6.6 NAT, PAT und private IP-Adressen

NAT gehört zum Umfeld von OSI-Schicht 3.

NAT steht für:

```
Network Address Translation
```

Auf Deutsch sinngemäß:

```
Netzwerkadressübersetzung
```

NAT wird verwendet, um IP-Adressen beim Übergang zwischen Netzwerken zu ändern.

Typisches Beispiel:

```
Ein privates Heim- oder Firmennetz nutzt interne IPv4-Adressen.
Beim Zugriff ins Internet werden diese in eine öffentliche IPv4-Adresse übersetzt.
```

Merksatz:

```
NAT = Übersetzung von IP-Adressen.
```

Warum braucht man NAT?

IPv4-Adressen sind knapp.

Deshalb verwenden viele lokale Netzwerke private IPv4-Adressen.

Private IPv4-Adressen sind im öffentlichen Internet nicht direkt erreichbar.

Damit Geräte mit privaten Adressen trotzdem ins Internet können, wird NAT verwendet.

Beispiel:

```
PC intern:
192.168.10.20

öffentliche Adresse des Routers:
```

```
93.184.100.10
```

Nach außen sieht die Verbindung so aus, als käme sie von der öffentlichen Adresse des Routers.

Merksatz:

```
NAT ermöglicht Internetzugang für private IPv4-Adressen.
```

Private IPv4-Adressen

Private IPv4-Adressen sind für interne Netzwerke reserviert.

Wichtige private Bereiche:

Bereich	CIDR
10.0.0.0 – 10.255.255.255	10.0.0.0/8
172.16.0.0 – 172.31.255.255	172.16.0.0/12
192.168.0.0 – 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 IPv4-Adressen

Öffentliche IPv4-Adressen sind im Internet eindeutig erreichbar und routbar.

Sie werden zum Beispiel verwendet für:

```
- Internetanschlüsse
- Webserver
- Mailserver
- öffentliche DNS-Server
- Cloud-Systeme
- VPN-Gateways
```

Ein Gerät mit privater IPv4-Adresse braucht für direkte Internetkommunikation normalerweise NAT über ein Gerät mit öffentlicher Adresse.

Merksatz:

```
Öffentliche IPv4-Adressen sind im Internet routbar.
```

Private und öffentliche IP-Adressen unterscheiden

Merkmal	private IPv4-Adresse	öffentliche IPv4-Adresse
Einsatz	internes Netz	Internet
direkt im Internet routbar	nein	ja
Beispiel	192.168.10.20	93.184.216.34
häufig mit NAT	ja	nein
weltweit eindeutig	nur im eigenen Netz	ja

Merksatz:

```
Privat = intern.
Öffentlich = im Internet routbar.
```

Grundprinzip von NAT

Ein internes Gerät sendet ein Paket ins Internet.

Beispiel:

```
Quell-IP intern:
192.168.10.20

Ziel-IP:
8.8.8.8
```

Der Router übersetzt die Quell-IP.

Nach außen sieht das Paket zum Beispiel so aus:

Quell-IP öffentlich:
93.184.100.10

Ziel-IP:
8.8.8.8

Die Antwort aus dem Internet geht zurück an die öffentliche IP des Routers.

Der Router ordnet die Antwort wieder dem internen Gerät zu.

Merksatz:

NAT ersetzt private Adressen durch öffentliche Adressen.

NAT-Tabelle

Ein NAT-Gerät merkt sich, welche interne Verbindung zu welcher externen Verbindung gehört.

Dafür nutzt es eine NAT-Tabelle.

Vereinfacht:

Intern	Extern
192.168.10.20	93.184.100.10
192.168.10.30	93.184.100.10

Bei PAT kommen zusätzlich Ports dazu.

Merksatz:

NAT-Tabelle merkt sich Übersetzungen.

PAT

PAT steht für:

Port Address Translation

PAT ist eine besondere Form von NAT.

Dabei teilen sich viele interne Geräte eine öffentliche IP-Adresse.

Die Unterscheidung erfolgt über Port-Zuordnungen.

Typisches Heimnetz:

```
viele interne Geräte
eine öffentliche IPv4-Adresse
```

Merksatz:

```
PAT = viele interne Geräte über eine öffentliche IP mit Port-Zuordnung.
```

Warum braucht man PAT?

Ohne PAT könnte ein Router bei vielen internen Geräten schwer unterscheiden, zu welchem Gerät eine Antwort gehört.

PAT nutzt deshalb zusätzlich Ports.

Beispiel:

Internes Gerät	interner Port	öffentliche IP	externer Port
192.168.10.20	51520	93.184.100.10	40001
192.168.10.30	51520	93.184.100.10	40002
192.168.10.40	51520	93.184.100.10	40003

Nach außen nutzen alle dieselbe öffentliche IP.

Die Ports unterscheiden die Verbindungen.

Merksatz:

```
PAT unterscheidet Verbindungen über Ports.
```

NAT und PAT im Vergleich

Begriff	Bedeutung	Typischer Einsatz
NAT	Übersetzung von IP-Adressen	private IP zu öffentlicher IP
PAT	Übersetzung mit Port-Zuordnung	viele Geräte teilen eine öffentliche IP

In der Praxis meint man mit „NAT im Heimrouter“ oft PAT.

Merksatz:

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

Source NAT

Source NAT verändert die Quelladresse eines Pakets.

Typischer Fall:

```
internes Gerät → Internet
```

Beispiel vorher:

```
Quell-IP:
192.168.10.20
```

Nach NAT:

```
Quell-IP:
93.184.100.10
```

Ziel:

```
Das Paket kann mit einer öffentlichen Adresse ins Internet gesendet werden.
```

Merksatz:

```
Source NAT verändert die Quell-IP.
```

Destination NAT

Destination NAT verändert die Zieladresse eines Pakets.

Typischer Fall:

Zugriff von außen auf internen Server

Beispiel:

öffentlich:
93.184.100.10:443

wird weitergeleitet an:

intern:
192.168.10.50:443

Das wird häufig bei Portweiterleitungen verwendet.

Merksatz:

Destination NAT verändert die Ziel-IP.

Portweiterleitung

Portweiterleitung bedeutet:

Ein bestimmter Port an der öffentlichen IP wird an ein internes Gerät weitergeleitet.

Beispiel:

öffentliche IP:
93.184.100.10

öffentlicher Port:
443

interner Server:
192.168.10.50

interner Port:
443

Anfragen von außen an 93.184.100.10:443 werden zum internen Server weitergeleitet.

Merksatz:

```
Portweiterleitung macht einen internen Dienst von außen erreichbar.
```

Portweiterleitung und Sicherheit

Portweiterleitungen müssen vorsichtig geplant werden.

Warum?

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

Mögliche Risiken:

```
- Angriffe aus dem Internet
- unsichere Dienste
- schwache Passwörter
- veraltete Software
- falsche Firewall-Regeln
- versehentlich freigegebene Systeme
```

Sinnvolle Schutzmaßnahmen:

```
- nur notwendige Ports freigeben
- Dienste aktuell halten
- starke Authentifizierung nutzen
- Firewall-Regeln einschränken
- VPN bevorzugen
- Logs und Monitoring prüfen
```

Merksatz:

```
Jeder freigegebene Port ist eine Angriffsfläche.
```

NAT und Firewall unterscheiden

NAT und Firewall werden oft verwechselt.

NAT macht:

```
Adressen übersetzen.
```

Firewall macht:

```
Verkehr erlauben oder blockieren.
```

Beide Funktionen können im gleichen Gerät sitzen.

Beispiel:

```
Ein Internet-Router macht NAT
und
filtert gleichzeitig eingehende Verbindungen.
```

Merksatz:

```
NAT ist Übersetzung.
Firewall ist Filterung.
```

NAT und Routing unterscheiden

Routing entscheidet:

```
Wohin wird ein Paket weitergeleitet?
```

NAT verändert:

```
Welche IP-Adresse im Paket steht?
```

Beispiel:

```
Routing:
Paket wird Richtung Internet geschickt.
```

NAT:
private Quell-IP wird zur öffentlichen Quell-IP.

Merksatz:

Routing findet den Weg.
NAT ändert Adressen.

NAT und Schichtenmodell

NAT wird meistens Schicht 3 zugeordnet, weil IP-Adressen verändert werden.

PAT hat zusätzlich Bezug zu Schicht 4, weil Ports verwendet werden.

Technik	Bezug
NAT	Schicht 3
PAT	Schicht 3 mit Schicht-4-Bezug
Firewall nach IP	Schicht 3
Firewall nach TCP-/UDP-Port	Schicht 4
Anwendungsschutz	Schicht 7

Merksatz:

NAT = Schicht 3.
PAT = Schicht 3 mit Ports aus Schicht 4.

Beispiel: Heimnetz mit PAT

Ein Heimnetz hat mehrere Geräte:

Gerät	private IP
Notebook	192.168.0.10
Smartphone	192.168.0.20
Smart-TV	192.168.0.30
NAS	192.168.0.40

Der Router hat nach außen eine öffentliche IPv4-Adresse:

```
93.184.100.10
```

Alle Geräte gehen über diese eine öffentliche Adresse ins Internet.

Der Router unterscheidet die Verbindungen über PAT.

Merksatz:

```
PAT ist typisch für Heimrouter und kleine Firmennetze.
```

Beispiel: Zugriff von innen nach außen

Ein PC öffnet eine Webseite.

Intern:

```
PC:
192.168.10.20

Ziel:
93.184.216.34:443
```

Am Router passiert:

```
Quell-IP wird übersetzt.
Quell-Port wird zugeordnet.
Verbindung wird in NAT-Tabelle gespeichert.
```

Nach außen:

```
öffentliche IP des Routers
mit einem zugeordneten Port
```

Antworten kommen zurück zum Router.

Der Router ordnet sie dem PC zu.

Merksatz:

Von innen nach außen funktioniert NAT meist automatisch.

Beispiel: Zugriff von außen nach innen

Ein externer Client möchte auf einen internen Server zugreifen.

Problem:

Der interne Server hat eine private IP-Adresse.
Diese ist aus dem Internet nicht direkt erreichbar.

Lösung:

Portweiterleitung oder VPN.

Beispiel Portweiterleitung:

Extern:
93.184.100.10:443

Intern:
192.168.10.50:443

Merksatz:

Von außen nach innen braucht man gezielte Freigabe oder VPN.

Statisches NAT

Statisches NAT bedeutet:

Eine interne IP-Adresse wird fest einer externen IP-Adresse zugeordnet.

Beispiel:

```
intern:
192.168.10.50

extern:
93.184.100.50
```

Diese Zuordnung bleibt gleich.

Typischer Einsatz:

```
Server,
die dauerhaft von außen erreichbar sein sollen.
```

Merksatz:

```
Statisches NAT = feste 1:1-Adressübersetzung.
```

Dynamisches NAT

Dynamisches NAT bedeutet:

```
Interne Geräte bekommen bei Bedarf eine externe Adresse aus einem Pool.
```

Beispiel:

```
interner Adressbereich:
192.168.10.0/24

öffentlicher Pool:
93.184.100.10 bis 93.184.100.20
```

Die Zuordnung kann sich ändern.

Merksatz:

```
Dynamisches NAT nutzt einen Adresspool.
```

NAT Overload

NAT Overload ist ein anderer Begriff für PAT.

Dabei teilen sich viele interne Geräte eine öffentliche IP-Adresse.

Die Unterscheidung erfolgt über Ports.

Typischer Einsatz:

```
Internetzugang für viele Clients über eine öffentliche IPv4-Adresse.
```

Merksatz:

```
NAT Overload = PAT.
```

CGNAT

CGNAT steht für:

```
Carrier-Grade NAT
```

Dabei verwendet der Internetanbieter selbst NAT.

Das bedeutet:

```
Der Kunde bekommt keine eigene öffentliche IPv4-Adresse direkt am Router,
sondern eine Adresse hinter dem NAT des Providers.
```

Mögliche Folge:

```
Eingehende Verbindungen von außen sind schwer oder nicht direkt möglich.
```

Typische Probleme:

```
- Portweiterleitung funktioniert nicht wie erwartet
- eigener Server von außen nicht erreichbar
- VPN von außen schwieriger
- Online-Dienste können Einschränkungen haben
```

Merksatz:

> CGNAT bedeutet:
> NAT findet schon beim Provider statt.

CGNAT erkennen

Hinweise auf CGNAT:

> WAN-IP am Router ist nicht die gleiche wie die öffentliche IP,
> die Webseiten anzeigen.

Oder:

> WAN-IP liegt in einem privaten oder speziellen Provider-NAT-Bereich.

Ein häufiger CGNAT-Bereich ist:

> 100.64.0.0/10

Wichtig:

> CGNAT hängt vom Anbieter und Anschluss ab.

Merksatz:

> Bei CGNAT hat der Router oft keine eigene echte öffentliche IPv4-Adresse.

100.64.0.0/10

Der Bereich:

> 100.64.0.0/10

wird häufig für Carrier-Grade NAT verwendet.

Er ist nicht normaler privater RFC1918-Bereich wie:

```
10.0.0.0/8
172.16.0.0/12
192.168.0.0/16
```

Er ist speziell für Provider-NAT vorgesehen.

Merksatz:

```
100.64.0.0/10 weist oft auf CGNAT hin.
```

NAT und Serverbetrieb

Wenn ein interner Server von außen erreichbar sein soll, müssen mehrere Dinge passen.

Prüfpunkte:

```
- öffentliche IP vorhanden?
- kein CGNAT?
- Portweiterleitung korrekt?
- Firewall-Regel erlaubt?
- Server hört auf richtigem Port?
- Ziel-IP intern korrekt?
- DNS zeigt auf richtige öffentliche IP?
- Zertifikat korrekt?
- Dienst sicher konfiguriert?
```

Merksatz:

```
Server hinter NAT braucht Portweiterleitung,
Firewall-Regel
und erreichbare öffentliche Adresse.
```

NAT und VPN

VPN kann helfen, interne Dienste sicher erreichbar zu machen.

Statt einzelne Ports ins Internet zu öffnen, baut man eine verschlüsselte Verbindung ins interne Netz auf.

Vorteile:

- weniger offene Ports
- Zugriff nur für berechtigte Benutzer
- bessere Kontrolle
- interne Dienste bleiben geschützt

Beispiele:

- Standort-VPN
- Remote-Access-VPN
- WireGuard
- IPsec
- OpenVPN

Merksatz:

VPN ist oft sicherer als viele Portweiterleitungen.

NAT und IPv6

Bei IPv6 ist NAT normalerweise nicht notwendig.

Warum?

IPv6 hat einen sehr großen Adressraum.

Geräte können global eindeutige IPv6-Adressen haben.

Aber:

Das bedeutet nicht,
dass sie ungeschützt sein sollen.

Statt NAT braucht man bei IPv6:

- Firewall-Regeln
- Netztrennung

- saubere Adressplanung
- Zugriffskontrolle

Merksatz:

IPv6 braucht normalerweise kein NAT,
aber trotzdem Firewall-Schutz.

NAT ist kein vollständiges Sicherheitskonzept

NAT wird manchmal als Sicherheitsfunktion verstanden.

Das ist nur teilweise richtig.

NAT verhindert oft unbeabsichtigte direkte eingehende Verbindungen, weil keine Zuordnung existiert.

Aber:

NAT ersetzt keine Firewall.
NAT prüft keine Anwendungssicherheit.
NAT erkennt keine Angriffe zuverlässig.
NAT schützt nicht vor unsicheren ausgehenden Verbindungen.

Merksatz:

NAT kann abschirmen,
ist aber keine vollständige Sicherheitslösung.

NAT und Protokollprobleme

Manche Protokolle kommen mit NAT schlechter zurecht.

Warum?

NAT verändert Adressen und manchmal Ports.

Probleme können entstehen bei:

- VoIP
- SIP
- bestimmten VPNs
- Peer-to-Peer-Anwendungen
- Spielen
- Protokollen mit IP-Adressen in den Nutzdaten

Mögliche Lösungen:

- spezielle NAT-Hilfsfunktionen
- STUN / TURN
- VPN
- Portweiterleitung
- Protokollanpassung

Merksatz:

NAT kann Protokolle stören,
wenn Adressen oder Ports wichtig sind.

Hairpin NAT

Hairpin NAT bedeutet:

Ein internes Gerät greift über die öffentliche Adresse auf einen internen Dienst zu.

Beispiel:

Internes Notebook öffnet:
https://meinedomain.de

DNS zeigt auf:

öffentliche IP des Routers

Der Dienst liegt aber intern auf:

```
192.168.10.50
```

Damit das funktioniert, muss der Router Hairpin NAT unterstützen.

Merksatz:

```
Hairpin NAT erlaubt internen Zugriff über die öffentliche Adresse auf interne Dienste.
```

Split DNS als Alternative

Split DNS bedeutet:

```
Interne Clients bekommen für einen Namen eine interne IP-Adresse.
Externe Clients bekommen für denselben Namen eine öffentliche IP-Adresse.
```

Beispiel:

```
intern:
wiki.firma.de → 192.168.10.50

extern:
wiki.firma.de → 93.184.100.10
```

Vorteil:

```
Interne Clients müssen nicht über Hairpin NAT gehen.
```

Merksatz:

```
Split DNS gibt intern und extern unterschiedliche Antworten.
```

NAT und Logs

Bei NAT ist Logging wichtig.

Warum?

Viele interne Geräte können nach außen dieselbe öffentliche IP-Adresse nutzen.

Ohne Logs ist später schwer nachvollziehbar:

welches interne Gerät
zu welcher Zeit
welche externe Verbindung genutzt hat.

Wichtige Informationen:

- interne IP
- interner Port
- öffentliche IP
- externer Port
- Zieladresse
- Zeitstempel

Merksatz:

Bei NAT braucht man Logs,
um Verbindungen nachvollziehen zu können.

Typische NAT-Fehler

Typische Fehler sind:

- NAT-Regel fehlt
- falsche interne Ziel-IP
- falscher Port
- Firewall blockiert
- Dienst läuft nicht
- CGNAT beim Provider
- DNS zeigt auf falsche IP
- doppelte Portweiterleitung
- falsches Interface
- NAT-Regel in falscher Reihenfolge
- Rückroute fehlt

- Hairpin NAT fehlt

Merksatz:

NAT-Fehler können wie Routing-, Firewall- oder DNS-Probleme aussehen.

Fehlerbild: Internet geht nicht

Mögliche NAT-bezogene Ursachen:

- Source NAT fehlt
- PAT falsch konfiguriert
- Default Route fehlt
- Firewall blockiert ausgehend
- Provider-Verbindung gestört
- DNS-Problem
- falsches Gateway
- Rückweg fehlt

Prüfung:

Client-IP prüfen.
Gateway prüfen.
Ping auf externe IP testen.
NAT-Regel prüfen.
Firewall prüfen.
DNS prüfen.

Merksatz:

Internetproblem kann Routing, NAT, Firewall oder DNS sein.

Fehlerbild: Portweiterleitung funktioniert nicht

Mögliche Ursachen:

- keine öffentliche IPv4-Adresse
- CGNAT
- falscher externer Port
- falsche interne IP
- interner Dienst läuft nicht
- Firewall blockiert am Router
- Firewall blockiert am Server
- DNS zeigt falsch
- Test aus internem Netz ohne Hairpin NAT
- ISP blockiert Ports

Merksatz:

Portweiterleitung braucht öffentliche Erreichbarkeit,
NAT-Regel,
Firewall-Freigabe
und laufenden Dienst.

Fehlerbild: Von innen geht es, von außen nicht

Wenn ein Dienst intern funktioniert, aber extern nicht, prüft man:

- öffentliche IP vorhanden?
- CGNAT?
- DNS zeigt auf richtige IP?
- Portweiterleitung korrekt?
- Firewall-Regeln korrekt?
- Dienst hört auf richtiger Schnittstelle?
- Zertifikat oder Reverse Proxy korrekt?
- Provider blockiert Port?

Merksatz:

Intern erreichbar heißt nicht automatisch extern erreichbar.

NAT und Rückweg

NAT funktioniert nur, wenn Antworten zurück zum NAT-Gerät gelangen.

Wenn der Rückweg falsch ist, kann die Verbindung scheitern.

Beispiel:

```
Paket geht über Router A hinaus.
Antwort kommt über Router B zurück.
```

Wenn Router B die NAT-Zuordnung nicht kennt, kann er die Antwort nicht korrekt zuordnen.

Merksatz:

```
NAT braucht passenden Hin- und Rückweg über dasselbe NAT-Gerät.
```

Asymmetrisches Routing und NAT

Asymmetrisches Routing bedeutet:

```
Hinweg und Rückweg nehmen unterschiedliche Pfade.
```

Bei NAT kann das problematisch sein.

Warum?

```
Das NAT-Gerät muss die Verbindung kennen,
um Antworten zurückübersetzen zu können.
```

Wenn die Antwort an einem anderen Gerät ankommt, fehlt dort die passende NAT-Tabelle.

Merksatz:

```
NAT und asymmetrisches Routing passen oft schlecht zusammen.
```

Einordnung in das OSI-Modell

Thema	Schicht
MAC-Adresse	2
VLAN	2
IP-Adresse	3

Thema	Schicht
Routing	3
NAT	3
PAT	3 / 4
TCP-Port	4
UDP-Port	4
Firewall nach IP	3
Firewall nach Port	4
DNS	7

Merksatz:

> NAT verändert IP-Adressen.
> PAT nutzt zusätzlich Ports.

Was NAT nicht macht

NAT macht nicht:

> - DNS-Namen auflösen
> - Dienste starten
> - Benutzer authentifizieren
> - Verschlüsselung bereitstellen
> - automatisch Firewall-Regeln sicher machen
> - Schwachstellen beseitigen
> - Routing ersetzen
> - VLANs trennen

NAT hat eine klare Aufgabe:

> Adressen übersetzen.

Merksatz:

> NAT ist Adressübersetzung,
> keine komplette Sicherheits- oder Netzwerklösung.

Typische IHK-Fragen

In AP1 und AP2 kann zum Beispiel gefragt werden:

- Was bedeutet NAT?
- Warum wird NAT bei IPv4 häufig verwendet?
- Was sind private IPv4-Adressen?
- Was ist der Unterschied zwischen privater und öffentlicher IP-Adresse?
- Was bedeutet PAT?
- Warum können viele interne Geräte eine öffentliche IP-Adresse nutzen?
- Was ist Source NAT?
- Was ist Destination NAT?
- Was ist eine Portweiterleitung?
- Was ist CGNAT?
- Warum funktioniert eine Portweiterleitung bei CGNAT oft nicht?
- Was ist der Unterschied zwischen NAT und Firewall?
- Was ist der Unterschied zwischen NAT und Routing?
- Warum braucht IPv6 normalerweise kein NAT?

Typische Prüfungsfallen

NAT = Network Address Translation.

PAT = Port Address Translation.

NAT übersetzt IP-Adressen.

PAT nutzt zusätzlich Ports.

Private IPv4-Adressen sind im Internet nicht direkt geroutet.

Öffentliche IPv4-Adressen sind im Internet routbar.

10.0.0.0/8 ist privat.

172.16.0.0/12 ist privat.

192.168.0.0/16 ist privat.

100.64.0.0/10 weist oft auf CGNAT hin.

Source NAT verändert die Quell-IP.

Destination NAT verändert die Ziel-IP.

Portweiterleitung macht interne Dienste von außen erreichbar.

NAT ist nicht dasselbe wie Firewall.

NAT ist nicht dasselbe wie Routing.

NAT ersetzt keine Sicherheitsplanung.

IPv6 braucht normalerweise kein NAT.

NAT kann Protokolle stören.

NAT braucht passenden Rückweg.

Wichtige Begriffe kurz erklärt

Begriff	Kurze Erklärung
NAT	Network Address Translation
PAT	Port Address Translation
Source NAT	Übersetzung der Quelladresse
Destination NAT	Übersetzung der Zieladresse
Portweiterleitung	Weiterleitung eines externen Ports an internes Ziel
private IPv4-Adresse	interne IPv4-Adresse, nicht öffentlich geroutet
öffentliche IPv4-Adresse	im Internet routbare IPv4-Adresse
NAT-Tabelle	Zuordnung übersetzter Verbindungen
NAT Overload	anderer Begriff für PAT
CGNAT	Provider-NAT beim Internetanbieter
100.64.0.0/10	häufiger Bereich für CGNAT
Hairpin NAT	interner Zugriff über öffentliche Adresse auf internen Dienst

Begriff	Kurze Erklärung
Split DNS	interne und externe DNS-Antworten unterscheiden sich
Rückroute	Weg zurück zum Absendernetz
asymmetrisches Routing	Hin- und Rückweg sind unterschiedlich

IHK-sichere Kurzformulierung

NAT steht für Network Address Translation und bezeichnet die Übersetzung von IP-Adressen beim Übergang zwischen Netzwerken. Es wird bei IPv4 häufig verwendet, damit Geräte mit privaten IP-Adressen über eine öffentliche IPv4-Adresse ins Internet kommunizieren können. PAT ist eine Form von NAT, bei der zusätzlich Ports verwendet werden, damit viele interne Geräte dieselbe öffentliche IP-Adresse nutzen können. Source NAT verändert die Quelladresse, Destination NAT verändert die Zieladresse und wird häufig bei Portweiterleitungen genutzt. NAT ist nicht dasselbe wie Routing oder Firewall und ersetzt keine Sicherheitsplanung.

Merksätze

NAT = Network Address Translation.

NAT = IP-Adressen übersetzen.

PAT = Port Address Translation.

PAT = NAT mit Port-Zuordnung.

Private IPv4-Adressen sind intern.

Öffentliche IPv4-Adressen sind im Internet routbar.

NAT ermöglicht privaten IPv4-Geräten Internetzugang.

Source NAT verändert die Quell-IP.

Destination NAT verändert die Ziel-IP.

Portweiterleitung macht interne Dienste von außen erreichbar.

NAT-Tabelle merkt sich Übersetzungen.

Heimrouter nutzen meist PAT.

NAT Overload = PAT.

CGNAT = NAT beim Provider.

100.64.0.0/10 weist oft auf CGNAT hin.

NAT ist nicht Firewall.

NAT ist nicht Routing.

Routing findet den Weg.

Firewall erlaubt oder blockiert.

NAT übersetzt Adressen.

IPv6 braucht normalerweise kein NAT.

IPv6 braucht trotzdem Firewall-Regeln.

NAT kann Protokolle stören.

NAT braucht passenden Rückweg.

Portweiterleitung braucht öffentliche Erreichbarkeit,
NAT-Regel,
Firewall-Freigabe
und laufenden Dienst.