Q&A

Media Authentication and Encryption Using Secure RTP on Cisco Multiservice and Integrated Services Routers

Media/Signaling authentication and encryption features on Cisco's portfolio of multiservice and integrated services routers ensures that voice conversations terminating on either TDM or analog voice gateway ports are protected from eavesdropping. These reliable, scalable features provide a secure environment for IP communications over a LAN (local area network) or WAN (wide area network)

FEATURES/BENEFITS

Q. What is media authentication and encryption?

A. Media authentication and encryption ensures that the media streams between authenticated devices (i.e. where the identities have been validated) are secure and that only the intended device receives and reads the data.

Q. What is signaling authentication and encryption?

A. Signaling information includes control information such as DTMF digits that are entered by the parties, call status, and media encryption keys. Signaling encryption ensures that all signaling messages that are sent between the device and the Cisco CallManager server are encrypted. Signaling authentication or signaling integrity validates that no tampering has occurred to signaling packets during transmission, and that the packets originated from the correct source.

Q. What is the media encryption feature supported on the Cisco Multiservice and Integrated Services Routers?

A. The media authentication and encryption feature using secure RTP (SRTP) on Cisco routersrouters delivers the ability to encrypt IP phone to gateway calls or gateway to gateway calls. This protects voice conversations or fax calls terminating in TDM or analog gateway ports from eavesdropping. This media authentication and encryption feature works with any Cisco IP phone that supports encryption.

Q. Do Cisco multiservice and integrated services routers support signaling encryption as well?

A. Yes. The signaling is encrypted from the gateway to the Cisco CallManager using an IPSec tunnel.

Q. Which protocol does the media encryption feature support?

A. In this phase, only MGCP 0.1 interworking with Cisco CallManager is supported.

Q. What type of gateway interfaces are supported with this feature?

A. The IP Communications Voice/Fax network modules (NM-HD-1V, NM-HD-2V, NM-HD-2VE), the IP Communications High-Density Digital Voice/Fax network modules (NM-HDV2, NM-HDV2-1T1/E1, NM-HDV2-2T1/E1), the Digital T1/E1 Packet Voice/Fax Network Module (NM-HDV and all bundle variations), the High-Density Analog and Digital Extension Module (EVM-HD) and the Packet Voice/Fax Digital Signal Processing Module (PVDM2) are supported. These interfaces support analog and TDM gateway ports, including FXS, FXO, T1, E1, fax etc.

Q. Which Cisco routers support this feature?

A. The media/signaling authentication and encryption features are supported on a wide range of platforms. These include the Cisco 2600XM, 2691, 2801, 2811, 2821, 2851, 3660, 3640A, VG224, 3700 series and 3800 series platforms.

Q. Is secure conferencing and transcoding supported?

A. No. Secure conferencing and transcoding is not supported. During conferencing calls and/or transcoding functions, secure calls will revert to non-secure.

Q. Which IP phones work with the Cisco Multiservice and Integrated Services Routers for secure IP phone to gateway calls?

A. The 7940, 7960 and 7970 IP phones support media authentication and encryption

Q. How can I tell if my gateway to gateway call or IP phone to gateway call is secure?

A. For gateway to gateway calls (example: secure fax to fax calls from one branch office to another), CLI commands are available to confirm that a +call is encrypted and provide details about an encrypted call. In addition, the IP phone will display a secure lock icon for encrypted IP phone to gateway calls, and encrypted IP phone to IP phone calls.

Q. When I see a secure lock icon on my IP phone for IP phone to PSTN gateway calls, does this mean the calls are encrypted across the PSTN?

A. No. The secure lock icon indicates that the call is secure for the IP leg of the call, from your IP phone to the PSTN gateway. Once the call is directed from the gateway to the PSTN network, the security of the call is beyond the IP network and our control. We make no claims on the security of the PSTN network.

Q. Which codecs are supported for media encryption?

A. G.711, G.729A and G.729 codecs are supported.

Q. Can the media encryption features using SRTP be used for securing calls in the LAN or WAN?

A. Media encryption using SRTP can be used to secure calls in both the LAN and the WAN. However, when SRTP packets are sent over an untrusted WAN, the headers may be exposed. You will need to ensure the packets are sent through an IPSec VPN tunnel.

SECURE SRST

Q. Is media encryption supported in SRST mode?

A. Yes. Media encryption in SRST mode is supported with Cisco IOS 12.3(14)T Advanced IP Services and Advanced Enterprise Services images. Media streams are encrypted using Secure RTP.

Q. Is the signaling encryption supported in SRST mode?

A. Yes. The signaling is encrypted between the IP phones and SRST router using TLS.

Q. What happens to my secure call when my call processing reverts to SRST mode?

A. Should you experience a WAN failure, and lose connectivity to Cisco CallManager, the call is reverted to the SRST router for backup call processing. If you configured SRST mode for secure calls (i.e. Secure SRST), you will continue to be able to place secure calls within the remote branch office. If you did not configure for Secure SRST, your secure call will fallback to non-secure.

Q. How do I select the phones which will support Secure SRST?

A. You can configure this in the Cisco CallManager Admin page, similar to how you select the types of phones which will support SRST.

Q. How is the SRST router authenticated?

A. The SRST router is authenticated using X.509 certificates. These certificates can be generated by a CA (Certificate Authority) server or from the Cisco IOS Certificate server. Mutual authentication between the SRST router and supported IP phones occurs when Cisco CallManager provides the SRST router certificate to the IP phones, and the IP phone certificates to the SRST router.

Q. What are the maximum number of IP phones that can be supported in secure SRST mode?

A. There is no impact to the number of IP phones that can be supported in secure SRST mode. The same numbers, as published in the following URL are supported: http://www.cisco.com/univercd/cc/td/doc/product/access/ip_ph/srs/srst32/srs32spc.htm

PERFORMANCE

Q. How many secure calls can be supported per interface?

A. Because media encryption occurs in the DSPs, the number of secure calls that can be supported are dictated by the type and number of DSPs on the interface. For instance, a PVDM2-16 has a single DSP that can support 16 calls in G.711 codec, 8 calls in medium complexity codec, and 6 calls in high complexity codec. In secure mode, the PVDM2-16 will support 10 calls in G.711 codec, 8 calls in medium complexity codec and 6 calls in high complexity codec. PVDM2s are supported on the NM-HD modules, NM-HDV2 modules and on the motherboard on the 2811, 2821, 2851 and 3800 series platforms.

	# DSPs	Non-Secure Calls (G.711 codec)	Secure Calls (G.711 Codec)	Secure Calls (Medium Complexity Codec)	Secure Calls (High Complexity Codec)
PVDM2-16	1	16	10	8	6
PVDM2-32	2	32	20	16	12
PVDM2-48	3	48	30	24	18
PVDM2-64	4	64	40	32	24

On the NM-HDV, secure calls are supported only in medium complexity mode. Only two secure calls are supported, versus four non-secure calls.

Q. Are there scalability issues with supporting media encryption?

A. No. Media encryption is performed on the DSPs, therefore it is a very scalable solution. As more GWs and voice interfaces are added, you can add more DSPs to support more secure calls.

Q. Are there delay issues with supporting media encryption?

A. No. The key exchange is done as part of the normal MGCP call setup, therefore there is no extra call setup delay. Also, because the encryption is performed on the DSPs, there are no voice media delay issues associated with packets being processed at a separate engine or in the router CPU.

SECURE RTP (SRTP) TECHNOLOGY

Q. What is secure RTP?

A. Secure RTP is an IETF (Internet Engineering Task Force) standard to transport encrypted voice. SRTP is developed just for voice packets. It is very efficient for voice and video packets as only the payload is encrypted. A SRTP-encrypted packet is indistinguishable from an RTP packet except for 4 bytes of authentication tag.

Q. What type of encryption algorithm does SRTP support?

A. SRTP supports AES-128 Counter Mode encryption. AES delivers a higher level of security strength and speed compared to other algorithms such as DES and 3DES. SRTP also supports the HMAC secure hash authentication algorithm (SHA 1).

Q. How does SRTP encryption compare with IPSec encryption?

A. Encryption using SRTP is more bandwidth-efficient than IPSec because only the payload is encrypted, and there are no additional encryption headers added to the packet. In addition, SRTP encryption can be delivered from end-to-end, i.e. IP phone to IP phone, while IPSec encryption is only from router to router.

POSITIONING OF MEDIA ENCRYPTION FEATURES USING SRTP

Q. How do the media encryption features fit with other security features available as part of Cisco's Self Defending Network (SDN) initiative?

A. While the initial layers of defense are to control and prevent access to the voice domain, media encryption using secure RTP (SRTP) delivers another layer of protection. It encrypts the voice conversation, rendering it unintelligible to internal or external hackers who have penetrated and gained access to the voice domain.

Q. When do we deploy SRTP versus IPSec V3PN?

A. Both IPSec V3PN and SRTP are complementary technologies. SRTP can be used to encrypt voice packets in the LAN, and these encrypted packets should be sent across an untrusted WAN in an IPSec V3PN tunnel. This protects the SRTP headers that are not encrypted from hackers. If the WAN is trusted, SRTP can be used to encrypt voice packets end-to-end across the LAN and WAN.

FEATURE AVAILABILITY

Q. Which Cisco IOS release supports media encryption?

A. Media encryption is supported starting with the 12.3(11)T2 IOS release. Media encryption in SRST mode is available beginning with the 12.3(14)T IOS release. The following table summarizes the interfaces, platforms and releases.

Module Support	Platform Support	Availability	Release (Internal Use Only)
NM-HD-1V, NM-HD-2V, NM-HD-2VE	Cisco 2600XM, 2691, 2811, 2821, 2851, 3660, 3700, 3800	September 2004	IOS 12.3(11)T2 and Cisco CallManager 4.1
NM-HDV2, NM-HDV2-1T1/E1, NM-HDV2-2T1/E1	Cisco 2600XM, 2691, 2811, 2821, 2851, 3700, 3800	September 2004	IOS 12.3(11)T2 and Cisco CallManager 4.1
PVDM2-8, PVDM2-16, PVDM2-32, PVDM2-48, PVDM2-64	Cisco 2801, 2811, 2821, 2851, 3825, 3845	September 2004	• IOS 12.3(11)T2 and Cisco CallManager 4.1 • IOS 12.3(14)T and Cisco CallManager 4.1—2801 platform
EVM-HD	Cisco 2821, 2851, 3825, 3845	September 2004	IOS 12.3(11)T2 and Cisco CallManager 4.1
NM-HDV (including all bundle variations)	Cisco 2600XM, 2691, 2811, 2821, 2851, 3700, 3800	February 2005	IOS 12.3(14)T and Cisco CallManager 4.1

Q. Which Cisco IOS feature sets support media encryption?

A. The Advanced IP Services images and the Advanced Enterprise Services images support media encryption.

Q. Which Cisco CallManager version does this feature interoperate with?

A. The media encryption feature interoperates with Cisco CallManager 4.1.

FOR MORE INFORMATION

For more information, refer to:

- **Datasheet**—http://www.cisco.com/en/US/products/ps5855/products_data_sheet0900aecd8016c784.html

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on **the Cisco Website at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

205481.P_ETMG_CC_10.05

Printed in the USA