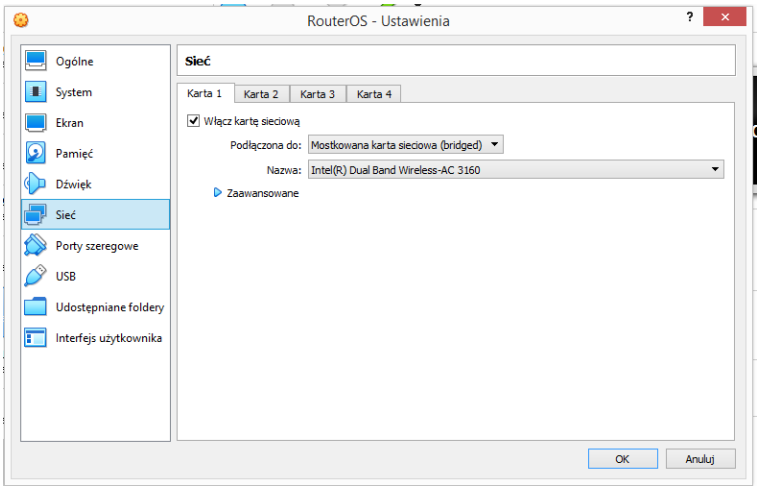
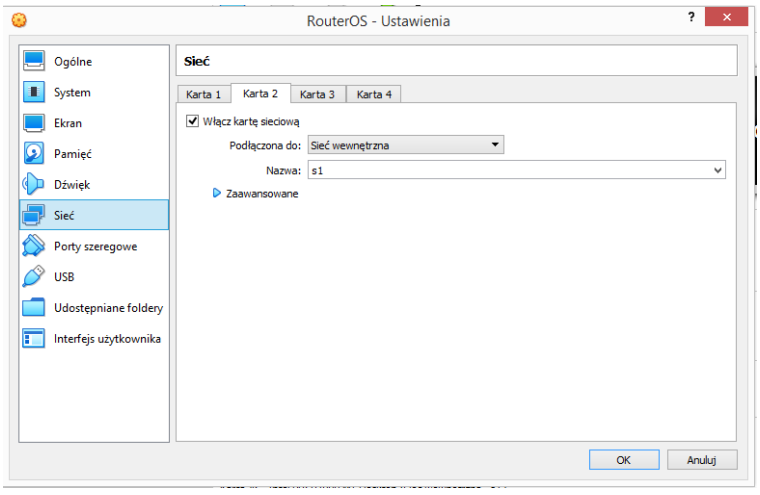
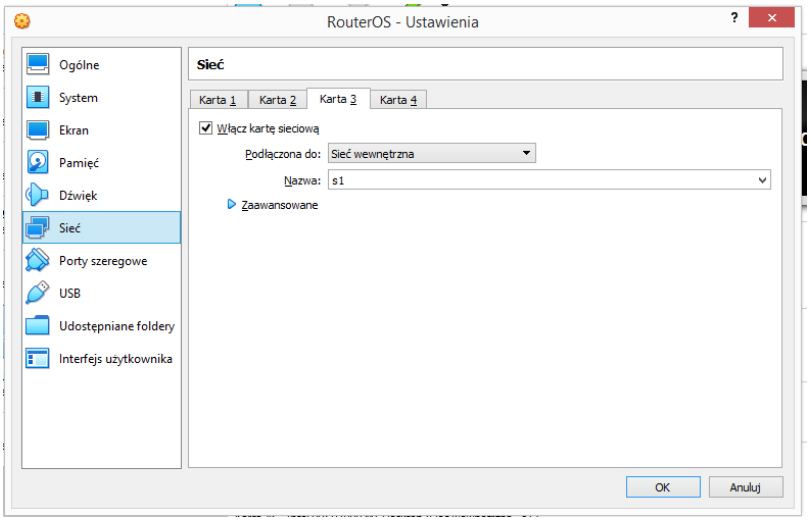
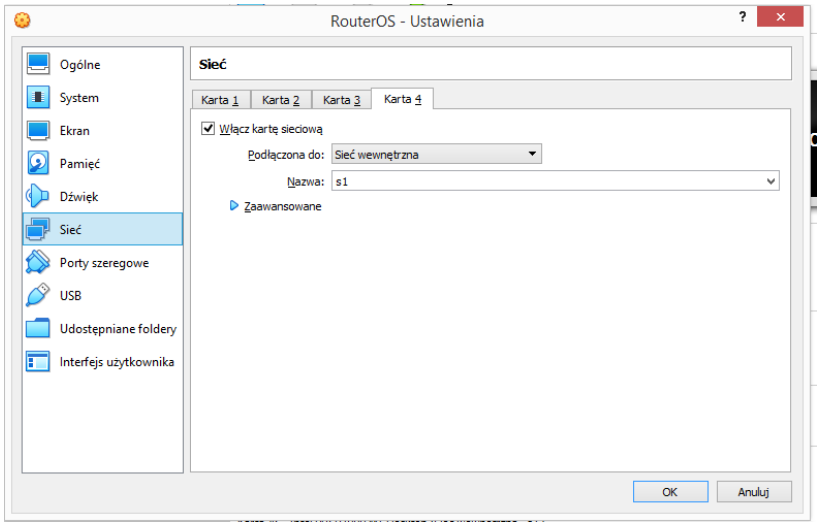
Konfiguracja połączenia VPN z wykorzystaniem protokołu L2TP IPSec na przykładzie routera Mikrotik

Wstępna konfiguracja RouterOS w Virtualbox:



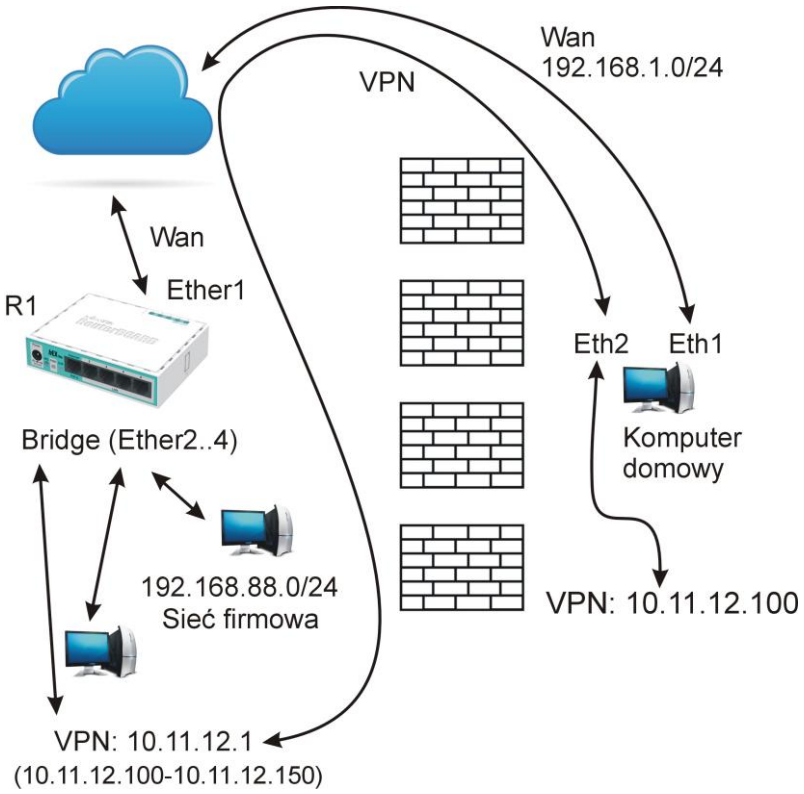



RouterOS - Ustawienia
Ogólne
System
Ekran
Pamięć
Dźwięk
Sieć
Porty szeregowe
USB
Udostępniane foldery
Interfejs użytkownika
Sieć
Karta 1
Karta 2
Karta 3
Karta 4
Włącz kartę sieciową
Podłączona do:
Sieć wewnętrzna
Nazwa:
s1
Zaawansowane
OK
Anuluj


RouterOS - Ustawienia
Ogólne
System
Ekran
Pamięć
Dźwięk
Sieć
Porty szeregowe
USB
Udostępniane foldery
Interfejs użytkownika
Sieć
Karta 1
Karta 2
Karta 3
Karta 4
Włącz kartę sieciową
Podłączona do:
Sieć wewnętrzna
Nazwa:
s1
Zaawansowane
OK
Anuluj

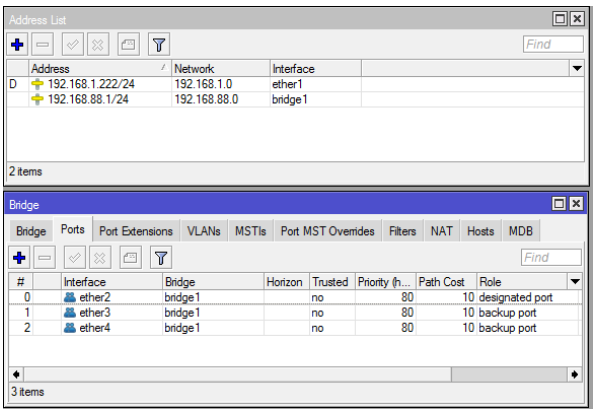
Topologia sieci

W przedstawionej konfiguracji występują dwie sieci, sieć publiczna oraz sieć prywatna. Szczegóły topologii zostały przedstawione na poniższym rysunku.



Konfiguracja VPN

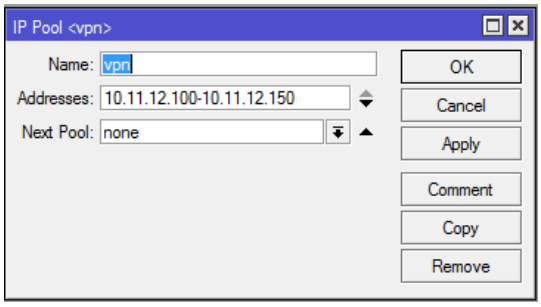
Ustawiamy interfejsy sieciowe wg. poniższej konfiguracji:



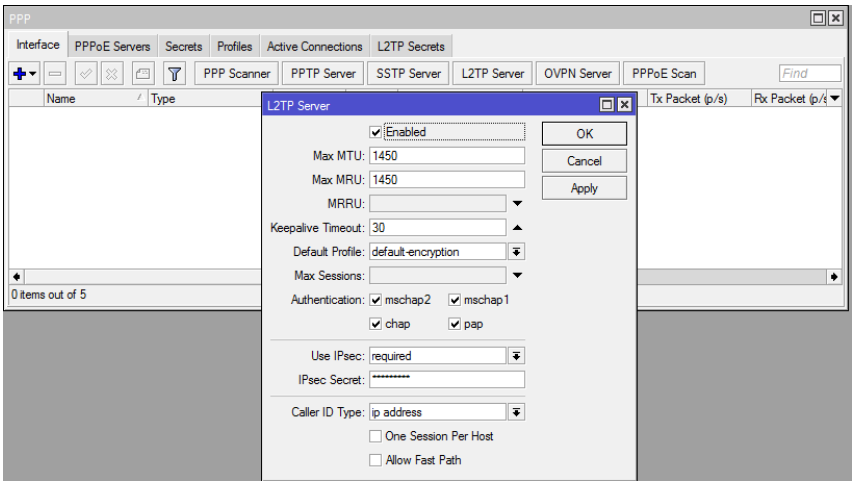
Interfejs ether1 jest podłączony do sieci WAN, i jest automatycznie konfigurowany przez DHCP dostawcy internetu.

Interfejs bridge zapewnia połączenia wewnątrz firmy, jest to sieć prywatna. Komputery w tej sieci uzyskują automatycznie adres z zakresu 192.168.88.2 - 192.168.88.254.

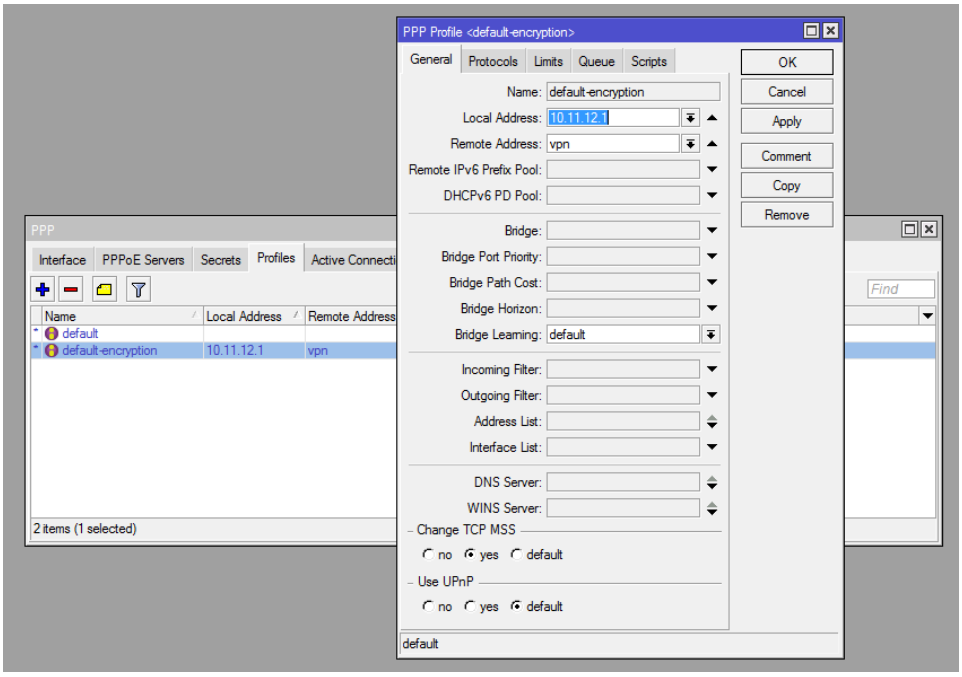
Ustalamy zakres adresów IP, jakie będą mogły być przydzielane w ramach połączenia VPN. W tym celu ustalamy pulę 50 adresów z zakresu 10.11.12.100 - 10.11.12.150.



W następnym kroku włączamy usługę L2TP Server, wybierając z menu PPP zakładkę Interface i pozycję L2TP Server:

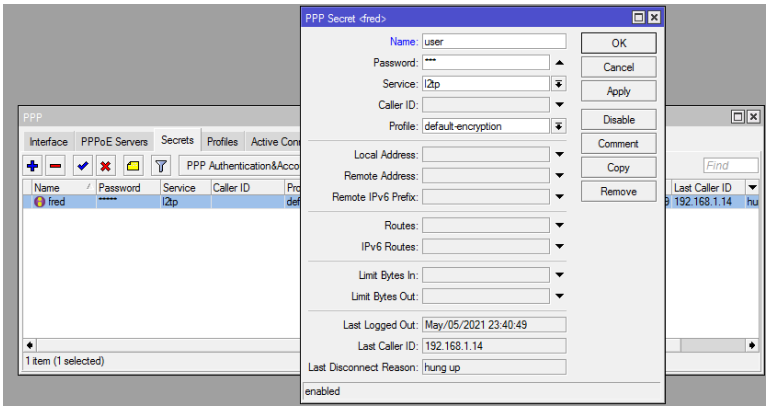


Zalecane jest włączenie opcji "Use IPsec" na required i podanie hasła. Typ autentykacji należy dobrać do środowiska, w jaki będą pracowały komputery korzystające z VPN. Profil szyfrowania możemy ustawić w pozycji "Default Profile". Można pozostawić domyślny, który zostanie zmodyfikowany w kolejnym kroku.



W domyślnym profilu PPP ustawiamy adres IP, który będzie bramą dla klientów poprawnie zalogowanych serwera. Przydzielony adres będzie pochodził z puli o nazwie "vpn".

W ostatnim kroku dodajemy użytkownika, za pomocą którego będzie można utworzyć połączenie VPN z siecią prywatną (firmową).

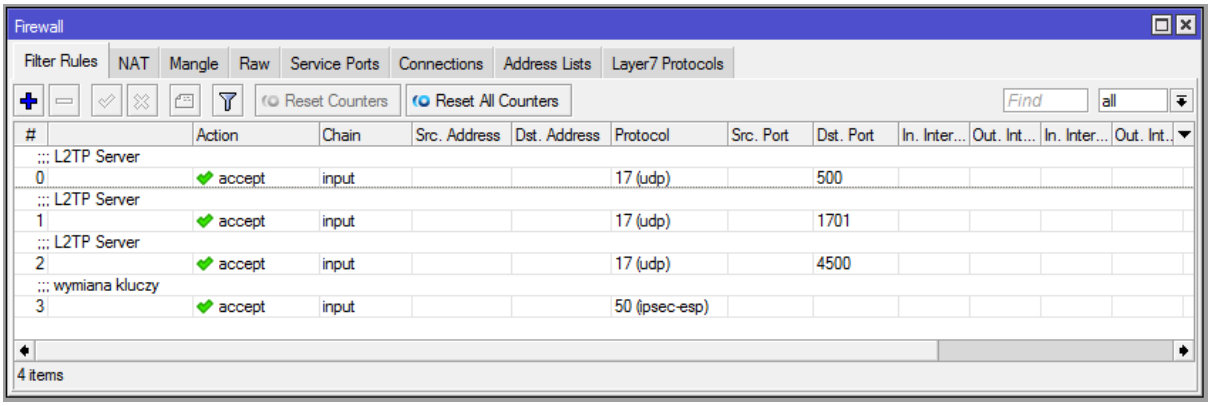


W tym kroku jest ważne, aby pozycja "Profile" wskazywała na wcześniej zmodyfikowany profil szyfrowania.

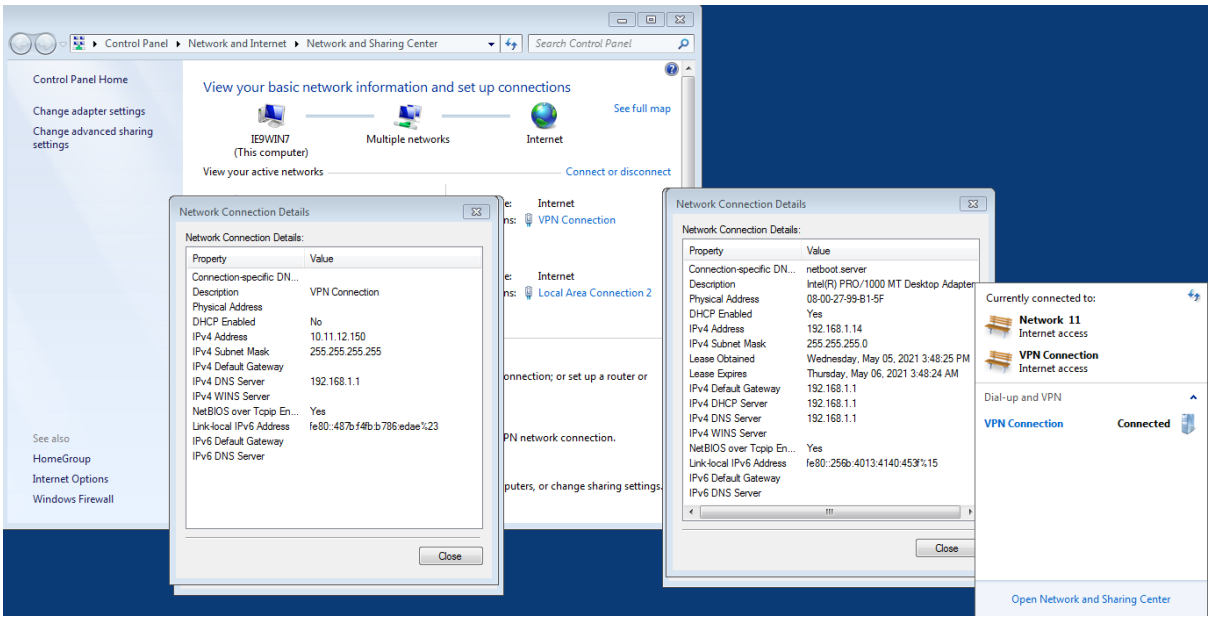
Ostatni etap konfiguracji dotyczy ustawień zabezpieczeń systemowych (firewall), które pozwolą na ustanawianie połączeń z zewnątrz, do sieci prywatnej z wykorzystaniem protokołów L2TP IPsec.

W tym celu należy odblokować możliwość wykonywania połączeń na portach: 500, 1701, 4500 dla protokołu UDP. Dodatkowo należy jeszcze zezwolić na połączenia typu ipsec-esp, które służą do wymiany kluczy autoryzacyjnych klientów z serwerem.

Konfiguracja firewalla powinna wyglądać następująco:



Jeśli serwer został poprawnie skonfigurowany, to możemy za pomocą połączenia WAN uzyskać dostęp do sieci firmowej, za pomocą połączenia VPN:



Aby autoryzacja się powiodła, przy nawiązywaniu połączenia VPN, należy wybrać typ sieci jako L2TP/IPsec z kluczem wstępnym, w przeciwnym wypadku połączenie nie zostanie nawiązane.