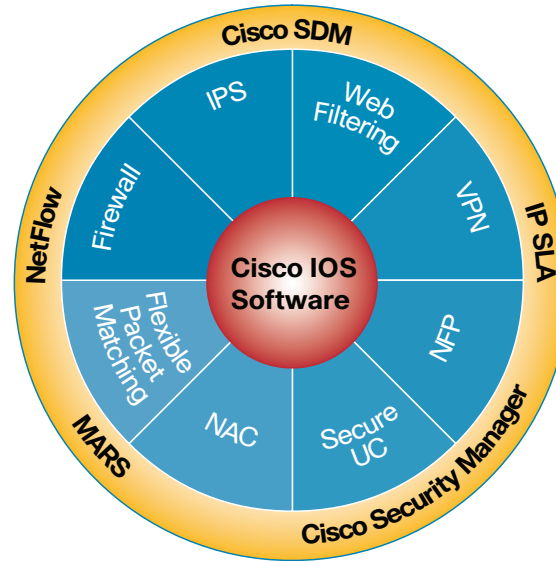


In a unified communications context, confidentiality usually relates to threats such as eavesdropping, where an attacker is able to intercept, listen to, and record voice conversations. From a business risk standpoint, loss of confidentiality can mean the loss or theft of sensitive company information, such as customer credit card numbers. This can lead to breaches of industry compliance regulations, consequent public disclosure, and loss of public reputation.

Eavesdropping has also been an issue in traditional PBX environments. If an attacker were able to gain access to a node within the PBX network they would be able to easily listen to and record conversations. Ensuring confidentiality in a PBX environment depended on limiting physical access to the devices and phone lines, and on the integrity of the systems themselves.

In a converged, IP-based unified communications solution, threats emerge from packet-based eavesdropping tools. An attacker uses these tools to intercept a stream of voice packets, listening and recording in real time, or assembling the packets and replaying them later. Measures such as placing phones in separate VLANs that are not accessible to PCs make it difficult to gain access to the voice packets. And there are no guarantees, even with such arrangements.

To ensure confidentiality in a unified communications deployment, organizations must employ strong authentication and encryption mechanisms that prevent voice conversations from being deciphered even when intercepted, thereby providing even higher levels of confidential communications than available with traditional PBXs.



Confidentiality Options

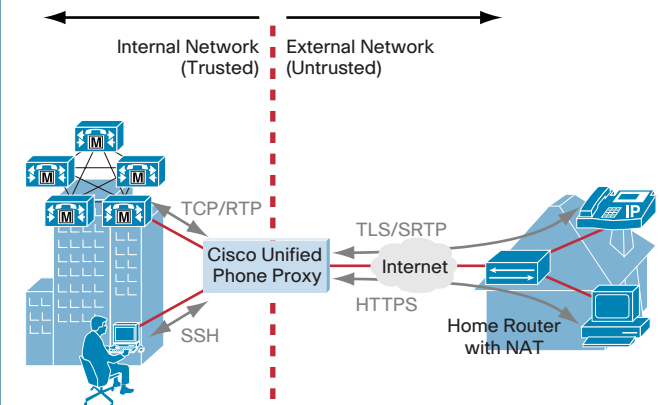
In corporate campus environments, native voice authentication and encryption schemes within the unified communications endpoints themselves are commonly deployed in order to secure voice signaling and media. For remote links, extending unified communications authentication and encryption is even more paramount—the ability to control access at remote sites is difficult, and is mandatory where Internet-based access is used. Native unified communications schemes have disadvantages: they are limited to voice traffic and specifically to phone devices. Remote sites usually require data traffic from a variety of devices to be encrypted as well.

For these reasons, it is common to use IP Security (IPsec) VPN and Secure Sockets Layer (SSL) VPN based authentication and encryption to secure remote WAN or Internet links, addressing data and unified communications at the same time.

Cisco Unified Phone Proxy

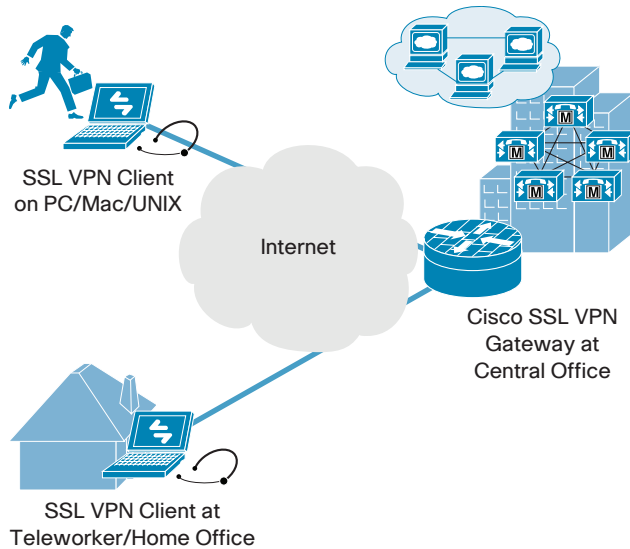
Cisco Unified Phone Proxy is a native unified communications confidentiality solution in which authentication and encryption are performed by the unified communications endpoints (such as an encryption-capable Cisco IP phone at a remote location). The IP phone uses Transport Layer Security (TLS) and Secure Real-Time Transport Protocol (SRTP) to encrypt the signaling and media, respectively. This allows voice calls to securely transit shared or public infrastructures such as the Internet. At the other end of the link, the Cisco Unified Phone Proxy platform terminates the encryption on behalf of the Cisco Unified Communications Manager.

While Cisco Unified Phone Proxy provides an uninterrupted user experience for voice users, it is limited to IP phones. It does not provide support for remote fax machines, printers, or computers, or for small office or home office (teleworker) deployments.



SSL VPN

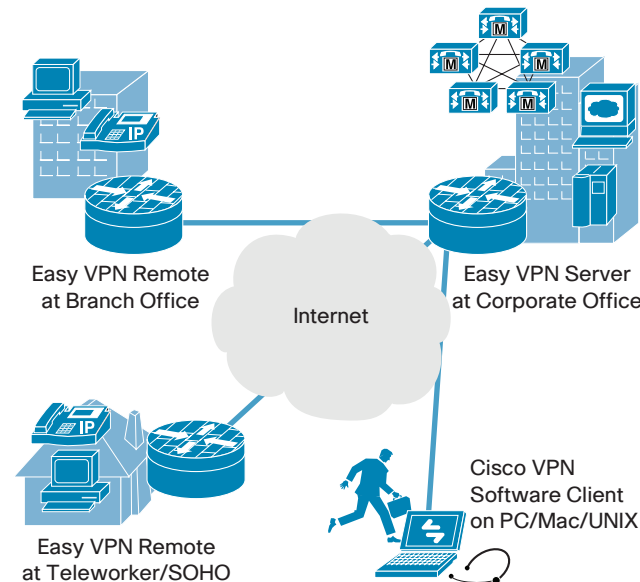
SSL VPNs encrypt soft phone communications, allowing mobile users to access voice applications while traveling. SSL VPN client software can be deployed easily. End users access a secure Website and install the client software; once installed, the client provides confidential communications to voice and all other data applications, providing unified, confidential access to the corporate intranet.



Cisco Easy VPN

With the ability to scale to thousands of mobile users and teleworkers, Cisco Easy VPN is an ideal solution for remote-access deployments. Cisco Easy VPN includes Cisco VPN Client software (for Windows, Mac, and UNIX operating systems) to support mobile users. Small offices or home offices can deploy Cisco security routers or appliances to provide encryption services for remote phones, fax machines, printers, PCs, and other devices, including wireless clients. Whenever new security policies need to be enforced, Cisco Easy VPN servers at the headquarters can push the policies automatically to remote users and devices, helping to ensure that policies remain up-to-date without having to physically access the remote devices.

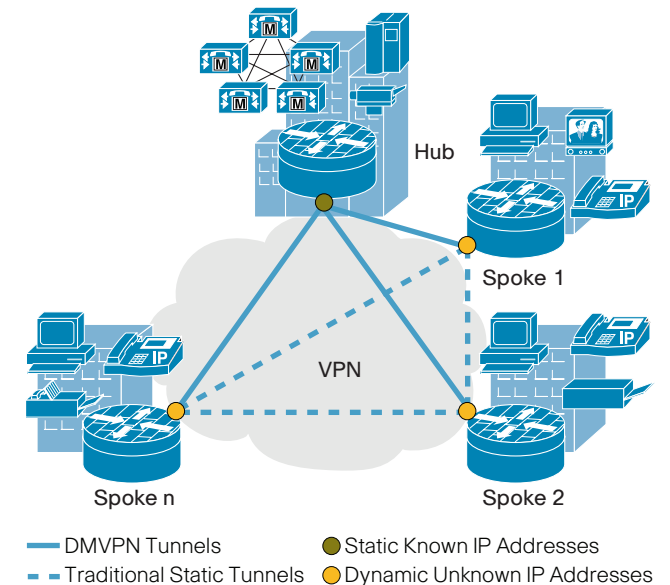
Cisco IOS® Software-based routers include Enhanced Easy VPN, which features advanced quality of service (QoS) integration, allowing differentiation on a per-user basis as well as tunnel-specific attributes. These features can help limit "bandwidth-hogging" by a few users and can help prioritize unified communications traffic over less-critical data.



Cisco DMVPN

Cisco Dynamic Multipoint VPN (DMVPN) provides voice and data confidentiality to large numbers of remote sites connected over private WAN or Internet links, in a scalable and manageable manner. As with Cisco Easy VPN, Cisco DMVPN supports encryption for numerous types of devices, including IP phones and soft phones.

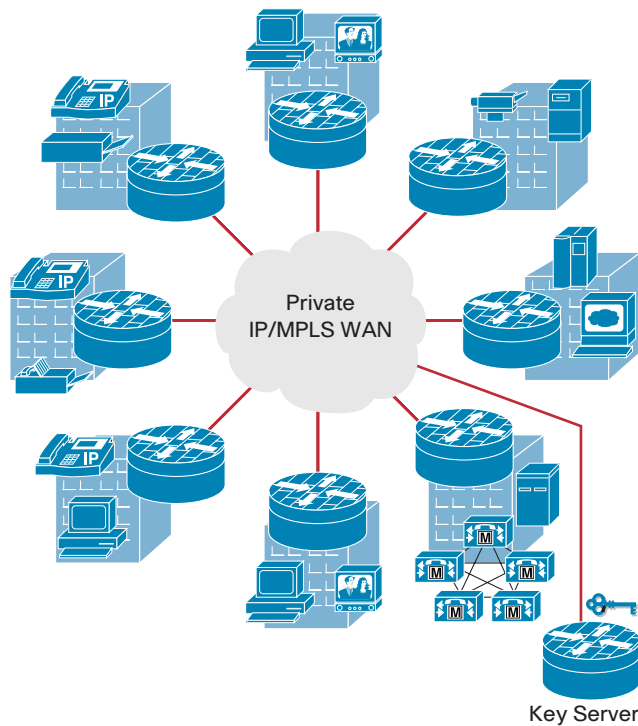
For most data applications, traffic usually flows from remote sites (also called spokes) to a central hub. With voice traffic, calls may be between two remote sites, adding an extra hop and increased latency. Cisco DMVPN allows direct spoke-to-spoke connections. Encrypted tunnels are built automatically between Cisco security routers as required, facilitating optimal encrypted voice performance with minimum administrative overhead. When not in use, these on-demand tunnels are removed, conserving resources on smaller remote routers and allowing the solution to scale more easily. Cisco DMVPN uses the extensive set of Cisco IOS QoS options, and is the premium solution for large unified communications deployments with Internet-connected remote sites.



Cisco GET VPN

Cisco Group Encrypted Transport VPN (GET VPN) provides voice and data confidentiality services for remote sites connected across private WAN or Multiprotocol Label Switching (MPLS) WAN infrastructures. Cisco GET VPN provides tunnelless encryption, avoiding both the need to overlay point-to-point IPsec tunnels over MPLS infrastructures and the associated complexity and scaling limitations.

Cisco GET VPN uses the intrinsic QoS, routing, and multi-cast services of the MPLS infrastructure, allowing organizations that have standardized on MPLS to deploy remote voice applications that use this secure communications method. Cisco GET VPN supports encryption for numerous types of devices, including IP phones and soft phones.



Remote Deployment Scenarios

When deploying confidential unified communications services into remote locations, the method used will depend on the size of the location.

Medium-Sized or Large Remote Sites or Branches

These locations are secured using what are commonly known as site-to-site VPNs. These deployments often require the ability to integrate dynamic routing protocol updates. Major technologies deployed include Cisco DMVPN, Cisco Easy VPN (static routing only), and Cisco GET VPN (private WAN IP/MPLS only).

Small or Home Office Locations, Including Teleworkers

Smaller locations with a only a few users or devices typically do not require dynamic routing protocols. As a result, more options are available to secure these locations. Major technologies deployed include Cisco Easy VPN, Cisco DMVPN, and Cisco Unified Phone Proxy.

Mobile Users

Mobile users generally do not require hardware-based VPN solutions. Providing secure unified communications to mobile users generally involves installing VPN client software that integrates voice and data traffic, along with the means to dynamically and automatically update the security policies on large numbers of end-user devices. Major technologies deployed include Cisco Easy VPN and SSL VPN.

Remote Device Support Requirements

Remote locations often have several devices that need to be supported in terms of authentication and encryption. These include IP phones, soft phones (PC-based software generally used by mobile users), and data devices (such as fax machines, printers, PCs and servers). Confidentiality measures must be able to protect multiple types of devices.

Unified Communications Confidentiality Options Summary Table

The following table summarizes remote unified communications confidentiality solutions.

Remote Unified Communications Confidentiality	Phone Proxy	SSL VPN	Cisco Easy VPN	Cisco DMVPN	Cisco GET VPN
Remote Location Scenarios					
Medium-Sized or Large Remote Sites or Branches	N	N	Static routing only	Y	Y
Small or Home Offices, Including Teleworkers	Phone only	Soft phone only	Y	Y	N
Mobile Users	N	Y	Y	N	N
Device Support					
IP Phone	Y	N	Y	Y	Y
Soft Phone	Authentication only	Y	Y	Y	Y
Data Devices (Fax, Printer, PC)	N	N	Y	Y	Y