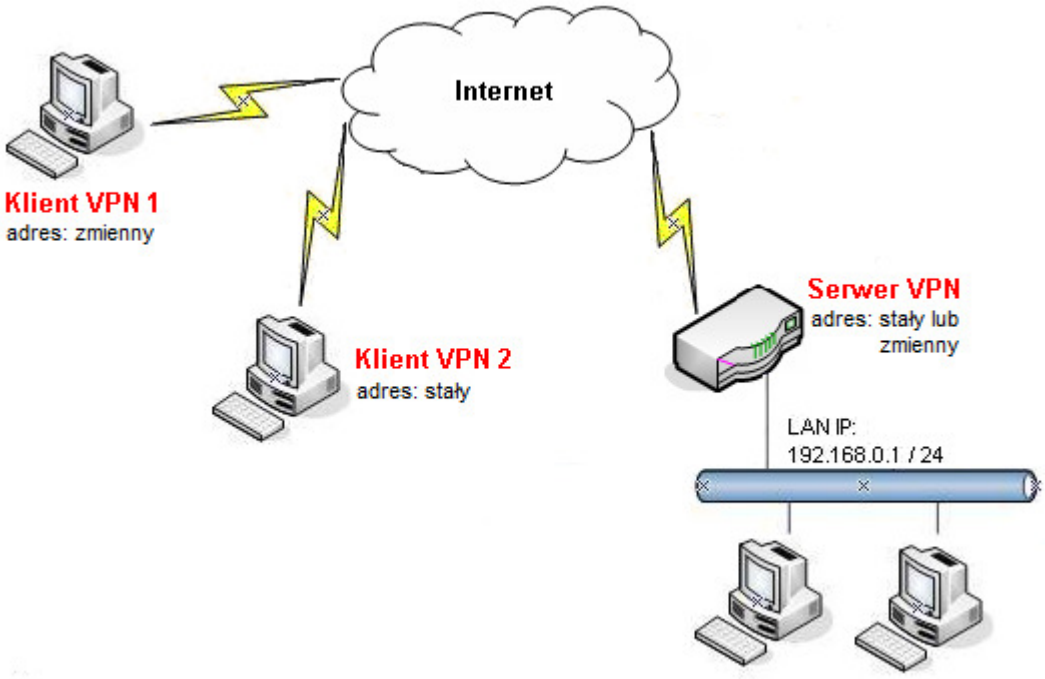
Procedura konfiguracji została oparta na poniższym przykładzie.



Główne założenia:

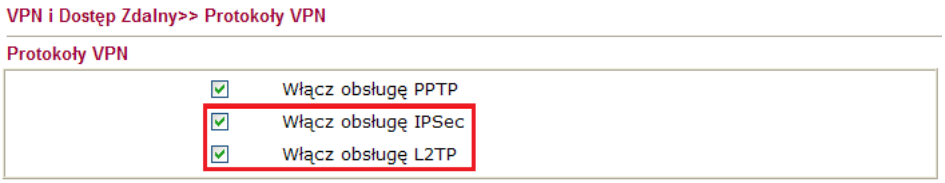
- typ tunelu: Host-LAN
- protokół VPN: L2TP over IPSec
- szyfrowanie: 3DES
- integralność: SHA1
- autentykacja: L2TP (nazwa użytkownika i hasło), IPSec (klucz IKE)
- Adres Serwera VPN: stały (IP - 99.99.99.10) lub zmienny (domenowy - serwer.abc.xyz)
- Adres Klienta VPN 1: zmienny
- Adres Klienta VPN 2: stały (IP - 99.99.99.12)

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.

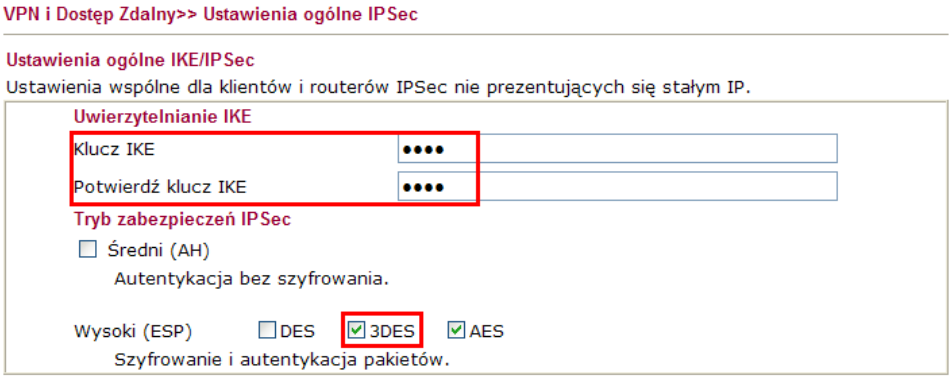
1.Konfiguracja serwera VPN

Przejdź do zakładki **VPN i Dostęp Zdalny>>Protokoły VPN** i sprawdź (lub zaznacz) czy jest włączona obsługa protokołu IPSec i L2TP.



1.1. Profil dla klienta ze zmiennym IP

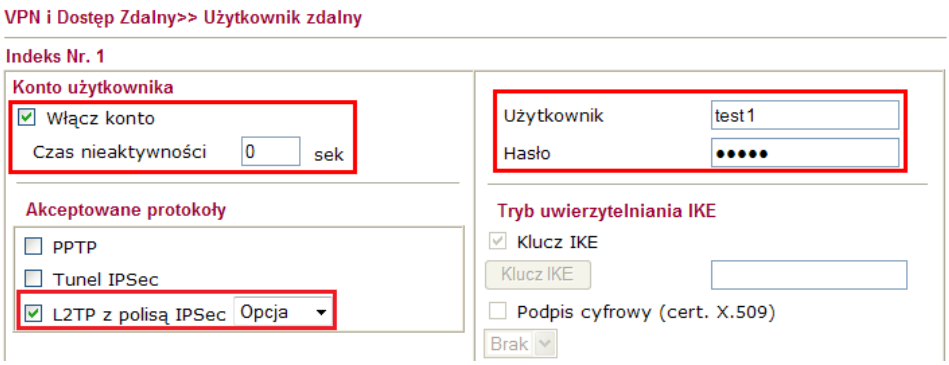
Przejdź do zakładki **VPN i Dostęp Zdalny>>Ustawienia ogólne IPSec**. Wpisz wspólny **klucz IKE** (w przykładzie użyto klucza 'test') oraz wybierz **3DES** jako Tryb zabezpieczeń IPSec.



Przejdź do zakładki **VPN i Dostęp Zdalny>>Połączenia Host-LAN**. Stwórz odpowiednie konto do obsługi tunelu.

Konfiguracja zgodna z założeniami przykładu:

- zaznacz **Włącz konto**
- ustaw **Czas nieaktywności**. Wpisz **0** w polu czas nieaktywności jeśli Vigor ma pozostawić połączenie pomimo braku ruchu. L2TP posiada wbudowane mechanizmy detekcji połączenia.
- jako akceptowany protokół zaznacz **L2TP z polisą IPSec.** Dla polisy IPSec Wybierz **Opcja** lub **Wymóg.**
- wpisz Użytkownika i Hasło dla L2TP. W przykładzie użyto użytkownika 'test1' i hasło 'test1'.
- kliknij przycisk OK, zatwierdzić ustawienia

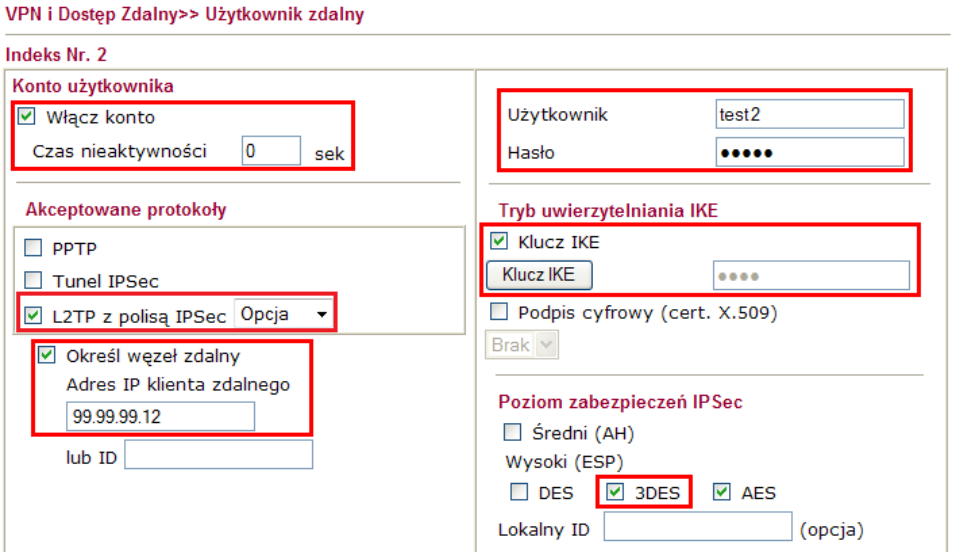


1.2. Profil dla klienta ze stałym IP

Przejdź do zakładki **VPN i Dostęp Zdalny>>Połączenia Host-LAN**. Stwórz odpowiednie konto do obsługi tunelu.

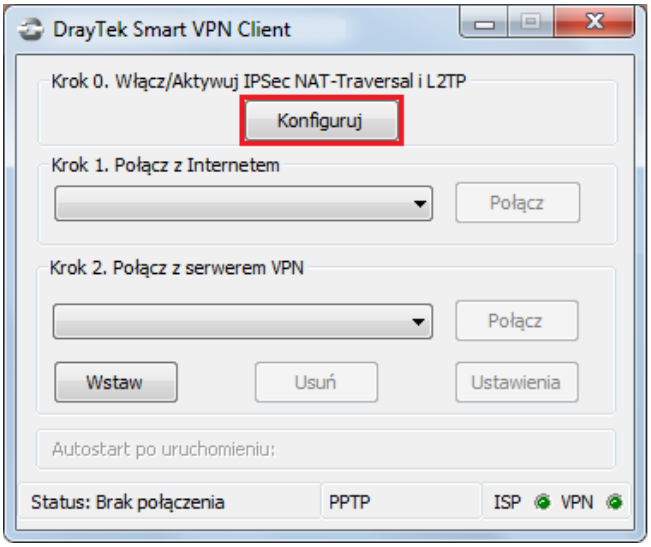
Konfiguracja zgodna z założeniami przykładu:

- zaznacz **Włącz konto**
- ustaw **Czas nieaktywności**. Wpisz **0** w polu czas nieaktywności jeśli Vigor ma pozostawić połączenie pomimo braku ruchu. L2TP posiada wbudowane mechanizmy detekcji połączenia.
- jako akceptowany protokół zaznacz **L2TP z polisą IPSec.** Dla polisy IPSec Wybierz **Opcja** lub **Wymóg.**
- zaznacz **Określ węzeł zdalny** i wprowadź odpowiedni adres. W przykładzie użyto 99.99.99.12
- wpisz Użytkownika i Hasło. W przykładzie użyto użytkownika 'test2' i hasło 'test2'.
- zaznacz **Klucz IKE**, kliknij przycisk **Klucz IKE** – pojawi się okienko w którym wpisz odpowiedni klucz. W przykładzie użyto klucza 'test'
- zaznacz odpowiedni **Poziom zabezpieczeń IPSec**. W przykładzie użyto 3DES.
- kliknij przycisk OK, zatwierdzić ustawienia

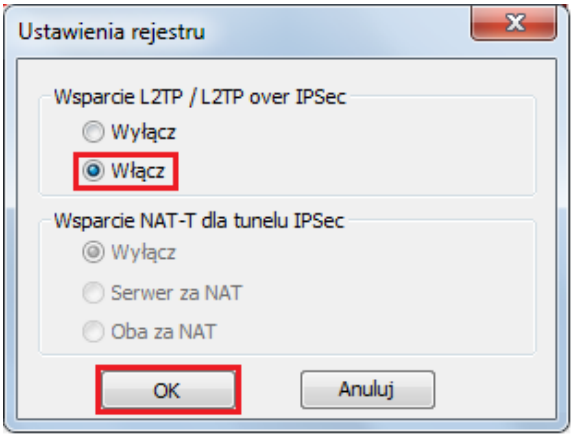


2. Konfiguracja klienta VPN

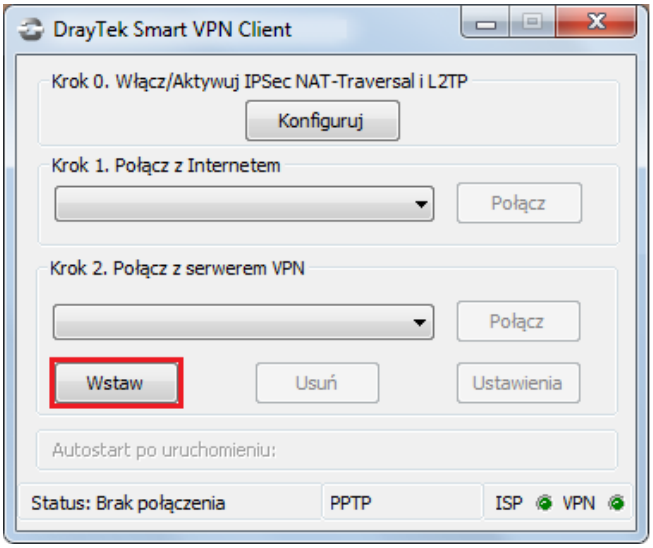
Kliknij przycisk **Konfiguruj**.



Włącz wsparcie L2TP over IPSec.

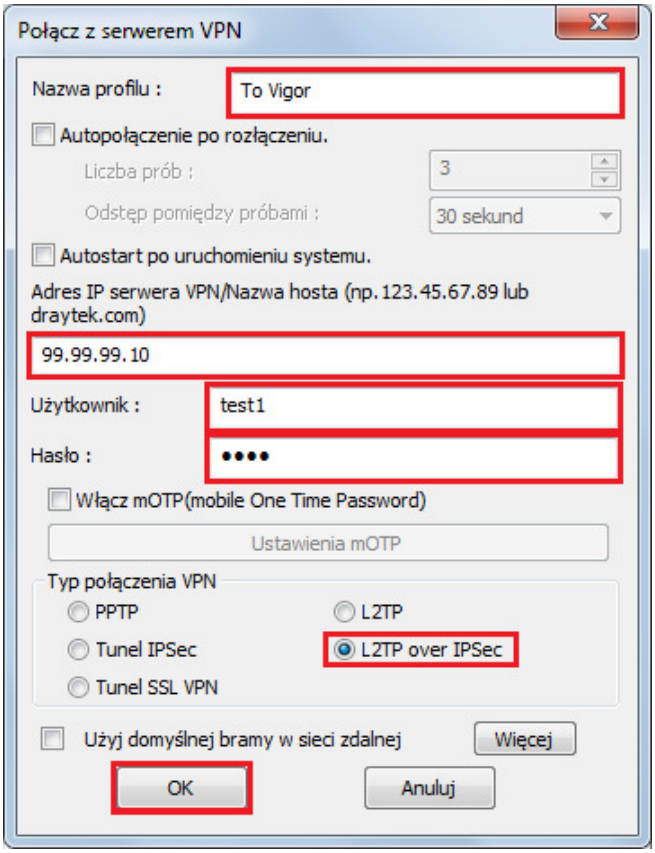


Kliknij przycisk **Wstaw**.



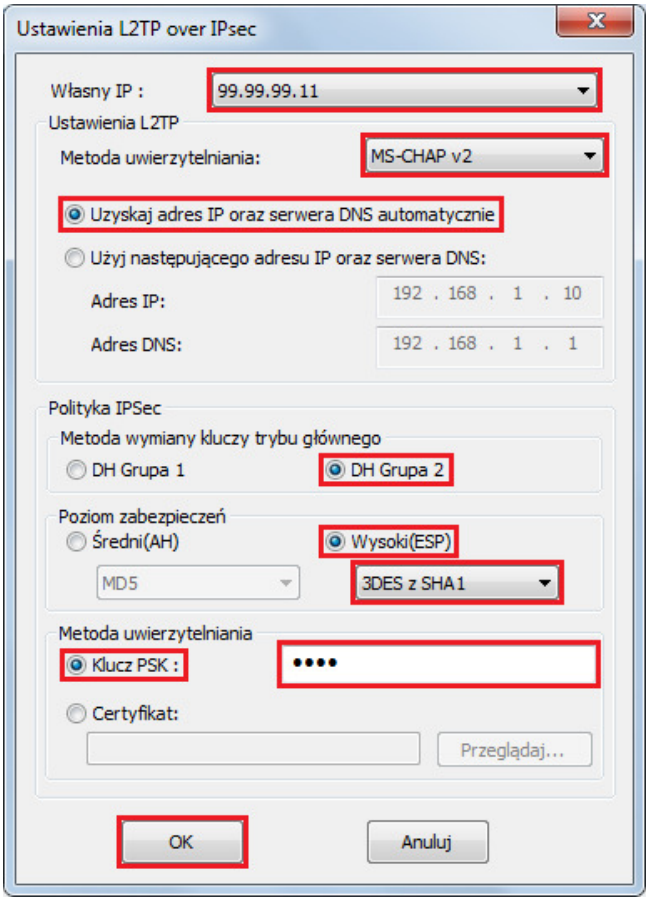
Wypełnij dane dotyczące adresu serwera i typu VPN:

- 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 'test1'
- w polu Hasło wpisz odpowiednie hasło zgodne ze stworzonym profilem. W przykładzie użyto 'test'
- w polu Typ połączenia VPN wybierz L2TP over IPSec
- kliknij przycisk OK, aby kontynować

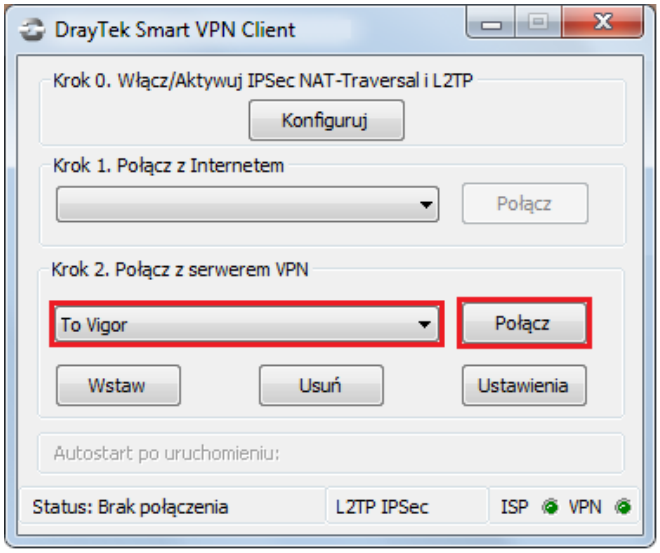


Wypełnij dane dotyczące Ustawień L2TP over IPSec

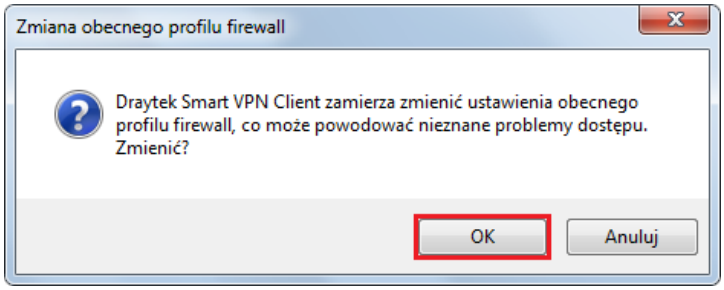
- w polu Mój adres IP wybierz odpowiedni adres IP swojego komputera. W przykładzie 99.99.99.11.
- w Ustawieniach L2TP w polu Metoda uwierzytelniania wybierz MS-CHAP v2
- w Polityce IPSec w polu Metoda uwierzytelniania wybierz klucz PSK i wpisz klucz. W przykładzie użyto klucza 'test'.
- kliknij przycisk OK, aby zapisać zmiany.



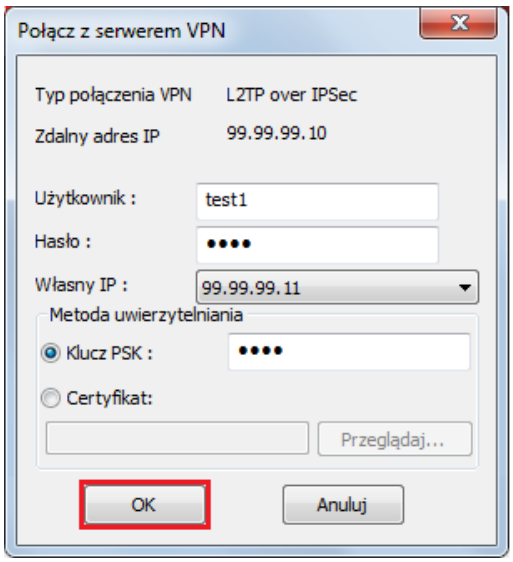
Wybierz odpowiedni profil a następnie kliknij Połącz.



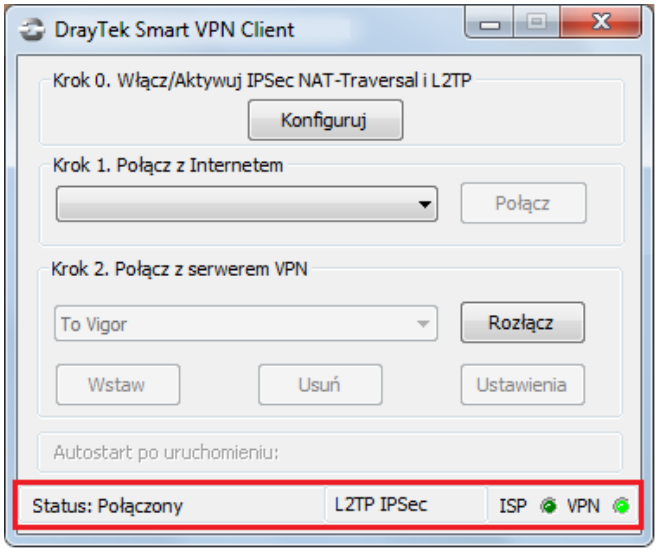
Zaakceptuj zmiany w Zaporze systemu Windows m.in. włączenie zapory, dodanie reguły zabezpieczeń połączeń.



Następnie kliknij OK.



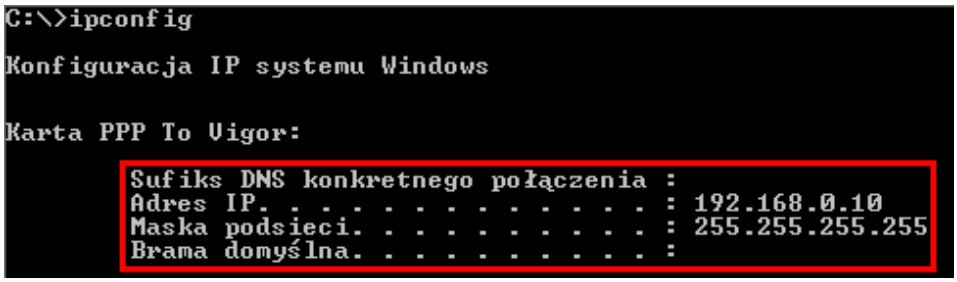
Przy poprawnym połączeniu zmieni się status na Połączony oraz zapali się zielone światełko przy polu VPN.



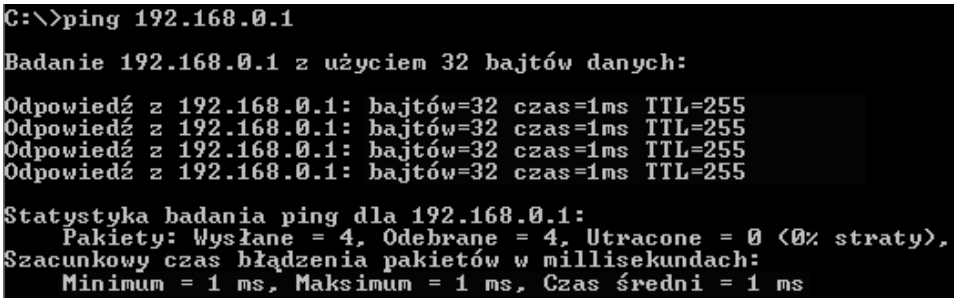
3. Status Połączenia

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 192.168.0.10.

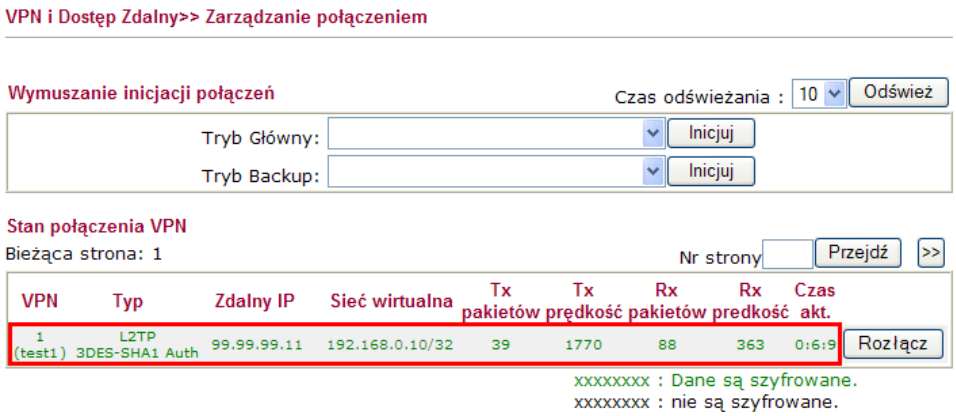


Dodatkowo wystarczy np. zwykły ping. Wykonaj polecenie ping adres_LAN_serwera (w przykładzie serwer VPN posiada adres LAN 192.168.0.1). Poprawna odpowiedź na ping świadczy o poprawnej komunikacji w tunelu VPN.



3.2. Serwer VPN

O tym, czy tunel został zainicjowany, możesz przekonać się wybierając **VPN i Dostęp Zdalny>>Zarządzanie połączeniem** (rysunek poniżej).



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