ZAKŁAD SYSTEMÓW ZŁOŻONYCH
Politechnika Rzeszowska

BEZPIECZEŃSTWO SYSTEMÓW KOMPUTEROWYCH

Temat 6:

Konfigurowanie bezpiecznych połączeń sieciowych z wykorzystaniem technologii VPN

Cel:

Celem ćwiczenia jest zestawienie bezpiecznego połączenia sieciowego VPN, opartego na systemie Windows i aplikacji OpenVPN.

Wstęp teoretyczny

Wirtualne Sieci Prywatne (Virtual Private Network) to technika realizacji sieci prywatnej w ramach dostępnej sieci publicznej. Polega ona na utworzeniu tunelu przez co klienci końcowi „nie widzą" węzłów sieci – tak jakby byli podłączeni bezpośrednio do siebie.

OpenVPN to pakiet VPN stworzony przez Jamesa Yonana. Umożliwia on tworzenie zaszyfrowanych połączeń między hostami – używa do tego celu biblioteki OpenSSL oraz protokołów SSLv3/TLSv1. W przeciwieństwie do innych rozwiązań VPN nie bazuje na protokole IPsec jako medium. Pakiet ten dostępny jest na platformach Linux, BSD, Mac OS X oraz Windows 2000/XP/Vista. Cały pakiet składa się z jednego kodu binarnego dla klienta i serwera, opcjonalnego pliku konfigurującego oraz z jednego lub więcej plików kluczy w zależności od metody uwierzytelnienia.

Przebieg ćwiczenia:

A. Przygotowanie środowiska do pracy:

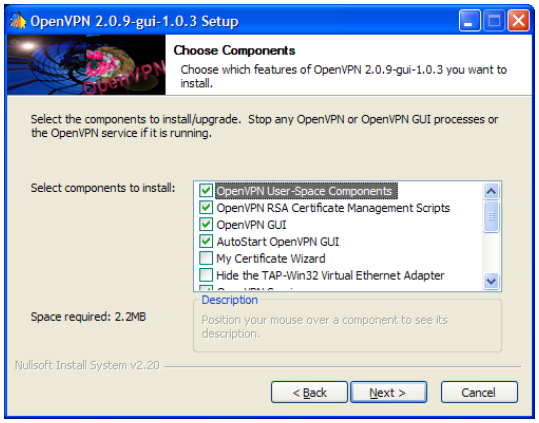
1. Uruchom komputer logując się jako Administrator (hasło wprowadza prowadzący zajęcia).

2. Zainstaluj aplikację OpenVPN, która znajduje się w katalogu *Bezpieczeństwo.*

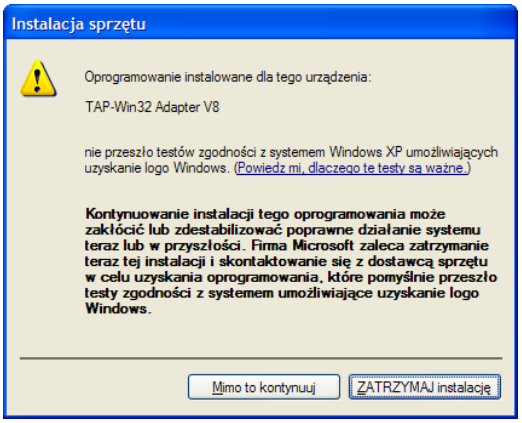
B. Przebieg instalacji OpenVPN

OpenVPN należy zainstalować na każdym z komputerów, które mają zostać połączone w wirtualną sieć.

Po uruchomieniu aplikacji, pojawia się instalator umożliwiający wybór komponentów do zainstalowania. Zainstaluj tylko składniki zaznaczone domyślnie.

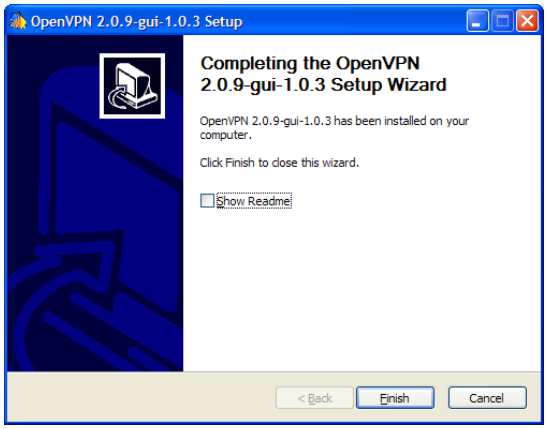


Rys. 1.Instalowanie komponentów

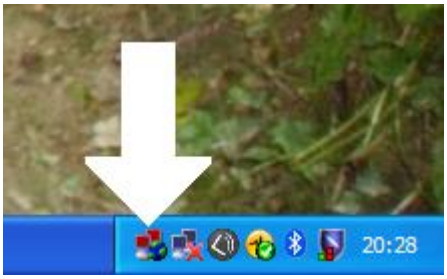


Rys. 2. Instalowanie wirtualnej karty sieciowej

Podczas instalacji *OpenVPN* tworzona jest wirtualna karta sieciowa, której sterownik nie posiada podpisu cyfrowego – po pojawieniu się poniższego komunikatu należy wybrać opcję „Mimo to kontynuuj".
Pomyślne zakończenie instalacji powoduje uruchomienie usługi OpenVPN oraz uruchomienie interfejsu GUI, widocznego w zasobniku systemowym (rys.4).



Rys. 3. Zakończenie instalacji



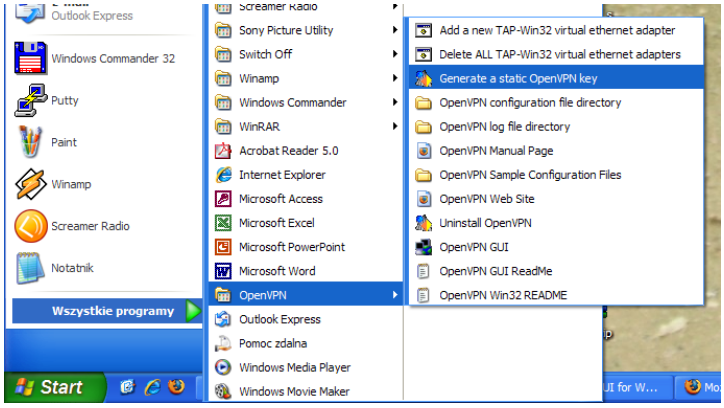
Rys. 4. Uruchomiony interfejs GUI

C. Konfiguracja OpenVPN

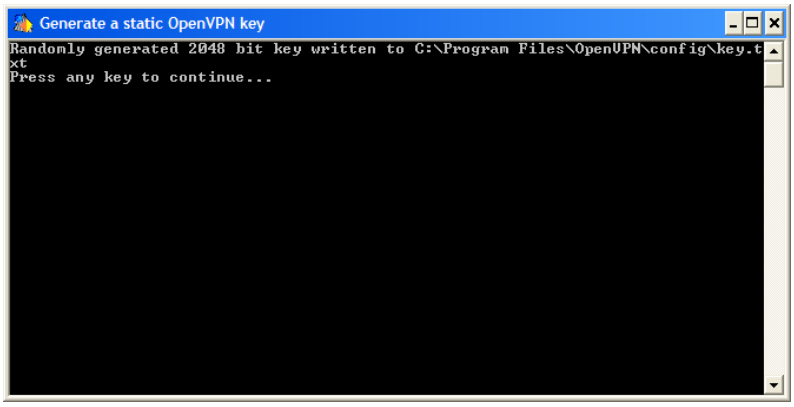
Zrealizuj połączenie wirtualne dwóch komputerów. W tym celu stwórz plik z kluczem statycznym oraz dwa pliki konfiguracyjne dla każdej z maszyn.

1. Tworzenie klucza

Aby utworzyć klucz statyczny należy na **jednym z komputerów** wybrać opcję „Generate a static OpenVPN key" (Menu Start -> Wszystkie programy -> OpenVPN -> Generate a static OpenVPN key).



Rys. 5. Tworzenie klucza



Rys. 6. Utworzony klucz

Klucz zostanie utworzony jako plik „key.txt" w folderze konfiguracji (C:\Program Files\OpenVPN\config\key.txt). **Plik należy skopiować do tego samego folderu na drugiej maszynie!!!!**

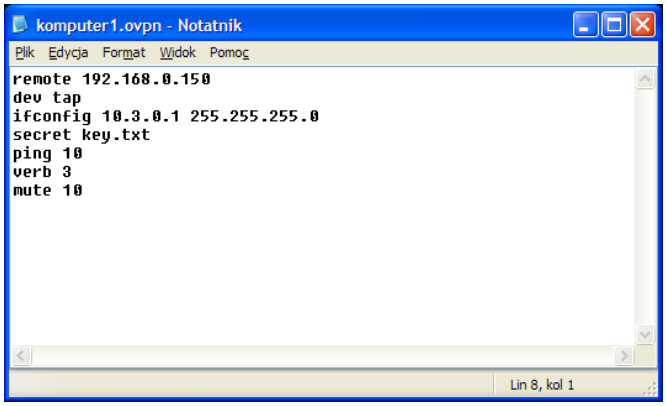
2. Tworzenie pliku konfiguracyjnego dla „komputera 1"

Sprawdź ustawienia karty sieciowej zapisując je do pliku tekstowego. Fizyczna karta sieciowa pierwszego komputera korzysta z adresu IP 192.168.0.X i maski podsieci 255.255.255.0.

W folderze konfiguracji (C:\Program Files\OpenVPN\config\) należy utworzyć plik nazwa.ovpn, w którym będzie znajdować się konfiguracja połączenia – np. „**komputer1.ovpn**" (C:\Program Files\OpenVPN\config\komputer1.ovpn) (rys. 7).

Plik powinien zawierać:

- remote **xxx.xxx.xxx.xxx** – gdzie xxx.xxx.xxx.xxx jest adresem IP ZDALNEGO komputera („komputer 2")
- dev tap – określenie wirtualnego interfejsu, wymagane dla systemów Windows
- ifconfig yyy.yyy.yyy.yyy zzz.zzz.zzz.zzz – gdzie yyy.yyy.yyy.yyy jest wirtualnym adresem IP LOKALNEGO komputera („komputer 1") a zzz.zzz.zzz.zzz wirtualną maską podsieci
- secret key.txt – klucz statyczny
- ping 10
- verb 3
- mute 10

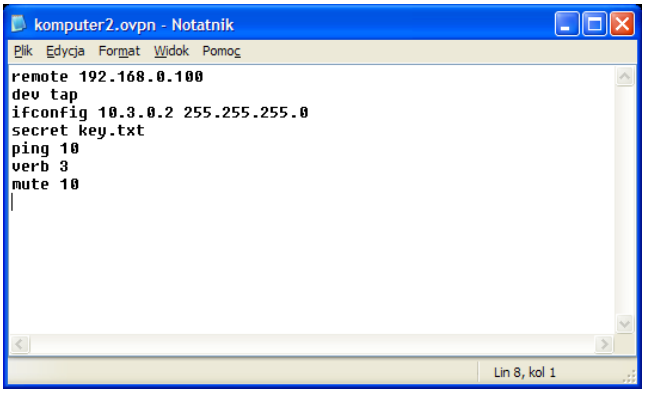


Rys. 7. Konfiguracja OpenVPN komputera 1

3. Tworzenie pliku konfiguracyjnego dla „komputera 2”

Sprawdź ustawienia karty sieciowej komputera 2.

Powtórz czynności konfiguracyjne dla komputera 2. W folderze konfiguracji (C:\Program Files\OpenVPN\config\) należy utworzyć plik nazwa.ovpn, w którym będzie znajdować się konfiguracja połączenia (C:\Program Files\OpenVPN\config\komputer2.ovpn) (rys. 8)



Rys. 8. Konfiguracja OpenVPN komputera 2

4. Uruchomienie połączenia

Jeżeli klucz statyczny i pliki konfiguracyjne są prawidłowo utworzone, wystarczy na każdym z komputerów wybrać opcję „Connect” klikając prawym klawiszem na ikonę GUI programu, widoczną w zasobniku systemowym.
Efektem prawidłowego zestawienia połączeń będzie komunikat „Nazwa_Pliku_Konfiguracyjnego is now connected”.

1. Dokonaj testu stworzonego wirtualnego kanału. W tym celu sprawdź możliwość udostępniana zasobów, np. na „komputerze 2” o wirtualnym adresie IP 10.3.0.2 udostępnij katalog *Bezpieczeństwo.*

2. Dokonaj próby zalogowania się z „komputera 1” do udostępnionych zasobów „komputera 2”.

3. Korzystając z poleceń opisanych w dodatku sprawdź połączenie sieciowe zarówno dla połączenia fizycznego oraz logicznego. Wyniki zapisz do pliku tekstowego. Zastosuj kolejno wszystkie możliwe opcje.

Dodatek:

ping **-** polecenie wysyła komunikaty ICMP Echo Request w celu weryfikacji poprawności konfiguracji protokołu TCP/IP oraz dostępności odległego hosta. Parametry polecenia pozwalają na szczegółowe określenie parametrów wysyłanej ramki. Polecenie w zależności od doboru parametrów może służyć do testowania wydajności sieci przy różnego rodzaju obciążeniu.

Składnia polecenia:

```
ping [-t] [-a] [-n liczba] [-l rozmiar] [-f] [-i TTL] [-v TOS] [-r liczba]
[-s liczba] [[-j lista_hostów] | [-k lista_hostów]] [-w limit_czasu]
lista miejsc docelowych
```

-t - odpytuje określonego hosta do czasu zatrzymania. Aby przejrzeć statystyki i kontynuować, naciśnij klawisze Ctrl+Break. Aby zakończyć, naciśnij klawisze Ctrl+C.
-a - tłumaczy adresy na nazwy hostów.
-n liczba - liczba wysyłanych powtórzeń żądania.
-l rozmiar - rozmiar buforu transmisji.
-f - ustaw w pakiecie flagę "Nie fragmentuj".
-i TTL - czas wygaśnięcia.
-v TOS - typ usługi.
-r liczba - rejestruj trasę dla przeskoków.
-s liczba - sygnatura czasowa dla przeskoków.
-j lista_hostów - swobodna trasa źródłowa wg listy lista_hostów.
-k lista_hostów - ściśle określona trasa źródłowa wg listy lista_hostów.
-w limit_czasu - limit czasu oczekiwania na odpowiedz (w milisekundach).

Przykłady:

- `PING -n 1 -w 7500 Server_06`

Wysyła jedno zapytanie do Server_06 i czeka 7,5 sekundy na odpowiedz

- `PING -w 7500 MyHost |find "TTL=" && ECHO MyHost found`

Sprawdza istnienie MyHost

- `PING -a 212.97.202.142`

Sprawdza adres domenowy hosta

tracert **-** umożliwia śledzenie ścieżki do docelowego systemu.

Składnia polecenia:

```
tracert [-d] [-h maks_przes] [-j lista_hostów] [-w limit_czasu] cel
```

-d - nie pobieraj nazw hostów używając adresów.
-h maks_przes - maksymalna liczba przeskoków w poszukiwaniu celu.
-j lista_hostów - swobodna trasa źródłowa według listy lista_hostów.
-w limit_czasu - limit czasu oczekiwania na odpowiedz w milisekundach.]

Przykłady:

- `TRACERT www.onet.pl`
- `TRACERT 123.45.67.89`

Pathping - umożliwia śledzenie ścieżki do docelowego systemu oraz raportowanie utraty pakietów w każdym z routerów znajdującym sie w tej ścieżce.

Składnia polecenia:

```
pathping [-n] [-h maks_liczba_przeskoków] [-g lista_hostów] [-p okres][-q
liczba_kwerend] [-w limit_czasu] [-t] [-R] [-r] nazwa_docelowa
```

-n - nie tłumacz adresów na nazwy hostów.
-h maks_liczba_przesk - maksymalna liczba przeskoków w poszukiwaniu celu.
-g lista_hostów - swobodna trasa z uwzględnieniem listy_hostów.
-p okres - okres oczekiwania (w milisekundach) miedzy odpytaniami.
-q liczba_kwerend - liczba kwerend na jeden przeskok.
-w limit_czasu - maksymalny limit czasu (w milisekundach) oczekiwania na poszczególne odpowiedzi.
-T - przetestuj przeskoki (zdolność nawiązania połączenia) zgodnie ze znacznikami priorytetów Warstwy-2.
-R - przetestuj, czy każde miejsce, do którego następuje przeskok, jest zgodne z RSVP.

***netstat* -** wyświetla statystyki protokołu i bieżące połączenia sieciowe TCP/IP.

Składnia polecenia:

```
netstat [-a] [-e] [-n] [-s] [-p protokół] [-r] [odstęp]
```

-a - wyświetla wszystkie połączenia i porty oczekujące.
-e - wyświetla statystyki Ethernet-u. Ta opcja może być używana razem z opcja -s.
-n - wyświetla adresy i numery portów w postaci liczbowej.
-p protokół - wyświetla połączenia dla określonego protokołu; może to być protokół TCP lub UDP. Jeżeli ta opcja użyta jest razem z opcja -s, do wyświetlenia wybranego protokołu, protokół może mieć wartość TCP, UDP lub IP.
-r - wyświetla tabele routingu.
-s - wyświetla statystykę wybranego protokołu. Domyślnie jest to statystyka protokołów TCP, UDP i IP; opcja -p może być użyta do określenia podzbioru domyślnego.
odstęp - wyświetla wybrana statystykę, odczekując zadaną ilość sekund pomiędzy każdym wyświetleniem. Naciśnij klawisze CTRL+C, aby przerwać wyświetlanie statystyk. Jeżeli ta zmienna nie zostanie określona, program netstat wydrukuje raz informacje o konfiguracji.