Konfiguracja połączenia tunelowanego VPN

z wykorzystaniem mechanizmów oprogramowania OpenWrt oraz OpenVPN

Niniejszy samouczek opisuje krok po kroku działania mające na calu 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
- <u>Putty</u>
- WinSCP

Zainstalowano klienta OpenVPN dla Windows, a następnie z pomocą skrótu "Generate a static OpenVPN key", wygenerowano klucz "key.txt" potrzebny do nawiązania tynelowanego połączenia.

Połączono się z konsolą OpenWrt poprzez SSH w Putty. Po zalogowaniu przeprowadzono instalację OpenVPN. Wprowadzono w tym celu następujące komendy:

opkg update

opkg install openvpn

💤 192.168.1.1 - PuTTY					
BusyBox v1.18.4 (2011-04-08 20:55:37 CEST) built-in shell (ash)	Ţ				
Enter 'help' for a list of built-in commands.					
	E				
_ WIRELESS FREEDOM					
ATTITUDE ADJUSTMENT (bleeding edge, r26534)	H				
* 1/4 oz Vodka Pour all ingredents into mixing	H				
* 1/4 oz Gin tin with ice, strain into glass.	H				
* 1/4 oz Amaretto	H				
* 1/4 oz Triple sec	H				
* 1/4 oz Peach schnapps					
* 1/4 oz Sour mix	H				
* 1 splash Cranberry juice	U				
	U				
root@OpenWrt:~# opkg update	H				
Downloading http://downloads.openwrt.org/snapshots/trunk/ar71xx/packages/Package	H				
s.gz.	H				
Inflating http://downloads.openwrt.org/snapshots/trunk/ar71xx/packages/Packages.					
gz.	U				
Updated list of available packages in /var/opkg-lists/snapshots.					
root@OpenWrt:~# opkg install openvpn					

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

🛐 config - root@192.168.1.:	1 - W	inSCP						×
File Commands Mark S	File Commands Mark Session View Help							
Address]] /etc/config	Address 📔 /etc/config 🗸 🕤							
	3	📝 🛳 🗙 💣 🧈 📑 🛤 📟 🚜 📭	A 🙀					
	E D of		u v ura					
	Dei							
⊡		Name Ext	Size	Changed	Rights	Owner	Group	
dev		📄 dhcp	885	2011-04-08 20:59	rw-rr	root	root	
etc		dropbear dropbear	134	2011-04-08 20:59	rw-rr	root	root	
config		irewall	1 244	2011-04-10 21:25	rw-rr	root	root	
crontabs		📄 fstab	341	2011-04-09 14:16	rw-rr	root	root	
defconfig		📄 luci	687	1970-01-01	rw-rr	root	root	
botolua d		network	711	2011-04-10 17:56	rw-rr	root	root	
init.d		ntpclient	449	2011-04-08 21:44	rw	root	root	
modules.d	=	openvpn	199	2011-04-12 10:41	rw	root	root	
📔 nixio		openvpn_recipes	2 959	2009-04-16	rw-rr	root	root	
openvpn		📄 samba	292	2011-04-11 23:09	rwxrr	root	root	
PPP rod		system	496	1970-01-01	rw-rr	root	root	
samba		timeserver	424	1970-01-01	rw-rr	root	root	
🔤 🚺 uci-defaults		transmission	1 995	2011-03-22 18:29	rwxr-xr-x	root	root	
lib		ucitrack	680	2011-02-20 19:35	rw-rr	root	root	
mnt _		📄 uhttpd	2 211	2011-04-08 21:44	rw	root	root	
overlay		wireless	913	2011-04-10 01:01	rw-rr	root	root	
rom								
- Toot								
🚺 sbin	Ψ.							
199 B of 14 620 B in 1 of 16					a	SCP):06:25

... 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

}

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:	<u>O</u> wner	√ R	V V	V X	Set UID
	<u>G</u> roup	✓ R	W	V X	Set GID
	Ot <u>h</u> ers	V R	W	V X	Sticky bit
	O <u>c</u> tal:	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'



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



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



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

😌 🕘 – 📕 «	OpenVPN ► config	▼ 49 PI	rzeszukaj: config	٩
Organizuj 🔻	Umieść w bibliotece 🔻	Udostępnij 👻 🛛 Nagr	aj » 📰	• 🔟 🔞
Nazwa	<u>^</u>	Data modyfikacji	Тур	Rozmiar
📄 key.txt		2011-03-29 17:23	Dokument tekstowy	1 KB
🕥 VPN.ovpn		2011-04-12 10:42	OpenVPN Config	1 KB

utworzono plik o nazwie przykładowej nazwie "VPN.opvn" 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.

GpenVPN Connection (VPN)	x
Current State: Connected	
Thu Apr 14 20:36:26 2011 NOTE: OpenVPN 2.1 requires 'script-security 2' or higher to call user-defined sc. Thu Apr 14 20:36:26 2011 Static Encrypt: Cipher 'BF-CBC' initialized with 128 bit key Thu Apr 14 20:36:26 2011 Static Encrypt: Using 160 bit message hash 'SHA1' for HMAC authentication Thu Apr 14 20:36:26 2011 Static Decrypt: Cipher 'BE-CBC' initialized with 128 bit key	
Thu Apr 14 20:36:26 2011 Static Decrypt: Using 160 bit message hash 'SHA1' for HMAC authentication Thu Apr 14 20:36:26 2011 TAP-WIN32 device [OpenVPN] opened: \\.\Global\{D98A53F9-2A9D-4B21-816 Thu Apr 14 20:36:27 2011 TAP-Win32 Driver Version 9.6 Thu Apr 14 20:36:27 2011 TAP-Win32 MTU-1500	
Thu Apr 14 20:36:27 2011 FAR Wind2 MHO (1300 Thu Apr 14 20:36:27 2011 Successful ARP Flush on interface [25] {D98A53F9-2A9D-4B21-816B-96921481 Thu Apr 14 20:36:27 2011 Data Channel MTU parms [L:1576 D:1450 EF:44 EB:4 ET:32 EL:0] Thu Apr 14 20:36:27 2011 Local Options hash (VER=V4): '8b888ddc' Thu Apr 14 20:36:27 2011 Local Options hash (VER=V4): '8b888ddc'	=
Thu Apr 14 20:36:27 2011 Expected Remote Uptions hash (VER=V4): '80888800c' Thu Apr 14 20:36:27 2011 Socket Buffers: R=[8192->8192] S=[8192->8192] Thu Apr 14 20:36:27 2011 UDPv4 link local: [undef] Thu Apr 14 20:36:27 2011 UDPv4 link remote: 89.72.173 1194	
Thu Apr 14 20:36:37 2011 Peer Connection Initiated with 89.72.173 1194 Thu Apr 14 20:36:43 2011 TEST ROUTES: 0/0 succeeded len=-1 ret=1 a=0 u/d=up Thu Apr 14 20:36:43 2011 Initialization Sequence Completed	
۲	Ť
Disconnect Reconnect Hide	

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

Szczegóły połączenia sieciowego						
Szczegóły połączenia siec	iowego:					
Właściwość	Wartość					
Sufiks DNS konkretneg Opis Adres fizyczny DHCP włączone Adres IPv4 Maska podsieci IPv4	Ian TAP-Win32 Adapter V9 00-FF-D9-8A-53-F9 Tak 192.168.1.199 255.255.255.0					
Dzierżawa uzyskana Dzierżawa wygasa Brama domyślna IPv4 Serwer DHCP IPv4 Serwer DNS IPv4 Serwer WINS IPv4	14 kwietnia 2011 22:16:16 15 kwietnia 2011 10:16:16 192.168.1.1 192.168.1.1 192.168.1.1					
System NetBIOS przez T. Adres IPv6 połączenia I Brama domyślna IPv6 Serwer DNS IPv6	Tak . fe80::28b1:3f3f:383c:75e1%25					
	Zamknij					

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

Project manager		
	L Lise PLC Address: 0 Connect Connection type C COM port C USB C Ethernet C Simulated PLC	Network selection IP address: 132.168.1.102 Imeout: 1000 ÷ Imeout: 1000 ÷ UDP port: 61682 ÷ Serial line converter One message per packet
		IP address: 87.205.148.234 imeout: 1000 ÷ ms UDP port: 61682 ÷ Internet One message per packet Repeat messages