INTERNATIONAL JOURNAL OF
INNOVATIVE RESEARCH & DEVELOPMENT

ISSN 2278 – 0211 (Online)

Network Security, Ensuring Maximum Protection through Firewall

Egere A. N.
Federal Polytechnic Bali, Nigeria
Ifeanyi E. Ukatu
University of Nigeria Nsukka, Nigeria

Abstract:
The connection of an internal network to an external network such as Internet has made it vulnerable to attacks. One class of network attack is unauthorized penetration into network due to the openness of networks. It is possible for an attacker or hackers to sum access to an internal network, this pose great danger to the network and network resources. Our objective and major concern of network design was to build a secured network, based on software firewall that ensured the integrity and confidentiality of information on the network. We proposed an Object-Oriented Methodology and developed an improved software based solution that allows all the inbound and outbound traffic to pass through the firewall. The firewall in turn determines which traffic should be allowed in or out of the network. The firewall algorithm was implemented using Java programming language, which was based on java security architecture. It also utilizes the concept of XML and HTML programming which enables network communication over the internet.

1. Introduction

Computer network is the engineering discipline concerned with communication between computer system and devices. The purposes of networking are exchange of data and resources sharing. With network, large volume of data can be exchanged through both short and long-range connections. Likewise computer resources such as hardware (printers, scanner etc.) and software can be remotely shared among network hosts.

With increased reliance on computer network, calls for serious monitoring of the traffic in and out of the system network. Attackeron the internet could break into the network and do harm in a number of ways; they can steal or damage important data, damage individuals computer or their entire network, and use the internal network computer resources. Due to some of these security threats, there was the need to build a defensive mechanism that ensures that attackers and their likes are not allowed into the network. Firewalls are designed to stop unwanted or suspected traffics from flowing into the internal network. Sets of rules are applied to control the type of networking traffic flowing in and out of the system. This would ensure that attackers have no access to the internal network.

1.1. Statement of Problem

The problem to be solved is the problem of organizations network. What can firms do to protect their network over potential threats against the “resources” they share on the network?

1.2. Objectives

To develop a firewall system to block unauthorized access to the network and prevent malicious attack which could lead to data loss

1.3. Significance of the Study

The significance of this study is to show how a firewall could prevent attack and protect network resources which will make harder for an attacker to penetrate into the system. The system will be able to offer online services. The probability of exploring vulnerability will be reduced to low risk and the system will be more stable

2. Literature Review

This chapter describes what firewalls can do for network security. What firewall need to control and protect and the impact of firewall in organisation network and users. A review on how network traffic can be monitored in order to prevent an unauthorized access to internal network.

Firewalls are usually the first component of network security. They separate networks in different security levels, by utilizing network access control policies. The major function of the firewall is to protect the private network from non-legitimate traffic.

Firewalls are located between the Internet and private network. They can monitor the outgoing and incoming traffic; also they can prevent the harmful traffic and attacks from Internet. They also can stop the non-legitimate outgoing traffic. If a computer from the local network is attacked by an intruder and generates non-legitimate traffic, the firewall can prevent and detect the computer. Firewall can detect such succeeded attack, so it can be recovered.

As information systems have come to be more comprehensive and a higher value asset of organizations, complex, *intrusion detection* subsystems have been incorporated as elements of operating systems, although not typically applications [8]. Most intrusion detection systems attempt to detect suspected intrusion, and then they alert a system administrator.

Intrusion *detection* involves determining that some entity, an *intruder*, has attempted to gain, or worse, has gained unauthorized access to the system. None of the automated detection approaches of which we are aware seeks to identify an intruder before that intruder initiates interaction with the system. Of course, system administrators routinely take actions to prevent intrusion. These can include requiring passwords to be submitted before a user can gain any access to the system, fixing known vulnerabilities that an intruder might try to exploit in order to gain unauthorized access, blocking some or all network access, as well as restricting physical access. Intrusion detection systems are used in addition to such preventative measures.

Intruders are classified in two groups. *External intruders* do not have any authorized access to the system they attack. *Internal intruders* have some authority, but seek to gain additional ability to take action without legitimate authorization. [9] divided internal intruders into three subgroups: masqueraders, clandestine, and legitimate [8]. In later related work, [10] has divided internal intruders into two categories. He separates internal users who have accounts on the system from pseudo-internal intruders who are, or can be thought of as being, physically in space of legitimate users, but have no accounts [8]. They do however have physical access to the same equipment used by those who have accounts. He shows how distinguishing the two categories can be distinguished enables better defense against the pseudo-internal intruders.

Intrusion detection is the process of monitoring and searching networks of computers and systems for security policy violations [12]. Intrusion Detection Systems (IDSs) are software or hardware products that automate this monitoring and analysis process. An IDS inspects all inbound and outbound network activity, system logs and events, and identifies suspicious patterns or events that may indicate a network or system attack from someone attempting to break into or compromise a system [13].

Theoretically, IDSs work like a burglar alarm, alerting security managers that an attack may be taking place so that they can respond accordingly. IDSs trigger these alerts by detecting anomalous traffic patterns or “signatures” that are characteristic of an attack. As in the physical world, our logical burglar alarm provides valuable notification that someone has managed to breach perimeter security measures, and should allow security managers to determine exactly what happened during the attack, and hopefully provide indications of how the security weakness might be addressed.

What does the firewall need to control or protect?

In order to make a sound decision, first identify what functions the firewall would need to perform. Will it control access to and from the network, or will it protect services and users?

What would the firewall control?

- Access into the network
- Access out of the network
- Access between internal networks, departments, or buildings
- Access for specific groups, users or addresses
- Access to specific resources or services
- What would it need to protect?
- Specific machines or networks
- Specific services
- Information - private or public
- Users

After identifying what the firewall needs to control or protect, determine what might happen without this control and protection. What would happen if users had access to things they should not? What would happen if the unprotected services or information were compromised? Is the risk of not having control or protection great enough to warrant taking the next step in the assessing the need for a firewall solution?

3. Methodology

This project work uses Object-Oriented Methodology to analyze the system and CISCO access-list format for specifying the rule set.

Objects-Oriented Analysis (OOA) looks at the problem domain, with the aim of producing a conceptual model of the information that exists in the area being analyzed. The result of object-oriented analysis is a description of what the system is functionally required to do, in the form of a conceptual model that will typically be presented as a set of use cases.

3.1. Algorithms for Analyzing Firewall

Network firewalls play a very important role in network traffic management. By regulating which packets are accepted by a firewall or router, both the security and performance of the network can be improved. Firewalls usually have rules which indicate which packets should be accepted and which rejected.

3.1.1. Rule Sets

Filter (routers and firewalls) rules come in several formats; typically these are proprietary formats. While the expressiveness and syntax of the formats differ, the following generic description gives a good feeling for what such rules sets look like. A rule set consists of a list of rules of the form if condition then action, where the action is either accept or reject.

- Example

access-list 111 permit tcp any host 152.8.1.1 eq 80

This permits any computer on the Internet to connect to the computer whose IP address is 152.8.1.1 using the TCP protocol and port 80.

access-list 123 deny any 178.22.8.9 0.0.255.255

This will prohibit any computer from accessing a computer on the 178.22 domain using any protocol.

access-list 101 permit tcp 20.9.17.8 0.0.0.0 121.11.127.20 0.0.0.0 range 23 27

This says that any TCP protocol packet coming from IP address 20.9.17.8 destined for IP address 121.11.127.20 is to be accepted provided the destination port address is in the range 23: 27.

The rules are searched one by one to see whether the condition matches the incoming packet: if it does, the packet is accepted or rejected depending on the action (which will either be accept or reject); if the condition does not match the rule, the search continues with the following rules. If none of the rules match the packet is rejected.

3.2. Analysis of the Proposed System

The new system titled “NETWORK SECURITYENSURING MAXIMUM PROTECTION THROUGH FIREWALL.” was hence proposed to use the algorithm above and implement a robust firewall software system using modern CISCO access-list format.

3.2.1. Specification of the Proposed System

The proposed system should be able to perform the following operations: Functional Requirements:

- The proposed system should be able to allow participants to configure their computer systems’ firewall using Cisco-like commands.
- The proposed system should be able to prompt participant to enter his/her name when he/she launches the system’s player client in other to identify him/herself to other participants.
- The system should be able to allow participant to take actions against other players once the actions are enabled by the administrator.
- The system should be able to allow participants to reconfigure their firewall to correct problems, if they receive messages that other players are successfully attacking their network.
- The system should be able to allow participants to reconfigure their firewall once new tasks are sent by the network administrator in other not to make their firewall vulnerable to related attacks by other players.
- It should be able to allow the network administrator to configure his firewall to protect his network and also attack the simulated networks of other participants in other earn or lose points.

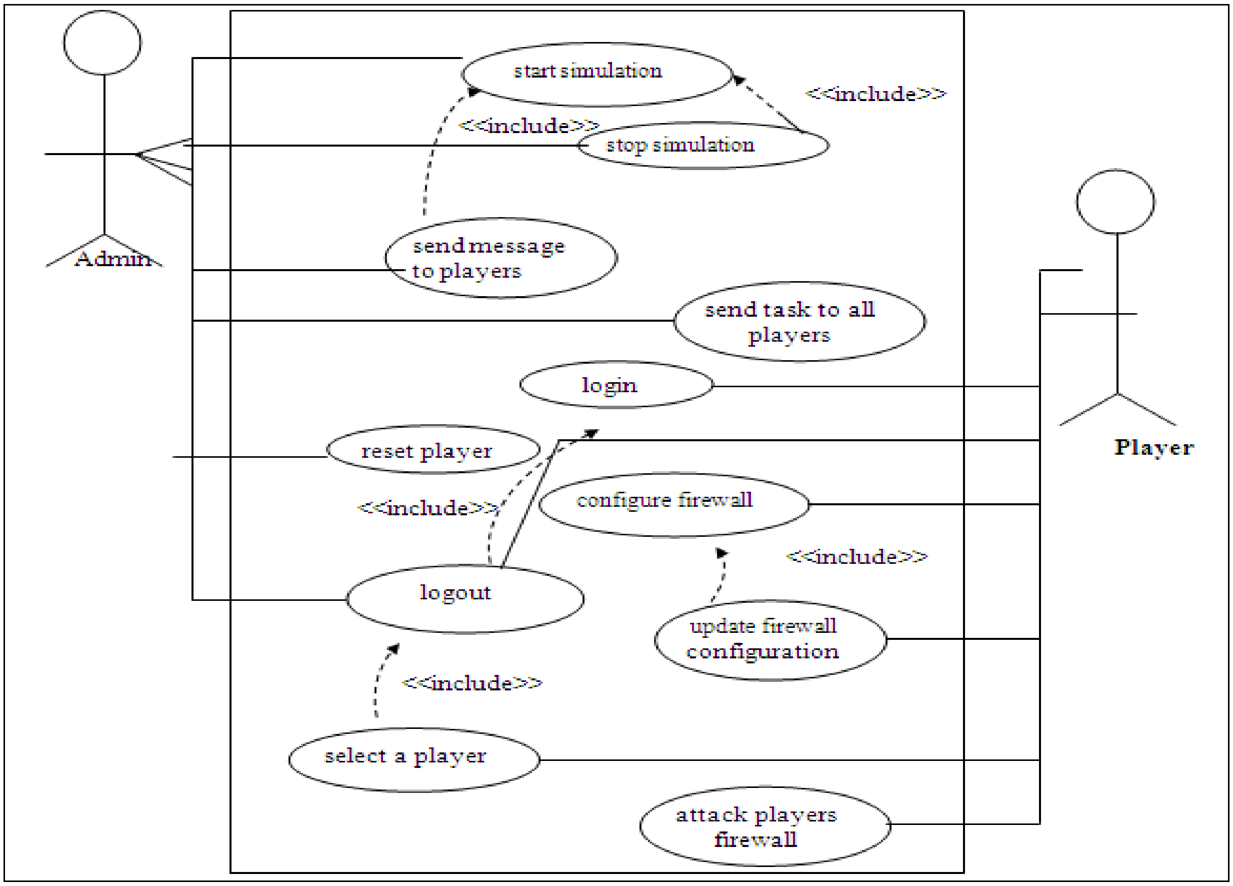

Figure 1: Use case boundary diagram

Note**:** In the above Boundary Diagram, the large rectangle is the system boundary. Everything inside the rectangle is part of the system under development. Outside the rectangle are the actors that act upon the system.

Actors are entities outside the system that provide the stimuli for the system. Typically, they are human users, or other systems. Inside the boundary rectangle are the use cases. These are the ovals with names inside. The lines connect the actors to the use cases that they stimulate.

An <<includes>> relationship indicates that the second use case is always invoked by the first use case.

An <<extends>> relationship indicates that the second use case may optionally invoke the first use case.

3.3. Design of the Proposed System

Object-Oriented Design (OOD) transforms the conceptual model produced in object-oriented analysis to take account of the constraints imposed by the chosen architecture and any non- functional technological or environmental-constraints, such as transaction throughput, response time, run-time platform, development environment, or programming language.

The concepts in the analysis model are mapped onto implementation classes and interfaces. The result is a model of the solution domain, a detailed description of how the system is to be built. Thus, class diagram, sequence diagrams, and deployment diagrams of Unified Modeling Language (UML) will be used for the design of the system.

3.4. Development Environment, Coding and Testing Technique

The coding of the entire program was done in NetBeans Integrated Development Environment (IDE).

The entire project comprises of three parts: the server which monitors the entire firewall simulation, the administrator client which is the applet for the firewall simulation administrator and the player client which is the applet for the firewall simulation player. The firewall monitor server was done with Java and XML whereas the administrator and player clients were done with Java, XML and HTML. The different parts are distributed.

In the course of the software implementation, testing was done several times to ensure that the software meets the users' requirements at each point. Testing was not done with the main software but on a duplicate of the software called the 'Test software' so as to have where to fall back on incase of any crash during testing.

In testing, we check both verification (the software compiles with the requirements) and validation (the software has been written correctly and effectively). The software is also tested against its analysis specifications.

There are different types of tests adopted at different stages. They include;

- Unit Testing – Testing each class or unit of the software interface.

- Integration Testing – Testing done during the combination of various class and various sub systems for compatibility check.
- Sub-System Testing – Testing done when on a subsystem before integration.
- System Testing –Testing after the combination of the various subsystems and the three different components to produce the required software.
- Acceptance Testing **-** In this stage, I choose to invite people who have used similar software to do the eventual users' testing and I also invited other software developers and finally my supervisor to do the acceptance testing.

Two different software testing techniques were adopted as a systematic testing approach and they are:

- White Box Testing – This technique focuses on the program control structure which involves close examination of procedure detail. Program statements, internal data structure, loop, logical paths and logical statements are tested. White box testing helps us to test the quality of the construction of the software.
- Black Box Testing – This technique tests the quality of the performance of the software and is conducted at the software interface. It tests the functionality of the system.

The aim of the two test techniques conducted was to ensure that the software has the following attributes: Completeness, Correctness, Reliability and Possibility of maintenance.

4. Summary

Information security has become an important concept in any organizations due to the fact that an unprotected information system can be exposed to danger in a network as a result of penetration tools at the disposal of hackers and crackers. Therefore, there was need to ensure adequate protection of internal network from hackers. This study has demonstrated that Firewall System can be employed to improve the organization internal network by blocking unauthorized access to organization network and give the best recommendation to the user on suitable parameter for threat detection.

5. Plans for the Future

The limitation of this work was the inability of the system to track traffic from dial-up connections. We therefore recommend that future work on this software should solve the problem of tracking down traffic from dial-up connections. The system supports 70 concurrent connections at a time and this can also be improved upon in future software development.

6. Conclusion

As organization tends to secure the resources they share on network, so also attackers or hackers will develop more ways of breaking into the system; making the devices face a new range of security threats. Therefore, there was need to ensure adequate protection of internal network from attackers. To achieve this, there are so many tools at the disposal of the network administrator and the security administrator, which include; Intrusion Prevention System (IPS), Firewall Security System and the Intrusion Detection System (IDS). This work focused on the firewall system that filtered what goes in and comes out of the network. It had the ability to block an unauthorized traffic and allow authorized traffic using the Internet Protocol (IP) table to ensure a stable network.

7. References

1. Chapman, D. Brent, Zwicky, Elizabeth D.(1995), Building Internet Firewalls. O'Reilly media, ISBN 978- 1-56592-124-5, pp. I –XXVI,1-517
2. Wack, J. P., Carnahan, L. J. (1995), "Keeping Your Site Comfortably Secure: An Introduction to Internet Firewalls", NIST Special Publication 800-100 U.S. Department of Commerce
3. WEB_1 2005. Check Point Software Technologies Ltd. "Stateful Firewall Technology Products and Solutions", retrieved today 05/09/2014 from http://www.checkpoint.com/products/technology
4. NIST 2002. National Institute of Standards and Technology (NIST)."Guidelines on Firewalls and Firewall Policy".
5. Shay, W. A.,(2000). "Firewall", University of Wisconsin-Green Bay.
6. WEB_4 2005. "An Introduction to Network Firewalls and the Firewall Selection Process", retrieved from http://www.more.net/technical/netserv/tcpip/firewalls/
7. Stalling, W., (2002). Network Security Essentials Applications and Standards. Prentice Hall, pp. 345
8. Jones Anita K. and Sielken Robert S. (2000) "Computer System Intrusion Detection: A Survey", Department of Computer Science University of Virginia