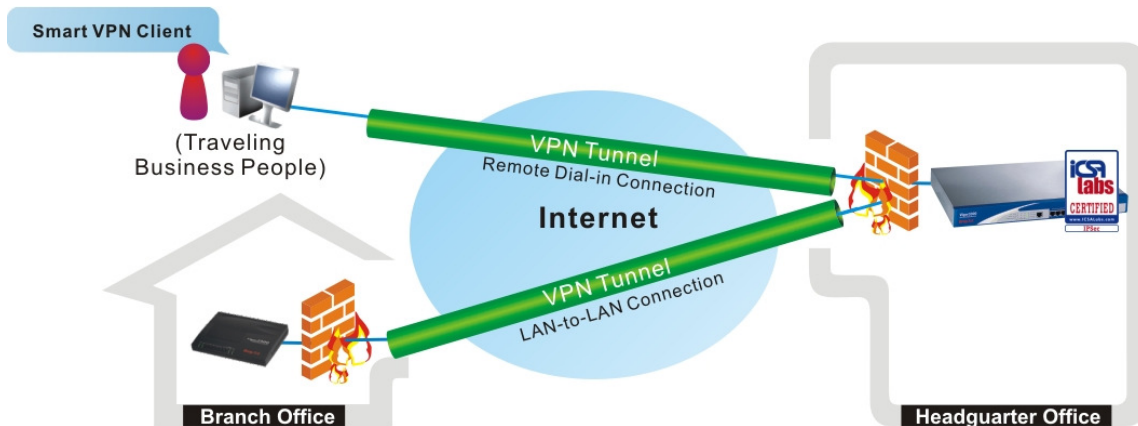


VPN (ang. *Virtual Private Network*) to oddzielny wachlarz możliwości komunikacyjnych routera Vigor. Warto zwrócić na niego uwagę, ponieważ pod tym względem DrayTek od dawna wyprzedza proste implementacje konkurencji w swojej klasie cenowej.

Mechanizmy VPN, oparte na tunelowaniu i mocnym szyfrowaniu pakietów pozwalają zachować bezpieczny zdalny dostęp do sieci komputerowej z dowolnego miejsca w Internecie.



Routery DrayTek realizują dwa rodzaje połączeń VPN:

- ❑ Połączenie typu Host-to-LAN (PC-to-LAN), w którym pojedynczy komputer inicjuje tunel na adres interfejsu routera. Po uwierzytelnieniu otrzymuje **adres prywatny z wnętrza sieci LAN**, i w ten sposób staje się jej członkiem. Vigor stosuje wówczas protokół proxy ARP, aby zdalny komputer mógł się komunikować z wszystkimi lokalnymi maszynami tak jakby sam był fizycznie podłączony do routera.
- ❑ Połączenie typu LAN-to-LAN (Gateway-to-Gateway), w którym tunel zestawia się pomiędzy dwoma routerami VPN w celu połączenia całych sieci komputerowych. Połączenie funkcjonuje w trybie pełnego routingu, to znaczy **odległe podsieci posiadają odrębną adresację IP**, zaś routery uwzględniają tunel VPN w tablicach routingu, traktując go jak jeszcze jeden interfejs komunikacyjny typu WAN.

Mechanizmy VPN towarzyszą produktom DrayTek wraz z wkroczeniem na rynek pierwszych modeli tej marki. W porównaniu z rozwiązaniami konkurencji są one wyjątkowo rozwinięte i dopracowane. **Routery Vigor w zależności od modelu, realizują najczęściej 16 lub 32 jednoczesne tunele, przy czym dostępne są produkty oferujące do 200 tuneli.** Tunele mogą być zestawiane za pomocą następujących protokołów (dotyczy obu typów połączeń VPN):

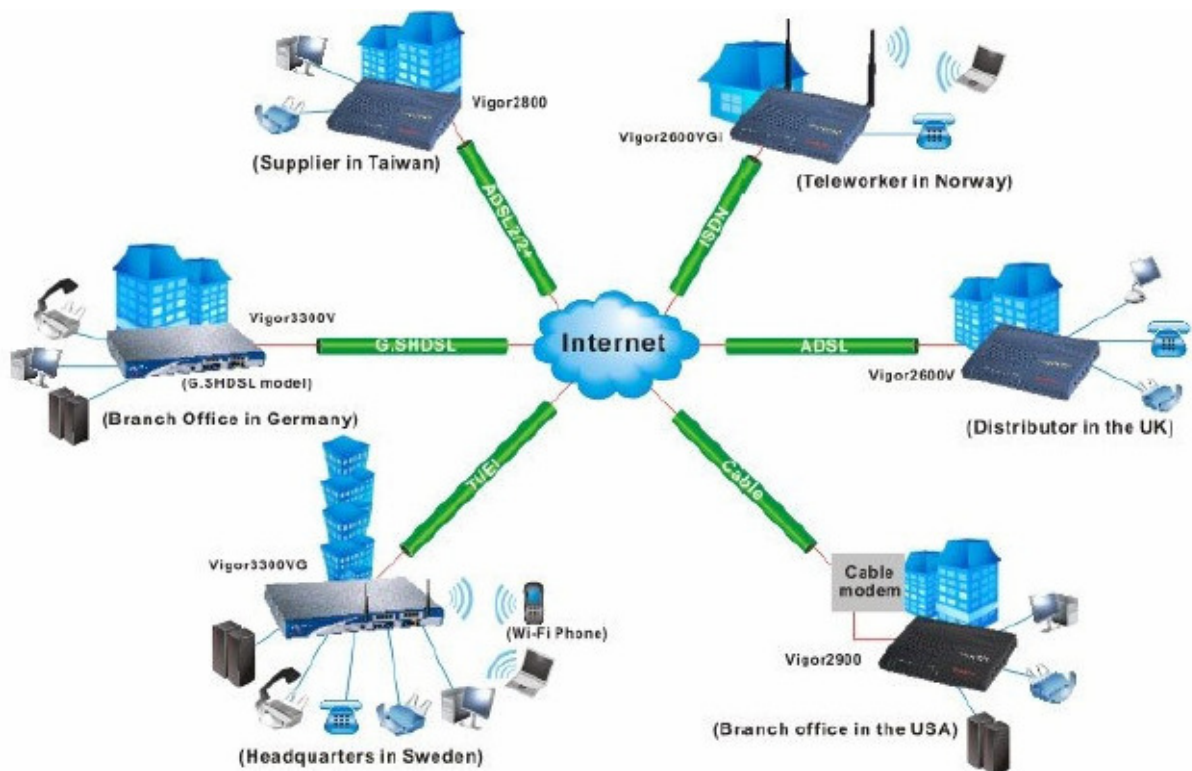
- ❑ PPTP (ang. *Point to Point Tunneling Protocol*) bez szyfrowania, lub z szyfrowaniem MPPE 48/128 bitów oraz obsługą uwierzytelniania CHAP, MS-CHAP i MS-CHAPv2. Wygodny i prosty w użyciu zwłaszcza przy tunelowaniu z użyciem systemów Windows.
- ❑ L2TP (ang. *Layer 2 Tunneling Protocol*) – wydajne tunelowanie z opcją uwierzytelniania PAP lub CHAP, ale bez szyfrowania. Przydatne w warunkach kiedy potrzebny jest sam tunel, bez ochrony danych.
- ❑ Tunel IPSec (ang. *IP Security*) – rozbudowany standard mechanizmów chroniących komunikację IP. Vigor obsługuje tryb tunelowania AH i ESP, a w ramach tych trybów uwierzytelnianie MD-5 i SHA-1 i szyfrowanie DES/3DES/AES. Protokół IKE może działać w trybie podstawowym oraz agresywnym oraz z opcją PFS.
- ❑ L2TP/IPSec (L2TP over IPSec) – tunel L2TP zabezpieczony szyfrowaniem IPSec (IPSec pracuje tu w wydajnym trybie transportu, nie tunelowania).

### Mocne strony VPN w wydaniu DrayTek'a

**Pokazana mnogość protokołów jest rzadko dostępna w routerach klasy SOHO/SMB.** Zwykle implementuje się wyłącznie IPSec, albo działający w trybie Host-LAN protokół PPTP. Dzięki bogactwu protokołów możliwa jest współpraca routerów DrayTek z wszelkimi innymi rozwiązaniami (Cisco, Microsoft ISA, Checkpoint, Linux, Watchguard itd.).

**Wobec pomieszczenia pojęć w świecie na rynku należy tutaj podkreślić, że Vigor jest w pełni funkcjonalnym serwerem VPN dla wszystkich wymienionych protokołów VPN.** Tymczasem nader często „obsługa” VPN wymieniana w opisach różnych urządzeń w praktyce oznacza jedynie zapewnienie wsparcia dla VPN w ramach mechanizmu NAT. Jest to ważne, ale zdecydowanie drugorzędne wymaganie, które notabene routery DrayTek również spełniają. Mechanizm NAT zapewnia pełną przezroczystość dla protokołów PPTP, L2TP i IPSec/ESP. A zwłaszcza przepuszczanie PPTP bywa rzadko osiągalne w innych routerach. Przezroczystość NAT (inaczej *VPN pass-through*) pozwala realizować połączenia VPN urządzeniom zlokalizowanym w sieci prywatnej i nie posiadającym adresów publicznych.

Routery DrayTek są dobrze przygotowane do pracy z wieloma tunelami, łączącymi różne lokalizacje firmy, jak na rysunku:



**Chodzi tutaj o realizację dowolnej formy routingu w ramach sieci VPN. Router pozwala na włączenie protokołu RIPv1 lub RIPv2 nie tylko na swoich rzeczywistych interfejsach fizycznych, ale także wewnątrz aktywnych tuneli VPN. Można więc zbudować złożoną, rozległą sieć prywatną z wykorzystaniem routingu dynamicznego.** Router będzie w stanie skierować pakiet do dowolnej odległej podsieci przez wybrany tunel VPN, przy czym lokalizacje można łączyć według topologii „każdy z każdym” lub „wszyscy do centrali”. **Co więcej, Vigor nie ogranicza komunikacji VPN tylko do podsieci bezpośrednio dołączonej do jego interfejsu. Jeżeli w lokalizacji istnieją dodatkowe routery i podsieci, one także będą mogły korzystać z tuneli utrzymywanych przez router Vigor (wystarczy odpowiednio skonfigurować routing na tych routerach).** Jest to poważna zaleta, rzadko oferowana przez konkurencję.

Routery DrayTek posiadają sprzętowe wsparcie dla szyfrowania DES i 3DES, znacznie zwiększające jego wydajność przy mniejszym obciążeniu procesora głównego. Sprzętowy koprocessor zmniejsza też opóźnienia dla pakietów VoIP przesyłanych tunelem VPN. Routery realizują też algorytm AES128 (w wypadku modelu 3300 – także AES192 i AES256). Nowsze modele poza uwierzytelnianiem IKE Preshared Key w ramach IPSec, realizują podpis cyfrowy RSA w oparciu o certyfikaty X.509 – również rzadko dostępne w routerach dla małego biznesu.

Mocne strony to także dodatkowe opcje konfiguracyjne, pomocne w planowaniu sieci VPN:

- ❑ router może inicjować połączenie VPN automatycznie „na żądanie”, i rozłączać je po wykryciu zadanego czasu nieaktywności
- ❑ router może utrzymywać tunel stale, oraz wykrywać awarie łącza u siebie i po drugiej stronie za pomocą mechanizmu keep-alive, w razie konieczności automatycznie resetując (renegocjując) połączenie
- ❑ **można skonfigurować indywidualne profile czasowe dla poszczególnych połączeń VPN (określamy w nich w jakie dni i o jakich godzinach tunel może być w ogóle użyty)**
- ❑ można narzucić rygory co do kierunku inicjacji połączenia VPN (tylko inicjowane do routera, tylko inicjowane przez router, obie możliwości), przy czym **dla obu kierunków inicjacji można stosować różne zasady zabezpieczeń (hasła, algorytmy szyfrujące a nawet inne protokoły VPN)**
- ❑ można określić zaufane adresy IP, spod których możliwe będzie inicjowanie tuneli do routera
- ❑ **router może inicjować i przyjmować połączenia VPN w warunkach gdy on sam i urządzenia odległe nie dysponują stałym adresem IP (router może posługiwać się nazwą DNS odległego urządzenia VPN oraz trybem agresywnym IKE) – przydatne w usługach typu Neostrada w połączeniu z niezłe działającym w Vigorach mechanizmem DynDNS**
- ❑ **można skierować trasę domyślną przez wybrany tunel VPN, aby np. zmusić lokalne komputery do korzystania ze zdalnej bramy czy serwera proxy w centrali firmy w celu komunikacji z Internetem**
- ❑ można ręcznie wpisać adresy wielu podsieci leżących w lokalizacji po drugiej stronie tunelu w celu umożliwienia dotarcia również do nich (routing statyczny), można także użyć RIP pomiędzy routerami w ramach sieci VPN
- ❑ **można wykorzystać mechanizm NAT wewnątrz tunelu w celu połączenia sieci o adresacji prywatnej z odległym intranetem o adresacji publicznej**
- ❑ **można uzyskać gwarancję pasma dla ruchu VPN dzięki regułom QoS**

Taką liczbę udogodnień trudno znaleźć w innych podobnych urządzeniach dostępnych na rynku. Vigory gwarantują sporą elastyczność w tworzeniu sieci VPN. Nawet bardzo złożonej i szybko się zmieniającej.

**Rzut oka na konfigurację VPN na przykładzie Vigor 2900 – menu główne VPN:**



## Menu Protokoły VPN

Jak widać, można selektywnie włączyć lub wyłączyć serwer danego protokołu VPN:

**Protokoły VPN** ←

Włącz obsługę PPTP

Włącz obsługę IPSec

Włącz obsługę L2TP

Włącz dostęp ISDN

Aby uruchomić odrębny serwer VPN w sieci prywatnej za routerem DrayTek, należy wyłączyć dany protokół VPN na liście i skonfigurować NAT.

## Menu Ustawienia ogólne PPP

Tutaj konfiguruje się lokalne adresy IP przyznawane użytkownikom zdalnym oraz uwierzytelnianie PPP wraz z szyfrowaniem MPPE dla połączeń PPTP:

**Ustawienia ogólne PPP** ←

Protokół PPP/MPPP	Adresy przydzielane klientom zdalnym
Uwierzytelnianie PPP: <input type="text" value="PAP lub CHAP"/>	Adres początkowy: <input type="text" value="192.168.10.200"/>
Opcje szyfrowania PPP(MPPE): <input type="text" value="Opcjonalny MPPE"/>	
Uwierzytelnianie zwrotne (PAP): <input type="radio"/> Tak <input checked="" type="radio"/> Nie	
Użytkownik: <input type="text"/>	
Hasło: <input type="text"/>	

## Menu Ustawienia ogólne IKE/IPSec

**Ustawienia ogólne IKE/IPSec** ←

Ustawienia wspólne dla klientów i routerów IPSec nie prezentujących się stałym IP.

**Uwierzytelnianie IKE**

Klucz IKE:

Wpisz klucz ponownie:

**Tryb zabezpieczeń IPSec**

Średni (AH)

Autentykacja bez szyfrowania.

Wysoki (ESP)  DES  3DES  AES

Szyfrowanie i autentykacja pakietów.

## Połączenie Host-LAN

<b>Konto użytkownika</b> <input checked="" type="checkbox"/> Włącz konto Czas nieaktywności <input type="text" value="300"/> sek	Użytkownik <input type="text" value="piotr"/> Hasło <input type="password"/>
<b>Akceptowane protokoły</b> <input checked="" type="checkbox"/> ISDN <input checked="" type="checkbox"/> PPTP <input checked="" type="checkbox"/> Tunel IPsec <input type="checkbox"/> L2TP z polisą IPsec <input type="text" value="Brak"/>	Klucz IKE <input type="text"/> <b>Tryb pracy IPsec</b> <input checked="" type="checkbox"/> Średni (AH) Wysoki (ESP) <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES Lokalny ID <input type="text"/> (opcja)
<input checked="" type="checkbox"/> Określ węzeł zdalny Adres IP lub nr ISDN klienta zdalnego <input type="text" value="83.18.248.122"/> lub ID <input type="text" value="ipsecpeerid"/>	<b>Callback</b> <input type="checkbox"/> Włącz Callback <input type="checkbox"/> Numer Callback Numer Callback <input type="text"/> <input checked="" type="checkbox"/> Włącz limit kosztów Callback Budżet Callback <input type="text" value="30"/> min

## Połączenie LAN-LAN

<b>1. Ustawienia wspólne</b>	
Nazwa profilu <input type="text" value="brinet-poz"/> <input checked="" type="checkbox"/> Włącz profil	Kierunek inicjacji <input type="radio"/> Oba <input checked="" type="radio"/> Dial-Out <input type="radio"/> Dial-In <input checked="" type="checkbox"/> Zawsze aktywne Czas nieaktywności <input type="text" value="-1"/> sek <input type="checkbox"/> Użyj PING dla podtrzymania PING na IP <input type="text" value="192.168.20.253"/>
<b>2. Ustawienia Dial-Out (inicjacja do innego routera)</b>	
<b>Protokół dla połączenia</b> <input type="radio"/> ISDN <input type="radio"/> PPTP <input checked="" type="radio"/> Tunel IPsec <input type="radio"/> L2TP z polisą IPsec <input type="text" value="Brak"/>	Typ łącza <input type="text" value="64kbit/s"/> Użytkownik <input type="text" value="???"/> Hasło <input type="password"/> Uwierzytelnianie PPP <input type="text" value="PAP/CHAP"/> Kompresja VJ <input checked="" type="radio"/> On <input type="radio"/> Wyłącz
IP/nazwa DNS serwera VPN. (jak np. draytek.com lub 123.45.67.89) <input type="text" value="83.18.248.124"/>	Klucz IKE <input type="password"/> <b>Poziom zabezpieczeń IPsec</b> <input type="radio"/> Średni(AH) <input checked="" type="radio"/> Wysoki(ESP) <input type="text" value="AES z autentykacją"/> <input type="button" value="Zaawansowane"/>
Harmonogram (1-15) <input type="text"/> , <input type="text"/> , <input type="text"/> , <input type="text"/>	
<b>Funkcja Callback (CBCP)</b> <input type="checkbox"/> Wymagaj połączenia zwrotnego <input type="checkbox"/> Przełącz numer ISDN drugiej stronie	

### Ustawienia zaawansowane IKE

Faza 1 IKE/tryb	<input type="radio"/> Tryb główny	<input checked="" type="radio"/> Tryb agresywny
Faza 1 IKE/propozycja	DES_MD5_G1/DES_SHA1_G1/3DES_MD5_G1/3DES_SHA1_G1	
Faza 2 IKE/propozycja	AES_SHA1	
Faza 1 IKE/czas klucza	28800	(900 ~ 86400)
Faza 2 IKE/czas klucza	3600	(600 ~ 86400)
Opcja PFS	<input checked="" type="radio"/> Wyłącz	<input type="radio"/> Włącz
Localny ID	vigor	

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

<b>Akceptowane protokoły</b> <input checked="" type="checkbox"/> ISDN <input type="checkbox"/> PPTP <input checked="" type="checkbox"/> Tunel IPsec <input type="checkbox"/> L2TP z polisą IPsec Brak		Użytkownik: ??? Hasło: Kompresja VJ: <input checked="" type="radio"/> On <input type="radio"/> Wyłącz
<input checked="" type="checkbox"/> Określ Zdalna brama VPN IP zdalnego serwera: lub ID: ipsecpeerid		Klucz IKE: <b>Poziom zabezpieczeń IPsec</b> <input type="checkbox"/> Średni (AH) Wysoki (ESP) <input type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES
		<b>Funkcja Callback (CBCP)</b> <input type="checkbox"/> Włącz Callback <input type="checkbox"/> Użyj tego numeru dla Callback Numer Callback: Budżet Callback: 0 min

### 4. Adresacja i routing oraz NAT dla połączenia

WAN IP (lokalny)	0.0.0.0	RIP dla VPN	Wyłącz
WAN IP (zdalny)	0.0.0.0	Wersja RIP	Wer. 2
IP zdalnej podsieci	192.168.20.0	NAT dla połączenia - traktuj podsieć zdalną jako:	
Maska zdalnej podsieci	255.255.255.0	Prywatna	
<input type="button" value="Więcej podsieci"/>		<input type="checkbox"/> Routing domyślny przez to połączenie	

Adres IP podsieci	192.168.21.0	Podsieć zdalna	192.168.21.0 / 24	<input type="button" value="Dodaj"/>
Maska	255.255.255.0 / 24		192.168.22.0 / 24	<input type="button" value="Usuń"/>
				<input type="button" value="Modyfikuj"/>
<input type="button" value="Zamknij"/>		<input type="button" value="OK"/>		

## Komentarze do ustawień

Normalnie klucze IKE przydziela się indywidualnie na podstawie adresu IP lub Peer ID urządzenia zdalnego (w ramach tworzonych profili połączeń Host-LAN lub LAN-LAN - patrz wcześniej). Jednak jeżeli zdalne urządzenie nie posiada stałego adresu, może nawiązać połączenie IPsec korzystając z ustawień wspólnych określonych w menu Ustawienia ogólne IKE/IPsec.

Router DrayTek pozwala na zdefiniowanie typowo do 32 profili połączeń typu Host-LAN. Są to indywidualne konta dla pojedynczych użytkowników zdalnych, określające dozwolone protokoły VPN wraz z zasadami zabezpieczeń, adres, spod którego mogą inicjować połączenie i różne opcje dodatkowe. **Stosują zewnętrzny serwer RADIUS, liczba kont użytkowników jest nieograniczona (mogą ich być setki).**

Można też zdefiniować do 32 profili połączeń typu LAN-to-LAN. Są to rozbudowane zespoły ustawień, gdzie wybiera się parametry dla obu kierunków inicjacji tunelu, towarzyszące im protokoły i wszelkie reguły zabezpieczeń. Poza tym definiuje się zasady adresowania i routingu IP wewnątrz tunelu.

Profil jest zbudowany z 4 segmentów. W części pierwszej określa się parametry ogólne połączenia LAN-to-LAN, jak dozwolone kierunki inicjacji, czas rozłączania lub stałą aktywność itp. Segment 2 to parametry związane z inicjowaniem połączenia przez router Vigor do odległego serwera VPN. Podaje się protokoły i szczegóły zabezpieczeń, w zależności od wymagań zaznaczonego protokołu, a także adres IP, numer ISDN lub nazwę DNS odległego serwera. Segment 3 odnosi się do odbioru połączenia inicjowanego przez inny router, i obejmuje dozwolone protokoły, zabezpieczenia, zdalny adres IP lub identyfikator. Wreszcie sekcja 4 to ustawienia protokołu IP: wskazanie adresu zdalnej podsieci prywatnej, użycie RIP i NAT, skierowanie trasy domyślnej przez tunel itp.

Rozwinięcie i komentarz do wybranych opcji:

*Użyj PING dla podtrzymania* – opcja ta może być wykorzystana do podtrzymania aktywności tunelu, jeżeli nie zaznaczono pola **Zawsze aktywne**. Sztuczne podtrzymywanie aktywności jest osiągane poprzez wysyłanie co pewien czas pakietu ICMP (ping) na podany poniżej adres. Ponadto, wysyłając pakiety na adres prywatny w zdalnej podsieci, router może monitorować stan połączenia VPN po drugiej jego stronie. Konkretnie, jeżeli nastąpi nagłe zerwanie połączenia z Internetem w routerze zdalnym, router Vigor przestanie otrzymywać odpowiedzi z sieci prywatnej. Uzna on, że należy zresetować tunel, aby możliwa była jego ponowna negocjacja, kiedy zdalny router uzyska ponownie dostęp do Internetu. Jest to ważne zwłaszcza w przypadku używania połączeń IPsec w niezbyt sprzyjających warunkach, typu niestabilne łącza czy zmienne adresy IP. Zwolnienie skojarzenia S.A. (ang. *Security Association*) znacznie przyspiesza ponowne zestawienie tunelu w sytuacjach krytycznych.

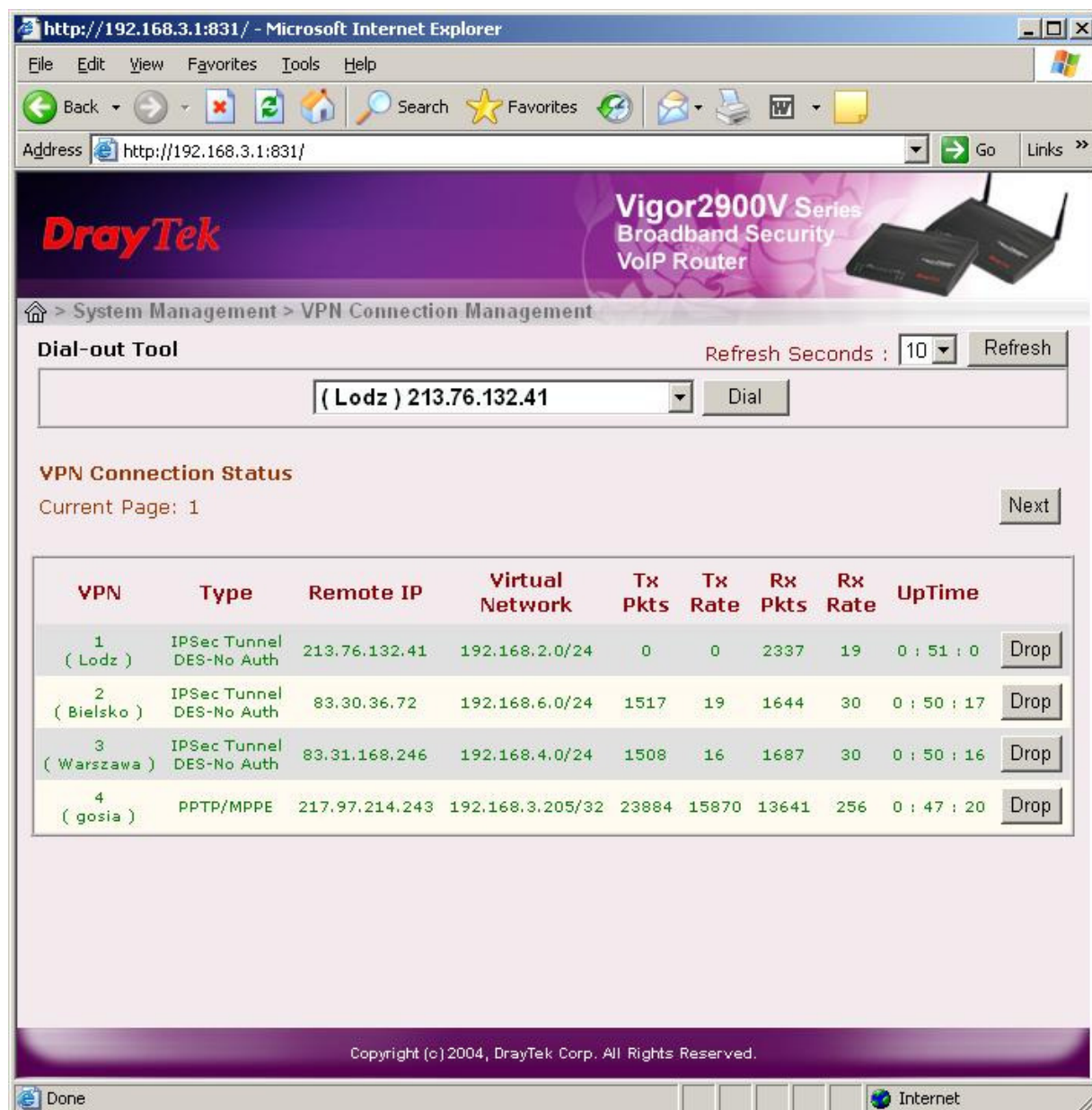
*Metoda zabezpieczeń:*

*Wysoka (ESP)* – zaznaczenie tej opcji spowoduje użycie protokołu ESP podczas inicjacji tunelu. Szyfrowanie i autoryzacja będą uzgadniane z uwzględnieniem algorytmu wybranego spośród poniższych kombinacji:

```
DES bez uwierzytelniania
DES z uwierzytelnianiem
3DES bez uwierzytelniania
3DES z uwierzytelnianiem
AES bez uwierzytelniania
AES z uwierzytelnianiem
```

## Opcje kontrolno-diagnostyczne

Interfejs Użytkownika oferuje graficzny obraz aktywnych połączeń VPN. Są tam najważniejsze informacje typu adresy IP, protokoły oraz wynegocjowane opcje zabezpieczeń. Dodatkowo tunele szyfrowane są wyświetlane na zielono, natomiast nieszyfrowane, na czarno. Można wymuszać nawiązanie oraz rozłączenie tuneli, i rejestrować czas ich aktywności. Jest to pomocne w diagnozowaniu problemów.



http://192.168.3.1:831/ - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address http://192.168.3.1:831/

**DrayTek** Vigor2900V Series Broadband Security VoIP Router

> System Management > VPN Connection Management

**Dial-out Tool** Refresh Seconds : 10 Refresh

(Lodz) 213.76.132.41 Dial

**VPN Connection Status** Next

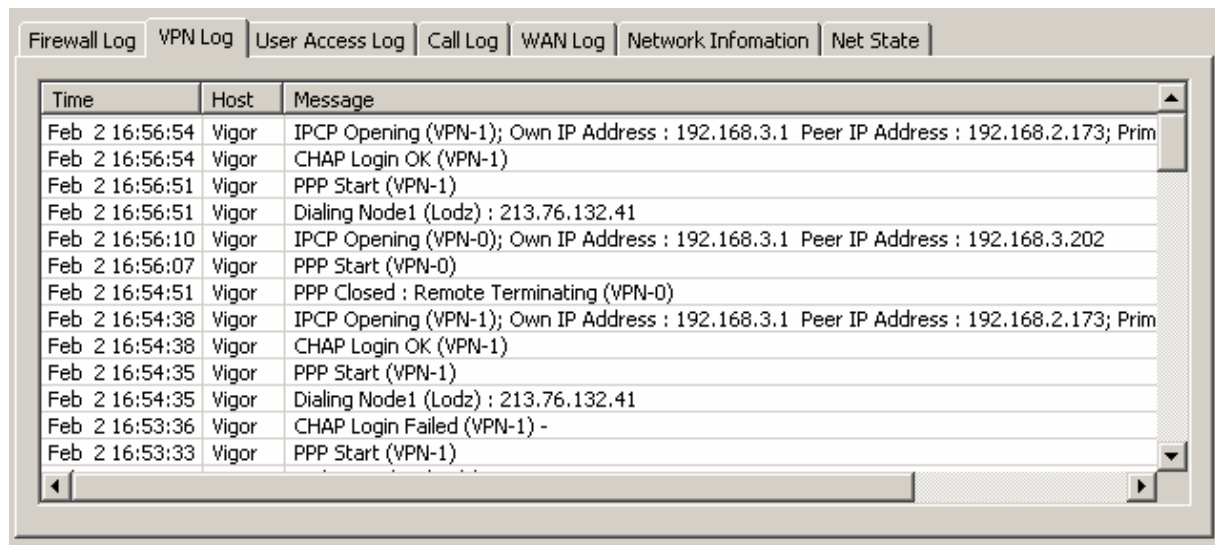
Current Page: 1

VPN	Type	Remote IP	Virtual Network	Tx Pkts	Tx Rate	Rx Pkts	Rx Rate	UpTime
1 (Lodz)	IPSec Tunnel DES-No Auth	213.76.132.41	192.168.2.0/24	0	0	2337	19	0 : 51 : 0
2 (Bielsko)	IPSec Tunnel DES-No Auth	83.30.36.72	192.168.6.0/24	1517	19	1644	30	0 : 50 : 17
3 (Warszawa)	IPSec Tunnel DES-No Auth	83.31.168.246	192.168.4.0/24	1508	16	1687	30	0 : 50 : 16
4 (gosia)	PPTP/MPPE	217.97.214.243	192.168.3.205/32	23884	15870	13641	256	0 : 47 : 20

Copyright (c) 2004, DrayTek Corp. All Rights Reserved.

Done Internet

Szczegółowa diagnostyka jest dostępna w ramach narzędzia SysLog dostarczanego razem z płytą CD. Program SysLog może wyświetlać szczegóły związane z zestawianiem połączeń VPN za pomocą różnych protokołów. Możliwy jest monitoring lokalny lub poprzez Internet oraz zapisywanie zdarzeń w pliku.



The screenshot shows a web-based interface with several tabs: Firewall Log, VPN Log, User Access Log, Call Log, WAN Log, Network Information, and Net State. The 'VPN Log' tab is selected, displaying a table of log entries. The table has three columns: Time, Host, and Message. The entries show various VPN connection events, including IPsec opening, CHAP login success/failure, and PPP start/closure.

Time	Host	Message
Feb 2 16:56:54	Vigor	IPCP Opening (VPN-1); Own IP Address : 192.168.3.1 Peer IP Address : 192.168.2.173; Prim
Feb 2 16:56:54	Vigor	CHAP Login OK (VPN-1)
Feb 2 16:56:51	Vigor	PPP Start (VPN-1)
Feb 2 16:56:51	Vigor	Dialing Node1 (Lodz) : 213.76.132.41
Feb 2 16:56:10	Vigor	IPCP Opening (VPN-0); Own IP Address : 192.168.3.1 Peer IP Address : 192.168.3.202
Feb 2 16:56:07	Vigor	PPP Start (VPN-0)
Feb 2 16:54:51	Vigor	PPP Closed : Remote Terminating (VPN-0)
Feb 2 16:54:38	Vigor	IPCP Opening (VPN-1); Own IP Address : 192.168.3.1 Peer IP Address : 192.168.2.173; Prim
Feb 2 16:54:38	Vigor	CHAP Login OK (VPN-1)
Feb 2 16:54:35	Vigor	PPP Start (VPN-1)
Feb 2 16:54:35	Vigor	Dialing Node1 (Lodz) : 213.76.132.41
Feb 2 16:53:36	Vigor	CHAP Login Failed (VPN-1) -
Feb 2 16:53:33	Vigor	PPP Start (VPN-1)

**UWAGA! Artykuł nie pokazuje wszystkich opcji VPN, np. podpisów cyfrowych i certyfikatów X.509, dostępnych w nowych seriach routerów – np. seria 2800. Dlatego należy odwołać się do konkretnego modelu z jego opisem na stronie draytek.pl.**