Win-Win Scenario for Corporate Communications Featuring QoS-Enabled Internet VPN

STANISLAV MILANOVIC *, NIKOS E. MASTORAKIS * #

* WSEAS, Highest Institute of Education, Science and Technology
Haghiou I. Theologou 17
15773, Zographou,
Athens, GREECE
Stanislav.Milanovic@wseas.org http://www.wseas.org/hiest

MILITARY INSTITUTIONS OF UNIVERSITY EDUCATION
HELLENIC NAVAL ACADEMY
Terma Hatzikyriakou, 18539, Piraeus, GREECE.
mastorakis@wseas.org http://www.hna.gr/index-hna.htm

Abstract: This paper describes adoption of QoS-enabled Internet VPN solution for corporate communications as an alternative to expensive private WAN. A large-scale customer sorted out the lack of knowledge and resources to deploy and manage enhanced Internet services by outsourcing the service management to its Internet Service Provider (ISP), which turned out to be a win-win scenario because the provider could profit from the economy of scale by sharing of technical and human resources. Furthermore, ISP saw management as a new product with greater potential service differentiation than a pure connectivity service. The security achieved in VPN was based on IPSec tunnels, while QoS was supported by mechanisms as proposed by the Differentiated Services being defined by the IETF.

Key-words: Internet VPN, QoS, DiffServ, SLA, IPSec, e-Business

1 Introduction

New business connections are deeply entwined with Internet connectivity and IP networking advances. Internet-based Virtual Private Network (Internet VPN) services that include guaranteed Quality-of-Service (QoS) and Service Level Agreements (SLAs) are proving to be among the most enabling solutions for enterprise connectivity. 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. Internet VPNs will drive the need for cost-effective bandwidth and help to proliferate the use of emerging technologies suitable for business applications [1]-[11].

Internet 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 Internet-based services such as hosted applications, voice services and video teleconferencing [12].

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 QoS-Enabled Internet VPN

Most vendors of VPN solutions identified three usage scenarios that are all placed around a corporate Intranet that is securely connected to friendly „entities“ over the Internet. The scenarios differ in the entities connected: remote users, branch office networks (Intranets) or business partners/suppliers networks (Extranet). Only network layer VPNs are general enough to handle all three scenarios. IP Security (IPSec) evolved from the IPv6 development of the IETF. It is an open architecture for IP-packet encryption and authentication, thus it is located in the network layer [13]. IPSec adds additional headers/trailers to an IP packet and can encapsulate (tunnel) IP packets into new ones. There are three main functionalities of IPSec separated in three protocols. One is the authentication through an Authentication Header (AH), the other is the encryption through an Encapsulating Security Payload (ESP) and, finally, an automated key management through the Internet Key Exchange (IKE) protocol (formerly called ISAKMP/Oakley). IPSec provides an architecture for key management, encryption, authentication and tunneling. Therefore, all of the previously defined VPN business scenarios can be implemented with IPSec.

Because of the absence of a scalable resource reservation mechanism for the Internet core networks, the IETF developed the Differentiated Services (DiffServ) concept. DiffServ is a light-weight and scalable QoS mechanism [14]. A single byte (DS Code Point, formerly called TOS) in the IP header is used to code different per-hop behaviors (PHB) that an IP packet can experience. Inside of a network, all IP traffic using the same code point is called “DiffServ behavior aggregate” and is treated the same way. DiffServ can provide scalability by aggregating the flows into a small number of DiffServ classes and by implementing traffic conditioning at the boundary routers of a network or an administrative domain.

A service level agreement is a contract negotiated between an ISP and its customers. One ISP can be a customer of another ISP. The SLA specifies a traffic profile, network behavior and payment/billing scenario. The SLA can refer to aggregated flow identifiers such as address prefixes. The SLA can be negotiated in a number of ways, for example via a phone call, e-mail or using bandwidth brokers [15]. To deliver the user data and to provide QoS through the entire network such as the Internet that consists of multiple administrative domains, a SLA would be required not only between the customer and the ISP, but also between ISPs [16]. Thus, each domain negotiates with its adjacent domain a bilateral SLA specifying the volume and the type of traffic. The agreements can be pre-negotiated and static or they can be established dynamically. The static agreements are defined with the initiation of the service and they change quite infrequently. The negotiation of static agreements is done by human interaction. In this model the network resources can be provisioned based on the expected negotiated traffic. The dynamic agreements may change more frequently based on the current users requirements [17]. This allows a user to react on current requests from its users. Over reservation of DiffServ capacities could be reduced. The agreements can be negotiated in case of having the traffic which is more conducive to a “pay-per-usage“ model. One example of this traffic is IP telephony, where users can pay on “per-call“ basis .

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 e-Business, customers want more than simple connectivity; they want secure access and control for personalized services, data, applications and content from anywhere, 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 Internet 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 Internet VPN provides the SLA-aware QoS, along with end-to-end 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 Application Scenario

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.

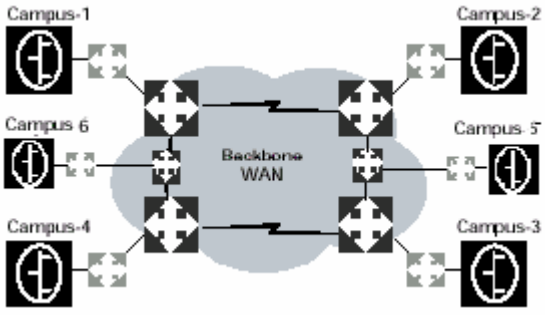

Figure 1. Original Corporate Intranet without VPN

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.

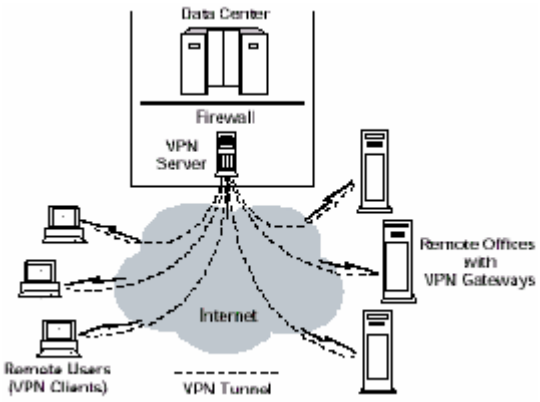

Figure 2 Deployed Remote Access using VPN

With a VPN, the Intranet backbone WAN was replaced by the Internet. The global corporation can engage now in business transactions or other communications in a secure and private manner by using 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.

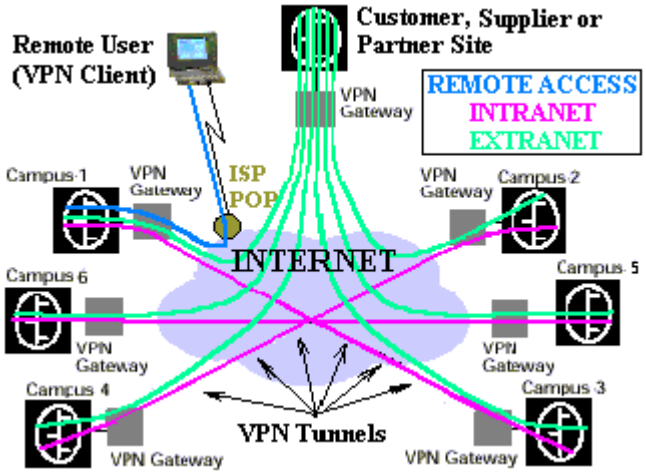

Figure 3. QoS-enabled Internet VPN delivering end-to-end security for corporate communications

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

QoS-enabled Internet VPNs will be a fundamental mechanism for service providers to deliver business services to customers efficiently and cost-effectively [18]. As customers turn to service providers for more than just access to the Internet, QoS-enabled Internet VPNs will enable providers to offer differentiated, value-added services to subscribers in a QoS compatible end-to-end secure 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, Nikos E. Mastorakis, "Architecting the Next Generation End-to-End e-Business Trust Infrastructure", WSEAS TRANSACTIONS on COMMUNICATIONS, Issue 1, Volume 1, July 2002, WSEAS Press, http://www.wseas.org/journals/communications Proceedings of WSEAS CSCC 2002, pp. CD-ROM, WSEAS Press, Rethymno, Crete Island, Greece, July 7-14, 2002, http://www.wseas.org/New_Books.htm

[2] Stanislav Milanovic, Nikos E. Mastorakis, "Internetworking the Storage Area Networks", WSEAS TRANSACTIONS on COMMUNICATIONS, Issue 1, Volume 1, July 2002, WSEAS Press, http://www.wseas.org/journals/communications. Proceedings of WSEAS CSCC 2002, pp. CD-ROM, WSEAS Press, Rethymno, Crete Island, Greece, July 7-14, 2002, http://www.wseas.org/New_Books.htm. Advances in Information Science and Soft Computing, pp. 152-157, WSEAS Press, 2002, http://www.wseas.org/8052602.doc, Proceedings of WSEAS ISA 2002, pp. CD-ROM, WSEAS Press, Cancun, Mexico, May 12-16, 2002, http://www.wseas.org/New_Books.htm

[3] Stanislav Milanovic, Nikos E. Mastorakis, "Delivering Enhanced Voice Services over the Internet", WSEAS TRANSACTIONS on SYSTEMS, Issue 1, Volume 1, pp. 74-80, January 2002,WSEASPress,http://www.wseas.org/SYSTEMS JANUARY2002.htm. Proceedings of WSEAS MMACTEE 2001, pp. CD-ROM, WSEAS Press, Vouliagmeni, Athens, Greece, December 29-31, 2001, http://www.wseas.org/History.htm

[4] Stanislav Milanovic, Nikos E. Mastorakis, "A Transition Path to Gigabit Ethernet over WDM in Support of Emerging e-Business Applications", WSEAS TRANSACTIONS on SYSTEMS, Issue 1, Volume 1, pp. 80-87, January 2002, WSEAS Press,http://www.wseas.org/SYSTEMSJANUARY2002.htm. Proceedings of WSEAS MMACTEE 2001, pp. CD-ROM, WSEAS Press, December 29-31, 2001, Vouliagmeni, Athens, Greece, http://www.wseas.org/History.htm

[5] Stanislav Milanovic, Zoran Petrovic, "Securing the Networked e-Business Throughout an Internet Distributed Organization", Advances in Intelligent Systems, Fuzzy Systems, Evolutionary Computation,

pp. 180-186, February 2002, WSEAS Press, http://www.wseas.org/New_Books.htm. Proceedings of the WSEAS EC'02, pp. CD-ROM, WSEAS Press, February 11-15, 2002, Interlaken, Switzerland, http://www.wseas.org/conferences/2002/interlaken/program.pdf

[6] Stanislav Milanovic, Zoran Petrovic, "Deploying IP-based Virtual Private Network across the Global Corporation", Communications World, pp.13-17, WSEAS Press, July 2001,, http://www.wseas.org/8052386.doc. Proceedings of WSEAS CSCC 2001 pp. CD-ROM, WSEAS Press, Rethymno, Crete Island, Greece, July 8-15, 2002, http://www.wseas.org/New_Books.htm

[7] Stanislav Milanovic, Zoran Petrovic, "A Practical Solution for Delivering Voice over IP", Proceedings of IEEE/IEE/WSES ICN'01, July 9-13, 2001, Colmar, France, http://iutsun1.colmar.uha.fr/pgmICN01.html, Lecture Notes in Computer Science (LNCS #2094), Part II, pp. 717-725, July2001, Springer-Verlag GmbH & Co. KG, http://link.springer.de/link/service/series/0558/tocs/t2094.htm

[8] Stanislav Milanovic, Zoran Petrovic, "Building the Enterprise-wide Storage Area Network". Proceedings of IEEE EUROCON 2001, Vol.1, pp. 136-139, July 5-7, 2001, Bratislava, Slovakia, http://www.ktl.elf.stuba.sk/EUROCON/program.htm

[9] Stanislav Milanovic, "At the Front End in Migrating to Gigabit Ethernet", Proceedings of IEEE SoftCOM 2000, Vol.1, pp. 369-378, October 10-14, 2000, Split, Rijeka (Croatia), Trieste, Venice (Italy), http://www.fesb.hr/SoftCOM/2000/IE/Network_Architectures.htm

[10] Stanislav Milanovic, Alessandro Maglianella: "ATM over ADSL Probe in Telecom Italia Environment", Computer Networks, Vol. 34, No. 6, pp. 965-980, December 2000, Elsevier Science, http://www.elsevier.nl/gej-ng/10/15/22/49/32/show/toc.htt. Proceedings of TERENA Networking Conference 2000, pp. CD-ROM, May 2000, Lisbon, Portugal, http://www.terena.nl/conferences/archive/tnc2000/proceedings/10A/10a3.pdf

[11] Stanislav Milanovic, Rifat Ramovic, Dimitrije Tjapkin, "Optimisation of Buffer Circuit's Characteristics Realized by the BiCMOS Technological Process", Proceedings of XXXVII Conference on Electronics, Telecommunications, Computers, Automation and Nuclear Engineering (ETRAN), Part IX, pp. 123-128, Belgrade, Yugoslavia,1993, http://galeb.etf.bg.ac.yu/~etran2001/istorija.htm

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

[13] St. Kent, R. Atkinson, "Security Architecture for the Internet Protocol"; RFC 2401, November, 1998.

[14] S. Blake, D. Black, M. Carlson, E. Davies, Z. Wang, W. Weiss, "An Architecture for Differentiated Services"; RFC 2475, December, 1998.

[15] Paul Ferguson, Geoff Huston, "Quality of Service: Delivering QoS on the Internet and in Corporate Networks", John Wiley & Sons, 1998.

[16] Xipeng Xiao, Lionel M. Ni, "Internet QoS: the Big Picture", Department of Computer Science, Michigan State University, 1999.

[17] T. Braun, M. Günter, I. Khalil, "Management of Quality of Service Enabled VPNs", IEEE Communications Magazine, May 2001.

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