Générer une demande CSR pour des certificats tiers et télécharger des certificats déchaînés sur le contrôleur de réseau local sans fil (WLC)

Contenu

Introduction

Ce document explique comment générer une demande de signature de certificat (CSR) afin d'obtenir un tiers certificat et comment télécharger un certificat désenchaîné à un contrôleur Sans fil du RÉSEAU LOCAL (WLAN) (WLC).

Conditions préalables

Conditions requises

Assurez-vous que vous répondez à ces exigences avant d'essayer cette configuration :

- La connaissance de la façon configurer le WLC, le point d'accès léger (LAP), et la carte de client sans fil pour le fonctionnement de base
- La connaissance de la façon utiliser la demande d'OpenSSL de Protocole SSL (Secure Socket Layer)

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco 4400 WLC qui exécute la version 4.2.61.0 de micrologiciels
- Demande d'OpenSSL de Microsoft Windows**Remarque:** OpenSSL 0.9.8 est exigé car le WLC ne prend en charge pas actuellement OpenSSL 1.0.
- Outil d'inscription qui est spécifique à la tiers autorité de certification (le CA)

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.

Conventions

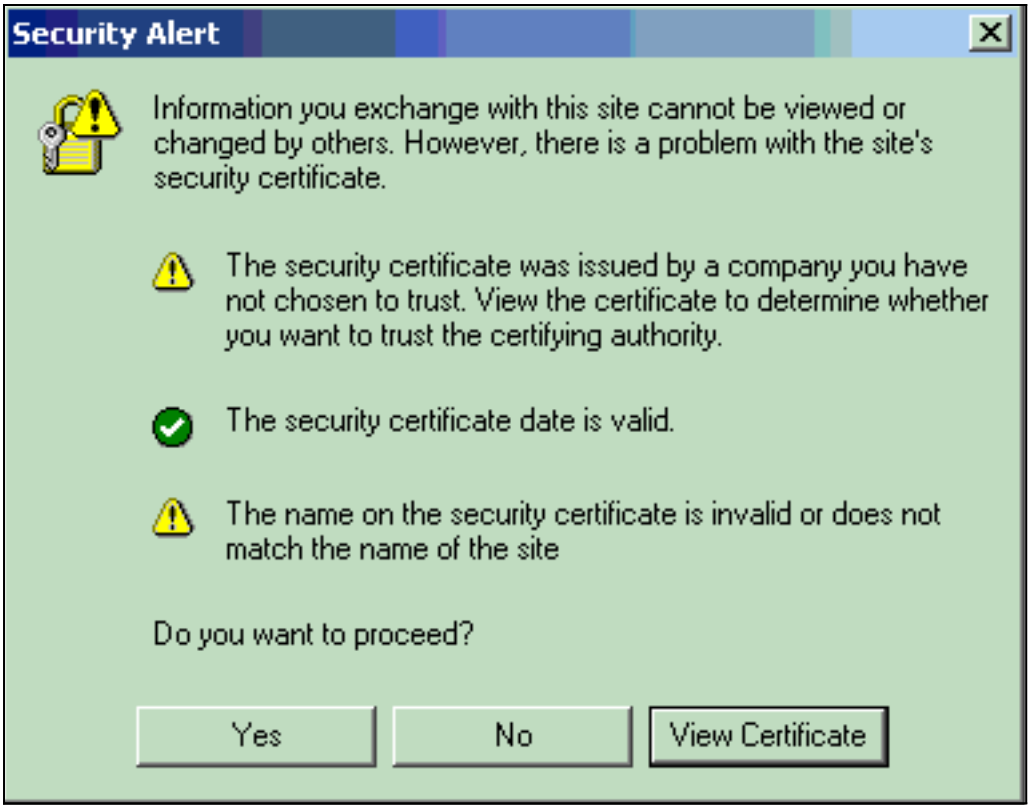
Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Informations générales

Par défaut, l'utilisation de WLCs une fonction intégrée auto-a signé le certificat ssl. L'utilisation de WLCs ce certificat ssl dans une de ces situations :

- Quand l'essai de clients à connecter au réseau WLAN à l'utilisation de l'authentification Web basée sur SSL
- Quand essais d'un utilisateur à ouvrir une session au WLC avec l'utilisation du HTTP Secure (HTTPS) (authentification de WebAdmin)

Dans l'un ou l'autre de cas, sur le premier essai d'accéder au WLC, vous pouvez recevoir une alerte sécurité de web browser qui ressemble à ceci :



Vous êtes incité à recevoir le certificat du WLC parce que les clients n'ont pas un certificat racine de confiance pour le certificat qui est installé sur le WLC. Le certificat ssl sur le WLC n'est pas dans la liste de Certificats aux lesquels le système client fait confiance. Il y a deux manières

d'arrêter la génération de cette fenêtre contextuelle d'alerte sécurité de web browser :

- Utilisez le certificat ssl auto-signé sur le WLC et configurez les stations client pour recevoir le certificat.Incluez le certificat auto-signé sur le WLC dans la liste de Certificats qui sont de confiance sur la station client.
- Générez un CSR et installez un certificat qui est signé par une source (une tierce partie CA) pour lequel les clients prennent déjà les certificats racine de confiance installés, comme Verisign.Vous pouvez faire ce hors ligne du WLC avec l'utilisation d'un programme comme OpenSSL. Référez-vous à l'OpenSSL Project pour plus d'informations sur OpenSSL.

Ce document explique comment générer un CSR pour un certificat de tiers et comment télécharger un certificat désenchaîné d'authentification Web au WLC.

Soutien de certificat enchaîné

Les versions de logiciel WLC plus tôt que 5.1.151.0 ne prennent en charge pas les Certificats enchaînés. Utilisez un du contournement de ces options cette question :

- Saisissez un certificat désenchaîné du CA, ainsi il signifie que la racine de signature est de confiance.
- Ayez tous les certificats racine valides de l'intermédiaire CA, faits confiance ou non approuvés, installés sur le client.

Avec la version 5.1.151.0 et plus tard, le support de WLCs a enchaîné des Certificats pour l'authentification Web. Les Certificats d'authentification Web peuvent être l'un de ces :

- Enchaîné
- Désenchaîné
- Autogenerated

Référez-vous génèrent le CSR pour de tiers Certificats et téléchargent les Certificats enchaînés au WLC pour les informations sur la façon dont utiliser les Certificats enchaînés sur WLC.

CSR

Un certificat est un document électronique que vous employez afin d'identifier un serveur, une société, ou une autre entité et associer cette identité avec une clé publique.

Les CAs sont des entités qui valident des identités et délivrent des Certificats. Le certificat que le CA fournit des grippages une clé publique particulière au nom de l'entité que le certificat identifie (comme le nom d'un serveur ou d'un périphérique). Seulement la clé publique que le certificat certifie des travaux avec la clé privée correspondante qui est possédée par l'entité que le certificat identifie. Les Certificats aident à empêcher l'utilisation de fausses clés publiques pour la personnification.

Un CSR est un message qu'un candidat envoie à un CA afin de solliciter un certificat d'identité numérique. Pour la plupart, une société de la tierce partie CA, comme confient ou Verisign, exige un CSR avant que la société puisse créer un certificat numérique.

La génération CSR est indépendant du périphérique sur lequel vous prévoyez d'installer un certificat externe. Ainsi un CSR et un fichier principal privé peuvent être générés sur n'importe quel Windows ou système Unix individuel. La génération CSR n'est pas commutateur-dépendante

ou appliance-dépendante dans ce cas.

Puisque le WLC ne génère pas un CSR, vous devez employer une application tierce telle qu'OpenSSL afin de générer un CSR pour le WLC.

La section génèrent un CSR discute les commandes que vous devez émettre sur l'application d'OpenSSL afin de générer une clé privée et le CSR.

Terminez-vous ces étapes afin d'obtenir un tiers certificat d'un CA :

1. Générez paire de clés privée/publique.
2. Avec l'utilisation de la clé publique, générez un CSR.
3. Soumettez le CSR à un CA.
4. Récupérez le certificat que le CA produit.
5. Combinez le certificat et la clé privée dans un fichier pkcs12.
6. Convertissez le fichier pkcs12 en fichier de codage du Privacy Enhanced Mail (PEM).
7. Téléchargez le nouveau tiers certificat (fichier .pem) sur le WLC.

Générez un CSR

Terminez-vous ces étapes afin de générer un CSR et soumettre le CSR à la tierce partie CA :

1. Installez et ouvrez l'application d'OpenSSL.**Remarque:** OpenSSL 0.9.8 est exigé car le WLC ne prend en charge pas actuellement OpenSSL 1.0.Dans Windows, par défaut, openssl.exe se trouve chez c:\openssl\bin.
2. Émettez la commande suivante :`OpenSSL>req -new -newkey rsa:1024 -nodes -keyout mykey.pem -out myreq.pem` **Remarque:** Support de WLCs une taille de clé maximum de **2048** bits.Après que vous émettiez la commande, il y a une demande pour quelques informations : nom du pays, état, ville, et ainsi de suite.
3. Fournissez l'information requise.La plupart d'informations importantes que vous devez fournir correctement sont le nom commun. Assurez-vous que le nom d'hôte qui est utilisé pour créer le certificat (nom commun) apparie l'entrée de nom d'hôte de Système de noms de domaine (DNS) pour l'IP d'interface virtuelle sur le WLC et que le nom existe réellement dans les DN aussi bien. En outre, après que vous apportiez la modification à l'interface de VIP, vous devez redémarrer le système pour que cette modification la prenne effet.**Remarque:** Le nom d'hôte de DN doit être écrit dans le WLC sous l'**Interfaces > Edit** pour l'interface virtuelle. Ceci est utilisé pour vérifier la source des Certificats quand le Web authentique est activé. Redémarrez le contrôleur pour faire le prendre effet cette modification.Après que vous fournissiez tous les détails priés, vous finissez par avec deux fichiers :une nouvelle clé privée qui a le nom mykey.pemun CSR qui a le nom myreq.pemCes fichiers sont enregistrés dans le répertoire par défaut où OpenSSL est installé (c:\openssl\bin, dans ce cas). Le fichier myreq.pem est le fichier qui contient les informations CSR. Ces informations doivent être soumises à la tierce partie CA de sorte que la tierce partie CA puisse générer un certificat numérique. Voici l'exemple de sortie de commande quand vous émettez cette commande avec l'utilisation de l'application d'OpenSSL :`OpenSSL>req -new -newkey rsa:1024 -nodes -keyout mykey.pem -out myreq.pem` Loading 'screen' into random state - done Generating a 1024 bit RSA private key .....++++++ .....++++++ writing new private key to 'mykey.pem' ----- You are about to be asked to enter information that will be incorporated into your certificate request. What you are about to enter is what is called a

```
Distinguished Name or a DN. There are quite a few fields but you can leave some blank For
some fields there will be a default value, If you enter '.', the field will be left blank.
----- Country Name (2 letter code) [AU]:US State or Province Name (full name) [Some-
State]:CA Locality Name (eg, city) []:San Jose Organization Name (eg, company) [Internet
Widgits Pty Ltd]:ABC Organizational Unit Name (eg, section) []:CDE Common Name (eg, YOUR
name) []:XYZ.ABC Email Address []:Test@abc.com Please enter the following 'extra'
attributes to be sent with your certificate request A challenge password []:Test123 An
optional company name []: OpenSSL>
```
Remarque: Souvenez-vous le mot de passe de défi et préservez le fichier principal. Très probablement, vous aurez besoin du mot de passe quand vous importez le certificat digitalement signé que la tierce partie CA envoie (à moins que la tierce partie CA envoie un nouveau mot de passe avec le certificat numérique qu'il génère pour vous ou votre organisation).

4. Maintenant que votre CSR est prêt, copiez et collez les informations CSR dans n'importe quel outil d'inscription CA.Afin de copier et coller les informations dans la forme d'inscription, ouvrez le fichier dans un éditeur de texte qui n'ajoute pas les caractères supplémentaires. Cisco recommande que vous utilisiez Microsoft Notepad ou UNIX vi. Référez-vous au site Web de la tierce partie CA pour plus d'informations sur la façon soumettre le CSR par l'outil d'inscription.Après que vous soumettiez le CSR à la tierce partie CA, la tierce partie CA digitalement signe le certificat et envoie de retour le certificat signé par l'intermédiaire du courrier électronique.
5. Copiez les informations de certificat signé que vous recevez de retour du CA dans un fichier.Cet exemple nomme le fichier CA.pem.
6. Combinez le certificat CA.pem avec la clé privée, et puis convertissez le fichier en fichier .pem.Émettez cette commande dans l'application d'OpenSSL :
```
openssl>pkcs12 -export -in CA.pem -inkey mykey.pem -out CA.p12 -clcerts -passin pass:check123 -passout pass:check123
!--- This command should be on one line.
openssl>pkcs12 -in CA.p12 -out final.pem -passin pass:check123 -passout pass:check123
```
Remarque: Dans cette commande, vous devez entrer un mot de passe pour les paramètres `- passin` et `- passout`. Le mot de passe qui est configuré pour `-` paramètre de `passout` doit apparier le paramètre de `certpassword` qui est configuré sur le WLC. Dans cet exemple, le mot de passe qui est configuré pour `- passin` et `- les` paramètres de `passout` est **check123**. Étape 4 de la procédure dans le téléchargement le tiers certificat à la section WLC de ce document discute la configuration du paramètre de `certpassword.Le final.pem est le` fichier qui est transféré par l'intermédiaire du TFTP vers le Cisco WLC.Maintenant que vous avez le certificat de la tierce partie CA, vous devez télécharger le certificat au WLC.

Téléchargez le tiers certificat au WLC

Utilisez un serveur TFTP afin de charger le nouveau certificat. Suivez ces instructions pour l'usage du TFTP :

- Si vous chargez le certificat par le port de service, le serveur TFTP doit être sur le même sous-réseau que le WLC parce que le port de service n'est pas routable. Cependant, si vous chargez le certificat par le port de réseau du système de distribution (DS), le serveur TFTP peut être sur n'importe quel sous-réseau.
- Le serveur TFTP ne peut pas fonctionner sur le même ordinateur que le Système de contrôle sans fil Cisco (WCS) parce que WCS et le serveur TFTP utilisent le même port de transmission.

Terminez-vous ces étapes afin de charger un certificat extérieurement généré HTTPS :

1. Déplacez le fichier final.pem au répertoire par défaut sur votre serveur TFTP.
2. Dans l'interface de ligne de commande (CLI), émettez la commande de **transfer download start** afin de visualiser les configurations en cours de téléchargement, et écrivez **n à la** demande.Voici un exemple :>**transfer download start**
```
Mode..................................... TFTP Data
Type..................................... Admin Cert TFTP Server
IP.............................. xxx.xxx.xxx.xxx TFTP
Path..................................... <directory path> TFTP
Filename................................. Are you sure you want to start? (y/n) n Transfer
Canceled
```
3. Émettez ces commandes afin de changer les configurations de téléchargement :>**transfer download mode tftp** >**transfer download datatype webauthcert** >**transfer download serverip** *<TFTP server IP address>* >**transfer download path** *<absolute TFTP server path to the update file>* >**transfer download filename** *final.pem*
4. Entrez le mot de passe pour le fichier .pem de sorte que le système d'exploitation puisse déchiffrer la clé et le certificat SSL.>**transfer download certpassword** *password* >Setting password to *password* **Remarque:** Soyez que le **certpassword** est identique que **- le** mot de passe sûr de paramètre de **passout** qu'étape 6 du générer par section CSR discute. Dans cet exemple, le **certpassword** doit être **check123**.
5. Émettez la commande de **transfer download start** afin de visualiser les configurations mises à jour. Écrivez alors **y au** prompt afin de confirmer les configurations en cours de téléchargement et commencer le téléchargement de certificat et de clé.Voici un exemple :
```
(Cisco Controller) >transfer download start
Mode..................................... TFTP Data
Type..................................... Admin Cert TFTP Server
IP.................................. 172.16.1.1 TFTP Packet
Timeout.............................. 6 TFTP Max Retries.............................
10 TFTP Path..................................... c:\OpenSSL\bin/ TFTP
Filename................................. final.pem This may take some time. Are you
sure you want to start? (y/N) y TFTP Webadmin cert transfer starting. Certificate
installed. Reboot the switch to use new certificate.
```
Remarque: Afin d'installer un tiers certificat pour l'authentification administrative (d'admin) (pour un utilisateur qui essaye d'ouvrir une session au WLC avec l'utilisation de HTTPS), changez le type de données au **webadmincert** dans la commande de **transfer download datatype**, et répétez les étapes 3 à 5 de cette procédure.
6. Émettez cette commande afin d'activer HTTPS :>**config network secureweb enable**
7. Sauvegardez le certificat ssl, introduisez, et sécurisez le mot de passe de Web à NVRAM de sorte que vos modifications soient retenues à travers des réinitialisations.>**save config** Are you sure you want to save? (y/n) y Configuration Saved!
8. Redémarrez le contrôleur.>**reset system** Are you sure you would like to reset the system? (y/n) y System will now restart! The controller reboots. **Remarque:** Si un certificat est déjà installé, la procédure pour télécharger un neuf efface le vieil.

Vérifiez

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

L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes **show**. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show** .

Vous pouvez employer la commande de **show certificate summary** sur le WLC afin de vérifier si le WLC utilise le tiers certificat comme prévu. Voici un exemple :

```
(Cisco Controller) >show certificate summary Web Administration Certificate.................
3rd Party Web Authentication Certificate.................. 3rd Party Certificate compatibility
mode:.................. off
```

La sortie confirme qu'un tiers certificat est utilisé en tant que le certificat d'administration web et certificat d'authentification Web.

La prochaine fois que cela des essais d'un utilisateur à ouvrir une session au réseau WLAN avec l'utilisation de l'authentification Web basée sur SSL, l'utilisateur n'est pas incité pour recevoir une alerte de sécurité Web, à condition que le tiers certificat qui est installé sur le WLC soit dans la liste de CAs de confiance ce les prises en charge du navigateur de client.

Dépannez

Remarque: Référez-vous aux informations importantes sur les commandes de débogage avant d'utiliser les commandes de **débogage**.

Vous pouvez utiliser la commande d'**enable de PKI de debug pm** sur le WLC. Exécutez la commande quand vous installez le certificat sur le WLC.

Toutes les fois que tous les transferts à ou du contrôleur se produisent, il est utile d'activer le **debug transfer toute la** commande d'**enable** et de réexécuter le transfert afin de voir les détails de ce qui s'est produit. Les transferts peuvent échouer en transit (le numéro approprié de bits ou les octets ne se déplacent pas du serveur au contrôleur), ou une fois que le fichier y arrive, le contenu est l'un ou l'autre d'illisible au contrôleur ou ne s'avère pas approprié pour la fonction désirée.

Informations connexes

- Mise à niveau logicielle du contrôleur LAN sans fil (WLC)
- Génération d'une demande CSR pour des certificats tiers et téléchargement des certificats chaînés sur le contrôleur de réseau local sans fil
- Dépannage du contrôleur LAN sans fil (WLC) - FAQ
- Guide de configuration du contrôleur LAN sans fil Cisco, version 4.0
- Assistance produit sans fil
- OpenSSL Project
- Support et documentation techniques - Cisco Systems