

WireGuard

Voraussetzungen

- IONOS VPS Server mit externe IPv4
- NAS im Heimnetz

Installation WG

- Auf der NAS und dem VPS Wireguard installieren
`apt update -y && apt install wireguard -y`
- Auf dem Handy WG Tunnel

Recher	IP	Tunnel IP	User	Passwort	Notes
IONOS VPS	217.160.11.95	10.30.250.1	root	xJ#p9\$*DfT	
NAS		10.30.250.2	root	romdz6!	
Handy		10.30.250.3			
X250 Laptop		10.30.250.4			
Firma Linux		10.30.250.5			
Doro		10.30.250.6			

Pub/Priv Key erstellen

- Auf jedem Peer folgendes ausführen
`wg genkey | tee server_private.key | wg pubkey > server_public.key`

Keys

Rechner	Private	Public
IONOS VPS	YFgaDQBWzcfCE25q8bUocKRqz5LT1GS6eGrX6SldT3s=	mFFQA1Qt3yMFpG6DbCtN61XXL379epc4MoL0mGM7H30=
NAS	EGPMX6pxjh86u0M+YaNUk21suG7iFI0l2jgkvVcf1ng=	4X0nKh1ZZs6cNVjyFEjTz3njPUYTta30SPTY4bsCLCs=
Handy	mJkKiZR0oUm0PtT15kF8b3xmNVMGKUHV7dP6SxEyDEs=	0r5f7b6myu8FfYU0GG9aqCxj6L38bKlzinszbT6tHhY=
X250 Notebook	wMXaNqJ5tSzinf+XaxK95sH5RHE0ThpR/qX0kKC5/3U=	UKHXpioh9pLZpdDGwLa+8CuxZ9mLYR3LftEbnf8cUHu=
Firma Linux	mPGz8a10B5X0x2BtisIeVPGb+NBiXqhWWZax/4WTrXs=	zUTHdHlfc99dx0pfr09i5qEVKTRFkoUkg5+JPEr6uCo=
Doro	YH5eJ8H7VilrltgpIr2J9jGPXARuCWsbxggV0+2MRXQ=	HUTtUWCQ1lfZkXJxzY1iL48ZfVqTQzFagr5rhcMa8VQ=

Konfigs

IONOS VPS

[VPS.conf](#)

```
[Interface]
Address = 10.30.250.1/24
PrivateKey = YFgaDQBWzcfCE25q8bUocKRqz5LT1GS6eGrX6SldT3s=
ListenPort = 51820
MTU = 1360
Table = off

# 1. Lokales Routing auf dem VPS, damit er weiß, wo deine Heimnetze
liegen
PostUp = ip route add 10.30.1.0/24 dev wg0
PostUp = ip route add 10.30.10.0/24 dev wg0
PostUp = ip route add 10.30.20.0/24 dev wg0
PostUp = ip route add 10.30.30.0/24 dev wg0
PostUp = ip route add 10.30.40.0/24 dev wg0

# 2. Policy Routing: Zwingt den Internet-Traffic der Clients (z.B.
Handy) in den Tunnel zur UDM
PostUp = ip rule add iif wg0 lookup 200
PostUp = ip route add default dev wg0 table 200

# 3. Erlaubt Linux, die Pakete innerhalb des Tunnels (Handy -> UDM)
weiterzuleiten
PostUp = iptables -I FORWARD -i wg0 -o wg0 -j ACCEPT
PreDown = iptables -D FORWARD -i wg0 -o wg0 -j ACCEPT

# Cleanup beim Beenden des Tunnels
PreDown = ip rule del iif wg0 lookup 200
PreDown = ip route flush table 200
PreDown = ip route del 10.30.40.0/24 dev wg0
PreDown = ip route del 10.30.30.0/24 dev wg0
PreDown = ip route del 10.30.20.0/24 dev wg0
PreDown = ip route del 10.30.10.0/24 dev wg0
PreDown = ip route del 10.30.1.0/24 dev wg0

# Peer 1: UDM Max (Dein neues Gateway ins Heimnetz und ins Internet)
[Peer]
PublicKey = 4X0nKh1ZZs6cNVjyFEjTz3njPUYTta30SPTY4bsCLCs=
# Die 0.0.0.0/0 ist hier essenziell, damit der VPS Anfragen ins
Internet an die UDM abgibt
AllowedIPs = 10.30.1.0/24, 10.30.10.0/24, 10.30.20.0/24, 10.30.30.0/24,
10.30.40.0/24, 0.0.0.0/0

# Peer 2: Handy
[Peer]
PublicKey = 0r5f7b6myu8FfyU0GG9aqCxj6L38bKlzinszbT6tHhY=
AllowedIPs = 10.30.250.3/32

# Peer 3: Notebook X250
[Peer]
PublicKey = UkHXpioh9plZpdDGwLa+8CuxZ9mLYR3LftEbnf8cUhU=
AllowedIPs = 10.30.250.4/32
```

```
# Peer 4: Firma Linux
[Peer]
PublicKey = zUTHdHlfc99dx0pfr09i5qEVKTRFkoUkg5+JPEr6uCo=
AllowedIPs = 10.30.250.5/32

# Peer 5: Doro
[Peer]
PublicKey = HUTtUWCQ1lfZkXJxzY1iL48ZfVqTQzFagr5rhcMa8VQ=
AllowedIPs = 10.30.250.6/32
```

UDM

Konfig direkt auf dem UDM Max

[download](#)

```
[Interface]
# HIER FEHLT DEIN PRIVATE KEY.
# Ohne diesen Schlüssel funktioniert der Tunnel nicht.
PrivateKey = <DEIN_GEHEIMER_SCHLÜSSEL_HIER_EINTRAGEN>

# HIER FEHLT DIE IP-ADRESSE DES CLIENTS.
# (z.B. 10.0.0.2/32 - wg show zeigt diese nicht an, du findest sie mit
'ip addr show wgclt1')
Address = <DEINE_INTERNE_WIREGUARD_IP_HIER_EINTRAGEN>

# Optional, aber aus deinem Output übernommen
ListenPort = 49845

[Peer]
# Der Public Key des Servers (Peer)
PublicKey = mFFQAlQt3yMFpG6DbCtN6lXXL379epc4MoL0mGM7H30=


# Endpoint (IP und Port des Servers)
Endpoint = 217.160.11.95:51820

# Welcher Traffic soll durch den Tunnel? (0.0.0.0/0 bedeutet: Alles)
AllowedIPs = 0.0.0.0/0

# "every 1 minute" entspricht 60 Sekunden in der Config
PersistentKeepalive = 60
```

Damit das auf der UDM klappt braucht es noch 3 Extras:




local Source **• 10.30.250.0/24**

Wireguard IP Ra...  Any

Search Settings

- Overview
- WiFi
- Networks
- Internet
- VPN
- CyberSecure
- High Availability

Policy Engine

-    **New**

System


UDM Pro Max

- Control Plane
- Identity


[Submit Support Ticket](#)

Network 10.4.57

Rule Type

Type 

Name

Action 

Protocol

Source

Source Type

Address Group

Port List

MAC Address


Destination


Destination Type


Address Group

Port List

Advanced

Match State 

Match IPsec 


Logging 

Simple **Advanced**

Internet In

Wireguard

Accept | Reject | Drop

All Before Predefined 

List

Wireguard IP Range **New**

Any **New**

Enter MAC Address

List

Any **New**

Any **New**

Auto Manual

New Invalid Established Related

Do not match IPsec Non-IPsec

Search Settings

- Overview
- WiFi
- Networks
- Internet
- VPN
- CyberSecure
- High Availability
- Policy Engine
 - New
- System
- UDM Pro Max
 - Control Plane
 - Identity
- [Submit Support Ticket](#)
- Network 10.4.57

Rule Type

Type ⓘ

Name

Action ⓘ

Protocol

Source

Source Type

Address Group

Port List

MAC Address

Destination

Destination Type

Address Group

Port List

Advanced

Match State ⓘ

Match IPsec ⓘ

Logging ⓘ

Simple **Advanced**

Internet Local

Wireguard-Local

Accept
 | Reject
 | Drop

All

Before Predefined ⓘ

List

Wireguard IP Range **New**

Any **New**

Enter MAC Address

List

Any **New**

Any **New**

Auto **Manual**

New
 Invalid
 Established
 Related

Do not match
 IPsec
 Non-IPsec

Name	Policy Type	Action	Protocol	Src. Zone	Source	Dst. Zone	Dest
WG-Clients Breakout	Masquerade NAT	Translate	All	-	Wireguard IP Range	-	Any
Translate Network ...	Masquerade NAT	Translate	All	-	Core Trusted +5	-	Any
Translate Network ...	Masquerade NAT	Translate	All	-	Core Trusted +5	-	Any

[Reorder](#) | [Manage](#)

WG-Clients Breakout

Name: WG-Clients Breakout

Type: Masquerade Src. NAT Dest. NAT

Interface/VPN Tunnel: Internet 1 (WAN1)

Translated Port

IP Version: IPv4 IPv6

Protocol: All TCP/UDP TCP UDP Custom

Source: Any Network IP

Specific List IPv6 Interface ID

Wireguard IP Range: [Dropdown] [New](#)

Match Opposite

Port: Any Specific List

Destination: Any Network IP

Port: Any Specific List

Syslog Logging

Exclude

Handy

Client.conf

```
[Interface]
# HIER den jeweiligen privaten Schlüssel des Geräts eintragen (Laptop,
Arbeit oder Frau)
PrivateKey = <JEWEILIGER_PRIVATE_KEY>

# IP anpassen: Laptop (.4), Arbeit (.5), Frau (.6)
Address = 10.30.250.X/32

DNS = 10.30.1.111
MTU = 1360

[Peer]
# Das ist und bleibt der Public Key deines IONOS Servers
PublicKey = mFFQAlQt3yMFpG6DbCtN61XXL379epc4MoL0mGM7H30=
Endpoint = 217.160.11.95:51820
AllowedIPs = 0.0.0.0/0, ::/0
```

```
PersistentKeepalive = 25
```

From:

<https://drklipper.de/> - **Dr. Klipper Wiki**

Permanent link:

<https://drklipper.de/doku.php?id=haussteuerung:wireguard:infos>

Last update: **2026/06/04 10:54**

