Tworzenie sieci VPN w środowisku Linux i Windows

1 Wprowadzenie

W wielu sytuacjach w których mamy do czynienia z rozbudowaną architekturą sieciową zależy nam aby całe środowisko rozproszone(np. oddziały firmy w różnych lokalizacjach) było jak najbardziej spójne. Dotyczy to również adresacji IP. Technologia wirtualnych sieci prywatnych(*ang. Virtual Private Network*) pozwala na rozwiązanie takich problemów. Dzięki utworzeniu sieci VPN można zbudować logiczną sieć komputerową, która będzie łączyć całe rozproszone środowisko ukrywając sieci łączące odległe od siebie lokalizacje i tym samym uprości wymianę danych między nimi.
Budując sieć VPN tworzymy logiczne tunele między wyznaczonymi lokalizacjami. W ten sposób technologia VPN tworzy iluzję w której odległe od siebie lokalizacje są fizycznie bezpośrednio połączone. Ta cecha sieci VPN wpływa na uproszenie sposobu wymiany ruchu między tymi lokalizacjami.

W obecnej chwili myśląc o technologii VPN oraz jej możliwościach oprócz wyżej wymienionej cechy bierzemy pod uwagę stopień bezpieczeństwa jaki zapewnia nam połączenie VPN. Tworzenie sieci VPN bez wsparcia dla bezpieczeństwa przysyłanych informacji w obecnej chwili jest rzadko stosowane z uwagi na wzrost poziomu poufności przesyłanych danych. Wielu producentów sprzętu sieciowego w swojej ofercie handlowej oferuje różnego typu rozwiązania do kompleksowej budowy sieci VPN. Rozwiązania te cechują się różnym stopniem bezpieczeństwa, skalowalności oraz łatwości wdrożenia. Przeważająca część tych rozwiązań VPN posiada wsparcie dla kryptograficznych mechanizmów ochrony poufności i/lub integralności przesyłanych danych.
Najprostsze rozwiązania mogą w ogóle nie wspierać ochrony poufności przesyłanych danych, bardziej zaawansowane mogą korzystać z mechanizmu współdzielonego klucza i algorytmów kryptografii symetrycznej do ochrony poufności, najbardziej zaawansowane rozwiązania korzystają z mechanizmów kryptografii klucza publicznego, certyfikatów cyfrowych.

Słowa kluczowe: ssl, vpn, ipsec, certyfikat cyfrowy, openvpn, openswan, tun/tap

2 Zastosowania technologii VPN

Głównym zastosowaniem technologii VPN jest tworzenie logicznych kanałów między zdalnymi lokalizacjami. Wiele dużych firm telekomunikacyjnych oferuje swoim klientom możliwość zestawiania połączeń VPN między zdalnymi lokalizacjami zamiast dzierżawy fizycznych łącz z uwagi na oszczędności dla klienta oraz większą elastyczności w zarządzaniu takimi połączeniami dla operatora telekomunikacyjnego. W rozwiązaniach typu SOHO(*ang. Small Office Home Office*) bardziej rozbudowane rozwiązania również wspierają tworzenie sieci VPN. Przydaje się to w sytuacjach, gdy pracownik pracuje w domu i potrzebuje połączenia do sieci firmowej. Inna możliwość to użycie odpowiedniego oprogramowania klienckiego na komputerze pracownika pracującego poza siedzibą firmy. Takie oprogramowanie zestawia połączenie VPN między komputerem pracownika a urządzeniem dostępowym w siedzibie firmy.

Oprócz tradycyjnych rozwiązań VPN wspierających protokół IPsec istnieje druga, również popularna grupa rozwiązań opartych o wykorzystanie protokołu SSL jako mechanizmu do budowy bezpiecznych kanałów wymiany danych. Sieci tworzone z użyciem mechanizmu SSL VPN określane są również jako „sieci bez klienta”(*ang. clientless*) z uwagi, że inaczej niż

ma to miejsce w klasycznych sieciach VPN opartych o IPsec, nie jest potrzebne dedykowane oprogramowanie klienckie dla klienta takiej sieci, wystarczy przeglądarka stron www wspierająca protokół SSL. Klient posiadający przeglądarkę wspierającą protokół SSL łączy się z serwerem dostępowym i po ustanowieniu połączenia SSL, po przez przeglądarkę uzyskuje dostęp do wewnętrznych zasobów sieci VPN. Istnieją również inne rozwiązania SSL, które posiadają dedykowane oprogramowanie do zestawiania połączeń SSL VPN. Dzięki takiemu podejściu możliwości połączeń SSL VPN zbliżają się do klasycznych sieci VPN opartych o protokół IPsec i pozwalają przesyłać ruch sieciowy dowolnej aplikacji opakowując go protokołem SSL. Takim rozwiązaniem jest program OpenVPN.

3 Oprogramowanie OpenVPN

Program OpenVPN jest narzędziem służącym do tworzenia szyfrowanego połączenia VPN w sieci TCP/IP. Instalacja tego programu nie wymaga ingerencji w jądro systemu operacyjnego Linux przez co rozwiązanie to jest proste i łatwe w uruchomieniu. Tunel jest tworzony z wykorzystaniem wirtualnych interfejsów sieciowych TUN/TAP. Utworzenie tunelu sprowadza się do utworzenia pliku konfiguracyjnego opisującego parametry połączenia i uruchomienie programu `openvpn` z tym plikiem jako parametrem. Z drugiej strony tunelu również wykorzystujemy ten sam program ale w roli klienta i przyłączamy się do poprzednio uruchomionego serwera. Bardzo dużą zaletą programu OpenVPN jest możliwość tworzenia szyfrowanych tuneli z hostami korzystającymi z systemu Windows ,co w niektórych sytuacjach może okazać się kluczowe przy wyborze darmowego oprogramowania do tworzenia sieci VPN. OpenVPN pozwala tworzyć szyfrowane połączenia w oparciu o dwie metody:

- „Pre-shared key" mechanizm w którym strony połączenia współdzielą między sobą tajny klucz służący do uwierzytelniania stron i szyfrowania komunikacji. OpenVPN wykorzystuje kryptograficzny algorytm blowfish z 128 bitowym kluczem w trybie CBC(*ang. Cipher Block Chaining*)
- Certyfikaty cyfrowe SSL, OpenVPN wykorzystuje bibliotekę OpenSSL do tworzenia certyfikatów cyfrowych SSL(tryb SSL/TLS)

3.1 Podstawy

Wygenerowanie współdzielonego klucza i zapisanie go do pliku następuje po wykonaniu komendy:

```
openvpn –genkey –secret shared.key
```

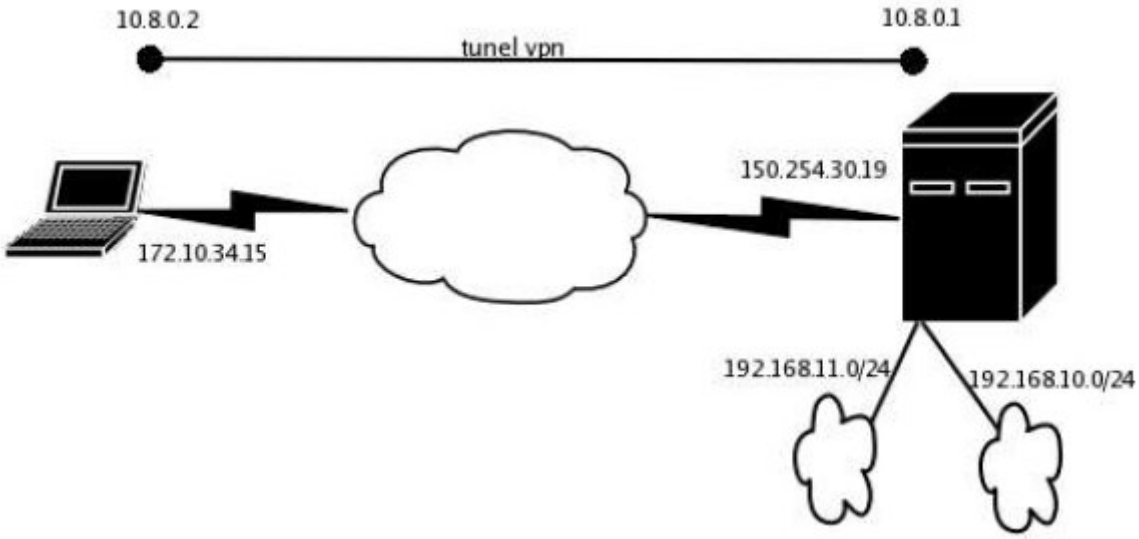
W pliku shared.key w bieżącym katalogu zostanie zapisany klucz, który posłuży do utworzenia bezpiecznego połączenia VPN.

Program OpenVPN nie posiada wyróżnionej części klienta i serwera. Dla obu stron połączenia wykorzystywany jest ten sam program zapisany w wykonywalnym pliku o nazwie `openvpn`. Odpowiednia opcja w pliku konfiguracyjnym wymusza działanie w trybie klienta lub serwera. Poniżej zaprezentowano komendę uruchamiającą program OpenVPN:

```
openvpn –config /etc/openvpn/static.conf
```

Program OpenVPN pozwala aby opcje konfiguracyjne zostały podane jako parametry podczas wywołania pliku wykonywanego openvpn jednak zapisanie opcji w pliku wydaje się bardziej wygodne.

Poniżej zaprezentowano przykładową architekturę połączenia VPN:



Rysunek 1 OpenVPN. Przykładowa architektura połączenia VPN.

Nawiązane połączenie VPN między komputerem przenośnym o serwerem powinno utworzyć podsieć 10.8.0.0/24 i po przez to połączenie komputer przenośny powinien uzyskać dostęp do dwóch podsieci po stronie serwera tj. 192.168.11.0/24 i 192.168.10.0/24.

3.2 Połączenie VPN Linux-Linux z wykorzystaniem mechanizmu współdzielonego klucza

Uwierzytelniania i szyfrowanie następuje z wykorzystaniem mechanizmu współdzielonego klucza. Serwer na którym jest uruchomiony program OpenVPN jest dostępny pod adresem ip 150.254.30.19 i nasłuchuje na porcie tcp 1194. Koniec połączenia VPN do strony serwera ma adres ip 10.8.0.1 a od strony klienta: 10.8.0.2.

3.2.1 Plik konfiguracyjny dla strony serwera

```
dev tun
ifconfig 10.8.0.1 10.8.0.2
secret /etc/openvpn/static.key
proto tcp-serwer
daemon
verb 4
log-append /var/log/openvpn.og
keepalive 10 900
inactive 3600
comp-lzo
```

Opcja `tcp-server` wymusza użycie protokołu TCP warstwy czwartej do utworzenia logicznego kanału danych oraz określa bieżącą stronę połączenia jako serwerową czyli oczekującą na połączenia. OpenVPN pozwala również na utworzenie połączenia VPN z użyciem protokołu UDP.

Opcja `ifconfig` definiuje oba końce połączenia VPN.

Opcja `secret` wskazuje na plik z współdzielonym kluczem.

Opis wszystkich parametrów programu OpenVPN znajduje się na stronie domowej projektu OpenVPN oraz w podręczniku systemowym do programu openvpn(*man openvpn*).

3.2.2 Plik konfiguracyjny dla strony klienta

```
dev tun
remote 150.254.30.19 1194
proto tcp-client
ifconfig 10.8.0.2 10.8.0.1
secret /home/piotr/openvpn.conf
keepalive 10 60
route 192.168.10.0 255.255.255.0
route 192.168.11.0 255.255.255.0
comp-lzo
```

Opcja `remote` określa adres i numer portu pod jakim serwer OpenVPN jest dostępny.
Opcja `ifconfig` definiuje oba końce połączenia VPN. Należy zwrócić uwagę na kolejność parametrów polecenie `ifconfig`.

Opis wszystkich parametrów programu OpenVPN znajduje się na stronie domowej projektu OpenVPN oraz w podręczniku systemowym do programu openvpn(`man openvpn`).

3.3 Połączenie VPN Linux-Linux z wykorzystaniem mechanizmu certyfikatów cyfrowych

Program OpenVPN pozwala wykorzystać infrastrukturę klucza publicznego do tworzenia bezpiecznych kanałów wymiany danych. Certyfikaty SSL pozwalają wynegocjować parametry połączenia VPN oraz uzgodnić jednorazowy klucz sesyjny służący do szyfrowania komunikacji między stronami połączenia. Użycie certyfikatów SSL to najbardziej zaawansowana i najbezpieczniejsza konfiguracja programu OpenVPN.

3.3.1 Plik konfiguracyjny dla strony serwera

```
dev tun
proto tcp-server
ifconfig 10.8.0.1 10.8.0.2
keepalive 10 60
verb 4
deamon
comp-lzo
log-append /var/log/openvpn.log
persist-tun
persist-local-ip
persist-remote-ip
persist-key
#############SSL#####
tls-server
tls-remote nazwa_strony_klienta
ca cacert.pem
dh dh1024.pem
cert newcert.pem
key newreq.pem
cipher aes-256-cbc
#############SSL#####
```

Opcja `tls-remote` wymaga podania nazwy `Common name` z certyfikatu klienta.
Opcja `dh` wskazuje na plik z dużą liczbą pierwszą.

Opis wszystkich parametrów programu OpenVPN znajduje się na stronie domowej projektu OpenVPN oraz w podręczniku systemowym do programu openvpn(*man openvpn*).

3.3.2 Plik konfiguracyjny dla strony klienta

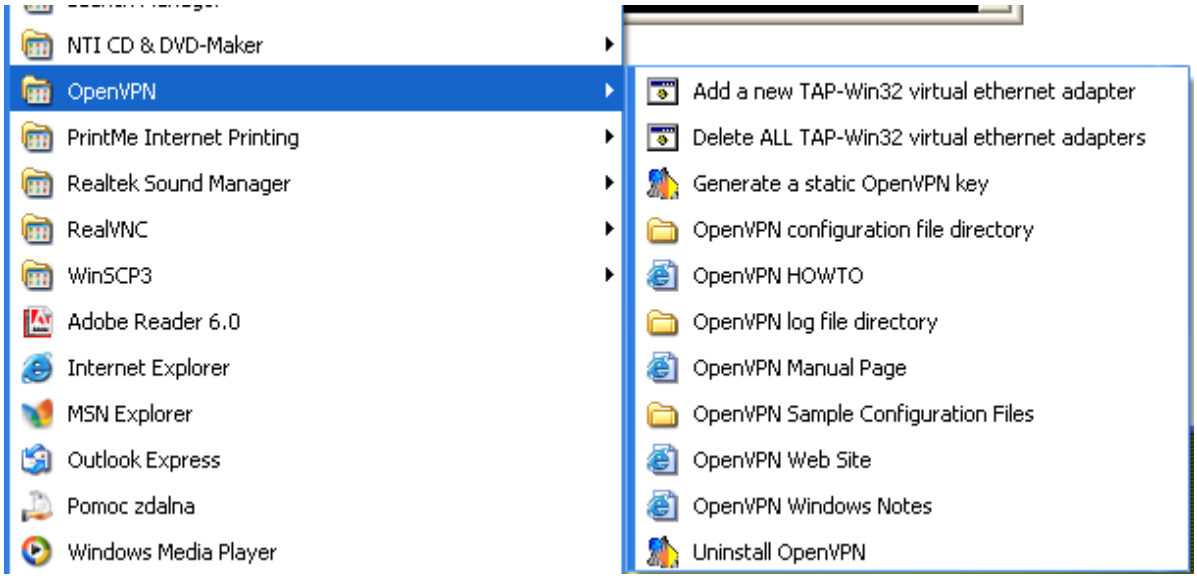
```
dev tun
proto tcp-client
comp-lzo
verb 4
log-append /var/log/openvpn.log
persist-tun
persist-local-ip
persist-remote-ip
persist-key
ifconfig 10.8.0.2 10.8.0.1
route 192.168.10.0 255.255.255.0
route 192.168.11.0 255.255.255.0
########SSL#####
tls-client
tls-remote nazwa_strony_serwera
ca cacert.pem
cert newcert.pem
key newreq.pem
cipher aes-256-cbc
########SSL#####
```

3.4 Połączenie VPN Linux-Windows z wykorzystaniem mechanizmu współdzielonego klucza

OpenVPN jest narzędziem, które pozwala na tworzenie tuneli nie tylko miedzy hostami działającymi pod kontrolą systemu Linux ale również pod Windows. Program openvpn posiada specjalną wersję pod Windows, która pozwala na uruchomienie tunelu np. między Linuxem a systemem Windows. Poniżej pokazano jak można utworzyć tunel VPN z użyciem mechanizmu współdzielonego klucza. Konfiguracja z użyciem certyfikatów SSL jest również możliwa.

3.4.1 OpenVPN w menu START

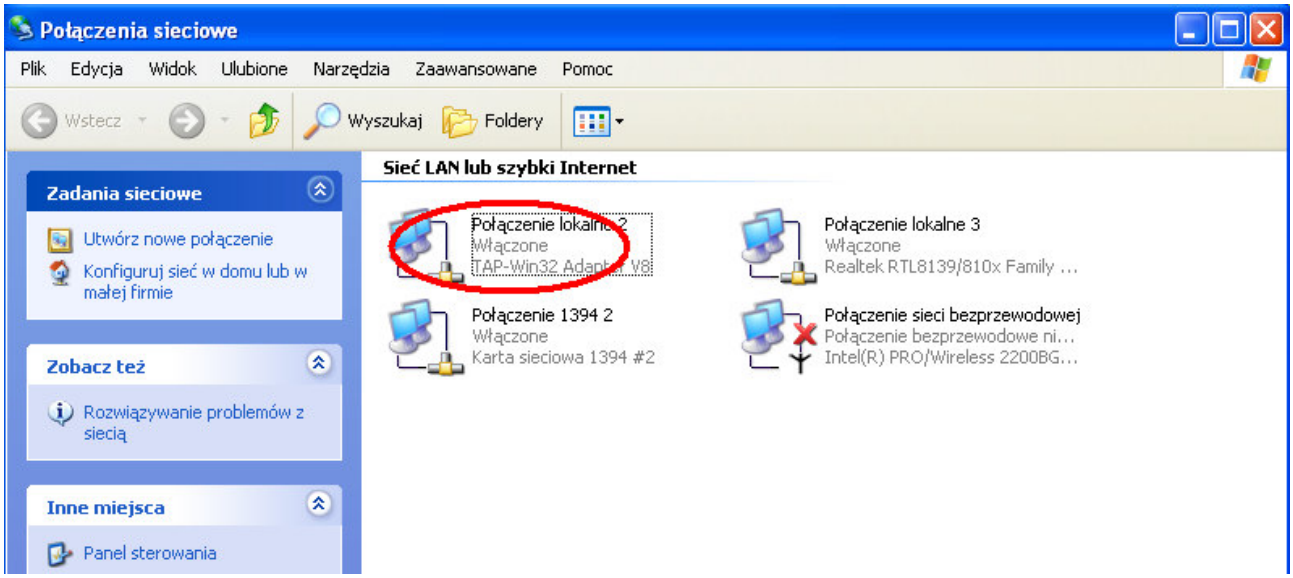
Po zainstalowaniu pod Windows OpenVPN posiada osobne podmenu.



Rysunek 2 OpenVPN. Menu programu OpenVPN pod Windows.

3.4.2 Nowe urządzenie sieciowe

Niezbędnym elementem zarówno w systemie Linux jak w Windows jest wirtualne urządzenie sieciowe wykorzystywane przez OpenVPN do komunikacji sieciowej. Instalując OpenVPN pod Windows oprócz samego programu, instalowany jest wirtualny interfejs sieciowy *TAP-win32 Adapter*.

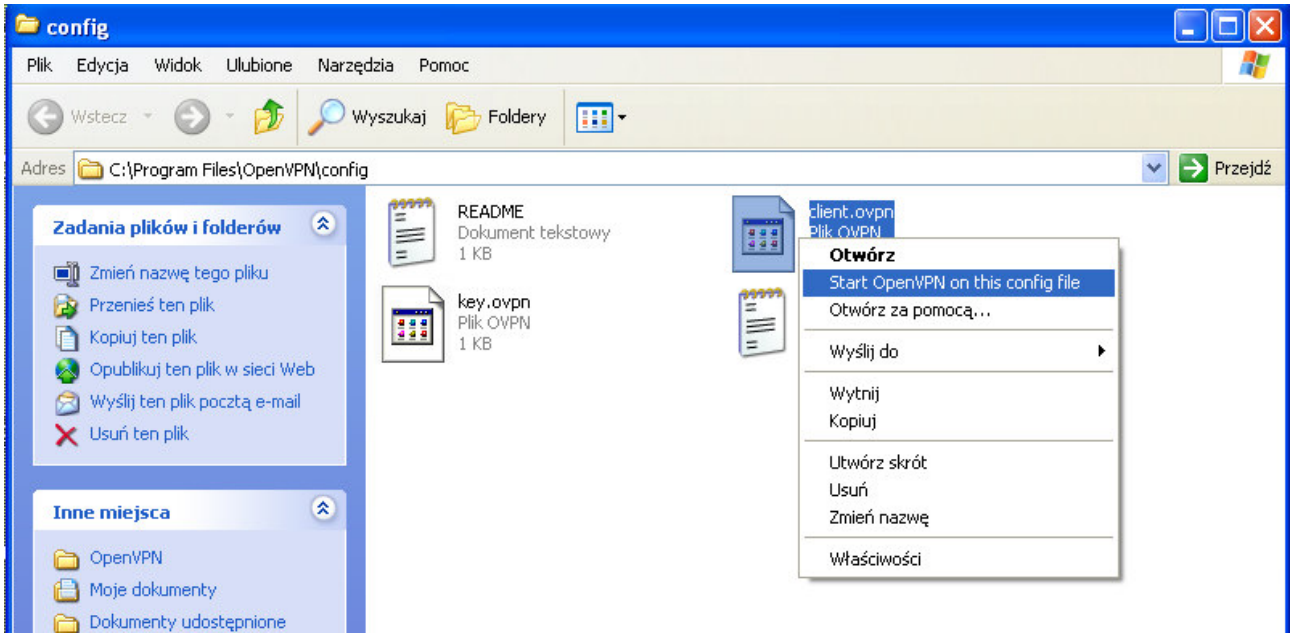


Rysunek 3 OpenVPN. Nowe urządzenie sieciowe wykorzystywane do zestawiania połączeń VPN.

3.4.3 Uruchomienie OpenVPN pod Windows

Wystarczy wybrać z menu kontekstowego odpowiednią opcję. Należy zwrócić uwagę na kilka rzeczy:

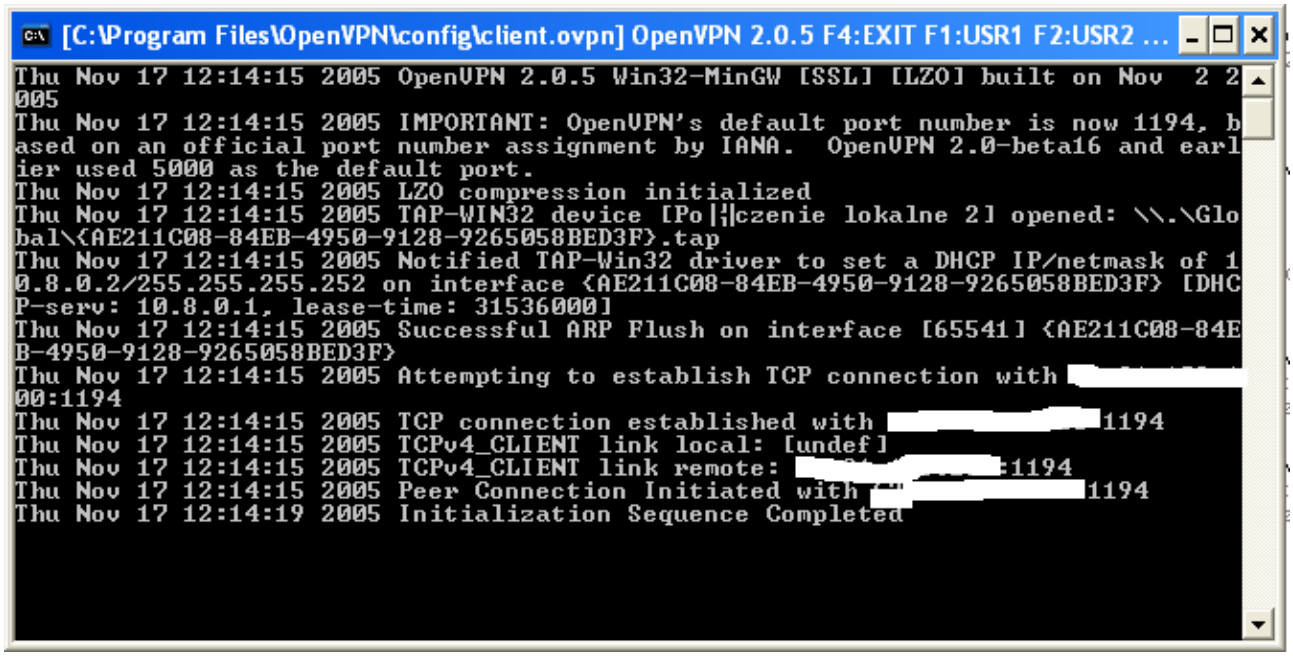
- plik konfiguracyjny musi mieć rozszerzenie `.ovpn`
- plik konfiguracyjny musi znajdować się w katalogu `config` programu openvpn (patrz ramka z adresem folderu)



Rysunek 4 OpenVPN. Uruchomienie programu OpenVPN.

3.4.4 Konsola tekstowa

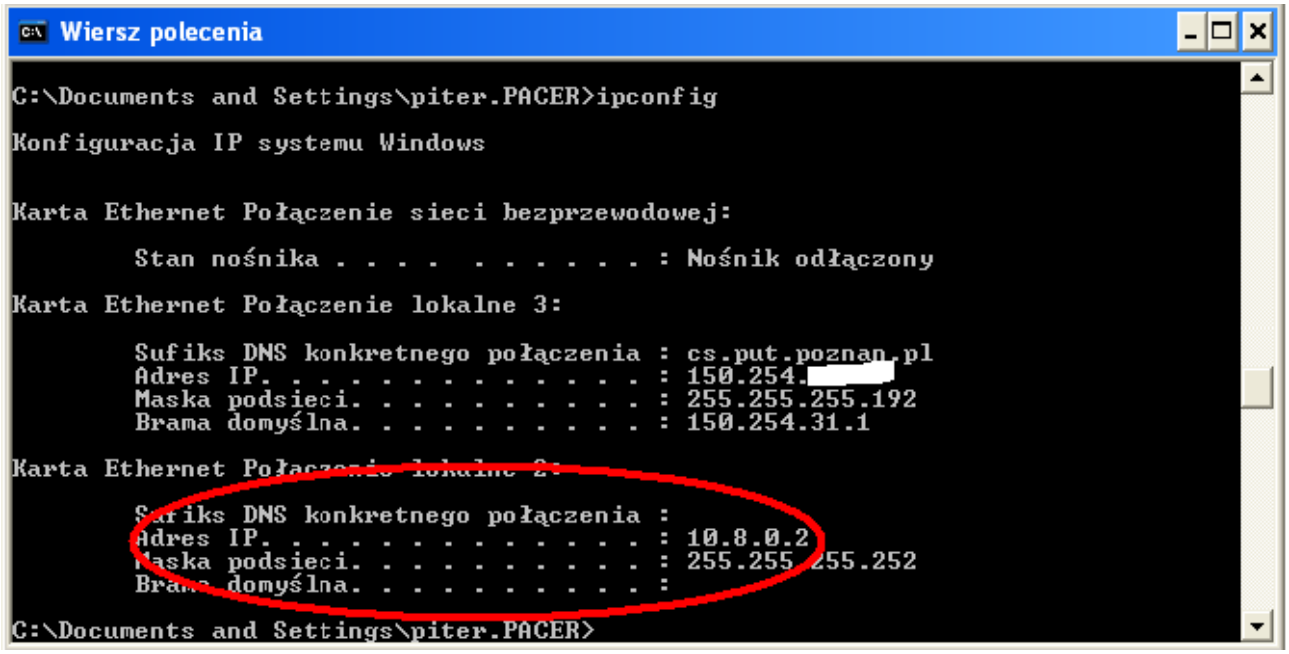
Wybranie opcji uruchomienia OpenVPN z menu kontekstowego spowoduje otwarcie okna konsoli tekstowej w której można obserwować postęp w negocjacji połączenia. Jeżeli zdecydujemy się aby logowanie odbywało się do pliku, na konsoli nie zobaczymy logów. Utworzenie tunelu następuje po zakończeniu procedury negocjacji parametrów połączenia(patrz ostatnia linia na zrzucie ekranowym poniżej).



Rysunek 5 OpenVPN. Konsola tekstowa programu OpenVPN.

3.4.5 Nowe połączenie VPN

Po zakończeniu procedury tworzenia tunelu wykonując polecenie systemowe `ipconfig` obserwujemy obecność nowego interfejsu sieciowego o adresie ip identycznym jak adres końca połączenia VPN dla danej strony.



Rysunek 6 OpenVPN. Zestawione połączenie VPN.

3.5 Podsumowanie możliwości programu OpenVPN

Program OpenVPN jest ciekawą alternatywą dla klasycznych rozwiązań VPN opartych o protokół IPsec. Konfiguracja połączeń VPN jest bardzo prosta i zrozumiała nawet dla użytkownika nieobeznanego z technologią sieci VPN. Bardzo dużą zaletą OpenVPN jest korzystanie z biblioteki OpenSSL, co sprawia, że rozwiązanie OpenVPN może być uznawane za mechanizm tworzenie sieci VPN o wysokim stopniu bezpieczeństwa. Można również zestawiać połączenia VPN z użyciem mechanizmu współdzielonego klucza dla mniej zaawansowanych przypadków użycia. Warto również zwrócić uwagę na możliwość łatwego zestawiania połączeń w środowisku mieszanym w którym występują systemy Linux i Windows. Wadą programu OpenVPN jest jego skalowalność. Chcąc zestawić więcej połączeń VPN z danego hosta należy uruchomić kolejną instancję programu OpenVPN. Wadą ta jest częściowo rekompensowana przez bardzo przejrzystą strukturę pliku konfiguracyjnego.

4 Protokół IPsec

Protokół sieciowy IP w wersji 4 nie posiada mechanizmów służących do sprawdzania integralności przesyłanych danych oraz zapewniania poufności tych danych. Słabości protokołu IP pod tym względem ma usprawnić protokół IPsec. W przypadku protokołu IP w wersji 4 IPsec jest opcjonalnym dodatkiem. W protokole IP w wersji 6 funkcjonalność IPsec jest wymagana.

4.1 Podstawy

Głównymi zdaniami protokołu IPsec jest ochrona integralności przesyłanych danych i zapewnienie poufności. Mechanizmy odpowiedzialne za te funkcjonalności są konfigurowalne i

w razie potrzeby można je wyłączyć w zależności od aktualnych potrzeb. Kolejna cecha protokołu IPsec to jego przezroczystość dla protokołów warstw wyższych. Protokół IPsec działa na poziomie warstwy 3 modelu sieciowego ISO/OSI i dlatego możliwe jest przysyłanie za jego pomocą ruchu sieciowego niezależnie od aplikacji generującej ten ruch oraz, co równie ważne obecność IPsec jest nie widoczna dla tych aplikacji. Ma to bardzo duże znaczenie praktyczne, gdyż nie ma potrzeby modyfikacji aplikacji sieciowych już napisanych a to w istotny sposób obniża koszty wdrożenia protokołu IPsec.

Protokół IPsec w ogólności składa się z kilku elementów. Są to protokoły AH i ESP oraz mechanizm negocjacji parametrów połączenia IKE. Protokół AH(*ang. Authentication Header*) jest odpowiedzialny za ochronę integralności przesyłanych danych jak i nagłówka samego pakietu. Jako mechanizmy zapewniające integralność stosowane są funkcje tworzące skrót kryptograficzny np. MD5, SHA1, RIPEMD-160. Protokół ESP(*ang. Encapsulation Security Payload*) jest odpowiedzialny za zapewnienie poufności przesyłanych danych. Wykorzystywane algorytmy do szyfrowania to DES, 3DES, Blowfish, Rijndael/AES.

IPsec może działać w dwóch trybach: transportowym i tunelowym. W trybie transportowym między nagłówek IP a nagłówek warstwy wyższej umieszczany jest nagłówek protokołu IPsec np. ESP. W ten sposób chroniona jest zawartość pakietu ale podsłuchujący wiem kto z kim wymienia dane, co nie koniecznie może być jawne. W trybie tunelowym cały pakiet danych wymienianych między stronami jest ukrywany przez zaszyfrowanie i opakowany przez protokół ESP. Ten tryb jest rozwiązaniem bardziej bezpiecznym i przydaje się w konfiguracji określanej NET-to-NET w której pomiędzy dedykowanymi hostami(*SA, ang. Security Gateway*) zestawione jest połączenie VPN trybie tunelowym a za hostami znajdują się wewnętrzne sieci. W taki skonfigurowanym połączeniu VPN podsłuchujący nie ma możliwości podejrzenia kto z kim wymienia dane ponieważ ruch sieciowy wymieniany jest tylko między hostami SA.

Protokół IKE(*ang. Internet Key Exchange*) jest odpowiedzialny za automatyczną negocjację parametrów połączenia VPN. IKE składa się z dwóch części:

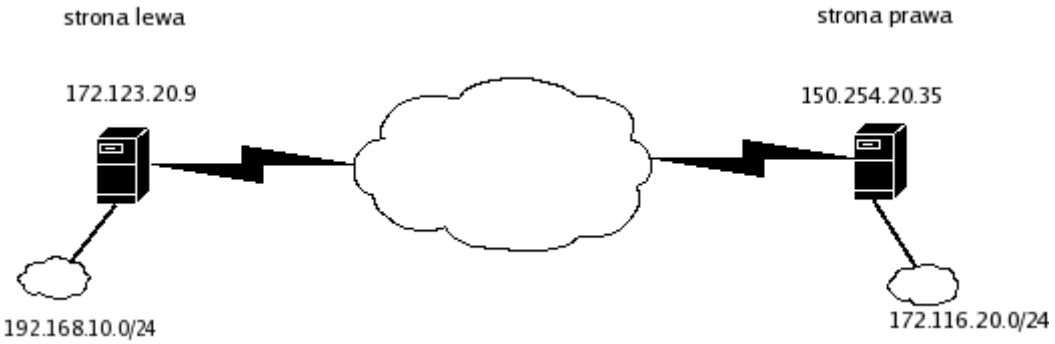
- ISAKMP(*ang. Internet Security Association and Key Management Protocol*) protokół negocjacji parametrów połączenia
- Oakley protokół wymiany kluczy za pomocą algorytmu Diffie-Hellmana

4.2 Budowanie sieci VPN z użyciem oprogramowania Openswan

Program Openswan jest ogólnie dostępną implementacją IPsec pod systemy Linux. Openswan pozwala wykorzystać możliwości IPsec i zestawiać połączenia nie tylko między systemami Linux ale również z systemami Windows oraz routerami czy bramami VPN. Openswan występuje jako rozszerzenie dla jądra systemu Linux. Można go pobrać ze strony projektu w postaci źródeł jak i postaci przygotowanego zestawu np. rpm. W niektórych dystrybucjach Linuxa np. SuSE Openswan jest dostarczany w formie rpm a jądro wspiera IPsec.

4.3 Połączenie VPN Linux-linux z użyciem kluczy RSA

Jedną z najprostszych konfiguracji połączenia VPN z użyciem Openswan jest zestawienie połączenia z użyciem kluczy RSA. Pliki konfiguracyjne dla obu stron połączenia VPN są bardzo podobne.
Poniżej zaprezentowano przykładową architekturę sieci w której między dwoma serwerami zostanie utworzone połączenie VPN.



Rysunek 7 Openswan. Przykładowa architektura połączenia VPN.

4.3.1 Generacja kluczy RSA

```
ipsec newhostkey --output /etc/ipsec.secrets --hostname
nazwa_domenowa_hosta
```

4.3.2 Edycja pliku konfiguracyjnego ipsec.conf

Aby zdefiniować połączenie VPN w pliku ipsec.conf należy dopisać nową sekcję, która będzie definiować parametry połączenia. Poniżej zaprezentowano przykładowy plik konfiguracyjny dla rysunku powyżej.

```
conn nazwa_polaczenia
      left=172.123.20.9
      leftsubnet=192.168.10.0/24
      leftnexthop=%defaultroute
      leftrsasigkey=...
      right=150.254.20.35
      rightsubnet=172.116.20.0/24
      rightnexthop=%defaultroute
      rightnexthop=...
      authby=rsasig
      auto=start
```

Parametry `leftrsasigkey` i `rightrsasigkey` wymagają jawnego podania wartości kluczy. Aby to zrobić ja jednym systemie będącym lewą stroną połączenia należy wydać polecenie:

```
ipsec showhostkey --left
```

Na hoście będącym prawą stroną połączenia należy wydać polecenie:

```
ipsec showhostkey --right
```

Wykonanie poleceń spowoduje wypisanie na okno terminala odpowiednich kluczy. Należy je skopiować pod podane wyżej parametry(`leftrsasigkey` i `rightrsasigkey`). Po zakończeniu tej procedury obie strony połączenia powinny dysponować identycznym plikiem `ipsec.conf`. Kwestia, która strona jest lewą lub prawą jest umowna.

4.3.3 Utworzenie połączenia VPN

Z uwagi na wartość ostatniego parametru(`auto=start`) ustanowienie połączenia VPN nastąpi w chwili uruchomienie programu ipsec.
W systemach SuSE będzie to polecenie `/etc/init.d/ipsec start` i `ipsec auto –up nazwa_polaczenia`

4.4 Podsumowanie możliwości programu Openswan

Program Openswan jest rozwiązaniem bardziej zaawansowanym niż OpenVPN. Pozwala tworzyć bardziej zaawansowane konfiguracje. Z uwagi na wykorzystywany protokół IPsec Openswan może służyć jako mechanizm do zestawiania połączeń z sieciowymi urządzeniami wspierającymi tworzenie sieci VPN takimi jak routery czy bramy VPN. Openswan wspiera również wykorzystanie certyfikatów cyfrowych.

5 Zadania

- Zestawienie połączenia VPN z użyciem programu OpenVPN z wykorzystaniem mechanizmu współdzielonego klucza.
- Zestawienie połączenia VPN z użyciem programu OpenVPN z wykorzystaniem mechanizmu certyfikatów cyfrowych.
- Zestawienie połączenia VPN z użyciem programu Openswan z wykorzystaniem kluczy RSA.

6 Problemy do dyskusji

- Jakie zagrożenia dla bezpieczeństwa niesie za sobą mechanizm współdzielonego klucza?
- Czy używanie certyfikatów SSL jest bezpieczniejsze niż mechanizm współdzielonego klucza i dlaczego?
- Czy można zestawiać połączenia VPN bez szyfrowania komunikacji?
- W jakich sytuacjach rozwiązania SSL VPN są wyborem bardziej optymalnym niż rozwiązania oparte o IPsec?

7 Bibliografia

- strona domowa projektu OpenVPN http://www.openvpn.net
- Artykuł „VPN na miarę" Maciej Koziński http://www.pckurier.pl/archiwum/art0.asp?ID=6130
- Techniczny biuletyn zabezpieczeń IT firmy Clico „Rozważania nt. Wariantów wdrożenia sieci IPsec VPN i SSL VPN" http://www.clico.pl/b/t/no_9/vpn_ipsec_ssl_fin.pdf

Dodatek A

Generacja certyfikatów SSL.
Wykorzystany zostanie skrypt `CA.sh` znajdujący się w podkatalogu misc/ biblioteki OpenSSL.

1. Utworzenie certyfikatu dla centrum certyfikacji(*ang. CA*)

```
CA.sh -newca
```

2. Utworzenie pliku z kluczem prywatnym wraz z prośbą o wydanie certyfikatu dla danej strony połączenia VPN.

```
CA.sh -newreq
```

Należy podać wszystkie dane niezbędne do utworzenia certyfikatu. Należy zwrócić uwagę na pole `Common Name`. Tekst wpisany w tym polu będzie potrzeby jako parametr dla pola `tls-remote` drugiej strony połączenia.

3. Wydanie certyfikatu.

```
CA.sh -sign
```

Po wykonaniu wszystkich kroków zostaną utworzone następujące pliki:

- `cacert.pem` – plik z certyfikatem dla centrum certyfikacji(krok nr 1)
- `newreq.pem` – plik z prośbą o wydanie certyfikatu oraz kluczem prywatnym jednej ze stron połączenia(krok nr 2)
- `newcert.pem` – plik z certyfikatem i z kluczem publicznym dla danej strony połączenia(krok 3)

Krok nr 1 należy wykonać tylko raz. Kroki nr 2 i 3 należy wykonać dwa razy po jednym dla każdej strony połączenia VPN.