# NAT und PAT

Autor: Moser Tobias

Datum: 30.08.2015

Typ: Aufgaben

Version: 1.0

**INHALT**

# 1 NAT - Network Address Translation

NAT ist ein Verfahren, dass in IP-Routern eingesetzt wird, die lokale Netzwerke mit dem Internet verbinden. Weil Internet-Zugänge in der Regel nur über eine IP-Adresse (IPv4) verfügen, müssen sich alle anderen Stationen im lokalen Netzwerk mit einer privaten IP-Adresse begnügen. Private IP-Adressen dürfen zwar mehrfach verwendet werden, aber besitzen in öffentlichen Netzen keine Gültigkeit. Stationen mit einer privaten IP-Adresse können somit nicht mit Stationen außerhalb des lokalen Netzwerks kommunizieren. Damit trotzdem alle Computer mit privater IP-Adresse Zugang zum Internet bekommen können, muss der Internet-Zugangs-Router in allen ausgehenden Datenpaketen die IP-Adressen der lokalen Stationen durch seine eigene, öffentliche IP-Adresse ersetzen. Damit die eingehenden Datenpakete der richtigen Station zugeordnet werden, speichert der Router die aktuellen TCP-Verbindungen in einer Tabelle. Der NAT-Router merkt sich sozusagen welche Datenpakete zu welcher TCP-Verbindung gehören. Dieses Verfahren nennt man NAT (Network Address Translation).

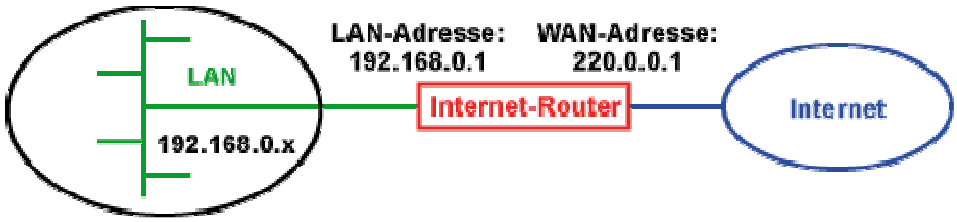
## 1.1 Warum NAT?

Die ersten IP-Netze waren anfangs eigenständige Netz ohne Verbindung nach außen. Deshalb wurden die Stationen häufig mit IP-Adressen aus den privaten Adressräumen versehen. Doch irgendwann entstand der Bedarf, E-Mails über die Grenzen von Unternehmensnetzen auszutauschen und auch auf das World Wide Web (WWW) zuzugreifen. Weil die Stationen ohne eigene öffentliche IP-Adresse keine Verbindung außerhalb des Netzwerks herstellen konnten, wurde mit NAT ein Verfahren eingeführt, dass es jeder Station möglich machte mit Rechnern außerhalb des lokalen Netzwerks zu kommunizieren.
Weil der Adressraum des Protokolls IPv4 zu verschwenderisch verteilt wurde, reichen die IP-Adressen nicht für jeden Computer aus. NAT ist also auch ein Ausweg, um die Adressknappheit von IPv4 kurzfristig aufzulösen. Langfristig muss jedoch ein Internet-Protokoll mit einem größeren Adressraum her. IPv6 ist ein solches Protokoll.

## 1.2 IPv6 und NAT

Durch IPv6 wird NAT überflüssig. Der Wegfall von NAT verbessert den Betrieb von Netzwerken erheblich. Fehler, die durch NAT verursacht wurden, fallen weg. Außerdem lassen sich Fehler schneller finden und beheben.
Ohne NAT werden Protokolle, wie STUN überflüssig. Das freut besonders Entwickler, weil jedes Protokoll, dass nicht implementiert werden muss, erst gar keine Sicherheitslücken aufreißen kann. Doch ohne NAT wird in Zukunft eine gut konfigurierte Firewall wichtiger werden. Bei IPv6 sollte die Firewall Verbindungsversuche von außen nach innen verhindern, wenn vorher keine Verbindung von innen nach außen bestanden hat.

## 2 SNAT - Source Network Address Translation

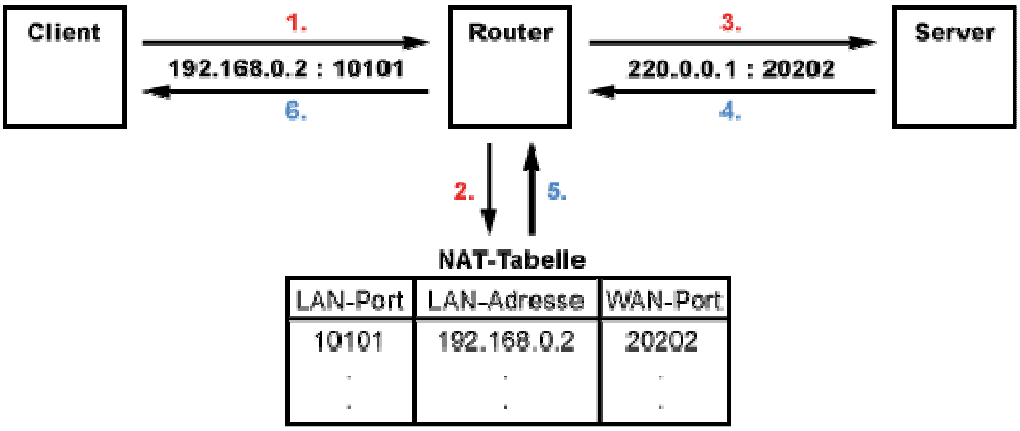



Der Betrieb eines NAT-Routers ist üblicherweise an einem gewöhnlichen Internet-Anschluss. Zum Beispiel über DSL oder Kabelmodem. Der eingesetzte Router dient als Zugang zum Internet und als Standard-Gateway für das lokale Netzwerk. In der Regel wollen über den Router mehr Geräte ins Internet, als öffentliche IP-Adressen zur Verfügung stehen. In der Regel nur eine einzige.
Beispielsweise bekommt der Router des lokalen Netzwerks die öffentliche IP-Adresse 222.0.0.1 für seinen WAN-Port vom Internet Service Provider (ISP) zugewiesen. Weil nur eine öffentliche IP-Adresse vom Internet-Provider zugeteilt wurde, bekommen die Stationen im LAN private IP-Adressen aus speziell dafür reservierten Adressbereichen zugewiesen. Diese Adressen sind nur innerhalb des privaten Netzwerks gültig. Private IP-Adressen werden in öffentlichen Netzen nicht geroutet. Das bedeutet, dass Stationen mit privaten IP-Adressen keine Verbindung ins Internet bekommen können. Damit das trotzdem funktioniert, wurde NAT entwickelt.

Innerhalb des lokalen Netzwerks hat der Router die IP-Adresse 192.168.0.1, die für den LAN-Port gilt und über die der Router im LAN direkt erreichbar und konfiguriert ist. Gleichzeitig handelt es sich dabei um die Adresse des Standard-Gateways und zum Beispiel des lokalen DNS-Servers. Der Router ist also das Standard-Gateway über das alle Verbindung laufen. Mit seiner öffentlichen IP-Adresse tritt der Router als Stellvertreter für alle Stationen seines lokalen Netzwerks (LAN) auf.
Wenn ein Datenpaket mit einer Ziel-Adresse außerhalb des lokalen Netzwerks adressiert ist, dann ersetzt der Router die Quell-Adresse durch seine öffentliche IP-Adresse. Die Port-Nummer (TCP oder UDP) wird durch eine andere Port-Nummer ersetzt. Um später die Antwortpakete der richtigen Station zuordnen zu können führt der Router eine Tabelle mit den geänderten Quell-Adressen und den dazugehörigen Port-Nummern. Wenn also Pakete mit einer bestimmten Port-Nummer zurückkommen, dann ersetzt NAT die Ziel-Adresse durch die richtige Adresse und Port-Nummer.

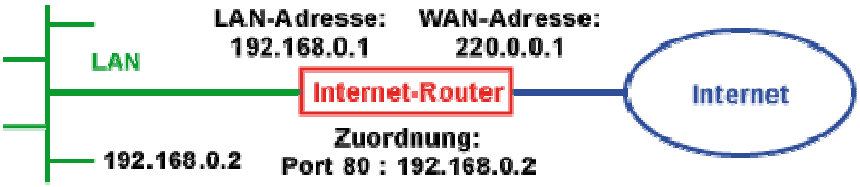
In der NAT-Tabelle hat jeder Eintrag auch eine Zeitmarkierung. Nach einer bestimmten Zeit der Inaktivität wird der betreffende Eintrag gelöscht. Auf diese Weise wird sichergestellt, dass keine Ports offen bleiben.
Weil dieses Verfahren die Absender-Adresse (Source) jedes ausgehenden Datenpakets ändert, nennt man dieses Verfahren Source NAT (SNAT). SNAT bezeichnet man in der Regel einfach als NAT.

## 2.1 Ablauf von SNAT




Der Client schickt seine Datenpakete mit der IP-Adresse 192.168.0.2 und dem TCP-Port 10101 an sein Standard-Gateway, bei dem es sich um einen NAT-Router handelt.
Der NAT-Router tauscht IP-Adresse (LAN-Adresse) und TCP-Port (LAN-Port) aus und speichert beides mit der getauschten Port-Nummer (WAN-Port) in der NAT-Tabelle.
Der Router leitet das Datenpaket mit der WAN-Adresse 220.0.0.1 und der neuen TCP-Port 20202 ins Internet weiter.
Der Empfänger (Server) verarbeitet das Datenpaket und schickt seine Antwort zurück.
Der NAT-Router stellt nun anhand der Port-Nummer 20202 (WAN-Port) fest, für welche IP-Adresse (LAN-Adresse) das Paket im lokalen Netz gedacht ist.
Er tauscht die IP-Adresse und die Port-Nummer wieder aus und leitet das Datenpaket ins lokale Netz weiter, wo es der Client entgegen nimmt.

# 3 DNAT - Destination Network Address Translation (Port-Forwarding)




NAT setzt dynamisch eine öffentliche IP-Adresse auf mehrere private IP-Adressen um. Jede ausgehende Verbindung wird mit IP-Adresse und Portnummer festgehalten. Anhand der Portnummer kann NAT eingehende Datenpakete einer lokalen Station zuordnen. Diese Zuordnung ist allerdings nur für kurze Zeit gültig. Das bedeutet, dass Verbindungen nur aus dem lokalen Netzwerk ins öffentliche Netz aufgebaut werden können, nicht umgekehrt.
Wenn man doch eine Station innerhalb des lokalen Netzwerks dauerhaft aus dem öffentlichen Netz erreichbar machen will, dann ist das nur über einen Umweg möglich. Das Verfahren nennt sich Destination NAT (DNAT), allgemein als Port-Forwarding bekannt. Dabei wird in der Router-Konfiguration ein TCP-Port fest einer IP-Adresse zugeordnet. Daraufhin leitet der Router alle auf diesem Port eingehenden Datenpakete an diese Station weiter.
Vorsicht ist beim Freischalten von TCP-Ports (Port-Forwarding) geboten. Wer keine Server-Dienste im Internet zur Verfügung stellt, sollte alle TCP-Ports des Routers (unter 1024) sperren. Gut vorkonfigurierte Router haben das schon automatisch eingestellt. Wer auf Port-Forwarding nicht verzichten kann, sollte aus Sicherheitsgründen eine Demilitarisierte Zone (DMZ) einrichten und so den Datenverkehr aus dem Internet aus dem lokalen Netzwerk heraus halten.

# 4 Probleme durch NAT

Die Einträge in der NAT-Tabelle sind nur für eine kurze Zeit gültig. Für eine Anwendung, die nur sehr unregelmäßig Daten austauscht, bedeutet das, dass ständig die Verbindung abgebrochen wird. Das hat zur Folge, dass diese Anwendung unter Umständen in einer NAT-Umgebung nicht funktionieren kann.
Um dauerhaft ein Loch in den NAT-Router zu bekommen, wird mit Port-Forwarding gearbeitet. Das bedeutet, dass ein eingehendes Datenpaket mit einem bestimmten TCP-/UDP-Port an eine bestimmte IP-Adresse im lokalen Netzwerk geschickt wird.
Zusätzlich wurden für viele Protokolle Umgehungsmechanismen für NAT entwickelt. In der Regel schicken die in regelmäßigen Abständen Datenpakete aus dem lokalen Netzwerk heraus, um die Einträge in der NAT-Tabelle des Routers aktuell zu halten. Dadurch werden viele Internet-Anwendungen und -Diensten komplizierter, was insgesamt zu mehr Sicherheitslücken führt.
Ein anderes Problem entsteht bei einer hohen Anzahl ausgehender Verbindungen. Dann können NAT-Tabellen überlaufen. Das bedeutet, dass einzelne Verbindungen aus der NAT-Tabelle fliegen und demzufolge Verbindungen abbrechen können.

# 5 NAT als Sicherheitsfeature?

NAT wird besonders in produktnahen Beschreibungen als Sicherheitsmerkmal bezeichnet. Damit ist der Mechanismus gemeint, der als Nebenprodukt verhindert, dass Stationen hinter dem NAT-Router von außerhalb direkt ansprechbar sind. Durch NAT werden von außen initiierte Verbindungsversuche verworfen und bekommen keinen Zugang zum lokalen Netzwerk. Hacker, die zyklisch alle TCP-Ports einer IP-Adresse nach offenen Ports absuchen (Port-Scan) bekommen keine Antwort vom Router.
Man kann sagen, NAT wirkt wie eine rudimentäre Firewall, die alle unberechtigten Zugriffe von außen blockt. Es handelt sich dabei um eine gewollte Schutzfunktion vor unaufgefordertem und unsicherem Datenverkehr.
Doch eher zufällig erweist sich NAT als Sicherheitsmerkmal für lokale Netzwerke. NAT ersetzt keinen Paketfilter und schon gar keine vollwertige Firewall. NAT als Sicherheitsmerkmal zu bezeichnen ist irreführend und fahrlässig. Trotzdem wird dem Laien NAT immer wieder gerne als Sicherheitsfeature verkauft. Doch das ist falsch. NAT verhindert nur Datenverbindungen, die nicht vom lokalen Netzwerk aus initiiert wurden oder für die vorher kein Datenverkehr registriert wurde.

# 6 PAT

**Port and Address Translation** (PAT) oder **Network Address Port Translation** (NAPT) ist eine Technik, die in Computernetzwerken verwendet wird. Sie ist eine spezielle Form von NAT (1 zu n NAT). Dabei werden im Gegensatz zu NAT nicht nur die IP-Adressen, sondern auch Port-Nummern umgeschrieben. **PAT** wird eingesetzt, wenn mehrere private IP-Adressen aus einem LAN zu *einer* öffentlichen IP-Adresse übersetzt werden sollen.

## 6.1 Beispiel

Angenommen für das lokale Netz `192.168.0.0/24` steht die öffentliche IP-Adresse `205.0.0.2` zur Verfügung.

### 6.1.1 Ausgehende Pakete (LAN → WAN)

lokales Netz (LAN) | öffentliches Netz (WAN)

| **Quell IP:Port** | **Ziel IP:Port** | | **Quell IP:Port** | **Ziel IP:Port** |
|---|---|---|---|---|
| **192.168.0.2:5000** | 170.0.0.1:80 | **Router ==========> Port Translation** | **205.0.0.2:6000** | 170.0.0.1:80 |
| **192.168.0.3:5000** | 170.0.0.1:80 | | **205.0.0.2:6001** | 170.0.0.1:80 |
| **192.168.0.5:5001** | 170.0.0.1:80 | | **205.0.0.2:6002** | 170.0.0.1:80 |

Die Quell-IP-Adressen werden durch die (einzige) öffentliche IP-Adresse ersetzt. Die internen Port-Nummern werden durch eindeutige öffentliche Port-Nummern ersetzt. Mittels einer Tabelle merkt sich der Router jeweils die interne Quell-IP-Adresse samt Port-Nummer und die öffentliche Port-Nummer des ausgehenden Pakets:

```
192.168.0.2:5000 ⇔ 6000
192.168.0.3:5000 ⇔ 6001
192.168.0.5:5001 ⇔ 6002
```

Wie im Beispiel ersichtlich, funktioniert dies auch, wenn mehrere Geräte gleichzeitig dieselbe IP mit demselben Port aufrufen. Zwar haben die Datenpakete alle die gleiche Ziel-IP und den gleichen Ziel-Port, jedoch werden die Antworten an die Quell-IP gesendet, mit jeweils unterschiedlichen Ports. Das aufrufende Gerät (Router oder ähnliches) kann nämlich eine HTTP Anfrage über den Port 80 stellen, dabei aber selbst als eigenen Port den Port 6001 angeben. Die Antwort vom HTTP-Server erfolgt dann an den Router auf dem Port 6001 und dieser übersetzt zurück auf die passende IP und den Port des aufrufenden Geräts.

### 6.1.2 Eingehende Pakete (LAN ← WAN)

lokales Netz (LAN) öffentliches Netz (WAN)

| **Quell IP:Port** | **Ziel IP:Port** | | **Quell IP:Port** | **Ziel IP:Port** |
|---|---|---|---|---|
| 170.0.0.1:80 | **192.168.0.2:5000** | **Router < ========== Port Translation** | 170.0.0.1:80 | **205.0.0.2:6000** |
| 170.0.0.1:80 | **192.168.0.3:5000** | | 170.0.0.1:80 | **205.0.0.2:6001** |
| 170.0.0.1:80 | **192.168.0.5:5001** | | 170.0.0.1:80 | **205.0.0.2:6002** |

Bei eingehenden Paketen kann anhand der Port-Nummer der Ziel-IP und des Tabelleneintrags (*connection tracking*) festgestellt werden, welcher Computer die Pakete angefordert hatte (hier: `192.168.0.2`, `192.168.0.3` und `192.168.0.5`). Der Router kann dadurch die Ziel-IP durch die ursprüngliche Quell-IP `192.168.0.2`, `192.168.0.3` bzw. `192.168.0.5` und die öffentliche Port-Nummer durch die ursprüngliche interne Port-Nummer austauschen.
Da hier jede IP-Adresse zu einer einzigen IP-Adresse übersetzt wird, spricht man von einer N:1-Übersetzung. Werden mehrere IP-Adressen zu weniger IP-Adressen abgebildet, dann handelt es sich um eine N:M-Übersetzung.