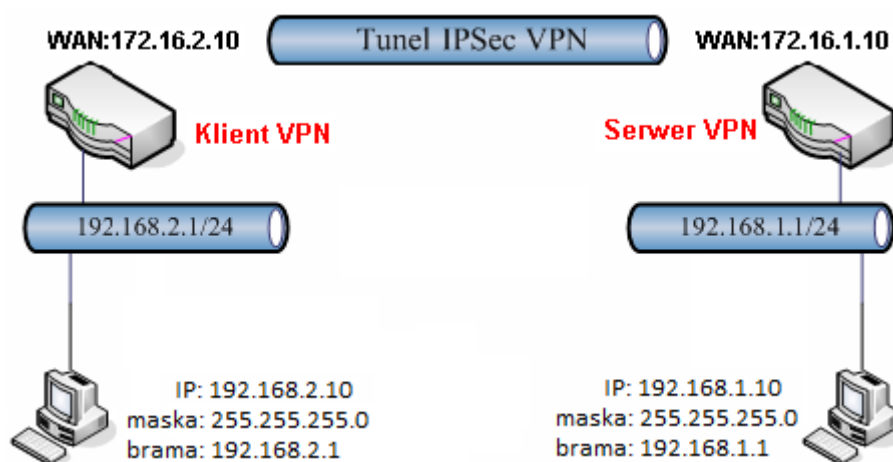


1. Konfiguracja serwera VPN
2. Konfiguracja klienta VPN
3. Status połączenia

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

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 **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)

Akceptowane protokoły <input type="checkbox"/> PPTP <input checked="" type="checkbox"/> Tunel IPSec <input type="checkbox"/> L2TP z polisą IPSec Brak		Użytkownik <input type="text" value="???"/> Hasło <input type="password"/> Kompresja VJ <input checked="" type="radio"/> Włącz <input type="radio"/> Wyłącz
<input checked="" type="checkbox"/> Określ Zdalna brama VPN IP zdalnego serwera <input type="text" value="172.16.2.10"/> lub ID <input type="text"/>		Tryb uwierzytelniania IKE <input checked="" type="checkbox"/> Klucz IKE <input type="text" value="....."/> <input type="checkbox"/> Podpis cyfrowy (cert. X.509) <input type="text" value="Brak"/>
		Poziom zabezpieczeń IPSec <input type="checkbox"/> Średni(AH) Wysoki(ESP) <input type="checkbox"/> DES <input type="checkbox"/> 3DES <input checked="" type="checkbox"/> 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

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"/> <input checked="" type="checkbox"/> IP zdalnej podsieci <input type="text" value="192.168.2.0"/> <input checked="" type="checkbox"/> Maska zdalnej podsieci <input type="text" value="255.255.255.0"/> IP lokalnej podsieci <input type="text" value="192.168.1.0"/> Maska lokalnej podsieci <input type="text" value="255.255.255.0"/> <input type="button" value="Więcej podsieci"/>	RIP dla VPN <input type="text" value="Wyłącz"/> 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)
---	--

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 **Ustawienia ogólne** zgodna z założeniami przykładu:

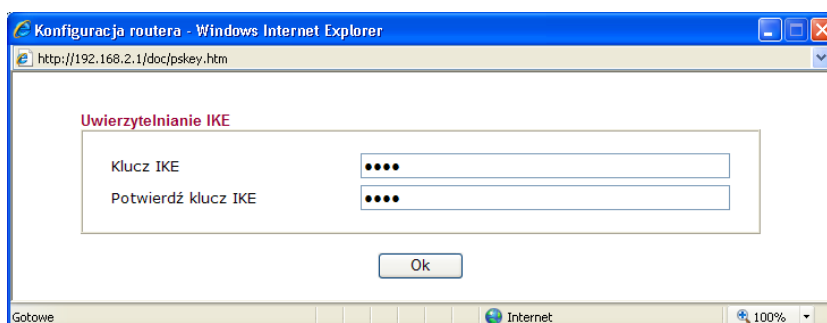
- wpisz dowolną nazwę profilu
- zaznacz **Włącz profil**
- jako kierunek inicjacji wybierz **Dial-Out**
- zaznacz **Zawsze aktywne** - ustawisz **czas nieaktywności -1**, gdy połączenie ma być aktywne cały czas.

1. Ustawienia ogólne

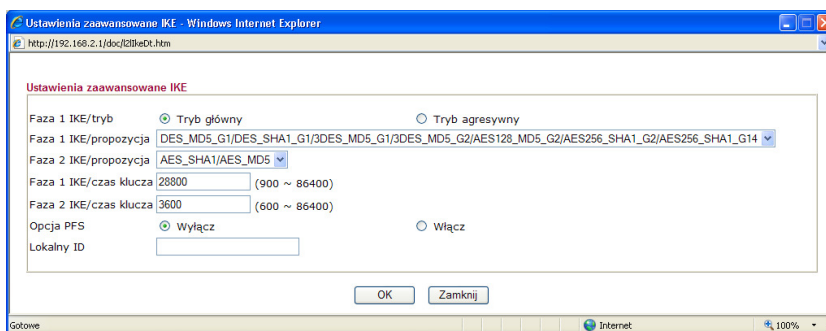
Nazwa profilu: do 5500	Kierunek inicjacji: <input type="radio"/> Oba <input checked="" type="radio"/> Dial-Out <input type="radio"/> Dial-In
<input checked="" type="checkbox"/> Włącz profil	<input checked="" type="checkbox"/> Zawsze aktywne
Połączenie VPN przez: WAN1 najpierw	Czas nieaktywności: -1 sek
	<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 **Tunel IPSec**
- w polu **IP/nazwa DNS serwera VPN** wpisz adres IP routera, do którego zestawiasz tunel VPN, albo jego nazwę. W przykładzie adres IP 172.16.1.10
- 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.



2. 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 <input type="text" value="Brak"/>		Użytkownik <input type="text" value="???"/> Hasło <input type="text"/> Uwierzytelnianie PPP <input type="text" value="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) <input type="text" value="172.16.1.10"/>		Tryb uwierzytelniania IKE <input checked="" type="radio"/> Klucz IKE <input type="text" value="Klucz IKE"/> <input type="text" value="....."/> <input type="radio"/> Podpis cyfrowy (cert. X.509) <input type="text" value="Brak"/>
		Poziom zabezpieczeń IPSec <input type="radio"/> Średni(AH) <input checked="" type="radio"/> Wysoki (ESP) <input type="text" value="AES z autentykacją"/> <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"/> IP zdalnej bramy <input type="text" value="0.0.0.0"/> <input checked="" type="text" value="192.168.1.0"/> <input checked="" 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 <input type="text" value="Wyłącz"/> <input checked="" type="text" value="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

Tryb Główny:	(do 5500) 172.16.1.10	<input type="button" value="Inicjuj"/>
Tryb Backup:		<input type="button" value="Inicjuj"/>

Stan połączenia VPN Nr strony

Bieżąca strona: 1

VPN	Typ	Zdalny IP	Sieć wirtualna	Tx pakietów	Tx predkość	Rx pakietów	Rx predkość	Czas
1	IPSec Tunnel (do 5500) AES-SHA1 Auth	172.16.1.10	192.168.1.0/24	61	60	63	60	0:1:4

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.

```
G:\>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
k.skowina@brinet.pl