NETWORK SECURITY TOOLS: FIREWALL, INTRUSION DETECTION AND PREVENTION SYSTEM (IDPS)

Neha Singh
Department Of Computer Science and Information Technology
Singhjass.singh@gmail.com

Abstract

Due to tremendous growth of usage of computer and Internet, the human has entered into an era where there is huge amount of information which is valuable and this information enter into their life via internet. No doubt that this kind of information, makes people's life faster and more convenient; on the other hand, various kinds of harmful contents are flooding the Internet, such as viruses, junk mails and so on, which do great harm not only to the individual but also to the whole society. Firewalls and intrusion detection systems are two most famous and important tools that are used to provide security. Firewall acts as first line of Defense against network attacks .They monitor network traffic in order to prevent unauthorized access. Although firewall can control network traffic but they cannot be entirely depended to provide security. Intrusion detection system (IDS) reduces security gaps and strengthens security of a network by analyzing the network assets for anomalous behavior and misuse.. Real time detection with prevention by Intrusion Detection and Prevention Systems (IDPS) takes the network security to an advanced level by Protecting the network against mischievous activities .In this Paper, we illustrate two important network security tools which includes firewalls and intrusion detection systems their classifications, shortcomings as well as their importance in network security.

Keywords: Firewall, IDS, IDPS, Intrusion prevention system (IPS).

I. INTRODUCTION

Nowadays, due to the boom in the usage of internet by people one of the most important aspects of networks is their security. Network security in today's world plays very important role there are many researches going on this domain by various people to provide more better security to the existing network. The network security and firewalls are two words which seem to be closely related to each other as we are aware of the fact that firewall provides security to network in organization efficiently. The need of firewall is not required to great extent if the network is only intranet based from network security point of view in comparison to the scenario where all the users are connecting with internet which acts as a medium from where the traffic (data) travel from outside to inside and vice-versa, in such case firewall are the first line of defense required at large because the surveillance of attackers increase and hence its mandatory to secure users data as well as to protect unauthorized user cum data to enter in network. In1980s emerged the concept of Firewall technology. The basic function of firewall is to provide access control between networks and to mediate connection requests based on predefined set of rules or policies of packet filters.

Firewalls generally comprise of some form of inspection engine that analyzes IP, TCP, and UDP packet headers and (possibly) packet application data against a "rule base". Due to large number of threats of network attacks, firewalls have become more important elements for defense than ever for any kind of network. Firewalls have been ideally designed for filtering

out unwanted network traffic coming from or going to the secured network. The filtering decision is based on the firewall policy [1] which is a set of ordered filtering rules defined according to predefined security policy requirements. The sequence of rules plays very important role in the firewall policy because matching will take place on the basis of first-match semantics where the firewall will take decision for accepting or rejecting a on the basis of the first rule that the packet matches. A firewall [6] is generally placed at the entry point between a private network and the outside Internet so that it can check all incoming and outgoing packets and decide whether to accept or discard a packet based on its policy. Firewall allows traffic with desired IP addresses and ports to pass through it, but it cannot identify whether the traffic is normal or Malicious one. Firewall no doubt has certain

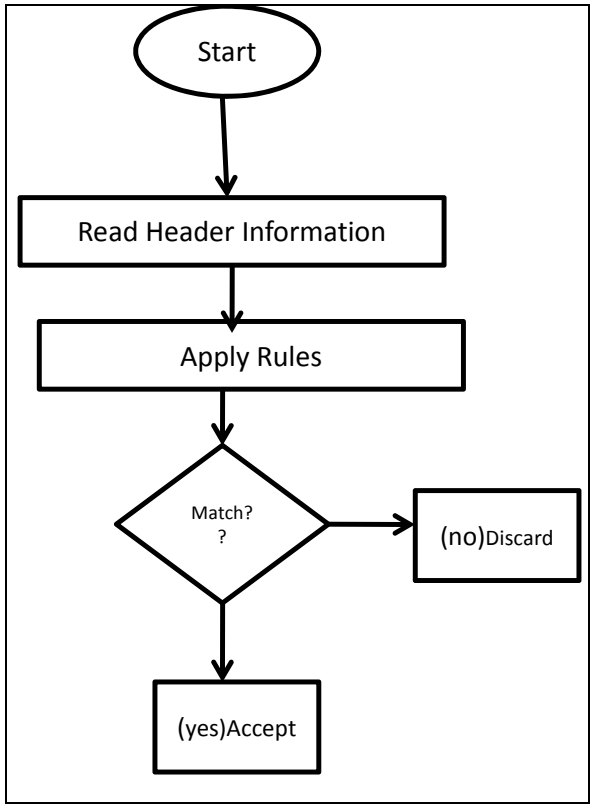

Fig.1. Packet Filter Firewall

advantages, but it lacks ability to detect attacks. On the other hand Intrusion detection system has the ability to detect threats and attacks by monitoring the network traffic. Whenever an intrusion occurs in a network, an alert is generated by IDS to the network administrator for taking an action to block the attack.History of intrusion events has proved that only detection is not enough to block the intruders from attacking the networks which brought intrusion detection and prevention system into existence (IDPS). IDPS not only report attack events to the administrator but also block them instantly. The paper is organized into different sections which include Introduction, Types of Firewall, Shortcomings Of firewall, Types Of Ids , IDPS, Conclusion .

I. BACKGROUND AND RELATED WORK

1) Different Types Of Firewall

Since firewall technology [2] evolved in era of 1980's there has been various changes made in their filtering techniques [4] adopted by them till now in order to make them more and more accurate so that they can provide high level of security to the network this lead into classification of firewall into different generation of firewalls. There are three different types of firewall First Generation Firewall evolved in (1988), Second Generation Firewall evolved in (1989-1990), Third Generation Firewall evolved in (1995–1998) now let's discuss each of them in detail.

1.1) First Generation Firewall (Packet Filters)

In 1988 evolved the first generation firewall which performed the filtering of the packet by evaluating the header contents of the packet .It have the ability to perform layers 3 or 4 inspection of packet data. IP Packet Filter Firewall takes decision whether to accept or to discard packet based on the header content of the packet's. Packet filter firewall uses the rule set to decide whether to accept or reject packet if the packet finds match against the rule set then packet is allowed otherwise it's discarded if it does not match with nay of the rules defined in the rule set. Packet filter firewall works on the network layer, physical layer, and transport layer of the OSI model .Packet filters maintain no state information (Connection State) to know whether the traffic is of existing stream or not which is one of the major drawback of First Generation firewall. This drawback lead to the evolution of Second Generation Firewall.

1.2) Second Generation Firewall (Statefull Filters)

In 1989-1990 evolved the Second generation firewall which performed the filtering of the packet by evaluating the header contents of the packet as well as overcome the drawback of First Generation Firewall by maintaining state table for each connection. Second generation firewall also known as Stateful packet filtering firewalls .Stateful Filters do not perform directly the filtering of the packets based on their header information but they retain packets until enough information is obtained in order to make decision about its state. It Have similar packet inspection capabilities, as that of Packet Filter Firewalls but it add the ability to interpret TCP session flags and establish a state table to monitor TCP connections. Second generation firewall records all connections that passes through it and decides whether a packet is new connection, or an existing connection, or not a connection. Now the rules contain connection state as one of their test criteria. What if an intruder performed Certain Denial of service attack in which attacker can attack firewall with thousands of fake connection requestto overflow the Stateful firewall connection state table. This leads to drawback and reason for evolution of Third Generation Firewall which will handle this kind of attack.

1.3) Third Generation Firewall (Application Layer)

Third Generation Firewall also known as Application Layer Firewall [6] evolved in 1995-1998 which worked on all the layers of OSI model specially more focus on the application layer to handle all the web attacks, traffic that come to or from the internet via application layer .It have the ability to inspect packet data all the way up through layer 7 of OSI model. Application Firewall is commonly known as proxy server. External network and internal network communicate via Proxy. It provides higher security than packet filtering Firewall. Application Firewall requires to inspect only few allowable Applications.

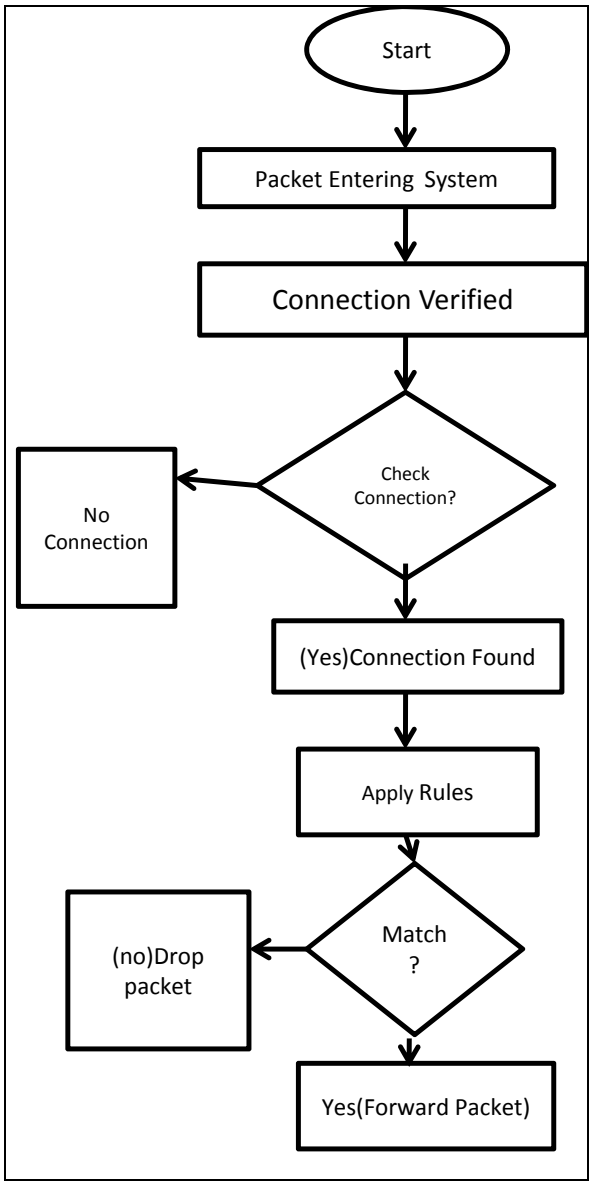

Fig.2.Statefull Firewall

All incoming traffic can be easily logged. Drawback of Application Firewall is that it requires Additional processing overhead on each connection. When the users wish to communicate, they do not communicate directly, instead proxy will act as intermediately between them. Function Offered by Proxy are Authentication mechanism**,** Content Filtering, Mature Log.

1.4) Shortcomings of Firewall

The Different Shortcomings [3] of Firewall includes Following Aspects. Firewall is not able to destroy the attack source. By setting appropriate Firewall it can stop internet virus, Trojan but can't clear the attack source. Firewall can't resist internal attacks behind of tight defensive firewalls; the internal network is likely

confused. For example, attackers through social engineering will send Trojan, Trojan email with URL in the way of internal host inject Trojan, and then the Trojan machine initiative connects to the attacker and destroy the firewall instantly. Own vulnerability Regardless of the hardware firewall or software firewall, there exists soft/hardware troubles, also more or less design flaws. The criminals may adopt these design problems to passthe firewall and launch attacks to the system. Firewall cannot analyze the network packets on the basis of signatures. It cannot detect malwares and viruses coming in from the known ports like port 80 and 110. Therefore we need a system which can analyze network traffic to detect malicious activity.

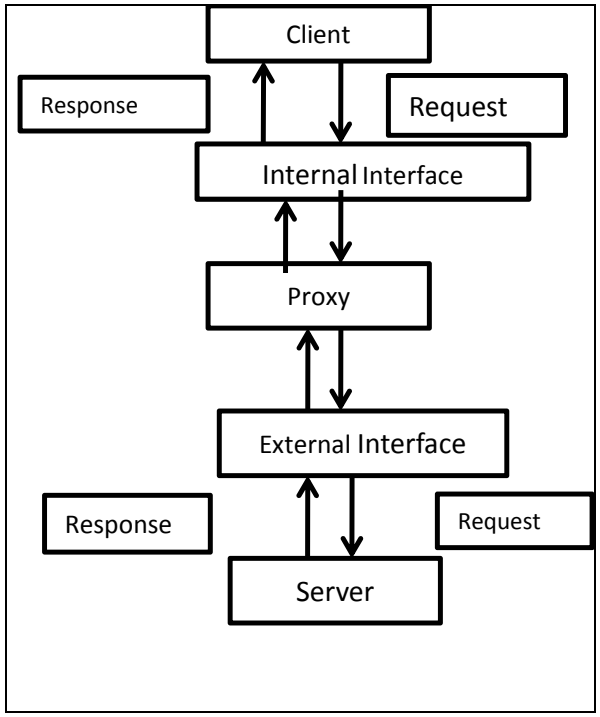

Fig.3.Application Firewall

1.5) Attacks On Firewalls

A) TCP attack on firewall

As dynamic state table is not maintained by packet filtering firewalls they are not able to purely evaluate incoming packets against the packet filters. By manipulating the TCP flags in the TCP packet header attacker can make it possible to force a TCP packet to pass through a packet filtering firewall by setting the "ACK" flag in the TCP header, which produces a match against a packet filter intended to allow return packets for outbound (Internet-bound) Domain Name System (DNS) requests.

B) IP Spoofing

The Process of manipulation of IP source address data in packets to achieve a match with a ruleset or packet filter configured on a firewall or access control device is known as IP Spoofing.If an attacker is able to spoof a source address associated with a "trusted" host, the attacker may be able to penetrate the firewall and enable the passing of packets to the target host.

C) Denial-of-Service

Firewalls and access control devices can be equally as vulnerable to application- or network-based denial-of-service as other devices, applications, and OS. If a firewall does not implement adequate resource safeguards, an attacker may be able to flood a target firewall with connection requests in an attempt to circumvent the firewall and operating systems TCP SYN Flood Attack Protection Mechanism: TCP SYN Flood Protection and connection rate limiters

D) Tiny Fragment Attack

TCP services are targeted by "Tiny Fragment" attack and they make use of IP packet fragmentation functionality to create small fragments that will force some of the TCP header information into a separate fragment. Such kind of attack can be used to bypass certain types of packet filtering devices where the device is unable to handle this type of exception.

Table.1. Different Firewalls

Firewall	License	Cost	OS
Cisco	Proprietary	Included On Cisco Switches and routers	Cisco hardware
Comodo Internet Security	Proprietary	Free	Windows 7,8, Vista
IpFilter	GPlv2	Free	Unix
IPCop	Various	Free	Linux
IPFire	GPL	Free	Linux

ipFirewall	BSD	Free	BSD Package
Netfilter /iptables	GPL	Free	Linux kernel Module
pfsense	ESF Licencse agreement	Free	Free BSD
Smooth wall	GPL	Free	Linux
Zeroshell	GPL ver 2	Free	Linux

2) Intrusion Detection System

An act of entering into a network or system forcibly with intent of either stealing information or damaging the system is known as "Intrusion". Intrusion detection system resides on the gateways or on the host machines to monitor the network traffic. If any malicious traffic is identified, an alert is generated by the IDS, informing responsible person to take action. The terminology "Intrusion Detection" addresses a range of technologies that are involved in the detection, reporting, and correlation of system and network security events. Intrusion detection technologies are detective rather than preventative they provide a security administrator with information on attempted or actual security events. Intrusion Detection Systems look for attack signatures, which are specific patterns that usually indicate malicious or suspicious intent.It can alleviate the following types of risks

- Data destruction
- Denial-of-service
- Hostile code
- Network or system eavesdropping
- System or network mapping
- System or network intrusion
- Unauthorized access

The IDSs are classified into three categories which are as follows .**Host-based IDSs** gets audit data from host audit trails. They are used to detect attacks against a single host. Security violations include attempted break-in, masquerading or successful breaking, penetration by legitimate user and etc.

Distributed IDSs collect information from multiple host and the network that connects the hosts. They are Capable of detecting attacks that involves multiple hosts.**Network-Based IDSs** make use of network traffic as the source of information, trying to reduce the burden of normal computing services provided by the hosts that .They are used to determine attacks from network.There are two basic types of IDS techniques, which are signature-based and anomaly based.

2.1) Signature based IDS (Misuse Detection)

On the basis of known list of attack signatures it detects malicious network packets. Database contains known list for latter comparison in real time mode. **Advantage:** It is very effective against known signatures of attacks **Disadvantage** lacks in detecting unknown attacks.

2.2) Anomaly based IDS

System profile is used to detect any anomaly in the data packets. Initially, system is trained with a normal expected traffic and a profile is built with normal system behavior. Later on the trained profile is used to detect anomalous activities. **Advantage** it is more effective against unknown attacks. **Disadvantage**: it has a high false positive rate.

2.3) Hybrid based approach

To block the malicious network packets this approach combines the signature-based IDS and anomaly-based IDS techniques. The strengths of both the techniques are combined to overcome their drawbacks.

Table.2.IDS Techniques

IDS TECHNIQUE	Advantage	Disadvantage
Misuse Detection	Accurately and generate much fewer false alarm	Cannot detect novel or unknown attacks
Anomaly Detection	detect unknown attacks	High false-alarm

3) Snort open Source IDS

Snort is an widely used *open source* intrusion detection system that has capability of performing traffic analysis based on the rules, content searching or content matching and can be used to detect a variety of attacks like OS fingerprinting ,buffer overflows, SMB probes,stealth port scans, CGI attacks, and so on . An example of widely used NIDS is Snort [6].Snort has Detection Engine which has ability to detect the threats and generate alert to administrator. The Architecture of snort is depicted in the figure below. Packets from different types of network interfaces are taken by Packet Decoder which then prepares packets for processing. Preprocessor detect anomalies in packet headers ,keeps data ready for detection engine, reassemble TCP streams ,packet defragmentation ,decode HTTP URL. Detection Engine applies rules to packets and then outputs the alert

4) IDS Hacking Exploits

Different hacking Exploits for Intrusion Detection System (IDS) are as follows:

4.1. Address Spoofing or Proxying

IP spoofing or ARP spoofing techniques can be used to destabilize an IDS in the sense that they may impact the IP information and IDS logs related to a particular security event.

4.2. Denial-of-Service

IDS can be affected by denial-of-service attack which can flood IDS with port probes or connection requests.

4.3. Packet Fragmentation and "Session Splicing."

IDS systems that are not able to perform appropriate packet reassembly may be vulnerable to attacks that fragment packets in a manner that splices an attack signature over multiple packets Packet fragmentation attacks against IDS involve using some of the packet fragmentation techniques to evade an IDS.

4.4. Port Scan Evasion

An attacker may be able to evade an IDS by slowing port scans over an extended time period, while conducting a portscan of a system or network. Attacker can circumvent an IDS by coordinating a scan among multiple machines or utilizing scan decoy or proxy bounce scanning options.

4.5. TCP Session Synchronization Attacks.

Some IDS evasion tactics involve "desynchronizing" the TCP session that is being monitored to confuse the IDS, and undermine its ability to maintain a sense of session "state.

4.6. Web Evasion Techniques.

Certain tools have the ability to bypass IDS systems by employing various forms of HTTP evasion techniques.Such as premature request ending, Parameter hiding, Misformatting, Long URLs.

5) Intrusion Detection and Prevention System (IDPS):

IDS have ability to detect attack and generate alert but it cannot block the attack on its own. This limitation of IDS is overcome by Intrusion detection and prevention systems IDPS [5] which not only detects the attack, but also stops it from entering into the network or system. IDPS works as network based IDS (NIDPS) and host based IDS (HIDPS).

Parameter	Anomaly	Signature	Hybrid
Resistance to Evasion	Medium	Low	High
High accuracy rate	Medium	Medium	High
Market Share	Medium	High	Medium
Scalability	Medium	High	Medium
Maturity Level	High	High	Medium
Overhead on Monitored System	Medium	Low	Medium
Maintenance	Low	Medium	Medium
Performance	Medium	High	Medium
Easy to Configure	No	Yes	No
Easy to Use	Medium	Low	Low
Protection against New Attacks	High	Low	High
False Positives	High	Low	Low
False Negatives	High	Medium	Low

Table.3.Parameters for Evaluating IDS

5.1. Network intrusion detection and prevention system (NIDPS)

It works at point from where it can monitor the traffic and block the malicious traffic on basis of either signature or anomaly methods**.**

5.2. Host based (HIDPS)

Host Based IDS detect security violations from abnormal patterns of system usage. Security violations include attempted break-in, masquerading or successful breaking, penetration by legitimate user and etc. Abnormal activity in a host is detected by HIDPS by monitoring the logs such as Kernel logs and application logs. Insider attacks happening in a host are also handled by HIDPS

II. CONCLUSION

Thus we have specified the two most popular tools that are used to provide security to the network which are Firewall and IDS , the classification of Firewall and Intrusion detection and Prevention Technology , the Shortcomings of each of them. The Future Work involves In Implementing these tools to Protect the Network From Growing Threats and evaluating them on the basis of level of security, performance, time, cost and other essential parameters

REFERENCES

1] VijenderKumar Solanki, Kumar Pal Singh, Dr. M Venkatesan,udhanshu Raghuwanshi" Firewalls Policies Enhancement Strategies Towards Securing Network" Proceedings of 2013 IEEEConference on Information and Communication Technologies (ICT 2013

2] Huaqing MAO, Li ZHU, Mingbiao LI" Current State and Future Development Trend of Firewall Technology" 978-1-61284-683-5/12/$31.00 ©2012 IEEE

3] Web Security : Theory And Applications; Hui Yan, Wei Wang, Yupeng Ning, Principle and Technology of Firewall.

4] David Mudzingwa ,Rajeev Agrawal " A study of Methodologies used in Intrusion Detection and Prevention Systems (IDPS)" 978-1-4673-1375-9/12/$31.00 ©2012 IEEE

5] Ghilman Ahmed, Mehdi Hussain and M.N.A. Khan "Characterizing Strengths of Snort-based IDPS "Research Journal of Recent Science April **(**2014)

6] Firewall Technology, 0278-6648/02/$17.00 © 2002 IEEE