Debian Destination-NAT einstellen

Description

In diesem Artikel gehe ich darauf ein, wie wir bei einem **Debian-Server** ein **Destination-NAT** einstellen kÃ¶nnen. Damit sind wir in der Lage, interne Webdienste z.B. Ã¼ber einen VPS mit einer Ã¶ffentlichen IP-Adresse verfÃ¼gbar zu machen.

Destination-NAT ist nichts anderes, als alle Anfragen, die auf einem bestimmten Port auf dem Debian-Server ankommen, an einen anderen Server weiterzuleiten. Auf das obige Beispiel beschrieben, kÃ¶nnten wir alle Anfragen auf Port **80** und **443** automatisch an einen internen Reverseproxy Server weiterleiten, welcher dann die einzelnen Webdienste Ã¼ber eine Subdomain mit einem entsprechendem SSL-Zertifikat erreichbar macht.

DurchfÃ¼hrung

Um beim Debian-Server jetzt das Destination-NAT einzurichten, brauchen wir im ersten Schritt eine Verbindung zwischen dem Debian-Server und dem Zielserver. In meinem Fall habe ich einen kleinen 1 â?¬ VPS angemietet, welcher per Wireguard mit meiner Firewall verbunden ist. So kann der VPS meine internen Server erreichen (Nur mit entsprechender Firewall-Regel). Die Verbindung kann ich mittels *`ping`* erstmal testen. Ob der Port erreichbar ist, kÃ¶nnen wir mittels *`telnet`* testen.

```
# Host-Erreichbarkeit
ping <ip-adresse>

# Port-Erreichbarkeit
telnet <ip-adresse> <port>
```

Sobald das gewÃ¤hrleistet ist, kÃ¶nnen wir mit der Konfiguration des NATs beginnen. Dazu mÃ¼ssen wir im ersten Schritt erstmal **IP-Forwarding** aktivieren. Dazu fÃ¼hren wir den folgenden Befehl aus:

```
echo 1 > /proc/sys/net/ipv4/ip_forward
echo "net.ipv4.ip_forward = 1" >> /etc/sysctl.conf
sysctl -p
```

Im nÃ¤chsten Schritt erstellen wir die **iptables-Regeln** fÃ¼r das Destination-NAT. Dazu fÃ¼hren wir den folgenden Befehl aus. Angepasst auf unsere Situation, mit dem richtigen **Interface-Namen**, dem **Port** und dem **Zielserver**. In meinem Fall leite ich hier den Port **80** und Port **443** Verkehr an den Zielserver weiter.

```
iptables -t nat -A PREROUTING -i ens6 -p tcp --dport 80 -j DNAT --to-destination
```

```
192.168.0.80:80
iptables -t nat -A PREROUTING -i ens6 -p tcp --dport 443 -j DNAT --to-destination
192.168.0.80:443
```

Jetzt mÃ¼ssen wir die **Masquerade-Regeln** fÃ¼r die RÃ¼ckantworten erstellen. Dazu mÃ¼ssen wir wieder den nachstehenden Befehl ausfÃ¼hren:

```
iptables -t nat -A POSTROUTING -o ens6 -j MASQUERADE
```

Jetzt mÃ¼ssten alle Anfragen, die auf Port **80** und Port **443** auf dem Debian-Server ankommen, an den Zielserver umgeleitet werden. Falls nicht, bitte einmal die Firewall des Servers und ggf. des Providers Ã¼berprÃ¼fen.

Als kleinen Bonus zeige ich jetzt noch kurz, wie wir die **IPTables-Regeln** jetzt persistent speichern kÃ¶nnen. Die Regeln werden nÃ¤mlich nach einem Neustart zurÃ¼ckgesetzt.

In der Regel schreibt man diese Regeln mit in die Netzwerkkonfiguration. Da ich die Trennung zwischen Netzwerkkonfiguration und **IPTables-Regeln** etwas schÃ¶ner finde, zeige ich hier, wie wir das bewerkstelligen kÃ¶nnen. Dazu mÃ¼ssen wir das **iptables-persistent** Paket installieren.

```
apt update
apt upgrade -y
apt install iptables-persistent
```

Um jetzt die Ã?nderungen zu speichern, fÃ¼hren wir den folgenden Befehl aus:

```
iptables-save > /etc/iptables/rules.v4
ip6tables-save > /etc/iptables/rules.v6
```

Nach einem Neustart sollten die Regeln gespeichert sein. Zum Ã?berprÃ¼fen kÃ¶nnen wir den folgenden Befehl verwenden:

```
iptables -t nat -L -n -v
```

Category

1. Linux

Date Created
10.04.2025
Author
administrator