Computersystemsicherheit

Prof. Marc Fischlin, Wintersemester 18/19

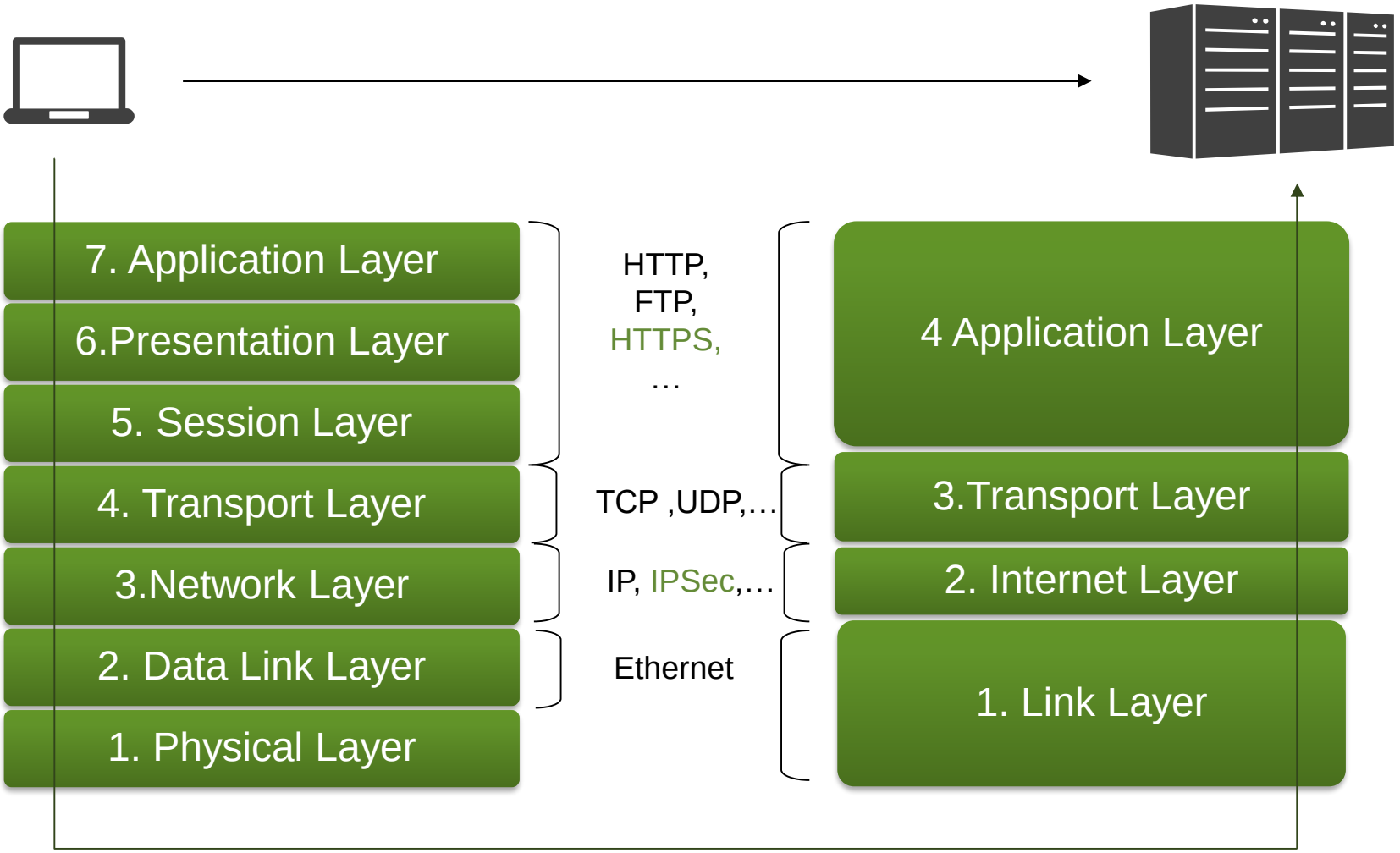
→ „Netzwerk-Sicherheit“

05

Netzwerksicherheit

Netzwerke - Grundlagen

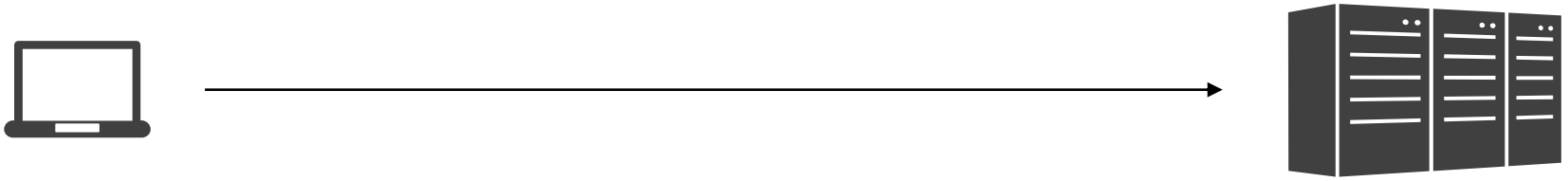
Netzwerk-Schichtenmodelle



Open Systems Interconnection (OSI) Modell

TCP/IP Modell

Kennzeichnungen

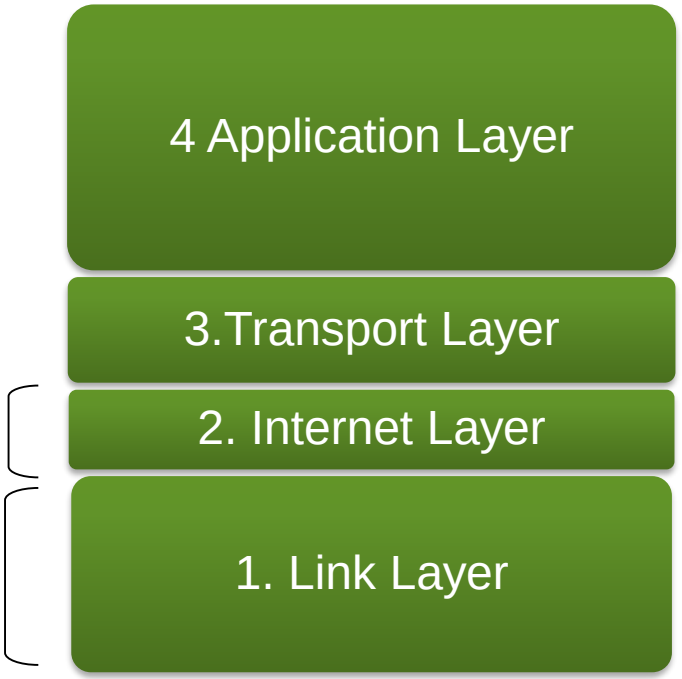


Internetnummer
(IPv4: 32 Bits, IPv6: 128 Bits)

IP Adresse : **`130.83.22.1`**

MAC Adresse : **`00:15:fe:23:d4:ce`**

Media Access Control;
eindeutige Hardware-Gerätenummer



Bereiche: **`130.83.22.0/24`** entspricht
`130.83.22.0 – 130.83.22.255`

MAC-Spoofing

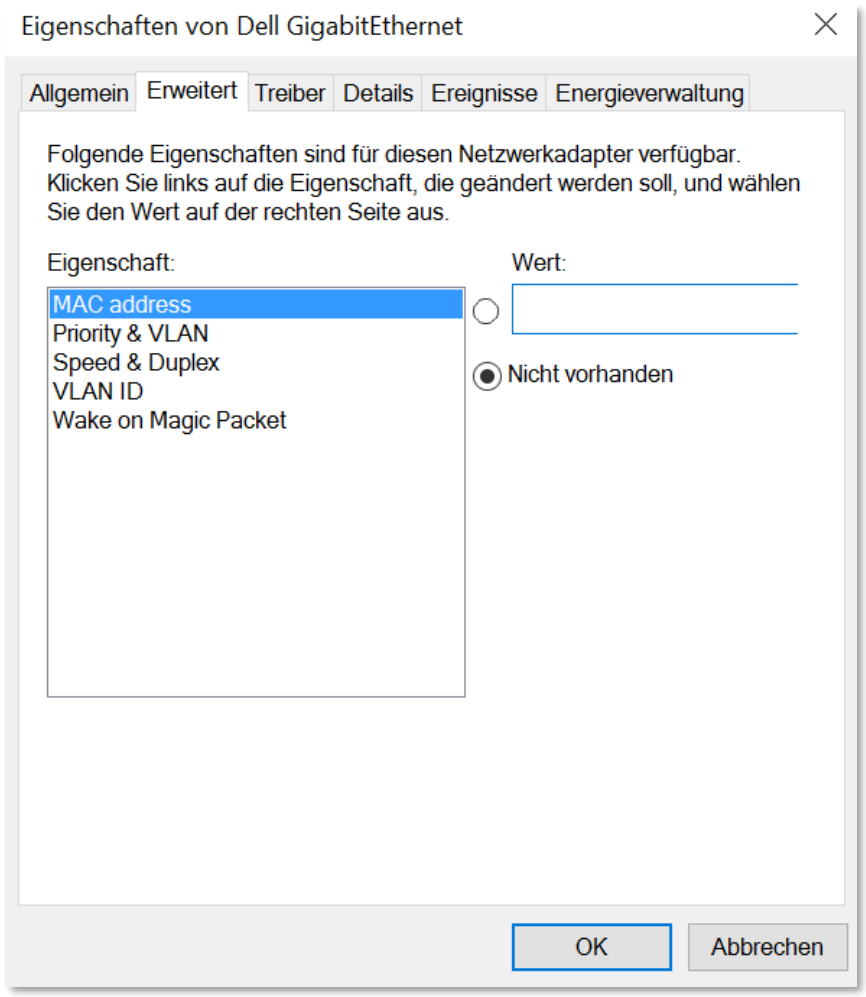
MAC-Adressen sind leicht zu ändern

–

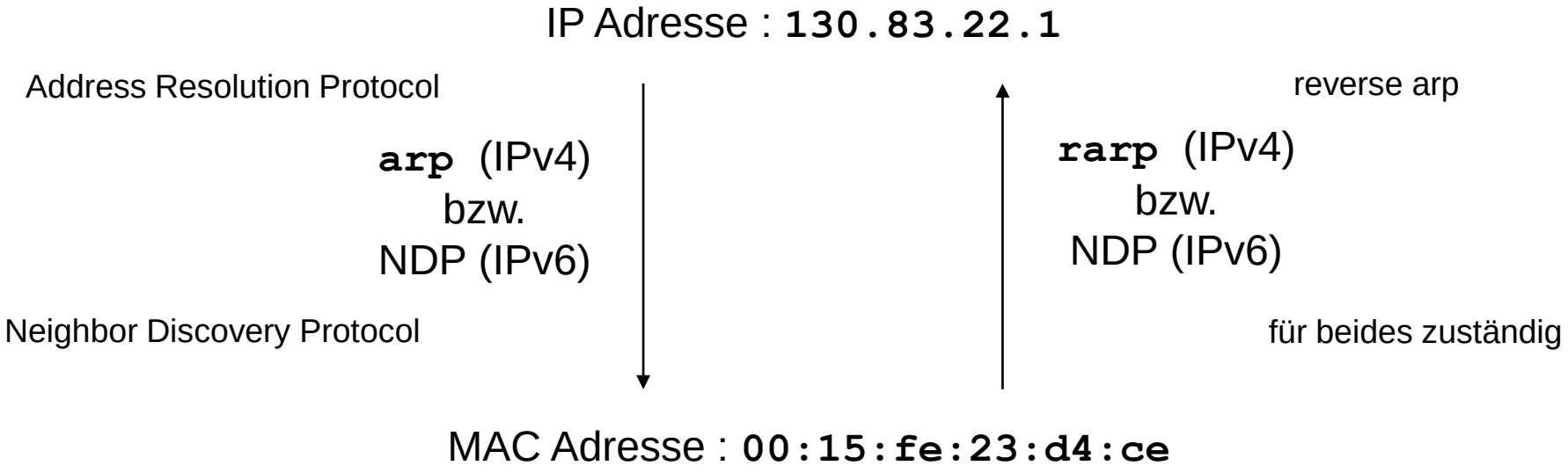
MAC-Filter z.B. bei Heim-WLANs keine verlässliche Zugriffskontrolle (alleine)

+

randomized MACs
erleichtern anonymes Surfen



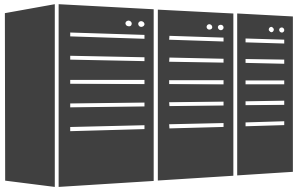
Übersetzung IP ↔ MAC im lokalen Subnetz



Routing

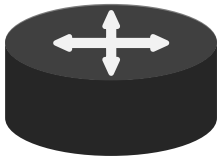
MAC: `00:18:34:de:f4:a8`
IP: `62.138.16.1`

MAC: `00:15:fe:23:d4:ce`
IP: `130.83.22.1`

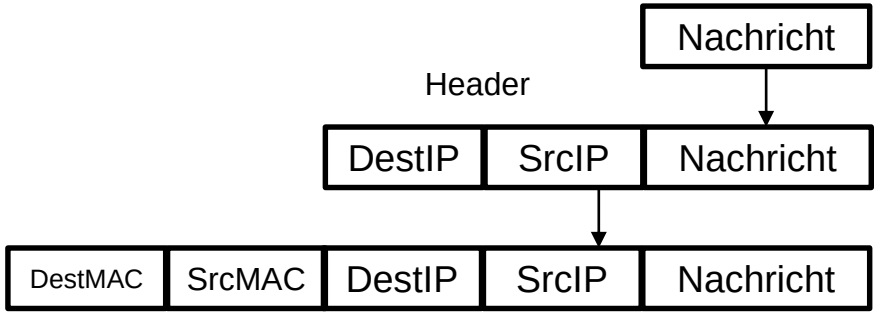


①
schickt an Gateway
SrcIP: `130.83.22.1`
DestIP: `62.138.16.1`
SrcMAC: `00:15:fe:23:d4:ce`
DestMAC: `00:27:de:88:a4:24`

Router/
Gateway



MAC: `00:27:de:88:a4:24`
IP: `130.83.239.1`



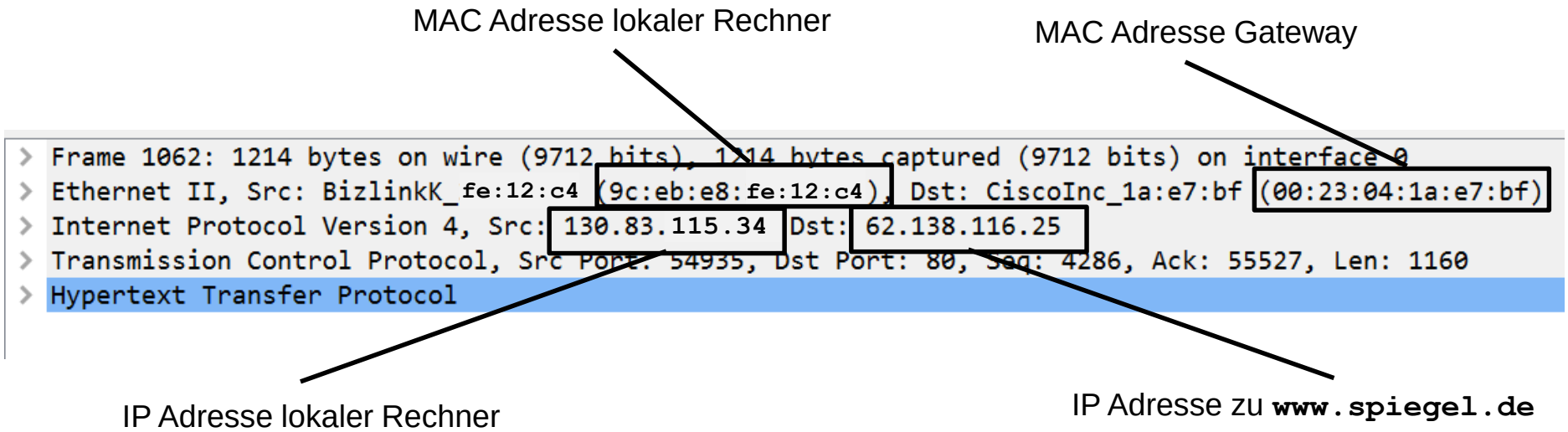
②
Ändert Source MAC zu `00:27:de:88:a4:24`
und Destination MAC zu `00:18:34:de:f4:a8`

Beispiel mittels Wireshark

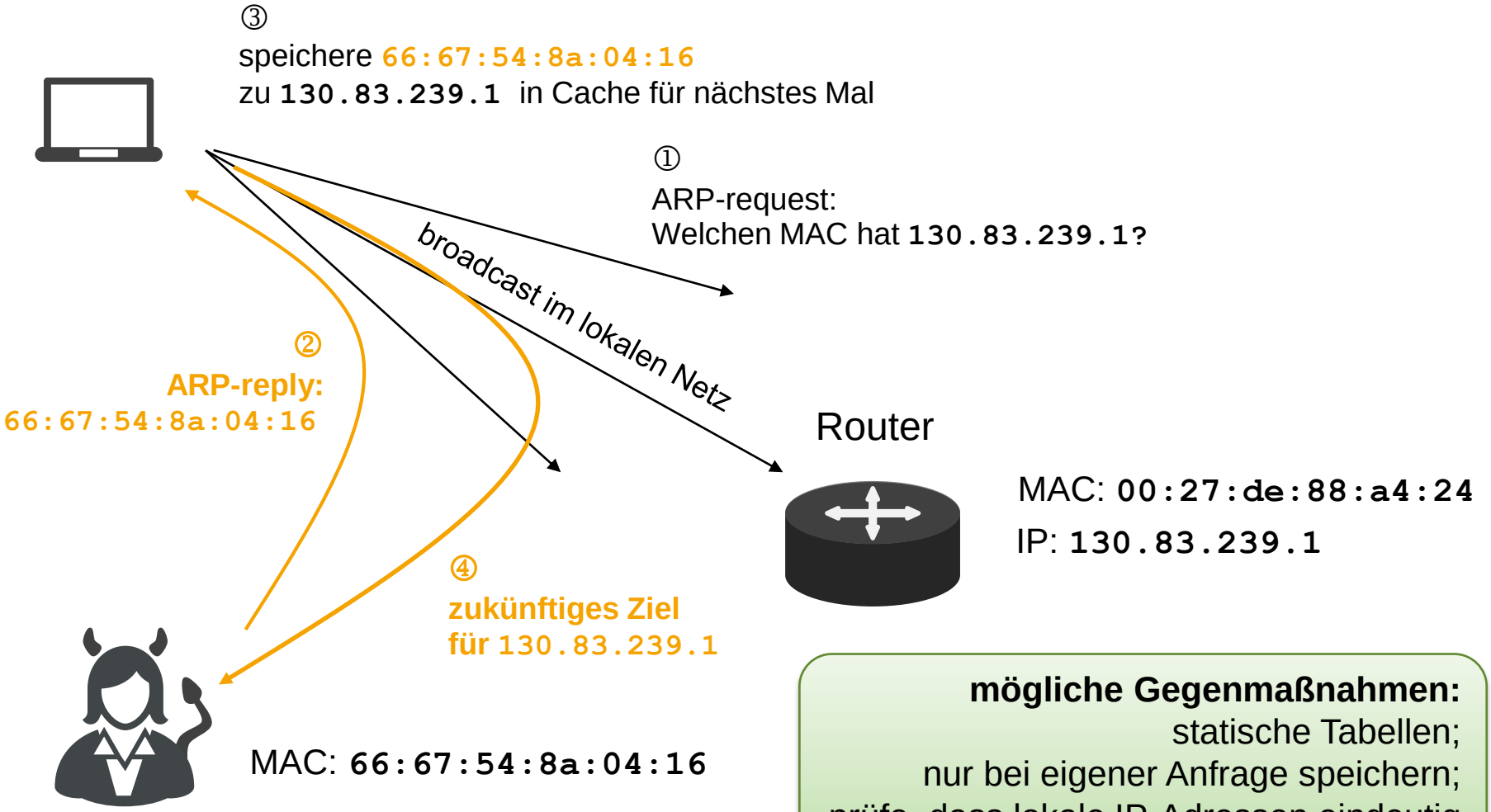
HTTP-Verbindung von lokalem Rechner zu **`www.spiegel.de`**

Verbindungsdaten per Wireshark aufgezeichnet

WIRESHARK
Quelle: www.wireshark.org



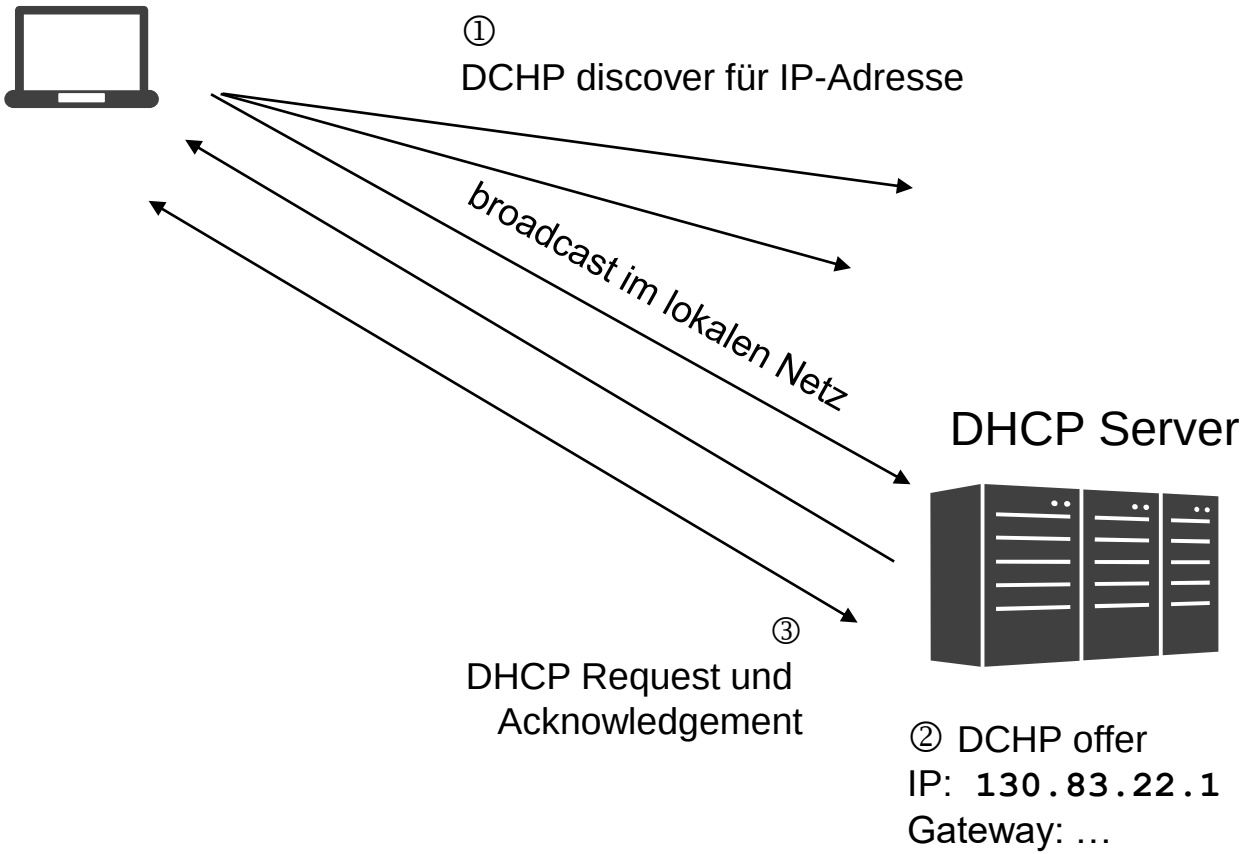
ARP Spoofing alias ARP Cache (or Request) Poisoning



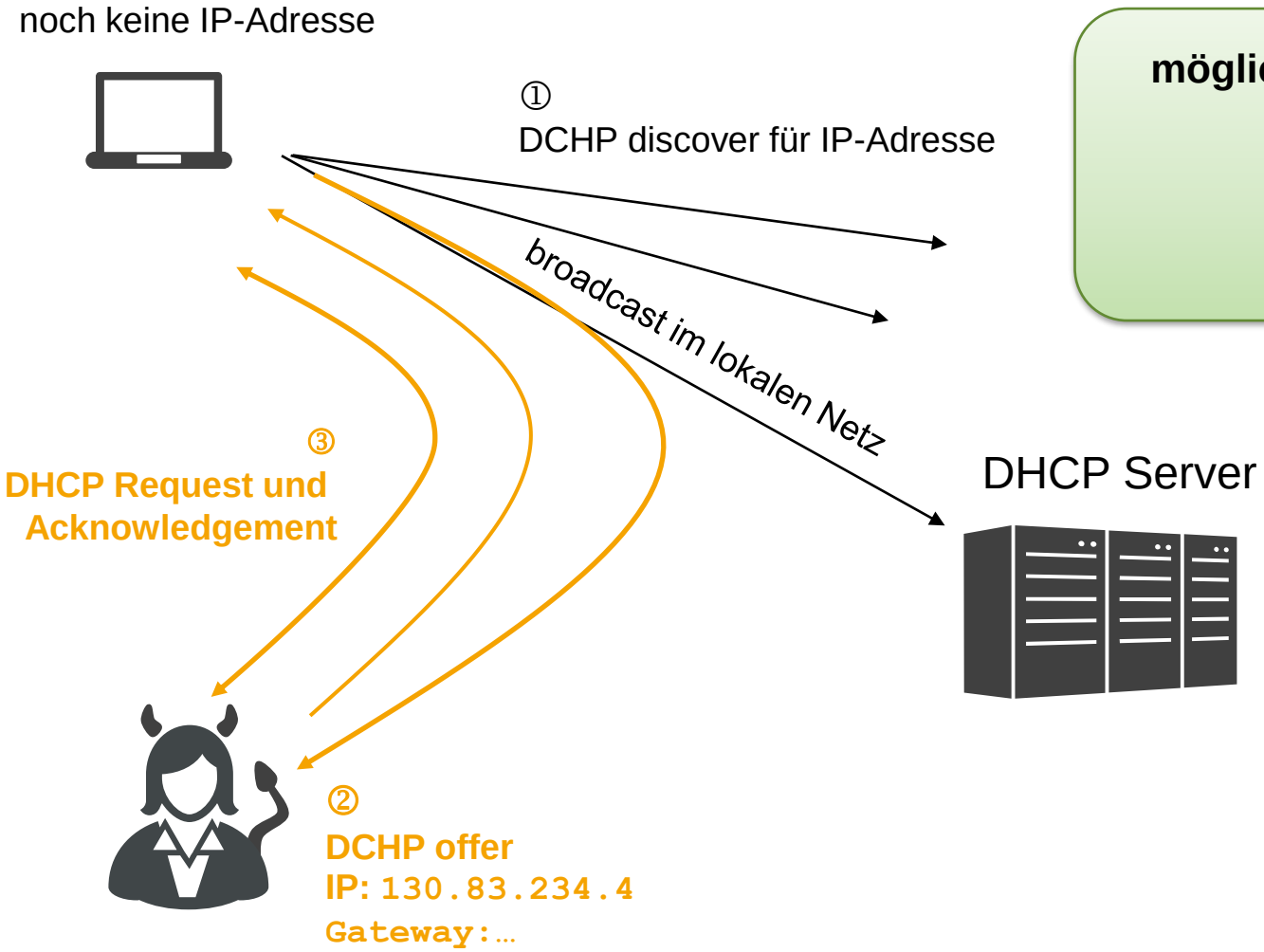
mögliche Gegenmaßnahmen:
statische Tabellen;
nur bei eigener Anfrage speichern;
prüfe, dass lokale IP-Adressen eindeutig

Dynamic Host Configuration Protocol (DHCP)

noch keine IP-Adresse



Rogue DHCP

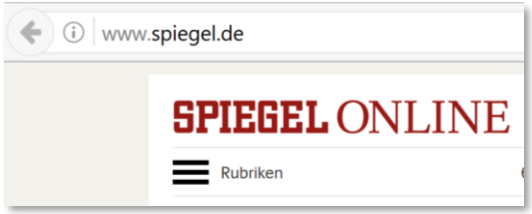


mögliche Gegenmaßnahmen:
DCHP Snooping,
das im lokalen Netz nur
vertrauenswürdige
DCHP-Server akzeptiert

Domain Name System (DNS)

möchte sich mit **`www.spiegel.de`** verbinden

Rechner kennt aber IP-Adresse
von **`www.spiegel.de`** (noch) nicht

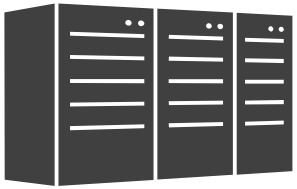


④ speichert
IP-Adresse
lokal

① suche IP von
`www.spiegel.de`

③ **`www.spiegel.de`**
hat IP **`62.138.116.25`**

DNS Server



IP-Adresse des DNS-Servers
meistens vorher durch
DHCP-Server zugewiesen

② kennt entweder IP-Adresse
oder fragt Root-Server zu
zuständigem Name-Server

DNS Spoofing (& Cache Poisoning)

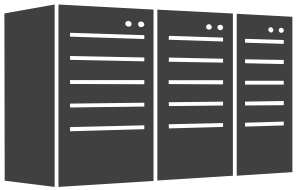
⑤ verbinde mit **165.34.23.66**

IP **165.34.23.66**

④ speichert IP-Adresse lokal

① suche IP von **www.spiegel.de**

DNS Server



③ **www.spiegel.de** hat IP **165.34.23.66**

Cache Poisoning:
kompromittiere DNS-Server
und schreibe falsche Daten
in Speicher

DNS Spoofing in der Praxis

The CoinJournal, 25. April 2018

Poisening
von DNS Servern

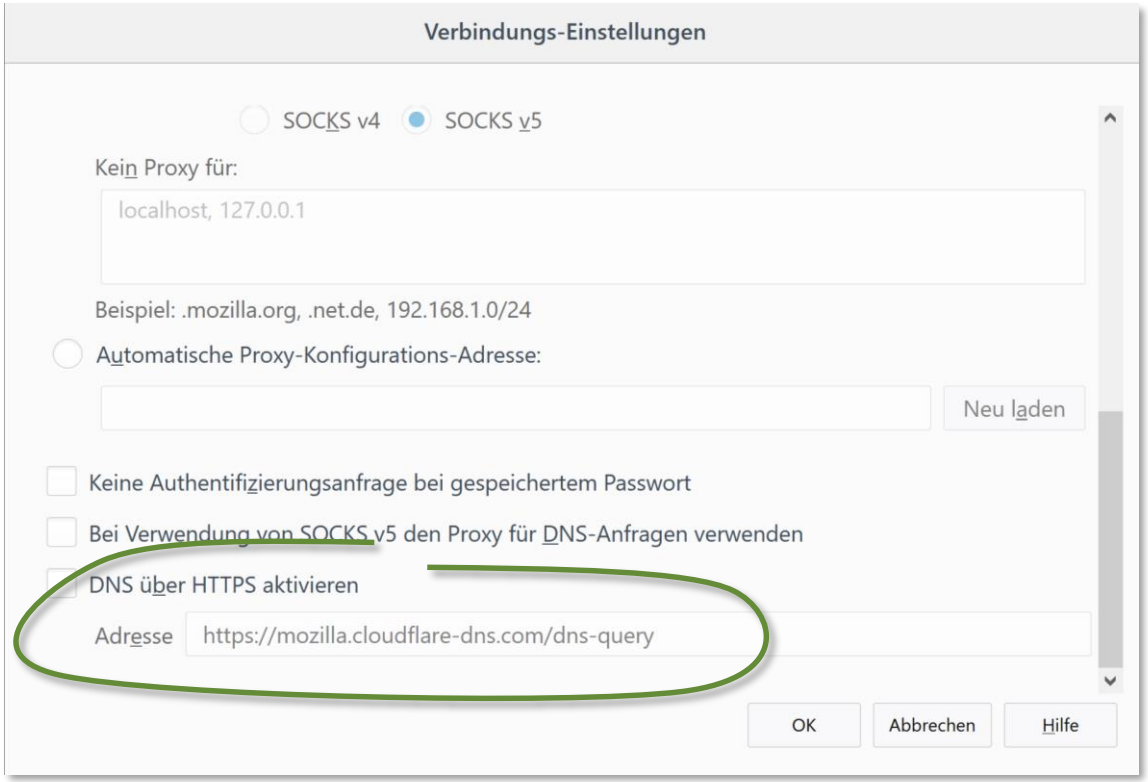
alle Anfragen an
`myetherwallet.com`
wurden auf Phishing-Seite
umgeleitet

Verlust ca. 150K US-$

Gegenmaßnahmen (DNS)

DNSSEC: Antworten signiert

DNS over TLS (DoT): sichere Verbindung zwischen Teilnehmer aufbauen



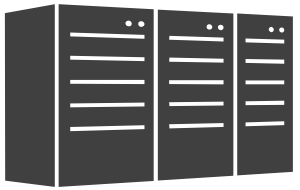
DNS over HTTPS (DoH): sichere HTTP-Verbindung aufbauen

(Standardisierung 19.10.2018 als RFC 8484 der IETF)

Ports

MAC: `00:18:34:de:f4:a8`

IP: `62.138.16.1`



16-Bit-“Anhängsel“ an IP-Adresse,
um Prozesse und Services zu identifizieren

Port Nummer	Dienst
25	SMTP (Mail)
80	http
143	imap
443	https
993	imaps (IMAP über SSL)
…	…

Port Scan mittels nmap

welche Ports sind offen?

identifiziert u.a. Betriebssystem

Nmap-Ausgabe | Ports / Rechner | Netzstruktur | Rechnereinzelheiten | Scans

```
nmap -T4 -A -v localhost
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disa
specify valid servers with --dns-servers
NSE: Script scanning 127.0.0.1.
Initiating NSE at 11:58
Completed NSE at 11:59, 30.07s elapsed
Initiating NSE at 11:59
Completed NSE at 11:59, 0.00s elapsed
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00065s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 997 closed ports
PORT     STATE SERVICE      VERSION
135/tcp  open  msrpc        Microsoft Windows RPC
445/tcp  open  microsoft-ds Windows 10 Home 14393 microsoft-ds
5357/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1511
Uptime guess: 0.752 days (since Sun Nov 27 17:56:20 2016)
Network Distance: 0 hops
TCP Sequence Prediction: Difficulty=259 (Good luck!)
IP ID Sequence Generation: Incrementing by 2
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

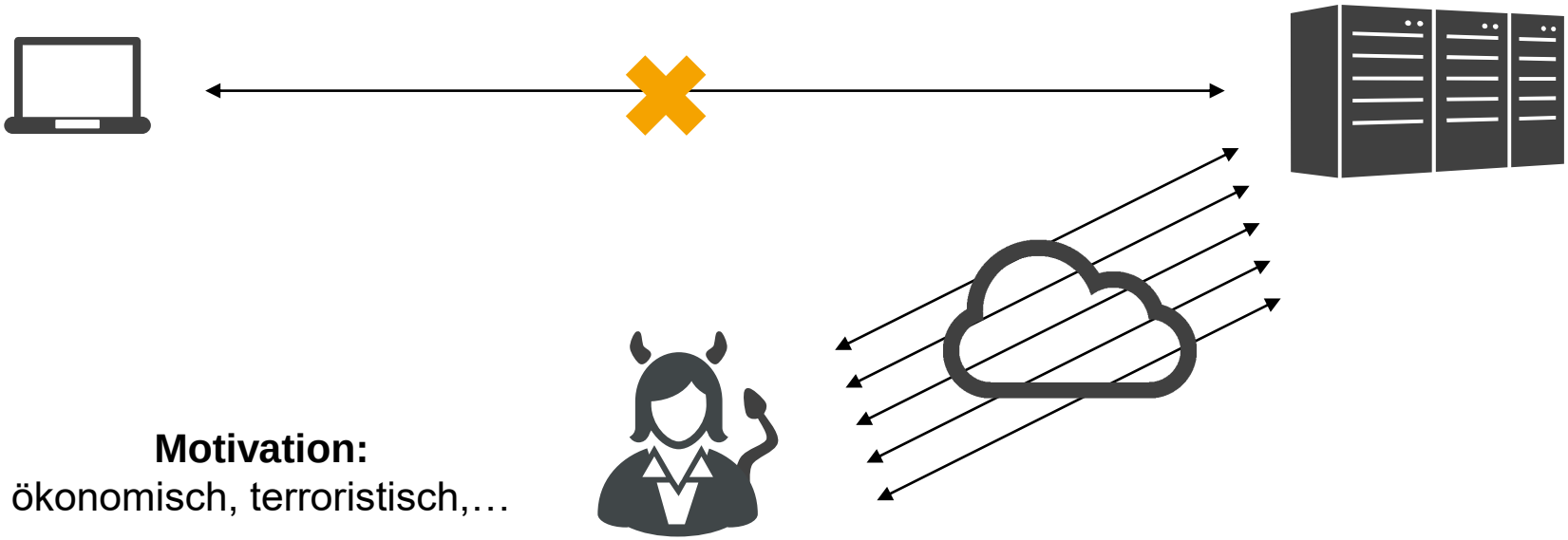
Erklären Sie den Unterschied zwischen einer IP-Adresse und MAC.

Was ist ein ARP-Spoofing-Angriff?

Warum kann man nicht einfach die Nachricht eines DHCP-Servers signieren, um einen Angriff zu verhindern?

Denial-of-Service-Angriffe

Allgemeines Ziel von DoS-Angriffen



Motivation:
ökonomisch, terroristisch,…

Ziel:
Überlaste Server (oder auch Provider!), so dass keine „normale“ Kommunikation mehr möglich

Vorgehen:
Smurf, SYN-ACK-Flooding,….

DoS-Angriffe passieren ständig

US politics world opinion sports soccer tech arts lifestyle fashion business travel environme

home › tech

Internet

Major cyber attack disrupts internet service across Europe and US

Denial of service attack from unknown culprits on domain name system company Dyn caused access to be severely restricted for users on Friday

Sam Thielman in New York and Chris Johnston in London

Friday 21 October 2016 12.06 EDT

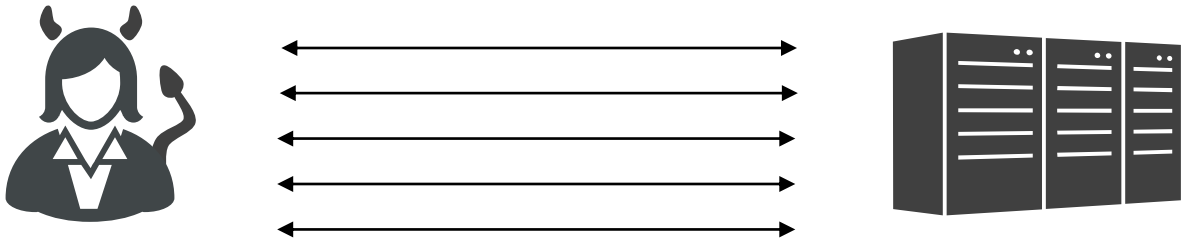
Quelle: The Guardian (21.Okt.2016)

Angriff nahm Netflix, Twitter, Sporitfy,
New York Times, Wall Street Journal usw.
vom Netz

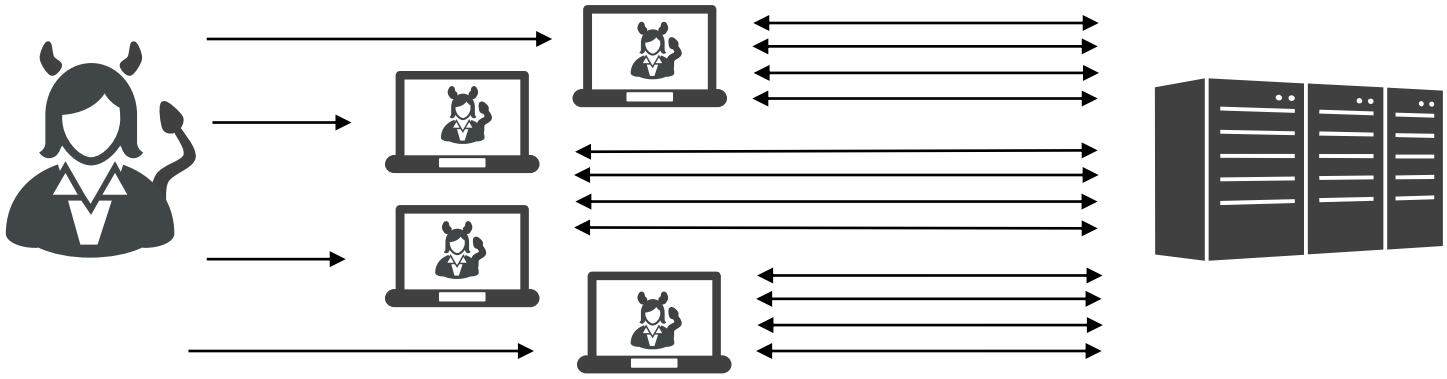
Link: Übersichtskarte über aktuelle DoS-Angriffe

Allgemeine Technik von DoS-Angriffen

DoS-Angriff: ein Rechner (evtl. aber weitere „ehrliche“ Rechner involviert)



Distributed DoS-Angriff (DDoS): mehrere infizierte Rechner (Botnet) involviert



Internet Control Message Protocol (ICMP)

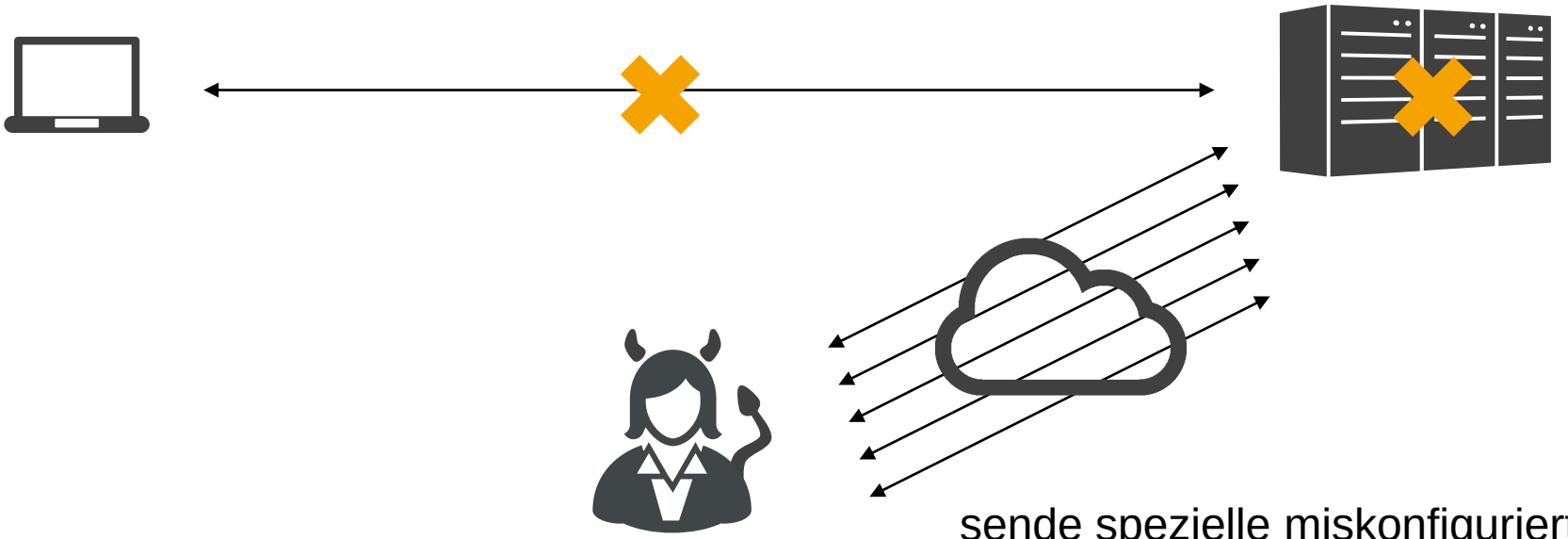
Internet Control Message Protocol (ICMP)
für Informations- und Fehlermeldungen des Netzwerks

ICMP-Beispiel: per **`ping`**
Verbindungslatenz prüfen

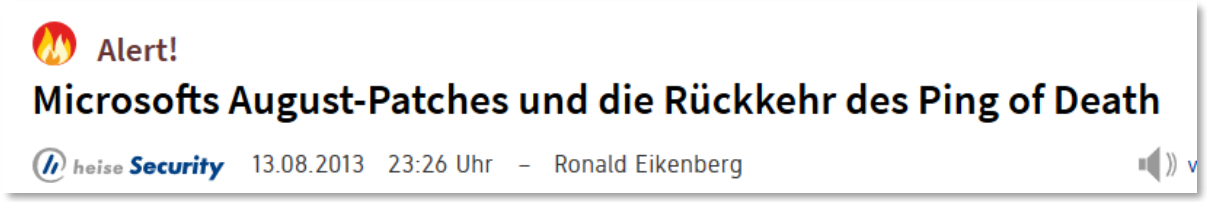
```
>ping 95.100.164.179

Ping wird ausgeführt für 95.100.164.179 mit 32 Bytes Daten:
Antwort von 95.100.164.178: Bytes=32 Zeit=1ms TTL=55
Antwort von 95.100.164.178: Bytes=32 Zeit=1ms TTL=55
Antwort von 95.100.164.178: Bytes=32 Zeit=1ms TTL=55
Antwort von 95.100.164.178: Bytes=32 Zeit=1ms TTL=55

Ping-Statistik für 95.100.164.179:
    Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0
    (0% Verlust),
Ca. Zeitangaben in Millisek.:
    Minimum = 1ms, Maximum = 1ms, Mittelwert = 1ms
```

Ping of Death (PoD)

vergleichbar: Teardrop Attack, bei dem
falsch fragmentierte Pakete
zum Absturz führen sollen

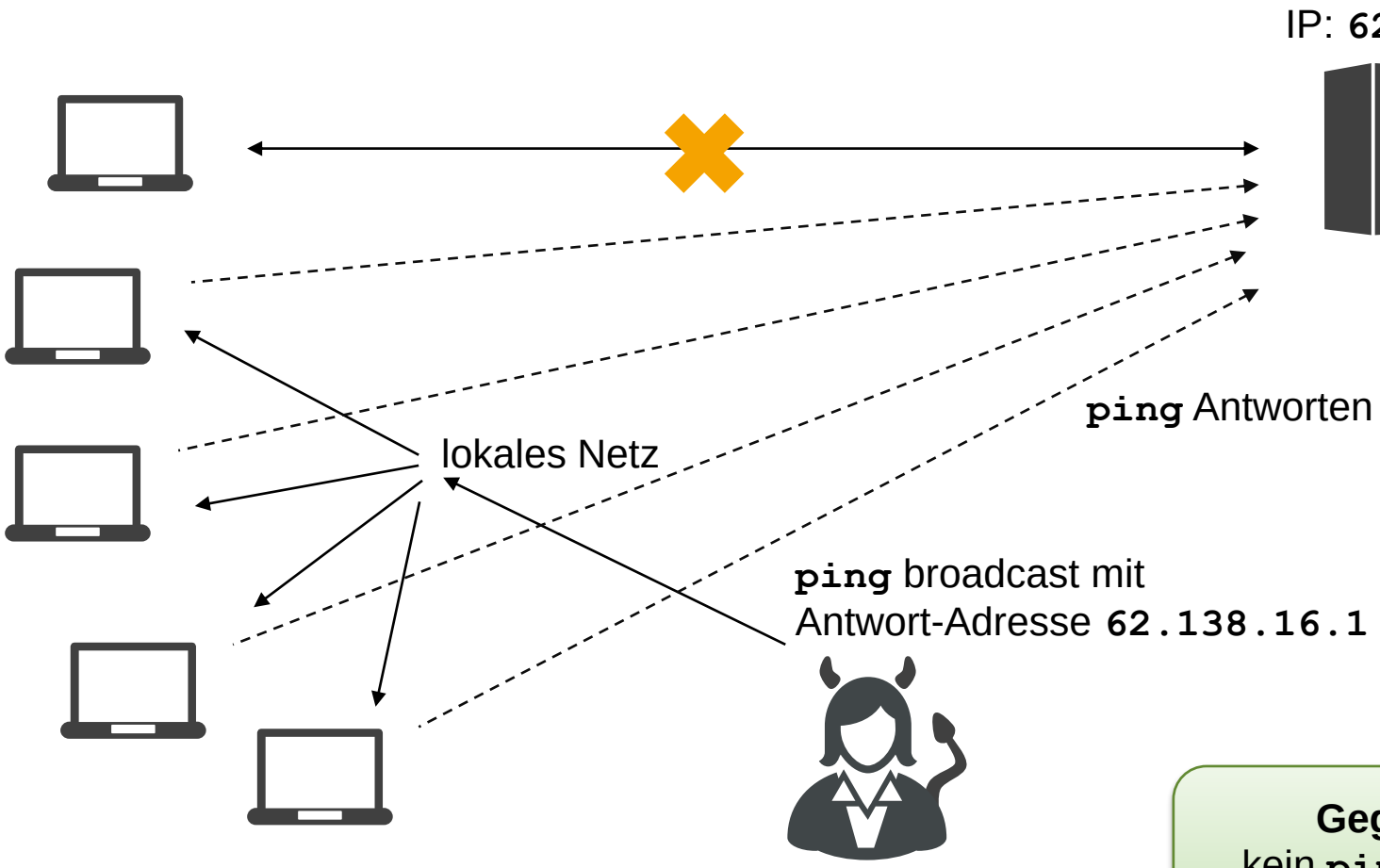


sende spezielle miskonfigurierte
ICMP-Nachrichten,
die zum Absturz des Servers führen



Quelle: heise Security (2013)

Smurf Attack

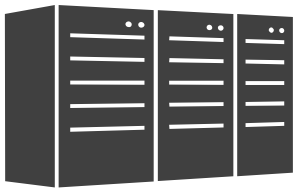


Amplification attack:
1 Anfrage erzeugt bis zu 255 Antworten

Gegenmaßnahme:
kein `ping` broadcast im lokalen Netz erlauben

Transmission Control Protocol (TCP)

Verbindungsaufbau („Handshake“)
auf Transport-Layer-Ebene per TCP



SYN

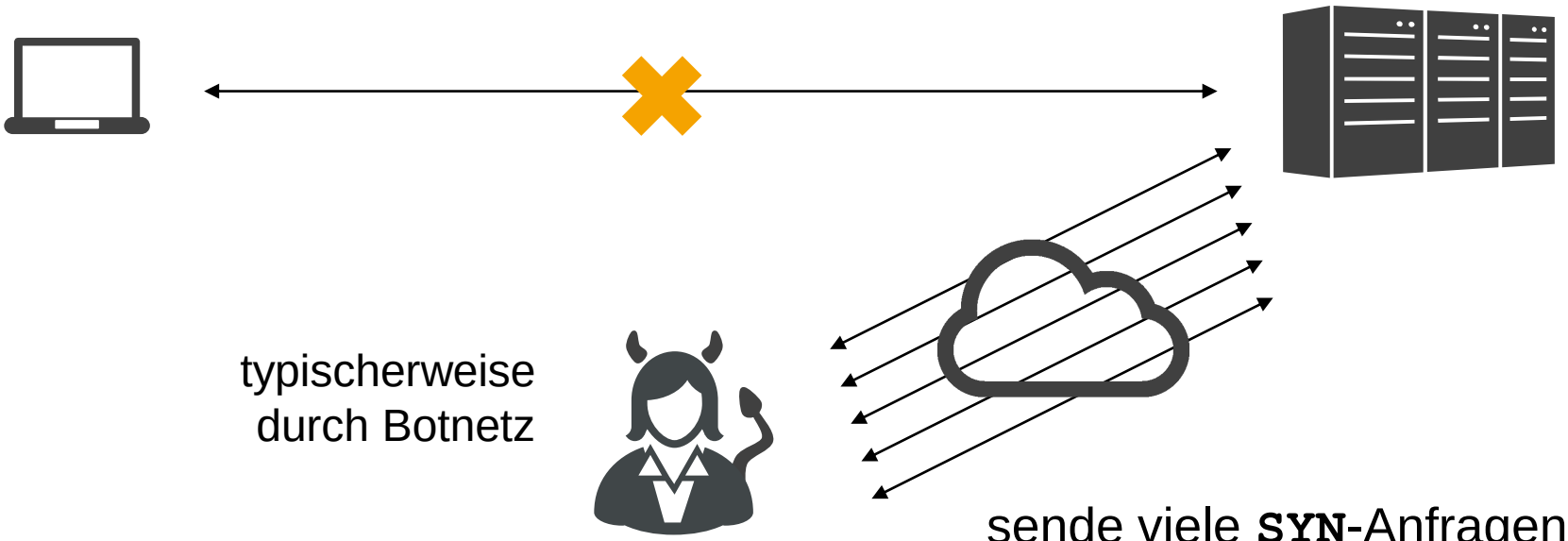
SYN-ACK

halte Verbindung
offen bis **ACK**

ACK

TCP ist verbindungsorientiert,
im Unterschied zum einfacheren User Datagram Protocol (UDP)

SYN Flood



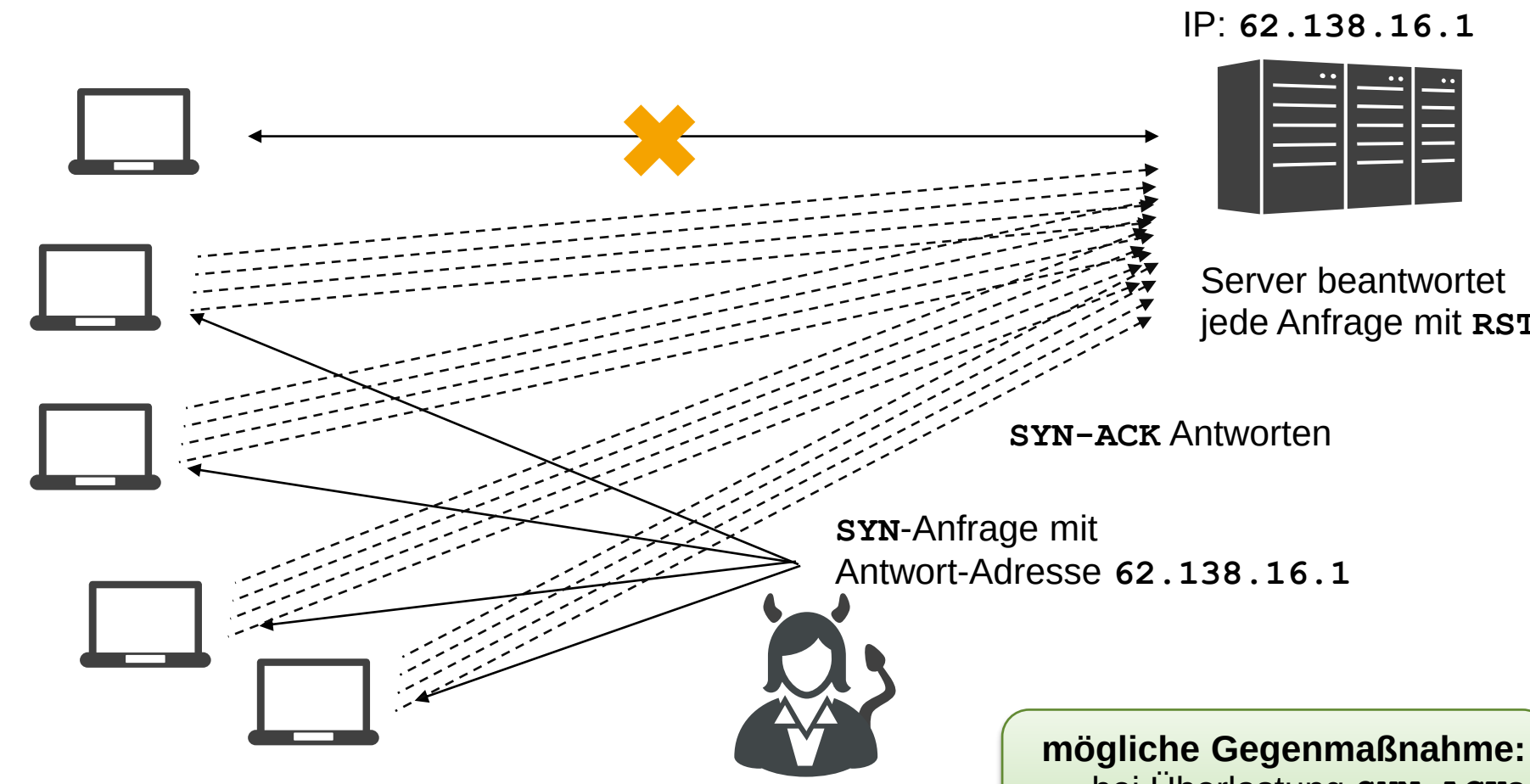
typischerweise
durch Botnetz

sende viele **SYN**-Anfragen,
ohne SYN-ACK mit **ACK**
zu beantworten

bis Server wegen
zu vieler offener TCP-Verbindungen
keine weitere Verbindungen anbieten kann

mögliche Gegenmaßnahme:
SYN cookies, die in Antwortsequenz-nummer Verbindung kodieren,
SYN-Anfrage erst löschen und
aus **ACK**-Anfrage später
SYN-Anfrage wieder rekonstruieren

SYN-ACK Flood (SYN Reflection Attack)



Amplification attack:
1 Anfrage erzeugt ca. 3-5 Antworten

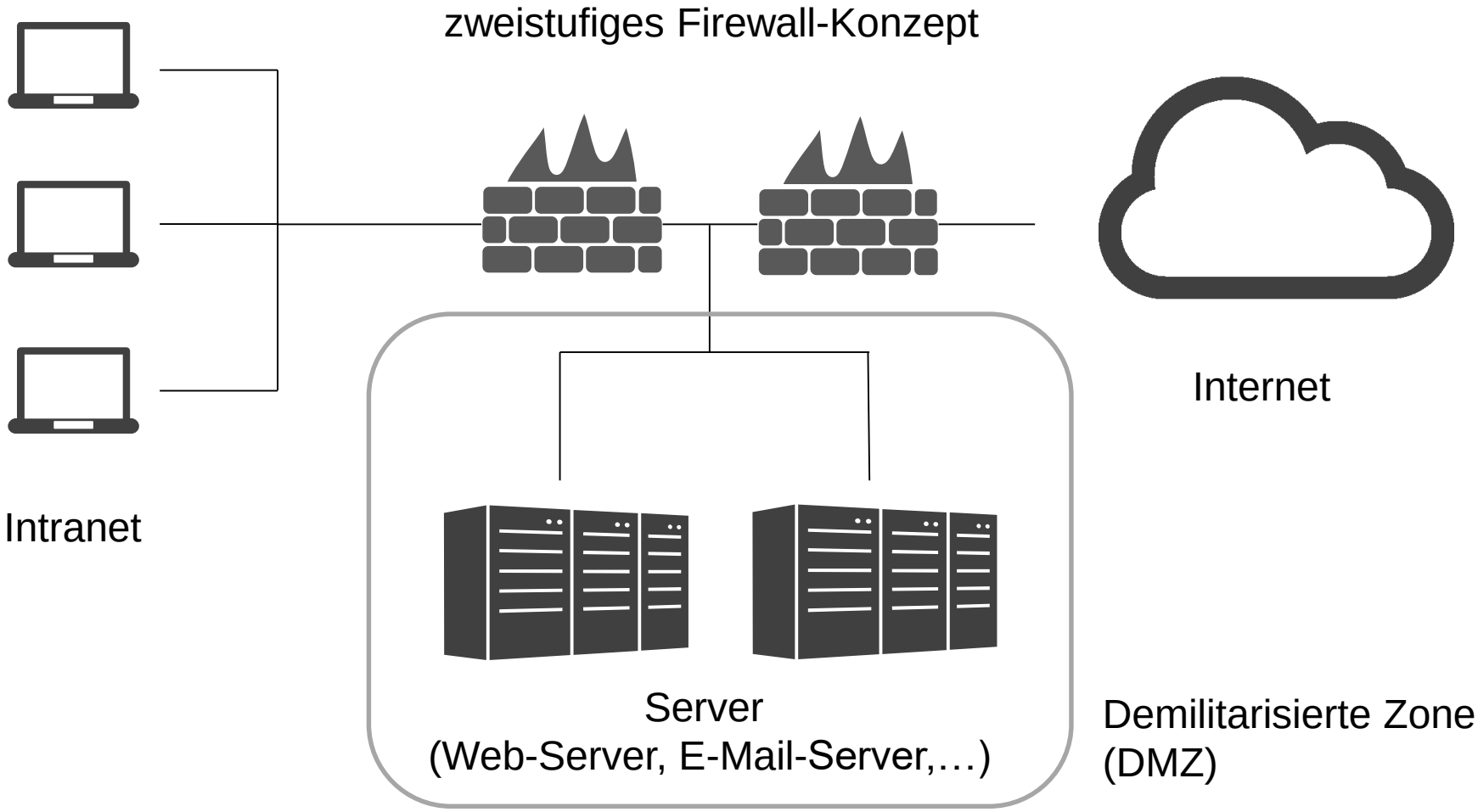
mögliche Gegenmaßnahme:
bei Überlastung **SYN-ACK**s durch Firewall filtern

Was ist der Unterschied zwischen einem DoS- und einem DDoS-Angriff?

Was ist der Unterschied zwischen einem SYN-Flood-Angriff und einem SYN-ACK-Flood-Angriff?

Firewalls &
Intrusion Detection und Prevention Systems

Firewalls



Firewalls im Schichtenmodell

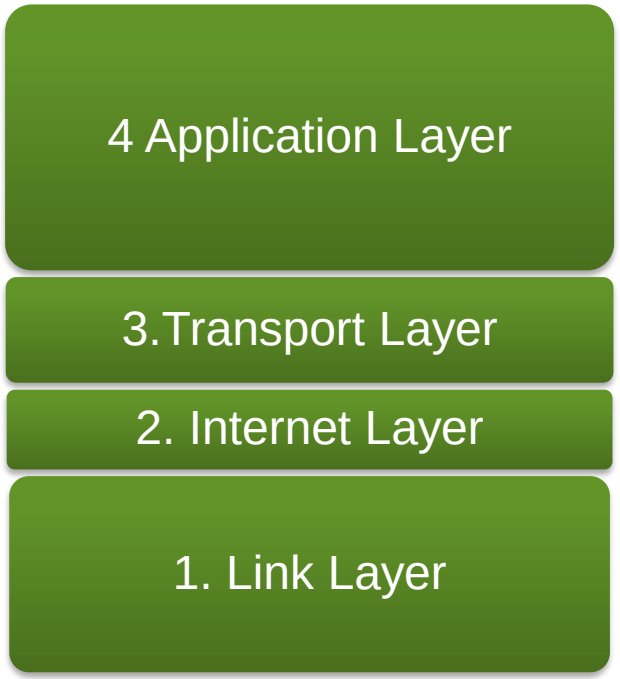
Schützen gegen Angriffe basierend auf Anwendungen (HTTP, Javascript,…), damit auch komplexer

Application (oder Proxy) Firewalls →

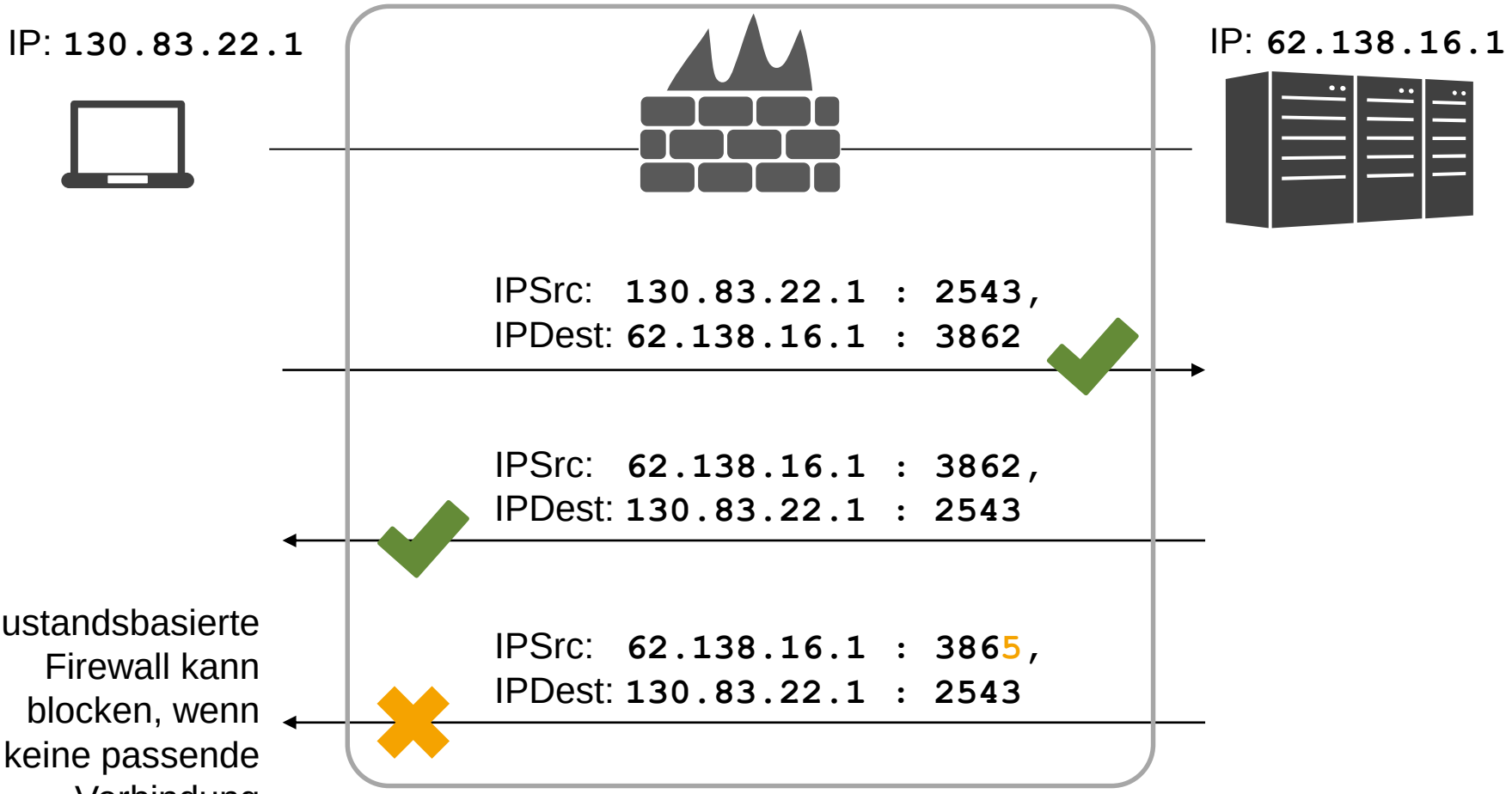
(Netzwerk-) Firewalls →

zustandslos oder zustandsbasiert

Schützen gegen Angriffe basierend auf UDP/TCP/ICMP,…



Zustandslose vs. zustandbasierte Firewalls



zustandsbasierte Firewall kann blocken, wenn keine passende Verbindung

zustandslose Firewall müsste Paket passieren lassen, sofern keine explizite Regel

Beispiel: Linux-basierte Netwerk-Firewalls per `iptables`

(„Paketfilter“)

Beispiel: Default-Regel

```
iptables -P INPUT DROP
iptables -P OUTPUT DROP
```

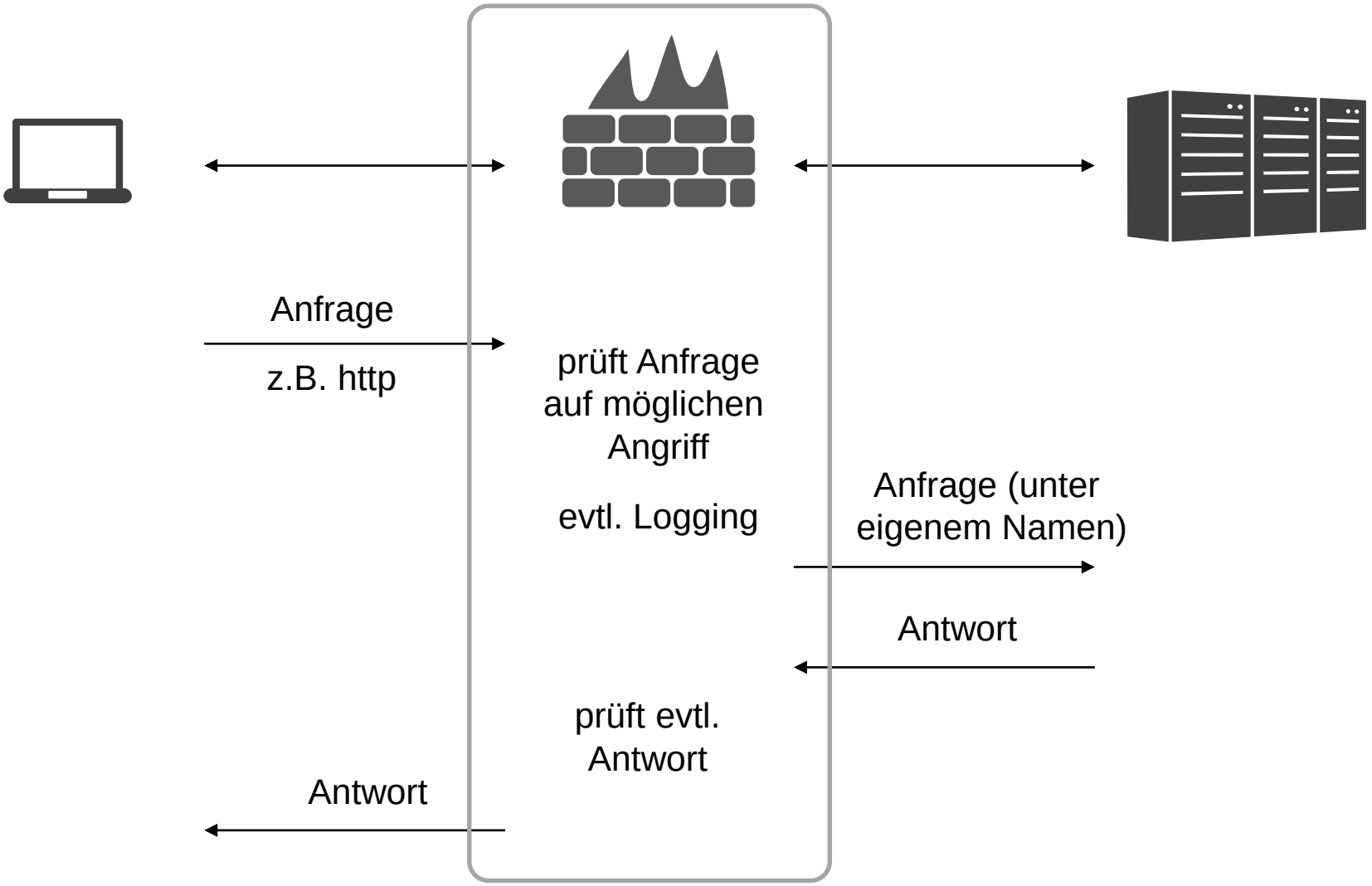
Beispiel: **`ping`** nur aus dem lokalen Netzwerk erlauben:

```
iptables -A INPUT -p icmp --src 130.83.22.0/24 -j ACCEPT
iptables –A INPUT –p icmp --icmp-type echo-request -j DROP
```

Beispiel: http-Verbindungen erlauben:

```
iptables -A INPUT -p tcp --dport 80 -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -p tcp --sport 80 -m state --state ESTABLISHED -j ACCEPT
```

Application-Firewalls

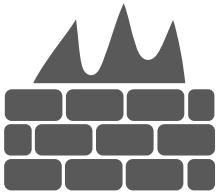


Intrusion Detection und Prevention Systems (IDS/IPS)

IDS untersucht auf Netzwerkebene Inhalt
und meldet verdächtige Kommunikation (z.B. Bytecode von Viren)

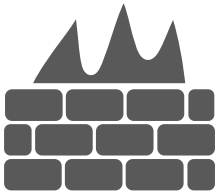
IPS kann verdächtige Kommunikation blockieren oder ändern

Unterschiede zu Firewalls (Übergänge fließend):



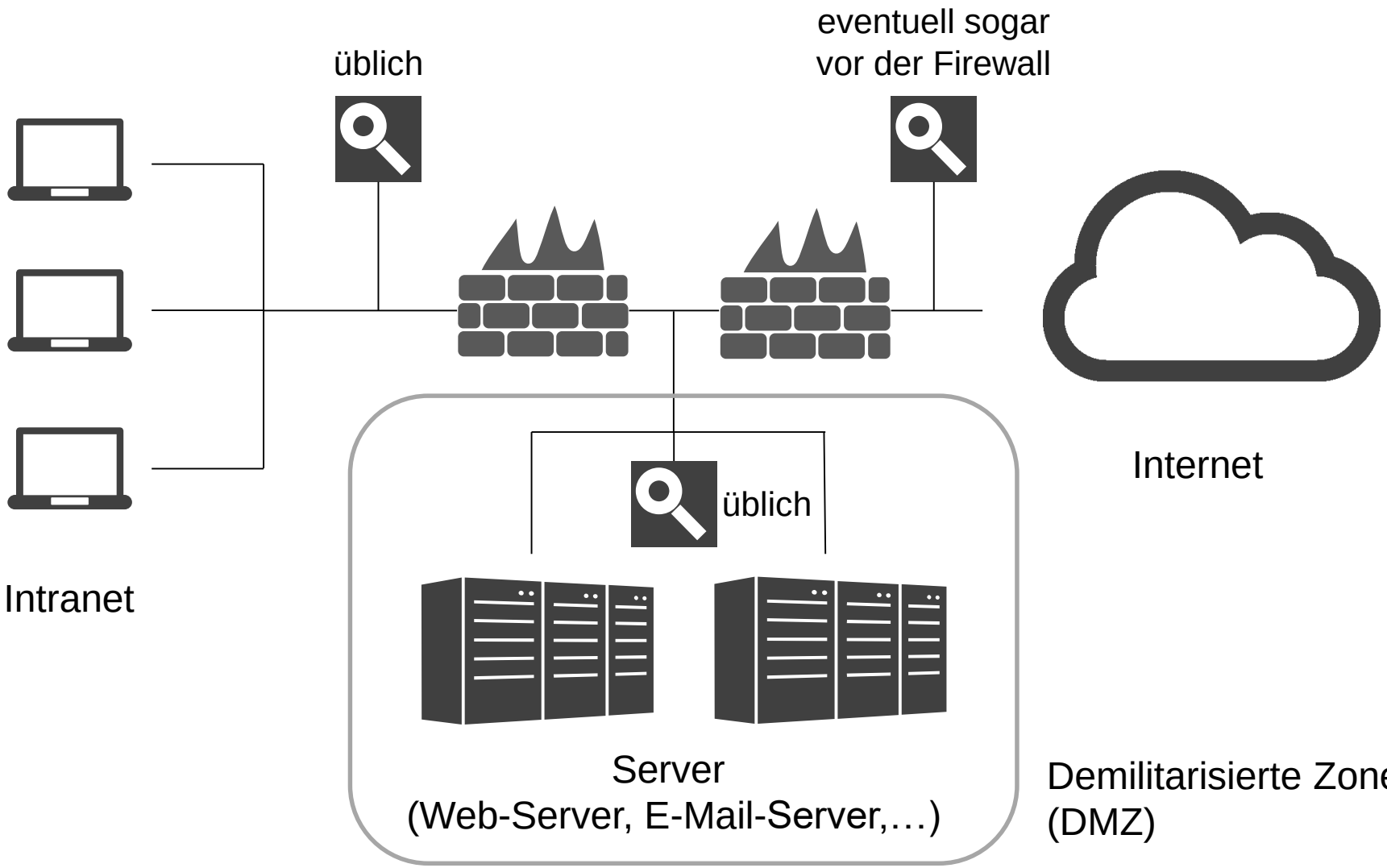
Netzwerk-Firewall:
untersucht nur Header

IDS/IPS:
untersucht auch Inhalt



Proxy-Firewall:
operiert auf Application-Layer

IPS und IDS im System



Beispiel: Snort

bekanntes OpenSource-IPS

Quelle: snort.org

EXAMPLE

Rule Header	`alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any`
Message	`msg: "BROWSER-IE Microsoft Internet Explorer CacheSize exploit attempt";`
Flow	`flow: to_client,established;`
Detection	`file_data; content:"recordset"; offset:14; depth:9; content:".CacheSize"; distance:0; within:100; pcre:"/CacheSize\s*=\s*/"; byte_test:10,>,0x3ffffffe,0,relative,string;`
Metadata	`policy max-detect-ips drop, service http;`
References	`reference:cve,2016-8077;`
Classification	`classtype: attempted-user;`
Signature ID	`sid:65535;rev:1;`

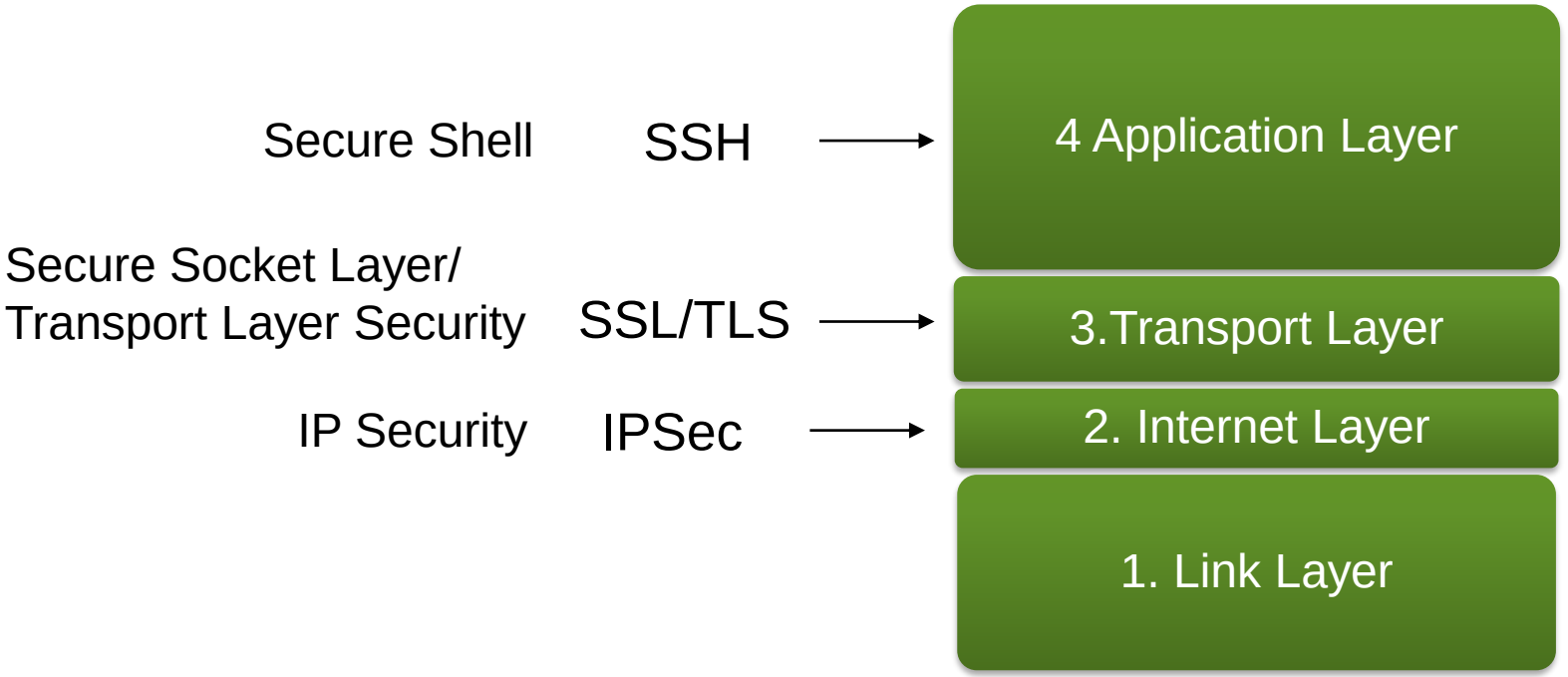
← „Netzwerk-Regel“

← Suchregeln,
z.B. per regulärem Ausdruck
wie weit in der Kommunikation,
…

Quelle: snort.org

Sichere Verbindungen

Sichere Verbindungen auf verschiedenen Ebenen

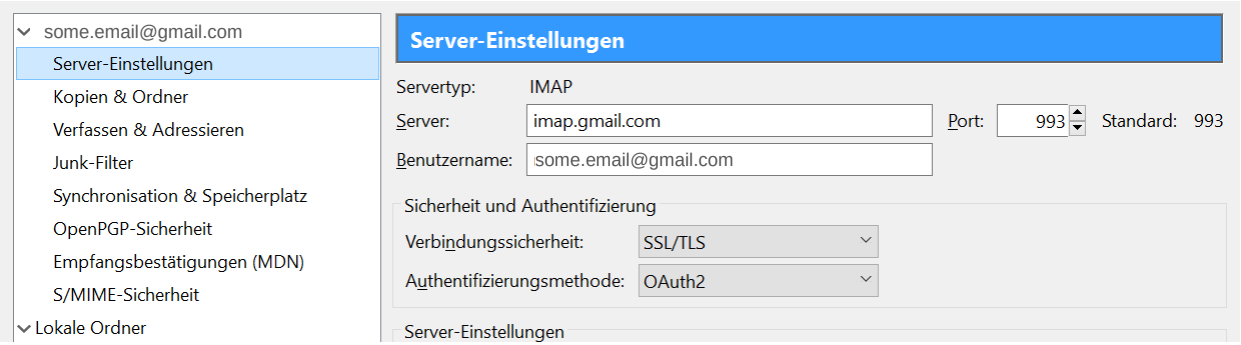


Transport Layer Security (TLS)

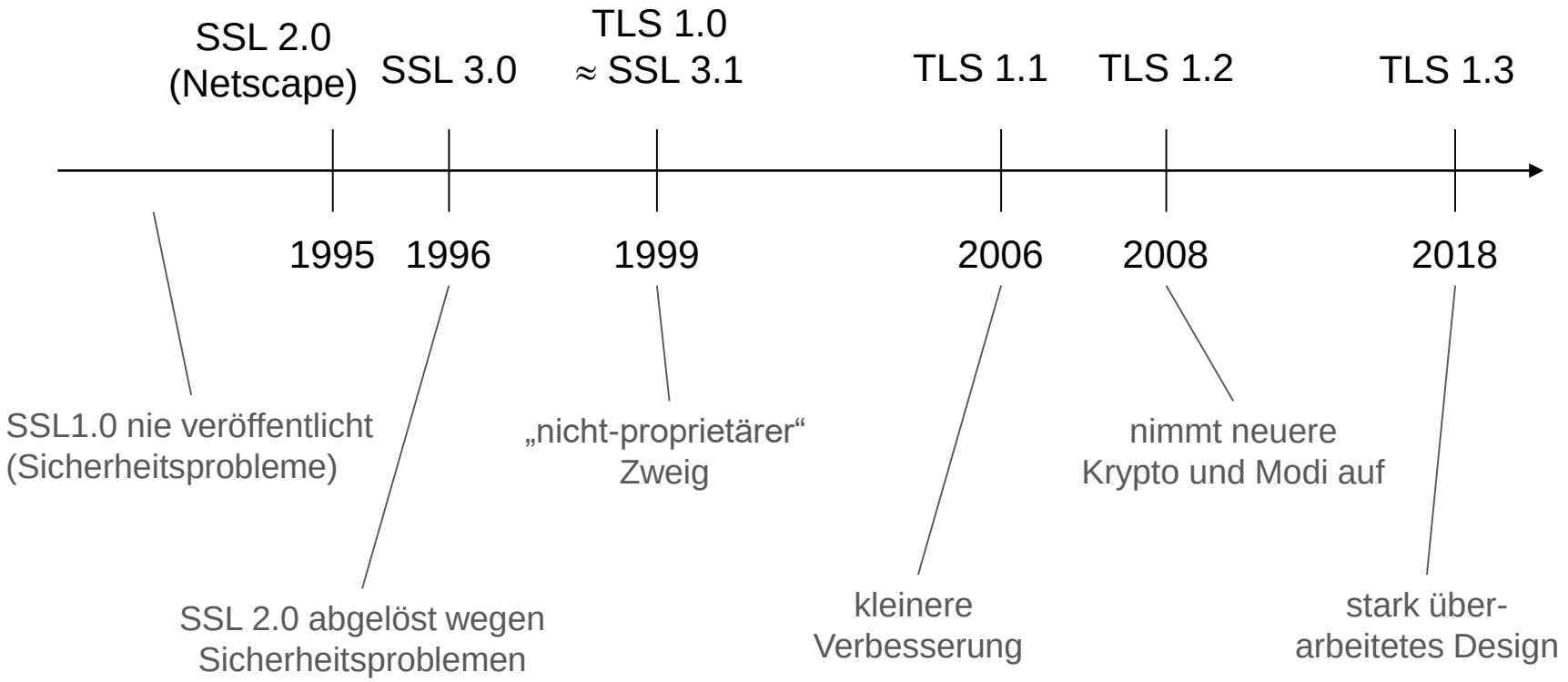
TLS heute das am häufigsten verwendet Kryptoverfahren

baut kryptographisch sichere Verbindung (Vertraulichkeit + Integrität) auf

insbesondere HTTP über TLS (HTTPS) und sicherer E-Mail-Abruf



Geschichte von SSL/TLS



Angriffe auf SSL/TLS

BEAST (2011)

3Handshake (2014)

Lucky Thirteen (2013)

DROWN (2016)

POODLE (2014)

FREAK (2013)

SLOTH (2016)

Logjam (2015)

Heartbleed (2013)

Sweet32 (2016)

in der Regel auf ältere Versionen (TLS 1.0 oder 1.1) oder
auf schwache Varianten von TLS 1.2 (z.B. wenn noch MD5 verwendet wird)

entsprechende Varianten sollten dann nicht mehr unterstützt werden

Einsatz von SSL/TLS

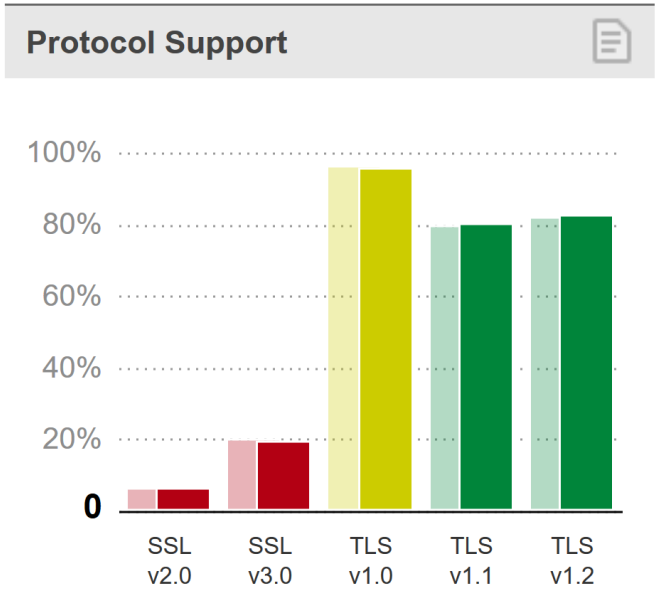
Theorie:

SSL 2.0 soll seit 2011 nicht mehr verwendet werden
SSL 3.0 soll seit 2015 nicht mehr verwendet werden

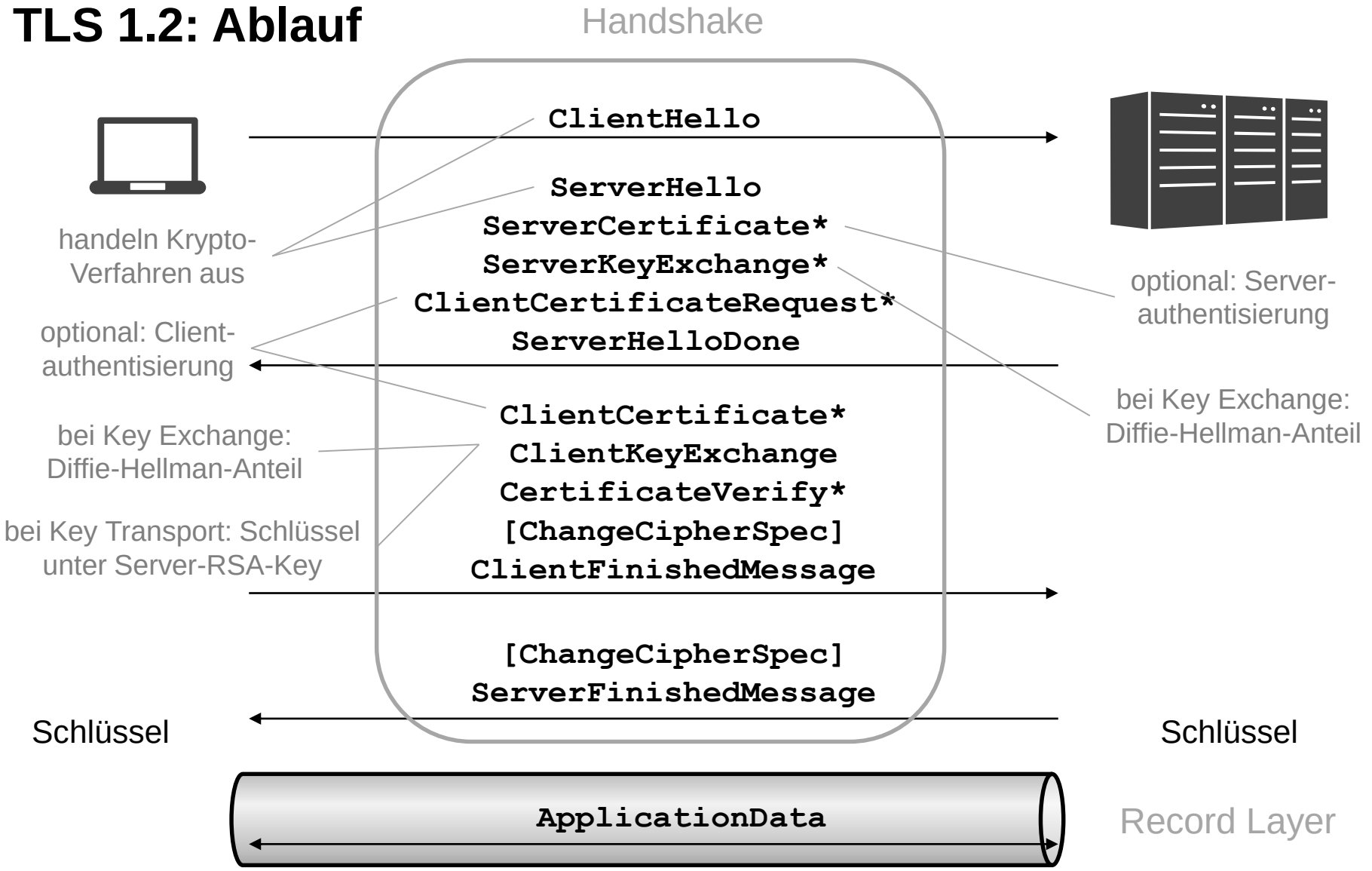
Praxis:

von ca. 140.000 populären Seiten:
ca. 6% unterstützen noch SSL 2.0
ca. 19% unterstützen noch SSL 3.0

Stand: Dezember 2016
https://www.trustworthyinternet.org/ssl-pulse/



TLS 1.2: Ablauf



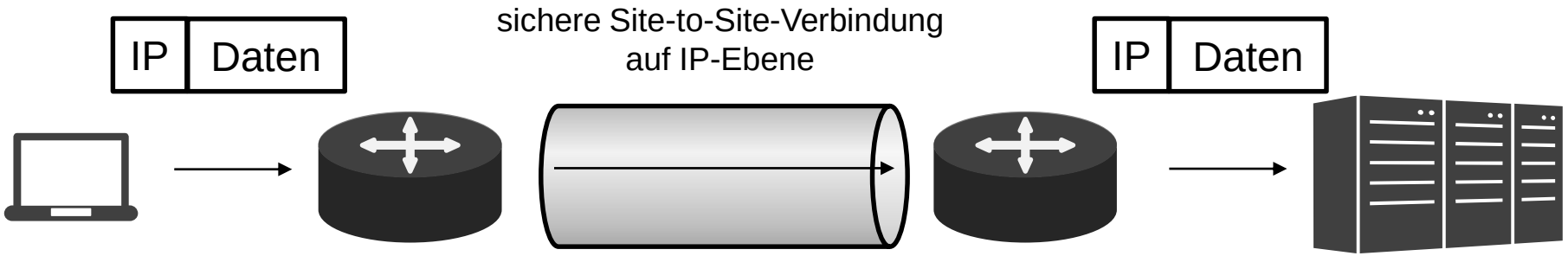
Nennen Sie einen Unterschied zwischen einer Netzwerk-Firewall und einem IDS.

Welche beiden Methoden zur Ableitung des gemeinsamen Schlüssels gibt es in TLS?

Können Sie sich den Sinn einer TLS-Verbindung ohne Client und ohne Server-Authentisierung vorstellen?

Virtual Private Networks (VPNs)

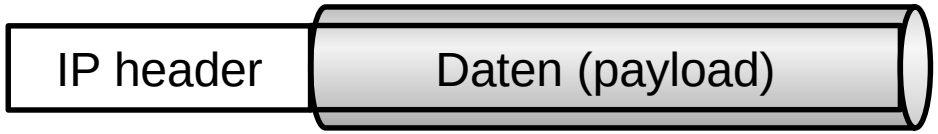
Transportieren oder Tunneln?



verschlüsselt

entschlüsselt

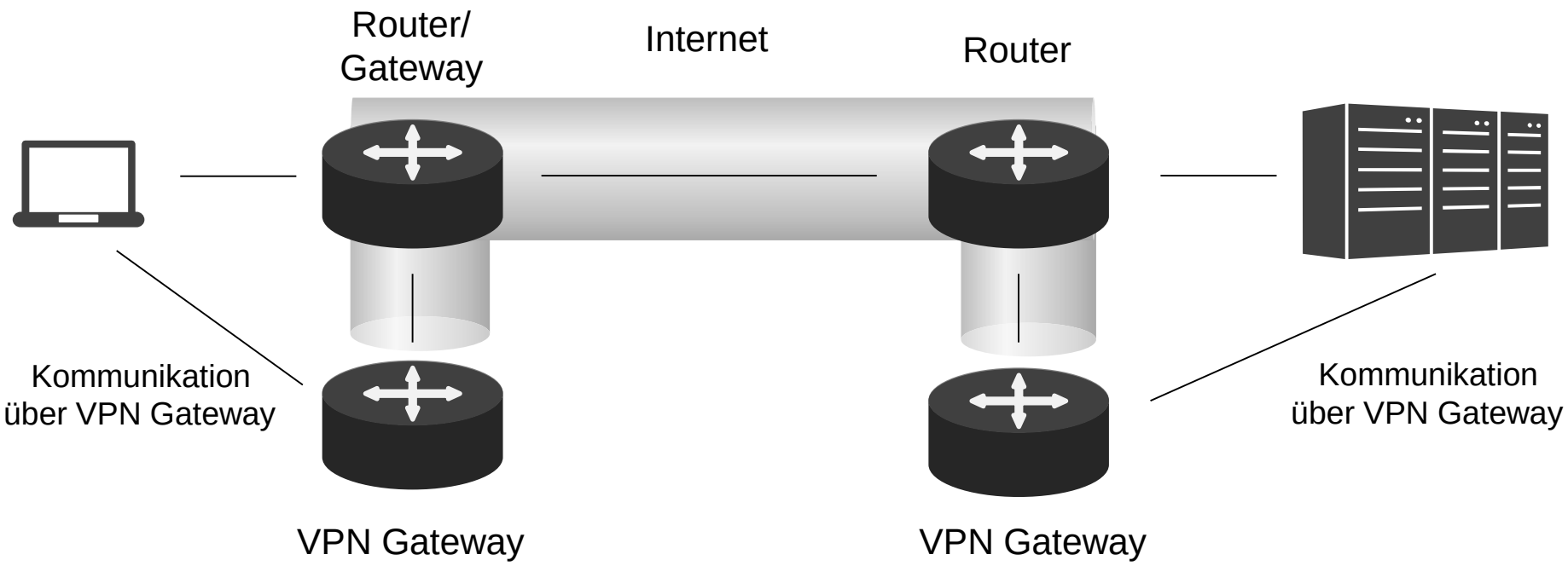
Transportmodus:



Tunnelmodus:

neuen Header mit Router-Adressen hinzufügen (Sender)
bzw. entfernen (Empfänger)

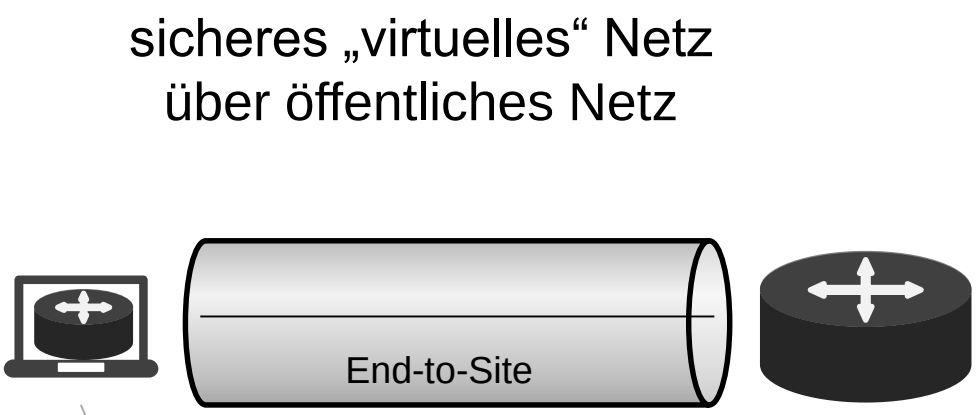
Tunneln über vorhandene Infrastruktur

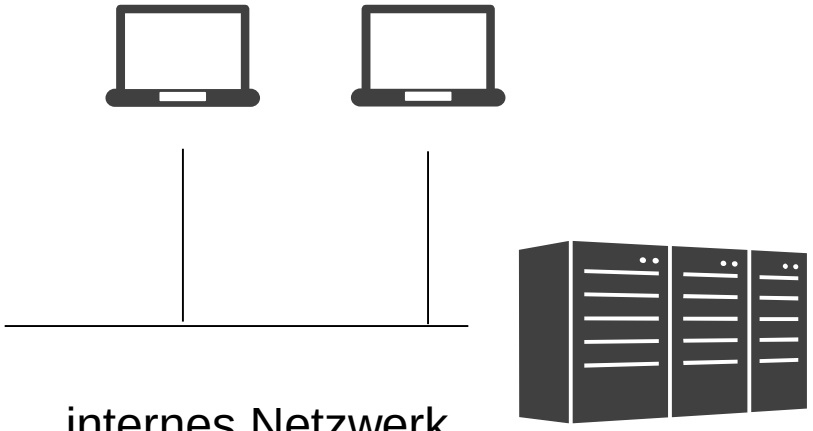


transparente, sichere Verbindung über öffentliches Netzwerk

Virtual Private Network (VPN)

sicheres „virtuelles“ Netz
über öffentliches Netz





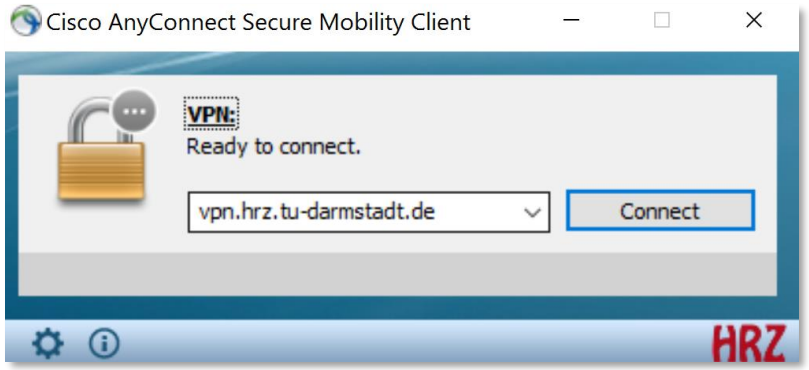
internes Netzwerk

IP : **130.83.22.0/24**

IP : **130.83.22.11**

Rechner virtuell im internen Netz

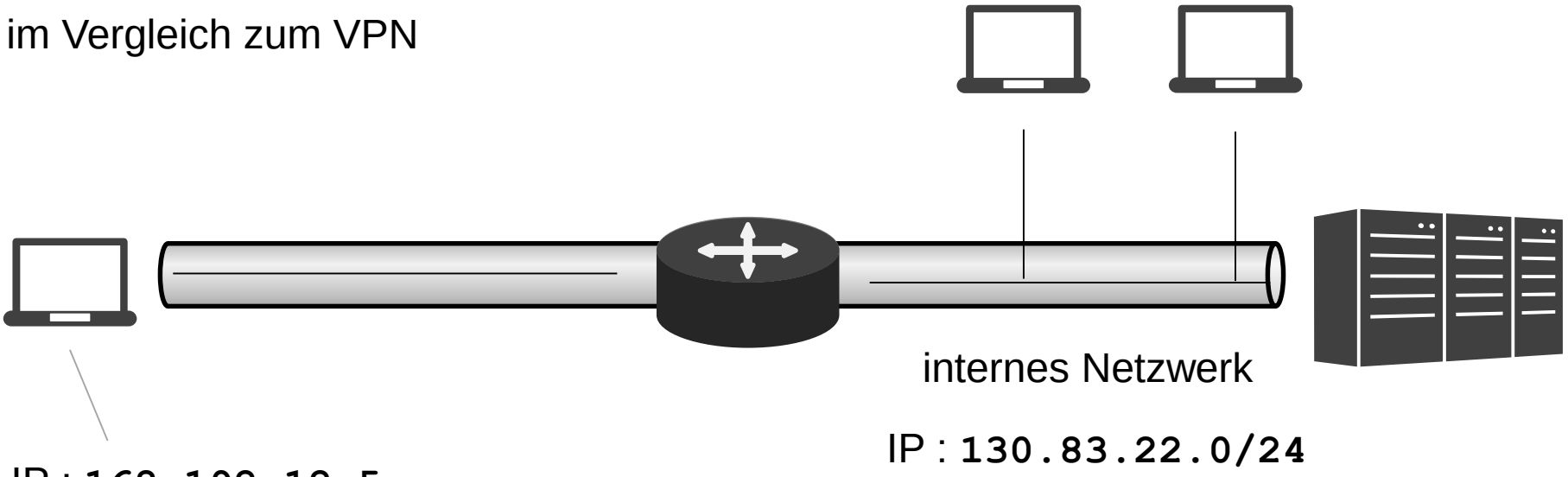
Sicherheit nur auf der Verbindung
bis zum internen Netzwerk



Beispiel: TU Darmstadt

Sichere Verbindung auf Applikationsebene

im Vergleich zum VPN



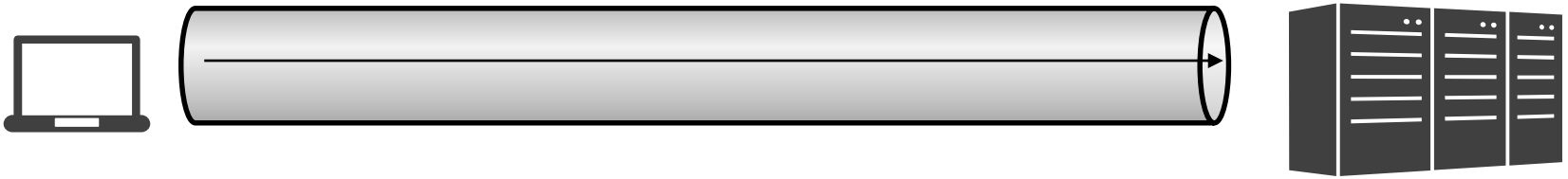
Rechner „bleibt außerhalb“ des internen Netzes

Vorteil: Ende-zu-Ende-Sicherheit

Nachteil: nur die Applikation gesichert

Anonymität (TOR)

Meta-Daten in sicheren Verbindung



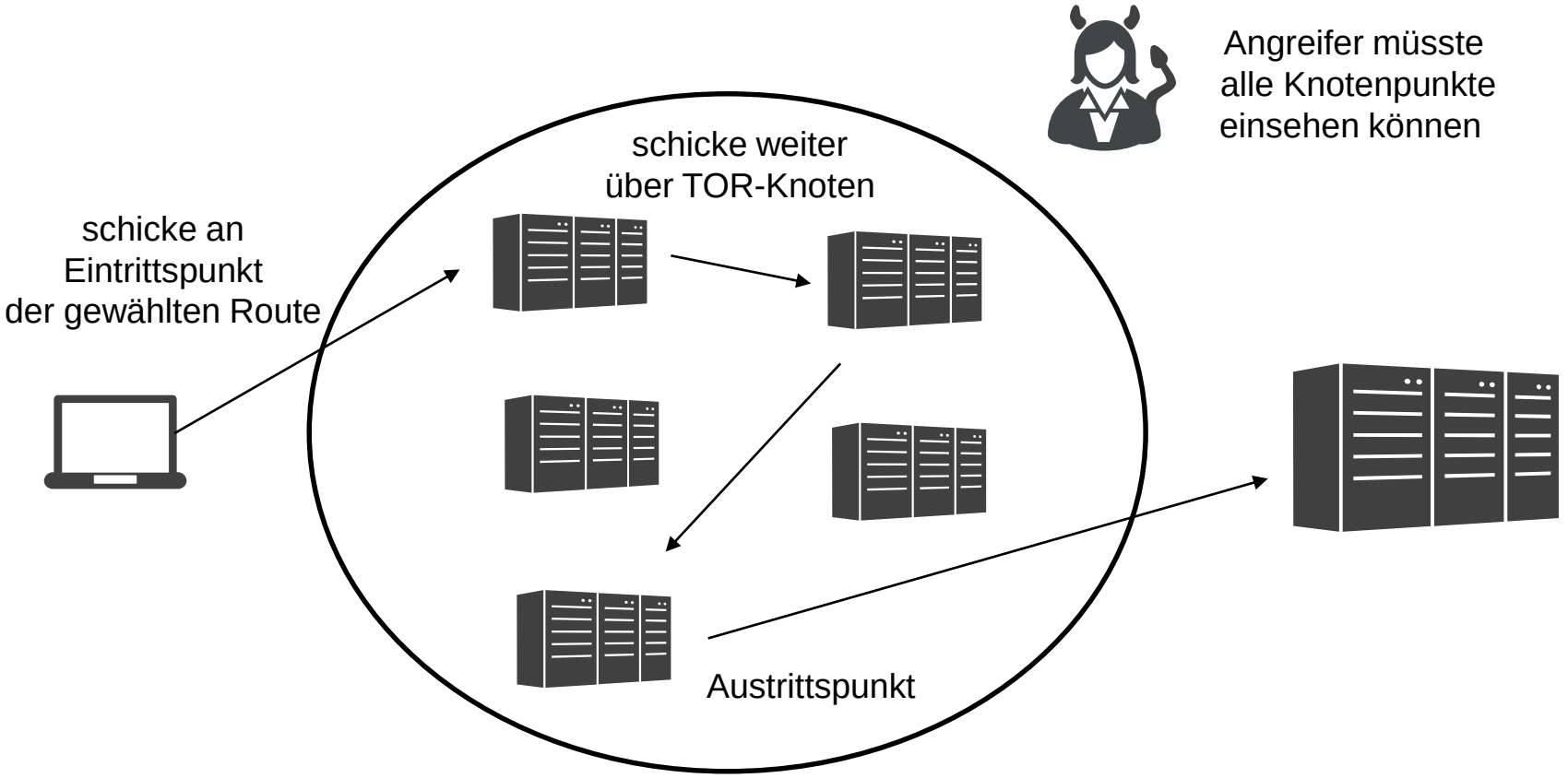
Angreifer kann Inhalt nicht bestimmen

sieht aber z.B. anhand der IP-Adressen,
wer miteinander kommuniziert

Onion-Routing via TOR

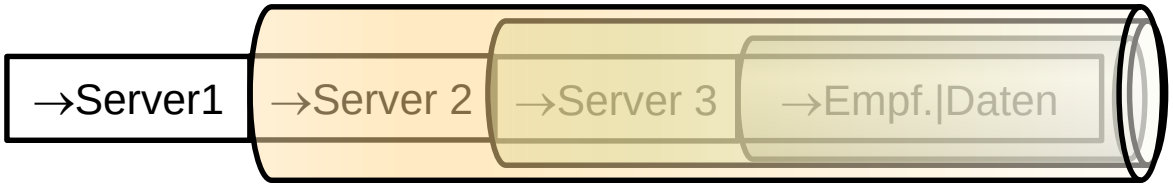
Ursprünglich von US-Militär entwickelt (2001)

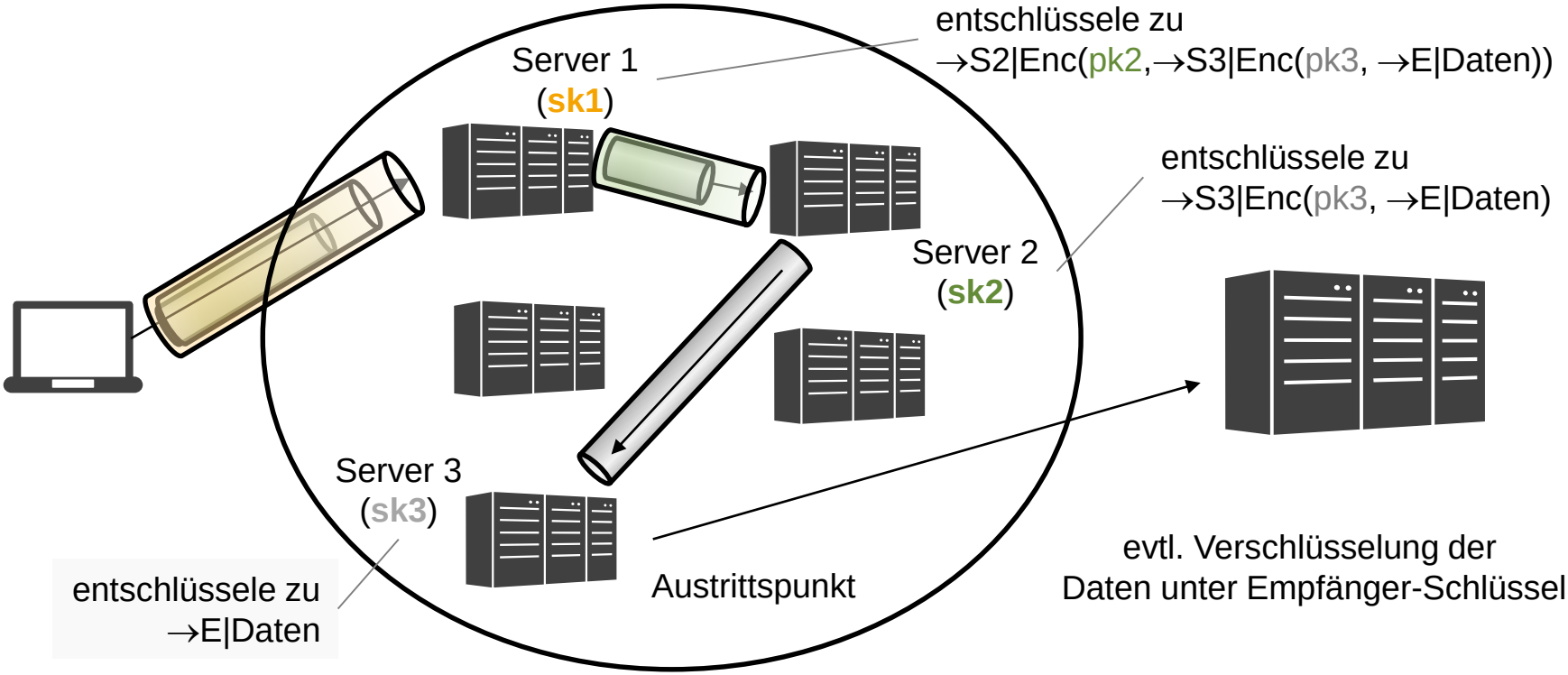
Quelle: Wikipedia



The Onion Routing

→S1|Enc(**pk1**, →S2|Enc(**pk2**, →S3|Enc(**pk3**, →Empfänger|Daten)))





Anonymität durch TOR?

TOR erschwert es, Datenströme zuzuordnen

bietet aber keine perfekte Anonymität:

Ein- und Ausgangsdaten korrelierbar,
sofern große Menge von Knotenpunkten
in Besitz eines Angreifers

Quelle: heise security (2015)

Erklären Sie den Unterschied zwischen Transportieren und Tunneln bei sicheren Verbindungen.

Wie funktioniert Onion-Verschlüsselung bei TOR?

Warum muss bei TOR der Sender die Route vorab wählen und überlässt die Wahl nicht den Knoten?

Was Sie gelernt haben sollten

Schichtenmodell

IP-Adressen, MACs, Ports, ARP, DHCP, DNS

Wireshark und nmap

DoS und DDoS-Angriffe

bekannte Vertreter von (D)DoS-Angriffen

Firewalls und Intrusion Prevention/Detection Systems

iptables und Snort

Sichere Verbindungen per TLS (SSH, IPSec)

Virtual Private Networks

TOR