

# ZASTOSOWANIE TECHNOLOGII IPVPN W ZARZĄDZANIU PRZEDSIĘBIORSTWEM

Andrzej DULBIŃSKI

**Streszczenie:** W publikacji zastała zaprezentowana nowoczesna technologia wirtualnych sieci prywatnych opartych na protokole IP, będących wydzielonym obszarem sieci rozległych. Na przykładzie firmy kurierskiej, posiadającej kilka oddziałów zaprezentowano budowę sieci korporacyjnej Intranet z wykorzystaniem technologii IPVPN. Wskazano korzyści z jej wdrożenia, wpływ jaki wywarła na funkcjonowanie organizacji oraz koszty, jakie poniesiono w wyniku jej wdrożenia.

**Słowa kluczowe:** wirtualna sieć prywatna, technologia informacyjna, transmisja danych, sieć rozległa, bezpieczeństwo informacji

## THE USE OF IPVPN TECHNOLOGY IN COMPANY MANAGEMENT

**Abstract:** The publication presents modern technology of virtual private networks based on the protocol IP which is a section of wide air networks. The structure of the corporate network Intranet using IPVPN technology has been described on the example of a courier service company which has a few subsidiaries. The article points out benefits of such an implementation, impact it has made on the company's functioning as well as the costs incurred as a result of its introduction.

**Key words:** virtual private network, information technology, data transmission, wide area network, information security.

### 1. Wprowadzenie

Od momentu, gdy informację uznano za kolejny - czwarty czynnik produkcji, silnie wzrosło jej znaczenie w procesach zarządzania organizacją. Rozwój technologii telekomunikacyjnych, informatycznych czy też teleinformatycznych w ostatnim dziesięcioleciu oraz wykorzystanie ich w przetwarzaniu i przesyłaniu informacji, diametralnie zmieniło sposób funkcjonowania dzisiejszej organizacji. Przedsiębiorstwa funkcjonujące w dzisiejszym świecie są zmuszone do walki i egzystencji w ciągłej konkurencji oraz w otoczeniu pełnym przemian. Firmy, w których nie stosuje się nowoczesnych technologii informacyjnych, przetwarzające informacje jedynie w sposób tradycyjny, nie są w stanie konkurować w dzisiejszej gospodarce rynkowej z przedsiębiorstwem nowoczesnym, w którym nastąpiła digitalizacja informacji, gdzie bezpieczeństwo, jakość i szybkość przetwarzania i dostarczania danych do oddziałów firmy lub kooperantów stanowi ważny element zarządzania i funkcjonowania. Jak wiadomo zarządzanie to ciągle podejmowanie decyzji przez kadre menedżerską przedsiębiorstwa, dlatego tak ważne jest zdobycie informacji często dla nich strategicznych w czasie możliwie krótkim, przesłanej bezbłędnie i przede wszystkim bezpiecznie. Ustanowienie przez Międzynarodową Organizację Normalizacji ISO (ang. International Organization for Standardization) Modelu Referencyjnego Połączonych Systemów Otwartych OSI (ang. Open Systems Interconnection) dotyczącego łączenia różnych technologii sieci komputerowych było początkiem powstania dzisiejszych rozległych sieci transmisji danych. Technologie, takie jak FrameRelay, czy ATM (ang. Asynchronous Transfer Mode) wykorzystywane są aktualnie w rozległych sieciach komputerowych WAN (ang. Wide Area Network), umożliwiając przesyłanie danych między poszczególnymi organizacjami rozproszonymi na terenie danego kraju i poza nim. Sieci szkieletowe stanowią doskonałą infrastrukturę sieciową realizującą funkcjonowanie sieci

wirtualnych VPN (ang. Virtual Private Network), dzięki którym przedsiębiorstwa mogą stworzyć szereg nowoczesnych, stabilnych i bezpiecznych kanałów dystrybucji informacji. Duża popularność protokołu IP w sieciach prywatnych oraz rozwój wielu aplikacji sieciowych, czy usług internetowych, oraz potrzeba ich wykorzystywania w przedsiębiorstwach, stała się przyczyną wzrostu popytu na technologię łatwą do wdrożenia, charakteryzującą się elastycznością i uniwersalnością w łączeniu lokalnych sieci komputerowych rozproszonych w oddziałach firmy. Kolejnym ważnym czynnikiem przemawiającym za wdrożeniem sieci VPN, jako elementu łączącego sieci firmowe przedsiębiorstwa jest bezpieczeństwo przesyłanych danych. O ile zabezpieczenie samych systemów informatycznych przed ingerencją z zewnątrz przedsiębiorstwa spoczywa w gestii wykwalifikowanej kadry informatycznej, o tyle w przypadku transmisji należy stosować takie technologie sieciowe, które w wysokim stopniu gwarantują poziom bezpieczeństwa, szybkość i jakość. Wzrost wydajności infrastruktury oraz obniżenie cen usług spowodowały znaczny zwrot zainteresowania użytkowników w stronę wirtualnych sieci prywatnych opartych na protokole IP. Wśród szerokiej gamy firm oferujących gotowe rozwiązania na dużą uwagę zasługuje oferta rozległej ogólnopolskiej komercyjnej sieci transmisji danych FR/ATM zarządzanej przez firmę Orange Polska.

## **2. Realizacja usługi IPVPN w sieci rozległej**

Ze względu na brak dotychczasowej możliwości skorzystania z gotowego rozwiązania sieci IPVPN, przedsiębiorstwa pragnące posiadać sieć, umożliwiającą połączenie swych placówek zmuszone były realizować swe przedsięwzięcie poprzez wykorzystanie tzw. kanałów wirtualnych, kreowanych w sieci rozległej operatora. Kanały te były zestawiane bezpośrednio pomiędzy dwoma punktami przesyłania informacji. Także dla przedsiębiorstwa posiadającego centralę oraz kilka oddziałów koniecznością było zestawienie takiej samej liczby kanałów. Poza tym musiały być poniesione znaczne koszty związane z konfiguracją, oprogramowaniem oraz z nabyciem urządzeń umożliwiających współpracę sieci lokalnej z siecią rozległą, tzw. ruterów. Sieci wirtualne pracujące z popularnym protokołem IP, w przeciwieństwie do zestawionych jedynie kanałów wirtualnych, pozwoliły na znacznie prostsze wdrożenie tejże technologii jako medium połączeniowego sieci lokalnych przedsiębiorstwa. Od pewnego czasu zauważyć można wprowadzenie na rynku transmisji danych usługi oferowanej przez operatorów sieci rozległych, polegającej na stworzeniu z własnych zasobów sieciowych sieci prywatnych, wykreowanych dokładnie pod kątem potrzeb klienta. Usługa IPVPN, świadczona przez Orange skierowana jest do organizacji oczekujących szybkiej niezawodnej sieci transmisji danych, wykorzystujących szereg różnych aplikacji sieciowych, dla których jakość przesyłanych informacji stanowi ważny czynnik. Sieć oparta jest na nowoczesnej technologii, pozwalającej na łączenie wielu sieci lokalnych, budowę sieci Intranetowych oraz dzięki dołączeniu kooperantów również Ekstranetowych. Wdrożenie IPVPN oferowanej przez operatora telekomunikacyjnego stanowi przykład wykorzystania outsourcingu telekomunikacyjnego. Rozwiązanie takie dla organizacji posiada wiele zalet, do których należy zaliczyć:

- zarządzanie siecią wirtualną jest realizowane przez operatora sieci rozległej,
- dostęp do sieci jest możliwy praktycznie na terenie całego kraju,

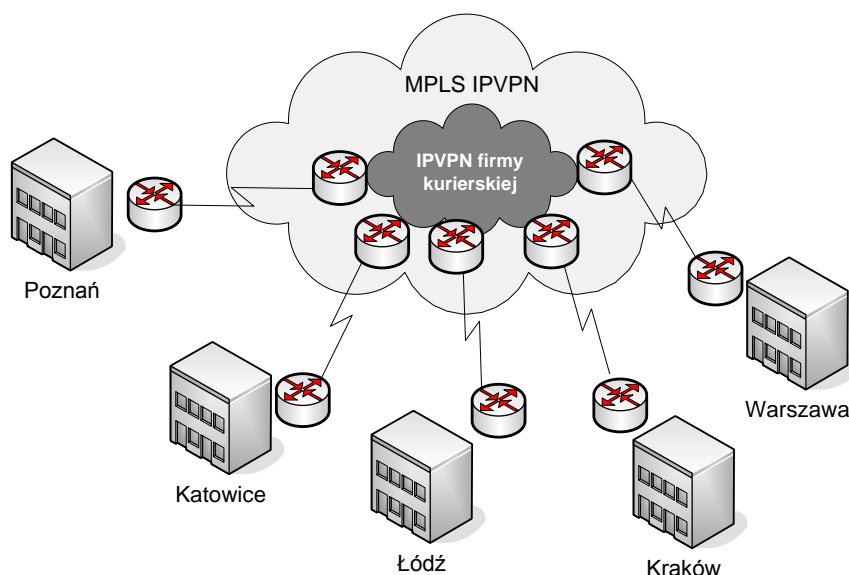
- wszystkie zmiany w konfiguracji dokonywane są przez operatora sieci z wcześniejszym ich zgłoszeniem,
- brak ponoszonych inwestycji w jakiegokolwiek urządzenia związane z siecią IPVPN ze strony przedsiębiorstwa; całe koszty są przeniesione na stronę operatora sieci (nie ma potrzeby zakupu ruterów, których rolą jest między innymi przejście ze standardu w sieci lokalnej do sieci rozległej; urządzenia takie dostarcza operator sieci wirtualnej),
- przedsiębiorstwo posiada szybką i bezpieczną sieć transmisji danych IPVPN, nadzorowaną i kontrolowaną przez zespół wykwalifikowanych specjalistów,
- brak konieczności zatrudniania administratora sieci wirtualnej,
- konsultacje i wsparcie techniczne w zakresie wdrożenia technologii IPVPN w sieci klienta.

Użytkownik sieci otrzymuje urządzenia umożliwiające bezpośrednio wpięcie własnej sieci lokalnej na poziomie standardu Ethernet; ma możliwości wprowadzenia własnej adresacji sieciowej, co w znacznym stopniu ułatwia mu skonfigurowanie sieci. W celu zapobiegnięcia przeciążeniom sieci został zaimplementowany mechanizm Quality of Service, w tym priorytetyzacji ruchu w sieci. Pozwala on skutecznie unikać przeciążeń w sieci oraz efektywnie wykorzystywać dostępne pasma IP, zapewnia też lepsze parametry jakościowe dla głównych aplikacji klienckich. W ramach tej usługi klientom oferuje się trzy poziomy ważności transmisji danych, a także nadanie specjalnego priorytetu dla transmisji głosu i video. Przedsiębiorstwo może skorzystać z jednego z trzech wariantów sieci IPVPN: standard, biznes i multimedia. W przypadku pierwszym użytkownik ma możliwości szybkiego uruchomienia sieci wirtualnej, ale bez możliwości nadawania jakichkolwiek priorytetów transmisji. Rozwiązanie to zalecane jest tam, gdzie organizacja nie wykorzystuje krytycznych aplikacji sieciowych dla jej funkcjonowania. Opcja druga pozwala wykorzystać wszystkie zalety sieci wirtualnej IP. Są już zaimplementowane mechanizmy zarządzania ruchem w celu uniknięcia przeciążenia, zagwarantowania lepszych parametrów jakościowych dla aplikacji szczególnie ważnych z punktu widzenia firmy oraz optymalizację wykupionego pasma IP. Stworzono możliwość hierarchizacji ruchu z aplikacji klienckiej do trzech poziomów z różnymi priorytetami ważności. W opcji multimedia użytkownikom poza posiadaniem wszystkich udogodnień klasy biznes udostępniono możliwość integracji transmisji danych z przekazami multimedialnymi, które posiadają bezwzględny priorytet. Poszczególne oddziały przedsiębiorstwa są podłączane według jednej z poniższych metod dostępu:

- FrameRelay z prędkością 64 kb/s, 128 kb/s, 256 kb/s, 512 kb/s, 1 Mb/s oraz 2 Mb/s,
- ATM z prędkością do 40 Mb/s,
- DSL podstawowy (ang. Digital Subscriber Line) symetryczny z prędkością 64 kb/s, 128 kb/s, 256 kb/s, 512 kb/s,
- DSL podstawowy asymetryczny z prędkością (prędkość od abonenta/prędkość w stronę sieci) 64/256 kb/s. 128/512 kb/s, 256/1024 kb/s, 512/2048 kb/s,
- DSL gwarantowany symetryczny z prędkością 64 kb/s, 128 kb/s, 256 kb/s, 512 kb/s,
- DSL gwarantowany asymetryczny 64/256 kb/s. 128/512 kb/s, 256/1024 kb/s, 512/2048 kb/s.

### 3. Wdrożenie sieci IPVPN w przedsiębiorstwie kurierskim

Przykładem wdrożenia technologii wirtualnej sieci prywatnej jest ogólnopolska firma zajmująca się dostarczaniem przesyłek kurierskich. Wykonanie projektu i doradztwo w zakresie realizacji sieci wirtualnej IP zostało przeprowadzone przez operatora sieci rozległej. Firma składa się z pięciu oddziałów rozmieszczonych na terenie Polski, do których zostały zainstalowane łącza dostępowe przez operatora sieci rozległej WAN (ang. Wide Area Network) przedstawiono na rysunku nr 1.



**Rys. 1. Topologia wirtualnej sieci IP firmy kurierskiej.**  
Źródło: Opracowanie własne na podstawie danych firmy

Dostęp do poszczególnych lokalizacji firmy pierwotnie miał być zrealizowany z prędkością 1 Mb/s. Niestety po dokonaniu analizy możliwości podłączenia oddziałów z tą prędkością została podjęta decyzja o zastosowaniu następujących technologii dostępowych (tab. 1).

**Tabela 1. Wykaz lokalizacji przyłączonych do sieci**

L.p.	Lokalizacja	Metoda dostępu do sieci wirtualnej
1	Warszawa	FrameRelay 1 Mb/s
2	Łódź	DSL asymetryczny 256 kb/s
3	Poznań	DSL symetryczny 256 kb/s
4	Katowice	FrameRealy 1 Mb/s
5	Kraków	FrameRelay 1 Mb/s

Źródło: Opracowanie własne na podstawie danych firmy

Jakość i szybkość przesyłanych informacji stanowi jedno z najważniejszych elementów wpływających na prawidłowe dostarczanie przesyłek kurierskich. Połączenie lokalnych sieci komputerowych w sieć Intranet umożliwiło wprowadzenie pracy on-line. Pracownicy otrzymali narzędzia pozwalające na kontrolę procesu dostarczania przesyłek kurierskich na terenie całego kraju. Wykorzystanie wirtualnych sieci prywatnych stanowi nie tylko doskonałe rozwiązanie techniczne, ale co jest równie ważne ekonomiczne. Stała łączność, szybkość, bezpieczeństwo oraz brak ograniczeń w wielkości przesyłanych danych stanowi bardzo atrakcyjną alternatywę w stosunku do stosowanych dotychczas technologii

przekazywania informacji za pośrednictwem łączy komutowanych. Koszty poniesione przez firmę przedstawiono w tabeli 2.

*Tabela 2. Koszty ponoszone w wyniku uruchomienia i utrzymania sieci IPVPN*

L.p.	Lokalizacja	Koszt aktywacji – opłata jednorazowa (netto)	Koszt miesięczny (netto)
1	Warszawa	1499	2599
2	Łódź	999	1299
3	Poznań	999	999
4	Katowice	1499	2599
5	Kraków	1499	2599

Źródło: Opracowanie własne na podstawie danych firmy

Opłaty za korzystanie z sieci IPVPN dotyczą dostępu i zarządzania siecią. Ich wysokość nie jest uzależniona od odległości pomiędzy lokalizacjami klienta, ale zależy jedynie od metody dostępu do sieci rozległej i parametrów z jakimi zostało skonfigurowane połączenie. W przypadku dostępu do sieci wirtualnej w technologii FrameRelay lub DSL (ang. Digital Subscriber Line) użytkownikowi zabezpiecza się minimalną gwarantowaną prędkość tzw. CIR (ang. Committed Information Rate), równy wykupionej prędkości dostępowej łącza.

#### **4. Podsumowanie**

Rozwój technologii związanych z przekazywaniem informacji uległ w ostatnim czasie dużym przemianom, które silnie wpłynęły na funkcjonowanie organizacji. Stosowanie ich wymusza ciągłą konkurencja na rynku. Brak inwestycji w nowoczesne technologie, oczywiście w ramach własnych możliwości i potrzeb jej wykorzystania stanowi nieodzowny element w zarządzaniu przedsiębiorstwem. Szczególnie rozwój transmisji danych, wzrost jakości i bezpieczeństwa ich przesyłania w rozległych sieciach nie mógł przejść obojętnie obok przedsiębiorstw. Trudno wyobrazić sobie firmę nie wykorzystującą u siebie cyfrowych technologii przetwarzania danych, nie posiadającą komputera, czy nie korzystającą z dobrodziejstw sieci Internet. Organizacje duże, rozproszone geograficznie są zmuszone korzystać z rozwiązań sieci rozległych, czy w postaci sieci IPVPN, lub innych. W przeciwnym wypadku konkurencja będzie działać sprawniej, a klient będzie czuł się dowartościowany i należycie obsłużony. Zwracając dużą uwagę na jakość i bezpieczeństwo danych firmy, których ochrona ma dużą wagę, wykorzystanie właśnie sieci wirtualnych w budowie sieci korporacyjnych stanowi prawidłową drogę w rozwoju wykorzystania technologii komunikacyjnych w dzisiejszym i przyszłym przedsiębiorstwie.

#### **Literatura**

1. Dudycz H.: Wizualizacja danych. Wyd. AE, Poznań 1998.
2. Kiełtyka L.: Komunikacja w zarządzaniu. Techniki, narzędzia i formy przekazu informacji. Wyd. Placet, Warszawa 2002.
3. Kiełtyka L.: Technologie informacyjne w funkcjonowaniu organizacji. Towarzystwo Naukowe Organizacji i Kierownictwa "Dom Organizatora", Toruń 2013.
4. Polaczek T.: Audyt bezpieczeństwa informacji w praktyce. Wydaw. HELION, Gliwice 2006.

5. Spotrack M.: Sieci komputerowe. Biblia. Wyd. Helion, Gliwice 2003.