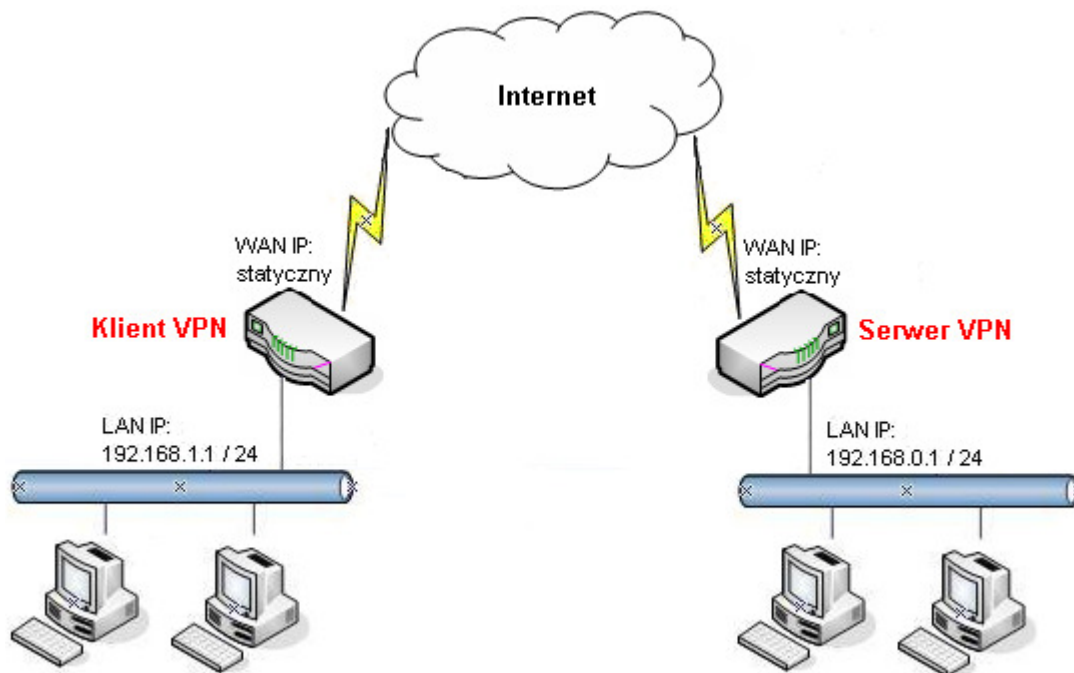


1. Konfiguracja serwera VPN (Vigor2960)
2. Konfiguracja klienta VPN (Vigor2920)

Procedura konfiguracji została oparta na poniższym przykładzie.



Główne założenia:

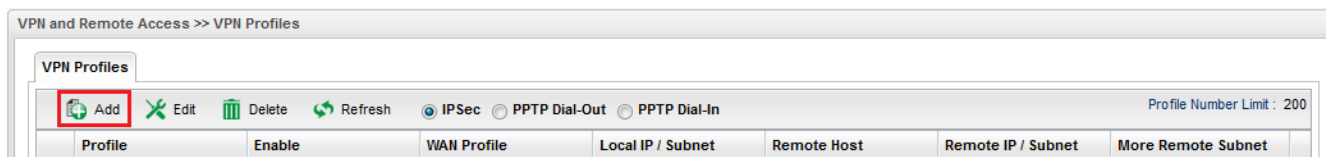
- typ tunelu: LAN-LAN z routingiem pomiędzy podsieciami
- protokół VPN: IPSec
- tryb główny IKE
- serwer VPN akceptuje wszystkie propozycje
- klient VPN proponuje szyfrowanie AES z SHA1/MD5
- autentykacja: klucz IKE 'test'
- adres IP Serwera VPN: statyczny. W przykładzie 99.99.99.10
- adres IP Klienta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

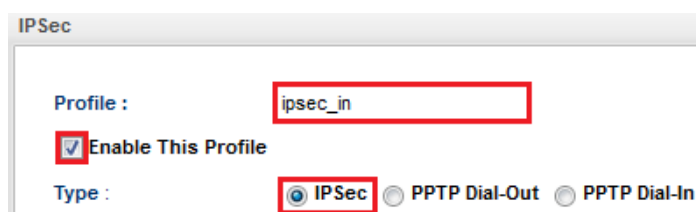
Przejdź do zakładki **VPN and Remote Accessy >> VPN Profiles**. Kliknij przycisk **Add(Dodaj)**.



Wpisz nazwę profilu.

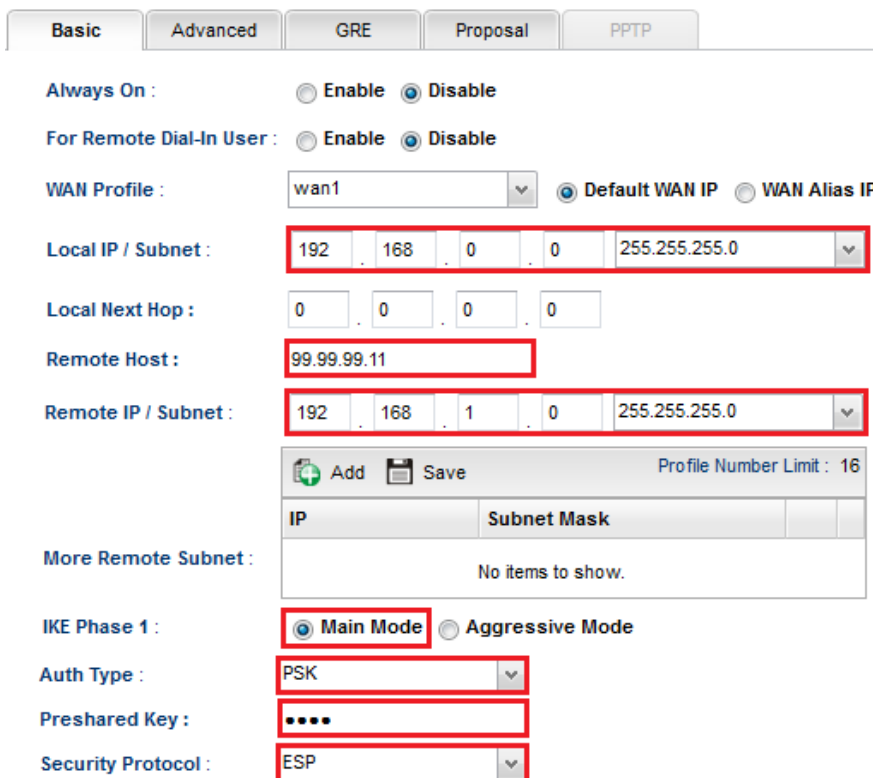
Zaznacz **Enable This Profile(Włącz ten profil)**.

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)**.

Basic	Advanced	GRE	<b>Proposal</b>	PPTP
IKE Phase1 Proposal [Dial-Out] :		DES_G1		
IKE Phase1 Authentication [Dial-Out] :		ALL		
IKE Phase2 Proposal [Dial-Out] :		3DES_with_auth		
IKE Phase2 Authentication [Dial-Out] :		ALL		
Accepted Proposal [Dial-In] :		acceptall		

### 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.

VPN i Dostęp Zdalny>> Protokoły VPN

Protokoły VPN	
<input checked="" type="checkbox"/>	Włącz obsługę PPTP
<input checked="" type="checkbox"/>	Włącz obsługę IPSec
<input checked="" type="checkbox"/>	Włącz obsługę 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:

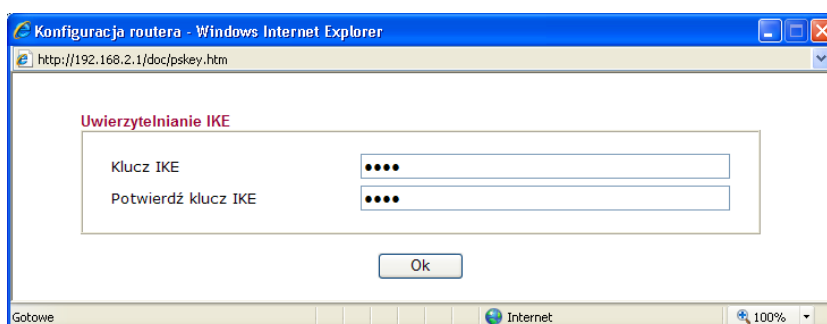
- wpisz dowolną nazwę profilu
- zaznacz **Włącz profil**
- jako kierunek inicjacji wybierz **Dial-Out**
- zaznacz **Zawsze aktywne** - ustawisz **czas nieaktywności -1**, gdy połączenie ma być aktywne cały czas.

1. Ustawienia ogólne

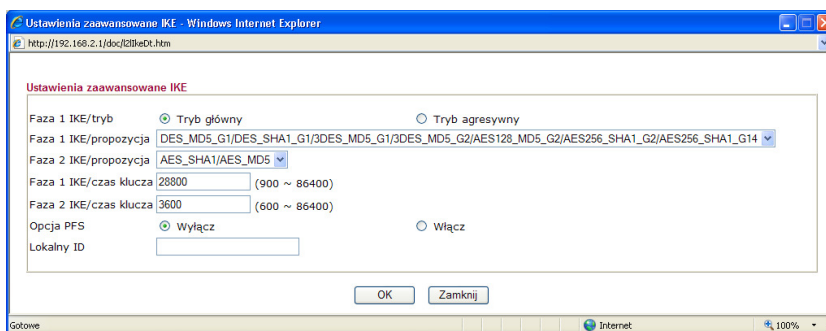
Nazwa profilu <input type="text" value="ipsec_out"/>	Kierunek inicjacji <input type="radio"/> Oba <input checked="" type="radio"/> <b>Dial-Out</b> <input type="radio"/> Dial-in
<input checked="" type="checkbox"/> Włącz profil	<input checked="" type="checkbox"/> Zawsze aktywne
VPN Dial-Out przez <input type="text" value="WAN1 najpierw"/>	Czas nieaktywności <input type="text" value="-1"/> sek
Nazwy NetBIOS <input checked="" type="radio"/> Przepuść <input type="radio"/> Blokuj	<input type="checkbox"/> Użyj PING dla podtrzymania
Multicast przez VPN <input type="radio"/> Przepuść <input checked="" type="radio"/> Blokuj (IGMP,Kamery IP,DHCP Relay..itd.)	PING na IP <input type="text"/>

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.



### 2. Ustawienia Dial-Out (inicjacja do innego routera)

<b>Protokół dla połączenia</b> <input type="radio"/> PPTP <input checked="" type="radio"/> <b>Tunel IPsec</b> <input type="radio"/> L2TP z polisą IPsec <input type="text" value="Brak"/>	Użytkownik <input type="text" value="???"/> Hasło <input type="text"/> Uwierzytelnianie PPP <input type="text" value="PAP/CHAP"/> Kompresja VJ <input checked="" type="radio"/> Włącz <input type="radio"/> Wyłącz
IP/nazwa DNS serwera VPN. (np. draytek.com lub 123.45.67.89) <input type="text" value="99.99.99.10"/>	<b>Metoda uwierzytelniania IKE</b> <input checked="" type="radio"/> <b>Klucz PSK</b> <input type="button" value="IKE PSK"/> <input type="text" value="●●●●●●●●"/> <input type="radio"/> Podpis cyfrowy (X.509) Peer ID <input type="text" value="Brak"/> Lokalny ID <input type="radio"/> Najpierw alternatywna nazwa podmiotu <input type="radio"/> Najpierw nazwa podmiotu
	<b>Poziom zabezpieczeń IPsec</b> <input type="radio"/> Średni(AH) <input checked="" type="radio"/> <b>Wysoki (ESP) AES with Authentication</b> <input type="button" value="Zaawansowane"/>

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

### 5. Adresacja i routing oraz NAT wewnątrz połączenia

Własny WAN IP <input type="text" value="0.0.0.0"/> IP zdalnej bramy <input type="text" value="0.0.0.0"/> IP zdalnej podsieci <input type="text" value="192.168.0.0"/> Maska zdalnej podsieci <input type="text" value="255.255.255.0"/> IP lokalnej podsieci <input type="text" value="192.168.1.0"/> Maska lokalnej podsieci <input type="text" value="255.255.255.0"/> <input type="button" value="Więcej podsieci"/>	RIP dla VPN <input type="text" value="Wyłącz"/> Z lokalnej podsieci do zdalnej podsieci, wykonaj <input type="text" value="Routing"/> <input type="checkbox"/> Zmień trasę domyślną do tego tunelu VPN ( Tylko dla pojedynczego WANu )
---	--

Krzysztof Skowina  
 Specjalista ds. rozwiązań sieciowych  
 BRINET Sp. z o.o.  
[k.skowina@brinet.pl](mailto:k.skowina@brinet.pl)