Deploying IP-based Virtual Private Network Across the Global Corporation

STANISLAV MILANOVIC
Serco Group plc
Via Sciadonna 24/26, 00044 Frascati (RM)
ITALY

ZORAN PETROVIC
Faculty of Electrical Engineering
University of Belgrade
Bulevar Kralja Aleksandra 73, 11000 Belgrade
YUGOSLAVIA
e-mail: zrpetrov@ubbg.etf.bg.ac.yu

Abstract: This paper discribes an implementation of the VPN (Virtual Private Network) over the Internet for a large-scale customer as a service provider managed service. Furnishing a global corporation with turnkey solution for it's inter and intrabusiness communication needs delivered security, quality and cost efficiencies. The accompanied highly reliable professional customer support further assisted the client in bringing the new applications onto the network quickly and efficiently.

Key-words: IP-VPN, Internet, Intranet/Extranet, IPSec, Tunneling, Encryption, Authentication

1 Introduction

The advent of the 21st century invites new ways of thinking about global networks. We are on the brink of a huge transformation as service providers seek to meet customer demand for global network services by building carrier-scale, intelligent networks. The second-generation e-Business is one that leverages networking to create a virtual corporation composed of a highly dynamic collection of employees, groups, corporate locations, partners, suppliers, and customers based on ever-changing business requirements. To survive in today's economy, businesses must be able to move quickly and immediately adapt to the environment as it changes around them. A competitive second-generation e-Business is built on the premise that the business model, partners and geographic locations it encompasses will change continually and thus it needs an adaptable, logical network infrastructure to support it. To meet increasingly important needs for adaptability, efficiency, and timeliness, companies must create a logical business network that enables users to share network resources and access company applications, regardless of where they are geographically located.

In recent times, as more businesses have found the need for high speed Internet connections to their private corporate networks, there has been significant interest in the deployment of IP-based VPNs (IP-VPNs) running across the Internet. This has been driven by the ubiquity and distance insensitive pricing of current Internet services, that can result in significantly lower costs than typical private line or frame relay services. IP-VPNs will drive the need for cost-effective bandwidth and help to proliferate the use of emerging technologies suitable for business applications [1], [2], [3], [4]. IP-VPNs provide corporations the ability to cost-effectively extend the corporate network to remote sites, telecommuters and mobile workers, reduce communications costs among

their existing corporate sites, and in communications with business partners. Once deployed, these services provide the infrastructure necessary to support additional IP-based services such as hosted applications, voice services and video teleconferencing over WANs [5].

E-business, e-commerce, e-marketplace, business-to-business (B2B) and business-to-consumer (B2C) are now common business parlance. Every organisation is defining and implementing its e-strategy. The question is no longer whether to migrate to an e-environment, but what is the best way to migrate to a Web- and Internet-based business model. One of the key technologies for using the Internet in a secure and private manner is the Virtual Private Network.

2 IP-VPNs Overview

The VPNs can be simply defined as the emulation of a private wide area network (WAN) facility using IP facilities (private IP networks or the public Internet). As such, there are as many types of VPNs as there are types of WANs. Where IP backbones are constructed using frame-relay or asynchronous transfer mode (ATM) networks protocols, by interconnecting routers over the switched backbone, the VPNs operate on top of this IP network and hence do not directly utilize the native mechanisms of the underlying backbone. Native VPNs are restricted to the scope of the underlying backbone, whereas IP based VPNs (IP-VPNs) can extend to the extent of IP reachability [6]. Classes of service required can be specified by policies implemented within the service provider network. Availability is enhanced by the connectionless nature of IP communications.

Three functions form the basis of IP-VPNs:

- Tunneling

Tunneling is a technology that supports the routing of non-routable private IP addresses over public networks such as the Internet [7]. To protect data, VPN hardware or software creates tunnels through the net. To create a tunnel, the source end encrypts its outgoing packets and encapsulates them in IP packets for transit across the Internet. At the receiving end, a gateway device removes and decrypts the packets, forwarding the original packets to their destination. A VPN device may terminate multiple IP tunnels and forward packets between these tunnels and other network interfaces in different ways. An IP tunnel is viewed as just another sort of link, which can be concatenated with another link.

- Authentication
  Authentication technology guarantees the identity of VPN participants (that gateways and client PCs are who they say they are) and that the information received has integrity and has not been tampered with (verifies that a packet has not been altered during its trip over the Internet).
- Encryption
  Encryption is a technique for scrambling and unscrambling information to guarantee the privacy of information as it flows over the Internet. With 3DES (Data Encryption Standard), the data is encrypted (56-bit key #1), decrypted (56-bit key #2) and encrypted again (56-bit key #3), but with three different keys. This results in an effective key-length of 168-bits.

Internet Protocol Security (IPSec) is an emerging standard for IP-VPN security [8]. The standard, which was written by Internet Engineering Task Force (IETF) committees, consists of a set of IP-level protocols for setting up an agreement between two IP stations about the encryption and digital signature methods that will be used [9]. IPSec supports tunneling, authentication and encryption for protecting the data. IPSec is often considered the best VPN solution for IP environments, as it includes the strongest encryption (3DES - Triple Data Encryption Standard) and authentication measures, as well as a management system for the required cryptographic keys (PKI — Public Key Infrastructure [10]) in its set of standards [11].

There are three types of IP-VPNs connectivity services [12]:

- Intranet IP-VPNs uses the public Internet or the service provider's IP backbone to establish secure tunnels between corporate sites replacing existing private lines, ATM or Frame Relay. Businesses that run their intranets over an IP-VPN service enjoy the same security, quality of service (QoS), reliability, and manageability as they do in their own private networks. Access technology ranges from dial-up or digital subscriber line (DSL) for smaller branch offices, to E1/T1 or E3/T3 for higher speed connections to corporate sites. When an IP-VPN is used to connect multiple enterprise sites, each site is connected to the nearest service

provider point of presence (POP). Here, only the link between the branch office (or corporate site) and the provider is tariffed on a monthly basis. Individual virtual circuits are no longer required for connections to multiple sites resulting in hard cost savings. Savings are even greater for international connectivity, where the costs for leased lines, ATM, or frame relay connections may be substantial.

- Remote access IP-VPNs service enables secure, anytime, anywhere access to a corporate network by remote and mobile workers. The access technologies in use today include dial-up, DSL, wireless, and cable. The privacy of the remote access session is assured by encrypting the link over the Internet or the service provider's backbone. IPSec provides a standardized, highly secure technology for this purpose. Service provider or corporate authentication servers identify users as being eligible to connect to the corporation. With a remote access VPN, users connect to the local service provider's POP and an IP-VPN software client on their PC is used to securely access their corporate network resources via IP-VPN gateway. The remote access IP-VPN eliminates long distance and/or 800 number per minute costs as well as a dedicated RAS (Remote Access Server) equipment.
- Business-to-Business (B2B) IP-VPNs (Extranets) enable e-commerce between corporations and their suppliers, distributors, and customers. The primary benefit is increased speed and improved business efficiency. Here, an IP-VPN will include the necessary access control and authentication mechanisms to provide groups of users, including business partners and cus-tomers, with dynamic access to corporate services and data. These connections can be both remote and dedicated connections between multiple private networks and/or between a private network and the Internet. This is essentially a policy decision that can be enforced via a firewall, router with an access list functionality, application gateway, or similar device that is capable of applying policy to transit traffic. Secure communication is ensured by IPsec tunnels, data encryption, and firewall protection. Extranets will require network address translation (NAT) to prevent overlap of IP address space within the IP-VPN. When an IP-VPN is used to connect an extranet site, the supplier site is connected to the nearest service provider POP. The Internet or service provider's backbone is then used as the transport before the final connection at the corporate site. The service provider typically manages the IP-VPN hardware configuration, tunnels, network address translation, and connectivity.

There are two complementary implementations of IP-VPNs. The first implementation is based on equipment owned and operated by the service provider but located on the customer's premises and known as CLE (customer located equipment) IP-VPN. The second implementation is based on equipment owned and operated by the service provider but located on the service provider's premises at the edge of his network and known as network-based IP-VPN. IP-VPNs for certain businesses can be offered using elements of both solutions, bringing the best attributes from each.

3 Objective

The main objective was to connect multiple, geographically distributed locations (whether they're partners, suppliers, employees, or other) in a seamless way without extensive or costly technical investments. This way, successful businesses should have converted their local area networks (LANs) into logical business networks (LBNs) that combine geographically dispersed networks under one roof, into one logical network. The result would be a network in which employees have access to all the company information and applications as if they were all in the same building. Whether working from a branch location, at home, or on the road, employees' experiences should be exactly as if they were at the company's headquarters.

These connectivity goals were the drivers behind the following, equally important, business objectives: improve network capabilities, reduce network costs, improve communications, organizational efficiency, streamline business processes, improve employee satisfaction and improve relationships with customers and partners.

4 Requirements

In the second wave of eBusiness, customers want more than simple connectivity; they want secure access and

control for personalized services, data, applications and content from any where, at any time, over any media. They want a secure personal business environment that allows them to access and deliver anything they need to do their jobs with exactly the level of service they require for the task at hand.

Business customer wanted support for its Intranet and Extranet applications to integrate data, voice, and video traffic securely over IP-VPN. It was also required the Access VPN options including dial, digital subscriber line (DSL), cable, and wireless to allow remote users to securely access their corporate intranet through the public infrastructure. It is mandatory that deployed IP-VPN provides security through the encryption of packets and authentication of users attempting to access the corporate sites. Classes of service required should be specified by policies implemented within the service provider network.

5 The IP-VPN Deployment

In the original corporate network (Figure 1), a business had an Intranet connecting remote locations with headquarters. Each campus had a router connecting the campus to a backbone router over a LAN or WAN link. A single router was connected to both the campus LAN and to the other campuses with a WAN link. WAN routers were mesh-connected using leased lines or a Frame Relay service.

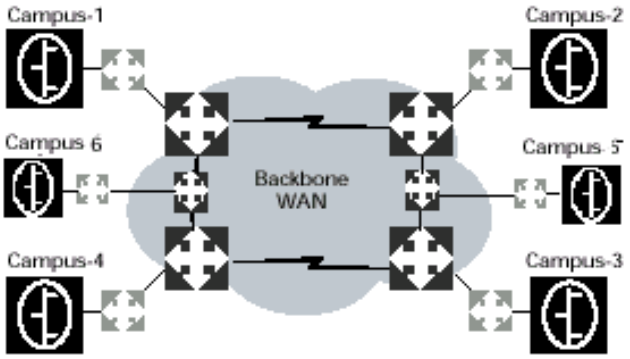

Figure 1. Original Corporate Intranet without VPN

Primary cost elements for original Intranet scenario included:

- Routers, both campus and backbone.
- Telecommunications services, in particular long distance. The cost of the Intranet backbone, depending on the traffic volume and geographical reach, can run from tens of thousands of dollars a month to hundreds of thousands of dollars a month. These costs were especially onerous for a multi-national organization.

When not using a VPN, mobile and remote users had used analog (dial-up modems) or ISDN switched services to connect to a headquarters data center. These connections were used to access e-mail, to download files and to execute other transactions. This type of connection had also been used by small offices that do not have a permanent connection to the enterprise Intranet.

With a VPN, as shown in Figure 2, remote users and branch offices set up dial-up connections to local ISPs and connect via the Internet to a VPN server at headquarters.

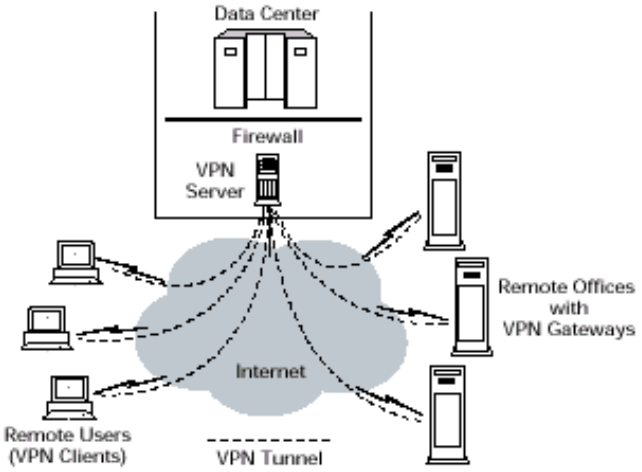

Figure 2 Deployed Remote Access using VPN

With a VPN, the Intranet backbone WAN was replaced by the Internet. The global corporation can engage now in business transactions (via the Intranet or Extranet connections) or other communications in a secure and private manner by using a VPN over the Internet. Figure 3 shows the new environment. The new costs for this configuration include the deployment and maintenance of VPN gateways at remote campuses and the deployment and maintenance of a VPN server at the headquarters site. In addition, each location pays for an Internet connection.

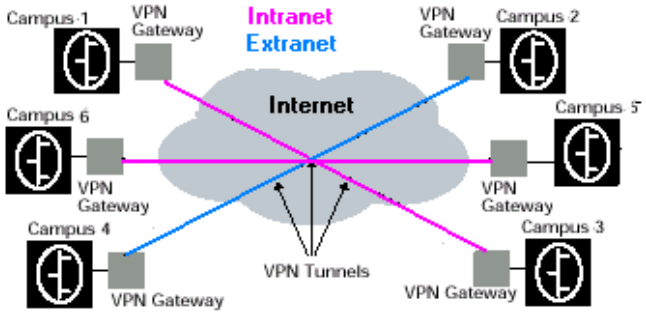

Figure 3. Deployed Corporate Intranet/Extranet with VPN over the Internet

VPN benefits include:

- Elimination of backbone routers.
- Elimination of system administration, configuration, and technical support for routers and elimination of the need to design and maintain routing tables.
- Elimination of long-distance services; as with the remote access case, this results in substantial savings. The amount of savings depends on the size of the intranet.
- Reduction in lost-opportunity cost due to the elimination of long provisioning cycles for long-distance service and for international telecommunications services.
- Better performance than an intranet due to higher speed facilities inside the Internet.

6 Conclusion

IP-VPNs will be a fundamental mechanism for service providers to deliver business services to customers. As customers turn to service providers for more than just access to the Internet, IP-VPNs will enable providers to offer differentiated, value-added services to subscribers in a secure, private network. By offering the subscriber more flexibility at lower cost, the service provider can grow market share, reduce customer churn, and improve their profitability.

References:

[1] Stanislav Milanovic, Alessandro Maglianella, "ATM over ADSL Probe in Telecom Italia Environment", Computer Networks, the International Journal of Computer and Telecommunications Networking, Vol. 34, No. 6, pp. 965-980, November 2000, published by Elsevier Science, http://www.elsevier.com/inca/publications/store/5/0/5/6/0/6/index.htt. Proceedings of TERENA Networking Conference 2000, the Trans-European Research and Education Networking Association Conference: "Pioneering Tomorrow's Internet", pp. CD-ROM, May 2000, Lisbon, Portugal, http://www.terena.nl/tnc2000/proceedings/10A/10a3.pdf

[2] Stanislav Milanovic, "At the Front End in Migrating to Gigabit Ethernet", Proceedings of SoftCOM 2000, the IEEE Conference on Software, Telecommunications and Computer Networks, pp.369-378, October 2000, http://www.fesb.hr/SoftCOM/2000/IE/Network_Architectures.htm

[3] Stanislav Milanovic, Zoran Petrovic, "A Practical Solution for Delivering Voice over IP", Lecture Notes in Computer Science, the International Journal for the reporting of new developments in computer science research, published by Springer Science, http://www.springer.de/comp/lncs/index.html. Proceedings of ICN'01, the International Conference on Networking, July 9-13, 2001, Colmar, France, http://iutsun1.colmar.uha.fr/pgmICN01.html

[4] Stanislav Milanovic, Zoran Petrovic, "Building the Enterprise-wide Storage Area Network", Proceedings of EUROCON 2001, the IEEE International Conference on Trends in Communication, pp. CD-ROM, July 5-7, 2001, Bratislava, Slovak Republic, http://www.ktl.elf.stuba.sk/EUROCON/

[5] "Broadband Service Node: IP-Based Virtual Private Networks", White Paper, Nortel Networks, 2000.

[6] "A Framework for IP Based Virtual Private Networks", INTERNET DRAFT, Internet Engineering Task Force, 2000.

[7] Mark Tuomenoksa, "Demystifying VPN-An Introduction to VPN Technology", OpenReach, Inc., 2000,

[8] Eric Zines, " VPNs Step Up to the Enterprise", Network World, Inc, 2000.

[9] "Private Use of Public Networks for Service Providers", Technical Paper, 3Com Corporation, 1998.

[10] "Consider These...The Top VPN User Concerns", Technology Report, Network World, Inc., 2000.

[11] Dave Kosiur, " Tech Talk: VPNs", White Paper, Technology Report, Network World, Inc., 2000.

[12] "A Practical Guide to the Right VPN Solution", The Technology Guide Series, The Applied Technologies Group, Inc., 2000.