STUDIA INFORMATICA 2003
Volume 24 Number 2B (54)

Adam DUSZEŃKO
Politechnika Śląska, Instytut Informatyki

SIECI IP VPN

Streszczenie. Tematem artykułu jest przybliżenie zasad działania sieci VPN, prezentacja wykorzystywanych protokołów, przedstawienie różnorakiego podejścia do zastosowań technologii VPN oraz technicznych problemów związanych z budową sieci VPN.

Słowa kluczowe: wirtualne, sieci, prywatne, VPN, bezpieczeństwo, poufność.

IP VPN NETWORKS

Summary. This paper presents basic principles of VPN technology, used protocols, variety of VPN applications and technical problems related to building VPN networks. It describes how to adapt Internet to get secure and cost-effective communication.

Keywords: virtual, private, network, secure.

1. Wstęp

Postępująca globalizacja wymaga udostępnienia szybkich i poufnych łączy zabezpieczających kontakt pomiędzy oddziałami firm, jak i pomiędzy firmą i pojedynczym klientem. Stale rozwijający się Internet może zapewnić wydajną wymianę informacji, o ile zastrzeżemy poufność przesyłanych danych. Stosunkowo tanim sposobem zapewnienia bezpieczeństwa i poufności danych jest technologia VPN. VPN - Wirtualna Sieć Prywatna (Virtual Private Network) jest wydzieloną częścią ogólnodostępnej sieci komputerowej, stanowiącą logicznie suwerenną całość. Nowe protokoły wykorzystywane w tej technologii dają coraz większy poziom bezpieczeństwa, umożliwiając w pełni korzystanie z ogólnodostępnej sieci globalnej Internet. VPN umożliwia z zachowaniem pełnej kontroli

bezpieczeństwa uczynienie informatycznych systemów firmy lepiej dostępnych zarówno dla wewnętrznych pracowników, jak i dla osób z zewnątrz, w tym współpracowników i klientów. Korzyści wynikające z zastosowania technologii VPN są uzależnione od konkretnie wybranych rozwiązań. Celem tego artykułu jest zarysowanie budowy i zasad działania tych rozwiązań.

Rozwiązania zaliczane do kategorii sieci VPN można podzielić zasadniczo na trzy grupy.

1.1. Zaufane sieci VPN (Trusted VPN)

Zaufane sieci VPN tworzone są przez dostawcę usług sieciowych. Definiuje on drogę poruszania się pakietów. Nie występuje tu żadna ochrona poufności transportowanych pakietów ani ich integralności. Dostawca usługi kontroluje jakość usługi (QoS). Użytkownik korzystający z tej usługi nie ma żadnej możliwości sprawdzenia, czy dostarczane połączenie jest w pełni kontrolowane tylko i wyłącznie przez dostawcę, pozostaje mu polegać tylko na zaufaniu do dostawcy. Ten typ sieci VPN opisano w dokumencie RFC 3031.

1.2. Bezpieczne sieci VPN (Secured VPN)

W tym podejściu do sieci VPN główny nacisk położono na zachowanie poufności i integralności pakietów. Uzyskuje się to na drodze szyfrowania przesyłanych pakietów. Nie jest definiowana trasa ruchu, dlatego nie ma gwarancji jakości usługi QoS.

1.3. Hybrydowe sieci VPN (Hybrid VPN)

Połączenie powyższych dwóch odmian technologii VPN polega na zakodowaniu części transmisji (lub całości) przesyłanej siecią zaufaną, co umożliwia zachowanie gwarancji poufności i integralności przy jednoczesnym zachowaniu kontroli jakości łącza.

2. Zasada działania VPN

2.1. Tunelowanie

Działanie VPN opiera się na tunelowaniu, czyli przesyłaniu pakietów z sieci lokalnej poprzez inną sieć (sieć Internet).

Zestawienie połączenia VPN pomiędzy odległymi sieciami nie wymaga tworzenia niezależnego fizycznego połączenia. Skrajne rutery sieci lokalnych mające wbudowane funkcje

obsługi połączeń VPN „opakowują" pakiety sieci lokalnej i jako dane przesyłają przez sieć globalną.

Sam proces przesyłania pakietów (tunelowania) składa się z dwóch podprocesów :

- enkapsulacji,
- szyfrowania.

2.1.1. Szyfrowanie

W zależności od potrzeb i uwarunkowań można stosować różne metody szyfrowania:

- szyfrowanie kluczem symetrycznym – wymaga niewygodnego i stwarzającego ryzyko utraty poufności danych, fizycznego dostarczenia identycznego klucza szyfrującego do nadawcy i odbiorcy danych;
- szyfrowanie kluczem publicznym i prywatnym – obecnie najbardziej preferowana metoda szyfrowania, dająca największy stopień bezpieczeństwa.

Co więcej, różne części pakietów mogą być objęte szyfrowaniem. Na przykład, mogą być szyfrowane tylko dane przesyłane w polu danych, a może być szyfrowany cały kapsułkowany pakiet.

2.1.2. Enkapsulacja

Wspomniana enkapsulacja polega na obudowaniu pakietu pobranego z sieci lokalnej w protokół warstwy sieciowej sieci, przez którą odbywa się prywatne wirtualne połączenie, i przesłaniu przez tę sieć.

2.2. Protokoły sieci VPN

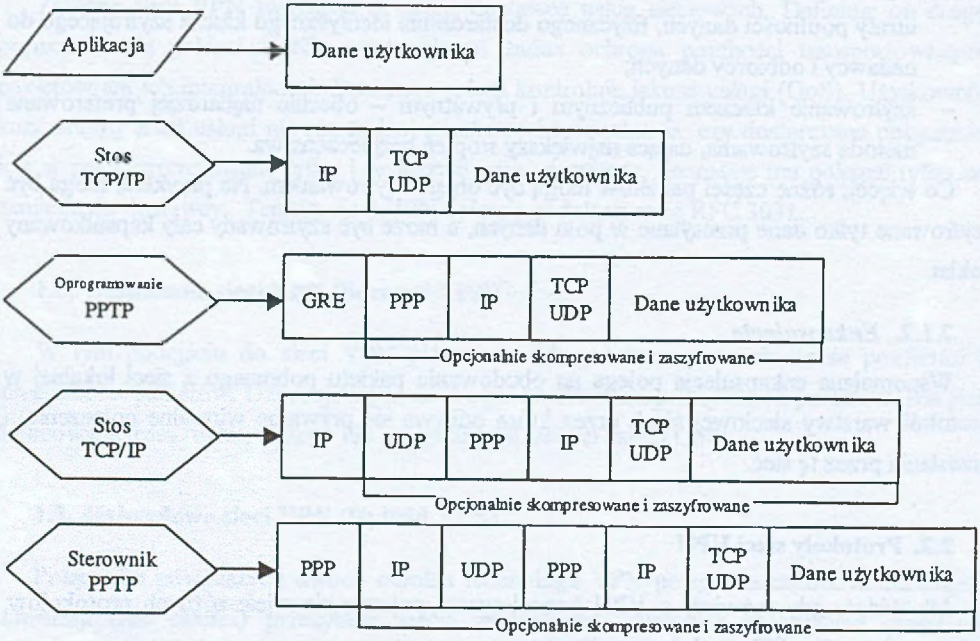
Jak widać, gdy mówimy o VPN i tunelowaniu, pojawia się wiele różnych protokołów, które można zakwalifikować do trzech grup:

- protokołów transportowych (Carrier Protocol) – protokoły, którymi przenoszone są zaszyfrowane pakiety sieci lokalnej, czyli protokoły w oparciu o które działa sieć typu WAN,
- protokołów kapsułkowania (Tunneling protocol) – protokoły dokonujące procesu tunelowania, czyli szyfrowania i kapsułkowania (IPSec, PPTP, L2TP),
- protokołów przenoszonych (Passenger) – protokoły w oparciu o które działają łączone sieci LAN (IPX , NetBEUI , IP).

Istotny jest fakt, że technologia VPN nie jest dedykowana ani protokołom tunelowanym, ani protokołom, przez które odbywa się tunelowanie.

2.3. Protokół PPTP

Jednym z pierwszych protokołów umożliwiających rozszerzenie zasięgu sieci lokalnych przez VPN z wykorzystaniem linii telekomunikacyjnych był protokół PPTP. W tym protokole (rys.1) pakiet, przygotowany przez stację nadawczą w jej stosie protokołów sieciowych, był obudowywany przez protokół TCP/IP, który zapewniał kontrolę utrzymania łącza oraz przesyłany jako datagramy IP z wykorzystaniem protokołu PPP (warstwa 2 OSI). Największą jego zaletą jest możliwość transportowania protokołów wyższych warstw.



Rys. 1. Enkapsulacja w protokole PPTP
Fig. 1. PPTP protocol encapsulation

2.4. Weryfikacja użytkownika

Oprócz zapewnienia bezpieczeństwa samej transmisji, równie istotne ze względów bezpieczeństwa jest zapewnienie weryfikacji klienta, chcącego uzyskać dostęp do kanału wirtualnego. W zależności od stosowanego protokołu kapsułkowania używa się różnych metod autoryzacji klientów:

- PAP
- CHAP
- MS-CHAP

2.4.1. PAP

Pierwszy z wymienionych, stosowany w połączeniu z protokołem PPTP, jest najsłabszy, gdyż przesyła login i hasło użytkownika prostym tekstem. Taki sposób uwierzytelniania może być stosowany tylko jednorazowo, to znaczy dane hasło może być użyte tylko raz, bo ponowne jego użycie nie daje gwarancji autentyczności klienta. Ten sposób uwierzytelniania jest już praktycznie nie stosowany.

2.4.2. CHAP

Metoda CHAP jest znacznie lepsza, gdyż chroni hasło użytkownika przed podsłuchaniem, nie przesyłając go wcale przez sieć do serwera VPN.

Po zgłoszeniu się klienta i prośbie o udostępnienie połączenia VPN, serwer VPN przesyła klientowi identyfikator sesji i łańcuch wezwania. Klient dołącza do tych danych swoje hasło i z powstałego ciągu znaków wylicza algorytmem MD5 sumę kontrolną, którą wraz z loginem przesyła do serwera. Serwer, na podstawie otrzymanego loginu i pobranego z bazy hasła, analogicznie wylicza sumę kontrolną, co daje podstawę do przeprowadzenia weryfikacji autentyczności klienta.

2.4.3. MS-CHAP

MS-CHAP jest firmową wersją protokołu CHAP stworzoną przez firmę Microsoft w celu zastosowania go w systemach Windows 2000.

2.5. Protokół IPSec

Protokół IPSec działa na poziomie warstwy sieci modelu OSI. Składa się z trzech protokołów, zapewniających wymianę kluczy wykorzystywanych do szyfrowania (Key Exchange), autoryzacji (AH) i enkapsulacji (ESP).

Protokół IPSec umożliwia m.in:

- szyfrowanie transmisji, na przykład algorytmem DES;
- badanie integralności danych, tzn. sprawdzanie, czy informacje nadana i odebrana są identyczne;
- autoryzację, czyli potwierdzanie, że otrzymane informacje pochodzą od właściwego nadawcy.

Protokół IPSec może działać w dwóch trybach:

- transportowym – szyfrowane są jedynie dane przenoszone przez pakiet. Nagłówek pakietu pozostaje widoczny, przez co adresy źródłowy i docelowy w tym trybie nie są chronione;

- tunelowym – cały pakiet jest szyfrowany włącznie z nagłówkiem. Tak utworzony pakiet opatrywany jest nowym nagłówkiem, zawierającym adresy ruterów będących końcami utworzonego w ten sposób tunelu.

3. Jakość w sieciach VPN (QoS)

Przy zapewnieniu bezpieczeństwa przesyłanych danych i uwierzytelnieniu użytkownika pozostaje jeszcze zapewnienie niezbędnej minimalnej przepustowości kanału wirtualnego. W sytuacji gdy sieć globalna opiera się na IP, a dostawcy zwykle nie dają gwarancji jakości świadczonych usług, zapewnienie niezbędnego transferu jest ważnym problemem. Chociaż istnieją już technologie i rozwiązania pozwalające na definiowanie jakości usług na poziomie rdzenia sieci IP, to nie są one jeszcze stosowane. Stosowanie mechanizmów kontroli jakości (Quality of Service) ma na celu zapewnienie wymaganego przez krytyczne aplikacje pasma przepustowości i optymalizację wykorzystania łączy sieci VPN. W sieciach VPN używane są mechanizmy QoS, takie jak:

- klasyfikacja pakietów (Packet Classification), Traffic Policing, Traffic Shaping;
- kontrolowanie i unikanie zatorów w sieci (Congestion Management - WFQ, Congestion Avoidance - RED, WRED).

W chwili obecnej IETF pracuje nad standardem mechanizmu Diff-Serv, polegającego na wykorzystaniu bajtu ToS (Type-of-Service), który miałby określać, jaka klasa QoS ma być zapewniona dla danego pakietu (bajt ten określono jako DS - Diff-Serv).

4. Funkcjonalne i techniczne aspekty sieci VPN

Sieci VPN możemy rozpatrywać w dwóch aspektach:

- funkcjonalnym,
- technicznym.

4.1. Funkcjonalny podział sieci VPN

Pod względem funkcjonalnym możemy rozróżniać sieci VPN jako rozwiązania łączące ze sobą odrębne sieci LAN oraz łączące sieć LAN z pojedynczym klientem.

Z tego powodu sieci VPN dzielimy na:

- sieci dostępowe – służące do rozszerzenia sieci lokalnej, umożliwiając podłączenie się do niej (za pomocą sieci publicznej) oddalonych, mobilnych pracowników, nie znajdujących się w zasięgu sieci korporacyjnej;
- sieci Site-to-Site;
  - intranetowe – są logicznie równoważne korporacyjnym sieciom WAN, umożliwiającym połączenie filii przedsiębiorstwa z centralnym systemem komputerowym. Wykorzystują sieci publiczne oparte na protokołach IP, Frame Relay lub ATM;
  - ekstranetowe – opierają się na protokołach z rodziny TCP/IP i łączą ze sobą równoważne jednostki, np. współpracujące korporacje; działają na tych samych zasadach co sieci intranetowe.

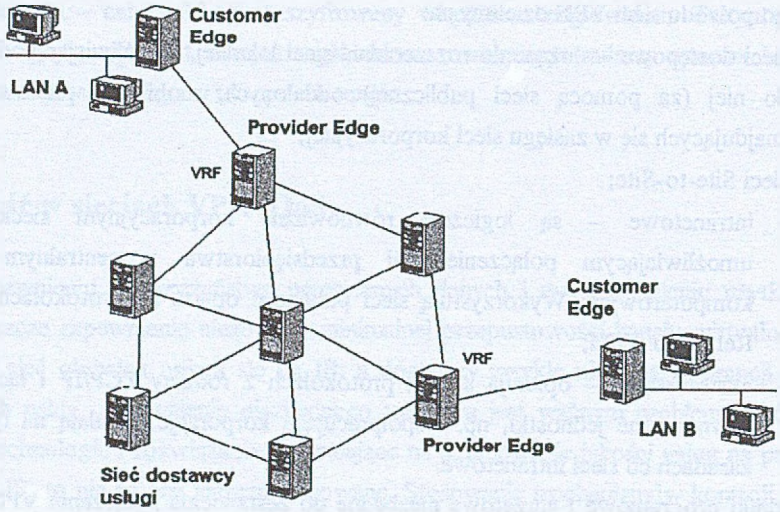
Składniki programowe i sprzętowe niezbędne do zestawienia połączenia VPN zależą od tego, co z czym łączymy. Jeżeli są to pojedyncze komputery, wystarczą systemy operacyjne wyposażone w mechanizmy wspierające VPN. W pozostałych przypadkach potrzebne są:

- klient usługi VPN – wbudowany w system operacyjny;
- serwer VPN łączący sieć lokalną z kanałem wirtualnym;
- urządzenie dedykowane typu firewall;
- NAS (Network Access Server) wykorzystywany przez dostawcę do zapewnienia dostępu do VPN przez zdalnego użytkownika.

Narzędzia VPN dostarczane są wraz z większością dostępnych na rynku systemów komputerowych. Narzędzia te umożliwiają zestawianie połączeń VPN bez stosowania rozwiązań firm trzecich. W przypadku niewystarczającej mocy obliczeniowej serwera VPN należy zastosować sprzętowe mechanizmy szyfrowania.

4.2. Przykładowa topologia sieci

Aspekt techniczny przedstawiono na przykładzie pokazanym na rys.2.



Rys. 2. Przykład topologii sieci
Fig. 2. Example of the network topology

Urządzenia biorące udział w działaniu sieci VPN możemy podzielić na następujące:

- urządzenia składające się na sieć LAN;
- urządzenie zapewniające klientowi LAN dostęp do sieci publicznej, jest to np. ruter. Ten element najczęściej jest nazywany Customer Edge (CE);
- ruter brzegowy operatora sieci publicznej nazywany jako Provider Edge;
- rutery wewnętrzne sieci dostawcy.

5. Trasowanie pakietów sieci VPN

Dla zapewnienia maksymalnej wygody użytkowania sieci VPN problem trasowania jest przerzucany na stronę dostawcy usługi. To właśnie urządzenie typu Provider Edge ma za zadanie rozwiązywanie problemu trasowania pakietów sieci VPN. Trasowanie jest rozwiązywane na podstawie tablicy VRF (VPN Routing and Forwarding), która jest budowana przez brzegowy ruter dostawcy. Rutery znajdujące się wewnątrz sieci, nie podłączone bezpośrednio z urządzeniami Customer Edge, przesyłają pakiety VPN nie wiedząc, że jest to transmisja w kanale wirtualnym.

Rutery brzegowe mogą problem trasowania rozwiązywać metodą statyczną, lecz dla zapewnienia wysokiej jakości usługi VPN i ułatwienia konfiguracji wykorzystuje się metody dynamicznego routingu, a spośród nich najczęściej algorytmy BGP. Wcześniejszy algorytm

RIP (Routing Information Protocol) jest wypierany przez BGP ze względu na to, że BGP przy generowaniu mniejszego ruchu zapewnia efektywniejszy sposób wybierania drogi pakietów.

5.1. Przykładowe rozwiązanie sprzętowe

Wraz z rozwojem zainteresowania technologią VPN pojawiają się nowe urządzenia typu CE udostępniające coraz większą funkcjonalność. W najbliższej przyszłości firma Optimus rozpocznie produkcję urządzenia ABA IPSec Gate, które na bazie standardowego komputera klasy PC pozwala między innymi na realizację szyfrowanych połączeń VPN przez sieć WAN. Urządzenie oparte jest na specjalnie opracowanej wersji Linux'a zapisanej w pamięci typu flash. Klucze sprzętowe potrzebne do szyfrowania danych przekazywane będą za pomocą portu USB i aktywowane po podaniu kodu za pomocą specjalnej klawiatury numerycznej.

6. Umiejscowienie firewall'a i serwera VPN

Osobnym problemem przy podłączaniu sieci lokalnej do usługi VPN jest wzajemne umiejscowienie względem siebie serwera VPN i firewall'a.

6.1. Architektura WAN-Firewall-VPN-LAN

W tym rozwiązaniu cała sieć LAN i serwer VPN są chronione od ataków z zewnątrz przez firewall, który filtrując nadchodzące pakiety, kontroluje usługi, z jakich usiłuje korzystać zdalny użytkownik. Pewną nienaturalną sytuacją jest fakt, że wszystkie pakiety kierowane do serwera VPN muszą zostać przepuszczone niezależnie od tego, co się w nich znajduje. Ponieważ są one zaszyfrowane, firewall nie może ich zbadać i musi przekazać je do serwera VPN. Jest to jednak dopuszczalne ze względu na to, że serwer VPN dokonując uwiarygodnienia połączenia kontroluje bezpieczeństwo.

6.2. Architektura WAN-VPN-Firewall-LAN

Wysunięcie serwera VPN przed firewall powoduje, że firewall w pełni kontroluje rodzaj usług i treści pakietów przesyłanych przez połączenie. Minusem jest jednak fakt, że serwer VPN jest praktycznie niechroniony przed atakami z zewnątrz, co powoduje konieczność dodatkowego uwiarygodnienia użytkownika, który już się uwiarygodnił w serwerze VPN ponownie na firewall'u.

Podsumowanie

Technologia VPN nie jest jednorodna i z góry zdefiniowana. Korzysta ona z wielu elementów składowych, których dobór stanowi zasadniczy element warunkujący końcowy efekt. Otwiera ona zupełnie nowe możliwości integracji odległych systemów i to często systemów zróżnicowanych, których bezpośrednie połączenie nie byłoby możliwe.

Przedstawione rozwiązania są podstawowymi sposobami realizacji zadań postawionych przed technologią VPN. Wraz z rozwojem algorytmów szyfrujących poziom bezpieczeństwa sieci VPN będzie wzrastał. Według prognoz technologia VPN ma szansę odegrać wiodącą rolę w zabezpieczaniu operacji wykonywanych poprzez sieć Internet, stając się prawdopodobnie jednym z podstawowych rozwiązań „business-to-business".

LITERATURA

1. Praca zbiorowa: Vademecum teleinformatyka. IDG, Warszawa 2002, tom II.
2. Niewiarowski C., Skiepko T.: Droga prywatna - wstęp wzbroniony. PC World Computer OnLine, 2002.
3. Zawadzki M.: Wirtualne sieci prywatne. PCkurier, 2001.
4. Koziński M.: Bezpieczne połączenie przy użyciu protokołu IPSec. PCkurier, 2002.
5. Praca zbiorowa: VPN Technologies: Definitions and Requirements. VPN Consortium, January 2003.
6. Praca zbiorowa: The Evolution of Internet Protocol Virtual Private Networks. Quarry Technologies, 2003.

Recenzent: Dr inż. Andrzej Białas

Wpłynęło do Redakcji 24 marca 2003 r.

Abstract

The article describes the way of adapting Internet to secure communication by using Virtual Private Networks (VPN) technology that make it possible for not only big business to cost-effectively connect multiple remote networks.

VPNs use a process called "tunneling" to pass encrypted traffic over the Internet. The packets that travel across the Internet can be encrypted.

A VPN consortium defines three types of VPN networks : trusted, secured and hybrid.

A trusted VPN is created by provider who defines the specific path between two ends of the communication tunnel. User has no way to verify if the provider does his work well and that is why this is called trusted VPN.

A secure VPN is created by using cryptography with no definition of the data path through the public network. Source packets are encrypted and encapsulated into new packet that passes the public network. Nobody can read or change the content of original packets.

A hybrid VPN is created by applying both previous techniques together. This solution gives us QoS control and security with no need to trust our provider.

The basic groups of protocols used in VPN are: carrier protocol (WAN protocols), tunneling protocols (IPSec, PPTP, L2TP) and passenger protocol (LAN protocol). This article focuses on secure VPN build on IP networks.

Adres

Adam DUSZEŃKO: Politechnika Śląska, Instytut Informatyki, ul. Akademicka 16, 44-101 Gliwice, Polska, duszek@polsl.gliwice.pl .