Enhancement of Firewall Filtering Techniques

Dilbag Singh¹, Richa Sharma² and Tajinder Singh³

¹ Global Institutes of management & emerging Technologies,
        Sultan wind Roud, 15/100, Amritsar

² Global Institutes of management & emerging Technologies,
        GIMET, Amritsar

³ Global Institutes of management & emerging Technologies,
        GIMET, Amritsar

Abstract: Network attacks are increasing both in number as well as complexity. Most of the Internet users depend on the firewalls to enforce their security policy. In this paper, we have focused on the origin, definition, functionalities, types and techniques of Firewalls. We have also focused on the new technique “Deep Content Inspection” and how it works. This paper covers how DCI is more beneficial than the rest of the techniques as well as where we can use Deep Content Inspection in future.

Keywords: Network, Firewall, Filtering, DCI.

1. INTRODUCTION

The internet is widely used in every field all over the world. At first the internet was built only as research-oriented and the communication protocols were designed for a non-malignant environment that now exists [2]. But with the time going on the internet is limited steadily from the initial one and its environment is less reliable. In the present day when the users are connected to internet they are enabled to reach and communicate with the outside world through the Internet [7]. Therefore it is very important for the user to protect their local system from the spiteful attacks from outside [13].

In the present time MNC Companies are doing their Business on the Internet. Secured Internet is heavily needed. One of the best solutions of this issue is firewall. Firewall is a set of rules which provide the authorize network access. The firewall technology was emerged in 1980s [11]. The firewall is a security system that controls the incoming data, analyzing the data packet and determining whether it is authorized or not.

The data travels on network in the form of the Packets. Firewall is responsible to scan the each packet for analysis that the coming packet is allowed or not. Therefore the firewall is a filtering Mechanism placed between the private network and outside world, so that traffic is pass through it to prevent unwanted access. Firewall protects computer from outside attacks via internet. The set of rules for filtering is known as the Policy [6]. When the Policy is created and it has been specified, the firewall needs to test to determine whether the policy implemented correctly or not.

Most of the firewalls implement the first match phenomenon. This means that if the first rule of the policy matches with the match field in the packet, it stops and discards all the packets which matches the rule. The packet matching involve on field from the TCP, UDP and IP Packet header. There is need to implement vary efficient matching algorithm to be deployed in modern firewalls to ensure that the firewall does not become a bottleneck.

The categories of Packet filtering are as follows.

- Basic Packet Filtering
- Stateful Packet Filtering

The first Generation firewalls used the basic packet filtering [4]. In this technique the firewall keeps no state. The Filtering decision is made for every packet. The Filtering determine based on the five basic fields. Source and destination IP address Protocol and Source and destination port numbers.

In the present days Stateful packet filtering [4] is used. In the Stateful technique the firewall keeps track of established flow and all packets that belong to and exiting flow, in the both direction are allowed to cross the firewall. This is done by keeping an entry in a Cache for each open flow. When first packet of new flow is allowed to enter the firewall then firewall inserts a entry in the Cache.

Types of firewalls [3]:-

- Packet Filter Firewall
- Stateful Inspection Firewall
- Application Gateway Firewall
- Circuit Level Gateway Firewall
Packet Filtering Firewall: This type of firewall is configured to filter packets on both directions[5]. Filter rules are based on information contained in network packets: Source IP Address, Destination IP Address, Source and Destination transport level address, IP protocol Field, Interface[7]. Fig. a shows the Packet Filtering firewall.

If one of the rule is matched then that rule is invoked to determine whether to forward or discard the packet. If there is no match to any rule then a default action is taken. There are two default policies possible. Default-Discard:- which is not expressly permitted is prohibited.

Default-Forward:- that which is not expressly prohibited is permitted.

A simple packet filter firewall permits the inbound traffic on high numbered ports for TCP Traffic. This thing creates the vulnerability that can be exploited by hackers (Unauthorized access).

Stateful Inspection Firewall [5]: - This type of firewall makes the decision based on the individual packet basis and does not consider any higher layer context. Most of the applications that run on the top of the TCP flow are client server Model [10]. A Stateful inspection firewall defines strict rule for the TCP traffic by making a directory of outgoing TCP connection. Stateful Inspection filtering stores the information about TCP Connection. When any packet is passed through the firewall it inserts the entry in cache. The Stateful inspection firewall is more secure than the Packet filtering firewall. Fig. (b) Shows the Stateful Inspection Firewall.

Application Gateway Firewall: - this firewall operates in Application layer of OSI Model. Application Gateway firewall generally a proxy Server which does not allow user to directly enter in the Network [7]. By the help of application gateway the firewall may be less transparent. This type of firewall logs all the activities on the network. The application layer firewall is also classified as isolation networks.

This firewall is based on computer or routers for the application level protection there is two common technologies are proxy firewall and intrusion protection system. These types of firewalls maintain complete connection state and sequencing information at application layer. This firewall may manage traffic for HTTP & FTP services.

After the network processing on the packet the data of packet passed through the kernel space to application space then to the proxy server that is working on specific TCP or UDP port. Fig (c) Show the application gateway firewall.

The application gateway firewall classified in two types:
1. Network based application gateway firewall (see fig. c.1)
2. Host based application gateway firewall (see fig. c.2).

The network based application gateway firewall is also known as a proxy based or reverses proxy based firewall. These types of firewall blocks the specified context, such as websites, viruses etc.

Host based application gateway firewall can monitor any application input, output or system services calls made
from to or by an application. The host based firewall only provides the protection to application running on the same host. Host based application firewall may also provide network based application filtering.

(c.2) Host based application gateway firewall

**Circuit Level gateway firewall [7]:** - The circuit level gateway firewall is similar to the application level gateway firewall, but only one thing is different which is that instead of the interfering host computer an isolated sub-network is created between the external and internal networks. In some others words we can say that it is specialized function performed by application level gateway for certain application. The circuit level gateway used in a situation in which the administrator trust on internal users. The gateway configured to support application level for internal connection and circuit level for the outbound connection. This firewall is works on Transport layer. In this firewall the process is to create a virtual circuit between the internal clients and proxy server. Clients send the request to the server and server forward the request to internet after changing the IP address. Only Server IP address is visible to the external user. These types of connection are only used to connect Trusted Internal clients to the Internet. (See Fig. (d).

(d) Diagram of circuit level gateway firewall [3]

**Common Attacks on Firewalls [3] [7]:** -The following attacks are occurred on the basic packet filtering firewall.
1. IP address spoofing
2. Source routing attacks
3. Tiny fragment attacks
4. Port Scan[12]
5. Network Traffic flood
6. Malformed network packet
7. Fragmentation attacks

**Present Techniques Used in Firewall [8]:** -
In the early generation firewall only the packet header and packet footer were scanned for the filtering and the security was provided only on the specific port which was configured in the firewall. But in present days techniques filter the packet by scanning the data part of Packet also [14]. This technique use pattern/string matching phenomenon and the technique is named as **Deep Content Inspection [8].**

The Deep content Inspection technique provides the services which keep tracks of each packet connection so that if there is need to find packet it can be found immediately [9]. This technique works on all 7 layers of the OSI Model. This technique is used by the Wedge Networks. (See Fig. (f).

(e) The Layer Architecture of Diagram of Deep Content Inspection [8]

**Features provided by DCI [9]**
This technology has ability to extract digital objects from the data.
This technology support both explicit Proxy mode and transparent proxy mode.
This technique provides ICAP and WCCP support for the explicit proxy mode which cause the network reconfiguration cost is reduced.
It supports Unlimited VLAN’s.
In the Deep content Inspection the filtering Policies managed by the software module and you can manage the anti-malware, HTTP, POP, LDAP, Radius and subnets of networks etc [14].The policies is managed according to the time based means specific period of time (see fig. (f)).

**Fig. (f) Deep Content Inspection Technique [1]**
CONCLUSION & FUTURE SCOPE:
Firewall is a set of rules which provide the authorize network access. There are two types firewall techniques used to filter the packet. Basic packet filtering and Stateful packet technique. In basic packet filtering the firewall keeps no state whereas Stateful packet filtering the firewall keeps the states. We have covered all the four firewall techniques that are packet filter firewall, Stateful inspection firewall, and application gateway firewall and circuit level gateway firewall as well as the different attacks. But now days a new firewall technique has come into account named as “Deep Content Inspection”. It has a special feature as compare to the previous techniques that is, in this the data part/field are also scanned along with header and footer which prevent them from attacks that are present in the data part/field. In future it is difficult to know what services subscribers want, but based on the behavior of today’s consumers, tomorrow must have a mixture of content based services and additional value added services that give rise to denial of service protection and parental control. This can be achieved by deep content inspection technique. Based on their opens and compliance with industry standard, their proven capabilities and their performance reputation DPI system are becoming more popular.

References:-
Middle boxes Reduce Security”, University of Michigan.

AUTHOR

Dilbag Singh Completed his Diploma in Computer Science & Engineering from Punjab State Board of Technical Education and Industrial training in 2008 and is presently pursuing A.M.I.E from Institution of Engineers, India. He is also working as an instructor at Global Institute of management & emerging Technologies.

Er. Rich Sharma received the B.Tech in Computer Science & Engineering from Punjab Technical University and at present now pursuing M.Tech in computer science and engineering from Punjab technical university. He is Working as an assistant professor at Global Institute of management & emerging Technologies.

Er. Tajinder Singh received the B.Tech in Computer Science & Engineering from Punjab Technical University and M.Tech in Computer Science & Engineering from Punjab Technical University. He is Working as Assistant professor in Global Institute of management & emerging Technologies.