Configurar e solucionar problemas de telefones VPN

Contents

Introduction

Este documento descreve como configurar e solucionar problemas do recurso de telefone VPN dos telefones IP da Cisco e do Cisco Unified Communications Manager.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco Unified Communications Manager (CUCM)
- Cisco Adaptive Security Appliance (ASA)
- Rede virtual privada (VPN) do AnyConnect
- Telefones IP da Cisco

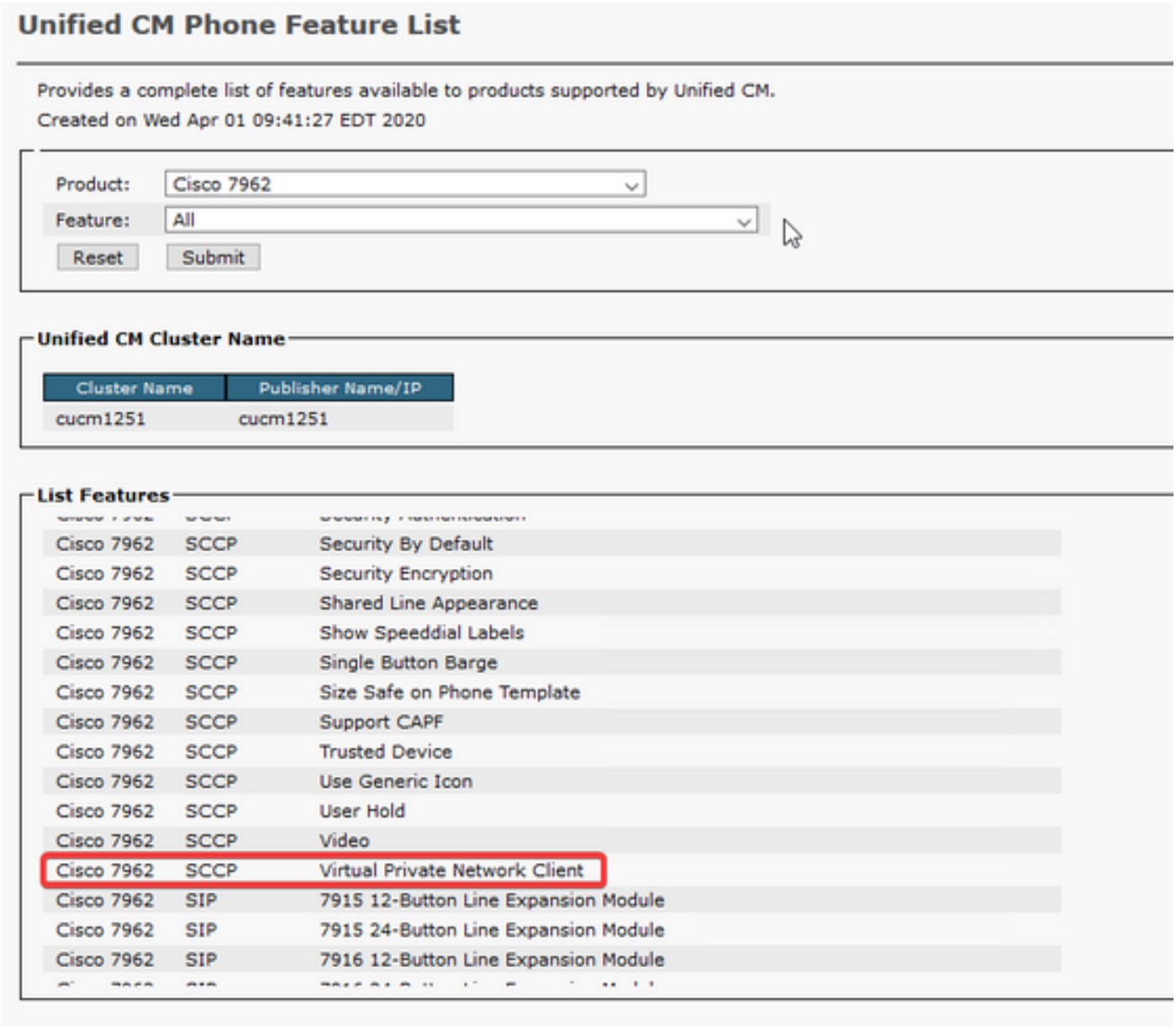
Componentes Utilizados

- 8861 14-0-1-0101-145
- ASAv 9.12(2)9
- CUCM 11.5.1.21900-40

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 ambiente de teste neste artigo inclui um 8861, ASAv e CUCM 11.5.1, mas há muitas variações diferentes desses produtos que você pode usar. Você deve verificar a Lista de recursos do telefone no CUCM para garantir que o modelo do telefone suporte o recurso VPN. Para usar a lista de recursos do telefone, acesse o editor do CUCM em seu navegador e navegue para **Cisco Unified Reporting > Lista de recursos do telefone Unified CM**. Gere um novo relatório e selecione o modelo do telefone no menu suspenso. Em seguida, é necessário pesquisar a seção List Features para Virtual Private Network Client, conforme mostrado na imagem:



Configurar

Os telefones VPN exigem que você tenha a configuração adequada em seu ASA e CUCM. Você pode começar com qualquer um dos produtos primeiro, mas este documento aborda a configuração do ASA primeiro.

Configuração do ASA

Etapa 1. Verifique se o ASA está licenciado para oferecer suporte ao AnyConnect para telefones VPN. O comando **show version** no ASA pode ser usado para verificar se o **Anyconnect para o Cisco VPN Phone** está ativado, como mostrado neste trecho:

```
[output omitted]
Licensed features for this platform:
Maximum VLANs : 50
Inside Hosts : Unlimited
Failover : Active/Standby
Encryption-DES : Enabled
Encryption-3DES-AES : Enabled
Security Contexts : 0
Carrier : Enabled
AnyConnect Premium Peers : 250
AnyConnect Essentials : Disabled
Other VPN Peers : 250
Total VPN Peers : 250
AnyConnect for Mobile : Enabled
AnyConnect for Cisco VPN Phone : Enabled
Advanced Endpoint Assessment : Enabled
Shared License : Disabled
Total TLS Proxy Sessions : 500
Botnet Traffic Filter : Enabled
Cluster : Disabled
```

Se esse recurso não estiver habilitado, você precisará trabalhar com a equipe de Licenças para obter a licença apropriada. Agora que você confirmou que o ASA suporta telefones VPN, você pode iniciar a configuração.

> **Note**: Todos os itens sublinhados na seção de configuração são nomes configuráveis que podem ser alterados. A maioria desses nomes é referenciada em outro lugar da configuração, portanto, é importante lembrar os nomes que você usa nessas seções (política de grupo, grupo de túnel etc.) porque você precisa deles mais tarde.

Etapa 2. Crie um pool de endereços IP para clientes VPN. Isso é semelhante a um pool de DHCP no fato de que quando um telefone IP se conecta ao ASA, ele recebe um endereço IP desse pool. O pool pode ser criado com este comando no ASA:

ip local pool vpn-phone-pool 10.10.1.1-10.10.1.254 mask 255.255.255.0

Além disso, se preferir uma rede ou máscara de sub-rede diferente, isso também pode ser alterado. Depois que o pool for criado, você precisará configurar uma política de grupo (um conjunto de parâmetros para a conexão entre o ASA e os telefones IP):

group-policy vpn-phone-policy internal

atributos de política de grupo vpn-telefone-política

split-tunnel-policy tunnelall

vpn-tunnel-protocol ssl-client

Etapa 3. Você precisa habilitar o AnyConnect se ele ainda não estiver habilitado. Para fazer isso, você precisa saber o nome da interface externa. Normalmente, essa interface é chamada **externa** (como mostrado no trecho), mas é configurável, portanto confirme se você tem a interface correta. Execute **show ip** para ver a lista de interfaces:

```
sckiewer-ASAv# show ip
System IP Addresses:
Interface Name IP address Subnet mask Method
GigabitEthernet0/0 outside 172.16.1.250 255.255.255.0 CONFIG
GigabitEthernet0/1 inside 172.16.100.250 255.255.255.0 CONFIG
Current IP Addresses:
Interface Name IP address Subnet mask Method
GigabitEthernet0/0 outside 172.16.1.250 255.255.255.0 CONFIG
GigabitEthernet0/1 inside 172.16.100.250 255.255.255.0 CONFIG
```

Nesse ambiente, a interface externa é nomeada **externamente**, de modo que esses comandos ativam o AnyConnect nessa interface.

webvpn
ativar fora
anyconnect enable

Etapa 4. Configure um novo grupo de túneis para aplicar a política de grupo criada anteriormente a qualquer cliente que se conecte em um URL específico. Observe a referência aos nomes do pool de endereços IP e da política de grupo que você criou anteriormente nas 3ª e 4ª linhas do trecho. Se você modificou os nomes do pool de endereços IP ou da política de grupo, é necessário usar substituir os valores incorretos pelos nomes modificados:

tunnel-group vpn-phone-group type remote-access
tunnel-group vpn-phone-group general-attribute
pool de endereços vpn-phone-pool
default-group-policy vpn-phone-policy
tunnel-group vpn-phone-group webvpn-attribute
certificado de autenticação
group-url https://asav.sckiewer.lab/phone enable

Você pode usar um endereço IP em vez de um nome para o **group-url**. Isso geralmente é feito se os telefones não tiverem acesso a um servidor DNS que possa resolver o FQDN (Fully Qualified Domain Name, nome de domínio totalmente qualificado) do ASA. Além disso, você pode ver que este exemplo usa autenticação baseada em certificado. Você também tem a opção de usar a autenticação de nome de usuário/senha, mas há mais requisitos no ASA que estão fora do escopo deste documento.

Neste exemplo, o servidor DNS tem o registro A, **asav.sckiewer.lab - 172.16.1.250** e você pode ver na saída **show ip** que 172.16.1.250 está configurado na interface chamada **fora**. Portanto, a configuração seria:

crypto ca trustpoint asa-identity-cert

inscrição automática

subject-name CN=asav.sckiewer.lab

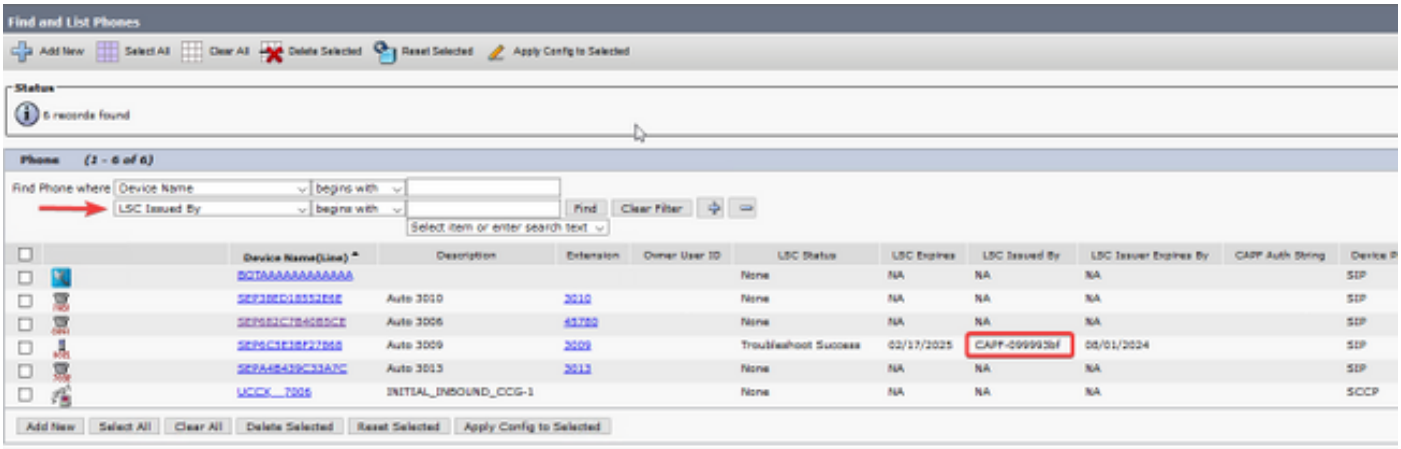
crypto ca enroll asa-identity-cert

ssl trust-point asa-identity-cert fora

Algumas observações:

1. Um novo ponto de confiança foi criado chamado asa-identity-cert e um nome de assunto foi aplicado a ele. Isso faz com que o certificado gerado deste ponto confiável use o nome de assunto especificado
2. Em seguida, o comando 'crypto ca enroll asa-identity-cert' permite que o ASA gere um certificado autoassinado e o salve nesse ponto de confiança
3. Finalmente, o ASA apresenta o certificado no ponto confiável para qualquer dispositivo que se conecta à interface externa

Etapa 5. Crie os pontos de confiança necessários para permitir que o ASA confie no certificado do telefone IP. Primeiro, você precisa determinar se seus telefones IP usam o Certificado instalado pelo fabricante (MIC) ou o Certificado localmente significativo (LSC). Por padrão, todos os telefones usam o MIC para conexões seguras, a menos que um LSC esteja instalado neles. No CUCM 11.5.1 e posterior, você pode executar uma pesquisa localizada em **Unified CM Administration > Device > Phone** para ver se os LSCs estão instalados, enquanto versões mais antigas do CUCM exigem que você verifique fisicamente as configurações de segurança em cada telefone. No CUCM 11.5.1, observe que você precisa adicionar um filtro (ou alterar o filtro padrão) ao **LSC Emitido por**. Dispositivos com **NA** na coluna **LSC Emitido por** utilizam o MIC, pois não têm um LSC instalado.

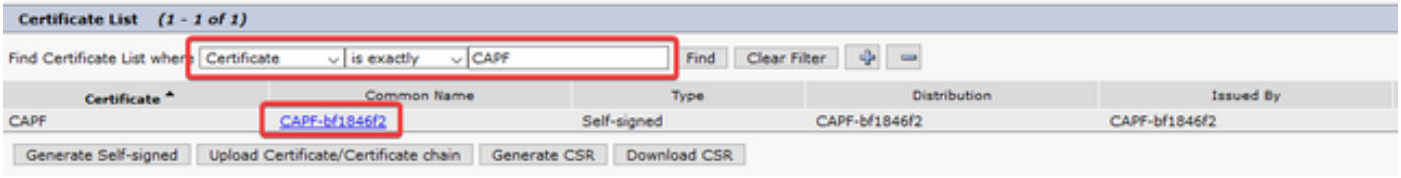


Se seu telefone se parece com o destacado na imagem, você precisa carregar o certificado CAPF do Editor do CUCM para o ASA para que o ASA valide o certificado do telefone para a conexão segura. Se quiser usar dispositivos sem LSC instalado, faça o upload dos certificados de fabricação da Cisco para o ASA. Esses certificados podem ser encontrados no Editor do CUCM no **Cisco Unified OS Administration > Security > Certificate Management**:

> **Note**: Você pode ver que alguns desses certificados em vários armazenamentos confiáveis (CallManager-trust e CAPF-trust). Não importa em qual loja confiável você faz download dos certificados, desde que você assegure-se de selecionar os certificados com esses nomes exatos.

- Cisco_Root_CA_2048 < Raiz SHA-1 MIC
- Cisco_Manufacturing_CA < MIC SHA-1 intermediário
- Cisco_Root_CA_M2 < Raiz do MIC SHA-256

- Cisco_Manufacturing_CA_SHA2 < MIC SHA-256 Intermediário
- CAPF do editor do CUCM < LSC



Em relação ao MIC, os modelos de telefones mais antigos, como as séries 79xx e 99xx, utilizam a cadeia de certificados SHA-1, enquanto os modelos de telefone mais novos, como a série 88xx, utilizam a cadeia de certificados SHA-256. A cadeia de certificados que seu(s) telefone(s) usa(m) precisa(m) ser carregada(s) no ASA.

Depois de ter os certificados necessários, você pode criar os pontos de confiança com:

crypto ca trustpoint cert1

terminal de inscrição

crypto ca authenticate cert1

O primeiro comando cria um ponto confiável chamado **cert1**, e o comando **crypto ca authenticate** permite colar o certificado codificado base64 na CLI. Você pode executar esses comandos quantas vezes precisar para obter os pontos de confiança apropriados no ASA, mas não se esqueça de usar um novo nome de ponto de confiança para cada certificado.

Etapa 6. Obtenha uma cópia do certificado de identidade ASA emitindo este comando:

crypto ca export asa-identity-cert identity-certificate

Isso exporta o certificado de identidade para o ponto confiável chamado asa-identity-cert. Ajuste o nome para que corresponda ao ponto de confiança criado na etapa 4.

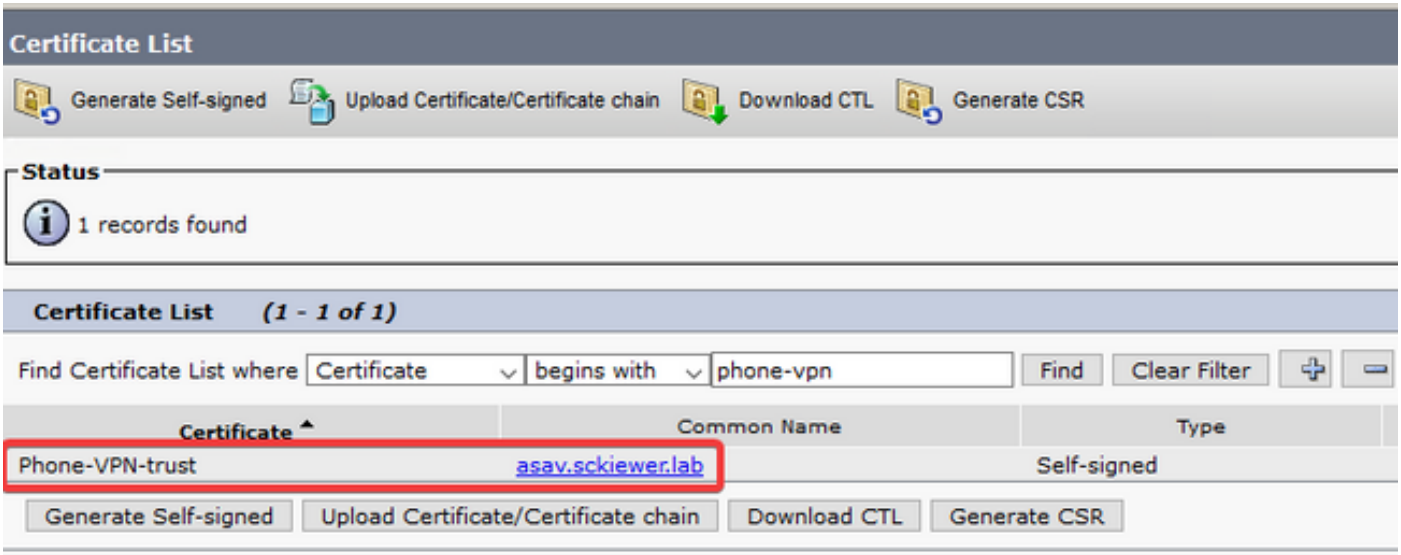
Aqui está a configuração completa do laboratório do ASA:

```
ip local pool vpn-phone-pool 10.10.1.1-10.10.1.254 mask 255.255.255.0

group-policy vpn-phone-policy internal
group-policy vpn-phone-policy attributes
     split-tunnel-policy tunnelall
     vpn-tunnel-protocol ssl-client

webvpn
     enable outside
     anyconnect enable

tunnel-group vpn-phone-group type remote-access
tunnel-group vpn-phone-group general-attributes
     address-pool vpn-phone-pool
     default-group-policy vpn-phone-policy

tunnel-group vpn-phone-group webvpn-attributes
     authentication certificate
     group-url https://asav.sckiewer.lab/phone enable

ssl trust-point asa-identity-cert outside
```

Neste ponto, a configuração do ASA está concluída e você pode prosseguir com a configuração do CUCM. Você precisa ter uma cópia do certificado ASA que acabou de coletar e o URL que foi configurado na seção grupo de túneis.

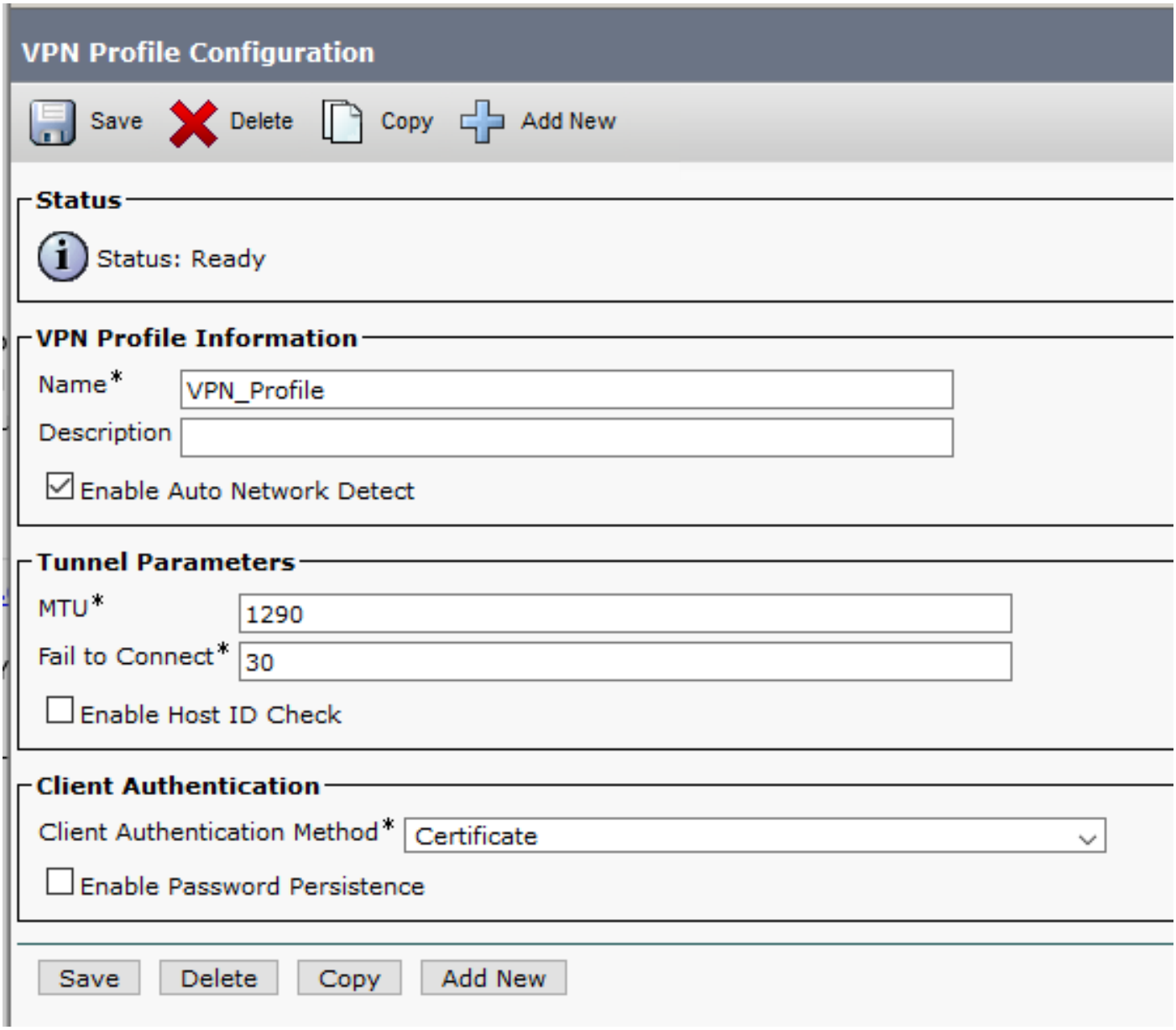
Configuração do CUCM

Etapa 1. No CUCM, navegue para **Cisco Unified OS Administration > Security > Certificate Management** e carregue o certificado ASA como **phone-vpn-trust**.

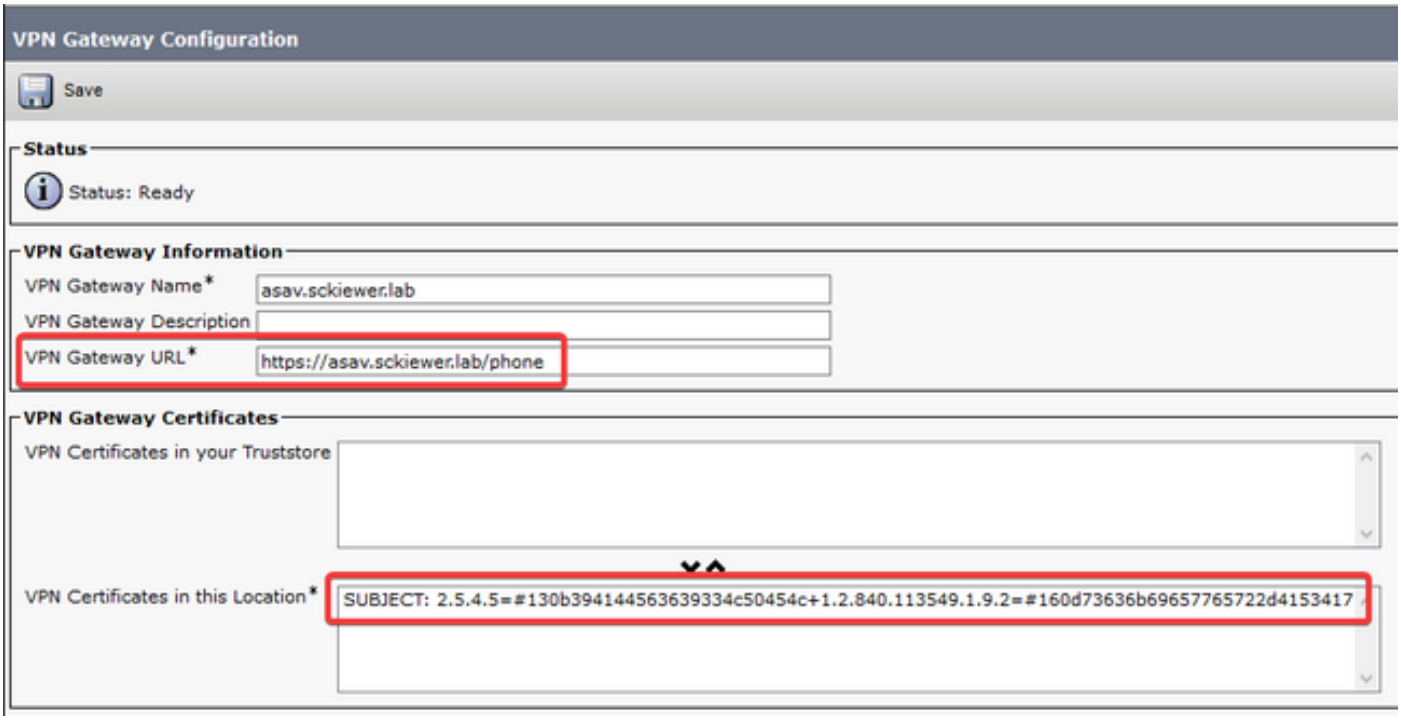


Etapa 2. Depois disso, navegue para **Cisco Unified CM Administration > Advanced Features > VPN > VPN Profile** e crie um novo perfil. Não há nenhum certo ou errado nesta seção. É importante entender o objetivo de cada configuração.

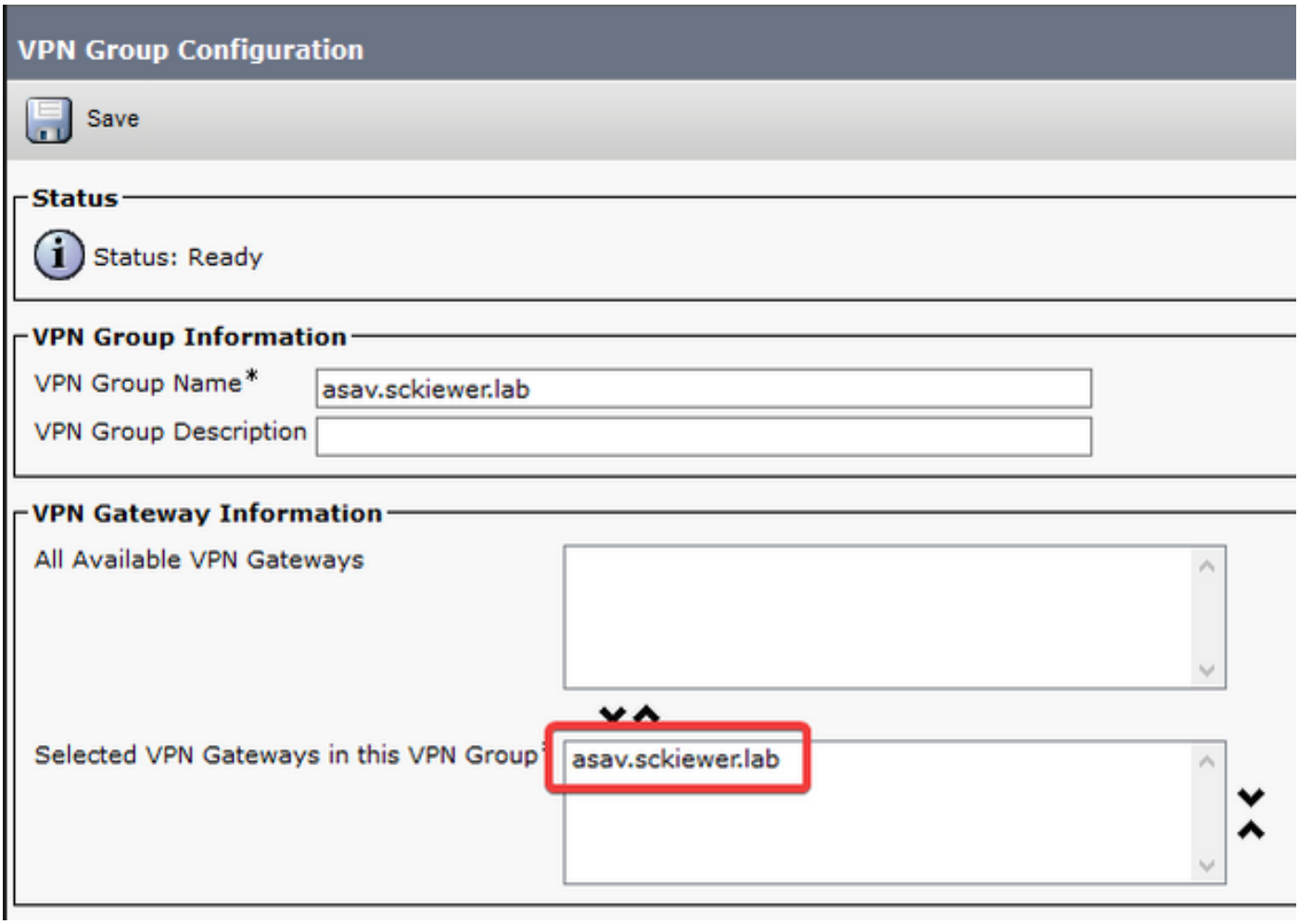
1. **Ativar detecção automática de rede** - quando esta opção está ativada, o telefone efetua ping no servidor TFTP quando é ligado. Se ele receber uma resposta a esse ping, não ativará a VPN. Se o telefone não receber uma resposta para esse ping, ele ativará a VPN. Quando esta configuração está ativada, a VPN não pode ser ativada manualmente.
2. **Verificação de ID do host** - quando ativada, o telefone inspeciona o URL da VPN do seu arquivo de configuração (https://asav.sckiewer.lab/phone é usado neste documento) e garante que o nome do host ou FQDN corresponda ao nome comum (CN) ou a uma entrada de SAN no certificado apresentado pelo ASA.
3. **Authentication Method** - controla que tipo de método de autenticação é usado para a conexão com o ASA. No exemplo de configuração deste documento, a autenticação baseada em certificado é usada.
4. **Persistência da senha** - se esta opção estiver ativada, a senha do cliente será armazenada no telefone até que ocorra uma falha na tentativa de login, o cliente limpará manualmente a senha ou o telefone será redefinido.



Etapa 3. Em seguida, navegue até **Cisco Unified CM Administration > Advanced Features > VPN > VPN Gateway**. Você precisa garantir que a URL do gateway de VPN corresponda à configuração do ASA e que mova o certificado da caixa superior para a caixa inferior, como mostrado na imagem:

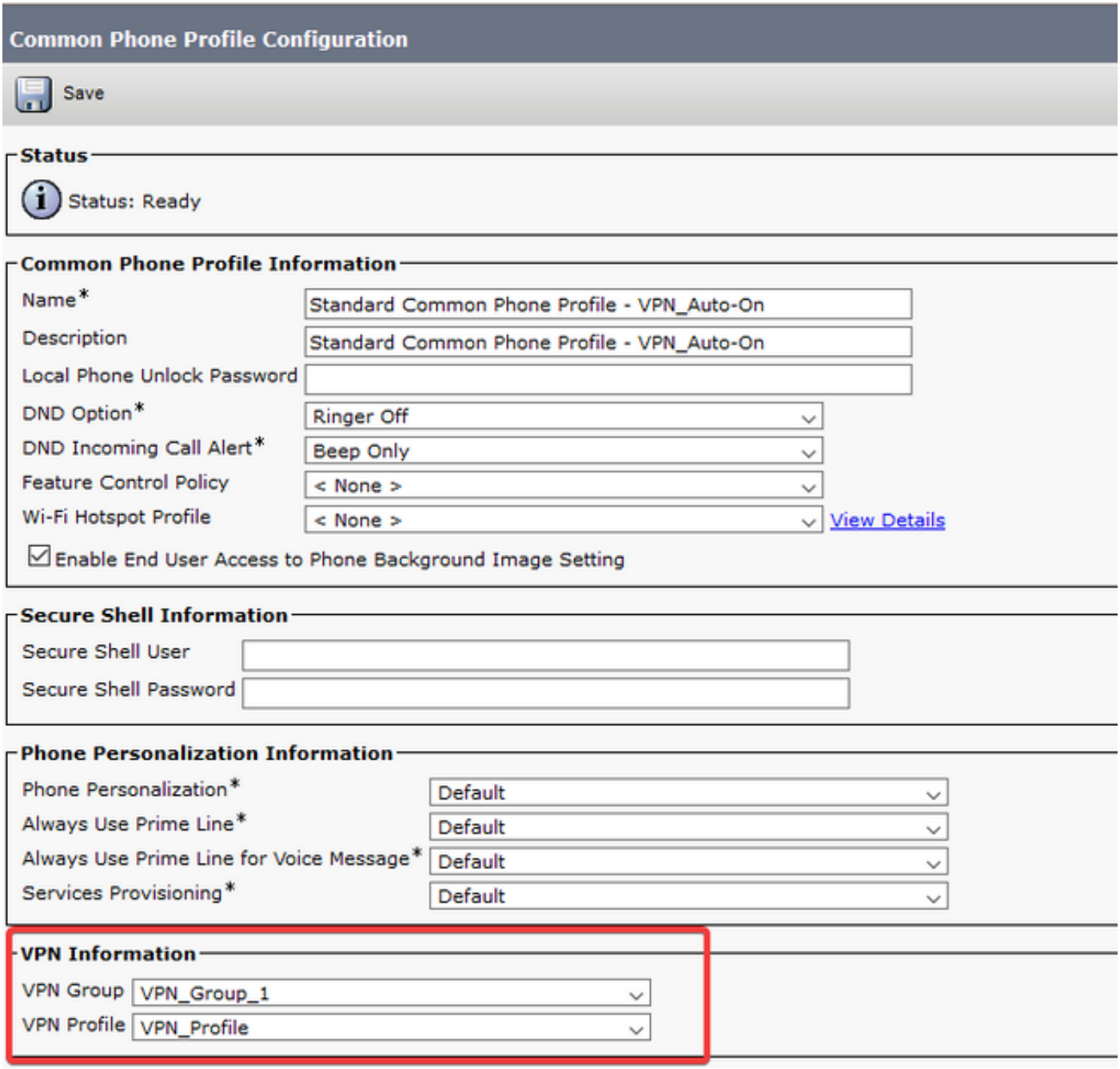


Etapa 4. Quando isso for salvo, você precisará navegar para **Cisco Unified CM Administration > Advanced Features > VPN > VPN Group** e mover o gateway que você criou para a caixa 'Seleted VPN Gateways in this VPN Group':



Etapa 5. Agora que as configurações de VPN foram configuradas, você precisa navegar para **Cisco Unified CM Administration > Device > Device Settings > Common Phone Profile**. Aqui, você deve copiar o perfil usado pelo telefone VPN desejado, renomeá-lo e selecionar seu grupo de

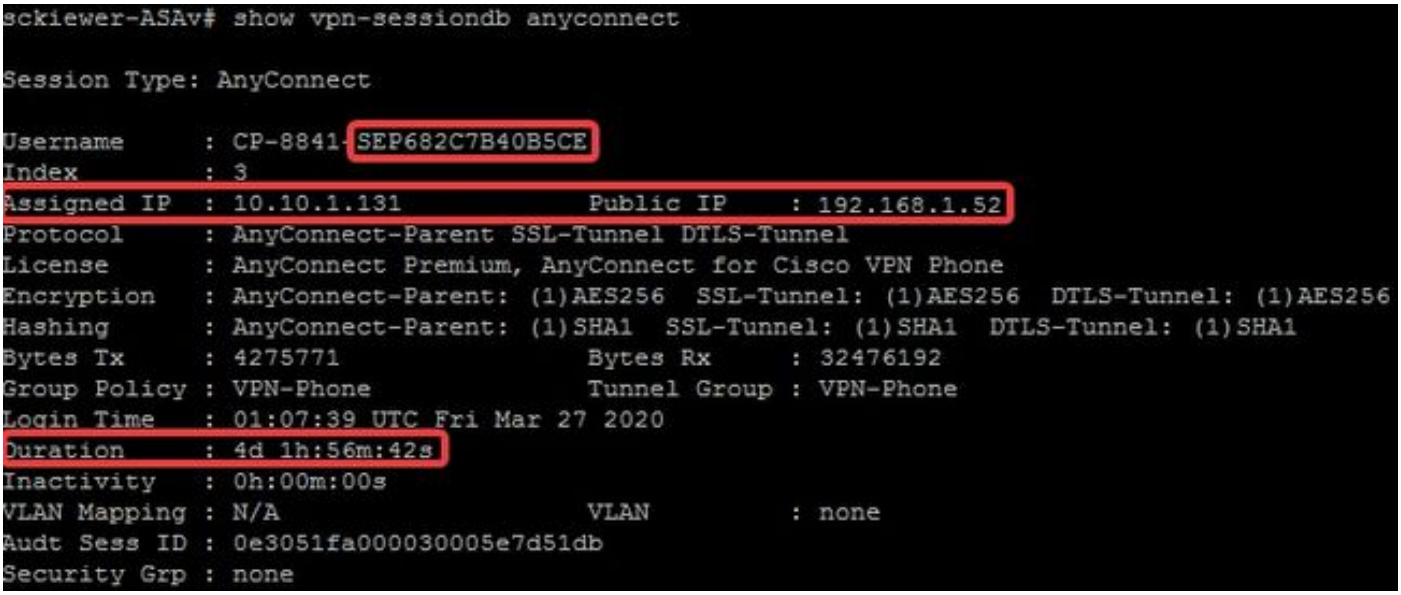
VPN e perfil de VPN e, em seguida, salvar o novo perfil:



Etapa 6. Finalmente, você precisa aplicar esse novo perfil ao telefone e reiniciá-lo enquanto ele estiver na rede interna. Isso permite que o telefone receba toda essa nova configuração, como o hash do certificado ASA e o URL da VPN.

> **Note**: Antes de testar o telefone, você precisa garantir que os telefones tenham um servidor 'TFTP alternativo' configurado. Como o ASA não fornece uma opção 150 para os telefones, o IP TFTP precisa ser configurado nos telefones manualmente.

Passo 7. Teste o telefone VPN e verifique se ele pode se conectar com êxito ao ASA e registrar-se. Você pode verificar se o túnel está ativo no ASA com, **show vpn-sessiondb anyconnect**:



Troubleshoot

Dados a serem coletados

Para solucionar um problema de telefone VPN, estes dados são recomendados:

- Depurações do ASA: logging buffered debuglogging debug-tracedebug crypto ca transactions 255debug crypto ca messages 255debug crypto ca 255debug webvpn 255debug webvpn anyconnect 255
- Registros do console do telefone (ou uma PRT se o telefone suportar - mais informações aqui)

Depois de reproduzir o problema com as depurações habilitadas, você poderá visualizar a saída com este comando, pois a saída de depuração sempre contém 711001:

show log | i 711001

Problemas comuns

> **Note**: Para os fins desta seção, os trechos de log são de um telefone 8861, pois essa é uma das séries telefônicas mais comuns implantadas como um telefone VPN. Lembre-se de que outros modelos podem escrever mensagens diferentes nos registros.

Atualizar o certificado de identidade autoassinado do ASA

Antes do certificado de identidade ASA expirar, um novo certificado precisa ser gerado e enviado para os telefones. Para fazer isso sem afetar os telefones VPN, use este processo:

Etapa 1. Crie um novo ponto de confiança para o novo certificado de identidade:

crypto ca trustpoint asa-identity-cert-2

inscrição automática

subject-name CN=asav.sckiewer.lab

crypto ca enroll asa-identity-cert-2

Etapa 2. Nesse ponto, você teria um novo certificado de identidade para o ASA, mas ele ainda não é usado em nenhuma interface. Você precisa exportar este novo certificado e carregá-lo no CUCM:

crypto ca export asa-identity-cert-2 identity-certificate

Etapa 3. Depois de ter o novo certificado de identidade, carregue-o em um dos nós do CUCM como phone-VPN-trust no **Cisco Unified OS Administration > Security > Certificate Management > Upload**.

> **Note**: O certificado de confiança de VPN do telefone atual estaria presente somente no nó do CUCM para o qual ele foi originalmente carregado (ele não é automaticamente propagado para outros nós, como alguns certificados). Se sua versão do CUCM for afetada pelo CSCuo58506, você deverá carregar o novo certificado ASA em um nó diferente.

Etapa 4. Quando o novo certificado for carregado em qualquer um dos nós no cluster, navegue para **Cisco Unified CM Administration > Advanced Features > VPN > VPN Gateway** no Editor do CUCM

Etapa 5. Selecione o gateway apropriado.

Etapa 6. Selecione o certificado na caixa superior (esta é a que você acabou de carregar) e selecione a seta para baixo para movê-lo para a parte inferior (isso permite que o TFTP adicione esse certificado aos arquivos de configuração do telefone VPN) e selecione Salvar.

Passo 7. Depois que isso tiver sido feito, redefina todos os telefones VPN. Neste ponto do processo, o ASA ainda apresenta o certificado antigo, de modo que os telefones podem se conectar, no entanto, eles adquirem um novo arquivo de configuração que contém o novo certificado e o antigo.

Etapa 8. Agora você pode aplicar o novo certificado ao ASA. Para fazer isso, você precisa do nome do novo ponto confiável e do nome da interface externa e, em seguida, execute esse comando com essas informações:

ssl trust-point asa-identity-cert-2 fora

> **Note**: Você pode navegar até a URL da webvpn no navegador para verificar se o ASA apresenta o novo certificado. Como esse endereço precisa ser publicamente acessível para que telefones externos o alcancem, seu PC também pode acessá-lo. Você pode verificar o certificado que o ASA apresenta ao seu navegador e confirmar que ele é o novo.

Etapa 9. Depois que o ASA estiver configurado para usar o novo certificado, redefina um telefone de teste e verifique se ele pode se conectar ao ASA e se registrar. Se o telefone for registrado com êxito, você poderá redefinir todos os telefones e verificar se eles podem se conectar ao ASA e registrar-se. Esse é o processo recomendado porque os telefones conectados ao ASA permanecem conectados após a alteração do certificado. Se você testar primeiro a atualização do certificado em um telefone, diminuirá o risco de um problema de configuração afetar um

grande número de telefones. Se o primeiro telefone VPN não puder se conectar ao ASA, você poderá coletar registros do telefone e/ou do ASA para solucionar problemas enquanto os outros telefones permanecerem conectados.

Etapa 10. Depois de verificar se os telefones podem se conectar e se registrar no novo certificado, o certificado antigo pode ser removido do CUCM.

ASA seleciona cifra da curva elíptica (EC)

Os ASAs oferecem suporte à criptografia da Curva Elíptica (EC) em 9.4(x), portanto, é comum ver que os telefones VPN em funcionamento anteriormente falham após uma atualização do ASA para 9.4(x) ou superior. Isso ocorre porque o ASA agora seleciona uma cifra EC durante o handshake TLS com modelos de telefone mais novos. Normalmente, há um certificado RSA associado à interface à qual o telefone se conecta, pois a versão anterior do ASA não suportava EC. Nesse ponto, como o ASA selecionou uma cifra EC, ele não pode usar um certificado RSA para a conexão, portanto ele gera e envia ao telefone um certificado autoassinado temporário que cria com o algoritmo EC em vez de RSA. Como esse certificado temporário não é reconhecido pelo telefone, a conexão falha. Você pode verificar se isso nos registros do telefone 88xx é bastante simples.

```
2101 NOT Mar 30 12:23:21.331861 (393:393) VPNC: -protocol_handler: current cipher -> ECDHE-RSA-
AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:AES256-SHA:AES128-SHA
2102 NOT Mar 30 12:23:21.331871 (393:393) VPNC: -protocol_handler: new cipher -> ECDHE-RSA-
AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:AES256-SHA:AES128-SHA
```

Os registros do telefone mostram que o ASA selecionou uma cifra EC para esta conexão, já que a linha 'nova cifra' contém cifras EC, o que causa falha na conexão.

Em um cenário em que o AES foi selecionado, você verá:

```
2691 NOT Mar 30 12:18:19.016923 (907:907) VPNC: -protocol_handler: current cipher -> ECDHE-RSA-
AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:AES256-SHA:AES128-SHA
2690 NOT Mar 30 12:18:19.016943 (907:907) VPNC: -protocol_handler: new cipher -> AES256-
SHA:AES128-SHA
```

Mais informações sobre isso podem ser encontradas aqui, CSCuu02848.

A solução para isso seria desabilitar cifras EC no ASA para a versão TLS que seu telefone usa. Mais informações sobre a versão TLS suportada por cada modelo de telefone podem ser encontradas aqui:

Table 6 lists the TLS versions supported by the Cisco IP phones.

Table 6. TLS version support

Version	Phone Models			
	7900	6900, 8900, 9900	7811, 7821, 7841, 7861	8811, 8821, 8841, 8845, 8851, 8861, 8865
TLS 1.0	Yes	Yes	Yes	Yes
TLS 1.2	No	No	Yes	Yes
Disable TLS 1.0 and TLS 1.1 with https for web access*	No	No	Yes	Yes
Selectively Disable TLS cipher suites used by TLS connection or handshake**	No	No	Yes	Yes

* With 12.1 firmware
** With 12.5 firmware

https://www.cisco.com/c/dam/en/us/products/collateral/collaboration-endpoints/unified-ip-phone-8800-series/white-paper-c11-739097.pdf

Depois de saber quais versões TLS são relevantes em seu ambiente, você pode executar esses comandos no ASA para desativar cifras EC para essas versões:

```
ssl cipher tlsv1 custom "AES256-SHA:AES128-SHA:AES256-GCM-SHA384:AES256-SHA256:AES128-GCM-SHA256:AES128-SHA256:AES256-SHA"
ssl cipher tlsv1.1 custom "AES256-SHA:AES128-SHA:AES256-GCM-SHA384:AES256-SHA256:AES128-GCM-SHA256:AES128-SHA256:AES256-SHA"
ssl cipher tlsv1.2 custom "AES256-SHA:AES128-SHA:AES256-GCM-SHA384:AES256-SHA256:AES128-GCM-SHA256:AES128-SHA256:AES256-SHA"
ssl cipher dtlsv1 custom "AES256-SHA:AES128-SHA:AES256-GCM-SHA384:AES256-SHA256:AES128-GCM-SHA256:AES128-SHA256:AES256-SHA"
```

Lembre-se de que os telefones IP usam DTLS (Datagram Transport Layer Security) por padrão, portanto é necessário executar a instrução cifra para DTLS e a versão TLS relevante para seus telefones. Além disso, é importante entender que essas alterações são alterações globais no ASA, para que impeçam que cifras da CE sejam negociadas por qualquer outro cliente AnyConnect que use essas versões TLS.

Falha de conexão DTLS

Em alguns casos, os telefones VPN não podem estabelecer uma conexão com o ASA com DTLS. Se o telefone tentar usar o DTLS mas falhar, ele continuará a tentar o DTLS repetidamente, sem êxito, porque sabe que o DTLS está ativado. Isso aparecerá nos registros do telefone 88xx:

```
3249 ERR Mar 29 15:22:38.949354 (385:385) VPNC: -dtls_state_cb: DTLSv0.9: write: alert: fatal:illegal parameter
3250 NOT Mar 29 15:22:38.951428 (385:385) VPNC: -vpnc_set_notify_netsd : cmd: 0x5 event: 0x40000 status: 0x0 error: 0x0
3251 ERR Mar 29 15:22:38.951462 (385:385) VPNC: -alert_err: DTLS write alert: code 47, illegal parameter
3252 ERR Mar 29 15:22:38.951489 (385:385) VPNC: -create_dtls_connection: SSL_connect ret -1, error 1
```

```
3253 ERR Mar 29 15:22:38.951506 (385:385) VPNC: -DTLS: SSL_connect: SSL_ERROR_SSL (error 1)
3254 ERR Mar 29 15:22:38.951552 (385:385) VPNC: -DTLS: SSL_connect: error:140920C5:SSL
routines:ssl3_get_server_hello:old session cipher not returned
3255 ERR Mar 29 15:22:38.951570 (385:385) VPNC: -create_dtls_connection: DTLS setup failure,
cleanup
3256 WRN Mar 29 15:22:38.951591 (385:385) VPNC: -dtls_state_cb: DTLSv0.9: write: alert:
warning:close notify
3257 ERR Mar 29 15:22:38.951661 (385:385) VPNC: -do_dtls_connect: create_dtls_connection failed
3258 ERR Mar 29 15:22:38.951722 (385:385) VPNC: -protocol_handler: connect: do_dtls_connect
failed
3259 WRN Mar 29 15:22:38.951739 (385:385) VPNC: -protocol_handler: connect : err: SSL success
DTLS fail
```

Isso pode ser causado pelo mesmo problema mencionado na seção Cifra de seleção de curva elíptica (EC) do ASA, portanto, você deve garantir que as cifras EC estejam desativadas para DTLS. Além disso, você pode desabilitar totalmente o DTLS, o que força os telefones VPN a usarem TLS. Isso não seria ideal, pois significaria que todo o tráfego utilizaria o TCP em vez do UDP, o que acrescentaria alguma sobrecarga. No entanto, em alguns cenários, esse é um bom teste, pois pelo menos confirma que a maior parte da configuração é boa, e o problema é específico para o DTLS. Se você quiser testar isso, é melhor fazer isso em um nível de política de grupo, pois os administradores normalmente usam uma política de grupo exclusiva para telefones VPN, então isso nos permite testar uma alteração sem afetar outros clientes.

atributos de política de grupo vpn-telefone-política
webvpn
anyconnect ssl dtls none

Outro problema de configuração comum que pode impedir uma conexão DTLS bem-sucedida é se o telefone não puder estabelecer a conexão TLS e DTLS com a mesma cifra. Exemplo de trecho de log:

```
%%%%% TLS Ciphers Offered
3905 NOT Apr 01 20:14:22.741838 (362:362) VPNC: -protocol_handler: new cipher -> ECDHE-RSA-
AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:AES256-SHA:AES128-SHA

%%%%% DTLS Ciphers Offered
4455 NOT Apr 01 20:14:23.405417 (362:362) VPNC: -process_connect: x-dtls-ciphersuite: AES128-SHA
4487 NOT Apr 01 20:14:23.523994 (362:362) VPNC: -create_dtls_connection: cipher list: AES128-SHA

%%%%% DTLS connection failure
4496 WRN Apr 01 20:14:53.547046 (362:474) VPNC: -vpnc_control: conn timer expired at:1585772093,
to abort connect
4497 NOT Apr 01 20:14:53.547104 (362:474) VPNC: -abort_connect: in dtls setup phase
```

Você pode ver as cifras TLS oferecidas na primeira linha do trecho. A opção mais segura que os dois lados suportam é selecionada (os registros não mostram a seleção, no entanto, você pode deduzir que é pelo menos AES-256 do trecho de log). Você também pode ver que a única cifra DTLS oferecida é AES128. Como a cifra TLS selecionada não está disponível para DTLS, a conexão falha. A correção neste cenário seria garantir que a configuração do ASA permita que os mesmos cifras sejam usados para TLS e DTLS.

O telefone não pode se conectar ao ASA após a atualização do certificado

Émuito importante que você carregue um novo certificado de identidade ASA como phone-vpn-trust no CUCM para que os telefones possam adquirir o hash desse novo certificado. Se esse processo não for seguido, depois da atualização e da próxima vez que um telefone VPN tentar se conectar ao ASA, o telefone receberá um certificado em que não confia, portanto a conexão

falhará. Isso pode ocorrer dias ou semanas após a atualização do certificado ASA porque os telefones não são desconectados quando o certificado é alterado. Enquanto o ASA continuar recebendo keepalives do telefone, o túnel VPN permanecerá ativo. Portanto, se você confirmou que o certificado ASA foi atualizado, mas o novo certificado não foi colocado no CUCM primeiro, você tem duas opções:

1. Se o certificado de identidade ASA antigo ainda for válido, reverta o ASA de volta para o certificado antigo e siga o processo fornecido neste documento para atualizar o certificado. Você pode ignorar a seção de geração de certificado se já tiver gerado um novo certificado.
2. Se o certificado de identidade antigo do ASA tiver expirado, você precisaria carregar o novo certificado do ASA para o CUCM e trazer os telefones de volta para a rede interna para receber o arquivo de configuração atualizado com o novo hash de certificado.

O telefone não consegue resolver o URL do ASA via DNS

Em alguns cenários, o administrador configura o URL da VPN com um nome de host em vez de um endereço IP. Quando isso é feito, o telefone precisa ter um servidor DNS para poder resolver o nome para um endereço IP. No trecho, você pode ver que o telefone tenta resolver o nome com seus dois servidores DNS, 192.168.1.1 e 192.168.1.2, mas não recebe uma resposta. Após 30 segundos, o telefone imprime um 'DnsLookupErr:'

```
3816 NOT Mar 3 15:38:03.819168 VPNC: -do_login: URL -> https://asav.sckiewer.lab/phone
...
3828 INF Mar 3 15:38:03.834915 dnsmasq[322]: query[A] asav.sckiewer.lab from 127.0.0.1
3829 INF Mar 3 15:38:03.835004 dnsmasq[322]: forwarded asav.sckiewer.lab to 192.168.1.1
3830 INF Mar 3 15:38:03.835030 dnsmasq[322]: forwarded asav.sckiewer.lab to 192.168.1.1
3831 INF Mar 3 15:38:17.845305 dnsmasq[322]: query[A] asav.sckiewer.lab from 127.0.0.1
3832 INF Mar 3 15:38:17.845352 dnsmasq[322]: forwarded asav.sckiewer.lab to 192.168.1.1
3833 INF Mar 3 15:38:17.845373 dnsmasq[322]: forwarded asav.sckiewer.lab to 192.168.1.2
3834 INF Mar 3 15:38:31.854834 dnsmasq[322]: query[A] asav.sckiewer.lab from 127.0.0.1
3835 INF Mar 3 15:38:31.854893 dnsmasq[322]: forwarded asav.sckiewer.lab to 192.168.1.1
3836 INF Mar 3 15:38:31.855213 dnsmasq[322]: forwarded asav.sckiewer.lab to 192.168.1.2
3837 ERR Mar 3 15:38:32.864376 VPNC: -parse_url: gethostbyname failed <asav.sckiewer.lab>
3838 NOT Mar 3 15:38:32.864435 VPNC: -vpnc_set_notify_netsd : cmd: 0x5 event: 0x40000 status:
0x0 error: 0x0
3839 ERR Mar 3 15:38:32.864464 VPNC: -do_login: parse URL failed ->
https://asav.sckiewer.lab/phone
3840 NOT Mar 3 15:38:32.864482 VPNC: -vpn_stop: de-activating vpn
3841 NOT Mar 3 15:38:32.864496 VPNC: -vpn_set_auto: auto -> auto
3842 NOT Mar 3 15:38:32.864509 VPNC: -vpn_set_active: activated -> de-activated
3843 NOT Mar 3 15:38:32.864523 VPNC: -set_login_state: LOGIN: 1 (TRYING) --> 3 (FAILED)
3844 NOT Mar 3 15:38:32.864538 VPNC: -set_login_state: VPNC : 1 (LoggingIn) --> 3 (LoginFailed)
3845 NOT Mar 3 15:38:32.864561 VPNC: -vpnc_send_notify: notify type: 1 [LoginFailed]
3846 NOT Mar 3 15:38:32.864580 VPNC: -vpnc_send_notify: notify code: 32 [DnsLookupErr]
3847 NOT Mar 3 15:38:32.864611 VPNC: -vpnc_send_notify: notify desc: [url hostname lookup err]
```

Isso geralmente indica um dos seguintes:

1. O telefone tem um servidor DNS inválido
2. O telefone não recebeu um servidor DNS via DHCP ou não foi configurado manualmente

Para corrigir esse problema, há duas opções:

1. Verifique a configuração no telefone para garantir que ele receba um servidor DNS do servidor DHCP quando for externo e/ou verifique se o servidor DNS do telefone pode resolver o nome usado na configuração do ASA

2. Alterar o URL na configuração do ASA e do CUCM para um endereço IP de modo que o DNS não seja necessário

O telefone não ativa a VPN

Como mencionado anteriormente neste documento, a detecção automática de rede faz com que o telefone faça ping no servidor TFTP e verifique se há uma resposta. Se o telefone estiver na rede interna, o servidor TFTP poderá ser alcançado sem VPN, de modo que quando o telefone receber respostas aos pings, ele não ativará a VPN. Quando o telefone NÃO está na rede interna, os pings falham, então o telefone ativaria a VPN e se conectaria ao ASA. Lembre-se de que a rede residencial de um cliente provavelmente não será configurada para fornecer ao telefone uma opção 150 via DHCP, e o ASA também não pode fornecer uma opção 150, portanto, 'TFTP alternativo' é um requisito para telefones VPN.

Nos registros, você gostaria de verificar algumas coisas:

1. O telefone faz ping no IP do servidor TFTP do CUCM?
2. O telefone recebe uma resposta aos pings?
3. O telefone ativa a VPN depois de não receber uma resposta aos pings?

Éimportante visualizar esses itens nesta ordem. Em um cenário em que o telefone está fazendo ping no IP errado e recebendo uma resposta, seria inútil ativar depurações no ASA porque o telefone não ativará a VPN. Valide esses 3 itens nesta ordem para que você possa evitar análises de log desnecessárias. Você verá isso nos registros do telefone 88xx se o ping falhar e a VPN estiver ativada depois:

```
5645 NOT Mar 27 11:32:34.630109 (574:769) JAVA-vpnAutoDetect: ping time out
5647 DEB Mar 27 11:32:34.630776 (710:863) JAVA-configmgr MQThread|cip.vpn.VpnStateHandler:? -
VpnStateHandler: handleVPN_ENABLED_STATE()
```

Registros de telefone, mas não é possível exibir o histórico de chamadas

Verifique se o telefone tem TFTP alternativo ativado e o TFTP IP correto configurado. O TFTP alternativo é um requisito para telefones VPN porque o ASA não pode fornecer uma opção 150.

Informações Relacionadas

- Suporte Técnico e Documentação - Cisco Systems