Firewall Implementation

By

Mr. Waqar Ahmad
MCS

T-0415

Supervised by:

Mrs. Farzana Khan

This report is submitted in partial fulfillment of requirement of the degree of MCS (communication & networks)

Bahria Institute of Management & Computer Sciences
Islamabad

Dedicated to our parents.

Acknowledgement

Ist of All we pay thanks to Almighty Allah who provided us energy and patience to work on this project.

We owe successful completion of this project to the fruitful guidance given by Madam Farzana Khan during the project.

We are thankful to Mr. Fazle Wahab Head of Compter Science Deptt. Who always shown a lot of trust on us which played a vital role in our personality development.

Thanks to our teachers for providing us quality education.

Many thanks go to our parents who always prayed for us. They always provided us every kind of support. Which we needed from childhood to this stage.

In the last but not least our special thanks goes to our classmates for making our stay in the Bahria University such a memorable one

Abstract

The increasing complexity of networks, and the need to make them more open due to the growing emphasis on and attractiveness of the Internet as a medium for business transactions, mean that networks are becoming more and more exposed to attacks, both from without and from within. The search is on for mechanisms and techniques for the protection of internal networks from such attacks. One of the protective mechanisms under serious consideration is the firewall. A firewall protects a network by guarding the points of entry to it. The document covers a general view of firewalls, its impact on the security of a network or a PC, different platforms where firewalls can be used, different kind of firewall technologies, techniques of implementing firewall software and hardware, improvements possible in the technology and a brief project code description at the end.

Final Approval

This is to certify that we have read the project report submitted by Waqar Ahmad and it is our judgment that this report is of well standard, and it is accepted by Bahria University Islamabad, for the degree of master of computer sciences, MCS.

Supervisor

Head of Department

Internal Examiner

External Examiner

Table of Contents

Contents	Page #
Dedication	i
Acknowledgement	ii
Abstract	iii
Certificate signs	iv
List of Tables	v
List of Figures	vi
1. Introduction	1
1.1. What is a firewall?	
1.2. What does a firewall do?	
1.3. What can't a firewall do?	
1.4. Who needs a firewall?	
1.5. How does a firewall work?	
1.6. OSI and TCP/IP models	
1.7. Firewall Types	
1.8. Implementation	
1.9. Is a firewall sufficient?	
1.10. IP Spoofing?	
1.11. Firewall Problems	
1.12. Benefits	
2. Types of firewall	12
2.1. Packet filtering firewall	
2.2. Application lever gateway	
2.3. Stateful inspection firewall	
3. Designing the firewall	42
3.1. Select firewall functions	
3.2. Select the firewall topology	
3.3. Perform architectural trade-off analysis	
3.4. Protect your firewall system from unauthorized access	
3.5. Determine required hardware components	
3.6. Determine required software components	
3.7. Determine required testing components	
3.8. Acquire all components	
4. Firewall documentation, training and support	56
4.1. Determine your training requirements	
4.2. Determine your support requirements	
4.3. Install a minimum acceptable operating system environment	
4.4. Install all applicable patches	
4.5. Restrict user and host access	
4.6. Disable IP forwarding	
4.7. Backup your system	

5. Configure IP routing ---------- 61
   5.1. Obtain IP addresses
   5.2. Establish routing configuration
   5.3. Configure firewall packet filtering
   5.4. Design the packet filtering rules
   5.5. Document the packet filtering rules
   5.6. Install packet filtering rules

6. Firewall Security Policy ---------- 72
   6.1. Firewall policy
   6.2. Implementing firewall ruleset
   6.3. Testing Firewall policy
   6.4. A sample topology and ruleset

- Brief description of Classes used in code
- Conclusion
- Appendix of Terminologies
- Bibliography and References

List of Figures

Figure #	Page #
1.1- Hardware Firewall	2
1.2- Software Firewall	2
1.3- Basic firewall operations	3
1.4- The OSI and TCP/IP model	6
1.5- Firewall have their own IP layer	6
1.6- Packet filtering firewall	7
1.7- Application layer gateway	8
1.8- Stateful inspection firewall	9
2.1- Filter table	22
2.2- Relationship between tables	27
2.3- Packet filtering firewall flowchart	28
3.1- Single layer architecture	50
3.2- Multi layer architecture	50
3.3- Application proxy	51
3.4- Basic firewall with DMZ network Architecture	51
3.5- Dual firewall with DMZ network Architecture	52
6.1- Sample firewall environment	80

List of Tables

Table #	Page #
2.1- Criteria for Packet filtering	16
2.2- Comparison of firewall technologies	16
6.1- Firewall Application traffic ruleset matrix	74
6.2- Sample ruleset for boundary router	82