Настройте перенаправление HTTPS через веб-аутентификацию

Содержание

Введение

Этот документ описывает конфигурацию о перенаправлении web-аутентификации по HTTPS. Это - функция, представленная в выпуске 8.0 единой беспроводной сети Cisco (UWN) (CUWN).

Предварительные условия

Требования

Корпорация Cisco рекомендует ознакомиться со следующими темами:

- Базовые знания о web-аутентификации контроллера беспроводной локальной сети (WLC)
- Как настроить WLC для Web-аутентификации.

Используемые компоненты

Сведения в этом документе основываются на WLC серии 5500 Cisco, который выполняет версию микропрограммы 8.0 CUWN.

> **Примечание:** Конфигурация и веб-подлинное пояснение, предоставленное в этом документе, применимы ко всем моделям WLC и любому образу CUWN, равному или позже, чем 8.0.100.0.

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.

Общие сведения

Web-аутентификация является функцией безопасности уровня 3. Это блокирует всего IP/трафик данных, кроме связанных с DHCP пакетов / связанные с DNS пакеты, от конкретного клиента, пока беспроводной клиент не предоставил допустимое имя пользователя и пароль. 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 клиент передает первый GET HTTP к порту TCP 80, контроллер перенаправляет клиента к https: <виртуальный IP>/login.html для обработки. Этот процесс в конечном счете переводит веб-страницу входа в систему в рабочее состояние.

До версий ранее, чем CUWN 8.0 (т.е. до 7.6), если беспроводной клиент представляет страницу HTTPS (TCP 443), страница не перенаправлена к порталу web-аутентификации. Поскольку все больше веб-сайтов начинает использовать HTTPS, эта функция включена в CUWN 8.0 версий и позже. С этой функцией на месте, если беспроводной клиент пробует https://<веб-сайт>, он перенаправлен к веб-подлинной странице входа. Также эта функция очень полезна для устройств, которые передают запросы HTTPS с приложением (но не с браузером).

Ошибка сертификата

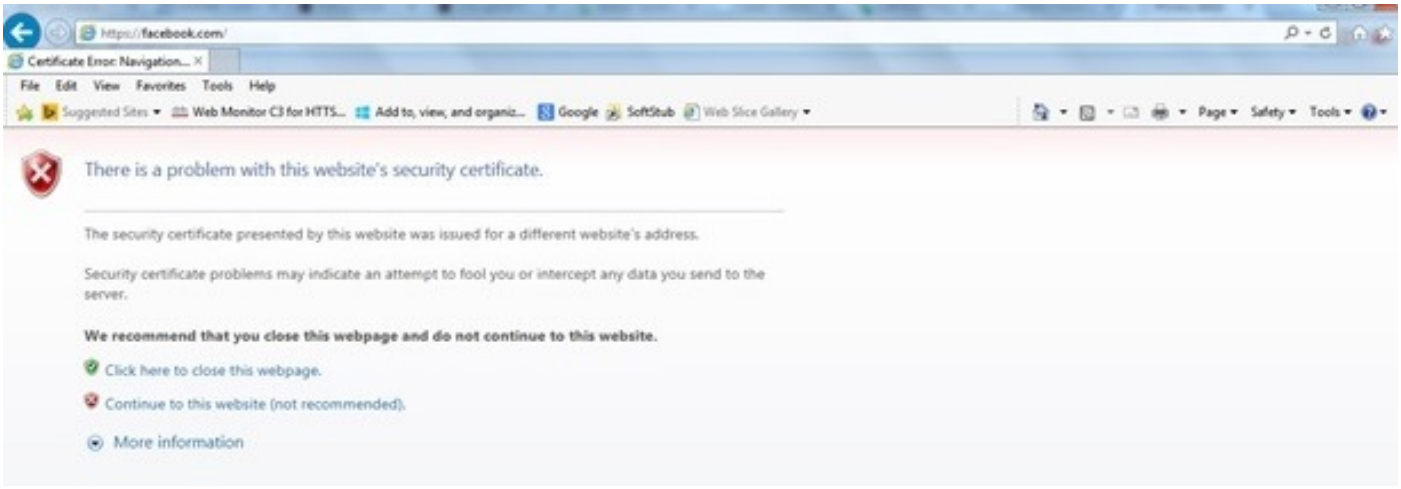
Предупреждающее сообщение "сертификат не выполнено доверенным центром сертификации". появляется на браузере после настройки функции перенаправления https. Даже если у вас есть допустимый root или объединенный в цепочку сертификат на контроллере как показано на рисунке 1 и рисунке 2, это замечено. Причина состоит в том, что certficiate, который вы установили на контроллере, выполнен к вашему виртуальному IP - адресу.

> **Примечание:** Если вы пробуете HTTP-перенаправление и имеете это certifcate на WLC, вы не получаете эту ошибку предупреждения сертификата. Однако, в случае перенаправления HTTPS, эта ошибка появляется.

Когда клиент попробует HTTPS://<веб-сайт>, браузер ожидает сертификат, выполненный к IP-адресу узла, решенного DNS. Однако то, что они получают, является сертификатом, который был выполнен к внутреннему веб-серверу WLC (виртуальный IP - адрес), который заставляет браузер выполнять предупреждение. Это просто из-за способа, которым HTTPS работает и всегда происходит, при попытке перехватить сеанс HTTPS для веб-подлинного перенаправления для работы.

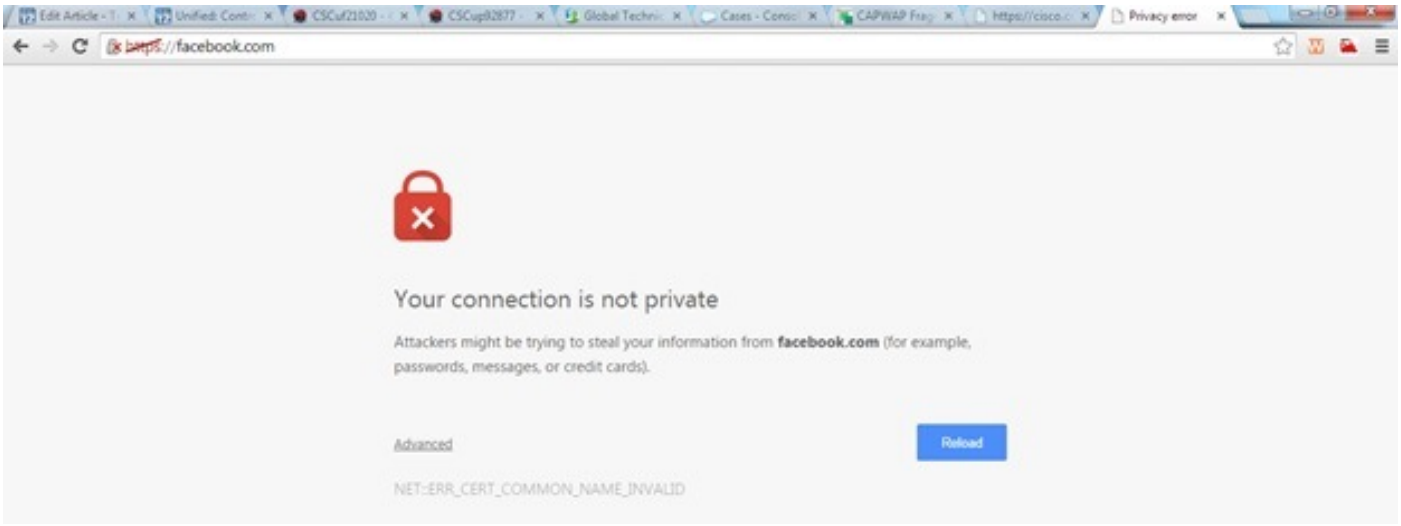
Вы могли бы видеть другие сообщения об ошибках сертификата в других браузерах, но все касаются той же проблемы, как ранее описано.

Рисунок 1



Это - пример того, как ошибка может появиться в Chrome:

Рис. 2



Настройка

Настройте WLC для перенаправления HTTPS

Эта конфигурация предполагает, что Беспроводная локальная сеть (WLAN) уже настроена для сети Уровня 3 опознавательная безопасность. Чтобы включить или отключить перенаправление HTTPS на этом Веб-подлинном WLAN:

```
(WLC)>config wlan security web-auth enable 10
(WLC)>config network web-auth https-redirect enable
WARNING! - You have chosen to enable https-redirect.
This might impact performance significantly
```

Поскольку пример конфигурации показывает, это могло бы повлиять на пропускную способность для перенаправления HTTPS, но не перенаправления HTTP

Для получения дополнительной информации и конфигурация WLAN web-аутентификации, посмотрите Web-аутентификацию на Контроллере беспроводной локальной сети.

Проверка

Этот раздел позволяет убедиться, что конфигурация работает правильно.

Средство интерпретации выходных данных (только зарегистрированные клиенты) поддерживает **некоторые команды show**. **Используйте Средство интерпретации выходных данных, чтобы просмотреть анализ выходных данных команды show.**

```
(WLC>show network summary

Web Auth Secure Web ..................... Enable
Web Auth Secure Redirection ............. Enable
```

1. Включите эти отладки:`(WLC) debug client <MAC address>`

   `(WLC)> debug web-auth redirect enable`
2. Проверьте отладки:`(WLC) >show debug`

   ```
   MAC Addr 1.............................. 24:77:03:52:56:80

   Debug Flags Enabled:
   webauth redirect enabled.
   ```
3. Свяжитесь клиент к веб-аутентификации включил SSID.
4. Ищите эти отладки:`*webauthRedirect: Jan 16 03:35:35.678: 24:77:3:52:56:80- received connection.
   client socket = 9
   *webauthRedirect: Jan 16 03:35:35.679: 24:77:3:52:56:80- trying to read on socket 95
   *webauthRedirect: Jan 16 03:35:35.679: 24:77:3:52:56:80- calling parser with bytes = 204
   *webauthRedirect: Jan 16 03:35:35.679: 24:77:3:52:56:80- bytes parsed = 204
   *webauthRedirect: Jan 16 03:35:35.679: captive-bypass detection enabled,
   checking for wispr in HTTP GET, client mac=24:77:3:52:56:80
   *webauthRedirect: Jan 16 03:35:35.679: 24:77:3:52:56:80- Preparing redirect
   URL according to configured Web-Auth type
   *webauthRedirect: Jan 16 03:35:35.679: 24:77:3:52:56:80- got the hostName
   for virtual IP(wirelessguest.test.com)
   *webauthRedirect: Jan 16 03:35:35.679: 24:77:3:52:56:80- Checking custom-web
   config for WLAN ID:10
   *webauthRedirect: Jan 16 03:35:35.679: 24:77:3:52:56:80- Global status is
   enabled, checking on web-auth type
   *webauthRedirect: Jan 16 03:35:35.679: 24:77:3:52:56:80- Web-auth type Customized,
   using URL:https://wirelessguest.test.com/fs/customwebauth/login.html`**Примечание:** Гарантируйте, что любая Безопасная сеть (config network secureweb позволить/запретить) или безопасная веб-аутентификация (веб-аутентификация сети config secureweb позволить/запретить) включена, чтобы заставить перенаправление HTTPS работать. Также обратите внимание, что могло бы быть небольшое сокращение пропускной способности , когда используется перенаправление по HTTPS.

Устранение неполадок

Для этой конфигурации в настоящее время нет сведений об устранении проблем.