Routery QNO QVF

Konfiguracja funkcji QVM Smart Link VPN

Poznań 2011

1. Cel instrukcji

Niniejsza instrukcja przedstawia przykład konfiguracji tunelu VPN Gateway to Gateway pomiędzy dwoma routerami QNO wyposażonymi w funkcje QVM Smart Link VPN.

2. Założenia

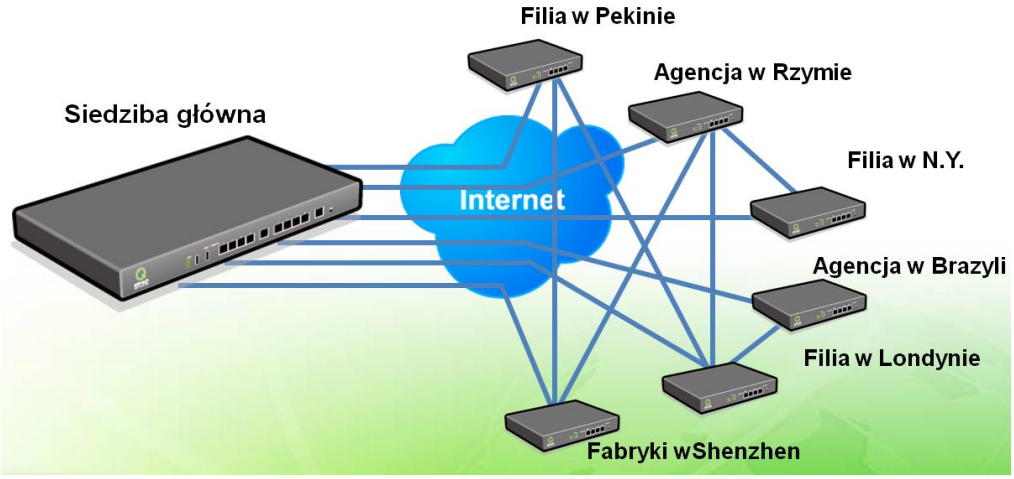
Wybrane modele routerów QNO z serii QVF73xx oraz QVF74xx wyposażone zostały w funkcję ułatwiającą tworzenie tuneli VPN - QVM Smart Link VPN. Funkcja ta ułatwia zestawienie tunelu VPN pomiędzy np. dwoma lokalizacjami(dwoma sieciami LAN), aby w bezpieczny sposób udostępnić zasoby danej lokalizacji dla drugiej strony oraz umożliwić przeglądanie zasobów korzystając z adresów lokalnych charakterystycznych dla obu sieci.

Funkcja QVM Smart Link VPN opiera się na architekturze klient-serwer, czyli ustawieniu jednego routera w trybie serwera terminującego połączenia VPN od wielu innych routerów(określany dalej jako serwer VPN) oraz konfiguracji pozostałych routerów w trybie klientów serwera(określanych dalej jako klient VPN).

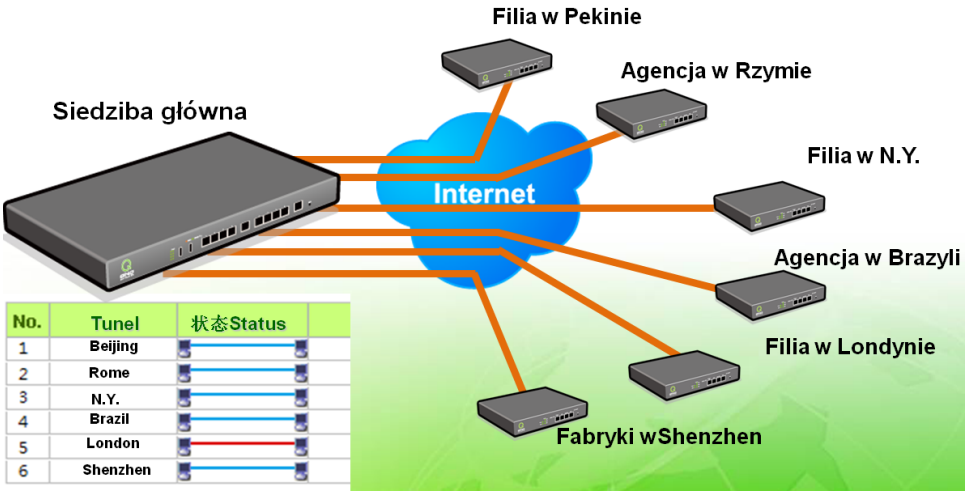
Oprócz typowego zestawiania tuneli Gateway to Gateway, pomiędzy klientem VPN, a serwerem VPN funkcja QVM Smart Link VPN pozwala na określenie na danym routerze kliencie, do 3 alternatywnych adresów IP z którymi tunel VPN ma być zestawiony, dzięki temu w przypadku awarii łącza na serwerze, klient, podejmie próbę zestawienia tunelu po łączach alternatywnych(funkcja wymaga oczywiście aby router w trybie serwera dysponował przynajmniej 2 aktywnymi interfejsami WAN).

Dodatkową zaletą funkcji Smart Link VPN, jest możliwość, ustawienia serwera VPN jako tzw. VPN Huba, tzn. koncentratora tuneli, przeprowadzającego routing ruchu pomiędzy wieloma tunelami zestawionymi do niego ze zdalnych lokalizacji. Dzięki tej funkcjonalności, nie trzeba zestawiać połączeń VPN pomiędzy wieloma lokalizacjami w topologii zupełnej, tj. każdy z każdym, a wystarczy podłączyć zdalne filie pod jeden router w trybie serwera VPN, który zajmie się routowaniem ruchu. Przykład takiej konfiguracji został przedstawiony na poniższym rysunku.

Bez funkcji Smart Link VPN i VPN Hub



Z funkcją Smart Link VPN i VPN Hub.



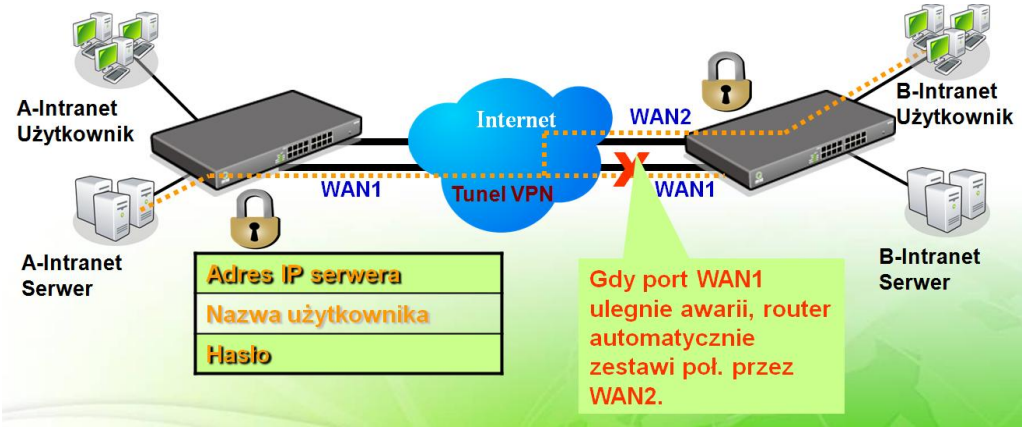
Samo zestawianie tuneli pomiędzy routerami wyposażonymi w funkcję Smart Link VPN jest bardzo proste i nie wymaga tak jak przy tradycyjnym tunelu IPSec podawania wielu parametrów które muszą zgadzać się po obu stronach tunelu aby do połączenia mogło w ogóle dojść. W przypadku funkcji Smart Link VPN wystarczy aby Administrator stworzył konta na serwerze VPN, a na routerach klienta podał:

- adres IP łącza głównego serwera VPN

- przypisaną do klienta nazwę użytkownika

- przypisane do klienta hasło

- opcjonalnie określił alternatywne adresy pod którymi VPN serwer jest dostępny w przypadku awarii łącza głównego



Aby sprawdzić czy dany router posiada funkcję QVM Smart Link VPN:

- Server – w przypadku gdy ma pełnić rolę głównego serwera VPN

- Client – w przypadku gdy ma podłączyć się jako klient do serwera

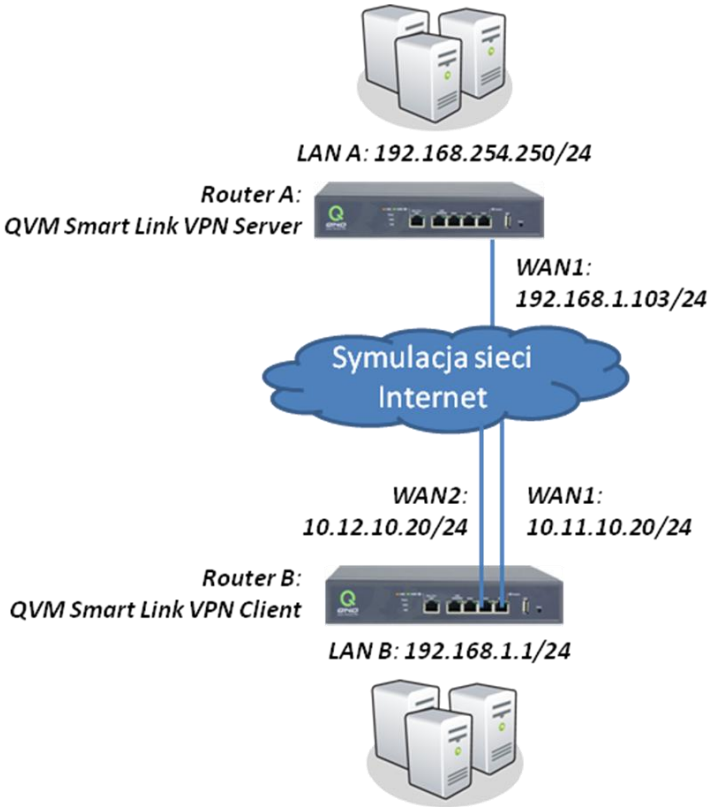
Sprawdź specyfikację wybranego urządzenia:

http://www.qno.com.tw/english/n_products_multiwan_vpn_security_router.asp

3. Przykład konfiguracji

Przykład opiera się na założeniu, że dysponujemy dwoma routerami(w przykładzie 2xQVF7303) i chcemy połączyć dwa Intranety(sieć LAN A oraz sieć LAN B) ze sobą za pomocą funkcji QVM Smart Link VPN Client.

Na poniższym rysunku przedstawiono połączenia pomiędzy routerami wraz ze schematem adresacji.



Jak można zauważyć obie sieci korzystają z różnych adresacji lokalnych, co jest wymagane przy zestawianiu tuneli VPN Gateway to Gateway, niezależnie od technologii(takie ustawienie ma na celu zachowanie poprawności w konfiguracji tablic routingu na routerach po obu stronach tuneli).

Router A, skonfigurowany zostanie jako serwer VPN, natomiast router B jako klient VPN.

Dostępność dwóch interfejsów WAN na routerze kliencie umożliwi w przypadku awarii jednego z łącz, automatyczne zestawienie tunelu VPN po interfejsie alternatywnym, funkcja ta działa automatycznie i nie wymaga dodatkowej konfiguracji.

3.1 Konfiguracja wstępna routera

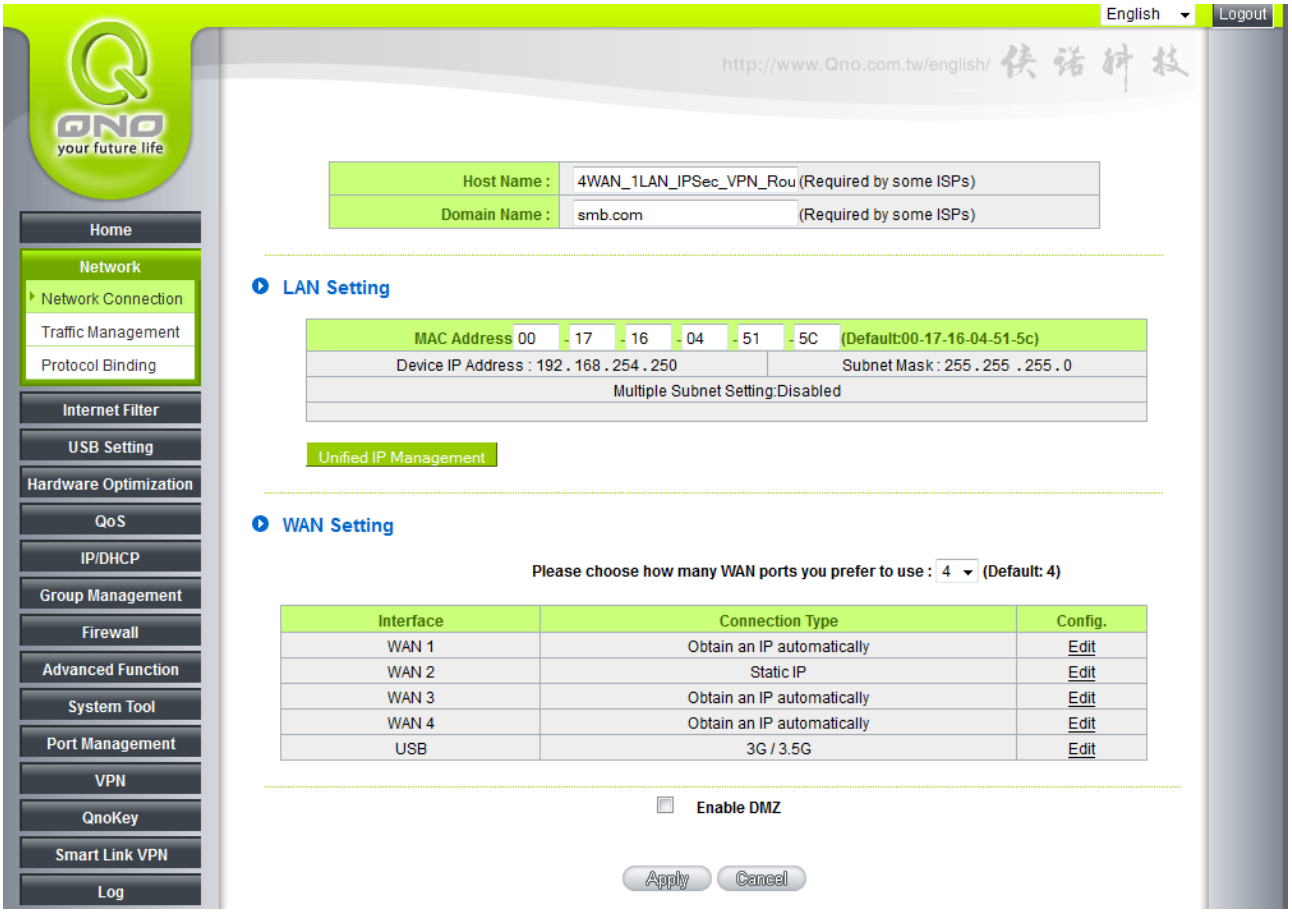
W pierwszym etapie należy skonfigurować parametry podstawowe routerów takie jak zabezpieczenie przed nieautoryzowanymi użytkownikami oraz dostęp do Internetu, czyli adresacja na interfejsach WAN.

Konfigurację tą wykonano w oparciu o podręcznik: QNO_podstawowa_konfiguracja dostępny pod adresem:

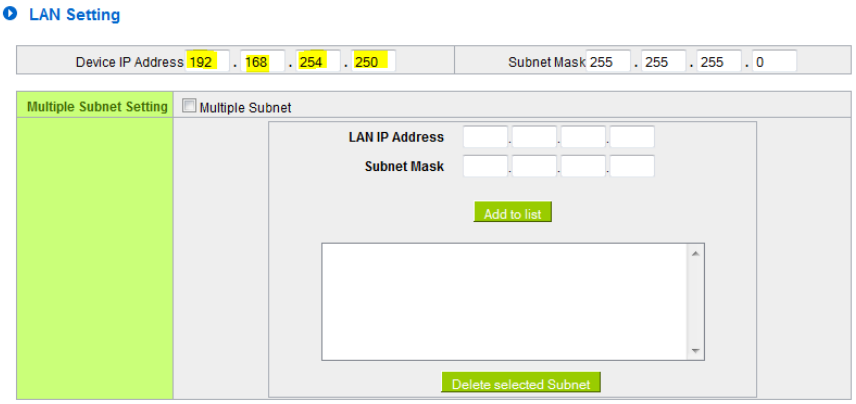
ftp.fen.pl/instrukcje/QNO

Po skonfigurowaniu interfejsu WAN1 na routerze A z adresem 192.168.1.103 oraz interfejsów WAN1 i WAN2 na routerze B z adresami odpowiednio 10.11.10.20 oraz 10.12.10.20 można przejść do konfiguracji adresacji sieci lokalnej na routerze A(jak wspomniano wcześniej adresacja lokalna po obu stronach tunelu musi być różna).

Aby zmienić konfigurację adresacji sieci lokalnej na routerach QNO, należy po zalogowaniu się do urządzenia przejść do zakładki: Network -> Network Connection i wybrać opcję Unified IP Management



Po wybraniu tej opcji pojawi się ekran konfiguracji sieci lokalnej.



Należy zmienić adres lokalny routera na odmienny od tego po drugiej stronie planowanego tunelu, zgodnie z wcześniejszym założeniem w tym wypadku jest to 192.168.254.250/24. Zmianę adresacji w tym wypadku dokonujemy tylko na routerze A, na routerze B, adresacja lokalna może pozostać bez zmian tj. 192.168.1.1/24, ponieważ podsieć ta nie koliduje z podsiecią lokalną na routerze A.

3.2 Konfiguracja funkcji QVM Smart Link VPN

Jak wspomniano na początku, funkcja QVM Smart Link VPN korzysta z architektury klient-serwer, konfiguracja tuneli między lokalizacjami będzie składała się z dwóch etapów:

- konfiguracji routera w trybie serwera

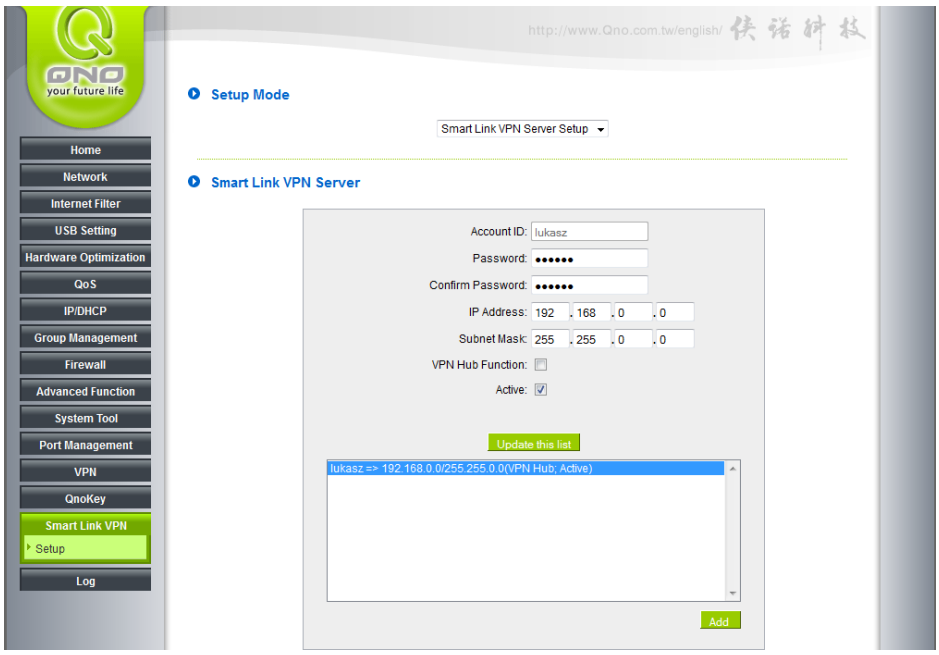
- konfiguracji routera w trybie klienta

Wykorzystywany w przykładzie QVF7303 posiada możliwość pracy zarówno jako serwer jak i klient QVM Smart Link VPN, dzięki czemu po obu stronach wykorzystać można ten sam model.

3.2.1 Konfiguracja routera w trybie serwera VPN

W pierwszym etapie skonfigurowany zostanie router w trybie serwera QVM Smart Link VPN – w naszym przykładzie będzie to router A.

Po zalogowaniu się do routera należy przejść do zakładki: Smart Link VPN -> Setup



Z listy dostępnych trybów należy wybrać opcję Smart Link VPN Server, a następnie wypełnić parametry:

- Account ID – nazwa użytkownika którą będzie logował się do serwera router klient(router B)

- Password – hasło które posłuży do autoryzacji użytkownika

- Confirm Password – powtórzenie hasła

- IP address – zakres adresacji dla której router ma pełnić funkcję serwera VPN

- VPN Hub Function – uaktywnienie funkcji VPN Hub, jeżeli planujemy przez router w trybie serwera łączyć ze sobą więcej niż jedną podsieć VPN

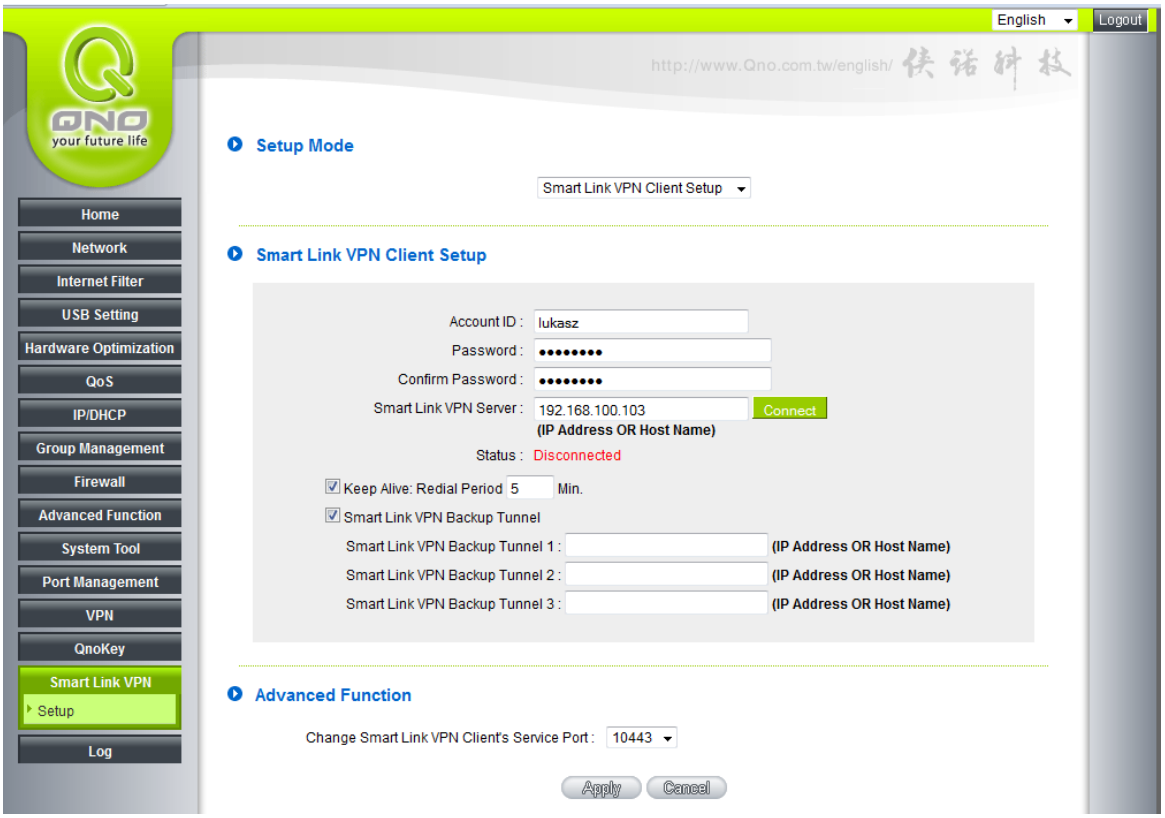
- Active – uaktywnienie tunelu dla danego użytkownika(dzięki tej opcji, Administrator ma możliwość odłączenia zdalnego tunelu i zawieszenia go na określony czas, bez konieczności usuwania konta użytkownika)

Nowe konto należy dodać wybierając opcję Add to List a następnie zatwierdzając konfiguracje przyciskiem Apply.

3.2.2 Konfiguracja routera w trybie klienta VPN

W drugim etapie skonfigurowany zostanie router w trybie klienta QVM Smart Link VPN – w naszym przykładzie będzie to router B.

Po zalogowaniu się do routera należy przejść do zakładki: Smart Link VPN -> Setup



Z listy dostępnych trybów należy wybrać opcję Smart Link VPN Client, a następnie określić:

- Account ID – nazwa użytkownika która została stworzona dla tego routera na serwerze routerze A

- Password – hasło które zostało ustalone na serwerze

- Confirm Password – powtórzenie hasła

- Smart Link VPN Server – adres IP interfejsu WAN routera w trybie serwera w naszym wypadku: 192.168.1.103

- Opcjonalnie parametr Keep Alive – wyrażany w minutach czas co który router ma dokonywać sprawdzenia aktywności tunelu w celu ewentualnego ponownego zestawienia połączenia

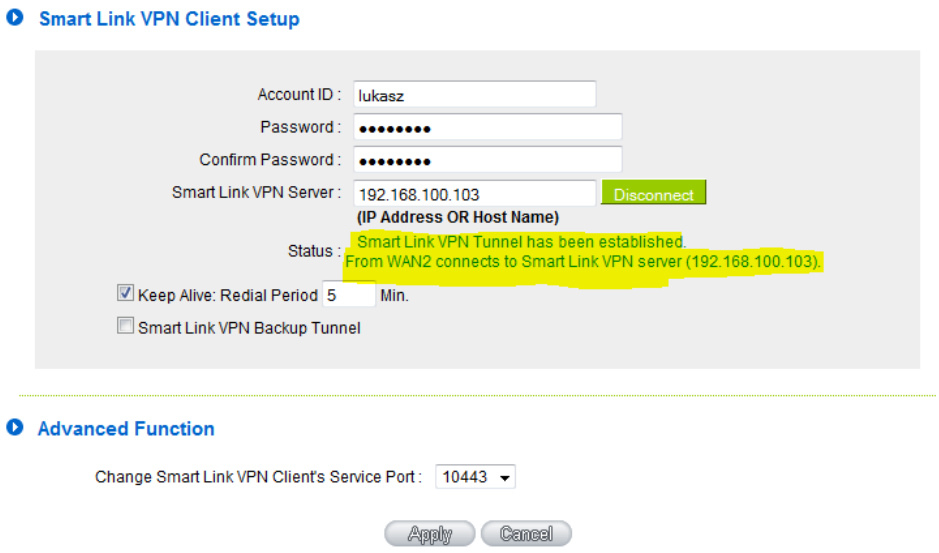
- Opcjonalnie do 3 dodatkowych adresów IP/nazw domenowych, pod którymi może być dostępny serwer VPN w przypadku awarii interfejsu głównego

Po wprowadzeniu danych, należy zapisać ustawienia przyciskiem Apply.

Po wybraniu opcji Connect tunel zostanie zestawiony (pod warunkiem, że po obu stronach tunelu dane zostały wypełnione prawidłowo, a ruch VPN nie jest blokowany przez dostawców internetowych po obu stronach tunelu).

Aby tunele VPN mogły zestawiać się prawidłowo wymagane jest by routery po obu stronach tunelu korzystały z adresów publicznych i po drodze nie była przeprowadzana translacja adresów NAT.

Potwierdzeniem poprawnego zestawienia tunelu będzie komunikat wyświetlony na routerze kliencie B, przedstawiony na poniższym rysunku[Smart Link VPN Server has been established].



Sprawdzenie poprawności działania tunelu można wykonać korzystając z komputera podłączonego do dowolnego z routerów, wiersza poleceń Windows i protokołu ICMP. Aby uruchomić wiersz poleceń wpisz komendę cmd, w pasku zadań systemu.

Następnie wprowadź komendę: ping lokalny_adres_IP_routera_po_drugiej_stronie_tunelu

W przykładzie, komenda została wywołana na komputerze podłączonym do routera B(czyli z lokalną adresacją 192.168.1.1/24) jako parametr podany został lokalny adres IP routera A, po drugiej stronie tunelu: 192.168.254.250

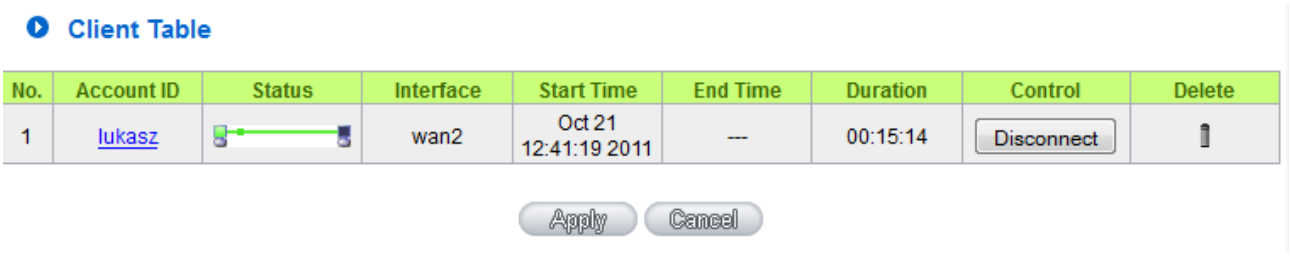
```
C:\Users\Lukasz>ping 192.168.254.250

Badanie 192.168.254.250 z 32 bajtami danych:
Odpowiedź z 192.168.254.250: bajtów=32 czas=2ms TTL=63
Odpowiedź z 192.168.254.250: bajtów=32 czas=2ms TTL=63
Odpowiedź z 192.168.254.250: bajtów=32 czas=2ms TTL=63
Odpowiedź z 192.168.254.250: bajtów=32 czas=4ms TTL=63

Statystyka badania ping dla 192.168.254.250:
    Pakiety: Wysłane = 4, Odebrane = 4, Utracone = 0
             (0% straty),
Szacunkowy czas błądzenia pakietów w millisekundach:
    Minimum = 2 ms, Maksimum = 4 ms, Czas średni = 2 ms
```

O poprawności zestawionego połączenia i możliwości przesyłania danych między lokalizacjami, informuje komunikat o 0% utraty pakietów przy transmisji. Analogiczny test można wykonać z komputerów podłączonych po drugiej stronie tunelu, czyli za serwerem VPN.

Śledzenie statusu tunelu możliwe jest również od strony serwera VPN, po zalogowaniu do serwera VPN przejdź do zakładki: Smart Link VPN -> Setup

U dołu strony dostępna jest statystyka aktualnych połączeń, wraz z czasem zestawienia połączenia, czasem zakończenia ostatniego połączenia oraz czasem trwania aktualnego połączenia.

Administrator ma możliwość odłączenia danego użytkownika(routera w trybie klient) na żądanie przy użyciu przycisku Disconnect.



Gwarancja:

Konsorcjum FEN Sp. z o.o. prowadzi serwis gwarancyjny produktów oferowanych w serwisie dealerskim www.fen.pl.

Procedury dotyczące przyjmowania urządzeń do serwisu są odwrotne do kanału sprzedaży tzn.: w przypadku uszkodzenia urządzenia przez klienta końcowego, musi on dostarczyć produkt do miejsca jego zakupu.

Skrócone zasady reklamacji sprzętu:

Reklamowany sprzęt powinien być dostarczony w stanie kompletnym, w oryginalnym opakowaniu zabezpieczającym lub w opakowaniu zastępczym zapewniającym bezpieczne warunki transportu i przechowywania analogicznie do warunków zapewnianych przez opakowanie fabryczne.

Szczegółowe informacje dotyczące serwisu można znaleźć pod adresem www.fen.pl/serwis

Konsorcjum FEN współpracuje z Europejską Platformą Recyklingu ERP w sprawie zbiórki zużytego sprzętu elektrycznego i elektronicznego. Lista punktów, w których można zostawiać niepotrzebne produkty znajduje się pod adresem www.fen.pl/download/ListaZSEIE.pdf

Informacja o przepisach dotyczących ochrony środowiska

Dyrektywa Europejska 2002/96/EC wymaga, aby sprzęt oznaczony symbolem znajdującym się na produkcie i/lub jego opakowaniu ("przekreślony śmietnik") nie był wyrzucany razem z innymi niesortowanymi odpadami komunalnymi. Symbol ten wskazuje, że produkt nie powinien być usuwany razem ze zwykłymi odpadami z gospodarstw domowych. Na Państwu spoczywa obowiązek wyrzucania tego i innych urządzeń elektrycznych oraz elektronicznych w wyznaczonych punktach odbioru. Pozbywanie się sprzętu we właściwy sposób i jego recykling pomogą zapobiec potencjalnie negatywnym konsekwencjom dla środowiska i zdrowia ludzkiego. W celu uzyskania szczegółowych informacji o usuwaniu starego sprzętu prosimy się zwrócić do lokalnych władz, służb oczyszczania miasta lub sklepu, w którym produkt został nabyty.

konsorcjum

Dział Wsparcia Technicznego

Konsorcjum FEN Sp. z o.o.

Kontakt: help@fen.pl