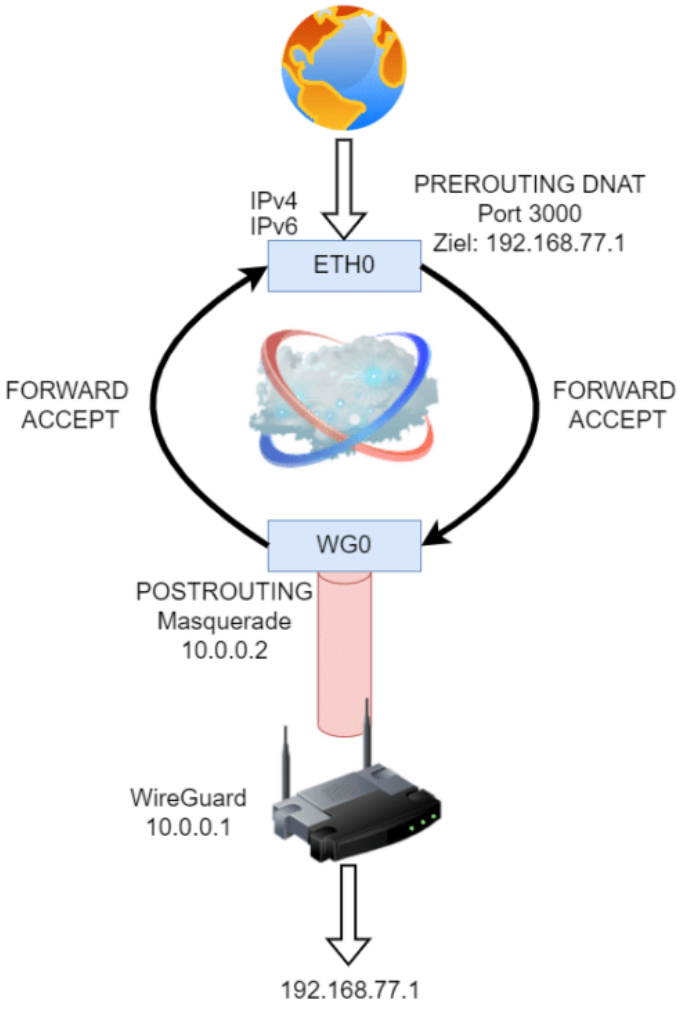
DS-Lite IPv6 Tunnel – Port Forwarding – NAT – WireGuard VPN

NAT IPv6 Port Forward Cloud Server

Viele Internetnutzer haben eine **Dual Stack** Internetverbindung mit einer nicht eigenen **IPv4 und/oder IPv6** Adresse. Dabei hat man schnell das Problem wenn man auf seine eigenen Dienst zugreifen möchte, keine Verbindung zu Stande kommt. Die IPv4 und die IPv6 Verbindung wechselt

eventuell oder die IPv4 ist eine NAT Adresse usw. Es gibt also viele Hürden wieso man nicht an seine Dienst immer dran kommt.

Im besten Fall sucht man sich also einen Punkt im Internet der gut erreichbar ist und der die Anfragen an deine Dienste weiterleitet. Hier in diesem Beispiel mieten wir uns einen Cloud Server mit einer eigenen IPv4 & IPv6 Adresse. Somit sind die Dienste immer über beide Internet Protokolle erreichbar.



Lösungsbeschreibung

Du brauchst folgendes

- **Cloud Server** -> z.B. Hetzner Cloud (kleinster Server) HIER 20€ STARTGUTHABEN
- **VPN Gateway** -> z.B. pfSense // Hardware Appliance

Es wird zwischen dem Cloud Server und deinem VPN Gateway ein Wireguard VPN Tunnel aufgebaut. Diese Verbindung kann über IPv4 oder IPv6 aufgebaut werden. Da diese Verbindung sowieso durch deine pfSense initiiert wird, ist es egal ob v4 oder v6.

Auf dem Cloud Server wird die unten stehen WireGuard Konfiguration genommen und somit auch die 4 Wunderregeln für das DNAT (Destination NAT).

```
[Interface]
Address = 10.0.0.2/24
ListenPort = 51820
PrivateKey = <YOUR-PRIVATE-KEY>
PostUp = iptables -A FORWARD -i eth0 -o wg0 -j ACCEPT
PostUp = iptables -A FORWARD -i wg0 -o eth0 -j ACCEPT
PostUp = iptables -t nat -A PREROUTING -i eth0 -p tcp -m multiport --dport 3000 -j DNAT --to 192
PostUp = iptables -t nat -A POSTROUTING -o wg0 -j MASQUERADE

PostDown = iptables -D FORWARD -i eth0 -o wg0 -j ACCEPT
PostDown = iptables -D FORWARD -i wg0 -o eth0 -j ACCEPT
PostDown = iptables -t nat -D PREROUTING -i eth0 -p tcp -m multiport --dport 3000 -j DNAT --to 1
PostDown = iptables -t nat -D POSTROUTING -o wg0 -j MASQUERADE

[Peer]
PublicKey = <YOUR-PUBLIC-KEY>
AllowedIPs = 192.168.77.0/24, 10.0.0.0/24
```

Mit dieser Konfiguration wird der Port 3000 eingehend auf dem Server mittels DNAT auf die Zieladresse 192.168.77.1 weitergeleitet. (**PREROUTING**)
Mit dem **PORTROUTING** wird dem Daten-Paket die IP-Adresse des Wireguard Tunnel aufgezwungen.
Die beiden **FORWARD** Regeln geben dem System die Freigabe Pakete zwischen beiden Interfaces zu verschieben.

Natürlich kann die besonders wichtige Regel „PREROUTING“ so angepasst werden das diese für euch passt. Man kann auch UDP Freigaben oder mehrere Ports gleichzeitig freigeben.

mit

```
iptables -I DOCKER-USER -i eth0 ! -s 127.0.0.1 -p tcp --dport 81 -j DROP
```

Wird die Managementseite des Proxys von außen gesperrt.

Alle weitere Informationen natürlich wie immer im Video.

Video
Ansichten: 13.909

Revision #4
Created 2024-11-02 20:47:55 UTC by willi
Updated 2025-05-03 15:48:19 UTC by willi