WireGuard

WireGuard® ist ein extrem einfaches, aber dennoch schnelles und modernes VPN, das modernste Kryptographie nutzt. Es zielt darauf ab, schneller, einfacher, schlanker und nützlicher als IPsec zu sein, während es die massiven Kopfschmerzen vermeidet. Es soll wesentlich leistungsfähiger sein als OpenVPN. WireGuard ist als Allzweck-VPN konzipiert, das sowohl auf eingebetteten Schnittstellen als auch auf Supercomputern läuft und für viele verschiedene Umstände geeignet ist. Ursprünglich für den Linux-Kernel veröffentlicht, ist es jetzt plattformübergreifend (Windows, macOS, BSD, iOS, Android) und weit verbreitet. Es wird derzeit intensiv weiterentwickelt, kann aber schon jetzt als die sicherste, benutzerfreundlichste und einfachste VPN-Lösung in der Branche angesehen werden.

Voraussetzungen

Wenn du deine Services zu Hause nutzen möchtest, egal wo du bist, sind folgende Schritte erforderlich.

Dynamic DNS

Wenn du keine statische IP von deinem Internet Service Provider (ISP) hast, ist ein dynamisches DNS (DDNS) erforderlich.
Du musst also ein Konto bei einem der unten aufgeführten Anbieter einrichten:

- https://freedns.afraid.org/
- https://www.duckdns.org/
- https://www.noip.com/

Überprüfe auch deinen Router auf diese Anbieter. Manchmal kannst du dort deine Anmeldedaten eingeben.

DDClient

Installiere `ddclient` und suche nach dem von dir gewählten Anbieter und gib dort deine Anmeldedaten ein.

```
pacman -S ddclient
nano /etc/ddclient/ddclient.conf
```

```
systemctl enable --now ddclient.service
```

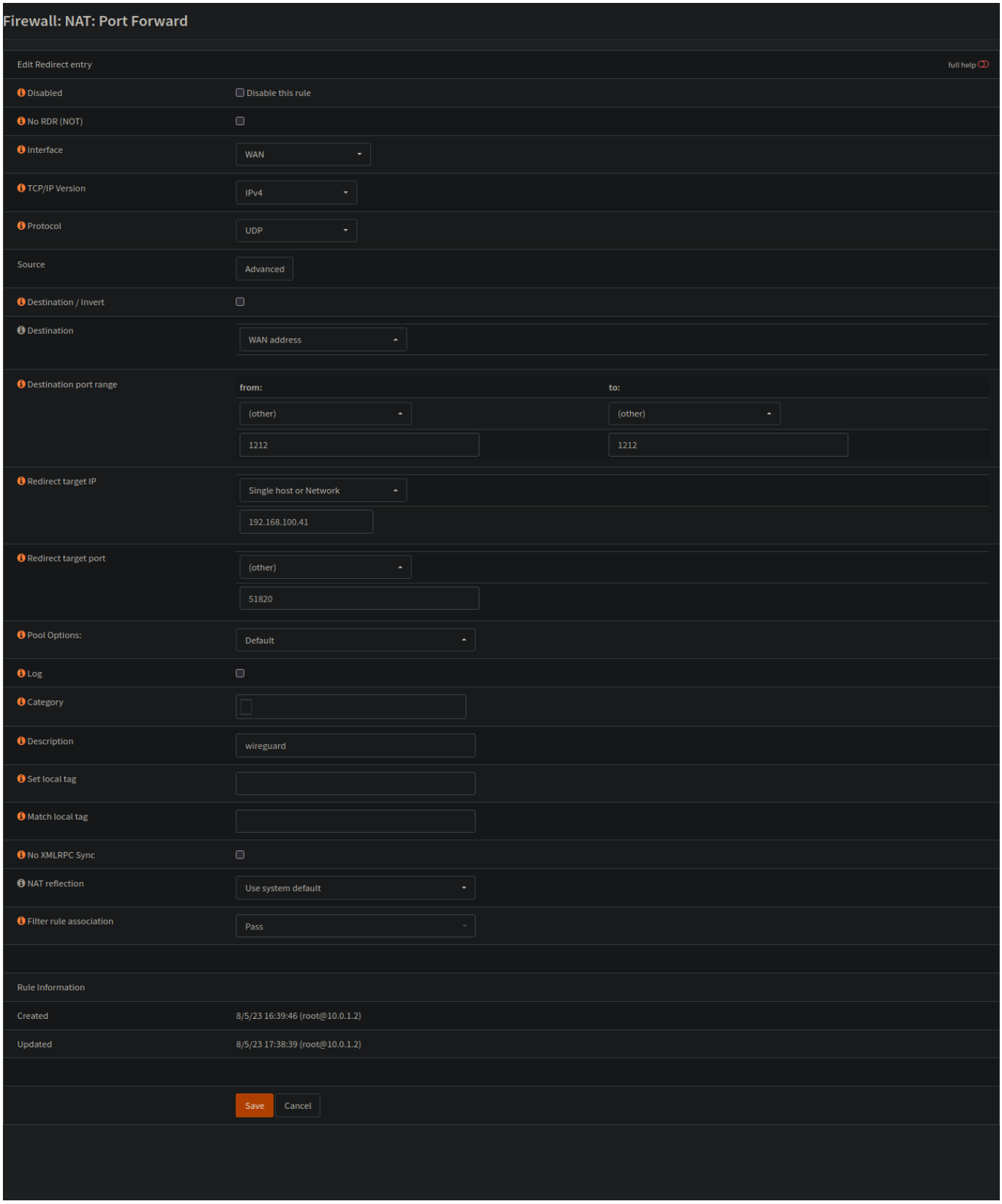
Siehe auch https://wiki.archlinux.org/title/Dynamic_DNS#ddclient. Einige Beispiele sind in der Tabelle zu finden.

Portweiterleitung

Was ist das?

Wir werden Wireguard verwenden, um über das Internet auf deinen Server zuzugreifen. Dazu musst du einen Port in deinem Router öffnen und ihn an deinen Server weiterleiten.
Der Wireguard-Port wird standardmäßig auf `51820` verwaltet. Wenn du dies ändern möchtest, musst du den Port auf die von dir gewählte Nummer umleiten und das Tutorial entsprechend anpassen.

Das folgende Beispiel basiert auf OPNsense, ist aber im Grunde auch für andere Geräte geeignet.
Das Beispiel unten hat auch einen anderen Zielport (1212). Wenn du diesen ebenfalls ändern möchtest, musst du `Endpoint = <server public IP or domain>:1212` unter clients ebenfalls ändern:



Server

Mach alles mit root.

```
su
```

Packet

```
pacman -S wireguard-tools
```

Keys

```
cd /etc/wireguard/
umask 077; wg genkey | tee privatekey | wg pubkey > publickey
```

wg0.conf

Interface

Kopiere den privaten Schlüssel und füge ihn unter `PrivateKey =` ein.

```
cat privatekey
```

```
nano wg0.conf
```

```
[Interface]
PrivateKey = <Private Key>
Address = 10.0.0.1/24
ListenPort = 51820
```

Peer

1. Gehe zuerst zu clients und befolge die Anweisungen.
2. Kopiere den **publickey** und den **presharedkey** von deinem client.

```
cat /etc/wireguard/clients/phones/pinephone/publickey
cat /etc/wireguard/clients/phones/pinephone/presharedkey
```

1. Füge den peer hinzu

```
nano /etc/wireguard/wg0.conf
```

```
[Peer]
# pinephone
PublicKey = <client public key>
PresharedKey = <preshared key>
AllowedIPs = 10.0.0.2/32
```

Clients

Erstelle Clients für *laptop*, *desktop*, *phone* und so weiter. Wofür auch immer du es brauchst.

```
mkdir -p /etc/wireguard/clients/phones/pinephone/
```

Es ist besser, sie woanders zu speichern. Auf einem USB-Stick oder so. Oder lösche sie einfach nach der Konfiguration.

Keys

```
cd /etc/wireguard/clients/phones/pinephone/
umask 077; wg genkey | tee privatekey | wg pubkey > publickey | wg genpsk > presharedkey
```

```
cat privatekey && cat /etc/wireguard/publickey && cat presharedkey
```

```
nano pinephone.conf
```

```
[Interface]
PrivateKey = <pinephones-privatekey>
Address = 10.0.0.2/24

[Peer]
PublicKey = <server public key>
PresharedKey = <preshared key>
Endpoint = <server public IP or domain>:51820
AllowedIPs = 0.0.0.0/0
```

Optional:
Füge in der Konfiguration deines Clients unter `[Interface]` einen weiteren DNS-Server hinzu, z.B. wenn du nicht den DNS-Server deines Providers verwenden willst.
`DNS = `dns server``

Berechtigungen

Setze die richtigen Berechtigungen.

```
chmod -R 600 /etc/wireguard/clients/
```

Kopiere die Datei

Kopiere deine Datei `.conf` auf dein Gerät.

```
scp pinephone.conf USER@IP:~/
```

Generiere einen QR Code

Du kannst auch einen QR-Code erstellen.

```
pacman -S qrencode
```

```
qrencode -t ansiutf8 < pinephone.conf
```

Zurück zu peer

Click

Mehr clients

Wenn du mehr Clients brauchst, folge einfach wieder dem clients-Prozess und füge den peer zu deinem Server zwischen deinen anderen Clients hinzu.

Stoppe Wireguard für das Hinzufügen neuer Clients/Peers.
`systemctl stop wg-quick@wg0.service`

Start

```
systemctl enable --now wg-quick@wg0.service
```

Firewall

Basierend auf firewalld.

1. Erstelle eine neue zone (nenne es: `wireguard`)
2. füge “`wg0` interface” zu deiner neuen ***wireguard zone*** hinzu
3. füge/öffne wireguards service (port 51820) zu deiner ***home zone***
4. füge/öffne https service (port 443) zu deiner ***wireguard zone*** (um deine Services zu erreichen, die auf ssl basieren)
5. füge masquerade zu deiner ***home zone*** hinzu
6. und erstelle eine neue policy für den Zugang zum Internet und zu deinen Services

Überprüfe

Du kannst die Verbindungen deiner Clients mit dem Befehl `wg` auf deinem Wireguard-Server überprüfen. Es wird Folgendes angezeigt:

```
  latest handshake: 1 minute, 52 seconds ago
  transfer: 1.22 MiB received, 3.80 MiB sent
```

Überprüfe auch die IP-Adresse deiner Clients, zum Beispiel mit https://dnsleaktest.com, die die IP-Adresse deines Zuhauses sein sollte, und klicke auf die Schaltfläche ***Extended test*** für den DNS-Server, den du verwendest, der auf deinem Android-Gerät anders sein kann, wenn DNS nicht auf der Clients-Seite eingestellt ist.