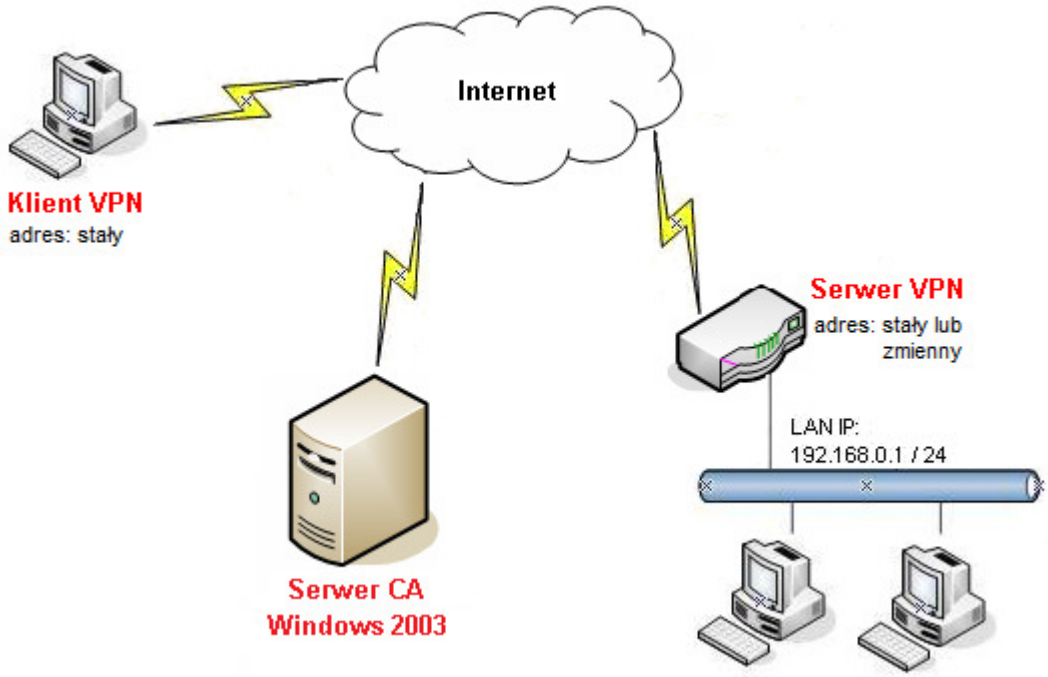
Procedura konfiguracji została oparta na poniższym przykładzie.



Główne założenia:

- typ tunelu: Host-LAN
- protokół VPN: IPSec (tryb główny)
- szyfrowanie: 3DES
- integralność: SHA1
- autentykacja: certyfikaty X.509
- Adres IP Serwera VPN: statyczny. W przykładzie 99.99.99.10
- Adres IP Klienta VPN : statyczny. W przykładzie 99.99.99.11
- Adres IP Serwera CA 99.99.99.100

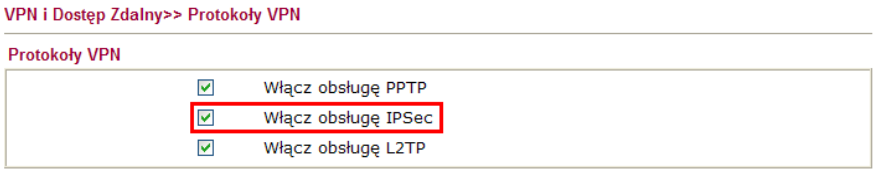
Uwagi

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 serwera VPN

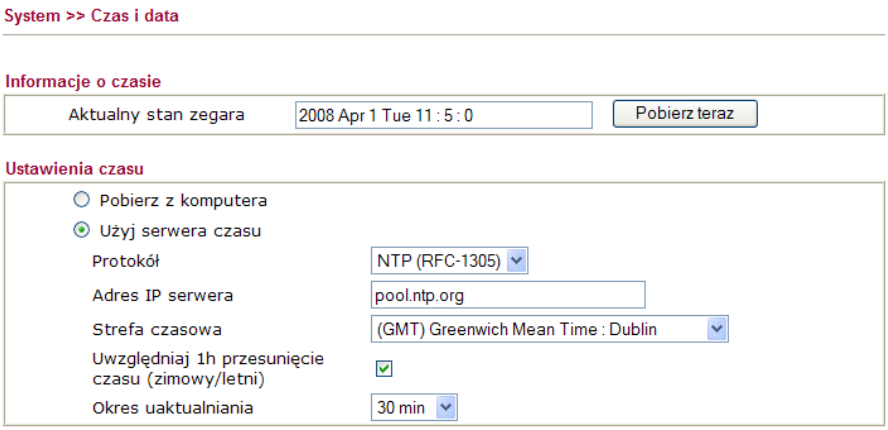
1.1. Włączenie obsługi IPSec

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



1.2. Ustawienie czasu

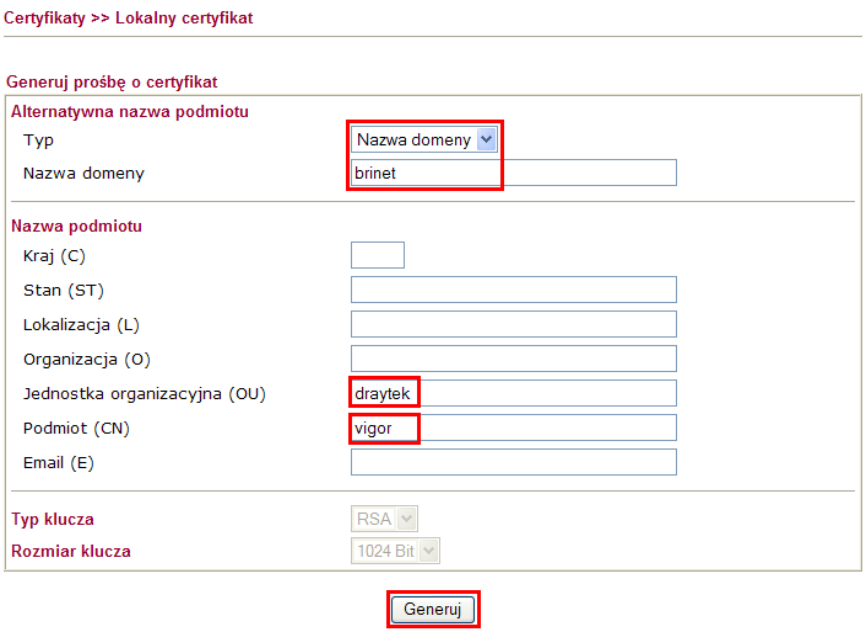
Ustaw aktualny czas na Vigorze, gdyż będzie on niezbędny do poprawnej pracy z certyfikatami X.509.



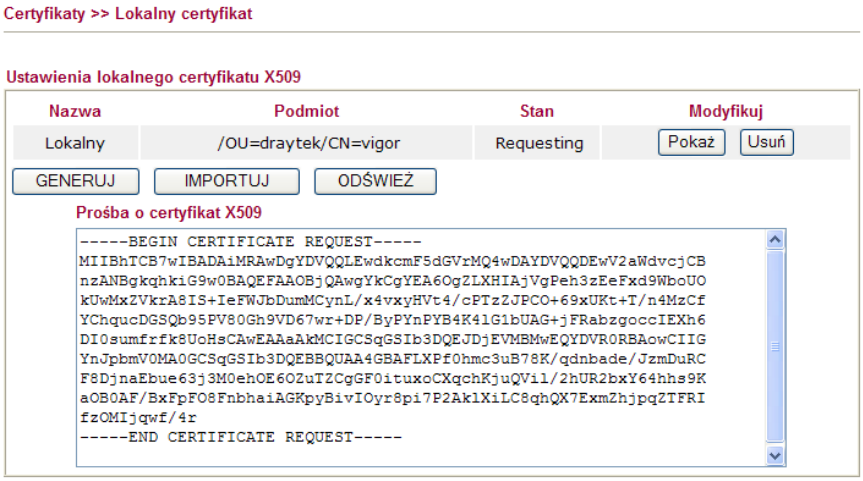
1.3. Lokalny certyfikat (żądanie certyfikatu z serwera CA)

Krok 1: Przejdź do zakładki **Certyfikaty>>Lokalny** certyfikat. Następnie kliknij przycisk **GENERUJ**.

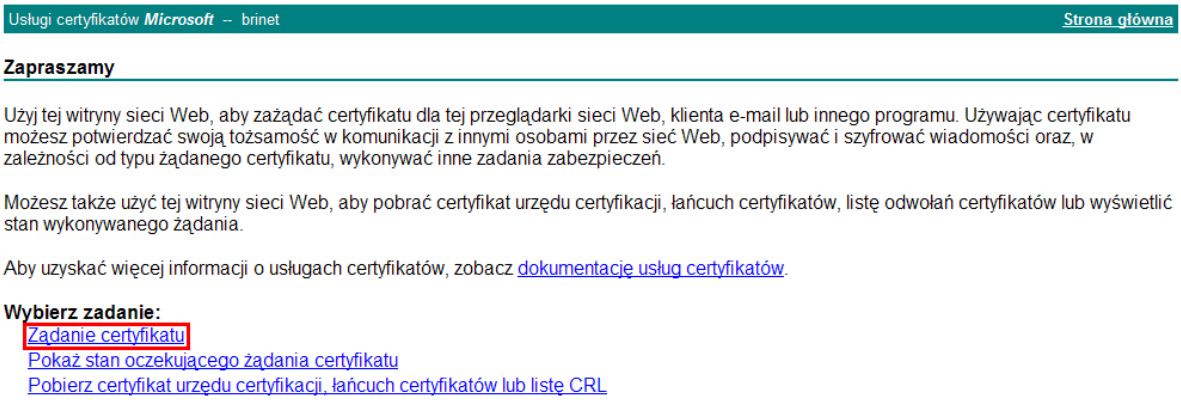
Krok 2: Wpisz odpowiednie dane w polach **Alternatywna nazwa podmiotu** i **Nazwa podmiotu**. W przykładzie użyto wartości pokazanych na następnym rysunku. Po wprowadzeniu danych kliknij przycisk **Generuj**.



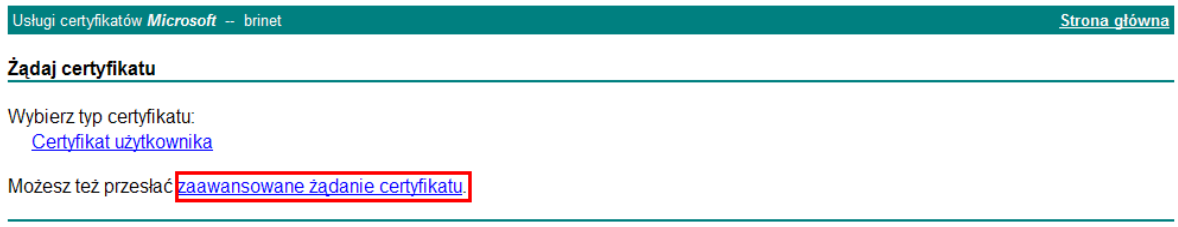
Krok 3: Wygenerowany tekst będzie potrzebny w kroku 7.



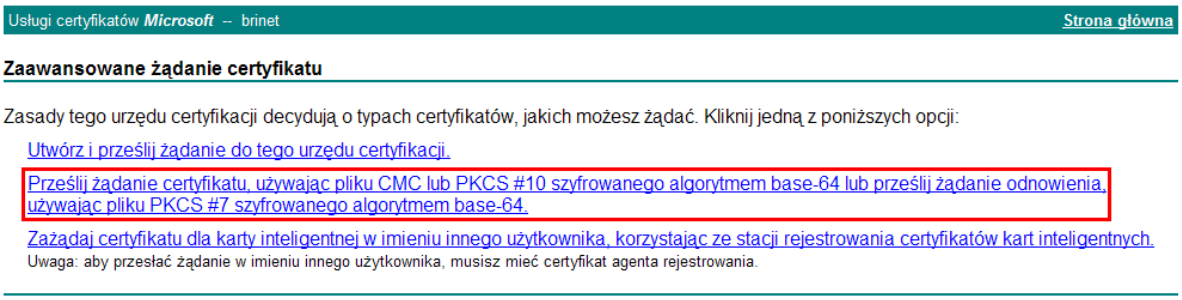
Krok 4. Połącz się z serwerem CA (w przykładzie http://99.99.99.100/certsrv). W przykładzie wykorzystano Windows Server 2003 RC2 jako serwer CA. Po zalogowaniu wybierz **Żądanie certyfikatu**.



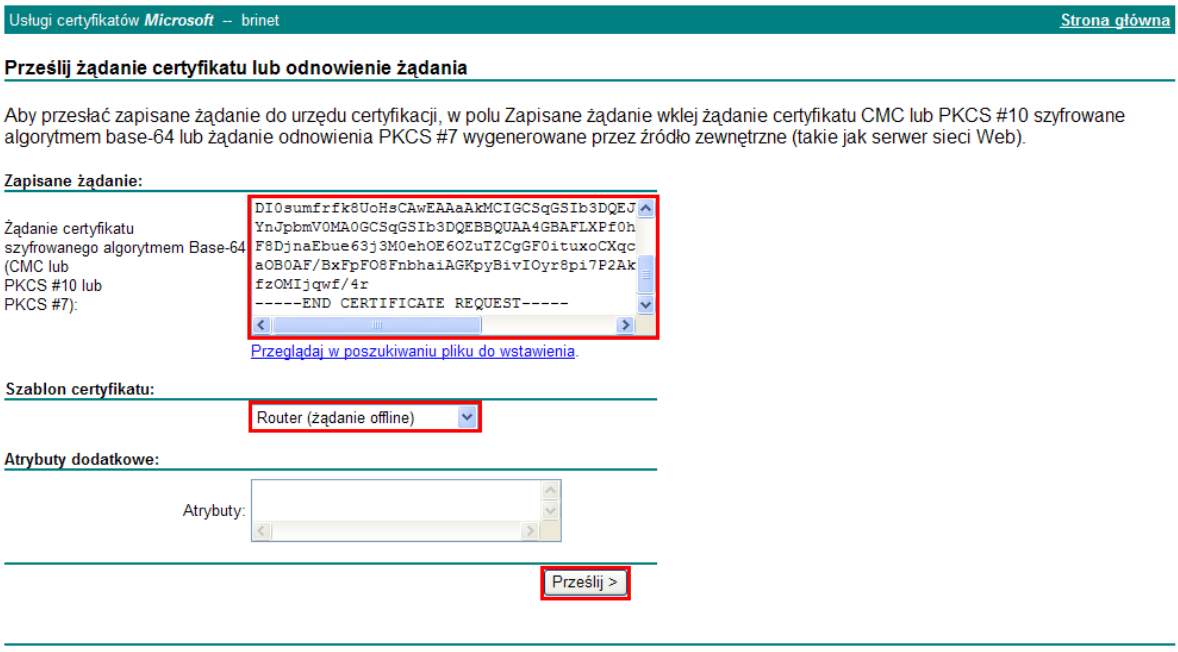
Krok 5: Wybierz **zaawansowane żądanie certyfikatu**.



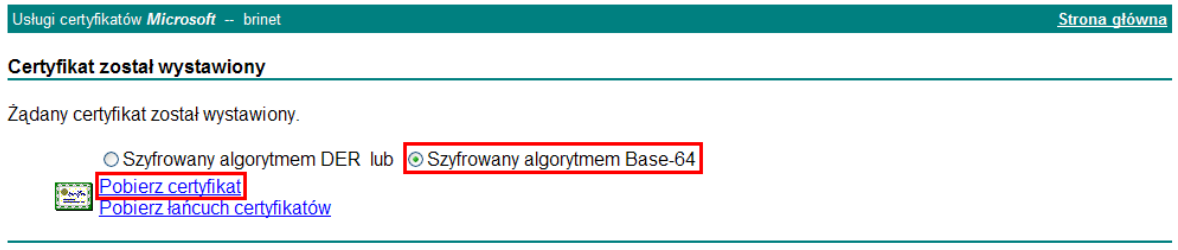
Krok 6: Wybierz drugą opcję – **Prześlij żądanie certyfikatu, używając …**



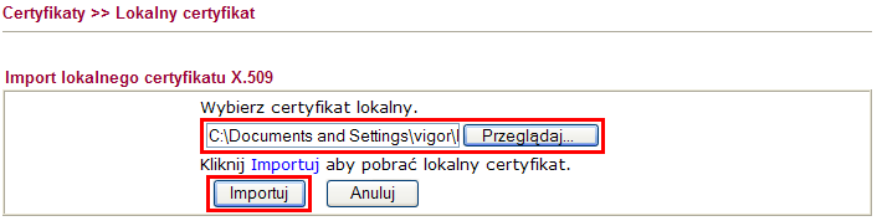
Krok 7. Wklej tekst wygenerowany w kroku 3. Wybierz opcję **Router (żądanie offline)** jako Szablon certyfiaktu. Następnie kliknij przycisk **Prześlij>**.



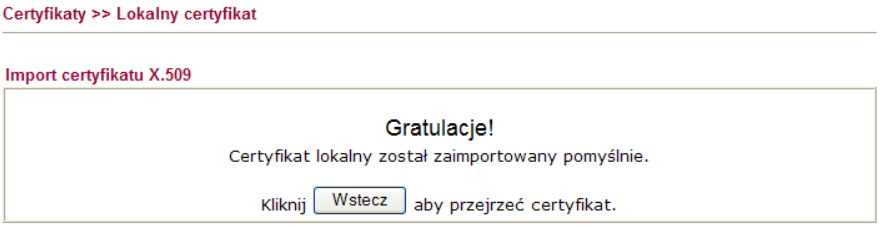
Krok 8: Pobierz certyfikat szyfrowany algorytmem Base-64



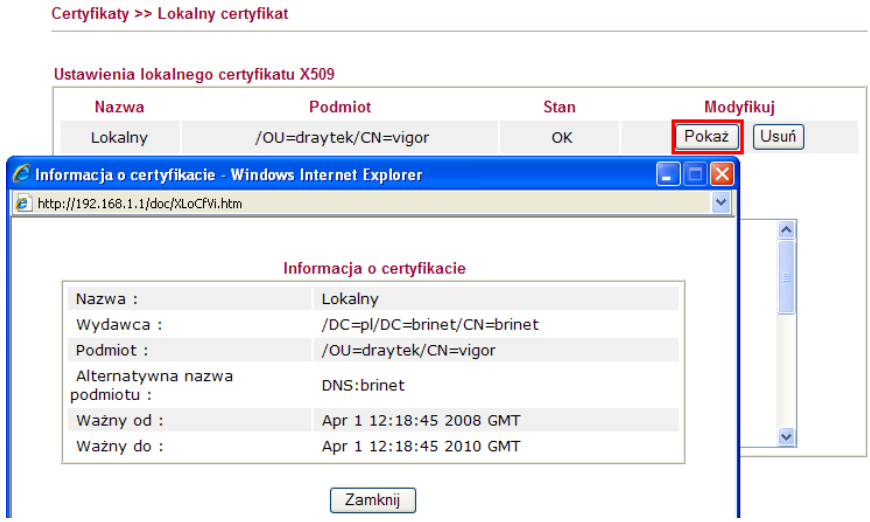
Krok 9: Zaimportuj lokalny certyfikat do Vigora – wybierz ścieżkę do certyfikatu i kliknij przycisk **Importuj**.



Krok 10: Pomyślna próba importu certyfikatu.

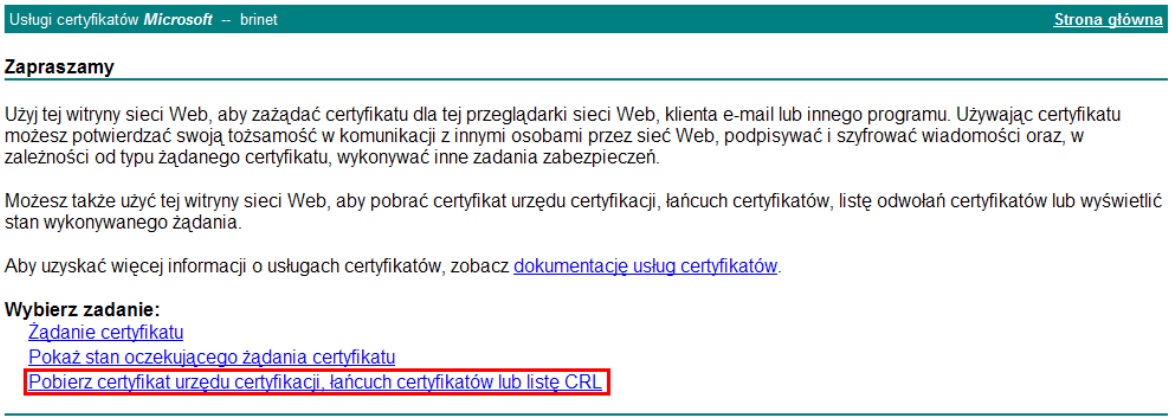


Aby zobaczyć certyfikat kliknij przycisk **Pokaż**.

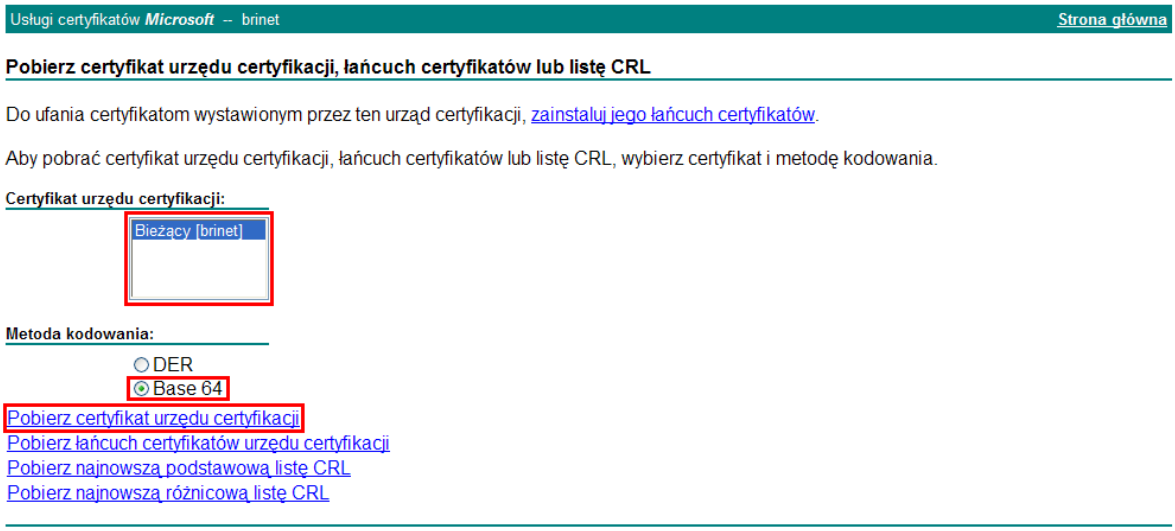


1.4. Certyfikat zaufanego CA

Krok 1: Połącz się z serwerem CA (w przykładzie http://99.99.99.100/certsrv). Po zalogowaniu wybierz **Pobierz certyfikat urzędu certyfikacji, łańcuch certyfikatów lub listę CRL**.

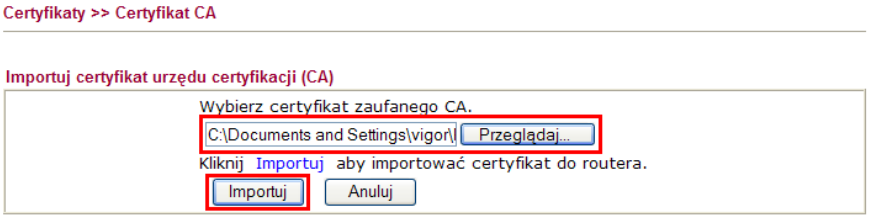


Krok 2: Wybierz odpowiedni certyfikat urzędu certyfikacji (w przykładzie brinet) oraz **Base 64** jako Metodę kodowania. Następnie wybierz opcję **Pobierz certyfikat urzędu certyfikacji** i zapisz na dysku.

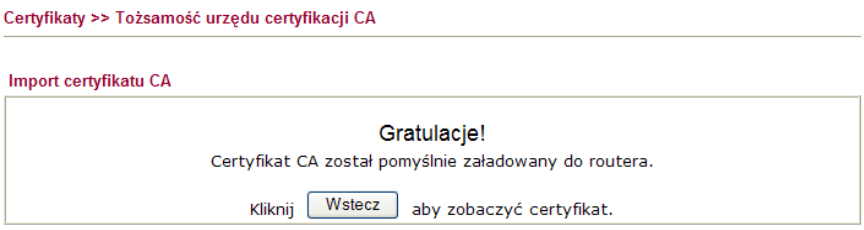


Krok 3: Przejdź do zakładki **Certyfikaty>>Certyfikat zaufanego CA**. Następnie kliknij przycisk **IMPORTUJ**.

Krok 4: Wskaż ścieżkę z certyfikatem zaufanego CA. Następnie kliknij przycisk **Importuj**.

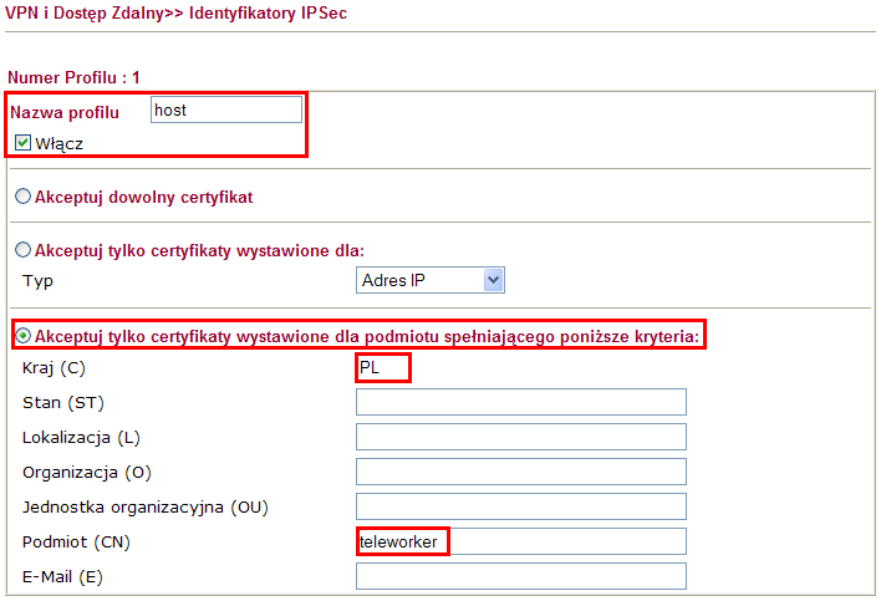


Krok 11: Pomyślna próba importu certyfikatu.



1.5. Identyfikator IPSec

Przejdź do zakładki **VPN i Dostęp Zdalny>>Identyfikatory IPSec**. Stwórz odpowiedni profil (w przykładzie użyto profilu nr 1). W przykładzie użyto wartości pokazanych na następnym rysunku.

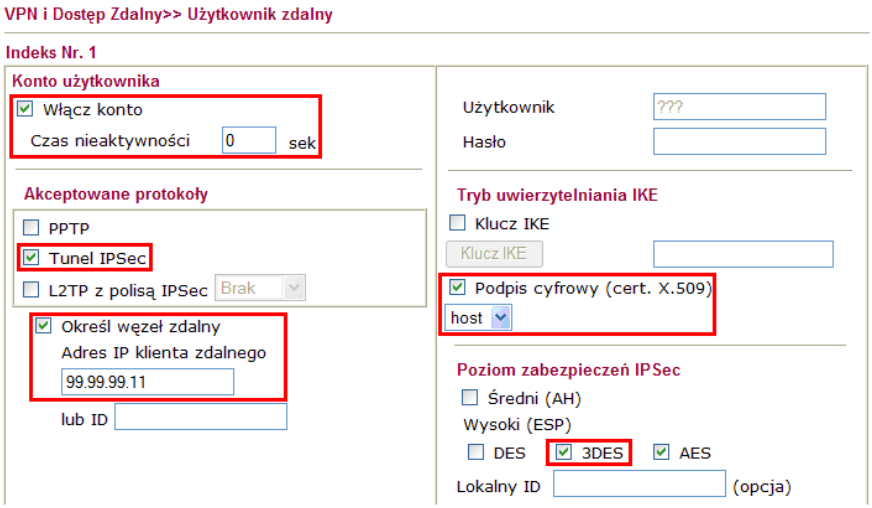


1.6. Profil Host-LAN

Przejdź do zakładki **VPN i Dostęp Zdalny>>Połączenia Host-LAN**. Stwórz odpowiednie konto do obsługi tunelu (w przykładzie użyto konta nr 1) i wpisz odpowiednie dane.

Konfiguracja zgodna z założeniami przykładu:

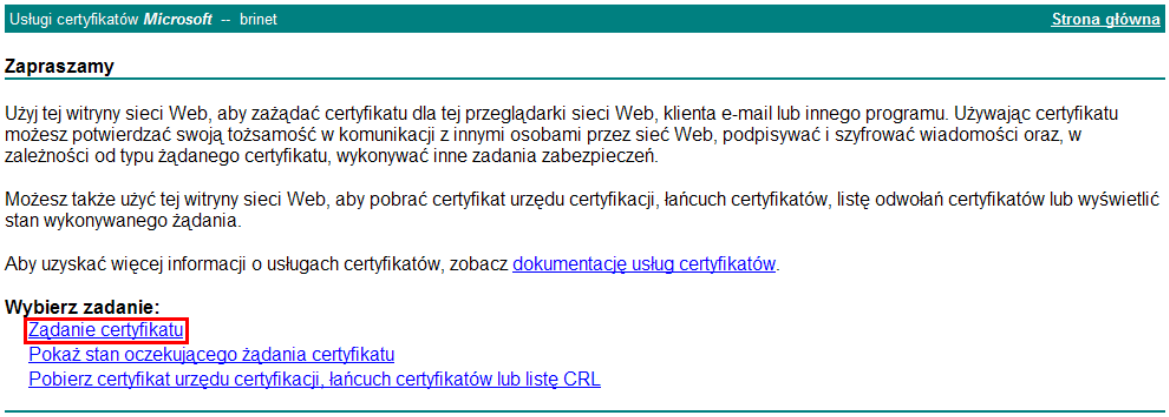
- zaznacz **Włącz konto**
- ustaw **czas nieaktywności 0**, gdy połączenie ma być aktywne cały czas. Domyślnie jest tam wartość 300 oznaczająca rozłączenie tunelu przez Vigor po 5 minutach.
- jako akceptowany protokół zaznacz **Tunel IPSec**
- zaznacz **Określ węzeł zdalny** i wpisz odpowiedni adres. W przykładzie użyto 99.99.99.11.
- zaznacz **Podpis cyfrowy (cert. X.509)** i wybierz stworzony wcześniej profil identyfikatora.
- zaznacz odpowiedni **Poziom zabezpieczeń IPSec**. W przykładzie użyto metody 3DES.



2. Konfiguracja klienta VPN (DrayTek Smart VPN Client)

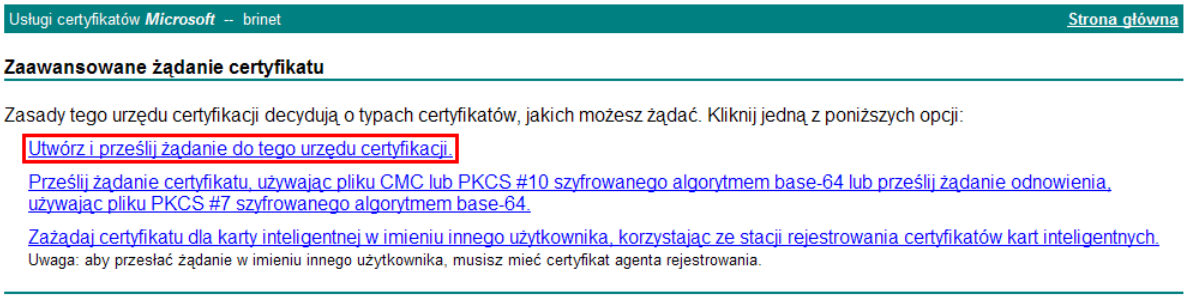
2.1 Zastosowanie certyfikatu z serwera CA do PC

Krok 1: Połącz się z serwerem CA (w przykładzie http://99.99.99.100/certsrv). Po zalogowaniu wybierz **Żądanie certyfikatu**.

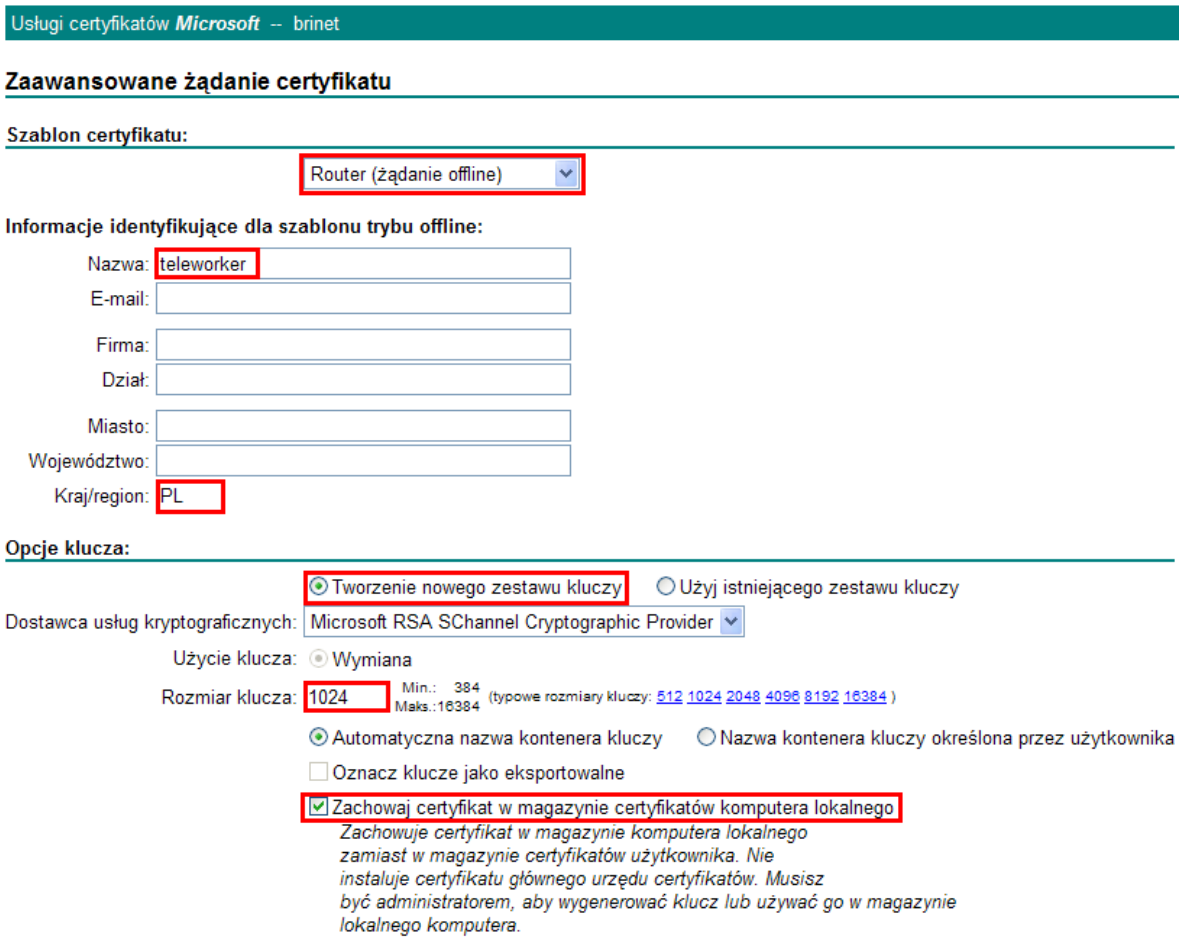


Krok 2: Wybierz **zaawansowane żądanie certyfikatu**.

Krok 3: Wybierz **Utwórz i prześlij żądanie do tego urzędu certyfikacji**.



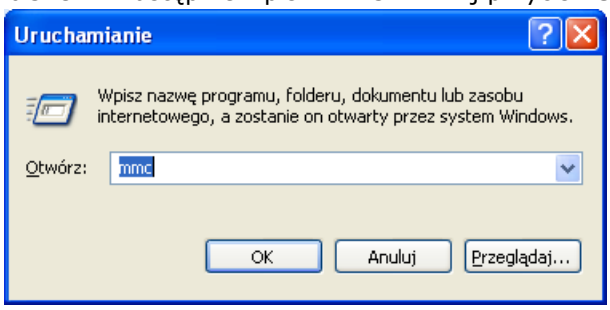
Krok 4: Wybierz opcję **Router (żądanie offline)** jako Szablon certyfiaktu. Wypełnij odpowiednie informacje identyfikujące dla szablonu w trybie offline. W opcjach kluczy wybierz **Tworzenie nowego zestawu kluczy**, Rozmiar klucza **1024** oraz **Zachowaj certyfikat w magazynie certyfikatów komputera lokalnego**. W przykładzie użyto wartości pokazanych na następnym rysunku.



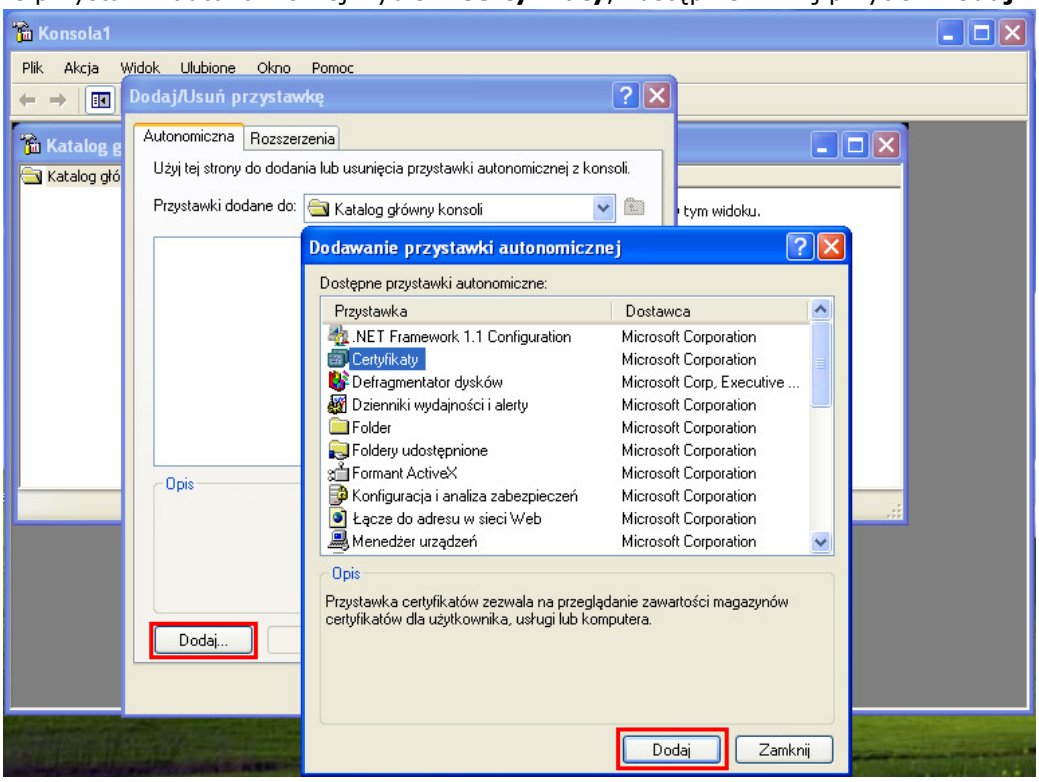
Krok 5: Zainstaluj wystawiony certyfikat.

Krok 6: Pomyślna próba zainstalowania certyfikatu na PC.

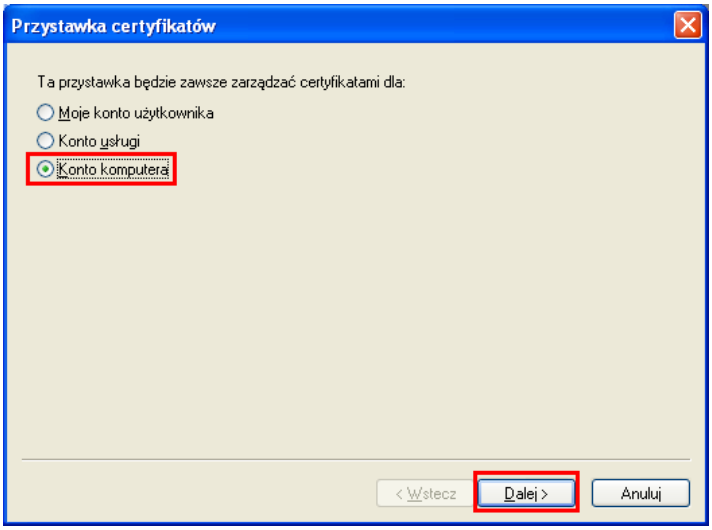
Krok 7: Z Menu start wybierz **Uruchom**. Następnie wpisz **mmc** i kliknij przycisk **OK**.



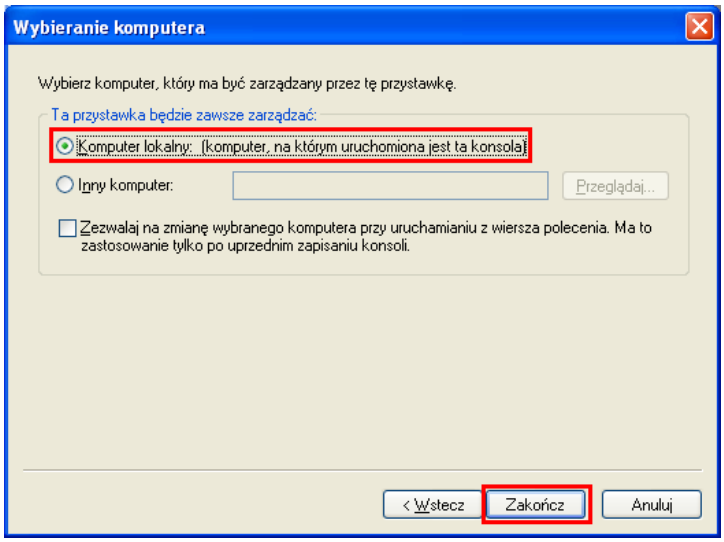
Krok 8: Otworzy się Konsola1. Wybierz **Plik->Dodaj/Usuń przystawkę**, następnie kliknij przycisk **Dodaj**. W oknie Dodawanie przystawki autonomicznej wybierz **Certyfikaty**, następnie kliknij przycisk **Dodaj**.



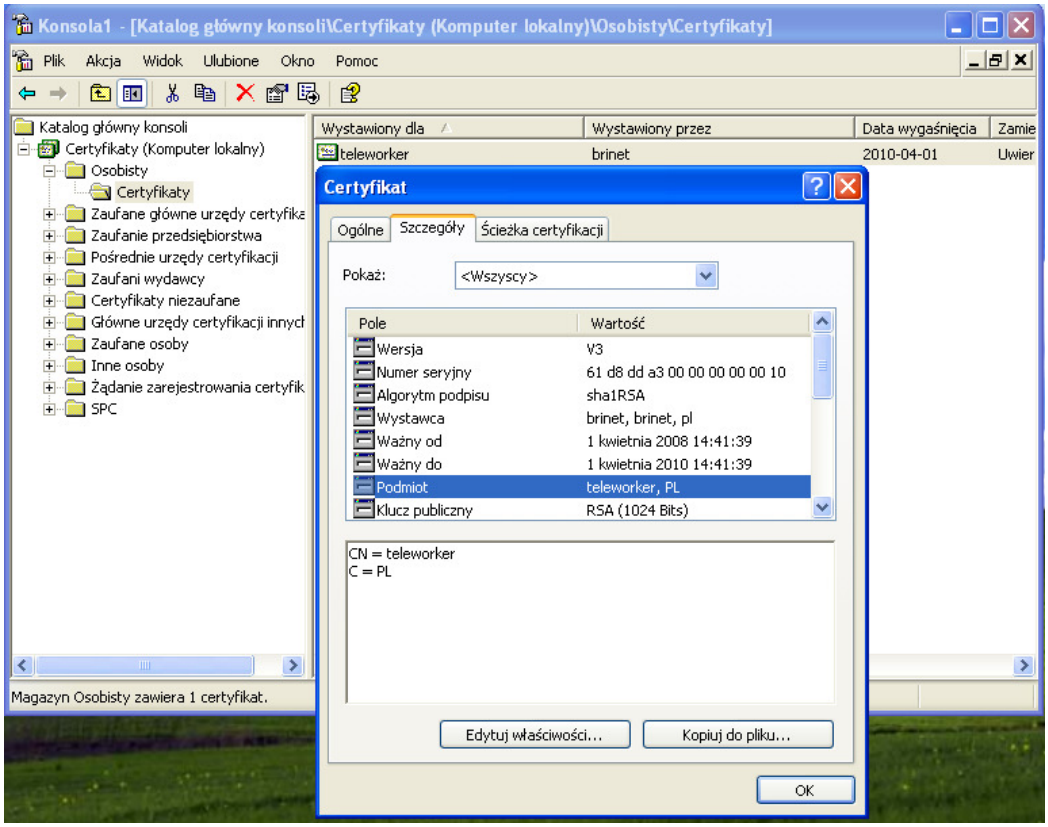
Krok 9: Wybierz **Konto komputera**. Następnie kliknij przycisk **Dalej>.**



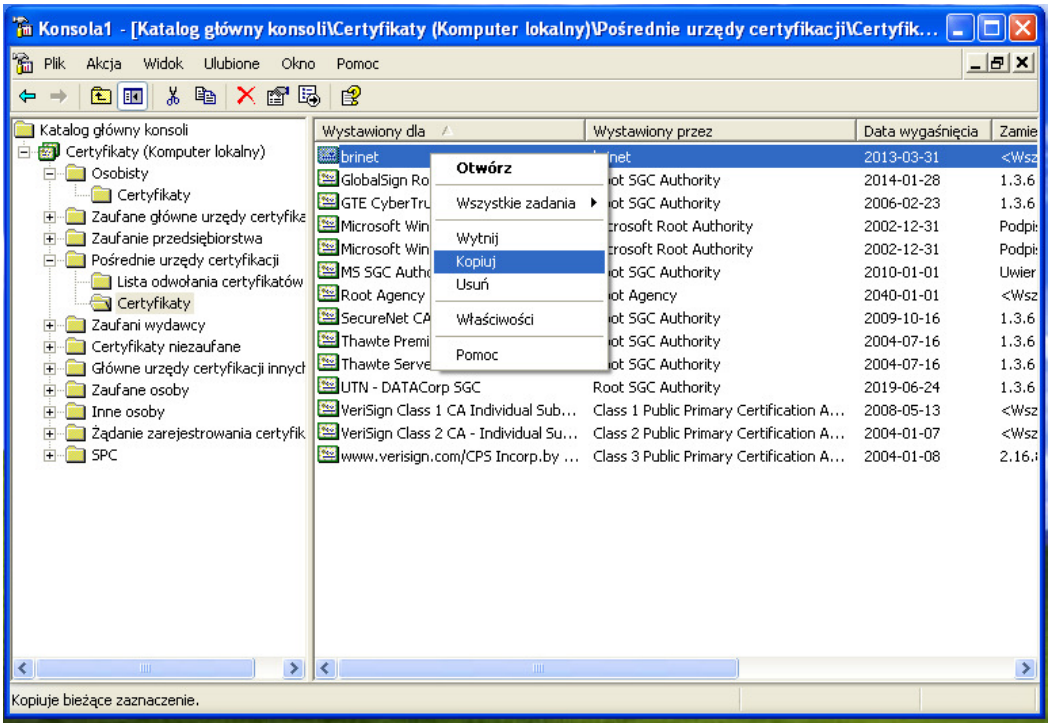
Krok 10: Wybierz **Komputer lokalny**. Następnie kliknij przycisk **Zakończ**.



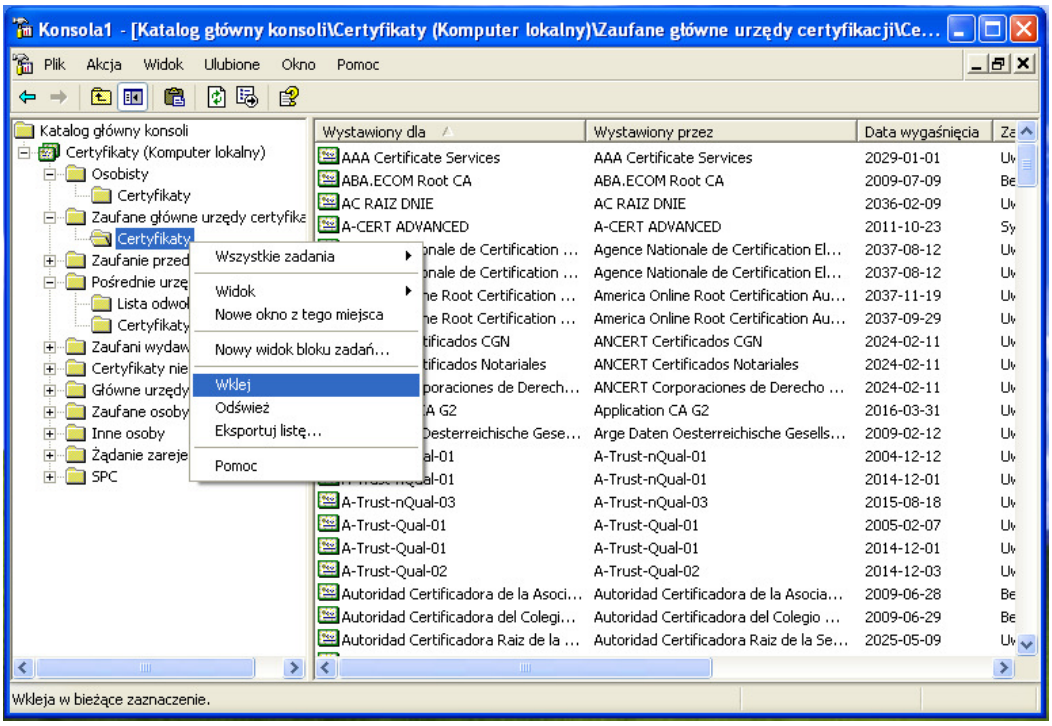
Krok 11: Zainstalowany certyfikat znajduje się w **Certyfikaty(komputer lokalny)>>Osobisty>>Certyfikaty**



Krok 12: Przejdź do **Certyfikaty(komputer lokalny)>>Pośrednie urzędy certyfikacji>>Certyfikaty** i **Kopiuj** odpowiedni certyfikat CA (w przykładzie wykorzystywano certyfikat brinet).

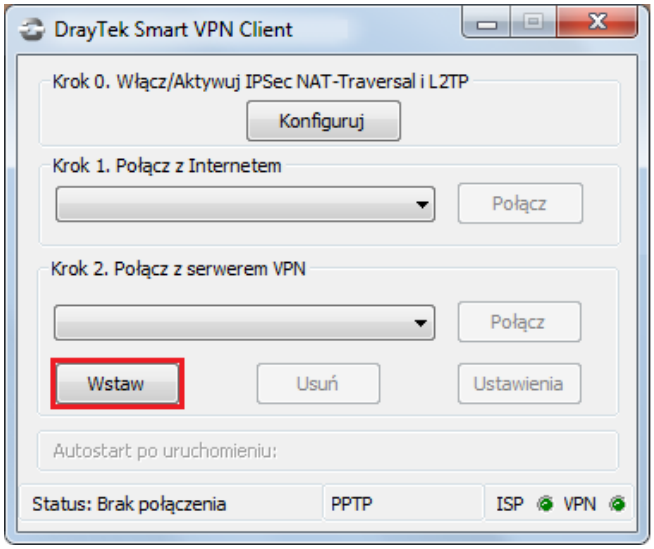


Krok 13: Przejdź do **Certyfikaty(komputer lokalny)>>Zaufane główne urzędy certyfikacji>>Certyfikaty** i **Wklej** odpowiedni certyfikat CA (w przykładzie wykorzystywano certyfikat brinet).



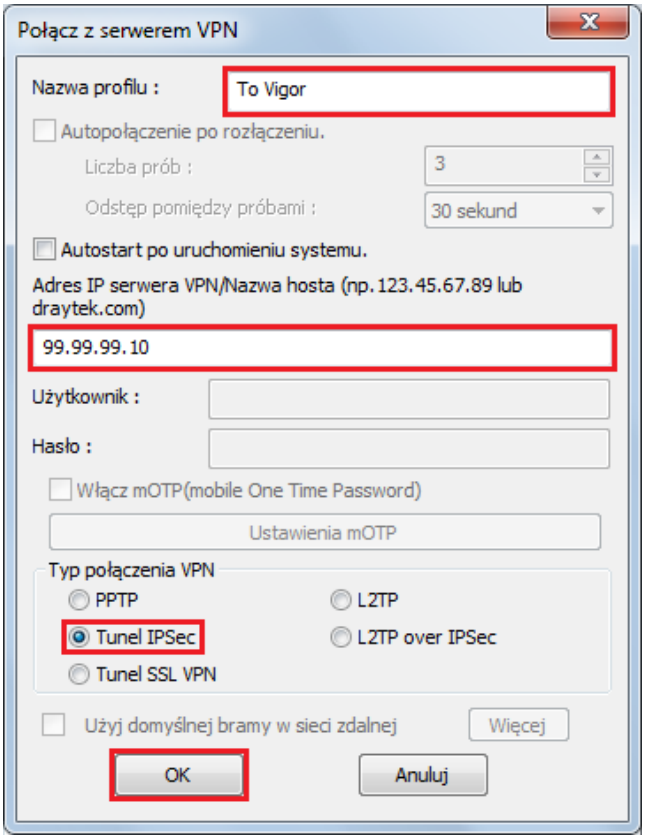
2.2 Konfiguracja DrayTek Smart VPN Client

Kliknij przycisk **Wstaw**



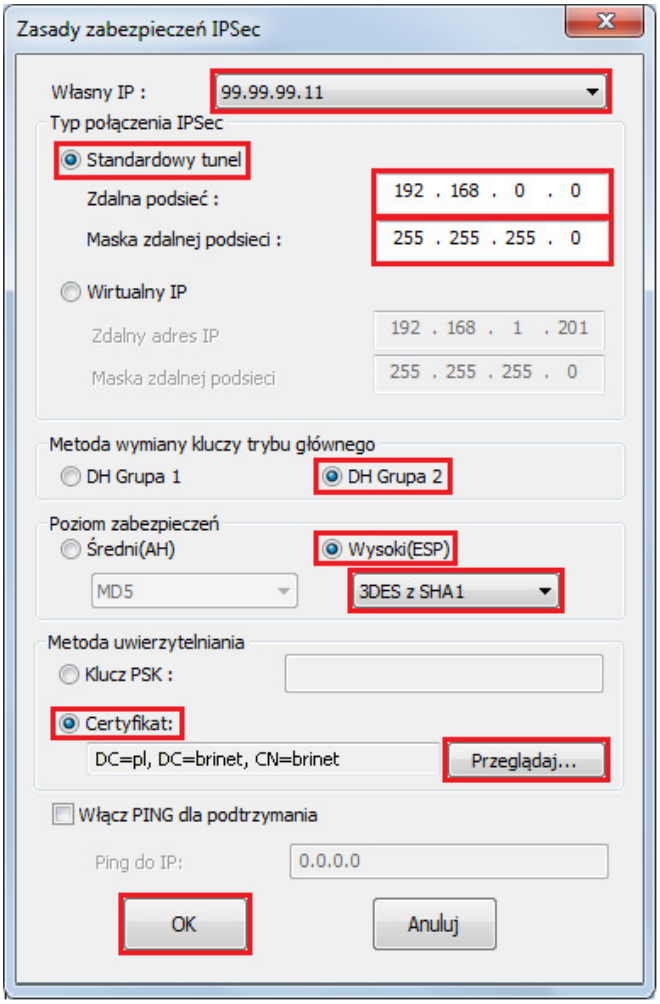
Wypełnij dane dotyczące adresu serwera i typu VPN:

- w polu Nazwa profilu wpisz dowolną nazwę dla połączeni np. To Vigor.
- w polu Adres IP Serwera/Nazwa Hosta wpisz adres IP routera (w przykładzie 99.99.99.10), do którego zestawiasz tunel VPN, albo jego nazwę (w przykładzie serwer.abc.xyz).
- w polu Typ połączenia VPN wybierz Tunel IPSec.
- kliknij OK, aby kontynuować



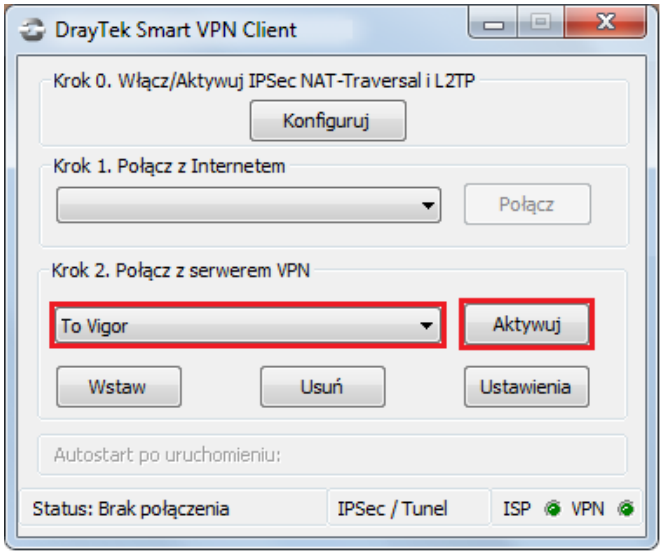
Wypełnij dane dotyczące zabezpieczeń IPSec:

- w polu Mój adres IP wybierz odpowiedni adres IP swojego komputera. W przykładzie 99.99.99.11.
- w polu Typ połączenia IPSec wybierz Standardowy tunel IPSec oraz wpisz adresację zdalnej podsieci. W przykładzie Zdalna podsieć: 192.168.0.0, Maska podsieci zdalnej: 255.255.255.0.
- w polu Metoda zabezpieczeń wybierz protokół realizujący szyfrowanie i uwierzytelnianie. W przykładzie wybrano Wysokie(ESP) oraz 3DES with SHA1.
- w polu Metoda uwierzytelniania wybierz Certyfikat. W przykładzie użyto certyfikatu 'brinet'.
- kliknij przycisk OK, aby zapisać zmiany.

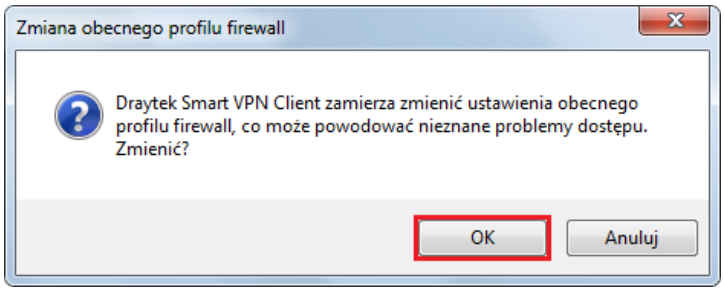


3. Zainicjowanie połączenia

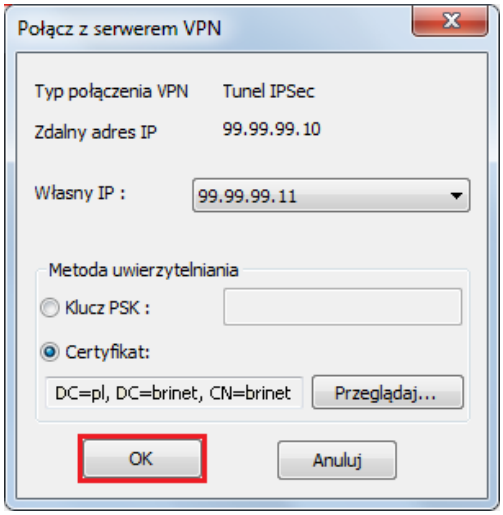
Wybierz odpowiedni profil a następnie kliknij przycisk Aktywuj.



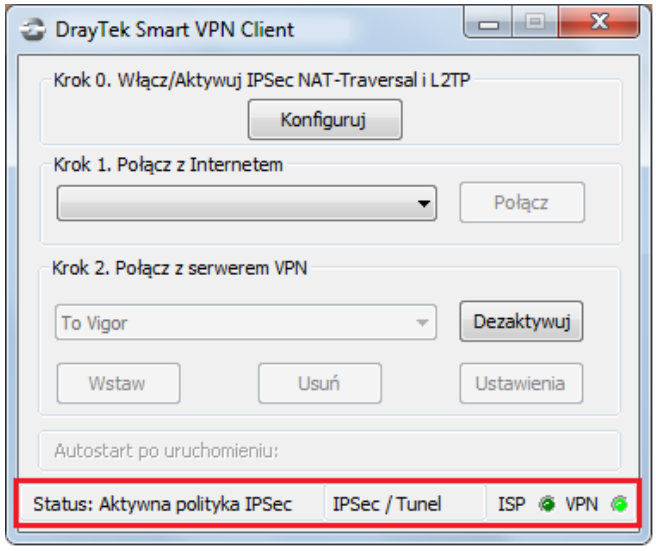
Zaakceptuj zmiany w Zaporze systemu Windows m.in. włączenie zapory, dodanie reguły zabezpieczeń połączeń.



Następnie kliknij OK.



Dla standardowego tunelu IPSec zmieni się status na Aktywna polityka IPSec oraz zapali się zielone światełko przy polu 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_hosta_LAN_serwera (w przykładzie adres zdalnego hosta 192.168.0.10). 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.

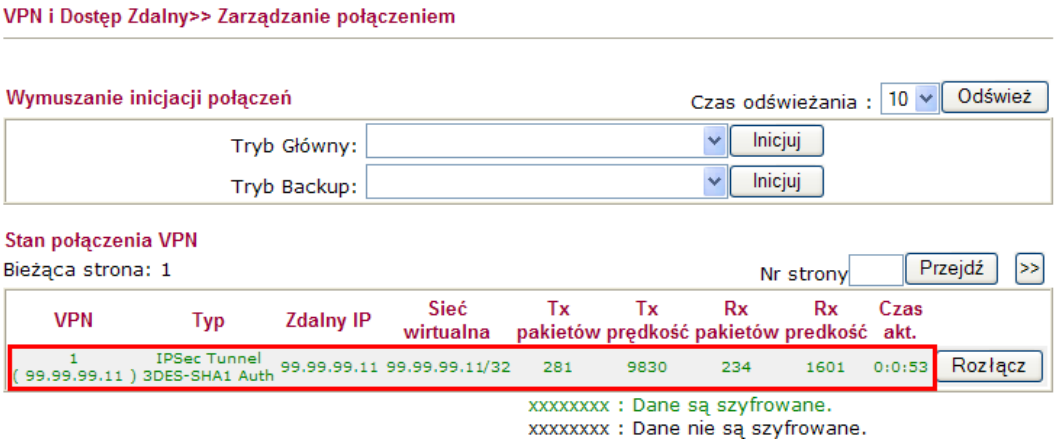
```
C:\>ping 192.168.0.10 -t

Badanie 192.168.0.10 z użyciem 32 bajtów danych:

Negocjowanie zabezpieczeń IP.
Negocjowanie zabezpieczeń IP.
Negocjowanie zabezpieczeń IP.
Negocjowanie zabezpieczeń IP.
Negocjowanie zabezpieczeń IP.
Negocjowanie zabezpieczeń IP.
Negocjowanie zabezpieczeń IP.
Negocjowanie zabezpieczeń IP.
Odpowiedź z 192.168.0.10: bajtów=32 czas=2ms TTL=127
Odpowiedź z 192.168.0.10: bajtów=32 czas=2ms TTL=127
Odpowiedź z 192.168.0.10: bajtów=32 czas=2ms TTL=127
Odpowiedź z 192.168.0.10: bajtów=32 czas=2ms TTL=127
Odpowiedź z 192.168.0.10: bajtów=32 czas=2ms TTL=127
Odpowiedź z 192.168.0.10: bajtów=32 czas=2ms TTL=127
Odpowiedź z 192.168.0.10: bajtów=32 czas=2ms TTL=127
Odpowiedź z 192.168.0.10: bajtów=32 czas=2ms TTL=127
Odpowiedź z 192.168.0.10: bajtów=32 czas=3ms TTL=127

Statystyka badania ping dla 192.168.0.10:
    Pakiety: Wysłane = 17, Odebrane = 9, Utracone = 8 (47% straty),
Szacunkowy czas błądzenia pakietów w millisekundach:
    Minimum = 2 ms, Maksimum = 3 ms, Czas średni = 2 ms
Control-C
^C
```

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