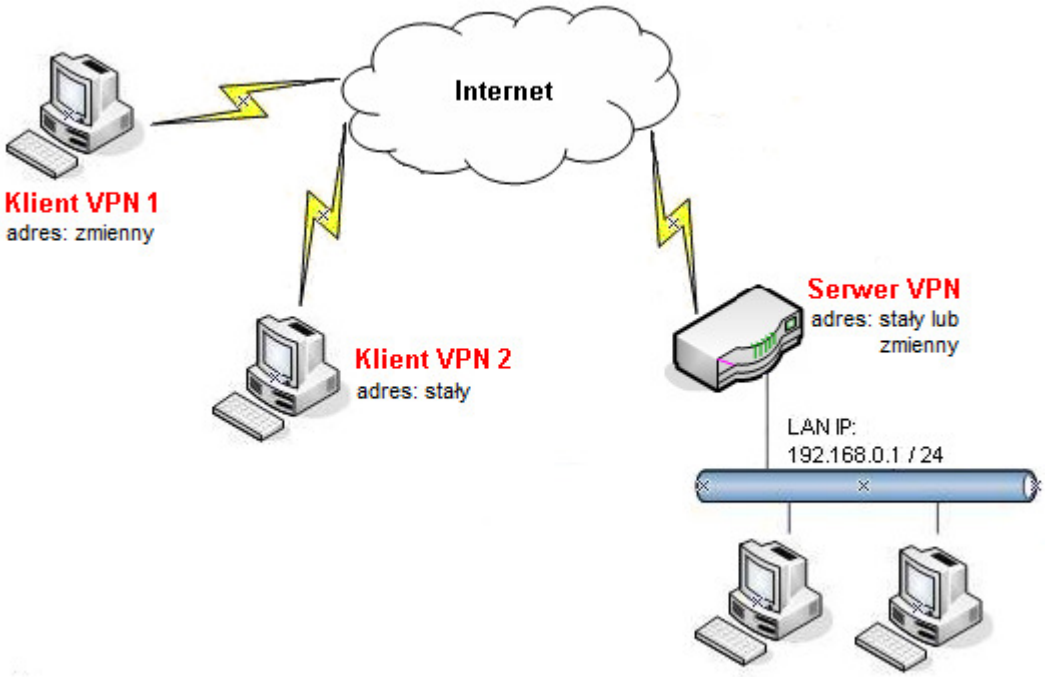
Procedura konfiguracji została oparta na poniższym przykładzie.



Główne założenia:

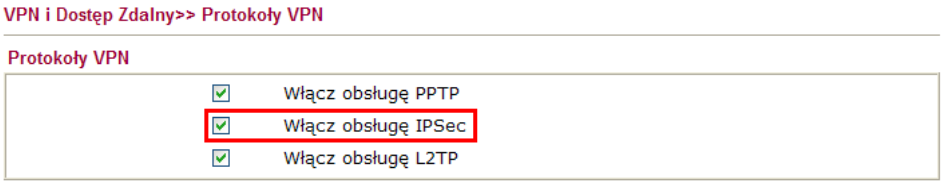
- typ tunelu: Host-LAN
- protokół VPN: IPSec (tryb główny)
- szyfrowanie: 3DES
- integralność: SHA1
- autentykacja: klucz IKE
- aktywność tunelu: ograniczona czasowo
- klient VPN nie wspiera DPD dla IPSec
- Adres Serwera VPN: stały (IP - 99.99.99.10) lub zmienny (domenowy - serwer.abc.xyz)
- Adres Klienta 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.

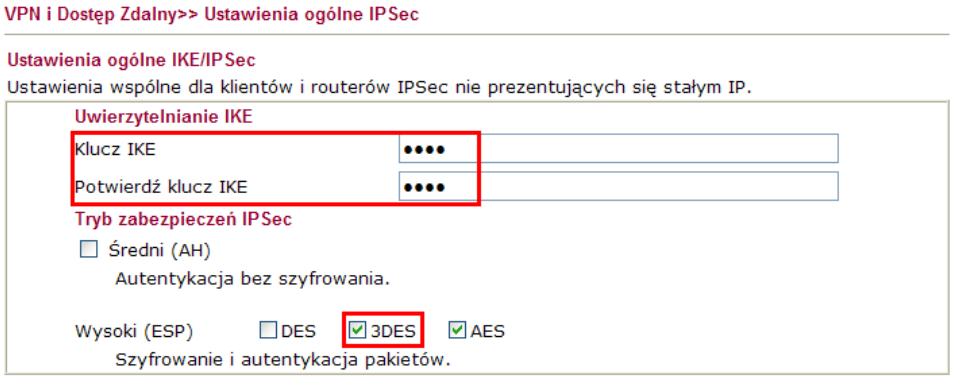
1.Konfiguracja serwera VPN

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



1.1. Profil dla klienta ze zmiennym IP

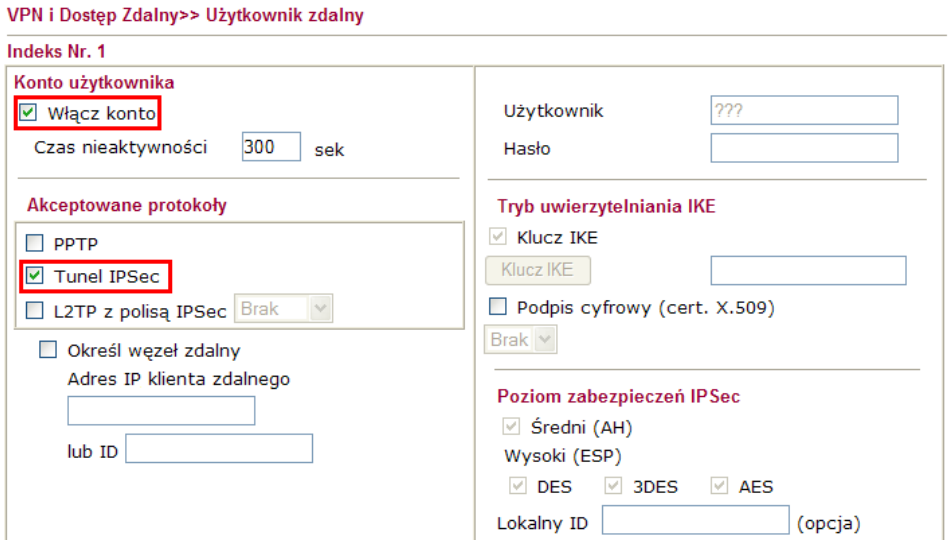
Przejdź do zakładki **VPN i Dostęp Zdalny>>Ustawienia ogólne IPSec**. Wpisz wspólny **klucz IKE** (w przykładzie użyto klucza 'test') oraz wybierz **3DES** jako Tryb zabezpieczeń IPSec.



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**. Domyślnie jest tam wartość 300 oznaczająca rozłączenie tunelu po 5 minutach, gdy Vigor nie odnotuje ruchu VPN. IPSec nie posiada wbudowanych mechanizmów detekcji połączenia – detekcja połączenia realizowana jest za pomocą DPD (Dead Peer Detection).
- jako akceptowany protokół zaznacz **Tunel IPSec**

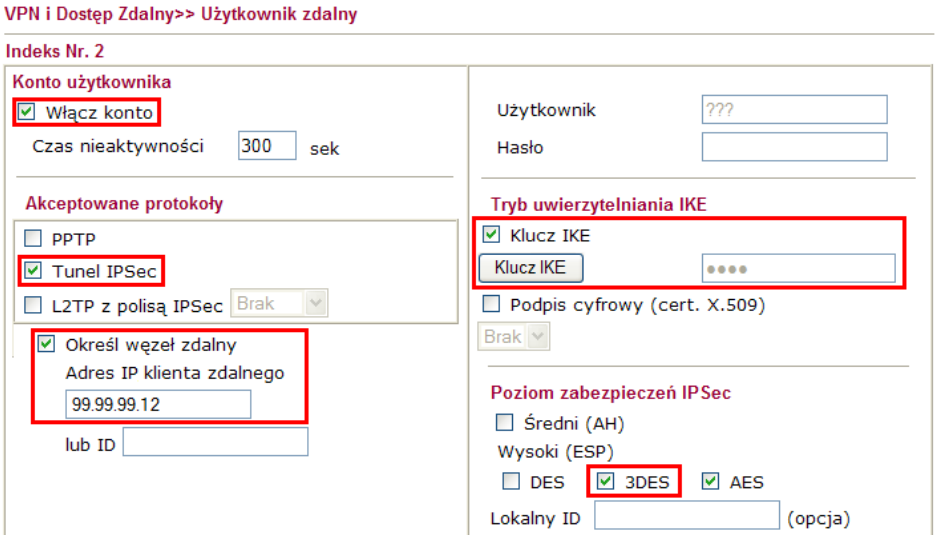


1.2. Profil dla klienta ze stałym IP

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

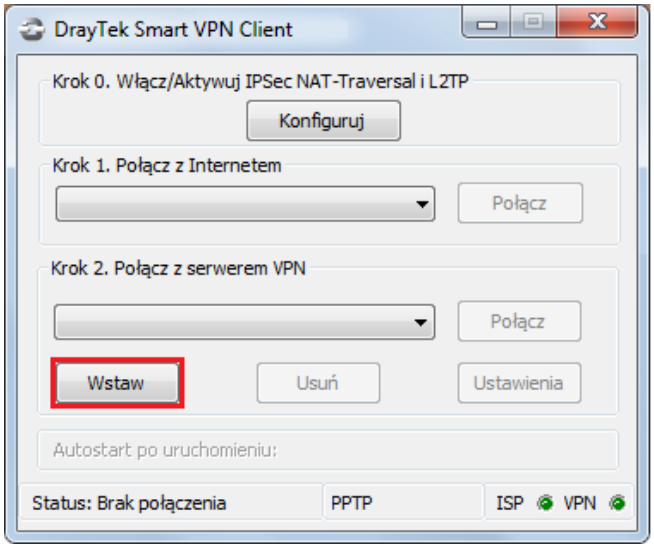
Konfiguracja zgodna z założeniami przykładu:

- zaznacz **Włącz konto**
- ustaw **Czas nieaktywności**. Domyślnie jest tam wartość 300 oznaczająca rozłączenie tunelu po 5 minutach, gdy Vigor nie odnotuje ruchu VPN. IPSec nie posiada wbudowanych mechanizmów detekcji połączenia – detekcja połączenia realizowana jest za pomocą DPD (Dead Peer Detection).
- zaznacz **Określ węzeł zdalny** i wpisz odpowiedni adres. W przykładzie użyto 99.99.99.12
- 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



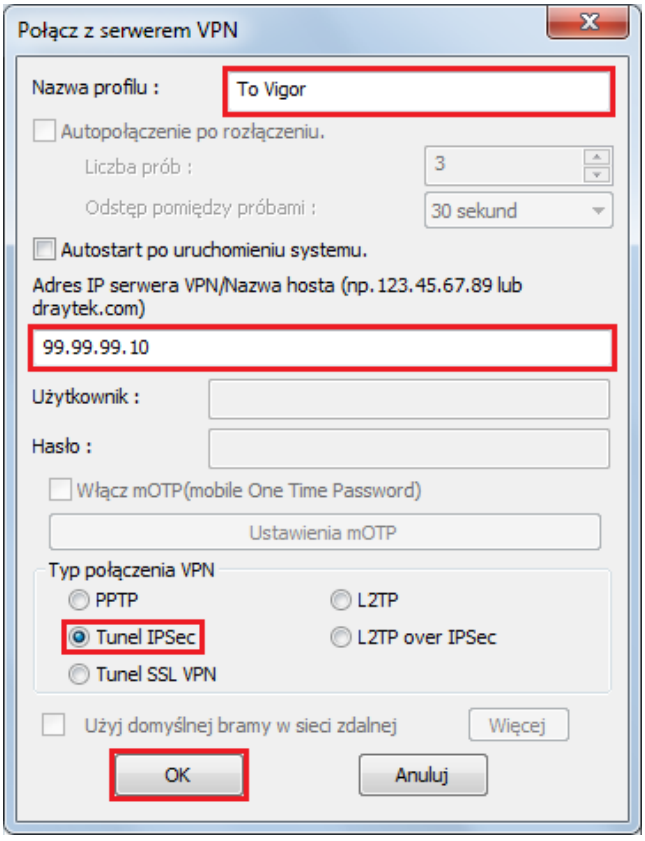
2. Konfiguracja klienta VPN

Kliknij przycisk **Wstaw**



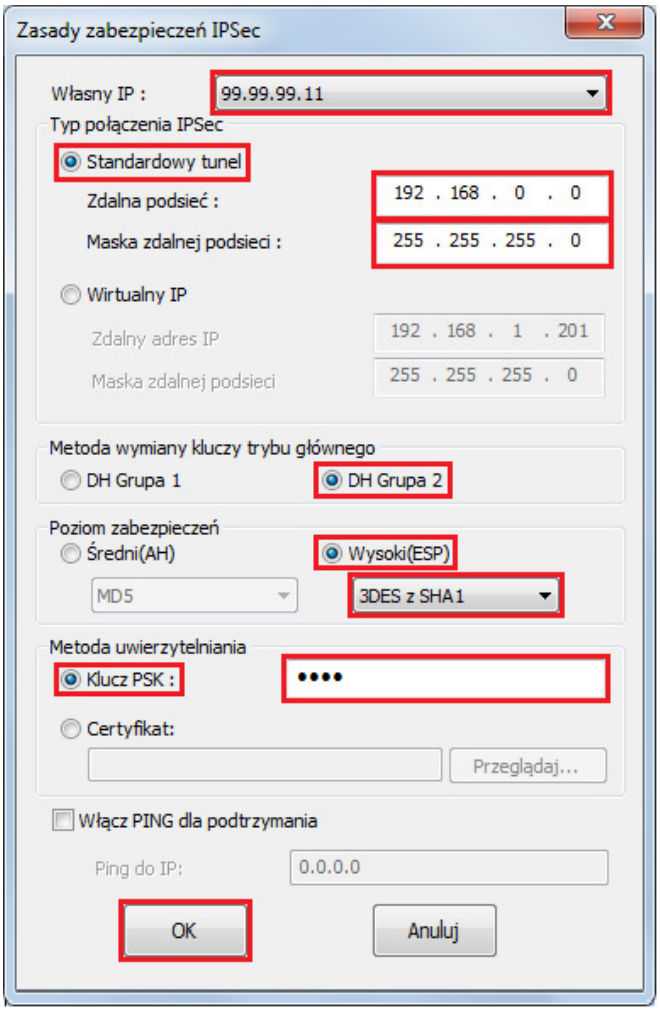
Wypełnij dane dotyczące adresu serwera i typu VPN:

- 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 Typ połączenia VPN wybierz Tunel IPSec.
- kliknij OK, aby kontynuować



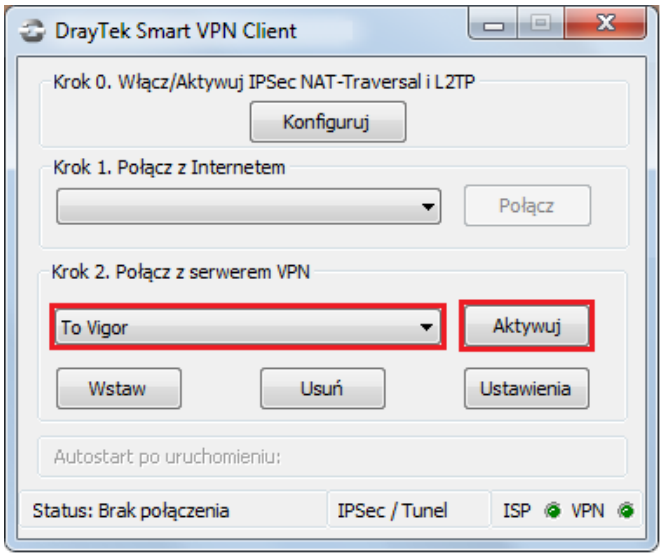
Wypełnij dane dotyczące zabezpieczeń IPSec:

- w polu Mój adres IP wybierz odpowiedni adres IP swojego komputera. W przykładzie 99.99.99.11.
- w polu Typ połączenia IPSec wybierz Standardowy tunel IPSec oraz wpisz adresację zdalnej podsieci. W przykładzie Zdalna podsieć: 192.168.0.0, Maska podsieci zdalnej: 255.255.255.0.
- w polu Metoda zabezpieczeń wybierz protokół realizujący szyfrowanie i uwierzytelnianie. W przykładzie wybrano Wysokie(ESP) oraz 3DES with SHA1.
- w polu Metoda uwierzytelniania wybierz Klucz PSK i wpisz klucz. W przykładzie użyto klucza 'test'.
- kliknij przycisk OK, aby zapisać zmiany.

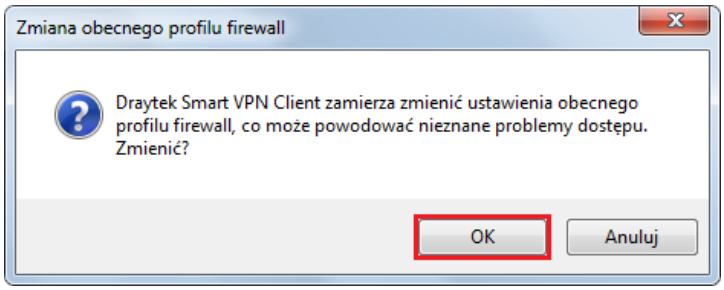


3. Zainicjowanie połączenia

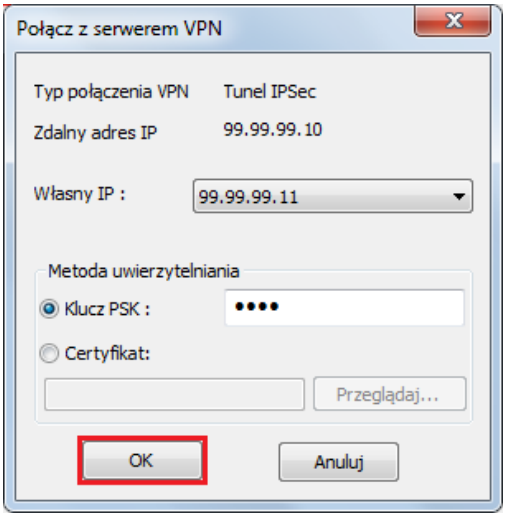
Wybierz odpowiedni profil a następnie kliknij przycisk Aktywuj.



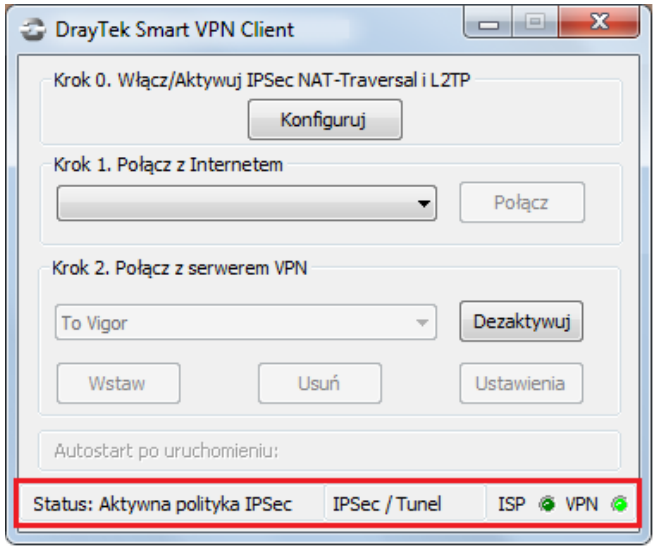
Zaakceptuj zmiany w Zaporze systemu Windows m.in. włączenie zapory, dodanie reguły zabezpieczeń połączeń.



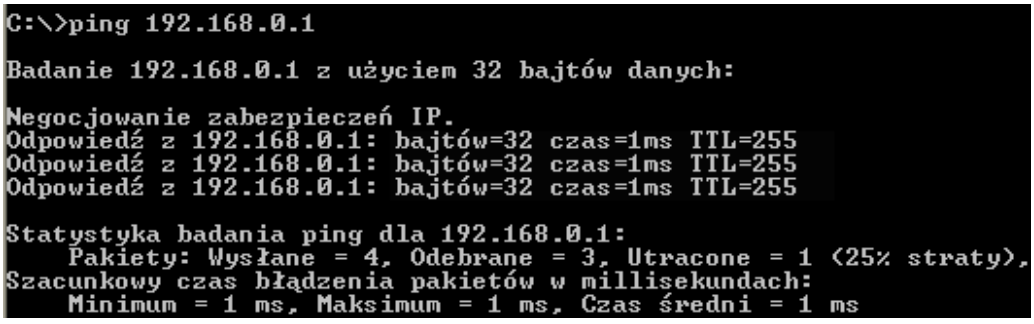
Następnie kliknij OK.



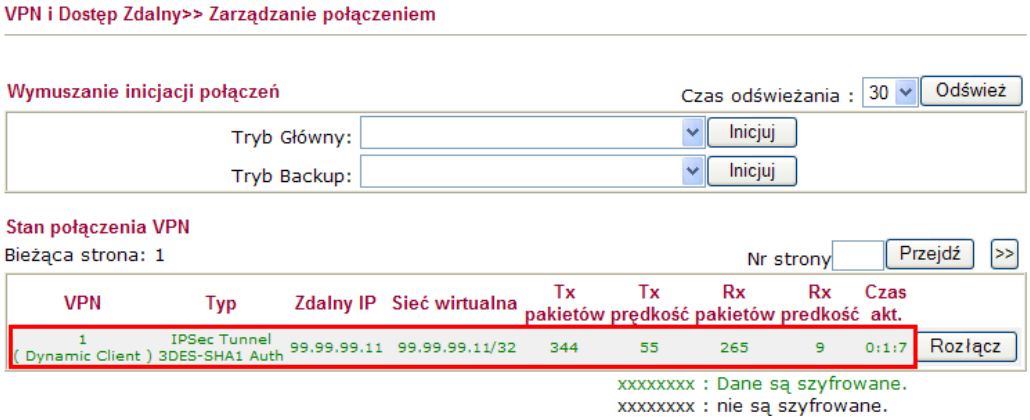
Dla standardowego tunelu IPSec zmieni się status na Aktywna polityka IPSec oraz zapali się zielone światełko przy polu VPN.



Aby „obudzić" tunel należy zainicjować dowolny ruch w kierunku routera. Wystarczy np. zwykły ping. Wybierz Menu Start a następnie Uruchom i wpisz cmd . Następnie wykonaj polecenie: ping adres_LAN_serwera (w przykładzie serwer VPN posiada adres LAN 192.168.0.1). Komunikat „Negocjowanie zabezpieczeń IP" świadczy o wymianie niezbędnych informacji do inicjacji tunelu. Po zainicjowaniu tunelu otrzymasz poprawną odpowiedź na ping – świadczy ona o poprawnej komunikacji w tunelu VPN.



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



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