IPSec Setup

IPSec 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.

IPsec Setup Within Network Infrastructures

This section does not describe how to configure IPsec. Instead, it provides considerations and recommendations for configuring IPsec in your network infrastructure. If you plan to configure IPsec in the network infrastructure and not between Unified Communications Manager and the device, review the following information before you configure IPsec:

- We recommend you to provision IPsec in the infrastructure rather than in the Unified Communications Manager itself.
- Before you configure IPsec, consider existing IPsec or VPN connections, platform CPU impact, bandwidth implications, jitter or latency, and other performance metrics.
- Review the *Voice and Video Enabled IPsec Virtual Private Networks Solution Reference Network Design Guide*.
- Review the *CiscoIOS Security Configuration Guide, Release 12.2* (or later).
- Terminate the remote end of the IPsec connection in the secure CiscoIOS MGCP gateway.
- Terminate the host end in a network device within the trusted sphere of the network where the telephony servers exist; for example, behind a firewall, access control list (ACL), or other layer three device.
- The equipment that you use to terminate the host-end IPsec connections depends on the number of gateways and the anticipated call volume to those gateways; for example, you could use Cisco VPN 3000 Series Concentrators, Catalyst 6500 IPsec VPN Services Module, or Cisco Integrated Services Routers.
- Perform the steps in the order that is specified in the topics related to setting up secure gateways and trunks.

Caution Failing to configure the IPsec connections and verify that the connections are active and may compromise privacy of the media streams.

Configure and Manage IPsec Setup Between Unified Communications Manager and Gateway or Trunks

For information on configuring IPSec between Unified Communications Manager and the gateways or trunks that are described, see the chapter "Manage IPSec Policies" in the Administration Guide for Cisco Unified Communications Manager.