H. 323 and firewalls: Problem Statement and Solution Framework

Author: Melinda Shore, Nokia

Presenter: Shannon McCracken

About this document

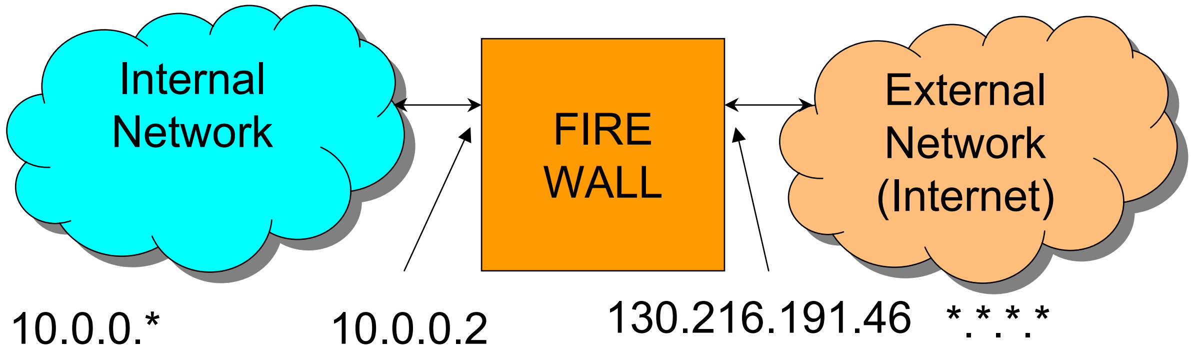
- It's an IETF Draft
  - Not an official standard
  - Expired July 2000.
- It describes the problems with trying to use H.323 through firewalls and NAT devices

What is H.323?

- Carries (video) phone over TCP/UDP/IP
- A telecommunications standard
- Rather complex protocol (compared with HTTP)
- Uses multiple TCP / UDP connections per call to carry the data

What is a firewall?

- Protects internal network from external threats by filtering traffic
- Can perform Network Address Translation (NAT)



Internal Network

FIRE WALL

External Network (Internet)

10.0.0.*

10.0.0.2

130.216.191.46

..*.*

The Combined Problem

- H.323 embeds connection addresses in signalling connection
- NAT causes a mismatch between IP header and H.323 stream
- End-to-end encryption prevents H.323 aware NAT rewriting the traffic
- Breaks IP address based authentication
- But we want encryption and NAT!

Further problems

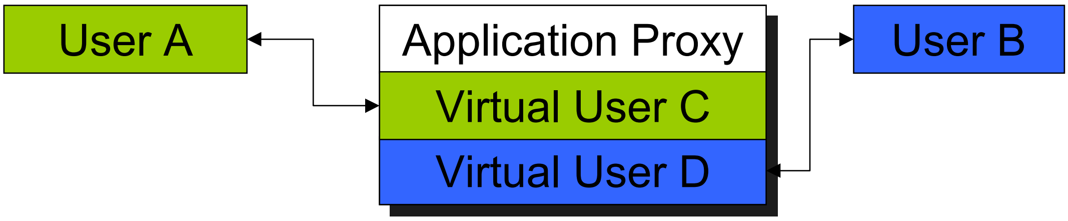
- RFC 2663: “NAT devices operate on the assumption that each session is independent.”
- Applications like H.323 that use control and follow-on sessions require gateways to interpret and translate the payload.
- Simple packet filtering will not work
- We need something more than just NAT or simple firewalls.

Possible solutions

- Stateful Inspection
- Application Proxy
- Virtual Private Network
- Circuit Proxies
- RSIP
- Firewall control protocol

Application Proxy

- Have a go-between that:
  - Is “an instance of the application (H.323)”
  - Runs on a trusted host
  - Like two phones taped together
- No end-to-end encryption
- Efficiency Considerations



Circuit Proxy / Firewall Control

- End clients open pinholes in firewall and communicate through them
  - For example, the SOCKS protocol
- End system must be aware of the circuit proxy—it’s not transparent.
- Works at the connection level (Circuit Proxy) or packet level (Firewall Control Protocol)

Session Initiation Protocol

- IETF Competitor to H323
- Uses SIP proxy and RTP proxy
- The same RTP that carries H323 data
- SIP proxy uses MCGP to open/close/control RTP proxy
- In effect circuit level

This slide is hidden and will not be presented.

Conclusion

- Firewalls and NATs are often difficult for some complex protocols
- H.323 alone can’t handle this problem.
- I think networks will end up having call servers for H.323 and similar protocols.

Questions?

- What applications (if any) need end-to-end encrypted signalling?

Another Question

- What to do about incoming connections?
- The author has not dealt with them