Traversal of IP Voice and Video Data through Firewalls and NATs

A RADVISION Technology White Paper

Contents

Introduction

In recent years the Voice over IP and the Multimedia over IP industries have been gradually moving from an experimental stage to real deployment. Multimedia over IP communications run on the same IP networks as other IP applications. Almost all these IP networks deploy Firewalls and/or NAT devices, for security

Unfortunately, the inherent characteristics of Multimedia over IP protocols are in conflict with most current mechanisms employed by Firewall and NATS, resulting in "slower-than-desired" deployment of Multimedia over IP communications. As a result of this trend there is a growing awareness of the Firewalls/IP predicament.

A number of organizations and vendors have presented proposals and solutions to overcome the problem. There is no single solution. The complexity of the problem together with the diversity of existing topologies means that different solutions are needed for different cases.

In this white paper RADVISION examines the implications of traversing voice and video packet data through Firewalls and NAT devices and describes a selection of solutions and the issues they raise.

Basics

This section takes a brief look at Firewalls and NATs, how they work and how they co-exist with Multimedia over IP Protocols.

Devices in the Middle

The most common method for preventing undesirable penetration of a network is to place a device between the "inside" network and the rest of the world, the "outside" network. These devices fall into two categories: Firewalls and Network Address Translation devices (or a combination of both).

Firewalls

A **Firewall** is a barrier device placed between two separate Networks.

The two most prevalent types of Firewalls are Packet Filters and Application Layer Gateways and they work as follows:

- **Packet Filters** block traffic. Packet Filters are also called Screening Routers. The filtering method is based on IP address and/or port numbers. Packet Filters examine information at the packet header level. They impose security restrictions at lower layers usually by inspecting IP and TCP /UDP packet headers against tables of filtering rules. Based on the information it extracts from the packet headers, the Packet Filter makes security decisions such as "forward this packet" or "don't forward this packet".

  "Packet Filters" Firewalls typically use static rules for allowing desirable data (that is normally blocked by them) to pass through.

  There are two kinds of static rules—well known and configurable:

  - An example of a well-known rule is the TCP port 443 used for HTTP over TLS/SSL (HTTPS). This address is traversable through any Firewall since Firewalls are not capable of decrypting the data transmitted on this secured connection.
  - Configurable rules typically consist of source and destination addresses that are allowed to send and receive data through the Firewall. Both source and

destination addresses are defined by a range of IP addresses, UDP or TCP port numbers and the protocol identifier, which is embedded in a UDP or a TCP payload. Not all Firewalls support configurable rules.

- **Application Level Gateways (ALGs)** serve as a relay between two networks. ALGs are application-aware entities that examine application protocol flows and only allow messages that conform to security policies to pass through. ALGs may also modify messages so that they will conform to the policies and be able to pass through. ALGs are discussed in detail in the section "Protocol-Aware Firewalls" below.

  Sometimes ALGs are erroneously referred to as Proxies. There is a difference between the two. ALGs are transparent to the multimedia entities but Proxies are not. Proxies are an integral part of the multimedia system. For example, for H.323 the Proxy would be a gatekeeper (most probably with basic/limited functionality) while for SIP it would be a specialized SIP Proxy.

A Firewall can be implemented in a single router that filters out unwanted packets or it can use a variety of technologies in a combination of routers and hosts. In the latter, network administrators centrally define and maintain the restriction policies. Today many Firewalls combine filtering functionality (described above) with NAT functions (described in the following section).

Network Address Translation Devices

Network Address Translation (NAT[1]) devices translate an IP address used within one network to a different IP address known within another network. One network is designated the *inside* network (for example, an enterprise LAN) and the other is the *outside* (for example, the Internet). Users on the inside network can see the outside network but the outside cannot see the inside users, as all communication with the outside network is via the translation device.

Each outgoing or incoming request must go through a translation process, which is dynamic and transparent to the applications. This provides an opportunity to qualify the data by matching the source and destination of a packet in one direction to those of a packet in the opposite direction.

Typically, NAT devices let all the outgoing traffic traverse network boundaries. The addressing information of the packet is stored with a timeout. Packets flowing in an opposite direction that have matching addresses are allowed into the internal network. This technique of creating dynamic rules is called "pinholing".

Typically, on outgoing packets a NAT device map local inside network addresses to one or more global outside IP addresses. On incoming packets the NAT device maps global IP addresses back into local IP addresses.

There are two flavors of Network Address Translation devices:

- A Network Address Translation (**NAT)** device allows an organization to use a range of private IP addresses when communicating within an inside network and to share a small pool of public IP addresses when communicating with an outside network.
- A Network Address Port Translator (**NAPT**) or Port Address Translator (**PAT** for short) device has a block of inside addresses and one or more outside addresses. The port number is the differentiator, as shown in Figure 1.

[1] The generic term NAT is used in this document to indicate both forms of Network Address Translation, unless otherwise specifically stated.

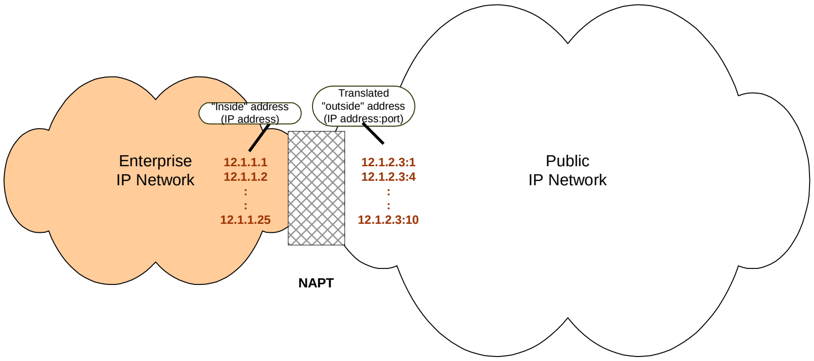

Figure 1: Network Address Port Translation

Multimedia Protocols over IP

Multimedia Protocols over IP have particular characteristics that impact Firewall and NAT solutions. To understand this, we take a brief look at what call setup/signaling and media stream traversal mean to Multimedia Protocols over IP.

Call Setup and Signaling

The protocols used for voice and video call setup and signaling over IP are SIP, H.323, MGCP and Megaco/H.248. These protocols use TCP as well as UDP for call setup and transport. TCP and UDP use port numbers to identify individual connections.

In all the above-mentioned IP protocols, transport addresses[2] are embedded in the messages of the protocol. This results in a “conflict of interests”.

Firewalls are configured with strict rules specifying static ports through which desirable data can pass while undesirable data is blocked. H.323 uses dynamically allocated port numbers. For example, an H.323 call typically requires a TCP connection for H.245 signaling and H.245 does not have a well-known port associated with it. The H.245 port is dynamic so it is clear that the Firewall will block the H.245 message and the call signaling procedure will fail.

Similar issues affect NAT devices. For example, a SIP User Agent A, inside the network and behind a NAT, sends an INVITE message to User Agent B on the outside. In the simplest case, User Agent B extracts the *From* address from the INVITE message and sends a *200* (Ok) response to this address. Because the INVITE message came from User Agent A behind the NAT, the *From* address is “fictitious” (private) and incorrect. The *200* will not succeed and the call will not be connected.

Traversal of Media Streams

All multimedia IP protocols use RTP for transporting the media streams. RTP runs over UDP and has no fixed ports associated with it[3]. Each type of media stream has one or more channels but each channel requires its own pinhole to be opened. This means that for the media stream to traverse the Firewall, the Firewall needs to open many UDP pinholes for each call session. Thus the network behind the Firewall is exposed defeating the *raison d'être* of the Firewall!

[2] Transport addresses are IP addresses together with UDP or TCP ports.
[3] The call signaling protocol dynamically assigns the ports.

Even if though the pinholing technique, described above, would be applied to the outgoing media flow, it would not solve the whole problem. Typically, the incoming and the outgoing media streams within the same multimedia session do not follow the same paths, in terms of UDP port numbers (and in some applications even in terms of IP addresses).

A further problem arises from the fact that multimedia protocols don't necessarily know the source port of the media stream. This means that in some cases even application-aware Firewalls would not be able to dynamically open minimal tight pinholes.

Because of its connection-oriented nature TCP has traditionally traversed Firewalls more easily. Some of the solutions suggest traversing of media over TCP or/and using TCP tunneling. However, TCP has been designed for reliable streaming of large blocks of time insensitive information. Voice and video data is time sensitive (real-time) and relies on fast delivery of small unreliable packets. UDP is well suited for real-time media streams while using TCP for media streams results in poor voice and video quality.

Deployment

Another factor to consider is the actual working environment of the network. Firewalls and NATs are widely deployed in many types of environments, supporting a variety of topologies and serving a variety of users. Each type of environment, topology or user may require a different type of security solution. For example, where an MIS department of a large enterprise administers and controls the network and its security policies, a small home office typically has a few computers, uses an off-the-shelf NAT device and relies on an ISP for network services.

Further, legacy investment in Firewalls and NATs, including the establishment of policies, results in a reluctance to change or upgrade hardware devices and/or security policies.

Solutions and Issues

The “Basics” section described the main types of devices that control the traversal of desirable data between separate networks and the conflict between these devices and the inherent characteristics of Multimedia over IP Protocols. This section presents a number of solutions and examines how effective they are in terms of protocol awareness, performance and stability, media stream traversal, deployment, and/or upgrading.

Protocol-Aware Firewalls

The mechanisms on which Firewalls and NAT devices are built need to know the IP address and/or port of the incoming or outgoing data. As all Multimedia over IP Protocols embed the IP addresses and ports in the protocol messages, a Firewall or NAT device needs to have knowledge of the protocol so that it can extract, use or alter the IP address/port. One way of making this knowledge available to the Firewall is at the application level. An ALG Firewall can be designed to be protocol-aware for specific protocols.

In order to complete the solution, usually ALGs also control new incoming calls by maintaining a configurable access list of the addresses of multimedia entities.

Figure 2 shows a SIP or H.323 IP phone inside an enterprise IP network calling a telephone on an outside Public Network via a protocol-aware ALG Firewall.

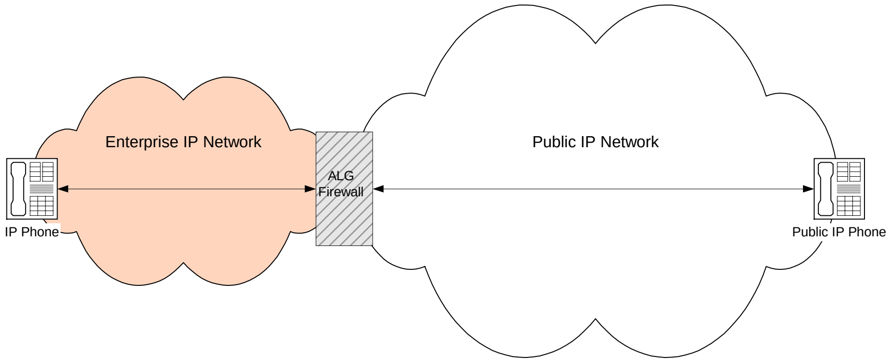

Figure 2: Protocol-Aware Firewall

Issues

Although the concept of a protocol-aware ALG Firewall seems a practical solution, the following issues should be considered:

Deployment and Upgrading

In systems where multimedia security schemes are implemented[4] there is a major drawback. If the protocol messages are encrypted and the ALG is not an application layer trusted entity in possession of the necessary keys and algorithms, the inspection at the ALG level will fail.

As most Firewalls deployed in networks today are not multimedia protocol-aware they would have to be upgraded to become protocol-aware. In actual networks, a chain of Firewalls and NAT devices is usually deployed along the traversal path of the multimedia streams. In order to ensure multimedia traversal, each Firewall needs to be a protocol-aware ALG. This means new investments and control changes to already deployed Firewalls.

Further, as multimedia protocols are on the technology edge and new versions of these protocols are frequently released, the ALGs need to be frequently upgraded to support new protocol versions.

The ALG approach is not applicable to SOHO environments, where simple NAT devices are widely in use.

Performance and Stability

ALG Firewalls are potential bottlenecks in the network since they require additional logic and processing to parse and understand the application protocol. Leading Firewall vendors provide development environments around their Firewalls. This enables third party vendors to develop and add-on their own functionality but it introduces additional security, stability and maintenance issues.

Availability

Most Firewalls currently available on the market are not multimedia protocol-aware. Although some Firewalls do support H.323 traversal, vendors do not all support the same or the latest version of H.323. Currently, there are no SIP-aware Firewalls in the market.

[4] Such as the ITU-T H.235 Recommendation, which is under the “umbrella” of H.323.

Certain vendors have declared that in the near future they will release ALG Firewalls with SIP functionality.

Some application level Firewalls are capable of performing NAT functions together with the Multimedia over IP Protocols but there are currently no stand-alone ALG NATs in the market.

Middlebox Communications

Middlebox Communications[5] (**MidCom**) is an emerging concept that makes Firewalls and NAT devices more controllable through third parties.

The idea is to allow third party trusted applications to make policy decisions on behalf of the middle entities enforcing transport policies. These trusted applications should be able to communicate their needs to the devices in the "middle" using the new protocol to be defined by MidCom. Trusted third parties assist the Firewalls or NAT devices to operate without having to resort to embedding application intelligence. By doing this, the Firewalls or NAT devices continue to provide security services while remaining protocol agnostic at the application level.

Figure 3 shows a SIP or H.323 IP phone on an inside enterprise network calling a telephone on an outside Public Network via a Firewall. A simple but highly secure protocol, the MidCom protocol, is defined with the dedicated task of opening and closing transport ports (UDP and TCP) and/or managing NAT mappings at the Firewall/NAT. A protocol agent, residing on the Firewall, dynamically opens pinholes upon request of the SIP Proxy or standard gatekeeper.

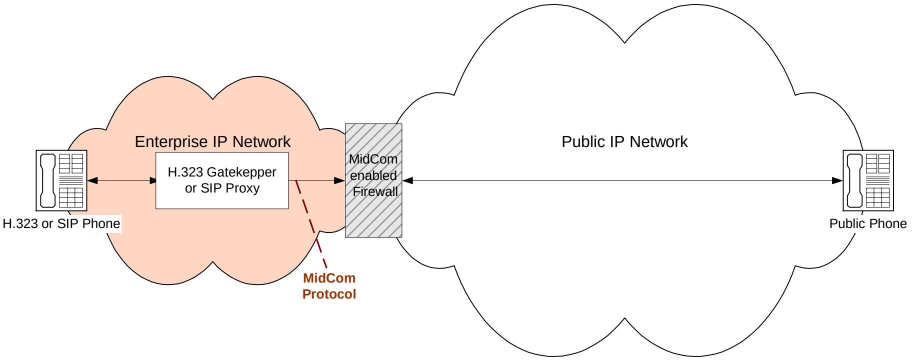

Figure 3: Middlebox Communications Solution

Issues

The Middlebox Communications approach solves the problem of encrypted communications. Unfortunately, the currently proposed schemes, especially for NAT environments, result in complicated scenarios requiring a considerable amount of coordination between many entities.

[5] The IETF has recently (2001) established a workgroup, Middlebox Communication (MidCom) to define this protocol. For more information see: www.ietf.cnri.reston.va.us/html.charters/midcom-charter.html

Performance

By offloading the resources required to process the protocols, the MidCom approach addresses performance issues in enterprise networks, where a multimedia IP protocol server such as a SIP Proxy or standard gatekeeper would be deployed anyway.

Deployment and Upgrading

The protocol agent, running in the Firewall, is protocol agnostic. Therefore, the deployment of Firewalls that support a MidCom protocol theoretically allow for a common infrastructure that supports all application protocols including various Multimedia over IP Protocols.

This kind of solution is suitable mostly for an enterprise as the enterprise administers its own Firewall. Further, for security purposes the SIP Proxy or standard gatekeeper is usually located behind the Firewall and the control protocol can thus also dynamically provide configuration information such as access lists.

Theoretically, MidCom is also suitable for ISP because an ISP could use a MidCom protocol to control a Firewall from outside of the Private Network. Practically, this is unlikely to happen because of security reasons. Furthermore, typically end users use two different service providers—one as a transport provider and the other as the multimedia or conference service provider.

Availability

The IETF MidCom Working Group is in a very early stage and no standard protocol definition is available yet. All currently available solutions are proprietary.

Application Servers

One of the solutions that addresses the UDP and the *many holes*[6] issue is an Application Server that provides the functionality of a SIP Proxy or standard gatekeeper and also acts as a proxy for multimedia RTP/RTCP streams.

The Application Server can be decomposed further into a Call Signaling part and RTP/RTCP units that are tightly controlled by the Call Signaling unit[7]. By providing a proxy for RTP/RTCP streams in a single entity, the enterprise now has the ability to apply more restrictive rules to the Firewall.

An example of this type of solution places an Application Server behind an existing Firewall. The Firewall is configured to allow multimedia communications *from* and *to* the Application Server for both signaling and media. This reduces the number of *holes* that UDP requires.

Further, if NAT is activated in the Firewall, the Firewall can be configured to allow all *from* and *to* traffic to bypass the NAT service.

[6] See “Traversal of Media Streams” on page 5

[7] More precisely, these units don’t need to be aware of RTP or RTCP. The forwarding may be accomplished on UDP and TCP layers.

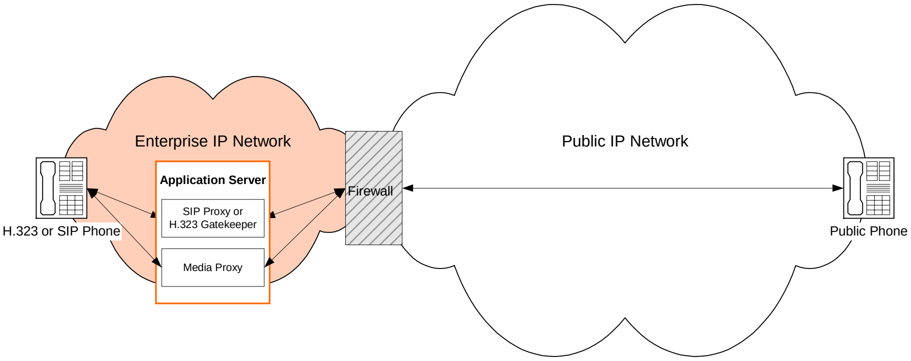

Figure 4: Application Server with a dedicated Media Proxy

In order to protect the Application Server, and provide a realistic solution for networks where NAT is deployed, the Application Server can be placed in a so-called Demilitarized Zone (**DMZ**). The DMZ technique enables an enterprise to host Application Servers with public access while still protecting its Private Network. The DMZ technique utilizes a Firewall architecture consisting of three separate segments with different security priorities. One segment is for the trusted corporate Private Network, one segment is for the distrusted Public Network, and the third segment is the Demilitarized Zone. Typically, the DMZ contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, e-mail (SMTP) servers and DNS servers. For these types of services, logically the DMZ resides between the Public (Internet) and the Private Networks.[8]

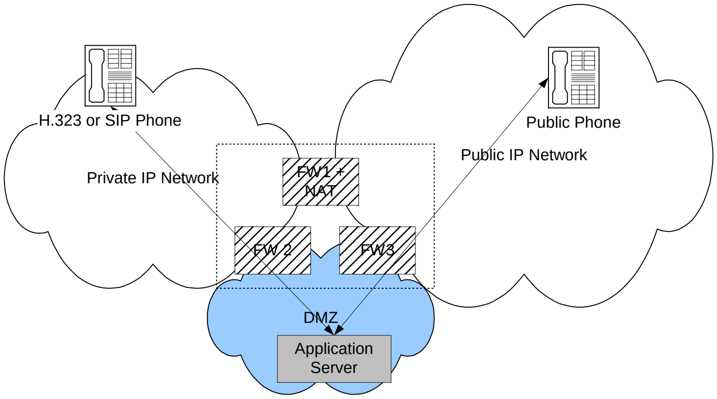

Figure 5: Application Server within a Demilitarized Zone

In the scenario shown in Figure 5, the DMZ is schematically implemented by a single Firewall with three different sets of rules represented in the picture by FW1, FW2 and FW3. The FW1 rules do not usually allow for any multimedia communications. In addition, NAT is activated to shield the private IP addresses from the Public Network.

The Application Server is located in the DMZ.

[8] A DMZ can be built using a single Firewall that has more than two NICs and an ability to configure a separate set of rules for each NIC. Alternatively, a DMZ can be built using a number of simple Firewalls, Gateways, and a NAT

On the Public Network side, the Application Server appears as a public SIP Proxy or standard gatekeeper that receives communications for enterprise users by their aliases. The destination address for both signaling and media streams is that of the Server itself. The SIP Proxy or the gatekeeper uses application layer address translation to cross the boundaries between public and private addressing schemes.

If the enterprise wishes to have open multimedia communications, FW3 rules would allow traffic to flow *from* and *to* the Application Server's public addresses. If the enterprise wishes more restrictive public communications, a limited list of specific allowed public addresses would be configured at FW3.

The Application Server uses a local addressing scheme towards the Private Network. For tighter security, FW2 rules may be defined to allow multimedia communications *from* and *to* the Application Server only.

Issues

Availability

A number of well-known vendors provide variations of Application Servers. All of them are *proxy* to the media. Usually these Application Servers have many configuration options in order to support various topologies defined by the enterprise.

Virtual Private Network (VPN) and Secure Tunneling

VPN technology is one of the approaches being used today for providing secure communications over IP Networks. Looking to the future, Virtual Private Routed Networks (VPRN), which will ensure both security and QoS characteristics, promises to be an attractive solution for Multimedia over IP communications.

Usually, the IPSec[9] layer below the UDP and TCP is used to provide secure IP communications. There is a conceptual problem with an IPSec based VPN technology as it has its own mechanisms that are not viable for NAT, particularly NAPT. The IPSec layer uses its own link identifier instead of UDP or TCP ports, on which NAPT is based, and further, the layers above the IPSec, which include UDP and TCP, are encrypted.[10]

[9] **IP SEC**urity is a security protocol from the IETF that provides authentication and encryption over the Internet.

[10] Currently IETF has started work for tunneling IPSec communications over open UDP connections in order to resolve the "VPN through NAT" problem.

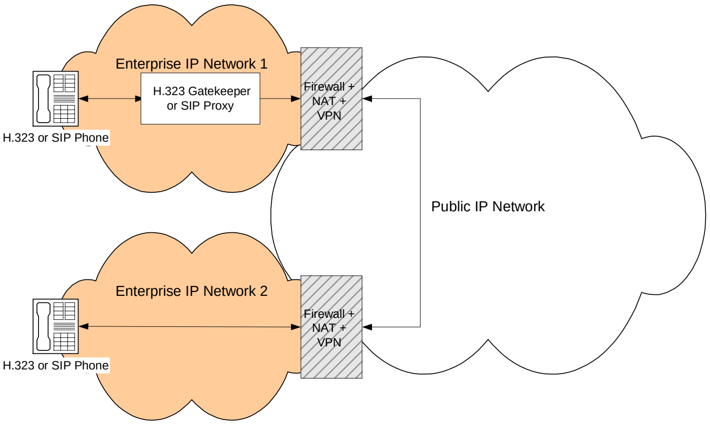

Figure 6: Using VPN

Issues

The VPN solution is very secure. Its major drawback is that it only allows for communication among sites belonging to the same VPN, and does not allow for connectivity *from* and *to* end users or services located on a Public Network.

Following are further issues to consider:

Deployment and Upgrading

In order to resolve the NAPT traversal problem, it is possible to choose a solution based on a single manufacturer that provides an application that integrates the Firewall, NAPT and VPN functions.

When communications are required between separate networks that have their own NAT private schemes none of the solutions are trivial. Again, SOHO environments that make use of stand-alone NAT solutions present acute problems for the use of IPSec technology.

It is possible to overcome the obstacles described above by implementing creative proprietary *VPN for multimedia* schemes, without actually using IPSec technology. For example, an approach would be to use an ALG or a Proxy, residing behind the Firewall/NAT, which makes as few as possible pinholes in the Firewall, even for the traversal of media streams. To achieve this, the ALG or Proxy can tunnel or multiplex the multimedia data over a small number of TCP, HTTP, or secure HTTP channels.

Application Server Agent

The Application Server Agent solution offers a totally new way of decomposing an Application Server. This solution is a combination of ideas borrowed from the “Virtual Private Network (VPN) and Secure Tunneling” solution with a straightforward way of addressing the NAT issues related to traversal of media over UDP, as described in “Traversal of Media Streams”.

An Application Server implements all the application logic from outside the Firewall and works together with an Agent located in the Private Network. Using a simple secure protocol, the Application Server instructs its Agent through a well-known rule in the Firewall. Upon receipt of the instructions, the Agent performs UDP and TCP transport layer switching and/or multiplexing of packets in both directions.

The communication between the Application Server and its Agent requires a very limited number of rules and pinholes through the Firewall. The multimedia data (signaling and RTP media streams) are either logically or physically multiplexed or tunneled through the pinholes.

The Application Server together with its Agent logically comprises a SIP Proxy or gatekeeper for both Private and Public Networks as shown in Figure 7 below.

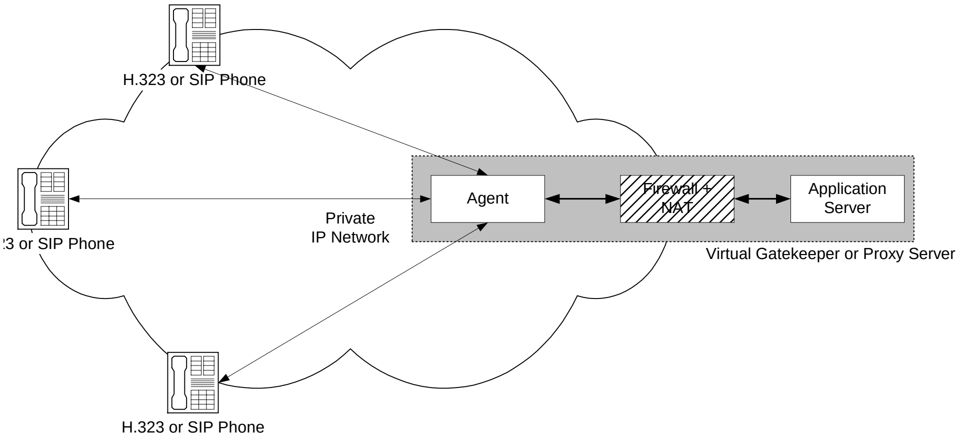

Figure 7: Application Server Agent Decomposition

In certain implementations, the multimedia packets do not carry additional multiplexing information. In order to associate packets to a call or a media stream, the Application Server and its Agent use the information exchanged by the control protocol and the IP transport addresses of the packets.

Figure 8 shows this solution applied in an ISP/SOHO topology. The ISP hosts the Application Server inside its DMZ. The Application Server is protected by the ISP Firewall and provides connectivity between the two Private Networks. These Private Networks are subscribed to the ISP service and run Agents inside the networks.

As shown in Figure 8, the ISP provides connectivity to public users or other ISPs using standard multimedia protocols. In this case the list of the public users/ISPs can be configured in the ISP Firewall

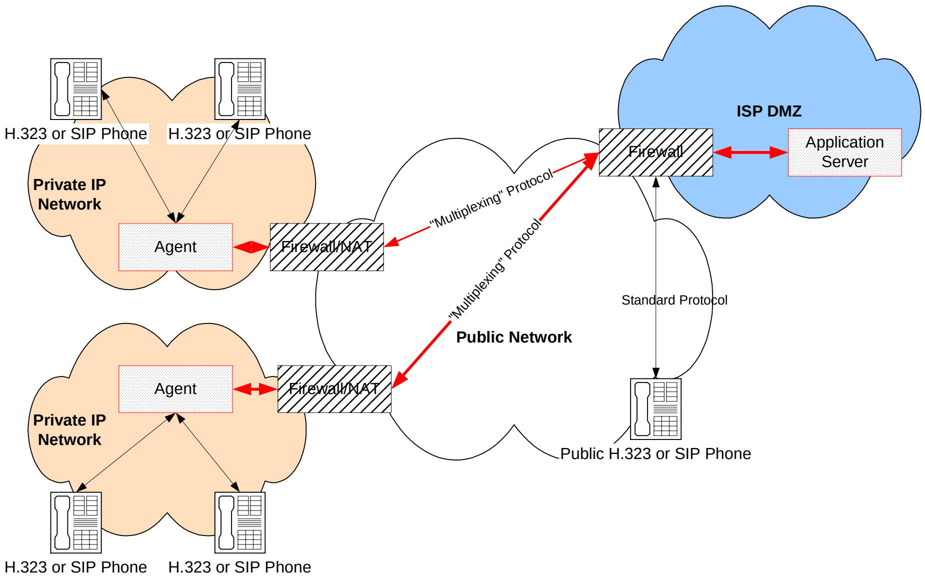

Figure 8: Application Server Agent in an ISP Topology

Issues

This new Application Server decomposition provides an effective solution for ISP and enterprise environments. Following are issues to consider:

Deployment and Upgrading

As there is currently no standard (although there are attempts to start a working group in the IETF) the control protocol running between the Application Server and its Agent is a proprietary solution.

In the Application Server Agent solution the Application Server is located at the premises of the Service Provider and is considered a trusted entity.

This solution does not compromise Firewall security because it is not based on Firewall and NAT control beyond a small number of static rules and utilization of pinholing methods in use on the Internet today.

If Firewall configuration is not available and/or it does not support pinholing, the well-known TCP traversal rules may be used and the solution still works. In the worst case, all the traffic can be tunneled through these holes that are the lowest common denominator for all Firewalls. For example, as a last resort you can tunnel using TLS/SSL on the HTTP port 443. Thus, the solution is also viable for complicated topologies involving a chain of uncontrolled and/or unknown Firewalls and NAT.

The Application Server Agent is application protocol agnostic because it performs packet switching on the Transport Layer only. Thus, the same Agent can be implemented and deployed for all multimedia protocols such as H.323, SIP, MGCP and MEGACO/H.248.

A single Agent can theoretically serve an unlimited number of users in the Private Network. Alternatively, a separate Agent that resides either in the same device or in an external box can be deployed for each end-user.

SIP Proposal

A SIP solution targeted for a SOHO/ISP environment has been proposed in an IETF draft[11]. In this solution the end user has little or no control over the Firewall or NAT, and the Firewall or NAT is completely ignorant of SIP. The solution may be applied for enterprises as well.

The resultant flow of signaling and media resembles the Application Server Agent approach described above. The SIP Solution differs from the Application Server Agent solution mainly because the SIP User Agents and Proxy Servers themselves implement the Firewall and NAT-oriented logic (according to the draft).

The assumption here is that SIP entities are aware of the Firewall/NAT deployment and use special techniques and additional procedures to work in this topology. This premise for network distributed support of Firewalls and NATs is based on significant functional changes to SIP systems and still needs to be proven for real deployment. The solution proposes TCP based call establishment, use of new SDP extensions and changes in RTP/RTCP operations.

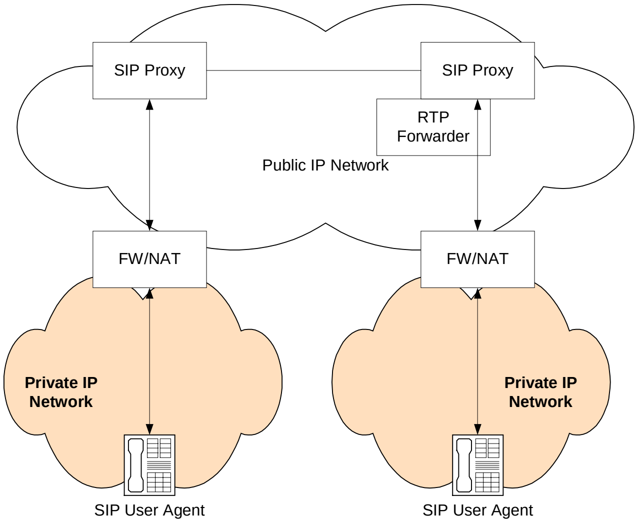

Figure 9: SIP Solution

Conclusions

In recent years the IP-Centric Conferencing industry has been slowly moving from an experimental stage to real deployment. As a result of this trend, the Firewalls/IP “predicament” has become evident and many solutions have been proposed on the market. Due to the complexity of the problem and a variety of existing topologies, different solutions should be applied for different cases.

If the Private Network needs to be isolated, a VPN, providing NAT functionality and ensuring appropriate QoS, is the simplest option to deploy.

For those who want to move Multimedia over IP communication to a global arena, the solutions and issues discussed in this paper indicate that the most promising options are:

[11] J. Rosenberg and H. Schulzrinne describe this solution in the IETF “draft-rosenberg-sip-entfw-02.txt”.

- **Protocol-aware Firewall**

  The most straightforward solution for an enterprise would be to deploy and continually upgrade a multimedia protocol-aware Firewall. However, the Protocol-aware Firewall solution ceases to be viable in environments where multimedia security schemes are deployed.

- **Application Server**

  This solution has an Application Server that combines the functionality of a standard gatekeeper or SIP Proxy with those of a proxy for RTP/RTCP multimedia streams. The Application Server can also perform address translation functions.

  Placing the Application Server in a DMZ of the enterprise improves the feasibility and security of the solution significantly. It allows for simpler functionality of the Application Server reducing the cost of its development, deployment and maintenance. In other words, with a DMZ, the division of labor between the non application-aware Firewall or NAT and the Application Server is achieved in the most balanced way.

  The Application Server can be further decomposed into the Call Signaling part and the RTP/RTCP units. This decomposition improves scalability of performance and provides a call signaling protocol-agnostic implementation of the media proxies.

- **Application Server Agent**

  To date, the most promising solution for ISP and consequently, SOHO environments, is the Application Server Agent. Assuming that SOHO environments do not deploy application-aware Firewalls or Firewalls with high-end Application Servers, a solution using a protocol-agnostic but simple Agent inside the Private Network is most attractive.

  The proposed SIP solution suggests a similar approach but defines new procedures within SIP in order to support it. Currently the SIP draft is a moving target and requires numerous network devices to coordinate at the application level in order to overcome Firewall/NAT potential deployment.

Table of Comparison

The following table summarizes the main features offered by the solutions described in this white paper.

	Suitable for Enterprise/ ISPs	**Requires Firewall/ NAT Upgrades**	**Additional Proxying of Media**	**Level of Maintenance**	**Needs Changes to Multimedia over IP Protocols**
VPN	Enterprise	Yes	No	Low	No
ALG	Both	Yes	No	High	No
MidCom	Enterprise	Yes	No	High	Not certain yet
Application Server	Enterprise	No	Yes	Low	No
Tunneling	Enterprise	No	Yes	Medium	No
Application Server Agent	Both	No	Yes	Low	No
SIP Proposal	Both	No	Yes	Medium	Yes

Glossary of Terms

Abbreviation	Description
ASA	Application Server Agent
H.235	H.323 security
H.323	The ITU standard for videoconferencing over packet switched networks
IETF	The Internet Engineering Task Force
IPSec	A security protocol from the IETF
ITU	International Telecommunications Union
MEGACO/H.248	H.248 (also known as the Megaco protocol) is the standard for allowing a media gateway controller (MGC) to control media gateways (MG).
MGCP	Media Gateway Control Protocol as defined by the IETF informational RFC2705
MidCom	Middlebox Communications
NAPT	Network Address Port Translation
NAT	Network Address Translation
NIC	Network Interface Card
PAT	Network Port Translation
QoS	Quality of Service
RAS	Registration Admission Status protocol
RTP/RTCP	Real-time Transport Protocol/ Real-time Transport Control Protocol
SIP	Session Initiation Protocol
SOHO	Small Office Home Office
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VPN	Virtual Private Network