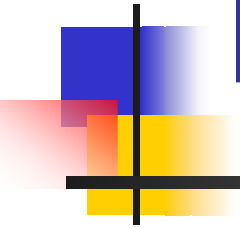
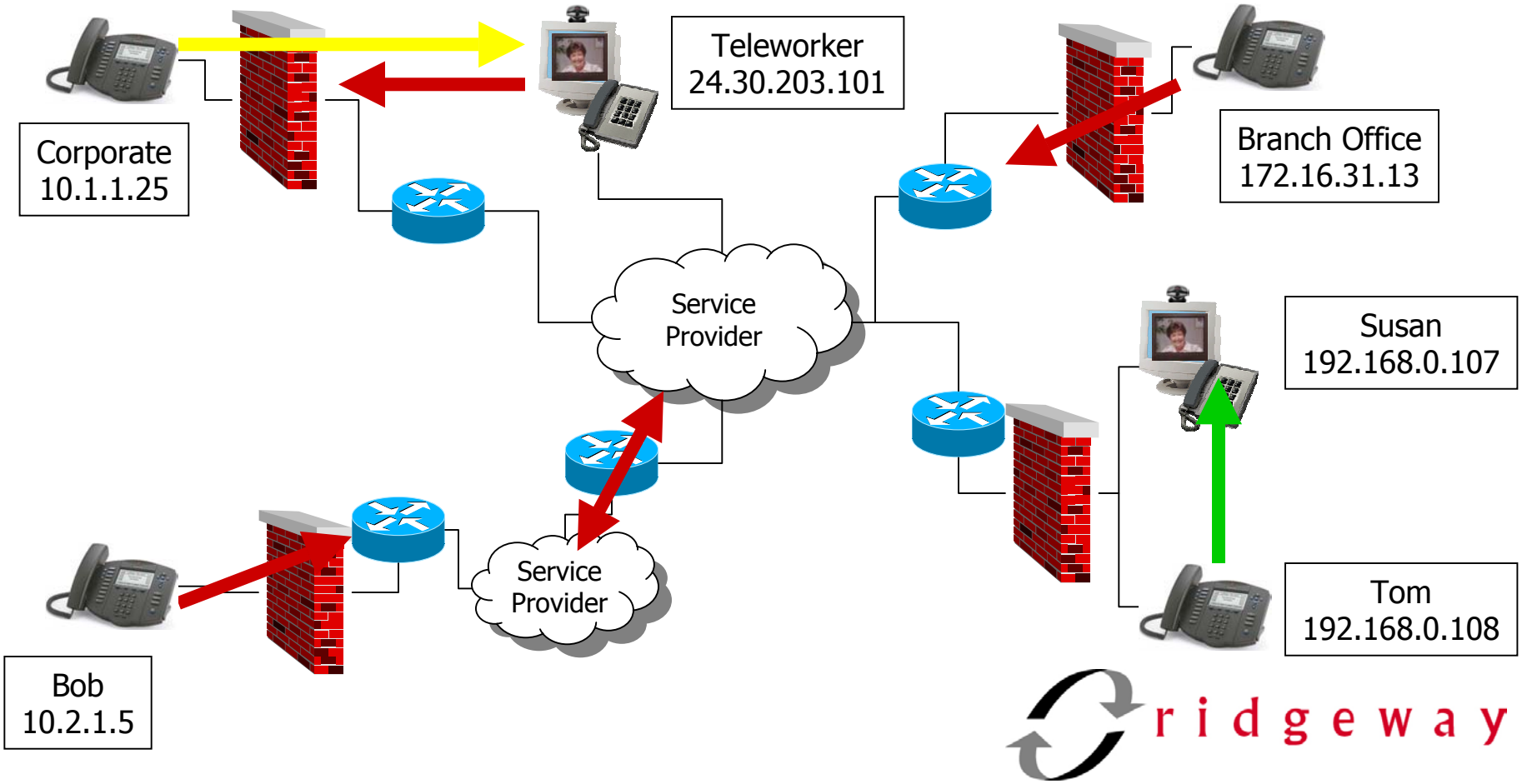


Boundary Traversal

Steve Davies

CTO, Ridgeway Systems & Software

Convergence – The Dream, The Reality

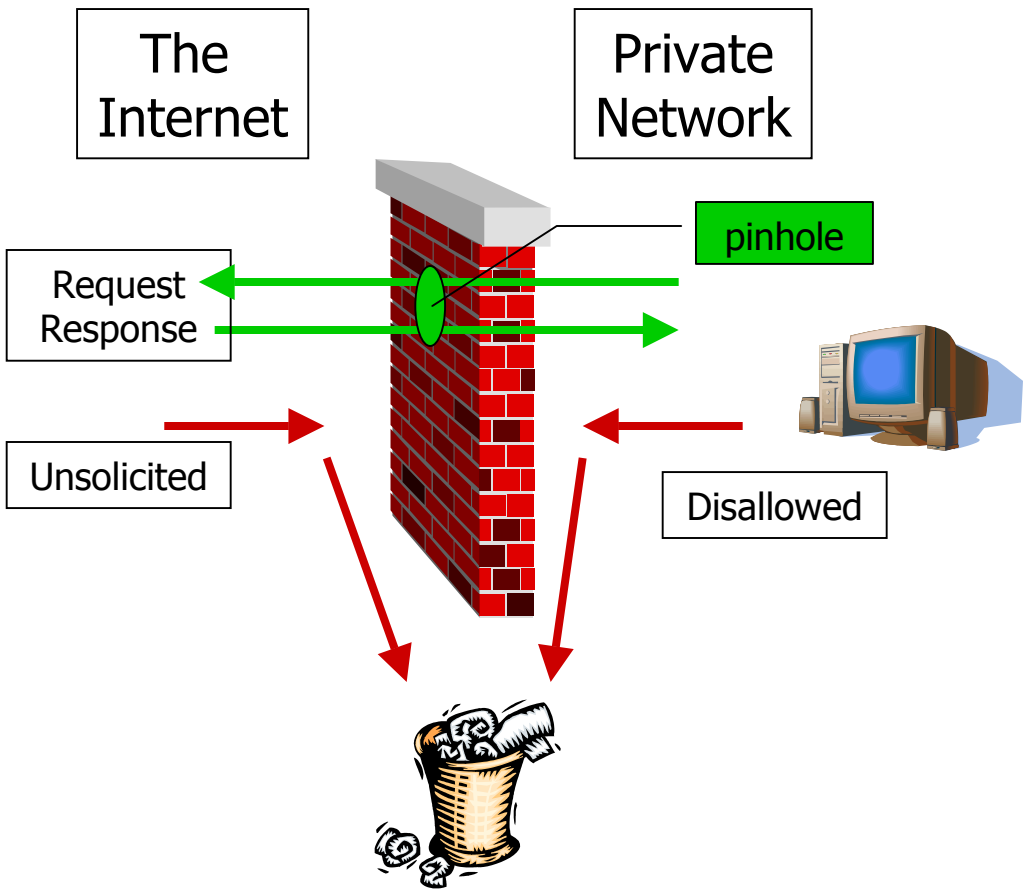


Why you should care about Firewalls and NATs

- Firewall and NATs protect your network
- Malicious attacks are increasing – over 70% organizations have experienced a security breach
- Network Address Translation (NAT) and Firewalls will **block your IP voice and video calls**.

ridgeway

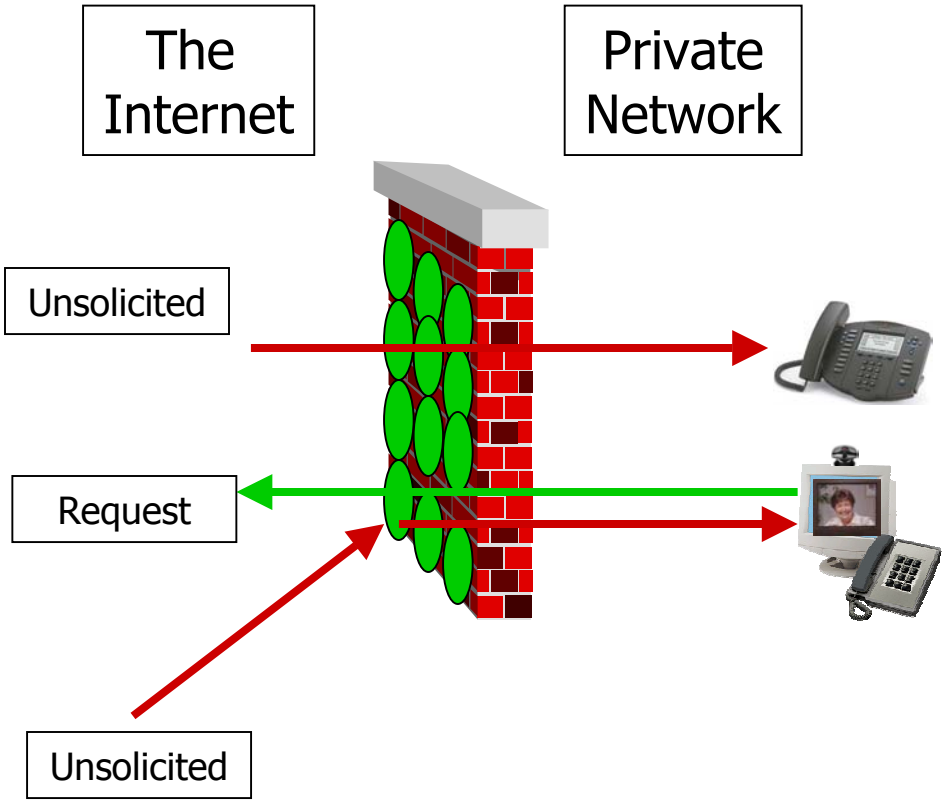
What is a Firewall?



- Separates and "Protects" the Private Network from the outside world.
- Examines every packet that goes in to or out from the enterprise.
- Typically blocks all unsolicited inbound packets
- Think of a mail room clerk filtering your inbound and outbound mail

ridgeway

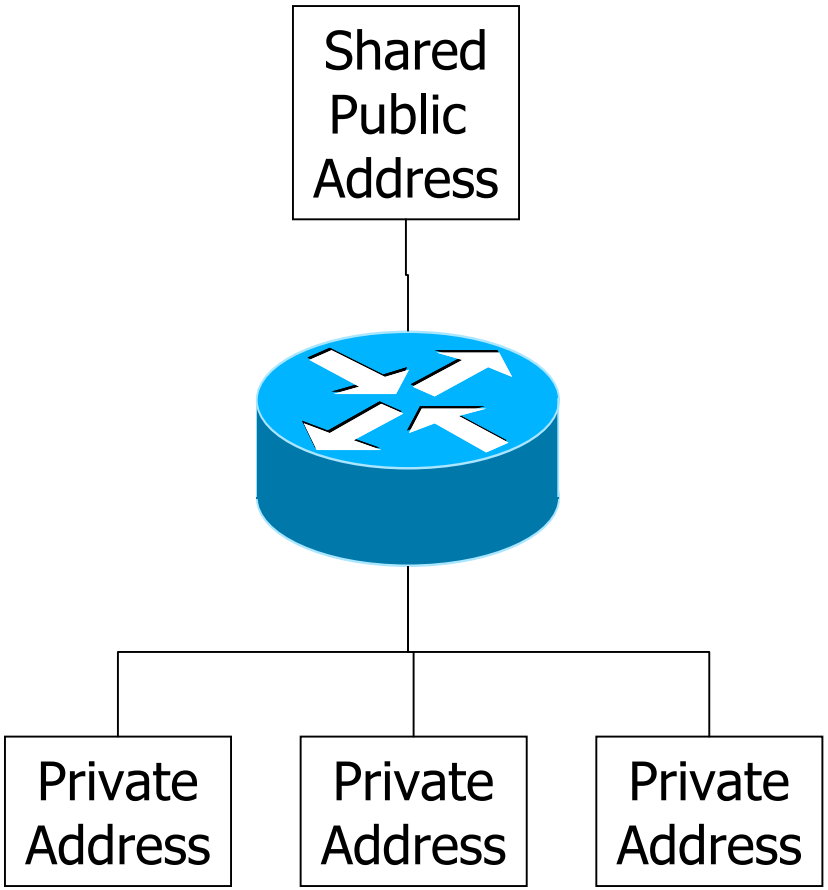
Firewalls and VoIP!



- Dynamic Ports implies a lot of pinholes!
- Need Inbound Connections
- Don't know who the sender is. The pinhole is open for everyone!

ridgeway

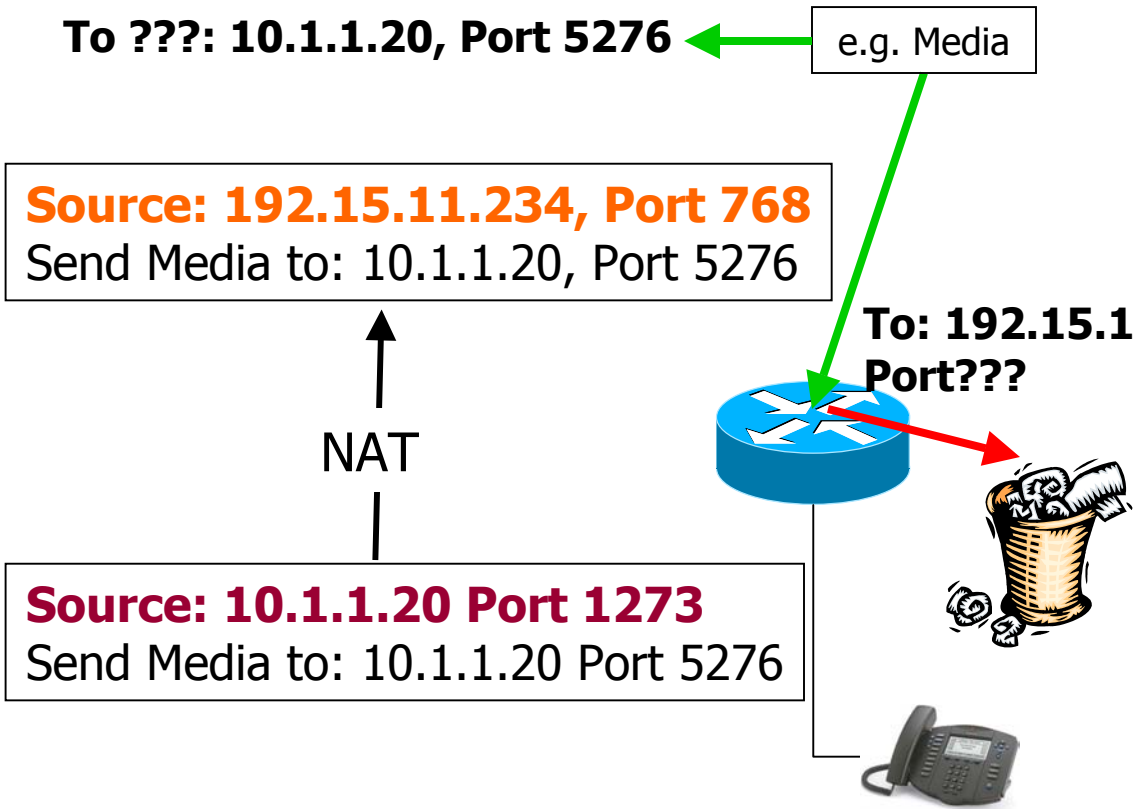
What is NAT?



- Network Address Translation
- Allows multiple users/devices to share a single public internet address
- Implemented within the router/firewall
- Think of it like a pre-DID PBX with a public trunk number and private extensions

ridgeway

NAT and VoIP!



- Can't directly address individuals uniquely
- Prevent Inbound Connections
- NATs don't change the 'protocol addresses'!

ridgeway

The Solution

- **Boundary Traversal**
  - Main Ingredient is the VoIP ALG (Application Level Gateway – H.323, SIP, … intelligence)
- **Requirements**
  - Resolve IP address issues
  - No compromise to security

ridgeway

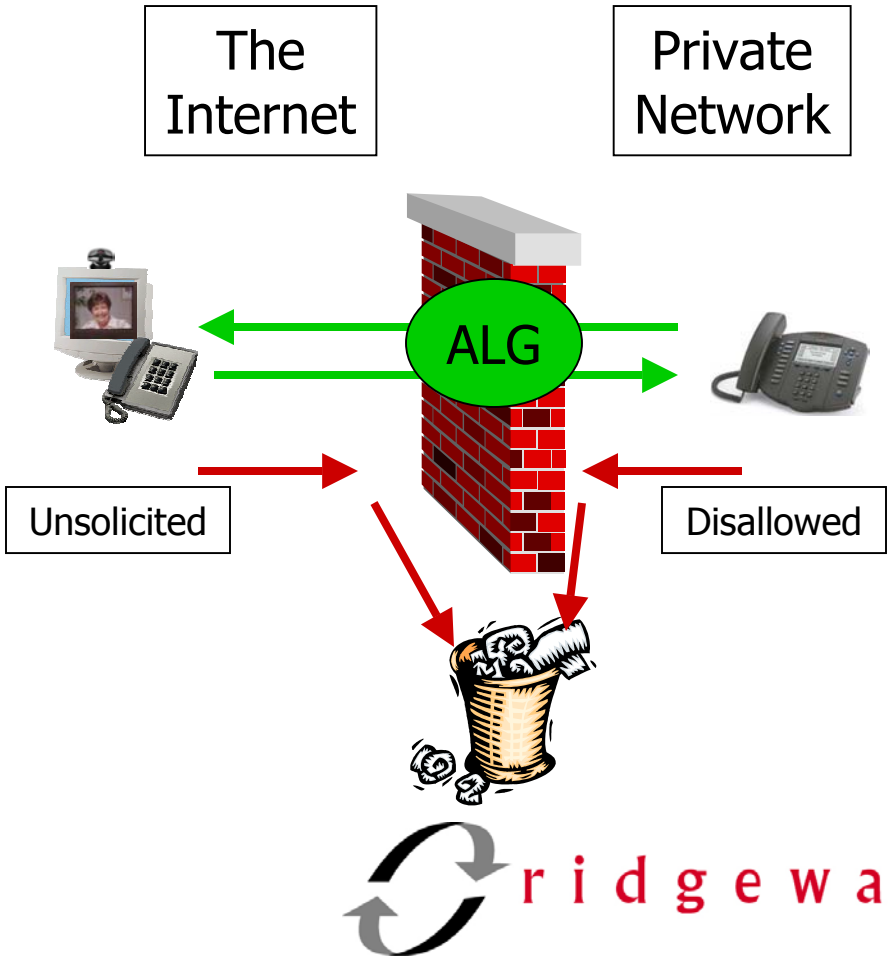
Boundary Traversal Solutions

- Traditional Approach: Upgrade each boundary
  - Firewall Upgrade
  - Companion Firewall
- Theoretical: In an ideal world
  - IETF Standards – MIDCOM
- New: Multi-boundary traversal

ridgeway

Firewall Upgrade/Replacement

- An ALG (Application Level Gateway) adds application intelligence inside the firewall/NAT
- The ALG performs the address manipulation on the protocol messages and becomes the NAT
- The ALG dynamically creates 'pinholes' for the dynamically created sessions (i.e audio)



ridgeway

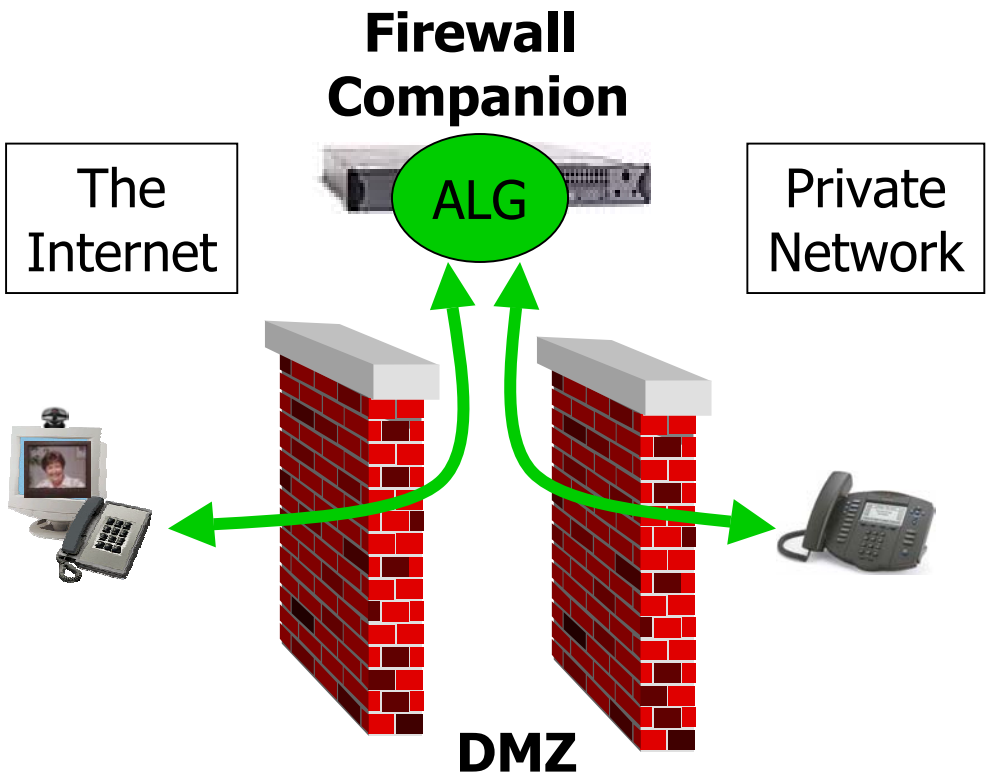
Firewall Upgrade

- Benefits
  - No additional devices
- Issues
  - Each and every boundary needs upgrading – a single boundary solution for single application
  - Not applicable to Centrex solutions - needs a local Gatekeeper/SIP Proxy to handle incoming calls
  - Replacement may be needed
  - Equipment may be "out of reach": physically, politically, or intellectually
  - Concern over the 'size' of the pinholes created
  - Firewall is mission critical component
  - Not encryption compatible

ridgeway

Companion Firewall

- An ALG is deployed in the DMZ with a public IP address and an internal IP address
- The external and internal FWs are programmed with forwarding rules
- NAT is disabled – the ALG performs this function

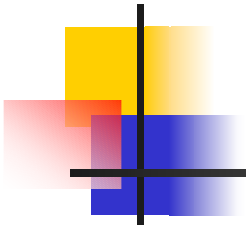


ridgeway

Companion Firewall

- Benefits
  - Compliments existing firewalls
- Issues
  - Needs a DMZ and an additional IP address
  - Single boundary solution – only works if no network based NATs
  - Requires a Gatekeeper/SIP Registrar/Proxy
  - On-board GK/Registrars pose a security risk
  - Local NATs must be disabled
  - Requires trusted/hardened solution

ridgeway

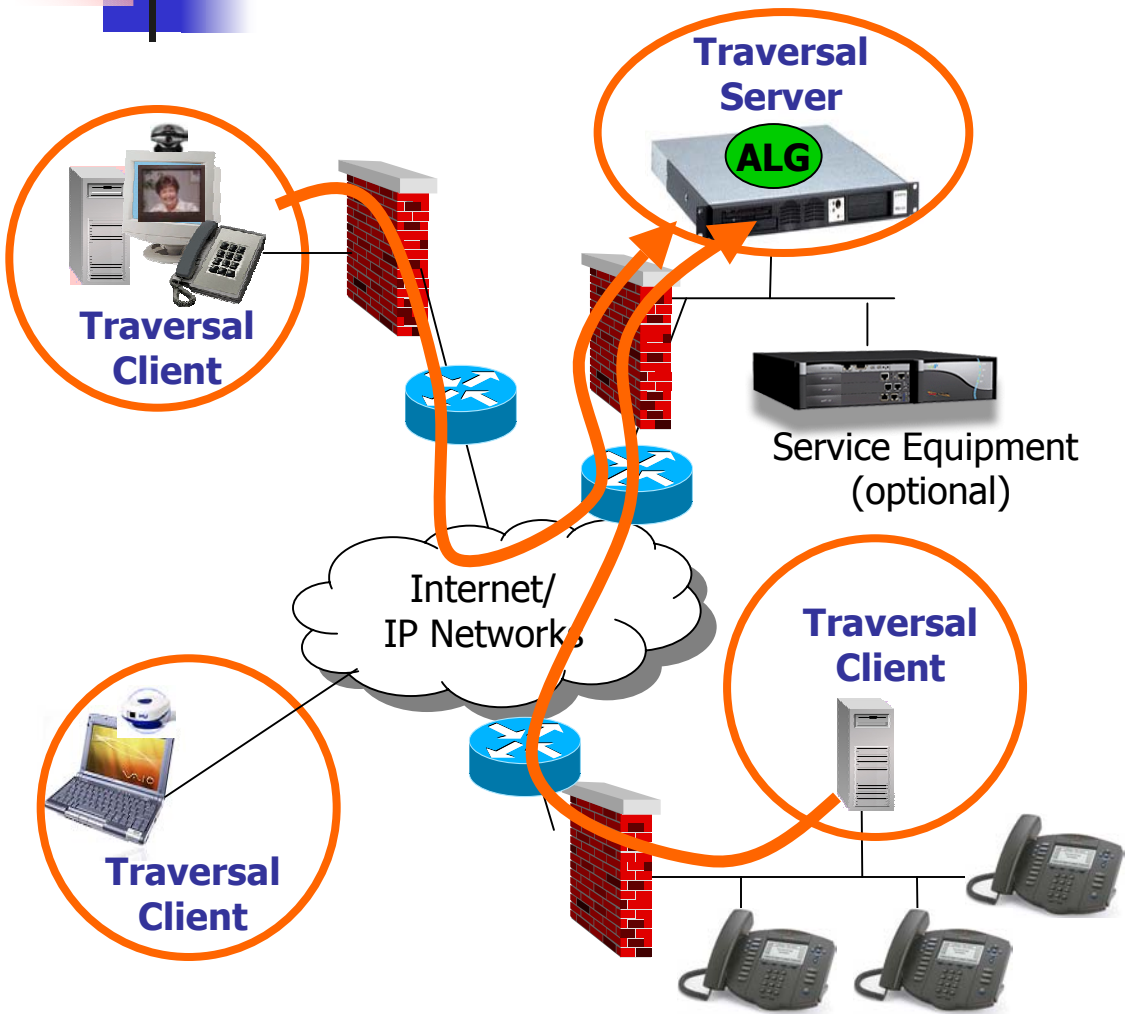


MIDCOM

- IETF Working Group trying to specify a standard:
  - Being going for over 2 years
  - Trying to define a firewall control protocol
  - Shackled by idealism and politics
    - NATs are bad
- Results to-date:
  - STUN – Interim solution to allow endpoints to discover their NAT'd address
    - Requires terminals change
    - Doesn't work with firewalls

ridgeway

Multi-boundary Traversal



- Place Traversal Server at "reachable address"
- Place Traversal Clients in private networks
- ✓ Firewall Compatible:
  Client-Server form a transparent 'real-time outbound tunnel' on restricted ports
- ✓ NAT Solution:
  ALG performs address resolution

ridgeway

Multi-boundary Traversal

- **Security Advantages**
  - ✓ Client authenticates with Server
  - ✓ Firewall can be programmed with very restrictive rules.
  - ✓ Client always connects (TCP and UDP). No inbound traffic is allowed unless outbound connection made.
  - ✓ Enterprise IP address + private network addresses are completely hidden.
  - ✓ Encryption compatible

- **Other Benefits**
  - ✓ Very easy to deploy - transparent
  - ✓ No upgrade to ***Mission Critical*** components required
  - ✓ Any number of Firewalls, NATs and VPNs may be traversed
  - ✓ No changes to existing protocols – Supports H.323, SIP, T.120, Windows Messenger, Mmusic-Co-media
  - ✓ Scales – from small to very,very large

ridgeway

Summary

- Convergence – VoIP and Video over IP present new connectivity and security challenges for enterprises and service providers
- Boundary Traversal solutions must provide connectivity without compromising security
- Multi-boundary traversal is the only solution that provides ubiquitous connectivity while adhering to existing security practices

ridgeway