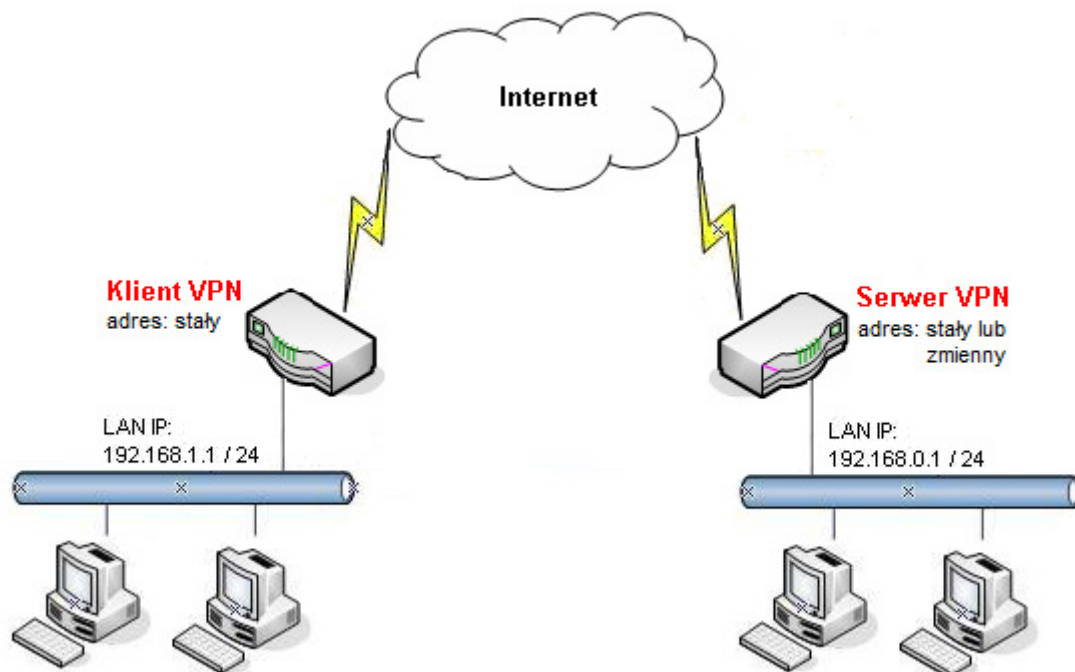


1. Konfiguracja serwera VPN
2. Konfiguracja klienta VPN
3. Status połączenia

Procedura konfiguracji została oparta na poniższym przykładzie.



Główne założenia:

- typ tunelu: Host-LAN
- protokół VPN: IPSec (tryb główny)
- szyfrowanie: 3DES
- integralność: SHA1
- autentykacja: klucz IKE
- aktywność tunelu: zawsze
- serwer VPN oraz klient VPN wspierają DPD dla IPSec
- Adres Serwera VPN: stały (IP - 99.99.99.10) lub zmienny (domenowy - serwer.abc.xyz)
- Adres Klienta VPN: stały (IP - 99.99.99.11)

Uwaga

Jeśli serwer VPN nie posiada stałego adresu IP to można wykorzystać opcję dynamicznego DNS (np. www.noip.com) w celu reprezentowania zmiennego adresu IP poprzez adres domenowy.

1. Konfiguracja serwera VPN

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

W kolejnym kroku przejdź do zakładki **VPN i Dostęp Zdalny >> Połączenia Host-LAN**. Stwórz odpowiednie konto do obsługi tunelu.

Konfiguracja zgodna z założeniami przykładu:

- zaznacz **Włącz konto**
- 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).
- jako akceptowany protokół zaznacz **Tunel IPSec**
- zaznacz **Określ węzeł zdalny** i wpisz odpowiedni adres. W przykładzie użyto 99.99.99.11
- zaznacz **Klucz IKE**, kliknij przycisk **Klucz IKE** – pojawi się okienko w którym wpisz odpowiedni klucz. W przykładzie użyto klucza 'test'
- zaznacz odpowiedni **Poziom zabezpieczeń IPSec**. W przykładzie użyto 3DES.
- kliknij przycisk OK, zatwierdzić ustawienia

VPN i Dostęp Zdalny >> Użytkownik zdalny

Indeks Nr. 1

Konto użytkownika

Włącz konto
Czas nieaktywności sek

Akceptowane protokoły

PPTP
 Tunel IPSec
 L2TP z polisą IPSec

Określ węzeł zdalny
Adres IP klienta zdalnego
lub ID

Użytkownik
Hasło

Tryb uwierzytelniania IKE

Klucz IKE

 Podpis cyfrowy (cert. X.509)

Poziom zabezpieczeń IPSec

Średni (AH)
Wysoki (ESP)
 DES 3DES AES
Lokalny ID (opcja)

2. Konfiguracja klienta VPN

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

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 <input type="text" value="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
VPN Dial-Out przez <input type="text" value="WAN1 najpierw"/>	Czas nieaktywności <input type="text" value="-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 99.99.99.10
- 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.

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

<p>Protokół dla połączenia</p> <p><input type="radio"/> PPTP</p> <p><input checked="" type="radio"/> Tunel IPSec</p> <p><input type="radio"/> L2TP z polisą IPSec Brak ▾</p>	<p>Użytkownik <input data-bbox="1038 584 1254 618" type="text" value="???"/></p> <p>Hasło <input data-bbox="1038 629 1254 663" type="text"/></p> <p>Uwierzytelnianie PPP PAP/CHAP ▾</p> <p>Kompresja VJ <input checked="" type="radio"/> Włącz <input type="radio"/> Wyłącz</p>
<p>IP/nazwa DNS serwera VPN. (np. draytek.com lub 123.45.67.89)</p> <p><input data-bbox="288 808 592 842" type="text" value="99.99.99.10"/></p>	<p>Metoda uwierzytelniania IKE</p> <p><input checked="" type="radio"/> Klucz PSK</p> <p><input data-bbox="807 831 903 864" type="button" value="IKE PSK"/> <input data-bbox="1038 831 1254 864" type="text" value="....."/></p> <p><input type="radio"/> Podpis cyfrowy (X.509)</p> <p><input data-bbox="807 898 879 931" type="text" value="Brak"/></p>
	<p>Poziom zabezpieczeń IPSec</p> <p><input type="radio"/> Średni(AH)</p> <p><input checked="" type="radio"/> Wysoki (ESP) AES z autentykacją ▾</p> <p><input data-bbox="807 1066 1007 1099" type="button" value="Zaawansowane"/></p>

Konfiguracja części **Adresacja i routing oraz NAT wewnątrz połączenia** zgodna z założeniami przykładu:

- w przykładzie Zdalna podsieć: 192.168.0.0, Maska podsieci zdalnej: 255.255.255.0
- aby Vigor pracował jako klient VPN dla połączenia Host-LAN dla opcji *Z lokalnej podsieci do zdalnej podsieci, wykonaj* wybierz **NAT**.

4. Adresacja i routing oraz NAT wewnątrz połączenia

<p>Własny WAN IP <input data-bbox="544 1357 759 1391" type="text" value="0.0.0.0"/></p> <p>IP zdalnej bramy <input data-bbox="544 1402 759 1435" type="text" value="0.0.0.0"/></p> <p><input data-bbox="544 1447 759 1480" type="text" value="192.168.0.0"/></p> <p><input data-bbox="544 1491 759 1525" type="text" value="255.255.255.0"/></p> <p><input data-bbox="544 1536 759 1570" type="button" value="Więcej podsieci"/></p>	<p>RIP dla VPN Wyłącz ▾</p> <p><input data-bbox="807 1402 1270 1435" type="text" value="Z lokalnej podsieci do zdalnej podsieci, wykonaj"/></p> <p><input data-bbox="1062 1447 1158 1480" type="text" value="NAT"/></p> <p><input type="checkbox"/> Zmień trasę domyślną do tego tunelu VPN (Tylko dla pojedynczego WANu)</p>
--	--

3. Status połączenia (od strony klienta VPN)

O tym, czy tunel został zainicjowany, możesz również przekonać się wybierając **VPN i Dostęp Zdalny>>Zarządzanie połączeniem** (rysunek poniżej).

VPN i Dostęp Zdalny>> Kontrola połączeń

Wymuszanie inicjacji połączeń Czas odświeżania : 10

Stan połączenia VPN

Bieżąca strona: 1

Nr strony

VPN	Typ	Zdalny IP	Sieć wirtualna	Tx pakietów	Tx prędk. (Bps)	Rx pakietów	Rx prędk. (Bps)	Czas akt.
1	IPSec Tunnel (do 5500) AES-SHA1 Auth	99.99.99.10	192.168.0.0/24	61	60	63	60	0:1:4

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

Inny sposób to np. zwykły ping. Wybierz Menu Start a następnie Uruchom i wpisz cmd . 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). Po zainicjowaniu tunelu otrzymasz poprawną odpowiedź na ping – świadczy ona o poprawnej komunikacji w tunelu VPN.

```
C:\>ping 192.168.0.10

Badanie 192.168.0.10 z użyciem 32 bajtów danych:

Odpowiedź z 192.168.0.10: bajtów=32 czas=3ms TTL=126
Odpowiedź z 192.168.0.10: bajtów=32 czas=3ms TTL=126
Odpowiedź z 192.168.0.10: bajtów=32 czas=3ms TTL=126
Odpowiedź z 192.168.0.10: bajtów=32 czas=3ms TTL=126

Statystyka badania ping dla 192.168.0.10:
    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
```