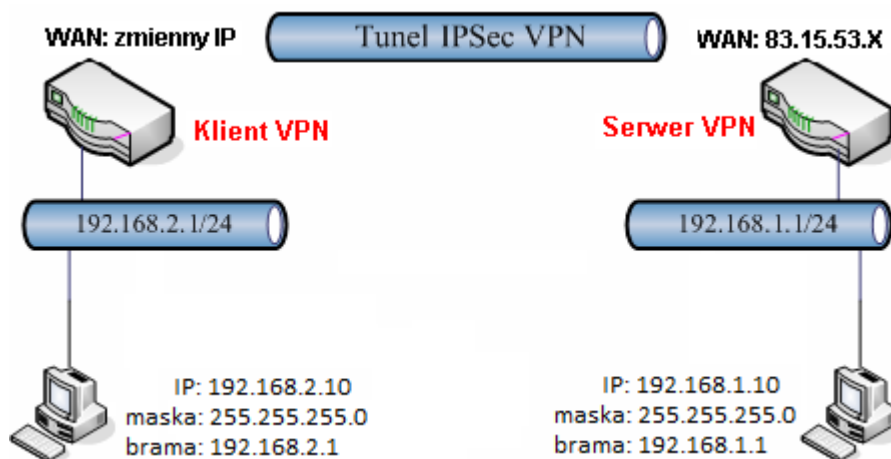


1. Konfiguracja serwera VPN
2. Konfiguracja klienta VPN
3. Status połączenia

Procedura konfiguracji została oparta na poniższym przykładzie.



Główne założenia:

- typ tunelu: LAN-LAN z routowaniem 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

☒	Włącz obsługę PPTP
☒	Włącz obsługę IPSec
☒	Włącz obsługę L2TP
☐	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. IPSec nie posiada wbudowanych mechanizmów detekcji połączenia – detekcja połączenia realizowana jest za pomocą DPD (Dead Peer Detection).

1. Ustawienia ogólne

Nazwa profilu od 2820 ☒ Włącz profil	Kierunek inicjacji ☐ Oba ☐ Dial-Out ☒ Dial-In ☐ Zawsze aktywne Czas nieaktywności 0 sek ☐ Użyj PING dla podtrzymania PING na IP
Połączenie VPN przez: WAN1 najpierw Nazwy NetBIOS ☒ Przepuść ☐ Blokuj	

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 **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'

Uwierzytelnianie IKE

Klucz IKE

Potwierdź klucz IKE

Ok

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

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

Akceptowane protokoły ☒ ISDN ☐ PPTP ☒ Tunel IPSec ☐ L2TP z polisą IPSec Brak	Użytkownik ??? Hasło Kompresja VJ ☒ Włącz ☐ Wyłącz
☒ Określ Zdalna brama VPN IP zdalnego serwera lub ID IDtest	Tryb uwierzytelniania IKE ☒ Klucz IKE Klucz IKE ☐ Podpis cyfrowy (cert. X.509) Brak
Poziom zabezpieczeń IPSec ☐ Średni(AH) Wysoki(ESP) ☐ DES ☐ 3DES ☒ 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 0.0.0.0 IP zdalnej bramy 0.0.0.0 ☒ IP zdalnej podsieci 192.168.2.0 ☒ Maska zdalnej podsieci 255.255.255.0 Więcej podsieci	RIP dla VPN Wyłącz Z lokalnej podsieci do zdalnej podsieci, wykonaj Routing ☐ 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	192.168.2.0
Maska zdalnej podsieci	255.255.255.0
IP lokalnej podsieci	192.168.1.1
Maska lokalnej podsieci	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 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
☐	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 ☒ Włącz profil	Kierunek inicjacji: ☐ Oba ☒ Dial-Out ☐ Dial-In
Połączenie VPN przez: WAN1 najpiew	☒ Zawsze aktywne Czas nieaktywności: -1 sek ☐ 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 adres IP 83.15.53.X
- 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'

Uwierzytelnianie IKE

Klucz IKE:

Potwierdź klucz IKE:

Ok

- 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').

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

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

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 Nr strony >>

Bieżąca strona: 1

VPN	Typ	Zdalny IP	Sieć wirtualna	Tx pakietów	Tx prędk. (Bps)	Rx pakietów	Rx prędk. (Bps)	Czas akt.
1	IPSec Tunnel	83.15.53.X	192.168.1.0/24	182	480	261	3947	0:9:20
(do 5500) AES-SHA1 Auth								

xxxxxxxx : Dane są szyfrowane.
xxxxxxxx : 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 millisekundach:
        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