Configurar o tronco do SORVO TLS no Gerenciador de Comunicações com um certificado assinado de CA.

Índice

Introdução
Pré-requisitos
Requisitos
Componentes Utilizados
Informações de Apoio
Configurar
Etapa 1. Use CA público ou CA estabelecido em Windows Server 2003
Etapa 2. Verifique o hostname e os ajustes
Etapa 3. Gerencia e transfira a solicitação de assinatura de certificado (o CSR)
Etapa 4. Assine o CSR com o Certificate Authority de Microsoft Windows 2003
Etapa 5. Obtenha o certificado de raiz de CA
Etapa 6. Certificado de raiz de CA da transferência de arquivo pela rede como a confiança do CallManager
Etapa 7. Certificado do CallManager CSR do sinal de CA da transferência de arquivo pela rede como o certificado do CallManager.
Etapa 8. Crie perfis de segurança do tronco do SORVO
Etapa 9. Crie troncos do SORVO
Etapa 10. Crie rotas padrão
Verificar
Troubleshooting
Recolha a captura de pacote de informação em CUCM
Recolha traços CUCM
Cisco relacionado apoia discussões da comunidade

Introdução

Este documento descreve um processo passo a passo para configurar o tronco do Transport Layer Security do Session Initiation Protocol (SIP) (TLS) no Gerenciador de Comunicações com um certificado assinado do Certificate Authority (CA).

Após ter seguido este documento, as mensagens do SORVO entre dois conjuntos serão cifradas usando o TLS.

Pré-requisitos

Requisitos

Cisco recomenda que você tem o conhecimento de:

- Gerente das comunicações unificadas de Cisco (CUCM)
- SORVO

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software:

- Versão 9.1(2) CUCM
- Versão 10.5(2) CUCM
- Microsoft Windows server 2003 como CA

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.

Informações de Apoio

Segundo as indicações desta imagem, saudação de SSL usando Certificados.

Configurar

Etapa 1. Use CA público ou CA estabelecido em Windows Server 2003

Refira o link: CA estabelecido em Windows 2003 separa

Etapa 2. Verifique o hostname e os ajustes

Os Certificados são baseados em nomes. Assegure-se de que os nomes estejam corretos antes de começar.

```
From SSH CLI
admin:show cert own CallManager
SignatureAlgorithm: SHA1withRSA (1.2.840.113549.1.1.5)
Issuer Name: CN=CUCMA, OU=cisco, O=cisco, L=cisco, ST=cisco, C=IN
Subject Name: CN=CUCMA, OU=cisco, O=cisco, L=cisco, ST=cisco, C=IN
```

A fim mudar o hostname, refira o link: Mude o hostname em CUCM

Etapa 3. Gerencia e transfira a solicitação de assinatura de certificado (o CSR)

CUCM 9.1(2)

A fim gerar o CSR, navegam ao > gerenciamento de certificado do > segurança **Admin do OS > gerenciem o CSR**

No campo de nome do certificado, selecione a opção do **CallManager da** lista de drop-down.

A fim transferir o CSR, navegue ao **> gerenciamento de certificado do > segurança Admin do OS**

> à transferência CSR

No campo de nome do certificado, selecione a opção do **CallManager da** lista de drop-down.

CUCM 10.5(2)

A fim gerar o CSR, navegue ao **> gerenciamento de certificado do > segurança Admin do OS > gerenciem o CSR**

1. No campo da **finalidade do certificado,** selecione o **CallManager da** lista de drop-down.

2. No campo do **comprimento chave,** selecione **1024 da** lista de drop-down.
3. No campo do **algoritmo de hash,** selecione o **SHA1 da** lista de drop-down.

A fim transferir o CSR, navegue ao **> gerenciamento de certificado do > segurança Admin do OS > à transferência CSR**

No campo da **finalidade do certificado,** selecione a opção do **CallManager da** lista de drop-down.

> **Note**: O CallManager CSR é gerado com as 1024 chaves de Rivest-Shamir-Addleman do bit (RSA).

Etapa 4. Assine o CSR com o Certificate Authority de Microsoft Windows 2003

Esta é uma informação opcional para assinar o CSR com Microsoft Windows 2003 CA.

1. Abra a autoridade de certificação.

2. Clicar com o botão direito o ícone de **CA** e navegue a **todas as tarefas > submetem o pedido novo**

3. Selecione o CSR e clique a opção **aberta** (aplicável em ambos os CSR (CUCM 9.1(2) e CUCM 10.5(2))

4. Todo o indicador aberto CSR no dobrador pendente dos pedidos. Clicar com o botão direito cada CSR e navegue a **todas as tarefas > edição** a fim emitir os Certificados. (Aplicável em ambos os CSR (CUCM 9.1(2) e CUCM 10.5(2))

5. A fim transferir o certificado, escolha o dobrador **emitido dos Certificados**.

Clicar com o botão direito o certificado e clique a opção **aberta**.

6. Os detalhes certificados são indicados. A fim transferir o certificado, selecione a aba dos **detalhes** e clique a **cópia do** botão **para arquivar…**

7. No wizard do assistente da exportação do certificado, clicam o **Base-64 codificaram X.509(.CER) o** botão de rádio.

8. Nomeiam o arquivo exatamente. Este exemplo usa o formato de **CUCM1052.cer**.

Para CUCM 9.1(2), siga o mesmo procedimento.

Etapa 5. Obtenha o certificado de raiz de CA

Abra o indicador da **autoridade de certificação**.

A fim transferir a CA raiz

1. Clicar com o botão direito o ícone de CA e clique a **opção de propriedades**.

2. No tab geral, clique o **certificado da vista.**

3. No indicador do **certificado**, clique a ABA dos detalhes.

4. Clique a **cópia para arquivar…**

Etapa 6. Certificado de raiz de CA da transferência de arquivo pela rede como a confiança do CallManager

A fim transferir arquivos pela rede o certificado de raiz de CA, início de uma sessão ao **> gerenciamento de certificado do > segurança Admin do OS > ao certificado/certificate chain da transferência de arquivo pela rede**

> **Note**: Execute estas etapas em ambos o CUCMs (CUCM 9.1(2) e CUCM 10.5(2))

Etapa 7. Certificado do CallManager CSR do sinal de CA da transferência de arquivo pela rede como o certificado do CallManager.

A fim transferir arquivos pela rede CA assine o CallManager CSR, início de uma sessão ao **> gerenciamento de certificado do > segurança Admin do OS > ao certificado/certificate chain da transferência de arquivo pela rede**

> **Note**: Execute estas etapas em ambos o CUCMs (CUCM 9.1(2) e CUCM 10.5(2))

Etapa 8. Crie perfis de segurança do tronco do SORVO

CUCM 9.1(2)

A fim criar o perfil de segurança do tronco do SORVO, navegue ao **> segurança do sistema > ao perfil de segurança do tronco do SORVO**.

Copie a existência perfil não seguro do tronco do SORVO e dê-lhe um novo nome. No exemplo, o perfil não seguro do tronco do SORVO foi rebatizado com perfil seguro TLS do tronco do SORVO.

No nome do sujeito X.509 use o Common Name (CN) do CUCM 10.5(2) (certificado assinado de CA) segundo as indicações desta imagem.

CUCM 10.5(2)

Navegue ao **> segurança do sistema > ao perfil de segurança do tronco do SORVO.**

Copie a existência perfil não seguro do tronco do SORVO e dê-lhe um novo nome. No exemplo, o perfil não seguro do tronco do SORVO foi rebatizado com perfil seguro TLS do tronco do SORVO.

No nome do sujeito X.509 use o CN do CUCM 9.1(2) (certificado assinado de CA) como destacado:

Ambos os perfis de segurança do tronco do SORVO ajustam uma porta de recebimento de 5061, em que cada conjunto escuta na porta TCP 5061 os atendimentos de entrada novos do SORVO TLS.

Etapa 9. Crie troncos do SORVO

Depois que os perfis de segurança são criados, crie os troncos do SORVO e faça as mudanças para o parâmetro de configuração abaixo no tronco do SORVO.

CUCM 9.1(2)

1. No indicador da **configuração de tronco do** SORVO, verifique o parâmetro de configuração **SRTP permitido a** caixa de seleção.

Isto fixa o Real-Time Transport Protocol (RTP) a ser usado para os atendimentos sobre este tronco. Esta caixa deve somente ser verificada quando você usa o SORVO TLS porque as chaves para o protocolo de transporte em tempo real seguro (SRTP) estão trocadas no corpo da mensagem do SORVO. A sinalização do SORVO deve ser fixada pelo TLS, se não qualquer um com a sinalização NON-segura do SORVO poderia decifrar o córrego correspondente SRTP sobre o tronco.

2. **Na seção de informação do SORVO do** indicador da **configuração de tronco do** SORVO, adicionar **perfil de segurança o endereço de destino**, a **porta do destino**, e do **tronco do SORVO.**

CUCM 10.5(2)

1. No indicador da **configuração de tronco do** SORVO, verifique o parâmetro de configuração **SRTP permitido a** caixa de seleção.

Isto permite que o SRTP seja usado para atendimentos sobre este tronco. Esta caixa deve somente ser verificada ao usar o SORVO TLS, porque as chaves para o SRTP são trocadas no corpo da mensagem do SORVO. A sinalização do SORVO deve ser fixada pelo TLS porque qualquer um com uma sinalização NON-segura do SORVO poderia decifrar o córrego seguro correspondente RTP sobre o tronco.

2. **Na seção de informação do SORVO do** indicador da **configuração de tronco do** SORVO, adicionar o **endereço IP de destino**, a **porta do destino**, e o **perfil de segurança**

Etapa 10. Crie rotas padrão

O método o mais simples é criar uma rota padrão em cada conjunto, apontando diretamente ao tronco do SORVO. Os grupos de rotas e as lista da rota poderiam igualmente ser usados.

Pontos CUCM 9.1(2) à **rota padrão** 9898 através do tronco do SORVO TLS ao CUCM 10.5(2)

Os pontos CUCM 10.5(2) à **rota padrão** 1018 através do tronco do SORVO TLS ao CUCM 9.1(2)

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshooting

O atendimento do SORVO TLS pode ser debugado com estas etapas.

Recolha a captura de pacote de informação em CUCM

A fim verificar a Conectividade entre o CUCM 9.1(2) e o CUCM 10.5(2), para tomar uma captura de pacote de informação nos server e no relógio CUCM para ver se há o SORVO TLS trafique.

O tráfego do SORVO TLS é transmitido na porta TCP 5061, considerada como o sorvo-TLS.

No exemplo seguinte há uma sessão CLI SSH estabelecida ao CUCM 9.1(2)

1. Captura de pacote de informação CLI na tela

Este CLI imprime a saída na tela para o tráfego do SORVO TLS.

```
admin:utils network capture host ip 10.106.95.200
Executing command with options:
interface=eth0
ip=10.106.95.200
19:04:13.410944 IP CUCMA.42387 > 10.106.95.200.sip-tls: P 790302485:790303631(1146) ack
3661485150 win 182 <nop,nop,timestamp 2864697196 5629758>
19:04:13.450507 IP 10.106.95.200.sip-tls > CUCMA.42387: . ack 1146 win 249 <nop,nop,timestamp
6072188 2864697196>
19:04:13.465388 IP 10.106.95.200.sip-tls > CUCMA.42387: P 1:427(426) ack 1146 win 249
<nop,nop,timestamp 6072201 2864697196>
```

2. Captações CLI a arquivar

Este CLI faz a captura de pacote de informação baseada no host e cria um arquivo nomeado pacotes.

```
admin:utils network capture eth0 file packets count 100000 size all host ip 10.106.95.200
```

Reinicie o tronco do SORVO em CUCM 9.1(2) e faça o atendimento da extensão 1018 (CUCM 9.1(2)) à extensão 9898 (CUCM 10.5(2))

A fim transferir o arquivo do CLI, execute este comando:

```
admin:file get activelog platform/cli/packets.cap
```

A captação é feita no formato do padrão .cap. Este exemplo usa Wireshark para abrir o arquivo packets.cap mas toda a ferramenta do indicador da captura de pacote de informação pode ser usada.

1. O sincronizar do Transmission Control Protocol (TCP) (SYN) para estabelecer a comunicação TCP entre o CUCM 9.1(2)(Client) e o CUCM 10.5(2)(Server).
2. O CUCM 9.1(2) envia os hellos do cliente para começar a sessão TLS.
3. O CUCM 10.5(2) envia os servidores hello, o certificado de servidor, e o pedido do certificado começar o processo de intercâmbio do certificado.
4. O certificado que o cliente CUCM 9.1(2) envia para terminar a troca do certificado.

5. Os dados do aplicativo que são sinalização cifrada do SORVO, mostram que a sessão TLS esteve estabelecida.

Promova a verificação se os Certificados corretos estão trocados. Após servidores hello, o server CUCM 10.5(2) envia seu certificado ao cliente CUCM 9.1(2).

O número de série e a informação sujeita que o server CUCM 10.5(2) tem, são apresentados ao número de série do cliente CUCM 9.1(2).The, assunto, expedidor, e as datas de validez todas são comparadas à informação na página do gerenciamento certificado Admin do OS.

O server CUCM 10.5(2) apresenta seu próprio certificado para a verificação, agora ele verifica o certificado do cliente CUCM 9.1(2). A verificação acontece nos ambos sentidos.

Se há uma má combinação entre os Certificados na captura de pacote de informação e os Certificados no página da web Admin do OS, a seguir os Certificados corretos não estão transferidos arquivos pela rede.

Os Certificados corretos devem ser transferidos arquivos pela rede na página CERT Admin do OS.

Recolha traços CUCM

Os traços CUCM podem igualmente ser úteis determinar que mensagens são trocadas entre o CUCM 9.1(2) e os server CUCM 10.5(2) e mesmo se a sessão de SSL está estabelecida corretamente.

No exemplo, os traços do CUCM 9.1(2) foram recolhidos.

Fluxo de chamadas:

Ext 1018 > CUCM 9.1(2) > TRONCO do SORVO TLS > CUCM 10.5(2) > Ext 9898

Análise de dígitos ++

```
04530161.009 |19:59:21.185 |AppInfo |Digit analysis: match(pi="2", fqcn="1018",
cn="1018",plv="5", pss="", TodFilteredPss="", dd="9898",dac="0")
04530161.010 |19:59:21.185 |AppInfo |Digit analysis: analysis results
04530161.011 |19:59:21.185 |AppInfo ||PretransformCallingPartyNumber=1018
|CallingPartyNumber=1018
|DialingPartition=
|DialingPattern=9898
|FullyQualifiedCalledPartyNumber=9898
```

O SORVO TLS ++ está sendo usado na porta 5061 para este atendimento.

```
04530191.034 |19:59:21.189 |AppInfo |//SIP/SIPHandler/ccbId=0/scbId=0/SIP_PROCESS_ENQUEUE:
createConnMsg tls_security=3
04530204.002 |19:59:21.224 |AppInfo
|//SIP/Stack/Transport/0x0/sipConnectionManagerProcessConnCreated: gConnTab=0xb444c150,
addr=10.106.95.200, port=5061, connid=12, transport=TLS Over TCP
04530208.001 |19:59:21.224 |AppInfo |SIPTcp - wait_SdlSPISignal: Outgoing SIP TCP message to
10.106.95.200 on port 5061 index 12
[131,NET]
INVITE sip:9898@10.106.95.200:5061 SIP/2.0
Via: SIP/2.0/TLS 10.106.95.203:5061;branch=z9hG4bK144f49a43a
From: <sip:1018@10.106.95.203>;tag=34~4bd244e4-0988-4929-9df2-2824063695f5-19024196
```

```
To: <sip:9898@10.106.95.200>
Call-ID: 94fffc00-57415541-7-cb5f6a0a@10.106.95.203
User-Agent: Cisco-CUCM9.1
```

A mensagem SIPCertificateInd do Signal Distribution Layer ++ (SDL) fornece detalhes sobre o CN e a informação de conexão sujeitos.

```
04530218.000 |19:59:21.323 |SdlSig   |SIPCertificateInd                    |wait
                  |SIPHandler(1,100,72,1)          |SIPTcp(1,100,64,1)
|1,100,17,11.3^*^*                      |[T:N-H:0,N:1,L:0,V:0,Z:0,D:0] connIdx= 12 --
remoteIP=10.106.95.200 --remotePort = 5061 --X509SubjectName
/C=IN/ST=cisco/L=cisco/O=cisco/OU=cisco/CN=CUCM10 --Cipher AES128-SHA --SubjectAltname =
04530219.000 |19:59:21.324 |SdlSig   |SIPCertificateInd
|restart0                       |SIPD(1,100,74,16)
|SIPHandler(1,100,72,1)          |1,100,17,11.3^*^*                       |[R:N-
H:0,N:0,L:0,V:0,Z:0,D:0] connIdx= 12 --remoteIP=10.106.95.200 --remotePort = 5061 --
X509SubjectName /C=IN/ST=cisco/L=cisco/O=cisco/OU=cisco/CN=CUCM10 --Cipher AES128-SHA --
SubjectAltname =
```