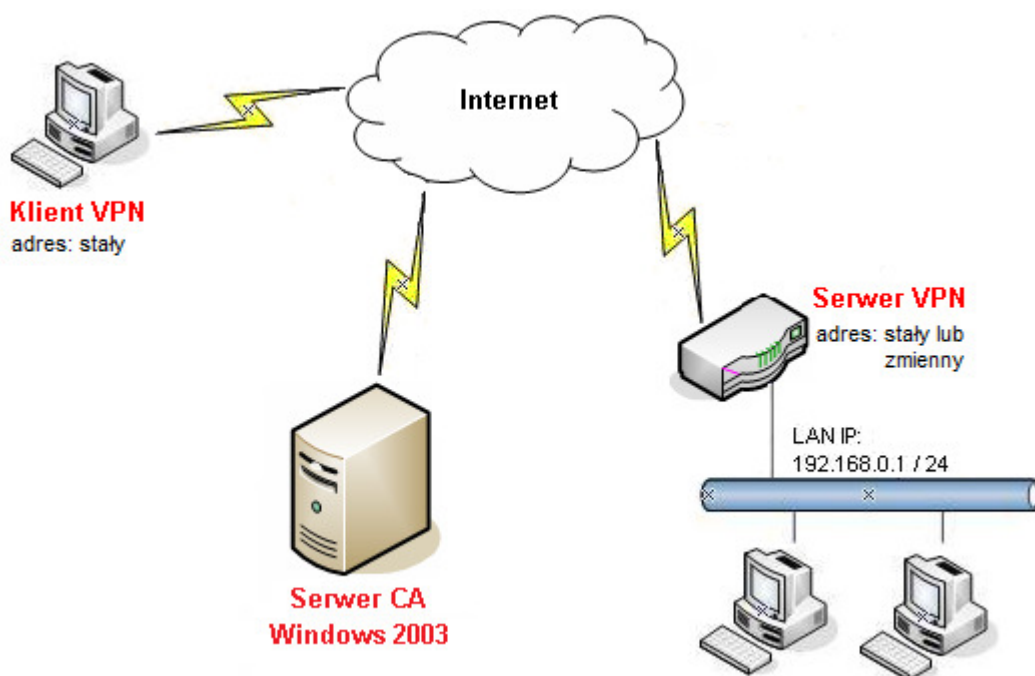


1. Konfiguracja serwera VPN
  - 1.1. Włączenie obsługi IPSec
  - 1.2. Ustawienie czasu
  - 1.3. Lokalny certyfikat (żądanie certyfikatu z serwera CA)
  - 1.4. Certyfikat zaufanego CA
  - 1.5. Identyfikator IPSec
  - 1.6. Profil Host-LAN
2. Konfiguracja klienta VPN
  - 2.1. Zastosowanie certyfikatu z serwera CA do PC
  - 2.2. Konfiguracja DrayTek Smart VPN Client
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: 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](http://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.

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

#### 1.2. Ustawienie czasu

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

System >> Czas i data

Informacje o czasie

Aktualny stan zegara: 2008 Apr 1 Tue 11:5:0 Pobierz teraz

Ustawienia czasu

Pobierz z komputera

Użyj serwera czasu

Protokół: NTP (RFC-1305)

Adres IP serwera: pool.ntp.org

Strefa czasowa: (GMT) Greenwich Mean Time : Dublin

Uwzględniaj 1h przesunięcie czasu (zimowy/letni):

Okres uaktualniania: 30 min

#### 1.3. Lokalny certyfikat (żądanie certyfikatu z serwera CA)

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

Certyfikaty >> Lokalny certyfikat

Ustawienia lokalnego certyfikatu X509

Nazwa	Podmiot	Stan	Modyfikuj
Lokalny	---	---	<span>Pokaż</span> <span>Usuń</span>

GENERUJ IMPORTUJ ODŚWIEŻ

Lokalny certyfikat X.509

**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**.

Certyfikaty >> Lokalny certyfikat

Generuj prośbę o certyfikat

**Alternatywna nazwa podmiotu**

Typ:    
 Nazwa domeny:

**Nazwa podmiotu**

Kraj (C):   
 Stan (ST):   
 Lokalizacja (L):   
 Organizacja (O):   
 Jednostka organizacyjna (OU):   
 Podmiot (CN):   
 Email (E):

Typ klucza:   
 Rozmiar klucza:

**Krok 3:** Wygenerowany tekst będzie potrzebny w kroku 7.

Certyfikaty >> Lokalny certyfikat

Ustawienia lokalnego certyfikatu X509

Nazwa	Podmiot	Stan	Modyfikuj
Lokalny	/OU=draytek/CN=vigor	Requesting	<input type="button" value="Pokaż"/> <input type="button" value="Usuń"/>

**Prośba o certyfikat X509**

```

-----BEGIN CERTIFICATE REQUEST-----
MIIBhTCB7wIBADAIMRAwDgYDVQQLEwdkcmF5dGVrMQ4wDAYDVQQDEwV2aWdvcjCB
nzANBgkqhkiG9w0BAQEFAAOBjQAwYkCgYEA6OgZLXHIAjVgPeh3zEeFxd9WboUO
kUwMxZVkrA8IS+IeFWJbDumMCynL/x4vxyHVt4/cPTzZJPCO+69xUKt+T/n4MzCf
YChqucDGSQb95PV80Gh9VD67wr+DP/ByPYnPYB4K41G1bUAG+jFRabzgocciEXh6
DIOsumfrfk8UoHsCAwEAAaAKMCIgCSqGSIb3DQEJDDjEVMwEQQYDVR0RBaowCIIG
YnJpbmV0MA0GCSqGSIb3DQEBBQUAA4GBAFLXPf0hmc3uB78K/qdnbade/JzmDuRC
F8DjnaEhue63j3M0ehOE6OZuTZCgGF0ituxoCXqchKjuQVil/2hUR2bxY64hhs9K
aOB0AF/BxFpF08FnbhaiAGKpyBivIOyr8pi7P2Ak1XiLC8qhQX7ExmZhpq2TFRI
fzOMIjqwF/4r
-----END CERTIFICATE REQUEST-----
    
```

**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**.

Usługi certyfikatów Microsoft -- brinet [Strona główna](#)

### Zapraszamy

Użyj tej witryny sieci Web, aby zażądać certyfikatu dla tej przeglądarki sieci Web, klienta e-mail lub innego programu. Używając certyfikatu możesz potwierdzać swoją tożsamość w komunikacji z innymi osobami przez sieć Web, podpisywać i szyfrować wiadomości oraz, w zależności od typu żadanego certyfikatu, wykonywać inne zadania zabezpieczeń.

Możesz także użyć tej witryny sieci Web, aby pobrać certyfikat urzędu certyfikacji, łańcuch certyfikatów, listę odwołań certyfikatów lub wyświetlić stan wykonywanego żądania.

Aby uzyskać więcej informacji o usługach certyfikatów, zobacz [dokumentację usług certyfikatów](#).

### Wybierz zadanie:

[Pokaż stan oczekującego żądania certyfikatu](#)

[Pobierz certyfikat urzędu certyfikacji, łańcuch certyfikatów lub listę CRL](#)

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

Usługi certyfikatów *Microsoft* -- brinet Strona główna

**Żądaj certyfikatu**

Wybierz typ certyfikatu:  
[Certyfikat użytkownika](#)

Możesz też przesłać **zaawansowane żądanie certyfikatu**.

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

Usługi certyfikatów *Microsoft* -- brinet Strona główna

**Zaawansowane żądanie certyfikatu**

Zasady tego urzędu certyfikacji decydują o typach certyfikatów, jakich możesz żądać. Kliknij jedną z poniższych opcji:

[Utwórz i prześlij żądanie do tego urzędu certyfikacji.](#)

**[Prześlij żądanie certyfikatu, używając pliku CMC lub PKCS #10 szyfrowanego algorytmem base-64 lub prześlij żądanie odnowienia, używając pliku PKCS #7 szyfrowanego algorytmem base-64.](#)**

[Zażądaj certyfikatu dla karty inteligentnej w imieniu innego użytkownika, korzystając ze stacji rejestrowania certyfikatów kart inteligentnych.](#)

Uwaga: aby przesłać żądanie w imieniu innego użytkownika, musisz mieć certyfikat agenta rejestrowania.

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

Usługi certyfikatów *Microsoft* -- brinet Strona główna

**Prześlij żądanie certyfikatu lub odnowienie żądania**

Aby przesłać zapisane żądanie do urzędu certyfikacji, w polu Zapisane żądanie wklej żądanie certyfikatu CMC lub PKCS #10 szyfrowane algorytmem base-64 lub żądanie odnowienia PKCS #7 wygenerowane przez źródło zewnętrzne (takie jak serwer sieci Web).

**Zapisane żądanie:**

Żądanie certyfikatu szyfrowanego algorytmem Base-64 (CMC lub PKCS #10 lub PKCS #7):

```

DIOsumfrfk8UoHsCAwEAAaAKMCIGCSqGS Ib3DQEJ
YnJpbmVOMA0GCSqGS Ib3DQEBBQUAA4GBAFLXPf0h
F8DjnaEbue63j3M0ehOE60ZuTZCGFOituxoCXqc
aOB0AF/BxFpF08FnbhaiAGKpyBivIOyr8pi7P2Ak
FzOMIjqqwF/4r
-----END CERTIFICATE REQUEST-----
    
```

[Przełącz w poszukiwaniu pliku do wstawienia.](#)

**Szablon certyfikatu:**

**Router (żądanie offline)**

**Atrybuty dodatkowe:**

Atrybuty:

**Prześlij >**

**Krok 8: Pobierz certyfikat szyfrowany algorytmem Base-64**

Usługi certyfikatów *Microsoft* -- brinet Strona główna

**Certyfikat został wystawiony**

Żądany certyfikat został wystawiony.

Szyfrowany algorytmem DER lub  Szyfrowany algorytmem Base-64

[Pobierz certyfikat](#)  
[Pobierz łańcuch certyfikatów](#)

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

Certyfikaty >> Lokalny certyfikat

---

Import lokalnego certyfikatu X.509

Wybierz certyfikat lokalny.  
C:\Documents and Settings\vigor\ Przełóżaj...  
Kliknij **Importuj** aby pobrać lokalny certyfikat.  
**Importuj** Anuluj

**Krok 10:** Pomyślna próba importu certyfikatu.

Certyfikaty >> Lokalny certyfikat

---

Import certyfikatu X.509

**Gratulacje!**  
Certyfikat lokalny został zaimportowany pomyślnie.  
Kliknij **Wstecz** aby przejrzeć certyfikat.

Aby zobaczyć certyfikat kliknij przycisk **Pokaż**.

Certyfikaty >> Lokalny certyfikat

---

Ustawienia lokalnego certyfikatu X509

Nazwa	Podmiot	Stan	Modyfikuj
Lokalny	/OU=draytek/CN=vigor	OK	<b>Pokaż</b> Usuń

Informacja o certyfikacie - Windows Internet Explorer  
http://192.168.1.1/doc/XLoCFvi.htm

**Informacja o certyfikacie**

Nazwa :	Lokalny
Wydawca :	/DC=pl/DC=brinet/CN=brinet
Podmiot :	/OU=draytek/CN=vigor
Alternatywna nazwa podmiotu :	DNS:brinet
Ważny od :	Apr 1 12:18:45 2008 GMT
Ważny do :	Apr 1 12:18:45 2010 GMT

Zamknij

### 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**.

Usługi certyfikatów *Microsoft* -- brinet Strona główna

---

**Zapraszamy**

Użyj tej witryny sieci Web, aby zażądać certyfikatu dla tej przeglądarki sieci Web, klienta e-mail lub innego programu. Używając certyfikatu możesz potwierdzać swoją tożsamość w komunikacji z innymi osobami przez sieć Web, podpisywać i szyfrować wiadomości oraz, w zależności od typu żadanego certyfikatu, wykonywać inne zadania zabezpieczeń.

Możesz także użyć tej witryny sieci Web, aby pobrać certyfikat urzędu certyfikacji, łańcuch certyfikatów, listę odwołań certyfikatów lub wyświetlić stan wykonywanego żądania.

Aby uzyskać więcej informacji o usługach certyfikatów, zobacz [dokumentację usług certyfikatów](#).

**Wybierz zadanie:**  
[Żądanie certyfikatu](#)  
[Pokaż stan oczekującego żądania certyfikatu](#)  
[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.

Usługi certyfikatów *Microsoft* -- brinet Strona główna

---

**Pobierz certyfikat urzędu certyfikacji, łańcuch certyfikatów lub listę CRL**

Do ufania certyfikatom wystawionym przez ten urząd certyfikacji, [zainstaluj jego łańcuch certyfikatów](#).

Aby pobrać certyfikat urzędu certyfikacji, łańcuch certyfikatów lub listę CRL, wybierz certyfikat i metodę kodowania.

**Certyfikat urzędu certyfikacji:**

**Metoda kodowania:**

DER  
 Base 64

[Pobierz certyfikat urzędu certyfikacji](#)  
[Pobierz łańcuch certyfikatów urzędu certyfikacji](#)  
[Pobierz najnowszą podstawową listę CRL](#)  
[Pobierz najnowszą różnicową listę CRL](#)

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

Certyfikaty >> Certyfikat zaufanego CA

---

Tożsamości zaufanych CA (certyfikaty X.509)

Nazwa	Podmiot	Stan	Modyfikuj	
CA-1	---	---	<input type="button" value="Pokaż"/>	<input type="button" value="Usuń"/>
CA-2	---	---	<input type="button" value="Pokaż"/>	<input type="button" value="Usuń"/>
CA-3	---	---	<input type="button" value="Pokaż"/>	<input type="button" value="Usuń"/>

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

Certyfikaty >> Certyfikat CA

---

Importuj certyfikat urzędu certyfikacji (CA)

Wybierz certyfikat zaufanego CA.

C:\Documents and Settings\vigor\

Kliknij **Importuj** aby importować certyfikat do routera.

**Krok 11:** Pomyślna próba importu certyfikatu.

Certyfikaty >> Tożsamość urzędu certyfikacji CA

---

Import certyfikatu CA

**Gratulacje!**

Certyfikat CA został pomyślnie załadowany do routera.

Kliknij  aby zobaczyć certyfikat.

### 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.

VPN i Dostęp Zdalny>> Identyfikatory IPSec

---

Numer Profilu : 1

Nazwa profilu	host
<input checked="" type="checkbox"/> Włącz	
<input type="radio"/> Akceptuj dowolny certyfikat	
<input type="radio"/> Akceptuj tylko certyfikaty wystawione dla:	
Typ	Adres IP
<input checked="" type="radio"/> Akceptuj tylko certyfikaty wystawione dla podmiotu spełniającego poniższe kryteria:	
Kraj (C)	PL
Stan (ST)	
Lokalizacja (L)	
Organizacja (O)	
Jednostka organizacyjna (OU)	
Podmiot (CN)	teleworker
E-Mail (E)	

### 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.

VPN i Dostęp Zdalny>> Użytkownik zdalny

---

Indeks Nr. 1

<p>Konto użytkownika</p> <input checked="" type="checkbox"/> Włącz konto Czas nieaktywności <input type="text" value="0"/> sek	<p>Użytkownik</p> <input type="text" value="???"/>
<p>Akceptowane protokoły</p> <input type="checkbox"/> PPTP <input checked="" type="checkbox"/> Tunel IPSec <input type="checkbox"/> L2TP z polisą IPSec <input type="text" value="Brak"/>	<p>Tryb uwierzytelniania IKE</p> <input type="checkbox"/> Klucz IKE Klucz IKE <input type="text"/> <input checked="" type="checkbox"/> Podpis cyfrowy (cert. X.509) host
<p>Określ węzeł zdalny</p> Adres IP klienta zdalnego <input type="text" value="99.99.99.11"/> lub ID <input type="text"/>	<p>Poziom zabezpieczeń IPSec</p> <input type="checkbox"/> Średni (AH) Wysoki (ESP) <input type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES Lokalny ID <input type="text"/> (opcja)



## 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**.

Usługi certyfikatów *Microsoft* -- brinet Strona główna

---

**Zapraszamy**

Użyj tej witryny sieci Web, aby zażądać certyfikatu dla tej przeglądarki sieci Web, klienta e-mail lub innego programu. Używając certyfikatu możesz potwierdzać swoją tożsamość w komunikacji z innymi osobami przez sieć Web, podpisywać i szyfrować wiadomości oraz, w zależności od typu żadanego certyfikatu, wykonywać inne zadania zabezpieczeń.

Możesz także użyć tej witryny sieci Web, aby pobrać certyfikat urzędu certyfikacji, łańcuch certyfikatów, listę odwołań certyfikatów lub wyświetlić stan wykonywanego żądania.

Aby uzyskać więcej informacji o usługach certyfikatów, zobacz [dokumentację usług certyfikatów](#).

**Wybierz zadanie:**  
[Żądanie certyfikatu](#)  
[Pokaż stan oczekującego żądania certyfikatu](#)  
[Pobierz certyfikat urzędu certyfikacji, łańcuch certyfikatów lub listę CRL](#)

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

Usługi certyfikatów *Microsoft* -- brinet Strona główna

---

**Żądaj certyfikatu**

Wybierz typ certyfikatu:  
[Certyfikat użytkownika](#)

Możesz też przesłać [zaawansowane żądanie certyfikatu](#)

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

Usługi certyfikatów *Microsoft* -- brinet Strona główna

---

**Zaawansowane żądanie certyfikatu**

Zasady tego urzędu certyfikacji decydują o typach certyfikatów, jakich możesz żądać. Kliknij jedną z poniższych opcji:  
[Utwórz i prześlij żądanie do tego urzędu certyfikacji](#)  
[Prześlij żądanie certyfikatu, używając pliku CMC lub PKCS #10 szyfrowanego algorytmem base-64 lub prześlij żądanie odnowienia, używając pliku PKCS #7 szyfrowanego algorytmem base-64.](#)  
[Zażądaj certyfikatu dla karty inteligentnej w imieniu innego użytkownika, korzystając ze stacji rejestrowania certyfikatów kart inteligentnych.](#)  
Uwaga: aby przesłać żądanie w imieniu innego użytkownika, musisz mieć certyfikat agenta rejestrowania.

**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.

Usługi certyfikatów *Microsoft* -- brinet

---

### Zaawansowane żądanie certyfikatu

---

Szablon certyfikatu:

Router (żądanie offline) ▼

Informacje identyfikujące dla szablonu trybu offline:

Nazwa: teleworker

E-mail:

Firma:

Dział:

Miasto:

Województwo:

Kraj/region: PL

Opcje klucza:

Tworzenie nowego zestawu kluczy  Użyj istniejącego zestawu kluczy

Dostawca usług kryptograficznych: Microsoft RSA SChannel Cryptographic Provider ▼

Użycie klucza:  Wymiana

Rozmiar klucza: 1024 Min.: 384 Maks.: 16384 (typowe rozmiary kluczy: 512 1024 2048 4096 8192 16384)

Automatyczna nazwa kontenera kluczy  Nazwa kontenera kluczy określona przez użytkownika

Oznacz klucze jako eksportowalne

Zachowaj certyfikat w magazynie certyfikatów komputera lokalnego  
*Zachowuje certyfikat w magazynie komputera lokalnego zamiast w magazynie certyfikatów użytkownika. Nie instaluje certyfikatu głównego urzędu certyfikatów. Musisz być administratorem, aby wygenerować klucz lub używać go w magazynie lokalnego komputera.*

**Krok 5:** Zainstaluj wystawiony certyfikat.

Usługi certyfikatów *Microsoft* -- brinet [Strona główna](#)

---

### Certyfikat został wystawiony

---

Żądany certyfikat został wystawiony.

 [Zainstaluj ten certyfikat](#)

**Krok 6:** Pomyślna próba zainstalowania certyfikatu na PC.

Usługi certyfikatów *Microsoft* -- brinet [Strona główna](#)

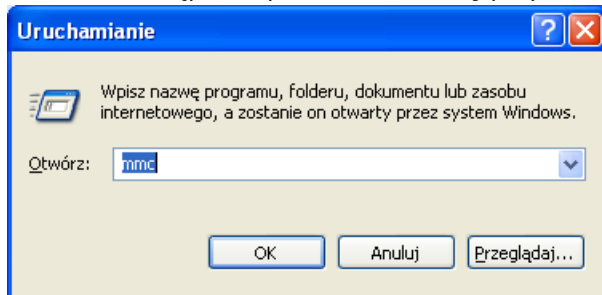
---

### Zainstalowano certyfikat

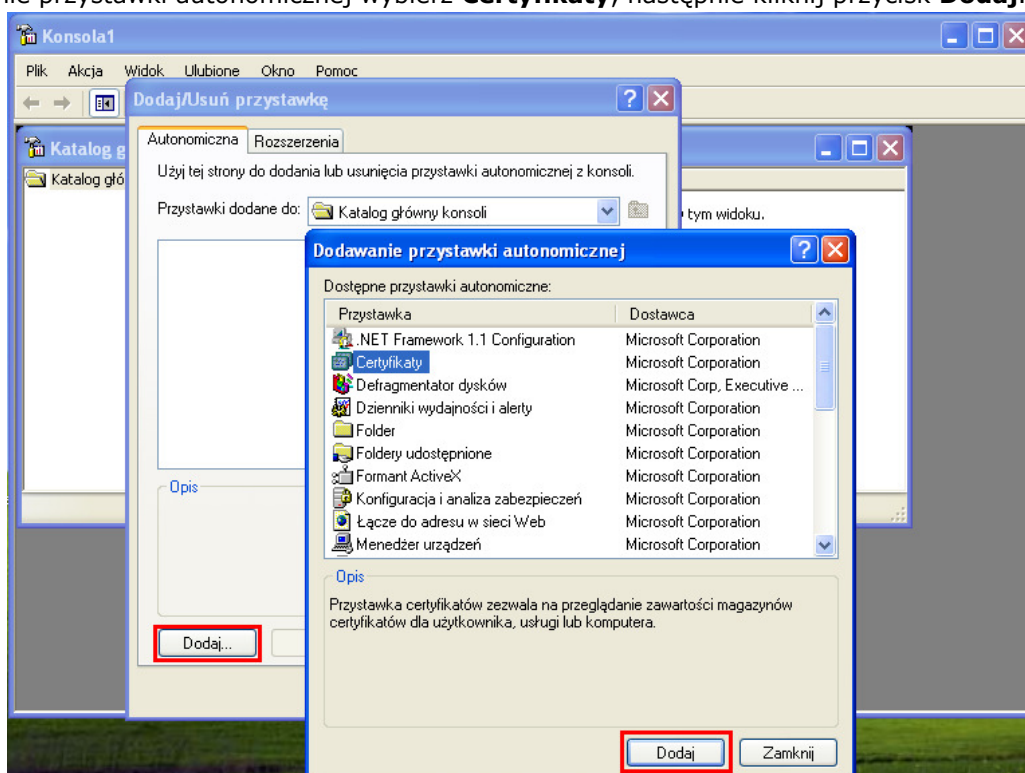
---

Nowy certyfikat został zainstalowany pomyślnie.

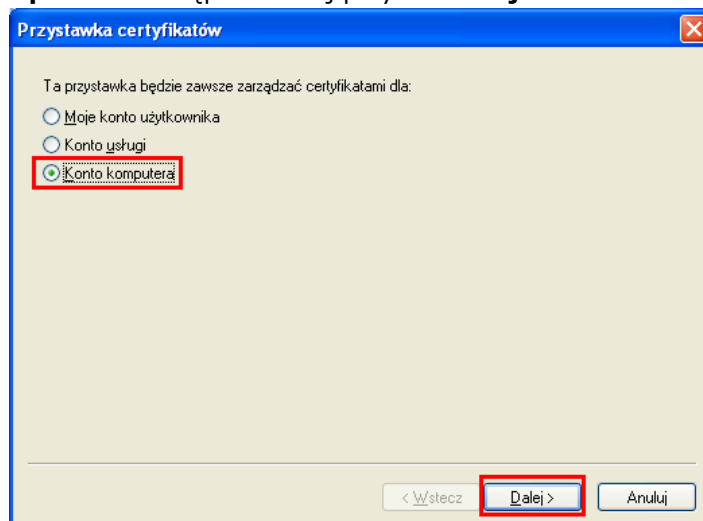
**Krok 7:** Z Menu start wybierz **Uruchom**. Następnie wpisz **mmc** i kliknij przycisk **OK**.



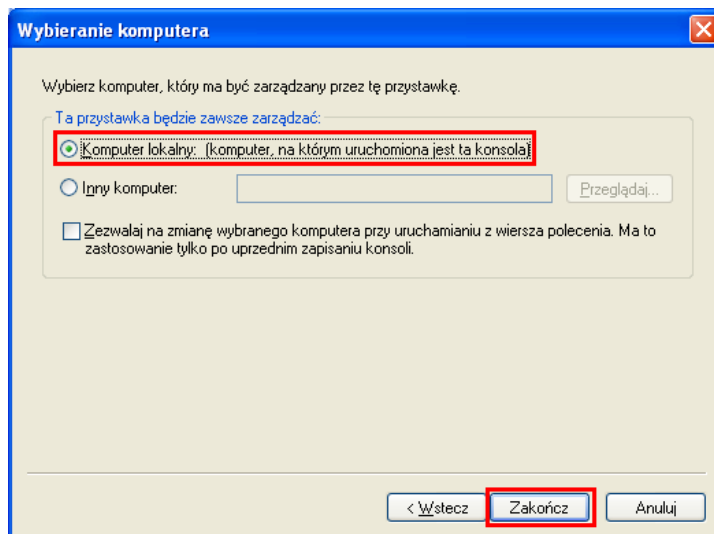
**Krok 8:** Otworzy się Konsola1. Wybierz **Plik->Dodaj/Usuń przystawkę**, następnie kliknij przycisk **Dodaj**. W oknie Dodawanie przystawki autonomicznej wybierz **Certyfikaty**, następnie kliknij przycisk **Dodaj**.



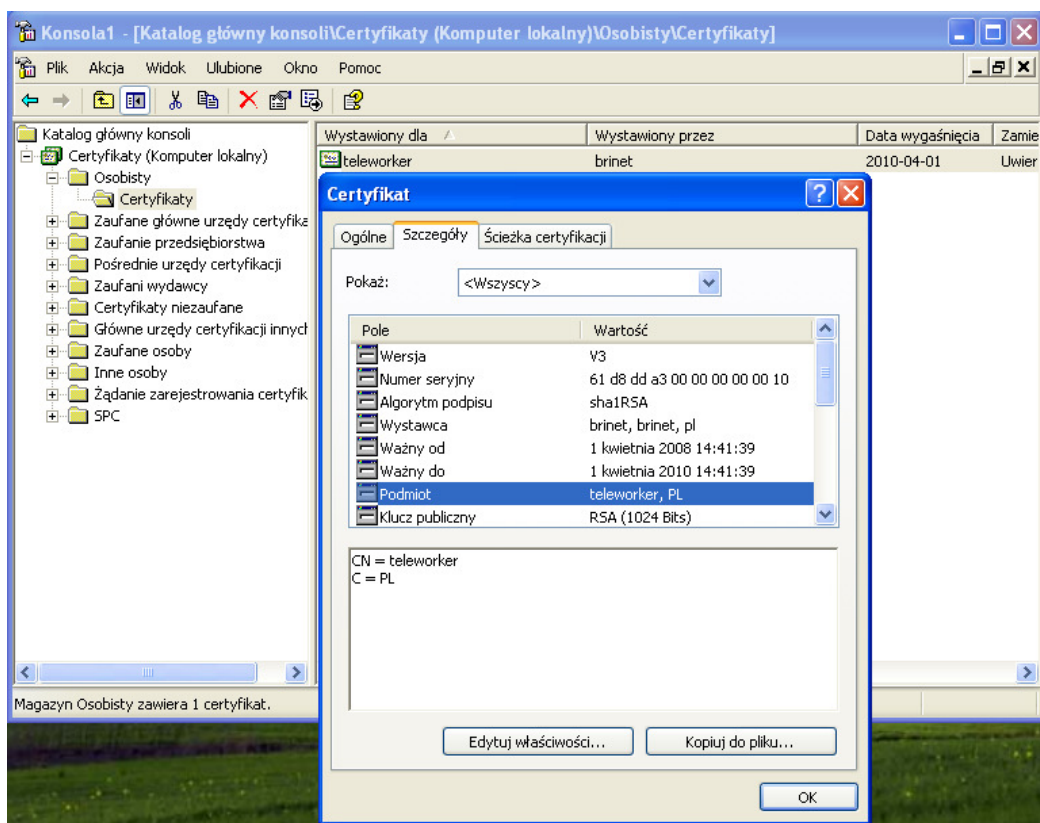
**Krok 9:** Wybierz **Konto komputera**. Następnie kliknij przycisk **Dalej>**.



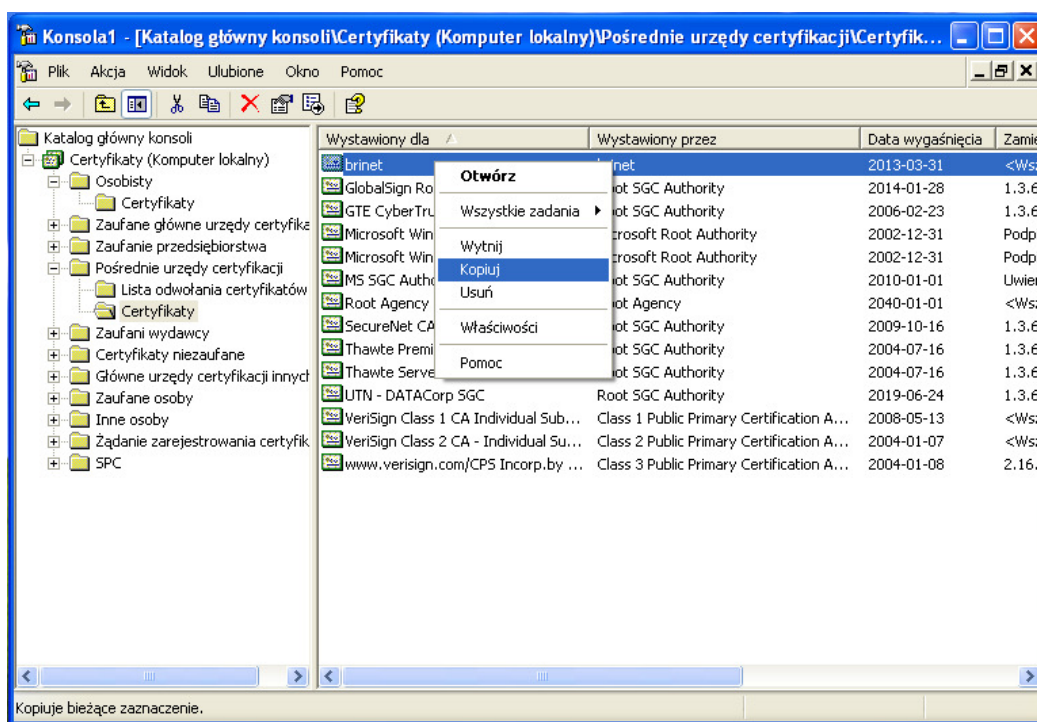
**Krok 10:** Wybierz **Komputer lokalny**. Następnie kliknij przycisk **Zakończ**.



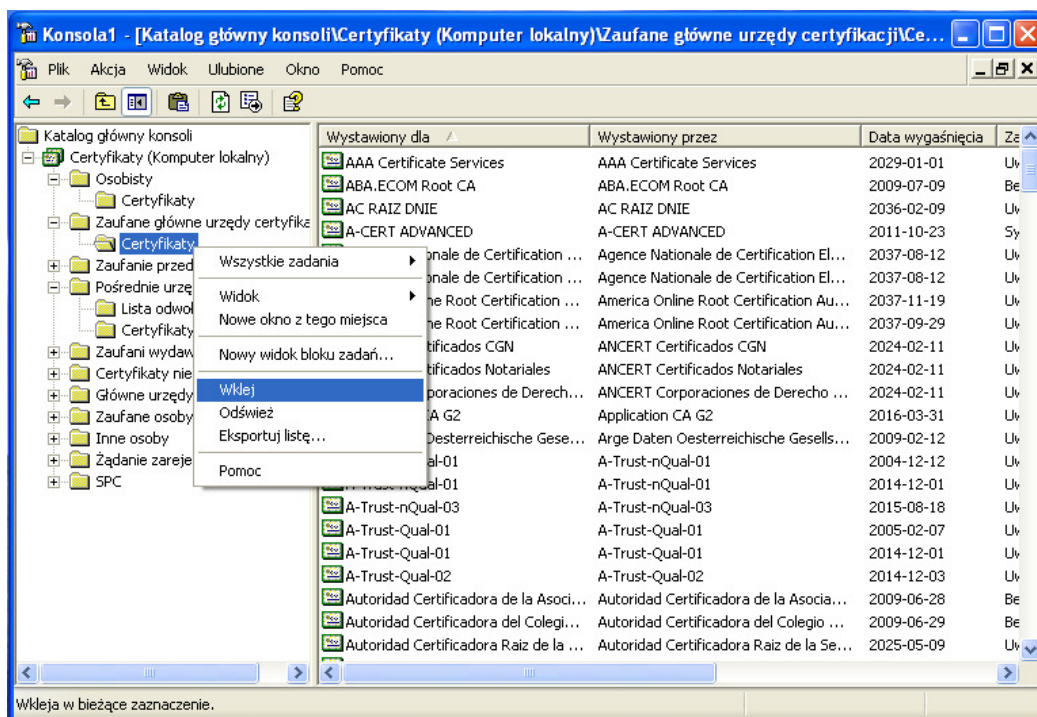
**Krok 11:** Zainstalowany certyfikat znajduje się w **Certyfikaty(komputer lokalny)>>Osobisty>>Certyfikaty**



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

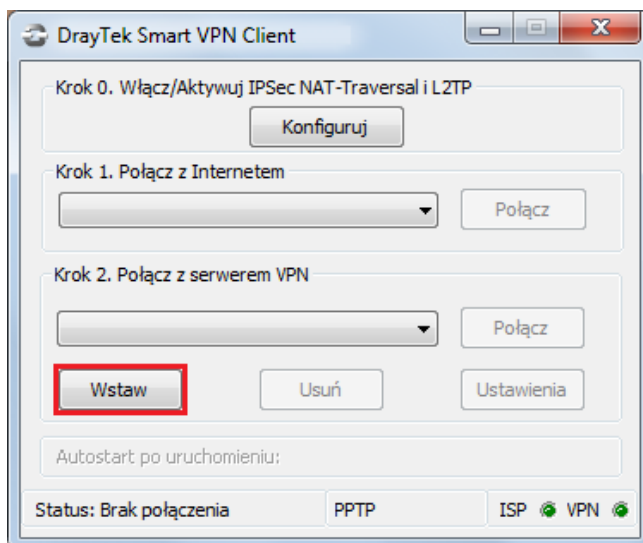


**Krok 13:** Przejdź do **Certyfikaty(komputer lokalny)>>Zaufane główne urzędy certyfikacji>>Certyfikaty i Wklej** odpowiedni certyfikat CA (w przykładzie wykorzystywano certyfikat brinet).



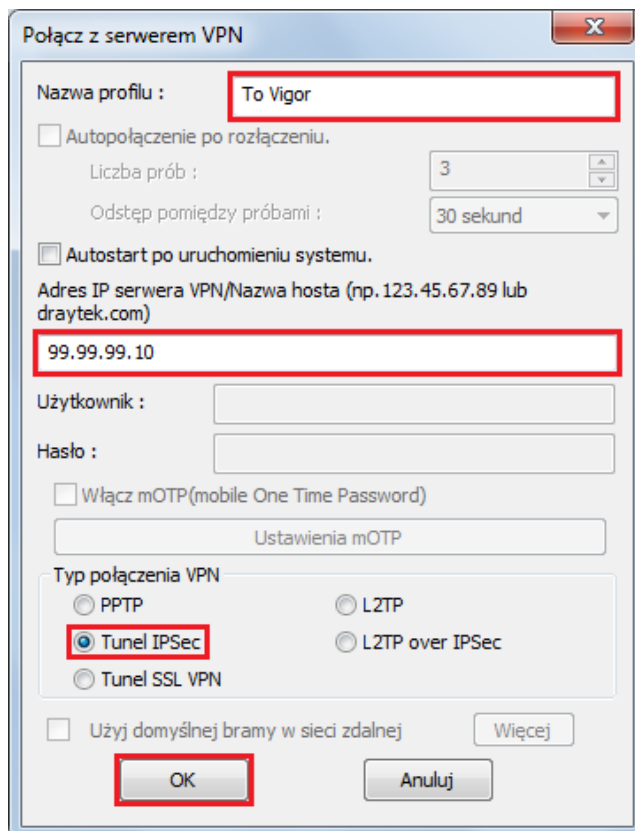
### 2.2 Konfiguracja DrayTek Smart VPN Client

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



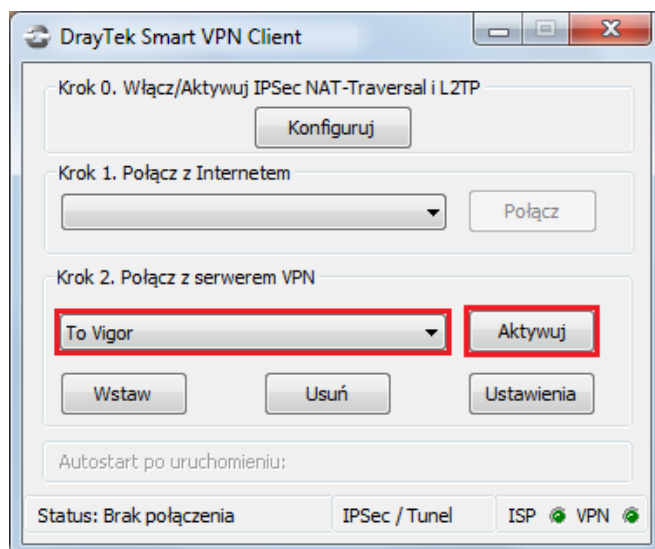


Wypełnij dane dotyczące zabezpieczeń IPSec:

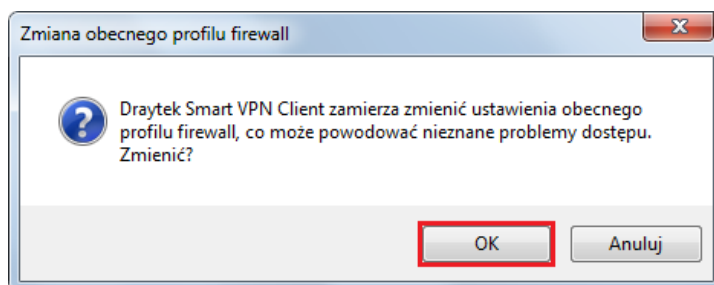
- w polu Mój adres IP wybierz odpowiedni adres IP swojego komputera. W przykładzie 99.99.99.11.
- w polu Typ połączenia IPSec wybierz Standardowy tunel IPSec oraz wpisz adresację zdalnej podsieci. W przykładzie Zdalna podsieć: 192.168.0.0, Maska podsieci zdalnej: 255.255.255.0.
- w polu Metoda zabezpieczeń 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

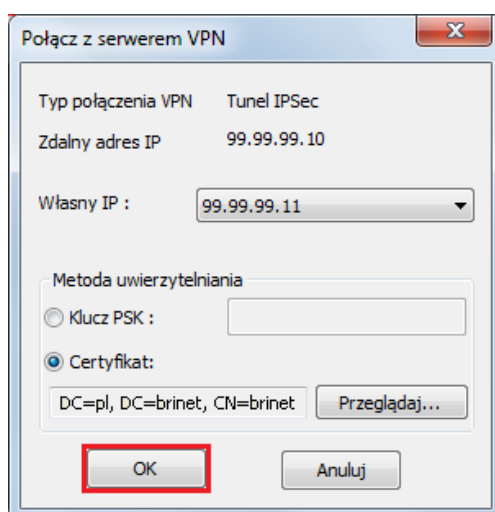
Wybierz odpowiedni profil a następnie kliknij przycisk Aktywuj.



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

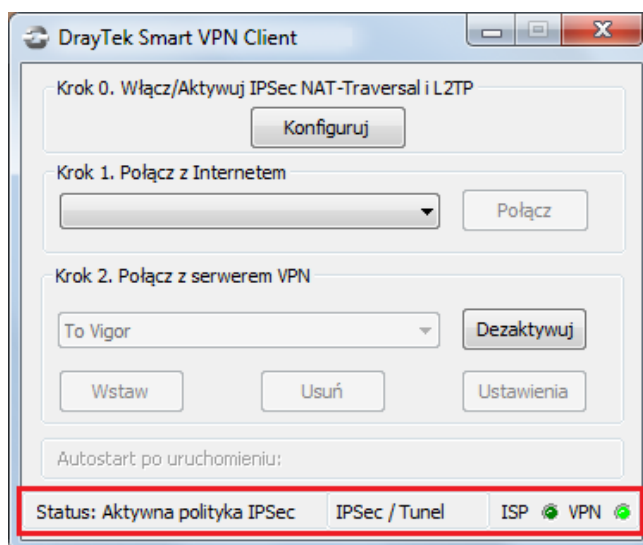


Następnie kliknij OK.





Dla standardowego tunelu IPSec zmieni się status na Aktywna polityka IPSec oraz zapali się zielone światelko 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.
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 błędzenia pakietów w milisekundach:
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).

### VPN i Dostęp Zdalny>> Zarządzanie połączeniem

#### Wymuszanie inicjacji połączeń

Czas odświeżania : 10

Tryb Główny:	<input type="text"/>	<input type="button" value="Inicjuj"/>
Tryb Backup:	<input type="text"/>	<input type="button" value="Inicjuj"/>

#### Stan połączenia VPN

Bieżąca strona: 1

Nr strony

VPN	Typ	Zdalny IP	Sieć wirtualna	Tx pakietów	Tx prędkość	Rx pakietów	Rx predkość	Czas akt.	
1	IPSec Tunnel	99.99.99.11	99.99.99.11/32	281	9830	234	1601	0:0:53	<input type="button" value="Rozłącz"/>

xxxxxxx : Dane są szyfrowane.

xxxxxxx : Dane nie są szyfrowane.