Konfigurieren der HTTPS-Umleitung über Web-Authentifizierung

Inhalt

[Einführung](#)
[Voraussetzungen](#)
[Anforderungen](#)
[Verwendete Komponenten](#)
[Hintergrundinformationen](#)
[Zertifikatfehler](#)
[Konfiguration](#)
[WLC für HTTPS-Umleitung konfigurieren](#)
[Überprüfung](#)
[Fehlerbehebung](#)

Einführung

Dieses Dokument beschreibt die Konfiguration der Web-Authentifizierungsumleitung über HTTPS. Diese Funktion wurde in Cisco Unified Wireless Network (CUWN) Version 8.0 eingeführt.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Grundlegende Kenntnisse der WLC-Webauthentifizierung (Wireless LAN Controller)
- Konfigurieren des WLC für die Webauthentifizierung

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf dem Cisco WLC der Serie 5500, auf dem die CUWN-Firmware Version 8.0 ausgeführt wird.

> **Hinweis:** Die in diesem Dokument vorgestellte Konfigurations- und Webauth-Erklärung gilt für alle WLC-Modelle und alle CUWN-Images gleich oder später als 8.0.100.0.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten

Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Hintergrundinformationen

Die Webauthentifizierung ist eine Layer-3-Sicherheitsfunktion. Er blockiert den gesamten IP-/Datenverkehr, mit Ausnahme von DHCP-bezogenen Paketen/DNS-bezogenen Paketen, von einem bestimmten Client, bis ein Wireless-Client einen gültigen Benutzernamen und ein gültiges Kennwort angegeben hat.Die Webauthentifizierung wird in der Regel von Kunden verwendet, die ein Gastzugriffsnetzwerk bereitstellen möchten.Die Webauthentifizierung beginnt, wenn der Controller das erste TCP-HTTP-GET-Paket (Port 80) vom Client abfängt.

Damit der Webbrowser des Clients dies erreichen kann, muss der Client zunächst eine IP-Adresse erhalten und die URL in eine IP-Adresse (DNS-Auflösung) für den Webbrowser übersetzen. Dadurch kann der Webbrowser wissen, welche IP-Adresse der HTTP GET gesendet werden soll. Wenn der Client das erste HTTP GET-Gerät an den TCP-Port 80 sendet, leitet der Controller den Client zur Verarbeitung an https:<virtual IP>/login.html um. Durch diesen Prozess wird schließlich die Anmelde-Webseite aufgerufen.

Wenn der Wireless-Client eine HTTPS-Seite (TCP 443) anzeigt, wird die Seite vor CUWN 8.0-Versionen (d. h. bis zu 7.6) nicht zum Web-Authentifizierungsportal umgeleitet. Da immer mehr Websites HTTPS verwenden, ist diese Funktion in CUWN 8.0 und höher enthalten. Wenn ein Wireless-Client nach https://<website> sucht, wird diese Funktion zur Anmeldeseite für die Webauthentifizierung umgeleitet. Diese Funktion ist auch sehr nützlich für Geräte, die HTTPS-Anfragen mit einer Anwendung (aber nicht mit einem Browser) senden.

Zertifikatfehler

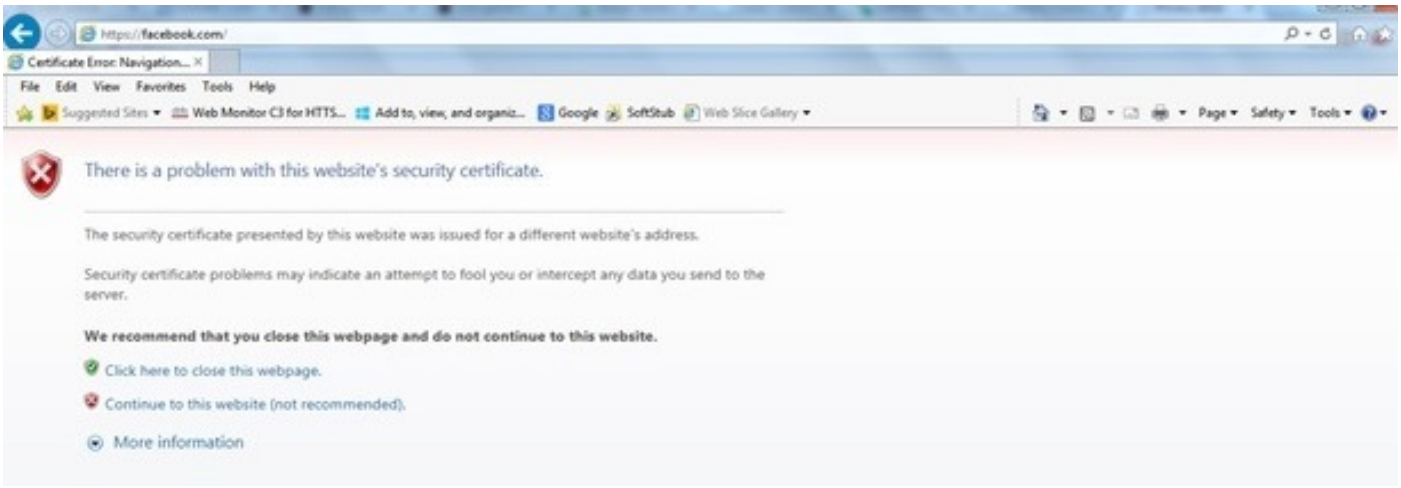
Die Warnmeldung "Das Zertifikat wird nicht von einer vertrauenswürdigen Zertifizierungsstelle ausgestellt." wird im Browser angezeigt, nachdem Sie die Funktion für die HTTPS-Umleitung konfiguriert haben. Dies ist auch dann der Fall, wenn ein gültiges Root- oder verkettetes Zertifikat auf dem Controller vorhanden ist (siehe Abbildung 1 und Abbildung 2). Der Grund hierfür ist, dass das Zertifikat, das Sie auf dem Controller installiert haben, an Ihre virtuelle IP-Adresse ausgegeben wird.

> **Hinweis:** Wenn Sie eine HTTP-Umleitung versuchen und dieses Zertifikat auf dem WLC haben, wird dieser Zertifikatwarnfehler nicht ausgegeben. Bei der HTTPS-Umleitung wird dieser Fehler jedoch angezeigt.

Wenn der Client HTTPS://<web-site> versucht, erwartet der Browser, dass das Zertifikat, das an die IP-Adresse der Site ausgegeben wird, vom DNS aufgelöst wird. Sie erhalten jedoch das Zertifikat, das dem internen Webserver des WLC (virtuelle IP-Adresse) ausgestellt wurde, wodurch der Browser die Warnung ausgibt. Dies ist ausschließlich auf die Funktionsweise von HTTPS zurückzuführen und geschieht immer, wenn Sie versuchen, die HTTPS-Sitzung abzufangen, um die Umleitung der Webauthentifizierung zu ermöglichen.

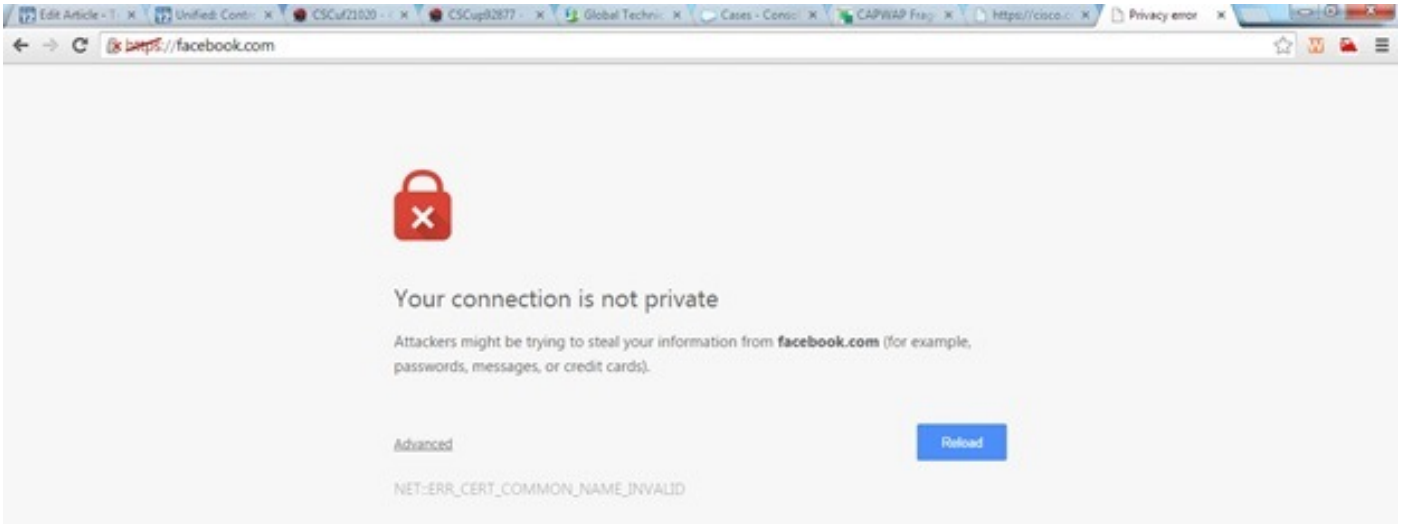
Möglicherweise werden in verschiedenen Browsern unterschiedliche Zertifikatfehlermeldungen angezeigt, aber alle beziehen sich auf dasselbe Problem wie zuvor beschrieben.

Abbildung 1



Dies ist ein Beispiel dafür, wie der Fehler in Chrome angezeigt werden kann:

Abbildung 2



Konfiguration

WLC für HTTPS-Umleitung konfigurieren

Bei dieser Konfiguration wird davon ausgegangen, dass das Wireless LAN (WLAN) bereits für die Web-Authentifizierungssicherheit auf Layer 3 konfiguriert ist. So aktivieren oder deaktivieren Sie die HTTPS-Umleitung in diesem Web-Authentifizierungs-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
```

Wie die Beispielkonfiguration zeigt, kann sich dies auf den Durchsatz für eine HTTPS-Umleitung auswirken, nicht jedoch auf die HTTP-Umleitung.

Weitere Informationen und eine Konfiguration der WLANs für die Webauthentifizierung finden Sie

unter Webauthentifizierung auf dem WLAN-Controller.

Überprüfung

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Das Output Interpreter Tool (nur registrierte Kunden) unterstützt bestimmte **show**-Befehle. Verwenden Sie das Output Interpreter Tool, um eine Analyse der **Ausgabe des** Befehls **show** anzuzeigen.

```
(WLC)>show network summary

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

1. Aktivieren Sie diese Debugger:
   ```
   (WLC) debug client
   ```

   ```
   (WLC)> debug web-auth redirect enable
   ```
2. Überprüfen Sie das Debuggen:
   ```
   (WLC) >show debug

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

   Debug Flags Enabled:
   webauth redirect enabled.
   ```
3. Ordnen Sie den Client der Web-Authentifizierungs-aktivierten SSID zu.
4. Suchen Sie nach diesen Debuggen:
   ```
   *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
   ```
   Hinweis: Stellen Sie sicher, dass entweder Secure Web (Konfigurieren von Secure Web (Aktivieren/Deaktivieren des Netzwerks) oder Web-Authorization Secure (Konfigurieren von Web-Authentifizierung, sicheres Web-Aktivieren/Deaktivieren) aktiviert sind, damit die HTTPS-Umleitung funktioniert. Beachten Sie auch, dass der Durchsatz bei Verwendung der Umleitung über HTTPS leicht verringert werden kann.

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.