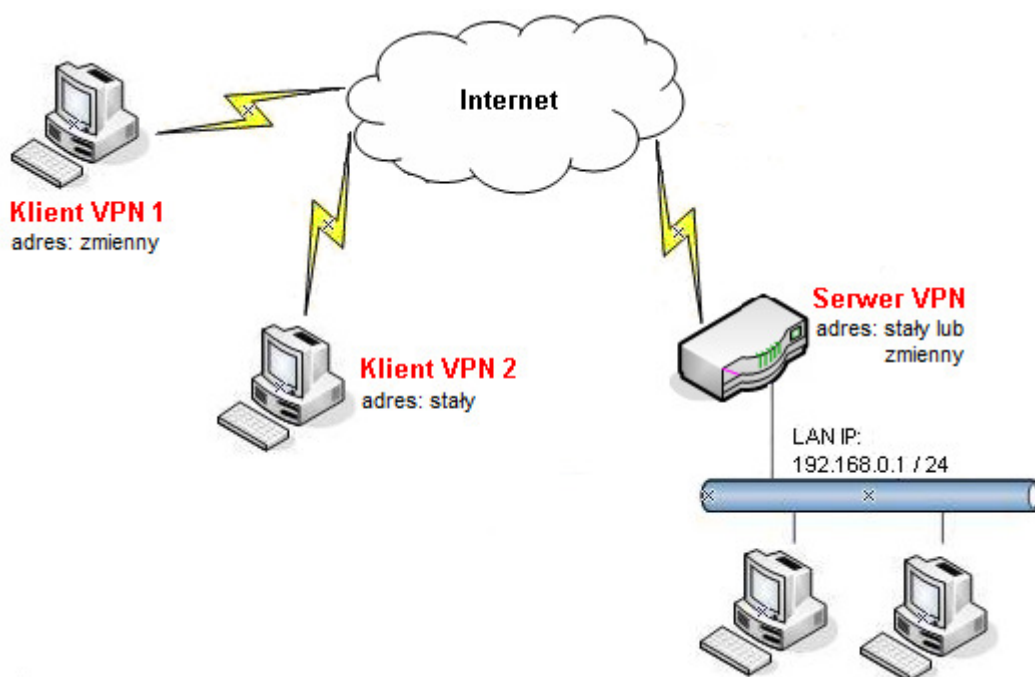


1. Konfiguracja serwera VPN
 - 1.1. Profil dla klienta ze zmiennym IP
 - 1.2. Profil dla klienta ze stałym IP
2. Konfiguracja klienta VPN
3. Zainicjowanie połączenia

Procedura konfiguracji została oparta na poniższym przykładzie.

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
- 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)

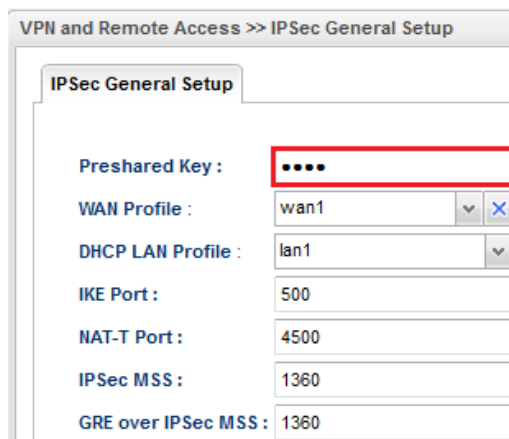
Uwagi

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

1.1. Profil dla klienta ze zmiennym IP

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



VPN and Remote Access >> IPsec General Setup

IPsec General Setup

Preshared Key :

WAN Profile : wan1

DHCP LAN Profile : lan1

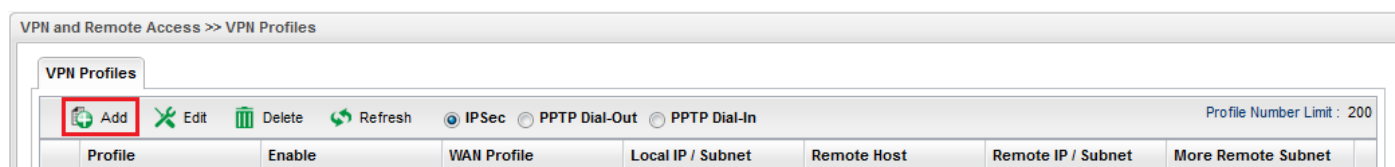
IKE Port : 500

NAT-T Port : 4500

IPsec MSS : 1360

GRE over IPsec MSS : 1360

Przejdź do zakładki **VPN and Remote Access >> VPN Profiles**. Kliknij przycisk **Add (Dodaj)**.



VPN and Remote Access >> VPN Profiles

VPN Profiles

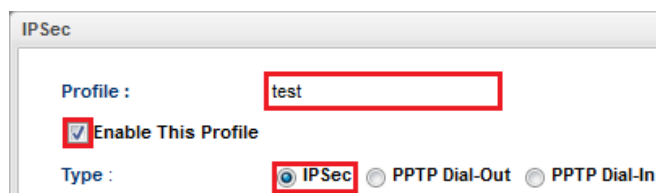
IPsec PPTP Dial-Out PPTP Dial-In Profile Number Limit : 200

Profile	Enable	WAN Profile	Local IP / Subnet	Remote Host	Remote IP / Subnet	More Remote Subnet

Wpisz nazwę profilu.

Zaznacz **Enable This Profile (Włącz ten profil)**.

Dla opcji **Type (Typ)** wybierz **IPsec**.



IPsec

Profile : test

Enable This Profile

Type : IPsec PPTP Dial-Out PPTP Dial-In

W ustawieniach Basic(Podstawowe):

- Dla opcji **For Remote Dial-in User(Dla użytkownika zdalnego)** wybierz **Enable(Włącz)**.
- W polu **Local IP(Lokalny IP)/Subnet(Maska)** wpisz odpowiedni adres IP oraz wybierz odpowiednią maskę.
- W polu **Remote Host(Zdalny host)** wpisz **0.0.0.0** (dowolny adres IP Klienta VPN)

Basic | Advanced | GRE | Proposal | PPTP

Always On : Enable Disable

For Remote Dial-In User : **Enable** Disable

WAN Profile : wan1 Default WAN IP WAN Alias IP

Local IP / Subnet : 192 . 168 . 0 . 0 255.255.255.0

Local Next Hop :

Remote Host : 0.0.0.0

Auth Type : PSK (While Remote Host as 0.0.0.0, PSK will be defined in IPSec General Setup)

Security Protocol : ESP

W ustawieniach Proposal(Propozycja):

- W polu Accepted Proposal [Dial-In] wybierz **acceptall(akceptuj wszystko)**.

Basic | Advanced | GRE | Proposal | PPTP

IKE Phase1 Proposal [Dial-Out] : DES_G1

IKE Phase1 Authentication [Dial-Out] : ALL

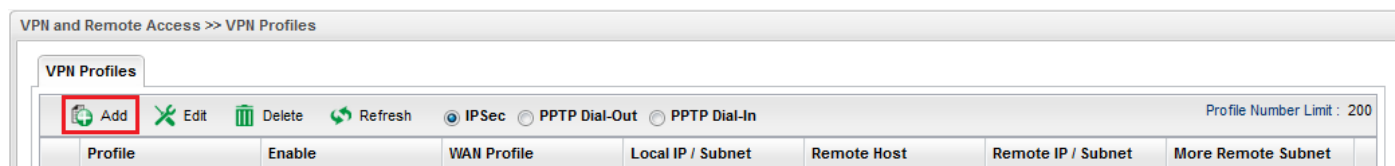
IKE Phase2 Proposal [Dial-Out] : 3DES_with_auth

IKE Phase2 Authentication [Dial-Out] : ALL

Accepted Proposal [Dial-In] : **acceptall**

1.2. Profil dla klienta ze stałym IP

Przejdź do zakładki **VPN and Remote Access >> VPN Profiles**. Kliknij przycisk **Add(Dodaj)**.



Wpisz nazwę profilu.

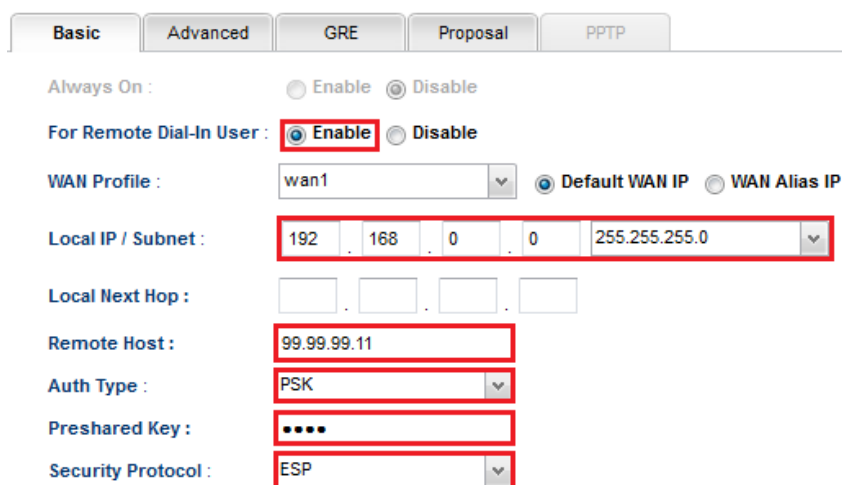
Zaznacz **Enable This Profile(Włącz ten profil)**.

Dla opcji **Type(Typ)** wybierz **IPSec**.



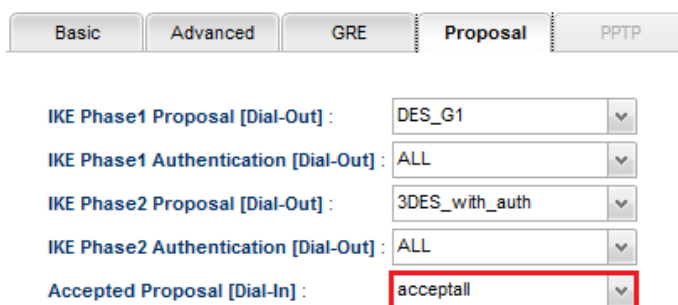
W ustawieniach Basic(Podstawowe):

- Dla opcji **For Remote Dial-in User(Dla użytkownika zdalnego)** wybierz **Enable(Włącz)**.
- W polu **Local IP(Lokalny IP)/Subnet(Maska)** wpisz odpowiedni adres IP oraz wybierz odpowiednią maskę.
- W polu **Remote Host(Zdalny Host)** wpisz odpowiedni adres IP Klienta VPN. W przykładzie 99.99.99.11.
- W polu **Preshared Key(Klucz PSK)** wpisz klucz. W przykładzie 'test'.



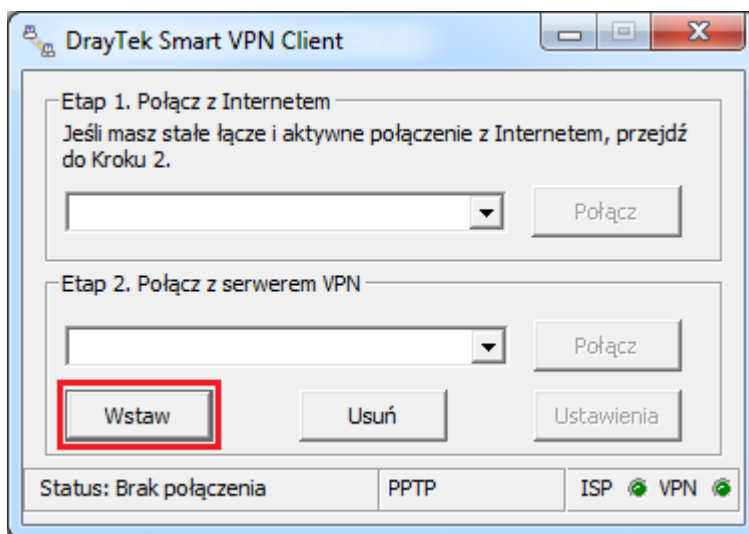
W ustawieniach Proposal(Propozycja):

- W polu Accepted Proposal [Dial-In] wybierz **acceptall(akceptuj wszystko)**.



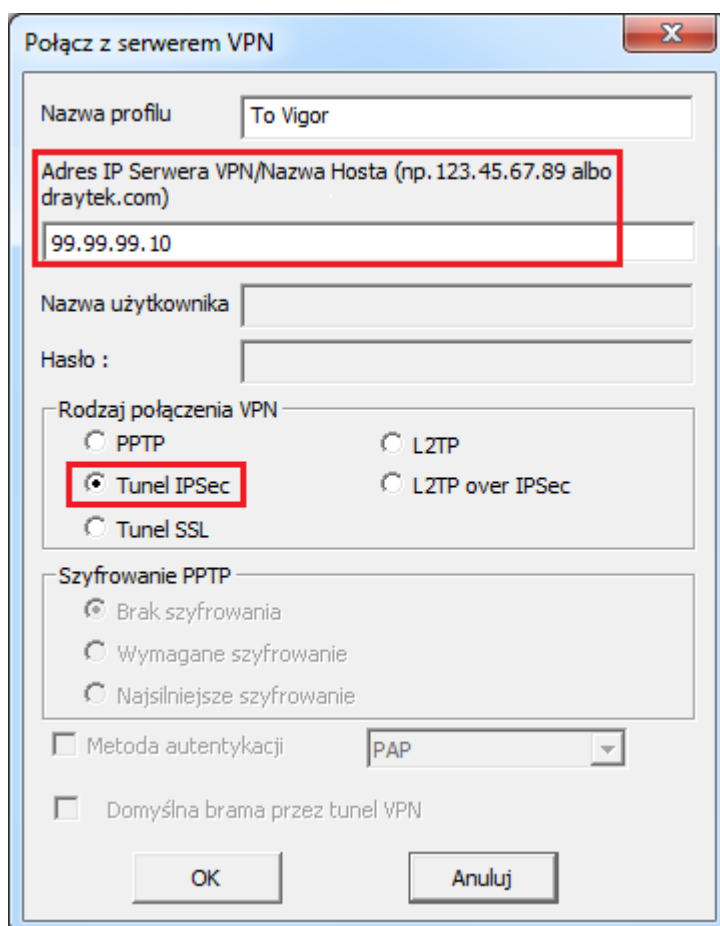
2. Konfiguracja klienta VPN

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 Rodzaj połączenia VPN wybierz Tunel IPSec.
- kliknij **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 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 autentykacji wybierz Klucz PSK i wpisz klucz. W przykładzie użyto klucza 'test'.
- kliknij przycisk OK, aby zapisać zmiany.

Zasady zabezpieczeń IPSec

Mój adres IP : 99.99.99.11

Typ połączenia IPSec

Standardowy Tunel

Zdalna podsieć: 192 . 168 . 0 . 0

Maska podsieci zdalnej : 255 . 255 . 255 . 0

Wirtualny IP

Zdalny adres IP 192 . 168 . 1 . 201

Zdalna maska podsieci 255 . 255 . 255 . 0

Metoda zabezpieczeń

Średnie(AH)

Wysokie(ESP)

MD5 3DES with SHA1

Metoda autentykacji

Klucz PSK : ****

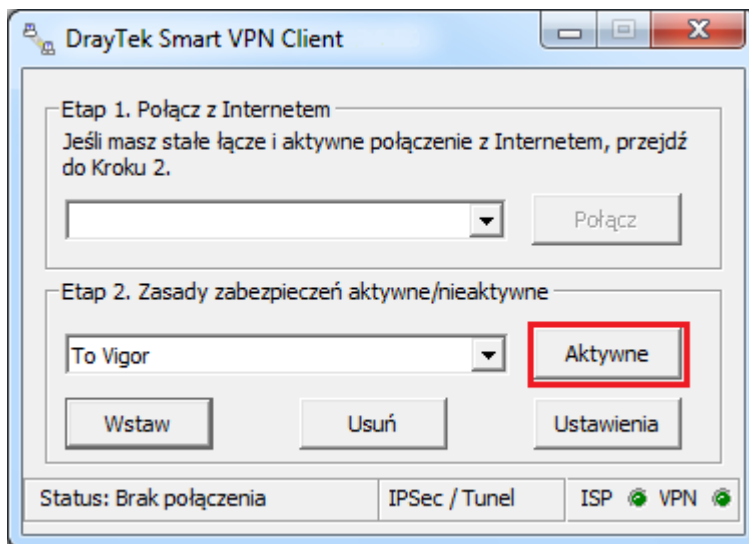
Certyfikat:

Przeglądaj...

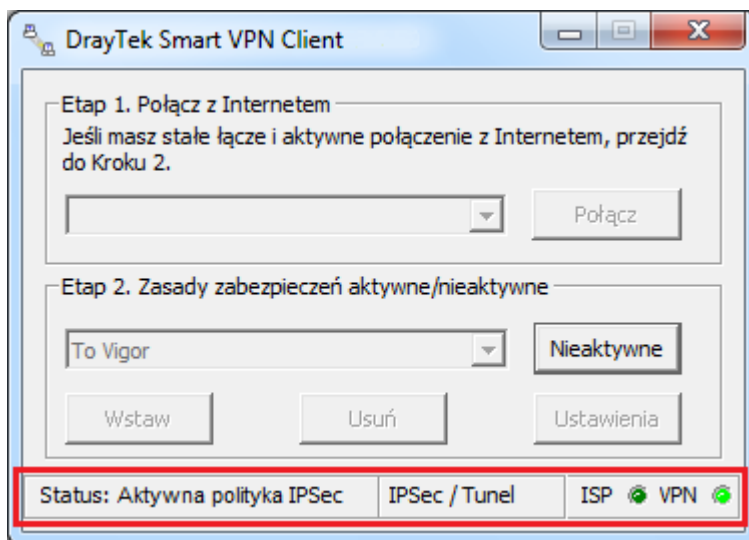
OK Anuluj

3. Zainicjowanie połączenia

Wybierz odpowiedni profil a następnie kliknij przycisk Aktywne.



Dla standardowego tunelu IPSec zmieni się status na Aktywna polityka IPSec oraz zapali się zielone światło 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.

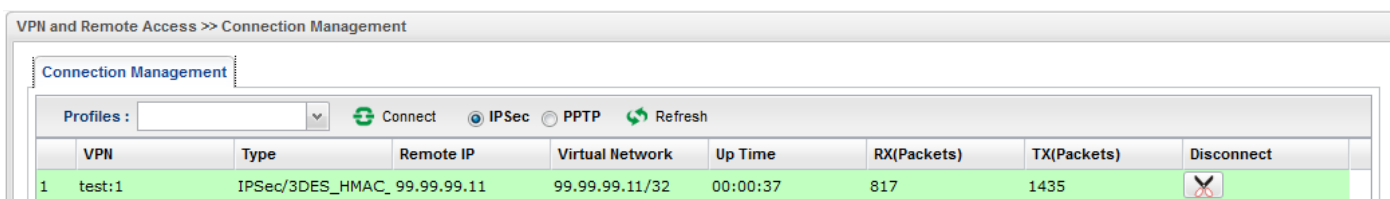
```
C:\>ping 192.168.0.1

Badanie 192.168.0.1 z użyciem 32 bajtów danych:

Negocjowanie zabezpieczeń IP.
Odpowiedź z 192.168.0.1: bajtów=32 czas=1ms TTL=255
Odpowiedź z 192.168.0.1: bajtów=32 czas=1ms TTL=255
Odpowiedź z 192.168.0.1: bajtów=32 czas=1ms TTL=255

Statystyka badania ping dla 192.168.0.1:
Pakiety: Wysłane = 4, Odebrane = 3, Utracone = 1 (25% straty),
Szacunkowy czas błędzenia pakietów w milisekundach:
Minimum = 1 ms, Maksimum = 1 ms, Czas średni = 1 ms
```

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