Inhaltsverzeichnis

1. [DNS 4](#_Toc96939920)

[Wofür steht die Abkürzung DNS? 4](#_Toc96939921)

[Was ist das DNS? 4](#_Toc96939922)

[Auf welcher OSI Schicht arbeitet das DNS? 4](#_Toc96939923)

[Nennen Sie 2 Aufgaben des DNS. 4](#_Toc96939924)

1. [DHCP 4](#_Toc96939925)

[Wofür steht die Abkürzung DHCP? 4](#_Toc96939926)

[Was ist das DHCP? 4](#_Toc96939927)

[Nennen sie drei Grundlegenden Betriebsmodi des DHCP. 5](#_Toc96939928)

[Welche Ports werden vom DHCP genutzt? 5](#_Toc96939929)

[Erläutern Sie die Zuweisung über DHCP nach DORA: 5](#_Toc96939930)

1. [NAT 6](#_Toc96939931)

[Wofür steht die Abkürzung NAT? 6](#_Toc96939932)

[Was ist das NAT? 6](#_Toc96939933)

[Was sind die zwei Typen des NAT Verfahren? Was wird bei den zwei NAT Typen umgesetzt? 6](#_Toc96939934)

1. [Datensicherung 6](#_Toc96939935)

[Welche Arten der Datensicherung gibt es? 6](#_Toc96939936)

[Nennen sie die Vorteile zu jeder Sicherungsart. 6](#_Toc96939937)

[Nennen sie die Nachteile zu jeder Sicherungsart. 6](#_Toc96939938)

[Wie funktioniert eine Differentielle Datensicherung? 7](#_Toc96939939)

[Wie funktioniert eine Vollsicherung? 7](#_Toc96939940)

1. [WLAN 7](#_Toc96939941)

[In welchen Frequenzbereich werden WLAN-Signale, in der heutigen Zeit, gesendet? 7](#_Toc96939942)

[Welche zwei Modis gibt es beim WLAN und was unterscheidet diese? 7](#_Toc96939943)

[Was bedeutet CSMA/CA und was ist seine Aufgabe? 7](#_Toc96939944)

[Wofür dient ein Frequenz Hopping Spread Spectrum? 8](#_Toc96939945)

[Nennen Sie drei Faktoren die beim Einrichten von WLAN Netzwerken zu beachten sind. 8](#_Toc96939946)

1. [Digitale Zertifikate 8](#_Toc96939947)

[Was ist ein digitales Zertifikat und wofür wird es verwendet ? 8](#_Toc96939948)

[Nennen Sie drei Angaben, die ein Zertifikat besitzen muss. 8](#_Toc96939949)

[Ergänzen Sie wozu Zertifikate bei folgenden Einsatzgebieten benutzt werden. 8](#_Toc96939950)

1. [Cloud Computing 9](#_Toc96939951)

[Was ist unter Cloud-Computing zu verstehen? 9](#_Toc96939952)

[Ergänzen Sie was man unter den Folgenden Begriffen versteht. 9](#_Toc96939953)

[SaaS (Software as a Service): 9](#_Toc96939954)

[PaaS (Platform as a Service): 9](#_Toc96939955)

[IaaS (Infrastructure as a Service): 9](#_Toc96939956)

[Nenne Sie je 3 Vor- und Nachteile von Cloud Computing. 9](#_Toc96939957)

1. [IPv6 10](#_Toc96939958)

[Aus welchem Grund wurde IPv6 entwickelt? 10](#_Toc96939959)

[Was versteht man bei IP-Adressen unter den Begriff Oktett? 10](#_Toc96939960)

[Kürzen Sie die IPv6 Adresse 2001:0db8:0000:dasd:acad:0000:0000:0402 10](#_Toc96939961)

[Erläutern Sie die Begriffe Unicast, Multicast, Anycast. 10](#_Toc96939962)

[Woran erkennt man eine Link-Local Adresse? 10](#_Toc96939963)

[Wofür nutzt man eine Link-Local-Adresse? 10](#_Toc96939964)

[Der Adressraum des IPv6 Netzes 2001:db8:acad:DD00::/56 soll in 8 gleich große Teilnetze aufgeteilt werden. 11](#_Toc96939965)

[Ergänzen sie die Tabelle: 11](#_Toc96939966)

1. [VLAN 11](#_Toc96939967)

[Wofür steht VLAN? 11](#_Toc96939968)

[Welchen Zweck hat VLAN? 11](#_Toc96939969)

[Nennen sie Vorteile eines VLAN gegenüber einem normalen LAN. 11](#_Toc96939970)

1. [VPN 11](#_Toc96939971)

[Nennen sie die drei Sicherheitsaspekte eines VPN. 11](#_Toc96939972)

[Welches Protokoll wird hierfür eingesetzt? 12](#_Toc96939973)

[Welche Betriebs-Modi kennen sie? 12](#_Toc96939974)

[Welche Verbindungsarten gibt es? 12](#_Toc96939975)

1. [PKI 12](#_Toc96939976)

[Wofür steht PKI? 12](#_Toc96939977)

[Nennen sie Beispiele für die Nutzung? 12](#_Toc96939978)

[Wofür stehen die Abkürzungen RA, CA und VA in der PKI? 13](#_Toc96939979)

1. [OSI-Modell 13](#_Toc96939980)

[In welche zwei Bereiche unterteilt man die 7 Schichten des OSI-Modells? 13](#_Toc96939981)

[Wie heißen die anwendungsorientierten Schichten? 13](#_Toc96939982)

[Nennen sie Geräte, die auf den Schichten 1 bis 3 genutzt werden. 14](#_Toc96939983)

1. [Verschlüsselung 14](#_Toc96939984)

[Was ist der Unterschied zwischen symmetrischer und asymmetrischer Verschlüsselung? 14](#_Toc96939985)

[Was versteht man unter einer hybriden Verschlüsselung? 14](#_Toc96939986)

[Worin liegt der Vorteil einer asymmetrischen Verschlüsselung? 14](#_Toc96939987)

1. [Storage – SAN und NAS 15](#_Toc96939988)

[Was versteht man unter einem blockbasierten Datenaustausch? 15](#_Toc96939989)

[Welches Kommunikationsprotokoll wird standartmäßig bei SAN verwendet? 15](#_Toc96939990)

[Beschreibe den Aufbau eines einfachen SAN 15](#_Toc96939991)

[Nenne drei Vorteile des NAS 15](#_Toc96939992)

[Wie wird ein DAS mit dem Computer verbunden? 15](#_Toc96939993)

1. [Switching 15](#_Toc96939994)

[Was versteht man unter einem Switch? 15](#_Toc96939995)

[Nenne zwei Switchingverfahren 16](#_Toc96939996)

[Warum werden beim Fragment Free Verfahren nur die ersten 64 Byte des Datenpakets überprüft? 16](#_Toc96939997)

1. [Strukturierte Verkabelung 16](#_Toc96939998)

[Beschreibe den Unterschied zwischen Primär- Sekundär- und Tertiärbereich 16](#_Toc96939999)

[Was ist die galvanische Trennung? 17](#_Toc96940000)

[Was versteht man unter einem Twisted-Pair-Kabel? 17](#_Toc96940001)

[Nenne drei Elemente, die für eine strukturierte Verkabelung benötigt werden 17](#_Toc96940002)

[Warum eignen sich Glasfaserkabel für die primäre Verkabelung besonders? 17](#_Toc96940003)

1. [Firewall 17](#_Toc96940004)

[Was ist der Unterschied zwischen einer Blacklist- und einer Whiteliststrategie? 17](#_Toc96940005)

[Was versteht man unter dem Paketfilter? 17](#_Toc96940006)

[Warum müssen für ein Verbindung zwei Regeln definiert werden? 17](#_Toc96940007)

[Was ist der Unterschied zwischen einer „Personal Firewall“ und einer externen Firewall? 17](#_Toc96940008)

Fragebogen mit Antworten zu den Lernzusammenfassungen

# DNS

## Wofür steht die Abkürzung DNS?

Domain Name System

## Was ist das DNS?

Ein Internetprotokoll, dass für die Namensauflösung da ist. Es übersetzt Klarnamen in IP und umgekehrt.

## Auf welcher OSI Schicht arbeitet das DNS?

Anwendungsschicht TCP/IP Layer 3

## Nennen Sie 2 Aufgaben des DNS.

Übersetzung von Domainnamen in IP-Adressen (Forward Lookup).

Auflösung der IP-Adressen in Domainnamen (Reverse Lookup)

# DHCP

## Wofür steht die Abkürzung DHCP?

Dynamic Host Configuration Protocol

## Was ist das DHCP?

Ein Internetprotokoll, dass IP-Adressen und weitere Parameter Computern dynamisch zuweist.

Nennen Sie zwei mögliche Zuweisungen des DHCP.

• IP-Adresse und Netzwerkmaske

• Default-Gateway

• Nameserver

• SMTP-Server

• WINS-Server

• Proxy-Konfiguration (nicht bei Windows-Systemen)

## Nennen sie drei Grundlegenden Betriebsmodi des DHCP.

Manuelle Zuordnung:

IP-Adressen werden den MAC-Adressen der Computer fest zugeordnet.

Nachteil: Keine zusätzlichen Clients können sich ohne Konfiguration einbinden.

Vorteil: Dies kann wiederum ein Vorteil sein, in Hinsicht auf Sicherheitsaspekte.

Automatische Zuordnung:

Definierter Bereich von IP-Adressen.

Auch hier wird die zu vergebene IP-Adresse an die MAC-Adresse des Clients gebunden.

Nachteil: Falls Adressbereich voll sein sollte kann kein zusätzlicher Client in das Netzwerk.

Dynamische Zuordnung:

Funktioniert im Allgemeinen wie die automatische Zuordnung.

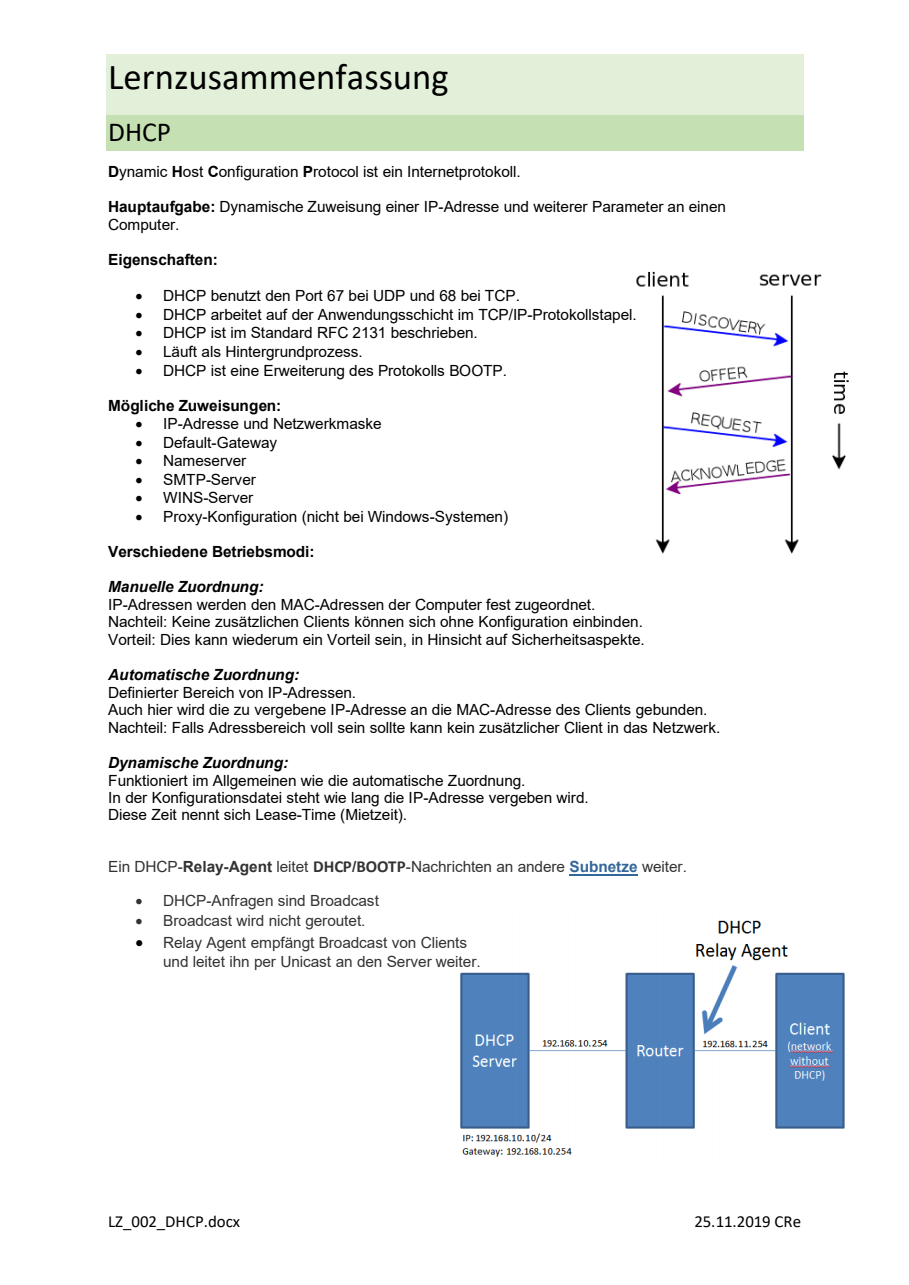
In der Konfigurationsdatei steht wie lang die IP-Adresse vergeben wird.

Diese Zeit nennt sich Lease-Time (Mietzeit).

## Welche Ports werden vom DHCP genutzt?

• DHCP benutzt den Port 67 bei UDP und 68 bei TCP

## Erläutern Sie die Zuweisung über DHCP nach DORA:



# NAT

## Wofür steht die Abkürzung NAT?

Network Address Translation

## Was ist das NAT?

ein Verfahren um automatisiert und transparent Adressinformationen in Datenpaketen durch andere zu ersetzen

## Was sind die zwei Typen des NAT Verfahren? Was wird bei den zwei NAT Typen umgesetzt?

Basic NAT: nur IP-Adressen werden umgesetzt

Network Address Port Translation (NAPT): Umsetzung von IP-Adressen und Port-Nummern

# Datensicherung

## Welche Arten der Datensicherung gibt es?

Vollsicherung (Full-Backup)

Differentielle Datensicherung

Inkrementelle Datensicherung

## Nennen sie die Vorteile zu jeder Sicherungsart.

Vollsicherung:

Die Erstellung bzw. Wiederherstellung der Sicherung ist schneller als eine differentielle oder inkrementelle Sicherung. Die Handhabung ist einfacher, da nur eine Datei für eine Wiederherstellung benötigt wird.

Differentielle Datensicherung:

Eine regelmäßig durchgeführte differentielle Sicherung benötigt weniger Speicherkapazität, als eine Vollsicherung

Inkrementelle Datensicherung:

Eine regelmäßig durchgeführte inkrementelle Sicherung benötigt weniger Speicherkapazität, als eine Vollsicherung oder differentielle Sicherung.

## Nennen sie die Nachteile zu jeder Sicherungsart.

Vollsicherung:

Eine regelmäßig durchgeführte Vollsicherung benötigt mehr Speicherkapazität und mehr Zeit, als eine differentielle oder inkrementelle Sicherung

Differentielle Datensicherung:

Eine Wiederherstellung der Sicherung ist langsamer als die der Vollsicherung Die Handhabung ist komplizierter, da zwei oder mehr Dateien für eine Wiederherstellung benötigt werden.

Inkrementelle Datensicherung:

Eine Wiederherstellung der Sicherung ist langsamer, als die der Voll- oder differentiellen Sicherung

## Wie funktioniert eine Differentielle Datensicherung?

Bei einer differentiellen Sicherung werden nur die seit dem letzten Vollbackup veränderten oder neu hinzugekommenen Daten gesichert. Ein solches Backup setzt deshalb eine zuvor erstellte Vollsicherung voraus. Für eine Wiederherstellung werden beide Dateien, also die Basis-Vollsicherung und die differentielle Sicherungsdatei benötigt. Das Archivbit bleibt gesetzt, so dass die Dateien beim nächsten differenziellen Backup erneut mitgesichert werden.

## Wie funktioniert eine Vollsicherung?

Bei einer Vollsicherung werden jedes Mal alle zu sichernden Daten in einer Sicherungsdatei auf dem Zieldatenträger gespeichert. Dadurch sind alle gesicherten Daten in nur einer Datei enthalten, was die Verwaltung der Backups vereinfacht.

# WLAN

## In welchen Frequenzbereich werden WLAN-Signale, in der heutigen Zeit, gesendet?

2,4 – 5,8 GHz

## Welche zwei Modis gibt es beim WLAN und was unterscheidet diese?

Ad-hoc-Modus

• Alle WLAN-Clients gleichberechtigt

• Jeder kann eine direkte Verbindung aufbauen

• Ohne Access Point

• Immer direkte Kommunikation

Infrastrukturmodus

• Router übernimmt Koordinierung des Datenverkehrs

• Kommunikation immer über den Router

• Reichweite durch Repeater erweiterbar

## Was bedeutet CSMA/CA und was ist seine Aufgabe?

Carrier Sense Multiple Access/Collision Avoidance vermeidet Kollisionen beim gleichzeitigen Start von Übertragungen.

## Wofür dient ein Frequenz Hopping Spread Spectrum?

Übertragung von 1 – 3 Bit danach wechsel der Frequenz. Signal lässt sich nicht abhören, weil ein Außenstehender nie weiß, auf welcher Trägerfrequenz sich nach dem nächsten Hop das Signal befindet.

## Nennen Sie drei Faktoren die beim Einrichten von WLAN Netzwerken zu beachten sind.

• Wanddicke / Störsender in der Nähe

• Frequenzbereich (2,4 GHz oder 5 GHz)

• Qualität der Geräte

• Benötigte Übertragungsbandbreite

# Digitale Zertifikate

## Was ist ein digitales Zertifikat und wofür wird es verwendet ?

Ein digitales Zertifikat ist ein digitaler Datensatz, der bestimmte Eigenschaften von Personen oder Objekten bestätigt und die Möglichkeit gibt dessen Authentizität und Integrität durch kryptografische Verfahren zu prüfen.

Anhand des Zertifikates kann überprüft werden, ob der Schlüssel von der/dem Person/Rechner/Organisation stammt, mit der/dem man kommunizieren möchte.

## Nennen Sie drei Angaben, die ein Zertifikat besitzen muss.

• Namen des Zertifikatsinhabers

• Zertifizierungsstelle

• Gültigkeitsdauer

• Seriennummer

• öffentlicher Schlüssel des Inhabers (damit kann die Echtheit des Schlüssels überprüft werden) und

• digitale Signatur der ausstellenden Zertifizierungsstelle, so dass verifiziert werden kann, ob das Zertifikat echt ist.

## Ergänzen Sie wozu Zertifikate bei folgenden Einsatzgebieten benutzt werden.

SSL/TLS: Bei Netzwerkprotokollen sollen Zertifikate sicherstellen, dass sich der Server identifiziert.

E-Mail-Verschlüsselung: zur Bestätigung der Echtheit von E-Mails werden ebenfalls Zertifikate eingesetzt.

Digitale Signatur: Zertifikate werden auch für die digitale Signatur benötigt, um Dokumente als unverfälscht ansehen zu können.

# Cloud Computing

## Was ist unter Cloud-Computing zu verstehen?

IT-Infrastrukturen (Rechenkapazität, Datenspeicher, Netzwerkkapazitäten und fertige Software) wird dynamisch an den Bedarf angepasst über ein Netzwerk zur Verfügung gestellt.

## Ergänzen Sie was man unter den Folgenden Begriffen versteht.

### SaaS (Software as a Service):

Die Software und die IT-Infrastruktur werden von einem externen IT-Dienstleisterbetrieben und vom Kunden als Service genutzt

### PaaS (Platform as a Service):

Eine Computer-Plattform wird für Entwickler von Webanwendungen in der Cloud zur Verfügung gestellt

### IaaS (Infrastructure as a Service):

Stellt die unterste Schicht im Cloud-Computing dar. Der Benutzer greift hier auf bestehende Dienste innerhalb des Systems zu, verwaltet seine virtuellen Server allerdings weitestgehend selbst.

## Nenne Sie je 3 Vor- und Nachteile von Cloud Computing.

Vorteile gegenüber eigenem Rechenzentrum:

• Verbrauchsgerechte Abrechnung

• Kostentransparenz

• Flexible Anpassung der IT-Infrastruktur an die Anfordernisse

• Geringere Personalkosten, da Aufgaben ausgelagert werden

• Einsparung von Energiekosten

Argumente gegen Cloud-Computing:

• Online-Anwendungen können ausfallen und Unternehmen in schwierige Situationen ohne funktionierende IT-Anwendungen führen

• Daten sind bei Providern nicht sicher (Firmendaten können ausgespäht werden)

• Datenschutz kann bei Providern nicht 100%ig sichergestellt werden

• rechtliche und technologische Abhängigkeit vom Provider

• verliert an Flexibilität

# IPv6

## Aus welchem Grund wurde IPv6 entwickelt?

• IPv4 bietet einen Adressraum von etwas über 4 Milliarden IP-Adressen.

• Viele der 4 Milliarden sind in der Praxis nicht nutzbar (z. B. Multicast)

• Als Resultat daraus herrscht Adressenknappheit. (Notlösungen: PAT, CIDR, NAT und dynamische Vergabe)

• IPv6 bietet einen Adressbereich von 2128. Das sind ca. 340 Sextillionen.

• 340.282.366.920.938.463.463.374.607.431.768.211.456

## Was versteht man bei IP-Adressen unter den Begriff Oktett?

Ein Block bestehend aus 8 Bit in binärer Schreibweise. Demzufolge sind auch 2 Hex-Ziffern ein Oktett.

## Kürzen Sie die IPv6 Adresse 2001:0db8:0000:dasd:acad:0000:0000:0402

2001:db8:0:dacd:acad::402

## Erläutern Sie die Begriffe Unicast, Multicast, Anycast.

Unicast

Bezieht sich auf eine Schnittstelle auf einem einzelnen Knoten.

Multicast

Bezieht sich auf eine Gruppe von Schnittstellen, in der Regel auf verschiedenen Knoten. Pakete, die eine Multicast-Adresse gesendet werden, werden an alle Mitglieder der Multicast-Gruppe geleitet.

Anycast

bezieht sich auf eine Gruppe von Schnittstellen, in der Regel auf verschiedenen Knoten. Pakete, die an eine Anycast-Adresse gesendet werden, gehen an den Mitgliedsknoten der Anycast-Gruppe, der dem Absender am nähesten ist.

## Woran erkennt man eine Link-Local Adresse?

Präfix: fe80::/10 vergleichbar zu 127.0.0.1 bei IPv4

## Wofür nutzt man eine Link-Local-Adresse?

Wird zur Information über die Anwesenheit von anderen IPv6-Hosts und -Routern verwendet.

## Der Adressraum des IPv6 Netzes 2001:db8:acad:DD00::/56 soll in 8 gleich große Teilnetze aufgeteilt werden.

### Ergänzen sie die Tabelle:

Netz Netz-Adresse

1 2001:db8:acad:DD00::

2 2001:db8:acad:DD\_\_:: 20

3 2001:db8:acad:DD\_\_:: 40

4 2001:db8:acad:DD\_\_:: 60

5 2001:db8:acad:DD\_\_:: 80

6 2001:db8:acad:DD\_\_:: A0

7 2001:db8:acad:DD\_\_:: C0

8 2001:db8:acad:DD\_\_:: E0

# VLAN

## Wofür steht VLAN?

Virtual Local Area Network

## Welchen Zweck hat VLAN?

ein virtuelles lokales Netz innerhalb eines physischen Netzes, in der nur Stationen des gleichen VLAN’s miteinander kommunizieren können, um die Sicherheit zu erhöhen und Traffic zu verringern.

## Nennen sie Vorteile eines VLAN gegenüber einem normalen LAN.

* Bessere Lastverteilung möglich
* Erhöhte Sicherheit durch Gruppierung (Subnetze)
* Priorisierung des Datenverkehrs möglich
* Weniger Kollisionsbereiche (Broadcastdomänen)
* Einfachere Softwarekonfiguration durch Software für die Gruppen

# VPN

## Nennen sie die drei Sicherheitsaspekte eines VPN.

Authentizität – Echtheit der Daten + Versender

Integrität – Daten sind unverändert

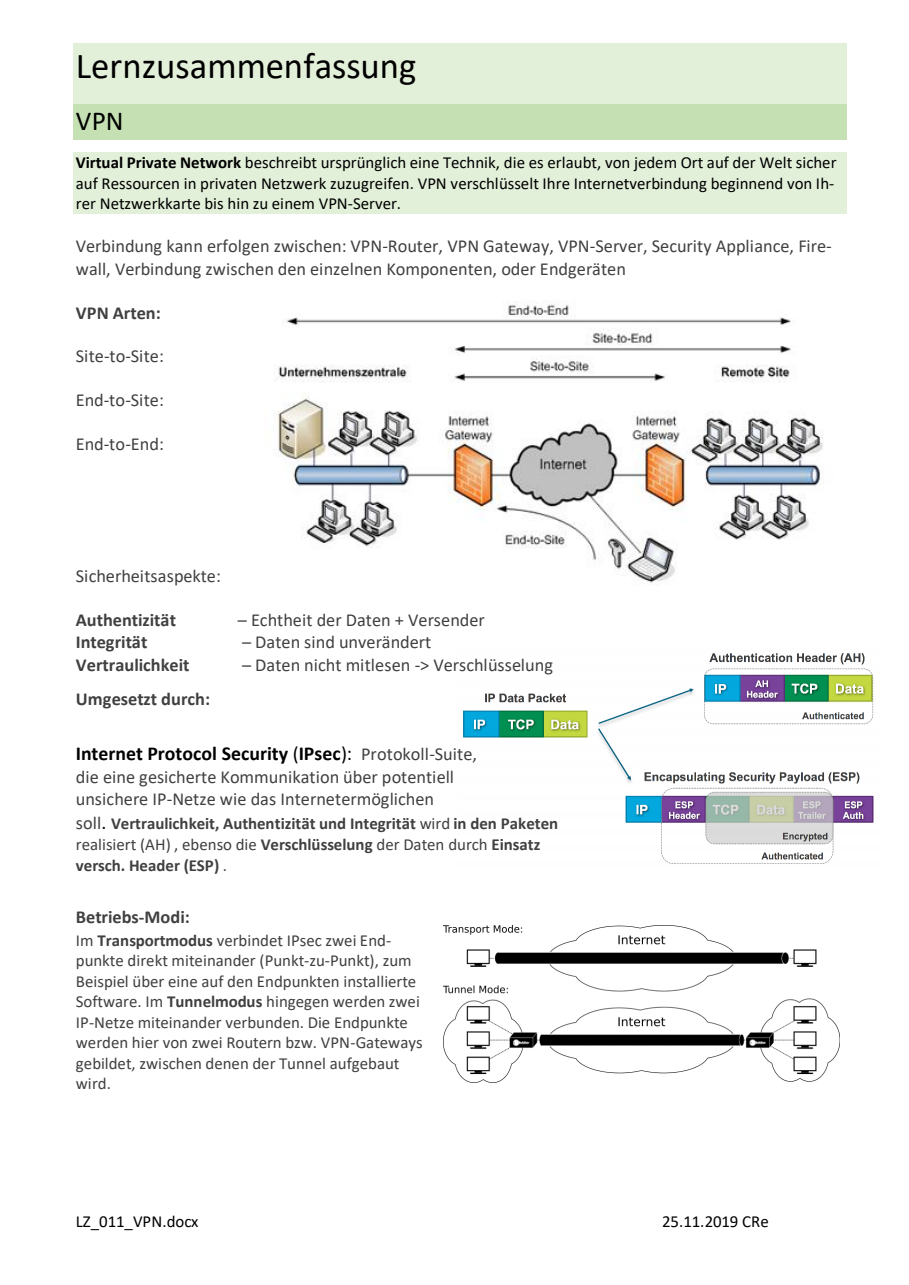
Vertraulichkeit – Daten nicht mitlesen -> Verschlüsselung

## Welches Protokoll wird hierfür eingesetzt?

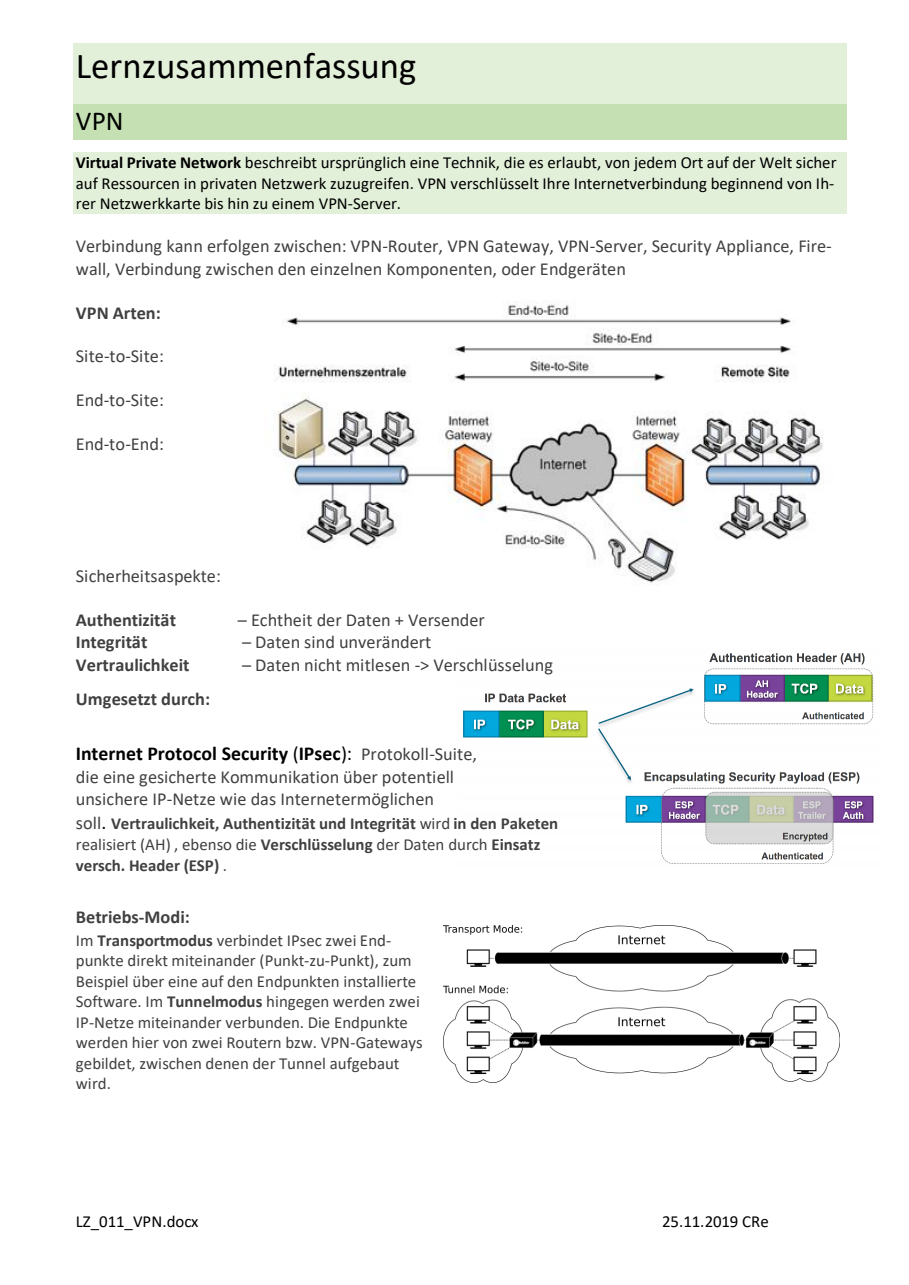
Internet Protocol Security (IPsec): Protokoll-Suite, die eine gesicherte Kommunikation über potentiell unsichere IP-Netze wie das Internet ermöglichen soll. Vertraulichkeit, Authentizität und Integrität wird in den Paketen realisiert (AH) , ebenso die Verschlüsselung der Daten durch Einsatz versch. Header (ESP)

## Welche Betriebs-Modi kennen sie?

Im Transportmodus verbindet IPsec zwei Endpunkte direkt miteinander (Punkt-zu-Punkt), zum Beispiel über eine auf den Endpunkten installierte Software. Im Tunnelmodus hingegen werden zwei IP-Netze miteinander verbunden. Die Endpunkte werden hier von zwei Routern bzw. VPN-Gateways gebildet, zwischen denen der Tunnel aufgebaut wird.



## Welche Verbindungsarten gibt es?



# PKI

## Wofür steht PKI?

Public-Key-Infrastrukturen (PKI - Öffentlicher-Schlüssel-Infrastruktur)

## Nennen sie Beispiele für die Nutzung?

• Starke Authentisierung für Intra-/Extra-/Internet-Ressourcen

• Sichere Kommunikation mit SSL/TLS/Signieren Verschlüsseln von E-Mail (S/MIME)

• Elektronischer Zeitstempel (Qualifiziert - Akkreditiert)

• Single Sign On

• Signatur von elektronischen Dokumenten

• Einsatz durch TrustCenter "getrusteter" elektronischer Zertifikate

• Internet der Dinge (z.B. Smart Meter Datenaustausch)

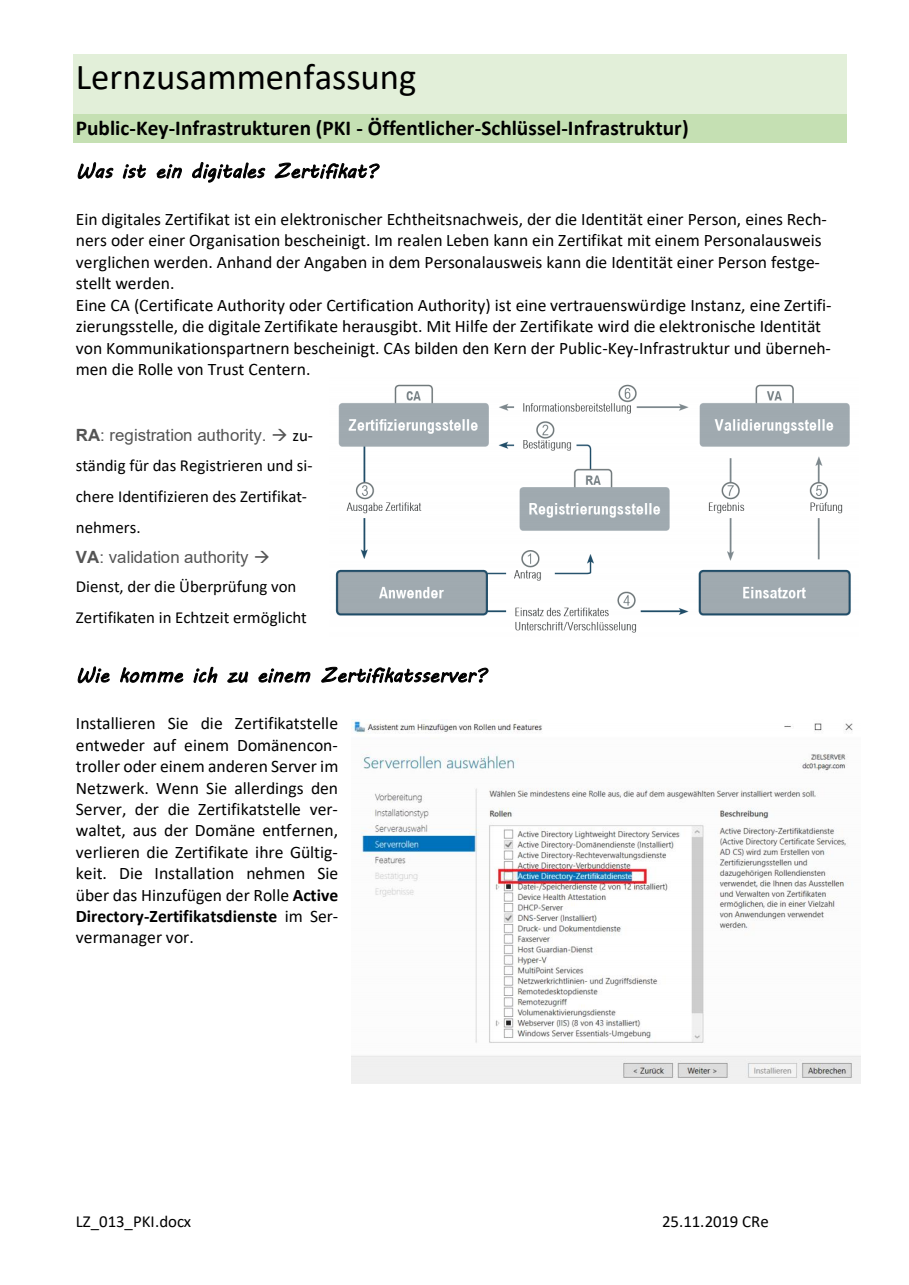
• Mobile PKI und Mobile Device Management u.v.m.

## Wofür stehen die Abkürzungen RA, CA und VA in der PKI?

Eine CA (Certificate Authority oder Certification Authority) ist eine vertrauenswürdige Instanz, eine Zertifizierungsstelle, die digitale Zertifikate herausgibt. Mit Hilfe der Zertifikate wird die elektronische Identität von Kommunikationspartnern bescheinigt. CAs bilden den Kern der Public-Key-Infrastruktur und übernehmen die Rolle von Trust Centern.

RA: registration authority. → zuständig für das Registrieren und sichere Identifizieren des Zertifikatnehmers.

VA: validation authority →Dienst, der die Überprüfung von Zertifikaten in Echtzeit ermöglicht



# OSI-Modell

## In welche zwei Bereiche unterteilt man die 7 Schichten des OSI-Modells?

Anwendungsorientierte Schichten (5-7)

Transportorientierte Schichten (1-4)

## Wie heißen die anwendungsorientierten Schichten?

Application Layer – Anwendungsschicht

Presentation Layer – Darstellungsschicht

Session Layer – Sitzungs- bzw Kommunikationsschicht

## Nennen sie Geräte, die auf den Schichten 1 bis 3 genutzt werden.

1 – Netzwerkkabel, Repeater, Hub

2 – Bridge, Switch, AP

3 – Router, Layer-3-Switch

# Verschlüsselung

## Was ist der Unterschied zwischen symmetrischer und asymmetrischer Verschlüsselung?

Symmetrische Verschlüsselung

• Benutzt nur ein Kennwort zum ver- und entschlüsseln

• Wie: Zahlenkombination am Fahrradschloss. Jeder der sie kennt kann mit dem Rad fahren.

• Austausch des Schlüssels notwendig. (z.B. über das Internet unsicher)

Asymmetrische Verschlüsselung

Hierbei kommen zwei verschiedene Schlüssel zum Einsatz: ein öffentlicher und ein geheimer (privater) Schlüssel.

Das Prinzip der asymmetrischen Verschlüsselung beruht im Wesentlichen darauf, dass sich jeder Kommunikationspartner jeweils ein Schlüsselpaar erzeugt.

• Einer der Schlüssel wird geheim gehalten, der so genannte private Schlüssel und

• der andere, der so genannte öffentliche Schlüssel wird jedem kommunikationswilligen Wesen zugänglich gemacht.

## Was versteht man unter einer hybriden Verschlüsselung?

Sie ist eigentlich sehr simpel und umso mehr genial. Sie verbindet die Vorteile der 2 anderen Systeme zu einem Neuen. Hybride Verschlüsselung vereinigt die Vorteile und besitzt eigentlich keine Nachteile. Sie funktioniert nämlich in Kürze so:

mit Hilfe eines asymmetrischen Verfahrens (z.B. RSA) wird ein selbst generierter Schlüssel verschlüsselt ausgetauscht, welcher für eine symmetrische Verschlüsselung (z.B. AES) verwendet wird.

## Worin liegt der Vorteil einer asymmetrischen Verschlüsselung?

Der große Vorteil dieses Verfahrens im Vergleich zur symmetrischen Verschlüsselung ist in der einfachen Verteilung des öffentlichen Schlüssels begründet. Dieser kann wirklich für jeden Menschen frei zugänglich sein, ohne dass dadurch das Verfahren unsicher wird.

# Storage – SAN und NAS

## Was versteht man unter einem blockbasierten Datenaustausch?

Bei einem blockbasierten Datenaustausch werden durch Rechner einzelne Datenblöcke von einer Festplatte angefordert. Im Gegensatz dazu werden bei einem dateibasierten Datenaustausch über CIFS oder NFS ganze Dateien angefordert.

## Welches Kommunikationsprotokoll wird standartmäßig bei SAN verwendet?

Bei SAN wird Standardmäßig das SCSI Kommunikationsprotokoll verwendet.

## Beschreibe den Aufbau eines einfachen SAN

Ein einfaches SAN besteht aus einem Fibre-Channel-Switch, einem oder mehreren Festplattensubsystemen und den Servern, die über so genannte Host Bus Adapter, kurz HBA, mit dem Fibre Channel Switch verbunden werden.

## Nenne drei Vorteile des NAS

Ein NAS ist,

• einfach zu installieren,

• leicht skalierbar,

• einfach zu administrieren

## Wie wird ein DAS mit dem Computer verbunden?

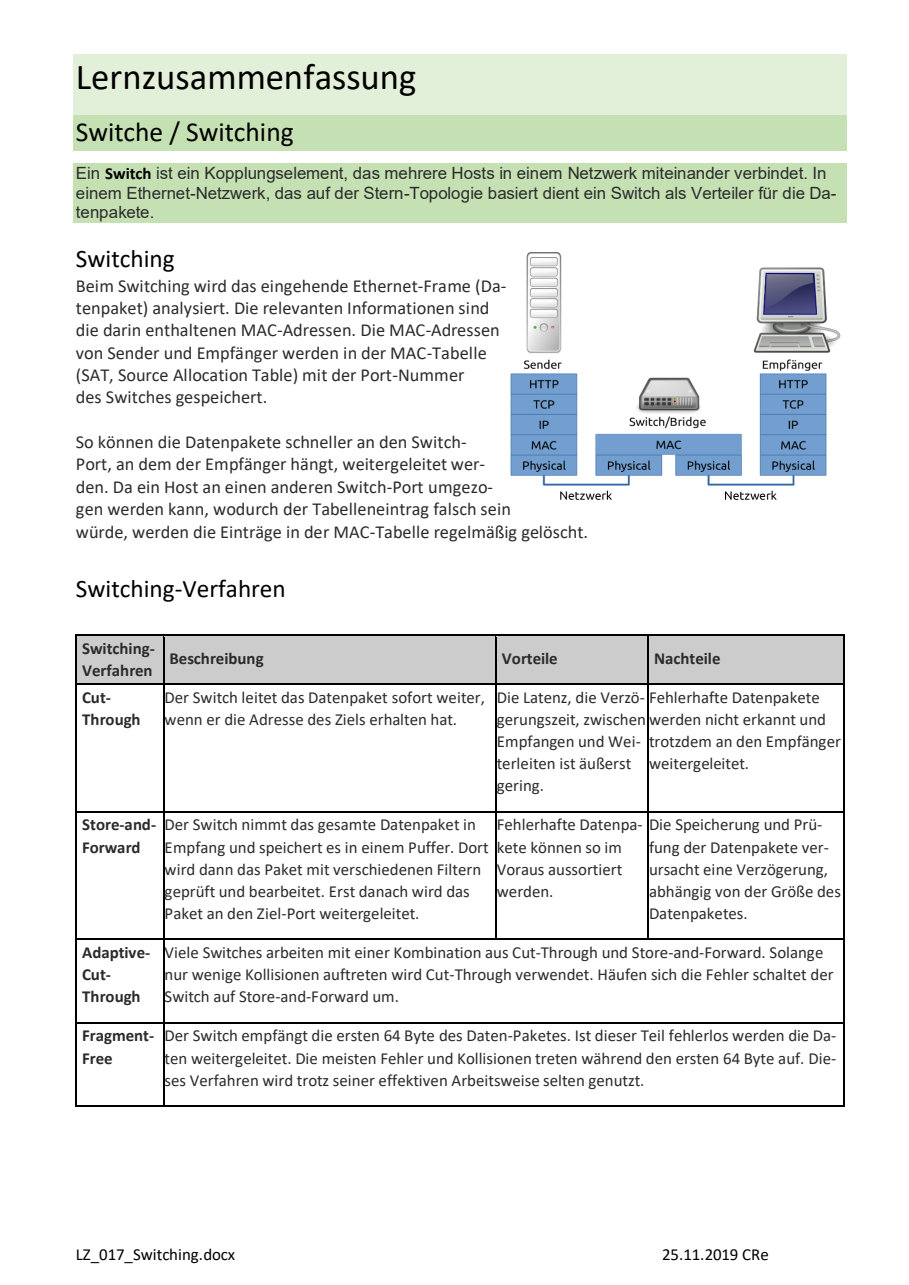
Direkt per Kabel über die Schnittstelle des Computers angeschlossen. Prozessor hat direkt Zugriff über Protokolle und Commandos. Z.B. Festplatte in einem Rechner

# Switching

## Was versteht man unter einem Switch?

Ein Switch ist ein Kopplungselement, das mehrere Hosts in einem Netzwerk miteinander verbindet. In einem Ethernet-Netzwerk, das auf der Stern-Topologie basiert dient ein Switch als Verteiler für die Datenpakete In welcher Netzwerktopologie dient der Switch als Verteiler der Datenpakete?

## Nenne zwei Switchingverfahren



## Warum werden beim Fragment Free Verfahren nur die ersten 64 Byte des Datenpakets überprüft?

Der Switch empfängt die ersten 64 Byte des Daten-Paketes. Ist dieser Teil fehlerlos werden die Daten weitergeleitet. Die meisten Fehler und Kollisionen treten während den ersten 64 Byte auf. Dieses Verfahren wird trotz seiner effektiven Arbeitsweise selten genutzt

# Strukturierte Verkabelung

## Beschreibe den Unterschied zwischen Primär- Sekundär- und Tertiärbereich

Primärbereich: Verkabelung der Gebäude eines Standortes untereinander. Der Primärbereich umfasst das Kabel von dem Standortverteiler zu einem Gebäudeverteiler, die Gebäudeverteiler und die Kabel zwischen den Gebäudeverteilern. Große Kabellängen notwendig. Deshalb ist das Glasfaserkabel wegen der kleinen Dämpfung bei einer großen Datenübertragungsrate besonders geeignet.

Sekundärbereich: vertikale Stockwerkverkabelung, also die Verkabelung der Stockwerke eines Gebäudes untereinander. Der Sekundärbereich umfasst die Kabel von dem Gebäudeverteiler zu den Stockwerkverteilern.

Tertiärbereich: horizontale Stockwerkverkabelung, also die Verkabelung innerhalb der Stockwerke eines Gebäudes und wird auch als Etagenverkabelung bezeichnet.

## Was ist die galvanische Trennung?

Unter galvanischer Trennung versteht man das Vermeiden der elektrischen Leitung zwischen zwei Stromkreisen, zwischen denen Leistung oder Signale ausgetauscht werden sollen

## Was versteht man unter einem Twisted-Pair-Kabel?

Als Twisted-Pair-Kabel oder Kabel mit verdrillten Adernpaaren bezeichnet man in der Telekommunikations-, Nachrichtenübertragungs- und Computertechnik Kabeltypen, in denen die Adern paarweise miteinander verdrillt sind.

## Nenne drei Elemente, die für eine strukturierte Verkabelung benötigt werden

• Elemente der Strukturierten Verkabelung

o Verteilerschränke

o Patchpanels

o Patchkabel

o Anschlussdosen

o Kabel

## Warum eignen sich Glasfaserkabel für die primäre Verkabelung besonders?

* Größere Entfernungen
* Keine Elektromagnetischen Störungen
* Geringere Latenz
* Schneller

# Firewall

## Was ist der Unterschied zwischen einer Blacklist- und einer Whiteliststrategie?

Blacklist-Strategie: Alles ist erlaubt, außer den verbotenen Adressen.

Whitelist-Strategie: Alles ist verboten, außer der erlaubten Adresse

## Was versteht man unter dem Paketfilter?

Der Paketfilter kontrolliert den Verkehr mittels Regeln, die sich hauptsächlich auf die Adressierung der Pakete, also die Sockets (IP-Adresse und TCP- oder UDP-Port) der Quelle und des Ziels, beziehen. Jede Form von gewünschter Verbindungsaufnahme zwischen zwei Sockets sollte explizit erlaubt und jede andere Kommunikation explizit verboten sein.

## Warum müssen für ein Verbindung zwei Regeln definiert werden?

Eine für eingehende und eine für ausgehende Pakete

## Was ist der Unterschied zwischen einer „Personal Firewall“ und einer externen Firewall?

Abhängig davon, wo die Firewall-Software installiert ist, wird unterschieden zwischen einer Personal Firewall (auch Desktop Firewall) und einer externen Firewall (auch Netzwerk- oder Hardware-Firewall genannt). In Abgrenzung zur Personal Firewall arbeitet die Software einer externen Firewall nicht auf dem zu schützenden System selbst, sondern auf einem separaten Gerät, das Netzwerke oder Netzsegmente miteinander verbindet und dank der Firewall-Software gleichzeitig den Zugriff zwischen den Netzen beschränkt.