

Debian Destination-NAT einstellen

Description

In diesem Artikel gehe ich darauf ein, wie wir bei einem **Debian-Server** ein **Destination-NAT** einstellen können. Damit sind wir in der Lage, interne Webdienste z.B. über einen VPS mit einer öffentlichen IP-Adresse verfügbar 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, könnten wir alle Anfragen auf Port **80** und **443** automatisch an einen internen Reverseproxy Server weiterleiten, welcher dann die einzelnen Webdienste über eine Subdomain mit einem entsprechendem SSL-Zertifikat erreichbar macht.

Durchführung

Um beim Debian-Server jetzt das Destination-NAT einzurichten, brauchen wir im ersten Schritt eine Verbindung zwischen dem Debian-Server und dem Zielservers. In meinem Fall habe ich einen kleinen 1-GB 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, können wir mittels *telnet* testen.

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

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

Sobald das gewährleistet ist, können wir mit der Konfiguration des NATs beginnen. Dazu müssen wir im ersten Schritt erstmal **IP-Forwarding** aktivieren. Dazu führen 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 nächsten Schritt erstellen wir die **iptables-Regeln** für das Destination-NAT. Dazu führen wir den folgenden Befehl aus. Angepasst auf unsere Situation, mit dem richtigen **Interface-Namen**, dem **Port** und dem **Zielservers**. In meinem Fall leite ich hier den Port **80** und Port **443** Verkehr an den Zielservers 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 müssen wir die **Masquerade-Regeln** für die Rückantworten erstellen. Dazu müssen wir wieder den nachstehenden Befehl ausführen:

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

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

Als kleinen Bonus zeige ich jetzt noch kurz, wie wir die **IPTables-Regeln** jetzt persistent speichern können. Die Regeln werden nämlich nach einem Neustart zurückgesetzt.

In der Regel schreibt man diese Regeln mit in die Netzwerkkonfiguration. Da ich die Trennung zwischen Netzwerkkonfiguration und **IPTables-Regeln** etwas schöner finde, zeige ich hier, wie wir das bewerkstelligen können. Dazu müssen wir das **iptables-persistent** Paket installieren.

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

Um jetzt die Änderungen zu speichern, führen 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 Überprüfen können wir den folgenden Befehl verwenden:

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

Category

1. Linux

Date Created

10.04.2025

Author

administrator