

# 

# Wydział Studiów Strategicznych i Technicznych

## **Kierunek: Informatyka, rok II, semestr III (2021/2022)**

**LABORATORIUM NR 2**

**PODSTAWY KRYPTOGRAFII**

Prowadzący: dr Piotr Dobosz

**Zespół laboratoryjny:**

Magdalena Szafrańska, nr albumu: 18345

# Spis treści

[**Cel ćwiczenia**](#_kkyfeo6kh4ft) **2**

[**Informacje wstępne**](#_kbmvft4bsc5q) **2**

[VPN](#_5hacspidj40v) 2

[Tunel](#_r0fee214ga4g) 3

[OpenVPN](#_93xwpgjph5em) 4

[PPTP](#_bmknuvhoubc3) 5

[**Użyte narzędzia i aplikacje**](#_frp4q2hkkf0) **5**

[**Przebieg ćwiczenia**](#_mb3jmynjuap9) **6**

[CZĘŚĆ I: Badanie ruchu w niezabezpieczonym tunelu](#_3qvgbpp83s7n) 6

[Konfiguracja VirtualBox (z Ubuntu)](#_13o7z1ycxq5x) 6

[Instalacja serwera PPTP (Ubuntu)](#_8cd4yip5ob4h) 6

[Konfiguracja klienta PPTP (Windows 10)](#_ogbdmeps0kx8) 10

[Analiza Wiresharka](#_f8a7vbvnilni) 12

[CZĘŚĆ II: Badanie ruchu w zabezpieczonym tunelu](#_wwsy0bot9qf9) 13

[Instalacja serwera OpenVPN (Ubuntu)](#_s2kaz0l9q88u) 13

[Konfiguracja klienta OpenVPN (Windows 10)](#_bpz6927a00xl) 17

[**Wnioski**](#_15zbcjfsfs4s) **19**

# 

# Cel ćwiczenia

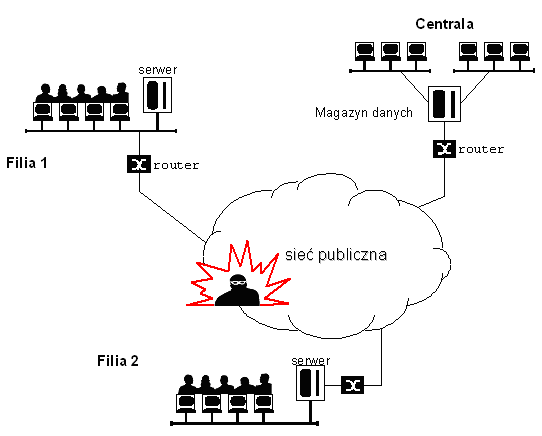
Celem laboratorium jest przetestowanie działania tuneli sieciowych z wykorzystaniem technologii VPN. Sprawdzenie które z połączeń zdalnych do wirtualnej sieci prywatnej jest najbezpieczniejsze i która technologia daje najlepszą ochronę przy jednoczesnej prostocie konfiguracji.

# Informacje wstępne

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 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 uproszczenie sposobu wymiany ruchu między tymi lokalizacjami.

### VPN

Virtual Private Network, w skrócie VPN to tunel wirtualny. Jest to kanał komunikacyjny chroniony przed niepowołanym dostępem (odczytem i modyfikacją) poprzez zastosowanie kryptografii. Tunel wirtualny VPN umożliwia chronioną transmisję w obszarze publicznej sieci rozległej, np. w celu realizacji bezpiecznego połączenia pomiędzy różnymi jednostkami, najczęściej geograficznie odległymi.



*Rys. Schemat sieci publicznej analizowany jako scenariusz zagrożeń*

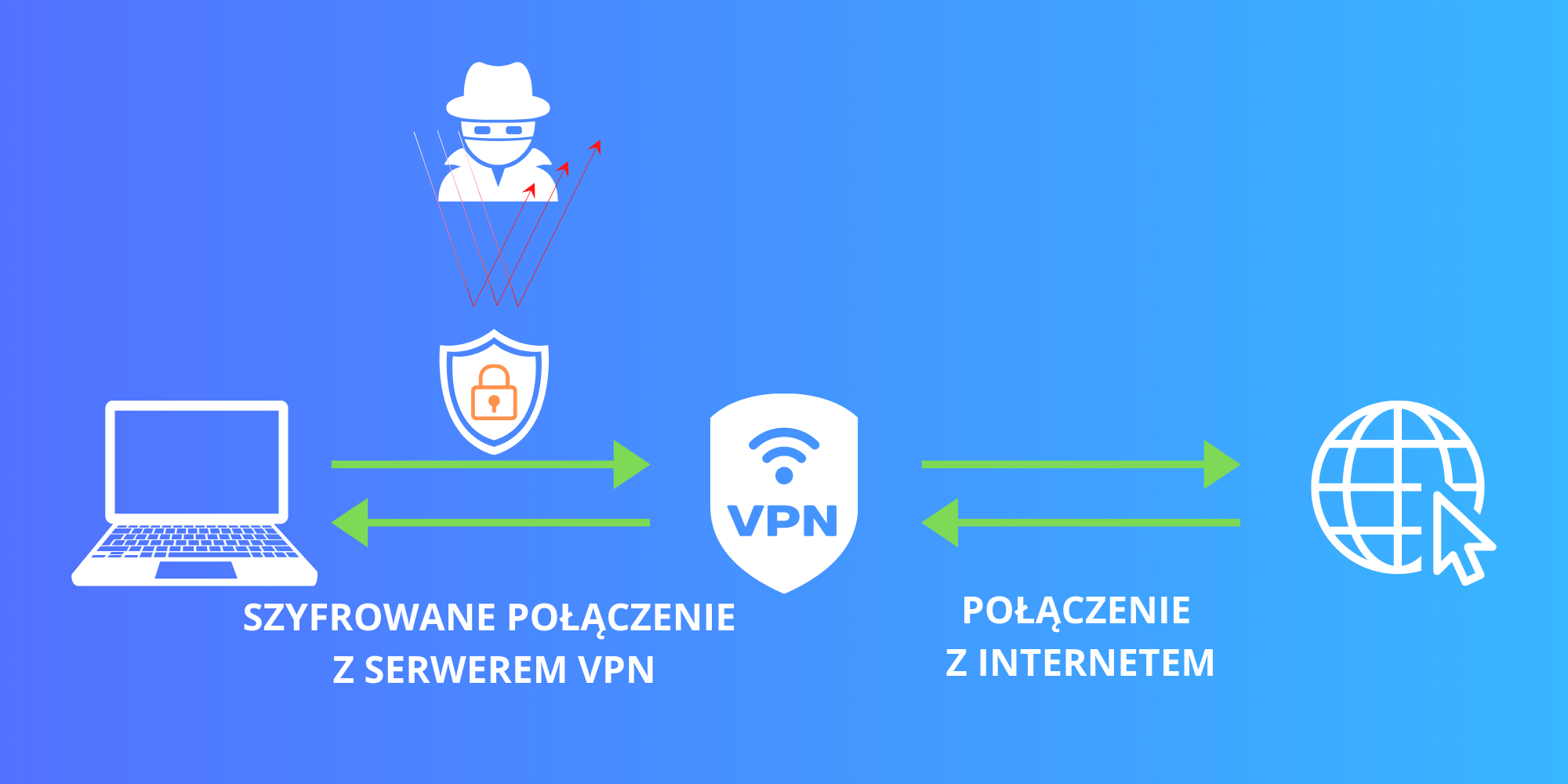
Najprostsze rozwiązania mogą w ogóle nie wspierać ochrony poufności przesyłanych danych, bardziej zaawansowane mogą korzystać z mechanizmu współdzielonego klucza i algorytmów kryptografii symetrycznej do ochrony poufności. Najbardziej zaawansowane rozwiązania korzystają z mechanizmów kryptografii klucza publicznego, certyfikatów cyfrowych.

**Dlaczego warto korzystać z VPN?**

Każda wizyta w Internecie pozostawia po sobie mnóstwo informacji, na podstawie których można zidentyfikować użytkownika, zebrać dane o jego zainteresowaniach, odwiedzanych witrynach, a czasami nawet bardziej poufne rzeczy, np. hasła do logowania.

Połączenie VPN maskuje te wszystkie połączenia, kierując je przez serwer VPN. Tworzy to niejako tunel (stąd nazwa tunelowanie), którym poruszają się informacje wymieniane między komputerem użytkownika i Internetem. Jest tylko jedno wyjście i wejście, nie można się do niego dostać „z boku” - zapobiega to atakowi Man in the middle.

Dodatkowo wszystko co wysyłane i odbierane zostaje zaszyfrowane: tunelowanie wychwytuje wszystkie pakiety, szyfruje i każdorazowo umieszcza w nowym pakiecie. Można to porównać do stworzenia pliku archiwum (zip, rar, 7z). Następnie serwer odpakowuje sobie te pakiety. Nawet, jeżeli ktoś przechwyciłby te dane, dostanie tylko mnóstwo niezrozumiałych, zakodowanych informacji których nie będzie umiał odczytać, bo nie ma klucza.



*Źródło: https://trybawaryjny.pl/co-to-vpn/*

### Tunel

Tunel to zestawienie połączenia między dwoma odległymi komputerami tak, by stworzyć wrażenie, że są połączone bezpośrednio. Przesłanki do tworzenia tuneli to:

* wygoda
* umożliwienie połączenia między komputerami ukrytymi w sieciach prywatnych (za firewallem, lub z adresami prywatnymi - warunek: jeden z hostów biorących udział w tworzeniu tunelu musi mieć adres publiczny)
* bezpieczeństwo - szyfrowanie połączenia: SSL/TLS, SSH
* możliwość przyspieszenia transmisji – kompresja sprawdza się szczególnie na wolnych łączach

Pojęcia ‘tunelowanie’ zazwyczaj używa się w odniesieniu do przesyłania poprzez tunel tylko jednego protokołu. Zwykle jest to jeden z typowych protokołów np.: POP3, SMTP, HTTP, które przesyłają dane w sposób jawny (w tym nazwy użytkowników i hasła) za pomocą bezpiecznych protokołów TLS/SSL lub SSH. Wirtualna sieć prywatna – umożliwia transmisję w sposób bezpieczny wielu protokołów poprzez publiczną sieć. Hosty będące po obu stronach VPN-u „widzą się” tak jakby były w jednej sieci. Takie sieci przeważnie działają w warstwie 3 modelu TCP/IP i tunelują warstwę 3 i wyższe - niektóre z nich umożliwiają także transmisję 2 warstwy (np tworzą wirtualną kartę sieciową). Kompresja powinna spełniać dwa podstawowe kryteria: niskie zapotrzebowanie na moc procesora i szybkość działania. Kompresji może zostać poddana całość transmisji lub tylko ładunek użyteczny

pakietów IP.

### OpenVPN

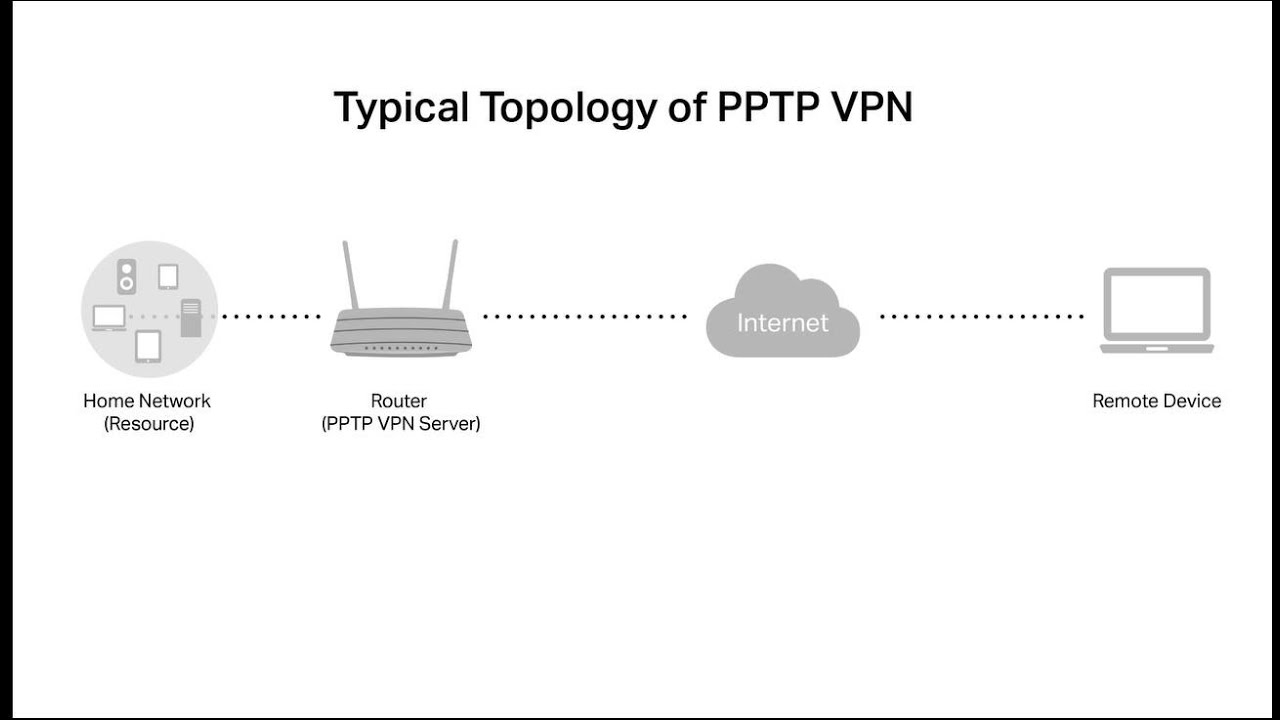
Jest to program umożliwiający tworzenie wirtualnych sieci prywatnych. Oparty jest na SSL/TLS i bibliotece OpenSSL, dostępny dla systemów uniksowych i Windows. OpenVPN zapewnia nam komplet mechanizmów, który pozwala nam zbudować bezpieczną sieć VPN – autoryzuje, uwierzytelnia, szyfruje i zapewnia integralność przesłanych danych. Ponadto chroni serwer (koncentrator) przed atakami DoS oraz sieć wirtualną przed wstrzykiwaniem obcych danych.

OpenVPN oferuje dwa rodzaje tuneli, których używamy w zależności od konkretnych potrzeb. W laboratorium skorzystam z rodzaju tunelu “tun**”.** Hosty mają przydzielony po obu stronach adres IP i odbywa się klasyczny routing: wystarczy w większości przypadków takich jak dostęp do sieci firmowej czy do Internetu.

**Zabezpieczenia OpenVPN** (generowane klucze, podpisy, szyfrowanie połączeń)

* Implementacja tunelu punkt-punkt z wykorzystaniem SSLv3/TLSv1, w odróżnieniu od wielu innych implementacji VPN nie bazuje na IPsec ale wykorzystuje wirtualny interfejs sieciowy tun/tap (tun – warstwa 3 protokół IP, tap – warstwa druga – np ethernet) dostępny jest m.in. dla Linux-a, BSD (w tym Mac OS X), Windows2000 w górę, Solaris.
* Autentykacja może odbywać się za pomocą współdzielonego klucza, certyfikatów oraz nazwy użytkownika i hasła.
* Pakiet składa się z jednego programu binarnego, dodatkowo można użyć pliku konfiguracyjnego oraz plików z kluczem współdzielonym lub certyfikatów.
* Szyfrowanie bazujące na SSL może być wspomagane przez mechanizm haszujący HMAC (Hash Message Authentication Code) w celu zwiększenia bezpieczeństwa.
* Pracuje w przestrzeni użytkownika i używa do komunikacji protokołu UDP lub TCP wykorzystując oficjalnie przyznany temu protokołowi przez IANA port 1194.
* Nie wymaga tak jak IPsec tworzenia 2 kanałów – w OpenVPN tunel jest dwukierunkowy i łatwiej przechodzi przez firewalle.
* Pozwala na równoległe tworzenie wielu tuneli i wspomaga ruting między nimi.
* Do kompresji używany jest szybki algorytm LZO podobny do gzip.
* Wspiera akcelerację sprzętową oraz karty procesorowe.

### PPTP

PPTP (Point-to-Point Tunneling Protocol) jest jest jednym z protokołów, w oparciu o który mogą działać wirtualne sieci prywatne. To protokół komunikacyjny umożliwiający tworzenie wirtualnych sieci prywatnych wykorzystując technologię tunelowania. Typową topologię protokołu PPTP w tunelu VPN przedstawia poniższy schemat.

*Źródło: https://www.youtube.com/watch?v=Wv42x6Gr4Yc*

Protokół PPTP umożliwia zdalne połączenie się do stacji roboczej lub sieci za pośrednictwem Internetu oraz tworzenie wirtualnego połączenia z lokalną siecią. Ma na celu zapewnienie bezpieczeństwa przy zdalnym przesyłaniu danych. Inicjalizacja połączenia wykonywana jest na port 1723.

Spośród wszystkich protokołów VPN, PPTP jest jednym z najczęstszych używanych, najłatwiejszych do skonfigurowania i najszybszych**.** Z tego powodu, protokół PPTP jest przydatny w aplikacjach, w których prędkość jest najważniejsza, jak streaming audio lub wideo oraz na starszych, wolniejszych urządzeniach z bardziej ograniczonymi procesorami.

PPTP wykazuje poważne luki w zabezpieczeniach. Podstawowe protokoły uwierzytelniania są zasadniczo niezabezpieczone i były wielokrotnie łamane w analizach bezpieczeństwa od czasu ich wprowadzenia. Z tego powodu PPTP nie jest zalecany z wyjątkiem przypadków, w których prędkość transmisji jest ważniejsza od jej bezpieczeństwa.

# Użyte narzędzia i aplikacje

* **Windows 10 Home** w wersji 21H1
* **Virtualbox** - maszyna wirtualna Oracle (u mnie z systemem Linux)
* **Ubuntu 20.04.3 LTS** (Fosal Fossa) - dystrybucja Linuxa
* **Wireshark** - sniffer pozwalający “podsłuchiwać” sieć także w czasie rzeczywistym; analizuje ruch sieciowy; umożliwia przechwytywanie i nagrywanie pakietów danych, a także ich dekodowanie
* **Npcap 1.55** - biblioteka windowsowa do Wiresharka; pozwala w czasie rzeczywistym śledzić dane, które przechodzą przez kartę sieciową komputera, dzięki niej widzimy wszystkie aktualnie przechwytywane interfejsy sieciowe
* **OpenVPN** - protokół wykorzystywany do tworzenia tuneli
* **PPTP** - protokół komunikacyjny umożliwiający tworzenie wirtualnych sieci prywatnych wykorzystujących technologię tunelowania
* **dostęp do sieci bezprzewodowej**

# Przebieg ćwiczenia

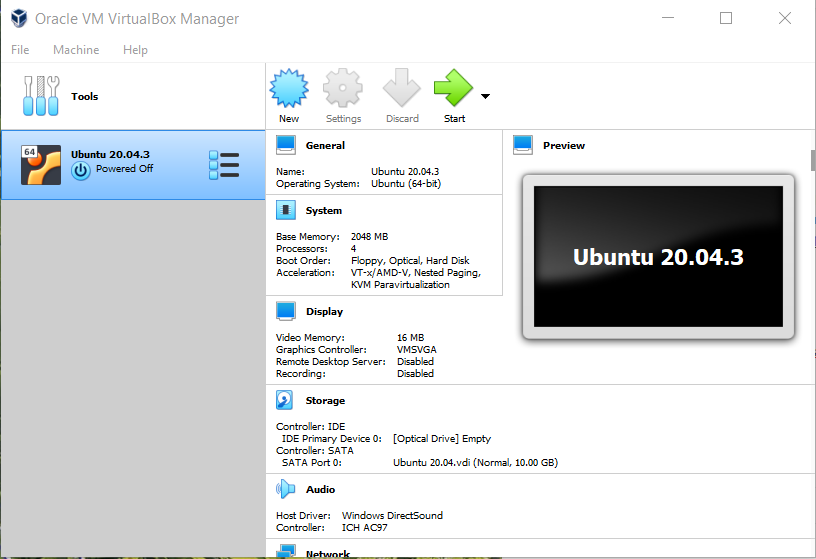
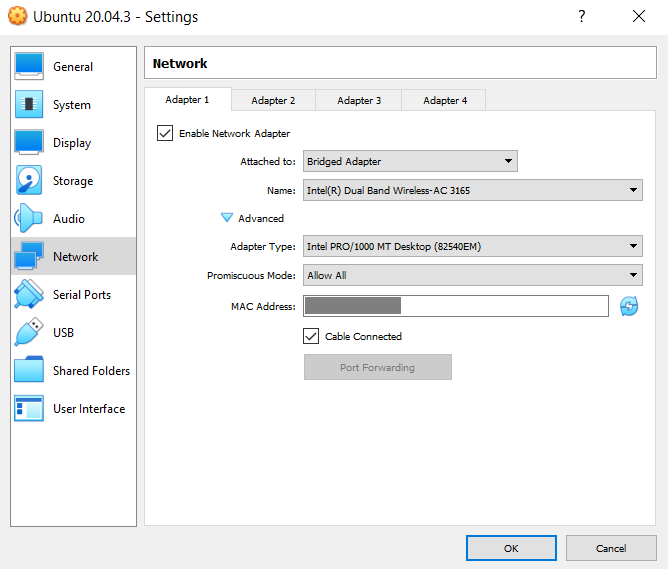
Laboratorium wykonywałam na komputerze z systemem Windows 10 oraz wirtualnej maszynie z Ubuntu. Na Ubuntu na wirtualnej maszynie zainstalowałam serwery PPTP oraz OpenVPN aby ustanowić tunelowanie. Na jednym z komputerów (klient z Windowsem) uruchomiłam program Wireshark, którym następnie śledziłam działania komputera atakowanego (serwera).

Laboratorium podzieliłam na dwie części: najpierw badałam tunelowanie z użyciem protokołu PPTP, a następnie z OpenVPN. We wnioskach na końcu zestawiłam obie technologie połączeniowe oraz porównałam ich poziomy skomplikowania konfiguracji - także z innymi systemami tunelowania.

## CZĘŚĆ I: Badanie ruchu w niezabezpieczonym tunelu

### Konfiguracja VirtualBox (z Ubuntu)

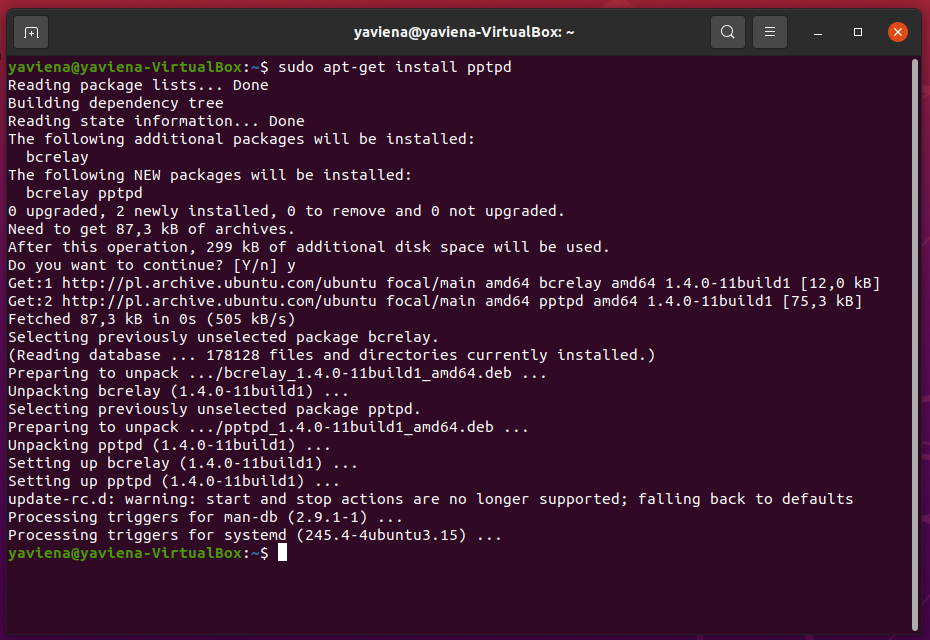
Dostosowałam konfigurację wirtualnej maszyny do potrzeb laboratorium zapewniając odpowiednią ilość miejsca, RAM oraz połączenie sieciowe niezbędne do ustanowienia tunelowania.

### Instalacja serwera PPTP (Ubuntu)

Do uruchomienia tunelowania użyłam distro Linuxa (Ubuntu) jako serwera, na którym wykonałam instalację i konfigurację technologii PPTP. Wprowadzając do terminala poszczególne polecenia pomyślnie zainstalowałam serwer PPTP.

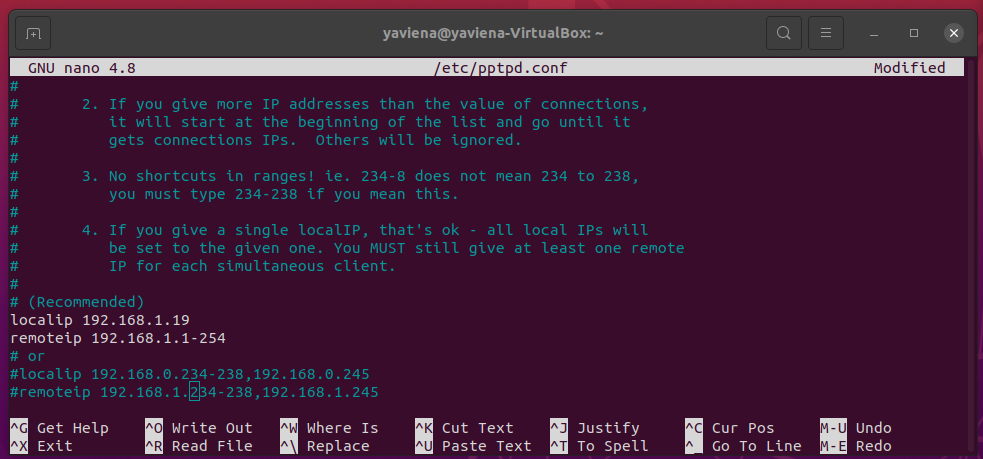
| **sudo** **apt-get update**  **sudo apt-get upgrade**  **sudo apt-get install pptpd** | aktualizacja oprogramowania  instalacja serwera PPTP |
| --- | --- |



| **sudo nano /etc/pptpd.conf**  **sudo nano /etc/ppp/pptpd-option** | konfiguracja pliku serwera PPTP  modyfikacja wpisu (dodanie swoich serwerów DNS) |
| --- | --- |

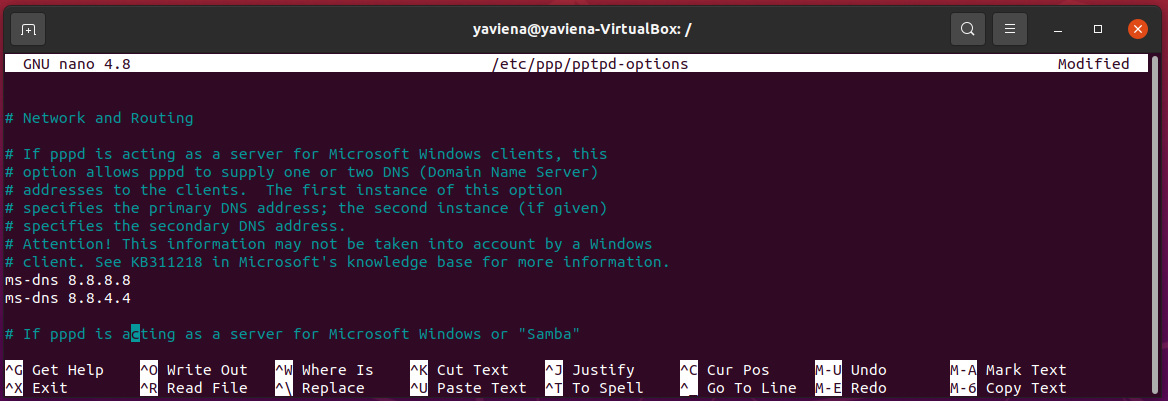
Edytując plik serwera PPTP ustawiam:

* **localip** - adres po stronie serwera PPTP
* **remoteip -** pulę adresów, które zostały mi przyznane przy podłączeniu się do servera VPN).



Zmodyfikowałam wpis dodając swoje serwery DNS.

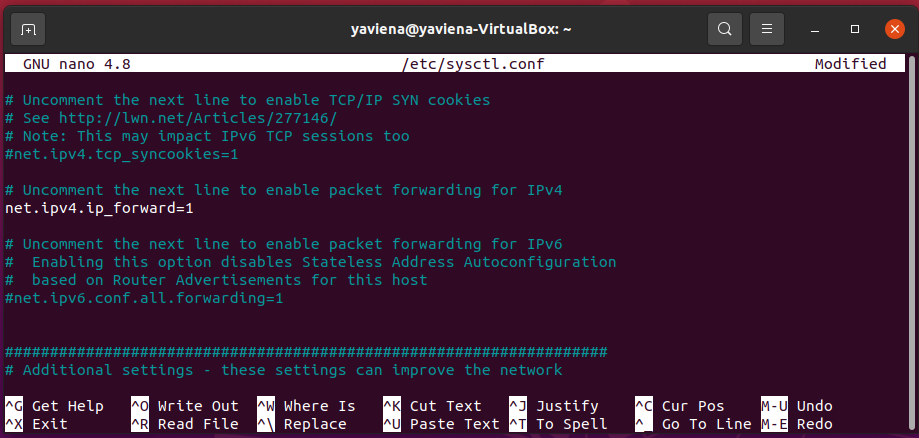
| **sudo nano /etc/ppp/pptpd-option** | modyfikacja wpisu i dodanie swoich serwerów DNS |
| --- | --- |



Domyślnie, w ubuntu przekazywanie pakietów IP (IP forwarding) jest wyłączone. Muszę to zmienić, aby przez moje połączenie VPN można było przeglądać Internet.

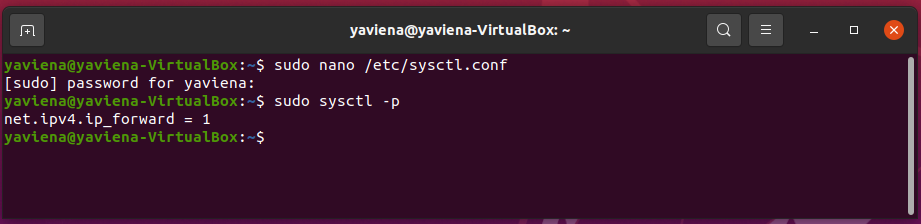
| **sudo nano /etc/sysctl.conf** | modyfikacja wpisu z przekazywaniem pakietów |
| --- | --- |

Odszukałam wpis “net.ipv4.ip\_forward=1” i usunęłam znak komentarza # przed wpisem.



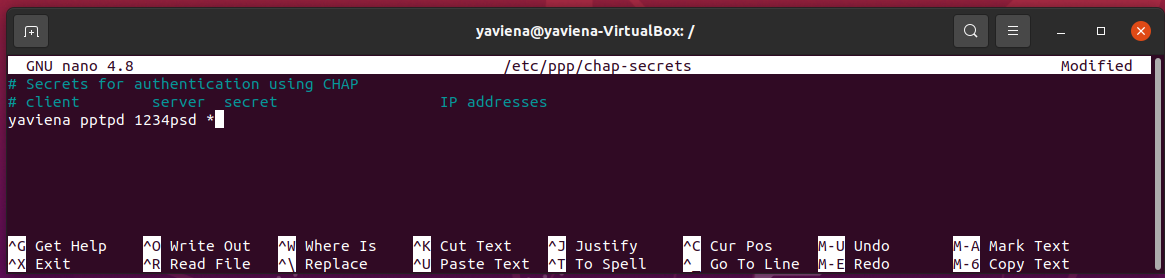
Potwierdziłam zmiany poleceniem:

| **sudo sysctl -p** | potwierdzenie zmian w zmodyfikowanym wpisie |
| --- | --- |



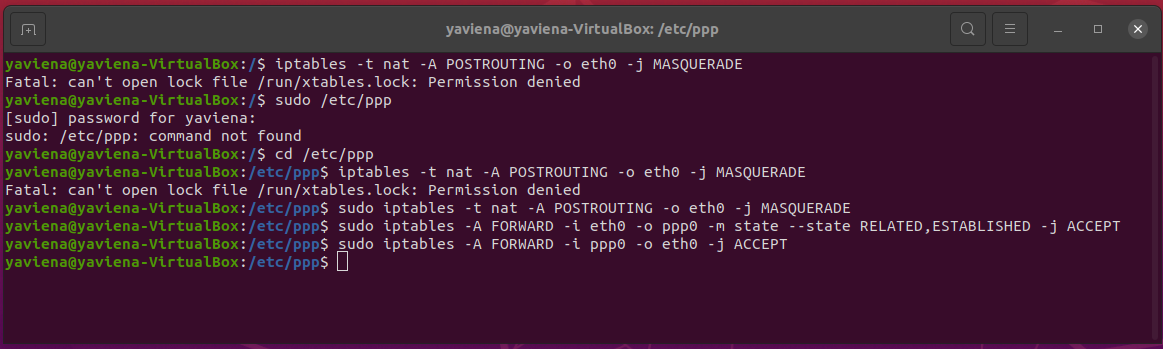
Przystąpiłam do konfiguracji użytkowników. Zedytowałam plik, w którym umieściłam użytkowników oraz hasła. Plik miał postać:

| **sudo nano /etc/ppp/chap-secrets** | konfiguruję użytkowników |
| --- | --- |



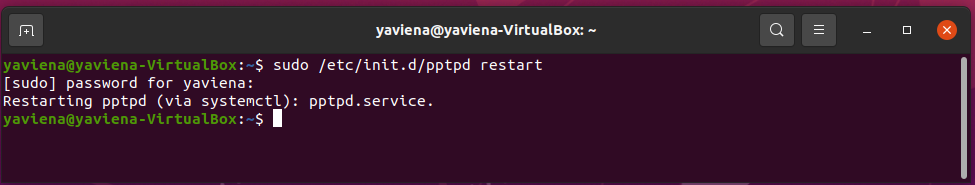
Dodałam kilka reguł do firewalla:

| **iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE**  **iptables -A FORWARD -i eth0 -o pppo -m state –state RELATED, ESTABLISHED -j ACCEPT**  **iptables -A FORWARD -i ppp0 -o eth0 -j ACCEPT** |
| --- |



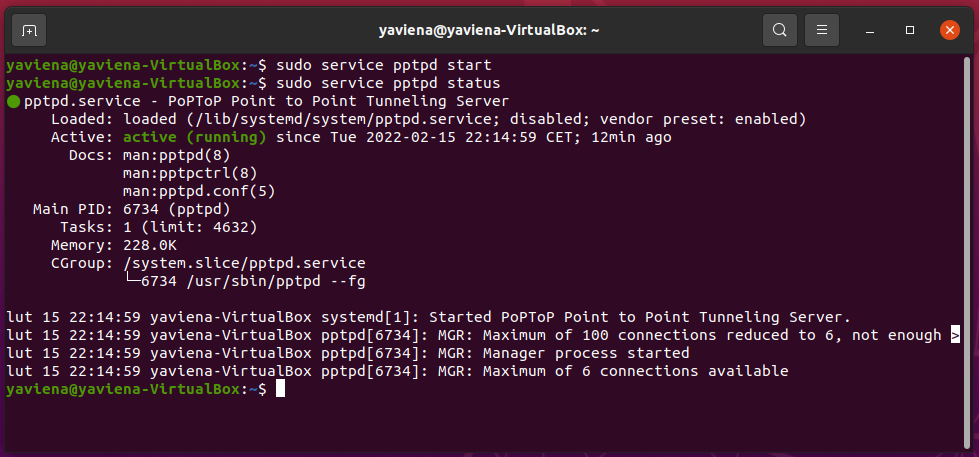
Następnie zrestartowałam serwer PPTP.

| **sudo /etc/init.d/pptpd restart** | restart serwera |
| --- | --- |



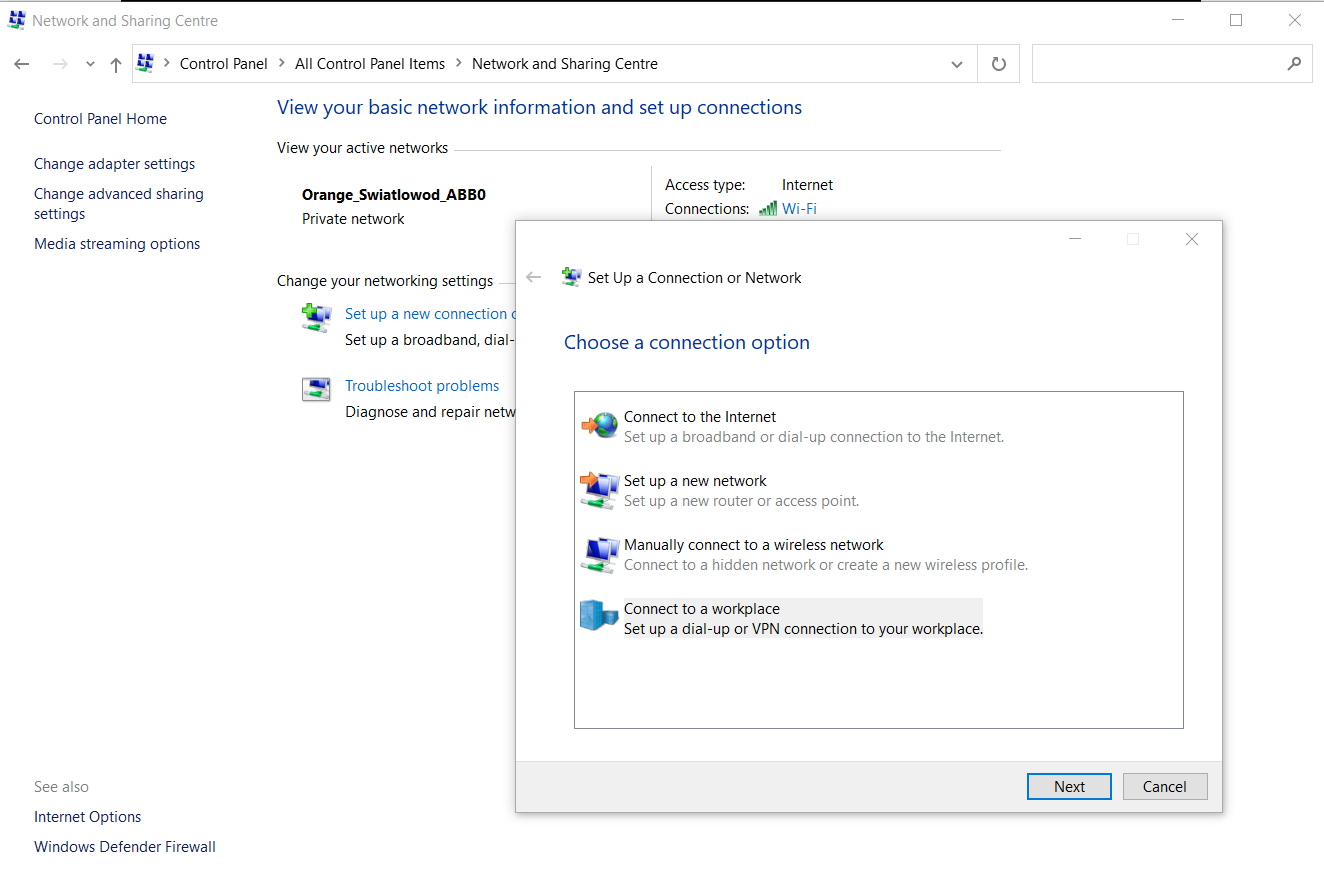
Na koniec sprawdziłam status zainstalowanego serwera PPTP.

| **service pptpd status** | konfiguruję użytkowników |
| --- | --- |

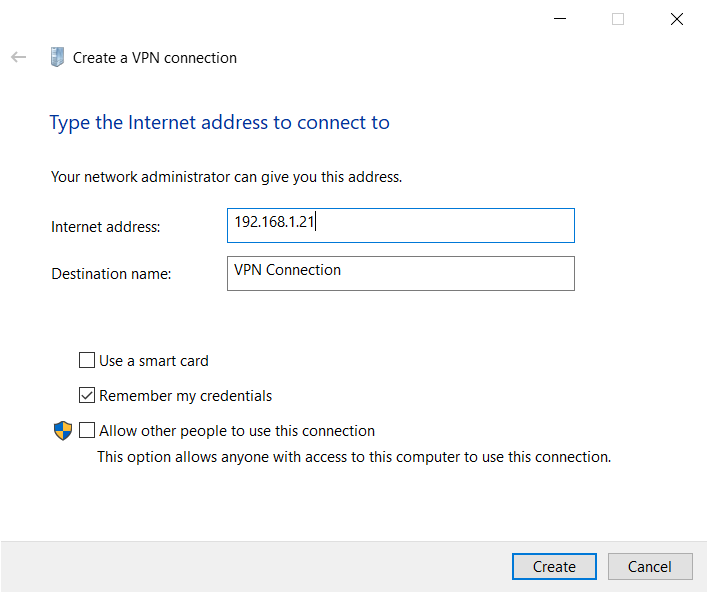


### Konfiguracja klienta PPTP (Windows 10)

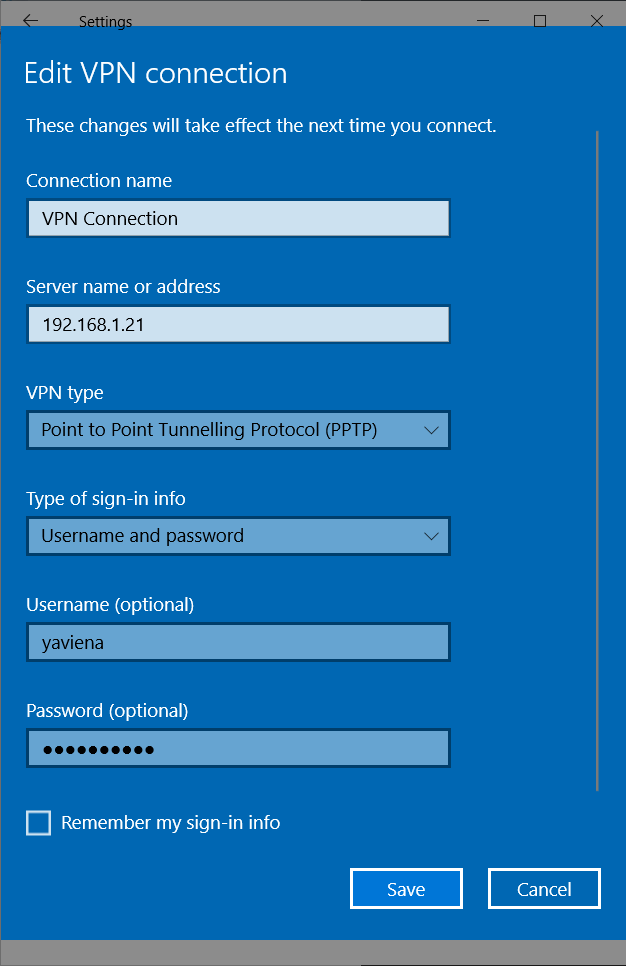
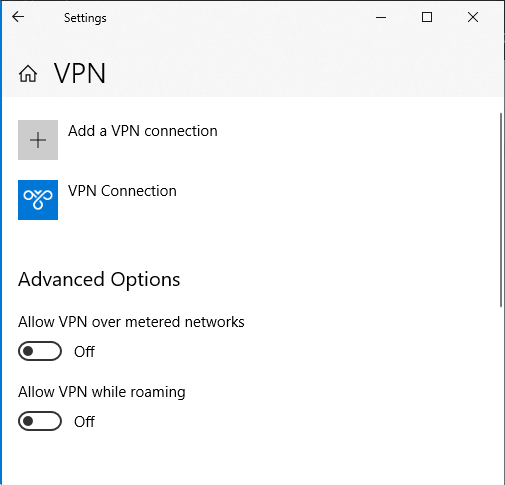
W kliencie na systemie Windows 10 w ustawieniach sieci i połączeń utworzyłam nowe połączenie VPN.



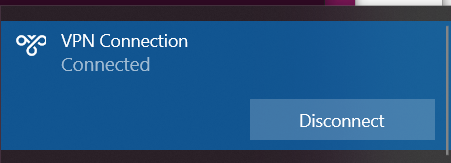
Podałam adres mojego servera VPN.



Zalogowałam się do nowego połączenia VPN podając utworzone wcześniej na serwerze hasło.

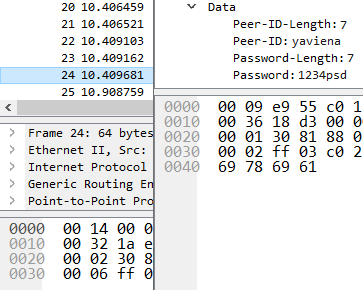
 

Po konfiguracji nawiązałam połączenie z wcześniej utworzonym kontem (*yaviena*) logując się tym samym do serwera PPTP.



### Analiza Wiresharka

Po nawiązaniu połączenia przeanalizowałam ruch sieciowy z wykorzystaniem programu WireShark. Przeprowadziłam analizę pakietu odpowiadającego za połączenie z serwerem PPTP. Widać gołym okiem przesłany zarówno login jak i hasło w analizowanym pakiecie. Oznacza to, że protokół ten nie jest bezpieczny.

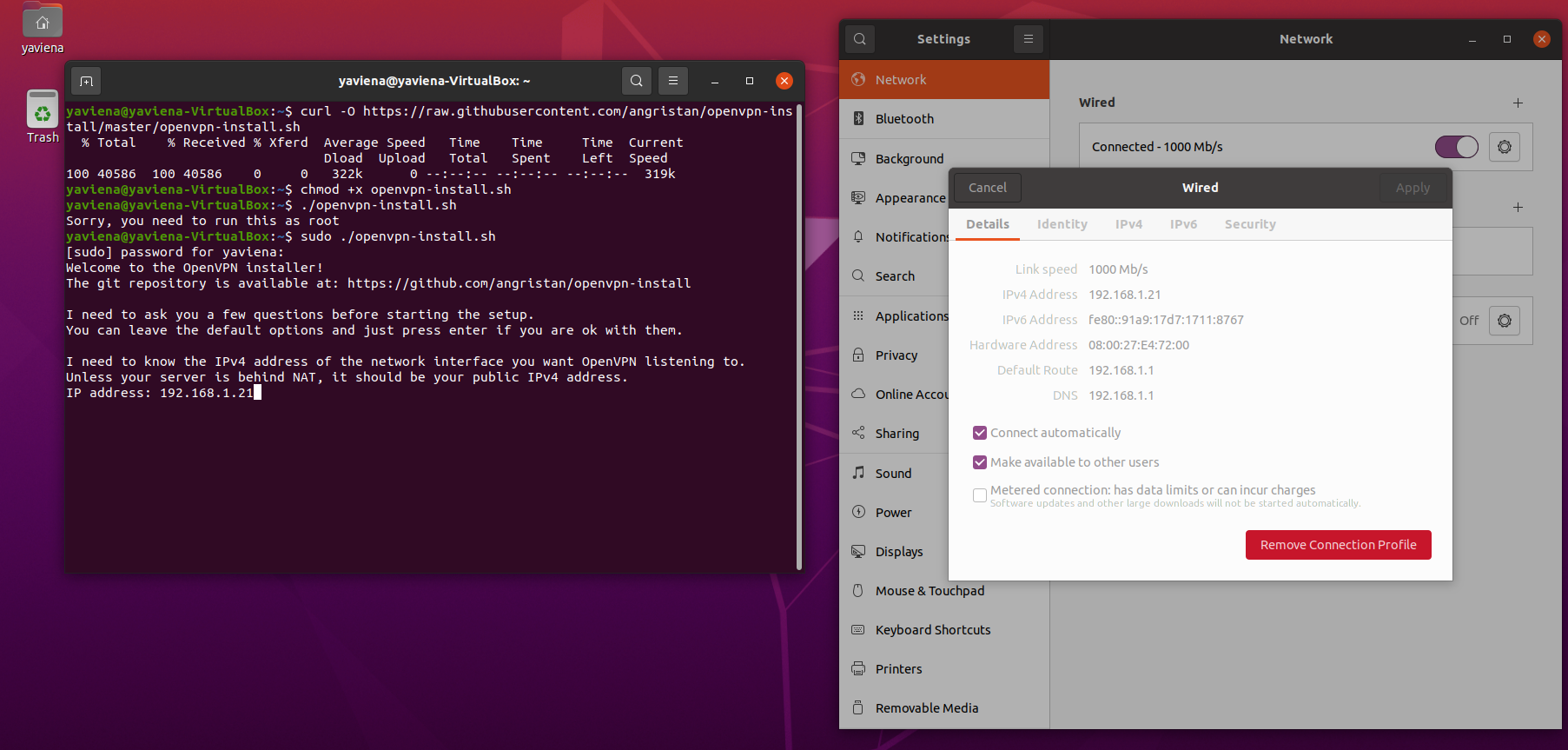


## 

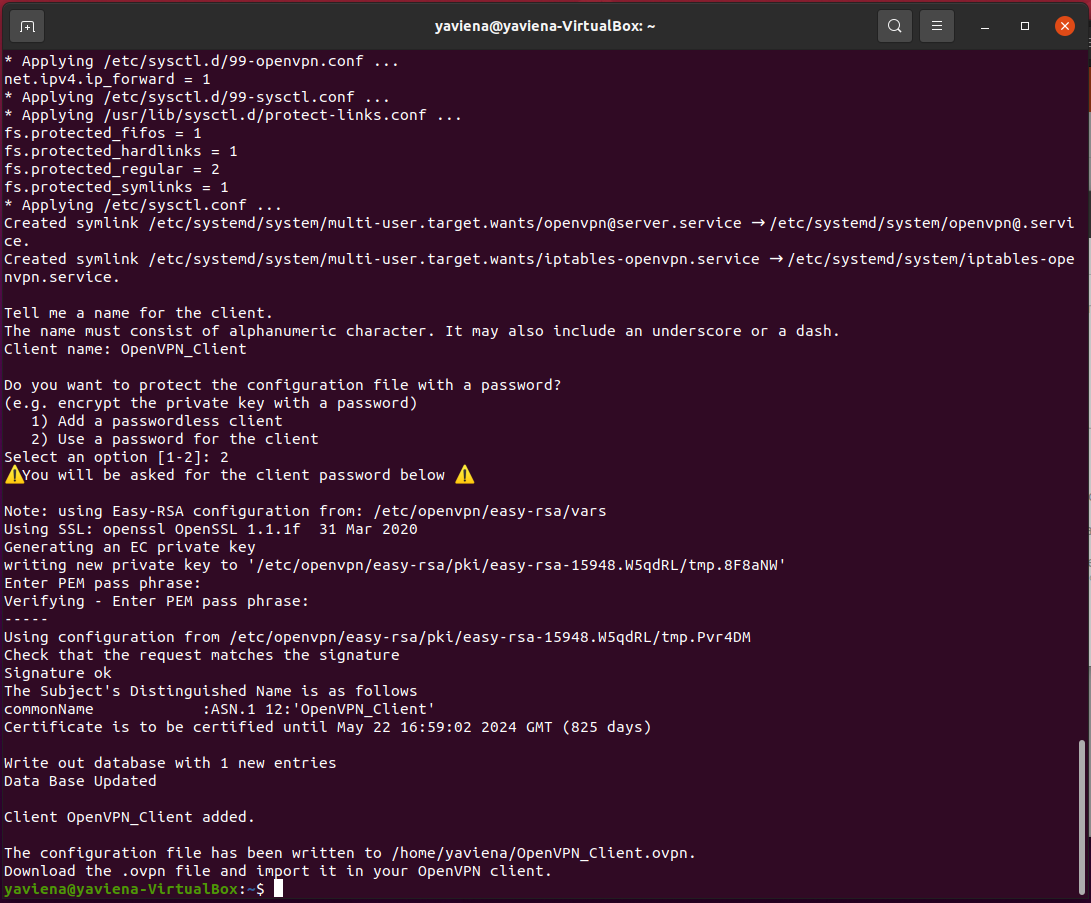
## CZĘŚĆ II: Badanie ruchu w zabezpieczonym tunelu

### Instalacja serwera OpenVPN (Ubuntu)

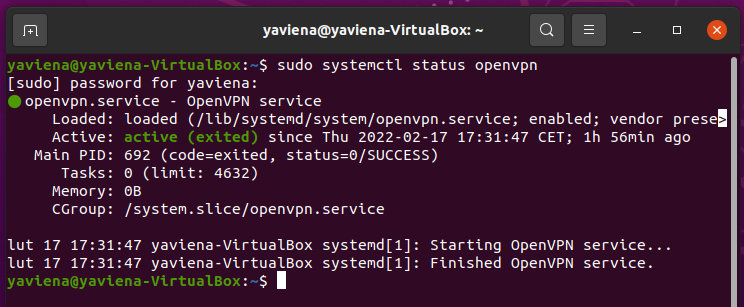
W drugiej części ćwiczenia zainstalowałam i skonfigurowałam na systemie Ubuntu w VirtualBoxie protokół OpenVPN.



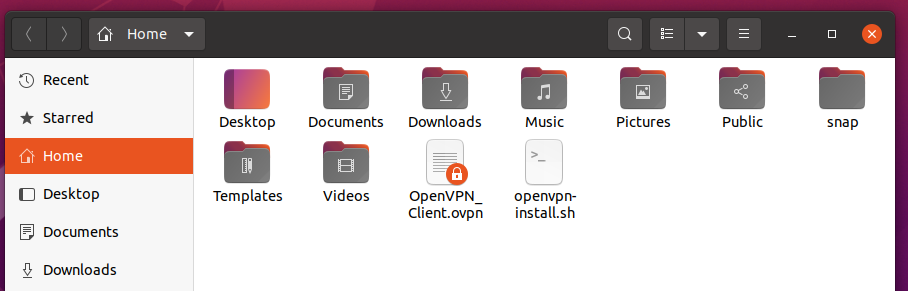
W jego ustawieniach wybrałam maksymalną ochronę, tj. każdy z użytkowników posiada własne klucze autoryzacyjne (z certyfikatem), zaś transmisja jest chroniona kierunkowym kluczem TLS.



Po ukończonej z sukcesem instalacji sprawdziłam poprawność zainstalowanego protokołu OpenVPN.

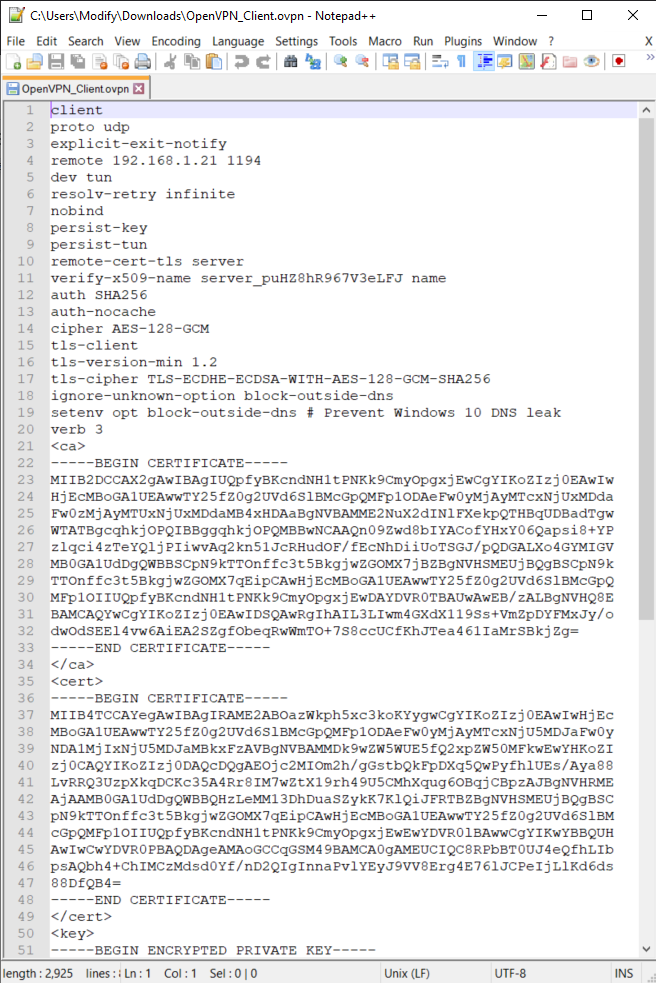
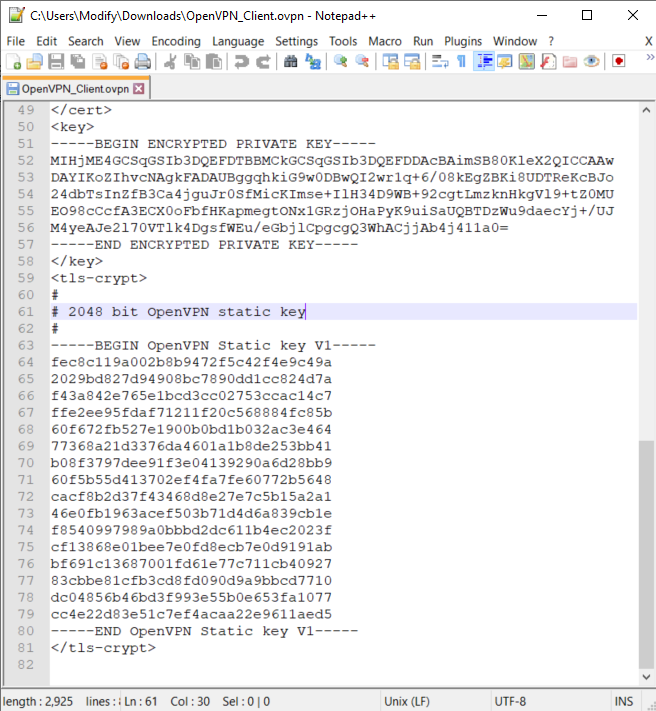


Utworzony plik konfiguracyjny z nowym kontem użytkownika stworzonym na serwerze skopiowałam na komputer (z systemem Windows), który będzie klientem łączącym się do tegoż serwera.

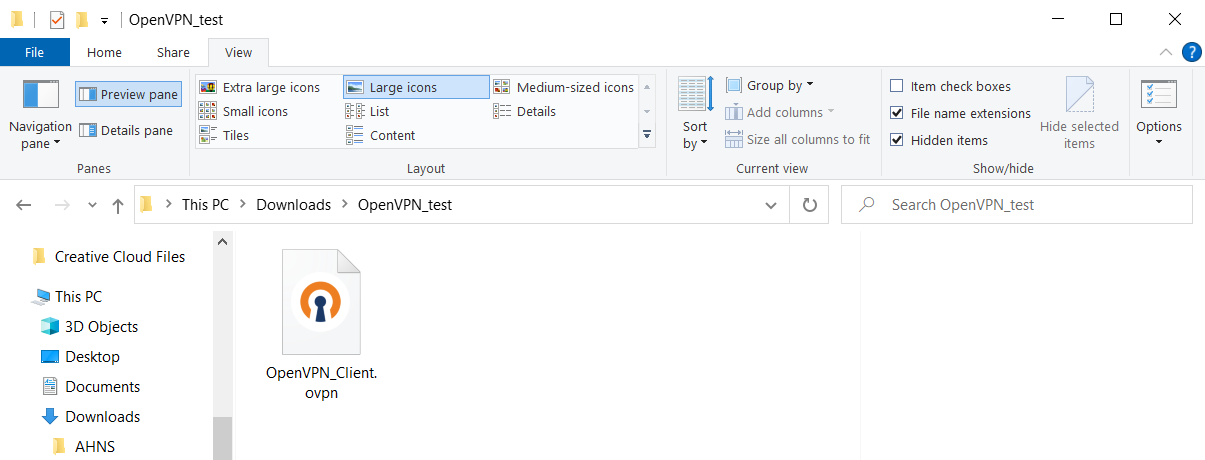


Skontrolowałam jak wygląda wygenerowany plik konfiguracyjny z kontem użytkownika. Widać w nim wyraźnie takie informacje jak m.in.:

* protokół połączenia,
* IP oraz port serwera, do którego można się połączyć,
* rodzaj szyfrowania,
* akceptowalną wersję protokołu TLS
* klucze certyfikatu.

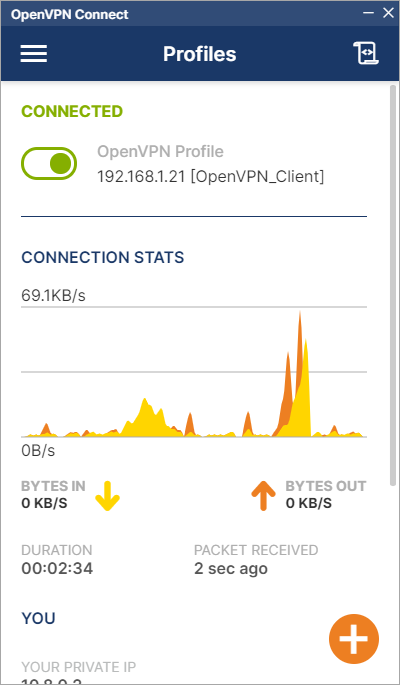
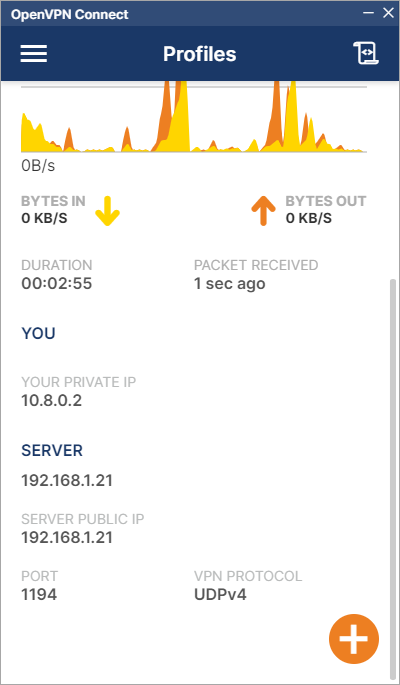
 

Skopiowałam plik konfiguracyjny na komputer - klienta (z systemem Windows), który będzie łączył się do serwera.

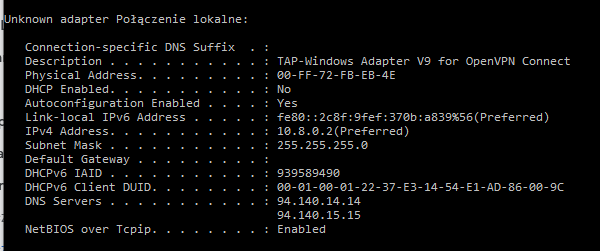


### Konfiguracja klienta OpenVPN (Windows 10)

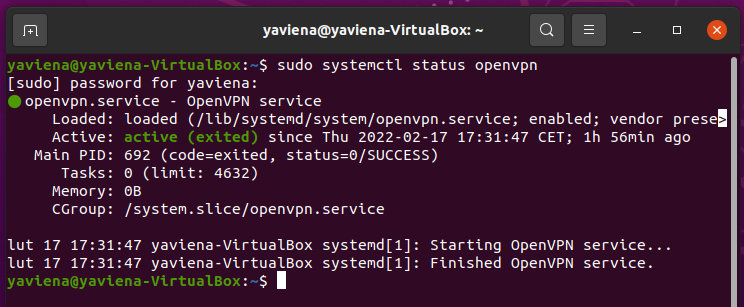
Klient OpenVPN będzie łączył się z serwerem. Po dodaniu do klienta pliku konfiguracyjnego wykonałam połączenie i sprawdziłam jego status.

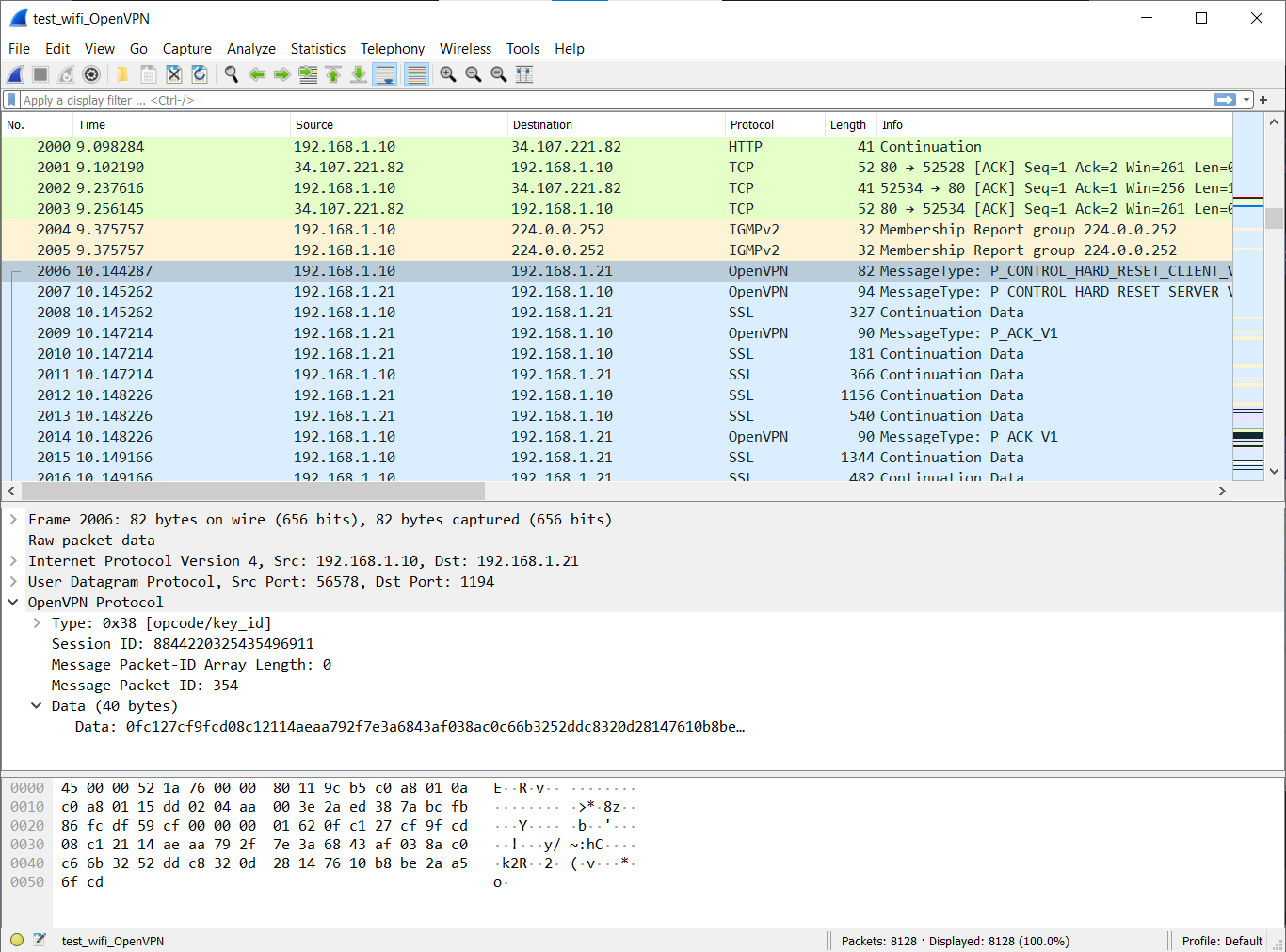
Upewniłam się, że mój adres IP na urządzeniu klienta został po połączeniu zmieniony na adres przypisany z serwera (10.8.0.2).



Upewniłam się, że pakiety danych na serwerze OpenVPN oraz ruch są przekierowywane poprawnie.



Programem Wireshark ponownie sprawdziłam jak będzie wyglądać proces logowania się do sieci poprzez protokół OpenVPN. Jak widać na poniższym zrzucie ekranu, klient jest podłączony do serwera i to przez niego przekierowywany jest cały ruch. Dodatkowo, wyraźnie widać kiedy nastąpiło połączenie poprzez OpenVPN. Nie można w tym wypadku odczytać danych logowania do serwera OpenVPN w żadnym z analizowanych pakietów.



# Wnioski

Celem laboratorium było przetestowanie działania tuneli sieciowych z wykorzystaniem technologii VPN.

Spośród wszystkich protokołów VPN, protokół PPTP jest jednym z najczęstszych, najłatwiejszych do skonfigurowania i najszybszych protokołów tuneli sieciowych. Z tego powodu, protokół PPTP jest przydatny w aplikacjach, w których prędkość jest najważniejsza, takich jak streaming audio lub wideo oraz na starszych, wolniejszych urządzeniach z bardziej ograniczonymi procesorami. Implementacja i konfiguracja protokołu PPTP jest prosta i wymaga zaangażowania o wiele mniejszych zasobów niż pozostałe protokoły VPN.

Jednak, PPTP również wykazuje poważne luki w zabezpieczeniach**.** Podstawowe protokoły uwierzytelniania (zazwyczaj MS-CHAP-v1/v2) są zasadniczo niezabezpieczone i były wielokrotnie łamane w analizach bezpieczeństwa od czasu ich wprowadzenia. Z tego powodu PPTP nie jest zalecany z wyjątkiem przypadków, w których bezpieczeństwo nie jest absolutnie konieczne.

OpenVPN jest nieco bardziej skomplikowany w konfiguracji zarówno po stronie serwera jak i po stronie klienta, który będzie łączył się do serwera. Komunikacja za pośrednictwem OpenVPN ma jednak nieporównywalnie wiele zalet:

* obsługuje różne systemy operacyjne (np. Linux, Solaris, różne BSD, OS X, Windows oraz iOS i Android),
* stabilność,
* skalowalność (tysiące klientów),
* relatywnie łatwa instalacja,
* dynamiczne adresy IP i NAT,
* model zabezpieczeń OpenSSL,
* SSL/TLS oraz X509 PKI (Public Key Infrastructure) do uwierzytelniania sesji,
* protokół IPsec ESP do bezpiecznego transportu tunelowego przez UDP.

OpenVPN wydaje się idealnym rozwiązaniem, jednak można i tu wskazać kilka wad. Przede wszystkim mniejsza szybkość połączenia oraz proces konfiguracji technicznej - szczególnie po stronie klienta. To właśnie tam (klient) należy obsłużyć wygenerowany przez serwer plik konfiguracyjny i odpowiednio połączyć go z klientem.

Reasumując, PPTP to najszybszy protokół VPN za sprawą słabszego szyfrowania, któremu poddawane są przesyłane dane. Straty prędkości połączenia z siecią są przez to minimalne. Najczęściej stosowane w protokole PPTP jest szyfrowanie 128-bitowe (algorytmy RC4 i RSA ), które w porównaniu do 256-bitowego szyfrowania w nowszych rozwiązaniach nie zapewnia pełnego bezpieczeństwa.

Zamiast PPTP lepiej jest korzystać z OpenVPN, WireGuard, IKEv2 lub L2TP/IPSec. Są to bezpieczne protokoły, które nie mają poważnych luk bezpieczeństwa.