WireGuard Site-To-Site VPN

Inhaltsverzeichnis

Kurzer Eintrag um die Einrichtung eines Site-To-Site VPNs mit Wireguard zu zeigen.

1 General

Fuer sichere Kumminikation zwischen Servern kann es ratsam sein, einen VPN tunnel auf zu bauen.
Dies erlaubt eine verschluesselte Verbindung zwischen zwei Endpunkten. In diesem Guide beschreibe ich zwei Wege dies zu tun.

Endpunkt 1 wird im Guide als "Server" bezeichnet. Endpunkt 2 als "Client".

2 Installation (monolithic architecture, based on Debian in this chapter)

Simple, but just in case:

Code

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

Das wars.

2.1 Server Configuration & Setup

Erstellen eines Public and Private Key fuer den Server:

Code

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

Erstelle eine config Datei unter `/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
```

Stelle sicher, dass die IP address range nicht in Benutzung am Server Client ist. Ersetze den Private Key mit dem vorher Erzeugten.
Aktiviere den Service um die Verwaltung zu vereinfachen und ein automatisches Starten zu erwirken:

Code

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

2.2 Client Configuration & Setup

Erstellen eines Public and Private Key fuer den Client:

Code

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

Erstelle eine config Datei unter `/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
```

Stelle sicher, dass die IP address range nicht in Benutzung am Server Client ist. Ersetze den Private Key mit dem vorher Erzeugten.
Aktiviere den Service um die Verwaltung zu vereinfachen und ein automatisches Starten zu erwirken:

Code

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

2.3 Final Configuration & Start

Auf sowohl Server als auch auf dem Client muss sichergestellt werden, dass die entsprechenden Public Keys korrekt eingetragen sind.
Starten des Server Endpunkt und anschliessend des Client Endpunkt mit:

Code

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

Fuer Statistics im Bezug auf Verbindungen kann der folgende Command genutzt werden:

Code

```
sudo wg show
```

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

3.1 General

Eine Alternative zu der monolithic architecture ist die Verwendung von Docker. Vorteile sind einfache Wartbarkeit und der Austausch des Root-Systems bei z.B. Updates.

3.2 Installation & Configuration

Code

```
services:
                                                    vpn_example_com:

   cap_add:


   environment:




                  -    PEERS=2    #    wie    viele    clients    sollen    erstellt    we
     - PEERDNS=10.122.20.3 # Alternativer DNS statt der vom Container, optional.
                      -    INTERNAL_SUBNET=10.150.0.0    #    Internes    Subnet    vom
         -  ALLOWEDIPS=0.0.0.0/0  #  falls  man  auf  IP  Netze  einschraenken  will.

   volumes:
                                                          -          /data/docker/persistent/sta

   dns:

   ports:

   sysctls:


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

Alles anzeigen

Das oben ist eine Example docker-compose welche natuerlich angepasst werden muss. Der Published Port ist 2362, kann aber auch auf den default belassen werden.

Die Private Keys und weiteren Infos wie z.B. den Code mit der Einrichtung findet ihr dann nach dem starten des Containers unter `/data/docker/persistent/stackname/vpn.example.com/config/` dort dann jeweils pro Peer einen Ordner:

Image not found or type unknown