VPN SOLUTION FOR ZOOMFINANCE.COM: TOWARD COST SAVING AND SECURITY EXERCISE

SIA SIE TUNG

UNIVERSITI UTARA MALAYSIA 2003

VPN SOLUTION
FOR ZOOMFINANCE.COM:
TOWARD COST SAVING AND SECURITY EXERCISE

A thesis submitted to the Graduate School in partial fulfilment of the requirements for the degree Master of Science (Information Technology) Universiti Utara Malaysia

by
Sia Sie Tung

Sekolah Siswazah
(Graduate School)
Universiti Utara Malaysia

PERAKUAN KERJA KERTAS PROJEK
(Certification of Project Paper)

Saya, yang bertandatangan, memperakukan bahawa
(I, the undersigned, certify that)

SIA SIE TUNG

calon untuk Ijazah
(candidate for the degree of) Sarjana Sains (Teknologi Maklumat)

telah mengemukakan kertas projek yang bertajuk
(has presented his/her project paper of the following title)

VPN SOLUTION FOR ZOOMFINANCE.COM : TOWARD COST SAVING AND SECURITY EXERCISE

seperti yang tercatat di muka surat tajuk dan kulit kertas projek
(as it appears on the title page and front cover of project paper)

bahawa kertas projek tersebut boleh diterima dari segi bentuk serta kandungan, dan meliputi bidang ilmu dengan memuaskan.
(that the project paper acceptable in form and content, and that a satisfactory knowledge of the field is covered by the project paper).

Nama Penyelia
(Name of Supervisor) : En. Muhammad Shakirin

Tandatangan
(Signature) :

Tarikh
(Date) : 22/5/2003

PERMISSION TO USE

In presenting this thesis in partial fulfillment of the requirements for a post graduate degree from Universiti Utara Malaysia, I agree that the University Library may make it freely available for inspection. I further agree that permission for copying of this thesis in any manner, in whole or in part, for scholarly purposes may be granted by my supervisor(s) or, in their absence, by the Dean of the Graduate school. It is understood that any copying or publication or use of this thesis or parts thereof for financial gain shall not be allowed without my written permission. It is also understood that due recognition shall be given to me and to Universiti Utara Malaysia for any scholarly use which may be made of any material from my thesis.

Requests for permission to copy or make other use of materials in this thesis, in whole or in part, should be addressed to:

Dean of Graduate School
Universiti Utara Malaysia
06010 UUM Sintok
Kedah Darul Aman

ABSTRAK

Pada masa kini banyak syarikat dan organisasi telah menggunakan Rangkaian Maya Persendirian (VPN) sebagai suatu penyelesaian yang mampu dalam mengurangkan kos dan membentuk persekitaran yang lebih selamat. Pasaran bagi VPN the berubah secara mendadak semenjak sepuluh tahun lepas di mana Internet telah berkembang dan semakin banyak syarikat telah menggunakannya sebagai satu kaedah untuk berkomunikasi. Laporan ini akan mendekati VPN sebagai suatu cara melayari sumber rangkaian persendirian melalui Internet secara selamat. Kemudian, saya akan membincangkan teknologi VPN yang telah digunakan pada masa kini di Internet. Ini termasuklah *tunneling, authentication, access control* dan sekuriti data. Selain itu, laporan ini juga akan melihat kepada rekabentuk dan topologi VPN. Untuk memasukkan unsur sekuriti VPN, saya akan membincangkan dan seterusnya mendirikan *firewall, encrypted data tunnel* dan juga *Intrusion Detection System (IDS).* Pada bahagian akhir keputusan dan peralatan percubaan juga akan dimasukkan selepas rekaan rangkaian baru dibentuk.

ABSTRACT

Many companies and organizations nowadays uses Virtual Private Network (VPN) as a solution, which enable them to save cost and create more secure environment. The VPN market has changed significantly in the past ten years as the Internet has grown and more companies have come to rely on it for communications. This report will look at VPN as a means of user to access private network resources securely over the Internet. Then I will look on the part of technologies for VPNs used today on the Internet including tunneling, authentication, access control and data security. Beside, this report will also including VPN architectures, and topologies. For integrated VPN security I will describe and setting up firewall, encrypted data tunnel and also Intrusion Detection System (IDS). Lastly, testing tools and result will be administered on the new configuration.

ACKNOWLEDGEMENT

This project is the result of a Master's project at Northern University of Malaysia (UUM) during the period November 2002 to April 2003.

I would like to take this opportunity to thank the following people for their valuable time and dedication that greatly helped me in my project. First of all to my supervisor, Mr. Muhammad Shakirin Shaari, for providing me with valuable advice since the inception of my project and also his guidance and attention in ensuring that my project was within the context of the chosen topic. Also to the executive manager of Zoomfinance for showing interest and becoming my project advisor.

Other people that I want to mention includes my dear friends and family for their great support. Thank you!

DECLARATION

I hereby declare that the thesis is based on my original work except for quotations and citations, which have been duly acknowledged. I also declare that it has not been previously or concurrently submitted for any other degree of UUM or other institutions.

.....

NAME: SIA SIE TUNG

DATE : 21 MEI 2003

DEDICATION

This thesis is dedicated to my family, with love.

TABLE OF CONTENTS	PAGES

LIST OF TABLES **PAGES**

LIST OF FIGURES PAGES

ABBREVIATIONS AND ACRONYMS

ACL	Access Control List
AH	Authentication Header
ATM	Asynchronous Transfer Mode
CGI	Common Gateway Interface
CHAP	Challenge Handshake Authentication Protocol
CIDF	Common Intrusion Detection Framework
CPE	Customer Premise Equipment
DES	Data Encryption Standard
DNS	Domain Name System
DOS	Deny of Service
DUN	Dialup Networking
ESP	Encapsulating Security Payload
FTP	File Transfer Protocol
FWTK	Firewall Toolkit
HQ	Headquarter
HTTP	Hypertext Transfer Protocol
IDS	Intrusion Detection System
IPSec	Internet Protocol Security
ISP	Internet Service Provider
L2TP	Layer Two Tunneling Protocol
LAN	Local Area Network
MPLS	Multi Protocol Label Switching
Nmap	Network Mapper
OC3	Optical Carrier 3
OS	Operating System
PAP	Password Authentication Protocol
PKI	Public Key Infrastructure
POP	Point of Presence
PPP	Point-to-Point Protocol

PPTP	Point-to-Point Tunneling Protocol
PSK	Pre-Shared Key
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RAS	Remote Access Server
SLA	Service level Agreements
SMTP	Simple Mail Transfer Protocol
SNA	System Networking Architecture
SSH	Secure Shell Protocol
SSL	Secure Socket Layer
TCP/IP	Transmission Control Protocol/Internet Protocol
TPM	Technology Park Malaysia
UDP	User Datagram Protocol
VPN	Virtual Private Network
WAN	Wide Area Network
WWW	World Wide Web

CHAPTER 1

INTRODUCTION

CHAPTER 1

INTRODUCTION

You're waiting to cross a crowded downtown street at night, when a long black limousine zooms past. Its darkened windows reflect neon signs, giving away nothing about who is inside or what they're doing. You can't help wondering what that sleek exterior hides: Diplomat? Crime boss? Movie star? The light changes, and the limo vanished into the night, leaving behind nothing but your speculations.

Translate that experience into the world of the Internet, and you can grasp what's cool about VPNs (Virtual Private Networks). Just as the limousine drives the public streets but keeps its contents private, a message sent via VPN travels the public Internet, but is encapsulated in encryption so that its content remains private. Only the originator and the receiver of the message see it in a clearly readable state. Any hacker trying to eavesdrop en route gets nothing but a scrambled mess. The path of a VPN message has "light" at each end but "darkness" (obscurity) at all the between-points, so it is called, metaphorically, a VPN tunnel.

In today's business world, the need for access to company data reaches beyond the walls of the office. The world has changed a lot in the last couple of decades. Instead of simply dealing with local or regional concerns, many businesses now have to think about global markets and logistics. Many companies have facilities spread out across the country or around the world, and there is one thing that all of them need: A way to maintain fast, secure and reliable communications wherever their offices are.

Where private business communications were once the privilege of the largest corporations, who could afford their own private networks, now VPN technology allows almost anyone with a computer and access to the Internet to send and receive data confidentially. VPNs are rapidly moving from merely being a trendy phrase, to being essential for wired business.

The contents of the thesis is for internal user only

References

1. Books and Journals

ADTRAN (2001), *A Technology Guide from ADTRAN: Understanding Virtual Private Networking*, September 2001.

Alan Zeichick (2002), *SnapGear Lite: An Inexpensive Home-Office/Small-Office Firewall and VPN Client*, Linux Journal, Vol 2002, Issue 96, April 2002.

Andrew G. Mason (2002), *Cisco secure Virtual Private Networks*, Cisco Pree, Indianpuls, USA.

Anonymous (2001), *Maximum Linux Security*, Second Edition, Sams Publishing, USA.

Barry Press & Marcia Press (2000), *Networking By Example,* Que Corporation, USA.

Bruce Perlmutter (2000), *Virtual Private Networking: A View from the Trenches*, Prentice Hall PTR, Upper Saddle River, New Jersey.

Configuring A VPN Solution, Microsoft Consulting Services Telecommunications Practice, 2000.

D. Brent Chapman & Elizabeth D. Zwicky (1995), *Building Internet Firewalls*, O'Reilly & Associates, Inc.

Douglas E. Comer (2001), *Computer Networks and Internets with Internet Applications*, Third Edition, Prentice Hall, New Jersey.

Eli Herscovitz (1999), *Secure Virtual Private Networks: The Future of Data Communications*, International Journal of Network Management, Int. J. Network Management.

Fairol Halim (2001), *The Effect of IT on Marketing Performance: The Case of Malaysian Companies*, Thesis Master of Business Administration, UPM, September 2001.

Graham P. Bell & David Kavanagh (1994), *Minimizing Risk in Your Wide Area Network Design,* Information Management & Computer Security, Volume 02, Number 2, pp. 26-28.

J.J. Gao & A.F. Lai (2000), *Redhat Linux 6.2, Chinese Edition*, Acore Publishing, Taipei, Taiwan.

John Mairs (2002), *VPNs: A Beginner's Guide*, McGraw-Hill, Berkeley, California, USA.

Jon Hall & Paul G. Sery (2001), *Redhat Linux 7 For Dummies*, IDG Books Worldwide, USA.

Khairol Najmy (2000), *Virtual Private Network: Architecture & Implementation*, UUM, Sintok.

Larry J. Hughes (1995), *Actually Useful Internet Security Techniques*, New Riders Publishing, Indiana.

Mairs, J. (2002), *VPNs: A Beginner's Guide*, McGraw Hill, Berkeley, California, USA.

Mark Merkow (1999), *virtual Private Networks for Dummies,* Foster City, IDG BOOKs Workwide.

Matthew Ramsay (2000), *PoPToP, a Secure and Free VPN Solution*, Linux Journal, Vol 2000, Issue 74es, June 2000.

McDysan, David E. (2000), *VPN Application Guide: Real Solution for Enterprise Networks*, Wiley Computer Publishing, Canada.

Niklas Ogren (2002), *Selecting/realization of Virtual Private Networks with Multiprotocol label Switching or Virtual Local Area Networks*, Master Thesis, Arrowhead, Solna.

Oleg Kolesnikov & Brian Hatch (2002), *Building Linux Virtual private Networks (VPNs)*, New Riders Publishing, Indiana, USA.

Ramon J. Hontanon (2001), *Linux Security*, Sybex Publishing, USA.

Richard Peterson (1998), *Linux: The Complete Reference*, Second Edition, McGraw-Hill, California, USA.

RSA Security Inc. (2002), *Implementing a Secure Virtual Private Network.* Avaiable at www.rsasecurity.com.

Ruixi Yuan & W. Timothy Strayer (2001), *Virtual Private Networks: Technologies and Solution*, Addison-Wesley, Upper Saddle River, New Jersey, USA.

Stephen Northcutt & Judy Novak (2002), *Network Intrusion Detection*, Third Edition, New Riders, USA.

Virtual Private Network Technologies: Definitions and Requirements, VPN Consortium, June 2002.

W.M. See (2002), *Redhat Linux 7.2*, Chinese Edition, Flag Publishing, Chinese Taipei, Taiwan.

2. Internet

http://cpmpnetworking.about.com/library/weekly/aa010701b.html

http://findvpn.com/providers/vpnware.cfm

http://firestarter.sourceforge.net/

http://umn.dl.sourceforge.net/sourceforge_/firestarter-0.8.3-1.i386rpm

http://www.cisco.com/warp/public/779/largeent/vpne/vpndocs/vpnhw.html

http://www.cites.uiuc.edu/vpn/security.html

http://www.corecom.com/html/vpn.html

http://www.howstuffworks.com/vpn.htm/printable)

http://www.idi.ntnu.no/~runhan/project/report-html/index.html

http://www.howstuffworks.com/vpn.htm

http://www.activsupport.com/network/vpn_security/vpn_faq.html

http://www.internetwk.com/VPN/paper.htm

http://www.nwfusion.com/news/2001/0307vpngp.html

http://www.snort.org/dl/binaries/linux/snort-1.9.1-/snort.i386.rpm

http://www.snort.org/dl/binaries/linux/snort-mysql-1.9.1-/snort.i386.rpm

http://www.snort.org/dl/contrib/data_analysis/acid/acid-0.9.6613.tar.gz

http://www.snort.org/dl/contrib/data_analysis/snortsnarf/snortsnarf-010108.1.tar.gz

http://www.ssimail.com/VPN_solutions.htm

http://www.sunworld.com/swol-06-1998/swol-06-ipsec.html

http://www.watchguard.com.

http://www.zoomfinance.com/