ANALYTICAL STUDY OF PACKET FILTERING FIREWALL

Akanksha Chaudhary
School of Computing Science and Engineering
Galgotias University
Greater Noida,India
myself.akanksha.chaudhary@gmail.com

Dr.Shrddha Sagar
School of Computing Science and Engineering
Galgotias University
Greater Noida,India
shrddha.sagar@galgotiasuniversity.edu.in

Abstract: Firewall is a network security device which manages, monitors and control the flow of traffic into and out of a network. It is a hardware and software based or combination of both. It establishes a barrier between secured inner network and outer unsecured network, such as internet. Firewall are generally installed to prevent attacks.

Keywords-Firewall, Packet Filtering, Traffic, Attack

1.OBJECTIVE

The security enhancement of the network and personal data is more important nowadays as attacking personal computers and intruding in personal data is increasing ,the terms and policies of the firewall need to be upgraded so that it can prevent the penetration of the security and attacks on the network and the system..
The main objective of a firewall is packet filtering. When a computer system sends a request over the Internet, it takes the shape of tiny packets of information, which travel through the network from source to their destination. The target server or system responds with its own packets of information or data, that come back on identical route. A firewall controls, monitors and manages each packet that passes through it, considering its source, destination and what style of information it contains, and it compares that information to its internal rule set. If the firewall detects that the packet is unauthorized or may contain any type of threats , it discards or rejects the information. Typically, firewalls permit traffic from common programs or sites such email or internet browsers, whereas rejecting most incoming requests. You can also configure a firewall to forbid access to certain websites or services to prevent employees, students or anyone from accessing irrelevant resources.
Moreover, the packet filtering rules within a firewall are only based on the network security's needs, even though it become harder to manage . Hence, there is a higher risk for mistakes to occur within the enterprise network.
Packet filtering firewall is a technique used to control and manage network access by monitoring outgoing and incoming packets or informations and permitting them to pass or halt based on the source and destination Internet Protocol (IP) addresses, protocols and ports.
Network layer firewalls outlined rule sets, which give extremely efficient security mechanisms.

Packet filtering can also be called static filtering. So to create the packet filter safer where we are working on sending the packet and receiving its acknowledgement, as we all know when the packet sent to the receiver therefore the receiver always provide the acknowledgment to the sender but sometimes when the package missed from receiver's side then the sender unable to get the proper acknowledgement on package missing ,so here we can fix this problem by which the proper acknowledgement will get to the sender, that package successfully reached or not to the receiver.

2.INTRODUCTION

Firewall means the wall which protects the network from fire, here fire means the unauthorized user or the attacker etc.
Its creates a barrier between trusted and untrusted network and it protects the confidential or private information as well as company from unethical use.
As we know the security of network from unauthorized access is the most important use of firewall security so first to analyze all types of attacks on the different firewall like-

- Packet filtering firewall
- Circuit level gateways
- Stateful inspection firewall
- Application level gateways or proxy firewall
- Next generation firewall

Firewall should be free from bugs and making the firewall 100% bug free.

Firewall is a network security device, both hardware or software based, which monitors and manages all incoming and outgoing traffic and supported by outlined set of security rules it accept, reject or drop that specific traffic.
Accept: permit the traffic.
Reject: block the traffic however reply with an "unreachable error".
Drop: block or forbid the traffic with no reply.

3.HISTORY AND NEED FOR FIREWALL

A specific IP address should be given permission or not to access the network is decided by the rules defined in ACLs.
But ACLs are unable to detect the behavior of packet it is blocking. To keep the network protected, ACLs along with other methods are used. The method was Firewall.

Internet connection is no longer required for the organizations. However, internet provides an upper hand to the companies. Connection between the outside network to the internal network is provided. This jeopardizes the security of the organization. Just to secure the internal network from such threats, Firewall is required.

4.HOW FIREWALL WORKS

The packets flowing in the network in matched against the rules described for the firewall. Associated action is taken over the packet, once the rules are matched. For example, a rule is defined that an employee from Project management cannot access the information of the Human Resource department.
As far as the matter of network traffic is concerned, it will move out or in the network. Distinct set of rules is maintained for distinct cases. Mostly, the packets going out of the network is less analyzed and easily allowed to pass.

Packets entering the network are examined differently. The categories of the incoming packets are mostly TCP, UDP or ICMP. Every packet contain destination address and source address as well. TCP and UDP have port numbers also but ICMP uses different technique of program to identify the purpose of a particular packet. ICMP does not uses port number.
Default policy: It is true that every rule of the firewall cannot be covered, so the requirement of Default policy is a prime concern. Default policy by default take the following actions:
(reject, accept or drop).
For instance, if no rule is defined on firewall about the connection of SSH to the server, then default policy will be followed. If default is set to accept, then SSH to server connection can be established outside your network. So, the default value which is preferred should be either drop or reject.

5.GENERATION OF FIREWALL

On the basis of generations, firewalls are divided into different categories-

First Generation:
Packet Filtering Firewall: As the name suggests, packet filtering firewall filters the incoming and outgoing packets based on their behavior. It manages and performs different operations such as dropping or blocking different factors such as protocols, destination and source protocol address and ports. Packet examining is done on the transport layer.
Every packet is examined and analyzed separately. Then don't have the protocol of functionality to gather whether a packet is the part of any traffic or coming stream. By seeing the Headers, the packets are accepted or rejected.
Acceptance or rejection of a packet is done by checking the filtering table maintained by the packet filtering firewall. For instance, the filtering table contains rules: Incoming packets from this source destined to this address via port 23, should be blocked. All services for 192.168.0.45 are allowed.
Second Generation:
Stateful inspection firewall: The work of this firewall is totally different from packet filtering firewall. It Captures the status of the packet connection making it more efficient than packet filtering firewall. This firewall monitors the path taken by the packet like TCP streams. Because of this, the filtering not only relies on predefined rules but also the path defined in the table would be the part of this process.
Third Generation:
Application Layer Firewall: This firewall works from physical layer to application layer in inspecting and analyzing the packets. Main feature of this firewall is to halt the misuse of protocols and application (like FTP,HTTP,SSH) and it also block some specific information. These firewalls are the host of proxy servers. The work of a proxy server is to prevent the connection between the sides of firewall. Based on predefined rules, the flowing traffic is either blocked or allowed.

Next Generation Firewall: In todays world where advance malware and viruses are use in cyber attacking, Next generation firewall are used to prevent these advance attacks. Inspection of application along with deep packet inspection is done under NGFW and many more functionalities exist to prevent and protect the machine from modern attacks.

6.TYPES OF FIREWALL

There are two types of firewalls:
1)Host-based
2)Network-based
Host-based firewalls: Every network node consist of a host based firewall which keep watch on every incoming and outgoing packets.Inside a network no such firewall have the protection which develops the need to install
host based firewalls. Any unauthorized access is blocked by the firewall.
Network based firewall: This type of firewall works on the network layer of Open Systems Interconnection model. These firwalls analyses all the packets comming front and forth from a port.
It protects the internal network by filtering the traffic using rules defined on firewall. Network-based firewall is usually a dedicated system with proprietary software.
COMODO FIREWALL
Many functionalities are there of this firewall including a Game mode,custom DNS servers etc which helps in blocking the process in a network. Handling programs to block and allow list is really appriciable.browing of the program would be sufficient.Many advanced features are also present in this firewall.Rating scan option is used to scan all the running processes and can be used if you suspect any amlfunctionality on your system.
Comodo KILLSWITCH is an advanced option which will make all the running process visible and can terminate as per your will.Comodo firewall installer is of 200 MB
Another free friewall which will block and helps you with hand full of notifications is TinyWall.It prompts like most other firewall software.One of the feature of this firewall is that it contains application scanner which added programs to the safe list of your system.You can either choose files,also choose the manual service which give firewall permissions permanentally or for a limited hours.
.Other features including the Autolearn mode in which we can choose among different programs you want to give access to such that open them and shut them down to add more quickly all the trusted programs in the safe list.

7.LITERATURE SURVEY

COMPARISION : Comparision here is shown between comodo firewall and Tinywall. As all the features above are shown above about both the friewalls, here are some points of comparision analysis.
As comodo firewall consists of different modes and features including a Game mode, custom DNS servers etc helps the network in blocking the firewall whereas TinyWall has an application scanner which runs on your system and adds program to its safe list.
Comodo has a advanced kill switch which kills all the running process which you select and shows it on your system's window wheras Tinywall provides you many features including choosing a file,a process and provides firewall permissions that are permanent or for a limited time period.

Comodokillswitch provide the user to kill or terminates all the background apps and software that are working or manually you want to kill.

One of the drawback of comodo firewall over tinywall firewall is it has a large file size of over 200 MB and it might create a problem in downloading and installing especially with the slower network but in case of tinywallfirewall,it just blocks the advertisement like all the other firewalls.

Tinywall firewall also added the computer file to a safe list.

BUT there is an advantage of tinywall firewall is that we can set it on autorun mode so that it can automatically select the files which it have to scan and which it have to leave.

Tinywall firewall monitors and see the packet transferring and send the report to the virus total,for online virus.

COMODO VS ZONEALARM

Comodo provides advance features which even high paid Antivirus cannot compete.	ZoneAlarm is free. It is used in conjunction with a separate firewall.
Comodo is a stand-alone antivirus that comes with advance features to defend a computer from any threat.	ZoneAlarm is usually used in conjunction with antivirus software because its most original feature is its outgoing firewall.
Comodo has a great detection rate.	ZoneAlarm has a weak detection rate.
Comodo is an ingoing firewall.	ZoneAlarm is an ingoing as well as outgoing firewall.
Comodo has less features as compared to ZoneAlarm.	ZoneAlarm has a lot of features, some of which are a necessity – such as protecting your Operating System when it's booting.
Comodo Antivirus can filter malicious email threats and is compatible with Qmail, Sendmail, and Exim MTA's.	ZoneAlarmhas a "stealth mode" that makes you invisible to attackers.

Comparison TABLE on the basis of firewall

throughput and vpn throughput.

Product	**Firewall Throughput (Rated)**	**VPN Throughput (Rated)**	**Maximum user**
Entry-level/Small Office UTM Appliances			
BarracudaX-series	1to1.9Gbps	100to200Mbps	100to200
Checkpoint NG Threat Protection appliances	750Mbpsto3Gbps	140to400Mbps	Upto100
CiscoMeraki	200Mbps	60 Mbps	40
Dell Sonicwall NSA Series	600 Mbps to 1.8 Gbps	150 Mbps to 1.1 Gbps	25 to 250
Fortinet Fortigate	799 Mbps to 2.4 Gbps	350Mbpsto1Gbps	10to60
JuniperSRXseries	700Mbpsto5.6Gbps	75to800Mbps	N/A
SophosSGseries	1.5to6Gbps	325Mbpsto1Gbps	Unrestricted
WatchGuard	200Mbpsto1.4Gbps	30to240Mbps	2900to500
MidrangeUTMAppliances			
BarracudaX-series	2.0 to 5.5 Gbps	250 to 750 Mbps	400 to 1000
Checkpoint NG Threat Protection appliances	3 to 30 Gbps	1.2 to 2.5 Gbps	Upto 1500
Cisco Meraki	250 to 750 Mbps	70 to 200 Mbps	500
Dell Sonicwall NSA Series	3.4 to 9 Gbps	1.5 to 4.5 Gbps	1000 to 4000
Fortinet Fortigate	8 to 16 Gbps	200 Mbps to 14 Gbps	600 to 2000
JuniperSRXseries	7 to 55 Gbps	1.25 to 14.5 Gbps	NA
SophosSGseries	10 to 26 Gbps	1.0 to 5.0 Gbps	Unrestricted
Watch Guard	2to 14 Gbps	250 Mbps to 10 Gbps	Unrestricted
High-end UTM Appliances			
Checkpoint NG Threat Protection appliances	77 to 110 Gbps	17Gbps to 50 Gbps	1500+
Cisco Meraki	1 Gbps	500 Mbps to 1 Gbps	10000
Dell Sonicwall NSA Series	12 Gbps	5 Gbps	6000
Fortinet Fortigate	10 to 45 Gbps	17 to 25 Gbps	20000
JuniperSRXseries	65 Gbps to 2Tbps	22 to 100 Gbps	N/A
SophosSGseries	40 to 60 Gbps	8 to 10 Gbps	Unrestricted
WatchGuard	10 to 35 Gbps	2 to 10 Gbps	Unrestricted

8.CONCLUSION

After comparing the all following networks,we can say that the BARRACUDA X series is best network firewall on the basis of firewall throughput and vpn throughput because Barracuda NextGen Firewalls are a cornerstone of our Total Threat Protection framework, that integrates purposely, best-of-breed, highly scalable and provides highly secure solutions to protect users, networks, and data center applications. Components like internet, email, web application, and secure remote access integrate with the firewall.

9.THE FUTURE OF FIREWALL

Firewalls can be used as both software and hardware applications, Firewalls have to be able to perform real-time network traffic introspection and controlling without affecting throughput. A set of rules that filters and monitors data packets impacts network performance and causes bottlenecks.

The future firewall must differentiate between legitimate and illegitimate traffic automatically to identify and detect threats or on the fly.Firewall must control and manage all types of security faults. Firewall must detect attacks or threats and inform the user about that .

10.REFERENCES

[1] Imran, Mohammad, Abdulrahman Algamdi, and Bilal Ahmad. "Role Of Firewall Technology In Network Security". International Journal of Innovations & Advancement in Computer Science. Print [04.02.2016].

[2] Taluja, Sachin, and Pradeep Kumar. “Network Security Using IP Firewalls". International Journal of Advanced Research in Computer Science and Software Engineering. Print [05.02.2016].

[3] M .malik and R. pal, (2013).”Impact of Firewall and VPN for WLAN”. International Journal of Advanced Research in Computer Science and Software Engineering. Print [05.02.2016].

[4] S.C. Tharaka, R.L.C. Silva, S. Sharmila, S.U.I. Silva, K.L.D.N Liyanage, A.A.T.K.K. Amarasinghe, D. Dhammearatchi, ”High Security Firewall: Prevent Unauthorized Access Using Firewall Technologies”, IJSRP, Volume 6, Issue 4. Print April 2016 Edition[ISSN 2250-3153]

[5] Dr. Ajit singh , Madhu Pahal , Neeraj Goyat. “A Review Paper On Firewall”, (IJRASET), Vol. 1 Issue II. Print September 2013[ISSN: 2321-9653].