

# IT Security

Ein System ist dann "sicher" wenn es sich so verhält wie man es erwartet.

[lukas.feiler@lukasfeiler.com](mailto:lukas.feiler@lukasfeiler.com)

<http://teaching.lukasfeiler.com>

# Grundwerte der IT-Sicherheit

- Vertraulichkeit
- Integrität
- Verfügbarkeit

Was ist ein (hohes) Risiko?

Das Produkt der Schadenshöhe und der Wahrscheinlichkeit des Schadenseintritts:

$$\text{Risiko} = \text{Schaden} * \text{Wahrscheinlichkeit}$$

Welche Risiken gibt es für IT-Systeme?

Physische Angriffe

Hardware-Fehler

- Datenverlust durch Platten-Crash

- Downtime durch Netzteil

Hack

- Datendiebstahl

- Daten-Löschung

- Daten-Fälschung

Denial of Service (DoS) & DDoS

Trojaner

Würmer & Viren

Versehentliche Daten-Löschung

Sniffing

Social Engineering

Phishing

**Welche Risiken gibt es für IT-Systeme?**

# Prinzipien im Bereich IT Security

- Least privilege
- Defense in depth
- Securing the weakest link
- Secure failure (Default Deny)
- Keep it simple
- Privacy (Need-To-Know)

## Für Workstations

- 1) Patches einspielen
- 2) Personal Firewall
- 3) Anti-Virus Software
- 4) Regelmäßige Backups auf externe Datenspeicher

## Für Server

- 1) Patches einspielen
- 2) Firewall
- 3) Vernünftige Konfiguration des Betriebssystems und der Dienste
- 4) Regelmäßige Backups auf externe Datenspeicher



# Intrusion Detection Systems (IDS)

- Host based (HIDS)
- Network IDS (NIDS)

## Honeypots

# Organisatorische Sicherheitsmaßnahmen

- Risk Assessment
- Security Policy
- Incident Response Plan, ...

# Risk Assessment

- 1) „Assets“ und ihren Wert identifizieren
- 2) Bedrohungen feststellen
- 3) Berechnung des Risikos

Assessment Tools: nessus, nmap, ...

# Security Policy

auch „Sicherheitskonzept“:

- was wird warum geschützt
- Verantwortlichkeiten
- allgemein gehalten (keine techn. Details)

z.B: Password Policy  
Backup Policy

# Incident Response Plan

- "Hope for the Best, Plan for the Worst"
- Wer ist wie zu informieren?
- Wer ist zuständig?

# Redundanz

- ein allgemeines Mittel zur Minderung des Risikos
- kein Single Point of Failure!

Murphy's law: "Everything that can go wrong, will go wrong"

# Gegenmaßnahmen gegen spezifische Risiken

Gegen welche Risiken gehe ich vor?

Um wie viel verringert sich die Eintrittswahrscheinlichkeit?

Rechtfertigt der Nutzen die Kosten?

## Risiko

Platten-Crash, Daten-Löschung aus Versehen od. durch Hacker

## Gegenmaßnahme

Backup:

Backup-Strategien (z.B inkrementell)

Windows-Tools: ntbackup

Linux-Tools: dump

Automatisiertes inkrementelles Backup:

<http://dumpnet.sourceforge.net>

nur gegen Platten-Crash:

RAID (Redundant Array of Independent Disks)



Risiko:

Zugangspasswort wird „gecrackt“ (erraten, brute force, dictionary attack, od. auf sonstigem Wege)

Gegenmaßnahme

Minimal 6-stelliges Passwort (besser: 8 od. 10 Stellen)  
bestehend aus Zahlen, Buchstaben und Sonderzeichen

Was ist ein „gutes“ Passwort?

Risiko:

Ausnutzung eines Bugs in einer PHP-Applikation durch  
z.B. „SQL-Injection“

Gegenmaßnahme

Den Bug beheben!

nicht zielführend:

eine Firewall einrichten

# Ausblick: Sicherheit in dezentralen Netzen?

[http://www.lukasfeiler.com/Sicherheitsrisiken\\_im\\_Internet.pdf](http://www.lukasfeiler.com/Sicherheitsrisiken_im_Internet.pdf)

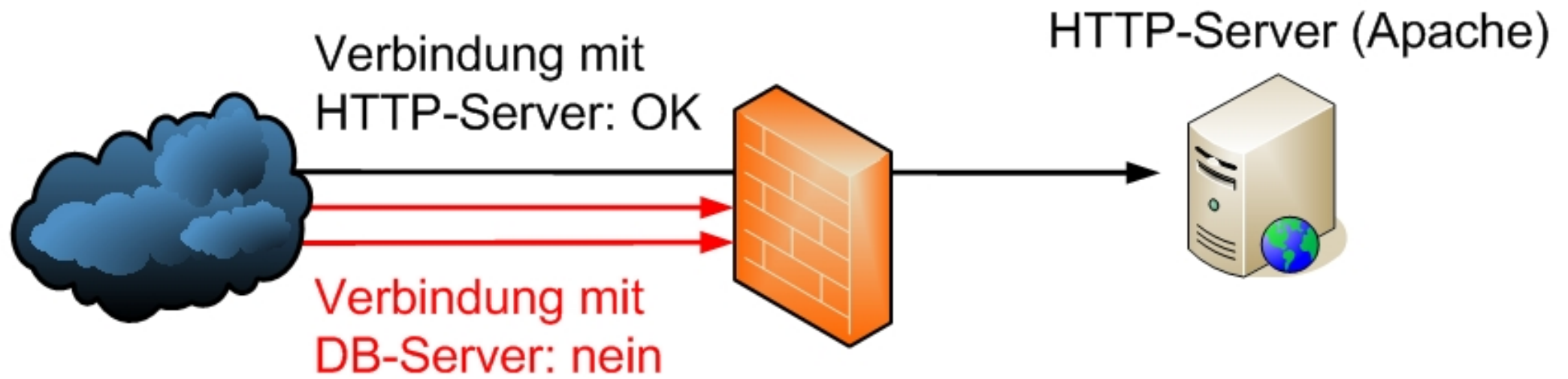
# Komplexe Netzwerkkomponenten

Können aus Soft –und Hardware bestehen:

- Firewall
- Proxy

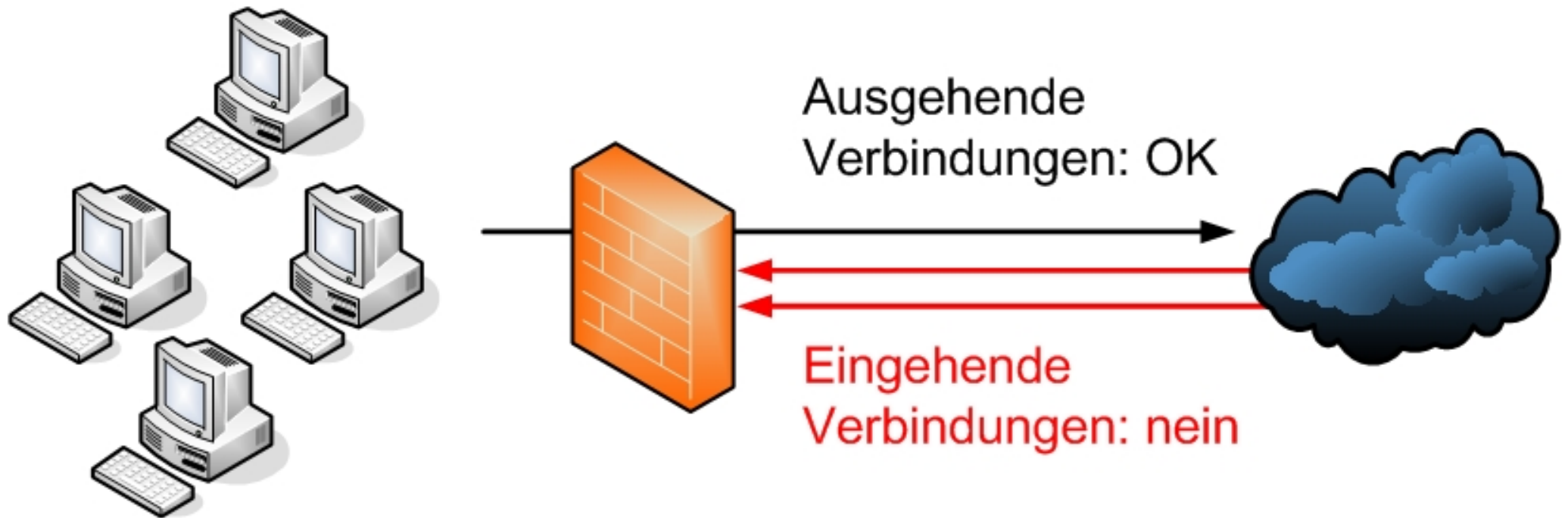
# Firewalls

Schutz eines od. mehrerer Rechner vor unbefugtem Zugriff



**Firewall schützt Server: TCP Connection Requests NUR an Port 80!**

## Workstations



**Firewall schützt Clients: keine Connection Requests hinein!**

Was eine Firewall kann...

- Durchsetzung der Security Policy
- Protokollierung

Was eine Firewall nicht kann...

- vor Angriffen von innerhalb der Firewall schützen
- vor Sicherheitslücken in einer erlaubten Anwendung schützen (z.B. Bug in Apache od. fehlerhaftes PHP Skript!)



Eingehend (ingress filtering):

TCP:

Port 80 (HTTP): Ja

Port 25 (SMTP): Ja, aber nur die IP 33.124.123.87

alle andern Ports: Nein

UDP: Nein

ICMP: Ja

Ausgehend (egress filtering):

TCP: Nein

UDP: Nein

ICMP: Nein

**Beispiel-Konfiguration um Web-Server „abzusichern“**

Eingehend:

TCP: Nein

UDP: Nein

ICMP: Nein

Ausgehend:

TCP: Ja

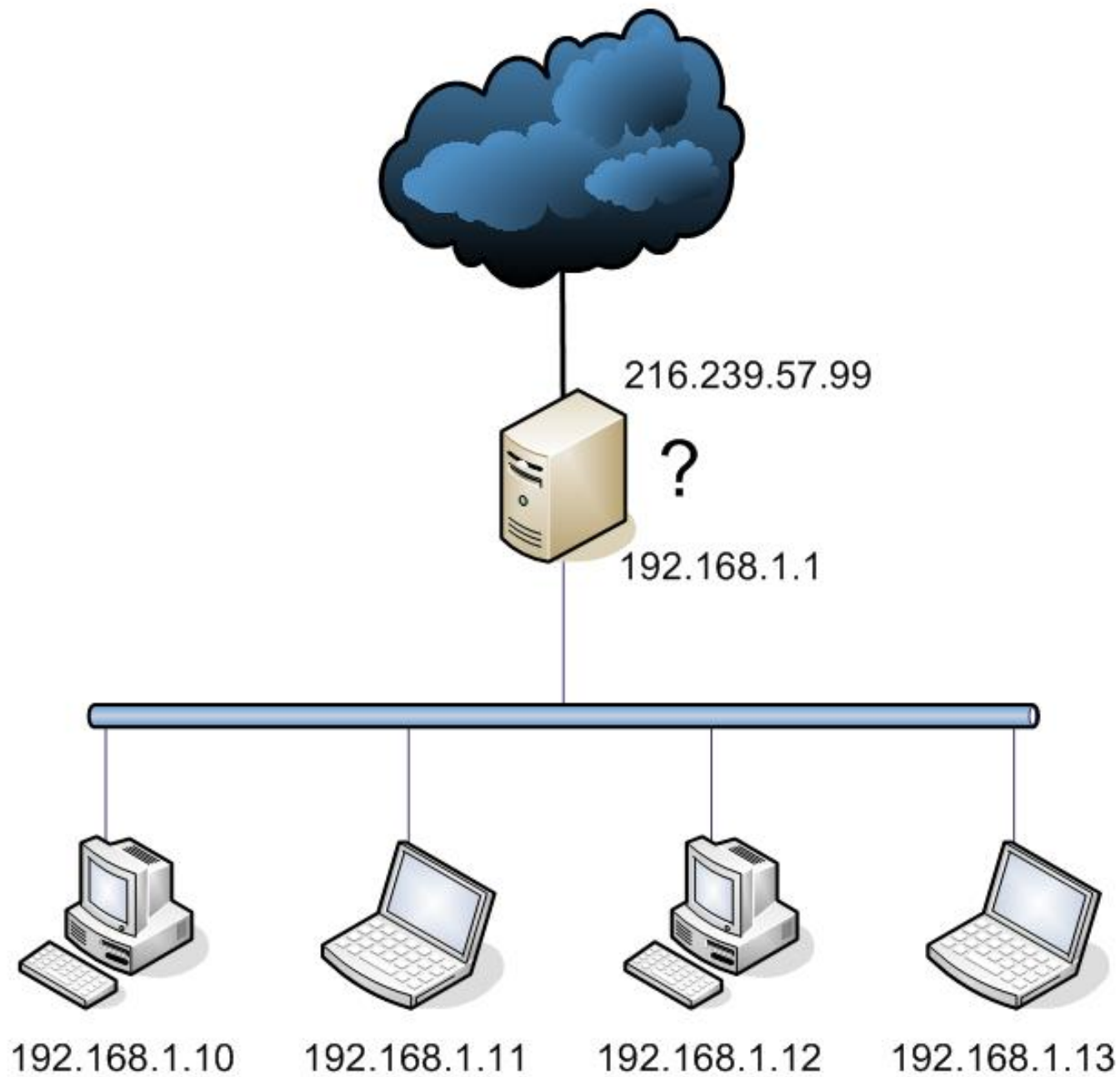
UDP: Ja

ICMP: Ja

**Beispiel-Konfiguration um Clients „abzusichern“**

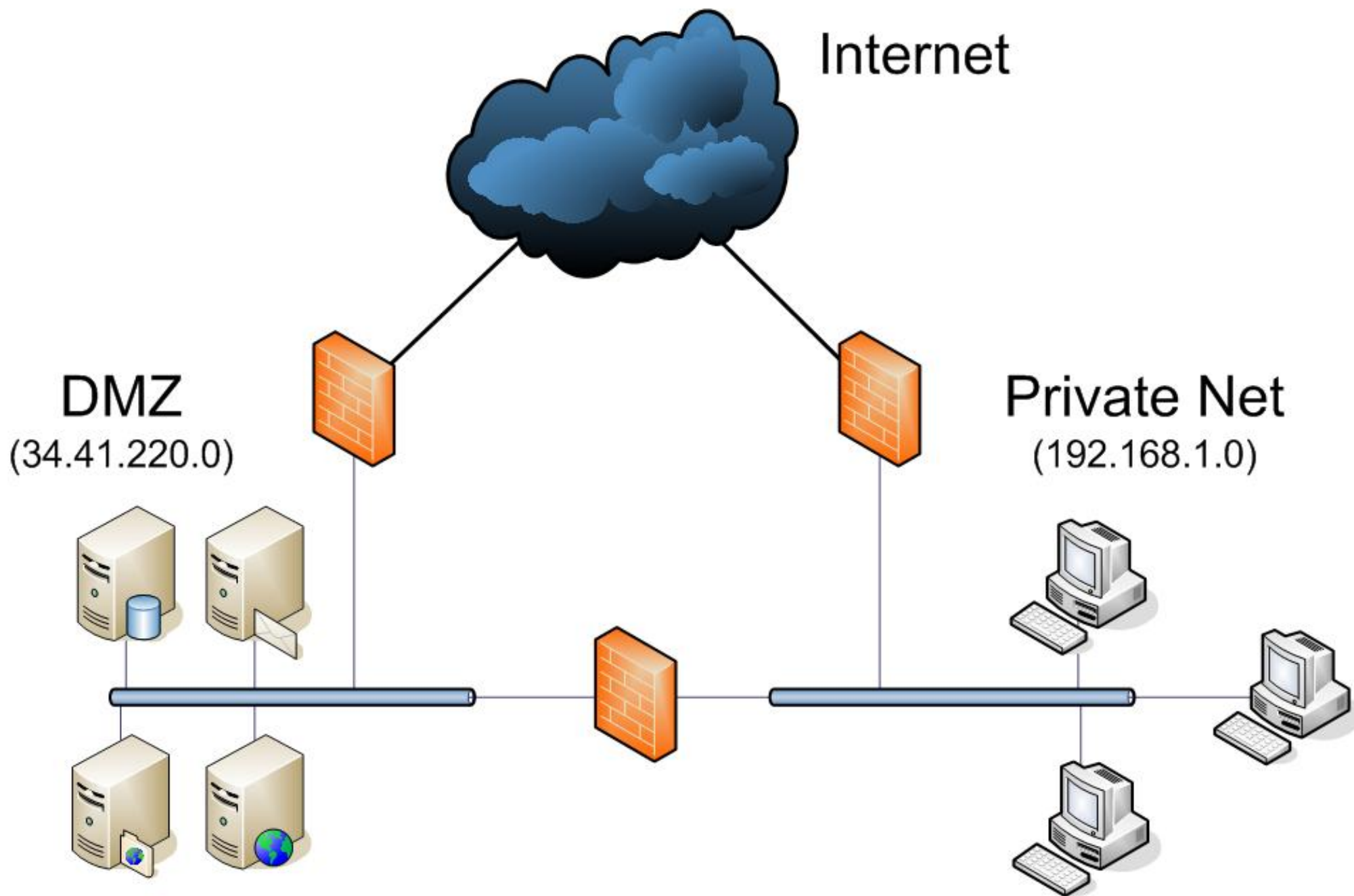
# Firewalls: NAT – Network Address Translation

- IPv4 kennt nur ca. 4 Mrd IP-Adressen



**(S)NAT: Firewall ändert Source-IP bei ausgehenden & Destination-IP bei eingehenden Paketen**

DMZ – Demilitarized Zone

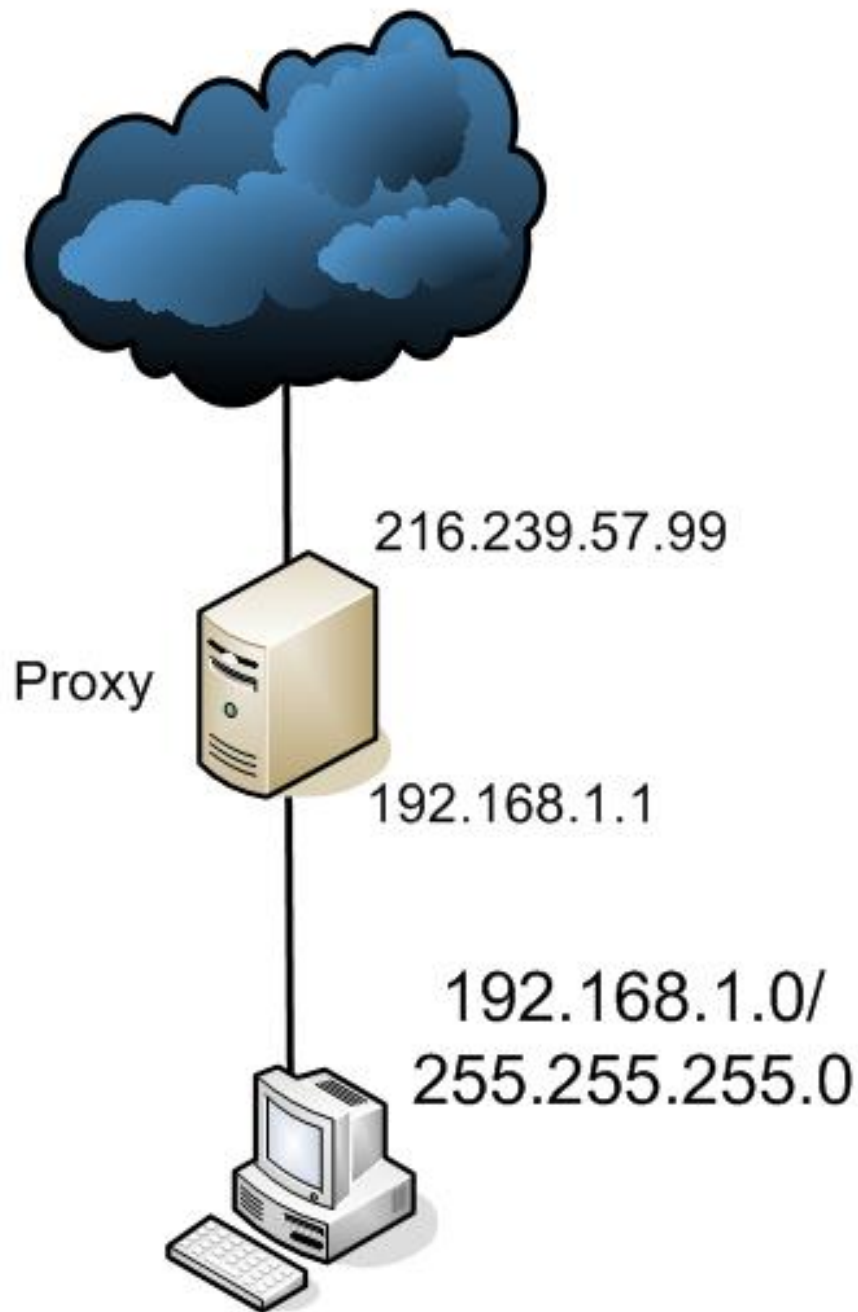


**Server in der DMZ sind durch Firewalls vor internen & externen Angreifern geschützt!**

Proxy – Eine „Stellvertretung“ für Clients

- Aus Sicht des Clients besteht eine direkte Verbindung mit dem Server im Internet.

- Aus Sicht des Servers besteht die Verbindung mit 98.122.42.87.



**Ein Proxy („Stellvertreter“) im Einsatz**



## Vorteile

- Mehr Sicherheit, da keine direkte Verbindung zwischen Client & Server
- Proxy versteht HTTP (Firewall idR nicht!); besseres Filtering und Logging möglich
- Caching: Zwischenspeicherung am Proxy zwecks schnellerer Verfügbarkeit

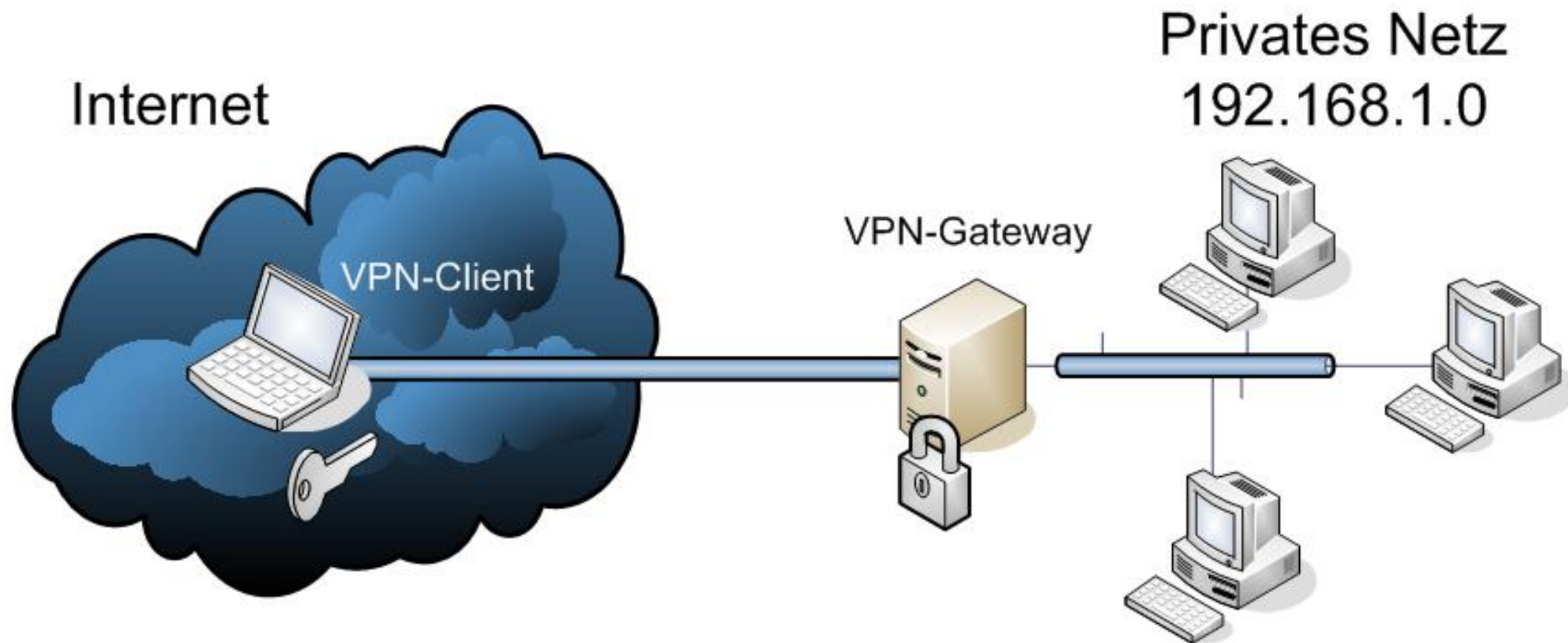
## Nachteile

- idR ist für jeden Dienst (HTTP, FTP, SMTP, ...) ein eigener Proxy zu konfigurieren
- höhere Komplexität

# VPN – Virtual Private Network

Das Problem: z.B. Außendienst-Mitarbeiter

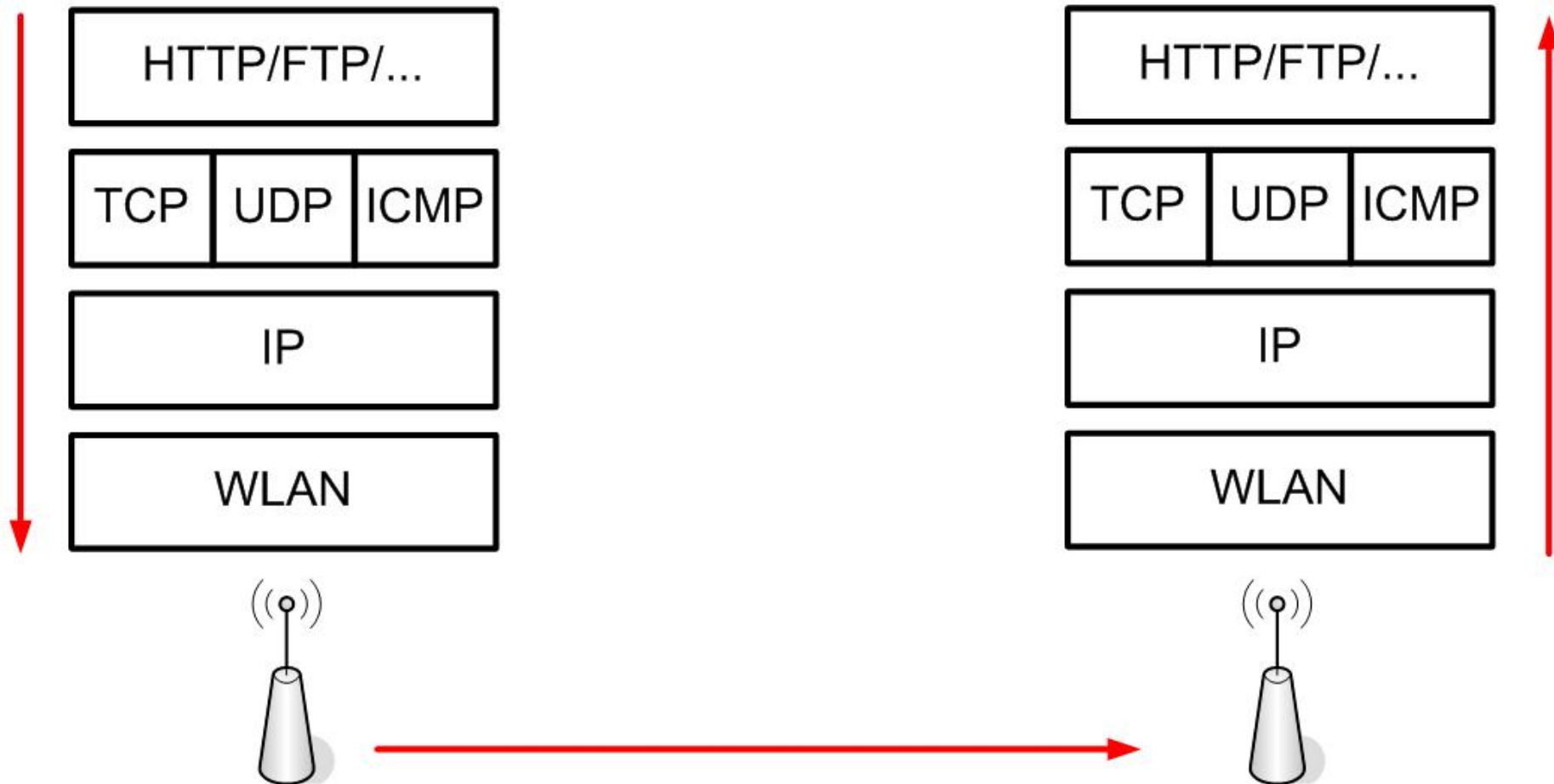
Die Lösung: durch Authentifizierung & Verschlüsselung



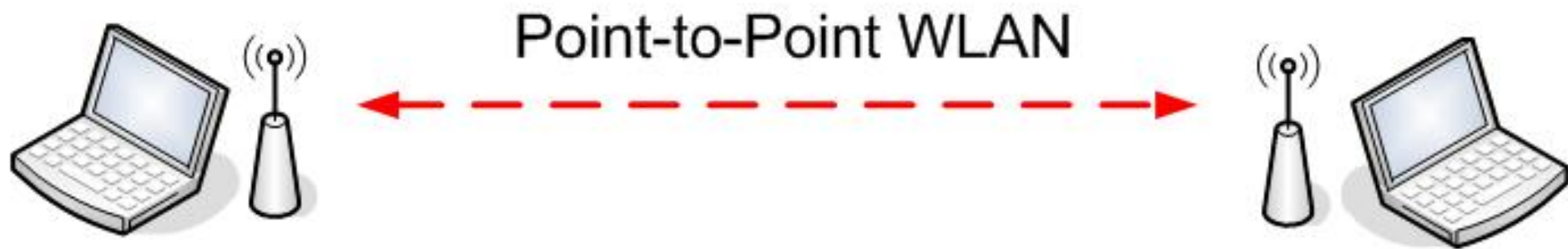
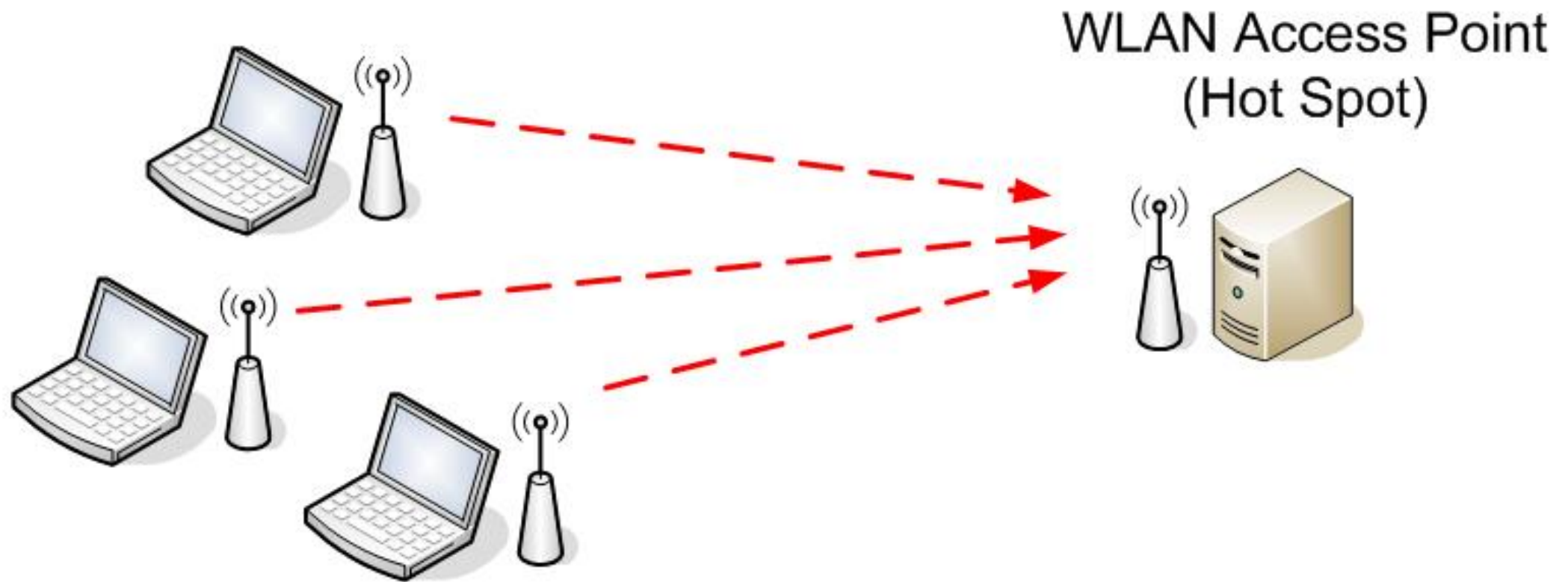
idR Verschlüsselung auf IP-Ebene: IPSec

# WLAN – Wireless Local Area Network

auch „Wi-Fi“



**WLAN anstatt Ethernet**



## 2 Einsatzmöglichkeiten von WLAN

IEEE 802.11b

11 MBit/s

bis zu 305m im Freien

IEEE 802.11g

54 MBit/s

Verschlüsselung

- WEP (Wired Equivalent Privacy): schwach
- IPSec: komplex
- WPA2 (Wi-Fi Protected Access 2)