Encryption Setup for Gateways and Trunks

This chapter provides information about encryption setup for gateways and trunks.

Cisco IOS MGCP Gateway Encryption

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, Unified Communications Manager generates a master encryption key and salt for secure calls and sends them to the gateway for the SRTP stream only. 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 Unified Communications Manager does not recognize whether an IPSec connection exists, the system sends the session keys to the gateway in the cleartext 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 Unified Communications Manager classifies the call as authenticated. 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.

The following are the facts about MGCP E1 PRI gateways:

- You must configure the MGCP gateway for SRTP encryption. Configure the gateway using the following command: **mgcppackage-capabilitysrtp-package**
- The MGCP gateway must specify an Advanced IP Services or Advanced Enterprise Services image.

  For example, **c3745-adventerprisek9-mz.124-6.T.bin**
- Protected status gets exchanged with the MGCP E1 PRI gateway by using proprietary FacilityIE in the MGCP PRI Setup, Alert, and Connect messages.
- Unified Communications Manager plays the secure indication tone only to the Cisco Unified IP Phone. A PBX in the network plays the tone to the gateway end of the call.
- If the media between the Cisco Unified IP Phone and the MGCP E1 PRI gateway is not encrypted, the call drops.

Note For more information about encryption for MGCP gateways, see *Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways* for the version of Cisco IOS software that you are using.

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 Unified Communications Manager if you configure an IPSec association in the Cisco Unified Communications Operating System. For information on creating an IPSec association between Unified Communications Manager and these devices, refer to the *Administration Guide for Cisco Unified Communications Manager* .

The H.323, H.225, and H.245 devices generate the encryption keys. These keys get sent to Unified Communications Manager through the signaling path, which you secure through IPSec. Although 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 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, Unified Communications Manager uses RTP to communicate with the device. If you check the check box, 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 Unified Communications Manager Administration, Cisco strongly recommends that you configure IPSec, so security-related information does not get sent in the clear.

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, Unified Communications Manager classifies the call as secure. If the MTP Required check box is checked, Unified Communications Manager disables audio pass-through for the call and classifies the call as nonsecure. If no MTP is involved in the call, Unified Communications Manager may classify the call as encrypted, depending on the SRTP capabilities of the devices.

For SRTP-configured devices, 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, 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.

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

Unified Communications Manager allows some types of gateways and trunks to transparently pass through the shared secret (Diffie-Hellman key) and other H.235 data between two H.235 endpoints, so the two endpoints can establish a secure media channel.

To enable the passing through of H.235 data, check the **H.235 pass through allowed** check box in the configuration settings of the following trunks and gateways:

- H.225 Trunk
- ICT Gatekeeper Control
- ICT non-Gatekeeper Control
- H.323 Gateway

For information about configuring trunks and gateways, see the *Administration Guide for Cisco Unified Communications Manager* .

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 **DeviceTrunkSIP Trunk** configuration window).

Caution If you check this check box, we recommend that you use an encrypted TLS profile, so that keys and other security-related information do not get exposed during call negotiations. If you use a non- secure profile, SRTP will still work but the keys will be exposed in signaling and traces. In that case, you must ensure the security of the network between Unified Communications Manager and the destination side of the trunk.

Set Up Secure Gateways and Trunks

Use this procedure 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 CiscoIOS MGCP gateways for security.

Procedure

Step 1 Verify that you have run the **utils ctl** command to set the cluster in mixed mode.

Step 2 Verify that you configured the phones for encryption.

Step 3 Configure IPSec.

Tip You may configure IPSec in the network infrastructure, or you may configure IPSec between 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.

Step 4 For H.323 IOS gateways and intercluster trunks, check the **SRTP Allowed** check box in Unified Communications Manager.

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 Administration Guide for Cisco Unified Communications Manager.

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.

Caution If you check the **SRTP Allowed** check box, we recommend that you use an encrypted TLS profile, so that keys and other security-related information does not get exposed during call negotiations. If you use a non-secure profile, SRTP will still work but the keys will be exposed in signaling and traces. In that case, you must ensure the security of the network between Unified Communications Manager and the destination side of the trunk.

Step 6 Perform security-related configuration tasks on the gateway.

For more information, see *Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways*.

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:

- Cisco recommends that you 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.

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 in this chapter, refer to the *Administration Guide for Cisco Unified Communications Manager* .

Allow SRTP Using Unified Communications Manager Administration

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

- 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 Unified Communications Manager.

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

Caution If you check the **SRTP Allowed** check box for a SIP trunk, we recommend that you use an encrypted TLS profile, so keys and other security-related information are not exposed during call negotiations. If you use a non-secure profile, SRTP will still work but the keys will be exposed in signaling and traces. In that case, you must ensure the security of the network between Unified Communications Manager and the destination side of the trunk.

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.)

Where to Find More Information About Gateway and Trunk Encryption

- Authentication, Integrity, and Authorization
- Encryption