Контроллере беспроводной локальной сети (WLC).

Предварительные условия

Требования

Cisco рекомендует иметь базовые знания о конфигурации WLC.

Используемые компоненты

Сведения в этом документе основываются на всех моделях оборудования WLC.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Web-аутентификация внутренние процессы

Позиция web-аутентификации как характеристика безопасности

Web-аутентификация (WebAuth) является безопасностью уровня 3. Это обеспечивает удобную для пользователя безопасность, которая работает на любую станцию, которая выполняет браузер. Это может также быть объединено с любой безопасностью предварительного общего ключа (PSK) (политика безопасности уровня 2). Несмотря на то, что комбинация WebAuth и PSK уменьшает удобную для пользователя часть значительно и часто не используется, это все еще имеет преимущество для шифрования трафика клиента. WebAuth является методом аутентификации без шифрования.

WebAuth не может быть настроен с 802.1X/RADIUS (СЛУЖБА ПРОВЕРКИ ПОДЛИННОСТИ УДАЛЕННОГО НАБОРНОГО ТЕЛЕФОННОГО ДОСТУПА ПОЛЬЗОВАТЕЛЯ), пока Выпуск 7.4 Программного обеспечения WLC не установлен, где это может быть настроено в то же время. Однако знайте, что клиенты должны пройти и dot1x и web-аутентификацию. Это не предназначено для гостя, но для добавления веб-портала для сотрудников (кто использует 802.1x). Нет единого идентификатора набора сервисов (SSID) для dot1x для сотрудников или веб-портала для гостей.

Как работает WebAuth

Процесс проверки подлинности 802.11 открыт, таким образом, можно аутентифицироваться и связаться без любых проблем. После этого вы привязаны, но не в WLC **ВЫПОЛНЕННОЕ** состояние. С включенной web-аутентификацией вы сохранены в **WEBAUTH_REQD**, где вы не можете обратиться ни к какому сетевому ресурсу (никакой эхо-запрос, и так далее). Необходимо получить IP-адрес DHCP с адресом сервера DNS в опциях.

Необходимо ввести допустимый URL в браузере. Клиент решает URL через протокол DNS. Клиент тогда передает его запрос HTTP к IP-адресу веб-сайта. Точки пересечения WLC, которые запрашивают и возвращают **webauth** страницу входа, которая имитирует IP-адрес веб-сайта. В случае внешнего WebAuth WLC отвечает с Ответом HTTP, который включает ваш IP-адрес веб-сайта и сообщает, что переместилась страница. Страница была перемещена во внешний веб-сервер, используемый WLC. Когда вы аутентифицируетесь, вы получаете доступ ко всем сетевым ресурсам и перенаправлены к URL, который первоначально запрашивают, по умолчанию (пока принудительное перенаправление не было настроено на WLC). Таким образом, WLC позволяет клиенту решать DNS и получать

IP-адрес автоматически в состоянии **WEBAUTH_REQD**.

Совет: Если вы хотите, чтобы WLC наблюдал другой порт вместо порта 80, можно использовать **config network web-auth-port <номер порта>** для создания перенаправления на этом порту также. Примером является веб-интерфейс Access Control Server (ACS), который находится на порту 2002 или других подобных приложениях.

> **Примечание о Перенаправлении HTTPS**: По умолчанию и в 7.x версии и ранее, WLC не перенаправил Трафик HTTPS. Это означает, что, если вы открываете свой браузер и вводите адрес HTTPS, ничто не происходит. Необходимо ввести Http - адрес, чтобы быть перенаправленными к странице входа, которая подавалась в HTTPS.
>
> В Версии 8.0 и позже, можно включить перенаправление Трафика HTTPS с **перенаправлением https веб-аутентификации сети config** команды CLI**, включают.**
>
> Знайте, что это - потребление ресурса для WLC в случае, если передаются много Запросов HTTPS. Также обратите внимание, что сертификат, предупреждающий, неизбежен в этом случае. Действительно, если ваши запросы клиента любой URL (такие как https://www. cisco . com), WLC все еще представляет свой собственный сертификат, выполненный для IP-адреса виртуального интерфейса. Это никогда не будет, очевидно, совпадать с URL/IP-АДРЕСОМ, который запрашивает клиент, и сертификату не будут доверять, пока клиент не вызовет исключение в своем браузере.

Показательное снижение производительности измерилось:

Webauth	Скорость достигнута
3 URL - HTTP	140/второй
1-й URL - HTTP 2-е и 3-и URL - HTTPS	20/второй
3 URL - HTTPS (большие развертывания)	<1 / второй
3 URL - HTTPS (макс. 100 клиентов)	10/второй

В этой таблице производительности эти 3 URL упоминаются как:

- Исходный URL, введенный конечным пользователем (веб-сайт пользователь хочет перейти к),
- URL WLC перенаправляет браузер к
- Заключительное учетное представление

Таблица производительности дает производительность WLC в случае, если все 3 URL являются HTTP, в случае, если все 3 URL являются HTTPS, или если клиент перемещается от HTTP до HTTPS (больше типичного сценария).

Как заставить внутренний (локальный) WebAuth работать с внутренней страницей

Если необходимо настроить WLAN с в рабочем состоянии динамическим интерфейсом, клиенты должны также получить IP-адрес сервера DNS через DHCP. Перед установкой любого **webauth** необходимо протестировать тот WLAN, работает должным образом, что можно решить запросы DNS **(nslookup)**, и что можно просмотреть веб-страницы. Затем можно установить web-аутентификацию как функции безопасности уровня 3. Можно создать

пользователей в локальной базе данных или на внешнем сервере RADIUS, например. См. документ Примера настройки веб-аутентификации в контроллере беспроводной сети LAN.

Как настроить пользовательский локальный WebAuth с пользовательской страницей

Пользовательский **webauth** может быть настроен с **redirectUrl** от **Вкладки Безопасность**. Это вызывает перенаправление к определенной веб-странице, которую вы вводите. Когда пользователь аутентифицируется, это отвергает исходный URL клиент, которого запрашивают, и отображает страницу, для которой было назначено перенаправление.

Пользовательское средство позволяет вам использовать пользовательскую страницу HTML вместо страницы для входа по умолчанию. Загрузите свой HTML и связку (bundle) графических файлов к контроллеру. На странице upload ищите **связку (bundle) webauth** в формате tar. Обычно, PicoZip создает tar, которые работают совместимо с WLC. Для примера связки (bundle) WebAuth обратитесь к Странице ПО Загрузки для Контроллера беспроводной локальной сети Бандлы WebAuth. Обязательно выберите соответствующий выпуск для вашего WLC. Хорошая рекомендация состоит в том, чтобы настроить связку (bundle), которая существует; не создавайте связку (bundle) с нуля.

Существуют некоторые ограничения с **пользовательскими webauth**, которые меняются в зависимости от версий и дефектов. Вещи наблюдать за включают:

- размер файла .tar (не больше, чем 5 МБ)
- количество файлов в .tar
- Длина имени файла файлов (должны быть не больше, чем 30 символов),

Если ваш пакет клиента не работает, попробуйте простым пользовательским пакетом. Затем добавьте файлы и сложность по одному для достижения пакета, который клиент пытался использовать. Это должно помочь вам определять проблему. Для примера о том, как настроить пользовательскую страницу, обратитесь к Созданию Специализированной Страницы для входа в веб-аутентификацию, раздела в руководстве по конфигурированию контроллера Cisco Wireless LAN, Выпуске 7.0.

Способ глобальной конфигурации замены

Для каждого WLAN вы настраиваете с **командой override global config** и устанавливаете тип WebAuth для каждого WLAN. Это означает, что у вас может быть внутренний/по умолчанию WebAuth с пользовательским внутренним/по умолчанию WebAuth для другого WLAN. Это также позволяет вам настраивать другие пользовательские страницы для каждого WLAN. Необходимо объединить все страницы в той же связке (bundle) и загрузить их к WLC. Затем можно установить пользовательскую страницу с **командой override global config** на каждом WLAN и выбрать, какой файл является страницей входа от всех файлов в связке (bundle). Можно выбрать другую страницу входа в связке (bundle) для каждого WLAN.

Проблема перенаправления

Существует переменная в связке (bundle) HTML, которая позволяет перенаправление. Не

помещайте свой принудительный URL перенаправления там. Для любых проблем перенаправления в пользовательском WebAuth Cisco рекомендует проверить связку (bundle). При вводе URL перенаправления с **+ =** в GUI WLC это могло бы перезаписать *или* добавить к URL, определенному в связке (bundle). Например, в GUI WLC, **redirectURL** поле установлено в www. cisco . com; однако, в связке (bundle) это показывает: **redirectURL + =** 'www.google.com'. **+ =** перенаправляет пользователей к www. cisco . comwww.google.com, который является недопустимым URL.

Как заставить внешнюю (локальную) web-аутентификацию работать с внешней страницей

Как уже кратко объяснено, использование внешнего сервера WebAuth является просто внешним репозиторием для страницы входа. Учетные данные пользователя все еще аутентифицируются WLC. Внешний веб-сервер только позволяет вам использовать специальную или другую страницу входа. Вот шаги, выполненные для внешнего WebAuth:

1. Клиент (конечный пользователь) открывает web-браузер и вводит URL.

2. Если клиент не аутентифицируется, и внешняя веб-аутентификация используется, WLC перенаправляет пользователя к URL внешнего веб-сервера. Другими словами, WLC передает перенаправление HTTP клиенту с поддельным IP-адресом веб-сайта и точками к IP-адресу внешнего сервера. URL входа в систему внешней веб-аутентификации добавлен с параметрами, такими как **AP_Mac_Address**, **client_url** (www.website.com) и **action_URL** что потребительские нужды для контакта с Web-сервером коммутатора.

3. URL внешнего веб-сервера передает пользователю к странице входа. Затем пользователь может использовать список контроля доступа (ACL) процедур, предшествующих аутентификации для доступа к серверу. ACL необходим для всех моделей WLC кроме серии 4400 и Wism1.

4. Страница входа берет ввод учетных данных пользователя и передает запрос обратно в **action_URL**, такой как http://1.1.1.1/login.html, Веб-сервера WLC. Это предоставлено как параметр ввода URL перенаправления клиента, где 1.1.1.1 адрес виртуального интерфейса на коммутаторе.

5. Веб-сервер WLC отправляет имя пользователя и пароль для аутентификации.

6. WLC инициирует запрос сервера RADIUS или использует локальную базу данных на WLC, и затем аутентифицирует пользователя.

7. Если аутентификация успешна, Веб-сервер WLC или вперед пользователь к настроенному URL перенаправления или к URL, клиент ввел.

8. Если аутентификация отказывает, то Веб-сервер WLC перенаправляет пользователя назад к URL входа в систему клиента.

Примечание: Если точки доступа (AP) находятся в режиме FlexConnect, **preauth** ACL не важен. ACL Flex могут использоваться для предоставления доступа на Web-сервер для

клиентов, которые не аутентифицировались. См. Внешнюю веб-аутентификацию с Примером конфигурации Контроллеров беспроводной локальной сети.

Веб-Passthrough

Это - изменение внутренней веб-аутентификации. Это отображает страницу с предупреждением или аварийным оператором, но не вызывает для учетных данных. Пользователь должен нажать **ok**. Можно включить почтовый ввод, и пользователь может ввести их адрес электронной почты, который становится их именем пользователя. Когда пользователь связан, проверьте, что ваши активные клиенты перечисляют; тот пользователь перечислен с адресом электронной почты, который они ввели как имя пользователя. Для получения дополнительной информации обратитесь к сети Контроллера беспроводной локальной сети Транзитный Пример конфигурации.

Условное веб-перенаправление

Если вы включаете условное веб-перенаправление, пользователь условно перенаправлен к определенной веб-странице после того, как аутентификация 802.1x успешно завершила. Можно задать страницу перенаправления и условия, при которых перенаправление происходит на сервере RADIUS. Условия могут включать пароль пользователя, когда он достигает даты окончания действия или когда пользователь должен оплатить счет для продолжительного использования/доступа. Если сервер RADIUS возвращает **перенаправление URL** AV-пары Cisco, то пользователь перенаправлен к указанному URL, когда они открывают браузер. Если сервер также возвращает **acl перенаправления URL** AV-пары Cisco, то указанный ACL установлен как ACL процедур, предшествующих аутентификации для этого клиента. Клиента не считают полностью авторизовавшим на этом этапе и может только передать трафик, позволенный ACL процедур, предшествующих аутентификации. После того, как клиент завершает определенную операцию в указанном URL (например, изменение пароля или оплата счета), тогда клиент должен пройти повторную проверку подлинности. Когда сервер RADIUS не возвращает **перенаправление URL**, клиента считают полностью авторизовавшим и разрешенным передать трафик.

Примечание: Условная веб-функция перенаправления доступна только для WLAN, которые настроены для 802.1x или безопасности уровня 2 WPA+WPA2.

После настройки сервера RADIUS можно тогда настроить условное веб-перенаправление на контроллере с графическим интерфейсом контроллера или CLI. См. эти пошаговые инструкции: Использование GUI для Настройки веб-Перенаправления и Использования CLI для Настройки веб-Перенаправления.

Веб-перенаправление страницы-заставки

Если вы включаете веб-перенаправление страницы-заставки, пользователь перенаправлен к определенной веб-странице после того, как аутентификация 802.1x завершила успешно. После перенаправления у пользователя есть полный доступ к сети. Можно задать страницу перенаправления на сервере RADIUS. Если сервер RADIUS возвращает **перенаправление URL** AV-пары Cisco, то пользователь перенаправлен к указанному URL, когда они открывают браузер. Даже если сервер RADIUS не возвращает **перенаправление URL**, клиент считается полностью авторизовавшим на этом этапе и разрешен передать трафик.

Примечание: Веб-функция перенаправления страницы-заставки доступна только для WLAN, которые настроены для 802.1x или безопасности уровня 2 WPA+WPA2.

После настройки сервера RADIUS можно тогда настроить веб-перенаправление страницы-заставки на контроллере с графическим интерфейсом контроллера или CLI.

WebAuth на сбое фильтра MAC

Это требует, чтобы вы настроили фильтры MAC в меню безопасности уровня 2. Если пользователи успешно проверены с их MAC-адресами, то они идут непосредственно в состояние **выполнения**. Если они не, то они переходят к состоянию **WEBAUTH_REQD**, и обычная web-аутентификация происходит.

Примечание: Это не поддерживается с веб-passthrough. Для получения дополнительной информации придерживайтесь действия на запросе на расширение CSCtw73512 .

Центральная веб-аутентификация

Центральная веб-аутентификация ссылается на сценарий, где WLC больше не размещает сервисов. Различие находится в факте, что клиент непосредственно передается веб-порталу ISE и не проходит 1.1.1.1 на WLC. Страница входа и весь портал воплощены.

Центральная веб-аутентификация имеет место, когда вам включили Network Admission Control (NAC) RADIUS в расширенных настройках WLAN, и фильтры MAC включили.

Общее понятие - то, что WLC передает Проверку подлинности RADIUS (обычно для фильтра MAC) к ISE, который отвечает с парой значения атрибута (AV) **URL перенаправления**. Пользователь тогда помещен в состояние **POSTURE_REQD**, пока ISE не дает авторизацию с запросом изменения авторизации (CoA). Тот же сценарий происходит в Положении или Центральном WebAuth. Центральный WebAuth не совместим с WPA-Enterprise/802.1x, потому что гостевой портал не может возвратиться, ключи сеанса для шифрования как он делает с Протоколом EAP.

Аутентификация внешнего пользователя (RADIUS)

Это только допустимо для Локального WebAuth, когда WLC обрабатывает учетные данные, или когда включена веб-политика Уровня 3. Можно тогда или аутентифицировать пользователей локально на WLC или внешне через RADIUS.

Существует заказ, в котором WLC проверяет для учетных данных пользователя.

1. В любом случае это сначала смотрит в его собственной базе данных.
2. Если это не находит пользователей там, это переходит к серверу RADIUS, настроенному в гостевом WLAN (если существует настроенный тот).
3. Это тогда регистрируется в глобальном списке сервера RADIUS против серверов RADIUS, где проверен **пользователь сети**.

Эта третья точка очень важна и отвечает на вопрос многих, кто не настраивает RADIUS для того WLAN, но замечает, что это все еще проверяет против RADIUS, когда пользователь не найден на контроллере. Это вызвано тем, что **пользователь сети** проверен против ваших

серверов RADIUS в глобальном списке.

WLC может аутентифицировать пользователей на сервере RADIUS с Протоколом аутентификации пароля (PAP), Протоколом аутентификации по квитированию вызова (CHAP) или EAP-MD5 (сообщение Digest5). Это - глобальный параметр и конфигурируемо от GUI или CLI:

От GUI: перейдите к **Контроллеру> веб-Проверка подлинности RADIUS**

От CLI: введите **RADIUSauth <pap|chap|md5chap> пользовательской сети config**

Примечание: Гостевой сервер NAC только использует PAP.

Как установить Проводной Гостевой WLAN

Легко настроить и очень близко к беспроводной гостевой конфигурации. Можно настроить его с одним или двумя контроллерами (только если каждый - автопривязка).

Выберите VLAN в качестве VLAN, в которую вы размещаете соединенных проводом гостей, например, на VLAN 50. Когда проводной гость будет хотеть получить доступ к Интернету, включите портативный ПК к порту на коммутаторе, настроенном для VLAN 50. Этот VLAN 50 должен быть позволен и подарок на пути через магистральный порт WLC. В случае двух WLC (одна привязка и одна внешняя), этот проводной гостевой VLAN должен привести к внешнему WLC (названный WLC1) а не к привязке. WLC1 тогда заботится о туннелировании трафика к WLC DMZ (привязка, названная WLC2), который освобождает трафик в протрассированной сети.

Вот пять шагов для настройки гостевого доступа к проводной сети:

1. **Настройте динамический интерфейс (VLAN) для проводного доступа гостя.**

   На WLC1 создайте динамический интерфейс VLAN50. На странице **конфигурации интерфейса** установите **Гостевой** флажок **LAN**. Затем исчезают поля, такие как **IP-адрес** и **шлюз**. Единственная вещь, которую ваш WLC должен знать об этом интерфейсе, состоит в том, что трафик маршрутизируется от VLAN 50. Эти клиенты являются соединенными проводом гостями.

2. **Создайте проводную LAN для доступа гостя.**

   На контроллере интерфейс используется, когда привязано к WLAN. Действие второе должно создать WLAN на ваших контроллерах главного офиса. Перейдите к **WLAN** и нажмите **New**. В **Типе WLAN** выберите **Guest LAN**.

   В **Имени профиля** и **SSID WLAN**, введите имя, которое определяет этот WLAN. Эти названия могут быть другими, но не могут содержать пробелы. Термин WLAN использован, но этот сетевой профиль не отнесен к профилю беспроводной сети.

   Вкладка Общие предлагает два выпадающих списка: **Вход** и **Выход**. Вход является VLAN, из которой пользователи происходят (VLAN 50); Выход является VLAN, к которой вы хотите передать им.

Для **Входа** выберите **VLAN50**.

Для **Выхода** это является другим. Если у вас есть только один контроллер, необходимо создать другой динамический интерфейс, **стандартный** на этот раз (не гостевая LAN), и вы передаете вашим проводным пользователям к этому интерфейсу. В этом случае передайте им к контроллеру DMZ. Поэтому для **Исходящего интерфейса**, выберите **Management Interface**.

Режимом безопасности для этой Гостевой LAN "WLAN" является WebAuth, который приемлем. Нажмите **Ok** для проверки.

3. **Настройте внешний контроллер (главный офис).**

   Из **списка WLAN** нажмите **Mobility Anchor** в конце **Гостевой** линии **LAN** и выберите свой контроллер DMZ. Предполагается здесь, что оба контроллера знают друг друга. Если они еще не знают друг друга, переходят **к Контроллеру> менеджмент Мобильности> Группа мобильности** и добавляют **DMZWLC** на WLC1. Затем добавьте **WLC1** на DMZ. Оба контроллера не должны быть в той же группе мобильности. В противном случае правила базовых мер безопасности нарушены.

4. **Настройте якорный контроллер (контроллер DMZ).**

   Ваш контроллер главного офиса готов. Теперь необходимо подготовить контроллер DMZ. Откройте сеанс web-браузера для своего контроллера DMZ и перейдите к **WLAN**. Создайте новый WLAN. В **Типе WLAN** выберите **Guest LAN**.

   В **Имени профиля** и **SSID WLAN**, введите имя, которое определяет этот WLAN. Используйте те же значения, как введено контроллер главного офиса.

   Входной интерфейс здесь не **Ни один**. Это фактически не имеет значения, потому что трафик получен через Ethernet по IP (EoIP) туннель. Это - то, почему вы не должны задавать Входной интерфейс.

   Исходящий интерфейс является тем, на котором клиенты, как предполагается, передаются. Например, **VLAN DMZ** является VLAN 9. Создайте стандартный динамический интерфейс для VLAN 9 на вашем DMZWLC, затем выберите **VLAN 9** в качестве Исходящего интерфейса.

   Необходимо настроить конец туннеля Привязки к Мобильности. Из **списка WLAN** выберите **Mobility Anchor for Guest LAN**. Передайте трафик к локальному контроллеру, **DMZWLC**. Оба конца теперь готовы.

5. **Подстройте гостевую LAN.**

   Можно также подстроить параметры настройки WLAN на обоих концах. Будьте осторожны, параметры настройки должны быть идентичными на обоих концах. Например, если вы принимаете решение нажать во **Вкладке Дополнительно WLAN**,

Позволить замену AAA на WLC1, необходимо установить тот же флажок на DMZWLC. Если существуют какие-либо различия в выборах в WLAN с обеих сторон, туннельных разрывах. DMZWLC отказывается от трафика; вы видите **при выполнении debug mobility**.

Следует иметь в виду, что все значения фактически получены из DMZWLC: IP-адреса, значения VLAN, и так далее. Настройте сторону WLC1 тождественно, так, чтобы она передала запрос к WLCDMZ.

Сертификаты для страницы входа

Этот раздел предоставляет процессы, которых необходимо придерживаться, если вы хотите поместить свой собственный сертификат на странице WebAuth, или если вы хотите скрыть 1.1.1.1 WebAuth URL и отобразить именованный URL.

Загрузите сертификат для web-аутентификации контроллера

Через GUI (**WebAuth> Сертификат**) или CLI (передача вводят **webauthcert**) можно загрузить сертификат на контроллере. Является ли это сертификатом, вы создали со своим центром сертификации (CA) или независимым поставщиком официальный сертификат, это должно быть в формате .pem. Перед передачей необходимо также ввести ключ сертификата.

После загрузки перезагрузка требуется для сертификата существовать. После того, как перезагруженный, перейдите к странице сертификата WebAuth в GUI, и это показывает вам подробные данные сертификата, который вы загрузили (законность и так далее). Важное поле является общим именем (CN), которое является названием, выполненным к сертификату. Это поле обсуждено в этом документе под разделом "Центр сертификации и Другие Сертификаты на Контроллере".

После того, как вы перезагрузили и проверили подробные данные сертификата, вам предоставляют новый сертификат контроллера на странице входа WebAuth. Однако может быть две ситуации.

1. Если ваш сертификат был выполнен одним из нескольких основных узлов CA, которым доверяет каждый компьютер, то это хорошо. Примером является VeriSign, но вы обычно подписываетесь Verisign подCA а не узлом CA. Можно зарегистрироваться хранилище сертификата браузера, если вы видите, что CA упомянул там, как доверяется.

2. Если вы получили свой сертификат от меньшей компании/CA, все компьютеры не доверяют им. Необходимо предоставить КОМПАНИЮ/СЕРТИФИКАТ CA клиенту также, и надо надеяться один из узлов CA выполнит тот сертификат. В конечном счете вы заканчиваете с цепочкой, такой как "Сертификат, был выполнен CA x> CA x, сертификат был выполнен CA y> CA y, сертификат был выполнен этим Trusted Root CA". Конечная цель должна достигнуть CA, которому действительно доверяет клиент.

Центр сертификации и другие сертификаты на контроллере

Чтобы быть избавленным от предупреждения "этого сертификата, не доверяется",

необходимо также ввести сертификат CA, который выполнил сертификат контроллера на контроллере. Затем контроллер представляет оба сертификата (сертификат контроллера и его сертификат CA). Сертификат CA должен быть доверяемым CA или имеет ресурсы для проверки CA., можно фактически создать цепочку сертификатов CA, которые приводят к доверяемому CA на вершине.

Необходимо разместить всю цепочку в тот же файл. Это означает, что ваш файл содержит содержание, такое как данный пример:

```
BEGIN CERTIFICATE ------ device certificate*   END CERTIFICATE ------ BEGIN
CERTIFICATE ------ intermediate CA certificate* END CERTIFICATE ------ BEGIN
CERTIFICATE ------ Root CA certificate* END CERTIFICATE ------
```

Как заставить сертификат совпадать с URL

WebAuth URL установлен в 1.1.1.1 для аутентификации себя, и сертификат выполнен (это - поле CN сертификата WLC). Если вы хотите изменить WebAuth URL на 'myWLC.com', например, войдите **в конфигурацию виртуального интерфейса** (эти 1.1.1.1 интерфейса), и там можно ввести **действительное Имя хоста DNS**, такое как myWLC.com. Это заменяет 1.1.1.1 в вашей панели URL. Это название должно также быть разрешимым. Отслеживание средств прослушивания показывает, как все это работает, но когда WLC передает страницу входа, WLC показывает адрес myWLC.com, и клиент решает это название с их DNS. Это название должно решить как 1.1.1.1. Это означает, что, если вы также используете название для управления WLC, необходимо использовать другое имя для WebAuth. Другими словами, при использовании myWLC.com, сопоставленного с управлением IP-адресами WLC необходимо использовать другое имя для WebAuth, такого как myWLCwebauth.com.

Решите проблемы сертификата

Этот раздел объясняет, как и что проверить для решения проблем сертификата.

Как проверить

Можно загрузить OpenSSL (для Windows, поиск Win32 OpenSSL) и установить его. Без любой конфигурации можно войти в каталог Bin и попробовать **openssl s_client - подключают** www mywebauthpage.com:443, если этот URL является URL, где страница WebAuth связана на DNS. См., "Что Проверить" раздел этого документа для примера.

Если ваши сертификаты используют частный CA, необходимо разместить Корневой сертификат CA в каталог на локальном компьютере и использовать openssl опцию**-CApath**. Если у вас есть Промежуточное звено CA, необходимо поместить его в тот же каталог также.

Для получения общей информации о сертификате и проверять его, используйте:

```
openssl x509 -in certificate.pem -noout -text
openssl verify certificate.pem
```

Могло бы быть также полезно преобразовать сертификаты с использованием openssl:

```
openssl x509 -in certificate.der -inform DER -outform PEM -out certificate.pem
```

Что следует проверить

Вы видите то, какие сертификаты передаются клиенту, когда это соединяется. Считайте сертификат устройства — CN должен быть URL, где веб-страница достижима. Читайте “выполненный” линией сертификата устройства. Это должно совпасть с CN второго сертификата. Затем этот второй сертификат, “выполненный”, должен совпасть с CN следующего сертификата и так далее. В противном случае это не делает реальную цепочку. В выходных данных OpenSSL, показанных здесь, вы видите, что **openssl** не может проверить сертификат устройства, потому что его “выполненный” не совпадает с названием предоставленного сертификата CA.

Выходные данные SSL

```
Loading 'screen' into random state - done CONNECTED(00000760) depth=0 /O=
<company>.ac.uk/OU=Domain Control Validated/CN=<company>.ac.uk verify error:
num=20:unable to get local issuer certificate verify return:1 depth=0 /O=
<company>.ac.uk/OU=Domain Control Validated/CN=<company>.ac.uk verify error:
num=27:certificate not trusted verify return:1 depth=0 /O=<company>.ac.uk/OU=
Domain Control Validated/CN=<company>.ac.uk verify error:num=21:
unable to verify the first certificate verify return:1 --- Certificate chain
0 s:/O=<company>.ac.uk/OU=
Domain Control Validated/CN=<company>.ac.uki:/C=US/ ST=
Arizona/L=Scottsdale/O=.com/OU=http://certificates.gocompany.com/repository/CN=
Secure Certification Authority/serialNumber=079
692871 s:/C=US/O=Company/OU=Class 2 Certification Authority
i:/C=US/O=Company/OU=Class 2 Certification Authority --- Server certificate

BEGIN CERTIFICATE-----
MIIE/zCCA+egAwIBAgIDRc2iMA0GCSqGSIb3DQEBBQUAMIHKMQswCQYDVQQGEwJV
output cut*
YMaj/NACviEU9J3iot4sfreCQSKkBmjH0kf/Dg1l0kmdSbc=

END CERTIFICATE-----
subject=/O=<company>.ac.uk/OU=Domain Control Validated/CN=<company>c.ac.uk
issuer=/C=US/ST=Arizona/L=Scottsdale/O=.com/OU=http://certificates.
.com/repository/CN=Secure Certification Authority/serialNumber=0
7969287 --- No client certificate CA names sent --- SSL handshake has read
2476 bytes and written 322 bytes --- New, TLSv1/SSLv3, Cipher is AES256-SHA
Server public key is 1024 bit Compression: NONE Expansion: NONE SSL-Session:

Protocol : TLSv1
Cipher : AES256-SHA
Session-ID: A32DB00A7AB7CD1CEF683980F3696C2BBA31A1453324F711F50EF4B86A4A7F03

Session-ID-ctx:Master-Key: C95E1BDAC7B1A964ED7324955C985CAF186B92EA34CD69E10
5F95D969D557E19
939C6A77C72350AB099B3736D168AB22

Key-Arg : None
Start Time: 1220282986
Timeout : 300 (sec)
Verify return code: 21 (unable to verify the first certificate)
---
```

Другая возможная проблема является сертификатом, не может быть загружен к контроллеру. В этой ситуации нет никакого вопроса законности, CA, и так далее. Для проверки этого вы можете первая проверка подключение Протокола TFTP и попытка передать файл конфигурации. Затем при вводе **команды debug transfer all enable** вы видите, что проблемой является установка сертификата. Это могло произойти из-за неправильного ключа, используемого с сертификатом. Могло также случиться так, что сертификат находится в неправильном формате или поврежден.

Cisco рекомендует сравнить содержание сертификата с известным, подтвержденным

сертификатом. Это позволяет вам видеть, показывает ли атрибут **LocalkeyID** весь 0s (уже произошел). Если так, тогда сертификат должен быть повторно преобразован. Существует две команды с OpenSSL, которые позволяют вам возвращаться от .pem до .p12, и затем переиздавать .pem с ключом по Вашему выбору.

Предварительный шаг: Если вы получили .pem, который содержит сертификат, придерживавшийся ключом, скопировать/вставить ключевая часть:**----BEGIN КЛЮЧЕВОЙ---- до-------КЛАВИША END------**от .pem в "key.pem".

1. **pkcs12 openssl - экспорт - в certificate.pem-inkey key.pem - newcert.p12**? Вам предлагают с ключом; введите **check123**.

2. **pkcs12 openssl - в newcert.p12 - workingnewcert.pem-passin pass:check123-passout pass:check123** Это приводит к в рабочем состоянии .pem с **паролем check123**.

Другие ситуации для устранения проблем

Несмотря на то, что **привязка к мобильности** не была обсуждена в этом документе, если вы находитесь в **привязанной гостевой** ситуации, удостоверьтесь, что обмен мобильности происходит правильно и что вы видите, что клиент поступает в привязку. Для дальнейших проблем WebAuth нужно устранение неполадок на привязке.

Вот некоторые общие проблемы, которых можно устранить неполадки:

- **Пользователи не могут связаться к гостевому WLAN**.

  Это не отнесено к WebAuth. Проверьте конфигурацию клиента, параметры безопасности на WLAN, если это включено, и являются ли радио активными и действующими и так далее.

- **Пользователи не получают IP-адрес**.

  В гостевой ситуации с привязкой это чаще всего, потому что внешнее и привязки не были настроены точно тот же путь. В противном случае проверьте конфигурацию DHCP, подключение, и так далее. Подтвердите, могут ли другие WLAN использовать тот же сервер DHCP без проблемы. Это все еще не отнесено к WebAuth.

- **Пользователь не перенаправлен к странице входа**.

  Это - наиболее распространенный признак, но более точно. Существует два возможных сценария.

  Пользователь не перенаправлен (пользователь вводит URL и никогда не достигает страницы WebAuth). Для этой ситуации проверьте:

  то, что допустимый сервер DNS был назначен на клиента через DHCP (**ipconfig / все**),

  то, что DNS достижим от клиента (**nslookup** www.website.com),

то, что пользователь ввел допустимый URL, чтобы быть перенаправленным,

то, что пользователь пошел на HTTP URL на порту 80 (например, для достижения ACS с http://, localhost:2002 не перенаправляет вас, так как вы передали на порту 2002 вместо 80).

Пользователь перенаправлен к 1.1.1.1 правильно, но не отображается сама страница.

Эта ситуация наиболее вероятна или проблема WLC (дефект) или клиентская проблема. Могло случиться так, что у клиента есть некоторый межсетевой экран или блокирующееся программное обеспечение или политика. Также могло случиться так, что они настроили прокси в своем web-браузере.

Рекомендация: Возьмите отслеживание средств прослушивания на клиентском компьютере. Нет никакой потребности в специальном программном обеспечении wireless, только Wireshark, который работает на беспроводном адаптере и показывает вам если ответы WLC и попытки перенаправить. У вас есть две возможности: или от WLC нет никакого ответа, или что-то неправильно с подтверждением связи SSL для страницы WebAuth. Для проблемы подтверждения связи SSL можно проверить, обеспечивает ли пользовательский браузер SSLv3 (некоторые только позволяют SSLv2), и если это слишком агрессивно на Проверке сертификата.

Это - общий шаг для ручного ввода http://1.1.1.1, чтобы проверить, появляется ли веб-страница без DNS. Фактически, можно ввести http://6.6.6.6 и получить тот же эффект. WLC перенаправляет любой IP-адрес, который вы вводите. Поэтому при вводе http://1.1.1.1 он не заставляет вас обойти веб-перенаправление. При вводе https://1.1.1.1 (безопасный) это не работает, потому что WLC не перенаправляет Трафик HTTPS (по умолчанию, это фактически возможно в Версии 8.0 и позже). Лучший способ загрузить страницу непосредственно без перенаправления состоит в том, чтобы ввести https://1.1.1.1/login.html.

- **Пользователи не могут аутентифицироваться**.

  Посмотрите раздел этого документа, который обсуждает аутентификацию. Проверьте учетные данные локально на RADIUS.

- **Пользователи могут успешно аутентифицироваться через WebAuth, но у них нет доступа в Интернет впоследствии**.

  Можно удалить WebAuth из безопасности WLAN, и затем у вас должен быть открытый WLAN. Можно тогда попытаться обратиться к сети, DNS и так далее. Если вы испытываете проблемы там также, удаляете параметры настройки WebAuth в целом и проверяете вашу конфигурацию интерфейсов.

Дополнительные сведения см. в: Устранение проблем web-аутентификации на контроллере беспроводной локальной сети (WLC).

Прокси-сервер HTTP и Как это Работает

Можно использовать Прокси-сервер HTTP. Если вам нужен клиент для добавления исключения в его браузере, который 1.1.1.1 не должен проходить прокси-сервер, можно заставить WLC прислушаться к трафику HTTP на порту прокси-сервера (обычно 8080).

Для понимания этого сценария необходимо знать то, что делает HTTP прокси. Это - что-то, что вы настраиваете на клиентской стороне (IP-адрес и порт) в браузере.

Обычный сценарий, когда пользователь посещает веб-сайт, должен решить название к IP с DNS, и затем это спрашивает веб-страницу на Web-сервер. Процесс должен всегда передавать запрос HTTP за страницей к прокси. Прокси обрабатывает DNS при необходимости и вперед на Web-сервер (если страница уже не кэшируется на прокси). Обсуждение является клиентом к прокси только. Получает ли прокси реальную веб-страницу, не важно клиенту.

Вот процесс веб-аутентификации:

- Пользователь вводит в URL.
- Клиентский компьютер передает к Прокси-серверу.
- Точки пересечения WLC и IP Прокси-сервера спуфинга; это отвечает на ПК с перенаправлением к 1.1.1.1.

На данном этапе, если ПК не настроен для него, это просит страницу 1.1.1.1 WebAuth к прокси, таким образом, это не работает. ПК должен сделать исключение для 1.1.1.1; тогда это передает запрос HTTP к 1.1.1.1 и продолжает WebAuth. Когда аутентифицируется, вся связь проходит прокси снова. Конфигурация исключения обычно находится в браузере близко к конфигурации прокси-сервера. Необходимо видеть сообщение: "Не используйте прокси для тех IP-адресов".

С Выпуском 7.0 WLC и позже, опция **webauth перенаправление прокси** может быть активирована в глобальных параметрах конфигурации WLC. Когда включено, WLC проверяет, настроены ли клиенты для ручного использования прокси. В этом случае они перенаправляют клиента к странице, которая показывает им, как модифицировать их параметры прокси, чтобы заставить все работать. Перенаправление прокси WebAuth может быть настроено для работы на множество портов и совместимо с Центральной веб-аутентификацией.

Для примера на перенаправлении прокси WebAuth обратитесь к Прокси-серверу веб-аутентификации на Примере конфигурации Контроллера беспроводной локальной сети.

Web-аутентификация на HTTP вместо HTTPS

Можно войти на web-аутентификации на HTTP вместо HTTPS. Если вы входите на HTTP, вы не получаете предупреждения сертификата.

Для ранее, чем код Выпуска 7.2 WLC, необходимо отключить управление HTTPS WLC и управление HTTP выхода. Однако это только разрешает управление web WLC по HTTP.

Для кода Выпуска 7.2 WLC используйте **веб-аутентификацию сети config secureweb, отключают** команду для отключения. Это только отключает HTTPS для web-аутентификации а не управления. Обратите внимание на то, что это требует перезагрузки контроллера!

На Выпуске 7.3 WLC и коде следующих версий, вы можете HTTPS позволить/запретить для WebAuth только через GUI и CLI.

Дополнительные сведения

- Пример настройки веб-аутентификации контроллера беспроводной LAN
- Загрузите программное обеспечение для контроллера беспроводной локальной сети Бандлы WebAuth
- Создание специализированной страницы для входа в веб-аутентификацию
- Пример настройки контроллера беспроводной сети с внешней веб-аутентификацией
- Пример настройки транзитного веб-шлюза контроллера беспроводной LAN
- Использование GUI для Настройки веб-перенаправления
- Использование CLI для Настройки веб-перенаправления
- Устранение проблем web-аутентификации на контроллере беспроводной локальной сети (WLC)
- Прокси-сервер веб-аутентификации на примере конфигурации контроллера беспроводной локальной сети
- Запросы комментариев (RFC)
- Cisco Systems – техническая поддержка и документация