Zestawienie tunelu VPN po protokole IPSec pomiędzy routerem Vigor 2910 (klient VPN) a VigorPro 5500 (serwer VPN).

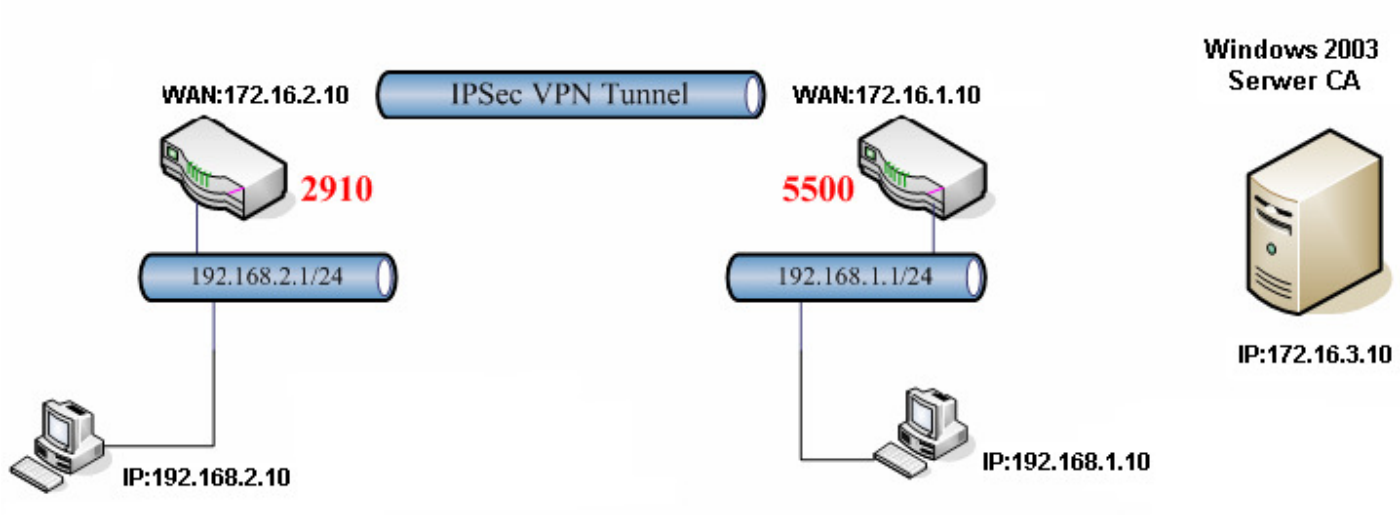
1. Certyfikaty na routerach Vigor
    1.1. Ustawienie czasu
    1.2. Lokalny certyfikat (żądanie certyfikatu z serwera CA)
    1.3. Certyfikat zaufanego CA

2. Konfiguracja serwera VPN

3. Konfiguracja klienta VPN

4. Status połączenia

Procedura konfiguracji została oparta na poniższym przykładzie.



Główne założenia:

- typ tunelu: LAN-LAN z routingiem pomiędzy podsieciami
- protokół VPN: IPSec
- szyfrowanie: AES
- integralność: SHA1 lub MD5
- autentykacja: certyfikaty X.509
- różne adresacje LAN:
  - serwer VPN: 192.168.1.1 /24
  - klient VPN: 192.168.2.1 /24

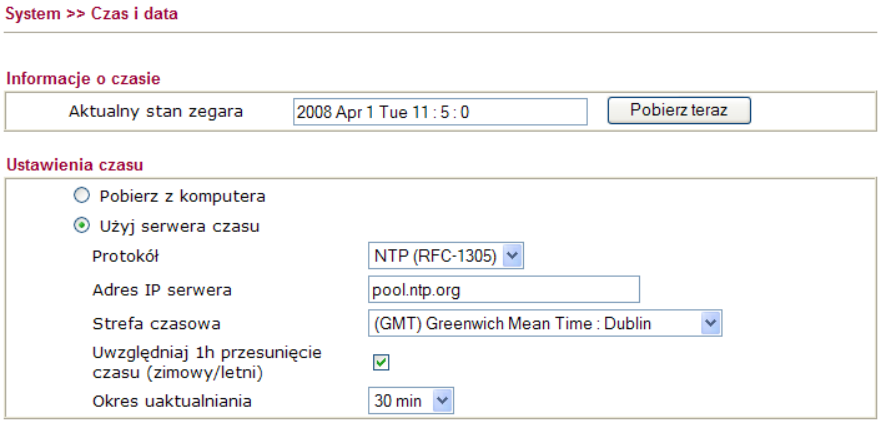
Uwaga!
Wymagane są różne adresacje sieci lokalnych

1. Certyfikaty na routerach Vigor

Uwaga!!! Poniższe kroki wykonaj zarówno dla Vigor 2910 jak i VigorPro 5500.

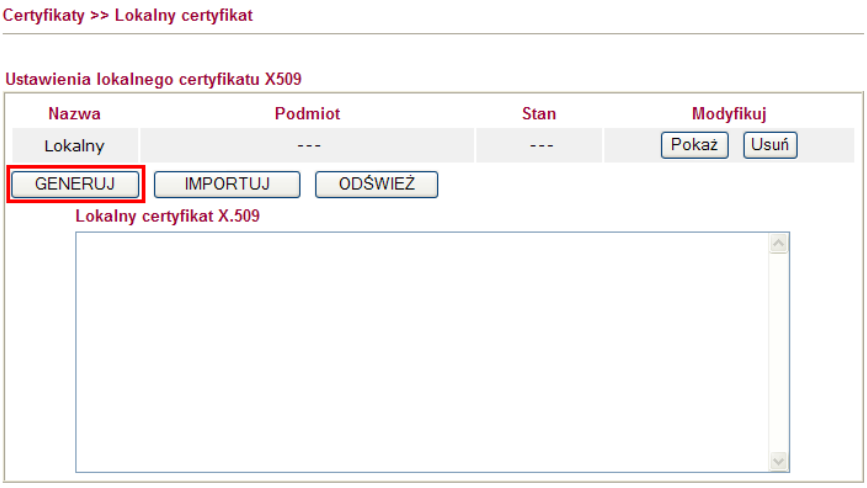
1.1. Ustawienie czasu

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

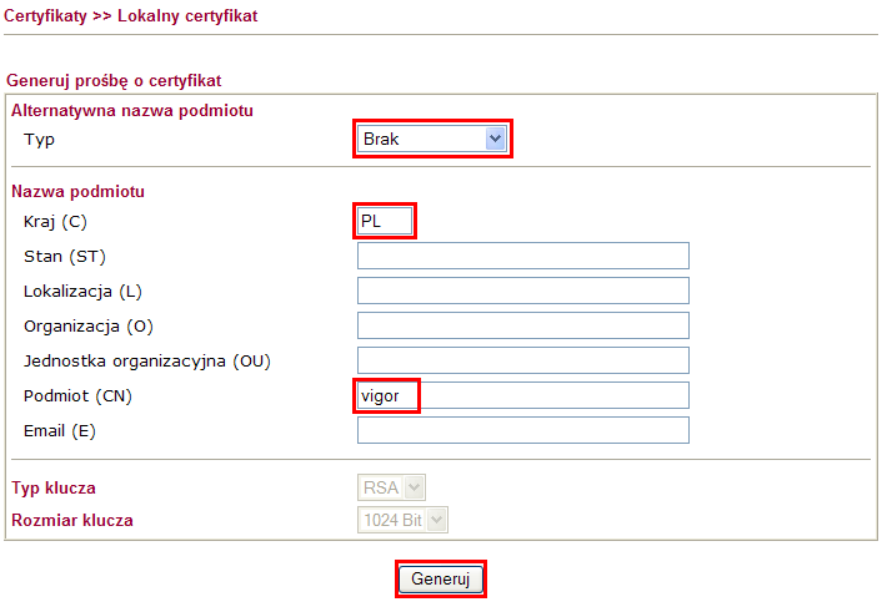


1.2. Lokalny certyfikat (żądanie certyfikatu z serwera CA)

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

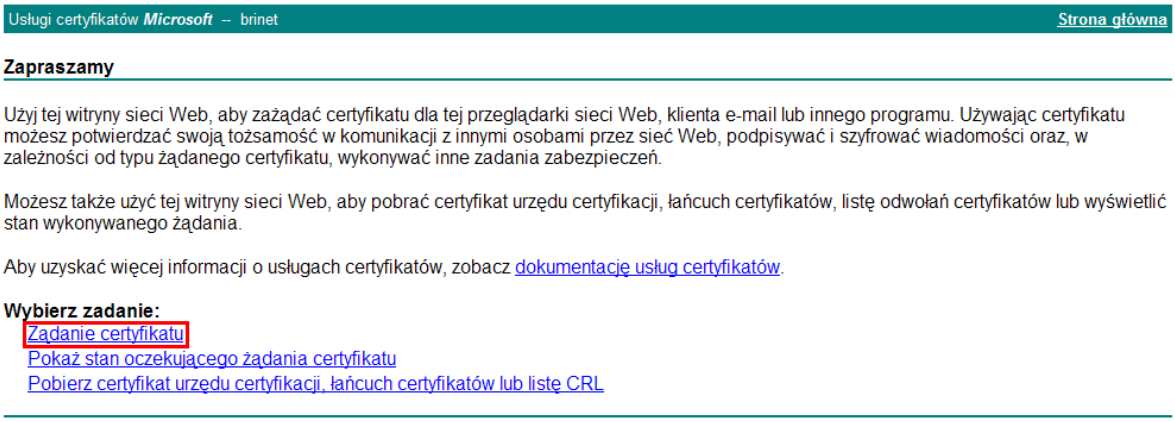


Krok 2: Wpisz odpowiednie dane w polach **Alternatywna nazwa podmiotu** i **Nazwa podmiotu**. W przykładzie użyto wartości pokazanych na następnym rysunku. Po wprowadzeniu danych kliknij przycisk **Generuj**.

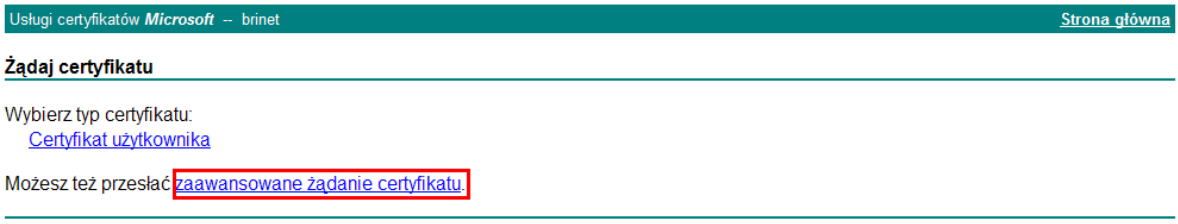


Krok 3: Wygenerowany tekst będzie potrzebny w kroku 7.

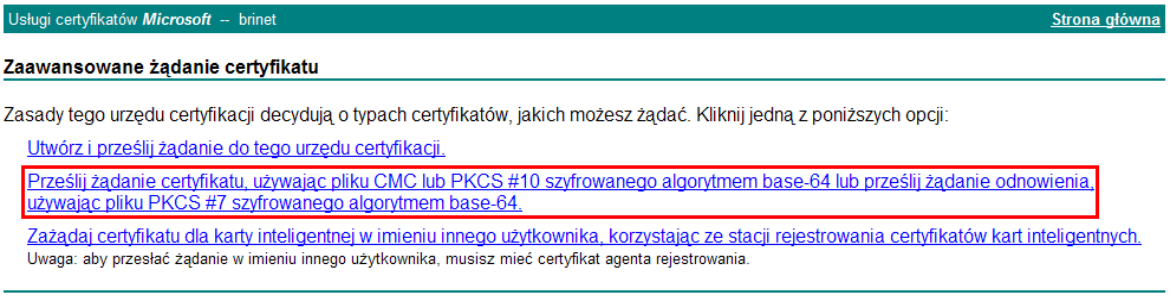
Krok 4. Połącz się z serwerem CA (w przykładzie http://172.16.3.10/certsrv). W przykładzie wykorzystano Windows Server 2003 RC2 jako serwer CA. Po zalogowaniu wybierz **Żądanie certyfikatu**.



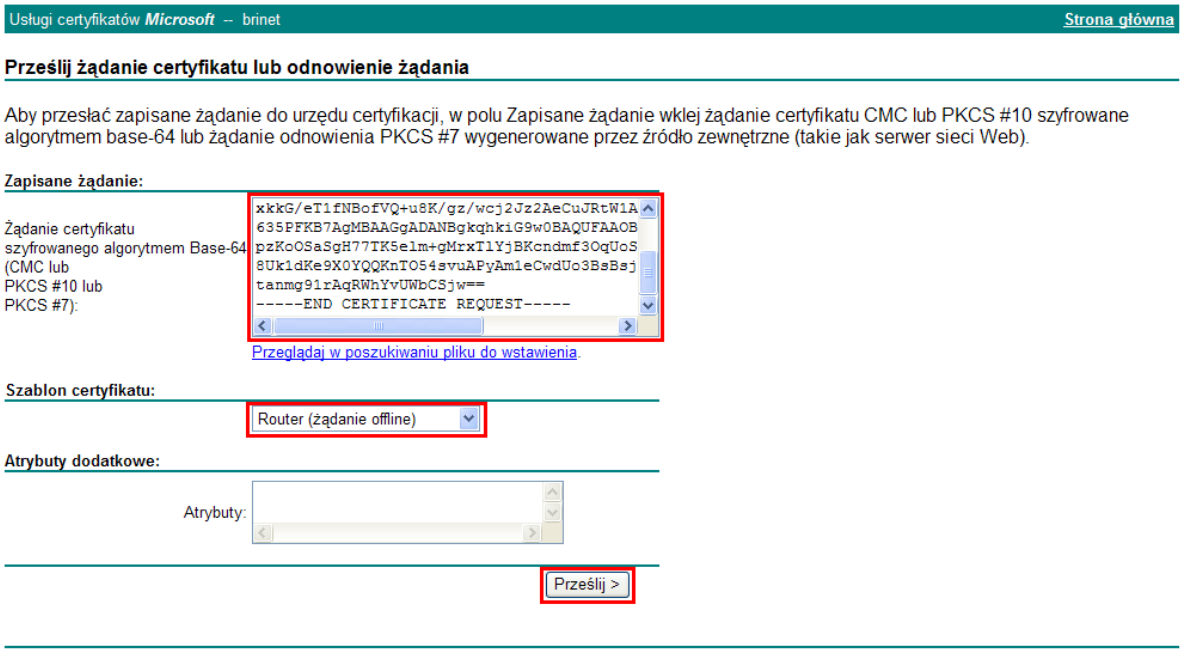
Krok 5: Wybierz **zaawansowane żądanie certyfikatu**.



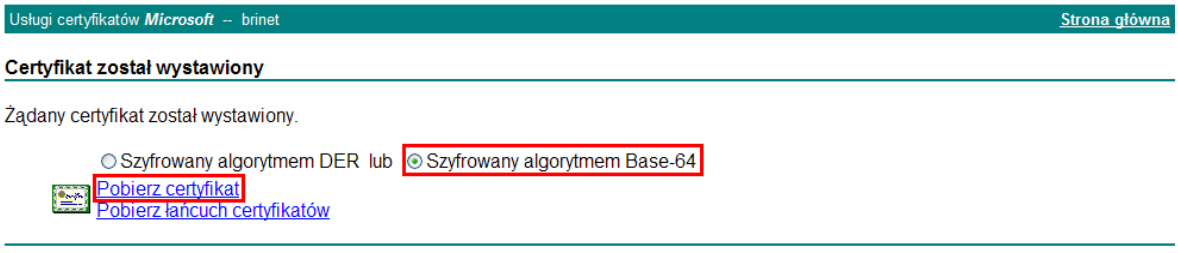
Krok 6: Wybierz drugą opcję – **Prześlij żądanie certyfikatu, używając …**



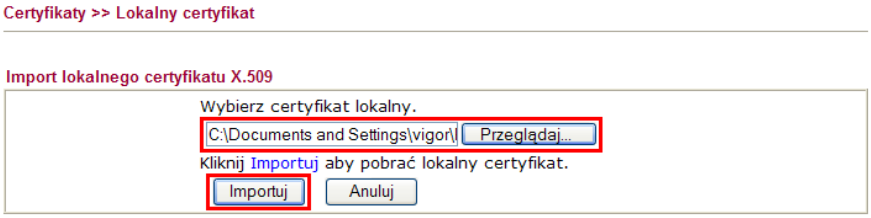
Krok 7. Wklej tekst wygenerowany w kroku 3. Wybierz opcję **Router (żądanie offline)** jako Szablon certyfiaktu. Następnie kliknij przycisk **Prześlij>**.



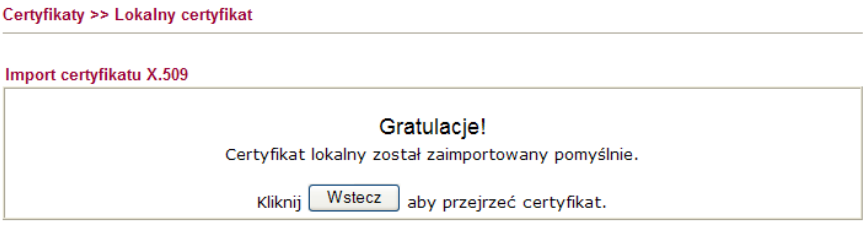
Krok 8: Pobierz certyfikat szyfrowany algorytmem Base-64



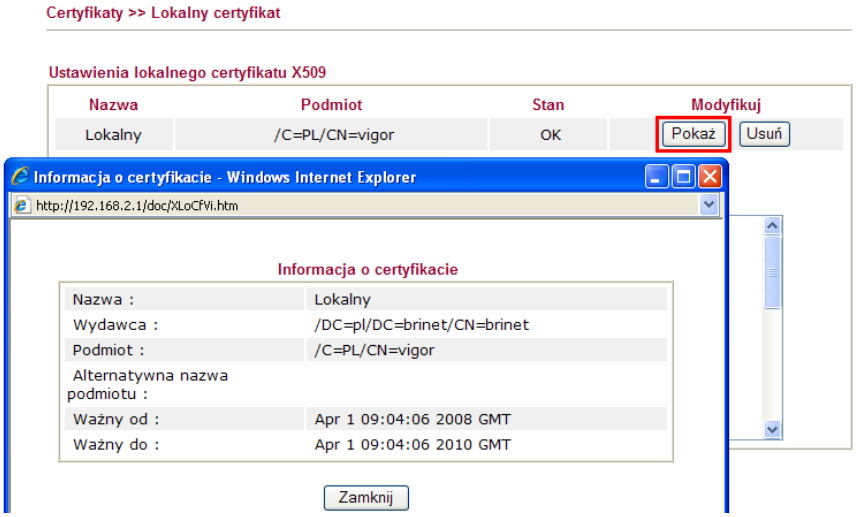
Krok 9: Zaimportuj lokalny certyfikat do Vigora – wybierz ścieżkę do certyfikatu i kliknij przycisk **Importuj**.



Krok 10: Pomyślna próba importu certyfikatu.

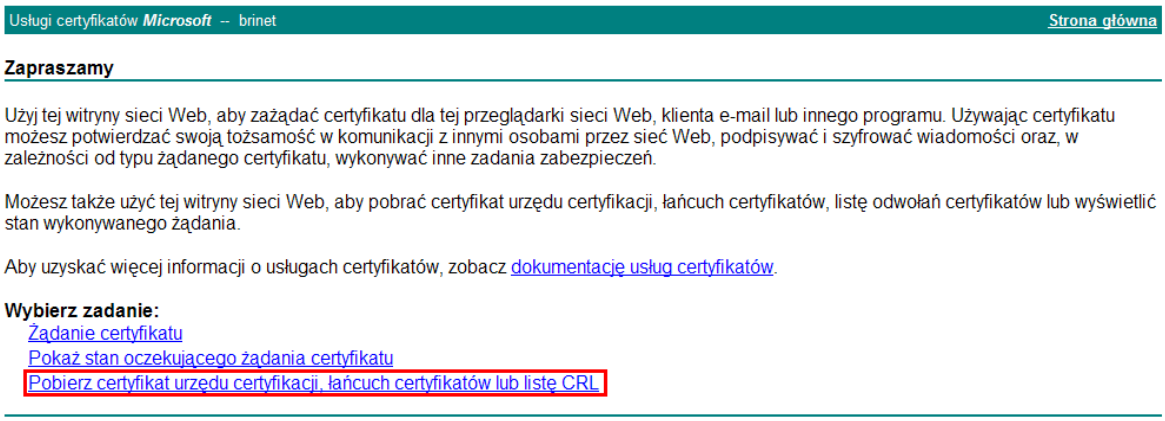


Aby zobaczyć certyfikat kliknij przycisk **Pokaż**.



1.3. Certyfikat zaufanego CA

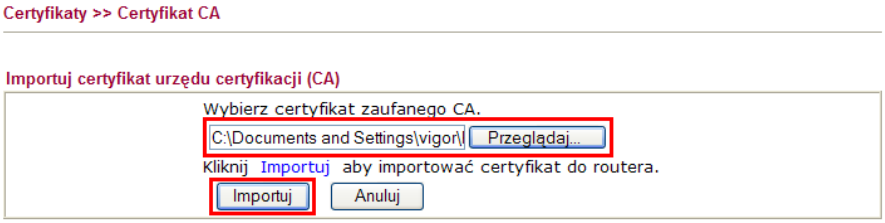
Krok 1: Połącz się z serwerem CA (w przykładzie http://172.16.3.10/certsrv). Po zalogowaniu wybierz **Pobierz certyfikat urzędu certyfikacji, łańcuch certyfikatów lub listę CRL**.



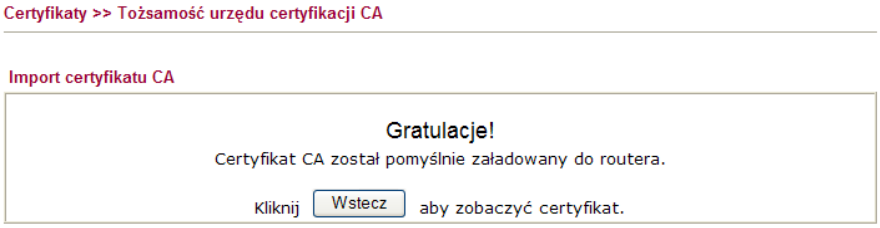
Krok 2: Wybierz odpowiedni certyfikat urzędu certyfikacji (w przykładzie brinet) oraz **Base 64** jako Metodę kodowania. Następnie wybierz opcję **Pobierz certyfikat urzędu certyfikacji** i zapisz na dysku.

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**.



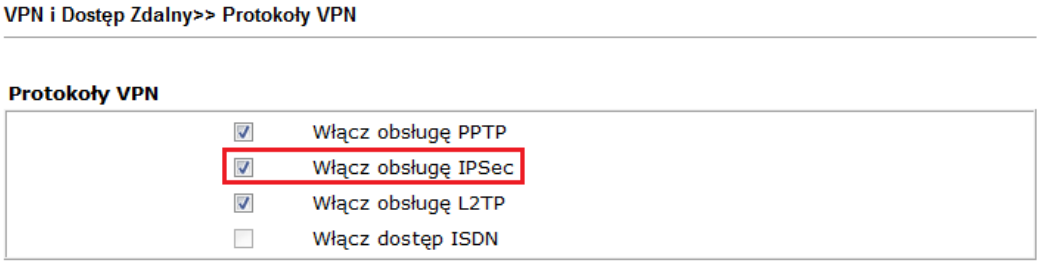
Krok 5: Pomyślna próba importu certyfikatu.



2. Konfiguracja serwera VPN (5500)

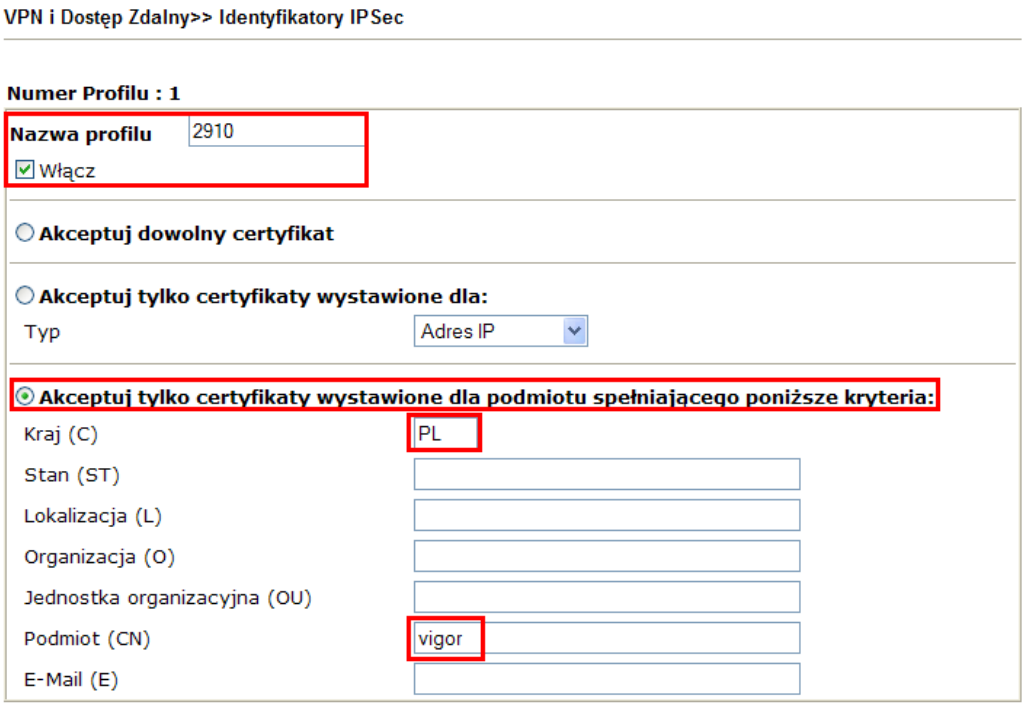
Włączenie obsługi IPSec

Przejdź do zakładki **VPN i Dostęp Zdalny>>Protokoły VPN** w panelu konfiguracyjnym routera i sprawdź (lub zaznacz) czy jest włączona obsługa protokołu IPSec. Domyślnie włączona jest obsługa protokołów PPTP, IPSec i L2TP.



Konfiguracja identyfikatora 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. Po wprowadzeniu danych kliknij przycisk **OK**.

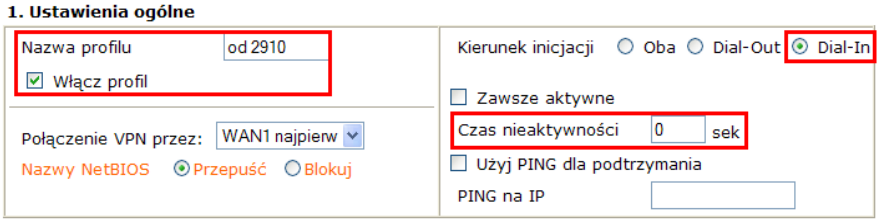


Konfiguracja profilu LAN-LAN

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

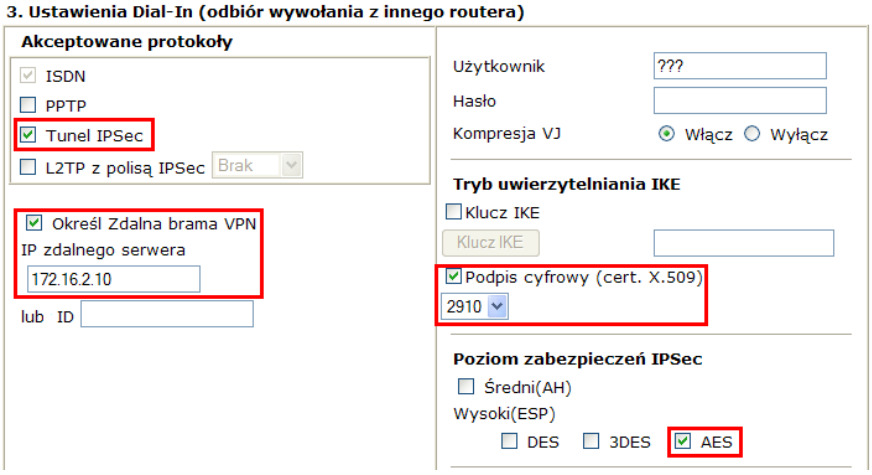
Konfiguracja części **Ustawienia ogólne** zgodna z założeniami przykładu:

- wpisz dowolną nazwę profilu
- zaznacz **Włącz profil**
- jako kierunek inicjacji wybierz **Dial-In**
- ustaw **czas nieaktywności 0**, gdy połączenie ma być aktywne cały czas.



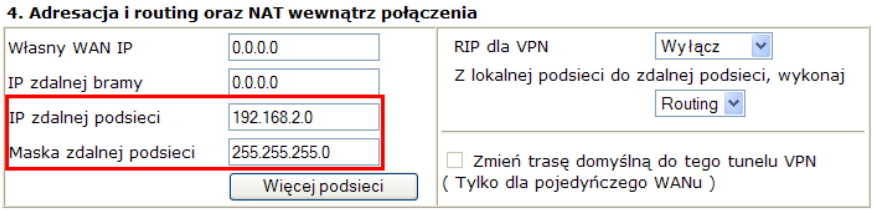
Konfiguracja części **Ustawienia Dial-In** zgodna z założeniami przykładu:

- w polu Protokół dla połączenia wybierz **Tunel IPSec**
- zaznacz **Określ Zdalna brama VPN**, a w polu **IP zdalnego serwera** wpisz adres IP routera – klienta VPN. W przykładzie użyto adresu IP 172.16.2.10
- w polu Tryb uwierzytelniania IKE wybierz **Podpis cyfrowy (cert. X.509)** i odpowiedni certyfikat. W przykładzie użyto '2910'
- w polu Poziom zabezpieczeń IPSec wybierz **AES**.



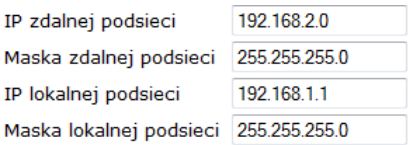
Konfiguracja części **Adresacja i routing oraz NAT wewnątrz połączenia** zgodna z założeniami przykładu:

- w przykładzie Zdalna podsieć: 192.168.2.0, Maska podsieci zdalnej: 255.255.255.0



Uwaga!!!

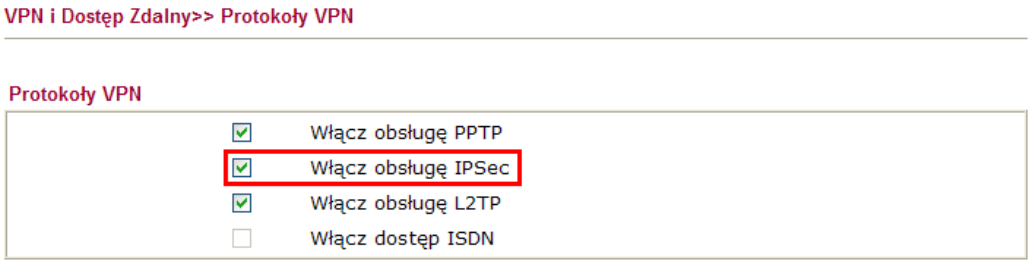
W niektórych modelach dostępne są dodatkowe pola określające IP lokalnej podsieci oraz jej maskę. Poniżej konfiguracja zgodna z założeniami przykładu.



3. Konfiguracja klienta VPN (2910)

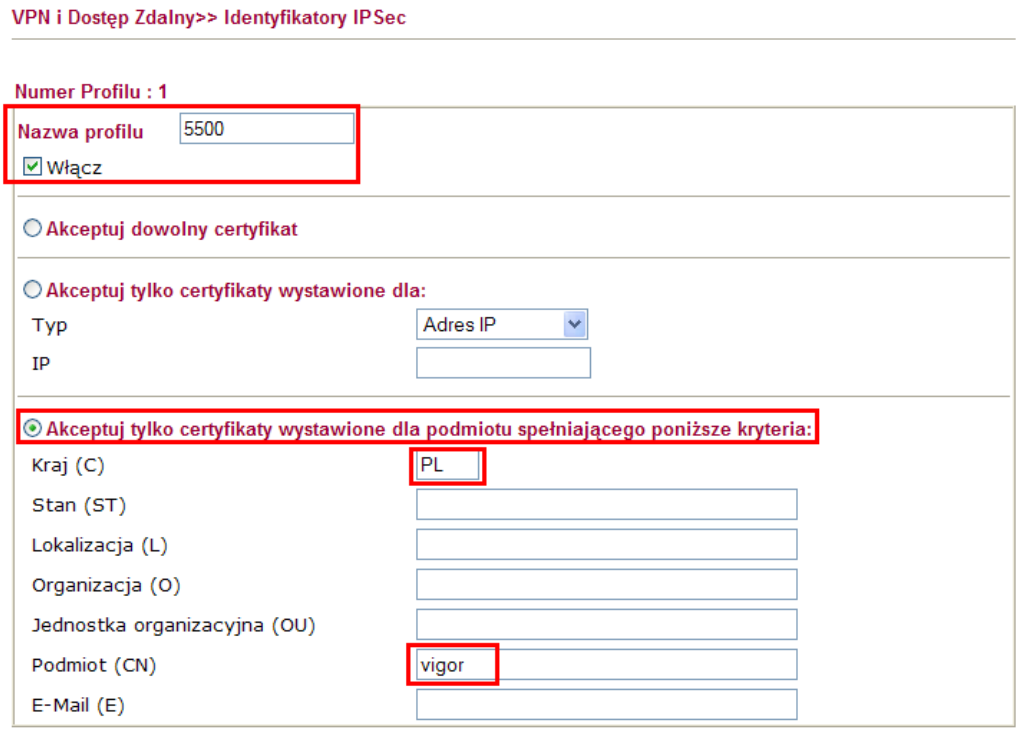
Włączenie obsługi IPSec

Przejdź do zakładki **VPN i Dostęp Zdalny>>Protokoły VPN** w panelu konfiguracyjnym routera i sprawdź (lub zaznacz) czy jest włączona obsługa protokołu IPSec. Domyślnie włączona jest obsługa protokołów PPTP, IPSec i L2TP.



Konfiguracja identyfikatora 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. Po wprowadzeniu danych kliknij przycisk **OK**.

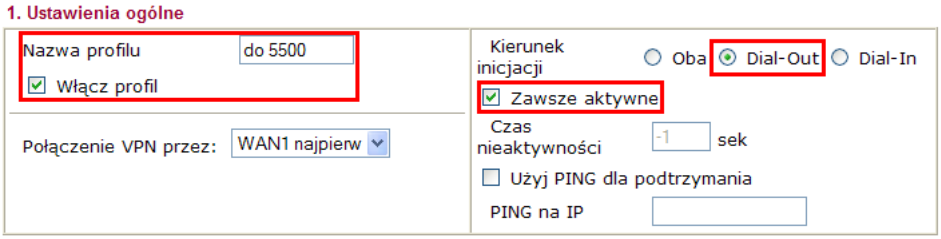


Konfiguracja profilu LAN-LAN

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

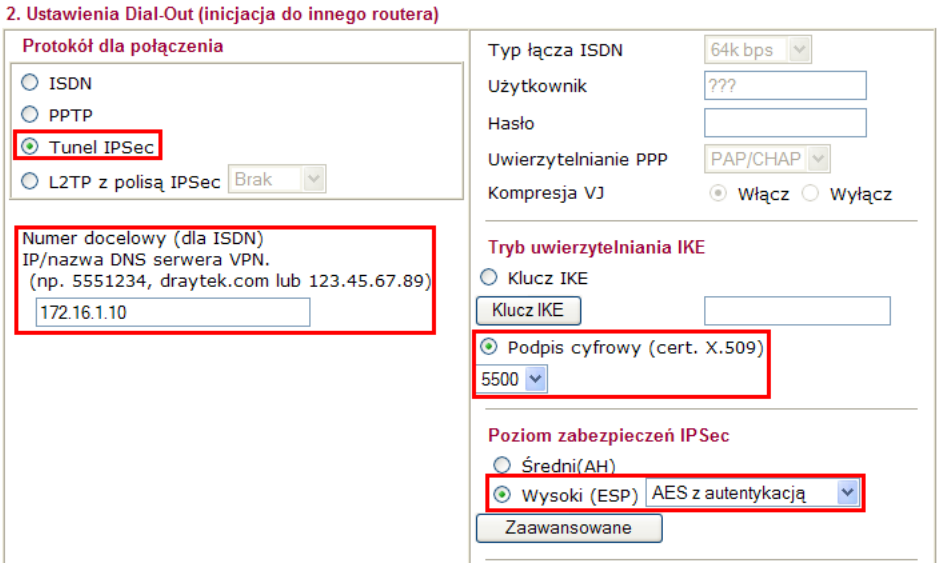
Konfiguracja części **Ustawienia ogólne** zgodna z założeniami przykładu:

- wpisz dowolną nazwę profilu
- zaznacz **Włącz profil**
- jako kierunek inicjacji wybierz **Dial-Out**
- zaznacz **Zawsze aktywne** - w ten sposób ustawisz **czas nieaktywności -1**, gdy połączenie ma być aktywne cały czas.



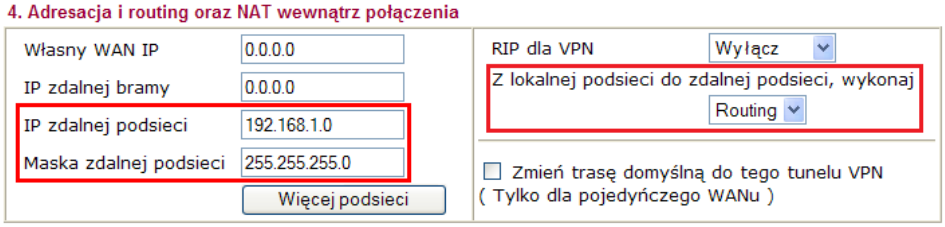
Konfiguracja części **Ustawienia Dial-Out** zgodna z założeniami przykładu:

- w polu Protokół dla połączenia wybierz **Tunel IPSec**
- w polu **IP/nazwa DNS serwera VPN** wpisz adres IP routera, do którego zestawiasz tunnel VPN, albo jego nazwę. W przykładzie adres IP 172.16.1.10
- w polu Tryb uwierzytelniania IKE wybierz **Podpis cyfrowy (cert. X.509)** i odpowiedni certyfikat. W przykładzie użyto '5500'
- w polu Poziom zabezpieczeń IPSec wybierz protokół realizujący szyfrowanie i uwierzytelnianie **Wysoki(ESP)**. W przykładzie użyto AES z autentykacją SHA1/MD5



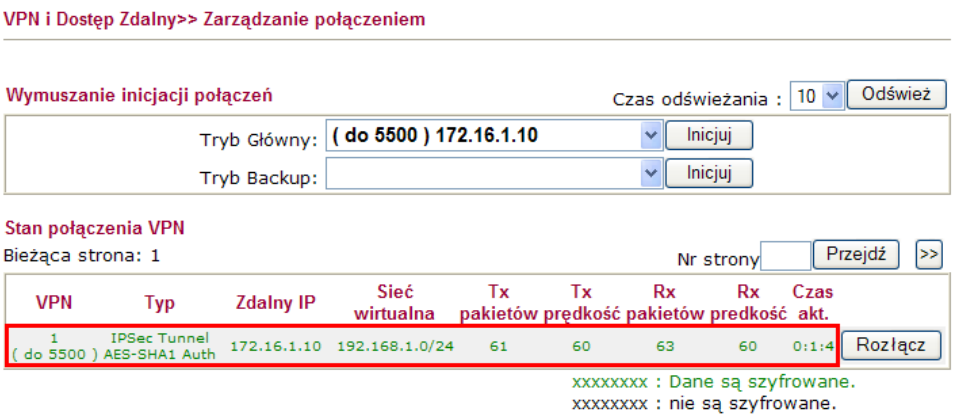
Konfiguracja części **Adresacja i routing oraz NAT wewnątrz połączenia** zgodna z założeniami przykładu:

- w przykładzie Zdalna podsieć: 192.168.1.0, Maska podsieci zdalnej: 255.255.255.0

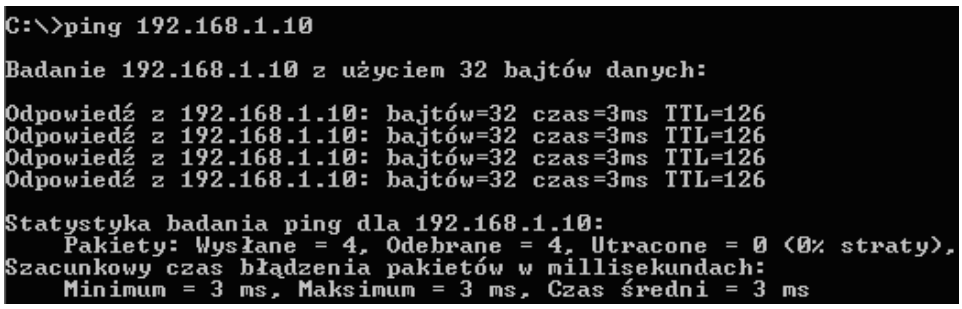


4. Status połączenia (od strony klienta VPN)

O tym, czy tunel został zainicjowany, możesz przekonać się wybierając **VPN i Dostęp Zdalny>>Zarządzanie połączeniem** (rysunek poniżej).



Inny sposób to np. zwykły ping. Wybierz Menu Start a następnie Uruchom i wpisz cmd . Następnie wykonaj polecenie: ping adres_hosta_w_LAN-ie (patrz rysunek poniżej, gdzie host posiada adres LAN-owy 192.168.1.10). Po zainicjowaniu tunelu otrzymasz poprawną odpowiedź na ping – świadczy ona o poprawnej komunikacji w tunelu VPN.



Krzysztof Skowina
Specjalista ds. rozwiązań sieciowych
BRINET Sp. z o.o.
k.skowina@brinet.pl