



Computing Center of Max-Planck-Society and
Institute of Plasmaphysics

Traversing H.323 audio/video thru firewalls

Introduction of an OpenSource solution for
the H.323 firewall issue – A gatekeeper/proxy

EFDA Remote Participation Training & Workshop
KFKI Budapest, Hungary
May 2004



Outline of talk

- Where am I?
- The Problem – A short introduction
- GnuGK – The OpenSource solution
 - Why GnuGK?
 - How does it work?
 - A few features
 - ViDeNet & GDS
 - Authentication schemes
 - ...
 - Security aspects
 - Statistics
- Summary & Acknowledgement





Where am I?

- ~ 18000km south-east of Budapest
- Aotearoa – Land of the long white cloud (apparently its (almost) winter I see some gray clouds too)
- ...or better known as “Land of Mordor” or “Middlearth”
- Has the same size as Colorado
- I share the country with
 - 4 Million New Zealanders (...ok, there are some Aussis as well 😊)
 - 60 Million sheep





Where am I?



Auckland, New Zealand
36° 51' S, 174° 46' E



Budapest, Hungary
47° 30' N, 19° 5' E

When every thing goes 'arse-up', NZ'ers come out on top.





The problem – a short introduction

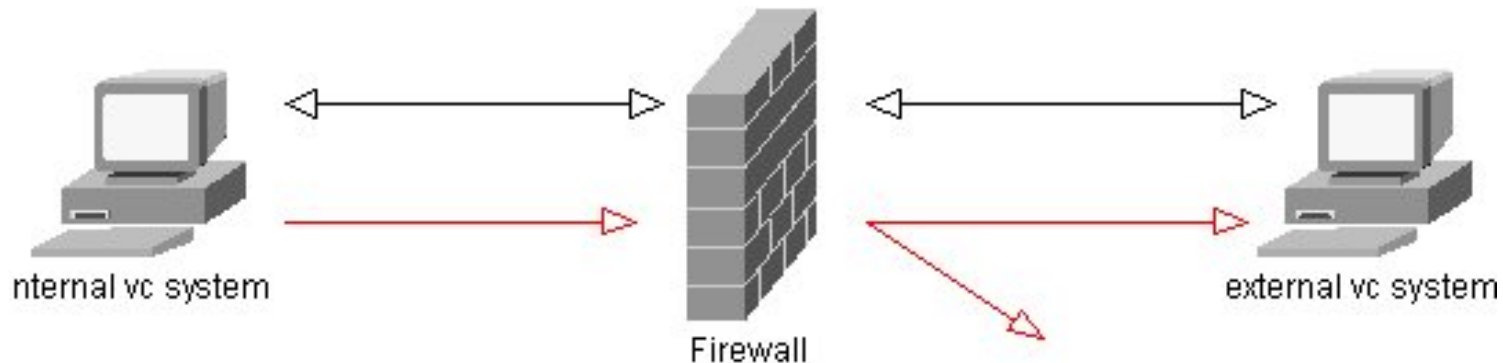
- Complexity of media streams
 - Several udp and tcp streams, e.g.
 - Q.931, H.245, H.225.0 are tcp (control) streams
 - Video and audio data are encapsulated in udp packets
 - Amount of data per second
 - A vc connection with 512kbit/s send approx. 90 udp packets with an average packet size of 750 bytes per second
- Dynamic Port allocation
 - H.323 uses a few fixed ports, e.g. 1719/tcp , 1720/tcp
 - Per connection approx. 6 to 8 ports needed
 - Ports are negotiated dynamically during the connection setup
 - Used port range: $> 2^{10}$ & $< 2^{16}$ (1024-65535)
 - How do you open ports (on a firewall) if you don't know them?





The problem – a short introduction

- “Blocked” communication or what happens if...
 - Setup (often) can pass firewall, but audio and video data are blocked
 - Standard scenario: external (unprotected) client gets audio and video, but internal (protected) system gets nothing





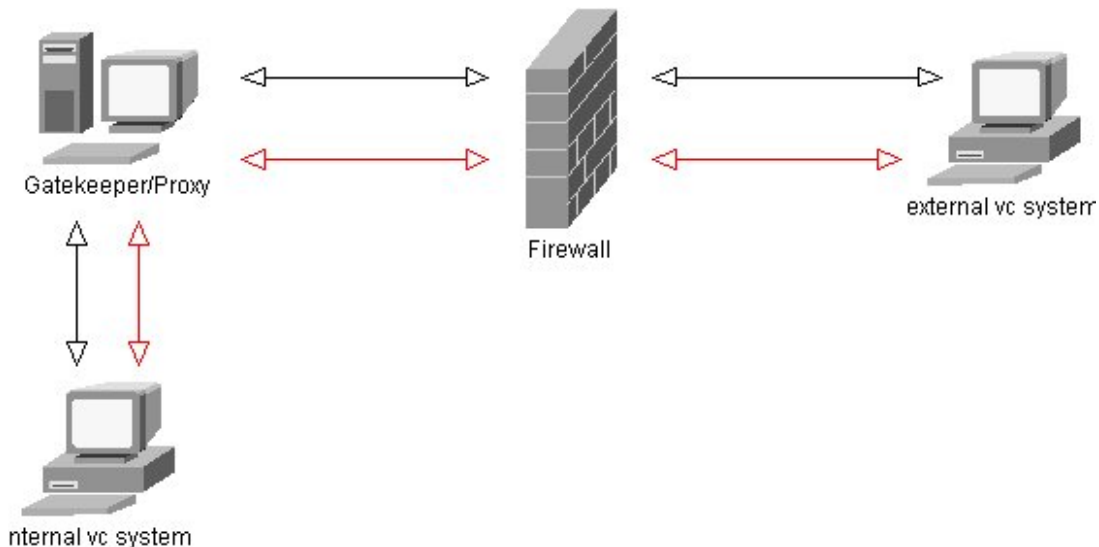
GnuGK – The OpenSource solution

- Why GnuGK?
 - It's free (GPL)
 - It runs on Linux...also free (Windows/Mac version also available)
 - It's a combination of a regular gatekeeper and a proxy
 - Fully H.323 v.4 compatible
 - 100% compatible to ViDeNet & GDS



GnuGK – The OpenSource solution

- How does it works?
 - Videoconferencing system communicates only with the proxy
 - ALL data, tcp data (control channels, etc.) as well as audio and video data (udp) are transmitted via the proxy





...just a few features...

- ViDeNet & GDS
 - GnuGK can be fully integrated into the existing ViDeNet & GDS (Global Dialing Scheme) structure → dialing of E.164 numbers rather than IPs
 - E.g. Gatekeeper in Garching has Zone 0049893299 → it is easier to remember an E.164 number: 00498932996004 instead of 130.183.2.60
- Authentication schemes
 - Many different authentication methods available, e.g. H.350 (LDAP), MySQL authentication, Radius authentication (incl. billing)





...just a few features...

- Proxy can be fully/partial deactivated, simply by setting

```
[Proxy]      [Proxy]      [Proxy]
Enable=0     Enable=1     Enable=1
                                   InternalNetwork=10.10.2.0/24
```

- Port range (H.245, Q.931, T.120, RTP) can be limited
 - This limits the amount of concurrent calls
 - May cause problems with MCU conferences
- NATed endpoints are supported
- Call queuing/forwarding
- Load balancing





Security aspects

- Firewall “just” open for gatekeeper/proxy → all videoconferencing systems are protected by the firewall and can’t be hacked/attacked
- System is as secure as any other system on the public internet
- Everything you have to “protect” is the gatekeeper/proxy
 - Switch off all unnecessary services, e.g. www, ftp, ssh (from outside)
 - Install all security fixes/patches





Security aspects

- **NOTICE: ALL SYSTEMS CAN BE HACKED/ATTACKED AS LONG AS THEY ARE CONNECTED TO A NETWORK/INTERNET/etc.**



Statistics (I)

- GnuGK is used for ALL videoconferences in IPP/RZG (intern↔intern, intern↔extern, extern↔intern, extern↔extern)
- System is in use since 08/02
 - Until 04/04: 1.6 GHz PIII, 256GB Ram, SuSE Linux 7.3
 - Since 05/04: IBM X3-35 eServer, 4 x Intel Xeon 2.8 GHz, 1.5GB Ram, RedHat 9
- Breakdowns (“old gatekeeper”) so far:
 - 2003: 2 breakdowns (1 x Kernel Panic, 1 x power failure in building)
 - 2004: 2 breakdowns (1 x failure of power supply, 1 x harddisk crashed → System was replaced by new GK)





Statistics (II)

- ~ 1500 calls per month (~ 40% multipoint)
- Connection speeds from 512kbit/s up to 3MBit/s (single connection)
- ~ 150GB monthly data throughput
- “Old” system was up and running for 239 days, more than 7000 calls were handled, about 2000 came from external institutions, e.g. KFKI, other EFDA members, MCUs, etc.
- We were not able to “force” proxy down



Summary

- GnuGK is **THE** solution for IPP/RZG
- Disadvantages
 - Monitoring just via telnet (allowed ips can be specified)
- Advantages
 - Its free
 - OpenSource
 - Bunch of authentication methods
 - Runs on Linux/Windows/Mac
 - E.164 rewriting
 - Accounting (Radius, File, SQL)
 - ...and much more

