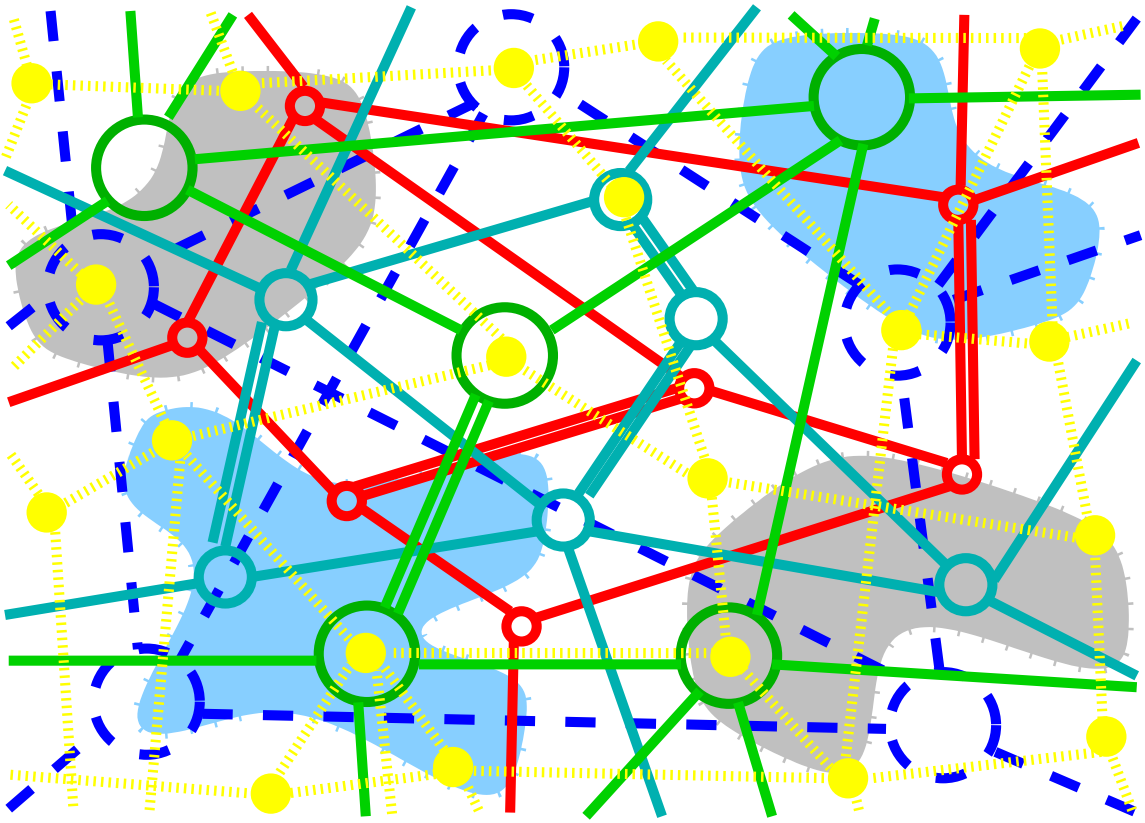
# Instrukcja do laboratorium sieci komputerowych

**Wirtualne sieci prywatne**

**dr inż. Piotr Arabas** **mgr inż. Jerzy Sobczyk** **dr inż. Edward Śliwa**



**9 września 2024**

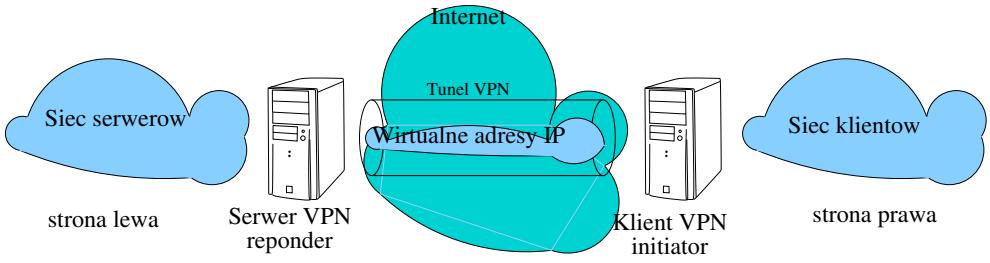
# 9 Ćwiczenie 9 Konfigurowanie wirtualnych sieci prywatnych

## Wstęp

Ćwiczenie to jest wykonywane przez dwa, współpracujące ze sobą, zespoły dwuosobowe, z których każdy konfiguruje jeden router MikroTik.

## 9.1 Cel ćwiczenia

Celem ćwiczenia jest praktyczne zapoznanie się z techniką wirtualnych sieci prywatnych.




Rysunek 23: Zasada działania sieci VPN

Tunel VPN tworzony jest pomiedzy dwoma komputerami/routerami w celu bezpiecznego przysyłania danych pomiedzy serwerami i komputerami klienckimi tej samej instytucji. Urządzenia będące końcami tunelu nawiązuja połączenie przy pomocy specjalnego protokołu (IPSec, OpenVPN, PPTP, SSTP, L2TP, ...). Poprzez to połączenie przesyłają zaszyfrowane pakiety pomiedzy komputerami klienckimi i serwerami. Ani komputery klienckie ani serwery nie muszą nic wiedzieć o istnieniu połączenia VPN. Połączenie VPN zwane jest tunelem i dla ułatwienia sterowania ruchem pakietów czesto otrzymuje swoje wirtualne adresy IP. W ten sposób z poziomu routingu IP tunel jest po prostu jednym segementem IP.

## 9.2 Przebieg ćwiczenia

Cwiczenie składa się z czterech etapów.

1. Konfiguracja routingu.

   Każdy z zespołów konfiguruje swój router tak aby umożliwić połączenia pomiędzy maszynami Net?1, Net?2, Net?3, Net?4.

   Nie należy wykonywać routingu dla sieci `192.168.2?6.0/24` i `192.168.2?7.0/24`.

2. Konfiguracja tunelu IPSec.

   Router `rtr?3` należy skonfigurować jako klienta (ang. initiator) tunelu IPSec, którego drugim końcem będzie maszyna `Net?2`. Na tej maszynie należy skonfigurować program `StrongSwan` do roli servera (ang. responder). Do testowania poprawności działania tunelu można wykorzystać adresy: `192.168.2?6.1` `192.168.2?6.2` `192.168.2?6.10`. dostepne poprzez interfejs `et1` komputera `Net?2`.

3. Rejestracja pakietów w połaczniu przez IPSec.

   Na routerze `rtr?1` należy uruchomić rejestrowanie pakietów i w tym czasie wykonać krótkie połączenie pomiędzy maszynami. Należy zapisać zarejestrowaną sekwencję pakietów. W tym samym czasie należy też rejestrować pakiety na interfejsach `et1` i `et2` komputera `Net?2`.

4. Konfiguracja tunelu OpenVPN.

   Router `rtr?1` należy skonfigurować jako klienta (ang. initiator) tunelu OpenVPN, którego drugim końcem będzie maszyna `Net?3`. Na tej maszynie należy skonfigurować program `SoftEther` do roli servera (ang. responder). Do testowania poprawności działania tunelu można wykorzystać adresy: `192.168.2?7.1` `192.168.2?7.2` `192.168.2?7.10`. podłączone do interfejsu `et2` komputera `Net?3`.

5. Rejestracja pakietów w połaczniu przez OpenVPN.

   Na routerze `rtr?3` należy uruchomić rejestrowanie pakietów i w tym czasie wykonać krótkie połączenie pomiędzy maszynami. Należy zapisać zarejestrowaną sekwencję pakietów. W tym samym czasie należy też rejestrować pakiety na interfejsach `et1` i `et2` komputera `Net?3`.

6. Konfiguracja ściany ogniowej dla IPSec.

   Na routerze `rtr?1` należy skonfigurować ścianę ogniową tak aby przepuszczała wszystkie pakiety z komputerów `Net?1` i `Net?2` oraz sieci `192.168.2?6.0/24`. Natomiast blokowała ruch w przeciwnym kierunku przepuszczając jedynie pakiety obu tuneli VPN (IPSec i OpenVPN).

7. Konfiguracja ściany ogniowej dla OpenVPN.

   Na routerze `rtr?3` należy skonfigurować ścianę ogniową tak aby przepuszczała wszystkie pakiety z komputerów `Net?3` i `Net?4` oraz sieci `192.168.2?7.0/24`. Natomiast blokowała ruch w przeciwnym kierunku przepuszczając jedynie pakiety obu tuneli VPN (IPSec i OpenVPN).

## 9.3 Sprawozdanie

Sprawozdanie powinno zawierać:

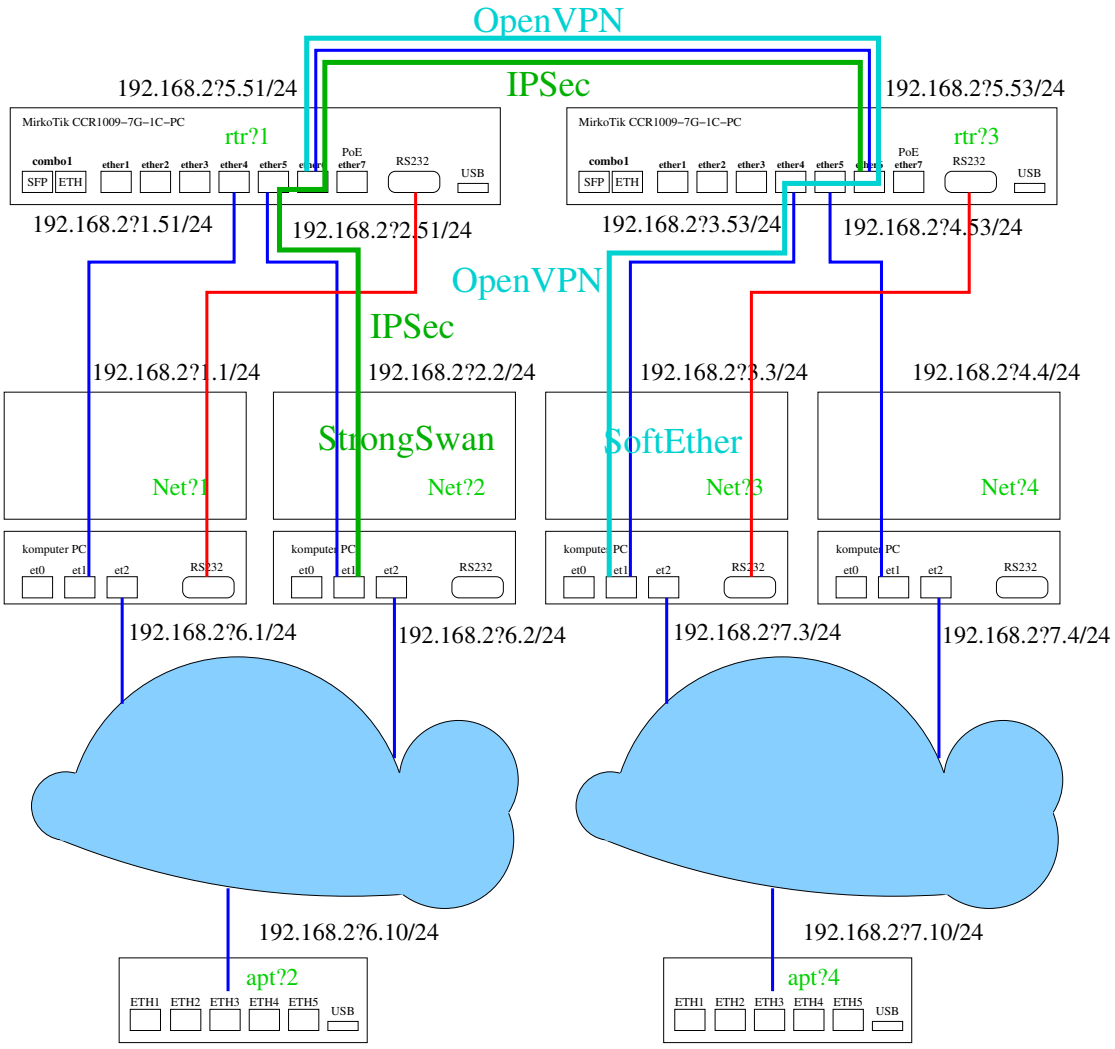
- Listę poleceń (wraz z wartościami parametrów) użytych do skonfigurowania każdego z routerów.
- Sekwencje pakietów zarejstrowanych w etapach 3 i 5. Należy wskazać istotne różnice zaobserwowane w sekwencjach zarejestrowanych na poszczególych interfejsach.
- Wyjaśnienia problemów i odpowiedzi na pytania zawarte w opisach etapów.
- Uwagi na temat problemów napotkanych w trakcie wykonywania ćwiczenia.

## 9.4 Szczegóły techniczne

Schemat połaczeń znaduje sie na rysunku 24. W ramach ćwiczenia tworzone są dwie sieci VPN których klientami sa routery MikroTik a serweremi wskazane komputery laboratoryjne. Połączenia te "idą" w przeciwnych kierynkach dlatego należy zwrócić uwagę na lokalizację serwera i klientów danego protokołu.

## 9.5 Zalecenia

1. Należy pamietać aby przy konfigurowaniu tunelu w obu końcach użyć tego samego klucza.
2. Aby połaczenie mogło zostać nawiązane wśród proponowanych metod szyfrowania muszą występować metody stosowane przez drugą stronę połaczenia.
3. Konfigurując połaczenie IPSec należy zastosować dwukrotną translacje adresów: na na kliencie (rtr1 *?*3 i serwerze Net *?*2.




Rysunek 24: Schemat połączeń ćwiczenia 9

## 9.6 Przydatne polecenia

### 9.6.1 Router MikroTik

| Polecenia routera MikroTik | |
|---|---|
| `/ip address print` | wyświetlenie konfiguracji adresów |
| `/ip address add address=`*adres_IP* `interface=`*interfejs* | dodanie adresu do interfejsu |
| `/ip route dst-address=`*adres_sieci* `gateway=`*adres_routera* | Dodanie trasy do sieci poprzez router. |
| `/tool sniffer start` | Rozpoczęcie rejestrowania pakietów. |
| `/tool sniffer stop` | Zakończenie rejestrowania pakietów. |
| `/tool sniffer pakcet print detail` | Wyświetlenie zarejestrowanej sekwencji pakietów. |
| `/ip ipsec profile add name=`*nazwa_profilu* `dh-group=`*metoda_wymiany_kluczy* `enc-algorithm=`*metoda_szyfrowania* | Utworzenie profilu. |
| `/ip ipsec proposal add name=`*nazwa_propozycji* `enc-algorithms=`*algorytmy_szyfrowania* `pfs-group=`*metoda_wymiany_kluczy* | Utworzenie propozycji paramatrów połączenia oferowanych drugiemu routerowi. |
| `/ip ipsec peer add name=`*nazwa_drugiego_route* `address=`*adres_drugiego_routera* `profile=`*nazwa_profilu* | Zdefiniowanie drugiego końca tunelu. |
| `/ip ipsec identity peer=`*nazwa_drugiego_route* `secret=`*wspólny_klucz* | Zdefiniowanie wspólnego klucza do szyfrowania komunikacji. |
| `/ip ipsec policy add peer=`*nazwa_drugiego_routera* `src-address=`*adres_sieci_1* `dst-address=`*adres_sieci_2* `src-port=any dst-port=any tunnel=yes action=encrypt proposal=`*nazwa_propozycji* `peer=`*nazwa_dugiego_routera* | Zdefiniowanie polityki decydujacej o tym, które pakiety będa podlegały tunelowaniu. |
| `/ip ipsec active-peers print` | Wyświetlenie aktywnych połaczeń tunelowych. |
| `/ip ipsec installed-sa print` | Wyświetlenie aktywnych skojarzeń kluczy. Dla działającego połączenia powinny być wyświetlone dwa skojarzenia oznaczone flagami HE. |
| `/ppp profile add name=`*nazwa_profilu* `change-tcp-mss=yes only-one=yes use-encryption=required use-mpls=no` | Definicja profilu PPP. |
| `/interface ovpn-client add name=`*nazwa_interfejsu* `connect-to=`*IP_serwera* `profile=`*nazwa_profilu_ppp* `user=`*login@hub* `password=`*hasło* | Utworzenie interfejsu OpenVPN. |
| `/interface ovpn-client print` | Wyświetleie interfejsów OpenVPN. Przy działającym interfejsie powinna być wyświetlona litera **R** - running. |
| **https://wiki.mikrotik.com/wiki/Manual:TOC** | |

| Polecenia routera MikroTik cd. | |
|---|---|
| `/ip firewall nat add action=masquerade chain=srcnat out-interface=` ***nazwa_interfejsu*** | Włączenie translacji adresów (maskarady) dla wskazanego interfejsu. |
| `/ip firewall filter add action=`***akcja*** `chain=`***łańcuch*** `in-interface=`***nazwa_interfejsu*** `dst-port=`***porty_docelowe*** `protocol=`***protokół*** `src-address=`***adresy_nadawców*** `dst-address=`***adresy_odbiorców*** `chain=`***łańcuch*** | Dodanie reguły filtracji pakietów do wybranego łańcucha (input, forward, output) z wybraną akcją (accept, drop, reject, jump, ...) spełniajacych wpisane kryteria. |
| `/ip firewall filter print` | Wyświetlenie listy reguł. |
| `/ip firewall filter move` ***nr_reguły pozycja_docelowa*** | Przeniesienie wybranej reguły na wskazaną pozycję. Reguła zajmująca tę pozycje i następujące po niej są przesuwane na kolejne pozycje. |
| **https://wiki.mikrotik.com/wiki/Manual:TOC** | |

### 9.6.2 Program StrongSwan

Program jest już zainstalowany w systemie ale jego użycie wymaga praw administratora więc należy korzystać z polecenia `sudo`.

| Polecenia programu StrongSwan (IPSec) | |
|---|---|
| `sudo ipsec start` | Uruchomienie serwera IPSec |
| `sudo ipsec stop` | Zatrzymanie serwera IPSec |
| `sudo ipsec restart` | Zatrzymanie i uruchomienie serwera IPSec |
| `sudo ipsec status` | Wyświetlenie stanu połączenia IPSec |
| `sudo ipsec ststusall` | Wyświetlenie pełnego stanu serwera IPSec |
| `tail /var/log/syslog` | Wyświetlenie końcówki pliku logów. |
| **https://docs.strongswan.org/docs/5.9/index.html** | |

**Plik ipsec.config**

```
conn nazwa_połączenia
                opcja1=wartość1
                opcja2=wartość2
                opcja3=wartość3
```

| Opcje pliku `ipsec.conf` | |
|---|---|
| `authby=`*metoda* | Matoda autoryzacji końców tunelu (zalecana `secret`). |
| `ike=`*szyfr1, szyfr2, ...* | Metody szyfrowania dla protokołu IKE (zalecane `aes256-sha2_256-modp2048`). |
| `esp=`*szyfr1, szyfr2, ...* | Metdy szyfrowania dla (zalecane `aes256-sha256-modp4096`). |
| `ikelifetime=`*czas* | Czas użytkowania kluczy protokołu IKE. Po tym czasie muszą być automatycznie zastąpione nowymi. |
| `keyingtries=`*liczba* | Ilość prób negocjacji parametrów połączenia. |
| `keyexchange=`*ike—ike1—ike2* | Wersja protokołu IKE (zalecane `ikev2`). |
| `mobike=`*yes—no* | Czy proponować protokół MOBIKE? (zalecane `no`) |
| `left=`*IP* | Adres IP serwera. |
| `leftid=`*tekst* | Identyfikator serwera do autentykacji. |
| `leftsubnet=`*zakres_IP* | Adres sieci serwerów usług. |
| `leftfirewall=`*yes—no* | Czy serwer filtruje ruch (wliczając funkcję NAT). |
| `right=`*IP* | Adres klienta. |
| `rightsubnet=`*zakres_IP* | Adres sieci klientów. |
| `auto=`*operacja* | Co zrobić z połączeniem przy starcie serwera? (zalecane `add`). |
| `leftsourceip=`*IP* | Wirtualny adres IP serwera wykorzystywany w trakcie połączenia. |
| `rightsourceip=`*zakres_IP* | Zakres wirtualnych adresów IP używanych w trakcie połączenia. Jeden z nich zostanie przyznany klientowi po nawiązaniu połączenia. |
| **https://wiki.strongswan.org/projects/strongswan/wiki/Connsection** | |

**Plik ipsec.secrets**

```
serwer klient : PSK "sekret"
: PSK "sekret"
```

| Elementy pliku `ipsec.secrets` | |
|---|---|
| *serwer* | Adres IP serwera tunelu IPSec. |
| *klient* | Adres IP klienta tunelu IPSec. |
| *sekret* | Hasło używane do aytentykacji drugiego końca tunelu IPSec. |
| **https://wiki.strongswan.org/projects/strongswan/wiki/Ipsecsecrets** | |

### 9.6.3 Program SoftEther

Program znajduje się w podkatalogu: `vpnserwer` katalogu domowego użytkownika `student`. Program należy uruchamiac z prawami uzytkownika `student`.

| Polecenia prograu SoftEther | |
|---|---|
| `./vpnserver start` | Uruchomienie serwera SoftEther |
| `./vpnserver stop` | Zatrzymanie serwera SoftEther |
| `./vpncmd start` | Uruchomienie interfejsu komend programu SoftEther. Jako adres serwera należy podać: 127.0.0.1:5555 |
| **https://www.softether.org/4-docs/1-manual/6** | |

| Wybrane polecenia prograu vpncmd | |
|---|---|
| `ServerPasswordSet` | Ustawienie hasła serwera. |
| `HubCreate` | Utworzenie wirtualnego huba. |
| `Hub` ***nazwa*** | Przejście do zarządzania wskazanym hubem wirtualnym. |
| `GroupCreate` | Utworzenie grupy użytkowników. |
| `UserPasswordSet` | Ustawienie hasła użytkownika. |
| `SecureNatEnable` | Włączenie translatora adresów.. |
| `OpenVpnEnable` | Włączenie serwera protokołu OpenVPN. |
| `DhcpSet` | Ustawienie parametrów serwera DHCP. |
| `DhcpGet` | Wyświetlenie parametrów serwera DHCP. |
| `SecureNatHostSet` | Ustawienie adresów translatora adresów. |
| `ConnectionList` | Wyświetlenie listy aktywnych połączeń. |
| **https://www.softether.org/4-docs/1-manual/6** | |

### 9.6.4 Przydatne strony

https://www.tecmint.com/setup-ipsec-vpn-with-strongswan-on-debian-ubuntu/

https://bidhankhatri.com.np/vpn/site-to-site-vpn-between-mikrotik-router-and-ubuntu-22.04-through-strongswan-using-ipsec-ikev2/

https://www.strongswan.org/testing/testresults/ikev2-stroke/net2net-psk/