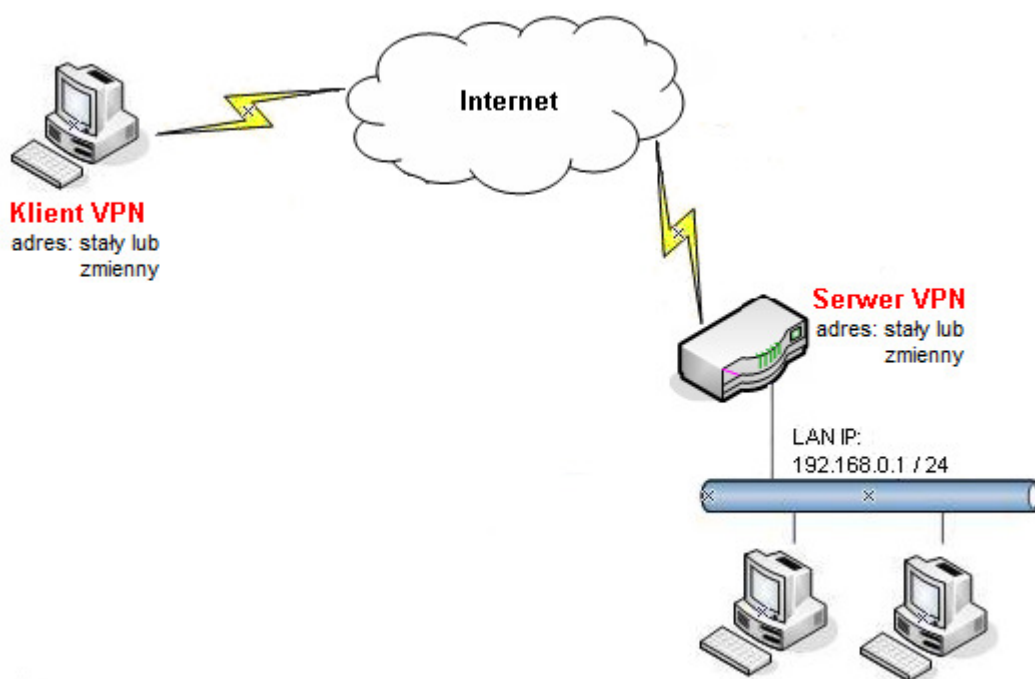


1. Konfiguracja serwera VPN
2. Konfiguracja klienta VPN
3. Status połączenia
 - 3.1. Klient VPN
 - 3.2. Serwer VPN
4. Problemy
5. Brama domyślna

Procedura konfiguracji została oparta na poniższym przykładzie.



Główne założenia:

- typ tunelu: Host-LAN
- protokół VPN: PPTP
- wymagane szyfrowanie
- Adres Serwera VPN: stały (IP - 99.99.99.10) lub zmienny (domenowy - serwer.abc.xyz)
- Adres Klienta VPN: stały lub zmienny

Uwagi

- Połączenie PPTP z szyfrowaniem MPPE wymaga uwierzytelniania MS-CHAP lub MS-CHAP v2.
- 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 PPTP.

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

Następnie przejdź do zakładki **VPN i Dostęp Zdalny>>Ustawienia Ogólne PPP**. Zmień Opcje szyfrowanie PPP(MPPE). W przykładzie użyto Wymagaj MPPE(40/128 bit).

VPN i Dostęp Zdalny>> Ustawienia ogólne PPP

Ustawienia ogólne PPP

<p>Parametry PPP dla VPN</p> <p>Uwierzytelnianie PPP <input type="text" value="PAP lub CHAP"/></p> <p>Opcje szyfrowania PPP(MPPE) <input type="text" value="Wymagaj MPPE(40/128 bit)"/></p> <p>Uwierzytelnianie zwrotne (PAP) <input type="radio"/> Tak <input checked="" type="radio"/> Nie</p> <p>Użytkownik <input type="text"/></p> <p>Hasło <input type="text"/></p>	<p>Adresy przydzielane klientom zdalnym (Używane, gdy wyłączony DHCP)</p> <p>Adres początkowy <input type="text" value="192.168.0.200"/></p>
--	---

W kolejnym kroku przejdź do zakładki **VPN i Dostęp Zdalny>>Połączenia Host-LAN**. Stwórz odpowiednie konto do obsługi tunelu.

Kliknij np. indeks 1 i wpisz odpowiednie dane. 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. Wpisz **0** w polu czas nieaktywności jeśli Vigor ma pozostawić połączenie pomimo braku ruchu. PPTP posiada wbudowane mechanizmy detekcji połączenia.
- jako akceptowany protokół zaznacz **PPTP**
- wpisz Użytkownika i Hasło. W przykładzie użyto użytkownika 'test' i hasło 'test'.

VPN i Dostęp Zdalny>> Użytkownik zdalny

Indeks Nr. 1

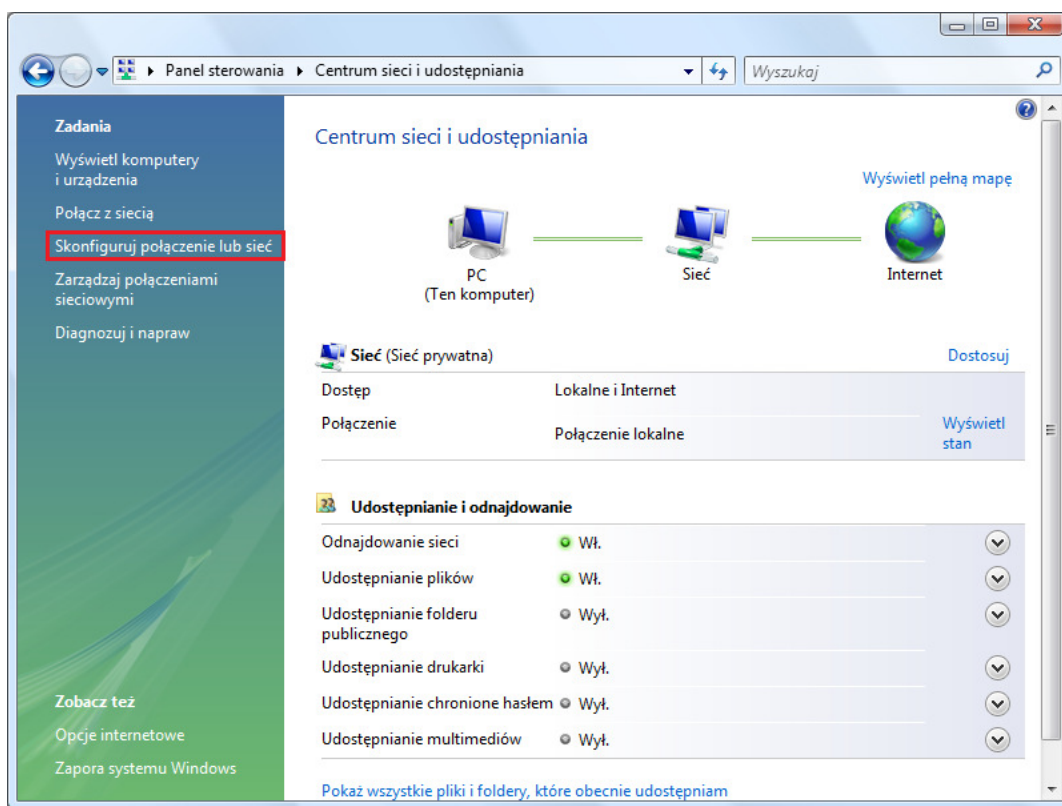
<p>Konto użytkownika</p> <p><input checked="" type="checkbox"/> Włącz konto</p> <p>Czas nieaktywności <input type="text" value="0"/> sek</p>	<p>Użytkownik <input type="text" value="test"/></p> <p>Hasło <input type="text" value="••••"/></p>
<p>Akceptowane protokoły</p> <p><input checked="" type="checkbox"/> PPTP</p> <p><input 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 type="text"/></p>	<p>Tryb uwierzytelniania IKE</p> <p><input checked="" type="checkbox"/> Klucz IKE</p> <p>Klucz IKE <input type="text"/></p> <p><input type="checkbox"/> Podpis cyfrowy (cert. X.509)</p> <p><input type="text" value="Brak"/></p>

- jeżeli chcesz dodatkowo weryfikować adres IP inicjującego połączenie zaznacz opcję **Określ węzeł zdalny**, a w polu **Adres IP klienta zdalnego** wpisz odpowiedni adres IP klienta VPN.

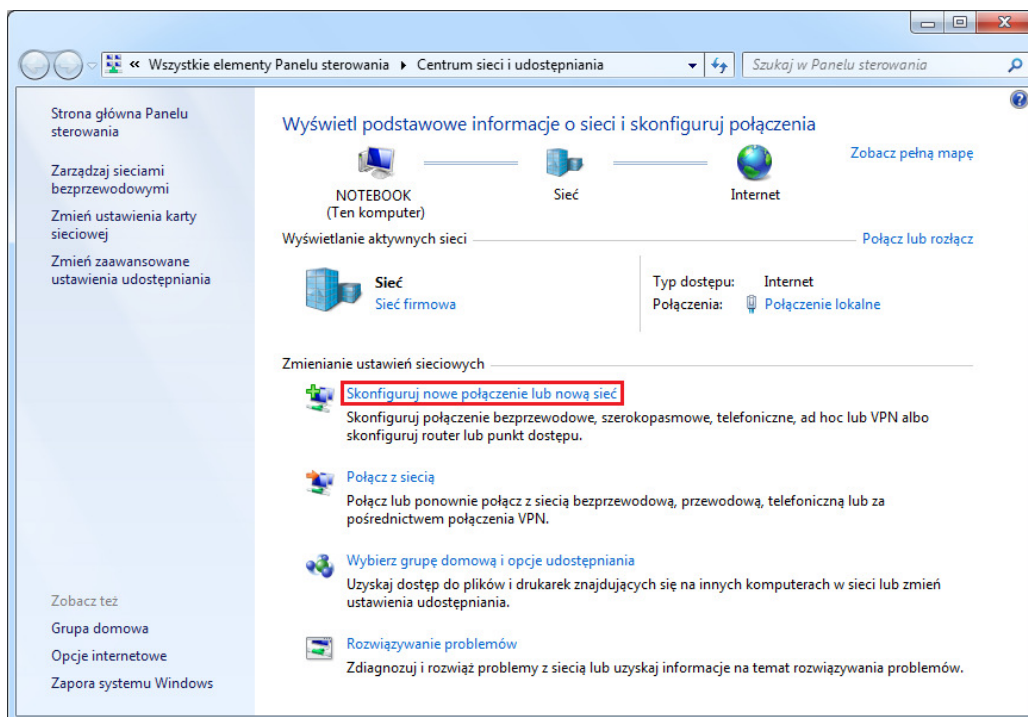
<input checked="" type="checkbox"/>	Określ węzeł zdalny
	Adres IP klienta zdalnego
	<input type="text" value="99.99.99.11"/>

2. Konfiguracja klienta VPN

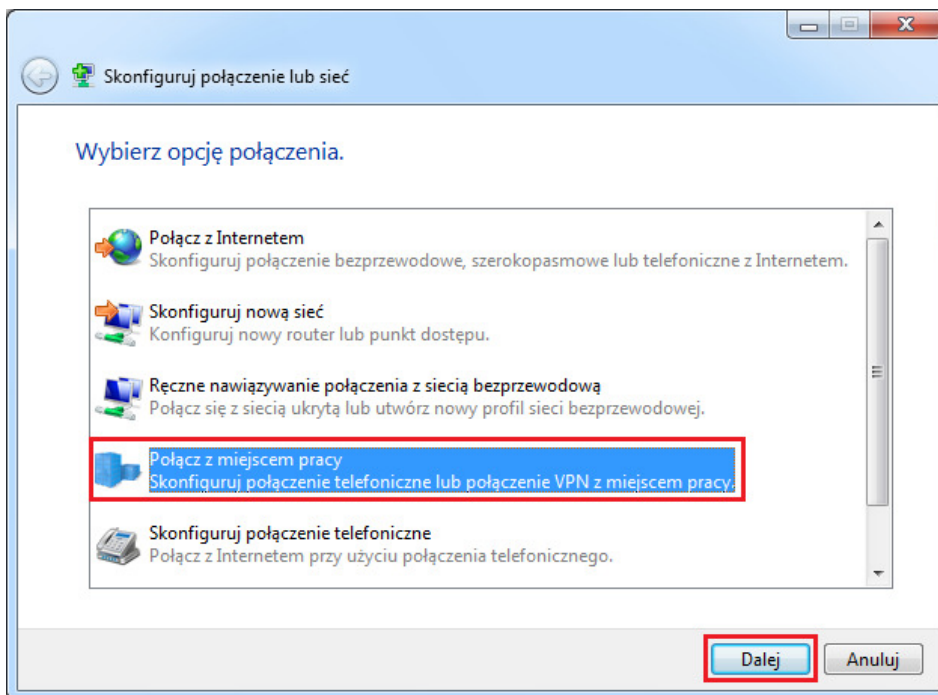
Windows Vista - W Centrum sieci i udostępniania wybierz **Skonfiguruj połączenie lub sieć**.



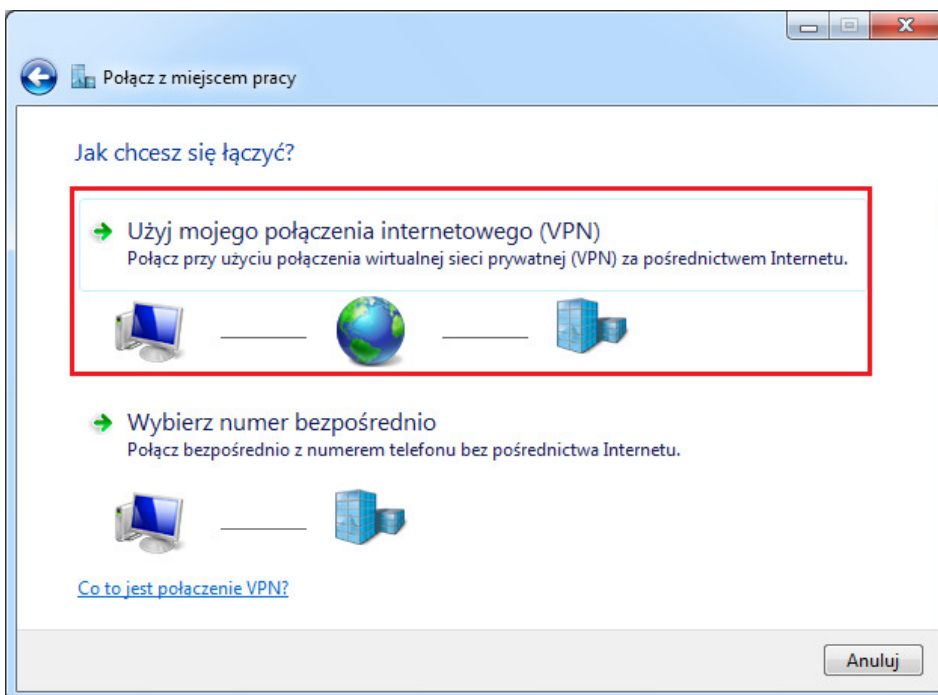
Windows 7 - W Centrum sieci i udostępniania wybierz **Skonfiguruj nowe połączenie lub nową sieć**.



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). Następnie kliknij przycisk Dalej.

Połącz z miejscem pracy

Wpisz adres internetowy, z którym chcesz się połączyć

Ten adres można uzyskać od administratora sieci.

Adres internetowy: 99.99.99.10

Nazwa miejsca docelowego: To Vigor

Użyj karty inteligentnej

Zezwalaj innym osobom na korzystanie z tego połączenia
Ta opcja zezwala dowolnej osobie z dostępem do tego komputera na używanie tego połączenia.

Nigdy łącz teraz; tylko skonfiguruj, aby można było połączyć się później

Dalej Anuluj

Wpisz Nazwę użytkownika i Hasło takie same jak w ustawieniach profilu na routerze Vigor. W przykładzie użyto użytkownika 'test' i hasła 'test'. Kliknij przycisk Połącz, aby rozpocząć proces łączenia.

Połącz z miejscem pracy

Wpisz nazwę użytkownika i hasło

Nazwa użytkownika: test

Hasło: ••••

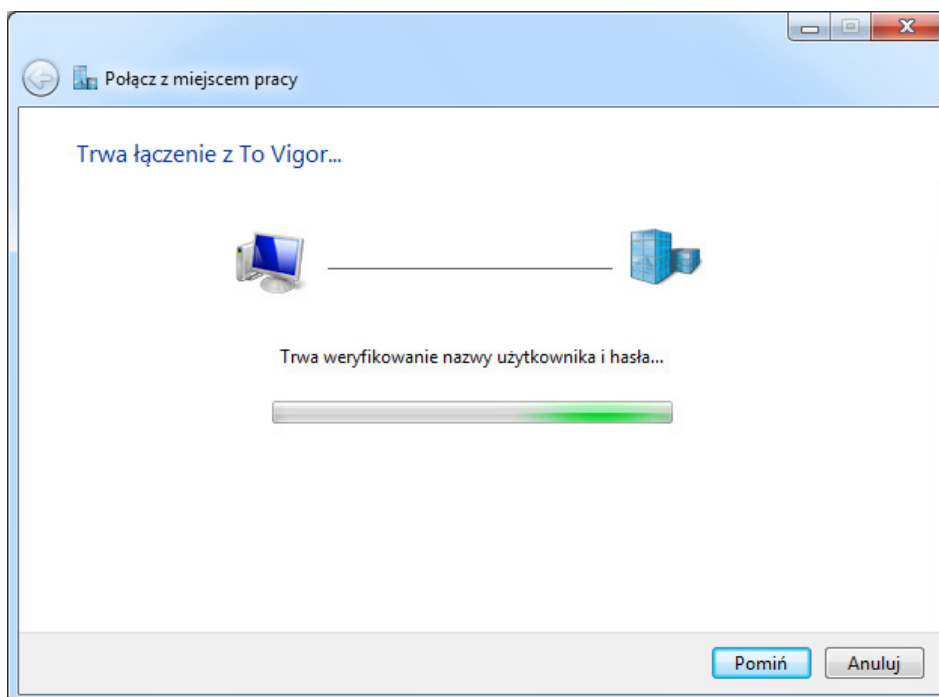
Pokaż znaki

Zapamiętaj to hasło

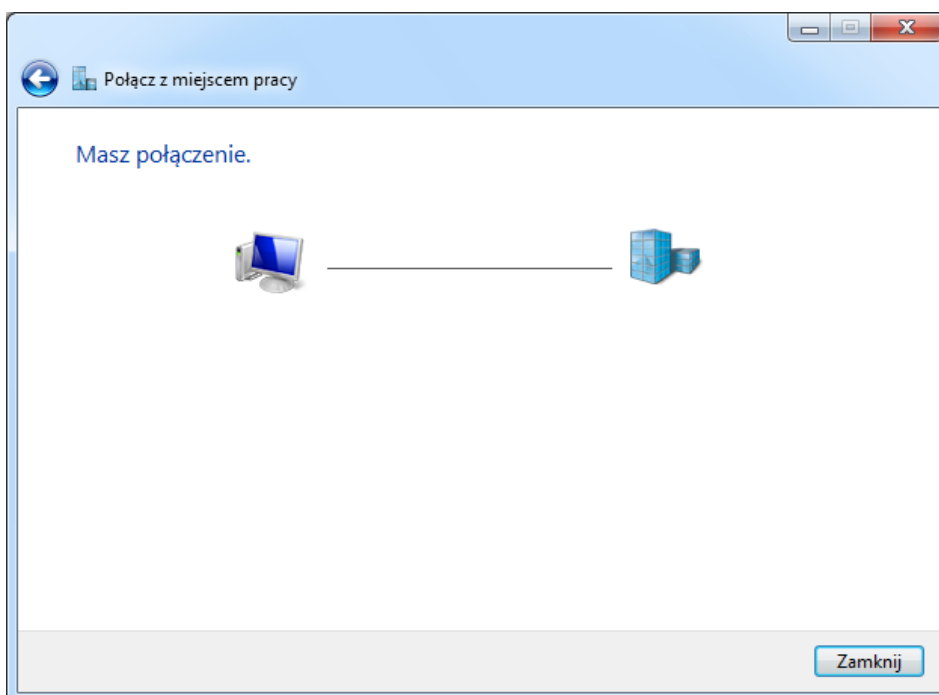
Domena (opcjonalne):

Połącz Anuluj

Jednym z etapów łączenia jest weryfikowanie nazwy użytkownika i hasła.



Przy poprawnym połączeniu pojawi się informacja *Masz połączenie.*



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 (test)	PPTP/MPPE	99.99.99.11	192.168.0.10/32	39	1770	88	363	0:6:9

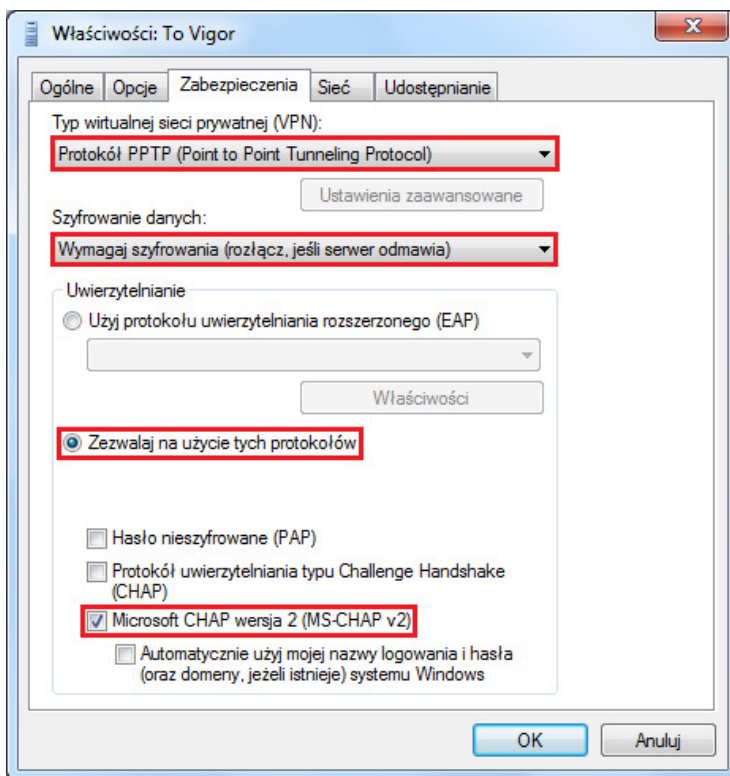
xxxxxxx : Dane są szyfrowane.
xxxxxxx : nie są szyfrowane.

4. Problemy

Przejdź do właściwości utworzonego połączenia.

W zakładce Zabezpieczenia:

- wybierz **Protokół PPTP**
- wybierz **Wymagaj szyfrowania**
- zezwalaj na użycie protokołu **MS-CHAP v2**

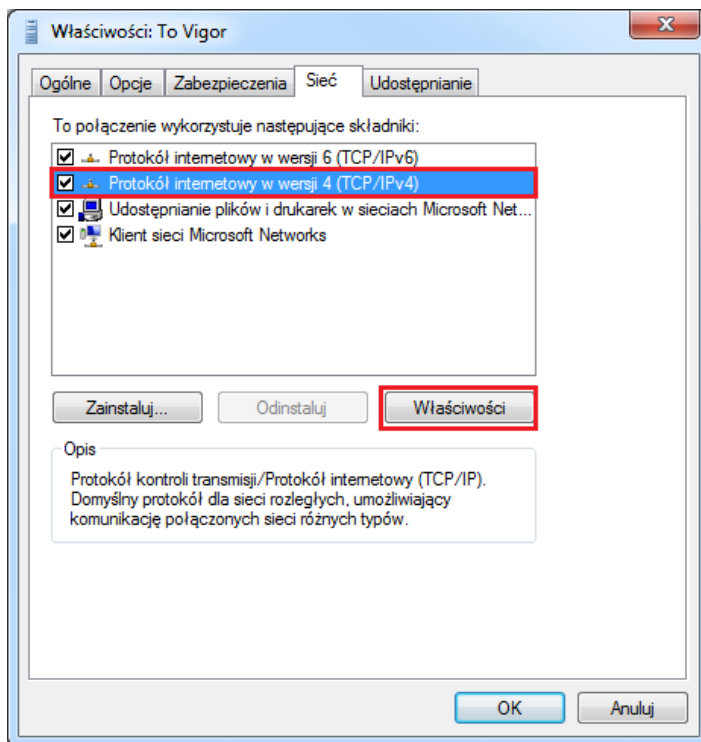


5. Brama domyślna

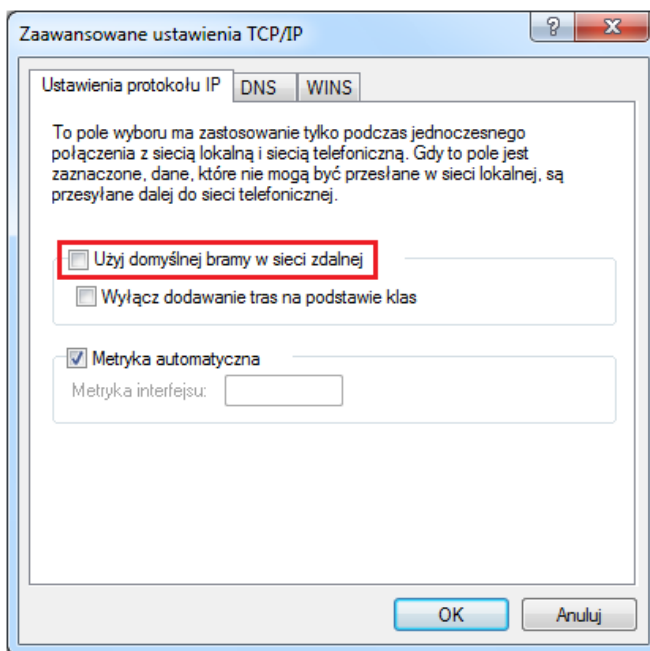
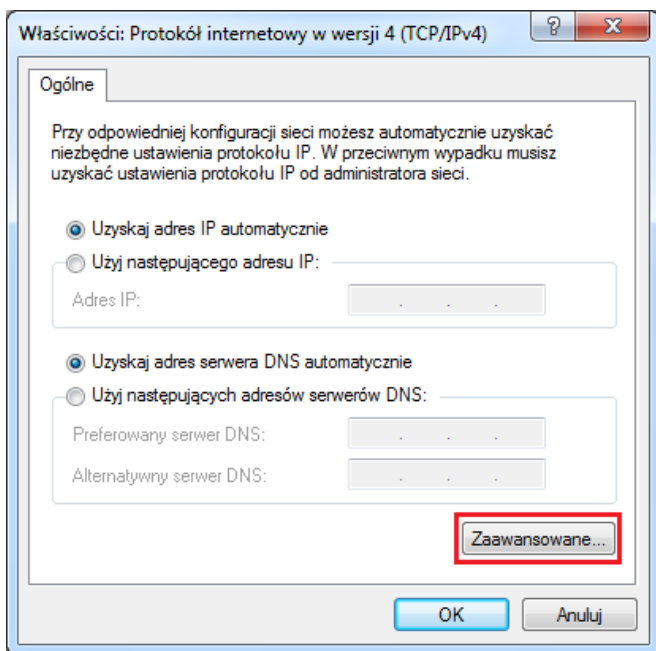
Domyślnie Windows Vista/7 kieruje cały ruch przez połączenie VPN.

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