

- 1. Konfiguracja serwera VPN
 - 1.1. Profil dla klienta ze zmiennym IP
 - 1.2. Profil dla klienta ze stałym IP
- 2. Konfiguracja klienta VPN
- 3. Zainicjowanie 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: ograniczona czasowo
- klient VPN nie wspiera DPD dla IPSec
- Adres Serwera VPN: stały (IP 99.99.99.10) lub zmienny (domenowy serwer.abc.xyz)
- Adres Klienta VPN 1: zmienny
- Adres Klienta VPN 2: stały (IP 99.99.99.12)

Uwagi

Jeśli serwer VPN nie posiada stałego adresu IP to można wykorzystać opcję dynamicznego DNS (np. <u>www.noip.com</u>) 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) czy jest włączona obsługa protokołu IPSec.

VPN i Dostęp Zdalny>> Protokoły VPN					
Protokoły VPN					
v		Włącz obsługę PPTP			
		Włącz obsługę IPSec			
	V	Włącz obsługę L2TP			

1.1. Profil dla klienta ze zmiennym IP

Przejdź do zakładki **VPN i Dostęp Zdalny>>Ustawienia ogólne IPSec**. Wpisz wspólny **klucz IKE** (w przykładzie użyto klucza `test') oraz wybierz **3DES** jako Tryb zabezpieczeń IPSec.

VPN i Dostęp Zdalny>> Ustawienia ogólne	IPSec	
Ustawienia ogólne IKE/IPSec		
Ustawienia wspólne dla klientów i routeró	ów IPSec ni	e prezentujących się stałym IP.
Uwierzytelnianie IKE		_
Klucz IKE	••••	
Potwierdź klucz IKE	••••	
Tryb zabezpieczeń IPSec		•
🗌 Średni (AH)		
Autentykacja bez szyfrowan	ia.	
Wysoki (ESP) 🗌 DES 🔽	3DES	AES
Szyfrowanie i autentykacja p	oakietów.	

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. IPSec nie posiada wbudowanych mechanizmów detekcji połączenia – detekcja połączenia realizowana jest za pomocą DPD (Dead Peer Detection).
- jako akceptowany protokół zaznacz Tunel IPSec

ndeks Nr. 1	
<mark>Konto użytkownika</mark> ☑ Włącz konto Czas nieaktywności 300 sek	Użytkownik ??? Hasło
Akceptowane protokoły	Tryb uwierzytelniania IKE
РРТР	Klucz IKE
Tunel IPSec	Klucz IKE
🗌 L2TP z polisą IPSec 🛛 Brak 🛛 🔽	Podpis cyfrowy (cert. X.509)
Określ wezeł zdalny	Brak 🗸
Adres IP klienta zdalnego	Poziom zabezpieczeń IPSec
lub ID	Wysoki (ESP)
	🗹 DES 🗹 3DES 🗹 AES
	Lokalny ID (opcja)



1.2. Profil dla klienta ze stałym IP

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. IPSec nie posiada wbudowanych mechanizmów detekcji połączenia – detekcja połączenia realizowana jest za pomocą DPD (Dead Peer Detection).
- zaznacz Określ węzeł zdalny i wpisz odpowiedni adres. W przykładzie użyto 99.99.99.12
- 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

Indeks Nr. 2	
Konto użytkownika Vłącz konto Czas nieaktywności 300 sek	Użytkownik ??? Hasło
Akceptowane protokoły	Tryb uwierzytelniania IKE
РРТР	Klucz IKE
✓ Tunel IPSec	Klucz IKE
🗌 L2TP z polisą IPSec 🛛 Brak 🔍	Podpis cyfrowy (cert. X.509)
Określ węzeł zdalny Adres IP klienta zdalnego 99.99.99.12 lub ID	Brak Poziom zabezpieczeń IPSec Średni (AH) Wysoki (ESP) DES Ø 3DES AES Lokalny ID (opcja)



2. Konfiguracja klienta VPN

Kliknij przycisk **Wstaw**

OrayTek Smart VPN Client
Krok 0. Włącz/Aktywuj IPSec NAT-Traversal i L2TP Konfiguruj
Krok 1. Połącz z Internetem Połącz Krok 2. Połącz z serwerem VPN
Połącz Wstaw Usuń Ustawienia
Autostart po uruchomieniu: Status: Brak połączenia PPTP ISP © VPN ©

Wypełnij dane dotyczące adresu serwera i typu VPN:

- w polu Nazwa profilu wpisz dowolną nazwę dla połączeni np. To Vigor.
- w polu Adres IP Serwera/Nazwa Hosta wpisz adres IP routera (w przykładzie 99.99.99.10), do którego zestawiasz tunel VPN, albo jego nazwę (w przykładzie serwer.abc.xyz).
- w polu Typ połączenia VPN wybierz Tunel IPSec.
- kliknij OK, aby kontynuować

Połącz z serwerem VPN	×				
Nazwa profilu : To Vigor					
Autopołączenie po rozłączeniu.					
Liczba prób :	3				
Odstęp pomiędzy próbami :	30 sekund 🔻				
🔲 Autostart po uruchomieniu systemu.					
Adres IP serwera VPN/Nazwa hosta (np. 123.4 draytek.com)	15.67.89 lub				
99.99.99.10					
Użytkownik :					
Hasło :					
Włącz mOTP(mobile One Time Password)					
Ustawienia mOTP					
Typ połączenia VPN					
© PPTP © L2TP					
Tunel IPSec C L2TP ov	/er IPSec				
Tunel SSL VPN					
Użyj domyślnej bramy w sieci zdalnej	Więcej				
ОК Ал	uluj				



Wypełnij dane dotyczące zabezpieczeń IPSec:

- w polu Mój adres IP wybierz odpowiedni adres IP swojego komputera. W przykładzie 99.99.99.11.
- w polu Typ połączenia IPSec wybierz Standardowy tunel IPSec oraz wpisz adresację zdalnej podsieci. W przykładzie Zdalna podsieć: 192.168.0.0, Maska podsieci zdalnej: 255.255.255.0.
- w polu Metoda zabezpieczeń wybierz protokół realizujący szyfrowanie i uwierzytelnianie. W przykładzie wybrano Wysokie(ESP) oraz 3DES with SHA1.
- w polu Metoda uwierzytelniania wybierz Klucz PSK i wpisz klucz. W przykładzie użyto klucza 'test'.
- kliknij przycisk OK, aby zapisać zmiany.

asady zabezpieczeń IPSec	×
Własny IP : 99.99.99.11	•
Typ połączenia IPSec	
Standardowy tunel	
Zdalna podsieć :	192 . 168 . 0 . 0
Maska zdalnej podsieci :	255 . 255 . 255 . 0
🔘 Wirtualny IP	
Zdalny adres IP	192 . 168 . 1 . 201
Maska zdalnej podsieci	255 . 255 . 255 . 0
 Sredni(AH) MD5 ✓ Metoda uwierzytelniania ⑥ Klucz PSK : 	rsoki(ESP) DES z SHA1 ▼
© Certyfikat:	Przeglądaj
🔲 Włącz PING dla podtrzymania	
Ping do IP; 0.0.0.0	
ОК	Anuluj



3. Zainicjowanie połączenia

Wybierz odpowiedni profil a następnie kliknij przycisk Aktywuj.

Krok 0. Włącz/Aktywuj IPSec NAT-Traversal i L2TP Konfiguruj						
Krok 1. Połącz z Internetem Połącz Krok 2. Połącz z serwerem VPN						
To Vigor - Aktywuj						
Wstaw Usuń	Ustawienia					
Wstaw Usuń Autostart po uruchomieniu;	Ustawienia					

Zaakceptuj zmiany w Zaporze systemu Windows m.in. włączenie zapory, dodanie reguły zabezpieczeń połączeń.



Następnie kliknij OK.

Połącz z serwerem VPN						
Typ połączenia VPN Zdalny adres IP	Tunel IPSec 99.99.99.10					
Własny IP :	99.99.99.11					
Metoda uwierzytelni Klucz PSK :	iania ••••					
) Certyfikat:	Przeglądaj					
ок	Anuluj					



Dla standardowego tunelu IPSec zmieni się status na Aktywna polityka IPSec oraz zapali się zielone światełko przy polu VPN.

DrayTek Smart VPN C	lient							
Krok 0. Włącz/Aktywuj IPSec NAT-Traversal i L2TP								
Konfiguruj								
Krok 1. Połącz z Interne	Krok 1. Połącz z Internetem							
		•	Połącz					
Krok 2. Połącz z serwerem VPN								
Krok 2. Połącz z serwere	em VPN							
Krok 2. Połącz z serwere	em VPN	~	Dezaktywuj					
To Vigor	em VPN	*	Dezaktywuj					
To Vigor Wstaw	em VPN	_	Dezaktywuj Ustawienia					
To Vigor Wstaw	em VPN	•	Dezaktywuj Ustawienia					
Krok 2. Połącz z serwere To Vigor Wstaw Autostart po uruchomie	Usuń		Dezaktywuj Ustawienia					

Aby "obudzić" tunel należy zainicjować dowolny ruch w kierunku routera. Wystarczy np. zwykły ping. Wybierz Menu Start a następnie Uruchom i wpisz cmd . Następnie wykonaj polecenie: ping adres_LAN_serwera (w przykładzie serwer VPN posiada adres LAN 192.168.0.1). Komunikat "Negocjowanie zabezpieczeń IP" świadczy o wymianie niezbędnych informacji do inicjacji tunelu. Po zainicjowaniu tunelu otrzymasz poprawną odpowiedź na ping – świadczy ona o poprawnej komunikacji w tunelu VPN.

C:∖>ping 192.168.0.1 Badanie 192.168.0.1 z użyciem 32 bajtów danych: Negocjowanie zabezpieczeń IP. Odpowiedź z 192.168.0.1: bajtów=32 czas=1ms TTL=255 Odpowiedź z 192.168.0.1: bajtów=32 czas=1ms TTL=255 Odpowiedź z 192.168.0.1: bajtów=32 czas=1ms TTL=255 Statystyka badania ping dla 192.168.0.1: Pakiety: Wysłane = 4, Odebrane = 3, Utracone = 1 (25% straty), Szacunkowy czas błądzenia pakietów w millisekundach: Minimum = 1 ms, Maksimum = 1 ms, Czas średni = 1 ms



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

VPN i Dostęp Zdalny>> Zarządzanie połączeniem

Wymuszanie inicjacji połączeń	Czas odświeżania : 30 🔽 Odśwież
Tryb Główny:	V Inicjuj
Tryb Backup:	Minicjuj
Stan połączenia VPN	
Bieżąca strona: 1	Nr strony Przejdź >>

_										U
	VPN	Тур	Zdalny IP	Sieć wirtualna	Tx pakietów	Tx prędkość	Rx pakietów	Rx predkość	Czas akt.	
	1 (Dynamic Client)	IPSec Tunnel 3DES-SHA1 Auth	99.99.99.11	99.99.99.11/32	344	55	265	9	0:1:7	Rozłącz
Ī						xxxxxxxx	: Dane s	ą szyfrov	wane.	

xxxxxxx : nie są szyfrowane.

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