Acc : 37698

THESIS APPROVAL STATUS FORM

JUDUL: PACKET FILTERING FIREWALL

SESI PENGAJIAN: 20004/2005

Saya MUHAMMAD SYAIFUL RIZA B MUHAMAD RAZI

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	

(TANDATANGAN PENULIS)

Alamat tetap : 1447, Jln Mawar 6,
Tmn Sultan Badlishah, Jln Pegawai
05050, Alor Star, Kedah Darul Aman

Tarikh : 23/10/2004

(TANDATANGAN PENYELIA)

EN. SHEKH FAISAL B. ABD. LATIP

Tarikh: 23/10/2004

PACKET FILTERING FIREWALL

MUHAMMAD SYAIFUL RIZA B MUHAMAD RAZI

This report is submitted in partial fulfillment of the requirements for the Bachelor of Information Technology and Communication (Computer Networks)

FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY
KOLEJ UNIVERSITI TEKNIKAL KEBANGSAAN MALYSIA
2004

ADMISSION

I admitted that this project title name of

PACKET FILTERING FIREWALL

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

STUDENT : ______________________ Date: 23 OCT 2004
(MUHAMMAD SYAIFUL RIZA B MUHAMAD RAZI)

SUPERVISOR: ______________________ Date: 23 OCT 2004
(MR. SHEKH FAISAL B ABDUL LATIP)

ACKNOWLEDGEMENT

Alhamdulillah, thank to Allah. This project (PSM) would not have been possible without the help of many people who had been very kind in giving their valuable advice and encouragement.. First and foremost, I would like to say a big thank you to my supervisor, Mr. Shekh Faisal bin Abdul Latip for his support, encouragement, advice and not to forget, patience throughout the entire project. His excellent supervision is one of the main reasons for the success of the Projek Sarjana Muda 1 (PSM1) and Projek Sarjana Muda II (PSMII).

Last but not least, I would like to take this opportunity to thank my beloved family and friends for their encouragement and help that was so meaningful to me throughout this project. I would like to thank my Dad, Mum and my beloved brothers for all their support. A very big thank you also goes all of my housemates, course mates and members of the Fakulti Teknologi maklumat dan Komunikasi (FTMK) Kolej Universiti Teknikal Kebangsaan Malaysia (KUTKM)

ABSTRACT

The main goal of this project is to design for fulfilling a condition set to qualify a Bachelor of Information Technology and Communication. The concept packet filtering firewall is the same like the packet filtering router technology. This system will filter the packets including with blocking and allowing the packets. The objective and scope on developing a Packet Filtering Firewall is to upgrade the security in LAN (Local Area Network) environment and easier for user to manage the security in LAN environment. The methodology during develop this utility is referred to the waterfall method that one of the SDLC. This method is use because it has a suitable phase that match with the PSM timeline and the system requirement to be developed. The software requirement is to develop on Microsoft Visual C++. Each student must complete PSM 1 before continuing with PSM 2. Students must give out the purpose project in this report as set the idea how to develop the real project in PSM 2. In PSM 2, students will develop a real project such as was proposed in PSM 1. PSM 2 is a project challenging which it will determine whether a successful project and usage testing will be done to define it will fulfill user's requirement. The usage this application does not means the current technology is not expedient any more in organization; it is just an alternative in networking.

ABSTRAK

Matlamat utama projek ini adalah untuk memenuhi syarat kelayakan bagi pengijazahan kursus Ijazah Sarjana Muda Teknologi Maklumat dan Komunikasi (Rangkaian Komputer) (BITC). Konsep yang diperkenalkan dalam packet filtering firewall sama seperti packet filtering technology. Sistem ini akan menghalang packet keluar dan masuk serta membenarkan dan menghalang kesemua packet. Objektif dan skop terhadap Packet Filtering Firewall adalah untuk meningkatkan konsep keselamatan di dalam persekitaran LAN (Local Area Network) dan memudahkan pengguna untuk mengawal dan mentadbir keselamatan melalui persekitaran LAN sahaja. Kaedah kajian semasa membangun kemudahan ini merujuk kepada kaedah Model air terjun yang digunakan didalam SDLC. Kaedah ini dipratikkan kerana mempunyai fasa yang bersesuaian dan serasi dengan garis panduan yang telah ditetapkan di dalam PSM dan keperluan pembangunan sistem. Perisian Microsoft Visual C++ digunakan bagi tujuan pembangunan sistem. Setiap pelajar dikehendaki mengambil PSM 1 sebelum lulus untuk menyambung PSM 2. Pelajar juga hendaklah menyertakan sebab utama pemilihan projek di dalam laporan yang hendak diserahkan kepada pihak fakulti, dimana laporan ini menwakili idea para pelajar terhadap projek yang sebenar didalam PSM 2. sememangnya PSM 2 merupakan satu projek yang benar-benar menduga kewibawaan para pelajar BITC. Kejayaan projek ini dapat dilihat sekiranya ianya dapat beroperasi disamping memenuhi keperluan pengguna. Aplikasi projek ini tidak bermaksud teknologi pada masa kini tidak beroperasi dengan baik tetapi ianya hanya sebagai alternatif lain dalam dunia rangkaian.

TABLE OF CONTENTS

TITLES **PAGES**

PROJECT METHODOLOGY AND PLANNING

ANALYSIS REVIEW

FIREWALL DESIGN

IMPLEMENTATION

TESTING

CONCLUSION

LIST OF FIGURE

LIST OF TABLE

LIST OF APPENDIX

ACRONYM

1. KUTKM	Kolej Universiti Teknikal Keb Malaysia
2. PSM	Projek Sarjana Muda
3. SNMP	Simple Network Management Protocol
4. LAN	Local Area Network
5. NT	New Technology
6. PC	Personal Computer
7. ICT	Information Communication Technology
8. IP	Internet Protocol
9. TCP	Transmission Communication Protocol
10. NMS	Network Management System
11. IT	Information Technology
12. CRC	Critical Request Check
13. PPP	Peer to Peer Protocol
14. ATM	Asynchronous Transfer Mode
15. WAN	Wide Area Network
16. MIB	Management Information Base
17. HTTP	Hyper Text Transfer Protocol
18. SSH	Secure Shell
19. HDLC	High-level Data Link Control
20. UTP	Unshielded Twisted Pair
21. HMP	Host Monitoring Protocol
22. ICMP	Internet Control Message Protocol
23. SDLC	System Development Life Cycle
24. FTP	File Transfer Protocol
25. UDP	User Datagram Protocol
26. NIC	Network Interface Card
27. Dos	Denial Of Service
28. MAC	Media Access Control

CHAPTER I

INTRODUCTION

The firewall has been known since the internet problem and computer crime is identified. It works as a wall to block incoming packet into the network. Firewall filters the TCP/IP and ICMP packets and act as a medium form internet to a network. There is two type of firewall (hardware and software).

The project is to build up the firewall software for server site. The firewall build using the object oriented programming (Visual C++). The firewall software build is using the basic of the packet filtering method which only blocks the inbound and outbound TCP/IP and ICMP packets. The implementation of this firewall is using Application Program Interface (API) method and the API-socket is suitable for the Windows platform. With this packet filtering type of firewall the server incoming and outgoing packets transfer is safe.

The purpose of this firewall is to protect the computer manipulate form hackers and crackers and improving the security level of an organization. This firewall is usually generated with the rule-set which can be altered by the administrator.

1.2 ISSUES AND PROBLEMS WITH FIREWALLS

A firewall cannot control anything which happens after a user has passed authentication and access check. This packet filtering firewall is block and allow TCP/IP and ICMP packet only.

Many of users are not familiar with the functionality of the packet filtering firewall because of the complicated and lot of condition use to block and allow. The complicated may cause a problem using the packet filtering firewall.

Some of the firewall not included with port scan utility. The port scan is important to assist user in defining the firewall rule-set. The port scan used to scan for the open port in the system and server. Without the port scan the user maybe forgotten which port is open and which is close. This problem will cause miss-configuring in the firewall rule-set and allowed the hackers and crackers burst into the system.

Given these benefits to the firewall approach, there are also a number of disadvantages, and there are a number of things that firewalls cannot protect against. A firewall is not by any means a panacea for Internet security problems.

1.2.1 Restricted Access to Desirable Services

The most obvious disadvantage of a firewall is that it may likely block certain services that users want, such as TELNET, FTP, X Windows, NFS, etc. However, these disadvantages are not unique to firewalls; network access could be restricted at the host level as well, depending on a site's security policy. A well-planned security policy that balances security requirements with user needs can help greatly to alleviate problems with reduced access to services.

Some sites may have a topology that does not lend itself to a firewall, or may use services such as NFS in such a manner that using a firewall would require a major restructuring of network use. For example, a site might depend on using NFS and NIS across major gateways. In such a situation, the relative costs of adding a firewall would need to be compared against the cost of the vulnerabilities associated with not using a firewall, i.e., a risk analysis, and then a decision made on the outcome of the analysis. Other solutions such as Kerberos may be more appropriate this solutions carry their own disadvantages as well [3] contains more information on Kerberos and other potential solutions.

1.2.2 Large Potential for Back Doors

Secondly, firewalls do not protect against back doors into the site. For example, if unrestricted modem access is still permitted into a site protected by a firewall, attackers could effectively jump around the firewall [1]. Modem speeds are now fast enough to make running SLIP (Serial Line IP) and PPP (Point-to-Point Protocol) a SLIP or PPP connection inside a protected subnet is in essence another network connection and a potential backdoor.

1.2.3 Little Protection from Insider Attacks

Firewalls generally do not provide protection from insider threats. While a firewall may be designed to prevent outsiders from obtaining sensitive data, the firewall does not prevent an insider from copying the data onto a tape and taking it out of the facility. Thus, it is faulty to assume that the existence of a firewall provides protection from insider attacks or attacks in general that do not need to use the firewall. It is perhaps unwise to invest significant resources in a firewall if other avenues for stealing data or attacking systems are neglected.

1.2.4 Other Issues

Other problems or issues with firewalls are as follows:

a) WWW, gopher

Newer information servers and clients such as those for World Wide Web (WWW), gopher, WAIS, and others were not designed to work well with firewall policies and, due to their newness, are generally considered risky. The potential exists for data-driven attacks, in which data processed by the clients can contain instructions to the clients; the instructions could tell the client to alter access controls and important security-related files on the host.

b) MBONE

Multicast IP transmissions (MBONE) for video and voice are encapsulated in other packets; firewalls generally forward the packets without examining the packet contents. MBONE transmissions represent a potential threat if the packets were to contain commands to alter security controls and permit intruders.

c) Viruses

Firewalls do not protect against users downloading virus-infected personal computer programs from Internet archives or transferring such programs in attachments to e-mail. Because these programs can be encoded or compressed in any number of ways, a firewall cannot scan such programs to search for virus signatures with any degree of accuracy. The virus problem still exists and must be handled with other policy and anti-viral controls.

d) Throughput

Firewalls represent a potential bottleneck, since all connections must pass through the firewall and, in some cases, be examined by the firewall. However, this is generally not a problem today, as firewalls can pass data at T1 (1.5 Megabits/second) rates and most Internet sites are at connection rates less than or equal to T1.

e) All eggs in single basket

A firewall system concentrates security in one spot as opposed to distributing it among systems. A compromise of the firewall could be disastrous to other less-protected systems on the subnet. This weakness can be countered; however, with the argument that lapses and weaknesses in security are more likely to be found as the number of systems in a subnet increase, thereby multiplying the ways in which subnets can be exploited.

1.3 FEATURES

- User can Block all Traffic (IP, TCP and ICMP packets) and can allow all traffic threw on mouse click
- User can add customaries rule-set to this firewall for the requirements of the server.
- User can define rule based on source and destination IP, source and destination Port number, and on Protocol used (IP, TCP, and ICMP).
- A Port scanner is also provided in this firewall to scan the system for open Ports.

1.4 OBJECTIVE

The objective to complete the Packet Filtering Firewall:

- The information of the firewall is taken from the case study that been examine in the past. The result from the case study is useful to gain an experience of the packet filtering characteristics in implementation of the firewall.

- From the research, studies and some revision of the packet filtering the requirement of the Packet Filtering Firewall is identified. The firewall will use the SDLC method to monitor the progress of the firewall implementation.

  The firewall objective is:

- To avoid the intrusion from the outside to inside network by closing the opened port that expose the network to the outsider. To identify the port that will expose to outside network the firewall is included with Port Scan utility.

- To improve the company security level by avoiding the resources form the bad intruders which will bring the profit lost.

1.5 PROJECT SCOPE

Firewall software implemented is basic packet filtering firewall and using API (Application Program Interface) method. The firewall implemented in windows platform and using API socket which offered by Microsoft. The firewall is currently implemented for the server site used.

The rule-set on this packet filtering firewall can be customized and altered by user. User cans manually define the rule-set based on destination IP, source and destination port number and on Protocols. The rule-set filter the basic of the IP, TCP and ICMP packet in the network.

The firewall is added with the Port Scan utility. A port scan is a series of messages sent by someone attempting to break into a computer to learn which computer network services, each associated with a "well-known" port number the computer provides. In this firewall the Port Scan used to scan the open port in the system. The opened port will allow the hackers to manipulate and burst into the system.

The firewall is using the Graphical User Interface (GUI) and object oriented programming method in the implementation of this firewall.

1.6 PROJECT SIGNIFICANCE

The general reasoning behind firewall usage is that without a firewall, a subnet's systems expose themselves to inherently insecure services such as NFS or NIS and to probes and attacks from hosts elsewhere on the network. In a firewall-less environment, network security relies totally on host security and all hosts must, in a sense, cooperate to achieve a uniformly high level of security. The larger the subnet, the less manageable it is to maintain all hosts at the same level of security. As mistakes and lapses in security become more common, break-ins occur not as the result of complex attacks, but because of simple errors in configuration and inadequate passwords. The following sections summarize the primary benefits of using a firewall.

1.6.1 Protection from Vulnerable Services

A firewall can greatly improve network security and reduce risks to hosts on the subnet by filtering inherently insecure services. As a result, the subnet network environment is exposed to fewer risks, since only selected protocols will be able to pass through the firewall.

Firewall could prohibit certain vulnerable services such as NFS from entering or leaving a protected subnet. This provides the benefit of preventing the services from being exploited by outside attackers, but at the same time permits the use of these services with greatly reduced risk to exploitation. Services such as NIS or NFS that are particularly useful on a local area network basis can thus be enjoyed and used to reduce the host management burden.

Firewalls can also provide protection from routing-based attacks, such as source routing and attempts to redirect routing paths to compromised sites via ICMP redirects. A firewall could reject all source-routed packets and ICMP redirects and then inform administrators of the incidents.

1.6.2 Controlled Access to Site Systems

A firewall also provides the ability to control access to site systems. For example, some hosts can be made reachable from outside networks, whereas others can be effectively sealed off from unwanted access. A site could prevent outside access to its hosts except for special cases such as mail servers or information servers.

This brings to the fore an access policy that firewalls are particularly adept at enforcing: do not provide access to hosts or services that do not require access. Put differently, why provide access to hosts and services that could be exploited by attackers when the access is not used or required? If, for example, a user requires little or no network access to her desktop workstation, then a firewall can enforce this policy.

1.6.3 Concentrated Security

A firewall can actually be less expensive for an organization in that all or most modified software and additional security software could be located on the firewall systems as opposed to being distributed on many hosts. In particular, one-time password systems and other add-on authentication software could be located at the firewall as opposed to each system that needed to be accessed from the Internet.

Other solutions to network security such as Kerberos [NIST94c] involve modifications at each host system. While Kerberos and other techniques should be considered for their advantages and may be more appropriate than firewalls in certain situations, firewalls tend to be simpler to implement in that only the firewall need run specialized software.

1.6.4 Enhanced Privacy

Privacy is of great concern to certain sites, since what would normally be considered innocuous information might actually contain clues that would be useful to an attacker. Using a firewall, some sites wish to block services such as finger and Domain Name Service. Finger displays information about users such as their last login time, whether they've read mail, and other items. But, finger could leak information to attackers about how often a system is used, whether the system has active users connected, and whether the system could be attacked without drawing attention.

Firewalls can also be used to block DNS information about site systems, thus the names and IP addresses of site systems would not be available to Internet hosts. Some sites feel that by blocking this information, they are hiding information that would otherwise be useful to attackers.

1.6.5 Logging and Statistics on Network Use, Misuse

If all access to and from the Internet passes through a firewall, the firewall can log accesses and provide valuable statistics about network usage. A firewall, with appropriate alarms that sound when suspicious activity occurs can also provide details on whether the firewall and network are being probed or attacked.

It is important to collect network usage statistics and evidence of probing for a number of reasons. Of primary importance is knowing whether the firewall is withstanding probes and attacks, and determining whether the controls on the firewall are adequate. Network usage statistics are also important as input into network requirements studies and risk analysis activities.