

# IP Forwarding

[sagou.in](https://sagou.in) is self hosted behind an internet provider router, meaning that it does not have a public IPv4. To remedy this, [Rhizome](#), a Compiègne association that provides internet services, is providing us a public IPv4 and a VPN connection to their servers to act as a storefront that forwards every request to the self hosted server via a VPN. Associated configurations and scripts are versioned on [gitea](#).

## Overview

A wireguard VPN is setup between the home server and VPS. Requests on specific ports of the VPS are routed to the home server through the VPN and back. Request originating from the home server also pass through the VPS to avoid leaking its real IP. A keepalive parameter is used to make sure that the home server initiates the VPN because the VPS cannot.



## Configuration

To route all traffic in the VPN in the home server side, the default route is simply replaced from the actual network interface to the wireguard interface. The wireguard configuration allows this with the `AllowedIPs` field.

```
[Interface]
```

```
Address = 80.67.182.35/27
```

```
PrivateKey = ...
```

```
DNS = 80.67.169.12,80.67.169.40 # FDN DNS
```

```
PostUp = ip route add default via 80.67.182.33 metric 50
```

```
PostUp = ip route add 80.67.182.71 via 192.168.1.1 dev eth0
```

```
PreDown = ip route delete default via 80.67.182.33 metric 50
```

```
PreDown = ip route delete 80.67.182.71 via 192.168.1.1 dev eth0
```

```
[Peer]
PublicKey = ...
AllowedIPs = 0.0.0.0/0
EndPoint = 80.67.182.71:1194 # vpn.rhizome-fai.net
PersistentKeepAlive = 25
```

These configurations are started with wg-tools upon start with a dedicated service

```
systemctl enable wgvps.service
```

```
[Unit]
Description=WireGuard tunnel to Rhizome VPS
After=network-online.target nss-lookup.target
Wants=network-online.target nss-lookup.target
PartOf=wg-quick.target

[Service]
Type=oneshot
Restart=on-failure
RemainAfterExit=yes
ExecStart=/usr/bin/wg-quick up wgvps
ExecStop=/usr/bin/wg-quick down wgvps
ExecReload=/bin/bash -c 'exec /usr/bin/wg synccnf wgvps <(exec /usr/bin/wg-quick strip wgvps)'
Environment=WG_ENDPOINT_RESOLUTION_RETRIES=infinity

[Install]
WantedBy=multi-user.target
```

---

Révision #3

Créé 27 décembre 2022 18:36:59 par ynhadmin

Mis à jour 27 décembre 2022 19:53:45 par ynhadmin