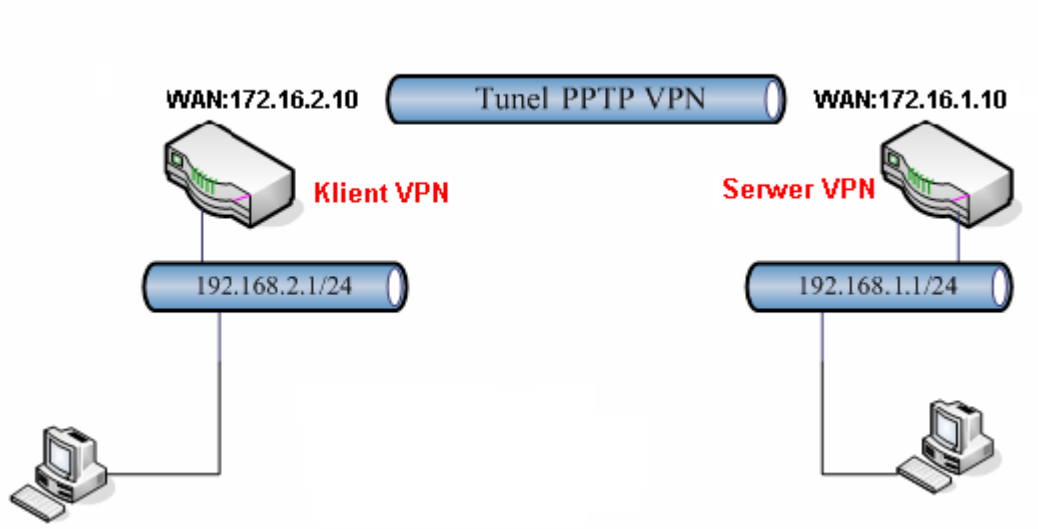
1. Konfiguracja serwera VPN

2. Konfiguracja klienta VPN

3. Status połączenia

Procedura konfiguracji została oparta na poniższym przykładzie.



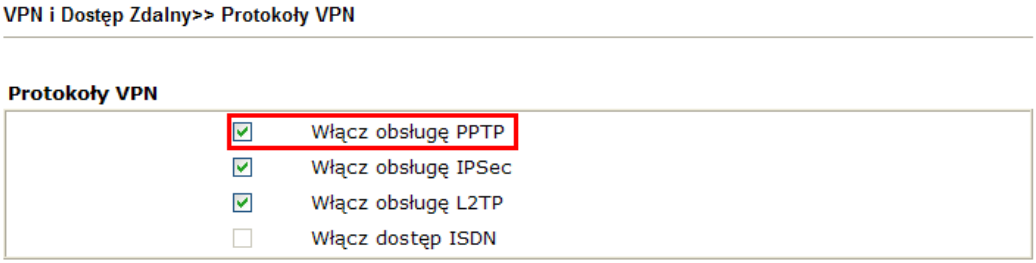
Główne założenia:

- typ tunelu: LAN-LAN z routingiem pomiędzy podsieciami
- protokół VPN: PPTP
- Adres IP Serwera VPN: statyczny. W przykładzie 172.16.1.10
- Adres IP Klienta VPN: statyczny lub dynamiczny. W przykładzie 172.16.2.10
- różne adresacje LAN:
  - serwer VPN: 192.168.1.1 /24
  - klient VPN: 192.168.2.1 /24

Uwaga!
Wymagane są różne adresacje sieci lokalnych

1. Konfiguracja serwera VPN

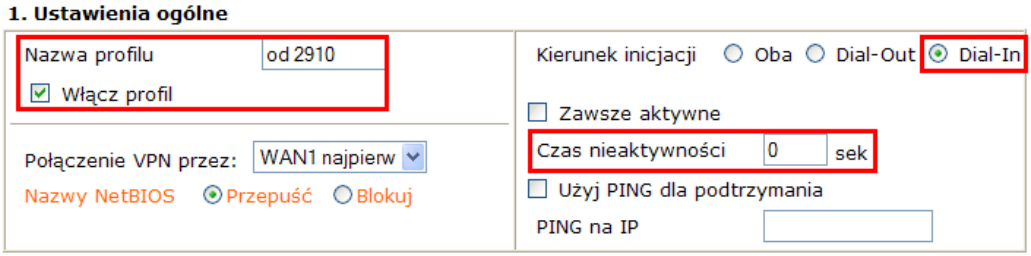
Przejdź do zakładki **VPN i Dostęp Zdalny>>Protokoły VPN** w panelu konfiguracyjnym routera i sprawdź (lub zaznacz) czy jest włączona obsługa protokołu PPTP. Domyślnie włączona jest obsługa protokołów PPTP, IPSec i L2TP.



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.

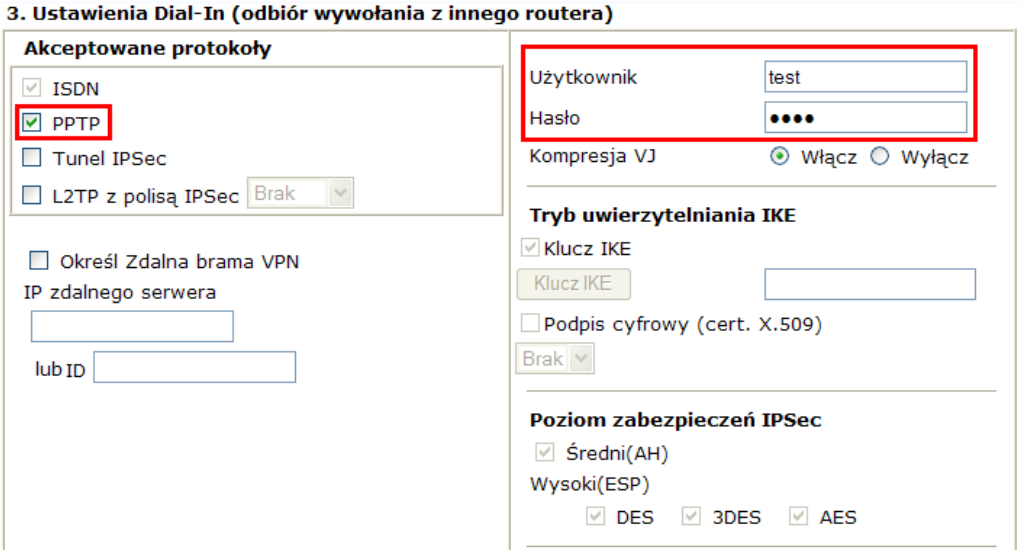
Konfiguracja części **Ustawienia ogólne** zgodna z założeniami przykładu:

- wpisz dowolną nazwę profilu
- zaznacz **Włącz profil**
- jako kierunek inicjacji wybierz **Dial-In**
- ustaw **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.

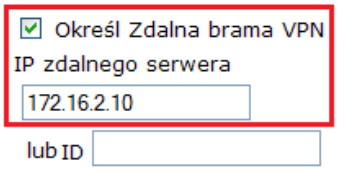


Konfiguracja części **Ustawienia Dial-In** zgodna z założeniami przykładu:

- w polu Protokół dla połączenia wybierz **PPTP**
- w polu **Użytkownik** wpisz odpowiednią nazwę użytkownika. W przykładzie użyto użytkownika 'test'
- w polu **Hasło** wpisz odpowiednie hasło. W przykładzie użyto hasła 'test'

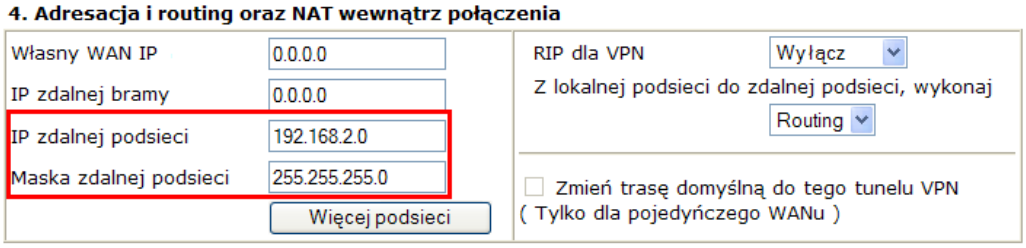


- jeżeli chcesz dodatkowo weryfikować adres IP inicjującego połączenie zaznacz opcję **Określ Zdalna brama VPN**, a w polu **IP zdalnego serwera** wpisz odpowiedni adres IP klienta VPN. W przykładzie 172.16.2.10.



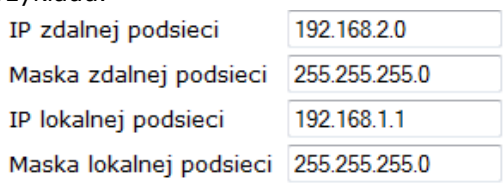
Konfiguracja części **Adresacja i routing oraz NAT wewnątrz połączenia** zgodna z założeniami przykładu:

- w przykładzie Zdalna podsieć: 192.168.2.0, Maska podsieci zdalnej: 255.255.255.0



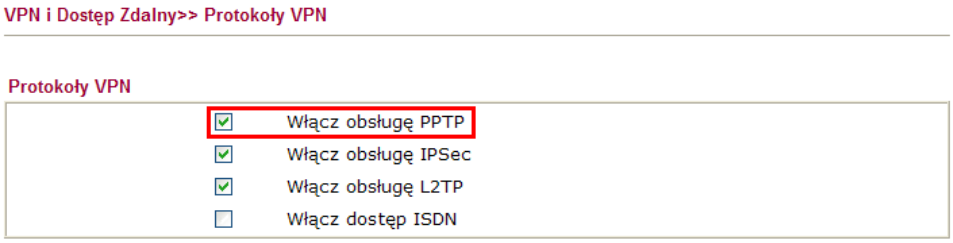
Uwaga!!!

W niektórych modelach dostępne są dodatkowe pola określające IP lokalnej podsieci oraz jej maskę. Poniżej konfiguracja zgodna z założeniami przykładu.



2. Konfiguracja klienta VPN

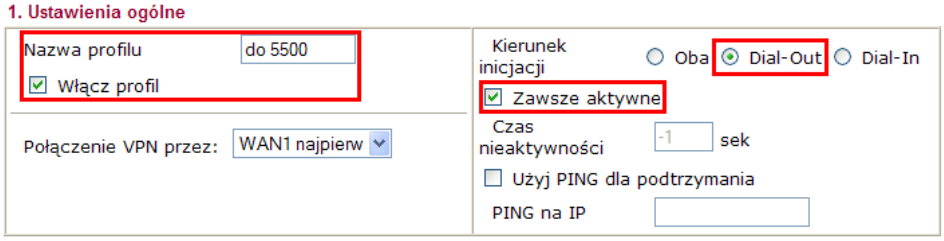
Przejdź do zakładki **VPN i Dostęp Zdalny>>Protokoły VPN** w panelu konfiguracyjnym routera i sprawdź (lub zaznacz) czy jest włączona obsługa protokołu PPTP. Domyślnie włączona jest obsługa protokołów PPTP, IPSec i L2TP.



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.

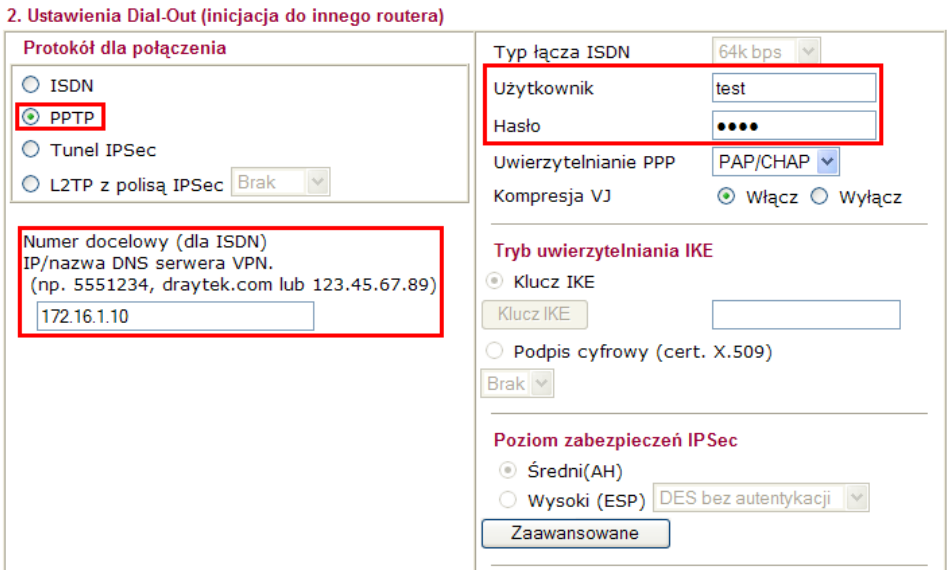
Konfiguracja części **Ustawienia ogólne** zgodna z założeniami przykładu:

- 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.



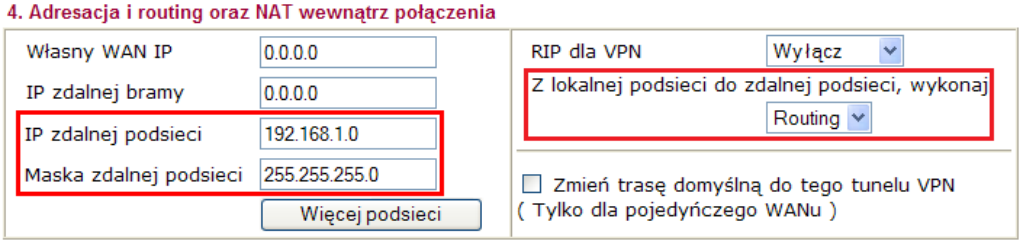
Konfiguracja części **Ustawienia Dial-Out** zgodna z założeniami przykładu:

- w polu Protokół dla połączenia wybierz **PPTP**
- w polu **IP/nazwa DNS serwera VPN** wpisz adres IP routera, do którego zestawiasz tunel VPN, albo jego nazwę. W przykładzie użyto adresu IP 172.16.1.10
- w polu **Użytkownik** wpisz odpowiednią nazwę użytkownika. W przykładzie użyto użytkownika 'test'
- w polu **Hasło** wpisz odpowiednie hasło. W przykładzie użyto hasła 'test'



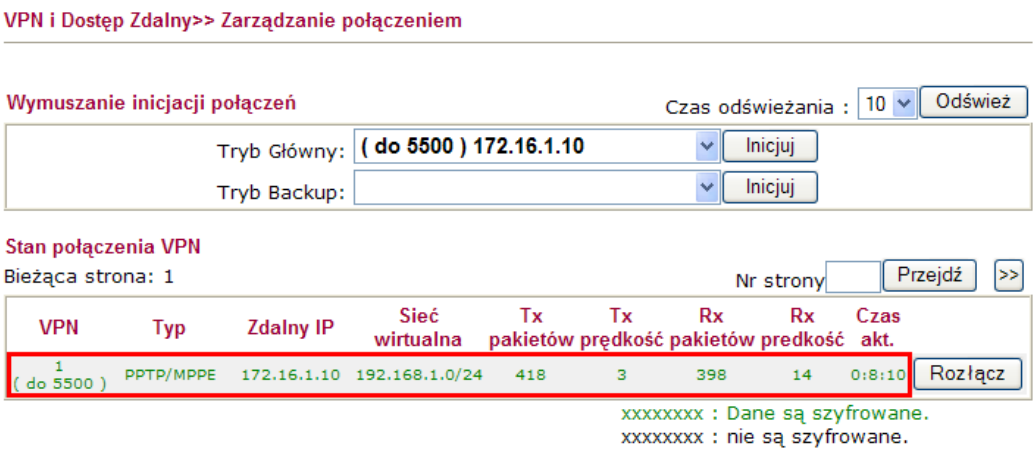
Konfiguracja części **Adresacja i routing oraz NAT wewnątrz połączenia** zgodna z założeniami przykładu:

- w przykładzie Zdalna podsieć: 192.168.1.0, Maska podsieci zdalnej: 255.255.255.0

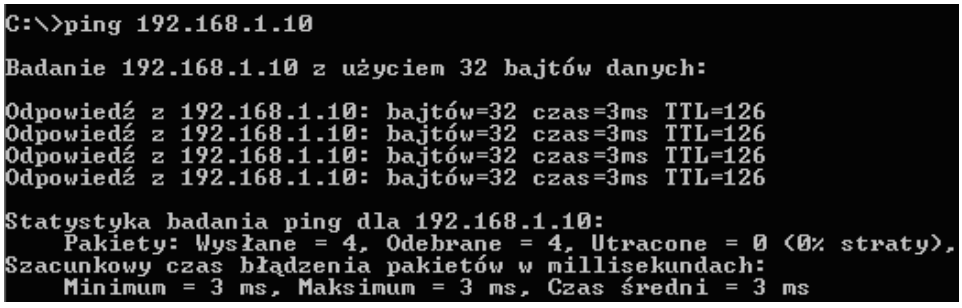


3. Status połączenia (od strony klienta VPN)

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



Inna metoda to np. zwykły ping. Wybierz Menu Start a następnie Uruchom i wpisz cmd . Następnie wykonaj polecenie: ping adres_hosta_w_LAN-ie (patrz rysunek poniżej, gdzie host posiada adres LAN-owy 192.168.1.10). Po zainicjowaniu tunelu otrzymasz poprawną odpowiedź na ping – świadczy ona o poprawnej komunikacji w tunelu VPN.



Krzysztof Skowina
Specjalista ds. rozwiązań sieciowych
BRINET Sp. z o.o.
k.skowina@brinet.pl