

Configurar o CUCM para a conexão IPSec entre Nós

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurar](#)

[Visão geral sobre a configuração](#)

[Verifique a conectividade IPSec](#)

[Verifique Certificados do IPsec](#)

[Transfira o certificado de raiz do IPsec do subscritor](#)

[Transfira arquivos pela rede o certificado de raiz do IPsec do subscritor ao editor](#)

[Configurar a política de IPsec](#)

[Verificar](#)

[Troubleshooting](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve como estabelecer a conectividade IPSec entre os Nós do gerente das comunicações unificadas de Cisco (CUCM) dentro de um conjunto.

Nota: À revelia, a conexão IPSec entre os Nós CUCM é desabilitada.

Pré-requisitos

Requisitos

Cisco recomenda que você tem o conhecimento do CUCM.

[Componentes Utilizados](#)

A informação neste documento é baseada na versão 10.5(1) CUCM.

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

Use a informação que é descrita nesta seção a fim configurar o CUCM e estabelecer a conectividade IPsec entre os Nós em um conjunto.

Visão geral sobre a configuração

Estão aqui as etapas que são envolvidas neste procedimento, cada qual é detalhado nas seções que seguem:

1. Verifique a conectividade IPsec entre os Nós.
2. Verifique os Certificados do IPsec.
3. Transfira os certificados de raiz do IPsec do nó do subscritor.
4. Transfira arquivos pela rede o certificado de raiz do IPsec do nó do subscritor ao nó do editor.
5. Configurar a política de IPsec.


Verifique a conectividade IPsec

Termine estas etapas a fim verificar a conectividade IPsec entre os Nós:


1. Registre no operating system (OS) a página de administração do server CUCM.
2. Navegue aos **serviços > ao sibilo**.
3. Especifique o endereço IP de Um ou Mais Servidores Cisco ICM NT do nó remoto.
4. Verifique a caixa de verificação do **IPsec da validação** e clique o **sibilo**.

Se não há nenhuma conectividade IPsec, a seguir você vê os resultados similares a este:

Ping Configuration

 Ping

Status

 Status: Ready

Ping Settings

Hostname or IP Address*

Ping Interval*

Packet Size*

Ping Iterations

Validate IPsec

Ping Results

IPsec connection failed..
Reasons :
a)No IPsec Policy on 10.106.110.8
b)Invalid Certificates IPsec connection failed..
Reasons :
a)No IPsec Policy on 10.106.110.8
b)Invalid Certificates

Verifique Certificados do IPsec

Termine estas etapas a fim verificar os Certificados do IPsec:

1. Registre no OS a página de administração.
2. Navegue ao > **gerenciamento de certificado da Segurança**.
3. Procure pelos Certificados do IPsec (log nos Nós da publisher e subscriber separadamente).

Nota: O certificado do IPsec do nó do subscritor não é geralmente visualizável do nó do editor; contudo, você pode ver os Certificados do IPsec do nó do editor em todos os Nós do subscritor como um certificado da IPsec-confiança.

A fim permitir a conectividade IPsec, você deve ter um certificado do IPsec de um nó ajustado como um certificado da IPsec-**confiança** no outro nó:

PUBLISHER

Certificate List (1 - 2 of 2) Rows p

Find Certificate List where Certificate begins with ipsec Find Clear Filter

Certificate	Common Name	Type	Distribution	Issued By	Expiration	Description
ipsec	cucm912pub	Self-signed	cucm912pub	cucm912pub	03/20/2019	Self-signed certificate generated by system
ipsec-trust	cucm912pub	Self-signed	cucm912pub	cucm912pub	03/20/2019	Trust Certificate

Generate Self-signed Upload Certificate/Certificate chain Download CTL Generate CSR Download CSR

IPSEC Root certificates

SUBSCRIBER

Certificate List (1 - 2 of 2) Rows

Find Certificate List where Certificate begins with ipsec Find Clear Filter

Certificate	Common Name	Type	Distribution	Issued By	Expiration	Description
ipsec	cucm10sub	Self-signed	cucm10sub	cucm10sub	12/14/2019	Self-signed certificate generated by system
ipsec-trust	cucm912pub	Self-signed	cucm912pub	cucm912pub	03/20/2019	Trust Certificate

Generate Self-signed Upload Certificate/Certificate chain Generate CSR

Certificado de raiz do IPsec da transferência do subscritor

Termine estas etapas a fim transferir o certificado de raiz do IPsec do nó do subscritor:

1. Registre no OS a página de administração do nó do subscritor.
2. Navegue ao > gerenciamento de certificado da Segurança.
3. Abra o certificado de raiz do IPsec e transfira-o no formato do .pem:

IPSEC Root certificates

SUBSCRIBER

Certificate List (1 - 2 of 2) Rows

Find Certificate List where Certificate begins with ipsec Find Clear Filter

Certificate	Common Name	Type	Distribution	Issued By	Expiration	Description
ipsec	cucm10sub	Self-signed	cucm10sub	cucm10sub	12/14/2019	Self-signed certificate generated by system
ipsec-trust	cucm912pub	Self-signed	cucm912pub	cucm912pub	03/20/2019	Trust Certificate

Generate Self-signed Upload Certificate/Certificate chain Generate CSR

Certificate Details for cucm10sub, ipsec

Regenerate Generate CSR Download .PEM File Download .DER File

Status

Status: Ready

Certificate Settings

File Name	ipsec.pem
Certificate Purpose	ipsec
Certificate Type	certs
Certificate Group	product-cpi
Description(friendly name)	Self-signed certificate generated by system

Certificate File Data

```
[
Version: V3
Serial Number: 6B71952138766EF415EFE831AEB5F943
SignatureAlgorithm: SHA1withRSA (1.2.840.113549.1.1.5)
Issuer Name: L=blr, ST=karnataka, CN=cucm10sub, OU=cucm, O=cisco, C=IN
Validity From: Mon Dec 15 23:26:27 IST 2014
          To: Sat Dec 14 23:26:26 IST 2019
Subject Name: L=blr, ST=karnataka, CN=cucm10sub, OU=cucm, O=cisco, C=IN
Key: RSA (1.2.840.113549.1.1.1)
Key value:
30818902818100a376b6ad7825abe3069a421538c851a32d815321de77791985f99f2f9a
4b695016352b98cc72b26461cc629d0d2b35fc774d20fa13ae6c476164b7ccca82eb73034
7b6ad7e5069d732468f501ba53a018f9bbe422f6c76a4e4023fbad9bcf2f7d122cbe681375
feb7adb41068344a97a4f9b224180c6f8b223f75194ec7d987b0203010001
Extensions: 3 present
]
```

Regenerate Generate CSR **Download .PEM File** Download .DER File

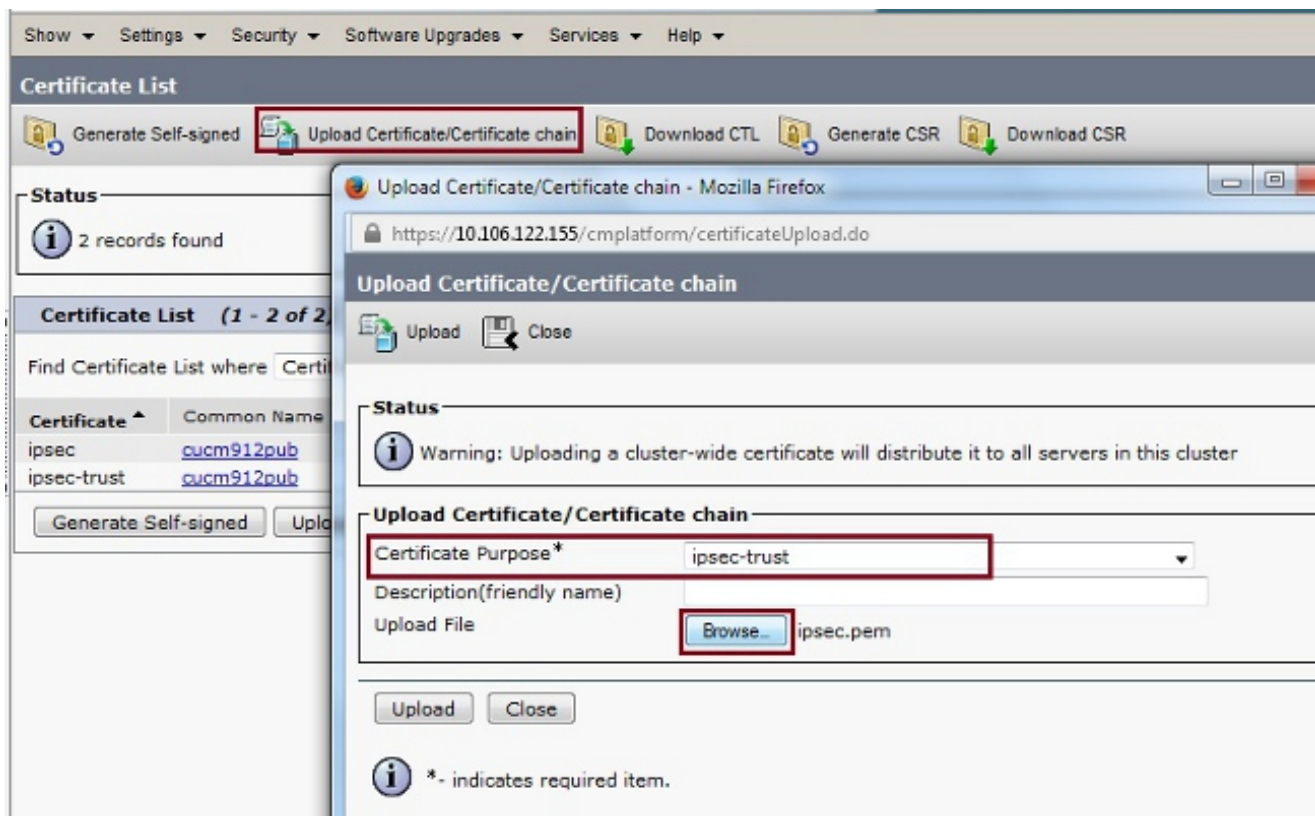
Close

Transfira arquivos pela rede o certificado de raiz do IPsec do subscritor ao editor

Termine estas etapas a fim transferir arquivos pela rede o certificado de raiz do IPsec do nó do subscritor ao nó do editor:

1. Registre no OS a página de administração do nó do editor.
2. Navegue ao > **gerenciamento de certificado da Segurança**.
3. Clique o **certificado/certificate chain da transferência de arquivo pela rede**, e transfira arquivos pela rede o certificado de raiz do IPsec do nó do subscritor como um certificado da

IPsec-confiança:



4. Depois que você transfere arquivos pela rede o certificado, verifique que o certificado de raiz do IPsec do nó do subscritor aparece como mostrado:

The screenshot shows the 'Certificate List' interface with a table of certificates. The table has columns for Certificate, Common Name, Type, Distribution, Issued By, Expiration, and Description. The 'ipsec-trust' certificate is highlighted. The 'PUBLISHER' label is visible above the table. The table contains the following data:

Certificate	Common Name	Type	Distribution	Issued By	Expiration	Description
ipsec	cucm912pub	Self-signed	cucm912pub	cucm912pub	03/20/2019	Self-signed certificate generated by system
ipsec-trust	cucm10sub	Self-signed	cucm10aub	cucm10aub	12/14/2019	Signed Certificate
ipsec-trust	cucm912pub	Self-signed	cucm912pub	cucm912pub	03/20/2019	Trust Certificate

Nota: Se você é exigido permitir a conectividade IPsec entre nós múltiplos em um conjunto, a seguir você deve transferir os certificados de raiz do IPsec para aqueles Nós também, e transfere-os arquivos pela rede ao nó do editor através do mesmo procedimento.

Configurar a política de IPsec

Termine estas etapas a fim configurar a política de IPsec:

1. Registre no OS a página de administração do editor e dos Nós do subscritor separadamente.
2. Navegue à **Segurança** > à **configuração IPsec**.
3. Use esta informação a fim configurar o IP e os detalhes certificados:

PUBLISHER : 10.106.122.155 & cucm912pub.pem

SUBSCRIBER: 10.106.122.15 & cucm10sub.pem

The screenshot shows the IPSEC Policy Configuration page for the PUBLISHER role. The page is titled "IPSEC Policy Configuration" and has a "PUBLISHER" label. It includes a "Save" button and a message: "The system is in non-FIPS Mode". The "IPSEC Policy Details" section contains the following fields:

Policy Group Name*	ToSubscriber
Policy Name*	ToSub
Authentication Method*	Certificate
Preshared Key	
Peer Type*	Different
Certificate Name*	cucm10sub.pem
Destination Address*	10.106.122.155
Destination Port*	ANY
Source Address*	10.106.122.155
Source Port*	ANY
Mode*	Transport
Remote Port*	500
Protocol*	TCP
Encryption Algorithm*	3DES
Hash Algorithm*	SHA1
ESP Algorithm*	AES 128

The "Phase 1 DH Group" section contains:

Phase One Life Time*	3600
Phase One DH*	Group 2

The "Phase 2 DH Group" section contains:

Phase Two Life Time*	3600
Phase Two DH*	Group 2

The "IPSEC Policy Configuration" section has a checked "Enable Policy" checkbox and a "Save" button.

The screenshot shows the IPSEC Policy Configuration page for the SUBSCRIBER role. The page is titled "IPSEC Policy Configuration" and has a "SUBSCRIBER" label. It includes a "Save" button and a message: "The system is in non-FIPS Mode". The "IPSEC Policy Details" section contains the following fields:

Policy Group Name*	ToPublisher
Policy Name*	ToPublisher
Authentication Method*	Certificate
Preshared Key	
Peer Type*	Different
Certificate Name*	cucm912pub.pem
Destination Address*	10.106.122.155
Destination Port*	ANY
Source Address*	10.106.122.155
Source Port*	ANY
Mode*	Transport
Remote Port*	500
Protocol*	TCP
Encryption Algorithm*	3DES
Hash Algorithm*	SHA1
ESP Algorithm*	AES 128

The "Phase 1 DH Group" section contains:

Phase One Life Time*	3600
Phase One DH*	Group 2

The "Phase 2 DH Group" section contains:

Phase Two Life Time*	3600
Phase Two DH*	Group 2

The "IPSEC Policy Configuration" section has a checked "Enable Policy" checkbox and a "Save" button.

Verificar


Termine estas etapas a fim verificar que seus trabalhos da configuração e que a conectividade IPsec entre os Nós está estabelecida:

1. Registre no OS a administração do server CUCM.
2. Navegue aos **serviços > ao sibilo**.
3. Especifique o endereço IP de Um ou Mais Servidores Cisco ICM NT do nó remoto.
4. Verifique a caixa de verificação do **IPsec da validação** e clique o **sibilo**.


Se a conectividade IPsec foi estabelecida, a seguir você vê uma mensagem similar a esta:

Show ▾ Settings ▾ Security ▾ Software Upgrades ▾ Services ▾ Help ▾

Ping Configuration

 Ping

Status

 Status: Ready

Ping Settings

Hostname or IP Address*

Ping Interval*

Packet Size*

Ping Iterations

Validate IPsec

Ping Results

Successfully validated IPsec connection to 10.106.122.159
Successfully validated IPsec connection to 10.106.122.159

Troubleshooting

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Informações Relacionadas

- [O Guia de Administração do sistema operacional das comunicações unificadas de Cisco, libera 8.6\(1\) – estabelecer uma política de IPsec nova](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)