OpenVPN

OpenVPN je open source program pro vytvoření VPN tunelu mezi hostitelskými stanicemi. Stáhnout lze zde. Běží jak na UNIXových OS, tak ve Windows. Linuxové distribuce ho mají obvykle v repozitářích.

Server

Instalace

Archlinux

```
pacman -S openvpn
```

Fedora

```
yum install openvpn
```

Konfigurace certifikační autority

V souboru /usr/share/openvpn/easy-rsa/vars nastavit následující informace o certifikační autoritě. Je lepší nepoužívat diakritiku.

```
export KEY_COUNTRY="CZ"
export KEY_PROVINCE="Kraj"
export KEY_CITY="Mesto"
export KEY_ORG="Organizace"
export KEY_EMAIL="muj@email.cz"
```

délku klíče nastavit na 2048 bitů

```
export KEY_SIZE=2048
```

ostatní proměnné KEY_* je možné zakomentovat

```
#export KEY_EMAIL=mail@host.domain
#export KEY_CN=changeme
#export KEY_NAME=changeme
#export KEY_OU=changeme
```

Vytvoření certifikační autority

adresář `/usr/share/openvpn/easy-rsa/`

```
$ cd /usr/share/openvpn/easy-rsa/
```

export proměnných

```
$ source ./vars
```

smazání všech předchozích certifikátů a klíčů

```
$ ./clean-all
```

vytvoření certifikační autority, Všechny otázky je možné odentrovat, protože se nastaví podle exportovaných proměnných.

```
$ ./build-ca
```

Generování klíčů a certifikátů

generování parametrů pro Diffie-Hellman

```
$ ./build-dh
```

generování klíče a certifikátu pro server, jméno serveru musí být unikátní

```
$ ./build-key-server jmeno_serveru
```

generování klíče a certifikátu pro klienta

```
$ ./build-key-server jmeno_klienta
```

Konfigurace

nastavení se dělá v souboru `/etc/openvpn/<nazev serveru>.conf`

```
# openvpn běží v modě server
mode server

# tento počítač je server
tls-server

# zařízení, které se vytvoří
dev tap0
```

```
# port
port 1194

# protokol
proto udp

# adresa serveru ve virtuální síti
ifconfig 192.168.2.1 255.255.255.0

# konfigurační parametry, které se pošlou klientovi
push "route 192.168.1.0 255.255.255.0"
push "route-gateway 192.168.2.1"

# adresy, které se budou přidělovat klientům
ifconfig-pool 192.168.2.10 192.168.2.50 255.255.255.0

# více klientů se může přihlásit naráz
duplicate-cn

# upravuje komunikaci klienta s klientem - paket odešle ihned OpenVPN démon
client-to-client

# certifikát certifikační autority
ca ca.crt

# certifikát serveru
cert VPN-Server.crt

# klíč serveru
key VPN-Server.key

# parametry pro Diffie-Hellman
dh dh2048.pem

# povolení komprese
comp-lzo

# soubor, kam ukládá server pravidelně svůj stav
log-append /var/log/vpn.log

# stupeň "ukecanosti" démona
verb 3
```

potřebné klíče a certifikáty je nutné zkopírovat z `/usr/share/openvpn/easy-rsa/keys/` do `/etc/openvpn/`

aby server fungoval, je potřeba povolit port 1194 v `iptables`

```
iptables -A INPUT -p udp --dport 1194 -j ACCEPT
iptables -A OUTPUT -p udp --sport 1194 -j ACCEPT
```

Konfigurace - bridge mode

pro vytvoření bridge je třeba nainstalovat `bridge-utils`, ve feodře

```
yum install bridge-utils
```

konfigurační soubor může vypadat následovně

```
server-bridge <adresa serveru> <maska sítě> <první adresa přidělovaná
serverem> <poslední adresa přidělovaná serverem>
tls-server
dev tap0
port 1194
proto udp
ifconfig-pool-persist ipp.txt
duplicate-cn
client-to-client
ca ca.crt
cert VPN-Server.crt
key VPN-Server.key
dh dh2048.pem
comp-lzo
log-append /var/log/vpn.log
verb 3
```

skript, který nastaví potřebná rozhraní

```
#!/bin/bash

### BEGIN INIT INFO
# Provides:             bridge
# Required-Start:       $remote_fs $syslog
# Required-Stop:        $remote_fs $syslog
# Default-Start:        2 3 4 5
# Default-Stop:
# Short-Description:    Bridge for OpenVPN
### END INIT INFO

# Define Bridge Interface
br="br0"
# Define list of TAP interfaces to be bridged,
# for example tap="tap0 tap1".
tap="tap0"
# Define physical ethernet interface to be bridged
# with TAP interface(s) above.
eth="<fyzicky interface>"
eth_ip="<adresa serveru>"
eth_netmask="<sitova maska>"
```

```
eth_broadcast="<broadcastova adresa>"
gw="<adresa brany>"

################################
# Set up Ethernet bridge on Linux
# Requires: bridge-utils
################################
start_bridge () {
    for t in $tap; do
        openvpn --mktun --dev $t
    done

    brctl addbr $br
    brctl addif $br $eth
    for t in $tap; do
        brctl addif $br $t
    done

    for t in $tap; do
        ifconfig $t 0.0.0.0 promisc up
    done
    ifconfig $eth 0.0.0.0 promisc up
    ifconfig $br $eth_ip netmask $eth_netmask broadcast $eth_broadcast up
    route add default gw $gw $br
}

####################################
# Tear Down Ethernet bridge on Linux
####################################
stop_bridge () {
    ifconfig $br down
    brctl delbr $br
    for t in $tap; do
        openvpn --rmtun --dev $t
    done
    ifconfig $eth $eth_ip netmask $eth_netmask broadcast $eth_broadcast up
    route add default gw $gw $eth
}

####################################
# OPTIONS
####################################
case "$1" in
    start)
        echo -n "Starting Bridge"
        start_bridge
        ;;
    stop)
        echo -n "Stopping Bridge"
        stop_bridge
        ;;
```

```
    restart)
        stop_bridge
        sleep 2
        start_bridge
        ;;
    *)
        echo "Usage: $0 {start|stop|restart}"
        exit 1
        ;;
esac
```

v iptables je potřeba nastavit následující pravidla

```
iptables -I INPUT -i tap+ -j ACCEPT
iptables -I INPUT -i br0 -j ACCEPT
iptables -I FORWARD -i br0 -j ACCEPT
```

skript jsem nastavil aby se spouštěl v `/etc/rc.d/rc.local`. Trochu byl problém, když jsem nastavoval statický adresy pro eth0. Po tom co jsem tuto volbu smazal z `/etc/sysconfig/network-scripts/ifcfg-eth0` tak vše beželo jak mělo.

Povolení openVPN se systemd

```
systemctl enable openvpn@.service
ln -s /lib/systemd/system/openvpn\@.service
/etc/systemd/system/multi-user.target.wants/openvpn\@<nazev serveru>.service
systemctl start openvpn\@<nazev serveru>.service
systemctl enable openvpn\@<nazev serveru>.service
```

Směrování

Aby se pakety přeposílaly mezi sítěmi, je třeba nastavit přeposílání mezi interfacy

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

nebo permanentně nastavit v souboru `/etc/sysctl.conf`

```
net.ipv4.ip_forward=1
```

Na routeru je třeba nastavit statickou cestu pro virtuální síť `192.168.2.0/24` na adresu serveru např. `192.168.1.1`. Jinak by router nedoručil pakety, které přichází zpět jako odpověď.

Klient

Linux

nastavení OpenVPN klienta

```
# adresa serveru
remote 192.168.1.1

# vyžaduje ověření certifikátu serveru - zabraňuje útoku men in the middle
remote-cert-tls server

# tento počítač je klient
tls-client
dev tap

# povoluje použít nastavení z push
pull

mute 10
ca ca.crt
cert klient.cert
key klient.key

comp-lzo
verb 3
```

Windows

Pro Windows je možné spustit OpenVPN GUI, které zobrazí tray ikonu. Pravým kliknutím na ni je možné měnit stav klienta.

Konfigurační soubory se umisťují do adresáře `c:\Program Files\OpenVPN\config\`. V konfiguračním souboru je nutné každé zpětné lomítko z cesty zdvojit, jinak je konfigurační soubor stejný jak v Linuxu.

Umístění certifikátu certifikační autority se napíše například takto:

```
ca "c:\\Program Files\\OpenVPN\\config\\ca.crt"
```

Směrování

Pokud chceme aby veškerý provoz šel přes VPN server je potřeba, aby bylo správně nastavené směrování. Komunikaci se serverem na adresu `192.168.1.1` musí jít přes fyzický interface a pak je

možné nastavit defaultní cestu přes virtuální síť.

Ve Windows je to možné nastavit například takto:

```
route add 192.168.1.1 mask 255.255.255.255 <původní default gateway> metric
20
route delete 0.0.0.0
route add 0.0.0.0 mask 0.0.0.0 192.168.2.1 metric 20
```