ISSN XXXX XXXX © 2017 IJESC

Research Article Volume 7 Issue No.6

Comparative Study on Firewall and Intrusion Detection System

Shardul Sharad Vichare
Student
Department of MCA
Vivekanand Education Society's Institute of Technology, Mumbai, India

Abstract:
The growth of computer networks has made it essential to develop network and system security. The development of IDS for detecting attacks in several network environments and Firewalls has been done. This paper gives a comparative study on Intrusion detection system and Firewall. To overcome the security related issues, intrusion detection systems is used which provides confidentiality, integrity and security. Similarly, there are firewalls that protect the systems from hazards.

Keywords: Firewall, Intrusion detection system, IDS.

I. INTRODUCTION

Usage of internet has increased in the recent years. Due to which, network security is becoming necessary so that security and confidentiality of a resource is maintained. For today's need firewalls have become the necessity of network security architectures. Firewalls provides mechanism for access control to network resources, and they have been deployed in the large majority of networks in many organizations. Intrusion detection system (IDS) are been used since last few years. Using IDS, we can find out if someone is trying to attack the network or particular hosts. The information collected can be used to hardening the security.

II. FIREWALL

A firewall is a network security device that monitors the incoming and outgoing network traffic. The firewall decides whether to allow or block traffic based on security rules. It acts as the cop in the network, as all communication should flow through it. Firewalls have been a first line of defense in network security. It establishes a barrier between secured and controlled internal networks that can be trusted, and untrusted outside networks like Internet. A firewall can be hardware, software, or both. Firewalls are network-based or host-based firewalls.

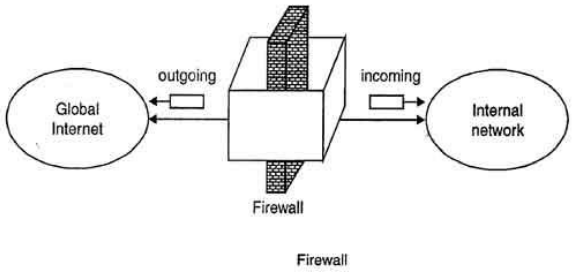

Figure.1. Firewall

A) Types of firewall

i) Packet Filtering Firewall: The packet filtering firewall looks at network addresses and ports of the packet. It determines if the packet should be allowed or blocked to enter. The firewalls inspect the packets that are being transferred between computers through the Internet. If a packet does not match the filtering rules of the firewall, the packet will be discarded. If the packet matches the filters, the packet is allowed to pass. It pays no attention to whether a packet is part of an existing stream of traffic. It does not store information on connection state. Instead, it filters each packet on the basis of the information contained in the packet itself. Packet filtering firewalls works on three layers of the OSI reference model, which are network layer, physical layer and transport layer. When a packet is sent from the sender and filters through a firewall, checking for matches to the rules is done and the decision of rejecting or dropping the packet is done.

ii) Stateful Inspection Firewall: It is also known as dynamic packet filtering firewall. Stateful inspection firewall is a firewall technology that monitors the state of active connections and uses this information to determine which network packets to allow through the firewall. It monitors communication packets and examines both incoming and outgoing packets. Outgoing packets that request some specific types of incoming packets are tracked and only those incoming packets constituting a proper response are allowed through the firewall.

iii) Application Gateway Firewall: An application firewall is a form of firewall that controls input, output, and/or access to an application or service system. It monitors and blocks the input, output, or system service calls that do not follow the rules of the firewall. This firewall is built to control all network traffic on any OSI layer up to the application layer. It is able to control applications or services specifically. There are two primary categories of application firewalls, network-based application firewalls and host-based application firewalls.

B) Limitations of firewall

Firewall offers good protection against network threats, but we cannot depend on them for a complete security solution. There are certain threats that cannot be controlled by the firewall. A firewall cannot protect against malicious insiders. It cannot give protection against connections that do not pass through it. A firewall cannot protect against threats new to it. Protection against viruses is not good enough. A firewall has to be set up by the administrator.

III. INTRUSION DETECTION SYSTEM

An Intrusion Detection System (IDS) is a network security technology built for detecting vulnerabilities against a target

application or computer or system. It monitors network traffic and suspicious activity and policy violations and then alerts the system administrator about the same. The Intrusion detection systems can be classified into host-based intrusion detection systems and network based intrusion detection systems.

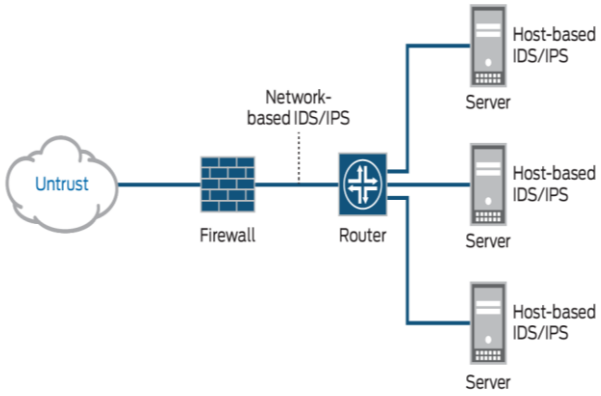

Figure.2. Intrusion detection system

A) Types of IDS

i) Network based intrusion detection system: Network Intrusion Detection Systems or NIDS are placed at points within the network to monitor traffic to and from all devices on the network. Scanning of all the inbound and outbound traffic is done. It performs analysis of passing traffic on the entire subnet, and matches the traffic that is passed on the subnets to the library of known attacks. Once an attack is identified or any abnormal behavior is noticed, alert is sent to the administrator.

ii) Host based intrusion detection system: Host Intrusion Detection Systems or HIDS run on individual hosts on the network. This system can look into system and application log files to detect any intruder activity. It monitors the inbound and outbound packets from the device and will alert the administrator.

iii) Signature based intrusion detection system: A signature based intrusion detection system monitors packets on the network. It compares them against a database of signatures from known malicious threats. This is similar to the way which most of the antivirus software detects malware. The issue is that there will be a delay between a new threat being discovered in the wild and the signature for detecting that threat being applied to your IDS. During that delay time your IDS would be unable to detect the new threat.

iv) Anomaly based intrusion detection system: An anomaly based intrusion detection system will monitor network traffic and compare it against an established baseline. The baseline will identify what is "normal" for that network, what bandwidth is generally used, the protocols that are used, ports and devices connected to each other. It alerts the administrator or user when traffic is detected which is anomalous, or significantly different, than the baseline.

B) Limitations of IDS

- Noisy and bad packets corrupt and limit the IDS.
- At times due to false positives, true attacks or true negatives are missed.
- Constant updation for IDS is required so as to protect against new attacks and vulnerabilities.
- For signature-based IDSs there will be lag between a new threat discovery and its signature being applied to the IDS. During this delay time the IDS will be unable to identify the threat.
- Encrypted packets are not processed by most intrusion detection devices.

IV. COMPARISON BETWEEN FIREWALL AND INTRUSION DETECTION SYSTEM

- A firewall is a hardware and/or software which functions in a networked environment to block unauthorized access while permitting authorized communications while an Intrusion Detection System (IDS) is a software or hardware device used to detect and report intrusion attempts to the network.
- Firewall stands between a local network and the Internet, while the IDS is installed on the network or host and inside the router and the firewall.
- Firewall is security personnel at the gate and an IDS device is a security camera after the gate.
- A firewall can block connection, while a Intrusion Detection System (IDS) cannot block connection. An Intrusion Detection System (IDS) alert any intrusion attempts to the security administrator.
- Firewall does not tell if the traffic is legit or not while the IDS detects and look at the traffic to see if it an attack.

V. CONCLUSION

In this comparative study, we saw two systems built for the security of the systems. We studied what is firewall and Intrusion Detection System, their basic working and types. Also we studied the difference between them. A firewall is placed at a different layer in the network topology and a intrusion detection system at a different layer. Both Firewall and IDS are commercially active systems for security and are equally important.

VI. ACKNOWLEDGEMENT

I am highly obliged to my respected teacher Ms. Nishi Tiku (HOD) and Ms. Meenakshi Gharg (Assistant Professor) heartily for their co-operation and perfect guidance, in the absence of which this research paper would never have been success. I would like to extend my gratitude and thanks to the guidance of Vivekanand Education Society's Institute of Technology, which gave me an opportunity to prepare this study paper.

VII. REFERENCES

[1]. Archana D Wankhade and Dr P.N.Chatur, "Comparison of Firewall and Intrusion Detection System " (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (1) , 2014, 674-678.

[2]. Mr. D.Shiva rama krishna, Mr. Siva Rama Prasad Kollu, Mr. Ch.V.V.Narasimha Raju, "A Comparative Study of Firewall and Intrusion Prevention System" International Journal of Innovative Research in Computer Science & Technology (IJIRCST) ISSN: 2347-5552, Volume-2, Issue-6, November-2014

[3]. Vinutha H.P., Dr.Poornima B, "A Survey - Comparative Study on Intrusion Detection System" International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 7, July 2015

[4]. Indraneel Mukhopadhyay , Mohuya Chakraborty , Satyajit Chakrabarti, "A Comparative Study of Related Technologies of Intrusion Detection & Prevention Systems" Journal of Information Security, 2011, 2, 28-38 doi:10.4236/jis.2011.21003 Published Online January 2011

[5]. K.C. Nalavade and B.B. Meshram, "Comparative Study of IDS and IPS" BIOINFO Computer Engineering Volume 1, Issue 1, 2011, pp-01-04

[6]. Nilotpal Chakraborty, "INTRUSION DETECTION SYSTEM AND INTRUSION PREVENTION SYSTEM: A COMPARATIVE STUDY" International Journal of Computing and Business Research (IJCBR) ISSN (Online): 2229-6166 Volume 4 Issue 2 May 2013.