



شبكة المعلومات الجامعية

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ



شبكة المعلومات الجامعية
@ ASUNET



شبكة المعلومات الجامعية التوثيق الالكتروني والميكرو فيلم



شبكة المعلومات الجامعية

جامعة عين شمس

التوثيق الالكتروني والميكروفيلم

قسم

نقسم بالله العظيم أن المادة التي تم توثيقها وتسجيلها
علي هذه الأفلام قد أعدت دون أية تغيرات



يجب أن

تحفظ هذه الأفلام بعيدا عن الغبار

في درجة حرارة من ١٥-٢٥ مئوية ورطوبة نسبية من ٢٠-٤٠%

To be Kept away from Dust in Dry Cool place of
15-25- c and relative humidity 20-40%

بعض الوثائق الأصلية تالفة

بالرسالة صفحات لم ترد بالاصل

Cairo University
Institute of Statistical Studies and Research
Department of Computer Science and Information

A Firewall Based Scheme for Computer Networks Security

Thesis

Submitted in Partial Fulfillment for the M.Sc.Degree in
Computer Sciences and Information

By
Omar Ibrahim Sherif

Supervised By

Prof. Dr. Sanaa El-Ola Hanafi Ahmed
Chairman of Information Technology Department
Faculty of Computers and Information
Cairo University

Dr. Osman Mohamed Ibrahim
Egyptian Armed Forces

997

Cairo University
2001

Acknowledgement

I would like to thank prof. Dr. Sanaa El_Ola H. Ahmed and Dr. Osman M. Ibrahim for their great assistance and constructive supervision. They have not denied me anything, time, effort, advices, and encouragement

I would also like to thank all the friends in my work (RDSC) for their help, specially Dr. A. H. Abou_Ali who gave me a big hand in acheiving this work.

My sincere thanks to my family, my wife, and my children for their patience, effort, and help for fulfilling this work.

APPROVAL SHEET

A Firewall Based Scheme for Computer Networks Security

Master Thesis

Submitted By
Omar Ibrahim Sherif

This Thesis is for the Master Degree in Computer Science and Information, Department of Computer Science and Information, Institute of Statistical Studies and Research, Cairo University, Has Been Approved By:

Name	Signature
Prof. Dr. Mohamed Zaki	M. Zaki
Prof. Dr. Sanaa El-Ola Hanafi	S.H. Ahmed
Dr. Abdel Aziz Khamis	A. Khamis

Date: 3/12/2001

STATEMENT

I certify that this work has not been accepted or submitted in candidature for any other degree.

Any portion of this thesis for which I am indebted to other sources are mentioned and explicit references are given.

Omar Ibrahim Sherif

Date: 3/12/2001

Abstract

Many organizations are in the process of connecting to the Internet to take the advantage of Internet services and resources. While Internet connectivity offers enormous benefits in terms of increased access to information, Internet connectivity is not necessary a good thing for sites with low levels of security. Firewalls are effective type of network security. Most of the firewalls protect the private network by controlling the traffic between the Internet and the private network based on the header information in the packets or the commands in the payload part of the packets.

In this thesis we propose a module, which can be added to the firewall to extend the firewall functionality, by controlling the communications based on the actual contents of messages that is to more secure the critical information of certain organization from being sent through the Internet.

The module depends on filtering the messages sent through the Internet according to some keywords predetermined to be a clue for the critical information of the organization.

Besides, we propose an artificial intelligence based intrusion detection module to be used in detecting and preventing the misuse intrusions. This module is added to the firewall to strengthen the firewall that is by detecting the malicious behavior of the new attackers using a new methodology of attacking the networks.

Keywords: -

Internet security, Firewalls, Packet filtering, Proxy services, Intrusion detection.

Contents

CHAPTER 1:Introduction.....	1
CHAPTER 2: Internet Security: An Overview.....	6
2.1 Introduction.....	7
2.2 Networking and ISO/OSI Reference Model.....	7
2.3 Internet.....	8
2.3.1 Transmission Control Protocol.....	10
2.3.2 Functions of TCP/IP layers.....	10
2.3.3 Ports.....	12
2.3.4 Common Internet Services.....	14
2.4 Internet Security	16
2.4.1 Internet security problems.....	20
2.4.1.1 TCP/IP Protocol problems.....	20
2.4.1.2 Forged E mail.....	21
2.4.1.3 Monitoring Network Traffic (Snooping).....	22
2.5 Network security Policy.....	22
2.5.1 Network Service Access Policy.....	23
2.5.2 System Specific Policies	24
2.5.3 Firewall Design Policy.....	24
2.5.4 Security Strategies	25
2.6 Summary	27
CHAPTER 3: Firewalls.....	28
3.1 Introduction.....	29
3.2 General Capabilities and limitations of Firewalls.....	30
3.3 Types of Firewalls.....	31
3.3.1 Packet Filtering Firewalls.....	31
3.3.2 Proxy Services.....	35

3.3.3 Circuit-level Proxy.....	37
3.3.4 Stateful Inspection Technique.....	38
3.4 Different Firewall Architectures.....	39
3.4.1 Dual-Homed Host architecture.....	39
3.4.2 screened Host architecture.....	41
3.4.3 Screened Subnet architecture.....	43
3.5 Summary.....	44
CHAPTER 4: Evaluating a Firewall Product.....	46
4.1 Introduction.....	47
4.2 Selection Criteria.....	47
4.2.1 Security Features.....	47
4.2.2 Implementation Features.....	50
4.2.3 User Features.....	51
4.3 Applying Criteria to Commercial Firewalls.....	52
4.3.1 Check-Point Firewall (FireWall-1).....	52
4.3.2 Gauntlet Firewall 6.0.....	58
4.3.3 Comparison between the two products.....	61
4.4 Conclusion.....	63
CHAPTER 5: Extending Traditional Firewall	
Functionality	64
5.1 Introduction.....	65
5.2 Why the extension.....	65
5.3 Natural Language Processing.....	66
5.3.1 Problems with Natural Language Systems.....	66
5.4 Explaining the Module.....	69
5.4.1 Simple Mail Transfer Protocol (SMTP).....	70
5.4.2 The SMTP Procedure.....	71

5.5 Methodology.....	74
5.5.1 Examining the message.....	75
5.5.2 Search Algorithm.....	75
5.6 Case Study.....	78
5.6.1 Results.....	80

CHAPTER 6: Adding an Intrusion Detection Module

to the Firewall.....	82
6.1 Introduction.....	83
6.2 Introduction to Intrusion Detection.....	83
6.2.1 Approaches of Intrusion Detection.....	83
6.3 Methods Of Intrusion Detection.....	84
6.3.1 State Transition Analysis.....	84
6.3.2 Bayesian Alarm Network.....	85
6.3.3 Rule-Based Expert Systems.....	86
6.4 Expert Systems in Detecting SYN Flood Attack.....	87
6.4.1 TCP/IP Connection Establishment.....	88
6.4.2 SYN Flooding Attack Occurrence.....	88
6.4.3 Detection the SYN Flooding Attack.....	89
6.4.3.1 TCP Dump Traffic Monitor.....	89
6.5. Procedure.....	90
6.5.1 Rule Set for Detecting SYN Flooding Attack.....	91
6.6 Case Study.....	93
6.6.1 Results.....	96
6.7 Conclusion.....	96

CHAPTER 7: Conclusion and Future work.....98

References

Appendix A: Visual Basic Forms Results

CHAPTER 1

Introduction

Introduction

The Internet is spreading very rapidly all over the world. Connecting to the internet helps exchanging information between all people connected to the internet .In spite of these benefits, the internet could be the source of a lot of problems affecting the organizations connected to it [1]. These problems, or security threats can be categorized into two main categories, the first category includes the problems affecting the confidentiality of the data, or simply thefting the data during traveling through internet .The second category includes the problems affecting the network resources such as computer, gateways, and routers. These problems are caused by malicious users who are granted illegal access to some private network through highly sophisticated tools. These users are called hackers or attackers.

The success of attacker in attacking the private networks depends in some types of attack in some bugs in the operating system, which implements the network protocol. Some expert attackers exploited these bugs and developed tools for attacking the private networks through the Internet. Some success depends on the ignorance of some users principles.

Several possible solutions to these problems have been proposed and implemented. Some of these solutions are proposed by Bellare [2,3], who proposed a solution for the security problems in TCP/IP protocol. Some of these problems are: TCP sequence number attacks, and source routing. These solutions depend on some change on TCP/IP protocol versions. The newest solutions now for protecting the local networks against security problems or attackers are the firewall systems.

Firewalls are set of hardware, software or combination of both which acts as a single point of connection between the private network