POLYCOM®

Network Systems Group

Creating Building Blocks For Voice & Video Over IP

TECHNICAL WHITE PAPER

Addressing issues with H.323, Security & Firewalls

TABLE OF CONTENTS PAGE

Section 1

INTRODUCTION

In the past, corporate adoption of interactive voice and video technologies over IP has fallen short of analyst expectations. The adoption of this technology has suffered from:

- The complexities of implementing the H.323 standard
- Lack of appropriate network infrastructure for time sensitive data types
- Obstacles introduced by Network Address Translation
- Conflict between current security practices and H.323 call requirements
- Limited management platforms for Voice and Video technologies

This paper summarizes the network infrastructure requirements for voice and video, focusing on issues found most frequently where the public Internet and private IP networks meet. It explores numerous solutions, pointing out their shortcomings and the need for a set of building blocks that address these issues without requiring network reconfiguration or exposing corporate assets to non-secure network conditions.

EXPANDING THE NETWORK INFRASTRUCTURE

One of the most formidable barriers facing the enterprise IT manager has been the design of an IP infrastructure suitable for interactive voice and video. The multi-stage network upgrade process includes:

- Replacing shared Ethernet hubs with switched Ethernet components
- Provisioning ample bandwidth in those segments of an enterprise network where video traffic is anticipated
- Introducing Quality of Service protocols in routers to give priority to video traffic
- Introducing specialized computing and network management resources for rich media applications (multipoint control units and gateways)
- Devising an appropriate address resolution scheme or directory so users can find one another (a directory application with or without a gatekeeper)
- Insuring the security of the enterprise network while at the same time permitting H.323 traffic to be exchanged with 'off net' entities.

As the initial stages of this process near completion in some enterprise networks, more attention will be focused at the intersection of public and private networks.

"In this next phase of expansion, network and port address resolution and maintaining network security present significant challenges."

Network Address System

Due to design limitations of the public Internet protocols and the success of the Internet as a destination, experts estimate that approximately half the total available IP addresses have been assigned. Each of these has a price and, for large enterprises, the cost of provisioning public IP addresses to hundreds of thousands of computers is prohibitive. To alleviate the problem, the Internet Engineering Task Force developed a 128-bit addressing scheme for the next version of the Internet Protocol (IPv6), but a number of issues stand in the way of this protocol's complete implementation throughout the Internet. Until such a time when IPv6 is widely deployed, anyone assigned and using an IPv6 address (a protocol that was approved by the IETF in July 2000) is virtually unreachable from the current Internet.

In addition to Network Address Translation, one public IP address can be used by many Internal IP addresses by assigning a different external IP port for each internal IP transport Address needed. To make this possible, many networks have Port Address Translation (PAT) and Network or Port Address Translation (NPAT) technologies embedded in a router or server where the NAT and firewall applications are running.

Basic NAT and PAT devices filter the incoming and outgoing IP packets and modify the header information. As the case for firewalls, discussed below, these products will interfere with applications that open dynamic ports during the connection (as is the case for H.323).

In order for someone who is 'off net' (outside the enterprise network address scheme) to place a call using H.323 with a person seated at a device behind a NAT or PAT device, the network manager must introduce new software or hardware. We will examine the attributes of such a product, but first we will describe the standard components of secure networks.

"One problem for real time H.323 voice and video traffic is that private addresses are only 'routable' by network components who view them as unique, and not by routers in the public Internet."

Security - The Purpose Of A Firewall

Regardless of the network's size or a company's business, a complete enterprise security solution must:

- Grant selective network access to authorized remote and corporate users
- Authenticate network users with strong authentication techniques before granting access to sensitive corporate data
- Ensure the privacy and integrity of communications over untrusted, public networks like the Internet
- Provide content security at the gateway to screen malicious content, such as viruses and malevolent Java/ActiveX applets
- Detect network attacks and misuse in real time and respond automatically to defeat an attack Protect internal network addressing schemes and conserve IP addresses
- Be available at all times to ensure users high availability to network resources and applications
- Offer local and remote management interfaces to authorized administrators
- Deliver detailed logging and accounting information on all communication attempts

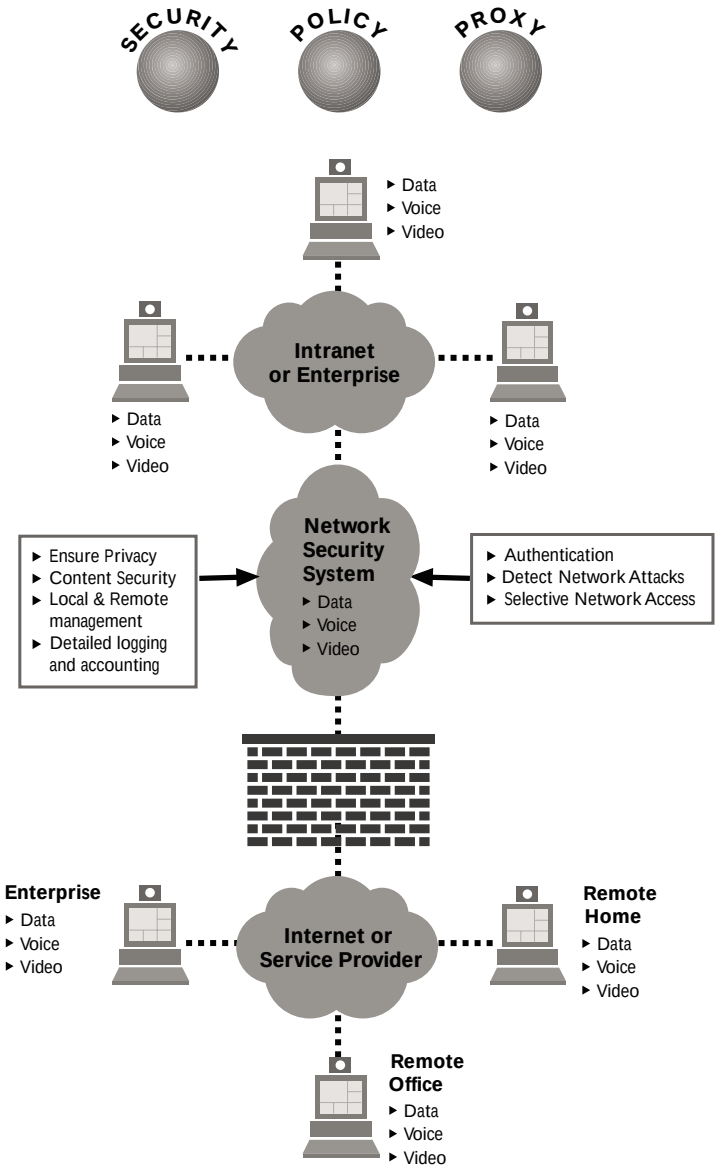
"The most popular network security devices in enterprise networks today are called 'firewalls.'"

Firewall code may be implemented in software and installed on open systems, such as Unix or Windows NT/2000, or run on appliances at the network gateway server. The programs provide security by literally checking all the data that enters a network.

Some firewalls use a technique called packet filtering. A packet filter firewall is a first-generation firewall technology that analyzes network traffic at the transport protocol layer. Each IP network packet is examined to see if it matches one of a set of rules defining which data flows are allowed. These rules identify whether communication is allowed based upon information contained within the Internet and transport layer headers and the direction that the packet is headed (internal to external network or vice-versa).

If a matching rule is found, and if the rule permits the packet, then the firewall allows the packet through, from one network to another. If a matching rule denies the packet, then the packet is dropped. If there is no matching rule, then the packet is dropped.

Another type of firewall, a 'proxy,' is a program with the authority to act (send and receive signals) on behalf of registered users on a network. The proxy has both a client and server component.



POLYCOM®
Network Systems Group

A proxy client is part of a user application that talks to the real server on the external network on behalf of the real client.

When a real client requests a service, the proxy server evaluates that request against the policy rules defined for that proxy and determines whether to approve it. If it approves the request, the proxy server forwards that request to the proxy client.The proxy client then contacts the real server on behalf of the client (thus the term 'proxy') and proceeds to relay requests from the proxy server to the real server and to relay responses from the real server to the proxy server. Likewise, the proxy server relays requests and responses between the proxy client and the real client.

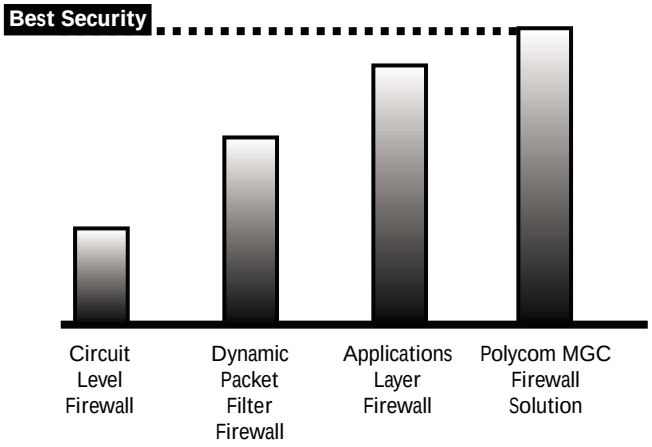
A proxy server acts as the end server for all connection requests originated on a trusted network by a real client.

That is, all communication between internal users and the Internet passes through the proxy server rather than allowing users to communicate directly with other users and servers on the Internet. An internal user, or client, sends a request to the proxy server for connecting to an external service, such as FTP or Telnet.The proxy server evaluates the request and decides to permit or deny the request based on a set of rules that are managed for the individual network service. Proxy servers understand the protocol of the service that they are evaluating, and therefore, they only allow those packets through that comply with the protocol definitions.There are many types of proxy servers. Some also enable additional benefits, such as detailed logging of session information and user authentication.

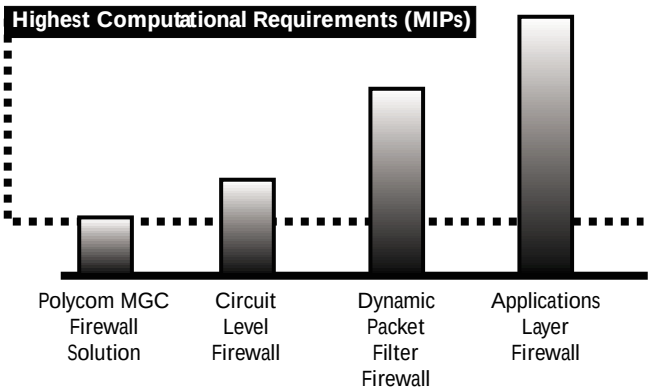
Finally, a proxy service is a software program that connects a user to a remote destination through an intermediary gateway.

There are special-purpose programs that manage traffic through a firewall for a specific service, such as HTTP or FTP, that is able to enforce security as well as provide valuable services such as logging. Proxy services tend to be specific to the protocol they are designed to forward, and they can provide increased access control, careful checks for valid data, and generate audit event records about the traffic that they transfer. In addition, proxy services tend to offer certain common features such as authentication, data caching, and application layer protocol validation.

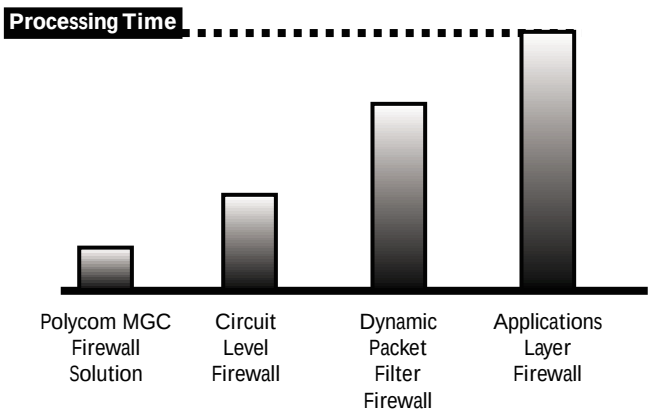
Security



Best Performance



Latency



When considering alternative firewall technologies, an architect will need to understand the trade-offs between performance and security.

The rule is that it all depends on how far up the network stack a network packet must travel, as well as what level of security checks are being performed on each packet. Packet filter firewalls generally provide the highest performance, followed by circuit level firewalls, dynamic packet filter firewalls, and application layer firewalls.

The level of security checks generally follows the reverse pattern because as network packets pass through more protocol layers, they are inspected in more detail. As a result, application layer firewalls are considered more secure than dynamic packet filter firewalls, which are considered more secure than circuit level firewalls, etc.

However, because a circuit level firewall does not perform extensive security checks, other than whether a network packet is associated with a valid connection, it can (and often does) perform faster than a packet filter firewall that contains a large set of accept and deny rules.

In general, application layer firewalls are the slowest architecture due to the fact that all network packets are sent up one network stack and down a different one, thus being treated as two separate network sessions.

Application layer firewalls also implement the broadest set of security data checks, which increases the processing time required. Throughout the industry, application layer firewalls are generally considered to provide the best security.

Increasing the capabilities and capacity of firewalls, proxy servers and network address translation devices will raise their respective bandwidth and computational (MIP) requirements, and management overhead, but as they stand today, these devices present very significant obstacles to those deploying H.323 applications.

Section 2

THE COMPLEXITIES OF H.323

In enterprise networks, interactive video using H.323 protocols is often under the control of an H.323-defined entity called the 'gatekeeper.' The gatekeeper performs address resolution, bandwidth management and injects policies into the network as needed.The first two of these three functions are heavily implicated during a gatekeeper routed call set up.

When a user wants to place a call, the initiating endpoint starts by requesting admission from the gatekeeper using an Admission Request (ARQ) message.The gatekeeper can accept (ACF) or deny the request (ARJ). If the call request is accepted and the user has the remote device's IP address (or the gatekeeper has this address in its database), the endpoint sends a Q.931 Setup message to the remote destination.The recipient of the Setup message in turn requests admission from its gatekeeper by sending an ARQ.When the call is accepted, the Q.931 call signaling sequence is completed followed by the H.245 message negotiation.The Admission Request (ARQ) message carries the initial bandwidth the endpoint requires for the duration of the conference.

With or without the gatekeeper, certain call set up procedures are necessary for a H.323 session to be complete. Upon receiving a Setup message from the remote party, endpoint B responds by sending a Q.931* Alerting message followed by a Connect message if the call is accepted. At this point, the call establishment signaling is complete, and the H.245 negotiation phase is initiated. Both terminals will send their terminal capabilities in the terminal Capability Set message.The terminal capabilities include media types, codec choices, and multiplex information. Each terminal will respond with a terminalCapabilitySetAck message.The terminals' capabilities may be resent at any time during the call provided TCP/IP ports are available.

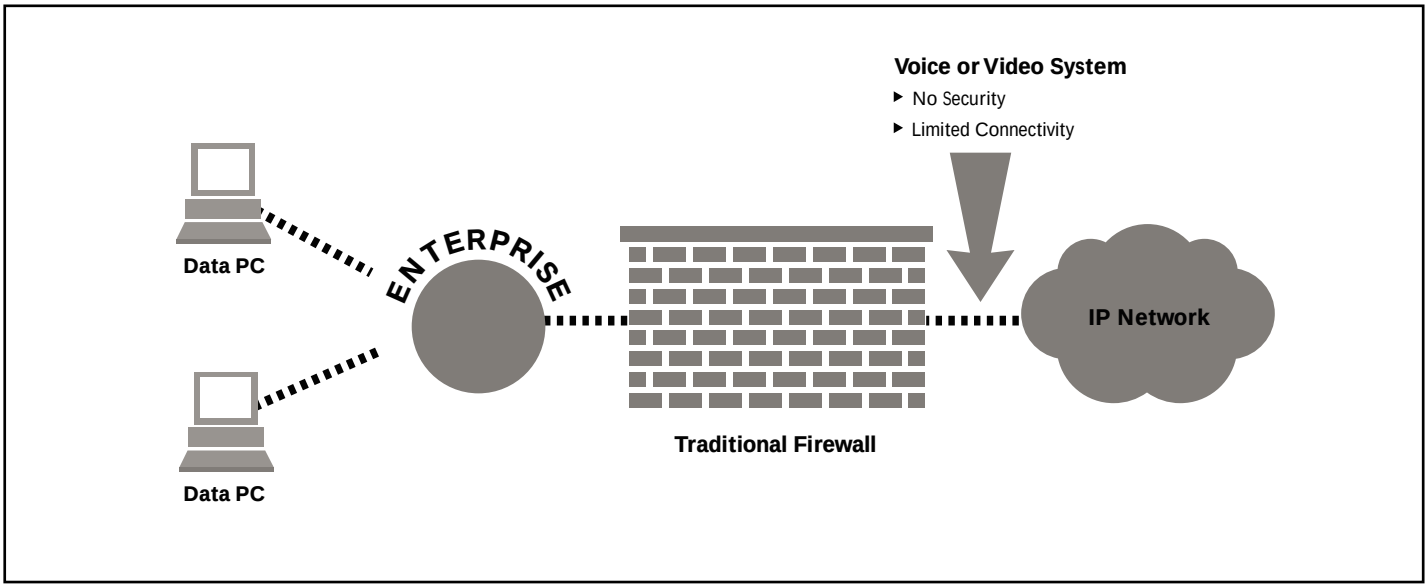
*H.225.0 - H.323 standard is a subset design of the Q.931 standards

If two end points are configured as peers, the Master/Slave determination procedure is then started.The H.245 Master/Slave determination procedure is used to resolve conflicts between two endpoints that can both be the MC for a conference, or between two endpoints that are attempting to open bi-directional channels at the same time. In this procedure, two endpoints exchange random numbers in the H.245 masterSlaveDetermination message to determine the master and slave endpoints. H.323 endpoints are capable of operating in both master and slave modes.

Following master/slave determination procedures, both terminals proceed to open logical channels using Universal Datagram Protocol (UDP). Both video and audio channels are uni-directional while data is bi-directional.Terminals may open as many channels as they want, but each logical channel uses a separate, randomly assigned port within a specific port range. Other H.245 control messages may be exchanged between the endpoints to change media format, request video key frames and change the bit rate during a call.

When vendors add authentication and encryption to their H.323 compliant systems, these additional complexities will require that firewall and NAT application proxies be updated to understand the authentication and encryption signaling. Since security and authentication are very important at the interface between public and private networks, supporting these protocols will be necessary but will also add compute complexity to the NATs and firewalls.

When these steps are performed on behalf of people on the same multimedia-ready IP network, the users are rewarded with a complete rich media experience. In order for those end points registered inside a secure network to reach people at end points outside the enterprise network, a caller must avoid Network Address Translation systems or have a consistent and reliable system to negotiate calls through both the NAT and firewall or proxy server. We will now examine some of the options currently open to network engineers and managers.



Limited Solutions for H.323 Voice,Video and Security

Prior to the introduction of the Polycom MGC's Firewall Solution, there has not been a product appropriate for ensuring network security and allowing inbound H.323 calls to be received by enterprise-managed H.323 end points.

The network manager had only the following options to propose if members of a virtual workgroup wished to place and receive H.323 voice or video calls:

- Isolate systems outside the firewall
- Install separate voice & video parallel to data networks
- Open multiple ports on a NAT firewall
- Deploy H.323 enabled firewalls & proxies
- Develop IP tunnels

Isolate Systems Outside the Firewall

One scenario is to put the H.323 end point device on the public Internet and to completely isolate it from the corporation's mission critical data network.

This scenario requires that the network manager place the H.323 endpoint device on the public Internet and prevent the user access to personal files on desktop PCs or corporate servers.The solution has been employed in small pilot or test situations to prove that IP based voice and video is realistic.

This type of configuration requires the following:

- Separate network connections from each device to the ISP
- Public IP addresses for every endpoint.
- The endpoint's IP address must be static.

It fails to offer the managers and/or users:

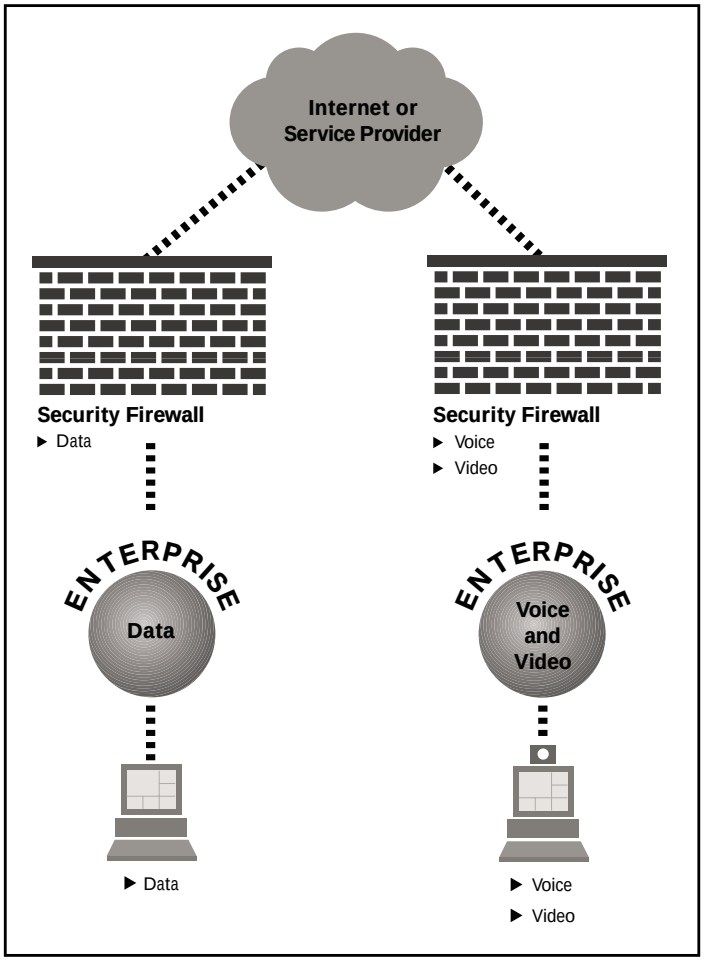
- Gatekeeper alias support.
- A way to manage or monitor bandwidth
- Protection of endpoint system from hostile attacks by systems outside the firewall.
- The ability to call users on the corporate network behind the firewall

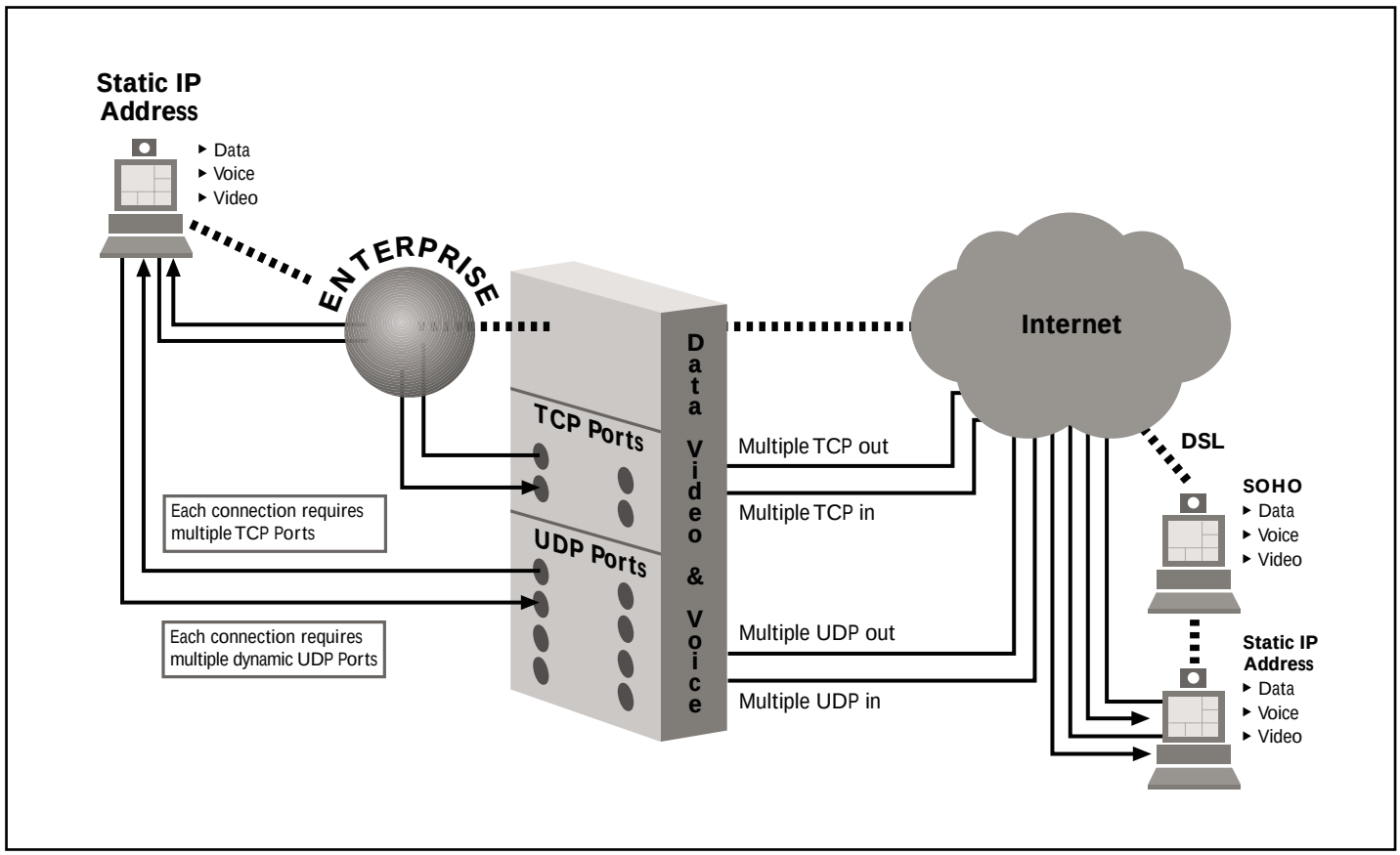
Separate Parallel Voice and Video Networks

Another scenario is to create a physically separate network of H.323 endpoint devices with special conferencing and security services.This would permit centralized management. It would also offer users access to gatekeeper functionality and pooled conferencing resources, such as multipoint control units and gateways to circuit switched networks, however, it will not be widely implemented because it fails to leverage a common core infrastructure.

This architectural approach:

- Requires separate network connections for each voice and video system, exposing the enterprise to costs and management overhead above and beyond those associated with a data network.
- Requires multiple LAN connections for a single system to have voice, video and data requirements inside the enterprise.
- Fails to secure networks from one another when a device has multiple connections to data, voice and video networks.
- Wide area communications would be unable to leverage existing data network capacity.

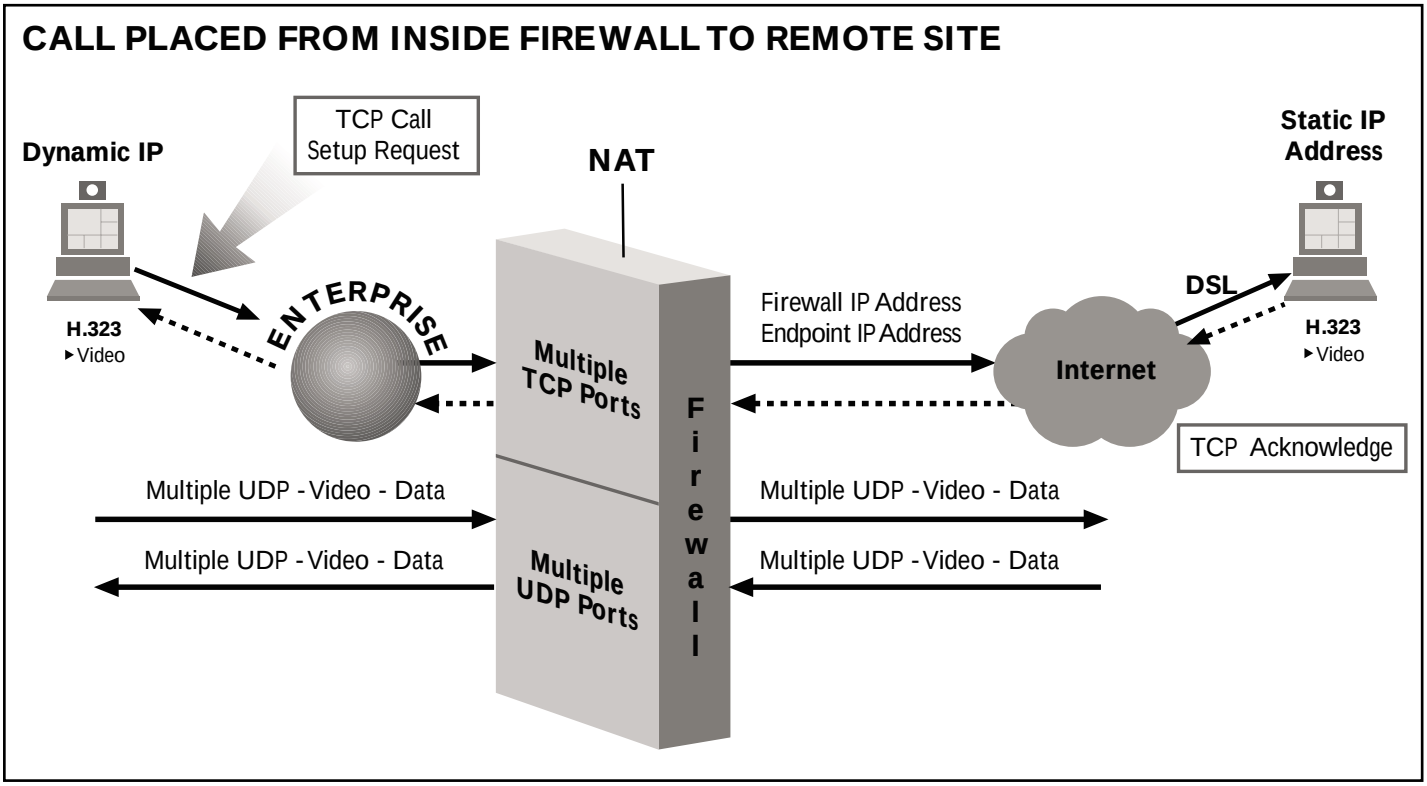




Opening Multiple Ports on a Non H.323-Ready NAT Firewall

A network manager can specify a larger than industry accepted range of ports open for TCP/IP and UDP traffic for use by H.323 entities with dynamic port needs.This scenario is unlikely to be widely implemented because it:

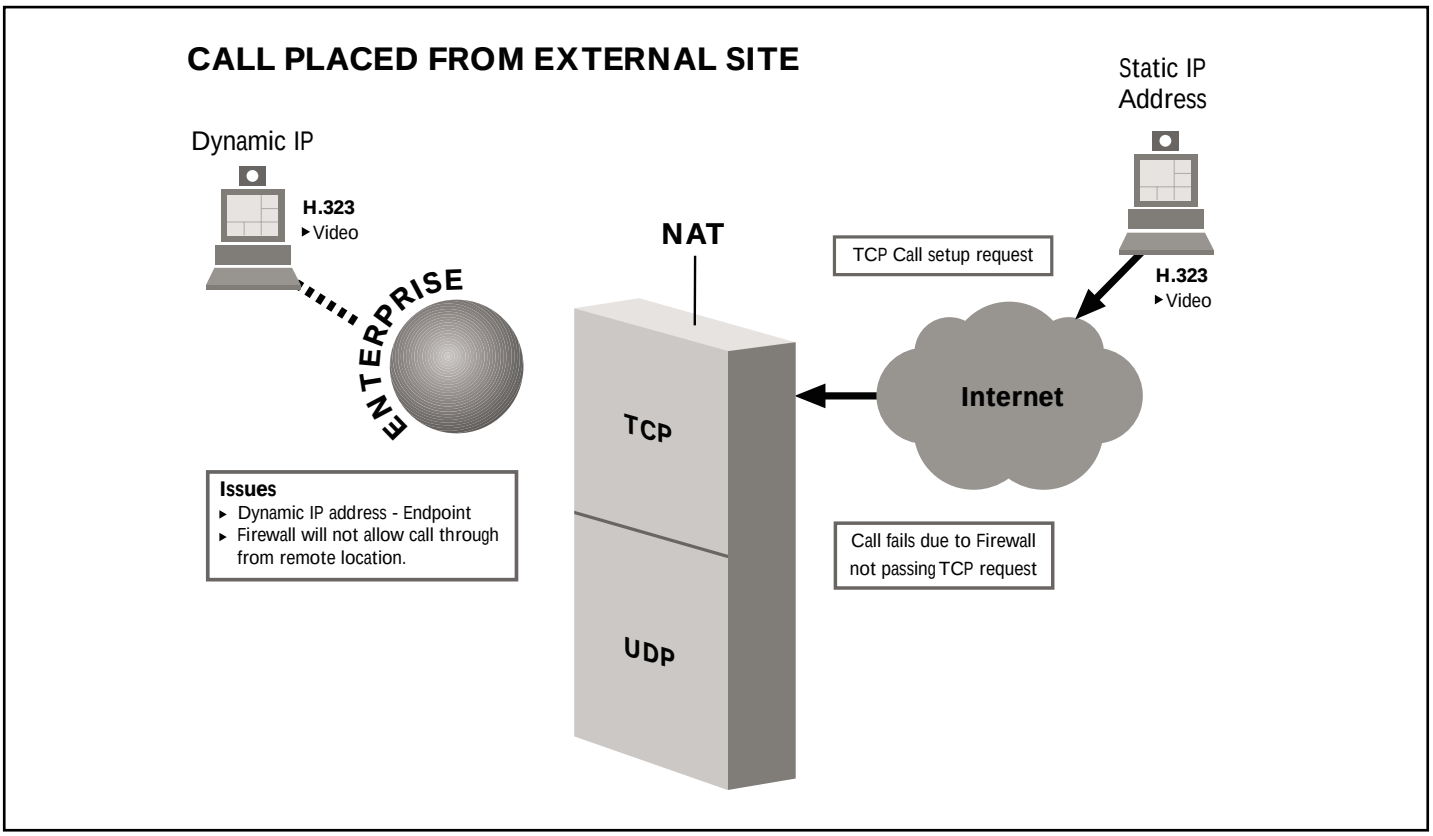
- Leaves the entire enterprise IP network open to security vulnerabilities from hackers.
- Requires multiple ports to be opened for every endpoint that requires a simultaneous point-to-point connection
- Lacks a mechanism to address the needs of multipoint connections and/or mixed voice and video connections.



H.323 Enabled NAT Firewalls & Proxies

There are H.323-compliant firewalls such as the Cisco PIX Firewall product or Check Point Software's Check Point FireWall-1. The latest versions of these products are capable of detecting H.323 protocols and passing limited address information between the secure and the public network. They perform intelligent filtering based on the application layer. When a requested session complies with policies, the firewalls permit calls leaving the enterprise network to be placed and for the media from the 'unknown' endpoint to return to the caller on the LAN.

Unfortunately, these solutions require that the firewall and security plan be modified to support voice and video. In addition, they may not scale to accommodate numerous simultaneous calls due to limitations of existing proxy server and network gateway servers' bandwidth and computational resources, as well as lack of management software designed specifically for H.323 sessions.



Even when an H.323-savvy NAT device or firewall is in place, typical solutions on the market today will terminate the media streams when the TCP H.225 channel is closed. In addition, the H.323-compliant NAT/PAT devices currently available do not support multicast because the network behind them appears as a single address preventing the router from detecting the identity of multicast requests received from inside the network.

To provide the highest level of functionality and security, a network engineer will look for solutions that offer H.323 firewalls, and proxy services that overcome NAT-related obstacles.The more functions and security, the greater the computational load on the gateway server. If the gateway server with firewall capability is unable to process and filter packets in less than 1 to 5 milliseconds it will introduce unacceptable delay in the media and reduce the spontaneity of the session and overall quality of the user's experience.

Finally, an H.323 enabled NAT Firewall is limited to one-way connection capability that allows connections to be established from inside a secure corporate network, but will not allow direct inbound dialing from 'off net'.

IP Tunneling

Some architects designing networks for real time traffic created dedicated connections around network segments they suspect to be over-subscribed or otherwise unsuitable for voice or video applications.This is known as IP tunneling.Two routers are basically hard coded to pass packets back and forth to each other under specific quality of service conditions. If two companies are known to have need for real time video and voice communications, their network managers can create IP tunnels from within two secure networks and treat the connection as a virtual private network.

This may be an option for companies who share a common business backbone, such as an industry exchange, however, it fails to offer a scalable solution for routine and ad hoc voice and video communications between business users or people on and off secure networks.

As discussed above, all current options have limitations. Most prevent effective collaboration with user files on the enterprise network or compromise security or manageability when permitting the corporate user to place calls to peers or anyone in or off the enterprise network.

While data network security weaknesses present risks most network managers will avoid at all costs, there are other less obvious risks to which the enterprise may be exposed. Opening a network to receive H.323 sessions initiated by 'off net' devices using a gatekeeper or H.323-ready proxy server may result in:

- Over-loading limited enterprise resources, such as bandwidth on IP segments or ISDN/IP gateway ports from unsolicited callers trying to reach enterprise users
- Breaches of conferencing service users' privacy from un-known and un-detected participants joining in multicast or multipoint conferences
- Inappropriate use of corporate accounts for wide area video network services via foreign computers emulating corporate users, or altering corporate user profiles

Section 3

REQUIREMENTS FOR ENABLING REAL WORLD VOICE & VIDEO OVER IP

If a product is to overcome all of the above issues, it must:

- ✓ Detect when industry standard firewalls receive H.323, H.225 or H.245 signals,
- ✓ Have the ability to route calls when the callers IP address is known to it, and caller placing an inbound call is approved
- ✓ Have sufficient bandwidth to and from it, and appropriate network interfaces (IP and IP or IP and ATM, for example) to accommodate rich media sessions
- ✓ Have ample backplane to never become a source of network delay during call set up or maintenance
- ✓ Have ample and specialized processing capability to receive and manage dozens of simultaneous sessions
- ✓ Be manageable via a secure yet browser-viewable interface, remotely and locally
- ✓ Produce reports comparable to those available for telephone or data network services
- ✓ Interoperate seamlessly with many third parties H.323 entities as well as data networking devices, and
- ✓ Be expandable to add functionality and user services as needs arise in the future.

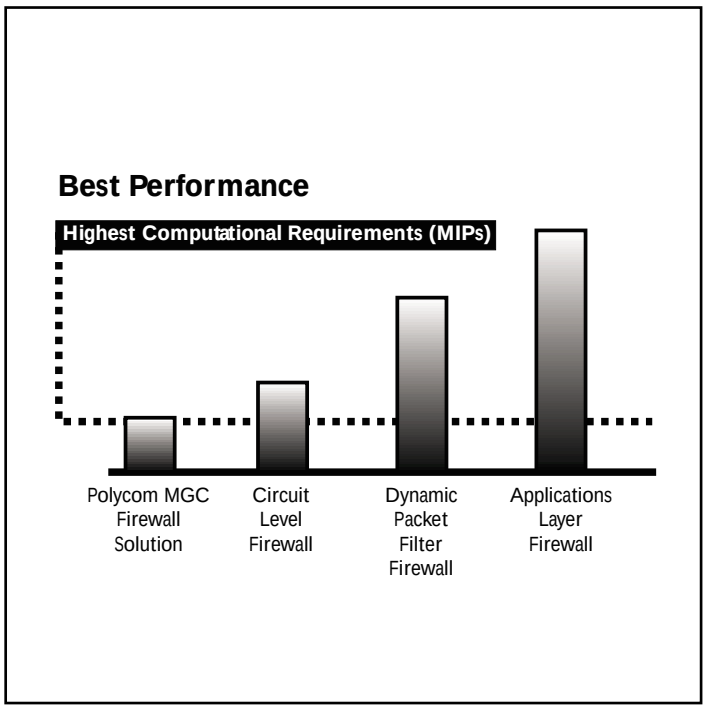
Section 4

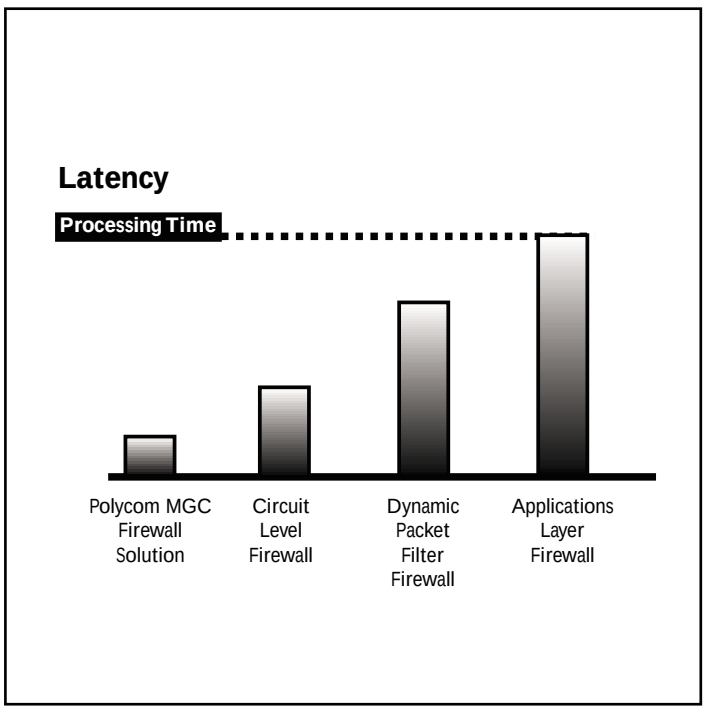
SOLVING THE CHALLENGES OF H.323 VOICE & VIDEO OVER IP NETWORKS

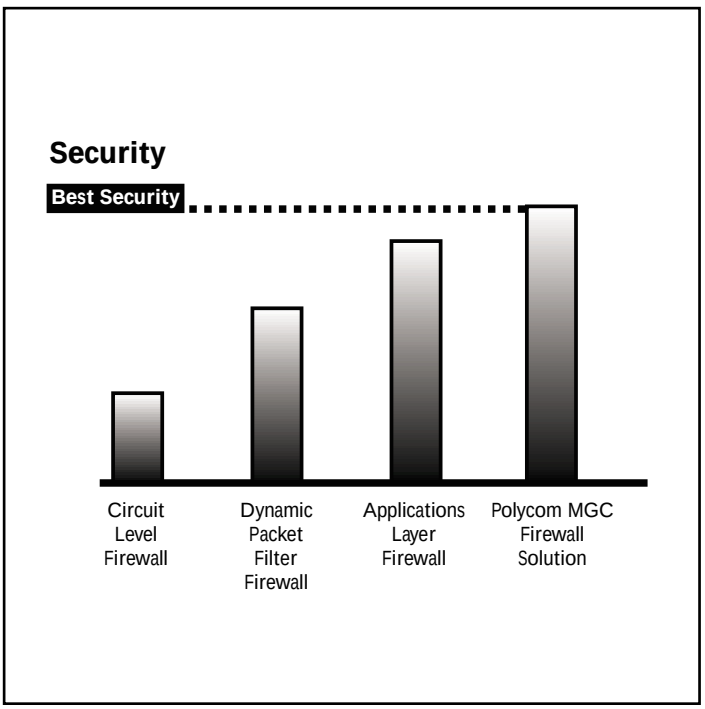
Applications that help people communicate with rich media data types and seek to use an IP infrastructure for voice and video transport and signaling must respect several overarching network design principles.

One of the most fundamental principles of an IP network designed for mission critical data applications is to protect the integrity of the network's resources and users from attack by hostile businesses or people.

It is evident that network address and port translations, enterprise data security and H.323-support have been difficult goals to reconcile without compromising enterprise network security. In response to these challenges, is the Polycom MGC Firewall Solution.







The Polycom MGC Firewall Solution is a Next Generation H.323 ITU-compliant gateway solution specifically designed to solve the issues of security, policy and NAT/PAT proxy for H.323 voice and video applications over IP networks. The system compliments the existing firewall and is easily managed via a standard web browser interface using the Polycom MGC's WebCommander Management Suite. The Firewall Solution supports from 12-48 simultaneous sessions.

The Firewall Solution supports a wide range of video and audio algorithms and even allows algorithms to be mixed in a call using the Polycom MGC's unique transcoding technology.

Algorithms Supported:

- Audio — G.711a, G.711u, G.722, G.722.1, G.723, G.728
- Video — H.261, H.263
- Data Rate — Up to 768k
- Frame Rate — 7.5fps, 15fps, 30fps
- Resolution — FCIF, QCIF

Scalable Broadband Visual Communications Architecture

The Polycom MGC's Firewall Solution provides enterprise class reliability in a stand-alone or rack mountable chassis.

- Supports 12-48 simultaneous sessions
- Connection speeds up to 768K (IP)
- Mission critical fault-tolerant design
- 8 or 16 slot chassis
- All modules:
  - Front accessible
  - Hot-swappable
  - Self-configuring
  - Compatible across the Polycom MGC platform

Advanced Transcoding (Optional)

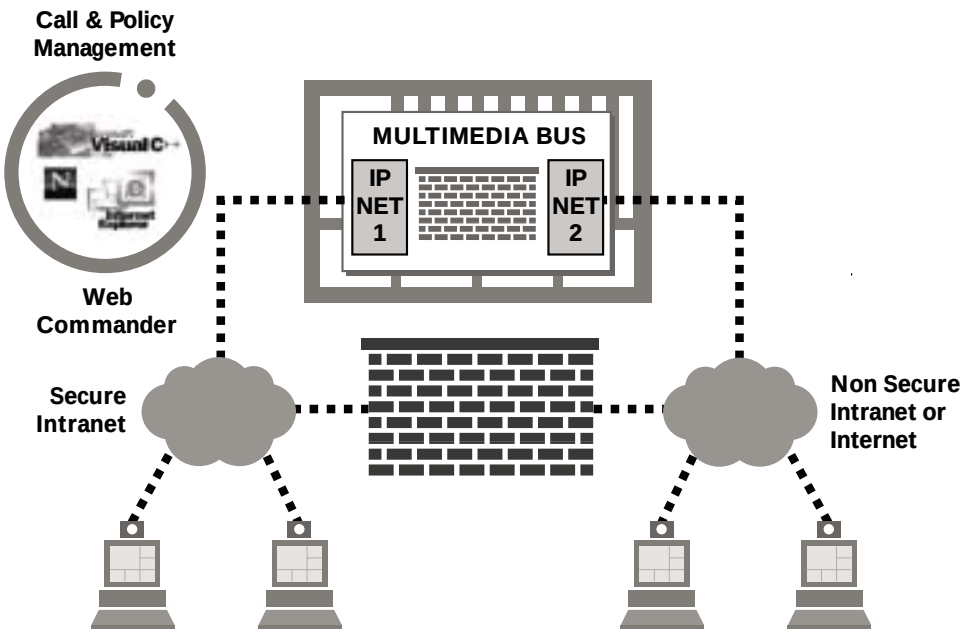
- Allows sites with different frame rates, connection speeds, audio algorithms, resolutions and network protocols to transparently connect with one another.
- Ensures that all sessions connect at their optimal capabilities.
- Ensures that sessions start on time by simplifying the connection process.
- Ensures conference reliability

Powerful Management System

The Firewall Solution provides the most flexible suite of system and session management applications of any gateway in its class.

- Web based end user management that allows easy setup up of on-demand and scheduled sessions via WebCommander™ Server software.
- Web based Administrator management that allows network managers to set policy based on group and user access via WebCommander Server software.
- Secure management via standard http port via WebCommander Server software.
- Comprehensive configuration, monitoring and diagnostic software that enable complete resource, conference and equipment management through MGC Manager™ .

The Polycom MGC's Firewall Solution seamlessly and transparently addresses the complexities of both the IP network manager and H.323 voice and video users. With the Firewall Solution, video network architects have the industry's simplest solution to a complex problem without compromising security, creating bottlenecks or limiting functionality originally envisioned for converged voice, video and data networks worldwide.



POLYCOM®

www.polycom.com

Polycom Inc., 1565 Barber Lane, Milpitas CA 95035 (T) 1.800.POLYCOM (North America) +1.408.526.9000 (F) +1.408.526.9100
Polycom Network Systems, 9040 Roswell Road, Suite 450, Atlanta, GA 30350 (T) +1.770.641.4400 (F) +1.770.641.4499
Polycom EMEA, 270 Bath Road, Slough, Berkshire, England SL1 4DX (T) +44 (0)1753 723000 (F) +44 (0)1753 723010
Polycom Hong Kong Ltd, Rm 1101 MassMutual Tower, 38 Gloucester Road, Wanchai, Hong Kong (T) +852-2861-3113 (F) +852-2866-8028

Inventory Number/Date