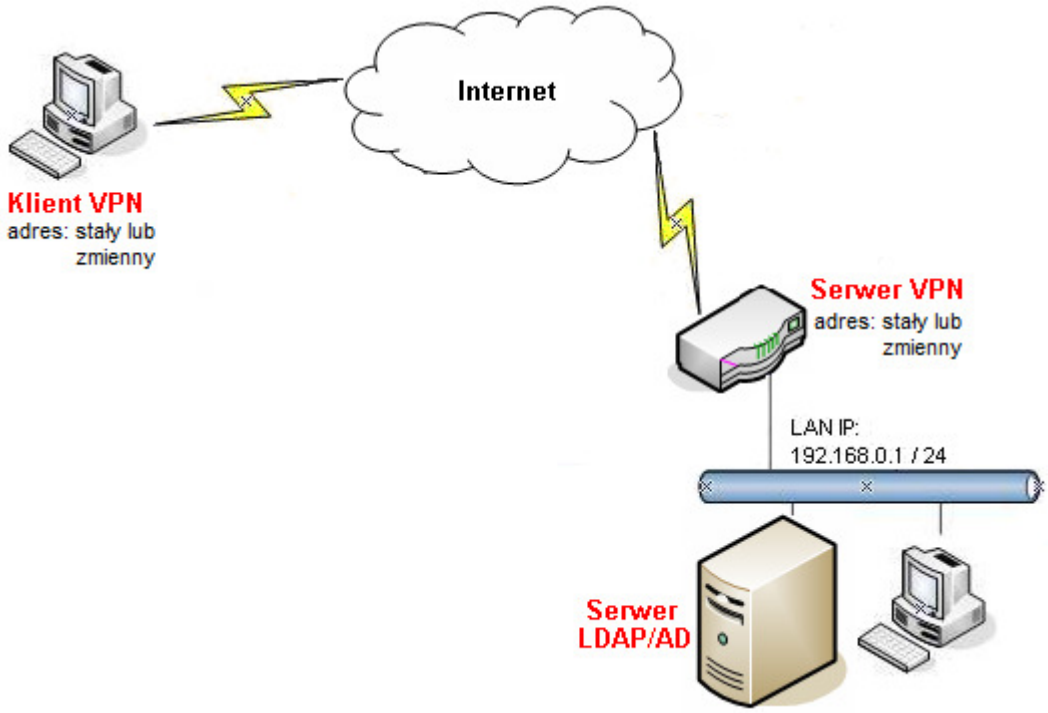
Procedura konfiguracji została oparta na poniższym przykładzie.



Główne założenia:

- typ tunelu: Host-LAN
- protokół VPN: PPTP
- brak szyfrowania
- uwierzytelnianie PAP
- Adres Serwera VPN: stały (IP - 99.99.99.10) lub zmienny (domenowy - serwer.abc.xyz)
- Adres Klienta VPN: stały (IP – 99.99.99.11) lub zmienny
- Serwer LDAP/AD:
  - adres IP: 192.168.0.254
  - domena: abc.xyz
  - użytkownik test znajduje się w CN=Users, DC=abc, DC=xyz

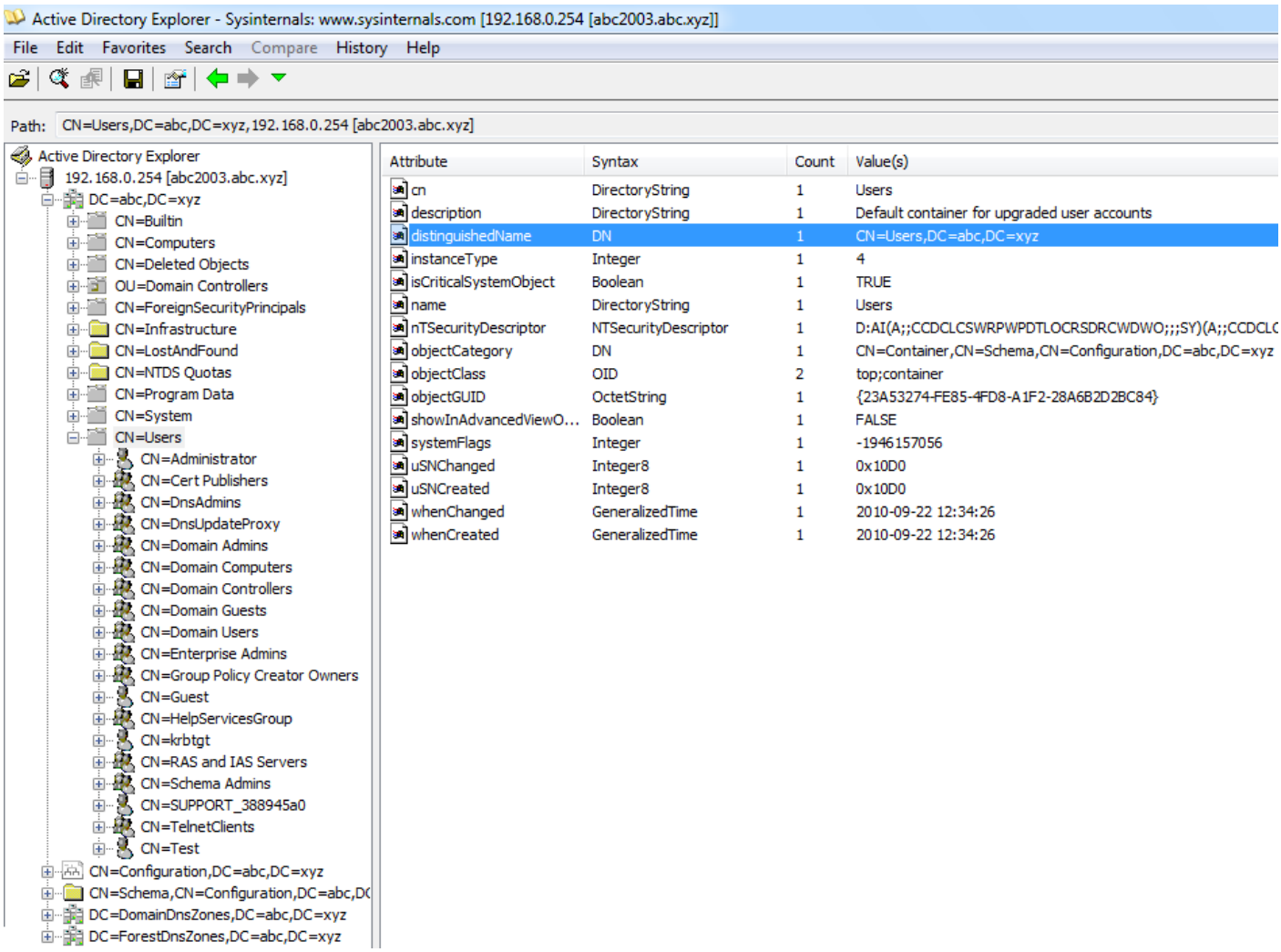
Uwagi

- Dla autentykacji LDAP/AD z użyciem PPTP Vigor wspiera tylko uwierzytelnianie PAP bez szyfrowania.
- 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

1.1. LDAP/AD

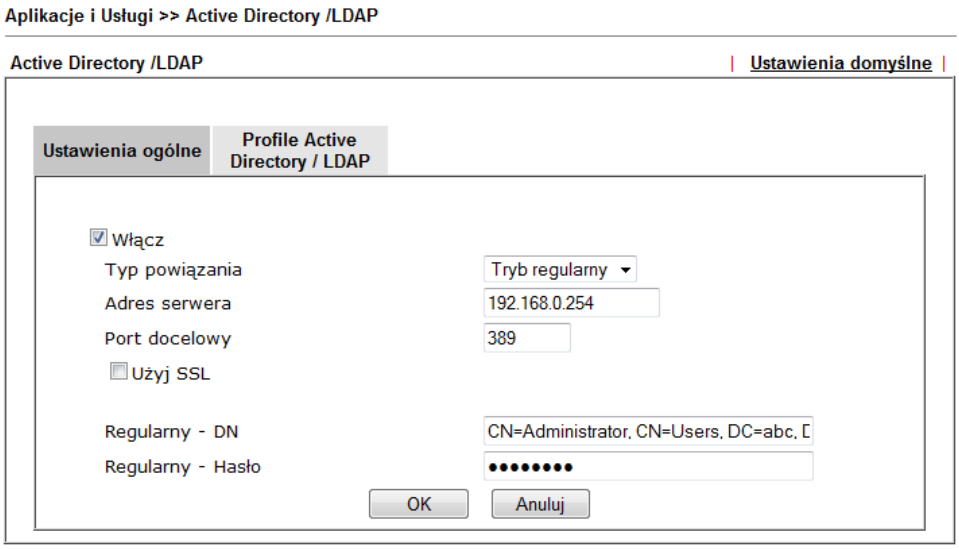
Przeglądarka serwera Active Directory:

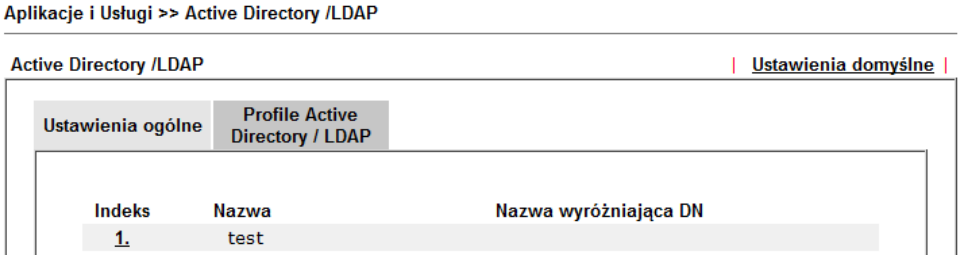


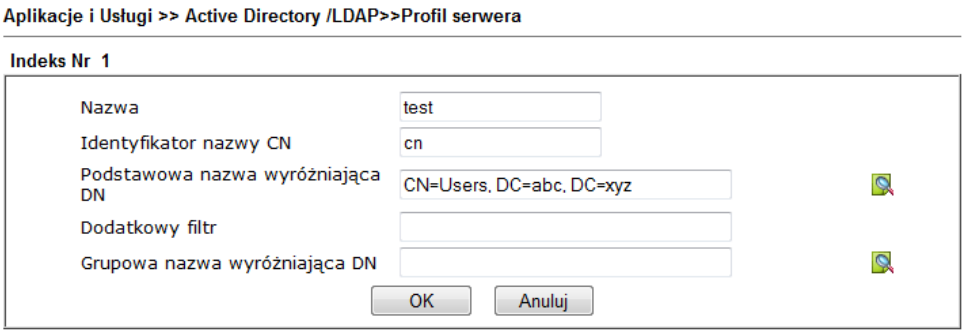
Przejdź do zakładki **Aplikacje i usługi>>LDAP/Active Director**.

Typy powiązania:
- prosty: uwierzytelnianie bez akcji wyszukiwania
- anonimowy: najpierw akcja anonimowego wyszukiwania, następnie uwierzytelnianie
- regularny: podobny do trybu anonimowego. Różnica polega na tym, że serwer sprawdza prawa do wyszukiwania. Konieczność zdefiniowania użytkownika oraz hasła.

Poniżej konfiguracja zgodna z założeniami przykładu.

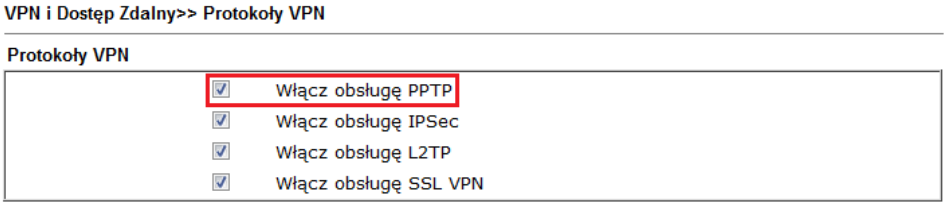




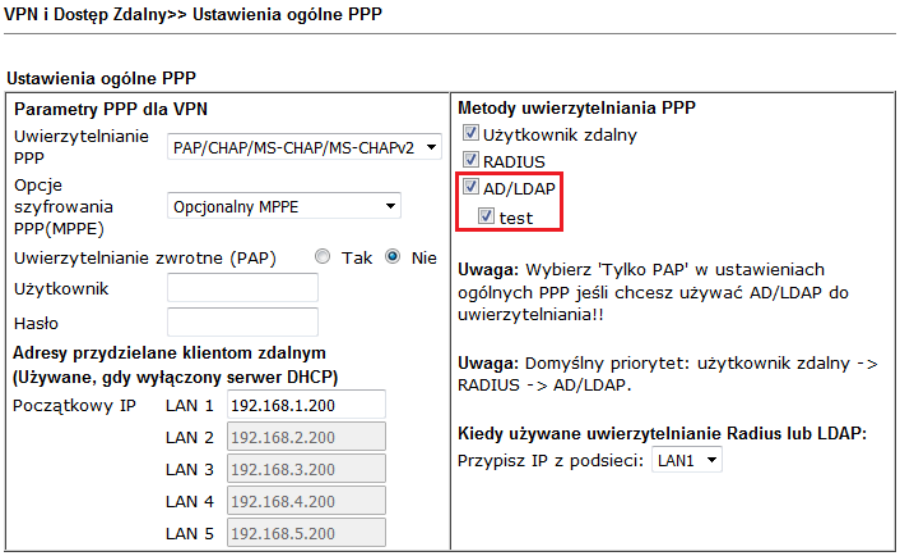


1.2. Ustawienia ogólne

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



Następnie przejdź do zakładki **VPN i Dostęp Zdalny>>Ustawienia Ogólne PPP**. Zaznacz stworzony profil AD/LDAP.



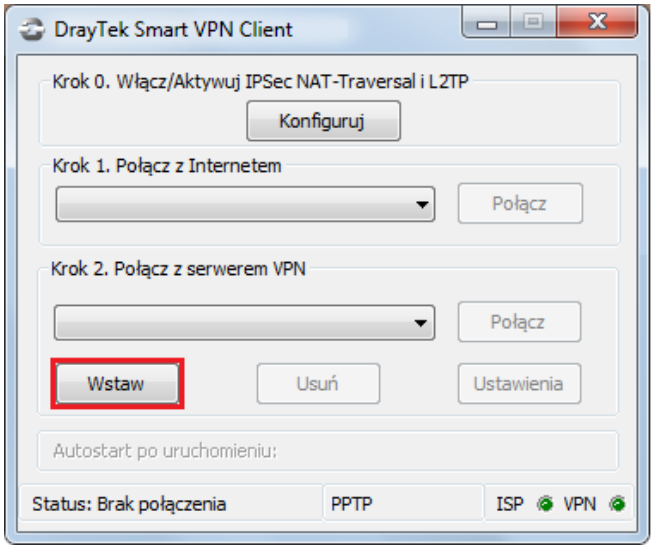
Uwaga

Kolejność sprawdzania konta użytkownika podczas uwierzytelniania:

1. Lokalna baza danych
2. RADIUS
3. AD/LDAP

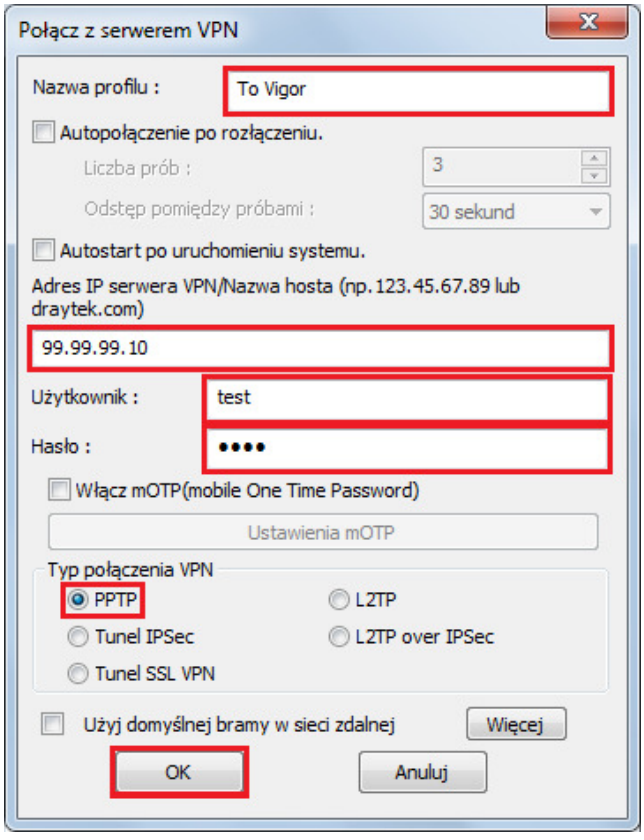
2. Konfiguracja klienta VPN

Kliknij przycisk **Wstaw**.



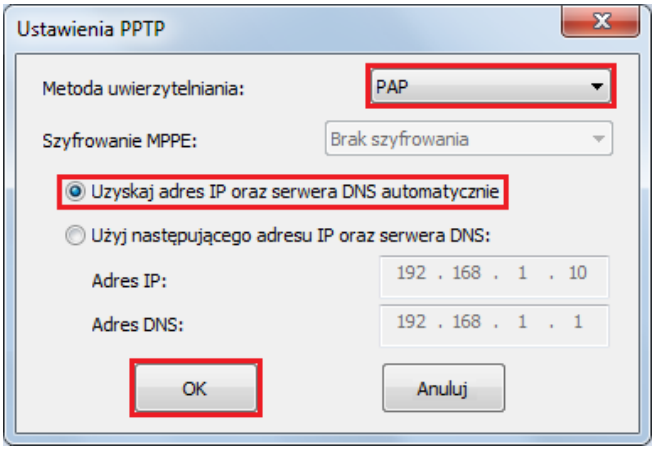
Wypełnij dane dotyczące adresu serwera i typu VPN:

- 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 odpowiednie hasło zgodne z serwerem LADAP/AD. W przykładzie użyto 'test'
- w polu Typ połączenia VPN wybierz PPTP
- kliknij przycisk OK, aby kontynuować

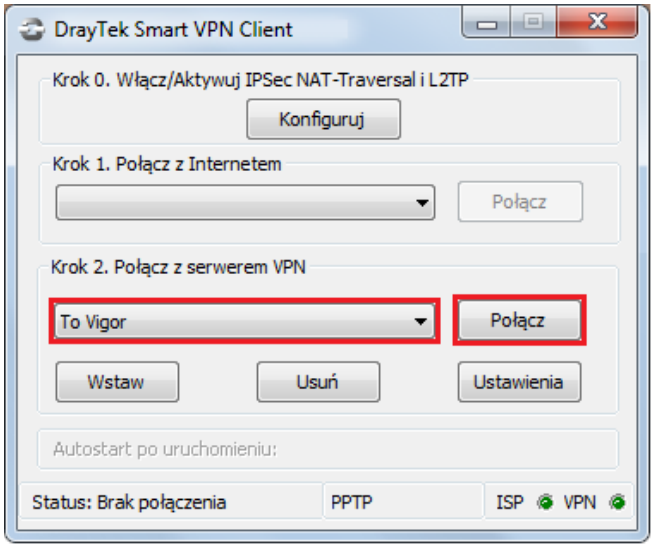


Wypełnij dane dotyczące Ustawień PPTP:

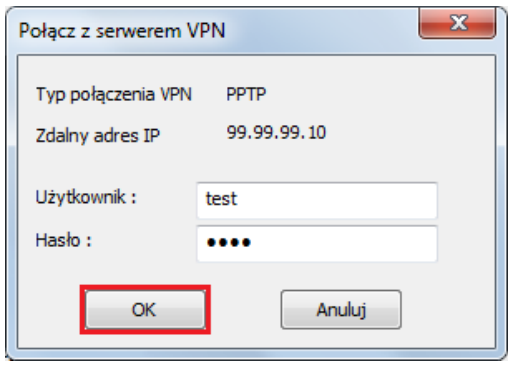
- w polu Metoda uwierzytelniania wybierz PAP
- kliknij przycisk OK, aby zapisać zmiany



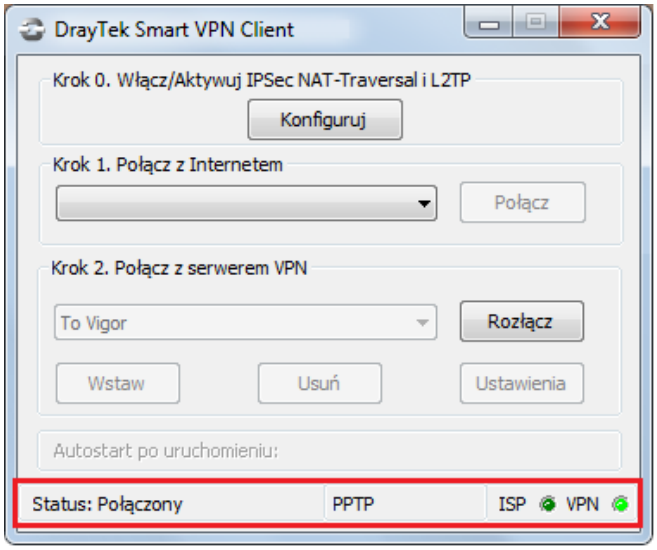
Wybierz odpowiedni profil a następnie kliknij Połącz.



Następnie kliknij OK.



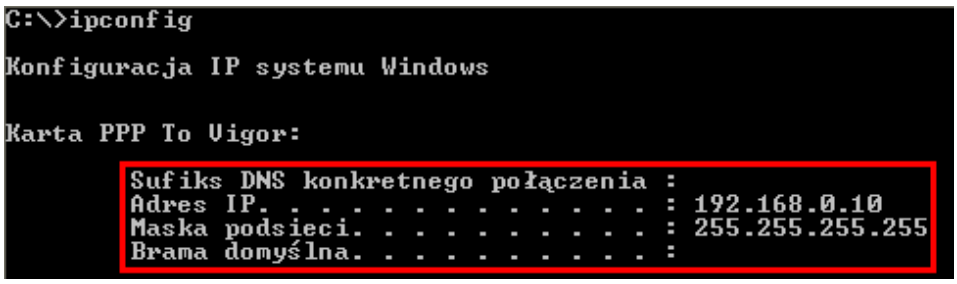
Przy poprawnym połączeniu zmieni się status na Połączony oraz zapali się zielone światełko przy polu VPN.



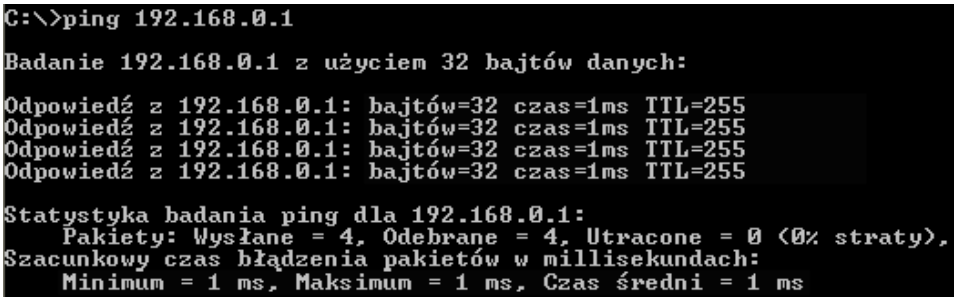
3. Status Połączenia

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.

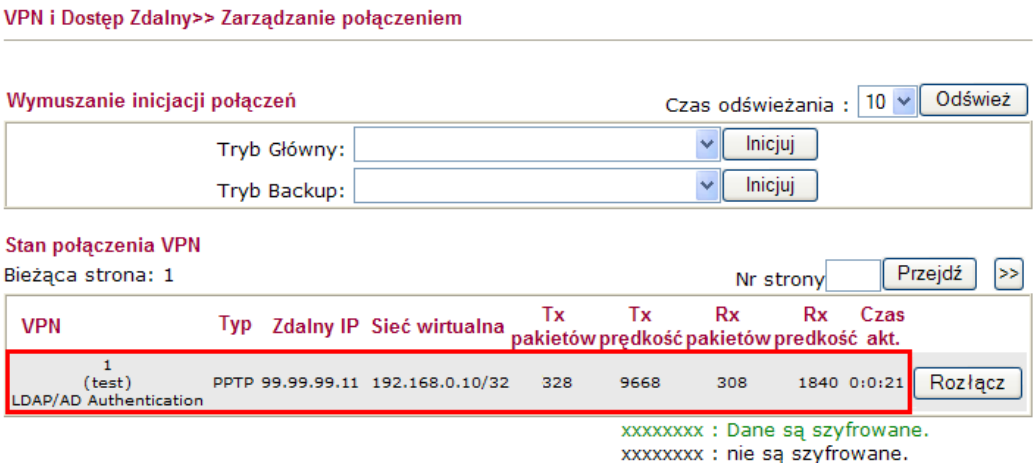


Dodatkowo wystarczy np. zwykły ping. Wykonaj polecenie ping adres_LAN_serwera (w przykładzie serwer VPN posiada adres LAN 192.168.0.1). Poprawna odpowiedź na ping świadczy o poprawnej komunikacji w tunelu VPN.



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

© BRINET – wyłączny przedstawiciel DrayTek w Polsce – www.brinet.pl – www.draytek.pl