CHAPTER 9

Security for Video Communications

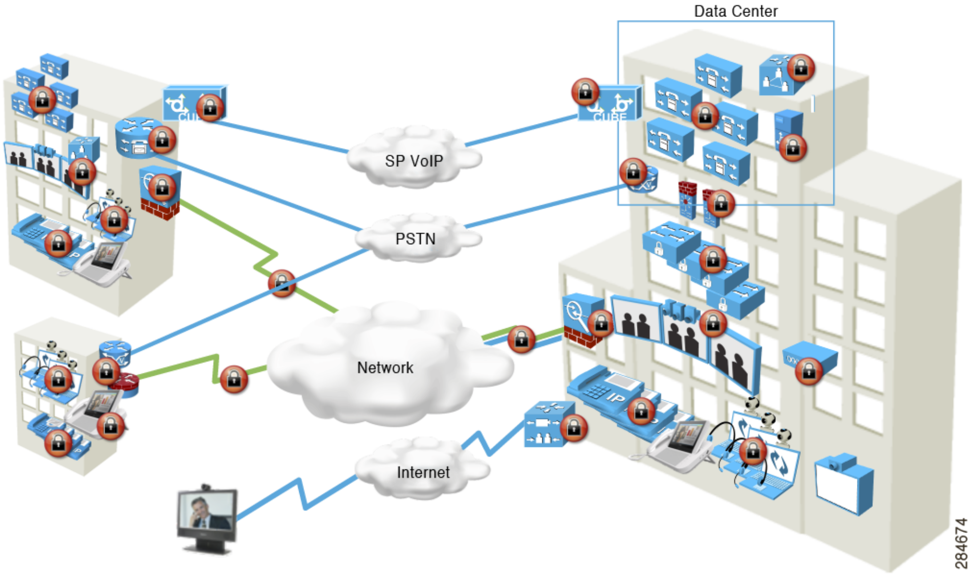
Revised: March 30, 2012, OL-27011-01

Securing video communications over the IP network in an enterprise requires implementing security for both the Unified Communications components and the network infrastructure that those communication streams traverse. This chapter focuses on the design and implementation options available within the Cisco Unified Communications System and the Cisco TelePresence Solution for securing the integrity, reliability, and confidentiality of video calls within an enterprise IP Telephony network. For more information on data network security, refer to the Cisco SAFE Blueprint documentation available at

http://www.cisco.com/en/US/netsol/ns744/networking_solutions_program_home.html

To securely implementing voice and video communications, Cisco recommends creating security policies associated with every network technology deployed within an enterprise (see Figure 9-1). The security policy defines which data in your network is sensitive so that it can be protected properly when transported throughout the network. Having a security policy helps define the security levels required for the types of data traffic that are on a network.

Figure 9-1 Security and Hardening Options in a Cisco Unified Communication System



Hardening the Cisco Unified Communications network involves establishing and maintaining authenticated communication streams, digitally signing configuration files, and encrypting media streams and call signaling between various Cisco Unified Communications and Cisco TelePresence components. All of these security features are not required for every network, but they provide options for increasing levels of security.

This chapter provides the design guidelines for these features. For the product configuration details, refer to the following security documentation for your specific version of Cisco Unified Communications Manager (Unified CM) and Cisco TelePresence:

- *Cisco Unified Communications Manager Security Guide*

  http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html
- *Cisco Unified Communications System SRND*

  http://www.cisco.com/go/ucsrnd
- *Cisco TelePresence Design Guide*

  http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns819/landing_vid_tPresence.html

Network Infrastructure Security

Securing video communications requires securing the network that is used for transporting the calls. This can be achieved by building layers of security, starting at the access port, continuing across the network and to the Internet edge. Cisco recommends always using firewalls, access control lists, authentication services, and other Cisco security tools to help protect your network infrastructure devices from unauthorized access.

Restricting access to the network devices is one of the most important requirements in securing the infrastructure. A typical enterprise network consists of many components, including routers, switches, firewalls, and intrusion prevention systems. Attackers are constantly trying to access these devices on networks. Restricting access to the management interface of each device lowers the opportunities that attackers have to compromise them. All of the devices on a network should be secured appropriately. Administrative and operational management of the network devices should be done using secured protocols such as Secure Shell (SSH) and Hyper-Text Transfer Protocol Secure (HTTPS). Transmission of passwords and configuration information over clear text, used in protocols such as Telnet, should be avoided as much as possible.

In addition to securing access to the infrastructure, the services used in the operation of a network also need to be secured. These include Domain Name System (DNS), Network Time Protocol (NTP), Dynamic Host Configuration Protocol (DHCP), and signaling protocols such as Session Initiation Protocol (SIP) and H.323. These services, which are vital to the successful operation of a network, are also prime targets for an attacker. Disrupting any of these services can cause denial of service and availability problems for the Unified Communications systems.

Separate Auxiliary VLAN

Cisco recommends implementing separate VLANs for RTP traffic (voice and video) and data traffic in a Unified Communications environment. In this configuration, all Cisco IP Phones and TelePresence endpoints are placed in a voice VLAN that is separate from the data VLANs. This implementation provides the following benefits:

- It makes it convenient to design VLAN access control lists (VACLs) that can be used to restrict traffic between voice and data network components. This also allows network administrators to more effectively implement management access restrictions on the network.
- It provides address space conservation and voice device protection from external networks. Private addressing of phones on the voice or auxiliary VLAN ensures address conservation and prevents phones from being accessible directly through public networks.
- It enables simplified Quality of Service (QoS) configuration and management. It also allows the QoS trust boundaries to be extended to voice and video devices without extending the trust and the QoS features to PCs and other data devices.
- VLAN access control, 802.1Q, and 802.1p tagging can prevent attempts by data devices to spoof information and gain access to priority queues through packet tagging.

Note The Cisco Unified IP Phones and the Cisco TelePresence endpoints have different service requirements, and placing them together in a single VLAN makes it more complicated to design regular access control lists.

Device Security

Cisco Unified IP Phones and TelePresence endpoints have multiple configuration options for securing them against attacks. However, these devices should not be considered hardened by default at the time of initial configuration. The security features vary among the different endpoints and include:

- Secure Management over HTTPS and SSH, page 9-3
- Administrative Passwords, page 9-4
- Device Access, page 9-4
- Signaling and Media Encryption, page 9-4

Refer to the endpoint administration guides for information on configuration details for these features. Also, refer to the phone hardening information in the *Cisco Unified Communications Manager Security Guide*, available at

http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

Secure Management over HTTPS and SSH

Cisco TelePresence endpoints support management through Secure Shell (SSH) and Hyper-Text Transfer Protocol over Secure Sockets Layer (HTTPs). Access to the endpoints using HTTP, HTTPS, SSH, or Telnet can be configured in the Network Services setting on the endpoint itself.

Cisco Unified IP Phones can be restricted to use HTTPS only or enabled for both HTTP and HTTPS.

Administrative Passwords

The endpoints ship with default administrative passwords, and Cisco recommends changing the passwords at the time of installation. Access to management functions should be restricted to authorized users with administrative privileges.

Device Access

The endpoints can be assigned to users who are given access based on defined roles and privileges. Passwords and PINs can be specified for these users to enable SSH or Telnet and web-based access. A credential management policy should be implemented to expire and change passwords periodically and to time-out logins when idle. This is necessary for limiting access to the devices to verified users.

For information on user authentication and credential management configurations, refer to the following documentation:

- *Cisco Unified Communication Manager Administration Guide*

  http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

- *Securing Cisco TelePresence Products*

  http://www.cisco.com/en/US/products/ps8332/products_installation_and_configuration_guides_list.html

Signaling and Media Encryption

For supported Cisco Unified Communications devices, signaling and media can be encrypted to prevent eavesdropping and reconnaissance attacks on active calls and during call establishment. The protocols and mechanisms used to provide secure communications and signaling within Unified Communications deployments include the following:

- Transport Layer Security (TLS), page 9-4, used for encrypting signaling traffic
- Secure Real-Time Transport Protocol (SRTP) and Secure Real-Time Transport Control Protocol (SRTCP), page 9-5, used for encrypting media
- Datagram Transport Layer Security (DTLS) Secure Real-Time Transport Protocol (SRTP), page 9-5, used for SRTP master key negotiation and/or exchange
- Digital Certificates, page 9-5
- Certificate Authority Proxy Function (CAPF), page 9-6
- The Certificate Trust List (CTL), page 9-6

Transport Layer Security (TLS)

Transport Layer Security (TLS) is a protocol designed to provide authentication, data integrity, and confidentiality for communications between two applications. TLS is based on Secure Sockets Layer (SSL) Version 3.0, although the two protocols are not compatible. The latest version, TLS 1.2, is defined in IETF RFC 5246. TLS operates in a client/server mode, with one side acting as the server and the other side acting as the client. TLS uses a handshake protocol to allow the client and server to authenticate each other using public key cryptography (digital certificates). This also enables reliable negotiation of a compression algorithm, message authentication algorithm, encryption algorithm, and the necessary cryptographic keys before any application data is sent.

Data authentication and encryption of the SIP signaling between Cisco Unified CM, Cisco Unified IP Phones, and Cisco TelePresence System components, is implemented using the Transport Layer Security (TLS) protocol. TLS is also used for the authentication and confidentiality of the web services signaling between the various Cisco TelePresence components.

The encryption of the signaling protocol is done using the Advanced Encryption Standard (AES) algorithm, using symmetric keying. Message authentication is done with the HMAC-SHA1 hash algorithm. The negotiation of keying material is done securely within the TLS Handshake Protocol layer through the Client and Server Key Exchange messages.

Secure Real-Time Transport Protocol (SRTP) and Secure Real-Time Transport Control Protocol (SRTCP)

Data authentication and confidentiality of the Real-time Transport Protocol (RTP) voice and video media flows use Secure Real-time Transport Protocol (SRTP) for both point-to-point and multipoint TelePresence meetings.

Secure RTP (SRTP) and Secure Real-time Transport Control Protocol (SRTCP) are both defined in IETF RFC 3711, which details the methods of providing confidentiality and data integrity for both RTP voice and video media as well as their corresponding RTCP streams.

In SRTP, encryption is applied only to the payload of the RTP packet using an Advanced Encryption Standard (AES) algorithm with a 128-bit key. SRTP also uses HMAC-SHA1 as the message authentication hash algorithm. Message authentication is applied to the RTP header as well as the RTP payload. SRTP protects against replay attacks by applying the message authentication to the RTP sequence number within the header.

As with SRTP packets, encryption applies only to the payload of the SRTCP packet, when utilized. Message authentication, however, is applied to both the RTCP header and the RTCP payload.

Datagram Transport Layer Security (DTLS) Secure Real-Time Transport Protocol (SRTP)

The Datagram Transport Layer Security (DTLS) protocol is designed to provide authentication, data integrity, and confidentiality for communications between two applications, over a datagram transport protocol such as User Datagram Protocol (UDP). The protocol is defined in IETF RFC 4347. DTLS is based on TLS, and it includes additional mechanisms such as sequence numbers and retransmission capability to compensate for the unreliable nature of UDP. DTLS-SRTP is an extension to DTLS for the negotiation of SRTP keying material within DTLS.

In a Cisco Telepresence solution, the DTLS handshake occurs directly between the TelePresence endpoints. The DTLS-SRTP session is established between the Cisco TelePresence codecs, within the RTP media streams between two endpoints, but not with any associated Cisco Unified IP Phone in the call. In each call, two DTLS-SRTP handshakes occur, one for voice and one for video media, and keys are negotiated for encryption and authentication of both streams.

Digital Certificates

The Cisco Unified Communications System uses X.509 v3 certificates as part of its Public Key Infrastructure (PKI) feature for generating public and private keys used for encrypting and decrypting messages. This PKI implementation generates key pairs that can encrypt messages with the private key that can be decrypted only with the public key that is exchanged between two devices. The private key is kept secure within the device and never exposed. The public key is available as an attribute defined on the X.509 digital certificate. The attributes are established by a Certificate Authority (CA), which digitally signs the certificate. The digital signature itself is a hash of the message, encrypted using the private key of the Certificate Authority. The digital signature of the Certificate Authority can be verified by the recipient using the public key of the Certificate Authority.

A certificate can be either a Manufacturing Installed Certificate (MIC) or a Locally Significant Certificate (LSC). MICs are pre-installed and LSCs are installed by the Cisco Certificate Authority Proxy Function (CAPF) on Cisco Unified Communications Manager (Unified CM). The MIC certificate can provide the credentials used by the endpoints to perform a first-time authentication and enrollment into Cisco Unified CM's security framework. When MICs are used, the Cisco CA and the Cisco Manufacturing CA certificates act as the root certificates.

Note The MIC is also used for establishing Datagram Transport Layer Security (DTLS) sessions between Cisco TelePresence endpoints.

Certificate Authority Proxy Function (CAPF)

The Cisco Certificate Authority Proxy Function (CAPF) is a software service installed as part of Cisco Unified CM. CAPF is not enabled by default and needs to be configured after installation. CAPF issues Locally Significant Certificates (LSCs) for Cisco Unified IP Phones and Cisco TelePresence endpoints. CAPF self-signs certificates under its own authority. However, it can be used as a proxy to request certificates from an external Certificate Authority (CA). It supports the signing of certificates by a third-party certificate authority (CA) using Public-Key Cryptography Standard (PKCS) #10 Certificate Signing Request (CSR).

When using third-party CAs, the CAPF can be signed by the CA, but the phone LSCs are still generated by the CAPF. When self-signed LSCs are used, the CAPF certificate is the root certificate. When an external CA is used, the CAPF acts as the subordinate CA, and the external CA is the root CA.

These certificates are then used to establish secure, authenticated connections for protocols such as SIP signaling over TLS.

The Certificate Trust List (CTL)

The CTL Provider is another software service, installed as part of Cisco Unified CM, that works together with a CTL Client to generate a Certificate Trust List (CTL). The CTL Client is a software plug-in that can be downloaded from the Cisco Unified CM server and run on a separate Windows PC. The Certificate Trust List itself is a predefined list of trusted certificates stored on the Unified CM server and downloaded as a file to the Cisco endpoints when they boot up. The CTL indicates the list of Unified CM servers that the Cisco Unified IP Phones and TelePresence endpoints can trust when they initiate SIP sessions over TLS for call signaling. In order to provide authentication for the CTL itself, a minimum of two separate Cisco Universal Serial Bus (USB) hardware security keys (etokens) are required. These USB keys are not part of the Cisco Unified CM product and must be purchased separately. These security keys are inserted into the PC running the CTL Client plug-in during the CTL generation process.

Configuration File Integrity and Encryption

The configuration files for Cisco TelePresence units and Cisco Unified IP Phones are stored within Cisco Unified CM. These files are downloaded to the endpoints each time they boot up. Configuration files are also automatically downloaded to a Cisco TelePresence device any time a change in configuration is made within Unified CM that would affect the endpoint's configuration. A configuration file download also resets the device.

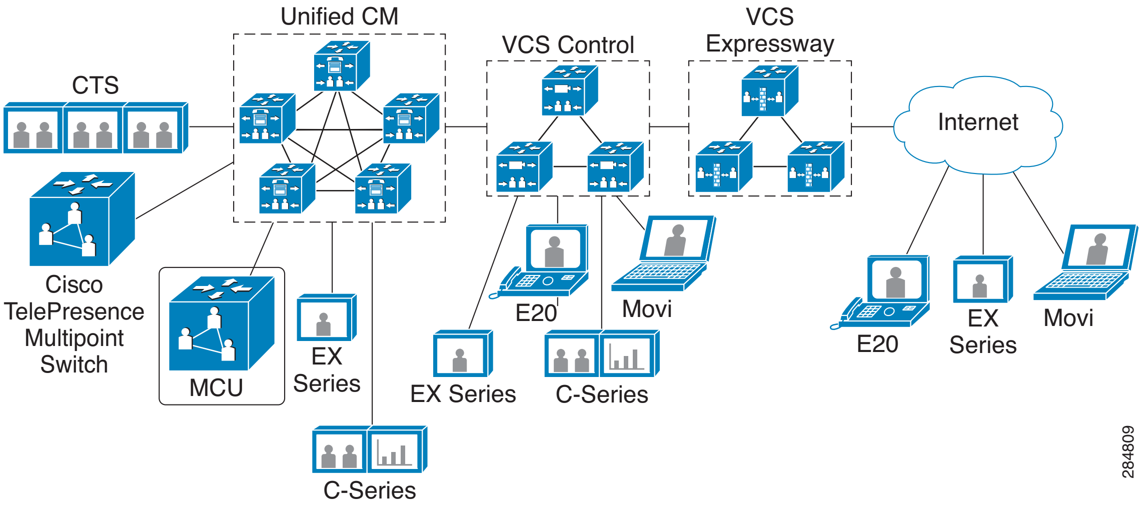
Device security profiles can be created on Cisco Unified CM that require encryption of the configuration files. This prevents configuration files from being changed by unauthorized users because they are digitally signed by Unified CM.

Media Encryption Details

Cisco Unified Communication Manager (Unified CM) supports Secure Real-time Transport Protocol (SRTP) for the audio portion of a voice call payload but does not support encryption for video media. Native support for Cisco TelePresence EX Series and C Series endpoints has been added to Cisco Unified CM 8.6 and later releases, but this does not include support for media encryption. Cisco TelePresence System and Video Communication Servers support SRTP for endpoints natively registered to them. Cisco TelePresence endpoints use Datagram Transport Layer Security (DTLS) for private-key exchange used in establishing SRTP.

Cisco Unified CM, Cisco TelePresence System (CTS), and Cisco Video Communication Servers (VCS) support secure signaling using TLS for SIP. In implementations where a SIP trunk is used for integrating Unified CM, VCS, and CTS, end-to-end signaling encryption of SIP protocol is supported using TLS (see Figure 9-2).

Figure 9-2 Integration of Cisco TelePresence System, Unified CM, and Video Communication Servers Using TLS



Implementing end-to-end SIP signaling encryption requires the configuration of a VCS neighbor zone to Unified CM to use TLS. This feature requires the installation of the appropriate feature key. In addition, Unified CM must be able to trust the VCS server's certificate. This can be done either by having both Unified CM and VCS use certificates from the same Certificate Authority or, if a common root CA is not used, then by exporting the VCS server certificate and uploading it to the Unified CM trust store

While signaling encryption is achieved using this configuration, this does not secure the media payload. Encryption of the video calls requires using DTLS between the endpoints for establishing a secure channel for key exchange. The AES encryption keys that are used for media encryption are then passed through this channel. This media encryption can be implemented on TelePresence endpoints configured to support media encryption but will not work on Unified CM IP Phones.

For step-by-step configuration instructions, refer to the *Cisco TelePresence Video Communication Server Cisco Unified Communications Manager Deployment Guide*, available at

http://www.cisco.com/en/US/products/ps11337/products_installation_and_configuration_guides_list.html

Integration with Firewalls and Access Control List Considerations

A secure enterprise network relies on firewalls in conjunction with access control lists (ACLs) to protect the network from various sorts of malicious threats. ACLs are also frequently used to enforce Quality of Service (QoS) settings, including marking, shaping, and policing traffic at various places in the network, such as at the access edge of a local area network (LAN) or at the intersection of a LAN and wide area network (WAN). Firewalls may also be used for access control within an enterprise campus and between two or more campus locations.

The servers and endpoints in a Cisco Unified Communications System use a large range of ports and services; therefore, using firewalls and ACLs to protect them and restrict access to them requires careful planning. Given the complexities that firewalls introduce into a network design, care is needed in placing and configuring the firewalls and the devices around the firewalls to allow the traffic that is considered correct to pass while blocking the traffic that needs to be blocked.

Because of the dynamic nature of the ports used by voice and video devices, having a firewall helps to control opening up a large range of ports needed for the different services used by the Cisco Unified Communications System. Application Layer Inspection functionality in firewalls simplifies traffic filtering by dynamically opening and closing required ports and sockets. It performs deep packet inspection to obtain the embedded IP addressing information for establishing media streams in a call. However, for this to function well, the firewall's inspection engine must support the specific protocol implementation of the Unified Communications components. The Cisco Adaptive Security Appliance (ASA) 5500 Series firewalls support version-specific implementations of Unified Communications protocols. This requires that the version of ASA implemented is compatible with the version of the Cisco Unified Communications solution in the network. Upgrading one might require upgrading the other.

The Cisco ASA 5500 firewalls restrict and allow traffic based on the trust levels assigned to its interfaces. This establishes different levels of trust within a network. Security levels range from 100, which is the most secure interface, to 0, which is the least secure interface. These are often referred to as the "inside" and "outside." By default, traffic initiated from a device on an interface with a higher security level is allowed to pass to a device on an interface with a lower security level. Return traffic corresponding to that session is dynamically allowed from the lower interface security level to the interface with the higher security level. This behavior works well with the Cisco TelePresence endpoints that use symmetric port numbering in point-to-point calls. However, multipoint TelePresence calls cannot always use symmetrically numbered ports.

In multipoint TelePresence calls, the audio and video User Datagram Protocol (UDP) streams flow between the Cisco TelePresence endpoints and the Cisco TelePresence Multipoint Switch. The endpoints each have one audio and one video call, but because the Multipoint Switch has a single IP address and has to support multiple UDP audio and video streams from multiple endpoints, the flows are not necessarily symmetric from a UDP port numbering perspective. This requires configuring application layer protocol inspection for SIP protocol in order to allow the firewall to open and close the necessary media ports dynamically.

Firewalls do not allow traffic initiated from a device on an interface with a lower security level to pass to a device on an interface with a higher security level. This behavior can be modified with an ingress access control list (ACL) on the lower security interface level. An ingress ACL applied to the interface with the higher security level may also be used to limit traffic going from higher level security interfaces to interfaces with lower security levels.

Cisco ASA 5500 Series firewalls can also be allowed to operate with interfaces having equal security levels. This requires configuring commands that permit same security interface traffic. ACLs can also be applied on each interface, and static translations can be used to specifically allow access between certain devices and protocols connected to interfaces with equal security levels.

For a list of TCP and UDP ports that need to be permitted between Cisco TelePresence components, refer to the *Securing Cisco TelePresence Products* document, available at

> http://www.cisco.com/en/US/products/ps7315/products_installation_and_configuration_guides_list.html

For a list of ports used by Cisco Unified CM, refer to the *Cisco Unified Communications Manager TCP and UDP Port Usage* guide, available at

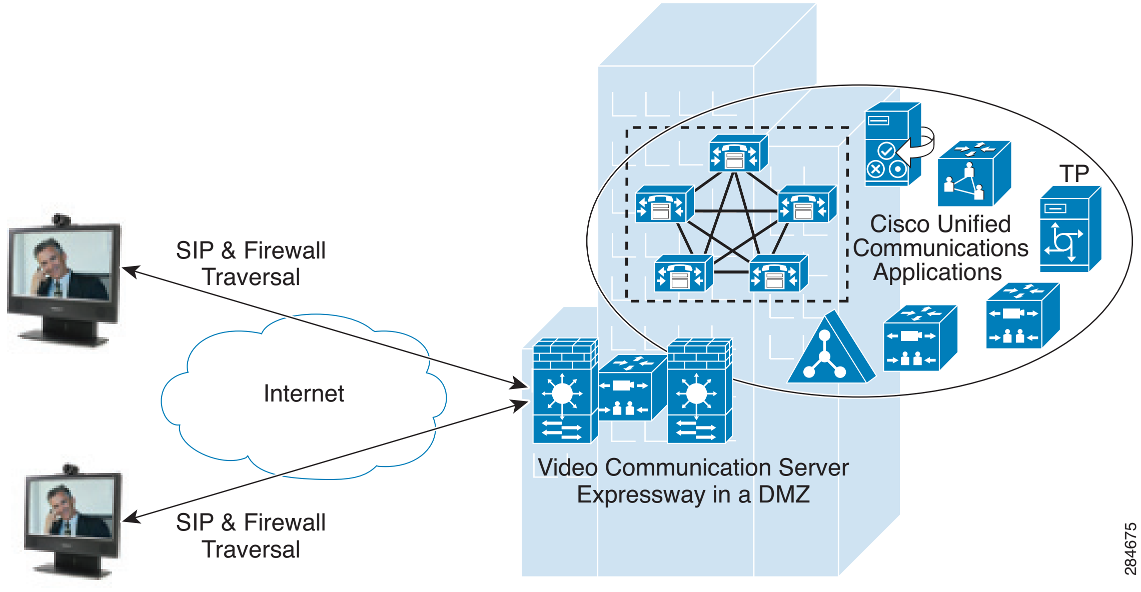
> http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

Firewall Traversal in the DMZ

The Cisco TelePresence Video Communication Server Expressway (VCS Expressway) can establish video communication calls with devices outside the enterprise network and across the Internet. The VCS Expressway must be placed outside the private network used by the Cisco Unified Communications solution to allow external callers to access the device. It can be deployed either on the public Internet or in a demilitarized zone (DMZ). By default, firewalls block unsolicited incoming requests, so the firewall must be configured to allow the VCS Expressway to establish a constant connection with the VCS Control server.

Positioning the VCS Expressway in the DMZ makes this implementation much more secure (see Figure 9-3). It uses VCS as the dedicated server for handling voice and video traffic, thus making the firewall configuration less complex. It can limit the management traffic to the VCS Expressway, restricting it to the internal private traffic and blocking access externally.

Figure 9-3 VCS Expressway in a DMZ


SIP & Firewall Traversal
Internet
SIP & Firewall Traversal
TP
Cisco Unified Communications Applications
Video Communication Server Expressway in a DMZ
284675