White Paper

Traversing Firewalls with Video over IP: Issues and Solutions

VCON
VISUAL COMMUNICATIONS

Table of Contents

Gordon Daugherty
Chief Marketing Officer
August 2003

Introduction

Firewalls serve a vital function in virtually every production data network. They provide a barrier that protects a private network from unauthorized traffic on the public network. Typically, firewalls are a "box" on the network that blocks unwanted traffic between the edge router and the rest of the private network (usually a LAN). The firewall allows access to the local network by opening ports to certain types of packets usually based on IP addresses or protocol types. When traversing a firewall, the H.323 protocol requires the use of certain static ports as well as a number of dynamic ports that are selected at random from a very wide range. Without some other technical solution, it would be required that all ports within this wide range be kept open to bi-directional traffic. This clearly compromises the ability to guarantee the security of an intranet and would render a firewall mostly ineffective.

In this document we will first describe in more detail the technical relationship between the H.323 protocol and firewalls. Then we will describe multiple possible solutions.

Role of a Firewall

A firewall is a set of related programs, located at a network gateway server that protects the resources of a private network from users of other networks. A firewall commonly works closely with the network router to filter various network packets and to determine whether to forward them to their destination. A firewall may also include, or work with, a proxy server that makes network requests on behalf of workstation users. A firewall is generally installed in a specially designated computer, separate from the rest of the network, so that no incoming request can directly access private network resources. The firewall serves as a single point of entry from the public network and a single point of management for the network administrator to apply the desired access and control policies.

There are a number of firewall screening methods. A simple method is to screen requests to make sure they come from acceptable (previously identified) domain names or IP addresses. For mobile users, firewalls can also allow remote access to the private network by means of secure logon procedures and authentication certificates (via VPN services).

Some firewalls also perform network address translation (NAT) or network address port translation (NAPT). As the name suggests, NAT and NAPT results in either the IP address or the port being translated in such a way that it is different on either side of the firewall (public versus private). The firewall itself maintains a table to always keep track of the translations that are being made. In addition to the benefit of reducing the number of routable IP addresses that are needed, NAT also gives the benefit of disguising the real IP address of users and devices on the private network. Also, it is not always the case that the NAT/NAPT function is performed in the firewall device. Sometimes it is performed in a function-specific device. In either case, it creates significant connectivity challenges as we will describe later.

Deployment Issues Relating to IP Video and Firewall Traversal

The H.323 standard uses a well-known port (1720) for signaling via the Q.931 protocol. Q.931 is the call signaling protocol for setup and termination of calls. Additionally, ports used for H.245 call parameter exchange are dynamically negotiated between endpoints at the start of each call. This use of dynamic ports makes it difficult to implement security, policy, and traffic shaping for videoconferencing applications. Worse yet, the audio and video streams associated with a videoconference also use a dynamic range of ports allowed by the industry standard. See the table at the end of this paper for a detailed description of most of the commonly used protocols and their associated ports.

The use of dynamically negotiated ports is one of several deployment issues that relate to firewall traversal. It is unlikely that a network administrator will open thousands of bi-directional ports (inbound or outbound) in the firewall. But it's not just that dynamic ports are used that causes the issue. In some of the streams that are

exchanged, the source address information that is used by the remote device to determine where to return its stream is embedded in the payload of the packet. In the case of NAT, this embedded address becomes invalid because the NAT translates the address in the packet header, and would not forward a packet that is returned to a different address. Also common in the case of NAT is that devices on the private network are assigned non-routable IP addresses (like 10.0.0.15). If the remote device used this IP address for its return streams, it would not be valid anyway.

A similar problem happens when ports are translated via the NAPT function. Since some ports used are well-known ports per the standard, if the NAPT translates to any other port, the remote device could return their stream using a port that is invalid per the standard.

The other challenge with most firewall/NAT configurations is that it is impossible for calls to be initiated from outside the firewall. The reason could be related to ports not being opened for inbound connections or due to the use of non-routable IP addresses on the private network. Yet even if all calls are initiated from inside the firewall, there are a number of inhibitors that might allow the call to connect but not allow inbound audio and video streams. It is a common symptom in which the remote user receives the audio and video streams from the user that is behind the firewall, but not the case for the user behind the firewall.

The next two sections describe various solutions for firewall traversal without threatening network security.

The VCON SecureConnect Solution

The VCON SecureConnect family of products extends the benefits of IP-based communications safely beyond the edges of the managed data network. The SecureConnect family includes components for both secure firewall traversal as well as encrypted communications, both of which can be deployed together for total security. The key components of SecureConnect are as follows:

- **VCON ALG Proxy Server** - This application level gateway (ALG) is a proxy server that is specialized in secure firewall/NAT traversal of H.323 traffic (both signaling streams and media streams). It overcomes the connectivity problems that are presented by firewalls and NAT servers.
- **VCON Advanced Encryption Server** - This server works in conjunction with the ALG and/or the VCON Encryption Client in order to fully encrypt videoconferences or other data transmissions across public or private networks.
- **VCON Encryption Client** - This software application can be installed on PC-based devices such as endpoints, MCUs or other servers in order to encrypt all data transmissions between them, including videoconferences. This client works in conjunction with the VCON Advanced Encryption Server.

Using the ALG Proxy, external devices never connect directly to the private network and internal devices never connect directly to the public network. All types of H.323 devices can benefit from the ALG Proxy's firewall traversal ability, including settop appliances, PC-based devices, MCUs, gateways and more. Scalable from 2 to 100 concurrent calls per server, the ALG Proxy can be placed at each firewall border that needs to be safely traversed. Once installed, the following traffic types can be proxied:

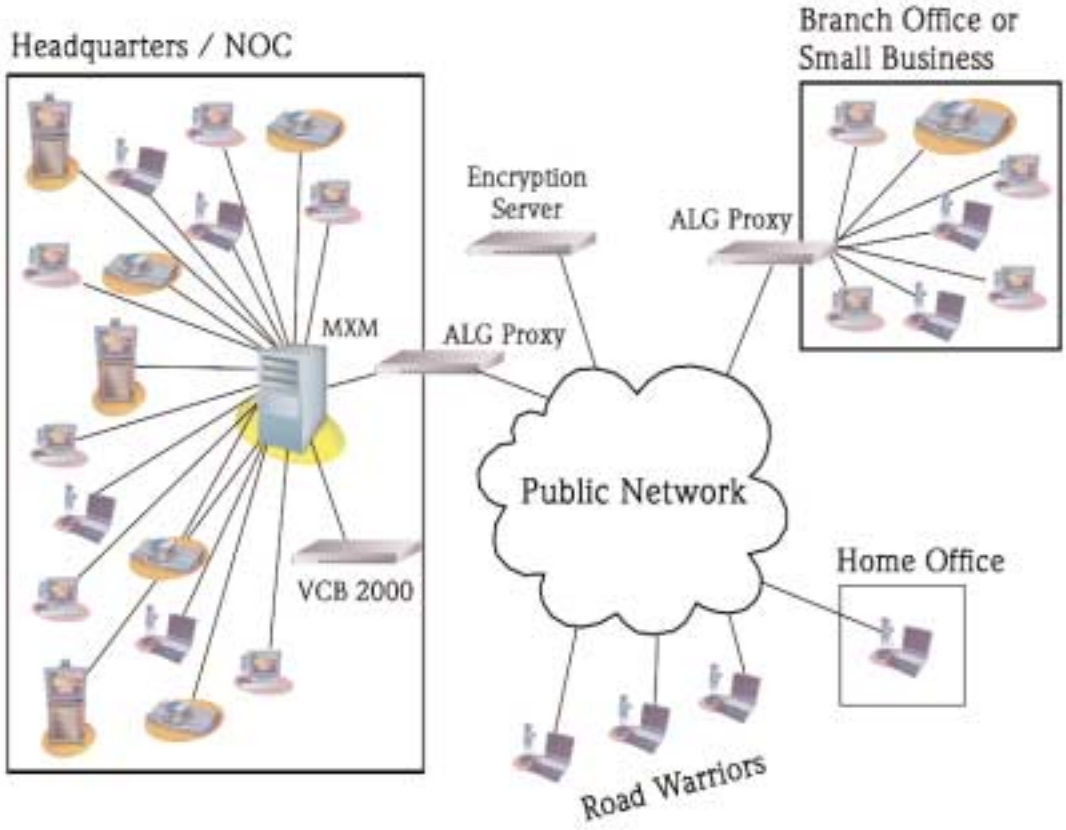
- Gatekeeper registration
- Call setup messages
- RTP-based media streams (audio & video)
- VCON interactive multicast streams
- VCON MXM administrator's console login
- Remote endpoint/device configuration (from MXM)

- Annex Q (far end camera control)
- Neighbor gatekeeper and directory gatekeeper messages (between MXM servers or to non-MXM gatekeepers that are not behind an ALG Proxy)

Even with the ALG Proxy in place, all traffic passes through the firewall. Pinholes are needed in the firewall for 3 specific ports. These pinholes are only opened in the outward direction, and the ports that are used by default can be changed if needed. Additionally, the traffic through the pinholes is directed specifically between the two proxy components of the ALG Proxy, and not the rest of the network.

The firewall does not need to open any new ports in the inward direction and it does not need to accommodate requests to open random or dynamic ports. Furthermore, all traffic that comes into the outside proxy (from the public network) is passed exclusively to the inside proxy through the firewall. Again, one key benefit of the ALG Proxy architecture is that external devices never connect directly to the private network and internal devices never connect directly to the public network. Another key benefit is that, during a conference, the media streams (audio and video) pass directly between the conference participants without having to first pass through some centralized server. This minimizes latency by allowing the packet streams to take the most direct path between devices.

The Advanced Encryption Server can be used for added security of all streams (signaling and media) as they traverse the public network. Scalable up to 10,000 concurrent client logins and 1,000 concurrent calls, the Advanced Encryption Server fully encrypts all streams using the DES, 3DES or AES encryption standards. Users of PC-based videoconferencing devices authenticate with the server using ID/password login. When combined with the ALG Proxy, communication sessions from appliance devices like settops and gateways can also be encrypted. This is due to the fact that the ALG Proxy can serve as a gateway of sorts between the encrypted and non-encrypted segments of the network.



The SecureConnect architecture also provides some key advantages over a traditional VPN solution. VPN solutions typically involve having the remote user authenticate with a VPN server (sometimes co-located in the firewall device), which results in them being logged in to the enterprise or service provider network just as if they were local on the LAN. This can be an effective method of overcoming the connectivity challenges presented by firewalls and NAT servers. However, many times it is not desirable to have remote users fully logged into the enterprise or service provider network just for the need to access application-specific resources (like a videoconferencing gatekeeper, MCU, gateway, or endpoint). With the VCON SecureConnect architecture (both the Advanced Encryption Server and the ALG Proxy), a specific workgroup or community of users that require these application-specific resources can be uniquely authorized without also giving them full access to all of the rest of the network resources. Authentication, signaling streams, and media streams only pass between specifically authorized devices - all fully encrypted where needed.

Other Workaround or Partial Solutions

As already explained above, the H.323 protocol uses a combination of well-known static ports as well as dynamic ports. This might otherwise require all ports in the range 1024 - 65535 (see table below) to be opened. This clearly compromises security and would mostly defeat the purpose of the firewall. However, in addition to the comprehensive VCON SecureConnect solution, a few different workaround or partial solutions might be explored depending on the network topology and level of security required.

- **"H.323 Aware" Firewall** - One option is to utilize a firewall that is "H.323 aware". One method used by such firewalls is called "snooping", in which the H.323 control channel is continuously examined and session requests authenticated. Once authenticated, the requested ports to be used for the H.323 session are opened for the duration of the conference. Upon termination of the conference, the ports are immediately closed by the firewall.

- **VPN** - Most of VCON's endpoints support a VPN connection, which typically results in two IP addresses - one physical and one virtual. By selecting the virtual IP address as the one to be used for the videoconferencing application, the remote user is able to login to a gatekeeper that is behind the firewall/NAT and also initiate calls to other users that are behind the firewall/NAT.

- **Port Range Configuration** - Via the VCON Media Xchange Manager (MXM), the RTP (Real Time Protocol), RTCP (Real Time Control Protocol) and H.245 port ranges used by VCON endpoints and the VCON Conference Bridge (VCB) can be configured. Narrowing the range of ports used by these devices can result in fewer firewall ports needing to being opened or configured for H.323 snooping.

- **Port Pinholing** - VCON endpoints support what is referred to as "port pinholing". The H.323 standard does not require that the outgoing media streams utilize the same port as the associated incoming media stream. However, via VCON's port pinholing feature the outgoing ports will match their associated incoming ports. This is especially helpful in NAPT environments, where the firewall actually translates the ports without the knowledge of the endpoint application. Since the remote VCON endpoint will return it's stream using the same port as the firewall used, the firewall is much more likely to accept the stream and forward it the proper destination.

- **NAT IP Address Mask** - VCON endpoints have a NAT IP Address Mask feature, which allows for the endpoint's public IP address to be manually configured into the endpoint application. This external address will be embedded into the payload of the H.323 signaling packets instead of the non-routable private IP address that otherwise would be used. This solution works well with static IP address mapping in the NAT server, but not well with dynamic IP address mapping. Additionally, since the endpoint behind the NAT is "invisible" to the public address space, calls typically must be initiated from the endpoint inside the NAT.

Summary

The H.323 connectivity problems introduced by firewalls are not unique to VCON. Rather, they apply to all vendors of media streaming products that are built on the H.323 (and even SIP, MGCP, and Megaco) standard. As an innovative leader in the area of video over IP, VCON continues to develop and introduce product enhancements that improve the deployability and manageability of IP video. This certainly includes continued enhancements in the area of firewall and NAT traversal.

Port	Type	Protocol	Description
Common/Required			
1719	Static	UDP	Gatekeeper RAS
1720	Static	TCP	Q.931 (Call Setup)
1024-65535	Dynamic	TCP	H.245 (Call Parameters)
1024-65535	Dynamic	UDP (RTP)	Video Data Streams
1024-65535	Dynamic	UDP (RTP)	Audio Data Streams
1024-65535	Dynamic	UDP (RTCP)	Control Information
Optional			
389	Static	TCP	ILS Registration (LDAP)
1002	Static	TCP	Site Server Registration (Windows 2000 Built-in LDAP)
1503	Static	TCP	T.120 (Data Channel)
1718	Static	UDP	Gatekeeper Discovery (requires multicast address 224.0.1.41)
22136	Static	TCP	VCON MXM - Remote VCON Endpoint Admin
26505	Static	TCP	VCON MXM - Remote Console Login

VCON
VISUAL COMMUNICATIONS

VCON Headquarters
Ph: +972-9-959-0059
Fx: +972-9-956-7244

VCON Americas
Ph: +1-512-583-7700
Fx: +1-512-583-7701

VCON Europe
Ph: +49-89-614-57-0
Fx: +49-89-614-57-399

VCON China
Ph: +86-10-65269791
Fx: +86-10-65269790

VCON France
Ph: +33-155-840-175
Fx: +33-155-840-179

VCON Germany
Ph: +49-89-614-57-0
Fx: +49-89-614-57-399

VCON Italy
Ph: +39-06-545-50-217
Fx: +39-06-592-09-24

VCON Spain
Ph: +34-91-444-0900
Fx: +34-91-444-0907

VCON United Kingdom
Ph: +44-1256-316-586
Fx: +44-1256-316-585

www.vcon.com

DOC 01030 Rev 5 08/03