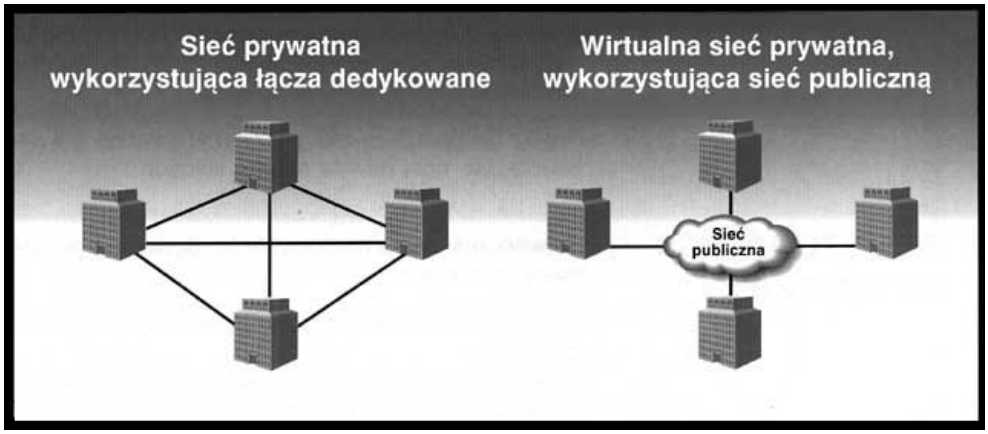
Wirtualne Sieci Prywatne
– bezpieczne sieci korporacyjne przez Internet

Roman Rekut, Paweł Skalski
Politechnika Zielonogórska, ul. Podgórna 50, 65-246 Zielona Góra

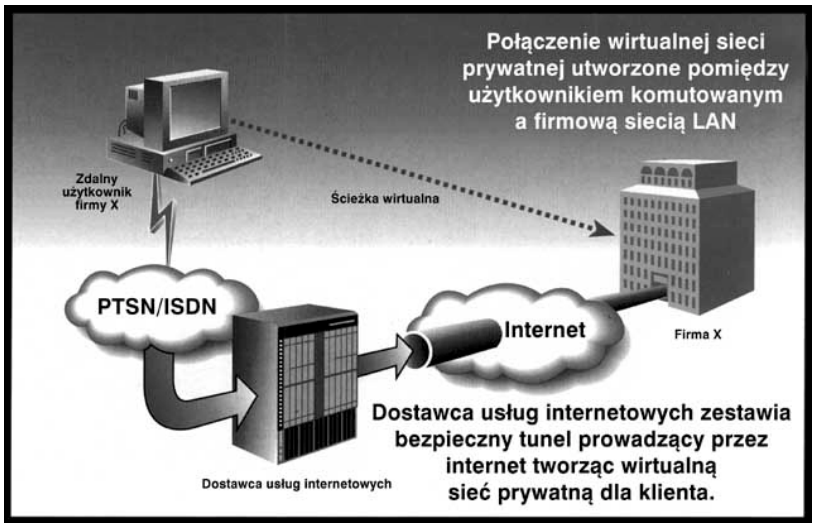
Termin Wirtualne Sieci Prywatne (Virtual Private Network – VPN) jest coraz częściej używany w odniesieniu do kierunku, w którym zmierzają komputerowe sieci rozległe. Pojęcie to często odnoszone jest do każdej publicznie dostępnej infrastruktury sieciowej, w ramach której definiowane są rozdzielne podsieci dla wykorzystania przez konkretnego klienta. Rozdział sieci dedykowanych konkretnym klientom ma w zasadzie zawsze charakter logiczny, ważne jest to, że dostawca usługi daje gwarancję prywatności. W myśl powyższej definicji VPN-y mogą być budowane w oparciu o publiczne sieci Frame-Relay, X.25 czy ATM.

Wraz z rozwojem firm tworzących nowe oddziały w innych miastach, województwach czy państwach, pojawia się problem skutecznej wymiany informacji między nimi. Tradycyjnym rozwiązaniem jest dzierżawa łączy teleinformatycznych łączących poszczególne lokalizacje. Pomijając aspekt ekonomiczny, który zezwala na stosowanie tego rozwiązania jedynie dużym i bogatym przedsiębiorstwom, w obecnych czasach koniecznym staje się jego uzupełnienie o funkcje dostępu do sieci firmowej dla pracowników terenowych (przedstawicieli handlowych, konsultantów itp.) Tradycyjnie bywa to realizowane poprzez doprowadzenie odpowiedniej ilości łącz telefonicznych oraz instalację centrali modemowej, kierującej tego typu połączenia do serwera zdalnego dostępu.
Z drugiej strony, obecne czasy scharakteryzować można jako okres gwałtownego rozprzestrzeniania się Internetu oraz traktowania go jako taniej i niezawodnej infrastruktury, umożliwiającej komunikację między dwoma dowolnymi punktami na Ziemi. Dlatego też wiele firm rozpoczęło poszukiwania tych nowo powstających możliwości komunikowania się ze swoimi, zlokalizowanymi w innych miejscach, oddziałami i partnerami.

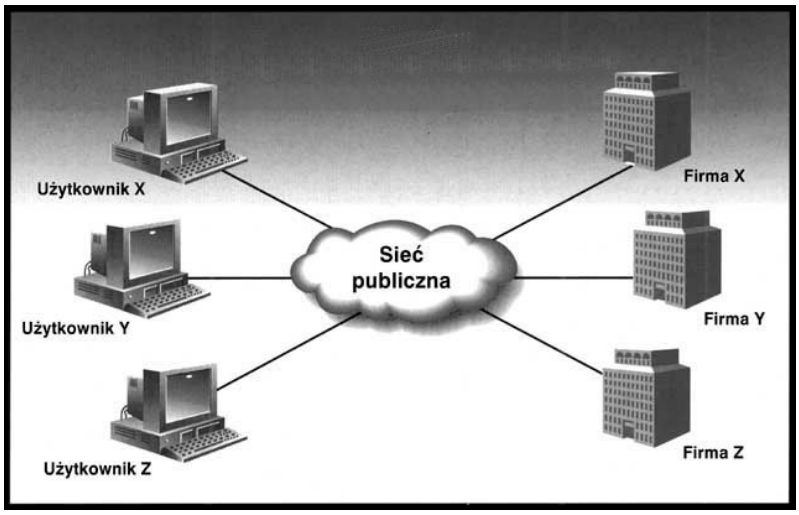
Wirtualne sieci prywatne (VPN) są jednym z możliwych rozwiązań, służących do rozwiązania wymienionych powyżej problemów. Podstawa działania VPN opiera się na wykorzystaniu Internetu jako medium transmisyjnego, łączącego poszczególne lokalizacje oddziałów firmy, jak i umożliwiającego pracownikom na zdalny dostęp do zasobów sieciowych firmy. Choć dla większości użytkowników Internet stanowi miejsce, gdzie można znaleźć strony WWW i korzystać z poczty elektronicznej, to w istocie jest on ogromną siecią komputerową, połączoną łączami teletransmisyjnymi o skomplikowanej i nadmiarowej, a przez to bardzo odpornej na awarie strukturze. Idea VPN polega na wydzieleniu w owej sieci - pomiędzy lokalizacjami, które należy połączyć – kanału wirtualnego (czyli nie związanego z fizyczną strukturą łączy), umożliwiającego zaszyfrowaną i praktycznie niezauważalną dla innych użytkowników transmisję danych. Również i sam użytkownik wirtualnej sieci prywatnej nie zauważa Internetu pośredniczącego w jego połączeniu.



W praktyce realizacja tej koncepcji sprowadza się do wydzierżawienia łączy stałych, łączących poszczególne lokalizacje oddziałów firmy z najbliższymi węzłami dostępowymi dostawcy usług internetowych. Jakkolwiek możliwa jest realizacja wirtualnej sieci prywatnej z wykorzystaniem łącz komutowanych, to zazwyczaj zapotrzebowanie na pasmo będzie przekraczało możliwości protokołu V.90 (transfer do 56 kb/s) czy pojedynczego kanału ISDN (transfer 64 kb/s). Następnie po zakupieniu routera (lub wydzierżawieniu go od dostawcy usług) i skonfigurowaniu protokołów transmisyjnych, można korzystać ze wszystkich zalet VPN. Poszczególne oddziały mogą korzystać z tej samej, replikowanej bazy danych; informacje o napływających zamówieniach i ich realizacji są dostępne dla wszystkich w zawsze aktualnej postaci; możliwe jest organizowanie pracy zespołowej, korzystając z programów *Lotus Notes* czy *Microsoft Exchange*. Przedstawiciele handlowi czy konsultanci, pracując w domu lub terenie – przy użyciu notebook'a i telefonu stacjonarnego lub komórkowego, uzyskują miejsce pracy nie różniące się pod względem komunikacji od swojego biurka w firmie. Eliminuje to konieczność korzystania z drogich połączeń międzymiastowych – korzysta się wyłącznie z połączeń lokalnych do dowolnego providera Internetu.



W stosunku do opisanego na wstępie tradycyjnego rozwiązania, którego koszty wdrożenia mogą sięgać setek tysięcy złotych, zaś opłaty miesięczne kilkudziesięciu, utworzenie wirtualnej sieci prywatnej sprowadza się do zainwestowania kilku tysięcy złotych w celu zakupu routerów dla każdej lokalizacji oraz wydatkowania kwoty rzędu kilkuset złotych miesięcznie na abonament łącza stałego.
Nie są to oczywiście jedyne możliwości, jakie oferuje technologia VPN. Korzystając z zakupionego już sprzętu można uruchomić np. system telefonii internetowej (*Voice over IP – VoIP)*, co niesie za sobą kolejne oszczędności.



Internet jako sieć publiczna o największej dostępności na świecie, stwarza możliwości utworzenia wielu tysięcy wirtualnych sieci prywatnych. Poza ewentualnymi problemami z szybkością transmisji (zbyt małe przepustowości łączy), nie ma problemów w łączności między lokalizacjami dołączonymi do różnych dostawców Internetu.

Wymagania stawiane Wirtualnym Sieciom Prywatnym

Aby VPN mogły skutecznie wypełniać swoje zadania, muszą spełniać pewne wymagania techniczne:
- gwarantować prywatność (bezpieczeństwo),
- gwarantować przewidywalne zachowanie zarówno w sensie przepustowości, jak i jakości świadczonych usług,
- umożliwiać komunikację dla protokołów innych niż IP

Sposoby realizacji prywatności.

Dla zapewnienia bezpieczeństwa w sieciach VPN stosowane są następujące technologie:
- autentykacja użytkowników
- tunelowanie i szyfrowanie
- autentykacja pakietów
- firewalle

Na potrzeby sieci VPN w celu weryfikacji użytkowników stosuje się: autentykację, autoryzację i accounting z możliwością wykorzystania centralnego serwera autentykacji, z którym urządzenia komunikują się protokołem TACACS+ lub RADIUS. Implementuje się następujące mechanizmy tunelowania: Ipsec, Layer 2 Tunelling Protocol (L2TP), Layer 2 Forwarding (L2F), Generic Routing Encapsulation (GRE) oraz technologie szyfrowania DES i 3DES.

Gwarancje jakości usług

W chwili obecnej dostawcy Internetu w Polsce nie dają standardowo gwarancji dla jakości świadczonych usług, zwłaszcza w przypadku transmisji międzymiastowych i międzynarodowych. Z drugiej strony, urządzenia wykorzystywane do budowy rdzenia Internetu (switche ATM, routery rdzeniowe) posiadają mechanizmy umożliwiające definiowanie jakości świadczonych usług. Można się spodziewać, że w niedalekiej przyszłości istnienie tych mechanizmów znajdzie odzwierciedlenie w cennikach dostawców Internetu.

Komunikacja dla wielu protokołów

Dzięki technologiom tunelowania ruchu istnieje możliwość transmisji poprzez sieci IP (w tym przez Internet) także innych protokołów sieciowych (na przykład IPX czy AppleTalk). Tunel widziany jest jako logiczny interfejs, na którym można uruchomić routing dowolnego protokołu.

Perspektywy rozwoju usług VPN w polskim Internecie

W chwili obecnej polscy dostawcy Internetu nie oferują usługi tworzenia VPN, zapewniają jedynie dostęp do sieci Internet. Dlatego firma, która zamierza stworzyć korporacyjną wirtualną sieć prywatną na obszarze regionu lub kraju, samodzielnie musi zakupić potrzebny sprzęt i oprogramowanie. Wydaje się jednak, że w nadchodzących latach sytuacja ta ulegnie zmianie. Dostawcy usług IP (już nie tylko Internetu, bo możliwość korzystania z tej sieci będzie jedną z możliwych usług), oferować będą usługi tworzenia VPN, gwarantując przy tym poufność i integralność przesyłanych danych, jak również jakość transmisji. Będzie to sytuacja bardzo korzystna dla firm, gdyż:

- eliminuje konieczność zakupu urządzeń zapewniających realizację kanałów VPN
- eliminuje konieczność aktualizacji sprzętu i oprogramowania w miarę publikowania nowych standardów technologii VPN (obowiązek ten spada na dostawcę usługi)
- koszty konserwacji i obsługi urządzeń są przenoszone głównie na dostawcę usługi

Podsumowanie

W komunikacji rozległej oparte o Internet prywatne sieci wirtualne (VPN) zapewniają elastyczną i efektywną alternatywę dla linii dzierżawionych. Przedsiębiorstwa mogą

błyskawicznie rozbudowywać swoją sieć wirtualną i zapewnić bezpieczną łączność ze swoimi odległymi komórkami i mobilnymi użytkownikami. Poprzez obsługę szerokiego zakresu standardów szyfrowania danych i negocjacji kluczy szyfrujących mogą zapewnić operatywną współpracę swojej sieci wirtualnej z sieciami swoich partnerów biznesowych. Wszystko to sprawia, iż prwadopodobnie w niedługim już czasie większość firm wdroży rozwiązania oparte o technologię VPN.