

Atualize o certificado ASA no CUCM para VPN de telefone com o recurso AnyConnect

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Como atualizar o certificado ASA sem interrupção de serviços de telefones VPN?](#)

[Verificar](#)

[Informações Relacionadas](#)

Introduction

Este documento descreve o processo correto para atualizar o certificado do Adaptive Security Appliance (ASA) no Cisco Unified Communications Manager (CUCM) para telefones sobre VPN (Virtual Private Network) com o recurso AnyConnect para evitar a interrupção do serviço telefônico.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- VPN do telefone com o recurso AnyConnect.
- Certificados ASA e CUCM.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco Unified Communications Manager 10.5.2.15900-8.
- Software Cisco Adaptive Security Appliance versão 9.8(2)20.
- Telefone 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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

O recurso VPN do telefone com o AnyConnect permite o fornecimento de serviço telefônico

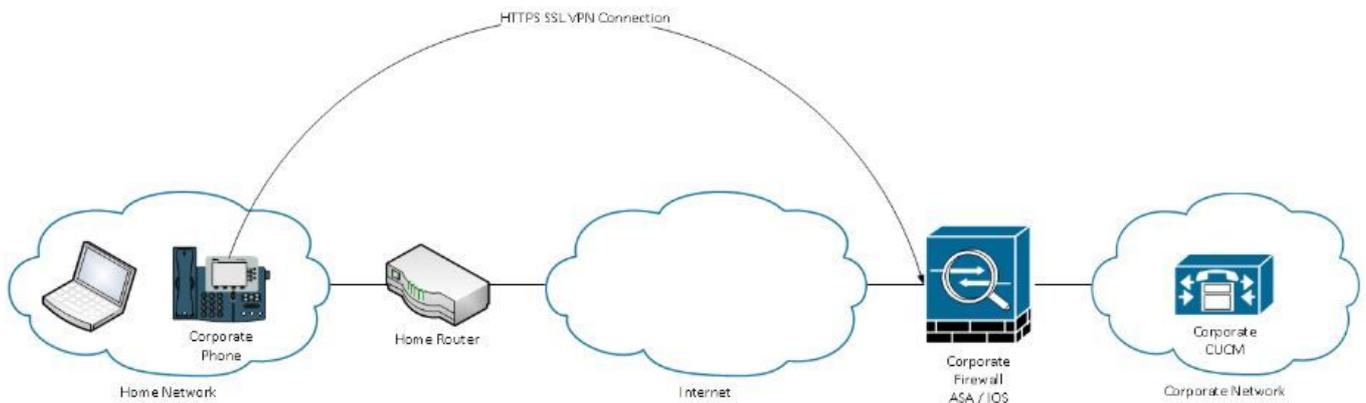
através da conexão VPN.

Antes que o telefone esteja pronto para a VPN, ele deve ser provisionado primeiro na rede interna. Isso exige acesso direto ao servidor TFTP do CUCM (Trivial file transfer Protocol).

A primeira etapa após a configuração completa do ASA é pegar o certificado ASA Hypertext Transfer Protocol Secure (HTTPS) e carregá-lo no servidor CUCM como Phone-VPN-trust e atribuí-lo ao gateway VPN correto no CUCM. Isso permite que o servidor CUCM crie um arquivo de configuração do telefone IP que diz ao telefone como chegar ao ASA.

O telefone deve ser provisionado dentro da rede antes que possa ser movido para fora da rede e usado o recurso VPN. Depois que o telefone for provisionado internamente, ele poderá ser movido para a rede externa para acesso VPN.

O telefone se conecta na porta TCP 443 sobre HTTPS ao ASA. O ASA responde com o certificado configurado e verifica o certificado apresentado.



Como atualizar o certificado ASA sem interrupção de serviços de telefones VPN?

Em algum momento, o certificado ASA precisa ser alterado, devido a quaisquer circunstâncias, por exemplo.

O certificado está prestes a expirar

O certificado é assinado por terceiros e a autoridade de certificação (CA) muda, etc

Há algumas etapas a serem seguidas para evitar a interrupção do serviço para telefones conectados ao CUCM via VPN com AnyConnect.

Caution: Se as etapas não forem seguidas, os telefones precisarão ser provisionados novamente na rede interna antes que possam ser implantados em uma rede externa.

Etapa 1. Gere o novo certificado ASA, mas ainda não o aplique à interface.

O certificado pode ser autoassinado ou CA assinado.

Note: Para obter mais informações sobre certificados ASA, consulte [Configuração de certificados digitais](#)

Etapa 2. Carregue esse certificado no CUCM como confiança de VPN do telefone no Editor do CUCM.

Faça login no Call Manager e navegue para **Unified OS Administration > Security > Certificate Management > Upload Certificate > Select Phone-VPN-trust.**

Como recomendação, faça o upload da cadeia completa de certificados, se os certificados raiz e intermediário já estiverem carregados no CUCM, vá para a próxima etapa.

Caution: Lembre-se de que se o certificado de identidade antigo e o novo tiverem o mesmo CN (Nome Comum), você precisará seguir a solução para o bug [CSCuh19734](#) para evitar que o novo certificado substitua o antigo. Dessa forma, o novo certificado está no banco de dados para a configuração do Gateway VPN do telefone, mas o antigo não é sobrescrito.

Etapa 3. No gateway VPN, selecione ambos os certificados (o antigo e o novo).

Navegue até **Cisco Unified CM Administration > Advanced Features > VPN > VPN Gateway.**

Certifique-se de ter ambos os certificados nos Certificados VPN neste campo Local.

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

Etapa 4. Verifique se o grupo VPN, o perfil e o perfil comum do telefone estão definidos corretamente.

Etapa 5. Reinicie os telefones.

Essa etapa permite que os telefones baixem as novas configurações e garante que os telefones

tenham ambos os hashes de certificados, para que possam confiar no antigo e no novo certificado.

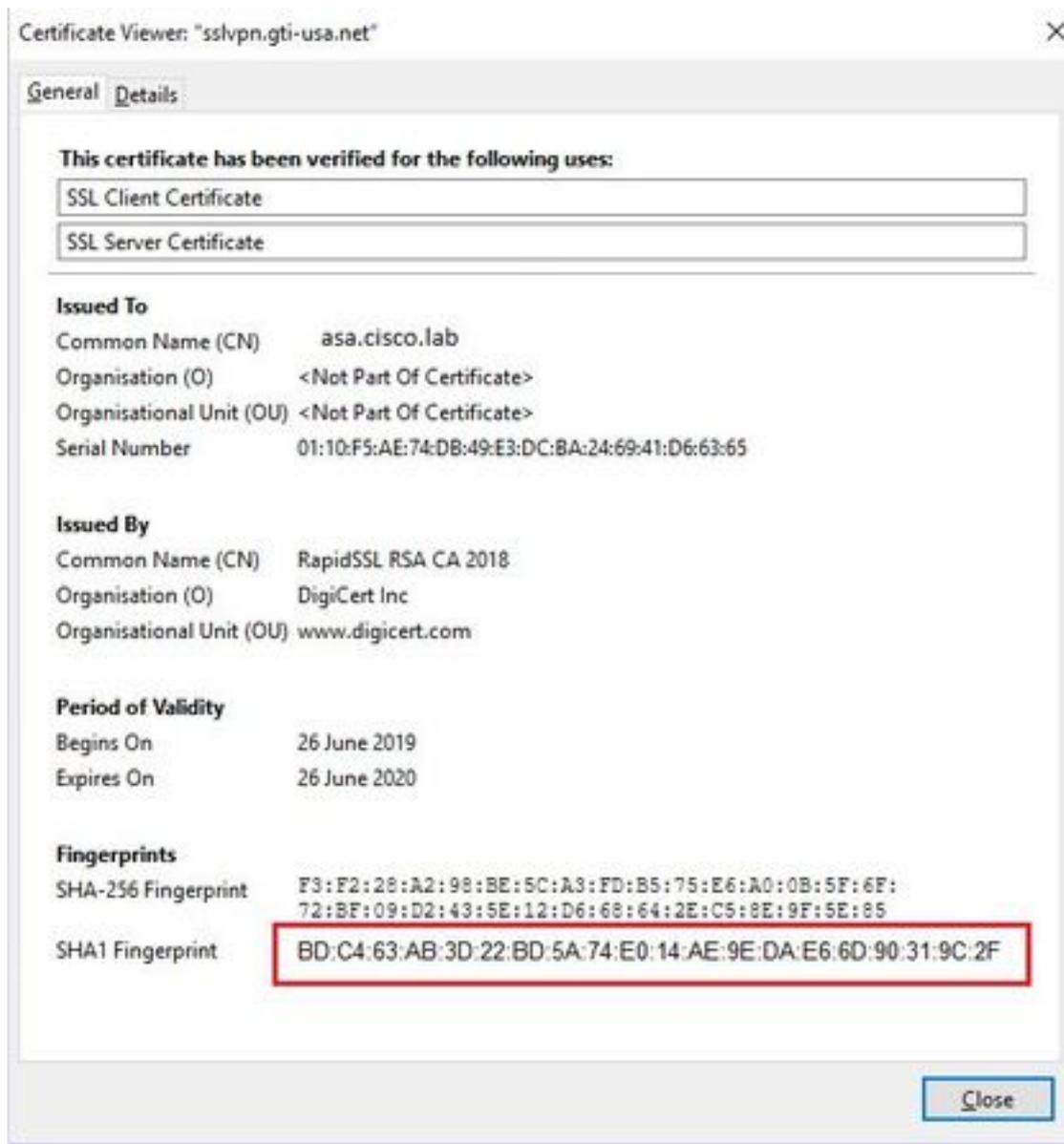
Etapa 6. Aplique o novo certificado na interface do ASA.

Depois que o certificado for aplicado na interface ASA, os telefones devem confiar nesse novo certificado, já que ambos têm hashes de certificado da etapa anterior.

Verificar

Use esta seção para confirmar que você seguiu as etapas corretamente.

Etapa 1. Abra os certificados ASA novos e antigos e anote a impressão digital SHA-1.



Etapa 2. Escolha um telefone que deve ser conectado via VPN e colete seu arquivo de configuração.

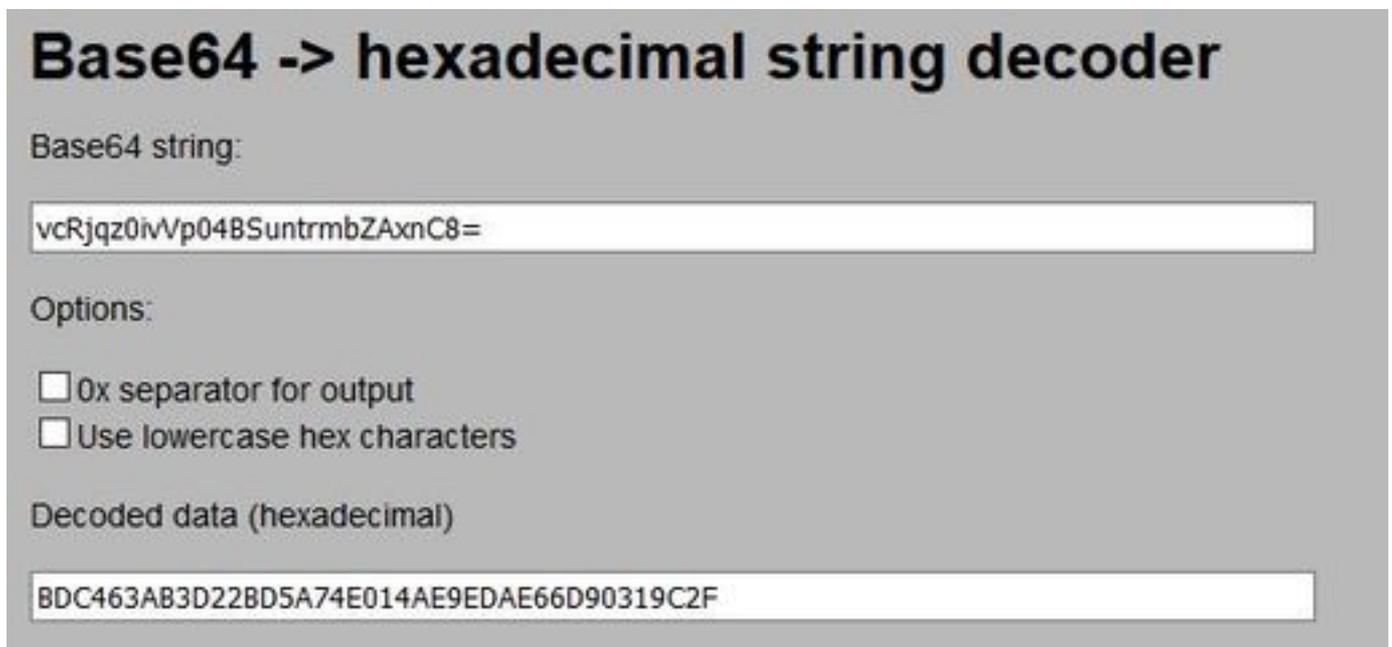
Note: Para obter mais informações sobre como coletar o arquivo de configuração do telefone, consulte [Duas Formas de Obter o Arquivo de Configuração de um Telefone do](#)

[CUCM](#)

Etapa 3. Depois de ter o arquivo de configuração, procure a seção:

```
<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>
```

Etapa 4. O hash no arquivo de configuração é impresso no formato Base 64 e no certificado ASA é impresso no formato hexadecimal, de modo que você pode usar um decodificador de Base 64 para Hexadecimal para verificar se ambos hash (telefone e ASA) correspondem.



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. At the bottom, there is a text output field displaying the decoded hexadecimal string "BDC463AB3D22BD5A74E014AE9EDAE66D90319C2F".

Informações Relacionadas

Para obter mais informações sobre o recurso Telefone VPN do AnyConnect:

- **Configure o telefone VPN do AnyConnect com autenticação de certificado em um ASA.**

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