Konfiguracja tuneli VPN na urządzeniach LINKSYS

Poznań 2007

Wstęp

Niniejszy poradnik obejmuje zakresem podstawowe zagadnienia związane z tunelami VPN. Przedstawiono, jak skonfigurować bezpieczne połączenie pomiędzy oddziałami firmy, lub uzyskać zdalny dostęp do firmowej sieci wykorzystując do tego urządzenia marki Linksys. Pomimo, iż konfiguracja była przeprowadzana na 2 modelach urządzeń: RV082 oraz WRV200, przedstawione wskazówki mogą zostać również zastosowane do pozostałych modeli urządzeń firmy Linksys.

VPN czyli Virtual Private Connection pozwala na stworzenie logicznego tunelu pomiędzy dwoma lokalizacjami przy wykorzystaniu istniejącej infrastruktury sieciowej. Z punktu widzenia tunelu VPN nie jest istotne przez jakie sieci przechodzi pakiet, najważniejsze, aby urządzenia na obu końcach tunelu były właściwie skonfigurowane do jego obsługi. Dane przesyłane tunelem VPN są pakowane w specjalnie szyfrowane pakiety ESP, w celu odtworzenia pakietu odbiorca musi znać klucz i algorytm którym informacje zostały zaszyfrowane. Do szyfrowania danych wykorzystuje się silne algorytmy takie jak DES/3DES/AES. Niektóre z algorytmów mogą obniżyć przepustowość łączy(sytuacja systematycznie się poprawia i w najnowszych wersjach oprogramowania tunele tworzone przy wykorzystaniu RV082 i algorytmów szyfrujących 3DES uzyskują prędkości rzędu 90 Mb/s). Dzięki szyfrowaniu możemy być pewni, że nasze dane nie zostaną podsłuchane. Tunele VPN znajdują zastosowanie przy łączeniu różnych oddziałów firmy, lub pozwalają na uzyskanie dostępu do firmowej sieci dla pracowników zdalnych(np. z domu lub lokalizacji publicznej). Wyróżniamy dwa główne rodzaje tuneli VPN:

- Gateway – to – Gateway – tunel w tym wypadku zestawiany jest pomiędzy dwoma urządzeniami, które posiadają funkcję tworzenia tuneli VPN tego typu, mogą to być np. dwa routery, zaletą tego trybu jest możliwość określenia, czy cała sieć ma mieć dostęp do tunelu zdalnego, czy tylko pojedyncze hosty występujące w tej sieci,

- Client – to – Gateway – tunel zestawiany jest pomiędzy hostem w zdalnej lokalizacji a urządzeniem sieciowym(routerem bądź serwerem VPN), który daje hostowi dostęp do sieci umieszczonej za nim,

Jako dodatkowy tryb routery firmy Linksys posiadają możliwość zestawiania tuneli client – to – gateway przy użyciu aplikacji dostarczonej przez firmę Linksys, oprogramowanie Quick VPN Client, pozwala w prosty i szybki sposób zestawić tunel VPN pomiędzy routerem a hostem zdalnym.

Gateway – to – Gateway

Client – to – Gateway

1. Zestawianie tuneli Gateway – to – Gateway:

W celu zestawienia tego typu tuneli, musimy upewnić się, że sieci lokalne, pomiędzy którymi zostanie zestawiony tunel VPN będą miały różną adresację. Jeżeli nie zastosujemy się do powyższej rady, pomimo, że będziemy w stanie zestawić tunel VPN pomiędzy dwoma urządzeniami, pakiety mogą być kierowane błędnie, co uniemożliwi komunikację pomiędzy sieciami.

Przykładowe ustawienia schematu adresacji dla sieci po obu stronach kanału VPN:

Przyjęto, że routery dysponują po stronie interfejsu WAN statycznymi adresami IP.

Komputery w sieciach lokalnych pobierają adresy IP dynamicznie z routerów.

Ustawienia routera 1:

Adres IP routera po stronie WAN: 192.168.10.11

Adres IP routera po stronie LAN: 192.168.1.1

Maska podsieci: 255.255.255.0

Serwer DHCP: 192.168.1.100 -254

Ustawienia routera 2:

Adres IP routera po stronie WAN: 192.168.10.10

Adres IP routera po stronie LAN: 192.168.2.1

Maska podsieci: 255.255.255.0

Serwer DHCP: 192.168.2.100 -254

1.1 Konfiguracja ustawień sieciowych

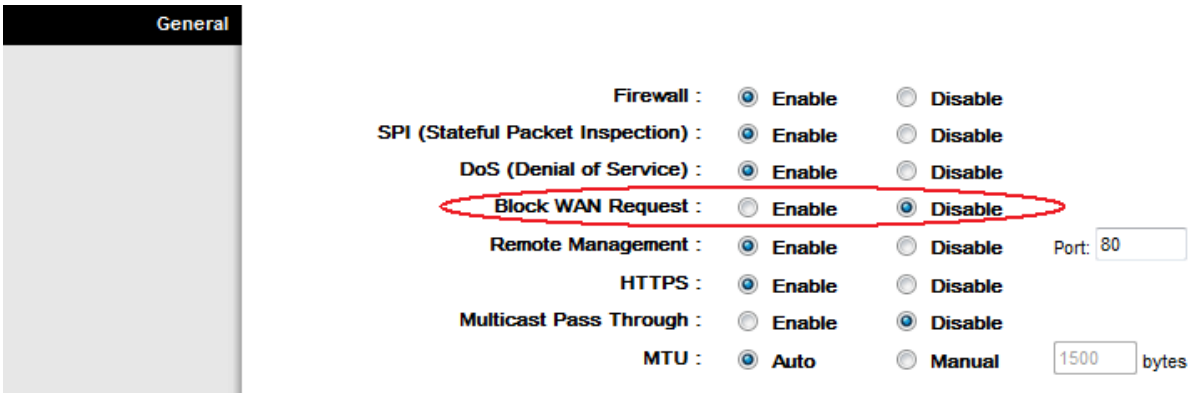
Wprowadzanie ustawień dotyczących zarówno schematów adresacji jak i tuneli VPN odbywa się przy wykorzystaniu interfejsu zarządzania www, wbudowanego w urządzenie. Domyślnie interfejs www jest dostępny pod adresem http://192.168.1.1 . Do konfiguracji urządzeń Linksys polecamy przeglądarkę IE Explorer w wersji 6.0 lub wyżej.

Więcej szczegółów o konfiguracji ustawień interfejsu WAN oraz konfiguracji sieci lokalnej w przewodniku użytkownika dedykowanym do tego urządzenia dostępnym na stronie http://www.linksys.com .

Po ustaleniu schematów adresacji, właściwego dla każdego z routerów należy właściwie skonfigurować zaporę wbudowaną w urządzenie. Zmiany należy wprowadzić w zakładce Firewall w następujących opcjach:

Block Anonymus Internet Request -> odznaczyć haczyk w polu obok parametru(WRV200)

Block Anonymus Internet Request -> zmienić wartość w polu na Disable(RV042/RV082)

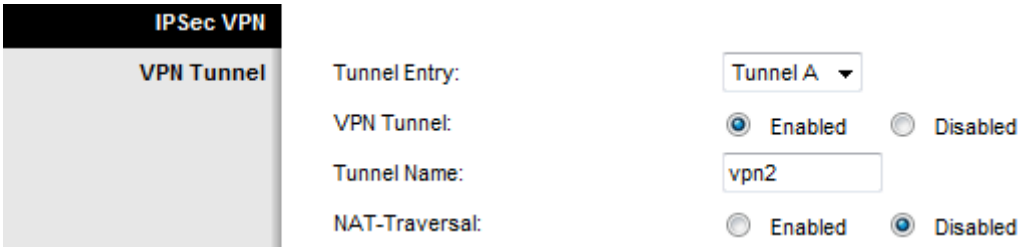


Dodatkowo w niektórych wersjach oprogramowania routerów RV042/RV082, w których występuje parametr Fragmented Packets Pass Through należy zmienić wartość tej opcji na Enabled.

W dalszej części przedstawiono zrzuty ekranowe z konfiguracji tuneli na WRV200, jednak występujące ustawienia są uniwersalne i mogą być z powodzeniem zastosowane do innych modeli urządzeń marki Linksys.

Po ustaleniu schematów adresacji właściwego dla każdego z routerów należy przejść do zakładki: VPN > IP Sec VPN(dla urządzenia WRV200, w urządzeniach RV przechodzimy do zakładki VPN, a następnie wybieramy interesujący nas typ tunelu).

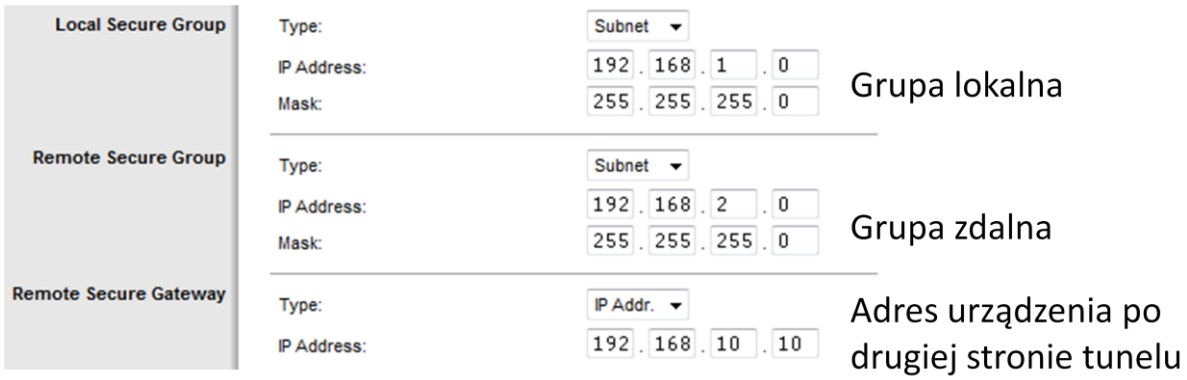
Należy wybrać tunel który ma zostać wykorzystany(ilość tuneli IPSec jest uzależniona od modelu urządzenia: RVL200/WRV200 – 5, RV042 – 50, RV082 – 100). Po wybraniu nr tunelu należy zaznaczyć opcję Enabled oraz wpisać jego nazwę. Nazwa tunelu może być różna po obu jego stronach.



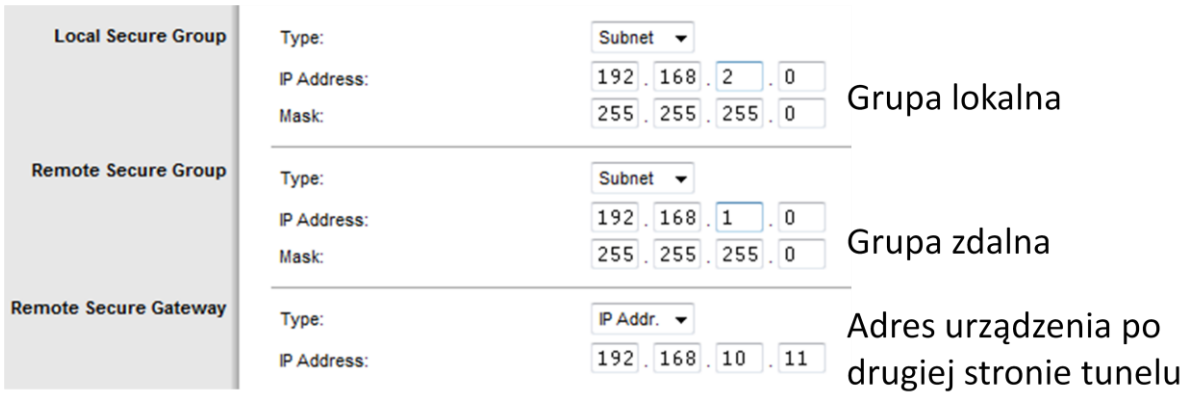
Następnym krokiem w tworzeniu tuneli VPN jest wybór które z hostów będą miały dostęp do tunelu i konfiguracja ustawień sieciowych. Rysunek przedstawiony na następnej stronie pokazuje część pozwalającą na wybór które z hostów mają mieć dostęp do tunelu VPN oraz konfigurację ustawień sieciowych tunelu. W naszym wypadku przyjęliśmy, że wszystkie hosty z obu sieci mają mieć dostęp do tunelu VPN.

W tym celu przypisano na urządzeniach następujące ustawienia:

Router 1:



Router 2:



Poszczególne parametry zostały wypełnione zgodnie ze schematem adresacji przedstawionym na początku rozdziału. Oczywiście nie jest to jedyna możliwa konfiguracja, użytkownik może zdecydować, czy dostęp do tunelu ma mieć pojedynczy komputer, część podsieci lub cała podsieć. Za decyzję które z hostów mają mieć dostęp do tunelu odpowiada parametr Type. Do wyboru użytkownik ma adres IP(czyli tunel zakończony będzie na urządzeniu zdalnym, wszystkie urządzenia podłączone do niego będą miały dostęp do tunelu), podsieć(Subnet – cała podsieć lub część podsieci będzie miała dostęp do tunelu), pojedynczy host(tunel będzie zakończony na routerze, a przekazanie ruchu odbywać się będzie poprzez przekierowanie portów routera na określony komputer w sieci).

1.2 Konfiguracja ustawień bezpieczeństwa

Po wpisaniu ustawień sieciowych właściwych dla zestawianego tunelu VPN, kolejnym krokiem jest konfiguracja ustawień bezpieczeństwa. Ustawienia bezpieczeństwa muszą zostać skonfigurowane jednakowo na urządzeniach po obu stronach tunelu, wprowadzenie różnych ustawień na którymkolwiek z urządzeń uniemożliwi zestawienie tunelu VPN.

Pierwszym elementem w konfiguracji bezpieczeństwa jest wybór sposobu wymiany klucza szyfrującego. Użytkownik ma do wyboru dwa tryby Auto (w RV082 odpowiada temu tryb – IKE with Pre Shared Key) lub Manual. Preferowanym trybem wymiany klucza szyfrującego jest tryb automatyczny.

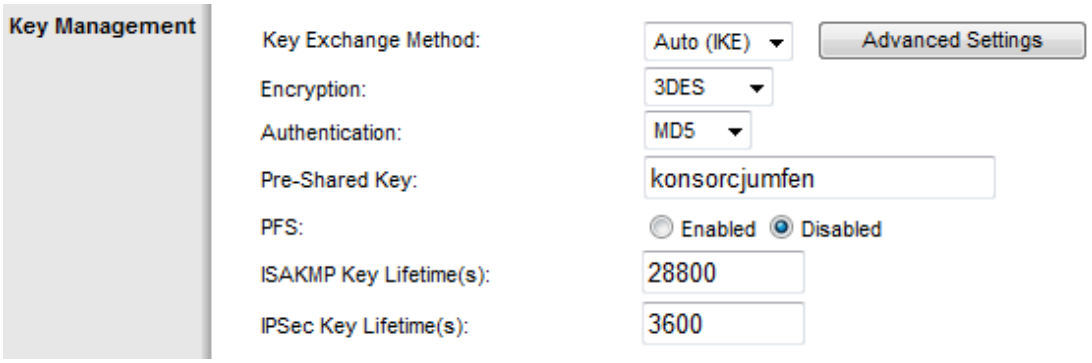
Kolejnym etapem jest wybór algorytmu szyfrującego, do wyboru użytkownik ma kilka algorytmów szyfrowania. Dostępne tryby szyfrowania to: DES, 3DES, AES (128, 192,156 bitów). Ze względu na siłę algorytmu zalecanym jest algorytm 3DES.

Następny krok w konfiguracji ustawień bezpieczeństwa to wybór sposobu uwierzytelniania pakietów ESP, routery oferują do wyboru dwie metody uwierzytelniania:

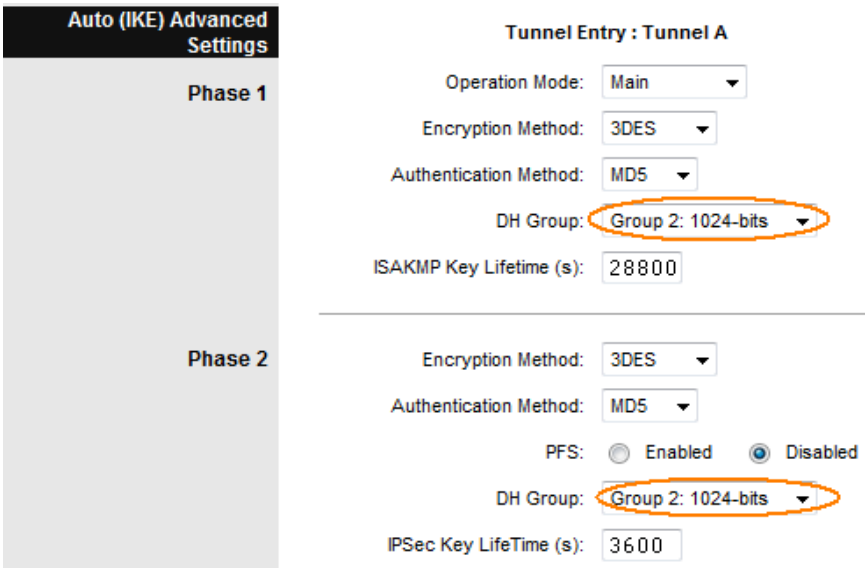
- MD5 - jednostronny algorytm szyfrujący, generujący 128 wzorzec
- SHA1 – jednostronny algorytm szyfrujący, generujący wzorzec 160 bitowy

Ponieważ SHA1 jest algorytmem silniejszym, jest zalecany, przy tworzeniu tuneli VPN.

Ostatnim krokiem przy podstawowej konfiguracji tuneli VPN jest przypisanie klucza używanego w procesie zestawiania tunelu VPN. Klucz szyfrujący wpisujemy w polu Pre-Shared-Key. Klucz to ciąg znaków alfanumerycznych o długości do 30 znaków. W celu zapewnienia maksymalnego bezpieczeństwa tuneli VPN poleca się regularne zmiany klucza szyfrującego.



UWAGA! W przypadku konfiguracji tuneli pomiędzy dwoma różnymi modelami urządzeń, należy zwrócić uwagę, aby ustawienia grupy DH(Diffie-Hellman) były jednakowe na obu urządzeniach. Ponieważ proces zestawiania tunelu VPN składa się z dwóch faz, w przypadku problemów z tunelem VPN należy sprawdzić czy ustawienia dla obu grup są wprowadzone jednakowo. Ustawienia grupy DH dostępne są w zakładce Advanced Settings. Poniżej przedstawiono przykładowe ustawienia dla grupy DH – 1024 bity. W zależności od wybranej grupy, klucz szyfrujący będzie dłuższy(im wyższa grupa tym dłuższy klucz) lub krótszy. Długość klucza szyfrującego ma znaczenie przy ocenie wydajności tunelu, krótszy klucz pozwala uzyskać lepsze wartości transferu, jednak dłuższy klucz zapewnia większe bezpieczeństwo.



Wszystkie wprowadzone zmiany należy zatwierdzić klikając Save Settings.

W zakładce VPN Summary mamy możliwość śledzenia stanu tunelu. Status tunelu może być określony nastepująco:

- C - tunel jest zestawiony poprawnie
- T - urządzenie próbuje zestawić tunel, w przypadku występowania w polu status literki T, należy spróbować odświeżyć stronę przyciskiem Refresh znajdującym się na w dolnej części zakładki VPN Summary, jeżeli przez dłuższy czas występuje literka T, należy kliknąć View VPN Log, logi związane z tunelami VPN pozwalają łatwiej zlokalizować błędy konfiguracyjne
- Stop – tunel został zatrzymany
- D – tunel został administracyjnie wyłączony Disabled
- Any – tunel oczekuje zainicjowanie przez zdalnego hosta
- NAT-T – tunel ma włączoną opcją NAT-T, umożliwiając wywołanie tunelu przez zdalnego hosta podlegającego translacji adresów.

Poprawne zestawienie tunelu sygnalizowane jest w urządzeniu literą C w statusie odpowiedniego tunelu w zakładce VPN Summary, lub poprzez wyświetlenie informacji logach VPN:

251 [Tue 12:50:01] "TunnelA" #30: STATE_QUICK_R2: IPsec SA established

W zależności od parametrów połączenia w nawiasie za tą wiadomością znajdą się parametry związane z poszczególnym tunelem.

Działanie tunelu możemy sprawdzić poprzez pingowanie bramy domyślnej znajdującej się po stronie LAN. Poniższy rysunek przedstawia odpowiedź na komendę ping wywołaną z komputera znajdującego się w sieci 192.168.1.0, przed i po zestawieniu tunelu VPN.

Odpowiedź hosta zdalnego przed zestawieniem tunelu VPN:

```
C:\>ping 192.168.2.1

Badanie 192.168.2.1 z 32 bajtami danych:

Odpowiedź z 192.168.10.1: Host docelowy jest nieosiągalny.
Odpowiedź z 192.168.10.1: Host docelowy jest nieosiągalny.
Odpowiedź z 192.168.10.1: Host docelowy jest nieosiągalny.
Odpowiedź z 192.168.10.1: Host docelowy jest nieosiągalny.

Statystyka badania ping dla 192.168.2.1:
    Pakiety: Wysłane = 4, Odebrane = 4, Utracone = 0 (0% straty),
```

Odpowiedź hosta zdalnego po zestawieniu tunelu VPN:

```
C:\>ping 192.168.2.1

Badanie 192.168.2.1 z 32 bajtami danych:

Odpowiedź z 192.168.2.1: bajtów=32 czas=1ms TTL=63
Odpowiedź z 192.168.2.1: bajtów=32 czas=1ms TTL=63
Odpowiedź z 192.168.2.1: bajtów=32 czas=1ms TTL=63
Odpowiedź z 192.168.2.1: bajtów=32 czas=1ms TTL=63

Statystyka badania ping dla 192.168.2.1:
    Pakiety: Wysłane = 4, Odebrane = 4, Utracone = 0 (0% straty),
Szacunkowy czas błądzenia pakietów w millisekundach:
    Minimum = 1 ms, Maksimum = 1 ms, Czas średni = 1 ms
```

Koniec rozdziału pierwszego poświeconego konfiguracji tuneli VPN typu Gateway – to – Gateway. Więcej informacji na temat zestawiania tuneli tego typu oraz dokładny opis poszczególnych parametrów dotyczących zakładek VPN w podręczniku obsługi przeznaczonym do konkretnego urządzenia dostępnym na stronie http://www.linksys.com .

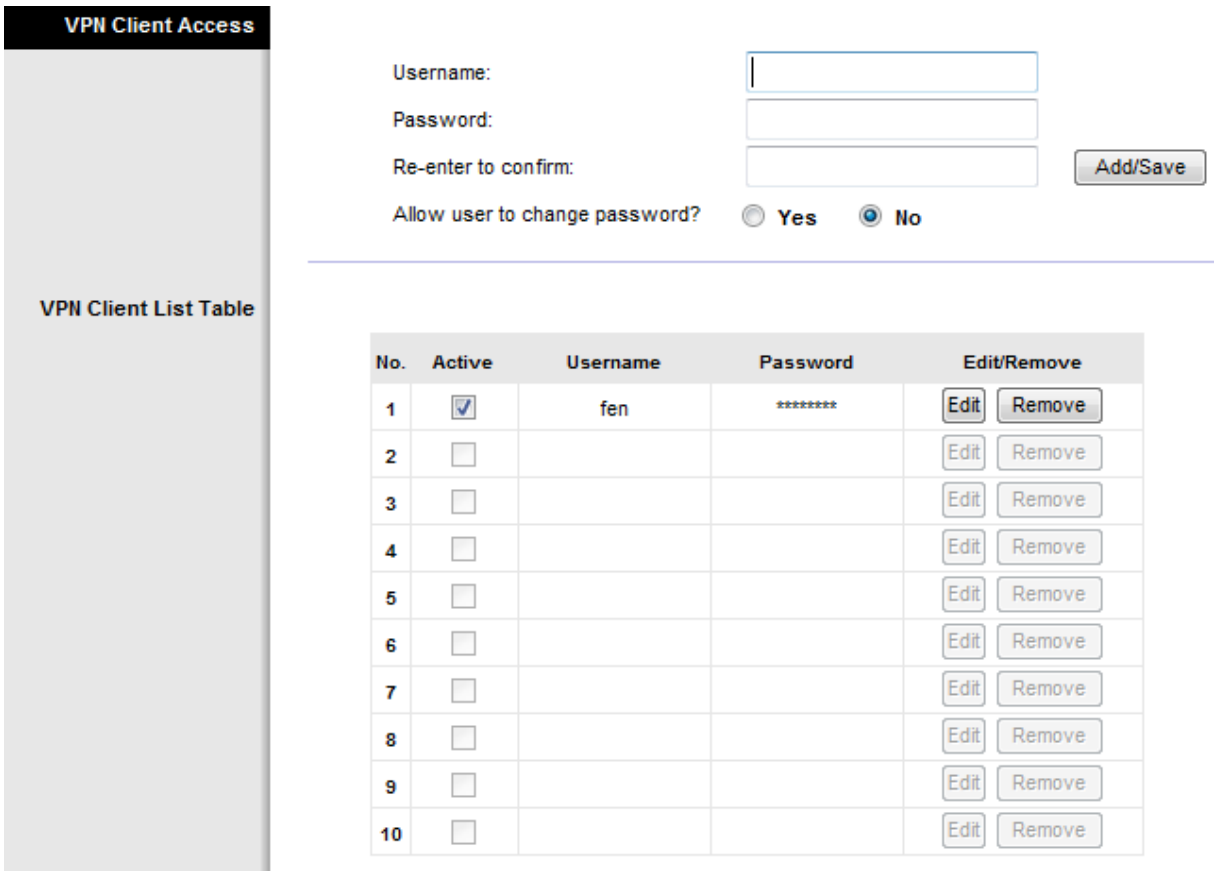
2. Zestawianie tuneli Client – to – Gateway:

Tunele typu Client – to – Gateway mogą być zestawiane przy wykorzystaniu oprogramowania dostarczonego przez firmę Linksys – Quick VPN Client, jak również oprogramowania wbudowanego w systemy operacyjne, lub darmowego oprogramowania klienckiego pobranego z Internetu. Zestawianie tuneli przy użyciu oprogramowania wbudowanego w systemy operacyjne, lub zewnętrznego oprogramowania, jest analogiczne do zestawiania tuneli typu Gateway – to – Gateway i wymaga zgodności informacji podawanych po stronie urządzenia dostępowego jak i klienta VPN. W zależności od urządzenia zestawianie tuneli tego typu może odbywać się poprzez wybranie pojedynczego adresu IP jako strony zdalnej(np. WRV200), lub poprzez konfigurację danych we właściwej zakładce urządzenia VPN > VPN Client – to – Gateway (np. RV082). Zestawianie tuneli tego typu przy wykorzystaniu oprogramowania dostarczanego przez firmę Linksys jest proste i wymaga od użytkownika podania wyłącznie podstawowych informacji, dlatego dalsza część instrukcji została poświęcona zestawianiu tuneli przy wykorzystaniu oprogramowania firmy Linksys. W zależności od modelu, użytkownik może zestawić 10(RVL/WRV200/RV042) lub 15(RV082) tuneli QuickVPN. Dodatkowo firma Linksys oferuje możliwość dokupienia licencji QuickVPN rozszerzającej liczbę klientów na urządzeniach RV042/RV082 do 50 użytkowników.

2.1 Linksys Quick VPN Client

W pierwszej kolejności należy ustalić nazwę użytkownika i hasło na routerze , robimy to w zakładce VPN > VPN Client Access. Po wpisaniu nazwy i hasła klikamy na Add/Save , zaznaczamy, a następnie zapisujemy zmiany > Save Settings.

Poniżej przedstawiono dodawanie kolejnego użytkownika do listy VPN Client List.

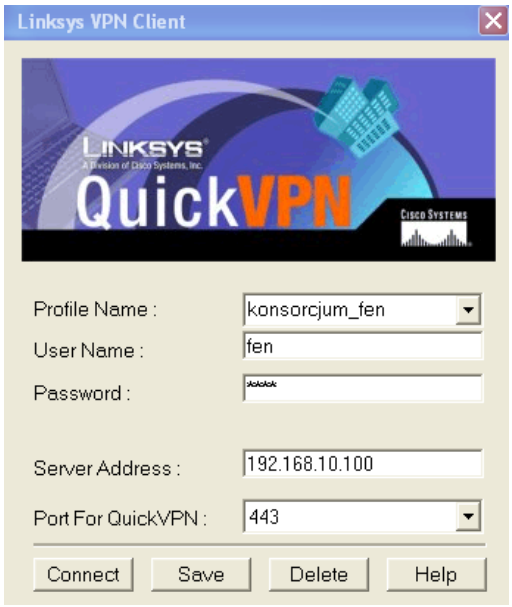


Kolejnym krokiem jest instalacja oprogramowania Linksys Quick VPN Client, na komputerze zdalnym z którego będziemy chcieli uzyskać połączenie z urządzeniem VPN. Oprogramowanie Quick VPN Client powinno znajdować się na płycie dołączonej do urządzenia, jeżeli nie posiadamy płyty lub brakuje na niej tego oprogramowania można je pobrać ze strony www.fen.pl dział download. Oprogramowanie jest zgodne z systemami operacyjnymi Win2K oraz WinXP.

UWAGA! Podobnie jak w przypadku zestawiania tuneli gateway – to – gateway, jeżeli komputer zdalny podłączony jest do sieci wewnętrznej i nie dysponuje publicznym adresem IP, należy zadbać, aby schemat adresacji w sieci do której podłączony jest komputer różnił się od adresacji sieci po drugiej stronie tunelu VPN.

Jeżeli powyższe czynności mamy za sobą należy uruchomić program Quick VPN Client. W pierwszym etapie tworzymy nazwę profilu dla naszego połączenia, np. nazwa firmy, w polach user i password wpisujemy takie same dane jakie ustawiliśmy na routerze. Następnie wpisujemy adres routera - aktywnego interfejsu WAN, lub adresu domenowego, jeśli dysponujemy zmiennym IP.

W poniższej konfiguracji router, z którym realizowane było połączenie dostępny był z zewnątrz pod adresem 192.168.10.100.



Klikamy Connect i połączenie zostaje zestawione. Rysunki przedstawione poniżej pokazują proces zestawiania połączenia.

Zestawianie połączenia

Aktywacja certyfikatu

Weryfikacja sieci

Po uruchomieniu aplikacji QuickVPN Client status połączenia wyświetlany jest w postaci ikony na pasku zadań systemu Windows.

Tunel aktywny

Tunel nieaktywny

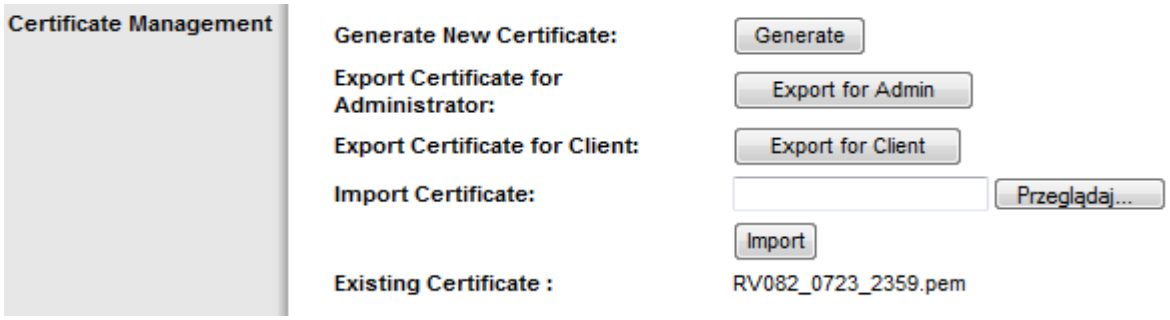
Podobnie jak w wypadku tuneli typu Client – to – Gateway, połączenie możemy przetestować używając do tego celu polecenia ping.

Jeżeli komputer zdalny znajduje się w sieci lokalnej oddzielonej od sieci Internet routerem istotne jest, aby lokalny router miał włączone przepuszczanie tuneli VPN typu IPSec. Urządzenia Linksysa dają możliwość włączenia przepuszczania tuneli VPN i funkcja ta jest domyślnie włączona. Więcej informacji na temat przepuszczania tuneli VPN w rozdziale 3 – Rozwiązywanie problemów.

Konfiguracja dodatkowa:

Bardziej zaawansowane routery dają możliwość wygenerowania nowego certyfikatu bezpieczeństwa, którego będzie używał nasz router i klienci. Opcja ta dostępna jest w urządzeniach RV042/RV082.

Aby wygenerować nowy certyfikat przechodzimy do zakładki VPN > VPN Client Access. W dolnej części zakładki mamy dostępną część poświęconą generowaniu i zapisywaniu nowych certyfikatów bezpieczeństwa.



Aby wygenerować nowy certyfikat bezpieczeństwa klikamy Generate. Dobrą praktyką jest zapisanie certyfikatu na komputerze administracyjnym, dzięki temu po utracie konfiguracji, lub przywróceniu routera do ustawień fabrycznych, będziemy mieli możliwość importu zapisanego wcześniej certyfikatu do routera.

Aby zapisać certyfikat wygenerowany dla routera klikamy na Export for Admin i zapisujemy na lokalnym komputerze.

Kolejnym krokiem jest eksport certyfikatu dla klientów, aby połączenie działało poprawnie należy umieścić certyfikat który eksportowaliśmy dla klientów w katalogu, w którym został zainstalowany Quick VPN Client na komputerze zdalnym. Aby wyeksportować certyfikat dla klientów klikamy Export for Client, zapisujemy plik na komputerze lokalnym, a następnie przenosimy go na komputer z zainstalowanym oprogramowaniem QuickVPN Client.

W ten sposób router i oprogramowanie klienckie będzie korzystało z unikalnego certyfikatu bezpieczeństwa dedykowanego tylko dla hostów podłączonych do tego routera.

Koniec rozdziału 2 poświęconego konfiguracji tuneli typu Client – to – Gateway. Szczegółowe informacje dotyczące konfiguracji tego typu tuneli np. przy użyciu oprogramowania wbudowanego w WinXP można znaleźć w podręczniku obsługi urządzenia WRV200.

3. Rozwiązywanie problemów:

A. Jeżeli połączenie VPN zostało zestawione prawidłowo, status połączenia w zakładce Summary pokazuje C lub Connected dla właściwego tunelu, a nie możemy wymieniać danych poprzez ten tunel należy sprawdzić, czy sieci po obu stronach tunelu VPN mają różny schemat adresacji(w przypadku zachowania takiego samego schematu adresacji komunikacja może nie przebiegać prawidłowo).

B. W przypadku niemożliwości zestawienia tunelu VPN należy sprawdzić ustawienia firewalli urządzeń dostępowych. W przypadku tuneli Client – to – Gateway, jeżeli zdalny host znajduje się za routerem, lub firewallem, należy włączyć opcję VPN Passthru(dla właściwego protokołu VPN(domyślnie urządzenia firmy Linksys mają włączoną opcję VPN Passthru dla IPSec, PPTP oraz L2TP), w przypadku, gdy urządzenie nie posiada opcji VPN Passthru należy odblokować porty, właściwe dla konkretnego protokołu np. dla PPTP należy otworzyć port TCP – 1723 (umożliwienie zestawienia tunelu VPN) dodatkowo włączyć przepuszczanie ruchu dla protokołu GRE(IP #47) - dane. Alternatywnie, należy sprawdzić możliwość zestawienia tunelu po wyłączeniu firewalla na urządzeniu.

C. Problem z zestawianiem połączenia VPN przy wykorzystaniu oprogramowania klienckiego innego niż Linksys Quick VPN Client, może wynikać z nie właściwych ustawień portów, lub protokołu VPN. Upewnij się, ze oprogramowanie wykorzystuje właściwy protokół. Zestawianie tuneli Client – to – Gateway na routerach Linksys odbywa się domyślnie z wykorzystaniem protokołu IPSec.

D. Problem z zestawieniem tunelu może wynikać, z różnych ustawień uwierzytelniania, lub algorytmów szyfrowania w poszczególnych fazach zestawiania połączenia. W zakładce VPN w ustawieniach zaawansowanych tunelu(Advanced Settings) możemy sprawdzić dokładne ustawienia dedykowane dla konkretnej fazy połączenia. Ważne, aby długość klucza, wartość grupy DH po obu stronach tunelu pokrywały się.

Więcej informacji dotyczących rozwiązywanie problemów z zestawianiem tuneli VPN w podręczniku obsługi dedykowanym do poszczególnych urządzeń.

LINKSYS®
A Division of Cisco Systems, Inc.

Pełna oferta dostępna na:

www.fen.pl