Certificado da atualização ASA em CUCM para o telefone VPN com característica de AnyConnect

Índice

Introdução

Este original descreve o processo correto para atualizar o certificado adaptável da ferramenta de segurança (ASA) no gerente das comunicações unificadas de Cisco (CUCM) para telefones sobre o Virtual Private Network (VPN) com característica de AnyConnect para evitar a interrupção do serviço de telefone.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Telefone VPN com característica de AnyConnect.
- Certificados ASA e CUCM.

Componentes Utilizados

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

- Gerente 10.5.2.15900-8 das comunicações unificadas de Cisco.
- Versão de software adaptável 9.8(2)20 da ferramenta de segurança de Cisco.
- Cisco IP Phone CP-8841.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

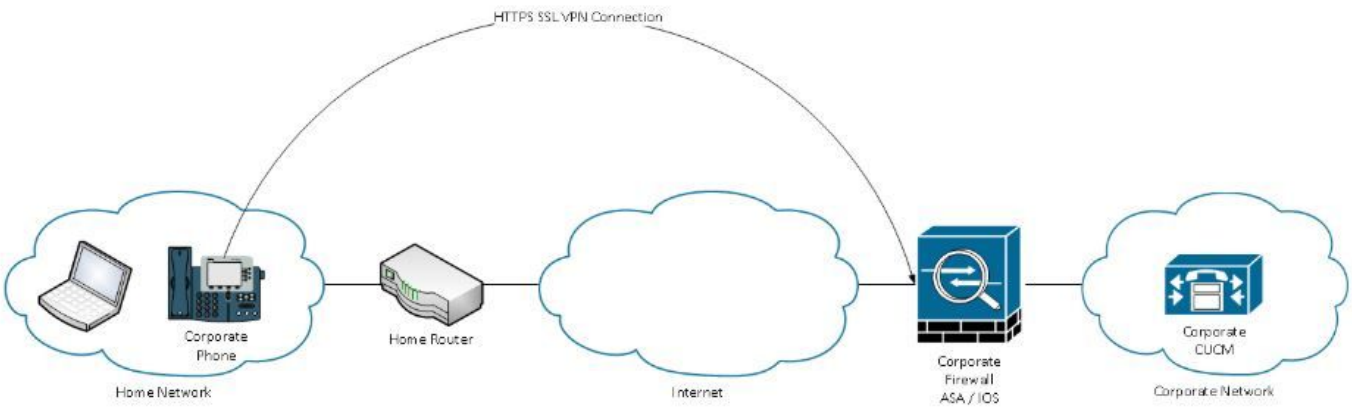
A característica do telefone VPN com AnyConnect permite a disposição de serviço de telefone sobre a conexão de VPN.

Antes que o telefone esteja pronto para o VPN, deve primeiramente ser provisioned na rede interna. Isto exige de acesso direto ao server do TFTP (protocolo de transferência de arquivo trivial) CUCM.

A primeira etapa depois que o ASA é configurado inteiramente, é tomar ao protocolo de transferência de hipertexto ASA o certificado (HTTPS) seguro e transferi-lo arquivos pela rede ao server CUCM como a Telefone-VPN-confiança, e atribui-a ao gateway de VPN correto em CUCM. Isto permite que o server CUCM construa um arquivo da configuração do telefone IP que diga ao telefone como obter ao ASA.

O telefone tem que ser provisioned dentro da rede antes que possa ser movido fora da rede e usar a característica VPN. Depois que o telefone provisioned internamente, pode ser movido para a rede externa para o acesso VPN.

O telefone conecta na porta TCP 443 HTTPS excedente ao ASA. O ASA responde para trás com o certificado configurado, e verifica o certificado apresentado.



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

Em algum momento, o certificado ASA precisa de ser mudança, devido a todas as circunstâncias por exemplo.

O certificado está a ponto de expirar

O certificado é 3ª parte assinada e a mudança do Certificate Authority (CA), etc.

Há algumas etapas a seguir a fim evitar a interrupção do serviço para os telefones que são conectados a CUCM através do VPN com o AnyConnect.

Cuidado: Se as etapas não são seguidas, os telefones precisam de ser provisioned outra

vez na rede interna antes que possam ser distribuídos em uma rede externa.

Etapa 1. Gerencia o certificado novo ASA mas não o aplique ainda à relação.

O certificado podia auto-ser assinado ou CA ser assinado.

> Nota: Para obter mais informações sobre do ASA os Certificados referem configurar Certificados digitais

Etapa 2. Transfira arquivos pela rede esse certificado em CUCM como a confiança do telefone VPN no editor CUCM.

Entre ao gerente de atendimento e navegue o **> segurança da administração ósmio > o certificado unificados do gerenciamento certificado > da transferência de arquivo pela rede > Telefone-VPN-confiança seleta.**

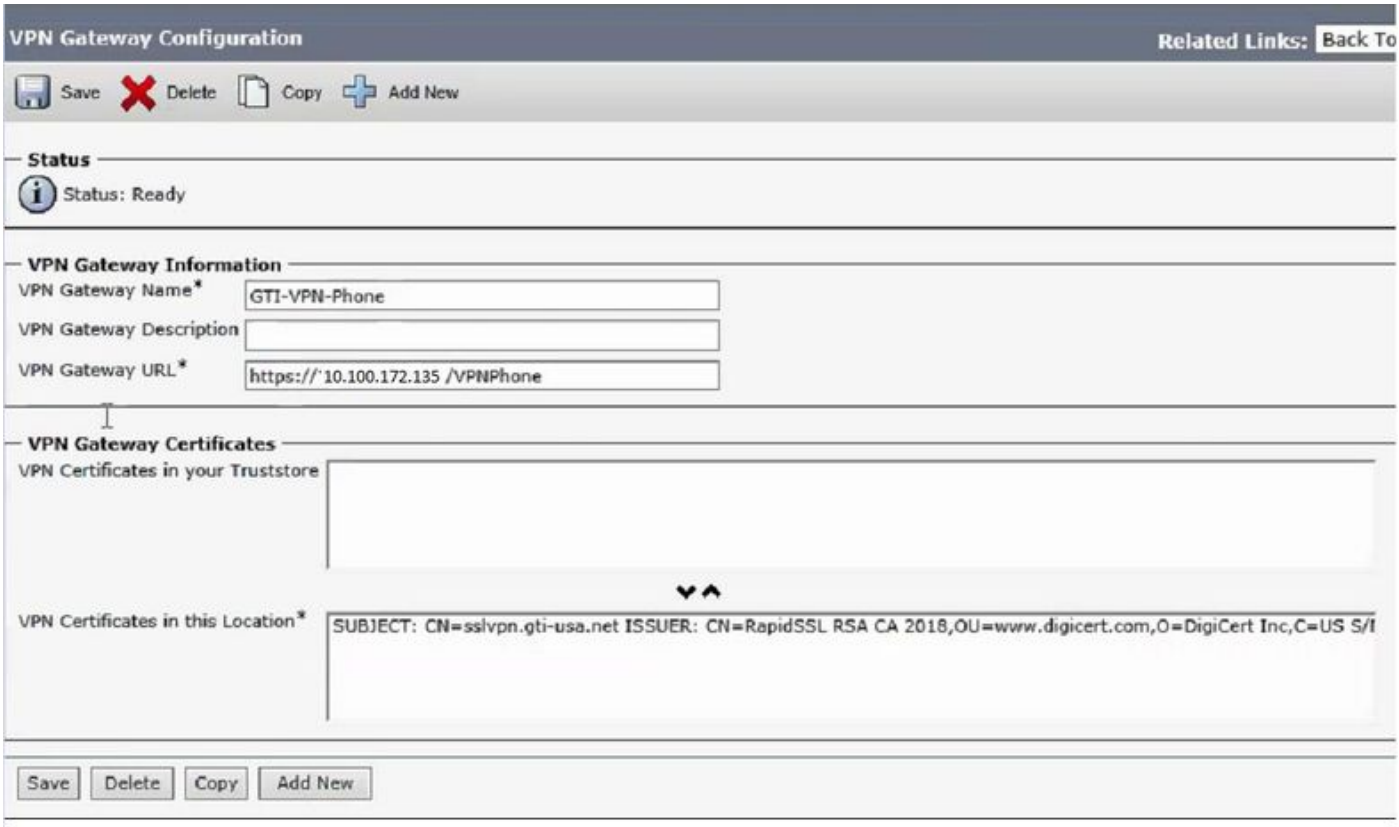
Como uma recomendação, transfira arquivos pela rede o certificate chain do complte, se os Certificados da raiz e do intermediário são transferidos arquivos pela rede já em CUCM, passam à próxima etapa.

> Cuidado: Mantenha por favor na mente se o certificado de identidade velho e o novo têm a mesma NC (Common Name) que você precisa de seguir a ação alternativa para o erro CSCuh19734 a fim evitar o certificado novo overwrites mais velho. Nessa maneira, o certificado novo está no base de dados para a configuração de gateway de VPN do telefone mas velha não overwritten.

Etapa 3. No gateway de VPN, selecione ambos os Certificados (o velho e o novo).

Navegue a **Cisco unificou características >Advanced a administração CM > VPN > gateway de VPN.**

Assegure-se de que você tenha ambos os Certificados nos Certificados VPN neste campo do lugar.



Etapa 4. Certifique-se do grupo de VPN, o perfil e o perfil comum do telefone estejam ajustados corretamente.

Etapa 5. Restaure os telefones.

Esta etapa permite que os telefones transfiram os ajustes de configuração novos e assegura-se dos telefones tenham ambos os Certificados piquem, assim que podem confiar no certificado velho e novo.

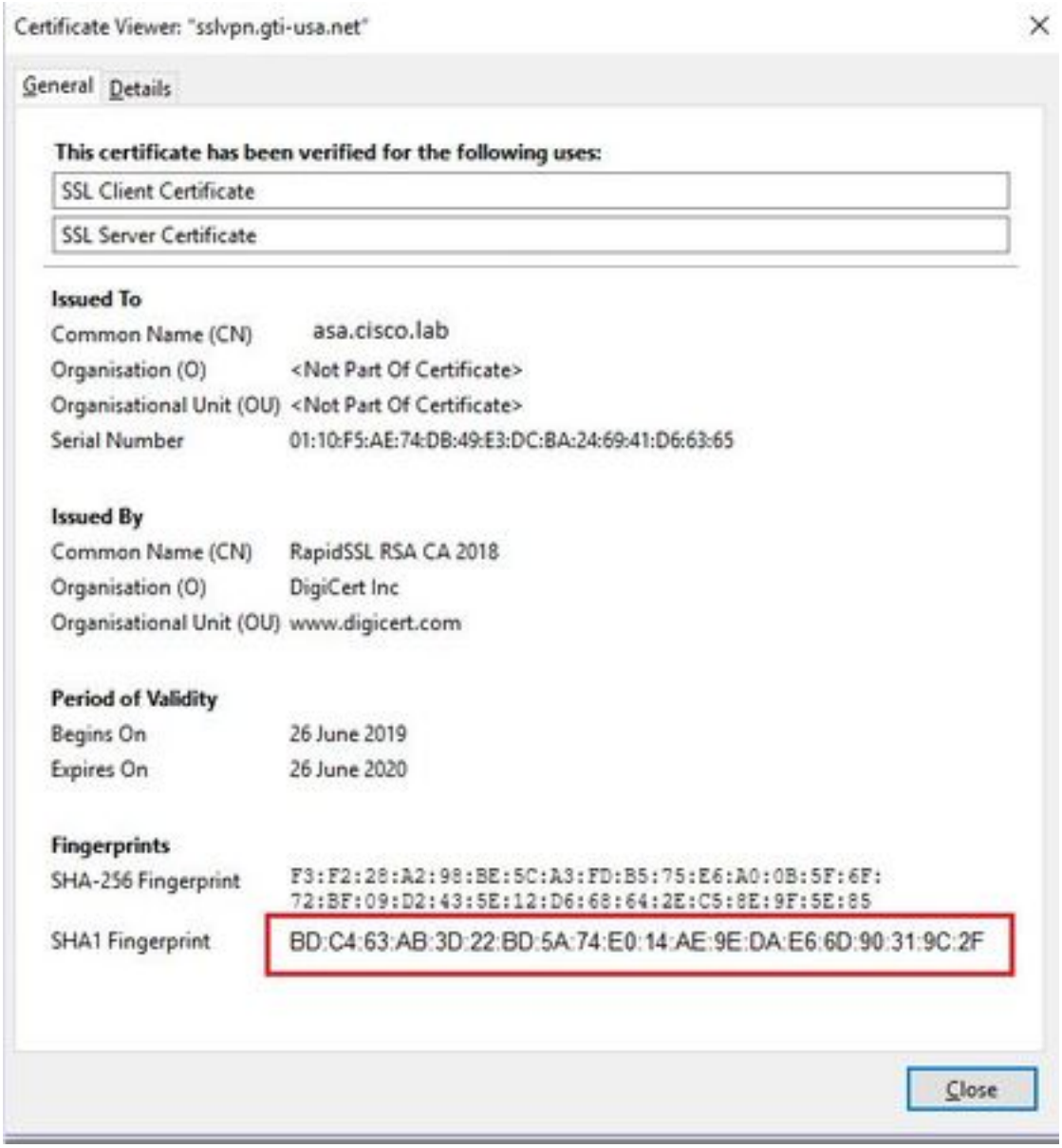
Etapa 6. Aplique o certificado novo na relação ASA.

Uma vez que o certificado é aplicado na relação ASA, os telefones devem confiar nesse certificado novo desde que têm ambos certificado picam da etapa precedente.

Verificar

Use esta seção a fim confirmar que você seguiu as etapas corretamente.

Etapa 1. Abra os Certificados velhos e novos ASA e note-os abaixo da impressão digital SHA-1.



Etapa 2. Escolha um telefone que deva ser conectado através do VPN e recolha seu arquivo de configuração.

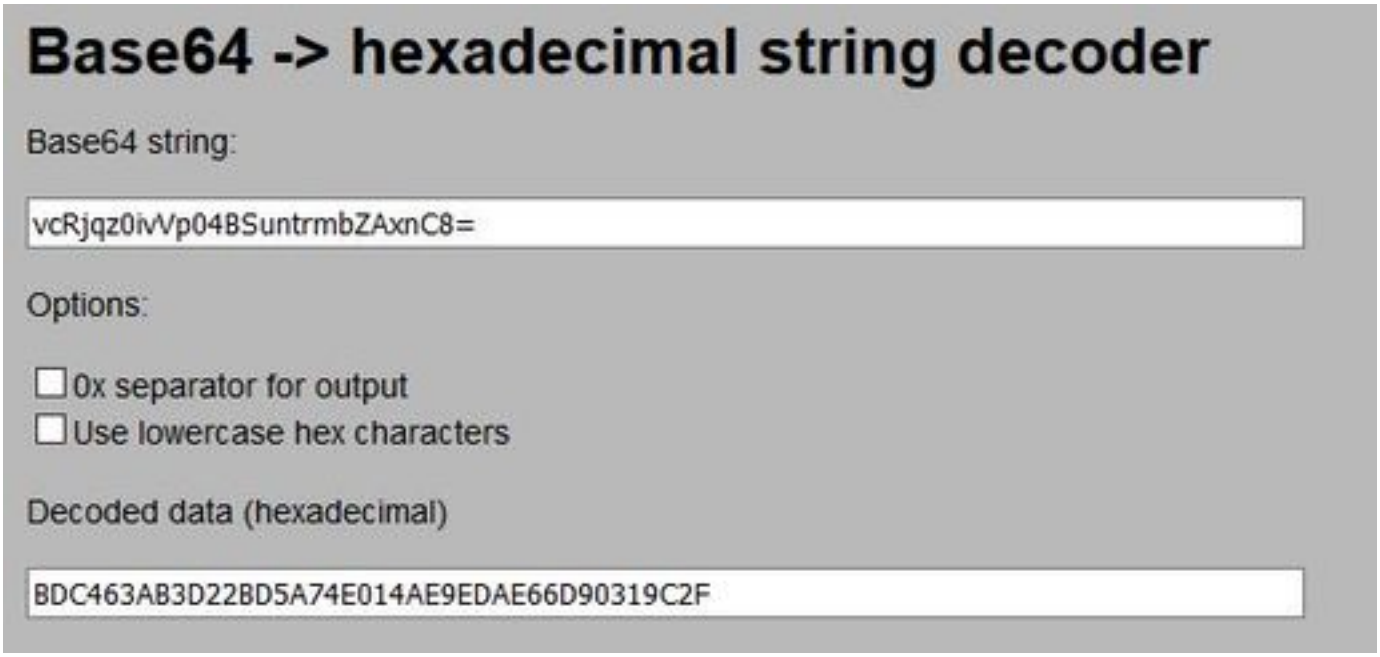
> Nota: Para obter mais informações sobre de como recolher o arquivo de configuração telefônica refira duas maneiras de obter o arquivo de configuração de um telefone de CUCM

Etapa 3. Uma vez que você tem 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>
<certHash1>vcRjqz0ivVp04BSuntrmbZAxnC8=</certHash1>
```

```
<certHash2>SEnDU8oo49agcRObtMBACXdaiTI=</certHash2>
</credentials>
</vpnGroup>
```

Etapa 4. A mistura no arquivo de configuração é imprimida no formato da base 64 e no ASA o certificado é imprimido no formato hexadecimal, assim que você pode usar um decodificador da base 64 ao hexadecimal para verificar que ambos picaram (telefone e ASA) o fósforo.



Informações Relacionadas

Para obter mais informações sobre dos recursos de telefone de AnyConnect VPN:

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

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