A Comparative Study of Firewall and Intrusion Prevention System

Mr. D.Shiva rama krishna, Mr. Siva Rama Prasad Kollu, Mr. Ch.v.v.Narasimha Raju

***Abstract*—In the real world a firewall is a solid barrier between a precious asset on one side and a hazard on the other. Firewalls are often used to protect an organization from hazards on the Internet but they can, and probably should, also be used within an organization to separate different departments, working areas or networks. Locked offices and buildings cannot protect information if the computers holding it are open to everybody on the network. 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. The rapid growth of computer networks has changed the prospect of network security. An easy accessibility condition causes computer networks to be vulnerable against numerous and potentially devastating threats from hackers. Intrusion Prevention Systems (IPS) evolved after that to resolve ambiguities in passive network monitoring by placing detection systems on the line of attack. IPS in other words is IDS that are able to give prevention commands to firewalls and access control changes to routers.IPS can be seen as an improvement upon firewall technologies. It can make access control decisions based on application content, rather than IP address or ports as traditional firewalls do.**

Index Terms*—firewall. Intrusion Prevention Systems *(key words)

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.

Intrusion prevention systems (IPS), also known as intrusion detection and prevention systems (IDPS) are network security appliances that monitor network and/or system activities for malicious activity. The main functions of intrusion prevention systems are to identify malicious activity, log information about this activity, attempt to block/stop it, and report it. Intrusion prevention systems are considered extensions of intrusion detection systems because they both monitor network traffic and/or system activities for malicious activity. The main differences are, unlike intrusion detection systems, intrusion prevention systems are placed in-line and are able to actively prevent/block intrusions that are detected. More specifically, IPS can take such actions as sending an alarm, dropping the malicious packets, resetting the connection and/or blocking the traffic from the offending IP address. An IPS can also correct Cyclic Redundancy Check (CRC) errors, unfragment packet streams, prevent TCP sequencing issues, and clean up unwanted transport and network layer options

II. TYPES OF FIRE WALLS

A Firewall conjures up images of a safe and protected environment, but how safe is the firewall that guards the network as the first line of defense? It's anything but a wall! Firewalls can block traffic, but in order to share data and Connect to networked resources, holes are punched through it. This then leaves the network vulnerable to exploits and opens to malware. Fig1 shows various types of firewalls from static packet filter to application gateway.

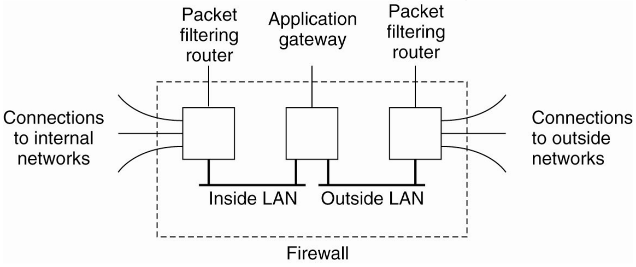

Fig 1: Firewall Types

A. *Static packet filtering firewalls*

Static packet filtering firewalls filter packets according to allow/deny rules based on the header fields like source/destination IP addresses and ports, protocol type and TCP flags. These firewalls do not look into the payload for malicious intent and it treats each packet as an individual entity. Border routers are good as static packet filters and are the first line of defense. The advantage is that it is fast, but it's prone to spoofing and fragmentation attacks. Stateful packet filtering firewalls are an improvement over static packet filtering firewalls, as it has a notion of *state*. In client/server applications, the client contacts the server with a request and receives a response. Since the client initiated the request the Response is allowed in, bypassing the firewall rules and optimizing the screening process,

Manuscript received November 20, 2014.

Mr D.Shiva rama krishna,Computer Science and Engineering, MLR Institute of Technology & management, Hyderabad, India, 9492673201.,

Mr K.Siva Rama Prasad,Computer Science and Engineering, MLR Institute of Technology & management, Hyderabad, India, 9866213002., (

Mr Ch.v.v.Narasimha Raju,Computer Science and Engineering, MLR Institute of Technology & management, Hyderabad, India, 9959969165.,

thereby improving firewall performance. However the firewall needs additional resources to maintain *state* tables. *State* tables can be maintained in hardware or software.

B. Application-gateway firewall

An application-gateway firewall is simply a type of proxy server that provides proxies for specific applications. The most common implementations of application-gateway firewalls address proxy services (such as mail, FTP, and telnet) so that they do not run on the firewall itself — something that is very good for the sake of security, given the inherent dangers associated with each. Mail services, for example, can be proxied to a mail server. Each connection is subject to a set of specific rules and conditions similar to those in packet-filtering firewalls except that the selectivity rules used by application-gateway firewalls are not based on ports, but rather on the to-be-accessed programs/services themselves (regardless of what port is used to access these programs). Criteria such as the source or destination IP address can, however, still be used to accept or reject incoming connections. Application-level firewalls can go even further by determining permissible conditions and events once a proxy connection is established. An FTP proxy could restrict FTP access to one or more hosts by allowing use of the get command, for example, while preventing the use of the put command. A telnet proxy could 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; these tools can similarly govern conditions of usage of a wide variety of applications, such as financial or process control applications.

Two basic types of application-gateway firewalls are currently available: (1) application-generic firewalls, and (2) application-specific firewalls. The former provide a uniform method of connection to every application, regardless of which particular one it is. The latter determine the nature of connections to applications on an application-by-application basis. Regardless of the specific type of application-gateway firewall, the security control resulting from using a properly configured one can be quite precise. When used in connection with appropriate host-level controls (e.g., proper file permissions and ownerships), application-gateway firewalls can render externally originated attacks on applications extremely difficult. Application-gateway firewalls also serve another extremely important function — hiding information about hosts within the internal network from the rest of the world, so to speak10. Finally, a number of commercial application-gateway firewalls available today support strong authentication methods such as token-based methods (e.g., use of hand-held authentication devices).

III. 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.

i) A firewall can't protect you against malicious insiders.
ii) A firewall can't protect you against connections that don't go through it.
iii) A firewall can't protect against completely new threats.
iv) A firewall can't fully protect against viruses.
v) A firewall can't set itself up correctly.
vi) A Firewalls don't deal with the real problem.

IV. INTRUSION PREVENTION SYSTEMS

Traditionally, firewalls and anti-virus programs try to block attacks and IDS tries to identify attacks as it occurs. Such techniques are critical to a defense in depth approach to security, but have limitations. A firewall can stop services by

Blocking certain port numbers but it does little to evaluate traffic that uses allowed port numbers. IDS can evaluate traffic that passes through these open ports but cannot stop it. IPS can proactively block attacks Signature based approaches focus on how an attack works, trying to detect certain strings. If the attacker makes minor changes by using the IDS evasion techniques discussed above, the previously written signatures no longer detect the attack. IPS focuses instead on what an attack does, which does not change.

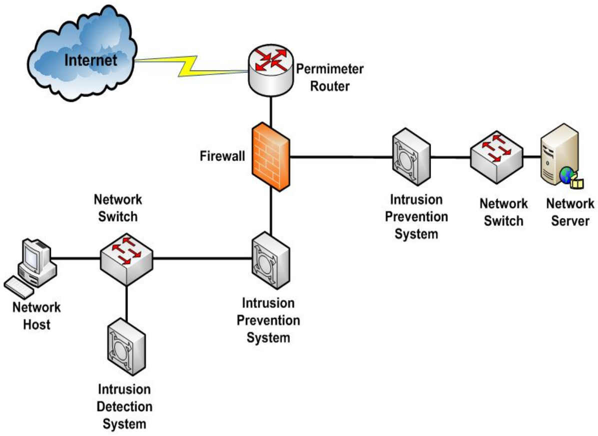

Fig 2: Intrusion Prevention System

V. TYPES OF INTRUSION PREVENTION SYSTEMS

Before you Intrusion prevention systems can be classified into four different types.

A. Network-based Intrusion Prevention System

Network-based intrusion prevention system (NIPS) monitors the entire network for suspicious traffic by analyzing protocol activity.

B. Wireless Intrusion Prevention Systems

Wireless intrusion prevention systems (WIPS) monitor a wireless network for suspicious traffic by analyzing wireless networking protocols.

C. Network Behavior Analysis

Network behavior analysis (NBA) examines network traffic to identify threats that generate unusual traffic flows, such as distributed denial of service (DDoS) attacks, certain forms of malware and policy violations.

D. Host-Based Intrusion Prevention System

Host-based intrusion prevention system (HIPS) an installed software package which monitors a single host for suspicious activity by analyzing events occurring within that host.

VI. DETECTION METHODS

One problem faced by all detection in IPS is that difficult to identify and recognized analyzing packet in real-time traffic. To detect suspicious threat, there are two approach (i) *Host-based approach* : Host-based are currently popular technologies, it is check for suspicious activity from the host or operating system level, the monitoring location use the agent component, which is useful before the host it reaches target of attack. The alarm triggered and provide intrusive this activity, and (ii) *Network-based approach*, the sniff and identify packet all inbound-outbound in out of the network. The combining Network-based with other security component, provides a active comprehensive network security

According to some reported work there are two categories based according to the detection method packet is shown in

Fig 3: (i) anomaly-based detection, and (ii) misuse-based detection

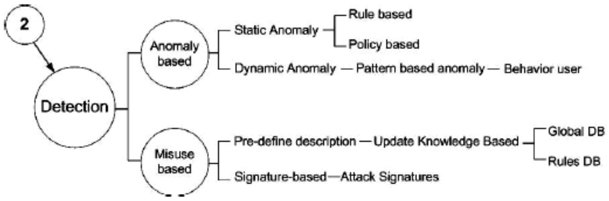
2
Detection
Anomaly based
Static Anomaly
Rule based
Policy based
Dynamic Anomaly — Pattern based anomaly — Behavior user
Misuse based
Pre-define description — Update Knowledge Based
Global DB
Rules DB
Signature-based—Attack Signatures

Fig 3: Mapping Problem

A. Anomaly-based

Anomaly-based detection, the key to the application of anomaly detection methods to the field known as threat consists in a simple but critical hypothesis. Hence, anomaly detection has the capability of detecting new types of intrusions and need list of profile data as a normal data, builds model of normal behaviour and automatically detect any violation of it to generate alarm.

Techniques used in anomaly detection, (i) threshold detection, (ii) statistical measures, and (ii) other technology (i.e. data mining, neural network, genetic algorithm and immune system model. According to Wu and Banzhaf in 2010, anomaly detection searches for intrusive activities by comparing network traffic to those established acceptable normal usage patterns learned from training data, they divided three classifications of the anomaly detection techniques according to the nature of the processing, such as (i) statistic based, (ii) knowledge based, and machine learning based. Advantage this approach is ability to detect novel attacks for which signatures have not been defined yet. Unfortunately, this approach produces many false alarms and dally time consuming for research intensive to obtain update accurate and comprehensive profiles of normal behavior. This means, it requires a large set of training data with consist network environment system log.

B. Misuse-based

In this approach its find threat by examine the network traffic in search of direct matches to known pattern of packet (signature or rules). Additionally, proposal depicts clearly different between misuse-based and anomaly-based with snort rule structure. Accordingly, a disadvantage of this approach is that it can only detect intrusion that match a pre-defined rule, the set of signature need to be constantly update manually to known the new threat. Fortunately, this method can be highly accurate to increasingly precision identify known attack and their variations. Furthermore, misuse-based produce low false alarm.

VII. IPS AND IDS VS FIREWALLS

Not having an IPS system result in attacks going unnoticed. Don’t forget a firewall does the filtering, blocking and allowing of addresses, ports, service, but also allows some of these through the network as well. However this means that the access allowed is just let through, and firewalls have no clever way of telling whether that traffic is legit and normal. This is where the IPS and IDS systems come into play. So where firewalls block and allow traffic through, IDS/IPS detect and look at that traffic in close detail to see if it is an attack. IDS/IPS systems are made up of sensors, analyzers and GUI’s in order to do their specialized job.

VIII. IPS TECHNIQUES TO DEFEND AGAINST ATTACKS

Intrusion prevention sensors look at header and data portions of the traffic looking for suspicious traffic that indicate malicious activity.

IPS/IDS solution have the ability to detect threats using a database of signatures, using anomaly detection techniques looking for abnormal behaviour within protocols and can also use or integrate with antivirus for malware detection. Anomaly detection systems target traffic that isn't necessarily bad but used with bad intentions such as lots of traffic to overwhelm a system. TCP Syn Flood attack is an example.

IPS have the ability to take actions on defined policies such as blocking a connection, providing alerts, logging the event, quarantining the host or a combination of these. Policies define the rules that specify what should be detected and type of response required. Policies will include both signature based rules and anomaly detection rules for learning typical network traffic and setting thresholds for these. DOS and reconnaissance rules are based on traffic statistics.

IPS solutions also provide logging and alerting on recent attacks so it should be easy to understand and trace an attack, and provide supporting tools that would aid in blocking attacks. Also clicking the attack should provide detailed information about the attack and what can be done to resolve such an attack. IPS and IDS systems have the ability to search for attacks using different characteristics of an attack such as by attack name, impacted applications, attack ID and so on.

IPS and IDS systems should be configured to only use signatures they require and to protect the assets required as using all signatures and pointing it to protect everything will use up much more resources such as CPU, memory and bandwidth. So if it were web server that required protection then only signatures for web servers should be utilised and protecting only the DMZ where web servers are located. This can also be further defined to be protocols such as HTTP, RDP, or systems like Unix, Windows or applications such as IIS and Adobe.

Attacks should have a severity level that ties to a response such as block, quarantine, log, notify or a combination of these.

IX. CONCLUSION & FUTURE WORKS

Firewalls, anti-virus, and IDS have their place in the security landscape, each with its unique features. Depending on business needs, budget constraints, and organizational requirements we need to draw up a security policy and that policy will determine the mix of components that need to be installed, to meet security goals.

IPS adds to the defence in depth approach to security and is an evolution of IDS technology. Its proactive capabilities will help to keep our networks safer from more sophisticated attacks. Today the use of tunnelling and encryption means putting more content outIPS has additional features to secure computer network system. The additional features identifying and recognizing suspicious threat trigger alarm, event notification, through responsible response. In this preliminary observation from previously researcher, hybrid techniques is one of solution for classification and detection intrusion threat. Proposed hybrid IPS takes the advantages to increase accuracy and precision normal or suspicious threat. There are some researchers combine misuse-based and anomaly-based to solve this problem. In this work we present approaches are state-of-the-art, considers and addresses several aspect of IPS, and also provide effort to summarizes the main current status and the promising and interesting future directions and challenges. In this paper, we present a mapping problem and challenges in IPS with others related work. There are some issues can be researched, i.e. heterogeneous sensor, distributed sensor, and combine hybrid early detection/ prevention mechanism with other approaches. Future work will focus on accuracy and precision with our algorithm based on behavior-based prevention, which is an experiment with our data set of real-traffic network.

REFERENCES

[1] E. Guillen, D. Padilla, and Y. Colorado, "based Intrusion Detection and Prevention Systems," Latin-American Conference Communications, 2009, pp. 0-4.

[2] B. Cao, Z. Zhihong, L. Tie, Y. Zhongde, and L. Jiren, "A Study on Performance Improvement of Gateway Anti-Virus System Based on File Scanning," Control and Decision Conference 09, 2009, pp. 2293-2295.

[3] T. Ghorbani, A.A., Lu, W., Network Intrusion Detection and Prevention : Concepts and Technique, Springer, 2009.

[4] Bace, Rebecca, and Peter Mell. " Intrusion Detection Systems." URL:
[5] Bobbitt, Mike. "Inhospitable Hosts." Information Security. Volume 5, No.10 (2002): 35-47.

[6] Carter, Earl, and Rick Stiffler. Cisco Secure Intrusion Detection System. Pearson Education, 2001.

[7]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.

[8] Eugene Spafford, Diego Zamboni, "Data Collection MechanismsFor Intrusion Detection" Conference (IM'2003), March 2003. E. Al-Shaer and H. Hamed.

[9] "Firewall Policy Advisor for Anomaly Detection and Rule Editing."IEEE/IFIP Integrated Management

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

Mr. D.Shiva Rama Krishna, has Bachelors and Master's Degree in the field of Computer science and Engineering. He has keen interest in the area of Cryptography & Network Security, Data Mining, Cloud Computing and has published several papers in National and International conferences and journals. He has attended several workshops and faculty development program.

Mr. Siva Rama Prasad Kollu, has Bachelors in the field of Information Technology and Master's Degree in the field of System Analysis and Computer Applications. He has keen interest in the area of Cryptography & Network Security, Cloud Computing and has published several papers in National and International conferences and journals. He has attended several workshops and faculty development program.

Mr. Ch.V.V.Narasimha Raju, , has Bachelors in the field of Information Technology and Master's Degree in the field of Computer science and Engineering.He has keen interest in the area of Cryptography & Network Security, Data Mining, and has published several papers in National and International conferences and journals. He has attended several workshops and faculty development program.