Conexão telefônica de AnyConnect VPN a um exemplo da configuração de roteador do Cisco IOS

Índice

Introdução

Este documento descreve como configurar os dispositivos do roteador e do gerenciador de chamada do ® do Cisco IOS de modo que os Telefones IP de Cisco possam estabelecer conexões de VPN ao roteador do Cisco IOS. Estas conexões de VPN são precisadas a fim fixar a comunicação com o qualquer um destes dois métodos de authenticação do cliente:

- Server ou base de dados local do Authentication, Authorization, and Accounting (AAA)
- Certificado do telefone

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

- Cisco IOS 15.1(2)T ou mais tarde
- Conjunto de recursos/licença: Universal (dados & Segurança & UC) para o roteador do serviço integrado do Cisco IOS (ISR)-G2
- Conjunto de recursos/licença: Segurança avançada para o Cisco IOS ISR
- Liberação 8.0.1.100000-4 do gerente das comunicações unificadas de Cisco (CUCM) ou mais atrasado
- Liberação 9.0(2)SR1S do telefone IP - Skinny Call Control Protocol (SCCP) ou mais tarde

Para uma lista completa de telefones apoiados em sua versão CUCM, termine estas etapas:

1. Abra esta URL: ***IP de servidor Address>:8443/cucreports/systemReports.do de*** **https://** ***<CUCM***
2. Escolha a **lista unificada dos recursos de telefone CM > gerenciem um relatório > uma característica novos: Virtual Private Network**.

As liberações usadas neste exemplo de configuração incluem:

- Liberação 15.1(4)M4 do roteador do Cisco IOS
- Liberação 8.5.1.10000-26 do gerenciador de chamada
- Liberação 9.1(1)SR1S do telefone IP

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 sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

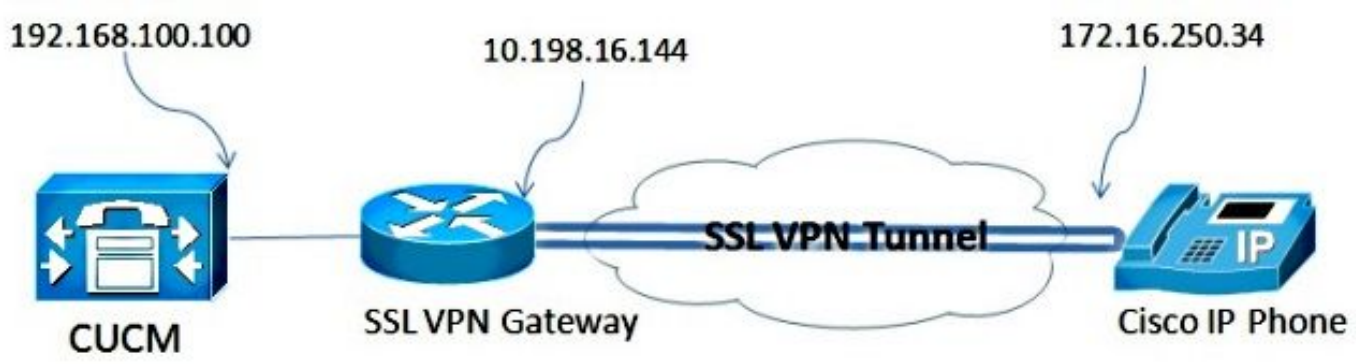
Configurar

Esta seção cobre a informação necessária a fim configurar as características descritas neste documento.

> Nota: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Topologia de rede

A topologia usada neste documento inclui um Cisco IP Phone, o roteador do Cisco IOS como o gateway de VPN do secure sockets layer (SSL), e CUCM como o gateway de voz.



Configuração de servidor de VPN SSL

Esta seção descreve como configurar a extremidade principal do Cisco IOS a fim permitir conexões de VPN de entrada SSL.

Etapas da configuração comum

1. Gerencia a chave de Rivest-Shamir-Adleman (RSA) com um comprimento de 1024 bytes:

   ```
   Router(config)#crypto key generate rsa general-keys label SSL modulus 1024
   ```
2. Crie o ponto confiável para o certificado auto-assinado, e anexe a chave SSL RSA:

   ```
   Router(config)#crypto pki trustpoint server-certificate
   enrollment selfsigned
   usage ssl-server
   serial-number
   subject-name CN=10.198.16.144
   revocation-check none
   rsakeypair SSL
   ```
3. Uma vez que o ponto confiável é configurado, registre o certificado auto-assinado com este comando:

   ```
   Router(config)#crypto pki enroll server-certificate
   % Include an IP address in the subject name? [no]: no
   Generate Self Signed Router Certificate? [yes/no]: yes

   Router Self Signed Certificate successfully created
   ```
4. Permita o pacote correto de AnyConnect na extremidade principal. O telefone próprio não transfere este pacote. Mas, sem o pacote, o túnel VPN não estabelece. Recomenda-se usar a versão de software do cliente a mais atrasada disponível no cisco.com. Este exemplo usa a versão 3.1.3103.

   Em umas versões do Cisco IOS mais velhas, este é o comando a fim permitir o pacote:
   ```
   Router(config)#webvpn install svc flash:anyconnect-win-3.1.03103-k9.pkg
   ```
   Contudo, na versão do Cisco IOS a mais atrasada, este é o comando:
   ```
   Router(config)#crypto vpn anyconnect flash:/webvpn/anyconnect-win-
   3.1.03103-k9.pkg sequence 1
   ```
5. Configurar o gateway de VPN. O gateway WebVPN é usado a fim terminar a conexão SSL do usuário.
   ```
   Router(config)#crypto vpn anyconnect flash:/webvpn/anyconnect-win-
   3.1.03103-k9.pkg sequence 1
   ```
   Nota: Um ou outro o endereço IP de Um ou Mais Servidores Cisco ICM NT usado aqui

precisa de estar na mesma sub-rede como a relação a que os telefones conectam, ou o gateway precisa de ser originado diretamente de uma relação no roteador. O gateway é usado igualmente a fim definir que certificado é usado pelo roteador a fim validar próprio ao cliente.

6. Defina o conjunto local que está usado a fim atribuir endereços IP de Um ou Mais Servidores Cisco ICM NT aos clientes quando conectam:
   ```
   Router(config)#crypto vpn anyconnect flash:/webvpn/anyconnect-win-
   3.1.03103-k9.pkg sequence 1
   ```

Configuração com autenticação de AAA

Esta seção descreve os comandos que você precisa a fim configurar o servidor AAA ou o base de dados local a fim autenticar seus telefones. Se você planeia usar a autenticação do certificado-somente para os telefones, continue à próxima seção.

Configurar a base de dados de usuário

O base de dados local do roteador ou um servidor AAA externo podem ser usados para a autenticação:

- A fim configurar o base de dados local, entre:
  ```
  Router(config)#crypto vpn anyconnect flash:/webvpn/anyconnect-win-
  3.1.03103-k9.pkg sequence 1
  ```
- A fim configurar um servidor para autenticação remoto dos RADIUS AAA, entre:
  ```
  Router(config)#crypto vpn anyconnect flash:/webvpn/anyconnect-win-
  3.1.03103-k9.pkg sequence 1
  ```

Configurar o contexto virtual e a Grupo-política

O contexto virtual é usado a fim definir os atributos que governam a conexão de VPN, como:

- Que URL a se usar quando você conectar
- Que pool a se usar a fim atribuir os endereços de cliente
- Que método de autenticação a se usar

Estes comandos são um exemplo de um contexto que use a autenticação de AAA para o cliente:

```
Router(config)#crypto vpn anyconnect flash:/webvpn/anyconnect-win-
3.1.03103-k9.pkg sequence 1
```

Configuração com do telefone IP o certificado significativo localmente - (LSC) para a authenticação do cliente

Esta seção descreve os comandos que você precisa a fim configurar a authenticação do cliente certificado-baseada para os telefones. Contudo, a fim fazer isto, o conhecimento dos vários tipos de Certificados do telefone é exigido:

- **Certificado instalado fabricante (MIC) -** Os MIC são incluídos em todos os 7941, 7961, e Telefones IP de Cisco do novo-modelo. Os MIC são os Certificados 2,048-bit chaves que são assinados pelo Certificate Authority (CA) de Cisco. Para que o CUCM confie o certificado MIC, usa os certificados de CA instalados CAP-RTP-001, CAP-RTP-002, e Cisco_Manufacturing_CA em sua loja da confiança do certificado. Porque este certificado é fornecido pelo fabricante próprio, como indicado no nome, não se recomenda usar este certificado para a authenticação do cliente.

- **LSC -** O LSC fixa a conexão entre CUCM e o telefone depois que você configura o modo da segurança do dispositivo para a autenticação ou a criptografia. O LSC possui a chave pública para o Cisco IP Phone, que é assinada pela chave privada da função do proxy do Certificate Authority CUCM (CAPF). Este é o método mais seguro (ao contrário do uso dos MIC). Cuidado: Devido ao risco de segurança aumentada, Cisco recomenda o uso dos MIC unicamente para a instalação LSC e não para o uso continuado. Os clientes que configuram Telefones IP de Cisco a fim usar MIC para a autenticação do Transport Layer Security (TLS), ou para toda a outra finalidade, fazem tão por sua conta e risco.

Neste exemplo de configuração, o LSC é usado a fim autenticar os telefones.

> Dica: A maneira a mais segura de conectar seu telefone é usar a autenticação dupla, que combina o certificado e a autenticação de AAA. Você pode configurar este se você combina os comandos usados para cada um sob um contexto virtual.

Configurar o ponto confiável a fim validar o certificado de cliente

O roteador deve ter o certificado CAPF instalado a fim validar o LSC do telefone IP. A fim obter esse certificado e instalá-lo no roteador, termine estas etapas:

1. Vá à página da web de administração do operating system (OS) CUCM.
2. Escolha o **> gerenciamento de certificado da Segurança**.
   Nota: Este lugar pôde mudar baseado na versão CUCM.
3. Encontre o certificado etiquetado **CAPF**, e transfira o arquivo do **.pem**. Salvar o como um arquivo de **.txt**
4. Uma vez que o certifcate é extraído, crie um ponto confiável novo no roteador, e autentique o ponto confiável com CAPF, como mostrado aqui. Quando alertado para o base-64 codificou o certificado de CA, selecionam e colam o texto no arquivo transferido do .pem junto com o COMEÇO e as linhas final.

```
Router(config)#crypto pki trustpoint CAPF
enrollment terminal
authorization username subjectname commonname
revocation-check none
Router(config)#crypto pki authenticate CAPF
Router(config)#

<base-64 encoded CA certificate>

quit
```

Coisas a notar:

- O método do registro é terminal porque o certificado tem que manualmente ser instalado no roteador.
- **O comando username da autorização** está exigido a fim dizer ao roteador o que usar-se como o username quando o cliente faz a conexão. Neste caso, usa o Common Name (CN).
- Uma verificação da revogação precisa de ser desabilitada porque os Certificados do telefone não têm um Certificate Revocation List (CRL) definido. Assim, a menos que for desabilitada, a conexão falha e o Public Key Infrastructure (PKI) debuga a mostra esta saída:

```
Jun 17 21:49:46.695: CRYPTO_PKI: (A0076) Starting CRL revocation check
Jun 17 21:49:46.695: CRYPTO_PKI: Matching CRL not found
Jun 17 21:49:46.695: CRYPTO_PKI: (A0076) CDP does not exist. Use SCEP to
query CRL.
Jun 17 21:49:46.695: CRYPTO_PKI: pki request queued properly
```

```
Jun 17 21:49:46.695: CRYPTO_PKI: Revocation check is complete, 0
Jun 17 21:49:46.695: CRYPTO_PKI: Revocation status = 3
Jun 17 21:49:46.695: CRYPTO_PKI: status = 0: poll CRL
Jun 17 21:49:46.695: CRYPTO_PKI: Remove session revocation service providers
CRYPTO_PKI: Bypassing SCEP capabilies request 0
Jun 17 21:49:46.695: CRYPTO_PKI: status = 0: failed to create GetCRL
Jun 17 21:49:46.695: CRYPTO_PKI: enrollment url not configured
Jun 17 21:49:46.695: CRYPTO_PKI: transaction GetCRL completed
Jun 17 21:49:46.695: CRYPTO_PKI: status = 106: Blocking chain verification
callback received status
Jun 17 21:49:46.695: CRYPTO_PKI: (A0076) Certificate validation failed
```

Configurar o contexto virtual e a Grupo-política

Isto parte da configuração é similar à configuração usada previamente, à exceção de dois pontos:

- O método de autenticação
- O ponto confiável os usos do contexto a fim autenticar os telefones

Os comandos são mostrados aqui:

```
Jun 17 21:49:46.695: CRYPTO_PKI: (A0076) Starting CRL revocation check
Jun 17 21:49:46.695: CRYPTO_PKI: Matching CRL not found
Jun 17 21:49:46.695: CRYPTO_PKI: (A0076) CDP does not exist. Use SCEP to
query CRL.
Jun 17 21:49:46.695: CRYPTO_PKI: pki request queued properly
Jun 17 21:49:46.695: CRYPTO_PKI: Revocation check is complete, 0
Jun 17 21:49:46.695: CRYPTO_PKI: Revocation status = 3
Jun 17 21:49:46.695: CRYPTO_PKI: status = 0: poll CRL
Jun 17 21:49:46.695: CRYPTO_PKI: Remove session revocation service providers
CRYPTO_PKI: Bypassing SCEP capabilies request 0
Jun 17 21:49:46.695: CRYPTO_PKI: status = 0: failed to create GetCRL
Jun 17 21:49:46.695: CRYPTO_PKI: enrollment url not configured
Jun 17 21:49:46.695: CRYPTO_PKI: transaction GetCRL completed
Jun 17 21:49:46.695: CRYPTO_PKI: status = 106: Blocking chain verification
callback received status
Jun 17 21:49:46.695: CRYPTO_PKI: (A0076) Certificate validation failed
```

Configuração do gerenciador de chamada

Esta seção descreve as etapas de configuração do gerenciador de chamada.

Exporte Auto-assinada ou o certificado de identidade do roteador para o CUCM

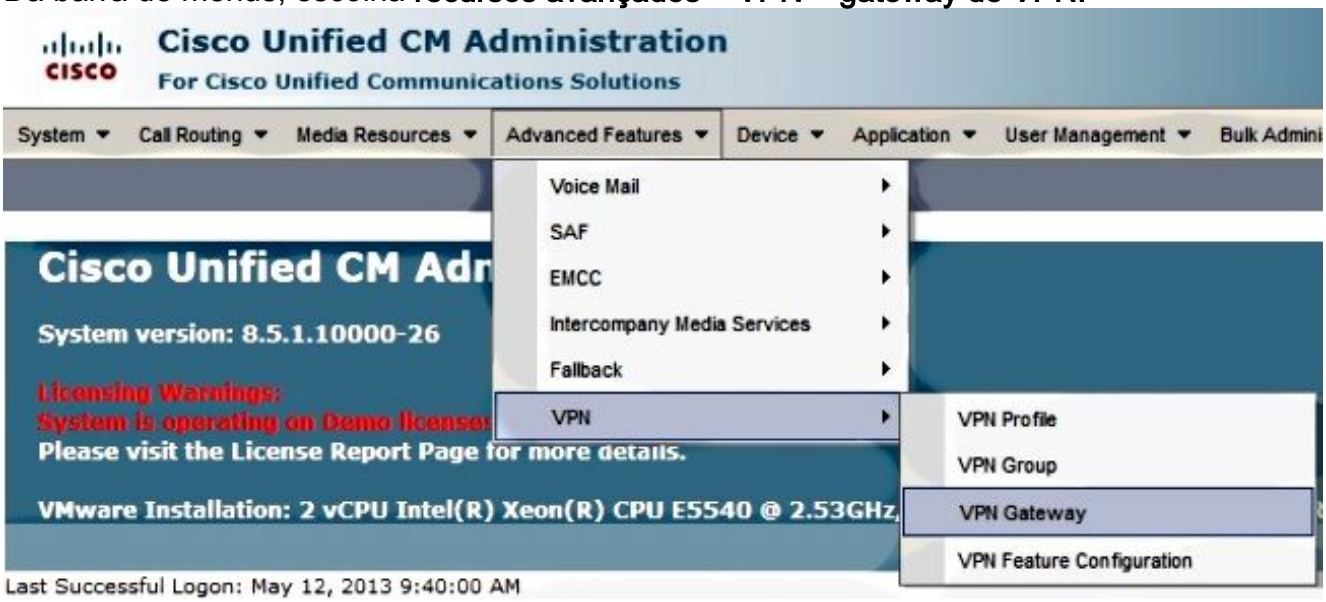
A fim exportar o certificado do roteador e importar o certificado no gerenciador de chamada como um certificado da Telefone-VPN-confiança, termine estas etapas:

1. Verifique o certificado usado para o SSL.
   ```
   Router#show webvpn gateway SSL
   SSL Trustpoint: server-certificate
   ```
2. Exporte o certificado.
   ```
   Router(config)#crypto pki export server-certificate pem terminal
   The Privacy Enhanced Mail (PEM) encoded identity certificate follows:
   -----BEGIN CERTIFICATE-----

   <output removed>

   -----END CERTIFICATE-----
   ```
3. Copie o texto do terminal e salvar o como um arquivo do **.pem**.
4. Entre ao gerenciador de chamada, e escolha o **> gerenciamento de certificado do >**

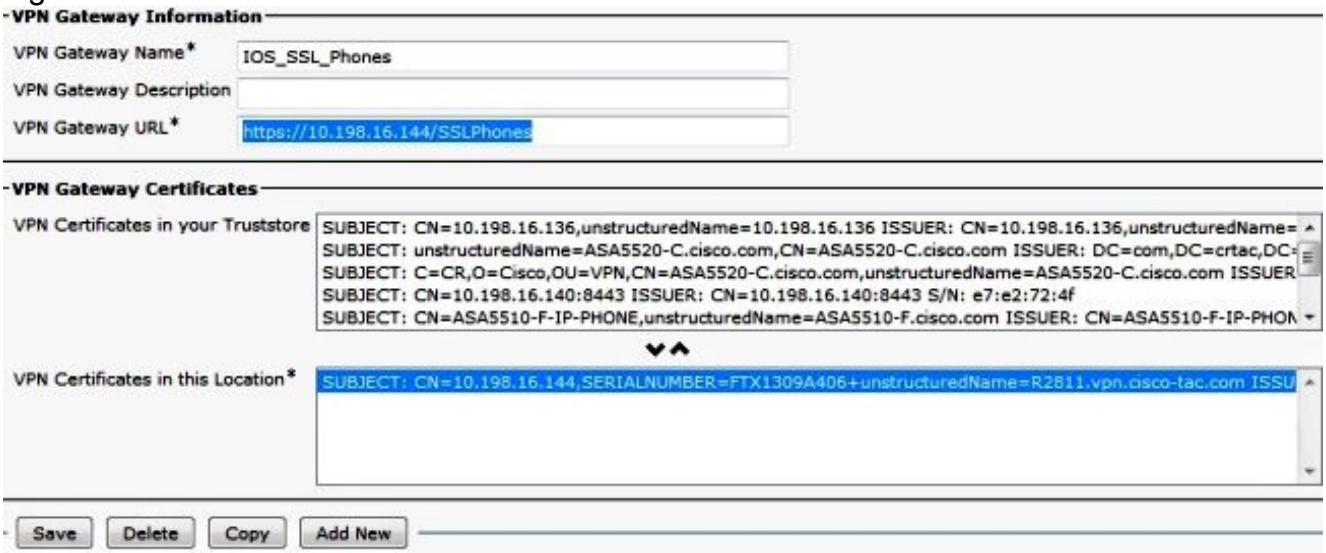
segurança da administração do OS > o certificado unificados da transferência de arquivo pela rede > Telefone-VPN-confiança seleta a fim transferir arquivos pela rede o arquivo certificado salvar na etapa precedente.

Configurar o gateway de VPN, o grupo, e o perfil no CUCM

1. Navegue a **Cisco unificou a administração CM**.
2. Da barra de menus, escolha **recursos avançados > VPN > gateway de VPN.**

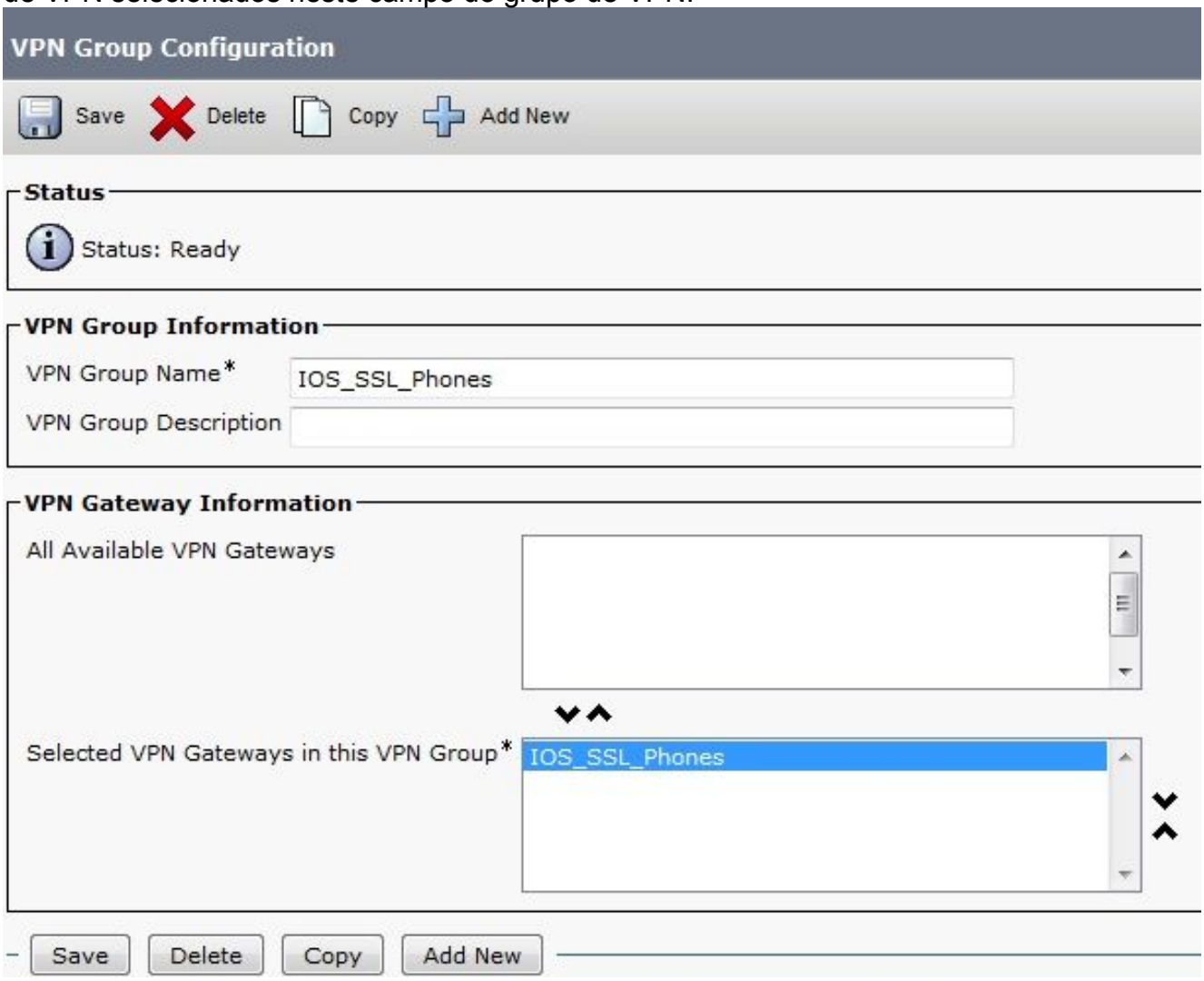


3. Na janela de configuração do gateway de VPN, termine estas etapas:
   No campo de nome do gateway de VPN, dê entrada com um nome. Este pode ser todo o nome.No campo de descrição do gateway de VPN, incorpore uma descrição (opcional).No campo URL do gateway de VPN, incorpore a grupo-URL definido no roteador.Nos Certificados VPN neste campo do lugar, escolha o certificado que foi transferido arquivos pela rede ao gerenciador de chamada previamente a fim o mover da loja da confiança para este
   lugar.

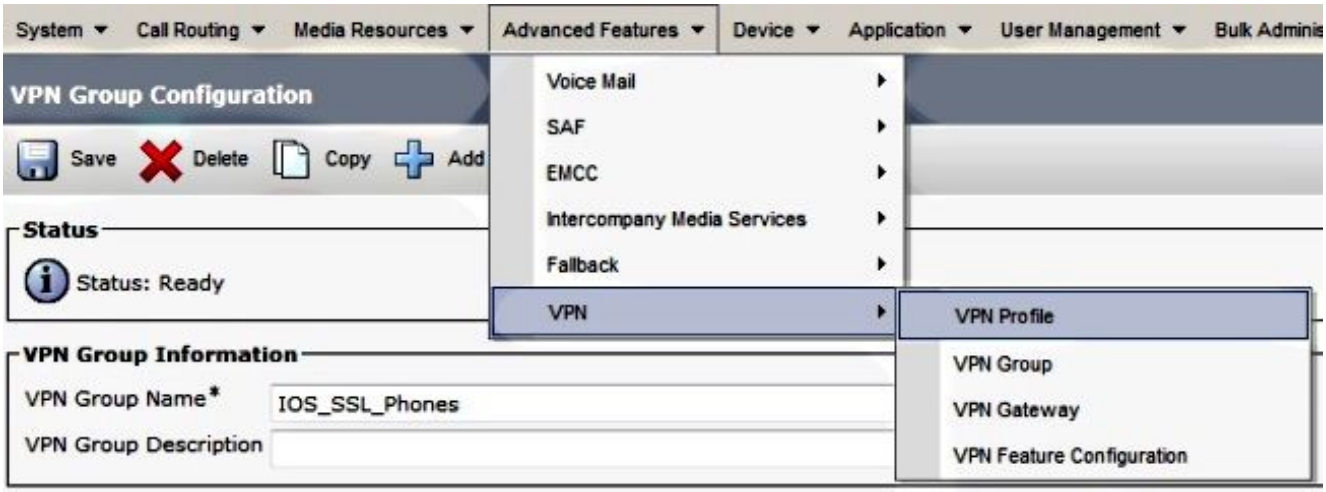


4. Da barra de menus, escolha **recursos avançados > VPN > grupo de VPN.**

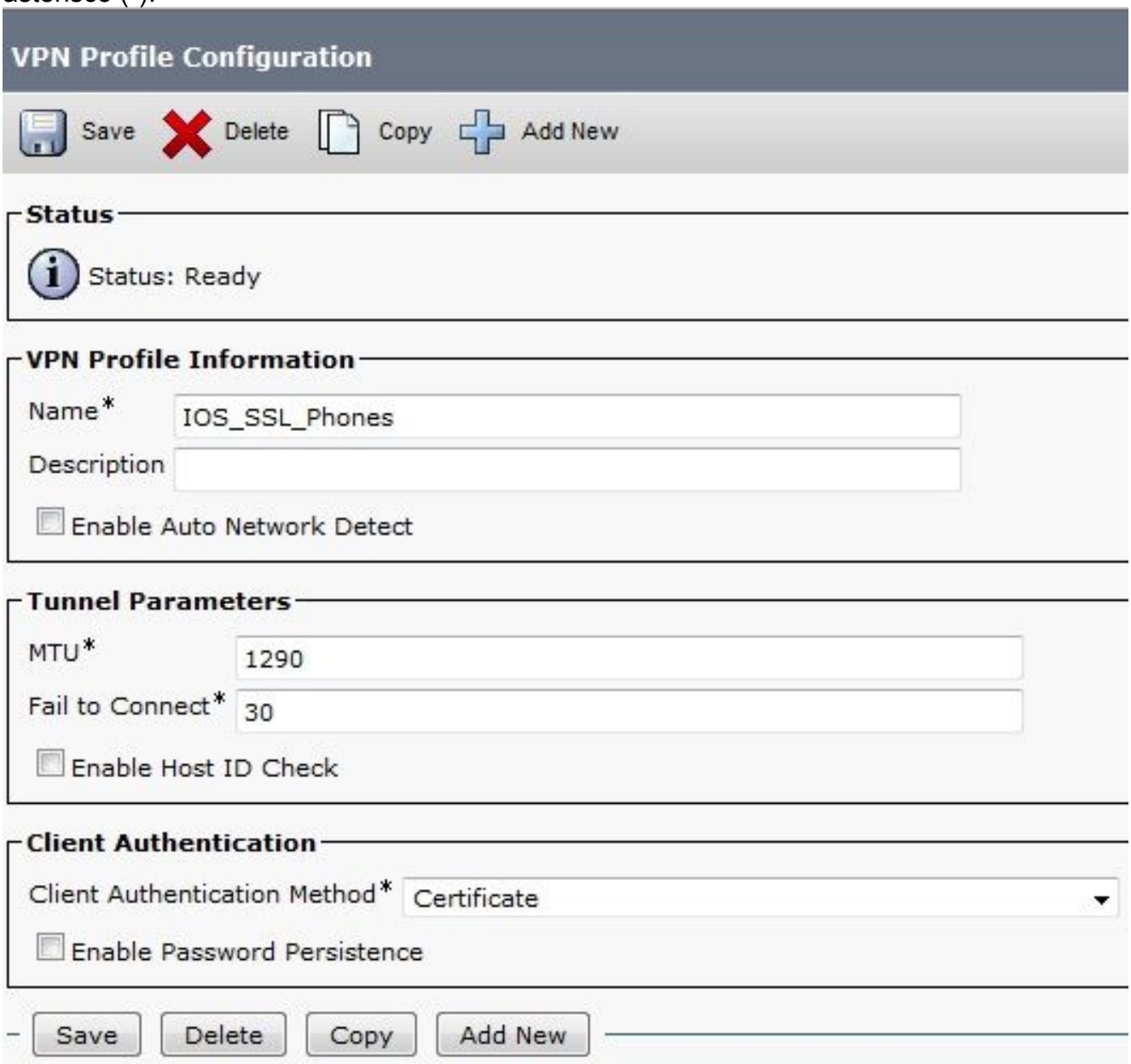
5. Em todos os gateways de VPN disponíveis coloque, escolha o **gateway de VPN** definido previamente. Clique a seta para baixo a fim mover o gateway selecionado para os gateways de VPN selecionados neste campo do grupo de VPN.



6. Da barra de menus, escolha **recursos avançados > perfil VPN > VPN.**



7. A fim configurar o perfil VPN, termine todos os campos que são identificados por meio de um asterisco (*).

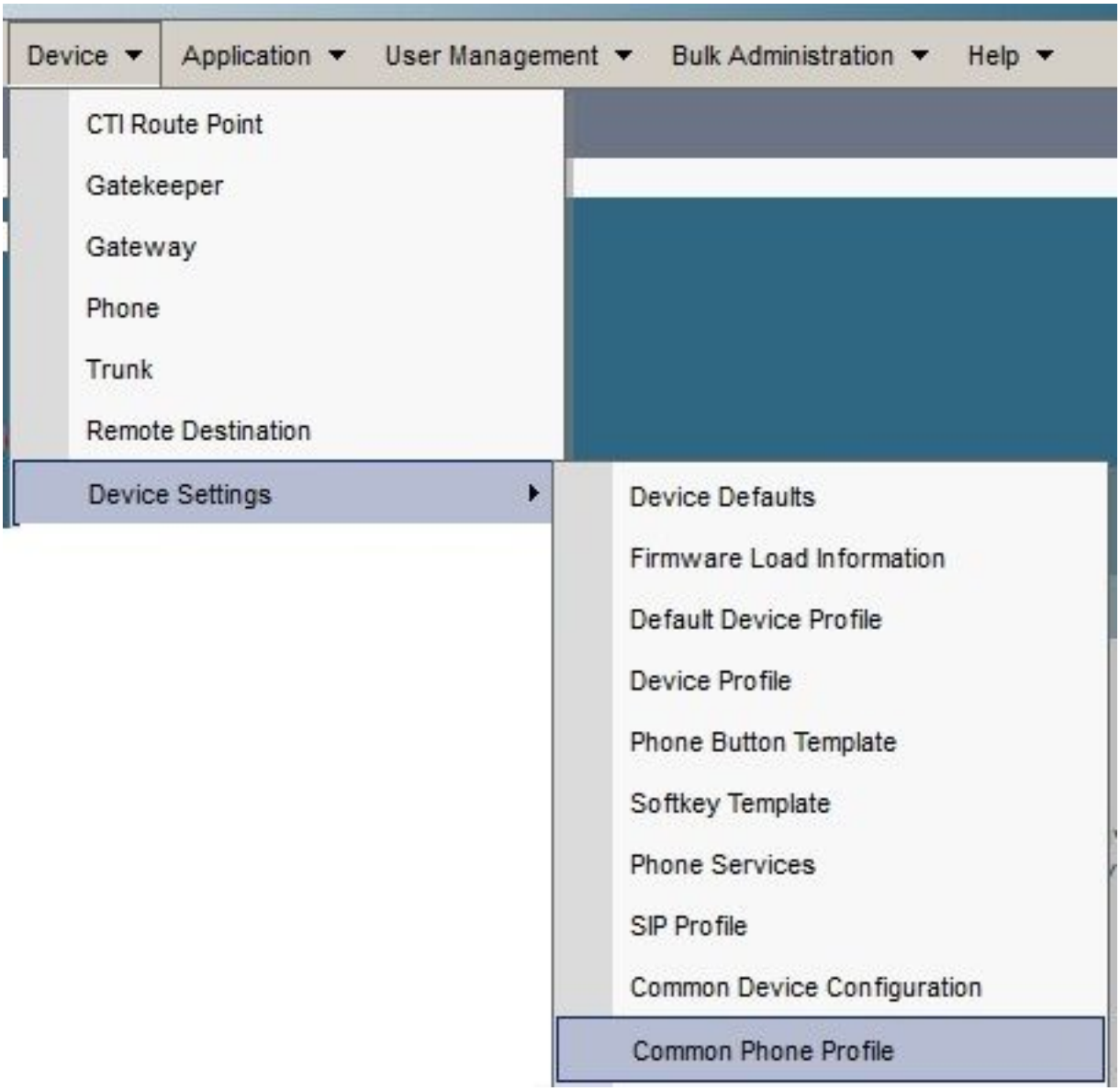


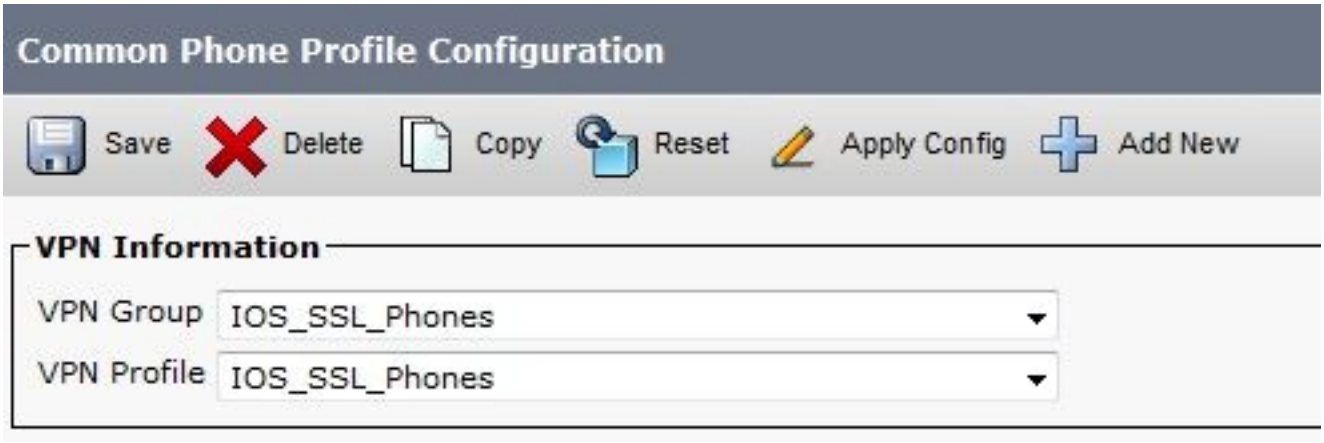
Permita a auto rede detectam: Se permitido, o telefone VPN sibila o servidor TFTP. Se nenhuma resposta é recebida, ele auto-novatos uma conexão de VPN.**Permita a verificação do ID do host:** Se permitido, o telefone VPN compara o nome de domínio totalmente qualificado (FQDN) do gateway de VPN URL contra a rede de área CN/Storage (SAN) do certificado. O cliente não conecta se estes artigos não combinam ou se um certificado do

convite com um asterisco (*) está usado.**Permita a persistência da senha:** Isto permite que o telefone VPN ponha em esconderijo o nome de usuário e senha para a tentativa seguinte VPN.

Aplique o grupo e o perfil ao telefone IP com o perfil comum do telefone

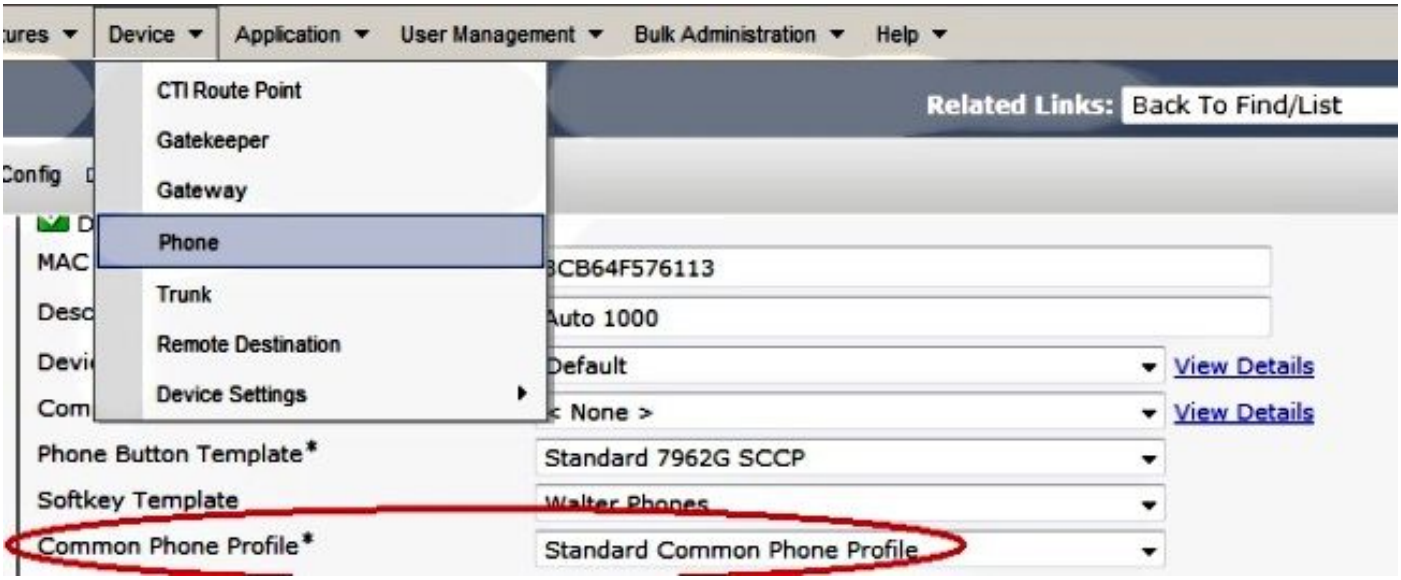
No indicador comum da configuração de perfil do telefone, o clique **aplica a configuração** a fim aplicar a configuração de VPN nova. Você pode usar o **perfil comum** padrão do **telefone** ou criar um perfil novo.





Aplique o perfil comum do telefone ao telefone IP

Se você criou um perfil novo para telefones/usuários específicos, navegue ao indicador da **configuração telefônica**. No campo comum do perfil do telefone, escolha o perfil **comum padrão do telefone**.



Instale localmente - os Certificados significativos (LSC) em Telefones IP de Cisco

O seguinte guia pode ser usado para instalar localmente - Certificados significativos em Telefones IP de Cisco. Esta etapa é precisada somente se a autenticação que usa o LSC é usada. A autenticação que usa o Manufacterer instalou o certificado (MIC) ou o nome de usuário e senha não exige um LSC ser instalado.

Instale um LSC em um telefone com o modo de segurança do conjunto CUCM ajustado NON-seguro.

Registrar o telefone ao gerenciador de chamada outra vez a fim transferir a configuração nova

Esta é a etapa final no processo de configuração.

Verificar

Verificação do roteador

A fim verificar as estatísticas da sessão de VPN no roteador, você pode usar estes comandos, e verifica as diferenças entre as saídas (destacadas) para ver se há o username e o certificado de autenticação:

Para o username/autenticação de senha:

```
Router#show webvpn session user phones context SSL
Session Type : Full Tunnel
Client User-Agent : Cisco SVC IPPhone Client v1.0 (1.0)

Username : phones               Num Connection : 1
Public IP : 172.16.250.34 VRF Name : None
Context : SSL Policy Group : SSLPhones
Last-Used : 00:00:29 Created : 15:40:21.503 GMT
Fri Mar 1 2013
Session Timeout : Disabled Idle Timeout : 2100
DPD GW Timeout : 300 DPD CL Timeout : 300
Address Pool : SSL MTU Size : 1290
Rekey Time : 3600 Rekey Method :
Lease Duration : 43200
Tunnel IP : 10.10.10.1 Netmask : 255.255.255.0
Rx IP Packets : 106 Tx IP Packets : 145
CSTP Started : 00:11:15 Last-Received : 00:00:29
CSTP DPD-Req sent : 0 Virtual Access : 1
Msie-ProxyServer : None Msie-PxyPolicy : Disabled
Msie-Exception :
Client Ports : 51534
DTLS Port : 52768
Router#

Router#show webvpn session context all
WebVPN context name: SSL
Client_Login_Name  Client_IP_Address  No_of_Connections  Created  Last_Used
phones             172.16.250.34              1         00:30:38  00:00:20
```

Para o certificado de autenticação:

```
Router#show webvpn session user SEP8CB64F578B2C context all
Session Type : Full Tunnel
Client User-Agent : Cisco SVC IPPhone Client v1.0 (1.0)

Username : SEP8CB64F578B2C      Num Connection : 1
Public IP : 172.16.250.34 VRF Name : None
CA Trustpoint  : CAPF
Context : SSL Policy Group :
Last-Used : 00:00:08 Created : 13:09:49.302 GMT
Sat Mar 2 2013
Session Timeout : Disabled Idle Timeout : 2100
DPD GW Timeout : 300 DPD CL Timeout : 300
Address Pool : SSL MTU Size : 1290
Rekey Time : 3600 Rekey Method :
Lease Duration : 43200
Tunnel IP : 10.10.10.2 Netmask : 255.255.255.0
Rx IP Packets : 152 Tx IP Packets : 156
CSTP Started : 00:06:44 Last-Received : 00:00:08
CSTP DPD-Req sent : 0 Virtual Access : 1
Msie-ProxyServer : None Msie-PxyPolicy : Disabled
Msie-Exception :
Client Ports : 50122
DTLS Port : 52932
```

```
Router#show webvpn session context all
WebVPN context name: SSL
Client_Login_Name  Client_IP_Address  No_of_Connections  Created  Last_Used
SEP8CB64F578B2C    172.16.250.34              1         3d04h     00:00:16
```

Verificação CUCM

Confirme que o telefone IP está registrado com o gerenciador de chamada com o endereço atribuído o roteador fornecido à conexão SSL.

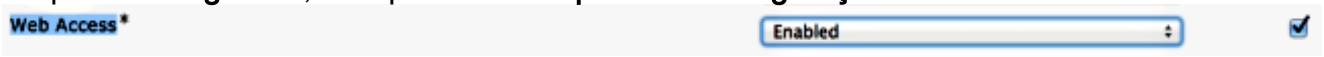
Troubleshooting

Debuga no servidor de VPN SSL

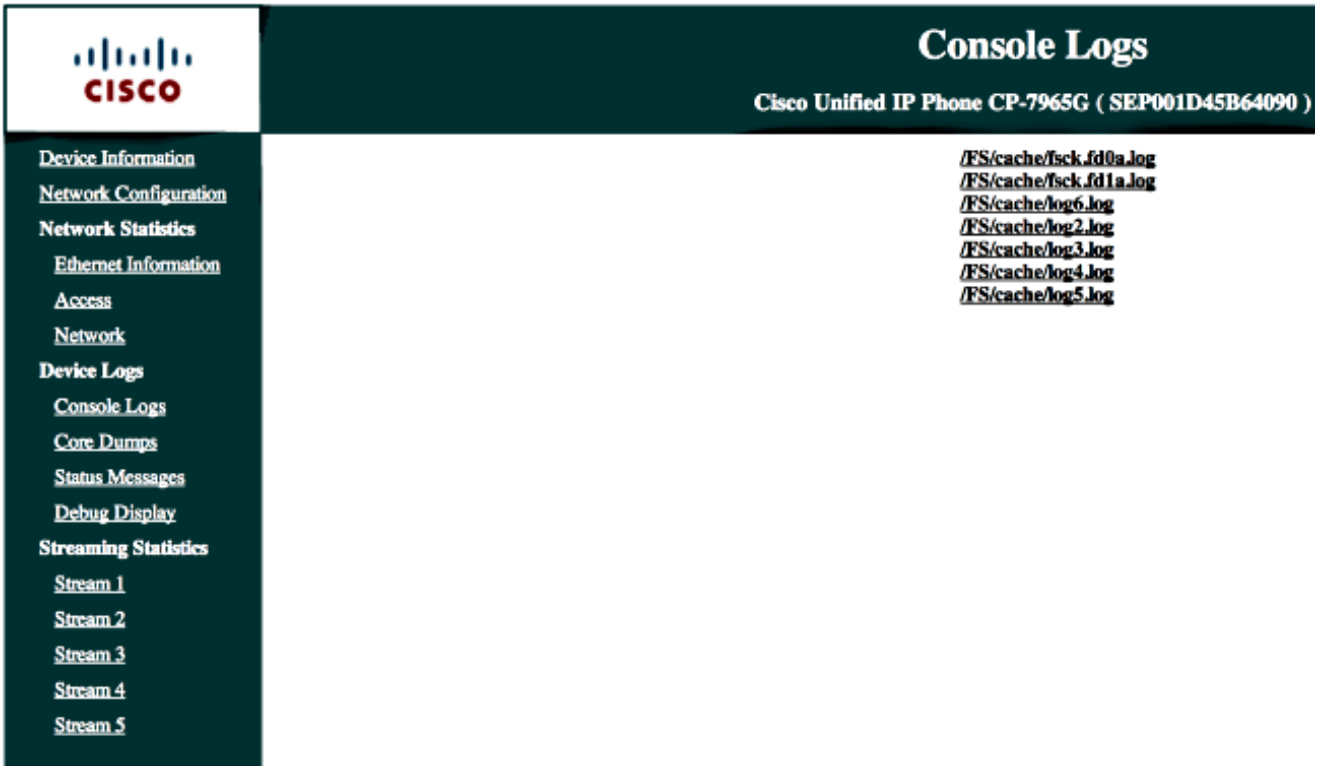
```
Router#show debug

WebVPN Subsystem:
WebVPN (verbose) debugging is on
WebVPN HTTP debugging is on
WebVPN AAA debugging is on
WebVPN tunnel debugging is on
WebVPN Tunnel Events debugging is on
WebVPN Tunnel Errors debugging is on
Webvpn Tunnel Packets debugging is on


PKI:
Crypto PKI Msg debugging is on
Crypto PKI Trans debugging is on
Crypto PKI Validation Path debugging is on
```

Debuga do telefone

1. Navegue ao **dispositivo > ao telefone de** CUCM.
2. Na página da configuração de dispositivo, ajuste o acesso à Web ao **permitido**.
3. Clique a **salvaguarda**, e clique-a então **aplicam a configuração**.



4. De um navegador, incorpore o endereço IP de Um ou Mais Servidores Cisco ICM NT do telefone, e escolha **logs do console do** menu à esquerda.



5. Transfira todos os arquivos do ***.log de /FS/cache/log**. Os arquivos do console log contêm a informação sobre porque o telefone não conecta ao VPN.

Erros relacionados

Identificação de bug Cisco CSCty46387, IO SSLVPN: Realce para mandar um contexto ser um padrão
Identificação de bug Cisco CSCty46436, IO SSLVPN: Realce ao comportamento da validação do certificado de cliente