Secure Connect

Secure Connect is an essential component in any video communications network where video calls need to be made across network boundaries. It can be paired with VMCi's Open Client and any other software client that adheres to the H.460 protocol. With Secure Connect, virtual meetings between users in different locations or different organizations are secure and simple. The technical obstacles created by the vital security features of global networks such as firewalls and network address translations (NAT) are not risked or compromised.

Service Overview

Secure Connect enables video calls and virtual meetings to securely traverse corporate firewalls and network boundaries. Its capabilities provide true mobility for dispersed teams enabling them to participate in virtual meetings wherever they have a broadband IP connection, be it at work, home, in a hotel, the airport – almost anywhere.

Secure Connect acts as a front-line border controller and simplifies the design and implementation of any video communications network in a number of ways as no changes are needed to existing infrastructure or systems. Secure Connect works in conjunction with any firewall/NAT router acting as a 'border controller' and proxy for video calls that traverse the network boundary. No firewall bypass is needed. Its 'transparency' means it can be deployed alongside exiting or any preferred 3rd party video infrastructure conforming to the ITU H.323 standard. Through one of its 3 traversal methods it connects a wide range of endpoints from systems supporting H.460 standard, to any legacy systems and software clients conforming to the H.323 standard. With its unique URI dialling capability that offloads any gatekeeper involvement, Secure Connect also enables calls to and from endpoints in remote networks.

Secure Connect is a software product that runs on standard off-the-shelf servers. It may be deployed in the public Internet or in a private DMZ and is used by both service providers and enterprises managing their own video network.

Product Highlights

- ☑ **Transparent**

  Maintain existing security policies. Use existing or preferred 3rd party video infrastructure.

- ☑ **Software and Scalable**

  Traversals can be added as needed and the software can run in a virtualized environment. Ease of administration and installation.

- ☑ **H.460 and Univeral Tunnelling**

  Old and new systems are equally supported.

- ☑ **URI Dialling**

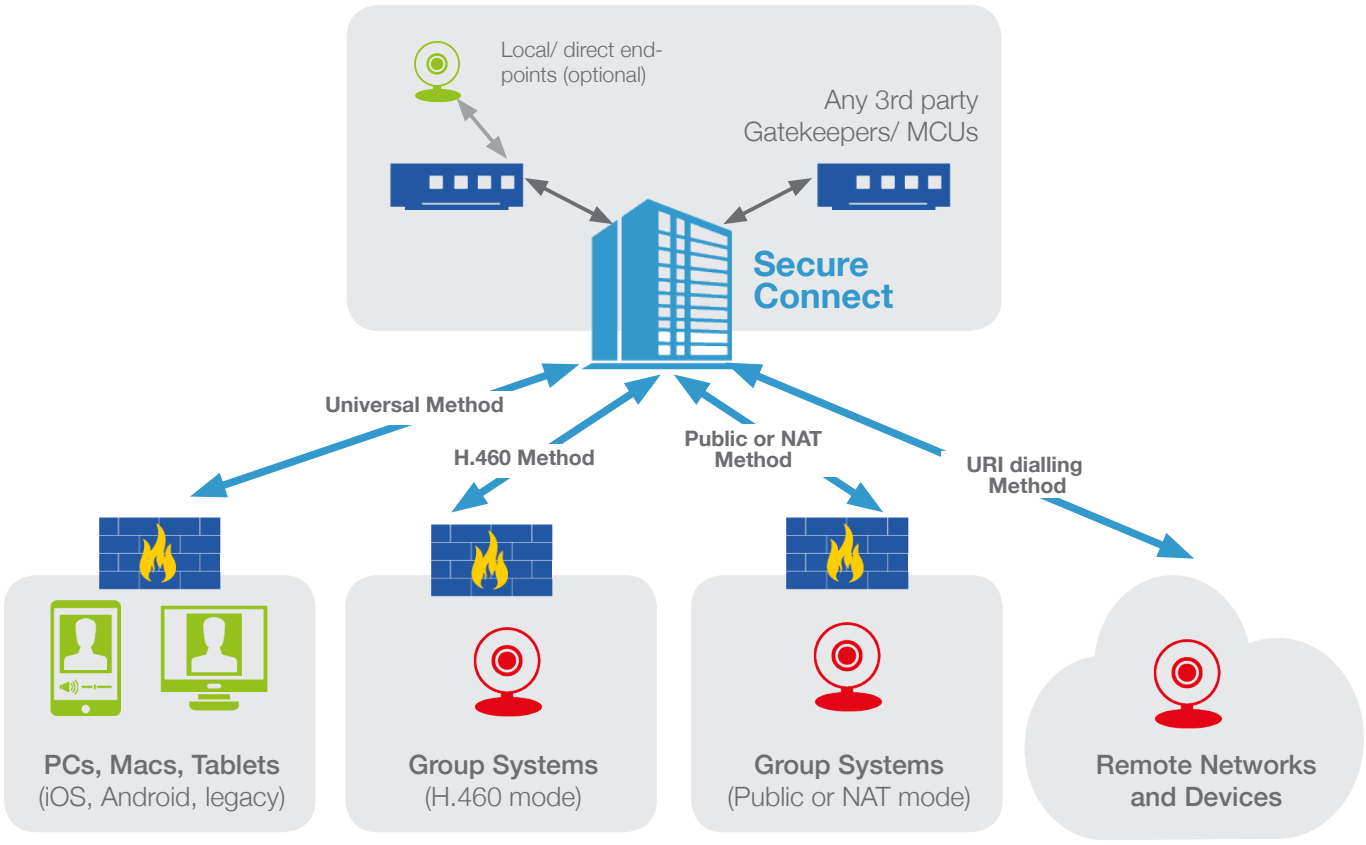
  Connect to endpoints in remote network easily and securely.

- ☑ **Multi-Vendor, Multi-Device**

  Support for devices and endpoints from all major manufacturers. Can be managed by existing gatekeepers.

- ☑ **Direct Media**

  When two endpoints in a call are detected as being in the same network (LAN or both public), media is routed directly instead of through the server.



Specifications

Protocols	H.323 version 4 and above, H.460, H.239 additional media channels
Interoperability	Multi-vendor support – any H.323 device.
Firewall/ NAT Traversal Methods	H.460.18 and H.460.19 Universal Tunnelling for legacy (non-H.460) systems and software clients. Public Tunnelling (DMZ deployments) for public or publically mapped IP address endpoints. URI dialling.
Default Universal Tunnel Ports	TCP port 8081, UDP ports 8081/8082
Default H.460 Traversal Ports	UDP 1719, TCP 1720, TCP 8082, UDP 8084/8085
Default Public Tunnel Ports	UDP 1719, TCP 1720, 1721, 1730+, TCP/UDP > 8090+
Server Software	64-bit REDHAT Linux or CentOS, version 5.x and above
Minimum Hardware Requirements	Intel Pentium 4 processor, 3GHz or higher, Intel Xeon processor, 2 GHz or higher (Dual processors are supported), 1 GB memory or higher; 100BASE-TX network interface. 64-bit Linux
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 384 kbps