🔐

OpenVPN + Wireguard

1.1 OpenVPN МЕЖДУ РОУТЕРАМИ

На COD-RTR (сервер):

Установка:

```
apt update
apt install -y openvpn easy-rsa
```

Создание сертификатов:

```
make-cadir ~/openvpn-ca
cd ~/openvpn-ca
./easyrsa init-pki
./easyrsa build-ca nopass
```

Когда спросит Common Name → нажми Enter

Сертификат сервера:

```
./easyrsa gen-req server nopass
./easyrsa sign-req server server
```

Когда спросит "Type 'yes'" → пиши `yes`

DH параметры:

```
./easyrsa gen-dh
```

TLS ключ:

```
openvpn --genkey secret ta.key
```

Сертификат для MAIN-RTR:

```
./easyrsa gen-req main-rtr nopass
./easyrsa sign-req client main-rtr
```

Конфиг сервера:

```
nano /etc/openvpn/server.conf
```

Вставь:

```
port 1194
proto udp
dev tun

ca /root/openvpn-ca/pki/ca.crt
cert /root/openvpn-ca/pki/issued/server.crt
key /root/openvpn-ca/pki/private/server.key
dh /root/openvpn-ca/pki/dh.pem
tls-auth /root/openvpn-ca/ta.key 0

server 10.8.0.0 255.255.255.0

push "route 10.10.10.0 255.255.255.0"
push "route 10.10.20.0 255.255.255.0"

keepalive 10 120
cipher AES-256-GCM
persist-key
persist-tun

status /var/log/openvpn-status.log
```

```
log-append /var/log/openvpn.log
verb 3
```

Запуск:

```
systemctl enable openvpn@server
systemctl start openvpn@server
```

На MAIN-RTR (клиент):

Установка:

```
apt install -y openvpn
```

Скопируй сертификаты с COD-RTR:

```
# На COD-RTR:
cd ~/openvpn-ca
tar -czf main-rtr-certs.tar.gz pki/ca.crt pki/issued/main-rtr.crt pki/private/main-rtr.key ta.key

# Перенеси файл на MAIN-RTR через scp
scp main-rtr-certs.tar.gz root@MAIN-RTR:/tmp/

# На MAIN-RTR:
cd /tmp
tar -xzf main-rtr-certs.tar.gz
mkdir -p /etc/openvpn/
mv pki/ca.crt /etc/openvpn/
mv pki/issued/main-rtr.crt /etc/openvpn/
mv pki/private/main-rtr.key /etc/openvpn/
mv ta.key /etc/openvpn/
```

Конфиг клиента:

```
nano /etc/openvpn/client.conf
```

Вставь:

```
client
dev tun
proto udp
remote <IP_COD-RTR> 1194

ca /etc/openvpn/ca.crt
cert /etc/openvpn/main-rtr.crt
key /etc/openvpn/main-rtr.key
tls-auth /etc/openvpn/ta.key 1

cipher AES-256-GCM
persist-key
persist-tun
verb 3
```

Замени `<IP_COD-RTR>` на реальный IP внешнего интерфейса COD-RTR (например 152.32.66.1)

Запуск:

```
systemctl enable openvpn@client
systemctl start openvpn@client
```

Проверка:

```
ip a show tun0
ping 10.8.0.1
```

1.2 Wireguard (РЕЗЕРВНЫЙ VPN)

На COD-RTR:

```
apt install -y wireguard
```

Генерация ключей:

```
cd /etc/wireguard
wg genkey | tee server_private.key | wg pubkey > server_public.key
```

Конфиг:

```
nano /etc/wireguard/wg0.conf
```

Вставь:

```
[Interface]
Address = 10.9.0.1/24
ListenPort = 51820
PrivateKey = ВСТАВЬ_СОДЕРЖИМОЕ_server_private.key

[Peer]
PublicKey = ВСТАВЬ_client_public.key_С_MAIN-RTR
AllowedIPs = 10.9.0.2/32
```

Запуск:

```
systemctl enable wg-quick@wg0
systemctl start wg-quick@wg0
```

На MAIN-RTR:

```
apt install -y wireguard
cd /etc/wireguard
```

```
wg genkey | tee client_private.key | wg pubkey > client_publi
c.key
```

Покажи публичный ключ:

```
cat client_public.key
```

Скопируй его и вставь в конфиг COD-RTR выше (в строку PublicKey)

Конфиг:

```
nano /etc/wireguard/wg0.conf
```

Вставь:

```
[Interface]
Address = 10.9.0.2/24
PrivateKey = ВСТАВЬ_СОДЕРЖИМОЕ_client_private.key

[Peer]
PublicKey = ВСТАВЬ_server_public.key_С_COD-RTR
Endpoint = <IP_COD-RTR>:51820
AllowedIPs = 10.9.0.0/24, 10.10.0.0/16
PersistentKeepalive = 25
```

НЕ запускаем Wireguard сейчас (он резервный!)

1.3 АВТОПЕРЕКЛЮЧЕНИЕ OpenVPN → Wireguard

На MAIN-RTR создай скрипт мониторинга:

```
nano /usr/local/bin/vpn-failover.sh
```

Вставь:

```
#!/bin/bash

while true; do
  if systemctl is-active --quiet openvpn@client; then
    if ! ping -c 2 -W 3 10.8.0.1 &>/dev/null; then
      systemctl stop openvpn@client
      systemctl start wg-quick@wg0
      logger "VPN failover: switched to Wireguard"
    fi
  else
    if ping -c 2 -W 3 10.9.0.1 &>/dev/null; then
      systemctl stop wg-quick@wg0
      systemctl start openvpn@client
      logger "VPN failover: switched back to OpenVPN"
    fi
  fi
  sleep 10
done
```

Сделать исполняемым:

```
chmod +x /usr/local/bin/vpn-failover.sh
```

Создать systemd service:

```
nano /etc/systemd/system/vpn-failover.service
```

Вставь:

```
[Unit]
Description=VPN Failover Monitor
After=network.target

[Service]
Type=simple
```

```
ExecStart=/usr/local/bin/vpn-failover.sh
Restart=always

[Install]
WantedBy=multi-user.target
```

Запуск:

```
systemctl daemon-reload
systemctl enable vpn-failover
systemctl start vpn-failover
```

1.4 OpenVPN ДЛЯ REMOTE-WORKER

На COD-RTR создать сертификат:

```
cd ~/openvpn-ca
./easyrsa gen-req remote-worker nopass
./easyrsa sign-req client remote-worker
```

Упаковать для клиента:

```
mkdir ~/remote-worker-vpn
cp pki/ca.crt ~/remote-worker-vpn/
cp pki/issued/remote-worker.crt ~/remote-worker-vpn/
cp pki/private/remote-worker.key ~/remote-worker-vpn/
cp ta.key ~/remote-worker-vpn/
```

Создать конфиг:

```
nano ~/remote-worker-vpn/remote-worker.ovpn
```

Вставь:

```
client
dev tun
proto udp
remote <IP_COD-RTR> 1194

ca ca.crt
cert remote-worker.crt
key remote-worker.key
tls-auth ta.key 1

cipher AES-256-GCM
verb 3
```

Перенеси папку `~/remote-worker-vpn` на REMOTE-WORKER

На REMOTE-WORKER:

```
apt install -y openvpn

# Скопируй все файлы в /etc/openvpn/
cp ~/remote-worker-vpn/* /etc/openvpn/
```

```
nano ~/Desktop/vpn-connect.sh
```

Вставь:

```
#!/bin/bash
sudo openvpn --config /etc/openvpn/remote-worker.ovpn --daemo
n
notify-send "VPN" "Подключение к VPN..."
```

Сделать исполняемым:

```
chmod +x ~/Desktop/vpn-connect.sh
```

Автоподключение при восстановлении сети:

```
nano /usr/local/bin/vpn-auto-reconnect.sh
```

Вставь:

```
#!/bin/bash

INTERFACE="eth0"

while true; do
  if ip link show $INTERFACE | grep -q "state UP"; then
    if ! pgrep -f "openvpn.*remote-worker" > /dev/null; then
      openvpn --config /etc/openvpn/remote-worker.ovpn --daemon
      logger "VPN auto-reconnected"
    fi
  fi
  sleep 10
done
```

Создать service:

```
chmod +x /usr/local/bin/vpn-auto-reconnect.sh

nano /etc/systemd/system/vpn-auto-reconnect.service
```

Вставь:

```
[Unit]
Description=VPN Auto Reconnect
After=network.target
```

```
[Service]
ExecStart=/usr/local/bin/vpn-auto-reconnect.sh
Restart=always

[Install]
WantedBy=multi-user.target
```

Запуск:

```
systemctl enable vpn-auto-reconnect
systemctl start vpn-auto-reconnect
```