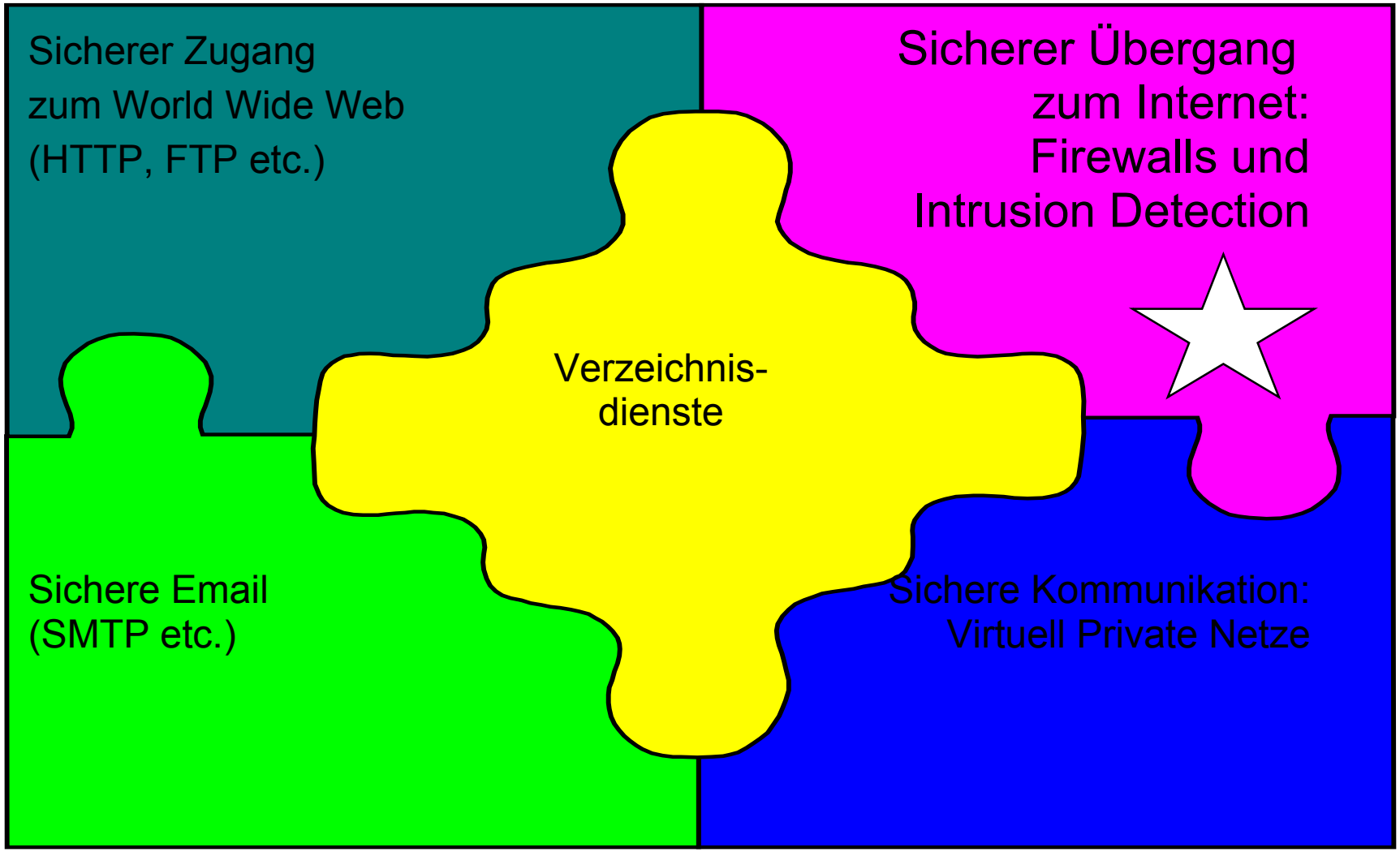
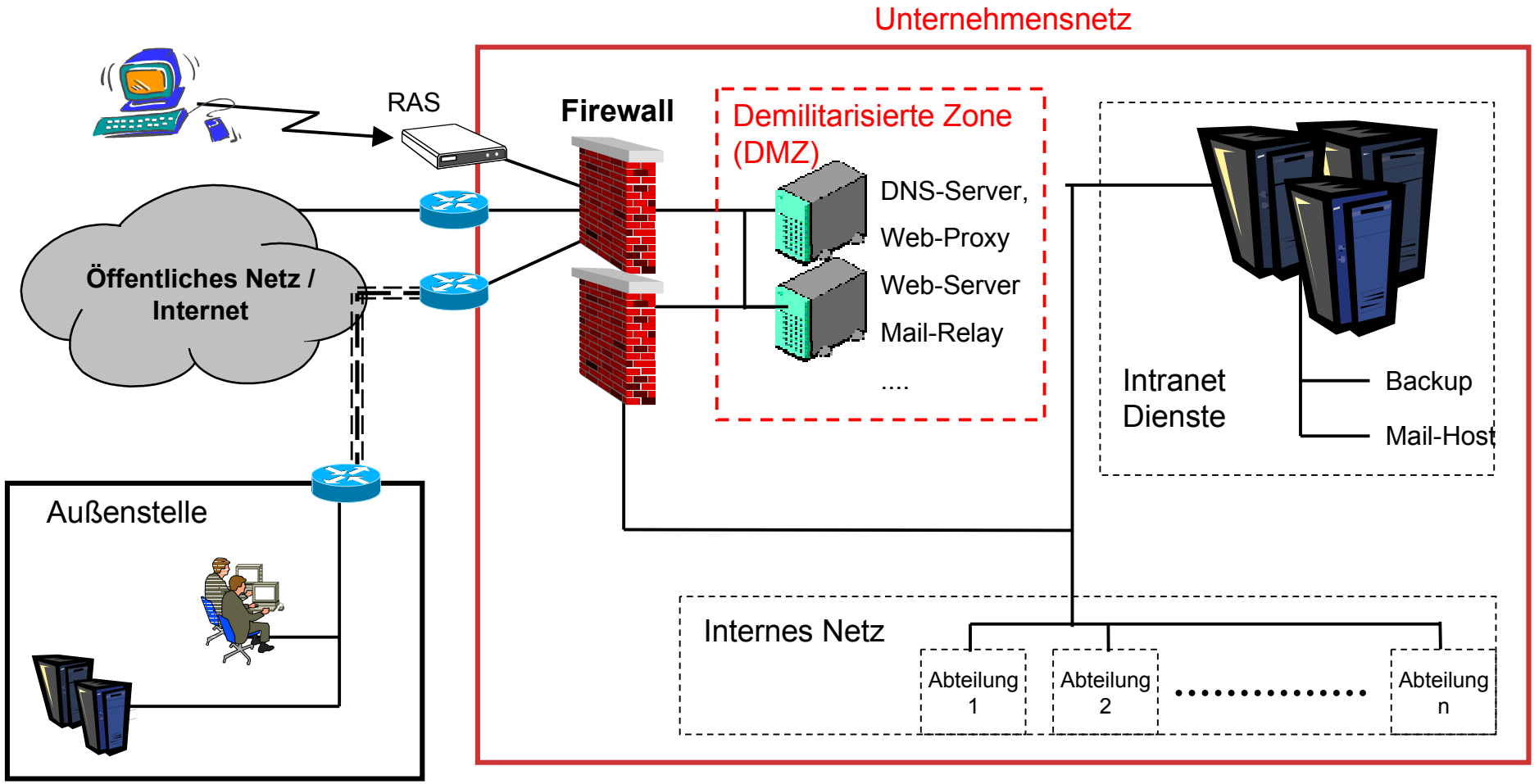
Sicherheitsdienste für große Firmen
=> Teil 2: Firewalls



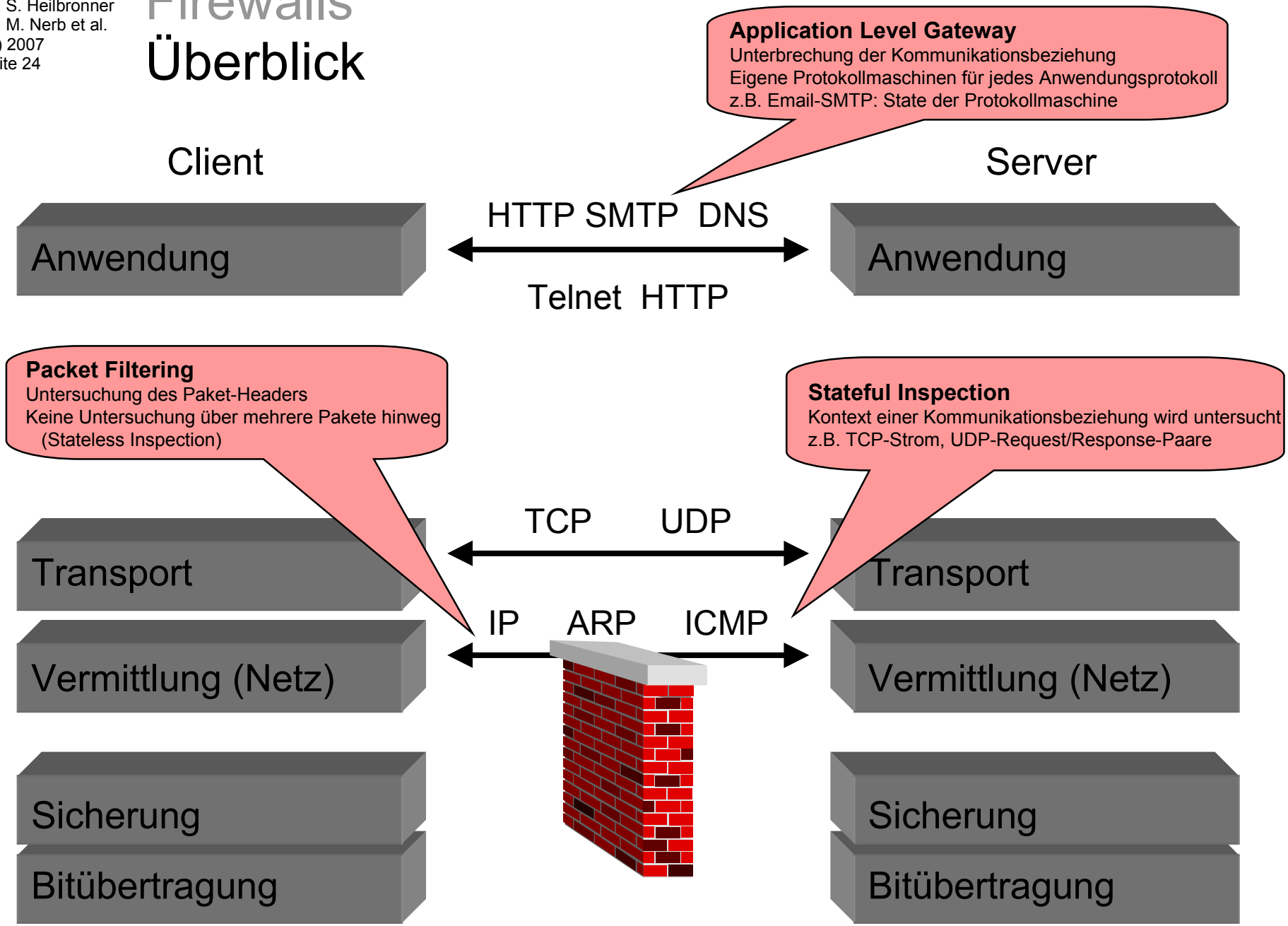
Firewalls
Einsatzzweck

- „*A Firewall helps you to keep **unauthorized** users from accessing your network **resources**. „*
  - Zugriffsrechteverwaltung für Kommunikationsbeziehungen (*Access Control Policy)*
- Grundprinzip:
  - Alles ist (zunächst) prinzipiell gesperrt.
  - Kommunikationsbeziehungen werden einzeln erlaubt.
- => ALLE Bereiche des Netzzugangs werden tangiert!
- Festlegung der Konfiguration in großen IT-Infrastrukturen
  - Iterativer Prozeß in Abstimmung mit vielen Beteiligten
  - Unterliegt ständigem „Change Management“
  - Umgehung durch Tunnelling vermeiden

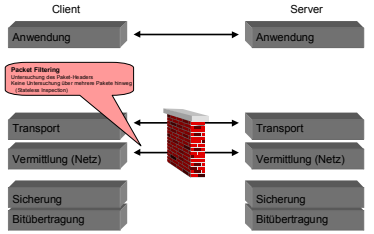
Internet-Übergang
Architektur



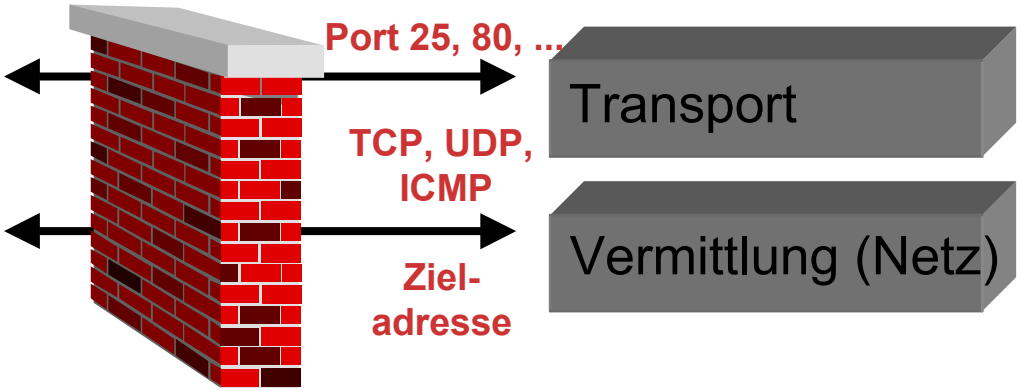
Firewalls
Überblick



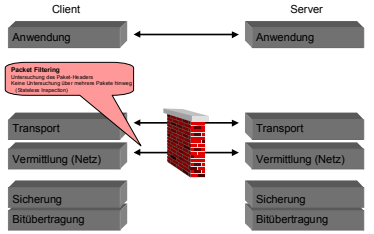
Firewalls
Packet Filtering



- Filterung erfolgt nach Bitmustern im Paket-Header, z.B.
  - IP-Absenderadresse, IP-Zieladresse
  - Protokolltyp: TCP / UDP / ICMP ....
  - Portnummern als Indiz für Dienst, z.B.
    - Port 80/TCP und 44s/TCP für HTTP /HTTPS
    - Port 25/TCP für SMTP (Email)
    - Port 22/TCP für SSH
    - Port 53/UDP für DNS

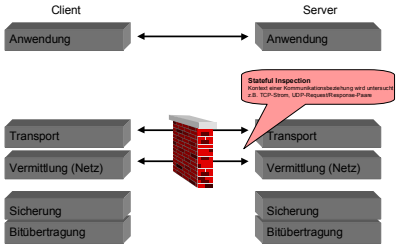


Packet Filtering
Bewertung



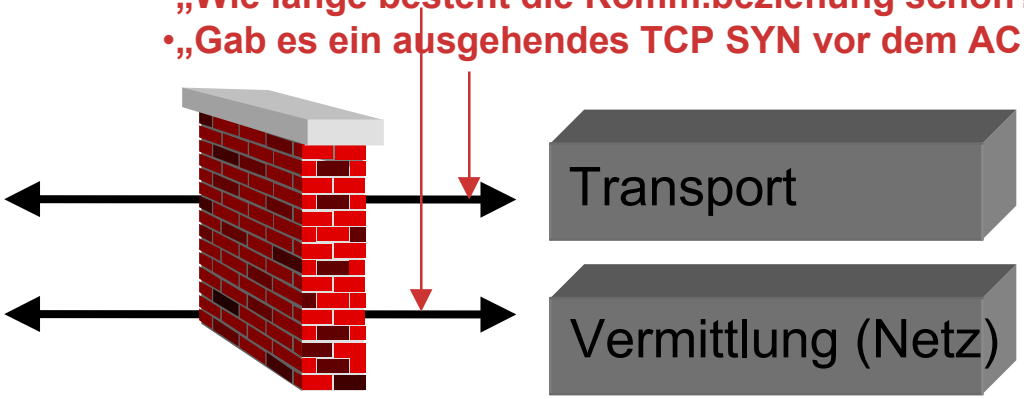
- Vorteile
  - transparent, keine spezielle Anpassung im Netzwerk nötig
  - flexibel, jedes gängige Client/Server-Protokoll wird unterstützt
  - geringe Kosten
  - hoher Durchsatz, in Routern hoch-performant implementierbar
- Nachteile
  - Regelsätze starr und schwer zu verwalten
  - unzureichende Authentifizierung (IP-Adresse nicht verifizierbar)
  - Gefälschte Information in Anwendungsprotokollen (z.B. Mail-Header) können in das interne Netz gelangen.

Stateful Inspection
Überblick

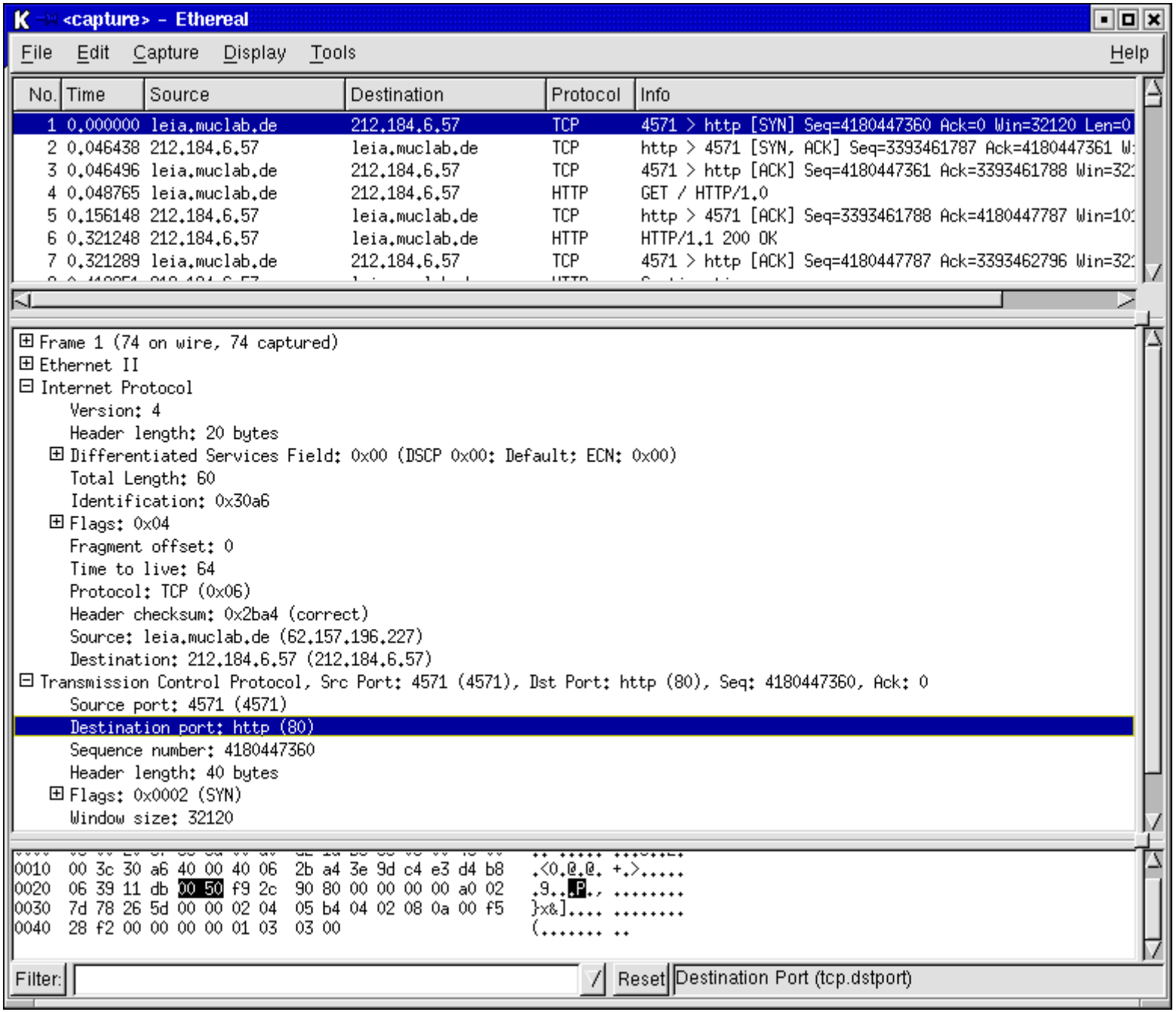


- Auch: „Stateful Inspection, Smart Filtering, Adaptive Screening“
- Zustände der „Verbindungen“ werden analysiert, z.B.
  - Verbindungsauf- und abbau
  - Dauer der Verbindung
- Verwnedung zusätzlich zum Packet Filtering
- Dynamische Reaktion des Filters wird realisiert, z.B.:
  - Datenpakete werden nur für etablierte Verbindung akzeptiert.
  - Ausgehendes UDP-Paket öffnet ein Zeitfenster für nachfolgende Antwortpakete.
- Beste „einfache“ Lösung

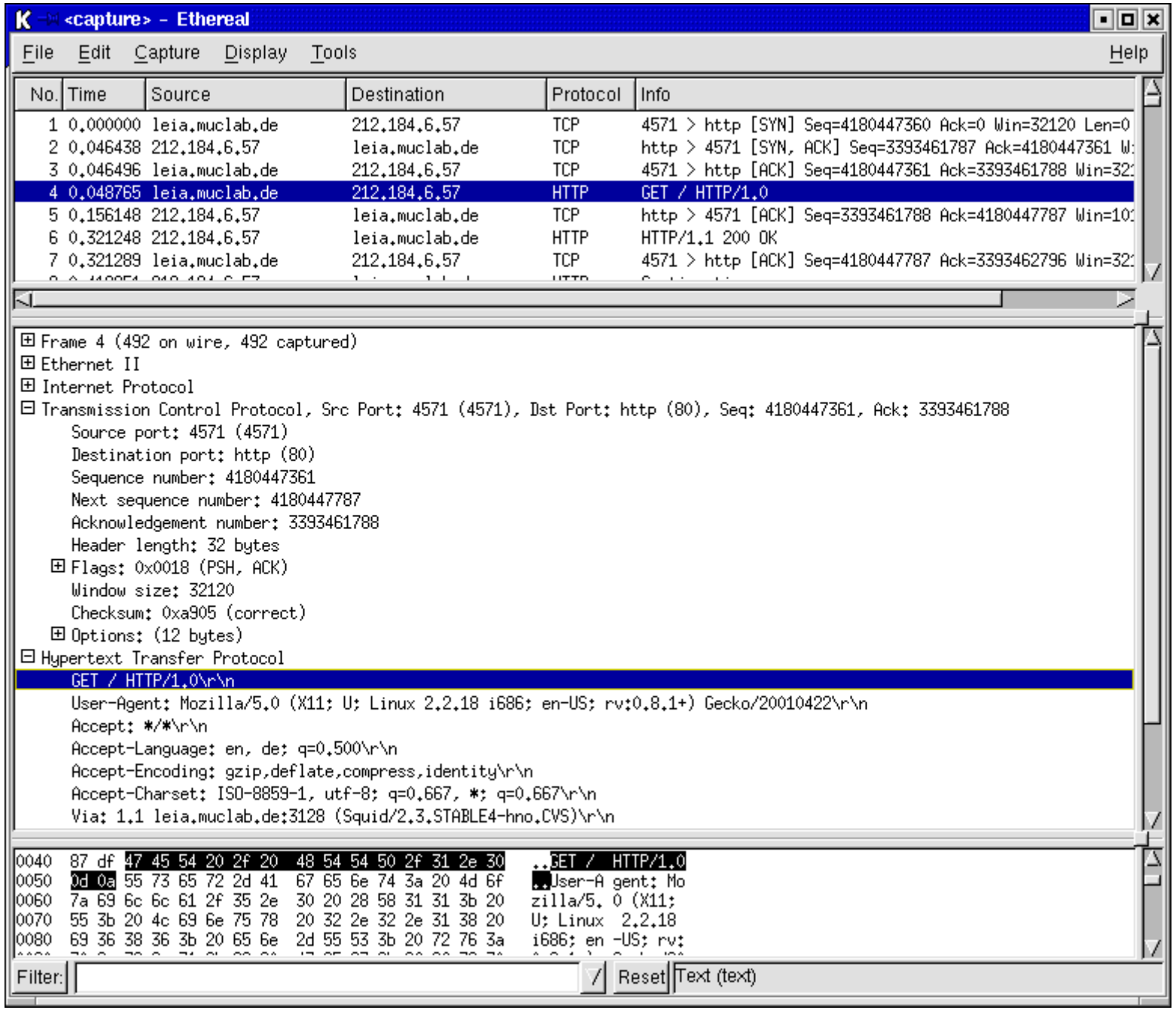
Beispiele:
•„Wie lange besteht die Komm.beziehung schon?“
•„Gab es ein ausgehendes TCP SYN vor dem ACK?“



Aufbau TCP-Verb.

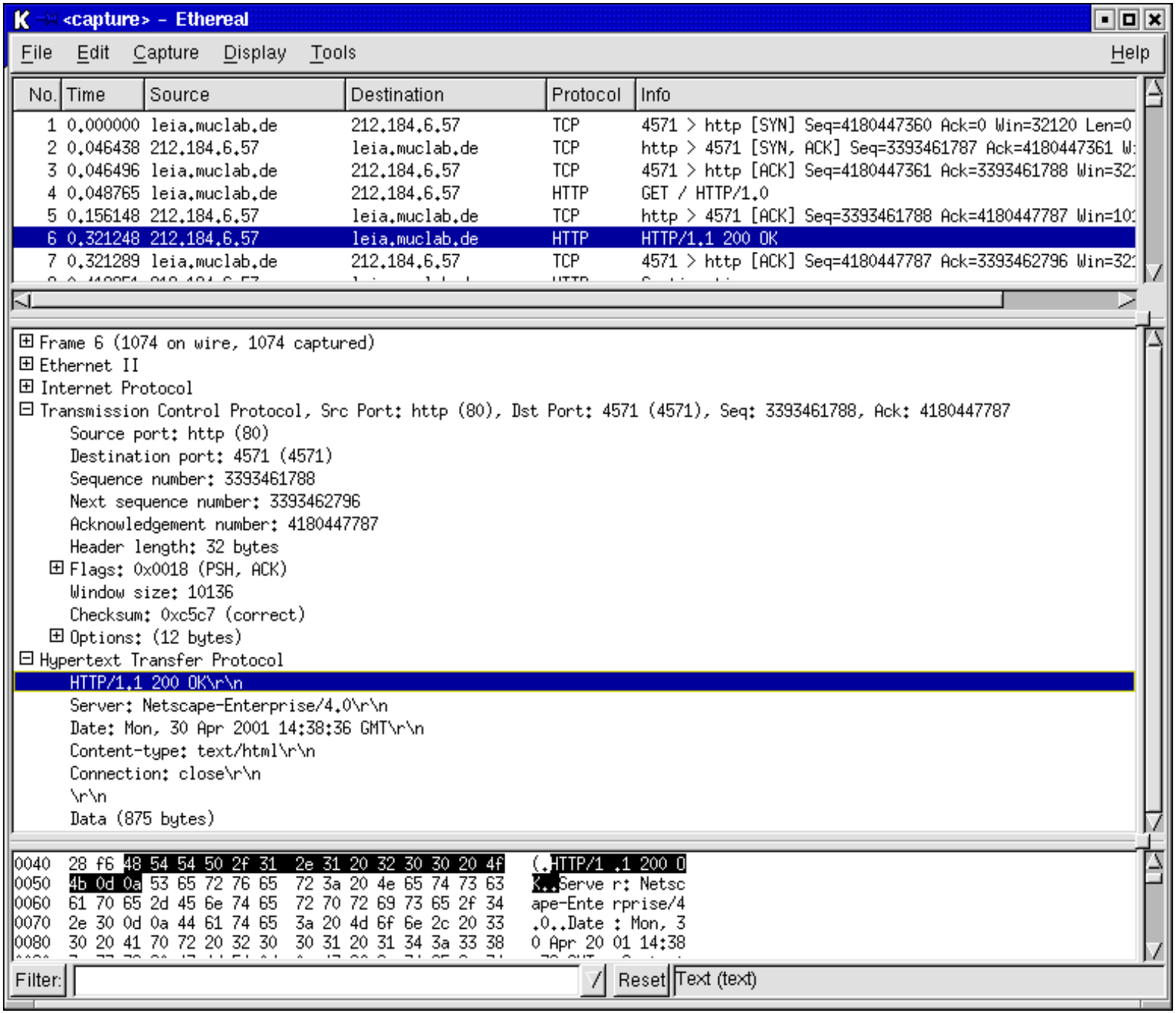


Aufbau TCP-Verb. HTTP-Anfrage

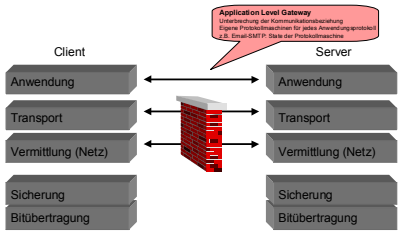


Aufbau TCP-Verb.
HTTP-Anfrage

Antwort



Application Level Gateways
Überblick



- Eigene Protokollinstanz für jedes Anwendungsprotokoll
- Typische Manipulationen und Prüfungen
  - Entscheidung, ob Protokollschritte ausgeführt bzw. Daten übertragen werden.
    - Ist dieser Ablauf (Schritte/Inhalte) inhaltlich zulässig?
    - „Wird Email mit diesem Inhalt von diesem Mail-Relay akzeptiert?“
  - Einhaltung des Protokolls
    - Hat sich die andere Protokollinstanz „korrekt“ verhalten?
  - Port-Umsetzung
  - Anonymisierung des Verkehrs

Vergleich

Paketfilter

- i.a. nur Daten der Vermittlungs-/Transport-Protokolle werden geprüft und gefiltert
- hohe Performanz, da nicht bis Anwendungsebene geprüft wird
- Regeln werden statisch definiert
- niedrigeres Sicherheitsniveau

Application Level Gateway

- Anwendungsdaten und -Protokolle werden geprüft und gefiltert
- geringere Performanz, da aufwendige und tiefgreifende Prüfung und Filterung
- Regelwerk kann dynamisch und flexibel angepasst werden
- hohes Sicherheitsniveau

Rückblick auf Firewalls

- Trennung und Filterung des internen / externen Netzverkehrs
- Vorteile heutiger Firewalls (bzw. deren Implementierung)
  - einfache Regelung des Netzverkehrverkehrs
  - Unterstützung und Prüfung aller wichtigen Protokolle: IP, UDP, TCP, Anwendungsprotokolle
  - Verbergen der internen Netzstruktur (durch „NAT“)
- Nachteile von Firewalls in großen Netzen
  - Regelwerk schnell unübersichtlich
  - häufige Konfigurationsänderungen notwendig
    - Komplexes Change Management
  - bei grossem Netzverkehr potentieller Engpaß