VIRTUAL PRIVATE NETWORKING

by

Khaleel ur Rehman

BAHRIA UNIVERSITY
~~MFN~~1109
Acc. No..........
T-0379
ISLAMABAD

Supervised

by

Mr. Fazal Wahab

A thesis submitted to the Department of Computer Sciences,

Bahria University, Islamabad.

In partial fulfillment of requirement for the degree of MCS.

Department of Computer Sciences
Bahria University, Islamabad

DEDICATION

To my family, friends and respected teachers.

ACKNOWLEDGEMENTS

First of all I would like to thank Almighty Allah for His blessings. I am very grateful to my family and friends, for their encouragement and motivation throughout the project. They have always been there for me. I am very grateful to my supervisor Mr. Fazal Wahab for his valuable advice and moral support.

Khaleel ur Rehman

CERTIFICATE

We accept the work contained in this report to the required standard for the partial fulfillment of the degree of MCS (Software Engineering).

Head of Department
Mr. Fazal Wahab

MFN
1109

Supervisor
Mr. Fazal Wahab

Shaftab Ah

Internal Examiner
Mr. Shaftab Ahmad

External Examiner
Prof. Dr. Irfan Zafar

ABSTRACT

Traditionally an organization that wanted to build a wide-area network needed to procure expensive, dedicated lines to connect their offices together. Only large companies could afford to purchase these lines outright, so most organizations "leased" their lines and paid a monthly charge, sometimes thousands of dollars, for the privilege of using cables that no one else could tap into.

A virtual private network (VPN) is the extension of a private network that encompasses links across shared or public networks like the Internet. A VPN enables you to send data between two computers across a shared or public internetwork in a manner that emulates the properties of a point-to-point private link. The act of configuring and creating a virtual private network is known as virtual private networking.

A VPN can support the same intranet/extranet services as a traditional WAN, but VPNs have also grown in popularity for their ability to support *remote access service*. In recent years, many organizations have increased the mobility of their workers by allowing more employees to telecommute. Employees also continue to travel and face an increasing need to stay "plugged in" to the company network.

TABLE OF CONTENTS

Dedication II

Acknowledgements III

Certificate IV

Abstract V

List of Figures X

1. Introduction 1~5

    1.1 Project Overview 2

    1.2 Introduction 2

    1.3 Present Communication Technology 3

    1.4 Reasons for New System 3

    1.5 Initial Investigation 4

2. Project Overview 6~23

    2.1 Basic VPN Requirements 7

    2.2 Tunneling Basics 8

    2.3 Tunneling Protocols 10

    2.4 How Tunneling works 10

    2.5 Tunneling Protocols and the Basic Requirements 11

        2.5.1 User Authentication 11

        2.5.2 Token Card Support 11

        2.5.3 Dynamic Address Assignment 11

        2.5.4 Data Compression 11

        2.5.5 Data Encryption 12

        2.5.6 Key Management 12

        2.5.7 Multi protocol Support 12

        2.5.8 Point-to-Point Protocol 12

    2.6 Phase 1: PPP Link Establishment 13

    2.7 Phase 2: User Authentication 13

        2.7.1 Password Authentication Protocol 13

        2.7.2 Challenge Handshake Authentication Protocol 14

2.7.3 Microsoft Challenge Handshake Authentication Protocol 14

2.7.4 MS-CHAP v2 15

2.8 Phase 3: PPP Callback Control 15

2.9 Phase 4: Invoking Network Layer Protocol(s) 16

2.10 Data Transfer Phase 16

2.10.1 Point-to-Point Tunneling Protocol 16

2.10.2 Layer Two Point Tunneling Protocol 17

2.10.3 Internet Protocol Security Tunnel Mode 18

2.11 Tunnel Types 19

2.11.1 Voluntary Tunneling 19

2.11.2 Compulsory Tunneling 20

2.12 Feasible Protocols 21

2.12.1 PPTP Compared to L2TP/IPSec 21

2.12.2 Advantages of L2TP/IPSec over PPTP 22

2.12.3 Advantages of PPTP over L2TP/IPSec 22

2.13 Proposed Protocol 23

3. Network Security 24~41

3.1 Network Security Overview 25

3.2 Network Security Threats 25

3.2.1 Unstructured Threats 25

3.2.1 Structured Threats 26

3.2.1 External Threats 26

3.2.1 Internal Threats 26

3.3 Network Attacks 26

3.3.1 Reconnaissance Attacks 26

3.3.2 Access Attacks 27

3.3.3 DoS Attacks 28

3.4 Network Security as a Continuous Process 28

3.4.1 Symmetric vs. Asymmetric Encryption 31

3.4.1.1 Automatic Key Management 32

3.4.1.1.1 Key Generation 32

3.4.1.1.2 Key Lengths 32

3.4.1.1.3 Dynamic Re-Keying 32

3.4.2 Certificates 33

3.4.3 Extensible Authentication Protocol 34

3.4.3.1 EAP Infrastructure 35

3.4.3.1.1 EAP-MD5 CHAP 35

3.4.3.1.2 EAP-RADIUS 35

3.4.3.1.3 Transport Level Security 36

3.4.4 Negotiated Security Association 36

3.4.4.1 Security Associations 37

3.4.4.2 Key Exchange 38

3.4.4.3 Key Information Exchange 39

3.4.4.3.1 Authentication 39

3.4.4.3.2 Data Protection 39

3.4.4.3.3 SA Lifetimes 40

3.4.4.3.4 Authentication Header 41

3.4.4.3.5 Encapsulating Security Payload 41

4. Proposed System 42~44

4.1 Proposed System Overview 43

5. VPN Deployment 45~68

5.1 VPN Clients 46

5.2 VPN-Capable Microsoft Operating Systems 46

5.2.1 Design Points: Configuring the VPN Client 47

5.3 VPN Server 48

5.3.1 Design Points: Configuring the VPN Server 50

5.4 Deploying L2TP-Based Remote Access 53

5.4.1 Deploying Certificate Infrastructure 53

5.4.1.1 Deploying Computer Certificates 54

5.4.1.2 Deploying User Certificates 55

5.4.2 Deploying Internet Infrastructure 55

5.4.2.1 Placing VPN Server in Perimeter Network 56

5.4.2.2 Installing Windows 2000 Server on VPN Servers 56

5.4.2.3 Adding Address Records to Internet DNS 56

5.4.3 Deploying AAA Infrastructure 57

5.4.3.1 Configuring Active Directory for user accounts 57

5.4.3.2 Configuring the Primary IAS Server 57

5.4.3.3 Configuring the Secondary IAS Server 59

5.4.4 Deploying VPN Servers 59

5.4.4.1 Configuring VPN Server connection to Internet 59

5.4.4.2 Running the Routing and Remote Access Server 59

5.4.5 Intranet Network Infrastructure 61

5.4.5.1 Configuring Routing on the VPN Server 61

5.4.5.2 Verifying Name Resolution and Reachability 61

5.4.5.3 Configuring Routing for Off-Subnet Pools 61

5.4.6 Deploying VPN Clients 62

5.4.6.1 Manually Configuring VPN Clients 62

6. Conclusion 69~70

Bibliography 71~72

LIST OF FIGURES

Figure 2.1 Tunneling 9

Figure 2.2 Structure of a PPTP packet containing user data 17

Figure 2.3 Structure of an L2TP packet containing user data 17

Figure 2.4 Encryption of an L2TP packet with IPSec ESP 18

Figure 3.1 Security Wheel 29

Figure 4.1 Proposed Network Layout 44

Figure 5.1 The VPN Server in front of the Firewall 63

Figure 5.2 The VPN Server behind the Firewall 65

Figure 5.3 The VPN Server between two Firewalls 68