

ASA Certificate op CUCM bijwerken voor telefoon VPN met AnyConnect-functie

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Hoe kan het ASA-certificaat zonder onderbreking van VPN-telefoons worden bijgewerkt?](#)

[Verifiëren](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft het juiste proces om het certificaat van Adaptieve security applicatie (ASA) aan te passen op Cisco Unified Communications Manager (CUCM) voor telefoons via Virtual Private Network (VPN) met AnyConnect om onderbreking van de telefoonservice te voorkomen.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Bel VPN met AnyConnect-functie.
- ASA- en CUCM-certificaten.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco Unified Communications Manager 10.5.2.15900-8.
- Software voor Cisco adaptieve security applicatie, versie 9.8(2)20.
- Cisco IP-telefoon CP-8841.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Achtergrondinformatie

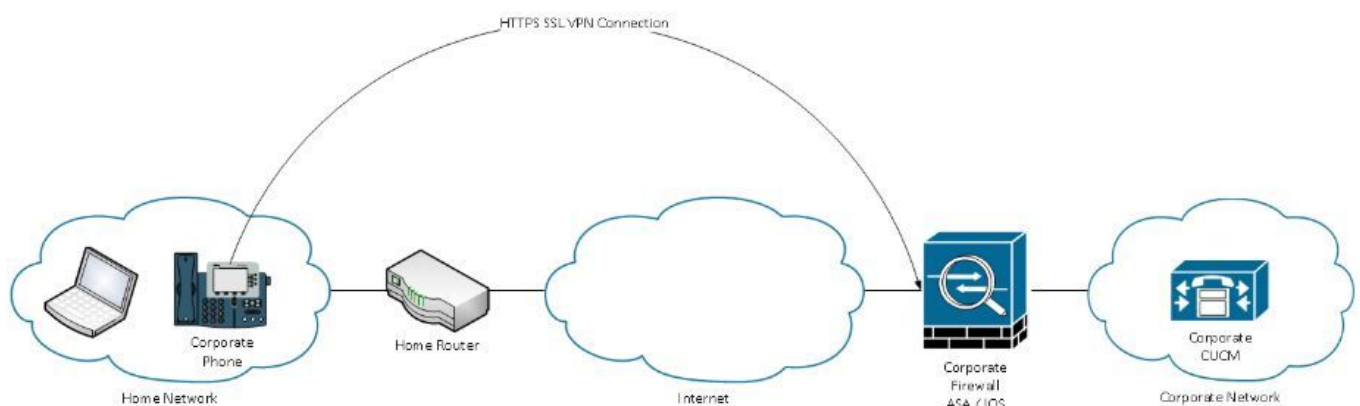
Telefonische VPN-functie met AnyConnect maakt telefoonservice via VPN-verbinding mogelijk.

Voordat de telefoon voor VPN klaar is, moet eerst de voorziening in het interne netwerk plaatsvinden. Dit vereist directe toegang tot de CUCM TFTP (Trivial File Transfer Protocol) server.

De eerste stap nadat de ASA volledig is geconfigureerd is om het ASA Hypertext Transfer Protocol Secure (HTTPS)-certificaat te nemen en het als telefoon-VPN-trust naar de CUCM-server te uploaden, en het toe te wijzen aan de juiste VPN-gateway in CUCM. Dit staat de CUCM-server toe om een IP-telefoon-configuratiebestand te bouwen dat de telefoon vertelt hoe te beginnen met de ASA.

De telefoon moet binnen het netwerk van tevoren zijn voorzien voordat hij buiten het netwerk kan worden verplaatst en de VPN-functie kan gebruiken. Nadat de telefoon intern is gevoed, kan het naar het externe netwerk voor de toegang van VPN worden verplaatst.

De telefoon sluit op TCP poort 443 over HTTPS aan op de ASA. De ASA reageert terug met het geconfigureerde certificaat en verifieert het aangeboden certificaat.



Hoe kan het ASA-certificaat zonder onderbreking van VPN-telefoons worden bijgewerkt?

Op een bepaald moment moet het ASA-certificaat worden gewijzigd, bijvoorbeeld door omstandigheden.

Het certificaat verstrijkt op het punt

Het certificaat is ondertekend door derden en de wijziging van de certificaatinstantie (CA), enz.

Er zijn een aantal stappen te volgen om onderbreking van de service voor telefoons die met CUCM via VPN met AnyConnect worden verbonden, te voorkomen.

Voorzichtig: Als de stappen niet worden gevolgd, moeten de telefoons opnieuw op het interne netwerk worden voorzien voordat ze op een extern netwerk kunnen worden ingezet.

Stap 1. Generate het nieuwe ASA certificaat maar pas het nog niet toe op de interface.

Het certificaat kan zelf ondertekend zijn of door CA ondertekend worden.

Opmerking: Raadpleeg voor meer informatie over ASA-certificaten de [configuratie van digitale certificaten](#)

Stap 2. Upload dat certificaat in CUCM als telefoon VPN op de CUCM Publisher.

Meld u aan bij Call Manager en navigeer naar **Unified OS-beheer > Beveiliging > Certificaatbeheer > Uploadcertificaat > Selecteer Phone-VPN-trust.**

Als een aanbeveling, uploadt u de gehele certificeringsketen, indien de wortel- en tussencertificaten al op CUCM zijn geüpload, naar de volgende stap.

Voorzichtig: Houdt u in gedachten Als het oude identiteitsbewijs en het nieuwe certificaat dezelfde GN hebben (Gemeenschappelijke Naam), dan moet u het werkkader voor het bug [CSCuh19734](#) volgen om te voorkomen dat het nieuwe certificaat de oudere overschrijft. Op die manier is het nieuwe certificaat in de database voor de configuratie van de VPN-gateway maar de oude niet overschreven.

Stap 3. Selecteer in de VPN-poort beide certificaten (de oude en de nieuwe).

Navigeer naar **Cisco Unified CM-beheer > Geavanceerde functies > VPN > VPN-gateway.**

Zorg ervoor dat u beide certificaten in het veld VPN-certificaten in dit veld Locatie hebt.

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

Save Delete Copy Add New

Status
Status: Ready

VPN Gateway Information
VPN Gateway Name* GTI-VPN-Phone
VPN Gateway Description
VPN Gateway URL* https://10.100.172.135 /VPNPhone

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

Stap 4. Controleer of de VPN-groep, het profiel en het gemeenschappelijke telefoonprofiel correct zijn ingesteld.

Stap 5. Zet de telefoons terug.

Deze stap stelt de telefoons in staat om de nieuwe configuratie instellingen te downloaden en

garandeert dat de telefoons beide certificaten hebben, zodat ze in het oude en in het nieuwe certificaat kunnen vertrouwen.

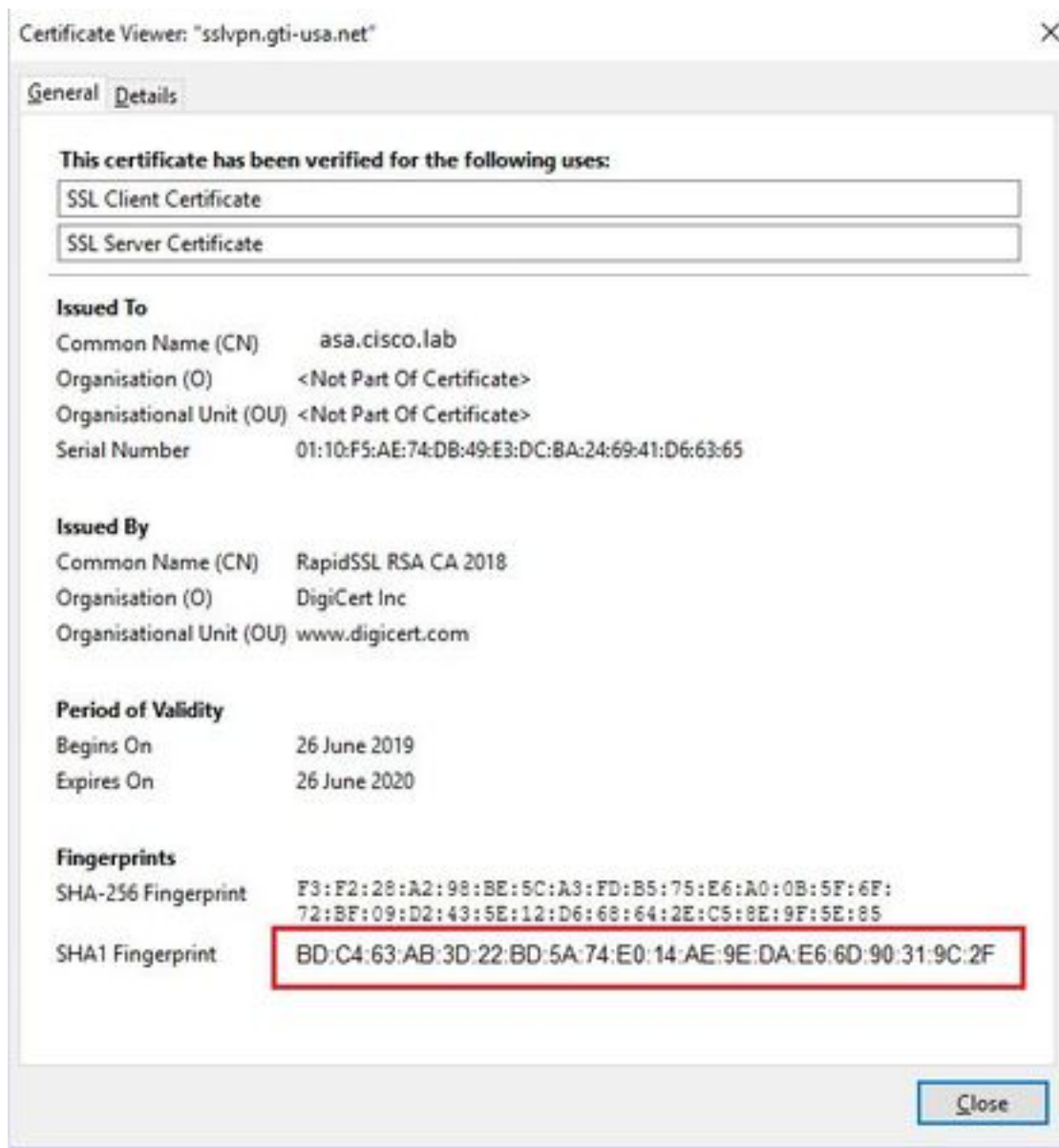
Stap 6. Pas het nieuwe certificaat op de ASA-interface toe.

Zodra het certificaat op de ASA interface wordt toegepast, zouden de telefoons in dat nieuwe certificaat moeten vertrouwen aangezien zij beide certificaat hebben van de vorige stap hebben.

Verifiëren

Gebruik dit gedeelte om te bevestigen dat u de stappen correct hebt gevolgd.

Stap 1. Open de oude en nieuwe ASA-certificaten en noteer de SHA-1-vingerafdruk.



Stap 2. Kies een telefoon die via VPN moet worden aangesloten en verzamel het configuratiebestand.

Opmerking: Raadpleeg voor meer informatie over het verzamelen van telefoonconfiguratiebestanden [twee manieren om het configuratiebestand van een telefoon](#)

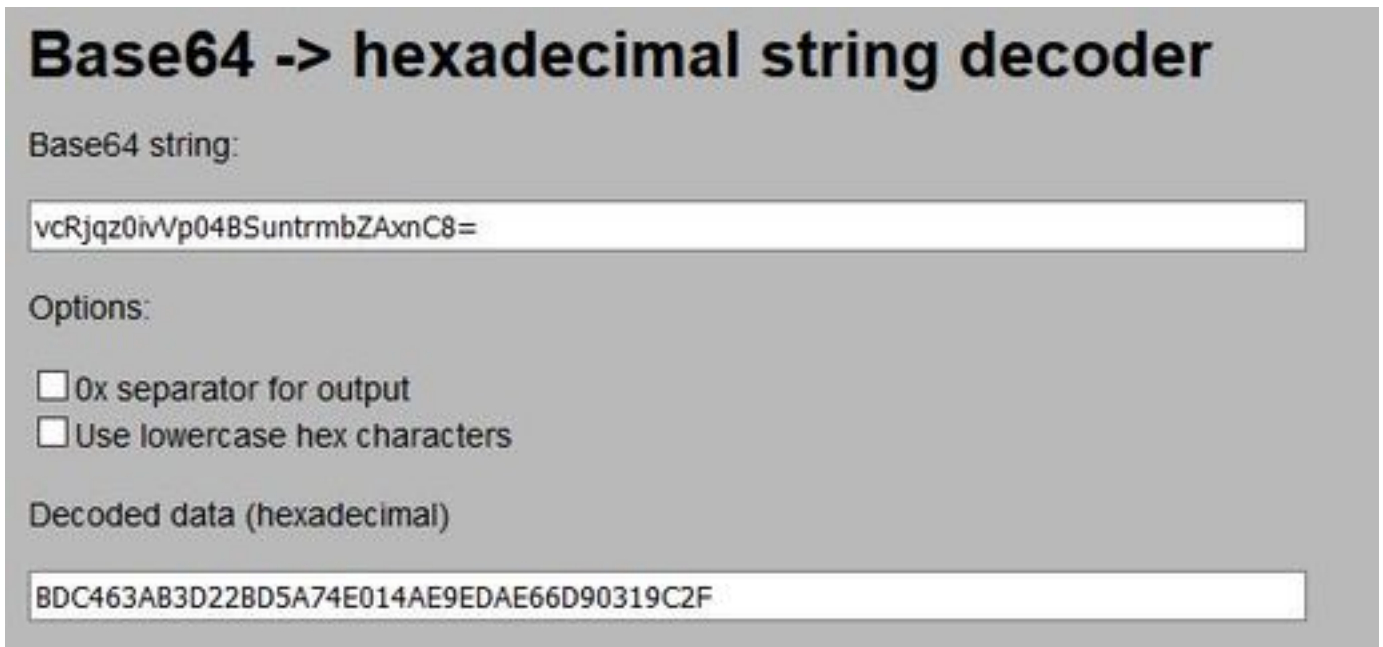
[in CUCM te verkrijgen](#)

Stap 3. Zodra u het configuratiebestand hebt, zoekt u het gedeelte:

```
<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>
```

Stap 4. De hash in het configuratiebestand is afgedrukt in Base64-formaat en in het ASA-certificaat is afgedrukt in hexadecimaal formaat, zodat u een decoder van Base64 naar Hexadecimaal kunt gebruiken om te controleren of beide hashed (telefoon en ASA)-match hebben.



The image shows a web-based tool titled "Base64 -> hexadecimal string decoder". It has a text input field containing the Base64 string "vcRjqz0ivVp04BSuntrmbZAxnC8=". Below the input field are two checkboxes: "0x separator for output" and "Use lowercase hex characters", both of which are unchecked. Below the checkboxes is a label "Decoded data (hexadecimal)" and a text output field containing the hexadecimal string "BDC463A83D22BD5A74E014AE9EDAE66D90319C2F".

Gerelateerde informatie

Voor meer informatie over de functie AnyConnect VPN-telefoon:

- Configuratie van AnyConnect VPN-telefoon met certificaatverificatie op een ASA.

<https://www.cisco.com/c/en/us/support/docs/unified-communications/unified-communications->

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