Secure Voice on Cisco Integrated Services Routers

Media authentication and encryption features on the Cisco Systems® portfolio of integrated services routers help ensure that voice conversations are protected from eavesdropping, information theft, media tampering, toll fraud, denial of service and other attacks.

The Cisco® Unified Communications system of voice, video and IP communications products and applications enables organizations to communicate more effectively-enabling them to streamline business processes, reach the right resource the first time and impact the top and bottom line. The Cisco Unified Communications portfolio is an integral part of the Cisco Business Communications Solution-an integrated solution for organizations of all sizes which also includes network infrastructure, security, and network management products, wireless connectivity, and a lifecycle services approach, along with flexible deployment and outsourced management options, end-user and partner financing packages, and third party communications applications.

Product Overview

Businesses are moving to IP communications to reduce operational expenses, increase productivity, and simplify network administration. The Cisco integrated services router portfolio i.e., Cisco 1861, Cisco 2800 Series, Cisco 2900 Series, Cisco 3800 Series, Cisco 3900 Series and VG-2xx Series platforms deliver powerful and scalable Unified Communications solutions for the most demanding enterprise environments.

A wide range of Unified Communications security features are available on Cisco integrated services routers to deliver high levels of security protection for businesses deploying IP communications solutions. The Cisco multilayer offering, based on the self-defending network model, starts with the network itself and extends to the endpoints and applications. The SAFE Blueprint from Cisco presents a detailed framework of best practices and tools to help secure business networks.

Media encryption using Secure Real-Time Transport Protocol (SRTP) delivers protection by encrypting the voice conversation, rendering it unintelligible to internal or external eavesdroppers who have gained access to the voice domain. Designed for voice packets, SRTP supports the AES encryption algorithm and is an IETF RFC 3711 standard.

Media encryption on Cisco routers works together with Cisco Unified Communications Manager (CUCM) software and the media encryption feature on Cisco Unified IP phones to secure both gateway-to-gateway calls and IP phone-to-gateway calls. This enables secure analog phone calls, secure fax calls, or secure calls among IP Phones and/or between an IP phone and the gateway, depending on the gateway interface type the media is terminated on. Voice encryption keys derived by Cisco Unified Communications Manager are securely sent by encrypted signaling path to Cisco Unified IP phones and Cisco Unified Border Element (CUBE) through the use of Transport Layer Security (TLS) and to gateways over IP Security (IPSec) protected links.

Media encryption features on Cisco routers are available beginning with Cisco IOS® Software release 12.3(11)T2 on 1861 & 2800/3800 series platforms with an upgrade to the Advanced Enterprise Services or Advanced IP Services IOS Software Feature Sets, and Universal Image release 15.0(1)M on 2900/3900 series platforms with UC and Security License PAK. The features are enabled on digital signal processing modules (DSPs) available on the PVDM2, PVDM3 and some NMs.

Features Table

Table 1 provides details on the media authentication and encryption solution.

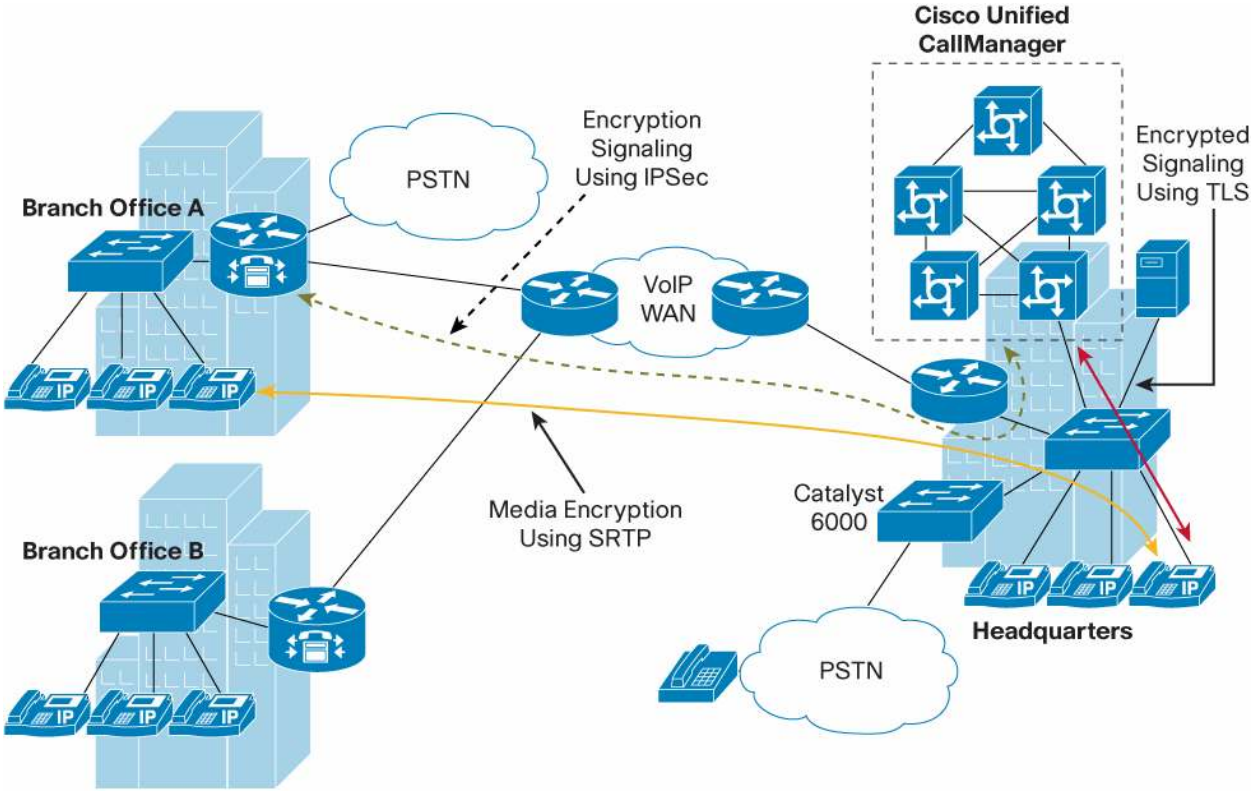
Table 1. Features Table

Authentication and Encryption Features	• Media encryption of voice RTP streams using SRTP • Exchange of RTP Control Protocol (RTCP) information using secure RTCP • SRTP to RTP fallback for calls between secure and insecure endpoints • Secure calls supported in Cisco Unified Survivable Remote Site Telephony (SRST) mode during WAN failover • Compressed RTP (CRTP) supported with media encrypted calls using SRTP
Authentication and Encryption Algorithm	• Supports AES-128 encryption algorithm • Supports the HMAC secure hash authentication algorithm (SHA 1)
Signaling Authentication and Encryption Features	• Gateway to Cisco Unified Communications Manager signaling and encryption uses IPSec for Media Gateway Control Protocol (MGCP), H.323 and SIP gateways • IP phone to Cisco Unified Survivable Remote Site Telephony router signaling and encryption uses TLS (Transport Layer Security)
Protocol Support	• MGCP 0.1 (supports MGCP gateways with Cisco Unified Communications Manager) • H.323 (supported on H.323 gateways and CUBE; Cisco Unified Communications Manager interoperability is optional) • Session Initiation Protocol (SIP) • SCCP (Cisco Unified IP Phone) in SRST mode
Module Support	• Any module that has PVDM2, PVDM3 and/or built-in DSP
Codec Support	• G.711, G.729A, and G.729

Applications

Media authentication and encryption on Cisco integrated services routers, together with media encryption on Cisco Unified IP phones and Cisco Unified Communications Manager, provides a highly secure environment for IP communications across a WAN or LAN. As illustrated in Figure 1, SRTP is used to encrypt voice calls placed on voice gateway network modules in branch office A. This provides secure calls from analog phone to analog phone, or fax machine to fax machine, within the office. Similarly, secure calls are enabled from time-division multiplexing (TDM) endpoints or analog phones at branch office A to Cisco Unified IP phones at the headquarters. The signaling between the gateway at branch office A and Cisco Unified Communications Manager is secured using IPSec, and the signaling between the IP phones at headquarters and Cisco Unified Communications Manager is secured using TLS.

Figure 1. Media Authentication and Encryption



Key Features and Benefits

Media Authentication and Encryption

Media encryption currently delivers end-to-end encryption for voice calls between Cisco Unified IP phones. The introduction of media encryption on Cisco routers adds the ability to place secure IP phone-to-gateway and gateway-to-gateway calls. Callers can now place encrypted calls to the PSTN gateway using IETF RFC3711 standards-based SRTP. SRTP encrypts only the payload of a voice packet without adding additional encryption headers. Because of this, an SRTP-encrypted voice packet is almost indistinguishable from an RTP voice packet, allowing features like quality of service (QoS) and compressed RTP to be supported without any additional development or packet manipulation. In addition, SRTP uses the largest practical key size supported by the AES

encryption standard for increased security. Voice encryption keys are generated for each call, ensuring a higher level of security protection. Media authentication also validates the identity of the devices encrypting the calls.

Media encryption using SRTP is suitable for voice privacy and confidentiality on the LAN to protect against internal threats. In addition, media encryption can also be delivered across an IP WAN or the Internet, using the same VPN infrastructure deployed for data.

Signaling Authentication and Encryption

Signaling authentication and encryption between the gateways/CUBE and Cisco Unified Communications Manager is protected using IPSec. This ensures that signaling information such as dual tone multifrequency (DTMF) digits, passwords, PINs, and voice encryption keys are secure. Both software-based IPSec, available in Cisco IOS Software, and hardware-based IPSec using the AIM-VPN modules are supported.

Scalability of Encrypted Calls

SRTP media encryption is performed on DSP modules and not on the router CPU. This enables efficient scalability as increasing the number of voice gateway interfaces with DSPs, or increasing the number of DSPs integrated on the platforms (such as on the integrated services routers), increases the number of DSPs available for secure calls.

Efficient Delay Optimization and Channel Capacity Impact

No additional call setup delays are introduced with encrypted calls, as the key exchange is completed as part of the normal call setup and no extra messages are introduced. Voice media delay is also not introduced because SRTP media encryption is performed in the DSP, and not by the router CPU or a separate encryption engine that processes the completed voice packet.

There is no channel capacity impact for encrypted calls in G.729 and G.729a modes, and minimal impact in G.711 mode (Table 2).

Table 2. Channel Impact per DSP (ex: PVDM2-16)

Codec	Regular Voice Call/DSP	Encrypted Voice Call/DSP
G.711	16 calls	10 calls
G.729a	8 calls	8 calls
G.729	6 calls	6 calls

Management Features

Media authentication and encryption is easily configured on Cisco routers using the command-line interface (CLI). In addition, features such as a lock icon indicator on Cisco IP Phones provide visual confirmation of encryption in calls to supported gateways. If a device within the call flow does not support media encryption or the security is compromised, the lock icon disappears. CLI commands are also available to confirm and provide details about an encrypted call and to debug calls.

Security in Cisco Unified Survivable Remote Site Telephony Mode

Cisco Unified Survivable Remote Site Telephony provides call processing redundancy when connectivity to Cisco Unified Communications Manager is lost. Media authentication and encryption is supported in Cisco Unified Survivable Remote Site Telephony mode, beginning with Cisco IOS Software release 12.3(14)T for ISR and 15.0(1)M for ISR-G2, providing the ability to place secure calls within a remote branch office when the WAN link or Cisco Unified Communications Manager goes down. When the WAN link or Cisco Unified Communications Manager is restored, Cisco Unified Communications Manager resumes secure call handling capabilities. The signaling from the Cisco Unified Survivable Remote Site Telephony router to the IP phones is encrypted using TLS.

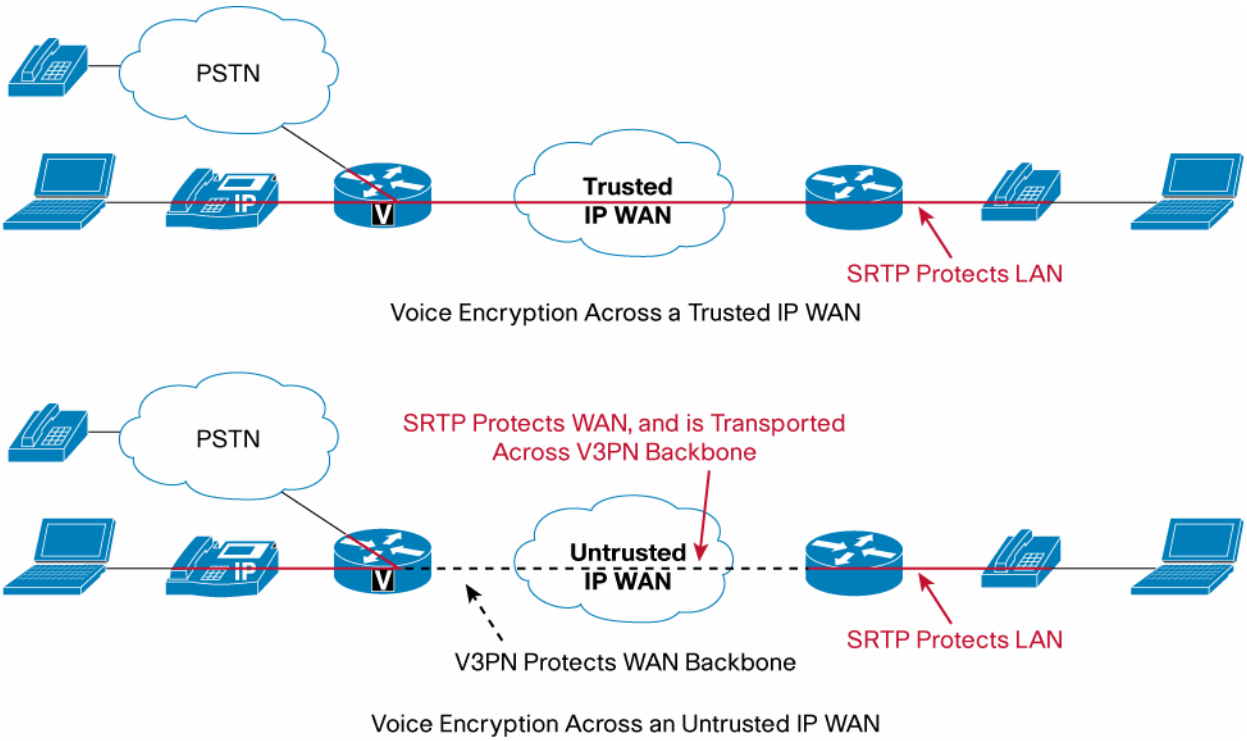
SRTP AND IPSEC VPNS

SRTP and IPSec are complementary VPN technologies. One of the key differences is that SRTP can deliver encryption from end to end, that is, from IP phone to IP phone, whereas IPSec VPN is a router-to-router tunnel-based encryption. In addition, SRTP encrypts only voice packets, whereas IPSec VPN tunnels can transport data, voice, and video (and thus are called V3PN).

This means that SRTP can add additional protection for voice traffic using an IPSec VPN.

For enterprises and small and medium-sized businesses that have a trusted WAN network, SRTP can be used to encrypt voice end to end across this network. However, most of these businesses conduct business across the Internet or across a WAN that is managed by a service provider. Therefore, the WAN may be insecure, and a VPN tunnel is used to transport data securely between branch offices. SRTP can be used to secure voice in the WAN across the same IPSec VPN network that is used for data. This is illustrated in Figure 2.

Figure 2. Secure RTP and V3PN



Feature Availability

Table 3. Feature Availability

Protocol/Feature Support	Platform Support (with Supported Modules in Table 4)	Release
MGCP Gateways (MGCP 0.1)	• Cisco 2901, 2911, 2921, 2951, 3925, and 3945 integrated services routers (ISR-G2) • Cisco 1861, 2801, 2811, 2821, 2851, 3825, and 3845 integrated services routers • Cisco AS5300/AS5400 Series Gateway • Cisco VG202/204, VG224 Analog Phone Gateway	• ISR-G2: Cisco IOS Software Release 15.0(1)M • ISR: Cisco IOS Software Release 12.3(11)T2 and Cisco Unified Communications Manager 4.1
H.323 Gateways, SIP Gateways and CUBE	• Cisco 2901, 2911, 2921, 2951, 3925, and 3945 integrated services routers (ISR-G2) • Cisco 1861, 2801, 2811, 2821, 2851, 3825, and 3845 integrated services routers • Cisco AS5300/AS5400 Series Gateway • Cisco VG224 Analog Phone Gateway • Cisco IAD 2430 Series Integrated Access Device • CUBE is supported in both flow-through and flow around mode.	• ISR-G2: Cisco IOS Universal Software Release 15.0(1)M • ISR: Cisco IOS Software Release 12.4(6)T1 • Interworking with Cisco Unified Communications Manager 5.0 is supported, but is optional
SCCP IP Phones in Cisco Unified SRST Mode	• Cisco 2901, 2911, 2921, 2951, 3925, and 3945 integrated services routers (ISR-G2) • • Cisco 2801, 2811, 2821, 2851, 3825, and 3845 integrated services routers (ISR)	• ISR-G2: Cisco IOS Software Release 15.0(1)M • ISR: Cisco IOS Software Release 12.3(14)T and Cisco Unified Communications Manager 4.1

Cisco Unified Communications Services and Support

Using the Cisco Lifecycle Services approach, Cisco Systems® and its partners offer a broad portfolio of end-to-end services to support the Cisco Unified Communications system. These services are based on proven methodologies for deploying, operating, and optimizing IP communications solutions. Upfront planning and design services, for example, can help you meet aggressive deployment schedules and minimize network disruption during implementation. Operate services reduce the risk of communications downtime with expert technical support. Optimize services enhance solution performance for operational excellence. Cisco and its partners offer a system-level service and support approach that can help you create and maintain a resilient, converged network that meets your business needs.

Conclusion

Media authentication and encryption provides an additional layer of security for enterprises and small and medium-sized businesses deploying IP communications. Voice conversations terminated on TDM or analog voice gateway ports or Cisco Unified IP phones are protected from eavesdropping, information theft, media tampering, toll fraud, denial of service and other attacks within the LAN and WAN using standards-based encryption.

Product Compatibility

Table 4. Product Compatibility

Product Compatibility	• Cisco 2901, 2911, 2921, 2951, 3925 and 3945 integrated services routers (ISR-G2) • Cisco 1861, 2801, 2811, 2821, 2851, 3825 and 3845 integrated services routers (ISR) • Cisco VG224 Analog Phone Gateway • Cisco IAD 2430 Series Integrated Access Device • Cisco Unified Communications Manager 4.1 for MCGP and SCCP (Cisco Unified SRST mode) • Cisco Unified Communications Manager 5.0 (H.323) • Cisco Unified Communications Manager 6.0 (SIP)
Software Compatibility	• Universal Image with UC and Security License PAK • Advanced IP Services Image • Advanced Enterprise Services Image
Protocols	• MGCP 0.1, H.323, SIP, SCCP (SRST mode)

Ordering Information

To place an order, contact your Cisco representative or visit the Cisco Website. See Table 5 for ordering information.

Table 5. Bundles for Ordering Information

Bundle	Description
Platform: 3900 Series Router	
C3925-VSEC/K9	Cisco 3925 Voice Sec. Bundle, PVDM3-64, UC and SEC License PAK
C3945-VSEC/K9	Cisco 3945 Voice Sec. Bundle, PVDM3-64, UC and SEC License PAK
Platform: 3800 Series Router	
C3825-35UC-VSEC/K9	3825 Voice Security Bundle with CME, CUE, and Phone licenses for 35 users, PVDM2-64,NME-CUE, Adv IP Serv, 128MB Flash and 512MB DRAM
C3845-35UC-VSEC/K9	3845 Voice Security Bundle with CME, CUE, and Phone licenses for 35 users, PVDM2-64,NME-CUE, Adv IP Serv,128MB Flash and 512MB DRAM
C3845-H-VSEC/K9	Cisco 3845 HVSEC Bundle with IOS Advanced IP Services, PVDM2-64, AIM-VPN/SSL-3, 100 User SRST License, 25 User SSL VPN License, 512 MB Flash/1GB DRAM
C3825-H-VSEC/K9	Cisco 3825 HVSEC Bundle with IOS Advanced IP Services, PVDM2-64, AIM-VPN/SSL-3, 100 User SRST License, 25 User SSL VPN License, 512 MB Flash/1GB DRAM
C3825-VSEC/K9	3825 Voice Security Bundle, PVDM2-64, Adv IP Serv, 128F/512D
C3825-VSEC-CCME/K9	3825 VSEC Bundle with PVDM2-64, FL-CCME-168, Adv IP Serv, 128F/512D
C3825-VSEC-SRST/K9	3825 VSEC Bundle with PVDM2-64, FL-SRST-168, Adv IP Serv, 128F/512D
C3845-VSEC/K9	3845 Voice Security Bundle, PVDM2-64, Adv IP Serv, 128F/512D
C3845-VSEC-CCME/K9	3845 VSEC Bundle with PVDM2-64, FL-CCME-240, Adv IP Serv, 128F/512D
C3845-VSEC-SRST/K9	3845 VSEC Bundle with PVDM2-64, FL-SRST-240, Adv IP Serv, 128F/512D
Platform: 2900 Series Router	
C2901-VSEC/K9	Cisco 2901 Voice Sec. Bundle, PVDM3-16, UC and SEC License PAK
C2911-VSEC/K9	Cisco 2911 Voice Sec. Bundle, PVDM3-16, UC and SEC License PAK
C2921-VSEC/K9	Cisco 2921 Voice Sec. Bundle, PVDM3-32, UC and SEC License PAK
C2951-VSEC/K9	Cisco 2951 Voice Sec. Bundle, PVDM3-32, UC and SEC License PAK
Platform: 2800 Series Router	
C2851-35UC-VSEC/K9	2851 Voice Security Bundle w/ CME, CUE, and Phone licenses for 35 users, PVDM2-48, NME-CUE, Adv IP Serv,128MB Flash and 256MB
C2821-25UC-VSEC/K9	2821 Voice Security Bundle w/ CME, CUE, and Phone licenses for 25 users, PVDM2-32, AIM-CUE, Adv IP Serv,128MB Flash and 256MB DRAM
C2811-15UC-VSEC/K9	2811 Voice Security Bundle with CME, CUE, and Phone licenses for 15 users, PVDM2-32, AIM-CUE, Adv IP Serv,128MB Flash and 256MB DRAM

Bundle	Description
C2801-10UC-VSEC/K9	2801 Voice Security Bundle with CME, CUE, and Phone licenses for 10 users, PVDM2-32, AIM-CUE, Adv IP Serv,128MB Flash and 256MB DRAM
C2851-H-VSEC/K9	Cisco 2851 HVSEC Bundle with IOS Advanced IP Services, PVDM2-48, AIM-VPN/SSL-2, 50 User SRST License, 10 User SSL VPN License, 256 MB Flash/512 MB DRAM
C2821-H-VSEC/K9	Cisco 2821 HVSEC Bundle with IOS Advanced IP Services, PVDM2-32, AIM-VPN/SSL-2, 50 User SRST License, 10 User SSL VPN License, 256 MB Flash/512 MB DRAM
C2811-H-VSEC/K9	Cisco 2811 HVSEC Bundle with IOS Advanced IP Services, PVDM2-16, AIM-VPN/SSL-2, 35 User SRST License, 10 User SSL VPN License, 256 MB Flash/512 MB DRAM
C2801-H-VSEC/K9	Cisco 2801 HVSEC Bundle with IOS Advanced IP Services, PVDM2-8, AIM-VPN/SSL-2, 25 User SRST License, 10 User SSL VPN License, 128 MB Flash/384 MB DRAM
C2801-VSEC/K9	2801 Voice Security Bundle, PVDM2-8, Adv IP Serv, 64F/256D
C2801-VSEC-CCME/K9	2801 VSEC Bundle with PVDM2-8, FL-CCME-24, Adv IP Serv, 128F/256D
C2801-VSEC-SRST/K9	2801 VSEC Bundle with PVDM2-8, FL-SRST-24, Adv IP Serv, 128F/256D
C2811-VSEC/K9	2811 Voice Security Bundle, PVDM2-16, Adv IP Serv, 64F/256D
C2811-VSEC-CCME/K9	2811 VSEC Bundle with PVDM2-16, FL-CCME-36, Adv IP Serv, 128F/256D
C2811-VSEC-SRST/K9	2811 VSEC Bundle with PVDM2-16, FL-SRST-36, Adv IP Serv, 128F/256D
C2821-VSEC/K9	2821 Voice Security Bundle, PVDM2-32, Adv IP Serv, 64F/256D
C2821-VSEC-CCME/K9	2821 VSEC Bundle with PVDM2-32, FL-CCME-48, Adv IP Serv, 128F/256D
C2821-VSEC-SRST/K9	2821 VSEC Bundle with PVDM2-32, FL-SRST-48, Adv IP Serv, 128F/256D
C2851-VSEC/K9	2851 Voice Security Bundle, PVDM2-48,Adv IP Serv,64F/256D
C2851-VSEC-CCME/K9	2851 VSEC Bundle with PVDM2-48, FL-CCME-96,Adv IP Serv,128F/256D
C2851-VSEC-SRST/K9	2851 VSEC Bundle with PVDM2-48, FL-SRST-96,Adv IP Serv,128F/256D
Platform: 1800 Series Router	
C1861-4F-VSEC/K9	1861,8-user CME,CUE,Ph Lic,4FXS,4FXO,8xPOE,HWIC slot,Adv IP
C1861-2B-VSEC/K9	1861,8-user CME,CUE,Ph Lic,4FXS,2BRI,8xPOE,HWIC slot,Adv IP

Cisco and Partner Services for the Branch

Services from Cisco and our certified partners can help you transform the branch experience and accelerate business innovation and growth in the Borderless Network. We have the depth and breadth of expertise to create a clear, replicable, optimized branch footprint across technologies. Planning and design services align technology with business goals and can increase the accuracy, speed, and efficiency of deployment. Technical services help improve operational efficiency, save money, and mitigate risk. Optimization services are designed to continuously improve performance and help your team succeed with new technologies. For more information, visit http://www.cisco.com/go/services.

For More Information

For more information about the Cisco media authentication and encryption feature, visit the following links or contact your local account representative.

Secure Unified Communication: http://www.cisco.com/go/secureuc

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C78-328543-03 1/10