

Secure Voice on Cisco Multiservice and Integrated Services Routers

시스코 시스템즈 멀티서비스 및 통합 서비스 라우터 포트폴리오에서 제공하는 미디어 인증 및 암호화 기능은 음성 통화 도청을 방지 해줍니다.

음성 및 IP 커뮤니케이션 제품과 애플리케이션의 Cisco Unified Communications 시스템은 조직의 보다 효과적인 커뮤니케이션을 이끌어 비즈니스 능력을 향상시켜주고, 한 번에 올바른 자원을 찾을 수 있게 하며 수익성을 높여줍니다. Cisco Unified Communications 포트폴리오는 모든 규모의 조직을 위한 통합 솔루션인 Cisco Business Communications Solution 의 핵심 구성요소입니다. Cisco Business Communications Solution 에는 또한 네트워크 인프라, 보안, 네트워크 관리 제품, 무선 연결 및 라이프사이클 서비스 접근 방법과 유연한 구축, 외주 관리 옵션, 최종 사용자 및 파트너 금융 패키지, 타사 커뮤니케이션 애플리케이션 등이 포함됩니다.

제품 개요

기업들은 운영 비용 절감, 생산성 향상 및 네트워크 관리 단순화를 위해 IP 커뮤니케이션으로 전환하고 있습니다. Cisco 1700 Series 에서부터 3800 Series 플랫폼까지 시스코 멀티서비스 및 통합 서비스 라우터 포트폴리오는 까다로운 엔터프라이즈 환경에 강력하고 확장 가능한 IP 커뮤니케이션 솔루션을 제공합니다.

시스코 멀티서비스 및 통합 서비스 라우터의 광범위한 음성 보안 기능은 IP 커뮤니케이션 솔루션을 구현하는 기업에 높은 수준의 보안을 제공합니다. 자가 방어 네트워크 모델에 기반한 시스코 멀티레이어 제품은 네트워크에서 시작하여 엔드포인트와 애플리케이션까지 확장됩니다. 시스코의 SAFE Blueprint 는 비즈니스 네트워크 보안을 지원하기 위한 모범사례 및 톨에 대한 상세한 프레임워크를 제시합니다.

SRTP(Secure Real-Time Transport Protocol)를 사용한 미디어 암호화는 음성 대화를 암호화하여, 음성 도메인에 액세스한 내외부의 도청자 가 대화 내용을 식별할 수 없게 함으로써 보안을 유지합니다. 음성 패킷을 위해 설계된 SRTP 는 IETF RFC 3711 표준으로 AES 암호화 알고리즘을 지원합니다.

시스코 라우터의 미디어 암호화 기능은 Cisco Unified CallManager 소프트웨어 및 Cisco Unified IP 폰의 미디어 암호화 기능과 함께 작동하여 게이트웨이 간 통화뿐 아니라 IP 폰과 게이트웨이 간 통화를 모두 보호합니다. 이것은 미디어가 연결되는 게이트웨이 인터페이스 유형에 따라 아날로그 통화, 보안 팩스 통화 또는 IP 폰과 게이트웨이 간의 안전한 통화를 지원합니다. Cisco Unified CallManager 에서 생성된 음성 암호화 키는 암호화된 시그널링 경로를 통해 TLS(Transport Layer Security)를 사용하여 Cisco Unified IP 폰으로 안전하게 전송되고 IPSec(IP Security)보호 링크를 통해 게이트웨이로 전달됩니다.

시스코 라우터의 미디어 암호화 기능은 Advanced Enterprise Services 및 Advanced IP Services IOS Software Feature Set 로 업그레이드한 Cisco IOS Software Release 12.3(11)T2 에서부터 사용 가능합니다. 이러한 기능들은 PVDM2, EVM-HD, NM-HD-, AIM-VOICE 및 NM-HDV2 음성 게이트웨이 네트워크 모듈에서 사용 가능한 DSP(digital signal processing) 모듈에서 제공됩니다.

기능 표

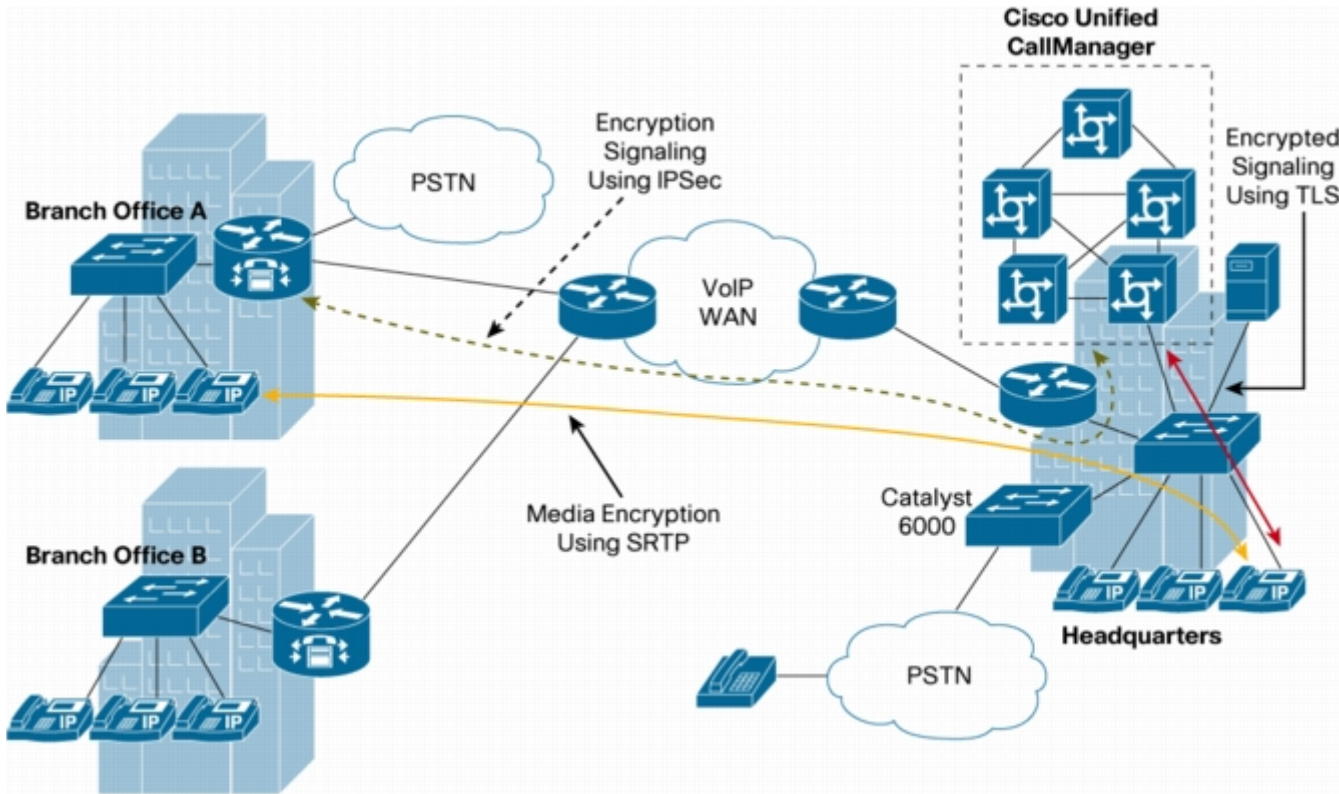
표 1은 미디어 인증 및 암호화 솔루션의 세부 내용을 표시합니다.

인증 및 암호화 기능	• SRTP를 사용한 음성 RTP 스트림 미디어 암호화 • 보안 RTCP(RTP Control Protocol)를 사용한 RTCP 정보 교환 • 보안 및 비보안 엔드포인트 간 통화를 위한 SRTP-RTP 폴백 • WAN 장에 복구 시 Cisco Unified SRST(Survivable Remote Site Telephony) 모드에서 안전한 통화 지원 • SRTP를 사용한 미디어 암호화 통화에 CRTP(압축 RTP) 지원
인증 및 암호화 알고리즘	• AES-128 암호화 알고리즘 지원 • HMAC 보안 해시 인증 알고리즘(SHA 1) 지원
시그널링 인증 및 암호화 기능	• MGCP(Media Gateway Control Protocol) 및 H.323 게이트웨이에서 게이트웨이-Cisco Unified CallManager 시그널링 및 암호화에 IPsec 사용 • IP 폰 - Cisco Unified Survivable Remote Site Telephony 라우터 시그널링 및 암호화는 TLS(Transport Layer Security) 사용
프로토콜 지원	• MGCP 0.1(Cisco Unified CallManager에서 MGCP 게이트웨이 지원) • H.323(H.323 게이트웨이 및 IPIP 게이트웨이에서 지원, Cisco Unified CallManager 상호 운용성 옵션) • SRST 모드에서 SCCP(Cisco Unified IP Phone)
모듈 지원	• PVDM 모듈: PVDM2-8, PVDM2-16, PVDM2-32, PVDM2-48, PVDM2-64 • 아날로그 음성 모듈: EVM-HD(PVDM 포함), NM-HD-1V, NM-HD-2V, NM-HD-2VE • 디지털 음성 모듈 NM-HDV2, NM-HDV2-1T1/E1, NM-HDV2-2T1/E1, NM-HDV (모든 버전), AIM-VOICE-30, AIM-ATM-VOICE-30
코덱 지원	• G.711, G.729A와 G.729

애플리케이션

시스코 멀티서비스 및 통합 서비스 라우터의 미디어 인증 및 암호화와 더불어 Cisco IP 폰 및 Cisco Unified CallManager의 미디어 암호화는 WAN 또는 LAN 사이의 IP 커뮤니케이션에 높은 수준의 보안 환경을 제공합니다. 그림 1과 같이 SRTP를 사용하여 지사 A의 음성 게이트웨이 네트워크 모듈에서 이루어지는 음성 통화를 암호화합니다. 이는 사무실 내의 아날로그 전화 간 또는 팩스 기기 간에 안전한 통화를 제공합니다. 이와 유사하게, 지사 A의 TDM(time-division multiplexing) 엔드포인트 또는 아날로그 전화에서부터 본사의 Cisco Unified IP 폰에 이르기까지 안전한 통화를 지원합니다. 지사 A의 게이트웨이와 Cisco Unified CallManager 사이의 시그널링은 IPsec을 사용하여 보호되고, 본사의 IP 폰과 Cisco Unified CallManager 사이의 시그널링은 TLS를 사용하여 보호됩니다.

그림 1. 미디어 인증 및 암호화



핵심 기능 및 이점

미디어 인증 및 암호화

미디어 암호화는 현재 Cisco Unified IP 폰 간의 음성 통화에 엔드투엔드 암호화를 제공합니다. 시스코 라우터에 미디어 암호화를 도입함으로써 IP 폰-게이트웨이 및 게이트웨이-게이트웨이 통화를 안전하게 할 수 있는 기능이 추가됩니다. 사용자는 이제 IETF RFC3711 표준 기반 SRTP 를 사용하여 PSTN 게이트웨이로 암호화된 통화를 할 수 있습니다. SRTP 는 추가 암호화 헤더를 추가하지 않고 음성 패킷의 페이로드만 암호화 합니다. 이 때문에 SRTP 암호화 음성 패킷은 RTP 음성 패킷과 거의 구별할 수 없어, 추가 개발 또는 패킷 조작 없이도 서비스 품질(QoS) 및 압축 RTP 를 지원할 수 있습니다. 또한 SRTP 는 AES 암호화 표준에서 지원하는 가장 큰 실제 키 크기를 사용하여 향상된 보안을 제공합니다. 통화별로 암호화 키가 생성되어 보다 높은 수준의 보안을 보장합니다. 또한 미디어 인증은 통화를 암호화하는 장치의 ID를 확인합니다. LAN 에서 음성 개인 정보 및 기밀 유지를 통해 내부 위협으로부터 보호하려면, SRTP 를 사용한 미디어 암호화가 적합합니다. 또한, 데이터용으로 배치된 VPN 인프라를 사용하여 IP WAN 또는 인터넷 상에서 미디어 암호화를 제공할 수 있습니다.

시그널링 인증 및 암호화

게이트웨이와 Cisco Unified CallManager 사이의 시그널링 인증 및 암호화는 IPSec 를 사용하여 보호됩니다. 이는 DTMF(dual tone multifrequency) 번호, 암호, PIN 및 음성 암호화 키와 같은 시그널링 정보를 안전하게 보호해줍니다. Cisco IOS Software 에서 사용 가능한 소프트웨어 기반 IPSec 및 AIM-VPN 모듈을 통한 하드웨어 기반 IPSec 이 모두 지원됩니다.

암호화된 통화의 확장성

SRTP 미디어 암호화는 라우터 CPU 가 아닌 DSP 모듈에서 수행됩니다. 이는 DSP 를 장착한 음성 게이트웨이 인터페이스의 개수 또는 플랫폼(통합 서비스 라우터 등)에서 통합된 DSP 의 개수가 증가함에 따라 보안 통화를 위해 사용 가능한 DSP 개수가 증가하기 때문에 효율적인 확장성을 보장합니다.

효율적인 지연 최적화 및 채널 용량 영향

정상적인 MGCP 통화 설정의 일부로 키 교환이 이루어지고 추가 메시지가 도입되지 않기 때문에 암호화된 통화에 추가적인 통화 설정 지연이 발생하지 않습니다. SRTP 미디어 암호화는 라우터 CPU 또는 완료된 음성 패킷을 처리하는 별도의 암호화 엔진에서 수행되는 것이 아니라 DSP 에서 수행되기 때문에 음성 미디어 지연도 발생하지 않습니다.

G.729 및 G.729a 모드에서 암호화된 통화에 대한 채널 용량 영향이 없으며 G.711 모드에서는 영향이 최소화됩니다.(표 2).

표 2. DSP별 채널 영향(예: PVDM2)

코덱	일반 음성 통화/DSP	암호화 음성 통화/DSP
G.711	통화 16 번	통화 10 번
G.729a	통화 8 번	통화 8 번
G.729	통화 6 번	통화 6 번

관리 기능

미디어 인증 및 암호화는 시스코 라우터의 CLI(command-line interface)를 사용하여 손쉽게 구성할 수 있습니다. 또한, Cisco IP 폰의 잠금 아이콘 표시기와 같은 기능은 지원 게이트웨이로 연결된 통화 시 암호화를 시각적으로 확인할 수 있도록 해줍니다. 콜 플로우 내의 장치가 미디어 암호화를 지원하지 않거나 보안이 노출된 경우, 잠금 아이콘이 사라집니다. 암호화된 통화 및 통화 디버깅에 대한 세부 내용을 확인할 수 있는 CLI 명령도 사용할 수 있습니다.

Cisco Unified Survivable Remote Site Telephony 모드에서의 보안

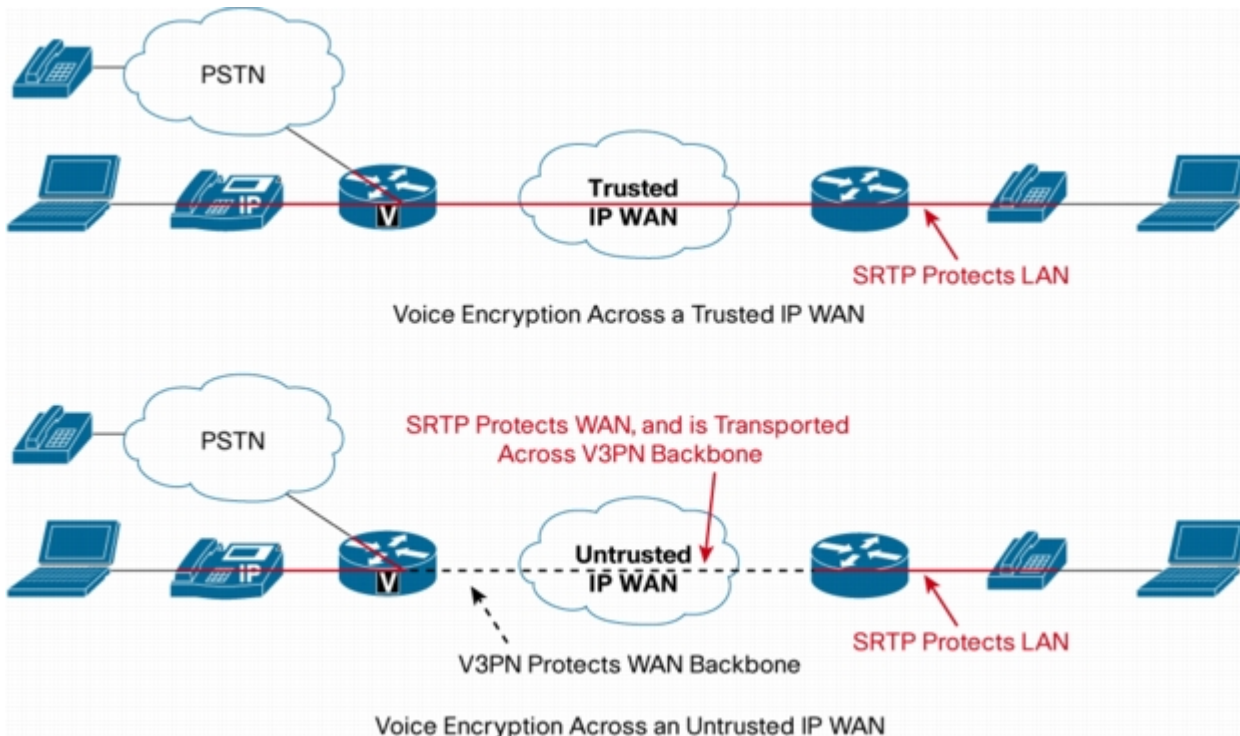
Cisco Unified Survivable Remote Site Telephony 는 Cisco Unified CallManager 와의 연결이 끊긴 경우 호 처리 리던던시를 제공합니다. Cisco IOS Software Release 12.3(14)T 부터 시작하여 Cisco Unified Survivable Remote Site Telephony 모드의 미디어 인증 및 암호화가 지원되므로, WAN 연결 또는 Cisco Unified CallManager 가 다운될 경우 원격 지사 내에서 안전한 통화가 가능한 기능을 제공합니다. WAN 연결 또는 Cisco Unified CallManager 가 복구되면 Cisco Unified CallManager 가 보안된 호처리 기능을 재개합니다. Cisco Unified Survivable Remote Site Telephony 라우터에서부터 IP 폰에 이르기까지 시그널링은 TLS 를 사용하여 암호화됩니다.

SRTP 및 IPSEC VPNS

SRTP와 IPSec은 상호 보완적인 VPN 기술입니다. 주요 차이점 중 하나는 SRTP는 끝에서 끝까지, 즉 IP 폰에서 IP 폰까지 암호화를 제공할 수 있는 반면 IPSec VPN은 라우터-라우터 터널 기반 암호화입니다. 또한, SRTP는 음성 패킷만 암호화하는 반면 IPSec VPN 터널은 데이터, 음성 및 비디오(V3PN이라 불림)를 전송할 수 있습니다. 이는 SRTP가 IPSec VPN을 사용하여 추가적인 음성 트래픽 보호를 제공할 수 있음을 의미 합니다.

신뢰할 수 있는 WAN 네트워크를 보유한 대기업 또는 중소기업의 경우, SRTP를 사용하여 이 네트워크 전체에 걸쳐 음성을 엔드투엔드로 암호화할 수 있습니다. 하지만, 대부분의 기업 업무는 인터넷 또는 서비스 제공업체가 관리하는 WAN을 사용하게 됩니다. 따라서 WAN이 보안되지 않았을 수 있기 때문에 VPN 터널을 사용하여 지사 간의 데이터를 안전하게 전송합니다. 데이터용으로 사용되는 IPSec VPN 네트워크를 통해 WAN 상에서 SRTP를 사용하여 음성 보안을 제공할 수 있습니다. 이는 그림 2에 설명되어 있습니다.

그림 2. 보안 RTP 및 V3PN



기능 가용성

표 3. 기능 가용성

프로토콜/기능 지원	플랫폼 지원(표 4의 지원 모듈 포함)	릴리스
MGCP 게이트웨이 (MGCP 0.1)	- Cisco 2600XM, 2691, 3660, 3725 및 3745 멀티서비스 플랫폼 - Cisco 2811, 2821, 2851, 3825 및 3845 통합 서비스 라우터 - Cisco VG224 Analog Phone Gateway	Cisco IOS Software Release 12.3(11)T2 및 Cisco Unified CallManager 4.1

H.323 게이트웨이 및 IPIP 게이트웨이	• Cisco 2600XM, 2691, 3725 및 3745 멀티서비스 플랫폼 • Cisco 2811, 2821, 2851, 3825 및 3845 통합 서비스 라우터 • Cisco VG224 Analog Phone Gateway • Cisco IAD 2430 Series Integrated Access Device • IPIP 게이트웨이는 flow-through 및 flow-around 모드에서 모두 지원됩니다.	• Cisco IOS Software Release 12.4(6)T • Cisco Unified CallManager 5.0 과의 상호 운용이 지원되지만 옵션임
G.729	• Cisco 2600XM, 2691, 3660, 3725 및 3745 멀티서비스 플랫폼 • Cisco 2811, 2821, 2851, 3825 및 3845 통합 서비스 라우터	• Cisco IOS Software Release 12.3(14)T 및 Cisco Unified CallManager 4.1

모듈 가용성

표 4. 모듈 가용성

모듈지원	플랫폼 지원	릴리스
NM-HD-1V, NM-HD-2V, NM-HD-2VE	• Cisco 2600XM, 2691, 3660, 3725 및 3745 멀티서비스 플랫폼 • Cisco 2811, 2821, 2851, 3825 및 3845 통합 서비스 라우터	• Cisco IOS Software Release 12.3(11)T2
H.323 게이트웨이 및 IPIP 게이트웨이	• Cisco 2600XM, 2691, 3725 및 3745 멀티서비스 플랫폼 • Cisco 2811, 2821, 2851, 3825 및 3845 통합 서비스 라우터	• Cisco IOS Software Release 12.3(11)T2
PVDM2-8, PVDM2-16, PVDM2-32, PVDM2-48, PVDM2-64*	• Cisco 2801, 2811, 2821, 2851, 3825 및 3845 통합 서비스 라우터	• Cisco IOS Software Release 12.3(11)T2-2801 이외의 모든 플랫폼 • Cisco IOS Software Release 12.3(14)T-2801 플랫폼
EVM-HD	• Cisco 2821, 2851, 3825 및 3845 통합 서비스 라우터	• Cisco IOS Software Release 12.3(11)T2 및 Cisco Unified CallManager 4.1
NM-HDV (번들 변경 포함)	• Cisco 2600XM, 2691, 3725 및 3745 멀티서비스 플랫폼 • Cisco 2811, 2821, 2851, 3825 및 3845 통합 서비스 라우터	• Cisco IOS Software Release 12.3(14)T 및 Cisco Unified CallManager 4.1
AIM-VOICE-30, AIM-ATM-VOICE-30, NM-HDA	• Cisco 2600XM, 2691, 3725 및 3745 멀티서비스 플랫폼	• Cisco IOS Software Release 12.3(6)T

* The PVDM2 패킷/음성 DSP 모듈은 Cisco 2801, 2811, 2821 및 2851 통합 서비스 라우터의 온보드 VICs/VWICs와 함께 사용됩니다. 또한, Cisco 2821, 2851, 3825 및 3845 통합 서비스 라우터에서 지원되는 EVM-HD(High-Density Analog and Digital Extension Module)와 함께 사용됩니다.

참고 : 시스코 멀티서비스 및 통합 서비스 라우터의 음성 게이트웨이 모듈은 미디어 암호화를 지원하는 Cisco Unified IP Phone 7940G, 7960G, 7970G와 상호운용됩니다. Cisco Unified IP Phone 7970G는 Cisco Unified CallManager 4.0 릴리스에서 미디어 암호화를 지원하며 Cisco Unified IP Phone 7960G와 7940G는 Cisco Unified CallManager 4.1 릴리스에서 미디어 암호화를 지원합니다.

CISCO UNIFIED COMMUNICATIONS 서비스 및 지원

Cisco Lifecycle Services 접근 방법을 통하여 시스코 시스템즈와 파트너들은 Cisco Unified Communications 시스템을 지원하기 위한 광범위 한 엔드투엔드 서비스 포트폴리오를 제공합니다. 이러한 서비스들은 IP 커뮤니케이션 서비스 구축, 운영 및 최적화에 입증된 방법론들을 기반으로 구성되었습니다. 예를 들어, 사전 계획 및 설계 서비스는 촉박한 구축 스케줄을 맞출 수 있게 해주며, 구현 중 네트워크 중단을 최소화시켜 줍니다. 운영 서비스는 전문적 기술 지원으로 커뮤니케이션 다운타임 위험을 줄여주며, 최적화 서비스는 솔루션 성능 향상을 통해 업무 효율성을 높여줍니다. 시스코 및 파트너들은 시스템 레벨 서비스 및 지원을 제공하여 업무적 요구사항을 만족시킬 수 있는 탄력적인 컨버지드 네트워크를 구축하고 유지할 수 있습니다.

결론

미디어 인증 및 암호화는 IP 커뮤니케이션을 구현하는 대기업 및 중소기업에 추가적인 보안 레이어를 제공합니다. TDM 또는 아날로그 음성 게이트웨이 포트 또는 Cisco Unified IP 폰으로 연결되는 음성 대화는 LAN 및 WAN 상의 표준 기반 암호화를 통해 도청으로부터 보호됩니다.

제품 호환성

표 5. 제품 호환성

제품 호환성	• Cisco 2600XM, 2691, 3725 및 3745 멀티서비스 플랫폼 • Cisco 2811, 2821, 2851, 3825 및 3845 통합 서비스 라우터 • Cisco VG224 Analog Phone Gateway • Cisco IAD 2430 Series Integrated Access Device • MGCP 및 SCCP 용 Cisco Unified CallManager 4.1(Cisco Unified SRST 모드) • Cisco Unified CallManager 5.0 (H.323)
소프트웨어 호환성	• Advanced IP Services Image • Advanced Enterprise Services Image
프로토콜	• MGCP 0.1, H.323, SCCP (SRST 모드)

주문 정보

주문을 하려면 시스코 고객 담당자에게 문의하거나 시스코 웹사이트를 방문하십시오. 주문 정보는 표 6을 참조하십시오.

표 6. 주문 정보

제품명	부품번호
IP Communications High Density Digital Voice Network Module	NM-HDV2
IP Communications High Density Digital Voice Network Module with One Built-in T1/E1 Port NM-	HDV2-1T1/E1
IP Communications High Density Digital Voice Network Module with Two Built-in T1/E1 Port NM-	HDV2-1T1/E1
One-Slot IP Communications Voice/Fax Network Module	NM-HD-1V
Two-Slot IP Communications Voice/Fax Network Module	NM-HD-2V

Two-Slot IP Communications Enhanced Voice/Fax Network Module	NM-HD-2VE
Digital T1/E1 Packet Voice/Fax Network Module	NM-HDV (모든 번들 변경 포함)
30-channel Voice/Fax DSP Advanced Integration Module	AIM-VOICE-30, AIM-ATM-VOICE-30
High-Density Analog and Digital Extension Module	EVM-HD
8-Channel Packet Fax/Voice DSP Module	PVDM2-8
16-Channel Packet Fax/Voice DSP Module	PVDM2-16
32-Channel Packet Fax/Voice DSP Module	PVDM2-32
48-Channel Packet Fax/Voice DSP Module	PVDM2-48
64-Channel Packet Fax/Voice DSP Module	PVDM2-64

추가 정보

시스코 미디어 인증 및 암호화 기능에 대한 자세한 정보는 다음 웹사이트를 방문하거나 시스코 고객 담당자에게 문의하십시오.

Cisco IOS MGCP 게이트웨이의 음성 보안 기능

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_11/qtsecure.htm

안전한 Cisco Unified Survivable Remote Site Telephony:

http://lbg.cisco.com/ucdit/cc/td/doc/product/software/ios123/123newft/123t/123t_106/sr_scur1.htm


www.cisco.com/kr

2007-05-02

■ Gold SI 파트너	· (주)데이타크레프트 코리아	02-6256-7000	· 쌍용정보통신(주)	02-2262-8114	· 삼성네트웍스(주)	02-3415-6754
	· (주)인네트	02-3451-5300	· 에스넷시스템(주)	02-3469-2400	· (주)LG 씨엔에스	02-6363-5000
	· (주)인성정보	02-3400-7000	· (주)랑네트	02-6675-1216	· SK 씨앤씨(주)	02-6400-0114
	· 한국 IBM	02-3781-7800	· 한국후지쯔(주)	02-3787-6000	· 한국 HP	02-2199-0114
	· (주)콤텍 시스템	02-3289-0114				
■ Silver SI 파트너	· 포스데이타주식회사	031-779-2114	· 한국 NCR	02-3279-4300		
■ Uncertified SI 파트너	· 오토에버시스템즈	02-3458-1400				
■ Local 디스트리뷰터	· (주)소프트뱅크 커머스 코리아	02-2187-0176	· (주)영우디지털	02-6004-7050	· (주) SK 네트워크	02-3788-3673
	· (주)아이넷뱅크	02-3400-7490				
■ IPCC 전문파트너	· 한국 IBM	02-3781-7114	· (주)인성정보	02-3400-7000	· GS 네오텍	02-2630-5280
	· 한국 HP	02-2199-4272	· 삼성네트웍스(주)	02-3415-6754		
■ Optical 전문 파트너	· (주)LG 씨엔에스	02-6363-5000	· 미리넷(주)	02-2142-2800	· 에스넷시스템(주)	02-3469-2900
■ IP Communication 전문 파트너	· 크리스넷	1566-2837	· (주)패킷시스템즈 코리아	02-558-7170	· 유엔넷시스템즈(주)	02-565-7034
■ Security 전문파트너	· 인포섹(주)	02-2104-5114	· (주)티아이에스에스	051-743-5940		
	· (주)나래시스템	02-2199-5533				
■ WLAN 전문파트너	· (주)에어키	02-584-3717	· 사운드파이프코리아(주)	02-568-5029	· (주)해창시스템	031-343-7800
■ Storage 전문 파트너	· (주)패킷시스템즈 코리아	02-558-7170	· 메크로임팩트	02-3446-3508		