Sub Station Router

History

V 0.3.2 12.sep.2023

Domain names inside tunnel
Windows commands

V 0.3.0 10.sep.2023

SubNet Domain Name

V 0.2.2 V 0.2.1 09.sep.2023

Added Try with separate SubNet 4 VPN Tunnel
Separate Tunnel must be.

V 0.2.0 06.sep.2023

First Success Tunnel with Router access and ssh

Intro

Goal

Create a OpenWRT Router as Sub Station.

The Router is a WLAN Client and contains a WireGuard Server.

On the LAN-Switch-Network-Outputs can be a SubProject; all connected Devices are accessible through the tunnel.

Devices connected at router-lan go into the Internet normally.

Clients puts a config File into Wireguard Client Software and activate the Tunnel; the they must access the Devices by understanding theis IP-Numbers.
Important: NOT MORE Complex actions on client side ! (Road Warriors)

Hardware

TP-Link TL-WDR4300 Ver. 1.7

TP-Link TL-WDR3600 Ver. 1.5

Software

OpenWRT 22.03.5

Basic Setup

LuCi

System->System:
Hostname: WDR3600 WDR4300
Timezone:Europe/Berlin

System->Administration
Change Password (Without no ssh) (b...k)

Network->Wireless:
Delete all SSID Masters
Add 5Ghz Client
Advanced Setting:DE

Network->Interfaces
->lan
Change Ipv4 Address

Network -> DHCP and DNS
General Settings -> LocalDomain
Give Names e.g.: station36; station43

MAGIC: Devices can be accessed by e.g.: pcname.station36

Save & Apply (Requires re-connect)

```
ipconfig /renew
```

Wireguard

Add Software

Before Running scripts the Wireguard Software must be installed

System->Software

->Filter: wireguard / Update Lists

Install: luci-app-wireguard

Automatic add installed:
wireguard-tools
kmod-wireguard
luci-i18n-wireguard-en
luci-proto-wireguard

Install: qrencode

Automatic add installed:
libqrencode

Reboot Device

Create script from Template:

https://openwrt.org/docs/guide-user/services/vpn/wireguard/automated

Change Defines in Head of script (separate for each device)

```
export interface="192.168.37"
export interface="192.168.42‟ # VPN SubNet

export DDNS="abcd1234abcd1234.myfritz.net"

export peer_IP="51"

export WG_${LAN}_server_port="36996"
```

```
export WG_${LAN}_server_port="43996"

export user_1="jisoo"
export user_2="jennie"
export user_3="rose"
export user_4="lisa"

export user_1="karina"
export user_2="giselle"
export user_3="winter"
export user_4="ningning"
```

Copy Script into root account

```
scp auto_wg_XX_username-id.sh root@192.168.43.1:~
```

ssh into router

```
ssh root@192.168.43.1
```

Execute in router

```
chmod +x auto_wg_XX_username-id.sh

./auto_wg_XX_username-id.sh
```

after script run

Read-Back Client scripts

```
scp -r root@192.168.XX.1:/etc/wireguard/** readbackXX/

pause ********* XXXXXXXXXXX **************
```

Post Processing

Modify the Peer config files after extraction

```
[Interface]
Address = X.X.X.X/24 # get Subnet 255.255.255.0 # necessary ????

DNS = 192.168.36.1 # change from VPN to LAN Subnet


[Peer]
# everything goes through the tunnel
AllowedIPs = 0.0.0.0/0, ::/0
# behind the tunnel are VPN and LAN SubNets
AllowedIPs = 192.168.36.0/24, 192.168.37.0/24

# ??? is this true ????
Outside Router Setup
```

Wireguard Port forwarding (Weiterleitung)

Setup xTernal Routers to forward 36996 and 43996 UDP

Ping inside VPN Tunnel with pc.domain names

Network -> DHCP and DNS -> Hostnames

Insert The Tunnel-End Ips an Give them a name

e.g. karina.sync -> 192.168.42.51

Setup differences per device

Device	Hostname	Lan Subnet domain name	Port Wireguard	Clients	VPN SubNet
WDR3600	WDR3600	192.168.36.1/24 station36	36996	Jisoo Jennie Rose Lisa	192.168.37.1/24
WDR4300	WDR4300	192.168.43.1/24 station43	43996	Karina Giselle Winter Ningning	192.168.42.1/24
Fritz 7490			58989	IU	

Ongoing

Show Routes on Windows Client

Route print

tracert <url>

nslookup <ip-number> or <url>

Questions

(Fritz Box mapped Tunnel Endpoints at same Sub-Net)

https://forum.openwrt.org/t/wireguard-connects-but-lan-not-reachable/146641

Options

All Subnets can be PING'ed

All Devices behind the tunnel can be accessed by name instead of IP Number

Clients connected by tunnel can connect each other.

IP numbers at Router WAN port are accessible / not accessible.
(Adjustable by Wireguard setup!)

Xthink

Subnet split

0-15 Internal Fix
16-63 xternal fix
64-127 dhcp
128-191 VPN Tunnel ends
192-254 options

Trap

.conf

Dont use wireguard configs for global connections inside network without necessary to go over global network. Inside intranet a separate .conf with internal numbers is necessary.

The Outside .conf works but makes lots of disciconnects

Links

main

https://openwrt.org/docs/guide-user/services/vpn/start

https://openwrt.org/docs/guide-user/services/vpn/wireguard/start

https://openwrt.org/docs/guide-user/services/vpn/wireguard/automated

full config generator

https://www.wireguardconfig.com/

qrcode generation from config file

https://www.wireguardconfig.com/qrcode

other

https://github.com/nyr

https://wiki.securepoint.de/UTM/VPN/%C3%9Cbersicht

https://www.youtube.com/watch?v=FnvP7dOmy9w&t=181s

https://www.apfeltalk.de/community/threads/os-x-ssh-remote-loesungen-unter-osx-dazu-vnc-kvm.35714/

https://github.com/pirate/wireguard-docs

https://openwrt.org/docs/guide-user/services/vpn/openvpn/client-luci

https://www.vpnunlimited.com/help/manuals/open-wrt-wireguard-setup

very other

https://sekurak.pl/more-information-about-tp-link-backdoor/

https://sekurak.pl/tp-link-httptftp-backdoor/