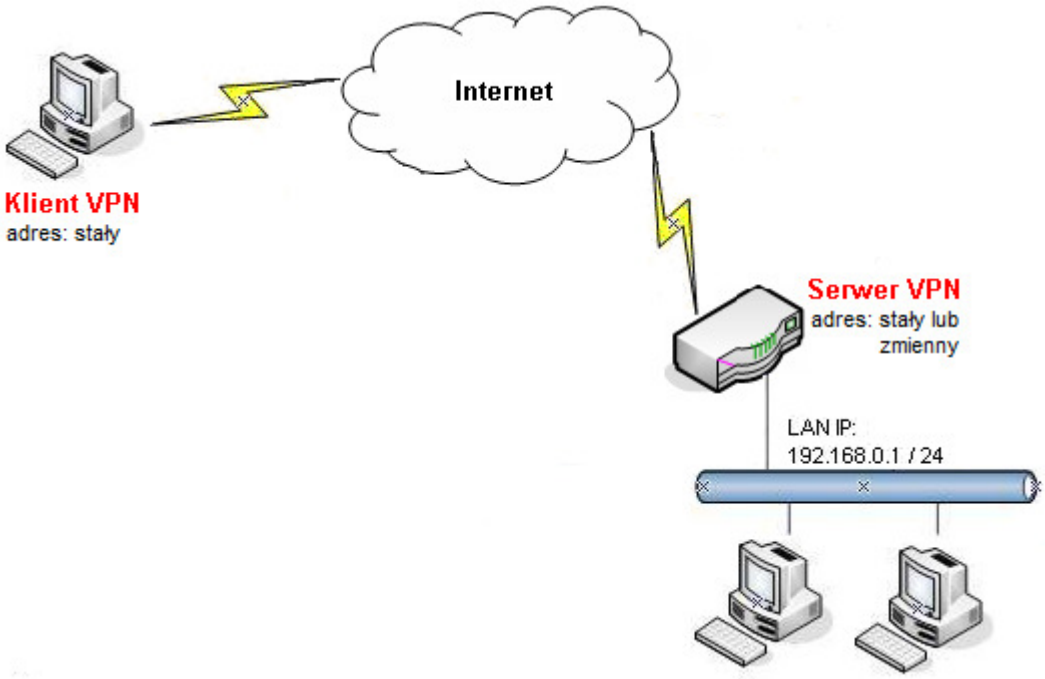
1. Konfiguracja serwera VPN

2. Konfiguracja klienta VPN

3. Zainicjowanie połączenia

Procedura konfiguracji została oparta na poniższym przykładzie.



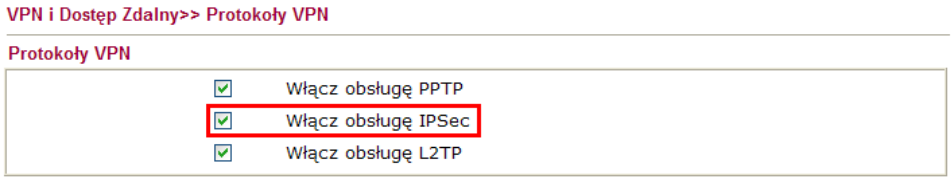
Główne założenia:

- typ tunelu: Host-LAN
- protokół VPN: IPSec (tryb główny)
- szyfrowanie: 3DES
- integralność: SHA1
- autentykacja: klucz IKE
- Adres Serwera VPN: stały (IP - 99.99.99.10) lub zmienny (domenowy - serwer.abc.xyz)
- Adres Klienta VPN: stały

Uwaga
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

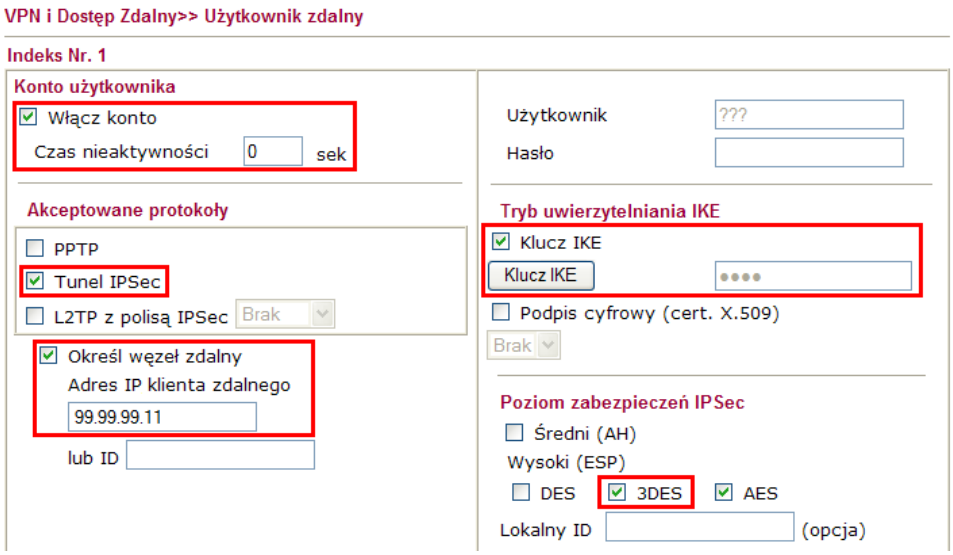
Przejdź do zakładki **VPN i Dostęp Zdalny>>Protokoły VPN** i sprawdź (lub zaznacz) czy jest włączona obsługa protokołu IPSec.



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

Kliknij np. indeks 1 i wprowadź odpowiednie dane. Konfiguracja zgodna z założeniami przykładu:

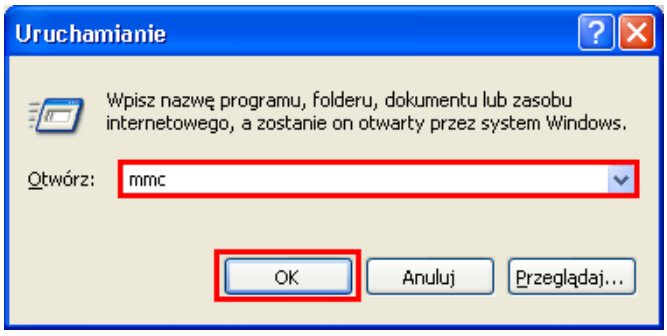
- zaznacz **Włącz konto**
- ustaw **czas nieaktywności 0**, gdy połączenie ma być aktywne cały czas. Domyślnie jest tam wartość 300 oznaczająca rozłączenie tunelu przez Vigor po 5 minutach.
- jako akceptowany protokół zaznacz **Tunel IPSec**
- zaznacz **Określ węzeł zdalny** i wprowadź odpowiedni adres.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



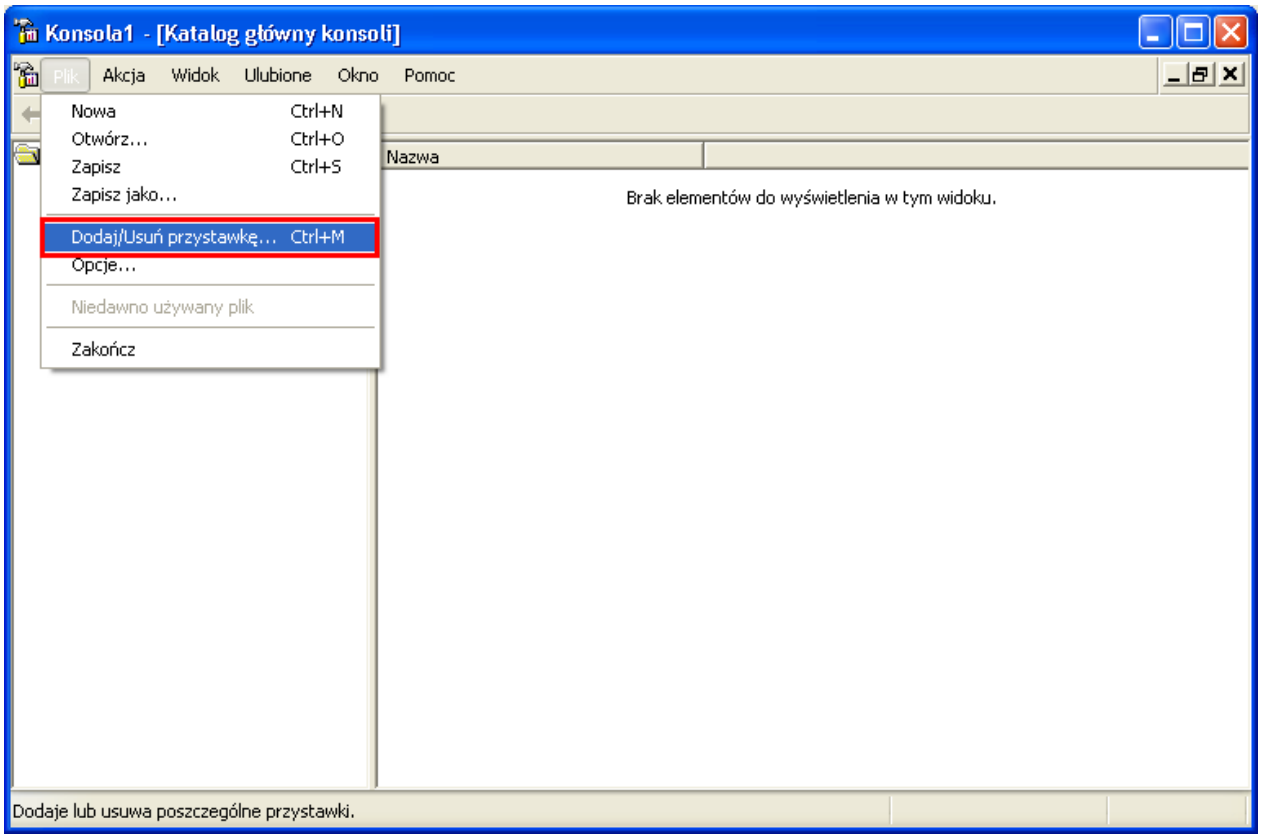
2. Konfiguracja klienta VPN

Konfiguracja **Zasad zabezpieczeń IP**:

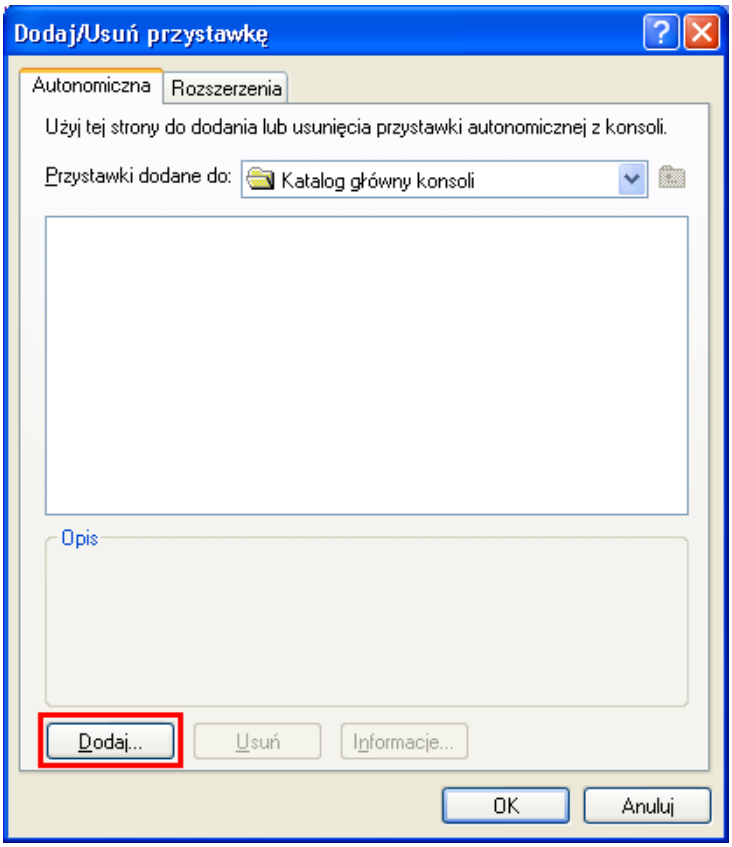
1. Uruchom mmc.exe



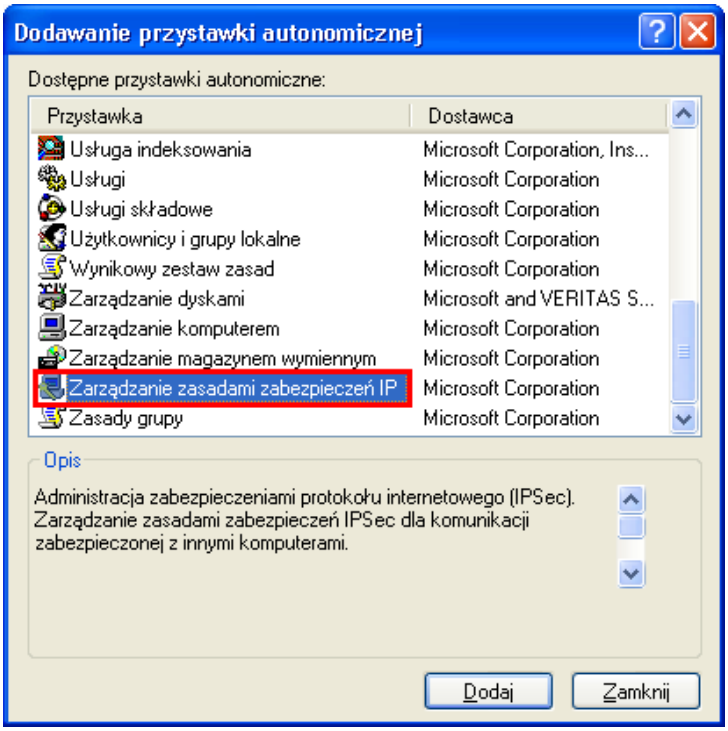
2. Dodaj **Zarządzanie zasadami zapezpieczeń IP** wybierając **Dodaj/Usuń przystawkę**



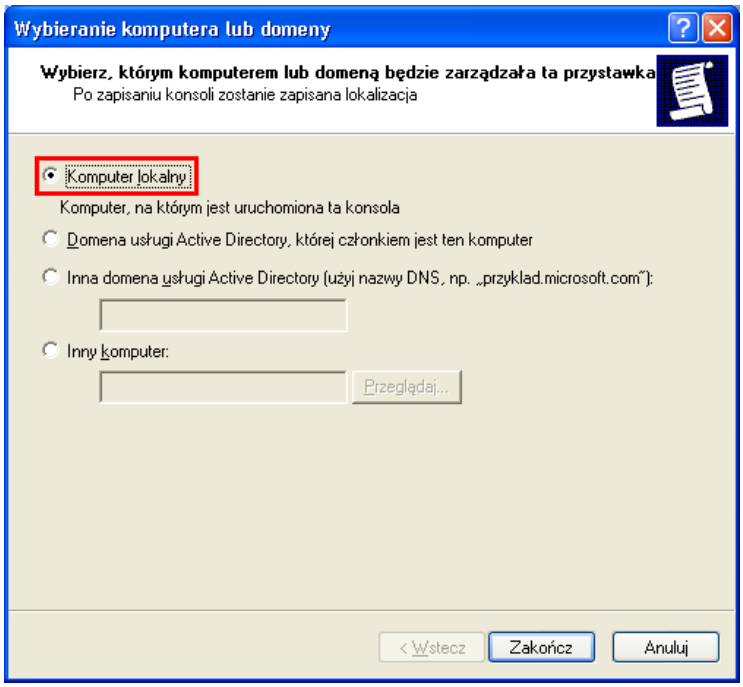
3. Kliknij **Dodaj**



4. Wybierz **Zarządzanie zasadami zapezpieczeń IP** i kliknij **Dodaj**.

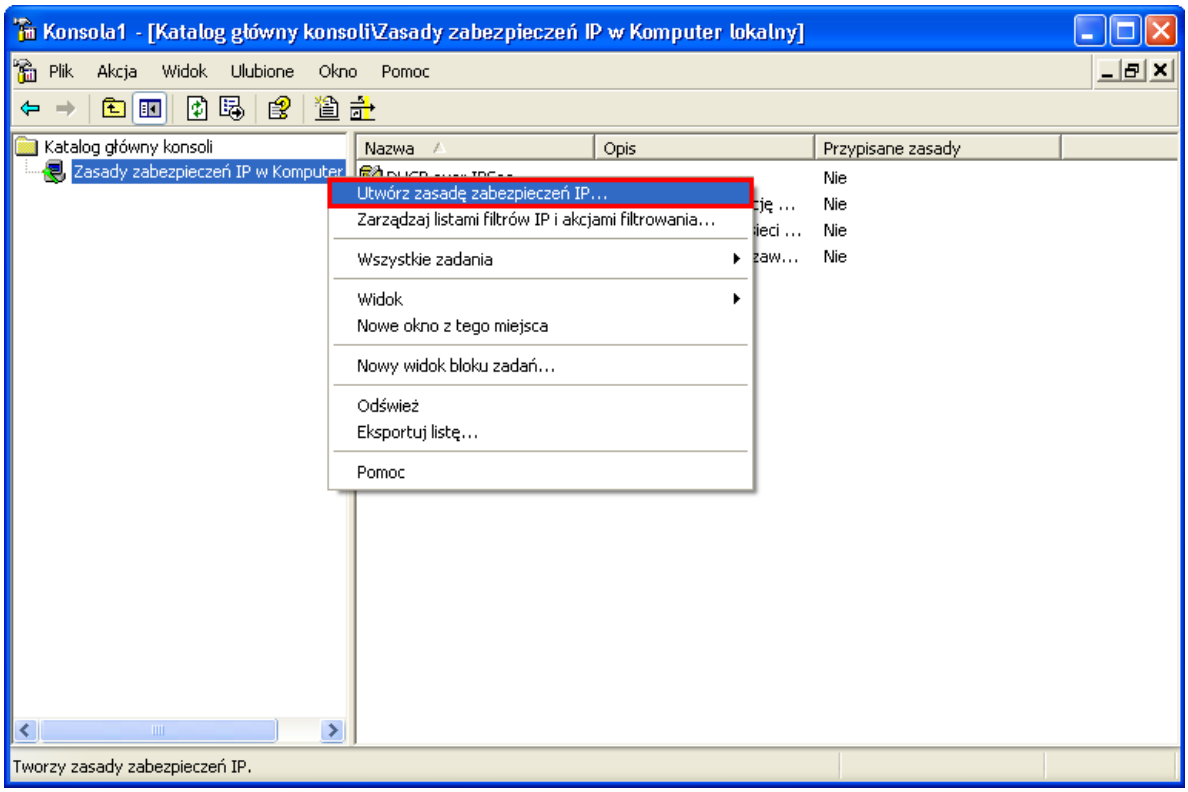


5. Wybierz **Lokalny komputer** i kliknij **Zakończ**.

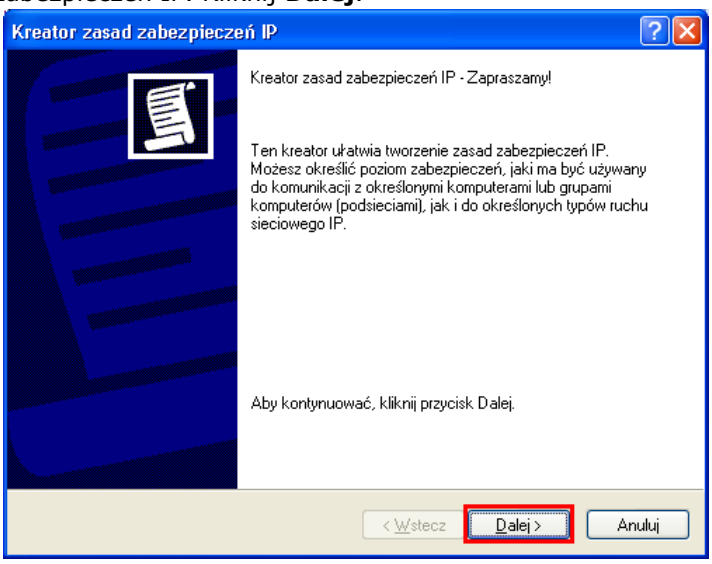


6. Została dodana opcja **Zarządzanie zasadami zapezpieczeń IP**.

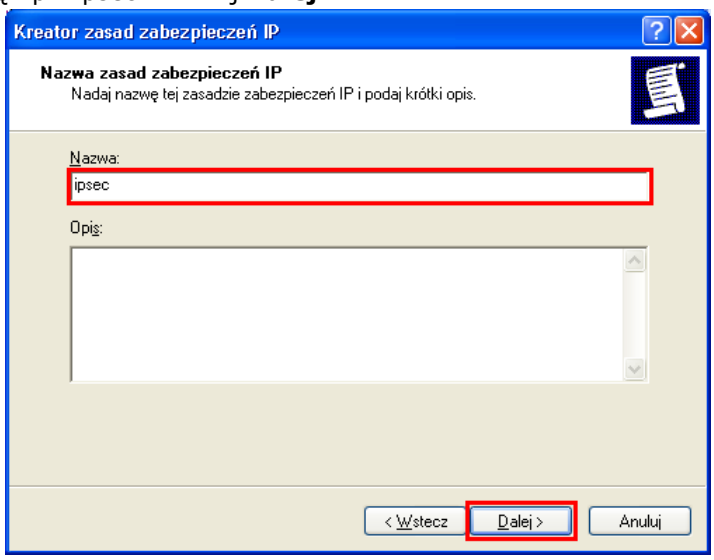
7. Wybierz **Utwórz zasadę zabezpieczeń IP**



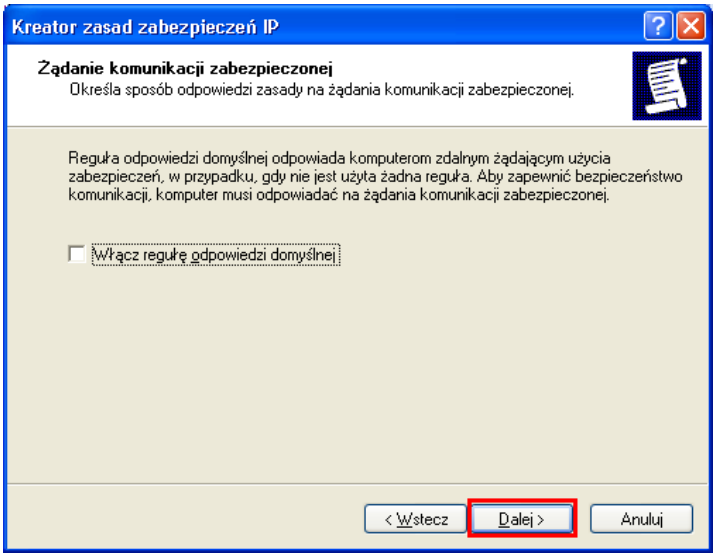
8. Pojawi się Kreator zasad zabezpieczeń IP. Kliknij **Dalej**.



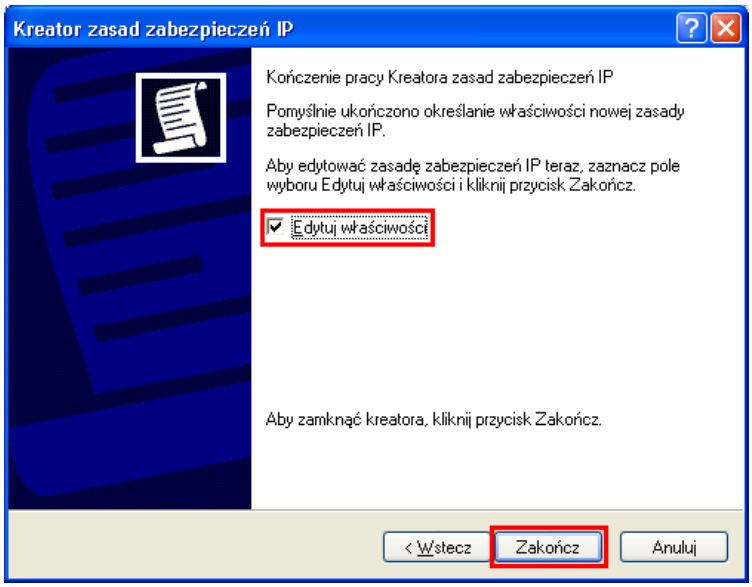
9. Wprowadź dowolną nazwę np. "ipsec". Kliknij **Dalej**.



10. Odznacz **Włącz regułę odpowiedzi domyślnej**. Kliknij **Dalej**.

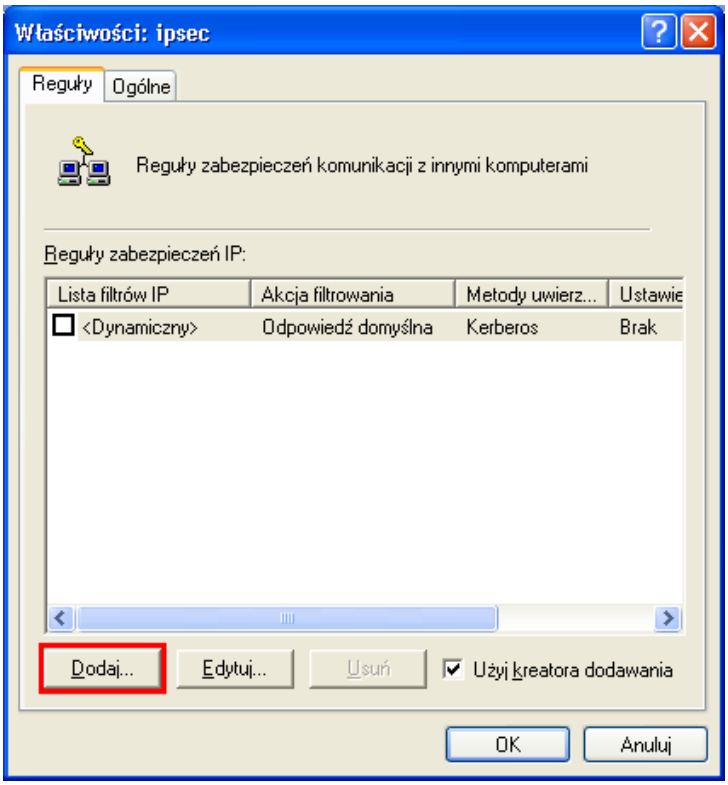


11. Zaznacz **Edytuj właściwości**. Kliknij **Zakończ**.

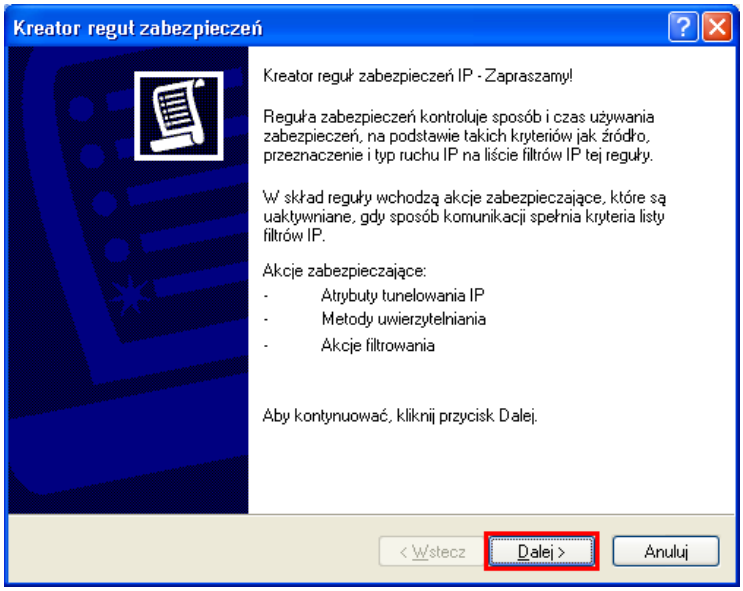


Dodanie reguły dla wychodzącego ruchu IPSec:

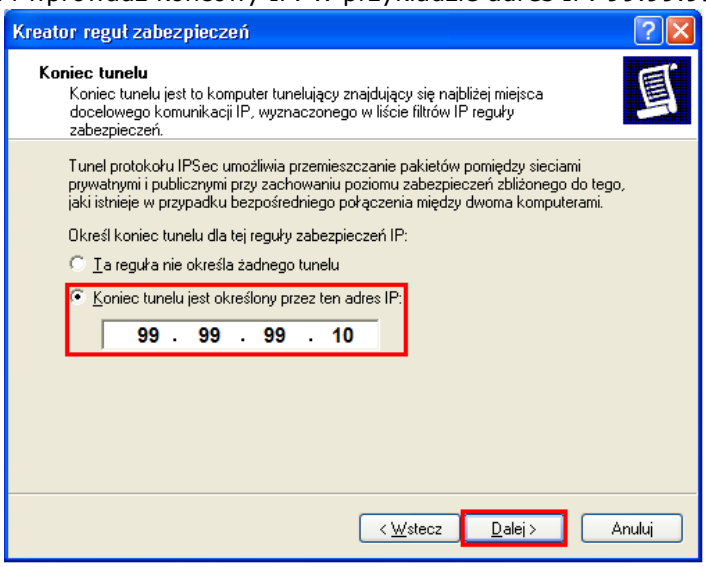
1. Otwórz właściwości stworzonej zasady **ipsec** . Kliknij **Dodaj**.



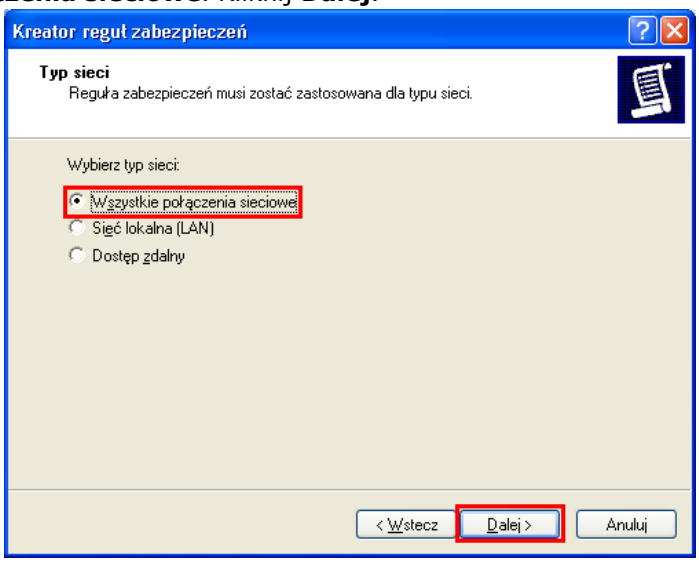
2. Pojawi się Kreator reguł zabezpieczeń IP. Kliknij **Dalej**.



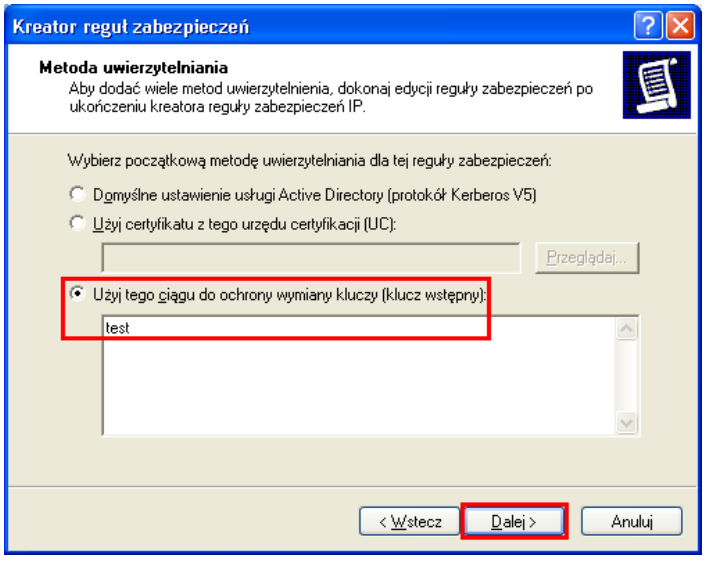
3. Wybierz **Koniec tunelu...** i wprowadź końcowy IP. W przykładzie adres IP: 99.99.99.10.



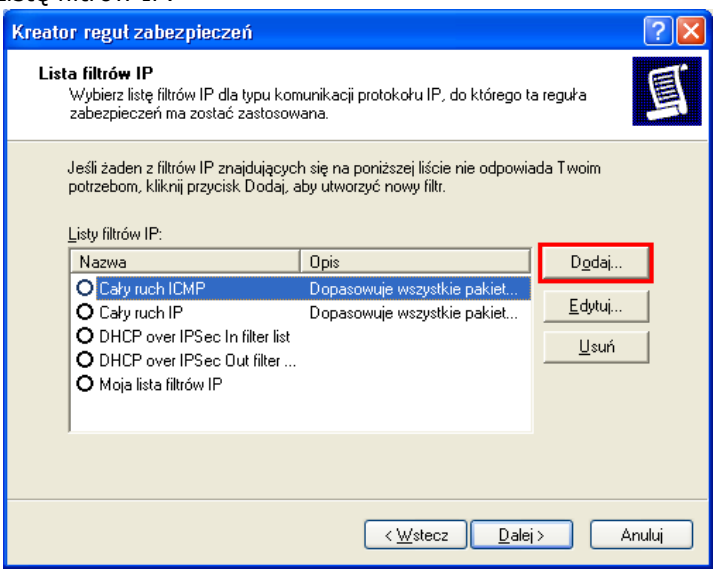
4. Wybierz **Wszystkie połączenia sieciowe**. Kliknij **Dalej**.



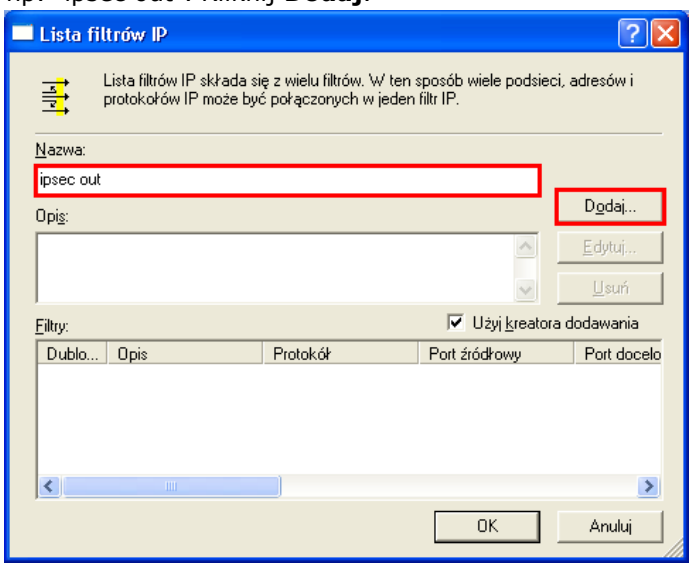
5. Wybierz **Użyj tego ciągu...** i wprowadź klucz. Kliknij **Dalej**.



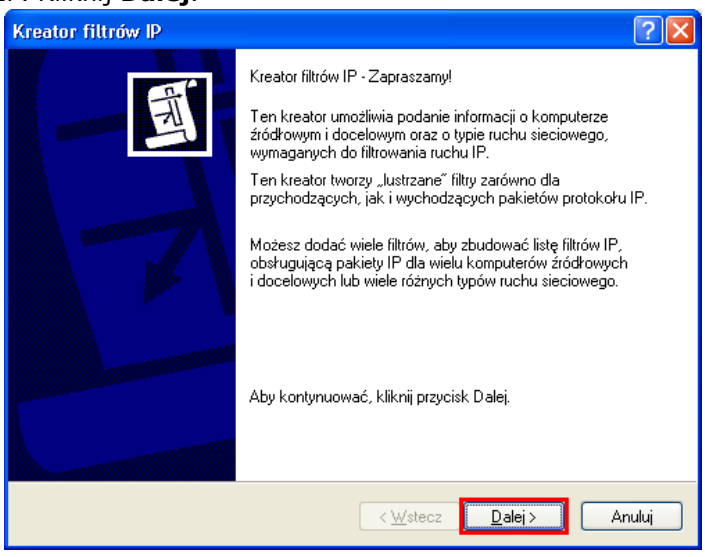
6. Kliknij **Dodaj** aby dodać Listę filtrów IP.



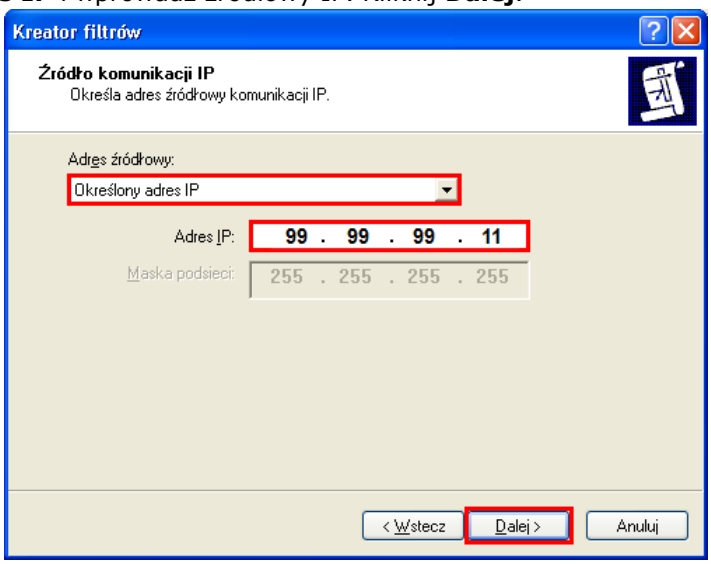
7. Wprowadź dowolną nazwę np. "ipsec out". Kliknij **Dodaj**.



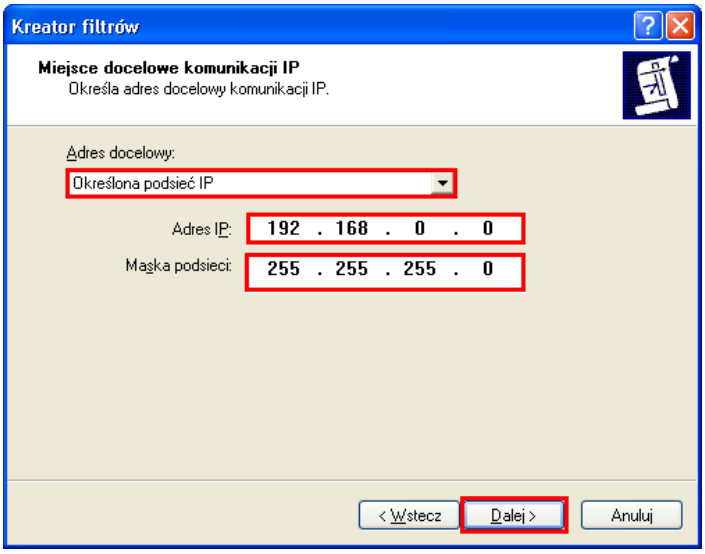
8. Pojawi się Kreator filtrów IP. Kliknij **Dalej**.



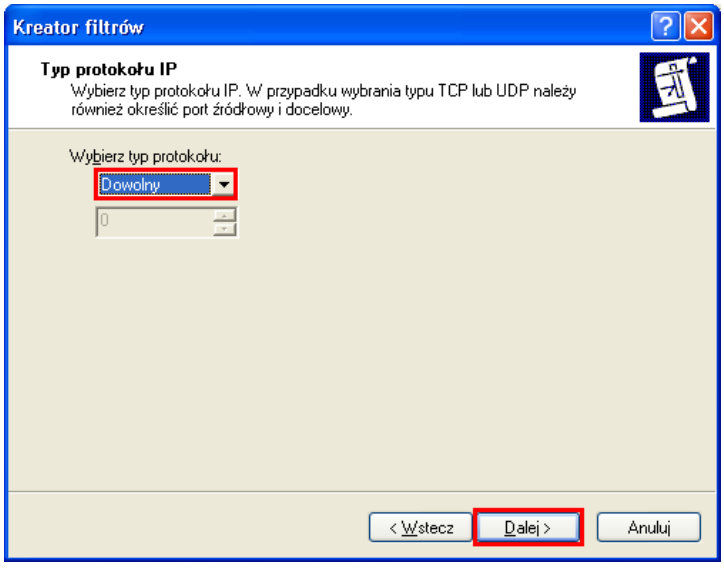
9. Wybierz **Określony adres IP** i wprowadź źródłowy IP. Kliknij **Dalej**.



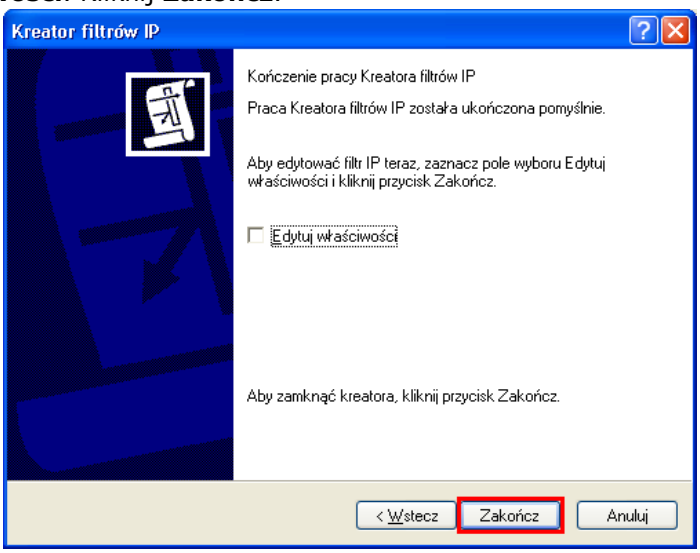
10. Wybierz **Określona podsieć IP** oraz wprowadź adres IP i maskę. Kliknij **Dalej**.



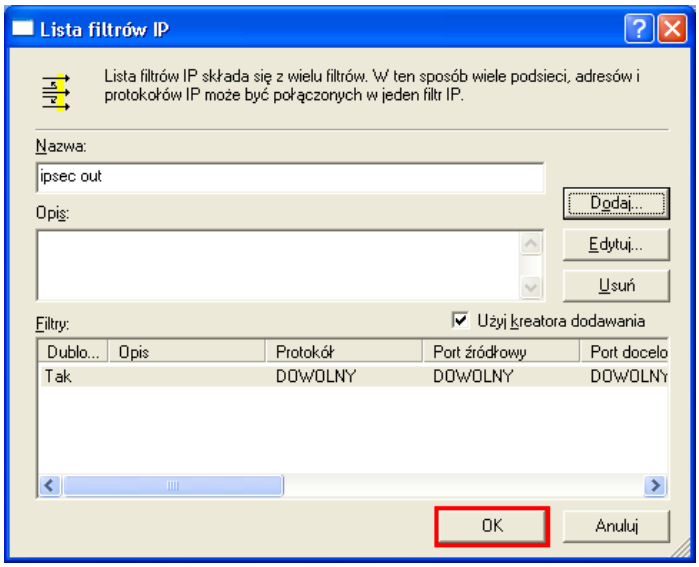
11. Wybierz **Dowolny** typ protokołu IP.



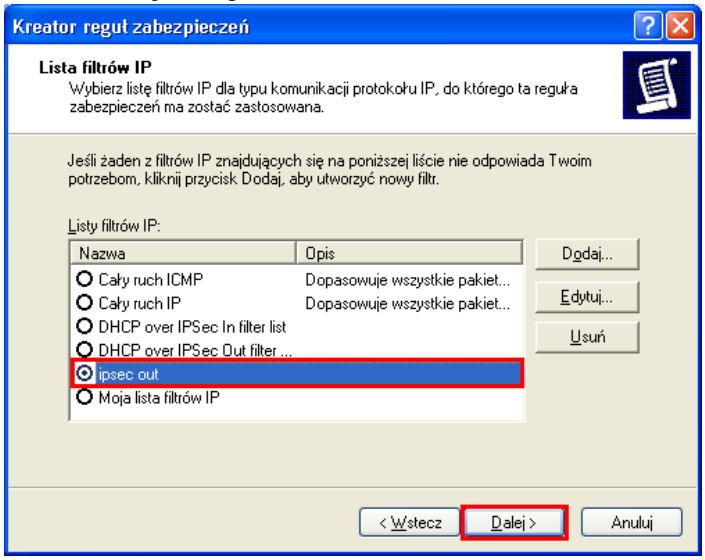
12. Odznacz **Edytuj właściwości**. Kliknij **Zakończ**.



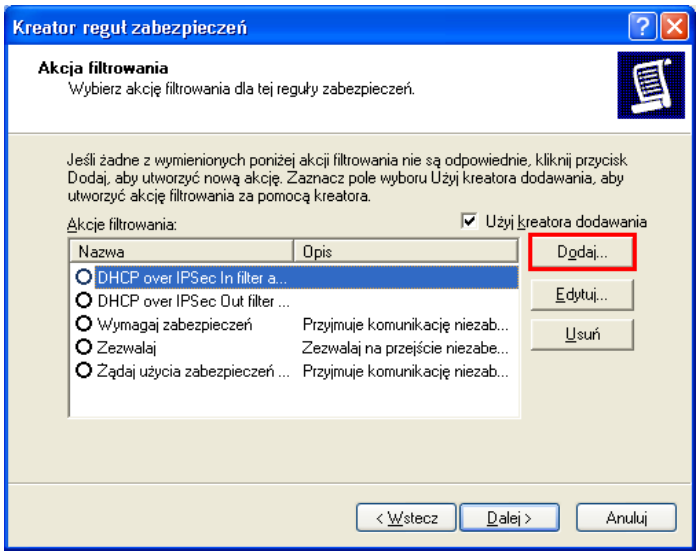
13. Kliknij **OK**.



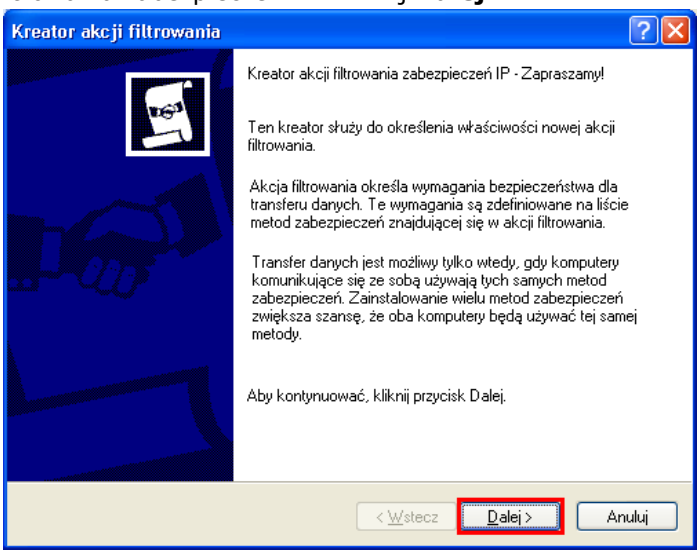
14. Wybierz listę filtrów **ipsec out**. Kliknij **Dalej**.



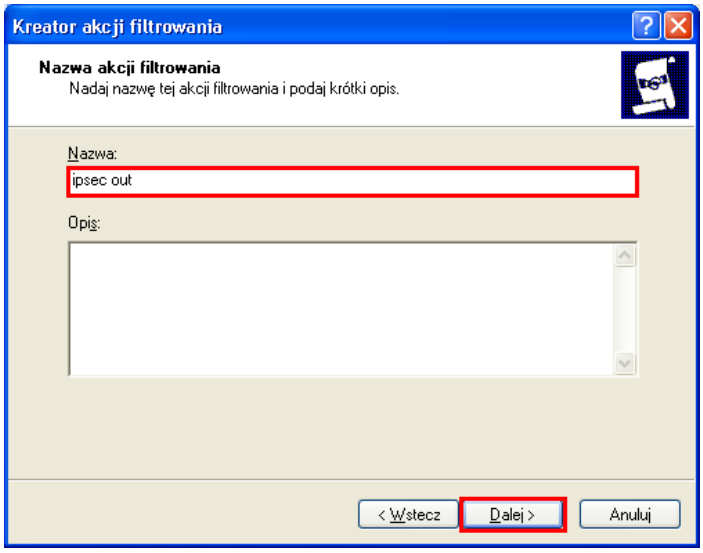
15. Kliknij **Dodaj**.



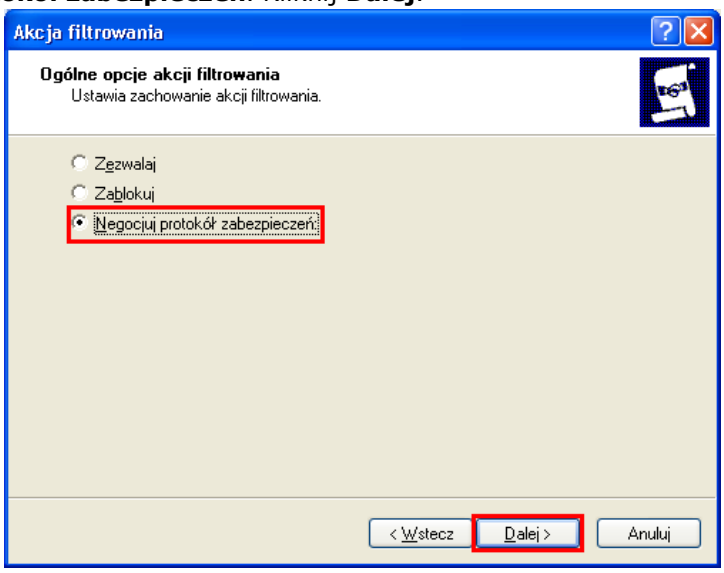
16. Pojawi się Kreator akcji filtrowania zabezpieczeń IP. Kliknij **Dalej**.



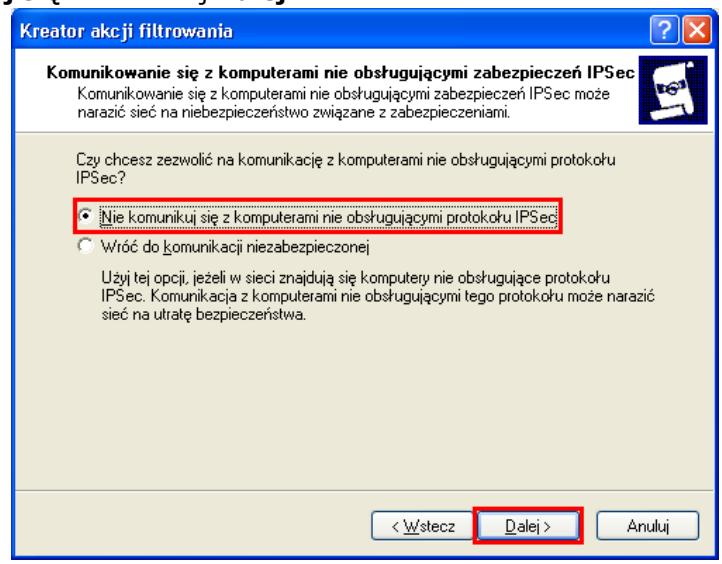
17. Wprowadź dowolną nazwę np. "ipsec out". Kliknij **Dalej**.



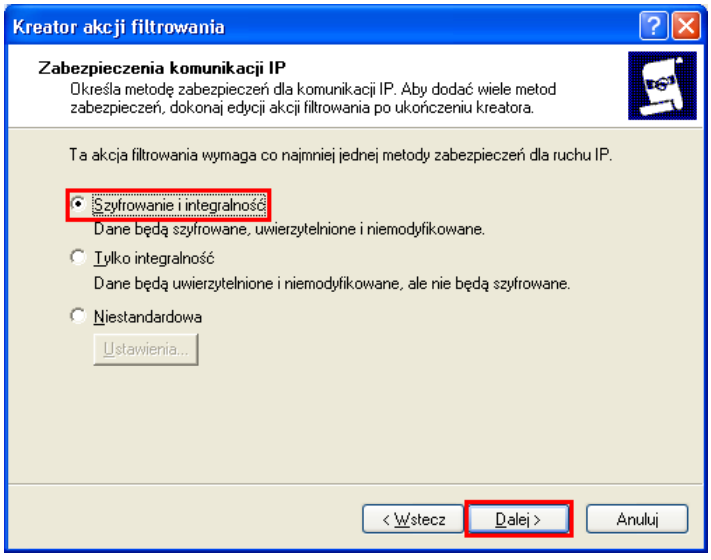
18. Wybierz **Negocjuj protokół zabezpieczeń**. Kliknij **Dalej**.



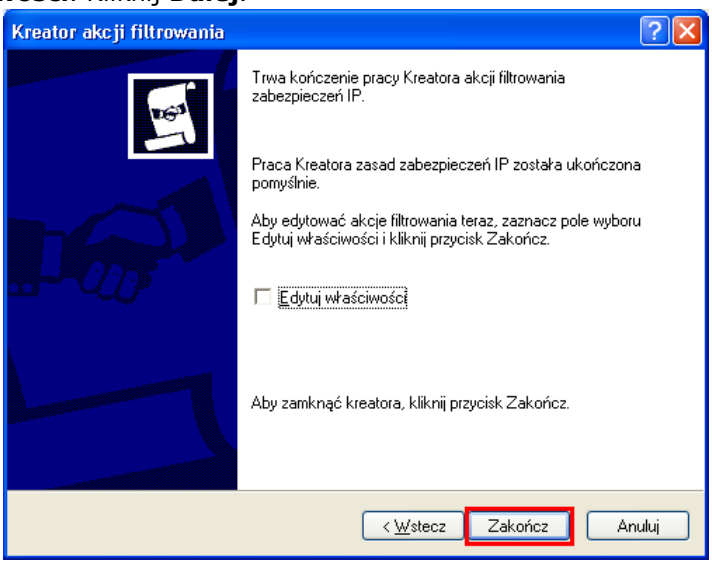
19. Wybierz **Nie komunikuj się z...** . Kliknij **Dalej**.



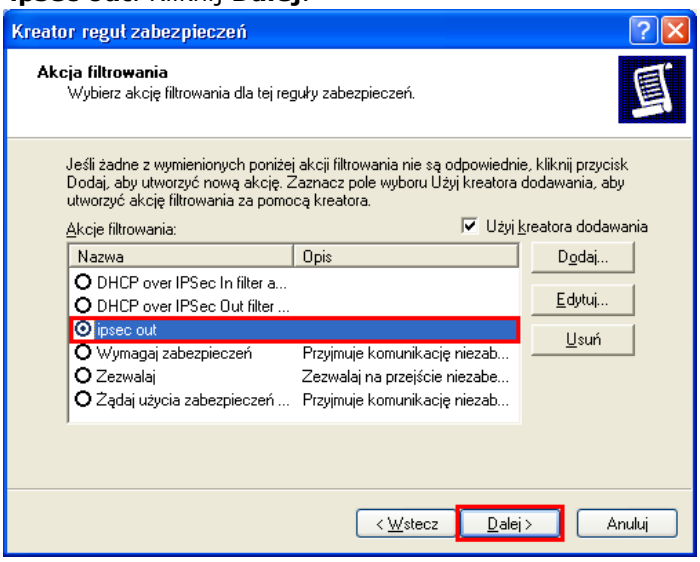
20. Wybierz **Szyfrowanie i integralność**. Kliknij **Dalej**.



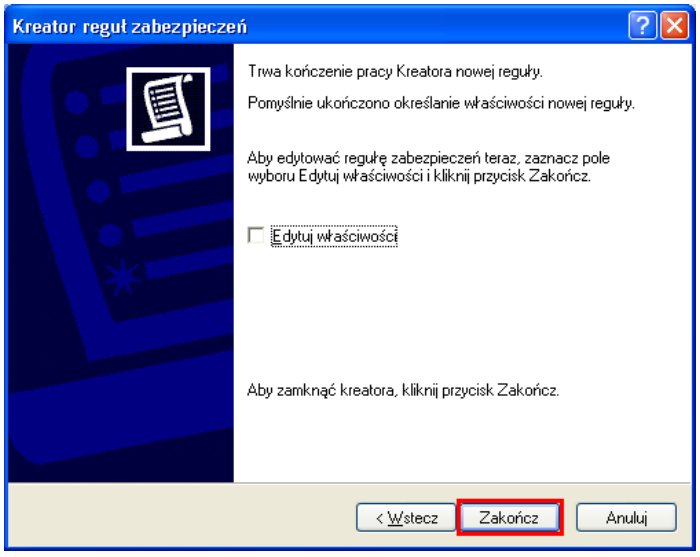
21. Odznacz **Edytuj właściwości**. Kliknij **Dalej**.



22. Wybierz akcję filtrowania **ipsec out**. Kliknij **Dalej**.

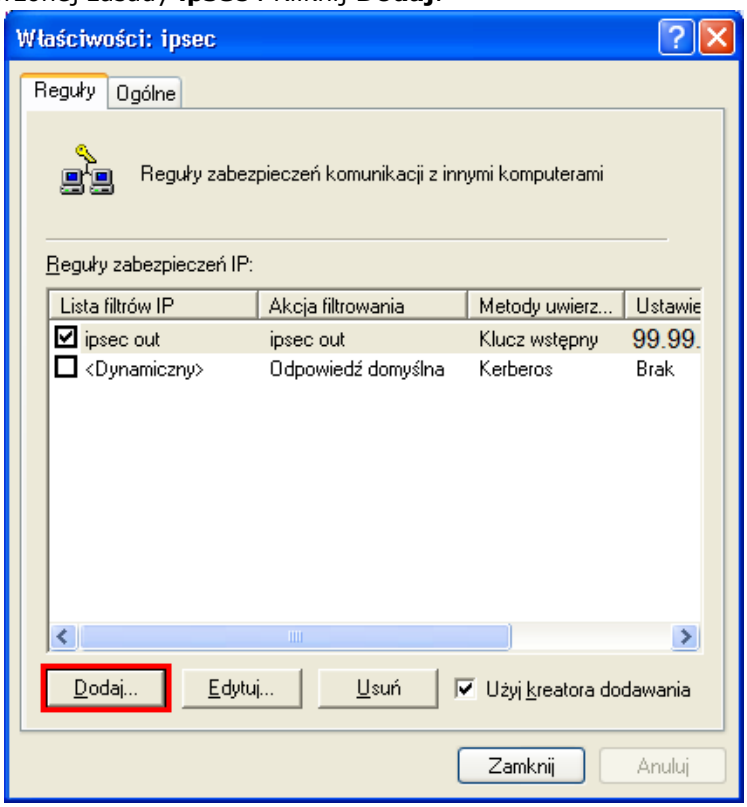


23. Odznacz **Edytuj właściwości**. Kliknij **Zakończ**.

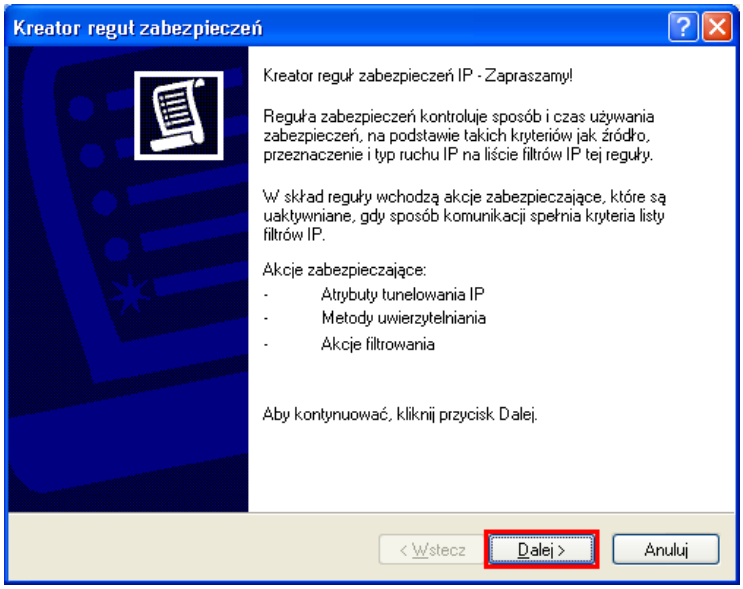


Dodanie reguły dla przychodzącego ruchu IPSec:

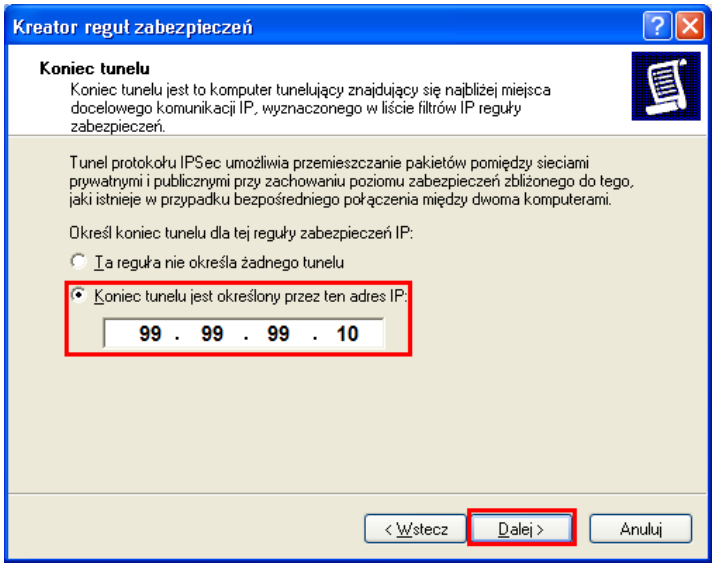
1. Otwórz właściwości stworzonej zasady **ipsec** . Kliknij **Dodaj**.



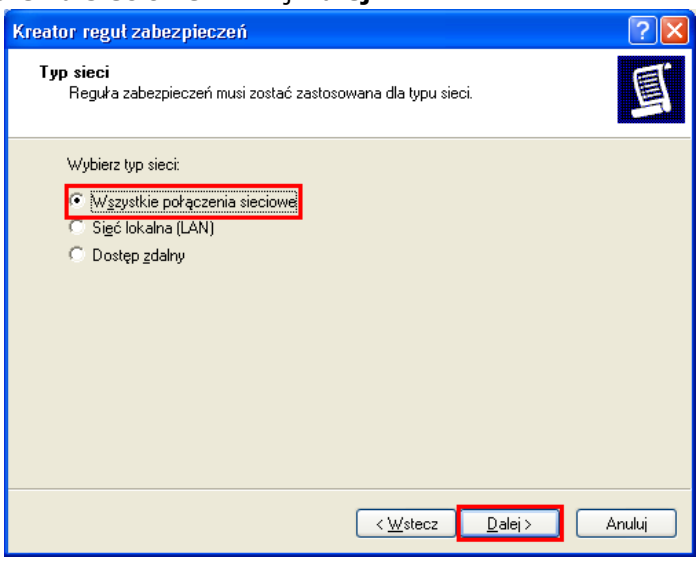
2. Pojawi się Kreator reguł zabezpieczeń IP. Kliknij **Dalej**.



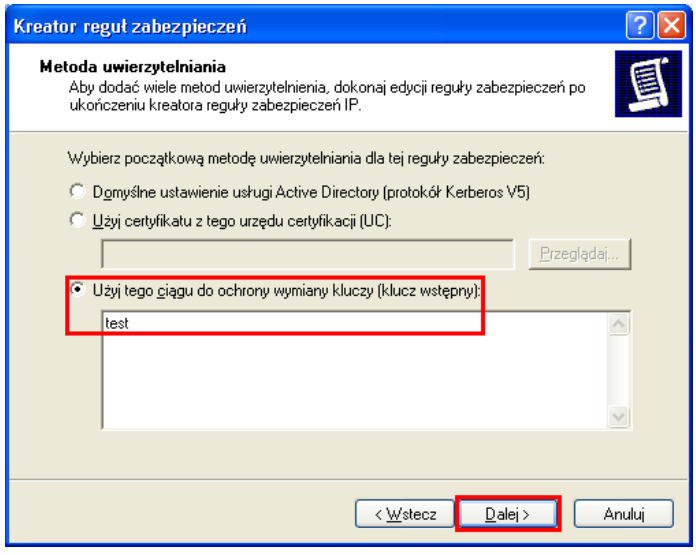
3. . Wybierz **Koniec tunelu...** i wprowadź końcowy IP. W przykładzie adres IP: 99.99.99.10.



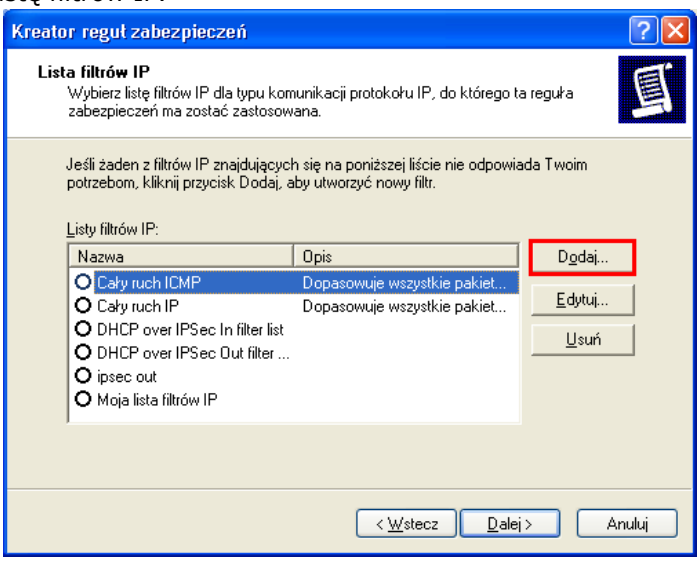
4. Wybierz **Wszystkie połączenia sieciowe**. Kliknij **Dalej**.



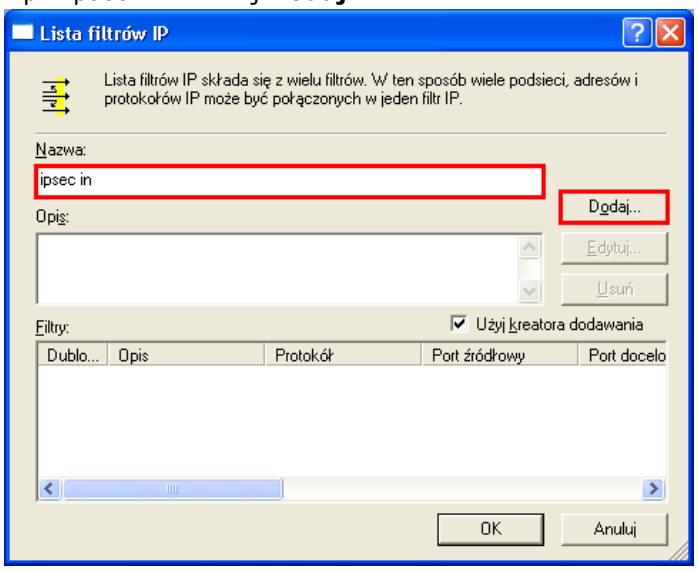
5. Wybierz **Użyj tego ciągu...** i wprowadź klucz. Kliknij **Dalej**.



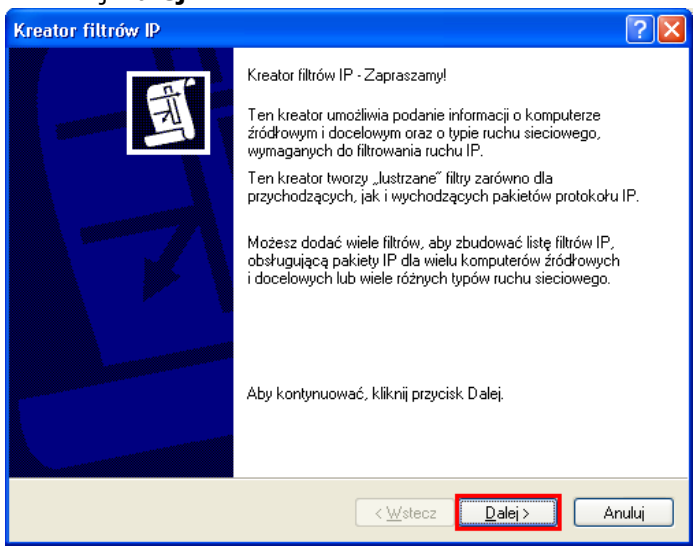
6. Kliknij **Dodaj** aby dodać Listę filtrów IP.



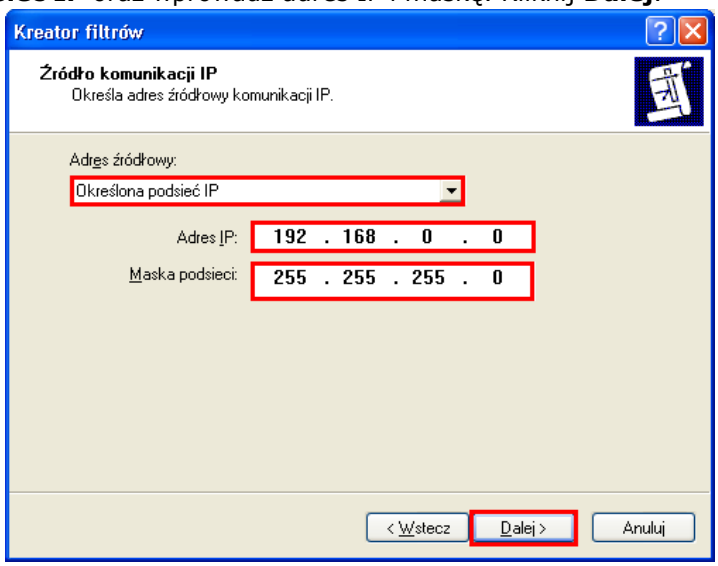
7. Wprowadź dowolną nazwę np. "ipsec in". Kliknij **Dodaj**.



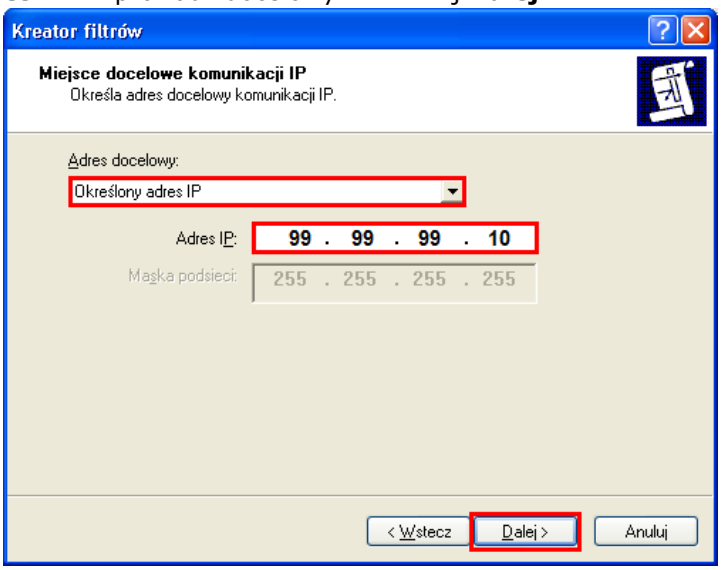
8. Pojawi się Kreator filtrów IP. Kliknij **Dalej**.



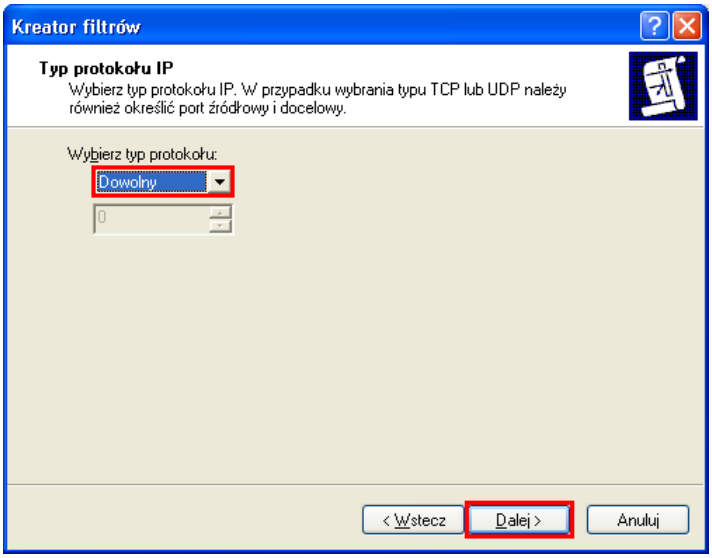
9. Wybierz **Określona podsieć IP** oraz wprowadź adres IP i maskę. Kliknij **Dalej**.



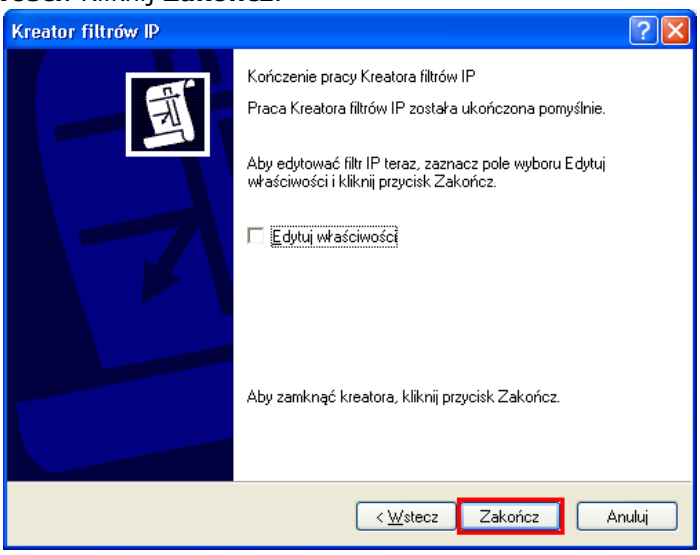
10. Wybierz **Określony adres IP** i wprowadź docelowy IP. Kliknij **Dalej**.



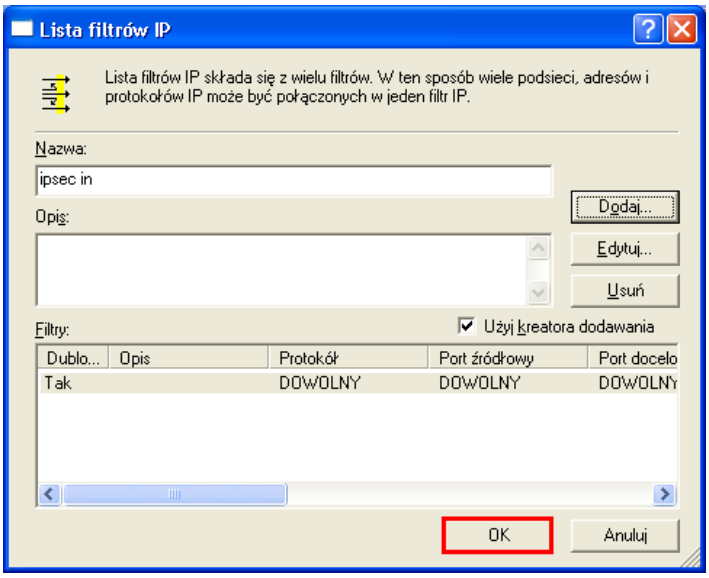
11. Wybierz **Dowolny** typ protokołu IP.



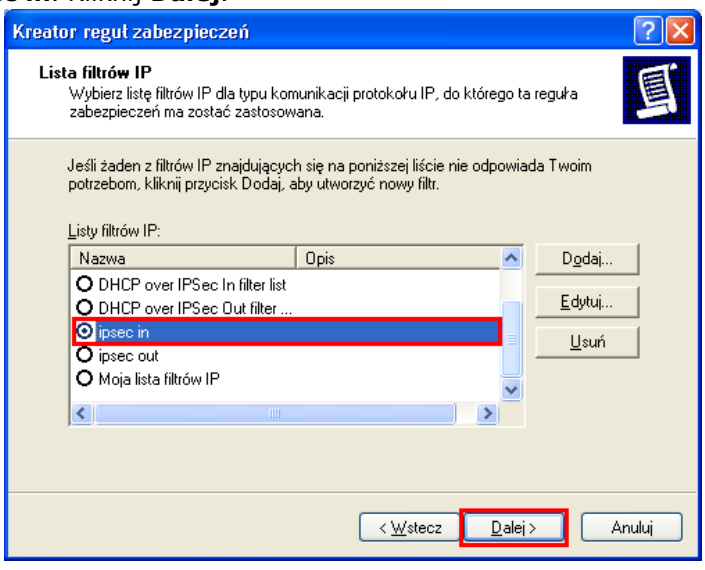
12. Odznacz **Edytuj właściwości**. Kliknij **Zakończ**.



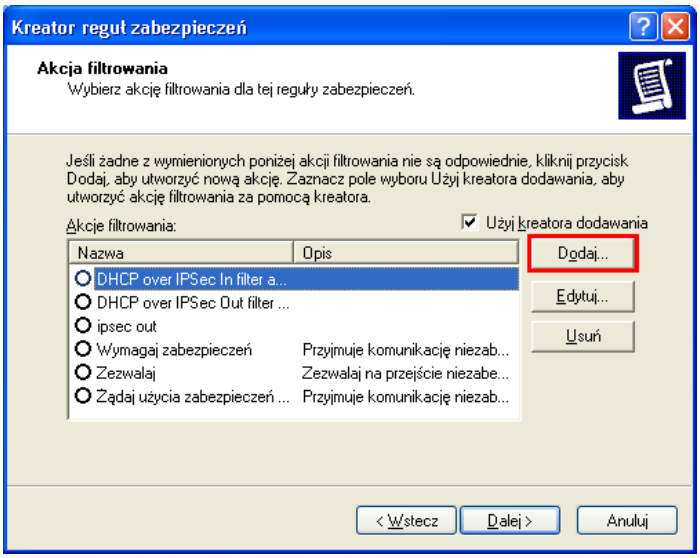
13. Kliknij **OK**.



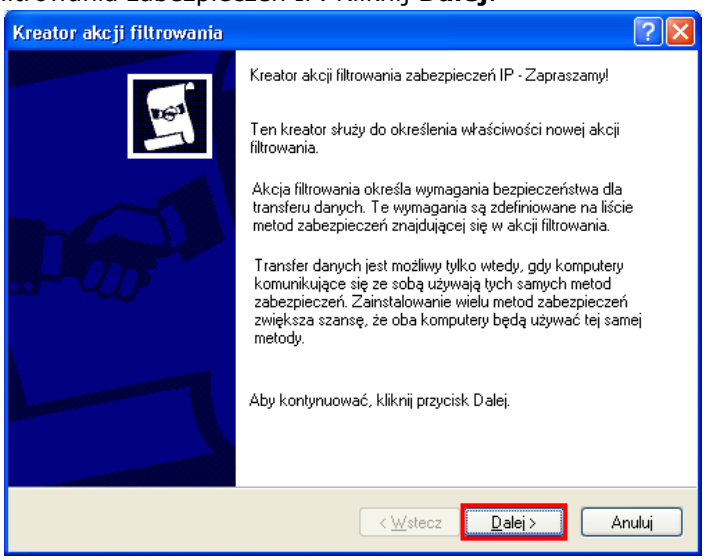
14. Wybierz listę filtrów **ipsec in**. Kliknij **Dalej**.



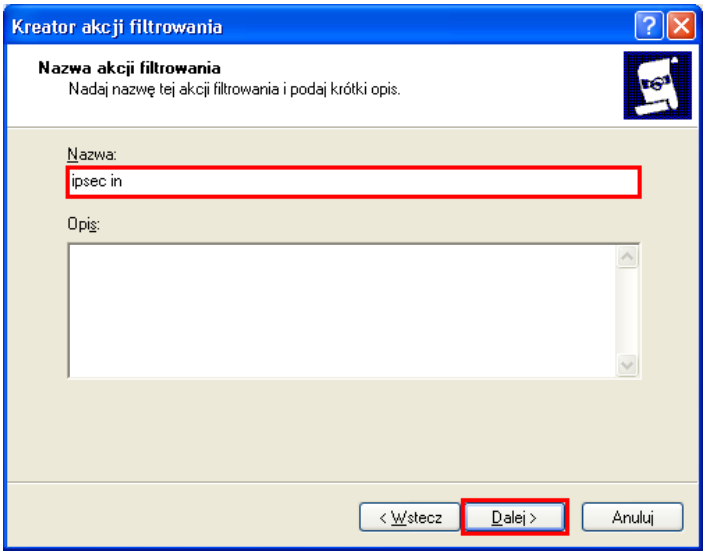
15. Kliknij **Dodaj**.



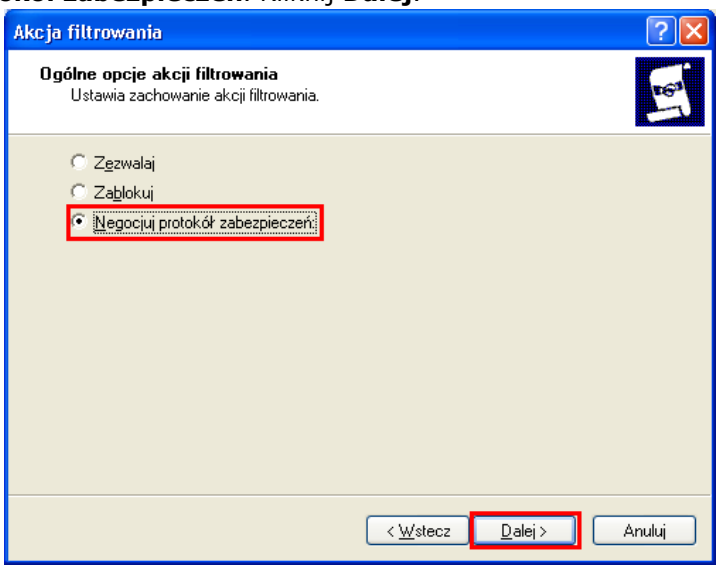
16. Pojawi się Kreator akcji filtrowania zabezpieczeń IP. Kliknij **Dalej**.



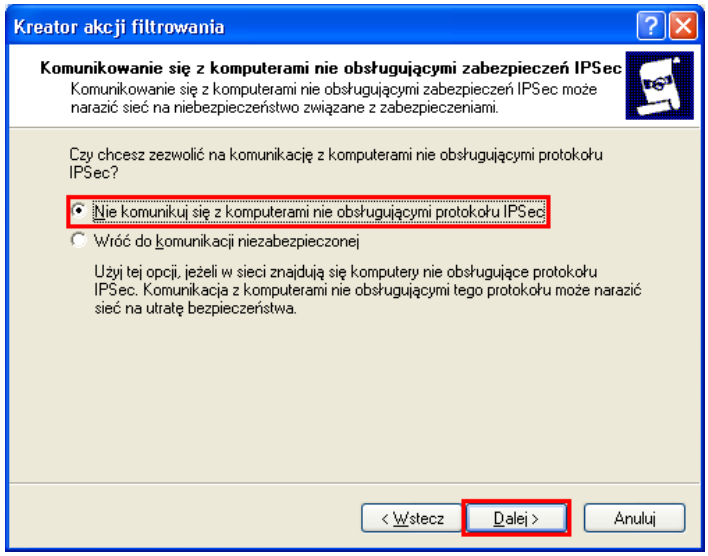
17. Wprowadź dowolną nazwę np. "ipsec in". Kliknij **Dalej**.



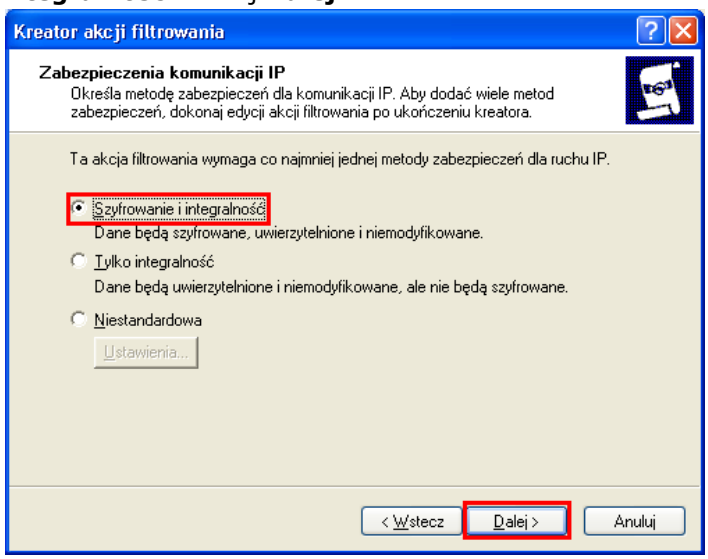
18. Wybierz **Negocjuj protokół zabezpieczeń**. Kliknij **Dalej**.



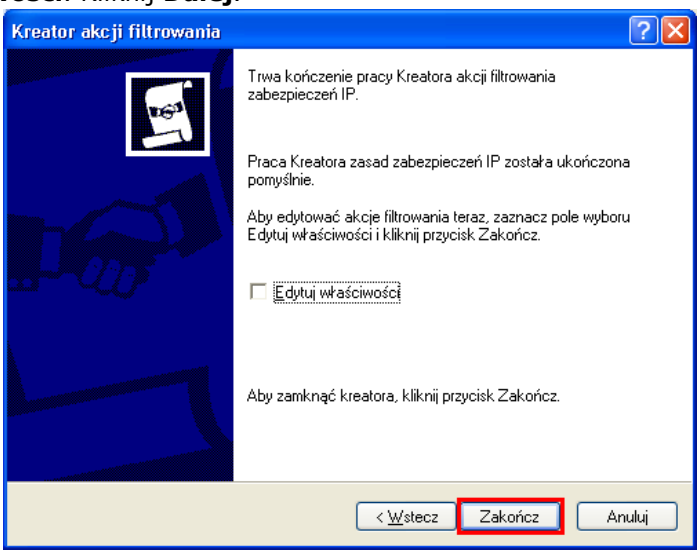
19. Wybierz **Nie komunikuj się z...** . Kliknij **Dalej**.



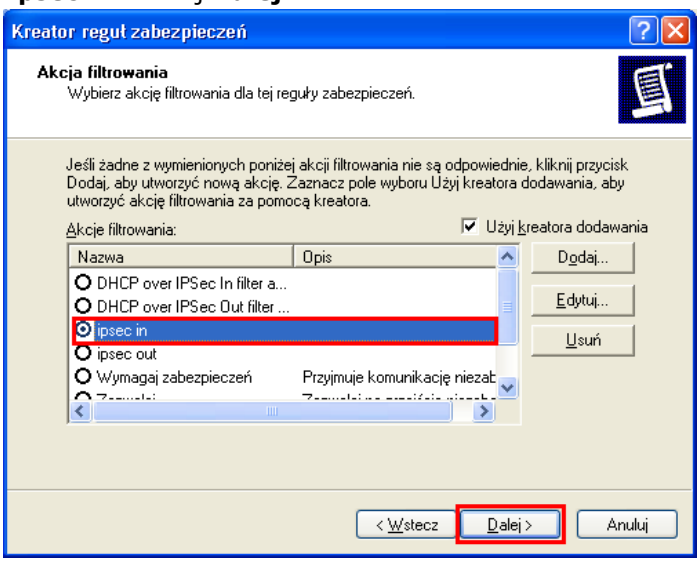
20. Wybierz **Szyfrowanie i integralność**. Kliknij **Dalej**.



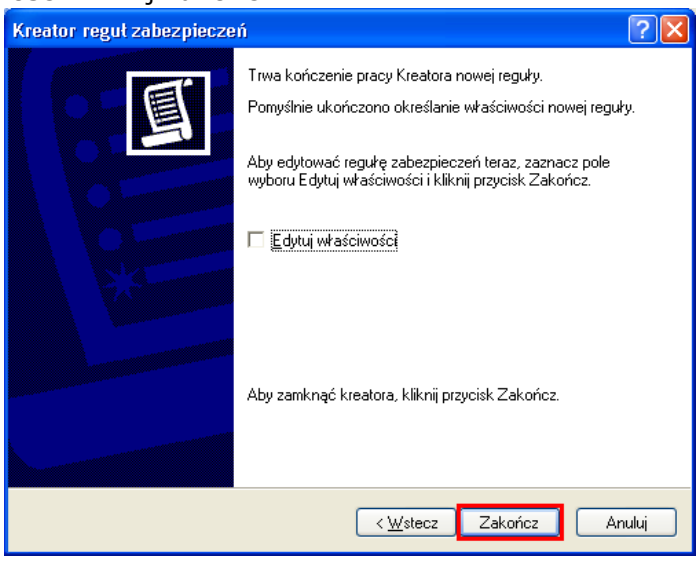
21. Odznacz **Edytuj właściwości**. Kliknij **Dalej**.



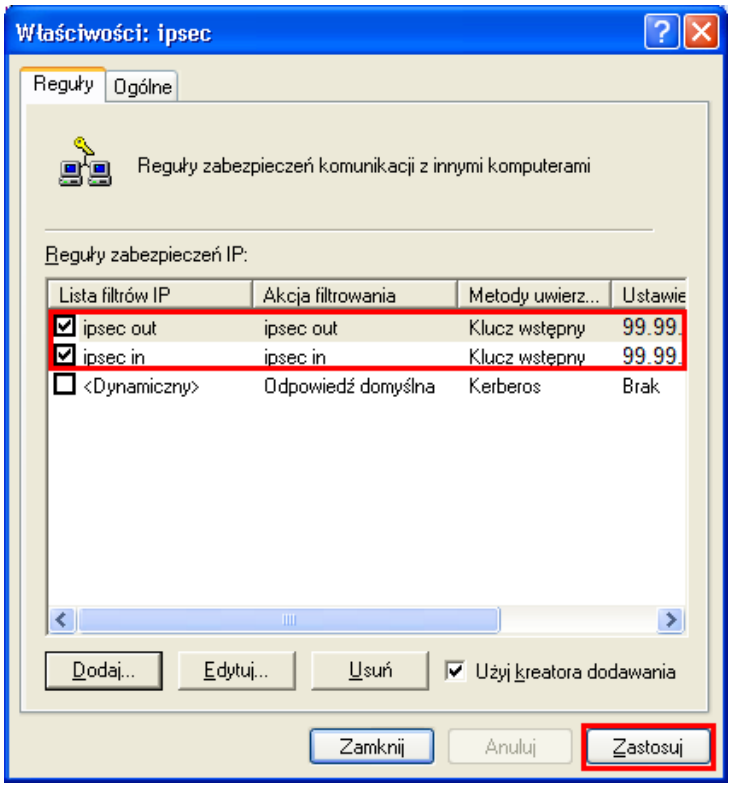
22. Wybierz akcję filtrowania **ipsec in**. Kliknij **Dalej**.



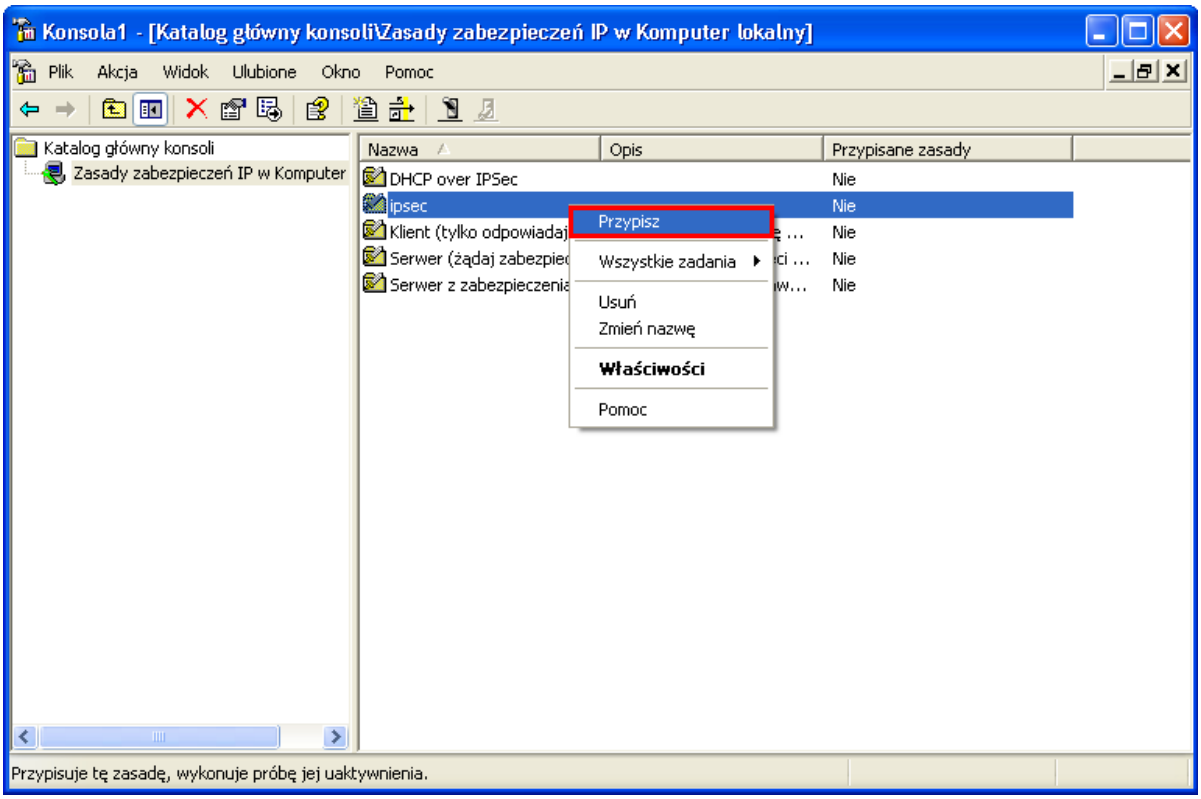
23. Odznacz **Edytuj właściwości**. Kliknij **Zakończ**.



W powyższych krokach stworzyłeś dwie reguły. Zaznacz obie reguły. Kliknij Zastosuj.



Wybierz **Przypisz** dla ipsec.



3. Zainicjowanie połączenia

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.

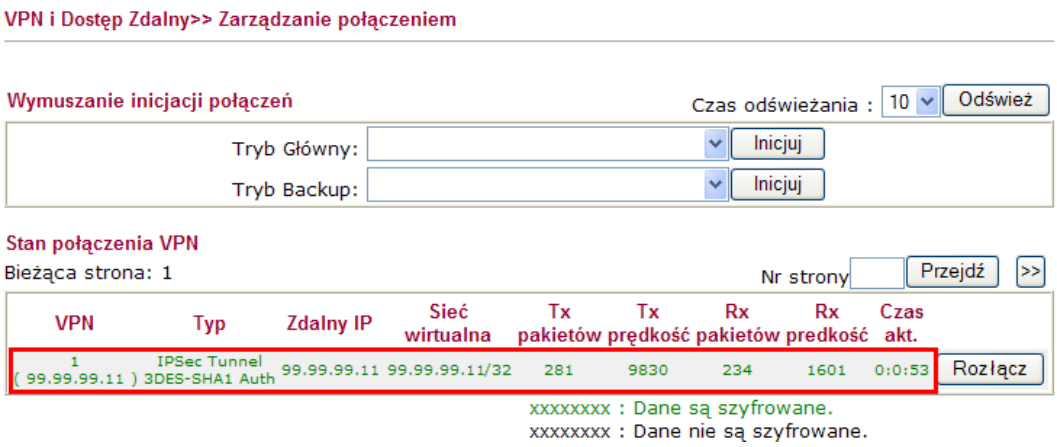
```
C:\>ping 192.168.0.1

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