Aktualisieren des ASA-Zertifikats auf dem CUCM für Telefon-VPN mit der AnyConnect-Funktion

Inhalt

Einführung

In diesem Dokument wird der richtige Prozess zur Aktualisierung des ASA-Zertifikats (Adaptative Security Appliance) von Cisco Unified Communications Manager (CUCM) für Telefone über Virtual Private Network (VPN) mit AnyConnect-Funktion beschrieben, um Unterbrechungen des Telefondienstes zu vermeiden.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Telefon-VPN mit AnyConnect-Funktion
- ASA- und CUCM-Zertifikate.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

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

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

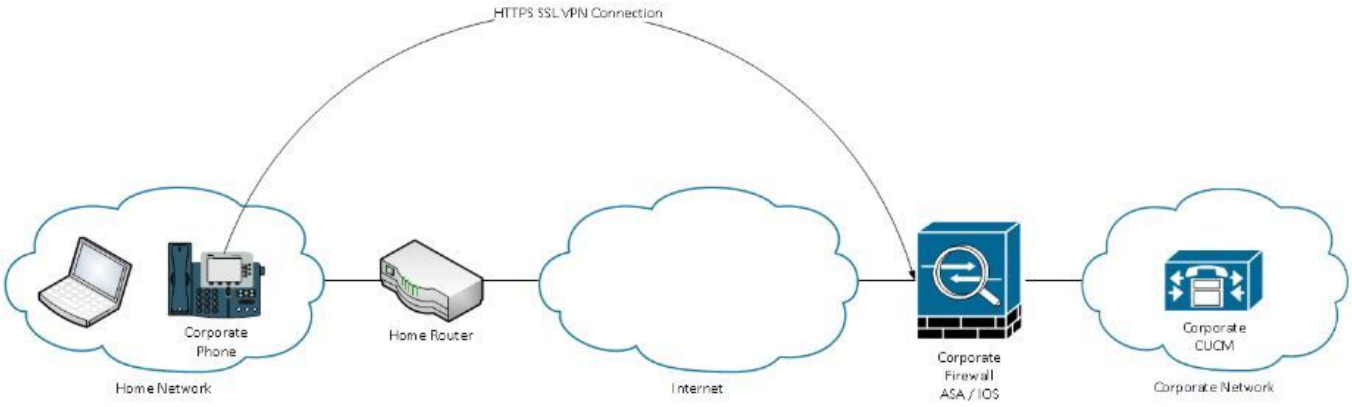
Die Telefon-VPN-Funktion mit AnyConnect ermöglicht die Bereitstellung von Telefondiensten über eine VPN-Verbindung.

Bevor das Telefon für VPN gerüstet ist, muss es zunächst im internen Netzwerk bereitgestellt werden. Hierzu ist ein direkter Zugriff auf den CUCM TFTP-Server (Trivial File Transfer Protocol) erforderlich.

Der erste Schritt nach der vollständigen Konfiguration der ASA besteht darin, das ASA Hypertext Transfer Protocol Secure (HTTPS)-Zertifikat hochzuladen und als Phone-VPN-trust auf den CUCM-Server hochzuladen und es dem richtigen VPN-Gateway im CUCM zuzuweisen. Auf diese Weise kann der CUCM-Server eine Konfigurationsdatei für das IP-Telefon erstellen, die dem Telefon mitteilt, wie es zur ASA gelangt.

Das Telefon muss innerhalb des Netzwerks bereitgestellt werden, bevor es aus dem Netzwerk verschoben werden kann und die VPN-Funktion verwendet werden kann. Nachdem das Telefon intern bereitgestellt wurde, kann es für den VPN-Zugriff in das externe Netzwerk verschoben werden.

Das Telefon verbindet sich über den TCP-Port 443 über HTTPS mit der ASA. Die ASA antwortet mit dem konfigurierten Zertifikat und verifiziert das angegebene Zertifikat.



Aktualisierung des ASA-Zertifikats ohne Unterbrechung der VPN-Telefondienste

Das ASA-Zertifikat muss irgendwann geändert werden, z. B. aufgrund von Umständen.

Das Zertifikat läuft bald ab.

Das Zertifikat ist von einem Drittanbieter signiert, und die Zertifizierungsstelle (Certificate Authority, CA) ändert usw.

Es müssen einige Schritte befolgt werden, um eine Unterbrechung des Diensts für Telefone zu vermeiden, die über VPN mit AnyConnect mit dem CUCM verbunden sind.

> **Vorsicht**: Wenn die Schritte nicht befolgt werden, müssen die Telefone erneut im internen Netzwerk bereitgestellt werden, bevor sie in einem externen Netzwerk bereitgestellt werden können.

Schritt 1: Generieren Sie das neue ASA-Zertifikat, wenden Sie es jedoch noch nicht auf die Schnittstelle an.

Das Zertifikat kann selbst signiert oder eine Zertifizierungsstelle signiert werden.

> **Hinweis**: Weitere Informationen zu ASA-Zertifikaten finden Sie unter Konfigurieren digitaler Zertifikate.

Schritt 2: Laden Sie dieses Zertifikat in CUCM als Phone VPN Trust auf den CUCM Publisher hoch.

Melden Sie sich beim Call Manager an, und navigieren Sie zu **Unified OS Administration > Security > Certificate Management > Upload Certificate > Select Phone-VPN-trust.**

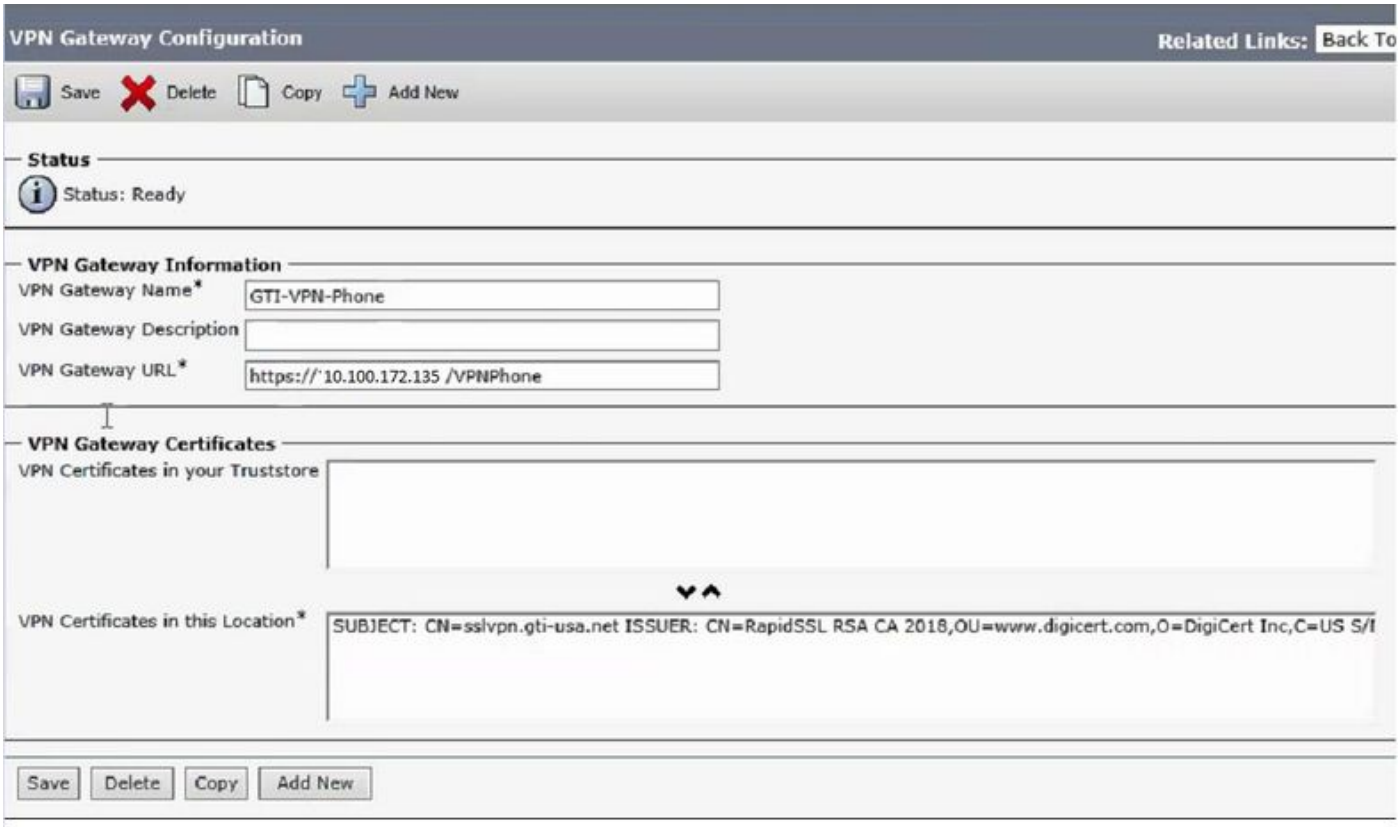
Laden Sie als Empfehlung die vollständige Zertifikatskette hoch. Wenn die Root- und Zwischenzertifikate bereits auf CUCM hochgeladen wurden, fahren Sie mit dem nächsten Schritt fort.

> **Vorsicht**: Wenn das alte Identitätszertifikat und das neue dasselbe CN (Common Name) haben, müssen Sie der Problemumgehung für den Fehler CSCuh19734 folgen, um zu verhindern, dass das neue Zertifikat das ältere überschreibt. Auf diese Weise befindet sich das neue Zertifikat in der Datenbank für die Telefon-VPN-Gateway-Konfiguration, das alte Zertifikat wird jedoch nicht überschrieben.

Schritt 3: Wählen Sie auf dem VPN-Gateway beide Zertifikate aus (das alte und das neue).

Navigieren Sie zu **Cisco Unified CM Administration > Advanced Features > VPN > VPN Gateway.**

Vergewissern Sie sich, dass beide Zertifikate im Feld "VPN Certificates" (VPN-Zertifikate) in diesem Feld "Location" (Ort) vorhanden sind.



Schritt 4: Überprüfen Sie, ob die VPN-Gruppe, das Profil und das allgemeine Telefonprofil korrekt eingestellt sind.

Schritt 5: Telefone zurückgesetzt.

Dieser Schritt ermöglicht es den Telefonen, die neuen Konfigurationseinstellungen herunterzuladen, und stellt sicher, dass beide Telefone über Hashes von Zertifikaten verfügen, sodass sie auf das alte und das neue Zertifikat vertrauen können.

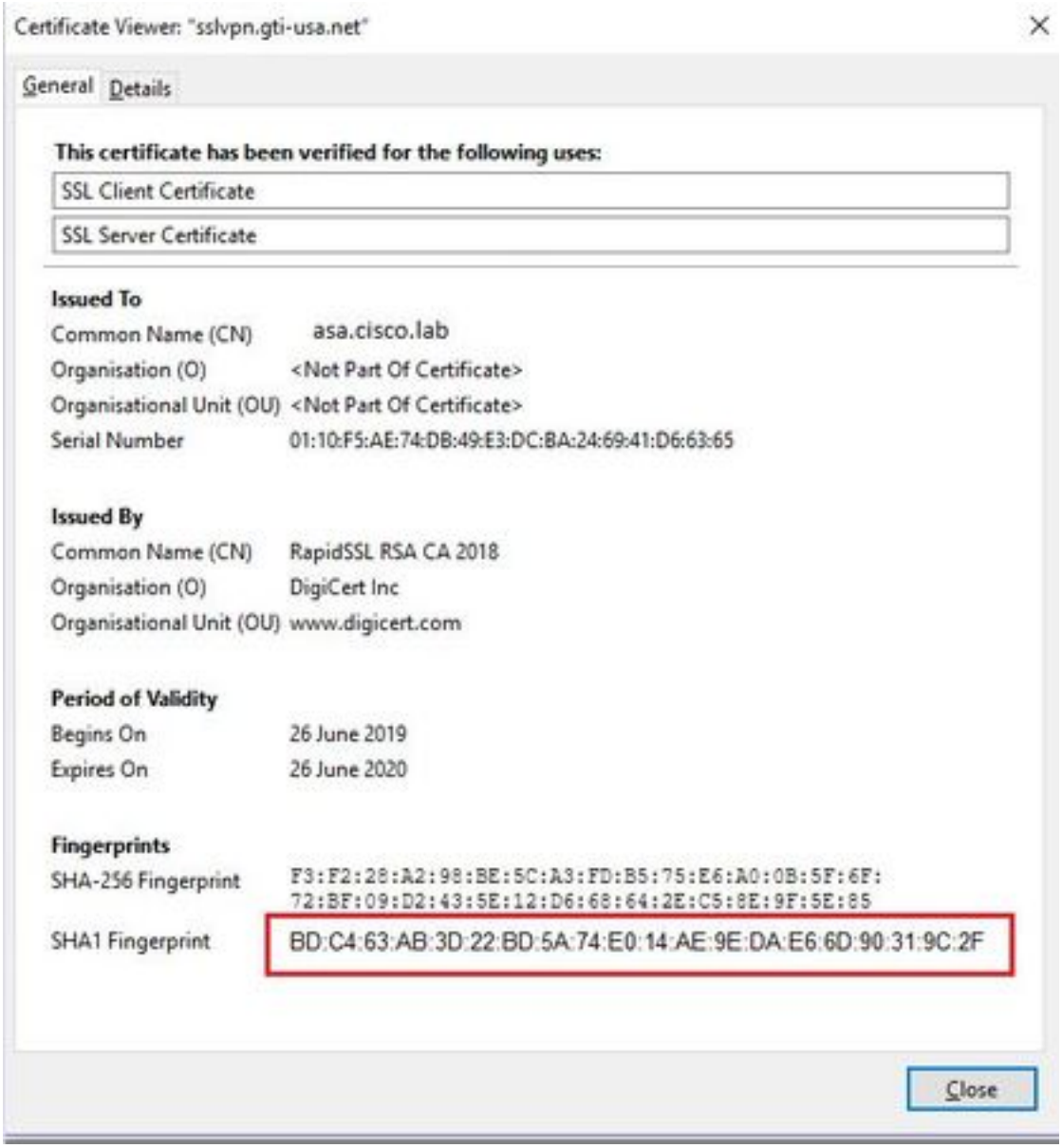
Schritt 6: Wenden Sie das neue Zertifikat auf der ASA-Schnittstelle an.

Wenn das Zertifikat auf der ASA-Schnittstelle angewendet wurde, sollten die Telefone diesem neuen Zertifikat vertrauen, da beide Zertifikatshashes aus dem vorherigen Schritt stammen.

Überprüfen

In diesem Abschnitt überprüfen Sie, ob Sie die Schritte ordnungsgemäß ausgeführt haben.

Schritt 1: Öffnen Sie die alten und neuen ASA-Zertifikate, und notieren Sie sich den SHA-1-Fingerabdruck.



Schritt 2: Wählen Sie ein Telefon aus, das über VPN verbunden werden soll, und sammeln Sie dessen Konfigurationsdatei.

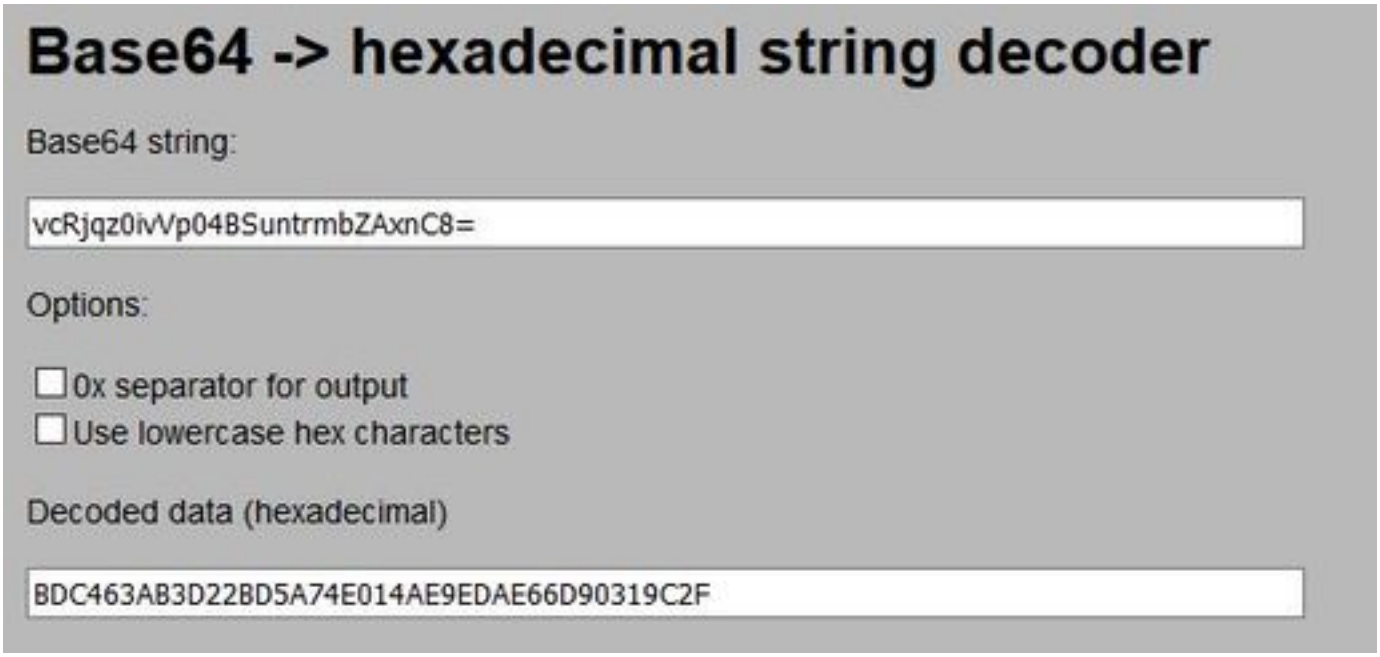
> **Hinweis**: Weitere Informationen zum Erfassen der Konfigurationsdatei für das Telefon finden Sie unter Two Ways to Obtain a Phone's Configuration File from CUCM (Zwei Möglichkeiten zum Abrufen der Konfigurationsdatei eines Telefons vom CUCM).

Schritt 3: Sobald Sie die Konfigurationsdatei haben, suchen Sie nach dem Abschnitt:

```
<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>
```

Schritt 4: Der Hash in der Konfigurationsdatei wird im Base 64-Format gedruckt, und das ASA-Zertifikat wird im Hexadezimalformat gedruckt. Sie können also einen Decoder von Base 64 bis Hexadezimal verwenden, um zu überprüfen, ob beide Hashs (Telefon und ASA) übereinstimmen.



Zugehörige Informationen

Weitere Informationen zur Funktion des AnyConnect VPN-Telefons finden Sie unter:

- **Konfigurieren Sie das AnyConnect VPN-Telefon mit der Zertifikatsauthentifizierung auf einer ASA.**

https://www.cisco.com/c/en/us/support/docs/unified-communications/unified-communications-manager-callmanager/115785-anyconnect-vpn-00.html