Wojciech Myszka

Laboratorium 3: Sieci wirtualne. OpenVPN wer. 30 z drobnymi modyfikacjami!

2020-06-22 08:30:22 +0200

Spis treści

1. Wprowadzenie 2
2. Dostępne rozwiązania 3
3. Cel ćwiczeń 4
4. Oprogramowanie 4
5. OpenVPN 5
5.1. Instalacja 5
5.2. Uruchomienie 5
5.3. Ubuntu 6
5.4. Windows 6
5.5. Android 7
6. Zadania do wykonania 8
7. Uwagi 9
8. Dodatkowe źródła informacji 10
9. Instrukcja w postaci jednego pliku... 10

1. Wprowadzenie

Bardzo często istnieje potrzeba połączenia zdalnego komputera (lub zdalnej sieci) do firmowej sieci lokalnej. Dobrym rozwiązaniem może być wydzierżawienie łącza telekomunikacyjnego i połączenie obu sieci (dołączenie zdalnego komputera do sieci lokalnej). Wydaje się jednak, że jest to dosyć nieracjonalne w sytuacji gdy (praktycznie) wszyscy mają dostęp do Internetu. Oprócz tego, dostawca łącza może łatwo uzyskać (albo udostępnić) dostęp do ruchu na łączu.

Z drugiej strony powstaje problem jak udostępniać zasoby sieci lokalnej tylko wybranym (być może podróżującym po świecie) użytkownikom i zapewnić wystarczającą prywatność (stanowiącą podstawę prowadzenia biznesu).

W ten sposób powstała idea VPN (*Virtual Private Network* — wirtualna sieć prywatna), która pozwala z dowolnego miejsca na świecie stworzyć szyfrowane, wirtualne „połączenie telekomunikacyjne" zdalnego komputera/sieci z siecią macierzystą firmy.

Innym zastosowaniem VPN jest ochrona przed monitorowaniem ruchu przez agendy rządowe: wybieramy dostawcę VPN za granicami kraju, nawiązujemy szyfrowane połączenie z serwerem VPN (fakt nawiązania połączenia będzie monitorowany, ale już przesyłane informacje już nie. W szczególności, poza zasięgiem lokalnych służb będą adresy z którymi nawiązujemy połączenie. Choć w przypadku skoordynowanej akcji służb — może to nie być żadną ochroną, a jedynie utrudnieniem.

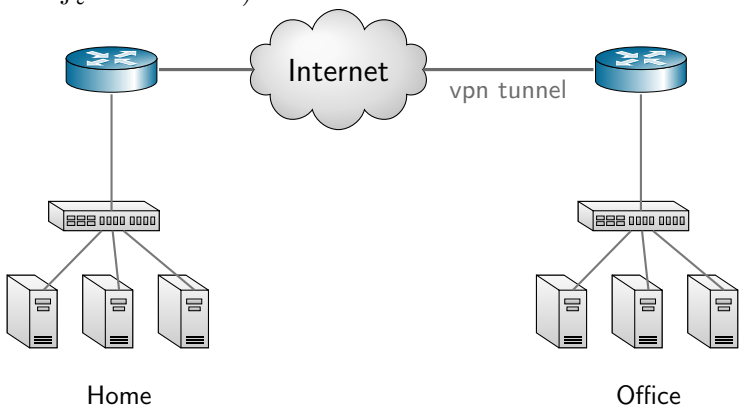
Kolejnym zastosowaniem VPN jest „oszukiwanie" dostawców usług, ktrzy ich dostępność ograniczają „terytorialnie" („W twoim kraju ta usługa jest niedostępna!"). Wybierając dostawcę VPN w odpowiednim miejscu, powodujemy, że (z punktu widzenia „drugiego końca połączenia") jesteśmy gdzie indziej.

Czasami może to być metoda na przekroczenie firewalla (oczywiście, przy założeniu że jednak dopuszcza on dostęp do jakichś usług (uznanych przez lokalne władze jako bezpieczne.)

Poniższa ilustracja pokazuje ideę realizowanego tunelu. Nazwę „Of-

fice" należy traktować symbolicznie: będzie to dostawca bezpiecznego połączenia z komputerem klienta. Home to albo indywidualny klient, albo oddział firmy.

Natomiast w przypadku sieci wirtualnych na potrzeby firm — sieć może być tak skonstruowana, że będzie pozwalała na pełną integrację lokalnego i zdalnego oddziału firmy. Można podejmować decyzję na temat sposobu organizacji dostępu do Internetu (przez odpowiednią realizację trasowania).



Sieci połączone tunelem mogą być również tak zorganizowane, że komputery będą się wzajemnie widziały, albo — gdy jest kilka oddziałów — połączenia VPN będą realizowały redundantną strukturę dostarczającą alternatywnych dróg połączeń.

2. Dostępne rozwiązania

1. PPTP – używany w MS Windows (i uważany za bardzo podatny na ataki oraz daleki od bezpieczeństwa)
2. L2TP – używany w MS Windows (udoskonalona wersja PPTP)
3. OpenVPN
4. IPsec (nieco ogólniejsza niż tylko VPN struktura do bezpiecznego przesyłania informacji)
5. SSTP (ang. Secure Socket Tunneling Protocol) firmy Microsoft

6. OpenConnect rozwiązanie bardzo podobne do AnyConnect firmy Cisco (i zgodne z nim)
7. ...

Oprócz tego istnieją rozwiązania „firmowe”:
— Cisco AnyConnect (stosowany przez Politechnikę Wrocławska)
— ...

3. Cel ćwiczeń

1. Pokazanie i praktyczne przećwiczenie korzystania z VPN.
2. Objaśnienie jak realizuje się transmisja sygnałów w złożonych sieciach.

Niestety, aby przeprowadzić te ćwiczenie będę musiał udostępnić jakiś serwer VPN. Zapewne wiąże się to z pewnym niebezpieczeństwem, ale wypada mi zaufać (wierząc, że groźba niezaliczenia jest wystarczającym argumentem).

Proszę o kontakt, gdyby okazało się, że usługa nie działa.

4. Oprogramowanie

Poniżej przykłady różnych rozwiązań VPN.

1. ~~Android: Opera VPN~~[1]
2. Zamiast niej przeglądarka Opera została/ma zostać wyposażona w klienta VPN.
3. ~~Android: OpenVPN Connect~~ (Niestety, nie chce współpracować z generowanymi przez mnie plikami konfiguracyjnymi).
4. Android: OpenVPN for Android Działa.
5. Android: Private Tunnel VPN – Fast & Secure Cloud VPN
6. Android: Cisco AnyConnect
7. Windows: OpenVPN

[1] Niestety usługa została zawieszona 30 kwietnia 2018.

Dostawcami VPN zajmować się nie będę — najczęściej (nawet jeżeli niezbyt drogie) są to rozwiązania komercyjne. Choć może warto przyjrzeć się Windscribe, w którym podsatwowy zakres usług jest darmowy, a plany płatne zaczynają się od 4$ za miesiąc.

5. OpenVPN

Do przeprowadzenia zajęć wybrałem oprogramowanie OpenVPN.

1. Jest darmowe.
2. Jest dosyć popularne.
3. Nie udało się uruchomić serwera PPTP.

5.1. Instalacja

1. Windows: Oprogramowanie jest do pobrania ze strony `https://openvpn.net/index.php/open-source/downloads.html`. W laboratorium nie trzeba pobierać — powinno być w kartotece `C:\software`. Plik `openvpn-install-2.4.5-I601.exe`.
2. Linux (Debian/Ubuntu): powinno być w standardowym zestawie pakietów.
   ```
   sudo apt-get install openvpn
   ```
3. Android: OpenVPN Connect ze sklepu.

5.2. Uruchomienie

Po zainstalowaniu oprogramowania trzeba je skonfigurować. Aby konfigurację uprościć przygotowałem indywidualne pliki konfiguracyjne dla każdego. Oprócz podstawowych informacji technicznych (adres serwera, port na którym nasłuchuje) zawierają one klucze i certyfikaty niezbędne do zapewnienia zaszyfrowanego połączenia (i zachowania minimum pewności, że „po drugiej stronie” jest ten serwer, który ma być).

Pliki „rozdam” na zajęciach. Mają one postać `123456.opvn` gdzie 123456 to numer albumu studenta.

W świecie realnych tuneli VPN plik taki powinien być strzeżony jak oko w głowie i nie powinien być nigdy przesyłany nieszyfrowanym kanałem. W naszym przypadku — tylko i wyłącznie do testów — nie będzie to takie istotne (tym bardziej, że tunel będzie działał przez krótki czas).

5.3. Ubuntu

Plik wgrywamy „gdziekolwiek" (na przykład do kartoteki `\$HOME`). Następnie musimy poddać go edycji. Szukamy linijek

```
# script-security 2
# up /etc/openvpn/update-resolv-conf
# down /etc/openvpn/update-resolv-conf
```

i usuwamy znak # (i odstęp), żeby uzyskać:

```
script-security 2
up /etc/openvpn/update-resolv-conf
down /etc/openvpn/update-resolv-conf
```

Zapisujemy i wychodzimy z edytora.

W starszych wersjach systemu Ubuntu:

— Tunel uruchamiamy poleceniem
`sudo openvpn --config 123456.opvn`
(123456 trzeba zastąpić własnym numerkiem.) Potrzebne będzie hasło administratora ~~(w laboratorium dostarczam w miarę potrzeb)~~. Kończymy pracę naciskając Ctrl-C w oknie terminala, w którym byłą uruchomiona aplikacja.

— W wersji najnowszej systemu wchodzimy w konfigurację połączeń sieciowych, dodajemy połączenie VPN i wybieramy opcję import z pliku. Wskazujemy otrzymany plik. Integruje się z Menedżerem Sieci.

5.4. Windows

Po zainstalowaniu oprogramowania (potrzebne są uprawnienia administratora) plik konfiguracyjny trzeba skopiować do kartoteki

`C:\ProgramFiles\OpenVPN\config`. Po uruchomieniu program będzie go tam znajdował. Program musi być uruchamiany w trybie administratora (po kliknięciu prawym klawiszem myszy na ikonie „uruchom jako administrator" czy jakoś tak).

Można tak wszystko skonfigurować, żeby program zawsze był uruchamiany z prawami administratora (po kliknięciu). Trzeba kliknąć prawym klawiszem myszy na ikonę programu, wybrać Właściwości i w zakładce „Zgodność"[2] wybieramy zmień ustawienia dla wszystkich użytkowników, a w kolejnym oknie zaznaczamy uruchom program jako administrator.

Każdorazowe uruchomienie programu będzie związane z pytaniem, czy chcesz by program wprowadził zmiany na komputerze. Program ląduje w zasobniku systemowym, ale nie uruchamia połączenia. Trzeba wskazać go i prawym klawiszem myszy wybrać odpowiednią pozycję menu (123456)[3] i wybrać Connect/Połącz.

Podobnie kończy się połączenie.

Uwaga 1: Ze względów oczywistych (nie posiadam komputera z Windows) nie mogłem tego przetrenować i sprawdzić.

Uwaga 2: Po zakończonych zajęciach należy usunąć plik konfiguracyjny z kartoteki `C:\ProgramFiles\OpenVPN\config`. To, niestety, są komputery publiczne.

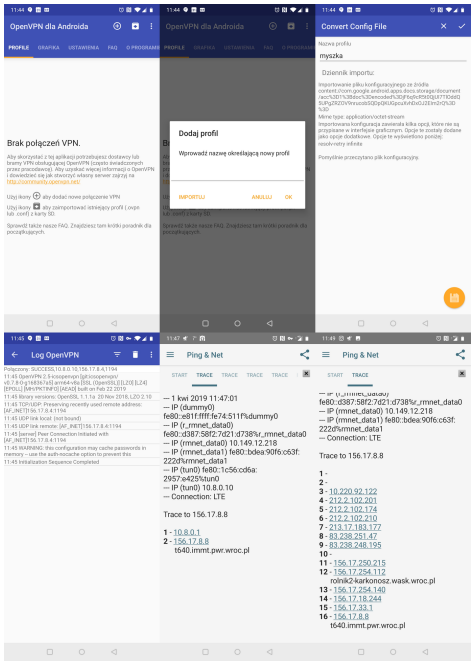
5.5. Android

Plik konfiguracyjny najlepiej wgrać do telefonu kabelkiem USB (i zapamiętać gdzie on jest).

Uruchamiamy aplikację i czytamy, że Brak połączeń VPN, klikamy folderek, ze strzałeczką, żeby zaimportować konfigurację i wybieramy plik `.ovpn` żeby go wczytać. Plik jest cztany, konwertowany, można nadać nazwę profilowi (proponowana jest nazwa zgodna z numerem

[2] Tłumaczę z angielskiego i nie mam możliwości sprawdzić jak to będzie po naszemu.

[3] Tu będzie numer albumu.



Rysunek 1. OpenVPN na Androidzie

albumu). Zapisujemy klikając w pomarańczową ikonę w prawym dolnym rogu.

Po kliknięciu w nazwę profilu łączy z siecią. Można oglądać jakieś wykresy ruchu.

Kolejne zrzuty ekranu przedstawiają pracę aplikacji (wraz z wykresem statystyk), wynik działania programu śledzącego trasę pakietów do serwera komputera w sieci katedralnej (156.17.8.8) z VPN i bez VPN.

6. Zadania do wykonania

Na początek ogromna prośba: nie nadużywajcie VPN.

1. Zajęcia wykonywane w domu[4] korzystając z komputera i/lub telefonu komórkowego[5].
2. Obejrzeć dokładnie otrzymany plik konfiguracyjny i przygotować pytania (na wykład?) o niezrozumiałe[6]
3. Wybrać sobie jakiś węzeł w sieci i sprawdzić połączenie[7] „normalne” i VPN
4. Sprawdzić czas ping do wybranego serwera: VPN vs normalnie.
5. Skorzystać z jakichś usług dostępnych jedynie wewnątrz sieci PWr (na przykład `http://intranet.pwr.edu.pl/doc/Docs.aspx?page=ordinance`).
   Można też wejść na stronę Biblioteki Głównej Politechniki Wrocławskiej i poszukać jakiegoś czasopisma w dziale Lista e-Źródła A-Z.
   Tu przykład artykułu: `https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8353801`.
6. Można przetestować speedtest, ale zwracam uwagę, że połączenie zawsze wychodzi przez łącze „domowe”, dodatkowo jest szyfrowane i kapsułkowane do UDP, więc nie będzie szybciej. Pytanie ile będzie wolniej.

   Tym razem proszę o krótkie sprawozdanie!

7. Uwagi

VPN może przydać się w bardzo różnych sytuacjach. Ale gdy znajdziemy się w sieci, w które cały ruch jest filtrowany — nie uzyskamy możliwości kontaktu z serwerem i nawiązania połączenia. Stąd bardzo

[4] W warunkach laboratorium wszystko będzie znacznie mniej spektakularne: jest ono w sieci PWr.

[5] Instrukcje dla IOS i OSX znaleźć można na osobnej stronie.

[6] Plik jest sformatowany dla linuksa, zwykły Notatnik może mieć problemy, ale Wordpad powinien sobie poradzić po zmianie rozszerzenia z opvn na txt. Zawsze zostaje jakiś inny, dobry edytor: na przykład Notepad++.

[7] Za pomocą jakiegoś programu do śledzenia trasy: tracert, aplikacja pod Android albo Windows.

często serwer korzysta z portu 443 — przeznaczonego dla bezpiecznych połączeń po HTTPS...

8. Dodatkowe źródła informacji

1. Microsoft udostępnia sporo różnych informacji na temat VPN: Virtual Private Networks
   a tam
2. Common configuration for the VPN server
3. Struktura sieci i metody projektowania z wykorzystanie IPSEC, PKI, SSL
4. Dokumentacja OpenVPN
   Instrukcja laboratoryjna zostałą opracowana na podstawie:
5. How To Set Up an OpenVPN Server on Ubuntu 16.04
   oraz
6. Keijser, J. J.: OpenVPN Cookbook, Packt Publishing Ltd., 2017
7. Bardzo dobry tekst na temat VPNa (i TORa) w czasach zarazy: Czym różni się VPN firmowy od komercyjnego ... i dlaczego nie TOR? z serwisu Niebezpiecznik.

9. Instrukcja w postaci jednego pliku...

...jest również dostępna.