Configurez HTTPS réorientent au-dessus du Web-auth

Contenu

Introduction

Ce document décrit la configuration au sujet de la redirection d'authentification Web au-dessus de HTTPS. C'est une fonctionnalité introduite dans la version 8.0 du réseau sans fil unifié Cisco (CUWN).

Conditions préalables

Conditions requises

Cisco recommande de posséder des connaissances sur ces sujets :

- Connaissance de base de l'authentification Web Sans fil du contrôleur LAN (WLC)
- Comment configurer le WLC pour l'authentification Web.

[Composants utilisés](#)

Les informations dans ce document sont basées sur la gamme Cisco 5500 WLC qui exécutent la version 8.0 de micrologiciels CUWN.

> Remarque: L'explication de configuration et de Web-auth fournie dans ce document s'applique à tous les modèles WLC et à n'importe quelle image CUWN égaux à ou plus tard que 8.0.100.0.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Informations générales

L'authentification Web est une fonctionnalité de sécurité de la couche 3. Il bloque tout le trafic IP/data, excepté les paquets liés aux dn de paquets liés au DHCP, d'un client particulier jusqu'à ce qu'un client sans fil ait fourni un nom d'utilisateur valide et un mot de passe. L'authentification Web est généralement utilisée par les clients qui veulent déployer un réseau d'accès invité. Les débuts d'authentification Web quand le contrôleur intercepte le premier HTTP de TCP (port 80) OBTIENNENT le paquet du client.

Pour que le navigateur Web du client obtienne ceci loin, le client doit d'abord obtenir une adresse IP, et fait une traduction de l'URL à l'adresse IP (résolution de DN) pour le navigateur Web. Ceci fait le navigateur Web connaître quelle adresse IP pour envoyer le HTTP OBTENEZ. Quand le client envoie le premier HTTP ARRIVEZ au port TCP 80, le contrôleur réoriente le client aux https : IP>/login.html <virtual pour le traitement. Ce processus évoque par la suite la page Web de procédure de connexion.

Avant des releases plus tôt que CUWN 8.0 (c.-à-d. jusqu'à 7.6), si le client sans fil présente une page HTTPS (TCP 443), la page n'est pas réorientée au portail d'authentification Web. Pendant que de plus en plus les sites Web commencent à utiliser HTTPS, cette caractéristique est incluse dans des releases CUWN 8.0 et plus tard. Avec cette configuration en place, si un client sans fil essaye le <website> de https://, il est réorienté à la page de connexion de Web-auth. Également cette caractéristique est très utile pour les périphériques qui envoient des demandes de https avec une application (mais pas avec un navigateur).

Erreur de certificat

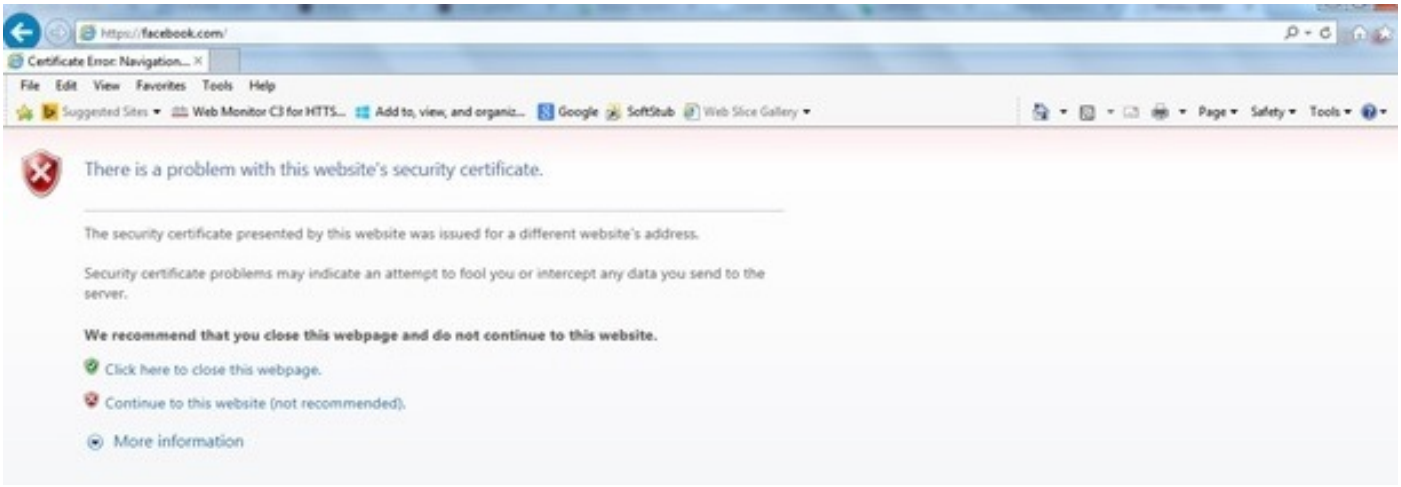
Le message d'avertissement « certificat n'est pas émis par une autorité de certification de confiance. » apparaît sur le navigateur après que vous configuriez la caractéristique de https-réorientation. Ceci est vu même si vous avez une racine valide ou un certificat enchaîné sur le contrôleur suivant les indications de la figure 1 et de la figure 2. La raison est que le certficiate que vous avez installé sur le contrôleur est fourni à votre adresse IP virtuelle.

> Remarque: Si vous essayez un http-redirect et avez ce certifcate sur le WLC, vous n'obtenez pas cette erreur d'avertissement de certificat. Toutefois dans le cas de HTTPS-réorientez, cette erreur apparaît.

Quand le client essaye le <website> de HTTPS://, le navigateur attend le certificat fourni à l'adresse IP du site résolu par les DN. Cependant, ce qu'elles reçoivent est le certificat qui a été fourni au web server interne du WLC (adresse IP virtuelle) qui fait émettre le navigateur l'avertissement. C'est purement en raison des travaux de la manière HTTPS et se produit toujours si vous essayez d'intercepter la session HTTPS pour que la redirection de Web-auth fonctionne.

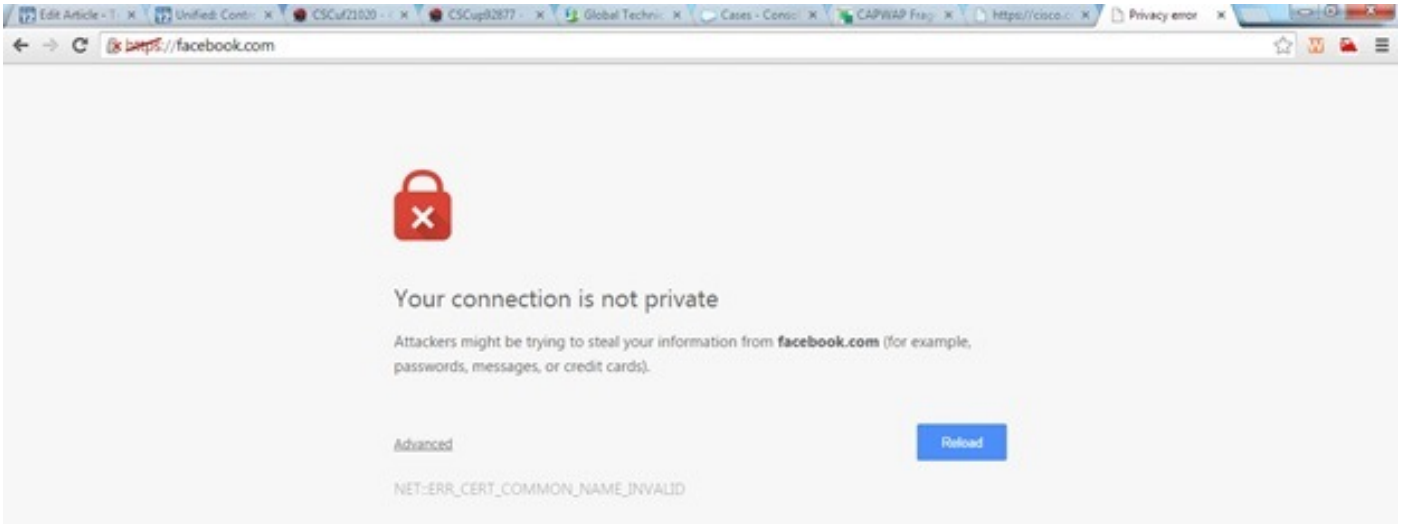
Vous pourriez voir différents messages d'erreur de certificat dans différents navigateurs mais tous associer au même problème comme décrit précédemment.

Figure 1



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

Figure 2



Configurez

Configurez le WLC pour la HTTPS-redirection

Cette configuration suppose que le RÉSEAU LOCAL Sans fil (WLAN) est déjà configuré pour la Sécurité d'authentciation de Web de la couche 3. Afin d'activer ou le débronchement HTTPS réorientent sur ce Web-auth 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
```

Car l'exemple de configuration affiche, ceci pourrait affecter le débit pour une redirection mais pas la redirection HTTP HTTPS

Le pour en savoir plus et une configuration de l'authentification Web WLAN, voient l'authentification Web sur le contrôleur WLAN.

Vérifiez

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

L'Output Interpreter Tool (clients enregistrés seulement) prend en charge certaines **commandes show**. Utilisez l'Output Interpreter Tool afin de visualiser une analyse de sortie de commande show.

```
(WLC)>show network summary

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

1. Activez ces derniers met au point :`(WLC) debug client <MAC address>`

   `(WLC)> debug web-auth redirect enable`
2. Vérifiez met au point :`(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 par Web-auth.
4. Recherchez ces derniers met au point :`*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`Remarque: Assurez-vous que le Web sécurisé (enable/disable de config network secureweb) ou le Web-auth sécurisé (enable/disable de secureweb de Web-auth de réseau de config) sont activés afin de faire le HTTPS réorienter le travail. Notez également qu'il pourrait y a une légère réduction du débit quand la redirection au-dessus de HTTPS est utilisée.

Dépannez

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