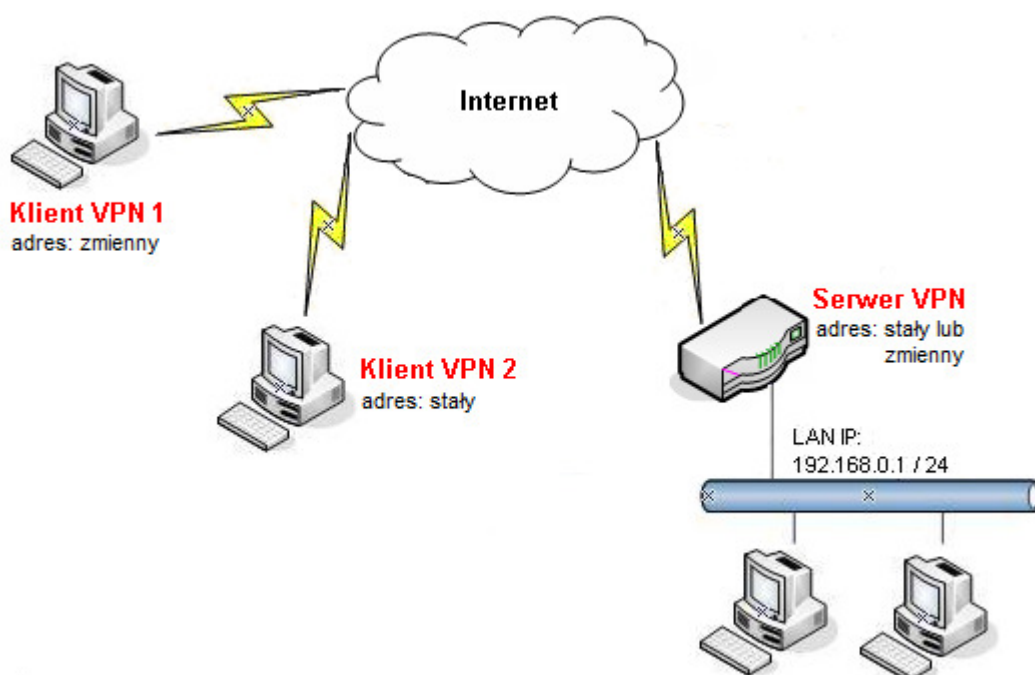


1. Konfiguracja serwera VPN
  - 1.1. Profil dla klienta ze zmiennym IP
  - 1.2. Profil dla klienta ze stałym IP
2. Konfiguracja klienta VPN
3. Status połączenia
  - 3.1. Klient VPN
  - 3.2. Serwer VPN
4. Brama domyślna

Procedura konfiguracji została oparta na poniższym przykładzie.



Główne założenia:

- typ tunelu: Host-LAN
- protokół VPN: L2TP over IPSec
- szyfrowanie: AES
- integralność: SHA1
- autentykacja: L2TP (nazwa użytkownika i hasło), IPSec (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)

#### **Uwaga**

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 i L2TP.

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 **AES** 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.

Uwierzytelnianie IKE

Klucz IKE:

Potwierdź klucz IKE:

Tryb zabezpieczeń IPSec

Średni (AH)  
Autentykacja bez szyfrowania.

Wysoki (ESP)  DES  3DES  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**. Wpisz **0** w polu czas nieaktywności jeśli Vigor ma pozostawić połączenie pomimo braku ruchu. L2TP posiada wbudowane mechanizmy detekcji połączenia.
- jako akceptowany protokół zaznacz **L2TP z polisą IPSec**. Dla polisy IPSec Wybierz **Opcja** lub **Wymóg**.
- wpisz Użytkownika i Hasło dla L2TP. W przykładzie użyto użytkownika 'test1' i hasło 'test1'.
- kliknij przycisk OK, zatwierdzić ustawienia

VPN i Dostęp Zdalny >> Użytkownik zdalny

Indeks Nr. 1

Konto użytkownika

Włącz konto

Czas nieaktywności:  sek

Użytkownik:

Hasło:

Akceptowane protokoły

PPTP

Tunel IPSec

L2TP z polisą IPSec

Tryb uwierzytelniania IKE

Klucz IKE

Klucz IKE:

Podpis cyfrowy (cert. X.509)

### 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**. Wpisz **0** w polu czas nieaktywności jeśli Vigor ma pozostawić połączenie pomimo braku ruchu. L2TP posiada wbudowane mechanizmy detekcji połączenia.
- jako akceptowany protokół zaznacz **L2TP z polisą IPSec**. Dla polisy IPSec Wybierz **Opcja** lub **Wymóg**.
- zaznacz **Określ węzeł zdalny** i wprowadź odpowiedni adres. W przykładzie użyto 99.99.99.12
- wpisz Użytkownika i Hasło. W przykładzie użyto użytkownika 'test2' i hasło 'test2'.
- 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 AES.
- kliknij przycisk OK, zatwierdzić ustawienia

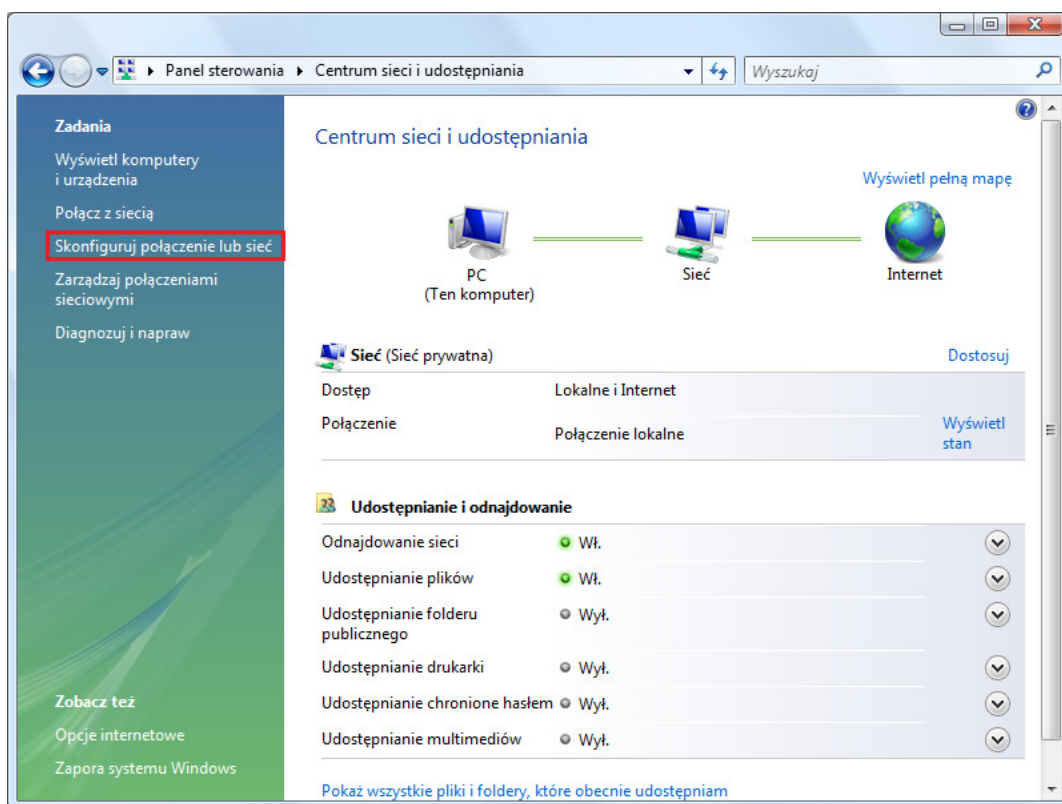
VPN i Dostęp Zdalny >> Użytkownik zdalny

Indeks Nr. 2

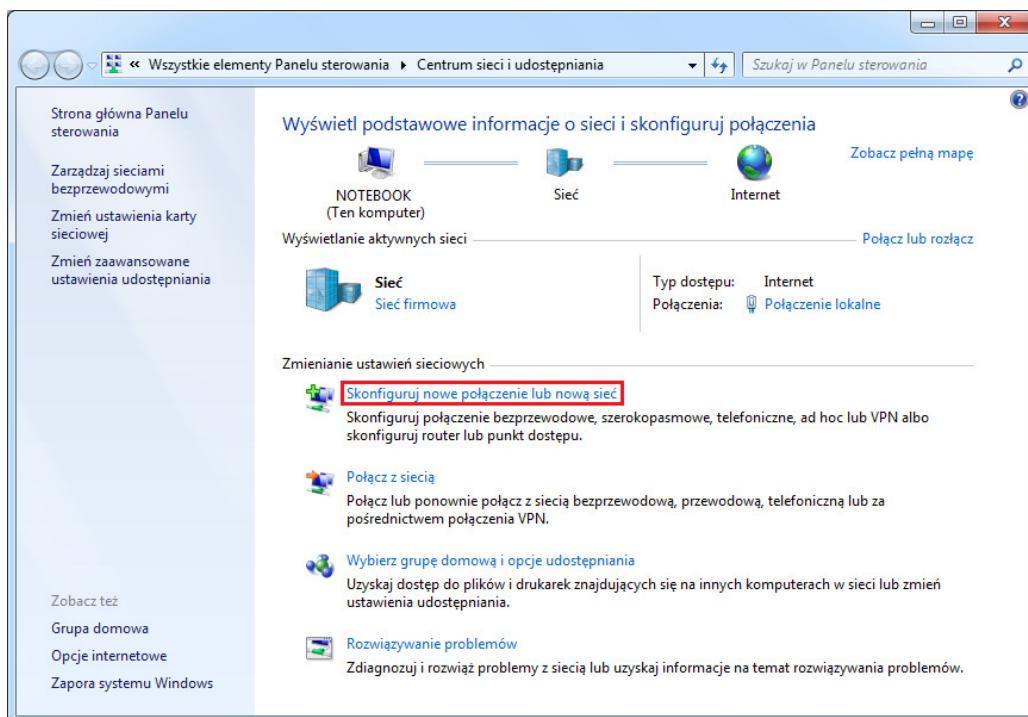
<p><b>Konto użytkownika</b></p> <p><input checked="" type="checkbox"/> Włącz konto</p> <p>Czas nieaktywności <input type="text" value="0"/> sek</p>	<p>Użytkownik <input type="text" value="test2"/></p> <p>Hasło <input type="password" value="•••••"/></p>
<p><b>Akceptowane protokoły</b></p> <p><input type="checkbox"/> PPTP</p> <p><input type="checkbox"/> Tunel IPSec</p> <p><input checked="" type="checkbox"/> L2TP z polisą IPSec <input type="text" value="Opcja"/></p>	<p><b>Tryb uwierzytelniania IKE</b></p> <p><input checked="" type="checkbox"/> Klucz IKE</p> <p><input type="text" value="Klucz IKE"/> <input type="password" value="••••"/></p> <p><input type="checkbox"/> Podpis cyfrowy (cert. X.509)</p> <p><input type="text" value="Brak"/></p>
<p><input checked="" type="checkbox"/> Określ węzeł zdalny</p> <p>Adres IP/nr ISDN klienta zdalnego</p> <p><input type="text" value="99.99.99.12"/></p> <p>lub ID <input 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"/> 3DES <input checked="" type="checkbox"/> AES</p> <p>Lokalny ID <input type="text"/> (opcja)</p>

### 2. Konfiguracja klienta VPN

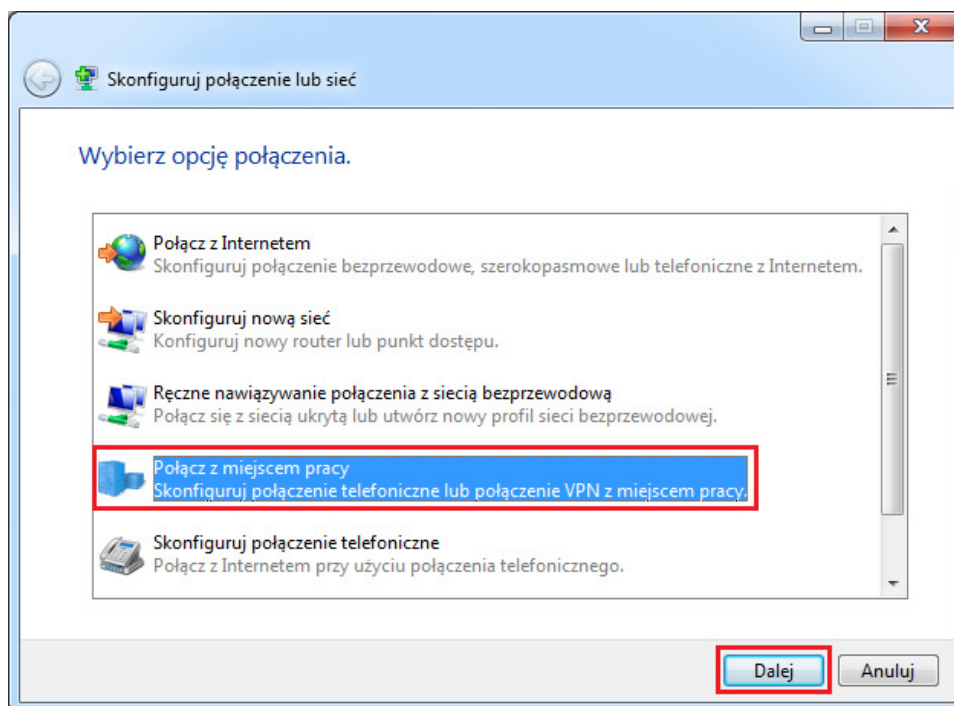
**Windows Vista** - W Centrum sieci i udostępniania wybierz **Skonfiguruj połączenie lub sieć**.



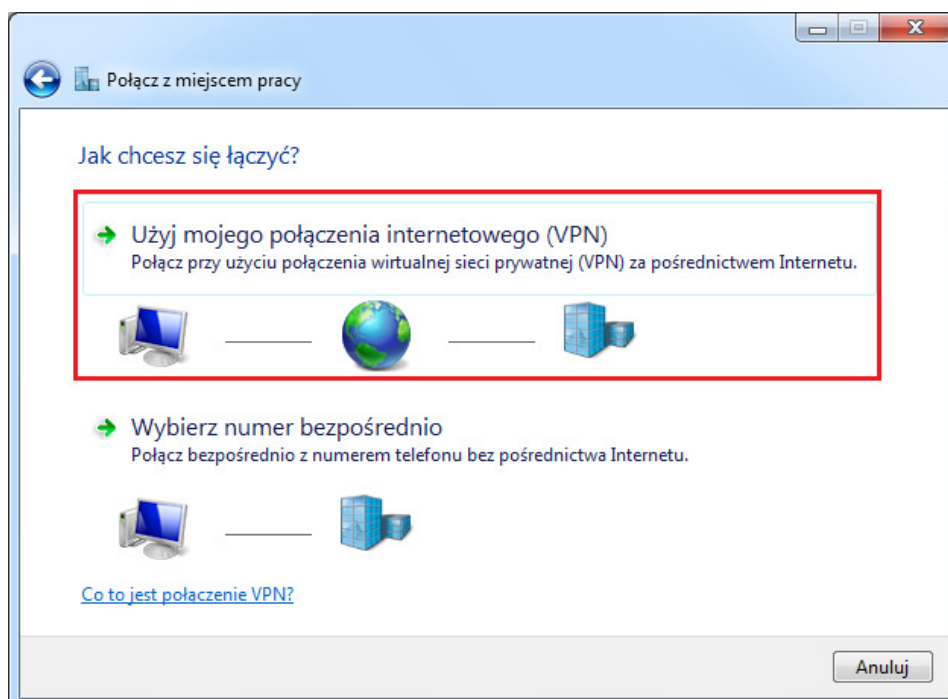
**Windows 7** - W Centrum sieci i udostępniania wybierz **Skonfiguruj nowe połączenie lub nową sieć**.



Wybierz Połącz z miejscem pracy. Następnie kliknij przycisk Dalej.



Jako sposób łączenia wybierz opcję Użyj mojego połączenia internetowego (VPN)



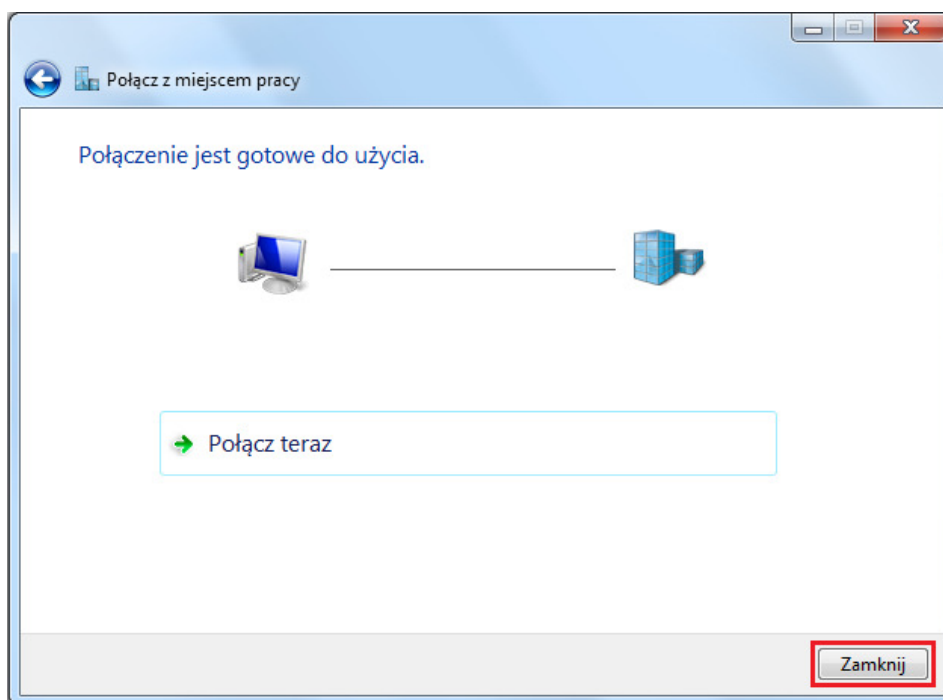
W polu Adres internetowy wpisz IP routera (w przykładzie 99.99.99.10), do którego zestawiasz tunel VPN, albo jego nazwę (w przykładzie serwer.abc.xyz).

Zaznacz opcję **Nie łącz teraz; tylko skonfiguruj, aby można było połączyć się później**.

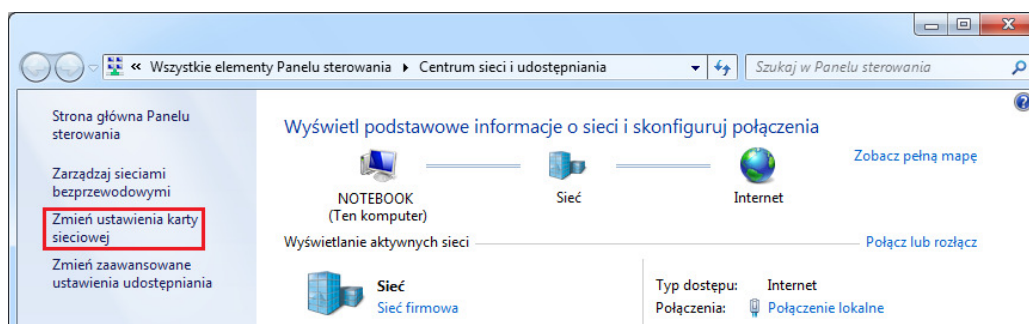
Następnie kliknij przycisk Dalej.

Wpisz Nazwę użytkownika i Hasło takie same jak w ustawieniach profilu na routerze Vigor. W przykładzie użyto użytkownika 'test1' i hasła 'test1'. Kliknij przycisk Utwórz.

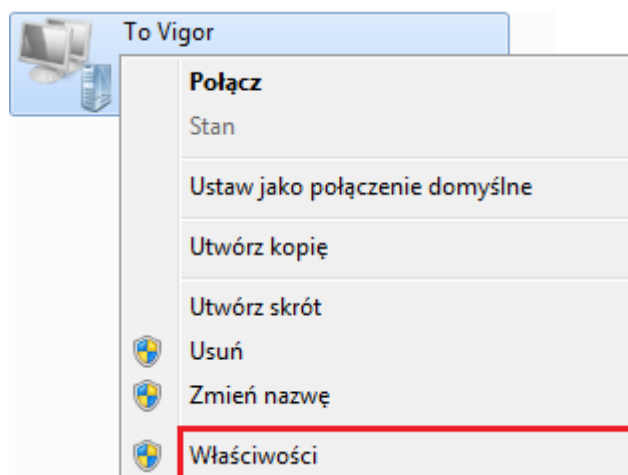
Kliknij przycisk Zamknij.



W Centrum sieci i udostępniania wybierz **Zmień ustawienia karty sieciowej**.

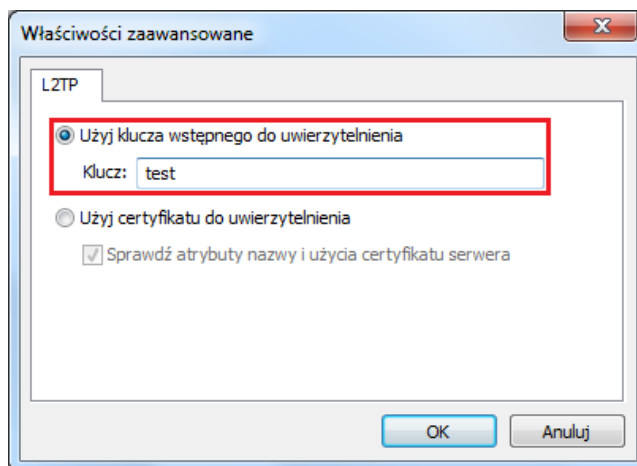
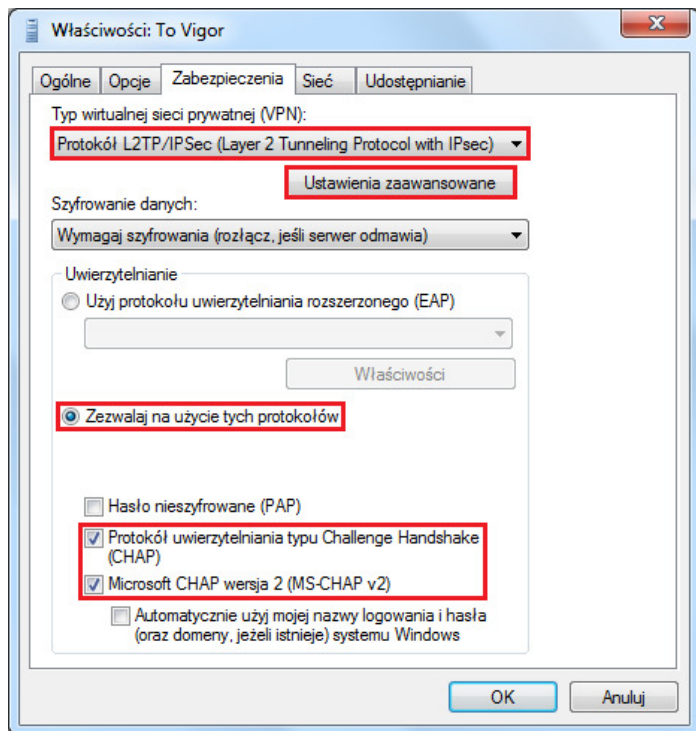


Przejdź do **Właściwości** utworzonego połączenie 'To Vigor'



W zakładce Zabezpieczenia

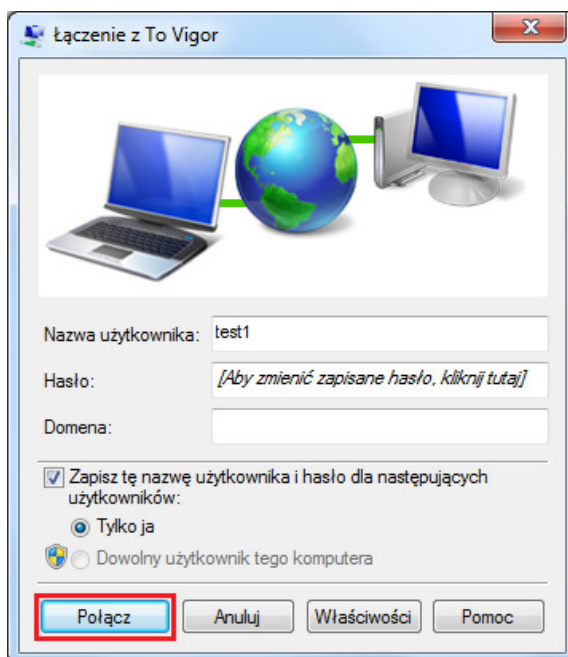
- wybierz **Protokół L2TP/IPSec**
- w Ustawieniach zaawansowanych wybierz **Użyj klucza wstępnego do uwierzytelniania** a następnie wpisz klucz. W przykładzie użyto 'test'
- zezwalaj na użycie protokołu **CHAP, MS-CHAP v2**



Kliknij dwukrotnie na połączeniu.



Kliknij przycisk **Połącz**.





### 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.

```
C:\>ipconfig

Konfiguracja IP systemu Windows

Karta PPP To Uigor:

Sufiks DNS konkretnego połączenia :
Adres IP. . . . . : 192.168.0.10
Maska podsieci. . . . . : 255.255.255.255
Brama domyślna. . . . . : 0.0.0.0
```

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.

```
C:\>ping 192.168.0.1

Badanie 192.168.0.1 z użyciem 32 bajtów danych:

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
Odpowiedź z 192.168.0.1: bajtów=32 czas=1ms TTL=255

Statystyka badania ping dla 192.168.0.1:
    Pakiety: Wysłane = 4, Odebrane = 4, Utracone = 0 (0% strat),
Szacunkowy czas błędzenia pakietów w milisekundach:
    Minimum = 1 ms, Maksimum = 1 ms, Czas średni = 1 ms
```

#### 3.2. Serwer VPN

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

VPN i Dostęp Zdalny>> Zarządzanie połączeniem

---

Wymuszanie inicjacji połączeń Czas odświeżania : 10

Tryb Główny:

Tryb Backup:

---

Stan połączenia VPN

Bieżąca strona: 1 Nr strony

VPN	Typ	Zdalny IP	Sieć wirtualna	Tx pakietów	Tx prędkość	Rx pakietów	Rx prędkość	Czas akt.
1 (test1)	L2TP AES-SHA1 Auth	99.99.99.11	192.168.0.10/32	39	1770	88	363	0:6:9

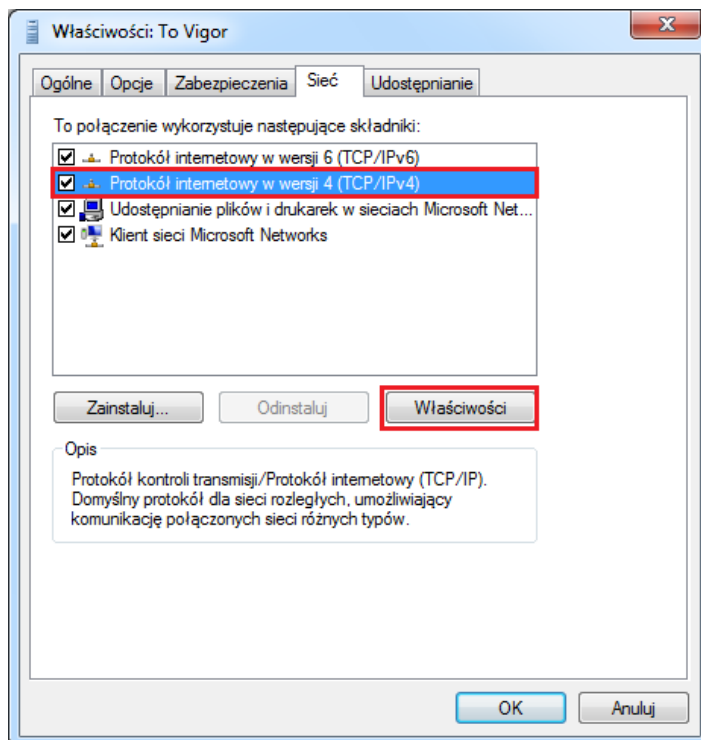
xxxxxxx : Dane są szyfrowane.  
xxxxxxx : nie są szyfrowane.

### 4. Brama domyślna

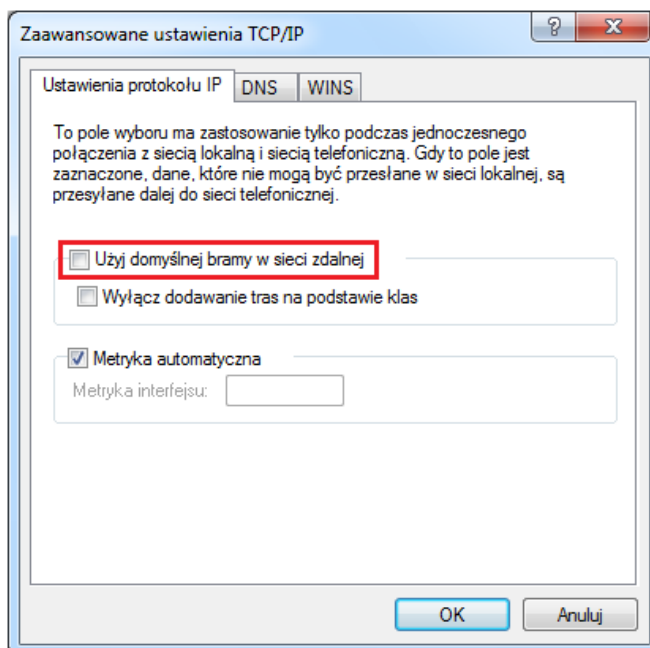
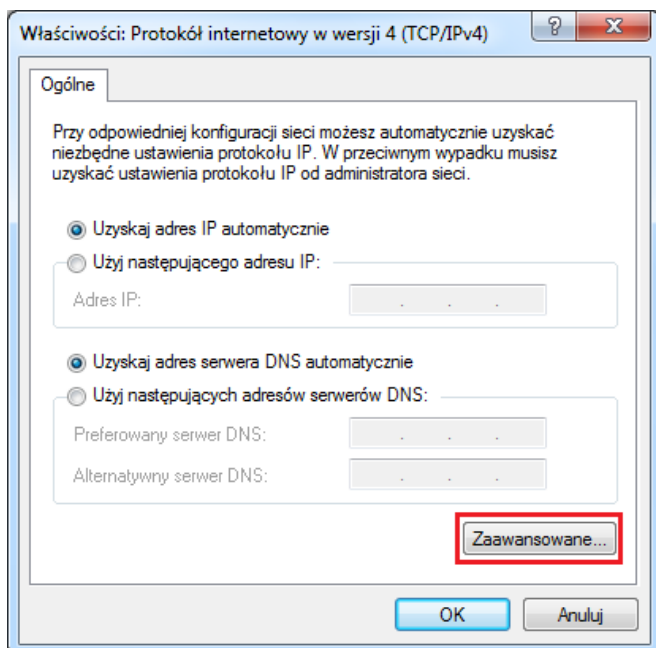
Domyślnie Windows Vista/7 kieruje cały ruch przez połączenie VPN.

Przejdź do właściwości utworzonego połączenia.

W zakładce Sieć przejdź do właściwości Protokołu internetowego(TCP/IPv4).



Następnie przejdź do ustawień zaawansowanych. Odznacz opcję **Użyj domyślnej bramy w sieci zdalnej**.



Krzysztof Skowina  
 Specjalista ds. rozwiązań sieciowych  
[k.skowina@brinet.pl](mailto:k.skowina@brinet.pl)