



LifeSize[®] Transit[™] Deployment Guide

June 2011

LifeSize Transit Server
LifeSize Transit Client

Firewall and NAT Traversal with LifeSize Transit

Firewalls and Network Address Translation (NAT) devices can interfere with calls from video communications systems outside your network. LifeSize Transit helps those calls traverse the firewall and NAT devices successfully.

This guide is for administrators responsible for configuring, maintaining, and troubleshooting video communications devices that use SIP or H.323 protocols on your network and assumes that you have a working knowledge of the supporting infrastructure (for example, SIP domains, SRV records, SIP registrars, and H.323 gatekeepers) that may be required to deploy these devices.

This guide describes the following:

- How LifeSize Transit handles firewall traversal for SIP and H.323 calls
- The configuration options available
- The associated tasks that you must perform to deploy the product
- Troubleshooting your deployment
- Maintaining LifeSize Transit

Configuration instructions in this guide identify the specific protocol to which they apply. If you are using both SIP and H.323 protocols, complete the configuration tasks applicable to both protocols and the deployment option that you choose. By default, both protocols are enabled on LifeSize video communications systems. Refer to your LifeSize video communications system's technical documentation for information about enabling or disabling these protocols.

How LifeSize Transit Works

LifeSize Transit addresses firewall and NAT traversal for SIP and H.323 calls using a client/server approach. LifeSize Transit Server, which resides in the DMZ on your network, is a unified set of firewall and NAT traversal technologies. It enables firewall and NAT traversal, session and media control for UDP, TCP, and HTTP media, as well as H.460 control. It also serves as an H.323 gatekeeper or SIP proxy and registrar. The LifeSize Transit Server is both an H.460 traversal server and a SIP traversal server.

LifeSize Transit Server includes a signaling server that handles firewall and NAT traversal, call setup, operation and maintenance services and a media server that is optimized for relaying the actual voice, video, and presentation data. When you install LifeSize Transit Server, you configure each of these servers with its own static, public IP address (either NATed or un-NATed). Refer to [Deploying LifeSize Transit Server with NAT](#). The public IP address of the signaling server is used by callers outside your network to place calls to your video communications devices.

LifeSize video communications systems residing behind the firewall in your private network include client software through which these devices register with LifeSize Transit Server. If your LAN includes a supported H.323 gatekeeper, an MCU, or supported third party video communications devices, LifeSize recommends you use LifeSize Transit Client—a standalone multi-user traversal client—to serve as a SIP and H.323 proxy for calls with LifeSize Transit Server.

The registration to LifeSize Transit Server, either from LifeSize video communications systems or from the LifeSize Transit Client, creates a connection to the server that is kept alive through small packets that are sent at measured intervals, enabling the server to communicate with the client when it receives an incoming call. The client can then initiate outbound connections on the firewall.

LifeSize Transit Configuration Options

You can deploy LifeSize Transit in one of the following ways:

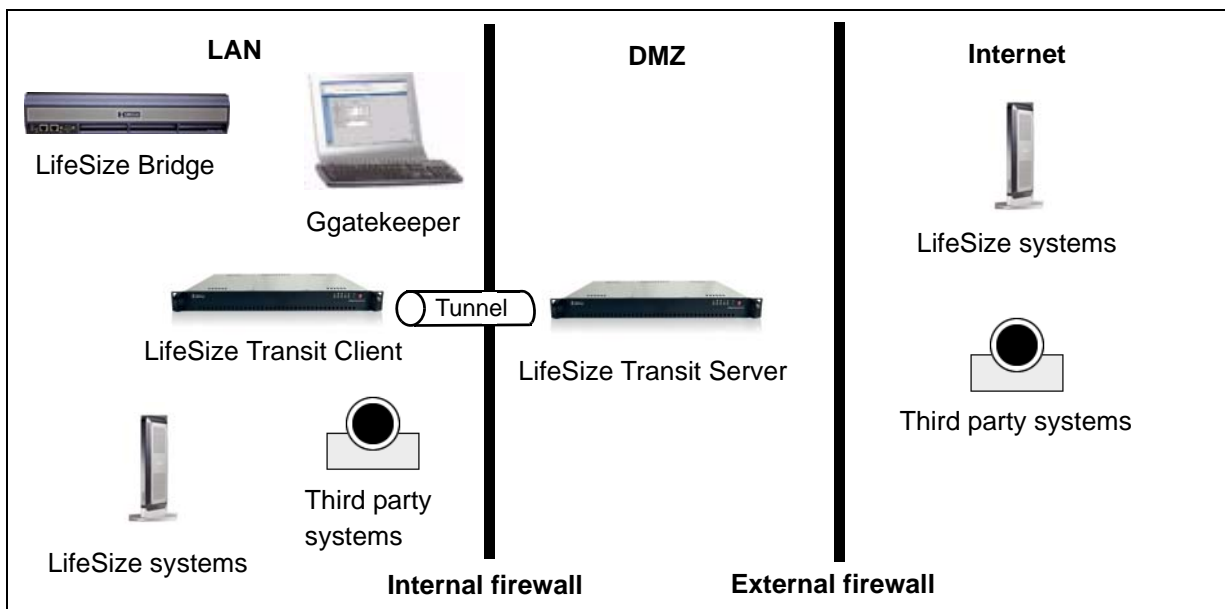
Option 1: Deploying LifeSize Transit Server with LifeSize Transit Client

LifeSize recommends this option. Deploy both LifeSize Transit Server and LifeSize Transit Client if your network meets **any** of the following conditions:

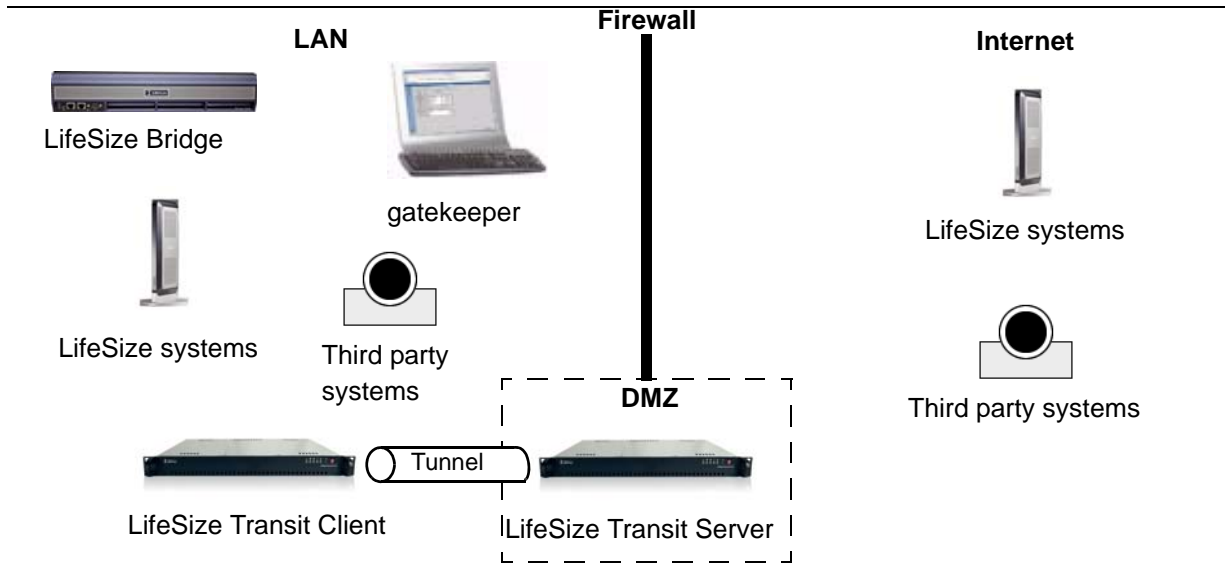
- You are using third party video communications devices that do not support H.460 or SIP STUN/TURN traversal.
- You are using LifeSize Bridge or some other supported MCU and/or an H.323 gatekeeper in your private network. Refer to the LifeSize Transit release notes for a list of supported MCUs and H.323 gatekeepers. This document is available at lifesize.com/support.

LifeSize recommends that if you deploy LifeSize Transit Client, you configure all devices, including LifeSize video communications systems to use LifeSize Transit Client, either directly if you are not using a gatekeeper in the LAN or through a gatekeeper.

LifeSize Transit Server and LifeSize Transit Client (Two Firewall Appliances)



LifeSize Transit Server and LifeSize Transit Client (One Firewall Appliance)

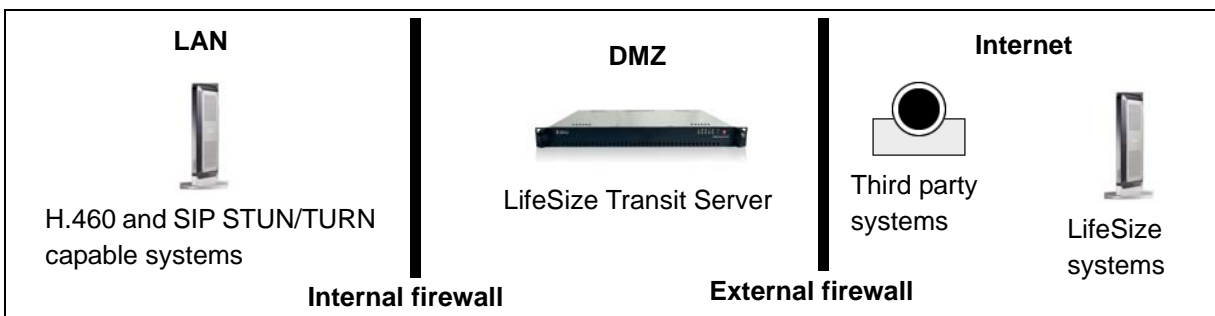


Option 2: Deploying LifeSize Transit Server Only

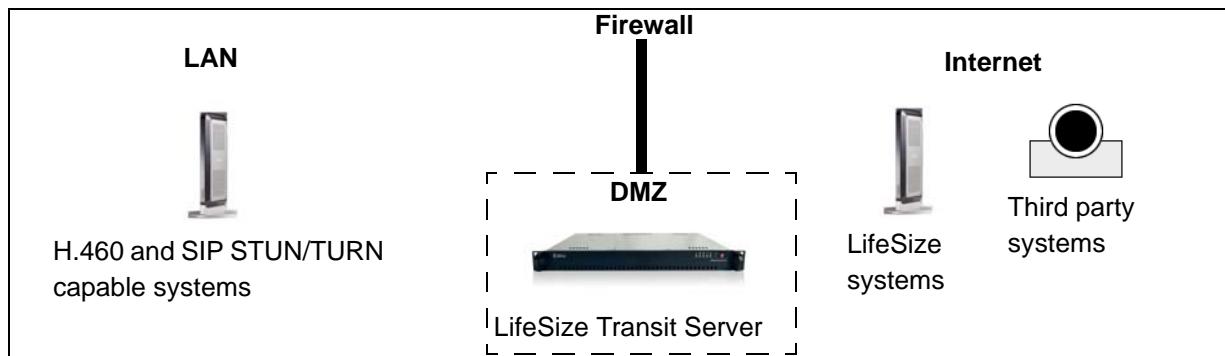
You can use LifeSize Transit Server by itself only if your network meets **all** of the following conditions:

- You are using only video communications systems behind the firewall in your private network that support either H.460 or SIP STUN/TURN traversal.
- An MCU or H.323 gatekeeper does not exist in your private network.

LifeSize Transit Server Only (Two Firewall Appliances)



LifeSize Transit Server Only (One Firewall Appliance)



Deploying LifeSize Transit Server with NAT

No matter which deployment option you choose, deploy LifeSize Transit Server in the DMZ. The server can be un-NATed with static public IP addresses for the signaling and media servers, or NATed with public IP addresses mapped to private IP addresses for the signaling and media servers. If deployed behind a static NAT, all other SIP/H.323 devices must communicate with LifeSize Transit Server by its public address. The server can not be deployed on the same LAN as the video communication systems.

If you chose to NAT the LifeSize Transit Server, use the public IP address of the signaling server when configuring the tunnel account from LifeSize Transit Client, and ensure **Use public address** is selected in **Configuration : SIP** and **Configuration : H323** on LifeSize Transit Server. When static NAT is configured, the public and internal addresses of the media and signaling server appear on the LifeSize Transit Server Dashboard.

NOTE You can configure the private IP address for static NAT only during the initial configuration or in console mode.

Deploying LifeSize Transit

Deploying LifeSize Transit includes the following tasks:

1. Install LifeSize Transit Server and, optionally, LifeSize Transit Client according to the deployment option that best fits your environment. You can deploy the server and client as hardware or virtual appliances. Refer to the *LifeSize Transit Installation Guide* or the *LifeSize Transit Virtual Appliance Installation Guide* for detailed instructions.

2. Optionally, create DNS entries.

For LifeSize Transit Server to be publicly accessible, the signaling and media servers need public addresses that are registered in the global DNS service. If your organization does not manage its domain names, ask your Internet Service Provider (ISP) to do this. The DNS entries chosen for the servers should match the name in the SSL certificate. For example:

- `pxs1.example.com` for the signaling server
- `me1.example.com` for the media server

3. Ensure that you can access the web administration interface of LifeSize Transit Server and, if installed, LifeSize Transit Client from a supported web browser in your private network. You must allow access to TCP port 8181 on LifeSize Transit Server and LifeSize Transit Client. LifeSize recommends that you restrict this access to systems in the private LAN.

For LifeSize Transit Server, enter the IP address or fully qualified domain name of the signaling server plus port 8181 on HTTPS. For example:

```
https://lifesize_transit_server_IP_address:8181
```

```
https://transitserver.example.com:8181
```

For LifeSize Transit Client, enter its IP address plus port 8181 on HTTPS. For example:

```
https://lifesize_transit_client_IP_address:8181
```

The default value for both the username and password on LifeSize Transit Server and LifeSize Transit Client is *admin*. Navigate to **Maintenance : Change Password** on both the server and client user interfaces to change the password.

Refer to the LifeSize Transit release notes for a list of supported web browsers.

4. Check for software updates and upgrade LifeSize Transit Server and LifeSize Transit Client to the latest versions to ensure they are compatible. Refer to the LifeSize Transit release notes and ensure that supported LifeSize and third party devices in your environment are installed with compatible software.
5. If you are placing or receiving H.323 calls with your video communications systems, refer to [Deploying LifeSize Transit for H.323 Calls](#).
6. If you are using the built-in gatekeeper in LifeSize Transit Server, and want to receive calls in the Annex O format (username@domain), create H.323 local domains and DNS SRV RR records. Refer to [Annex O Dialing](#).
7. If you are placing or receiving SIP calls with your video communications systems, create SIP domains and DNS SRV RR records. Refer to [Deploying LifeSize Transit for SIP Calls](#).
8. Create a user account in LifeSize Transit Server for each video communications system and MCU in your private network. Refer to [Creating User Accounts](#).
9. Create a tunnel account for LifeSize Transit Client if included in your installation. Refer to [Creating Tunnel Accounts](#).
10. Configure firewall settings to enable communication between the clients in your private network and LifeSize Transit Server in the DMZ. Refer to [Configuring Ports for LifeSize Transit](#).
11. Configure the video communications devices in your private network to use LifeSize Transit. Refer to [Configuring LifeSize Systems for Firewall Traversal](#).
12. Test the installation by placing and monitoring calls. Instructions appear in each section of this manual that describes how to configure LifeSize video communications systems.

Updating Certificates for LifeSize Transit Server

LifeSize Transit Server employs certificate security for connecting to the server from a browser, using SIP/TLS, and secure tunneling on port 443. Although LifeSize Transit Server has pre-installed certificates, LifeSize recommends you replace these with certificates customized to your implementation from a certificate authority. LifeSize Transit accepts certificates in the OpenSSL style PEM file format.

Replacing the Trusted Root Certificate for SIP/TLS

Apply to a certificate authority for a trusted root certificate and then complete the following steps:

1. From LifeSize Transit Server, navigate to **Configuration : SIP : Certificates** or **Configuration : Tunnel Certificates**.
2. Click **Add root certificate**.
3. Browse to the certificate file
4. Click **Save**.

Replacing the SIP/TLS Certificates

If you want to use SIP/TLS, upload a PEM file with a server certificate and a private key that matches the SIP domain of the server. Apply to a certificate authority for a server certificate and then complete the following steps:

1. From LifeSize Transit Server, navigate to **Configuration : SIP : Certificates**.
2. Under **TLS Certificates**, click **Replace**.
3. Click **Browse** and locate the certificate file.
4. Enter the password for the file.
5. Click **Save**.

If no SIP/TLS certificate has been installed, the tunnel certificates are used for SIP/TLS.

Replacing Tunnel Certificates

If you want to use secure tunneling on port 443, you should upload a tunnel certificate that matches the hostname of the server. Apply to a certificate authority for a server certificate and then complete the following steps:

1. From LifeSize Transit Server, navigate to **Configuration : Tunnel Certificates**.
2. Under **TLS Certificates**, click **Replace**.
3. Click **Browse** and locate the certificate file.
4. Enter the password for the file.
5. Click **Save**.

Deploying LifeSize Transit for SIP Calls

LifeSize Transit Server includes a SIP registrar that stores user registrations and handles authentication. You create user accounts on LifeSize Transit Server for each video communications device that will place or receive SIP calls. You then use the information from these accounts to configure your video communications devices to register with the SIP registrar on LifeSize Transit Server and use the SIP traversal technologies included in both the client and the server.

The SIP registrar on LifeSize Transit Server can handle more than one domain at a time and can simultaneously work as a proxy for other SIP domains. It can restrict which SIP domains are allowed to register through the server, but does not limit the registered users to place or receive calls from foreign domains.

If you are planning to place or receive SIP calls with your video communications devices, you must do the following:

1. Configure a SIP domain on LifeSize Transit Server. Refer to [Configuring SIP Domains](#).
2. Create SIP DNS SRV records. Refer to [Configuring DNS SRV Records for SIP](#).

For an overview of how LifeSize Transit SIP NAT traversal works, refer to [NAT Traversal for SIP Calls](#).

Configuring SIP Domains

You must configure a SIP domain name to use the LifeSize Transit Server for SIP calls.

1. From LifeSize Transit Server, navigate to **Configuration : SIP : Registrar**.
2. In **Add domain**, enter your SIP domain name.
3. Click **Add**.

Configuring DNS SRV Records for SIP

To make your SIP domain reachable from other clients or other SIP servers, set up a SIP DNS SRV record, so that you do not need to configure external systems with the IP address of LifeSize Transit Server. If all calls go through the LifeSize Transit Server or LifeSize devices, your SIP domain does not have to resolve through DNS.

The signaling server on LifeSize Transit Server acts as the registrar for the particular domain(s). Use its IP address as the target in SIP SRV records. A typical SIP SRV RR for the registrar at domain example.com looks like the following:

_Service._Proto.Name	TTL	Class	Priority	Weight	Port	Target
_sip._udp.example.com		IN	0	0	5060	<i>Signaling server IP address</i>
_sip._tcp.example.com		IN	0	0	5060	<i>Signaling server IP address</i>
_sips._tcp.example.com		IN	0	0	5061	<i>Signaling server IP address</i>

NAT Traversal for SIP Calls

NAT Traversal for SIP calls with LifeSize Transit Server relies on a suite of protocols: Session Traversal Utilities for NAT (STUN), Traversal Using Relay NAT (TURN), and Interactive Connectivity Establishment (ICE). If NAT traversal using these protocols is not possible, the server attempts to use a proprietary method referred to as tunneled mode.

LifeSize Transit attempts to use the most efficient traversal method in the following order: STUN with ICE, TURN, and the LifeSize proprietary tunneling mode. In tunneled mode, LifeSize systems or the LifeSize Transit Client establish a tunneled connection to LifeSize Transit Server using TCP port 444 (if available) or TCP port 443.

At startup and at regular intervals thereafter, a LifeSize system that is configured to work with LifeSize Transit probes the network toward LifeSize Transit Server to determine what traversal methods are possible. When these clients connect from NAT using SIP, the public address is noted instead of what is reported from the client. Based on the reported client capabilities, the server decides whether relay is needed when this client participates in a call. The server also ensures that the signaling channel is kept open while the client is registered.

STUN, TURN, and ICE

STUN enables your LifeSize devices behind your firewall to discover the public IP address and port mappings that they can use to communicate with other devices during a call and to instruct the other devices where to send media. LifeSize Transit Server includes a STUN server on both the signaling and media servers.

TURN is an extension of STUN. It allocates a public IP address and port on a server and uses this allocation to relay media between the devices in a call. LifeSize Transit Server is a TURN server. These relay sessions consume resources on the servers, and, therefore, must be authenticated. The credentials in the tunnel account that you create in LifeSize Transit Server for each device are used for this purpose.

ICE is a protocol that makes use of STUN and TURN. It determines the best method for traversal based on a list of transport addresses—a combination of an IP address and UDP port—that each device in a call gathers through STUN, TURN, and from physical or logical network interfaces. ICE is enabled on LifeSize video communications systems by default in **Administrator Preferences : Network : LifeSize Transit** when you configure the devices to use LifeSize Transit for SIP calls.

To ensure ICE uses efficient, direct communication with remote endpoints, configure the firewall rules to allow UDP connections from the LAN toward any remote host, and accept return traffic on the same ports.

Deploying LifeSize Transit for H.323 Calls

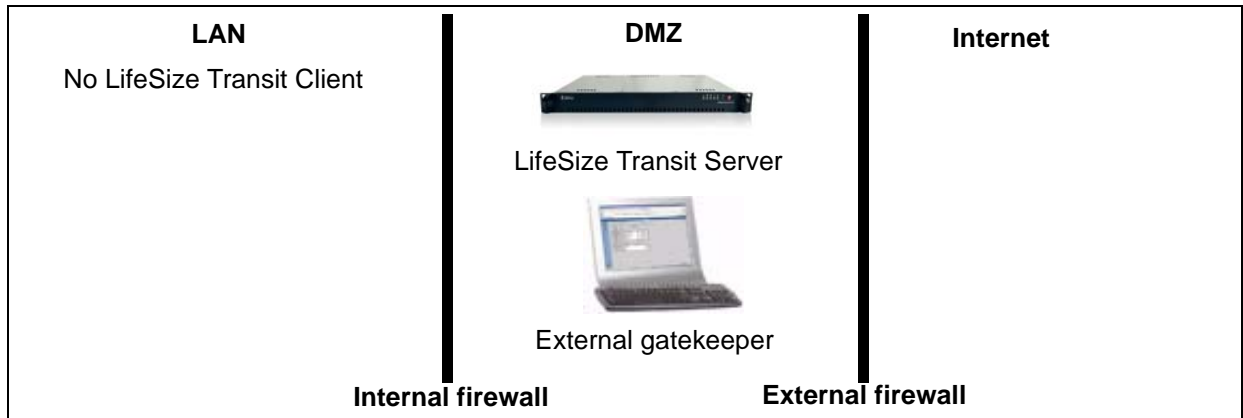
LifeSize Transit supports H.460.18 for H.323 traversal call control and call establishment and H.460.19 for H.323 media traversal control in addition to H.323 on the server side. The deployment consists of the LifeSize Transit Server, which includes an H.460 server, an H.323 gatekeeper, and the clients that you configure to use the server.

To use LifeSize Transit with H.323 calls, you must configure each video communications system with a gatekeeper address. LifeSize Transit can work with a private gatekeeper in the LAN, an external gatekeeper, or use the built-in gatekeeper functionality on LifeSize Transit Server.

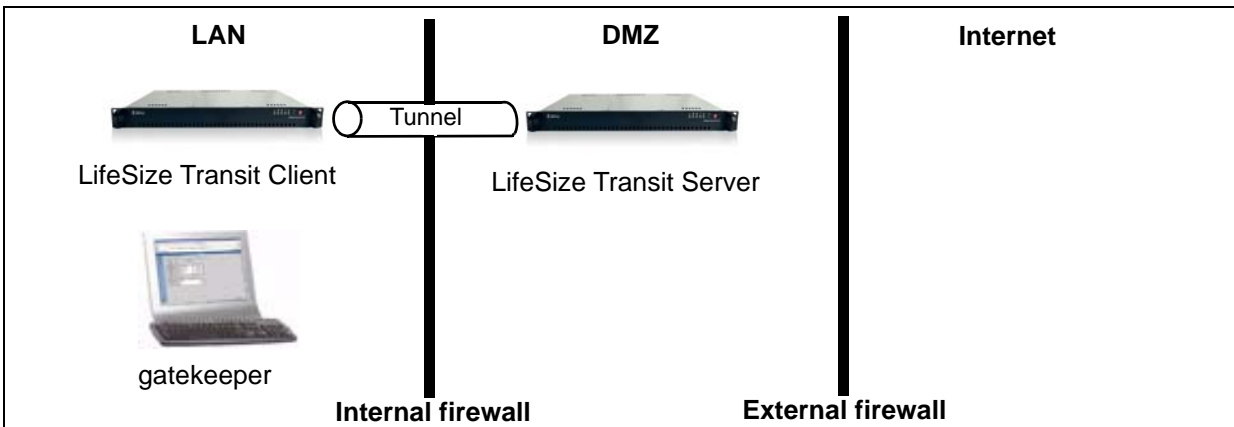
Built-in Gatekeeper with or without LifeSize Transit Client



External Gatekeeper with No LifeSize Transit Client



Gatekeeper in the LAN with LifeSize Transit Client



Annex O Dialing

LifeSize Transit handles Annex O dialing (username@domain) to external gatekeepers and video communications devices automatically by looking up the H.323 DNS SRV records for the external systems with fallback to DNS A records.

If you are using the built-in gatekeeper and want to receive H.323 calls in Annex O format, complete the following steps:

1. Configure an H.323 local domain on LifeSize Transit Server. Refer to [Configuring H.323 Local Domains](#).
2. Create H.323 DNS SRV records. Refer to [Configuring DNS SRV Records for H.323](#).

Configuring H.323 Local Domains

You must configure an H.323 domain name to use the LifeSize Transit Server for receiving H.323 calls. To configure an H.323 local domain, follow these steps:

1. From LifeSize Transit Server, navigate to **Configuration : H.323 : Local Domains**.
2. In **Add domain**, enter your H.323 local domain name.
3. Click **Add**.

The IP address is automatically recognized as an H.323 local domain. Domain names must be defined as H.323 local domains to be recognized by the built-in gatekeeper.

Configuring DNS SRV Records for H.323

To make your H.323 domain reachable from other clients or other H.323 servers through the Annex O format, set up an H.323 DNS SRV record, so that you do not need to configure external systems with the IP address of the LifeSize Transit Server. If all calls go through the LifeSize Transit Server or LifeSize devices, your H.323 domain does not have to resolve through DNS.

The signaling server on LifeSize Transit Server acts as the gatekeeper for the domains. Use its IP address as the target in H.323 SRV records. Typical H.323 SRV records for the gatekeeper at the domain *example.com* look like the following:

_Service._Proto.Name	TTL	Class	Priority	Weight	Port	Target
_h323ls._udp.example.com		IN	0	0	1719	<i>Signaling server IP address</i>
_h323cs._tcp.example.com		IN	0	0	1720	<i>Signaling server IP address</i>

Using the Built-In or an External Gatekeeper

LifeSize Transit Server without LifeSize Transit Client

If you are using LifeSize Transit Server and its built-in gatekeeper or an external gatekeeper, configure your video communications devices with the signaling server IP address as the gatekeeper address and ensure that H.460 is enabled on the device. Refer to [Deploying LifeSize Transit Server with NAT](#) if you chose to NAT the signaling server IP address. With an external gatekeeper, you must also configure LifeSize Transit Server to use the external gatekeeper. You can choose the gatekeeper option that applies to your deployment from the **Configuration : H.323 : Configuration** page in the LifeSize Transit Server web administration interface. When you choose the option to use an external gatekeeper, you specify the IP address and vendor of the external gatekeeper. If the gatekeeper employs H.235 authentication, enter the gatekeeper username and password.

Deploying LifeSize Transit Client with Built-In Gatekeeper

If you are using LifeSize Transit Client with the built-in gatekeeper in LifeSize Transit Server, configure the connection between the LifeSize Transit Client and the server and then configure your video communications systems to use the IP address of LifeSize Transit Client as the gatekeeper address. Because traversal is handled by the LifeSize Transit Client in this configuration, ensure that H.460 is not enabled on the video communications devices.

Complete the following steps before configuring video communications devices to use LifeSize Transit.

1. Ensure that LifeSize Transit Server and LifeSize Transit Client are installed on your network.
2. Ensure that a tunnel account for LifeSize Transit Client exists on the **Configuration : Tunnel Accounts** page on LifeSize Transit Server. Refer to [Creating Tunnel Accounts](#).
3. Configure the firewall to allow communication between LifeSize Transit Server and LifeSize Transit Client. Refer to [Configuring Ports for LifeSize Transit](#).
4. From LifeSize Transit Server, navigate to **Configuration : H.323 : Configuration**.
5. For the **Gatekeeper mode**, select **Use built-in gatekeeper**.
6. If the gatekeeper is configured for H.235 authentication, select *H.235* from **Q931 Authentication** and **RAS Authentication**.
7. From LifeSize Transit Client, navigate to the **Configuration : Tunnel**.
8. In **Servers**, enter the IP address of the signaling server on LifeSize Transit Server. Refer to [Deploying LifeSize Transit Server with NAT](#) if you chose to NAT this address.
9. Enter the username and password for LifeSize Transit Client tunnel account that you created on the LifeSize Transit Server.
10. Click **Apply**.
11. Ensure that the **Connection Status** on the **Status : Tunnel** page changes to **Connected**.
12. Navigate to **Configuration : H.323**.
13. If you leave the **H.460 Server** field set to *None* or blank, a tunneled connection is used between LifeSize Transit Client and LifeSize Transit Server for H.323 communication. TCP port 444 will be tried first. If it is not available, TCP port 443 is used. If you wish to use the H.460.18/19 traversal server, enter the IP address of the signaling server in this field. Refer to [Configuring Ports for LifeSize Transit](#) to compare the port usage and firewall configuration for each of these options.

Using a Gatekeeper in the Private LAN

When you use a supported gatekeeper in the private LAN, you must use LifeSize Transit Client. All video communications devices and LifeSize Transit Client must register to the same private gatekeeper in the LAN.

Deploying LifeSize Transit Client with a Private Gatekeeper

Complete the following steps to configure a route to the gatekeeper from LifeSize Transit Server through LifeSize Transit Client. Complete these steps before configuring video communications devices to use LifeSize Transit.

1. Ensure that LifeSize Transit Server and LifeSize Transit Client are installed on your network.
2. Ensure that a tunnel account for LifeSize Transit Client exists on LifeSize Transit Server.
3. Configure the firewall to allow communication between LifeSize Transit Server and LifeSize Transit Client. Refer to [Configuring Ports for LifeSize Transit](#).
4. From LifeSize Transit Server, navigate to **Configuration : H.323 : Configuration**.

5. For the **Gatekeeper mode**, select **Use gatekeeper at private LAN**.
6. From LifeSize Transit Client, navigate to **Configuration : Tunnel**.
7. In **Servers**, enter the IP address of the signaling server on LifeSize Transit Server. Refer to [Deploying LifeSize Transit Server with NAT](#) if you chose to NAT this address.
8. Enter the username and password for LifeSize Transit Client tunnel account that you created on LifeSize Transit Server.
9. Click **Apply**.
10. Navigate to **Configuration : H.323**, ensure that **H.460 Server** is set to *None* or is blank.
11. Ensure that the **Connection Status** on the **Status : Tunnel** page changes to **Connected**.
12. For LifeSize Transit Server to access the gatekeeper in the LAN through LifeSize Transit Client for incoming calls, add a route in LifeSize Transit Server to redirect incoming calls from the server to the gatekeeper in the private network through LifeSize Transit Client. Complete the following steps:
 - a. From LifeSize Transit Server, navigate to **Configuration : H.323 : Routing**.
 - b. Click **Add route**.
 - c. Enter an **H.323 prefix**. Only alphanumeric characters, a period (.), and a hyphen (-) are allowed.
 - d. In **H.323 gatekeeper host**, enter the IP address of the gatekeeper in the private network.
 - e. In **Tunnel**, enter the user ID of the LifeSize Transit Client. This is the user ID that you created in the **Configuration : Tunnel Accounts : Add** page in LifeSize Transit Server.
 - f. For **Gatekeeper vendor**, select *Radvision* or *Cisco*. For gatekeeper vendors not listed, select *Radvision*.
 - g. Click **Save** to add the route.
13. Configure the outbound prefix on LifeSize Transit Client for placing outbound calls:
 - a. From LifeSize Transit Client, navigate to **Dashboard**. If a connection between LifeSize Transit Client and LifeSize Transit Server was established successfully and the incoming route was added in step 12, the **H.323 internal gatekeeper** field is automatically populated with a value from the server. Ensure that the address of the gatekeeper is correct.
 - b. Navigate to **Configuration : H.323**. For **Outbound prefix**, specify a prefix number for outbound calls. This must be a unique, numeric prefix not already in use by the gatekeeper and not the same as the prefix configured on LifeSize Transit Server for routing incoming calls to the gatekeeper.
 - c. Select **Strip prefix** and **Register gatekeeper**.
 - d. If are using H.235 authorization on the gatekeeper, enter the gatekeeper username and password.
 - e. Click **Apply**.
 - f. Navigate to **Status : Gatekeeper**.
 - g. Ensure that **Registration status** is *Registered*, and the **Internal gatekeeper address** is correct.

When LifeSize Transit Client registers with the gatekeeper, the registration automatically adds the outbound prefix as a user-defined service prefix in the gatekeeper. When the gatekeeper receives an outbound call that includes this prefix, it routes the call to LifeSize Transit Client.

User and Tunnel Accounts

Creating User Accounts

Use the instructions in this section to create a user account in LifeSize Transit Server for each video communications device, MCU, or instance of LifeSize Desktop that makes or receives calls. A single account can be used for both SIP and H.323 calls.

All devices that make or receive SIP calls must register with the SIP registrar in LifeSize Transit Server. When you create these accounts, make note of the **SIP Username**, **SIP Authorization name**, and **Password** from the **Configuration : Users : Add** page in LifeSize Transit Server. You will need these values for each device later when you configure the devices to register to the SIP registrar.

For H.323 calls make note of the **H323 extension** you create in this account.

Follow these steps to create a user account for each video communications system, MCU, and LifeSize Desktop in your environment:

1. From LifeSize Transit Server, navigate to **Configuration : Users**.
2. Click **Add user**.
3. Enter the information for the new user account.

Label	Description
SIP username	Required field for SIP calls. For example, user@sipdomain.com. 50 characters maximum.
SIP authorization name	Required field for SIP calls. Usually this is the <i>user</i> portion of the SIP username <i>user@sipdomain.com</i> . At least 4, 50 characters maximum.
SIP extension/ H.323 extension	Required field for H.323 calls. The H.323 extension, which can also be used as the SIP phone extension. 50 numeric characters maximum.
H.323 name	An alias for the H.323 user. 50 characters maximum.
Password	Required field for SIP calls. 50 characters maximum.
Disabled	Select to prevent this device from registering to LifeSize Transit Server.

Except where noted, you can use alphanumeric characters, the period, the underscore, the tilde, and the dash. The @ is only valid in the SIP username. Click **Show Advanced Settings** for more optional fields.

4. Click **Save**. The new account should appear in the **Configuration : Users** page. You can edit, delete, or search for user accounts from this listing.

Creating Tunnel Accounts

You must create a tunnel account for LifeSize Transit Client if it is included in the deployment, regardless of the protocols you use on your network for video communication.

If you are using LifeSize Transit Server only, you must create a tunnel account for any device that needs to use tunneled signaling, media traversal, or TURN traversal.

As you create the tunnel accounts, make note of the **Username** and **Password** that you enter in the **Configuration : Tunnel Accounts : Add account** page. You will need these credentials to authenticate tunneling on LifeSize Transit Client and LifeSize video communications devices.

Follow these steps to create a tunnel account for LifeSize Transit Client, or if you are using LifeSize Transit Server alone, each device in your environment that must use tunneled SIP or tunneled H.323:

1. From LifeSize Transit Server, navigate to **Configuration : Tunnel Accounts**.
2. Click **Add account**.
3. Enter the **Tunnel Account ID** and **Password**. You can use alphanumeric characters, the period, the underscore, the tilde, and the dash.
4. If you select **Account disabled**, the tunnel account cannot access LifeSize Transit Server.
5. Click **Save**. The new account should appear in the **Configuration : Tunnel Accounts** page. You can edit, delete, or search for tunnel accounts from this listing.

Configuring Ports for LifeSize Transit

You must add rules to your firewall to allow inbound traffic from any IP address and port to the ports listed in the following tables as well as rules to allow outbound traffic from the ports listed in the following tables to any IP address and port. Each table and diagram is followed by an example of a full set of firewall rules for using a particular protocol with LifeSize Transit.

The example firewall rules assume that the firewall is configured to allow return traffic on any allowed connection. LifeSize recommends turning off any H.323 and SIP fix up protocols as these can cause problems in cases where they are not updated to the latest versions of the H.323 and SIP standards.

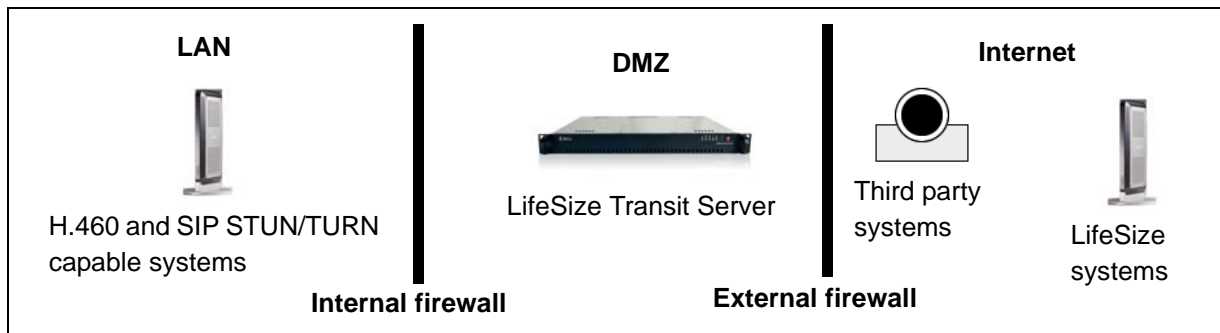
The ports and port ranges in these rules reflect the default ports for LifeSize Transit. If you change them, adjust the rules to match.

To ensure that ICE uses efficient, direct communication to remote endpoints, configure the firewall rules to allow UDP connections from the LAN toward any remote host, and accept return traffic on the same ports.

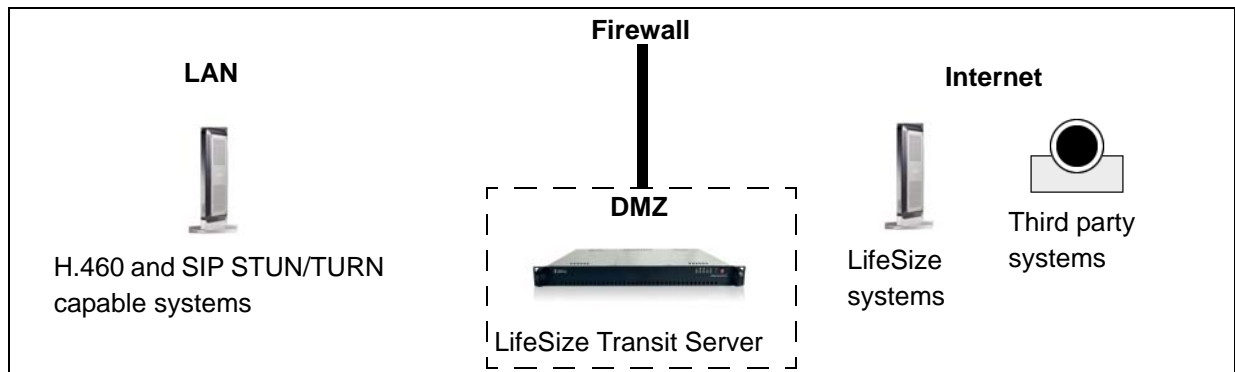
Firewalls, the LAN and the DMZ

The following firewall rules assume that your network has a DMZ, in which LifeSize Transit Server resides, and a LAN, in which your video communication systems, and, optionally, LifeSize Transit Client reside. You can achieve this environment by implementing two firewall appliances, the internal firewall forming the LAN while the external firewall forms the DMZ. However, you can also use one firewall appliance to create both the LAN and the DMZ. These two options are depicted in the following diagrams.

Two Firewall Appliances Creating the DMZ



One Firewall Appliance Generating the LAN and the DMZ



The examples that follow each table identify rules for both an external firewall and an internal firewall. If your environment does not actually have two firewall appliances, think of the external firewall as the rules that separate the DMZ from the Internet, and the internal firewall as the rules separating the private network from the DMZ. The inbound direction is always from the Internet towards the private network. The outbound direction is always from the private network towards the Internet.

NTP, DNS, SYSLOG, and SNMP Ports

Ensure that the firewall is open to that LifeSize Transit Server can access NTP (destination port 123), DNS (destination port 53), SYSLOG (destination port 514), and SNMP (destination port 162) of the respective servers.

Configuring Ports for SIP

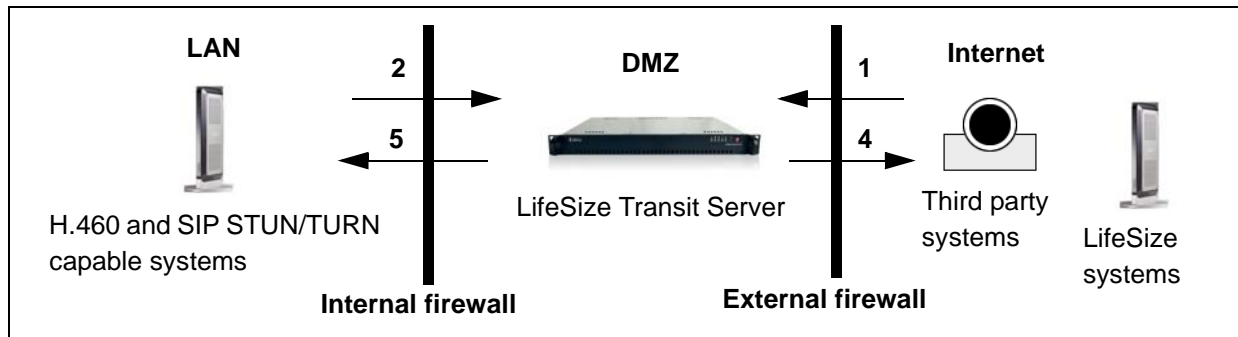
To use standards-based SIP, enable the ports listed in the following table for LifeSize Transit Server. Refer to the example set of firewall rules that follow the table.

	Signaling Server TCP	Signaling Server UDP	Media Server TCP	Media Server UDP
Basic SIP	5060, 5061	5060	NA	
STUN	NA	3478, 34501	NA	3478, 34501
TURN	3560	3560	3560	3560
RTP/Media	NA	NA	NA	45100-46699

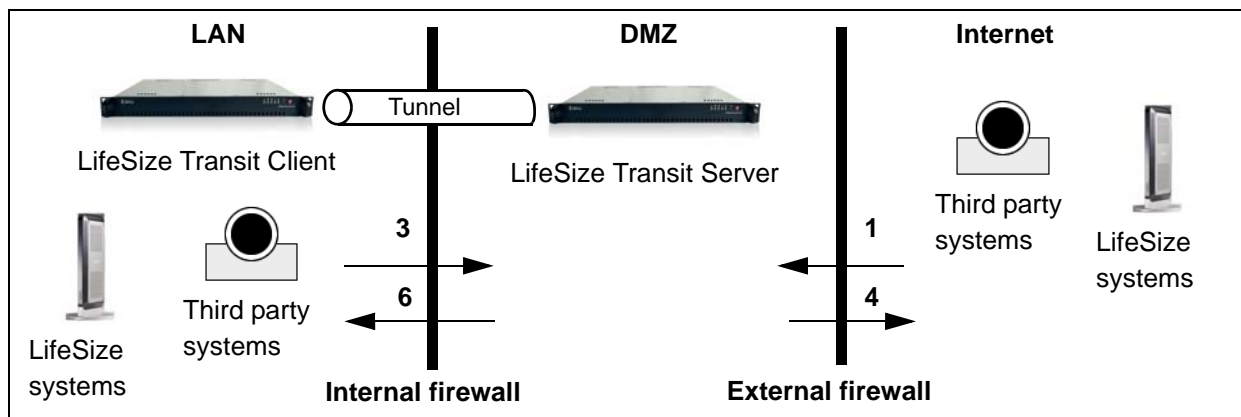
Firewall Rules for SIP/STUN/TURN/RTP with LifeSize Transit

Refer to the numbered set of rules that correspond to the numbers in the graphics.

LifeSize Transit Server Alone



LifeSize Transit Server and LifeSize Transit Client



1. External Firewall, Inbound Rules, All Cases

Allow SRC_IP=any	SRC_PORT=any	DST_IP=SignalingIP	DST_PORT=5060tcp
Allow SRC_IP=any	SRC_PORT=any	DST_IP=SignalingIP	DST_PORT=5061tcp
Allow SRC_IP=any	SRC_PORT=any	DST_IP=SignalingIP	DST_PORT=5060udp
Allow SRC_IP=any	SRC_PORT=any	DST_IP=SignalingIP	DST_PORT=3478udp
Allow SRC_IP=any	SRC_PORT=any	DST_IP=SignalingIP	DST_PORT=34501udp
Allow SRC_IP=any	SRC_PORT=any	DST_IP=SignalingIP	DST_PORT=3560tcp
Allow SRC_IP=any	SRC_PORT=any	DST_IP=SignalingIP	DST_PORT=3560udp
Allow SRC_IP=any	SRC_PORT=any	DST_IP=MediaIP	DST_PORT=3478udp
Allow SRC_IP=any	SRC_PORT=any	DST_IP=MediaIP	DST_PORT=34501udp
Allow SRC_IP=any	SRC_PORT=any	DST_IP=MediaIP	DST_PORT=3560tcp
Allow SRC_IP=any	SRC_PORT=any	DST_IP=MediaIP	DST_PORT=3560udp
Allow SRC_IP=any	SRC_PORT=any	DST_IP=MediaIP	DST_PORT=45100-46699udp

2. Internal Firewall, Outbound Rules, LifeSize Transit Server Alone

Allow SRC_IP=any	SRC_PORT=any	DST_IP=SignalingIP	DST_PORT=5060tcp
Allow SRC_IP=any	SRC_PORT=any	DST_IP=SignalingIP	DST_PORT=5061tcp
Allow SRC_IP=any	SRC_PORT=any	DST_IP=SignalingIP	DST_PORT=5060udp
Allow SRC_IP=any	SRC_PORT=any	DST_IP=SignalingIP	DST_PORT=3478udp
Allow SRC_IP=any	SRC_PORT=any	DST_IP=SignalingIP	DST_PORT=34501udp
Allow SRC_IP=any	SRC_PORT=any	DST_IP=SignalingIP	DST_PORT=3560tcp
Allow SRC_IP=any	SRC_PORT=any	DST_IP=SignalingIP	DST_PORT=3560udp
Allow SRC_IP=any	SRC_PORT=any	DST_IP=MediaIP	DST_PORT=3478udp
Allow SRC_IP=any	SRC_PORT=any	DST_IP=MediaIP	DST_PORT=34501udp
Allow SRC_IP=any	SRC_PORT=any	DST_IP=MediaIP	DST_PORT=3560tcp
Allow SRC_IP=any	SRC_PORT=any	DST_IP=MediaIP	DST_PORT=3560udp
Allow SRC_IP=any	SRC_PORT=any	DST_IP=MediaIP	DST_PORT=45100-46699udp

3. Internal Firewall, Outbound Rules, LifeSize Transit Server and LifeSize Transit Client

Allow SRC_IP=TC_IP	SRC_PORT=any	DST_IP=SignalingIP	DST_PORT=5060tcp
Allow SRC_IP=TC_IP	SRC_PORT=any	DST_IP=SignalingIP	DST_PORT=5061tcp
Allow SRC_IP=TC_IP	SRC_PORT=any	DST_IP=SignalingIP	DST_PORT=5060udp
Allow SRC_IP=TC_IP	SRC_PORT=any	DST_IP=SignalingIP	DST_PORT=3478udp
Allow SRC_IP=TC_IP	SRC_PORT=any	DST_IP=SignalingIP	DST_PORT=34501udp
Allow SRC_IP=TC_IP	SRC_PORT=any	DST_IP=SignalingIP	DST_PORT=3560tcp
Allow SRC_IP=TC_IP	SRC_PORT=any	DST_IP=SignalingIP	DST_PORT=3560udp
Allow SRC_IP=TC_IP	SRC_PORT=any	DST_IP=MediaIP	DST_PORT=3478udp
Allow SRC_IP=TC_IP	SRC_PORT=any	DST_IP=MediaIP	DST_PORT=34501udp
Allow SRC_IP=TC_IP	SRC_PORT=any	DST_IP=MediaIP	DST_PORT=3560tcp
Allow SRC_IP=TC_IP	SRC_PORT=any	DST_IP=MediaIP	DST_PORT=3560udp
Allow SRC_IP=TC_IP	SRC_PORT=any	DST_IP=MediaIP	DST_PORT=45100-46699udp

4. External Firewall, Outbound Rules, All Cases

Allow SRC_IP=SignalingIP	SRC_PORT=5060udp	DST_IP=any	DST_PORT=any
Allow SRC_IP=SignalingIP	SRC_PORT=3478udp	DST_IP=any	DST_PORT=any
Allow SRC_IP=SignalingIP	SRC_PORT=34501udp	DST_IP=any	DST_PORT=any
Allow SRC_IP=SignalingIP	SRC_PORT=3560udp	DST_IP=any	DST_PORT=any
Allow SRC_IP=SignalingIP	SRC_PORT=anyudp	DST_IP=any	DST_PORT=any
Allow SRC_IP=MediaIP	SRC_PORT=3478udp	DST_IP=any	DST_PORT=any
Allow SRC_IP=MediaIP	SRC_PORT=34501udp	DST_IP=any	DST_PORT=any
Allow SRC_IP=MediaIP	SRC_PORT=3560tcp	DST_IP=any	DST_PORT=any
Allow SRC_IP=MediaIP	SRC_PORT=3560udp	DST_IP=any	DST_PORT=any
Allow SRC_IP=MediaIP	SRC_PORT=45100-46699udp	DST_IP=any	DST_PORT=any

5. Internal Firewall, Inbound Rules, LifeSize Transit Server Alone

Allow SRC_IP=SignalingIP	SRC_PORT=5060tcp	DST_IP=any	DST_PORT=any
Allow SRC_IP=SignalingIP	SRC_PORT=5061tcp	DST_IP=any	DST_PORT=any
Allow SRC_IP=SignalingIP	SRC_PORT=5060udp	DST_IP=any	DST_PORT=any
Allow SRC_IP=SignalingIP	SRC_PORT=3478udp	DST_IP=any	DST_PORT=any
Allow SRC_IP=SignalingIP	SRC_PORT=34501udp	DST_IP=any	DST_PORT=any
Allow SRC_IP=SignalingIP	SRC_PORT=3560tcp	DST_IP=any	DST_PORT=any
Allow SRC_IP=SignalingIP	SRC_PORT=3560udp	DST_IP=any	DST_PORT=any
Allow SRC_IP=MediaIP	SRC_PORT=3478udp	DST_IP=any	DST_PORT=any
Allow SRC_IP=MediaIP	SRC_PORT=34501udp	DST_IP=any	DST_PORT=any
Allow SRC_IP=MediaIP	SRC_PORT=3560tcp	DST_IP=any	DST_PORT=any
Allow SRC_IP=MediaIP	SRC_PORT=3560udp	DST_IP=any	DST_PORT=any
Allow SRC_IP=MediaIP	SRC_PORT=45100-46699udp	DST_IP=any	DST_PORT=any

6. Internal Firewall, Outbound Rules, LifeSize Transit Server And LifeSize Transit Client

Allow SRC_IP=SignalingIP	SRC_PORT=5060tcp	DST_IP=TC_IP	DST_PORT=any
Allow SRC_IP=SignalingIP	SRC_PORT=5061tcp	DST_IP=TC_IP	DST_PORT=any
Allow SRC_IP=SignalingIP	SRC_PORT=5060udp	DST_IP=TC_IP	DST_PORT=any
Allow SRC_IP=SignalingIP	SRC_PORT=3478udp	DST_IP=TC_IP	DST_PORT=any
Allow SRC_IP=SignalingIP	SRC_PORT=34501udp	DST_IP=TC_IP	DST_PORT=any
Allow SRC_IP=SignalingIP	SRC_PORT=3560tcp	DST_IP=TC_IP	DST_PORT=any
Allow SRC_IP=SignalingIP	SRC_PORT=3560udp	DST_IP=TC_IP	DST_PORT=any
Allow SRC_IP=MediaIP	SRC_PORT=3478udp	DST_IP=TC_IP	DST_PORT=any
Allow SRC_IP=MediaIP	SRC_PORT=34501udp	DST_IP=TC_IP	DST_PORT=any
Allow SRC_IP=MediaIP	SRC_PORT=3560tcp	DST_IP=TC_IP	DST_PORT=any
Allow SRC_IP=MediaIP	SRC_PORT=3560udp	DST_IP=TC_IP	DST_PORT=any
Allow SRC_IP=MediaIP	SRC_PORT=45100-46699udp	DST_IP=TC_IP	DST_PORT=any

NOTE The UDP port range in the last item of each of the previous port tables is based on the default setting in LifeSize Transit Server. If you change this range, be sure to reflect the new range in these firewall rules.

Configuring Ports for Tunneler SIP and Tunneler H.323 with or without LifeSize Transit Client

In SIP calls with LifeSize video communications systems, LifeSize Transit Server attempts to use a tunneled connection between the LifeSize system and the server if other SIP traversal methods fail.

With software v4.8 and later, you can configure LifeSize video communications systems to use tunneled H.323 without LifeSize Transit Client.

If you are using LifeSize Transit Client with H.323 calls, the connection between the client and LifeSize Transit Server is tunneled if you configure LifeSize Transit Server to use a gatekeeper in the private LAN. The signaling and the media will be tunneled. For other gatekeeper configurations you can use either a tunneled connection or an H.460.18/19 connection to LifeSize Transit Server.

The tunnel is created on TCP port 444 or TCP port 443 (if TCP port 444 is not available). If you decide not to open port 444, you must allow unencrypted traffic on port 443 or tunneled signaling will fail.

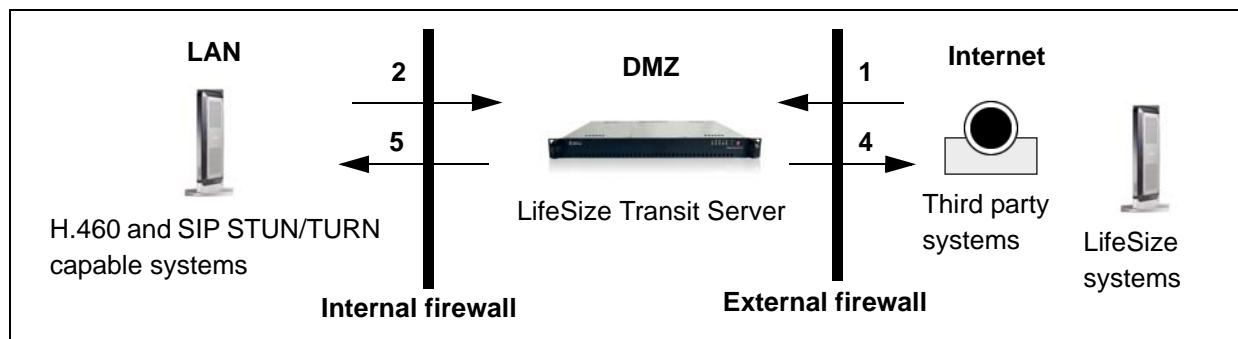
	Signaling Server TCP	Media Server TCP
LifeSize Transit tunneled connections	443 or 444	443 or 444

NOTE These rules only allow calls between LifeSize devices in tunneling mode and devices registered to LifeSize Transit Clients. If you want to make SIP/H.323 calls to external systems, you must also open the external firewall ports as described in [Firewall Rules for SIP/STUN/TURN/RTP with LifeSize Transit](#) and [Configuring Ports for H.323 and H.460](#).

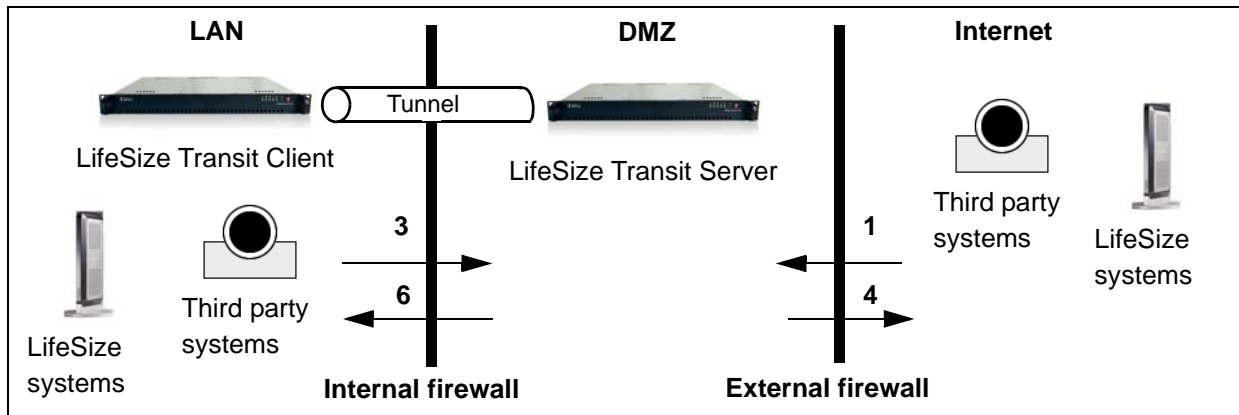
Firewall Rules for LifeSize Transit Tunneled SIP and H.323 Connections

Refer to the numbered set of rules that correspond to the numbers in the graphics.

LifeSize Transit Server Alone



LifeSize Transit Server and LifeSize Transit Client



1. External Firewall, Inbound Rules, All Cases

Allow SRC_IP=any	SRC_PORT=any	DST_IP=SignalingIP	DST_PORT=443tcp
Allow SRC_IP=any	SRC_PORT=any	DST_IP=SignalingIP	DST_PORT=444tcp
Allow SRC_IP=any	SRC_PORT=any	DST_IP=MediaIP	DST_PORT=443tcp
Allow SRC_IP=any	SRC_PORT=any	DST_IP=MediaIP	DST_PORT=444tcp
Allow SRC_IP=any	SRC_PORT=any	DST_IP=MediaIP	DST_PORT=45100-46699udp

2. Internal Firewall, Outbound Rules, LifeSize Transit Server Alone

Allow SRC_IP=any	SRC_PORT=any	DST_IP=SignalingIP	DST_PORT=443tcp
Allow SRC_IP=any	SRC_PORT=any	DST_IP=SignalingIP	DST_PORT=444tcp
Allow SRC_IP=any	SRC_PORT=any	DST_IP=MediaIP	DST_PORT=443tcp
Allow SRC_IP=any	SRC_PORT=any	DST_IP=MediaIP	DST_PORT=444tcp

3. Internal Firewall, Outbound Rules, LifeSize Transit Server and LifeSize Transit Client

Allow SRC_IP=TC_IP	SRC_PORT=any	DST_IP=SignalingIP	DST_PORT=443tcp
Allow SRC_IP=TC_IP	SRC_PORT=any	DST_IP=SignalingIP	DST_PORT=444tcp
Allow SRC_IP=TC_IP	SRC_PORT=any	DST_IP=MediaIP	DST_PORT=443tcp
Allow SRC_IP=TC_IP	SRC_PORT=any	DST_IP=MediaIP	DST_PORT=444tcp

4. External Firewall, Outbound Rules, All Cases

Allow SRC_IP=SignalingIP	SRC_PORT=443tcp	DST_IP=any	DST_PORT=any
Allow SRC_IP=SignalingIP	SRC_PORT=444tcp	DST_IP=any	DST_PORT=any
Allow SRC_IP=MediaIP	SRC_PORT=443tcp	DST_IP=any	DST_PORT=any
Allow SRC_IP=MediaIP	SRC_PORT=444tcp	DST_IP=any	DST_PORT=any
Allow SRC_IP=MediaIP	SRC_PORT=45100-46699udp	DST_IP=TC_IP	DST_PORT=any

5. Internal Firewall, Inbound Rules, LifeSize Transit Server Alone

Allow SRC_IP=SignalingIP	SRC_PORT=443tcp	DST_IP=any	DST_PORT=any
Allow SRC_IP=SignalingIP	SRC_PORT=444tcp	DST_IP=any	DST_PORT=any
Allow SRC_IP=MediaIP	SRC_PORT=443tcp	DST_IP=any	DST_PORT=any
Allow SRC_IP=MediaIP	SRC_PORT=444tcp	DST_IP=any	DST_PORT=any

6. Internal Firewall, Inbound Rules, LifeSize Transit Server and LifeSize Transit Client

Allow SRC_IP=SignalingIP	SRC_PORT=443tcp	DST_IP=TC_IP	DST_PORT=any
Allow SRC_IP=SignalingIP	SRC_PORT=444tcp	DST_IP=TC_IP	DST_PORT=any
Allow SRC_IP=MediaIP	SRC_PORT=443tcp	DST_IP=TC_IP	DST_PORT=any
Allow SRC_IP=MediaIP	SRC_PORT=444tcp	DST_IP=TC_IP	DST_PORT=any

Configuring Ports for H.323 and H.460

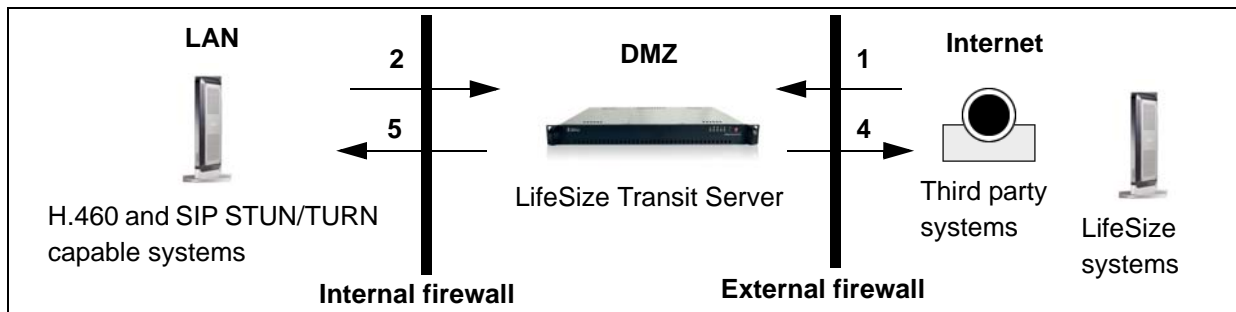
Enable the ports listed in the following table for LifeSize Transit to use H.323 and H.460. H.323 is appropriate for external systems that are not behind a firewall or NAT.

	TCP Signaling Server	UDP Signaling Server
(H.323 and H.460) H.225	1720	1719
(H.460) H.245	1722	NA
(H.323) H.245	37000-41105	NA
(H.460) RTP/Media	NA	6768, 6769
(H.323) RTP/Media	NA	45100-46699

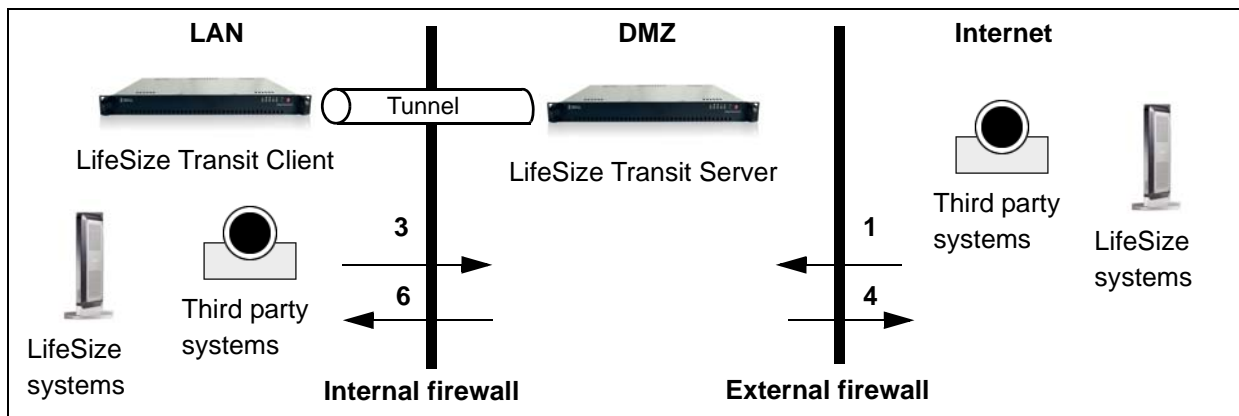
Firewall Rules for LifeSize Transit Using H.323 and H.460

Refer to the numbered set of rules that correspond to the numbers in the graphics.

LifeSize Transit Server Alone



LifeSize Transit Server and LifeSize Transit Client



1. External Firewall, Inbound Rules

Allow SRC_IP=any	SRC_PORT=any	DST_IP=SignalingIP	DST_PORT=1719udp
Allow SRC_IP=any	SRC_PORT=any	DST_IP=SignalingIP	DST_PORT=1720tcp
Allow SRC_IP=any	SRC_PORT=any	DST_IP=SignalingIP	DST_PORT=1722tcp
Allow SRC_IP=any	SRC_PORT=any	DST_IP=SignalingIP	DST_PORT=6768-6769udp
Allow SRC_IP=any	SRC_PORT=any	DST_IP=SignalingIP	DST_PORT=37000-41105tcp
Allow SRC_IP=any	SRC_PORT=any	DST_IP=SignalingIP	DST_PORT=45100-46699udp

2. Internal Firewall, Outbound Rules, LifeSize Transit Server Alone

Allow SRC_IP=any	SRC_PORT=any	DST_IP=SignalingIP	DST_PORT=1720tcp
Allow SRC_IP=any	SRC_PORT=any	DST_IP=SignalingIP	DST_PORT=1722tcp
Allow SRC_IP=any	SRC_PORT=any	DST_IP=SignalingIP	DST_PORT=1719udp
Allow SRC_IP=any	SRC_PORT=any	DST_IP=SignalingIP	DST_PORT=6768-6769udp

3. Internal Firewall, Outbound Rules, LifeSize Transit Server and LifeSize Transit Client

Allow SRC_IP=TC_IP	SRC_PORT=any	DST_IP=SignalingIP	DST_PORT=1720tcp
Allow SRC_IP=TC_IP	SRC_PORT=any	DST_IP=SignalingIP	DST_PORT=1722tcp
Allow SRC_IP=TC_IP	SRC_PORT=any	DST_IP=SignalingIP	DST_PORT=1719udp
Allow SRC_IP=TC_IP	SRC_PORT=any	DST_IP=SignalingIP	DST_PORT=6768-6769udp

4. External Firewall, Outbound Rules

Allow SRC_IP=SignalingIP	SRC_PORT=1719udp	DST_IP=any	DST_PORT=any
Allow SRC_IP=SignalingIP	SRC_PORT=6768-6769udp	DST_IP=any	DST_PORT=any
Allow SRC_IP=SignalingIP	SRC_PORT=45100-46699udp	DST_IP=any	DST_PORT=any
Allow SRC_IP=SignalingIP	SRC_PORT=anytcp	DST_IP=any	DST_PORT=anytcp

5. Internal Firewall, Inbound Rules, LifeSize Transit Server Alone

Allow SRC_IP=SignalingIP	SRC_PORT=1720tcp	DST_IP=any	DST_PORT=any
Allow SRC_IP=SignalingIP	SRC_PORT=37000-41105tcp	DST_IP=any	DST_PORT=any
Allow SRC_IP=SignalingIP	SRC_PORT=1719udp	DST_IP=any	DST_PORT=any
Allow SRC_IP=SignalingIP	SRC_PORT=6768-6769udp	DST_IP=any	DST_PORT=any

6. Internal Firewall, Inbound Rules, LifeSize Transit Server and LifeSize Transit Client

Allow SRC_IP=SignalingIP	SRC_PORT=1720tcp	DST_IP=TC_IP	DST_PORT=any
Allow SRC_IP=SignalingIP	SRC_PORT=37000-41105tcp	DST_IP=TC_IP	DST_PORT=any
Allow SRC_IP=SignalingIP	SRC_PORT=1719udp	DST_IP=TC_IP	DST_PORT=any
Allow SRC_IP=SignalingIP	SRC_PORT=6768-6769udp	DST_IP=TC_IP	DST_PORT=any

NOTE The UDP port range in the last item of each of the previous tables is based on the default setting in LifeSize Transit Server. If you change this range, be sure to reflect the new range in these firewall rules.

Configuring Ports for LifeSize Transit Server Web Administration

To allow access to the web administration interface of LifeSize Transit Server or LifeSize Transit Client, you must allow access to port 8181 on the server and client. LifeSize recommends that you provide this access only to systems behind the firewall or NAT.

Testing Your Firewall Configuration

Test the validity of your firewall configuration by using the verify deployment mode on the server and client. Refer to [Verify Deployment Mode](#) for more information.

Configuring LifeSize Systems for Firewall Traversal

Before you configure LifeSize systems to work with LifeSize Transit, ensure that you have configured your server, client, and firewall settings correctly for the deployment option that you chose. Ensure that you have created all the necessary accounts on the server for each device you intend to use. Also ensure that each LifeSize system that you intend to configure is software compatible with the LifeSize Transit. Refer to the LifeSize Transit release notes at www.lifesize.com/support for compatible software versions.

Configuring LifeSize Devices for SIP Firewall Traversal

If you are using LifeSize Transit for SIP firewall and NAT traversal, use the instructions in this section to configure LifeSize systems to use STUN, TURN, and ICE and the SIP registrar included with LifeSize Transit. If you are not using SIP in your environment, skip this section and configure your LifeSize devices to use H.460 for H.323 calls. Refer to [Configuring LifeSize Devices for H.323/H.460 Firewall Traversal](#).

The configuration instructions differ depending on whether you are using LifeSize Transit Server alone or with LifeSize Transit Client.

CAUTION Ensure that you configure preferences on your LifeSize systems in the order listed in this section. Otherwise, the LifeSize systems may register directly to the LifeSize Transit Server without using the SIP firewall traversal software included with the systems.

Configuring LifeSize Devices for SIP Tunneling with LifeSize Transit Server Only

1. From the LifeSize system, navigate to **Administrator Preferences : Network : LifeSize Transit**.
2. In **Transit Hostname**, enter the IP address of the LifeSize Transit Server signaling server. This address appears on the **Dashboard** of the LifeSize Transit Server web administration interface.
3. In the **Transit Username** and **Transit Password** fields, enter the tunnel username and password that you created for the device on LifeSize Transit Server.
4. Ensure that **Transit ICE** is set to *Enabled*.

- f. Place a SIP call from a system that has a public IP address, if available, to this system by dialing *sip_user@signaling_IP* where *sip_user* is the SIP user name of the system and *signaling_IP* is the IP address of the LifeSize Transit signaling server. You can also dial *sip_user@SIP_domain* where *SIP_domain* is the SIP domain on LifeSize Transit Server. Repeat steps c through e for this call.

Configuring LifeSize Devices for SIP with LifeSize Transit Client

1. From the LifeSize system, navigate to **Administrator Preferences : Communications : SIP**.
2. Ensure that **SIP** is set to *Enabled*.
3. Enter the **SIP Username** (without *@domain*) and **Authorization Name** that you entered in the user account for this device in LifeSize Transit Server.
4. For **Authorization Password**, enter the password that you entered when you created a user account for this device in LifeSize Transit Server.
5. Ensure that **SIP Server Type** is set to *Auto*.
6. Ensure that **SIP Registration** is set to *Through Proxy*.
7. For the **SIP Proxy** preference, choose *Enabled*.
8. In the **Proxy Hostname** preference, enter the IP address of the LifeSize Transit Client.
9. If you are using software version 4.6 or earlier, ensure that the **Proxy IP Port** is set to *5060*.
10. For **SIP Registrar**, choose *Enabled*.
11. In **Registrar Hostname**, enter the SIP domain on the LifeSize Transit Server (which might be its IP address).
12. If you are using software version 4.6 or earlier, ensure that **Registrar IP Port** is set to *5060*.
13. If you are using software version 4.6 or earlier, accept the defaults for the **UDP Signaling Port** (*5060*), **TCP Signaling** (*Disabled*), and **TLS Signaling** (*Disabled*). Otherwise ensure that **SIP Signaling** is set to *Auto* and **UDP Signaling Port** is set to *5060*.
14. Select the **Register** button and press **OK**. The registration is successful if **Registrar Status** above the **Register** button changes to **Registered**.
15. Test the configuration.
 - a. From LifeSize Transit Server, navigate to **Status : Clients : SIP**.
 - b. Ensure that the SIP registration for the system appears on this page.
 - c. From LifeSize Transit Client, navigate to **Status : Users**.
 - d. Ensure that the SIP registration for the system appears on this page.
 - e. Place an outbound call from the system to another video communications system that has a public IP address by dialing *sip:IP_address* of the SIP user you are calling
 - f. From LifeSize Transit Server, navigate to **Status : Calls**.
 - g. Ensure that the call appears in **Active calls**.
 - h. From LifeSize Transit Client, navigate to **Status : Calls**.
 - i. Ensure that the call appears in the **Calls** section.

- j. Place an inbound call from a system that has a public IP address, if available, to this system by dialing *sip_user@signaling_IP* where *sip_user* is the SIP user name of the system you are calling and *signaling_IP* is the IP address of the LifeSize Transit signaling server. Repeat steps f through i for this call.

Configuring LifeSize Bridge for SIP with LifeSize Transit Client

1. In the LifeSize Bridge Utility, navigate to **Preferences : SIP**.
2. Enter the **SIP Username** and **Authorization Name** that you entered in the user account for LifeSize Bridge in LifeSize Transit Server.
3. For **Authorization Password**, enter the password that you entered when you created the user account for LifeSize Bridge in LifeSize Transit Server.
4. Ensure that **Enable the SIP registrar** is selected.
5. In **Registrar Hostname**, enter the SIP domain on the LifeSize Transit Server (which might be its IP address).
6. Ensure that **Registrar Port** is set to *5060*.
7. Ensure that **Enable SIP proxy server** is selected.
8. In the **Proxy Hostname** preference, enter the IP address of the LifeSize Transit Client.
9. Ensure that **Proxy Port** is set to *5060*.
10. Ensure that **UDP Signaling Port** is set to *5060*.
11. Click **Save**.
12. Ensure that **Registrar Status** changes to *Registered*.

Configuring a Codian MCU for SIP with LifeSize Transit Client

Use the LifeSize Transit Server IP address as the SIP registrar domain and use the LifeSize Transit Client IP address as the SIP proxy address.

1. Access the administrative or web administration interface of the Codian MCU that you wish to configure.
2. Configure the Codian MCU to use the LifeSize Transit Client as the SIP proxy and the LifeSize Transit Server as the SIP registrar in the SIP settings page.
 - a. Select **Allow conference registration** for **SIP registration settings**.
 - b. For **SIP registrar domain**, enter the LifeSize Transit Server IP address.
 - c. Select **Standard SIP** for **SIP registrar type**.
 - d. Enter the username and password you created for the MCU in step 1.
 - e. For **SIP proxy address**, enter the LifeSize Transit Client IP address.

Configuring LifeSize Bridge in the DMZ for SIP

You can deploy LifeSize Bridge in the DMZ as an unregistered device.

All devices, whether in the LAN registered to LifeSize Transit Server through LifeSize Transit Client, or in the internet, registered or not to the SIP registrar in LifeSize Transit Server, must dial `<conference ID@LifeSize Bridge IP address>`.

Configuring LifeSize Devices for H.323/H.460 Firewall Traversal

LifeSize systems support the H.460 protocol for firewall and NAT traversal of H.323 calls. By default, H.460 is disabled on LifeSize systems. If you are using LifeSize Transit for H.323 calls, use the instructions in this section to configure LifeSize systems for firewall traversal of H.323 calls with LifeSize Transit. The configuration instructions differ depending on whether you are using LifeSize Transit Server alone or with LifeSize Transit Client.

Configuring LifeSize Devices for H.323 traversal without LifeSize Transit Client

1. From the LifeSize system, navigate to **Administrator Preferences : Communications : H.323**.
2. Configure the preferences on this page as described in the H.323 settings section of your LifeSize video communications systems administrator guide with the following exceptions:
 - a. Choose *Manual* for **Gatekeeper Mode**.
 - b. For the **Gatekeeper IP Address 1**, enter the IP address and port number of the LifeSize Transit signaling server.
 - c. Ensure that the **Gatekeeper Port 1** preference is set to *1719* (the default).
 - d. If your gatekeeper requires authentication, enable **Gatekeeper Authentication** and enter the authentication username and password.
 - e. If you are using software v4.8 or later, you can enable either **H.460** or **H.323 Tunneling**. Otherwise enable **H.460**.
 - f. Navigate to **Register** and press **OK**.

NOTE If you enable H.460 and specify the IP address and port number of a secondary gatekeeper in **Gatekeeper IP Address 2** and **Gatekeeper Port 2**, the system ignores the secondary gatekeeper. The system also ignores preferences in **Administrator Preferences : Network : NAT**.

3. Test the configuration.
 - a. From LifeSize Transit Server, navigate to **Status : Clients**.
 - b. Ensure that the **User ID** appears.
 - c. Place an outbound call from the device to another video communications system that has a public IP address by dialing the public IP address.
 - d. From LifeSize Transit Server, navigate to **Status : Calls**.

- e. Ensure that the call appears in the **Active calls**.
- f. Place an inbound call from a system that has a public IP address, if available, to the system by dialing `<signaling_server_IP>##<H.323_Extension>` where `<signaling_server_IP>` is the IP address of the LifeSize Transit signaling server and `<H.323_Extension>` is the H.323 extension of the system you are calling.
- g. Repeat steps d and e for this call.

Configuring LifeSize Devices for H.323 with LifeSize Transit Client and a Private Gatekeeper

1. From LifeSize video communications system, navigate to **Administrator Preferences : Communications : H.323**.
2. Configure the preferences on this page as described in the H.323 settings section of your LifeSize video communications systems administrator guide with the following exceptions:
 - a. Add the route prefix that you created in LifeSize Transit Server (the **H.323 prefix** field) to the beginning of the value in the **H.323 Extension** preference. For example, if the route prefix is 22 and the H.323 extension of the video communications system is 1234, then the value of the **H.323 Extension** preference is 221234.
 - b. Choose *Manual* for **Gatekeeper Mode**.
 - c. For the **Gatekeeper IP Address 1** and **Gatekeeper Port 1** preferences, enter the address of the gatekeeper in the private LAN.
 - d. if your gatekeeper requires authentication, enable **Gatekeeper Authentication** and enter the authentication username and password.
 - e. Ensure that **H.460** and **H.323 Tunneling** (v4.8 and later) are *Disabled* (the default).
4. Navigate to **Register** and press **OK**.
5. Test the configuration by placing an outbound call. The device can call another device with a public IP address that is not registered to the internal gatekeeper using the dial string `<outbound_prefix>##<public_IP_address>` or `<outbound_prefix><public_IP_address>`. Both dialing patterns are supported.

Configuring LifeSize Devices for H.323 with LifeSize Transit Client and Built-In Gatekeeper

1. From the LifeSize device, navigate to **Administrator Preferences : Communications : H.323**.
2. Configure the preferences on this page as described in the H.323 settings section of your LifeSize video communications systems administrator guide with the following exceptions:
 - a. Choose *Manual* for the **Gatekeeper Mode** preference.
 - b. For the **Gatekeeper IP Address 1** preference, enter the IP address of LifeSize Transit Client.
 - c. For the **Gatekeeper Port 1** preference, ensure that it is set to 1719 (the default).
 - d. Ensure that **H.460** and **H.323 Tunneling** (v4.8 and later) are *Disabled* (the default).
3. Navigate to **Register** and press **OK**.

4. Test the configuration.
 - a. From LifeSize Transit Server, navigate to **Status : Clients : H.323**.
 - b. Ensure that the H.323 registration for the system appears on this page and that *H.460.18* appears in the **Transport** column.
 - c. From LifeSize Transit Client, navigate to **Status : Users**.
 - d. Ensure that the H.323 registration for the system appears on this page and *H.460* appears in the **Mode** column.
 - e. Place an outbound call from the system to another video conference system that has a public IP address by dialing the IP address.
 - f. From LifeSize Transit Server, navigate to **Status : Calls**.
 - g. Ensure that the call appears in **Active Calls**.
 - h. From LifeSize Transit Client, navigate to **Status : Calls**.
 - i. Ensure that the call appears and *H.460_client* appears in the **Media method** column.
 - j. Place an inbound call to the system from a video conference system with a public IP address by dialing `<signaling_server_IP>##<H.323_Extension>` where `<signaling_server_IP>` is the IP address of the LifeSize Transit signaling server and `<H.323_Extension>` is the H.323 Extension of the system you are calling.
 - k. Repeat steps f through i.

Configuring LifeSize Bridge In the LAN for H.323 with LifeSize Transit Client In the LAN

If you are using a gatekeeper in the private LAN, register LifeSize Bridge to the gatekeeper in the LifeSize Bridge Utility.

1. From the **Preference** tab, click **H.323**.
2. Ensure **Enable H.323** is selected.
3. Configure the **Gatekeeper** section:
 - a. For **H.323 Name**, enter the H.323 ID, if required by your gatekeeper.
 - b. For **H.323 Extension**, enter your H.323 extension, if required by your gatekeeper.
 - c. Enter the **Gatekeeper ID**, if required by your gatekeeper.
 - d. Set **Gatekeeper Mode** to *Manual*.
 - e. For **Gatekeeper Hostname**, enter the IP address of the gatekeeper.
 - f. Enter the **Gatekeeper Port**. The default is *1719*.
4. Click **Save**.

If there is no standalone gatekeeper, register LifeSize Bridge to the LifeSize Transit Client in the LifeSize Bridge Utility.

1. From the **Preference** tab, click **H.323**.
2. Ensure **Enable H.323** is selected.

3. Configure the **Gatekeeper** section:
 - a. For **H.323 Name**, enter the H.323 ID if required by your gatekeeper.
 - b. For **H.323 Extension**, enter your H.323 extension, if required by your gatekeeper.
 - c. Enter the **Gatekeeper ID**, if required by your gatekeeper.
 - d. Set **Gatekeeper Mode** to *Manual*.
 - e. For **Gatekeeper Hostname**, enter the IP address of the LifeSize Transit Client.
 - f. Enter the **Gatekeeper Port**. The default is 1719.
4. Click **Save**.

Configuring LifeSize Bridge in the DMZ for H.323

You can deploy LifeSize Bridge in the DMZ with a public address, unregistered to the gatekeeper in LifeSize Transit Server.

No Gatekeeper

Devices in the LAN registered to LifeSize Transit Server with H.460 enabled dial *<LifeSize Bridge IP address##conference ID>*. Devices in the LAN registered to LifeSize Transit Client dial *<LifeSize Bridge IP address##conference ID>*. Public LifeSize devices dial *<LifeSize Bridge IP address##conference ID>*.

Gatekeeper in the LAN

Devices in the LAN registered to the gatekeeper dial *<outbound prefix##LifeSize Bridge IP address##conference ID>*.

All public devices, registered to the gatekeeper or not, dial *<LifeSize Bridge IP address##conference ID>*.

External Gatekeeper

Devices in the LAN registered to the gatekeeper in DMZ through the LifeSize Transit Server dial *<LifeSize Bridge IP address##conference ID>*.

All public devices registered to the LifeSize Transit Server dial *<LifeSize Bridge IP address##conference ID>*.

All public devices unregistered to LifeSize Transit Server dial *<LifeSize Bridge IP address##conference ID>* if the external firewall is configured to allow traffic to LifeSize Bridge directly.

Configuring LifeSize Desktop for use with LifeSize Transit

If you are using LifeSize Desktop to place calls to other LifeSize devices or LifeSize Desktop installations in your organization through LifeSize Transit, you must configure LifeSize Desktop to use LifeSize Transit. For configuration instructions, refer to the technical note *Configuring LifeSize Desktop for Use with LifeSize Transit*. This technical note is available at lifesize.com/support.

Maintaining LifeSize Transit

To perform any of the maintenance operations available from the **Maintenance** tab on LifeSize Transit Server and LifeSize Transit Client, you must first enter maintenance mode.

Maintenance mode puts the device into a suspended state and prevents new calls from connecting. The **Force maintenance mode** option also disconnects all current calls in addition to entering maintenance mode.

Verify Deployment Mode

Use the **Verify deployment mode** options on the server and client to test whether your firewall configuration is properly configured.

1. From your LifeSize Transit Server, navigate to **Maintenance : Maintenance Mode** and click **Enter maintenance mode**.
2. Click **Verify deployment mode**.
3. From your LifeSize Transit Client, navigate to **Maintenance : Maintenance Mode** and click **Enter maintenance mode**.
4. Click **Verify deployment mode**.

NOTE The server must be in verify deployment mode before you enter verify deployment mode on the client, otherwise you will receive an error stating you have lost the TCP connection.

The IP address of the server to which the client is tunneled and the client's tunnel account username appears. If these are incorrect, you must reconfigure the clients tunnel account on the server. Refer to [User and Tunnel Accounts](#).

5. Click **Begin verification**. It may take several minutes the process to complete. When the process completes, a page reports the success or failure of the overall deployment and of its constituent parts. Descriptions and error messages provide help in troubleshooting configuration failures.
6. Click **Export** to create a copy of the verification report that you can download.
7. Exit maintenance mode on both the server and client.

Upgrading Software

Before upgrading LifeSize Transit software, note the serial number of the device that you wish to upgrade. The serial number is visible on the **Dashboard** of the client and server web administration interfaces.

Follow these steps to upgrade the software for LifeSize Transit:

1. Obtain the upgrade software package from the Support page of lifesize.com/support. Click the **Download Software** link and follow the instructions.
2. From your server or client, navigate to **Maintenance : Maintenance Mode** and click **Enter maintenance mode**.
3. Click **Software Update**.
4. Browse for the upgrade file that you downloaded in step 1.
5. Click **Update software**.

NOTE This may take several minutes; do not disrupt the upgrade process.

A system upgrade status message appears when the upgrade is complete.

6. Exit maintenance mode.

Database Backup and Restore

To back up the server database, follow these steps:

1. From your server, navigate to **Maintenance : Maintenance Mode** and click **Enter**.
2. Click **System**.
3. Click **Back up**.
4. Click **Continue**.
5. Click the name of the backup file to download it.
6. Exit maintenance mode.

To restore the server database, follow these steps:

1. From your server, navigate to **Maintenance : Maintenance Mode** and click **Enter** maintenance mode.
2. Click **System**.
3. Click **Restore**.
4. Browse for the backup file, and click **Continue**. The server reboots with the database restored.

Reset and Reboot

While in maintenance mode you can also reset the server and reboot the client or server on the **Maintenance mode : System** page.

Resetting the server returns it to factory settings after rebooting.

Rebooting the server or client turns the server or client off and on again.

Troubleshooting and Diagnostics

This section describes the most common issues that you may encounter with a LifeSize Transit deployment.

Previous Version of the User Interface Persists after Upgrade

Clear the browser cache to load the new user interface.

User Interface Locked after Certificate File Upload or Password Change

If you cannot access the administrator account after changing the password, or uploading a new certificate file, connect a console to the serial port of the device with a null modem cable to reset the password or certificate to factory defaults.

Invalid DNS Configuration

LifeSize Transit Server fails to function properly if it is not configured to use a valid, available DNS server. Ensure that you have properly configured the DNS settings on the server and that the DNS server is available.

Call Status Page

In LifeSize Transit Server, navigate to **Status : Calls : All calls** to see active and closed calls. Click **Closed calls** to view ended and failed calls. Use the **Search** box to find specific calls. Use the **Details** field in the call to troubleshoot a failed call.

You can view the following details about a call:

Field	Description
Caller ID	Unique call identifier for the call that is useful when matching records from multiple systems.
Caller IP address	Public address of the device. It may also be the address of a remote SIP server/gatekeeper if it hides the internal addresses.
Recipient ID	Location of the called party.
Recipient IP address	Actual IP address the called device. This may also be the address of a remote SIP server/gatekeeper.

Field	Description
Duration	Length of the call.
Active	Whether the call is ongoing.
Details	Details of the call. Refer to Events for a list of reasons a call may fail.

Events

To configure events, navigate to **Configuration : Events**.

SMTP server is the outgoing SMTP server address.

Username is the username to use to authenticate at the SMTP server.

Password is the password to use to authenticate at the SMTP server.

Recipients is mail addresses of the recipients separated by a comma.

Trap receiver address is the address of the trap receiver.

Use the **Status : Events** page in the web administration interface of LifeSize Transit Server to view events on the signaling server.

Field	Description
#	Event number.
Event name	Logical name of the event.
Severity	Severity of the event (corresponds to log level for each event). Refer to Log Files .
Info	Textual explanation of the event.
Time raised	Timestamp when the event was raised.
Customer ID	ID of the customer.
Key	Unique ID of the event.
Clear	Clears the event.

Diagnostic Files and Utilities

Use these features only if directed to do so by a LifeSize Technical Services representative.

Log Files

Both client and server allow you to log events to a file for later download. Navigate to **Status : Logs** for controls to set the LifeSize Transit and system log levels and indicate the system log host. LifeSize Technical Services may instruct you to download and send these files to LifeSize for analysis if needed.

Diagnostic File

You can download a file that contains diagnostic information by clicking the **Download diagnostic file** button in **Status: Logs** on the server. A dialog box appears so that you can download the file. Create this file only when instructed to do so by a LifeSize Technical Services representative.

Enabling Remote Diagnostic Access

The **SSH access enabled** option in **Maintenance : System** is only available after you enter maintenance mode. It enables remote access to your installation for troubleshooting purposes with a LifeSize Technical Services representative. Refer to your LifeSize Technical Services representative for instructions.

Downloading Call Detail Records

You can also download call detail records (CDRs) from the **Status : Calls** page of the LifeSize Transit Server web administration interface by clicking **Download CDR**. This is a text file that contains information available in the **Closed calls** section of the **Status : Calls** page.

Copyright Notice

©2006–2011 Logitech, and its licensors. All rights reserved.

LifeSize Communications, a division of Logitech, has made every effort to ensure that the information contained in this document is accurate and reliable, but assumes no responsibility for errors or omissions. Information in this document is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless noted. This document contains copyrighted and proprietary information which is protected by United States copyright laws and international treaty provisions. No part of the document may be reproduced or transmitted, in any form or by any means, electronic or mechanical, for any purpose, without the express written permission from LifeSize Communications.

Trademark Acknowledgments

LifeSize, the LifeSize logo and other LifeSize marks, are registered trademarks or trademarks of Logitech. All other trademarks are the property of their respective owners.

Patent Notice

For patents covering LifeSize® products, refer to lifesize.com/support/legal.

Contacting Technical Services

LifeSize Communications welcomes your comments regarding our products and services. If you have feedback about this or any LifeSize product, please send it to feedback@lifesize.com. Refer to lifesize.com/support for additional ways to contact LifeSize Technical Services.