

使用AnyConnect功能更新CUCM上的ASA证书，用于电话VPN

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[如何更新ASA证书而不中断VPN电话服务？](#)

[验证](#)

[相关信息](#)

简介

本文档介绍在Cisco Unified Communications Manager(CUCM)上通过具有AnyConnect功能的虚拟专用网络(VPN)为电话更新自适应安全设备(ASA)证书的正确过程，以避免电话服务中断。

先决条件

要求

Cisco 建议您了解以下主题：

- 具有AnyConnect功能的电话VPN。
- ASA和CUCM证书。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科统一通信管理器10.5.2.15900-8。
- 思科自适应安全设备软件版本9.8(2)20。
- 思科IP电话CP-8841。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

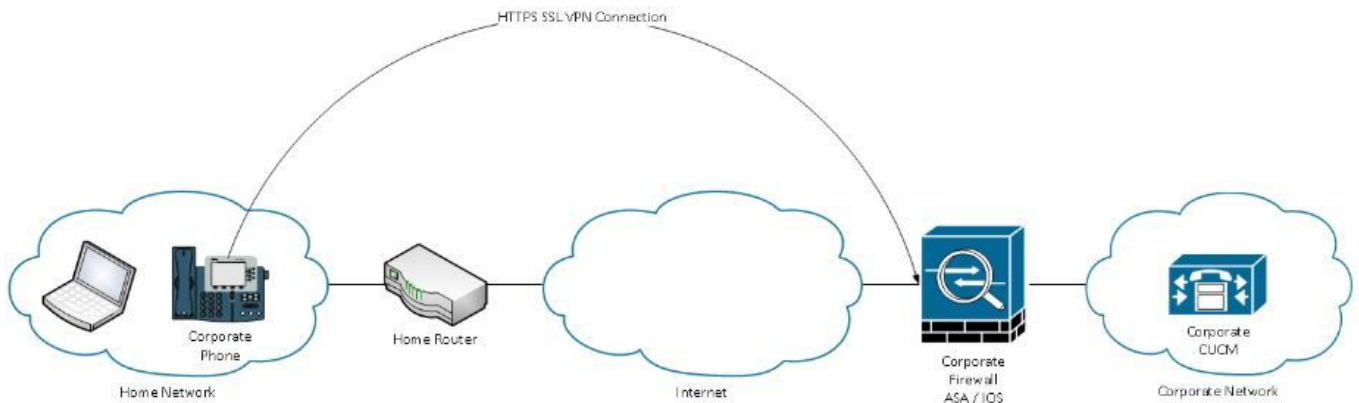
带AnyConnect的电话VPN功能允许通过VPN连接调配电话服务。

在电话准备好使用VPN之前，必须先在内网中进行调配。这需要直接访问CUCM TFTP（简单文件传输协议）服务器。

完全配置ASA后的第一步是获取ASA超文本传输协议安全(HTTPS)证书并将其作为Phone-VPN-trust上传到CUCM服务器，并将其分配到CUCM中的正确VPN网关。这允许CUCM服务器构建IP电话配置文件，告知电话如何到达CUCMASA。

电话必须在网络内部调配，才能在网络外部移动并使用VPN功能。在内部调配电话后，可将其移至外部网络进行VPN访问。

电话通过HTTPS在TCP端口443上连接到ASA。ASA以已配置的证书作出响应，并验证所提供的证书。



如何更新ASA证书而不中断VPN电话服务？

在某些时候，ASA证书需要更改，例如，由于任何情况。

证书即将过期

证书是第3方签名的，证书颁发机构(CA)更改等

要避免通过VPN和AnyConnect连接到CUCM的电话的服务中断，需要执行一些步骤。

警告：如果不执行这些步骤，则需要在内部网络上重新调配电话，然后才能在外部网络上部署电话。

步骤1.生成新的ASA证书，但尚未将其应用到接口。

证书可以是自签名或CA签名。

注意：有关ASA证书的详细信息，请参阅[配置数字证书](#)

步骤2.在CUCM中将该证书上传为CUCM发布者上的Phone VPN信任。

登录Call Manager并导航至Unified OS Administration > Security > Certificate Management > Upload Certificate > Select Phone-VPN-trust。

建议上传完整的证书链（如果根证书和中间证书已上传到CUCM上），请转至下一步。

警告：请记住，如果旧身份证书和新身份证书具有相同的CN（公用名），您需要遵循[Bug CSCuh19734](#)的解决方法，以避免新证书覆盖旧证书。这样，新证书就位于电话VPN网关配置的数据库中，但旧证书不会被覆盖。

步骤3.在VPN网关上，选择两个证书（旧证书和新证书）。

导航至Cisco Unified CM Administration > Advanced Features > VPN > VPN Gateway。

确保在此位置字段的VPN证书中同时包含两个证书。

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

Save ✖ Delete Copy + Add New

Status
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*

Save Delete Copy Add New

步骤4.检查VPN组、配置文件和通用电话配置文件是否设置正确。

步骤5.重置电话。

此步骤允许电话下载新配置设置，并确保电话具有两个证书散列，以便他们可以信任旧证书和新证书。

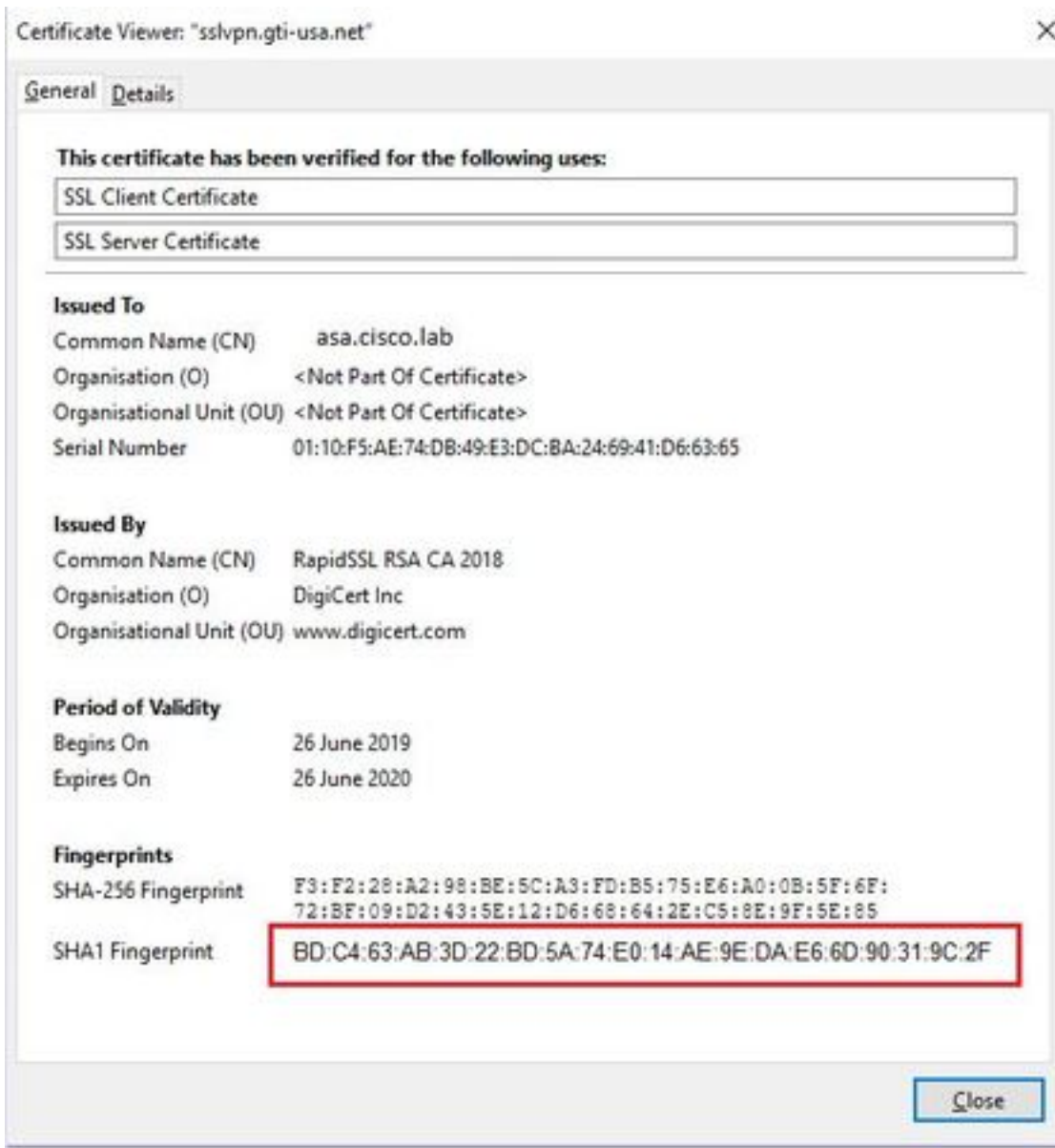
步骤6.在ASA接口上应用新证书。

在ASA接口上应用证书后，电话应信任该新证书，因为它们具有上一步中的两个证书散列。

验证

使用此部分可确认您正确执行了这些步骤。

步骤1.打开旧ASA证书和新ASA证书，并记下SHA-1指纹。



步骤2.选择应通过VPN连接的电话并收集其配置文件。

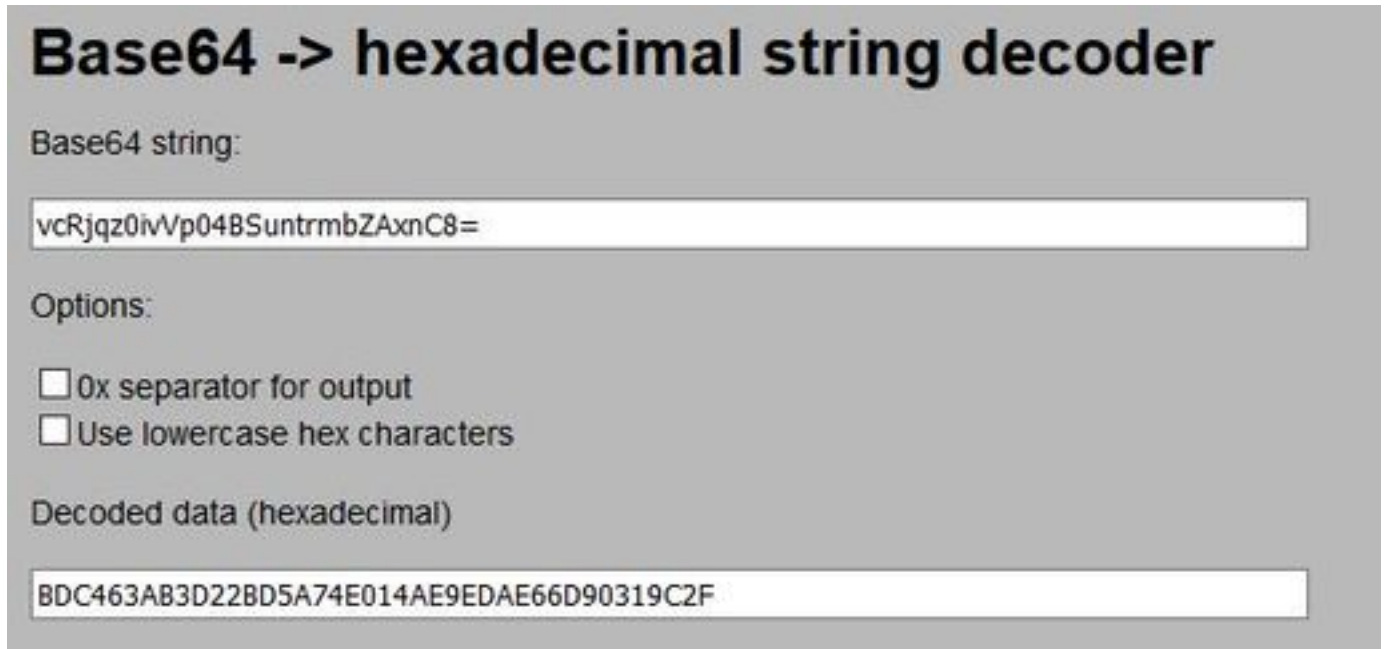
注意：有关如何收集电话配置文件的详细信息，请[参阅从CUCM获取电话配置文件的两种方法](#)

步骤3.获得配置文件后，请查找以下部分：

```
<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>
```

步骤4. 配置文件中的哈希以基64格式打印，ASA证书以十六进制格式打印，因此，您可以使用以64为基数的十六进制解码器来验证哈希（电话和ASA）是否都匹配。



Base64 -> hexadecimal string decoder

Base64 string:

vcRjqz0ivVp04BSuntrmbZAxnC8=

Options:

0x separator for output

Use lowercase hex characters

Decoded data (hexadecimal)

BDC463A83D22BD5A74E014AE9EDAE66D90319C2F

相关信息

有关AnyConnect VPN电话功能的详细信息：

- 在ASA上配置AnyConnect VPN电话的证书身份验证。

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