International Journal of Engineering Research and Development
e-ISSN: 2278-067X, **p**-ISSN: 2278-800X, www.ijerd.com
Volume 6, Issue 5 (March 2013), PP. 112-118

Analysis of Firewall Policy Rules a Comparative Study

V. Anantha Krishna[1], Dr. T. Aruldoss Albert Victoire[2],

[1]Research Scholar, Department of Computer Science and Engineering, [2.]Asst.Professor, Department of Electrical and Electronics Engineering, Anna University Coimbatore, Coimbatore,India-641047

Abstract:- A firewall is a system for enforcing access control policy between two networks and is one of the most important measures to protect against network attacks. Firewalls traditionally protect the internal network from outside threats. But there has been increasing need for preventing the misuses of the network by the internal users which most previous firewalls overlook. Now a days, the Internet users are traditionally relied on the firewalls to enforce their security policy by protecting their local network systems from the network- based security threat and illegal data access. However, these controls do not provide a comprehensive solution to secure a private network connected to the Internet. Depending on the institution’s local policy, authentication may be restricted to computers located in offices in which there is an individual who is responsible for use of the machine. Such a policy may be enforced in order to provide some means of security against hacking remote services. This paper deals with how to simulate the Firewall based on different policy rules and Compare it with some other security system.

Keywords:- Network security, information Technology, Firewalls, Filtering, Policy, Rules, Threat.

I. INTRODUCTION

The Internet has made large amounts of information available to the average computer user at home, in business and in education. For many people, having access to this information is no longer just an advantage, it is essential. Yet connecting a private network to the Internet can expose critical or confidential data to malicious attack from anywhere in the world. Users who Connect their computers to the Internet must be aware of these dangers, their implications and How to protect their data and their critical systems. Firewalls can protect both individual Computers and corporate networks from hostile intrusion from the Internet, but must be understood to be used correctly.

A firewall protects networked computers from intentional hostile intrusion that could compromise confidentiality or result in data corruption or denial of service. It may be a hardware device or a software program running on a secure host computer. In either case, it must have at least two network interfaces, one for the network it is intended to protect and one for the network it is exposed to. A firewall sits at the junction point or gateway between the two networks, usually a private network and a public network such as the Internet. The earliest firewalls were simply routers. The term firewall comes from the fact that by segmenting a network into different physical sub networks, they limited the damage that could spread from one subnet to another just like fire doors or firewalls. A firewall examines all traffic routed between the two networks to see if it meets certain criteria. If it does, it is routed between the networks, otherwise it is stopped. A firewall filters both inbound and outbound traffic. It can also manage public access to private networked resources such as host applications. It can be used to log all attempts to enter the private network and trigger alarms when hostile or unauthorized entry is attempted. Firewalls can filter packets based on their source and destination addresses and port numbers. This is known as address filtering. Firewalls can also filter specific types of network traffic. This is also known as protocol filtering because the decision to forward or reject traffic is dependant upon the protocol used, for example HTTP, ftp or telnet. Firewalls can also filter traffic by packet attribute or state.

A firewall cannot prevent individual users with modems from dialing into or out of the network, bypassing the firewall altogether. Employee misconduct or carelessness cannot be controlled by firewalls. Policies involving the use and misuse of passwords and user accounts must be strictly enforced. These are management issues that should be raised during the planning of any security policy but that cannot be solved with firewalls alone. Anyone who is responsible for a private network that is connected to a public network needs firewall protection. Furthermore, anyone who connects so much as a single computer to the Internet via modem should have personal firewall software. Many dial-up Internet users believe that anonymity will protect them. They feel that no malicious intruder would be motivated to break into their computer. Dial up users who have been victims of malicious attacks and who have lost entire days of work, perhaps having to reinstall their operating system, know that this is not true. Irresponsible pranksters can use automated robots to scan random IP addresses and attack whenever the opportunity presents itself. There are two access denial methodologies used by firewalls. A firewall may allow all traffic through unless it meets certain criteria or it may deny all traffic unless it meets certain criteria. The type of criteria used to determine whether traffic should be allowed through varies from one type of firewall to another. Firewalls may be concerned with the type of traffic or with source or destination addresses and ports. They may also use complex rule bases that analyze the application data to determine if the traffic should be allowed through. How a firewall determines what traffic to let through depends on which network layer it operates at.

1.1.Security Issues: Practical Considerations: Currently, most web sites are simply vehicles for disseminating information such as corporate profiles and descriptions of products /services For owners of such sites, the greatest concern is keeping unauthorized users from accessing the site and corrupting their data. But as business increasingly embrace true electronic commerce taking orders on-line, accepting credit cad info and digital-cash payments, both companies and their customers will demand higher levels of security.

1.1.1. Vulnerabilities of the web:-Businesses are looking to internet to achieve a global presence and become more accessible to catering to customers. Web site consist of 1. an application (the server) running on a local operating system 2. data (web pages) stored in a local database or file management system. As such, web sites are vulnerable to all the techniques that intruders have been developing for years to attack operating systems and databases

1.1.2.Principal threats:- There are 4 principal threats such **as** unauthorized alteration of data, unauthorized access to the underlying operating systems, eavesdropping on messages passed between a server and a browser and impersonation.

At first glance, the chances of the first two breaches occurring may appear negligible. After all, If a server is dedicated to web site access, what can potential intruders really do, aside from executing relatively simple commands allowing them to view information. But already weaknesses are becoming apparent.

1.2. Securing a Web site : There are two basic lines of attacks in improving Web security 1. securing the site itself and 2. securing the applications running on the sites. Both are essential.

1.2.1.Securing the site :- Install all operating system security patches recommended by the vendor, the Department of energy's computer incident advisory capability and the computer emergency responses team. After that, it is a matter of keeping up with the latest security advisories and promptly installing patches as flaws turn up.

1.2.2. Securing the application running on it:- Install the web sever software with minimal system privileges. If full privileges are given, anyone who gets past the server and into its file directory has access to everything on the system including additional applications, pass word files and other critical information.

There are several new technologies that can be used to improve use authentication. These technologies include the following:

1.3.Message digest: A calculation performed on a message. The calculation is based on a secret key. Message digests are used in a login authentication scheme called the "Challenge Handshake".

1.4.Public-key-encryption:-A method of encryption for which the key used to encrypt a message is different from the key used to decrypt the message. The public key is made available to anyone who needs to communicate. They encrypt the message to be sent with that key, but only user can decrypt it. This is based on practical methods used to encrypt entry forms and email.

1.5.Use of a firewall:- This offers the most common and effective approach by far. A firewall is an application software that sits on a computer between user LAN and the Internet. All Internet messages must pass through the firewall. To reach the server from the internet, user must have a firewall account that defines users user ID, password, group ID, system administrator and given permissions. Permissions include any combination of reading, writing or execution files in the network.

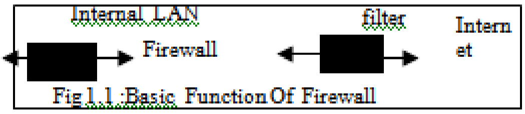


Fig 1.1 :Basic Function Of Firewall

The complete framework of firewall testing should contain two components: (1) generating test packets that test the firewall given a certain policy, and (2) generating various policies scenarios to test the firewall handling of different policy styles/configuration. Although both are needed to claim a complete testing environment for firewalls, our focus is on the first problem, *i.e.*, given a firewall/policy, how to ensure that the firewall implements this policy configuration correctly.

II. FIREWALL DESIGN PRINCIPLES:

Information systems in corporations, government agencies and other organizations have undergone a steady evolution:
1.Centralized data processing system, with a central mainframe supporting a number of directly connected terminals.
2.Local area networks (LANs) interconnecting PCs and terminals to each other and the mainframe.
3.Premises network, consisting of a number of LANs, interconnecting PCs, servers and perhaps a mainframe or two.
4.Enterprise-wide network, consisting of multiple, geographically distributed premises networks interconnected by a private wide area network (WAN).
5.Internet connectivity, in which the various premises networks all hook into the Internet and may or may not also be connected by a private WAN.

Internet connectivity is no longer optional for organizations. The information and services available are essential to the organization. Moreover, individual users within the organization want and need Internet access, and if this is not provided via their LAN, they will use dial-up capability from their PC to an Internet service provider (ISP). However, while Internet access provides benefits to the organization, it enables the outside world to reach and interact with local network assets. This creates a threat to the organization. While it is possible to equip each workstation and server on the premises network with strong security features, such as intrusion protection, this is not a practical approach. Consider a network with hundreds or even thousands of systems, running a mix of various versions of UNIX, plus Windows. When a security flaw is discovered, each potentially affected system must be upgraded to fix that flaw. The alternative, increasingly accepted, is the firewall. The firewall is inserted between the premises network and the Internet to establish a controlled link and to erect an outer security wall or perimeter. The aim of this perimeter is to protect the premises network from Internet-based attacks and to provide a single choke point where security and audit can be imposed. The firewall may be a single computer system or a set of two or more systems that cooperate to perform the firewall function. In this section, we look at the general characteristics of firewalls.

2.1.Firewall Characteristics:- The following design goals for a firewall:
1. All traffic from inside to outside, and vice versa, must pass through the firewall. This is achieved by physically blocking all access to the local network except via the firewall.
2. Only authorized traffic, as defined by the local security policy, will be allowed to pass. Various types of firewalls are used, which implement various types of security policies.
3. The firewall itself is immune to penetration. This implies that use of a trusted system with a secure operating system. Generally there are four techniques that firewalls use to control access and enforce the site's security policy. Originally, firewalls focused primarily on service control, but they have since evolved to provide all four:

2.1.1.Service control: Determines the types of Internet services that can be accessed, inbound or outbound. The firewall may filter traffic on the basis of IP address and TCP port number; may provide proxy software that receives and interprets each service request before passing it on; or may host the server software itself, such as a Web or mail service.

2.1.2.Direction control: Determines the direction in which particular service requests may be initiated and allowed to flow through the firewall.

2.1.3.User control: Controls access to a service according to which user is attempting to access it. This feature is typically applied to users inside the firewall perimeter (local users). It may also be applied to incoming traffic from external users; the latter requires some form of secure authentication technology.

2.1.4.Behavior control: Controls how particular services are used. For example, the firewall may filter email to eliminate spam, or it may enable external access to only a portion of the information on a local Web server.

2.2.The following capabilities are within the scope of a firewall:

1. A firewall defines a single choke point that keeps unauthorized users out of the protected network, prohibits potentially vulnerable services from entering or leaving the network, and provides protection from various kinds of IP spoofing and routing attacks. The use of a single choke point simplifies security management because security capabilities are consolidated on a single system or set of systems.
2. A firewall provides a location for monitoring security-related events. Audits and alarms can be implemented on the firewall system.
3. A firewall is a convenient platform for several Internet functions that are not security related. These include a network address translator, which maps local addresses to Internet addresses, and a network management function that audits or logs Internet usage.
4. A firewall can serve as the platform for IPSec. Using the tunnel mode capability, the firewall can be used to implement virtual private networks.

2.3.Firewalls have their limitations, including the following:

1. The firewall cannot protect against attacks that bypass the firewall. Internal systems may have dial-out Capability to connect to an ISP. An internal LAN may support a modem pool that provides dial-in capability for traveling employees and telecommuters.
2. The firewall does not protect against internal threats, such as a disgruntled employee or an employee who unwittingly cooperates with an external attacker.
3. The firewall cannot protect against the transfer of virus-infected programs or files. Because of the variety of operating systems and applications supported inside the perimeter, it would be impractical and perhaps impossible for the firewall to scan all incoming files, e-mail, and messages for viruses.

III. DESIGNING OF FIREWALL

3.1 Processing Model:- Packet filtering is a core functionality of network firewalls. The main idea is that the firewall resides on a network Node (Host or Router) and inspects all network traffic. Inspection is performed in accordance to network security policy. Based on this policy, the firewall makes a decision regarding what action to perform on a given packet. The most commonly performed actions are:

Accept the packet is permitted to pass through

Deny/Drop the packet is silently dropped

3.2 Policy:- The firewall's behavior is controlled by the "Policy". Policy consists of "Rules. Each rule consist of condition and action. Condition describes the criteria used to match individual packets. Action describes the activity to be performed if matches have been made. Basic conditions consist of tests, matching individual fields of the packet such as source address, destination address, packet type, etc. In the case of stateful inspection, connection-related variables like connection state could be checked. Finally, various system state variables like current time of day, CPU load, or system-wide configuration parameters could be taken into account. The condition could be viewed as a predicate. Usually, for a packet to match a condition, all tests must be satisfied (logical conjunction).The sequence of rules processing differs significantly between various firewall implementations. There are two common matching strategies: "single trigger" processing means that an action of the first matching rule will be performed. "multi-trigger" processing means that all rules will be matched and an action from the last matching rule will be performed. Some firewalls like ipfilter support "multi-trigger" policy by default, but allow individual rules to specify quick option which signifies that no further processing should be done on matched packet. Some firewall like iptables have even more complex processing logic, which allows for branching by organizing rules in into chains and providing special actions to redirect control from one chain to another.

IV. FORMAL MODELS

One direction of research is the definition of special high-level languages (sometimes graphical) to describe firewall policy. In such languages, the policy representation is translated to the native policy description language of an actual firewall platform. Examples are: Firewall Builder, HLFL, FLIP, Firmato, INSPECT, ,XACML. Some of these languages allow user to describe the policy of a single firewall, while others allow user to define an organization security policy which is translated to policy files for multiple firewalls. The research in this area is fragmented. A single, generally accepted mathematical model describing firewall policies is yet to emerge. Below we highlight some of the work in this area: Ehab S. Al-Shaer and Hazem H. Hamed ,use fixed rule structure, they call "5-tuple filter": order, protocol, src ip, src port, dst ip, dst port, action In order to formally model firewall policy, these researchers start by defining the relationship between rules in the policy.

Then they define the following relations between two rules: "completely disjoined", "exactly matched", "inclusively matched", "partially disjoing", "correlated". Next Al-Shaer and Hamed proved that these relationships are distinct and that their union represents the universal set of relations between any two k-tuple filters in a firewall policy. The policy is represented as a single-rooted tree, where each node represents a field of a filtering rule and each branch at this node represents a possible value of the associated tree.

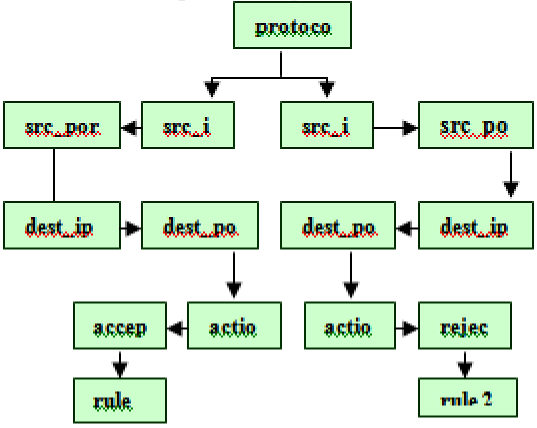


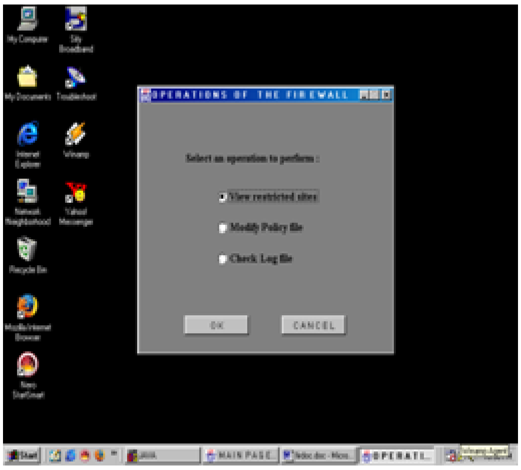
Fig 3: Example of policy representation as a tree string

4. Simulation Process:- This firewall is packet filtering system based on policies working at windows. This policy database is stored Ms_Access is configurable with JAVA as a language tool. This task is carried out by a simple JDBC-ODBC driver that delivers policies from ms_access to user space depending on configured policies, the firewall will either drop or allow the packet into the network. Different policies are to be configured for incoming and outgoing packets arriving on different interfaces, taking into consideration the arrival time of the packets , the source and destination IP address, source and destination ports and protocol. Also considering sub_nettting, overcoming the internal spoof attacks and NAT(Network Address Translation) taking us a step further in making our firewall run more efficiently. This project developed with Java language in win 2000 environment to run over multi home host. The steps involved in creating a firewall policy are as follows: 1.Identification of network applications deemed necessary 2. identification of vulnerabilities associated with applications 3.Cost-benefits analysis of methods for securing the applications 4. Creation of applications traffic matrix showing protection method, and implementing a firewall rule set 5. Creation of firewall rule set based on applications traffic matrix.

4.1. Main Objectives: The main objectives are A. To sniff the packets B. To accept or reject the packet based on specific policies defined over a. source IP Address b. Destination IP Address c. Protocol d. Source Port e. Destination Port C. To develop a stateless packet filtering system with additional capabilities such as overcoming internal spoofing

4.2. Assumptions & Constraints: The firewall we designed for a single host computer will function the same when placed in a router, which is connected to an external network.1. This firewall requires windows Platform**.** 2. We are capturing the packets at IP Layer only

V. SAMPLE SCREENS


OPERATIONS OF THE FIREWALL

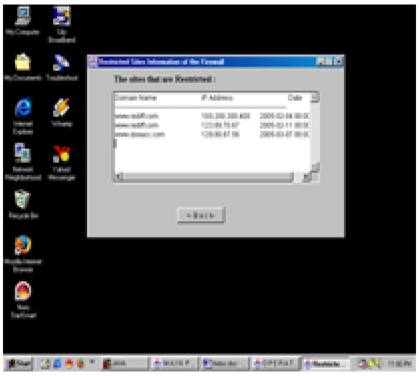
Select an operation to perform :

● View restricted sites

○ Modify Policy file

○ Check Log file

Fig5.1: This screen shows a pop up menu that to view the restricted web sites through this firewall.

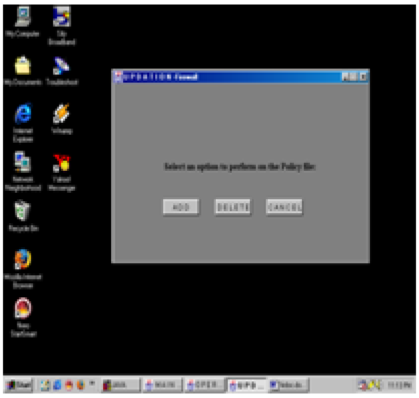


Restricted Sites Information of the Firewall

The sites that are Restricted :

Domain Name	IP Address	Date
www.rediff.com	100.200.300.400	2005-03-04 00:0
www.rediff.com	123.89.78.67	2005-03-11 00:0
www.[illegible].com	129.00.67.56	2005-03-07 00:0

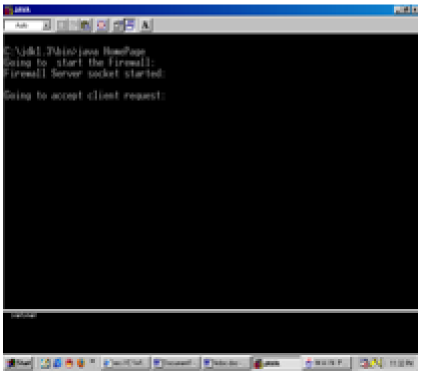
Fig5.2: This screen shows the restricted web sites through this firewall.



OPERATION Firewall

Select an option to perform on the Policy file:

Fig5.3: This screen shows a pop up menu that to allow add/delete new policy to this firewall.



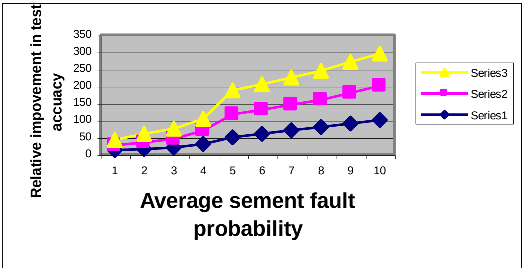
```
C:\jdk1.3\bin>java HomePage
Going to  start the Firewall:
Firewall Server socket started:

Going to accept client request:
```

Fig5.4: This screen shows one of the two operations that can be performed on the list of Restricted Sites as accept.

VI. TESTING THE PROJECT

The complete framework of firewall testing should contain two components: (1) generating test packets that test the firewall given a certain policy, and (2) generating various policies scenarios to test the firewall handling of different policy styles/configuration. Although both are needed to claim a complete testing environment for firewalls, the researcher in this study focuses on the first problem, i.e., given a firewall/policy, how to ensure that the firewall implements this policy configuration correctly. Testing the firewall by exhaustively injecting all possible packets into the firewall will be enough. However, this is infeasible due to the huge number of packets needed. Even if we try to restrict the test traffic to the range of relevant.

Evaluation of different factors affecting the improvement in the firewall test accuracy relative to random-sampling test.



VII. CONCLUSION

The project “firewall implementation ” facilitates the working of internet access in the most efficient and restricted way. All the requirements were considered while developing this application. The project is complete in the sense it meets all the requirements of the establishment Grievance Cell. Even then there is always a scope for improvement. Keeping in view the user-friendly approach required for the package, certain standards of the corporation are followed. The project “Firewall Implementation”, facilitates the better restrictions which can be imposed by the administrator, in a user-friendly manner. Our policy structure concentrates mainly on the basic five tuples.

REFERENCE

[1]. E. Al-Shaer and H. Hamed. “Firewall Policy Advisor for Anomaly Detection and Rule Editing.” IEEE/IFIP Integrated Managem

[2]. Alex X. Liu, *Member, IEEE,* Mohamed G. Gouda, *Member, IEEE “*Diverse Firewall Design*”*

[3]. Rongbo Du, Rei Safavi-Naini and Willy “Design and Implementation of A Content Filtering Firewall”

[4]. William Stallings “Cryptography and Network Security Principles and practices” pearson 2nd edition.

[5]. Asian Journal of Information Technology –Med well Journal online-ISSN1682-3915 –2007.

Biographie: Anantha Krishna V received his M.C.A degree from Sri Venkateswara University and M.Tech. Degree in Computer Science and Engineering Degree from Osmania University, India. With more than 10 years of teaching experience in various reputed Engineering Colleges in and around South India, he is now working as Assistant Professor in the Department of Computer Science & Engineering at Aalim Muhammed Salegh College of Engineering, Chennai. He is a life member of Indian Society of Technical Education (ISTE) and Student member of Institute of Electrical and Electronic Engineers.

He has presented many technical papers in International Conference and published papers in reputed International Journal. He has participated and coordinated several Faculty Development Programmes, workshop, seminars and conference.

His other areas of interests are Network security, Mobile Computing, Ad hoc networks, Wireless sensor Networks, Distributed systems and Multicast Distribution. And his career plan is to continue the research in the wireless networking area.