



# **Videoconferencing Systems**



## **SecureConnect Family**

### **Getting Started Guide**

**© 2003 VCON Ltd. All Rights Reserved.**

Information in this document is subject to change without notice. No part of this document can be reproduced or transmitted in any form or by any means - electronic or mechanical - for any purpose without written permission from VCON Ltd.

Media Xchange Manager is a trademark of VCON Ltd.

MeetingPoint is a registered trademark of VCON Inc. in the United States.

Windows is a trademark of Microsoft Corporation.

All other product names are trademarks or registered trademarks of their respective companies or organizations.

### ***Limited Warranty***

VCON Ltd. warrants that SOFTWARE will perform according to accompanying user documentation for a period of 90 (ninety) days from the date of receipt; replacement SOFTWARE will be warranted for 90 (ninety) days from the date of receipt. This Limited Warranty shall not apply to any product that in the opinion of VCON Ltd. has not been installed or upgraded according to accompanying documentation from VCON Ltd. or been subject to misuse, misapplication, negligence or accident while in the hands of the purchaser.

**GRANT OF LICENCE** VCON Ltd. grants the Purchaser a non-exclusive and non-transferable license to use the SOFTWARE product and to make one copy solely for backup or archival purposes, which may include user documentation provided via online or other electronic form. Additional copies may not be made nor may anyone else be allowed to copy or otherwise reproduce any part of the licensed software without prior written consent of VCON Ltd.

**COPYRIGHT** All trademarks(s), logo(s), name(s), software, documentation and other supporting materials relating to the Product are trademarked, copyrighted or owned by VCON Ltd. as proprietary information protected by United States copyright laws and international and applicable national treaty provisions and laws. Software protection extends beyond its literal code to structure, sequence and organization; any unauthorized use or modification would constitute a misappropriation of VCON's proprietary rights and a violation of the License agreement.

**LIABILITIES** VCON's entire liability and the Purchaser's exclusive remedy shall be at VCON's option, either return of the price paid or repair/replacement of the Product not meeting VCON's declared Limited warranty. VCON or its suppliers shall not be liable in any event to anyone for any indirect, incidental, consequential, special or exemplary damages including without limitation damages for loss of business profits, business interruptions, business information or other pecuniary loss arising out of the use of or inability to use the said Product even if advised of the possibility of such damages. In any case, VCON's entire liability under any provision of this agreement shall be limited to the amount actually paid by the Purchase for the Product.

## ***About this Getting Started Guide***

This Getting Started guide introduces you to the VCON SecureConnect system. The following chapter summary briefly describes this guide's contents:

- Chapter 1**            **Negotiating NATs and Firewalls - The SecureConnect Solution**  
Description of the conditions which previously prevented the wide-spread implementation of H.323 videoconferencing in networks protected by NATs and firewalls. Introduction to VCON's SecureConnect system as a recommended solution to this problem.
  
- Chapter 2**            **Reinstalling the ALG Proxy Software**  
VCON supplies pre-installed ALG Proxy systems. Therefore, these instructions are applicable only if you need to reinstall the system at a later time.
  
- Chapter 3**            **Installing the Encryption Client**  
Instructions for installing the Encryption Client.
  
- Chapter 4**            **Operation of Encryption Client**  
Instructions for logging into the Advanced Encryption Server and connecting to a workgroup.
  
- Chapter 5**            **MXM/Gatekeeper Management**  
Examples of basic SecureConnect topologies for networks which receive management services from VCON's Media Xchange Manager™ (MXM) or another gatekeeper. The illustrations provide a guide for configuring ALG Proxies and end points within SecureConnect-protected networks.

## ***VCON Technical Support***

This Administrator's Guide was designed to help you set up and work with your MXM easily so that you can enjoy its many features.

If a situation occurs that is not covered by the supplied documentation, please request help from our Technical Support channels. VCON's organization will make its strongest efforts to help you resume your videoconferencing as soon as possible.

1. Contact your local VCON distributor, and request assistance from its technical support department.
2. Send an e-mail message fully describing the condition plus your system's configuration to [techsup@vcon.co.il](mailto:techsup@vcon.co.il).

# TABLE OF CONTENTS

Limited Warranty.....	ii
About this Getting Started Guide.....	iii
VCON Technical Support.....	iv
<b>1 Negotiating NATs and Firewalls - The SecureConnect Solution....</b>	<b>1</b>
1.1 NATs and Firewalls in Enterprises.....	1
1.2 Effects of Firewalls and NATs on H.323 Videoconferencing.....	2
1.3 The SecureConnect System Solution.....	4
1.4 Working with SecureConnect Encryption.....	6
<b>2 Reinstalling the ALG Proxy Software .....</b>	<b>7</b>
2.1 Encrypted Network Managed by an Advanced Encryption Server.....	8
2.2 Two NICs in One ALG Proxy Server.....	9
2.3 Two ALG Proxy Servers - One NIC in Each .....	10
<b>3 Installing the Encryption Client.....</b>	<b>13</b>
3.1 Minimum System Requirements .....	13
3.2 Running the Installation Program .....	14
<b>4 Operation of Encryption Client.....</b>	<b>17</b>
<b>5 MXM/Gatekeeper Management.....</b>	<b>19</b>
5.1 Registering Nodes Inside NATs to the MXM .....	19
5.2 Negotiating Firewalls.....	23
5.3 ALG Proxy Employment in Multiple NATs .....	27



# 1 **NEGOTIATING NATs AND FIREWALLS - THE SECURECONNECT SOLUTION**

VCON's SecureConnect family provides a solution for allowing organizations to conduct H.323 audio and video communication, while continuing to protect their local area networks (LANs) with NATs and firewalls.

## 1.1 **NATs and Firewalls in Enterprises**

To protect the nodes within their networks, many organizations employ firewalls and NAT (Network Address Translation) devices. Together or separately, these devices present challenges for implementing IP videoconferencing solutions.

### **Network Address Translation Devices (NATs)**

NAT is a protocol in which a LAN uses one set of IP addresses for internal communication (within an organization's LAN) and a different address for communication with external network, such as the Internet. It provides a solution for two main conditions:

- ❑ **Network security** - Internal IP addresses are hidden from external users. This helps protect the network's computers from hackers and spammers.
- ❑ **Finite number of available IP addresses** - The number of public IP addresses is limited. By defining addresses for internal use only, an organization can use a large number of different addresses without conflicting with addresses used elsewhere.

Within a NAT, the nodes have internal addresses which are inherently unreachable to nodes from outside. Without a traversing device, internal nodes cannot receive calls or communication from external nodes. Even if a node within the NAT initiates communication, it cannot receive a reply - the reply is being sent to a non-routable IP address.

A NAT device maps public IP addresses to private IP addresses and ports. It also assigns ports to nodes within its network, but the private IP addresses remain unknown to outside users. To enable external communication, the NAT device opens a channel to the public network. The NAT appends the public IP address to all data packets sent outside the network. Likewise, for incoming data, the NAT device replaces its public address with the mapped internal address.

Usually, NAT assignments last for a short period of time and are then released. It's important that a NAT assignment remain valid for the duration of an open connection. To accomplish this, any node communicating through a NAT device must send a "keep-alive" packet periodically to prevent remapping during an open session.

### **Firewalls**

To protect their networks and data resources from external hazards such as hacking and virus propagation, some organizations install firewalls.

Firewalls check the IP address and destination port of each data packet received from external sources. The type of permitted incoming traffic depends on the firewall's configuration. For example, the firewall may allow traffic from an external source to pass if a node inside the firewall initiated communication with it. Usually, they will block or discard unsolicited packets.

In order to deal with desirable requests for information while protecting most of their user nodes, many organizations place relevant information on a web server inside the firewall. The firewall is then configured to permit traffic to and from the web server's IP address and port 80 to pass.

### **1.2 Effects of Firewalls and NATs on H.323 Videoconferencing**

Compared to other data communications protocols such as HTTP and FTP, H.323 has unique characteristics that cause difficulties in enterprise environments protected by firewalls and NATs.

1. H.323 transmissions include the embedding of the sender's IP address inside the data packets. The call recipient transmits audio and video in return to the initiating user at the IP address embedded in the original transmissions. If this IP address is private, Internet routers typically discard the audio and video packets sent from the external endpoint because they are being sent to an un-routable private IP address.
2. During H.323 communications, several protocol parameters, including IP port values, are determined dynamically during call setup negotiation instead of in advance. This poses a problem in security devices such as firewalls, which usually require a security schema based on opening specific known ports.



3. The use of H.323 video and voice communication requires a firewall to open a wide range of ports so that traffic can pass unhindered. The IP voice and video communications protocols require several 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. Therefore, network administrators would have to open up all the firewall ports to allow the H.323 traffic to pass through. This constitutes a breach of the firewall's purpose, which prefers to close as many ports as possible.

In most organizations, firewalls are configured to severely limit the types of inbound data traffic that will arrive to internal users' workstations, servers, and peripheral equipment.

Firewalls support many different protocols, but they do not specialize in H.323 communications. This may cause variations in the level of support for H.323 among different vendors' firewalls. This results in occasional call failures.

NATs also impose obstacles for IP voice and video communications. NATs assign private IP addresses to workstations and servers located within a private LAN. However, most routing devices that control the flow of information across the Internet can send data only to devices with routable or public IP addresses. The addresses of users in NAT-protected networks are unknown to devices on the public side of the NAT. As a result, the users behind the NAT cannot receive calls from the public side of the LAN.

NATs also hinder H.323 calls which are dialed out by private LAN users to the public side. As previously mentioned, the IP address of the sender is embedded in the video and audio transmissions. If this IP address is unroutable, any return transmission will not penetrate the network protected by the NAT. The user behind the NAT never receives the public side user's audio and video.

### 1.3 The SecureConnect System Solution

VCON's SecureConnect family of products provides connectivity for videoconferencing networks within organizations that are protected by NAT and firewalls.

SecureConnect components are:

- ALG Proxy Server
- Advanced Encryption Client
- Encryption Client

#### ALG Proxy Server



Throughout this guide, the name, "ALG Proxy," refers to the ALG Proxy Server.

The VCON ALG (Application Level Gateway) Proxy translates H.323 messages between the private LAN or NAT and the public WAN. It also routes management channels across network boundaries. It translates private IP addresses to public ones and conversely, from public to private addresses. The ALG Proxy also relays every packet towards the correct destination according to its mapping configuration. Network interface cards (NIC) connect the private LAN and public networks.

#### Permitted Network Traffic

The ALG Proxy allows passage by the following types of network traffic:

- Gatekeeper registration
- Call setup messages
- RTP-based audio and video streams
- Interactive multicast streams
- MXM Administrator login
- Remote end point/device configuration (from MXM Administrator)
- Annex Q far end camera control (FECC)
- Neighboring gatekeeper and directory gatekeeper messages (between MXMs or to non-MXM gatekeepers that are not behind an ALG Proxy).

### **Hardware Configurations**

ALG Proxies may be set up in one of the following hardware configurations:

- 1 ALG Proxy with 2 NICs - 1 NIC may be configured for encryption.
- 2 ALG Proxies with 1 NIC connected to each other. For example, one server is located within the private LAN and the other one is in the public network.

Each proxy configuration may handle up to 100 concurrent video calls.

### **ALG Proxy Support in a Firewall**

If a firewall is installed in the organization, the ALG Proxy requires that you open pinholes through four specific ports, outward to the public network. You do not have to open any ports inward, and the firewall does not have to accommodate requests to open random or dynamic ports. Traffic through the pinholes is directed through SecureConnect components only.

As a result, external addresses never connect directly to the private network and devices in the private network never connect directly to the public network.

### **ALG Proxy Support in Non-MXM Gatekeeper**

The ALG Proxy is compatible with non-MXM gatekeepers that support the transfer of non-standard data elements in H.323 messages. The following features are not available for non-MXM gatekeepers located behind an ALG Proxy:

- Neighboring Gatekeeper
- Accord Meeting Room
- Receiving true IP address of registering entity; instead, the gatekeeper receives the ALG's IP address.

### **QoS Support**

VCON's PacketAssist Architecture, which delivers Quality of Service (QoS) to IP videoconferencing, is integrated into the ALG Proxy. The QoS helps provide the best possible audio and video quality, at a given data rate, for all H.323 end points located behind the ALG Proxy. The ALG Proxy's QoS settings override the local QoS settings of any of the end points behind it.

The QoS settings are accessible either directly through the ALG Proxy's configuration utility or through the MXM Administrator (for those systems installed in MXM-managed networks).

### 1.4 Working with SecureConnect Encryption

SecureConnect provides encryption for videoconferences and other data transmissions, through the employment of an Advanced Encryption Server and Encryption Clients in your organization's end points and other networking devices located behind the ALG Proxy.

- ❑ The **Advanced Encryption Server** authenticates the various clients and assigns public encryption keys to them. The AES encrypts videoconferences and other data transmissions across public or private networks.
- ❑ The **Encryption Client** is an application which may be installed on PC-based devices such as end points, MCUs and other servers within your organization. The Encryption Client operates as a virtual network card, and encrypts all data transmissions from devices in which this client application is installed. The Encryption Client applies the encryption to signaling and media streams immediately as they leave the Client's host.

The Advanced Encryption Server allows users to videoconference with other end points directly or through MCUs and gateways without having to grant them full access to other network resources. Authentication, signaling streams, and media streams pass only between specifically authorized entities, with full encryption if it's invoked. Conversely, if one of the users in a conference does not have the Encryption Client running, the conference is not encrypted.

Depending on the license that your organization purchases, the Advanced Encryption Server provides encryption for up to 1000 concurrent calls, which may arrive from a PC-based end point/network device or an ALG Proxy. Since ALG proxies may have up to several hundred devices located behind them, the maximum number of devices with access to encryption at the same time is 10,000.

The Advanced Encryption Server supports the DES, 3DES, and AES encryption standards. The method of encryption is chosen and controlled through the Advanced Encryption Server.

Individual users can run the Encryption Client from their desktops by logging in with their sign-in name and a password. If the videoconferencing application is VCON's vPoint or MeetingPoint 4.6, the user must then choose which IP address to use while videoconferencing (the computer's network address or a virtual address (172.x.x.x) assigned by the Advanced Encryption Server).

If a VCON Conference Bridge (VCB) is installed in the network, an Encryption Client installed on its host provides encrypted multipoint videoconferencing for end points also running the Encryption Client.

## **2 REINSTALLING THE ALG PROXY SOFTWARE**

If your organization purchased a SecureConnect solution, it received an installed, configured system of SecureConnect products. However, if you need to reinstall the ALG Proxy, run the SecureConnect installation program according to your network's configuration. The available configurations are:

- Encrypted network managed by an Advanced Encryption Server
- Two NICs in one ALG (Application Level Gateway) Proxy Server
- Two ALG Proxies with one NIC in each.

### 2.1 ***Encrypted Network Managed by an Advanced Encryption Server***

To implement a more secure communication environment, use the VCON Advanced Encryption Server.

➤ **To reinstall the SecureConnect software**

1. Insert the SecureConnect Setup CD-ROM in your computer's CD-ROM drive.
2. If Autorun is enabled, the Installation program appears automatically.  
Otherwise, click **Start** in the Windows taskbar and then click **Run**. Browse to the CD-ROM drive and double-click the *Setup.exe* file.
3. Follow the instructions in the Setup Wizard, clicking **Next** to continue. The installation program installs the Server components.
4. In the Wizard's SecureConnect Server Parameters page, select **Using the ServiceConnect Encryption Server** and click **Next**.
5. Select a network adapter for communicating with H.323 end points on the LAN. The adapter must be located on the LAN side. Click **Next**.
6. Enter the IP address of the associated gatekeeper management and click **Next**.

If the MXM/Gatekeeper is in the same network as this ALG Proxy, enter the MXM/Gatekeeper's IP address.

If the MXM/Gatekeeper is in a different network from this ALG Proxy, enter the IP address of a SecureConnect Proxy which is located in the same network as the MXM/Gatekeeper.

7. When the Wizard informs that the installation is complete, click **Finish**.
8. Restart the computer. In the Administrator Main View, the SecureConnect Server appears under the System Servers object.

## 2.2 Two NICs in One ALG Proxy Server

### ► To reinstall the SecureConnect Server software

1. Insert the SecureConnect Setup CD-ROM in your computer's CD-ROM drive.
2. If Autorun is enabled, the Installation program appears automatically.  
Otherwise, click **Start** in the Windows taskbar and then click **Run**. Browse to the CD-ROM drive and double-click the *Setup.exe* file.
3. Follow the instructions in the Setup Wizard, clicking **Next** to continue. The installation program installs the Server components.
4. In the Wizard's SecureConnect Proxy Parameters page, select **Not Using the ServiceConnect Encryption Server** and click **Next**.
5. Select **Running the Proxy on a Computer with 2 NICs** and click **Next**.



Make sure that one of the NICs has an IP address inside a private LAN and the other NIC has an IP address from the public WAN.

6. Select a network adapter for communicating with H.323 end points on the LAN. The adapter must be located on the LAN side. Click **Next**.
7. Select a network adapter for communicating with H.323 end points in the public network. The adapter must be located on the WAN side. Click **Next**.
8. Select the side that the MXM/Gatekeeper is located, private **LAN** or public **WAN**, and click **Next**.
9. Enter the IP address of the proxy's source of gatekeeper management and click **Next**.  
  
If the MXM/Gatekeeper is in the same network as the proxy, enter the MXM/Gatekeeper's IP address.  
  
If the MXM/Gatekeeper is in a different network from this proxy, enter the public IP address of a SecureConnect Proxy which is located in the same network as the MXM/Gatekeeper.
10. When the Wizard informs that the installation is complete, click **Finish**.
11. Restart the computer. In the Administrator Main View, the SecureConnect proxies appear under the System Servers object.

### 2.3 Two ALG Proxy Servers - One NIC in Each

#### ► To reinstall the SecureConnect Server software

1. Insert the SecureConnect Setup CD-ROM in your computer's CD-ROM drive.
2. If Autorun is enabled, the Installation program appears automatically.  
Otherwise, click **Start** in the Windows taskbar and then click **Run**. Browse to the CD-ROM drive and double-click the *Setup.exe* file.
3. Follow the instructions in the Setup Wizard, clicking **Next** to continue. The installation program installs the Server components.
4. In the Wizard's SecureConnect Proxy Parameters page, select **Not Using the ServiceConnect Encryption Server** and click **Next**.
5. Select **The Proxy will use only 1 NIC** and click **Next**.
6. Select the side that this proxy is located, private **LAN** or public **WAN**, and click **Next**.
7. Select a network adapter for communicating with H.323 end points. Click **Next**.
8. Select the side that the MXM/Gatekeeper is located, private **LAN** or public **WAN**, and click **Next**.
9. Enter the IP address of the ALG Proxy's source of gatekeeper management and click **Next**.

If the MXM/Gatekeeper is in the same LAN as the ALG *OR* in the public WAN, enter the MXM/Gatekeeper's IP address.

If the MXM/Gatekeeper is in a different LAN from this ALG, enter the IP address of a public-side ALG which is associated with the same network as the MXM/Gatekeeper.

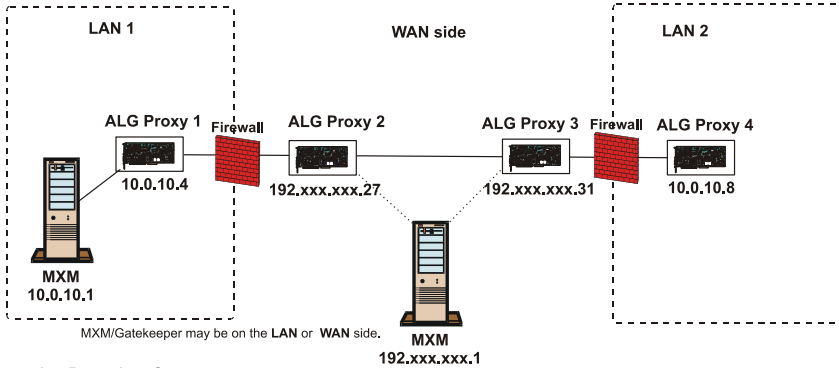
For a guide about which IP address to enter, see the illustration and table on the next page.

10. Enter the IP address of the second ALG's computer (in this configuration, the two NICs are on two different computers) and click **Next**.
11. When the Wizard informs that the installation is complete, click **Finish**.
12. Restart the computer. In the Administrator Main View, the ALG Proxy appears under the ALG Proxy Server object.



Repeat this procedure to install the software for the other ALG Proxies.

The sample application in the following illustration and table provide a guide for determining which IP address to define as the source of gatekeeper management.



**Installation Procedure Steps**  
(See previous page) →

- 8 Select the side that the MXM/Gatekeeper is located, private LAN or public WAN, and click **Next**.
- 9 Enter the IP address of the ALG Proxy Server's source of gatekeeper management and click **Next**.  
  
If the MXM/Gatekeeper is in the same LAN as the ALG OR in the public WAN, enter the MXM/Gatekeeper's IP address.  
  
If the MXM/Gatekeeper is in a different LAN from this ALG, enter the IP address of a public-side ALG which is associated with the same network as the MXM/Gatekeeper. For a guide about which IP address to enter, see the table on page .
- 10 Enter the IP address of the second ALG's computer (in this configuration, the two NICs are on two different computers) and click **Next**.

While installing this ALG Proxy	If the MXM is located here	Enter this IP address as the Gatekeeper Management Address
<b>ALG Proxy 1</b>	LAN 1	MXM
<b>ALG Proxy 1</b>	WAN	MXM
<b>ALG Proxy 2</b>	LAN 1	MXM
<b>ALG Proxy 2</b>	WAN	MXM
<b>ALG Proxy 3</b>	LAN 1	ALG Proxy 2
<b>ALG Proxy 3</b>	WAN	MXM
<b>ALG Proxy 4</b>	LAN 1	ALG Proxy 2
<b>ALG Proxy 4</b>	WAN	MXM



## 3 *INSTALLING THE ENCRYPTION CLIENT*

### 3.1 *Minimum System Requirements*

The VCON Encryption Client application may be installed on any workstation(s) that meet the following minimum specifications:

<b>Operating System</b>	Microsoft Windows 98/XP/2000/NT 4.0 with Service Pack 4 or higher.
<b>Minimum CPU Speed</b>	200 MHz
<b>Minimum Memory</b>	64 MB
<b>Minimum Free Disk Space</b>	7 MB
<b>Web Browser</b>	Internet Explorer 5 (for Windows 98FE) Internet Explorer 4.01 with Service Pack 1 (for Windows 98SE, 98ME, NT4, 2000, XP).

### 3.2 *Running the Installation Program*

You can install the Encryption Client through one of the following methods:

- Through the Advanced Encryption Server
- Through the VCON website.

➤ **To install the Encryption Client**

<b>Through the Advanced Encryption Server</b>	<b>Through the VCON Website</b>
<ol style="list-style-type: none"><li>1. Enter the URL for your organization's Advanced Encryption Server. Ask your system administrator for this address (see the illustration on the next page).</li><li>2. Click <b>Login to Server</b>.</li><li>3. Enter your Sign-in Name and Password.</li><li>4. Click <b>Login</b>.</li><li>5. Click <b>Download</b>.</li><li>6. From the Client section, download the <b>Encryption Client</b> application.</li><li>7. When the installation program finishes, restart your computer.</li></ol>	<ol style="list-style-type: none"><li>1. Go to the VCON website (<a href="http://www.vcon.com">http://www.vcon.com</a>).</li><li>2. Click the Support and the Download links.</li><li>3. Locate and click the Secure Connect <b>Encryption Client</b> link.</li><li>4. Enter your User Name and password for VCON downloads and click <b>Download</b>.</li><li>5. When the installation program finishes, restart your computer.</li></ol>

Naji mxm08 Online	Privileged User <b>VCON</b>	Privileged User 213.8.49.35	workgroup mounted none
----------------------	--------------------------------	--------------------------------	---------------------------

**VCON**  
VISUAL COMMUNICATIONS

Powered by Netmount

NETMOUNT WEB CLIENT

[HOME](#) [MY PROFILE](#) [DOWNLOAD](#) [HELP](#) [LOGOUT](#)

### User Home Page

System message: Welcome to Netmount User Page



You are a member of **5 workgroups**.

Native client on your computer is logged in.  
Login time: **July 28, 2003 9:13:08 AM GMT+02:00**.





**NEW WORKGROUP**

**ACTIVE WORKGROUP**

**YOUR WORKGROUPS**

-  [BasicSec-Group](#)
-  [LowSec-Group](#)
-  [MedjumSec-Group](#)
-  [AdvanceSec-Group](#)
-  [AllUsers](#)

**LEGEND**

-  Admin
-  Community Admin
-  Member
-  Connected
-  Invited

Invitations: 0.  
[Messages: 0.](#)

**TIP OF THE DAY**

You choose which workgroup to join.

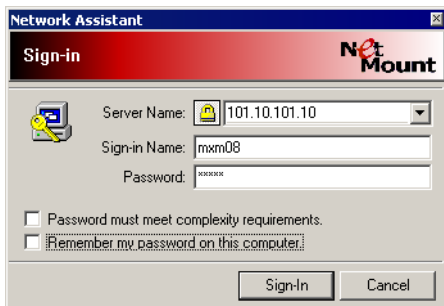
*Advanced Encryption Server's Download Page*



## 4 OPERATION OF ENCRYPTION CLIENT

### ► To run the Encryption Client

1. In the Windows desktop, double-click the Network Assistant icon.
2. Click the **Click Here to Sign In** link.

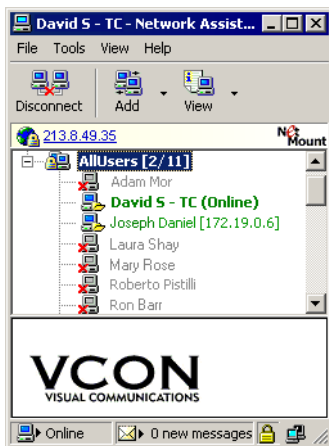


3. Enter the IP address or DNS name of the Advanced Encryption Server, the sign-in name and the password.

Ask your system administrator for this information.

4. Click **Sign-in**.

By default, you are placed into the AllUsers workgroup.



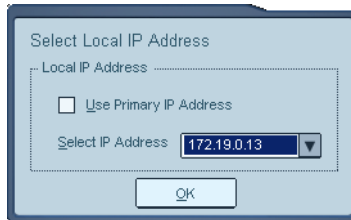
## 4 Operation of Encryption Client

5. If no one else is connected to this workgroup, wait for another Workgroup member to connect. Your client will then receive a Virtual IP address (172.x.x.x).

If other members of the workgroup is logged on, a notification appears on your screen.



6. If you want to connect to another workgroup, select the workgroup in the Network Assistant window and then click **Connect**.
7. Run your vPoint or MeetingPoint application. During the startup, a the Select IP Address dialog box opens.



8. From the list, choose the virtual IP address (172.x.x.x).



To receive calls from remote users who are not logged into the same MXM as your system, they must dial your virtual IP address.



## 5 ***MXM/GATEKEEPER MANAGEMENT***

This chapter provides examples of basic topologies for networks which receive management services from VCON's Media Xchange Manager™ (MXM) or another gatekeeper. Each sample illustration provides examples of typical locations for ALG Proxies and end points within these topologies and the IP addresses required to receive MXM/gatekeeper management.



For reasons of clarity, the sample topologies presented in this chapter show either single ALG Proxy server (with two NICs) OR dual server (with one NIC in each) configurations set up in a given network. However, both single-server and dual-server configurations are functionally equivalent for all of the topologies described herein.

### ***5.1 Registering Nodes Inside NATs to the MXM***

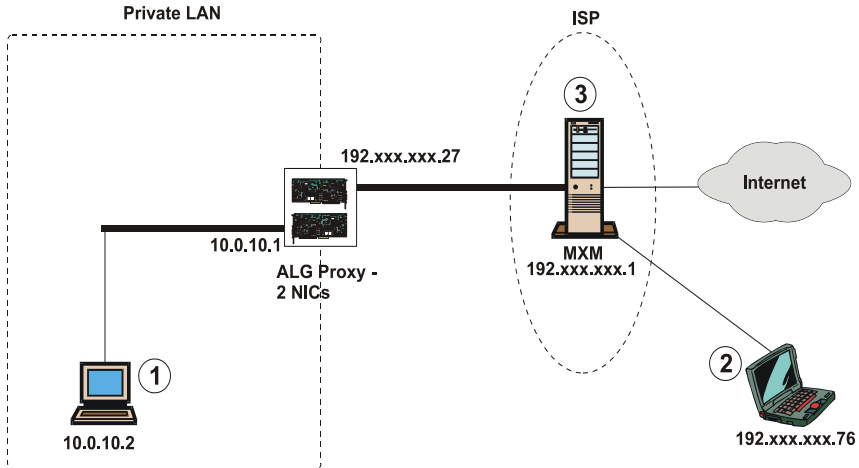
This section suggests several basic NAT network scenarios and guidelines for registering the affected nodes with the MXM:

- MXM Outside of NAT***
- MXM Inside NAT***
- Two NATs - MXM Inside One of the NATs***

## MXM Outside of NAT

In this configuration, an ALG Proxy with two NICs provides a channel between the nodes inside the NAT and external networks. The MXM is located outside the NAT. To register with the MXM, the local nodes send login requests to the ALG Proxy, which relays them to the MXM.

Registration of nodes to the MXM requires the configuration settings described in the following illustration.



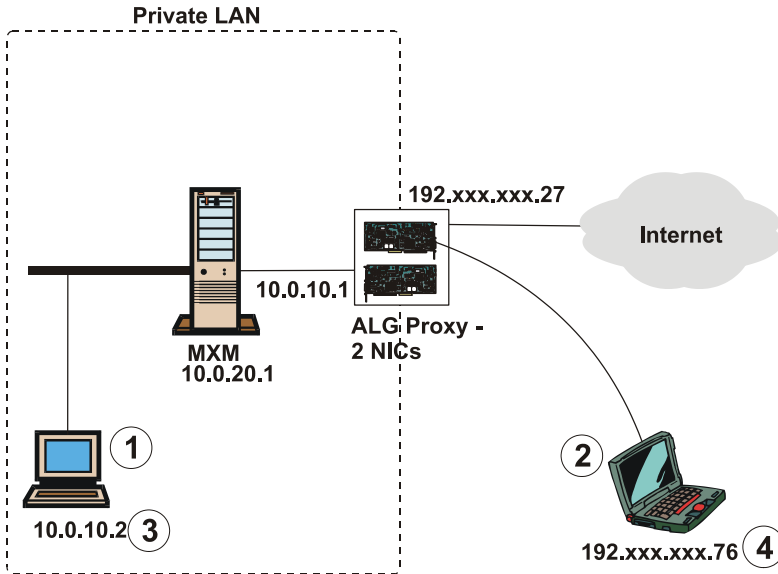
- 1 Private LAN's nodes enter the private address of the ALG Proxy (**10.0.10.1**) as its MXM/Gatekeeper.
- 2 Public network nodes enter the MXM's address (**192.xxx.xxx.1**) as the MXM/Gatekeeper.
- 3 In the MXM Main Viewer, all of the private LAN's nodes display their own IP addresses.

*MXM Outside of NAT*

## MXM Inside NAT

In this configuration, the MXM routes all signalling packets through the ALG Proxy. Data passes through the ALG Proxy only during calls between public and private network devices (not for public-public or private-private calls).

Registration of nodes to the MXM requires the configuration settings described in the following illustration.



- 1 Private LAN's nodes enter the MXM's address (**10.0.20.1**) as the MXM/Gatekeeper.
- 2 Public network nodes enter the public address of the ALG Proxy (**192.xxx.xxx.27**) as the MXM/Gatekeeper.
- 3 In the MXM Main Viewer, all of the private LAN's nodes display their private IP addresses (**10.0.x.x**) as their own address.
- 4 In the MXM Main Viewer, all of the public nodes display their own IP addresses.

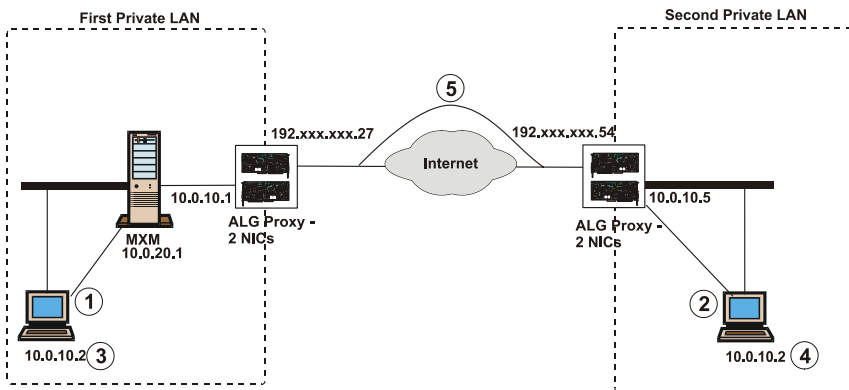
*MXM Inside NAT*

## Two NATs - MXM Inside One of the NATs

In this configuration, nodes from one private LAN call to nodes on a second private LAN through the second LAN's ALG Proxy's public IP address. The MXM resides in one of the LANs and nodes in that LAN register directly.

However, individual nodes inside the second LAN cannot register with the MXM directly - the nodes send registration requests to the second LAN's ALG Proxy's private IP address. This server then relays the request to the first LAN's ALG Proxy, which forwards the request to the MXM. For the MXM, all communication to and from the second LAN and the public network goes through the first LAN's ALG Proxy.

Registration of nodes to the MXM requires the configuration settings described in the following illustration.



- 1 First private LAN's nodes register to MXM directly, entering **10.0.20.1** as the MXM/Gatekeeper.
- 2 Second private LAN's nodes enter the private address of that LAN's AGL Proxy (**10.0.10.5**) as the MXM/Gatekeeper.
- 3 In the MXM Main Viewer, all of the first private LAN's nodes display their private IP addresses (**10.0.x.x**) as their own address.
- 4 In the MXM Main Viewer, all of the second LAN's nodes display their own IP addresses.
- 5 The second LAN's ALG Proxy relays registration requests for the MXM through the first LAN's ALG Proxy's public IP address.

*Multiple NATs - MXM in One of the NATs*

## 5.2 *Negotiating Firewalls*

To enable H.323 videoconferencing to traverse firewall-protected networks, VCON suggests employing its SecureConnect family of products within the following firewall negotiation solutions:

- [Routing H.323 Videoconferencing Through a Firewall](#)
- [Employing an Advanced Encryption Server for Added Security](#)

To support implementation of these solutions, open pinholes outward in your firewall as directed below.

### **Setting Up the Firewall to Support the ALG Proxy**

To add ALG Proxy support to your firewall, open pinholes outward for four specific ports. The outgoing and incoming traffic through the pinholes flows between two specific SecureConnect components only. As a result, it is not required to open ports inward or to open random or dynamic ports. External users cannot connect directly to the private LAN and the LAN's users cannot connect directly to the public network.

#### **► To add ALG Proxy support to a firewall**

- In the firewall's configuration, open any range of three ports outward as the pinholes. We recommend that you use the suggested default port selections although you may change them if your networking specifications require it.  
The fourth port must be **1720** and cannot be changed.



The lowest of the range of three ports must be set identically in the **Signalling Ports Start At** box of the ALG Proxy Firewall/Network Settings in the MXM Administrator.

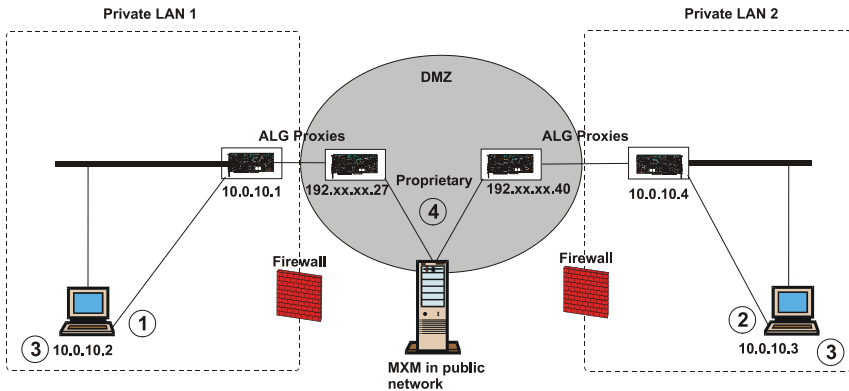
## Routing H.323 Videoconferencing Through a Firewall

In this configuration, the ALG Proxies each contain one network card and are located on both sides of the firewalls. The public ALG Proxies, residing in DMZs (DeMilitarized Zone), relay registration requests from their associated LANs to the MXM.

A communications channel between the two ALG Proxies handles address translations, enabling wanted traffic to pass through. A data packet sent to a node inside a private LAN must be addressed to the ALG Proxy outside the firewall - if the destination is known in the translation mapping, the packet is routed through to the destination.

In this solution, the administrator defines the QoS levels of the media passing through the ALG Proxy. The ALG-level QoS settings overrule QoS settings of individual end points.

Registration of nodes to the MXM requires the configuration settings described in the following illustration.

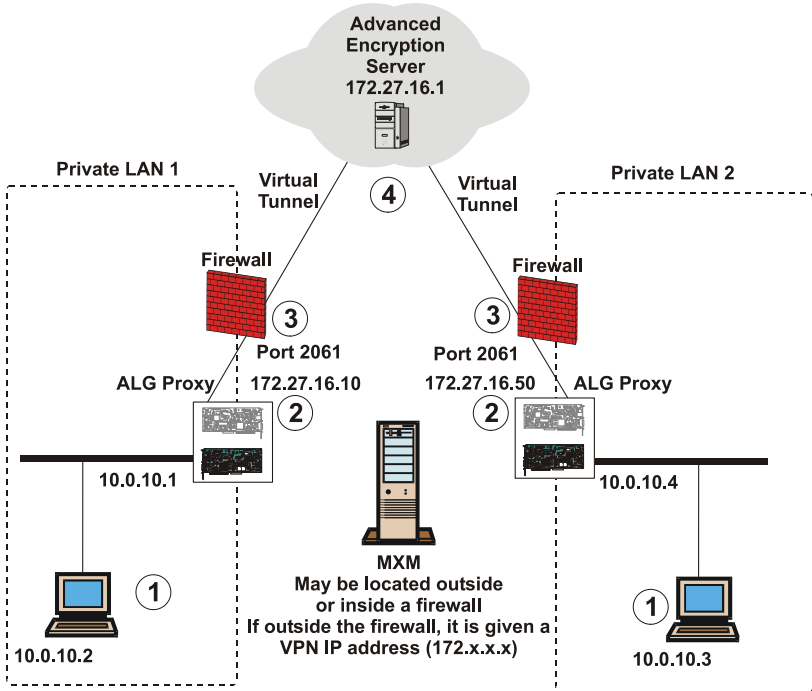


- 1 Private LAN 1's nodes enter their LAN's ALG Proxy's private address (10.0.10.1) as the MXM/Gatekeeper.
- 2 Private LAN 2's nodes enter their LAN's ALG Proxy's private address (10.0.10.4) as the MXM/Gatekeeper.
- 3 In the MXM Main Viewer, all of the Private LANs' nodes display their own IP addresses.
- 4 The public sides of the ALG Proxies relay registration requests from their respective LANs to the MXM.

### *Routing Videoconferencing Through Firewalls*

## Employing an Advanced Encryption Server for Added Security

In this configuration, the NATs communicate with each other through an encrypted network set up by an organization specifically for negotiating a firewall. This setup enables the organization's networks to engage in H.323 IP videoconferencing while retaining firewall protection against unwanted messages and requests.



- 1 Private LAN's node sends videoconference call to ALG Proxy (10.0.10.1, 10.0.10.4).
- 2 Call exits ALG Proxy through an Encryption Client (172.27.16.10, 172.27.16.50).
- 3 ALG Proxy negotiates the firewall by routing the call through port 2061.
- 4 The videoconferencing call is routed through the Advance Encryption Server towards its destination, which may also be inside a firewall.

### *Routing Videoconferences Through a More Secure, Encrypted Network*

The ALG Proxy should have two NICs - one connected to the private LAN's nodes, the other one is a VCON Encryption Client connected through a virtual tunnel to VCON Advanced Encryption Server set up outside the firewall. To route traffic through the Advanced Encryption Server, open port 2061 on the firewall.

## 5 MXM/Gatekeeper Management

In this configuration, an MXM may reside either inside a private network or outside a firewall in the public network. Registration of nodes to the MXM depends on the MXM's location, and requires the following configuration settings:

<b>MXM Inside Firewall of a Private LAN</b>	<b>MXM Outside Firewall</b>
<ol style="list-style-type: none"><li>1. The MXM LAN's nodes register directly, entering the MXM's address as the MXM/Gatekeeper.</li><li>2. The public network nodes enter the virtual IP address (<b>172.27.16.10</b>, <b>172.27.16.50</b>) of the MXM LAN's ALG Proxy.</li></ol>	<ol style="list-style-type: none"><li>1. Private LAN nodes enter their respective LAN's ALG Proxy's private address (<b>10.0.10.1</b>, <b>10.0.10.4</b>) as the MXM/Gatekeeper.</li><li>2. In the MXM Main Viewer, all of the Private LAN nodes display their own IP addresses.</li></ol>



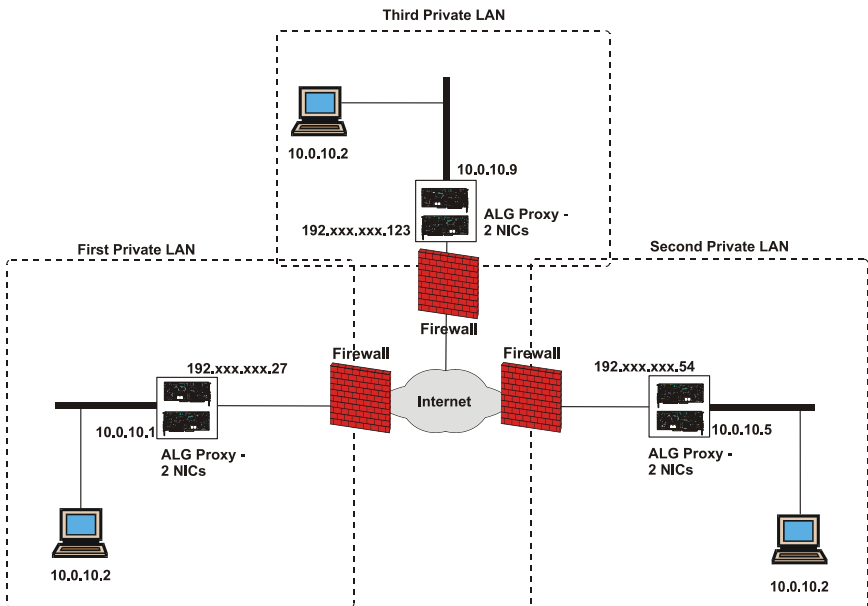
### 5.3 ALG Proxy Employment in Multiple NATs

This section suggests possible topologies for ALG Proxy employment in NATs within WANs that include more than two NATs. The suggested topologies are:

- 1 ALG Proxy (2 NICs in each) Installed at Each NAT
- 2 ALG Proxies (1 NIC in each) Installed at Each NAT
- Encryption Client Installed at Each NAT

#### 1 ALG Proxy (2 NICs in each) Installed at Each NAT

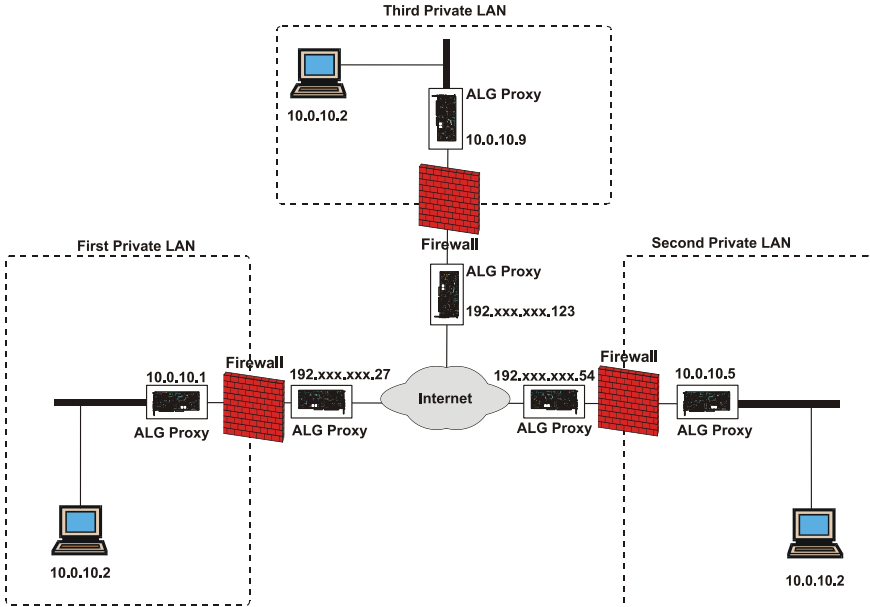
In this configuration, each NAT has its own ALG Proxy containing a NIC with a private IP address and a NIC with a public IP address. This configuration requires that all ALG-associated ports (to set ports, see “[Setting Up the Firewall to Support the ALG Proxy](#)” on page 23) in the firewall be open for routing data to and from the ALG Proxy.



*1 ALG Proxy (2 NICs in Each) Installed at Each NAT*

## 2 ALG Proxies (1 NIC in each) Installed at Each NAT

In this configuration, one ALG Proxy resides inside each NAT while its corresponding server resides outside the NAT's firewall. To allow data to pass between the NICs, open the required ports.

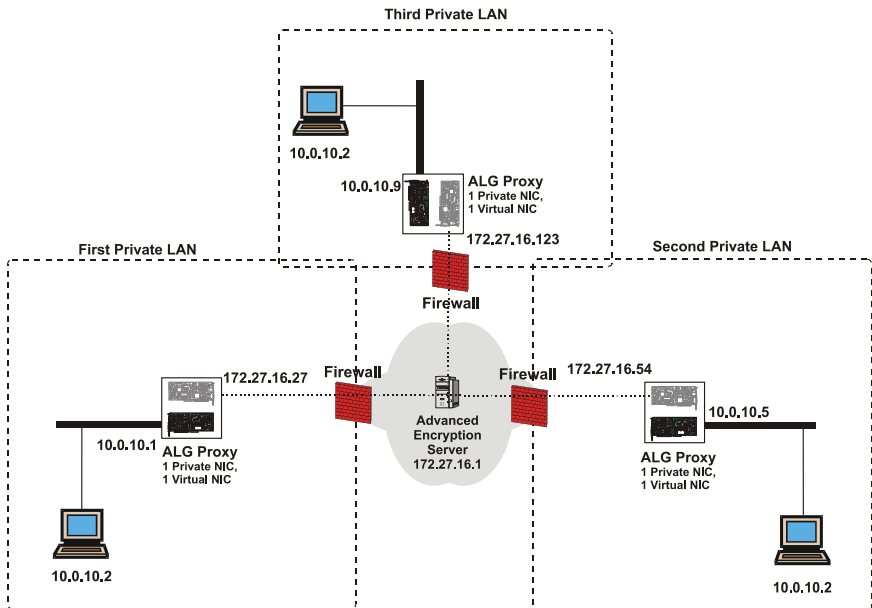


*2 ALG Proxies (1 NIC in Each) Installed at Each NAT*

## Encryption Client Installed at Each NAT

In this configuration, one ALG Proxy resides inside each NAT and includes a NIC with a private IP address and a VCON Encryption Client connected to an Advanced Encryption Server located outside the NAT's firewall. Port 2061 of the firewall is open for all data whose source or destination is the Advanced Encryption Server.

Of all the suggested solutions that were presented in this section, this one is the most cost-efficient for providing videoconferencing services while maintaining a secure network. Although any VPN Client/Server application may be used, the VCON Advanced Encryption Server solution is optimal because of its tight integration with the VCON SecureConnect family's functionality.



*Encryption Client Installed at Each NAT*

