Configure the CUCM for IPsec Connection Between Nodes

Document ID: 118928

Contributed by Ramesh Balakrishnan, Cisco TAC Engineer.
Apr 21, 2015

Contents

Introduction
Prerequisites
- Requirements
- Components Used

Configure
- Configuration Overview
- Verify IPsec Connectivity
- Check IPsec Certificates
- Download IPsec Root Certificate from Subscriber
- Upload IPsec Root Certificate from Subscriber to Publisher
- Configure IPsec Policy

Verify
Troubleshoot
Related Information

Introduction

This document describes how to establish IPsec connectivity between the Cisco Unified Communications Manager (CUCM) nodes within a cluster.

Note: By default, the IPsec connection between the CUCM nodes is disabled.

Prerequisites

Requirements

Cisco recommends that you have knowledge of the CUCM.

Components Used

The information in this document is based on the CUCM Version 10.5(1).

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. If your network is live, make sure that you understand the potential impact of any command.

Configure

Use the information that is described in this section in order to configure the CUCM and establish IPsec connectivity between the nodes in a cluster.

Configuration Overview

Here are the steps that are involved in this procedure, each of which is detailed in the sections that follow:

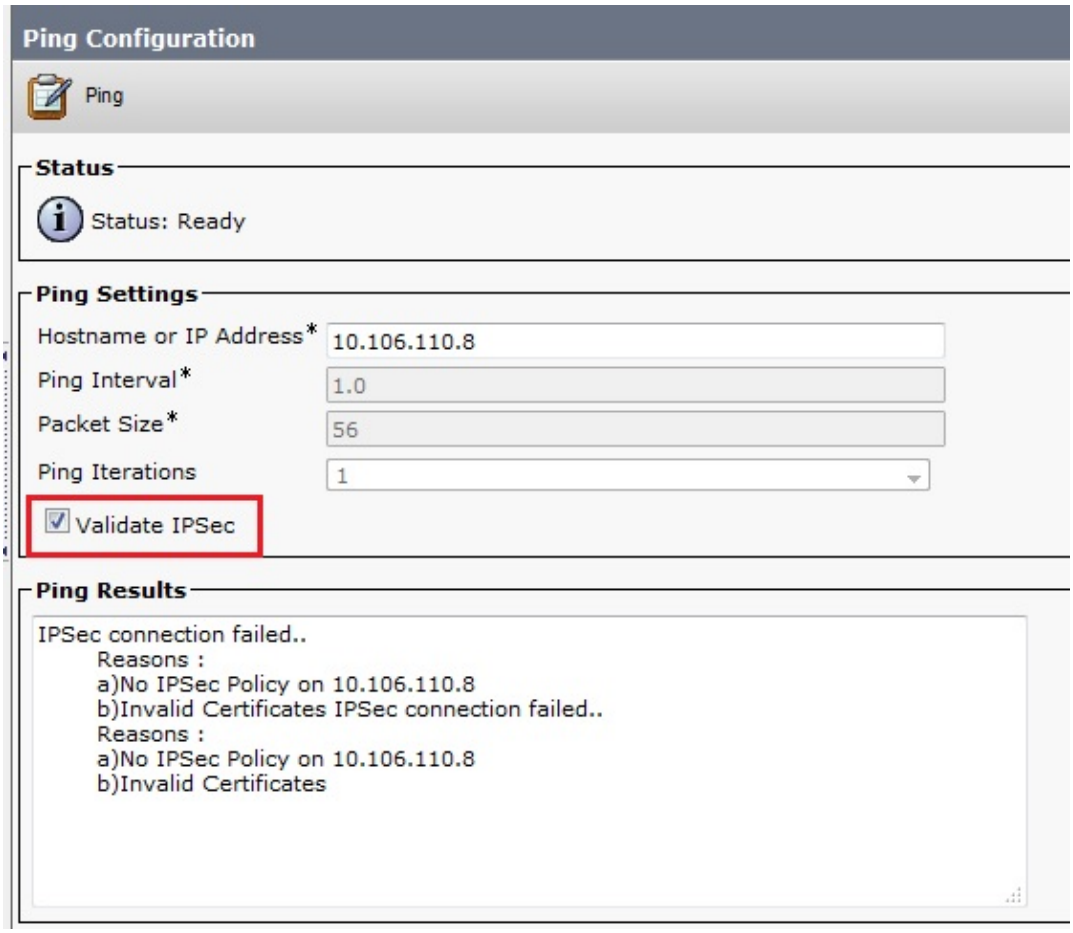
1. Verify the IPsec connectivity between the nodes.
2. Check the IPsec certificates.
3. Download the IPsec root certificates from the Subscriber node.
4. Upload the IPsec root certificate from the Subscriber node to the Publisher node.
5. Configure the IPsec policy.

Verify IPsec Connectivity

Complete these steps in order to verify the IPsec connectivity between the nodes:

1. Log into the Operating System (OS) Administration page of the CUCM server.
2. Navigate to ***Services*** > ***Ping***.
3. Specify the remote node IP address.
4. Check the ***Validate IPsec*** check box and click ***Ping***.

If there is no IPsec connectivity, then you see results similar to this:



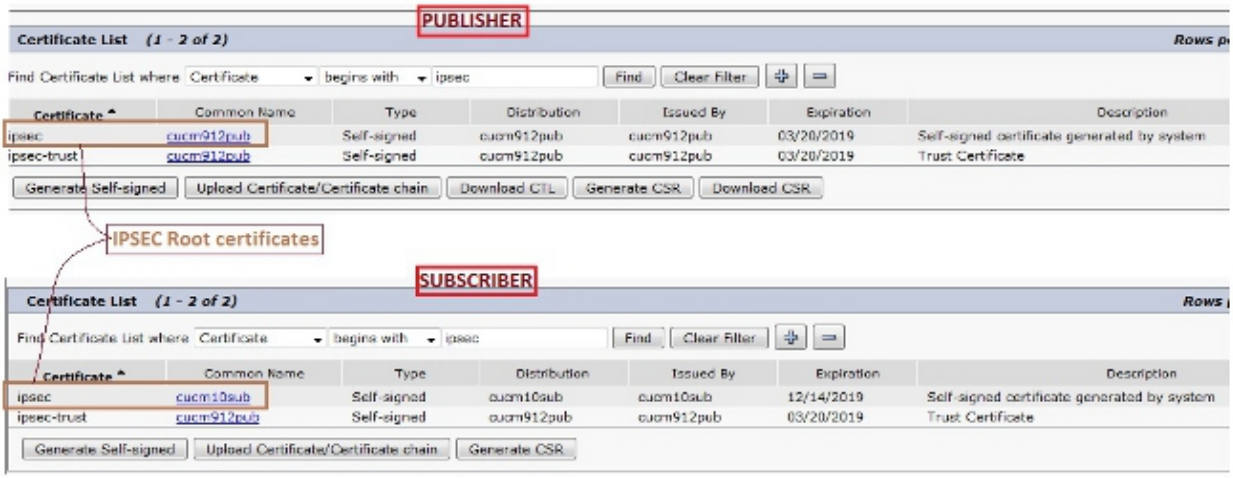
Check IPsec Certificates

Complete these steps in order to check the IPsec certificates:

1. Log into the OS Administration page.
2. Navigate to ***Security > Certificate Management***.
3. Search for the IPsec certificates (log into the Publisher and Subscriber nodes separately).

Note: The Subscriber node IPsec certificate is not usually viewable from the Publisher node; however, you can see the Publisher node IPsec certificates on all of the Subscriber nodes as an IPsec−Trust certificate.

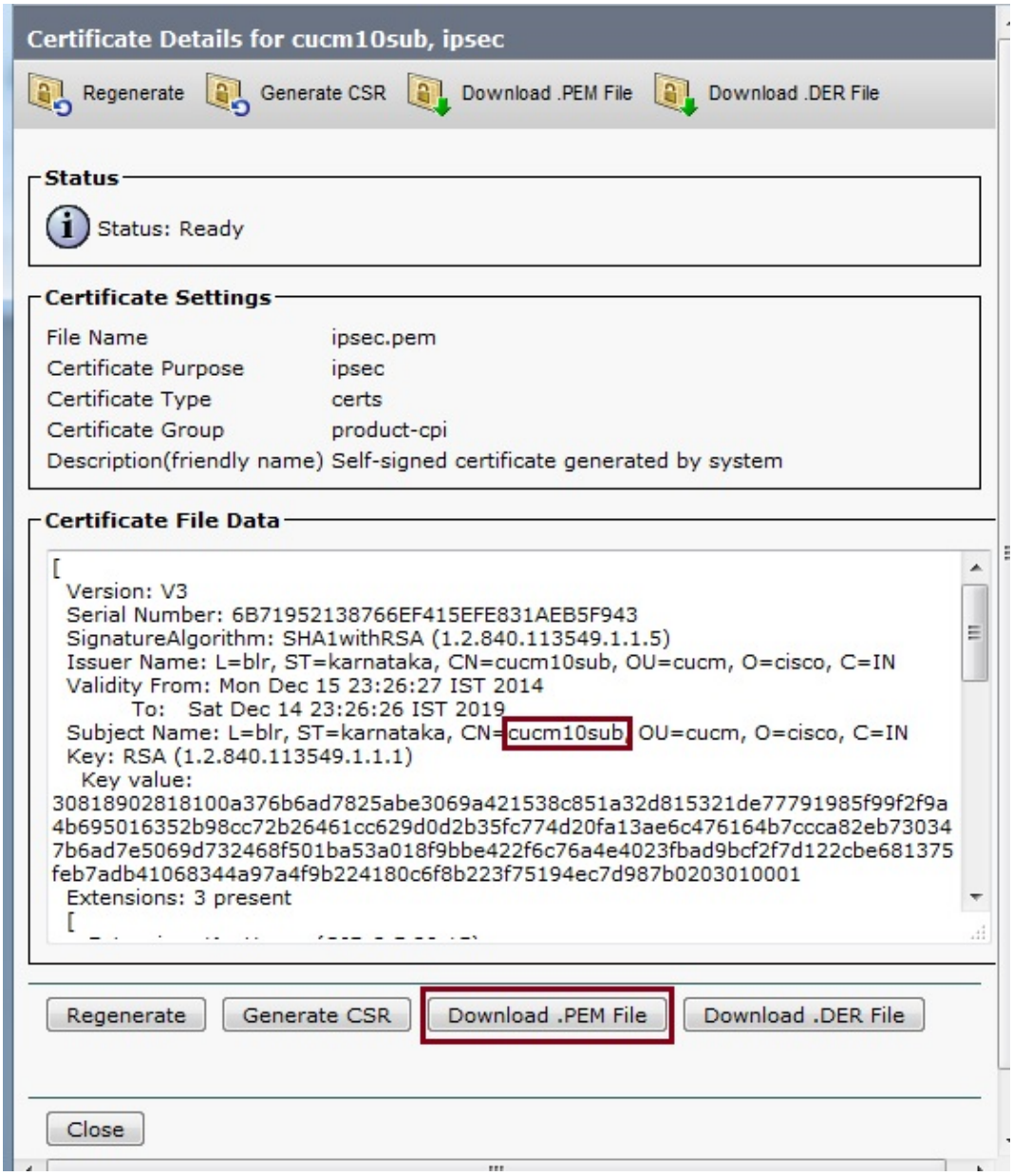
In order to enable IPsec connectivity, you must have an IPsec certificate from one node set as an ***ipsec−trust*** certificate on the other node:



Download IPsec Root Certificate from Subscriber

Complete these steps in order to download the IPsec root certificate from the Subscriber node:

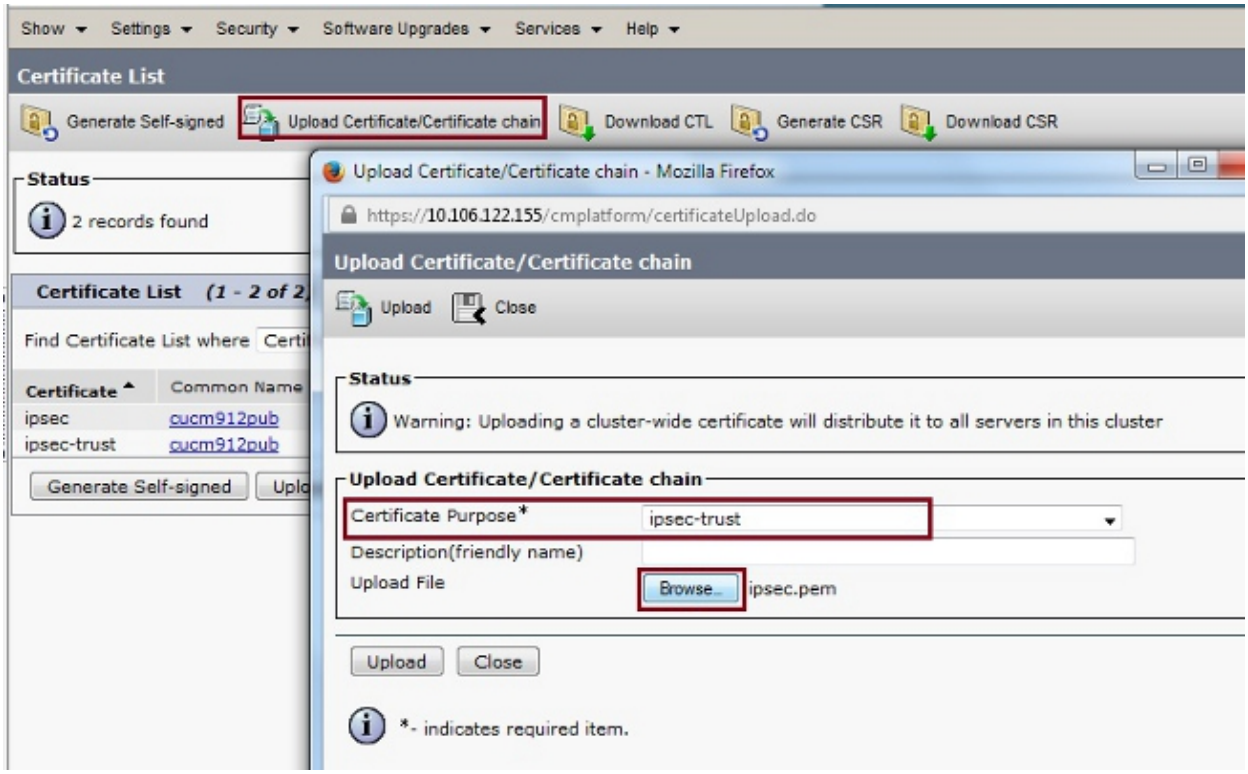
1. Log into the OS Administration page of the Subscriber node.
2. Navigate to ***Security > Certificate Management***.
3. Open the IPsec root certificate and download it in ***.pem*** format:



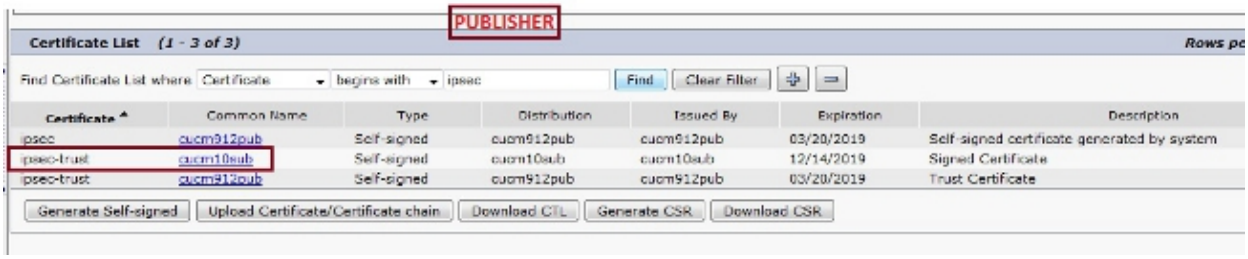
Upload IPsec Root Certificate from Subscriber to Publisher

Complete these steps in order to upload the IPsec root certificate from the Subscriber node to the Publisher node:

1. Log into the OS Administration page of the Publisher node.
2. Navigate to ***Security > Certificate Management***.
3. Click ***Upload Certificate/Certificate chain***, and upload the Subscriber node IPsec root certificate as an ***ipsec−trust*** certificate:



4. After you upload the certificate, verify that the Subscriber node IPsec root certificate appears as shown:



Note: If you are required to enable IPsec connectivity between multiple nodes in a cluster, then you must download the IPsec root certificates for those nodes as well, and upload them to the Publisher node via the same procedure.

Configure IPsec Policy

Complete these steps in order to configure the IPsec policy:

1. Log into the OS Administration page of the Publisher and the Subscriber nodes separately.

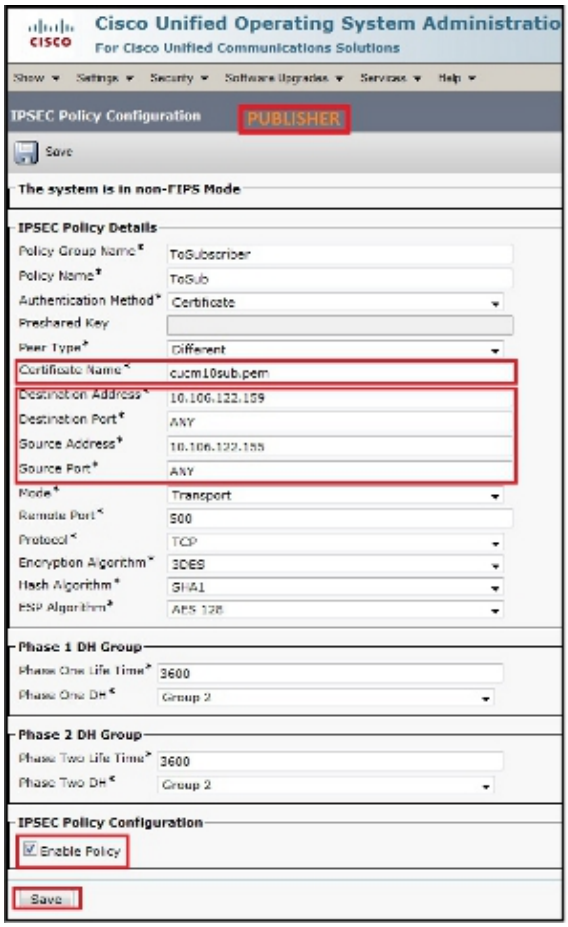
2. Navigate to ***Security > IPSEC Configuration***.

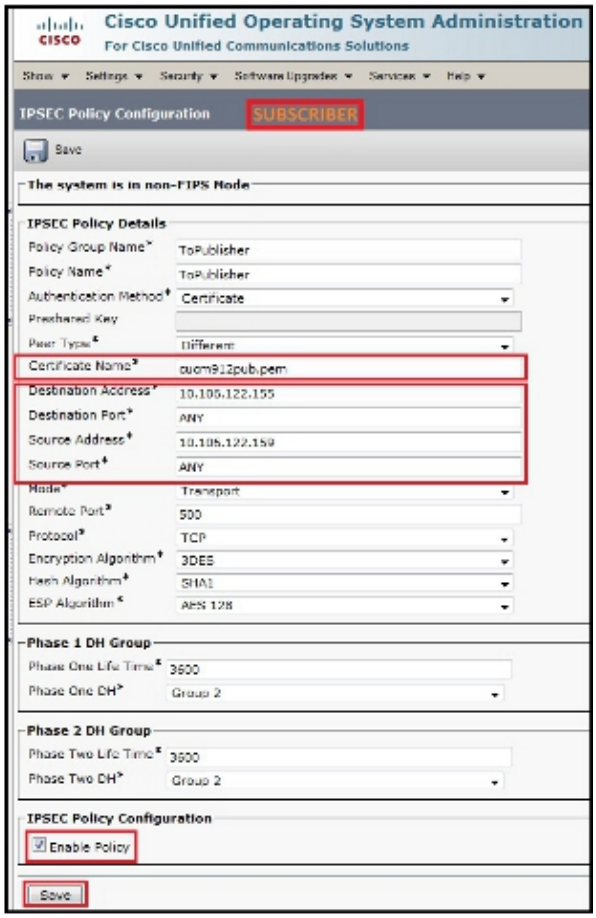
3. Use this information in order to configure the IP and certificate details:

```
*****

PUBLISHER : 10.106.122.155 & cucm912pub.pem
SUBSCRIBER: 10.106.122.15 & cucm10sub.pem

*****
```



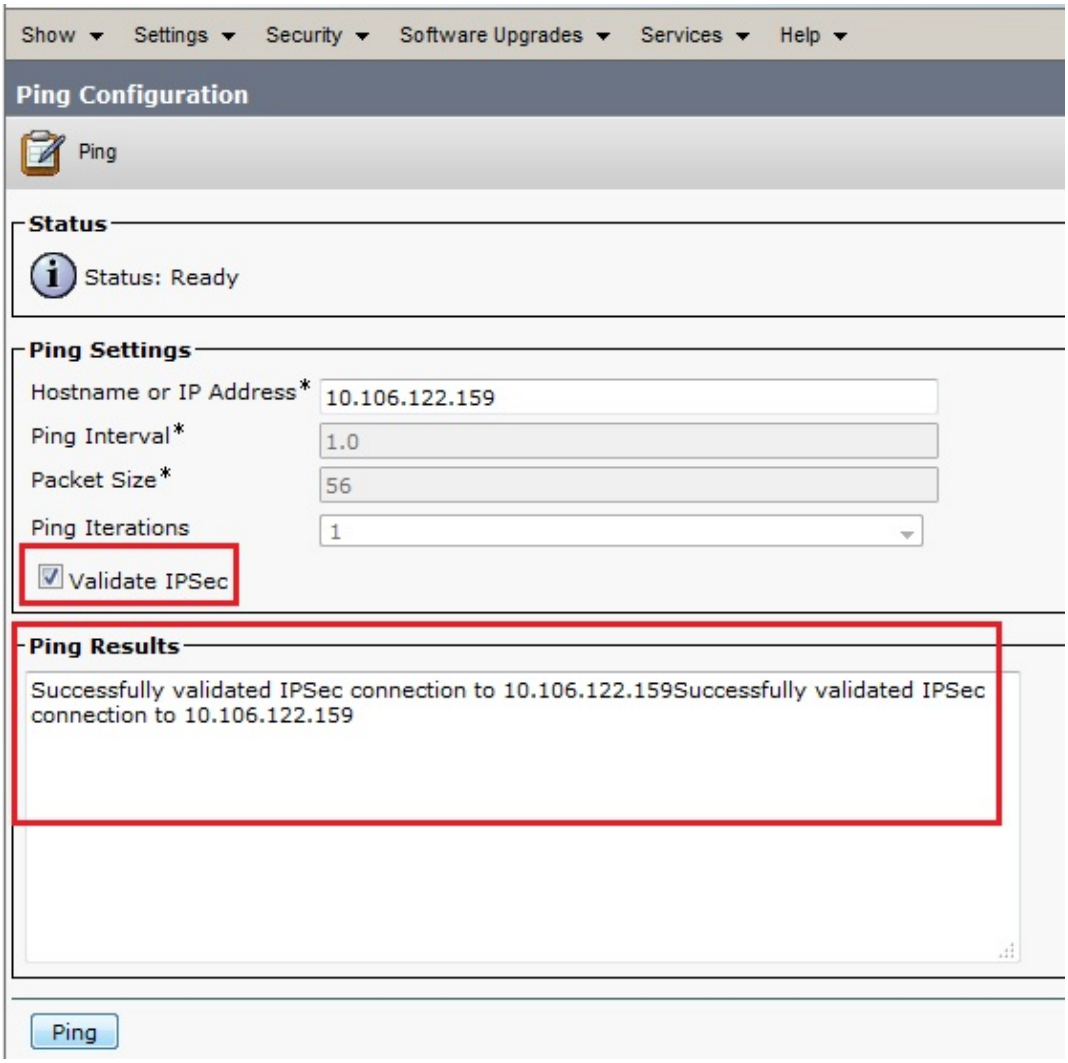


Verify

Complete these steps in order to verify that your configuration works and that the IPsec connectivity between the nodes is established:

1. Log into the OS Administration of the CUCM server.
2. Navigate to ***Services*** > ***Ping***.
3. Specify the remote node IP address.
4. Check the ***Validate IPsec*** check box and click ***Ping***.

If the IPsec connectivity has been established, then you see a message similar to this:



Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

Related Information

- ***Cisco Unified Communications Operating System Administration Guide, Release 8.6(1) Set Up a New IPsec Policy***
- ***Technical Support & Documentation − Cisco Systems***

Updated: Apr 21, 2015 Document ID: 118928