

Mettre à jour le certificat ASA sur CUCM pour Phone VPN avec la fonctionnalité AnyConnect

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Informations générales](#)

[Comment mettre à jour le certificat ASA sans interruption des services de téléphones VPN ?](#)

[Vérification](#)

[Informations connexes](#)

Introduction

Ce document décrit le processus correct de mise à jour du certificat ASA (Adaptative Security Appliance) sur Cisco Unified Communications Manager (CUCM) pour les téléphones sur un réseau privé virtuel (VPN) avec la fonctionnalité AnyConnect afin d'éviter toute interruption du service téléphonique.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- VPN téléphonique avec fonctionnalité AnyConnect.
- Certificats ASA et CUCM.

Components Used

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

- Cisco Unified Communications Manager 10.5.2.15900-8.
- Logiciel Cisco Adaptive Security Appliance Version 9.8(2)20.
- Téléphone IP Cisco CP-8841.

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

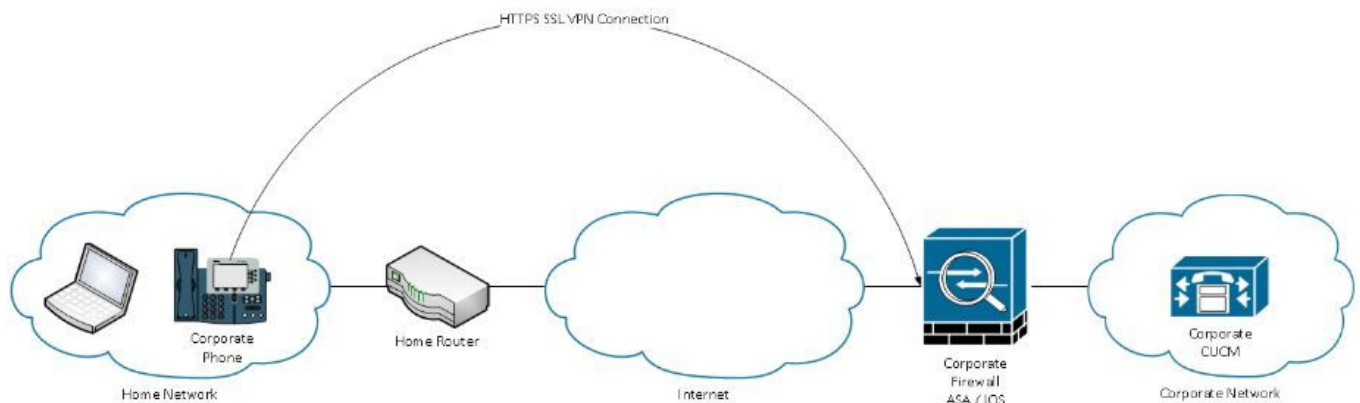
La fonctionnalité VPN téléphonique avec AnyConnect permet la fourniture d'un service téléphonique via une connexion VPN.

Avant que le téléphone ne soit prêt pour le VPN, il doit d'abord être configuré dans le réseau interne. Cela nécessite un accès direct au serveur TFTP CUCM (Trivial File Transfer Protocol).

La première étape après la configuration complète de l'ASA est de prendre le certificat HTTPS (Hypertext Transfer Protocol Secure) ASA et de le télécharger sur le serveur CUCM en tant que Phone-VPN-trust, et de l'affecter à la passerelle VPN correcte dans CUCM. Cela permet au serveur CUCM de créer un fichier de configuration de téléphone IP qui indique au téléphone comment accéder à l'ASA.

Le téléphone doit être configuré à l'intérieur du réseau avant de pouvoir être déplacé hors du réseau et utiliser la fonctionnalité VPN. Une fois le téléphone configuré en interne, il peut être déplacé vers le réseau externe pour l'accès VPN.

Le téléphone se connecte sur le port TCP 443 via HTTPS à l'ASA. L'ASA répond avec le certificat configuré et vérifie le certificat présenté.



Comment mettre à jour le certificat ASA sans interruption des services de téléphones VPN ?

À un moment donné, le certificat ASA doit être modifié, en raison de circonstances par exemple.

Le certificat est sur le point d'expirer

Le certificat est signé par un tiers et l'autorité de certification (AC) change, etc.

Il y a quelques étapes à suivre afin d'éviter l'interruption de service pour les téléphones qui sont connectés à CUCM via VPN avec AnyConnect.

Attention : Si les étapes ne sont pas suivies, les téléphones doivent à nouveau être configurés sur le réseau interne avant d'être déployés sur un réseau externe.

Étape 1. Générez le nouveau certificat ASA mais ne l'appliquez pas encore à l'interface.

Le certificat peut être autosigné ou signé par l'autorité de certification.

Note: Pour plus d'informations sur les certificats ASA, reportez-vous à [Configuration des certificats numériques](#)

Étape 2. Téléchargez ce certificat dans CUCM en tant qu'approbation VPN téléphonique sur le serveur de publication CUCM.

Connectez-vous à Call Manager et accédez à **Unified OS Administration > Security > Certificate Management > Upload Certificate > Select Phone-VPN-trust.**

Par recommandation, téléchargez la chaîne de certificats complète, si les certificats racine et intermédiaire sont déjà téléchargés sur CUCM, passez à l'étape suivante.

Attention : N'oubliez pas que si l'ancien certificat d'identité et le nouveau ont le même CN (Common Name) vous devez suivre la solution de contournement pour le bogue [CSCuh19734](#) afin d'éviter que le nouveau certificat écrase l'ancien. De cette manière, le nouveau certificat se trouve dans la base de données pour la configuration de la passerelle VPN téléphonique, mais l'ancien n'est pas écrasé.

Étape 3. Sur la passerelle VPN, sélectionnez les deux certificats (l'ancien et le nouveau).

Accédez à **Cisco Unified CM Administration > Advanced Features > VPN > VPN Gateway.**

Vérifiez que vous avez les deux certificats dans le champ Certificats VPN de ce site.

VPN Gateway Configuration Related Links: [Back To](#)

Save ✖ Delete Copy + Add New

Status

i Status: Ready

VPN Gateway Information

VPN Gateway Name*

VPN Gateway Description

VPN Gateway URL*

VPN Gateway Certificates

VPN Certificates in your Truststore

▼ ▲

VPN Certificates in this Location*

SUBJECT: CN=sslvpn.gti-usa.net ISSUER: CN=RapidSSL RSA CA 2018,OU=www.digicert.com,O=DigiCert Inc,C=US S/I

Save Delete Copy Add New

Étape 4. Vérifiez que le groupe VPN, le profil et le profil de téléphone commun sont définis correctement.

Étape 5. Réinitialisez les téléphones.

Cette étape permet aux téléphones de télécharger les nouveaux paramètres de configuration et de s'assurer que les deux certificats sont hachés, afin qu'ils puissent faire confiance à l'ancien et au nouveau certificat.

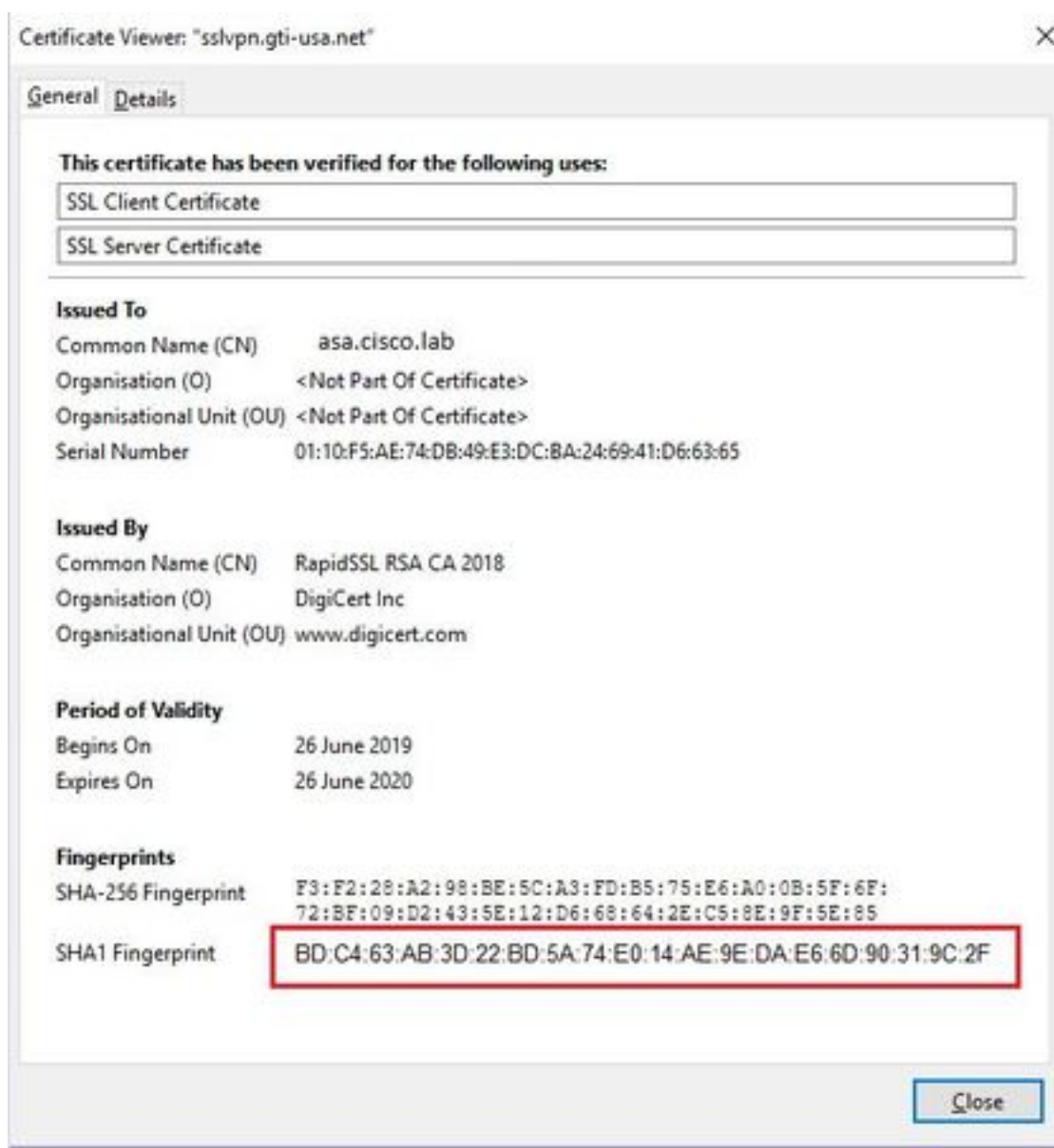
Étape 6. Appliquez le nouveau certificat sur l'interface ASA.

Une fois le certificat appliqué à l'interface ASA, les téléphones doivent faire confiance à ce nouveau certificat car ils ont les deux hachages de certificat de l'étape précédente.

Vérification

Utilisez cette section afin de confirmer que vous avez suivi correctement les étapes.

Étape 1. Ouvrez les anciens et nouveaux certificats ASA et notez l'empreinte SHA-1.



Étape 2. Choisissez un téléphone qui doit être connecté via VPN et collectez son fichier de configuration.

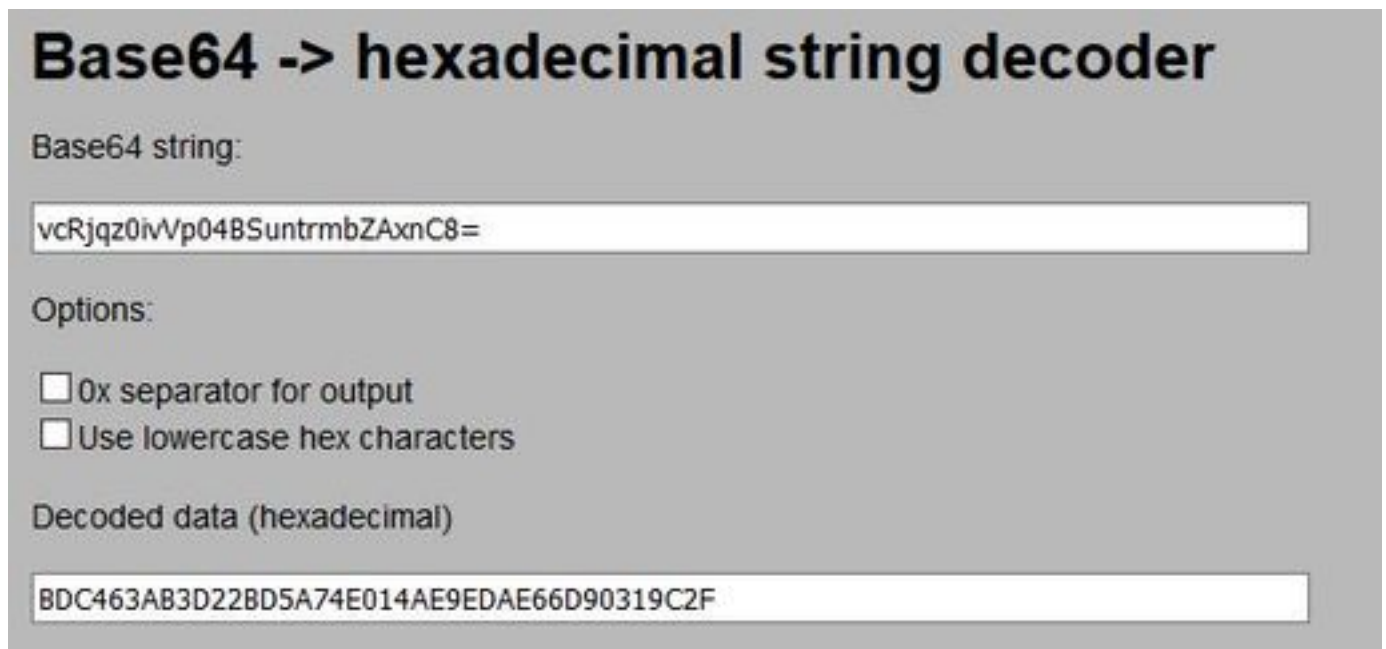
Note: Pour plus d'informations sur la collecte du fichier de configuration du téléphone,

reportez-vous à la section [Deux façons d'obtenir le fichier de configuration d'un téléphone à partir de CUCM](#)

Étape 3. Une fois que vous avez le fichier de configuration, recherchez la section :

```
<vpnGroup>  
<mtu>1290</mtu>  
<failConnectTime>30</failConnectTime>  
<authMethod>2</authMethod>  
<pswdPersistent>0</pswdPersistent>  
<autoNetDetect>1</autoNetDetect>  
<enableHostIDCheck>0</enableHostIDCheck>  
<addresses>  
<url1> https://radc.cgsinc.com/Cisco_VOIP_VPN</url1>;  
</addresses>  
<credentials>  
<hashAlg>0</hashAlg>  
  
    </credentials>  
</vpnGroup>
```

Étape 4. Le hachage dans le fichier de configuration est imprimé au format Base 64 et dans le certificat ASA est imprimé au format hexadécimal. Vous pouvez donc utiliser un décodeur de Base 64 à Hexadécimal pour vérifier que les deux hachages (téléphone et ASA) correspondent.



Base64 -> hexadecimal string decoder

Base64 string:

vcRjqz0ivVp04BSuntrmbZAxnC8=

Options:

0x separator for output

Use lowercase hex characters

Decoded data (hexadecimal)

BDC463A83D228D5A74E014AE9EDAE66D90319C2F

Informations connexes

Pour plus d'informations sur la fonction Téléphone VPN AnyConnect :

- Configurez le téléphone VPN AnyConnect avec authentification de certificat sur un ASA. <https://www.cisco.com/c/en/us/support/docs/unified-communications/unified-communications->

<manager-callmanager/115785-anyconnect-vpn-00.html>