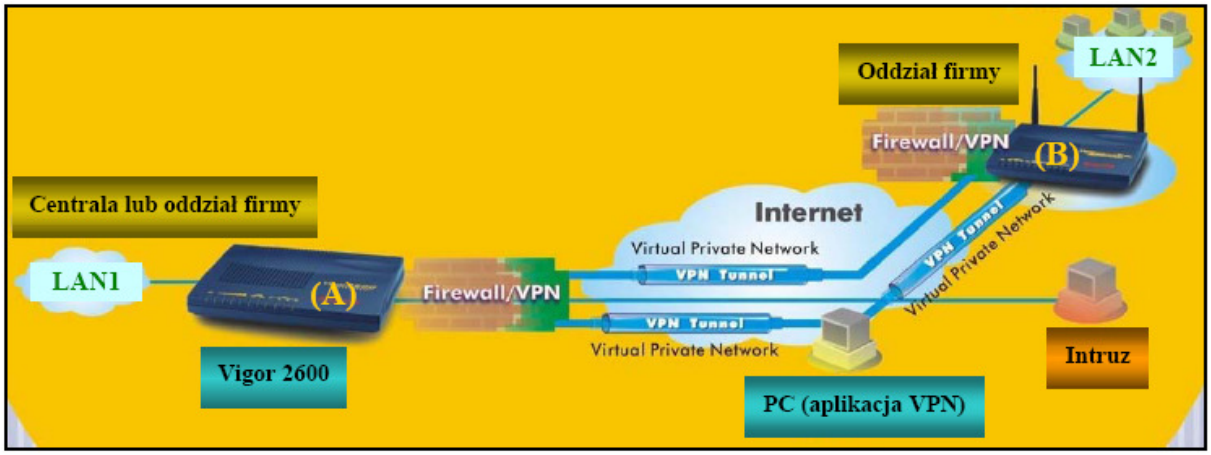
Vigor jest rozwiniętym funkcjonalnie routerem dostępowym, pozwalającym na łatwą budowę sieci lokalnej oraz zapewniającym komputerom z tej sieci bezpieczne korzystanie z zasobów Internetu. Bezpieczeństwo to jest wielowymiarowe, i realizowane głównie w ramach funkcji NAT oraz Filtr/Firewall

Koncepcja zdalnego dostępu natomiast obejmuje oddzielny, istotny wachlarz możliwości komunikacyjnych routera. Pozwala bowiem uprawnionym do tego osobom/urządzeniom, fizycznie odległym, a więc znajdującym się poza siecią lokalną (np. w Internecie), na korzystanie z zasobów tej sieci. Ten rodzaj komunikacji narzuca swoje własne wymagania odnośnie aspektów bezpieczeństwa, i tylko po części odpowiadają one wymaganiom obowiązującym dla dostępu do Internetu. Tutaj bowiem router jest dodatkowo stroną weryfikującą prawa dostępu, negocjującą szczegóły zabezpieczeń i ewentualnie akceptującą połączenie.

Funkcjonalnie istnieją dwa podstawowe sposoby realizacji zdalnego dostępu. Pierwszy to dostępem niesymetryczny, inicjowany przez pojedynczy, fizycznie odległy komputer w celu chwilowego skorzystania z lokalnych zasobów (np. skopiowania potrzebnych plików z dysku komputera w sieci firmowej). W roli zdalnego komputera może wystąpić router, jednak zwykle musi on się „prezentować" jednym, konkretnym adresem IP (a więc realizować translację adresów). Wówczas taka jednostronna sesja komunikacyjna może być inicjowana na rzecz wielu komputerów ukrytych poza routerem NAT. Choć dostęp niesymetryczny pozwala na przesyłanie pakietów w obie strony, to jednak nawiązanie połączenia możliwe jest tylko przez stronę zdalną (odległy komputer). Zadaniem routera jest wówczas sprawdzić prawa dostępu i zabezpieczyć ewentualną komunikację, zarządzając przy tym czasem połączenia. Drugi rodzaj dostępu to symetryczne, wzajemne połączenie dwóch odległych sieci LAN (tzw. LAN-to-LAN). Symetria oznacza tutaj, że obie strony połączenia pełnią wobec siebie te same role, to znaczy mogą inicjować połączenie oraz je odbierać, tworząc równorzędną komunikację w obu kierunkach. W obu kierunkach można niezależnie zastosować mechanizm NAT, jednak możliwy jest też klasyczny routing pomiędzy lokalnymi podsieciami IP (każdemu połączeniu LAN-to-LAN będzie odpowiadał oddzielny wpis w tablicy routingu).

Od strony technicznej realizacja zdalnego dostępu w Internecie odbywa się z wykorzystaniem koncepcji VPN (ang. *Virtual Private Network*). Pod tym szerokim pojęciem mieści się cała gama mechanizmów, mających na celu zapewnienie bezpiecznego, przeźroczystego przekazu informacji pomiędzy oddalonymi sieciami prywatnymi z wykorzystaniem zasobów sieci publicznej. Do tworzenia takich bezpiecznych połączeń stosuje się specjalnie do tego celu stworzone protokoły. Ze względu na złożoność zagadnień ich omówienie zostanie ograniczone do informacji niezbędnych dla zrozumienia procesu konfiguracji.

Technika VPN realizowana w Internecie opiera się głównie na tunelowaniu IP. Tunel jest tworzony z wykorzystaniem dwóch publicznych adresów IP i służy do przenoszenia pakietów bezpośrednio pomiędzy sieciami prywatnymi czy też pomiędzy siecią a pojedynczym węzłem (komputerem korzystającym z aplikacji VPN i podłączonym do Internetu):



Oryginalny pakiet, wysyłany przez komputer pracujący w sieci **LAN2** do komputera w sieci **LAN1**, jest przez router **B** umieszczany wewnątrz innego pakietu (enkapsulacja). Nowy pakiet w polu adresu źródłowego używa

publicznego adresu IP, którym dysponuje router **B**, zaś adresem przeznaczenia jest adres publiczny routera **A**. Oryginalny pakiet, łącznie z nagłówkiem, jest umieszczany w polu danych nowo tworzonego pakietu:

Po dotarciu do routera **A** oryginalny pakiet jest odzyskiwany (deenkapsulacja) i kierowany do właściwego hosta w sieci **LAN1**. Analogiczny proces zachodzi dla przeciwnego kierunku komunikacji (z **LAN1** do **LAN2**). Tunel stanowi zatem komunikacyjny pomost, realizujący przeźroczystą transmisję pakietów pomiędzy lokalnymi sieciami z zachowaniem ich oryginalnych, prywatnych adresów.

Komunikacja odbywa się tak, jak gdyby obie sieci znajdowały się w tej samej lokalizacji (routing bezpośredni), lub były połączone dedykowanym łączem dzierżawionym. W tym miejscu ujawnia się korzyść ekonomiczna – aby połączyć oddziały firmy wystarczy posiadać dostęp do Internetu, niekoniecznie zaś drogie łącze dedykowane.

Prezentowany przykład ilustruje samą ideę tunelowania. W rzeczywistości protokoły VPN stosują wielokrotną enkapsulację danych, połączoną z różnymi opcjami autoryzacji, szyfrowania i zapewnienia integralności oryginalnych pakietów. Chodzi o uzyskanie pewności, iż nie będą one po drodze odczytywane czy modyfikowane przez użytkowników Internetu. Należy bowiem podkreślić, iż tunelowanie służy jedynie realizacji przeźroczystej transmisji, czyli de facto umożliwia stworzenie wirtualnej sieci prywatnej (VPN) w jej wymiarze komunikacyjnym. Jako takie nie gwarantuje jednak absolutnego bezpieczeństwa, stanowiąc dopiero punkt wyjścia do jego osiągnięcia.

Bezpieczne połączenie VPN jest zestawiane według typowej architektury klient-serwer. Klientem jest strona inicjująca (np. oddalony komputer) żądająca dostępu do zasobów, zaś serwerem urządzenie akceptujące połączenie (zwykle router). Jeżeli klientem jest router, który potrafi w imieniu wielu lokalnych hostów zestawić połączenie do odległego serwera VPN, jest on zwykle określany bramą VPN (ang. *VPN gateway*). Ustanowiony tunel VPN stanowi odpowiednik jeszcze jednego fizycznego interfejsu routera. Taki wirtualny interfejs pojawia się normalnie w tablicy routingu i można go wykorzystać podczas definiowania trasy statycznej do odległej prywatnej podsieci, czy też uwzględnić w routingu dynamicznym RIP. Istnieje też możliwość skierowania trasy domyślnej do wnętrza tunelu VPN.

Implementacja zdalnego dostępu w routerze Vigor

Routery DrayTek mogą pełnić rolę zarówno serwera, jak i klienta VPN. Oznacza to możliwość bezpiecznego łączenia odległych sieci lokalnych, oraz zezwalania na dostęp pojedynczym, oddalonym komputerom. Dodatkowo modele z indeksem „i" dysponujące interfejsem ISDN BRA mogą realizować obie formy zdalnego dostępu poprzez łącza ISDN (wykorzystując to samo tunelowanie IP, jednak przesyłając pakiety w kanale ISDN zestawionym bezpośrednio pomiędzy klientem i serwerem). ISDN nie oferuje dużych przepływności, jednak wprowadza dodatkowy element bezpieczeństwa – dane nie są bowiem transmitowane poprzez Internet.

Tunel VPN może być aktywowany tylko na żądanie (ang. *on demand*) dla przesłania małej porcji danych, po czym automatycznie rozłączany. Połączenia mogą być zestawiane poprzez Internet (z wykorzystaniem publicznego adresu IP routera), lub w ramach sieci lokalnej (z wykorzystaniem drugiego adresu IP interfejsu LAN).

Vigor realizuje także tzw. VPN pass-through, to znaczy potrafi pośredniczyć w zestawianiu tunelu pomiędzy urządzeniem znajdującym się w sieci lokalnej (np. innym routerem lub komputerem ukrytym za NAT) a urządzeniem odległym. W trybie pass-through Vigor nie ingeruje w procesy zachodzące w tunelu, a tylko przekazuje pakiety pomiędzy jego właściwymi końcami (klientem i serwerem).

Konfiguracja

Po wybraniu opcji VPN i Dostęp Zdalny otwiera się okno główne. Oferuje ono dostęp do podstawowych obszarów ustawień o charakterze ogólnym, oraz do ustawień poszczególnych profili połączeń.

Protokoły VPN

Router Vigor obsługuje komunikację VPN bazującą na popularnych i sprawdzonych protokołach, opracowanych przez największych producentów sprzętu i oprogramowania (Cisco Systems, Microsoft Corporation) oraz ujednoliconych i przyjętych jako standardy przez organizację IETF (ang. *Internet Engineering Task Force*), opracowującą standardy komunikacji dla sieci Internet.

Aby uruchomić tryb VPN pass-through na rzecz właściwego serwera VPN pracującego w sieci lokalnej za routerem Vigor, należy w routerze Vigor wyłączyć obsługę odpowiedniego protokołu VPN. Ponadto aby umożliwić klientom z zewnątrz inicjowanie połączeń należy odpowiednio skonfigurować mechanizm NAT. Chodzi o wykonanie przekierowania portu do serwera VPN (PPTP używa portu 1723 TCP, IPSec to port 500 UDP, zaś L2TP wykorzystuje port 1701 UDP).

PPTP

Włączenie obsługi protokołu PPTP oznacza, że router będzie potrafił zestawiać tunele według zasad zdefiniowanych tym protokołem. PPTP (ang. *Point-to-Point Tunneling Protocol*) jest stworzonym przez Microsoft sposobem realizacji prywatnych połączeń dwupunktowych poprzez sieć opartą na protokole IP. Połączenie dwupunktowe realizuje się za pomocą protokołu PPP, którego jednostki są przenoszone (enkapsulowane) w pakietach IP tak, aby mogły dotrzeć do odległego celu (np. poprzez Internet). Klient i serwer VPN nawiązują połączenie wymieniając stosowne komunikaty sterujące, po czym powstaje uniwersalny tunel (pomost) IP, przenoszący sesję PPP. Na poziomie PPP realizowane są typowe dla tego protokołu mechanizmy uwierzytelniania, bądź opcjonalnie – szyfrowania. W fazie IPCP można także realizować negocjację adresów IP. Odległy komputer lub router NAT otrzymuje od serwera adres wzięty z lokalnej sieci prywatnej, dzięki czemu staje się jej logicznym członkiem. Natomiast w trybie LAN-to-LAN oba końce połączenia PPP mogą zaproponować własne adresy IP, aby realizować klasyczny routing w obu kierunkach. Po ustanowieniu sesji PPP następuje normalna wymiana prywatnych pakietów. Istotę tunelowania PPTP przedstawiono na rysunku:

W rzeczywistości do logicznej obsługi połączenia wykorzystuje się protokół TCP (port 1723), który transportuje ramki PPP zawierające oryginalne pakiety IP. Na rysunku dla uproszczenia nie uwzględniono nagłówka TCP, zaznaczono natomiast obecność nagłówka ramki PPP.

Protokół PPTP nie posiada tak rozwiniętego systemu zabezpieczeń jak np. IPSec (patrz dalej). Umożliwia jednak komputerom-klientom z systemem MS Windows na efektywną, szybką współpracę z routerem Vigor jako serwerem VPN. System Windows NT/Windows 2000 Server może także pracować jako serwer VPN obsługujący tunel PPTP do routera Vigor (LAN-to-LAN). W takich sytuacjach Vigor potrafi obsłużyć dodatkowe rozszerzenia PPP stworzone przez Microsoft (autoryzacja MS CHAP, szyfrowanie MPPE). Informacje o PPTP można znaleźć w RFC 2637.

IPSec

Uruchomienie obsługi mechanizmów IPSec umożliwi routerowi realizację złożonych zasad zabezpieczeń przewidzianych przez ten protokół dla połączeń VPN. Określenie protokół w przypadku IPSec jest uwarunkowane historycznie i nie oddaje obecnego stan rzeczy. W istocie bowiem jest to silnie rozbudowany i ciągle rozwijany zestaw protokołów, mających na celu zabezpieczenie komunikacji bazującej na IP. I tak, oddzielne standardy określają metody przenoszenia (enkapsulacji) prywatnych pakietów poprzez sieć publiczną, sposoby ich szyfrowania i autoryzacji oraz sposoby wzajemnego uwierzytelniania komunikujących się stron. Każda z tych dziedzin oferuje całe grupy algorytmów, które mogą być automatycznie uzgadniane podczas nawiązywania połączenia VPN lub trwale przyjęte po obu końcach. Parametry te mogą być renegocjowane po upłynięciu określonego czasu. Sam proces negocjowania zasad zabezpieczeń jest realizowany przez specjalnie do tego stworzone protokoły.

Podstawowym zagadnieniem IPSec jest realizacja komunikacji – przewiduje się tryb tunelowania oraz tryb transportu. Jeżeli nie istnieje potrzeba ukrycia i zabezpieczenia nagłówków oryginalnych pakietów, tunel nie jest konieczny. Tryb transportowy przewiduje bowiem te same algorytmy szyfrowania czy autoryzacji, jednak stosują się one tylko do pola danych. Oryginalny nagłówek pakietu nie jest ukrywany (pozostaje czytelny), aby mógł brać udział w normalnym routingu poprzez Internet (patrz seria rysunków dalej).
Kolejnym aspektem IPSec, dotyczącym zarówno trybu tunelowania jak i transportu, jest poziom zabezpieczenia realizowanej komunikacji.

Koncepcja nagłówka autoryzacji **AH** (ang. *Authentication Header*) polega na użyciu specjalnych algorytmów kluczujących (ang. *hash funcion*) w celu uwierzytelnienia strony zdalnej oraz zapewnienia integralności przenoszonej informacji. Uwierzytelnianie pozwala uzyskać pewność, że urządzenie wysyłające dane jest ciągle tym samym urządzeniem, tzn. że nikt niepowołany nie występuje w jego imieniu. Integralność natomiast daje gwarancje, że dane wysłane przez zaufaną stronę nie zostały po drodze celowo zmienione przez kogoś trzeciego. W ramach AH Vigor pozwala wykorzystać algorytm MD5 (ang. *Message Digest 5*) lub SHA-1 (ang. *Secure Hash Algorithm-1*). Algorytmy te używają tajnego klucza (16 bajtowego dla MD5 i 20 bajtowego dla SHA-1), aby na podstawie przenoszonej porcji informacji wyliczyć pewien ciąg danych (tzw. *digest message*), nazywany niekiedy skrótem. Ciąg ten jest dołączany do oryginalnej informacji w postaci dodatkowego nagłówka AH. Po odebraniu pakietu następuje niezależne obliczenie ciągu AH i jego porównanie z wartością oryginalną, wydobytą z wnętrza pakietu. Jeżeli ciągi są różne, pakiet jest odrzucany jako nie budzący zaufania.

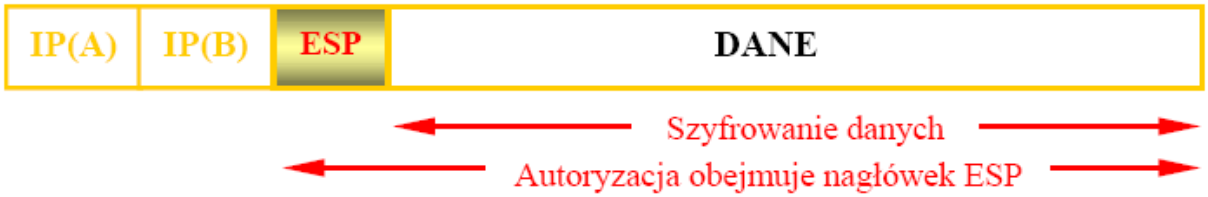
Należy podkreślić, że w wypadku przejęcia pakietów protokół AH nie zabezpiecza przed odczytem ich zawartości, gdyż jej nie modyfikuje. Aby uczynić przenoszoną informację niemożliwą do odczytania dla strony trzeciej, należy zastosować mechanizm szyfrowania. W ramach IPSec funkcjonuje oddzielny protokół **ESP** (ang. *Encapsulating Security Payload*), który obok własnych funkcji uwierzytelniania realizuje także szyfrowanie informacji zawartej w pakiecie. Router Vigor w wypadku opcji ESP pozwala na wybór algorytmów szyfrujących DES i 3DES (ang. *Data Encryption Standard*), oraz nowszego, szybkiego algorytmu AES (ang. *Advanced Encryption Standard*). Analogicznie do techniki AH, generowany jest nagłówek ESP niosący pewne kluczowe dla strony zdalnej informacje, niezbędne podczas weryfikacji informacji po drugiej stronie tunelu.

Tak więc Vigor w ramach ESP może realizować:

- szyfrowanie DES (z pominięciem procesu autoryzacji pakietów)
- szyfrowanie 3DES (z pominięciem procesu autoryzacji pakietów)
- szyfrowanie AES (z pominięciem procesu autoryzacji pakietów)
- szyfrowanie DES w połączeniu z autoryzacją SHA-1 lub MD5
- szyfrowanie 3DES w połączeniu z autoryzacją SHA-1 lub MD5
- szyfrowanie AES w połączeniu z autoryzacją SHA-1 lub MD5

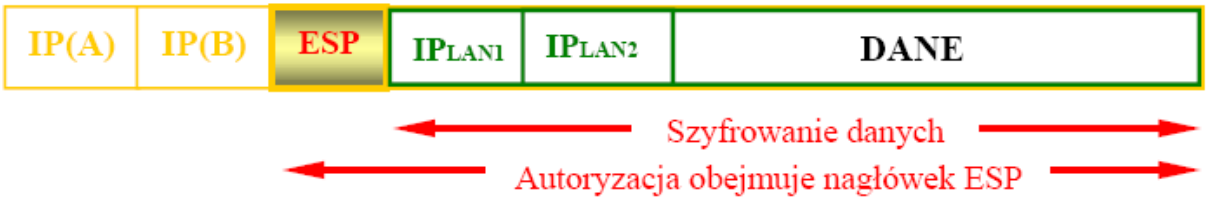
Podsumowując, IPSec przewiduje następujące metody realizacji bezpiecznej komunikacji za pomocą protokołu IP:
1. Tryb transportu z opcją zabezpieczeń AH:

2. Tryb transportu z opcją zabezpieczeń ESP:



3. Tryb tunelowania z opcją zabezpieczeń AH. Oryginalny pakiet IP łącznie z nagłówkiem jest enkapsulowany wewnątrz nowego pakietu celem ukrycia oryginalnych adresów prywatnych. Powstaje przezroczysty, autoryzowany pomost pomiędzy sieciami:

4. Tryb tunelowania z opcją zabezpieczeń ESP. Oprócz ukrycia adresów prywatnych następuje ich zaszyfrowanie wraz z ewentualną autoryzacją zaszyfrowanej informacji. Powstaje przezroczysty, autoryzowany i szyfrowany pomost pomiędzy odległymi sieciami:

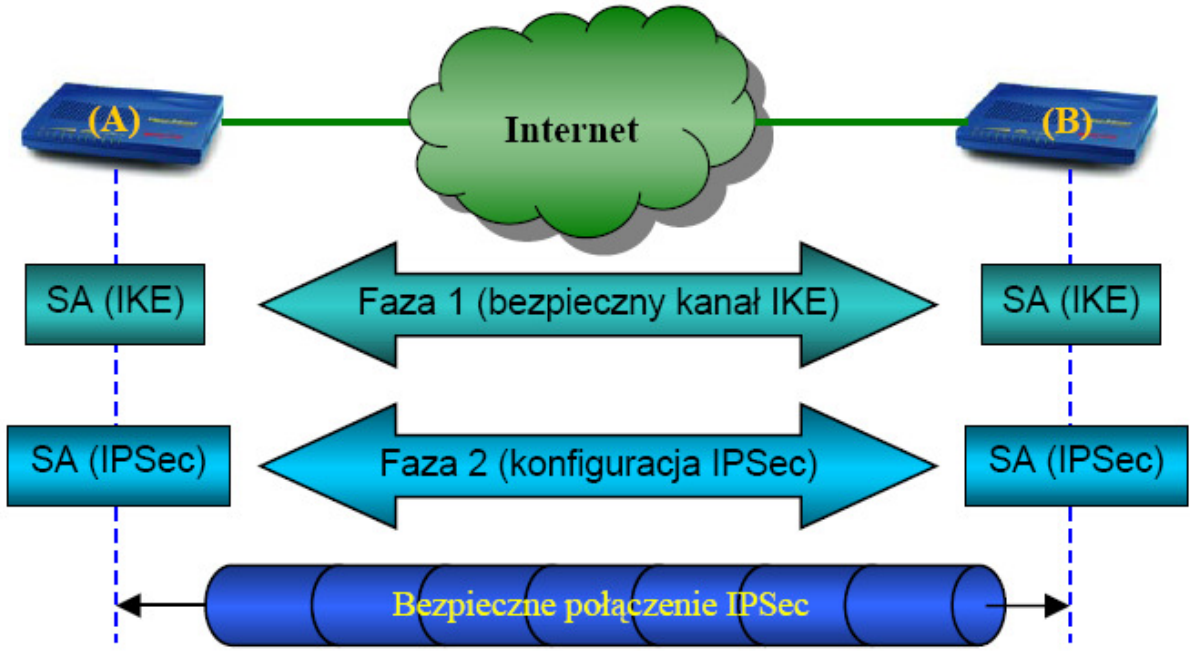


Na rysunkach dla uproszczenia pominięto fakt, że do obsługi tunelu IPSec używa się transportu UDP o numerze portu 503. W praktyce tryb tunelu stosuje się w sytuacji kiedy przynajmniej na jednym końcu połączenia występuje brama VPN obsługująca lokalne hosty (np. router). Natomiast dla bezpiecznego połączenia dwóch komputerów (pojedyncze adresy IP) bądź odległych sieci stosujących adresy publiczne, odpowiedni będzie tryb transportu. Niemniej i w takim przypadku można zastosować tunel – np. celem zaszyfrowania rzeczywistych adresów IP, co pozwala na ukrycie wewnętrznej struktury obu połączonych sieci.
Szczegóły mechanizmów IPSec zostały opisywane w serii dokumentów RFC (m.in. podstawowe RFC 1825/2401/3168, dalej seria RFC 2402 – 2406 i inne).

Protokoły AH i ESP dotyczą operacji niskiego poziomu, definiując różne sposoby bezpiecznego przekazu informacji. Jak to zostało pokazane, operacje szyfrowania czy autoryzacji mogą być potencjalnie realizowane przez wiele różnych algorytmów. Co więcej, każdy algorytm korzysta z tajnego, symetrycznego klucza, który musi być znany obu stronom przed nawiązaniem komunikacji VPN. Dodatkowo przyjmuje się, że klucze powinny być co jakiś czas zmieniane, aby udaremnić ich odkrycie na podstawie długookresowej analizy przechwyconej informacji. Wszystko to sprawia, że proces ręcznej konfiguracji parametrów połączeń staje się wysoce nieefektywny, zwłaszcza gdy

pojawia się potrzeba zespolenia wielu odległych lokalizacji według topologii każdy z każdym (ang. *mesh*) za pomocą IPSec. Dlatego IPSec przewiduje wykorzystanie oddzielnego protokołu, przeznaczonego specjalnie do automatycznej negocjacji parametrów połączenia. Jest to protokół **IKE** (ang. *Internet Key Exchange*), definiujący szereg operacji bezpiecznego negocjowania i późniejszego odświeżania parametrów wymaganych przez mechanizmy IPSec. Uzgodniony przez oba końce połączenia zbiór parametrów bezpieczeństwa jest określany mianem skojarzenia SA (ang. *Security Association*). SA obejmuje zatem tryb transmisji (AH czy ESP), konkretne algorytmy dla AH i ESP, klucze dla tych algorytmów, czas, po jakim należy renegocjować klucze itp. IKE jest bardzo złożonym mechanizmem, bazującym m. in. na starszych protokołach ISAKMP oraz Oakley. Bywa nawet zamiennie nazywany ISAKMP (z taką nomenklaturą można się spotkać konfigurując niektóre parametry VPN w urządzeniach Cisco).

Negocjacje, zmierzające do ustanowienia bezpiecznego połączenia VPN przebiegają w dwóch podstawowych fazach:



Faza pierwsza – IKE ustanawia pomocnicze skojarzenie SA, tworząc bezpieczny kanał do negocjowania właściwych parametrów IPSec. Najpierw następuje weryfikacja tożsamości obu stron za pomocą wcześniej ustalonych kluczy (ang. *pre-shared key*) bądź systemu specjalnych certyfikatów. Następnie negocjowane są metody szyfrowania i autoryzacji pakietów, które mają chronić kanał IKE w fazie właściwej negocjacji parametrów połączenia IPSec.

Faza druga – pod ochroną zestawionego połączenia, IKE przystępuje do ustalania szczegółów, które będą obowiązywać dla danego połączenia IPSec. Strony uzgadniają m. in. sposób komunikacji (transport czy tunel) oraz rodzaj jej zabezpieczenia (ESP czy AH). Dla ESP i AH negocjuje się odpowiednie algorytmy oraz ustala klucze, jakie będą przez nie wykorzystywane. Wybór kluczy nie następuje bezpośrednio – wybiera się raczej matematyczny punkt wyjścia do ich uzyskania, podając numer tzw. grupy DH (ang. *Diffie-Helman group*). Tak powstaje skojarzenie SA, czyli zbiór parametrów IPSec niezbędnych do przesyłania danych w danym kierunku. Te same parametry negocjowane są oddzielnie dla przeciwnego kierunku przepływu pakietów – połączenie IPSec wymaga ustanowienia dwóch SA.

W ramach każdej z faz strony przyjmują pewien maksymalny okres czasu, po którym powinna nastąpić ponowna negocjacja kluczy. Renegocjacja (zwłaszcza w fazie 2 IKE) zachodzi bardzo szybko, dzięki czemu sieć VPN nie wymaga powtarzających się, żmudnych ingerencji administratora. Raz skonfigurowane połączenie IPSec może być rozłączane i ponownie automatycznie ustanawiane bez obniżenia poziomu bezpieczeństwa. Po zestawieniu tunelu pakiety są oznaczane indeksem SPI (ang. *Security Parameters Index*), który jest liczbą losową wybraną podczas

negocjacji. Mówi on obu stronom połączenia, które skojarzenie SA należy zastosować do obsługi pakietu, czyli identyfikuje tunel.

Powyższy opis prezentuje podstawy funkcjonowania IKE. Szczegóły zdefiniowano między innymi w RFC 2408/2407/2409/2412. Router Vigor obsługuje obie fazy IKE, z tym, że w fazie pierwszej wstępna autoryzacja jest przeprowadzana w oparciu o wspólny, wpisany po obu stronach klucz (pre-shared key). Stosowne komentarze znajdują się dalej – w ramach opisu konkretnych ustawień.

L2TP

Zaznaczenie tego pola w oknie Media i protokoły włączy obsługę protokołu L2TP (ang. *Layer 2 Tunneling Protocol*). Jest to następca opracowanego przez Cisco protokołu L2F (ang. *Layer 2 Forwarding*), który miał za zadanie tunelowanie protokołów warstwy 2 wewnątrz innych protokołów. W wypadku sesji PPP umożliwiało to m.in. przedłużenie połączenia PPP (normalnie kończącego się w serwerze dostawcy usług) bezpośrednio do routera brzegowego firmy. L2TP został opracowany przez IETF. Łączy on zalety L2F oraz PPTP, oferując niezbędne dla komunikacji internetowej opcje szyfrowania i autoryzacji. Podobnie jak PPTP, L2TP pozwala przenosić sesję PPP poprzez sieć IP. Jednak posiada bardziej rozwiniętą obsługę połączeń, co jest osiągane przez wprowadzenie specjalnego nagłówka L2TP, obecnego w każdym pakiecie IP:

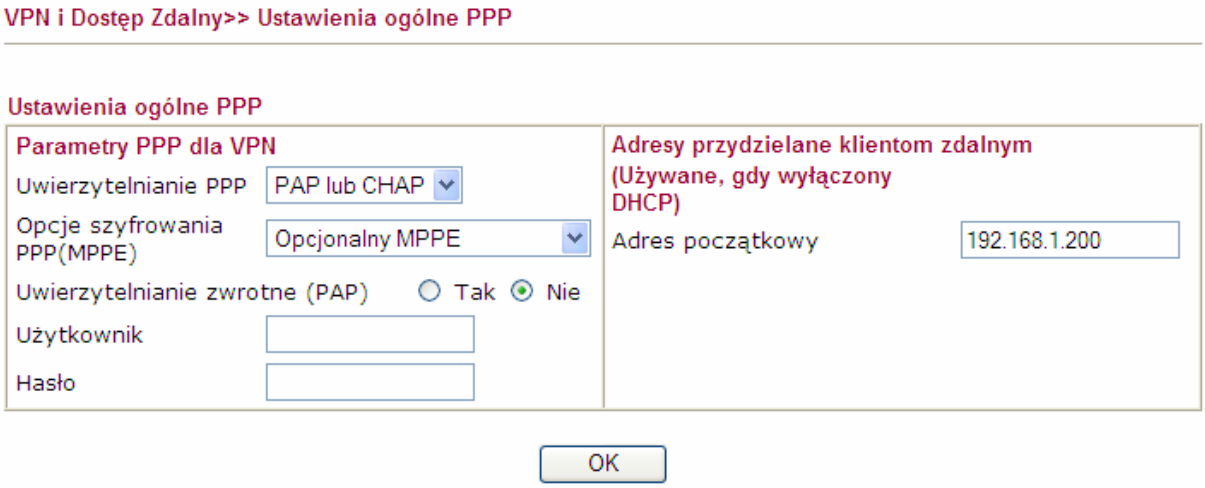
Tunelowanie w sieci IP korzysta z transportu UDP (port 1701), zaś niezawodność jest zagwarantowana na poziomie L2TP. Tworzone są w tym celu logiczne kanały danych, oraz odpowiednie kanały sterujące komunikacją. Na rysunku pominięto nagłówek UDP, aby uwypuklić obecność nagłówka L2TP, poprzedzającego ramkę PPP niosącą właściwy pakiet IP.

Wraz z rozwojem architektury IPSec opracowano standard VPN znany jako L2TP over IPSec. Jest to ustanowienie bezpiecznego połączenia IPSec po to, aby w jego wnętrzu zrealizować połączenie L2TP. Łączne zastosowanie zalet obu protokołów przynosi konkretne korzyści. L2TP nie posiada bowiem tak bogatego systemu zabezpieczeń jak IPSec, zatem wprowadzając dodatkowo np. szyfrowanie uzyskuje się znaczną jego poprawę. Z drugiej strony, IPSec stanowi system zabezpieczeń opracowany wyłącznie dla pakietów IP. Wprowadzenie do tunelu IPSec połączenia L2TP pozwala np. realizować kontrolę dostępu (nazwa użytkownika i hasło), i negocjować adresy IP wewnątrz tunelu (z wykorzystaniem PPP).

Router Vigor potrafi obsłużyć zarówno połączenia L2TP, jak i L2TP over IPSec. Protokół L2TP został opisany m. in. w RFC 2661 i 2889, zaś L2TP over IPSec opisano w RFC 3193.

Ustawienia ogólne PPP

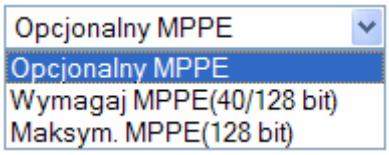
Okno to dotyczy wyłącznie metod zdalnego dostępu korzystających z protokołu PPP (połączenia ISDN oraz PPTP, L2TP i L2TP over IPSec). Ustawienia tutaj zawarte wykorzystywane są w sytuacji, kiedy odległy węzeł jest pojedynczym komputerem lub routerem NAT nie posiadającym stałego adresu IP, bądź kiedy adres proponowany przez zdalny węzeł nie może być zaakceptowany przez router Vigor podczas negocjacji PPP.



Uwierzytelnianie PPP– narzucenie strategii uwierzytelniania dla sesji PPP inicjowanej przez zdalny węzeł:

- **Tylko PAP** – akceptowany będzie wyłącznie protokół PAP (ang. *Password Authentication Protocol*). Jest to prosty mechanizm, polegający na wysyłaniu parametrów autoryzacji w postaci jawnej, i oczekiwaniu na odpowiedź pozytywną bądź odrzucenie przez odległy system.
- **PAP lub CHAP** – jako pierwszy zostanie zaoferowany bezpieczniejszy protokół CHAP (ang. *Challenge-Handshake Authentication Protocol*), który utrudnia przechwycenie parametrów autoryzacji dzięki ich utajnieniu. Muszą one być oprócz tego wysyłane w losowych odstępach czasu na żądanie routera, wielokrotnie podczas trwania sesji PPP. Jeżeli druga strona (odległy węzeł) nie obsługuje metody CHAP, router zaproponuje protokół PAP. Vigor obsługuje zwykły CHAP oraz MS-CHAP i MS-CHAPv2.

Opcje szyfrowania PPP (MPPE) – negocjowanie opcji szyfrowania według standardu MPPE (ang. *Microsoft Point-to-Point Encryption Protocol*). Jest to opracowany przez Microsoft stosunkowo nowy standard szyfrowania sesji PPP za pomocą algorytmu RSA RC-4 (klucz 40 lub 128 bitów). Można wymusić szyfrowanie jako warunek przyznania dostępu, lub potraktować MPPE jako dodatkową opcję proponowaną zdalnemu węzłowi:



Uwierzytelnianie zwrotne (PAP) – jeżeli zdalny węzeł wymaga od routera uwierzytelnienia zwrotnego, operacja taka może być wykonana wyłącznie kiedy zaznaczona jest opcja **Tak**. W pola **Nazwa użytkownika** i **Hasło** należy wpisać ciągi znaków, które mają być w takiej sytuacji wysyłane przez router. Uwierzytelnianie obustronne jest obsługiwane tylko w trybie PAP.

Adresy przydzielane klientom zdalnym – w polu podaje się adres IP należący do sieci lokalnej (domyślnie 192.168.1.200). Adres ten zostanie przydzielony zdalnemu węzłowi dla potrzeb prywatnego routingu wewnątrz tunelu. Dysponując adresem wziętym z lokalnej podsieci, węzeł staje się jej logicznym członkiem i może komunikować się z innymi hostami. Jeżeli w tym samym czasie inny węzeł zażąda dostępu, otrzyma kolejny adres (np. 192.168.1.201), itd.

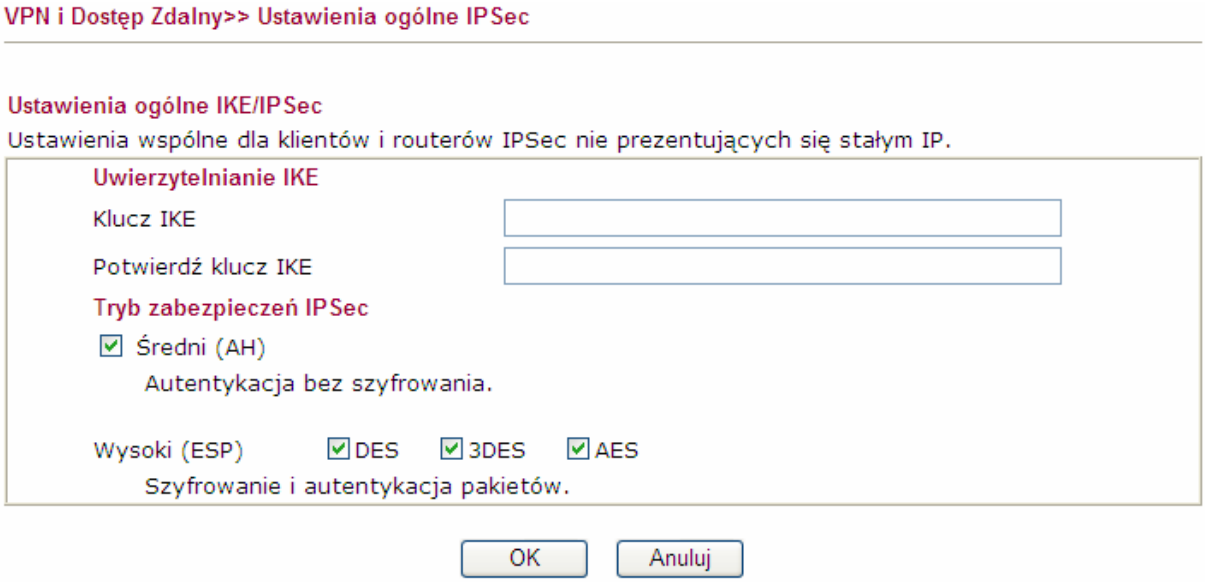
W przypadku tunelu PPP realizowanego poprzez Internet, zdalny węzeł będzie posiadał publiczny (zwykle zmienny) adres IP, który zostanie wykorzystany do samego zestawienia tunelu. Nie należy go jednak mylić z adresem

prywatnym, używanym wewnątrz tunelu – może on być dynamicznie przydzielony przez router Vigor w ramach negocjacji PPP (faza IPCP).

Jeżeli zdalny węzeł prezentuje się stałym adresem IP czy numerem ISDN (co zwykle oznacza że nie zmienia on swojego położenia), może realizować indywidualną negocjację adresów według wytycznych skonfigurowanych w danym profilu LAN-to-LAN (patrz dalej). Każda ze stron proponuje wówczas własny adres IP i następuje próba ustanowienia połączenia routowanego. W rezultacie w tablicy routingu pojawia się wirtualny interfejs (IF4-IF11) i pozycja informująca o zdalnej podsieci. Niemniej jeżeli negocjacja adresów nie skończy się sukcesem (np. wskutek niewłaściwej konfiguracji parametrów IP w profilu LAN-to-LAN), router może skorzystać z powyższego adresu i zaproponować go stronie zdalnej. Odległy router wykorzysta ten adres na drugim końcu połączenia PPP, przez co stanie się dla routera Vigor bramą do zdalnej podsieci.

Ustawienia ogólne IKE/IPSec

Jeżeli zdalny węzeł (komputer lub router) posiada stały adres IP/numer ISDN, którym się zawsze prezentuje, można go obsługiwać za pomocą indywidualnego profilu LAN-to-LAN czy Użytkownicy zdalni. Dla zdalnych węzłów chcących realizować dostęp IPSec spod różnych adresów IP/numerów ISDN w poniższym oknie ustawia się wspólne (tzn. takie same) parametry IKE/IPSec:



Uwierzytelnienie IKE – dotyczy pierwszej fazy IKE:

Klucz IKE – klucz pre-shared key wymagany do wzajemnego uwierzytelnienia stron, rozpoczynającego pierwszą fazę IKE (patrz wcześniej - opis faz IKE). Należy go potwierdzić, wpisując ponownie w polu poniżej.

Metoda zabezpieczeń IPSec – dotyczy drugiej fazy IKE:

- **Średni (AH)** – zaznaczenie tej opcji spowoduje wysłanie do strony inicjującej połączenie żądania użycia protokołu AH (druga faza IKE)
- **Wysoki(ESP)**: **DES/3DES/AES** – zaznaczenie którejkolwiek opcji spowoduje wysłanie do strony inicjującej żądania użycia protokołu ESP. Szyfrowanie będzie uzgadniane z uwzględnieniem zaznaczonych algorytmów. Jeżeli żaden z nich nie będzie obsługiwany przez stronę zdalną, połączenie nie dojdzie do skutku. Można tego uniknąć zaznaczając przynajmniej DES, gdyż jako obowiązkowy składnik każdej implementacji ESP musi on być obsługiwany przez każde urządzenie.

  Jednoczesne użycie AH i ESP oznacza, że pakiet zabezpieczony zgodnie z ESP będzie dodatkowo w całości autoryzowany protokołem AH.

Połączenia Host-LAN (użytkownik zdalny)

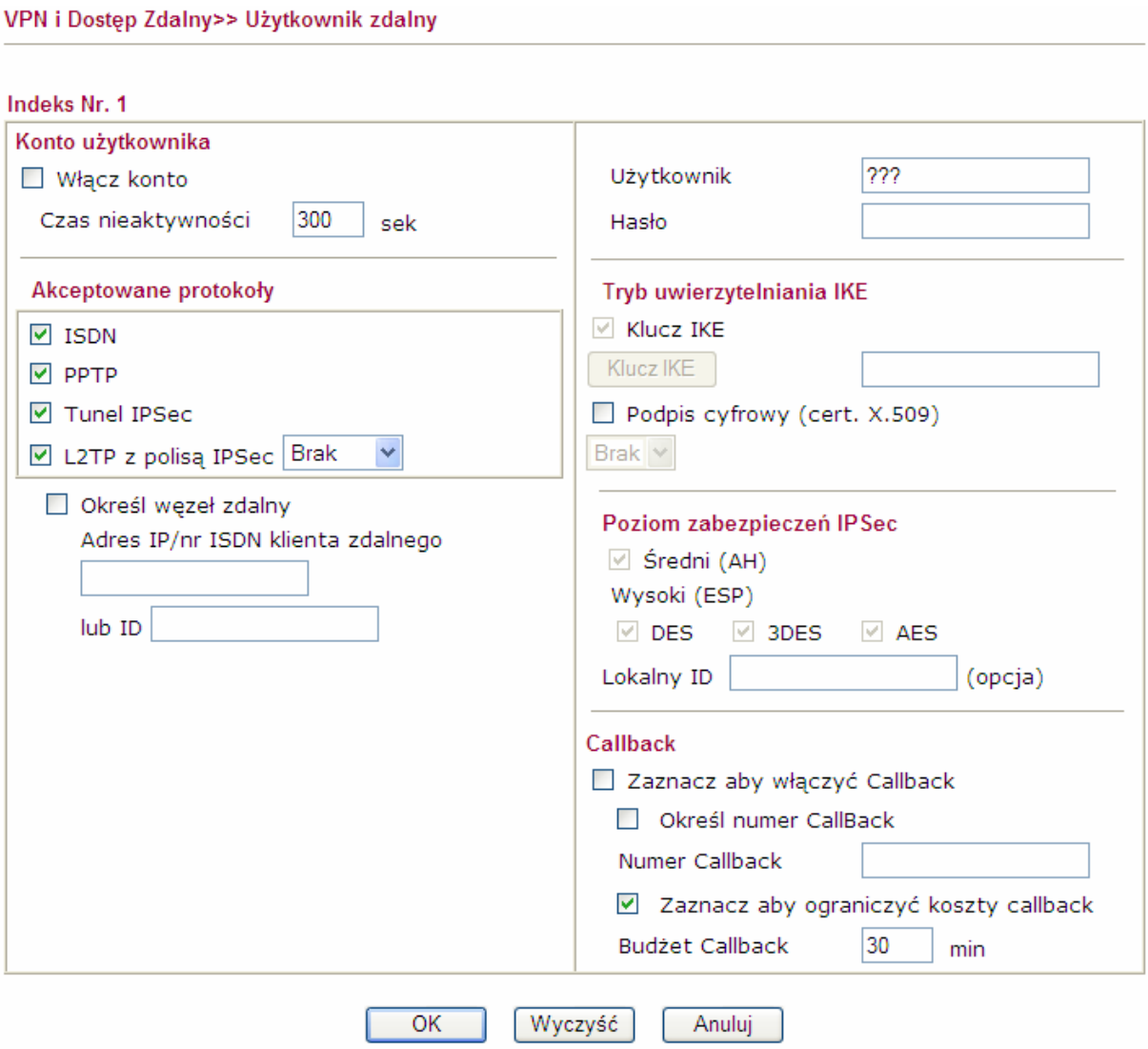
Definiuje się tutaj indywidualne prawa dostępu dla pojedynczych użytkowników zdalnych, przy czym chodzi wyłącznie o dostęp niesymetryczny, inicjowany przez pojedynczy komputer (ewentualnie router NAT) do routera Vigor jako serwera VPN. Vigor pozwala zdefiniować indywidualne konta użytkowników, zawierające niezależne ustawienia połączeń.

VPN i Dostęp Zdalny>> Użytkownik zdalny

Konta użytkowników zdalnych: | Ustawienia domyślne |

Indeks	Użytkownik	Status	Indeks	Użytkownik	Status
1.	???	X	17.	???	X
2.	???	X	18.	???	X
3.	???	X	19.	???	X
4.	???	X	20.	???	X
5.	???	X	21.	???	X
6.	???	X	22.	???	X
7.	???	X	23.	???	X
8.	???	X	24.	???	X
9.	???	X	25.	???	X
10.	???	X	26.	???	X
11.	???	X	27.	???	X
12.	???	X	28.	???	X
13.	???	X	29.	???	X
14.	???	X	30.	???	X
15.	???	X	31.	???	X
16.	???	X	32.	???	X

Omówienie profilu użytkowników zdalnych:



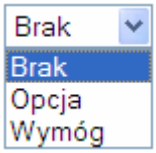
Włącz konto – włączenie konta sprawi, że będzie ono brane pod uwagę podczas obsługi połączeń inicjowanych przez odległe węzły.

Czas nieaktywności – jeżeli połączenie VPN pozostaje niewykorzystane (brak transmisji przez określony czas), router Vigor jako serwer zarządzający czasem połączenia może je rozłączyć. Dynamiczne zestawianie i rozłączanie tuneli podnosi efektywność wykorzystania routera jako serwera VPN (większa liczba użytkowników obsłużonych w tym samym czasie).

Akceptowane protokoły – podaje się tutaj akceptowane protokoły VPN, których może użyć zdalny węzeł (klient VPN inicjujący połączenie):

- **ISDN** – możliwy jest „czysty" dostęp ISDN z wykorzystaniem protokołu PPP. Strona zdalna posługuje się numerem ISDN przypisanym do routera Vigor, po czym w fazie negocjacji IPCP otrzymuje adres IP wzięty z lokalnej podsieci (patrz wcześniej – Ustawienia ogólne PPP). Typowy klient to komputer z kartą (modemem) ISDN, zaś połączenie konfiguruje się tak samo jak połączenie PPP do Internetu (z uwzględnieniem właściwego dla routera numeru dostępowego i parametrów autoryzacji ustawionych w profilu).
- **PPTP** – tunel PPTP inicjowany przez węzeł dysponujący publicznym (niekoniecznie stałym) adresem IP. Będzie to np. klient PPTP wbudowany w system operacyjny Windows, pracujący na komputerze posiadającym dostęp do Internetu.

- **Tunel IPSec** – połączenie w trybie tunelowania IPSec (protokół AH i/lub ESP). Węzeł inicjujący to komputer z odpowiednim oprogramowaniem IPSec i dostępem do Internetu lub router NAT obsługujący IPSec.
- **L2TP z polisą IPSec** – tunel L2TP zabezpieczony na poziomie IP przez mechanizmy IPSec (tzw. *L2TP over IPSec*). Można wymagać od klienta obsługi IPSec, bądź zaproponować ją jako opcję dodatkową lecz niekonieczną:



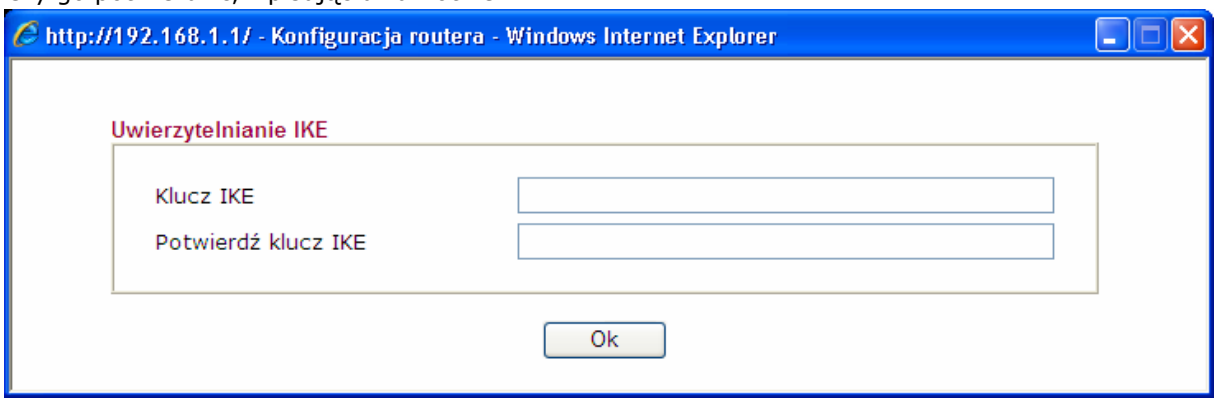
Dla opcji **Brak** możliwa będzie wyłącznie realizacja tunelu L2TP (bez IPSec).

Określ węzeł zdalny – opcję tę można zaznaczyć tylko w przypadku kiedy zdalny węzeł (klient VPN) posiada stały adres IP/numer ISDN, którym się prezentuje podczas każdego inicjowania dostępu.

Odpowiednią wartość należy wpisać w polu **Adres IP/nr ISDN klienta zdalnego**. Dostęp będzie możliwy wyłącznie spod tego adresu/numeru, co stanowi dodatkową ochronę (sprawdzenie tożsamości). W przypadku klienta stosującego IPSec jest to wymóg bezwzględny, tylko bowiem na tej podstawie możliwe będzie przydzielenie indywidualnych ustawień IKE/IPSec, tzn. skonfigurowanie profilu użytkownika. Dla klientów IPSec posiadających nieokreślony (zmienny) adres/numer obowiązują wspólne Ustawienia VPN IKE/IPSec. Natomiast dla połączeń VPN wykorzystujących PPP (PPTP/L2TP) można używać oddzielnych, indywidualnych profili użytkownika, nawet jeżeli druga strona (klient) nie dysponuje stałym adresem IP.
ID – pole pozwala wprowadzić dodatkowy ciąg znaków, określający konkretny tunel VPN.

Użytkownik/Hasło – parametry autoryzacji dostępu wykorzystywane w protokole PPP (dotyczy tylko dostępu opartego na protokołach ISDN, PPTP, L2TP, L2TP over IPSec). Możliwe jest wykorzystanie protokołu PAP lub CHAP w połączeniu z szyfrowaniem MPPE (obowiązują Ustawienia protokołu PPP – patrz wcześniej opis tego menu).
Po określeniu zdalnego węzła (IP lub numer ISDN) można zdefiniować indywidualne ustawienia dla protokołu IPSec:

Klucz IKE – klucz wstępny wymagany do wzajemnego uwierzytelnienia stron, rozpoczynającego pierwszą fazę IKE. Należy go potwierdzić, wpisując dwukrotnie:



Przydzielenie użytkownikowi indywidualnego klucza IKE jest możliwe dopiero po zaznaczeniu opcji **Określ węzeł zdalny** oraz wpisaniu zdalnego adresu lub numeru ISDN w polu poniżej.

Poziom zabezpieczeń IPSec – dotyczy drugiej fazy IKE:

- **AH** – zaznaczenie tej opcji spowoduje wysłanie do strony inicjującej połączenie żądania użycia protokołu AH (druga faza IKE)
- **DES/3DES/AES** – zaznaczenie którejkolwiek opcji spowoduje wysłanie do strony inicjującej żądania użycia protokołu ESP. Szyfrowanie będzie uzgadniane z uwzględnieniem zaznaczonych algorytmów. Jeżeli

żaden z nich nie będzie obsługiwany przez stronę zdalną, połączenie nie dojdzie do skutku. Można tego uniknąć zaznaczając przynajmniej DES, gdyż jako obowiązkowy składnik każdej implementacji ESP musi on być obsługiwany przez każde urządzenie.

Jednoczesne użycie AH i ESP oznacza, że pakiet zabezpieczony zgodnie z ESP będzie dodatkowo w całości autoryzowany protokołem AH.

Callback – dotyczy wyłącznie dostępu ISDN i pozwala wykorzystać opcję połączenia zwrotnego (ang. *Call-Back*) wbudowaną w PPP:

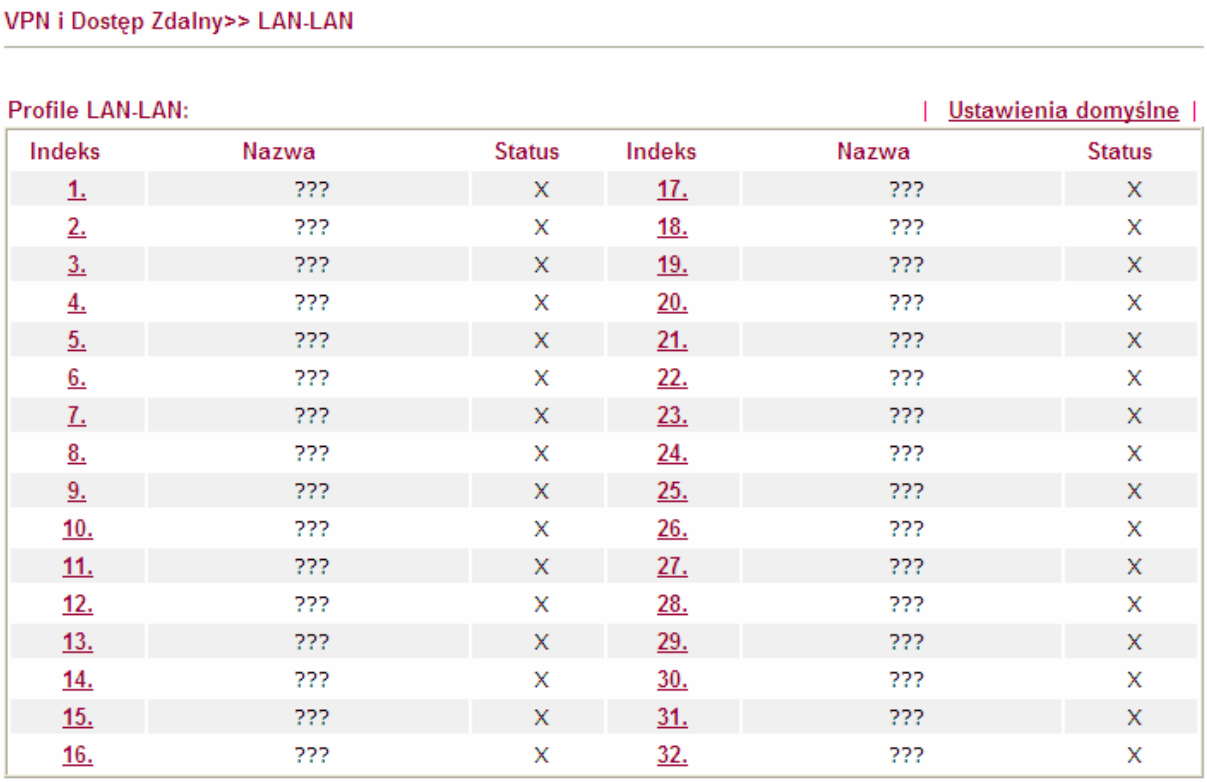
Zaznacz aby włączyć Callback – po zaznaczeniu tej opcji router po uwierzytelnieniu użytkownika może zaakceptować jego żądanie nawiązania połączenia zwrotnego (a więc na własny koszt).

Określ numer Callback – numer ISDN na który ma nastąpić ewentualne połączenie zwrotne

Zaznacz aby ograniczyć koszty Callback – można tutaj ograniczyć czas trwania, a tym samym koszty połączeń zwrotnych do wartości podanej w polu **Budżet Callback**.

LAN-to-LAN

Ta opcja zdalnego dostępu VPN dotyczy symetrycznego łączenia oddalonych sieci LAN na równorzędnych zasadach. Oznacza to, że połączenie VPN, o ile nie ma być zestawione na stałe, może być inicjowane przez każdą ze stron. Jest to możliwe dlatego, że Vigor potrafi pełnić rolę zarówno serwera, jak i klienta-bramy VPN. Drugą zasadniczą różnicą w relacji do dostępu typu „pojedynczy użytkownik/adres IP", jest możliwość realizacji routingu pomiędzy indywidualnymi adresami IP przez stworzenie osobnej pozycji w tablicy routingu każdego z routerów. Pozycja ta definiuje odległą podsieć jako dostępną za pośrednictwem wirtualnego interfejsu, w rzeczywistości oznaczającego konkretny tunel VPN. Poniższe okno pozwala zdefiniować do 32 profe połączeń typu LAN-to-LAN. Każdy z nich dotyczy innej sieci odległej:


VPN i Dostęp Zdalny>> LAN-LAN

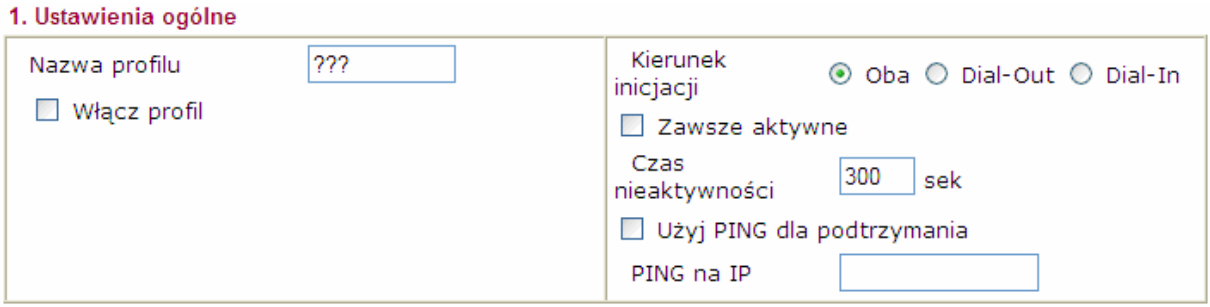
Profile LAN-LAN: | Ustawienia domyślne |

Indeks	Nazwa	Status	Indeks	Nazwa	Status
1.	???	X	17.	???	X
2.	???	X	18.	???	X
3.	???	X	19.	???	X
4.	???	X	20.	???	X
5.	???	X	21.	???	X
6.	???	X	22.	???	X
7.	???	X	23.	???	X
8.	???	X	24.	???	X
9.	???	X	25.	???	X
10.	???	X	26.	???	X
11.	???	X	27.	???	X
12.	???	X	28.	???	X
13.	???	X	29.	???	X
14.	???	X	30.	???	X
15.	???	X	31.	???	X
16.	???	X	32.	???	X

Profil LAN-LAN jest zbudowany z kilku elementów:

1. Ustawienia ogólne

W części pierwszej określa się parametry ogólne połączenia LAN-to-LAN:



Nazwa profilu – dowolny ciąg znaków, identyfikujący dany profil pośród innych zdefiniowanych w routerze (nazwa ma znaczenie lokalne, tzn. nie dotyczy samej realizacji połączenia)

Włącz profil – zdefiniowany profil należy włączyć, jeżeli ma on być aktywny, tzn. uwzględniany przez router w procesie komunikacji z innymi sieciami

Kierunek inicjacji – pozwala zarządzać prawem do inicjowania połączeń VPN, przydzielając je obu stronom lub tylko jednej. Należy podkreślić, iż nie chodzi tutaj o kierunek przepływu informacji, w aktywnym tunelu możliwa jest bowiem równorzędna komunikacja dwustronna. Chodzi natomiast o określenie, która strona może inicjować zestawianie połączenia dla potrzeb późniejszej komunikacji:

- **Oba** – router będzie mógł zarówno inicjować połączenie (wykorzystując ustawienia z obszaru Ustawienia Dial-Out), jak i je odbierać (zgodnie z menu Ustawienia Dial-In)
- **Dial-Out** – w ramach profilu możliwa będzie jedynie realizacja połączenia wychodzącego (ustawienia Ustawienia Dial-Out). Menu Odbiór połączeń nie będzie brane pod uwagę.
- **Dial-In** – tylko odbiór wywołań (router będzie odpowiadał na żądania zestawienia tunelu zgodnie z ustawieniami menu Ustawienia Dial-In). Ustawienia Nawiązywanie połączenia nie są wówczas brane pod uwagę.

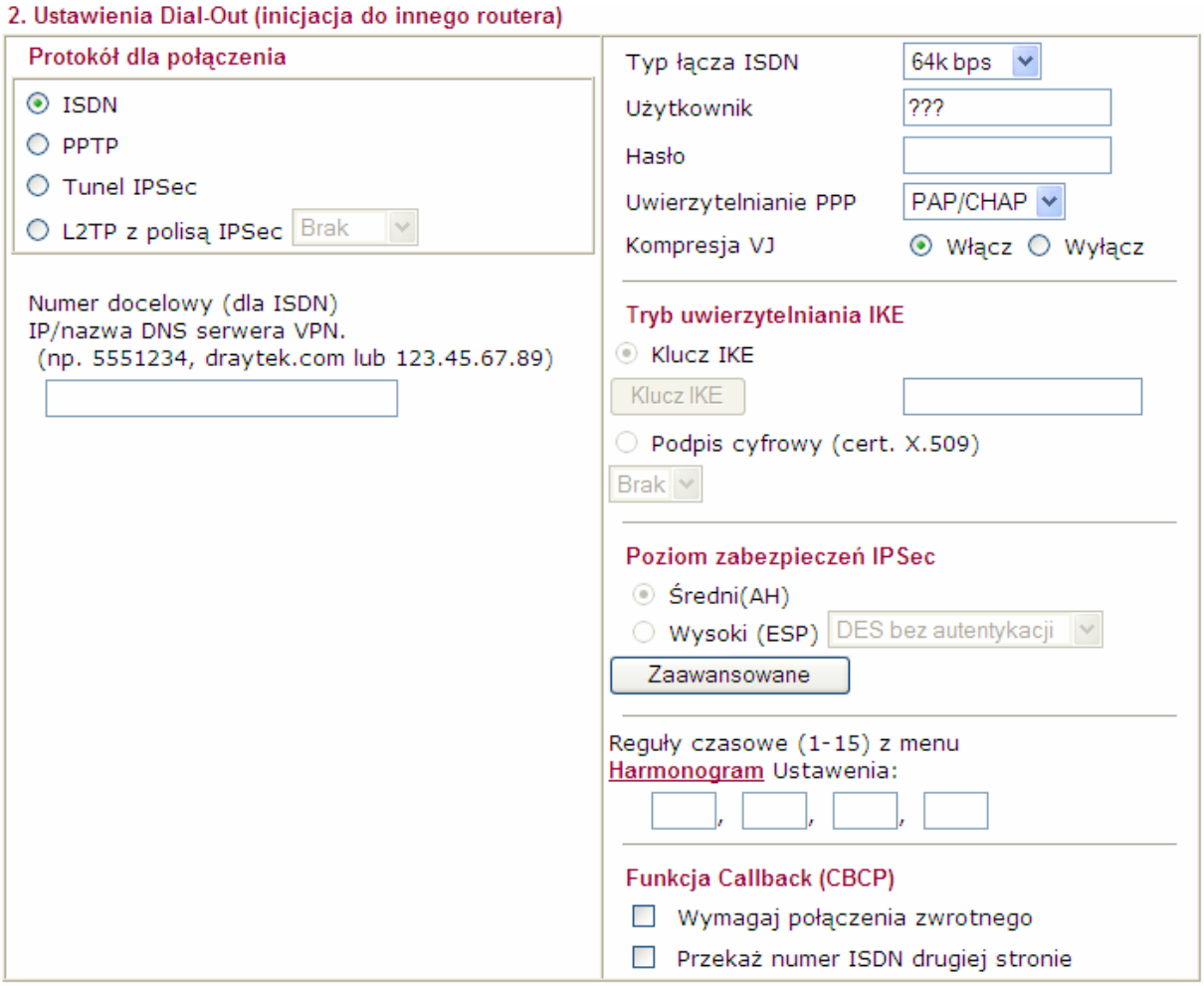
Zawsze aktywne – jeżeli tunel ma być utrzymywany ciągle, na wzór połączenia dzierżawionego, należy zaznaczyć tę opcję.

Czas nieaktywności – czas nieaktywności, po którym połączenie VPN pracujące w trybie „na żądanie" ma być rozłączane. Brak aktywności jest rozumiany jako brak wymiany pakietów pochodzących z sieci LAN.

Użyj PING do 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 **Ping na IP**. Tym samym można realizować ważną funkcję informowania drugiej strony połączenia (serwera VPN) o ewentualnych problemach z połączeniem na poziomie IP. Konkretnie, jeżeli nastąpi np. nagłe zerwanie połączenia z Internetem po stronie klienta, odległy serwer nie zostanie o tym poinformowany. Uzna on, iż brak pakietów oznacza brak aktywności hostów, i będzie normalnie oczekiwał na dalsze pakiety, np. IPSec. Jeżeli tunel był zestawiony na stałe, serwer nie zamknie połączenia, co z kolei może powodować kłopot z jego ponownym, rzeczywistym ustanowieniem przez klienta (po zniknięciu jego problemów z komunikacją IP). Natomiast zanik określonej liczby komunikatów ping będzie dla serwera informacją o kłopotach, jakich być może doświadcza strona zdalna, co spowoduje zamkniecie tunelu i gotowość do jego ustanowienia od nowa. Dlatego w polu poniżej powinien się znajdować adres zdalnego serwera VPN (dla samego podtrzymania aktywności można podać inny odległy adres IP).

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

Obszar następny zawiera parametry, które router wykorzysta do inicjowania połączenia do serwera VPN (np. innego routera):



Protokół dla połączenia – określa się tutaj konkretny protokół (jeden), który ma być użyty przez router podczas próby zestawienia tunelu z serwerem. Dla L2TP z polisą IPSec (L2TP over IPSec) można użyć mechanizmów IPSec jako opcji, lub wymusić ich stosowanie przez drugą stronę.

Numer docelowy (dla ISDN) IP/nazwa DNS servera VPN – kluczowy parametr precyzujący docelowy serwer VPN. Vigor do nawiązania łączności z serwerem może użyć jego adresu publicznego lub nazwy DNS. Opcja z nazwą jest o tyle istotna, że docelowy serwer może posiadać zmienny adres IP (przykładem jest usługa ADSL o komercyjnej nazwie Neostrada). Jeżeli zdalnym serwerem jest router Vigor, nożna na nim uruchomić klienta DynDNS, po czym kierować się stałą nazwą DNS po stronie klienta. Tunel taki będzie możliwy, dopóki nie nastąpi zmiana adresu IP serwera, jednak może być zestawiany na żądanie i rozłączany. W przypadku opcji ISDN (modele z indeksem „i") podaje się numer zdalnego serwera

Typ łącza ISDN – dotyczy tylko połączeń ISDN (modele z indeksem „i"):
64 kbit/s – połączenie z użyciem jednego kanału B
128 kbit/s – połączenie z użyciem dwóch kanałów B

Użytkownik/Hasło – parametry dostępu do serwera VPN dla sesji PPP (ISDN, PPTP, L2TP, L2TP over IPSec).

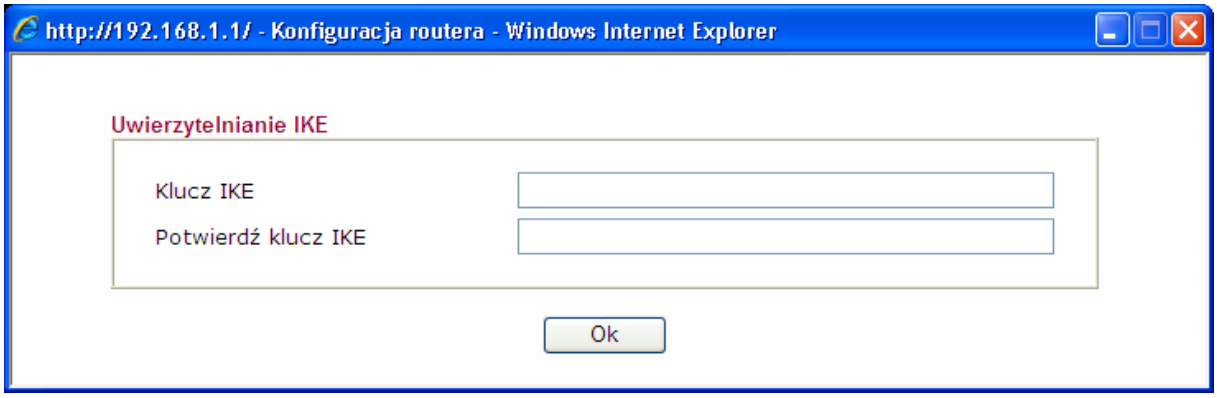
Uwierzytelnianie PPP – dotyczy strategii uwierzytelniania dla połączeń wykorzystujących protokół PPP (a więc wszystkich z wyjątkiem tunelu IPSec):

- **Tylko PAP** – realizowany będzie wyłącznie protokół PAP (ang. *Password Authentication* Protocol). Jest to prosty mechanizm, polegający na wysyłaniu parametrów autoryzacji w postaci jawnej, i oczekiwaniu na odpowiedź pozytywną bądź odrzucenie przez odległy system.

- **PAP/CHAP** – jako pierwszy będzie negocjowany bezpieczniejszy protokół CHAP (ang. *Challenge-Handshake Authentication Protocol*), który utrudnia przechwycenie parametrów autoryzacji dzięki ich utajnieniu. Muszą one być oprócz tego wysyłane w losowych odstępach czasu na żądanie routera, wielokrotnie podczas trwania sesji PPP. Jeżeli druga strona (odległy węzeł) nie obsługuje metody CHAP, router użyje protokołu PAP.

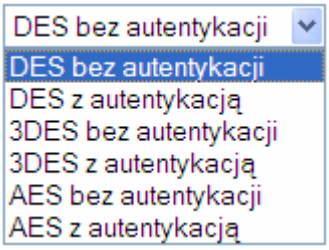
Kompresja VJ – opcja PPP kompresji nagłówka TCP według algorytmu Van Jacobsona (pozwala zwiększyć dostępne pasmo)
Kolejne ustawienia dotyczą wyłącznie połączeń wykorzystujących protokół IPSec:

Klucz IKE – klucz wstępny wymagany do wzajemnego uwierzytelnienia stron, rozpoczynającego pierwszą fazę IKE. Należy go potwierdzić, wpisując dwukrotnie:



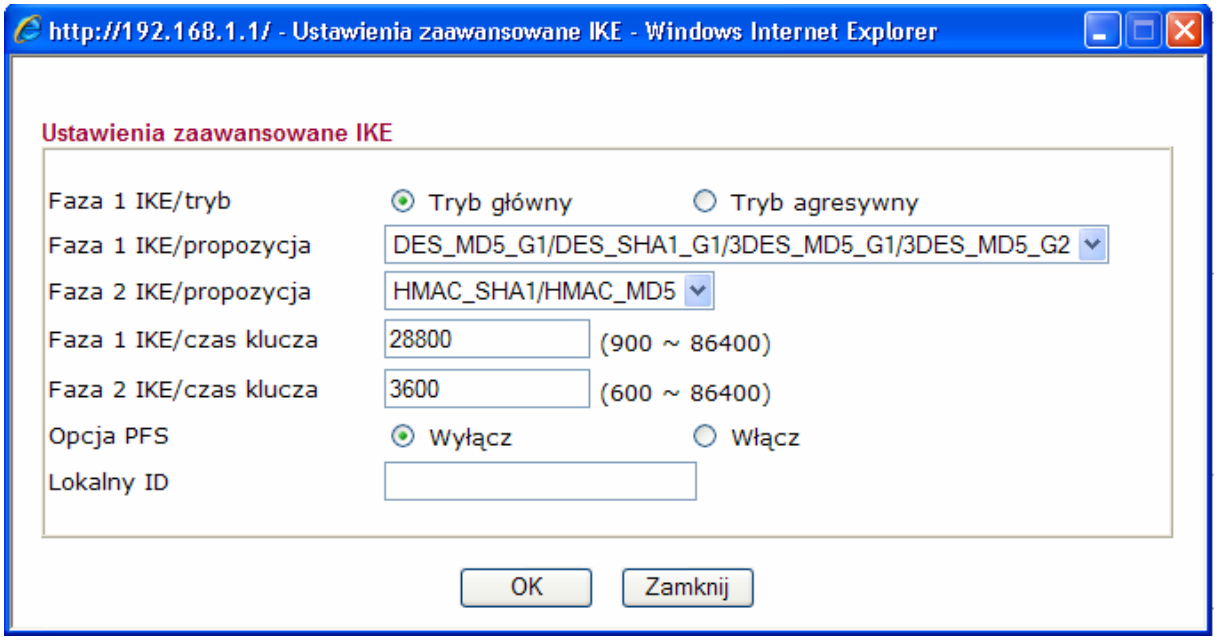
Poziom zabezpieczeń IPSec – dotyczy drugiej fazy IKE:

- **Średni (AH)** – zaznaczenie tej opcji spowoduje wysłanie do serwera żądania użycia protokołu AH (druga faza IKE)
- **Wysoki (ESP)** – zaznaczenie tej opcji spowoduje wysłanie do serwera żądania użycia protokołu ESP. Szyfrowanie i autoryzacja będą uzgadniane z uwzględnieniem wybranego algorytmu. Jeżeli żaden z nich nie będzie obsługiwany przez stronę zdalną, połączenie nie dojdzie do skutku:



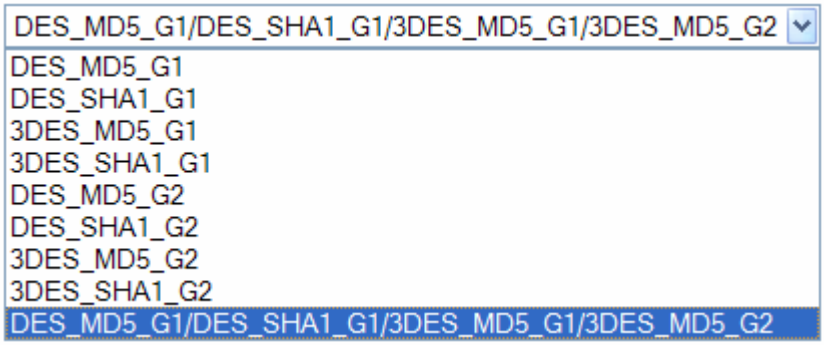
Jednoczesne użycie AH i ESP oznacza, że pakiet zabezpieczony zgodnie z ESP będzie dodatkowo w całości autoryzowany protokołem AH.

Zaawansowane – zaawansowane ustawienia dla procesu negocjacji IKE, indywidualne dla danego profilu:

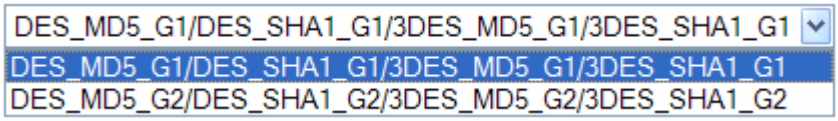


Faza 1 IKE/tryb – domyślnie negocjowanie w fazie pierwszej przebiegają według tzw. trybu standardowego.

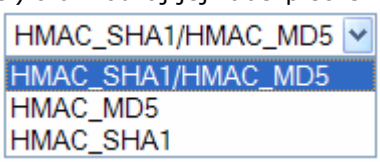
Faza 1 IKE/propozycja - polega on na wysyłaniu konkretnej propozycji, obejmującej algorytmy szyfrowania i autoryzacji oraz numer tzw. grupy Diffie-Helmana (ozn. literą G), która ma służyć wygenerowaniu kluczy szyfrujących. Po jej wysłaniu następuje oczekiwanie na zaakceptowanie bądź odrzucenie propozycji przez stronę zdalną (serwer). W wypadku braku akceptacji wysyłane są kolejne propozycje:



Można zmienić ustawienia domyślne, wymuszając prowadzenie negocjacji w tzw. trybie agresywnym, który jednak musi być obsługiwany przez implementację IKE po drugiej stronie połączenia. Jak widać, następuje tutaj przyspieszenie procesu negocjacji przez wysłanie oferty obejmującej kilka propozycji na raz:



Faza 2 IKE/propozycja – podobnie jak **Faza 1 IKE/propozycja** polega na wysyłaniu konkretnej propozycji. IKE przystępuje do ustalania szczegółów, które będą obowiązywać dla danego połączenia IPSec. Strony uzgadniają m. in. sposób komunikacji (transport czy tunel) oraz rodzaj jej zabezpieczenia (ESP czy AH).



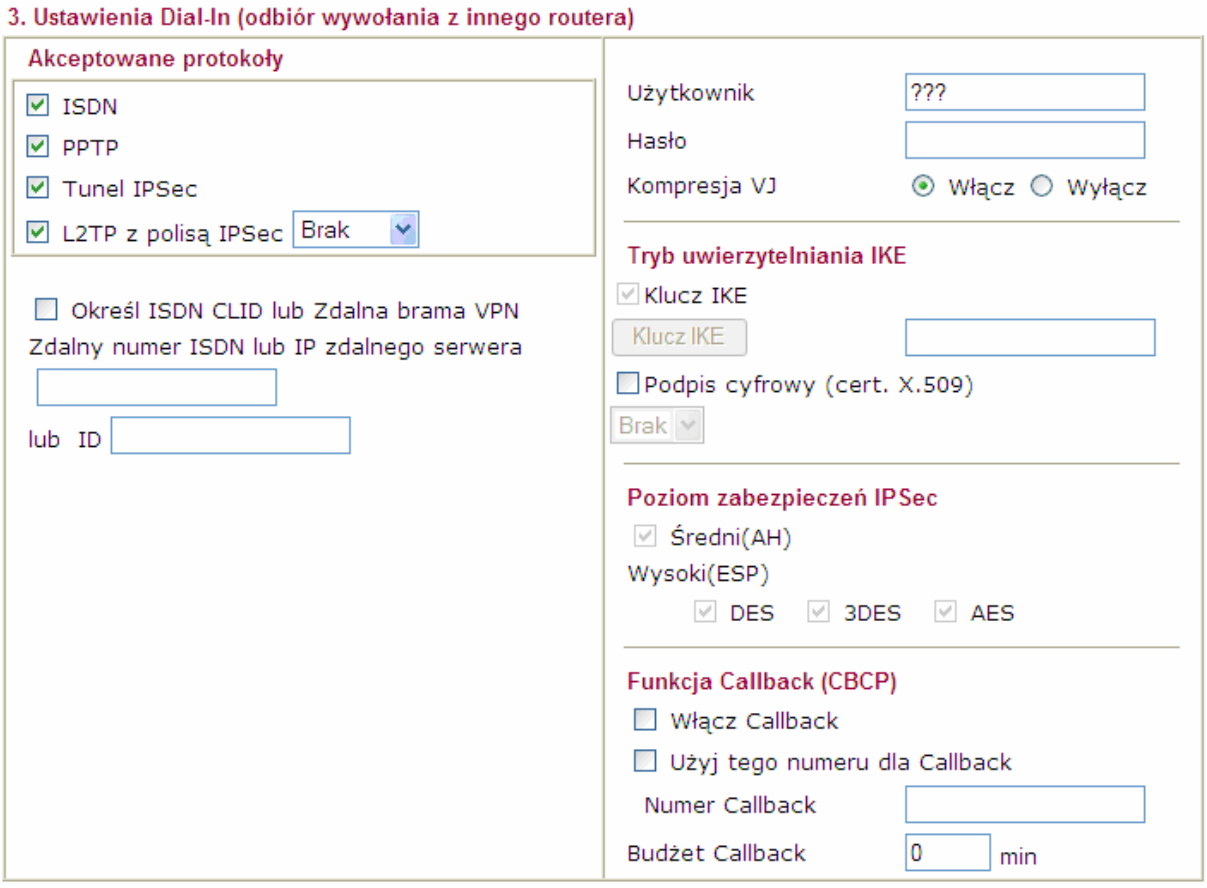
Faza 1 IKE/czas życia klucza / Faza 2 IKE/czas życia klucza - można skrócić lub wydłużyć domyślne uzgodnienia odnośnie okresu czasu, w którym strony decydują się korzystać z tego samego klucza IKE dla danej fazy. Klucz podaje się w sekundach. Jak widać, domyślnie co godzinę (3600 sekund) będą negocjowane nowe klucze szyfrujące dla algorytmów ASP/ESP tworzących tunel (oczywiście odbywa się to automatycznie i nie wymaga rozłączenia aktywnego tunelu).

Opcja PFS – oznacza dodatkową, zaawansowaną opcję IKE, realizowaną przez router Vigor. Polega ona na wymuszeniu takich mechanizmów negocjowania kluczy, aby niemożliwe było złamanie algorytmów szyfrujących nawet po nagromadzeniu dużej ilości zaszyfrowanych danych i ich długookresowej analizie. Gdyby doszło tą drogą do poznania klucza (co teoretycznie wymaga zaangażowania ogromnych środków technicznych, przez co absolutnie nie grozi np. zwykłej firmie czy użytkownikowi), nie będzie możliwe odczytanie pełnej informacji, a tylko niektórych fragmentów. Dodatkowo istnieje gwarancja, że uzyskany klucz będzie już bezużyteczny dla aktualnie przechwytywanych pakietów.

Lokalny ID – parametr ustalany przez każdą ze stron (ciąg do 47 znaków), wykorzystywany w trybie agresywnym zamiast adresu IP do autentykacji z serwerem VPN.

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

Kolejny obszar menu jest związany z reagowaniem przez serwer VPN na żądania zestawienia połączenia pochodzące od zdalnych klientów:



Akceptowane protokoły – określa się tutaj protokoły (jeden lub kilka), których powinien użyć klient podczas próby zestawienia tunelu z serwerem (routerem Vigor). Dla L2TP z polisą IPSec (L2TP over IPSec) można użyć mechanizmów IPSec jako opcji, lub wymusić ich stosowanie przez drugą stronę.

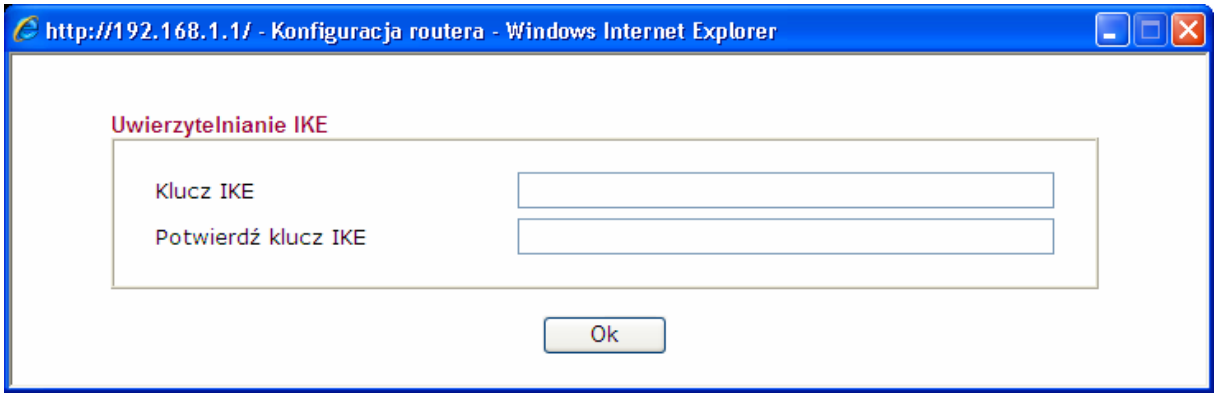
Określ ISDN CLID lub Zdalna brama VPN – parametr precyzujący adres odległego w węzła o zaznaczeniu pola, dostęp będzie możliwy wyłącznie spod podanego natomiast dla połączeń VPN wykorzystujących PPP (PPTP/L2TP) można użyć mechanizmów IPSec jako opcji, lub wymusić ich stosowanie przez drugą stronę.

Zdalny numer ISDN lub IP zdalnego serwera – parametr precyzujący adres odległego w węzła (serwera/klienta VPN), który jest uprawniony do inicjowania połączenia (należy podać adres IP lub numer ISDN). Jeżeli zdalny węzeł nie posiada stałego adresu (np. dysponuje dostępem typu Neostrada), nie należy zaznaczać tej opcji, nie jest bowiem możliwe podanie nazwy DNS jako argumentu w polu poniżej.
Po zaznaczeniu pola, dostęp będzie możliwy wyłącznie spod podanego adresu/numeru, co stanowi dodatkową ochronę (sprawdzenie tożsamości). W przypadku klienta stosującego IPSec jest to wymóg bezwzględny, tylko bowiem na tej podstawie możliwe będzie przydzielenie indywidualnych ustawień IKE/IPSec, tzn. skonfigurowanie profilu użytkownika. Dla klientów IPSec posiadających nieokreślony (zmienny) adres/numer obowiązują wspólne Ustawienia ogólne IKE/IPSec (patrz wcześniej).

ID – pole pozwala wprowadzić dodatkowy ciąg znaków, określający konkretny tunel VPN.

Dla połączeń VPN wykorzystujących PPP (PPTP/L2TP) można używać oddzielnych, indywidualnych profili użytkownika, nawet jeżeli druga strona (klient) nie dysponuje stałym adresem IP. Parametry **Użytkownik/Hasło** oraz **Kompresja VJ** dotyczą właśnie połączeń wykorzystujących protokół PPP (a więc wszystkich z wyjątkiem tunelu IPSec), i zostały opisane wcześniej.

Kolejne ustawienia dotyczą tylko połączeń wykorzystujących protokół IPSec:
Klucz IKE – klucz wstępny wymagany do wzajemnego uwierzytelnienia stron, rozpoczynającego pierwszą fazę IKE. Należy go potwierdzić, wpisując dwukrotnie:

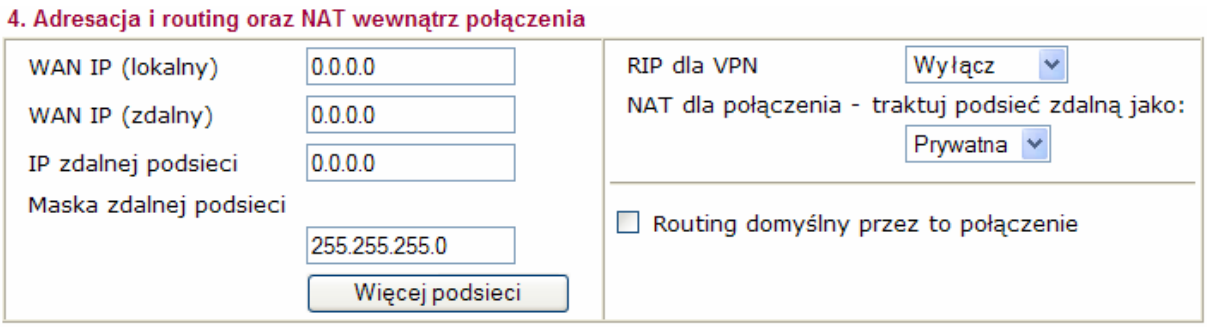


Poziom zabezpieczeń IPSec – dotyczy drugiej fazy IKE:

- **Średnii (AH)** – zaznaczenie tej opcji spowoduje, że akceptowane będą tylko żądania zestawienia tunelu według protokołu AH (druga faza IKE)
- **Wysoki (ESP)** – zaznaczenie którejkolwiek opcji spowoduje wysłanie do strony inicjującej żądania użycia protokołu ESP. Szyfrowanie będzie uzgadniane z uwzględnieniem zaznaczonych algorytmów **DES/3DES/AES**. Jeżeli żaden z nich nie będzie obsługiwany przez stronę zdalną, połączenie nie dojdzie do skutku. Można tego uniknąć zaznaczając przynajmniej DES, gdyż jako obowiązkowy składnik każdej implementacji ESP musi on być obsługiwany przez każde urządzenie.

  Jednoczesne użycie AH i ESP oznacza, że pakiet zabezpieczony zgodnie z ESP będzie dodatkowo w całości autoryzowany protokołem AH.

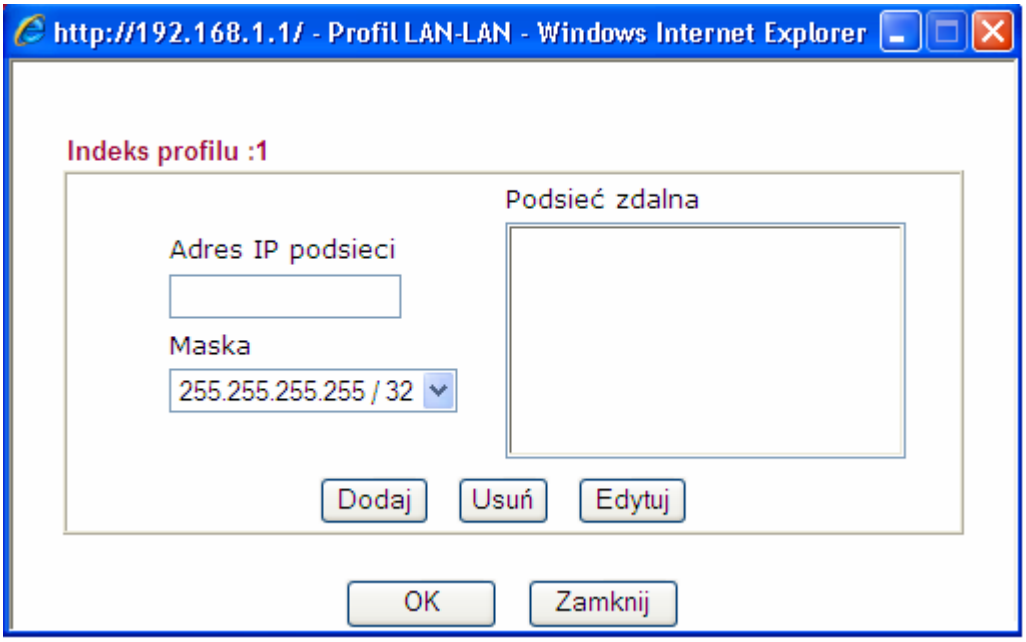
4. Adresacja i routing oraz NAT wewnątrz połączenia
Ostatni obszar ustawień dotyczy zagadnienia negocjowania adresów IP dla potrzeb komunikacji wewnątrz tunelu VPN, jak i samej realizacji tej komunikacji:



Poniższe parametry zostaną wykorzystane przez router do zdefiniowania osobnej pozycji w tablicy routingu, informującej o zdalnej podsieci i możliwości dotarcia do niej poprzez tunel (wirtualny interfejs) VPN:

- **WAN IP (lokalny)** – publiczny adres IP routera możliwy do zastosowania tylko w przypadku użycia protokołu ISDN, PPTP lub L2TP (z lub bez polisy IPSec). Domyślna wartość 0.0.0.0 oznacza, że router pobierze właściwy adres w fazie negocjacji IPCP.
- **WAN IP (zdalny)** – adres IP urządzenia w zdalnej podsieci, które ma pełnić funkcję bramy w dalszym procesie routingu (tzn. decydować o skierowaniu pakietu do właściwego urządzenia lub innej podsieci) możliwy do zastosowania tylko w przypadku użycia protokołu ISDN, PPTP lub L2TP (z lub bez polisy IPSec). Domyślna wartość 0.0.0.0 oznacza, że router pobierze właściwy adres w fazie negocjacji IPCP.
- **IP zdalnej podsieci** – adres odległej podsieci
- **Maska zdalnej podsieci** - określa maskę, obowiązującą dla odległej podsieci

Więcej podsieci – oprócz podstawowej trasy, którą definiuje się za pomocą opisanych powyżej pozycji, można stworzyć dodatkowe statyczne definicje tras:



Podczas kiedy trasa podstawowa będzie pozwalała osiągnąć podsieć pracującą bezpośrednio na drugim końcu tunelu (dołączoną do zdanego routera-bramy), trasy dodatkowe mogą prowadzić do dalszych podsieci funkcjonujących np. w ramach złożonej struktury oddziału przedsiębiorstwa. Warto podkreślić, że router Vigor na podstawie takiej definicji wyśle pakiety zaadresowane do zdalnej podsieci na adres wskazanej bramy. Jeżeli jednak wskazany zdalny router nie posiada prawidłowej informacji na temat dodatkowych podsieci, lub nie potrafi skierować odpowiedzi do routera Vigor (z powrotem przez tunel), komunikacja z takimi podsieciami nie będzie możliwa.

Wewnątrz tunelu możliwy jest też routing dynamiczny z wykorzystaniem protokołu RIP w wersji 1 lub 2 (do wyboru). Jeżeli druga strona (zdalny serwer) również korzysta z RIP, a więc potrafi dostarczyć informacji o strukturze odległej sieci, nie jest konieczne tworzenie definicji tras statycznych (m. in. wszystkie pola po lewej stronie można pozostawić puste).

RIP dla VPN – określa, czy router Vigor ma ograniczyć routing dynamiczny do wysyłania komunikatów RIP do sieci po drugiej stronie tunelu, odbierania i uwzględniania w tablicy routingu komunikatów otrzymanych z odległej sieci, czy też realizować obie operacje, a więc pełen routing RIP. Można też wyłączyć wysyłanie rozgłoszeń RIP poprzez tunel. Jest to na przykład konieczne jeżeli tunel ma pracować w trybie „na żądanie" (np. poprzez ISDN). Inaczej bowiem każde uaktualnienie RIP spowoduje niepotrzebne nawiązanie połączenia.

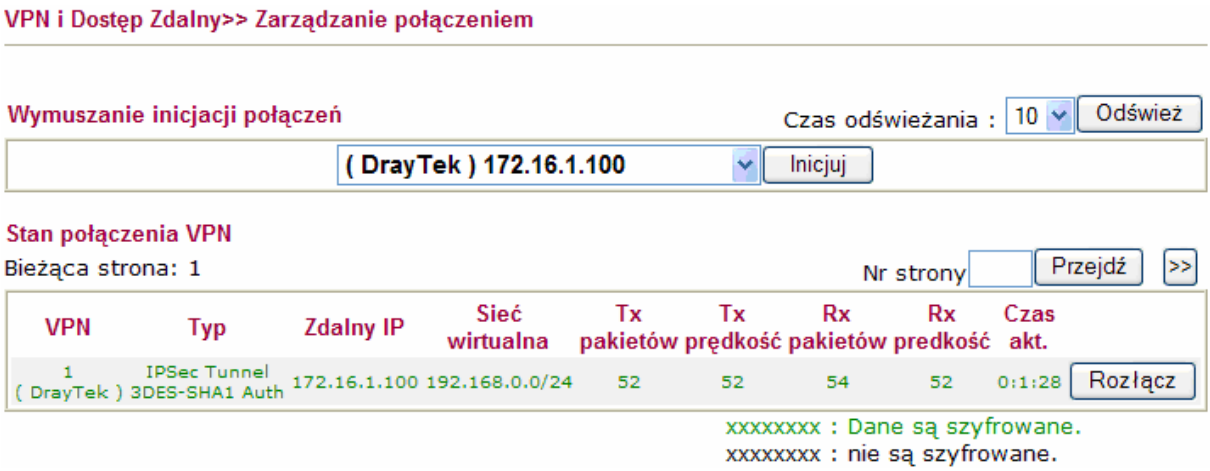
NAT dla połączenia – traktuj podsieć zdalną jako - możliwe jest zestawienie tunelu pomiędzy podsieciami prywatnymi, publicznymi, oraz publiczną i prywatną. Ostatnia opcja wymaga zastosowania NAT wewnątrz tunelu.

- **Prywatna** – router zakłada, że na drugim końcu tunelu znajduje się podsieć z adresami prywatnymi
- **Publiczna** – router przyjmuje że łączy się z siecią stosującą adresy publiczne (w razie potrzeby zastosuje NAT)

Routing domyślny przez to połączenie – jeżeli pole zostanie zaznaczone, trasa domyślna routera zostanie skierowana na wirtualny interfejs tunelu VPN (IF4-IF11). Oznacza to, że cały ruch wychodzący z sieci LAN będzie kierowany poprzez ten tunel, chyba że dla danej sieci docelowej router dysponuje innym wpisem w tabeli routingu.

Zarządzanie połączeniami VPN

Komunikacja z wykorzystaniem VPN posiada cechy logicznego połączenia, obejmującego fazę nawiązania bezpiecznej sesji komunikacyjnej wraz z odpowiednią negocjacją parametrów, jak i fazę rozłączenia. Organizacja połączenia odbywa się według typowej architektury klient-serwer, co oznacza, że w procesie tym obie strony pełnią nieco odmienna rolę. Dopiero po ustanowieniu komunikacji pomiędzy klientem i serwerem VPN powstaje swoisty podkład komunikacyjny dla właściwego ruchu, np. wymiany pakietów pomiędzy prywatnymi sieciami IP.
Aby przeprowadzić diagnostykę skonfigurowanego połączenia VPN czy też przetestować współpracę z rozwiązaniami innych producentów, można się posłużyć specjalnym narzędziem zaimplementowanym przez producenta. Pozwala ono wymusić nawiązanie połączenia VPN, skłonić router do jego rozłączenia, a podczas trwania sesji dostarcza podstawowych informacji na jej temat (więcej szczegółów prezentuje monitor SysLog):



Wymuszanie inicjacji połączeń – w oknie można dokonać wyboru dowolnego spośród wszystkich skonfigurowanych w routerze wychodzących połączeń wirtualnych. Połączenie jest opisane nazwą profilu (patrz konfiguracja LAN-to-LAN) oraz docelowym adresem IP/nazwą serwera VPN. Kliknięcie Inicjuj sprawi, że router, zgodnie z posiadaną konfiguracją, będzie próbował skontaktować się z serwerem w celu zorganizowania połączenia.

Stan połączenia VPN – jest to lista wszystkich trwających aktualnie połączeń VPN (także tych przychodzących, w których Vigor pełni rolę serwera). Zawiera ona dane właściwe dla każdego z nich:

VPN – numer połączenia i nazwa profilu

Typ – rodzaj połączenia VPN – informuje o użytych protokołach, opcjach autoryzacji i szyfrowania itp. (patrz rozdział poświęcony konfiguracji VPN).

Zdalny IP – adres IP serwera VPN, pracującego na drugim końcu połączenia. Jeżeli połączenie wirtualne jest zestawiane w sieci publicznej (Internet), adres ten musi być adresem publicznym (globalnie routowalnym).

Sieć wirtualna – adres IP docelowej prywatnej podsieci, korzystającej z połączenia VPN. Pakiety z wnętrza sieci prywatnej mogą być przesyłane poprzez tunel VPN z zachowaniem oryginalnych adresów, jako że są przenoszone przez właściwy, publiczny strumień pakietów (dodatkowa enkapsulacja).

Tx pakietów / Tx prędkość – liczba pakietów IP wysłanych podczas aktualnego połączenia VPN i średnia prędkość wysyłania (w oktetach/s)

Rx pakietów / Rx prędkość - liczba pakietów odebranych podczas aktualnego połączenia wirtualnego i średnia prędkość napływu (w oktetach/s)

Czas akt. – czas jaki upłynął od momentu rozpoczęcia połączenia VPN

Szczegóły dotyczące połączeń VPN są rejestrowane przez oprogramowanie DrayTek SysLog, które jednak nie potrafi wymusić operacji nawiązania bądź zerwania połączenia, stąd dla celów diagnostycznych najlepiej połączyć oba rozwiązania.