WireGuard Site-To-Site VPN

Inhaltsverzeichnis

Short guide on how to efficiently setup a site-to-site VPN based on the proven solution WireGuard.

1 General

For secure communication between servers, a WireGuard site-to-site VPN can be setup to serve this purpose.
This guide provide the baseline for getting the setup right. It ensures security and efficiency.

It covers both the monolithic approach and a dockerized approach.

2 Installation

Simple, but just in case:

Code

```
sudo apt-get install wireguard
```

Nothing else is needed.

2.1 Server Configuration & Setup

Create Public and Private Key for the Server:

Code

```
umask 077
wg genkey | tee privatekey | wg pubkey > publickey
```

Create a config file at `/etc/wireguard/wg0.conf`:

Code

```
[Interface]
Address                                =                                10.170.10.1/32
ListenPort                                    =                                44660
PrivateKey                             =                             SERVER_PRIVATE_KEY

[Peer]
PublicKey                              =                              CLIENT_PUBLIC_KEY
AllowedIPs = 10.170.10.2/32
```

Make sure the IP address range is not in use both on the server and the client. Replace the Private Key with the one created earlier.
Create the service which allows for automatic startup:

Code

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

2.2 Client Configuration & Setup

Create Public and Private Key for the Client:

Code

```
umask                                                                          077
wg genkey | tee privatekey | wg pubkey > publickey
```

Create a config file at `/etc/wireguard/wg0.conf`:

Code

```
[Interface]
Address                                =                                10.170.10.2/32
PrivateKey                             =                             CLIENT_PRIVATE_KEY

[Peer]
PublicKey                              =                              SERVER_PUBLIC_KEY
AllowedIPs                               =                                10.170.10.1/32
Endpoint = PUBLIC_SERVER_IP:44660
```

Make sure the IP address range is not in use both on the server and the client. Replace the Private Key with the one created earlier.

Create the service which allows for automatic startup:

Code

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

2.3 Final Configuration & Start

On both the server and the client make sure that the respective public keys are entered correctly.
Then start the server VPN and after that the client VPN with:

Code

```
sudo systemctl start wg-quick@wg0.service
```

For checking the connection statistics the following command can be used:

Code

```
sudo wg show
```

3 Installation (containerised approach, based on Docker in this chapter)

3.1 General

A good alternative for the monolithic architecture is the use of docker. Some benefits are easier updates and instant swap of the root-system underneath (where docker runs on).

3.2 Installation & Configuration

Code

```
services:
                                                    vpn_example_com:

   cap_add:


   environment:




                          -     PEERS=2     #     how     many     clients     should     be
      - PEERDNS=10.122.20.3 # Alternative DNS sinstead of the comntainer DNS, optional.
                          -    INTERNAL_SUBNET=10.150.0.0    #    Internal    subnet    of    the    V
ALLOWEDIPS=0.0.0.0/0 #optionalrestrictionsofconnectionsubnetsOtherwiseleavedefaultroute.

   volumes:
                                                          -          /data/docker/persistent/sta

   dns:

   ports:

   sysctls:


   networks:
     nhcloudnet-nhsites-sec-prod:
         ipv4_address: 10.122.24.20
```

Alles anzeigen

Above is a sample docker-compose that must be adjusted before use. The example above exposes port 2362 which can however be changed to the default. Note: If the default port doesn't work, check for any firwall blocks.

The private keys and additional infos like e.g. the QR code for the setup you will find after the container has started via `/data/docker/persistent/stackname/vpn.example.com/config/` in the peer folders.

Image not found or type unknown