Configurer la redirection de l’authentification Web sur HTTPS

Contenu

Introduction

Ce document décrit la configuration pour la redirection de l’authentification Web sur HTTPS. Il s’agit d’une fonctionnalité introduite dans la version 8.0 de Cisco Unified Wireless Network (CUWN).

Conditions préalables

Conditions requises

Cisco recommande de posséder des connaissances sur ces sujets :

- Connaissance de base de l'authentification Web du contrôleur de réseau local sans fil (WLC)
- Comment configurer le WLC pour l'authentification Web.

Components Used

Les informations de ce document sont basées sur le WLC de la gamme Cisco 5500 qui exécute le microprogramme CUWN version 8.0.

> **Note**: L'explication de configuration et d'authentification Web fournie dans ce document s'applique à tous les modèles WLC et à toute image CUWN égale ou postérieure à 8.0.100.0.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Informations générales

L'authentification Web est une fonction de sécurité de couche 3. Il bloque tout le trafic IP/données, à l'exception des paquets DHCP/DNS, d'un client particulier jusqu'à ce qu'un client sans fil ait fourni un nom d'utilisateur et un mot de passe valides.L'authentification Web est généralement utilisée par les clients qui veulent déployer un réseau d'accès invité.L'authentification Web commence lorsque le contrôleur intercepte le premier paquet HTTP TCP (port 80) GET du client.

Pour que le navigateur Web du client puisse aller aussi loin, le client doit d'abord obtenir une adresse IP et faire une traduction de l'URL en adresse IP (résolution DNS) pour le navigateur Web. Cela permet au navigateur Web de savoir quelle adresse IP envoyer à HTTP GET. Lorsque le client envoie le premier HTTP GET au port TCP 80, le contrôleur redirige le client vers https:<virtual IP>/login.html pour traitement. Ce processus finit par ouvrir la page de connexion.

Avant les versions antérieures à CUWN 8.0 (c'est-à-dire jusqu'à 7.6), si le client sans fil présente une page HTTPS (TCP 443), la page n'est pas redirigée vers le portail d'authentification Web. À mesure que de plus en plus de sites Web commencent à utiliser HTTPS, cette fonctionnalité est incluse dans les versions CUWN 8.0 et ultérieures. Si cette fonctionnalité est en place, si un client sans fil tente https://<site Web>, il est redirigé vers la page de connexion de l'authentification Web. Cette fonctionnalité est également très utile pour les périphériques qui envoient des requêtes https avec une application (mais pas avec un navigateur).

Erreur de certificat

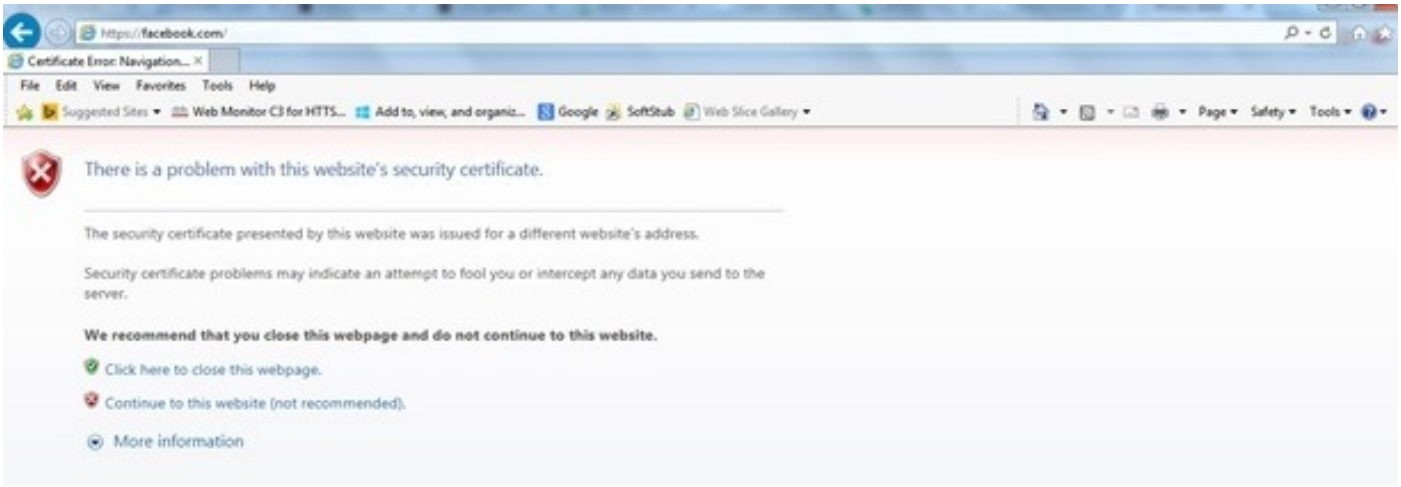
Le message d'avertissement « certificat n'est pas émis par une autorité de certification de confiance. » apparaît dans le navigateur après avoir configuré la fonction https-redirect. Ceci est visible même si vous avez un certificat racine ou chaîné valide sur le contrôleur, comme illustré à la Figure 1 et à la Figure 2. La raison en est que le certificat que vous avez installé sur le contrôleur est attribué à votre adresse IP virtuelle.

> **Note**: Si vous essayez une redirection HTTP et que vous avez ce certificat sur le WLC, vous n'obtenez pas cette erreur d'avertissement de certificat. Cependant, dans le cas de HTTPS-redirect, cette erreur apparaît.

Lorsque le client tente HTTPS://<site Web> , le navigateur attend le certificat émis à l'adresse IP du site résolue par le DNS. Cependant, ce qu'ils reçoivent est le certificat qui a été émis au serveur Web interne du WLC (adresse IP virtuelle), ce qui fait que le navigateur émet l'avertissement. Ceci est uniquement dû à la façon dont HTTPS fonctionne et se produit toujours si vous essayez d'intercepter la session HTTPS afin que la redirection d'authentification Web fonctionne.

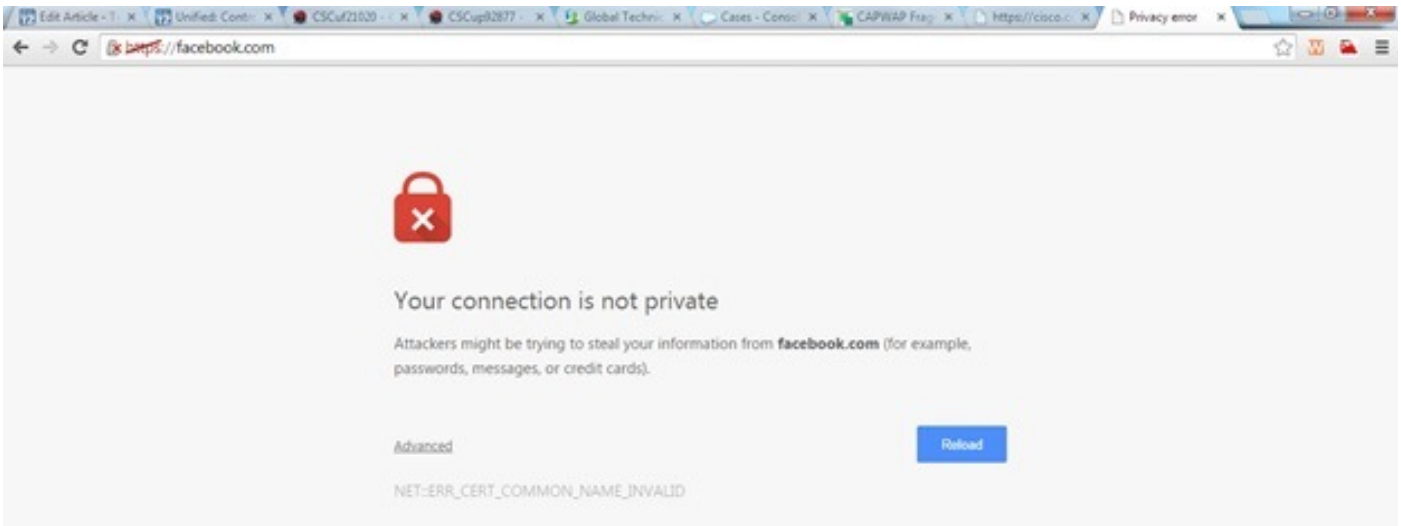
Vous pouvez voir différents messages d'erreur de certificat dans différents navigateurs, mais tous se rapportent au même problème que décrit précédemment.

Figure 1



Voici un exemple de la façon dont l'erreur peut apparaître dans Chrome :

Figure 2



Configuration

Configurer le WLC pour la redirection HTTPS

Cette configuration suppose que le LAN sans fil (WLAN) est déjà configuré pour la sécurité de l'authentification Web de couche 3. Afin d'activer ou de désactiver la redirection HTTPS sur ce WLAN d'authentification Web :

```
(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
```

Comme le montre l'exemple de configuration, ceci peut avoir un impact sur le débit d'une redirection HTTPS, mais pas de la redirection HTTP

Pour plus d'informations et une configuration des WLAN d'authentification Web, consultez Authentification Web sur le contrôleur WLAN.

Vérification

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

L'Outil d'interprétation de sortie (clients enregistrés seulement) prend en charge certaines commandes d'affichage. Utilisez l'Outil d'interprétation de sortie afin de visualiser une analyse de commande d'affichage de sortie .

```
(WLC)>show network summary

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

1. Activez ces débogages :
   ```
   (WLC) debug client
   ```

   ```
   (WLC)> debug web-auth redirect enable
   ```
2. Vérifiez les débogages :
   ```
   (WLC) >show debug

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

   Debug Flags Enabled:
   webauth redirect enabled.
   ```
3. Associez le client au SSID activé pour l'authentification Web.
4. Recherchez ces débogages :
   ```
   *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
   ```
   Note: Assurez-vous que Secure Web (config network secureweb enable/disable) ou Web-auth secure (config network web-auth secureweb enable/disable) sont activés afin de faire fonctionner la redirection HTTPS. Notez également qu'il peut y avoir une légère réduction du débit lorsque la redirection sur HTTPS est utilisée.

Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.