CHAPTER 15

Configuring Encryption for Gateways and Trunks

This chapter contains information on the following topics:

Overview for Cisco IOS MGCP Gateway Encryption

Cisco Unified Communications Manager supports gateways that use the MGCP SRTP package, which the gateway uses to encrypt and decrypt packets over a secure RTP connection. The information that gets exchanged during call setup determines whether the gateway uses SRTP for a call. If the devices support SRTP, the system uses a SRTP connection. If at least one device does not support SRTP, the system uses a RTP connection. SRTP-to-RTP fallback (and vice versa) may occur for transfers from a secure device to a non-secure device, conferencing, transcoding, music on hold, and so on.

When the system sets up an encrypted SRTP call between two devices, Cisco Unified Communications Manager generates a master encryption key and salt for secure calls and sends them to the gateway for the SRTP stream only. Cisco Unified Communications Manager does not send the key and salt for SRTCP streams, which the gateway also supports. These keys get sent to the gateway over the MGCP signaling path, which you should secure by using IPSec. Although Cisco Unified Communications Manager does not recognize whether an IPSec connection exists, the system sends the session keys to the gateway in the clear if IPSec is not configured. Confirm that the IPSec connection exists, so the session keys get sent through a secure connection.

Tip If the MGCP gateway, which is configured for SRTP, is involved in a call with an authenticated device, for example, an authenticated phone that is running SCCP, a shield icon displays on the phone because Cisco Unified Communications Manager classifies the call as authenticated. Cisco Unified

Communications Manager classifies a call as encrypted if the SRTP capabilities for the devices are successfully negotiated for the call. If the MGCP gateway is connected to a phone that can display security icons, the phone displays the lock icon when the call is encrypted.

Overview for H.323 Gateway and H.323/H.225/H.245 Trunk Encryption

H.323 gateways and gatekeeper or non-gatekeeper controlled H.225/H.323/H.245 trunks that support security can authenticate to Cisco Unified Communications Manager if you configure an IPSec association in the Cisco Unified Communications Operating System. For information on creating an IPSec association between Cisco Unified Communications Manager and these devices, refer to the *Cisco Unified Communications Operating System Administration Guide*.

The H.323, H.225, and H.245 devices generate the encryption keys. These keys get sent to Cisco Unified Communications Manager through the signaling path, which you secure through IPSec. Although Cisco Unified Communications Manager does not recognize whether an IPSec connection exists, the session keys get sent in the clear if IPSec is not configured. Confirm that the IPSec connection exists, so the session keys get sent through a secure connection.

In addition to configuring an IPSec association, you must check the SRTP Allowed check box in the device configuration window in Cisco Unified Communications Manager Administration; for example, the H.323 Gateway, the H.225 Trunk (Gatekeeper Controlled), the Inter-Cluster Trunk (Gatekeeper Controlled), and the Inter-Cluster Trunk (Non-Gatekeeper Controlled) configuration windows. If you do not check this check box, Cisco Unified Communications Manager uses RTP to communicate with the device. If you check the check box, Cisco Unified Communications Manager allows secure and nonsecure calls to occur, depending on whether SRTP is configured for the device.

Caution If you check the SRTP Allowed check box in Cisco Unified Communications Manager Administration, Cisco strongly recommends that you configure IPSec, so security-related information does not get sent in the clear.

Cisco Unified Communications Manager does not confirm that you configured the IPSec connection correctly. If you do not configure the connection correctly, security-related information may get sent in the clear.

If the system can establish a secure media or signaling path and if the devices support SRTP, the system uses a SRTP connection. If the system cannot establish a secure media or signaling path or if at least one device does not support SRTP, the system uses a RTP connection. SRTP-to-RTP fallback (and vice versa) may occur for transfers from a secure device to a non-secure device, conferencing, transcoding, music on hold, and so on.

Tip If the call uses pass-through capable MTP, if the audio capabilities for the device match after region filtering, and if the MTP Required check box is not checked for any device, Cisco Unified Communications Manager classifies the call as secure. If the MTP Required check box is checked, Cisco Unified Communications Manager disables audio pass-through for the call and classifies the call as nonsecure. If no MTP is involved in the call, Cisco Unified Communications Manager may classify the call as encrypted, depending on the SRTP capabilities of the devices.

For SRTP-configured devices, Cisco Unified Communications Manager classifies a call as encrypted if

the SRTP Allowed check box is checked for the device and if the SRTP capabilities for the devices are successfully negotiated for the call. If the preceding criteria are not met, Cisco Unified Communications Manager classifies the call as nonsecure. If the device is connected to a phone that can display security icons, the phone displays the lock icon when the call is encrypted.

Cisco Unified Communications Manager classifies outbound faststart calls over a trunk or gateway as nonsecure. If you check the SRTP Allowed check box in Cisco Unified Communications Manager Administration, Cisco Unified Communications Manager disables the Enable Outbound FastStart check box.

Overview for SIP Trunk Encryption

SIP trunks can support secure calls both for signaling as well as media; TLS provides signaling encryption and SRTP provides media encryption.

To configure signaling encryption for the trunk, choose the following options when you configure the SIP trunk security profile (in the **System > Security Profile > SIP Trunk Security Profile** window):

- From the Device Security Mode drop-down list, choose “Encrypted.”
- From the Incoming Transport Type drop-down list, choose “TLS.”
- From the Outgoing Transport Type drop-down list, choose “TLS.”

After you configure the SIP trunk security profile, apply it to the trunk (in the **Device > Trunk > SIP Trunk** configuration window).

To configure media encryption for the trunk, check the “SRTP Allowed” check box (also in the **Device > Trunk > SIP Trunk** configuration window).

For more information about configuring the SIP Trunk security profile, see the “Configuring the SIP Trunk Security Profile” chapter.

Secure Gateway and Trunk Configuration Checklist

Use Table 15-1 in conjunction with the document, *Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways*, which provides information on how to configure your Cisco IOS MGCP gateways for security. You can obtain this document at the following URL:

http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a0080357589.html

Table 15-1 Configuration Checklist for Securing the MGCP Gateway

Configuration Steps		Related Procedures and Topics
Step 1	Verify that you installed and configured the Cisco CTL Client; verify that the cluster security mode equals Mixed Mode.	Configuring the Cisco CTL Client, page 3-1
Step 2	Verify that you configured the phones for encryption.	Phone Security Overview, page 4-1

Table 15-1 Configuration Checklist for Securing the MGCP Gateway

Configuration Steps		Related Procedures and Topics
Step 3	Configure IPSec. **Tip** You may configure IPSec in the network infrastructure, or you may configure IPSec between Cisco Unified Communications Manager and the gateway or trunk. If you implement one method to set up IPSec, you do not need to implement the other method.	• Considerations for Configuring IPSec in the Network Infrastructure, page 15-4 • Considerations for Configuring IPSec Between Cisco Unified Communications Manager and the Gateway or Trunk, page 15-5
Step 4	For H.323 IOS gateways and intercluster trunks, check the SRTP Allowed check box in Cisco Unified Communications Manager Administration.	The SRTP Allowed check box displays in the Trunk Configuration or Gateway Configuration window. For information on how to display these windows, refer to the trunk and gateway chapters in the *Cisco Unified Communications Manager Administration Guide.*
Step 5	For SIP trunks, configure the SIP trunk security profile and apply it to the trunk(s), if you have not already done so. Also, be sure to check the "SRTP Allowed" check box in the **Device > Trunk > SIP Trunk** configuration window.	• Overview for SIP Trunk Encryption, page 15-3 • Configuring the SIP Trunk Security Profile, page 16-3
Step 6	Perform security-related configuration tasks on the gateway.	• *Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways*

Considerations for Configuring IPSec in the Network Infrastructure

This document 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 Cisco Unified Communications Manager and the device, review the following information before you configure IPSec:

- Cisco recommends that you provision IPSec in the infrastructure rather than in the Cisco 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*, which you can obtain at the following URL:

  http://www.cisco.com/application/pdf/en/us/guest/netsol/ns241/c649/ccmigration_09186a00801ea79c.pdf
- Review the *Cisco IOS Security Configuration Guide, Release 12.2* (or later), which you can obtain at the following URL:

  http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_book09186a0080087df1.html
- Terminate the remote end of the IPSec connection in the secure Cisco IOS 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 "Secure Gateway and Trunk Configuration Checklist" section on page 15-3.

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

Considerations for Configuring IPSec Between Cisco Unified Communications Manager and the Gateway or Trunk

For information on configuring IPSec between Cisco Unified Communications Manager and the gateways or trunks that are described in this chapter, refer to the *Cisco Unified Communications Operating System Administration Guide*.

Configuring the SRTP Allowed Check Box

The SRTP Allowed check box displays in the following configuration windows in Cisco Unified Communications Manager Administration:

- H.323 Gateway Configuration window
- H.225 Trunk (Gatekeeper Controlled) Configuration window
- Inter-Cluster Trunk (Gatekeeper Controlled) Configuration window
- Inter-Cluster Trunk (Non-Gatekeeper Controlled) Configuration window
- SIP Trunk Configuration window

To configure the SRTP Allowed check box for H.323 gateways and gatekeeper or non-gatekeeper controlled H.323/H.245/H.225 trunks or SIP trunks, perform the following procedure:

Procedure

Step 1 Find the gateway or trunk, as described in the *Cisco Unified Communications Manager Administration Guide.*

Step 2 After you open the configuration window for the gateway/trunk, check the SRTP Allowed check box.

Step 3 Click **Save**.

Step 4 To reset the device, click **Reset**.

Step 5 Verify that you configured IPSec correctly for H323. (For SIP, make sure you configured TLS correctly.)

Additional Information

See the "Related Topics" section on page 15-6.

Where to Find More Information

Related Topics

- Authentication, Integrity, and Authorization Overview, page 1-17
- Encryption Overview, page 1-21
- Overview for Cisco IOS MGCP Gateway Encryption, page 15-1
- Overview for H.323 Gateway and H.323/H.225/H.245 Trunk Encryption, page 15-2
- Overview for SIP Trunk Encryption, page 15-3
- Secure Gateway and Trunk Configuration Checklist, page 15-3
- Considerations for Configuring IPSec in the Network Infrastructure, page 15-4
- Considerations for Configuring IPSec Between Cisco Unified Communications Manager and the Gateway or Trunk, page 15-5

Related Cisco Documentation

- *Cisco Unified Communications Operating System Administration Guide*
- *Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways*
- *Cisco IOS Security Configuration Guide, Release 12.2* (or later)
- *Voice and Video Enabled IPSec Virtual Private Networks Solution Reference Network Design Guide*