Overcoming Firewall & NAT problems in H.323

QUESTnet 2005, Coolum, Australia
July 2005

aarnet
Australia's Academic and Research Network

Author: K. Stoeckigt (kewin.stoeckigt@aarnet.edu.au)

Outline

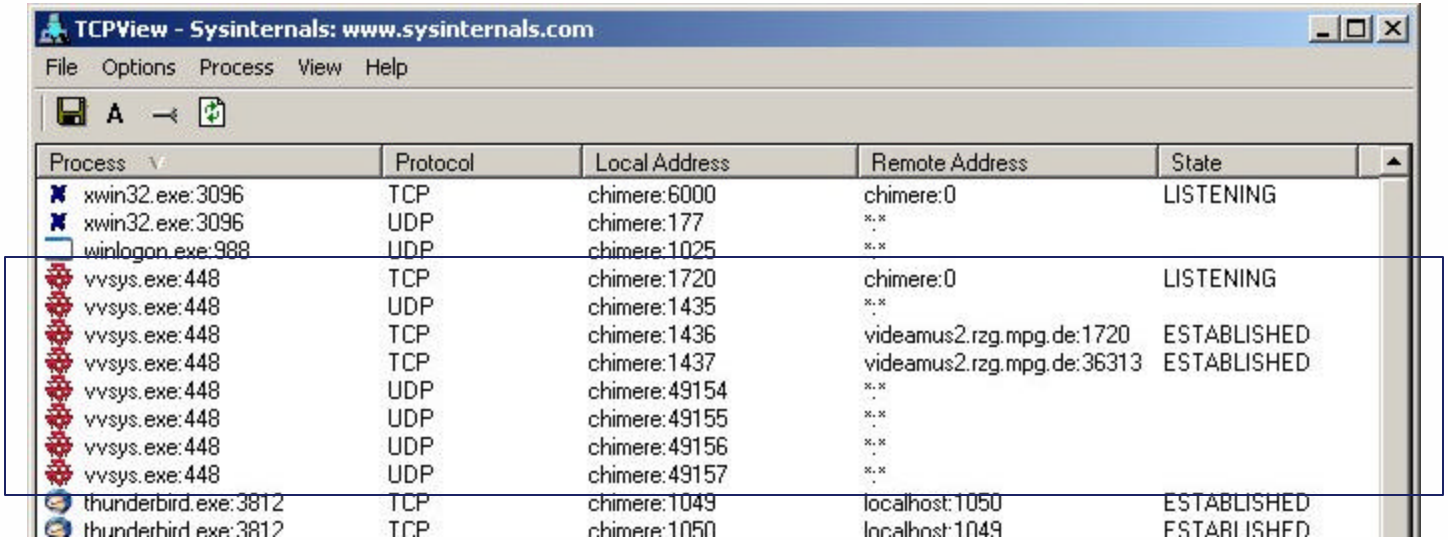
- The problem (…a brief description)
- Solutions
- The proxy – How does it work?
- What proxy to use?
- ?? Wait a second, this talk is supposed to say something about NAT…??
- Lets talk about security again
- Is this a reliable system?
- Resources/Additional information

The problem (…a brief description)

- Complexity and diversity of media/signaling streams
  - Use of several sub-protocols for each channel per sessions, e.g. H.225, H.245, Q.931, …
  - Complexity makes it hard to analyze (and debug!!)
- Dynamic allocation of communication ports
  - H.323 uses a few fixed ports, e.g. 1719, 1720 (for signaling only)
  - The ports for the audio/video streams are dynamically negotiated during the setup process
    - Used port range: $> 2^{10} < 2^{16}$
    - About 6 to 8 ports necessary per videoconference ? next slide
    - “How do you open ports on a firewall if you don’t know them before?”

The problem (…a brief description)

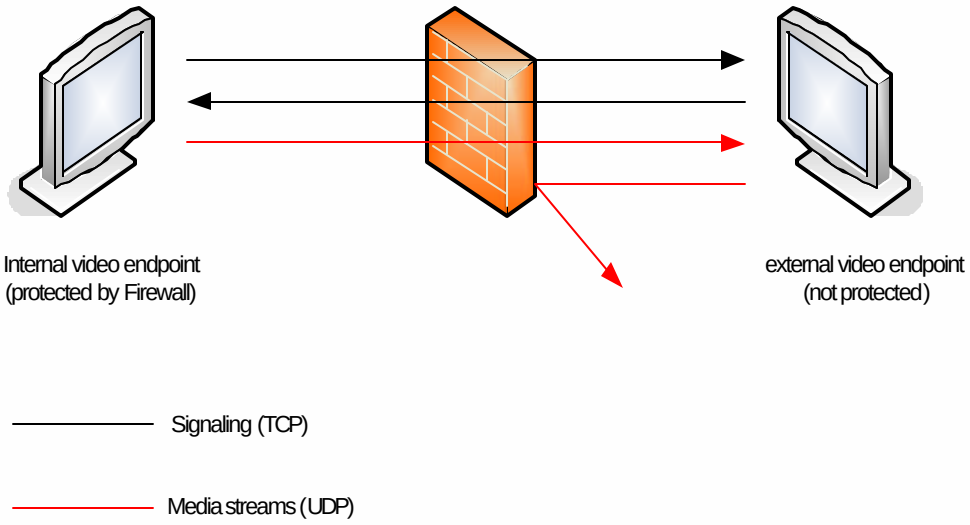
- Example: Screenshot below shows a videoconference using a Viavideo
  - 8 channels opened
    - 3 TCP (Setup, H.225, H.245)
    - 5 UDP (media streams (audio/video))



Author: K. Stoeckigt (kewin.stoeckigt@aarnet.edu.au)

The problem (…a brief description)

- The big picture, or what happens if…
  - Connection gets established (TCP)
  - The external video client receives audio and video
  - The internal video client receives nothing (black screen of silence)
    - Firewall blocks the incoming traffic



Author: K. Stoeckigt (kewin.stoeckigt@aarnet.edu.au)

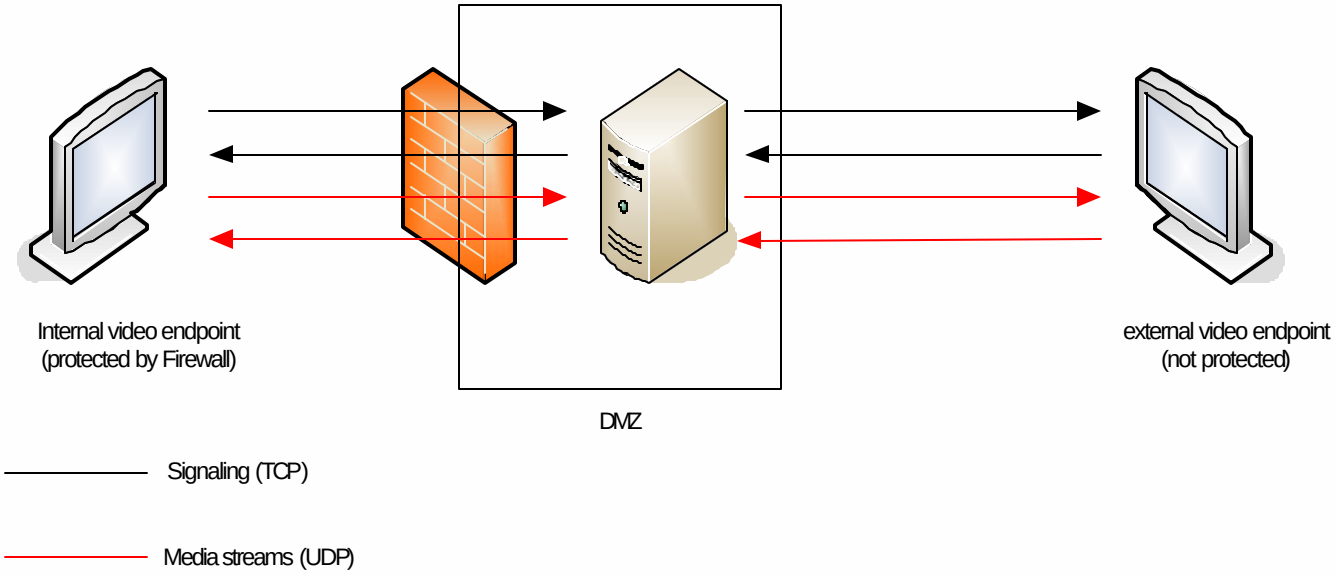
Solutions

- There are several solutions
  - Do not use H.323 ? ☹
  - "OpenFirewalling" ? ☹
    - Open the Firewall for all video endpoints
      - Only "acceptable" for a very small number of endpoints (1-5)
      - Only "acceptable" if only set-top systems
        - » Not "acceptable" if desktop systems only
  - Use of a commercial solution/statefull firewall
    - You get great support, but it still doesn't work
  - Use a proxy solution (this is the main topic of this talk ☺)

Author: K. Stoeckigt (kewin.stoeckigt@aarnet.edu.au)

The proxy – How does it work?

- The proxy acts as an intermediate systems
  - It takes all streams (TCP/UDP) coming from each endpoint and forwards it to the other (all streams are “proxied”)
  - The endpoints don’t know that they are not talking directly with each other



Author: K. Stoeckigt (kewin.stoeckigt@aarnet.edu.au)

The proxy – How does it work?

- How does it solve the Firewall problem?
  - The easiest way is to place the Proxy in the DMZ
  - If you don't have a DMZ, place the Proxy in the internal network, and just open the Firewall for this one IP address ? all other clients are still protected by the Firewall
- Is it secure?
  - No, no system which is connected to the Internet in one way or another is protected against attacks, hijack attempts, etc. beside that, YES it is secure (and its possible to make the structure even more secure ? a bit later

Author: K. Stoeckigt (kewin.stoeckigt@aarnet.edu.au)

What proxy to use?

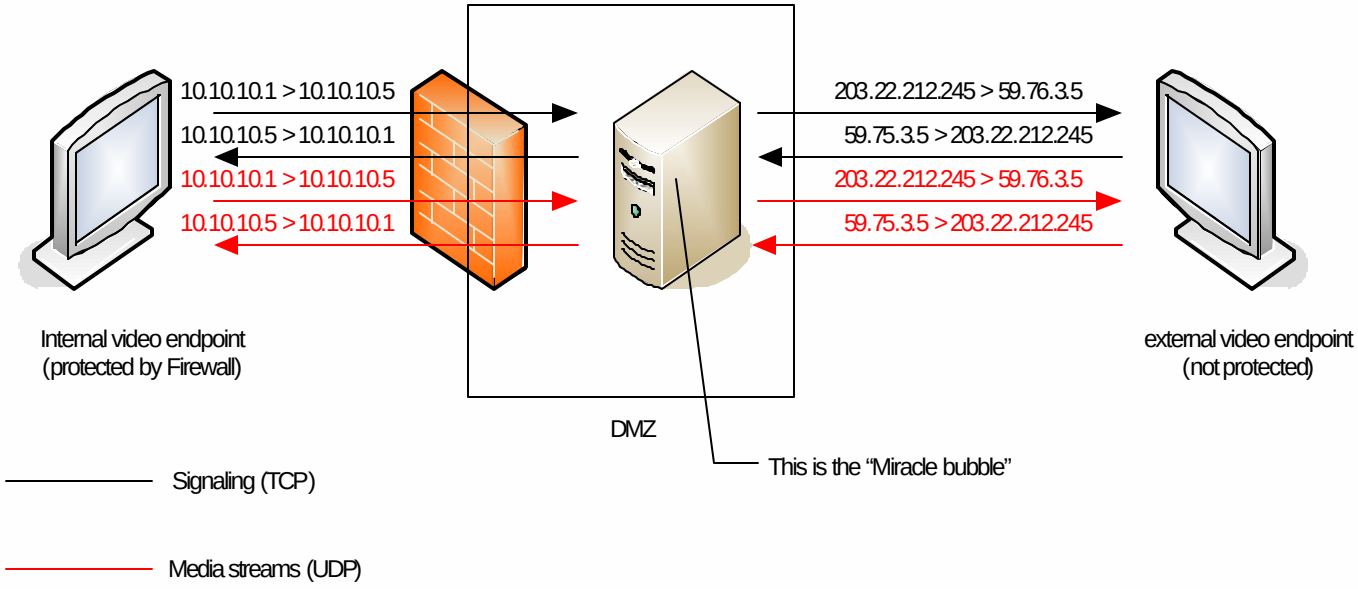
- AARNet decided to use GnuGK because:
  - Its free
    - It runs on Linux, Windows and Macs
  - It works
    - Many institutions, organizations and companies around the world use it, e.g. Max-Planck Gesellschaft (Germany), KFKI (Hungary), AARNet (Australia), Ohio State University (USA), and many many more…
  - It comes with a Gatekeeper
  - It is H.350 aware
    - It also supports several other authentication/authorization methods
  - Several other options
    - Proxy can be (partially) disabled ? standard Gatekeeper functionality
    - Port range limitation
    - Support for NATed endpoints
    - LoadBalacing
    - Can “proxy” basically every protocol (except SIP)
      - H.323, H.225, H.245, H.239, T.120, T.38, DuoVideo, People+Content, H.26x, G.7xx, AES/DES encrypted media streams
    - …

?? Wait a second, this talk is supposed to say something about NAT…??

- NAT
  - Network Address Translation (can) cause a lot of trouble, and it usually doesn't work with H.323
    - Problem: Translation of IP address private? public and vice versa
  - GnuGK supports NATed endpoints and it works
    - The internal endpoint talks only to the internal address of the GK/Proxy
    - The external endpoint "talks" only to the external address of the GK/Proxy
    - The GK/Proxy talks to each endpoint on the specific interface (internal/external) and the proxy "forwards" the streams
  - Does it work?
    - Yes, I installed two systems using GK/Proxy and NAT
      - University of Ljubljana (Slovenia), JET (UK)

?? Wait a second, this talk is supposed to say something about NAT…??

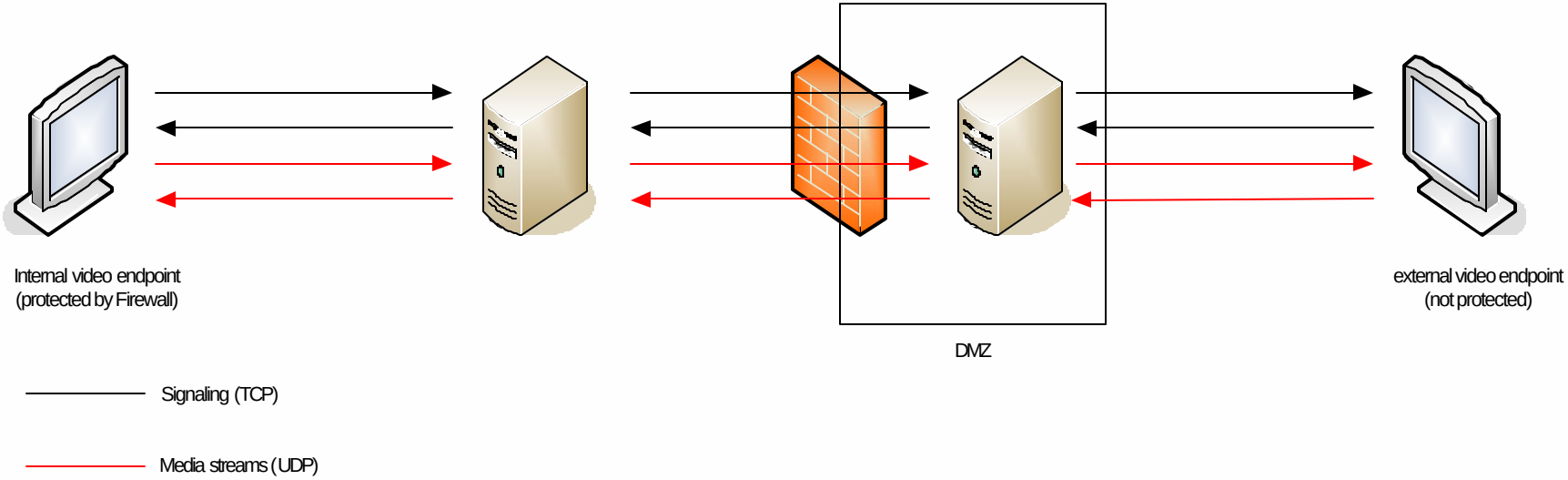
- Example: The GK/Proxy has two interfaces
  - Internal: 10.10.10.5
  - External: 203.22.212.245



Author: K. Stoeckigt (kewin.stoeckigt@aarnet.edu.au)

Lets talk about security again

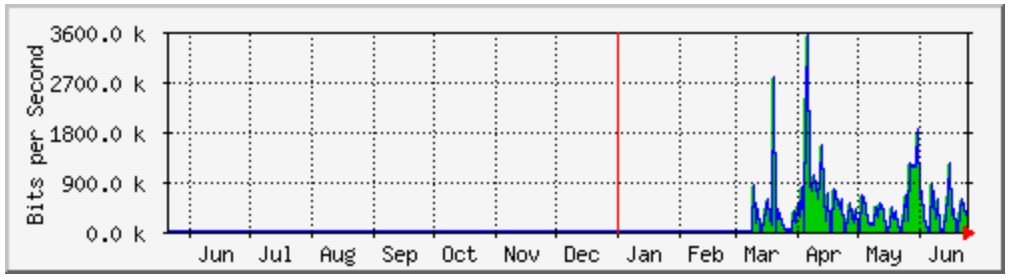
- The GK/Proxy solution in general is secure (as secure as any other system with a network connection)
- Is it possible to make the structure even more secure?
  - Yes – DualProxy
    - Only the two GK/Proxy IPs are allowed to bypass the Firewall, and only if they “talk” to each other



Author: K. Stoeckigt (kewin.stoeckigt@aarnet.edu.au)

Is this a reliable system?

- GnuGK proved to be very reliable
  - A few numbers (GK/Proxy of Max-Planck in 2004)
    - ~ 11000 videoconferences
    - >> 2TB of traffic proxied
    - Max. Bandwidth used at one time: > 60Mb/s
    - System availability: 98.63%
  - In 2005 (until 5/2005)
    - > 5500 videoconferences
    - ~ 2TB of traffic



Average per day: 3.5Mb/s

Author: K. Stoeckigt (kewin.stoeckigt@aarnet.edu.au)

Is this a reliable system?

- Hardware needed:
  - Depending on the amount of traffic, usually a modern standard PC should do the job
    - One of my first systems (was up and running for ~ 2 years (died of a disk failure))
      - PIII, 1.6GHz; 256MB Ram; SuSE Linux 7.3
    - Second system (still in use)
      - IBM x35; Quad Intel Xeon 2.4GHz; 1.5GB Ram, Redhat Linux 9

Resources/Additional information

- You should have joined my workshop yesterday ☺
- Use these slides
- New audio/videoconferencing website of AARNet (coming soon), http://www.aarnet.edu.au
- K. Stoeckigt, E. Verharen; "*Secure realtime audio/video communication – H.350, encryption and Gatekeeper/Proxy – using H.323*", 19th Apan Meeting, Bangkok, Thailand
- K. Stoeckigt; "*Setup and maintaining GnuGK*", 3rd TelOzConf
- K. Stoeckigt; "*Experiences with an OpenSource Solution for the H.323 Firewall issues*", Sura/Vide 6th annual video workshop, Indianapolis, USA
- K. Stoeckigt, "*H.323 videoconferencing*", NZNOG'04, Hamilton, New Zealand
- http://www.gnugk.org
- http://www.rzg.mpg.de/vc
- If you are interested in running a 'hands-on' workshop in your organization, University, etc. send me an email

Author: K. Stoeckigt (kewin.stoeckigt@aarnet.edu.au)


aarnet
Australia's Academic
and Research Network