

Virtual Private Networks

Hohe Sicherheit wird bezahlbar













Paul Schöbi, cnlab AG

paul.schoebi@cnlab.ch

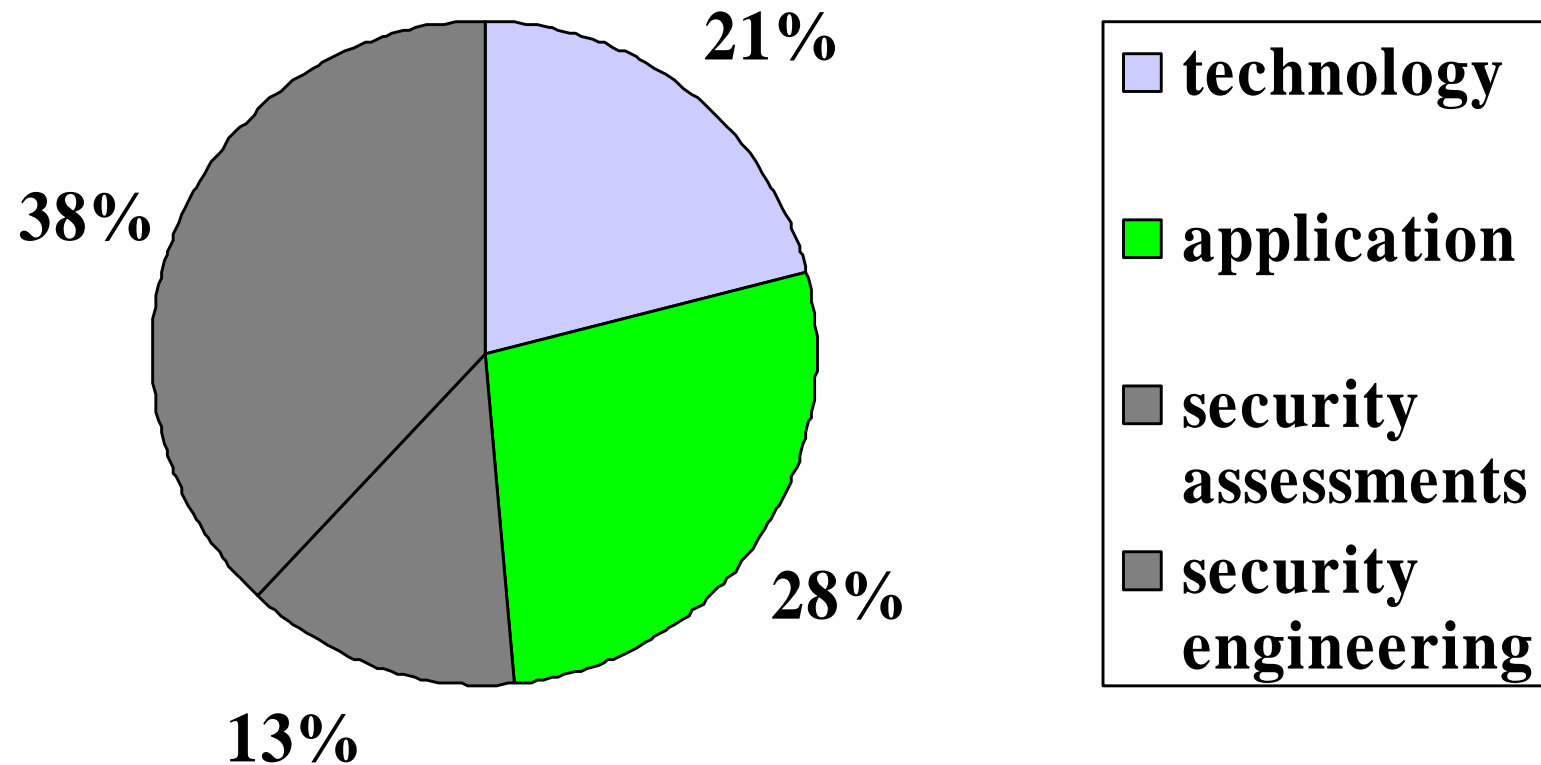
www.cnlab.ch

Präsentation unter ‚repertoire‘ verfügbar

cnlab ag: Internet Engineering

| | | | | |
|--------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|--|
|  <p>Dr. Paul Schöbi Managing Director</p> |  <p>Lukas Frey Dipl. El. Ing. ETHZ</p> |  <p>Thomas Lüthi Dipl. El. Ing. FH</p> |  <p>Reto Diethelm Dipl. El. Ing. FH</p> | |
|  <p>Prof. Dr. Peter Heinzmann Technical Director</p> |  <p>Rene Vogt Dipl. Inf. Ing. FH</p> |  <p>Christian Birchler Elektroniker, Sys Admin</p> |  <p>Max Wegmüller Dipl. Inf. Ing. FH, Assistent</p> | |
|  <p>Prof. Dr. Ueli Maurer VR cnlab Software AG</p> |  <p>Prof. Hansjörg Huser Professor für Datenbanksysteme</p> |  <p>Dr. Christoph Schnell Multimedia, umea</p> |  <p>Theo Schneider Dipl. El. Ing. EPFL, Assistent</p> | |

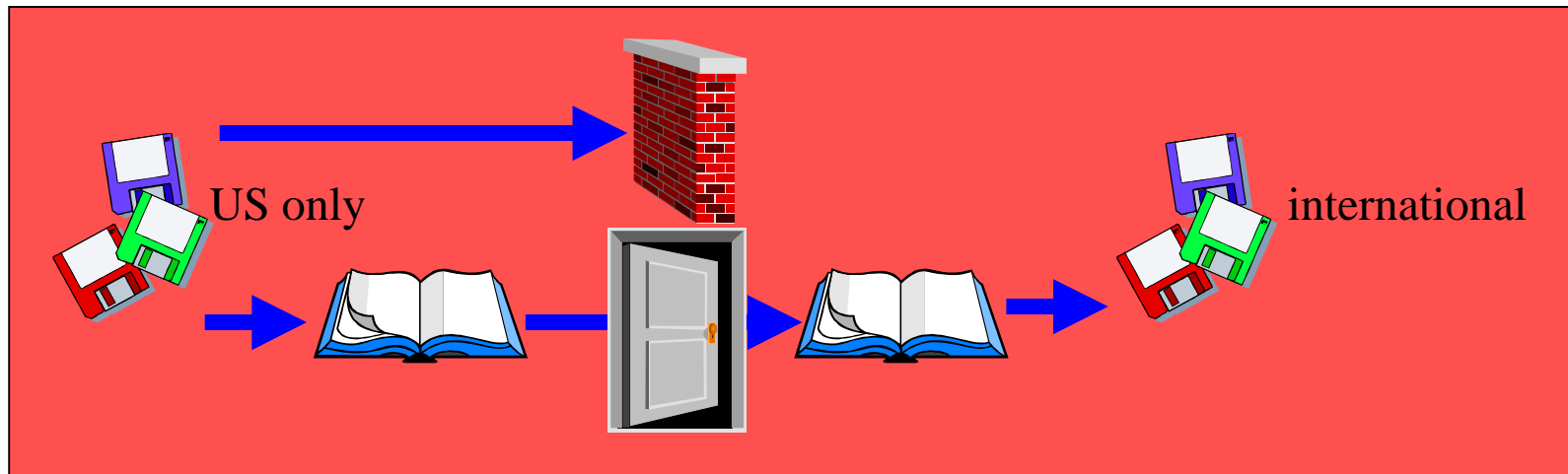
Cnlab activities by volume



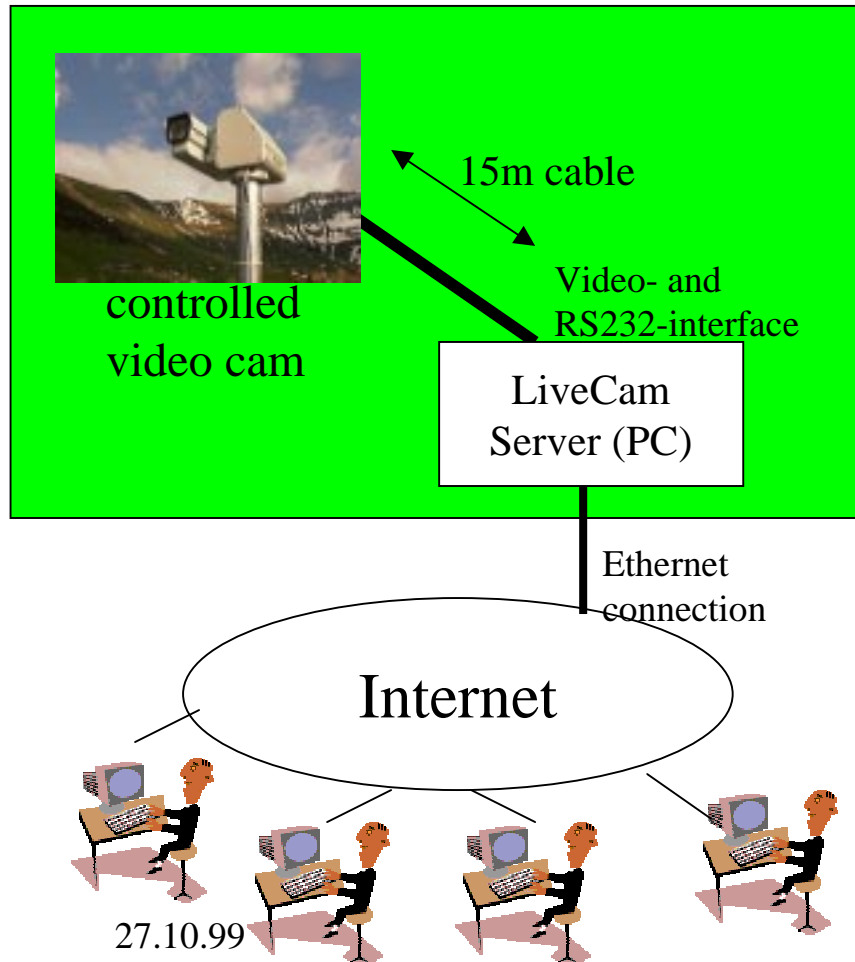
Pretty Good Privacy (PGP)



- Strong encryption and signatures
- U.S. export restrictions
- production by **cnlab software AG**



Internet LiveCam



- Snapshot or video
- position and zoom control via internet
- additional services

<http://www.cnlab.ch/livecam/>

Virtual Private Networks

Hohe Sicherheit wird bezahlbar



Theorie



Praxis

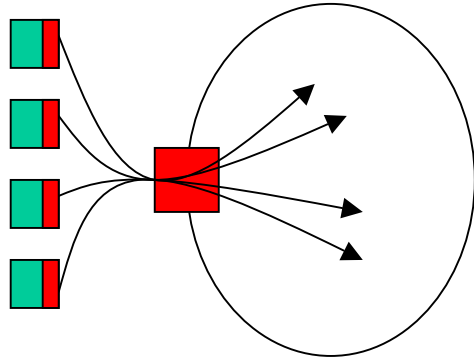


Zukunft

Theorie: VPN

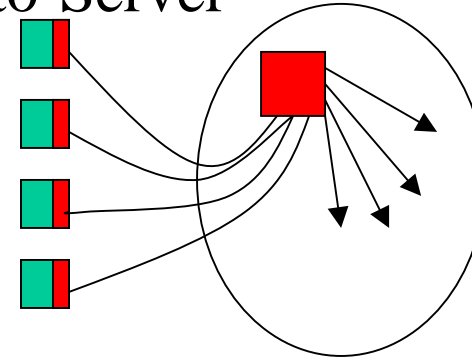
VPN mit IPSec-Produkten

End-to-Gateway



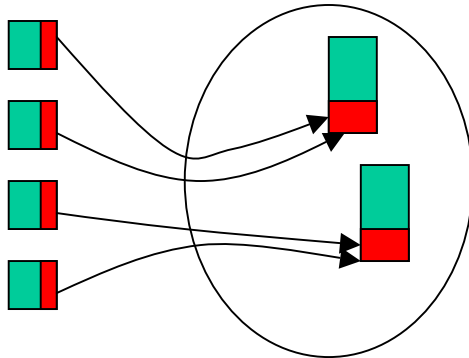
Checkpoint
PGP/Gauntlet
Utimaco
...

End-to-Server



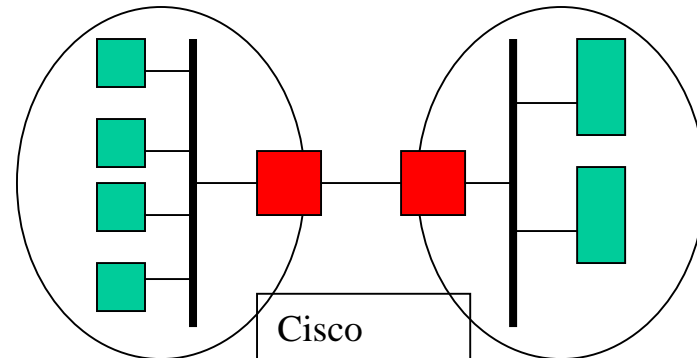
Checkpoint
PGP/Gauntlet
DataFellows
Win2000
...

End-to-end



DataFellows
PGP
Win2000
...

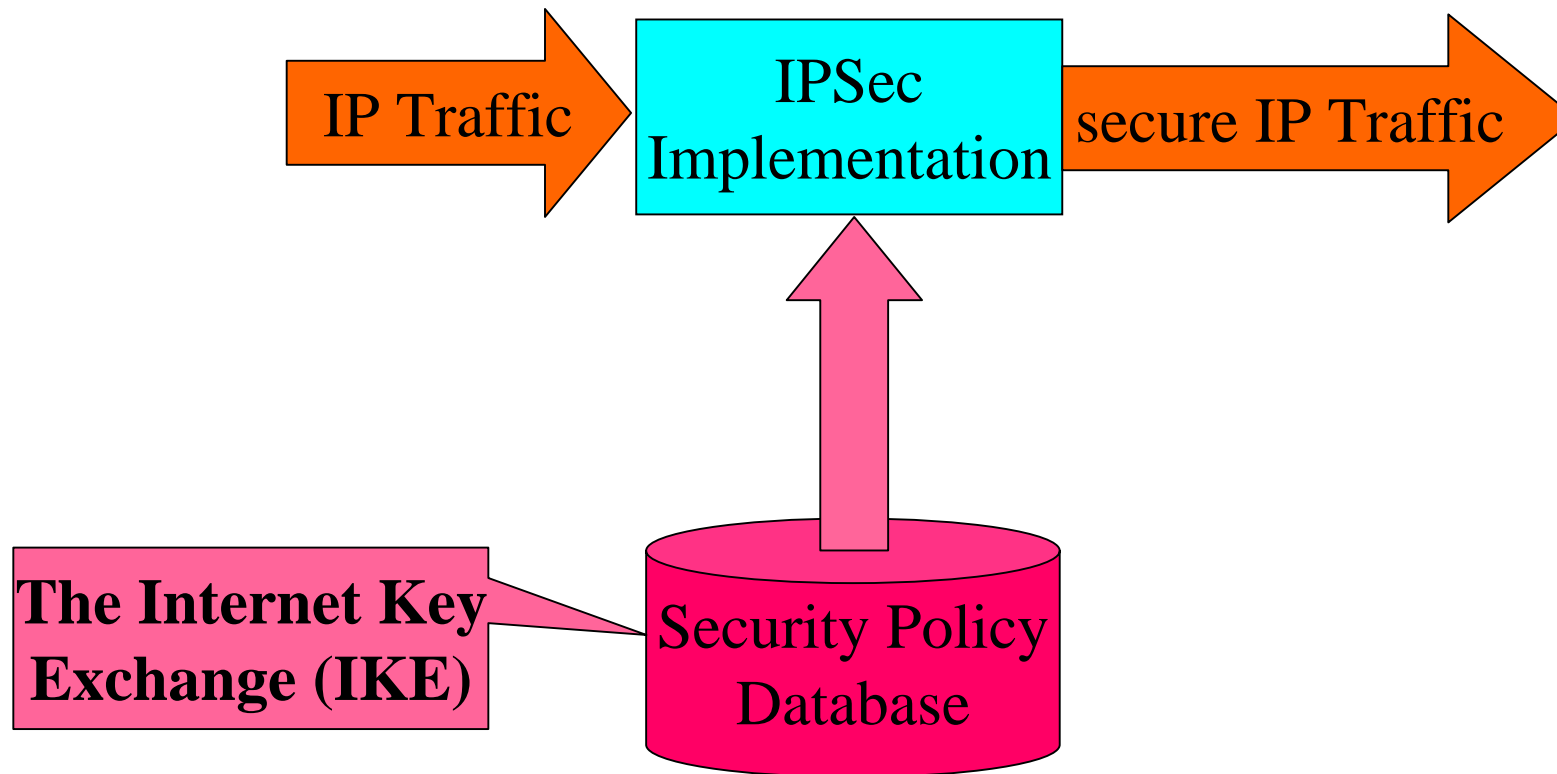
Site-to-site



Cisco
Checkpoint
Gauntlet
Utimaco
Win2000
...

Theorie: IPSec

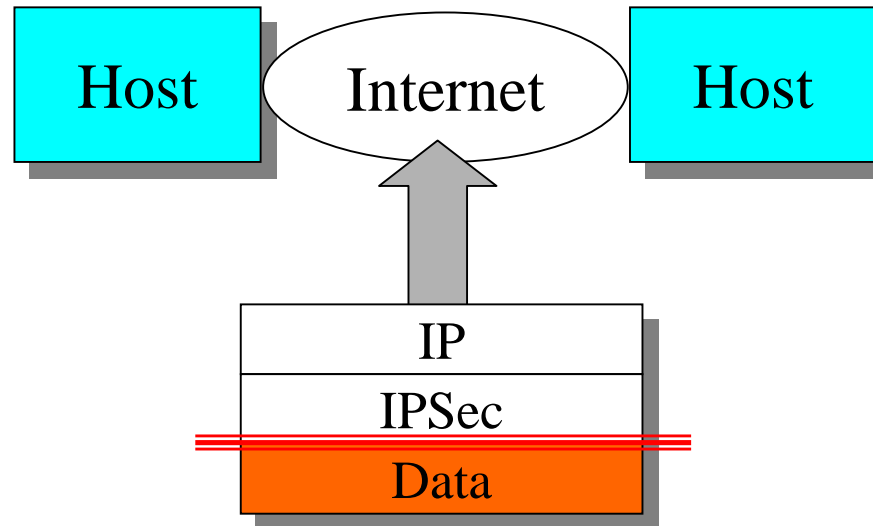
Security Architecture for the Internet Protocol (IPSec)



IPSec Status

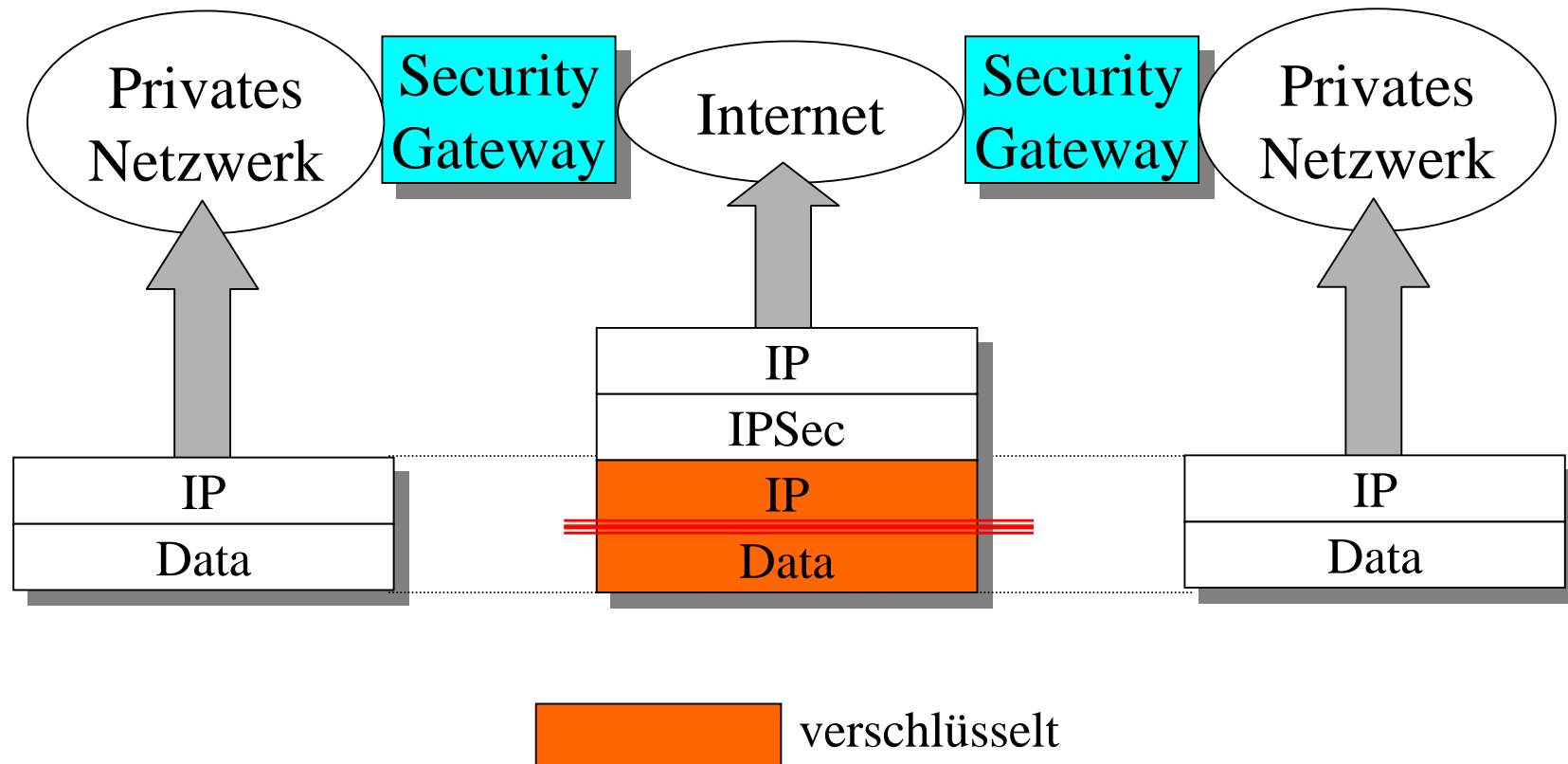
- IETF Internet Drafts Juli 1998
- Ist Teil von IPv6, kann aber auch in IPv4 eingesetzt werden.
- Implementiert in Windows NT 5.0 zur sicheren Übertragung von L2TP
- Implementiert in Firewalls, Routern und Network Access Servern

IPSec: Transport Mode



 verschlüsselt

IPSec: Tunnel Mode



IPSec Protokolle (die wichtigsten Standards)

IP Authentication Header (AH) RFC 1826

- connectionless integrity
- data origin authentication

Encapsulating Security Payload protocol (ESP) RFC 1827

- confidentiality

Internet Key Exchange (IKE) RFC 2409

- Schlüsselvereinbarung,
- Security Associations

z.B. PGPnet

IP Authentication Header (AH) RFC 1826

- connectionless integrity
- data origin authentication

Triple DES
IDEA
CAST
(128 bit)

Encapsulating Security Payload protocol (ESP) RFC 1827

- confidentiality

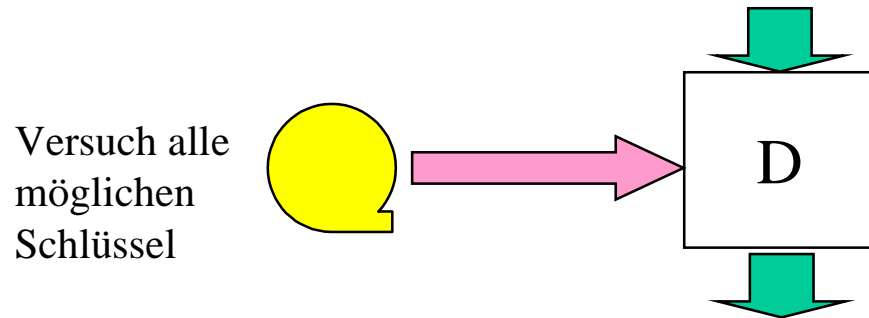
Internet Key Exchange (IKE) RFC 2409

- Schlüsselvereinbarung,
- Security Associations

RSA (min.1024 bit)
D/H (min. 2048 bit)

Wie sicher ist „128 Bit“ ?

.....XççAçç55sa4A4asw4ççGfddv456adacrlaf..4345m.....



.....dies ist lesbarer Deutscher Text, wir haben den Schlüssel.....

| unit | for 40 bit | for 56 bit | for 128 bit | nof keys per sec |
|------|------------|------------|-------------|----------------------------|
| hour | 2.78E-01 | 2.78E+03 | 2.78E+24 | 1.00E+10 |
| day | 1.16E-02 | 1.16E+02 | 1.16E+23 | |
| year | 3.17E-05 | 3.17E-01 | 3.17E+20 | age of the universe |
| | | | | 1.00E+11 years |

27.10.9

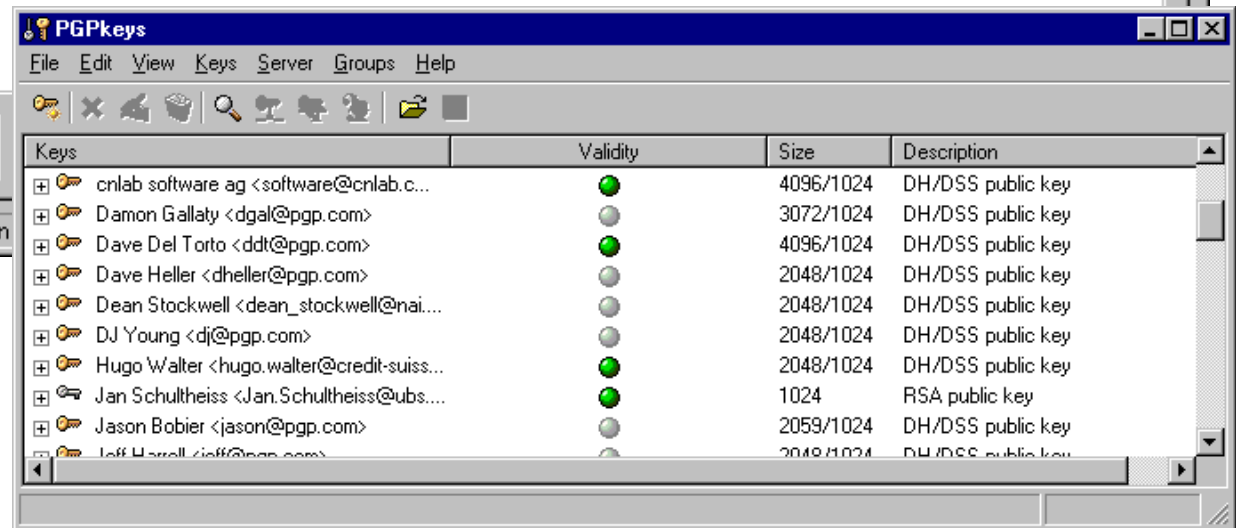
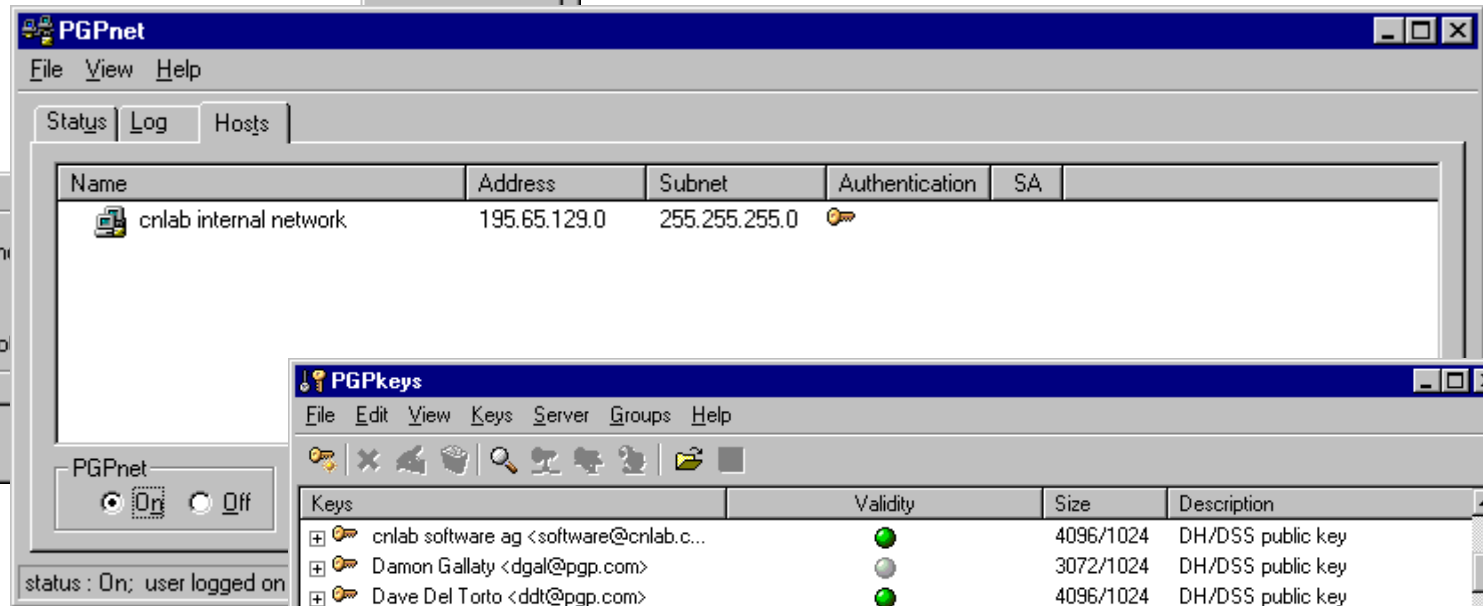
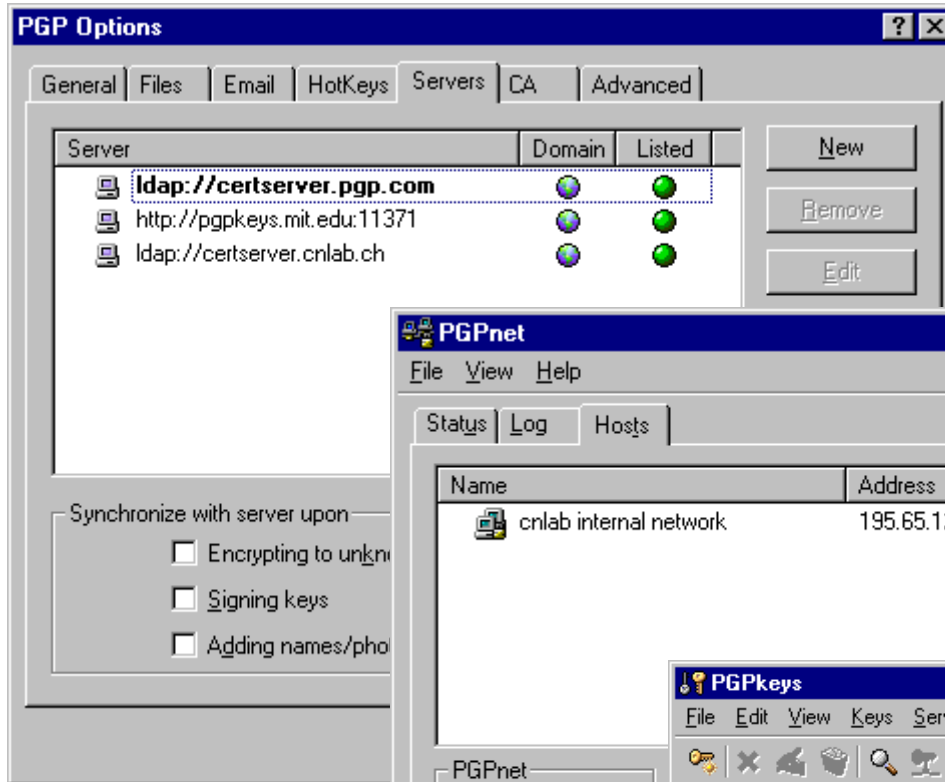
„Export“ SSL
MS Windows

DES

PGP

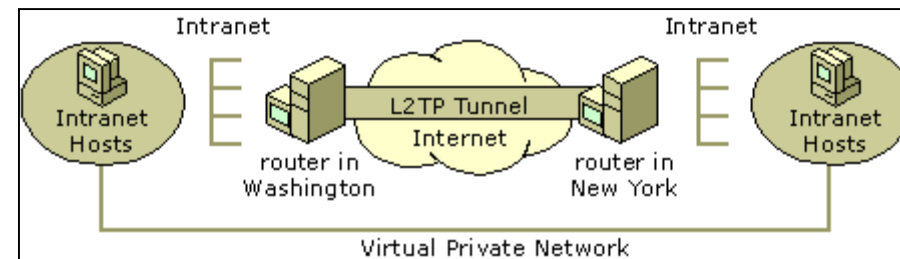
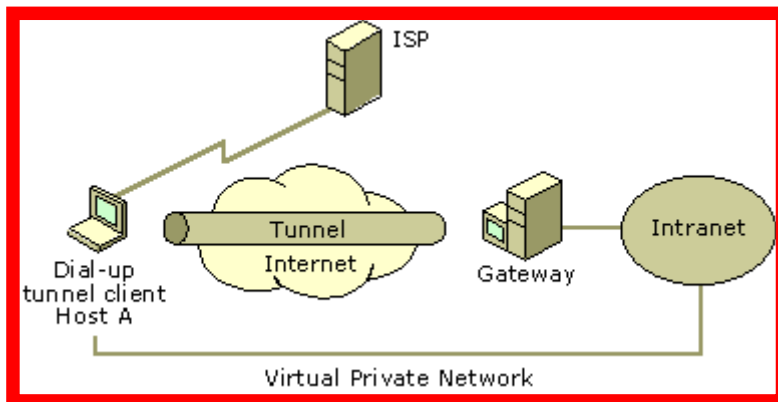
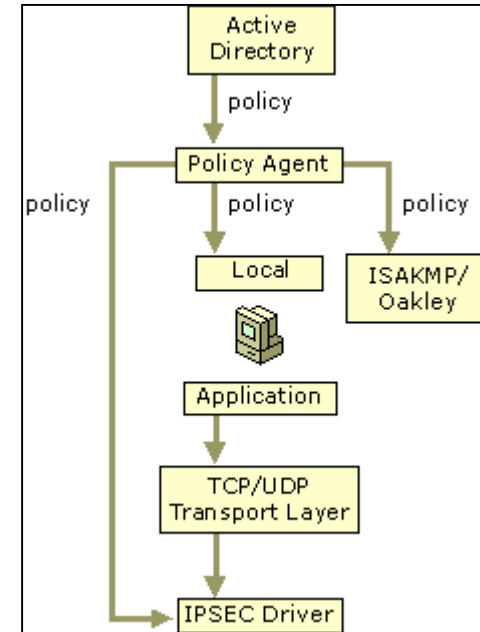
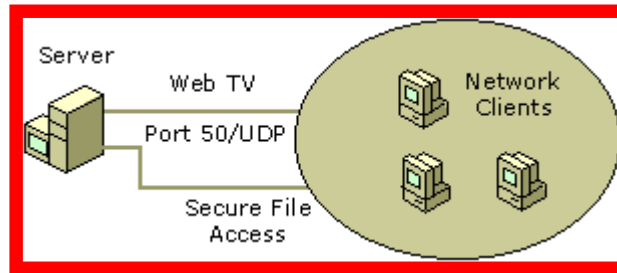
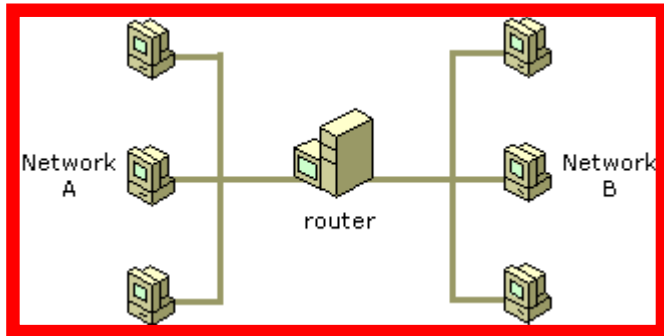
Praxis: bezahlbar

PGPnet Policies



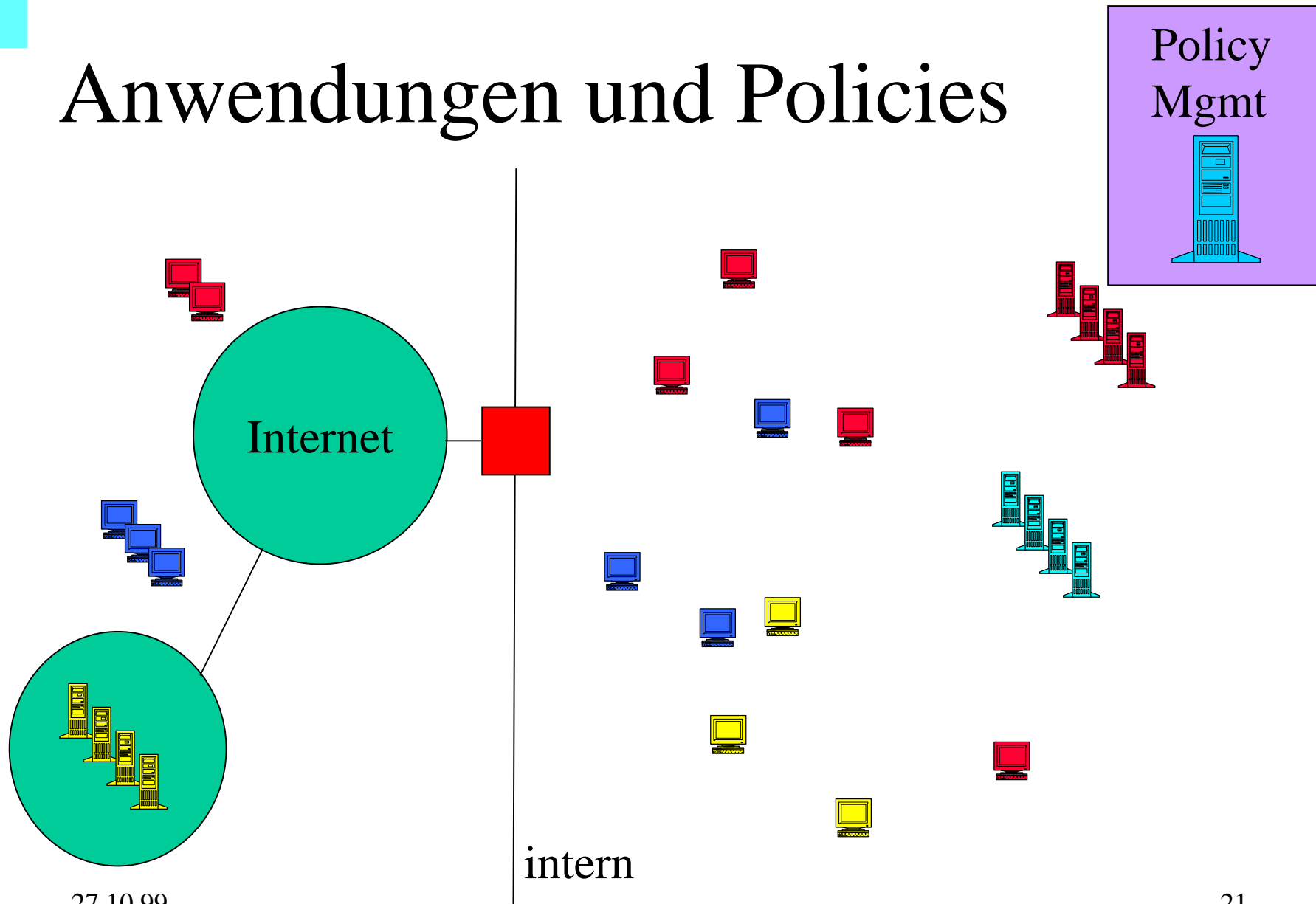
Win2000: Die VPN-Lösung ?

Win2000 Server: NT5.0 Server
 Win2000 Professional: NT5.0 Workstation



Praxis: noch nicht trivial

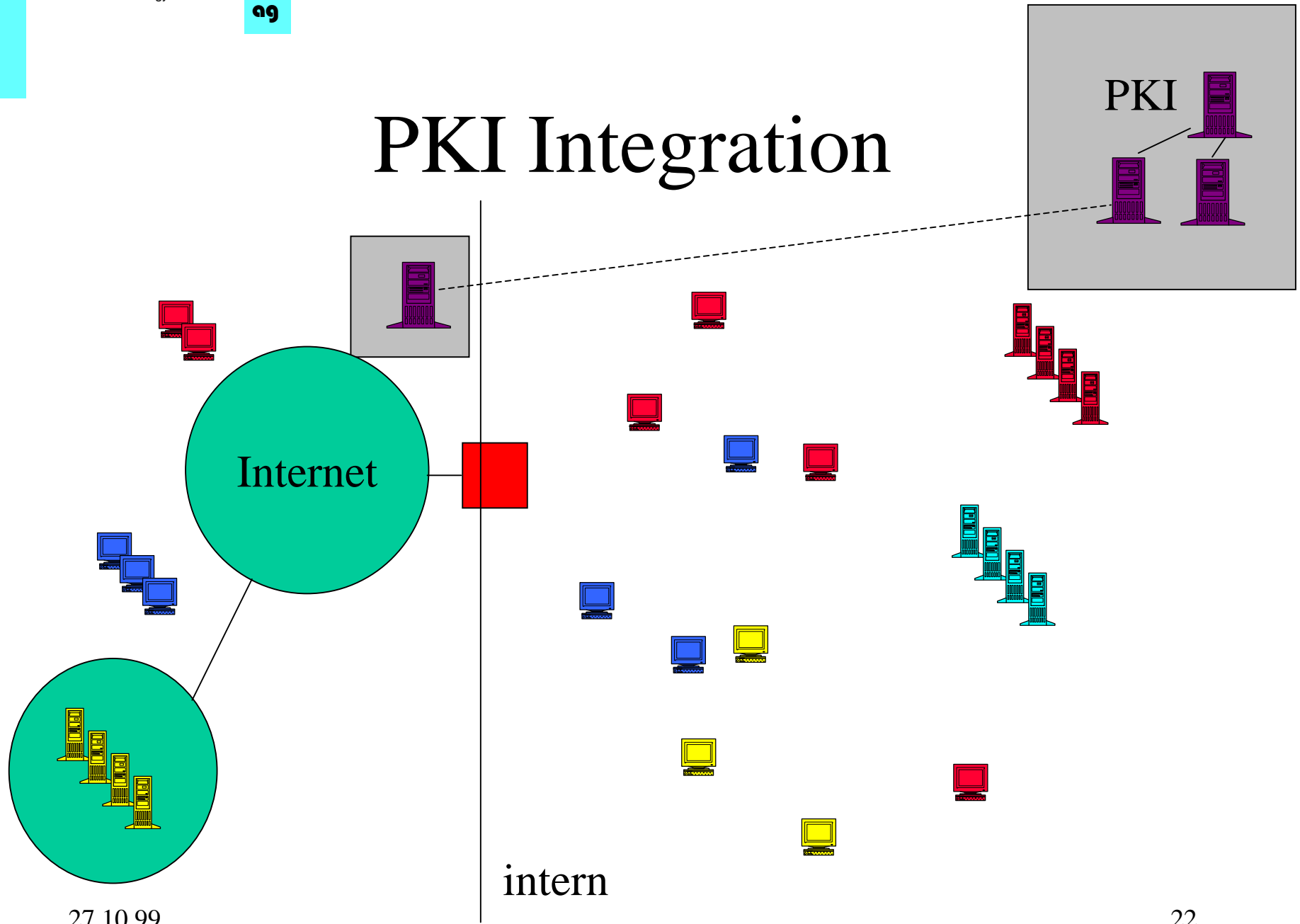
Anwendungen und Policies



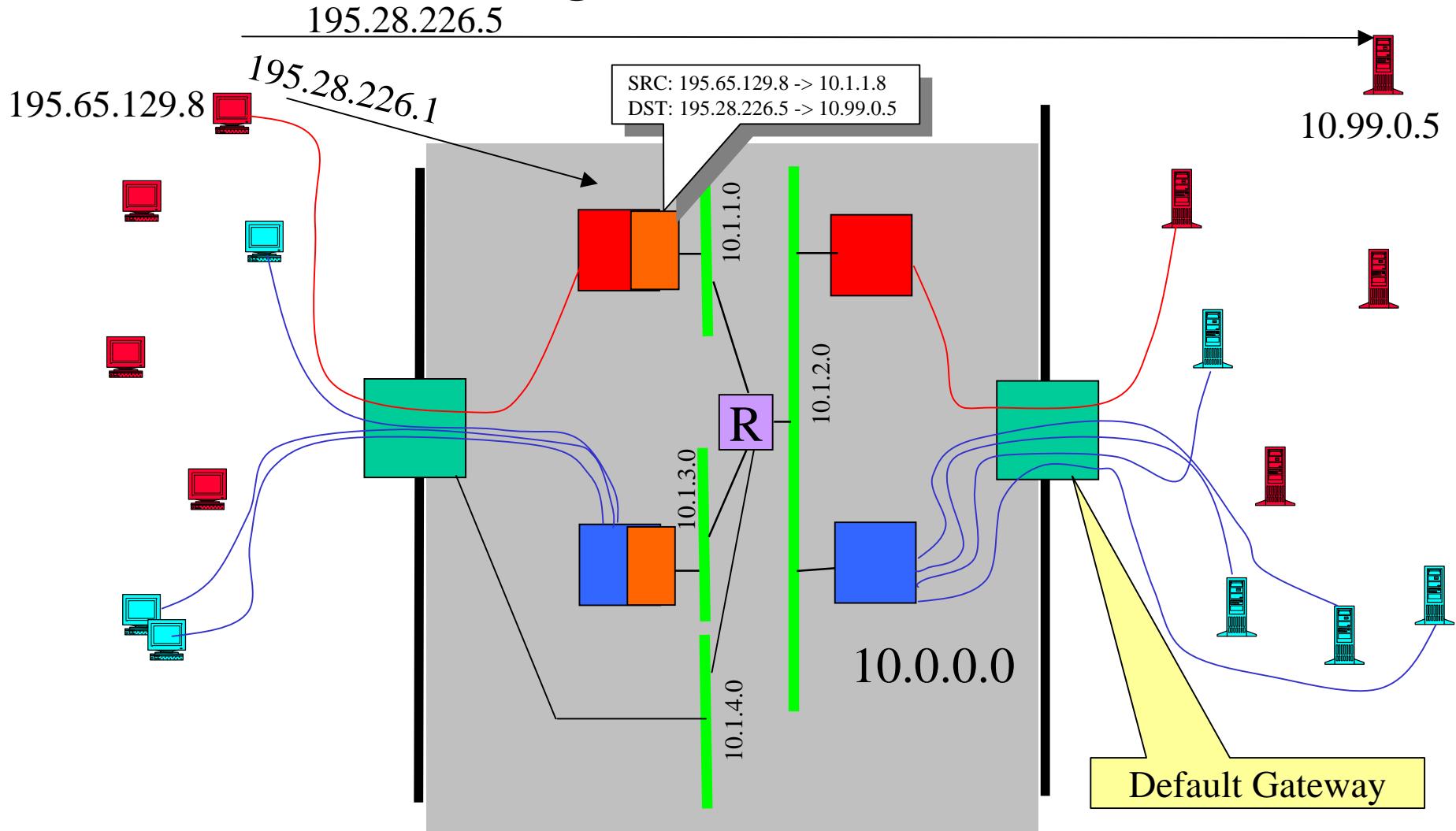
27.10.99

intern

PKI Integration



Adressierung und Remote Access





VPN Zusammenfassung

- Grosse Flexibilität.
- Hohe Sicherheit
- Viele Produkte heute erhältlich.
- Kompatibel mit Standard-PKI.
- IPSec ist gute fundiert.
- Kleine Netze erprobt

- Kaum Erfahrung mit grossen Netzen
- Technisch nicht trivial bei komplexen Netzen
- PKIs sind noch nicht bereit.

Prognose

- Jetzt ist die Zeit der Investitionsentscheide.
- Einige grosse Netze werden im Laufe des Jahres 2000 in der Schweiz entstehen.
- Im nächsten Jahr werden die ersten produktiven PKI aufgebaut.
- Ende 2000 werden wir auch Erfahrung mit grossen Netzen haben.