Ruter VPN – ALL-VPN10

Żyjemy w czasach, w których egzystencja bez Internetu wydaje się niemożliwa. Poprzez Internet organizujemy swoje życie tak prywatne, jak i zawodowe, dokonujemy transakcji bankowych i giełdowych, sterujemy poważnymi systemami automatyki. Liczba urządzeń korzystających z sieci czy to w domach, czy w biurach, rośnie lawinowo. Konieczne staje się sięganie po nowoczesne rutery zapewniające bezpieczny i szybki dostęp do Internetu.

Produkt dostępny na www.conrad.pl

Jednym z najważniejszych parametrów sieci, w której pracują komputery, niezależnie od tego, czy stanowią one własność prywatną, czy firmową, jest bezpieczeństwo. Znane są dość liczne często bardzo spektakularne włamania do sieci korporacyjnych, a nawet rządowych skutkujące wykradzeniem poufnych danych, zainfekowaniem komputerów groźnym oprogramowaniem czy nawet ingerencją w systemy zarządzania lub sterowania. Metod obrony przed takimi przypadkami jest wiele. Jak można przypuszczać, żadna z nich nie daje stuprocentowej gwarancji. Nie oznacza to jednak, że nie należy szukać rozwiązań zapewniających możliwie wysoki poziom bezpieczeństwa.

VPN – Virtual Private Network

Jedną z metod zwiększania bezpieczeństwa korzystania z sieci jest stosowanie prywatnych sieci wirtualnych (VPN). Funkcję tę realizują niektóre typy ruterów, jak na przykład opisywany w artykule ALL-VPN10. VPN przekierowuje połączenie internetowe użytkownika do zdalnego serwera obsługiwanego przez dostawcę usługi VPN. Serwer ten daje użytkownikowi pewną prywatność przy korzystaniu online z Internetu, nie pozwalając na śledzenie go przez dostawcę usług lub reklamodawców. Podczas połączeń z Internetem przez publiczne sieci Wi-Fi chronione są również dane użytkownika. Trzeba też wspomnieć o możliwości dostępu do pewnych treści online, które bez VPN nie byłyby osiągalne z lokalizacji użytkownika. Kolejną cechą VPN jest szyfrowanie ruchu online i ukrywanie adresu IP przed ewentualnymi szpiegami. Dzięki VPN użytkownicy systemów firmowych mogą bezpiecznie korzystać z sieci firmowych nie tylko w biurze, ale również z miejsc oddalonych.

Charakterystyka rutera ALL-VPN10

Ruter ALL-VPN10 ma dwa porty WAN 10/100 Base-T/TX Ethernet (gniazda RJ45) charakteryzujące się dużą elastycznością konfiguracji. Obsługują one DHCP, stały adres IP, PPPoE, ruting statyczny i dynamiczny, NAT, PAT, przezroczysty most, MAC clone oraz DDNS. Zestawienie bezpiecznego, szyfrowanego tunelu pomiędzy urządzeniami sieciowymi za pośrednictwem Internetu wymaga stosowania zestawu protokołów IPSec. W przypadku rutera ALL-VPN10 są to szyfry: DES, 3DES, AES128, AES192, AES256, MD5, SH1, IKE Pre-Share Key oraz hasła ustawiane ręcznie.

Realizacja wszystkich funkcji z firewallem włącznie wymaga dużej mocy obliczeniowej rutera. Aby spełnić te wymagania, w ALL-VPN10 zastosowano szybki i wydajny procesor z pamięcią SDRAM i 64-bitową akceleracją sprzętową. Rozwiązania takie są stosowane w profesjonalnych urządzeniach obsługujących duże firmy. W przypadku zerwania połączenia ruter VPN łączy się ponownie.

Podstawowym protokołem wykorzystywanym w wirtualnych sieciach prywatnych jest PPTP (*Point to Point Tunneling Protocol*). Jest on oczywiście zaimplementowany w ruterze ALL-VPN10. Każdy port WAN może być skonfigurowany z wieloma DDNS-ami jednocześnie. Możliwe jest ponadto nawiązywanie połączeń VPN z dynamicznymi adresami IP.

Łatwość konfigurowania rutera ALL-VPN10 wynika z zaimplementowanej w nim funkcji QVM SmartLink VPN. Cała procedura ogranicza się do wpisania adresu IP serwera VPN oraz podania nazwy użytkownika i hasła. Wszystkie wymagane operacje są następnie wykonywane już automatycznie nawet bez udziału administratora sieci. Dzięki temu możliwe jest rozwiązywanie szeregu problemów organizacyjno-technicznych w firmach. Główna funkcja sterowania umożliwia hostowi logowanie się do zdalnych komputerów w dowolnym momencie.

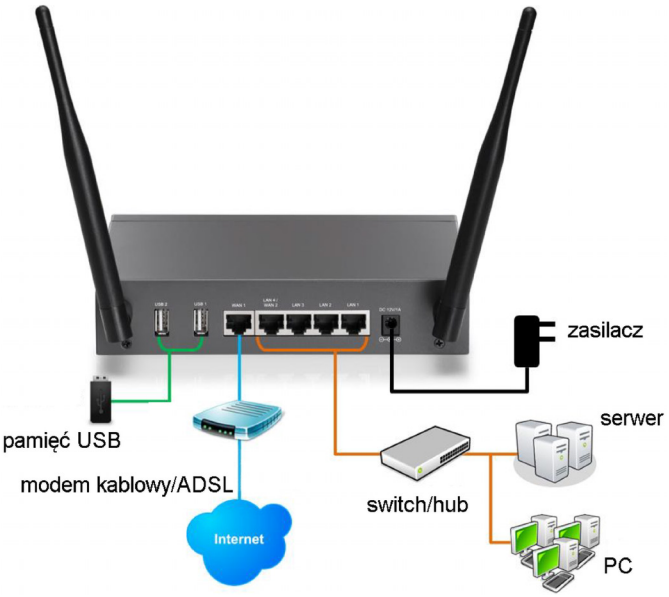
Czynnikiem ułatwiającym obsługę rutera ALL-VPN10 jest też interfejs oparty na przeglądarce internetowej. Za jego pomocą można tworzyć własne dla danego przedsiębiorstwa reguły określające dostęp do sieci. Możliwe jest więc blokowanie lub monitorowanie wybranych stron internetowych, o czym decyduje odpowiedni filtr. Cecha ta jest wręcz nieodzowna np. w szkołach i innych placówkach, w których z sieci korzystają dzieci i młodzież.

Bezpieczeństwo

Ruter ALL-VPN10 pełni ponadto jeszcze jedną, bardzo ważną dla bezpieczeństwa korzystania z sieci funkcję. Jest nią wbudowana, bardzo zaawansowana zapora sieciowa (firewall), pozwalająca na skuteczne odpieranie większości ataków z Internetu. Wykorzystywana jest do tego technika aktywnego, wspieranego sprzętowo wykrywania SPI (Stateful Packet Inspection). Do ruchu sieciowego dopuszczane są tylko te pakiety, które mają odpowiednie zezwolenie. Ciągłe śledzenie nagłówków pakietów jest wspierane sprzętowo. Jest to operacja praktycznie niezauważalna przez użytkownika. Skutkiem poniekąd ubocznym jest odrzucanie połączeń z niestandardowymi protokołami.

Instalacja – teoria

Na **rysunku 1** przedstawiono połączenia sieciowe rutera ALL-VPN10. Wszystkie gniazda urządzeń zewnętrznych oraz gniazda



Rysunek 1. Ruter ALL-VPN10 z dołączonymi urządzeniami zewnętrznymi

anten zgromadzono na tylnej ścianie urządzenia. Dwa gniazda USB są przeznaczone do dołączania pamięci masowej USB. Dostęp do Internetu zapewnia modem kablowy xDSL/ADSL dołączany do gniazda WAN1. Mogą być do niego wpinane również modemy światłowodowe, przełączniki (switche) i huby oraz inne zewnętrzne rutery udostępniające Internet. Kolejne gniazda: LAN4/WAN2, LAN3...LAN1, są przeznaczone dla urządzeń sieci lokalnej, takich jak przełączniki i huby, a także pojedyncze stacje PC oraz serwery. Są one monitorowane i filtrowane po wykonaniu konfiguracji Physical Port Management. Do ostatniego gniazda jest dołączany firmowy zasilacz wtyczkowy. Użytkownik dostaje ponadto w komplecie dwie anteny oraz wtyk kątowy do zasilacza ułatwiający umieszczenie rutera blisko ściany (**fotografia 2**). Dodatkową korzyścią wynikającą z zastosowania tego wtyku jest możliwość wyłączania zasilania za pomocą umieszczonego w nim wyłącznika mechanicznego. Elementy sygnalizacyjne zgromadzone na ścianie przedniej przedstawiono na **fotografii 3**.

W materiałach opisujących ruter ALL-VPN10 można znaleźć informację, że jego instalacja jest tak prosta, że może ją wykonać nawet babcia. Prawda, jak zwykle, jest tylko częściowa. Każdy, kto potrafi czytać ze zrozumieniem po angielsku, pewnie z instalacją rutera sobie jakoś poradzi. Znacznie gorzej będzie prawdopodobnie z jego optymalną konfiguracją, a to z dwóch powodów. Po pierwsze ze względu na sporą liczbę okien, przez które trzeba przebrnąć, a w których są ustawiane najróżniejsze, często bardzo szczegółowe parametry samego rutera oraz obsługiwanych przez niego sieci. Bez specjalistycznej, mimo wszystko, wiedzy trudno taką konfigurację przeprowadzić optymalnie. Pewnym ułatwieniem jest czarodziej prowadzący krok po kroku przez procedury instalacji i konfiguracji urządzenia. Po drugie, w dokumentacji technicznej co krok natrafiamy na tajemnicze skróty, akronimy i nazwy urządzeń teleinformatycznych, które dla laika mogą być niezrozumiałe. Zobaczmy, jak to wygląda w praktyce.

Instalacja – praktyka

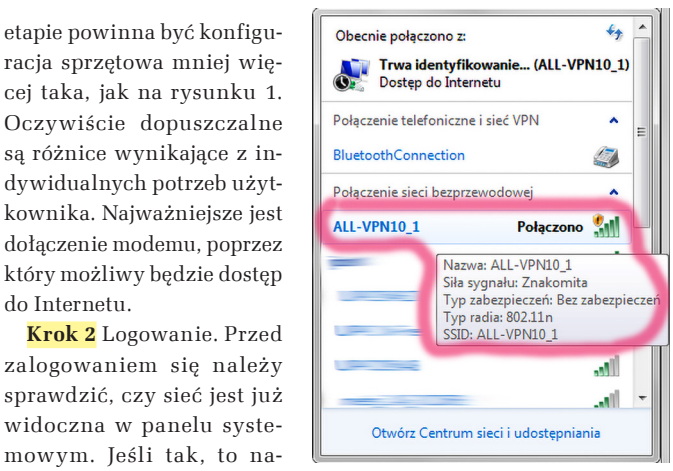
Krok 1 Podłączenie rutera i współpracujących z nim urządzeń. Jest to czynność czysto manualna. Wynikiem działań wykonanych na tym

Fotografia 2. Wtyk kątowy zasilacza

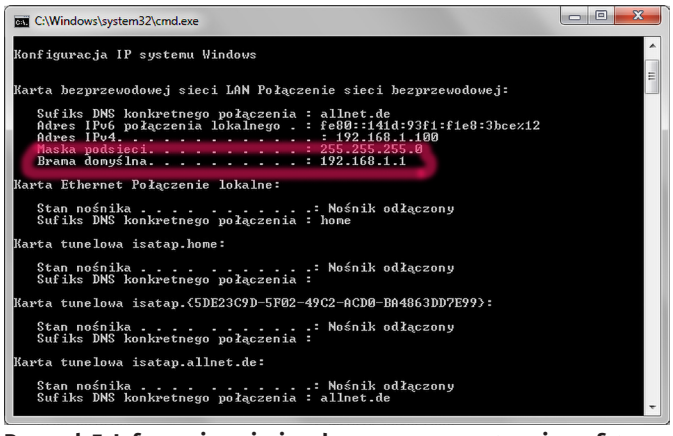
Fotografia 3. Płyta przednia rutera z elementami sygnalizacyjnymi

etapie powinna być konfiguracja sprzętowa mniej więcej taka, jak na rysunku 1. Oczywiście dopuszczalne są różnice wynikające z indywidualnych potrzeb użytkownika. Najważniejsze jest dołączenie modemu, poprzez który możliwy będzie dostęp do Internetu.

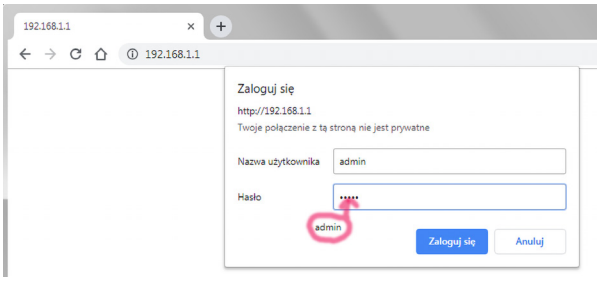
Krok 2 Logowanie. Przed zalogowaniem się należy sprawdzić, czy sieć jest już widoczna w panelu systemowym. Jeśli tak, to należy się z nią połączyć. Sieć ma domyślną nazwę ALL-VPN10_1 nadawaną automatycznie po wstępnej instalacji (**rysunek 4**). **Uwaga: na tym etapie sieć nie ma żadnych zabezpieczeń.** Następnie należy sprawdzić IP. W tym celu w oknie poleceń DOS otwieranym poleceniem `cmd` należy uruchomić program `ipconfig`. W efekcie zostają wyświetlone informacje zawierające m.in. adres IP rutera (**rysunek 5**). Domyślny adres to: 192.168.1.1. Taki adres należy wpisać w oknie przeglądarki internetowej aby uzyskać dostęp do procedur konfiguracyjnych. Dopiero w tym momencie zostaje wyświetlone okno logowania (**rysunek 6**), w którym użytkownikiem domyślnym jest `admin` mający takie samo hasło (`admin`). Dane te powinny być natychmiast zmienione, aby uniemożliwić dostęp do sieci osobom postronnym. Jest to niezwykle istotne, gdyż logujemy się na konto administratora.



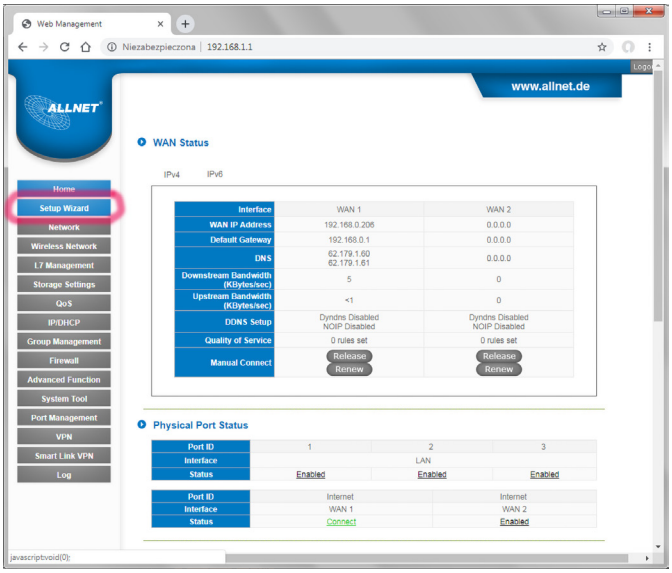
Rysunek 4. Identyfikacja sieci w panelu systemowym



Rysunek 5. Informacja o sieci podawana przez program ipconfig



Rysunek 6. Okno logowania do rutera



Rysunek 7. Okno konfiguracji sieci z listą dostępnych poleceń

Krok 3 Po zalogowaniu się można rozpocząć procedurę konfigurowania rutera. Zakładając, że wykonuje ją laik rozsądne będzie skorzystanie z czarodzieja (wizarda), który poprowadzi nas krok po kroku przez wszystkie niezbędne etapy (**rysunek 7**). Już w tym momencie pojawia się jednak pierwszy problem, gdyż należy określić typ połączenia dla sieci WAN. Do wyboru jest: DHCP (z automatycznym ustalaniem IP), PPPoE (dla sieci Poin-to-Point), static IP (stały adres IP). Załóżmy, że wybieramy opcję pierwszą.

Krok 4 Dla sieci z automatycznie ustalanym adresem IP krok 4 kończy procedurę konfiguracyjną. Podaje się w nim nazwę sieci i współdzielony klucz, bez którego znajomości nie będzie możliwe korzystanie z sieci.

Od tego momentu można już w pełni korzystać z sieci i mieć dostęp do Internetu. Faktycznie, konfigurowanie nie było zbyt skomplikowane. Kwestia – czy poradzi sobie z tym każdy pozostaje jednak otwarta. Należy pamiętać, że tak skonfigurowany ruter wykorzystuje domyślne wartości wszystkich parametrów, które w konkretnych przypadkach nie muszą być optymalne. Ich zmiana wymaga już pewnej fachowej wiedzy. Dla użytkowników z pewnością najważniejsze będą tryby zabezpieczeń, ale w środowisku, w którym funkcjonuje kilka sieci, równie ważny może być też np. wybór kanałów. Standardowo są one przydzielane automatycznie, ale często prowadzi to do nakładania się kilku sieci na jeden kanał. W takich przypadkach korzystniejsze jest ręczne ich ustawienie. Program konfiguracyjny ma wbudowany skaner umożliwiający ocenę zajętości kanałów włącznie z orientacyjnym pomiarem jakości sygnału w każdym z nich. Nie jest więc konieczne korzystanie z programów zewnętrznych, takich jak inSSIDer.

Na pewno warto kilka chwil poświęcić firewallowi, w którym ustalane są zasady dostępu i filtrowania zasobów sieciowych. Ma to kluczowe znaczenie dla bezpieczeństwa użytkowników sieci.

Nieco bardziej złożone jest konfigurowanie pozostałych typów sieci, ale opisanie wszystkich opcji przekraczałoby znacznie rozmiary artykułu. Można tylko dodać, że instrukcja do rutera ma 175 stron.

Inne cechy funkcjonalne rutera

1. WAP – bezprzewodowy punkt dostępowy. Realizacja WAP zwiększa zasięg sieci bez konieczności stosowania połączeń kablowych. Nazwa sieci bezprzewodowej (SSID) i klucze szyfrowania są generowane automatycznie i rozsyłane do urządzeń klienckich.
2. L7 VIP Priority Channel + WMM – kanał priorytetowy L7 VIP wraz z WMM (Wi-Fi Multi Media) pozwalają na priorytetową realizację pozbawionych jitteru połączeń telefonicznych z Internetem (VoIP) oraz strumieniową transmisję wideo wysokiej rozdzielczości.
3. Guest Networks Access – funkcja umożliwiająca korzystanie z sieci przez użytkowników na prawach gości. Nie są do tego potrzebne dodatkowe urządzenia, licencje i złożona konfiguracja VLAN. Dzięki wbudowanej zaporze firewall oraz serwerowi DHCP użytkownik – gość może bezpiecznie korzystać tylko z Internetu.
4. L7 Management-Blocking – rozpoznawanie i blokowanie aplikacji działających na tym samym porcie. Lista blokujących aplikacji jest kontrolowana przez administratora.
5. L7 QoS – kontrolowanie przepustowości wykorzystywanej przez poszczególne aplikacje i odpowiednie kolejkowanie ruchu w celu optymalizacji zajmowanego pasma.
6. QoS Bandwidth Management – przydzielanie pasma użytkownikom lub grupom w zależności od różnych przedziałów czasu w celu dopasowania do różnych środowisk sieciowych.
7. Łatwy w użyciu system zarządzania siecią. Administrator zarządza siecią za pośrednictwem aplikacji uruchamianej w przeglądarce internetowej. Stosowne działania może podejmować na podstawie logów zapisywanych w przypadku wszelkich nieprawidłowości. Aplikacja wymaga zalogowania się do konta administratora z podaniem unikatowego hasła.

Ocena

Ruter ALL-VPN10 można polecić zarówno użytkownikom niemającym specjalistycznej wiedzy na temat działania sieci komputerowych, jak i użytkownikom wymagającym, pragnącym świadomie uzyskać maksimum korzyści z tego urządzenia. Dla użytkowników pierwszej kategorii najważniejszą cechą jest łatwość instalacji i konfiguracji. Wszystkie wymagane czynności można wykonać dosłownie w kilka minut, by móc w pełni korzystać z sieci i z Internetu. Stosunek ceny do wykorzystywanych możliwości nie będzie jednak w takim przypadku zbyt korzystny ze względu na nieoptymalne wykorzystywanie funkcji rutera lub wręcz rezygnację z niektórych z nich. Zupełnie inaczej jest, gdy ruter ma spełniać określone funkcje i zadania wymagające bardziej świadomego i złożonego skonfigurowania. Wówczas stosunek ceny do możliwości staje się już bardzo korzystny. Testy wykazały, że ruter ALL-VPN10 zapewnia silny sygnał, połączenia są stabilne i pewne.

Dużą zaletą zastosowań w przedsiębiorstwach jest możliwość używania 2-portowej, 100-megabitowej sieci WAN o zrównoważonym obciążeniu i redundancji gwarantujących wymianę danych biznesowych. Funkcjonalność rutera zwiększają wbudowane 100-megabitowe switche LAN (max. 3 do 4). Użytkownicy pragnący zachować poufność i bezpieczeństwo przesyłanych przez sieć danych mają do dyspozycji do 10 tuneli IPSec VPN o przepływności do 100 Mb/s. Ruter obsługuje do 5 połączeń PPTP VPN. Dwie anteny, w jakie jest wyposażony ruter ALL-VPN10. zapewniają bardzo dobry sygnał nawet w pomieszczeniach o dużej powierzchni – dużych domach i biurach.

Jarosław Doliński, EP