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=	mFFQAlQt3yMFpG6DbCtN61XXL379epc4MoL0mGM7H30=
NAS	EGPMX6pxjh86u0M+YaNUk21suG7iFIOl2jgkvVcf1ng=	4XOnKh1ZZs6cNVjyFEjTz3njPUYTta3OSPTY4bsCLCs=
Handy	mJkKiZROoUm0PtT15kF8b3xmNVMGKUHv7dP6SxEyDEs=	Or5f7b6myu8FfYUOGG9aqCxj6L38bKlzinszbT6tHhY=
X250 Notebook	wMXaNqJ5tSzinf+XaxK95sH5RHEOThpR/qXOkKC5/3U=	UkHXpioh9plZpdDGwLa+8CuxZ9mlYR3LftEbnf8cUhU=
Firma Linux	mPGz8alOB5X0x2BtisIeVPGB+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 = 4XOnKh1ZZs6cNVjyFEjTz3njPUYTta3OSPTY4bsCLCs=
# 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 = Or5f7b6myu8FfYUOGG9aqCxj6L38bKlzinszbT6tHhY=
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

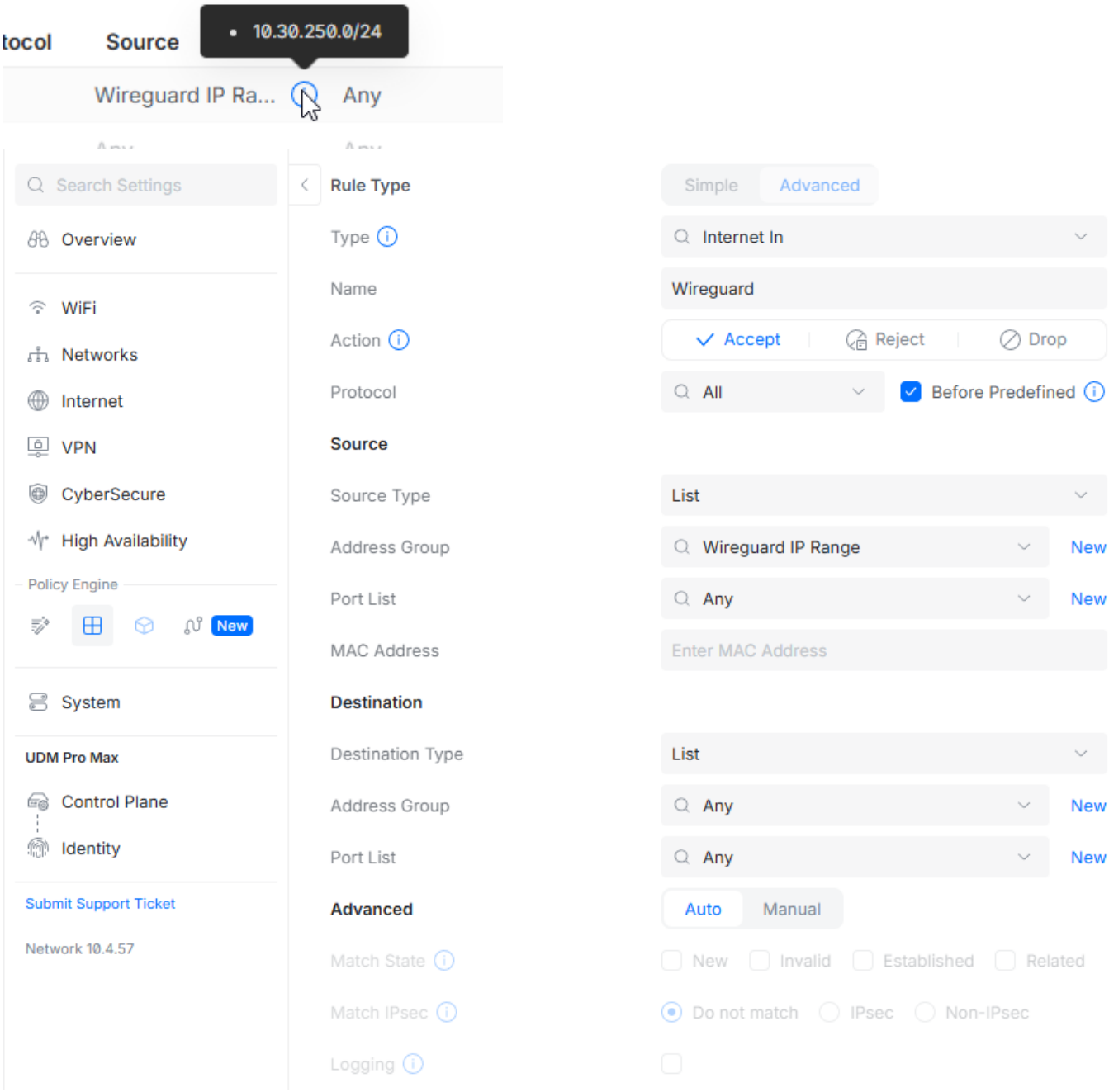
[Peer]
# Der Public Key des Servers (Peer)
PublicKey = mFFQAlQt3yMFpG6DbCtN61XXL379epc4MoL0mGM7H30=

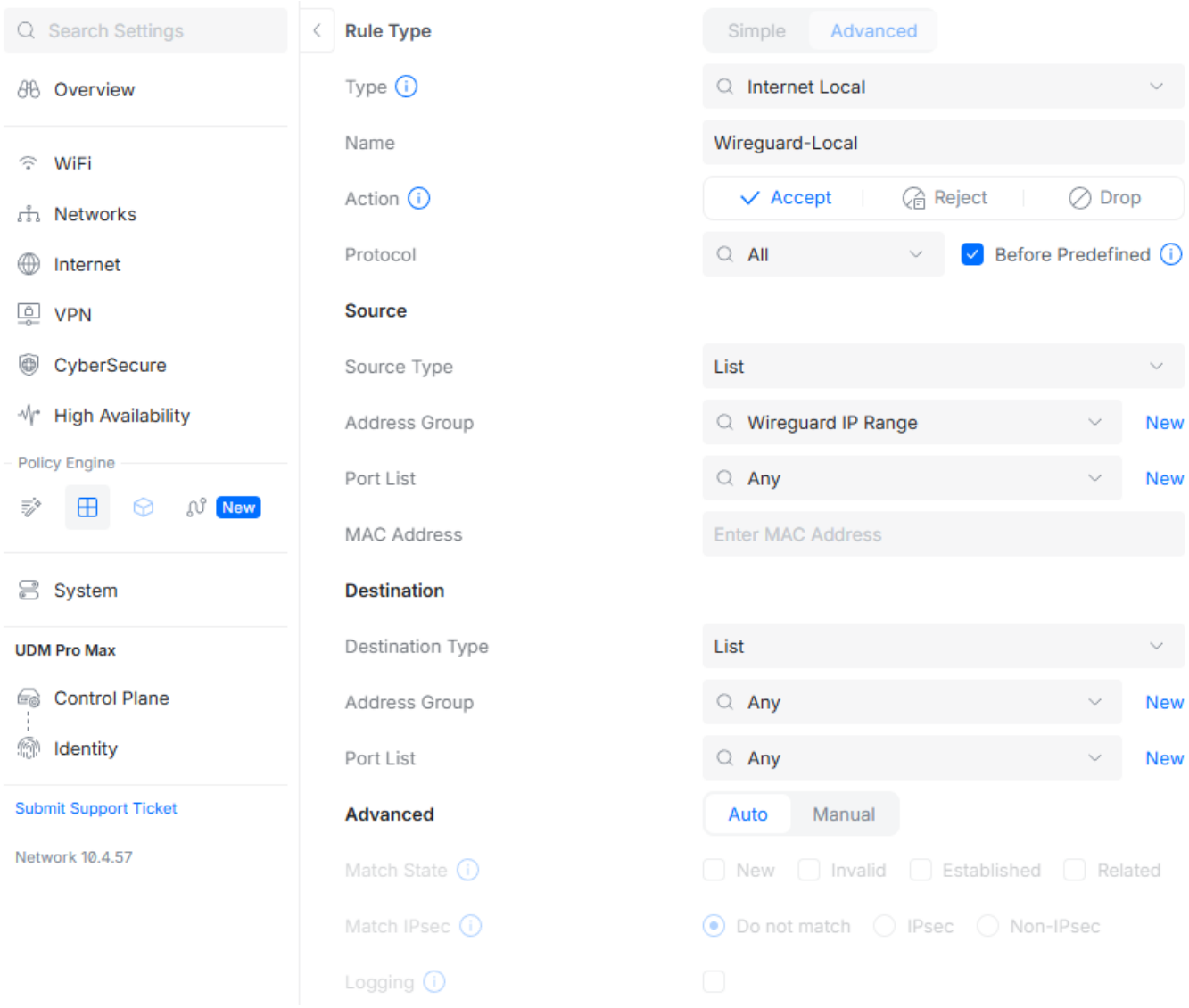
# Endpoint (IP und Port des Servers)
Endpoint = 217.160.11.95:51820

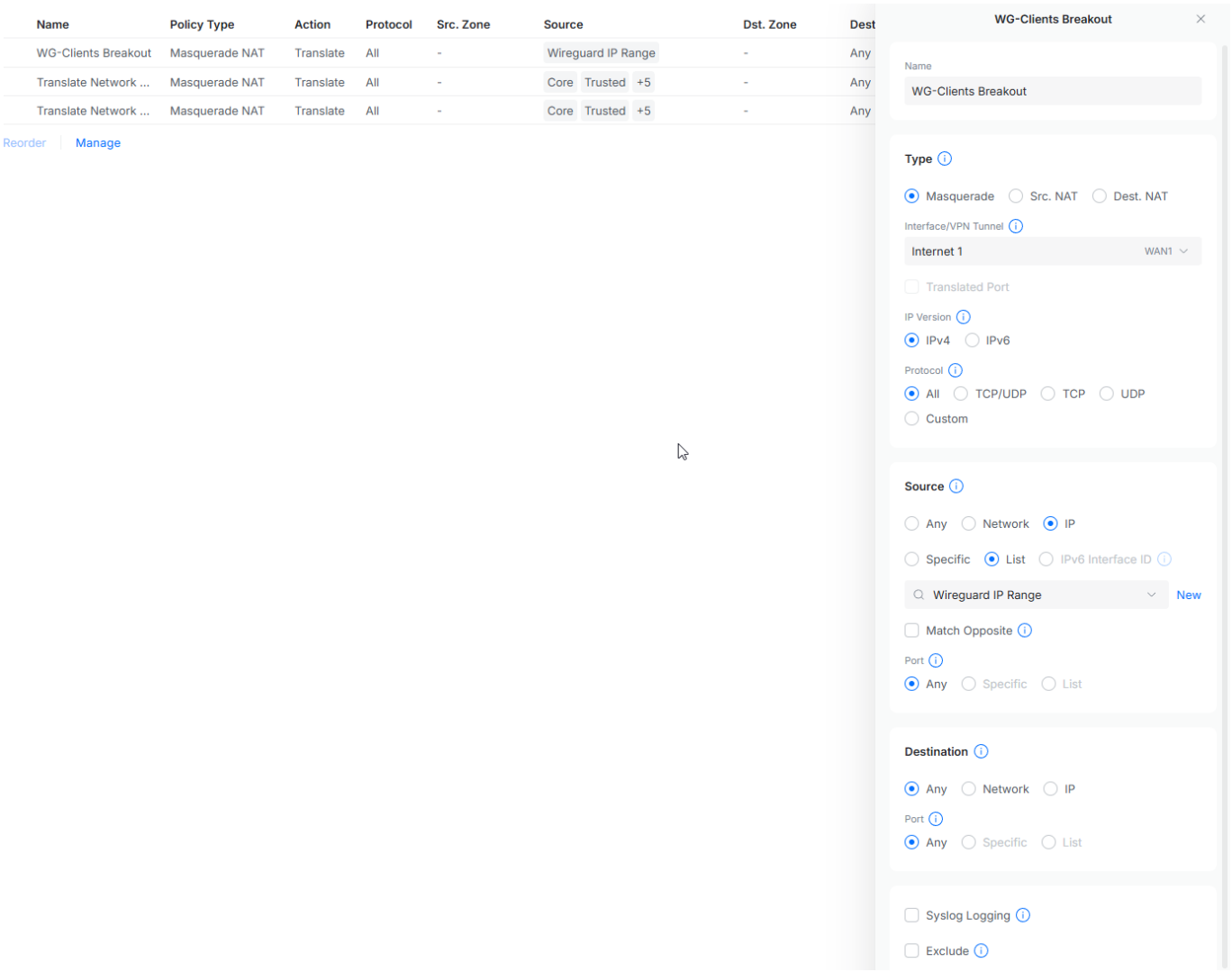
# Welcher Traffic soll durch den Tunnel? (0.0.0.0/0 bedeutet: Alles)
AllowedIPs = 0.0.0.0/0

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

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


tocol
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
Simple
Advanced
Type
Internet In
Name
Wireguard
Action
Accept
Reject
Drop
Protocol
All
Before Predefined
Source
Source Type
List
Address Group
Wireguard IP Range
New
Port List
Any
New
MAC Address
Enter MAC Address
Destination
Destination Type
List
Address Group
Any
New
Port List
Any
New
Advanced
Auto
Manual
Match State
New
Invalid
Established
Related
Match IPsec
Do not match
IPsec
Non-IPsec
Logging


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
Simple
Advanced
Type
Internet Local
Name
Wireguard-Local
Action
Accept
Reject
Drop
Protocol
All
Before Predefined
Source
Source Type
List
Address Group
Wireguard IP Range
New
Port List
Any
New
MAC Address
Enter MAC Address
Destination
Destination Type
List
Address Group
Any
New
Port List
Any
New
Advanced
Auto
Manual
Match State
New
Invalid
Established
Related
Match IPsec
Do not match
IPsec
Non-IPsec
Logging



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://www.drklipper.de/ - **Dr. Klipper Wiki**

Permanent link:
https://www.drklipper.de/doku.php?id=haussteuerung:wireguard:infos

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