Firewall technology in network security

Tushar Wason, Anubhav Chandra
Student, Department of Information Technology
Dronacharya College of Engineering, Gurgaon, Hr, India

***Abstract*—This paper analyzes the network security features and the main threat , on the basis of various firewalls' principles, advantages and shortcomings. Through the synthesis and compare of various techniques, in-depth study of the main factors affection firewall performance, combined with the network status quo of Heilongjiang Provincial Center, this paper researches the firewall technology of the actual application in the computer network security, then refers the new technique called tight coupling firewall, finally the article leads to a lack of firewall technology and the direction of its development.**

***Index Terms*- Firewall, Network Security, wire shark, ip tables**

I. INTRODUCTION

Network security is an important task that must be seriously considered when designing a network. Network security is defined as the policies and procedures followed by a network administrator to protect the network devices from threats and simultaneously, the unauthorized users must be prevented from accessing the network. Network firewalls are devices or systems that control the flow of traffic between networks employing different security postures. The

network traffic flow is controlled according to a firewall policy. The filtering decision is based on a firewall policy defined by network administrator. For each type of network traffic, there are one or more different rules. Every network packet, which arrives at firewall, must be checked against defined rules until first matching rule is found. The packet will be then allowed or banned access to the network, depending on the action specified in the matching rule Packet filtering allows you to explicitly restrict or allow packets by machine, port, or machine and port. For instance, you can restrict all packets destined for port 80 (WWW) on all machines on your LAN except machine X and Y. Ip firewalls are used to set up, maintain, and inspect the tables of IP packet filter rules in the Linux kernel. Several different tables may be defined. Each table contains a number of built-in chains and may also contain user- defined chains.

II. FIREWALLS

While in theory firewalls allow only authorized communications between the internal and external networks, new ways are always being developed to compromise these systems. However, properly implemented, they are very effective at keeping out unauthorized users and stopping unwanted activities on an internal network. Firewall systems protect and facilitate your network at a number of levels. They allow e-mail and other applications, such as file transfer protocol (FTP) and remote login as desired, to take place while otherwise limiting access to the internal network. Firewall systems provide an authorization mechanism that assures that only specified users or applications can gain access through the firewall. They typically provide a logging and alerting feature, which tracks designated usage and signals at specified events. These systems offer address translation, which masks the actual name and address of any machine communicating through the firewall. For example, all messages for anyone in the technical support department would have his/her address translated to techsupp@company.com, effectively hiding the name of an actual user and network address. Firewall system providers are adding new functionality, such as encryption and virtual private network (VPN) capabilities.

Firewall systems can also be deployed within an enterprise network to compartmentalize ifferent

servers and networks, in effect controlling access within the network. For example, an enterprise may want to separate the accounting and payroll server from the rest of the network and only allow certain individuals to access the information. Unfortunately, all firewall systems have some performance degradation. As a system is busy checking or rerouting data communications packets, they do not flow through the system as efficiently as they would if the firewall system were not in place.

III. NETWORK ADDRESS TRANSLATION

Firewalls often have network address translation {NAT} functionality, and the hosts protected behind a firewall commonly have addresses in the "private address range", as defined in RCF Firewalls often have such functionality to hide the true address of protected hosts. Originally, the NAT function was developed to address the limited number of IPv4 routable addresses that could be used or assigned to companies or individuals as well as reduce both the amount and therefore cost of obtaining enough public addresses for every computer in an organization. Hiding the addresses of protected devices has become an increasingly important defense against network reconnaissance.

IV. PASSWORD MECHANISMS

Passwords are a way to identify and authenticate users as they access the computer system. Unfortunately, there are a number of ways in which a password can be compromised. For Example, someone wanting to gain access can listen for a username password as an authorized user gains access over a public network. In addition, a potential intruder can mount an attack on the access gateway, entering an entire dictionary of words (or license plates or any other list) against a password field. Users may loan their password to a co-worker or inadvertently leave out a list of system passwords. Fortunately, there are password technologies and tools to help make your network more secure. Useful in ad hoc remote access situations, one-time password generation assumes that a password will be compromised. Before leaving the internal network, a list of passwords that will work only one time against a given username is generated. When logging into the system remotely, a password is used once and then will no longer be valid. Password aging is a feature that requires users to create new passwords every so often. Good password policy dictates that passwords must be a minimum number of characters and a mix of letters and numbers. Smart cards provide extremely secure password protection. Unique passwords, based on a challenge-response scheme, are created on a small credit-card device. The password is then entered as part of the log-on process and validated against a password server, which logs all access to the system. As might be expected, these systems can be expensive to implement. Single sign-on overcomes what can only be the ultimate irony in system security: as a user gains more passwords, these passwords become less secure, not more, and the system opens itself up for unauthorized access. Many enterprise computer networks are designed to require users to have different passwords to access different parts of the system. As users acquire more passwords—some people have more than 50—they cannot help but write them down or create easy-to-remember passwords. A single sign-on system is essentially a centralized access control list which determines who is authorized to access different areas of the computer network and a mechanism for providing the expected password. A user need only remember a single password to sign onto the system.

V. ANALYSIS OF FIREWALL ACTIVITY

There are several queries of the user about the usage and traffic control in firewall activity. Some of these enquiries are as follows:

- Particular source and target and their services which may be accessible by source should be investigated.
- Comparison between two distributed firewall to check their configuration and to enforce same policy.
- Investigation about the active firewall.
- The influence of a node compromises to interface the firewall.
- Investigation about the conducted policy configuration to meet the organization requirement.
- All the open ports that may not to be open to inbound or outbound of the available nodes should be disabled.
- The ports according to the organization policy, which require communicating, should be defined in firewall policy.
- Correctness of the rules updated on the basis of organization policy should be examined.

With the above examining procedure the firewall policy utilization based on its specification utilized and any similarity or conflict in the policy is indicated to the administrator.

As it is shown in firewall connectivity of TCP/IP after receiving the packets (inbound and outbound) firewall performs to open command to receive and initial its investigation. In next firewall is starting to validate the packet based on its policies and somehow updating. In the parallel activity, firewall check for monitoring the network topology and its status. For the first part after monitoring the packet it will check for filtering, relay or update, in the second, the network topology it checks for capability of this topology, and in last, the status for immediate action and response is checked.

VI. CONCLUSIONS

The Firewall which works as the gateway for the network should be configured in such a way that it should not allow unauthorized users entering the network or accessing the information. Network audit informationsuch as log messages and network monitoring tool's record will also help in securing the network by providing information about the network access In this research paper, work has been done on capturing the live traffic using the network protocol analyzer Wire shark and on the basics of analyzed data packets further explored and designed the script using Ip firewalls to allow/deny the network traffic on the basics of the IP address of the computer sending the packets, the IP address of the computer receiving the packets, the type of packet (TCP, UDP, etc.), The port number, and URL's etc.This enables us to protect our system from a wide variety of hazards, including service attacks and hack attempts. The script discussed here can be used for the purpose of network Security. From this implementation and research of enhancing network security, we found that; security is not only limited in choosing a secured operating system or secured server configurations, but also related to both physical and application security configured in the network. Moreover, periodical enhancement of network security is to be performed in order to get rid of day to day attacks. Servers which contain important information are to be configured securely and placed in a secured environment.

REFERENCES

[1] http://ijircce.com/upload/2013/april/40_Distributed_H.pdf

[2] https://www.cerias.purdue.edu/assets/pdf/bibtex_archive/96-07.pdf

[3] http://www.jatit.org/volumes/research-papers/Vol4No2/Operating%20System%20Security%20(OSS),%20File%20Transfer%20Protocol%20(FTP),%20Virtual%20Private%20Network%20(VPN),%20Digital%20Encryption%20Standard%20(DES),%20Pretty%20Good%20Privacy%20(PGP),%20Privacy%20Enhanced%20Mail%20(PEM)..pdf

[4] http://www.ijarcsse.com/docs/papers/8_August2012/Volume_2_issue_8/V2I800280.pdf

[5] http://en.wikipedia.org/wiki/Firewall_(computing)