Quintum Tech. Assistance Center (QTAC)
71 James Way
Eatontown, NJ 07724 USA

QUINTUM The perfect fit.

Toll Free (US Only): 1-877-435-7553
Internationally: 1-732-460-9399
Email: service-ticket@quintum.com

Application Note - Using Tenor behind a Firewall/NAT

Introduction

This document has been created to assist Quintum Technology customers who wish to install equipment behind a firewall and NAT (Network Address Translation) server for their application.

The information and application examples provided here may not match your application exactly, but should provide the necessary information to understand how you might want to configure the Tenor for your application.

Tenor Hardware & Software

This document covers the following Quintum products:

- Tenor AX/AS/AF
- Tenor DX/BX
- Tenor CMS
- Call Relay 60
- Call Relay SP

The Challenge

One of the major issues that has faced companies wishing to deploy H.323-based VoIP telephony networks has been concern about maintaining the security and integrity of the corporate LAN infrastructure. Until now it has been impossible to deploy H.323-based VoIP equipment behind most NAT firewalls without opening up the firewall to the point where the security of the corporate LAN is seriously compromised.

Solutions to this problem have included:

- Deploying the Gateway outside of the firewall on the “Public” section of the LAN.
- Deploying the Gateway behind the firewall in the “De-Militarized Zone” (DMZ).
- Deploying the Gateway behind the firewall on the “Private” section of the LAN but with the firewall partially opened up to enable H.323 traffic to pass through it correctly.

Typical LAN Infrastructure

Corporate LAN infrastructures typically contain three domains, at a minimum, as follows:

- "Public" domain, which is located behind the main router but in front of the firewall

  The public LAN is used to deploy any IP devices that must be easily accessible by any other IP device. These devices must use addresses from the range reserved for public usage. They are fully exposed to the WAN and are not protected in any way.

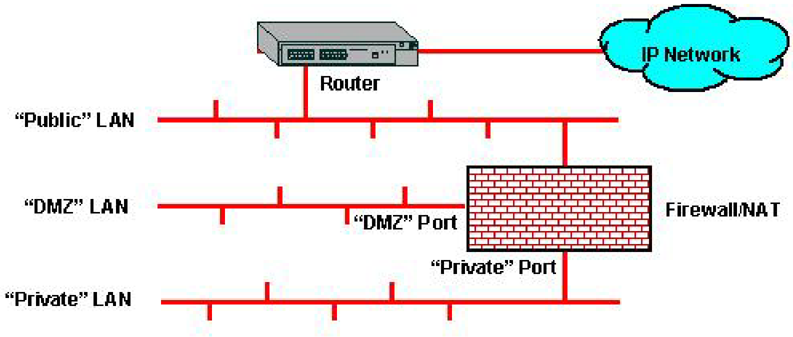
- Demilitarized Zone, or "DMZ," which is connected to the DMZ port of the firewall

  The DMZ LAN is used to deploy IP devices in a more secure area where they have broad public access and are somewhat protected by some of the features of the firewall. Examples would be Web servers, or FTP servers, which need to be exposed to the WAN but can be protected to some extent by the IP address and port screening techniques used for packet filtering in the firewall. In the case of a Web server, for example, the firewall could be configured to restrict all traffic in and out of the DMZ to HTTP and HTTPS (ports 80 and 443) only.

- "Private" domain, which is located completely behind the firewall

  The private LAN is used to support all internal IP devices within the corporation and is very secure, as it is entirely behind the firewall. The firewall can employ techniques such as packet filtering, stateful (dynamic) packet inspection, and Network Address Translation (NAT) to provide a high degree of protection to all the devices on the internal network. Devices on the private LAN use IP addresses assigned for private use.

Figure 1 – Typical Enterprise LAN Infrastructure



NAT Firewalls and the H.323 Protocol

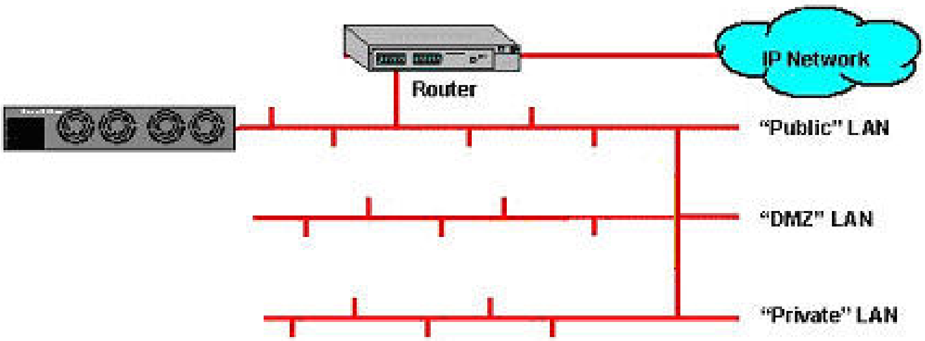
Network address translation is a very powerful technique providing a high degree of security for the private LAN. All the IP addresses for devices on the private LAN are translated into a single public IP address on the public LAN. In this way, the internal infrastructure and its addresses are hidden from public view. This also has the advantage of requiring only one public IP address to support many devices on the private LAN side.

Using NAT does pose problems for some applications. In the case of the H.323 protocol, some of the addressing information is contained in the IP packet header and some in the packet itself. In the course of the NAT process, the firewall unpacks the packet headers and translates all the addresses that it finds into another “alias” address, and keeps a table of these translations. However, it does not translate the addresses contained in the IP packets and, as a result, the H.323 communication session fails. This problem often exhibits itself in such a way that the H.323 session connects correctly but the voice connections only work in one direction.

Deploying H.323 Gateways in the Public Domain

A common way of bypassing the problems caused by NAT firewalls is to place the H.323 Gateway outside of the firewall on the public LAN. In this way, it is fully accessible to other IP Gateways throughout the WAN. However, there are security concerns in the form of unauthorized usage of the Gateway, and exposure to malicious attacks from hackers who may be able to reconfigure or disable the Gateway.

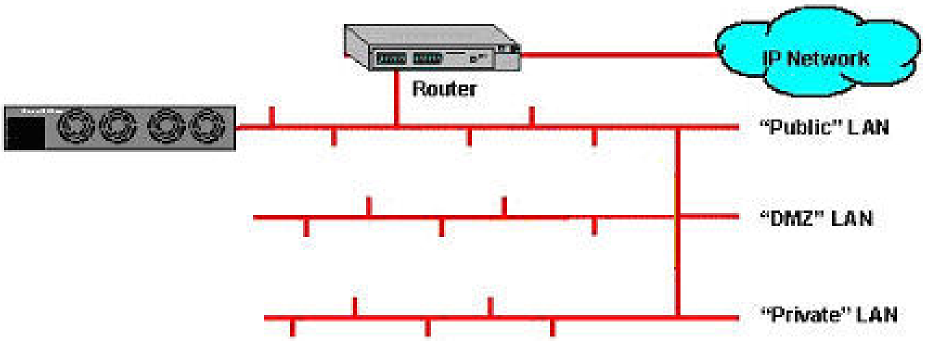
Figure 2 – Deploying a conventional VoIP Gateway on the “Public” LAN



Deploying H.323 Gateways in the DMZ Domain

The next most secure method of deploying an H.323 Gateway in a corporate network is to place it in the DMZ. In this way, it is fully accessible to other IP Gateways throughout the WAN, but is somewhat protected by the packet filtering regime imposed in the firewall. However, this only improves the security to the extent that it limits traffic to specific addresses and ports used by the H.323 application. The same concerns apply as in the public domain, except that any would-be attacker must be familiar with all the ports used in the H.323 protocol.

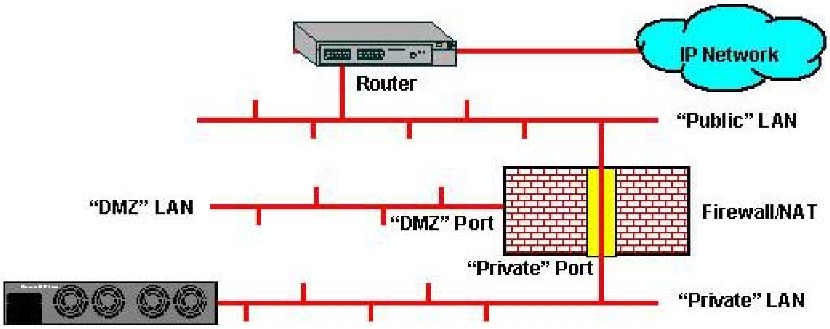
Figure 3 – Deploying a Conventional VoIP Gateway in the "DMZ" of the Firewall



Deploying H.323 Gateways in the Private Domain

The most secure way to deploy the H.323 Gateway is behind the firewall on the private LAN. Theoretically, it can take advantage of all the security measures imposed on the LAN. In practice, it is necessary to open up a significant number of ports to support H.323 applications. Opening up these ports creates a "hole" in the firewall, which somewhat reduces the security provided by the firewall. In addition to this reduction in the efficacy of the firewall, problems will be experienced in the connection of H.323 calls if the firewall uses Network Address Translation as part of its armory of security tools.

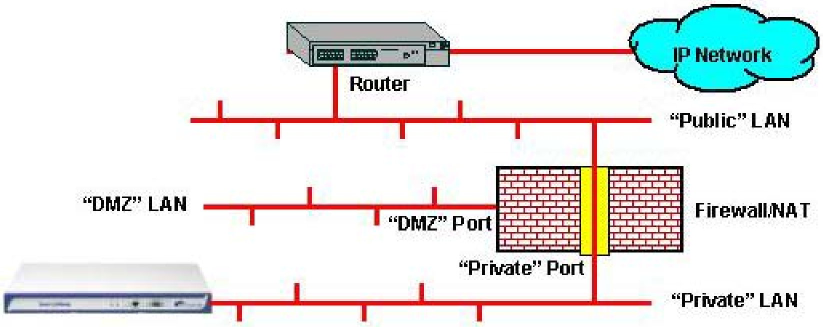
Figure 4 – Deploying a Conventional VoIP Gateway on the "Private" LAN



NATAccess Technology Provides the Solution

Quintum's NAT*Access* technology enables the Tenor MultiPath VoIP Switches to operate correctly behind a NAT-equipped firewall (this feature does not apply to the CMS and Call Relay SP). This means that the Tenor can be successfully deployed on the private LAN behind the NAT firewall. This eliminates one of the major security concerns expressed by network administrators when working with H.323 VoIP, and greatly eases installation in conventional network infrastructures. NAT*Access* is built-in to every Tenor VoIP switch and enables the Tenor to operate directly on the private LAN if it is the only H.323 endpoint on the LAN.

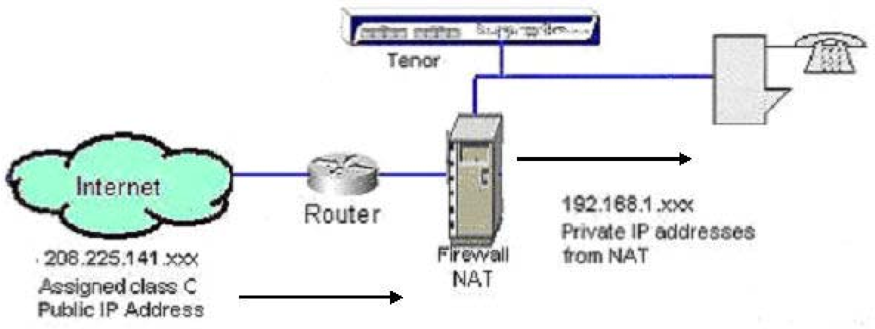
Figure 5 – Deploying the Quintum Tenor with NAT*Access* on the "Private" LAN



Quintum's CallRelay™, a separate standalone unit, may be used in the event that there are multiple H.323 endpoints deployed on the LAN.

Application Example

Figure 6 – Tenor Connected to an Internal LAN



As shown in the figure above, this example shows a Tenor connected to an internal LAN or private network. The Tenor is behind a Firewall/NAT, which provides two main functions.

- The first is to secure the internal network by not allowing unknown outside users to initiate connections to the internal network. This is done by securing the different ports (and sometimes IP addresses) that are used.
- The second function is to avoid using any public IP addresses on the internal network. This allows the customer to purchase a small amount of public IP addresses from the ISP, but have virtually unlimited endpoints on the internal network.

To state it simply, when a user on the internal network initiates a request to the Internet, his/her private IP address is translated to the public IP address when the request goes through the firewall/NAT to the Internet. This is so the destination site knows the IP address to which it should return the information. The firewall/NAT maintains a log of which endpoints requested what destinations, and when a response is received from a destination site, the firewall/NAT directs it to the endpoint that made the original request.

Issues and Solution

When set up as in the previous Application Example, if you only provide the Tenor with a private IP address and the Tenor needs to send and receive calls from the public IP address, the calls do not work. This could be for two reasons: the firewall does not allow the traffic out or in based on the ports requested; or the IP address is sent out incorrectly. Both are explained below.

Firewall Port Access

Because firewalls are used to secure the internal network from attacks from the public network, they typically have many of the port numbers required for VoIP disabled or closed from being accessed. If they are closed, then you will not be able to get a VoIP call up between your internal network and anywhere on the public network. In order to make this work, you will need to re-configure your firewall to open specific inbound port(s) for VoIP. Below is a list of port numbers, protocols, and uses that you will need to consider opening to make this work. Not every port needs to be opened. Check on your needs and only open the ones you require, and ensure that there is no blocking on outbound ports.

Tenor Port – System-level

Name	Type	Port #	Comments	Configuration Manager Configuration
				Command Line Interface Configuration
Ping	ICMP			
FTP	TCP	20, 21	Software upgrade	
Telnet	TCP	23	CLI	
SNTP Client	UDP	123	Time setting	
SNMP	UDP	161	Management	
HTTP	TCP	8080	Configuration Manager	Only configurable in CLI
				config-EthernetInterface-SL1DV1EI1# **set wsp {num}**
Alarms	TCP	9000	Alarm reporting	
Call Events	TCP	9001	Call events reporting	
CDR	TCP	9002, 9003, 9004*, 9005*	CDR Delivery	Systemwide Configuration > CDR Servers > CDR Server-n > CDR Server Port
				config-CDRServer-n# **set cdrserverport {num}**
				config-CDRServer-n# **set cdrserverport {num}**
Tenor Monitor	TCP	9021	NMS protocol used to monitor Tenor events	

*CR-SP and CMS only

Media (needed for both H.323 and SIP)

Name	Type	Port	Comments
PacketSaver	UDP	10064	GW-to-GW communications
RTP/RTCP Media	UDP	10240 - 13120	Voice-related packets GW-to-GW Each VoIP call needs 2 UDP ports (one for RTP and the other for RTCP). **AS/AX/AF/BX/DX**: 10240 – 11200 (960 ports – 480 RTP and 480 RTCP) **CMS**: 10240 – 12160 (1920 ports – 960 RTP and 960 RTCP) **Call Relay SP**: 10240 – 13120 (2880 ports – 1440 RTP and 1440 RTCP)

H.323 Signaling

Name	Type	Port #	Comments	Configuration Manager Configuration
				Command Line Interface Configuration
Discovery (RAS)	UDP	1718	GW-to-GK RAS communications	VoIP Configuration > Gatekeeper/Border Element > General tab > GK Listening Port
				config-GateKeeperParam-1# **set gklp {num}**
Registration (RAS)	UDP	1719	GW register to GK RAS communications	VoIP Configuration > Gatekeeper/Border Element > General tab > Registration Port
				config-GateKeeperParam-1# **set rp {num}**
Call Signaling (Q.931)	TCP	1720	GW-to-GW communications (Q.931-H.225.0 Signal)	

Name	Type	Port #	Comments	Configuration Manager Configuration
				Command Line Interface Configuration
H.245 Signaling	TCP	2000 – 3999	GW-to-GW communications where H.245 tunneling is not used. One port needed for each active VoIP call.	
Service / BE Control	UDP	5001	GK register to BE communications	

BE = Border Element, GK = Gatekeeper, GW = Gateway

SIP Signaling

Name	Type	Port #	Comments	Configuration Manager Configuration
				Command Line Interface Configuration
Session Initiation Protocol	SIP	5060	All SIP signaling. 5060 is the default Listening Port for the first SIP User Agent – be sure to take account of all Listening Ports configured in all SIP Signaling Groups.	VoIP Configuration > SIP Signaling Groups > SIP Signaling Group-n > User Agent tab > Add button > Add User Agent dialog > SIP Listen Port
				config-SIPSignalingGroup-1# **add Ip {ListenPort}**

Once you configure your firewall to allow the correct ports to be opened for communication, the application will work at this level. You still need to check the NAT function.

NAT Translation

As shown in Figure 6 at the beginning of this Application Example, when the Tenor is on a private network and needs to access the public network, the call goes through a NAT, or Network Address Translation Server. The NAT translates the IP address in the IP header, but generally, it is not able to translate the IP address in the H.323 frame. There are a number of things that must be done for this to work correctly.

- First, your NAT must be configured to map a public IP address to the Tenor. For example, the NAT would be configured so that 208.225.141.100 is mapped to 192.168.1.100 (Tenor private IP address), so that any incoming calls to 208.225.141.100 are sent to the Tenor at 192.168.1.100.
- Additionally, if your NAT can perform H.323 translation, this should be turned off. The reason for this is that in the NAT servers we have seen to date that can perform this function, they can only do so for basic VoIP software like NetMeeting and do not perform this function correctly on higher end VoIP Gateways like the Tenor.
- Finally, in the Tenor, you must configure the EthernetInterface External NAT IP as the public IP address. So the Tenor will have two IP addresses at the Ethernet Interface prompt. The IP Address is the private IP address (192.168.1.100) and the External NAT IP is the public IP address (208.225.141.100). When the Tenor needs to send or receive a call to/from the public IP, the Tenor translates the IP address in the H.323 frames and the NAT translates the IP packet address.

If your ISP connection is using DHCP, you may not always know the public IP to assign to the Tenor. Please refer to the document called *Auto External IP* located on our web site in our Customer Service area under the *Cross-Platform Technical Documentation - Networking and Interop* section.