

Overcoming Secure Visual Communication Obstacles with TANDBERG Expressway™

Deploying visual communication services over an IP network? Concerned about security?

Security and investment are two of the top concerns when deploying visual communication services over IP, and organizations are looking for a practical solution that does not require costly infrastructure upgrades.

Security and dialing plans are the top two concerns when implementing visual communication services over an IP network

There are two key issues affecting IP communications service deployments:

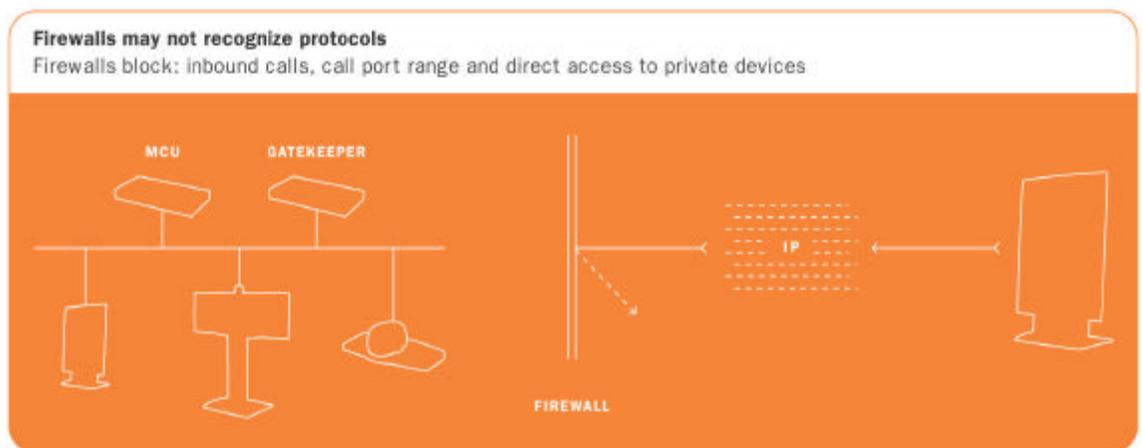
- Security – Firewall integrity & network address translations
- Dialing Plans – how to create a universal dialing plan

This document discusses each in turn.

Security

Firewall Integrity – The Challenges

The key issue for firewall integrity is that the real-time IP communication protocols are designed to provide point-to-point connectivity. For any given call, there is a caller and a recipient. For visual communication to succeed, everyone must be prepared to receive calls from time to time. For visual communication to become ubiquitous, these calls may come from a variety of callers, including suppliers, customers and telecommuters.



Most firewalls are not designed for rules that allow everyone to connect to everyone.

In security terms, such broad, ad hoc connectivity is a serious concern with most firewall solutions. Rules that allow everyone to connect to everyone else are unusual and unwelcome to the security administrator. Added to that, the IP communication protocols use a wide range of network ports, and the protocols are indistinguishable from other protocols unless the firewalls are designed with specific protocol awareness.

Upgrades are costly and would be required every time a new protocol is introduced

The obvious route to secure, open communications involves costly upgrade of firewalls to provide the protocol awareness for IP communications protocols. To provide universal service, the upgrade needs to be repeated by the great mass of enterprises, and repeated for every time a new protocol is introduced.

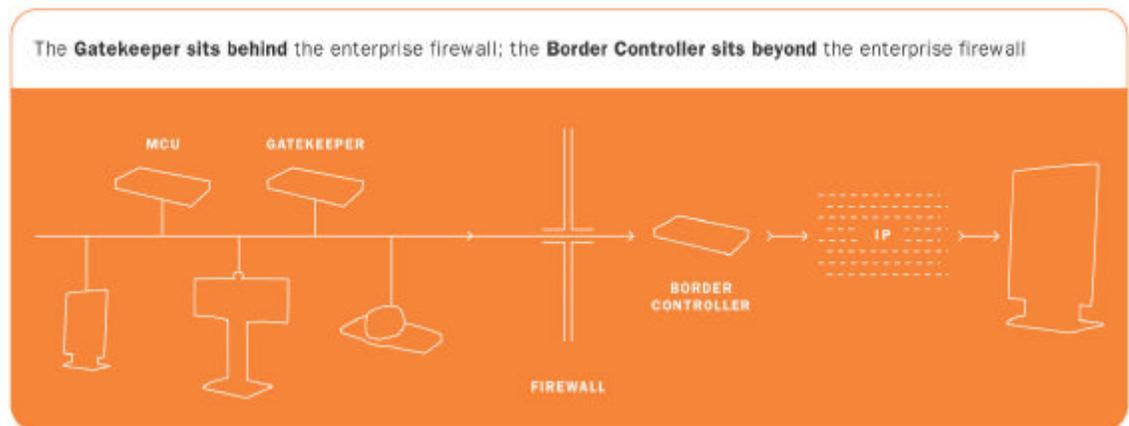
Instead, security administrators are looking to avoid costly upgrades to critical equipment, and define a small set of firewall rules that allow very few entities to communicate through very few ports. TANDBERG Expressway meets that need.

TANDBERG provides a secure traversal method that does not require costly upgrades

TANDBERG Resolves the Firewall Challenges

TANDBERG resolves firewall issues by providing a secure traversal method. TANDBERG's Expressway solution for firewall and network address translation (NAT) traversal has two elements: a secure path element for control of information, and a relay element for forwarding media without additional overhead. Video communication uses Expressway to traverse a secure path through the firewall.

The TANDBERG solution is implemented with two components: a Border Controller and the TANDBERG Gatekeeper or a TANDBERG MXP product. The Gatekeeper sits within the space behind an enterprise firewall. The Border Controller sits in the public space beyond the firewall.



The Border Controller might even be hosted by a service provider, or hosted in an enterprise DMZ along with the enterprise mail and web proxies. Therefore, the Border Controller and Gatekeeper (or MXP endpoints) are on either side of the firewall that would typically need upgrading.

The firewall only needs to allow connections between the solution components, and the Gatekeeper, Border Controller and MXP endpoints are designed to use a very small number of registered ports. Rather than using the wide port range normally exploited by communication devices, TANDBERG's Expressway solution allows the firewall rules to be tighter still.

The TANDBERG Expressway solution works with almost any firewall or endpoint registered to the TANDBERG Gatekeeper

What about Non-MXP endpoints? Endpoints other than the TANDBERG MXP visual communication devices within the private network use the TANDBERG Gatekeeper to achieve the same results. All outbound video call traffic is directed to the Gatekeeper which relays it to the Border Controller. The visual communication device can use any port to connect to the Gatekeeper, but the Gatekeeper relays the traffic to the registered ports of the Border Controller. The behavior of the visual communication device is unaffected, and the firewall rules are simple and require no protocol awareness in the firewall.

Network Address Translation – The Challenges

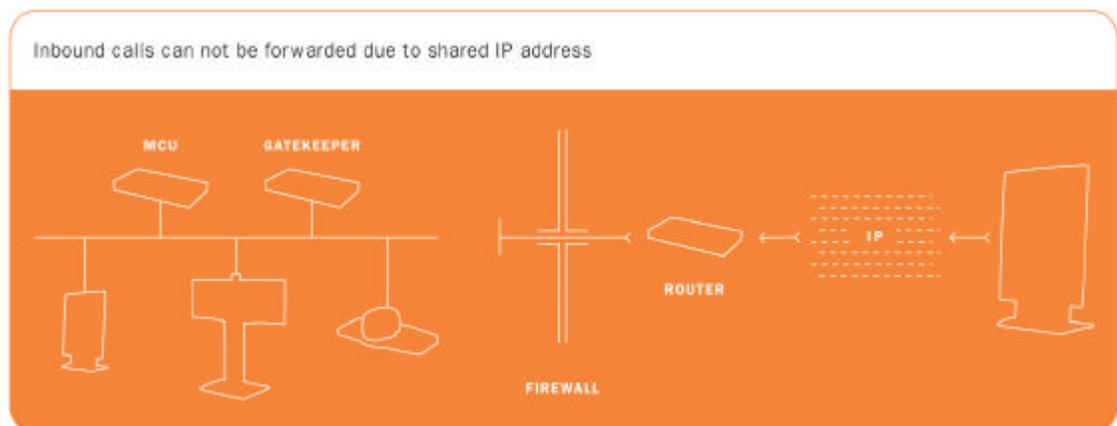
Network address translation (NAT) enables organizations to use private addressing schemes for their networks, but provide devices with public addresses as and when required. However, for IP communication protocols such as SIP and H.323, organizations find themselves compromised by this very same mechanism, presenting a deployment issue for anyone who wants to communicate across network boundaries.

Network Address Translation (NAT) is a challenge for anyone who want to communicate across network boundaries

Typically, enterprises use a single, shared public address to represent many internal devices. When a device needs to make a connection to an external network, the translation function assigns a port on the shared address. This assignment is discarded as soon as the connection ends.

This translation function is widely exploited as a security feature. The assignment of a port to a particular device exists only for the lifetime of a connection. The ability to discard assignments as soon as a connection ends means that a malicious external agent attempting to use a port to gain access to the enterprise will find that it is either already in use for a connection and therefore inaccessible to a new connection, or not assigned to anything, and therefore a dead-end. Either way, the uninvited connection goes no further.

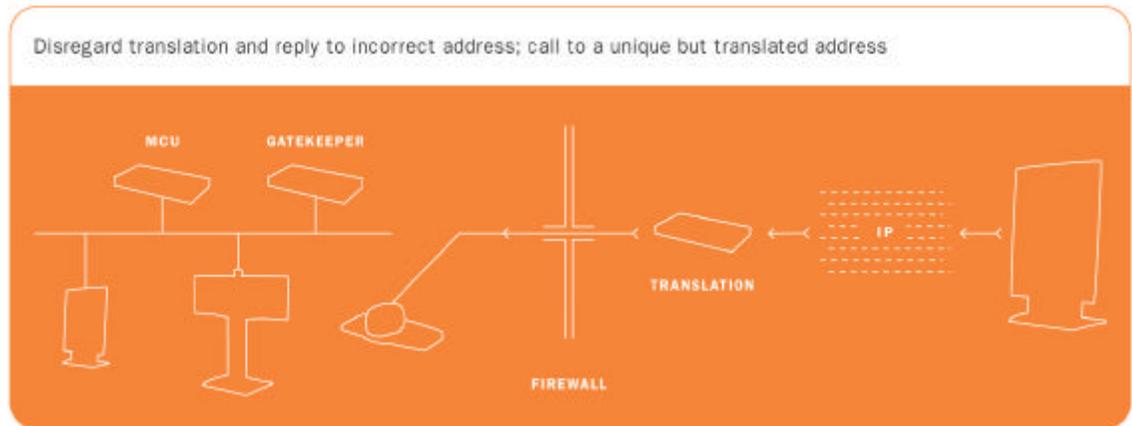
Unfortunately, this practice is an obstacle to IP communication protocols. A device that wants to initiate a call needs to know what address and port to send it to. There is a well known port for call signaling, but if many devices are sharing a single public address, there is no way to determine for which particular device the call is intended.



Securing unique public addresses for all voice and multimedia devices is impractical and not secure

In order to enable the traffic to flow, enterprises are faced with the prospect of securing unique public addresses for all their voice and multimedia devices. This is impractical and not secure.

Furthermore, address translation typically applies to packet headers, but not to the protocol within the packets. Upon receipt of a packet from another private network space, a device will discard the public address on the header, and attempt to respond to the private address within the packets. This, at best, causes a connection to a device with that address in the recipient's network.



Again, enterprises face the prospect of assigning unique addresses to devices so that they do not get translated en route. Alternatively, enterprises can upgrade their equipment to recognize the communication protocols and translate addresses within the packets as well as in the packet headers. However, this only solves the problem if all enterprises upgrade critical equipment to handle all of the popular communication protocols. Waiting for all enterprises to upgrade is a major obstacle to the adoption of voice and video over IP, and an obstacle that arises again whenever protocols change or new protocols emerge in the marketplace.

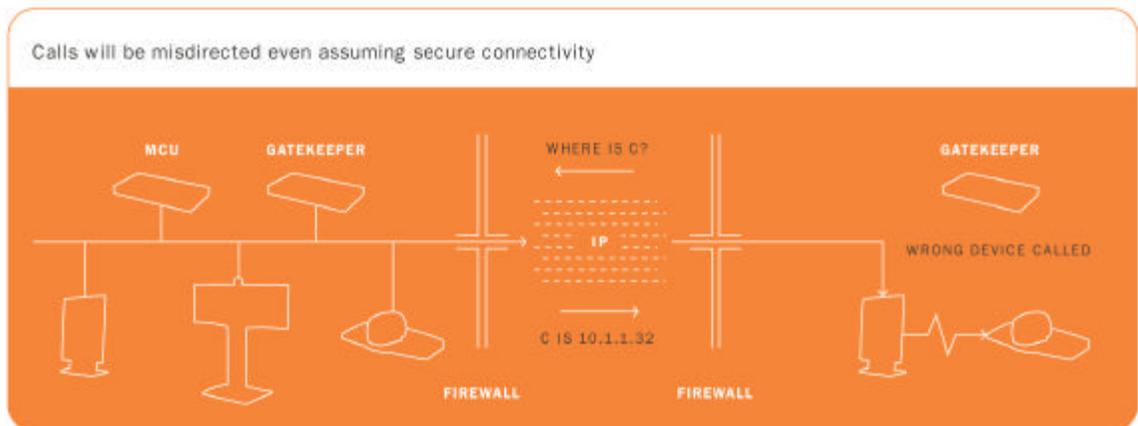
It would be preferable for translations to be compensated for without any upgrade to the communication devices or the translation function itself. Only by working with existing equipment can communication services hope to be adopted quickly and cost-effectively. Not until this happens will visual communication truly be adopted for use outside the enterprise - speaking to suppliers, customers and telecommuters.

Finally, devices typically refer to network servers for information about other devices. For example, the H.323 protocol allows devices to refer to a gatekeeper for information on other H.323 devices.

In theory, network servers can inter-work to translate device aliases into network addresses. However, servers in different private address spaces will provide each other with address information that is of no practical use. To be useful, the information returned from a location information server needs to take into account the translation function that will be applied to device addresses as call traffic passes between devices. Alternatively, the translation function needs to be disabled and public addresses assigned to all devices, which is unacceptable.

EXAMPLE: Calls will be misdirected even assuming secure connectivity

For example, if two enterprises both use the commonplace 10.1.1.* addressing schema for their private devices, any address information passed between the enterprise network servers will appear to be an address for a local private device rather than a device in another enterprise's private network.



Calls will therefore be misdirected even assuming that secure connectivity can be established between the two private networks. To allow communication, administrators need to assign addresses that do not get translated, such that the information provided by network servers is useful beyond the private network. This is an unwelcome compromise to security best practices. Alternatively, costly upgrades need to be implemented throughout the communication network.

What is needed is a solution that maintains the security advantages of address translation without upgrading the translation devices or network servers to understand the protocols. An upgrade solution is costly and needs to be repeated for all enterprises for each protocol as often as the protocols change.

TANDBERG's Expressway solution enables address translation without costly equipment upgrades

TANDBERG Resolves Address Translation Challenges

Again, TANDBERG provides a practical, patent pending solution to address translation issues. TANDBERG's Expressway solution enables multiple devices to continue to share a single public address, and avoids costly equipment upgrades.

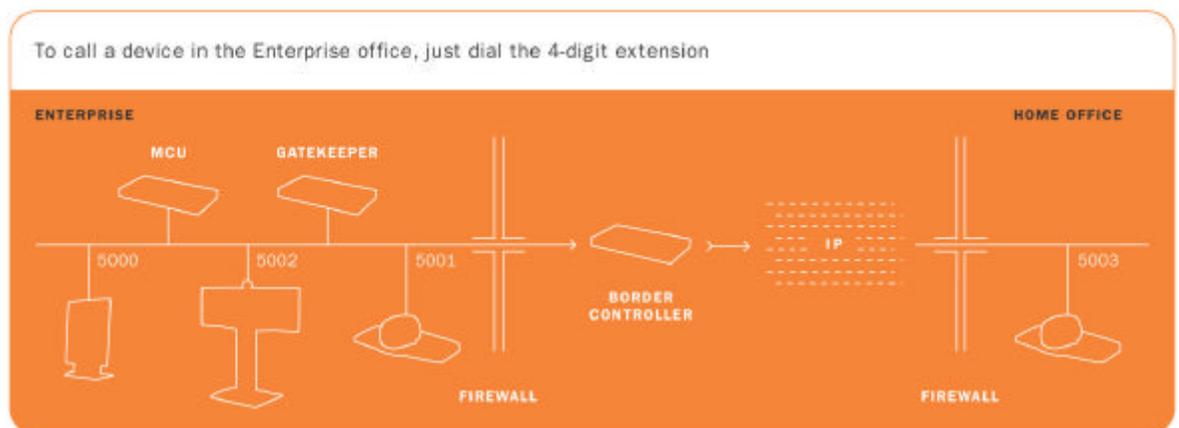
As with the firewall solution, the key is that TANDBERG places a component on each side of the address translation function. In fact, the TANDBERG solution is effective even if communication traffic passes through multiple address translations. It is also effective if the translator is integrated with the firewall.

The solution has two elements: a secure path and a media relay.

Solution creates a secure path for signal and control and a media relay

- The secure path uses a TCP connection that is subject to address translation in the normal manner. The TANDBERG Gatekeeper or MXP endpoint is assigned a public address when it connects to the server. This assignment is temporary, but remains valid for as long as the two components are connected. This secure connection carries all call control traffic.
- The media relay element uses temporary UDP connections. The traversal method allows the creation and deletion of these connections as required by calls, the association of particular connections and translations with particular calls, and the efficient relay of media over the connections.

The net result is that private network devices transmit and receive data to and from the Gatekeeper or other endpoints, external devices transmit and receive data to and from the Border Controller, and the secure path and relay elements provide secure traversal of the infrastructure between the Gatekeeper (or MXP endpoint) and Border Controller.



Complete transparency and total anonymity for the devices

Neither device can detect that calls are being redirected. Neither can they detect that the other device is in a different network space, and neither can determine the true address of the other. Each device thinks that its local end of the TANDBERG solution connection is actually the other device. TANDBERG therefore provides complete transparency and total anonymity for the devices.

Dialing Plans

TANDBERG Extends Address Space into the URI Domain

Support for URI dialing -between different private address spaces using email style URIs

Extending the Expressway solution one step further, TANDBERG provides support for URI dialing. In a typical network setup, servers in different private address spaces will provide each other with address information that is of no practical use because, as mentioned previously, the information returned from a location information server needs to be able to uniquely identify the specific location or domain within which the device being called is located.

However, if one identifies each Border Controller using a unique domain name and the address of the border controller is registered in DNS by an administrator, the result will be that the public address of that Border Controller permeates throughout the entire Public Network cloud. This mechanism thus permits dialing between different private address spaces using email style URIs.

How the call works

Accessing a public network's DNS services attached to a Border Controller at the call initiating side will result in a resolution of the address for the relevant Border Controller at the call recipient's side and hence direct its call to the correct Border Controller. Identical numbering plans at two separate locations are no longer an issue as location of local private addresses is identified by the domain name. This mechanism permits secure, transparent calling between all organizations who are utilizing Expressway and who are sharing the same network, e.g. the public Internet.

Example: Dialing from 1234@companyA.com to 1234@companyB.com requires only that the companyA system dial the full 1234@companyB.com address. The Border Controller at companyA obtains a DNS resolution for companyB.com and sends its call directly to companyB's Border Controller requesting to connect to the system known to CompanyB's Border Controller by the alias 1234.

EXAMPLE:
Dialing from
1234@companyA.com
to
1234@companyB.com

A further extension of this mechanism allows an individual email address, as well as a phone number, to both become aliases for a visual communication system. If systems are able to register both E.164 aliases (numeric aliases) and H.323 aliases (alphanumeric aliases) with their local gatekeeper, then if John Smith has the email address john.smith@companyA.com and the phone number 202-555-1234 then dialing "john.smith@companyA.com" or "2025551234@companyA.com" would produce the same result, a secure, transparent connection to the visual communication system associated with John Smith. The TANDBERG Expressway solution will enable URI dialing for any H.323 device.

Conclusions

Visual communication is growing, and the widespread adoption of IP makes video, voice and multimedia communication more cost-effective. Until now, there was no easy way to reach outside the enterprise visually without less cost-effective ISDN services. Without secure and seamless traversal of firewalls and a common numbering plan, multimedia communication was isolated to internal environments or extended outside the organization with substantial security risks.

With solutions that are secure, scalable, deployable and manageable, TANDBERG has answered the firewall challenge with the Expressway solution for end-to-end IP. A simple solution integrated into TANDBERG endpoints, Border Controller and Gatekeeper, the Expressway solution is easily deployable and works with non-TANDBERG endpoints and infrastructure. In addition, no features are lost, and it works with H.264, MPEG4 audio, encryption and more.

For more information on TANDBERG's Expressway firewall traversal solution, contact:

TANDBERG WORLD HEADQUARTERS

Philip Pedersens vei 22
1366 Lysaker, Norway
Tel: +47 67 125 125
Fax: +47 67 125 234
Video: +47 67 117 777
E-mail: tandberg@tandberg.net

200 Park Avenue, Suite 2005
New York, NY U.S.A. 10166
Tel: +1 212 692 6500
Tel: +1 800 538 2884 (toll free in the U.S.)
Fax: +1 212 692 6501
Video: +1 212 692 6535
E-mail: tandberg@tandbergusa.com