ISSN:0975-9646

Comparison of Firewall and Intrusion Detection System

Archana D wankhade[1] Dr P.N.Chatur[2]

[1]*Assistant Professor ,Information Technology Department, GCOE, Amravati, India.*
[2]*Head and Professor in Computer Science and Engineering Department, GCOE, Amravati, India.*

Abstract: **Firewall has many shortages, such as it cannot keep away interior attacks, it cannot provide a consistent security strategy, and it has a single bottleneck spot and invalid spot, etc. 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 cooperation of them can implement the network security to a great extent. on the one hand, 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; on the other hand, firewall loads dynamic rules to hold up the intrusion, controls the data traffic of IDS and provides the security protection of IDS**

Keywords— ***Protocol, Detection, Generation, Prevention,***

I INTRODUCTION

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 and Intrusion Detection (IDS) are adopted more frequently. Network attacks a crucial element in providing networks with the reliability required in today's competitive environment. However, while most firewalls provide effective access control, many are not designed to detect an attacks at the application level.

Many methods have been developed to secure the network infrastructure and communication over the Internet, among them the use of firewalls, encryption, decryption and virtual private networks. Intrusion detection is a relatively new addition to such techniques. Intrusion detection system started appearing in the last few years. Using intrusion detection system, you can collect and use information from known types of attacks and find out if someone is trying to attack your network or particular hosts. The information collected can be used to hardening your network security, and legal purposes.

The Internet is a network of computer networks. It has evolved from the interconnection of networks around the globe. Internet connection may be used by “hackers” (or as some would rather call them “crackers”) to gain unauthorised access to your local network. Availability of computing facilities can also be targeted by Denial of Service (DoS) attacks. So the comparison of different types of firewalls and IDS are required for providing security to networks.

II . FIREWALL

Device that provides secure connectivity between networks used to implement and enforce a security policy for communication between networks. The term firewall has been around for quite some time and originally was used to define a barrier constructed to prevent the spread of fire from one part of a building or structure to another. Network firewalls provide a barrier between networks that prevents or denies unwanted or unauthorized traffic. Simple stated a firewall is protective device. It 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.

A) Types of Firewall

1) Packet Filtering Firewall

Packet filtering systems route packets between internal and external hosts, but they do it selectively. They allow or block certain types of packets in a way that reflects a site's own security policy.

2)Stateful-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 multipacket flows. Unlike packet-filtering firewalls, stateful firewalls keep track of the state of a connection: whether the connection is in an initiation, data transfer, or termination state. This is useful when you want to deny the initiation of connections from external devices, but allow your users to establish connections to these devices and permit the responses to come back through the Stateful firewall.

3)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, by itself, provide any security, but it helps to conceal the internal network layout and to force connections to go through a choke point. Connections to untranslated addresses will not work. 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). Network address translation systems can use different schemes for translating between internal and external addresses: Allocate one external host address for each internal address and always apply the same translation. This provides no savings in address space, and it slows down connections; it is normally a temporary measure used by sites that have been using illegal address spaces but are in the process of moving to using valid addresses. Dynamically allocate an external host address each time an internal host initiates a connection, without modifying port numbers. This limits the number of internal hosts that can simultaneously access the Internet to the number of available external addresses. Create a fixed mapping from internal addresses to externally visible addresses, but use port mapping so that multiple internal machines use the same external addresses.

Dynamically allocate an external host address and port pair each time an internal host initiates a connection. This makes the most efficient possible use of the external host addresses.

4) Application Based Firewall (Proxy Firewall)

It is a software package that allows or denies access across networks. Records can be kept of who tried to get in and what those who were allowed in did. In this approach, the firewall goes still further in its regulation of traffic. The Application Level Gateway acts as a proxy for applications, performing all data exchanges with the remote system in their behalf. This can render a computer behind the firewall all but invisible to the remote system [HYPERLINK \l "16" 4].

It can allow or disallow traffic according to very specific rules, for instance permitting some commands to a server but not others, limiting file access to certain types, varying rules according to authenticated users and so forth. This type of firewall may also perform very detailed logging of traffic and monitoring of events on the host system, and can often be instructed to sound alarms or notify an operator under defined conditions.

Operations on Application Firewall:

Step -1 :HTTP Request initiated from 192.168.6.77:3128 Client Browser

Step- 2 : Firewall – HTTP Proxy Get request and filter based on rules and policy

Step-3: Examined HTTP Request from 60.45.2.6(application Firewall) towards web application server.

Step- 4: HTTP Response for 60.45.2.6 from internet server.

Step- 5: Again Proxy Firewall do content based filtering.

Step- 6: Response object forwarded to client machine's browser.

5) Hybrid firewalls

Recent advances in network infrastructure engineering and information security have caused a blurring of the lines that differentiate the various firewall platforms discussed earlier. As a result of these advances, firewall products currently incorporate functionality from several different classifications of firewall platforms. For example, many Application-Proxy Gateway firewall vendors have implemented basic packet filter functionality in order to provide better support for UDP (User Datagram) based applications. Likewise, many packet filter or Stateful inspection packet filter firewall vendors have implemented basic application-proxy functionality to offset some of the weaknesses associated with their firewall platform. In most cases, packet filter or Stateful inspection packet filter firewall vendors implement application proxies to provide improved network traffic logging and user authentication in their firewalls.

Often, the best choice is a firewall that offers a hybrid architecture combining packet filtering and application layer proxies. This lets organizations their firewall protection to optimize performance while maintaining the appropriate level of security for the corresponding risk. Hybrid firewalls use simple packet filtering to provide high throughput for lowest-risk traffic, State full inspection for slightly riskier traffic, and the application layer gateway where the risk of data-driven attacks is highest.

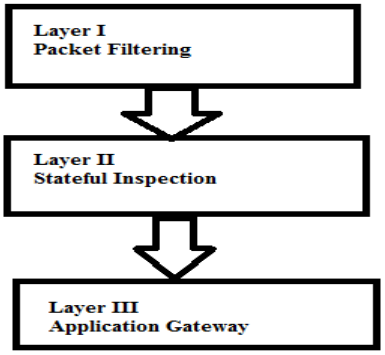

Figure 1.1 Hybrid firewalls architecture

B) Comparison of different types of Firewalls

We can summarize the differences among the several types of firewalls we have studied in depth. The comparisons are shown in Table 1.1

Table 1.1 Comparison of firewall Types

Packet Filtering	Stateful Inspection	Application Proxy	Hybrid Firewall
Simplest	More complex	Even more complex	Similar to packet filtering firewall
Sees only addresses and service protocol type	Can see either addresses or data	Sees full data portion of packet	Can see full data portion of packet
Auditing difficult	Auditing possible	Can audit activity	Can and usually does audit activity
Screens based on connection rules	Screens based on information across packets—in either header or data field	Screens based on behavior of proxies	Typically, screens based on information in a single packet, using header or data
Complex addressing rules can make configuration tricky	Usually preconfigured to detect certain attack signatures	Simple proxies can substitute for complex addressing rules	Usually starts in "deny all inbound" mode, to which user adds trusted addresses as they appear

C) Limitations of firewall

Firewalls offer excellent protection against network threats, but they aren't a complete security solution. Certain threats are outside the control of the firewall. You need to figure out other ways to protect against these threats by incorporating physical security, host security, and user education into your overall security plan. Some of the weaknesses of firewalls are discussed in the sections that follow.

- A firewall can't protect you against malicious insiders
- A firewall can't protect you against connections that don't go through it
- A firewall can't protect against completely new threats
- A firewall can't fully protect against viruses
- A firewall can't set itself up correctly
- A Firewalls don't deal with the real problem

III. INTRUSION DETECTION SYSTEM

Intrusion detection is a set of techniques and methods that are used to detect suspicious activity both at the network and host level. Intrusion detection systems fall into two basic categories: signature-based intrusion detection systems and anomaly detection system. Intruders have signatures, like computer viruses, that can be detected using software. You try to find data packets that contain any known intrusion-related signatures or anomalies related to Internet protocols. Based upon a set of signatures and rules, the detection system is able to find and log suspicious activity and generate alerts. Anomaly-based intrusion detection usually depends on packet anomalies present in protocol header parts. In some cases these methods produce better results compared to signature-based IDS. Usually an intrusion detection system captures data from the network and applies its rules to that data or detects anomalies in it.

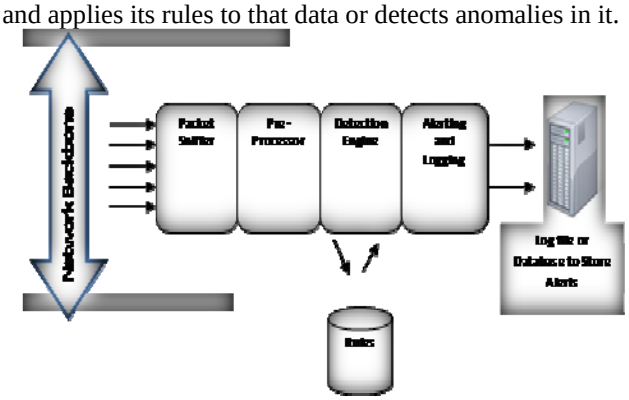

Fig. 1.2 Intrusion Detection Systems

Fig 1.2 shows very basic structure of Intrusion Detection System. Snort is primarily a rule-based IDS, however input plug-ins are present to detect anomalies in protocol headers.Snort uses rules stored in text files that can be modified by a text editor. Rules are grouped in categories. Rules belonging to each category are stored in separate files. These files are then included in a main configuration file called “snort.conf”. Snort reads these rules at the start-up time and builds internal data structures or chains to apply these rules to captured data. Finding signatures and using them in rules is a tricky job, since the more rules you use, the more processing power is required to process captured data in real time. It is important to implement as many signatures as you can using as few rules as possible. Snort comes with a rich set of pre-defined rules to detect intrusion activity and you are free to add your own rules at will. You can also remove some of the built-in rules to avoid false alarms.

A) Types of IDS

1) Network IDS

NIDS are intrusion detection systems that capture data packets travelling on the network media (cables, wireless) and match them to a database of signatures. Depending upon whether a packet is matched with an intruder signature, an alert is generated or the packet is logged to a file or database. One major use of Snort is as a NIDS30]

2) Host IDS or HIDS

Host-based intrusion detection systems or HIDS are installed as agents on a host. These intrusion detection systems can look into system and application log files to detect any intruder activity. Some of these systems are reactive, meaning that they inform you only when something has happened. Some HIDS are proactive; they can sniff the network traffic coming to a particular host on which the HIDS is installed and alert you in real time[HYPERLINK \l "Bry" 26].

3) Protocol based IDS

Orifice based IDS is installed on a server and it analyzes the server. IT sits at the fromt end of the server, monitoring and analyzing the dynamic behavior and state of the communication protocol between a connected device and server.

4)Application protocol based IDS

Application protocol based IDS normally sit between group of services/processes monitors and analyze the behavior and state of application protocol in use by the system between two connected devices.

5)Anomaly based IDS

Anomaly based IDS detects computer intrusions by monitoring system activity and classifying it is either normal or anomalous. It attempts to characterize abnormal behavior, and tries to detect any deviation from normal behavior. The advantage of anomaly based detection is a relatively high detection rate for new types of intrusions.

6) Misuse Based

It is also called as Signature based IDS. It performs the simple process of matching patterns corresponding to a known attack type. It is also known as pattern based IDS. The main advantage of signature based IDS is that it has a relatively low rate of false alarms, which means it has relatively high precision. And the main disadvantage of these IDS is that the detection rate of attacks is relatively low, because attacker will try to modify the basic attack signature in such a way that it will not match the known signatures of that attack and it cannot detect a new attack for which a signature is not yet installed in the database.

7) Hybrid based

Hybrid based IDS combines one or more approaches. Host agent data is combined with network information to form a comprehensive view of the network.

B) Function of IDS

Intrusion Detection System performs variety of functions

- Monitoring and analysis for user and system activity
- Auditing of system configurations and vulnerabilities
- Assessing the integrity of critical system and data files
- Recognition of activity patterns reflecting known attacks
- Statistical analysis for abnormal activity patterns
- Operating System audit trail management, with recognition of user activity reflecting policy violations.

C) Limitations of IDS

- Detect attack only after they have entered the network, and do nothing to stop attacks only just attacks traffic and send alert to trigger.
- Cannot expect to detect all malicious activity at all-time handling alert to trigger false positive or false negative alarm.
- Cannot integrated with filtering rules security to stop traffic from attacking.

IV .WHERE FIREWALL AND IDS SHOULD BE PLACED IN NETWORK TOPOLOGY?

Depending upon your network topology, you may want to position intrusion detection systems at one or more places. It also depends upon what type of intrusion activities you want to detect: internal, external or both. For example, if you want to detect only external intrusion activities, and you have only one router connecting to the Internet, the best place for an intrusion detection system may be just inside the router or a firewall. If you have multiple paths to the Internet, you may want to place one IDS box at every entry point. However if you want to detect internal threats as well, you may want to place a box 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. Your decision really depends upon your security policy, which defines what you really want to protect from hackers. Figure shows typical locations where you can place an intrusion detection system.

Typically you should place IDS behind each of your firewalls and routers. In case your network contains a demilitarized zone (DMZ).

Figure 1.3 shows where IDS and firewall should be placed in network topology.

We have studied different types of firewalls , types of IDS, their functioning, where firewall and IDS should be placed in network topology and their limitations . So to improve security system in networking it is necessary to implement Intrusion prevention system.

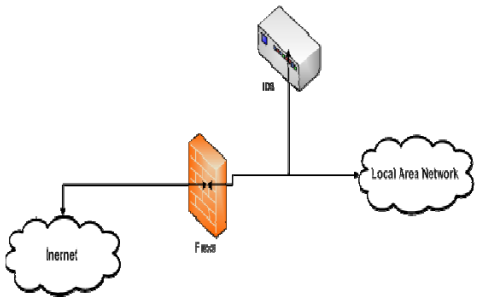

Figure 1.3 Typical locations for an intrusion detection system and firewall.

V. INTRUSION PREVENTION SYSTEM

Intrusion Prevention System adds the firewall rules for dropping the incoming malicious packets. The IPS stops the attack itself and terminate the network connection or user session that is being used for the attack, Block access to the target (or possibly other likely targets) from the offending user account, IP address, or other attacker attribute .Block all access to the targeted host, service, application, or other resource. The IPS could change the configuration of other security controls to disrupt an attack. Common examples are reconfiguring a network device (e.g., firewall, router, switch) to block access from the attacker or to the target, and altering a host-based firewall on a target to block incoming attacks. Some IPSs can even cause patches to be applied to a host if the IPS detects that the host has vulnerabilities.

A) The IPS can change the content of attack

Some IPS technologies can remove or replace malicious portions of an attack to make it benign. A simple example is an IPS removing an infected file attachment from an e-mail and then permitting the cleaned email to reach its recipient. A more complex example is an IPS that acts as a proxy and normalizes incoming requests, which means that the proxy repackages the payloads of the requests, discarding header information. This might cause certain attacks to be discarded as part of the normalization process.

B) Functions of IPS

- To supervise the behavior of the application
- To create rules for the application
- To issue alerts in case of violations
- To understand the IP networks
- It has a mastery over the network probes and the logs analysis
- It can defend the vital functions of the network carrying out an analysis with high velocity.

VI. CONCLUSION

This study has proved that both the firewall and intrusion detection systems still need to be improved to ensure an unfailing security for a network. They are not reliable enough (especially in regard to false positives and false negatives) and they are difficult to administer. To assure an effective computerized security, it is strongly recommended to have a combination of several types of Intrusion detection system.

However, these technologies require to be developed in the coming years due to the increasing security needs of businesses and changes in technology that allows more efficient operation detection systems. This paper provided a new way of looking at network research including types of firewalls, types of intrusion detection that are necessary, complete, and mutually exclusive to aid in the fair comparison of firewall, intrusion detection system and to aid in focusing research in this area of new trends like Intrusion Prevention System.

REFERENCES

[1] Korosh Golnabi, Richard K. Min, Latifur Khan, Ehab Al-Shaer, "*Analysis of Firewall Policy Rules Using Data Mining Techniques*", Network Operations and Management Symposium, 2006. NOMS 2006. 10th IEEE/IFIP .

[2] Robert Winding, Timothy Wright, and Michael Chapple, "*System Anomaly Detection: Mining Firewall Logs*", 2006 ,IEEE

[3] Wenke Lee, "*A Data Mining Framework for Constructing Features and Models for Intrusion Detection Systems*"

[4] Yuebin Bai, Hidetsune Kobayashi, "*Intrusion Detection System: Technology And Developement*", Proceedings of the17 th International Conference on Advanced Information Networking and Applications (AINA'03),IEEE

[5] Eugene Spafford, Diego Zamboni, "*Data Collection Mechanisms For Intrusion Detection*"

[6] Conference *(IM'2003)*, March 2003. E. Al-Shaer and H. Hamed. "*Firewall Policy Advisor for Anomaly Detection and Rule Editing.*" *IEEE/IFIP* Integrated Management

[7] Ehab Al-Shaer and Hazem Hamed, "*Discovery of Policy Anomalies in Distributed Firewalls*" in Proc. of IEEE INFOCOMM'04, vol. 23, no. 1, March 2004 pp. 2605-2616.

[8] D. Chapman and E. Zwicky. ,Building Internet Firewalls, Second Edition, Orielly & Associates Inc., 2000.

[9] Intrusion Detection & Prevention by Carl Endorf, Eugene Schultz and Jim Mellander McGraw -Hill © 2004

[10] A Database of Computer Attacks for the Evaluation of Intrusion Detection Systems by Kristopher Kendall

[11] C. Elkan, "Results of the KDD'99 classifier learning contest," *SIGKDD Explorations. ACM SIGKDD"*, vol. 1, no. 2, pp. 63–64, 2000.

[12] B. Mukherjee, L. T. Heberlein, and K. N. Levitt, "Network intrusion detection", *IEEE Network*, 8(3): 26-41, May/June 1994.

[13] W. Li, "A Genetic Algorithm Approach to Network Intrusion Detection", SANS Institute, USA, 2004.