SIP-TLS entre o gateway do SORVO IO e o exemplo da configuração do CallManager

Índice

Introdução
Pré-requisitos
Requisitos
Componentes Utilizados
Convenções
Configurar
Diagrama de Rede
Configurações
Transfira o certificado auto-assinado do CallManager da Cisco
Configuração de gateway do SORVO do Cisco IOS
O certificado do gateway do SORVO do Cisco IOS da transferência de arquivo pela rede a Cisco Unified CallManager
Configuração de tronco do SORVO no CallManager da Cisco
Verificar
Troubleshooting
Comandos debug
Informações Relacionadas

Introdução

Este documento contém uma configuração de exemplo para a criptografia de sinalização SIP (SIP em Segurança de camada de transporte) entre um gateway Cisco IOS® e Cisco Unified CallManager.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

- Cisco IOS gateway: Cisco 2821, Cisco IOS Software Release12.4(15)T1 com conjunto de recursos avançado dos serviços de empreendimento

- CallManager da Cisco 5.1.2

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.

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

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

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:

Configurações

Este documento utiliza as seguintes configurações:

- Transfira o certificado auto-assinado do CallManager da Cisco
- Configuração de gateway do SORVO do Cisco IOS
- Transfira arquivos pela rede o certificado do gateway do SORVO do Cisco IOS a Cisco Unified CallManager
- SORVA a configuração de tronco no CallManager da Cisco

Transfira o certificado auto-assinado do CallManager da Cisco

Conclua estes passos:

1. O log na página de administração unificada Cisco do OS no CallManager da Cisco no **endereço IP de Um ou Mais Servidores Cisco ICM NT >/platform_gui/do <ccm de https://**, e escolhe o **>** gerenciamento de certificado da **Segurança >** a **transferência Certificate/CTL**.
2. **A transferência do** clique **possui o CERT**.
3. **CallManager do** clique como o tipo do certificado existente.
4. Clique o **nome do certificado**.
5. Clique em **Continuar**.
6. Clicar com o botão direito o **link CallManager.pem**, e Savelink seleto **como a fim** transferir o certificado.

Configuração de gateway do SORVO do Cisco IOS

Configuração de gateway do SORVO IO

```
maui-soho-01#

!--- Enable IP TCP MTU Path Discovery. ip tcp path-mtu-
discovery !--- Configure NTP Server. ntp server
172.18.108.15 !--- Upload the CCM Certificate to Cisco
IOS Gateway. crypto pki trustpoint CCM-Cert enrollment
terminal revocation-check none !--- Download the Cisco
CallManager certificate, and paste !--- the contents of
the certificate, pem format. Router(config)#crypto ca
authenticate CCM-Cert Enter the base 64 encoded CA
certificate. End with a blank line or the word "quit" on
a line by itself -----BEGIN CERTIFICATE-----
MIICIjCCAYugAwIBAgIIS4xQN3bIZUowDQYJKoZIhvcNAQEFBQAwFzEV
MBMGA1UE
AxMMUlRQTVMtQ0NNLTUxMB4XDTA3MDcyMzIzMjI0OVoXDTEyMDcyMzIz
MjI0OVow
FzEVMBMGA1UEAxMMUlRQTVMtQ0NNLTUxMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCB
iQKBgQD6HIRcgDXQmO/EWosnaMBaoqjzARIR0erx31uR9WOiaZqsgRY+
Am5/E3FG
n1nJ/4NVmA45z1Q54vK0WULXgMBGANGHnBZFCNiJOiNeBfiEh1LGGMre
VTLFqKB/
lNAMtTppc0AVyYFjAAcJtZfUGxolZCanY5TWfmlwGBMIDhnqQQIDAQAB
o3cwdTAL
BgNVHQ8EBAMCArwwJwYDVR0lBCAwHgYIKwYBBQUHAwEGCCsGAQUFBwMC
BggrBgEF
BQcDBTAeBgNVHREEFzAVhhNzaXA6Q049UlRQTVMtQ0NNLTUxMB0GA1Ud
DgQWBBQr
pCXbwcRZ09AkO7V0HgHihiKpZzANBgkqhkiG9w0BAQUFAAOBgQAvNQqa
VKKoZxUD
HCBIA292qZSsOht859FY3UJkWfGD+kjlGhjgjlxEQcaJOa7pDlorzH+H
QIjFpcv6
1cl0tOdOrs2L6IAGd9e5DQ3qDwWxaB7TIsBPTkv9FLVURnKtJtVHbqjM
d+AAtsDl /DV5TbDUdre6Org1mn4uaMdrYzt1kQ== -----END
CERTIFICATE----- Certificate has the following
attributes: Fingerprint MD5: 1EF154E3 70E40379 1C7003B9
B29E111B Fingerprint SHA1: CAFA0F83 B04B2E65 71104B73
64BF6AEB ABE9EED9 % Do you accept this certificate?
[yes/no]: yes Trustpoint CA certificate accepted. %
Certificate successfully imported !--- Configure a
trustpoint in order to generate the self-signed !---
certificate of the Gateway. crypto pki trustpoint CCM-
SIP-1 enrollment selfsigned fqdn none subject-name
CN=SIP-GW revocation-check none rsakeypair CCM-SIP-1
Router(config)#crypto ca enroll CCM-SIP-1 % The fully-
qualified domain name will not be included in the
certificate % Include the router serial number in the
subject name? [yes/no]: no % Include an IP address in
the subject name? [no]: no Generate Self Signed Router
Certificate? [yes/no]: yes Router Self Signed
Certificate successfully created !— View the certificate
in PEM format, and copy the Self-signed CA certificate
!--- (output starting from “----BEGIN” to “CERTIFICATE--
---“) to a file named SIP-GW.pem Router(config)#crypto
pki export CCM-SIP-1 pem terminal % Self-signed CA
certificate: -----BEGIN CERTIFICATE-----
MIIBhDCCAS6gAwIBAgIBATANBgkqhkiG9w0BAQQFADARMQ8wDQYDVQQD
EwZTSVAt
R1cwHhcNMDcwOTA1MjAwMTA3WhcNMjAwMTAxMDAwMDAwWjARMQ8wDQYD
VQQDEwZT
SVAtR1cwXDANBgkqhkiG9w0BAQEFAANLADBIAkEAzgvQDbs9BgdrxxXW
```

```
1S/h4CZC
6JcMbBrhyO/VWOLWVe6BCFG+baJjUdYtyyvaMnlyeeVEh0/MuqCfsDo8
TvJJKwID
AQABo3EwbzAPBgNVHRMBAf8EBTADAQH/MBwGA1UdEQQVMBOCEUYzNDAu
MjguMjUt
MjgwMC0yMB8GA1UdIwQYMBaAFF6gnOpo7VY8BHL4mbSvwNxCKi62MB0G
A1UdDgQW
BBReoJzqaO1WPARy+Jm0r8DcQioutjANBgkqhkiG9w0BAQQFAANBAHhn
QS4EKcP6
IBVdtA4CM/74qCjhtsu/jciaIe90BXs56wrj7ZC4m1sIMzDAHfsl7dJl
B2IOw9Sk s980Np7dLJU= -----END CERTIFICATE----- %
General Purpose Certificate: -----BEGIN CERTIFICATE-----
MIIBhDCCAS6gAwIBAgIBATANBgkqhkiG9w0BAQQFADARMQ8wDQYDVQQD
EwZTSVAt
R1cwHhcNMDcwOTA1MjAwMTA3WhcNMjAwMTAxMDAwMDAwWjARMQ8wDQYD
VQQDEwZT
SVAtR1cwXDANBgkqhkiG9w0BAQEFAANLADBIAkEAzgvQDbs9BgdrxxXW
1S/h4CZC
6JcMbBrhyO/VWOLWVe6BCFG+baJjUdYtyyvaMnlyeeVEh0/MuqCfsDo8
TvJJKwID
AQABo3EwbzAPBgNVHRMBAf8EBTADAQH/MBwGA1UdEQQVMBOCEUYzNDAu
MjguMjUt
MjgwMC0yMB8GA1UdIwQYMBaAFF6gnOpo7VY8BHL4mbSvwNxCKi62MB0G
A1UdDgQW
BBReoJzqaO1WPARy+Jm0r8DcQioutjANBgkqhkiG9w0BAQQFAANBAHhn
QS4EKcP6
IBVdtA4CM/74qCjhtsu/jciaIe90BXs56wrj7ZC4m1sIMzDAHfsl7dJl
B2IOw9Sk s980Np7dLJU= -----END CERTIFICATE----- !---
Configure the SIP stack in the Cisco IOS GW to use the
self-signed !--- certificate of the router in order to
establish a SIP TLS connection from/to !--- Cisco
CallManager. sip-ua crypto signaling remote-addr
172.18.110.84 255.255.255.255 trustpoint CCM-SIP-1
strict-cipher !--- Configure the T1 PRI. controller T1
1/0/0 framing esf linecode b8zs pri-group timeslots 1-24
!--- Configure the ISDN switch type and incoming-voice
under the D-channel !--- interface. interface
Serial1/0/0:23 no ip address encapsulation hdlc isdn
switch-type primary-ni isdn incoming-voice voice no cdp
enable !--- Configure a POTS dial-peer that is used as
an inbound dial-peer for calls !--- that come in across
the T1 PRI line. dial-peer voice 2 pots description PSTN
PRI Circuit destination-pattern 9T incoming called-
number . direct-inward-dial port 1/0/0:23 !--- Configure
an outbound voip dial-peer in order to route calls to
the !--- Cisco CallManager. dial-peer voice 3 voip
destination-pattern 75... session protocol sipv2 session
target ipv4:172.18.110.84:5061 session transport tcp tls
dtmf-relay rtp-nte codec g711ulaw
```

O certificado do gateway do SORVO do Cisco IOS da transferência de arquivo pela rede a Cisco Unified CallManager

Conclua estes passos:

1. O log na página de administração unificada Cisco do OS no CallManager da Cisco no *endereço IP de Um ou Mais Servidores Cisco ICM NT >/platform_gui/do <ccm de https://*, e escolhe o **>** gerenciamento de certificado da **Segurança >** a **transferência de arquivo pela rede Certificate/CTL**.
2. **CERT da confiança da transferência de arquivo pela rede do** clique.

3. **CallManager-confiança do** clique.
4. Entre ou consulte ao lugar do certificado do Cisco IOS, do arquivo the.pem, e da **transferência de arquivo pela rede do** clique.
5. Verifique o resultado da transferência de arquivo pela rede.

SORVA a configuração de tronco no CallManager da Cisco

Conclua estes passos:

1. O log em Cisco unificou a página de administração do OS no CallManager no **>/ccmadmin/do** *endereço IP de Um ou Mais Servidores Cisco ICM NT do* **<ccm de https://**. Configurar um perfil de segurança do tronco do SORVO:Escolha o **perfil de segurança do perfil do >** segurança do **sistema >** do **tronco do SORVO**.Clique o botão **novo adicionar** com os parâmetros mostrados nesta figura:
2. Configurar um tronco do SORVO:Escolha o **dispositivo >** o **tronco**.Clique o botão **novo adicionar**.Selecione o **tronco do SORVO** para o `tipo de tronco`, como mostrado:
3. Configurar uma rota padrão:Escolha o **roteamento de chamada >** a **rota/caça >** a **rota padrão**.Clique o botão **novo adicionar**, como mostrado:

Verificar

Use esta seção a fim confirmar que sua configuração trabalha corretamente no gateway do SORVO do Cisco IOS.

A Output Interpreter Tool (apenas para clientes registrados) (OIT) suporta determinados comandos show. Use o OIT a fim ver uma análise do emissor de comando de execução.

- **Mostre a certificado cripto do pki CCM-SIP-1 verboso**

```
Router Self-Signed Certificate

  Status: Available

  Version: 3

  Certificate Serial Number: 0x1

  Certificate Usage: General Purpose

  Issuer:

    cn=SIP-GW

  Subject:

    Name: SIP-GW

    cn=SIP-GW

  Validity Date:

    start date: 16:01:07 EST Sep 5 2007

    end   date: 20:00:00 EST Dec 31 2019
```

```
  Subject Key Info:

    Public Key Algorithm: rsaEncryption

    RSA Public Key: (512 bit)

  Signature Algorithm: MD5 with RSA Encryption

  Fingerprint MD5: 3F9612FB C0E435F1 F445B5C4 0344E6A9

  Fingerprint SHA1: E6520255 B799818F C1067042 1A7E2EE9 4DDFD0C8

  X509v3 extensions:

    X509v3 Subject Key ID: 5EA09CEA 68ED563C 0472F899 B4AFC0DC 422A2EB6

    X509v3 Basic Constraints:

        CA: TRUE

    X509v3 Subject Alternative Name:

        F340.28.25-2800-2

    X509v3 Authority Key ID: 5EA09CEA 68ED563C 0472F899 B4AFC0DC 422A2EB6

    Authority Info Access:

  Associated Trustpoints: CCM-SIP-1
```

- Mostre a certificado cripto do pki o CCM-CERT verboso

```
CA Certificate

  Status: Available

  Version: 3

  Certificate Serial Number: 0x4B8C503776C8654A

  Certificate Usage: General Purpose

  Issuer:

    cn=RTPMS-CCM-51

  Subject:

    cn=RTPMS-CCM-51

  Validity Date:

    start date: 19:22:49 EST Jul 23 2007

    end   date: 19:22:49 EST Jul 23 2012

  Subject Key Info:

    Public Key Algorithm: rsaEncryption

    RSA Public Key: (1024 bit)

  Signature Algorithm: SHA1 with RSA Encryption
```

```
  Fingerprint MD5: 1EF154E3 70E40379 1C7003B9 B29E111B

  Fingerprint SHA1: CAFA0F83 B04B2E65 71104B73 64BF6AEB ABE9EED9

  X509v3 extensions:

    X509v3 Key Usage: BC000000

      Digital Signature

      Key Encipherment

      Data Encipherment

      Key Agreement

      Key Cert Sign

    X509v3 Subject Key ID: 2BA425DB C1C459D3 D0243BB5 741E01E2 8622A967

    X509v3 Subject Alternative Name:

    Authority Info Access:

  Associated Trustpoints: CCM-Cert
```

- Mostre o detalhe dos tls tcp da conexão sorvo-UA

```
Total active connections      : 2

No. of send failures          : 0

No. of remote closures        : 0

No. of conn. failures         : 2

No. of inactive conn. ageouts : 0

Max. tls send msg queue size of 0, recorded for 0.0.0.0:0

TLS client handshake failures : 2

TLS server handshake failures : 0


---------Printing Detailed Connection Report---------

Note:

 ** Tuples with no matching socket entry

    - Do 'clear sip <tcp[tls]/udp> conn t ipv4:<addr>:<port>'

      to overcome this error condition

 ++ Tuples with mismatched address/port entry

    - Do 'clear sip <tcp[tls]/udp> conn t ipv4:<addr>:<port>

   id <connid>' to overcome this error condition
```

```
Remote-Agent:172.18.110.84, Connections-Count:2

  Remote-Port Conn-Id Conn-State  WriteQ-Size

  =========== ======= =========== ===========

         5061       1 Established           0

        51180       2 Established           0
```

- Show call ative voice brief

```
11F0 : 7 8990160ms.1 +2670 pid:20001 Answer 7960 active

 dur 00:00:10 tx:483/83076 rx:510/81600

 Tele 1/0/0:23 (228) [1/0/0.1] tx:9660/9660/0ms g711ulaw noise:0 acom:0  i/0:0/0 dBm


11F0 : 8 8990980ms.1 +1840 pid:3 Originate 75001 active

 dur 00:00:10 tx:483/1246360336 rx:513/82080

 IP 14.50.202.26:28232 SRTP: off rtt:0ms pl:4720/1ms lost:0/0/0 delay:0/0/0ms

 g711ulaw TextRelay: off media inactive detected:n media contrl rcvd:n/a

 timestamp:n/a long duration call detected:n long duration call

 duration:n/a timestamp:n/a


Telephony call-legs: 1

SIP call-legs: 1

H323 call-legs: 0

Call agent controlled call-legs: 0

SCCP call-legs: 0

Multicast call-legs: 0

Media call-legs: 0

Total call-legs: 2
```

Troubleshooting

Esta seção fornece a informação que você pode se usar a fim pesquisar defeitos sua configuração.

Comandos debug

A Output Interpreter Tool (apenas para clientes registrados) (OIT) suporta determinados comandos show. Use o OIT a fim ver uma análise do emissor de comando de execução.

Configurar o Cisco IOS gateway para registrar debuga em seu logging buffer e desabilitam o **console de registro**.

Note: Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos **debug**.

Estes são os comandos usados a fim configurar o gateway para armazenar debugam no logging buffer:

- **service timestamps debug datetime msec**
- **preste serviços de manutenção à sequência**
- **nenhum console de registro**
- **registrando 5000000 protegidos debugar**
- **cancele o log**

Estes são os comandos usados a fim debugar a configuração neste documento:

- **debug isdn q931**
- **debug voip ccapi inout**
- **debugar o ccsip todo**
- **debugar erros do OpenSSL SSL**
- **debugar msg do OpenSSL SSL**
- **debugar estados do OpenSSL SSL**

Informações Relacionadas

- Suporte à Tecnologia de Voz
- Suporte ao Produto de Voz e Comunicações Unificadas
- Troubleshooting da Telefonia IP Cisco
- Suporte Técnico e Documentação - Cisco Systems