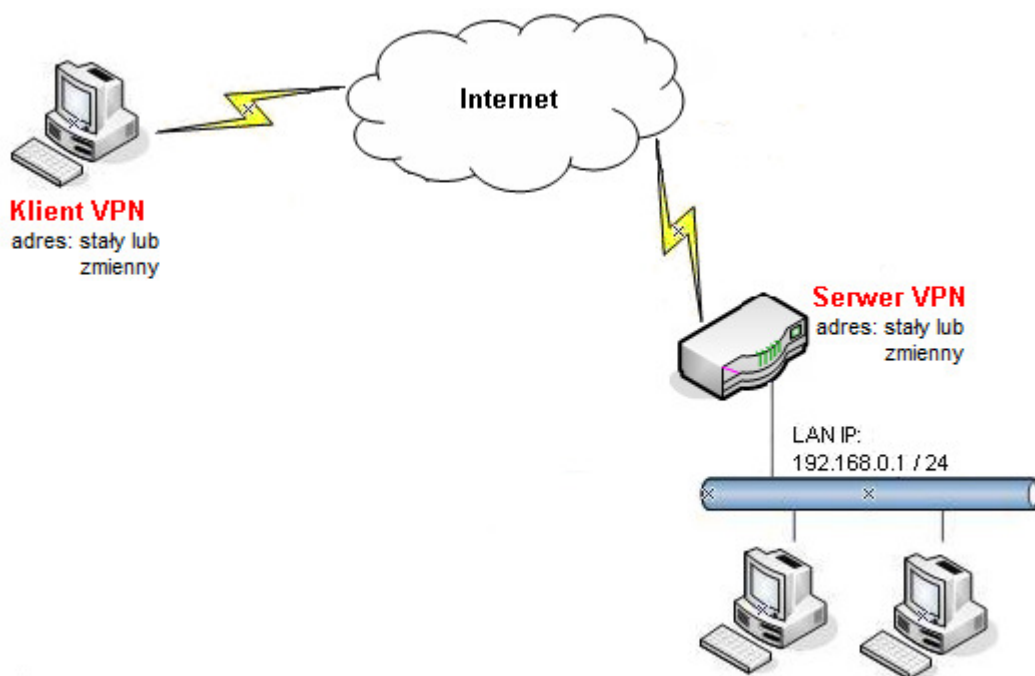


1. Konfiguracja serwera VPN
2. Konfiguracja klienta VPN
3. Status połączenia
 - 3.1. Klient VPN
 - 3.2. Serwer VPN
4. Problemy
5. Brama domyślna

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

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

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

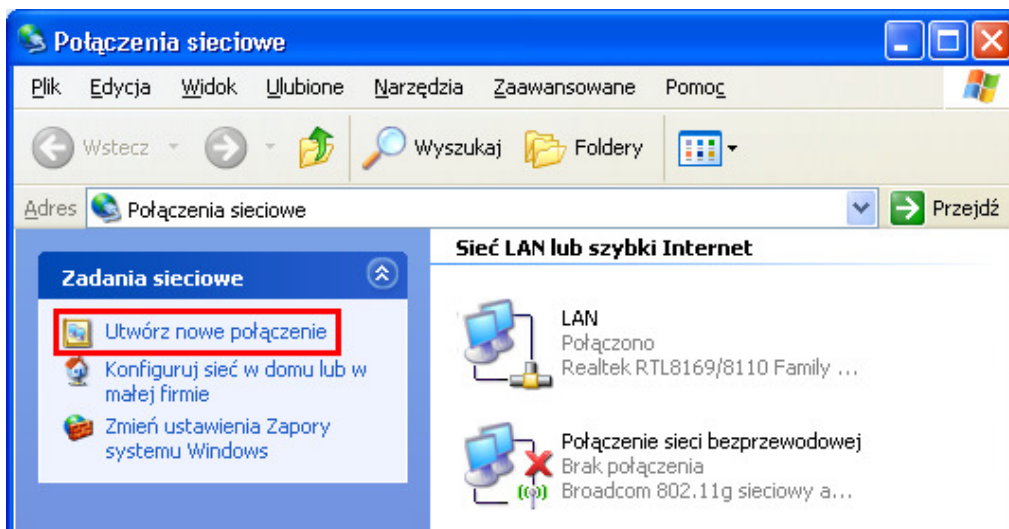
Konto użytkownika <input checked="" type="checkbox"/> Włącz konto Czas nieaktywności <input type="text" value="0"/> sek		Użytkownik <input type="text" value="test"/> Hasło <input type="text" value="****"/>	
Akceptowane protokoły <input checked="" type="checkbox"/> PPTP <input type="checkbox"/> Tunel IPSec <input type="checkbox"/> L2TP z polisą IPSec <input type="text" value="Brak"/>		Tryb uwierzytelniania IKE <input checked="" type="checkbox"/> Klucz IKE Klucz IKE <input type="text"/> <input type="checkbox"/> Podpis cyfrowy (cert. X.509) <input type="text" value="Brak"/>	
<input type="checkbox"/> Określ węzeł zdalny Adres IP klienta zdalnego <input type="text"/>			

- 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.

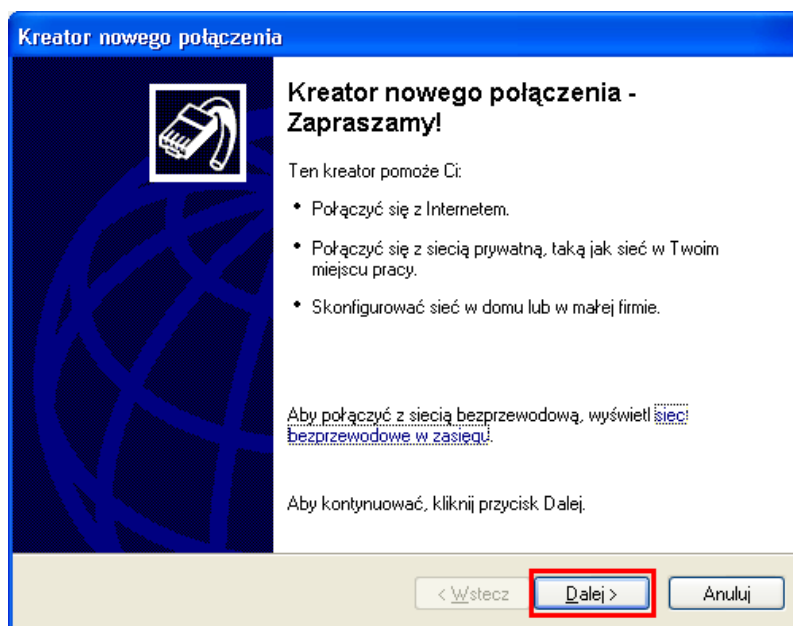
<input checked="" type="checkbox"/>	Określ węzeł zdalny
	Adres IP klienta zdalnego
	<input type="text" value="99.99.99.11"/>

2. Konfiguracja klienta VPN

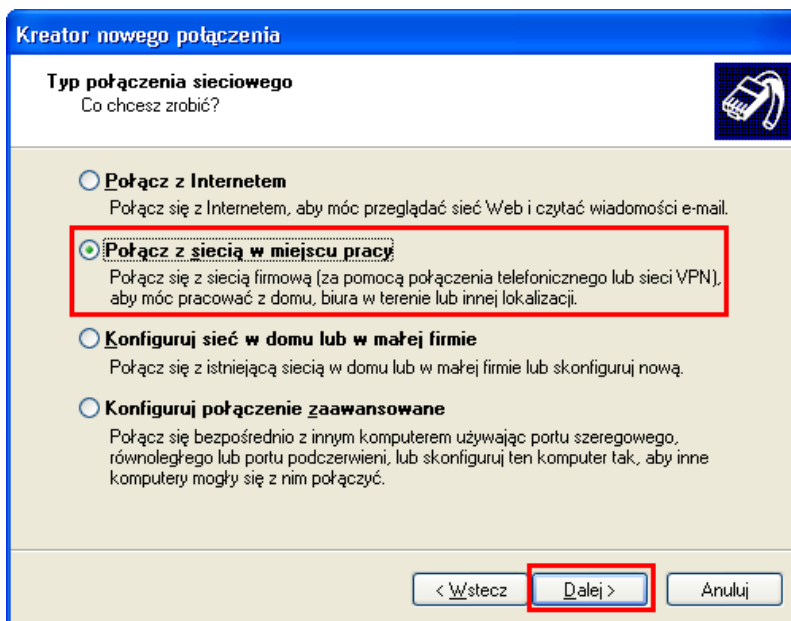
W Windows XP przejdź do ustawień Połączenia sieciowe w Panelu sterowania. Następnie wybierz opcję **Utwórz nowe połączenie**.



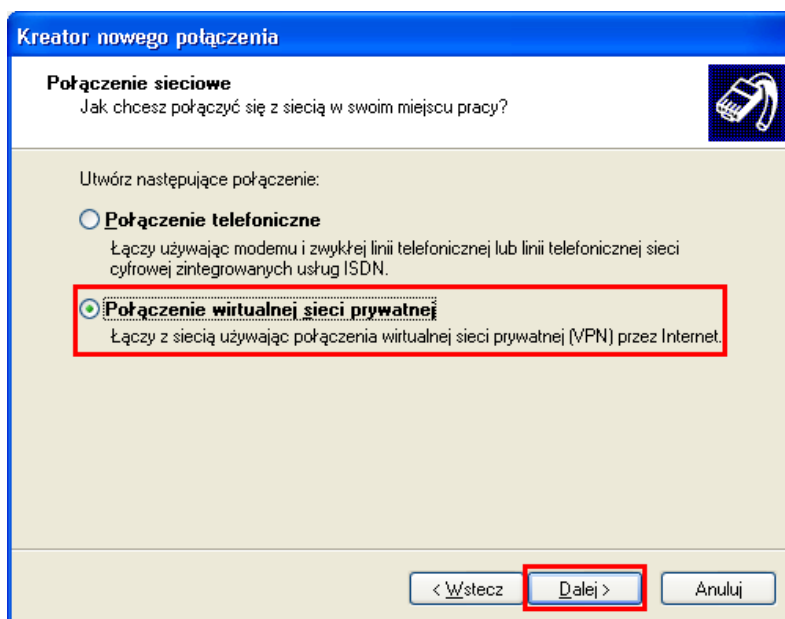
Pojawi się Kreator nowego połączenia. Kliknij przycisk **Dalej>**.



Wybierz **Połącz z siecią w miejscu pracy**. Następnie kliknij przycisk **Dalej>**.



Wybierz **Połączenie wirtualnej sieci prywatnej**. Następnie kliknij przycisk **Dalej>**.



Wpisz dowolną nazwę połączenia. Następnie kliknij przycisk **Dalej>**.

Kreator nowego połączenia

Nazwa połączenia
Podaj nazwę tego połączenia do swojego miejsca pracy.

W poniższym polu wpisz nazwę tego połączenia.

Nazwa firmy
To Vigor

Na przykład możesz wpisać nazwę swojego miejsca pracy lub nazwę serwera, z którym się łączysz.

< Wstecz **Dalej >** Anuluj

Wpisz Nazwę hosta (w przykładzie serwer.abc.xyz) lub adres IP (w przykładzie 99.99.99.10) serwera VPN. Następnie kliknij przycisk **Dalej>**.

Kreator nowego połączenia

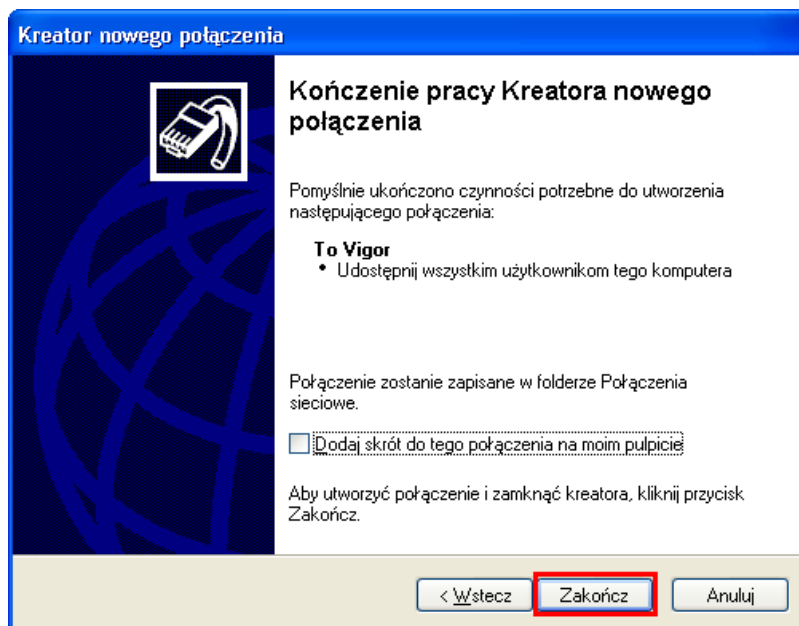
Wybór serwera sieci VPN
Jaka jest nazwa lub adres serwera sieci VPN?

Podaj nazwę hosta lub adres protokołu internetowego (IP) komputera, z którym się łączysz.

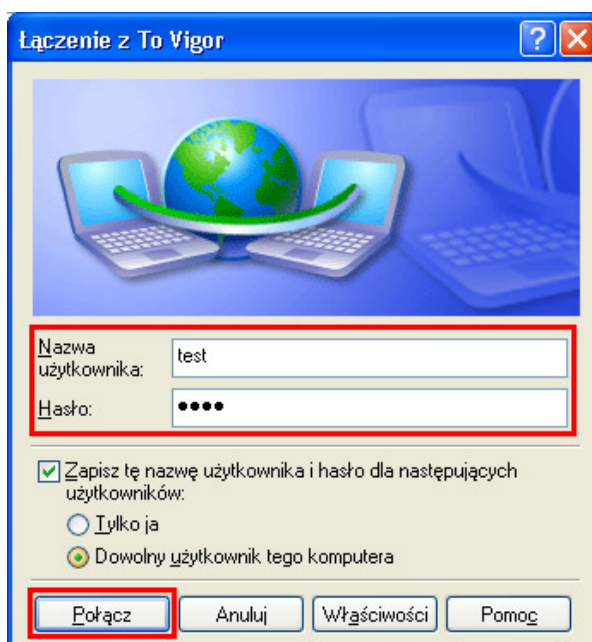
Nazwa hosta lub adres IP (np. microsoft.com lub 157.54.0.1):
99.99.99.10

< Wstecz **Dalej >** Anuluj

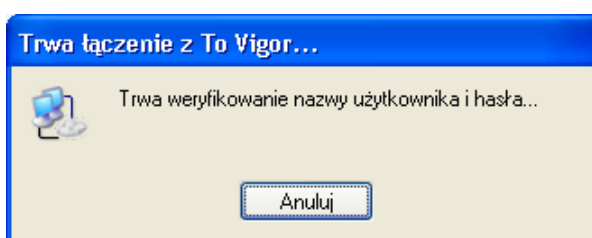
Kliknij przycisk **Zakończ**, aby zakończyć pracę kreatora.



Pojawi się okienko do **Łączenia z ...** (w przykładzie **To Vigor**). Wypełnij pola **Nazwa użytkownika** i **Hasło**. W przykładzie użyto nazwy użytkownika i hasła 'test'. Następnie kliknij przycisk **Połącz**.



Jednym z etapów łączenia jest weryfikacja nazwy użytkownika i hasła.



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. . . . . : 192.168.0.10
```

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% straty),
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 Nr strony

Bieżąca strona: 1

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	<input type="button" value="Rozłącz"/>

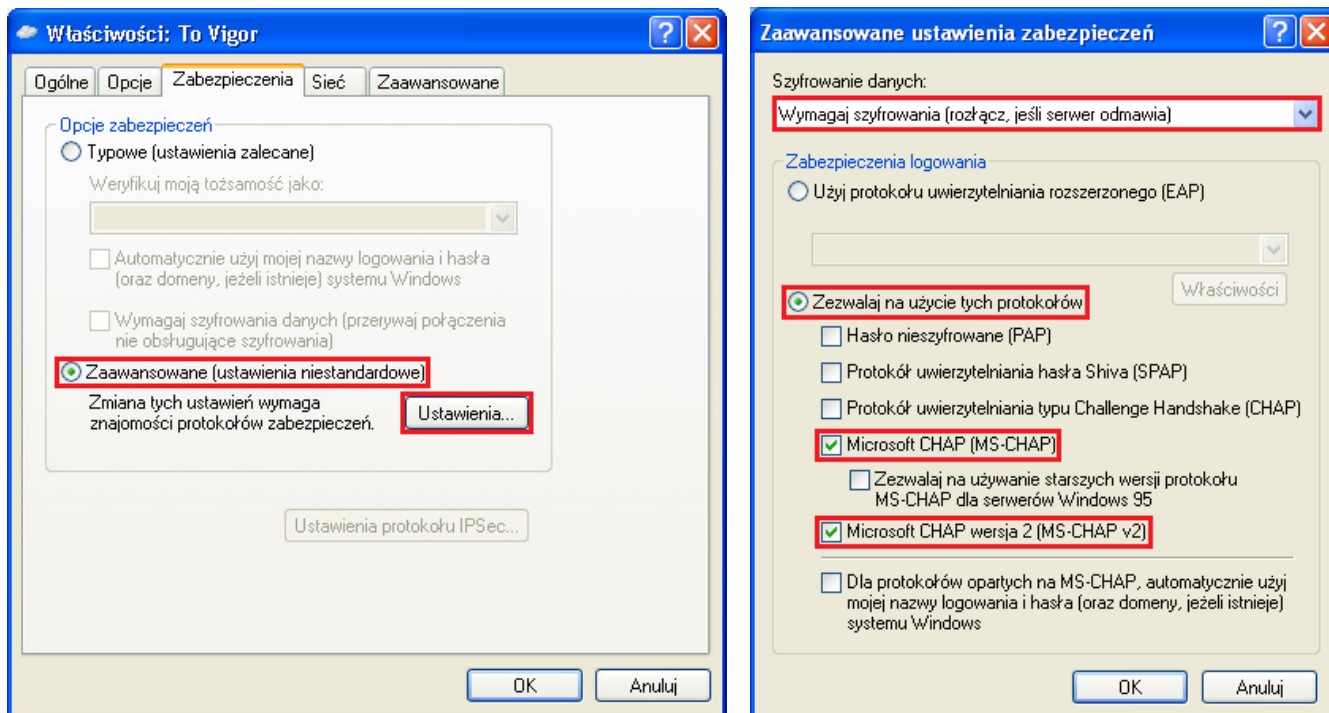
xxxxxxx : Dane są szyfrowane.
xxxxxxx : nie są szyfrowane.

4. Problemy

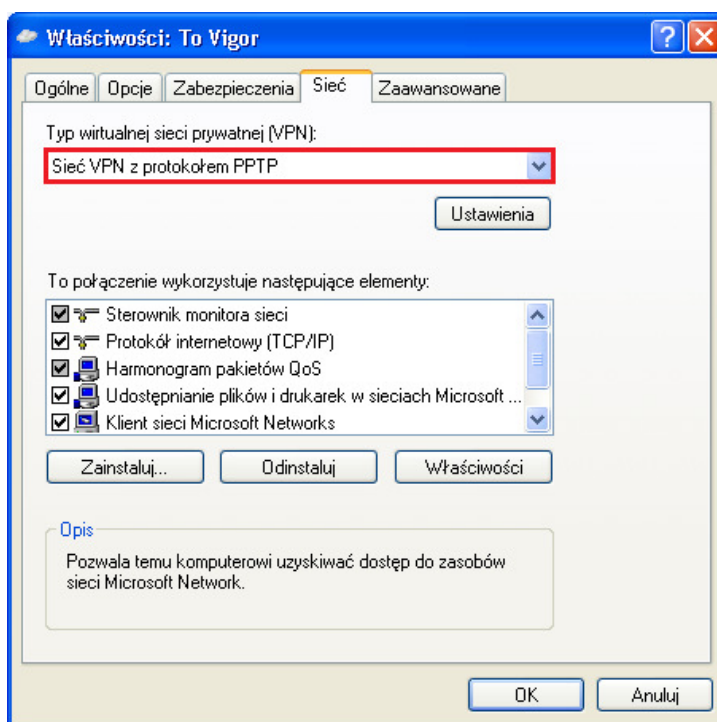
Przejdź do właściwości utworzonego połączenia.

W zakładce Zabezpieczenia przejdź do ustawień zaawansowanych.

Wybierz **Wymagaj szyfrowania** oraz zezwalaj na użycie protokołu **MS-CHAP v2**.



W zakładce Sieć wybierz **Sieć VPN z protokołem PPTP**.

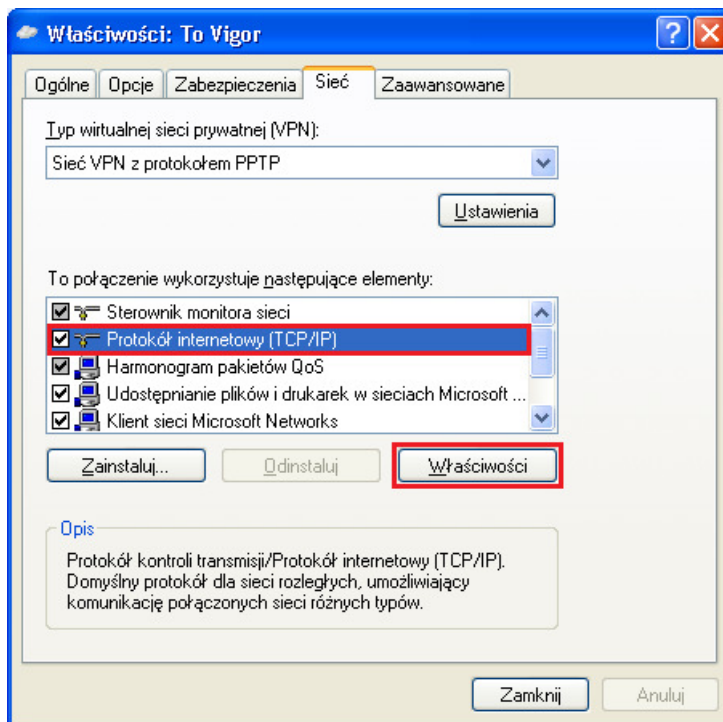


5. Brama domyślna

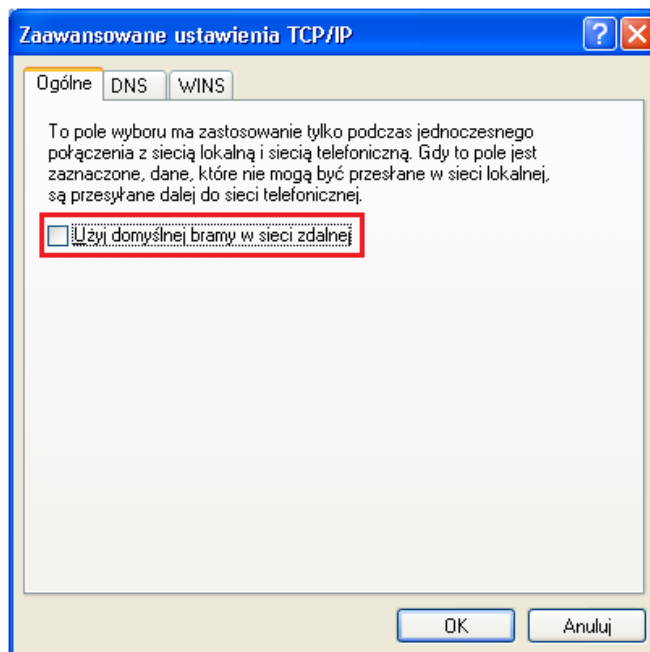
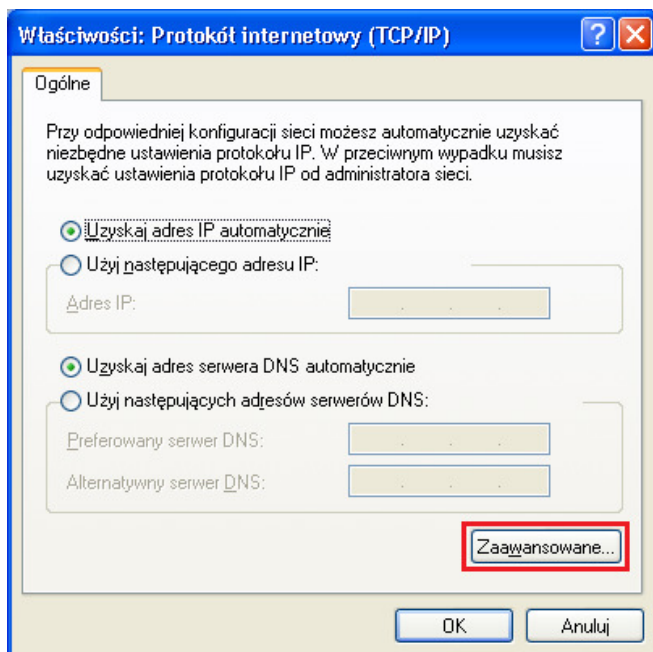
Domyślnie Windows XP kieruje cały ruch przez połączenie VPN.

Przejdź do właściwości utworzonego połączenia.

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



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



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