ISSN No.: 2454- 2024 (online)

International Journal of Technical Research & Science

USE OF FIREWALL AND IDS TO DETECT AND PREVENT NETWORK ATTACKS

Dr. Abid Hussain
E-Mail Id: abid.hussain@cpur.edu.in
Assistant Professor, School of Computer Applications, Career Point University, Kota, Rajasthan, India

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 [1]. 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 [5].

Keywords- Firewall, IDS, IDPS, Network Security, Proxy, Packet-Filtering Firewall, Software, Hardware, HIDS, NIDS, PIDS, VMIDS.

1. INTRODUCTION

There are many different types of devices and mechanisms within the security environment to provide a layered approach of defense so that if an attacker is able to bypass one layer, another layer stands in the way to protect the network. Two of the most popular and significant tools used to secure networks are firewalls and intrusion detection systems. The rudimentary functionality of a firewall is to screen network traffic for the purpose of preventing unauthorized access between computer networks.

In this paper, we will examine the use of firewalls and intrusion detection systems, as well as understand the architecture behind these technologies. We will touch attack indications and the countermeasures that should be applied in order to secure the network from breach. This research paper describes the importance of firewall and intrusion detection system, and why they must be a part of every network security administrator's defense plan. We are aware of the fact that firewall provides security to network in organization efficiently. We will also discuss about the usability of firewall with intrusion detection system to detect and prevent network attacks and create a secure architecture for the organization where the transmission of files could be useful for us [10]. 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 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, and Working Architecture of firewall, Classification of Firewalls, Types of Ids, Indication of Intrusions, and Conclusion.

2. NETWORK SECURITY SOLUTIONS

The number of people connecting to the Internet is increasing very rapidly. The ease of use and the connectivity the Internet provides is highly useful but the risks involved and malicious intrusions are also increasing day by day. Exploitation of computer networks is getting more common. It is completely critical for business organization as well as individuals to protect their data from serious threats that would aim to steal their information. There are many security solutions available in the market. Some of them are like Firewall, Intrusion Detection System (IDS) which are explained below.

2.1 Firewall

A firewall is a device installed between the internal network of an organization and the rest of the network. It is designed to forward some packets and filter others. For example, a firewall may filter all incoming packets destined for a specific host or a specific server such as HTTP or it can be used to deny access to a specific host or a service in the organization [3]. The following image depicts a firewall installation in the network.

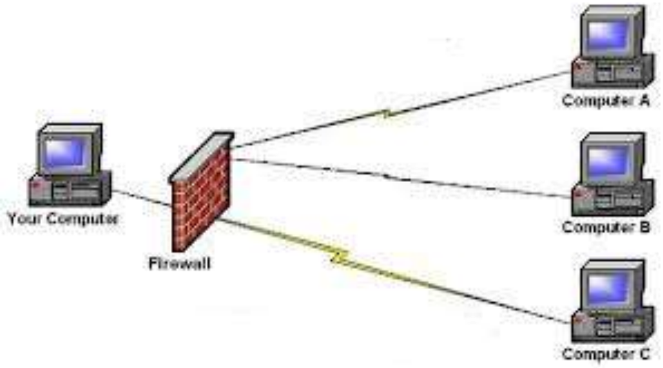

Fig. 2.1 Working of Firewall

Firewalls are a set of tools that monitors the flow of traffic between networks. Placed at the network level and working closely with a router, it filters all network packets to determine whether or not to forward them towards their destinations.

2.2 Working Architecture

A firewall is often installed away from the rest of the network so that no incoming requests get directly to the private network resource. If it is configured properly, systems on one side of the firewall are protected from systems on the other side [4]. Firewalls generally filter traffic based on two methodologies:

- A firewall can allow any traffic except what is specified as restricted. It relies on the type of firewall used, the source, the destination addresses, and the ports.
- A firewall can deny any traffic that does not meet the specific criteria based on the network layer on which the firewall operates.
- The type of criteria used to determine whether traffic should be allowed through varies from one type to another.
- A firewall may be concerned with the type of traffic or with source or destination addresses and ports.
- A firewall may also use complex rules based on analyzing the application data to determine if the traffic should be allowed through.

2.3 Firewalls Pros and Cons

Every security device has advantages and disadvantages and firewalls are no different. If we applied strict defensive mechanisms into our network to protect it from breach, then it might be possible that even our legitimate communication could malfunction, or if we allow entire protocol communications into our network, then it can be easily hacked by malicious users [9]. So, we should maintain a balance between strictly-coupled and loosely-coupled functionalities.

2.4 Firewall Classification

The way a firewall provides greater protection relies on the firewall itself, and on the policies that are configured on it. The main firewall technologies available today are:

2.5 Hardware Firewall

A hardware firewall is preferred when a firewall is required on more than one machine. Hardware firewall provides an additional layer of security to the physical network. The disadvantage of this approach is that if one firewall is compromised, all the machines that it serves are vulnerable.

2.6 Software Firewall

A software firewall is a second layer of security and secures the network from malware, worms and viruses, and email attachments. It looks like any other program and can be customized based on network requirements. Software firewall can be customized to include antivirus programs and to block sites and images.

2.7 Packet-Filtering Firewall

Packet-Filtering firewall filters at the network or transport layer. It provides network security by filtering network communications based on the information contained in the TCP/IP header of each packet. The firewall examines these headers and uses the information to decide whether to accept and route the packets along to their destinations or deny the packet by dropping them. A Packet-Filter firewall is a router that uses a filtering table to decide which packets must be discarded.

2.8 Proxy Firewall

The Packet-Filter firewall is based on information available in the network and transport layer header. However, sometimes we need to filter a message based on the information available in the message itself (at the application layer). For example, assume that an organization only allows those users who have previously established business relations with the company, then access to other users must be blocked.

3. INTRUSION DETECTION SYSTEM

Intrusion Detection (ID) is the process of monitoring for and identifying attempted unauthorized system access or manipulation. An ID system gathers and analyzes information from diverse areas within a computer or a network to identify possible security breaches which include both intrusions (attack from outside the organization) and misuse (attack from within the organization).

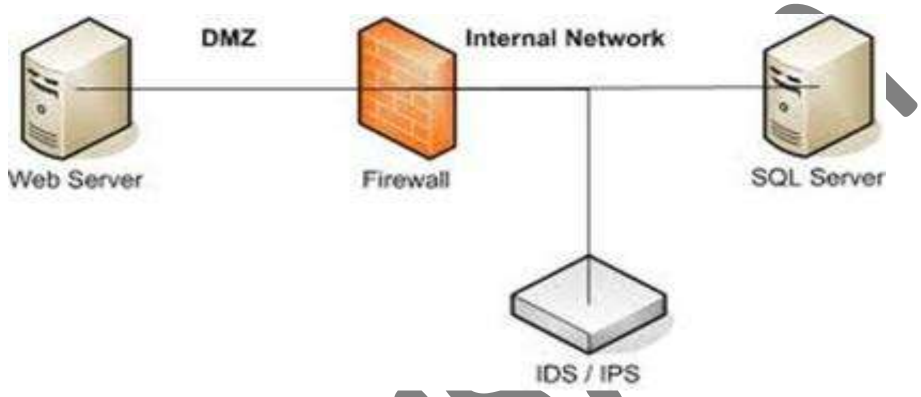

Fig. 3.1 Working of Intrusion Detection System

An Intrusion Detection System (IDS) is yet another tool in the network administrator's computer security arsenal. It inspects all the inbound and outbound network activity. The IDS identifies any suspicious pattern that may indicate an attack the system and acts as a security check on all transactions that take place in and out of the system [2].

3.1 Types of IDS

For the purpose of dealing with IT, there are four main types of IDS [6]:

3.1.1 Network Intrusion Detection System (NIDS)

It is an independent platform that identifies intrusions by examining network traffic and monitors multiple hosts. Network intrusion detection systems gain access to network traffic by connecting to a network hub, a network switch configured for port mirroring, or a network tap. In a NIDS, sensors are placed at choke points in the network to monitor, often in the demilitarized zone (DMZ) or at network borders. Sensors capture all network traffic and analyze the content of individual packets for malicious traffic. An example of a NIDS is Snort.

3.1.2 Host-Based Intrusion Detection System (HIDS)

It consists of an agent on a host that identifies intrusions by analyzing system calls, application logs, file-system modifications (binaries, password files, capability databases, Access control lists, etc.) and other host activities and state. In a HIDS, sensors usually consist of a software agent. Some application-based IDS are also part of this category. An example of a HIDS is OSSEC. Intrusion detection systems can also be system-specific using custom tools and honeypots. In the case of physical building security, IDS is defined as an alarm system designed to detect unauthorized entry.

3.1.3 Perimeter Intrusion Detection System (PIDS)

Detects and pinpoints the location of intrusion attempts on perimeter fences of critical infrastructures. Using either electronics or more advanced fiber optic cable technology fitted to the perimeter fence, the PIDS detects disturbances on the fence, and if an intrusion is detected and deemed by the system as an intrusion attempt, an alarm is triggered.

3.1.4 VM Based Intrusion Detection System (VMIDS)

It detects intrusions using virtual machine monitoring. By using this, we can deploy the Intrusion Detection System with Virtual Machine Monitoring. It is the most recent type and it's still under development. There's no need for a separate intrusion detection system since by using this, we can monitor the overall activities.

4. COMPARISION WITH FIREWALL AND IDS

Though they both relate to network security, an intrusion detection system (IDS) differs from a firewall in that a firewall looks outwardly for intrusions in order to stop them from happening. Firewalls limit access between networks to prevent intrusion and do not signal an attack from inside the network. An IDS evaluates a suspected intrusion once it has taken place and signals an alarm [7]. An IDS also watches for attacks that originate from within a system. This is traditionally achieved by examining network communications, identifying heuristics and patterns (often known as signatures) of common computer attacks, and taking action to alert operators [8]. A system that terminates connections is called an intrusion prevention system, and is another form of an application layer firewall.

CONCLUSION

In this paper, we provided an in-depth overview of firewalls and IDS, and their roles in protecting the corporate network. There are four main types of firewalls: packet-filters, application gateways, circuit-level gateways, and other firewalls. Though some have predicted the end of the firewall, its strategic location in the network makes it an indispensable tool for protecting assets. Good security practices dictate that firewalls should be deployed between any two networks of differing security requirements.

This paper illustrates the importance of IDS and its various types. IDS monitor hosts for system alteration or sniffs network packets off the wire, seeking for malicious contents. Security Administrators should contemplate using combinations of HIDS and NIDS, with both signature-detection and anomaly-based engines. IDS can be configured purely as monitoring and detection devices or it can participate as an inline device and prevent threats. Its biggest weaknesses are the high number of false-positives and the maintenance effort needed to keep signatures up to date and fine-tuned.

REFERENCES

[1] K. Scarfone and P. Mell, "Guide to Intrusion Detection and Prevention Systems (IDPS)," Gaithersburg, MD, Rep. NIST Special Publication 800-94,Feb. 2007.

[2] D.Rozenblum, "Understanding Intrusion Detection System,October 31, 2003.

[3] S. Nassar, A.E. Sayed, N. Aiad, "Improve the Network Performance By using Parallel Firewalls," in Proc. of 6th International Conference on Networked Computing, May 2010, pp. 1-5.

[4] S. Ioannidis et al., "Implementing a Distributed Firewall," in Proceedings of the ACM Computer and Communication Security (CCS), pp. 190-199, 2000.

[5] W. Stallings, Cryptography and Network Security Principles and Practices. 4th ed.,Prentice Hall, 2005.

[6] X. Jhang, C. Li, W. Zheng, "Intrusion Prevention System Design." in Proc. of 4th International Conference on Computer and Information Technology, pp. 386-390, Sept. 2004

[7] Samrah, "Intrusion Detection Systems; Definition, Need and Challenges," http://www.sans.org/reading_room/whitepapers/detection/intrusion-detectionsystems-definition-challenges_343, October 31, 2003.

[8] Harek Haugerud, "Intrusion detection and firewall security," Available: http://www.iu.hio.no/teaching/materials/MS004A/html/pictures/ids.png

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

[10] John E. Canavan," Fundamentals of Network Security", http://www.artechhouse.com