

TESIS APPROVAL STATUS FORM

JUDUL: SIMPLE FIREWALL

SESI PENGAJIAN: 01/04

Saya MOHD AZAHA ABDUL GHANI


mengaku membenarkan tesis (PSM/Sarjana/Doktor Falsafah) ini disimpan di Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dengan syarat-syarat kegunaan seperti berikut:


1. Tesis adalah hakmilik Kolej Universiti Teknikal Kebangsaan Malaysia.
2. Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dibenarkan membuat salinan untuk tujuan pengajian sahaja.
3. Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dibenarkan membuat salinan tesis ini sebagai bahan pertukaran antara institusi pengajian tinggi.
4. ** Sila tandakan (/)

_____ SULIT (Mengandungi maklumat yang berdarjah keselamatan atau kepentingan Malaysia seperti yang termaktub di dalam AKTA RAHSIA RASMI 1972)

_____ TERHAD (Mengandungi maklumat TERHAD yang telah ditentukan oleh organisasi/badan di mana penyelidikan dijalankan)

 / TIDAK TERHAD


(MOHD AZAHA ABDUL GHANI)


(PN NURUL AZMA ZAKARIA)

Alamat tetap : NO 19 JALAN IM 5/6
INDERA MAHKOTA
KUANTAN PAHANG

Tarikh : 20/10/04

Tarikh : 20/10/2004

CATATAN: ** Jika tesis ini SULIT atau TERHAD, sila lampirkan surat daripada pihak berkuasa.
Tesis dimaksudkan sebagai Laporan Projek Sarjana Muda (PSM)

raf

TK5105.59 .M39 2004



0000037000

Simple firewall system / Mohd Azaha Abdul Ghani.

SIMPLE FIREWALL SYSTEM

MOHD AZAHA B. ABDUL GHANI

**This report is submitted in partial fulfillment of the requirements for the
Bachelor of Information Technology and Communication in Networking**

**FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY
NATIONAL TECHNICAL UNIVERSITY COLLEGE OF MALAYSIA
2004**


ADMISSION

I admitted that this project title name of

SIMPLE FIREWALL SYSTEM

is written by me and is my own effort and that no part has been plagiarized without
citations.

STUDENT

: 

(MOHD AZAHA B. ABDUL GHANI)

Date

: 20/10/04

SUPERVISOR

: 

(PN NURUL AZMA BT ZAKARIA)

Date

: 20/10/04

DEDICATION

First and foremost, I would like to say Alhamdulillah to the almighty Allah S.W.T for without His blessings and guidance, this thesis would not be completed in time. Not to forget, thank you to my parents for believe in every and single thing that I'm doing.

ACKNOWLEDGEMENTS

I would like to thank Madam Nurul Azma Zakaria for giving assistant to complete this project successfully for his time, support, an encouragement for this project.

To my parent Abdul Ghani Jaafar and Maznah Abdullah give me strength and support until I finish this thesis.

I do thanks also to all my roommates and classmates, Ludin, Kamil, Starman, Che Din, Rizul and especially to my beloved fiance Rida for her patience, encouragement, support and love throughout the completion of this thesis

ABSTRACT

Since the Internet has become popular since 1980, it has been used by most people as a platform to gain knowledge. In term of business strategy, the information web site is one of the ways to get easy in work. This is because World Wide Web is universal where anyone can use it anywhere. With Internet user is estimated about 30 million user, the Internet is the world largest computer network. Security is one of the most important building blocks of internetworking world today. As reflect to that, this **Simple Firewall system** is specifically prototyped, configured and implemented to make a Local Area Network (LAN) more secure. There are many Firewalls available in market nowadays such as WatchGuard offered by multinational computer Hardware Company like 3COM and Dlink. However these devices tend to be expensive for small organizations. The system device can give organizations more options in implementing the secured internetworking on their environment. Once the above prototype system proves economically viable and goes through the process of production, it will be a tiny, configurable device connecting small organizations' network to its ISP. Such product, manufactured in large amount may prove to be even less than RM 2000.

TABLE OF CONTENTS

TITLE	PAGE
ADMISSION	iii
ACKNOWLEDGEMENT	v
ABSTRACT	vi
TABLE OF CONTENTS	vii
LIST OF FIGURE	xi
LIST OF TABLE	xii
ACRONYMS	xiii
CHAPTER I INTRODUCTION	
1.1 Introduction	1
1.1.1 Problem Statement	2
1.1.2 What Is Firewall	3
1.1.3 Why Used Firewall	5
1.1.4 Why Develop Firewall	7
1.2 Project Objective	8
1.3 Project Scope	9
1.4 Project Advantage	10
1.5 Conclusion	10
CHAPTER II LITERATURE REVIEW	
2.1 Introduction	11
2.1.1 Conceptual Overview	13
2.2 Firewall Application	14
2.3 Case Study	15
2.4 Research Overview in Firewall Application	17
2.5 Conclusion	13

CHAPTER III PROJECT METHODOLOGY AND DEVELOPMENT

3.1	Introduction	20
3.2	Project Methodology	21
3.2.1	Prototype Evolution	22
3.3	Methodology Justification	24
3.3.1	Advantage Of Prototyping	25
3.3.2	Disadvantage Of Prototyping	26
3.4	Hardware and Software Needs	27
3.4.1	Hardware Needs	27
3.4.2	Software Needs	28
3.4.3	Network Needs	29
3.5	Conclusion	29

CHAPTER IV ANALYSIS REVIEW

4.1	Introduction	30
4.2	Business Study	31
4.2.1	Firewall Protection	32
4.3	Problem Analysis	33
4.4	Analysis Requirement	34
4.4.1	Business Requirement	35
4.4.2	Software Requirement	35
4.4.3	Hardware Requirement	35
4.4.5	Network Requirement	36
4.4.6	Implementation Requirement	36
4.5	Conclusion	36

CHAPTER V DESIGN

5.1	Introduction	37
5.2	Preliminary/High-Level Design	38
5.2.1	Raw Data	38

5.3	System Architecture	40
5.4	System Design	41
5.4.1	Context Diagram	41
5.4.2	Data Flow Diagram	42
5.5	User Interface Design	42
5.5.1	Physical Design	43
5.5.2	Input Output Specification	44
5.6	Security Requirement	47
5.7	Conclusion	48

CHAPTER VI IMPLEMENTATION

6.1	Introduction	49
6.1.1	Setup A Priority	50
6.1.2	Run The Rule	50
6.2	Software Configuration Management	51
6.2.1	Configuration Environment setup	51
6.3	Hardware Configuration Management	52
6.3.1	Hardware Setup	52
6.4	Development Status	53

CHAPTER VII TESTING

7.1	Introduction	54
7.2	Test Plan	55
7.2.1	Test Organization	57
7.2.2	Test Environment	58
7.2.3	Test Schedule	59
7.3	Test Strategy	60
7.3.1	Type of Tests.	60
7.4	Test Design	62
7.4.1	Test Description	62
7.4.2	Test Data	63
7.5	Test Case Result	65

7.6	Conclusion	67
-----	------------	----

CHAPTER VIII CONCLUSION

8.1	Weaknesses and Strengths	68
8.1.1	Weaknesses	68
8.1.2	Strengths	69
8.2	Propositions for improvement	70
8.3	Conclusion	72

BIBLIOGRAPHYS	73
----------------------	----

APPENDIXES	74
-------------------	----

LIST OF FIGURE

Figure 1.1	Hardware Firewall	4
Figure 1.2	Computer with Firewall Software	4
Figure 2.1	Scheme of a firewall	13
Figure 3.1	Steps involved in Prototyping Method	23
Figure 5.1	Context Diagram of Simple Firewall	41
Figure 5.2	Data Flow Diagram of Simple Firewall	42
Figure 5.3	Physical Design	43
Figure 5.4	Picture Main Frame Input Output	45
Figure 5.5	Picture Menu Frame Input Output	46

LIST OF TABLE

Table 2.1	Firewall Product	16
Table 5.1	Main Frame Raw Data	39
Table 5.2	Menu Frame Raw Data	40
Table 5.3	Main Frame Input Output	44
Table 5.4	Menu Frame Input Output	46
Table 6.1	Development Status	53
Table 7.1	Test Cycles and Duration Table	59
Table 7.2	List of Test	63
Table 7.3	List of Testing at Keeping Data	64
Table 7.4	List of Testing at Save or Load	64
Table 7.5	List of Testing at Run Rule	65
Table 7.6	Test Case Result	66

ACRONYMS

***IP* - Internet Protocol**

This is the core protocol used for transporting virtually all information across the internet; most other protocols (including the ones which follow) use this as their underlying communication layer.

***ICMP* - Internet Control Message Protocol**

This protocol is used for passing connection and control information across the net. It's what is used when ping to another computer or use trace route to see where problems are occurring on the net.

***DNS* – Domain Name System**

The Domain Name System (DNS) is a distributed internet directory service. DNS is used mostly to translate between domain names and IP addresses, and to control email delivery. Most internet services rely on DNS to work. If DNS fails or is too slow, web sites cannot be located and email delivery stalls.

***UDP* - User Datagram Protocol**

Provides unreliable unidirectional packet transmission. Basically, a data packet is sent but whether or not it is received is not reported and no retransmission is attempted by this protocol. This may seem silly, but on a reliable network where the overwhelming majority of packets get through, this can greatly increase throughput because of the lower overhead required in sending a packet this way. Even though UDP is not as popular as TCP, common services on many computers are available using either TCP or UDP.

TCP - Transmission Control Protocol

Provides a reliable bidirectional connection between two computers, will deliver the packet, or let we know it failed. This is the primary work horse of high level internet information transfer, though it is much less efficient than UDP.

NAT – Network Address Translation

The Network address translation allows using any address space for the internal network. Using a private (RFC-1918) address space that is not routed on the Internet provides an additional level of security as well. For NAT to know how to route traffic must be first define the internal and external interfaces in the NAT Configuration Applet.

INTRANET (Hosts)

Intranet host objects identify internal hosts for applying Firewall policy and VPN access control. This enables the Firewall Policy and VPN Access Control lists to control traffic to and from these hosts. Viewing, editing and adding Intranet hosts and host ranges is done from the Intranet tab of the Security Policy Configuration window. An Intranet host object can define an individual host or a range of hosts. The two default Intranet host definitions include the Broadcast Host, which defines all broadcast traffic and Others, which represents all Intranet hosts and Intranet host ranges that are not explicitly defined

Firewall Policy

Firewall incorporates an advanced static packet filtering technique that maintains a state table for all connections. Only expected responses to active state table entries that are permitted by firewall policy or initiation requests permitted by firewall policy are allowed through the firewall.

TCP Packet

TCP (Transmission Control Protocol) is a set of rules (protocol) used along with the Internet Protocol (IP) to send data in the form of message units between computers over the Internet. While IP takes care of handling the actual delivery of the data, TCP takes care of keeping track of the individual units of data (called packets) that a message is divided into for efficient routing through the Internet.

TCP is known as a connection-oriented protocol, which means that a connection is established and maintained until such time as the message or messages to be exchanged by the application programs at each end have been exchanged. TCP is responsible for ensuring that a message is divided into the packets that IP manages and for reassembling the packets back into the complete message at the other end. In the Open Systems Interconnection (OSI) communication model, TCP is in layer 4, the Transport Layer.

UDP Packet

UDP is an unreliable protocol where no attempt is made to keep track of packets as to being in a sequence, order, or verify that they were received. Checks are made to see if the packet appears to be the same packet transmitted by evaluation of a checksum and comparison to the packets checksum. These packets are dropped if the destination calculations of the checksum differ from the packets claimed checksum

ICMP Packet

ICMP stands for the Internet Control Message Protocol, and it was designed to send control messages between routers and hosts. For example, an ICMP packet may be sent when a router is experiencing congestion or when a destination host is unavailable.

An ICMP packet has a slightly different structure than we've seen before. An ICMP header follows the IP header in an IP packet, but it is not considered to be a Layer 4 header like TCP or UDP. Instead, ICMP is considered to be an integral part of IP; in fact, every vendor's implementation of IP is required to include ICMP.

CHAPTER I

INTRODUCTION

The rapid growth of interest in the Internet and the Windows operating system, network security has become a major concern to companies throughout the world. The fact that the information and tools needed to penetrate the security of corporate networks are widely available has only increased that concern.

Because of this increased focus on network security, network administrators often spend more effort protecting their networks than on actual network setup and administration. New tools that probe for system vulnerabilities, such as the Security Administrator Tool for Analyzing Networks (SATAN), assist in these efforts, but these tools only point out areas of weakness instead of providing a means to protect networks. Thus, network administrators are constantly trying to keep abreast of the wide number of security issues confronting in today's world.

1.1.1 Problem Statement

Today, most of people in the world use internet. User used internet for their business and communication.

When connect from private network to the Internet, user are physically connecting the network to well over 50,000 unknown networks and all of their users. While such connections open the door to many useful applications and provide great opportunities for information sharing, most private networks contain some information that should not be shared with outside users on the Internet. In addition, not all Internet users are involved in lawful activities. These two statements foreshadow the key questions behind most security issues on the Internet:

- How do protect confidential information from those who do not explicitly need to access it?
- How do protect the network and its resources from malicious users and accidents that originate outside of the network?

User need firewall if user computer's files need to be accessed remotely across the Internet, user are operating any sort of Internet server such as Personal Web Server, user use any sort of Internet-based remote control or remote access program such as PC Anywhere, user want to properly and safely monitor Internet connection for intrusion

attempts and if user want to preemptively protect themselves from compromise by "inside the wall" Trojan horse programs like NetBus and Back Orifice.

1.1.3 What Is Firewall

A computer firewall protects networked computers from intentional hostile intrusion that could compromise confidentiality or result in data corruption or denial of service. It may be a hardware device (see Figure 1) or a software program (see Figure 2) running on a secure host computer. In either case, it must have at least two network interfaces, one for the network it is intended to protect, and one for the network it is exposed to. A network firewall sits at the junction point or gateway between the two networks, usually a private network and a public network such as the Internet. The earliest computer firewalls were simple routers. The term "firewall" comes from the fact that by segmenting a network into different physical sub networks, they limited the damage that could spread from one subnet to another - just like fire doors or firewalls.

Figure 1.1 Hardware Firewall

Hardware firewall providing protection to a Local Network

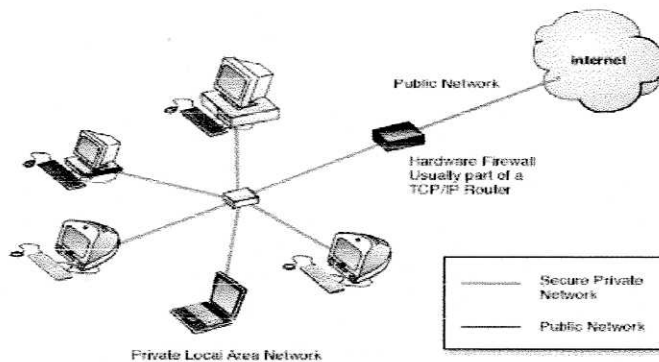
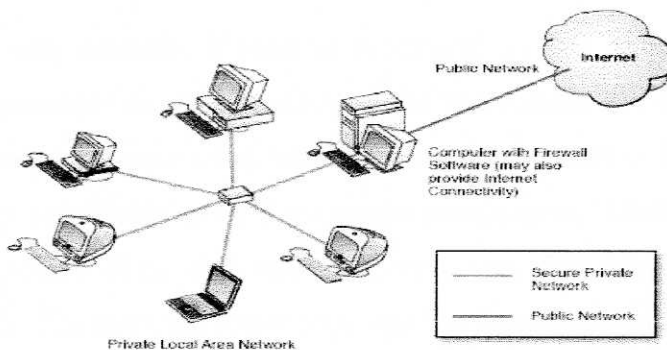


Figure 1.2 Computers with Firewall Software

Computer running firewall software to provide protection



An Internet firewall examines all traffic routed between your network and the Internet to see if it meets certain criteria. If it does, it is routed between the networks, otherwise it is stopped. A network firewall filters both inbound and outbound traffic. It can also manage public access to private networked resources such as host applications. It can be used to log all attempts to enter the private network and trigger alarms when

hostile or unauthorized entry is attempted. Firewalls can filter packets based on their source, destination addresses and port numbers. This is known as address filtering. Firewalls can also filter specific types of network traffic. This is also known as protocol filtering because the decision to forward or reject traffic is dependant upon the protocol used, for example HTTP, ftp or telnet. Firewalls can also filter traffic by packet attribute or state.

1.1.3 Why Use Firewall

Until very recently, if used an occasional dial-up connection to the internet, it was not unreasonable to just take a few minor precautions and not worry about security, though of course for those of us with full time connections at least a primitive firewall was generally considered to be a minimum requirement. Most people could get away with this by virtue of the fact that there were very few people on the net (relatively speaking) who had both the knowledge and the inclination to break into other peoples computers, and when they did go after someone, it was usually a large and/or high profile company, so for the rest of us, we were safe by virtue of being small and not worth their time. Today this has all changed, the few who have the skills now put their knowledge into automated programs and shell scripts which can be used to scan for security holes and attack many computers simultaneously. What's worse, once a system is breached they can put that computer to work scanning for openings and attacking more computers. The situation was bad enough at this point, but they went one step

further and started using the internet to distribute the attack programs they had created, so that anyone who wanted to could attack other computers. This created the "script kiddies" phenomenon which is basically thousands of bored children (or childish adults) who lack the expertise to be any kind of a threat, using software downloaded from the internet to implement broad scale attacks against anyone and everyone on the net. Because of this new approach, no one connected to the net is safe at any time, since the entire internet is continuously being scanned for insecure systems from many different sources. It is probably a rare computer IP address which does not get probed for security holes at least once a week.

There are many communication protocols used for passing information over the internet, some are for local communication such as Ethernet and various modem protocols, used to relay information between directly connected computers. Layered on top of these low level communication protocols are higher level ones which are used to relay information across the many different interconnected computers and devices which make up the internet. The most important protocols are:

- ***IP*** - Internet Protocol
- ***ICMP*** - Internet Control Message Protocol
- ***UDP*** - User Datagram Protocol
- ***TCP*** - Transmission Control Protocol

While these higher level protocols are the primary means by which useful information is passed across the internet (such as email and web pages), there are many other protocols available as well, but since they are usually rather specialized and rarely used (relatively speaking), there is little point in dealing with them further at this point.

1.1.4 Why Develop Firewall

As hacking attacks and cyber crime incidents continue to increase, many companies are extremely interested in getting insights on the measures their enterprises should take to secure corporate networks. The firewall market has bucked the slowdown in IT spending experienced by the rest of the industry in the first half to 2001. The firewall is the healthy and growing segment in IT market. The Internet is now a critical part of corporate networks, and Internet downtime can cause lost productivity and revenue. The explosion of e-commerce and the growth of the mobile workforce have significantly increased security challenges for the enterprises. Firewall vendors continue to add new features to their products as they compete to solve the increasingly complex problems of securing connections to the Internet, Intranets and Extranets. The following statistics published by International Data Corporation shows how rapidly firewall market is growing up in recent years.

According to International Data Corporation (IDC), the worldwide firewall market will create at least US \$1.6 billion in revenues this year, and that figure could go up to US \$2.1 billion. IDC is predicting that the market will not approach the saturation point at least for another four years, and meanwhile 50 % of large business, 41% of medium-sized businesses and 14% of small businesses in the United States will have firewalls installed. The U.S. is the largest firewall market, which claimed almost 61% of worldwide revenue in 2000. (www.advisor.com)

According to ITSecurity.com, worldwide firewall revenue totaled \$1.7 billion in 2001, and is forecasted to reach \$3.8 billion in 2005

1.2 Project Objective

The Goal of this project is to implement Different Firewall and develop a system to evaluate, compare and test different firewalls on architecture. Depending on the result from the tests and research, design a Firewall for Company's Network, as per its security requirements.

Objective of this system is:

- To make sure this system is fully automatic, have little or no customer configuration for novice user and insufficient button access to block and allow all protocol.
- Non-intrusive installation, the system should not change system programs or install shim and use system features-avoid protected-mode drivers.
- Application and service specific authorization to communicate with one time or for all time and automatically detected at each attempt.
- Provide specific socket enable
- Should be configurable and able to be monitored by another application such as the proposed system hardening tool.