



Konfiguracja połączenia tunelowanego VPN

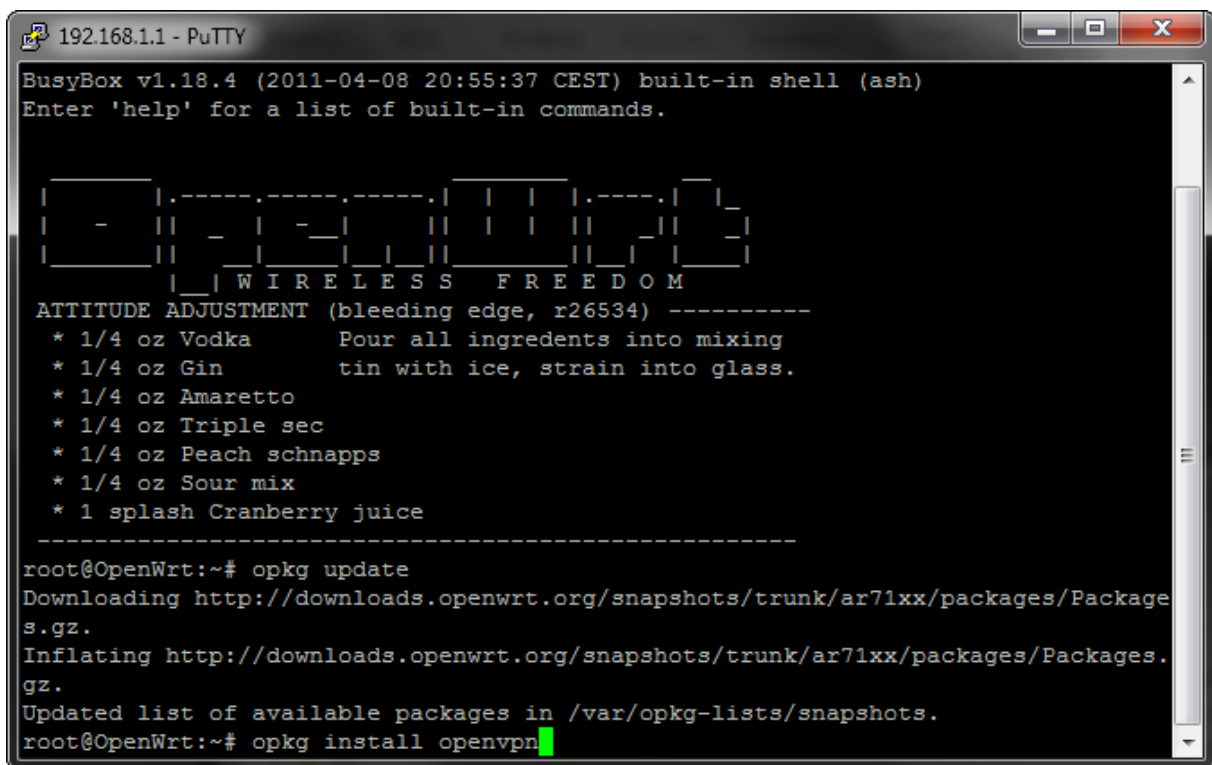
*z wykorzystaniem mechanizmów
oprogramowania OpenWrt oraz OpenVPN*

Niniejszy samouczek opisuje krok po kroku działania mające na celu uruchomienie serwera połączenia sieci wirtualnej VPN na routerze wyposażonym w alternatywne oprogramowanie OpenWrt.

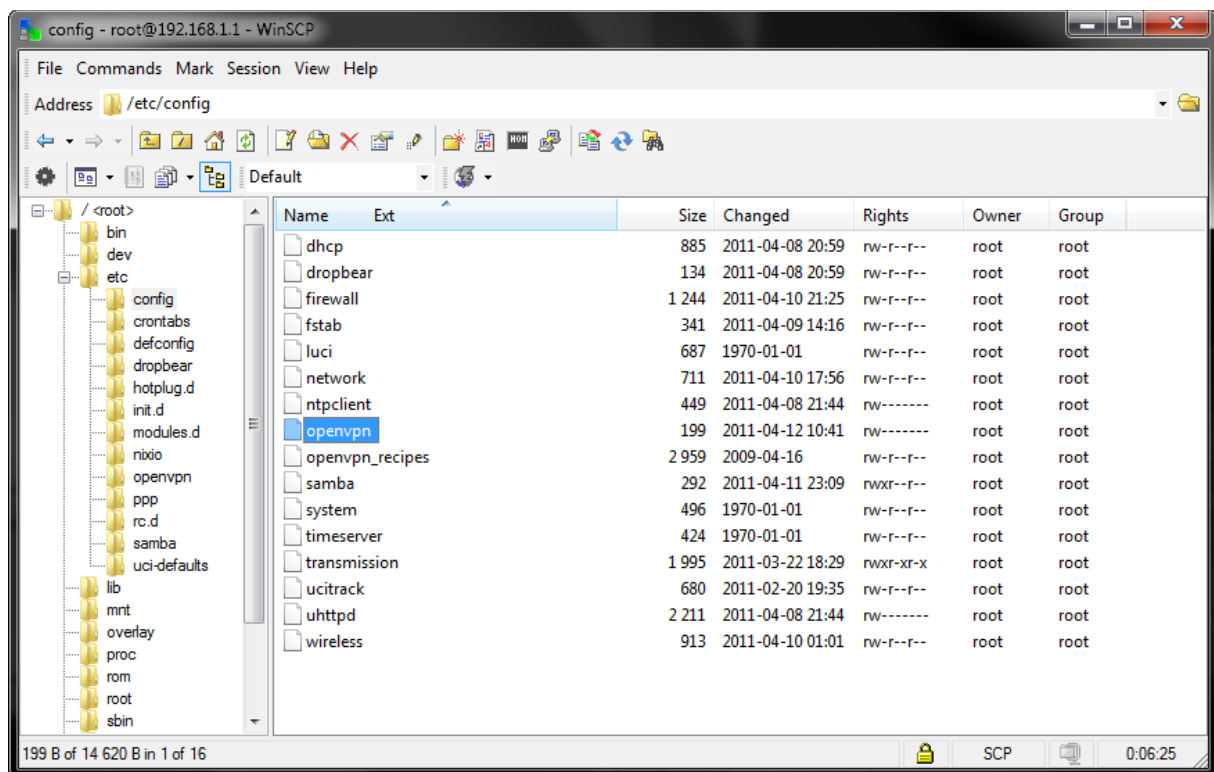
VPN (*Virtual Private Network*) Wirtualna Sieć Prywatna opisywana jako tunel, przez który płynie ruch w ramach sieci prywatnej pomiędzy klientami końcowymi za pośrednictwem sieci publicznej takiej jak Internet. Sieć ta istnieje jedynie jako struktura logiczna działająca w rzeczywistości w ramach sieci publicznej. Pomimo takiego mechanizmu działania stacje końcowe mogą korzystać z VPN dokładnie tak jak gdyby istniało pomiędzy nimi fizyczne łącze prywatne.

Potrzebne narzędzia:

- OpenVPN dla Windows
- Router wyposażony w OpenWRT
- Putty
- WinSCP

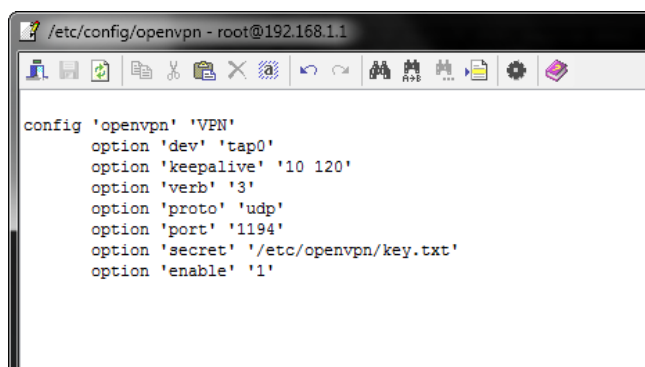


Zainstalowano WinSCP. Zalogowano z użyciem protokołu SCP oraz przeprowadzono edycję pliku „/etc/config/openvpn” ...



... poprzez utworzenie następującego wpisu, stanowiącego konfigurację serwera OpenVPN o przykładowej nazwie „VPN”:

```
config 'openvpn' 'VPN'
  option 'dev' 'tap0'
  option 'keepalive' '10 120'
  option 'verb' '3'
  option 'proto' 'udp'
  option 'port' '1194'
  option 'secret' '/etc/openvpn/key.txt'
  option 'enable' '1'
```



W katalogu „/etc” utworzono podfolder o nazwie „openvpn” i skopiowano do niego utworzony na początku plik „key.txt”.

W katalogu „/init.d”, utworzono nowy plik, dla przykładu: „openvpn_relay”.

Jego treść stanowi następujący skrypt, który przed startem właściwego programu tworzy wirtualny interfejs „tap0” oraz łączy jego pulę adresową z pulą właściwego interfejsu LAN:

```
#!/bin/sh /etc/rc.common
```

```
START=94
```

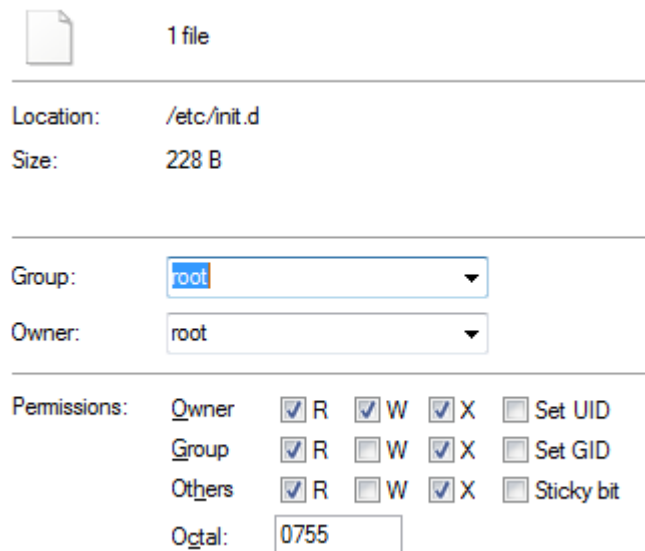
```
start() {  
    openvpn --mktun --dev tap0  
    brctl addif br-lan tap0  
    ifconfig tap0 0.0.0.0 promisc up  
}
```

```
stop() {  
    ifconfig tap0 0.0.0.0 down  
    brctl delif br-lan tap0  
    openvpn --rmtun --dev tap0  
}
```



```
/etc/init.d/openvpn_relay - root@192.168.1.1  
#!/bin/sh /etc/rc.common  
  
START=94  
  
start() {  
    openvpn --mktun --dev tap0  
    brctl addif br-lan tap0  
    ifconfig tap0 0.0.0.0 promisc up  
}  
  
stop() {  
    ifconfig tap0 0.0.0.0 down  
    brctl delif br-lan tap0  
    openvpn --rmtun --dev tap0  
}
```

Zmieniono atrybuty nowo utworzonego pliku:



1 file

Location: /etc/init.d
Size: 228 B

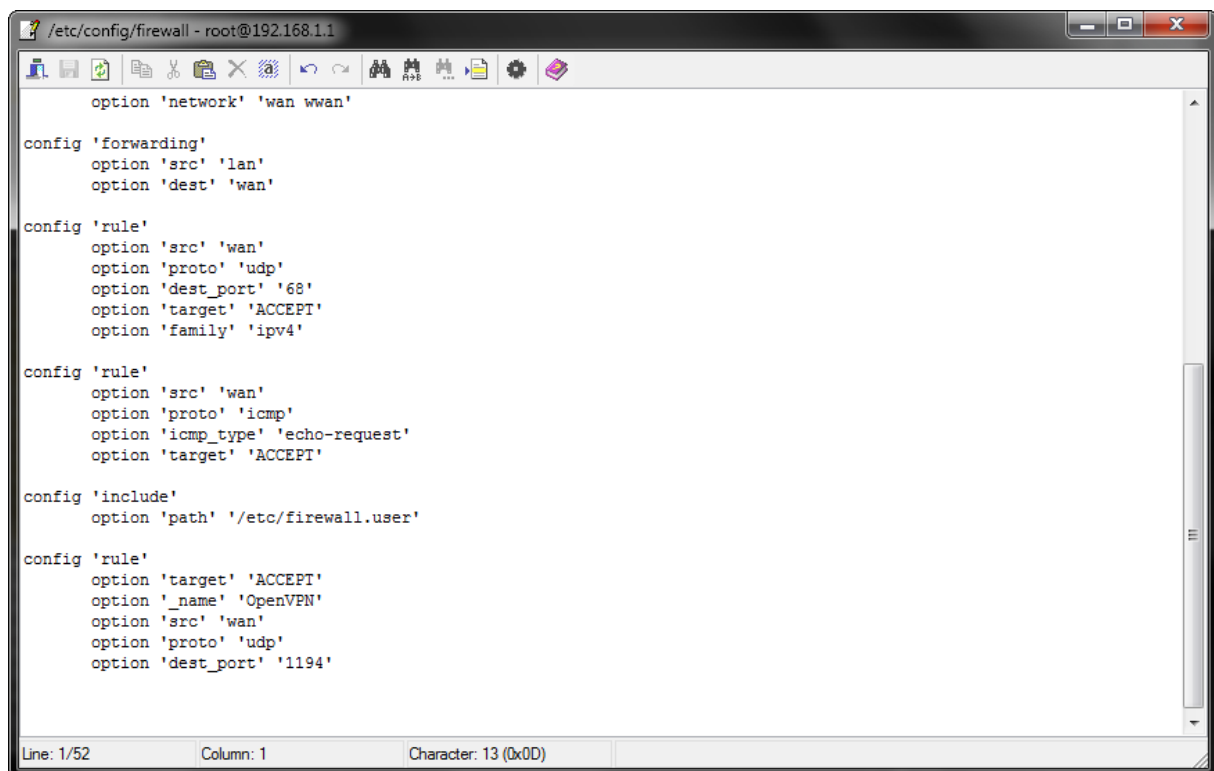
Group: root
Owner: root

Permissions: Owner ☒ R ☒ W ☒ X ☐ Set UID
Group ☒ R ☐ W ☒ X ☐ Set GID
Others ☒ R ☐ W ☒ X ☐ Sticky bit
Octal: 0755

Skonfigurowano firewall poprzez stworzenie stosownych reguł pozwalających na dostęp od strony sieci WAN.

W pliku „/etc/config/firewall” dodano następującą sekcję:

```
config 'rule'
    option 'target' 'ACCEPT'
    option '_name' 'OpenVPN'
    option 'src' 'wan'
    option 'proto' 'udp'
    option 'dest_port' '1194'
```



The screenshot shows a terminal window titled "/etc/config/firewall - root@192.168.1.1". The window displays the following configuration:

```
option 'network' 'wan wwan'

config 'forwarding'
    option 'src' 'lan'
    option 'dest' 'wan'

config 'rule'
    option 'src' 'wan'
    option 'proto' 'udp'
    option 'dest_port' '68'
    option 'target' 'ACCEPT'
    option 'family' 'ipv4'

config 'rule'
    option 'src' 'wan'
    option 'proto' 'icmp'
    option 'icmp_type' 'echo-request'
    option 'target' 'ACCEPT'

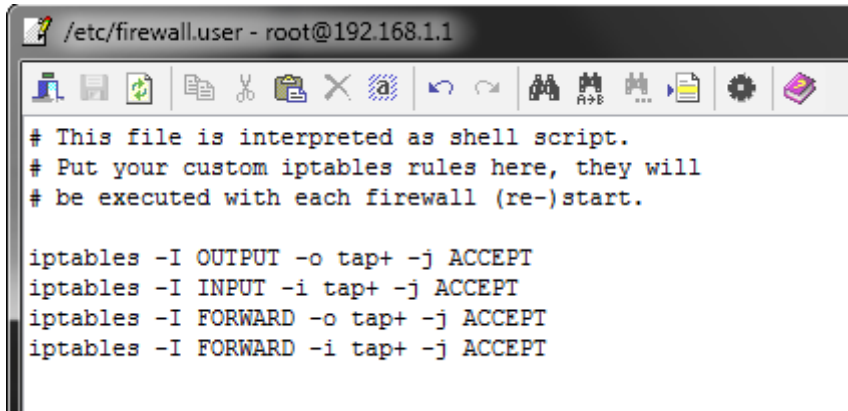
config 'include'
    option 'path' '/etc/firewall.user'

config 'rule'
    option 'target' 'ACCEPT'
    option '_name' 'OpenVPN'
    option 'src' 'wan'
    option 'proto' 'udp'
    option 'dest_port' '1194'
```

The terminal window has a standard Linux desktop environment with a taskbar at the top and a status bar at the bottom showing "Line: 1/52", "Column: 1", and "Character: 13 (0x0D)".

Zawartość pliku „/etc/firewall.user” wyedytowano poprzez dodanie wpisu mającego na celu stworzenie przekierowania do interfejsu „tap”:

```
iptables -I OUTPUT -o tap+ -j ACCEPT
iptables -I INPUT -i tap+ -j ACCEPT
iptables -I FORWARD -o tap+ -j ACCEPT
iptables -I FORWARD -i tap+ -j ACCEPT
```



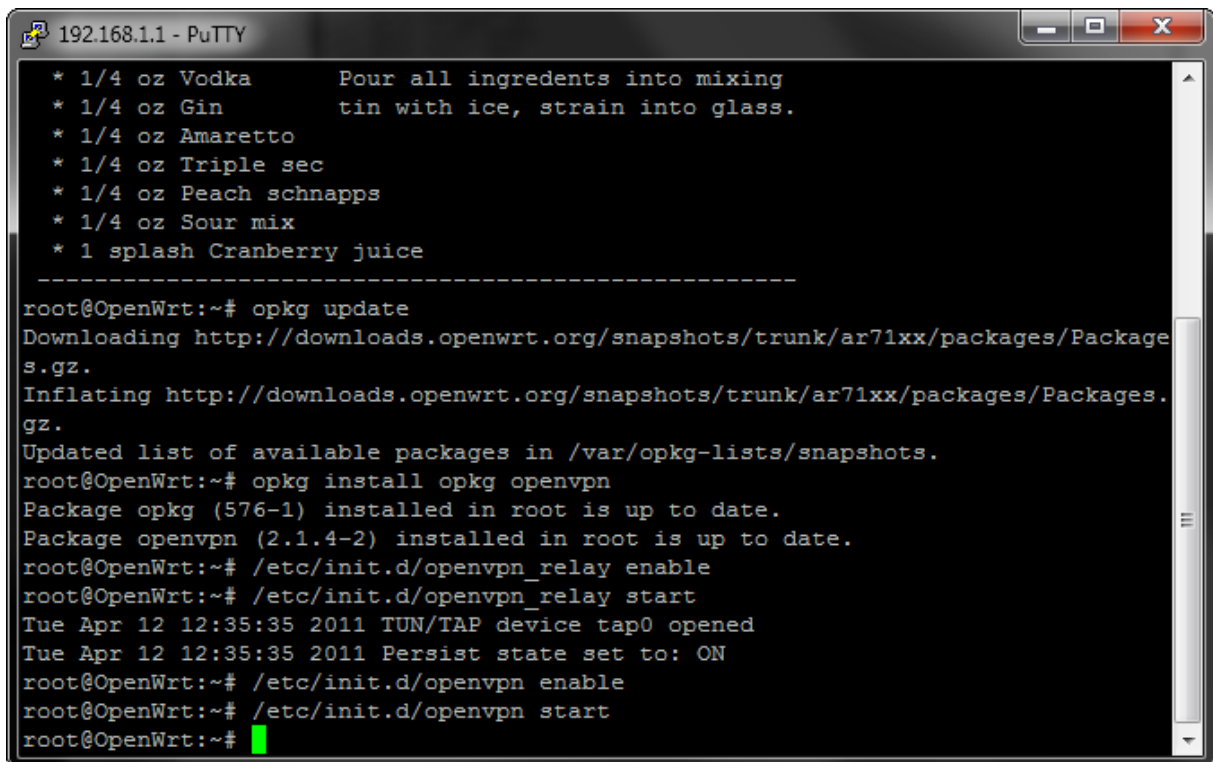
```
/etc/firewall.user - root@192.168.1.1

# This file is interpreted as shell script.
# Put your custom iptables rules here, they will
# be executed with each firewall (re-)start.

iptables -I OUTPUT -o tap+ -j ACCEPT
iptables -I INPUT -i tap+ -j ACCEPT
iptables -I FORWARD -o tap+ -j ACCEPT
iptables -I FORWARD -i tap+ -j ACCEPT
```

W konsoli wprowadzono komendy mające za zadanie dodać do autostartu nowo utworzone skrypty:

```
/etc/init.d/openvpn_relay enable
/etc/init.d/openvpn_relay start
/etc/init.d/openvpn enable
/etc/init.d/openvpn start
```



```
192.168.1.1 - PuTTY

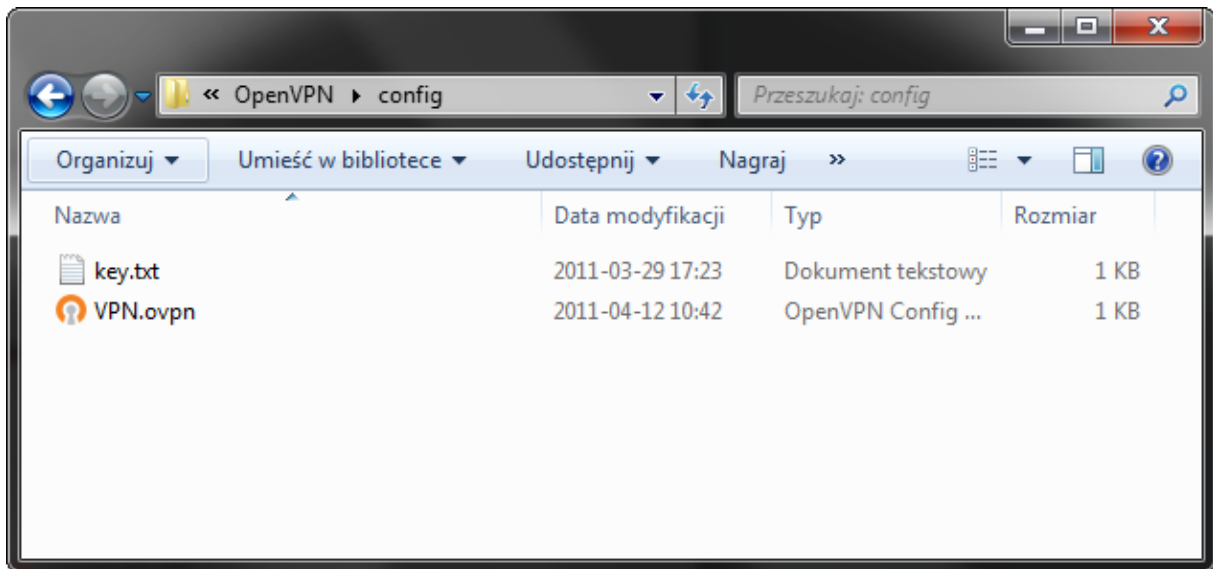
* 1/4 oz Vodka      Pour all ingredients into mixing
* 1/4 oz Gin        tin with ice, strain into glass.
* 1/4 oz Amaretto
* 1/4 oz Triple sec
* 1/4 oz Peach schnapps
* 1/4 oz Sour mix
* 1 splash Cranberry juice
-----
root@OpenWrt:~# opkg update
Downloading http://downloads.openwrt.org/snapshots/trunk/ar71xx/packages/Package
s.gz.
Inflating http://downloads.openwrt.org/snapshots/trunk/ar71xx/packages/Package.
gz.
Updated list of available packages in /var/opkg-lists/snapshots.
root@OpenWrt:~# opkg install opkg openvpn
Package opkg (576-1) installed in root is up to date.
Package openvpn (2.1.4-2) installed in root is up to date.
root@OpenWrt:~# /etc/init.d/openvpn_relay enable
root@OpenWrt:~# /etc/init.d/openvpn_relay start
Tue Apr 12 12:35:35 2011 TUN/TAP device tap0 opened
Tue Apr 12 12:35:35 2011 Persist state set to: ON
root@OpenWrt:~# /etc/init.d/openvpn enable
root@OpenWrt:~# /etc/init.d/openvpn start
root@OpenWrt:~#
```

W systemie Windows stworzono konfigurację połączenia klienta OpenVPN:

W folderze:

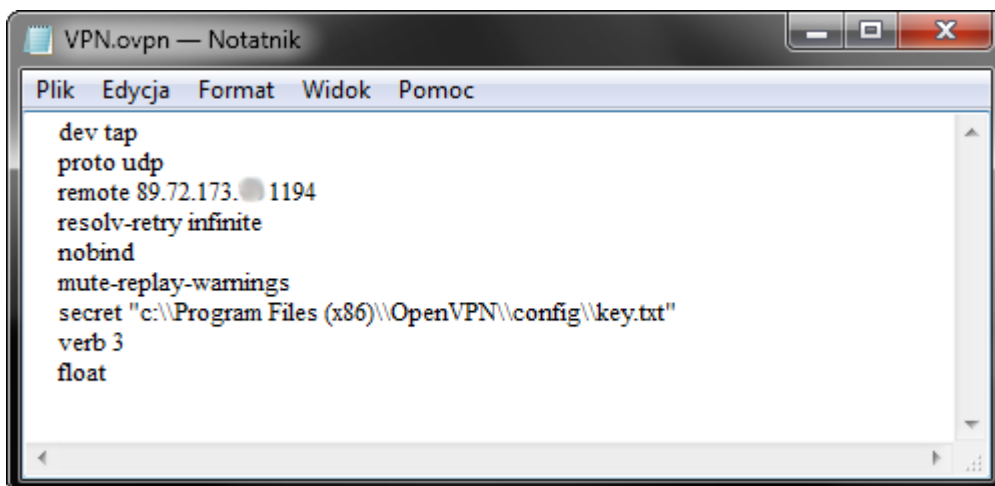
C:\Program Files\OpenVPN\config

bądź C:\Program Files (x86)\OpenVPN\config dla systemów 64 bitowych

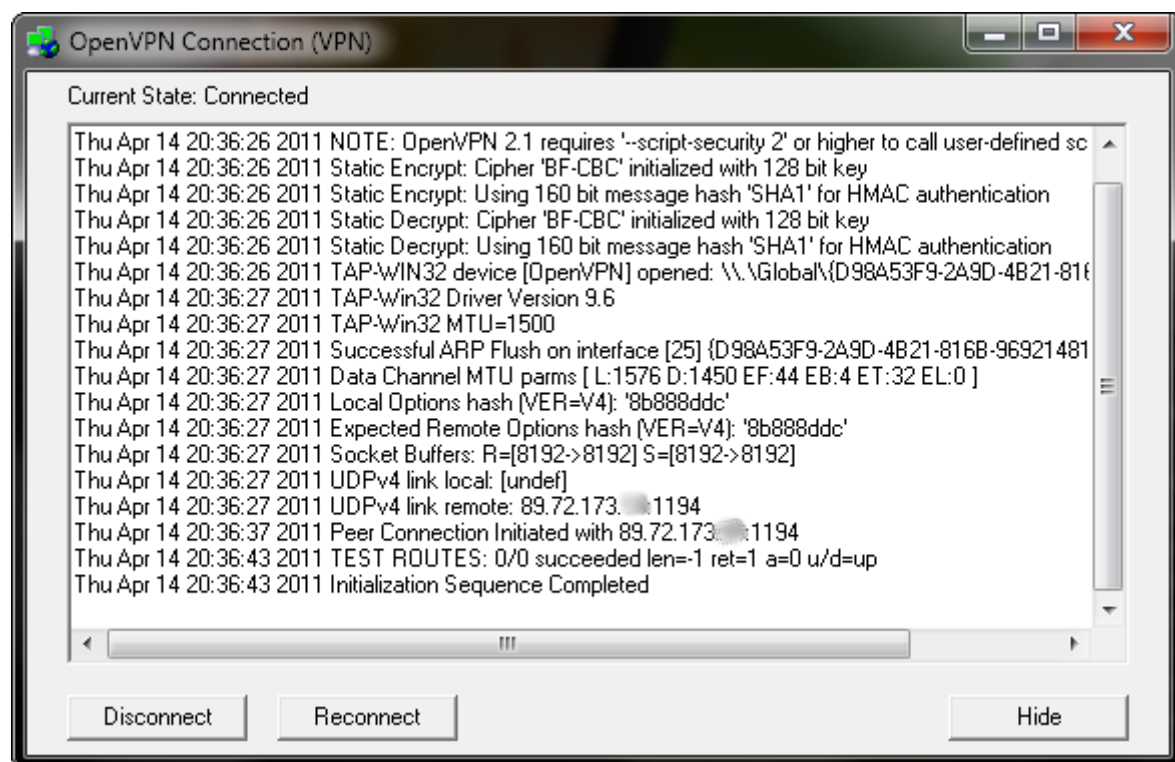


utworzono plik o nazwie przykładowej nazwie „VPN.ovpn” oraz następującej treści:

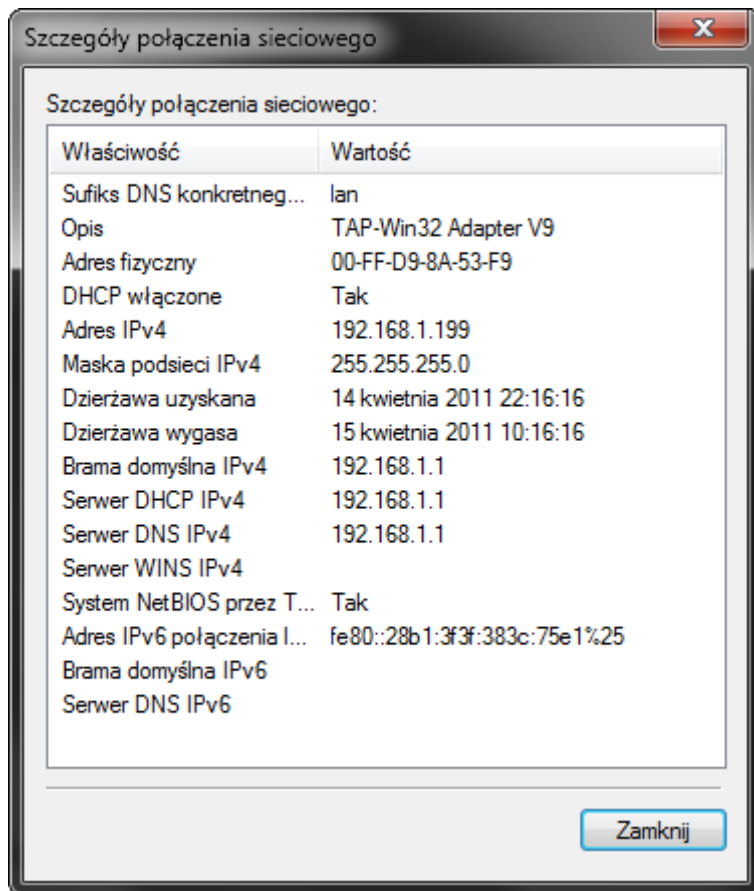
```
dev tap
proto udp
remote zewnętrzne IP 1194
resolv-retry infinite
nobind
mute-replay-warnings
secret "c:\\Program Files\\OpenVPN (x86)\\config\\key.txt"
verb 3
float
```



Uruchomiono aplikację OpenVPN GUI.



Po wykonaniu powyższych kroków wirtualnej karcie sieciowej nadany został adres IP pochodzący z lokalnej puli routera, z którym nawiązano tunelowane połączenie.



Dzięki temu połączenie ze sterownikiem zrealizowano tak jakby znajdował się on w tej samej sieci lokalnej.

