POLYCOM®
Network Systems Group

Deploying Secure Enterprise Wide IP Videoconferencing Across Virtual Private Networks

Solutions Guide

Document Overview

This document provides an overview of how to effectively and securely provide IP-based videoconferencing applications between multiple locations within a corporate enterprise, using dynamically created Virtual Private Networks across the Internet.

POLYCOM®
Network Systems Group

TABLE OF CONTENTS

POLYCOM®
Network Systems Group

Introduction

With the ever-increasing reach of the Internet, corporations are taking advantage of its flexibility and cost-effectiveness to expand and enhance their traditional IP-based enterprise networks and applications. This increases demand for greater capacities across the Internet.

Corporations have also discovered the value of IP-based, real-time voice and video applications. As these applications become more commonplace, network managers are creating networks that overlay voice and video applications on top of the traditional enterprise network. When real-time, media-rich applications are merged with traditional enterprise applications and networks, several key issues must be addressed, including latency, jitter, security, NAT and firewalls.

This document focuses on solutions involving internal, enterprise-wide IP videoconferencing. Additionally, it looks at the challenges of deploying internal IP videoconferencing when there is more than one geographic location involved. In this scenario, virtual private networks provide a way to implement videoconferencing applications securely between multiple locations within an enterprise, while taking advantage of the Internet for wide area coverage. Issues relating to NAT, firewalls and remote access are also solved for internal videoconferencing using VPN tunneling.

Addressing Challenges To Wide Scale Video Deployment

As discussed earlier, IP-based videoconferencing has not been widely embraced due to issues with security, NAT, firewalls, and the two current IP videoconferencing standards, H.323 & SIP.

The Standards

H.323 is an ITU standard that provides a comprehensive suite of sub-elements for call setup, control and payload. This standard is more mature than and was defined to be compatible with the previous circuit-switched H.320 standard.

Session Initiation Protocol (SIP), on the other hand, is a new and emerging standard defined by the IETC. SIP was conceived to provide call setup and control for voice, video and other multimedia applications, much the way other Internet applications work. Its concept is to not be an entire suite of capabilities such as H.323, but to provide simple, straightforward call setup and control for multimedia applications over IP.

In either case, H.323 and SIP share the same issues with security, NAT and traditional firewalls. Virtual Private Networks provide solutions for network managers when deploying both H.323 and SIP-based videoconferencing.

Security & Firewall Issues

Because of multiple security risks from viral and hacker-based attacks, network managers have no desire to compromise the integrity of their organizations' enterprise networks. IT managers have their hands full simply trying to protect and secure the traditional enterprise. There is an understandable reluctance to deploy IP-based audio and video applications. Opening multiple TCP and dynamically changing UDP ports on the firewall is not a viable option to complete a single audio or video session across the Internet. Doing so could compromise the security of the enterprise.

Network Address Translation (NAT)

Finally, there is the issue of Network Address Translation (NAT). When, and until, Internet Protocol version 6 (IPv6) is widely embraced and deployed across the Internet, there will be issues involving NAT. Since the combination of a firewall and NAT achieves the goal of keeping outsiders from unauthorized access or entry into the secured enterprise, and provides a means for insiders to access the outside world, most traditional, non-realtime applications do not suffer.

POLYCOM®
Network Systems Group

IP-based videoconferencing, however, seeks to create a real-time session between two or more endpoints, at more than one secure location. This creates real-world issues that are not addressed in today's firewall technologies. This issue is not easily resolved by NAT-enabled firewalls or H.323-enabled firewalls, even within a single enterprise with multiple geographic locations.

Network Basics

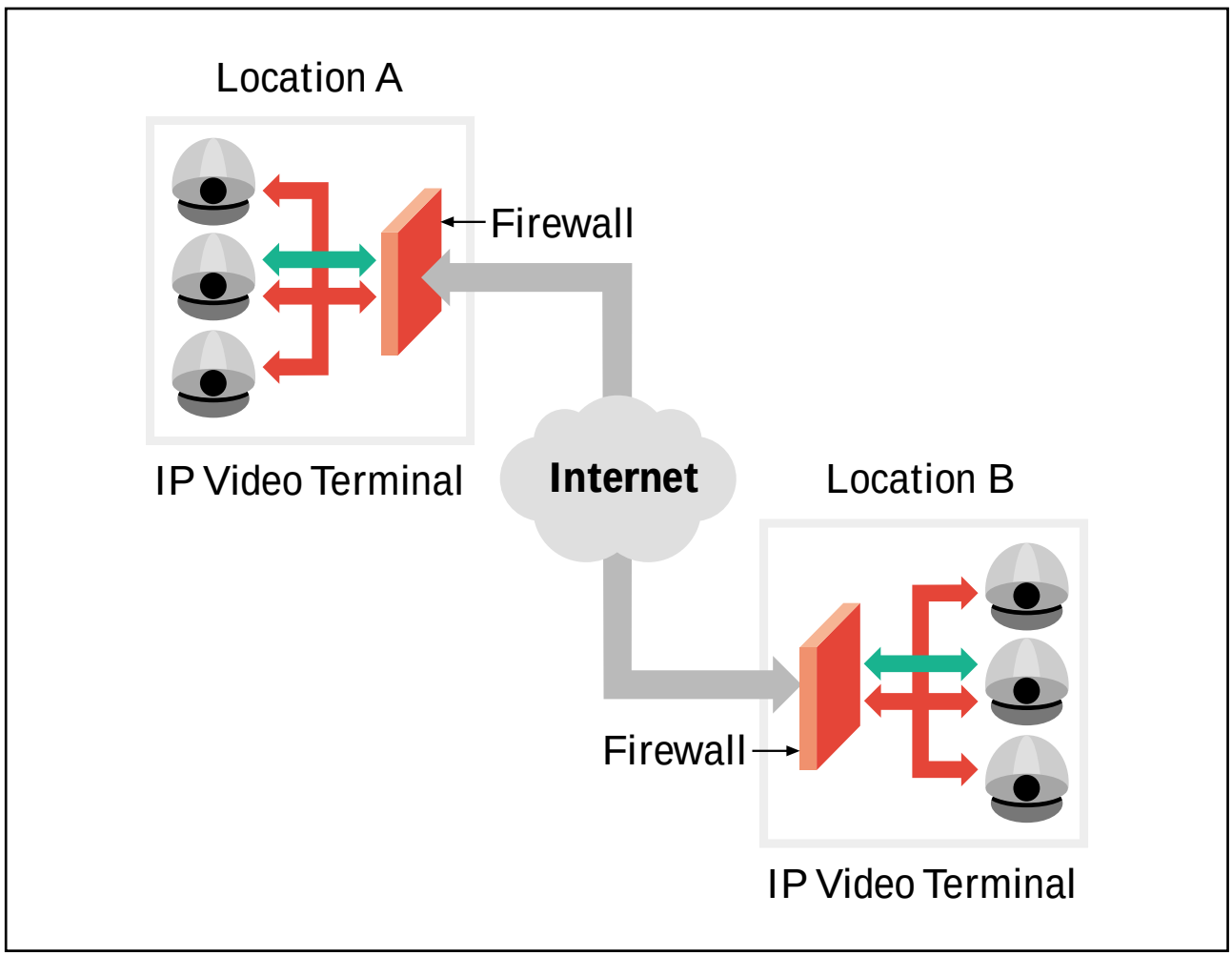
In this particular application we are going to assume that a enterprise has more than one geographic location. We will base our discussion around the example in Figure 1.

In this example, note that each geographic location has its own individual NAT-based firewall solution to secure the corporate enterprise.

Although some firewall manufacturers offer H.323 options, they do not realistically solve real-world IP video applications involving or spanning more than one firewall.

Since WAN access is directly tied to the Internet, it is not realistic to allow video connections to simply pass through the firewall, because of the potential threats and vulnerabilities of multiple dynamic TCP and UDP ports opened to the outside.

Figure 1. Typical Network Scenario



POLYCOM®
Network Systems Group

VPN Basics For IP Videoconferencing

Technologies from Polycom, in conjunction with VPN technologies from companies such as Checkpoint and Microsoft, allow corporations to deploy secure IP videoconferencing applications to multiple locations while using the Internet as the public transport mechanism.

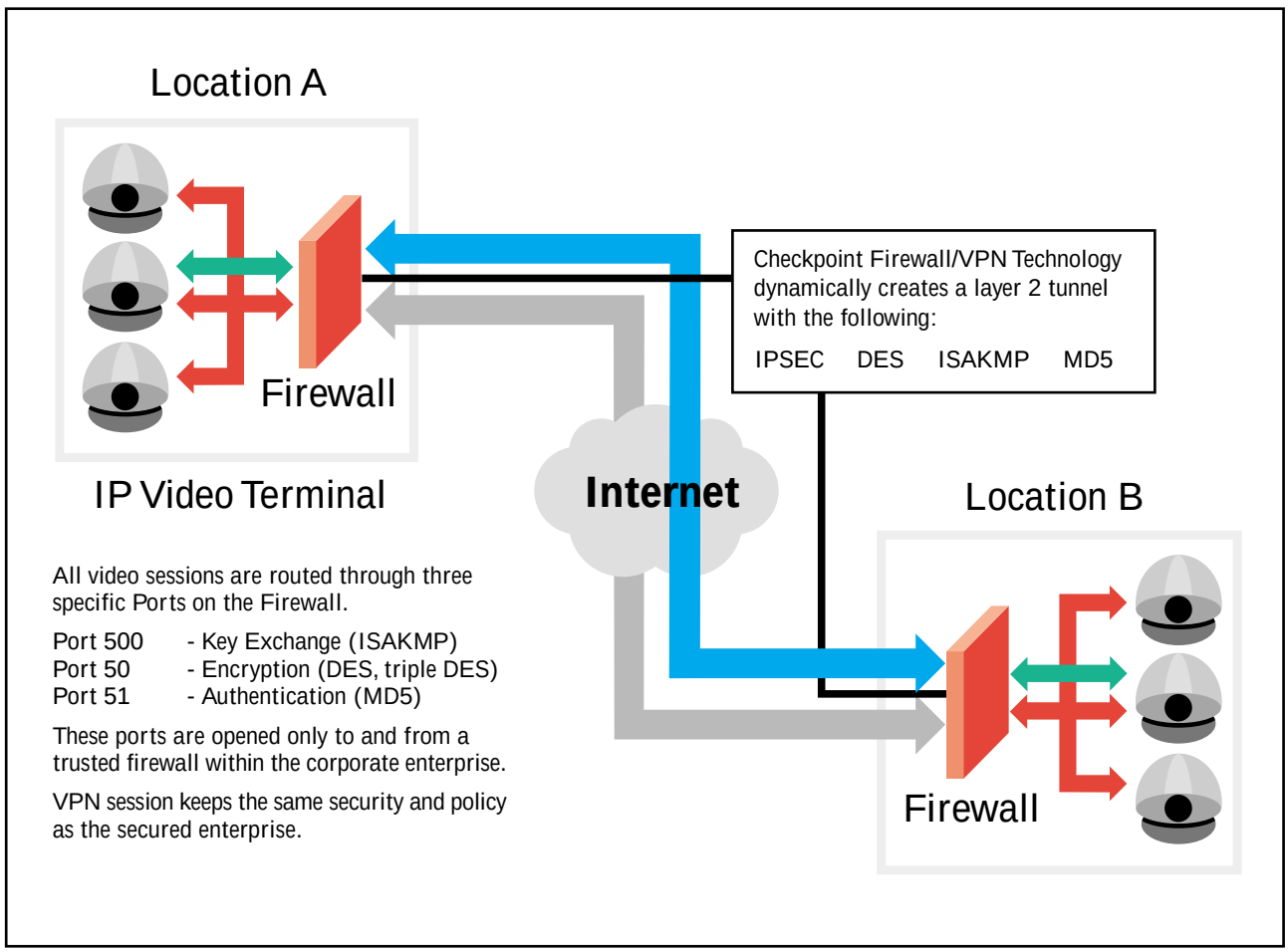
A VPN typically allows the network administrator to create a secure, policy-based overlay network within the Internet. Imagine a VPN using the Internet as a transport while creating a secured tunnel within it. The key is that the tunnels are always to a trusted destination such as another geographic location within the same enterprise.

Figure 2 demonstrates how the VPN tunnel creates an overlay to the existing data network as illustrated earlier.

Virtual Private Network tunnels provide a unique and scaleable means to easily deploy IP-based H.323 videoconferencing within a corporate enterprise. Easier deployment and scaleability allows greater usage and improved productivity.

The deployment becomes very straightforward when using Polycom's video terminal and network equipment in conjunction with Checkpoint's Firewall-1 firewall systems.

Figure 2. VPN Tunnel with IP Video



POLYCOM®
Network Systems Group

As shown in Figure 2, all locations are trusted domains between the Checkpoint Firewall-1 systems, all with the same internal NAT-based IP structure.

- The local video system, initiating the call, sends TCP and UDP data to the local Checkpoint firewall.
- The local Checkpoint Firewall–1 system then sets up a layer 2 tunnel, an ISAKMP key exchange, an MD5 hash authentication scheme and DES encryption algorithm to the trusted firewall at the far end location.
- The local Checkpoint Firewall-1 forwards the encrypted data to the remote trusted Checkpoint Firewall–1 system.
- The remote Checkpoint Firewall-1 system receives the encrypted data and compares it to the key exchange and authentication measures, then decrypts the TCP and UDP data and sends it to the requested video system.

Note that this all happens within the three ports (50, 51, & 500) described in Figure 3.

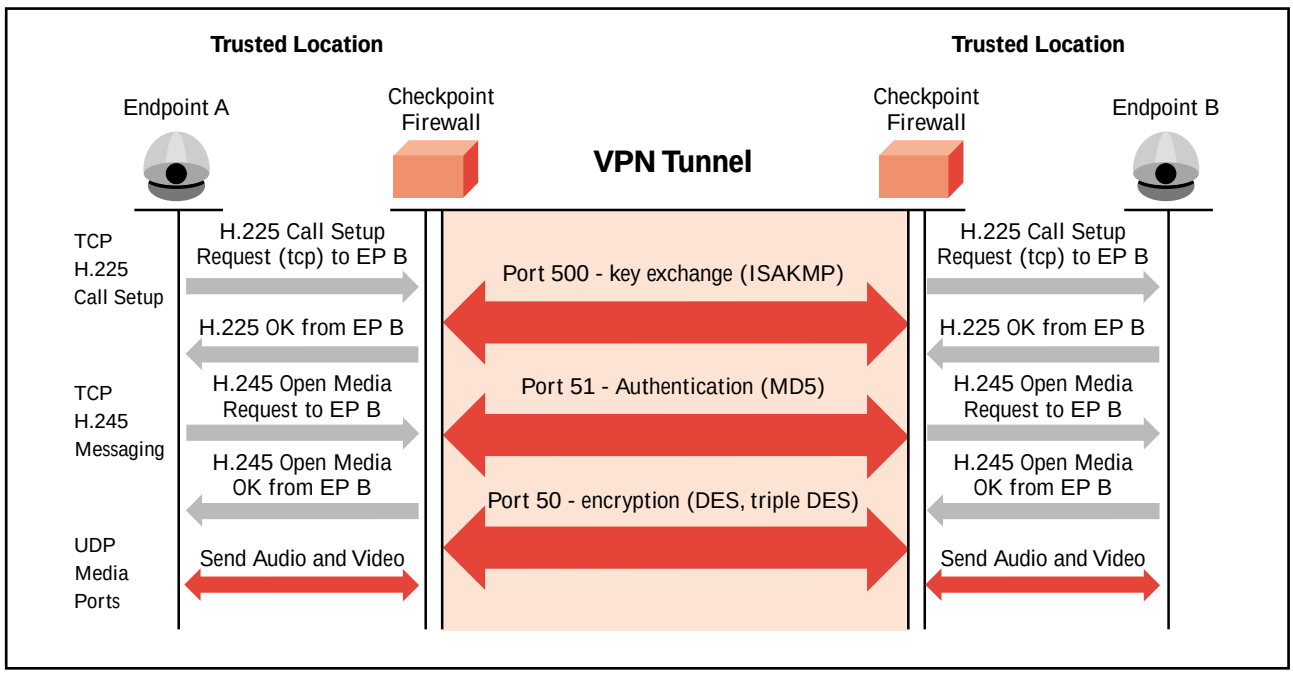
Call Flow

Figure 3 shows a typical H.323 call flow using VPN tunneling over the wide area network. Notice how the normal call flow is intercepted by the local enterprise firewall/VPN service. It is then rerouted across three ports dedicated to securing, authenticating and encrypting the VPN link to the far end VPN/firewall service for the enterprise. This type of solution does not require that multiple dynamic TCP and UDP ports be opened, which is the normal case for H.323 IP video communications crossing data firewalls.

The number of simultaneous calls and call quality is affected by several factors:

1) Appropriated bandwidth and network infrastructure
2) The amount of processing power of the Firewall/VPN service
3) The ability to process multiple authenticated and encrypted streams of real-time IP-based videoconferencing data

Figure 3. H.323 Call Flow Over Enterprise Using VPN



POLYCOM®
Network Systems Group

Usage Scenarios

It is important to understand just how this type of technology affects the network administrator and the user of the service. Polycom's line of MCUs and Gateways provide the following usage scenarios for internal videoconferences over VPN tunnels.

■ IP Point-To-Point Conferences

Point-to-point calls may be placed between any Polycom H.323 IP desktop and/or group system in a point-to-point conference using the VPN technologies described above.

■ IP Multipoint Conferences

H.323 IP-based Multipoint conferences to and from any Polycom desktop and/or group system may be placed using Polycom's MGC and IP-based MCU products.

■ IP & ISDN Mixed Conferences

IP & ISDN mixed point-to-point conferences may be placed to or from any Polycom H.323 IP-based desktop and or group system. Polycom MGC-based MCUs and Gateways may also provide internal IP to ISDN point-to-point and multipoint services to or from any Polycom desktop or group system supporting VPN service.

■ Secure Gateway Conferences Outside of the Corporate Enterprise

It is important to remember that deploying VPN service only provides IP-based video deployments for internal or inter-company calls. The VPN security only provides access to multiple geographic locations within an enterprise.

Enterprise VPN configurations using Polycom desktop and group video systems can also provide IP-based videoconferencing outside the secure enterprise while maintaining the same security and policies internally. This is accomplished by deploying Polycom's Firewall Gateway/Proxy technologies that are supported by Polycom's line of MCUs and Gateways. These products allow secure video communications with other companies or organizations over IP or ISDN networks. Network administrators are not required to modify any security or policy-based measures and configurations within their existing network or firewall.

Benefits

This type of deployment creates the ability for an enterprise to rapidly implement real-time video solutions within the enterprise. The benefits of real-time video include:

- Increased Productivity
- Improved Resource Efficiency
- Less Travel
- Reduced Travel Costs
- Improved Morale

This implementation also marks the convergence of video services and data within the same network infrastructure. Video equipment and resources can be managed using the same platform as other network components.

Using VPNs provides an easy-to-use connectivity model. The user can simply call another person much as they would use the phone. Products such as gatekeepers and directory managers allow users even more freedom. Colleagues can be called using their phone number, extension or email address. This solution is governed by the enterprise network's security and policy since all geographic locations are linked via the secure VPN tunnel.

POLYCOM®
Network Systems Group

Limitations

The quality and quantity of calls are determined by the processing power of the firewall/VPN solution. Network administrators must plan how many simultaneous video sessions will be required to run across the VPN, as well as current data capacity that would run via the tunnel. Scaleability and performance are directly impacted by the processing power on the firewall/VPN server.

This solution does not address the use of IP-based videoconferencing to other enterprises; rather, internal IP video communications for a single enterprise to multiple locations only.

For information on how to provide secure IP videocommunications outside a secure corporate enterprise, without compromising the integrity of the network, see our related White Papers on:

– Polycom's Certified Firewall Gateway/Proxy Technologies, 'Addressing Issues with H.323 as it relates to Security, Firewalls, NAT & PAT'
– 'MGC Firewall Certification Report'

These documents can be accessed on Polycom's website, www.polycom.com, at North America/Products/Network Systems Products/Technical Documents.

Polycom's Firewall Gateway/Proxy technologies allow network managers to combine VPN solutions, such as those described in this document, with secure IP video communications to other enterprises, organizations or partners that are vital to your business.

Conclusion

As enterprises better utilize and advance their IP-based Internet services, VPN tunneling is an option that provides a means of sharing the public Internet backbone, while maintaining the privacy of a dedicated internal network. VPN tunnels provide scaleable and secure services for internal videoconferencing in enterprises that need to communicate effectively between multiple physical locations.

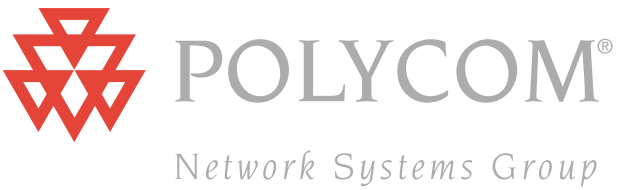
Using Polycom endpoints, MCUs, gateways and management platforms within the internal VPN service provides seamless end-to-end videoconferencing solutions for both internal and external IP-based videoconferencing applications.

Notes & Assumptions

This document assumes the appropriate IP bandwidth, network equipment and network resources have been accurately calculated, designed and implemented to sustain the desired service level, quality and capacity requirements for IP-based videoconferencing applications.

It also assumes the typical issues of security, capacity, latency and jitter have all been assessed and designed to meet the needs of real-time applications.

For further assistance with assessing load requirements, preparing your network for video and/or video specific consultation, contact your local Polycom representative to schedule an initial networking analysis.



Polycom Network Systems

United States Office
9040 Roswell Road
Suite 450
Atlanta, GA 30350-1877
United States
Tel: +1 770-641-4400
Fax: +1 770-641-4499

Israel Office
94 Derech Em Hamoshavot P.O.B. 3654
Petach-Tikva 49130
Israel
Tel: +972 3 925 1444
Fax: +972 3 921 1571

www.polycom.com

European Office
270 Bath Road
Slough
Berkshire, SL1 4DX
United Kingdom
Tel: +44 (0) 1753 723000
Fax: +44 (0) 1753 723357

Asia-Pacific Office
Suite 1008
Beijing Fortune Building
5 Dong Sanhuan Bei-lu Chaoyang District,
Beijing 100004
China
Tel: +86 (10) 6590 8321
Fax: +86 (10) 6590 8368