# OSI-Modell

OSI-Modell – Geräte & Firewall-Bezug IHK-sichere Hauptzuordnung der Schichten, Geräte und Firewall-Arten  Schicht Name Worum geht es? Typische Geräte / Komponenten Firewall-Bezug Layer 7 Anwendungs- schicht Anwendungen und Dienste Proxy, Application Gateway, Webserver, DNS-Server ▣ ◉ ▤ ◌ Proxy-Firewall, Application-Level Gateway, WAF, NGFW-Anwendungsfilter Layer 6 Darstellungs- schicht Datenformat, Verschlüsselung, Komprimierung meist keine klassischen Netzwerkgeräte; ggf. TLS-/SSL-Proxy Prüfung hier meist nur bei TLS-Inspection  Layer 5 Sitzungs- schicht Aufbau, Verwaltung und Abbau von Sitzungen meist keine klassischen Netzwerkgeräte; teilweise Proxy/Gateway für die IHK eher Zusatzwissen, nicht Haupt-Firewall-Schicht  Layer 4 Transport- schicht Ports, Ende-zu-Ende- Verbindungen, TCP/UDP Firewall, Load Balancer ▦ ⚖ Stateful Firewall, Portfilter, TCP-/UDP-Regeln  Layer 3 Vermittlungs- schicht IP-Adressierung und Routing zwischen Netzen Router, Layer-3-Switch, Firewall ◎ ⇄ ▦ Paketfilter-Firewall, ACLs, IP-Filter  Layer 2 Sicherungs- schicht Kommunikation im lokalen Netz über MAC-Adressen Switch, Bridge, Access Point, Netzwerkkarte ▤ ≋ ◖ VLAN-Trennung, MAC-Filter, transparente/Bridge-Firewall als Sonderfall  Layer 1 Bitübertragungs- schicht Physische Übertragung von Bits Kabel, Hub, Repeater, Medienkonverter ⌁ ▭ ↻ Keine klassische Firewall-Funktion  Wichtige IHK-Merksätze ✓ Layer 2 = MAC / Switch ✓ Layer 3 = IP / Router / Paketfilter ✓ Layer 4 = TCP/UDP / Ports / Stateful Firewall ✓ Layer 7 = Anwendung / Proxy / WAF  Wichtiger Hinweis Reale Geräte können mehrere OSI-Schichten abdecken. Für die IHK ist meistens die Hauptzuordnung entscheidend.

Kurz merken: Switch = Layer 2 · Router = Layer 3 · Stateful Firewall = Layer 3/4 · Proxy/WAF = Layer 7 · NGFW = Layer 3 bis 7

**OSI-Modell – Geräte und Firewall-Bezug (IHK-sicher)**

Das OSI-Modell teilt Netzwerkkommunikation in **7 Schichten** ein. Für die IHK ist wichtig, dass du nicht nur die Namen der Schichten kennst, sondern auch verstehst, **welche Aufgabe die jeweilige Schicht hat**, **welche Geräte dort typischerweise arbeiten** und **welche Firewall-Art dazu passt**.

Wichtig: Das OSI-Modell ist ein **theoretisches Referenzmodell**. Reale Geräte arbeiten oft auf mehreren Schichten gleichzeitig. Für Prüfungsaufgaben zählt meistens die **Hauptzuordnung**.

| OSI-Schicht | Name | Worum geht es? | Typische Geräte / Komponenten | Firewall-Bezug |
|---|---|---|---|---|
| **7** | **Anwendungsschicht** | Anwendungen und Dienste | Proxy, Application Gateway, Webserver, DNS-Server | Proxy-Firewall, Application-Level Gateway, WAF, NGFW-Anwendungsfilter |
| **6** | **Darstellungsschicht** | Datenformat, Verschlüsselung, Komprimierung | meist keine klassischen Netzwerkgeräte; ggf. TLS-/SSL-Proxy | Prüfung hier meist nur bei TLS-Inspection |

| OSI-Schicht | Name | Worum geht es? | Typische Geräte / Komponenten | Firewall-Bezug |
|---|---|---|---|---|
| **5** | **Sitzungsschicht** | Aufbau, Verwaltung und Abbau von Sitzungen | meist keine klassischen Netzwerkgeräte; teilweise Proxy-/Gateway-Funktionen | Für die IHK eher Zusatzwissen, nicht die Haupt-Firewall-Schicht |
| **4** | **Transportschicht** | Ports, Ende-zu-Ende-Verbindungen, TCP/UDP | Firewall, Load Balancer | Stateful Firewall, Portfilter, TCP-/UDP-Regeln |
| **3** | **Vermittlungsschicht** | IP-Adressierung und Routing zwischen Netzen | Router, Layer-3-Switch, Firewall | Paketfilter-Firewall, ACLs, IP-Filter |
| **2** | **Sicherungsschicht** | Kommunikation im lokalen Netz über MAC-Adressen | Switch, Bridge, Access Point, Netzwerkkarte | VLAN-Trennung, MAC-Filter, transparente/Bridge-Firewall als Sonderfall |
| **1** | **Bitübertragungsschicht** | Physische Übertragung von Bits | Kabel, Hub, Repeater, Medienkonverter | Keine klassische Firewall-Funktion |

---

### Layer 7 – Anwendungsschicht

Die **Anwendungsschicht** ist die oberste Schicht des OSI-Modells. Hier befinden sich Netzwerkdienste und Anwendungen, mit denen Benutzer oder Programme arbeiten.

Typische Beispiele sind:

- HTTP
- HTTPS
- DNS
- SMTP
- FTP
- IMAP
- SSH

Auf dieser Schicht geht es nicht mehr nur darum, **welche IP-Adresse** oder **welcher Port** verwendet wird, sondern darum, **welche Anwendung oder welcher Dienst** tatsächlich kommuniziert.

Beispiel:

Wenn ein Benutzer eine Webseite aufruft, findet die eigentliche Webkommunikation über HTTP oder HTTPS auf der Anwendungsschicht statt.

Typische Komponenten:

- Proxy
- Application Gateway
- Webserver
- DNS-Server
- Web Application Firewall (WAF)

Firewall-Bezug:

Eine **Proxy-Firewall** oder ein **Application-Level Gateway** arbeitet auf Anwendungsebene. Sie betrachtet nicht nur IP-Adressen und Ports, sondern kann anwendungsbezogene Inhalte prüfen.

Eine **WAF** schützt speziell Webanwendungen. Sie prüft HTTP- und HTTPS-Anfragen zum Beispiel auf Angriffe wie SQL-Injection oder Cross-Site-Scripting.

Eine **NGFW** kann ebenfalls Anwendungen erkennen und filtern, zum Beispiel Webmail, Streaming, Messenger oder andere Dienste.

IHK-Merksatz:

**Layer 7 = Anwendung, Inhalte, Proxy, WAF**

---

**Layer 6 – Darstellungsschicht**

Die **Darstellungsschicht** kümmert sich darum, wie Daten dargestellt, codiert, verschlüsselt oder komprimiert werden.

Typische Aufgaben:

- Datenformate umwandeln
- Zeichencodierung festlegen
- Daten komprimieren
- Daten verschlüsseln oder entschlüsseln

Typische Beispiele:

- TLS/SSL
- UTF-8
- JPEG
- PNG
- Komprimierung

Für die IHK ist wichtig: Layer 6 ist eher eine theoretische Schicht. In vielen praktischen Netzwerkaufgaben stehen Layer 2, 3, 4 und 7 stärker im Vordergrund.

Firewall-Bezug:

Eine Firewall kann verschlüsselten HTTPS-Verkehr nicht vollständig inhaltlich prüfen, solange sie den Verkehr nicht entschlüsselt. Eine tiefere Inhaltsprüfung ist nur mit **TLS-Inspection** beziehungsweise **SSL-Inspection** möglich.

Wichtig: TLS/SSL wird in Lernunterlagen oft der Darstellungsschicht zugeordnet, in der Praxis liegt es technisch zwischen Anwendung und Transport. Für IHK-Lernzwecke reicht: **Layer 6 = Verschlüsselung, Darstellung, Datenformat**.

IHK-Merksatz:

**Layer 6 = Darstellung, Format, Verschlüsselung, Komprimierung**

---

**Layer 5 – Sitzungsschicht**

Die **Sitzungsschicht** ist für den Aufbau, die Verwaltung und den Abbau von Sitzungen zuständig.

Eine Sitzung ist ein logischer Kommunikationszusammenhang zwischen zwei Systemen. Dabei geht es zum Beispiel darum, eine Verbindung beziehungsweise einen Dialog zu starten, aufrechtzuerhalten und sauber zu beenden.

Typische Aufgaben:

- Sitzung aufbauen
- Sitzung verwalten
- Sitzung beenden
- Dialogsteuerung
- Wiederaufnahme von Kommunikationsabläufen

Für die IHK ist wichtig: Layer 5 ist meistens weniger praxisnah als Layer 2, 3, 4 und 7. In Firewall-Fragen wird Layer 5 normalerweise nicht als wichtigste Schicht abgefragt.

Firewall-Bezug:

Manche Gateway- oder Proxy-Funktionen können sitzungsbezogene Informationen berücksichtigen. Für die Prüfung solltest du aber vor allem diese klare Zuordnung lernen:

- Paketfilter-Firewall = Layer 3/4
- Stateful Firewall = Layer 3/4
- Proxy-Firewall = Layer 7
- WAF = Layer 7
- NGFW = Layer 3 bis 7

IHK-Merksatz:

**Layer 5 = Sitzung aufbauen, verwalten und beenden**

---

**Layer 4 – Transportschicht**

Die **Transportschicht** regelt die Kommunikation zwischen Anwendungen auf zwei Systemen. Hier sind vor allem **TCP**, **UDP** und **Ports** wichtig.

Wichtige Begriffe:

- TCP
- UDP
- Portnummern
- Verbindungen
- Verbindungsstatus
- Ende-zu-Ende-Kommunikation

TCP ist verbindungsorientiert. Das bedeutet: Es wird eine Verbindung aufgebaut, Daten werden geordnet übertragen und der Empfang kann bestätigt werden.

UDP ist verbindungslos. Das bedeutet: Es ist einfacher und schneller, bietet aber keine gleiche zuverlässige Verbindungssteuerung wie TCP.

Typische Ports:

| Dienst | Protokoll / Port |
|---|---|
| HTTP | TCP 80 |
| HTTPS | TCP 443 |
| DNS | UDP/TCP 53 |
| SSH | TCP 22 |
| RDP | TCP 3389 |
| SMTP | TCP 25 |

Typische Geräte / Komponenten:

- Firewall
- Layer-4-Load-Balancer

Firewall-Bezug:

Eine Firewall kann auf Layer 4 prüfen, welche Ports und Transportprotokolle verwendet werden.

Eine **Stateful Firewall** prüft zusätzlich, ob ein Paket zu einer bereits erlaubten Verbindung gehört. Sie führt dafür eine Verbindungstabelle.

Beispiel:

Ein Client aus dem internen Netzwerk baut eine HTTPS-Verbindung zu einem Webserver auf. Die Antwortpakete aus dem Internet werden erlaubt, weil sie zu dieser bestehenden Verbindung gehören.

IHK-Merksatz:

**Layer 4 = TCP/UDP, Ports, Verbindungen, Stateful Firewall**

---

**Layer 3 – Vermittlungsschicht**

Die **Vermittlungsschicht** ist für IP-Adressierung und Routing zuständig. Hier wird entschieden, wie Datenpakete von einem Netzwerk in ein anderes Netzwerk gelangen.

Wichtige Themen:

- IPv4
- IPv6
- Routing
- Subnetze
- Standardgateway
- ICMP
- IPsec
- Paketweiterleitung

Typische Geräte:

- Router
- Layer-3-Switch
- Firewall

Ein Router verbindet unterschiedliche Netzwerke miteinander. Er entscheidet anhand der Ziel-IP-Adresse, wohin ein Paket weitergeleitet wird.

Ein Layer-3-Switch kann zusätzlich zu klassischen Switch-Funktionen auch Routing-Funktionen übernehmen, zum Beispiel zwischen VLANs.

Firewall-Bezug:

Eine Paketfilter-Firewall prüft auf Layer 3 zum Beispiel:

- Quell-IP-Adresse
- Ziel-IP-Adresse
- Protokoll
- Netzbereich
- Richtung des Datenverkehrs

Sobald zusätzlich Ports geprüft werden, ist auch Layer 4 beteiligt. Deshalb ist die IHK-sichere Formulierung:

**Paketfilter-Firewall = Layer 3/4**

Beispielregel:

Ein internes Netz `192.168.10.0/24` darf per TCP-Port `443` ins Internet, aber nicht per TCP-Port `23`.

IHK-Merksatz:

**Layer 3 = IP-Adresse, Routing, Router, Paketfilter**

---

**Layer 2 – Sicherungsschicht**

Die **Sicherungsschicht** ist für die Kommunikation im lokalen Netzwerk zuständig. Hier geht es vor allem um **MAC-Adressen**, **Ethernet-Frames**, **Switching** und **VLANs**.

Wichtige Themen:

- MAC-Adressen
- Ethernet-Frames
- Switches
- Bridges
- VLANs
- ARP
- WLAN im lokalen Netz
- Fehlererkennung auf Frame-Ebene

Typische Geräte:

- Switch
- Bridge
- Access Point
- Netzwerkkarte

Ein Switch arbeitet hauptsächlich auf Layer 2. Er lernt MAC-Adressen und leitet Frames an den passenden Port weiter.

Für die IHK ist sehr wichtig:

**Switch = MAC-Adresse = Layer 2**

Ein Switch verwendet also normalerweise MAC-Adressen, während ein Router IP-Adressen verwendet.

Firewall-Bezug:

Layer 2 ist nicht die klassische Firewall-Schicht. Trotzdem gibt es sicherheitsrelevante Funktionen auf Layer 2:

- VLAN-Trennung
- MAC-Filter
- Port-Security
- transparente Firewall / Bridge-Firewall als Sonderfall

Wichtig: MAC-Filter allein sind kein starker Schutz, weil MAC-Adressen gefälscht werden können. Für IHK-Grundlagen reicht aber die Einordnung: MAC-Adressen gehören zu Layer 2.

IHK-Merksatz:

**Layer 2 = MAC-Adresse, Switch, lokales Netzwerk**

---

**Layer 1 – Bitübertragungsschicht**

Die **Bitübertragungsschicht** ist die unterste Schicht des OSI-Modells. Hier geht es um die physische Übertragung von Bits.

Wichtige Themen:

- elektrische Signale
- optische Signale
- Funkübertragung
- Kabel
- Stecker
- Netzwerkkarte auf physischer Ebene
- Repeater
- Hub
- Medienkonverter

Typische Geräte und Komponenten:

- Netzwerkkabel
- Glasfaserkabel
- Hub
- Repeater
- Medienkonverter
- Stecker und Ports

Ein Hub arbeitet auf Layer 1. Er verteilt Signale, trifft aber keine intelligenten Weiterleitungsentscheidungen wie ein Switch.

Ein Repeater arbeitet ebenfalls auf Layer 1. Er verstärkt oder erneuert ein Signal.

Firewall-Bezug:

Auf Layer 1 gibt es keine klassische Firewall-Funktion. Eine Firewall entscheidet nicht anhand von reinen elektrischen oder optischen Signalen, sondern anhand von Informationen höherer Schichten.

IHK-Merksatz:

**Layer 1 = Kabel, Signal, Bits, physische Übertragung**

---

## Firewall-Arten und OSI-Zuordnung

| Firewall-Art | OSI-Zuordnung | Prüft hauptsächlich | Wichtig für die IHK |
|---|---|---|---|
| **Paketfilter-Firewall** | **Layer 3/4** | IP-Adressen, Protokolle, Ports | einfache Filterregeln |
| **Stateful Firewall** | **Layer 3/4** | IPs, Ports und Verbindungsstatus | merkt sich erlaubte Verbindungen |
| **Proxy-Firewall** | **Layer 7** | Anwendungsdaten und Inhalte | arbeitet stellvertretend für den Client |
| **Application-Level Gateway** | **Layer 7** | anwendungsspezifische Protokolle | prüft Inhalte auf Anwendungsebene |
| **WAF** | **Layer 7** | HTTP-/HTTPS-Anfragen an Webanwendungen | Schutz für Webanwendungen |
| **NGFW** | **Layer 3 bis 7** | IPs, Ports, Anwendungen, Inhalte | kombiniert mehrere Sicherheitsfunktionen |
| **Hardware-Firewall** | keine eigene OSI-Schicht | abhängig von Funktion | Bauform, nicht OSI-Schicht |
| **Software-Firewall** | keine eigene OSI-Schicht | abhängig von Funktion | Installationsart, nicht OSI-Schicht |

---

## Wichtige IHK-Merksätze

| Thema | Merksatz |
|---|---|
| **Switch** | arbeitet hauptsächlich auf Layer 2 |
| **Router** | arbeitet hauptsächlich auf Layer 3 |
| **Hub** | arbeitet auf Layer 1 |
| **Repeater** | arbeitet auf Layer 1 |
| **Bridge** | arbeitet hauptsächlich auf Layer 2 |
| **Portfilter** | arbeitet hauptsächlich auf Layer 4 |
| **Paketfilter** | arbeitet auf Layer 3/4 |
| **Stateful Firewall** | arbeitet auf Layer 3/4 und merkt sich Verbindungen |

| Thema | Merksatz |
|---|---|
| **Proxy-Firewall** | arbeitet auf Layer 7 |
| **WAF** | arbeitet auf Layer 7 |
| **NGFW** | kann Layer 3 bis Layer 7 auswerten |
| **Layer 6 und 5** | eher theoretisch, bei Firewall-Zuordnung meist Zusatzwissen |

---

### Ganz kurzer Prüfungs-Merksatz

### Layer 2 = MAC / Switch

### Layer 3 = IP / Router / Paketfilter

### Layer 4 = TCP/UDP / Ports / Stateful Firewall

### Layer 7 = Anwendung / Proxy / WAF

---

### Beispiel zur Einordnung

Ein Benutzer öffnet eine Webseite über HTTPS.

| Schritt | OSI-Schicht | Erklärung |
|---|---:|---|
| Kabel oder WLAN überträgt Signale | Layer 1 | Bits werden physisch übertragen |
| Der Switch leitet Frames im lokalen Netz weiter | Layer 2 | Weiterleitung anhand von MAC-Adressen |
| Der Router leitet Pakete ins Internet | Layer 3 | Weiterleitung anhand von IP-Adressen |
| Die Verbindung nutzt TCP-Port 443 | Layer 4 | Kommunikation über TCP und Portnummer |
| TLS verschlüsselt die Verbindung | Layer 6 | Verschlüsselung und Darstellung |
| Der Browser ruft eine Webseite per HTTPS auf | Layer 7 | Anwendungsebene |
| Eine Stateful Firewall erlaubt Antwortpakete | Layer 3/4 | Verbindung wurde vorher erlaubt |
| Eine WAF prüft HTTP-/HTTPS-Anfragen | Layer 7 | Schutz der Webanwendung |

---

### Typische Prüfungsfallen

| Falsche oder ungenaue Aussage | Besser / IHK-sicher |
|---|---|
| Eine Firewall arbeitet immer nur auf Layer 3 | Kommt auf die Firewall-Art an |
| Paketfilter arbeitet nur auf Layer 3 | Besser: Paketfilter arbeitet Layer 3/4 |

| Falsche oder ungenaue Aussage | Besser / IHK-sicher |
|---|---|
| Eine WAF schützt das ganze Netzwerk vollständig | Eine WAF schützt vor allem Webanwendungen auf Layer 7 |
| Hardware-Firewall ist eine eigene OSI-Schicht | Nein, Hardware beschreibt nur die Bauform |
| Switch und Router machen dasselbe | Nein, Switch = Layer 2 / MAC, Router = Layer 3 / IP |
| Layer 6 und 5 sind die wichtigsten Firewall-Schichten | Nein, für Firewalls sind meist Layer 3/4 und Layer 7 wichtig |

Revision #1
Created 21 May 2026 02:28:22 by Admin
Updated 3 June 2026 06:18:12 by Admin