50 Fragen und Antworten: Schicht 4, Ports, NAT, Firewall und DMZ

50 Fragen und Antworten: Schicht 4, Ports, NAT, Firewall und DMZ

---

1. Was ist die Aufgabe der Schicht 4 im Netzwerkmodell?

Die Schicht 4 ist die Transportschicht. Sie sorgt dafür, dass Daten nicht nur beim richtigen Rechner ankommen, sondern auch bei der richtigen Anwendung oder dem richtigen Dienst auf diesem Rechner.

---

2. Warum reicht eine IP-Adresse allein nicht aus?

Eine IP-Adresse bestimmt nur den Zielrechner. Auf einem Rechner können aber mehrere Dienste gleichzeitig laufen, zum Beispiel Webserver, Maildienst oder Dateifreigabe. Deshalb braucht man zusätzlich einen Port, um den richtigen Dienst anzusprechen.

---

3. Was ist ein Port?

Ein Port ist eine Nummer, über die ein bestimmter Dienst oder eine Anwendung auf einem Rechner angesprochen wird.

Beispiel:

```
192.168.1.11:80
```

Die IP-Adresse ist `192.168.1.11`.
Der Port ist `80`.
Port 80 steht typischerweise für HTTP.

---

4. Was ist ein Socket?

Ein Socket ist die Kombination aus IP-Adresse und Port.

```
Socket = IP-Adresse + Port
```

Beispiel:

```
192.168.1.11:80
```

---

5. Was bedeutet die Schreibweise 192.168.1.11:80?

Diese Schreibweise bedeutet:

```
192.168.1.11 = Zielhost
80           = Zielport
```

Der Zugriff geht also an den Rechner mit der IP-Adresse `192.168.1.11` und dort an den Dienst auf Port `80`.

---

6. Wie schreibt man eine IPv6-Adresse mit Port korrekt?

Bei IPv6 muss die Adresse in eckige Klammern gesetzt werden, damit der Port eindeutig erkennbar ist.

```
[2001:1234:5678:90AB:CDEF:1A2B:3C4D:5E6F]:80
```

Ohne Klammern wäre nicht klar erkennbar, wo die IPv6-Adresse endet und wo der Port beginnt.

---

7. In welche drei Bereiche werden Ports eingeteilt?

Ports werden in drei Bereiche eingeteilt:

```
0 bis 1023      = System Ports
1024 bis 49151  = User Ports
49152 bis 65535 = Dynamic/Private Ports
```

8. Was sind System Ports?

System Ports sind die bekannten Ports von `0` bis `1023`. Sie werden für wichtige Standarddienste verwendet.

Beispiele:

```
22  = SSH
53  = DNS
80  = HTTP
443 = HTTPS
```

9. Was sind User Ports?

User Ports liegen im Bereich von `1024` bis `49151`. Sie werden für registrierte Anwendungen und Dienste verwendet.

Beispiele:

```
3128  = Squid Proxy
3306  = MySQL
9100  = Druckerport
10000 = Webmin
```

10. Was sind Dynamic oder Private Ports?

Dynamic oder Private Ports liegen im Bereich von `49152` bis `65535`.

Sie werden oft automatisch und kurzfristig von Clients verwendet, wenn eine Verbindung aufgebaut wird.

11. Welcher Port wird typischerweise für HTTP verwendet?

HTTP verwendet typischerweise Port `80`.

```
HTTP = Port 80
```

---

12. Welcher Port wird typischerweise für HTTPS verwendet?

HTTPS verwendet typischerweise Port `443`.

```
HTTPS = Port 443
```

---

13. Welcher Port wird typischerweise für SSH verwendet?

SSH verwendet typischerweise Port `22`.

```
SSH = Port 22
```

SSH wird häufig zur sicheren Fernadministration von Linux-Systemen genutzt.

---

14. Welcher Port wird typischerweise für DNS verwendet?

DNS verwendet typischerweise Port `53`.

DNS nutzt meistens UDP, kann aber in bestimmten Fällen auch TCP verwenden.

---

15. Welche Ports verwendet DHCP?

DHCP verwendet die Ports `67` und `68`.

```
Port 67 = DHCP-Server
Port 68 = DHCP-Client
```

DHCP nutzt UDP.

---

16. Was ist UDP?

UDP ist ein verbindungsloses Transportprotokoll.

Eigenschaften:

```
schnell
wenig Verwaltungsaufwand
keine feste Verbindung
keine Garantie für Zustellung
keine eingebaute Reihenfolgekontrolle
```

---

17. Wann wird UDP häufig verwendet?

UDP wird häufig verwendet, wenn Geschwindigkeit wichtiger ist als vollständige Kontrolle.

Beispiele:

```
DNS
DHCP
NTP
Streaming
VoIP
Online-Gaming
```

---

18. Was ist TCP?

TCP ist ein verbindungsorientiertes Transportprotokoll.

Eigenschaften:

```
Verbindungsaufbau
Bestätigung empfangener Daten
Kontrolle der Reihenfolge
zuverlässige Datenübertragung
```

```
mehr Verwaltungsaufwand als UDP
```

19. Wann wird TCP häufig verwendet?

TCP wird genutzt, wenn Daten zuverlässig und vollständig übertragen werden müssen.

Beispiele:

```
HTTP
HTTPS
SSH
FTP
SMTP
IMAP
POP3
SMB
```

20. Was ist der wichtigste Unterschied zwischen TCP und UDP?

TCP ist verbindungsorientiert und kontrolliert die Übertragung.
UDP ist verbindungslos und schneller, aber ohne eingebaute Zustellgarantie.

Kurz:

```
TCP = zuverlässig, aber aufwendiger
UDP = schneller, aber weniger kontrolliert
```

21. Was ist der TCP-3-Wege-Handshake?

Der TCP-3-Wege-Handshake ist der Verbindungsaufbau bei TCP.

Ablauf:

```
1. Client -> Server: SYN
2. Server -> Client: SYN + ACK
3. Client -> Server: ACK
```

Danach ist die TCP-Verbindung aufgebaut.

---

22. Wofür steht SYN?

SYN steht für Synchronisation.

Beim TCP-Verbindungsaufbau sendet der Client zuerst ein SYN-Paket an den Server, um eine Verbindung zu starten.

---

23. Wofür steht ACK?

ACK steht für Acknowledgement, also Bestätigung.

Ein ACK bestätigt, dass ein Paket oder ein Verbindungsschritt angekommen ist.

---

24. Wie wird eine TCP-Verbindung kontrolliert abgebaut?

Der TCP-Verbindungsabbau erfolgt typischerweise in vier Schritten:

```
1. FIN
2. ACK
3. FIN
4. ACK
```

Merksatz:

```
TCP-Aufbau = 3 Schritte
TCP-Abbau  = 4 Schritte
```

---

25. Was ist ein SYN-Flood-Angriff?

Bei einem SYN-Flood-Angriff werden sehr viele SYN-Anfragen an einen Server gesendet.

Der Server reserviert Ressourcen für halboffene Verbindungen. Wenn die abschließende Bestätigung ausbleibt, können diese Ressourcen blockiert werden.

Das kann zu einer Überlastung des Servers führen.

---

26. Was ist QUIC?

QUIC ist ein modernes Transportprotokoll, das auf UDP basiert.

Es soll Geschwindigkeit, Zuverlässigkeit und Verschlüsselung verbinden.

Kurz:

```
QUIC = UDP-Basis + moderne Verbindungskontrolle + Verschlüsselung
```

---

27. Warum ist QUIC im modernen Web wichtig?

QUIC ist wichtig, weil es schnelle Verbindungen ermöglichen soll und gleichzeitig Verschlüsselung fest integriert.

Es wird vor allem für moderne Webkommunikation eingesetzt.

---

28. Was ist Portknocking?

Portknocking bedeutet, dass bestimmte Ports in einer festgelegten Reihenfolge angesprochen werden müssen.

Nur wenn die Reihenfolge stimmt, wird eine Aktion ausgelöst.

Beispiel:

```
Port 1111
Port 2222
Port 3333
```

Erst danach wird ein Dienst freigegeben oder ein Ereignis ausgelöst.

---

29. Was ist der Vorteil von Portknocking?

Der Vorteil ist, dass ein Dienst nicht dauerhaft offen sichtbar sein muss.

Er wird erst nach der richtigen „Anklopf-Reihenfolge“ erreichbar oder aktiviert.

---

30. Ist Portknocking ein Ersatz für sichere Authentifizierung?

Nein.

Portknocking kann eine zusätzliche Schutzmaßnahme sein, ersetzt aber keine sichere Authentifizierung, keine starken Passwörter und keine sauber abgesicherten Dienste.

---

31. Was ist Portforwarding?

Portforwarding leitet eine Anfrage von außen an einen internen Dienst weiter.

Beispiel:

```
11.1.2.4:80 -> 192.168.178.11:80
```

Eine externe Anfrage an Port `80` der öffentlichen Adresse wird an den internen Webserver weitergeleitet.

---

32. Was ist Destination NAT?

Destination NAT bedeutet, dass die Zieladresse oder der Zielport eines Pakets verändert wird.

Beim Portforwarding wird zum Beispiel aus:

```
11.1.2.4:80
```

intern:

```
192.168.178.11:80
```

---

33. Warum kann Portforwarding gefährlich sein?

Portforwarding öffnet einen Weg aus dem Internet in das interne Netzwerk.

Wenn der interne Dienst schlecht abgesichert oder veraltet ist, kann das ein Sicherheitsrisiko darstellen.

---

34. Welche sichere Alternative gibt es oft zu Portforwarding?

Eine sichere Alternative ist häufig ein VPN oder ein privater Zugriffsdienst wie Tailscale.

Dann muss ein Dienst nicht direkt öffentlich aus dem Internet erreichbar sein.

---

35. Was ist NAT?

NAT bedeutet Network Address Translation.

Dabei werden IP-Adressen beim Übergang zwischen zwei Netzen umgeschrieben.

Im Heimnetz wird meist die private interne IP-Adresse durch die öffentliche IP-Adresse des Routers ersetzt.

---

36. Was ist PAT?

PAT bedeutet Port Address Translation.

Dabei teilen sich mehrere interne Geräte eine öffentliche IP-Adresse. Der Router unterscheidet die Verbindungen über Ports.

Kurz:

```
Viele interne Geräte -> eine öffentliche IP
Unterscheidung über Ports
```

---

37. Was ist Source NAT?

Source NAT bedeutet, dass die Quelladresse eines Pakets verändert wird.

Beispiel:

```
Interner PC: 192.168.178.11
Router extern: 11.1.2.4
```

Wenn der PC ins Internet geht, ersetzt der Router die private Quelladresse durch seine öffentliche Adresse.

---

38. Was ist der Unterschied zwischen NAT/PAT und Portforwarding?

NAT/PAT wird verwendet, wenn interne Geräte nach außen ins Internet kommunizieren.

Portforwarding wird verwendet, wenn externe Geräte von außen auf einen internen Dienst zugreifen sollen.

Kurz:

```
NAT/PAT       = innen nach außen
Portforwarding = außen nach innen
```

---

39. Was ist eine Allowlist?

Eine Allowlist arbeitet nach dem Prinzip:

```
Alles ist verboten, außer es ist ausdrücklich erlaubt.
```

Nur Einträge, die auf der Allowlist stehen, dürfen genutzt werden.

---

40. Was ist eine Blocklist?

Eine Blocklist arbeitet nach dem Prinzip:

```
Alles ist erlaubt, außer es ist ausdrücklich verboten.
```

Nur Einträge, die auf der Blocklist stehen, werden gesperrt.

---

41. Was ist strenger: Allowlist oder Blocklist?

Eine Allowlist ist strenger.

Bei einer Allowlist ist zunächst alles verboten. Nur ausdrücklich erlaubte Ziele oder Dienste dürfen genutzt werden.

---

42. Was ist der Nachteil einer reinen Allowlist?

Eine reine Allowlist hat einen hohen Pflegeaufwand.

Jede erlaubte Webseite, jeder erlaubte Dienst oder jedes erlaubte Ziel muss vorher eingetragen werden.

---

43. Was ist der Nachteil einer reinen Blocklist?

Eine Blocklist ist nie vollständig.

Neue gefährliche oder unerwünschte Seiten können fehlen und dadurch trotzdem erreichbar sein.

44. Was ist SquidGuard?

SquidGuard ist ein Filterwerkzeug, das Webseiten anhand von Listen oder Kategorien blockieren oder erlauben kann.

Beispiele für Kategorien:

```
Dating
Mailing
Hacking
Werbung
Malware
Glücksspiel
```

45. Was ist eine Firewall?

Eine Firewall kontrolliert Netzwerkverkehr anhand von Regeln.

Sie entscheidet, ob ein Paket erlaubt oder blockiert wird.

Kurz:

```
Firewall = kontrolliert Datenverkehr
```

46. Was ist eine Personal-Firewall?

Eine Personal-Firewall schützt einen einzelnen Rechner.

Sie läuft direkt auf dem PC oder Server und kontrolliert dessen ein- und ausgehenden Netzwerkverkehr.

47. Was ist eine Unternehmens-Firewall?

Eine Unternehmens-Firewall schützt ein ganzes Netzwerk oder mehrere Teilnetze.

Sie steht meistens zwischen internem LAN und externem Netz beziehungsweise Internet.

---

48. Was ist der Unterschied zwischen Paketfilter und Stateful Packet Inspection?

Ein einfacher Paketfilter prüft einzelne Pakete anhand von Regeln.

Eine Stateful-Packet-Inspection-Firewall merkt sich zusätzlich den Zustand einer Verbindung.

Vorteil von SPI:

```
Der Hinweg wird erlaubt.
Der passende Rückweg wird automatisch erkannt.
```

---

49. Was bedeuten INPUT, OUTPUT und FORWARD bei iptables?

Bei iptables gibt es wichtige Regelketten:

```
INPUT   = Verkehr zur Firewall selbst
OUTPUT  = Verkehr von der Firewall selbst nach außen
FORWARD = Verkehr durch die Firewall hindurch
```

Beispiele:

```
INPUT   = SSH-Zugriff auf die Firewall
OUTPUT  = Firewall fragt NTP-Server ab
FORWARD = PC im LAN geht über Firewall ins Internet
```

---

50. Was ist eine DMZ und warum ist sie sinnvoll?

Eine DMZ ist eine demilitarisierte Zone, also ein separates Zwischennetz.

Dort stehen Server, die von außen erreichbar sein müssen, zum Beispiel:

```
Webserver
Mailserver
DNS-Server
Reverse Proxy
```

Der Vorteil:

Wenn ein Server in der DMZ angegriffen wird, befindet er sich nicht direkt im internen LAN.

Kurz:

```
DMZ = Sicherheitszone zwischen Internet und internem Netzwerk
```

Revision #1
Created 27 May 2026 11:04:29 by Admin
Updated 3 June 2026 06:18:12 by Admin