تكوين إعادة توجيه HTTPS عبر مصادقة الويب

المحتويات

المقدمة
المتطلبات الأساسية
المتطلبات
المكونات المستخدمة
معلومات أساسية
خطأ في الشهادة
التكوين
تكوين عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) لـ HTTPS-Redirection
التحقق من الصحة
استكشاف الأخطاء وإصلاحها

المقدمة

يصف هذا المستند التكوين حول إعادة توجيه مصادقة الويب عبر HTTPS. هذه ميزة مقدمة في Cisco Unified Wireless Network (CUWN)، الإصدار 8.0.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- معرفة أساسية بمصادقة الويب لوحدة تحكم الشبكة المحلية اللاسلكية (WLC)
- كيفية تكوين عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) لمصادقة الويب.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى Cisco 5500 Series WLC الذي يشغل الإصدار 8.0 من البرنامج الثابت CUWN.

ملاحظة: ينطبق شرح التكوين ومصادقة الويب الوارد في هذا المستند على جميع نماذج WLC وأي صورة CUWN مساوية لـ 8.0.100.0 أو أحدث منه.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة

المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

مصادقة الويب هي ميزة أمان من الطبقة 3. وهو يحظر جميع حركة مرور IP/البيانات، باستثناء الحزم المرتبطة ب DHCP/الحزم المرتبطة ب DNS، من عميل معين حتى يقوم عميل لاسلكي بتوفير اسم مستخدم وكلمة مرور صحيحين.يتم إستخدام مصادقة الويب بشكل نموذجي من قبل العملاء الذين يرغبون في نشر شبكة وصول الضيف.تبدأ مصادقة الويب عندما تعترض وحدة التحكم أول TCP HTTP (المنفذ 80) الحصول على حزمة من العميل.

حتى يصل مستعرض ويب الخاص بالعميل إلى هذا الحد، يجب على العميل أولا الحصول على عنوان IP، وإجراء ترجمة لعنوان URL إلى عنوان IP (دقة DNS) لمستعرض الويب. يتيح هذا لمستعرض الويب معرفة عنوان IP الذي سيتم إرسال HTTP GET. عندما يرسل العميل أول HTTP إلى منفذ TCP 80، تقوم وحدة التحكم بإعادة توجيه العميل إلى https:<virtual ip>/login.html للمعالجة. تؤدي هذه العملية في النهاية إلى إظهار صفحة ويب تسجيل الدخول.

قبل الإصدارات الأقدم من CUWN 8.0 (أي ما يصل إلى 7.6)، إذا قدم العميل اللاسلكي صفحة HTTPS (TCP 443)، فلن تتم إعادة توجيه الصفحة إلى مدخل مصادقة الويب. مع بدء المزيد والمزيد من مواقع الويب في إستخدام HTTPS، يتم تضمين هذه الميزة في الإصدارات CUWN 8.0 والإصدارات الأحدث. مع وجود هذه الميزة، إذا حاول عميل لاسلكي https://<web>، فسيتم إعادة توجيهها إلى صفحة تسجيل دخول مصادقة الويب. كما أن هذه الميزة مفيدة جدا للأجهزة التي ترسل طلبات https مع تطبيق (ولكن ليس مع متصفح).

خطأ في الشهادة

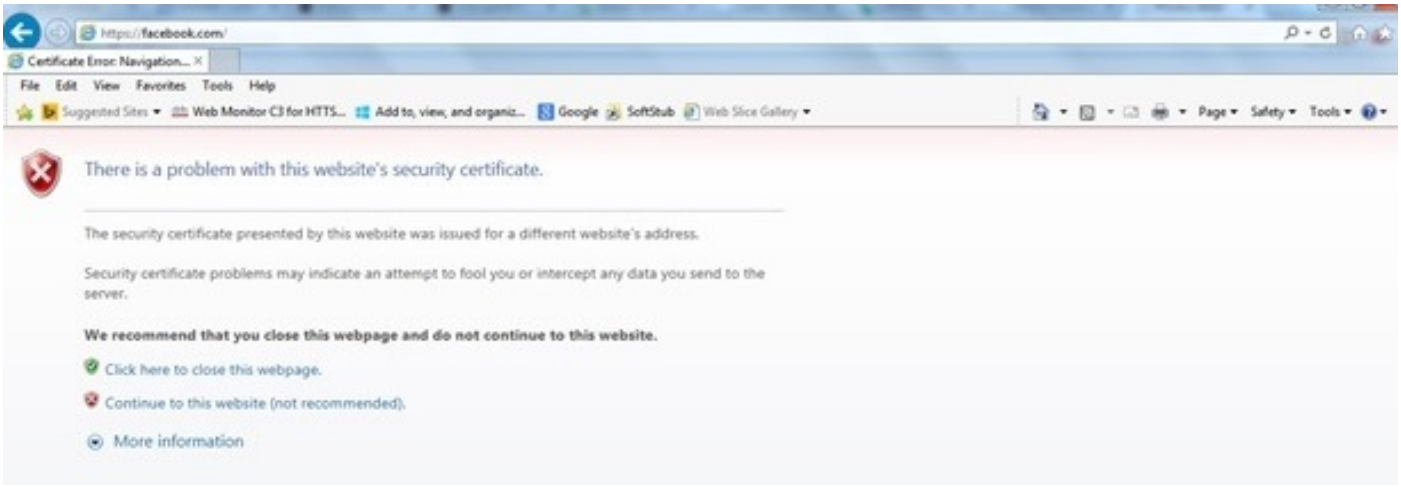
تظهر رسالة التحذير "لم يتم إصدار الشهادة من قبل مرجع مصدق موثوق به" على المستعرض بعد تكوين ميزة إعادة توجيه https. وهذا يظهر حتى إذا كان لديك شهادة جذر أو سلسلة صالحة على وحدة التحكم كما هو موضح في الشكل 1 والشكل 2. والسبب هو إصدار الشهادة التي قمت بتثبيتها على وحدة التحكم لعنوان IP الظاهري الخاص بك.

ملاحظة: إذا حاولت إعادة توجيه HTTP وكان لديك هذا الترخيص على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC)، فلن تحصل على خطأ تحذير الشهادة هذا. ومع ذلك في حالة إعادة توجيه HTTPS، يظهر هذا الخطأ.

عندما يحاول العميل HTTPS://<web-site>، يتوقع المستعرض الشهادة التي تم إصدارها لعنوان IP للموقع الذي تم حله بواسطة DNS. ومع ذلك، فإن ما يتلقونه هو الشهادة التي تم إصدارها إلى خادم الويب الداخلي الخاص ب WLC (عنوان IP الظاهري) والتي تتسبب في إصدار المستعرض التحذير. يرجع ذلك فقط إلى طريقة عمل HTTPS ويحدث دائما إذا حاولت اعتراض جلسة HTTPS لكي تعمل إعادة توجيه مصادقة الويب.

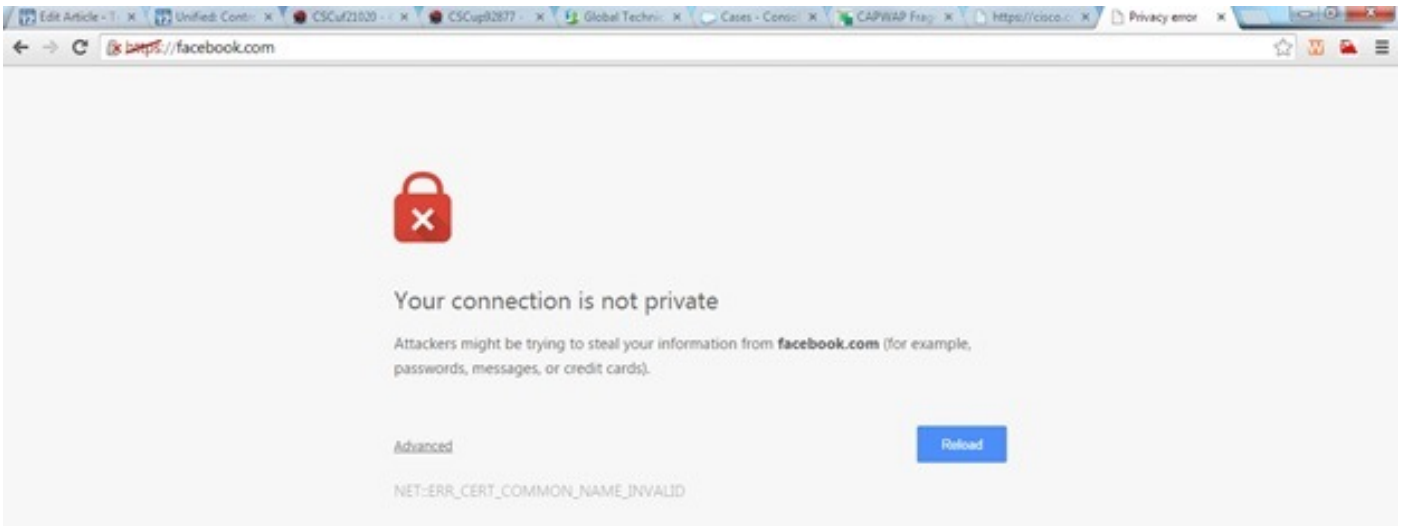
قد تظهر لك رسائل أخطاء شهادات مختلفة في مستعرضات مختلفة ولكن جميعها مرتبطة بنفس المشكلة كما تم وصفها سابقا.

شكل 1



هذا مثال من كيف الخطأ يستطيع ظهرت في Chrome:

شكل 2



التكوين

تكوين عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) ل HTTPS-Redirection

يفترض هذا التكوين أن شبكة LAN اللاسلكية (WLAN) تم تكوينها بالفعل لأمان مصادقة الويب للطبقة 3. لتمكين إعادة توجيه HTTPS أو تعطيلها على شبكة WLAN الخاصة بمصادقة الويب هذه:

```
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
```

كما يوضح مثال التكوين، قد يؤثر هذا على سعة المعالجة لإعادة توجيه HTTPS ولكن ليس إعادة توجيه HTTP

للحصول على مزيد من المعلومات وتكوين شبكات WLAN لمصادقة الويب، راجع مصادقة الويب على وحدة التحكم في الشبكة المحلية اللاسلكية (WLAN).

التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

تدعم أداة مترجم الإخراج (للعملاءالمسجلين فقط) بعض أوامر **show**. استخدم "أداة مترجم الإخراج" لعرض تحليل لمُخرَج الأمر **show**.

```
WLC)>show network summary)

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

1. تمكين تصحيح الأخطاء التالي:

```
WLC) debug client)
```

```
WLC)> debug web-auth redirect enable)
```

2. دققت ال debugs:

```
WLC) >show debug)

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

:Debug Flags Enabled
.webauth redirect enabled
```

3. قم بإقران العميل ب SSID الممكن لمصادقة الويب.
4. ابحث عن تصحيح الأخطاء التالي:

```
.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
```

ملاحظة: تأكد من تمكين إما الويب الآمن (config network secureWeb enable/disable) أو مصادقة الويب الآمنة (config network web-auth secure reweb enable/disable) من أجل إعادة توجيه HTTPS. لاحظ أيضا أنه قد يكون هناك انخفاض طفيف في الخرج عند إستخدام إعادة التوجيه عبر HTTPS.

استكشاف الأخطاء وإصلاحها

لا تتوفر حاليًا معلومات محددة لاستكشاف الأخطاء وإصلاحها لهذا التكوين.

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).