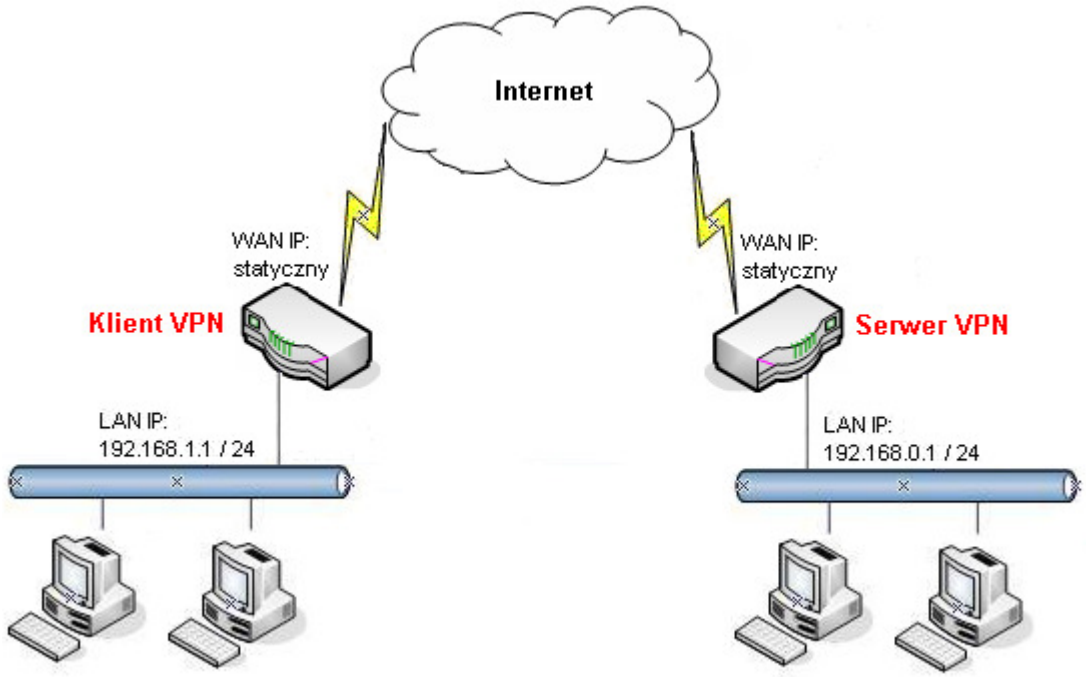
1. Konfiguracja serwera VPN (Vigor2960)

2. Konfiguracja klienta VPN (Vigor2920)

Procedura konfiguracji została oparta na poniższym przykładzie.



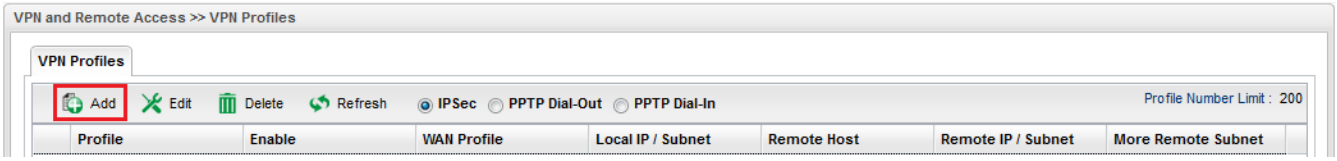
Główne założenia:

- typ tunelu: LAN-LAN z routingiem pomiędzy podsieciami
- protokół VPN: IPSec
- tryb główny IKE
- serwer VPN akceptuje wszystkie propozycje
- klient VPN proponuje szyfrowanie AES z SHA1/MD5
- autentykacja: klucz IKE 'test'
- adres IP Serwera VPN: statyczny. W przykładzie 99.99.99.10
- adres IP Klienta VPN: statyczny. W przykładzie 99.99.99.11
- różne adresacje LAN:
  - serwer VPN: 192.168.0.1 /24
  - klient VPN: 192.168.1.1 /24

Uwaga!
Wymagane są różne adresacje sieci lokalnych.

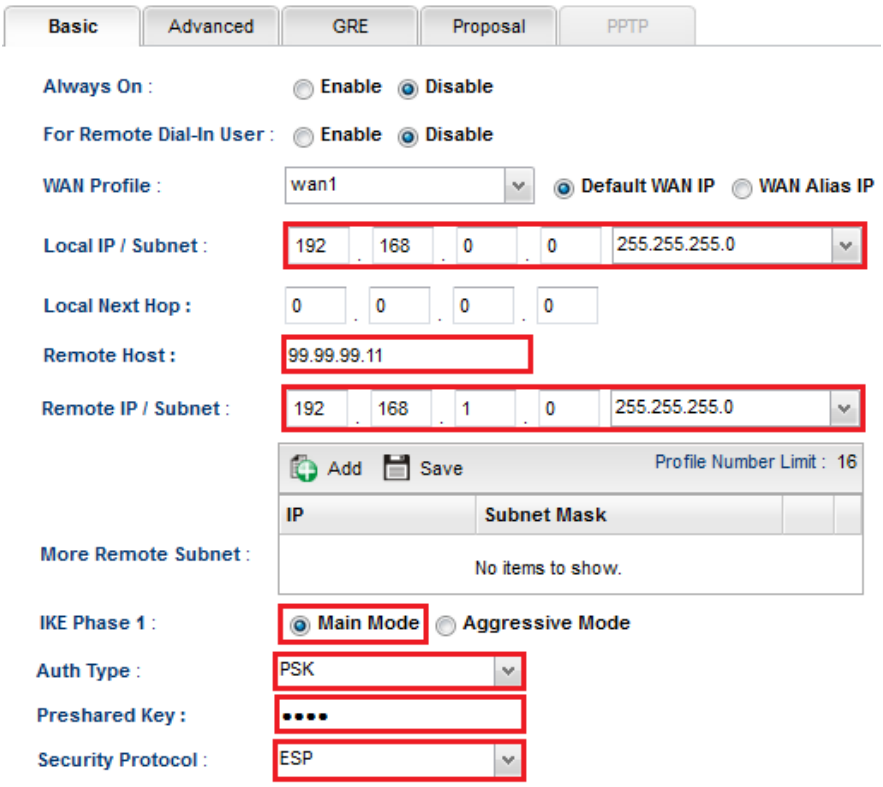
1. Konfiguracja serwera VPN (Vigor2960)

Przejdź do zakładki **VPN and Remote Accessny>>VPN Profiles**. Kliknij przycisk **Add(Dodaj)**.

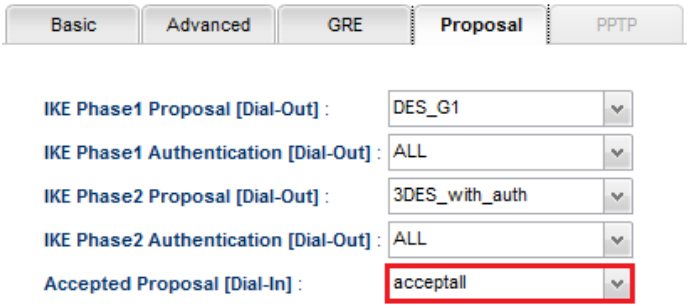


Wpisz nazwę profilu.
Zaznacz **Enable This Profile(Włącz ten profil)**.
Dla opcji **Type(Typ)** wybierz **IPSec**.

W ustawieniach Basic(Podstawowe):
- W polu **Local IP(Lokalny IP)/Subnet(Maska)** wpisz odpowiedni adres IP oraz wybierz odpowiednią maskę.
- W polu **Remote Host(Zdalny Host)** wpisz odpowiedni adres IP Klienta VPN. W przykładzie 99.99.99.11.
- W polu **Remote IP(Zdalny IP)/Subnet(Maska)** wpisz odpowiedni adres IP oraz wybierz odpowiednią maskę.
- Dla opcji **IKE Phase 1** wybierz **Main mode (Tryb główny)**
- W polu **Preshared Key(Klucz PSK)** wpisz klucz. W przykładzie 'test'.

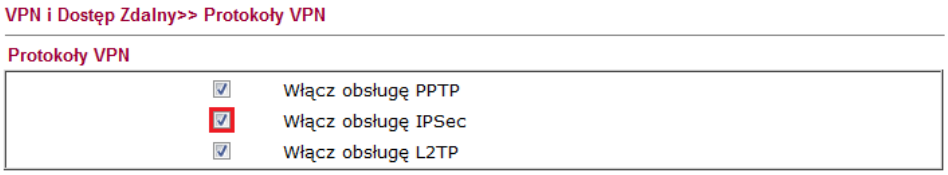


W ustawieniach Proposal(Propozycja):
- W polu Accepted Proposal [Dial-In] wybierz **acceptall(akceptuj wszystko)**.



2. Konfiguracja klienta VPN (Vigor2920)

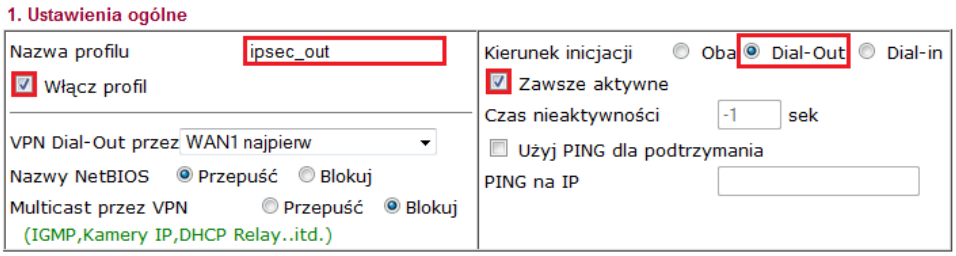
Przejdź do zakładki **VPN i Dostęp Zdalny>>Protokoły VPN** w panelu konfiguracyjnym routera i sprawdź (lub zaznacz) czy jest włączona obsługa protokołu IPSec. Domyślnie włączona jest obsługa protokołów PPTP, IPSec i L2TP.



Przejdź do zakładki **VPN i Dostęp Zdalny>>Połączenia LAN-LAN**. Stwórz odpowiedni profil do obsługi tunelu (w przykładzie użyto profilu nr 1) i wpisz odpowiednie dane.

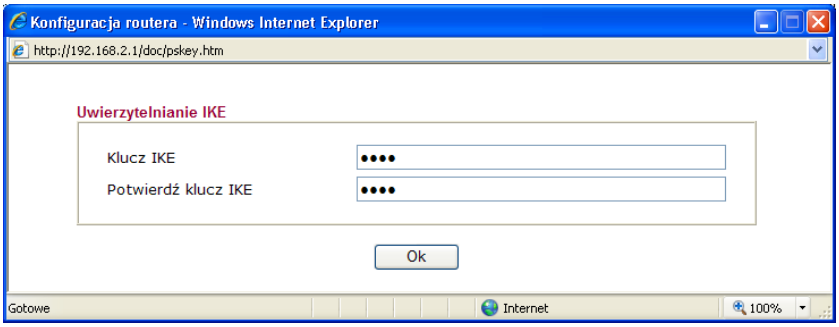
Konfiguracja części **Ustawienia ogólne** zgodna z założeniami przykładu:

- wpisz dowolną nazwę profilu
- zaznacz **Włącz profil**
- jako kierunek inicjacji wybierz **Dial-Out**
- zaznacz **Zawsze aktywne** - ustawisz **czas nieaktywności -1**, gdy połączenie ma być aktywne cały czas.

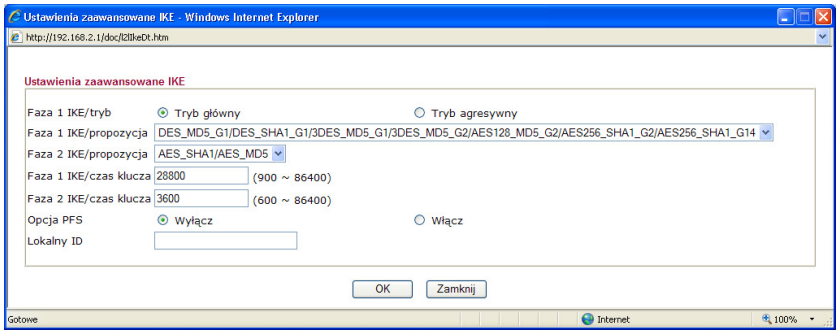


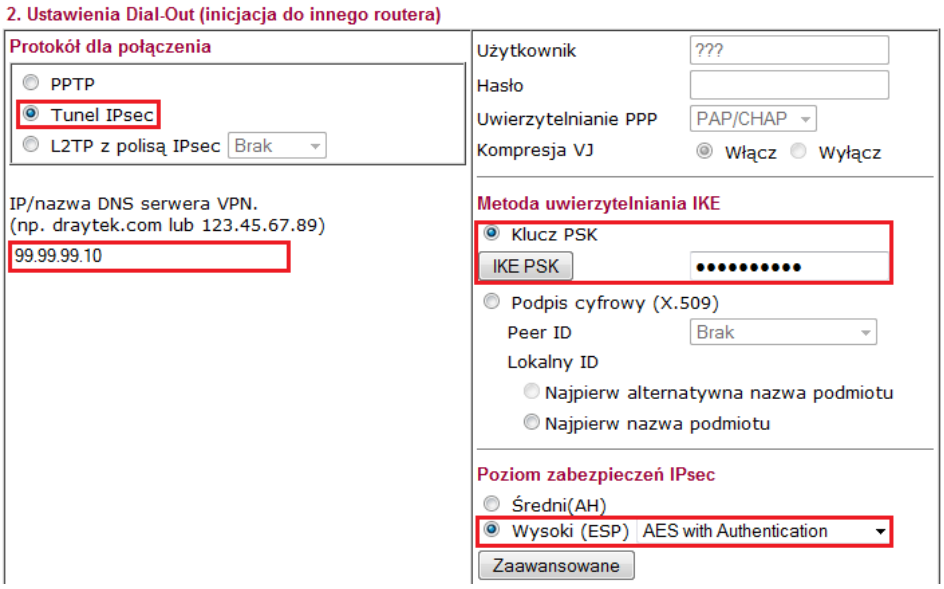
Konfiguracja części **Ustawienia Dial-Out** zgodna z założeniami przykładu:

- w polu Protokół dla połączenia wybierz **Tunel IPSec**
- w polu **IP/nazwa DNS serwera VPN** wpisz adres IP routera, do którego zestawiasz tunel VPN, albo jego nazwę. W przykładzie adres IP 99.99.99.10
- w polu Tryb uwierzytelniania IKE wybierz **Klucz IKE**. Kliknij przycisk **Klucz IKE** – pojawi się okno, w które wpisz odpowiedni klucz. W przykładzie użyto klucza 'test'



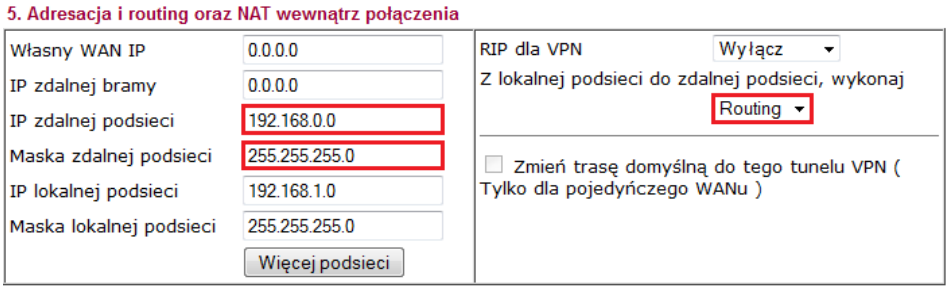
- w polu Poziom zabezpieczeń IPSec wybierz protokół realizujący szyfrowanie i uwierzytelnianie **Wysoki(ESP)**. W przykładzie użyto AES z autentykacją. Kliknij przycisk **Zaawansowane** – pojawi się okno, w którym możesz zmodyfikować Ustawienia zaawansowane IKE.





Konfiguracja części **Adresacja i routing oraz NAT wewnątrz połączenia** zgodna z założeniami przykładu:

- w przykładzie Zdalna podsieć: 192.168.0.0, Maska podsieci zdalnej: 255.255.255.0



Krzysztof Skowina
Specjalista ds. rozwiązań sieciowych
BRINET Sp. z o.o.
k.skowina@brinet.pl