

Aethra Solutions

to

NAT - FIREWALL Interoperability

1 Executive Summary

Strategic advantages exist for organizations and enterprises when their voice, video, and data communications run over a single converged IP network infrastructure. Unfortunately, the ability to capitalize on IP communications systems has been severely delayed because nearly all corporate networks have Firewall and Network Address Translation devices (NATs) that effectively block IP voice and video calls:

1. Firewalls block IP voice and video traffic by placing a barrier to any unsolicited, incoming communications.
2. NATs block IP communications traffic because the IP voice and video devices behind the NAT have private IP addresses that are not routable outside their local domain or on the public Internet.

Several solutions exist for overcoming the NAT and Firewall problem for IP communications including bypassing the firewall and NAT, upgrading the network infrastructure devices using an Application Level Gateway (ALG), and navigating across the Firewall and NAT using a semi-tunneling traversal method.

Bypassing the Firewall and NAT is clearly not an option for most organizations. Removing firewall protection or employing a device such as a proxy or MCU at strategic locations in the network to bridge around the Firewall/NAT may compromise network security. These “device” solutions may also be costly, and they require physical, political, and/or intellectual access to the enterprise-critical network Firewalls and NATs. In addition, one of these bypass devices will be needed at every location along the communications path where a Firewall or NAT presently exists.

Upgrading the Firewall/NAT with an ALG is another possibility, albeit intrusive and potentially expensive. ALGs are essentially vendor specific software upgrades to the firewall devices that examine each data packet attempting to cross the firewall to see if it is of a known protocol type, such as H.323 or SIP. If packets contain the known protocol type, the firewall allows the packets to pass. However, like the proxy or MCU bypass solutions, ALGs require political and intellectual access to the firewall, and every Firewall/NAT in the call path must be upgraded with the ALG software. Furthermore, as new protocols are developed, a new vendor specific firewall ALG software upgrade will be required.

2 Traversing Firewalls and NATs with Voice and Video Over IP

Using existing computer network infrastructure for voice, video, and collaborative data communications promises compelling strategic advantages for organizations of all sizes. Collectively known as rich media communications or Internet Protocol (IP) communications, these *converged networking* technologies offer unprecedented opportunities to communicate, coordinate, and collaborate with customers, suppliers, business partners, colleagues, and associates around the globe.

Unfortunately, the protocols used for communicating rich media over IP networks conflict with most network security mechanisms like Firewalls and Network Address Translation devices (NATs), resulting in slower or delayed deployment of IP voice and video applications.

2.1 How Network Firewalls and NATs Work

On an IP network, every device is assigned a unique IP address. Computers, IP telephones, and videoconferencing devices (often called terminals or endpoints) also have approximately 65,000 network data ports, which are used to establish communication channels for transmitting data between devices on the network.

Messages between network devices consist of data packets containing the following elements:

1. The IP address of the device originating the message and the port number where the message originated from
2. The IP address of the device to receive the message and the port number on that device where the message is to go, and
3. The data to be transmitted.

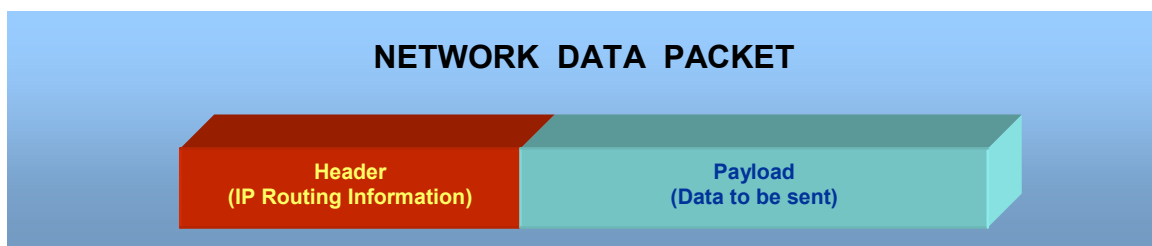


Figure 1. Network data packets contain a header with routing information and the payload containing the data to be sent.

2.2 Firewalls

Organizations that make the Internet available to their workers typically install a firewall to prevent intruders from getting into the organization's private data resources. A firewall is a device located on a private network that protects the resources of the network from outside malicious intent.

Firewalls examine the IP address and destination port of each data packet received from the outside world. Firewalls are often configured so that if a computer on the *inside* of the firewall requests data from a computer on the *outside* of the firewall, the firewall will let the data from the computer outside the firewall pass, but only if it sends the data packets to the same IP address and port number of the computer on the inside of the firewall

that originated the request. If the firewall receives a packet destined for a computer on the inside of the firewall, and it determines that the destination computer did not first initiate a request for data on that port number, the firewall will typically discard the incoming data packet.

Firewalls are almost always configured to block all unsolicited incoming network traffic. One exception is providing a web server inside the firewall for access by the outside world. In this case, the organization will configure the firewall to allow packets destined for port 80 and the web server's IP address to pass through. This enables those outside the organization to send unsolicited packets to the organization's web server requesting some type of data the organization has hosted on that server.

2.3 Network Address Translation (NAT)

Network Address Translation is an Internet standard that enables a Local-Area Network (LAN) to use one set of IP addresses for internal traffic and a second address or set of addresses when connecting to services on an external network, such as the Internet. NAT devices are located where the LAN meets the Internet and are designed to make all the necessary IP packet address translations. NAT serves two main purposes:

- ✓ Many organizations use NAT as a network security device because it hides internal IP addresses – if hackers do not know the IP address of a particular machine, it is much more difficult to break into that machine.
- ✓ NAT enables a company to use more internal IP addresses. Since these addresses are used internally only, there is no possibility of conflict with the IP addresses used by other companies and organizations.

2.4 Firewalls and NATs Obstruct IP Voice and Video Communications

IP-based voice and video protocols, like H.323, require voice or video endpoints to establish data communication channels with each other using IP addresses and data ports.

Herein lies a dilemma: the endpoints must be “listening” for incoming calls in order to establish a data connection, but the firewall is usually configured so that unsolicited data packets are blocked. Even if the network administrator opened up one firewall port to receive call initiation packets, such as “well-known TCP port” 1720, the IP voice and video communications protocols require additional open ports to receive call control messages and to establish the voice and video data channels.

These additional port numbers are determined dynamically, not in advance, which implies that the network administrator would have to open up all the firewall ports to allow voice and video communications, effectively disabling the firewall. Few organizations would allow a wide-open firewall for network security reasons.

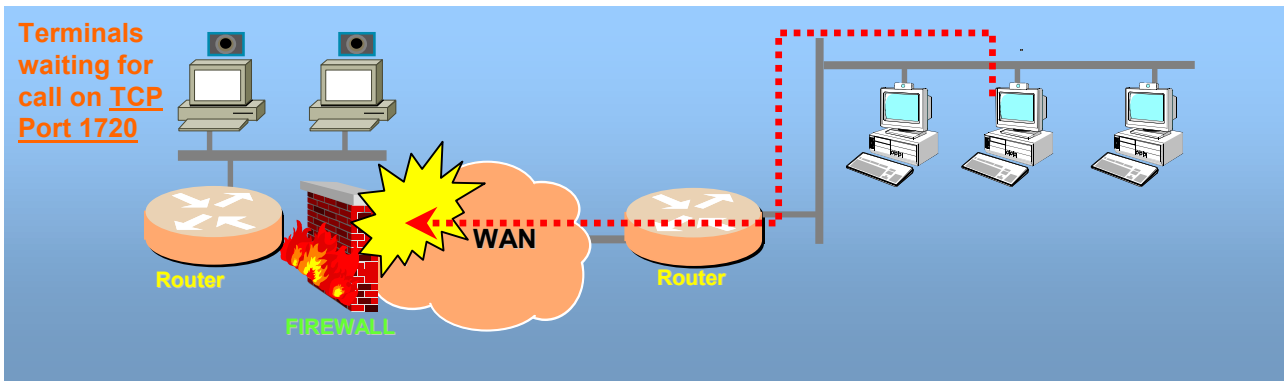


Figure 2. Most firewalls block call setup packets.

NATs also cause challenges for IP voice and video communications. A NAT allows an organization to assign private IP addresses to devices on the local area network (LAN). Unfortunately, routing devices that control the flow of information across the Internet can send data only to devices with routable or public IP addresses.

An endpoint behind a NAT can initiate an IP call with any other endpoint on the same LAN because the IP addresses on the inside of the LAN are internally routable. However, because their IP addresses are private and are not routable beyond the LAN, endpoints behind the NAT cannot receive calls from endpoints outside the LAN.

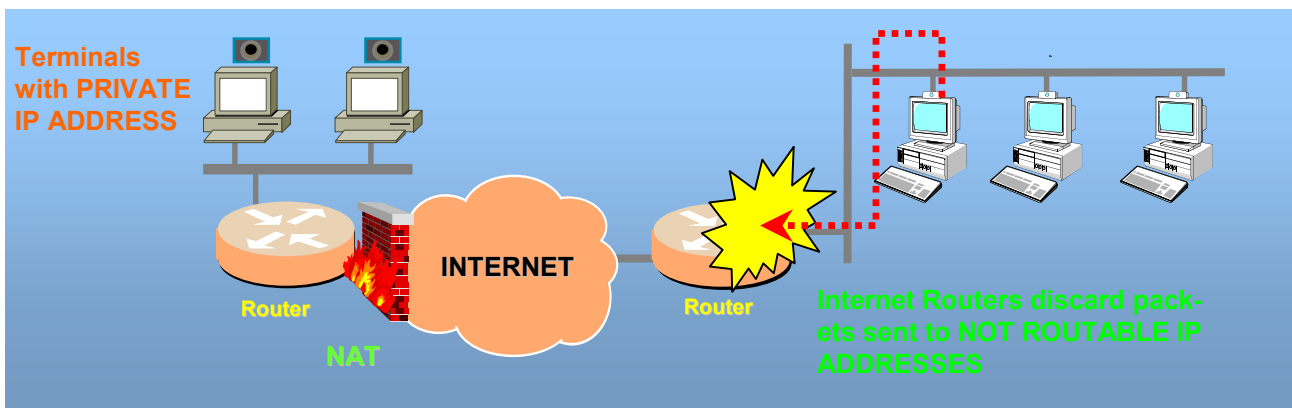


Figure 3. Endpoints behind NAT cannot receive incoming Internet call invitations. In this case the routers on the Internet are not able to route the private IP packets, and they are discarded, causing the call to fail.

Even if the endpoint behind the NAT initiates the call to an endpoint outside the NAT, there is still a problem. When an IP call is initiated, the IP address of the endpoint initiating the call is embedded within the data packet payload. The endpoint being called receives the call initiation packets, opens them, and begins transmitting audio and video data back to the initiating endpoint at its IP address obtained from the packet payload. If this IP address is private, Internet routers will discard audio and video data packets sent from the external endpoint to the internal endpoint because they are being sent to an un-routable IP address. The call will appear to have connected, but the endpoint behind the NAT never receives the external endpoint's audio and video.

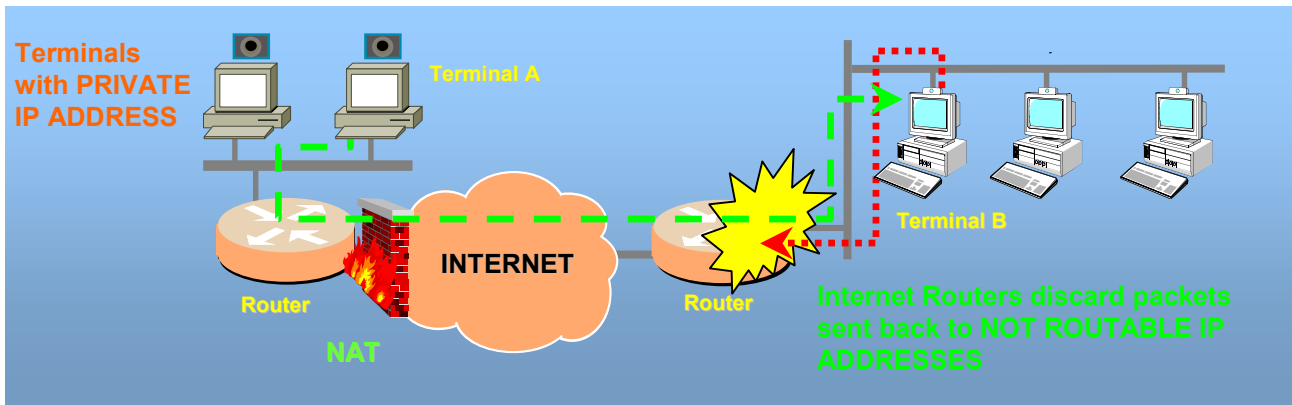


Figure 4. A NAT modifies the message data packet header information. When endpoint A creates a packet intended for endpoint B, the IP addresses of both A and B are placed in the packet header. The IP address of A is also placed in the data packet payload. NAT substitutes its own IP address, C, in the message header. B receives the message and uses the IP address of A from the packet payload as the destination for return packets. However, since A has a non-routable IP address, the return packet from B cannot be routed back to A.

3 Solutions to NAT-Firewall problem

The only devices that does not create the type of problem above reported are NAT/Firewall fully H.323 compatible. In this case the Firewall does not block the well know TCP Port 1720 and also the additional H.323 port numbers, determined dynamically, will be allowed to pass through the firewall.

Moreover, since the private videoconferencing system IP addresses of the are not routable from the external routers, the network administrator can define a Static NAT (a Private IP address assigned statically to an additional Public one and dedicated only to the H.323 conferences) for each terminal that needs to be connected to the “rest of the world”.

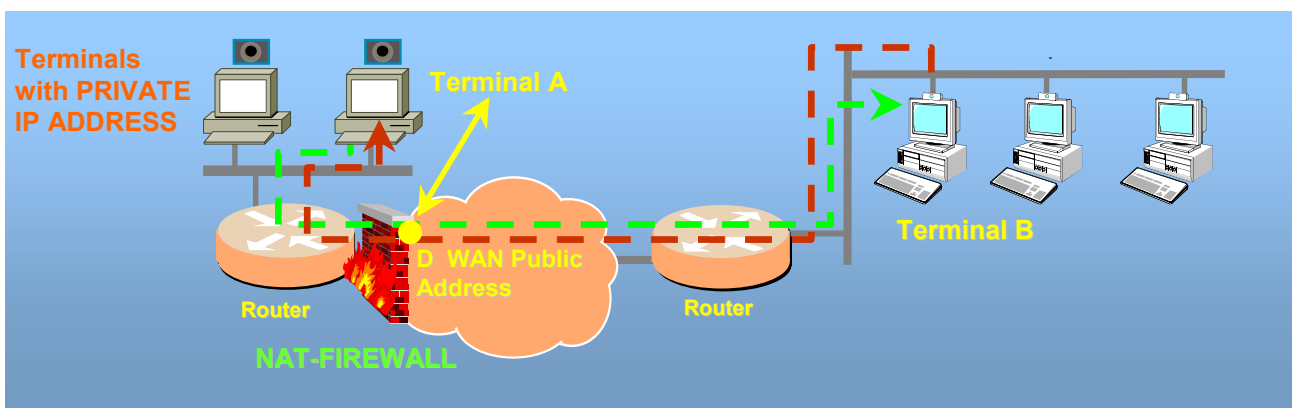


Figure 5. NAT-FIREWALL maps statically its D IP public address to Terminal A leaving C for all other services

In this case the NAT substitutes its additional Static IP address, D, in the message header and payload. B receives the message and uses the IP address of D from the

packet payload as the destination for return packets. The return packet from B will be then routed back to A through the NAT IP address of D.

3.1 Aethra VTC systems vs NAT-Firewall

According to the above scenario, all Aethra videoconferencing systems were successfully tested with:

- ✓ Cisco PIX Firewall (Firewall H.323 compliant - rel 6.1 or higher)
- ✓ Cisco MCM Proxy (NAT H.323 compliant– IOS rel. 12.2 or higher)

In case of NAT device, NOT H.323 compliant, all Aethra New Generation Videoconferencing systems (starting form the Vega2) support the “Aethra NAT” feature. This allows the network administrator to insert, inside the “H.323 Advanced Settings” menu, the Public IP Address statically NATted with the VTC Private IP Address.



Figure 6. Configuration menu of Aethra NAT feature

So it's the Aethra videoconferencing system that automatically “does the job” to replace its Private IP Address inside the IP packets payload. Moreover the network administrator has also the possibility to define a range for the allowed H.323 TCP/UDP ports.

When the Aethra NAT is active, the policy used is to:

- ✓ Check the IP address for each incoming/outcoming call from/to a videoconferencing system.
- ✓ If the IP address is NOT a Public one (according to the RFC 1597: 10.0.0.0 mask 255.0.0.0, 172.16.0.0 mask 255.240.0.0, 192.168.0.0 mask 255.255.0.0), the system does not make any change to its packet payload.
- ✓ For all the other IP addresses (Public), it replaces the IP address inside its packet payload.

Also using a NOT H.323 compliant NAT, Aethra videoconferencing systems were successfully tested with the Cisco IOS NAT (rel. 12.2 or higher).

Of course the “Aethra NAT” feature MUST BE DISABLED in presence of H.323 compliant NAT/Firewall.

3.2 Aethra Application Level Gateway

Application Level Gateways (ALG) are firewalls that are programmed to understand specific IP protocols, like H.323.

Rather than simply looking at packet header information to determine if packets can or cannot pass, ALGs go deeper by parsing the data in the packet payload. H.323 put critical control information in the payload, such as which data ports the voice or video endpoint is expecting to use to receive the voice and video data from the other endpoint in the call. By understanding which ports need opening, the ALG dynamically opens only those ports needed by the application, leaving all others securely closed.

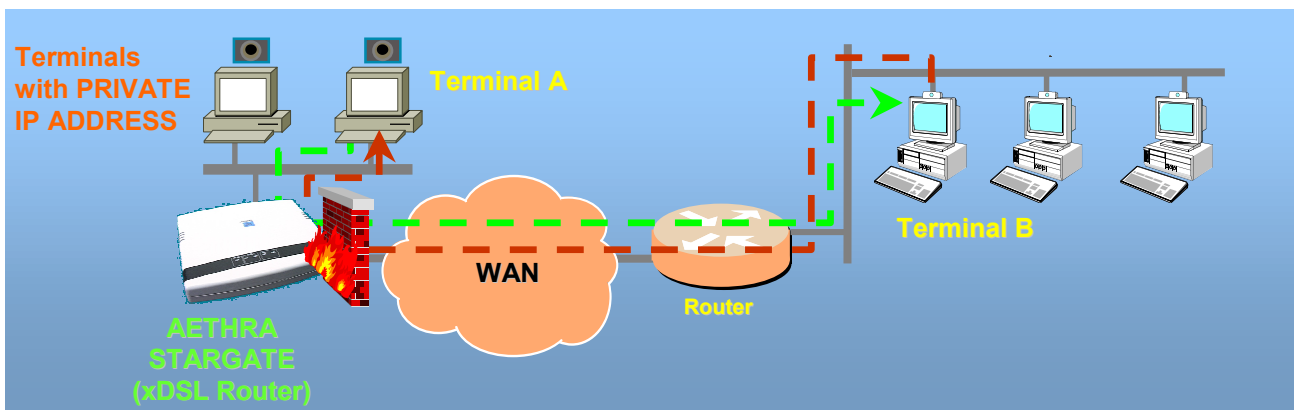


Figure 7. Aethra Stargate Application Level Gateway

The Aethra Application Level Gateway feature is present in the Aethra Stargate xDSL Router and allows to any vendor videoconferencing system to overcome the NAT/Firewall problem. Consequently the Stargate is able to check any incoming/outcoming H.323 calls and dynamically opens only the ports needed for H.323 videoconferencing.

Moreover, since the Aethra Stargate has also NAT capability, it's able to replace automatically the Private IP Addresses (put in the IP packets payload by the H.323) with the Public ones.

Of course, when using the Aethra Application Level Gateway feature in conjunction with any Aethra videoconferencing systems, the "Aethra NAT" feature MUST BE DISABLED since we are in presence of an H.323 compliant device.