

# Virtualisierung

Montag, 18. September 2023 13:01

## Virtualisierung von Betriebssystemen

mehrere Instanzen eines BS teilen sich  
eine starke Hardware

Vorteile:

- das Testen von neuen BS  
/ Testen neue Applikationen auf BS
- Schulung: Environments, die man einfach wieder löschen kann
- Virtualisierung Konzept 60er Jahre:  
mehrere Benutzerkonten
  - ↳ später BS sowieso Mehrbenutzerfähig
- Virtualisierung „Wiedererfindung“ ~2010
  - neue Anwendungen / BS testen
  - HW-Resourcen besser ausnutzen
    - ↳ Domain Controller zw. 8 und 9 (im Unternehmen)  
viele Anmeldungen weil Büroarbeiter eintödeln.
    - Anschließend Mail Server, File Server, Print Server stark ausgelastet.
    - ↳ Virtualisierung erlaubt Rechenleistung d. Hosts bedarf zuweisen (DC mehr zw. 8 und 9, ...)

bedarf zuweisen (DC mehr zw. 8 und 7, ...)

## ↳ SKALIERUNG

→ Snapshots erstellen und wiederherstellen

↳ nächtlich immer zurücksetzen (Unternehmen)

→ Cloud Hosting Server "mieten"

Host: Gastgeber, auf welchen die BSe laufen

Guest: Das virtuellere Betriebssystem läuft am Host.

## HYPERVISOR (VMM)

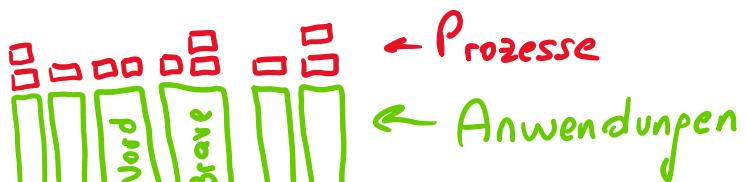
Ein Manager, welcher  
Instanzen steuert und verwaltet.

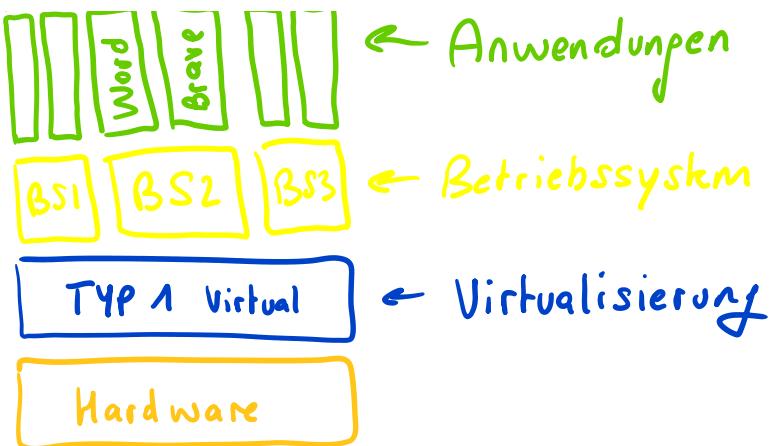
→ Hardwarezuweisung, RAM, Speicher

## Typ 1 Virtualisierung:

auch Bare-Metall Visualisation genannt.

z.B.: VMWare ESX, Citrix Xen, Hyper-V

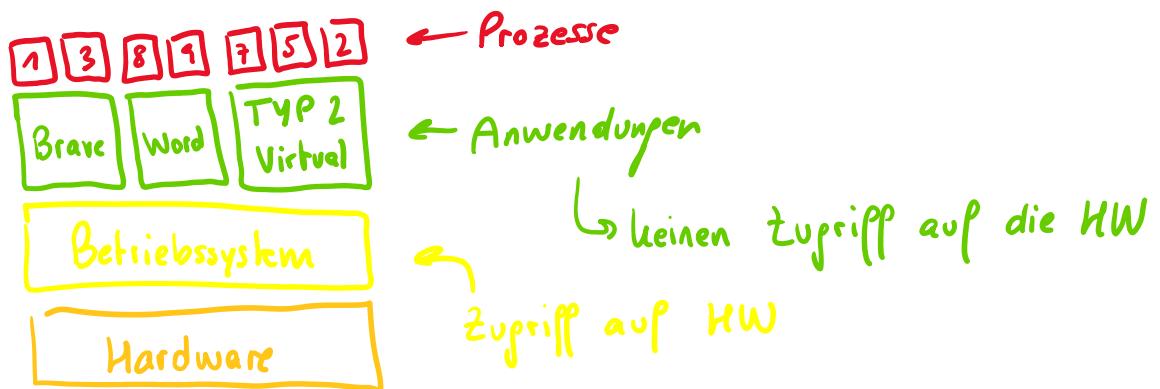




Virtualisierer muss via Betriebssystem installiert werden. Deswegen kann bei dessen Installation nichts anderes installiert werden, da dies erst später auf den virtuellen Maschinen passiert.

## Typ 2 Virtualisierung

Virtualisierer ist selbst nur ein Anwendungsprogramm  
z.B.: VirtualBox, VMware Player



Dem virtualisierten BS muss vorgepackelt werden, das es als einziger Zugriff auf die HW hat.

das es als einziger Zugriff auf die HW hat.  
Das kann die Anwendung allerdings nicht, weil  
sie selbst auch verwaltet wird.

---

Kernel / System mode: bei PC nur Betriebssystem  
und Interrupt Service Routine

User mode: Anwendungen  
(ruft mithilfe eines System calls  
die Betriebssystemfunktionalität auf)  
↳ z.B.: SSD lesen  
→ Kontrolle kurzfristig an BS übergeben

## Container - Virtualisierung

Docker Container haben keinen eigenen Kern.  
Sie nutzen den Kern des Hosts.

## Para - Virtualisierung

zusätzliche Schnittstellen schicht :

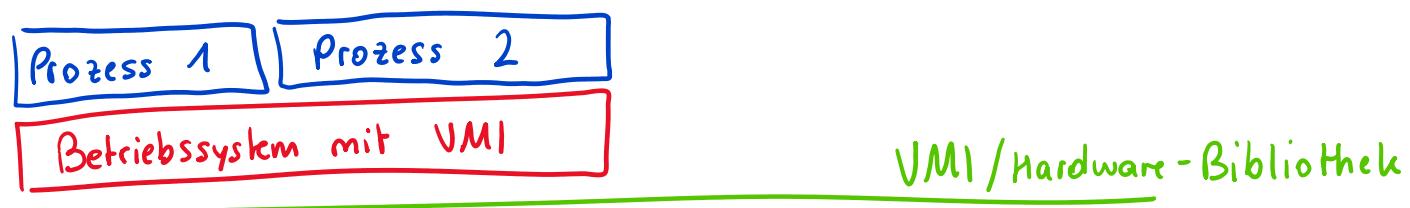
Wenn Guest UW direkt aufruft, ruft er eigentlich  
eine „API“ für Betriebssysteme auf.

## Funktionsbibliothek (andere Seite d. API)

FB werden an die Schnittstelle gebunden.

Daten werden entweder an die HW übergeben  
(von Schnittstelle) oder an die virtualisierte  
HW / den Hypervisor.

VMI = Virtual Machine  
Interface



Betriebssystem mit VMI

VMI / Hardware-Bibliothek

↓ Befehle werden von  
HW ausgeführt



Prozess 1

Prozess 2

Betriebssystem mit VMI

VMI / Hardware-Bibliothek

↓ Hypervisor-Aufruf



## Ausfallsicherheit

- ↳ zentrale Speicherlösung
- ↳ am Host liegen nur VMs (kein Speichersystem)

## Speichersystem

↳ Network Attached Storage (NAS)

→ OpenMediaVoll, XigmaNas (SW-RAID)

Fileshare, RAID (Redundanz)

→ im echten Betrieb auf unterschiedlichen physischen Platten

NAT-Boxen (HW-RAIDs)

→ Synology, PiNet, ...

→ NAS ist eigener PC mit eigenem BS

↳ BS nimmt Speicherverwaltung

↳ managed Filesharing

→ NAS ist ein Netzwerkclient

↳ Trafik belastet das LAN

↳ NAS hat IP-Adresse

↳ Daten := lauter IP-Pakete verpackt

- ↪ NAS hat IP-Adresse
  - ↪ Daten in lauter IP-Pakete verpackt
    - ↪ Fragmentierung d. Daten
    - ↪ viel Overhead
  - einfach integrierbar
  - eigene Berechtigungsverwaltung
- 
- ```

graph LR
    NAS[NAS] --- Switch[Switch]
    Switch --- C1[C1]
    Switch --- C2[C2]
  
```
- Protokolle: Server Message Blocks (SMB)  
Network File System (NFS)  
Common Internet File System (CIFS) (OBSOLETE)

## Daten Sichern

- Belastet das LAN
- anderes NAS, Magnetband
- Small Office Home Office (SOHO)

↪ Storage Area Network (SAN)

↪ LAN nicht überlastet

↪ teuer

↪ 1 . . . verschiedene Locations sein

→ teuer

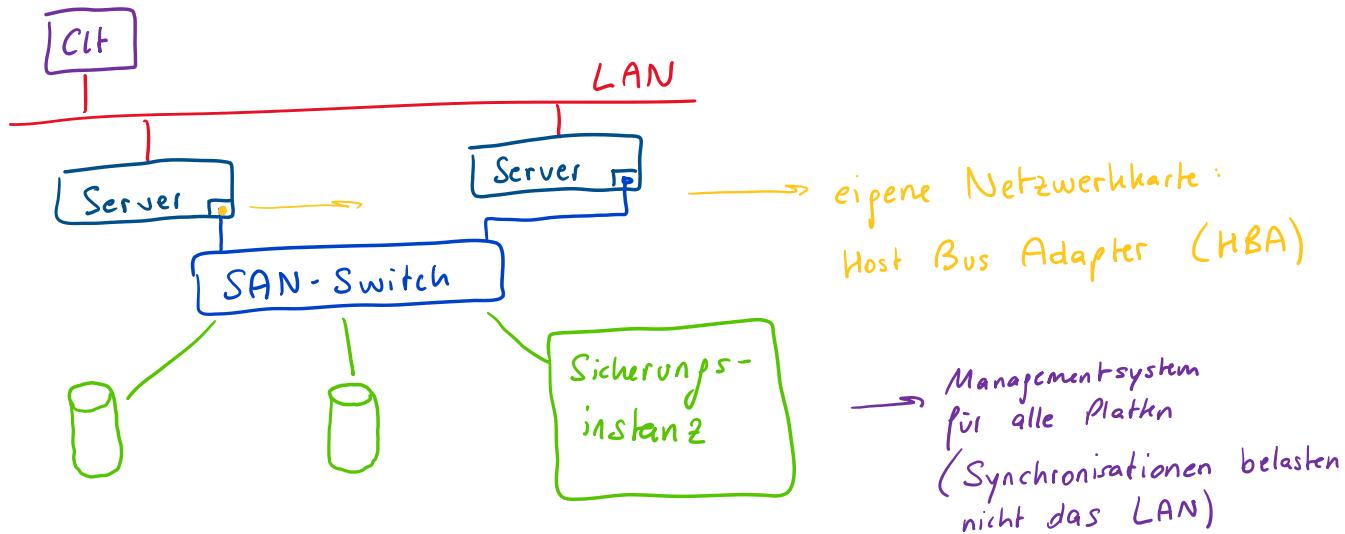
↳ kann in verschiedenen Locations sein

↳ eigenes Netzwerk mit Speichermedien

↳ Verwaltung vom aufrufenden Gerät (Management dazwischen)

→ SAN-Switches, Netzwerktopologie

→ von einem Gerät auf Sicherungsstation



→ Protokolle

↳ Fibre Channel (FC): für LWL und Kupferleiter

→ am besten: **SINGLE VENDOR** Lösungen  
(alles vom gleichen Hersteller)

→ HBA: transparent für Server  
Server "plaut" Platten sind DAS

↳ Direct Attached Storage (DAS)

↳ Festplatte im PC

# Backup

Montag, 9. Oktober 2023 13:28

## BACKUP

→ keine Verpflichtung für Datensicherung

→ Unternehmen:

→ Buchhaltung 7 Jahre Pflicht

→ IT-Zertifizierungen (ISO-Normen)

↳ 9000 (Qualitätsmanagement)

↳ 14000 (Umweltmanagement)

↳ 27000 (IT-Sicherheit)

→ Datensicherheitsschranke (safe)

## SICHERUNGSSTRATEGIEN

↳ muss an alle Mitarbeiter kommuniziert werden

**WIE?**

- Wie erfolgt die Sicherung von Nutzdaten?

↳ vollständig / komplett

Kopie des Mediums  
keine Flexibilität bzgl. Änderungen  
hoher Speicherbedarf  
simple Handhabung

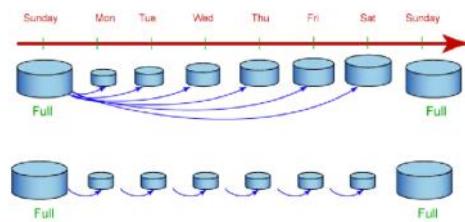
täglich alle Daten sichern

Aufwand steigt

↳ differentiell

regelmäßige Komplettsicherung  
+ Teilsicherungen aller Änderungen  
zur letzten Komplettsicherung

tägliche Teilsicherung;  
wöchentlich komplett



↳ inkrementell

regelmäßige Komplettsicherung  
+ Teilsicherungen aller Änderungen  
zur letzten Teilsicherung

tägliche Teilsicherung;  
wöchentlich komplett

Speicherbedarf sinkt

**1:1 - Plattensicherung**

hierbei wird das OS mitgesichert

## WER?

- Wer ist verantwortlich?

- Wer kümmert sich um die Datenträger ...

(z.B.: Helpdesk, Funktion, ...)

- Wer weiß über Strategien Bescheid?

↳ alle Mitarbeiter müssen wissen, was, wann gesichert wird

## WANN?

- Wann wird die Sicherung durchgeführt?

↳ meistens täglich um eine bestimmte Uhrzeit



↳ nachts, damit wenige aktive Nutzer

↳ ERP - Systeme / Spitäler mit nächtlichem Betrieb

↳ oft Kalkulation nachts, deswegen Backup vorher / nachher

## WO?

- Wo bewahre ich die Sicherung auf?

→ eigener Raum? / eigenes Gebäude?

→ Datensicherheitsschrank?

→ physisch geschützt vor Feuer / Wasser / ...

## WIE LANGE?

- Wie lange werden die Sicherungen aufgehoben?

→ Gesetz / Finanzamt gibt teilweise Zeitraum vor

→ muss man alles oder nur bestimmte Dokumente aufbewahren?

## WELCHE DATEN

- Welche Datentypen sollen gesichert werden?

- kein OS
- keine Programme
- nur Nutzdaten
- Auswahl muss mit Mitarbeiter kommuniziert werden
- Mitarbeiter müssen wissen: Wo? WELCHE DATEN?
- lokale Workstation-Files eher weniger
- Einschränkung auf Datentypen?

## WELCHES MEDIUM?

- Worauf wird gesichert?

- Datenband (schnelles Schreiben)
- Magnetband
- SSD
- :

## VERSCHLÜSSELUNG

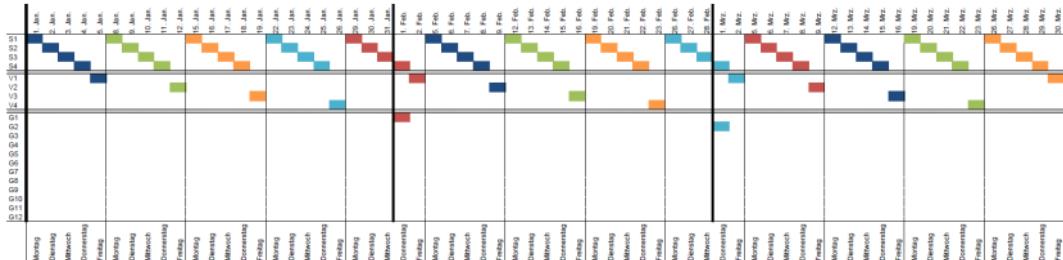
- notwendig?
- welche Verschlüsselung?

## WIEDERHERSTELLUNG?

- regelmäßige Testung der Datei-Wiederherstellung
- Testung der Funktionalität dieser Dateien
- ca. 1x pro Jahr

## GENERATIONENPRINZIP

- Speicherplatz strategisch verringern



S... Sohn / Kind    V... Vater / Eltern    G... Großvater / Großeltern

In logarithmischen Abständen erstellt man neue Generationen bis zum gesamten Jahr. Bei jeder Sicherung in eine höhere Generation werden alle Daten der darunterliegenden Generation zu einer Vollsicherung zusammengefasst.

Um 7 Jahre Daten zu speichern, benötigt man nur 29 Medien.

- 7 Jahresmedien,
- 12 Monatsmedien des aktuellen Jahres
- 4 Wochenmedien des aktuellen Monats
- 6 Tagesmedien der aktuellen Woche

## Linear Tape Open

Montag, 6. November 2023 13:19

Linear Tape Open (LTO Ultrium) → Standard für Sicherungsmedien

Band wird von Bandstation durch Chip identifiziert

### Generationen

Laufwerk Gen 9: kann 7, 8, 9 Bänder lesen  
und 8, 9 Bänder schreiben

2 vorherige Gen lesen  
1 vorherige Gen schreiben

### Verschlüsselungsmechanismen

WORM → Write Once Read Many

## Fernwartung für Systeme ohne Benutzer (Steuerungsanlage)

↳ Problembehandlung

↳ laufende Parameter erfassen

↳ remote Administrieren

↳ schneller, bequemer (nicht hingehen müssen → Anfahrtskosten billiger)

↳ Serielle Schnittstelle (USART, ...)

über Modem (modulieren / demodulieren),

Telefonleitung oder Internet

↓  
Früher analog; heute über VoIP

↳ Predictive Maintenance

→ wenn z.B.: Temperatur immer wärmer wird

## Fernwartung für benutzergesteuerte Endgeräte

→ nur sehen (Bildschirmübertragung)

→ Kontrolle (Team Viewer, ...)

↳ aktive Fernwartung

↳ passive Fernwartung

Warum braucht jeder einen eigenen Benutzeraccount?

→ eigene Dateienordner

→ Rechte / Isolation

↳ Datenschutz bei Fernwartung:  
da Dateien / Mails sehen können  
/ Personalverteilung: Gehälter sehen

↓ Richtlinien

- Die Person, welche Hilfe benötigt, muss wissen,  
dass Bildschirm geteilt wird  
(Popup mit Bestätigung & Zustimmung)
- Ständige Anzeige (Pop-Up), dass Fernwartung  
aktiv
- Aufzeichnung der Fernwartung  
(Zeitdauer protokollieren bis Aufnahme)  
↳ da Fernwarter Zugriff auf Benutzerkonto  
(Schutz)
- Betriebsvereinbarung: Initialzustimmungsrichtlinien  
(alles rechtlich geklärt; nicht einfach „drauf los“)
- Konfiguration der Fernwartung darf nicht  
verändert werden
- Sitzung muss protokolliert werden

Fernwartung im LAN vs WAN

## Fernwartung im LAN vs WAN

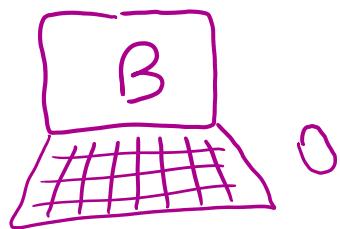
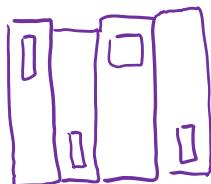
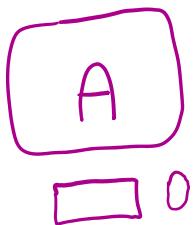
z.B.: Citrix-Server mit Server-Anwendung  
& Thin-Client (gesamte Rechenleistung am Server)

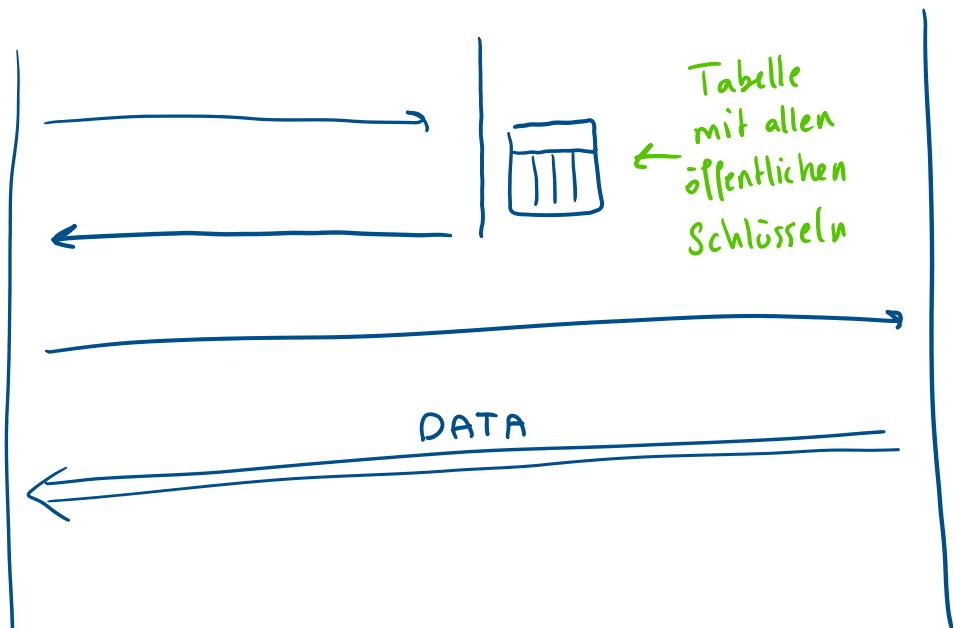
↳ FW einfacher, da Sitzung mit Supportmitarbeiter gezeigt  
werden kann

→ Unternehmenspolitische Entscheidungen

Beispiele:

Remote Desktop (RDP) mit Remote Desktop Protocol (RDP)  
Citrix mit Independent Computer Architecture (ICA)  
VNC mit Remote Framebuffer (Protokoll)





# VPN

Montag, 15. Januar 2024 13:42

VPN

Virtual Privat Network

Verwendung bestehendes Netzwerkes (WAN)

↳ deswegen virtuell

→ reine Softwarelösung (VPN-Gateway = HW)

→ garantiert Authentizität (Nutzer identifiziert)  
/ liefert Vertraulichkeit

Integrität (man weiß, wer dabei ist)

site to site

↳ 2 oder mehrere Standorte verbinden

↳ jede Seite braucht VPN-Gateway

↳ 1 Site = 1 LAN (größeres Netzwerk; Unternehmen)

end to site

## end to site

- ↳ Verbindung eines Clients zum großen Netzwerk
- ↳ zB Home-Office (PC zuhause ins FirmennW)
- ↳ Mitarbeiter erstellt TUNNEL zu Unternehmens-LAN
- ↳ Client braucht **VPN-Client**

## end to end

- ↳ 2 Rechner mittels TUNNEL verbunden
- ↳ 2 **VPN-Clients**

## TUNNEL

ein weiteres Paket um das Paket runderum  
Router im WAN wissen den genauen Adressaten  
nicht, sondern nur den Zielrouter, welcher das  
äußere Paket entpackt.

**äußere Paket entpacken.**

→ ein Protokoll in einem anderen verstecken.

RFC 2003

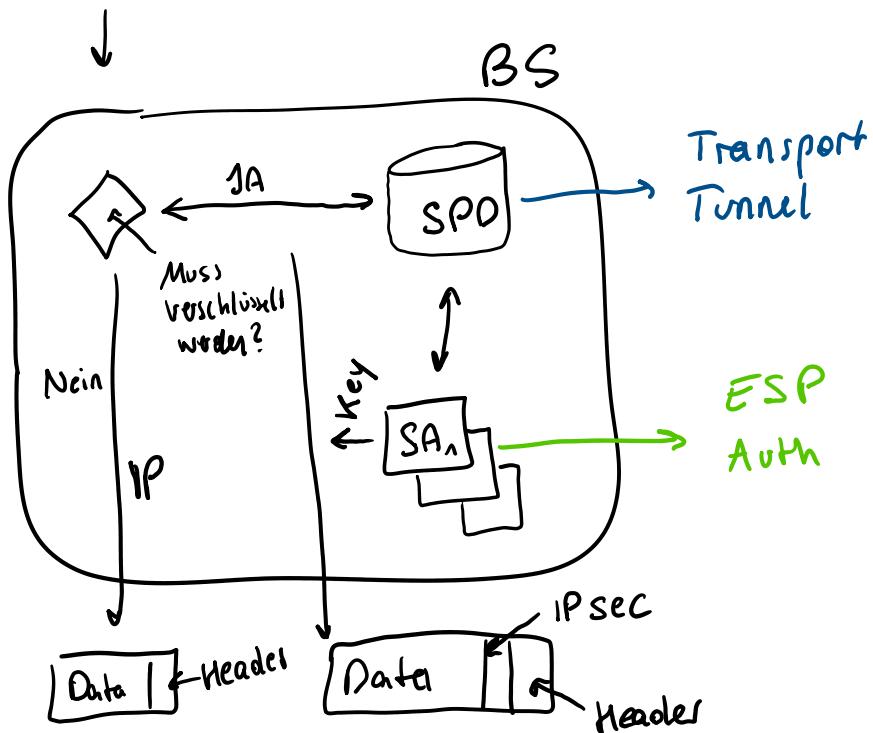
Zusätzliche Informationen im Header (Outer IP Header)

- Ursprüngliches Paket muss kleiner sein
- Fragmentierung kann helfen, um Paket kleiner zu machen (bei ersten Fragment Timer -> wenn TimeOut alle Fragmente bisher weg)

Tunnel MTP Discovery

→ ursprünglich für IPv6

Daten



→ Transport-Modus

↳ Kommunikations- & Verschlüsselungsendpunkte  
sind gleich (end to end)

→ Tunnel-Modus

↳ Teil des Weges verschlüsselt (site to site / site to end)

↳ bei Modi können jeweils mit Authentication  
header oder mit Security Payload betrieben werden

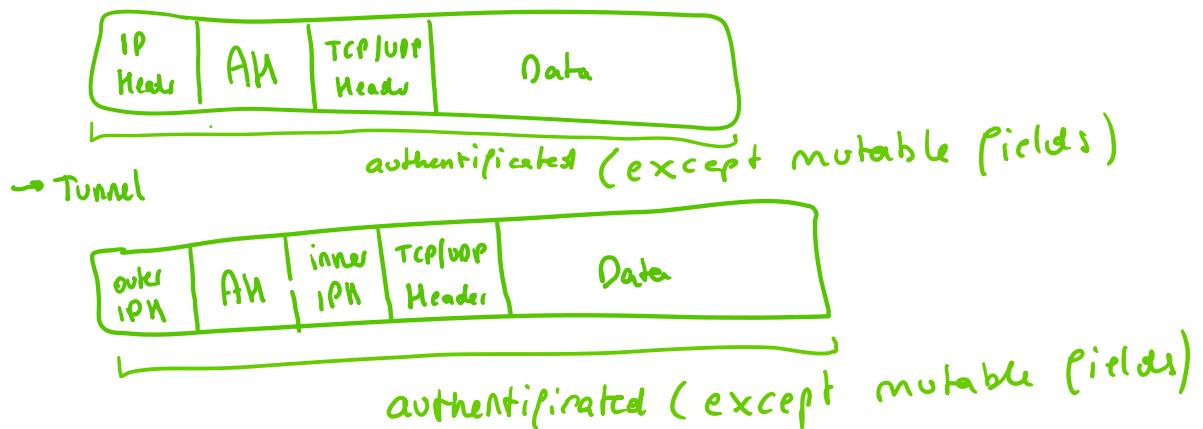
= 11 ähnliche Varianten

Header oder mit security

= 4 mögliche Varianten

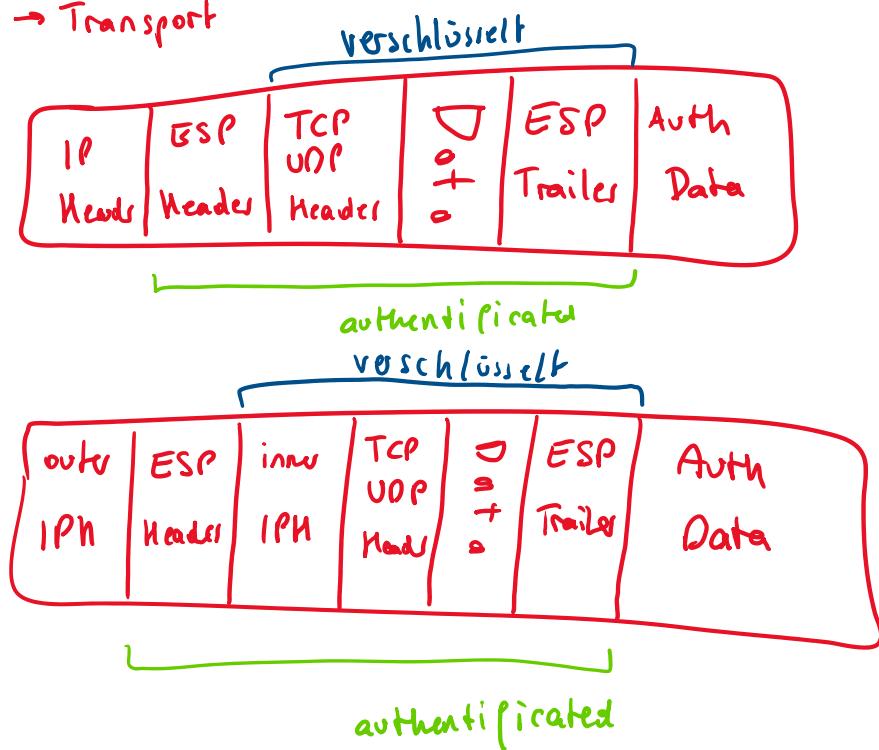
→ Authentification:

→ Transport



→ Encryption Security Payload

→ Transport



→ RFC

2401

→ RFC

2402

→ Auth Headers

→ RFC 2406 → ESP

→ RFC 2408 → Protocol automated Schlüsselaustausch  
(sicher) → ISAKMP

# SSL / TLS

Montag, 4. März 2024 13:18

Secure Sockets Layer / Transport Layer Security

Andere Möglichkeit für Verschlüsselung

Auch ein VPN

SSL verschlüsselt zwischen Anwendungen

SSL geht nur im Browser, dafür kein Konfigurationsaufwand

Key muss vorher ausgetauscht werden (Key Management Protokoll)

Flexibel, wo man ist, da Anwendungen verschlüsselt werden und nicht Geräte

# Firewall

Montag, 11. März 2024 13:08

## Ausbreitung von Bedrohungen verhindern

technische Ebene:

- Policy wird durch Regeln definiert
- einfache Sprachen für Regeln
  - ↳ Cisco IOS ACL

- Regeln können von Kontextbedingungen abhängen

↳ zustandslos: statisch / Kontext egal

↳ behaftet: dynamisch / z.B.: vorheriger Verkehr entscheidend