Cisco VPN and Encryption Solutions for Secure Unified Communications Confidentiality

Positioning Guide

Confidentiality of data has long been a security challenge for enterprises. In a unified communications context, confidentiality most often relates to threats such as eavesdropping, where an attacker is able to intercept, listen to, and record voice traffic. Eavesdropping has been an issue in the traditional PBX since the inception of telecommunications, but the move toward converged, IP-based voice systems has heightened concerns about the potential loss of confidentiality. Although the risks associated with eavesdropping have not changed, the means to mitigate the risks have become varied. Most commonly, organizations look to encryption technology solutions to mitigate risks associated with eavesdropping.

This guide discusses the differing encryption solutions available for providing confidentiality in a unified communications deployment. It is important to note that the scope is not exclusive to IP voice. Rather, the guide encompasses the increasing number of other communication and collaboration mediums used by organizations, such as video and instant messaging.

The guide begins with a discussion of the broad topological options before considering the different architectures that make up the potential solutions. Features and benefits of each solution are discussed, including the positioning of each solution based on typical confidentiality requirements. Finally, the guide provides a comparison of Cisco® security platforms to assist in the selection of the appropriate platform for a given solution.

Confidentiality in a Secure Unified Communications Deployment

Concerns over the security of the underlying IP infrastructure in a unified communications deployment have heightened interest in applying confidentiality measures to media streams. Often discussed in terms of business risk, loss of confidentiality can mean the loss or theft of sensitive company information. This can lead to related business impact such as a loss of public reputation or a breach of industry compliance regulations.

In traditional PSTN or PBX networks, confidentiality is based entirely on the integrity of the systems themselves. If an attacker were able to gain access to a node within the network they would, in general, be able to easily listen to and record conversations. In unified communications, the deployment of voice and data services on a single converged network platform suggests that reliance on a closed network based on the integrity of the system is insufficient to reduce the risks of eavesdropping. Instead, alternative risk mitigation options are available, such as encryption and authentication schemes to ensure that the voice media cannot be understood if it is intercepted. This is in stark contrast to existing PBX systems, where encryption services are rare.

The encryption options described in this document in conjunction with other security countermeasures can provide an equal and arguably more confidential communications solution than those available in a traditional PBX environment.

Secure Unified Communications Topologies: Internal Network and Remote Access

To determine the unified communications confidentiality requirements of an organization, it is important to distinguish between internal network requirements and remote-access requirements. In remote-access situations, the unified communications solution will not use the traditional PSTN; it will either use SIP trunk services from a service provider or the Internet as the transport medium. In internal network situations, most organizations have a security policy requiring the encryption of confidential communications, be they data or voice. The decision of which solution to deploy

should be made within the context of the organization's existing remote-access security solutions, ideally using architectures that have been deployed for data applications.

The case for applying confidentiality to unified communications endpoints located on the internal network is usually less persuasive and will depend on an organization's evaluation of the risks from an internal threat. If the loss of confidentiality through internal employees intercepting voice calls to other employees is a significant risk, deploying encryption services from some or all of the IP phones may be necessary. Encryption for remote access is common, but the same is not true for internal network deployments, which are usually driven by the need for compliance with industry regulations or a specific internal security policy.

Architecture Options: VPN and Native Voice Encryption Solutions

Several common cryptographic algorithms and authentication schemas are used to provide confidentiality, such as 128- or 256-bit Advanced Encryption Standard (AES) or Secure Hash Algorithm (SHA) 1 or 2. Within a confidentiality framework, all these schemas can be divided into two broad categories for unified communications: VPN and native voice encryption solutions.

VPN solutions are usually application- and platform-independent, providing confidentiality as a service. These solutions use a single architecture to provide encryption for both voice and data communications. Typically, these solutions are not an integrated part of the platforms deployed specifically for unified communications, such as Cisco Unified Communications Manager. These solutions are most commonly deployed on VPN routers and security appliances to secure communications between remote sites and users, and are often part of a combined service for voice and data.

Native voice encryption solutions are inherent within the unified communications system itself. Fully integrated and specific to IP voice traffic, the protocols and architecture used are optimized to support confidentiality for voice media. These solutions are most commonly employed to provide confidentiality to internal network deployments.

Confidentiality Positioning Guide: Overview

Table 1 illustrates how the two broad architectural approaches to unified communications confidentiality relate to the three key topologies that an organization is likely to use. Further details on these architectures are covered in the subsequent sections of this document.

Table 1. Architectural Approaches to Unified Communications Confidentiality

Architecture	Remote Access	Site to Site	Campus Network
Generic VPN	Common	Common	Rare
Native Voice Encryption	Sometimes (usually hybrid solutions)	Sometimes	Common

VPN Solutions: Converged Voice and Data VPNs

VPN solutions are designed to secure data confidentiality for IP-based applications. For unified communications solutions that integrate voice, video, and data applications running over a common IP infrastructure, it is possible to provide confidentiality by using IP-based VPN services. Typically, these solutions use well-understood protocols such as SSL and IPsec. These protocols usually incorporate recognized encryption algorithms such as AES, Triple Data Encryption Standard (3DES), and Message Digest 5 (MD5), or SHA 1 or 2 for peer and packet authentication.

As unified communications solutions such as presence and instant messaging integrate more data applications into the unified communications architecture, converged confidentiality architectures like IPsec and SSL have become more attractive and are increasingly being considered as part of a unified communications deployment.

VPN Benefits and Drawbacks

VPN Benefits

- Ideal for securing the increasing number of data applications within a unified communications infrastructure, including presence, SMS, and integrated messaging
- Simplified management and deployment of confidentiality solutions for unified communications and non-unified-communications networked applications
- Possible use of existing VPN architectures deployed for data services
- Greater scalability with certain VPN architectures (site to site)

VPN Drawbacks

- VPN protocols such as SSL and IPsec may add additional delay to voice media traffic (Real-Time Transport Protocol [RTP]) due to:
  - The packet overhead of IPsec and SSL
  - TCP-based transport of IPsec and SSL, where the retransmission of lost packets introduces additional delay (although most IPsec/SSL clients can now use User Datagram Protocol [UDP] as a transport instead)

VPN Solutions: Site-to-Site and Remote-Access VPN

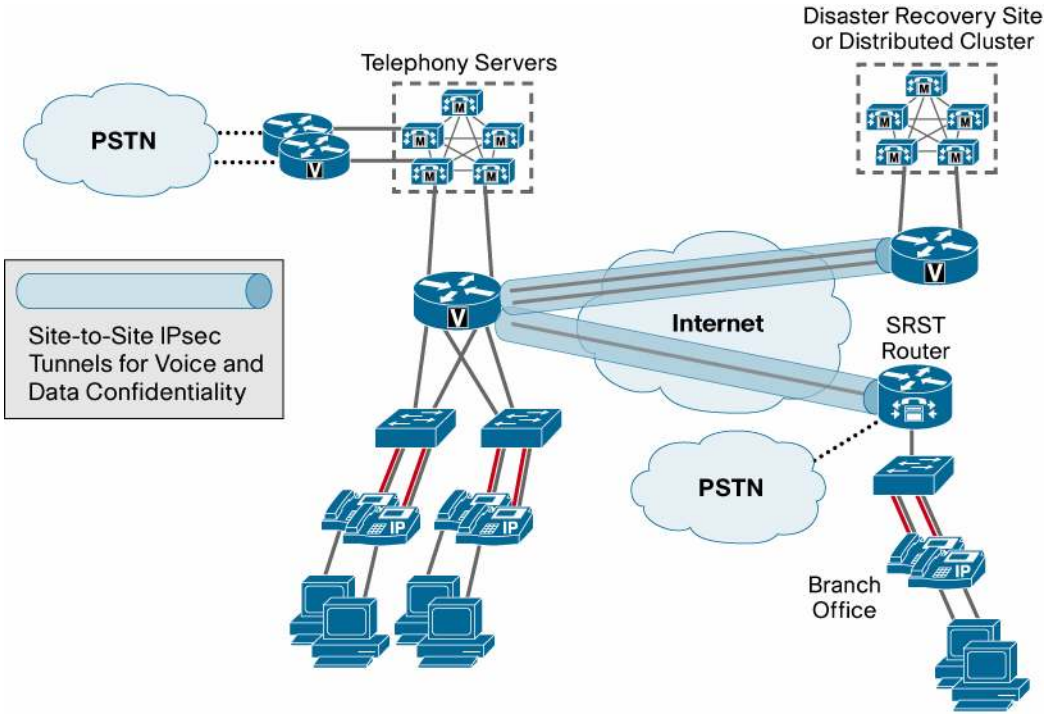
Several VPN architectures address various deployment scenarios. These can be divided into two topological categories: site-to-site and remote-access VPN.

Site-to-Site VPN

When an organization requires confidentiality of communication over WAN links, IPsec architectures, often using an underlying routed network, provide a scalable confidentiality solution. IPsec provides network-layer confidentiality, allowing the transport of both voice and data across the VPN with quality of service (QoS) markings being preserved from the original headers. This enables differentiated QoS services to be applied to the voice even though it will share the same VPN tunnel with the data applications. This ensures that voice packets can achieve the necessary quality metrics of latency and jitter required to maintain the quality of the call.

Cisco offers several innovative IPsec-based site-to-site VPN solutions that provide scalable, secure alternatives to private WAN connectivity. These architectures are most often applied to unified communications networks that seek to connect remote sites to centralized call processing architectures that centrally consolidate PSTN connectivity. In these site-to-site scenarios, the confidentiality applied to converged voice and data applications is applied by network devices such as VPN-enabled routers on behalf of the endpoints (Figure 1). This solution provides a more scalable and efficient use of resources by minimizing the number of encrypted sessions that need to be established. For securing voice traffic between sites, these IPsec-based architectures are preferable to native phone encryption solutions.

Figure 1. Site-to-Site VPN Architecture



Site-to-Site VPN Architectures and Scenarios

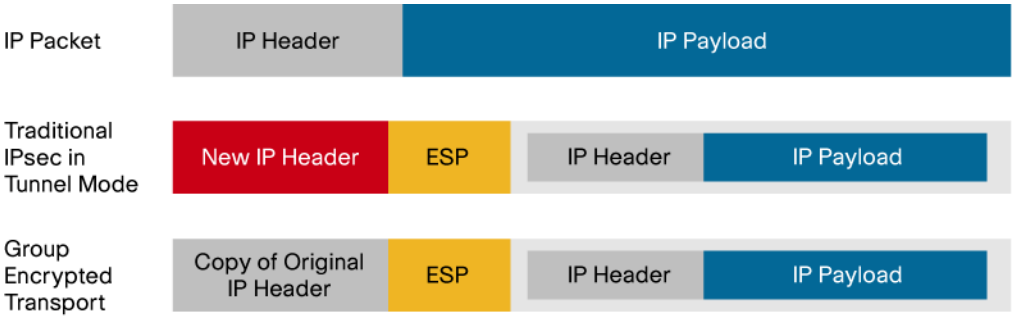
Two key site-to-site IPsec architectures developed by Cisco are Group Encrypted Transport VPN (GET VPN) and Dynamic Multipoint VPN (DMVPN). GET VPN is a Cisco IPsec architecture designed to deliver converged VPN services across MPLS networks that provide the underlying intersite connectivity. DMVPN is more suitable for site-to-site connectivity provided through public Internet connections.

Site-to-Site VPN: GET VPN

Increasingly, customers who have moved to MPLS WAN architectures as part of managed WAN services expect service providers to provide the necessary QoS guarantees for critical traffic such as IP voice. Although many customers are satisfied with the logical separation that MPLS provides, there can be requirements for providing overlay encrypted VPN solutions as a supplementary security service. A common issue with enterprises providing their own IPsec VPN overlay architectures has been the potential for disconnection between the enterprise routing and QoS domain and that of the service provider's MPLS network. Native IPsec VPNs encapsulate the original traffic in logical IPsec tunnel packets and are able to preserve the original QoS markings of the original packet. However, this still results in a separate overlay architecture that can become inconsistent with the traffic engineering of the underlying MPLS network. This can lead to suboptimal routing of traffic, which can cause unnecessary packet delay for the voice traffic.

GET VPN is a unique Cisco IPsec VPN architecture that enables the deployment of encryption services for MPLS deployments. Rather than encapsulate the packets within an IPsec tunnel, GET VPN preserves the original header, complete with QoS settings, to ensure consistency with the MPLS provider's underlying architecture (Figure 2).

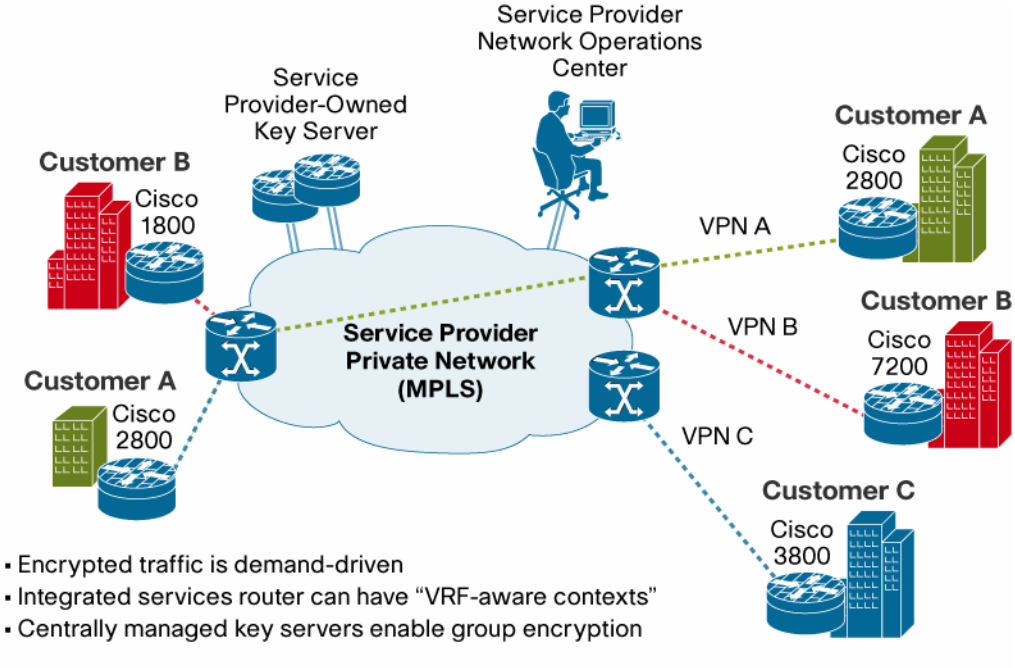
Figure 2. GET VPN Headers Enable Encryption in MPLS Deployments



For scenarios where IP voice needs to be encrypted across MPLS WAN connections, GET VPN is the optimal solution (Figure 3).

Site-to-Site VPN Implementation Case 1: The MPLS WAN and GET VPN

Figure 3. MPLS WAN and GET VPN



For more information about GET VPN, visit http://www.cisco.com/go/getvpn.

Site-to-Site VPN: DMVPN

The Internet has become an increasingly popular medium for site-to-site connectivity in recent years. Retail enterprises with large numbers of small remote sites see the benefit of replacing expensive dedicated links with the more flexible and cost-effective Internet option. In these environments, there is a clear demand for confidentiality for both data and voice IP applications.

Challenges of using IPsec VPN for securing IP voice over the Internet include the scaling of the solution and the optimization of the media traffic flow. With large numbers of small remote sites, configuring IPsec devices for every potential site that may connect can result in scaling difficulties.

Large unwieldy configuration files create an operational “headache” when new sites are added to the architecture.

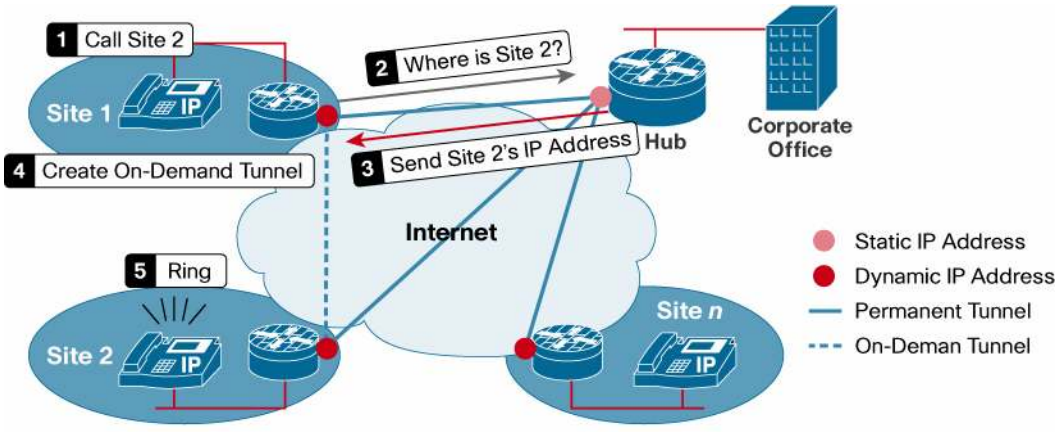
DMVPN resolves these problems by creating an on-demand IPsec architecture (Figure 4). Rather than having to statically configure each remote site to know about all the other sites within the system, DMVPN enables the remote-site VPN device to establish a single connection with the central office through a simple registration. This enables phones to register with the centralized Cisco Unified Communications Manager cluster without any need to pre-establish logical tunnels to other sites. This reduces the configuration for both the remote and central-site VPN devices and means that when a new site is brought into the system, there is no need to reconfigure the hub or other spokes. This provides a scalable, manageable IPsec VPN architecture that can easily grow to accommodate new remote sites.

From a unified communications perspective, only a single VPN connection is required for all phones at a remote site, simplifying and scaling the solution. When a phone at a remote site wishes to make a call to a phone at another site, the DMVPN architecture enables the VPN devices to dynamically provision an on-demand VPN tunnel between the two spoke sites while the phones are sending signaling to the Unified Communications Manager clusters (Figure 4). With recent enhancements, the on-demand tunnels can be established before the media begins to flow between the devices, ensuring a near-seamless and secure phone conversation provisioned by the remote VPN devices on behalf of the phones.

By enabling dynamic, on-demand tunnels, DMVPN enables the IP voice media to provide the most direct path for the encrypted voice media without the need to traverse via the hub site, which is common in most standard IPsec VPN architectures.

Site-to-Site VPN Implementation Case 2: The Centralized Office with DMVPN

Figure 4. DMVPN for Optimized Remote Site UC Connectivity



One consideration that needs to be accounted for in an Internet-based VPN solution is the inability to guarantee QoS for the voice calls. Recent releases of the DMVPN solution have provided the ability to apply QoS on a per-tunnel basis to optimize the voice experience. However, as the Internet is beyond the control of the enterprise and service provider, it is not possible to guarantee QoS.

For more information about DMVPN, visit http://www.cisco.com/go/dmvpn.

Site-to-Site VPN: Intercluster Trunks and Secure Signaling

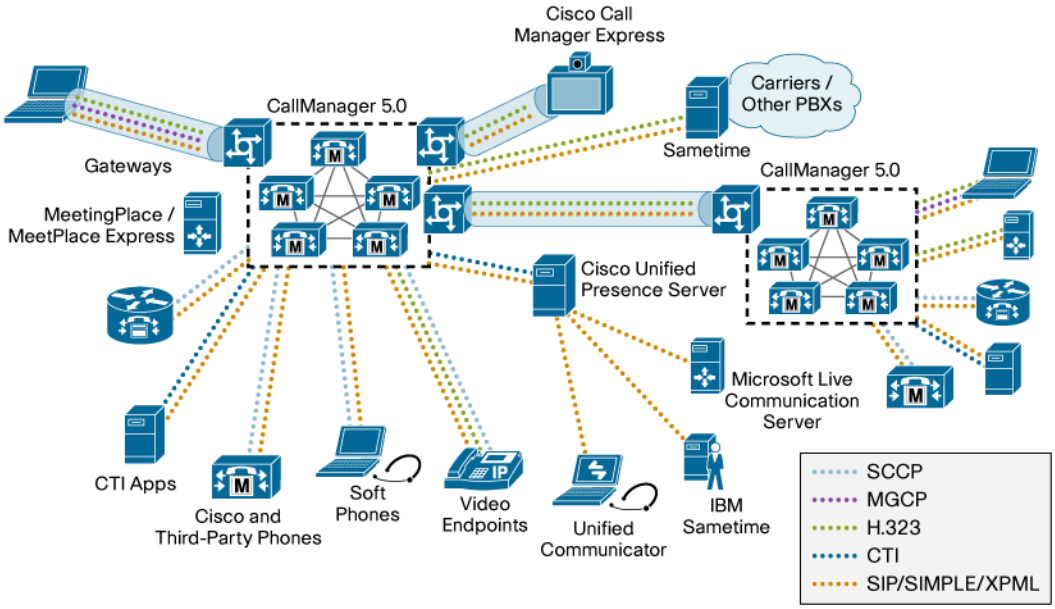
DMVPN and GET VPN provide IPsec architectures for securing IP voice and data for WAN architectures. In addition, IPsec VPN services are an appropriate means to provide confidentiality specific to voice signaling between Unified Communications Manager clusters. Signaling information is critical to the operation of enterprise unified communications systems, and ensuring the integrity and confidentiality of the signaling data is a basic security principle to maintain system availability.

Within Cisco Unified Communications Manager deployments, IPsec can be used to establish encrypted connections to other Communications Manager clusters (intercluster trunks) or to voice gateways (Figure 5). IPsec not only encrypts the connections, but also ensures that the integrity of each signaling packet is maintained in transit.

One design option that can relieve the burden of configuring encryption from each Communications Manager in a cluster is to offload the IPsec services to network devices, such as routers. The routers are usually positioned between the Communications Manager and the connection to the gateway or cluster at the other site, and are configured to classify the voice signaling traffic and to encrypt the signaling before it transits the untrusted network (Figure 5).

Site-to-Site VPN Implementation Case 3: Securing Intercluster Trunks and Voice Gateways

Figure 5. IPsec Site-to-Site VPN for Secure Intersite Signaling



Using Routers to Secure Traffic to Gateways and Between Clusters

Remote-Access VPN

Teleworking and mobile computing requirements for unified communications can be resolved using existing remote-access VPN architectures. IPsec and SSL provide solutions for secure remote connectivity. The solutions support a variety of topologies, ranging from home or teleworking solutions at fixed locations to mobile solutions using wireless technologies. Increased flexibility and business productivity are clear drivers for providing solutions for data applications.

Customers are increasingly looking to add unified communications to these services to avoid having to support separate remote-access voice and data solutions. This reduces the overall total cost of ownership and provides an integrated architecture for small office/home office workers.

Remote-Access VPN: Easy VPN

For fixed locations, the Cisco Easy VPN solution uses IPsec to provide remote-access encryption solutions for unified communications. The architecture supports both software- and hardware-based clients, allowing organizations to support a range of remote-access requirements. The underlying use of IPsec enables the copying of the type of service field bits from the original voice packets to the encrypted packet headers, which can be used to prioritize the voice over the data traffic. However, organizations are increasingly using Internet-based rather than service-provider-based connectivity to reduce cost. The impact on voice communications within a teleworker unified communications solution is that there is no longer a guarantee of service, so although voice can be prioritized as it leaves the home office network, there is no guarantee of service while it traverses the public Internet. This is true, regardless of whether encryption is enabled or not. The increasing use of consumer voice clients such as Skype and Vonage that use the Internet as the transport infrastructure suggests that the trend toward cost savings will continue.

Enterprises that require guaranteed levels of service should use a service-provider-provisioned service and could then use the prioritization of voice within the Easy VPN solution.

For more information on Cisco Easy VPN, visit http://www.cisco.com/go/easyvpn.

For more details on how Easy VPN can be deployed to support unified communications, a detailed guide illustrating the design scenarios, features, and benefits is available at http://www.cisco.com/go/secureuc.

Remote-Access VPN: SSL VPN

SSL is the most popular session-layer protocol for protecting e-commerce and front-ended encryption service for web-based applications. In recent years, the technology has evolved to provide secure remote-access connectivity for businesses. SSL for remote access generally requires the downloading of an SSL tunnel client to enable seamless encryption for all applications running on a remote client machine, though some solutions only require a web-browser-based connection.

In unified communications terms, the solution exhibits many of the same attributes as an IPsec solution. Both typically rely on TCP as the underlying transport protocol and can provide a single encrypted tunnel in which to secure voice and data. However, the perceived ease of deployment and management of SSL VPNs, in particular for soft client solutions, has led to SSL being adopted to provide a converged VPN solution for unified communications.

For more details on how SSL VPN can be deployed on Cisco IOS® Software-based routers to support unified communications, a detailed guide illustrating the design scenarios, features, and benefits is available here http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6657/white_paper_securing_voice_traffic_with_cisco_ios_ssl_vpn.html.

For more details on how SSL VPN can be deployed on Cisco ASA appliances to support unified communications, a detailed guide illustrating the design scenarios, features, and benefits is available here http://www.cisco.com/go/secureuc.

Cisco Virtual Office (CVO)

Cisco has embraced DMVPN and Easy VPN as a foundation for its own internal teleworker solution: the Cisco Virtual Office. Targeted at providing an enterprise-class teleworking solution for data and unified communications requirements, the Cisco Virtual Office is the recommended solution for fixed location telecommuting.

For more information on the Cisco Virtual Office, visit http://www.cisco.com/go/cvo.

VPN Summary

VPN technologies are often suitable for providing unified communications confidentiality, usually as part of a generic VPN architecture for voice and data. Although there are drawbacks to the use of a generic VPN architecture, the cost and manageability benefits will make it attractive, especially in remote-access and site-to-site deployments. For internal campus deployments, native phone encryption solutions are likely to be more appropriate.

Native Voice Encryption Solutions (TLS/SRTP)

In contrast to generic VPN architectures, native voice encryption solutions provide confidentiality from within the unified communications system itself. Rather than applying the encryption and authentication at the network layer, these solutions are application-specific and are targeted primarily to protect voice media and signaling. Native voice encryption solutions are used within Cisco Unified Communications Manager to provide the confidentiality for Cisco voice communications from Cisco desktop phones.

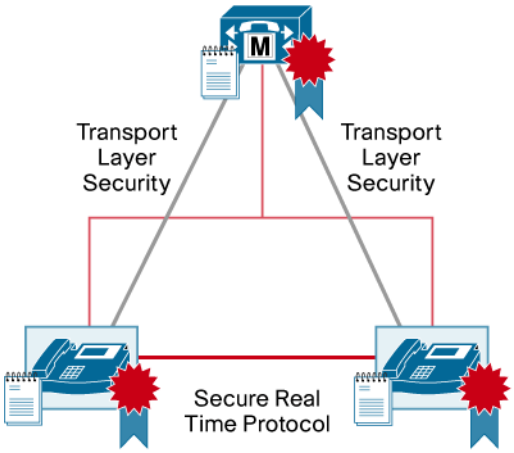
Native Voice Encryption Services for the Internal Network: TLS/SRTP

The most common solution for confidentiality within internal network unified communications deployments is to use the native voice encryption functions within the unified communications system itself. In the case of Cisco Unified Communications Manager, this is an implementation of Transport Layer Security (TLS) and Secure Real Time Protocol (SRTP). The signaling between the endpoint and the unified communications infrastructure is protected by TLS while the media is protected by SRTP. Both utilize similar encryption and authentication algorithms to those used by generic VPN architectures; however, these have been adapted to suit the needs of real-time protocols such as voice (Figure 6).

For signaling, TLS provides authentication and encryption between the endpoints and Communications Manager and also to the voice gateways. Confidentiality is important, as the encryption keys used for the media are passed to the communicating endpoints through the signaling. Thus, the strength of the media confidentiality is dependent on that provided to the signaling.

SRTP is optimized to provide media encryption for real-time traffic such as voice. Using UDP as the underlying transport avoids any retransmission issues caused by lost packets. While TCP is useful for data applications to recover lost data packets, there is little benefit in resending a lost voice packet; in fact, this can impact the ability of the endpoint codecs to process out of order packets. In addition, unlike VPN protocols such as IPsec and SSL, there is very low packet overhead. With voice being sensitive to jitter and delay, both UDP transport and TLS/SRTP provide an optimized and focused solution for securing voice traffic on the internal network.

Figure 6. Native Phone Encryption



TLS/SRTP does not, however, support confidentiality for the increasing number of data applications that are deployed as part of a unified communications system. Presence information and web-based phone applications are just two examples of data applications that would not be protected by TLS/SRTP, so organizations would need to consider a VPN architecture to provide the confidentiality.

In remote-access and mobile deployments in particular, the exposure of the Communications Manager directly to the Internet would add significant risk to the deployment, but this would be required to use TLS/SRTP. To overcome this concern, network security platforms have been developed to modify TLS/SRTP to allow a trusted security device to proxy external connections before they reach the Communications Manager (see Phone Proxy below). VPN solutions, especially if already deployed for data applications, might be more suitable.

Detailed configuration guidance for native phone encryption within the Cisco Unified Communications Manager platform is available here http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_administration_guide_chapter09186a00802e470c_4container_ccmigration_09186a0080255f67.html.

A Q&A document is available for native phone encryption (TLS/SRTP) on Cisco voice gateway platforms here http://www.cisco.com/en/US/products/hw/gatecont/ps2250/products_qanda_item0900aecd8016c49f.shtml.

Secure SRST (Survivable Remote Site Telephony): Maintaining Confidentiality Under Failure Scenarios

Cisco IP phones that use encryption and are located at remote sites can communicate securely over the WAN with Cisco Unified CallManager. But if the WAN link or CallManager goes down, all communication through the remote phones could become insecure because they would re-register with the local SRST router. In order to overcome this situation, gateway routers can now function in what is called secure SRST mode. This activates when the WAN link or Cisco Unified CallManager goes down. When the WAN link or CallManager is restored, the CallManager resumes secure call-handling capabilities.

Secure SRST provides SRST with the equivalent security features an encrypted phone would have when it communicates with a Communications Manager cluster. In Secure SRST mode, the

functions are seamlessly transferred over to the SRST router that takes over the call processing for that remote site.

A secure SRST configuration example is available here http://www.cisco.com/en/US/products/sw/voicesw/ps2169/products_configuration_example09186a0080509462.shtml.

TLS/SRTP and Firewall Interoperability Considerations

Although TLS/SRTP is usually a function employed between the endpoints and the call control platform, it does have security implications for firewall deployments. In many vendor solutions, encryption and firewalling are not interoperable, forcing enterprises to choose between the two security mechanisms.

The problem lies with the requirement for the signaling to be encrypted. In most unified communications platforms the call processing agent, for reasons of performance and scalability, determines the encryption keys the endpoints will use to encrypt their media. These keys are passed to the phones in the signaling messages; therefore, it is critical to ensure that the signaling is encrypted to protect those keys from being read by an attacker. By encrypting the signaling the firewalls that are employed to protect the Communications Manager and other applications no longer have access to the information to function as a unified-communications-aware firewall. Unified communications Network Address Translation (NAT), the dynamic opening of pinholes for the media, and the application of policy and protocol conformance are all lost as the firewall is unable to decrypt the signaling.

Cisco has developed a unique feature called TLS Proxy on the ASA platform to address this specific integration issue. With TLS Proxy, the firewall is added to the Certificate Trust List (CTL) used by the phone. The trust list determines which devices the phone is allowed to establish a TLS-encrypted signaling session with. In effect, the Cisco ASA appliance, as a trusted device within the Cisco Unified Communications Manager system, is able to intercept the encrypted signaling, mutually authenticate with the endpoint, and decrypt the signaling. Once the signaling is decrypted, the appliance is able to retrieve all the necessary signaling information and apply all the inspection and policy enforcement actions. To maintain secure connectivity from end to end, the ASA appliance then initiates a secondary TLS session back to the Communications Manager. The signaling and communications between endpoint and Communications Manager remain functionally the same and the firewall is able to deliver its unified communications security services.

For more information on Cisco ASA TLS Proxy, visit http://www.cisco.com/go/secureuc.

Native Voice Encryption for Remote Access: Phone Proxy

Cisco ASA Phone Proxy enables remote Cisco IP phones to use the existing encryption functionality (TLS/SRTP) to provide confidentiality and integrity as they connect back to a Communications Manager cluster at the corporate office. Without relying on a remote device such as a router to provide these services, typically using IPsec VPN, the Cisco ASA appliance supports the casual teleworker deployment by adapting the TLS Proxy function to suit remotely deployed phones. This enables users to plug their Cisco IP phone directly into their home office DSL connection or network device and have secure calls made through the centralized Communications Manager via the Internet.

In contrast to TLS Proxy, the ASA Phone Proxy function can be configured to support encrypted remote phones without the need for the Communications Manager cluster to run in secure mode.

Internal phones that will communicate with the remote phone also do not need to have encryption enabled. This is an important consideration as most organizations do not encrypt all calls. ASA Phone Proxy provides the necessary interworking to ensure that the external phones traffic remains encrypted even if the rest of the system is not.

The ASA Phone Proxy function also manipulates the call signaling to ensure all media is routed via the ASA appliance. This allows the ASA appliance to perform decryption of encrypted media traffic from the remote phone to the unencrypted internal phone. It also ensures that the remote phone can successfully send media to internal phones that most typically use unregistered IP address ranges, such as network 10.x.x.x addresses. Without the ASA Phone Proxy forcing the media via itself, the remote phones would not be able to route the media traffic to a phone on the internal network.

The key differences between TLS Proxy and ASA Phone Proxy functions are that the ASA Phone Proxy provides decryption and proxies both the media and the signaling traffic. TLS Proxy is only concerned with decrypting and inspecting the signaling and is therefore only effective if encryption is used within the corporate network and between endpoints and Communications Managers. TLS Proxy would not be able to provide the necessary interworking required to ensure traffic is successfully routed and decrypted in a remote-access topology. Cisco ASA Phone Proxy provides these integration services to enable the deployment of Cisco IP phones outside the corporate environment.

The key benefits of the ASA Phone Proxy are that organizations can seamlessly deploy remote Cisco IP phones and use the native phone encryption to provide the confidentiality. This makes this an ideal solution for a casual teleworking environment that does not require a remote network device such as a router. The solution overcomes a range of integration issues, including routing and decryption of media from the Internet to the phones on the internal network.

Native Phone Encryption (TLS/SRTP) Benefits and Drawbacks

Native Phone Encryption (TLS/SRTP) Benefits

- Optimized for real-time traffic such as voice.
- Small packet overhead, unlike IPsec and SSL
- UDP-based transport avoids complications associated with retransmission of lost packets (which can introduce unnecessary jitter and delay)

Native Phone Encryption (TLS/SRTP) Drawbacks

- Does not provide confidentiality for the increasing number of data applications within a unified communications infrastructure, including presence, SMS, and integrated messaging
- Not integrated with existing confidentiality solutions deployed for data.
- Not supported on all client endpoints (e.g., Cisco Unified Personal Communicator)
- Does not integrate with firewall unless TLS Proxy is used
- Has security implications for remote-access client deployments unless ASA Phone Proxy is used
- Increased load on Communications Manager clusters

Native Phone Encryption (TLS/SRTP) Summary

Undeniably, native phone encryption is the appropriate architecture for providing confidentiality within the internal network and is the optimal solution for encrypting voice. Similarly, secure SRST provides security for site-to-site connections under failure scenarios. For remote access, organizations that wish to use this architecture should consider deploying ASA Phone Proxy to address some of the security implications of exposing the Communications Manager clusters to the Internet. It also provides a flexible remote access option for the increasingly common, casual teleworker requirement. Within the internal network it is important to understand the impact of employing encryption using Communications Manager and the integration of encryption with other security services, such as firewalls.

Cisco Unified Communications Confidentiality Platforms

Cisco offers several network security platforms that can support both generic VPN and native voice encryption solutions. Table 2 provides a summary of which platforms support the solutions described previously in this document.

Table 2.

Solution	Cisco IOS Software-Based Routers	Cisco ASA Adaptive Security Appliances	Cisco Unified Communications Manager/Express	Cisco Unified Communications Gateways	Cisco Unified Border Element (SBC)
Generic Site-to-Site VPN (IPsec)	Yes	Yes	–	Yes (with VSEC Security Image)	Yes (with VSEC Security Image)
GET VPN (IPsec)	Yes	No	–	Yes (with VSEC Security Image)	Yes (with VSEC Security Image)
DMVPN (IPsec)	Yes	No	–	Yes (with VSEC Security Image)	Yes (with VSEC Security Image)
Cisco Easy VPN (IPsec)	Yes	Yes	–	Yes (with VSEC Security Image)	Yes (with VSEC Security Image)
SSL VPN	Yes	Yes	–	Yes (with VSEC Security Image)	Yes (with VSEC Security Image)
Secure SRST	Yes	No	Yes	Yes	Yes
TLS Proxy	No	Yes	Yes (with ASA)	No	No
ASA Phone Proxy	No	Yes	Yes (with ASA)	No	No
Native Phone TLS/SRTP	No	Yes (via Phone/TLS Proxy)	Yes	Yes	No

For a more detailed discussion of the VPN options available with Cisco network security solutions, an online document is available at http://www.cisco.com/en/US/products/ps6635/prod_brochure09186a00801f0a72.html.

Summary

When considering confidentiality for unified communications deployments, the first step should be to evaluate the risk of not implementing these countermeasures. This will vary between organizations but will provide the benchmark of what measures need to be considered, if any at all. If confidentiality is required to mitigate these risks, it is important to consider which topological environments the solution needs to apply to. Based on these assessments, set within the context of any existing confidentiality deployments for data applications, an organization can evaluate the benefits of using generic or native encryption architectures to maintain confidentiality.

VPN solutions such as IPsec and SSL provide an ideal solution for a converged confidentiality architecture to support voice and data applications. Routinely used for site-to-site connections but

also used to provide confidentiality for remote desktops running soft clients, the Cisco VPN architectures have been enhanced to ensure that the requirements for both voice and data can be met.

Native phone encryption is evolving to meet the needs of casual remote-access teleworking, moving beyond the internal enterprise network where it is most commonly deployed. With enhancements such as the ASA Phone Proxy, native phone encryption solutions (TLS/SRTP) have been extended to enable remote Cisco IP phones to connect securely across the Internet and other external networks.

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 C07-494660-00 09/08