Media and Signaling Authentication and Encryption

The Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways feature provides support for Cisco Secure Survivable Remote Site Telephony (SRST) and voice security features that include authentication, integrity, and encryption of voice media and related call control signaling.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Media and Signaling Authentication and Encryption

Make sure that the following tasks have been completed before configuring the Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways feature:

- Cisco IOS Media Gateway Control Protocol (MGCP) is configured.

- Cisco Unified Communications Manager 4.1(2) or a later release is running.

- Cisco Secure SRST is configured on the router. For more information on configuring secure SRST on the router, refer to the document Setting up Secure SRST.
- Cisco IOS gateways have the prerequisite Cisco IOS images installed. Voice security features are delivered on Advanced IP Services or Advanced Enterprise Services images.

It is recommended that IP security (IPsec) be configured on the Cisco IOS gateway. Both software and hardware-based IPsec connections are supported.

For more information on configuring Cisco IOS-based (software) IPsec, refer to the following:

- *Cisco IOS Security Configuration Guide*, Release 12.3
- *Cisco IOS Security Command Reference*, Release 12.3

For more information on configuring hardware-based IPsec on the gateway, refer to the following books:

- *Cisco 2621 Modular Access Router with AIM-VPN/BP Security Policy*
- *Cisco 2651 Modular Access Router with AIM-VPN/BP Security Policy*
- *Cisco 3640 Modular Access Router with AIM-VPN/BP Security Policy*
- *Cisco 3660 Modular Access Router with AIM-VPN/BP Security Policy*

It is recommended that IPsec be configured on the Cisco CallManager. For more information, refer to the Microsoft Knowledge Base article " Configuring IPsec Between a Microsoft Windows 2000 Server and a Cisco Device. "

If you want to interoperate with Cisco IP phones, make sure that the following tasks have been completed before configuring the Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways feature:

- Cisco CallManager is set up for secure mode operation, and a certificate trust list (CTL) client is installed. For more information on CTL client setup, refer to Cisco IP Phone Authentication and Encryption for Cisco CallManager 4.0(1), "Authentication, Integrity and Encryption" chapter.
- The phones are configured to support secure calls if the gateways will interoperate with Cisco IP phones. For more information on Cisco IP phone configuration, refer to the following:
  - Cisco IP Phone Model 7960G and 7940G Administration Guide for Cisco CallManager Release 4.2, "Security Configuration Menu" section.
  - *Cisco IP Phone 7970 Administration Guide for Cisco CallManager, Release 4.x and later*, "Understanding Security Features for Cisco IP Phones" section.

Restrictions for Media and Signaling Authentication and Encryption

The Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways feature is supported on Cisco IOS MGCP 0.1 and Cisco IOS MGCP 1.0.

Cisco IOS MGCP SRTP support on the Cisco AS5400XM gateway is limited to the c5510 digital signal processors (DSP) series.

Cisco IOS MGCP gateways support voice security features on the following endpoints only: T1, E1, FXS, and FXO.

When a Cisco IOS MGCP voice gateway is used in conjunction with the Cisco CallManager, the automatic download feature that allows you to complete the gateway configuration on the Cisco CallManager server by downloading the configuration to that gateway through a TFTP server is not supported with voice security features.

Voice security during conferencing, transcoding, and music-on-hold is not supported.

Note If one component in the voice gateway path is not secure, the entire call falls back to nonsecure mode.

The table below provides a list of supported IP phones, gateways and network modules for voice security features.

Table 1: Supported Products for Voice Security Features

Supported Cisco IP Phones	Supported Gateways	Supported Network Modules
• Cisco IP Phone 7940 • Cisco IP Phone 7960 • Cisco IP Phone 7970	• Cisco 2600XM • Cisco 2691 • Cisco 2811 • Cisco 2821 • Cisco 2851 • Cisco 3640A • Cisco 3660 • Cisco 3700 • Cisco 3825 • Cisco 3845 • Cisco VG224 • Cisco AS5400XM	• EVM-HD • NM-HDV2 • NM-HDV2-1T1/E1 • NM-HDV2-2T1/E1 • NM-HD-1V • NM-HD-2V • NM-HD-2VE • PVDM2

Voice security features impact quality of service (QoS) as follows:

- The Secure Real-Time Transport Protocol Control Protocol (SRTCP) packet size increases by an 80-bit authentication tag, a 31-bit index field, and a 1-bit encryption flag.
- The bandwidth of Real-Time Transport Protocol (RTP) streams increases slightly with the introduction of the 32-bit authentication tag on every SRTP packet sent. Additional bandwidth is required for supported SRTP codecs as shown in the table below.

Table 2: SRTP Codec Bandwith Requirements

Codec	Packetization Period (milliseconds)	RTP Bandwidth (kbps)	SRTP Bandwidth (kbps)
G.711 mu-law, G.711 A-law	10-20	96-80	99.2-81.6
G.729, G.729A	10-220	40-9.454	43.2-9.6

Only Clear Channel, G.711, and G.729 codecs support voice security features.

Voice security features support channel density on the TI-5510 DSP as shown in the table below.

Table 3: TI -5510 DSP Channel Density

Codec	Number of Nonsecure Calls	Number of Secure Calls
Clear Channel, G.711	16	10
G.729	6	6
G.729A	8	8

Use the **codec complexity** command in voice-card configuration mode to specify secure codec complexity and call density per DSP.

Information About Media and Signaling Authentication and Encryption

Benefits of Media and Signaling Authentication and Encryption

- Provides privacy and confidentiality for voice calls
- Protects against voice security violations

Feature Design

The Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways feature implements voice security features that include signaling authentication along with media and signaling encryption on MGCP gateways.

The feature provides secure VoIP calls by addressing security requirements for privacy, integrity, and confidentiality of voice conversations. The Cisco IP telephony network establishes and maintains authenticated communications using authentication and encryption technology. Signaling authentication validates that no tampering has occurred to signaling packets during transmission.

Encryption, the process of converting clear-text data into enciphered data, provides data integrity and authentication. IPsec, a standards-based set of security protocols and algorithms, ensures that signaling information (that is, Dual Tone Multi-Frequency (DTMF) digits, passwords, personal identification numbers

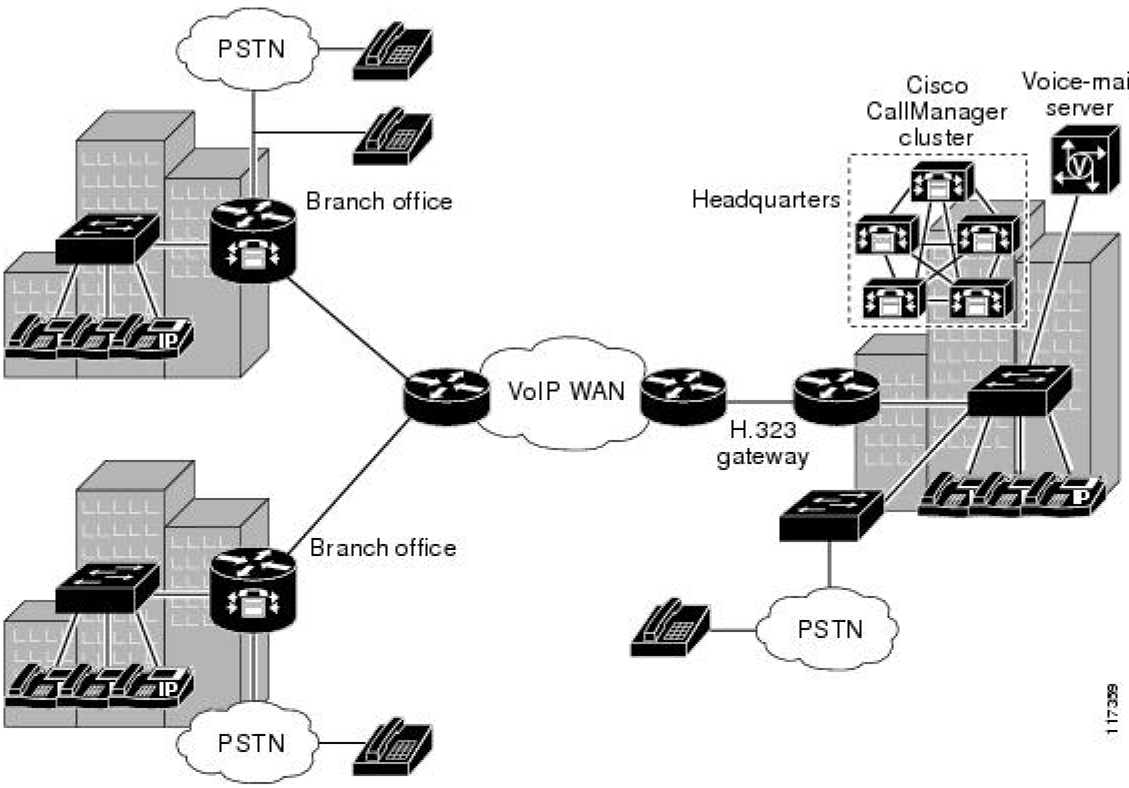
(PINs), and encryption keys) that is sent between the gateway and Cisco CallManager is encrypted. Media encryption using standards-based SRTP ensures that media streams between supported devices are secure.

Voice security features support the following capabilities between gateways and from gateways to IP phones that support the encryption feature:

- Gateway to Cisco CallManager call control authentication and encryption using IPsec
- Media encryption and authentication of voice RTP streams using SRTP
- Exchange of RTP Control Protocol (RTCP) information using SRTCP
- SRTP to RTP fallback for calls between secure and nonsecure endpoints
- Secure to clear-text fallback for new calls during SRST operation

The figure below shows a typical topology where voice security features are deployed.

Figure 1: Voice Security Features in the Telephony Network



MGCP Gateway Behavior and Voice Security Features

To implement voice security features in Cisco CallManager networks, the MGCP gateway communicates with Cisco CallManager over a secure IPsec connection that provides encryption of IP packets. To ensure that your signaling information is secure, estacblish an IPsec connection between the CallManager and the gateways, as described in the Prerequisites for Media and Signaling Authentication and Encryption, on page 1 section. You can verify that the IPsec tunnel is secure using the commands listed in the Verifying Voice Security Features, on page 13 section.

Note Although you may enable media authentication and encryption without signaling encryption, this practice is discouraged. If the gateway to Cisco CallManager connection is not secure, media keys will be sent in clear-text and your voice call will not be considered secure.

After the IPsec tunnel is established, all call control and signaling of MGCP packets between the gateway and Cisco CallManager go through the secured IPsec tunnel, with the Cisco CallManager directing the MGCP gateway to set up and tear down SRTP streams. SRTP media keys are distributed by Cisco CallManager through the secured IPsec tunnel.

Cisco implements voice security features on MGCP gateways by supporting the SRTP package and SRTP Session Description Protocol (SDP) extensions, as defined in the Internet Engineering Task Force (IETF) specifications draft-ietf-mmusic-sdescriptions-02.txt (*Security Descriptions for Media Streams* and RFC 4568, *Session Description Protocol (SDP) Security Descriptions for Media Streams*).

SRTP package capability is disabled by default. Use the Cisco IOS command-line interface (CLI) to enable the feature. For more information, see theConfiguring Voice Security Features, on page 11 section.

Cisco uses the Internet Key Exchange (IKE) standard to implement IPsec. IKE provides authentication of the IPsec peers and negotiates IPsec keys and IPsec security associations (SAs). An IPsec SA describes how two or more entities will use security services to communicate securely. For example, an IPsec SA defines the encryption algorithm, the authentication algorithm, and the shared session key to be used during the IPsec connection. Both IPsec and IKE require and use SAs to identify the parameters of their connections. IKE can negotiate and establish its own SA. The IPsec SA is established either by IKE or by manual user configuration. IKE has two phases of key negotiation: phase 1 and phase 2. Phase 1 negotiates a security association (a key) between two IKE peers. The key negotiated in phase 1 enables IKE peers to communicate securely in phase 2. During phase 2 negotiation, IKE establishes keys (security associations) for other applications, such as IPsec.

The Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways feature also implements an extended codec selection algorithm that combines selection of a codec with selection of a cryptographic suite to be used to encrypt the RTP stream. Cisco IOS Release 12.3(11)T supports the AES_CM_128_HMAC_SHA1_32 cryptographic suite, which includes the AES-128-countermode encryption algorithm and the Hashed Message Authentication Codes (HMAC) Secure Hash Algorithm1 (SHA1) authentication algorithm.

Note MGCP for SRTP on Cisco IOS gateways can be configured to use either MGCP 1.0 signaling support with the Cisco public switched telephone network (PSTN) Gateway (PGW) 2200 carrier-class call agent, or MGCP 0.1 signaling support with Cisco Unified Communications Manager.

Voice Security Features Interoperability with Endpoints

Cisco IOS MGCP gateways support voice security features on T1, E1, FXS, and FXO endpoints supported by network modules listed in *Voice Security Features Interoperability with Endpoints*, thereby enabling secure calls from analog phone to analog phone, or fax machine to fax machine. Similarly, secure calls are enabled from time- division multiplexing (TDM) endpoints or analog phones to Cisco IP phones. For a Cisco IP Phone to make and receive secure calls, all endpoints, that is, phones of all call participants, must support voice security features. If a call is nonsecure, no special icon displays on the phone. If a call is secure, the phone displays either the authenticated or encrypted call icons. For more information on secure call icons, refer to

Cisco IP Phone 7970 Administration Guide for Cisco CallManager, Release 4.x or later, "Identifying Encrypted and Authenticated Phone Calls" section.

How to Configure Media and Signaling Authentication and Encryption Feature

Installing Cisco CallManager

This task installs Cisco CallManager and configures it to work with IPsec and the Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways feature.

SUMMARY STEPS

1. Install Cisco CallManager on the server.
2. Determine the Windows OS version by going to C:\utils and double-clicking MCSVer.exe program. If you have Windows 2000.2.6sr3, no additional Windows upgrade is required. If you have Windows 2000.2.5 or a prior version, you must upgrade to Windows 2000.2.6. If you have Windows 2000.2.6, you must upgrade to Windows 2000.2.6sr3.
3. Upgrade from Windows 2000.2.5 or a prior version.
4. Upgrade from Windows 2000.2.6 to Windows 2000.2.6.sr3.
5. Upgrade Cisco CallManager to version 4.1.
6. Use the **ping** command on both the gateway and Cisco CallManager to test the connection between the gateway and Cisco CallManager. See the section, 'Configuring IPsec on Cisco CallManger'.

DETAILED STEPS

Step 1 Install Cisco CallManager on the server.

- Insert Cisco CallManager HW Detection CD version 2000.2.6, Disk1.
- When prompted, insert Cisco CallManager Base OS CD , Disk3 or 4.

Step 2 Determine the Windows OS version by going to C:\utils and double-clicking MCSVer.exe program. If you have Windows 2000.2.6sr3, no additional Windows upgrade is required. If you have Windows 2000.2.5 or a prior version, you must upgrade to Windows 2000.2.6. If you have Windows 2000.2.6, you must upgrade to Windows 2000.2.6sr3.

Step 3 Upgrade from Windows 2000.2.5 or a prior version.

- Go to 'http://www.cisco.com/cgi-bin/tablebuild.pl/cmva-3des', to download the following files:
  - win-OS-Upgrade-K9.2000-2-6.exe.
  - win-OS-Upgrade-K9.2000-2-6-Readme.htm

Follow the steps listed in the ReadMe file.

Step 4 Upgrade from Windows 2000.2.6 to Windows 2000.2.6.sr3.

- Go to 'http://www.cisco.com/cgi-bin/tablebuild.pl/cmva-3des', to download the following files:

- win-OS-Upgrade-K9.2000-2-6sr3.exe
- win-OS-Upgrade-K9.2000-2-6sr3-Readme.htm.

Follow the steps listed in the ReadMe file.

Step 5 Upgrade Cisco CallManager to version 4.1.

- Go to 'http://www.cisco.com/cgi-bin/tablebuild.pl/cmva-3des'.
- Copy CiscoCallManagerUpgrade.exe to the local system.
- Run the upgrade.

Step 6 Use the **ping** command on both the gateway and Cisco CallManager to test the connection between the gateway and Cisco CallManager. See the section, 'Configuring IPsec on Cisco CallManger'.

Configuring IPsec on Cisco CallManager

This task configures the IPsec connection between the MGCP gateway and the Cisco CallManager.

SUMMARY STEPS

1. Create an IPsec policy on the Windows 2000 server.
2. Build a filter from the Cisco CallManager to the gateway.
3. Build a filter from the gateway to the Cisco CallManager.
4. Configure a rule to negotiate tunnel security.
5. Set key exchange security methods.
6. Assign the new IPsec policy to the Windows 2000 gateway.
7. Use the **ping** command on both the gateway and Cisco CallManager to test the connection between the gateway and Cisco CallManager.
8. Run **ipsecmon.exe** on the Cisco CallManager to verify the configuration.
9. Use the **show crypto isakmp sa** command on the gateway to verify the IPsec configuration.

DETAILED STEPS

Step 1 Create an IPsec policy on the Windows 2000 server.

- Use the Microsoft Management Console (MMC) to work on the IP Security Policy Management snap-in. Click **Start**, click **Run**, and then enter **secpol.msc**.
- Right-click **IP Security Policies on Local Machine**, and then click **Create IP Security Policy**.
- Click **Next**, and then type a name for your policy.
- Clear the **Activate the default response rule** check box, and then click **Next**.
- Click **Finish**, while keeping the **Edit**check box chosen.

Step 2 Build a filter from the Cisco CallManager to the gateway.

- In the properties for the new policy created in *Configuring IPsec on Cisco CallManager*, clear the **Use Add Wizard** check box, and then click **Add** to create a new rule.
- On the IP Filter List tab, click **Add**.
- Enter an appropriate name for the filter list, clear the **Use Add Wizard** check box, and then click **Add**.
- In the Source address area, choose the option **My IP Address**from the drop-down arrow. Enter the Cisco CallManager IP address.
- In the Destination address area, click **A specific IP Subnet**from the drop-down arrow. Enter the IP address of the router interface in the same subnet as the Cisco CallManager.
- Clear the **Mirrored**check box.
- On the Protocol tab, make sure the protocol type is set to Any. (IPsec tunnels do not support protocol-specific or port-specific filters.)
- (Optional) If you want to enter a description for your filter, click the **Description**tab. It is recommended that you give the filter the same name you used for the filter list. The filter name is displayed in the IPsec monitor when the tunnel is active.
- Click **OK**, and then click **Close**.

Step 3 Build a filter from the gateway to the Cisco CallManager.

- On the IP Filter List tab, click **Add**.
- Type an appropriate name for the filter list, clear the **Use Add Wizard** check box, and then click **Add**.
- In the Source address area, click **A specific IP Subnet**from the dropdown arrow. Enter the IP address of the router interface in the same subnet as the Cisco CallManager.
- In the Destination address area, choose the option **My IP Address**from the dropdown arrow.
- Clear the **Mirrored**check box.
- (Optional) If you want to enter a description for your filter, click the **Description** tab.
- Click **OK**, and then click **Close**.

Step 4 Configure a rule to negotiate tunnel security.

- On the IP Filter List tab, click the filter list you created in *Configuring IPsec on Cisco CallManager*.
- On the Tunnel Setting tab, choose the option **Tunnel Setting - encryption peers**. For Cisco-Microsoft and for Microsoft-Cisco, configure the setting according to: http://www.cisco.com/en/US/tech/tk583/tk372/technologies_configuration_example09186a00800b12b5.shtml
- On the Connection Type tab, click **All network connections**.
- On the Filter Action tab, clear the **Use Add Wizard** check box, and then click **Add** to create a new filter action.

Note You must create a new filter; otherwise the default filter action allows incoming traffic in the clear.

- Keep the Negotiate security option enabled, and click the **Accept unsecured communication**, but clear the **always respond using IPsec** check box.

Note You must perform this step to ensure secure operation.

- Choose the **Custom** option to add a security method. Click the **Data integrity and encryption** box for Encapsulating Security Payload (ESP). Click **MD5** for the Integrity algorithm. Click **DES**for the Encryption algorithm. Check the **Generate a new Key every 3600 seconds** box.
- Click **OK**. On the General tab, enter a name for the new filter action and then click **OK**.
- Choose the filter action you created in *Configuring IPsec on Cisco CallManager*.
- On the Authentication Methods tab, perform the steps to configure a preshared key.

Note The preshared key must match the key configured on the router.

- Click **Close**.

Step 5 Set key exchange security methods.

- Right-click the IP Security Policy created in *Configuring IPsec on Cisco CallManager* and choose **Properties**.
- Click the **General** tab.
- Click the **Advanced**button.
- Click the **Methods** button.
- Ensure that the security Method with the following settings is at the top of the preference order: Type--IKE, Encryption--DES, Integrity--SHA1, Diffie-Hellman--Low(1)
- Save the configuration.

Step 6 Assign the new IPsec policy to the Windows 2000 gateway.

- In the IP Security Policies on Local Machine MMC snap-in, right-click the new policy, and then click **Assign**. A green arrow appears in the folder icon next to the new policy.

Step 7 Use the **ping** command on both the gateway and Cisco CallManager to test the connection between the gateway and Cisco CallManager.

Step 8 Run **ipsecmon.exe** on the Cisco CallManager to verify the configuration.

Step 9 Use the **show crypto isakmp sa** command on the gateway to verify the IPsec configuration.

Configuring the Cisco PGW

MGCP for SRTP on Cisco IOS gateways can be configured for use with the Cisco PSTN gateway (PGW) 2200 carrier-class call agent.

To configure this feature, you must first tell the Cisco PGW 2200 Softswitch that the media gateways support SRTP. Then you specify that SIP and TDM trunk groups support SRTP.

For a detailed description of the configuration tasks, see the "Secure Real-time Transport Protocol Support" feature guide.

Configuring Voice Security Features

This task configures voice security features on the Cisco IOS MGCP gateway.

Before you begin

We strongly recommend that you first establish an IPsec connection between the Cisco CallManager and the MGCP gateway before you use the MGCP SRTP package. Otherwise, media keys will be sent in clear text and your voice call will not be considered secure. For more information, see the "Installing Cisco CallManager, on page 7" and "Configuring IPsec on Cisco CallManager, on page 8" sections.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mgcp package-capability srtp-package**
4. **mgcp validate call-agent source-ipaddr**
5. **mgcp crypto rfc-preferred**
6. **voice-card** *slot*
7. **codec complexity secure**
8. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**mgcp package-capability srtp-package** **Example:** `Router(config)# mgcp package-capability srtp-package`	Enables the MGCP gateway capability to process SRTP packages.
Step 4	**mgcp validate call-agent source-ipaddr** **Example:** `Router(config)# mgcp validate call-agent source-ipaddr`	(Optional) Enables MGCP application validation that packets received are sent by a configured call agent.
Step 5	**mgcp crypto rfc-preferred** **Example:**	(Optional) Enables support for the media-level SDP a=crypto attribute on the Cisco IOS MGCP gateway.

	Command or Action	Purpose
	`Router(config)# mgcp crypto rfc-preferred`	
Step 6	**voice-card** *slot* **Example:** `Router(config)# voice-card 1`	Enters voice-card configuration mode and configures the voice card in the specified network module slot.
Step 7	**codec complexity secure** **Example:** `Router(config-voice-card)# codec complexity secure`	Restricts the number of channels per NM-HDV network module from four to two, enabling SRTP support on the TI-549 DSP. **Note** You need not specify secure codec complexity for TI-5510 DSPs, which support SRTP capability in all complexity modes.
Step 8	**exit** **Example:** `Router(config-voice-card)# exit`	Exits the current configuration mode.

Configuring Secure IP Telephony Calls

This task enables secure IP telephony calls from gateway to IP phone.

Voice security features use digital certificates contained in eTokens for device authentication. This process validates the identity of a device and ensures that the entity is who it claims to be. Device authentication occurs between the Cisco CallManager server and supported IP phones when each entity accepts the certificate of the other entity. Cisco implements device authentication using the CTL feature on the Cisco CallManager. The CTL Client creates a certificate on each server in the cluster and generates a CTL file in the TFTP Path of the server for the phones to download. This file provides the IP phone with a list of certified hosts that it can trust. For more information, refer to *Cisco IP Phone Authentication and Encryption for Cisco CallManager 4.0(1)*, "Signaling Authentication" chapter .

Before you begin

- CTL Provider service must be running on the Cisco CallManager server.
- Smart Card service must be running on the Cisco CallManager server.
- Two USB eTokens are required.

SUMMARY STEPS

1. Install CiscoCTLClient.exe from c:\CiscoPlugins\Client\.
2. Launch Cisco CTL Client from the desktop shortcut.
3. Enter the Cisco CallManager IP address and password, then click **Next**.
4. Choose **Set CallManager Cluster to Secure Mode**, then click **Next**.
5. Click **Add** for Security Token Information.

6. Click **Add Tokens**for CTL Entries.
7. When prompted, insert the first USB eToken, then click **OK**.
8. Repeat and *Configuring Secure IP Telephoney Calls* for the second eToken.
9. Click **Finish** for CTL Entries, then enter your eToken Password when prompted and click **OK**.
10. Verify that voice security features are enabled.

DETAILED STEPS

Step 1 Install CiscoCTLClient.exe from c:\CiscoPlugins\Client\.

Step 2 Launch Cisco CTL Client from the desktop shortcut.

Step 3 Enter the Cisco CallManager IP address and password, then click **Next**.

Step 4 Choose **Set CallManager Cluster to Secure Mode**, then click **Next**.

Step 5 Click **Add** for Security Token Information.

Step 6 Click **Add Tokens**for CTL Entries.

Step 7 When prompted, insert the first USB eToken, then click **OK**.

Step 8 Repeat and *Configuring Secure IP Telephoney Calls* for the second eToken.

Step 9 Click **Finish** for CTL Entries, then enter your eToken Password when prompted and click **OK**.

Step 10 Verify that voice security features are enabled.

- Open Cisco CallManager Administration, choose **Access System**, then **Enterprise Parameters**. Scroll down to Security Parameters, and verify that Cluster Security is set to 1.
- Set the Cisco CallManager Enterprise Parameter to **Encrypted**to force all devices in the cluster to run encrypted mode. You can also set each IP phone individually to encrypted mode by choosing **Device**, then **Phone**, then **Find**, then **Security Mode = Encrypted**. Reboot the IP phones and verify that the Security Mode displays Encrypted under Security Settings.

Verifying Voice Security Features

This task verifies voice security feature configuration and MGCP gateway to Cisco CallManager IPsec connections.

SUMMARY STEPS

1. **show mgcp**
2. **show mgcp connection**
3. **show mgcp srtp** {**summary**| **detail** [*endpoint*]}
4. **show mgcp statistics**
5. **show call active voice**
6. **show voice call** *port*
7. **show voice call status**
8. **show voice call status** *call-id*
9. **show voice dsp**
10. **show rtpspi call**

11. **show rtpspi statistics**
12. **show ccm-manager**
13. **show crypto engine accelerator statistic**
14. **show crypto ipsec sa**
15. **show crypto isakmp sa**
16. **show crypto session**
17. **show crypto session detail**

DETAILED STEPS

Step 1 **show mgcp**

Use this command to display the state of the **mgcp package-capability srtp-package** and **mgcp validate call-agent source-ipaddr** commands.

Example:

```
Router# show mgcp
MGCP Admin State ACTIVE, Oper State ACTIVE - Cause Code NONE
MGCP call-agent: 10.7.0.200 Initial protocol service is MGCP 0.1
```

The following line shows that call-agent validation is enabled:

Example:

```
MGCP validate call-agent source-ipaddr ENABLED
MGCP block-newcalls DISABLED
MGCP send SGCP RSIP: forced/restart/graceful/disconnected DISABLED
MGCP quarantine mode discard/step
MGCP quarantine of persistent events is ENABLED
MGCP dtmf-relay for VoIP disabled for all codec types
MGCP dtmf-relay for VoAAL2 disabled for all codec types
MGCP voip modem passthrough disabled
MGCP voaal2 modem passthrough disabled
MGCP voip modem relay: Disabled.
MGCP TSE payload: 100
MGCP T.38 Named Signalling Event (NSE) response timer: 200
MGCP Network (IP/AAL2) Continuity Test timer: 200
MGCP 'RTP stream loss' timer disabled
MGCP request timeout 500
MGCP maximum exponential request timeout 4000
MGCP gateway port: 2427, MGCP maximum waiting delay 3000
MGCP restart delay 0, MGCP vad DISABLED
MGCP rtrcac DISABLED
MGCP system resource check DISABLED
MGCP xpc-codec: DISABLED, MGCP persistent hookflash: DISABLED
MGCP persistent offhook: ENABLED, MGCP persistent onhook: ENABLED
MGCP piggyback msg DISABLED, MGCP endpoint offset DISABLED
MGCP simple-sdp ENABLED
MGCP undotted-notation DISABLED
MGCP codec type g711ulaw, MGCP packetization period 20
MGCP JB threshold lwm 30, MGCP JB threshold hwm 150
MGCP LAT threshold lwm 150, MGCP LAT threshold hwm 300
MGCP PL threshold lwm 1000, MGCP PL threshold hwm 10000
MGCP CL threshold lwm 1000, MGCP CL threshold hwm 10000
MGCP playout mode is adaptive 60, 4, 200 in msec
MGCP Fax Playout Buffer is 300 in msec
```

```
MGCP media (RTP) dscp: ef, MGCP signaling dscp: af31
MGCP default package: line-package
```

The following lines show that the **srtp-package**command is enabled:

Example:

```
MGCP supported packages: gm-package dtmf-package mf-package trunk-package
         line-package ms-package dt-package mo-package mt-package
         sst-package fxr-package srtp-package
MGCP Digit Map matching order: shortest match
SGCP Digit Map matching order: always left-to-right
MGCP VoAAL2 ignore-lco-codec DISABLED
MGCP T.38 Fax is ENABLED
MGCP T.38 Fax ECM is ENABLED
MGCP T.38 Fax NSF Override is DISABLED
MGCP T.38 Fax Low Speed Redundancy: 0MGCP T.38 Fax High Speed Redundancy: 0
MGCP control bound to interface FastEthernet0/0
MGCP media bind :DISABLED
MGCP Upspeed payload type for G711ulaw: 0,  G711alaw: 8
MGCP Dynamic payload type for G.726-16K codec
MGCP Dynamic payload type for G.726-24K codec
MGCP Dynamic payload type for G.Clear codec
```

Step 2 **show mgcp connection**

Use this command to display information on active connections, including the encryption suite.

Example:

```
Router# show mgcp connection
Endpoint        Call_ID(C) Conn_ID(I) (P)ort (M)ode (S)tate (CO)dec (E)vent[SIFL] (R)esult[EA]
Encryption(K)
```

The following line shows that encryption status is enabled, K=1.

Example:

```
1. S1/DS1-0/1   C=2,1,2  I=0x2  P=18204,0  M=2  S=4,4 CO=1 E=0,0,0,0  R=0,0 K=1
```

Step 3 **show mgcp srtp** {**summary**| **detail** [*endpoint*]}

Use this command to display SRTP connections and validate master keys and salts for endpoints.

Example:

```
Router# show mgcp srtp summary
MGCP SRTP Connection Summary
Endpoint             Conn Id    Crypto Suite
aaln/S3/SU0/0        8          AES_CM_128_HMAC_SHA1_32
aaln/S3/SU0/1        9          AES_CM_128_HMAC_SHA1_32
S3/DS1-0/1           6          AES_CM_128_HMAC_SHA1_32
S3/DS1-0/2           7          AES_CM_128_HMAC_SHA1_32
4 SRTP connections active
Router# show mgcp srtp detail
MGCP SRTP Connection Detail for Endpoint *
Definitions: CS=Crypto Suite, KS=HASHED Master Key/Salt, SSRC=Syncronization Source, ROC=Rollover
Counter, KDR=Key Derivation Rate, SEQ=Sequence Number, FEC=FEC Order, MLT=Master Key Lifetime,
MKI=Master Key Index:MKI Size
Endpoint aaln/S3/SU0/0 Call ID 2 Conn ID 8
  Tx:CS=AES_CM_128_HMAC_SHA1_32 KS=3NaOYXS9dLoYDaBHpzRejREfhf0= SSRC=Random ROC=0 KDR=1 SEQ=Random
 FEC=FEC->SRTP MLT=0x80000000 MKI=0:0
  Rx:CS=AES_CM_128_HMAC_SHA1_32 KS=llYCQoqxtxtdf7ECe+x+DK+G9v4= SSRC=Random ROC=0 KDR=1 SEQ=Random
```

```
 FEC=FEC->SRTP MLT=0x80000000 MKI=0:0
Endpoint aaln/S3/SU0/1 Call ID 101 Conn ID 9
  Tx:CS=AES_CM_128_HMAC_SHA1_32 KS=l1YCQoqxtxtdf7ECe+x+DK+G9v4= SSRC=Random ROC=0 KDR=1 SEQ=Random
 FEC=FEC->SRTP MLT=0x80000000 MKI=0:0
  Rx:Not Configured
Endpoint S3/DS1-0/1 Call ID 1 Conn ID 6
  Tx:CS=AES_CM_128_HMAC_SHA1_32 KS=3NaOYXS9dLoYDaBHpzRejREfhf0= SSRC=Random ROC=0 KDR=1 SEQ=Random
 FEC=FEC->SRTP MLT=0x80000000 MKI=0:0
  Rx:CS=AES_CM_128_HMAC_SHA1_32 KS=l1YCQoqxtxtdf7ECe+x+DK+G9v4= SSRC=Random ROC=0 KDR=1 SEQ=Random
 FEC=FEC->SRTP MLT=0x80000000 MKI=0:0
Endpoint S3/DS1-0/2 Call ID 100 Conn ID 7
  Tx:CS=AES_CM_128_HMAC_SHA1_32 KS=l1YCQoqxtxtdf7ECe+x+DK+G9v4= SSRC=Random ROC=0 KDR=1 SEQ=Random
 FEC=FEC->SRTP MLT=0x80000000 MKI=0:0
  Rx:Not Configured
4 SRTP connections displayed
Router# show mgcp srtp detail S3/DS1-0/*
MGCP SRTP Connection Detail for Endpoint S3/DS1-0/*
Definitions: CS=Crypto Suite, KS=HASHED Master Key/Salt, SSRC=Syncronization Source, ROC=Rollover
Counter, KDR=Key Derivation Rate, SEQ=Sequence Number, FEC=FEC Order, MLT=Master Key Lifetime,
MKI=Master Key Index:MKI Size
```

The following lines allow you to compare and validate a hashed version of the master key and salt, as indicated by the KS field, without the display revealing the actual master key and salt.

Example:

```
Endpoint S3/DS1-0/1 Call ID 1 Conn ID 6
  Tx:CS=AES_CM_128_HMAC_SHA1_32 KS=3NaOYXS9dLoYDaBHpzRejREfhf0= SSRC=Random ROC=0 KDR=1 SEQ=Random
 FEC=FEC->SRTP MLT=0x80000000 MKI=0:0
  Rx:CS=AES_CM_128_HMAC_SHA1_32 KS=l1YCQoqxtxtdf7ECe+x+DK+G9v4= SSRC=Random ROC=0 KDR=1 SEQ=Random
 FEC=FEC->SRTP MLT=0x80000000 MKI=0:0
Endpoint S3/DS1-0/2 Call ID 100 Conn ID 7
  Tx:CS=AES_CM_128_HMAC_SHA1_32 KS=l1YCQoqxtxtdf7ECe+x+DK+G9v4= SSRC=Random ROC=0 KDR=1 SEQ=Random
 FEC=FEC->SRTP MLT=0x80000000 MKI=0:0
  Rx:Not Configured
2 SRTP connections displayed
```

Step 4 **show mgcp statistics**

Use this command to display statistics, including dropped packets from unconfigured call agents.

Example:

```
Router# show mgcp statistics
 UDP pkts rx 0, tx 0
 Unrecognized rx pkts 0, MGCP message parsing errors 0
 Duplicate MGCP ack tx 0, Invalid versions count 0
```

The following line shows the number of dropped packets from unconfigured call agents.

Example:

```
 rx pkts from unknown Call Agent 0
 CreateConn rx 0, successful 0, failed 0
 DeleteConn rx 0, successful 0, failed 0
 ModifyConn rx 0, successful 0, failed 0
 DeleteConn tx 0, successful 0, failed 0
 NotifyRequest rx 0, successful 0, failed 0
 AuditConnection rx 0, successful 0, failed 0
 AuditEndpoint rx 0, successful 0, failed 0
 RestartInProgress tx 0, successful 0, failed 0
 Notify tx 0, successful 0, failed 0
 ACK tx 0, NACK tx 0
```

```
 ACK rx 0, NACK rx 0
 IP address based Call Agents statistics:
 No Call Agent message.
 System resource check is DISABLED. No available statistic
```

Step 5 **show call active voice**

Use this command to display encryption statistics.

Example:

```
Router# show call active voice
GENERIC: SetupTime=21072 Index=0 PeerAddress= PeerSubAddress= PeerId=0
PeerIfIndex=0 LogicalIfIndex=0 ConnectTime=0 CallState=3 CallSecurity = On CallOrigin=2 ChargedUnits=0

InfoType=0 TransmitPackets=375413 TransmitBytes=7508260 ReceivePackets=377734
ReceiveBytes=7554680
VOIP: ConnectionId[0x19BDF910 0xAF500007 0x0 0x58ED0] RemoteIPAddress=17635075
RemoteUDPPort=16394 RoundTripDelay=0 SelectedQoS=0 SessionProtocol=1
SessionTarget= OnTimeRvPlayout=0 GapFillWithSilence=0 GapFillWithPrediction=600
GapFillWithInterpolation=0 GapFillWithRedundancy=0 HiWaterPlayoutDelay=110
LoWaterPlayoutDelay=64 ReceiveDelay=94 VADEnable=0 CoderTypeRate=0
GENERIC: SetupTime=21072 Index=1 PeerAddress=+14085271001 PeerSubAddress=
PeerId=0 PeerIfIndex=0 LogicalIfIndex=5 ConnectTime=21115 CallState=4 CallOrigin=1
ChargedUnits=0 InfoType=1 TransmitPackets=377915 TransmitBytes=7558300
ReceivePackets=375594 ReceiveBytes=7511880 TotalPacketsEncrypted=375594
```

The following lines show statistics for encrypted and decrypted packets.

Example:

```
TotalPacketsDecrypted=375594 DecryptionFailurePacketCount=0 TotalPacketsAuthenticated=375594
AuthenticationFailurePacketCount=0 DuplicateReplayPacketCount=0 OutsideWindowReplayPacketCount=0
TELE: ConnectionId=[0x19BDF910 0xAF500007 0x0 0x58ED0] TxDuration=16640
VoiceTxDuration=16640 FaxTxDuration=0 CoderTypeRate=0 NoiseLevel=0 ACOMLevel=4
OutSignalLevel=-440 InSignalLevel=-440 InfoActivity=2 ERLLevel=227
SessionTarget=
```

Step 6 **show voice call** *port*

Use this command to display SRTP statistics.

Example:

```
Router# show voice call 1/0/0
1/0/0
      vtsp level 0 state = S_CONNECTvpm level 1 state = FXSLS_CONNECT
vpm level 0 state = S_UP
calling number , calling name unavailable, calling time 01/08 03:44
c3745_13#       ***DSP VOICE TX STATISTICS***
Tx Vox/Fax Pkts: 108616, Tx Sig Pkts: 0, Tx Comfort Pkts: 0
Tx Dur(ms): 2172320, Tx Vox Dur(ms): 2172320, Tx Fax Dur(ms): 0
        ***DSP VOICE RX STATISTICS***
Rx Vox/Fax Pkts: 108602, Rx Signal Pkts: 0, Rx Comfort Pkts: 0
Rx Dur(ms): 2172320, Rx Vox Dur(ms): 2171990, Rx Fax Dur(ms): 0
Rx Non-seq Pkts: 3, Rx Bad Hdr Pkts: 0
Rx Early Pkts: 0, Rx Late Pkts: 0
        ***DSP VOICE VP_DELAY STATISTICS***
Clk Offset(ms): -2819596, Rx Delay Est(ms): 65
Rx Delay Lo Water Mark(ms): 65, Rx Delay Hi Water Mark(ms): 65
        ***DSP VOICE VP_ERROR STATISTICS***
Predict Conceal(ms): 250, Interpolate Conceal(ms): 0
Silence Conceal(ms): 0, Retroact Mem Update(ms): 0
```

```
Buf Overflow Discard(ms): 0, Talkspurt Endpoint Detect Err: 0
        ***DSP LEVELS***
TDM Bus Levels(dBm0): Rx -37.7 from PBX/Phone, Tx -35.5 to PBX/Phone
TDM ACOM Levels(dBm0): +5.0, TDM ERL Level(dBm0): +5.0
TDM Bgd Levels(dBm0): -35.9, with activity being silence
        ***DSP VOICE ERROR STATISTICS***
Rx Pkt Drops(Invalid Header): 0, Tx Pkt Drops(HPI SAM Overflow): 0
        ***DSP VOICE SRTP STATISTICS***
```

The following lines show voice SRTP statistics.

Example:

```
*Jan  8 2004 04:21:01.743 PAT: TotalPacketsEncrypted: 108616  TotalPacketsDecrypted: 108602
DecryptionFailurePacketCount: 0  TotalPacketsAuthenticated: 108602
AuthenticationFailurePacketCount: 0 DuplicateReplayPacketCount: 0
OutsideWindowReplayPacketCount: 0  packetsBadReceivedSSRC: 0
```

Note When a T.38 fax call (nonsecure) is attempted and the fax call goes through, then switches back to secure voice (SRTP) mode, output for the **show voice call** *port* command displays an authentication failure packet count of 20. This is a normal occurrence and should not affect voice quality. The authentication failure packet count occurs because the gateways do not switch back to secure voice at the same time; that is, one side of the call is in SRTP voice mode for a short period of time while the other side is in T.38 fax mode.

Example:

Step 7 **show voice call status**

Use this command to display status of all voice ports.

Example:

```
Router# show voice call status
CallID     CID  ccVdb      Port      DSP/Ch  Called #   Codec    Dial-peers
0x5        11DE 0x660B24D0 1/0/0     1/1                g711ulaw 999100/0
0x7        11E1 0x665031A8 1/0:23.-1 1/2    *           g729ar8  0/999
0x11       11E4 0x6652B3B4 1/1:1.1   1/3     232222     g729ar8  999/0
3 active calls found
```

Step 8 **show voice call status** *call-id*

Use this command to display status of a specific call.

Example:

```
Router# show voice call status 5
Gathering information (10 seconds)...
CallID     Port      DSP/Ch  Codec    Rx/Tx     En/De     ERL/Reflctr Jitter
0x5        1/0/0     1/1     g711ulaw 500/500   500/500   5.0/3       65/0
Router# show voice call status 7
Gathering information (10 seconds)...
CallID     Port      DSP/Ch  Codec    Rx/Tx     En/De     ERL/Reflctr Jitter
0x7        1/0:23.-1 1/2     g729ar8  500/500   500/500   6.0/4       70/0
Router# show voice call status 11
Gathering information (10 seconds)...
CallID     Port      DSP/Ch  Codec    Rx/Tx     En/De     ERL/Reflctr Jitter
0x11       1/1:1.1   1/3     g729ar8  500/500   500/500   7.0/4       70/0
```

Step 9 **show voice dsp**

Use this command to display the status of DSP voice channels.

Example:

```
Router# show voice dsp
DSP   DSP         DSPWARE  CURR   BOOT                   PAK TX/RX
TYPE NUM CH CODEC     VERSION  STATE STATE   RST AI VOICEPORT TS ABORT PACK COUNT
==== === == ======== ======= ===== ======= === == ======== === ==== ===========
C549 1   01 {medium} 4.4.3   IDLE   idle       0   0   1/0:0       1       0     9357/9775
C549 1   02 {medium} 4.4.3   IDLE   idle            0   1/0:0        2     0     0/0
C549 2   01 {medium} 4.4.3   IDLE   idle         0   0   1/0:0       3       0     0/0
C549 2   02 {medium} 4.4.3   IDLE   idle            0    1/0:0       4   0     0/0
C549 3   01 {medium} 4.4.3   IDLE   idle       0   0   1/0:0       5       0         0/13
C549 3   02 {medium} 4.4.3   IDLE   idle            0   1/0:0       6       0     0/13
```

Step 10 **show rtpspi call**

Use this command to display active SRTP call details.

Example:

```
Router# show rtpspi call
RTP Service Provider info:
No. CallId dstCallId Mode      LocalRTP RmtRTP LocalIP    RemoteIP   SRTP
1   6      5         Snd-Rcv   18662    19392  0xA0A0A0D  0xA0A0A0B    1
2   8      7         Snd-Rcv   18940    16994  0xA0A0A0D  0xA0A0A0B    1
3   16     17        Snd-Rcv   19038    17198  0xA0A0A0D  0xA0A0A0B    1
```

Step 11 **show rtpspi statistics**

Use this command to display RTP statistics.

Example:

```
Router# show rtpspi statistics
RTP Statistics info:
No. CallId     Xmit-pkts Xmit-bytes Rcvd-pkts  Rcvd-bytes Lost pkts  Jitter Late
nc
1   6          0x842C    0x54AC30   0x842A     0x54AAE8   0x0        0x41     0x2
2   8          0x52B8    0x7C140    0x52B5     0x7C0F8    0x0        0x46     0x2
3   16         0x2EB0    0x46080    0x2EAF     0x46068    0x0        0x46     0x2
```

Step 12 **show ccm-manager**

Use this command to display the status and availability of Cisco CallManager.

Example:

```
Router# show ccm-manager
MGCP Domain Name: router
Priority        Status                   Host
============================================================
Primary         Registered               10.10.10.130
First Backup    Duplicate of Primary     10.10.10.130
Second Backup   None
Current active Call Manager:    10.10.10.130
Backhaul/Redundant link port:   2428
Failover Interval:              30 seconds
Keepalive Interval:             15 seconds
Last keepalive sent:            04:06:40 PAT Jan 8 2004 (elapsed time: 00:00:04)
Last MGCP traffic time:         04:06:40 PAT Jan 8 2004 (elapsed time: 00:00:04)
Last failover time:             None
```

```
Last switchback time:           None
Switchback mode:                Graceful
MGCP Fallback mode:             Enabled/OFF
Last MGCP Fallback start time:  03:42:25 PAT Jan 8 2004
Last MGCP Fallback end time:    03:42:44 PAT Jan 8 2004
MGCP Download Tones:            Disabled
Backhaul Link info:
    Link Protocol:      TCP
    Remote Port Number: 2428
    Remote IP Address:  10.10.10.130
    Current Link State: OPEN
    Statistics:
        Packets recvd:   7
        Recv failures:   0
        Packets xmitted: 13
        Xmit failures:   0
    PRI Ports being backhauled:
        Slot 1, port 0
Configuration Error History:
FAX mode: cisco
```

Step 13 **show crypto engine accelerator statistic**

Use this command to display statistics and error counters for the onboard hardware accelerator of the router for IPsec encryption.

Example:

```
Router# show crypto engine accelerator statistic
Virtual Private Network (VPN) Module in slot : 0
        Statistics for Hardware VPN Module since the last clear
         of counters 1814 seconds ago
                   638 packets in                        638 packets out
                 88640 bytes in                        87601 bytes out
                     0 paks/sec in                         0 paks/sec out
                     0 Kbits/sec in                        0 Kbits/sec out
                   315 packets decrypted                 323 packets encrypted
                 37680 bytes before decrypt            49921 bytes encrypted
                 21104 bytes decrypted                 67536 bytes after encrypt
                     0 packets decompressed                0 packets compressed
                     0 bytes before decomp                 0 bytes before comp
                     0 bytes after decomp                  0 bytes after comp
                     0 packets bypass decompr              0 packets bypass compres
                     0 bytes bypass decompres              0 bytes bypass compressi
                     0 packets not decompress              0 packets not compressed
                     0 bytes not decompressed              0 bytes not compressed
                 1.0:1 compression ratio               1.0:1 overall
                    33 commands out                       33 commands acknowledged
               Last 5 minutes:
                    60 packets in                         60 packets out
                     0 paks/sec in                         0 paks/sec out
                   121 bits/sec in                       120 bits/sec out
                  1720 bytes decrypted                  1140 bytes encrypted
                    46 Kbits/sec decrypted                30 Kbits/sec encrypted
                 1.0:1 compression ratio               1.0:1 overall
        Errors:
           ppq full errors         :        0   ppq rx errors           : 0
           cmdq full errors        :        0   cmdq rx errors          : 0
           no buffer               :        0   replay errors           : 0
           dest overflow           :        0   authentication errors   : 0
           Other error             :        0   RNG self test fail      : 0
           DF Bit set              :        0   Hash Miscompare         : 0
           Unwrappable object      :        0   Missing attribute       : 0
           Invalid attrribute value:        0   Bad Attribute           : 0
```

```
           Verification Fail       :        0   Decrypt Failure         : 0
           Invalid Packet          :        0   Invalid Key             : 0
           Input Overrun           :        0   Input Underrun          : 0
           Output buffer overrun   :        0   Bad handle value        : 0
           Invalid parameter       :        0   Bad function code       : 0
           Out of handles          :        0   Access denied           : 0
Warnings:
           sessions_expired        :        0   packets_fragmented      : 0
           general:                :        0
        HSP details:
           hsp_operations          :        0   hsp_sessions            : 0
```

Step 14 **show crypto ipsec sa**

Use this command to display the settings used by current SAs.

Example:

```
Router# show crypto ipsec sa

interface: FastEthernet0/0
    Crypto map tag: Gateway, local addr. 10.10.10.13
   protected vrf:
   local  ident (addr/mask/port/port): (10.10.10.13/255.255.255.255/0/0)
   remote ident (addr/mask/port/port): (10.10.10.130/255.255.255.255/0/0)
   current_peer: 10.10.10.130:500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 324, #pkts encrypt: 324, #pkts digest: 324
    #pkts decaps: 316, #pkts decrypt: 316, #pkts verify: 316
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 71, #recv errors 0
     local crypto endpt.: 10.10.10.13, remote crypto endpt.: 10.10.10.130
     path mtu 1500, media mtu 1500
     current outbound spi: 9073D35
     inbound esp sas:
      spi: 0x9FCB508(167556360)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 5121, flow_id: 1, crypto map: gateway
        crypto engine type: Hardware, engine_id: 2
        sa timing: remaining key lifetime (k/sec): (4446388/1913)
        ike_cookies: 6A391EE1 E57F3670 D4D78758 2F5C8E7C
        IV size: 8 bytes
        replay detection support: Y
      spi: 0xD132AE54(3509759572)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 5123, flow_id: 3, crypto map: gateway
        crypto engine type: Hardware, engine_id: 2
        sa timing: remaining key lifetime (k/sec): (4402107/1913)
        ike_cookies: 6A391EE1 E57F3670 D4D78758 2F5C8E7C
        IV size: 8 bytes
        replay detection support: Y
     inbound ah sas:
     inbound pcp sas:
     outbound esp sas:
      spi: 0x7D078A45(2097646149)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 5122, flow_id: 2, crypto map: gateway
        crypto engine type: Hardware, engine_id: 2
        sa timing: remaining key lifetime (k/sec): (4446388/1911)
```

```
        ike_cookies: 6A391EE1 E57F3670 D4D78758 2F5C8E7C
        IV size: 8 bytes
        replay detection support: Y
      spi: 0x9073D35(151469365)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 5124, flow_id: 4, crypto map: gateway
        crypto engine type: Hardware, engine_id: 2
        sa timing: remaining key lifetime (k/sec): (4402077/1911)
        ike_cookies: 6A391EE1 E57F3670 D4D78758 2F5C8E7C
        IV size: 8 bytes
        replay detection support: Y
     outbound ah sas:
     outbound pcp sas:
   protected vrf:
   local  ident (addr/mask/prot/port): (10.10.10.13/255.255.255.255/0/0)
   remote ident (addr/mask/prot/port): (10.10.10.131/255.255.255.255/0/0)
   current_peer: 10.10.10.131:500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0
     local crypto endpt.: 10.10.10.13, remote crypto endpt.: 10.10.10.131
     path mtu 1500, media mtu 1500
     current outbound spi: 0
     inbound esp sas:
     inbound ah sas:
     inbound pcp sas:
     outbound esp sas:
     outbound ah sas:
     outbound pcp sas:
```

Step 15 **show crypto isakmp sa**

Use this command to display current IKE SAs at a peer.

Example:

```
Router# show crypto isakmp sa
dst             src             state          conn-id slot
10.10.10.130    10.10.10.13     QM_IDLE              1    0
```

Step 16 **show crypto session**

Use this command to display the status of the current crypto session.

Example:

```
Router# show crypto session
Crypto session current status
Interface: FastEthernet0/0
Session status: UP-ACTIVE
Peer: 10.10.10.130/500
  IKE SA: local 10.10.10.13/500 remote 10.10.10.130/500 Active
  IPSEC FLOW: permit ip host 10.10.10.13 host 10.10.10.130
        Active SAs: 4, origin: crypto map
```

Step 17 **show crypto session detail**

Use this command to display IPsec details and statistics of the current crypto session.

Example:

```
Router# show crypto session detail
Crypto session current status
Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, X - IKE Extended Authentication
Interface: FastEthernet0/0
Session status: UP-ACTIVE
Peer: 10.10.10.130/500 fvrf: (none) ivrf: (none)
      Phase1_id: 10.10.10.130
      Desc: (none)
  IKE SA: local 10.10.10.13/500 remote 10.10.10.130/500 Active
          Capabilities:(none) connid:1 lifetime:07:30:00
  IPSEC FLOW: permit ip host 10.10.10.13 host 10.10.10.130
        Active SAs: 4, origin: crypto map
        Inbound:  #pkts dec'ed 335 drop 0 life (KB/Sec) 4402106/1800
        Outbound: #pkts enc'ed 327 drop 71 life (KB/Sec) 4402076/180
```

Configuration Examples for Media and Signaling Authentication and Encryption

Voice Security Features Example

The following example shows voice security features enabled:

```
Router# show running-config
Building configuration...
Current configuration : 2304 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname router
!
boot-start-marker
boot-end-marker
!
voice-card 1
 no dspfarm
!
voice-card 2
 no dspfarm
!
```

The following lines show secure codec complexity enabled:

```
voice-card 4
 codec complexity secure
 dspfarm
!
!
no aaa new-model
```

```
ip subnet-zero
!
ip cef
no ip domain lookup
!
ip domain name cisco.com
```

The IP domain name should match the domain name configured on Cisco CallManager.

```
!
Cisco CallManager-manager mgcp
!
crypto isakmp policy 1
 authentication pre-share
 lifetime 28800
crypto isakmp key cisco123 address 10.1.1.12
```

The crypto key should match the key configured on Cisco CallManager. This method and encapsulation mode should also match the method and encapsulation mode configured on Cisco CallManager. Other methods of key exchange are also supported. For more information refer to *Cisco IOS Security Configuration Guide*, Release 12.3 .

```
!
crypto ipsec transform-set rtpset esp-des esp-md5-hmac
mode transport
```

The crypto IPsec configuration should match the Cisco CallManager configuration.

```
!
crypto map rtp 1 ipsec-isakmp
 set peer 10.1.1.12
 set transform-set rtpset
 match address 115
!
interface FastEthernet0/1
 ip address 10.1.1.212 255.255.255.0
 load-interval 30
 duplex auto
 speed auto
 crypto map rtp
!
```

The following line shows the IPsec access list.

```
access-list 115 permit ip host 10.1.1.212 host 10.1.1.12
!
voice-port 1/0/0
!
voice-port 2/0/0
!
mgcp
mgcp call-agent 10.1.1.12 service-type mgcp version 0.1
```

The **mgcp package-capability** command enables the MGCP application ability to manage SRTP calls and advertise SRTP capability in SDP sent to remote gateways.

```
mgcp package-capability srtp-package
!
mgcp profile default
!
dial-peer voice 100 pots
```

```
 application mgcpapp
 port 1/0/0
!
dial-peer voice 200 pots
 application mgcpapp
 port 2/0/0
!
dial-peer voice 201 pots
 application mgcpapp
 port 2/0/1
!
dial-peer voice 202 pots
 application mgcpapp
 port 2/0/2
!
dial-peer voice 203 pots
 application mgcpapp
 port 2/0/3
!
dial-peer voice 101 pots
 application mgcpapp
 port 1/0/1
!
dial-peer voice 110 pots
 application mgcpapp
 port 1/1/0
!
dial-peer voice 111 pots
 application mgcpapp
 port 1/1/1
!
!
alias exec k show mgcp conn | inc K=
alias exec sr sh call active voi | inc SRTP
alias exec rs sh rtpspi call | inc Snd-Rcv
alias exec vc sh voi call
alias exec m sh mgcp conn
alias exec cav sh call active voi
alias exec rsa sh rtpspi call
alias exec cc clear counters
alias exec sta sh int fa0/1 stat
alias exec cef sh ip cef
!
line con 0
 exec-timeout 0 0
 logging synchronous
line aux 0
line vty 0 4
 login
!
!
end
```

Additional References

The following sections provide references related to the Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways feature.

Related Documents

Related Topic	Document Title
Cisco CallManager configuration	Cisco IP Phone Authentication and Encryption for Cisco CallManager 4.0(1)
Cisco CallManager and IPsec configuration	• " How to Configure IPsec Tunneling in Windows 2000 ," Microsoft Knowledge Base article • " Step-by-Step Guide to Internet Protocol Security (IPsec) ," "Building A Custom IPsec Policy" section, Microsoft Knowledge Base article
Cisco IP Phone 7940 and 7960 administration	Cisco IP Phone Model 7960G and 7940G Administration Guide for Cisco CallManager
Cisco IP Phone 7970 administration	*Cisco IP Phone 7970 Administration Guide for Cisco CallManager*
Cisco 2621 configuration	*Cisco 2621 Modular Access Router with AIM-VPN/BP Security Policy*
Cisco 2651 configuration	*Cisco 2651 Modular Access Router with AIM-VPN/BP Security Policy*
Cisco 3640 configuration	*Cisco 3640 Modular Access Router with AIM-VPN/BP Security Policy*
Cisco 3660 configuration	*Cisco 3660 Modular Access Router with AIM-VPN/BP Security Policy*
Secure SRST router configuration	Setting Up Secure SRST
Advanced Encryption Standard (AES) feature	*Advanced Encryption Standard*
IPsec configuration	*Cisco IOS Security Configuration Guide*, Release 12.3
IPsec commands	*Cisco IOS Security Command Reference,* Release 12.3
Cisco IOS voice configuration	*Cisco IOS Voice Configuration Library*
Cisco IOS voice command reference	*Cisco IOS Voice Command Reference*
Configuring IPsec Between a Microsoft Windows 2000 Server and a Cisco Device	Configuring IPsec Between a Microsoft Windows 2000 Server and a Cisco Device
Secure Real-time Transport Protocol Support	Secure Real-time Transport Protocol Support

Standards

Standards	Title
IETF draft draft-ietf-mmusic-sdescriptions-02.txt	Security Descriptions for Media Streams

MIBs

MIB	MIBs Link
CISCO-VOICE-DIAL-CONTROL-MIB	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 3711	*Secure Real-time Transport Protocol*
RFC 4040	RTP Payload Format for a 64 kbit/s Transparent Call
RFC 4568	Session Description Protocol (SDP) Security Descriptions for Media Streams

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

Feature Information for Media and Signaling Authentication and Encryption

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 4: Feature Information for Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways

Feature Name	Releases	Feature Information
Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways	12.3(11)T2 12.3(14)T	In 12.3(11)T2, this feature was introduced. In 12.3(14)T support was added for the Cisco Secure SRST feature and the NM-HDV network module.
Support for MGCP 1.0 Call Control for SRTP on Cisco IOS Gateways	15.0(1)XA	This feature provides support for MGCP 1.0 call control for SRTP on Cisco IOS gateways, and for fax pass-through and the Clear Channel codec at the media level under MGCP 1.0 and 0.1. The following command was introduced: **mgcp crypto rfc-preferred**.

Glossary

CCM --Cisco Call Manager.

CLI --command-line interface.

CTL --Certificate Trust List.

DTMF --dual-tone multifrequency

HMAC --Hashed Message Authentication Codes.

IETF --Internet Engineering Task Force. Standards body for Internet standards.

IKE --Internet Key Exchange.

IPsec --IP security.

MGCP --Multimedia Gateway Control Protocol.

PIN --Personal identification number.

RTCP --Real-Time Transport Protocol Control Protocol.

RTP --Real-Time Transport Protocol

SDP --Session Description Protocol.

SHA1 --Secure Hash Algorithm1.

SRST --Survivable Remote Site Telephony.

SRTP --Secure RTP.

SRTCP --Secure RTCP.

VoIP --Voice over IP.