IT-Sicherheit:

Netz-sicherheit

"On the Internet, nobody knows you're a dog."

Cartoon by Peter Steiner. The New Yorker, July 5, 1993 issue (Vol.69 (LXIX) no. 20) page 61

Update:

- (Zum Vergleich die 2010er-Version ☺)
- Für heutige Vorlesung ist Datenschutz (Privacy) von Anwendungs-systemen nicht im Fokus

http://www.geekculture.com/joyoftech/joyarchives/1468.html

Software im Netz

- Server sitzen da und warten auf Verbindungen
  - Meist identifiziert über IP-Adresse und Port-Nummer
- Client stellt Verbindung her, stellt Anfrage

- „Remote exploit“: Anfrage an Server, die unmittelbar zum unkontrollierten Zugriff führt
- „Local exploit“: Angriff wird erst nach Authentisierung und Erlangung eigener Zugriffsrechte (Programmausführung) möglich

Angriffe auf verschiedenen Schichten: Schicht 1

- Ethernet-Repeater, jede Art von Kommunikationsleitung:
  - Abhören (Angriff auf Vertraulichkeit)
  - Verändern, Einschleusen
    - (allerdings meist einfacher auf höheren Schichten)
- Gegenmittel: Quantenkryptographie
  - Beobachtung verändert Phänomen
    - Angriff kann erkannt werden
  - Nützlich vor allem zur Übertragung von Schlüsselmaterial

Angriffe auf verschiedenen Schichten: Schicht 2

- Switches: Verunreinigen der Switch-Datenbank
  - Verkehr wird an alle Ports verteilt
- ARP-Spoofing
  - Abhören (Angriff auf Vertraulichkeit), verfälschen
  - Tools: Dsniff, Ettercap
- Vortäuschen einer fremden MAC-Adresse
  - Umgehung Zugriffsschutz (z.B. WLAN)
  - Tools: ifconfig … ether …

Angriffe auf verschiedenen Schichten: Schicht 3

- Router: Verunreinigen des Routing-Protokolls
  - Verkehr wird umgeleitet
  - Abhören (Angriff auf Vertraulichkeit)
  - Verkehr wandert in schwarzes Loch
- Vortäuschen einer fremden IP-Adresse
  - Umgehung Zugriffsschutz (z.B. bei NFS)
  - Einschleusen von Daten (Session Hijacking)
- Loose-Source-Routing
  - Paket wird nicht an eigentliche Adresse zurückgeschickt, sondern via umgedrehter Source-Route
  - Hebelt TCP-Handshake aus

Finding victims: Scanning

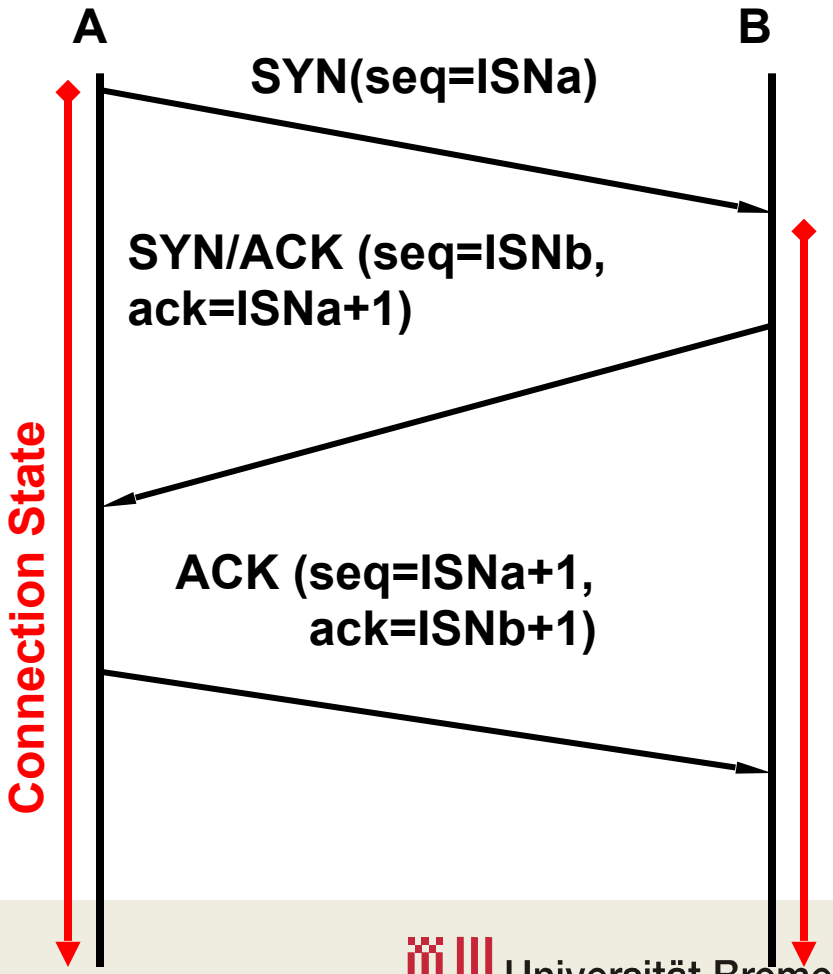
- Reconnaissance: Finding potentially vulnerable Hosts
- IPv4 address space is densely populated
  - Of ~ 4.3E9 IPv4 addresses, ~ 3.7E9 can be used as unicast addresses; of these ~ 3.4E9 are allocated (91 %)
  - Of these, ~ 2.5E9 are routed globally (67 % of the usable, 74 % of the allocated address space)
  - > 0.5E9 of these have a web server (netcraft.com), which is > 20 %!
- IPv6 makes scanning much harder
  - > 1E34 addresses are allocated (0.03 % of the currently usable space)
  - Enumerating these at 1 Gbit/s takes ~ 1E20 years
  - However, there are other ways to collect IPv6 addresses, e.g.
    - DNS analysis
    - Snooping traffic

Angriffe auf verschiedenen Schichten: Schicht 4

- RST-Attacks
  - Abbrechen einer TCP-Verbindung
  - Kann Routing-System (BGP) empfindlich stören (DoS)
- SYN-Flooding
  - Aufbau von Zustand
  - Überlastung stört normale Verbindungen (DoS)
  - Mehr dazu gleich im Exkurs…

RN1 Wiederholung: Three-way handshake

- ISN (Initial Sequence Number): 32 bit
- Sequence Number (seq)
- Auswahl der ISN gesteuert jeweils durch jede Seite
- Echo zurück in Acknow-ledgement Number (ack)



SYN-flood attack

- Objective: clog server
- Bonus: do this without giving hints about identity of attacker
- TCP: protected by three-way-handshake
  - Connection only is completed when peer answers with correct sequence number
  - Cannot easily fake source address
- Idea: just send SYN packet only
  - Easy to fake source address
  - Server needs to establish state (Timeout after several minutes)
- 1 Gbit/s ≈ 3×10^6 packets/s ≈ 0.5×10^9 half-open connections

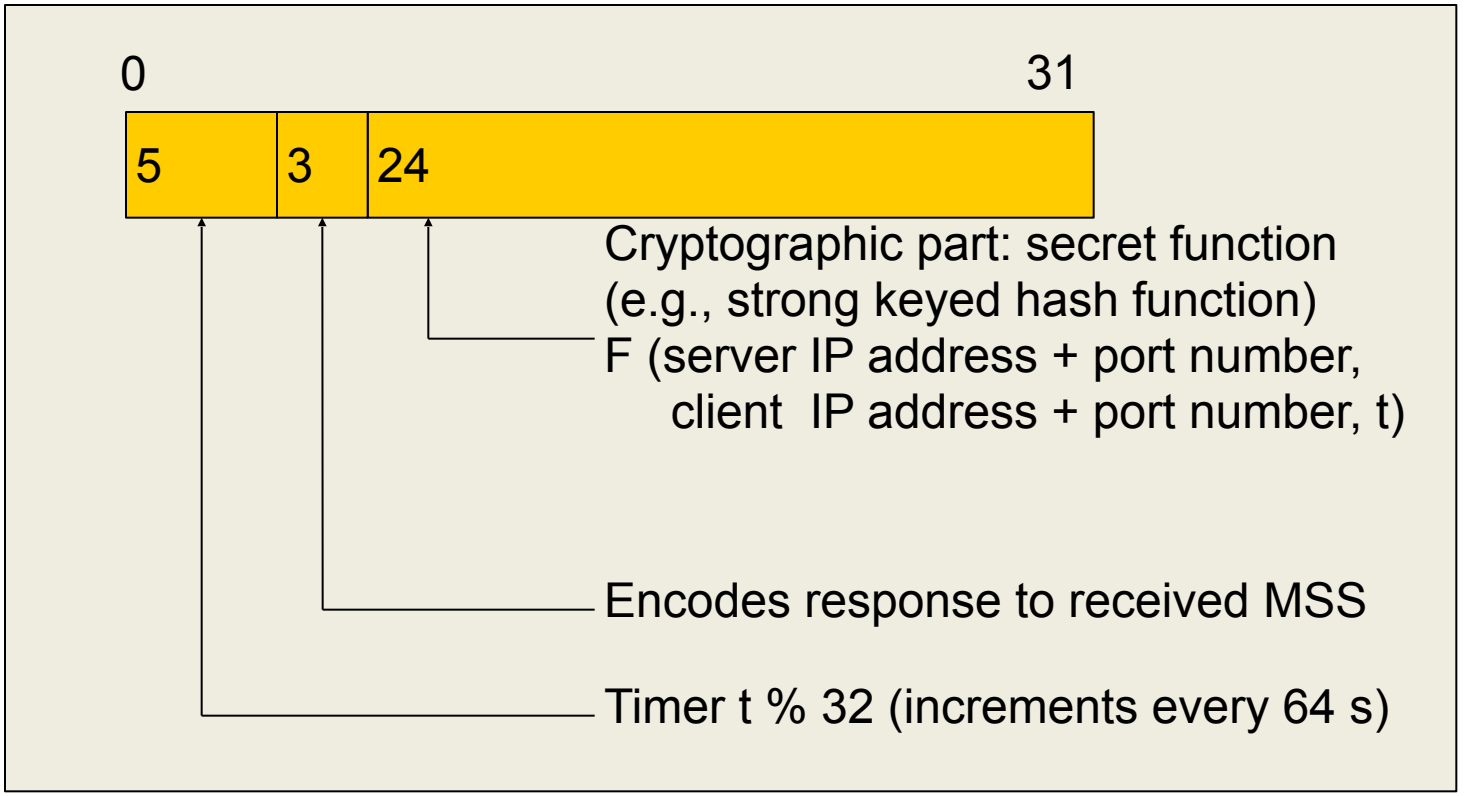
Countering Resource Depletion

- Attackers attempt to bind more resources on the target system than required to mount the attack
  - Make your system perform many and/or expensive computational operations
    - Particularly relevant with security checks (e.g., signature or certificate validation)
  - Make your system create state information
  - (Make your system transmit data, preferably to somebody else)
- Issue: distinguishing legitimate work from attack
  - There is not necessarily a well-defined user behavior
  - Example HTTP: Botnet fetching pages, search crawlers, site replication (wget)
    - Some web sites inspect the HTTP `User-Agent:` header and deny access to bots
- General Approach
  - Avoid creating (much) state early on the server side
  - Make the client work harder (client-side easier to scale anyway)

Example: TCP SYN Cookies (1)

- Normal TCP operation when a SYN packet comes in
  - Create protocol control block (PCB), choose random initial sequence number, set cleanup timeout (in case you never get an ACK), send SYN-ACK back
  - State will last until timeout expires
- TCP SYN Cookie idea (D. J. Bernstein, 1996)
  - Do not create state
  - Encode the local state you would create in 32-bit sequence number
    - Part of this is protected cryptographically
  - Send SYN-ACK
  - If ACK comes back: recreate state from acknowledgement number
  - If no ACK comes back: nothing lost except for a few CPU cycles
  - Equalizes the burden
    - Attacker needs to respond and thus bind local resources
    - Attacker can no longer use random source addresses

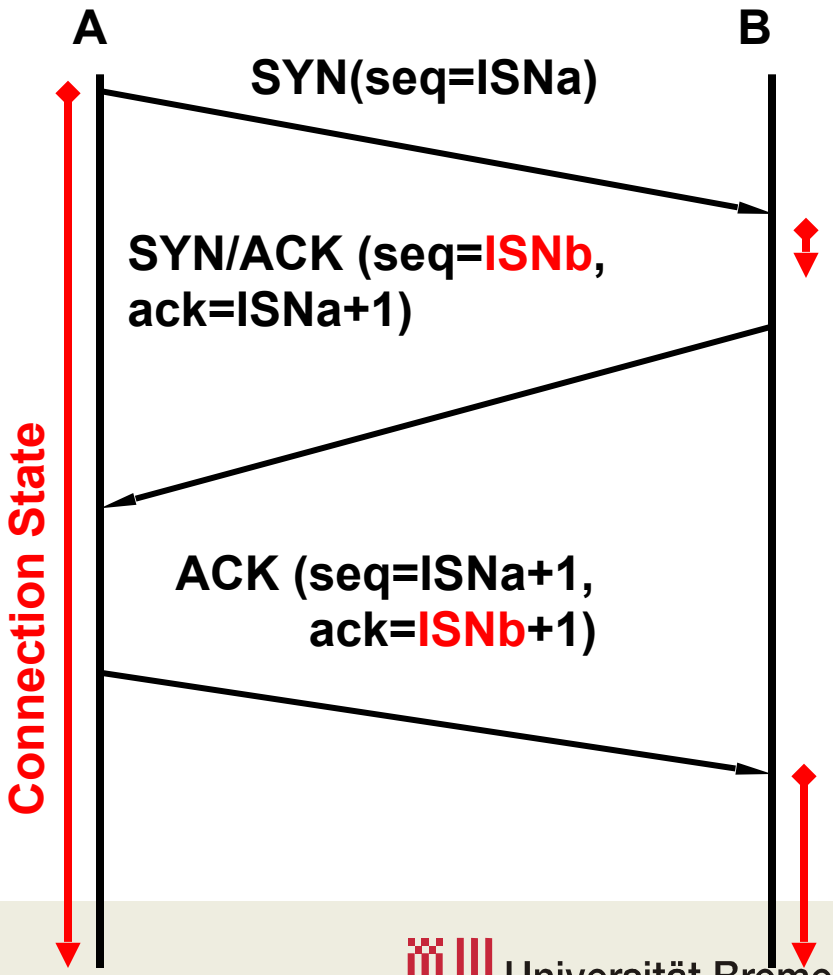
Example: TCP SYN Cookies (2)



- Issues: limits TCP option negotiation capabilities
  - E.g., large windows, SACK

SYN Cookies

- Nur B kann aus den Parametern ISNb ausrechnen
- Erst ACK legt Zustand an
- Weist Empfang der „geheimen“ ISNb nach
- Adresse von A authentisiert (return routability)



Angriffe auf verschiedenen Schichten: Schicht 7

- DNS-Spoofing
  - Verunreinigen der Caches von DNS-Servern
- Email-Spoofing
- Web-Spoofing, Phishing
- Angriffe auf Programme: Buffer Overflows etc.

Gemeinsamkeiten

- On-Path-Angreifer kann abhören
  - Durch gezielte Angriffe kann man “on-path” gelangen
  - Abhilfe: Verschlüsselung (Kryptographie)
- Identitätsbehauptungen können gefälscht werden
  - Abhilfe: Authentisierung
  - Muss resistent gegen Abhören sein
    - Kryptographische Authentisierung

The Internet threat model

(Dolev-Yao threat model, 1983)

- Assumption: The end-systems are not compromised
  - There are ways to minimize damage even in this case, e.g., perfect forward secrecy
  - Can validate the assumption with *attestation*
- However, the communications channel is completely compromised, i.e., attacker can:
- Read any PDU
- Undetectably remove, modify, inject any PDU
  - Including PDUs that appear to be from a “trusted” machine

Types of attacks

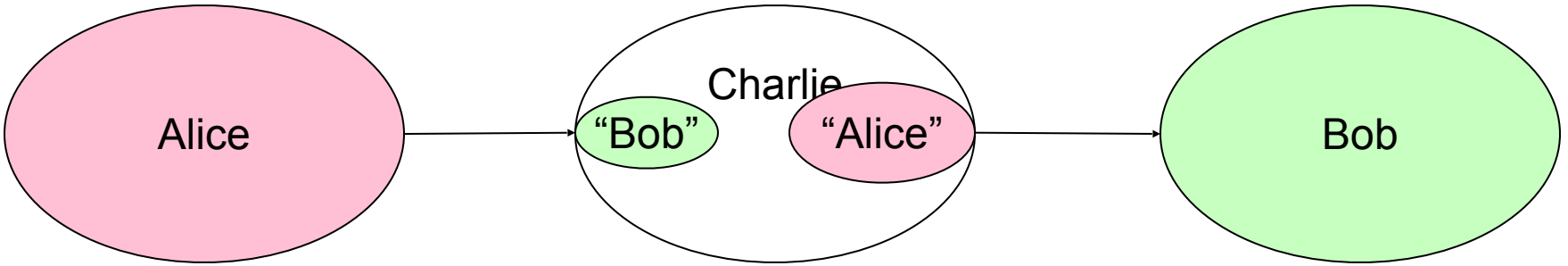
- Passive attacks:
  - Attacker only reads packets (“sniffing”)
  - Extremely easy on wireless
  - Relatively easy on shared media such as Ethernet
  - Can only really be excluded by quantum cryptography
- Active attacks:
  - Attacker also injects new packets into the network
  - Source address can be spoofed
    - Egress/ingress filtering can make this harder
  - Blind attacks: can only write, not read
  - Replay attacks: inject copy of previous good packet (“launch rocket now”)

Combinations

- Passive followed by active attack:
  - Password sniffing (passive) + login using sniffed password (active)
  - Can be supported by an offline attack, e.g. dictionary attack
    - If sniffed information can be used offline to determine whether guessed password is correct
- Active attack to facilitate passive attack:
  - Subvert forwarding/routing system to divert traffic via attacker
  - Quite easy at layer 2 (tools: dsniff, ettercap)
  - Subverting routing at layer 3 may be harder
  - Compromised router/switch can be used as tool

Man-in-the-middle-Angriff = MITM = Janus-Angriff

- Der Man-in-the-middle-Angreifer täuscht jedem Kommunikationspartner vor, der andere zu sein:
  - Nachrichten können auf dem Weg beliebig abgehört oder verfälscht werden



- Abhilfe: Kryptographie (Authentisierung/Verschlüsselung)

•https://en.wikipedia.org/wiki/Janus#/media/File:Janus1.JPG

On-path vs. off-path attacks

- On-path attacker can easily eavesdrop, spoof, suppress, inject
- Off-path attacker typically is limited to blind attacks
  - Unless topology can be subverted to convert off-path into on-path situation
- Many protocols protect well against off-path attackers, not so well against on-path
  - E.g., TCP random sequence numbers are worthless if overheard by on-path attackers
- (Note that real Internet paths are often asymmetric.)

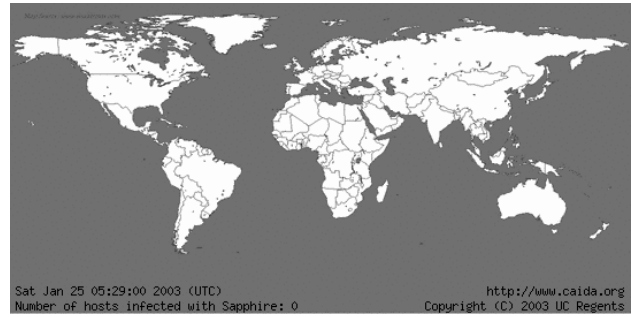
DoS-Angriffe

- Außer Gefecht setzen (Absturz, fehlerhafter Zustand)
- Überwältigen (viel Verkehr)
  - Erleichtert durch Zombies/Botnets (DDoS)

- Amplifier-Angriffe: z.B. Smurf
  - Paket mit gefälschter Absenderadresse (Opfer) an „directed broadcast“
  - Alle Zielsysteme schicken ICMP-Antwort „nicht erreichbar“ an Opfer
  - Directed broadcast aus Routern heute praktisch verschwunden
  - Nebeneffekt: ICMP gilt bei vielen Admins als bösartig (vgl. auch „ping of death“)
    - Probleme mit Path MTU discovery

SQL-Slammer/Sapphire

- 25. Januar 2003: Korea praktisch offline
- UDP-Paket mit 376 Bytes Nutzlast
  - Wird mit maximaler Geschwindigkeit an zufällig generierte IP-Adressen versendet
- Warhol-Wurm: infizierte die meisten der ≥ 75 000 Opfer innerhalb von 10 Minuten
  - Verdopplung alle 8.5 Sekunden
  - Trotz Bug in PRNG
- Basis: Verwundbarkeit in MSSQL-Server
  - seit 24.07.2002 bekannt
- Abhilfe: Port 1434 (MSSQL) schließen



Internet Background Radiation

- Würmer wie SQL-Slammer sind immer aktiv
- „Hintergrundstrahlung“: Ca. 0,15–2 Bytes/s/IP-Adresse
- Ungepatchtes Windows-System ans Internet anschließen?
  - Infektionen innerhalb von Minuten (Sekunden?)
  - Kompletter Absturz nach ca. 30 Minuten
- + Absichtliche Angriffe
- Unternehmensnetze brauchen nicht unbedingt volle Internet-Konnektivität
  - ☛ Firewalls

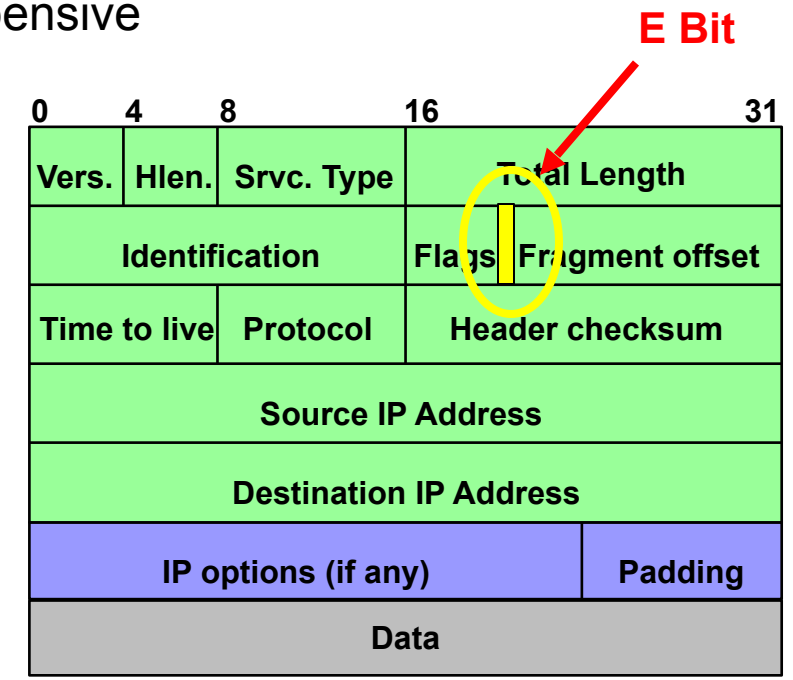
Geschützte Werkstätten (Unternehmensnetze und Firewalls)

“The primary purpose of **firewalls** has always been to **shield buggy code** from **bad guys**.”

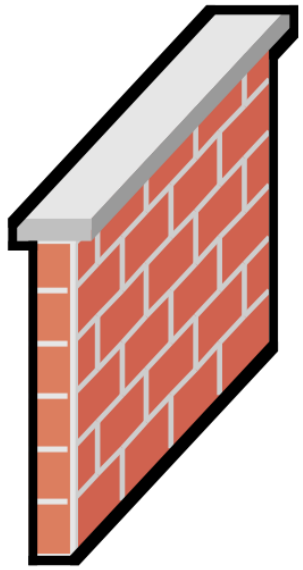
Steve Bellovin, IETF Security AD

Classifying Traffic: The E(vil)-Bit

- Key question: how to identify malicious or other unwanted traffic
- Potentially intense processing required per packet
  - Source + destination IP addresses and port numbers, protocol type
  - Stateful packet inspection even more expensive
- Solution: RFC 3514 (1 April 2003)
  - "The Security Bit in the IPv4 Header"
  - Straightforward traffic identification
  - Fail-safe, easy to implement
  - E == 1: packet has evil content
  - E == 0: packet is ok
  - Firewalls simply discard evil packets
  - Extension for IPv6: "evil strength"

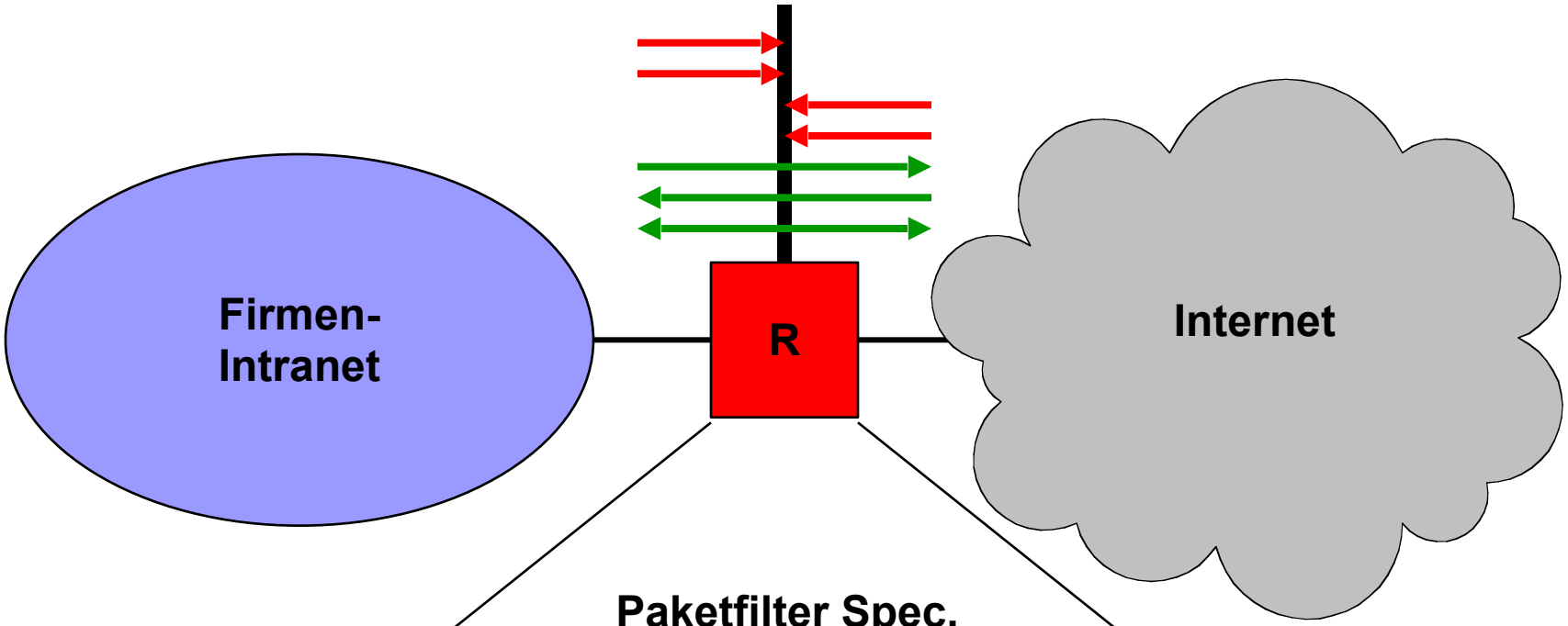


Firewall



- Perimeterschutz: “Crunchy outside, mushy inside”
- Unternehmensnetze und Internet werden nicht direkt verbunden, sondern über **Firewall**
- Nur „erwünschte Kommunikation“ wird durchgelassen
  - Problem: wie identifiziert man diese?
- Interne Systeme werden vor Angriffen von außen geschützt
  - Sinnvoll: auch umgekehrt
- Gefahr: trügerische Sicherheit
  - Schützt nicht gegen Insider!

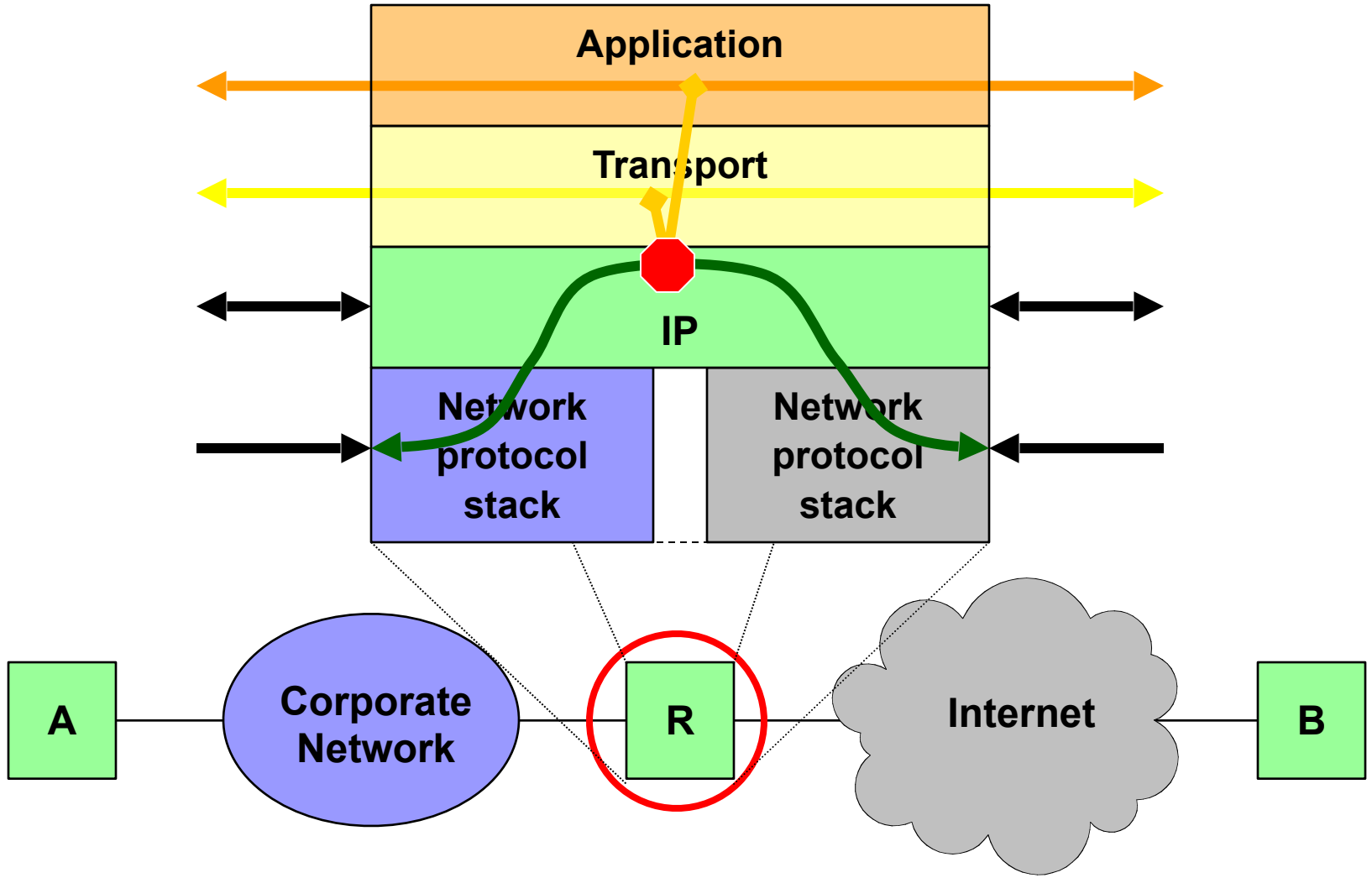
Paketfilter



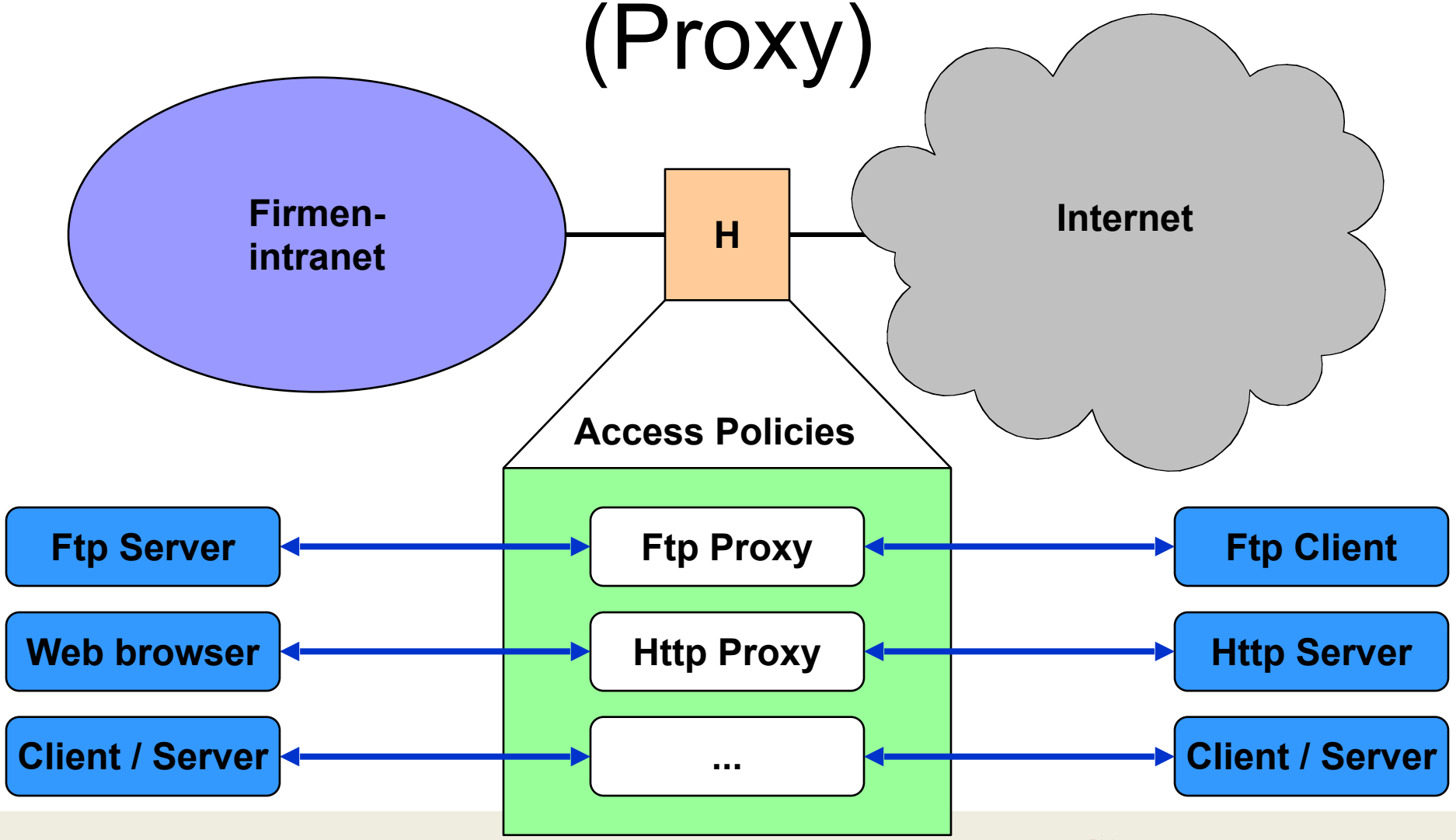
Kriterien für Paketfilter

- Keine „merkwürdigen“ Pakete, Protokollverletzungen
  - Keine IP-Optionen wie *loose source routing*
  - Evtl. auch Fragmente ausschließen (oder reassemblieren!)
  - Keine Martians/Bogons/Pakete von außen mit innerer IP-Src
- 5-Tupel (IP-Src, IP-Dst, IP-Protokoll, Src-Port, Dst-Port)
  - access-list 115 deny udp any any eq 1434 (SQL-Slammer)
  - Besser: explizit nur gewünschte Kommunikation zulassen
  - Problem: IPsec verdeckt Port-Nummern (nur noch IP-Src/IP-Dst)
- TCP: Aufbauversuche (SYN ohne ACK) evtl. nur in eine Richtung zulassen
  - access-list 120 permit tcp any any established

Stateful Packet Inspection



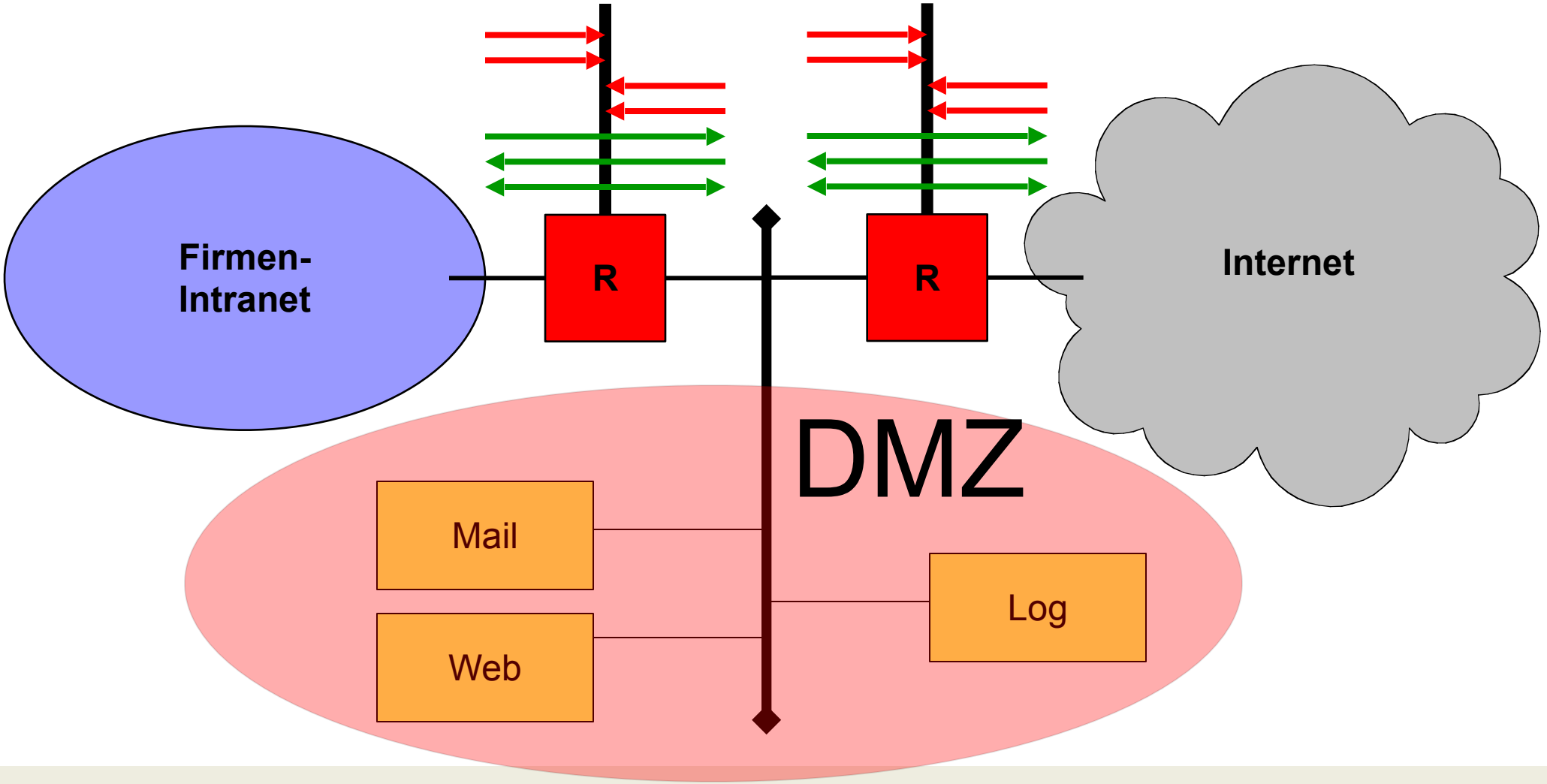
Application Layer Gateway (Proxy)



Aufgaben eines ALG

- Kann „tief“ in Anwendungsflüsse hineinsehen
- Protokollverletzungen nicht durchlassen
- Anwendungsregeln realisieren
  - Kein Zugriff auf bestimmte Websites
  - Kein „unerwünschter Inhalt“ (Viren/Trojanische Pferde)
  - Bekannte Angriffe abwehren (Buffer overflows etc.)
- Anwendungsprotokolle terminieren
  - Z.B. Mail von außen entgegennehmen, dann intern ausliefern (und umgekehrt)
- SPF (stateful packet filter): ALG für Arme

Klassische Firewall-Anordnung

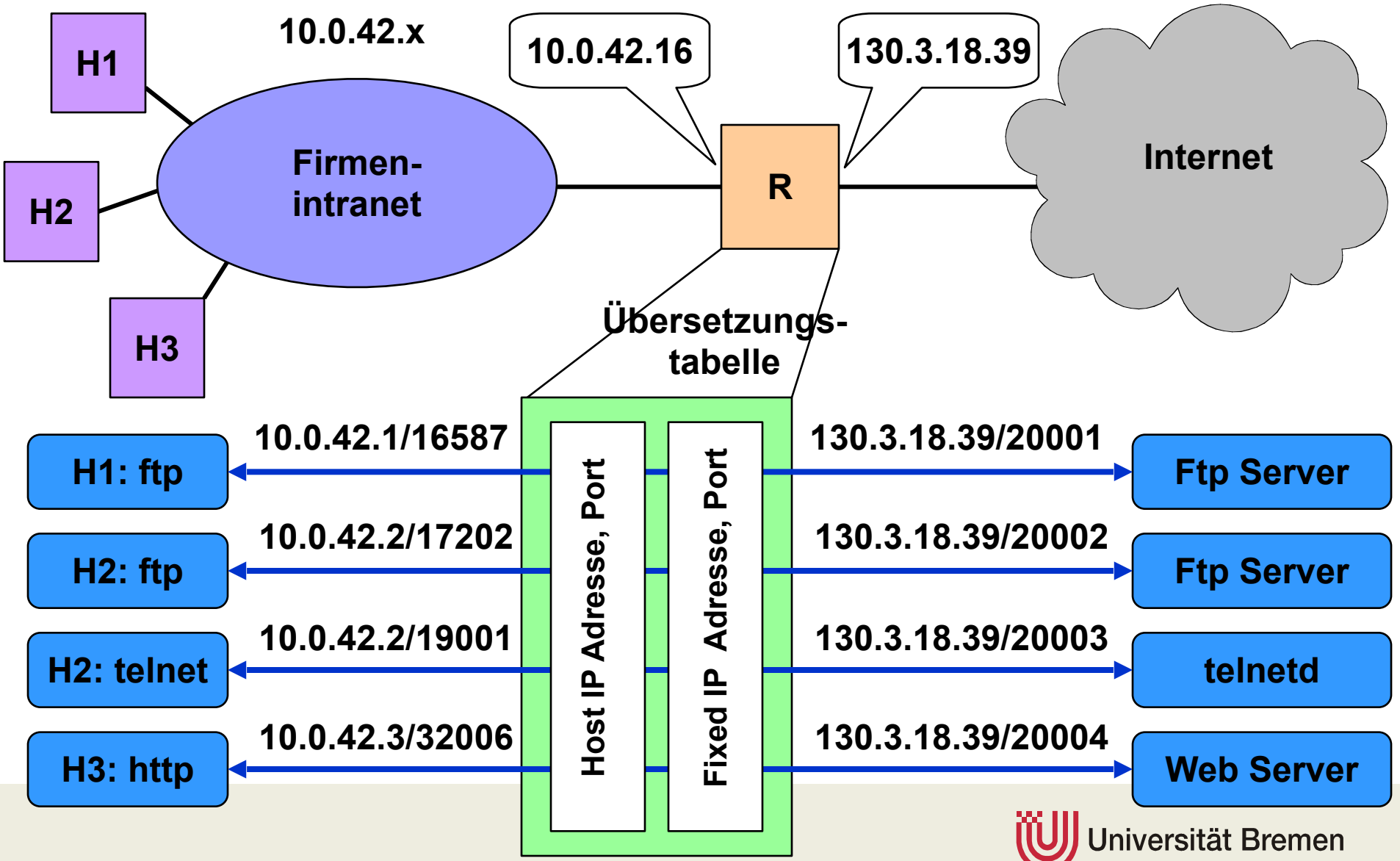


DMZ (Grenznetz)

- Von außen sichtbare Dienste
- Proxies/ALGs
  - “Bastion Hosts”

- Paket-Filter nach außen schützt DMZ
- Paket-Filter nach innen schützt internes Netz
  - Kombination lässt kein Paket durch

Network Address Translator (NAT)



NAT: kein Firewall

- NAT löst Adressraumprobleme
- Nebeneffekt: verhindert kommende Verbindungen
  - Krude Firewall-Funktionalität
  - Kommerzielle Firewalls meist um Paketfilter erweitert (5-Tupel)
- Keine weiteren Analyse-/Logging-Funktionen
- IPv6 (hat keine NATs):
  RFC 6092 schlägt äquivalente Funktion vor
  (“Recommended **Simple Security** Capabilities
  in Customer Premises Equipment (CPE)
  for Providing Residential IPv6 Internet Service”)

Logging

- Was ist passiert?
- Logfile: Meldungen mitschreiben
  - Ereignisse rekonstruieren
  - Eindringlinge erkennen
- Logfile vor Angreifern schützen!

Der Einfluss von Firewalls auf das Internet

- Neue Dienste lassen sich nur nach Firewall-Upgrade ausrollen
- Hindernisse
  - Neue Software-Versionen erforderlich
  - Schulung der Admins; Fortschreiben der Betriebsregeln, …
- Ergebnis: Viele Protokolle heute benutzen HTTP, „um durch die Firewalls zu kommen“
  - „Web-Services“
  - SSH over HTTP, IP over HTTP!
- Firewalls müssten nun eine Stufe höher einsetzen

“firewall friendly”

- Neue Protokolle müssen „Firewall-freundlich“ sein
- Oberflächlich: Alles über HTTP
- Wirklich: Flüsse müssen selbstbeschreibend sein
  - Politiken müssen allein auf den Flüssen realisiert werden können
  - Trennung Steuerung/Datenflüsse erschwert (vgl. SIP)
- Fallback: Middlebox-Steuerung
  - Z.B. via UPnP, besser: PCP (war: NAT-PMP)
- Fallback: HTTP-Proxy authentication, SOCKS
  - Authentisierter Zugriff auf Proxy