Gursewak Singh *et al*, International Journal of Computer Science and Mobile Applications,
Vol.6 Issue. 1, January- 2018, pg. 43-51 **ISSN: 2321-8363**
Impact Factor: 5.515

NETWORK SECURITY TECHNOLOGY BASED ON FIREWALL AND INTRUSION DETECTION SYSTEM

Gursewak Singh[1], Bohar Singh[2]
[1]Computer Science and Application, mgursewak@gmail.com
[2] Computer Science and Application, bohar2@gmail.com

Abstract
As rapid growth of internet, computer network and network devices are becoming more vulnerable to various types of attacks. Network security tools such as Firewall and Intrusion Detection System (IDS) are used for monitoring the network and protecting it from the intruder, but both of Firewall and IDS has its own merits and demerits. Firewall has shortages, such as it cannot keep away interior attacks, it cannot provide a consistent security strategy. Intrusion Detection System (IDS) also has many defects, such as low detection ability, lack of effective response mechanism, poor manageability, etc. If firewall and IDS are integrated, the integration of both can result in greater network security to network. IDS monitors the network, provides a real time detection of attacks from the interior and exterior, and automatically informs firewall and dynamically alters the rules of firewall once an attack is found; In this paper Firewall and IDS are discussed along with their types, functionality and limitations and then discuss the integration Firewall and IDS in network topology.

Keywords: Intrusion Detection System (IDS), Firewall, NIDS, HIDS, NAT, FTP.

1. Introduction

With the rapid progress in the internet based technology new application areas for computer network have emerged. In instances, the fields like business, financial, industry, security and healthcare sectors the LAN and WAN applications have progressed. All of these application areas made the network an attractive target for the abuse and a big vulnerability for the community [1]. Intruders or hackers use the organization's internal systems to collect information's and cause vulnerabilities like Software bugs, Lapse in administration, leaving systems to default configuration. 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 but in this paper we will describe Firewall and Intrusion Detection (IDS) which are adopted more frequently. Today Firewalls have become the staple of network security architectures, primarily providing access control to network resources, and they have been successfully deployed in the large majority of networks like government organization and individual users. Firewall technique is one of the popular protection techniques and it is used to protect the private network from the public network. IDS are used in network related activities, medical applications, credit card frauds, Insurance agency [2]. An Intrusion Detection System is an application used for monitoring the network and protecting it from the intruder.

1.1 Principles of Security

Network security refers to protection of data from damage and loss at physical level and also refers to data integrity, data confidentiality, data availability and control access of data at logical level. There are four basic principles of security[4]:

(1) **Data integrity**: Data integrity means without any authorization the data cannot be changed. Thus only allowed people can change data.

(2) **Confidentiality**: the principal of confidentiality refers that only the sender and concerned recipient can access the content of a massage and therefore provides the protection against passive attack.

(3) **Availability**: The principal of availability means resources should be available to authorized users every times as per requirement. Hence, the attackers are not allowed to occupy all of the resources.

(4) **Access control**: The principal of access control states that who should be able to access what. Thus access control provides controlled access to the host system. Access control makes sure that each and every authorized user has privilege to access the resources.

1.2 Security Mechanism

(1) Encryption technology*:* Encryption technology means protect information transmitted over network. Encryption technology encodes the massage transmitted over the network in non-readable code. The original massage is called plain text and the encoded massage is called cipher text. It is shown in figure 1.

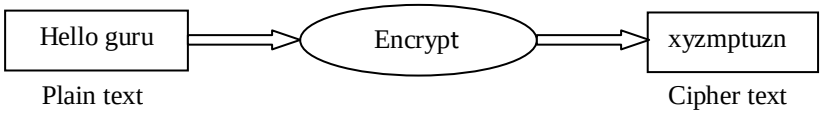

Figure 1. Encryption process

The reverse process of Encryption is Decryption. In Decryption cipher text message is decoded back to plain text. It is shown in figure 2.

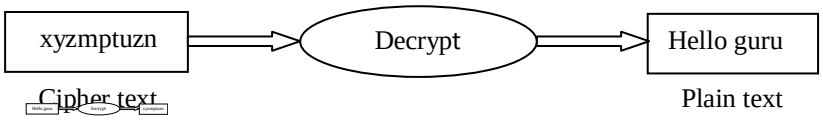

Figure 2. Decryption Process

In this process, both the sender and receiver must agree on a common algorithm for any meaningful communication takes place. This algorithm requires Key system. The key system can be divided into secret key or public key method. In Secrete key method the encryption and decryption use the same the key. This method is used to save a large number of keys, and hence to enhance the security factor. The basic algorithm used is DES algorithm. The Public key method algorithm requires two keys, a private key and a public key. The sender first encrypts the data by using recipient's public key. Then the sender sends the encrypted data to the recipient. The recipient received encrypted data and decrypts the cipher text back into plain text by using his own private key. The basic algorithms used are RSA algorithm.

(2) Authentication: The authentication requires personal identification number, password, smart cards, individual's physical characteristics, such as fingerprints etc.

(3) Firewall Technology: This technology has the control for incoming and outgoing network traffic for security purposes. Firewall is an important tool for network security that is located between two networks. It prevents any unauthorized internal or external users to make an intrusion to the computer network.

(4) Intrusion detection system (IDS): IDS is a set of techniques and methods used to detect any suspicious activity both at the network level and host level. Intrusion detection system (IDS) is usually deployed as a second line of defence along with other preventive security mechanisms, such as access control and authentication.

2. FIREWALL

A firewall is simply a program or hardware device that filters the information coming through the Internet connection into your private network or computer system. It monitors the incoming and outgoing network traffic and decides whether to allow or block traffic based on security rules. It establishes a barrier between secured and controlled internal networks that can be trusted, and untrusted outside networks like Internet. Firewalls are network-based or host-based firewalls. Network firewalls provide a barrier between networks that prevent or denies unwanted or unauthorized traffic. In simple words a firewall is protective device that provides a controlled point of entry into and out of your computer resource. The firewall also is your network security measures first line of defence.

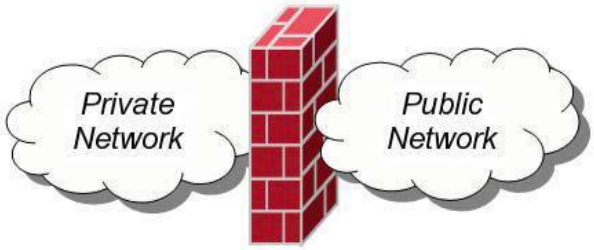

Figure 3. Firewall

2.1 Types of firewall

1) Packet Filter Firewall:-Packet filtering applies a set of rules to each packet and based on outcome, decides to either forward or discard the packet. A packet filtering router should be able to filter IP packets based on information included source IP address, destination IP address, TCP/UDP source port and TCP/UDP destination port. It is used to block connections from specific hosts or networks, block connections to specific hosts or networks, block connections to specific ports and block connections from specific ports. In Packet filtering IP packets are either forwarded or discarded without checking their contents [1]. This type of firewall allows all traffic between "trusted" hosts. All the packets that incoming to the networks will be checks in detail by the packet filtering firewall. The firewall system wills checks basic information that resides in the packet such as source and destination address, source and destination port numbers, protocol and others that related. Then, a comparison will be making between information on the packets with the rules, which had configure on the firewall system. An example of firewall configuration is as follows:

Protocol	Transport Protocol	Source IP	Source Port	Destination IP	Destination Port	Action
HTTP	TCP	Any	Any	192.168.0.1	80	Allow
HTTPS	TCP	Any	Any	192.168.0.1	443	Allow
Telnet	TCP	10.0.0.1/24	Any	192.168.0.5	223	Allow

Figure 4. Example of Packet Filter

Simplicity, High speed and Transparent to the user are advantages of this firewall. It does not support advanced authentication schemes and cannot prevent attacks that employ application specific vulnerabilities or functions.

2) Stateful Packet Inspection firewall:-Stateful-inspection is an enhancement of the packet filter technology. Besides inspecting individual packet content, the Stateful-inspection also inspects the attributes of the multi-packet flows. A dynamic or "stateful packet inspection" also referred to as connection–state filtering packet in which firewall maintains a table of active TCP sessions and UDP sessions. Each entry in the state table records the sessions, source and destination IP address and port numbers and the current TCP sequence number. Entries are created only for those TCP connections or UDP streams that satisfy a defined security policy. The packets associated with these sessions are permitted to pass through the firewall. Sessions that do not match any policy or any packets received that do not match an existing table entry are denied [2]. It only allows packets belonging to an allowed session so it is more secure than packet filtering. A stateful inspection firewall ensures that packets belong to an existing session and it can authenticate the user when the session is established. Firewall system check each field in the IP packet like the source address, destination address, protocol type(TCP, UDP and others), port number and service type(Telnet, FTP and others). It records all details information of each and every packet that passes through network in a log file [4]. The rules that used for filtering will be applying based on that information. In addition, it examines the packet header information from the network layer of the OSI model to the application layer to verify that the packet is part of a legitimate connection and the protocols are behaving as expected.

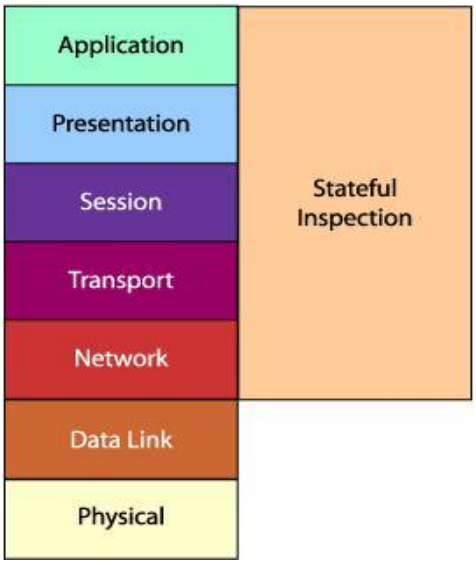

Figure 5. Stateful inspection at OSI layers

3) Application-gateway firewall: An application-gateway firewall [3] is simply a type of proxy server that provides proxies for specific applications. The most common implementations of application-gateway firewalls provide proxy services, such as mail, file transfer protocol (FTP) and telnet, so that they do not run on the actual firewall, which increases security. The source or destination Internet protocol (IP) address, however, can be used to accept or reject incoming connections. Application-level firewalls also determine permissible conditions and events when a proxy connection has been established. An FTP proxy can restrict FTP access to one or more hosts by allowing the get command and at the same time, preventing the put command. A telnet proxy can terminate a connection if the user attempts to perform a shell escape or to gain root access. Application-gateway firewalls are not limited only to applications that support TCP/IP services, however. These tools can similarly govern conditions of usage for a variety of applications, such as financial or process control applications.

The two basic types of application-gateway firewalls are:

1) Application-generic firewalls
2) Application-specific firewalls.

The application-generic type provides a uniform method of connection for every application, regardless of type [5].

The application-specific firewall determines the nature of connections to applications on an application-by-application basis.

Application-gateway firewalls are the best-selling of all types of firewalls. Nevertheless, they have some notable limitations. Most significant, for every TCP/IP client for which the firewall provides proxies, the client must be aware of the proxy that the firewall runs on its behalf. Therefore, each client must be modified accordingly. A second limitation is that, unless one uses a generic proxy mechanism, every application needs its own custom proxy.

4) Network Address Translation (NAT) Firewall: Network address translation allows a network to use one set of network addresses internally and a different set when dealing with external networks. Network address translation does not provide any security by itself but it helps to hide the internal network layout and to force connections to go through a choke point. The choke point does the translation. Like packet filtering, network address translation works by having a router do extra work. In this case, not only does the router send packets on, but it also modifies them. When an internal machine sends a packet to the outside, the network address translation system modifies the source address of the packet to make the packet look as if it is coming from a valid address. When an external machine sends a packet to the inside, the network address translation system modifies the destination address to turn the externally visible address into the correct internal address. The network address translation system can also modify the source and destination port numbers (this is sometimes called Port and Address Translation or PAT).

5) Proxy firewall

Application proxy firewalls are also more secure than packet filtering, but are generally slower than stateful inspection. Two TCP connections are established in an application proxy firewall: one between the packet source and the firewall, another between the firewall and the packet destination. Application proxies intercept arriving packets on behalf of the destination, examine application payload, and then relay permitted packets to the destination [3].

It is called a proxy server, because it acts as deputy or substitute and decides about flow of applications. Internal users contact the proxy server using HTTP or TELNET. The proxy servers ask the user about remote host with which the user want to set up a connection for actual communication. The proxy server now accesses the remote host on behalf of the user and passes the packet of the user to remote host. The proxy changes the IP address in the packets from the end user's IP address to its own. Thus the IP address of the computer of the internal users is hidden from outside world. If we are using the proxy server as a firewall we can get the benefit in protecting our computer network .Because it has a good control on the connections such as allowing or denying access to the server based on its IP address or based on IP address of the user that requesting the connection. The figure 6 illustrates the concept of proxy server, in this IP address of inside host is 178.29.10.90 and proxy server change it to 178.29.10.70 which is shown to outside the network.

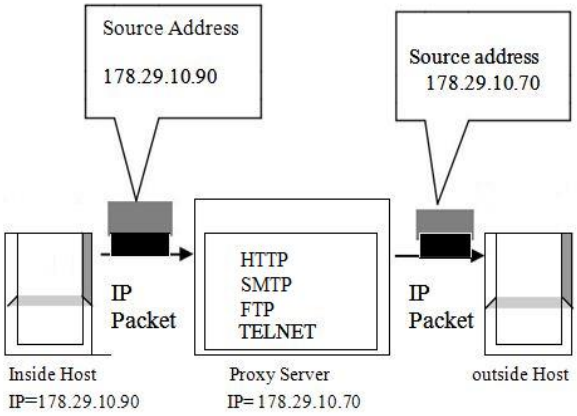

Figure 6: Proxy Server Operation.

2.2 Limitations of Firewall

- The firewall cannot protect against attacks that bypass the firewall.
- Firewalls cannot prevent attacks coming from Intranet.
- The firewall may not protect fully against internal threats, such as a disgruntled employee or an employee who unwittingly cooperates with an external attacker.
- Most firewalls do not analyze the contents of the data packets that make up network traffic.
- An improperly secured wireless LAN may be accessed from outside the organization. An internal firewall that separates portions of an enterprise network cannot guard against wireless communications between local systems on different sides of the internal firewall.
- A firewall may not protect against threats new to it such as viruses.
- A laptop, PDA, or portable storage device may be used and infected outside the corporate network, and then attached and used internally.

3. Intrusion Detection System

For several reasons intrusion detection system became necessary part of the entire defence system because number of traditional defence systems and applications were developed without considering security as important aspect. In some cases, traditional defence systems and applications may become vulnerable when deployed because they were developed without considering working in a different environment. So, Intrusion detection system complements these protective mechanisms to improve the system security.

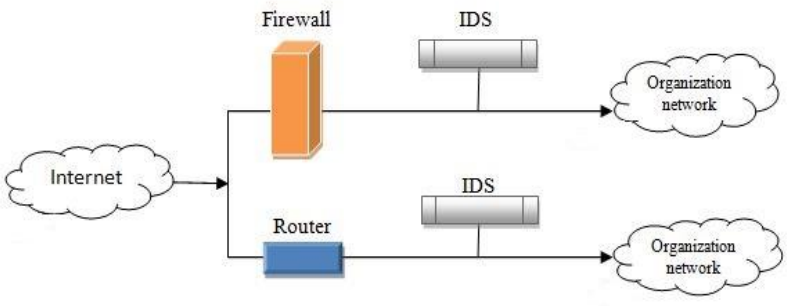

Figure 7. Intrusion Detection system (IDS)

There are two basic categories of intrusion detection system: signature-based intrusion detection systems and anomaly detection system [4][5]. In signature-based intrusion detection system, intruders may have signatures and intruders can be detected using software and data packets because they contain any known intrusion-related signatures. So by using these set of signatures, intrusion detection system is able to monitor and log any unwanted intruder activity and generate alerts. Second Anomaly-based intrusion detection system usually based upon packet anomalies present in protocol header parts. In some cases anomaly based intrusion detection systems produce better results as compared to signature-based intrusion detection systems.

3.2 Types of IDS

Figure 8 shows different types of Intrusion detection system.

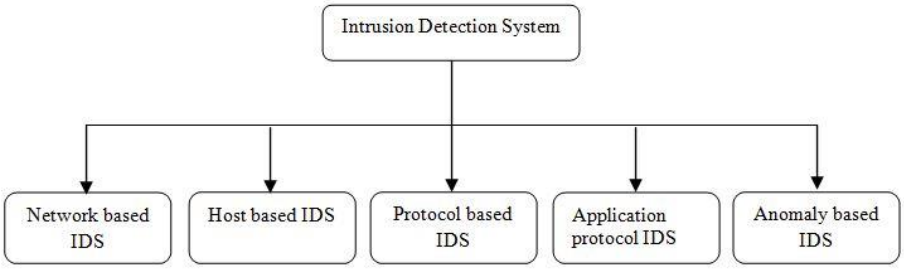

Figure 8. Types of IDS

1) Network based IDS (NIDS): NIDS are intrusion detection systems that capture data packets transmitted on the network media and match them to a database of signatures. When a packet is matched with an intruder signature, an alert is generated.

2) Host based IDS (HIDS): Host-based intrusion detection systems are installed as agents on host. These intrusion detection systems can look into system log files to detect any intruder activity [7]. Some HIDS inform you only when some intruder activity has happened and some HIDS can sniff the network traffic regularly coming to a particular host on which the HIDS is installed and alert you in real time.

3) Protocol based IDS: Protocol based IDS is installed on a server and it analyzes the server. It analyzes and monitors the dynamic behaviour and communication between the server and connected devices.

4) Application protocol based IDS: Application protocol based IDS normally sit between groups of services/processes and monitors the behaviour and state of application protocol used by the system between two connected devices.

5) Anomaly based IDS: Anomaly based IDS monitor the system activity and classifying it as either normal or anomalous to detect computer intrusions. The advantage of anomaly based detection is relatively high detection rate for new types of intrusions.

3.2 Functions of IDS

The IDS consist of four key functions namely, data collection, feature selection, analysis and action, which is given in Figure 9.

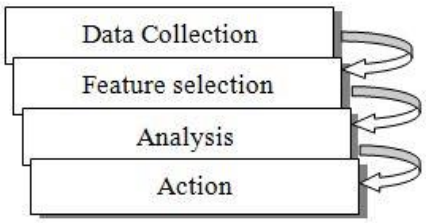

Figure 9. IDS Functionality

1) Data collection: This module collects the data and passes the data as input to the IDS. The data is recorded into a file for analysis. If the system detects the attack then it forward the information about the attack.

2) Feature selection*:* The particular features are selected from the large data available in the network and then these features are evaluated for intrusion. For example, the Internet protocol address of the source and destination system, protocol type, header length and size could be taken as a key feature for intrusion detection.

3) Analysis: In this module data is analysed to find the correctness. For example signature based IDS analyze the data by checking the incoming traffic against predefined signature and Anomaly based IDS analyse the data by monitoring the system behaviour.

4) Action: This module defines about the attack and reaction of the system. It can either inform the system administrator with all the required data through email or alarm. It can also play an active role in the system by closing the port or dropping packets so that it does not enter the system.

3.3 Limitations of IDS

- IDS can detect attack only after they have entered the network.
- IDS do nothing to prevent attacks, it only send alert to trigger.
- IDS cannot detect all malicious activity at all-time handling alert to trigger false positive or false negative alarm.
- IDS cannot integrate with filtering rules security to stop traffic from attacking.
- These system can collect a large number of alerts in a day, overloading your work
- In IDS various tasks like analyzing and filtering has to be done manually

4. Intrusion Detection System and Firewall in Network Topology

Intrusion detection systems can be positioned at one or more places depend upon network topology. It also depends upon the types of intrusion activities to be detected either internal, external or both. For example, if only external intrusion activities to be detected and have only one router connecting to the Internet then the best place for an intrusion detection system may be just inside the router or a Firewall. If there are multiple paths to the Internet, then one IDS may place at every entry point. However if internal threats to be detected then IDS is to be placed in every network segment. In many cases you don't need to have intrusion detection activity in all network segments and you may want to limit it only to sensitive network areas. Note that more intrusion detection systems mean more work and more maintenance costs. So decision of placing IDS really depends upon security policy, which defines what really want to protect from hackers.

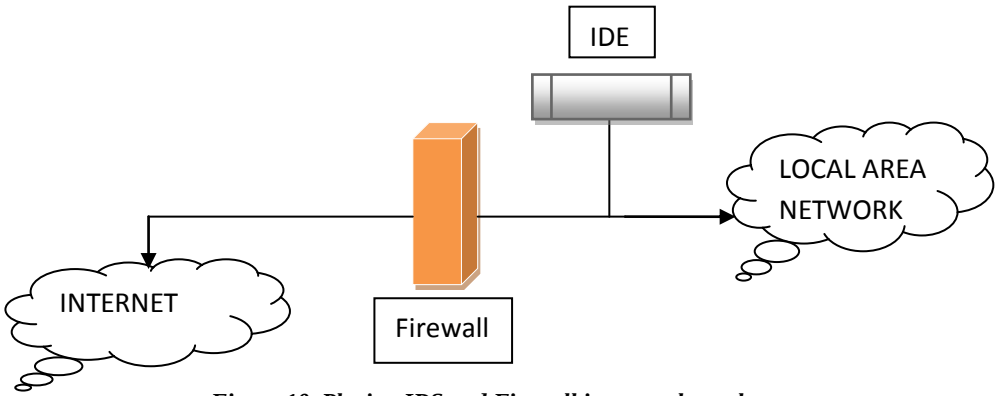

Figure 10. Placing IDS and Firewall in network topology

Figure shows typical locations to place an intrusion detection system. Typically you should place IDS behind each of your firewalls and routers.

5. Conclusion

This study discuss about firewall technology and IDS along with their classification, functionalities, merit and demerit. This study reflects that either firewall or IDS individually are not able to cope up with all security requirements and still need to be improved to ensure a complete security for a network. So as to provide the better security solution firewall technology integrated with IDS to protect network system from malicious intruders. In this way computer network can be secured in reliable manner.

REFERENCES

[1] Wankhade, Archana D. "Comparison of Firewall and Intrusion Detection System."International Journal of Computer Science & Information Technologies 5.1 (2014).
[2] B. H. A. Firkhan Ali, "A Study of Technology in Firewall System," IEEE symposium on business, 2011.
[3] W. C. Y. W. Xin Vue, "The Research of Firewall Technology in Computer Network Security," Computational Intelligence and Industrial Applications, pp. 421-424, 2009.
[4] Anand, Amrita, and Brajesh Patel. "An Overview on Intrusion Detection System and Types of Attacks It Can Detect Considering Different Protocols."International Journal of Advanced Research in Computer Science and Software Engineering, IJARCSSE 8 (2012): 94-98.
[5] Dr. Vijayarani, and Sylviaa.S Maria. "Intrusion Detection System- A study."International Journal of Security, Privacy and Trust Management (IJSPTM),vol 4, no.1, February 2015.
[6] "Firewall concept," [Online]. Available:http://ctc.kbu.ac.th/manatsarin/wp-content/uploads/2007/08/chapter-7-firewall.pdf. [Accessed 2 April 2015].
[7] Peyman Kabiri and Ali A.Ghorbani-"Research on Intrusion Detection and Response Survey"-International Journal of Network Security, Vol.1, No.2, PP.84–102, Sep. 2005
[8] Christopher Low –"Understanding Wireless attacks & detection "-GIAC Security Essentials Certification (GSEC) Practical Assignment 13 April 2005 -SANS Institute InfoSec Reading Room.
[9] H. Ling-fang, "The Firewall Technology Study of Network Perimeter Security," in Asia-Pacific Services Computing Conference, 2012.

