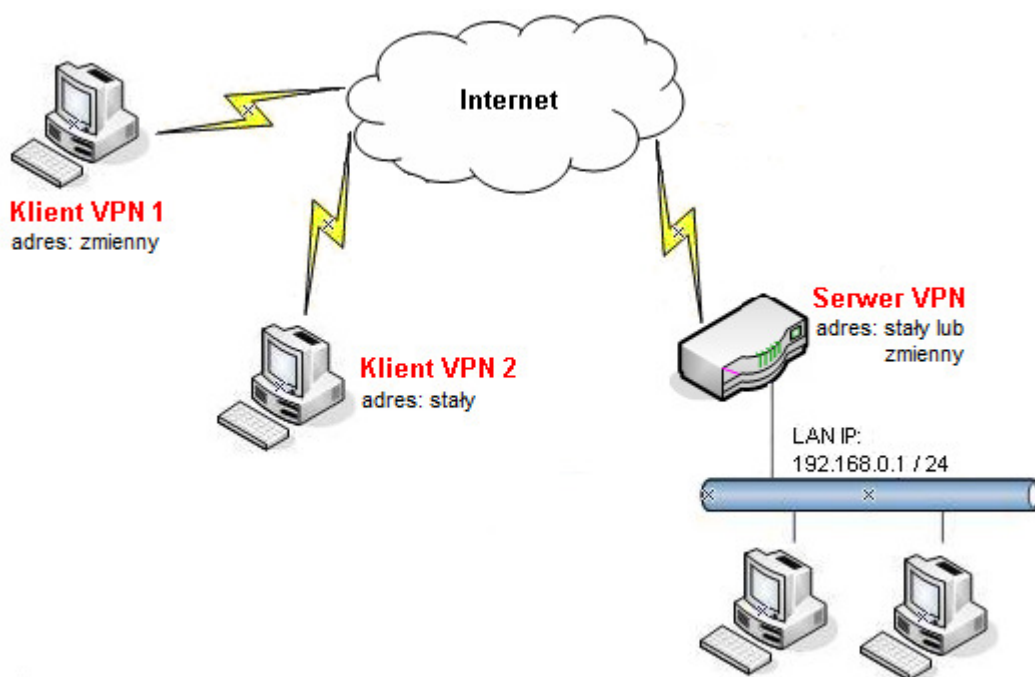


1. Konfiguracja serwera VPN
  - 1.1. Profil dla klienta ze zmiennym IP
  - 1.2. Profil dla klienta ze stałym IP
2. Konfiguracja klienta VPN
3. Zainicjowanie połączenia

Procedura konfiguracji została oparta na poniższym przykładzie.



### 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](http://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.

VPN i Dostęp Zdalny >> Protokoły VPN

Protokoły VPN

<input checked="" type="checkbox"/>	Włącz obsługę PPTP
<input checked="" type="checkbox"/>	Włącz obsługę IPSec
<input checked="" type="checkbox"/>	Włącz obsługę 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.

VPN i Dostęp Zdalny >> Ustawienia ogólne IPSec

Ustawienia ogólne IKE/IPSec

Ustawienia wspólne dla klientów i routerów IPSec nie prezentujących się stałym IP.

<b>Uwierzytelnianie IKE</b>	
Klucz IKE	.....
Potwierdź klucz IKE	.....
<b>Tryb zabezpieczeń IPSec</b>	
<input type="checkbox"/> Średni (AH)	Autentykacja bez szyfrowania.
<input type="checkbox"/> Wysoki (ESP)	<input type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES
Szyfrowanie i autentykacja pakietów.	

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**

VPN i Dostęp Zdalny >> Użytkownik zdalny

Indeks Nr. 1

<p><b>Konto użytkownika</b></p> <p><input checked="" type="checkbox"/> Włącz konto</p> <p>Czas nieaktywności <input type="text" value="300"/> sek</p>	<p>Użytkownik <input data-bbox="1034 1559 1219 1585" type="text" value="???"/></p> <p>Hasło <input data-bbox="1034 1599 1219 1626" type="text"/></p>
<p><b>Akceptowane protokoły</b></p> <p><input type="checkbox"/> PPTP</p> <p><input checked="" type="checkbox"/> Tunel IPSec</p> <p><input type="checkbox"/> L2TP z polisą IPSec <input type="text" value="Brak"/></p> <p><input type="checkbox"/> Określ węzeł zdalny</p> <p>Adres IP klienta zdalnego <input data-bbox="387 1854 572 1881" type="text"/></p> <p>lub ID <input data-bbox="443 1895 628 1921" type="text"/></p>	<p><b>Tryb uwierzytelniania IKE</b></p> <p><input checked="" type="checkbox"/> Klucz IKE</p> <p>Klucz IKE <input data-bbox="1034 1715 1219 1742" type="text"/></p> <p><input type="checkbox"/> Podpis cyfrowy (cert. X.509)</p> <p><input type="text" value="Brak"/></p>
	<p><b>Poziom zabezpieczeń IPSec</b></p> <p><input checked="" type="checkbox"/> Średni (AH)</p> <p>Wysoki (ESP)</p> <p><input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES</p> <p>Lokalny ID <input data-bbox="927 1966 1112 1993" type="text"/> (opcja)</p>

### 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

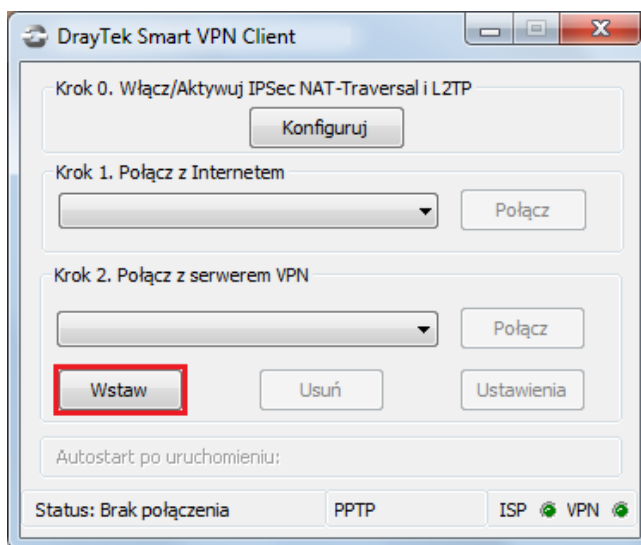
VPN i Dostęp Zdalny >> Użytkownik zdalny

Indeks Nr. 2

<p><b>Konto użytkownika</b></p> <p><input checked="" type="checkbox"/> <b>Włącz konto</b></p> <p>Czas nieaktywności <input type="text" value="300"/> sek</p>	<p>Użytkownik <input data-bbox="1034 831 1217 860" type="text" value="???"/></p> <p>Hasło <input data-bbox="1034 869 1217 898" type="password"/></p>
<p><b>Akceptowane protokoły</b></p> <p><input type="checkbox"/> PPTP</p> <p><input checked="" type="checkbox"/> <b>Tunel IPSec</b></p> <p><input type="checkbox"/> L2TP z polisą IPSec <input type="text" value="Brak"/></p>	<p><b>Tryb uwierzytelniania IKE</b></p> <p><input checked="" type="checkbox"/> <b>Klucz IKE</b></p> <p><input data-bbox="810 987 1235 1016" type="text" value="Klucz IKE"/></p> <p><input type="checkbox"/> Podpis cyfrowy (cert. X.509)</p> <p><input type="text" value="Brak"/></p>
<p><input checked="" type="checkbox"/> <b>Określ węzeł zdalny</b></p> <p>Adres IP klienta zdalnego</p> <p><input data-bbox="395 1122 579 1151" type="text" value="99.99.99.12"/></p> <p>lub ID <input data-bbox="451 1167 635 1196" type="text"/></p>	<p><b>Poziom zabezpieczeń IPSec</b></p> <p><input type="checkbox"/> Średni (AH)</p> <p>Wysoki (ESP)</p> <p><input type="checkbox"/> DES <input checked="" type="checkbox"/> <b>3DES</b> <input checked="" type="checkbox"/> AES</p> <p>Lokalny ID <input data-bbox="927 1234 1110 1263" type="text"/> (opcja)</p>

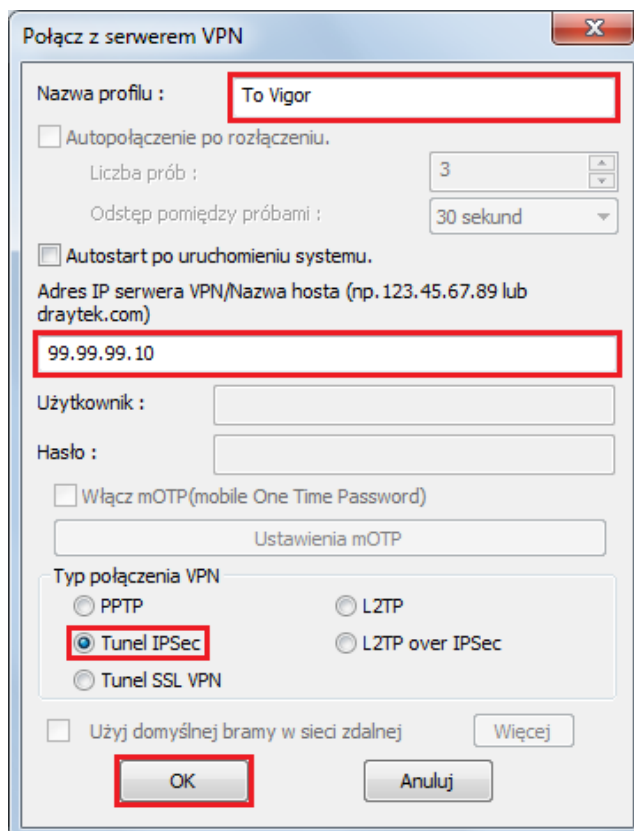
### 2. Konfiguracja klienta VPN

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

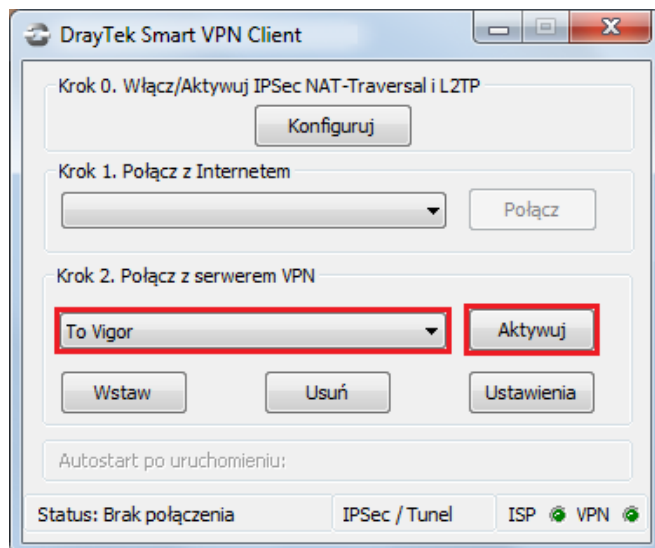


Wypełnij dane dotyczące zabezpieczeń IPSec:

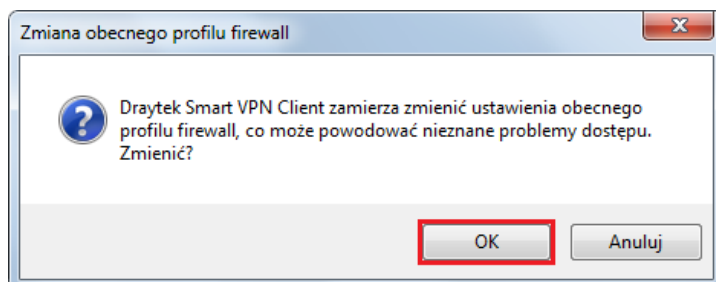
- w polu Mój adres IP wybierz odpowiedni adres IP swojego komputera. W przykładzie 99.99.99.11.
- w polu Typ połączenia IPSec wybierz Standardowy tunel IPSec oraz wpisz adresację zdalnej podsieci. W przykładzie Zdalna podsieć: 192.168.0.0, Maska podsieci zdalnej: 255.255.255.0.
- w polu Metoda zabezpieczeń 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

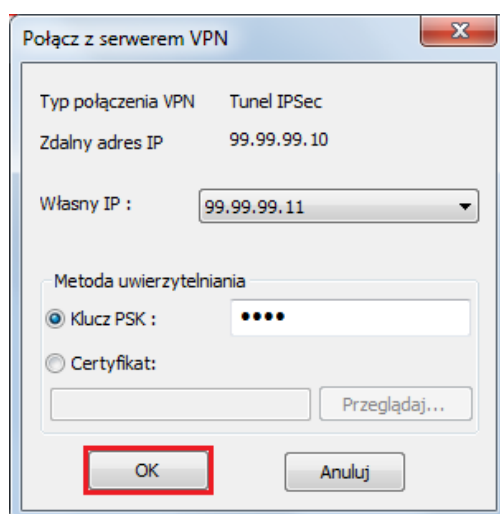
Wybierz odpowiedni profil a następnie kliknij przycisk Aktywuj.



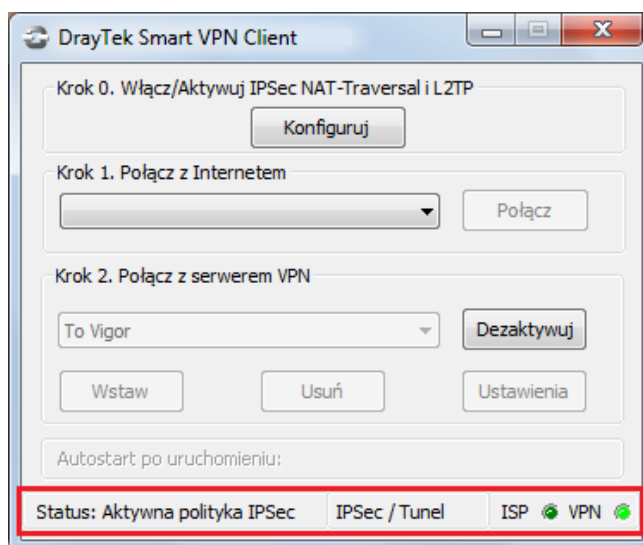
Zaakceptuj zmiany w Zaporze systemu Windows m.in. włączenie zapory, dodanie reguły zabezpieczeń połączeń.



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.

```
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 i Dostęp Zdalny >> Zarządzanie połączeniem** (rysunek poniżej).

### VPN i Dostęp Zdalny >> Zarządzanie połączeniem

#### Wymuszanie inicjacji połączeń

Czas odświeżania : 30

Tryb Główny:	<input type="text"/>	<input type="button" value="Inicjuj"/>
Tryb Backup:	<input type="text"/>	<input type="button" value="Inicjuj"/>

#### Stan połączenia VPN

Bieżąca strona: 1

Nr strony

VPN	Typ	Zdalny IP	Sieć wirtualna	Tx pakietów	Tx prędkość	Rx pakietów	Rx predkość	Czas akt.	
1	IPSec Tunnel ( Dynamic Client ) 3DES-SHA1 Auth	99.99.99.11	99.99.99.11/32	344	55	265	9	0:1:7	<input type="button" value="Rozłącz"/>

xxxxxxx : Dane są szyfrowane.  
xxxxxxx : nie są szyfrowane.