20.8 Trainer – Firewall, NAT, PAT, Portweiterleitung und DMZ

Diese Trainer-Seite wiederholt Firewalls, NAT, PAT, Portweiterleitung und DMZ.

Ziel ist, typische Prüfungsfragen zu Sicherheitszonen, Firewall-Regeln, Adressübersetzung, öffentlichen Diensten und Fehlersuche sicher zu beantworten.

Merksatz:

```
Firewall filtert.
NAT übersetzt.
PAT nutzt Ports.
DMZ trennt öffentliche Dienste vom internen Netz.
```

Lernziele

Nach dieser Seite solltest du sicher können:

```
- Firewall und NAT unterscheiden
- Firewall-Regeln fachlich sauber beschreiben
- Default Deny erklären
- Any-to-Any-Regeln bewerten
- NAT,
  PAT
  und Portweiterleitung unterscheiden
- private IPv4-Adressen einordnen
- DMZ erklären
- Sicherheitszonen verstehen
- typische Fehler bei Firewall,
  NAT
  und Portweiterleitung erkennen
```

Kurzüberblick

Begriff	Hauptaufgabe
Firewall	Verkehr erlauben oder blockieren

Begriff	Hauptaufgabe
NAT	IP-Adressen übersetzen
PAT	IP-Adressen und Ports übersetzen
Portweiterleitung	externen Port auf internen Dienst weiterleiten
DMZ	öffentlich erreichbare Dienste vom internen Netz trennen
Default Deny	standardmäßig blockieren, nur gezielt erlauben
Any-to-Any	jede Quelle zu jedem Ziel, meist kritisch

Merksatz:

```
Nicht alles,
was auf demselben Gerät läuft,
ist fachlich dasselbe.
```

Aufgabe 1

Was macht eine Firewall?

Antwort anzeigen

Eine Firewall filtert Netzwerkverkehr.

Sie entscheidet anhand von Regeln, ob Verkehr erlaubt oder blockiert wird.

Typische Kriterien:

```
Quelle

Ziel

Port

Protokoll

Richtung

Zone
```

Benutzer

Anwendung

Zustand der Verbindung

Merksatz:

Firewall = kontrollierter Verkehr.

Aufgabe 2

Welche Angaben gehören in eine saubere Firewall-Regel?

Antwort anzeigen

Eine saubere Firewall-Regel enthält:

Quelle

Ziel

Protokoll

Port

Richtung

Aktion

Zweck

Verantwortlicher

Datum oder Änderungsgrund

Beispiel:

Quelle	Ziel	Protokoll	Port	Aktion	Zweck
Adminnetz	Server	TCP	22	erlauben	SSH-Administration
Internet	Datenbank	TCP	5432	blockieren	Datenbank schützen
Clientnetz	Webserver-DMZ	TCP	443	erlauben	HTTPS-Zugriff

Merksatz:

> Firewall-Regeln brauchen Quelle,
> Ziel,
> Port,
> Protokoll
> und Zweck.

Aufgabe 3

Was bedeutet Default Deny?

Antwort anzeigen

Default Deny bedeutet:

> Standardmäßig ist Verkehr verboten.

Nur ausdrücklich erlaubter Verkehr wird zugelassen.

Vorteile:

> kleinere Angriffsfläche
>
> bessere Kontrolle
>
> weniger unbeabsichtigte Freigaben

klarere Sicherheitsstruktur

Merksatz:

Erst blockieren,
dann gezielt erlauben.

Aufgabe 4

Warum ist eine Any-to-Any-Regel kritisch?

Antwort anzeigen

Any-to-Any bedeutet:

jede Quelle

zu

jedem Ziel

Risiken:

sehr große Angriffsfläche

schlechte Nachvollziehbarkeit

Sicherheitszonen werden umgangen

unnötige Freigaben

Fehler schwerer erkennbar

Besser:

genaue Regel mit Quelle,
Ziel,
Port,
Protokoll
und dokumentiertem Zweck.

Merksatz:

Any-to-Any ist fast immer kritisch.

Aufgabe 5

Was ist der Unterschied zwischen Stateless Firewall und Stateful Firewall?

Antwort anzeigen

Stateless Firewall:

prüft jedes Paket einzeln

merkt sich keinen Verbindungszustand

Stateful Firewall:

merkt sich bestehende Verbindungen

lässt Antwortpakete zu bestehenden Verbindungen automatisch zu

Beispiel:

Client startet HTTPS-Verbindung nach außen.

Stateful Firewall erkennt,
dass die Antwortpakete zur bestehenden Verbindung gehören.

Merksatz:

```
Stateful Firewall kennt Verbindungszustände.
```

Aufgabe 6

Was ist eine Firewall-Zone?

Antwort anzeigen

Eine Firewall-Zone ist ein Netzbereich mit bestimmtem Schutzbedarf.

Beispiele:

```
Internet

DMZ

internes Netz

Servernetz

Clientnetz

Gastnetz

Managementnetz
```

Ziel:

```
Regeln übersichtlich nach Sicherheitsbereichen aufbauen.
```

Merksatz:

```
Zonen strukturieren Sicherheitsregeln.
```

Aufgabe 7

Was ist eine DMZ?

Antwort anzeigen

DMZ steht für:

```
Demilitarized Zone
```

Eine DMZ ist ein getrenntes Netzwerk für Dienste, die von außen erreichbar sein müssen.

Beispiele:

```
Webserver

Reverse Proxy

Mail-Gateway

VPN-Gateway
```

Ziel:

```
öffentliche Dienste vom internen Netz trennen.
```

Merksatz:

```
DMZ trennt öffentliche Dienste vom internen Netz.
```

Aufgabe 8

Warum stellt man öffentlich erreichbare Server nicht direkt ins interne Netz?

Antwort anzeigen

Öffentlich erreichbare Server haben eine größere Angriffsfläche.

Wenn ein solcher Server kompromittiert wird, soll der Angreifer nicht direkt Zugriff auf interne Systeme erhalten.

Deshalb werden solche Systeme in eine DMZ gestellt und durch Firewall-Regeln vom internen Netz getrennt.

Merksatz:

```
Öffentliche Dienste gehören in eine getrennte Zone.
```

Aufgabe 9

Welche Regel ist sicherer?

```
A:
Internet zu internes Netz,
any,
erlauben

B:
Internet zu Webserver-DMZ,
TCP 443,
erlauben
```

Antwort anzeigen

Sicherer ist:

```
B
```

Begründung:

```
Die Regel ist gezielter.
Sie erlaubt nur HTTPS-Verkehr zum Webserver in der DMZ.
Regel A erlaubt dagegen sehr breit Verkehr aus dem Internet ins interne Netz.
```

Merksatz:

Je genauer die Regel,
desto besser kontrollierbar.

Aufgabe 10

Was ist NAT?

Antwort anzeigen

NAT steht für:

Network Address Translation

Aufgabe:

IP-Adressen übersetzen.

Typischer Einsatz:

private interne IPv4-Adressen werden beim Zugriff ins Internet
in eine öffentliche IPv4-Adresse übersetzt.

Merksatz:

NAT übersetzt Adressen.

Aufgabe 11

Warum wird NAT häufig eingesetzt?

Antwort anzeigen

Gründe:

private IPv4-Adressen intern nutzen

öffentliche IPv4-Adressen sparen

vielen Clients Internetzugriff ermöglichen

interne Adressen nach außen verbergen

Wichtig:

NAT ersetzt keine Firewall.

Merksatz:

NAT hilft bei Adressübersetzung,
ist aber kein vollständiges Sicherheitskonzept.

Aufgabe 12

Welche privaten IPv4-Bereiche gibt es?

Antwort anzeigen

Private IPv4-Bereiche:

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

Merksatz:

Private IPv4-Adressen werden im Internet nicht direkt geroutet.

Aufgabe 13

Was ist PAT?

Antwort anzeigen

PAT steht für:

Port Address Translation

PAT ist eine Form von NAT, bei der zusätzlich Portnummern genutzt werden.

Zweck:

Viele interne Clients können über eine öffentliche IP-Adresse ins Internet,
weil Verbindungen über Ports unterschieden werden.

Merksatz:

PAT nutzt Ports zur Unterscheidung mehrerer Verbindungen.

Aufgabe 14

Was ist der Unterschied zwischen NAT und PAT?

Antwort anzeigen

NAT:

übersetzt IP-Adressen

PAT:

übersetzt IP-Adressen und Ports

Typischer Praxisfall:

Viele interne Geräte nutzen über PAT eine gemeinsame öffentliche IP-Adresse.

Merksatz:

```
NAT übersetzt Adressen.
PAT übersetzt Adressen und Ports.
```

Aufgabe 15

Was ist Portweiterleitung?

Antwort anzeigen

Portweiterleitung bedeutet:

```
Eingehender Verkehr auf einem externen Port
wird an einen internen Dienst weitergeleitet.
```

Beispiel:

```
öffentliche IP:
TCP 443

wird weitergeleitet an:

interner Webserver:
192.168.10.20 TCP 443
```

Merksatz:

```
Portweiterleitung macht interne Dienste von außen erreichbar.
```

Aufgabe 16

Warum erhöht Portweiterleitung die Angriffsfläche?

Antwort anzeigen

Portweiterleitung macht einen internen Dienst von außen erreichbar.

Dadurch kann der Dienst aus dem Internet angegriffen werden.

Risiken:

```
Exploits

Brute-Force-Angriffe

Fehlkonfiguration

Datenabfluss

DoS
```

Schutzmaßnahmen:

```
nur notwendige Ports freigeben

Dienst patchen

starke Authentifizierung

TLS nutzen

Logging aktivieren

Zugriff einschränken

DMZ verwenden
```

Merksatz:

```
Jeder veröffentlichte Port ist eine mögliche Angriffsfläche.
```

Aufgabe 17

Was ist der Unterschied zwischen ausgehendem NAT und Portweiterleitung?

Antwort anzeigen

Ausgehendes NAT:

```
interne Clients greifen nach außen zu

private IP wird nach außen übersetzt
```

Portweiterleitung:

```
externe Clients greifen auf internen Dienst zu

externer Port wird nach intern weitergeleitet
```

Merksatz:

```
NAT nach außen ist nicht dasselbe wie Zugriff von außen nach innen.
```

Aufgabe 18

Was ist der Unterschied zwischen NAT und Firewall?

Antwort anzeigen

NAT:

```
übersetzt Adressen
```

Firewall:

```
erlaubt oder blockiert Verkehr
```

Wichtig:

Viele Geräte kombinieren beide Funktionen.
Fachlich bleiben sie verschieden.

Merksatz:

NAT übersetzt.
Firewall filtert.

Aufgabe 19

Ein Client erreicht lokale Geräte, aber keine Internetziele.

Welche Themen sind wahrscheinlich?

Antwort anzeigen

Mögliche Ursachen:

Standardgateway fehlt

Standardgateway falsch

Routingfehler

NAT fehlt oder fehlerhaft

Firewall blockiert

Providerverbindung gestört

DNS zusätzlich bei Zugriff über Namen

Merksatz:

Lokal ja,
extern nein:

```
Gateway,
Routing,
NAT
oder Firewall prüfen.
```

Aufgabe 20

Ein Client erreicht eine externe IP-Adresse, aber keine Webseite per Namen.

Ist NAT wahrscheinlich das Hauptproblem?

Antwort anzeigen

Eher nein.

Wenn externe IP-Adressen erreichbar sind, funktionieren Gateway, Routing und NAT wahrscheinlich grundsätzlich.

Wenn nur Namen nicht funktionieren, ist DNS wahrscheinlicher.

Merksatz:

```
IP ja,
Name nein:
DNS.
```

Aufgabe 21

Eine Portweiterleitung auf einen internen Webserver funktioniert nicht.

Nenne mögliche Ursachen.

Antwort anzeigen

Mögliche Ursachen:

falscher externer Port

falsche interne IP-Adresse

falscher interner Port

Webdienst läuft nicht

Dienst lauscht nicht auf richtiger Schnittstelle

lokale Firewall blockiert

Router-Firewall blockiert

NAT-Regel fehlt oder falsch

DNS zeigt auf falsche öffentliche IP

doppeltes NAT

CGNAT beim Provider

Zertifikat oder Anwendung fehlerhaft

Merksatz:

Portweiterleitung braucht DNS,
NAT,
Firewall
und laufenden Dienst.

Aufgabe 22

Was ist doppeltes NAT?

Antwort anzeigen

Doppeltes NAT bedeutet:

```
Verkehr wird durch zwei NAT-Geräte übersetzt.
```

Beispiel:

```
Provider-Router

und dahinter

eigener Router
```

Problem:

```
Portweiterleitungen werden schwieriger,
weil beide Geräte korrekt konfiguriert werden müssen.
```

Merksatz:

```
Doppeltes NAT erschwert eingehende Verbindungen.
```

Aufgabe 23

Was ist CGNAT?

Antwort anzeigen

CGNAT steht für:

```
Carrier-Grade NAT
```

Dabei teilt der Provider öffentliche IPv4-Adressen auf mehrere Kunden auf.

Problem:

Der Kunde hat oft keine eigene öffentlich erreichbare IPv4-Adresse.
Eingehende Portweiterleitungen funktionieren dadurch meist nicht direkt.

Merksatz:

CGNAT erschwert Zugriff von außen auf eigene Dienste.

Aufgabe 24

Warum kann eine Portweiterleitung trotz korrekter Router-Regel nicht funktionieren, wenn der Provider CGNAT nutzt?

Antwort anzeigen

Bei CGNAT liegt die öffentliche IPv4-Adresse nicht direkt am eigenen Router.

Der Router ist hinter einer NAT-Struktur des Providers.

Dadurch erreichen eingehende Verbindungen die eigene Portweiterleitung nicht direkt.

Merksatz:

Ohne eigene öffentliche IPv4-Adresse ist Portweiterleitung von außen schwierig.

Aufgabe 25

Was ist Hairpin NAT oder NAT Loopback?

Antwort anzeigen

Hairpin NAT oder NAT Loopback bedeutet:

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

Der Router leitet die Verbindung wieder zurück ins interne Netz.

Problem:

Nicht jeder Router unterstützt das sauber.

Merksatz:

Hairpin NAT betrifft internen Zugriff über externe Adresse.

Aufgabe 26

Warum kann ein Dienst intern funktionieren, aber extern nicht?

Antwort anzeigen

Mögliche Ursachen:

Portweiterleitung fehlt

externe Firewall blockiert

öffentliche IP falsch

DNS zeigt falsch

doppeltes NAT

CGNAT

Dienst bindet nur an interne Adresse

Zertifikat oder Hostname falsch

Provider blockiert Port

Merksatz:

Intern erreichbar heißt nicht automatisch extern erreichbar.

Aufgabe 27

Warum kann ein Dienst extern funktionieren, aber intern über die öffentliche Domain nicht?

Antwort anzeigen

Mögliche Ursachen:

Hairpin NAT fehlt

Split-DNS fehlt

interne DNS-Auflösung zeigt auf falsche Adresse

Firewall-Regel für internen Zugriff fehlt

Zertifikat oder Hostname passt nicht

Merksatz:

Externe Domain intern nutzen:
Hairpin NAT oder Split-DNS prüfen.

Aufgabe 28

Was ist Split-DNS im Zusammenhang mit internen Diensten?

Antwort anzeigen

Split-DNS bedeutet:

Ein Name kann intern und extern unterschiedlich aufgelöst werden.

Beispiel:

```
extern:
app.firma.de zeigt auf öffentliche IP

intern:
app.firma.de zeigt auf interne IP
```

Vorteil:

```
interne Clients können den Dienst direkt intern erreichen,
ohne Hairpin NAT zu benötigen.
```

Merksatz:

```
Split-DNS kann interne und externe Wege trennen.
```

Aufgabe 29

Ein Webserver in der DMZ soll aus dem Internet erreichbar sein.

Welche Regel ist sinnvoll?

Antwort anzeigen

Sinnvolle Regel:

```
Quelle:
Internet

Ziel:
Webserver in der DMZ

Protokoll:
TCP
```

Port:
443

Aktion:
erlauben

Zweck:
HTTPS-Zugriff auf Webserver

Wichtig:

Nicht pauschal Zugriff vom Internet ins interne Netz erlauben.

Merksatz:

Öffentlich nur den benötigten Dienst freigeben.

Aufgabe 30

Ein Webserver in der DMZ braucht Zugriff auf eine interne Datenbank.

Wie sollte die Regel aussehen?

Antwort anzeigen

Gezielte Regel:

Quelle:
Webserver-DMZ

Ziel:
Datenbankserver intern

Protokoll:
TCP

Port:
Datenbankport,
zum Beispiel 5432 oder 3306

Aktion:
erlauben

Zweck:
Anwendung greift auf Datenbank zu

Wichtig:

Nur exakt benötigten Zugriff erlauben.
Kein Any-to-Any zwischen DMZ und internem Netz.

Merksatz:

DMZ zu intern nur minimal und gezielt erlauben.

Aufgabe 31

Warum sollte ein Datenbankserver nicht direkt aus dem Internet erreichbar sein?

Antwort anzeigen

Ein Datenbankserver enthält oft sensible Daten und ist ein attraktives Angriffsziel.

Risiken:

Brute Force

Exploits

Datenabfluss

Manipulation

```
DoS
```

Besser:

```
Zugriff nur vom Anwendungsserver

Firewall-Beschränkung

kein direkter Internetzugriff

starke Authentifizierung

Monitoring
```

Merksatz:

```
Datenbankports gehören nicht offen ins Internet.
```

Aufgabe 32

Was ist eine gute Regel für ein Gastnetz?

Antwort anzeigen

Typische Regeln:

```
Gastnetz zu Internet:
erlauben

Gastnetz zu internem Netz:
blockieren

Gastnetz zu Managementnetz:
blockieren
```

```
Gastnetz zu Servernetz:
blockieren,
außer ausdrücklich benötigte Dienste
```

Merksatz:

```
Gastnetz nur ins Internet,
nicht ins interne Netz.
```

Aufgabe 33

Was ist eine gute Regel für ein Managementnetz?

Antwort anzeigen

Ein Managementnetz sollte nur für Administration genutzt werden.

Typische Regeln:

```
Adminnetz zu Servern:
benötigte Adminports erlauben

Adminnetz zu Switches:
SSH oder HTTPS erlauben

normale Clientnetze zu Management:
blockieren

Internet zu Management:
blockieren
```

Merksatz:

```
Managementzugänge besonders schützen.
```

Aufgabe 34

Ein Porttest von außen schlägt fehl. Welche Punkte prüfst du?

Antwort anzeigen

Prüfen:

```
richtige öffentliche IP?

DNS zeigt auf richtige IP?

Portweiterleitung korrekt?

externe Firewall erlaubt?

interne Firewall erlaubt?

Dienst läuft intern?

Dienst lauscht auf richtigem Port?

Dienst lauscht auf richtiger Schnittstelle?

doppeltes NAT?

CGNAT?

Provider blockiert Port?
```

Merksatz:

```
Externer Porttest:
DNS,
NAT,
Firewall,
Dienst
und Provider prüfen.
```

Aufgabe 35

Warum reicht die Aussage „Firewall prüfen“ in der Prüfung oft nicht aus?

Antwort anzeigen

Die Aussage ist zu ungenau.

Besser ist:

```
Quelle prüfen

Ziel prüfen

Port prüfen

Protokoll prüfen

Richtung prüfen

Zone prüfen

Regelreihenfolge prüfen

Firewall-Logs prüfen
```

Merksatz:

```
Firewallprüfung braucht konkrete Angaben.
```

Aufgabe 36

Was ist Regelreihenfolge bei Firewalls?

Antwort anzeigen

Viele Firewalls verarbeiten Regeln in einer bestimmten Reihenfolge.

Eine frühere Regel kann spätere Regeln überdecken.

Beispiel:

Eine Block-Regel vor einer Erlauben-Regel kann Zugriff verhindern.

Merksatz:

Bei Firewalls auch Regelreihenfolge prüfen.

Aufgabe 37

Welche Antwort ist besser?

Aufgabe:

Warum ersetzt NAT keine Firewall?

Antwort A:

Weil NAT anders heißt.

Antwort B:

NAT übersetzt IP-Adressen.
Eine Firewall entscheidet dagegen,
welcher Verkehr erlaubt oder blockiert wird.
NAT kann interne Adressen verbergen,
ersetzt aber keine gezielte Zugriffskontrolle.

Antwort anzeigen

B ist besser.

Begründung:

Die Antwort trennt die Funktionen fachlich korrekt.

Merksatz:

NAT übersetzt,
Firewall kontrolliert.

Aufgabe 38

Welche Antwort ist besser?

Aufgabe:

Warum ist eine DMZ sinnvoll?

Antwort A:

Weil man das bei Servern macht.

Antwort B:

Eine DMZ trennt öffentlich erreichbare Dienste vom internen Netz.
Wenn ein Server in der DMZ kompromittiert wird,
soll der Zugriff auf interne Systeme durch Firewall-Regeln begrenzt bleiben.

Antwort anzeigen

B ist besser.

Begründung:

Die Antwort erklärt den Sicherheitszweck der DMZ.

Merksatz:

DMZ begrenzt Schaden bei öffentlichen Diensten.

Aufgabe 39

Welche Antwort ist besser?

Aufgabe:

```
Eine Portweiterleitung funktioniert nicht.
Nennen Sie sinnvolle Prüfungen.
```

Antwort A:

```
Router ist wahrscheinlich kaputt.
```

Antwort B:

```
Es sollten öffentliche IP,
DNS,
externer Port,
interne Ziel-IP,
interner Port,
Dienststatus,
lokale Firewall,
Router-Firewall,
doppeltes NAT
und CGNAT geprüft werden.
```

Antwort anzeigen

B ist besser.

Begründung:

```
Die Antwort nennt systematisch die beteiligten Komponenten.
```

Merksatz:

```
Portweiterleitung ist Zusammenspiel aus DNS,
NAT,
Firewall
```

und Dienst.

Aufgabe 40

Welche Antwort ist besser?

Aufgabe:

Warum ist Any-to-Any kritisch?

Antwort A:

Weil viel erlaubt ist.

Antwort B:

Any-to-Any erlaubt Verkehr von jeder Quelle zu jedem Ziel.
Dadurch entsteht eine große Angriffsfläche,
Sicherheitszonen werden umgangen
und die Regel ist schwer nachvollziehbar.
Besser sind gezielte Regeln mit Quelle,
Ziel,
Port,
Protokoll
und Zweck.

Antwort anzeigen

B ist besser.

Begründung:

Die Antwort nennt konkrete Risiken
und eine bessere Alternative.

Merksatz:

Bewertung braucht Risiko und bessere Maßnahme.

Mini-Prüfung: schnelle Zuordnung

Frage	Antwort
Was macht eine Firewall?	Verkehr filtern
Was macht NAT?	IP-Adressen übersetzen
Was macht PAT?	IP-Adressen und Ports übersetzen
Was macht Portweiterleitung?	externen Port nach intern weiterleiten
Was bedeutet DMZ?	getrennte Zone für öffentliche Dienste
Was bedeutet Default Deny?	standardmäßig blockieren
Warum ist Any-to-Any kritisch?	zu breite Freigabe
Was sind private IPv4-Bereiche?	10/8, 172.16/12, 192.168/16
Was ist CGNAT?	NAT beim Provider
Was ist doppeltes NAT?	zwei NAT-Geräte hintereinander
Was ist Split-DNS?	interne und externe Namensauflösung unterschiedlich
Was ist Hairpin NAT?	interner Zugriff über öffentliche Adresse

Mini-Prüfung: Fehlerbild erkennen

Fehlerbild	Wahrscheinliches Thema
lokal geht, Internet nicht	Gateway, Routing, NAT, Firewall
externe IP geht, Name nicht	DNS
Portweiterleitung extern geht nicht	NAT, Firewall, DNS, Dienst, CGNAT
intern geht, extern nicht	Portweiterleitung, Firewall, öffentliche IP
extern geht, intern über Domain nicht	Hairpin NAT oder Split-DNS
nur bestimmter Port geht nicht	Firewall, Dienst, Portregel
DMZ-Server erreicht Datenbank nicht	Regel DMZ zu intern prüfen
Gastnetz erreicht interne Server	Firewall-Regeln oder VLAN-Trennung falsch
Datenbank öffentlich erreichbar	Sicherheitsrisiko
Any-to-Any-Regel vorhanden	Sicherheitsrisiko

IHK-sichere Kurzformulierung

Eine Firewall filtert Netzwerkverkehr anhand von Regeln wie Quelle, Ziel, Port, Protokoll, Richtung und Aktion. NAT übersetzt IP-Adressen, während PAT zusätzlich Portnummern nutzt, damit mehrere interne Clients über eine öffentliche IP-Adresse kommunizieren können. Portweiterleitung leitet eingehenden Verkehr von einem externen Port an einen internen Dienst weiter und erhöht dadurch die Angriffsfläche. Eine DMZ ist ein getrenntes Netzwerk für öffentlich erreichbare Dienste, damit diese vom internen Netz getrennt sind. Default Deny bedeutet, dass Verkehr standardmäßig blockiert und nur gezielt erlaubt wird. Any-to-Any-Regeln sind kritisch, weil sie sehr breite Kommunikation erlauben und Sicherheitszonen umgehen können.

Merksätze

Firewall filtert.

NAT übersetzt.

PAT nutzt Ports.

Portweiterleitung veröffentlicht interne Dienste.

DMZ trennt öffentliche Dienste vom internen Netz.

Default Deny ist sicherer als alles erlauben.

Any-to-Any ist kritisch.

Firewall-Regeln brauchen Quelle,
Ziel,
Port,
Protokoll,
Richtung
und Zweck.

Stateful Firewall kennt Verbindungen.

Stateless Firewall prüft Pakete einzeln.

NAT ersetzt keine Firewall.

Private IPv4-Adressen werden im Internet nicht direkt geroutet.

10.0.0.0/8 ist privat.

172.16.0.0/12 ist privat.

192.168.0.0/16 ist privat.

PAT ermöglicht vielen Clients eine öffentliche IP.

Portweiterleitung erhöht die Angriffsfläche.

Öffentliche Dienste gehören in eine DMZ.

Datenbankports gehören nicht offen ins Internet.

Gastnetz gehört nicht ins interne Netz.

Managementzugänge besonders schützen.

Doppeltes NAT erschwert Portweiterleitungen.

CGNAT erschwert eingehende Verbindungen.

Hairpin NAT betrifft internen Zugriff über öffentliche Adresse.

Split-DNS kann interne und externe Wege trennen.

Portweiterleitung braucht DNS,
NAT,
Firewall
und Dienst.

Firewallprüfung braucht konkrete Angaben.

Regelreihenfolge beachten.

DMZ zu intern nur minimal erlauben.

Je genauer die Regel,
desto besser kontrollierbar.