UNIVERSITI PUTRA MALAYSIA

AN INTEGRATED FIREWALL SYSTEM MODEL IN A MULTICLIENT-SERVER ENVIRONMENT

HUSSEIN A. TAQI AL-KAZWINI

AN INTEGRATED FIREWALL SYSTEM MODEL IN A MULTICLIENT-SERVER ENVIRONMENT

By

HUSSEIN A. TAQI AL-KAZWINI

Thesis Submitted to the School of Graduate Studies, Universiti Putra Malaysia in Fulfilment of the Partial Requirements for the Degree of Master of Science

February 2005

Dedicated

To

My country Iraq,

Abstract of thesis presented to the Senate of Universiti Putra Malaysia in fulfilment of the partial requirements for the degree of Master of Science

AN INTEGRATED FIREWALL SYSTEM MODEL IN A MULTICLIENT-SERVER ENVIRONMENT

By

HUSSEIN A. TAQI AL-KAZWINI

February 2005

Chairman: **Associate Professor Abdul Rahman Ramli, Ph.D.**

Faculty: **Engineering**

As the Internet grows, and the use of computers is getting more common, the need to secure networks and protect them from the Internet, while still being able to access it, is increasing. The easiest way to achieve a lot of this protection is through firewalls.

Firewall technology is the most widely deployed security technology on the Internet. Firewalls have been around for several years. They are a fact of life on the Internet and it is not likely they will disappear in the future. Ongoing development and research in the field of firewall technology have shown a continually addition of features and services to conventional firewall systems.

This thesis introduces a new concept for applying the security policy rules by both firewall administrators and users. The proposed firewall system solves some known problems which arise with the use of conventional firewalls residing at the networks perimeter. The developed firewall system integrates the main network firewall and the second-line firewalls into one system by the use of client/server technology to facilitate firewall configuration in a way that affords more convenience to users providing the new integrated firewall using multiclient-server scheme. It centralizes security functions in a single point, simplifying configuration and administration.

The new system makes it easier to configure and administrate a firewall in a way in which it is not a source of annoyance to users which offering them higher level of flexibility by giving them the chance to participate in the process of configuration of the firewall using the client side of the system and without affecting the network security policy. It also makes the progress of configuration and administration of the firewall system smoother by reducing the administrator efforts to maintain the system.

Good results have been achieved by using the program package. Results show that this system helps keeping the network traffic as low as possible, increasing the efficiency of the network and reducing the threats of malicious data passing in the network. It reduces the efforts and cost of overall system administration and maintenance as well. In addition, it affords users a system which is acceptable and preferable more than conventional firewall systems.

Abstrak tesis yang dikemukan kepada Senat Universiti Putra Malaysia sebagai memenuhi sebahagian keperluan untuk ijazah Master Sains

MODEL SISTEM DINDING API BERSEPADU MENGGUNAKAN KAEDAH TERAGIH PELBAGAI PELANGGAN-PELAYAN

Oleh

HUSSEIN A. TAQI AL-KAZWINI

Februari 2005

Pengerusi: **Profesor Madya Abdul Rahman Ramli, Ph.D.**

Fakulti: **Kejuruteraan**

Apabila Internet menjadi semakin pesat, penggunaan komputer menjadi suatu kebiasaan, justeru itu keselamatan rangkaian menjadi keperluan untuk melindungi para pengguna. Cara yang paling mudah dan berkesan untuk mencapai perlindungan ini ialah dengan menggunakan dinding api.

Teknologi dinding api ialah teknologi keselamatan yang popular di Internet. Dinding api telah digunakan semenjak beberapa tahun dulu. Ia menjadi suatu keperluan dan ia pasti akan terus digunakan pada masa hadapan. Pembangunan berterusan di dalam bidang dinding api telah menunjukkan penambahan berterusan kepada ciri-ciri dan perkhidmatan kepada sisitem dinding api yang biasa.

Tesis ini memperkenalkan konsep baru untuk melaksanakan peraturan polisi keselamatan oleh penyelia dinding api dan para penguna. Sistem dinding api yang dicadangkan menyelesaikan beberapa masalah-masalah yang timbul dengan penggunaan dinding api biasa di pintu masuk rangkaian. Dinding api yang dibangunkan, mengabungkan dinding api utama dan dinding api ke dua kepada suatu sistem dengan menggunakan teknologi pelanggan/pelayan untuk memudahkan konfigurasi dinding api. Konfigurasi ini memudahkan para pengguna untuk menyediakan dinding api bersepadu menggunakan kaedah pelbagai pelanggan-pelayan. Ia mengumpulkan fungsi-fungsi keselamatan pada suatu tempat, justeru itu memudahkan konfigurasi dan penyeliaan.

Sistem yang baru dibangunkan ini memudahkan konfigurasi dan penyeliaan dinding api agar ianya tidak meyusahkan para pengguna. Ia memberikan mereka keanjalan dengan membenarkan mereka turut serta di dalam proses konfigurasi dengan menggunakan pelanggan tanpa menggangu polisi keselamatan. Ia juga dapat melicinkan konfigurasi dan penyelenggaraan dengan mengurangkan beban penyelia.

Keputusan yang memberangsangkan telah dicapai dengan menggunakan program yang dibangunkan. Keputusan menunjukkan sistem ini dapat membantu mengurangkan trafik rangkaian, menambah keberkesanan rangkaian dan mengurangkan ancaman kepada rangkaian. Ia mengurangkan beban dan kos pentadbiran sistem dan penyelenggaraan. Selain itu, ia membolehkana para pengguna membantu menyelenggara dinding api dan ini adalah suatu kelebihan berbanding sistem dinding api yang biasa.

ACKNOWLEDGEMENTS

All praise to supreme almighty Allah swt. the only creator, cherisher, sustainer and efficient assembler of the world and galaxies whose blessings and kindness have enabled the author to accomplish this project successfully.

The author gratefully acknowledges the guidance, advice, support and encouragement he received from his supervisor, Associate Professor Dr. Abdul Rahman Ramli, who keeps advising and commenting throughout this project until it turns to real success.

Great appreciation is expressed to Associate Professor Dr. Md. Nasir Sulaiman and Mr. Syed Abdul Rahman Al-Hadad for their valuable remarks, help advice and encouragement.

Appreciation also to the Faculty of Engineering for providing the facilities and the components required for undertaking this project.

The author would like to thank his father and mother for their sacrifices, support, patience, inspiration, encouragement, help and cooperation during the whole period of study. The author is grateful to his sister Zaineb A. Al-Kazwini for her unfailing support and help.

I certify that Examination Committee met on 21st of February 2005 to conduct the final examination of Hussein A. Taqi Al-Kazwini on his Master of Science thesis entitled "An Integrated Firewall System Model in a Multiclient-Server Environment" in accordance with Universiti Pertanian Malaysia (Higher Degree) Act 1980 and Universiti Pertanian Malaysia (Higher Degree) Regulations 1981. The Committee recommends that the candidate be awarded the relevant degree. Members of the Examination Committee are as follows:

Elsadiq Ahmed Mohamed Babiker, Ph.D.
Lecturer
Faculty of Engineering
Universiti Putra Malaysia
(Chairman)

Khairi Yusuf, Ph.D.
Lecturer
Faculty of Engineering
Universiti Putra Malaysia
(Member)

Shamala Subramaniam, Ph.D.
Lecturer
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Member)

Abdullah Embong, Ph.D.
Associate Professor
School of Computer Science
Universiti Sains Malaysia
(Independent)

GULAM RUSUL RAHMAT ALI, Ph.D.
Professor/Deputy Dean
School of Graduate Studies
Universiti Putra Malaysia

Date:

This thesis submitted to the Senate of Universiti Putra Malaysia and has been accepted as fulfilment of the partial requirements for the degree of Master of Science. The members of the Supervisory Committee are as follows:

Abdul Rahman Ramli, Ph.D.
Associate Professor
Faculty of Engineering
Universiti Putra Malaysia
(Chairman)

Md. Nasir Sulaiman, Ph.D.
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Member)

Syed Abdul Rahman Al-Hadad
Lecturer
Faculty of Engineering
Universiti Putra Malaysia
(Member)

AINI IDERIS, Ph.D.
Professor/Dean
School of Graduate Studies
Universiti Putra Malaysia

Date:

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 at UPM or other institutions.

_____

HUSSEIN A. TAQI AL-KAZWINI

Date: **01 JUL 2004**

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

HTTP	Hyper text Transfer Protocol
FTP	File Transfer Protocol
CSIRT	Computer Security Incident Response Team
TCP	Transmission Control Protocol
IP	Internet Protocol
UDP	User Datagram Protocol
API	Application Programming Interfaces
URL	Uniform Resource Locator
OSI	Open Systems Interconnection
ISO	International Organization of Standards
IETF	Internet Engineering Task Force
ISP	Internet Service Provider
GUI	Graphical User Interface
BASIC	Beginners All-Purpose Symbolic Instruction Code
IDE	Integrated Development Environment
IIS	Internet Information Server
PC	Personal Computer

CHAPTER 1

INTRODUCTION

1.1 Background

The widespread usage of Internet and networking, whilst increasing the productivity, efficiency and knowledge sharing has resulted in additional problems in the hands of the computer security personnel. The increase in the vulnerability of the systems connected to the Internet is not only due to the fact that more systems are available for the attack, but also due to the fact that more systems are available from which the attack could be carried out. Also, the advancement in technology has provided sophisticated attack tools, which can be used even by people not having much competence. Hence, a day probably does not pass without some sort of compromise in the private networks (Negi, 2001).

Like the locks used to help keep tangible property secure, computers and data networks need provisions that help keep information secure. Security in the Internet environment is both important and difficult. It is important because information has significant value. Security in the Internet is difficult because security involves understanding when and how participating users, computers, services, and networks can trust one another as well as understanding the technical details of network hardware and protocols. Security is required on every computer and every protocol; a single weakness can compromise the security of an entire network (Comer, 2000).

Mechanisms that control Internet access handle the problem of screening a particular network from unwanted communication. Such mechanisms can help prevent outsiders from: obtaining information, changing information, or disruption communication a private network. A single technique known as an Internet Firewall has emerged as the basis for Internet access control (Marcus, 1999).

The degree of protection that exists on any given host depends on how much time and effort has been put into applying mechanisms to protect this host. Often times, this requires much more time and effort than is desired by the various system administrators and many systems are left in a quite open and extremely vulnerable state. Also, many of these security mechanisms have a significant effect on the performance of a system and thus may not be used for this reason as well. Additional layers of security are needed for the protection and so products like the Firewalls and Intrusion Detection Systems are being used by a lot of companies in response to the new threats (Negi, 2001).

A firewall insulates a private network from a public network using carefully established controls on the types of requests they will route through to the private network for processing and fulfillment (Merkow and Breithaupt, 2000).

Firewalls provide security for corporate networks by applying a set of logical rules to the traffic accessing the private network resources. The firewall fulfils the security requirements by also performing other security related functions such as user identification and authentication, access control, encryption, intrusion detection,

connection tracking, virus scanning, tunneling, traffic balancing, log history and alert reporting (Stonesoft, 2003).

Firewall core is a gateway that implies network traffic filters for inbound and outbound network traffic. The security level is defined by the security policy. The policy is formed by combining simple rules together and applying all of them against the traffic (Goncalves, 2001).

1.2 Problem Statement

All networking devices and servers require regular monitoring for optimal and trouble free performance. Because firewalls are typically the first line of defense against intruders, their configuration must be carefully implemented and tested.

The main function of a firewall is to protect internal computer networks and the computers within them from unauthorized access or attacks from external networks. Only authorized traffic, as defined by the local security policy, is allowed to pass through the firewall.

Defining one security policy that satisfies all the needs of internal networks and/or internal computers is not a possible choice. Usually the solution is to use internal firewalls for internal networks or to use personal firewalls for internal workstations increasing the number of used firewall systems. In both cases, additional cost for all these firewalls is needed and extra efforts for configuration and administration are

needed as well. Another problem arises; networks that use more than one firewall system miss the homogeneity which can affect the security of the overall system.

One of the motivations behind this research was the need to find a convenient way to apply different required security policies using one integrated firewall system which reduces cost and efforts dedicated originally to maintain, manage and administrate many firewall systems that are used to apply the different security policies.

1.3 Objectives

In this research, several objectives for enhancing the way used to administrate remote firewalls will be proposed:

1. To study and understand firewalls technologies
2. To design and implement a prototype that represents the firewall (server side)
3. To realize the multiclient-server distributed firewall model by designing a prototype representing the client part

1.4 Contribution of the Work

Ongoing development and research in the field of firewall technology have shown a continually addition of features and services to conventional firewall systems. The effectiveness of firewalls at providing their benefits is largely a function of the flexibility and usability of the tools provided to users and administrators (Oppliger, 2002).

The proposed system integrates the conventional firewall system with personal firewalls or whatever firewalls behind it into one system providing very high level of flexibility and usability to both users and administrators and enhancing the overall process of securing the network being protected by the new firewall system.

In addition, it reduces the required cost and effort to maintain, configure and administrate a conventional firewall system to reach somewhat similar results.

1.5 Thesis Organization

This thesis is organized in five chapters. Chapter I presents a general background of the research problem, problem statement, and the objectives of the research. Chapter II covers the literature review. While Chapter III contains the methodology used in designing the proposed system. The results are discussed in Chapter IV. Finally, Chapter V summarizes the research findings and suggests potential future work.

CHAPTER 2

LITERATURE REVIEW

2.1 Internet Evolution and Growth

The beginnings of the Internet go back to 1969, when the American Defense Advanced Research Projects Agency (DARPA) began experimenting with building a network to allow scientists to share data that would also be robust enough to survive partial outrages, such as a bomb attack. The Internet itself came in the mid 1980s when the US National Science Foundation funded the building of a communications backbone to connect five regional supercomputing centers so that the nation's universities could all share their facilities. Access then was mostly limited to scientists, academic researchers, and government employees using policies prohibited commercial traffic across the Internet. It did not take long for similar networks in other countries to start hooking themselves up to the Internet, along with other small, independent local networks. Consequently, the Internet became a worldwide collection of loosely connected networks that are accessible by individual computer hosts in a variety of ways; including gateways, routers, dial-up connections, and Internet service providers. By 1994, the Internet was spreading everywhere, fuelled partly by changes in policy to allow the carriage of commercial traffic, partly by the advent of the World Wide Web as the most important unifying interface to what had become a sprawling incoherent mass of information and partly

by the availability of affordable access to those outside the academic, research and government communities where it began (Grossman, 1999).

The Internet supports a vast and growing community of computers users around the world. Unfortunately, this network can provide anonymous access to this community by the unscrupulous, careless, or dangerous. On any given Internet there is a certain percentage of poorly-maintained systems. The Internet is easily accessible to anyone with a computer and a network connection. Individuals and organizations worldwide can reach any point on the network without regard to national or geographic boundaries or time of day (Cheswick, 1990).

Many organizations are looking at connecting to the Internet but are terrified of the risk of being broken into by hackers, industrial spies, or other electronic miscreants. It is very hard to get an accurate picture of the size of the threat, or the real risk that any individual organization runs by connecting to the Internet. These days, however, it is becoming equally clear that not being connected to the Internet is also a business risk which may also equate to lost revenue, time-to-market, or customer perception (Zwicky, et al, 2000).

2.2 Internet Security

Although the Internet was originally conceived of and designed as a research and education network, usage patterns have radically changed. The Internet has become a home for private and commercial communication, and it is still expanding into important areas of commerce, medicine, and public services (Dekker, 1997).

With the continuing growth of the Internet and its ever-increasing interconnection of information technology (IT) devices, it is not surprising that security aspects are of major concern right now. Increased reliance on the Internet is expected over the next few years, along with increased attention to its security. The architecture of Internet was not originally designed with security in mind. In the past decades, researchers have put enormous amounts of effort into introducing security features to the architecture, in order to protect users from malicious individuals. These "blackhats" exploit weaknesses in the architecture in order to gain access to other systems, steal or destroy valuable data, or prevent legitimate users from accessing Internet services. The level of sophistication required to achieve this varies greatly; unfortunately the Internet itself provides well-written and easy-to-use exploit programs that allow even amateurs to cause significant damage (Kreibich, 2003).

Security is one of the most important fields dealing with the Internet. The ability to access and transfer information in a few seconds allows governments, companies, educational institutions, and individuals to accelerate the decision process or simply be “informed.” However, information can be very valuable and there is a need for better and faster security systems to protect information and networks (Harris, 2002).

Intruders often attempt to gain access to networked systems by pretending to initiate connections from trusted hosts. They squash the emissions of the genuine host using a denial-of-service attack and then attempt to connect to a target system using the address of the genuine host. To counter these address-spoofing attacks and enforce