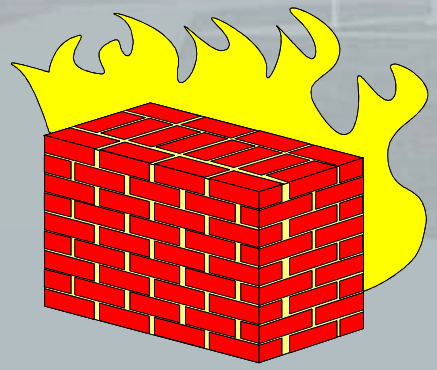
Firewalls - the adaptive tools…



EBU NMC Seminar
Geneva, 16 and 17 June 2004

Agenda:

1. Introduction – the need for firewalls

1. Motivation for attacks
2. Attributes of networked communication
3. What threats may broadcasters estimate?
4. What can firewalls perform and which risks still remain?
5. An example of a broadcasters network
6. Used applications and the resulting bandwidth

1. Conclusion

Introduction – the need for firewalls

- Why do we need firewalls (FW) for our networks?
  - in the strict sense we don't need any FW for computer-networks!
    ..but for security and reliability.
- Convergence of networks
  - More complexity – more ways to attack
  - Tools used by hackers getting more powerful too
- What is meant by „firewall"?
  - „single-machine" or „overall concept" (like ISO 17799)
  - „home-made network-filter" or „managed cluster of tools"

Motivation for attacks:

- „White hat“ hackers who just want to discover risks
- The „just for fun and thrill script kiddies“
- Criminals looking e.g. for creditcard informations
- Political motivated hackers
- Ex-staff and maybe insiders (looking for revenge)
- Spies (industry, secret service...)

Attributes of networked communication

- Availability of the networked workflow
- Integrity of my connections and infrastructure
- Confidential information and essence

What threats may broadcasters estimate?

- Server, network-trunks or router could deny their service
  - Denial of service (DoS) attacks through the internet, endangering the workflow
  - Installing viruses/ trojans/ worms (which may destroy data or the performance of the networks)
- Foes get permission to the broadcaster's corporate network
  - Strangers could access the internal network, database or even playlists
  - Espionage and manipulation of incoming or outgoing information/ data
  - Abuse of the internet connection/ server e.g. for spam mailing or hosting of (illegal) material
- Altering or deleteing of files
  - Mostly there is not enough time to check everything – the source has to be trustable
  - maybe content theft (problematic)

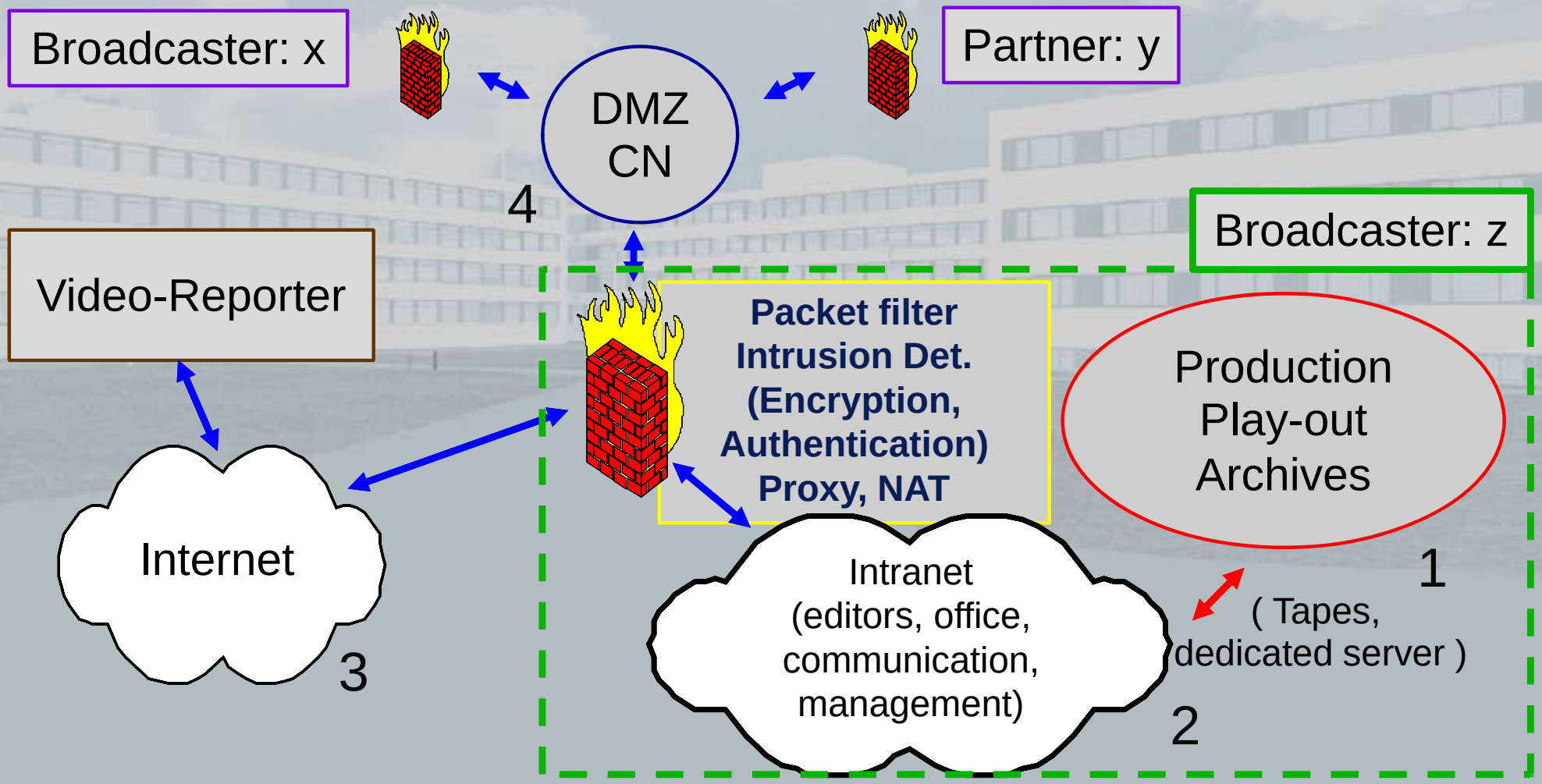
a) What can firewalls perform... ?

- Control your traffic by listening to your network traffic and applying filtering rules
  - Dangerous packets are dropped
  - Unwanted connections / services refused
- Intrusion detection systems (IDS)
  - Logging bogus events and send a alarm-message
- Encrypt your data
  - Establish network-tunnels (Virtual Private Network – VPN ...)
  - User and source authentication (e.g. by certificates)
- Application-proxy-services and caching
- Hide your infrastructure (NAT, Proxy)

... and b) which risks still remain?

- Viruses, trojan and worms (especially user activated)
- User attached devices
  - like wireless LAN and bluetooth
  - Portable memory (Memorystick, compact DAS/NAS)
  - Mobile phones (UMTS)
- Notebooks
- The user itself
- Natural disaster (fire, accidents)
- physical access control
- Weak passwords (may be controlled by admin)

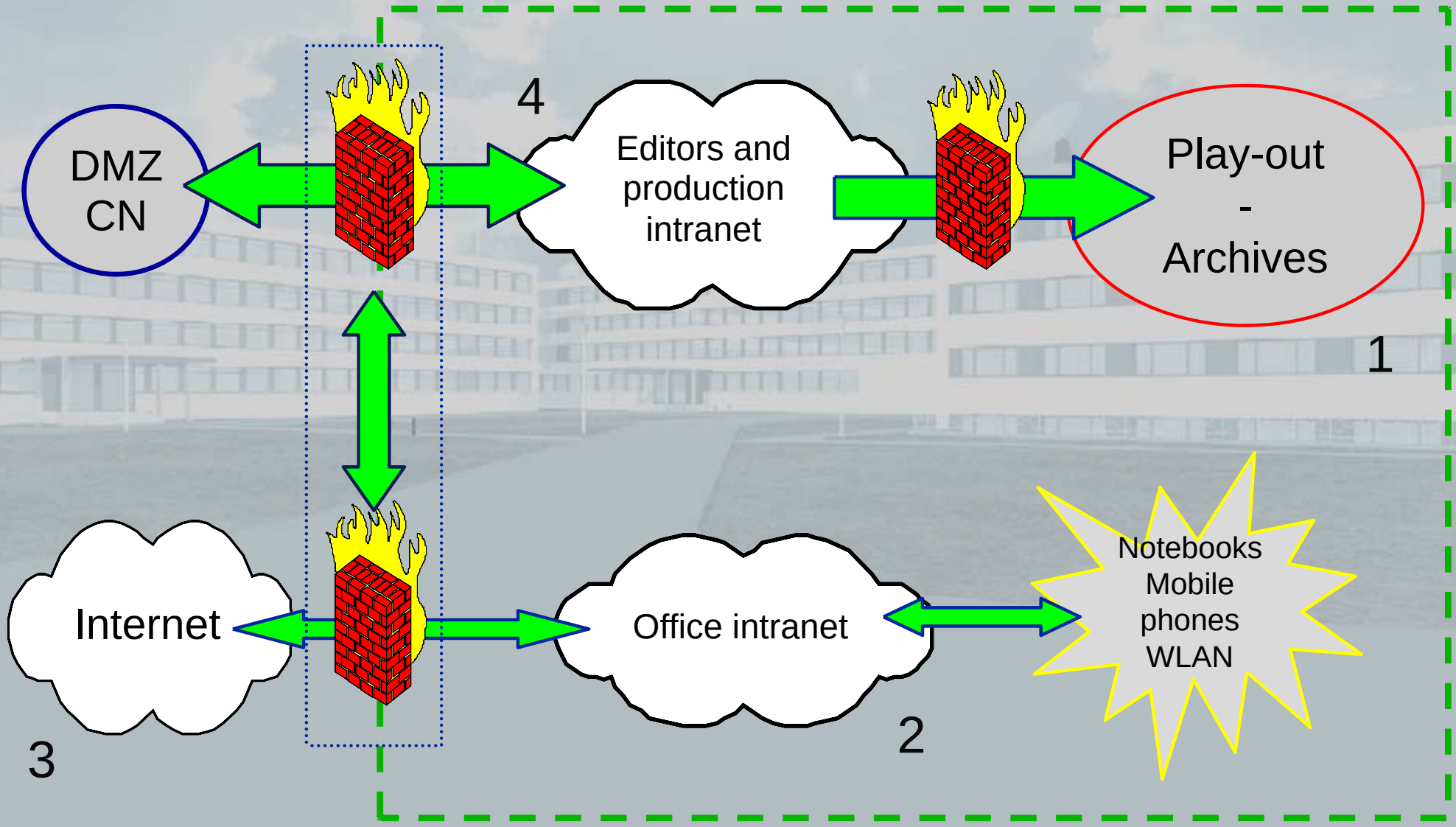
An example of an broadcasters network:



Used applications and the resulting bandwidth

- Intranet (e-mail, office, low resolution browsing)
  - depends, rather 100 Mbps than 1 Gbps
- Internet – interface to the “dangerous” world (e-mail, web server, www)
  - less than 10 Mpbs but many small connections with different protocols
- “Video Reporters” connected via WWW (few Mbps)
- Network for production and play-out (high resolution)
  - internal, 25 up to 270 Mbps per transfer (Gb-trunks are common)
- Backbone for protected contribution like “video-file-transfer”
  - DMZ, e.g. in case of HYBNET/ARD STM4-trunks (up to 622 Mbps)

Possible segmentation:



Resulting firewalling effort

- In summary the amount of broadcasters traffic is high but possible to deal with…
- Firewalls can provide encrypted connections (VPN – IPsec, SSH) up to 1 Gb-linespeed
- Multiple (external) interfaces (DMZ, www, intranet) may result in a multiple firewall-concept
- Administration of a firewall is a never ending story! ☺

Conclusion:

- The broadcasters world is getting more and more networked – resulting in new possibilities and new dependencies
- … security has to be part of all plans from the beginning

- Firewalls have to be seen just as a subset of a necessary overall security concept (like ISO 17799 and BSI 7799)

- You have always to calculate with the new and unexpected…

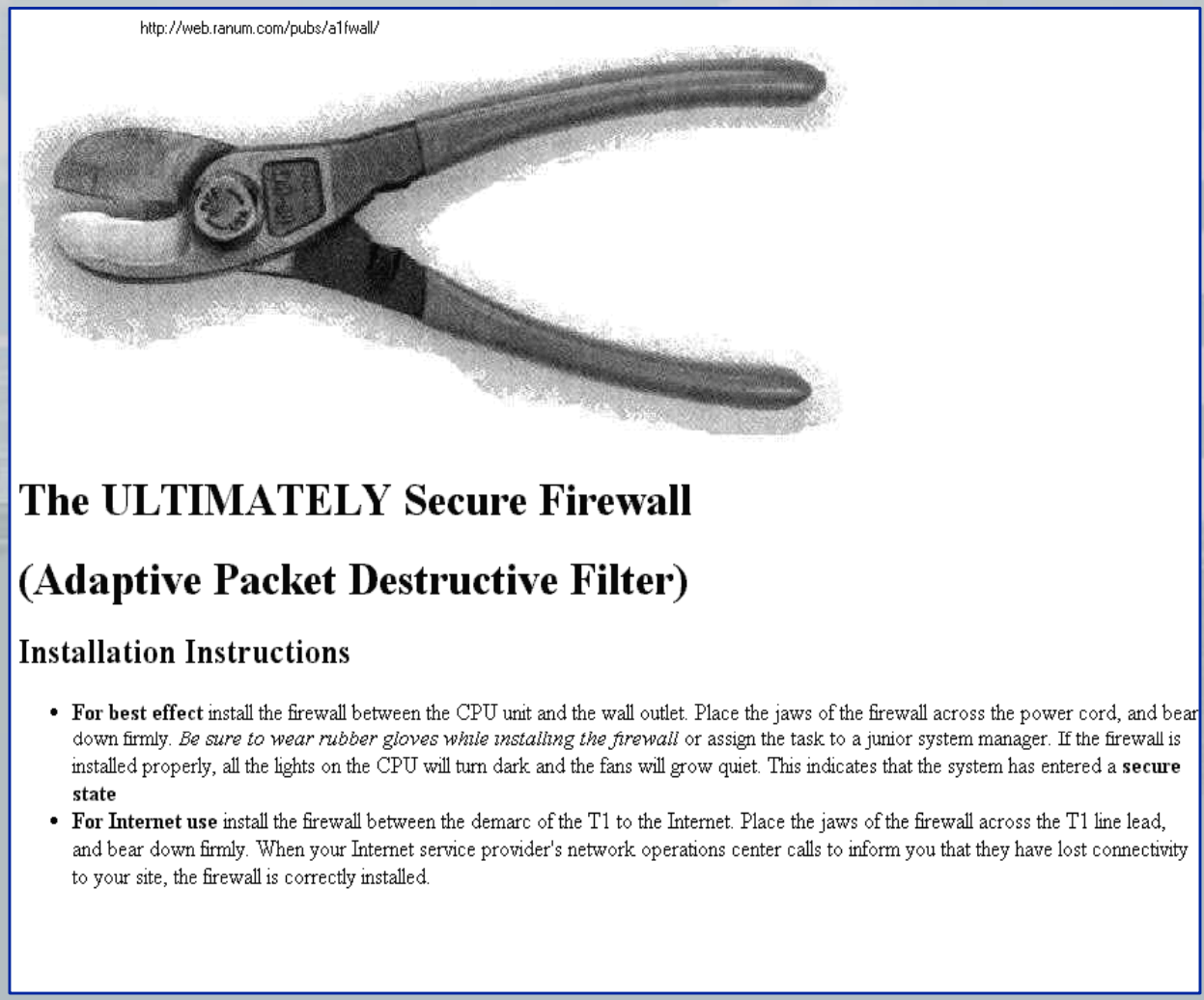
- Security costs money – no security quite sure too...

- Risk analysis: How secure do you have to be? – How secure do you want to feel?

Thank you for your attention…

Contact:

Matthias Hammer
Hammer@IRT.de
+49-89-32399-446
Floriansmühlstr. 60
80939 München
Germany


http://web.ranum.com/pubs/a1fwall/

The ULTIMATELY Secure Firewall

(Adaptive Packet Destructive Filter)

Installation Instructions

- **For best effect** install the firewall between the CPU unit and the wall outlet. Place the jaws of the firewall across the power cord, and bear down firmly. *Be sure to wear rubber gloves while installing the firewall* or assign the task to a junior system manager. If the firewall is installed properly, all the lights on the CPU will turn dark and the fans will grow quiet. This indicates that the system has entered a **secure state**
- **For Internet use** install the firewall between the demarc of the T1 to the Internet. Place the jaws of the firewall across the T1 line lead, and bear down firmly. When your Internet service provider's network operations center calls to inform you that they have lost connectivity to your site, the firewall is correctly installed.