Praktische Netzwerksicherheit: (3) VPNs und Co.

Prof. Dr. Klaus-Peter Kossakowski

Gliederung der Vorlesung

- Firewall
- Denial of Service
- Virtual Private Networks und ähnliches

Inhalte dieses Kapitels

In diesem Kapitel wird der Schutz der Übertragung von ansonsten ungeschützten Informationen durch kryptographische Anwendungen behandelt und die gängigsten Konzepte hierfür vorgestellt.

Besonders wird darauf eingegangen, wie sich diese Anwendungen in eine Netzwerkarchitektur einpassen lassen bzw. eben auch nicht. Wieder wird auf Eigenschaften der Netzwerk- sowie der Transport-protokolle eingegangen.

Kryptographische Algorithmen und deren Stärke werden nicht im Detail besprochen (> Wahlpflicht Sicherheit in verteilten Systemen).

Ziele dieses Kapitels

Sie können erklären, welche Konzepte für den Schutz von übertragenen Informationen grundsätzlich zur Verfügung stehen, was dies für die Anwendungen aber auch den Schutz durch Firewalls bedeutet.

Sie kennen verschiedene konkrete Angriffe und Probleme und können geeignete Mechanismen innerhalb einer Netzwerkarchitektur identifizieren und platzieren.

Sie können die individuellen Vor- und Nachteilen einzelner Mechanismen benennen und vergleichen.

Worum geht es eigentlich?

Schutzziele (Wiederholung)

- In der Informationssicherheit werden verschiedene Schutzziele definiert, um Bedrohungen zu klassifizieren
- Schutz heißt hier: Sicherstellen der Eigenschaften von Objekten und somit mehr als „nur“ Vermeidung von Angriffen
- Traditionell spricht man hierbei von CIA
  - Confidentiality – Vertraulichkeit
  - Integrity – Integrität
  - Availability – Verfügbarkeit

Schutzziele: CIA

- **Confidentiality – Vertraulichkeit**
  - Schutz von Daten vor Kenntnisnahme durch Unbefugte
- **Integrity – Integrität**
  - Schutz von Daten und Systemen vor nicht autorisierten Änderungen
- **Availability – Verfügbarkeit**
  - Sicherstellung der Verfügbarkeit von Daten und Systemen für Befugte

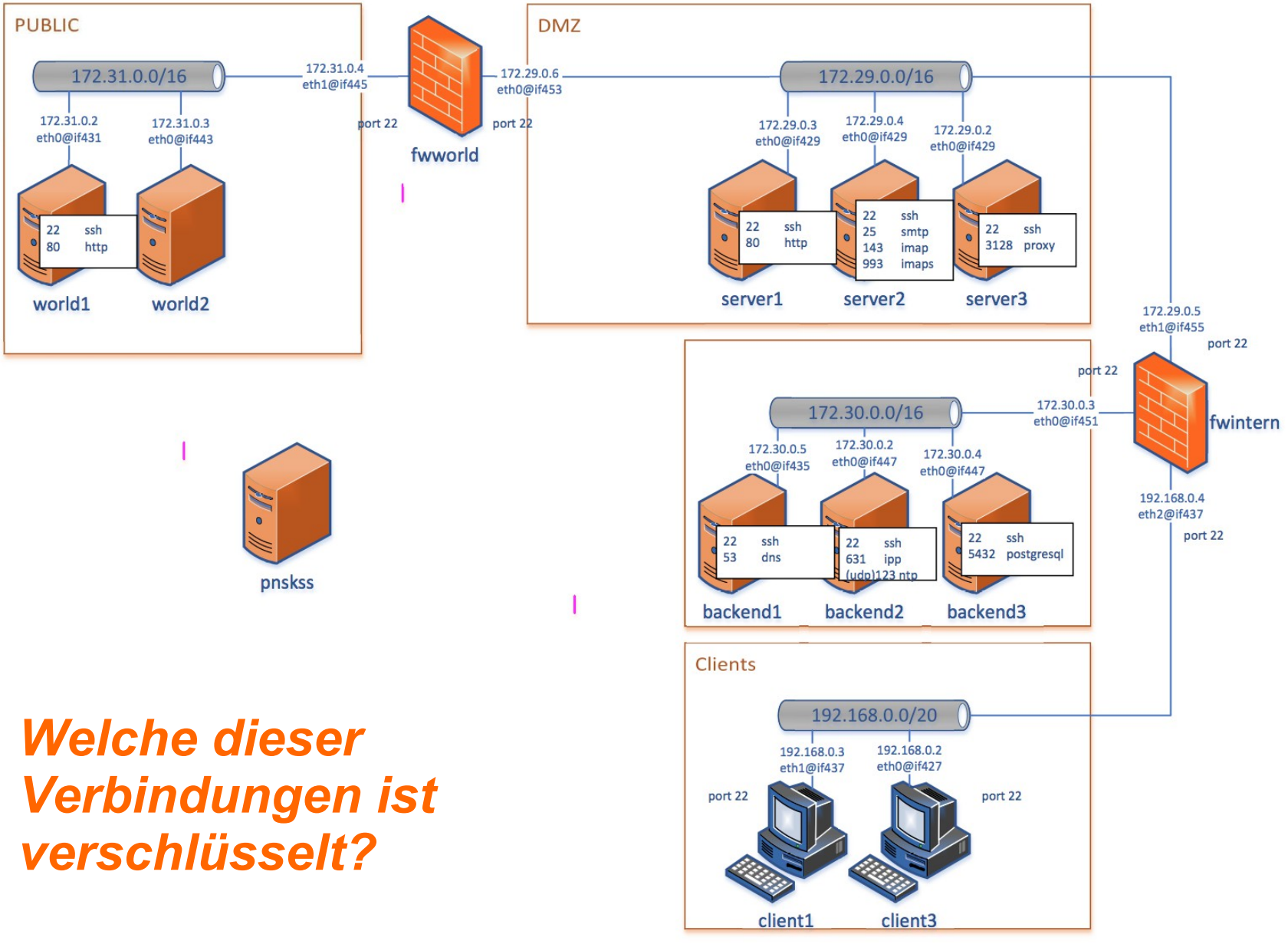
Vertraulichkeit (== Verfügbarkeit)

- **Zugänglichkeit von Daten und Systemen für Befugte**
  - Daten
    - Kundendaten, Webseite, Fotosammlung, Bachelorarbeit
  - Dienste
    - Webseite (Abruf), E-Mail, Netzwerkzugang, Datenbankserver, Hotline
  - Systeme / Anwendungen
    - Arbeitsplatz-PC, Router
    - E-Mail-Client, Webserver

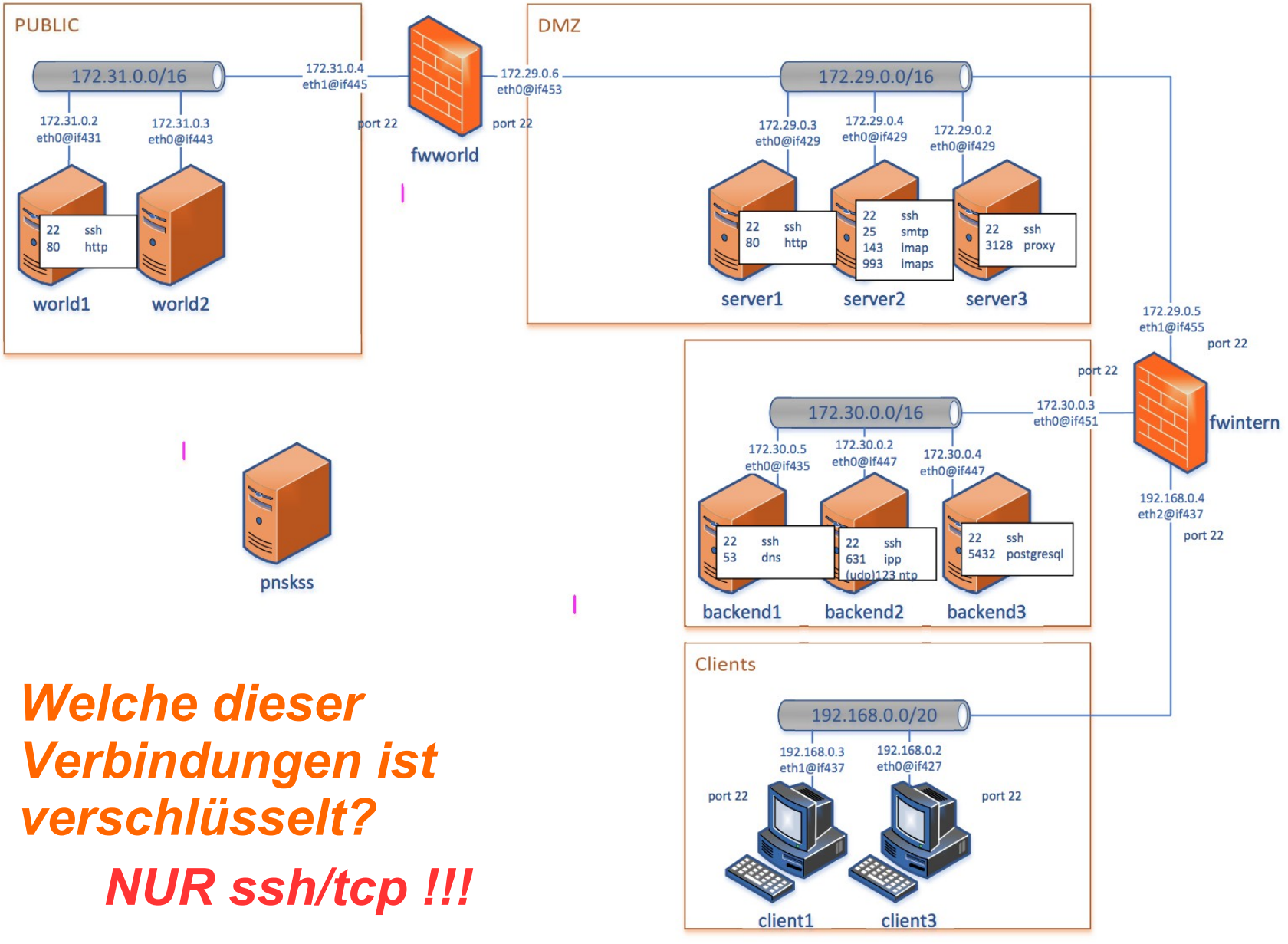
Vertraulichkeit (== Verfügbarkeit)

- **Zugänglichkeit von Daten und Systemen für Befugte**
  - Daten
  - Dienste
  - Systeme / Anwendungen
- **Aber in diesem Kontext wichtiger ist die Umkehrung der Aussage:**

  Keine Zugänglichkeit von Schutzobjekten für Un-Befugte!



Welche dieser Verbindungen ist verschlüsselt?



Welche dieser Verbindungen ist verschlüsselt?

NUR ssh/tcp !!!

Noch ganz andere Probleme

- **Zugänglichkeit von Daten und Systemen für Befugte wollen wir sicherstellen, aber ...**
- **Es gibt besondere Anforderungen, die wir noch gar nicht im Netzplan sehen können:**
  - Remote Access für Berechtigte
  - Zusammenschluss von Standorten
  - Kooperation mit anderen Organisationen
  - …

Schutz der Vertraulichkeit

- Zugänglichkeit von Daten und Systemen für Befugte wollen wir sicherstellen.
- Hierbei gibt es zwei grundlegende Ansätze:

  a) Anwendungen und Dienste stellen den Schutz selbst sicher
  → Änderung der Komponenten

  b) Zusätzliche Komponenten werden eingeführt, die den Schutz übernehmen
  → Änderung der Architektur
- Weitere Anforderung: Benutzertransparenz!

Schutz der Vertraulichkeit

- Zugänglichkeit von Daten und Systemen für Befugte wollen wir sicherstellen.
- Hierbei gibt es zwei grundlegende Ansätze:

  a) Anwendungen und Dienste stellen den Schutz selbst sicher
  → Änderung der Komponenten

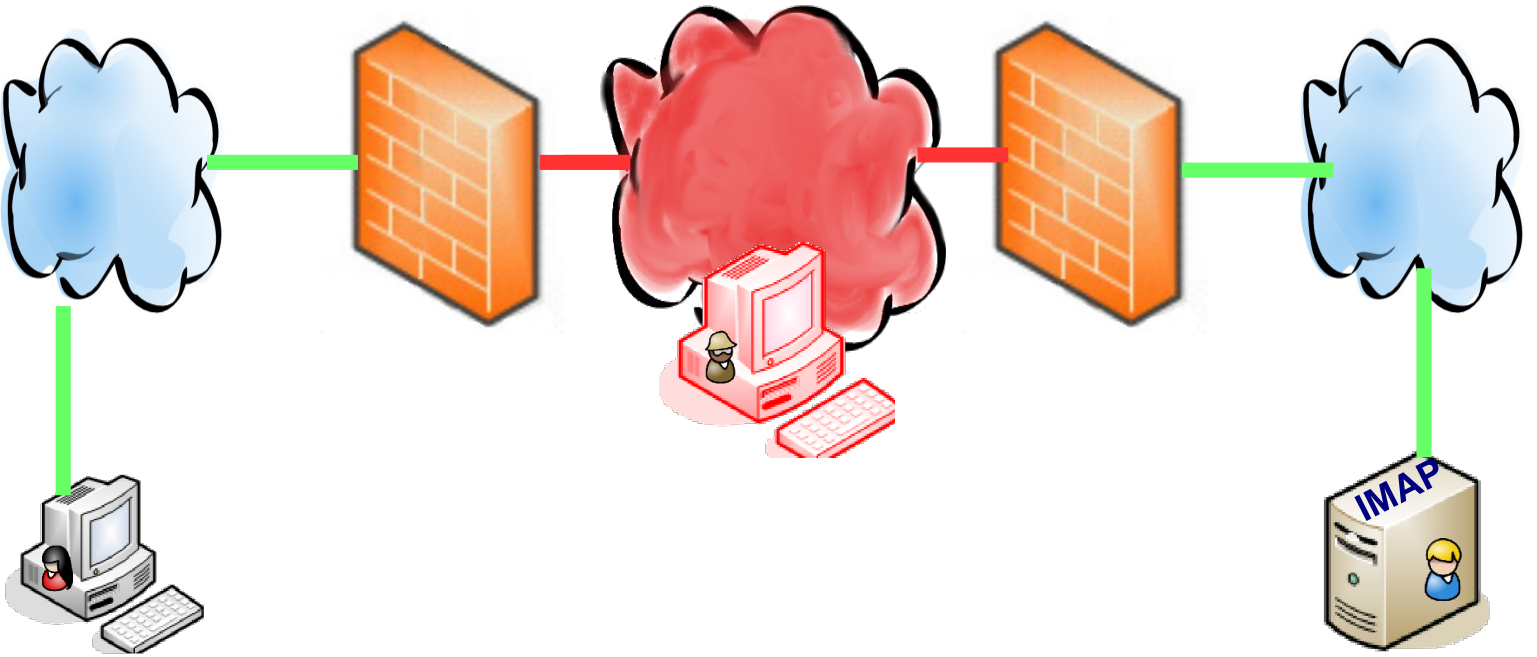
  b) Zusätzliche Komponenten werden eingeführt, die den Schutz übernehmen
  → Änderung der Architektur
- Weitere Anforderung: Benutzertransparenz!

Grundlegende Architekturen:

a) LAN-to-LAN

b) Host-to-LAN

Wie bekommen wir eine transparente Verbindung hin, ohne Anwendungen selbst zu verändern?



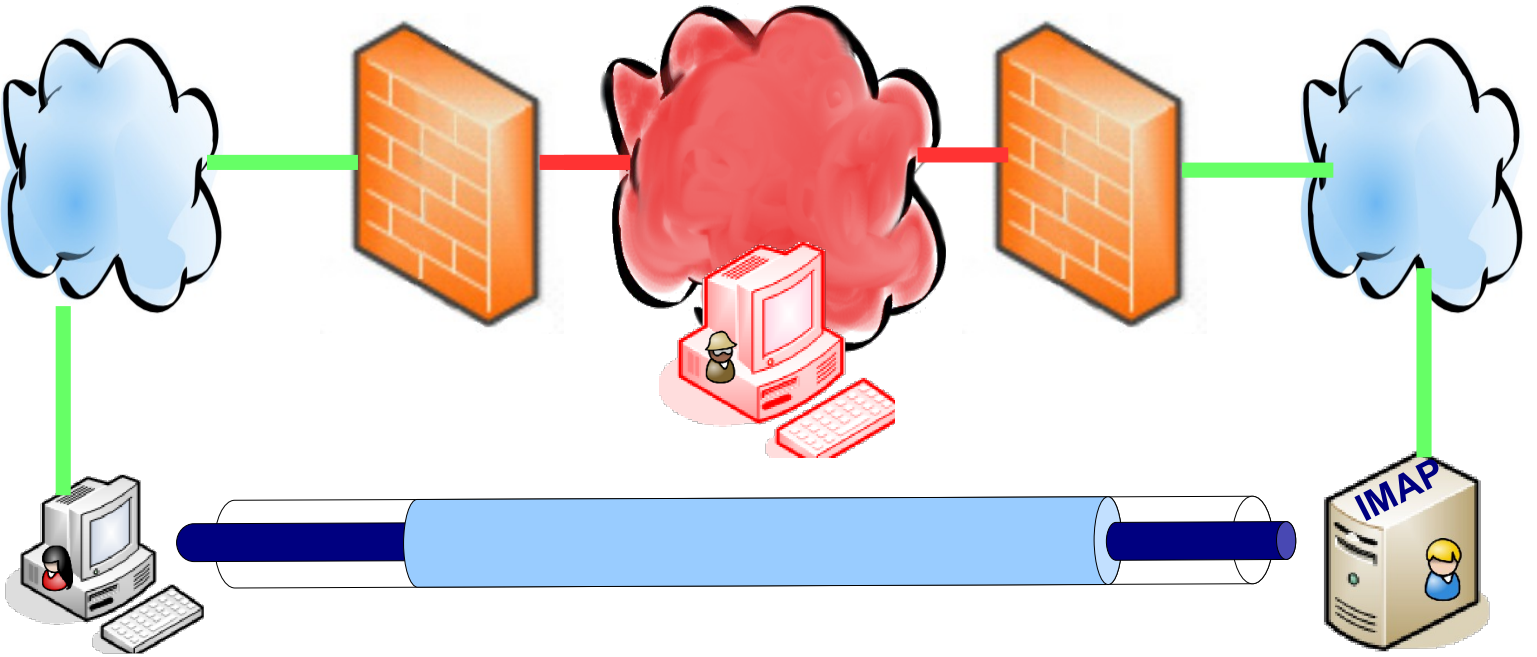
Wie bekommen wir eine transparente Verbindung hin, ohne Anwendungen selbst zu verändern? (2)

weitere Anwendung oder das Betriebssystem erlaubt eine sichere Kommunikation

Wie bekommen wir eine transparente Verbindung hin, ohne Anwendungen selbst zu verändern? (3)

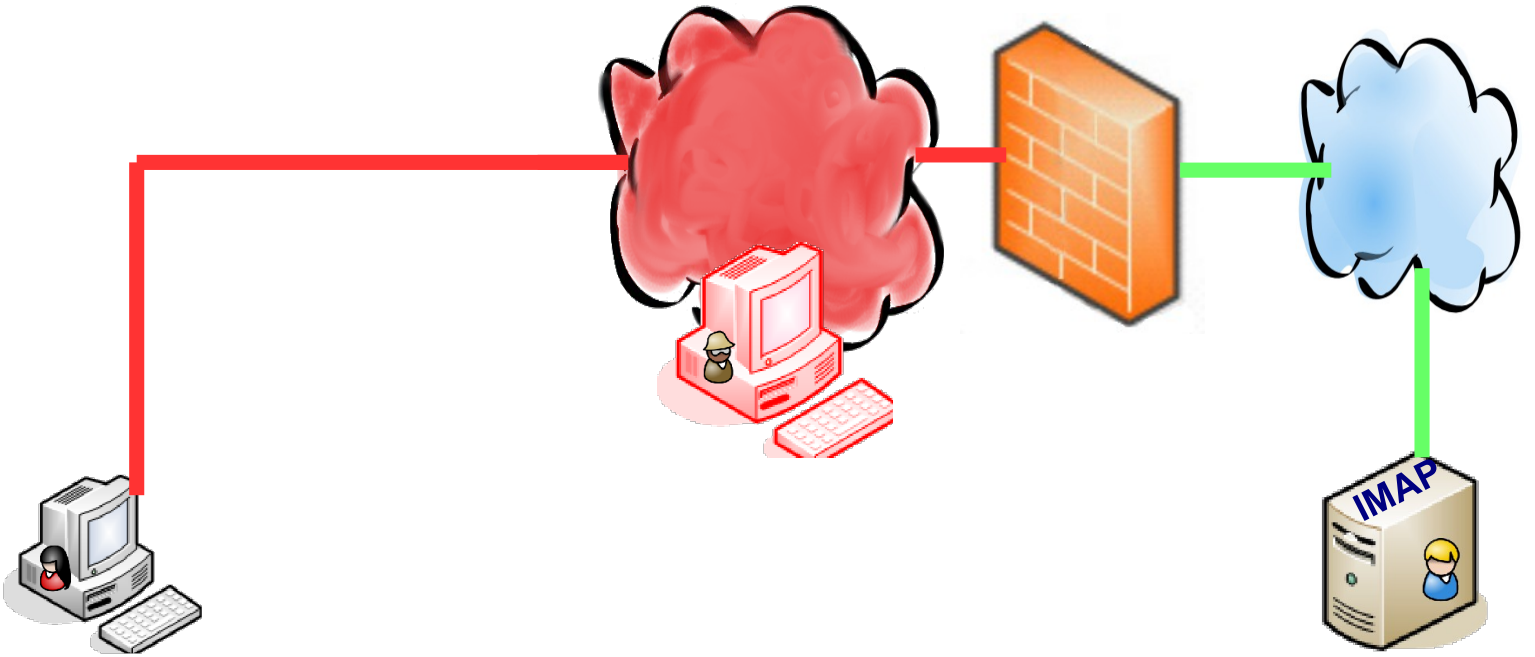
Zwischen den Netzen wird eine sichere Kommunikation angeboten

Wie bekommen wir eine transparente Verbindung hin, ohne Anwendungen selbst zu verändern? (4)



... gibt es auch gleichzeitig!

Wie bekommen wir eine transparente Verbindung hin, ohne Anwendungen selbst zu verändern? (5)



Wie bekommen wir eine transparente Verbindung hin, ohne Anwendungen selbst zu verändern? (6)

weitere Anwendung oder das Betriebssystem erlaubt eine sichere Kommunikation

Wie bekommen wir eine transparente Verbindung hin, ohne Anwendungen selbst zu verändern? (7)

Zum Netz hin wird eine sichere Kommunikation angeboten

Wie bekommen wir eine transparente Verbindung hin, ohne Anwendungen selbst zu verändern? (7)

Auch in diesem Szenario geht beides miteinander ...

Konzept eines „sicheren“ Tunnels

- **Welche „Zutaten“ braucht solch ein „Tunnel“?**
  - Authentisierung der Tunnelendpunkte bzw. der Benutzerprozesse, die diesen nutzen
  - „Data origin authentication“, also die gesicherte Herkunft von Daten bzw. Urheberschaft
  - Vertraulichkeit gegenüber Unberechtigten
- **Was liefern Tunnel nicht?**
  - Gesicherte Verfügbarkeit
  - Keine Zusicherung des Empfangs
  - Zusicherungen auf Ebene der Anwendungen

Technische Grundlagen für Vertraulichkeit

- **Ohne Verschlüsselung kein Schutz vor unberechtigtem Zugriff**
  - Schlüsselmanagement als wesentliche Teilaufgabe beim Betrieb von „Tunneln“
- **Hier könnten wir jetzt tagelang in die Kryptographie ein- oder absteigen**
  - Das ist jedoch Aufgabe anderer Vorlesungen
  - Viele Details nachzulesen unter https://users.informatik.haw-hamburg.de/~kpk/itsicherheit.html

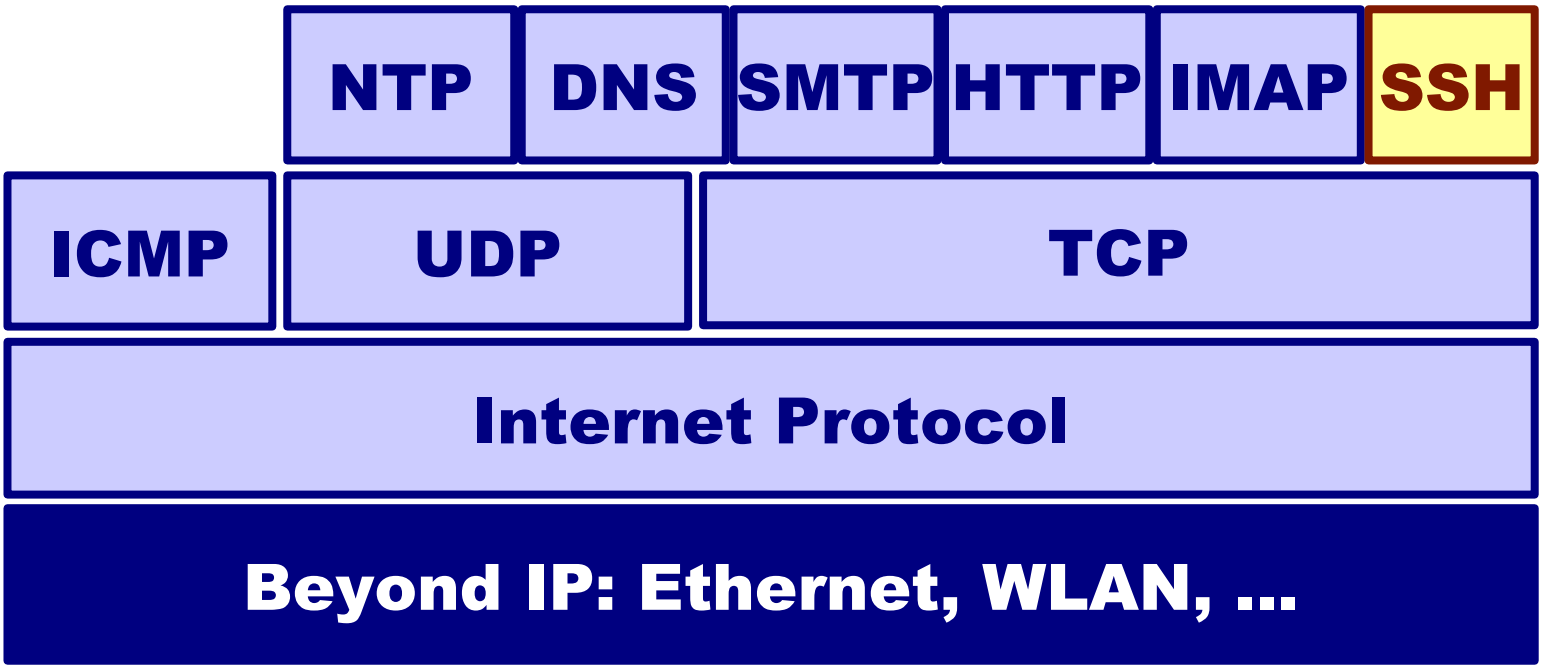
Technische Standards für sichere Tunnel

Besser bekannt als „Virtual Private Networks“

Standard	L2F	L2TP	PPTP	IPsec	mit SSH
non-IP	✓	✓	✓	✗	✗
LAN-to-LAN	○	○	○	✓	○
Host-to-LAN	✓	✓	✓	○	○
Host-to-Host	✗	✗	✗	○	✓
Schicht	2	2	2	3	4: tcp 7: tcp

Einfache Lösung für alle TCP-basierten Anwendungen: Secure Shell (ssh, 22/tcp)

SSH im TCP/IP-Stack



SSH: Überblick

SSH = Secure Shell.

- Ersetzte nach 1993 die sehr unsicheren Anwendungen rsh, rlogin, rcp und telnet
- Vor allem zunächst sicherer Zugang für Administratoren
- Dann Unterstützung von sicherem Datei-Transfer, auch sftp
- Durch generisches (TCP-) Port Forwarding einfache Möglichkeit, Anwendungen gegen Abhören zu schützen → Vertraulichkeit!

SSH-1 versus SSH-2

(Zu-) viele Schwachstellen waren enthalten:

- SSH-1 Insertion attack exploiting weak integrity mechanism (CRC-32) and unprotected packet length field
- SSHv1.5 session key retrieval attack (theoretical)
- Man-in-the-middle attacks (z.B. mit dsniff)
- DoS attacks
- Overload server with connection requests
  - Buffer overflows

SSH: Überblick (2)

SSH-1 fehlerhaft, SSH-2 mit neuer Architektur

- Erfordert Änderungen bei Architektur des Netzes (neuer Server, eventuell mehrere)
- Erfordert Anpassungen der Konfiguration
- Bedingt Schulung der Anwender
- Schützt nur TCP-Verbindungen und muss auch durch die Firewall durchgesetzt werden

SSH: Überblick (3)

SSH Communications Security (SCS).

- www.ssh.com.
- Gründed durch Tatu Ylonen, Entwickler von SSH-1.

Open source version heißt OpenSSH

IETF Secure Shell (SECSH) working group:

- Standard für SSH nach langer, langer Diskussion und viel Streit über die „richtige“ Architektur und die „beste“ Lösung

SSH RFCs (Auswahl)

- RFC 4250 – The Secure Shell (SSH) Protocol Assigned Numbers
- RFC 4251 – The Secure Shell (SSH) Protocol Architecture
- RFC 4252 – The Secure Shell (SSH) Authentication Protocol
- RFC 4253 – The Secure Shell (SSH) Transport Layer Protocol
- RFC 4254 – The Secure Shell (SSH) Connection Protocol
- RFC 4255 – Using DNS to Securely Publish Secure Shell (SSH) Key Fingerprints
- RFC 4256 – Generic Message Exchange Authentication for the Secure Shell Protocol (SSH)
- RFC 4335 – The Secure Shell (SSH) Session Channel Break Extension
- RFC 4344 – The Secure Shell (SSH) Transport Layer Encryption Modes
- RFC 4345 – Improved Arcfour Modes for the Secure Shell (SSH) Transport Layer Protocol
- RFC 4419 – Diffie-Hellman Group Exchange for the Secure Shell (SSH) Transport Layer Protocol
- RFC 4432 – RSA Key Exchange for the Secure Shell (SSH) Transport Layer Protocol
- RFC 4462 – Generic Security Service Application Program Interface (GSS-API) Authentication and Key Exchange for the Secure Shell (SSH) Protocol
- RFC 4716 – The Secure Shell (SSH) Public Key File Format
- RFC 4819 – Secure Shell Public Key Subsystem

SSH-2 Architektur

Mit SSH-2 kommen drei Schichten/Protokolle:

SSH Transport Layer Protocol

- Initiale Verbindung
- Server Authentication
- Sicherer Kanal zwischen Client und Server

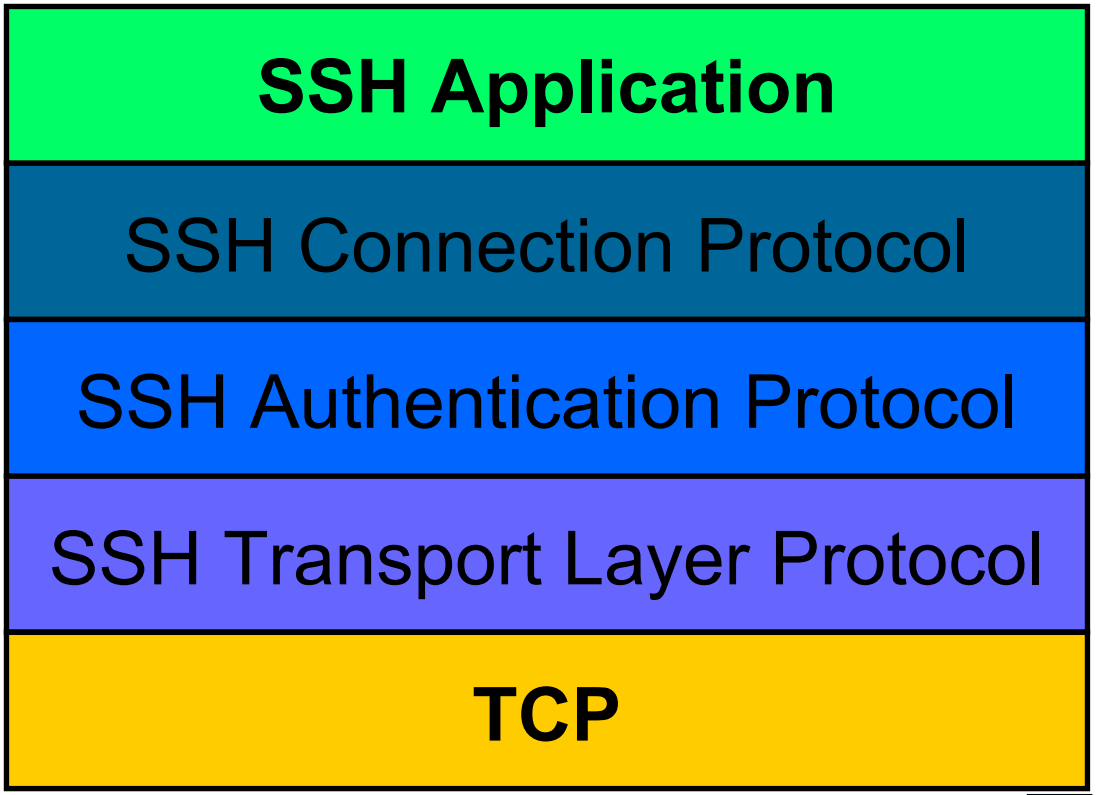
SSH Authentication Protocol

- Client Authentication über etablierten Kanal

SSH Connection Protocol

- Multiplexing und Session Re-Use

SSH-2 Architektur (2)



SSH-2 Sicherheitszusicherungen

- **In Bezug auf die Authentisierung**
  - Server wird immer authentisiert (transport layer protocol)
    - Public Key (DSS oder RSA)
  - Client wird immer authentisiert (authentication protocol)
    - Entweder Public Key (DSS, RSA, SPKI, OpenPGP, ...)
    - Oder das „normale“ Benutzerpasswort
- **Durch sicheren Kanal keine Klartextübertragung von Passworten!**

SSH-2 Algorithmen (für Fortgeschrittene)

Generierung eines „frischen“ Shared Secrets

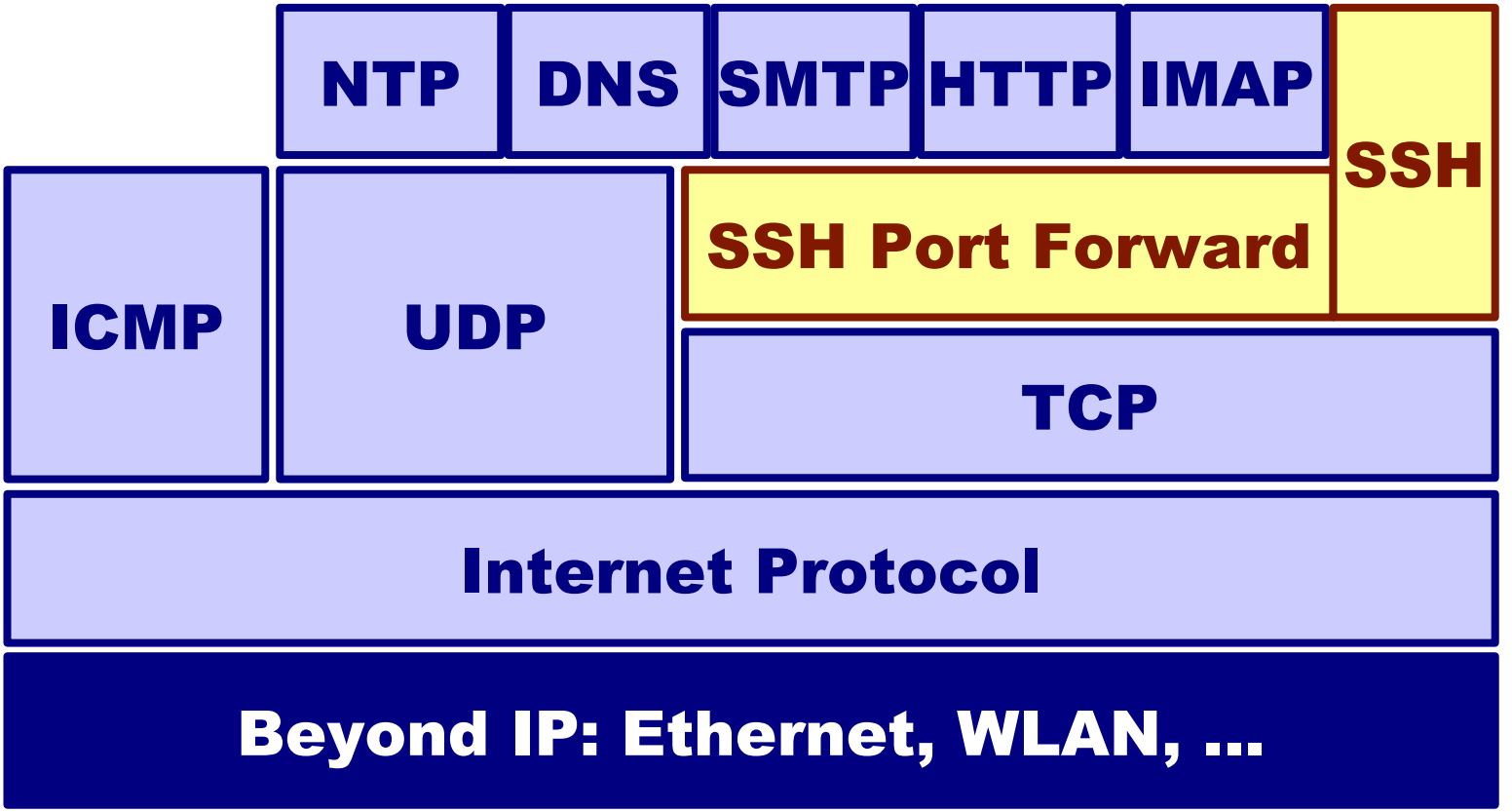
- Von diesem wird weiteres kryptographisches Material abgeleitet
- Sichert Vertraulichkeit und Authentisierung (transport layer protocol)

Diffie-Hellman key exchange

Einigung auf kryptographische Verfahren

- 3DES, RC4 oder AES
- HMAC-SHA1 oder HMAC-MD5
- Kompressionsalgorithmen

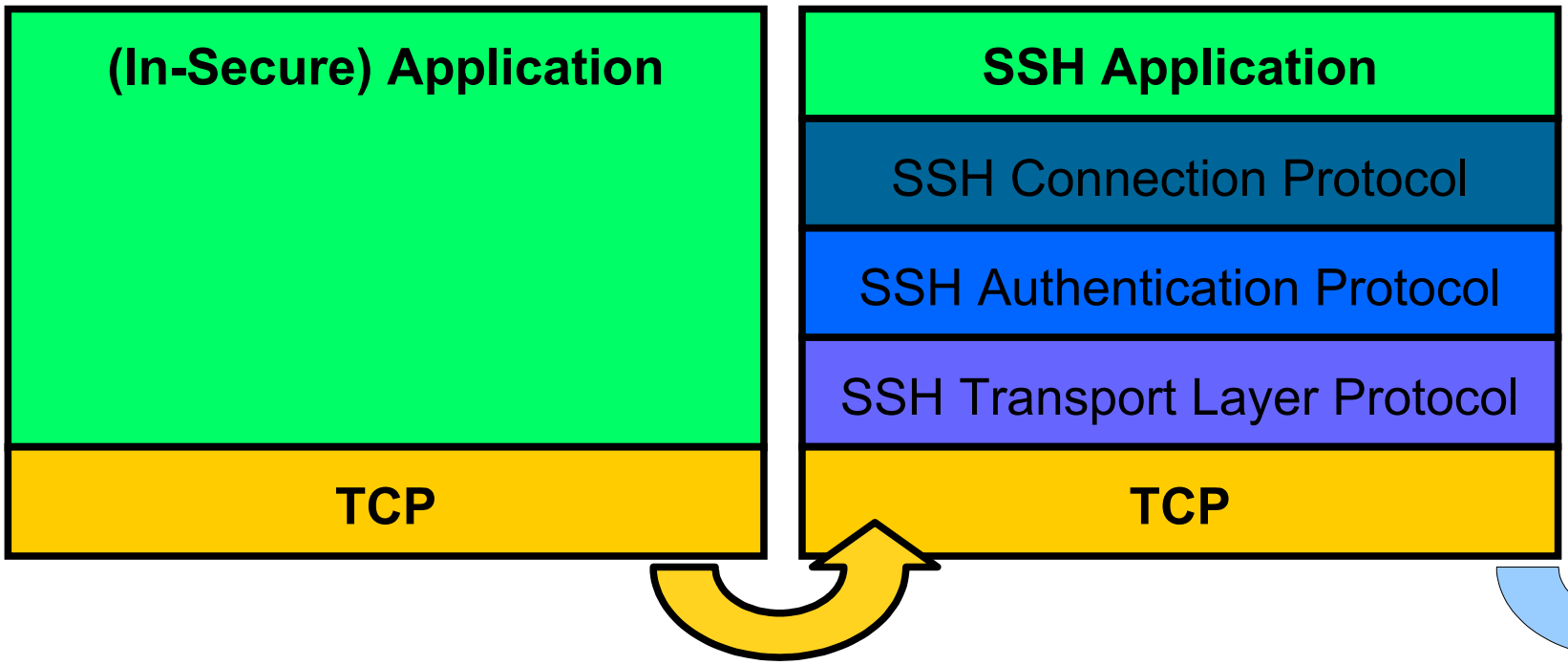
SSH im TCP/IP-Stack – Port Forward



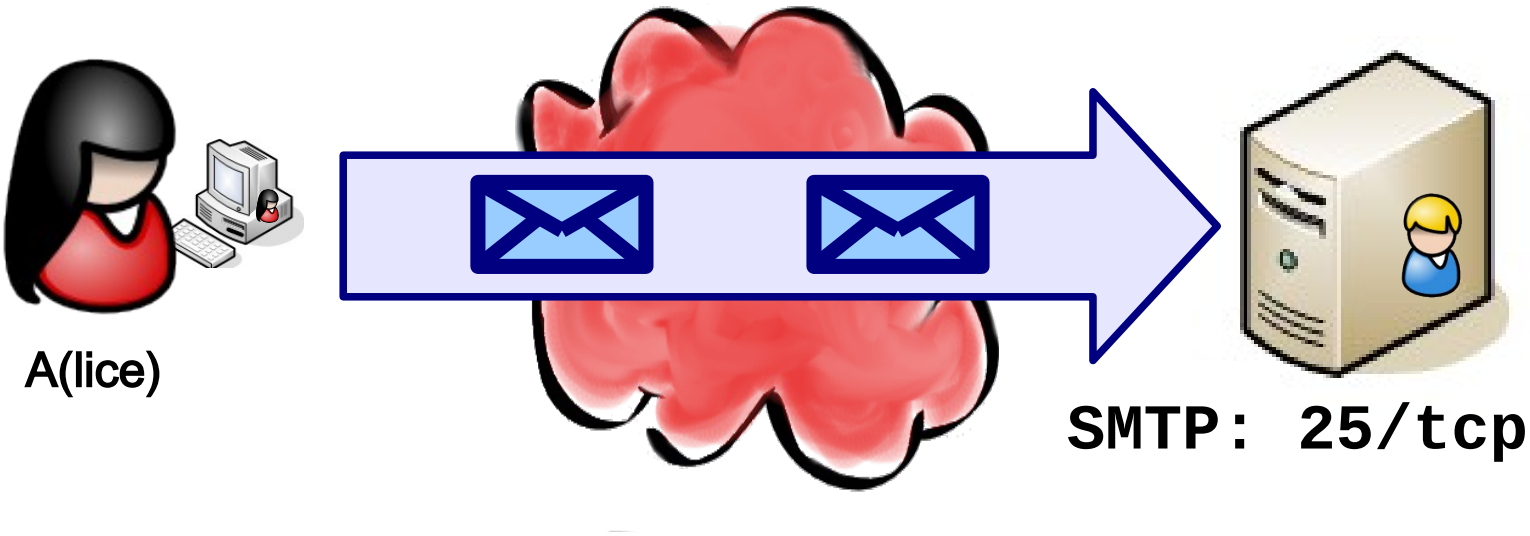
SSH-2 Architektur (3) : Forwarding

A(lice)

- Alice startet erst SSH, dann die eigentliche Anwendung
- Kommunikation über localhost mit TCP



Nun zum Wesentlichen: (TCP-) Port-Forwarding



SSH Port Forwarding

TCP-Dienste werden über Ports differenziert!!!

SSH-Client auf lokaler Maschine (localhost):

- Empfängt z. B TCP-Verbindung über Port 5113/tcp
- Durch Konfiguration wird dieser Port an einen entfernten Port geknüpft
  - z. 5113/tcp → 25/tcp auf Host “smtp”
- Daten werden an SSH-Server geschickt

SSH-Server:

- Empfängt Daten vom Client / „legt“ diese aufs Netz
- Antworten des Hosts „smtp“ schickt er “zurück“

SSH Port Forwarding: Konfiguration

A(lice)

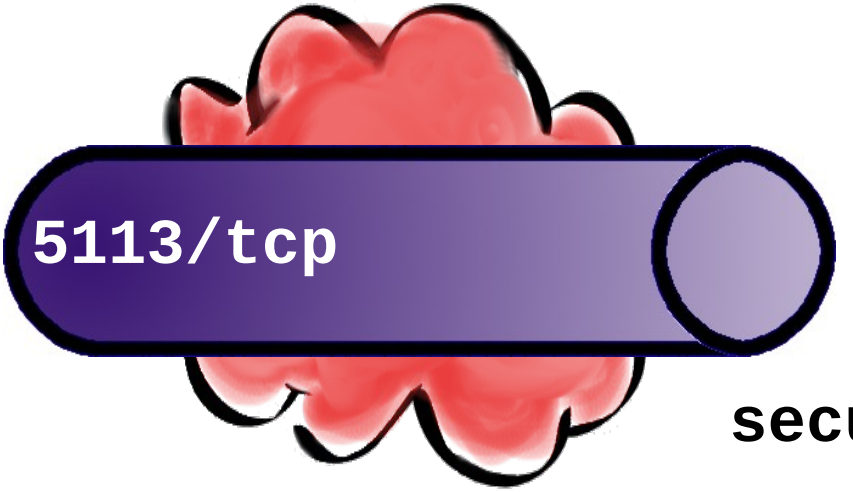
secure: 22/tcp

```
%alice@laptop> more .ssh/config
Host secure.domain.de
    User alice
    IdentityFile /home/alice/.ssh/intern
    Port 22
    Protocol 2
    LocalForward 5113 smtp.domain.de:25
    [...]
    EscapeChar ~
    KeepAlive yes
```

smtp: 25/tcp

SSH Port Forwarding: Aufbau SSH

A(lice)



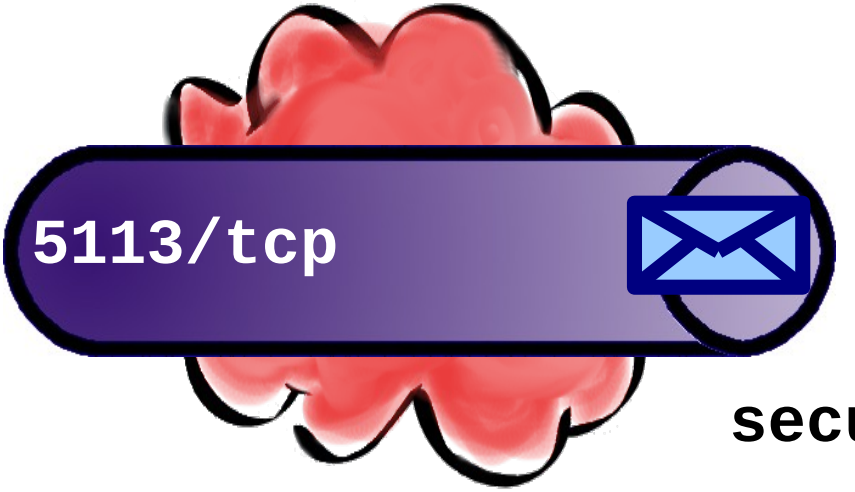
secure: 22/tcp

```
%alice@laptop> ssh secure.domain.de
Last login on 2 February 2009
                  from dsl.somewhere.de
Have a lot of fun!
%[alice@laptop]@secure>
```

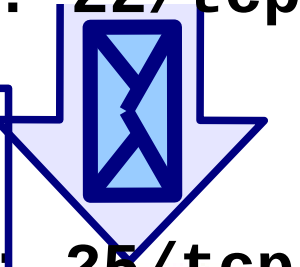
smtp: 25/tcp

SSH Port Forwarding: Email senden

A(lice)



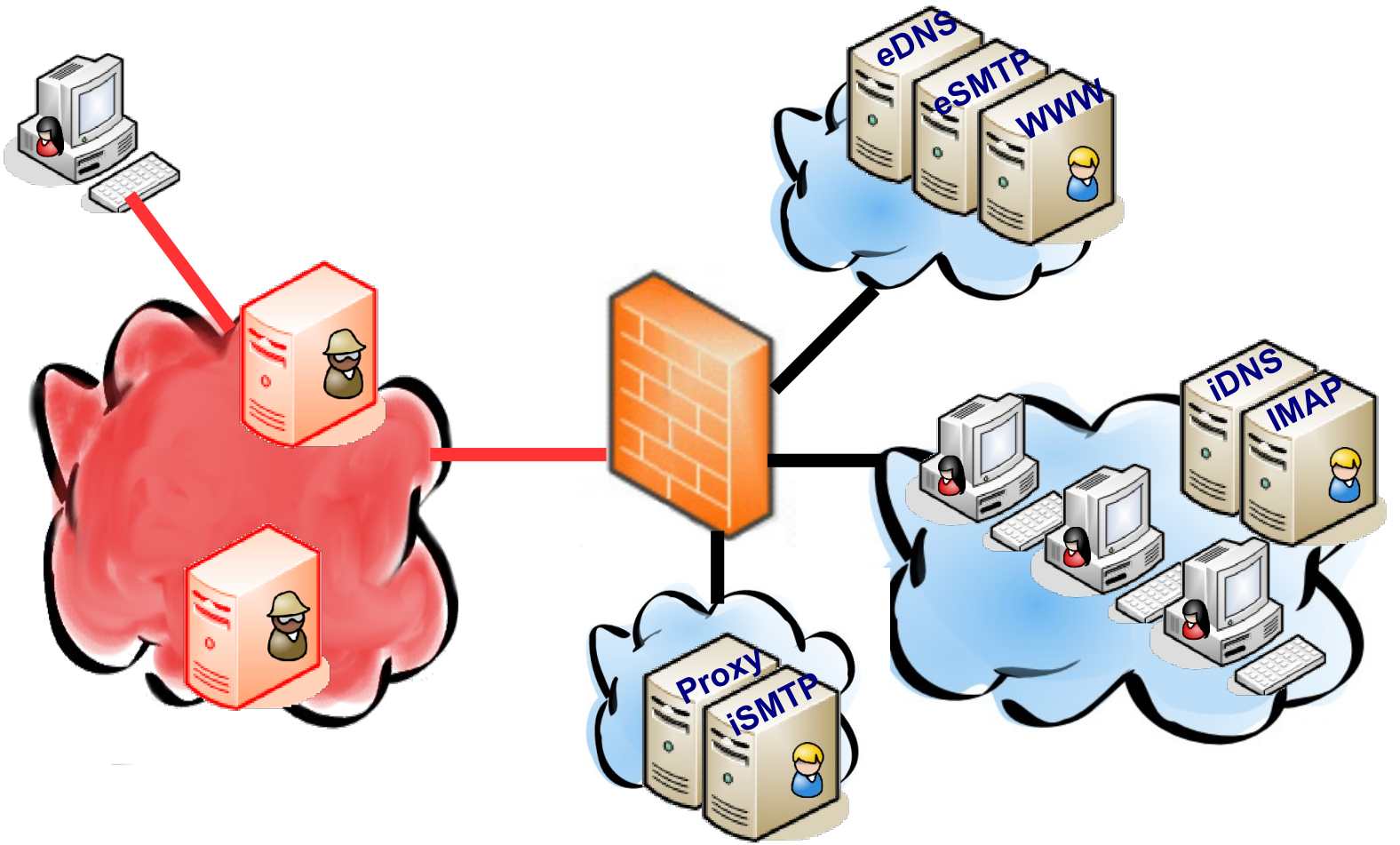
secure: 22/tcp



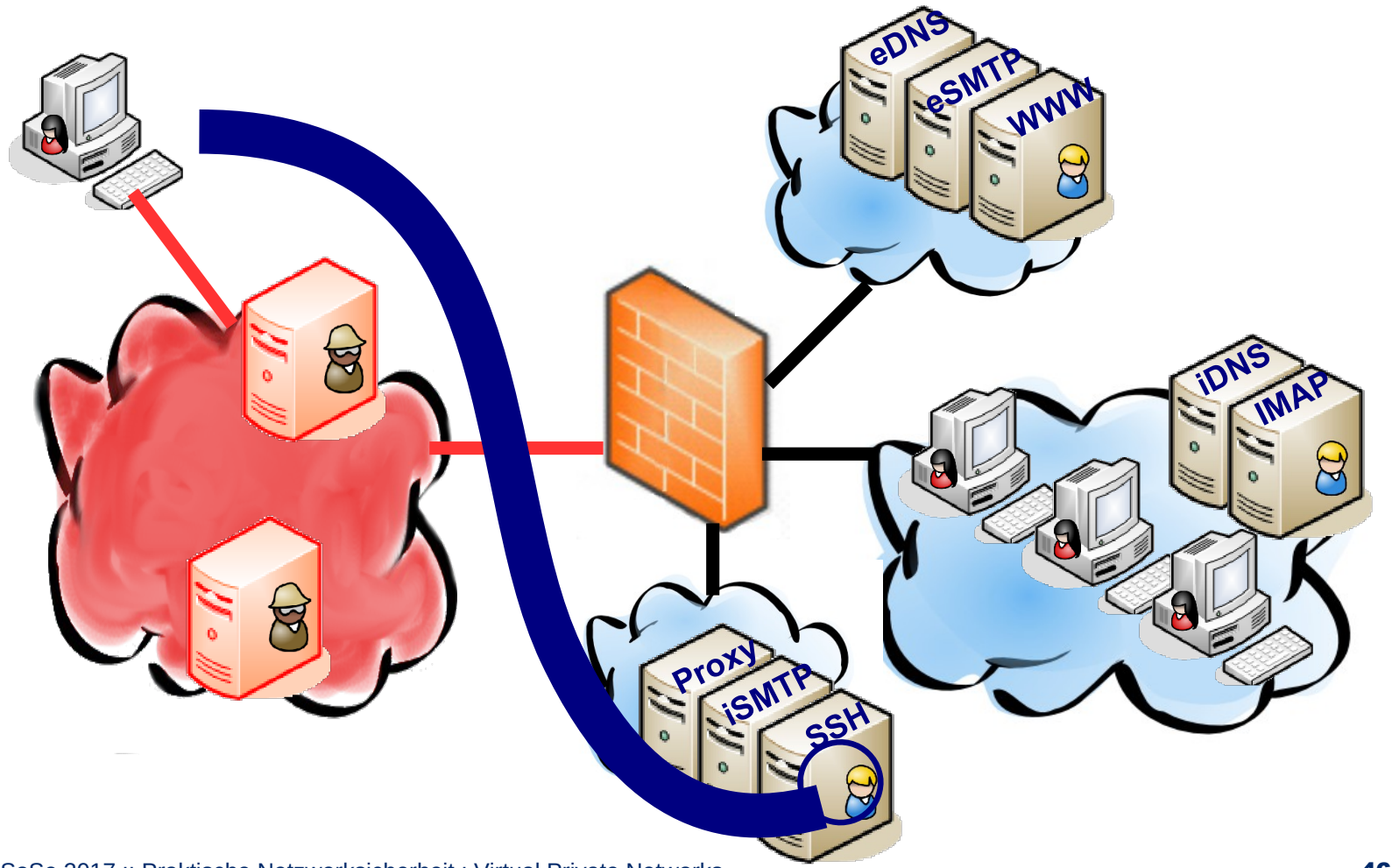
smtp: 25/tcp

```
%alice@laptop> telnet localhost:25
Trying 127.0.0.1 ...
Connected to localhost.
Escape character is '^]'.
220 smtp.domain.de ESMTP Postfix ...
HELO laptop.domain.de
250 secure.domain.de Hello laptop, pleased to meet you
MAIL FROM: alice@domain.de
250 alice@domain.de ... Sender ok
RCPT TO: someone@somewhere.de
250 someone@somewhere.de ... Recipient ok
DATA
```

Und wo jetzt hin mit dem SSH-Server?

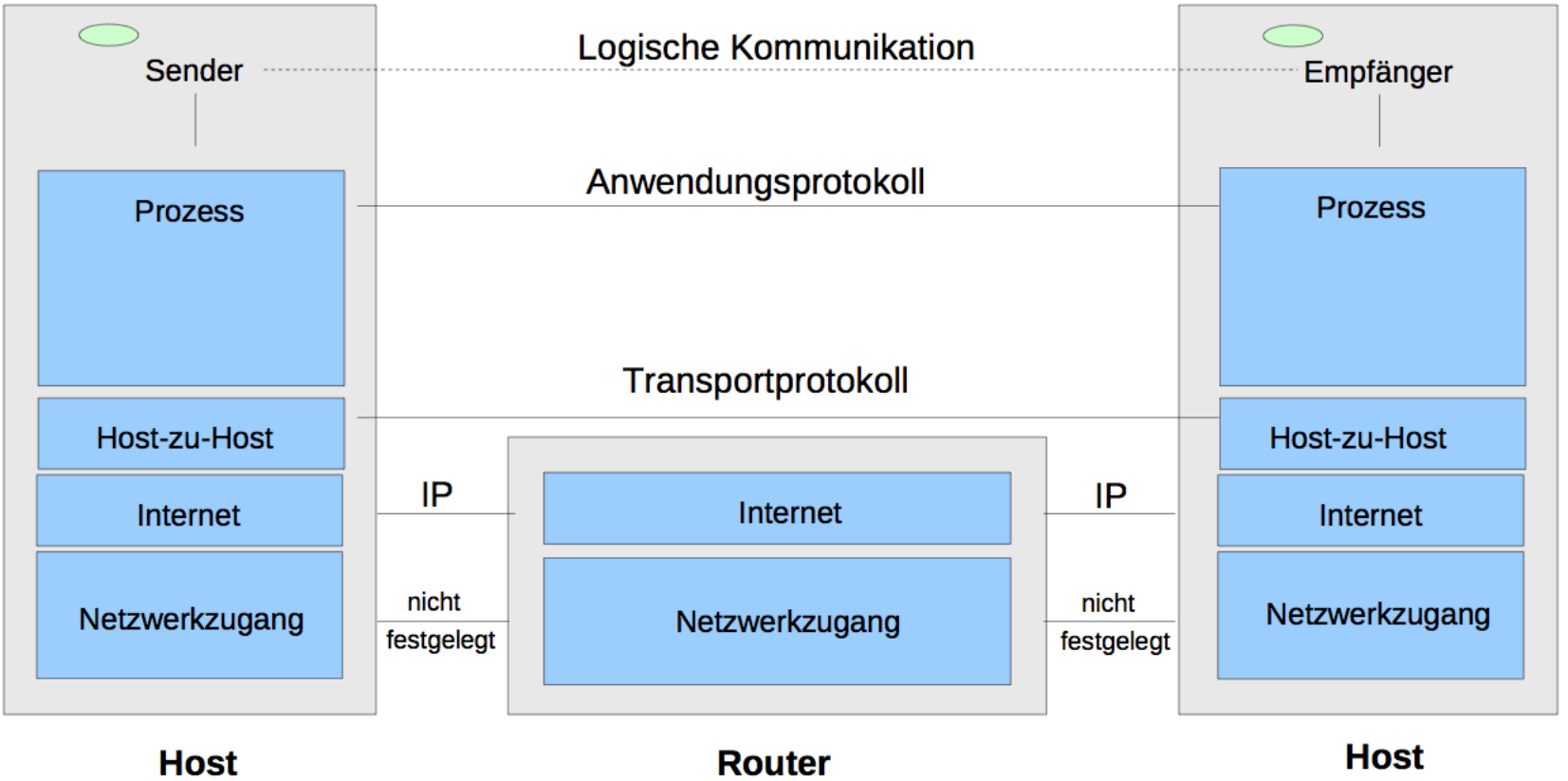


Und wo jetzt hin mit dem SSH-Server? (2)

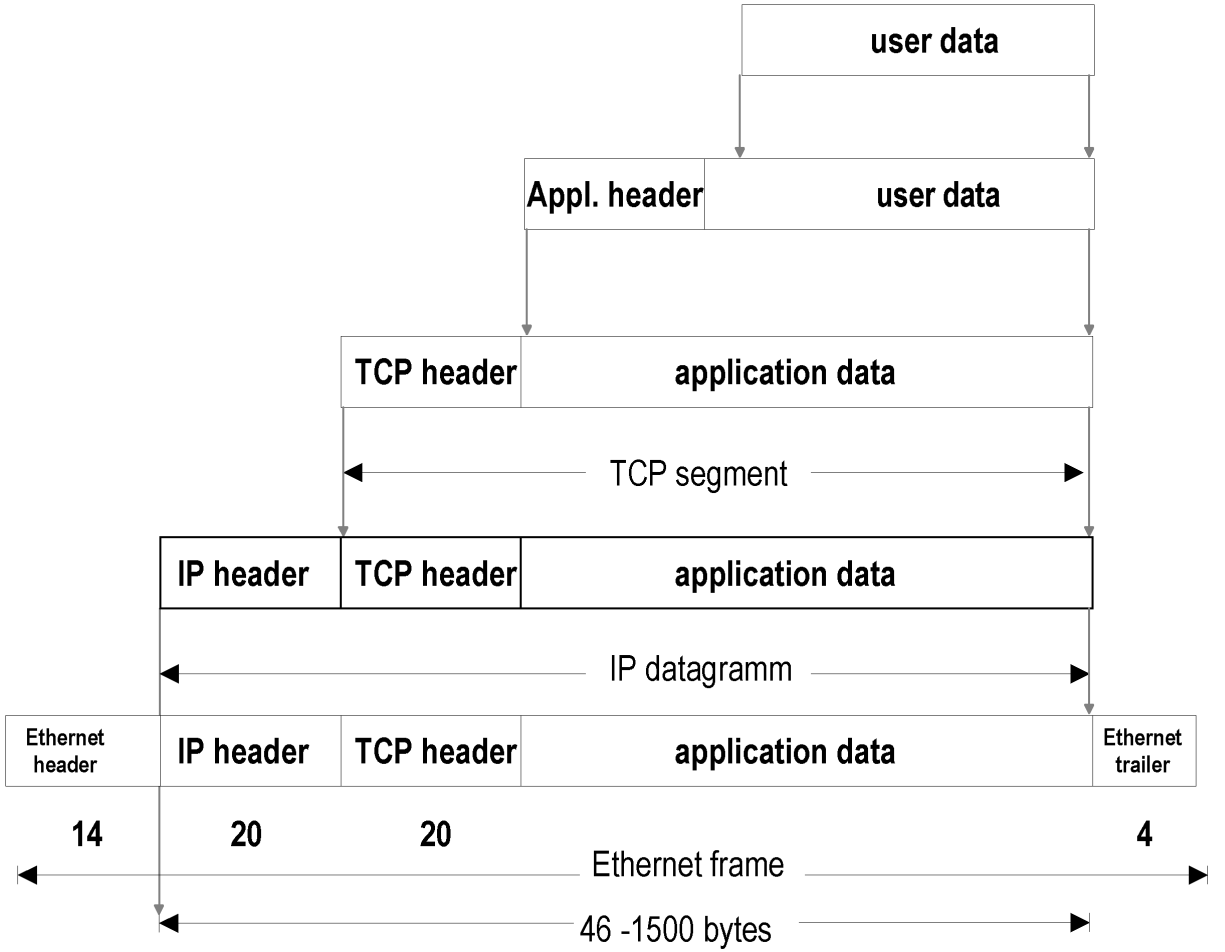


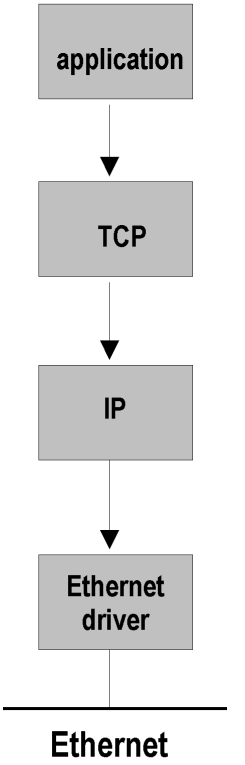
Aber wohin mit den größeren Lösungen?

TCP/IP Schichtenmodell



Jedem Protokoll seinen Header

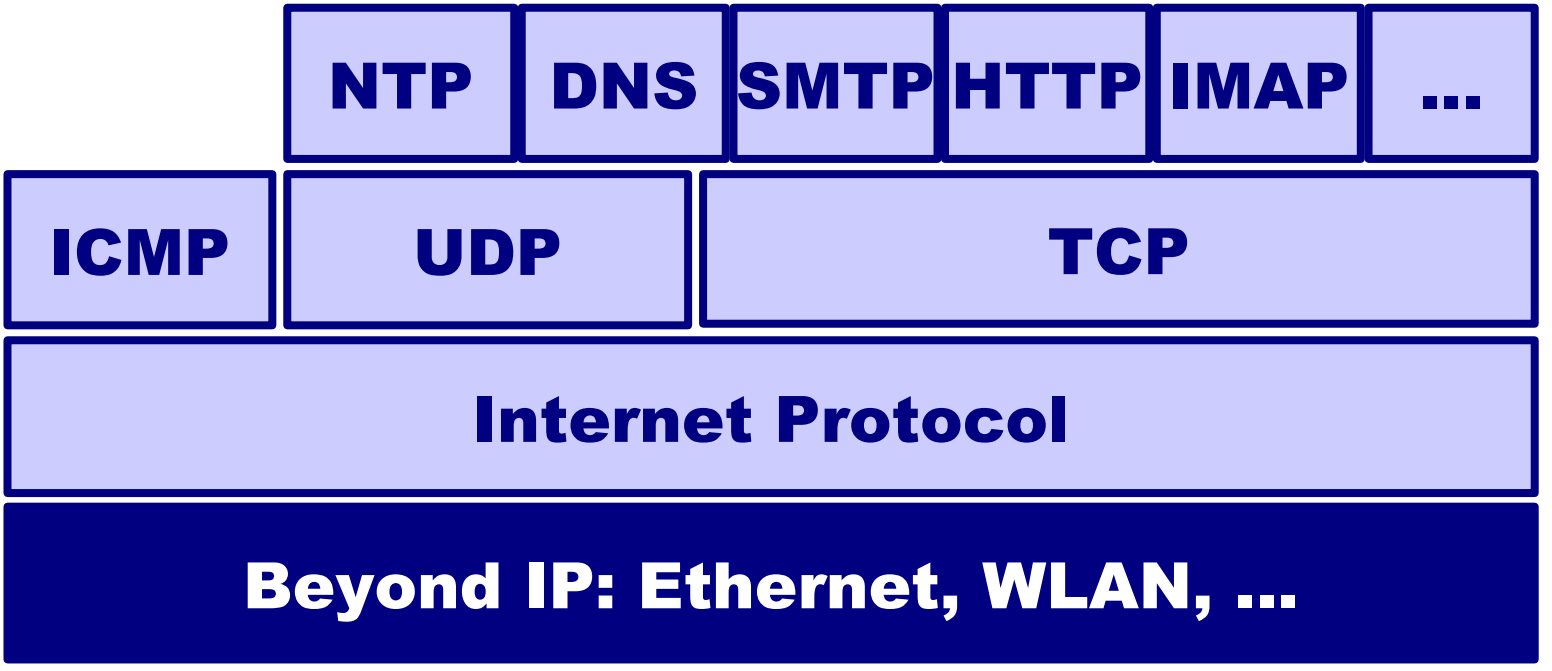




Wo gehört den Sicherheit hin?

- **Bei den Überlegungen zum TCP/IP-Stack waren Sicherheitsziele eher nicht im Fokus der Entwickler**
  - Das Internet sollte keine kritischen Informationen haben
  - Das die Gesellschaft davon abhängen würde, war niemandem (okay, es gab schon Mahner und ein paar Visionäre) klar [damals war Internet wirklich „Neuland“, und niemand hätte gedacht, das es Leute gibt, die im Neuland zuhause sind und jemand anderem den Krieg erklären ...]

Wie immer die Qual der Wahl! (2)



Wo gehört den Sicherheit hin? (2)

- **Bei den Überlegungen zum TCP/IP-Stack waren Sicherheitsziele eher nicht im Fokus der Entwickler**
- **Erst nach und nach gab es konkrete Erkenntnisse:**

  a) Internet Sniffer

  - Seit Anfang der 80er Jahre bekannt
  - Erst 1993 laufen Festplatten über, weil zuviele Passworte mitgeschrieben wurden
  - 1985: TCP Sequence Number Guessing

Wo gehört den Sicherheit hin? (3)

- **Bei den Überlegungen zum TCP/IP-Stack waren Sicherheitsziele eher nicht im Fokus der Entwickler**
- **Erst nach und nach gab es konkrete Erkenntnisse:**
  - **a) Internet Sniffer**
  - **b) IP Spoofing**
    - 1985: Bellovin (u.a.) warnt vor ratbaren Sequenznummern
    - 1994: CERT Advisory wegen Verbreitung eines funktionierenden Angriffswerkzeugs

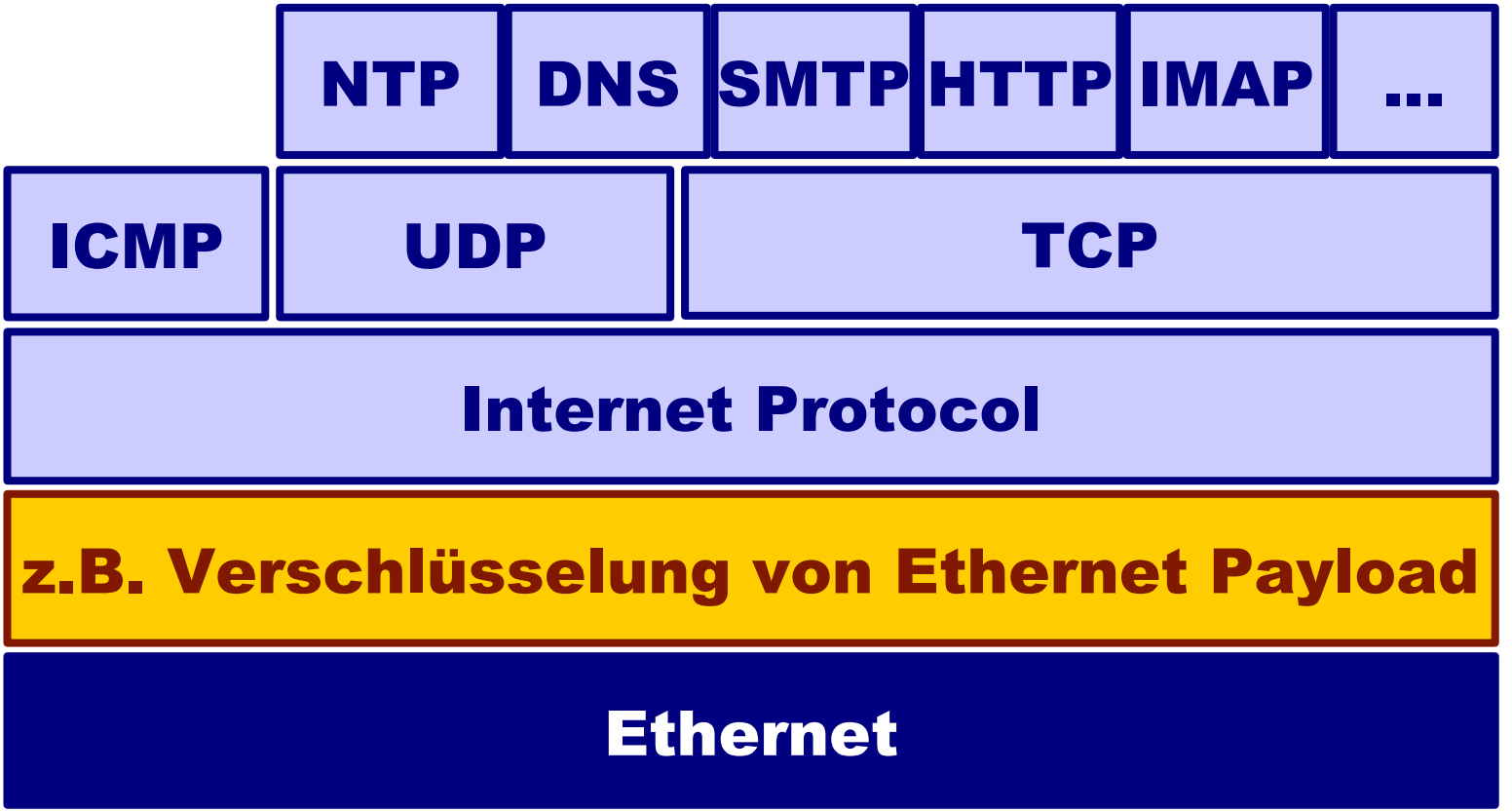
Gibt es Sicherheit auf Schicht 1?

- **Angriffe auf Schicht 1**
  - Kabel haben u.a. magnetische Abstrahlung
  - Glasfaser kann gebogen und ausgelesen werden
  - Funk ist in gewissen Abständen direkt mitlesbar
    - Kann nicht direkt beobachtet werden!
- **Kabel werden durchaus in Röhren gepackt, in denen ein Gas enthalten ist, damit kann z.B. geprüft werden, ob jemand dran geht**

Gibt es Sicherheit auf Schicht 2?

- **Tatsächlich dient die Schicht 2 ja vor allem technischen Anbindung des Mediums aus Schicht 1**
  - Aber tatsächlich gibt es hier Software (!)
  - Mit allen bekannten Problemen (!!)
- **Gibt es spezifische Angriffe auf dieser Schicht?**
  - Klar (!!!)
  - Aber wenige, und oft ein begrenzter Scope
    - z.B. ARP-Spoofing bei Ethernet

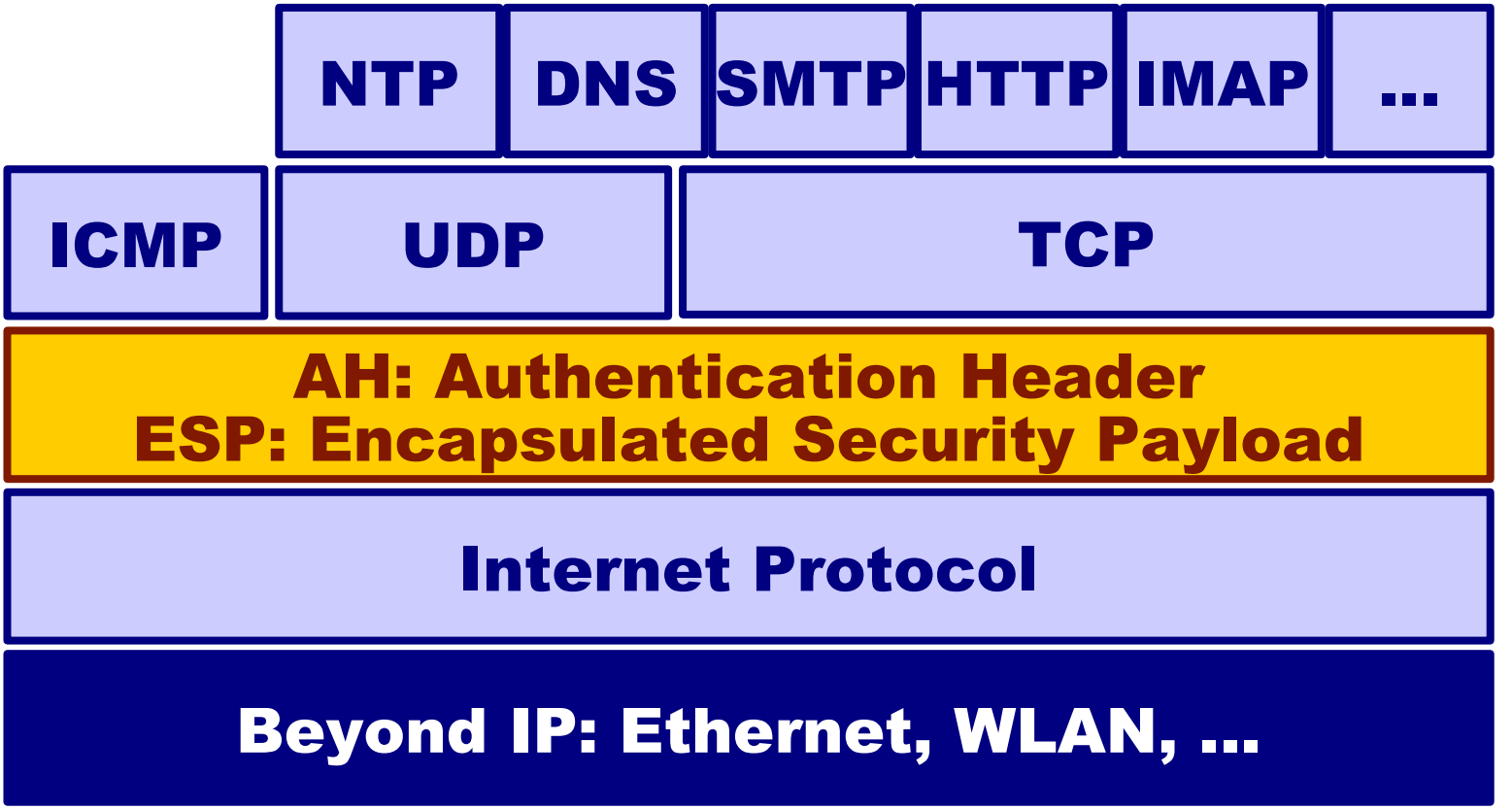
Was könnte man machen?
LAN-Crypter



Gibt es Sicherheit auf Schicht 3?

- **Die Grundlage des TCP/IP-Stacks ermöglicht die weltweite Adressierung (IP-Adressen) und realisiert das Routing, so dass IP-Pakete tatsächlich ankommen**
  - Router schauen nur auf Empfängeradresse
  - IP-Adressen können gesetzt werden
  - IP-Pakete sind unverschlüsselt und nicht signiert
- **Gibt es spezifische Angriffe auf dieser Schicht?**
  - Angriffe betreffen auch höhere Schichten!

Es muss in den Standard passen: IPsec (optional bei IPv4) oder IPv6



Mit AH und ESP können z.B. solche Strukturen aufgebaut werden

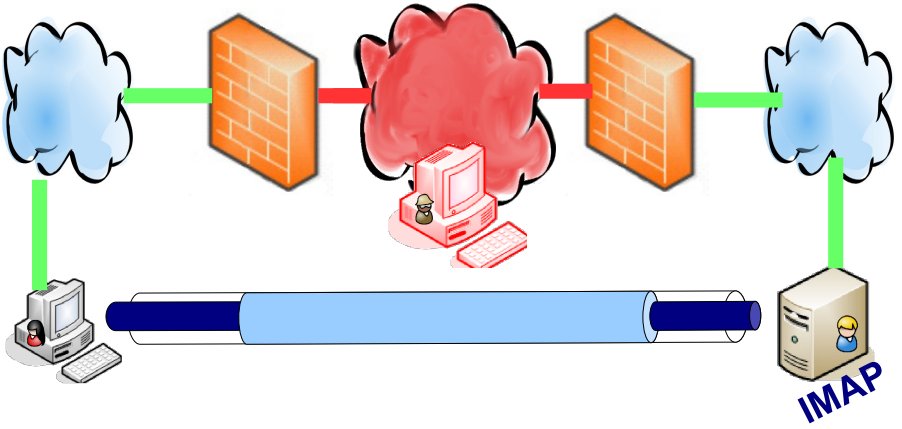
... tatsächlich sind dies 16 mögliche Kombinationen!

Mit AH und ESP können z.B. solche Strukturen aufgebaut werden (2)

*) keine gefälschten Pakete zwischen FWs

**) wie *) nur indirekt

***) auch im LAN kein Mitlesen



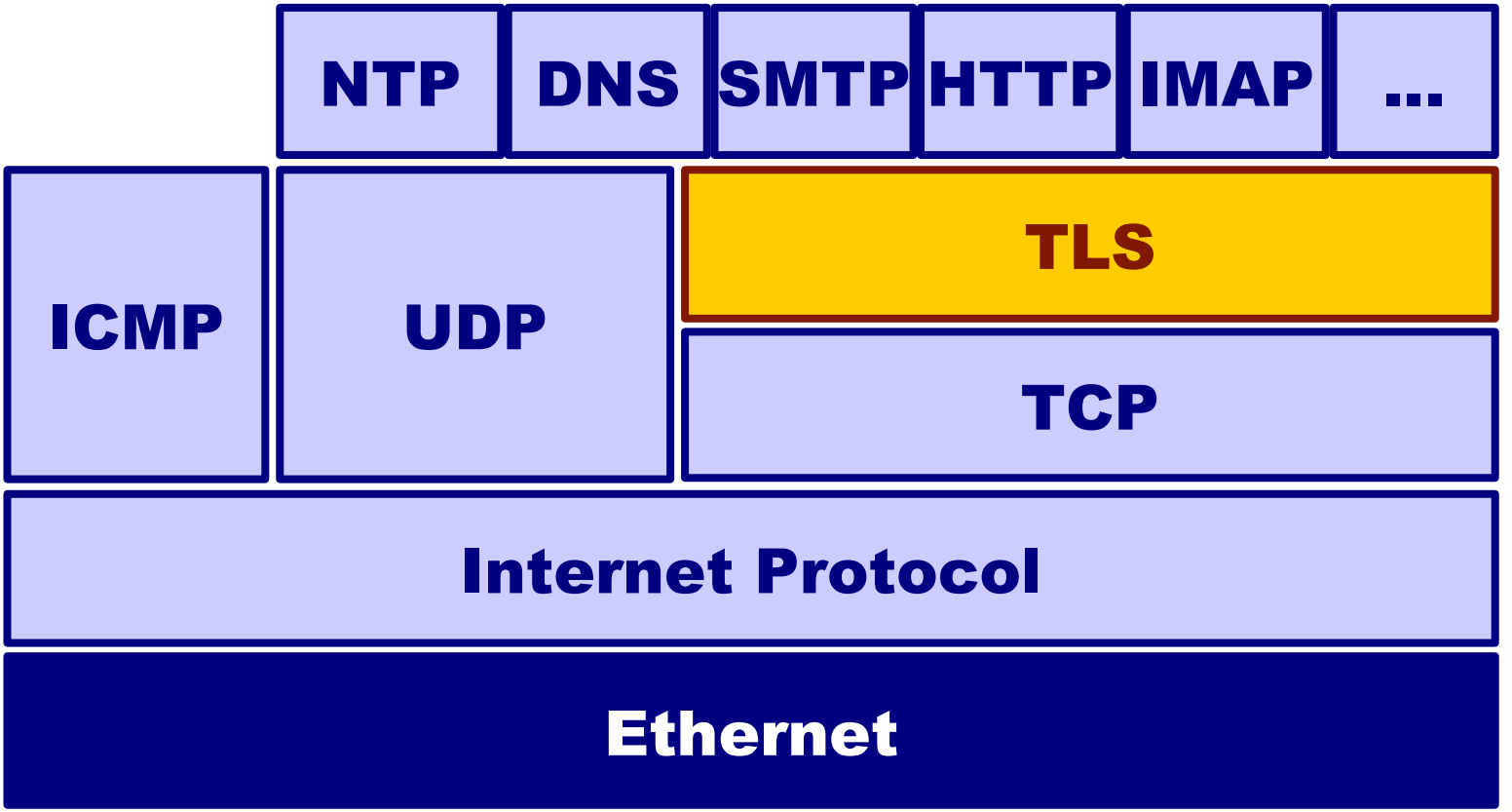
<table>
<tr><th>Host \ FW</th><th>NULL</th><th>AH</th><th>ESP</th><th>AH+ESP</th></tr>
<tr><td>NULL</td><td>NULL</td><td colspan="3">FW-to-FW</td></tr>
<tr><td>AH</td><td rowspan="3">Host-to-Host</td><td>Nur AH</td><td colspan="2">Klartext im LAN</td></tr>
<tr><td>ESP</td><td rowspan="2">*)</td><td>Keine AH</td><td>***)</td></tr>
<tr><td>AH+ESP</td><td>**)</td><td>Maximal</td></tr>
</table>

Gibt es Sicherheit auf Schicht 4?

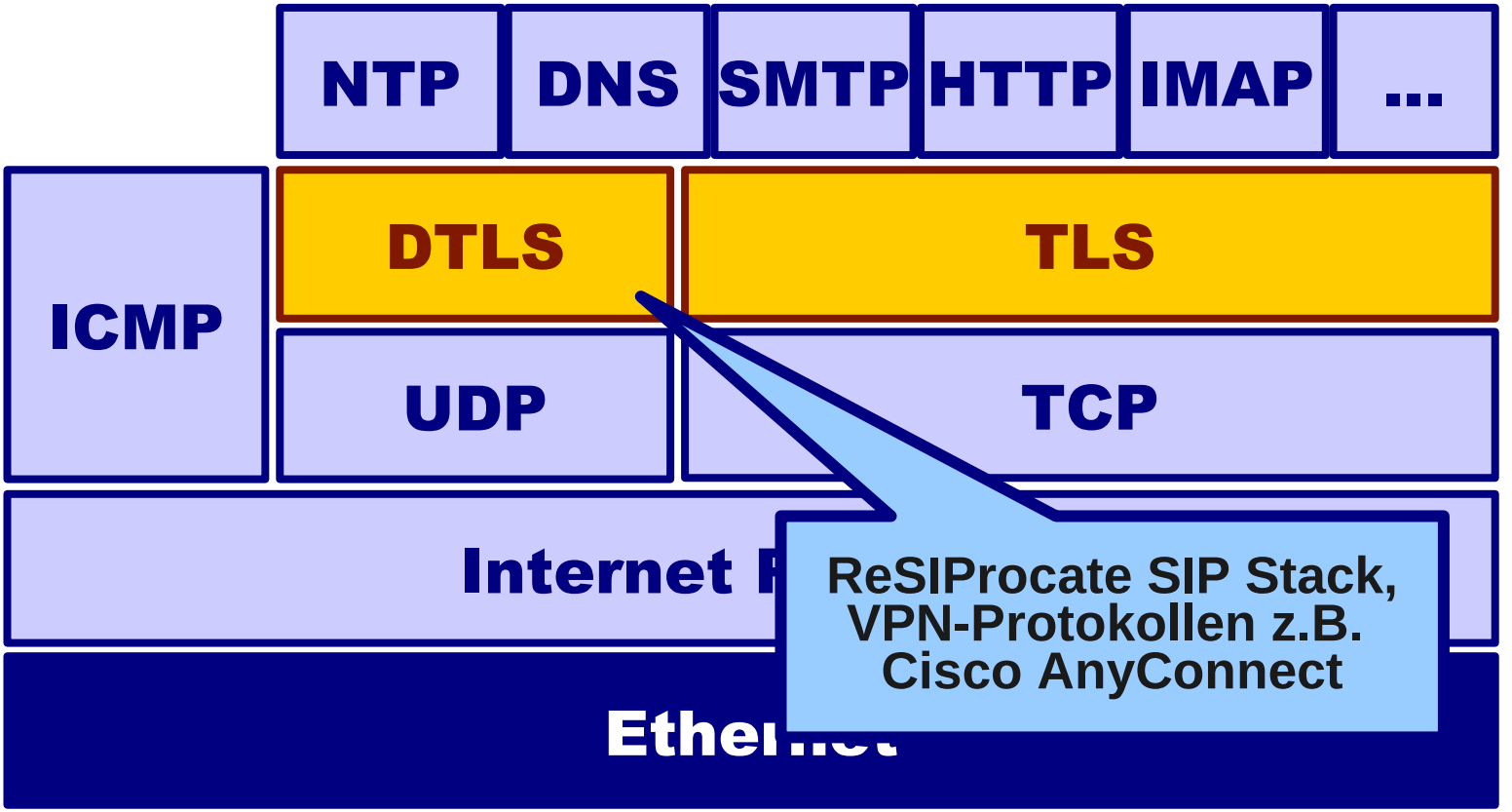
- **Nun ja, die Schicht 4 dient ja dem Transport**
  - Entweder liefert die Netzwerkschicht,
  - Oder die Anwendung muss es leisten
- **Trotzdem gibt es ein Sicherheitsprotokoll, das extra in der Transportschicht „gelandet“ ist, damit die Anwendungen entlastet werden: Transport Layer Security**

https://users.informatik.haw-hamburg.de/~kpk/itsicherheit.html (05 proto)

TLS – Transport Layer Security



DTLS – [RFC4347, April 2006]
Datagram Transport Layer Security



Gibt es Sicherheit auf Schicht 7?

- **Na hoffentlich …**

  Applikationen machen, was sie wollen!
- **Beispiele:**
  - GPG/PGP, S/MIME zum Schutz von Emails
    - Kein Schutz gegen Verkehrsflussanalysen
- **Aber: (TCP-) Applikationen verlassen sich auf TLS als „Silver Bullet“**
  - Eigenschaften der Netzwerksicherheit (vertrauliche Übertragung, Authentizität der Benutzer-/Server-Prozesse) werden nicht an übertragene Objekte gebunden!

Fazit: Vergleich der Schichten

Data Link (Network Interface) layer:

- ✓ Schützt den gesamten Verkehr auf dem Link
- ✓ Unabhängig vom Protokoll darüber
- ✗ Schutz nur bis zum nächsten „Hop“ (Router)

Network (Internet) layer:

- ✓ Schützt den Verkehr zwischen IP-Hosts
- ✓ Gleichzeitig alle Anwendungen & transparent
- ✗ Keine Steuermöglichkeiten durch Anwendung
- ✗ Konzept passt nicht wirklich, da das Protokoll keine Zustände kennt und keine Reihenfolge

Fazit: Vergleich der Schichten (2)

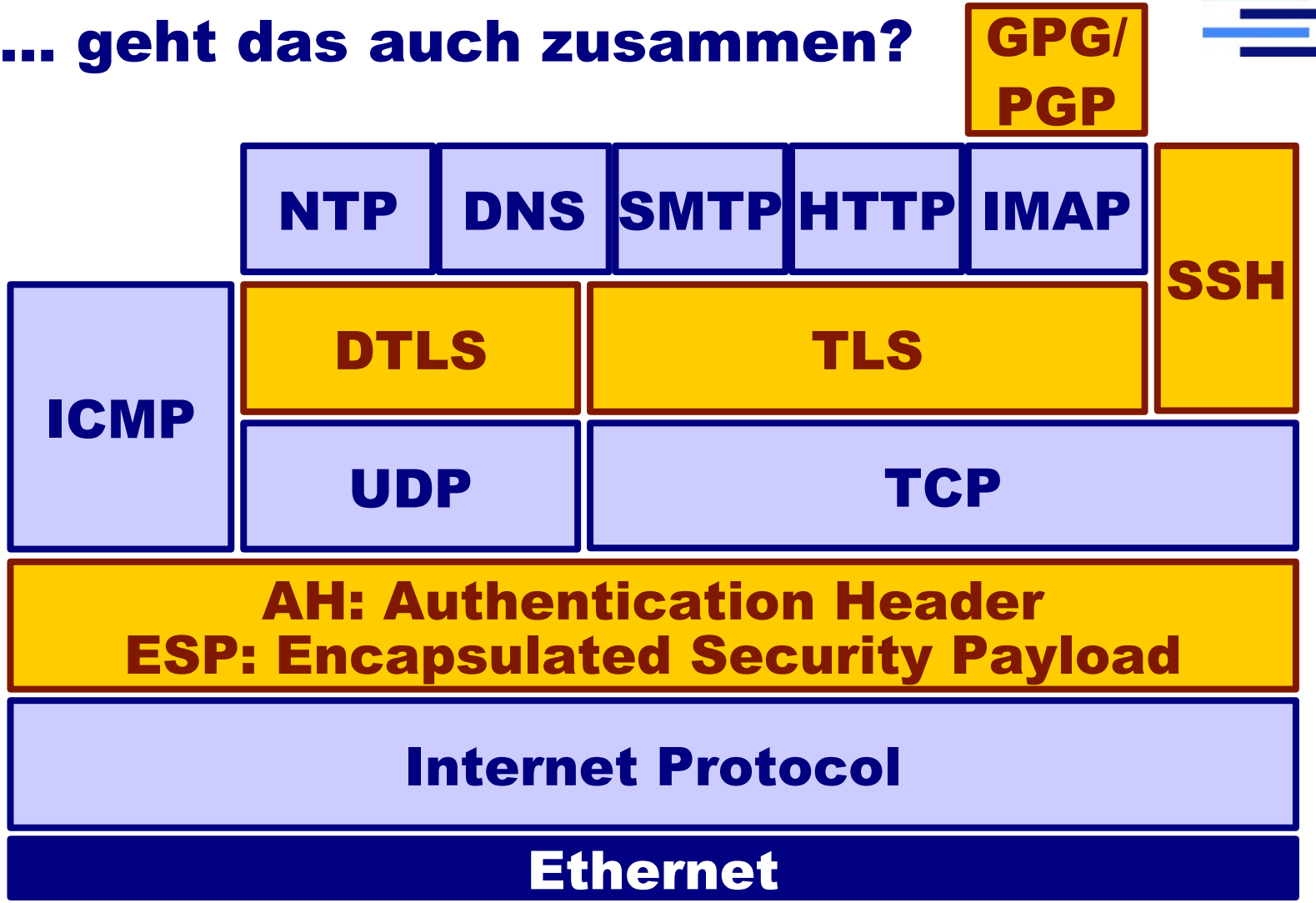
Transport layer:

- ✓ Schützt den Verkehr zwischen Endpunkten
- ✓ Gewisse Kontrolle durch die Anwendungen
- ✓ Transport-Protokolle üblicherweise mit State
- ✗ Anwendungen müssen verändert werden

Application layer:

- ✓ Schutz angepasst an konkrete Nutzdaten
- ✗ Kein Skalierungsbonus – jede Anwendung muss alles selbst machen, und die Anwender müssen das auch noch kennen

... geht das auch zusammen?



... Netzwerksicherheit löst alles?

Ein (fälschlicherweise) Prof. Eugene Spafford zugeschriebenes Zitat:

Using encryption on the Internet
is the equivalent of arranging
an armored car to deliver
credit-card information
from someone living in a cardboard box
to someone living on a park bench.

openVPN … to be continued

Verkehrsflussanalyen und Meta-Data

Observations by a Pizza Delivery Service:

„Pentagon orders doubled up the night before the Panama attack; same thing happened before the Grenada invasion.
Last Wednesday, we got a lot of orders, starting around midnight. We figured something was up..."

**This time the news arrived quickly:
Iraq's surprise invasion of Kuwait.**

And Bomb the Anchovies, Time, p. 13, 8/13/90

Kontakt

Prof. Dr. Klaus-Peter Kossakowski

Email: klaus-peter.kossakowski@haw-hamburg.de

Mobil: +49 171 5767010

https://users.informatik.haw-hamburg.de/~kpk/