

# Proxy systems for H.323

8<sup>th</sup> SURA/ViDe conference

Atlanta, USA

March 2006

# The problem(s) (??)

- H.323 and Firewalls and/or NAT - Is this really a problem?
  - It is known for quite some time now
  - There are solutions available who:
    - a. Work
    - b. Don't work
    - c. Pretend to work
    - d. Are expensive
    - e. Are cheap
    - f. Are free

... and all Permutation of the above...

# The problem(s) (??)

- Complexity of media streams
  - Several sub-protocols for many different channels per sessions are used
- Dynamic negotiation of ports
  - H.323 uses some fixed ports, e.g. 1719, 1720, etc. (Session/Channel control)
  - Media channels are negotiated dynamically during the setup
    - Used port range:  $> 2^{10}$  &  $< 2^{16}$
    - ~ 4 to 6 ports per Session
  - How do you open ports if you don't know them before?

# The problem(s) (??) (cont.)

- NAT traversal
  - Private IP address will be converted into a public IP address, BUT IP address in H.323 packet is still private!!
  - How do you call an internal IP address??

[...]

H.225.0 CS

H323\_userInformation

h323-uu-pdu

T\_h323\_message\_body

h323-message-body: Connect (2)

connect

protocolIdentifier: 0.0.8.225 [...]

H245TransportAddress

h245Address: h245ipAddress (0)

h245ipAddress

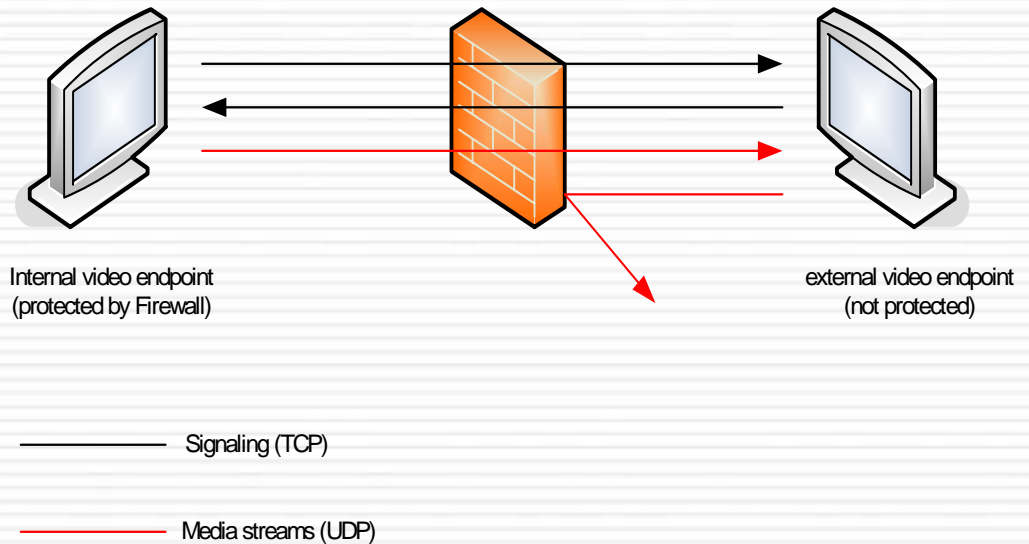
h245ipv4: 10.10.1.5 [...]

h245ipv4port: 4833

[...]

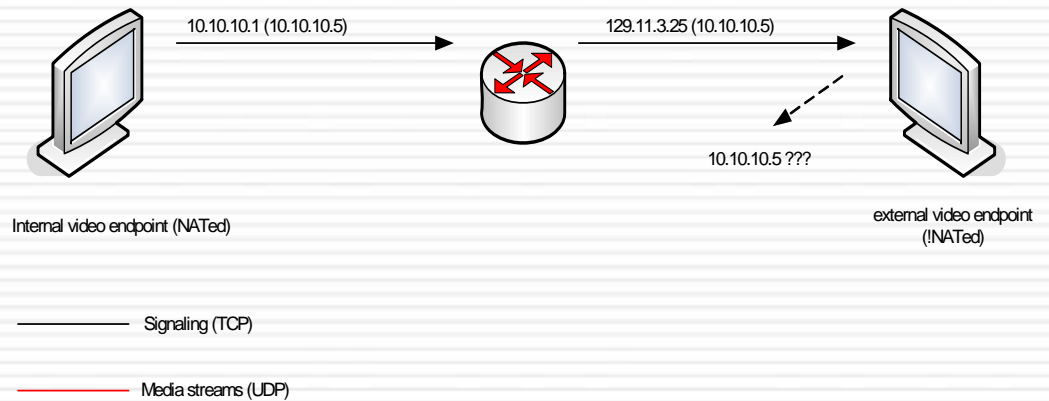
# What happens if...

- Dynamic port negotiation
  - Firewall blocks the traffic
    - Signaling (usually) goes through the FW
    - Media streams from ext. participant is blocked (*"Can you see me??"*)



# What happens if...

- NAT traversal
  - Private IP address still used in H.245 packets
    - The external H.323 device does not know 10.10.10.5

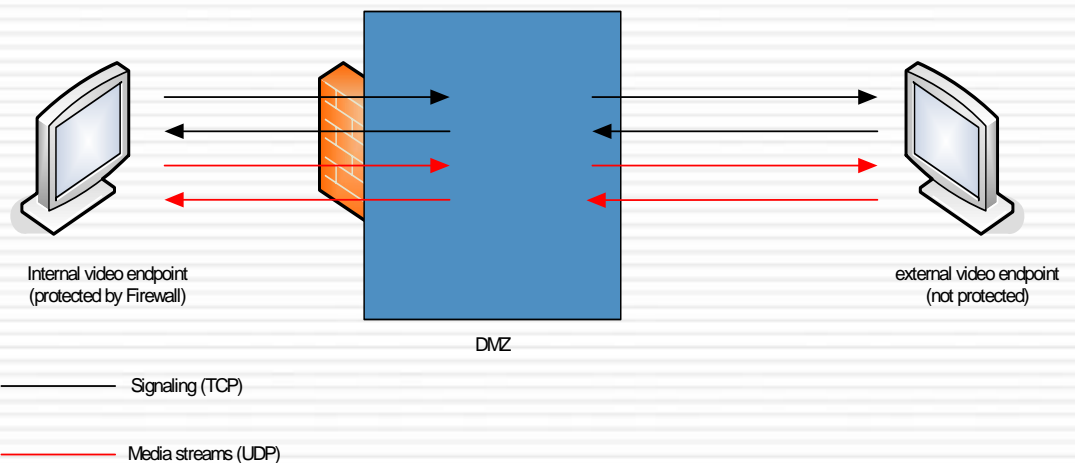


# Solutions...

- ...for NAT
    - Don't use NAT at all
      - Not an option for entities who only have a few public IP addresses
  - ...for the Firewall problem
    - Don't use H.323
      - ☹️ hmmm...not a solutions, since other protocols will also fail when a Firewall comes to play...
    - "Open Firewalling" – Open the Firewall for your H.323 systems
      - Possible for only a small number of systems (<5) {think about it twice if it is a PC based system}
- Use a H.323 proxy system

# H.323 proxy systems

- How do they work?
  - Act as a “man in the middle” (similar to a web proxy)
  - “Tunnel” ALL H.323 traffic (tcp/udp)
    - Only open the Firewall for the Proxy system
    - Should be located in the DMZ



# H.323 proxy systems

- How do they work? (cont')
  - A (ext|int) wants to call B (int|ext)
  - A dials B's E.164 {ENUM}
    - Lookup via GDS {DNS}
  - A receives B's proxy IP address and sends the setup request to B's proxy
  - The proxy identifies the E.164 {ENUM} to the endpoint and establishes a **new** call to B
    - Neither A nor B know that the proxy is not A or B

# H.323 proxy systems

- What systems are available
  - Radvision ECS Gatekeeper/Pathfinder
    - >> Please talk to Radvision or some one who has experiences this system...that wouldn't be me
  - GnuGK
    - Widely used
    - Free!!
    - Support many authentication methods
      - DB authentication
      - H.350
      - ...
    - Supports GDS and since version 2.2.4 also ENUM
    - ...

# H.323 proxy systems

- Do they work?
  - Yes they do
- Are they used/Who is using one?
  - Max-Planck Gesellschaft, Munich, Germany
    - ~ 1000 calls per month, >>3.5TB traffic pa
  - UW, Seattle, USA
    - ~ 600 calls per month
  - Flinders University, Adelaide, Australia
  - SWITCH, Zurich, Switzerland
    - MOST Universities in Switzerland!!!
  - ....