LifeSize® UVC Transit™ Deployment Guide

November 2013

LifeSize UVC Transit Server
LifeSize UVC Transit Client

LifeSize UVC Transit

LifeSize UVC Transit is a unified set of firewall and Network Address Translation (NAT) traversal technologies that enable session and media traversal for the H.323 and SIP protocols.

Planning	Describes how LifeSize UVC Transit functions in basic deployments.	Planning for LifeSize UVC Transit
Deploying	Describes deploying LifeSize UVC Transit.	Deploying LifeSize UVC Transit
Configuring LifeSize Systems	Describes how to manually configure LifeSize systems for LifeSize UVC Transit. Alternatively, you can use the LifeSize UVC Platform auto configuration feature. Refer to the *LifeSize UVC Platform Deployment Guide* to learn more.	Configuring LifeSize Systems for Firewall Traversal
Maintaining	Learn how to back up and restore the system and perform troubleshooting.	Maintaining LifeSize UVC Transit

NOTE If you are using LifeSize UVC Access as the gatekeeper for your deployment, refer also to the deployment guide for that application.

Related documentation is available from lifesize.com/support.

Section 1: Planning for LifeSize UVC Transit

LifeSize UVC Transit Server is a firewall traversal solution for H.323 and SIP and includes:

- A signaling server that handles call setup, operation, and maintenance services.
- A media server that is optimized for relaying the actual voice, video, and presentation data.

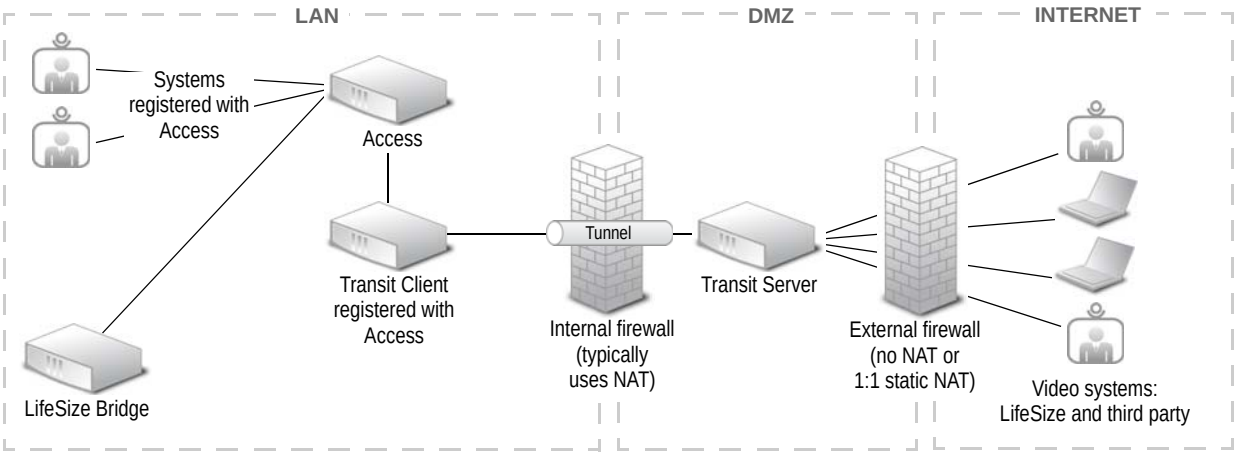
When you enable LifeSize UVC Transit Server, you configure each of these servers with its own static, public IP address. The IP addresses can use 1:1 static NAT or no NAT.

NOTE LifeSize UVC Transit Server always resides in the DMZ in your network.

LifeSize UVC Transit Client is a standalone multi-user traversal client that can serve as a SIP and H.323 proxy for calls with LifeSize UVC Transit Server. LifeSize recommends deploying both LifeSize UVC Transit Server and LifeSize UVC Transit Client if your network includes the following:

- LifeSize and third party video systems and MCUs (such as LifeSize Bridge) that do not support H.460 or SIP traversal and that reside behind the firewall in your private network.
- An H.323 gatekeeper that resides behind the firewall in your private network. In this case, LifeSize UVC Transit Client serves as an H.323 proxy for calls with LifeSize UVC Transit Server.

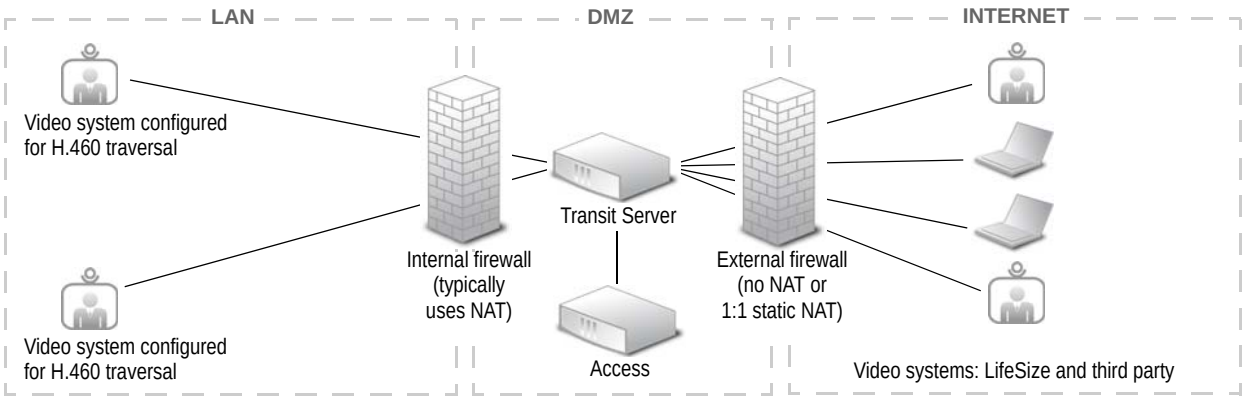
Deployment Scenario: LifeSize UVC Transit Server in the DMZ and LifeSize UVC Transit Client and LifeSize UVC Access in the LAN



If the external firewall uses 1:1 static NAT, callers must use the public IP address of the signaling server to place calls to your video systems.

Deployment Scenario: LifeSize UVC Transit Server and LifeSize UVC Access (as an External Gatekeeper) in the DMZ

You can use LifeSize UVC Transit Server with LifeSize UVC Access serving as an external gatekeeper only if you are using video systems that support H.460 traversal behind the firewall in your private network.



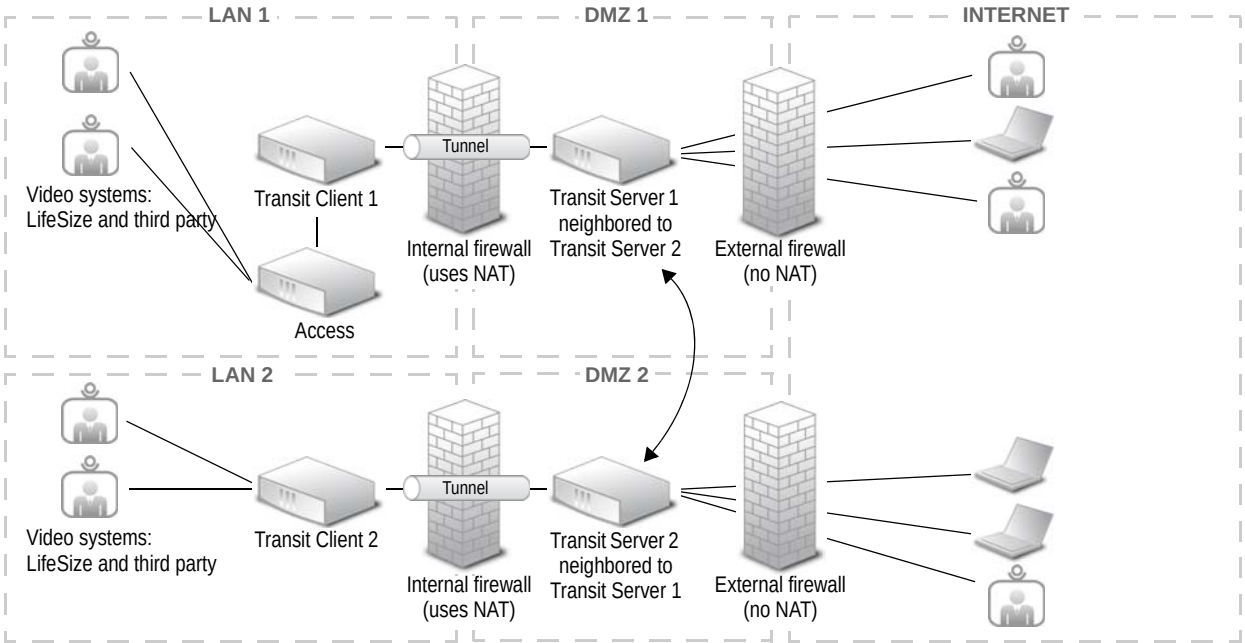
If the external firewall uses 1:1 static NAT, callers must use the public IP address of the signaling server to place calls to your video systems.

Deployment Scenarios: Multiple LANs

A single company may employ more than one deployment scenario to manage high-volume traffic or a workforce that is geographically dispersed.

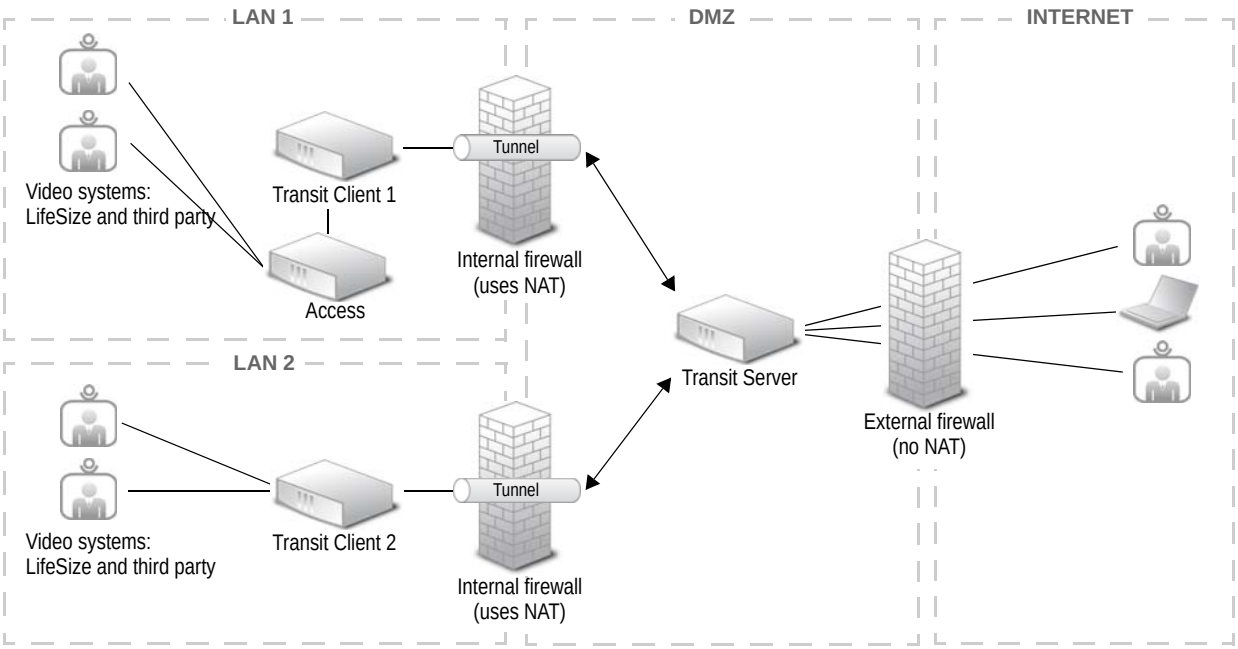
Neighboring LifeSize UVC Transit

The following configuration allows LifeSize or third party video systems in LAN 1 to communicate with other LifeSize or third party video systems in LAN 2.



LANs in Multiple Geographies

The following configuration allows LifeSize or third party video systems in different LANs in the same company to communicate with one another.



Using STUN, TURN, and ICE in Firewall and NAT Traversal

Firewall and NAT traversal for SIP and H.323 calls rely on a suite of protocols: STUN, TURN, and ICE. LifeSize UVC Transit uses ICE to determine the most efficient traversal method in the following order:

1. STUN
2. TURN
3. The LifeSize proprietary tunneling mode

   In tunneled mode, LifeSize systems or the LifeSize UVC Transit Client establishes a tunneled connection to LifeSize UVC 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 UVC Transit probes the network to determine what traversal methods are possible. When LifeSize UVC Transit Client uses SIP to connect from NAT, LifeSize UVC Transit Server notes the public address instead of what is reported from LifeSize UVC Transit Client. Based on the reported LifeSize UVC Transit Client capabilities, LifeSize UVC Transit Server decides whether relay is needed when LifeSize UVC Transit Client participates in a call. LifeSize UVC Transit Server also ensures that the signaling channel is kept open while LifeSize UVC Transit Client is registered.

Protocol	Description
STUN	Enables LifeSize systems behind your firewall to discover the public IP address and port mappings that they use to communicate with other devices during a call and to instruct the other devices where to send media. LifeSize UVC Transit Server includes a STUN server that uses the signaling and media IP addresses.
TURN	An extension of STUN that allocates a public IP address and port on a server and uses this allocation to relay media between the devices in a call. LifeSize UVC Transit Server includes a TURN server. These relay sessions consume resources on the servers and must be authenticated. The credentials in the tunnel account you create in LifeSize UVC Transit Server for each system are used for this purpose.
ICE	Determines the best method for traversal based on a list of transport addresses—a combination of an IP address and UDP port—that each system in a call gathers through STUN, TURN, and from physical or logical network interfaces. ICE is enabled on LifeSize video systems by default when you configure the devices to use LifeSize Transit. To ensure ICE uses direct communication with remote devices, configure the firewall rules to allow UDP connections from the LAN toward any remote host, and accept return traffic on the same ports.

Section 2: Deploying LifeSize UVC Transit

Deploying LifeSize UVC Transit includes the following tasks:

Complete installation and initial configuration.	Initial Configuration
Update certificates.	Updating Certificates for LifeSize UVC Transit Server
Check for software updates and upgrade to the latest versions to ensure they are compatible.	*LifeSize UVC Platform Deployment Guide*
Configure firewall settings to enable communication between the clients in your private network and LifeSize UVC Transit Server in the DMZ.	Configuring Firewalls
Complete the LifeSize UVC Transit configuration wizards.	Using the LifeSize UVC Transit Configuration Wizards
Optionally, configure neighboring gatekeepers or Annex O dialing (username@domain).	Configuring Additional Options
If you are placing or receiving SIP calls with your video systems, create SIP domains and DNS SRV RR records.	Setting Up a SIP DNS SRV Record
Create a user account in LifeSize UVC Transit Server for each video system and MCU in your private network.	Creating User Accounts
Optionally, add static routes to other domains and networks.	Creating Static Routes
Optionally, configure domain and network filtering.	SIP Domain Filtering Creating a Network Filter
Configure the video devices in your private network to use LifeSize UVC Transit.	Configuring LifeSize Systems for Firewall Traversal

Initial Configuration

1. Install the LifeSize UVC Platform hardware or virtual machine according to the instructions in the *LifeSize UVC Platform Installation Guide*.
2. Log in to the LifeSize UVC Platform from a browser and activate a license for LifeSize UVC Transit. Refer to the *LifeSize UVC Platform Deployment Guide*.

> NOTE If your deployment includes both LifeSize UVC Transit Client and LifeSize UVC Transit Server, you must enable them on separate instances of LifeSize UVC Platform. LifeSize UVC Transit Server must reside in the DMZ.

3. Complete the initial configuration for LifeSize UVC Transit. Read more at Enabling LifeSize UVC Transit.

4. *Optional*: Create DNS entries.

   For LifeSize UVC Transit Server to be publicly accessible, the signaling server needs a public address that is registered in the global DNS service. If your organization does not manage its domain names, ask your Internet Service Provider (ISP) to do so. The DNS entries chosen for the servers should match the name in the SSL certificate. For example:

   - `signal.example.com` for the signaling server

5. Ensure that you can access LifeSize UVC Transit from your private network. You must allow access to TCP port 8181. LifeSize recommends that you restrict this access to systems in the private LAN.

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

   `https://`*`lifesize_UVC_transit_server_IP_address`*`:8181`

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

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

   `https://`*`lifesize_UVC_transit_client_IP_address`*`:8181`

6. Log in to LifeSize UVC Transit Server or LifeSize UVC Transit Client. The default administrator credentials for LifeSize UVC Platform and all enabled applications are:

   Username: *administrator*

   Password: *admin123*

NOTE You can also create an administrator account with separate credentials for logging in to LifeSize UVC Transit. Refer to step 4 of Enabling LifeSize UVC Transit.

Enabling LifeSize UVC Transit

1. Open a browser and log in to LifeSize UVC Platform:

   Username: *administrator*

   Password: *admin123*

2. Ensure sufficient IP addresses are available for configuring LifeSize UVC Transit.

   LifeSize UVC Transit Server requires two static, public IP addresses, and LifeSize UVC Transit Client requires one static IP address.

   If your configuration uses static NAT, ensure sufficient static, private IP addresses are available. Enable LifeSize UVC Transit by assigning the IP addresses from this pool.

   a. Navigate to **System Settings : IP Addresses – Edit**.

   b. Click **Add address**.

c. Enter the new IP address.

NOTE Press **Tab** to enter the remaining values, or enter each remaining value. Ensure that you review the values entered by the server.

d. Optionally, enter an IPv6 address.

e. Click **Apply Changes**.

3. Enable LifeSize UVC Transit Server or LifeSize UVC Transit Client. Ensure port 8180 is open to your LifeSize UVC Platform.

   a. Navigate to **Operations and Maintenance : Applications enabled – Edit**.

   b. In **Enable new application**, select **Transit Server** or **Transit Client**.

   c. Select the IP address. For LifeSize UVC Transit Server, select two IP addresses: one for signaling and one for media.

   d. Click **Enable Application**.

   NOTE Callers outside of your network must use the public IP address of the signaling server to place calls to your video communications systems. Configure the public IP address (of the signaling server and the media server) for static NAT from LifeSize UVC Transit Server in **Configuration : Server**. You configure the private IP address for static NAT when you enable the application through LifeSize UVC Platform by using this procedure.

4. *Optional*: Create administrator accounts for LifeSize UVC Transit Server and LifeSize UVC Transit Client.

   a. Navigate to **User Management : Users – Add**.

   b. Enter a username and password.

   c. Click **Save**.

   d. In **Transit Server** (or **Transit Client**) **Permissions**, select **Transit Server** (or **Transit Client**) **Administrator**.

   e. Click **Save**.

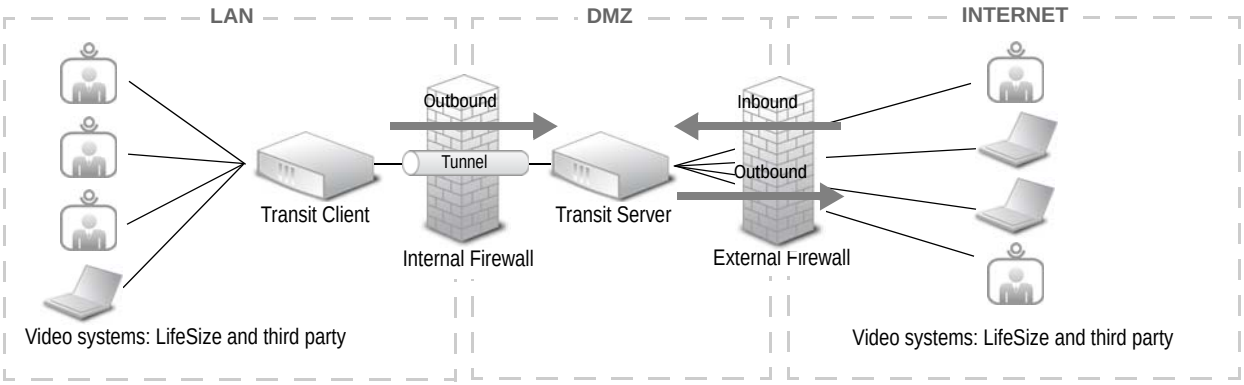
Updating Certificates for LifeSize UVC Transit Server

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

- To use SIP/TLS, replace the TLS certificate in **Configuration : SIP : Certificates**. 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 replace the file. If no SIP/TLS certificate has been installed, the tunnel certificates are used for SIP/TLS.
- To use secure tunneling on port 443, replace the trusted root certificate in **Configuration : Tunnel Certificates**. Upload a tunnel certificate that matches the hostname of the server. Apply to a certificate authority for a server certificate and then replace the file.

Configuring Firewalls

If your video systems reside in the LAN, you typically implement two firewalls: the internal firewall that separates the LAN from the DMZ, and the external firewall that separates the DMZ from the Internet. The inbound direction is always from the Internet towards the private network. The outbound direction is always from the private network toward the Internet.



The firewall rules included in this guide assume that the firewall is configured to allow return traffic on any connection. LifeSize recommends disabling any H.323 and SIP application layer gateway functions, because these can cause problems.

The ports and port ranges in these rules reflect the default ports for LifeSize UVC Transit. The rules also assume that LifeSize UVC Transit Server is allowed to open outbound TCP connections to the public Internet from any source port to any destination port. To ensure that ICE uses efficient, direct communication to remote devices, configure the firewall rules to allow UDP connections from the LAN to any remote host, and to accept return traffic on the same ports.

Access to the LifeSize UVC Transit interface requires opening port 8181 on the server and client. LifeSize recommends that you provide this access only to systems in the private LAN.

Firewall Rules

Open the firewall for LifeSize UVC Transit Server and LifeSize UVC Transit Client to access the following destination ports and addresses:

DNS (mandatory)	<*dns-server-address*>:53
NTP	<*ntp-server-address*>:123
SNMP	<*control-server-address*>:162
SYSLOG	<*syslog -server-address*>:514

These rules are not necessary for NAT or firewall configurations that do not apply specific rules to block IP addresses or ports.

The rules assume ClientIP is the source of communication to the LifeSize UVC Transit Server. ClientIP can be a LifeSize UVC Transit Client or an IP-range of video communication devices connecting directly to the LifeSize UVC Transit Server. SignalIP and MediaIP refer to the signaling server and media server, respectively, on LifeSize UVC Transit Server.

NOTE When IPv6 addresses are configured for LifeSize Transit, SignalingIP and MediaIP indicate both the IPv4 and IPv6 addresses.

Internal Firewall Rules

Internal firewall rules allow communication between devices in the internal network using NAT and the LifeSize UVC Transit Server in the DMZ. These rules apply only to outbound traffic from the LAN to the DMZ and assumes return traffic is allowed.

H.460

The following rules are sufficient for H.323 devices with H.460 enabled to communicate with the LifeSize UVC Transit Server.

Source IP Addresses	Source Ports	Destination IP Addresses	Destination Ports
ClientIP	any	SignalingIP	1720tcp 1722tcp 1719udp 6768-6769udp

Tunneling Only

The following rules apply for communication between LifeSize UVC Transit Client or LifeSize video communications systems and a LifeSize UVC Transit Server with tunneling enabled. These rules apply to both SIP devices and H.323 devices with H.460 disabled.

Source IP Addresses	Source Ports	Destination IP Addresses	Destination Ports
ClientIP	any	SignalingIP	443tcp 444tcp
ClientIP	any	MediaIP	443tcp 444tcp

Tunneling with UDP Media

LifeSize recommends enabling UDP for media traversal unless other important considerations make this impossible. These rules apply to both SIP devices and H.323 devices with H.460 disabled. To enable UDP media from tunneling clients, include the following rules in addition to the rules listed in Tunneling Only .

Source IP Addresses	Source Ports	Destination IP Addresses	Destination Ports
ClientIP	any	SignalingIP	3478udp 34501udp
ClientIP	any	MediaIP	45100-46699udp 3478udp 34501udp

SIP

These rules apply to SIP devices connecting directly to LifeSize UVC Transit Server. Apply these rules in addition to the rules in Tunneling with UDP Media.

Source IP Addresses	Source Ports	Destination IP Addresses	Destination Ports
ClientIP	any	SignalingIP	5060tcp 5060udp 5061tcp 3560tcp 3560udp
ClientIP	any	MediaIP	3560tcp 3560udp

For direct media toward external hosts, neither the internal nor external firewall should perform IP address or port blocking for UDP connections.

External Firewall Rules

The LifeSize UVC Transit Server and the external public systems are peers and connections can be initiated in either direction. Therefore, this section contains both inbound and outbound rules.

Inbound Rules for Public External H.323 Systems

Source IP Addresses	Source Ports	Destination IP Addresses	Destination Ports
any	any	SignalingIP	1719udp 1720tcp 37000-41105tcp 45100-46699udp
any	any	MediaIP	45100-46699udp

Outbound Rules for Public External H.323 Systems

Source IP Addresses	Source Ports	Destination IP Addresses	Destination Ports
SignalingIP	1719udp 45100-46699udp	any	any
SignalingIP	anytcp	any	any
MediaIP	45100-46699udp	any	any

Inbound Rules for Public External SIP Systems

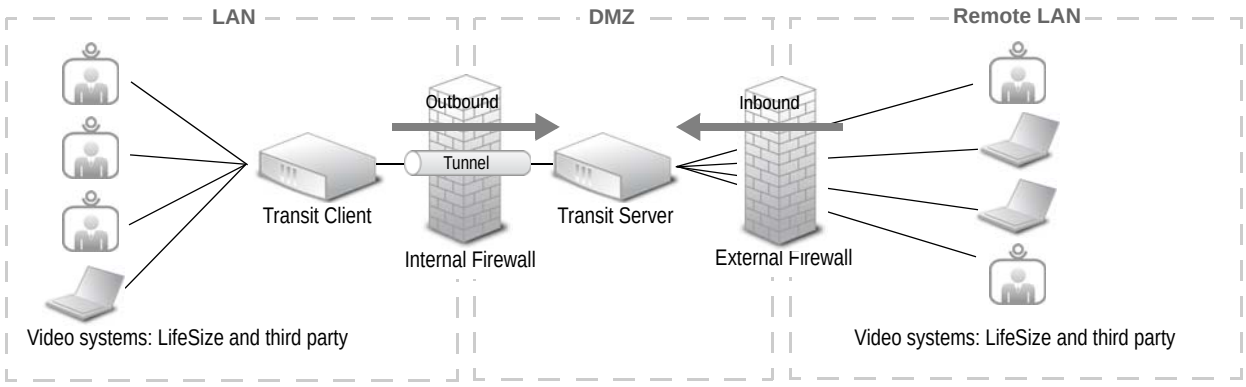
Source IP Addresses	Source Ports	Destination IP Addresses	Destination Ports
any	any	SignalingIP	5060udp 5060tcp 5061tcp
any	any	MediaIP	45100-46699udp 45100-46699tcp

Outbound Rules for Public External SIP Systems

Source IP Addresses	Source Ports	Destination IP Addresses	Destination Ports
SignalingIP	5060udp	any	anyudp
SignalingIP	anytcp	any	anytcp
MediaIP	45100-46699udp	any	any

Remote LANs

If video communications systems are located in remote LANs outside the external firewall, and they are not using a VPN, they are clients to the LifeSize UVC Transit Server, and you must also apply the rules from the internal firewall section to the inbound rules of the external firewall.

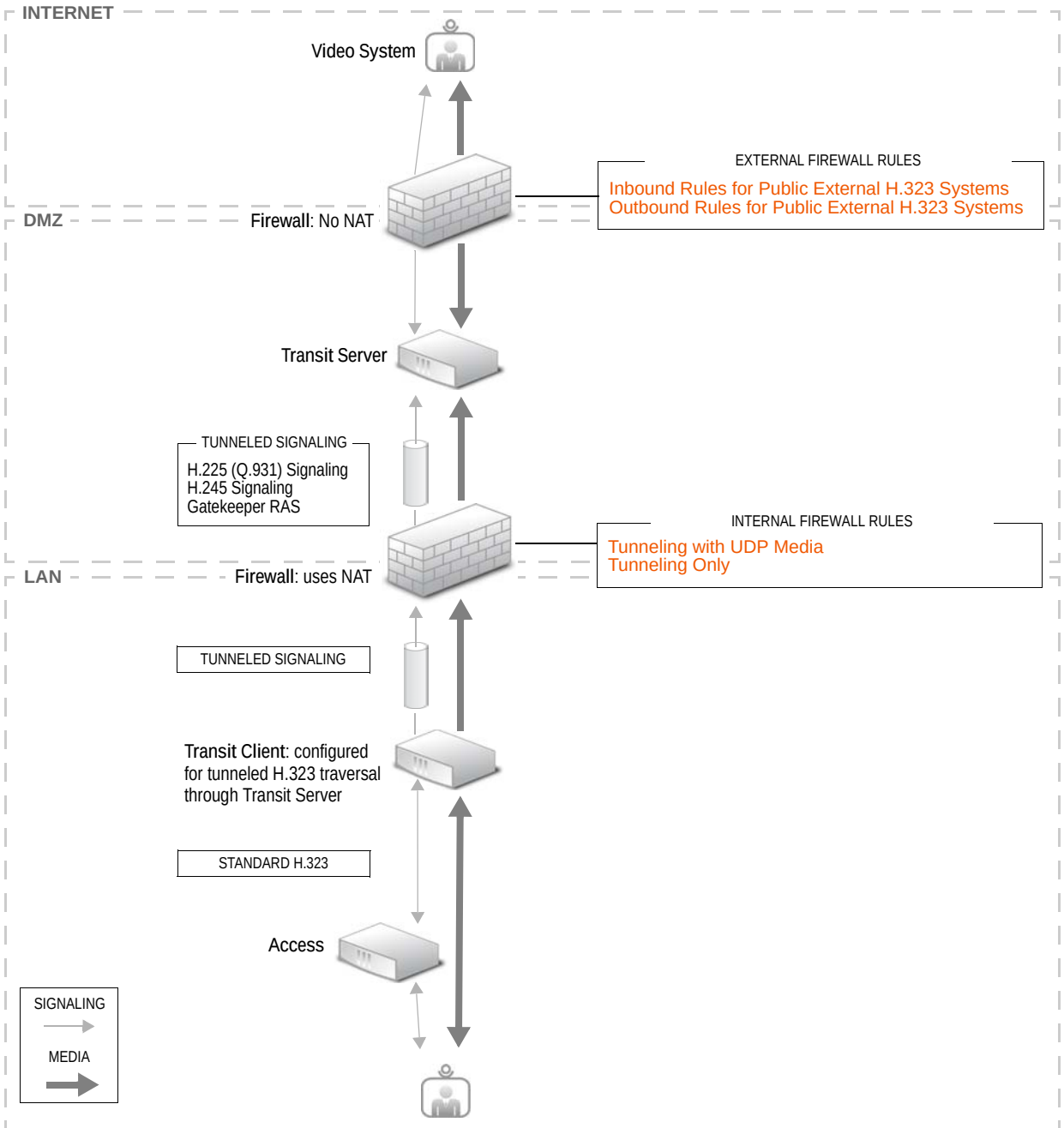


Traversal Examples

The following examples depict how signaling and media flow between the various elements of a video communications system using LifeSize UVC Transit in several common scenarios.

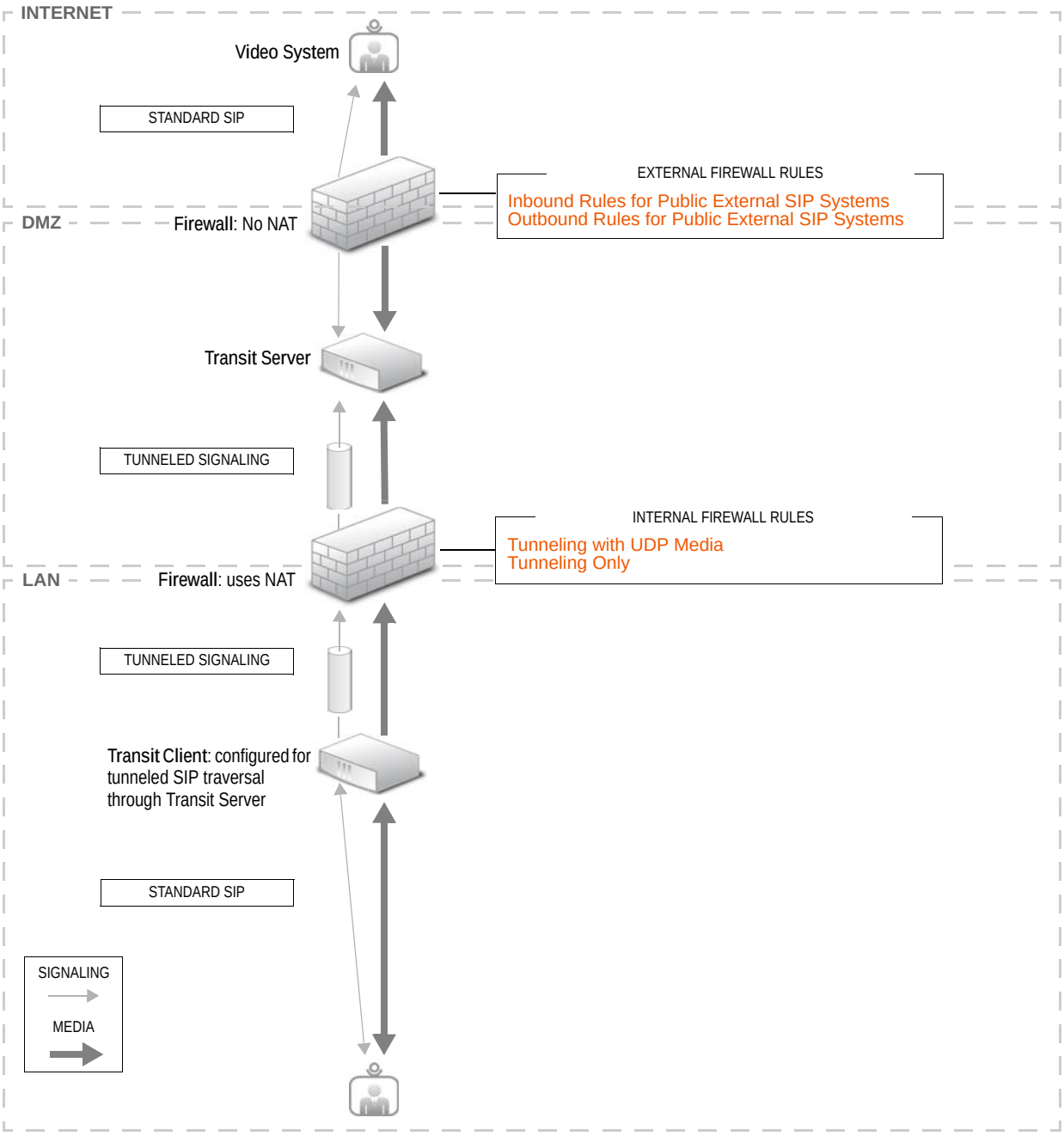
Tunneled H.323 Signaling with a Private Gatekeeper in the LAN

In the following example, all media passes between LifeSize UVC Transit Client and LifeSize UVC Transit Server. In the default configuration, all signaling is sent between LifeSize UVC Transit Client and LifeSize UVC Transit Server on a single TCP port: either TCP port 444 or 443, whichever is configured and available. This scenario includes LifeSize UVC Access in the LAN.



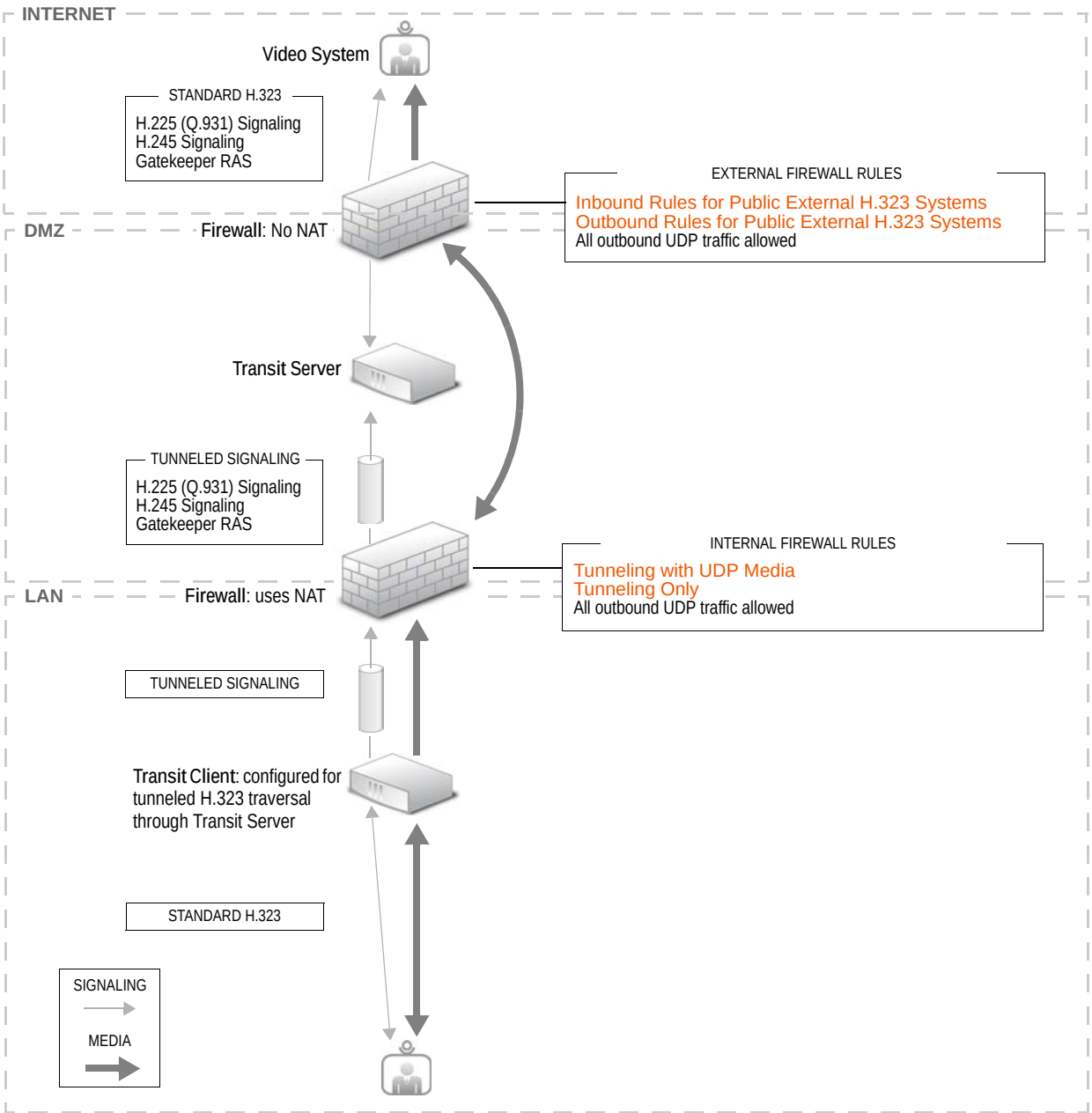
Tunneled SIP Signaling and Relayed Media

In the following example, all media passes between LifeSize UVC Transit Client and LifeSize UVC Transit Server. In the default configuration, all signaling is sent between LifeSize UVC Transit Client and LifeSize UVC Transit Server on a single TCP port: either TCP port 444 or 443, whichever is configured and available.



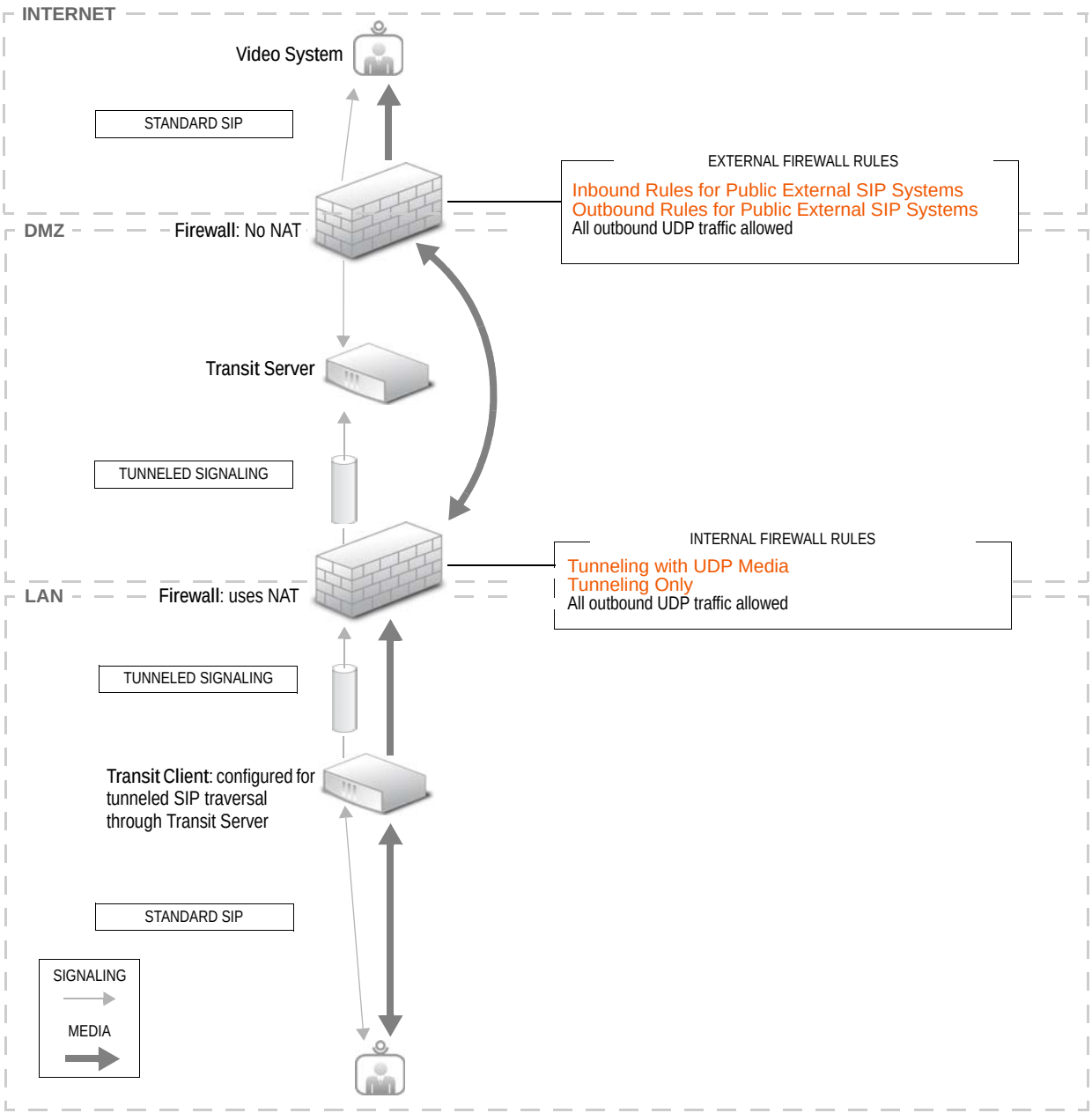
Tunneled H.323 Signaling and Direct/STUN Media

In the following example, the internal firewall uses NAT, which allows UDP traffic so that LifeSize UVC Transit Client can send RTP/RTCP media directly to the external video system. The external video system can send packets back to the firewall, which delivers them to LifeSize UVC Transit Client. In the default configuration, all signaling is sent between LifeSize UVC Transit Client and LifeSize UVC Transit Server on a single TCP port: either TCP port 444 or 443, whichever is configured and available.



Tunneled SIP Signaling and Direct/STUN Media

In the following example, the internal firewall uses NAT, which allows UDP traffic so that LifeSize UVC Transit Client can send RTP/RTCP media directly to the external video system. Likewise, the external video system sends media directly to LifeSize UVC Transit Client through the media IP and ports (which use NAT) on the internal firewall. In the default configuration, all signaling is sent between LifeSize UVC Transit Client and LifeSize UVC Transit Server on a single TCP port: either TCP port 444 or 443, whichever is configured and available.



Using the LifeSize UVC Transit Configuration Wizards

Use the wizards to configure your LifeSize UVC Transit Server and LifeSize UVC Transit Client. You must complete the configuration wizards before LifeSize UVC Transit can accept calls.

Server Configuration

During initial configuration, only the **Dashboard** and **Configuration Wizard** tabs are available and the system is in maintenance mode.

1. Click the **Configuration Wizard** tab.
2. Optionally, complete the **Static NAT configuration**. Skip this step if you are not using static NAT in the DMZ.

   You must deploy LifeSize UVC Transit Server in the DMZ. Optionally, you can deploy the server in the DMZ behind a static NAT. If you do, enter public static IP addresses for the signaling server and the media server in this step. These public addresses are mapped to the private addresses you entered when you activated the LifeSize UVC Transit Server application. All other SIP and H.323 devices communicate with LifeSize UVC Transit Server by using its public address.

   When static NAT is configured, the public and private addresses of the media and signaling server appear on the LifeSize UVC Transit Server dashboard.
3. Click **Next**.
4. Select the ports to use for tunneling.

   In SIP calls with LifeSize video systems, LifeSize UVC 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 systems to use tunneled H.323 without LifeSize UVC Transit Client. This configuration can improve H.323 call completion.

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

   You can choose TCP port 444 or TCP port 443. Ensure that the same port, 444 or 443, is open for both the signaling and media IP addresses.

   These rules allow only calls between LifeSize systems in tunnel mode and systems registered to LifeSize UVC Transit Clients. To place SIP/H.323 calls to external systems, you must also open the external firewall ports as described in Firewall Rules.
5. Click **Next**.
6. Create the tunnel account.

   Regardless of the protocols you use for video communication, you must create a tunnel account for LifeSize UVC Transit Client. If you are using LifeSize UVC Transit Server only, create a tunnel account for any system that uses tunneled signaling, media traversal, or TURN traversal.

   Make note of the username and password, as you will need these credentials to authenticate tunneling on LifeSize UVC Transit Client and LifeSize video systems. The credentials are also used in the LifeSize UVC Transit Client wizard to verify the deployment.

7. Click **Next**.
8. By default the H.323 and SIP communication protocols are enabled. You must enable at least one protocol. If you disable a protocol, the wizard hides the associated configuration steps.
9. Click **Next**.
10. Configure your gatekeeper. This step is required if you enabled H.323.

    LifeSize UVC Transit supports the following gatekeeper configurations:

    - A private gatekeeper in the LAN: Deployment Scenario: LifeSize UVC Transit Server in the DMZ and LifeSize UVC Transit Client and LifeSize UVC Access in the LAN

      With this option, you must configure H.323 routing.

H.323 prefix	Inbound calls that use this prefix are rerouted to the corresponding tunnel.
H.323 gatekeeper host	Enter the IP address of the gatekeeper in the LAN.
Gatekeeper vendor	Select *LifeSize UVC Access, Radvision*, or *Cisco*. For unlisted vendors, select *Other*.
Username **Password**	When H.235 is enabled, enter the username and password created on the internal gatekeeper for LifeSize UVC Transit Server.

    - An external gatekeeper in the DMZ: Deployment Scenario: LifeSize UVC Transit Server and LifeSize UVC Access (as an External Gatekeeper) in the DMZ

      Configure the following options:

External gatekeeper address	Enter the IP address of the external gatekeeper.
External gatekeeper vendor	Select *LifeSize UVC Access, Radvision*, or *Cisco*. For unlisted vendors, select *Other*.
Username **Password**	When H.235 is enabled, enter the username and password created on the external gatekeeper for LifeSize UVC Transit Server.

11. Click **Next**.
12. Configure SIP.

    LifeSize UVC Transit Server includes a SIP registrar that authenticates and stores user registrations. Create user accounts on LifeSize UVC Transit Server for each video device that will place or receive SIP calls. Use this account information to configure your video systems to register with the SIP registrar on LifeSize UVC Transit Server and use the SIP traversal technologies included in both the client and the server. Refer to Creating User Accounts.

    The SIP registrar on LifeSize UVC 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, and optionally with which foreign domains the registered users can participate in calls.

    a. Enter the **Local domain**.

       To allow other systems to call a domain, add the domain to the DNS for this host. Refer to Setting Up a SIP DNS SRV Record. You can add more domains in the **Configuration : SIP : SIP Registrar page** after completing the wizard.

b. Select a **Security Level**. The default is *Medium*.
   - *Full*: Authenticate all requests.
   - *Medium*: Authenticates all requests from the local domain.
   - *Registration*: Authenticates all registration requests from the local domain.
   - *None*: No authentication.

c. Select the **Proxy mode**. The proxy mode affects the routing between SIP users on external hosts or other SIP servers. Requests to and from users on this server are always forwarded.

13. Click **Next**.
14. The deployment verification tool reports on the success of the LifeSize UVC Transit Server public deployment. LifeSize recommends that you do not skip this step. Troubleshoot any deployment failures reported before completing the wizard.

NOTE The tool reports an error on the SIP TLS port (5061) if the server does not have an AES enabled license.

15. Click **Next**. Complete the configuration wizard on LifeSize UVC Transit Client before completing this step. Do not continue with this wizard until you complete the client wizard.
16. Click **Next**.
17. Click **Next** to exit maintenance mode.

Client Configuration Wizard

During initial configuration, only the **Dashboard** and **Configuration Wizard** tabs are available, and the system is in maintenance mode.

1. Click the **Configuration Wizard** tab.
2. Enter the tunnel configuration information:

Tunnel Server	Enter the IP address of the signaling server on LifeSize UVC Transit Server.
Tunnel account ID **Password**	Enter the tunnel account ID and password for the LifeSize UVC Transit Client tunnel account that you created on the LifeSize UVC Transit Server in step 6 of the sever configuration wizard.

3. Click **Next**.
4. By default the H.323 and SIP communication protocols are enabled. You must enable at least one protocol.
5. Click **Next**.

6. In **GateKeeper configuration**, enter the following:

Outbound prefix	Specify a unique prefix for outbound calls. This prefix must not be the same as the prefix configured on LifeSize UVC Transit Server for routing incoming calls to the gatekeeper.
Strip prefix	Enable to strip the prefix in the dial string of an outbound call.
Register gatekeeper	Registers LifeSize UVC Transit Client with the gatekeeper to enable forwarding outbound calls to LifeSize UVC Transit Server.
Gatekeeper username **Gatekeeper password**	If you are using H.235 authorization on the gatekeeper in the LAN, use the credentials you created on that gatekeeper for this client.

NOTE LifeSize UVC Transit Server must be in verification mode before you proceed to the next step. If you came to this wizard directly from step 15 of the server configuration wizard, the server is in verification mode and you can proceed to the next step. Otherwise, from the server, navigate to **Maintenance : Maintenance Mode : Verify deployment mode** before proceeding.

7. Click **Next**.
8. The client deployment verification tool reports on the success of the LifeSize UVC Transit Client deployment with the LifeSize UVC Transit Server. Troubleshoot any deployment failures reported before completing the wizard.
9. Click **Next**.
10. Click **Next** to exit maintenance mode.
11. Return to the LifeSize UVC Transit Server wizard and complete the steps.

On the LifeSize UVC Transit Client dashboard, if a connection between LifeSize UVC Transit Client and LifeSize UVC Transit Server was established successfully and the incoming route was added, the **H.323 internal gatekeeper** field is automatically populated with a value from the server.

In LifeSize UVC Transit Client in **Status : H.323**, ensure that **Gatekeeper registration status** is *Registered,* and the **Internal gatekeeper address** is correct.

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

NOTE Verify the registration status on LifeSize UVC Access in **Status : Clients** or in **Configuration : H.323 : Routing**.

You can change any of the settings you made in the configuration wizards in the server or client on the **Configuration** tab. If you must reset the server or client to factory settings for any reason, you must once again use the configuration wizards to reconfigure them. The **Wizard** tab contains a security configuration wizard that walks you through configuring SIP domain filtering and network filtering, and a verification wizard to check for configuration errors.

Configuring Additional Options

Neighboring Gatekeeper Configuration

Configure a neighboring gatekeeper by adding a prefix or domain route to the remote gatekeeper. In LifeSize UVC Transit Server, navigate to **Configuration : H.323 : Routing** and specify the H.323 prefix. To add a default gatekeeper, use the zone prefix "*****". Location requests will be sent to the default gatekeeper if no zone prefix match is found. Ensure that both neighbor gatekeepers configure the H.323 prefix of the neighbor.

Annex O Dialing

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

To enable video systems to receive H.323 calls in Annex O format, create an H.323 DNS SRV record for each client or H.323 server that requires access to your H.323 domain through Annex O.

If all calls go through the LifeSize UVC Transit Server or LifeSize systems, your H.323 domain does not need to resolve addresses through DNS. Use its IP address as the target in H.323 SRV records.

Typical H.323 SRV records for the gatekeeper at the example.com domain are as follows:

_Service._Proto.Name	TTL	Class	Priority	Weight	Port	Target
_h323ls._udp.example.com	Length of time the client can cache the result	IN	0	0	1719	Signaling server IP address
_h323cs._tcp.example.com	Length of time the client can cache the result	IN	0	0	1720	Signaling server IP address

Setting Up a SIP DNS SRV Record

To make your SIP domain reachable from other clients or other SIP servers without configuring them with the IP address of LifeSize UVC Transit Server, set up a SIP DNS SRV record.

Typical SIP SRV records for the registrar at the example.com domain are as follows:

_Service._Proto.Name	TTL	Class	Priority	Weight	Port	Target
_sip._udp.example.com	Length of time the client can cache the result	IN	0	0	5060	Signaling server IP address
_sip._tcp.example.com	Length of time the client can cache the result	IN	0	0	5060	Signaling server IP address
_sips._tcp.example.com	Length of time the client can cache the result	IN	0	0	5061	Signaling server IP address

Creating User Accounts

You must create a user account in LifeSize UVC Transit Server for each video communications system, MCU and its conferences, or instance of LifeSize Desktop that makes or receives calls. You can use a single account for SIP and H.323 calls.

Create user accounts in LifeSize UVC Transit Server in **Configuration : Users**. Enter the following information for each new user account:

SIP username	Required for SIP calls. For example, user@sipdomain.com.
SIP authorization name	Required for SIP calls. This is typically the *user* portion of the SIP username *user@sipdomain.com*.
SIP extension/ H.323 extension	Required for H.323 calls. You can also use the H.323 extension as the SIP phone extension.
H.323 name	An optional alias for the H.323 user.
Password	Required for SIP calls and H.323 gatekeepers that require H.235 authentication.
Enabled	Leave unchecked to temporarily prevent this device from registering to LifeSize UVC Transit Server, rather than removing the device registration completely. NOTE: If you disable the LifeSize Bridge user account when H.235 authentication is enabled, the device and all of its conferences are disabled.

All video systems that receive SIP calls must register with the SIP registrar in LifeSize UVC Transit Server. When you create these accounts, make note of the **SIP username**, **SIP authorization name,** and **Password**. You will need these values when you configure systems to register with the SIP registrar. For H.323 calls, make note of the **H.323 extension**.

NOTE To avoid creating user accounts for each conference on an MCU, add the MCU as a trusted host by navigating to **Configuration : SIP : Registrar** – **Add trusted host**.

Creating Static Routes

A static route determines which gateway to use to reach a particular network or a host.

1. From LifeSize UVC Platform, navigate to **System Settings : Routes – Edit**.
2. Click **Add Route**.
3. Enter the destination IP address and the subnet mask and gateway IP address of the network.

If invalid routes render the system unreachable, you can reset the routes through the console.

Console Command	Action
staticroute show	Displays the current static route configuration.

Console Command	Action
staticroute add <destination-ip-address> <network-mask> <gateway-ip>	Sets the static route configuration for the destination IP address.
staticroute delete <destination-ip-address>	Deletes the static route configuration for the destination IP address.
staticroute reset	Resets the system static route configuration.

SIP Domain Filtering

Enable SIP domain filtering to allow or block traffic to and from domains.

1. From LifeSize UVC Transit Server, navigate to **Configuration : SIP : Domain Filtering**.
2. Enter a domain name
3. Click **Add**. The domain is listed in **Allowed domains**. LifeSize UVC Transit allows registrations only from these domains.
4. By default, **Allow external calls** is enabled, permitting users in the allowed domains to participate in calls with users not in the **Allowed domains** list. Optionally, disable this option.
5. Click **Save**.

Creating a Network Filter

Enable network filtering to allow or block traffic to and from networks.

1. From LifeSize UVC Transit Server, navigate to **Advanced : Network Filter**.
2. Select **Enabled**. Every UDP packet or TCP connection is counted. When number of packets divided by the number configured in **Sampling interval** from an address exceeds the number configured in **Threshold**, the address is blocked for the time in seconds in **IP blocked timeframe**.
3. IP addresses you add to **Allowed IP addresses** will never be blocked.
4. IP addresses you add to **Blocked IP addresses** will always be blocked.

Section 3: Configuring LifeSize Systems for Firewall Traversal

This section describes how to manually configure LifeSize video systems and MCUs for firewall traversal with LifeSize Transit. Alternatively, you can use the LifeSize UVC Platform auto configuration feature to automatically configure LifeSize video systems. The auto-configure option does not support MCUs or software clients. Refer to the *LifeSize UVC Platform Deployment Guide* to learn more.

Before you configure LifeSize systems for use with LifeSize UVC Transit, configure your server, client, and firewall settings. Ensure that you have created all the necessary accounts on the server for each device you intend to use.

The following lists the manual configuration options for LifeSize systems by protocol:

H.323	H.323: Configuring LifeSize Systems without LifeSize UVC Transit Client H.323: Configuring LifeSize Systems with LifeSize UVC Transit Client and a Private Gatekeeper H.323: Configuring LifeSize Bridge with LifeSize UVC Transit Client in the LAN H.323: Configuring LifeSize Bridge in the DMZ
SIP	SIP: Configuring LifeSize Systems without LifeSize UVC Transit Client SIP: Configuring LifeSize Systems with LifeSize UVC Transit Client SIP: Configuring LifeSize Bridge with LifeSize UVC Transit Client SIP: Configuring a Codian MCU with LifeSize UVC Transit Client SIP: Configuring LifeSize Bridge in the DMZ

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.

H.323: Configuring LifeSize Systems without LifeSize UVC Transit Client

From the LifeSize system, navigate to **Administrator Preferences : Communications : H.323** and set the following preferences. When you are finished, navigate to the **Register** button and click **OK** on the remote control.

H.323	Enabled by default.
H.323 Name	Enter a value when the gatekeeper requires the system to register with an H.323 ID.
H.323 Extension	Required for H.323 calls. Enter the extension of the device used.
Gatekeeper ID	Set only when required by the gatekeeper. This value must match the gatekeeper ID configured for the gatekeeper to which the system is registering.
Gatekeeper Mode	Set to *Manual*.
Gatekeeper IP Address 1	Enter the IP address of the LifeSize UVC Transit Server signaling server.
Gatekeeper Port 1	Set to *1719* (the default).
H.460	Enable to specify firewall traversal of H.323 calls using H.460 protocols.
H.323 Tunneling	Enable to instruct the system to send all signaling and media through the TCP tunnel. This preference requires the LifeSize video system to be running software version 4.8 or later.
Gatekeeper IP Address 2 and **Gatekeeper Port 2**	Allows you to configure a secondary H.323 gatekeeper.
Gatekeeper Authentication	If required, enable gatekeeper authentication and enter the authentication username and password.

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**.

To test the configuration, complete these steps:

1. From LifeSize UVC Transit Server, navigate to **Status : Clients** and ensure that the correct **User ID** for the video system appears.
2. Place an outbound call: Dial the public IP address of another video system.
3. From LifeSize UVC Transit Server, navigate to **Status : Calls** and ensure that the call appears in **Active calls**.

4. Place an inbound call from a video system that has a public IP address to the system by dialing <*signalingServerIP*>##<*H.323Extension*>.
5. From LifeSize UVC Transit Server, navigate to **Status : Calls** and ensure that the call appears in **Active calls**.

H.323: Configuring LifeSize Systems with LifeSize UVC Transit Client and a Private Gatekeeper

From the LifeSize system, navigate to **Administrator Preferences : Communications : H.323** and set the following preferences. When you are finished, navigate to the **Register** button and click **OK** on the remote control.

H.323	Enabled by default.
H.323 Name	Enter a value when the gatekeeper requires the system to register with an H.323 ID.
H.323 Extension	Add the route prefix that you created in LifeSize UVC Transit Server (**H.323 prefix**) to the beginning of the value of **H.323 Extension**. For example, if the route prefix is 22 and the H.323 extension of the video system is 1234, then the value of **H.323 Extension** is 221234. NOTE: You must provision the extension on LifeSize UVC Access. If LifeSize Transit Client is not deployed on the same LAN as LifeSize UVC Access, ensure that you configure LifeSize UVC Transit with a route to LifeSize UVC Access with a matching extension.
Gatekeeper ID	Set only when required by the gatekeeper. This value must match the gatekeeper ID configured for the gatekeeper to which the system is registering.
Gatekeeper Mode	Set to *Manual*.
Gatekeeper IP Address 1	Enter the IP address of the gatekeeper in the private LAN.
Gatekeeper Port 1	Enter the port number of the gatekeeper in the private LAN.
H.460	Disable this preference.
H.323 Tunneling	Disable this preference.
Gatekeeper IP Address 2 and **Gatekeeper Port 2**	Allows you to configure a secondary H.323 gatekeeper.
Gatekeeper Authentication	If required, enter the authentication username and password.

Test the configuration by placing an outbound call. The video system can call another video system with a public IP address that is not registered to the internal gatekeeper using one of the following dial string patterns:

- <*outbound-prefix*>##<*video-system-public-IP-address*>
- <*outbound-prefix*><*video-system-public-IP-address*>

H.323: Configuring LifeSize Bridge with LifeSize UVC Transit Client in the LAN

From the LifeSize Bridge utility, navigate to **Preferences : H.323** and enable H.323. Configure the gatekeeper as follows:

H.323 Name	Enter a value when the gatekeeper requires the system to register with an H.323 ID.
H.323 Extension	If required by your gatekeeper, enter the H.323 extension.
Gatekeeper ID	If required by your gatekeeper, enter the gatekeeper ID. NOTE: If your gatekeeper does not use a static IP address, you must specify a gatekeeper ID. If **Gatekeeper Mode** is *Manual*, you can also enter the gatekeeper ID on the video system or MCU.
Gatekeeper Mode	Set to *Manual*.
Gatekeeper Hostname	If you are using a gatekeeper in the private LAN, enter the IP address of the gatekeeper.
Gatekeeper Port	Enter the gatekeeper port number. Set to *1719*, the default.

H.323: Configuring LifeSize Bridge in the DMZ

You can deploy LifeSize Bridge in the DMZ with a public address that is registered to the gatekeeper configured in LifeSize UVC Transit Server. Systems use the following dialing patterns:

System Location	Registration Status	Dial String
LAN	Registered to LifeSize UVC Transit Client or LifeSize UVC Transit Server with H.460 enabled.	*conference-ID*
Public	Registered. The external firewall must allow direct traffic to LifeSize Bridge.	*conference-ID*
	Unregistered. The external firewall must allow direct traffic to LifeSize Bridge.	*Transit-IP-address##conference-ID*
LAN	Registered to the gatekeeper.	*outbound-prefix##LifeSize Bridge-IP-address##conference-ID*
LAN	Registered to the gatekeeper in the DMZ through LifeSize UVC Transit Server.	*LifeSize Bridge-IP-address##conferenceID*

If the conference requires a password, the dial pattern is as follows:

*<conference-ID>**<password>*

NOTE This configuration does not support static NAT.

SIP Firewall Traversal

CAUTION To ensure proper configuration, configure preferences on your LifeSize systems in the order listed. Otherwise, the LifeSize systems may register directly to the LifeSize UVC Transit Server without using the SIP firewall traversal software included with the systems.

SIP: Configuring LifeSize Systems without LifeSize UVC Transit Client

Enable LifeSize Transit on the video system. From the LifeSize system, navigate to **Administrator Preferences : Network : LifeSize Transit** and set the following preferences. When you are finished, ensure that the LifeSize Transit status is *Connected*.

LifeSize Transit	Set to *Enabled*.
Transit Hostname	If LifeSize UVC Transit Server is configured with static NAT, enter the public IP address of the LifeSize UVC Transit Server signaling server. This address appears on the dashboard of LifeSize UVC Transit Server. You can also enter the DNS entry for LifeSize UVC Transit Server, if configured.
Transit Username **Transit Password**	Enter the tunnel username and password that you created for the device on LifeSize UVC Transit Server.
Transit ICE	Set to *Enabled* (the default).
Transit Signaling	If you select *UDP, TCP*, LifeSize systems probe the network and select the most efficient SIP transport from among UDP, TCP, or tunneled. If you select *TCP Only* (the default), signaling is tunneled on port 444/443.
Web Proxy URL **Web Proxy Username** **Web Proxy Password**	If your firewall allows traffic only through a web proxy, enter the web proxy address (URL), username, and password. Otherwise, leave these fields empty.

Configure the LifeSize system to use the LifeSize UVC Transit Server SIP registrar. Navigate to **Administrator Preferences : Communications : SIP** and set the following preferences:

SIP	Set to *Enabled*.
SIP Username **Authorization Name** **Authorization Password**	Enter the SIP username (without the *@domain*), SIP authorization name, and password that you entered in the user account for this system in LifeSize UVC Transit Server.
SIP Server Type	Set to *Auto*.
SIP Registration	Set to *Through Proxy*.
SIP Proxy **Proxy Hostname**	Enabling LifeSize Transit in the previous procedure automatically configures the proxy preferences. CAUTION: Do not change these settings.
SIP Registrar	Set to *Enabled*.

Registrar Hostname	Enter the SIP domain on the LifeSize UVC Transit Server. The value of this preference can be the IP address for LifeSize UVC Transit Server. Because LifeSize UVC Transit Server may include multiple domains, ensure that you enter the domain in which this system's user account resides.
SIP Signaling	Set to *Auto*.
UDP Signaling Port	Set to *5060*.

When you are finished, navigate to the **Register** button and click **OK** on the remote control. The status changes to **Registered** if the registration is successful.

NOTE If you are using software version 4.7 or earlier, ensure **Registrar IP Port** is set to the IP port number of the SIP registrar server. The default is 5060. Also, 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*.

To test the configuration, complete these steps:

1. From LifeSize UVC Transit Server, navigate to **Status : Clients : SIP**. Ensure that the SIP registration for the video system appears on this page.
2. Place a call from the video system to another SIP video system by dialing the *sip:IP address*.
3. From LifeSize UVC Transit Server, navigate to **Status : Calls** and ensure that the call appears in **Active calls**.
4. Place a SIP call from a video system to this system by dialing *sip_user@signaling_IP* or *sip_user@SIP_domain*.
5. Repeat step 3 for this call.

SIP: Configuring LifeSize Systems with LifeSize UVC Transit Client

Configure the LifeSize system to use the LifeSize UVC Transit Server SIP registrar. Navigate to **Administrator Preferences : Communications : SIP** and set the following preferences:

SIP	Set to *Enabled*.
SIP Username **Authorization Name** **Authorization Password**	Enter the SIP username (without the @*domain*), SIP authorization name, and password that you entered in the user account for this system in LifeSize UVC Transit Server.
SIP Server Type	Set to *Auto*.
SIP Registration	Set to *Through Proxy*.
SIP Proxy	Set to *Enabled*.
Proxy Hostname	Enter the IP address of the LifeSize UVC Transit Client.
SIP Registrar	Set to *Enabled*.

Registrar Hostname	Enter the SIP domain on the LifeSize UVC Transit Server. The value of this preference can be the IP address for LifeSize UVC Transit Server.
SIP Signaling	Set to *Auto*.

When you are finished, navigate to the **Register** button and click **OK** on the remote control. The status changes to **Registered** if the registration is successful.

NOTE If you are using software version 4.7 or earlier, set the **Proxy IP Port** to *5060* and the **Registrar IP Port** to *5060*. Also, 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*.

To test the configuration, complete these steps:

1. From LifeSize UVC Transit Server, navigate to **Status : Clients : SIP**. Ensure that the SIP registration for the video system appears on this page.
2. From LifeSize UVC Transit Client, navigate to **Status : Users**. The SIP registration for the system appears on this page.
3. Place a call from the video system to another SIP video system by dialing the *sip:IP address* of the SIP user.
4. From LifeSize UVC Transit Server, navigate to **Status : Calls** and ensure that the call appears in **Active calls**.
5. From LifeSize UVC Transit Client, navigate to **Status : Calls** and ensure that the call appears in **Calls**.
6. Place an inbound call to this system by dialing *sipUser@signalingIP*.
7. Repeat steps 3 and 4 for this call.

SIP: Configuring LifeSize Bridge with LifeSize UVC Transit Client

Ensure that you add LifeSize Bridge as a trusted host in LifeSize UVC Transit Server. From LifeSize UVC Transit Server, select **Configuration : SIP : Registrar** and add the IP address for LifeSize Bridge as a trusted host.

NOTE To register the LifeSize Bridge conference, ensure that you create a user account in LifeSize UVC Transit Server with username *conferenceID* and the password for the LifeSize Bridge SIP account. Read more at Creating User Accounts.

From the LifeSize Bridge utility, navigate to **Preferences : SIP** and set the following preferences:

SIP Username **Authorization Name** **Authorization Password**	Enter the SIP username, authorization name, and password that you entered in the user account for LifeSize Bridge in LifeSize UVC Transit Server.
Enable the SIP registrar	Select this option.
Registrar Hostname	Enter the SIP domain on the LifeSize UVC Transit Server. The value of this preference may be IP address for LifeSize UVC Transit Server.
Registrar Port	Set to *5060*.
Enable SIP proxy server	Select this option.
Proxy Hostname	Enter the IP address of the LifeSize UVC Transit Client.
Proxy Port **UDP Signaling Port**	Set to *5060*.

SIP: Configuring a Codian MCU with LifeSize UVC Transit Client

From the SIP settings page of the Codian MCU, set the following:

SIP registration settings	Set to allow conference registration.
SIP registrar domain	Enter the LifeSize UVC Transit Server IP address.
SIP registrar type	Set to standard SIP.
Username **Password**	Enter the username and password that you created on LifeSize UVC Transit Server for the MCU.
SIP proxy address	Enter the LifeSize UVC Transit Client IP address.

SIP: Configuring LifeSize Bridge in the DMZ

You can deploy LifeSize Bridge in the DMZ as an unregistered device. All devices, whether in the LAN registered to LifeSize UVC Transit Server through LifeSize UVC Transit Client, or in the Internet, registered (or not) to the SIP registrar in LifeSize UVC Transit Server, must use the following dial string:

<conference-ID@LifeSize Bridge-IP-address>

SIP: Configuring LifeSize Desktop

You must configure LifeSize Desktop to place calls to other LifeSize devices or LifeSize Desktop installations through LifeSize UVC 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.

Section 4: Maintaining LifeSize UVC Transit

Maintenance Mode

Before you perform maintenance and configuration, enter maintenance mode from LifeSize UVC Transit Server in **Maintenance : Maintenance Mode : Enter maintenance mode**. Maintenance mode puts the device into a suspended state and prevents new calls from connecting. After all calls are disconnected, the server enters maintenance mode. The **Force maintenance mode** option also disconnects all current calls and enters maintenance mode immediately.

Back Up, Restore, Reset

From maintenance mode in LifeSize UVC Transit Server, navigate to **Maintenance : System** and select *Back Up*, *Restore*, or *Reset* to create a backup file, restore from a back up file, or reset the service to factory defaults.

Verify Deployment Mode

Verify the LifeSize UVC Transit deployment to test whether your firewall is properly configured for communication between LifeSize UVC Transit Server and LifeSize UVC Transit Client:

1. From LifeSize UVC Transit Server, select **Maintenance : Maintenance Mode : Verify deployment mode**.
2. LifeSize UVC Transit Client, enter maintenance mode: **Maintenance : Maintenance Mode : Enter maintenance mode**.
3. Click **Deployment Verification** and **Begin verification**.

   The verification report appears in LifeSize UVC Transit Client.
4. To save the report, click **Export**.

Troubleshooting and Diagnostics

Following are common issues that you may encounter with LifeSize UVC Transit.

Issue	Workaround
A previous version of the interface persists after the upgrade.	Clear the browser cache to load the new interface.
The interface is locked after certificate file upload or password change.	If you cannot access the server through the web interface after changing the password or uploading a new certificate file, access LifeSize UVC Platform through the console. Refer to the *LifeSize UVC Platform Installation Guide.*
Invalid DNS configuration.	LifeSize UVC 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.

Error Codes

Error Codes for LifeSize UVC Transit Server and LifeSize UVC Transit Client

Number (if applicable)	Message	Meaning
404	Service down	Returned when the application is restarting.
500	Service down	Returned when the application is starting up.
	An error occurred when collecting call details.	
	An error occurred when collecting tunnel details.	

Connection Errors for LifeSize UVC Transit Client

Message	Action (if applicable)
Lost TCP connection to the Transit Server.	Ensure the LifeSize UVC Transit Server is reachable and try again.
Failed to create a TCP connection to the Transit Server.	Ensure TCP port is open on the internal firewall.
Transit Server authorization data is missing.	Supply the authorization data and retry.
The authenticator received unknown input from the Transit Server.	
The authentication method requested by the HTTP proxy is not supported.	Reconfigure the HTTP proxy with a supported authentication method and retry.
The control tunnel is not connected.	
Failed to establish an SSL connection.	Ensure SSL certificates are valid and try again.
The HTTP proxy requires authentication, but authentication credentials are not provided.	Supply the authentication credentials and try again.
The tunnel configuration was updated.	

Message	Action (if applicable)
The signaling server disabled the Transit Client.	
Failed to bind to the SIP port.	
Failed to resolve the signaling server address.	Ensure the LifeSize UVC Transit Server is reachable and try again.
Connected to the HTTP proxy, but unable to access the requested port.	Ensure the port is open on the internal firewall.
Failed to resolve the HTTP proxy address.	Verify the HTTP proxy address and try again.

Call Status Page

From LifeSize UVC Transit Server, navigate to **Status : Calls : All calls** to view active and ended calls. Click **Closed calls** to view ended and failed calls. The following details are available for a call**:**

Call ID	Unique call identifier.
Caller ID	ID of the caller. A caller ID can be the H.323 alias or the SIP username.
Caller IP address	Public address of the device or the address of a remote SIP server/gatekeeper if the internal addresses is hidden.
Recipient ID	ID as dialed of the call recipient.
Recipient IP address	IP address of the called device. This value can also be the address of a remote SIP server/gatekeeper.
Duration	Length of the call.
Status	Active or inactive.
Details	Includes additional information about the call, including the originating and terminating tunnel and user IDs, IP addresses, and client types; and details about the originating and terminating media.

Events

LifeSize UVC Transit can send email or SNMP traps to certain events. From LifeSize UVC Transit Server, navigate to **Configuration : Events**.

SMTP server	The outgoing SMTP server address.
Username **Password**	Authentication credentials at the SMTP server.
Recipients	The mail address of the recipients (separated by a comma).
Trap receiver address	The address of the SNMP trap receiver.

To view events on the LifeSize UVC Transit Server signaling server, navigate to **Status : Events**.

Order	Event number.
Event name	Logical name of the event.
Severity	Severity of the event (corresponds to the log level for each event).
Information	Explanation of the event.
Time of event	Timestamp when the event occurred.
Customer ID	ID of the customer.
Clear	Clears the event.

Diagnostics

Both LifeSize UVC Transit Client and LifeSize UVC Transit Server allow you to log events. CDRs can include information that is useful for diagnostics and are now included in the log files. Download log files in **Status : Logs**.

Set the log level in **Configuration : Logs** for controls to set the LifeSize UVC Transit and system log levels and system log host. LifeSize Technical Services may instruct you to download and send these files to LifeSize for analysis.

Enable remote access through the LifeSize UVC Platform in **Operations and Maintenance : Remote access**.

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.