11.1 Firewalls, NAT und DMZ

Firewalls, NAT und DMZ gehören zu den wichtigsten Themen der Netzwerksicherheit.

Sie werden verwendet, um Netzwerke zu schützen, Zugriffe zu steuern und interne Systeme vom Internet zu trennen.

Wichtige Begriffe:

- Firewall
- Paketfilter
- Stateful Inspection
- Firewall-Regel
- Allow
- Deny
- NAT
- PAT
- Portweiterleitung
- DMZ
- interne Zone
- externe Zone
- Sicherheitszone

Merksatz:

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

Grundidee einer Firewall

Eine Firewall kontrolliert Netzwerkverkehr.

Sie entscheidet:

Darf dieser Datenverkehr durch?
Oder wird er blockiert?

Dabei prüft sie je nach Art und Konfiguration zum Beispiel:

```
- Quell-IP-Adresse
- Ziel-IP-Adresse
- Protokoll
- Quellport
- Zielport
- Verbindungsstatus
- Richtung
- Benutzer
- Anwendung
- Sicherheitszone
```

Merksatz:

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

Warum braucht man Firewalls?

Ohne Firewall könnten Systeme oft zu viele Verbindungen annehmen.

Eine Firewall reduziert die Angriffsfläche.

Sie schützt vor:

```
- unerwünschten Zugriffen
- offenen Diensten
- unkontrolliertem Datenverkehr
- Angriffen aus fremden Netzen
- ungewollter Kommunikation zwischen Netzbereichen
- direktem Zugriff auf interne Systeme
```

Merksatz:

```
Firewall-Regeln begrenzen,
wer mit wem sprechen darf.
```

Firewall ist nicht gleich Virenschutz

Eine Firewall kontrolliert Netzwerkverkehr.

Ein Virenschutz prüft Dateien, Programme oder Verhalten auf Schadsoftware.

Unterschied:

Schutz	Hauptaufgabe
Firewall	Netzwerkverkehr erlauben oder blockieren
Virenschutz	Schadsoftware erkennen und blockieren
EDR	Verhalten auf Endgeräten überwachen
IDS/IPS	Angriffe im Netzwerk erkennen oder blockieren

Merksatz:

```
Firewall schützt Netzwerkzugriffe,
ersetzt aber keinen Virenschutz.
```

Firewall im OSI-Modell

Firewalls können auf verschiedenen Schichten arbeiten.

Firewall-Art	typische Schicht	Prüft vor allem
Paketfilter	3 / 4	IP-Adressen, Protokoll, Ports
Stateful Firewall	3 / 4	Verbindungsstatus zusätzlich
Application Firewall	7	Anwendungsdaten und Protokolle
Web Application Firewall	7	HTTP/HTTPS-Anfragen

Merksatz:

```
Firewalls können je nach Art auf mehreren Schichten arbeiten.
```

Paketfilter

Ein Paketfilter entscheidet anhand einzelner Pakete.

Typische Kriterien:

```
- Quell-IP
- Ziel-IP
- Protokoll
```

- Quellport
- Zielport
- Richtung
- Interface

Beispiel:

Erlaube TCP von 192.168.10.0/24 nach 10.0.0.5 auf Port 443.

Merksatz:

Paketfilter prüft IP-Adressen und Ports.

Stateful Firewall

Eine Stateful Firewall merkt sich den Zustand von Verbindungen.

Sie erkennt:

Gehört dieses Paket zu einer bestehenden Verbindung?

Beispiel:

Client aus internem Netz baut HTTPS-Verbindung nach außen auf.
Antwortpakete vom Webserver werden erlaubt,
weil sie zu dieser bestehenden Verbindung gehören.

Vorteil:

Rückverkehr muss nicht immer als komplett neue Verbindung erlaubt werden.

Merksatz:

Stateful Firewall kennt bestehende Verbindungen.

Stateful Inspection

Stateful Inspection bedeutet:

```
Die Firewall prüft den Verbindungszustand.
```

Sie unterscheidet zum Beispiel:

```
neue Verbindung
bestehende Verbindung
zugehörige Antwort
ungültiges Paket
```

Das ist besonders wichtig bei TCP.

Merksatz:

```
Stateful Inspection prüft,
ob Verkehr zu einer erlaubten Verbindung gehört.
```

Stateless Firewall

Eine Stateless Firewall merkt sich keine Verbindungen.

Sie betrachtet Pakete einzeln.

Nachteil:

```
Rückverkehr muss oft explizit geregelt werden.
```

Vorteil:

```
einfacher,
schneller,
aber weniger intelligent.
```

Merksatz:

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

Firewall-Regel

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

Typische Bestandteile:

```
- Aktion
- Quelle
- Ziel
- Dienst oder Port
- Protokoll
- Richtung
- Interface oder Zone
- Kommentar oder Beschreibung
```

Beispiel:

```
Erlaube
Quelle: Internes Netz
Ziel: Webserver in DMZ
Dienst: HTTPS TCP 443
```

Merksatz:

```
Firewall-Regel = Bedingung plus Aktion.
```

Allow und Deny

Firewall-Regeln haben meist eine Aktion.

Wichtige Aktionen:

```
Allow
Deny
Drop
Reject
```

Allow bedeutet:

Verkehr erlauben.

Deny, Drop oder Reject bedeuten:

Verkehr blockieren.

Merksatz:

Allow erlaubt.
Deny blockiert.

Drop und Reject unterscheiden

Drop bedeutet:

Paket wird verworfen,
ohne Antwort.

Reject bedeutet:

Paket wird abgelehnt,
mit Antwort an den Absender.

Unterschied:

Aktion	Verhalten
Drop	still verwerfen
Reject	aktiv ablehnen
Allow	erlauben

Merksatz:

Drop schweigt.
Reject antwortet.

Default Deny

Default Deny bedeutet:

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

Das ist ein wichtiges Sicherheitsprinzip.

Beispiel:

```
Alle Verbindungen blockieren.
Nur notwendige Dienste erlauben.
```

Vorteil:

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

Merksatz:

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

Default Allow

Default Allow bedeutet:

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

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

Merksatz:

```
Default Allow ist bequem,
aber oft unsicherer.
```

Regelreihenfolge

Viele Firewalls arbeiten Regeln von oben nach unten ab.

Die erste passende Regel entscheidet.

Beispiel:

```
Regel 1:
Blockiere Ziel TCP 443

Regel 2:
Erlaube Ziel TCP 443
```

Ergebnis:

```
Wenn Regel 1 zuerst passt,
wird blockiert.
```

Merksatz:

```
Reihenfolge der Firewall-Regeln ist entscheidend.
```

Spezifische Regeln vor allgemeinen Regeln

Spezifische Regeln sollten vor allgemeinen Regeln stehen.

Beispiel:

```
Erlaube Admin-PC zu Server auf SSH.
```

Danach:

```
Blockiere restliches SSH.
```

Wenn die allgemeine Blockregel zuerst steht, kommt die spezifische Erlaubnis nie zum Tragen.

Merksatz:

```
Spezifisch vor allgemein.
```

Firewall-Zonen

Viele Firewalls arbeiten mit Zonen.

Typische Zonen:

```
- LAN
- WAN
- DMZ
- Gastnetz
- Servernetz
- Managementnetz
- VPN
- IoT-Netz
```

Zonen helfen, Netzbereiche logisch zu trennen.

Merksatz:

```
Zone = Sicherheitsbereich im Netzwerk.
```

LAN und WAN

LAN steht für:

```
Local Area Network
```

WAN steht für:

```
Wide Area Network
```

Vereinfacht:

```
LAN = internes Netz
WAN = externes Netz oder Internetseite
```

Merksatz:

```
LAN innen,
WAN außen.
```

Interne Zone

Die interne Zone enthält normalerweise vertrauenswürdigere Systeme.

Beispiele:

```
- Clients
- interne Server
- Drucker
- Verwaltungsgeräte
- interne Anwendungen
```

Trotzdem gilt:

```
Auch intern sollte nicht alles blind erlaubt sein.
```

Merksatz:

```
Intern ist nicht automatisch sicher.
```

Externe Zone

Die externe Zone ist meist das Internet oder ein fremdes Netz.

Von dort kommen potenziell untrusted Verbindungen.

Deshalb werden eingehende Verbindungen besonders streng kontrolliert.

Merksatz:

```
Extern = nicht vertrauenswürdig.
```

DMZ

DMZ steht für:

```
Demilitarized Zone
```

Eine DMZ ist ein separates Netz, in dem Dienste stehen, die von außen erreichbar sein müssen.

Beispiele:

```
- Webserver
- Reverse Proxy
- Mailgateway
- VPN-Gateway
- öffentliche API
- DNS-Server für externe Anfragen
```

Merksatz:

```
DMZ = eigenes Netz für öffentlich erreichbare Dienste.
```

Warum gibt es eine DMZ?

Eine DMZ schützt das interne Netz.

Idee:

```
Öffentliche Dienste sollen nicht direkt im internen LAN stehen.
```

Wenn ein Server in der DMZ kompromittiert wird, soll der Angreifer nicht automatisch Zugriff auf das interne Netz erhalten.

Merksatz:

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

DMZ-Grundaufbau

Typischer Aufbau:

```
Internet
→ Firewall
→ DMZ
→ Firewall-Regeln
→ internes LAN
```

Oder mit drei Zonen:

```
WAN
DMZ
LAN
```

Regeln werden gezielt zwischen diesen Zonen erstellt.

Merksatz:

```
DMZ liegt kontrolliert zwischen Internet und internem Netz.
```

Regeln für eine DMZ

Typische Regelidee:

```
Internet darf nur bestimmte Dienste in der DMZ erreichen.
```

Beispiel:

```
Internet → DMZ-Webserver:
TCP 443 erlaubt

Internet → internes LAN:
blockiert

DMZ → internes LAN:
nur notwendige Verbindungen erlaubt

internes LAN → DMZ:
Administration nur von Admin-Systemen
```

Merksatz:

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

DMZ und internes Netz

Ein häufiger Fehler ist:

```
DMZ-Server dürfen alles im internen Netz erreichen.
```

Das ist gefährlich.

Besser:

```
Nur notwendige Verbindungen erlauben.
```

Beispiel:

```
Webserver in DMZ darf nur zur Datenbank auf TCP 5432.
```

Oder:

```
Reverse Proxy in DMZ darf nur zu bestimmten internen Webdiensten.
```

Merksatz:

```
Von DMZ ins LAN nur gezielt erlauben.
```

DMZ und Administration

Administrationszugriff auf DMZ-Systeme sollte eingeschränkt sein.

Beispiele:

```
Admin-Netz → DMZ-Server SSH erlauben
normale Clients → DMZ-Server SSH blockieren
Internet → DMZ-Server SSH blockieren
```

Sinnvoll:

```
Administration über VPN,
Managementnetz
oder Bastion Host.
```

Merksatz:

```
DMZ-Administration nur kontrolliert erlauben.
```

Bastion Host

Ein Bastion Host ist ein besonders abgesicherter Sprungserver.

Er wird genutzt, um administrative Zugriffe zu bündeln.

Beispiel:

```
Admin verbindet sich zum Bastion Host.
Von dort aus erfolgt Zugriff auf Server in der DMZ.
```

Vorteile:

```
- zentrale Kontrolle
- Protokollierung
- weniger direkte Zugriffe
- bessere Absicherung
```

Merksatz:

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

NAT

NAT steht für:

```
Network Address Translation
```

NAT übersetzt IP-Adressen.

Typische Nutzung:

```
private interne IP-Adressen
werden beim Zugriff ins Internet
```

in eine öffentliche IP-Adresse übersetzt.

Beispiel:

intern:
192.168.10.50

extern sichtbar:
öffentliche Router-IP

Merksatz:

NAT übersetzt IP-Adressen.

Warum braucht man NAT?

IPv4-Adressen sind knapp.

Private IPv4-Adressen werden intern verwendet und sind im Internet nicht direkt geroutet.

NAT ermöglicht, dass viele interne Geräte über eine oder wenige öffentliche IPv4-Adressen ins Internet gehen.

Merksatz:

NAT spart öffentliche IPv4-Adressen.

Private IPv4-Adressbereiche

Private IPv4-Adressbereiche sind:

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 Adressen werden im Internet nicht direkt geroutet.

Merksatz:

```
Private IPv4-Adressen sind für interne Netze gedacht.
```

Öffentliche IP-Adresse

Eine öffentliche IP-Adresse ist im Internet routbar.

Sie wird zum Beispiel vom Provider vergeben.

Beispiel:

```
Router hat öffentliche IP-Adresse am WAN.
```

Interne Clients verwenden private Adressen und werden per NAT nach außen übersetzt.

Merksatz:

```
Öffentliche IP ist im Internet erreichbar,
private IP normalerweise nicht.
```

Source NAT

Source NAT ändert die Quelladresse eines Pakets.

Typischer Fall:

```
interner Client geht ins Internet.
```

Vor NAT:

```
Quelle: 192.168.10.50
Ziel: 93.184.216.34
```

Nach NAT:

```
Quelle: öffentliche Router-IP
Ziel: 93.184.216.34
```

Merksatz:

```
Source NAT ändert die Quelle.
```

Destination NAT

Destination NAT ändert die Zieladresse eines Pakets.

Typischer Fall:

```
Portweiterleitung von außen nach innen.
```

Vor NAT:

```
Ziel: öffentliche IP TCP 443
```

Nach NAT:

```
Ziel: interner Webserver 192.168.10.20 TCP 443
```

Merksatz:

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

PAT

PAT steht für:

```
Port Address Translation
```

PAT übersetzt zusätzlich Ports.

Dadurch können viele interne Clients gleichzeitig eine öffentliche IP-Adresse nutzen.

Beispiel:

```
Client A intern:
192.168.10.10:50001
```

```
Client B intern:
192.168.10.11:50002
```

Extern sichtbar über dieselbe öffentliche IP, aber mit unterschiedlichen Ports.

Merksatz:

```
PAT = viele interne Geräte über eine öffentliche IP mit Portübersetzung.
```

NAT und PAT unterscheiden

Begriff	Bedeutung
NAT	Übersetzung von IP-Adressen
PAT	Übersetzung von IP-Adressen und Ports
Source NAT	Quelladresse wird geändert
Destination NAT	Zieladresse wird geändert
Portweiterleitung	eingehender Port wird intern weitergeleitet

Merksatz:

```
NAT übersetzt Adressen.
PAT übersetzt zusätzlich Ports.
```

Portweiterleitung

Portweiterleitung bedeutet:

```
Eine Verbindung von außen auf einen bestimmten Port
wird an ein internes Ziel weitergeleitet.
```

Beispiel:

```
öffentliche IP TCP 443
→ interner Server 192.168.10.20 TCP 443
```

Typische Nutzung:

- Webserver
- Reverse Proxy
- VPN-Gateway
- Mailserver
- Spielserver
- Testsysteme

Merksatz:

Portweiterleitung macht internen Dienst von außen erreichbar.

Portweiterleitung und Sicherheit

Portweiterleitung erhöht die Angriffsfläche.

Warum?

Ein interner Dienst wird von außen erreichbar.

Deshalb wichtig:

- nur notwendige Ports öffnen
- Dienste aktuell halten
- starke Authentifizierung
- TLS verwenden
- Logs prüfen
- Zugriff einschränken
- nach Möglichkeit DMZ nutzen
- keine Admin-Dienste offen ins Internet

Merksatz:

Jeder geöffnete Port ist ein potenzielles Risiko.

Firewall-Regel und NAT-Regel unterscheiden

Eine NAT-Regel übersetzt Adressen oder Ports.

Eine Firewall-Regel erlaubt oder blockiert Verkehr.

Beides ist nicht dasselbe.

Beispiel:

```
NAT-Regel:
öffentliche IP TCP 443 → interner Webserver TCP 443

Firewall-Regel:
Erlaube Internet → Webserver TCP 443
```

Wenn NAT gesetzt ist, aber Firewall blockiert, funktioniert der Zugriff trotzdem nicht.

Merksatz:

```
NAT leitet um.
Firewall erlaubt oder blockiert.
```

Inbound und Outbound

Inbound bedeutet:

```
eingehender Verkehr in Richtung eines Netzes oder Systems.
```

Outbound bedeutet:

```
ausgehender Verkehr aus einem Netz oder System.
```

Beispiel:

```
Client im LAN ruft Webseite im Internet auf:
outbound aus LAN

Internet greift auf Webserver in DMZ zu:
inbound zur DMZ
```

Merksatz:

Inbound hinein,
outbound hinaus.

East-West und North-South Traffic

North-South Traffic bedeutet:

Verkehr zwischen internem Netz und externen Netzen.

Beispiel:

Client ins Internet

East-West Traffic bedeutet:

Verkehr innerhalb eines Rechenzentrums oder interner Netze.

Beispiel:

Webserver spricht mit Datenbankserver.

Merksatz:

North-South = nach außen oder innen.
East-West = intern zwischen Systemen.

Firewall und Routing

Firewall und Routing sind nicht dasselbe.

Routing entscheidet:

Wohin wird ein Paket weitergeleitet?

Firewall entscheidet:

```
Darf das Paket weiter?
```

Beides muss passen.

Beispiel:

```
Route vorhanden,
aber Firewall blockiert:
Verbindung geht nicht.

Firewall erlaubt,
aber Route fehlt:
Verbindung geht nicht.
```

Merksatz:

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

Firewall und DNS

DNS-Probleme können wie Firewall-Probleme aussehen.

Beispiel:

```
Benutzer ruft service.firma.de auf.
DNS zeigt auf falsche IP.
```

Dann erreicht der Client vielleicht den falschen Server oder bekommt gar keine Verbindung.

Merksatz:

```
Vor Firewall-Fehlersuche auch DNS prüfen.
```

Firewall und TLS

Eine Firewall kann TCP 443 erlauben, aber HTTPS kann trotzdem fehlschlagen.

Mögliche Ursachen:

- Zertifikat ungültig
- falscher Hostname
- falsches Backend
- Reverse Proxy falsch
- TLS-Version inkompatibel
- Anwendung antwortet falsch

Merksatz:

Port 443 offen heißt nicht:
HTTPS funktioniert korrekt.

Firewall und Protokolle

Ein Port allein beschreibt nicht immer alles.

Beispiele:

DNS nutzt UDP und TCP 53.
FTP nutzt Steuer- und Datenverbindungen.
SIP oder VoIP können zusätzliche Ports nutzen.
HTTP/3 nutzt UDP 443.
VPN-Protokolle nutzen unterschiedliche Ports und Protokolle.

Merksatz:

Immer Protokoll,
Port
und Verbindungsverhalten beachten.

Firewall-Logs

Firewall-Logs sind wichtig für Fehlersuche und Sicherheit.

Sie zeigen zum Beispiel:

- erlaubte Verbindungen
- blockierte Verbindungen

- Quell-IP
- Ziel-IP
- Port
- Protokoll
- Regelname
- Zeitstempel
- Interface oder Zone

Merksatz:

Firewall-Logs zeigen,
ob Verkehr erlaubt oder blockiert wurde.

Typische Firewall-Fehler

Typische Fehler sind:

- falsche Regelreihenfolge
- falsche Quelle
- falsches Ziel
- falscher Port
- falsches Protokoll
- Regel in falscher Richtung
- falsche Zone
- NAT fehlt
- Rückweg fehlt
- DNS zeigt auf falsches Ziel
- Dienst läuft nicht
- asymmetrisches Routing

Merksatz:

Firewall-Fehler sind oft Regel-, Richtungs- oder Zonenfehler.

Fehlerbild: Dienst von außen nicht erreichbar

Mögliche Ursachen:

- Portweiterleitung fehlt
- Firewall-Regel fehlt
- falscher Zielserver
- falscher Zielport
- Dienst läuft nicht
- öffentliche IP falsch
- DNS zeigt falsch
- Provider blockiert Port
- CGNAT
- Reverse Proxy falsch
- Zertifikat fehlerhaft

Merksatz:

Externer Zugriff braucht DNS,
NAT,
Firewall,
Dienst
und Rückweg.

Fehlerbild: Intern funktioniert, extern nicht

Mögliche Ursachen:

- externe Firewall blockiert
- NAT oder Portweiterleitung fehlt
- externer DNS-Eintrag falsch
- öffentliche IP falsch
- CGNAT
- Zertifikat nur intern passend
- Dienst nur auf interner Adresse gebunden
- Reverse Proxy nur intern konfiguriert

Merksatz:

Intern und extern getrennt prüfen.

Fehlerbild: Extern funktioniert, intern nicht

Mögliche Ursachen:

- internes DNS zeigt falsch
- Split DNS fehlt
- Hairpin NAT fehlt
- interne Firewall blockiert
- interne Route fehlt
- Zertifikatname passt intern nicht
- Proxy- oder Gatewayproblem

Merksatz:

Extern erreichbar heißt nicht automatisch intern erreichbar.

Hairpin NAT

Hairpin NAT wird gebraucht, wenn interne Clients über die öffentliche Adresse auf einen internen Dienst zugreifen sollen.

Beispiel:

interner Client ruft öffentliche Domain auf.
DNS liefert öffentliche IP.
Router muss Verbindung wieder nach innen leiten.

Wenn Hairpin NAT fehlt, funktioniert der Dienst extern, aber intern über den öffentlichen Namen nicht.

Merksatz:

Hairpin NAT ermöglicht internen Zugriff über öffentliche Adresse.

Split DNS als Alternative

Split DNS kann Hairpin NAT vermeiden.

Dabei liefert DNS intern und extern unterschiedliche Antworten.

Beispiel:

```
service.firma.de extern:
öffentliche IP

service.firma.de intern:
interne IP
```

Vorteil:

```
interne Clients gehen direkt zur internen Adresse.
```

Merksatz:

```
Split DNS liefert intern passende interne Adressen.
```

CGNAT

CGNAT steht für:

```
Carrier Grade NAT
```

Dabei hat der Anschluss keine eigene echte öffentliche IPv4-Adresse.

Der Provider nutzt NAT für viele Kunden.

Folge:

```
eingehende Portweiterleitungen funktionieren oft nicht direkt.
```

Mögliche Lösungen:

```
- echte öffentliche IPv4 buchen
- IPv6 nutzen
- VPN-Tunnel
- Cloud-Tunnel
- Reverse Proxy über externen Server
```

Merksatz:

```
CGNAT verhindert oft direkte eingehende IPv4-Verbindungen.
```

Asymmetrisches Routing

Asymmetrisches Routing bedeutet:

```
Hinweg und Rückweg laufen über unterschiedliche Wege.
```

Das kann Firewalls stören, weil eine Stateful Firewall den Verbindungszustand auf einem Weg sieht, aber die Antwort über einen anderen Weg zurückkommt.

Folge:

```
Verbindung wird möglicherweise blockiert.
```

Merksatz:

```
Stateful Firewalls brauchen passenden Hin- und Rückweg.
```

Any-Any-Regel

Eine Any-Any-Regel erlaubt sehr viel.

Beispiel:

```
Quelle: any
Ziel: any
Dienst: any
Aktion: allow
```

Das ist gefährlich, weil fast jeder Verkehr erlaubt wird.

Any-Any-Regeln sollten vermieden oder sehr gut begründet werden.

Merksatz:

```
Any-Any ist bequem,
aber riskant.
```

Least Privilege bei Firewall-Regeln

Auch bei Firewall-Regeln gilt:

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

Beispiel schlecht:

```
Erlaube gesamtes LAN zur DMZ auf alle Ports.
```

Besser:

```
Erlaube Admin-PC zur DMZ auf TCP 22.
Erlaube Webserver zur Datenbank auf TCP 5432.
```

Merksatz:

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

Dokumentation von Firewall-Regeln

Firewall-Regeln sollten dokumentiert werden.

Wichtige Angaben:

```
- Zweck
- Quelle
- Ziel
- Dienst
- Verantwortlicher
- Erstellungsdatum
- Ablaufdatum bei temporären Regeln
- Ticket oder Änderungsgrund
```

```
- Risiko
- Kommentar
```

Merksatz:

```
Undokumentierte Firewall-Regeln werden schnell zum Sicherheitsproblem.
```

Temporäre Firewall-Regeln

Temporäre Regeln sollten ein Ablaufdatum haben.

Problem:

```
Testregel wird erstellt.
Niemand entfernt sie.
Dienst bleibt unnötig offen.
```

Besser:

```
temporäre Regel mit Ablaufdatum,
Kommentar
und Review.
```

Merksatz:

```
Temporär darf nicht dauerhaft vergessen werden.
```

Firewall-Review

Firewall-Regeln sollten regelmäßig überprüft werden.

Ziel:

```
- alte Regeln entfernen
- unnötige Freigaben schließen
- Any-Any-Regeln vermeiden
- Dokumentation aktualisieren
- Sicherheitsrisiken reduzieren
```

```
- Regelreihenfolge prüfen
```

Merksatz:

```
Firewall-Regeln brauchen regelmäßige Pflege.
```

Typische Sicherheitszonen

Zone	Zweck
WAN	externes Netz / Internet
LAN	internes Clientnetz
DMZ	öffentlich erreichbare Dienste
Servernetz	interne Server
Managementnetz	Administration
Gastnetz	Gäste ohne Zugriff auf intern
IoT-Netz	Geräte mit eingeschränktem Vertrauen
VPN-Zone	entfernte Benutzer nach VPN-Einwahl

Merksatz:

```
Zonen trennen Systeme nach Schutzbedarf.
```

Gastnetz

Ein Gastnetz ist ein separates Netz für Besucher oder private Geräte.

Ziel:

```
Internetzugang ermöglichen,
aber internes Netz schützen.
```

Typische Regeln:

```
Gastnetz → Internet erlaubt
Gastnetz → internes LAN blockiert
Gastnetz → Managementnetz blockiert
```

Merksatz:

```
Gastnetz darf nicht ins interne Netz führen.
```

Managementnetz

Ein Managementnetz dient zur Administration von Systemen.

Dort können liegen:

```
- Switch-Management
- Firewall-Management
- Server-Management
- Hypervisor-Management
- Storage-Management
- IPMI / iLO / iDRAC
```

Dieses Netz sollte besonders geschützt sein.

Merksatz:

```
Managementzugänge besonders abschotten.
```

IoT-Netz

Ein IoT-Netz trennt Geräte mit höherem Risiko vom restlichen Netz.

Beispiele:

```
- Kameras
- smarte Sensoren
- Türsysteme
- Mediengeräte
- Smart-Home-Geräte
- Drucker je nach Umgebung
```

Regelidee:

```
IoT darf nur notwendige Ziele erreichen.
```

Merksatz:

```
IoT-Geräte nicht blind ins Hauptnetz lassen.
```

Firewall und VPN

VPN-Zugänge sollten in Firewall-Regeln berücksichtigt werden.

Beispiel:

```
VPN-Benutzer dürfen nur bestimmte interne Dienste erreichen.
```

Nicht automatisch:

```
VPN darf alles im LAN.
```

Besser:

```
VPN-Zone mit gezielten Regeln.
```

Merksatz:

```
VPN-Zugriff ebenfalls nach Least Privilege regeln.
```

Firewall und Monitoring

Firewalls sollten überwacht werden.

Wichtige Punkte:

```
- CPU und RAM
- Verbindungsanzahl
- blockierte Angriffe
- VPN-Verbindungen
- Regel-Treffer
```

- ungewöhnlicher Traffic
- Interface-Auslastung
- Lizenzstatus
- Updates
- Log-Speicher

Merksatz:

Firewall ist kritische Infrastruktur und muss überwacht werden.

Firewall-Fehlersuche systematisch

Eine sinnvolle Reihenfolge:

1. Quelle bestimmen.
2. Ziel bestimmen.
3. Protokoll bestimmen.
4. Port bestimmen.
5. Richtung bestimmen.
6. Zone oder Interface bestimmen.
7. DNS-Auflösung prüfen.
8. Routing prüfen.
9. NAT-Regeln prüfen.
10. Firewall-Regeln prüfen.
11. Logs prüfen.
12. Dienst auf Zielsystem prüfen.
13. Rückweg prüfen.

Merksatz:

Quelle,
Ziel,
Port,
Richtung
und Logs sind entscheidend.

Was Firewalls nicht machen

Firewalls machen nicht automatisch:

- Anwendungen fehlerfrei
- Benutzer sicher
- Passwörter stark
- Systeme gepatcht
- Malware unmöglich
- Daten verschlüsselt
- Berechtigungen korrekt
- Backups vorhanden
- Logs automatisch ausgewertet

Merksatz:

Firewall ist wichtig,
aber nur ein Teil des Sicherheitskonzepts.

Typische IHK-Fragen

In AP1 und AP2 kann zum Beispiel gefragt werden:

- Was macht eine Firewall?
- Was ist der Unterschied zwischen Firewall und NAT?
- Was bedeutet Stateful Inspection?
- Was ist eine DMZ?
- Warum stellt man öffentliche Server in eine DMZ?
- Was ist NAT?
- Was ist PAT?
- Was ist eine Portweiterleitung?
- Was ist der Unterschied zwischen Source NAT und Destination NAT?
- Warum ist Default Deny sicherer?
- Warum ist die Regelreihenfolge wichtig?
- Warum sollte man Any-Any-Regeln vermeiden?
- Warum funktioniert ein Dienst trotz NAT-Regel nicht?
- Was ist der Unterschied zwischen Routing und Firewall?
- Warum können interne und externe Zugriffe unterschiedlich funktionieren?
- Was ist Hairpin NAT?
- Was ist Split DNS?

- Was bedeutet CGNAT?

Typische Prüfungsfallen

Firewall ist nicht NAT.

NAT ist nicht automatisch Firewall.

NAT übersetzt Adressen.

Firewall erlaubt oder blockiert Verkehr.

PAT übersetzt zusätzlich Ports.

Portweiterleitung macht interne Dienste von außen erreichbar.

NAT-Regel allein reicht nicht,
wenn Firewall blockiert.

Firewall-Regeln haben eine Richtung.

Regelreihenfolge ist wichtig.

Spezifische Regeln vor allgemeine Regeln.

Default Deny ist sicherer als Default Allow.

Any-Any-Regeln vermeiden.

DMZ ist nicht das interne LAN.

DMZ-Server dürfen nicht automatisch alles im LAN erreichen.

Öffentliche Dienste gehören besser in die DMZ.

Routing entscheidet den Weg.

Firewall entscheidet die Erlaubnis.

Port 443 offen heißt nicht,
dass HTTPS korrekt funktioniert.

CGNAT kann eingehende Portweiterleitungen verhindern.

Hairpin NAT betrifft internen Zugriff über öffentliche Adresse.

Split DNS kann Hairpin NAT vermeiden.

Wichtige Begriffe kurz erklärt

Begriff	Kurze Erklärung
Firewall	kontrolliert Netzwerkverkehr
Paketfilter	prüft IP-Adressen, Ports und Protokolle
Stateful Firewall	merkt sich Verbindungszustände
Stateful Inspection	Prüfung, ob Verkehr zu bestehender Verbindung gehört
Regel	Bedingung mit Aktion
Allow	erlauben
Deny	blockieren
Drop	still verwerfen
Reject	aktiv ablehnen
Default Deny	alles blockieren außer ausdrücklich erlaubt
Zone	Sicherheitsbereich im Netzwerk
DMZ	separates Netz für öffentliche Dienste
NAT	Übersetzung von IP-Adressen
PAT	Übersetzung von IP-Adressen und Ports
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-Antworten
CGNAT	Provider-NAT für mehrere Kunden
Any-Any	sehr weit gefasste Regel
Bastion Host	abgesicherter Sprungserver

Begriff	Kurze Erklärung
Managementnetz	Netz für Administration

IHK-sichere Kurzformulierung

Eine Firewall kontrolliert Netzwerkverkehr zwischen Systemen oder Netzbereichen und entscheidet anhand von Regeln, ob Verbindungen erlaubt oder blockiert werden. Typische Kriterien sind Quelle, Ziel, Protokoll, Port, Richtung und Zone. Eine Stateful Firewall berücksichtigt zusätzlich den Zustand bestehender Verbindungen. NAT übersetzt IP-Adressen, während PAT zusätzlich Ports übersetzt. Eine Portweiterleitung ist eine Form von Destination NAT, bei der ein externer Port an ein internes Ziel weitergeleitet wird. Eine DMZ ist ein separates Netz für Dienste, die von außen erreichbar sein müssen, damit diese nicht direkt im internen LAN stehen. Firewall, NAT, Routing und DNS müssen gemeinsam korrekt konfiguriert sein, damit ein Dienst erreichbar ist.

Merksätze

Firewall kontrolliert Verkehr.

NAT übersetzt Adressen.

PAT übersetzt Adressen und Ports.

Firewall ist nicht NAT.

NAT ist nicht automatisch Firewall.

Routing findet den Weg.

Firewall erlaubt den Weg.

Default Deny ist sicherer.

Regelreihenfolge ist wichtig.

Spezifisch vor allgemein.

Any-Any vermeiden.

Drop schweigt.

Reject antwortet.

Stateful Firewall kennt Verbindungen.

DMZ = separates Netz für öffentliche Dienste.

DMZ schützt internes LAN.

DMZ darf keine freie Brücke ins LAN sein.

Portweiterleitung macht internen Dienst extern erreichbar.

NAT-Regel plus Firewall-Regel müssen passen.

Source NAT ändert Quelle.

Destination NAT ändert Ziel.

Private IPv4-Adressen sind intern gedacht.

Öffentliche IP-Adressen sind im Internet routbar.

CGNAT erschwert eingehende Verbindungen.

Hairpin NAT = intern über öffentliche Adresse.

Split DNS = intern andere Antwort als extern.

Jeder offene Port ist ein Risiko.

Firewall-Regeln dokumentieren und regelmäßig prüfen.