



The Visual Nexus® Secure Transport 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 these to access their company information and network service wherever they have a broadband IP connection, be it at work, home, in a hotel, the airport – almost anywhere.

- **A Transparent Solution**
No change to existing infrastructure or behavioural change from multi-media devices is required.
- **Multi-Version H.323 Support**
Old and new versions of the communication protocol 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 configurable traversal ports.
- **Any Size Deployment**
Scales from one to thousands of traversals.
- **Privacy When You Need It**
Encryption option available for all media.

The Visual Nexus Secure Transport 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.

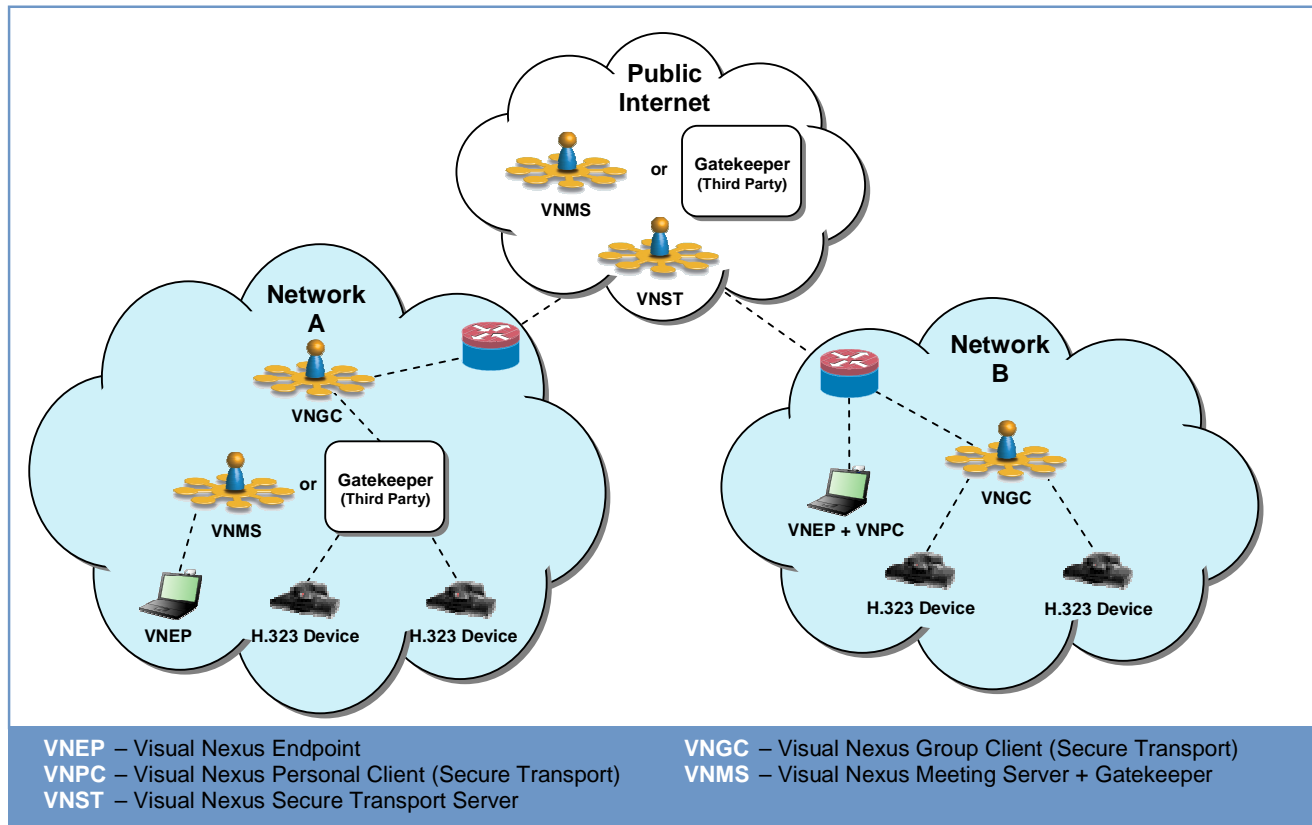
Built on a client-server architecture where the server application software runs on Intel®, or compatible server with a Linux operating system. The client software runs on a Windows® PC.

The Visual Nexus Secure Transport 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 the Visual Nexus visual collaboration solution.

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



Secure Transport



Specifications

Protocols	H.323 version 4 and above (ITU-T), T.120 (T.124:GCC and T.122/T.125: MCS) (ITU-T), 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)
Clients	Personal Client for mobility or small deployments Group Client for multiple devices in single LAN
Server Software	REDHAT Linux: Enterprise Server 4 and 5; Advanced Server 4 and 5 CentOS 4.4 and 5
Minimum Hardware Requirements	Intel® Pentium® 4 processor, 3GHz or higher, Intel® Xeon® processor, 2GHz or higher (Dual-processors are supported), 1GB memory or higher; 100BASE-TX network interface
Load Balancing & Redundancy	Client fails over to secondary server Central licensing shared by multiple servers allows load balancing
Privacy	Encryption of H.323 audio video and data by AES (128, 192 and 256 bit)
Scaling	Scales linearly by adding additional servers

In our constant effort to improve solutions, Visual Nexus Ltd. reserves the right to change or modify features and specifications without notice. VN321-03-03-003 Issue 004