

## Configuring your LifeSize System for Firewall Traversal

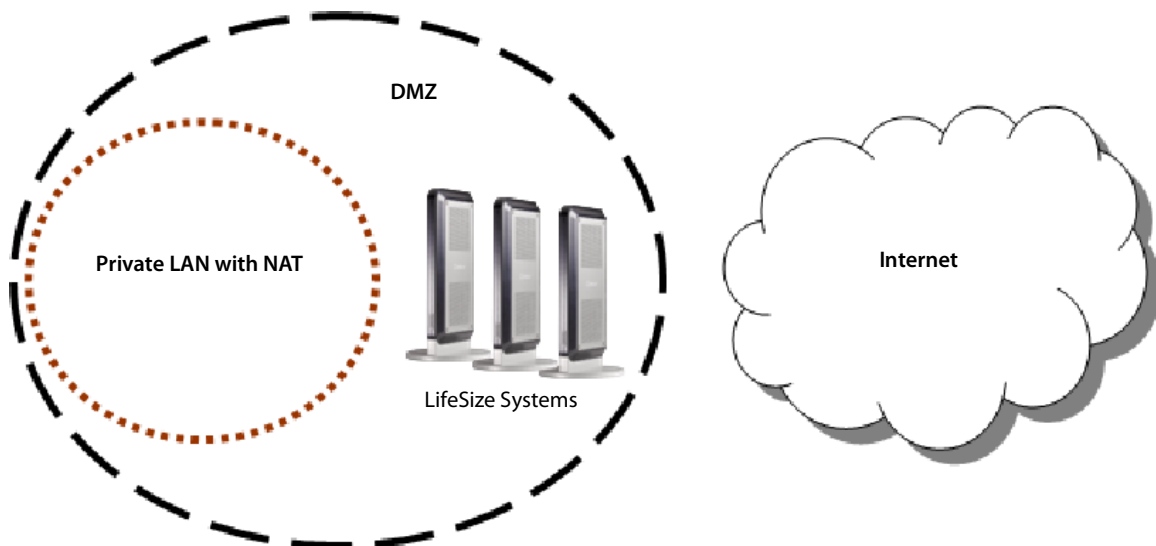
This document explains how to configure your LifeSize video communications systems for firewall traversal, assuming you are not using firewall traversal products such as LifeSize Transit. If you are using LifeSize Transit, refer to the *LifeSize Transit Deployment Guide* for more information about configuring your systems to work in that environment.

### Placement Behind a Firewall

LifeSize recommends you place your system behind a firewall. You can place it in the DMZ with a public IP address or in a private LAN with Network Address Translation (NAT).

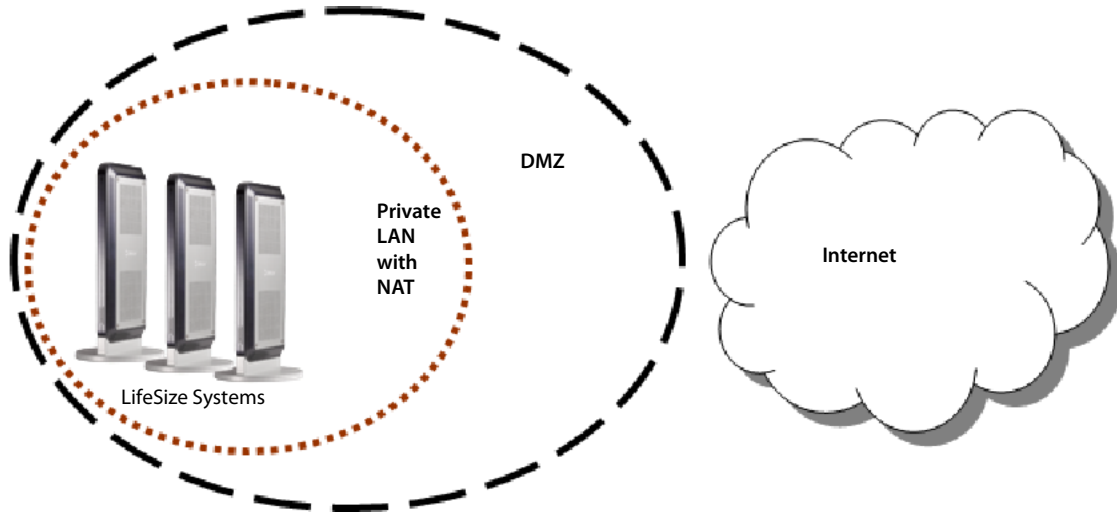
#### *DMZ with a Public IP Address*

Placing your systems in the DMZ allows you to assign them public IP addresses, making it easier to connect with public video communications devices in the Internet.



## Private LAN with NAT

Placing your video communications systems in the private LAN with NAT obscures their private IP addresses but makes calls with systems outside of your network more complicated.



## Firewall Settings for Ports

At a minimum, block external or inbound access to the following ports:

- 22 (ssh)
- 23 (telnet)
- 80 (http)
- 443 (https)

LifeSize recommends these ports remain open for internal administrator access. Ensure that you change the default administrator and command line interface passwords to be secure. For information about changing the default administrator password, refer to the administrator guide for your LifeSize system or the LifeSize Passport user guide. For information about changing the command line interface password, refer to the automation command line interface guide for your system.

You can disable ssh and web access on the system. Telnet access is disabled by default. For more information about remote access, refer to the administrator guide for your system, or the LifeSize Passport user guide.

To place calls to other systems through the firewall, you must configure your firewall to allow incoming and outgoing traffic to the system through the following:

- TCP port 1720 (for H.323 call negotiation)
- UDP port 5060 (for SIP call negotiation)
- TCP port 5060 (for SIP call negotiation if TCP signaling is enabled for SIP calls)
- TCP port 5061 (for TLS signaling in SIP calls if TLS signaling is enabled)
- Required TCP and UDP ports in the range specified in **Administrator Preferences : Network : Reserved Ports**.

## Restricting Reserved Ports

To place calls to other devices through a firewall, you must configure your firewall to allow incoming and outgoing traffic to the LifeSize system through the reserved ports. Users placing calls through a firewall to systems with public IP addresses may experience one-way audio or video if the firewall is not properly configured to allow two-way video and audio traffic.

By default, LifeSize systems communicate through TCP and UDP ports in the range 60000 - 64999 for video, voice, presentations, and camera control. LifeSize systems use only a small number of these ports during a call. The exact number depends on the number of participants in the call, the protocol used, and the number of ports required for the type (video or voice) of call.

To minimize the number of UDP and TCP ports that are available for communication, you can restrict the range by changing values in **Administrator Preferences : Network : Reserved Ports**. LifeSize recommends that the range you choose, if other than a subset of the default range, begins with a port number greater than 10000. The UDP range must start with an even number and end with an odd number, resulting in an even number of ports. For example, set the lower end of the range to 62000 and the upper end of the range to 62055 to allocate a range of 56 ports.

**Note:** Changing the TCP range causes an automatic reboot of the system

An H.323 video call with a presentation requires more ports than other types of calls. The following table identifies the number of UDP and TCP ports needed for an H.323 video call with a presentation based on the maximum number of connections. SIP uses fewer ports so if your range accommodates the required number of ports for H.323, it will also accommodate SIP.

LifeSize Video Communications System	Maximum Connections	Required Ports for an H.323 Call	Port Range Example
LifeSize Room 220	Eight-way video call and a presentation	56 UDP 14 TCP	60000 – 60055 60000 – 60013
LifeSize Room 200, LifeSize Room	Six-way video call and a presentation	40 UDP 10 TCP	60000 – 60039 60000 – 60009
LifeSize Team 220, LifeSize Team 200, LifeSize Team MP	Four-way video call and a presentation	24 UDP 6 TCP	60000 – 60023 60000 – 60005
LifeSize Express 220, LifeSize Express 200, LifeSize Express, LifeSize Passport	Two-way video call with a presentation and an audio call	10 UDP 4 TCP	60000 – 60009 60000 – 60003

## Using LifeSize Systems in a Private LAN with NAT

If you choose to place your video communications systems in a private LAN, you must use NAT to communicate with outside systems. This may include enabling static NAT on your LifeSize system. Refer to Enabling Network Address Translation (NAT) in your administrator guide, the LifeSize Passport user guide.

On your firewall, whether standalone or built into your router, you must do one of the following:

- Use one to one NAT and open the ports listed in the previous table over that connection bidirectionally with an access list.
- Forward the ports listed in the previous table to your LifeSize system.

Refer to your firewall vendor's documentation for more information.

## Testing your NAT Environment

1. Place a call from the system in the private LAN to a system in the Internet. If the far end system receives your internal, non-routable IP address (for example 192.168.x.x, or 10.10.x.x, or 172.x.x.x), your firewall is not implementing NAT properly and you must enable NAT on your private LifeSize system.
2. Place a call from a system on the Internet to your system in the private LAN. If your private system connects within the first two seconds after answering, your NAT configuration is working properly. If the call does not connect after answering, and finally disconnects after 30 to 50 seconds, the reserved port settings on your codec do not match the settings on your firewall. Ensure the system and firewall settings for UDP/TCP ports match.
3. If you still cannot place a successful call, you may have to disable the stateful packet inspection feature on the firewall. Some firewall vendors may call this feature dynamic packet filtering. Refer to your firewall vendor's documentation for more information.