Sicherheit bei Videokommunikation

ZKI-Herbsttagung 2002

Dresden, 01./02.10.2002

Sicherheit bei Videokommunikation

Lösungsansätze von Videokonferenzen für

firewallgeschütze Netze oder

zu Geräten mit inoffiziellen IP-Adressen

- Problembeschreibung
- Überblick für mögliche Lösungsansätze
- Datenschutzprobleme

Videokonferenzen und Firewall

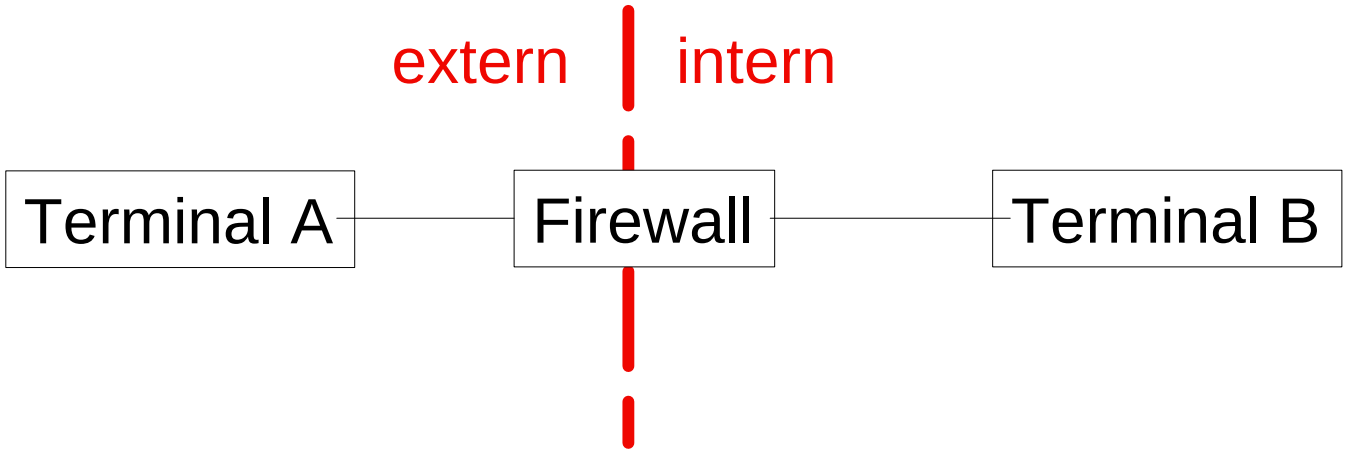
Widerspruch - Funktionsumfang / Sicherheit

IP-Adressen: Interne / externe

NAT	n / m (n > m)
masquerading	n / 1

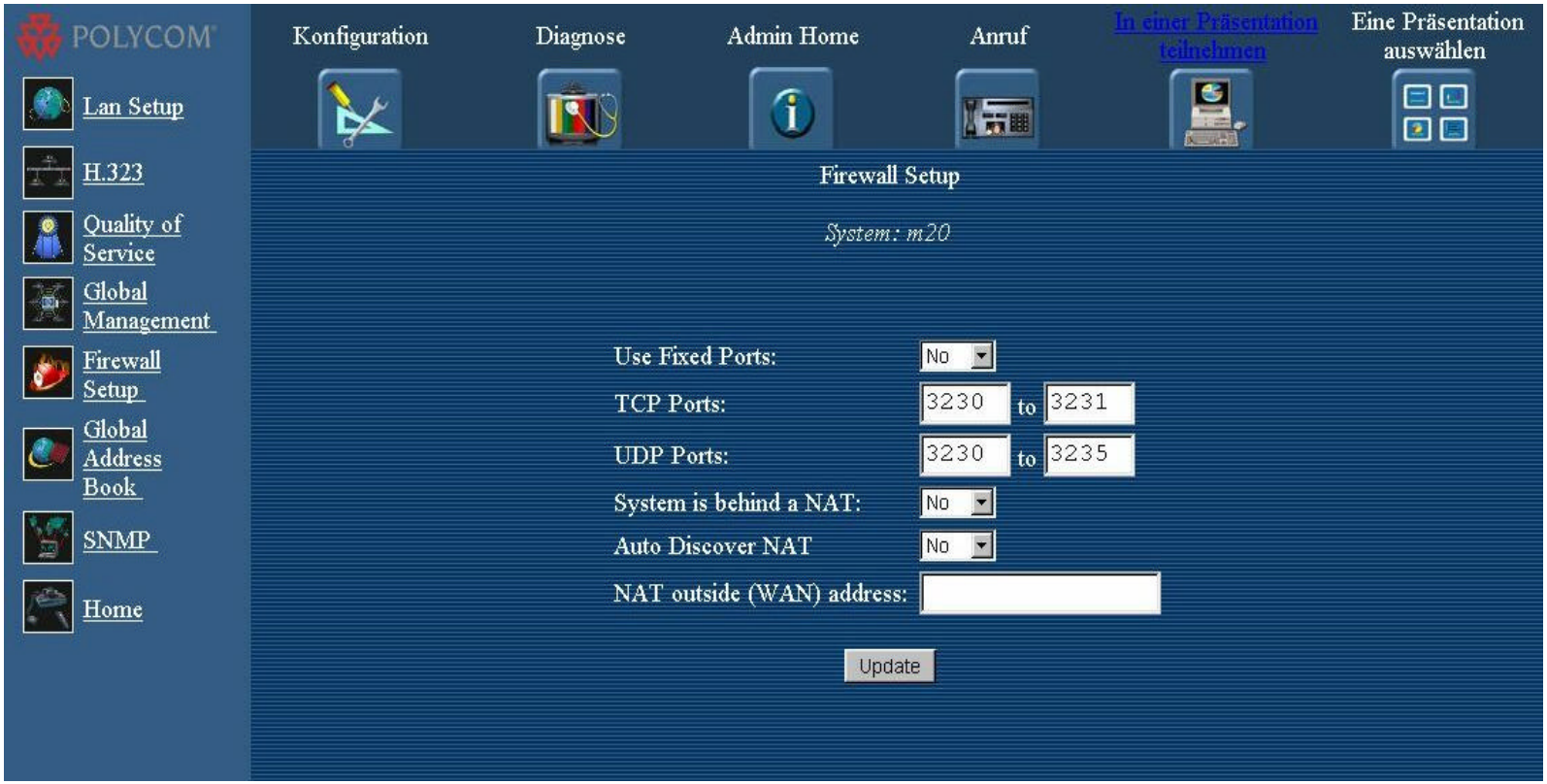
viele feste Portnummern: 389, 522, 1503, 1719, 1720, 1731

dynamische Portnummern: TCP, 4 / 8 x UDP ab 1024



Videokonferenzen und Firewall

Möglichkeit der Festlegung fester Portnummern:
z. B. Polycom, TANDBERG



Lösungsmöglichkeiten

VC-Systeme außerhalb der Firewall

Firewall: Check Point FireWall-1, Cisco PIX, ...

Proxy:

- Cisco MCM
- KOMproxyd [10]
- ridge way [11]
- avrit
- OpenH323Proxy

propietär: VCON

MCU: Accord

Tunnel: IP - IP

Unterstützung durch die Firewall selbst

Checkpoint FireWall-1

- Picturetel: H.323-Protokoll wird verfolgt, benötigte Ports werden geöffnet [1]
  (Check Point FireWall-1 V3.0a with latest H.323 macro 17.09.1997)
- Chris Shenton fand keine Anhaltspunkte von H.323-Protokoll-Verfolgung [2]
  (Check Point FireWall-1 V3.0b 12.03.1998)
- Firewall Handbuch für Linux: keine Anhaltspunkte von H.323-Protokoll-Verfolgung
  (Guido Stepken, Version 3.0, 30. August 1999) [3]
  (Check Point FireWall-1 V3.0b)
- Release Notes Checkpoint Firewall-1 Version 4.1 sp3 (41814): [4]
  H.323 connection between two FireWalls did not work.

Cisco PIX Firewall and Cisco IOS Firewall Feature Set

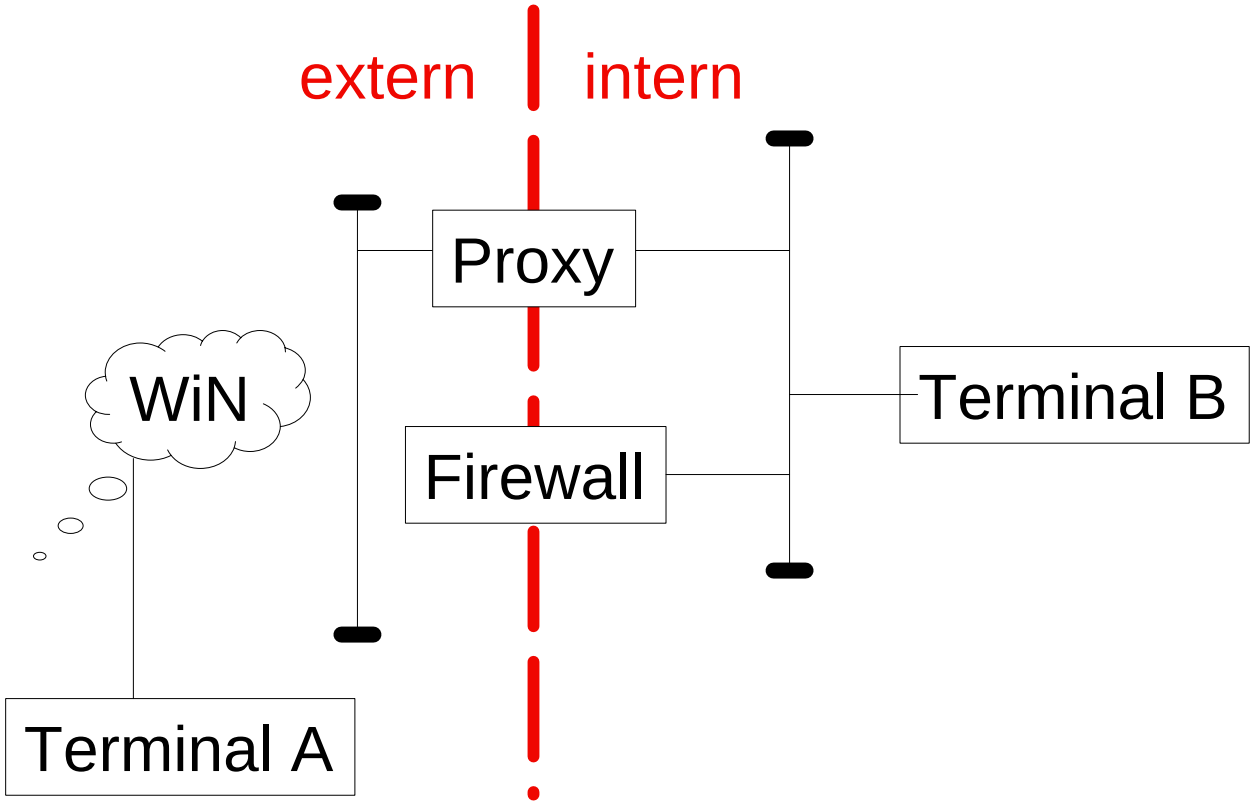
- Überwachung des H.323 Kontrollkanals

H.323-Proxy

H.323-Proxy = Gateway H.323 / H.323

Audio-, Video-, Anwendungsdaten:

- an Firewall vorbeileiten
- analysieren
- Adressen und Portnummern ersetzen



H.323-Proxy: Cisco MCM

[5]

- Gatekeeper und Proxy
- Cisco IOS software feature set
- Cisco 2500, 3600, 3810 platforms
- wird empfohlen von Cisco, Radvision, VCON, ...

VCON - VCON (proprietär)

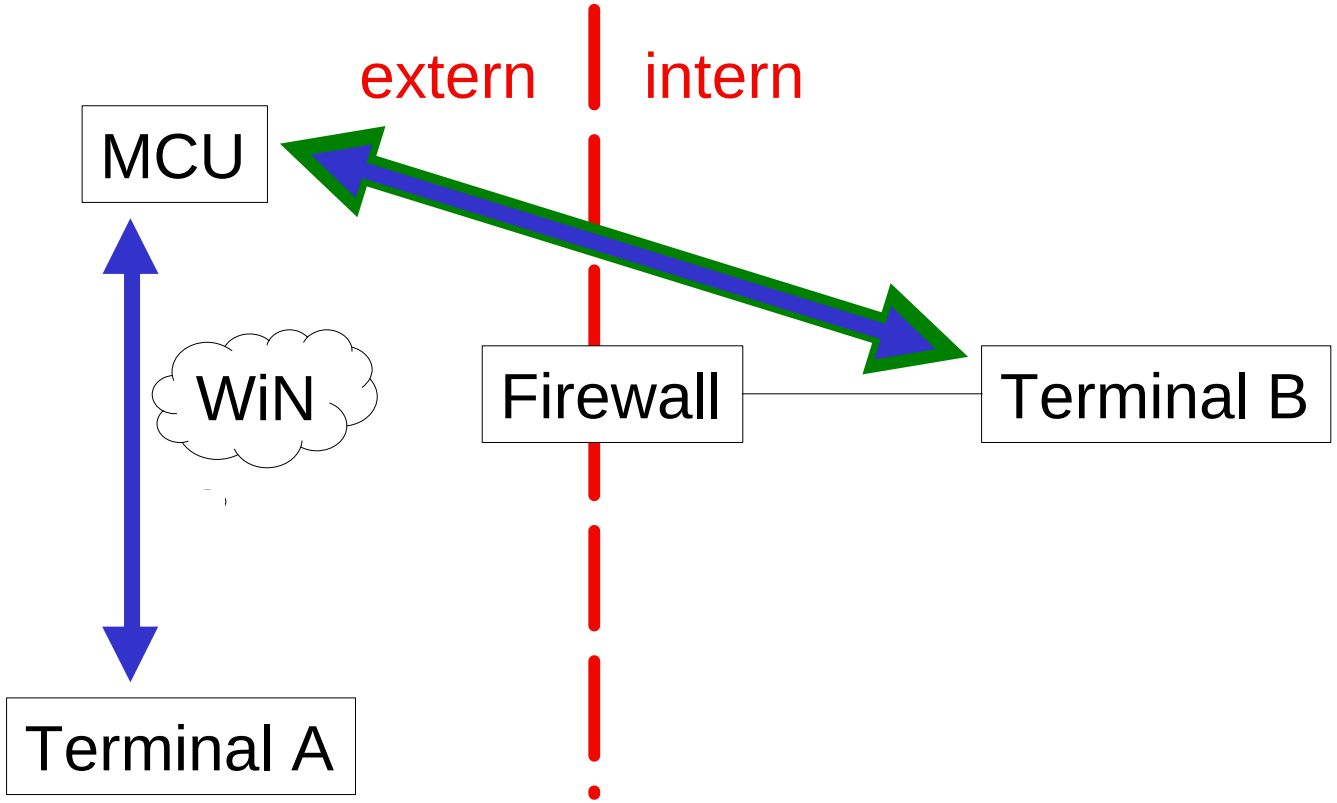
VCON MXM und Meetingpoint 4.5 [9]

- Definition im MXM
- Kommunikation über fest vordefinierte Ports
- keine dynamischen Ports
- nur zwischen zwei VCON-Systemen nutzbar
- Test am BZVD: demnächst

IP - IP Tunnel

Möglichkeiten:

- intern - extern oder intern - extern - intern
- Gatekeeper extern oder extern / intern
- Durchwahl über MCU
- Terminal vom internen Netz isolierbar für Konferenzdauer?



IP Tunnel vom internen Terminal zur externen MCU

AV-Verbindung zwischen Terminals und MCU

Firewall und Videokonferenzen - Offene Fragen

Sicherheitseinschränkungen:

- Applicationsharing (T.120)
- Netzsicherheit

benötigte Funktionen

- Protokoll der Verbindungen
- Alarm

neue Funktionen

- Rufweiterleitung
- Gruppenrufe

Gatekeeper

- bester Punkt für Hacker-Angriffe; enormes Sicherheitsrisiko
- Anmeldung erfolgt mit Zahl oder IP-Adresse; damit ist das Vortäuschen einer falschen Identität sehr einfach
- Beispiele
  - ACCORD - MCU zeigt keine Teilnehmer an
  - RADVision - MCU zeigt Teilnehmer erst nach Aktivierung des Data-Sharing an
  - beide können über WWW-Oberflächen gesteuert werden, damit treten die üblichen Probleme des Internets auf
- Schutzmaßnahmen:
  - Sicherheitsstufen benutzen
  - Festlegung von zugelassenen IP-Adressen (Anmeldung damit aber auch nur Rechner- und nicht personenbezogen)

Sicherheit bei Videokommunikation

[1] http://www.sepscor.org/Firewall_pictel.htm

[2] http://www.shenton.org/~chris/nasa-hq/netmeeting/

[3] http://www2.little-idiot.de/firewall/zusammen-190.html

[4] http://www.intersec.com/support/checkpt/relnotes.htm

[5] http://www.cisco.com/warp/public/732/net_enabled/mcm/

[6] http://www.accordtelecom.com/cr_products/vipera/v2solutions.html

[7] http://www.avirt.com/voice/index.html

[8] http://openh323proxy.sourceforge.net/

[9] http://www.vcon.de/

[10] http://www.kom.e-technik.tu-darmstadt.de/KOMproxyd/

[11] http://www.ridgeway-sys.com/Products/