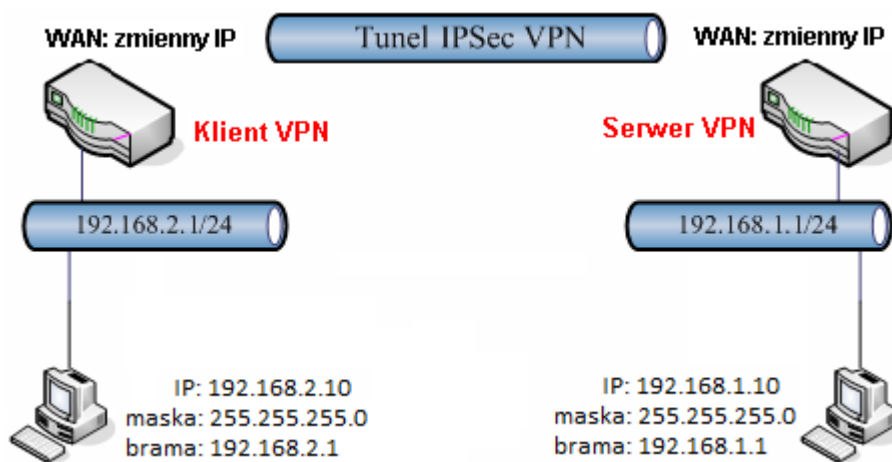


1. Konfiguracja serwera VPN
2. Konfiguracja klienta VPN
3. Status połączenia

Procedura konfiguracji została oparta na poniższym przykładzie.



Główne założenia:

- typ tunelu: LAN-LAN z routingiem pomiędzy podsieciami
- protokół VPN: IPSec
- szyfrowanie: AES
- integralność: SHA1 lub MD5
- autentykacja: klucz IKE
- aktywność tunelu: zawsze
- serwer VPN oraz klient VPN wspierają DPD dla IPSec
- 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 **Aplikacje>>Ustawienia Dynamicznego DNS**. Zarejestruj odpowiednie konto. W przykładzie użyto konta 'vigortest.no-ip.org'.

Aplikacje >> Ustawienia Dynamicznego DNS

Ustawienia Dynamicznego DNS | [Ustawienia domyślne](#)

Włącz Dynamiczny DNS Pokaż Log Wymuś aktualizację

Accounts:

Indeks	Interfejs WAN	Nazwa domeny	Aktywne
1.	WAN1 Najpierw	vigortest.no-ip.org	v
2.	WAN1 Najpierw	.	x
3.	WAN1 Najpierw	.	x

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.

VPN i Dostęp Zdalny>> Protokoły VPN

Protokoły VPN

Włącz obsługę PPTP

Włącz obsługę IPSec

Włącz obsługę L2TP

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. IPSec nie posiada wbudowanych mechanizmów detekcji połączenia – detekcja połączenia realizowana jest za pomocą DPD (Dead Peer Detection).

1. Ustawienia ogólne

Nazwa profilu: Włącz profil

Połączenie VPN przez:

Kierunek inicjacji: Oba Dial-Out Dial-In

Zawsze aktywne

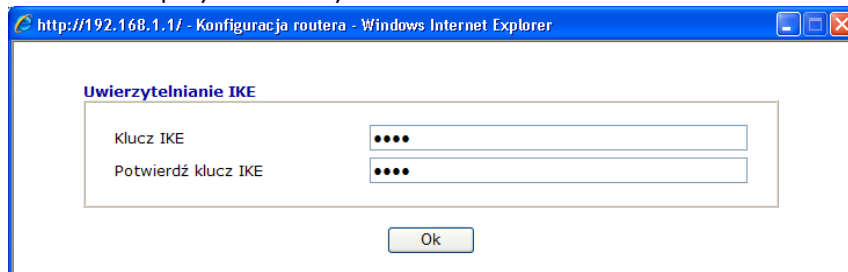
Czas nieaktywności: sek

Użyj PING dla podtrzymania

PING na IP:

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

- w polu Protokół dla połączenia wybierz **Tunel IPSec**
- zaznacz **Określ Zdalna brama VPN** i w polu **ID** wpisz odpowiedni identyfikator. W przykładzie użyto 'IDtest'.
- w polu Tryb uwierzytelniania IKE wybierz **Klucz IKE**. Kliknij przycisk Klucz IKE – pojawi się okno, w które wpisz odpowiedni klucz. W przykładzie użyto klucza 'test'



- w polu Poziom zabezpieczeń IPSec wybierz **AES**.

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

<p>Akceptowane protokoły</p> <p><input type="checkbox"/> PPTP</p> <p><input checked="" type="checkbox"/> Tunel IPSec</p> <p><input type="checkbox"/> L2TP z polisą IPSec Brak</p>	<p>Użytkownik <input data-bbox="1050 824 1257 857" type="text" value="???"/></p> <p>Hasło <input data-bbox="1050 869 1257 902" type="text"/></p> <p>Kompresja VJ <input checked="" type="radio"/> Włącz <input type="radio"/> Wylącz</p>
<p><input checked="" type="checkbox"/> Określ Zdalna brama VPN</p> <p>IP zdalnego serwera <input data-bbox="308 1037 515 1070" type="text"/></p> <p>lub ID <input data-bbox="308 1081 571 1115" type="text" value="IDtest"/></p>	<p>Tryb uwierzytelniania IKE</p> <p><input checked="" type="checkbox"/> Klucz IKE</p> <p>Klucz IKE <input data-bbox="1050 1037 1177 1070" type="text" value="....."/></p> <p><input type="checkbox"/> Podpis cyfrowy (cert. X.509)</p> <p>Brak</p>
	<p>Poziom zabezpieczeń IPSec</p> <p><input type="checkbox"/> Średni(AH)</p> <p>Wysoki(ESP)</p> <p><input type="checkbox"/> DES <input type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES</p>

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

<p>Własny WAN IP <input data-bbox="555 1462 730 1496" type="text" value="0.0.0.0"/></p> <p>IP zdalnej bramy <input data-bbox="555 1507 730 1541" type="text" value="0.0.0.0"/></p> <p><input checked="" type="checkbox"/> IP zdalnej podsieci <input data-bbox="555 1552 730 1585" type="text" value="192.168.2.0"/></p> <p><input checked="" type="checkbox"/> Maska zdalnej podsieci <input data-bbox="555 1597 730 1630" type="text" value="255.255.255.0"/></p> <p>IP lokalnej podsieci <input data-bbox="555 1641 730 1675" type="text" value="192.168.1.0"/></p> <p>Maska lokalnej podsieci <input data-bbox="555 1686 730 1720" type="text" value="255.255.255.0"/></p> <p><input data-bbox="555 1709 730 1742" type="button" value="Więcej podsieci"/></p>	<p>RIP dla VPN Wyłącz</p> <p>Z lokalnej podsieci do zdalnej podsieci, wykonaj Routing</p> <p><input type="checkbox"/> Zmień trasę domyślną do tego tunelu VPN (Tylko dla pojedynczego WANu)</p>
--	---

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 IPSec. 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

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 **Zwykłe ustawienia (Ustawienia ogólne)** zgodna z założeniami przykładu:

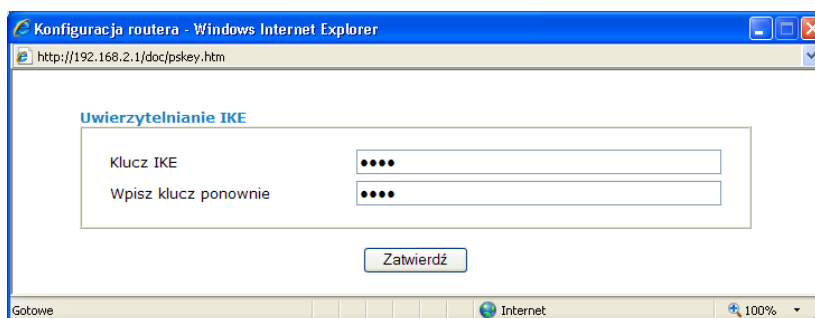
- wpisz dowolną nazwę profilu
- zaznacz **Włącz profil**
- jako kierunek inicjacji wybierz **Dial-Out**
- zaznacz **Zawsze aktywne** - ustawisz **czas nieaktywności -1**, gdy połączenie ma być aktywne cały czas.

Zwykłe ustawienia

Nazwa profilu	do 2820
<input checked="" type="checkbox"/> Włącz profil	
Kierunek inicjacji	<input type="radio"/> Oba <input checked="" type="radio"/> Dial-Out <input type="radio"/> Dial-In
	<input checked="" type="checkbox"/> Zawsze aktywne
Czas nieaktywności	-1 sek
<input type="checkbox"/> Użyj PING dla podtrzymania	
PING na IP	

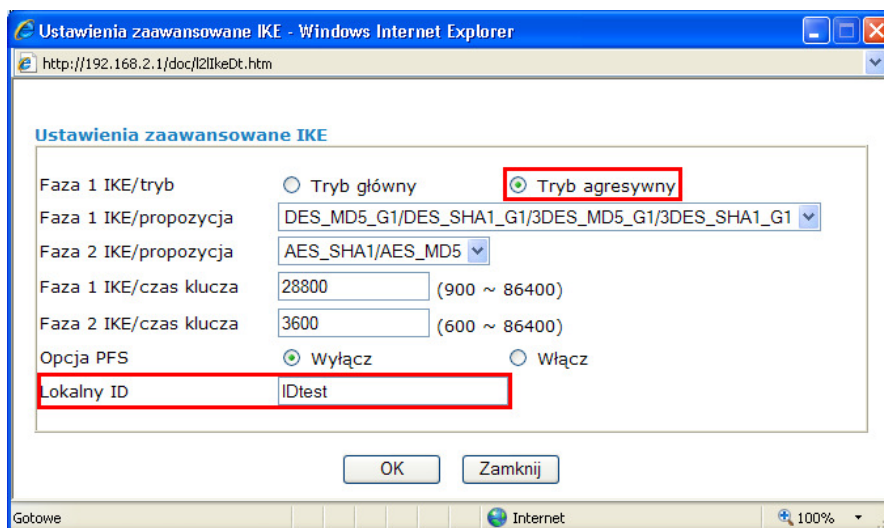
Konfiguracja części **Ustawienia Dial-Out** zgodna z założeniami przykładu:

- w polu Protokół dla połączenia wybierz **Tunel IPSec**
- w polu **IP/nazwa DNS serwera VPN** wpisz adres IP routera, do którego zestawiasz tunel VPN, albo jego nazwę. W przykładzie użyto `vigortest.no-ip.org`
- w polu Tryb uwierzytelniania IKE wybierz **Klucz IKE**. Kliknij przycisk **Klucz IKE** – pojawi się okno, w które wpisz odpowiedni klucz. W przykładzie użyto klucza 'test'



- w polu Poziom zabezpieczeń IPSec wybierz protokół realizujący szyfrowanie i uwierzytelnianie **Wysoki(ESP)**. W przykładzie użyto AES z autentykacją. Kliknij przycisk **Zaawansowane** – pojawi się

okno, w którym możesz zmodyfikować Ustawienia zaawansowane IKE. Wybierz **Tryb agresywny** i wpisz **Lokalny ID** (w przykładzie użyto 'IDtest').



Ustawienia Dial-Out (inicjacja do innego routera)

Protokół dla połączenia <input type="radio"/> PPTP <input checked="" type="radio"/> Tunel IPSec <input type="radio"/> L2TP z polisą IPsec Brak		Użytkownik <input type="text" value="???"/> Hasło <input type="text"/> Uwierzytelnianie PPP PAP/CHAP Kompresja VJ <input checked="" type="radio"/> Włącz <input type="radio"/> Wyłącz
IP/nazwa DNS serwera VPN. (np. dyndns.com lub 123.45.67.89) <input type="text" value="vigortest.no-ip.org"/>		Tryb uwierzytelniania IKE <input checked="" type="radio"/> Klucz IKE <input type="text" value="....."/> <input type="radio"/> Podpis cyfrowy (cert. X.509) <input type="text" value="???"/>
		Poziom zabezpieczeń IPsec <input type="radio"/> Średni(AH) <input checked="" type="radio"/> Wysoki(ESP) AES z autentykacją <input type="button" value="Zaawansowane"/>

Konfiguracja części **Ustawienia sieci TCP/IP** zgodna z założeniami przykładu:

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

Ustawienia sieci TCP/IP

Własny WAN IP <input type="text" value="0.0.0.0"/> IP zdalnej bramy <input type="text" value="0.0.0.0"/> <input checked="" type="checkbox"/> IP zdalnej podsieci <input type="text" value="192.168.1.0"/> <input checked="" type="checkbox"/> Maska zdalnej podsieci <input type="text" value="255.255.255.0"/> IP lokalnej podsieci <input type="text" value="192.168.2.0"/> Maska lokalnej podsieci <input type="text" value="255.255.255.0"/> <input type="button" value="Więcej podsieci"/>	RIP dla VPN Wyłącz <input checked="" type="checkbox"/> Z lokalnej podsieci do zdalnej podsieci, wykonaj <input type="text" value="Routing"/> <input type="checkbox"/> Zmień trasę domyślną do tego tunelu VPN (Tylko dla pojedynczego WANu)
---	---

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

Stan połączenia VPN

Bieżąca strona: 1

VPN	Typ	Zdalny IP	Sieć wirtualna	Tx pakietów	Tx prędkość	Rx pakietów	Rx prędkość	Czas akt.
1	IPSec Tunnel (do 2820) AES-SHA1 Auth	79.184.8.178	192.168.1.0/24	145	498	125	75	0 : 1 : 10

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

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.

```
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% straty),
Szacunkowy czas błędzenia pakietów w milisekundach:
    Minimum = 3 ms, Maksimum = 3 ms, Czas średni = 3 ms
```

Krzysztof Skowina
 Specjalista ds. rozwiązań sieciowych
k.skowina@brinet.pl