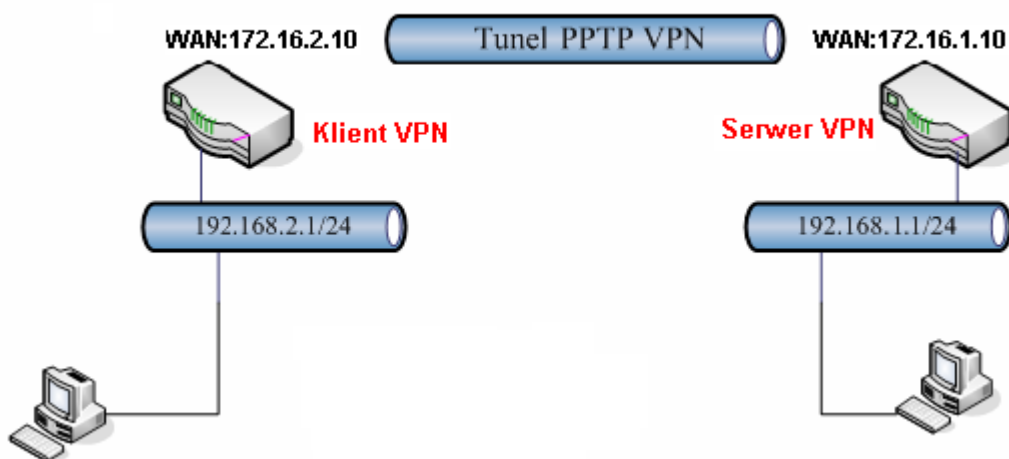


1. Konfiguracja serwera VPN
2. Konfiguracja klienta VPN
3. Status połączenia

Procedura konfiguracji została oparta na poniższym przykładzie.



Główne założenia:

- typ tunelu: LAN-LAN z routingiem pomiędzy podsieciami
- protokół VPN: PPTP
- Adres IP Serwera VPN: statyczny. W przykładzie 172.16.1.10
- Adres IP Klienta VPN: statyczny lub dynamiczny. W przykładzie 172.16.2.10
- 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. Konfiguracja serwera VPN

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

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
<input type="checkbox"/>	Włącz dostęp ISDN

Przejdź do zakładki **VPN i Dostęp Zdalny>>Połączenia LAN-LAN**. Stwórz odpowiedni profil do obsługi tunelu (w przykładzie użyto profilu 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**. Domyślnie jest tam wartość 300 oznaczająca rozłączenie tunelu po 5 minutach, gdy Vigor nie odnotuje ruchu VPN. Wpisz **0** w polu czas nieaktywności jeśli Vigor ma pozostawić połączenie pomimo braku ruchu. PPTP posiada wbudowane mechanizmy detekcji połączenia.

#### 1. Ustawienia ogólne

Nazwa profilu <input type="text" value="od 2910"/> <input checked="" type="checkbox"/> Włącz profil	Kierunek inicjacji <input type="radio"/> Oba <input type="radio"/> Dial-Out <input checked="" type="radio"/> Dial-In <input type="checkbox"/> Zawsze aktywne Czas nieaktywności <input type="text" value="0"/> sek <input type="checkbox"/> Użyj PING dla podtrzymania PING na IP <input type="text"/>
Połączenie VPN przez: <input type="text" value="WAN1 najpierw"/> Nazwy NetBIOS <input checked="" type="radio"/> Przepuść <input type="radio"/> Blokuj	

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

- w polu Protokół dla połączenia wybierz **PPTP**
- w polu **Użytkownik** wpisz odpowiednią nazwę użytkownika. W przykładzie użyto użytkownika 'test'
- w polu **Hasło** wpisz odpowiednie hasło. W przykładzie użyto hasła 'test'

### 3. Ustawienia Dial-In (odbiór wywołania z innego routera)

**Akceptowane protokoły**

- ISDN
- PPTP
- Tunel IPsec
- L2TP z polisą IPsec Brak ▾

Określ Zdalna brama VPN  
 IP zdalnego serwera   
 lub ID

Użytkownik   
 Hasło   
 Kompresja VJ  Włącz  Wyłącz

**Tryb uwierzytelniania IKE**

- Klucz IKE  
 Klucz IKE
- Podpis cyfrowy (cert. X.509)  
 Brak ▾

**Poziom zabezpieczeń IPsec**

- Średni(AH)
- Wysoki(ESP)
  - DES
  - 3DES
  - AES

- jeżeli chcesz dodatkowo weryfikować adres IP inicjującego połączenie zaznacz opcję **Określ Zdalna brama VPN**, a w polu **IP zdalnego serwera** wpisz odpowiedni adres IP klienta VPN. W przykładzie 172.16.2.10.

Określ Zdalna brama VPN  
 IP zdalnego serwera  
  
 lub ID

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

### 4. Adresacja i routing oraz NAT wewnątrz połączenia

Własny WAN IP <input type="text" value="0.0.0.0"/> IP zdalnej bramy <input type="text" value="0.0.0.0"/> IP zdalnej podsieci <input type="text" value="192.168.2.0"/> Maska zdalnej podsieci <input type="text" value="255.255.255.0"/> <div style="text-align: right; margin-top: 5px;"><input type="button" value="Więcej podsieci"/></div>	RIP dla VPN <span style="float: right;">Wyłącz ▾</span> Z lokalnej podsieci do zdalnej podsieci, wykonaj <span style="float: right;">Routing ▾</span>
<input type="checkbox"/> Zmień trasę domyślną do tego tunelu VPN ( Tylko dla pojedynczego WANu )	

#### Uwaga!!!

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

IP zdalnej podsieci	<input type="text" value="192.168.2.0"/>
Maska zdalnej podsieci	<input type="text" value="255.255.255.0"/>
IP lokalnej podsieci	<input type="text" value="192.168.1.1"/>
Maska lokalnej podsieci	<input type="text" value="255.255.255.0"/>

### 2. Konfiguracja klienta VPN

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

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
<input type="checkbox"/>	Włącz dostęp ISDN

Przejdź do zakładki **VPN i Dostęp Zdalny >> Połączenia LAN-LAN**. Stwórz odpowiedni profil do obsługi tunelu (w przykładzie użyto profilu 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** - ustawisz **czas nieaktywności -1**, gdy połączenie ma być aktywne cały czas.

1. Ustawienia ogólne

Nazwa profilu: do 5500	Kierunek inicjacji: <input type="radio"/> Oba <input checked="" type="radio"/> Dial-Out <input type="radio"/> Dial-In
<input checked="" type="checkbox"/> Włącz profil	<input checked="" type="checkbox"/> Zawsze aktywne
Połączenie VPN przez: WAN1 najpierw	Czas nieaktywności: -1 sek
	<input type="checkbox"/> Użyj PING dla podtrzymania
	PING na IP: <input type="text"/>

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

- w polu Protokół dla połączenia wybierz **PPTP**
- w polu **IP/nazwa DNS serwera VPN** wpisz adres IP routera, do którego zestawiasz tunel VPN, albo jego nazwę. W przykładzie użyto adresu IP 172.16.1.10
- w polu **Użytkownik** wpisz odpowiednią nazwę użytkownika. W przykładzie użyto użytkownika 'test'
- w polu **Hasło** wpisz odpowiednie hasło. W przykładzie użyto hasła 'test'

2. Ustawienia Dial-Out (inicjacja do innego routera)

<b>Protokół dla połączenia</b> <input type="radio"/> ISDN <input checked="" type="radio"/> PPTP <input type="radio"/> Tunel IPsec <input type="radio"/> L2TP z polisą IPsec <input type="text" value="Brak"/>	Typ łącza ISDN: 64k bps Użytkownik: test Hasło: ●●●● Uwierzytelnianie PPP: PAP/CHAP Kompresja VJ: <input checked="" type="radio"/> Włącz <input type="radio"/> Wyłącz
Numer docelowy (dla ISDN) IP/nazwa DNS serwera VPN. (np. 5551234, draytek.com lub 123.45.67.89) 172.16.1.10	<b>Tryb uwierzytelniania IKE</b> <input checked="" type="radio"/> Klucz IKE Klucz IKE: <input type="text"/> <input type="radio"/> Podpis cyfrowy (cert. X.509) Brak
<b>Poziom zabezpieczeń IPsec</b> <input checked="" type="radio"/> Średni(AH) <input type="radio"/> Wysoki (ESP) DES bez autentykacji <input type="button" value="Zaawansowane"/>	

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. Adresacja i routing oraz NAT wewnątrz połączenia

Własny WAN IP	<input type="text" value="0.0.0.0"/>	RIP dla VPN	<input type="text" value="Wyłącz"/>
IP zdalnej bramy	<input type="text" value="0.0.0.0"/>	<input checked="" type="checkbox"/> Z lokalnej podsieci do zdalnej podsieci, wykonaj	
IP zdalnej podsieci	<input type="text" value="192.168.1.0"/>	<input type="text" value="Routing"/>	
Maska zdalnej podsieci	<input type="text" value="255.255.255.0"/>	<input type="checkbox"/> Zmień trasę domyślną do tego tunelu VPN ( Tylko dla pojedynczego WANu )	
<input type="button" value="Więcej podsieci"/>			

### 3. Status połączenia (od strony klienta VPN)

O tym, czy tunel został zainicjowany, możesz 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: ( do 5500 ) 172.16.1.10

Tryb Backup:

**Stan połączenia VPN**

Bieżąca strona: 1 Nr strony

VPN	Typ	Zdalny IP	Sieć wirtualna	Tx pakietów	Tx prędkość	Rx pakietów	Rx prędkość	Czas akt.	
1 ( do 5500 )	PPTP/MPPE	172.16.1.10	192.168.1.0/24	418	3	398	14	0:8:10	<input type="button" value="Rozłącz"/>

xxxxxxx : Dane są szyfrowane.  
xxxxxxx : nie są szyfrowane.

Inna metoda 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.

```
C:\>ping 192.168.1.10

Badanie 192.168.1.10 z użyciem 32 bajtów danych:

Odpowiedź z 192.168.1.10: bajtów=32 czas=3ms TTL=126
Odpowiedź z 192.168.1.10: bajtów=32 czas=3ms TTL=126
Odpowiedź z 192.168.1.10: bajtów=32 czas=3ms TTL=126
Odpowiedź z 192.168.1.10: bajtów=32 czas=3ms TTL=126

Statystyka badania ping dla 192.168.1.10:
    Pakiety: Wysłane = 4, Odebrane = 4, Utracone = 0 (0% strat),
Szacunkowy czas błędzenia pakietów w milisekundach:
    Minimum = 3 ms, Maksimum = 3 ms, Czas średni = 3 ms
```

Krzysztof Skowina  
Specjalista ds. rozwiązań sieciowych  
BRINET Sp. z o.o.  
[k.skowina@brinet.pl](mailto:k.skowina@brinet.pl)