



The Global V C S Secure Connect software enables video calls and collaborative conferences to securely traverse network boundaries.

Visual collaboration between users in different locations and different organisations becomes secure and easy. The technical obstacles created by the vital elements of global networks, such as firewalls and network address translations (NAT) are not risked, or breached.

Secure traversal capabilities provide true mobility for dispersed teams enabling them to meet face-to-face wherever they have a broadband IP connection, be it at work, home, in a hotel, the airport – almost anywhere in the world.

- A Transparent Solution**
 All traversal/connections are multiplexed onto one or two fixed ports through firewall/NAT. Port numbers are defined by administrator for flexibility
- H.460 support for support of Video Conferencing systems**
 Old and new systems are equally supported.
- Multi-Vendor and Multi-Device Support**
 Supports devices and endpoints from all major manufacturers. Can be managed by existing gatekeepers.
- Fits into Existing Corporate Security and Quality of Service Policies**
 Supports HTTP Proxy traversal.
- Server to Server failover**
 Clients stay connected when multiple servers are deployed.
- Privacy When You Need It**
 Encryption options available for all media.

Global V C S Secure Connect simplifies the design and implementation of multi-media networks, as existing infrastructures require no changes. This software product works in conjunction with any firewall/NAT router and acts as a 'border controller' and proxy for video calls and conferences that need to traverse a network boundary.

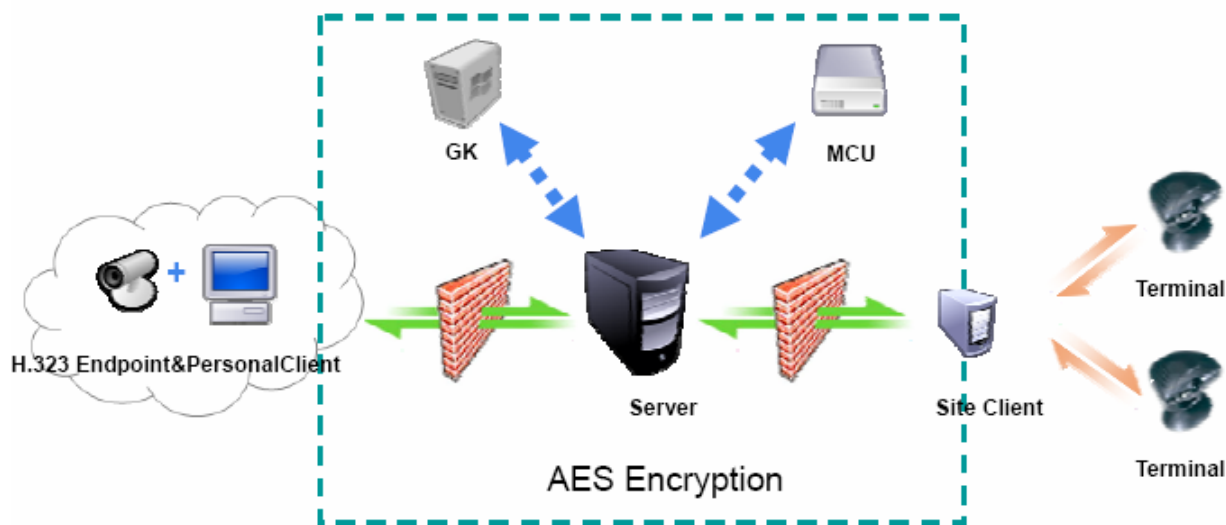
Built on a client-server architecture where the server application software runs on Intel®, or compatible server with a Linux operating system. The client software runs on a Windows® PC or Linux client.

Global V C S Secure Connect enables people on different networks to traverse their enterprises' firewall and NATs routers and securely communicate across the public Internet using voice, video and data collaboration. It can be used as a standalone product or as part of an integrated visual collaboration solution.

Seamless communication can take place across multiple network boundaries, without compromising security.



Secure Connect



Protocols	H.323 version 4 and above (ITU-T), H.460 Firewall NAT Traversal Standard, H.239 Additional Media Channels (ITU-T), SIP Version available on request
Interoperability	Multi-vendor support – any H.323 device
Firewall / Nat Traversal	Client-Server transparent tunnelling model. Only “outbound” initiated connections on configurable port or port range. TCP only tunnelling or TCP/UDP tunnelling modes. Client located with application (Personal Client), or on local network (Group Client). Server located in DMZ, or public Internet. Server acts as full proxy dealing with any network address translation (NAT).
Default Traversal Ports	TCP port 8081, UDP Ports 8081, 8082 (optional)
HTTP Proxy	Capable of traversal through an HTTP proxy
Clients	Personal Client for mobility or small deployments Group Client for multiple devices in single LAN
Server Software	REDHAT Linux: Enterprise Server 3 and 4; Advanced Server 3 and 4 CentOS 4.4
Client Software	Windows XP or Vista, Linux client
Load Balancing & Redundancy	Client fails over to secondary server
Privacy	Encryption of H.323 audio video and data by AES (128, 192 and 256 bit)
Scaling	Scales linearly by adding additional servers. Single server can support 80 calls at 384Kb using a 100Mb NIC card