

Point to Point Tunnelling Protocol

- prosty sposób na VPN.

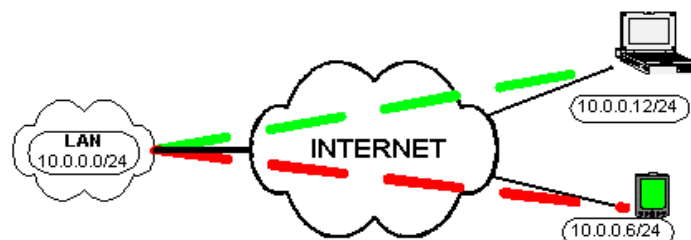
Na pewno wielu z Was konfigurowało serwery Linuxowe, które stawały się bramkami do internetu. Sprawa jest prosta: wrzucić na dysk płyty z ulubioną dystrybucją, dokonać wstępnej konfiguracji, kilka linijek ipchains czy iptables (żeby być w zgodzie z modą i ostatnimi trendami) i wszystko gra. Możemy korzystać z internetu: pani Basia zamiast pasjansa przerzuca się na GG i wszyscy są uszczęśliwieni.

Problem pojawia się, kiedy szef zaczyna często podróżować i chciałby mieć wygodny dostęp do zasobów sieci w firmie. Sam dostęp do internetu obecnie przestaje być problemem: GPRS, WiFi, powszechność internetu w hotelach itp. miejscach zapewnia swobodny dostęp do internetu. Ale jak dostać się do sieci w samej firmie?

To, że szef nauczy się korzystać z ssh czy X Window jest raczej mało prawdopodobne. Świetnym rozwiązaniem byłby ipsec, ale jest ono zarówno skomplikowane jak i dość niewygodne, zwłaszcza gdy u szefa na notebooku króluje dumnie Win98SE. Potrzebne jest rozwiązanie a – bezpieczne, b – względnie łatwo konfigurowalne, c – dostępne na możliwie jak największą ilość systemów operacyjnych.

PPTP: szczypta teorii

Okazuje się, że takie rozwiązanie istnieje. PPTP – Point to Point Tunneling Protocol jest protokołem pozwalającym na bazie protokołu IP tworzyć połączenia VPN poprzez tunelowanie protokołu PPP. Tunele te mogą przenosić protokoły takie jak IP, IPX czy NetBEUI. Rozwiązanie to stworzone zostało przez PPTP Forum przy udziale firm takich jak Ascend Communications, Microsoft Corporation, 3Com/Primary Access, ECI Telematics, i U.S. Robotics. Jest to rozwiązanie idealne dla naszego szefa. Specyfikacja protokołu jest ogólnie dostępna, dzięki czemu mogło powstać wiele oprogramowania klienckiego na różne platformy, co znacznie ułatwia stosowanie tego rozwiązania, a udział M\$ w rozwoju tego protokołu zapewnia nam istnienie klientów pod wszystkie maści M\$ Windows.



PPTP mimo swojej prostoty korzysta z kilku mechanizmów, które powodują, że jest rozwiązaniem znacznie bezpieczniejszym od zwykłego połączenia, niekorzystającego z żadnych ogólnie dostępnych metod zabezpieczeń kryptograficznych.

Połączenie PPTP może korzystać ze standardowych metod autoryzacji wykorzystywanych w ppp takich jak PAP, CHAP, czy nowszych MSCHAP. PAP wymienia hasła za pomocą czystego tekstu, więc odpada; CHAP jest pewną poprawą, choć MS-CHAPv1, MS-CHAPv2 będą najlepszym wyborem i - co ważne - dostępnym także w wersji Linuxowej klientów jak i serwerów.

Przy skonfigurowanym już procesie autentykacji dobrze byłoby zaszyfrować całą transmisję. Można to uzyskać dzięki zastosowaniu MPPE (Microsoft Point-to-Point Encryption). Żeby wykorzystać MPPE należy użyć dodatkowej łątki na kernel oraz na sam

pppd (szczegóły poniżej). Dzięki temu będzie można używać algorytmu RC4 z długością klucza 40, 56 i 128 bitów.

Dodatkowo, korzystając z MPPC (Microsoft Point-to-Point Compression), którego obsługę otrzymuje się także za pomocą wyżej wspomnianego patcha, dane transmitowane można kompresować, co pozwala na pewne zaoszczędzenie pasma.

Z takimi podstawami teoretycznymi można przejść do konkretów. Poniżej omówione będą kolejno: konfiguracja serwera pptp, konfiguracja klienta Linuxowego oraz konfiguracja klienta z systemu Windows98SE.

Konfiguracja serwera pptp

Konfigurację serwera pptp zaczyna się od przygotowania kernela. Ponieważ kernel, przynajmniej w chwili obecnej, nie zawiera obsługi MPPC i MPPE, trzeba będzie spatchować go łątką zawierającą obsługę tych dwóch rozszerzeń.

W konfiguracji kernela należy pamiętać o wyborze następujących opcji:

```
Device Drivers -> Networking Options -> "PPP support"
```

```
"Microsoft PPP compression/encryption (MPPC/MPPE)"
```

```
# tar zxvf linux-2.6.6.tar.gz
# ln -s linux-2.6.6 linux
# gunzip linux-2.6.6-mppe-mppc-1.0.patch.gz
# patch -p0 -i linux-2.6.6-mppe-mppc-1.0.patch
# cd linux
# make menuconfig (konfigurujemy kernel)
# make bzImage
```

W tej chwili pozostaje tylko dodać nowy kernel do konfiguracji Lilo/Grub i sprawdzić czy z nim można uruchomić system.

Następnie, podobnie jak kernel trzeba przygotować samo pppd do obsługi MPPE i MPPC. Tu także będzie potrzebna dodatkowa łątka.

```
# tar zxvf ppp-2.4.2.tar.gz
# gunzip ppp-2.4.2-mppe-mppc-1.0.patch.gz
# patch -p0 -i ppp-2.4.2-mppe-mppc-1.0.patch
# cd ppp-2.4.2
# ./configure
# make (Uwaga! Skrypt configure nie wykrywa np. brak libpcap-dev)
# make install
```

Mamy już gotowy nowy kernel, pppd z dodaną obsługą szyfrowania i kompresji, pozostaje skompilowanie samego serwera pptpd.

```
# tar zxvf pptpd-1.2.0-b4.tar.gz
# cd pptpd-1.2.0-b4
# ./configure
# make
# make install
```

Konfiguracja

Zacznijmy od konfiguracji pptpd, która wydaje się być najbanalniejsza. Plik `/etc/pptpd.conf` może wyglądać następująco:

```
option /etc/ppp/options-pptpd
localip 10.0.0.1
remoteip 10.0.0.10-10.0.0.30
```

co kolejno oznacza, że przy uruchamianiu połączenia pppd będzie używał pliku z opcjami /etc/ppp/options-pptpd. Druga linia to adres ip jaki zostanie przypisany interfejsowi serwera po naszej stronie. Trzecia opisuje pulę adresów, która zostanie przydzielona klientom, którzy łączą się z serwerem pptpd. Konfiguracja jak widać jest banalna.

Przy uruchamianiu pptpd na początku może się przydać opcja "-d", która powoduje logowanie większej ilości informacji na temat zestawianego połączenia. Uruchamiając "tail -f /var/log/syslog" na wolnej konsoli można obserwować proces ustanawiania połączenia.

Trochę bardziej skomplikowana będzie konfiguracja pppd dotycząca połączenia poprzez PPTP. Całość tej konfiguracji będzie zawierać się w pliku /etc/ppp/options-pptpd, tak jak to już wcześniej określono.

```
auth
require-mschap-v2
mppe required
mppe no40
mppe no56
```

Linia pierwsza wymusza autoryzację, kolejna powoduje, że pppd będzie żądał autoryzacji przy pomocy MSCHAPv2. Dodatkowo trzeba wymusić szyfrowanie, najlepiej najwyższe dostępne, czyli 128-bitowe.

Dodatkowym plikiem, który będzie potrzebny przy autoryzacji ppp jest "/etc/ppp/chap-secrets". Warto zwrócić uwagę na prawa dostępu do tego pliku, ponieważ będzie on zawierał hasła przechowywane otwartym tekstem.

#Klient	Serwer	Hasło	Adres IP
szef	*	tajne_haslo	*
domena\\szef	*	tajne_haslo	*

Warto pamiętać, że niektóre z systemów M\$ autoryzując się dodają do nazwy użytkownika nazwę domeny.

I to by było na tyle konfiguracji po stronie serwera.

Konfiguracja klienta Linux

Klienta PPTP pod Linuxa można pobrać ze strony <http://pptpclient.sourceforge.net/>. Jest to mały programik, który wykorzystuje się następnie podczas połączeń za pomocą pppd z serwerem pptpd.

Instalacja klienta PPTP.

```
# tar zxvf pptp-1.4.0.tar.gz
# cd pptp-1.4.0
# make
# make install
```

Program ten nie zawiera skryptu configure, więc ten krok został pominięty celowo;).

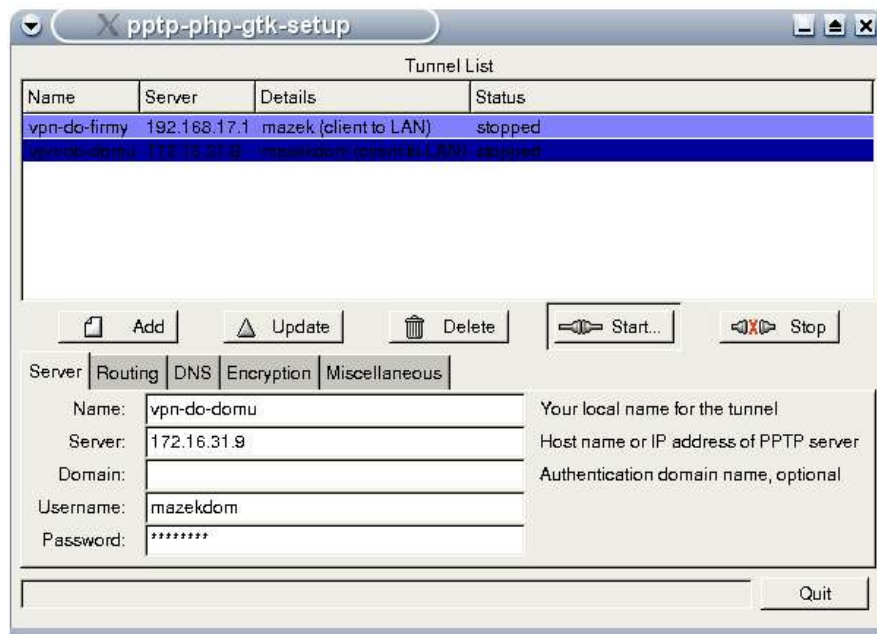
Warto w tym miejscu zwrócić uwagę na to, że w katalogu `./Reference` znajdują się zebrane RFC i inne dokumenty dotyczące PPTP.

Poniżej przykładowe połączenie wykonane z Linuksa do serwera pptp znajdującego się pod adresem 10.0.0.5.

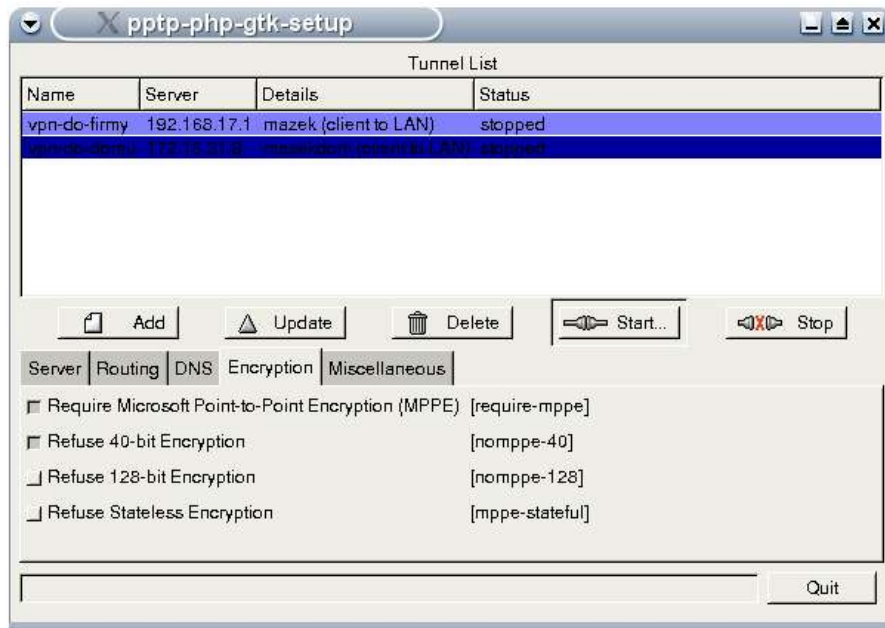
```
pppd noauth nobsdcomp nodeflate mppe-128 mppe-stateless \  
name domena\\\\\\user remotename PPTP require-chapms-v2 pty \  
"pptp 10.0.0.5 --nolaunchpppd"
```

Konfiguracja klienta Linuxowego jest jak widać bardzo prosta. Należy tylko pamiętać, że tak jak w przypadku konfiguracji serwera tak i przy konfiguracji klienta trzeba użyć wspomnianej wcześniej łatki aby pppd mogło korzystać z MPPE i MPPC.

Aby uprościć sprawę konfiguracji i ustanawiania połączeń, można wykorzystać nakładkę pod Xy: <http://quozl.netrek.org/pptp/php-gtk>. Dzięki temu tandemowi stają się one zupełnie proste.



Jest to pierwsze okno po uruchomieniu pptp-php-gtk pozwalające na podanie adresu serwera pptp oraz nazwy użytkownika i hasła. W polu "Name" należy używać krótkiego opisu, który będzie później wykorzystany jako nazwa pliku i połączenia. Wszelkie polskie znaki i spacje odpadają.



W zakładce "Encryption" można wymusić stosowanie szyfrowania oraz wykorzystanie odpowiednio mocnej kryptografii.

Całość jest bardzo prosta i wygodna w korzystaniu. Jedyna rzecz, na którą trzeba zwrócić tutaj dodatkowa uwagę, to albo ustawienie praw do zapisu tej aplikacji tak aby mogła ona zapisywać swoje konfiguracje do katalogu "/etc/pptp-php-gtk" oraz plików "/etc/ppp/peers", "/etc/ppp/chap-secrets" i "/etc/ppp/pap-secrets", lub uruchamianie jej z prawami użytkownika root.

Konfiguracja klienta Windows

Tu sprawa jest równie prosta, dla systemów Windows95, Windows98 i Windows98SE należy pobrać rozszerzenia dostępne na stronie Microsoft, pozwalające na korzystanie z połączenie pptp:

Win95:

<http://download.microsoft.com/download/win95/Update/17648/W95/EN-US/dun14-95.exe>

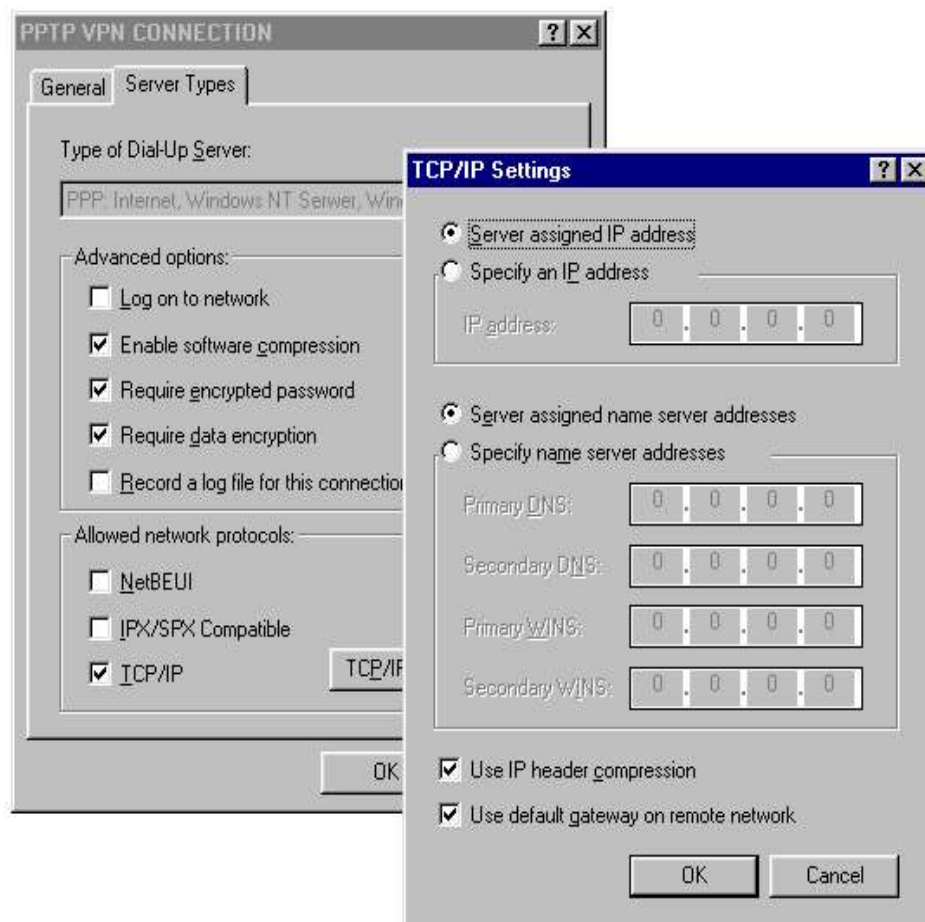
Win98:

<http://download.microsoft.com/download/win98/Update/17648/W98/EN-US/dun14-98.exe>

Win98SE:

<http://download.microsoft.com/download/win98SE/Update/17648/W98/EN-US/dun14-SE.exe>

Przy założeniu, że DialupNetworking jest zainstalowany w systemie w nim tworzy się nowe połączenia, a podczas wybierania typu połączenia "Select a device" wybiera się Microsoft VPN Adapter". Następnie podaje się adres serwera pptp i zamyka kreatora. We właściwościach nowo utworzonego połączenia należy zaznaczyć "Require encrypted password" i "Require data encryption" aby korzystać z dobrodziejstw szyfrowania. I to w zasadzie wszystko co jest potrzebne do połączenia się z serwerem pptp.



Konfiguracja połączenie w M\$ Win98SE.

W przypadku W2k i WinXP nie potrzeba instalować żadnych dodatkowych rozszerzeń.

Co zamiast pptp

pptp **nie** jest protokołem bezpiecznym, co bardzo dokładnie zostało opisane na stronie Bruce Schneiera <http://www.schneier.com/pptp-faq.html>. Wskazał on na bardzo wiele wad, które ten protokół posiada, zwłaszcza w swojej implementacji w systemach MS Windows. Jeśli istnieje taka możliwość, warto rozważyć korzystanie z protokołu IPSec, jeśli jednak jesteśmy zdani na pptp, warto mieć świadomość wszelkich wad jakie ze sobą niesie oraz wykorzystywać maksymalnie możliwości zabezpieczania go. Można przyjąć następujący podział: kiedy potrzebujemy komunikacji pomiędzy dwoma sieciami poprzez szyfrowany tunel VPN – używajmy IPSec. Jeśli potrzebujemy **bardzo** bezpiecznego połączenia pomiędzy określoną siecią a przemieszczającymi się klientami – używajmy IPSec. Jeśli potrzebujemy prostego rozwiązania aby korzystać z zasobów sieci będąc w danym momencie poza nią - PPTP jest tym czego szukamy.

Jest to świetne rozwiązanie w sytuacji gdy potrzeba w prosty i względnie bezpieczny sposób dostać się z domu do firmowej sieci LAN.

Linki:

1. Patche MPPE i MPPC na pppd i kernel: <http://free.polbox.com/h/hs001/>
2. Serwer PPTP: <http://www.poptop.org/>
3. Klient PPTP: <http://pptpclient.sourceforge.net/>
4. Nakładka GTK na klienta PPTP: <http://quozl.netrek.org/pptp/php-gtk>
5. Repozytorium pppd: <http://www.samba.org/ppp/>
6. Kernel Linuxowy: <http://www.kernel.org/> :)

Dokumentacja:

1. Świetna analiza protokołu PPTP: <http://www.schneier.com/pptp.html>
2. Trochę mniej krytyczne informacje na temat ten sam temat ze strony M\$ <http://www.microsoft.com/ntserver/ProductInfo/faqs/PPTPfaq.asp>