Manage IPSec Policies

IPsec Policies Overview

IPsec is a framework that ensures private, secure communications over IP networks through the use of cryptographic security services. IPsec policies are used to configure IPsec security services. The policies provide varying levels of protection for most traffic types in your network. You can configure IPsec policies to meet the security requirements of a computer, organizational unit (OU), domain, site, or global enterprise.

Configure IPsec Policies

Note

- Because any changes that you make to an IPsec policy during a system upgrade will be lost, don't modify or create IPsec policies during an upgrade.
- IPsec requires bidirectional provisioning, or one peer for each host (or gateway).
- When you provision the IPsec policy on two Unified Communications Manager nodes with one IPsec policy protocol set to “ANY” and the other IPsec policy protocol set to “UDP” or “TCP”, the validation can result in a false negative if run from the node that uses the “ANY” protocol.
- IPsec, especially with encryption, affects the performance of your system.
- After the Unified CM node reboot, if the IPsec connection isn't up, ensure that you restart the IPsec service using the command **utils ipsec restart** to establish the IPsec connection successfully. This workaround is to mitigate any issues with IPsec service restart before the network connectivity is established.

Procedure

Step 1 From Cisco Unified OS Administration, choose **Security** > **IPSec Configuration**.

Step 2 Click **Add New**.

Step 3 Configure the fields on the **IPSEC Policy Configuration** window. See the online help for more information about the fields and their configuration options.

Step 4 Click **Save**.

Step 5 (Optional) To validate IPsec, choose **Services** > **Ping**, check the **Validate IPsec** check box, and then click **Ping**.

Manage IPsec Policies

Because any changes that you make to an IPsec policy during a system upgrade are lost, do not modify or create IPsec policies during an upgrade.

Caution Any changes that you make to the existing IPsec certificate because of hostname, domain, or IP address changes require you to delete the IPsec policies and recreate them, if certificate names are changed. If certificate names are unchanged, then after importing the remote node's regenerated certificate, the IPsec policies must be disabled and enabled.

Procedure

Step 1 From Cisco Unified OS Administration, choose **Security** > **IPSEC Configuration**.

Step 2 To display, enable, or disable a policy, follow these steps:

a) Click the policy name.
b) To enable or disable the policy, check or uncheck the **Enable Policy** check box.
c) Click **Save**.
d) If you disable the policy, you must run the **utils ipsec restart** command for the disable changes to take effect.

Step 3 To delete one or more policies, follow these steps:

a) Check the check box next to each policy that you want to delete.

You can click **Select All** to select all policies or **Clear All** to clear all the check boxes.

b) Click **Delete Selected**.