

Firewalls, NAT's and VPN's

Version 1.8.1028
November 15, 2007

AliceStreet
Conference Center



Put a
real conference room
on your **desktop...**

IBM Server **Proven**

AliceStreet Conference Center

A real conference room on your desktop

1.	Connectivity overview	3
1.1	How the client connects to the server	3
1.2	How protocols work	3
1.2.1	H.323	3
1.2.2	T 120	3
1.2.3	Possible Complications	4
2.	Firewalls	4
2.1	Port opening.....	6
2.2	H,323-aware firewalls	7
2.3	Establish a VPN.....	7
3.	Network address translation.....	7
3.1	Why NATs can cause problems.....	7
3.2	Client behind a NAT	8
3.3	Server behind a NAT	8
4.	VPN's	9

1. Connectivity overview

1.1 How the client connects to the server

The overall connection process works as follows:

- when you connect to the server using Internet Explorer, the server tells the client what IP address to connect to
- the client then connects to that IP address using the H.323 protocol. H.323 is used to communicate voice, video, and information about direction of view within the room
- once an H.323 connection is established, the client separately connects to the server IP address using the T.120 protocol. T.120 is used to communicate slides, user names, and other data sharing capabilities.

Unfortunately, whilst the H.323 and T.120 protocols are extremely useful and robust, they are comparatively complicated. The fact that you can connect to the server using a web browser (HTTP) does not necessarily mean that the client will be able to connect using H.323 and T.120.

1.2 How protocols work

1.2.1 H.323

The H.323 protocol parts of the connection work as follows:

1. the client establishes a TCP connection to the server on a designated port (1)
2. the client establishes a further TCP connection to the server on a different port
3. the client and server then tell each other what UDP ports they will receive real-time (voice and video) traffic on
4. each then starts to transmit packets to those UDP ports, containing the voice and video RTP and RTCP traffic.

The range of ports used for points 2 and 3 above can be configured on the server (see the administrator's guide). You need to reserve 5 ports per concurrent user in this range if not using AliceStreet Secure Channel.

1.2.2 T 120

The T.120 protocol (if used) establishes a TCP connection to the server on port 1503. T.120 is used only for the whiteboard and application sharing functionality.

- (1) This defaults to 1730 for the AliceStreet Conference Center, but a different default port can be configured on the server. See the administrator's guide.

1.2.3 Possible Complications

Firewalls

Firewalls can complicate matters because firewall(s) between the client and the server may block inbound (and in some cases outbound) traffic on some or all of the ports.

In particular, firewalls that don't understand H.323 often won't allow the inbound UDP packets to reach their destination so both the client and server may think they're connected but not in fact be able to exchange any voice and video traffic.

NAT (Network Address Translation)

Although NATs are well known to cause problems for many Voice over IP deployments, the AliceStreet Conference Center's technology should seamlessly traverse any NATs that may be found between the client and the server.

VPN (Virtual Private Network)

In general, running the AliceStreet Conference Center over a VPN should present no problems. However, we have observed issues in some scenarios due to the way the VPNs are implemented.

In particular:

- some VPN clients don't handle UDP packets well
- some VPN servers cannot handle the volume of packets which are generated by a real-time voice and video application.

2. Firewalls

Firewalls may block traffic on some or all of the ports which are used by the system. There are a number of ways to overcome these problems.

2.1 AliceStreet Secure Channel

AliceStreet Secure Channel is a completely encrypted SSL VPN channel running from the users PC to the AliceStreet Conference Center. The system supports SSL VPN and provides the secure channel between the AliceStreet client application and the AliceStreet Conference Center.

There are two types of secure connections for AliceStreet.

- Enterprise users who have installed AliceStreet servers within their own operating environment. Please contact your Administrator for your secure connection details. AliceStreet solutions will work with most VPN vendor appliances from major manufacturers. If the Enterprise user is not operating an appliance based VPN, then AliceStreet Secure Channel can be deployed on CPE or be hosted in one of AliceStreet's Secure Global Conference Centres.

AliceStreet Conference Center

A **real** conference room on your desktop

- Licensed users who are subscribing to AliceStreet solutions located in one of AliceStreet's Secure Global Conference Centres. The following applies to all users in this category including any on demand pay as you go users.

AliceStreet is using Secure Sockets Layer (SSL) as cryptographic protocols that provide secure communications, for the AliceStreet application, on the Internet for connecting to AliceStreet Conference Centres around the world.

Securing only AliceStreet applications allows the user to use all of his or her other regular applications while in an AliceStreet Conference. All that the user requires is to be able to browse the internet using port 443 or HTTPS sites with authorization to use HTTPS, SSL, UDP and TCP protocols. In that way he can connect from his company through the firewall to the SSL VPN and establish an AliceStreet meeting.

AliceStreet Secure Channel uses appliances from SonicWall. The appliances AliceStreet has chosen have been selected for their ability to deal with the following technical concerns:

- Application Encryption
- Compatibility to the already heavily compressed data generated by AliceStreet
- Tight integration to authentication databases
- Latency
- Ease of use
- MTBF
- Stability
- Low bandwidth overhead

Secure Channel Advantages

AliceStreet Secure Channel rounds out the AliceStreet solution and assists in the overall technical mission in delivering to the marketplace a secure audio, video and data communications solution. The technical advantages:

- Multipoint video (up to 16 people simultaneously)
- Single secure port access
- Fully encrypted conferencing
- Fully encrypted data collaboration tools.
- Low user bandwidth with full encryption
- Low latency with full encryption

Refer to diagram 2.0.

AliceStreet Conference Center

A real conference room on your desktop

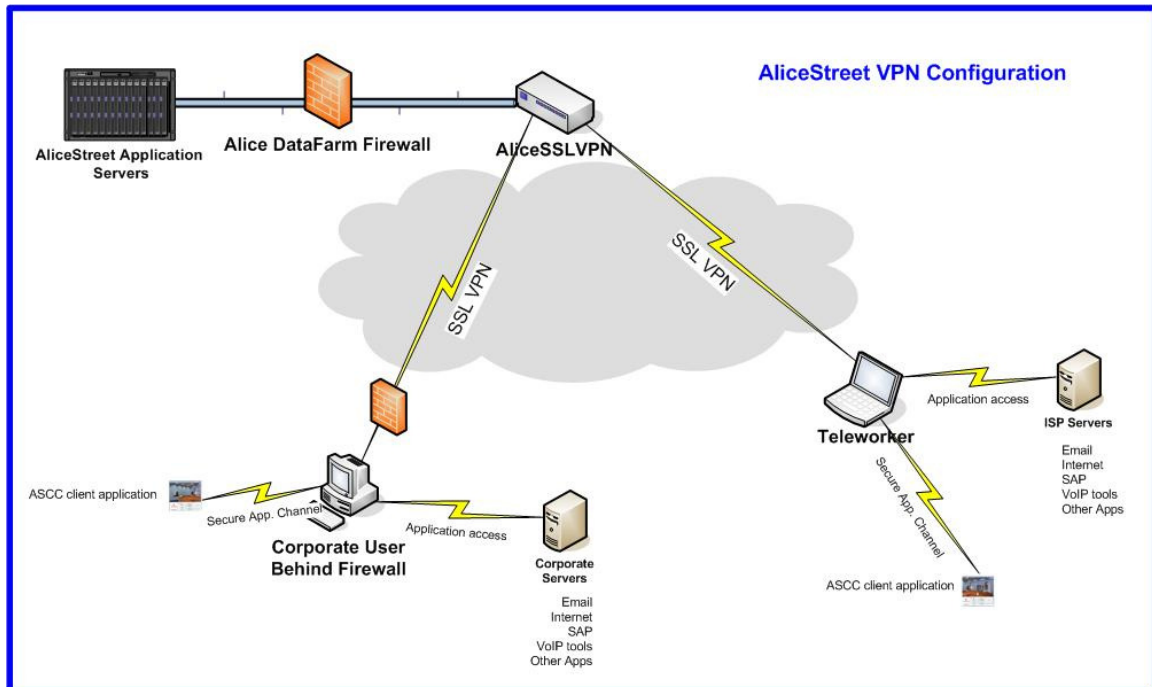


Figure 2.0 AliceStreet Secure Channel

2.2 Port opening

Although not recommended, you can avoid firewall issues by opening the relevant ports in your firewall(s) on a permanent basis should you not have your own VPN or elect not to use AliceStreet's Secure Channel. AliceStreet discourages general port opening, and will only advise use if the clients and server is entirely within a corporate firewall.

Outbound port opening for client PCs

Client PCs should be able to open outbound ports for:

- Port 80: to access login page and directly open to the server, and TCP to transfer name tag data
- TCP on the H.323 listener port defaults to 1730 but otherwise the default is 1720 (as defined in H323)
- TCP and UDP on the port range used for media. By default this could be any port range but can be configured on the server using the "Fix Port Range" option. Note that an average of 5 ports should be allowed for each concurrent user. AliceStreet generally defaults to the range 5000 to 6160 for a 32 connection server.

Client PCs should be able to open outbound ports for UDP on:

- the port range specified on the server (if no port range is specified on the server then all ports must be openable outbound).

Inbound port opening for servers

Server PCs should have inbound ports open for both TCP and UDP on:

AliceStreet Conference Center

A real conference room on your desktop

- Port 80: to access login page and directly open to the server and TCP to transfer name tag data
- TCP on the H.323 listener port defaults to 1730 but otherwise the default is 1720 (as defined in H323)
- TCP and UDP on the port range used for media. By default this could be any port range but can be configured on the server using the —Fix Port Range“ option. Note that an average of 5 ports should be allowed for each concurrent user. AliceStreet generally defaults to the range 5000 to 6160 for a 32 connection server.

2.3 H,323-aware firewalls

Some brands of firewall are explicitly aware of H.323 traffic. As a result, when the client signals that it will receive UDP packets on certain ports, the firewall will then allow UDP packets from the server on those ports to pass (and vice versa).

Note that some H.323-aware firewalls may present incompatibilities with the AliceStreet Conference Center in particular, if they do not support —FastStart“. For this reason, the default H.323 listener port is set to 1730 rather than the usual H.323 port of 1720.

2.4 Establish a VPN

You can use a VPN to place both client and server on the same virtual network, thus bypassing the firewall. Refer to AliceStreet Secure Channel.

3. Network address translation

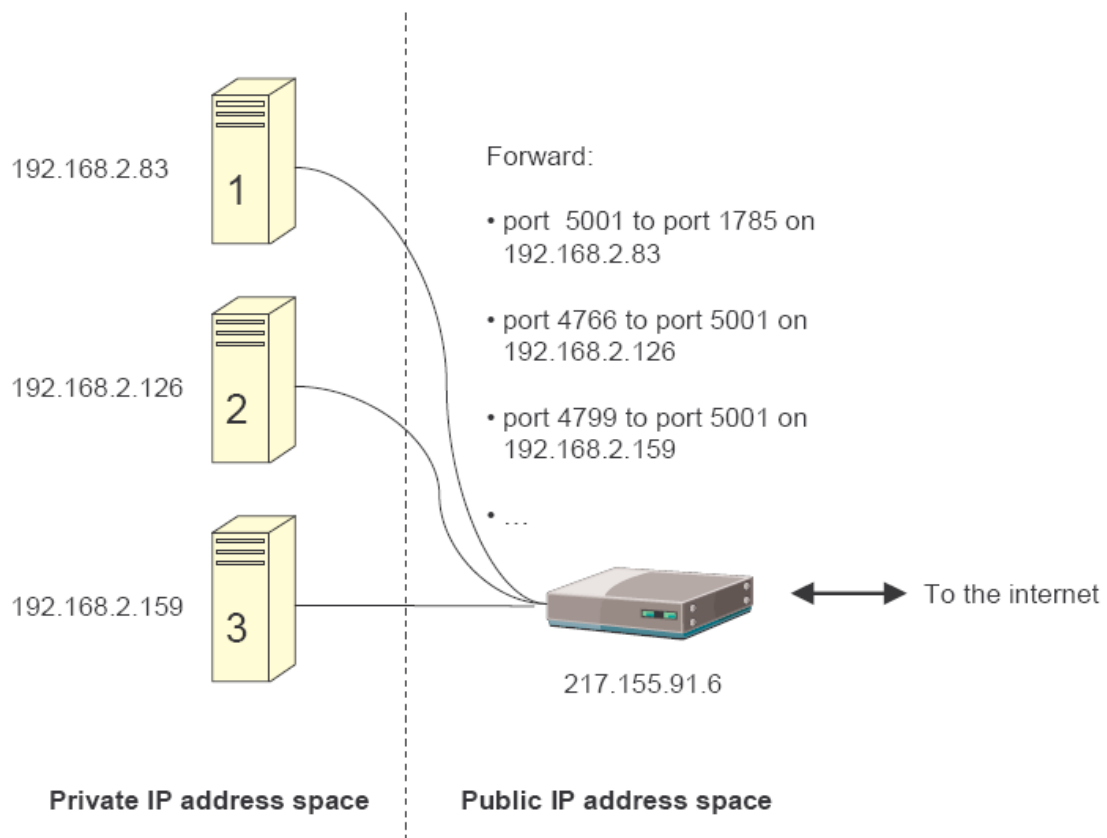
3.1 Why NATs can cause problems

NATs complicate all H.323-based systems because the IP address which the outside world perceives for PC behind a NAT is not the same as the IP address which the PC itself perceives.

For example, in the figure below, all 3 of the computers appear to the Internet as IP address 217.155.91.6, but the machines themselves think that their IP addresses are 192.168.2.xxx. Standard H.323 signalling will tell the other endpoint to send packets to 192.168.2.xxx but if the other endpoint is on the Internet side of the NAT, these addresses will be unreachable.

AliceStreet Conference Center

A real conference room on your desktop



In addition, in this example, both machines 2 and 3 have opened port 5001 for inbound UDP traffic. However, the NAT is forwarding packets received on port 5001 to machine 1.

3.2 Client behind a NAT

AliceStreet's technology overcomes the issues above and means that a client behind a NAT should encounter no problems connecting to the server. If you do encounter problems connecting it is most likely to be a firewall issue.

3.3 Server behind a NAT

In cases where the AliceStreet server is behind a NAT, you will need to configure both the server and the NAT appropriately.

To do this, on the server:

- go to [http://\[server\]/admin](http://[server]/admin) and logon appropriately
- enable —NAT routed— and specify the public IP address of the NAT device
- set a fixed port range

On the NAT:

AliceStreet Conference Center

A real conference room on your desktop

- reserve the fixed port ranges configured on the server as well as
 - 1730 (or other H.323 listener port as configured on the server)
 - 1719 (if an H.323 gatekeeper is used)
- set the NAT to forward these ports untranslated to the server. Consult your NAT device's documentation for information on how to configure this port forwarding.

4. VPN's

In general, using a VPN (Virtual Private Network) is an excellent way of connecting to the conference server, as well as ensuring security for the meeting.

However, there are some things to take care with due to specific issues relating to different vendors' implementations of VPN.

In particular:

- When using the Microsoft VPN client with L2TP/IPSec, we have found that 30%-50% of all RTP packets received by the client are lost. This makes use of voice and video impossible.

Solution: install a different VPN client or use AliceStreet Secure Channel.

More generally:

- use of voice and video over IP typically involves the use of a large number of comparatively small packets, and the AliceStreet Conference Center is no exception. The large number of packets traversing the VPN may cause problems for some software VPN servers which may lack the processing power to cope with this number of packets.

Solution: use a more powerful VPN server or use AliceStreet Secure Channel.

- using some VPN technologies that are based on SSL (—SSL VPN“) is not always recommended. These VPN technologies are fundamentally TCP-based and this means that the performance profile required for UDP is not achieved. As a result, you can expect to hear significant interference in your audio quality and see significant delay in your video. However, recent improvements in various manufacturers processes have allowed for successful deployment using AliceStreet. Currently SonicWALL, Netilla SSL VPN, Cisco and Checkpoint based are known to be deployed successfully. Please contact your local partner to discuss VPN options.