



KW-23

# VPN- Dokumentation



Naemi Ross

# 1 Inhaltsverzeichnis

2	Tabellenverzeichnis.....	1
3	Abbildungsverzeichnis.....	1
4	Einleitung.....	2
5	Namensschema.....	2
6	Netzwerkplan.....	2
7	IP-Konzept .....	2
8	Gerätebeschreibung.....	2
9	Installation / Konfiguration.....	3
10	Testen .....	8
10.1	Testkonzept .....	8
10.2	Testprotokoll .....	8

## 2 Tabellenverzeichnis

Tabelle 1 Namensschema.....	2
Tabelle 2 IP-Konzept .....	2
Tabelle 3 Gerätebeschreibung.....	2
Tabelle 4 Testkonzept T01 .....	8
Tabelle 5 TestKonzept T02 .....	8
Tabelle 6 Testprotokoll .....	8

## 3 Abbildungsverzeichnis

Abbildung 1 Netzwerkplan .....	2
Abbildung 2 Anmeldung Proxmox .....	3
Abbildung 3 Anmeldung vom Server .....	3
Abbildung 4 SSH Verbindung für Server .....	4
Abbildung 5 Erstellen von Client.....	4
Abbildung 6 Server Updaten/-graden.....	5
Abbildung 7 Privet und Publik Schlüssel erstellen .....	5
Abbildung 8 wg0 aktivieren Server .....	5
Abbildung 9 konfiguration von Server.....	5
Abbildung 10 Schlüssel nachschauen .....	6
Abbildung 11 konfiguration von Client .....	6
Abbildung 12 wg0 starten Client.....	6
Abbildung 13 ping von Client zu Server .....	7
Abbildung 14 erweiterte konfiguration von Cleint .....	7

## 4 Einleitung

In dieser Dokumentation wird die Einrichtung einer VPN-Verbindung beschrieben, die zwischen einem Linux-Client und einem Linux-Server hergestellt wird. Der Server ist über Proxmox zugänglich, während sich der Linux-Client lokal auf meinem Gerät befindet. Beide Systeme laufen in virtuellen Maschinen. Ziel ist es, vom Client aus eine VPN-Verbindung zum Server herzustellen.

## 5 Namensschema

Tabelle 1 Namensschema

Gerät	Name	Namens Erläuterung
Linux Client	linux-client-XX	XX = zufällige Zahl
Linux Server	wghost16	

## 6 Netzwerkplan

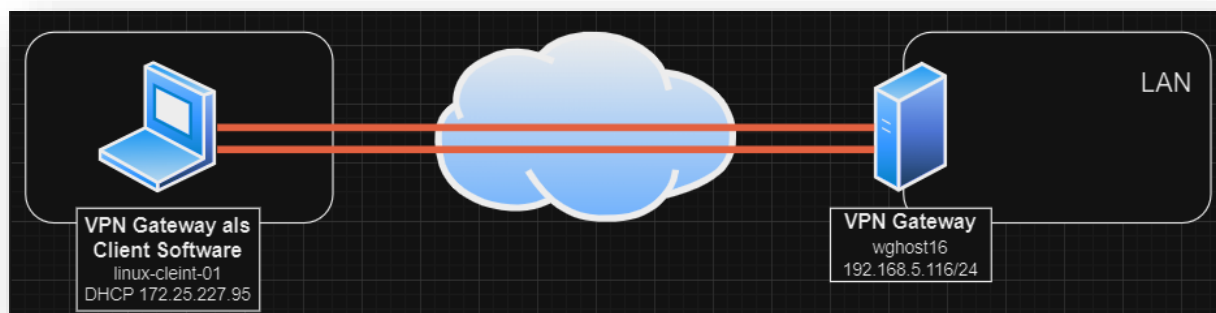


Abbildung 1 Netzwerkplan

## 7 IP-Konzept

Tabelle 2 IP-Konzept

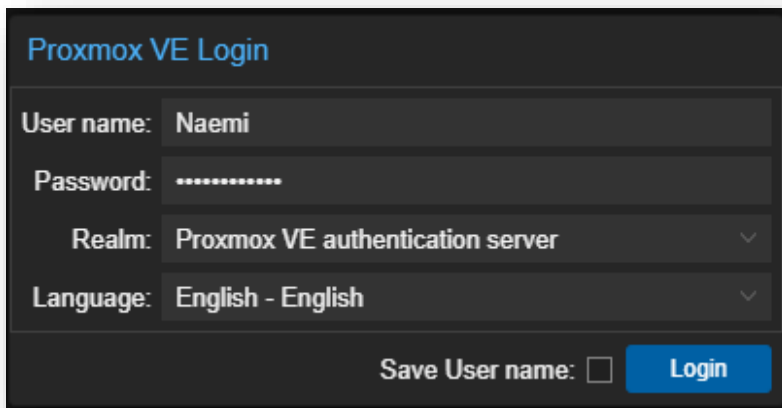
Gerätetyp	Art	IP-Adressen
Server	Statisch	192.168.5.116/24
Client	Dynamisch	172.25.227.95/24

## 8 Gerätebeschreibung

Tabelle 3 Gerätebeschreibung

Gerätetyp	Service
Server	Linux, Wireguard
Client	Linux

## 9 Installation / Konfiguration



Proxmox VE Login

User name: Naemi

Password: .....

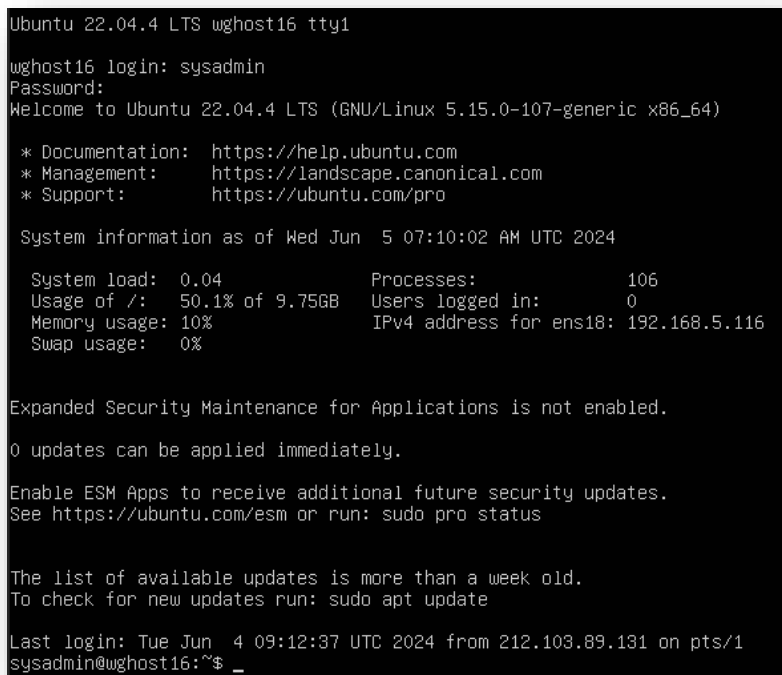
Realm: Proxmox VE authentication server

Language: English - English

Save User name: ☐ Login

Abbildung 2 Anmeldung Proxmox

Username, Passwort und “Proxmox VE authentication server” eintragen.



```
Ubuntu 22.04.4 LTS wghost16 tty1
wghost16 login: sysadmin
Password:
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 5.15.0-107-generic x86_64)

* Documentation:  https://help.ubuntu.com
* Management:    https://landscape.canonical.com
* Support:       https://ubuntu.com/pro

System information as of Wed Jun  5 07:10:02 AM UTC 2024

System load:  0.04               Processes:            106
Usage of /:   50.1% of 9.75GB    Users logged in:     0
Memory usage: 10%               IPv4 address for ens18: 192.168.5.116
Swap usage:   0%

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Tue Jun  4 09:12:37 UTC 2024 from 212.103.89.131 on pts/1
sysadmin@wghost16:~$
```

Abbildung 3 Anmeldung vom Server

In der VM anmelden.

```
C:\Users\naemi>ssh -p 828 sysadmin@vivaldi.daffre.com
sysadmin@vivaldi.daffre.com's password:
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 5.15.0-107-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

System information as of Wed Jun  5 07:12:48 AM UTC 2024

System load:  0.0           Processes:            110
Usage of /:   50.1% of 9.75GB Users logged in:          1
Memory usage: 10%          IPv4 address for ens18: 192.168.5.116
Swap usage:   0%

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

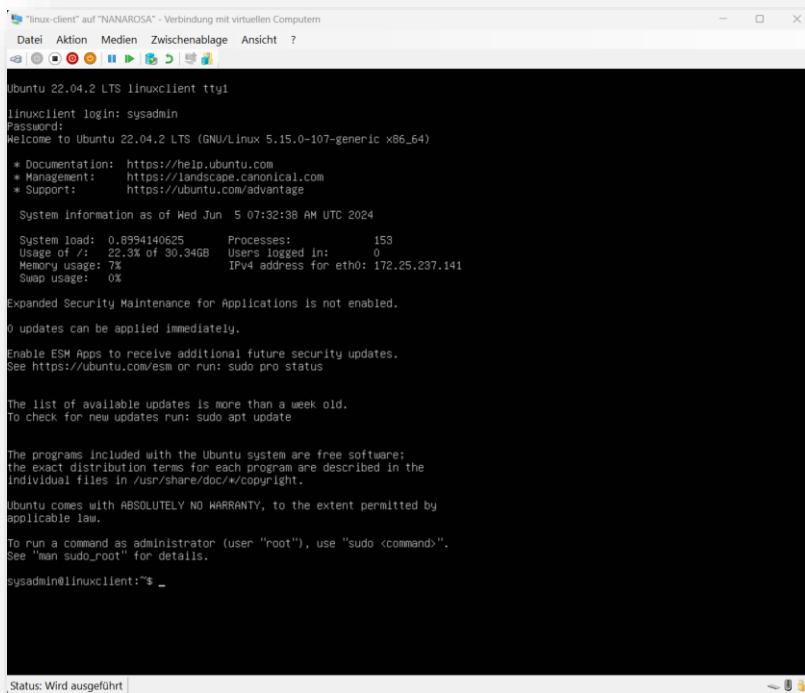
Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Wed Jun  5 07:10:03 2024
sysadmin@wghost16:~$
```

Mit SSH verbinden.

Abbildung 4 SSH Verbindung für Server



```
linux-client auf "NANAROSA" - Verbindung mit virtuellen Computern
Datei  Aktion  Medien  Zwischenablage  Ansicht  ?

Ubuntu 22.04.2 LTS linuxclient tty1
linuxclient login: sysadmin
Password:
Welcome to Ubuntu 22.04.2 LTS (GNU/Linux 5.15.0-107-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Wed Jun  5 07:32:38 AM UTC 2024

System load:  0.8994140625   Processes:            153
Usage of /:   22.3% of 30.94GB Users logged in:          0
Memory usage: 7%           IPv4 address for eth0: 172.25.237.141
Swap usage:   0%

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

sysadmIn@linuxclient:~$
```

Erstelle lokal einen  
Linux Client.

Abbildung 5 Erstellen von Client

```

sysadmin@wghost16:~$ sudo apt install wireguard
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  wireguard-tools
Suggested packages:
  openresolv | resolvconf
The following NEW packages will be installed:
  wireguard wireguard-tools
0 upgraded, 2 newly installed, 0 to remove and 2 not upgraded.
Need to get 90.0 kB of archives.
After this operation, 345 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://ch.archive.ubuntu.com/ubuntu jammy/main amd64 wireguard-tools amd64 1.0.20210914-lubuntu2 [86.9 kB]
Get:2 http://ch.archive.ubuntu.com/ubuntu jammy/universe amd64 wireguard all 1.0.20210914-lubuntu2 [3,114 B]
Fetched 90.0 kB in 0s (472 kB/s)
Selecting previously unselected package wireguard-tools.
(Reading database ... 74590 files and directories currently installed.)
Preparing to unpack .../wireguard-tools_1.0.20210914-lubuntu2_amd64.deb ...
Unpacking wireguard-tools (1.0.20210914-lubuntu2) ...
Selecting previously unselected package wireguard.
Preparing to unpack .../wireguard_1.0.20210914-lubuntu2_all.deb ...
Unpacking wireguard (1.0.20210914-lubuntu2) ...
Setting up wireguard-tools (1.0.20210914-lubuntu2) ...
wg-quick.target is a disabled or a static unit not running, not starting it.
Setting up wireguard (1.0.20210914-lubuntu2) ...
Processing triggers for man-db (2.10.2-1) ...
Scanning processes...
Scanning linux images...

Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
sysadmin@wghost16:~$

```

Mache ein Update und ein Upgrade. Danach kannst du Wireguard installieren.

Abbildung 6 Server Updaten/-graden

```
sysadmin@wghost16:~$ wg genkey | tee privatekey | wg pubkey > publickey
```

Abbildung 7 Privaten und Public Schlüssel erstellen

Jetzt kann man mit diesem Befehl im Server einen Privat und Public key machen

```

GNU nano 6.2 /etc/wireguard/wg0.conf
[Interface]
PrivateKey=AKs9j5M6OD1lWJx8iG0TvG1r2QLA7xVDXyxr8zfzm8=
Address=10.0.0.1/8
SaveConfig=true
PostUp=iptables -A FORWARD -i wg0 -j ACCEPT; iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE;
PostDown=iptables -D FORWARD -i wg0 -j ACCEPT; iptables -t nat -D POSTROUTING -o eth0 -j MASQUERADE;
ListenPort=51826

```

Abbildung 8 Konfiguration von Server

Jetzt kannst du eine Konfigurationsdatei erstellen. Und sie konfigurieren wie auf dem Bild zu sehen.

```

sysadmin@wghost16:~$ wg-quick up wg0
[#] ip link add wg0 type wireguard
[#] wg setconf wg0 /dev/fd/63
[#] ip -4 address add 10.0.0.1/8 dev wg0
[#] ip link set mtu 1420 up dev wg0
[#] iptables -A FORWARD -i wg0 -j ACCEPT; iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE;

```

Abbildung 9 wg0 aktivieren Server

Jetzt kann man mit dem Befehl «wg-quit up wg0» wg0 aktivieren.

```
sysadmin@linuxclient:~$ wg genkey | tee privatekey | wg pubkey > publickey
sysadmin@linuxclient:~$ ls
privatekey  publickey
sysadmin@linuxclient:~$ cat privatekey
ILywiu2UMCqIH8Tj9WBpCgAcWweLdUJPjEtm5qsj8nM=
```

Abbildung 8 Schlüssel nachschauen

Jetzt kannst du in den Client wechseln und auch hier Privat und Public keys erstellen.

```
GNU nano 6.2 /etc/wireguard/wg0.conf
[Interface]
Address = 10.0.0.2/8
SaveConfig = true
ListenPort = 48846
FwMark = 0xca6c
PrivateKey = ILywiu2UMCqIH8Tj9WBpCgAcWweLdUJPjEtm5qsj8nM=

[Peer]
PublicKey = eqoIHH0r2PXtjpGtEAqt+05w/DbuhrtGrzAGZYgrUX8=
AllowedIPs = 0.0.0.0/0
Endpoint = 77.56.3.149:51826
PersistentKeepalive = 30
```

Abbildung 9 Konfiguration von Client

Jetzt eine Konfigurationsdatei erstellen. Und konfigurieren wie auf dem Bild. 77.56.3.149 ist die öffentliche IP vom Server (mit dem Befehl «curl ifconfig.me» kannst du die öffentliche IP herausfinden)

```
sysadmin@linuxclient:~$ wg-quick up wg0
[#] ip link add wg0 type wireguard
[#] wg setconf wg0 /dev/fd/63
[#] ip -4 address add 10.0.0.2/8 dev wg0
[#] ip link set mtu 1420 up dev wg0
[#] ip -4 route add 0.0.0.0/0 dev wg0 table 51820
[#] ip -4 rule add not fwmark 51820 table 51820
[#] ip -4 rule add table main suppress_prefixlength 0
[#] sysctl -q net.ipv4.conf.all.src_valid_mark=1
[#] nft -f /dev/fd/63
```

Abbildung 10 wg0 starten Client

Jetzt noch mal wg0 aktivieren.

```
sysadmin@linuxclient:~$ ping 10.0.0.1
PING 10.0.0.1 (10.0.0.1) 56(84) bytes of data.
64 bytes from 10.0.0.1: icmp_seq=1 ttl=64 time=33.1 ms
64 bytes from 10.0.0.1: icmp_seq=2 ttl=64 time=20.4 ms
64 bytes from 10.0.0.1: icmp_seq=3 ttl=64 time=21.5 ms
64 bytes from 10.0.0.1: icmp_seq=4 ttl=64 time=22.1 ms
```

Abbildung 11 ping von Client zu Server

Um zu überprüfen, ob es funktioniert pinge den Server an.

```
GNU nano 6.2 /etc/wireguard/wg0.conf
[Interface]
Address = 10.0.0.2/8
SaveConfig = true
PostUp = ip rule add table 200 from 192.168.5.116
PostUp = ip route add table 200 default via 192.168.5.1
PreDown = ip rule delete table 200 from 192.168.5.116
PreDown = ip route delete table 200 default via 192.168.5.1
ListenPort = 51826
FwMark = 0xca6c
PrivateKey = ILYwIU2UMCqIH8Tj9WBpCgAcWweLdUJPjEtm5qsj8nM=

[Peer]
PublicKey = eqoIHH0r2PXtjpGtEAqt+05w/DbuhrtGrzAGZYgrUX8=
AllowedIPs = 0.0.0.0/0
Endpoint = 77.56.3.149:51826
PersistentKeepalive = 30
```

Abbildung 12 erweiterte Konfiguration von Client

Damit die ganze Internetverbindung über den VPN-Tunnel geht muss man einfach in der Konfigurationsdatei des Clients kleine Anpassungen durchführen. Danach kannst du wg0 wieder aktivieren und 8.8.8.8 vom Client anpingen, um zu testen ob es funktioniert hat (Die IP musst du von deinem Client angeben die findest du durch den Befehl «ip -brief address show ens18») (ens 18 kannst du ersetzen durch den Output dieses Befehls «ip route list table main default»)



# 10Testen

## 10.1 Testkonzept

Tabelle 4 Testkonzept T01

ID	T01
<b>Testfall</b>	VPN Tunnel Testung zwischen Client und Server
<b>Host</b>	wghost16 / linux-client-01
<b>Beschreibung</b>	Es wird überprüft, ob ein VPN-Tunnel zwischen Client und Server entstanden ist. Sodass sie miteinander kommunizieren können.
<b>Testmethoden/ Testschritte</b>	Für diesen Test muss von Client der Server angepingt werden muss.
<b>Erweitertes Ergebnis</b>	Das Anpingen vom Server hat funktioniert, da eine Antwort zurückgekommen ist.

Tabelle 5 Testkonzept T02

ID	T02
<b>Testfall</b>	Benutzung von VPN-Tunnel für die ganze Internetverbindung
<b>Host</b>	wghost16 / linux-client-01
<b>Beschreibung</b>	Es wird überprüft ob die ganzen Internetverbindungen durch den VPN-Tunnel zwischen Client und Server gehen kann.
<b>Testmethoden/ Testschritte</b>	Für diesen Test muss von Client z.B. Google (8.8.8.8) angepingt werden.
<b>Erweitertes Ergebnis</b>	Das Anpingen vom Client zu 8.8.8.8 hat noch nicht richtig funktioniert, weil keine Rückmeldung kommt.

## 10.2 Testprotokoll

Tabelle 6 Testprotokoll

Nr.	Datum	Testname	Ergebnis
<b>T01</b>	06.06.2024	Testung von VPN-Tunnel zwischen Client und Server	Erfolgreich
<b>T02</b>	06.06.2024	Testen von Ganze Internetverbindung über VPN-Tunnel	Nicht erfolgreich