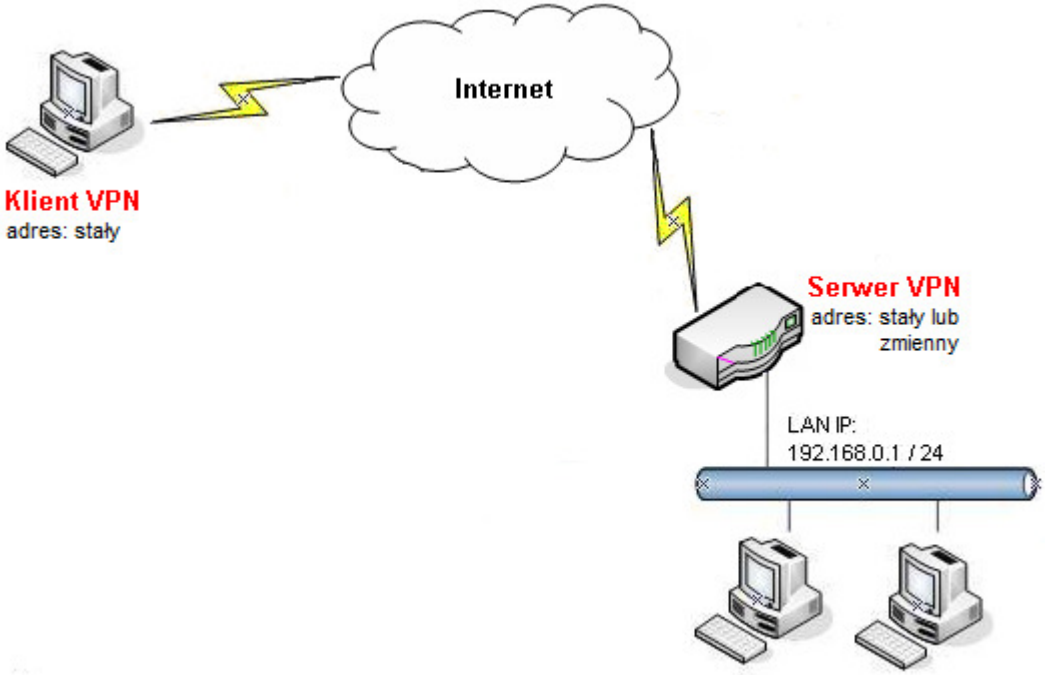
1. Konfiguracja routera

2. Konfiguracja klienta VPN

3. Zainicjowanie połączenia

Procedura konfiguracji została oparta na poniższym przykładzie.



Główne założenia:

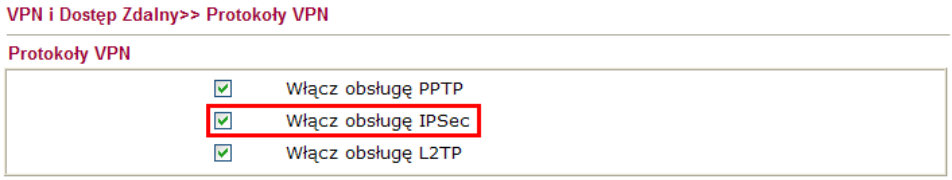
- typ tunelu: Host-LAN
- protokół VPN: IPSec (tryb główny)
- algorytm wymiany kluczy: grupa Diffie'go-Hellmana 1
- szyfrowanie: 3DES, AES128
- integralność: SHA1
- autentykacja: klucz IKE
- Adres Serwera VPN: stały (IP - 99.99.99.10) lub zmienny (domenowy - serwer.abc.xyz)
- Adres Klienta VPN: stały

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 routera

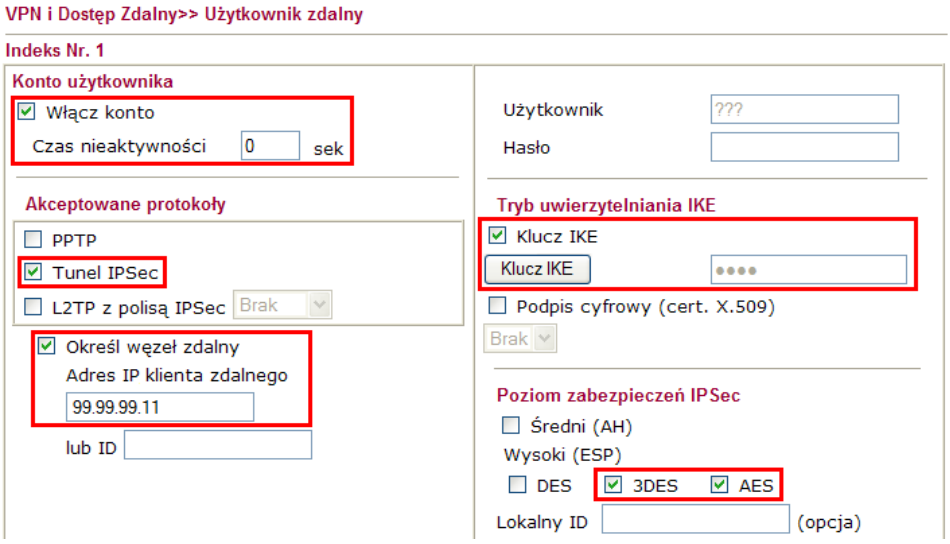
Przejdź do zakładki **VPN i Dostęp Zdalny>>Protokoły VPN** i sprawdź (lub zaznacz) czy jest włączona obsługa protokołu IPSec.



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

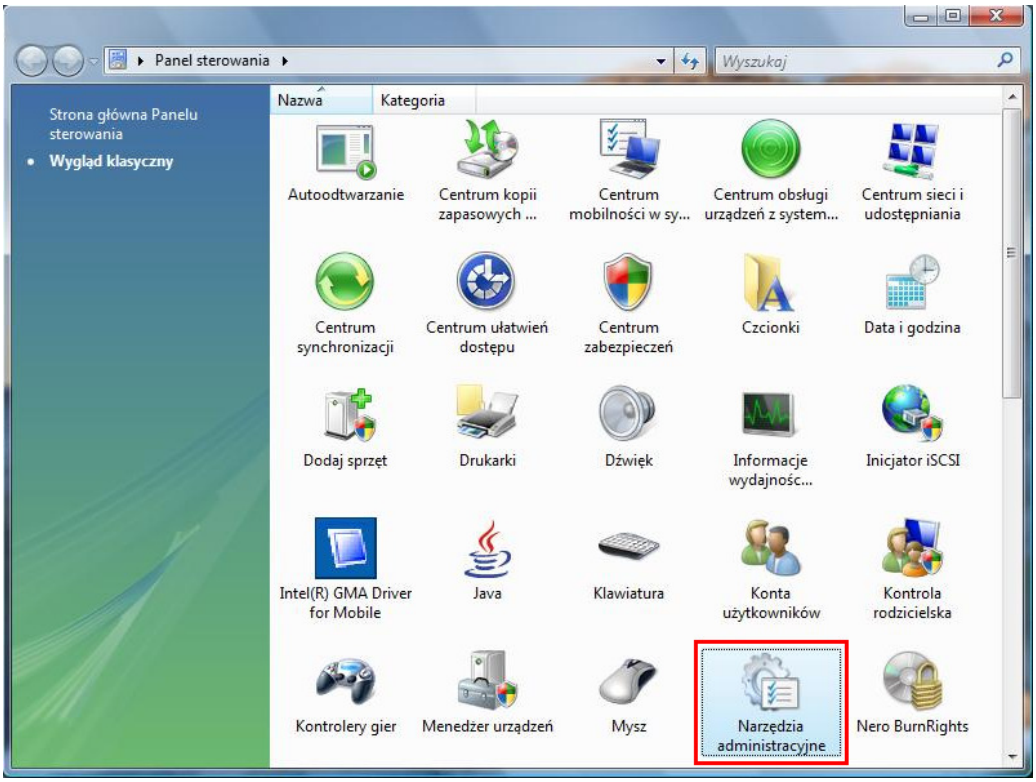
Konfiguracja zgodna z założeniami przykładu:

- zaznacz **Włącz konto**
- ustaw **czas nieaktywności 0**, gdy połączenie ma być aktywne cały czas. Domyślnie jest tam wartość 300 oznaczająca rozłączenie tunelu przez Vigor po 5 minutach.
- jako akceptowany protokół zaznacz **Tunel IPSec**
- zaznacz **Określ węzeł zdalny** i wprowadź odpowiedni adres. W przykładzie użyto 99.99.99.11
- 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 oraz AES
- kliknij przycisk OK, aby zatwierdzić ustawienia

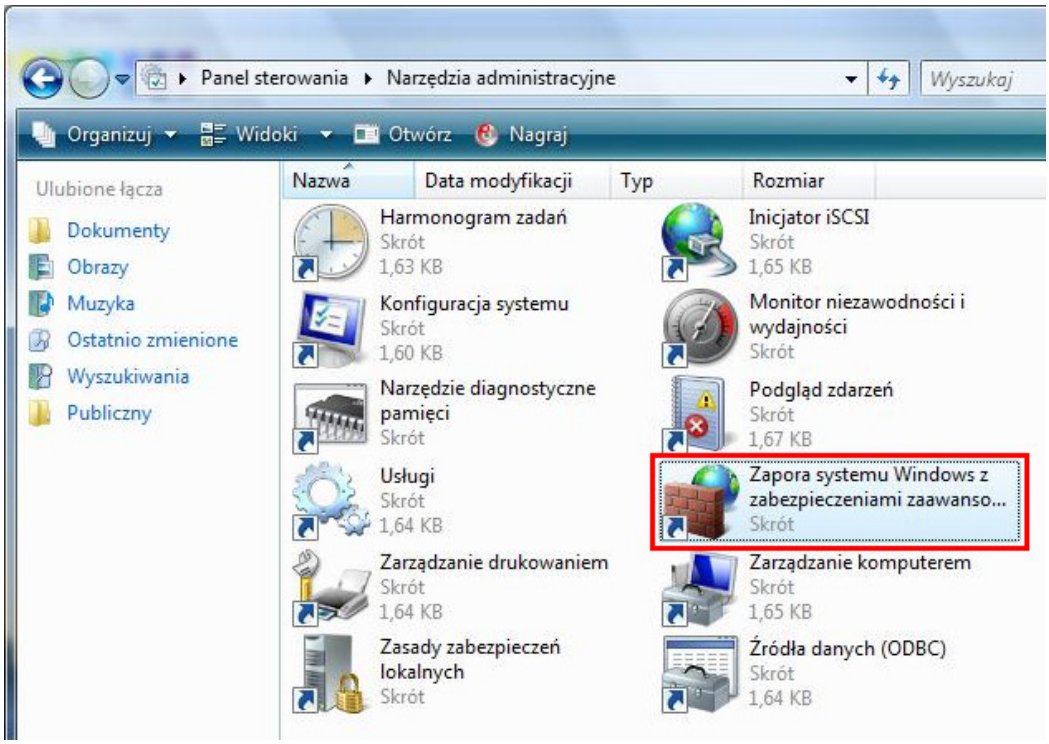


2. Konfiguracja klienta VPN

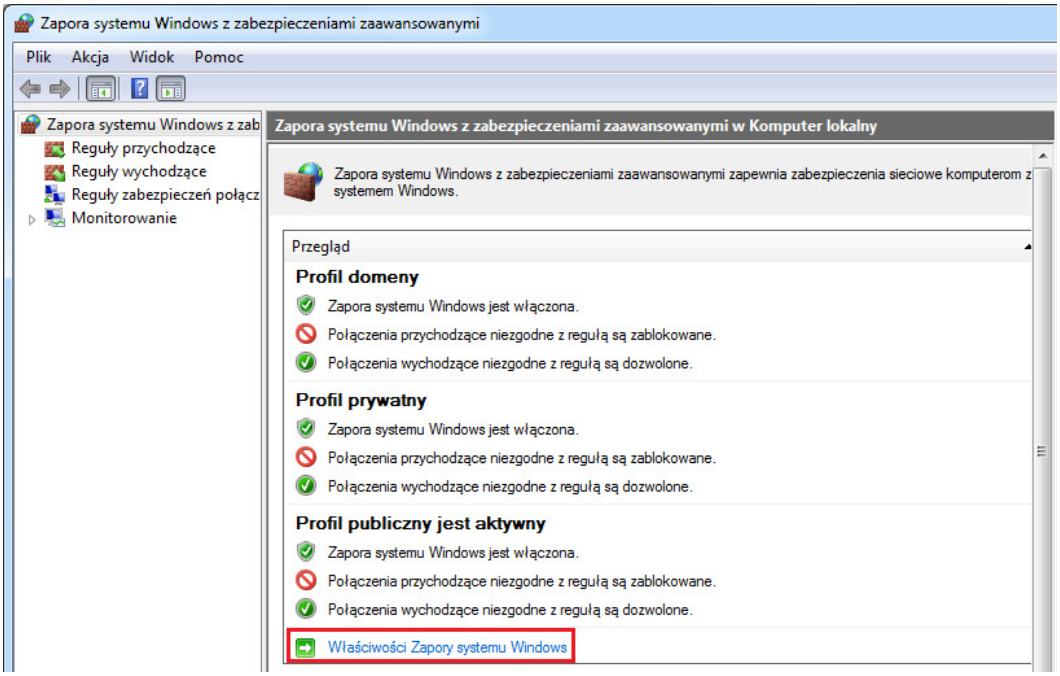
Otwórz Panel sterowania. Następnie wybierz Narzędzia administracyjne.



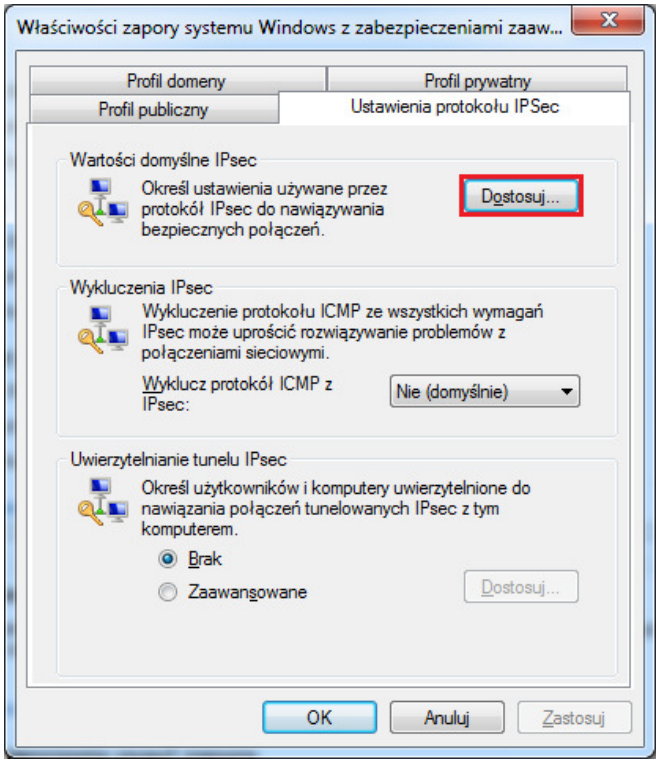
Otwórz Zaporę systemu Windows z zabezpieczeniami zaawansowanymi.



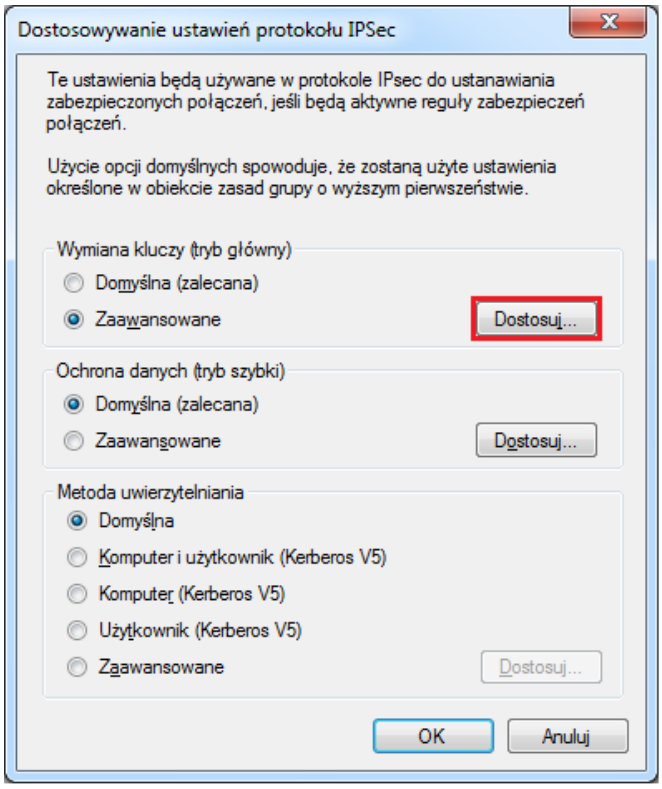
Otwórz Właściwości Zapory systemu Windows



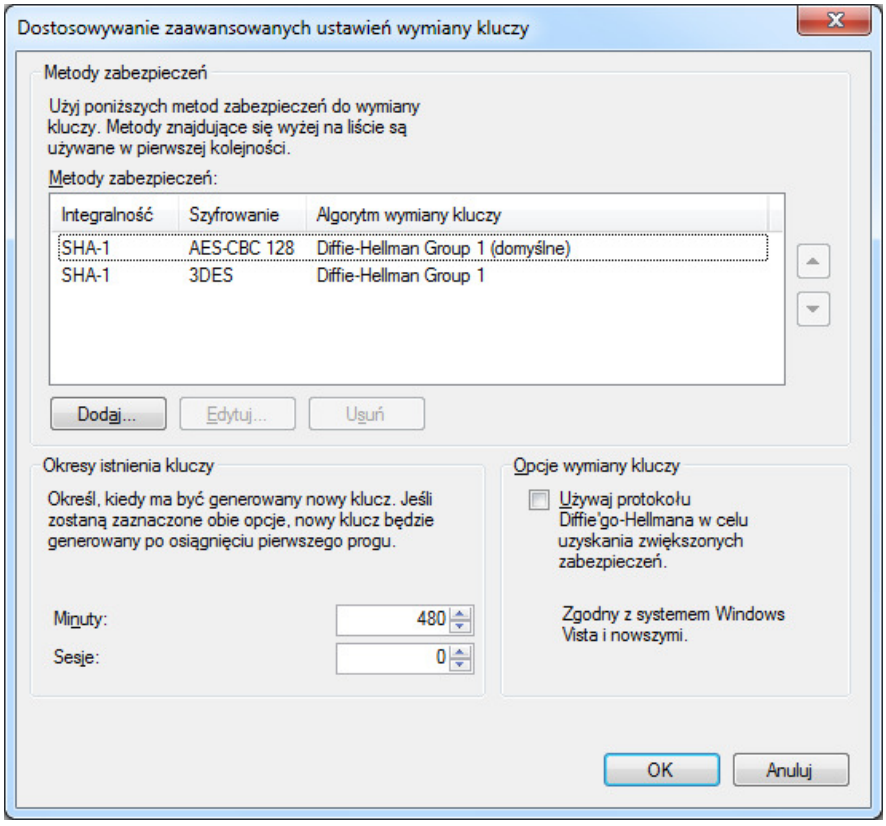
Następnie przejdź do Ustawień protokołu IPSec i kliknij przycisk Dostosuj…



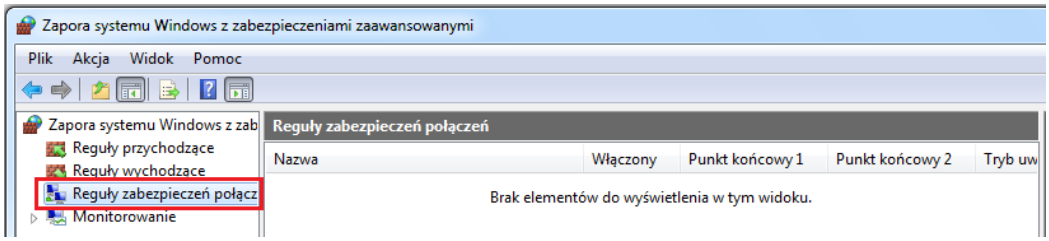
Dostosuj ustawienia zaawansowane Wymiany kluczy(tryb główny).

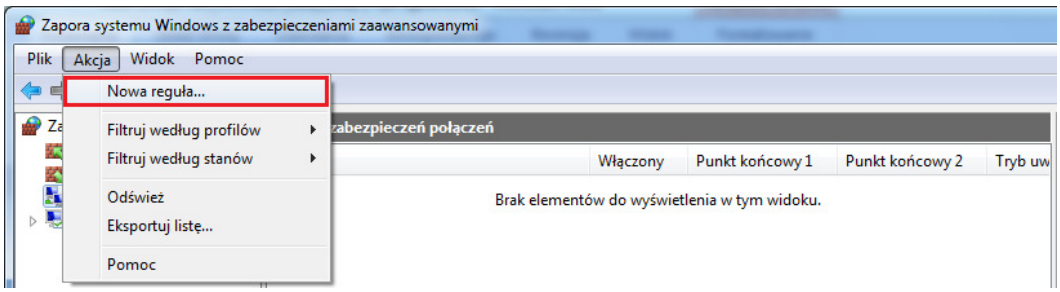


Wymiana kluczy (tryb główny):

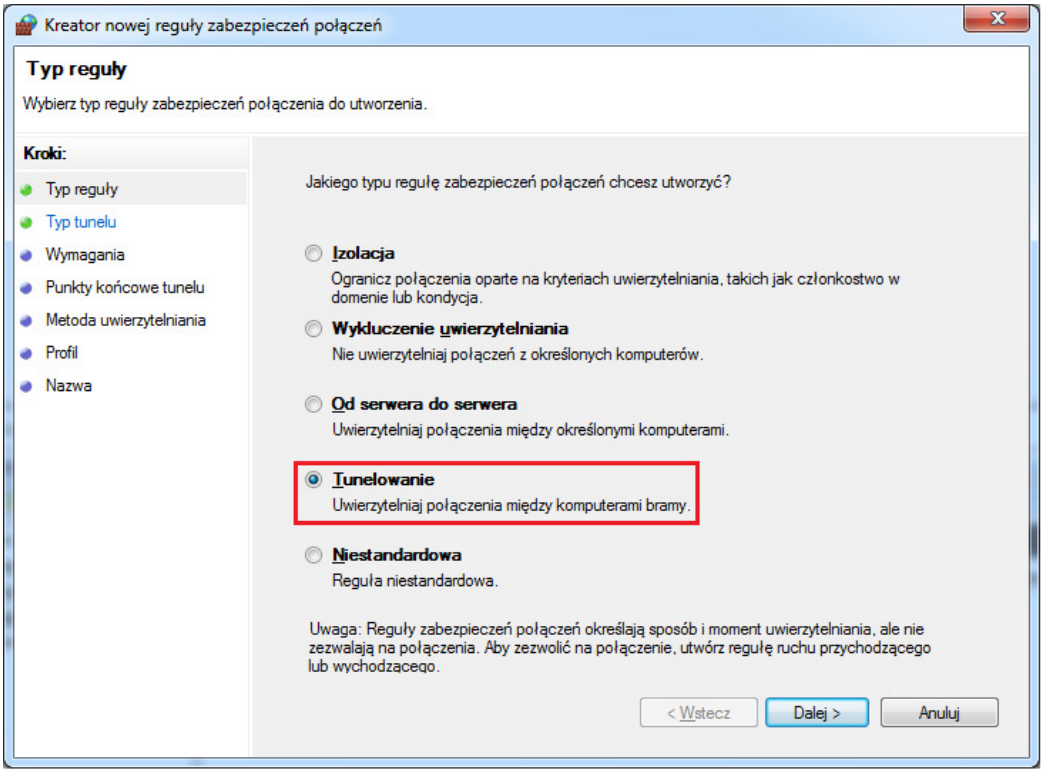


W następnym kroku stwórz Nową regułę.

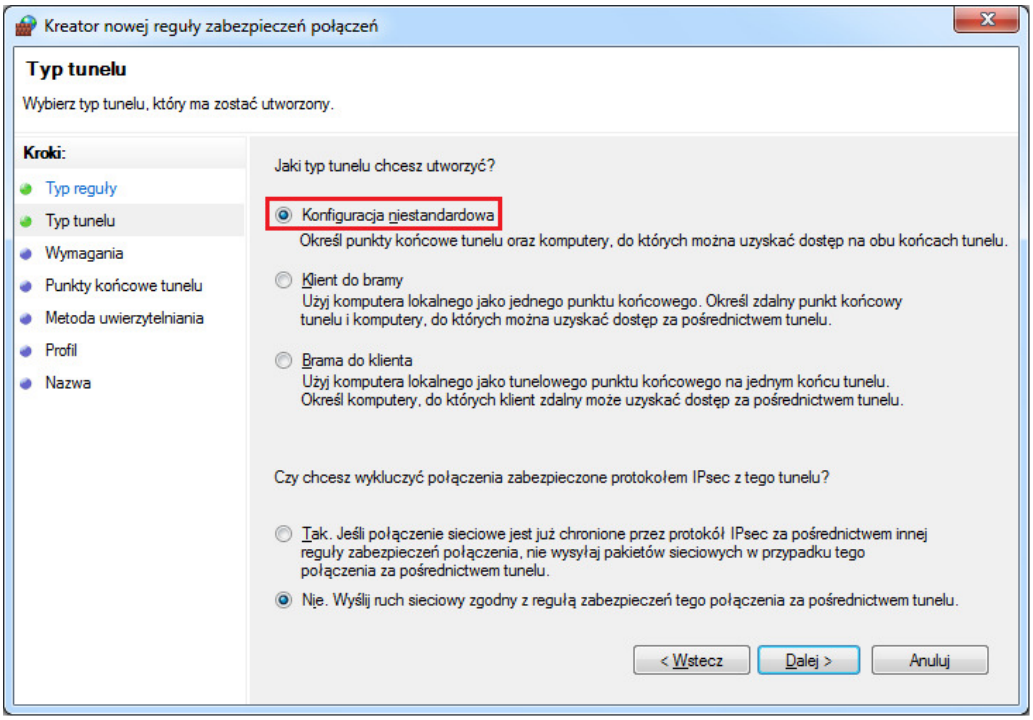




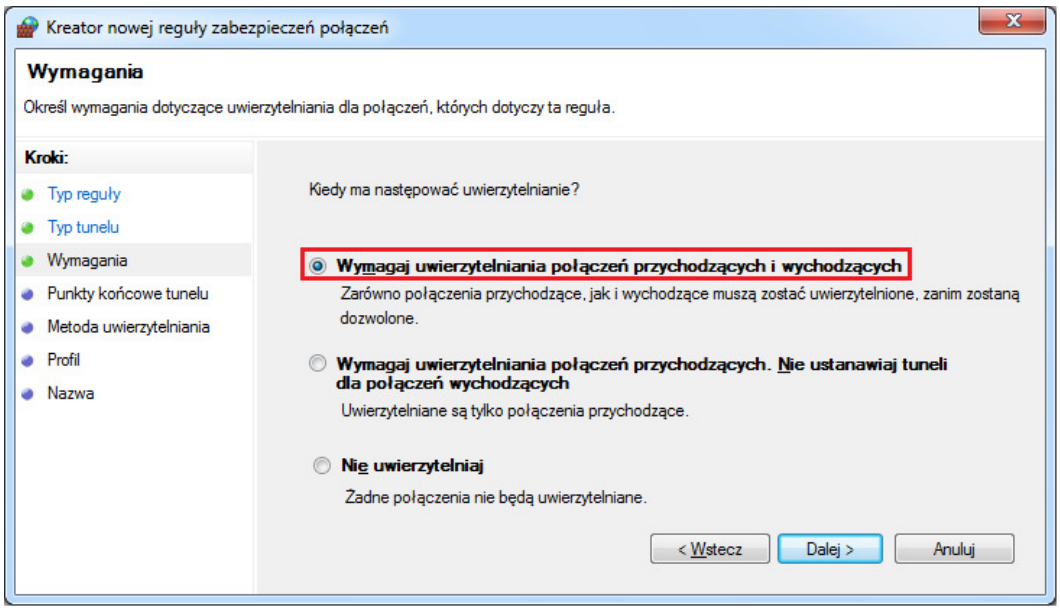
Typ reguły (Windows Vista/7): wybierz Tunelowanie.



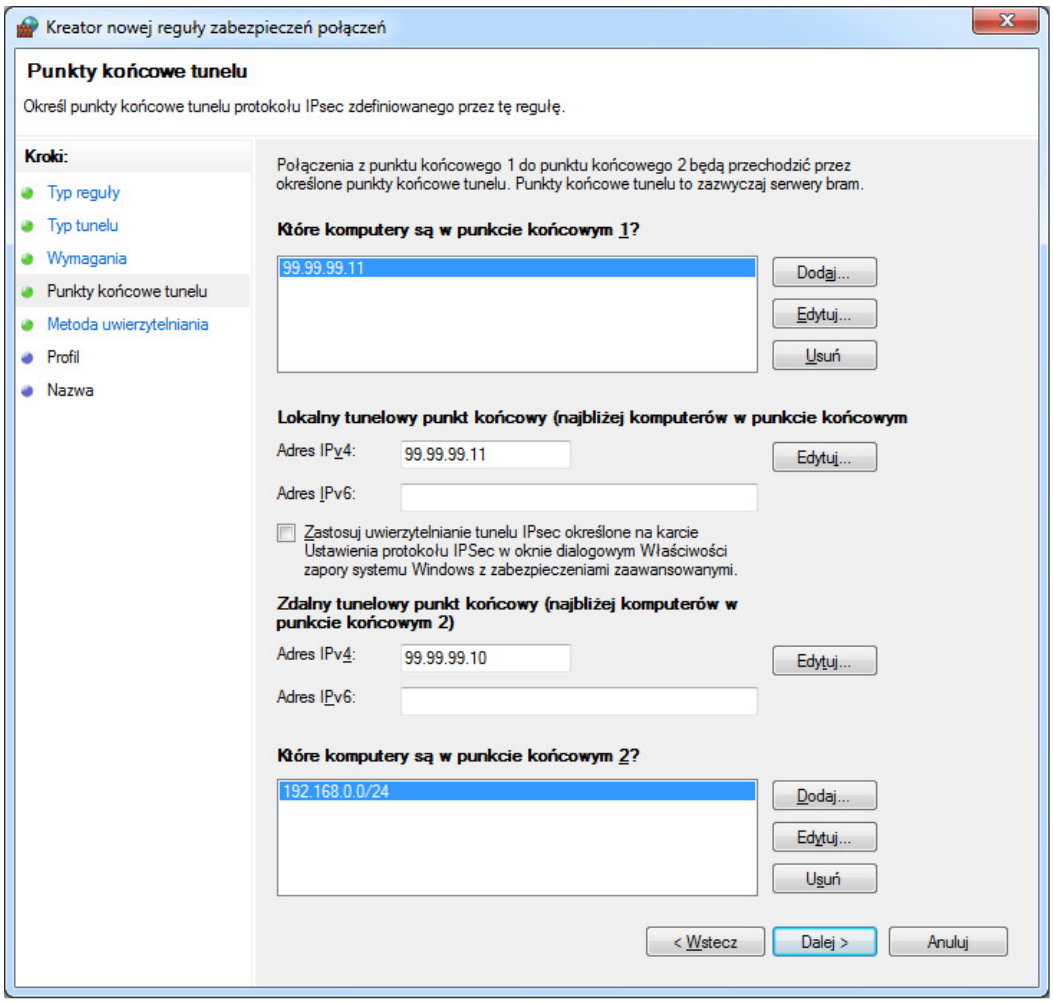
Typ tunelu (tylko Windows 7): wybierz Konfiguracja niestandardowa.



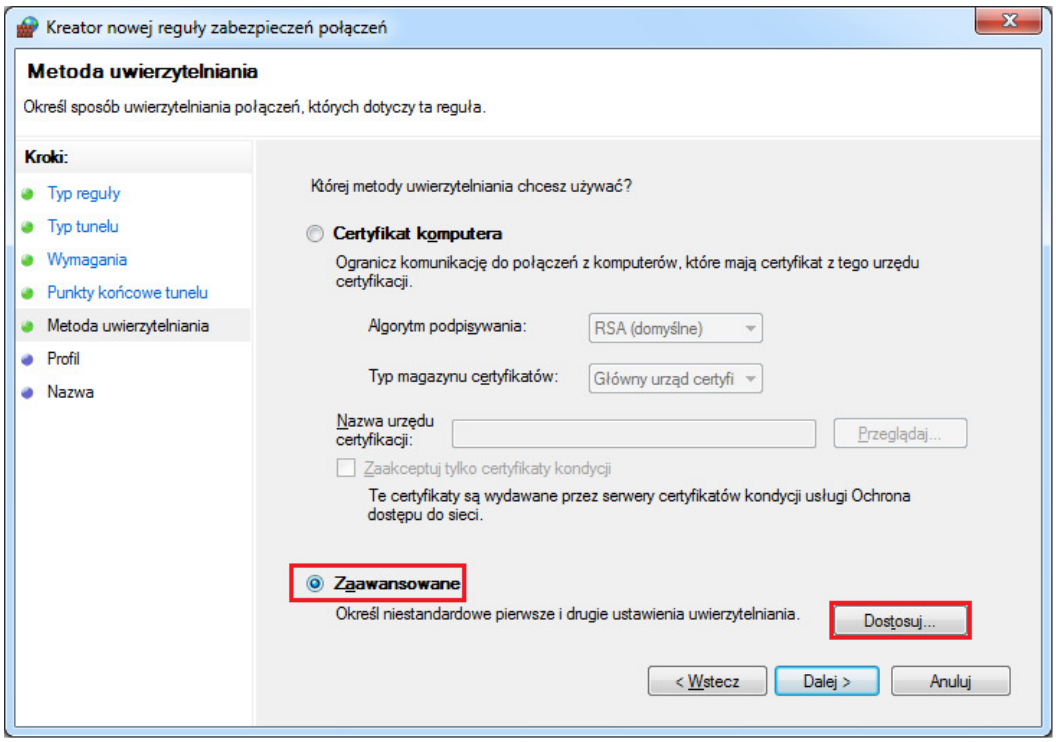
Wymagania (tylko Windows 7): wybierz Wymagaj uwierzytelniania połączeń przychodzących i wychodzących.

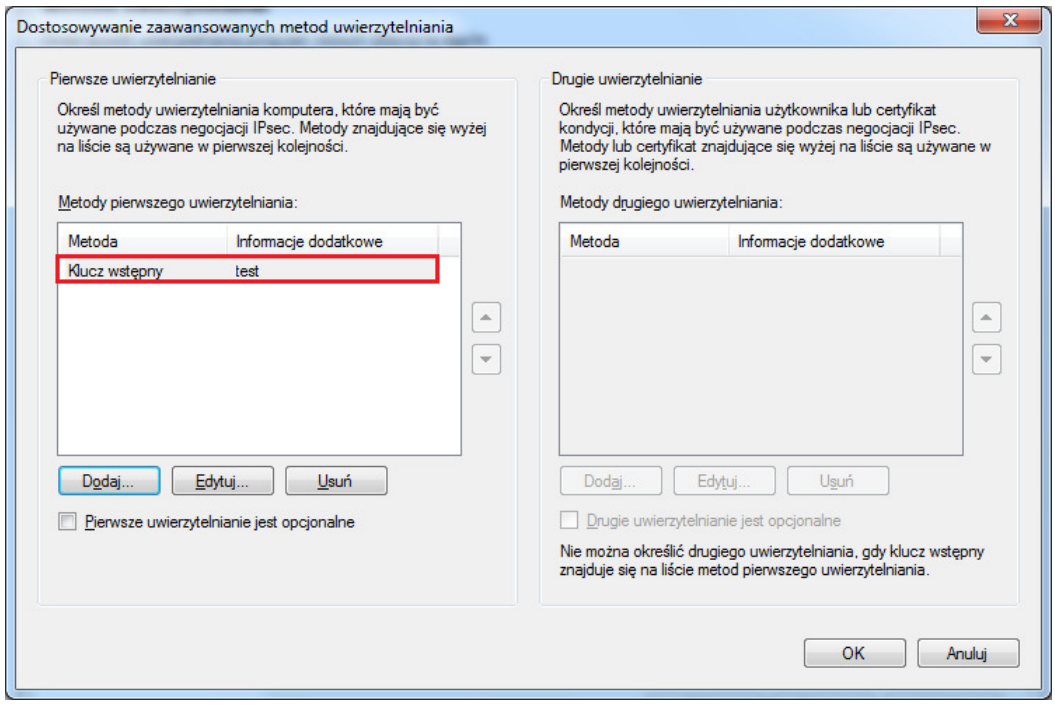


Typ tunelu (Windows Vista/7): Wpisz odpowiednie adresy IP punktów końcowych tunelu VPN. W przykładzie użyto adresacji jak na obrazku poniżej.

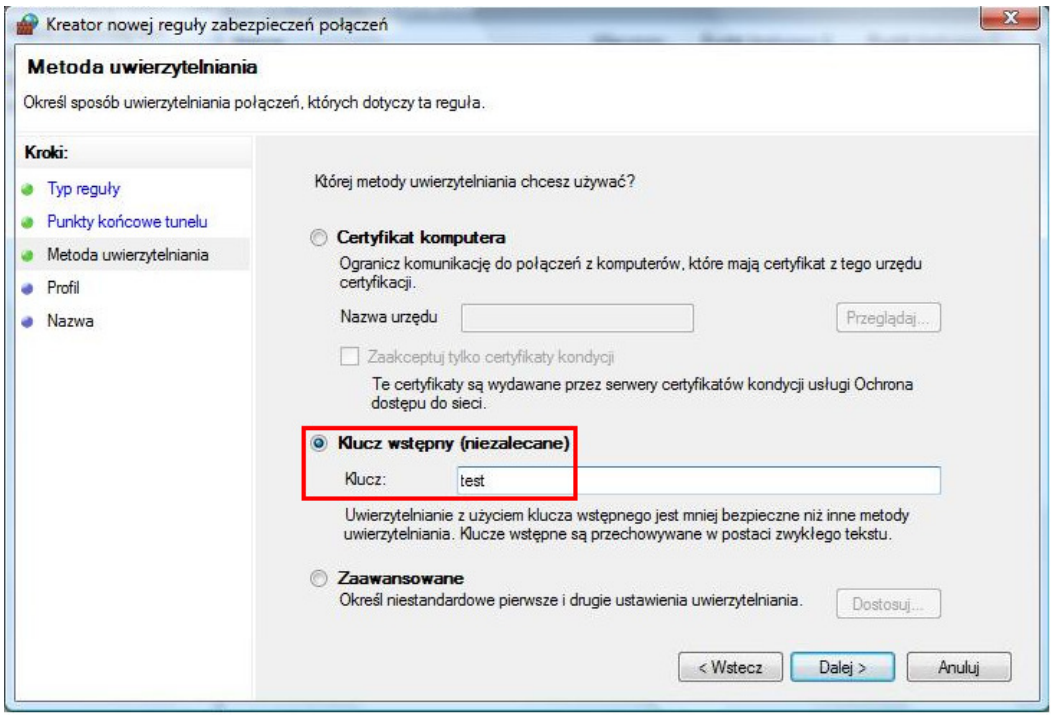


Metoda uwierzytelniania (Windows 7): Wybierz Zaawansowane. Następnie kliknij przycisk Dostosuj. Dodaj odpowiedni klucz. W przykładzie użyto klucza 'test'.

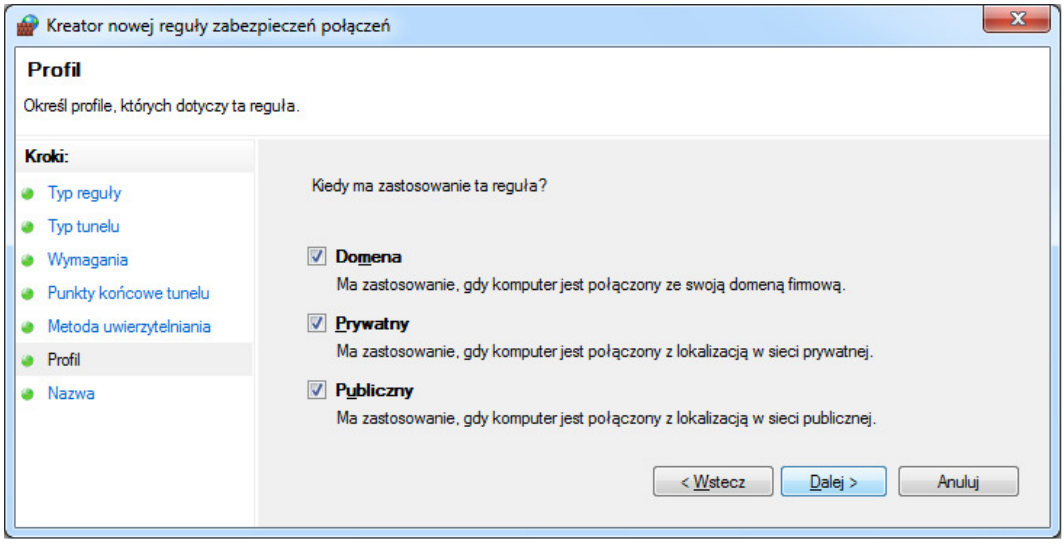




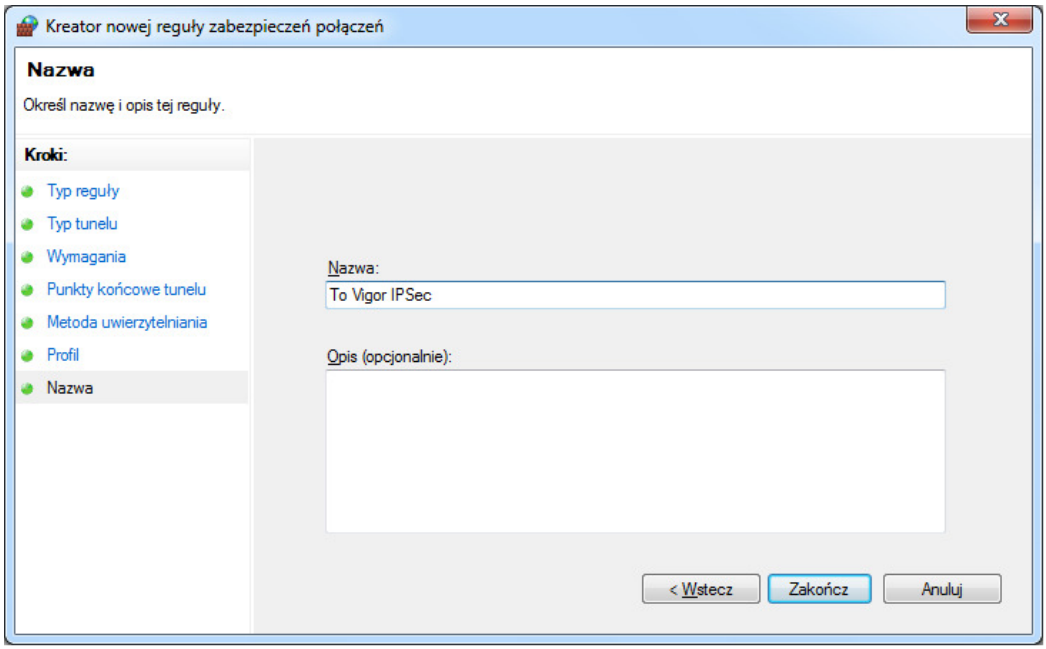
Metoda uwierzytelniania (Windows Vista): Wybierz klucz wstępny jako metodę uwierzytelniania. Wpisz odpowiedni klucz. W przykładzie użyto klucza 'test'.



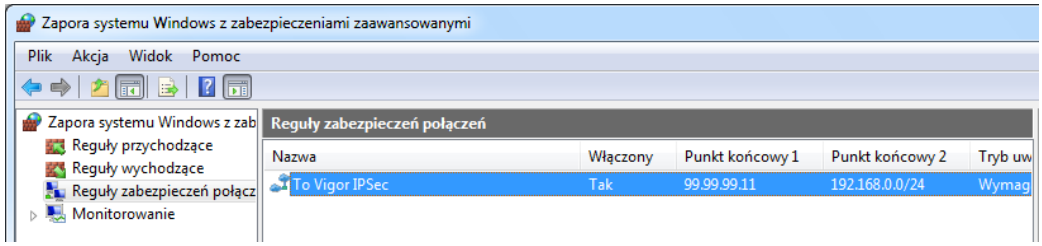
Profil (Windows Vista/7): Zaznacz kiedy ma być zastosowana reguła.



Nazwa (Windows Vista/7): Wpisz nazwę reguły np. To Vigor IPSec.



Po tych krokach w Zaporze systemu Widnows z zabezpieczeniami zaawansowanymi pojawi się stworzone reguła. Sprawdź czy na pewno proces dodawania reguły przebiegł prawidłowo i reguła rzeczywiście powstała.



3. Zainicjowanie połączenia (od strony klienta 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.

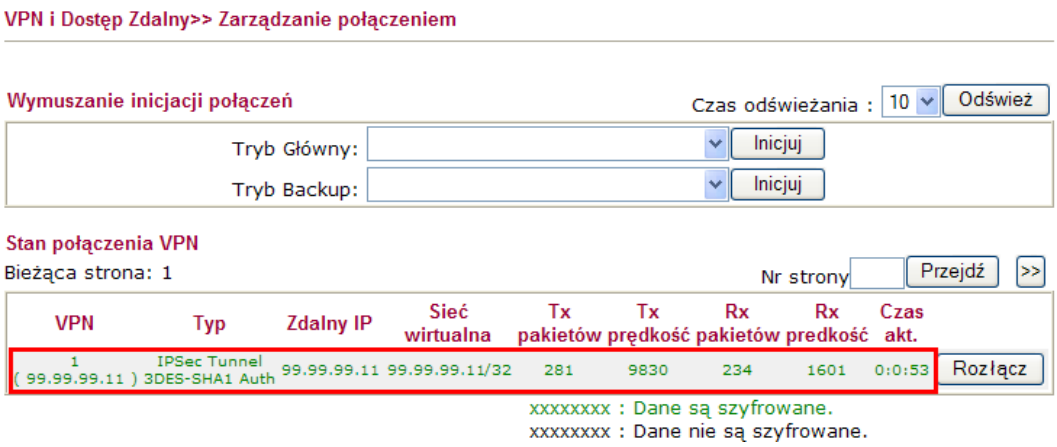
```
C:\>ping 192.168.0.1

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 błądzenia pakietów w millisekundach:
    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).



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