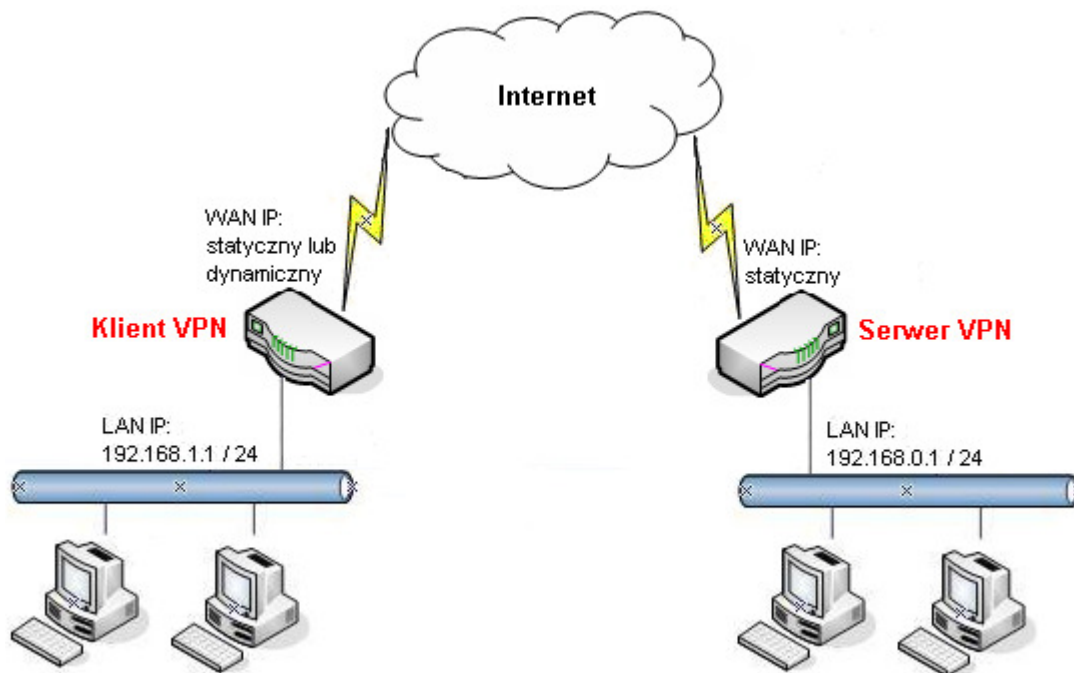


1. Konfiguracja serwera VPN (Vigor2960)
2. Konfiguracja klienta VPN (Vigor2920)

Procedura konfiguracji została oparta na poniższym przykładzie.



### Główne założenia:

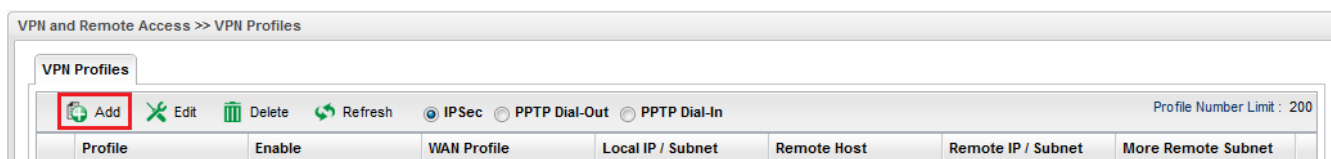
- typ tunelu: LAN-LAN z routowaniem pomiędzy podsieciami
- protokół VPN: IPSec
- tryb agresywny IKE:
  - 2920: lokalny ID `vigor2920`
  - 2960: zdalny ID `vigor2920`
- serwer VPN akceptuje wszystkie propozycje
- klient VPN proponuje szyfrowanie AES z SHA1/MD5
- autentykacja: klucz IKE `test`
- adres IP Serwera VPN: statyczny. W przykładzie 99.99.99.10
- adres IP Klienta VPN: statyczny lub dynamiczny. 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)

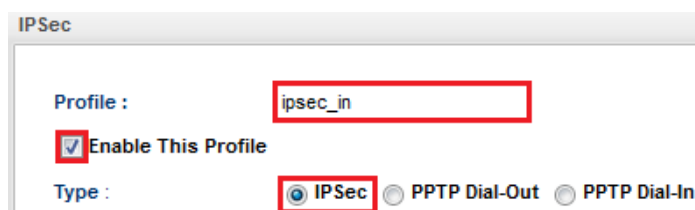
Przejdź do zakładki **VPN and Remote Access**>>**VPN Profiles**. Kliknij przycisk **Add(Dodaj)**.



Wpisz nazwę profilu.

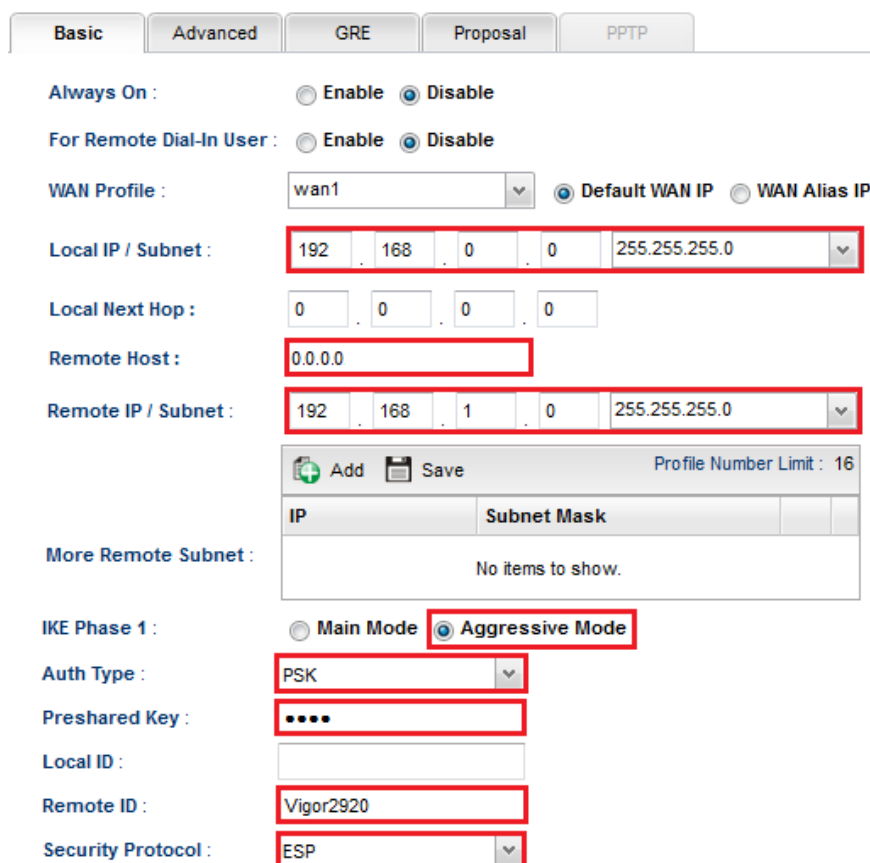
Zaznacz **Enable This Profile(Włącz ten profil)**.

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)** pozostaw 0.0.0.0.
- W polu **Remote IP(Zdalny IP)/Subnet(Maska)** wpisz odpowiedni adres IP oraz wybierz odpowiednią maskę.
- Dla opcji **IKE Phase 1** wybierz **Aggressive mode (Tryb agresywny)**.
- W polu **Preshared Key(Klucz PSK)** wpisz klucz. W przykładzie 'test'.
- W polu **Remote Peer ID(Zdalny ID)** wpisz identyfikator. W przykładzie 'Vigor2920'.



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.

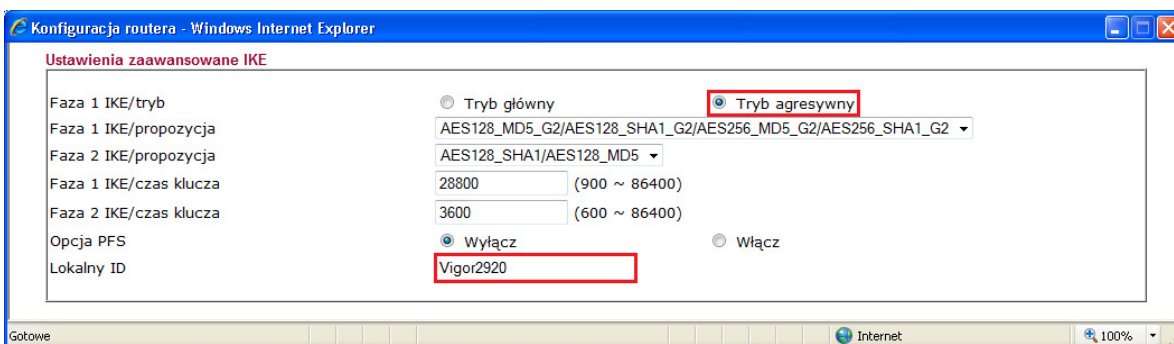
1. Ustawienia ogólne

Nazwa profilu <input type="text" value="ipsec_out"/>	Kierunek inicjacji <input type="radio"/> Oba <input checked="" type="radio"/> Dial-Out <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. Wybierz **Tryb agresywny** i wpisz **Lokalny ID** (w przykładzie użyto 'Vigor2920').



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

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

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

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

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