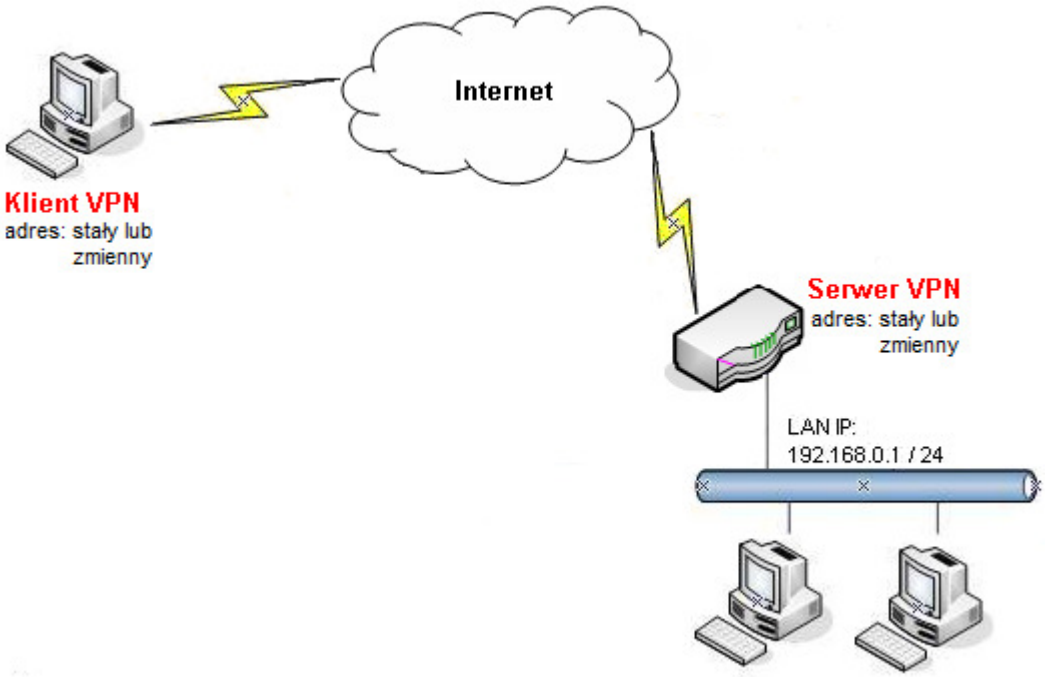
Procedura konfiguracji została oparta na poniższym przykładzie.



Główne założenia:

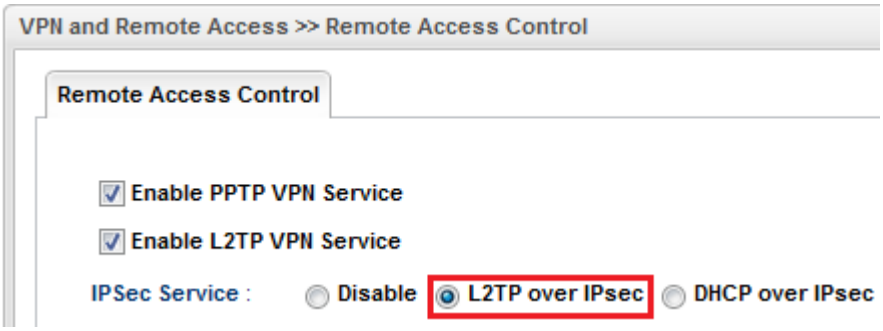
- typ tunelu: Host-LAN
- protokół VPN: L2TP over IPSec
- szyfrowanie: 3DES
- integralność: SHA1
- autentykacja: L2TP (nazwa użytkownika i hasło), IPSec (klucz IKE)
- Adres Serwera VPN: stały (IP - 99.99.99.10) lub zmienny (domenowy - serwer.abc.xyz)
- Adres Klienta VPN: stały lub zmienny

Uwagi

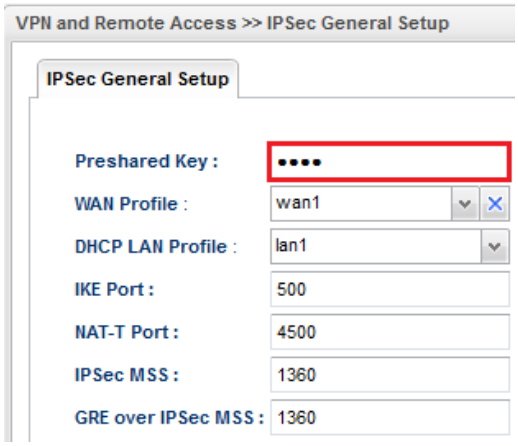
Jeśli serwer VPN nie posiada stałego adresu IP to można wykorzystać opcję dynamicznego DNS (np. www.noip.com) w celu reprezentowania zmiennego adresu IP poprzez adres domenowy.

1.Konfiguracja serwera VPN

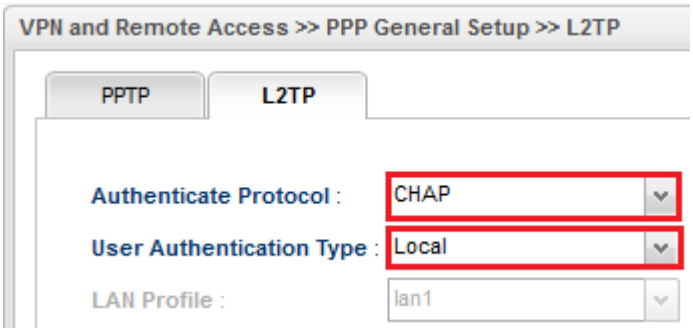
Przejdź do zakładki **VPN and Remote Access>>Remote Access Control** i sprawdź (lub zaznacz) czy jest zaznaczona opcja **L2TP over IPSec.**



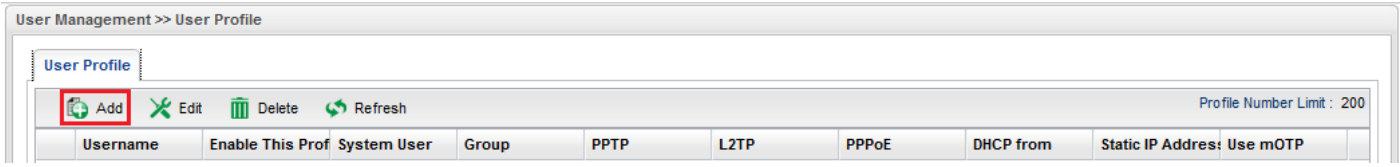
Przejdź do zakładki **VPN and Remote Access>>IPSec General Setup**. W polu **Preshared Key(Klucz PSK)** wpisz klucz. W przykładzie 'test'.



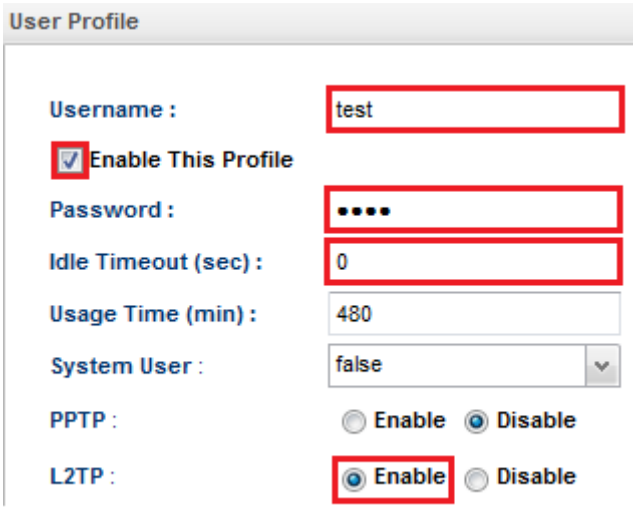
Przejdź do zakładki **VPN and Remote Access>>PPP General Setup.**
Authenticate Protocol(Protokół uwierzytelniania) **CHAP**
User Authentication Type(Typ uwierzytelniania użytkownika) **Local(Lokalny)**



Przejdź do zakładki **User Management>>User Profile**. Kliknij przycisk **Add(Dodaj)** w celu utworzenia lokalnego konta użytkownika.

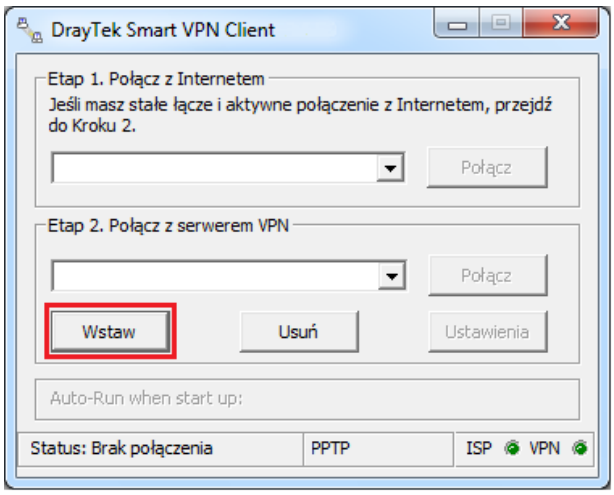


Wpisz nazwę użytkownika – w przykładzie 'test'.
Zaznacz **Enable This Profile(Włącz ten profil)**.
Wpisz hasło – w przykładzie 'test'.
Ustaw **Idle Timeout(Czas nieaktywności)**. Domyślnie jest tam wartość 300 oznaczająca rozłączenie tunelu po 5 minutach, gdy Vigor nie odnotuje ruchu VPN. Wpisz **0** w polu czas nieaktywności jeśli Vigor ma pozostawić połączenie pomimo braku ruchu. PPTP posiada wbudowane mechanizmy detekcji połączenia.
Dla **L2TP** wybierz **Enable(Włącz).**



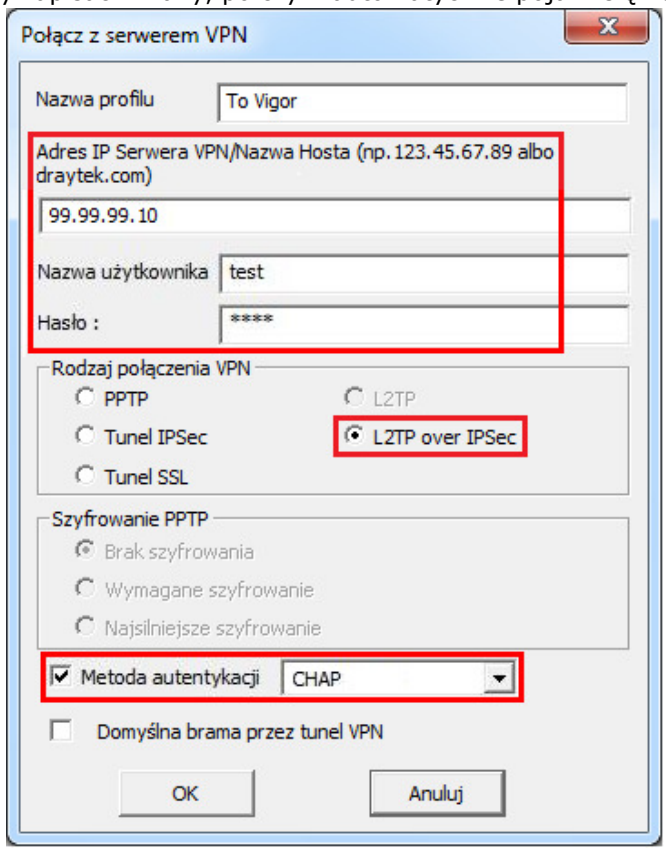
2. Konfiguracja klienta VPN

Kliknij przycisk **Wstaw**.



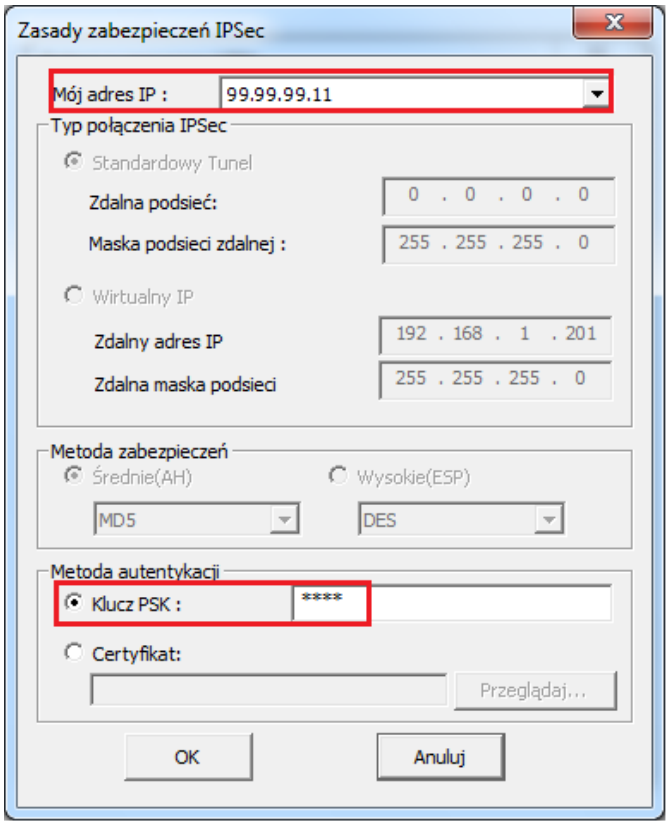
Wypełnij dane dotyczące adresu serwera i typu VPN:

- w polu Nazwa profilu wpisz dowolną nazwę dla połączeni np. To Vigor
- w polu Adres IP Serwera/Nazwa Hosta wpisz adres IP routera (w przykładzie 99.99.99.10), do którego zestawiasz tunel VPN, albo jego nazwę (w przykładzie serwer.abc.xyz).
- w polu Nazwa użytkownik wpisz odpowiednią nazwę zgodną ze stworzonym profilem. W przykładzie użyto 'test'
- w polu Hasło wpisz odpowienie hasło zgodne ze stworzonym profilem. W przykładzie użyto 'test'
- w polu Rodzaj połączenia VPN wybierz L2TP over IPSec
- zaznacz Metodę autentykacji i wybierz CHAP
- kliknij przycisk OK, aby zapisać zmiany, po czym automatycznie pojawi się kolejne okno.

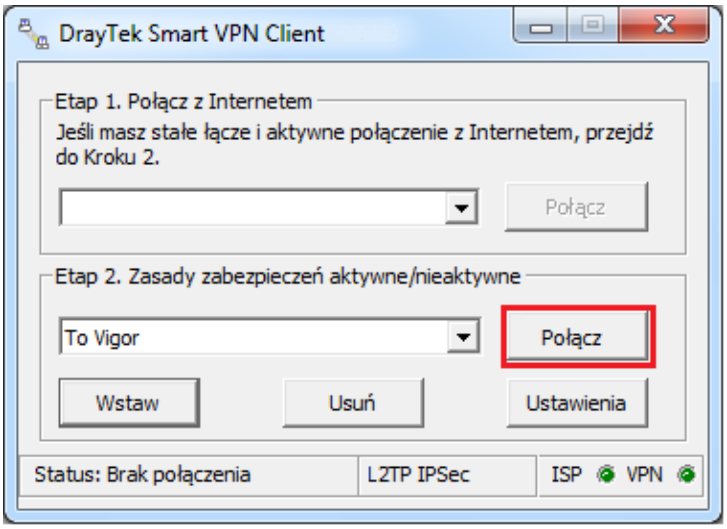


Wypełnij dane dotyczące zabezpieczeń IPSec:

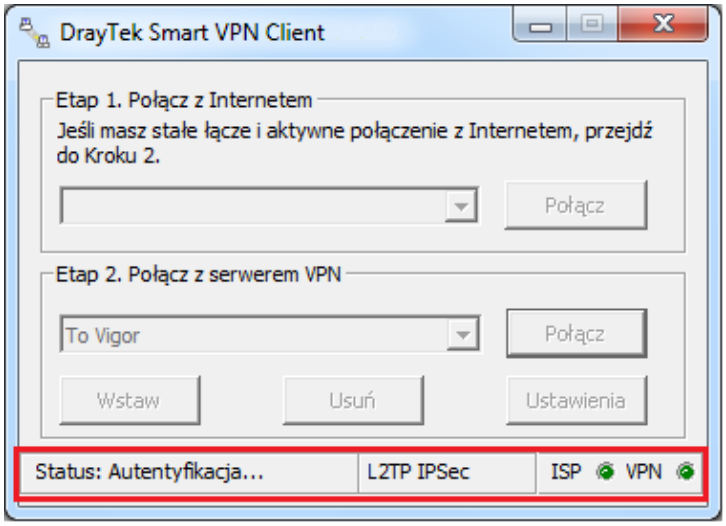
- w polu Mój adres IP wybierz odpowiedni adres IP swojego komputera. W przykładzie 99.99.99.11.
- w polu Metoda autentykacji wybierz Klucz PSK i wpisz klucz. W przykładzie użyto klucza 'test'.
- kliknij przycisk OK, aby zapisać zmiany.



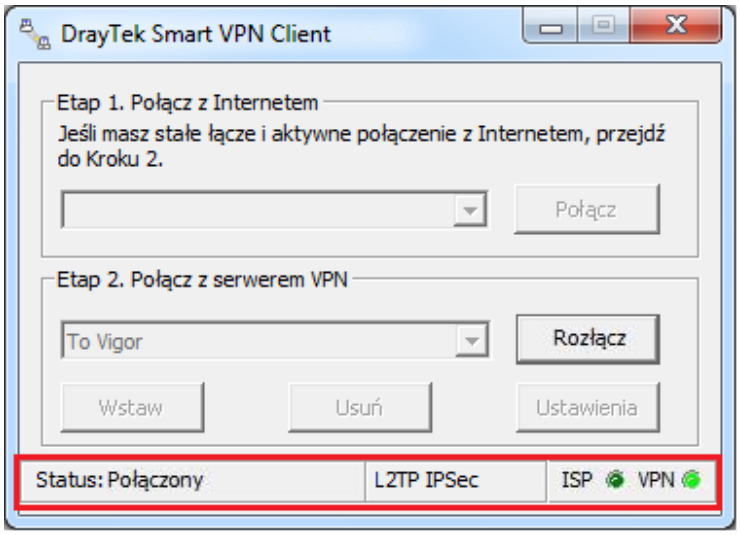
Wybierz odpowiedni profil a następnie kliknij Połącz.



Jednym z kroków ustanawiania połączenia L2TP over IPSec jest Autentyfikacja.



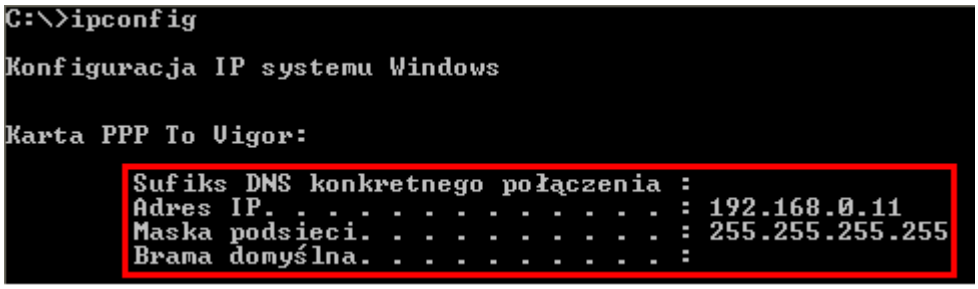
Przy poprawnym połączeniu zmieni się statut na Połączony oraz zapali się zielone światełko przy polu VPN.



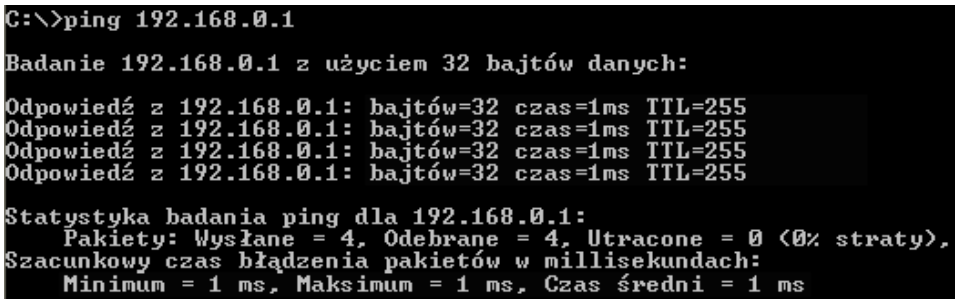
3. Status Połączenia

3.1. Klient VPN

Wybierz Menu Start a następnie Uruchom i wpisz cmd. Następnie wykonaj polecenie: ipconfig. Po wcześniejszym zainicjowaniu tunelu otrzymasz adres IP z sieci zdalnej. W omawianym przykładzie 192.168.0.11.

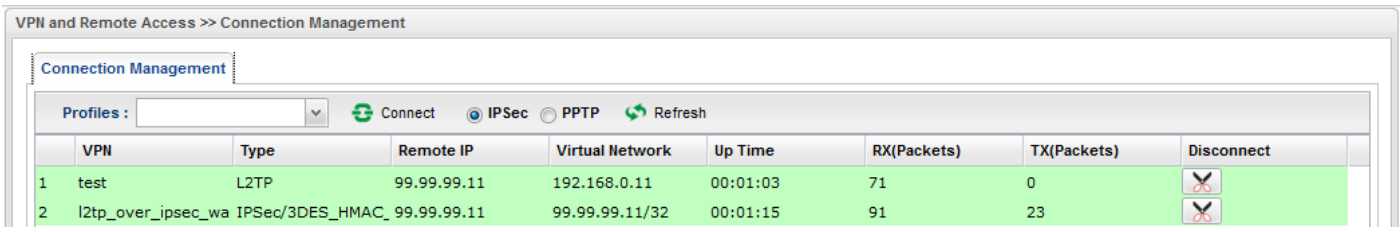


Dodatkowo wystarczy np. zwykły ping. Wykonaj polecenie ping adres_LAN_serwera (w przykładzie serwer VPN posiada adres LAN 192.168.0.1). Poprawna odpowiedź na ping świadczy o poprawnej komunikacji w tunelu VPN.



3.2. Serwer VPN

O tym, czy tunel został zainicjowany, możesz również przekonać się wybierając **VPN and Remote Access>>Connection Management** (rysunek poniżej).



Krzysztof Skowina
Specjalista ds. rozwiązań sieciowych
k.skowina@brinet.pl