Устранение проблем web-аутентификации на контроллере беспроводной локальной сети (WLC)

Содержание

Введение

Этот документ предоставляет советы для решения проблем web-аутентификации в среде Контроллера беспроводной локальной сети (WLC).

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Знание Протокола LWAPP / Контроль и Инициализация Точек беспроводного доступа (CAPWAP)
- Знание настройки Облегченной точки доступа (LAP) и WLC для главной операции.
- Базовые знания о web-аутентификации web-аутентификации и настройки на WLC. Для получения информации о настройке web-аутентификации на WLC обратитесь к Примеру настройки веб-аутентификации в контроллере беспроводной сети LAN.

Используемые компоненты

Сведения в этом документе основываются на WLC 5500, который выполняет версию микропрограммы 7.0.98.0.

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.

Родственные продукты

Этот документ может также использоваться с этими аппаратными средствами:

- Контроллеры беспроводной локальной сети Cisco серии 5500
- Контроллеры беспроводных LAN серии Cisco 4400
- Cisco 4100 Series Wireless LAN Controllers
- Контроллеры беспроводной сети Cisco серии 2500
- Cisco 2100 Series Wireless LAN Controllers
- Контроллеры беспроводных LAN серии Cisco 2000
- Cisco Airespace 3500 Series WLAN Controller
- Cisco 4000 Series Wireless LAN Controller
- Cisco Wireless LAN Controller Module
- Cisco Catalyst 6500 Series Wireless Services Module (WiSM)
- Контроллеры беспроводной локальной сети Cisco Flex серии 7500
- Сервисный модуль беспроводной сети Cisco 2 (WiSM2)
- Cisco Catalyst 3750 Series Integrated Wireless LAN Controllers

Условные обозначения

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

Web-аутентификация на WLC

Web-аутентификация является функцией безопасности уровня 3, которая заставляет контроллер не позволять IP - трафик, кроме связанных с DHCP пакетов / связанные с DNS пакеты, от конкретного клиента, пока тот клиент правильно не предоставил допустимое имя пользователя и пароль за исключением трафика, позволенного через Предподлинный ACL. Web-аутентификация является единственной политикой безопасности, которая позволяет клиенту получать IP-адрес перед Аутентификацией. Это - метод простой проверки подлинности без потребности в соискателе или служебной программе клиента. Web-аутентификация может быть сделана или локально на WLC или по серверу RADIUS. Web-аутентификация, как правило, используется клиентами, которые хотят развернуть сеть гостевого доступа.

Когда контроллер перехватывает первый HTTP TCP (порт 80) пакет GET от клиента, web-аутентификация запускается. Для web-браузера клиента для получения настолько далеко клиент должен сначала получить IP-адрес и сделать трансляцию URL к IP-адресу (Разрешение DNS) для web-браузера. Это позволяет web-браузеру знать который IP-адрес передать GET HTTP.

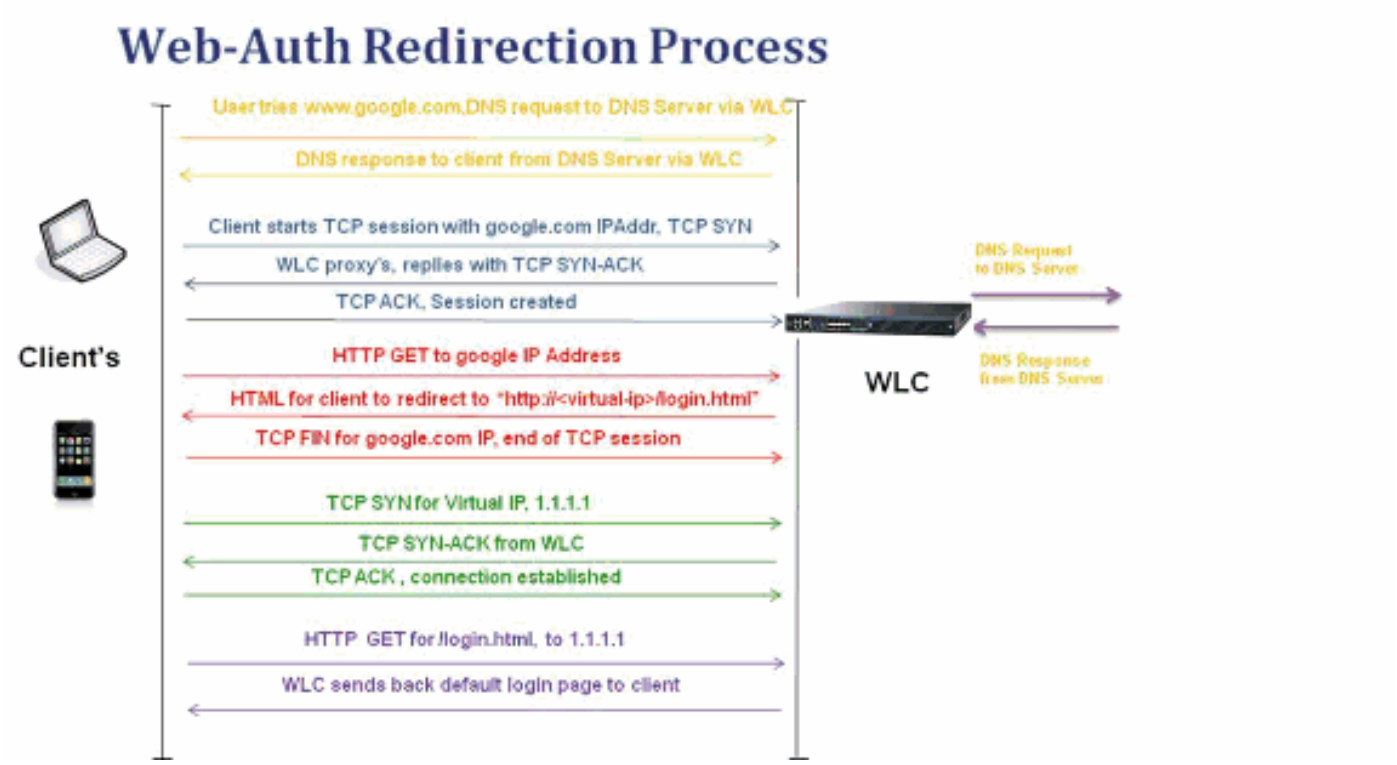
Когда web-аутентификация настроена на WLAN, контроллер блокирует весь трафик (пока процесс проверки подлинности не завершен) от клиента, за исключением DHCP и трафика DNS. Когда клиент передает первый GET HTTP к порту TCP 80, контроллер перенаправляет клиента к https:1.1.1.1/login.html для обработки. Этот процесс в конечном счете переводит

веб-страницу входа в систему в рабочее состояние.

Примечание: При использовании внешнего веб-сервера для web-аутентификации некоторым платформам WLC нужен ACL процедур, предшествующих аутентификации для внешнего веб-сервера, который включает Контроллер серии 5500 Cisco, Cisco Контроллер серии 2100, серия Cisco 2000 и модуль контроллерной сети. Для других платформ WLC ACL процедур, предшествующих аутентификации не является обязательным.

Примечание: Но, это - полезный прием для настройки ACL процедур, предшествующих аутентификации для внешнего веб-сервера при использовании внешней веб-аутентификации.

Этот раздел объясняет процесс переадресации Web-аутентификации подробно.



- Вы открываете web-браузер и тип в URL, например, `http://www.google.com`. Клиент отсылает запрос DNS для этого URL для получения IP для назначения. WLC обходит запрос DNS к серверу DNS, и сервер DNS отвечает назад ответом DNS, который содержит IP-адрес целевого `www.google.com`, который в свою очередь передан беспроводным клиентам
- Клиент тогда пытается открыть TCP - подключение с IP - адресом назначения. Это отсылает Пакет TCP SYN, предназначенный в IP-адрес `www.google.com`.
- WLC имеет правила, настроенные для клиента, и следовательно может действовать как прокси для `www.google.com`. Это передает пакет SYN-ACK TCP обратно клиенту с источником как IP-адрес `www.google.com`. Клиент передает пакет ACK TCP обратно для завершения трех способов, которыми полностью установлены квитирование TCP - подключения и TCP - подключение.
- Клиент передает пакет GET HTTP, предназначенный к `www.google.com`. WLC перехватывает этот пакет, передает его за обработкой перенаправления. Шлюз приложений HTTP готовит "тело" HTML и передает его обратно как ответ на GET HTTP, который запрашивает клиент. Этот HTML делает клиента, чтобы перейти к URL веб-

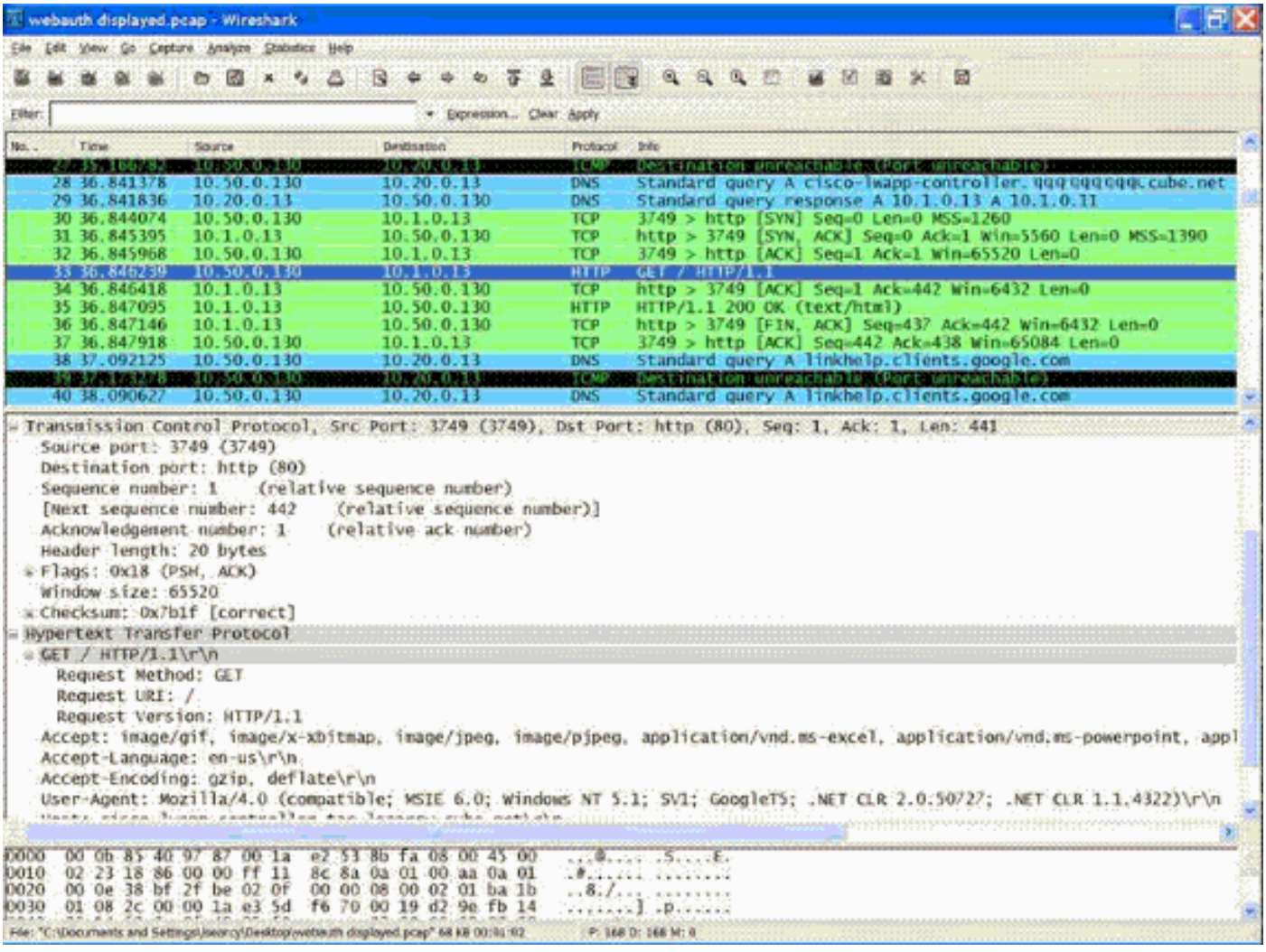
страницы по умолчанию WLC, например, `http://<Virtual-Server-IP>/login.html`.

- Клиент закрывает TCP - подключение с IP-адресом, например `www.google.com`.
- Теперь клиент хочет перейти `http://1.1.1.1/login.html` и таким образом, он пытается открыть TCP - подключение с виртуальным IP - адресом WLC. Это передает Пакет TCP SYN за 1.1.1.1 к WLC.
- WLC отвечает назад SYN-ACK TCP, и клиент передает ACK TCP обратно в WLC для завершения квитирования.
- Клиент передает GET HTTP за/login.html, предназначенным к 1.1.1.1 для запроса на страницу входа.
- Этот запрос позволен до Web-сервера WLC, и сервер отвечает назад страницей для входа по умолчанию. Клиент получает страницу входа на окне браузера, где пользователь может идти вперед и войти.

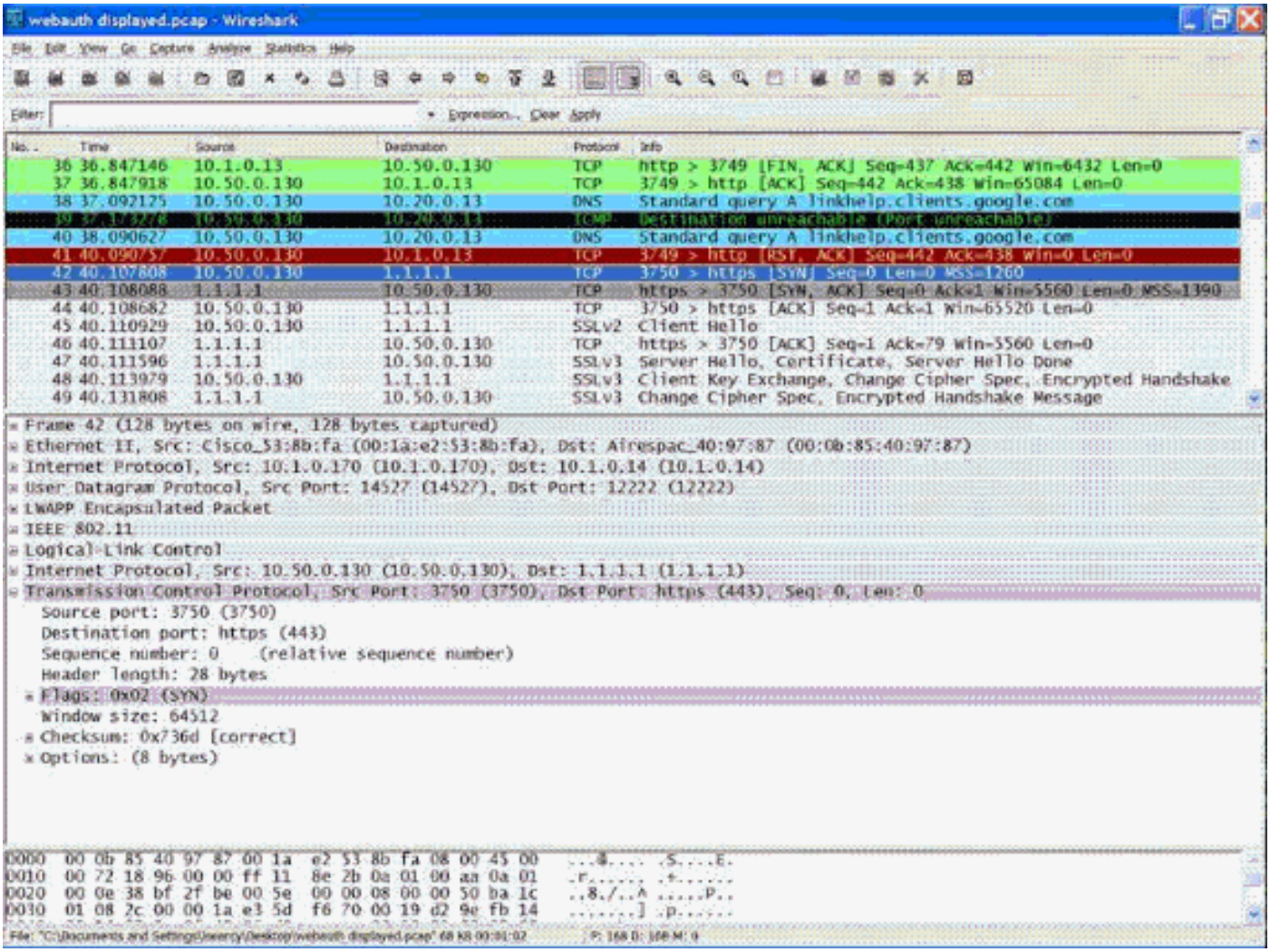
Например. В данном примере IP-адрес клиента 10.50.0.130. Клиент решил URL на Web-сервер, к которому он обращался 10.1.0.13. Как вы можете видеть клиент сделал трехэтапное квитирование для запуска TCP - подключения и затем передал пакет GET HTTP начиная с пакета 30. Контроллер перехватывает пакеты и отвечает с кодом 200. Пакет кода 200 имеет URL перенаправления в нем:

```
<HTML><HEAD><TITLE>Cisco Systems Inc. Web Authentication Redirect</TITLE><META
http-equiv="Cache-control" content="no-cache"><META http-equiv="Pragma"
content="no-cache"><META http-equiv="Expires" content="-1"><META http-equiv="refresh"
content="1; URL=https://1.1.1.1/login.html?redirect=cisco-lwapp-controller.qqq.qqqqq.
cube.net/"></HEAD></HTML>
```

Это тогда закрывает TCP - подключение посредством трехэтапного квитирования.



Клиент тогда запускает Подключение HTTPS к URL перенаправления, который передает его к этим 1.1.1.1, который является виртуальным IP - адресом контроллера. Клиент должен проверить серверный сертификат или проигнорировать его для внедрения туннеля SSL. В этом случае это - подписанный сертификат, таким образом, клиент проигнорировал его. Веб-страница входа в систему передается через этот туннель SSL. Пакет 42 начинает транзакции.



У вас есть опция для настройки доменного имени для виртуального IP - адреса Контроллера беспроводной локальной сети. При настройке доменного имени для виртуального IP - адреса это доменное имя возвращено в пакете OK HTTP из контроллера в ответ на пакет GET HTTP от клиента. Тогда необходимо выполнить Разрешение DNS для этого доменного имени и как только это получает IP-адрес из Разрешения DNS, это пытается открыть сеанс TCP с тем IP-адресом, который является IP, настроенным на виртуальном интерфейсе контроллера.

В конечном счете веб-страницу передают через туннель клиенту, и пользователь передает имя пользователя/пароль обратно через туннель SSL.

Web-аутентификация выполнена одним из этих трех методов:

- Web-аутентификация с помощью страницы Внутренней сети (по умолчанию).. См. Выбор Default Web Authentication Login Page для получения дополнительной информации об использовании страницы веб-страницы по умолчанию.
- Web-аутентификация с помощью Настроенной страницы для входа. См. Создание

Специализированной Страницы для входа в веб-аутентификацию для получения дополнительной информации о том, как использовать Настроенную страницу для входа.
- Web-аутентификация с помощью страницы входа от внешнего веб-сервера. См. Использование Специализированной Страницы для входа в веб-аутентификацию от Внешнего веб-сервера для получения дополнительной информации о том, как использовать страницу входа от внешнего веб-сервера.

Примечание: Специализированная веб-подлинная связка (bundle) имеет предел до 30 символов для имен файлов. Гарантируйте, что никакие имена файлов в связке (bundle) не больше, чем 30 символов.

Примечание: От выпуска 7.0 WLC и далее, если Web-аутентификация включена на WLAN и у вас также есть правила списка прав доступа (ACL) ЦП, клиент базировался, правила Web-аутентификации всегда берут более высокий приоритет, пока клиент является не прошедшим поверку подлинности в состоянии `WebAuth_Reqd`. Как только клиент переходит к состоянию , правила списка прав доступа (ACL) ЦП применены.

Примечание: Поэтому, Если ACL ЦП включены в WLC, позволять правило для IP виртуального интерфейса требуется (В направлении ANY) в этих условиях:

- Когда ACL ЦП не имеет позволять правила ALL для обоих направлений.
- Когда там существует позволять правило ALL, но там также существует ЗАПРЕЩАТЬ правило для порта 443 или 80 более высокого приоритета.

Примечание: Позволять правило для виртуального IP должно быть для протокола TCP и порта 80, если secureweb отключен, или порт 443, если включен secureweb. Когда ACL ЦП существуют, это необходимо для предоставления доступа клиента к успешной аутентификации поста IP-адреса виртуального интерфейса.

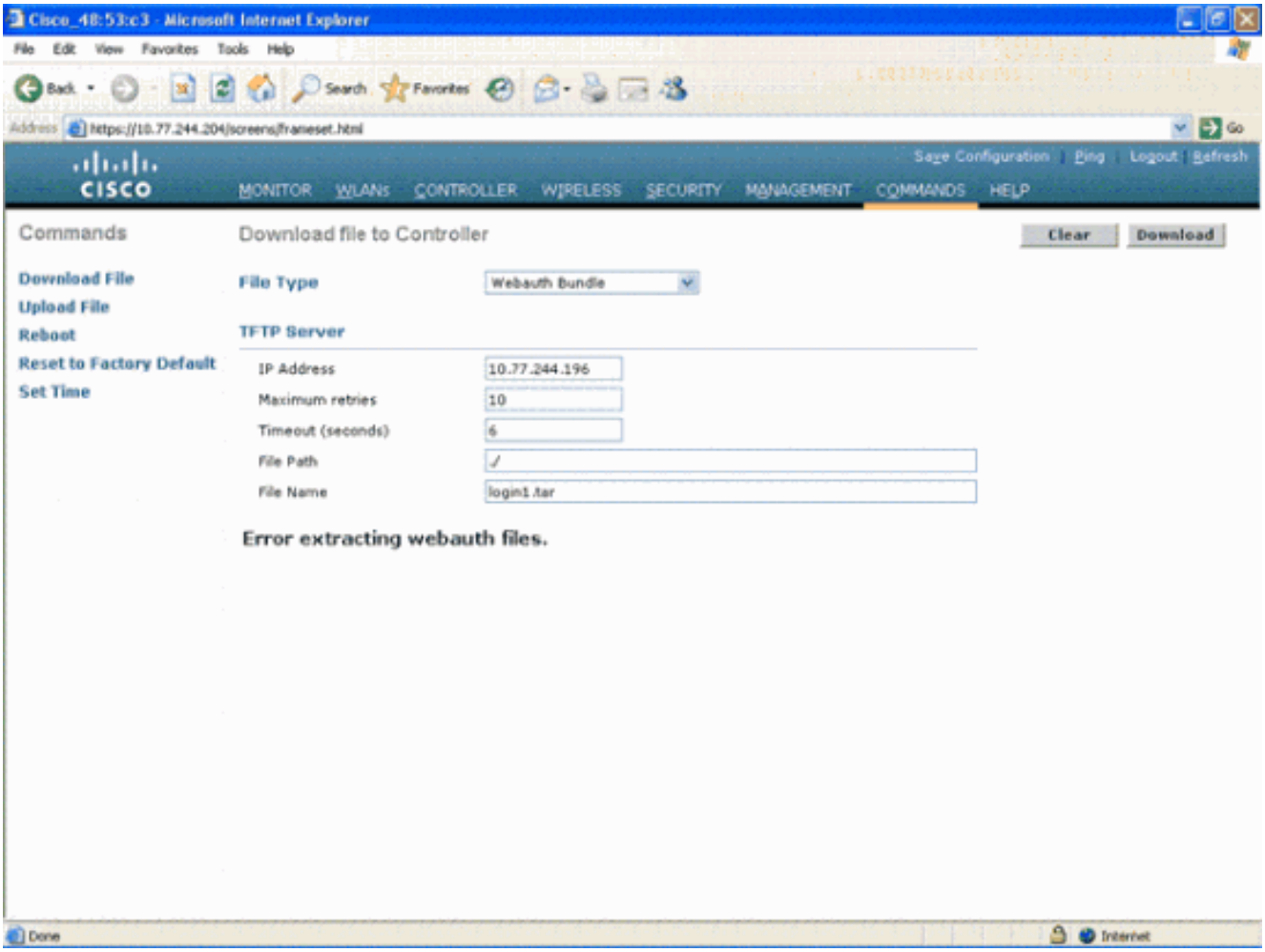
Устранение проблем web-аутентификации

После настройки web-аутентификации если функция не работает как ожидалось, завершите эти действия по устранению проблем:

1. Проверьте, получает ли клиент IP-адрес. В противном случае пользователи могут снять флажок **с DHCP, Требуемым** на WLAN, и дать беспроводному клиенту статический IP - адрес. Это принимает ассоциацию с точкой доступа. См. *IP-адресацию выполняет* раздел *Устранения проблем Клиентов выдал в единой беспроводной сети Cisco (UWN) для устранения проблем связанных проблем DHCP*.
2. На версиях WLC ранее, чем 3.2.150.10, необходимо вручную ввести **https://1.1.1.1/login.html** для навигации к окну web-аутентификации.Следующим шагом в процессе является Разрешение DNS URL в web-браузере. Когда клиент WLAN соединяется с WLAN, настроенным для web-аутентификации, клиент получает IP-адрес из сервера DHCP. Пользователь открывает web-браузер и вводит адрес веб-сайта. Клиент тогда выполняет Разрешение DNS для получения IP-адреса веб-сайта. Теперь, когда клиент пытается достигнуть веб-сайта, WLC перехватывают HTTP, Получают сеанс клиента, и перенаправляет пользователя к странице для входа в веб-аутентификацию.
3. Поэтому гарантируйте, что клиент в состоянии выполнить Разрешение DNS для перенаправления для работы. На Windows выберите **Start> Run**, введите **cmd**, чтобы открыть окно командной строки и сделать “nslookup www. cisco . com" и видит,

возвращается ли IP-адрес.На Macs/Linux: откройте окно терминала и сделайте “nslookup www. cisco . com" и видит, возвращается ли IP-адрес.Если вы полагаете, что клиент не получает Разрешение DNS, вы можете также:Введите любого IP-адрес URL (например, http://www. cisco . com является http://198.133.219.25),Попытайтесь непосредственно достигнуть webauth страницы контроллера с https://<Virtual_interface_IP_Address>/login.html. Как правило, это - http://1.1.1.1/login.html.Ввод этого URL переводят веб-страницу в рабочее состояние? Если да, это наиболее вероятно Проблема DNS. Это могла бы также быть проблема сертификата. Контроллер, по умолчанию, использует подписанный сертификат, и большинство web-браузеров предупреждает против использования их.

4. Для web-аутентификации с помощью специализированной веб-страницы гарантируйте, что код HTML для специализированной веб-страницы является соответствующим.Можно загрузить типовой сценарий Web-аутентификации от Загрузок Программного обеспечения Cisco. Например, для этих 4400 контроллеров, выберите **Products> Wireless> Wireless LAN Controller> Standalone Controllers> Cisco 4400 Series Wireless LAN Controllers> Cisco 4404 Wireless LAN Controller> Software on Chassis> Wireless Lan Controller Web Authentication Bundle 1.0.1** и загрузите **webauth_bundle.zip** файл.Когда интернет-браузер пользователя перенаправлен к настроенной странице для входа, эти параметры добавлены к URL:ap_mac — MAC-адрес точки доступа, к которой привязан пользователь беспроводной связи.switch_url — URL контроллера, к которому должны быть зарегистрированы учетные данные пользователя.перенаправление — URL, к которому пользователь перенаправлен после аутентификации, успешен.код состояния — код статуса возвратился из сервера web-аутентификации контроллера.wlan — SSID WLAN, к которому привязан пользователь беспроводной связи.Это доступные коды статуса:Код статуса 1: "В вас уже входят. Никакие дальнейшие действия не требуются с Вашей стороны".Код статуса 2: "Вы не настроены для аутентификации против веб-портала. Никакие дальнейшие действия не требуются с Вашей стороны".Код статуса 3: "Заданное имя пользователя не может использоваться в это время. Возможно, в имя пользователя уже входят система?"Код статуса 4: "Вы были исключены".Код статуса 5: "Комбинация Имени пользователя и пароля, которую вы ввели, недопустима. Повторите попытку."
5. Все файлы и изображения, которые должны появиться на Специализированной веб-странице, должны быть связаны в файл .tar прежде, чем загрузить к WLC. Гарантируйте, что один из файлов, включенных в связку (bundle) tar, является login.html. Если вы не включаете login.html файл, вы получаете это сообщение об ошибках:



См. Рекомендации для Специализированного раздела Web-аутентификации Примера настройки веб-аутентификации в контроллере беспроводной сети LAN для получения дополнительной информации о том, как создать специализированное окно web-аутентификации.**Примечание:** Файлы, которые являются большими и файлы, которые имеют длинные имена, приведут к ошибке экстракции. Рекомендуется, чтобы изображения были в формате .jpg.

6. Internet Explorer 6.0 SP1 или позже является браузером, рекомендуемым для использования web-аутентификации. Другие браузеры могут или могут не работать.
7. Гарантируйте, что опция **Scripting** не заблокирована на клиентском браузере, поскольку специализированная веб-страница на WLC является в основном HTML-сценарием. На IE 6.0 это отключено по умолчанию для целей обеспечения безопасности.**Примечание:** Блокировщик всплывающих окон должен быть отключен на браузере при настройке каких-либо Всплывающих сообщений для пользователя.**Примечание:** Если вы переходите к узлу **https**, перенаправление не работает. См. идентификатор ошибки Cisco CSCar04580 (только зарегистрированные клиенты) для получения дополнительной информации.
8. Если вам настроили **имя хоста** для **виртуального интерфейса** WLC, удостоверьтесь, что Разрешение DNS доступно для имени хоста виртуального интерфейса.**Примечание:** Перейдите к меню **Controller> Interfaces** от GUI WLC для присвоения **Имени хоста DNS** на виртуальный интерфейс.
9. Иногда межсетевой экран, установленный на компьютере клиента, блокирует страницу для входа в веб-аутентификацию. Отключите межсетевой экран, прежде чем вы попытаетесь обратиться к странице входа. Межсетевой экран может быть включен снова, как только завершена web-аутентификация.

10. Межсетевой экран топологии/решения может быть размещен между клиентом и веб-сервером проверки подлинности, который зависит от сети. Что касается каждой организации сети / внедренное решение, конечный пользователь должен удостовериться, что эти порты позволены на межсетевом экране.
11. Для web-аутентификации для появления клиент должен сначала связаться к соответствующему WLAN на WLC. Перейдите к меню **Monitor> Clients** на GUI WLC, чтобы видеть, привязан ли клиент к WLC. Проверьте, есть ли у клиента действительный IP - адрес.
12. Отключите Параметры прокси на клиентском браузере, пока не будет завершена web-аутентификация.
13. Метод аутентификации веб-страницы по умолчанию является PAP. Гарантируйте, что Аутентификация PAP позволена на сервере RADIUS для этого работать. Для проверки статуса аутентификации клиента проверьте отладки и сообщения журнала от сервера RADIUS. Можно использовать **команду debug aaa all** на WLC для просмотра отладок от сервера RADIUS.
14. Обновите драйвер оборудования на компьютере к последнему коду от веб-сайта изготовителя.
15. Проверьте параметры настройки в соискателе (программа на портативном ПК).
16. То, когда вы используете соискателя Windows Zero Config, встроило в Windows:Проверьте, что пользователю установили последние исправления.Выполните отладки на соискателе.
17. На клиенте включите EAPOL (WPA+WPA2) и журналы RASTLS от окна командной строки, Пуска> Выполнить> cmd:`netsh ras set tracing eapol enable`
    `netsh ras set tracing rastls enable`Для отключения журналов выполните ту же команду, но замена включает с, отключают. Для XP все журналы будут расположены в C:\Windows\tracing.
18. Если вы все еще не имеете никакой веб-страницы входа в систему, собираете и анализируете эти выходные данные от одиночного клиента:`debug client <mac_address in format xx:xx:xx:xx:xx:xx>`
    ```
    debug dhcp message enable
    debug aaa all enable
    debug dot1x aaa enable
    debug mobility handoff enable
    ```
19. Если вопрос не решен после того, как вы выполняете эти шаги, собираете эти отладки и используете Инструмент запросов службы технической поддержки (TAC) (только зарегистрированные клиенты) для открытия Запроса на обслуживание.`debug pm ssh-appgw enable`
    ```
    debug pm ssh-tcp enable
    debug pm rules enable
    debug emweb server enable
    debug pm ssh-engine enable packet <client ip>
    ```

Дополнительные сведения

- Пример настройки веб-аутентификации контроллера беспроводной LAN
- Пример настройки контроллера беспроводной сети с внешней веб-аутентификацией
- Cisco Systems – техническая поддержка и документация