Pool 4: Betrieb von IKT-Systemen, Netzwerk und Systemsicherheit

Ich übernehme keine Verantwortung für fehlende oder falsche Informationen.

Ethernet

Ethernet ist ein paketvermittelnde Netzwerktechnik, die auf der Schicht 1 und 2 des OSI-Schichtenmodells die Adressierung und die Zugriffskontrolle auf das Übertragungsmedium definiert. Die Daten kommen bereits in Paketen von den darüberliegenden Schichten. Zum Beispiel von TCP/IP. Zusätzlich werden diese Datenpakete mit einem Header und einer Prüfsumme versehen. Danach werden sie übertragen.

1. Was sind Ethernet Frames?

Ethernet ist ein paketvermittelndes Netzwerk. Die Daten werden in mehrere kleine Pakete aufgeteilt. Diese Pakete werden Frames oder Rahmen genannt.
Einem Ethernet Frame geht voraus:

- **Präambel** (8 Byte): Sie dient zur Synchronisation der Empfänger
- **Start Frame Delimiter** (SFD): Eine Bitfolge, die das Frame einleitet

Ein Ethernet Frame beinhaltet:

- **Zieladresse und Quelladresse** (MAC-Adressen für die jeweils 6 Byte zur Verfügung stehen)
- **Steuerinformationen** (nehmen je nach Format unterschiedlich viel Platz ein)
- **Daten**
- **Frame Check Sequence** (FCS – 4 Byte): Eine Prüfsumme, die über das gesamte Frame, exklusive Präambel und SFD berechnet wird.

Nach dem Senden kommt:

- **Inter Frame Gap**: Die Pause nach dem Senden beträgt 9,6 Mikrosekunden

2. Welche Ethernet Frames gibt es?

- **Ethernet II**: Dabei handelt es sich um die klassische Struktur. Merkmal ist die Typeninformation mit 2 Byte.

Präambel	SFD	Ethernet-Frame: min. 64 Byte / max. 1518 Byte					Inter Frame Gap 9,6 µs
101010..		Zieladresse	Quelladresse	Typ	Daten	FCS	
8 Byte		6 Byte	6 Byte	2 Byte	46 - 1500 Byte	4 Byte	

- **Ethernet 802.3 raw (von Novell für IPX)**: Es kann nur IPX (Netzwerkprotokoll von Novell) transportieren, deshalb gibt es auch kein Typenfeld. Das letzte Bit des SFD ist immer eine 1, daran erkennt man, dass das Frame beginnt. Dieses Format erkennt man an der Folge von 1 nach dem Längenfeld. Wäre dieses nicht vorhanden, könnt man es mit Ethernet II verwechseln.

Präambel	SFD	Ethernet-Frame: min. 64 Byte / max. 1518 Byte						Inter Frame Gap 9,6 µs
101010..	10101011	Zieladresse	Quelladresse	Länge	0xFFFF	Daten	FCS	
8 Byte		6 Byte	6 Byte	2 Byte	2 Byte	44 - 1498 Byte	4 Byte	

- **Ethernet 802.3**: Diese verzichten auf ein Typenfeld. Es folgen der Destination Service Access Point (DSAP) und der Source Service Access Point (SSAP). Das Control-Feld enthält den Typ des Logical Link Control (LLC)-Frames (siehe Glossar für mehr Informationen).

Präambel	SFD	Ethernet-Frame: min. 64 Byte / max. 1518 Byte								Inter Frame Gap 9,6 µs
101010..	10101011	Zieladresse	Quelladresse	Länge	DSAP	SSAP	Control	Daten	FCS	
8 Byte		6 Byte	6 Byte	2 Byte	1 Byte	1 Byte	1 Byte	42 - 1497 Byte	4 Byte	

- **Ethernet 802.3 SNAP**: Dieses Ethernet-Frame hat als DSAP und SSAP immer "0xAA" und im Control-Feld immer "0x03". Das SNAP-Feld (Subnetwork Access Protocol) enthält den Organizationally Unique Identifier (OUI) des Herstellers (3 Byte) und die Protokollnummer (Typenfeld, 2 Byte).

Präambel	SFD	Ethernet-Frame: min. 64 Byte / max. 1518 Byte								Inter Frame Gap 9,6 µs
101010..	10101011	Zieladresse	Quelladresse	Länge	DSAP	SSAP	Control	SNAP	Daten	FCS	
8 Byte		6 Byte	6 Byte	2 Byte	0xAA	0xAA	0×03	5 Byte	38 - 1492 Byte	4 Byte	

- **Tagged Frames**: Diese enthalten nach der Quelladresse eine Kennzeichnung (Tag bzw. VLAN-Tag), um Frames einem VLAN zuzuordnen. Daran erkennen Stationen zu welchem VLAN das Frame gehört.

Ethernet II tagged

Präambel	SFD	Ethernet-Frame: min. 68 Byte / max. 1522 Byte						Inter Frame Gap 9,6 µs
101010..		Zieladresse	Quelladresse	Tag	Typ	Daten	FCS	
8 Byte		6 Byte	6 Byte	4 Byte	2 Byte	46 - 1500 Byte	4 Byte	

Ethernet 802.3 tagged

Präambel	SFD	Ethernet-Frame: min. 68 Byte / max. 1522 Byte									Inter Frame Gap 9,6 µs
101010..	10101011	Zieladresse	Quelladresse	Tag	Länge	DSAP	SSAP	Control	Daten	FCS	
8 Byte		6 Byte	6 Byte	4 Byte	2 Byte	1 Byte	1 Byte	1 Byte	42 - 1497 Byte	4 Byte	

3. Was ist Fast-Ethernet (IEEE 802.3u / 100Base-TX)?
Fast-Ethernet ist sowohl für Glasfaser- als auch für Twisted-Pair-Kabel spezifiziert.
Merkmale:

- Es erlaubt die Übertragung von **100 Mbit/s (vollduplex)**.
- Bei der Übertragung werden 4 Bit binäre Dateninformationen in 5 Bit binäre Übertragungsinformationen codiert.
- Die Reichweite ist auf **100 Meter** beschränkt.
- Da Fast-Ethernet vollduplexfähig ist, benötigt es **Flow-Control** (siehe Frage 8).
- Fast-Ethernet-Komponenten beherrschen **Auto-Negation**. Dabei können Ethernet-Stationen automatisch die Ethernet-Variante der Station am anderen Ende der Leitung erkennen.

4. Was ist Gigabit-Ethernet (1GBase-T / 1000Base-T / IEEE 802.3z / IEEE 802.3ab)?
Gigabit-Ethernet ist sowohl für Glasfaser- als auch für Twisted-Pair-Kabel spezifiziert.
Merkmale:

- Es erlaubt die Datenübertragung von **1Gbit/s**.
- Es ist ein **Muss**, wenn man Server und Speichergeräte in ein Netzwerk einbinden will und es viele Teilnehmer geben soll.
- Übertragung durch 250Mbit/s auf allen 4 Adernpaaren des Twisted-Pair-Kabels.
- Für Strecken bis **10m**: **CAT5**
- Für Strecken über **10m**: **CAT5e**

Standards:

- IEEE 802.3z / Gigabit Ethernet auf Glasfaser und Twinax-Kabel (davon gibt es 3 versch. Arten)
- IEEE 802.3ab / Gigabit Ethernet über Twisted-Pair-Kabel

5. Was ist 10-Gigabit-Ethernet (10GBase-T / IEEE 802.3ae / IEEE 802.3an)?
10-Gigabit-Ethernet ist sowohl für Glasfaser- als auch für Twisted-Pair-Kabel spezifiziert.
Merkmale:

- Es erlaubt die Datenübertragung von **10Gbit/s**.
- 10-Gigabit-Ethernet wird weniger für **LAN** und mehr für **WAN** verwendet.
- **Jumbo-Frames** sind in 10GBase-T standardisiert (siehe Glossar).

Standards:

- **IEEE 802.3ae / 10-Gigabit-Ethernet über Glasfaserkabel**: Je nach Art bietet dieser Standard eine max. Übertragungsstrecke von 300m bis 40km.

- **IEEE 802.3ak / 10-Gigabit-Ethernet über Twinax-Kabel**: über 8 Twinax-Paare auf 15m
- **IEEE 802.3an / 10-Gigabit-Ethernet über Twisted-Pair-Kupferkabel:** über CAT6a und CAT7

6. Was sind 40- und 100-Gigabit-Ethernet (IEEE 802.3ba)?
Auf dem Weg zu 100-Gigabit-Ethernet ist 40-Gigabit-Ethernet ein Zwischenschritt, der notwendig ist, da die Implementierung von 100-Gigabit-Ethernet sehr teuer und anspruchsvoll ist.
100 GBit/s kann man zum Beispiel dadurch erreichen, dass 10 x 10 GBit/s gebündelt werden. Doch das ist für den Einsatz im WAN nicht praktikabel und auch nicht wirtschaftlich.
Merkmale:

- **Standards**: Je nach Standard kann eine Reichweite zwischen **1m** und **40km** erreicht werden.
- **100-Gigabit-Ethernet über Kupfer?** Kupferkabel sollen bei beiden Geschwindigkeitsstufen auf Twinax-Kabel für Strecken von maximal **10m** möglich sein.
  Mit IEEE 802.3bq ist ein Standard für 40 GBit/s über Kupferkabel in Arbeit.

7. Was ist CSMA/CD?
CSMA/CD (Carrier Sense Multiple Access with Collision Detection) ist ein Zugriffsverfahren von Ethernet, um auf das Übertragungsmedium zugreifen zu können. Dabei spielt die Behandlung von Kollisionen bei der Signalübertragung ein große Rolle. Halbduplex-Ethernet basiert auf dem CSMA/CD-Verfahren.

- **Carrier Sense:** Jede Station prüft, ob das Übertragungsmedium frei ist.
- **Multiple Access:** Mehrere Stationen teilen sich das Übertragungsmedium.
- **Collision Detection:** Wenn mehrere Stationen gleichzeitig senden, erkennen sie die Kollision.

Ablauf:

1. Alle Stationen hören das Übertragungsmedium ab. Bei einem freien medium darf gesendet werden.
2. Ist der Bus frei, beginnt eine Station zu senden.
3. Während der Übertragung prüft die Station ob das gesendete Signal mit dem auf dem Bus identisch ist. Ist dies nicht der Fall, hat eine andere Station gleichzeitig gesendet. Man spricht von einer Kollision.
4. Wenn eine Kollision aufgetreten ist, wird die Übertragung abgebrochen. Die Station, die die Kollision als erstes erkannt hat, sendet ein Signal, damit alle wissen, dass das Netzwerk blockiert ist.
5. Nach einer Wartezeit beginnt das Verfahren erneut.

Kollisionsdomäne:
Diese umfasst ein Netzwerk oder ein Teilnetzwerk. Darin müssen die Kollisionen innerhalb einer bestimmten Zeit jede Station erreichen. Ist die Kollisionsdomäne zu groß, dann besteht die Gefahr, dass sendende Stationen Kollision nicht bemerken können. Deswegen ist die maximale Anzahl der Station in einer Kollisionsdomäne auf 1023 begrenzt.

Wie kann man Kollisionen vermeiden?
Je weniger Stationen sich in einer Kollisionsdomäne befinden, desto weniger Kollisionen können auftreten. Deswegen wird ein Netz auf der Schicht 2 in mehrere Teilnetze aufgeteilt.

8. Was ist Flow-Control?
Wenn eine Ethernet-Station zu viele Datenpakete bekommt, dann besteht die Gefahr, dass die Datenpakete teilweise verworfen werden. Mit Flow-Control kann die Station der Gegenstelle signalisieren, eine Sendepause einzulegen. Die betroffene Station schickt dem Verursacher ein PAUSE-Paket. Entweder an eine spezielle Multicast-MAC-Adresse oder direkt an die MAC-Adresse des Verursachers. Im PAUSE-Paket steht dann die gewünschte Wartezeit.

9. Was ist eine MAC-Adresse?
Jede Station in einem Ethernet-Netzwerk hat eine eigene Adresse. Diese Adresse soll die Stationen eindeutig identifizieren. Sie wird einmalig hardwareseitig vom Hersteller konfiguriert und lässt sich im Regelfall nicht verändern.
Aufbau:
Eine MAC-Adresse besteht aus 48 Bit.

- Die ersten beiden Bit kennzeichnen die Art der Adresse (Unicast oder Multicast bzw. unveränderbar oder lokal veränderbar).
- Die Bits 3 bis 24 kennzeichnen den Hersteller (Organizationally Unique Identifier)
- Die Bits 25 bis 48 werden vom Hersteller vergeben (Organizationally Unique Address)

I/G	U/L	OUI	OUA
1. Bit	2. Bit	3. - 24. Bit	25. - 48. Bit

Darstellung: Eine MAC-Adresse lässt sich als Bitfolge oder in der kanonischen Form (hexadezimal) darstellen. Man teilt die Adresse in 6 Teile zu jeweils 8 Bit auf. Vor der Umwandlung in die kanonische Form, müssen die einzelnen Teile gespiegelt werden.
Broadcast-Adresse: Diese geht an alle Stationen im Netzwerk. Sie besteht aus lauter 1er.

10. Was ist Switching?
Switching ist ein Mechanismus in paketorientierten Netzwerken, um für eingehende Datenpakete den richtigen Ausgang zu ermitteln. Dabei geht es darum auf Basis von Sender und Empfänger-Adressen eine Verbindung zwischen einem Eingangs-Port und einem Ausgangs-Port zu schalten.
Methoden:

- **Cut-Through**: Der Switch analysiert die Ethernet-Frames, bevor sie vollständig eingetroffen sind. Hat er die Ziel-Adresse identifiziert, wird das Frame sofort an den Ziel-Port ausgegeben. Die Verzögerungszeit zwischen Empfangen und Weiterleiten eines Frames ist äußerst gering. Es verzichtet auf die vollständige Analyse der Frames, wobei fehlerhafte oder beschädigte Frames unerkannt bleiben und ungehindert weitergeleitet werden.
- **Store-and-Forward**: Der Switch nimmt stets das gesamte Frame in Empfang und speichert es in einem Puffer. Erst danach wird das Frame auf Struktur und Prüfsumme überprüft. Danach wird die Ziel-MAC-Adresse ausgelesen, überprüft und das Frame weitergeleitet.
- **Adaptive-Cut-Through:** In jedem Fall wird auf eine Kombination aus Cut-Through und Store-and-Forward gesetzt. Im einen Fall werden die Frames mit Cut-Through weitergeleitet, aber anhand der Prüfsumme geprüft. Wird eine bestimmte Fehlerrate überschritten wird automatisch auf Store-and-Forward umgeschaltet. Geht die Fehlerrate zurück, wird auf Cut-Through zurückgeschaltet.

Eine anderen Art von Adaptive-Cut-Through entscheidet anhand der Länge des Frames, welches Verfahren angewendet wird. Ist keine Anpassung der Datenrate nötig, werden Frames mit einer Länge über 512 Byte per Cut-Through weitergeleitet. Kürzere Frames werden vor der Weiterleitung mit Store-and-Forward analysiert.

- **Fragment-Free-Cut-Through:** Dieses Verfahren stammt von Cisco und geht von einem Erfahrungswert bei fehlerhaften Frames aus. Man hat festgestellt, dass Übertragungsfehler am häufigsten innerhalb der ersten 64 Byte eines Frames auftreten. Deshalb überprüft ein, mit Fragment-Free-Cut-Through arbeitender, Switch die ersten 64 Byte auf Fehler. Ist es fehlerfrei wird das Frame per Cut-Through weiterverarbeitet.

11. Was ist VLAN (Virtual Local Area Network / IEEE 802.1q)?

Ein VLAN ist ein virtuelles Teilnetz innerhalb eines physikalischen LANs. Es dient dazu, physikalische Netze in Teilnetze aufzuteilen und diese voneinander zu trennen.
VLANs werden mit Switche realisiert, die in gewisser Weise die Vorteile von Switching und Routing vereinen. Es gilt die Regel: Verbleibt der Netzwerkverkehr innerhalb eines VLANs, wird geswitcht, andernfalls wird in ein anderes VLAN geroutet. Wobei Switching schneller ist als Routing.
Durch VLANs kann die Performance und die Sicherheit eines Netzwerkes erhöht werden.

12. Wie erhöhe ich die Performance und die Sicherheit eines Netzwerkes?

Beides lässt sich durch die Unterteilung des Netzwerkes in Subnetze anhand von VLANs bewerkstelligen.

Performance:

Mit VLANs lassen sich zeitkritische Dienste priorisieren. Weiters lässt sich damit die Broadcast-Domäne verkleinern. Anfragen über unbekannte Zielsysteme werden damit nicht über das gesamte physische Netz übermittelt, sondern lediglich über die logischen Teilnetze.
Durch eine Aufteilung des Netzes kann man auch die Auswirkungen defekter Netzwerkkarten und Broadcaststürme eingrenzen: Statt des gesamten LANs wird damit nur noch ein VLAN lahmgelegt.

Sicherheit:

Mit VLANs lassen sich beispielsweise Webserver oder öffentlich zugängliche Rechner von Systemen, die sensible Firmendaten enthalten, welche sich im gleichen Netzwerk befinden, trennen. Weiters ist es ratsam, zwischen den VLANs eine Intranetfirewall einzubauen.

13. Was ist der Unterschied zwischen einem Router und einem Layer-3-Switch?

Router: Sie vermitteln auf Layer 3-Ebene und werden meist im WAN eingesetzt.
Layer-3-Switch: Dabei handelt es sich um einen Switch, der gewisse Ports routen kann (meist VLAN)

Firewalls

Eine Firewall ist ein Sicherungssystem, das ein Rechnernetz oder einen einzelnen Computer vor unerwünschten Netzwerkzugriffen schützt. Die Firewall-Software dient dazu, den Netzwerkzugriff zu beschränken. Sie überwacht den durch die Firewall laufenden Datenverkehr und entscheidet anhand festgelegter Regeln, ob bestimmte Netzwerkpakete durchgelassen werden oder nicht.

1. Welche Angriffe kann es geben?

- **Mitlesen der Pakete die über Traffic laufen**. Wird meist über den Provider geregelt.
- **Hijacking**: Manipulieren der Daten im TCP Header.
- **Denial of Service Attacke**: Server wird mit Anfragen "überflutet" und somit zum Absturz gebracht.
- **Vieren, Trojaner, Spyware**: Meist in Javascript oder C geschrieben.
- **Internen Angriff**: Person befindet sich im Netzwerk und hat gewisse Zugriffe.
- **Malicious Software**: Reproduzierende Software geeignet für Sniffer oder für Backdoor Einstellungen.

2. Welche Funktionen kann eine Firewall übernehmen?

- **Paketfilter**
- **Application Firewalls** (soll vor Angriffen über HTTP schützen)
- **Logging** (Mitprotokollierung was im Netzwerk geschieht)
- **Alerting** (SMS/EMail an Systemadministrator bei unerlaubtem Zugriff)
- **Authentifizierung** (Benutzername/Passwort für Änderungen der Filterregel)
- **VPN** (Unterstützung von Virtualisierung)

3. Welche Arten von Firewalls gibt es?

Personal Firewall (Desktop Firewall): Dabei handelt es sich um eine auf dem Computer installierte Firewall-Software. Zu ihrer Aufgabe gehört es, ungewollte Zugriffe von außen auf Netzwerkdienste des Computers zu unterbinden. Abhängig vom Produkt kann sie zudem versuchen, Anwendungen davon abzuhalten, ohne das Einverständnis des Anwenders mit der Außenwelt zu kommunizieren.

Externe Firewall (Netzwerk- oder Hardware-Firewall): Sie kontrolliert die Verbindung zwischen zwei Netzen und dient dazu, den Netzwerkzugriff zu beschränken, basierend auf Absender- oder Zieladresse und genutzten Diensten. Sie überwacht den durch die Firewall laufenden Datenverkehr und entscheidet anhand festgelegter Regeln, ob bestimmte Netzwerkpakete durchgelassen werden oder nicht. Auf diese Weise versucht sie, unerlaubte Netzwerkzugriffe zu unterbinden.
Realisiert wird das Konzept bei der externen Firewall durch eine Software, die auf einer eigenen Hardware läuft. Die Hardware ist dabei lediglich für das Empfangen und Senden der einzelnen Datenpakete zuständig und die Software regelt den Verkehr.

4. Welche Komponenten hat eine Firewall?

Ein Firewall-System kann aus ein bis drei Komponenten bestehen:

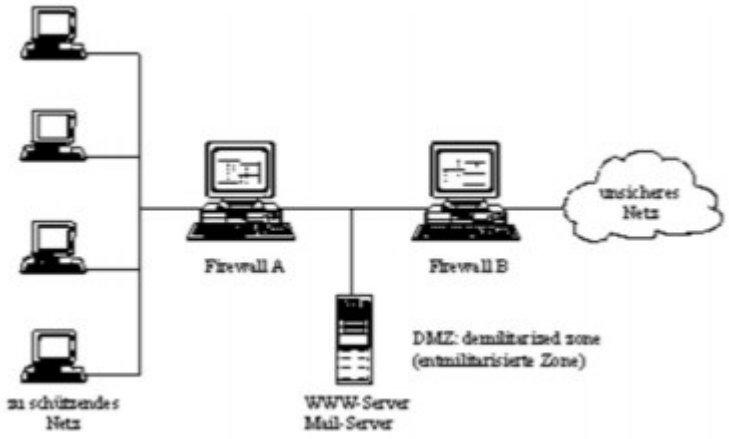
- Paketfilterungs-Router
- Proxy-Server (Application Level Gateway)
- Verbindungs-Gateway (Circuit Level Gateway)

Grundsätzlich konkurrieren zwei Firewall-Konzepte: die "passive" Paketfiltertechnologie und die "aktiven" Application Level Gateways. Alle anderen Firewall-Systeme sind Varianten und Weiterentwicklungen dieser beiden Konzepte oder werden damit kombiniert.
https://www.tecchannel.de/a/firewall-grundlagen,401927,5

5. Was sind einarmige, zweiarmige und dreiarmige Firewalls?

Einarmige Firewall: Sie ist die einzige Schnittstelle zwischen dem zu schützenden Netzwerk und den unsicheren Netzwerken. Für das geschützte Netzwerk gilt eine einheitliches Sicherheitsniveau, somit ist eine weitere Unterscheidung nach Sicherheitsstufen auf Netzebene nicht möglich.

Zweiarmige Firewall: Dabei bedient man sich zwei Firewalls, um dazwischen die DMZ aufzubauen.



Die Firewall B ist eine sogenannte Zentrale Firewall und bietet einen Grundschutz für das Gesamte Netzwerk. Firewall A ist eine Dezentrale Firewall und bietet einen erweiterten Schutz für Subnetze des Netzwerkes.

Grundsätzlich sind zwei armige Firewalls zu bevorzugen, da sie zweistufig ist. Sie benötigt aber mehr administrativen Aufwand und ist teurer. Die zwei Firewalls sollten von unterschiedlichen Herstellern sein, um Fehler zu vermeiden.

Dreiarmige Firewall: Hier ist eine einzige Firewall für LAN, DMZ und WAN zuständig. Sie kann alleine arbeiten.

6. Was ist die DMZ (demilitarisierte Zone)?

Dabei handelt es sich um ein eigenständiges Netzwerk, das als Pufferzone zwischen einem externen Netz und dem internen Netzwerk agiert. In dem Puffernetzwerk befinden sich beispielsweise Webserver oder Mailserver, deren Kommunikation durch Firewalls überwacht ist.

7. Welche Filtertechnologien gibt es?

- **Paketfilter:** Zur Aufgabe einer Paketfilter-Firewall gehört es, Netzwerkpakete anhand ihrer Netzwerkadresse zu sperren oder durchzulassen. Dafür wertet sie die Header-Informationen der Netzwerkpakete aus.
  Pakete können von einer Firewall ausgewertet werden und diese entsprechend filtern, indem sie anhand der Firewall-Regeln entscheidet, welche Anfragen zulässig sind und welche nicht.
- **Stateful Inspection (SPI:** Dabei wird jedes Datenpaket bei der Übertragung auf der Vermittlungsschicht analysiert und als Ergebnis der Analyse wird eine dynamische Zustandstabelle der Verbindung geführt. Dies ermöglicht die Ermittlung der Korrelation zusammengehöriger Datenpakete und einen Abgleich mit einem korrekten Protokollverhalten. Datenpakete die nicht erwarteten Kriterien zugeordnet werden können, also z.B. zu einer DoS-Attacke gehören, werden verworfen.

- **Deep Packet Inspection (DPI):** Das ist eine Erweiterung des SPI. Zusätzlich werden zu den Headerinformationen auch noch die übertragenen Daten gefiltert. Somit können Spammails verhindert werden.
- **Proxy Filter:** Es handelt sich um ein Security System, das die Kommunikation auf Anwendungsebene überwachen und filtern kann. Im Gegensatz zu den rein paketorientiert arbeitenden Firewalls wertet sie nicht nur Adress- und Protokolldaten von IP-Paketen aus, sondern analysiert den Traffic direkt in der Anwendungsschicht (mehr zum Thema Proxy: siehe Frage 8).
- **Content Filter:** Dieser Inhaltsfilter ist eine Form des Proxyfilters, der die Nutzdaten einer Verbindung auswertet und zum Beispiel dafür gedacht ist, ActiveX und/oder JavaScript aus angeforderten Webseiten herauszufiltern oder allgemein bekannte Schadsoftware beim Herunterladen zu blockieren. Auch das Sperren von unerwünschten Webseiten anhand von Schlüsselwörtern und Ähnliches fallen darunter.
  Einfache Content Filter: Sie überprüfen nur das Vorkommen bestimmter Auswahlkriterien.
  Intelligent Content Filter: Sie arbeiten intelligente Filter mit Gewichtungen und weisen eine Seite erst dann zurück, wenn eine bestimmte Relevanz überschritten wird.

8. Was ist ein Proxy?

Der Proxy Server ist ein Vermittler oder Stellvertreter und nimmt Anfragen entgegen, die er unter seiner eigenen Identität weiterleitet. Die Funktion des Proxy Servers kann als zusätzliche Software auf einem Rechner oder auf einem dedizierten Server installiert sein.
Kommt eine Verbindung zwischen einem Client und einem Server zustande, bleiben die Adressen von Client und Server den Kommunikationspartnern jeweils verborgen. Im Gegensatz zu NAT (siehe Glossar) führt der Proxy Server die Kommunikation selbst. Er kann übertragene Pakete analysieren und gegebenenfalls verändern.
Vereinfacht gesagt, geht der Proxy für einen ins Internet.

9. Firewallregeln?

Die Regeln werden für jedes Paket (bei SPI für jede neue Verbindung) der Reihe nach geprüft, und die erste zutreffende Regel wird angewendet. Die Reihenfolge der Regeln ist daher relevant.

Eine Firewall-Regel setzt sich meist aus sechs Komponenten zusammen:

- Absender-IP-Adresse (auch Netzwerk-Adressen wie z. B. 192.168.0.0/24)
- Ziel-IP-Adresse
- Netzwerkprotokoll (TCP, UDP, ICMP, …)
- Port-Nummer (bei TCP und UDP)
- Aktion (erlauben, verwerfen oder ablehnen)
- Protokollieren (engl. "log") ja/nein

Was passiert mit den Paketen?

- **DENY / DROP**: Das Paket wird verworfen, ohne weiter darauf zu reagieren.
- **REJECT:** Das Paket wird verworfen und dem Absender wird mitgeteilt, dass die Verbindung abgelehnt wurde.
- **ALLOW / PASS:** Die Netzwerkanfrage ist erlaubt und wird durchgelassen. Diese Begriffe beziehen sich meist auf den ausgehenden Datenverkehr.
- **FORWARD / PERMIT:** Die Netzwerkanfrage ist erlaubt und wird weitergeleitet. Diese Begriffe beziehen sich vorwiegend auf den eingehenden Datenverkehr .

Port Filterung: Ports werden statisch und dynamisch gefiltert.

- **statisch (0-1023):** Beachten Incoming und Outgoing-Regeln.
  Outgoing (von innen nach außen): offen
  Incoming (von außen nach innen): gesperrt
- **dynamisch (1024- 65535):** Incoming und Outgoing ist eine einzige Regel.

10. Was ist das besondere bei FTP (File Transfer Protocol)?

FTP benötigt jeweils einen eigenen Port für die Verbindung selbst und die Daten (Ports 20 & 21). Eine zweite Verbindung muss beim Verbindungsaufbau dynamische Ports nehmen, da es sonst zwei Sockets auf dem gleichen Port geben würde. Die Firewall führt dann eine SPI durch und leitet das Paket weiter.

Redundante Systeme

Redundanz ist das „Vorhandensein von funktional gleichen Ressourcen in einem technischen System“ .

1. Welche Arten von Redundanz gibt es?

- **Hot Spare:** Die redundante Komponente ist aktiviert und wartet auf Ausfall der Hauptkomponente.
- **Cold Spare:** Fällt die Hauptkomponente aus, wird die redundante Komponente erst aktiviert.
- **Dual System:** Beide (alle) Komponenten arbeiten gleichzeitig an der gleichen Aktion.
- **n + 1:** Es gibt n arbeitende Komponenten und eine passive Standby Komponente.

2. Welche Ausfallverhalten gibt es?

- **Fail-Safe:** Die ausgefallene Einheit steht nicht mehr zur Verfügung und begibt sich in einen beherrschbaren Ausgangszustand.
- **Fail-Passive:** Die Anlage muss aus 2 Fail-Safe-Systemen aufgebaut sein muss und über eine Fehlererkennung und Fehlerunterdrückung verfügen muss. Beide Systeme müssen ihre Ausgangsergebnisse miteinander vergleichen können. Kommen sie zu verschiedenen Ergebnissen, muss das resultierende Ausgangsergebnis null sein. Somit verhält sich die Anlage passiv.
- **Fail-Operational:** Die Anlage arbeitet im Fehlerfall weiter. Sie nimmt keinen Fehlerzustand ein, sie bleibt operativ. Um das zu erreichen, muss die Anlage mindestens aus 3 Systemen bestehen, die ebenfalls über eine Fehlerdiagnose und Fehlerunterdrückung verfügen müssen.

3. Was ist „Hochverfügbarkeit“?

Darunter versteht man die Wahrscheinlichkeit das ein System trotz Ausfall einer oder mehrerer Komponenten den Betrieb aufrecht halten kann.
Dies wird in Verfügbarkeitsklassen eingeteilt (Availabilty Environment Classification (AEC), 9er System).

4. Wie erreicht man Redundanz im Netzwerk?

Spanning Tree (STP): Dabei gibt es einen bevorzugten und einen redunandten Weg. Ergebnis des Spannung Tree Protocols ist eine Baumtopologie, in der keine doppelten Verbindungen zwischen Quelle und Ziel mehr vorhanden sind. Gleichzeitig ist jeder vernetzte Punkt von einem anderen vernetzten Punkt über die bestmögliche Verbindung erreichbar. Kommt es zu einer Unterbrechung einer Verbindung oder zum Ausfall eines Switches, reorganisiert das Spanning Tree Protocol dem Baum und ermittelt neue Verbindungspfade. Die Umschaltzeiten können relativ lange dauern.

Multiple Spanning Tree (MSTP): Dabei handelt es sich um ein standardisiertes Spanning-Tree-Protokoll mit nicht nur einem Spanning Tree, der sich über das gesamte Netzwerk erstreckt, sondern mit mehreren kleineren Spanning Trees, die über ein größeres physikalisches Netz aufgebaut werden können. Bei großen Netzen hat ein einzelner Spanning Tree den Nachteil, dass die Rekonfigurationszeiten relativ lange dauern. Dies kann durch mehrere Spanning Trees mit kürzeren STP-Instanzen vermieden werden.

Rapid Spanning Tree (RSTP): Werden beim STP beim Ausfall einer Netzkomponente (Switch, Bridge etc.) noch sämtliche Verbindungen unterbrochen, bis die neue Topologie berechnet ist, so fallen beim RSTP nur die Pfade aus, die über die defekte Komponente liefen. Ansonsten bleiben die

bisherigen Pfade bestehen, bis die Berechnung der neuen Topologie beendet ist. Die Umschaltung auf die neue Topologie erfolgt dann sehr schnell.

Link Aggregation (Trunking): Link Aggregation fast mehrere parallele Verbindungen zu einer logischen Verbindung zusammen. Dadurch erhöht sich der Datendurchsatz und die Ausfallsicherheit gegenüber einer einfachen Netzwerkschnittstelle.

Resilient TCMP: Dieses Verfahren verteilt Aufgaben an Leitungen, ist teuer. Dazu findet man komischerweise nichts im Internet.

Multipoint Link Aggregation (MPLA): Dabei kommunizieren Switches über redundante Hochleistungsverbindungen miteinander. Alle Server sind an alle Switches angebunden und bei Ausfall wird sofort auf einen anderen geschalten. Es kommt zu symmetrischer Lastverteilung und Clusterbildung, ist aber sehr teuer.

5. Wie erreicht man Redundanz bei Servern?
Serverspiegelung: Dabei wird zur Laufzeit kontinuierlich eine exakte Kopie eines Servers erstellt. Durch Duplizieren des gesamten Inhalts eines Servers auf einem anderen Remote- oder Inhouse-Server können Daten wiederhergestellt werden, wenn der primäre Server ausfällt.

Windows Domäne mit mehreren Domänencontrollern die sich gegenseitig referenzieren:
Fällt der primäre Domänencontroller aus, übernimmt ein anderer seine Funktion.

6. Wie schafft man Redundanz bei der Stromversorgung?
Dies geht durch USV (unterbrechungsfreie Stromversorgung).
Online USV: Diese gelten als echte Stromgeneratoren, die ständig eine eigene Netzspannung erzeugen. Damit werden angeschlossene Verbraucher dauerhaft ohne Einschränkungen mit Netzspannung versorgt. Zeitgleich wird die Batterie aufgeladen.
Interactive USV: Diese werden erst aktiviert, wenn der Strom ausfällt. Die Umschaltzeit von Netzbetrieb auf Batteriebetrieb dauert 2 bis 4 ms.

7. Was sind RAID-Systeme (Redundant Array of Independent Disks)?
Mehrere Festplatten verhalten sich nach außen wie eine.

- **RAID 0:** Hier gibt es zwei Festplatten, die beide Daten enthalten. Redundanz fehlt zwar, dafür kann die Kapazität verdoppelt werden.
- **RAID 1:** Die Daten werden auf zwei Festplatten gespiegelt. Dadurch hat man schnelleren Zugriff (um ¼ Umdrehung), kann aber nur die Hälfte der Gesamtkapazität verwenden.
- **RAID 5:** Hier kommt „Stripping“ zum Einsatz. Bei maximal fünf Festplatten beinhalten vier die datenstreifen und eine einen Paritätsstreifen. Dieser befindet sich immer auf einer anderen Platte.
- **RAID 6:** Dazu benötigt man mind. vier Datenplatten und mind. zwei Paritätsplatten. Dadurch können gleichzeitig zwei Plattenfehler auftreten.
- **RAID 10:** Dabei handelt es sich um eine Kombination aus RAID 0 und RAID 1. Bei mind. vier Festplatten werden die daten immer auf ein Festplattenpaar unterschiedlich (RAID 0) und in einem Festplattenpaar synchron (RAID 1) gespeichert.
- **RAID Kombinationen:** Man kann einzelnen Verfahren kombinieren, um deren Vorteile zu nutzen. RAID 50 besteht beispielsweise aus einem RAID 0, welches aus mehreren RAID 5 besteht.

8. Was ist VRRP (Virtual Router Redundancy Protocol)?
Es handelt sich dabei um ein Internet-Protokoll, womit sich ein oder mehrere Backup-Router betreiben lassen. Mithilfe von VRRP eine virtuelle Adresse als Standard spezifiziert. Diese virtuelle Adresse wird von mehreren Routern gemeinsam genutzt. Das gilt sowohl für den, der als Master definiert ist als auch für den oder die Backups. Fällt der Master nun aus, dann wird die virtuelle IP-Adresse einfach einem der Backup Router zugewiesen. Dessen IP-Adresse wird überschrieben und somit wird der Backup zum Master.

VPN (Virtual Private Network)

VPN ist ein logisches privates Netzwerk auf einer öffentlich zugänglichen Infrastruktur. Nur die Kommunikationspartner, die zu diesem privaten Netzwerk gehören, können miteinander kommunizieren und Informationen und Daten austauschen.

1. Wie funktioniert VPN?

VPN ist ein Netzwerk, dass eine virtualle Verbindung zwischen Nutzern und dem VPN-Server aufbaut. Dieses Netzwerk ist privat, da der Zugriff eine Authentifizierung erfordert.
Ist man eingeloggt, kann eine Verbindung mit dem Server hergestellt werden, welcher dann eine Verbindung zum Internet herstellt. Innerhalb eines (VPN) sind verschiedene Teilnehmer eines IP-Netzwerks zu einem in sich geschützten Teilnetz verbunden. Die Verbindungen sind verschlüsselt. Zwischen den einzelnen Teilnehmern entstehen Tunnelverbindungen, die von außen nicht einsehbar sind.

2. Was ist Tunneling?

Mit einem Tunneling-Protokoll wird eine verschlüsselte Verbindung aufgebaut. Dieser Tunnel erlaubt es, die Pakete eines Netzwerkprotokolls in die Pakete eines anderen einzukapseln. Am Startpunkt werden die Pakete eingekapselt und am Endpunkt wieder ausgekapselt. Dies kann entweder auf Schicht 2 oder Schicht 3 der OSI-Schichtenmodells passieren.

3. Welche Typen von VPN-Verbindungen gibt es?

End-to-Site-VPN (Host-to-Gateway-VPN): Dabei werden die Heimarbeitsplätze oder mobile Benutzer in ein Unternehmensnetzwerk eingebunden. Der externe Mitarbeiter soll so arbeiten, als ob er sich im Netzwerk des Unternehmens befindet.

Site-to-Site-VPN (LAN-to-LAN-VPN): Dieser Typ von VPN wird verwendet, um das Netzwerk des Hauptstandortes mit anderen Niederlassungen zu verbinden, oder um Verbindungen zu anderen Unternehmen herzustellen. Es bildet eine virtuelle Brücke, die Netzwerke an verschiedenen Standorten vereint.

End-to-End-VPN (Host-to-Host-VPN): Ein Client versucht auf einen anderen Client in einem entfernten Netzwerk zuzugreifen. Der VPN-Tunnel erstreckt sich über die gesamte Verbindung zwischen zwei Hosts.

4. Welche VPN-Technologien gibt es (die auch noch genutzt werden)?

a) IPSec (Internet Protocol Security) VPN:

Es ist eine Erweiterung von IP um Verschlüsselungs- und Authentifizierungsmechanismen. Damit erhält das Internet-Protokoll die Fähigkeit IP-Pakete kryptografisch gesichert über öffentliche und unsichere Netze zu transportieren.

Es gibt zwei Übertragungsmodi:

- **Transportmodus:** Dieser stellt Punkt-zu-Punkt-Kommunikation zwischen zwei Endpunkten her. Dafür wird ein zusätzlicher Protokollkopf zwischen den IP-Protokollkopf und den eigentlichen IP-Nutzdaten des betroffenen Pakets eingefügt.
- **Tunnelmodus:** Dieser verbindet zwei Netze über zwei Router.

Die zentralen Funktionen in der IPSec-Architektur sind das AH-Protokoll (Authentification Header), das ESP-Protokoll (Encapsulating Security Payload) und die Schlüsselverwaltung (Key Management).
AH-Protokoll: Es sorgt für die Authentifizierung der zu übertragenen Daten und Protokollinformationen.
ESP-Protokoll: Es erhöht die Datensicherheit in Abhängigkeit des gewählten Verschlüsselungsalgorithmus.

b) SSL (Secure Socket Layer) VPN:

Es ist eine Art Remote-Access-VPN, das eine Alternative zu IPSec darstellt. Während die meisten VPN-Techniken relativ komplex und fehleranfällig sein können, kommt SSL-VPN durch jede Firewall und durch jedes Netzwerk hindurch.
SSL bzw. SSL-VPN beherrscht kein Tunneling und eignet sich deshalb ausschließlich für Remote-Access oder Extranet-Anwendungen. Um Standorte zu vernetzen ist SSL-VPN eher ungeeignet.
SSL-VPN kann über einen Browser, als VPN-Client oder als Kombination von beidem erfolgen.

c) L2TP (Layer 2 Tunneling Protocol) over IPsec

L2TP over IPsec ist eine Kombination aus dem Sicherheitsprotokoll IPsec und dem Tunneling-Protokoll L2TP. L2TP over IPsec setzt L2TP Punkt-zu-Punkt-Verbindungen zwischen zwei virtuellen Netzwerk-Schnittstellen ein. Dabei wird L2TP durch IPsec getunnelt.
Durch die Kombination von L2TP und IPsec haben sich die Schwächen beider Protokolle gegenseitig auf. L2TP und IPsec miteinander zu kombinieren bedeutet, ein flexibles Tunneling-Protokoll mit höchster Sicherheit einsetzen zu können.

5. Welche VPN-Technologien gibt es noch?

- PPTP (Point to Point Tunneling Protocol) VPN
- L2F (Layer 2 Forwarding) VPN
- L2TP (Layer 2 Tunneling Protocol) VPN
- PPP (Point-to-Point Protocol)

6. Welche Technologien setzt man wo ein?

Eine Firma möchte mehrere Standorte miteinander verbinden.

Dazu handelt es sich um eine **Site-to-Site-Verbindung**. Man sollte **IPSec** wählen. Es handelt sich um eine Layer 3 Technologie und man muss am Client nichts einstellen.

Eine Firma möchte einen Mitarbeiter im Außendienst einbinden.
Dabei handelt es sich um eine End-to-Site-verbindung. Man kann entweder IPSec wählen und am Rechner einen VPN-Client installieren oder man entscheidet sich für **L2TP over IPSec.** Bei L2TP läuft das Internet dann nicht mehr über meine Verbindung, sondern über die des VPN-Servers, damit man keine Viren einschleppt.

Ein Kunde soll über das Web zugreifen.
Hier ist **SSL-VPN** die beste Wahl, da der Zugriff über den Webbrowser erfolgen soll und der Kunde nichts installieren muss.

Glossar

Logical Link Control (LLC)	Steuerung der Datenübertragung auf der oberen Teilschicht der Sicherungsschicht (2. Schicht) im OSI-Modell. Die Sicherungsschicht wurde in die Teilschichten Logical Link Control (LLC) und Medium Access Control (MAC) unterteilt.
Destination Service Access Point (DSAP)	Die individuelle Adresse des angesprochenen Dienstzugangspunktes für Zugriff auf die höheren Schichten des Netzwerk-Protokoll-Stacks.
Source Service Access Point (SSAP)	Die individuelle Quelladresse für Zugriff auf die höheren Schichten des Netzwerk-Protokoll-Stacks.
Jumbo-Frame	In Jumbo-Frames passen bis zu 9014 Byte Nutzdaten in ein Ethernet-Frame. Vorher waren es nur 1500 Byte. Der Anteil des Overheads an der Übertragung hat sich durch Jumbo-Frames reduziert.
Network Address Translation (NAT)	NAT ermöglicht es, die Ziel- oder Quell-IP-Adressen eines Datenpakets durch eine andere Adresse zu ersetzen.