

- 1. Konfiguracja serwera VPN (Vigor2960)
- 2. Konfiguracja klienta VPN (Vigor2920)

Procedura konfiguracji została oparta na poniższym przykładzie.



Główne założenia:

- typ tunelu: LAN-LAN z routingiem pomiędzy podsieciami
- protokół VPN: IPSec
- tryb agresywny IKE:
 - 2920: lokalny ID 'vigor2920'
 - 2960: zdalny ID 'vigor2920'
- serwer VPN akceptuje wszystkie propozycje
- klient VPN proponuje szyfrowanie AES z SHA1/MD5
- autentykacja: klucz IKE 'test'
- adres IP Serwera VPN: statyczny. W przykładzie 99.99.99.10
- adres IP Klienta VPN: statyczny lub dynamiczny. W przykładzie 99.99.99.11
- różne adresacje LAN:
 - serwer VPN: 192.168.0.1 /24
 - klient VPN: 192.168.1.1 /24

Uwaga!

Wymagane są różne adresacje sieci lokalnych.



1. Konfiguracja serwera VPN (Vigor2960)

Przejdź do zakładki VPN and Remote Accessny>>VPN Profiles. Kliknij przycisk Add(Dodaj).

V	VPN and Remote Access >> VPN Profiles									
	VPN Profiles									
	🕼 Add 🔀 Edit	👖 Delete 🛛 🗳 Refresh	IPSec OPPTP Dial-O	ut 🔘 PPTP Dial-In			Profile Number Limit : 200			
	Profile	Enable	WAN Profile	Local IP / Subnet	Remote Host	Remote IP / Subnet	More Remote Subnet			

Wpisz nazwę profilu.

Zaznacz Enable This Profile(Włącz ten profil). Dla opcji Type(Typ) wybierz IPSec.

IPSec		
		I
Profile :	ipsec_in	
Enable This Profile		
Туре :	IPSec PPTP Dial-Ou	t 💿 PPTP Dial-In

W ustawieniach Basic(Podstawowe):

- W polu Local IP(Lokalny IP)/Subnet(Maska) wpisz odpowiedni adres IP oraz wybierz odpowiednią maskę.
- W polu Remote Host(Zdalny Host) pozostaw 0.0.0.0.
- W polu Remote IP(Zdalny IP)/Subnet(Maska) wpisz odpowiedni adres IP oraz wybierz odpowiednią maskę.
- Dla opcji IKE Phase 1 wybierz Aggressive mode (Tryb agresywny).
- W polu Preshared Key(Klucz PSK) wpisz klucz. W przykładzie 'test'.
- W polu Remote Peer ID(Zdalny ID) wpisz identyfikator. W przykładzie 'Vigor2920'.

Basic	Advanced	GR	E	Propo	sal		PPTP		
Always On	:	Enal	ble 🍥 D	isable					
For Remot	e Dial-In User :	Enal	ble 💿 D	isable					
WAN Profile :		wan1			*	O Det	fault WAN	IP 🔘 WAN	Alias IP
Local IP / Subnet :		192	. 168	. 0	. (0	255.255.2	255.0	~
Local Next	Hop:	0	0	0	. (D			
Remote Ho	ost:	0.0.0.0	0.0.0.0						
Remote IP	/ Subnet :	192	168	. 1	. (0	255.255.2	55.0	~
		🚯 Add 📄 Save				Profile Number Limit: 16			
More Remote Subnet :		IP Subnet Mask							
		No items to show.							
IKE Phase 1 :		Main	Mode	Aggi	ressi	ve Moo	le		
Auth Type :		PSK			~				
Preshared Key :									
Local ID :									
Remote ID :		Vigor2920							
Security Protocol :		ESP							



W ustawieniach Proposal(Propozycja):

- W polu Accepted Proposal [Dial-In] wybierz **acceptall(akceptuj wszystko)**.

Basic	Advanced	GRE	Proposal	PPTP
		_		
IKE Phase1	Proposal [Dial-(Dut] : [DES_G1	~
IKE Phase1	Authentication	[Dial-Out] :	ALL	*
IKE Phase2	Proposal [Dial-0	Dut] :	3DES_with_auth	*
IKE Phase2	Authentication	[Dial-Out] :	ALL	*
Accepted I	Proposal [Dial-In]: 4	acceptall	~



2. Konfiguracja klienta VPN (Vigor2920)

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.

/PN i Dostęp Zdalny>> Protokoły VPN					
Protokoły VPN					
	V	Włącz obsługę PPTP			
		Włącz obsługę IPSec			
	\checkmark	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 ipsec_out	Kierunek inicjacji 🛛 💿 Oba 💿 Dial-Out 🔍 Dial-in
🔽 Włącz profil	Zawsze aktywne
	Czas nieaktywności -1 sek
VPN Dial-Out przez WAN1 najpierw 👻	Użyj PING dla podtrzymania
Nazwy NetBIOS 🔍 Przepuść 🔘 Blokuj	PING na IP
Multicast przez VPN 🛛 🔍 Przepuść 💿 Blokuj	
(IGMP,Kamery IP,DHCP Relayitd.)	

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'

🖉 Konfiguracja routera - Windows Internet Explorer							
	Uwierzytelnianie IKE						
	Klucz IKE	••••					
	Potwierdź klucz IKE	••••					
Ok							
Gotowe		😜 Internet	€ 100% -				

 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 'Vigor2920').



Jstawienia zaawansowane IKE			
Faza 1 IKE/tryb	Tryb głó	wny 💿 Tryb agresywny	
Faza 1 IKE/propozycja	AES128_MD	5_G2/AES128_SHA1_G2/AES256_MD5_G2/AES256_SHA1_G2 -	
Faza 2 IKE/propozycja	AES128_SH	A1/AES128_MD5 -	
Faza 1 IKE/czas klucza	28800	(900 ~ 86400)	
Faza 2 IKE/czas klucza	3600	(600 ~ 86400)	
Opcja PFS	Wyłącz	Włącz	
Lokalny ID	Vigor2920		

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

Protokół dla połączenia	Użytkownik ???
◎ РРТР	Hasło
Tunel IPsec	Uwierzytelnianie PPP PAP/CHAP -
💿 L2TP z polisą IPsec 🛛 🖛 💌	Kompresja VJ 💿 Włącz 🔍 Wyłącz
IP/nazwa DNS serwera VPN.	Metoda uwierzytelniania IKE
(np. draytek.com lub 123.45.67.89)	Klucz PSK
99.99.99.10	IKE PSK
	Podpis cyfrowy (X.509)
	Peer ID Brak 👻
	Lokalny ID
	Najpierw alternatywna nazwa podmiotu
	Najpierw nazwa podmiotu
	Poziom zabezpieczeń IPsec
	Sredni(AH)
	Wysoki (ESP) AES with Authentication •
	Zaawansowane

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

). Adresacja i routing oraz NAT wewnątrz połączenia						
Własny WAN IP	0.0.0.0	RIP dla VPN	Wyłącz 👻			
IP zdalnej bramy	0.0.0.0	Z lokalnej podsieci do zda	nej podsieci, wykonaj			
IP zdalnej podsieci	192.168.0.0		Routing 👻			
Maska zdalnej podsieci	255.255.255.0	Zmień trase domyślna	do tego tunelu VPN (
IP lokalnej podsieci	192.168.1.0	Tylko dla pojedyńczego W	/ANu)			
Maska lokalnej podsieci	255.255.255.0					
	Więcej podsieci					

Krzysztof Skowina Specjalista ds. rozwiązań sieciowych <u>k.skowina@brinet.pl</u>