Ставим OpenVPN на OpenWRT
для туннельного сервиса VPNKI.ru
by XamleTT

Дано:
- 2 роутера. Оба с OpenWRT
- сеть на Хазе 192.168.1.0
- сеть на Даче 192.168.2.0

Цель:
- создать ВПН-туннель с Дачи на Хазу

Задача:
- просто вводить в компе Хазы IP-адрес дачного устройства и попадать на это устройство, не взирая на Серые IP с обеих сторон, NAT, Firewall и прочую муть

1.
Ставим пакеты:
- openvpn-openssl
- luci-app-openvpn

```
opkg update
opkg install openvpn-openssl
opkg install luci-app-openvpn
```

2.
Обновляем страницу LuCi
во вкладе Services должна появиться вкладка OpenVPN.
если вдру не появилась - отлогиниваемся из LuCi и залогиниваемся заново.
если снова нету - перегуз. Если и после перегруза нету, то см. п.1

3.
Идем на ВПНКИ, ставим галку **openvpn** на настройках туннелей, скачиваем файл **.ovpn**.
каждая новая поставновка галки генерирует **НОВЫЙ** файл, поэтому скачиваем его один раз, или используем последний из скаченных.
Файл этот внурти состоит из трех частей. Открываем его как TXT и разбираем на части.

Часть-1 **Настройки от ВПНКИ.ру**

```
client
remote msk.vpnki.ru
port номер-вашего-порта
proto udp
cipher AES-128-CBC
ns-cert-type server
key-direction 1
dev tun
auth-user-pass
explicit-exit-notify 2
reneg-sec 0
```

Часть-2 **Root CA Certificate**:
<ca>
-----BEGIN CERTIFICATE-----
Тут всякие символы
-----END CERTIFICATE-----
</ca>
Эту часть, <ca> и </ca> НЕ надо, помещаем текстовым редактором в отдельный файл и называем его **ca.crt**

Часть-3 **TLS-auth Key:**
<tls-auth>
-----BEGIN OpenVPN Static key V1-----
Тут всякие символы
-----END OpenVPN Static key V1-----
</tls-auth>
Эту часть, <tls-auth> и </tls-auth> НЕ надо, помещаем текстовым редактором в отдельный файл и называем его **tlsauth.key**

4.
Текстовым редактором создаем файл **userpass.txt**
В первой строчке только логин. Во второй строчке только пароль на нужный нам туннель.

user666
portwein777

Три готовых файла отложили в отдельную папку.
Больше никакие файлы не нужны! На Gargoyle (говорят, что..) не дает сохранить профиль, пока не присунешь туда "валидные" client.key и client.crt. Используйте OpenWRT, а не всякие форки типа Гаргульи, ГолденОрб и прочие недосборки.

5.
Через puTTy заходим на роутер по SSH.

6.
Чистим конфигурацию openvpn от разных sample-примеров, которые там болтаются.
echo > /etc/config/openvpn

7.
Придумываем название своему OpenVPN профилю. Скажем очень оригинальное: ovpnki

```
uci set openvpn.ovpnki=openvpn
uci set openvpn.ovpnki.enabled=1
uci set openvpn.ovpnki.verb=3
uci set openvpn.ovpnki.client=1
uci set openvpn.ovpnki.remote=msk.vpnki.ru
uci set openvpn.ovpnki.port= номер-вашего-порта-из-файла-настроек
uci set openvpn.ovpnki.proto=udp
uci set openvpn.ovpnki.cipher=AES-128-CBC
uci set openvpn.ovpnki.ns_cert_type=server
uci set openvpn.ovpnki.key_direction=1
uci set openvpn.ovpnki.dev=tun
uci set openvpn.ovpnki.explicit_exit_notify=2
uci set openvpn.ovpnki.reneg_sec=0
uci set openvpn.ovpnki.ca=/etc/openvpn/ca.crt
uci set openvpn.ovpnki.tls_auth=/etc/openvpn/tls.key
uci set openvpn.ovpnki.auth_user_pass=/etc/openvpn/userpass.txt
uci commit openvpn
```

Можно и нужно копировать и применять весь блок, а не по одной строчке.

8.
Проверяем содержание файла **/etc/config/openvpn**
скажем через
nano /etc/config/openvpn
(предварительно установив на OpenWRT редактор **nano**, или по старинке через **vi**)

```
config openvpn 'ovpnki'
        option enabled '1'
        option verb '3'
        option client '1'
        option remote 'msk.vpnki.ru'
        option port 'номер-вашего-порта'
        option proto 'udp'
        option cipher 'AES-128-CBC'
        option ns_cert_type 'server'
        option key_direction '1'
        option dev 'tun'
        option explicit_exit_notify '2'
        option reneg_sec '0'
        option ca '/etc/openvpn/ca.crt'
        option tls_auth '/etc/openvpn/tls.key'
        option auth_user_pass '/etc/openvpn/userpass.txt'
```

9.
Мутим себе openvpn интерфейс **tun0** с именем **ovpn**:
```
uci set network.ovpn=interface
uci set network.ovpn.ifname=tun0
uci set network.ovpn.proto=none
uci set network.ovpn.auto=1
uci commit network
/etc/init.d/network reload
```

10.
Мутим себе **фаерволл** для openvpn интерфейса:

```
uci set firewall.vpn=zone
uci set firewall.vpn.name=vpn
uci set firewall.vpn.network=ovpn
uci set firewall.vpn.input=ACCEPT
uci set firewall.vpn.forward=REJECT (REJECT- если юзаете vpn как замену WAN)
uci set firewall.vpn.output=ACCEPT
uci set firewall.vpn.masq=1
uci set firewall.vpn_forwarding_lan_in=forwarding
uci set firewall.vpn_forwarding_lan_in.src=vpn
uci set firewall.vpn_forwarding_lan_in.dest=lan
uci set firewall.vpn_forwarding_lan_out=forwarding
uci set firewall.vpn_forwarding_lan_out.src=lan
uci set firewall.vpn_forwarding_lan_out.dest=vpn
uci commit firewall
/etc/init.d/firewall reload
```

11.
Три файла, что были ранее в п. 3, закидываем по адресу **/etc/config/openvpn**
Имена файлов:
ca.crt
tlsauth.key
userpass.txt
Это можно сделать через софтину WinSCP, по протоколу SCP. Помним, что для всех маршрутов **ca.crt** и **tlsauth.key** - это одни и те же файлы. А вот **userpass.txt** разный для каждого маршрута. В каждом роутере файл **userpass.txt** свой. Это если у вас много ВПНКИ-роутеров.

12.
Очевидно туннель у вас уже работает по протоколу PPtP, но херово. (А иначе бы ты в настройку опенвипиенки на опенвээртэшке не полез. ☺) Теперь в настройках PPtP можно с сервера **msk.vpnki.ru** убрать **ru**. Выключить интерфейс, потом restart для ovpn интерфейса. **Должен заработать туннель уже на OpenVPN**, что можно проверить на сайте в "состояниях туннелей". Таким же образом можно переходить назад. Если же оставить запуск автоматом для обоих интерфейсов, то хорошего ничего не будет. При достаточной смекалке можно удаленно перенастроить роутер с PPTP на OpenVPN, не перегружая его gsm-розетками и не выезжая на место его установки.

14.
Не забываем про **Статические Маршруты** в ВПНКИ-роутерах.
Без них связи не будет.
В кажом из двух роутеров прописываем маршруты: (для Хаза)
- к сети 172.16.0.0. маска /16, шлюз 172.16.0.1
- к своей удаленной сети 192.168.Сеть.Дача, маска /24, шлюз 172.16.0.1

Если ВПНКИ-роутеры подключены к основным роутерам, раздающим инет (подключение должно быть из LAN-порта основного роутера в LAN-порт ВПНКИ-роутера), то там тоже нужно прописать два статических мрашрута:
- к сети 172.16.0.0. маска /16, шлюз 192.168.Ваш_Впнки.Роутер_на_хазе
- к своей удаленной сети 192.168.Сеть.Дача, маска /24,
шлюз 192.168.Ваш_Впнки.Роутер_на_хазе

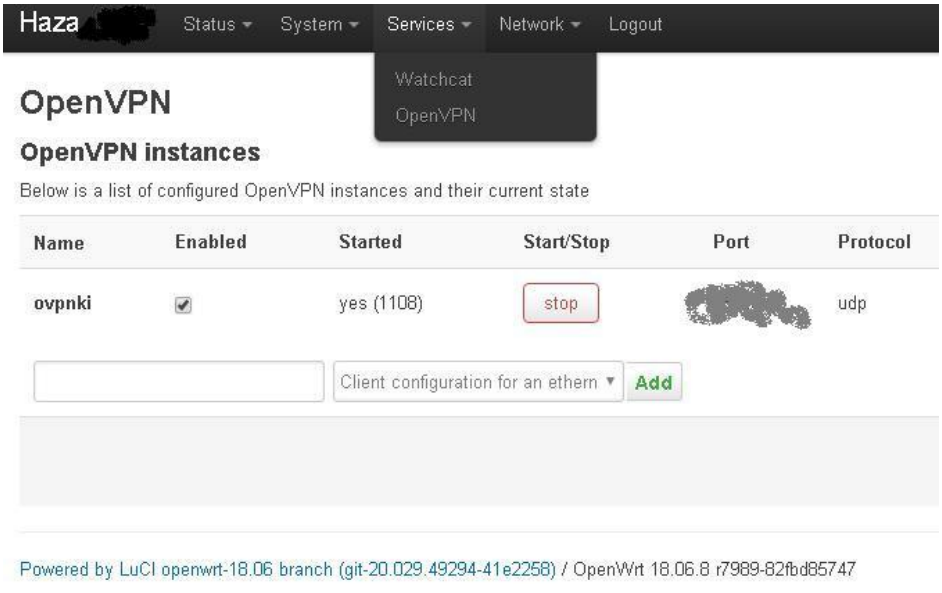
Для тех кто не одупляет как пользоваться консольным uCI, а привык к web-интерфейсу LuCI я понаснимаю скрин-шотов того, что получилось.

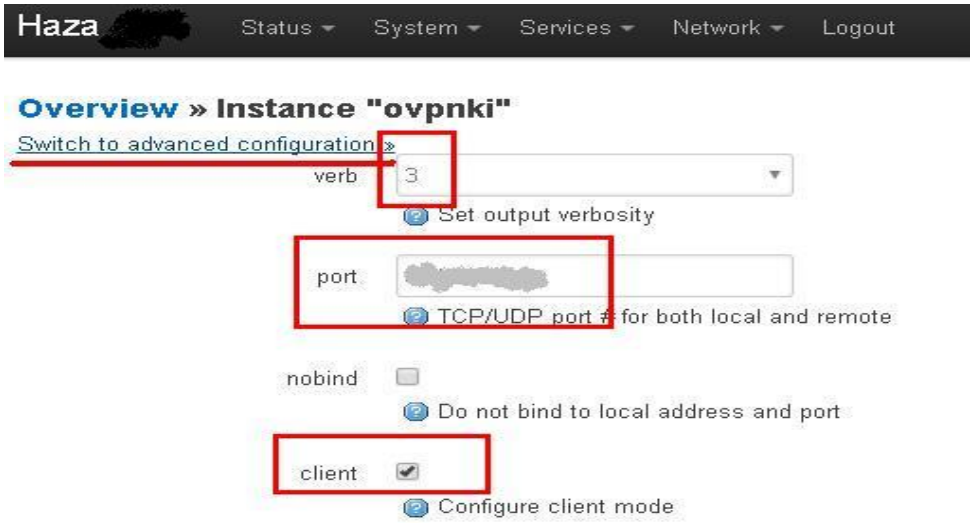
15.
Скрипты
Так же в систему надо вставить скрипты:
- перегрузка интерфейса по отсутствию пинга на шлюз сервер ВПНКИ, 172..16.xx.xx
- перегрузка роутера по отсутствию пинга на инет, скажем на гугл 8.8.8.8
- перегрузка роутера по шедулеру раз в сутки
- прописать настройки для трех светодиодов, чтобы было визуально видно:
--- связь роутера с сервером ВПНКИ на , 172..16.xx.xx
--- связь вашего роутера с другим вашим роутером, т.е. рабочий поднятый туннель
--- RX-TX данные по туннелю, чтоб диоды красиво мигали в момент обмена данными.

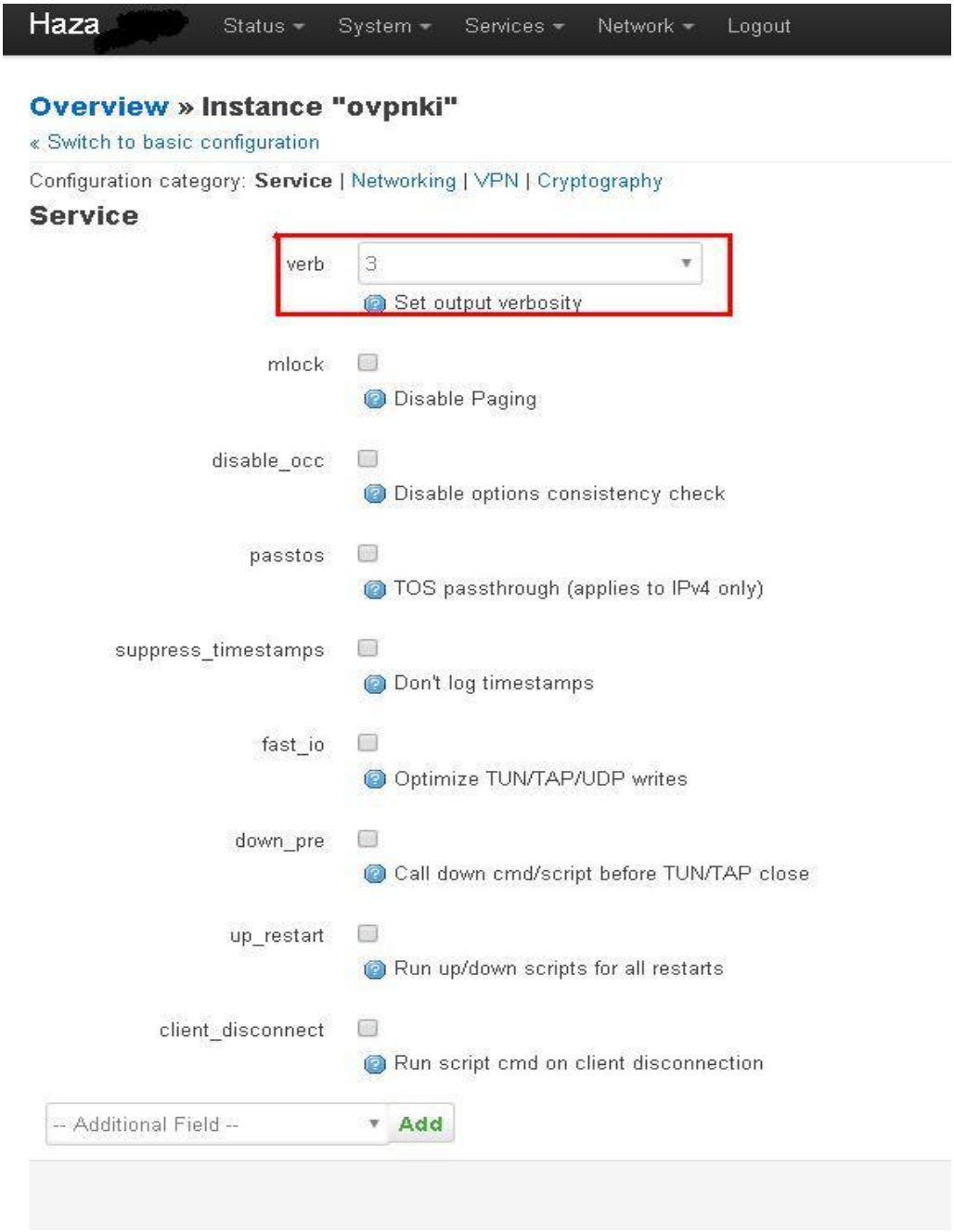
® XamleTT, 2021.02.07

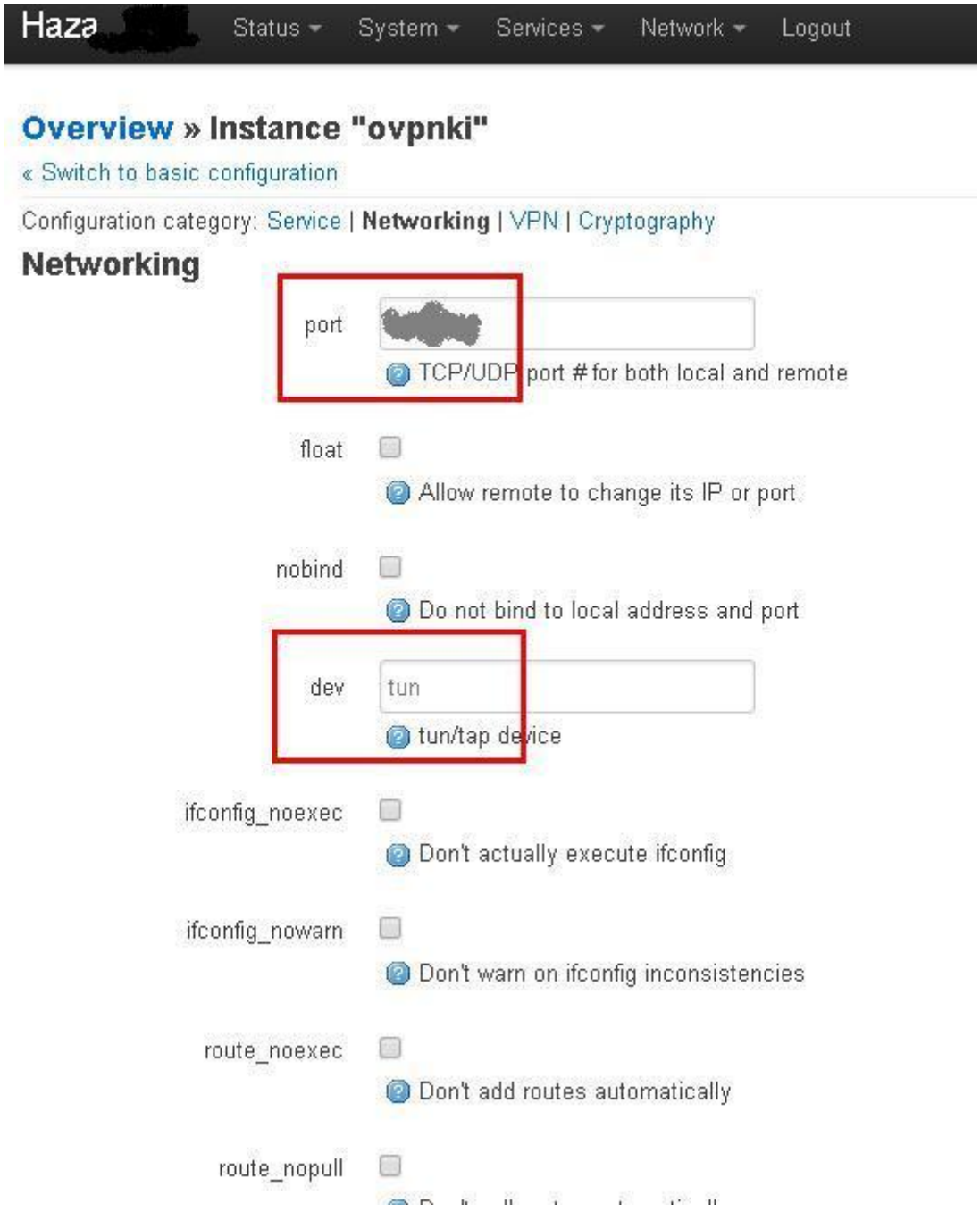
Extra-read:
https://openwrt.org/docs/guide-user/services/vpn/openvpn/start

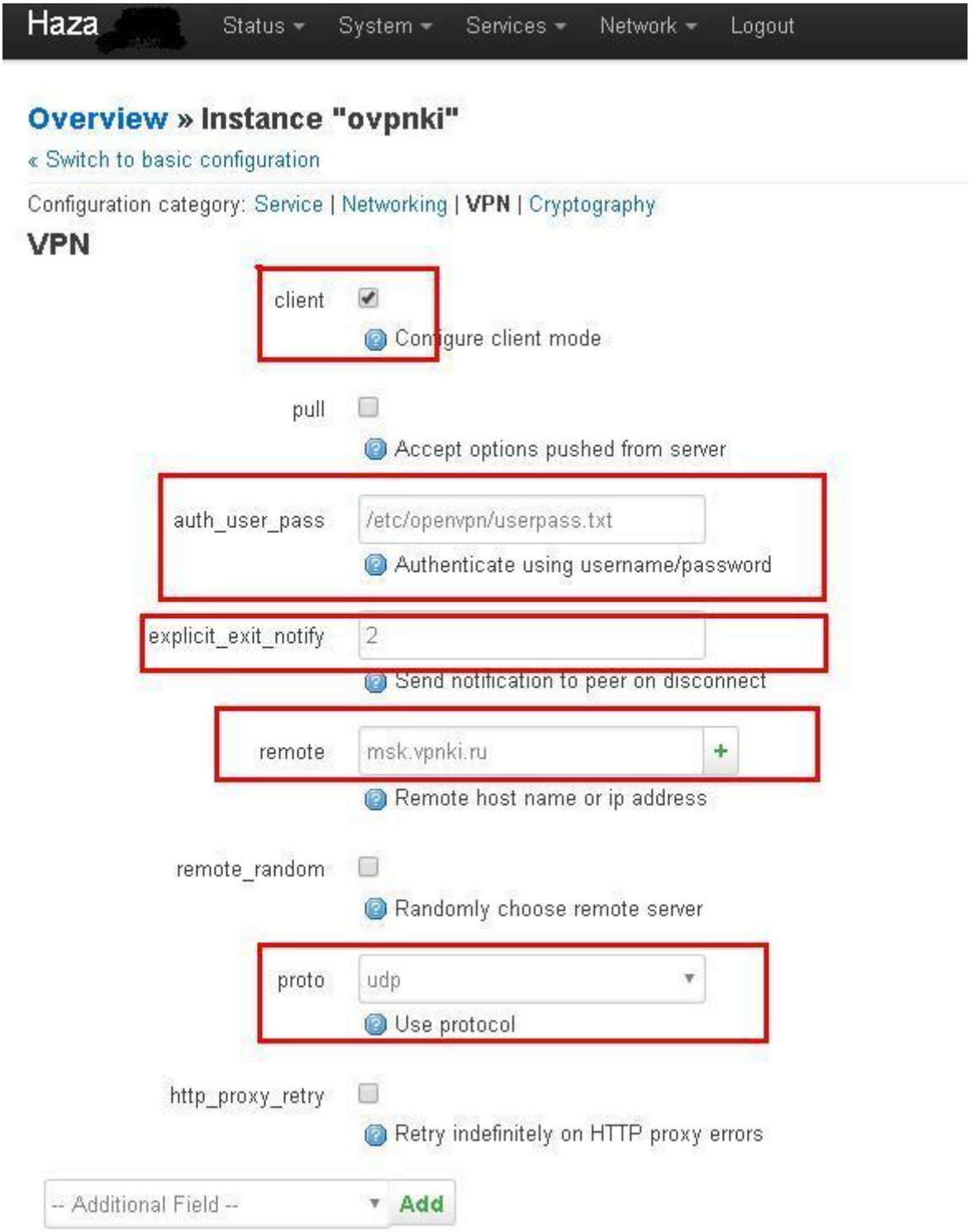
Скрины для LuCi-дрочеров

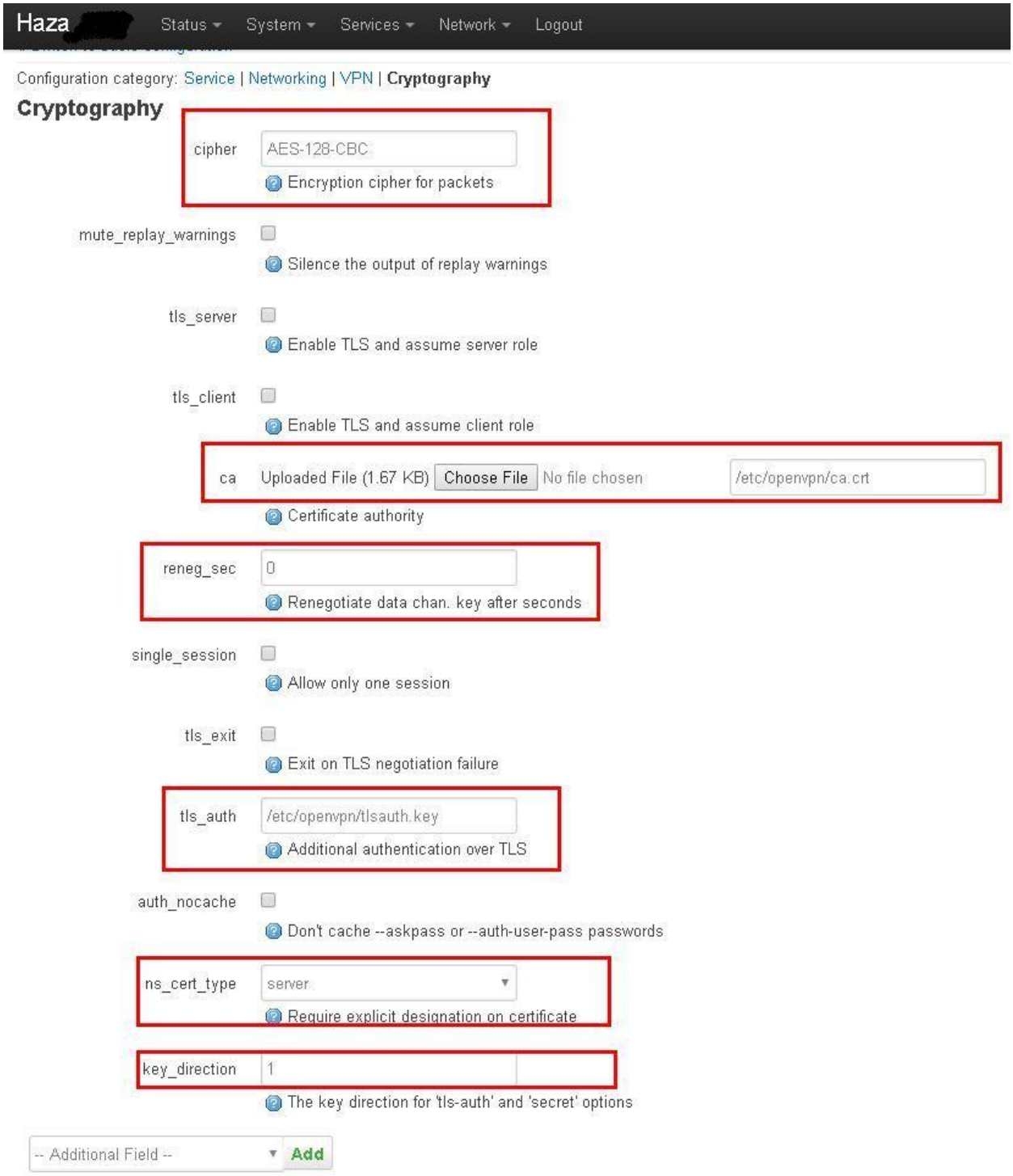


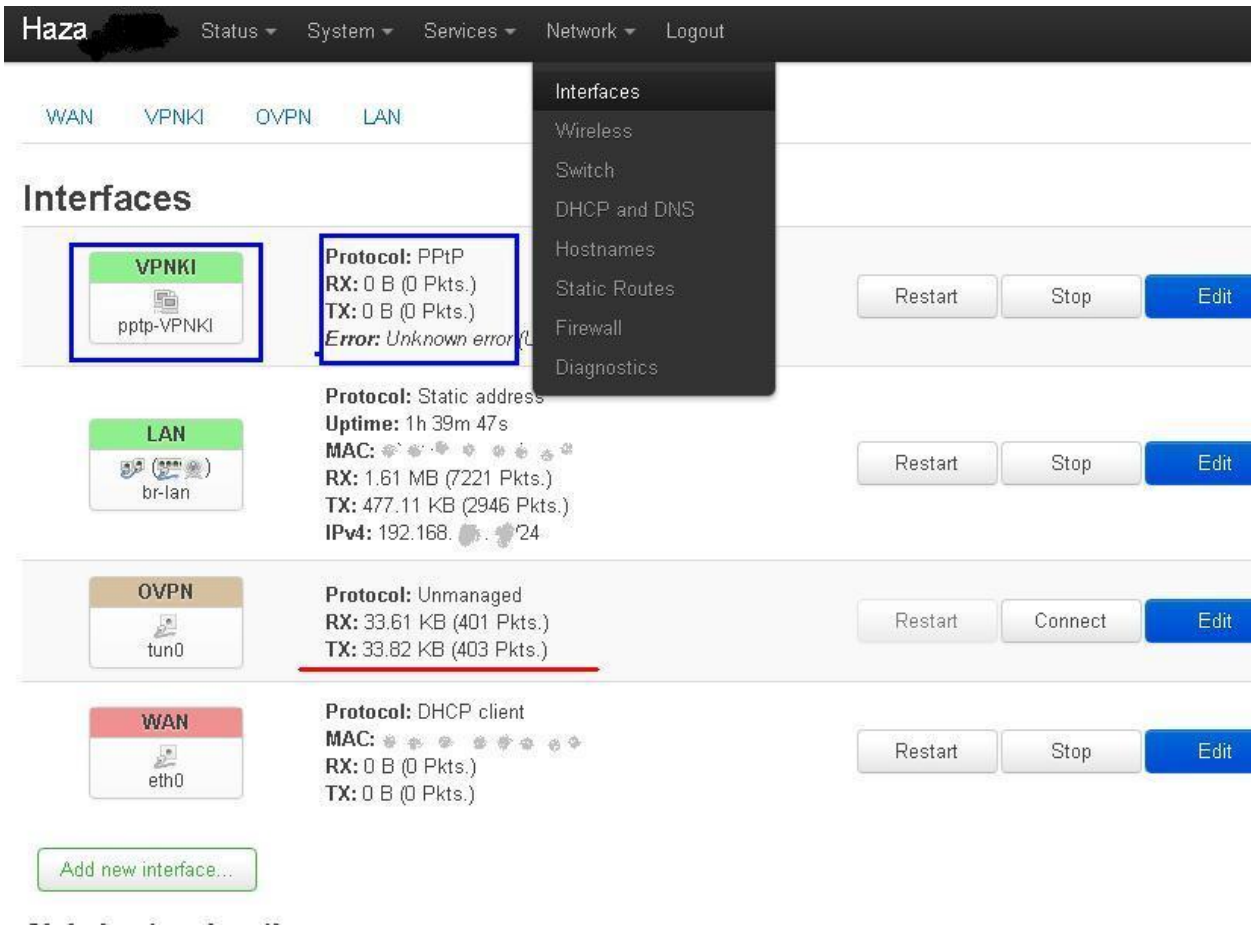

Haza
Status
System
Services
Network
Logout
Overview » Instance "ovpnki"
Switch to advanced configuration »
verb
3
Set output verbosity
port
TCP/UDP port # for both local and remote
nobind
Do not bind to local address and port
client
Configure client mode

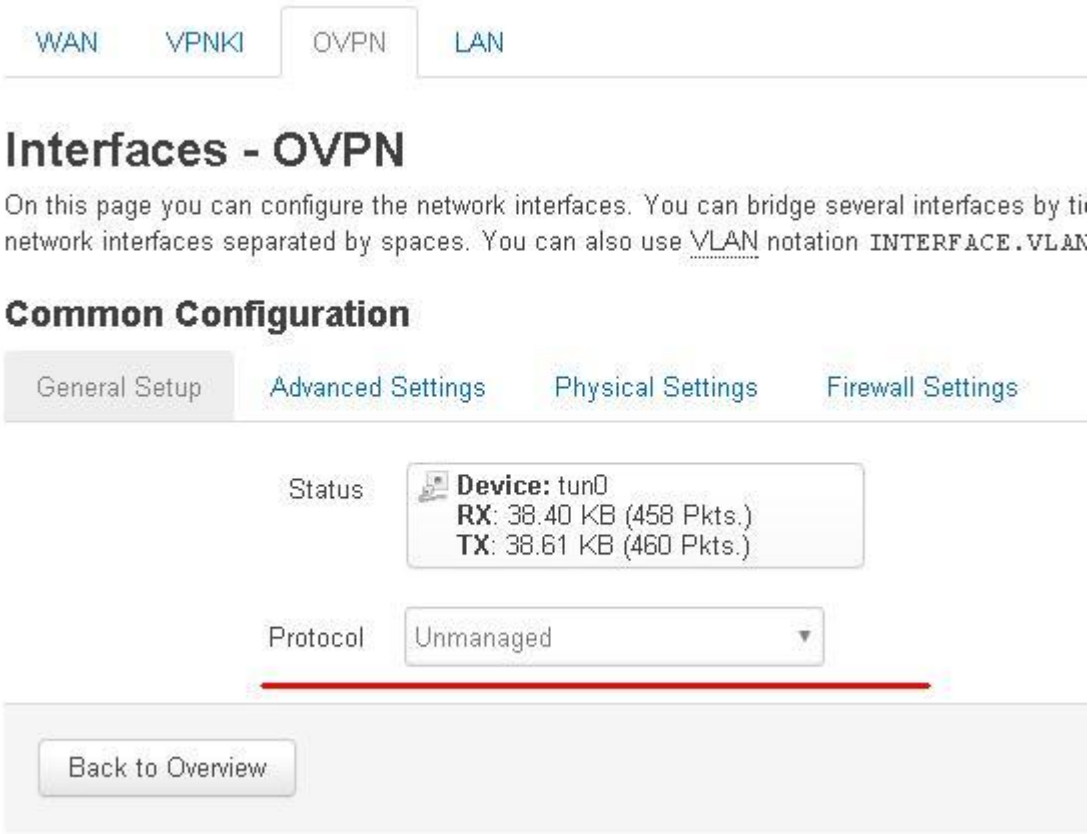

Haza
Status
System
Services
Network
Logout
Overview » Instance "ovpnki"
« Switch to basic configuration
Configuration category: Service | Networking | VPN | Cryptography
Service
verb
3
Set output verbosity
mlock
Disable Paging
disable_occ
Disable options consistency check
passtos
TOS passthrough (applies to IPv4 only)
suppress_timestamps
Don't log timestamps
fast_io
Optimize TUN/TAP/UDP writes
down_pre
Call down cmd/script before TUN/TAP close
up_restart
Run up/down scripts for all restarts
client_disconnect
Run script cmd on client disconnection
-- Additional Field --
Add

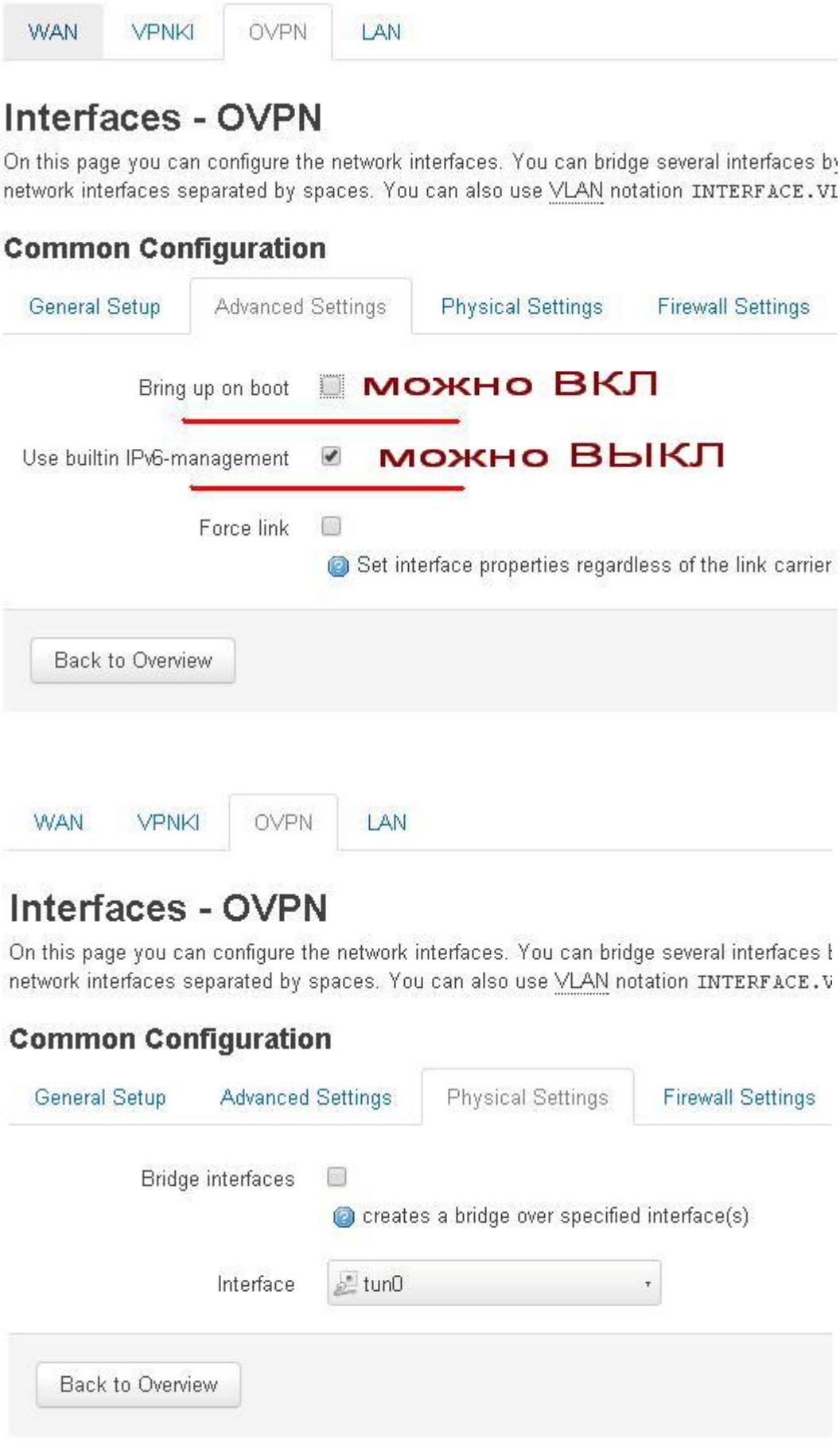

Haza
Status
System
Services
Network
Logout
Overview » Instance "ovpnki"
« Switch to basic configuration
Configuration category: Service | Networking | VPN | Cryptography
Networking
port
TCP/UDP port # for both local and remote
float
Allow remote to change its IP or port
nobind
Do not bind to local address and port
dev
tun
tun/tap device
ifconfig_noexec
Don't actually execute ifconfig
ifconfig_nowarn
Don't warn on ifconfig inconsistencies
route_noexec
Don't add routes automatically
route_nopull


Haza
Status
System
Services
Network
Logout
Overview » Instance "ovpnki"
« Switch to basic configuration
Configuration category: Service | Networking | VPN | Cryptography
VPN
client
Configure client mode
pull
Accept options pushed from server
auth_user_pass
/etc/openvpn/userpass.txt
Authenticate using username/password
explicit_exit_notify
2
Send notification to peer on disconnect
remote
msk.vpnki.ru
Remote host name or ip address
remote_random
Randomly choose remote server
proto
udp
Use protocol
http_proxy_retry
Retry indefinitely on HTTP proxy errors
-- Additional Field --
Add


Haza
Status
System
Services
Network
Logout
Configuration category: Service | Networking | VPN | Cryptography
Cryptography
cipher
AES-128-CBC
Encryption cipher for packets
mute_replay_warnings
Silence the output of replay warnings
tls_server
Enable TLS and assume server role
tls_client
Enable TLS and assume client role
ca
Uploaded File (1.67 KB)
Choose File
No file chosen
/etc/openvpn/ca.crt
Certificate authority
reneg_sec
0
Renegotiate data chan. key after seconds
single_session
Allow only one session
tls_exit
Exit on TLS negotiation failure
tls_auth
/etc/openvpn/tlsauth.key
Additional authentication over TLS
auth_nocache
Don't cache --askpass or --auth-user-pass passwords
ns_cert_type
server
Require explicit designation on certificate
key_direction
1
The key direction for 'tls-auth' and 'secret' options
-- Additional Field --
Add


Haza
Status
System
Services
Network
Logout
Interfaces
Wireless
Switch
DHCP and DNS
Hostnames
Static Routes
Firewall
Diagnostics
WAN
VPNKI
OVPN
LAN
Interfaces
VPNKI
pptp-VPNKI
Protocol: PPtP
RX: 0 B (0 Pkts.)
TX: 0 B (0 Pkts.)
Error: Unknown error
Restart
Stop
Edit
LAN
br-lan
Protocol: Static address
Uptime: 1h 39m 47s
MAC:
RX: 1.61 MB (7221 Pkts.)
TX: 477.11 KB (2946 Pkts.)
IPv4: 192.168.
'24
Restart
Stop
Edit
OVPN
tun0
Protocol: Unmanaged
RX: 33.61 KB (401 Pkts.)
TX: 33.82 KB (403 Pkts.)
Restart
Connect
Edit
WAN
eth0
Protocol: DHCP client
MAC:
RX: 0 B (0 Pkts.)
TX: 0 B (0 Pkts.)
Restart
Stop
Edit
Add new interface...


WAN
VPNKI
OVPN
LAN
Interfaces - OVPN
On this page you can configure the network interfaces. You can bridge several interfaces by ti
network interfaces separated by spaces. You can also use VLAN notation INTERFACE.VLAN
Common Configuration
General Setup
Advanced Settings
Physical Settings
Firewall Settings
Status
Device: tun0
RX: 38.40 KB (458 Pkts.)
TX: 38.61 KB (460 Pkts.)
Protocol
Unmanaged
Back to Overview


WAN
VPNKI
OVPN
LAN
Interfaces - OVPN
On this page you can configure the network interfaces. You can bridge several interfaces by
network interfaces separated by spaces. You can also use VLAN notation INTERFACE.VI
Common Configuration
General Setup
Advanced Settings
Physical Settings
Firewall Settings
Bring up on boot
можно ВКЛ
Use builtin IPv6-management
можно ВЫКЛ
Force link
Set interface properties regardless of the link carrier
Back to Overview
WAN
VPNKI
OVPN
LAN
Interfaces - OVPN
On this page you can configure the network interfaces. You can bridge several interfaces b
network interfaces separated by spaces. You can also use VLAN notation INTERFACE.V
Common Configuration
General Setup
Advanced Settings
Physical Settings
Firewall Settings
Bridge interfaces
creates a bridge over specified interface(s)
Interface
tun0
Back to Overview

WAN VPNKI OVPN LAN

Interfaces - OVPN

On this page you can configure the network interfaces. You can bridge several interfaces by ticking network interfaces separated by spaces. You can also use VLAN notation INTERFACE.VLANNR (e

Common Configuration

General Setup | Advanced Settings | Physical Settings | Firewall Settings

Create / Assign firewall-zone: vpn: ovpn:

Choose the firewall zone you want to assign to this interface. zone or fill out the *create* field to defi e a new zone and attac

Back to Overview

General Settings | Port Forwards | Traffic Rules | Custom Rules

Firewall - Zone Settings

The firewall creates zones over your network interfaces to control network traffic flow.

General Settings

Enable SYN-flood protection

Drop invalid packets

Input: accept

Output: accept

Forward: accept

Zones

Name	Zone ⇒ Forwardings	Input	Output	Forward	Masquerading	MSS clamping	
lan	lan ⇒ wan vpn	accept	accept	accept	☑	☑	Edit
wan	wan ⇒ lan	accept	accept	accept	☑	☑	Edit
vpn	vpn ⇒ lan	accept	accept	accept	☑	☑	Edit

Add