# Network Adress Translation (NAT)

## Was ist NAT?

NAT ist die Abkürzung für Network-Address-Translation, eine "Adressübersetzung" zwischen zwei Netzwerken. Meist implementiert der Router diese Adressübersetzung. NAT wird verwendet um, lokale Netzwerke mit dem Internet zu verbinden. Man unterscheidet zwei Typen: Source-NAT (SNAT) und Destination-NAT (DNAT).

## Source-NAT

Privatnutzer kommen mit der Netzwerkadressübersetzung meist in Form von Source-NAT in Berührung. Das Verfahren findet sowohl in Heim- als auch in Firmennetzwerken Anwendungheim, wenn ein Netzwerkgerät mit privater IPv4-Adresse über eine öffentliche IP aufs Internet zugreifen soll. Private IPv4 Subnetze sind IP-Adressen, die für nicht öffentliche IPv4 Bereiche reserviert sind, sie sind nicht direkt im Internet erreichbar.

| Netzadressbereich | CIDR-Notation |
|---|---|
| 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 |

Im allgemeinen Sprachgebrauch wird der Begriff NAT jedoch nicht immer trennscharf verwendet.

## NAT und PAT

Man muss unterscheiden, ob jeder einzelnen privaten IP-Adresse in einem lokalen Netzwerk eine eigene öffentliche IP-Adresse zugeordnet wird, dann findet also eine 1:1-Übersetzung statt, oder ob sich alle Netzwerkgeräte im LAN dieselbe öffentliche IP-Adresse teilen müssen - dann spricht man von einer n:1-Übersetzung.

Eigentlich ist nur eine 1:1-Übersetzung eine Network-Address-Translation, in diesem Fall werden nur die Netzwerkadressen umgeschrieben. Eine n:1-Übersetzung erfordert zusätzlich eine Anpassung der Portnummer. Dieses Verfahren wird deswegen auch als PAT (Port-and-Address-Translation) oder NAPT (Network-Address-Port-Translation) bezeichnet.

Wenn man in IPv4-basierten Heim- und Firmennetzen von NAT spricht, ist damit meistens PAT gemeint, da für gewöhnlich für das gesamte private Netzwerksegment nur eine öffentliche "echt" IPv4 Adresse zur Verfügung steht.

# Wie funktioniert PAT?

Im Regelfall kommt die Netzwerkadressübersetzung in Form von PAT zum Einsatz, um mehrere lokale Geräte über eine gemeinsame IP-Adresse mit dem Internet zu verbinden.

Da private IPs nicht routbar sind (im Internet somit keine Bedeutung haben), müssen Datenpakete, die ein Rechner (Client) im LAN an einen Server im Internet versendet, vom Router mit einer öffentlichen IP versehen werden. Dazu tauscht dieser die im Header des Datenpakets hinterlegte private IP-Adresse des Clients gegen seine eigene öffentliche IP-Adresse aus.

Zudem wird die intern verwendete Portnummer durch einen freien Port des Routers ersetzt. Dieser tritt gegenüber Servern im Internet somit als Absender aller Datenpakete auf, die aus dem lokalen Netzwerk versendet werden.

Sämtliche Verbindungsinformationen (IP-Adressen, Ports und Timeouts) werden in der sogenannten NAT-Tabelle gespeichert (streng genommen müsste man auch hier von einer PAT-Tabelle sprechen). Beantwortet der adressierte Server die Anfrage des lokalen Computers mit einem Datenpaket, wird dieses zunächst an den entsprechenden Port des Routers zurückgesendet. Dieser hat nun die Aufgabe, das eingehende Datenpaket dem jeweiligen Netzwerkgerät zuzuteilen, das die Anfrage gestartet hat. Alles was der Router dazu benötigt, sind die in der NAT-Tabelle hinterlegten Verbindungsinformationen. Verdeutlichen lässt sich dies an einem Beispiel:

Wir nehmen an, ein Router hat von einem Internetserviceprovider (ISP) die öffentliche IP-Adresse 217.229.111.18 zugewiesen bekommen und fungiert als Standardgateway für ein lokales Netzwerk. Dieses stellt für Netzwerkgeräte den privaten IP-Adressbereich 192.168.0.0/24 zur Verfügung (alle Adressen von 192.168.0.0 bis 192.168.0.24). Will nun eines dieser Geräte (z. B. ein Rechner mit der privaten IP-Adresse 192.168.0.2) eine Verbindung ins Internet herstellen (z. B. zu einem Webserver mit der öffentlichen IP 71.123.239.82 an dessen Portnummer 80), reserviert dieses einen internen Port (z.B. 22433) und übermittelt die Aufforderung zum Verbindungsaufbau an den als Standardgateway eingetragenen Router. Dieser ist intern über die private IP 192.168.0.1 adressierbar und kommuniziert nach außen hin mit der öffentlichen IP 217.229.111.18.

Der Router bekommt somit folgende Informationen: Gerät 192.168.0.2 will an Port 22433 eine Verbindung zu 71.123.239.82 an Port 80 aufbauen. Um diesem Wunsch nachzukommen, muss der Router die Quelladresse des LAN-Geräts (IP-Adresse und Portnummer) durch die eigene Absenderadresse ersetzen. Er reserviert daher einen beliebigen freien Port (z. B. 61001) und leitet die Netzwerkadressübersetzung ein: Aus 192.168.0.2:22433 wird 217.229.111.18: 61001. Alle relevanten Informationen werden in der NAT-Tabelle auf dem Router hinterlegt. Private IP des Clients Port des Clients Öffentliche IP des Routers Öffentlicher Port des Routers 192.168.0.2 22433 217.229.111.18 61001

Beim Webserver eingegangen, wird die Anfrage verarbeitet und, wenn möglich, mit dem angeforderten Datenpaket (z. B. den Daten einer Website) beantwortet. Diese Antwort erreicht zunächst den Router und wird von diesem mithilfe der gespeicherten Verbindungsinformationen weitergeleitet: Laut NAT-Tabelle ist der externe Port 61001 für Antwortpakete reserviert, die an den Port 22433 des Netzwerkgeräts 192.168.0.2 zu senden sind.

Neben IP-Adressen und Portnummern notieren Router in der NAT-Tabelle für jede Verbindung eine Zeitmarkierung. Diese dient als Timeout und gibt an, wann der betreffende Eintrag gelöscht werden

kann. So lässt sich sicherstellen, dass Ports bei Inaktivität nicht dauerhaft geöffnet bleiben und möglicherweise zum Einfalltor für Angriffe aus dem Internet werden.