11.6 Merksätze und Prüfungswissen zu Firewalls, NAT und DMZ

Diese Seite fasst die wichtigsten Inhalte zu Firewalls, NAT, PAT, Portweiterleitung und DMZ zusammen.

Diese Themen gehören zu den wichtigsten Grundlagen der Netzwerksicherheit.

Wichtige Begriffe:

- Firewall
- Regelwerk
- Paketfilter
- Stateful Inspection
- NAT
- PAT
- Portweiterleitung
- DMZ
- Sicherheitszone
- Default Deny
- Allow
- Drop
- Reject
- Source NAT
- Destination NAT
- Hairpin NAT
- Split DNS
- CGNAT

Merksatz:

Firewall kontrolliert Verkehr.
NAT übersetzt Adressen.
DMZ trennt öffentliche Dienste vom internen Netz.

Grundidee

Firewalls, NAT und DMZ haben unterschiedliche Aufgaben.

Firewall:

```
entscheidet,
ob Verkehr erlaubt oder blockiert wird.
```

NAT:

```
übersetzt IP-Adressen.
```

PAT:

```
übersetzt IP-Adressen und Ports.
```

DMZ:

```
trennt öffentlich erreichbare Dienste vom internen LAN.
```

Merksatz:

```
Firewall,
NAT
und DMZ nicht miteinander verwechseln.
```

Firewall

Eine Firewall kontrolliert Netzwerkverkehr.

Sie prüft je nach Art zum Beispiel:

```
- Quell-IP-Adresse
- Ziel-IP-Adresse
- Protokoll
- Quellport
- Zielport
- Richtung
- Interface
- Zone
```

```
- Verbindungsstatus
- Anwendung
```

Merksatz:

```
Firewall = kontrollierter Übergang zwischen Netzen.
```

Firewall-Regel

Eine Firewall-Regel beschreibt, welcher Verkehr erlaubt oder blockiert wird.

Typische Bestandteile:

```
- Aktion
- Quelle
- Ziel
- Dienst
- Protokoll
- Port
- Richtung
- Zone
- Kommentar
- Logging
```

Merksatz:

```
Firewall-Regel = Quelle,
Ziel,
Dienst
und Aktion.
```

Aktionen einer Firewall

Aktion	Bedeutung
Allow	Verkehr erlauben
Deny	Verkehr blockieren
Drop	Paket still verwerfen

Aktion	Bedeutung
Reject	Paket aktiv ablehnen
Log	Treffer protokollieren

Merksatz:

```
Allow erlaubt.
Drop schweigt.
Reject antwortet.
```

Drop und Reject

Drop bedeutet:

```
Paket wird ohne Antwort verworfen.
```

Reject bedeutet:

```
Paket wird aktiv abgelehnt,
und der Absender erhält eine Antwort.
```

Typische Wirkung:

```
Drop führt oft zu Timeout.
Reject führt oft zu schneller Fehlermeldung.
```

Merksatz:

```
Drop = keine Antwort.
Reject = aktive Ablehnung.
```

Paketfilter

Ein Paketfilter prüft vor allem:

```
- IP-Adressen
- Protokoll
- Ports
- Richtung
- Interface
```

Er arbeitet hauptsächlich auf Schicht 3 und 4.

Merksatz:

```
Paketfilter prüft IP und Port.
```

Stateful Firewall

Eine Stateful Firewall merkt sich Verbindungen.

Sie erkennt:

```
neues Paket
bestehende Verbindung
zugehörige Antwort
ungültiges Paket
```

Vorteil:

```
Rückverkehr zu erlaubten Verbindungen kann automatisch zugelassen werden.
```

Merksatz:

```
Stateful Firewall kennt den Verbindungszustand.
```

Stateful Inspection

Stateful Inspection bedeutet:

```
Die Firewall prüft,
ob Pakete zu einer bekannten Verbindung gehören.
```

Besonders wichtig bei TCP:

```
SYN
SYN-ACK
ACK
```

Merksatz:

```
Stateful Inspection prüft Verbindungszusammenhang.
```

Stateless Firewall

Eine Stateless Firewall betrachtet Pakete einzeln.

Sie merkt sich keinen Verbindungszustand.

Folge:

```
Hin- und Rückverkehr müssen genauer einzeln geregelt werden.
```

Merksatz:

```
Stateless = jedes Paket einzeln.
```

Default Deny

Default Deny bedeutet:

```
Alles ist verboten,
was nicht ausdrücklich erlaubt wurde.
```

Das ist ein wichtiges Sicherheitsprinzip.

Vorteil:

```
unbekannter oder unnötiger Verkehr wird nicht automatisch erlaubt.
```

Merksatz:

```
Erst alles blockieren,
dann gezielt erlauben.
```

Default Allow

Default Allow bedeutet:

```
Alles ist erlaubt,
was nicht ausdrücklich verboten wurde.
```

Das ist oft unsicherer, weil vergessene oder neue Dienste automatisch erreichbar sein können.

Merksatz:

```
Default Allow ist bequem,
aber riskant.
```

Regelreihenfolge

Viele Firewalls prüfen Regeln von oben nach unten.

Die erste passende Regel entscheidet.

Deshalb ist wichtig:

```
spezifische Regeln vor allgemeine Regeln
```

Beispiel:

```
Erlaube Admin-PC → Server SSH
```

vor:

```
Blockiere restliches SSH
```

Merksatz:

```
Die erste passende Regel gewinnt.
```

Spezifisch vor allgemein

Spezifische Regeln beschreiben einen engen Fall.

Allgemeine Regeln beschreiben einen breiten Fall.

Richtig:

```
erst Ausnahme erlauben,
dann allgemein blockieren.
```

Falsch:

```
zuerst allgemein blockieren,
dann Ausnahme erlauben.
```

Merksatz:

```
Spezifisch vor allgemein.
```

Any und Any-Any

Any bedeutet:

```
beliebig
```

Any-Any bedeutet meistens:

```
Quelle beliebig
Ziel beliebig
Dienst beliebig
```

Das ist sehr weit geöffnet und meist gefährlich.

Merksatz:

Any-Any vermeiden.

Firewall-Zonen

Eine Zone ist ein Sicherheitsbereich.

Typische Zonen:

Zone	Zweck
WAN	Internet oder externes Netz
LAN	internes Clientnetz
DMZ	öffentliche Dienste
Servernetz	interne Server
Managementnetz	Administration
Gastnetz	Gäste
IoT-Netz	Geräte mit eingeschränktem Vertrauen
VPN-Zone	entfernte Benutzer nach VPN-Einwahl

Merksatz:

Zonen trennen Netze nach Schutzbedarf.

LAN, WAN und DMZ

LAN:

internes Netz

WAN:

externes Netz oder Internet

DMZ:

eigenes Netz für öffentlich erreichbare Dienste

Merksatz:

```
LAN innen.
WAN außen.
DMZ dazwischen.
```

DMZ

DMZ steht für:

```
Demilitarized Zone
```

Eine DMZ enthält Dienste, die von außen erreichbar sein müssen.

Beispiele:

```
- Webserver
- Reverse Proxy
- Mailgateway
- VPN-Gateway
- öffentlicher DNS-Server
- Bastion Host
```

Merksatz:

```
DMZ = separates Netz für öffentliche Dienste.
```

Zweck einer DMZ

Eine DMZ schützt das interne LAN.

Wenn ein öffentlich erreichbarer Server kompromittiert wird, soll der Angreifer nicht direkt ins interne Netz gelangen.

Merksatz:

```
DMZ begrenzt Schaden bei öffentlichen Diensten.
```

DMZ-Regelprinzip

Typische Regelidee:

```
Internet → DMZ:
nur notwendige öffentliche Dienste erlauben

Internet → LAN:
blockieren

DMZ → LAN:
nur zwingend notwendige Verbindungen erlauben

Managementnetz → DMZ:
Administration gezielt erlauben
```

Merksatz:

```
DMZ darf keine freie Brücke ins LAN sein.
```

Reverse Proxy in der DMZ

Ein Reverse Proxy nimmt externe Anfragen an und leitet sie an interne Dienste weiter.

Vorteile:

```
- zentrale TLS-Verwaltung
- mehrere Webdienste über eine öffentliche IP
- weniger direkte Veröffentlichung interner Server
- bessere Kontrolle
- bessere Protokollierung
```

Merksatz:

```
Reverse Proxy bündelt und schützt Webzugriffe.
```

Bastion Host

Ein Bastion Host ist ein besonders abgesicherter Sprungserver.

Er dient dazu, administrative Zugriffe zu bündeln und zu kontrollieren.

Typisch:

```
Admin → Bastion Host → Zielsystem
```

Merksatz:

```
Bastion Host = abgesicherter Zugangspunkt für Administration.
```

NAT

NAT steht für:

```
Network Address Translation
```

NAT übersetzt IP-Adressen.

Typischer Einsatz:

```
private IPv4-Adresse
wird beim Zugriff ins Internet
in öffentliche IPv4-Adresse übersetzt.
```

Merksatz:

```
NAT übersetzt IP-Adressen.
```

Warum NAT bei IPv4 wichtig ist

Private IPv4-Adressen sind im Internet nicht direkt geroutet.

NAT ermöglicht, dass interne Geräte mit privaten Adressen trotzdem ins Internet können.

Außerdem spart NAT öffentliche IPv4-Adressen.

Merksatz:

NAT ermöglicht Internetzugriff mit privaten IPv4-Adressen.

Private IPv4-Adressbereiche

Bereich	CIDR
10.0.0.0 bis 10.255.255.255	10.0.0.0/8
172.16.0.0 bis 172.31.255.255	172.16.0.0/12
192.168.0.0 bis 192.168.255.255	192.168.0.0/16

Diese Bereiche sind für interne Netze vorgesehen.

Merksatz:

Private IPv4-Adressen werden im Internet nicht direkt geroutet.

Öffentliche IP-Adresse

Eine öffentliche IP-Adresse ist im Internet routbar.

Sie wird zum Beispiel vom Provider zugewiesen.

Interne Geräte sind meist über NAT hinter dieser öffentlichen Adresse sichtbar.

Merksatz:

Öffentliche IP-Adresse ist im Internet erreichbar.

Source NAT

Source NAT ändert die Quelladresse.

Typischer Fall:

Client im LAN baut Verbindung ins Internet auf.

Vorher:

```
Quelle:
private IP
```

Nachher:

```
Quelle:
öffentliche IP des Routers oder der Firewall
```

Merksatz:

```
Source NAT ändert die Quelle.
```

Destination NAT

Destination NAT ändert die Zieladresse.

Typischer Fall:

```
externer Zugriff wird an internes Ziel weitergeleitet.
```

Beispiel:

```
öffentliche IP:443
→ interner Webserver:443
```

Merksatz:

```
Destination NAT ändert das Ziel.
```

PAT

PAT steht für:

```
Port Address Translation
```

PAT übersetzt zusätzlich Ports.

Dadurch können viele interne Geräte gleichzeitig über eine öffentliche IP-Adresse kommunizieren.

Merksatz:

> PAT = NAT mit Portübersetzung.

NAT und PAT unterscheiden

Begriff	Bedeutung
NAT	IP-Adressen werden übersetzt
PAT	IP-Adressen und Ports werden übersetzt
Source NAT	Quelladresse wird geändert
Destination NAT	Zieladresse wird geändert
Portweiterleitung	externer Port wird intern weitergeleitet

Merksatz:

> NAT = Adresse.
> PAT = Adresse plus Port.

Portweiterleitung

Portweiterleitung bedeutet:

> Ein externer Port wird an ein internes Ziel weitergeleitet.

Beispiel:

> WAN TCP 443
> → 192.168.10.20 TCP 443

Portweiterleitung ist eine Form von Destination NAT.

Merksatz:

> Portweiterleitung macht interne Dienste extern erreichbar.

Portweiterleitung und Sicherheit

Eine Portweiterleitung erhöht die Angriffsfläche.

Warum?

```
Ein interner Dienst wird von außen erreichbar.
```

Deshalb wichtig:

```
- nur notwendige Ports öffnen
- Dienste aktuell halten
- starke Authentifizierung
- TLS nutzen
- Logs prüfen
- Zugriff einschränken
- keine Admin-Dienste direkt veröffentlichen
```

Merksatz:

```
Jeder veröffentlichte Port ist ein Risiko.
```

Was man nicht direkt veröffentlichen sollte

Normalerweise nicht direkt ins Internet:

```
- SMB TCP 445
- RDP TCP 3389
- Telnet TCP 23
- Datenbankports
- NAS-Adminoberflächen
- Hypervisor-Management
- Drucker
- interne Adminoberflächen
```

Besser:

VPN,
Reverse Proxy,
Bastion Host,
Zero-Trust-Zugriff
oder
kontrollierte Quellbeschränkung.

Merksatz:

Interne Admin-Dienste nicht direkt ins Internet öffnen.

NAT-Regel und Firewall-Regel unterscheiden

NAT-Regel:

Wohin wird Verkehr übersetzt oder weitergeleitet?

Firewall-Regel:

Darf dieser Verkehr passieren?

Beide müssen passen.

Beispiel:

NAT leitet WAN:443 an Server weiter.
Firewall blockiert WAN → Server TCP 443.
Ergebnis:
Zugriff funktioniert nicht.

Merksatz:

NAT leitet um.
Firewall erlaubt oder blockiert.

Routing und Firewall unterscheiden

Routing entscheidet:

```
welchen Weg ein Paket nimmt.
```

Firewall entscheidet:

```
ob ein Paket erlaubt wird.
```

Beides muss stimmen.

Merksatz:

```
Routing findet den Weg.
Firewall erlaubt den Weg.
```

Hairpin NAT

Hairpin NAT bedeutet:

```
Ein interner Client greift über die öffentliche Adresse auf einen internen Dienst zu.
```

Beispiel:

```
Client im LAN ruft cloud.firma.de auf.
DNS liefert öffentliche IP.
Router leitet Verbindung wieder nach innen.
```

Merksatz:

```
Hairpin NAT = intern über öffentliche Adresse.
```

Split DNS

Split DNS liefert intern und extern unterschiedliche DNS-Antworten.

Beispiel:

cloud.firma.de extern:
öffentliche IP

cloud.firma.de intern:
interne IP

Vorteil:

interne Clients erreichen den Dienst direkt intern.

Merksatz:

Split DNS kann Hairpin NAT vermeiden.

CGNAT

CGNAT steht für:

Carrier Grade NAT

Dabei teilt der Provider eine öffentliche IPv4-Adresse auf mehrere Kunden auf.

Folge:

eingehende Portweiterleitungen funktionieren oft nicht direkt.

Merksatz:

CGNAT verhindert oft direkte eingehende IPv4-Verbindungen.

Double NAT

Double NAT bedeutet:

Zwei NAT-Geräte sind hintereinander aktiv.

Beispiel:

```
Provider-Router macht NAT.
Eigener Router macht NAT.
```

Folge:

```
Portweiterleitungen müssen auf beiden Geräten passen.
```

Merksatz:

```
Double NAT erschwert Portweiterleitungen.
```

Firewall und DNS

DNS ist bei Firewall- und NAT-Themen sehr wichtig.

Beispiel:

```
DNS zeigt auf falsche öffentliche IP.
Dann erreicht der Client nicht das richtige Ziel.
```

Oder:

```
intern wird ein anderer DNS-Eintrag benötigt als extern.
```

Merksatz:

```
Falsches DNS kann wie ein Firewallproblem aussehen.
```

Firewall und TLS

Ein offener Port 443 bedeutet nicht automatisch, dass HTTPS korrekt funktioniert.

Mögliche zusätzliche Probleme:

```
- falsches Zertifikat
- Zertifikat abgelaufen
- Hostname passt nicht
```

- Reverse Proxy falsch
- Backend nicht erreichbar
- TLS-Version passt nicht

Merksatz:

Port 443 offen heißt nicht:
HTTPS funktioniert korrekt.

Firewall und Rückweg

Eine Verbindung braucht Hinweg und Rückweg.

Wenn der Rückweg fehlt, funktioniert die Verbindung nicht.

Mögliche Ursachen:

- falsches Gateway
- fehlende Route
- asymmetrisches Routing
- NAT-Zuordnung fehlt
- Antwort geht über falsches Interface

Merksatz:

Ohne Rückweg keine funktionierende Verbindung.

Asymmetrisches Routing

Asymmetrisches Routing bedeutet:

Hinweg und Rückweg laufen über unterschiedliche Wege.

Das kann Stateful Firewalls stören, weil sie den Verbindungszustand nur auf einem Weg sehen.

Merksatz:

Stateful Firewalls brauchen passenden Hin- und Rückweg.

Firewall-Logs

Firewall-Logs zeigen, was mit Verkehr passiert.

Wichtige Angaben:

- Quelle
- Ziel
- Port
- Protokoll
- Aktion
- Zeit
- Regelname
- Zone
- Interface
- NAT-Übersetzung

Merksatz:

Logs zeigen,
ob Verkehr erlaubt oder blockiert wurde.

Typische Fehler bei Firewalls

Typische Fehler:

- falsche Quelle
- falsches Ziel
- falscher Port
- TCP und UDP verwechselt
- falsche Richtung
- falsche Zone
- falsche Regelreihenfolge
- Regel deaktiviert
- Host-Firewall blockiert
- Dienst läuft nicht
- Rückweg fehlt
- DNS zeigt falsch

Merksatz:

```
Firewall-Fehler sind oft Detailfehler.
```

Typische Fehler bei NAT

Typische Fehler:

```
- NAT-Regel fehlt
- falsche öffentliche IP
- falsches internes Ziel
- falscher interner Port
- falscher externer Port
- TCP und UDP verwechselt
- CGNAT
- Double NAT
- alte NAT-Regel greift
- DNS zeigt auf falsche IP
- Hairpin NAT fehlt
```

Merksatz:

```
NAT-Fehler betreffen oft Adresse,
Port
oder Ziel.
```

Typische Fehler bei DMZ

Typische Fehler:

```
- öffentliche Dienste im LAN statt in DMZ
- DMZ darf zu viel ins LAN
- Adminzugang aus Internet erlaubt
- Firewall-Regel zu breit
- Reverse Proxy erreicht Backend nicht
- DNS falsch
- Zertifikat falsch
- ausgehender DMZ-Verkehr ungefiltert
```

- Monitoring fehlt
- Logs fehlen

Merksatz:

DMZ-Fehler sind oft Zonen- oder Regelprobleme.

Systematische Fehlersuche

Eine sinnvolle Reihenfolge:

1. Quelle bestimmen.
2. Ziel bestimmen.
3. Port und Protokoll bestimmen.
4. Richtung und Zone bestimmen.
5. DNS prüfen.
6. Routing prüfen.
7. NAT prüfen.
8. Firewall-Regel prüfen.
9. Regelreihenfolge prüfen.
10. Firewall-Logs prüfen.
11. Host-Firewall prüfen.
12. Dienststatus prüfen.
13. Rückweg prüfen.
14. Anwendung testen.
15. Änderungen prüfen.

Merksatz:

Firewall-Fehlersuche ist eine Verbindungskette.

Ping reicht nicht aus

Ping prüft nur ICMP-Erreichbarkeit.

Ping sagt nicht:

```
ob TCP 443 offen ist
ob HTTPS korrekt funktioniert
ob NAT stimmt
ob Zertifikat passt
ob Anmeldung funktioniert
ob Anwendung antwortet
```

Merksatz:

```
Ping ist kein vollständiger Diensttest.
```

Porttest reicht nicht aus

Ein Porttest zeigt nur:

```
Port erreichbar oder nicht erreichbar.
```

Er zeigt nicht automatisch:

```
Anwendung korrekt
Zertifikat korrekt
Anmeldung korrekt
Rechte korrekt
Datenformat korrekt
Backend korrekt
```

Merksatz:

```
Offener Port heißt nicht:
Dienst funktioniert.
```

Timeout

Timeout bedeutet:

```
Es kommt keine Antwort innerhalb der erwarteten Zeit.
```

Mögliche Ursachen:

- Firewall droppt
- Routingproblem
- Dienst antwortet nicht
- Rückweg fehlt
- falsches Ziel
- Provider blockiert

Merksatz:

Timeout bedeutet oft:
keine passende Antwort.

Connection Refused

Connection refused bedeutet:

Zielsystem ist erreichbar,
aber der Dienst nimmt auf dem Port keine Verbindung an.

Mögliche Ursachen:

- Dienst läuft nicht
- falscher Port
- Dienst lauscht nur lokal
- Host-Firewall lehnt ab

Merksatz:

Connection refused deutet eher auf Zielsystem oder Dienst hin.

Wichtige Testwerkzeuge

Werkzeug	Zweck
ping	grobe Erreichbarkeit
traceroute / tracert	Weg zum Ziel

Werkzeug	Zweck
nslookup	DNS prüfen
dig	DNS detailliert prüfen
curl	HTTP/HTTPS testen
nc	TCP-/UDP-Port testen
Test-NetConnection	Windows-Porttest
openssl s_client	TLS prüfen
tcpdump	Verkehr mitschneiden
Wireshark	Pakete analysieren
Firewall-Logs	Regeltreffer prüfen
Serverlogs	Dienstfehler prüfen

Merksatz:

> Werkzeug nach Fehlerbild auswählen.

Sicherheitsprinzipien

Wichtige Prinzipien:

- Default Deny
- Least Privilege
- nur notwendige Ports öffnen
- Adminzugänge nicht öffentlich machen
- Zonen trennen
- DMZ verwenden
- Regeln dokumentieren
- temporäre Regeln befristen
- Logs aktivieren
- Updates einspielen
- Monitoring einsetzen

Merksatz:

> Sicherheit entsteht durch mehrere Maßnahmen zusammen.

Least Privilege bei Firewall-Regeln

Least Privilege bedeutet:

```
Nur erlauben,
was wirklich benötigt wird.
```

Beispiel schlecht:

```
DMZ → LAN any erlauben
```

Beispiel besser:

```
Reverse Proxy → interner Webdienst TCP 8080 erlauben
```

Merksatz:

```
Firewall-Regeln so eng wie möglich setzen.
```

Dokumentation

Firewall- und NAT-Regeln sollten dokumentiert werden.

Wichtige Angaben:

```
- Zweck
- Quelle
- Ziel
- Port
- Protokoll
- Richtung
- NAT-Ziel
- Verantwortlicher
- Ticket
- Datum
- Ablaufdatum bei temporären Regeln
```

Merksatz:

Undokumentierte Regeln werden später zum Risiko.

Regelreview

Firewall-Regelwerke sollten regelmäßig geprüft werden.

Dabei sucht man:

- alte Regeln
- ungenutzte Regeln
- temporäre Regeln ohne Ablauf
- Any-Any-Regeln
- zu breite Freigaben
- fehlende Kommentare
- shadowed rules
- redundante Regeln

Merksatz:

Firewall-Regeln altern und müssen gepflegt werden.

Typische IHK-Fragen

In AP1 und AP2 kann zum Beispiel gefragt werden:

- Was ist die Aufgabe einer Firewall?
- Was ist der Unterschied zwischen Firewall und NAT?
- Was ist eine Stateful Firewall?
- Was bedeutet Stateful Inspection?
- Was bedeutet Default Deny?
- Warum ist die Regelreihenfolge wichtig?
- Warum sind Any-Any-Regeln gefährlich?
- Was ist NAT?
- Was ist PAT?
- Was ist Source NAT?
- Was ist Destination NAT?
- Was ist eine Portweiterleitung?
- Warum reicht eine NAT-Regel allein nicht aus?

- Was ist eine DMZ?
- Warum stellt man öffentliche Dienste in eine DMZ?
- Warum darf die DMZ nicht frei ins LAN?
- Was ist Hairpin NAT?
- Was ist Split DNS?
- Was ist CGNAT?
- Wie geht man bei Firewall-Fehlersuche vor?

Typische Prüfungsfallen

Firewall ist nicht NAT.

NAT ist nicht Firewall.

NAT übersetzt Adressen.

PAT übersetzt Adressen und Ports.

Portweiterleitung ist Destination NAT.

NAT-Regel ersetzt keine Firewall-Regel.

Firewall-Regel ersetzt keine NAT-Regel.

Routing entscheidet den Weg.

Firewall entscheidet die Erlaubnis.

DNS kann wie ein Firewallproblem wirken.

Port offen heißt nicht:
Anwendung funktioniert.

TCP und UDP nicht verwechseln.

Regelrichtung beachten.

Regelreihenfolge beachten.

Spezifisch vor allgemein.

Default Deny ist sicherer.

Any-Any vermeiden.

Drop und Reject unterscheiden.

DMZ ist nicht LAN.

DMZ darf nicht frei ins LAN.

Öffentliche Dienste gehören besser in die DMZ.

RDP nicht direkt ins Internet öffnen.

SMB nicht direkt ins Internet öffnen.

CGNAT kann Portweiterleitung verhindern.

Hairpin NAT betrifft interne Zugriffe über öffentliche Adresse.

Split DNS kann Hairpin NAT vermeiden.

Rückweg prüfen.

Logs prüfen.

Wichtige Begriffe kurz erklärt

Begriff	Kurze Erklärung
Firewall	kontrolliert Netzwerkverkehr
Firewall-Regel	Bedingung mit Aktion
Paketfilter	prüft IP-Adressen und Ports
Stateful Firewall	kennt Verbindungszustände
Stateful Inspection	Prüfung des Verbindungsstatus
Default Deny	alles blockieren, außer erlaubt
Allow	erlauben

Begriff	Kurze Erklärung
Deny	blockieren
Drop	still verwerfen
Reject	aktiv ablehnen
Zone	Sicherheitsbereich
LAN	internes Netz
WAN	externes Netz
DMZ	Netz für öffentliche Dienste
NAT	Adressübersetzung
PAT	Adress- und Portübersetzung
Source NAT	Quelladresse wird geändert
Destination NAT	Zieladresse wird geändert
Portweiterleitung	externer Port wird intern weitergeleitet
Hairpin NAT	interner Zugriff über öffentliche Adresse
Split DNS	intern und extern unterschiedliche DNS-Antwort
CGNAT	Provider-NAT für mehrere Kunden
Double NAT	zwei NAT-Geräte hintereinander
Reverse Proxy	leitet Webanfragen an Backends
Bastion Host	abgesicherter Sprungserver
Any-Any	sehr breite Regel
Rückweg	Antwortweg zurück zur Quelle
asymmetrisches Routing	Hin- und Rückweg unterschiedlich

IHK-sichere Gesamtformulierung

Eine Firewall kontrolliert Netzwerkverkehr zwischen Systemen oder Netzbereichen und entscheidet anhand von Regeln, ob Verbindungen erlaubt oder blockiert werden. Typische Kriterien sind Quelle, Ziel, Port, Protokoll, Richtung und Zone. NAT übersetzt IP-Adressen, während PAT zusätzlich Ports übersetzt. Eine Portweiterleitung ist eine Form von Destination NAT und macht einen internen Dienst von außen erreichbar. NAT-Regeln und Firewall-Regeln sind zu unterscheiden und müssen zusammenpassen. Eine DMZ ist ein separates Netz für Dienste, die von außen erreichbar sein müssen. Sie schützt das interne LAN, indem öffentliche Dienste getrennt platziert und Zugriffe zwischen WAN, DMZ und LAN gezielt geregelt werden.

Wichtigste Merksätze

Firewall kontrolliert Verkehr.

NAT übersetzt Adressen.

PAT übersetzt Adressen und Ports.

DMZ trennt öffentliche Dienste vom LAN.

Firewall ist nicht NAT.

NAT ist nicht Firewall.

Routing findet den Weg.

Firewall erlaubt den Weg.

NAT-Regel leitet um.

Firewall-Regel erlaubt oder blockiert.

Source NAT ändert Quelle.

Destination NAT ändert Ziel.

Portweiterleitung ist Destination NAT.

Private IPv4-Adressen sind intern.

Öffentliche IP-Adressen sind im Internet routbar.

Default Deny ist sicherer.

Die erste passende Regel gewinnt.

Spezifisch vor allgemein.

Any-Any vermeiden.

Drop schweigt.

Reject antwortet.

Stateful Firewall kennt Verbindungen.

Rückweg muss passen.

Asymmetrisches Routing kann stören.

DMZ ist nicht LAN.

DMZ darf nicht frei ins LAN.

Öffentliche Dienste gehören besser in die DMZ.

Reverse Proxy kann Dienste bündeln.

RDP nicht direkt ins Internet öffnen.

SMB nicht direkt ins Internet öffnen.

CGNAT kann Portweiterleitungen verhindern.

Hairpin NAT = intern über öffentliche Adresse.

Split DNS = intern andere DNS-Antwort.

DNS,
NAT,
Firewall,
Dienst
und Logs gemeinsam prüfen.