VCON
VISUAL COMMUNICATIONS

Overcoming NAT and Firewall Issues

1 CLICK AWAY
From Being There.

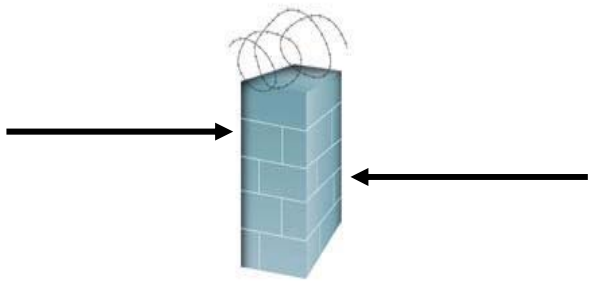
Ultimate Objective Checklist

- ☑ Security
- ☑ Connectivity
- ☑ Management & Administration
- ☑ Transparency (Seamless Use)

VCON
VISUAL COMMUNICATIONS

Firewalls and IP-Based Communications

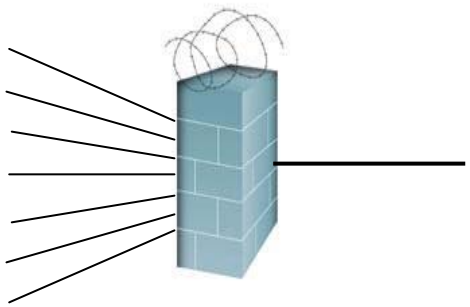
- **The role of a firewall is to apply RULES that provide some level of network security**
  - Protocols allowed (inbound versus outbound)
  - IP addresses (from-to)
  - Port usage ("well known" versus application-specific)
- **When a session is initiated from "inside" the firewall, usually returned data streams to the originating IP address and port are allowed**
  - However, H.323 allows for a dynamically-selected and very wide range of ports to be used for these return streams



VCON
VISUAL COMMUNICATIONS

NAT and IP-Based Communications

- **Network Address Translation (NAT) allows many private (non-routable) IP addresses to share fewer (even a single) public IP address**
  - Outbound connections allowed, but the IP address in the packet header gets translated
  - Unfortunately, there is also IP address information in the payload of voice/video over IP packets, which does not get translated
  - No way to initiate connections from the outside because the IP addresses on the inside are "invisible"
- **Network Address Port Translation (NAPT)**
  - Conflicts with "well known" ports that are used for voice/video over IP



VCON
VISUAL COMMUNICATIONS

Messages Involved

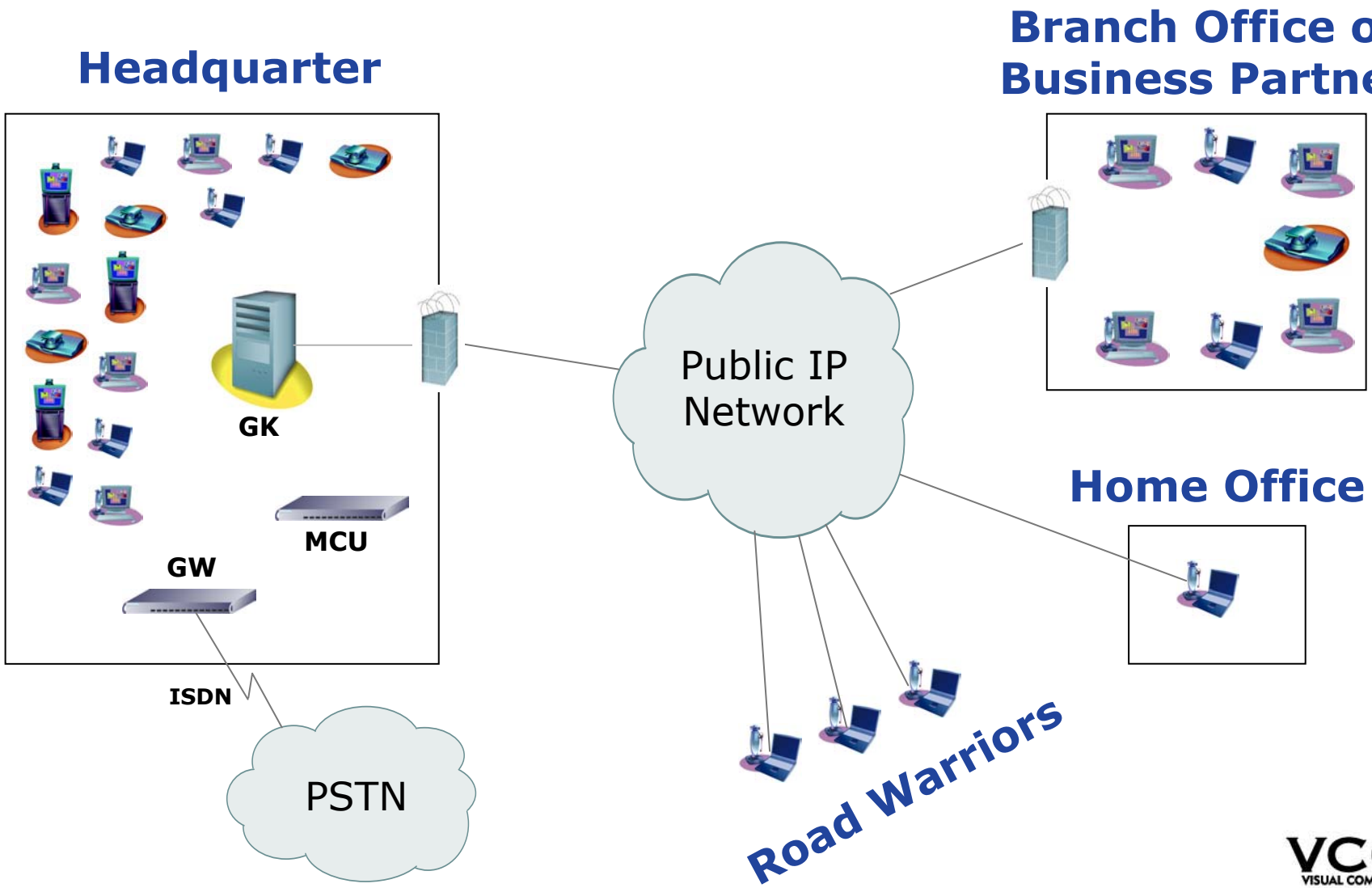
- Gatekeeper registration
- Call setup messages
- Call signaling
- Keep-alive messages
- Audio and video media streams
- Neighbor gatekeeper messages
- Remote device administration
- Far-end camera control

UDP & TCP Streams

Static & Dynamic Ports

VCON VISUAL COMMUNICATIONS

Each Location Provides a Different Challenge



VCON
VISUAL COMMUNICATIONS

VCON
VISUAL COMMUNICATIONS

Solution Alternatives

1 CLICK AWAY
From Being There.

Client/Endpoint-Based Deployment Alternatives

- **Place voice/video endpoints outside the firewall with public IP addresses**
  - Might be OK for settop appliances, but not desktop systems
  - Consumes a public IP address for each endpoint
- **NAT IP address mask**
  - Allows the endpoint to embed a routable, public IP address in the IP packet payload
  - Requires static mappings of IP addresses for voice/video endpoints
- **Port range configuration**
  - Directs the endpoint to use specific UDP and TCP ports instead of a wide dynamic range
  - Requires these ports to be opened in the firewall and not subjected to port translation

VCON VISUAL COMMUNICATIONS

Client/Endpoint-Based Deployment Alternatives

- **Port pinholing**
  - Returned streams use the same ports as the original incoming streams
  - Requires calls to be initiated from inside the firewall
  - Does not work when both endpoints are behind a firewall/NAT
- **VPN**
  - Commonly used for home office workers already, but more complicated to use with branch offices
  - Encryption and authentication built-in
  - May give access to more network resources than desired

A combination of the above alternatives can be implemented. However, they typically only serve as a partial workaround solution.

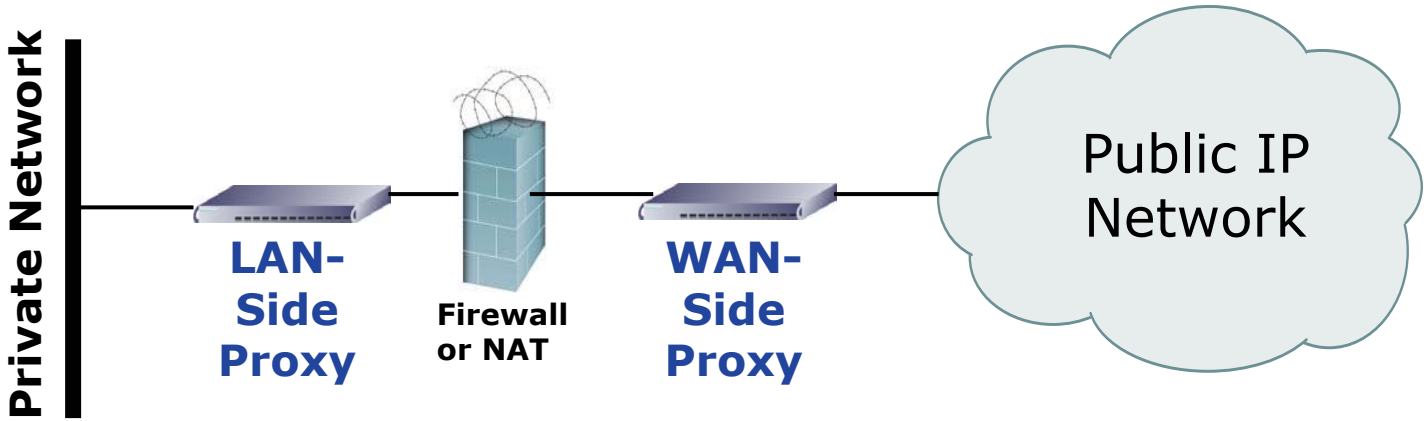
VCON
VISUAL COMMUNICATIONS

Server-Based Deployment Alternatives

- **Protocol-aware firewall**
  - Able to identify valid voice/video messages and dynamically act accordingly
    - Example: H.323 snooping allows ports to be opened for a validated session and then closed when done
  - Does not necessarily solve the inbound NAT connection problem or the dual-firewall/NAT problem
- **Application Level Gateway (ALG) or other proxy-based solution**
  - Protocol aware: only processes messages that it understands
  - Makes all resources appear local, while still requiring that traffic pass through the firewall for security
  - Commonly combined with encryption option for added security

VCON
VISUAL COMMUNICATIONS

Architecture of a Proxy-Based Solution



- Prevents direct connections between private and public network devices
- Firewall does not need to accommodate requests for dynamic or random ports
- All traffic still passes through the firewall

VCON
VISUAL COMMUNICATIONS

Other Considerations and Common Oversights

- **Don't forget about conferencing requirements with locations/devices not under your control**
  - Customer
  - Business partners
- **QoS provisioning: does the solution selected preserve it?**
- **Gatekeeper registration is still very much needed**
  - Networked gatekeepers (neighbored or hierarchical) require special considerations
- **Online directories still must be "visible" by all endpoints**
- **A solution that works for PC-based devices may not necessarily work for appliance devices (settop, GW, MCU)**
- **Scalability is important – what happens if the voice/video network grows dramatically?**

VCON
VISUAL COMMUNICATIONS

The VCON SecureConnect Solution

- **Able to securely proxy:**
  - Gatekeeper registration
  - Call setup messages & signaling
  - Media streams (audio & video)
  - Neighbor gatekeeper messages
  - VCON Interactive Multicast streams
  - MXM admin console login and remote device administration
  - Far-end camera control messages

- **Overcomes firewall and NAT hurdles without jeopardizing security**
- **Encryption option (DES, 3DES, AES)**
- **Highly scalable**

VCON
VISUAL COMMUNICATIONS

Summary

- **The technical issues of firewall/NAT traversal are complex, but not rocket science**
- **Choice of a workaround solution or a comprehensive server-based solution**
- **Interaction with the gatekeeper, management system and online directory is critical**

- ☑ **Security**
- ☑ **Connectivity**
- ☑ **Management & Administration**
- ☑ **Transparency (Seamless Use)**

VCON
VISUAL COMMUNICATIONS