International Journal of Electronics Communication and Computer Engineering
Volume 5, Issue 6, ISSN (Online): 2249–071X, ISSN (Print): 2278–4209

Security Policy Based on Firewall and Intrusion Detection System

Hemdeep Kaur Bimbraw, O. P. Gupta
School of Electrical Engineering and Information Technology
Punjab Agricultural University, Ludhiana-141004

***Abstract* – Firewalls are usually the first component of network security. They separate networks in different security levels by utilizing network access control policies. The major function of the firewall is to protect the private network from non-legitimate traffic. The main purpose of a firewall system is to control access to or from a protected network. It implements a network access policy by forcing connections to pass through the firewall, where they can be examined and evaluated. Intrusion detection is the process of monitoring and searching networks of computers and systems for security policy violations. Intrusion Detection Systems (IDSs) are software or hardware products that automate this monitoring and analysis process. An IDS inspects all inbound and outbound network activity, system logs and events, and identifies suspicious patterns or events that may indicate a network or system attack from someone attempting to break into or compromise a system. The network security in today's world is a major concern because of increasing threats from malicious users. Therefore, designing a correct network security policy is a challenging task. To design filtering rules to formulate a sound firewall security policy and implement intrusion detection system to capture network packets and detect attacks to fulfill this gap.**

***Keywords* – Firewall, Intrusion Detection System, Network, Security Policy.**

I. INTRODUCTION

The growth of internet and the amount of information shared between networks has resulted in increased possibility of attacks. Most users suffer from attacks caused by hackers on the internet. Many users are still not aware of the network security measures that they need to adopt to prevent theses attackers from gaining unauthorized access to the network. Installing a firewall is the most basic security technique to prevent such illegitimate attacks. But the firewall must be configured correctly to make most use of it. Also another security measure is intrusion detection system which has the capability to detect any attack on the network by an outside user. Once this attack has been detected corrective steps can be taken to maintain network security. According to the technology of firewall, there are four basic types: packet-filtering, network address translation, agent-based and monitoring. Packet filtering technology has the advantage of simple and low cost application. The system requirements are as given: use a Linux host a firewall and intrusion detection system configured on it. Packet filtering firewall is a software to view the packets flow through the header which determines the fate of the whole package. It may decide to discard this package, accept the package or implement some other complex action. In the Linux system, the packet filtering is built into the core. At the same time, there are a number of skills on top of the packets, but it is most commonly still the examining header that used to determine the package fate. Packet filtering firewall makes use of filters. An intrusion detection system (IDS) is a device or software application that inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system. IDS can be categorized into misuse detection or anomaly detection. In misuse detection, the IDS analyses the information it gathers and compares it to large databases of attack signatures. Essentially, the IDS look for a specific attack that has already been documented. In anomaly detection, the system administrator defines the baseline, or normal, state of the network's traffic load, breakdown protocol, and typical packet size. The anomaly detector monitors network segments to compare their state to the normal baseline and look for anomalies. Snort is an open source IDS that works fine for many individuals, small businesses, and departments. This lightweight network intrusion detection system excels at traffic analysis and packet logging on IP networks. Through protocol analysis, content searching, and various preprocessors, Snort detects thousands of worms, vulnerability exploit attempts, port scans, and other suspicious behavior. Snort uses a flexible rule-based language to describe traffic that it should collect or pass, and a modular detection engine. Packet filtering module, the intrusions prevention function of the IPS, is deployed in both inbound and outbound of the network, and transparent packet forward or filter the packet data according the rules library. Netfilter is a packet filtering subsystem in the Linux kernel stack and has been there since kernel 2.4.x. Netfilter is a framework for packet filtering and can be expanded easily. Iptables is a user space application program that allows a system administrator to configure the tables provided by the Linux kernel firewall and the chains and rules it stores. Snort is an open source, freely available intrusion detection systems. It is based on Libpcap, and can be modified and reprogramming. According to the characters above, we can combine Snort and Netfilter easily. There are seven alert modes available at the command line: full, fast, socket, syslog, console, cmg, and none. The default logging and alerting mechanisms are to log in decoded ASCII format and use full alerts. The full alert mechanism outputs the alert message in addition to the full packet headers, it would need more time and space.

The network security in today's world is a major concern because of increasing threats from malicious users. Therefore, designing a correct network security

policy is a challenging task. To design filtering rules to formulate a sound firewall security policy and implement intrusion detection system to capture network packets and detect attacks to fulfill this gap.

II. METHODOLOGY

In this paper describes the firewalls and intrusion detection system. Security depends on firewalls type, location, installation, network packets, protocols and services. It also depends upon the intrusion detection types and methods for knowledge of the reader and improving the network security, privacy, activities. Author explains the different possibilities to improve the security of network security by reporting the work of different workers of this field. This paper will also be beneficial for the students of information technology and also for those are working in the field of information technology.

III. FIREWALLS

Firewalls are usually the first component of network security. They separate networks in different security levels by utilizing network access control policies. The major function of the firewall is to protect the private network from non-legitimate traffic. Firewalls are located between the Internet and private network. They can monitor the outgoing and incoming traffic; also they can prevent the harmful traffic and attacks from Internet. They also can stop the non-legitimate outgoing traffic. If a computer from the local network is attacked by an intruder and generates non-legitimate traffic, the firewall can prevent and detect the computer. Firewall can detect such succeeded attack, so it can be recovered. A firewall is the most effective way to connect a network to the Internet and still protect that network [1]**.** Firewalls create a separation between public networks (Internet) and private networks by examining the traffic according to the predefined policy, and allowing only legitimate traffic to pass between the public and private network. They help implementing a larger security policy that defines the services and access to be permitted. It is an implementation of that policy in terms of a network configuration, one or more host systems and routers, and other security measures such as advanced authentication in place of static passwords. A firewall system can be a router, a personal computer, a host, or a collection of hosts and/or routers, set up specifically to shield a site or subnet from protocols and services that can be abused from hosts outside the subnet [2]**.**

Firewalls must be installed at the choke points to control network traffic and implement network security policy of the organization. Firewalls achieve this by examining the all incoming and outgoing network traffic according to the predefined firewall policy. All network traffic must pass through the firewall, which ensures that only permitted traffic are allowed through [3]**.** Firewalls have some advantage like firewalls can stop non-legitimate traffic at first point, can filter protocols and services that are either not necessary or that cannot be adequately secured from exploitation [4]**,** can "hide" names of internal systems and internal network schema, thereby revealing less information to outside hosts [4] and can concentrate extended logging of network traffic on one system. Firewalls also disadvantages as firewalls utilize manually configured set of rules to differentiate legitimate traffic from non-legitimate traffic, can't react to a network attack – nor can it initiate effective counter-measures [4], can only examine network packets that pass through them, do not examine network traffic between any two inside hosts, most firewalls do not analyze the contents of the data packets that make up network traffic and firewall policies can vary in effectiveness, depending on the expertise of the security manager and the complexity of the network environment.

A. Significance of firewalls

A firewall is a focus for security decisions: All traffic in and out must pass through this single, narrow checkpoint. A firewall provides enormous amount of advantages for network security because it will think to concentrate your security measures on this choke point: the point where your network connects to the Internet. Focusing your security in this way is far more efficient than spreading security decisions and technologies around, trying to cover all the bases in a piecemeal fashion. Although firewalls at most sites find that concentrating the most effective security hardware and software at the firewall is less expensive, more effective than other security measures, and certainly less expensive than having inadequate security. In particular, one-time password systems and other add-on authentication software could be located at the firewall as opposed to each system that needed to be accessed from the Internet. It is also the only way to collect manageable network usage statistics which is helpful for detecting whether it is implementing the desired policy and detecting any intrusion.

It can enforce security policy: A firewall provides the means for implementing and enforcing a network access policy. In effect, a firewall provides access control to users and services. A firewall can greatly improve network security and reduce risks to hosts protected on the subnet by filtering inherently insecure services. Many of the services that people want from the Internet are inherently insecure. The firewall enforces the site's security policy, allowing only "approved" services to pass through and those only within the rules set up for them. For example, one site might decide that only one internal system can communicate with the outside world. Still another site might decide to allow access from all systems of a certain type, or belonging to a certain group; the variations in site security policies are endless. A firewall may be called upon to help enforce policies that are more complicated. For example, perhaps only certain systems within the firewall are allowed to transfer files to and from the Internet; by using other mechanisms to control which users have access to those systems, you can control which users have these capabilities. Depending on the technologies you choose to implement your firewall, a firewall may have a greater or lesser ability to enforce such policies.

It provides enhanced privacy: Privacy is of great concern to certain sites that would be considered innocuous information might actually contain clues that will be useful to an attacker. Using a firewall, some sites wish to block services such as 'finger' and 'Domain Name Service'. Finger displays information about users such as their last login time whether they've read mail, and other items. But, 'finger 'could leak information to attackers about how often a system is used whether the system has active users connected, and whether the system could be attacked without drawing attention. Firewalls can also be used to block DNS information about site systems, thus the names and IP addresses of site systems would not be available to Internet hosts. Some sites feel that by blocking this information, they are hiding information that would otherwise be useful to attackers.

It can log internet activities: The firewall can log accesses and provide valuable statistics about network usage. A firewall is appropriate alarms that sound when suspicious activity occurs can also provide details on whether the firewall and network are being probed or attacked. It is important to collect network usage statistics and evidence of probing for a number of reasons. Network usage statistics are also important as input into network requirements studies and risk analysis activities. A firewall can log Internet activity efficiently because all traffic passes through the firewall, the firewall provides a good place to collect information about system and network use and misuse. As a single point of access, the firewall can record what occurs between the protected network and the external network [1].

It limits your exposure: Sometimes, a firewall will be used to keep one section of your site's network separate from another section. By doing this, the problem that affects one section protects from spreading through the entire network. In some cases, you will do this because one section of your network may be more trusted than another; in other cases, because one section is more sensitive than another. Whatever the reason, the existence of the firewall limits the damage that a network security problem can do to the overall network.

The main purpose of a firewall system is to control access to or from a protected network. It implements a network access policy by forcing connections to pass through the firewall, where they can be examined and evaluated.

Firewalls in network security: Firewalls can control all incoming and outgoing traffic because they are placed at the choke point between the public network and private network. Firewalls act like traffic cops and perform the critical task of filtering traffic crossing the network boundary according to the predefined security rules (firewall policy).These rules can be specified at the network layer and/or at the application layer. Firewalls utilize these static, manually configured, security policies to differentiate legitimate traffic from non-legitimate traffic. Typical reasons for using a firewall to protect a private network to prevent unauthorized external users from accessing computing resources on the internal network. This is necessary because it is extremely difficult and costly to attempt to secure all the hosts within a private network, to control internal user access to the external network to prevent the export of proprietary information, to avoid the negative public relations impact of a break in, to provide a dependable and reliable connection to the Internet, so that employees do not implement their own insecure private connections [5].

Firewalls not complete security solution: Although, firewalls are an important part of network security, they do not provide airtight perimeter protection and, thus, are not a complete security solution. The average firewall is designed to deny clearly suspicious traffic – such as an attempt to Telnet to a device when corporate security policy forbids Telnet access completely – but is also designed to allow some traffic through – Web traffic to an internal Web server, for example. Certain threats are outside the control of the firewall. Some of the weaknesses of firewalls are [1]:

A firewall cannot protect against malicious insiders: A firewall might keep a system user from being able to send proprietary information out of an organization over a network connection; so would simply not have a network connection. However, that same user could copy the data onto disk, tape, or paper and carry it out of the building in his or her briefcase. Once a back door has been installed on a server, the attacker has ensured that he will have unfettered access to that machine at any point in the future [6]. That is to say, firewalls can prevent most of the malicious access attempts but they cannot stop attacks if they are not specified in their rule sets.

It cannot protect against connections that don't go through it: A firewall can effectively control the traffic that passes through it; however, there is nothing a firewall can do about traffic that doesn't pass through it. For example, if the site allows dial-in access to internal systems behind the firewall, it has absolutely no way of preventing an intruder from getting in through such a modem. Sometimes, technically expert users or system administrators set up their own "back doors" into the network, either temporarily or permanently, because they chafe at the restrictions that the firewall places upon them and their systems. The firewall can do nothing about this. It is really a people-management problem, not a technical problem.

It cannot protect from new threats: A firewall is designed to protect against known threats. Firewall monitors traffic according to predefined rules and decide whether to allow or prevent the connection. No firewall can automatically defend against every new threat that arises. A well-designed one may also protect against new threats. (For example, by denying any but a few trusted services, a firewall will prevent people from setting up new and insecure services.)

It cannot protect from viruses: Firewalls determine certain parts of the network packets mostly for source and destination addresses and port numbers, not for the details of the data. They cannot prevent from the attacks that are in the other parts of the packets.

B. Network Packets, Protocols and Services

Firewall makes decisions based on the network packets content. Content of the packets depends on the network

protocols. The most popular one is TCP/IP protocol suite. The function of the TCP/IP protocol stack, or suite, is the transfer of information from one network device to another. TCP/IP protocol suits layers are [7]:

Application Layer (Layer 4): The application layer supports addressing protocols and network management. It also has protocols for file transfer, e-mail, and remote login. Examples of these protocols are: *DNS* (Domain Name System), *WINS* (Windows Internet Naming Service), *POP3* (Post Office Protocol), *SMTP* (Simple Mail Transport Protocol), *SNMP* (Simple Network Management Protocol), *FTP* (File Transfer Protocol), *TFTP* (Trivial File Transfer Protocol) and *HTTP* (Hypertext Transfer Protocol).

Transport Layer (Layer 3): The transport layer enables a user's device to segment several upper-layer applications for placement on the same transport layer data stream, and enables a receiving device to reassemble the upper-layer application segments [7]. The transport layer data stream is a logical connection between the endpoints of a network, and provides transport services from a host to a destination. This service is sometimes referred to as end-to-end service. The two protocols found at the transport layer are TCP (Transmission Control Protocol) and UDP (User Datagram Protocol). Either of these two protocols is used by the application layer process, the choice depends on the application's transmission reliability requirements.

TCP (Transmission Control Protocol) is a connection-oriented, reliable protocol. TCP provides flow control by using sliding windows and ensures reliability by using sequence numbers and acknowledgments. TCP re-sends anything that is not received correctly and supplies a virtual circuit between end-user applications. The advantage of TCP is that it provides guaranteed delivery of segments.

UDP is responsible for transmitting messages, no software checking for segment delivery is provided at this layer. The advantage that UDP provides is speed. Since UDP provides no acknowledgments, less traffic is sent across the network, making the transfer faster. UDP is used for data streaming of audio and video where consistent speed is more important than reliable delivery. Protocols that use UDP include TFTP, SNMP, Network File System (NFS), and Domain Name System (DNS).

Internet Layer (Layer 2): The Internet layer of the TCP/IP stack corresponds to the network layer of the OSI model. These layers are responsible for getting packets through a network using software addressing. Several protocols operate at the TCP/IP Internet layer that corresponds to the OSI network layer:

IP -- provides connectionless, best-effort delivery routing of datagram; is not concerned with the content of the datagram; looks for a way to move the datagram to their destination

ICMP -- provides control and messaging capabilities

ARP -- determines the Data Link Layer (MAC) addresses for known IP addresses

RARP -- determines network addresses when data link layer addresses are known

Network Access Layer (Layer1): The combination of OSI data link and physical layers deals with pure hardware (wires, satellite links, network interface cards, etc.) and access methods such as CSMA/CD (carrier sensed multiple access with collision detection). Ethernet exists at the network access layer - its hardware operates at the physical layer and its medium access control method (CSMA/CD) operates at the data link layer [8].

There are number of standard Internet services that users want and that most sites try to support. HTTP for web services, SMTP for e-mail and FTP for file transfer.

HTTP (Hypertext Transfer Protocol) is the Internet standard that supports the exchange of information on the World Wide Web, as well as on internal networks. It supports many different file types including text, graphics, sound, and video. It defines the process by which Web browsers originate requests for information to send to Web servers.

SMTP (Simple Mail Transport Protocol) governs the transmission of e-mail over computer networks. It does not provide support for transmission of data other than plain text.

FTP (File Transfer Protocol) is a reliable connection-oriented service that uses TCP to transfer files between systems that support FTP. It supports bi-directional binary file and ASCII file transfers.

Every packet from the upper layer is the data for lower layer; it adds a header to packet and pass to lower layer. Firewalls are mostly dealing with the information the header contains. The content of the header includes source and destination of IP address, transport protocol, source and destination application port, eventually, specific protocol flags (e.g. TCP's ACK- and SYN-flag) and network interface a packet.

C. Firewall Controls

There are four general techniques that firewalls use to control access and enforce the site's security policy. Originally, firewall focused primarily on service control, but they have since evolved to provide all four [9]:

Service Control: Determines the types of Internet services that can be accessed, inbound or outbound. The firewall may filter traffic on the basis of IP address and TCP port number; may provide proxy software that receives and interprets each service request before passing it on; or may host the server software itself, such as a Web or mail service.

Direction Control: Determines the direction in which particular service requests may be initiated are allowed to flow through the firewall.

User Control: Controls access to a service according to which user is attempting to access it. This feature is typically applied to users inside the firewall perimeter (local users). It may also be applied to incoming traffic from external users; the latter requires some form of secure authentication technology.

Behavior Control: Controls how particular services are used. For example, the firewall may filter e-mail to eliminate spam, or it may enable external access to only a portion of the information on a local Web server.

D. Firewall types

There are several types of firewall products. Firewalls are classified into three main types based on their mechanism; packet filter firewalls, stateful inspection firewalls and application proxy-gateway firewalls [4].

Packet Filters: Packet filter firewalls are the most fundamental type of firewalls; they are the simplest firewalls to implement. Packet filters provide an efficient and general way to control network traffic. Packet filters provide transparent security since they work at lower layers. No changes are required to client and host applications. They filter the traffic based on packet's header content according to predefined specification criteria [4]:

- The source address of the packet, i.e., the Layer 3 address of the computer system or device the network packet originated from.
- The destination address of the packet, i.e., the Layer 3 address of the computer system or device the network packet is trying to reach.
- The type of traffic, that is, the specific network protocol being used to communicate between the source and destination systems or devices (often Ethernet at Layer 2 and IP at Layer 3).
- Possibly some characteristics of the Layer 4 communications sessions, such as the source and destination ports of the sessions (e.g., TCP: 80 for the destination port be-longing to a web server, TCP:1320 for the source port belonging to a personal computer accessing the server).
- Sometimes, information pertaining to which interface of the router the packet came from and which interface of the router the packet is destined for; this is useful for routers with 3 or more network interfaces.

Packet filter firewalls has two strengths: speed and flexibility. Since they operate at lover layers and do not usually examine the data above Layer 3 (OSI model Network layer), they can operate very quickly. Since most networks can be accommodated using Layer 3 and below, they can be used to secure almost any type of network. Packet filter firewalls also possess several weaknesses [4].

E. Weaknesses of packet filter firewalls

- Packet filter firewalls do not examine upper-layer data, they cannot prevent attacks that employ application-specific vulnerabilities or functions. For example, a packet filter firewall cannot block specific application commands; if a packet filter firewall allows a given application, all functions available within that application will be permitted.
- The limited information available to the firewall, the logging functionality present in packet filter firewalls is limited. Packet filter logs normally contain the same information used to make access control decisions (source address, destination address, and traffic type).
- Most packet filter firewalls do not support advanced user authentication schemes. Once again, this limitation is mostly due to the lack of upper-layer functionality by the firewall.
- They are generally vulnerable to attacks and exploits that take advantage of problems within the TCP/IP specification and protocol stack, such as network layer address spoofing. Many packet filter firewalls cannot detect a network packet in which the OSI Layer 3 addressing information has been altered. Spoofing attacks are generally employed by intruders to bypass the security controls implemented in a firewall platform.
- Finally, due to the small number of variables used in access control decisions, packet filter firewalls are susceptible to security breaches caused by improper configurations. In other words, it is easy to accidentally configure a packet filter firewall to allow traffic types, sources, and destinations that should be denied based upon an organization's information security policy.

IV. Intrusion Detection Systems (IDS)

When a user of an information system takes an action that user was not legally allowed to take, it is called *intrusion* [10]. The intruder may come from outside, or the intruder may be an insider, who exceeds his limited authority to take action. Whether or not the action is detrimental, it is of concern because it might be detrimental to the health of the system, or to the service provided by the system. As information systems have come to be more comprehensive and a higher value asset of organizations, complex, *intrusion detection* subsystems have been incorporated as elements of operating systems, although not typically applications [10]. Most intrusion detection systems attempt to detect suspected intrusion, and then they alert a system administrator. Intrusion *detection* involves determining that some entity, an *intruder*, has attempted to gain, or worse, has gained unauthorized access to the system. None of the automated detection approaches of which we are aware seeks to identify an intruder before that intruder initiates interaction with the system. Of course, system administrators routinely take actions to prevent intrusion. These can include requiring passwords to be submitted before a user can gain any access to the system, fixing known vulnerabilities that an intruder might try to exploit in order to gain unauthorized access, blocking some or all network access, as well as restricting physical access. Intrusion detection systems are used in addition to such preventative measures.

Intruders are classified in two groups. *External intruders* do not have any authorized access to the system they attack. *Internal intruders* have some authority, but seek to gain additional ability to take action without legitimate authorization. J. P. Anderson divided internal intruders into three subgroups: masqueraders, clandestine, and legitimate [10]. In later related work, Brownell Combs has divided internal intruders into two categories. He separates internal users who have accounts on the system from pseudo-internal intruders who are, or can be thought of as being, physically in space of legitimate users, but have no accounts [10]. They do however have physical access to the same equipment used by those who have accounts. He shows how distinguishing the two categories can be distinguished enables better defense against the pseudo-internal intruders. To limit the scope of the problem of

detecting intrusions, system designers make a set of assumptions. Total physical destruction of the system, which is the ultimate denial of service, is not considered. Intrusion detection systems are usually based on the premise that the operating system, as well as the intrusion detection software, continues to function for at least some period of time so that it can alert administrators and support subsequent remedial action.

Second layer in the perimeter defense is intrusion detection systems (IDSs). The audits of security existed before the intrusion detection. Audit is the process of generating, storing and revising events of a system chronologically. IDS is the evolved version of the traditional audits [11].

Intrusion detection is the process of monitoring and searching networks of computers and systems for security policy violations [12]. Intrusion Detection Systems (IDSs) are software or hardware products that automate this monitoring and analysis process. An IDS inspects all inbound and outbound network activity, system logs and events, and identifies suspicious patterns or events that may indicate a network or system attack from someone attempting to break into or compromise a system [13].

Theoretically, IDSs work like a burglar alarm, alerting security managers that an attack may be taking place so that they can respond accordingly. IDSs trigger these alerts by detecting anomalous traffic patterns or "signatures" that are characteristic of an attack. As in the physical world, our logical burglar alarm provides valuable notification that someone has managed to breach perimeter security measures, and should allow security managers to determine exactly what happened during the attack, and hopefully provide indications of how the security weakness might be addressed.

It is also assumed that intrusion detection is not a problem that can be solved once; continual vigilance is required. Complete physical isolation of a system from all possible, would-be external intruders is a simple and effective way of denying external intruders, but it may be unacceptable because physical isolation may render the system unable to perform its intended function. Some possible solution approaches cannot be used because they are in conflict with the service to be delivered.

In addition, potential internal intruders legitimately have access to the system for some purposes. Therefore, it is assumed that at least internal intruders, and possibly external intruders, have some access and therefore have some tools with which to attempt to penetrate the system. It is typically assumed that the system, usually meaning the operating system, does have flaws that can be exploited. Today, software is too complicated to assume otherwise. New flaws may be introduced in each software upgrade. Patching the system could eliminate known vulnerabilities. However, some vulnerabilities are too expensive to fix, or their elimination would also prevent desired functionality [10]. Vulnerabilities are usually assumed to be independent. Even if a known vulnerability is removed, a system administrator may run intrusion detection software in order to detect *attempts* at penetration, even though they are guaranteed to fail. Most intrusion detection systems do not depend on whether specific vulnerabilities have been eliminated or not. This use of intrusion detection tools can identify a would-be intruder so that his or her other activities may be monitored. New vulnerabilities may, of course, be discovered in the future.

IDSs have gained acceptance as a necessary addition to every organization's security infrastructure. Since they are first put on the security market, those organizations have several compelling reasons to acquire and use IDSs. Some of them are listed below [12].

A. Important reasons for the use of IDSs

- To prevent problematic behaviors by increasing the perceived risk of discovery and punishment for those who would attack or otherwise abuse the system,
- To detect attacks and other security violations that are not prevented by other security measures,
- To detect and deal with the preambles to attacks (commonly experienced as network probes and other reconnaissance activities),
- To document the existing threat to an organization,
- To act as quality control tool for security design and administration, especially for large and complex enterprises,
- To provide useful information about intrusions that take place, allowing detailed analysis, recovery, and correction of causative factors.
- Intrusion detection systems have the same critical job. It is critical that the system's detection mechanisms are accurate enough to differentiate between the good and bad traffic allowed by the firewall. The following are all possible results of intrusion detection:
- Undetected bad traffic (false negative)
- Detected bad traffic (true negative)
- Good traffic that the system thinks is bad (false positive – false alarm)
- Good traffic that the system identifies as good (true positive)

Undetected bad traffic: Failure to identify malicious traffic as an attack. This is the worst thing that can happen, because it means the IDS failed to do its job. Failing to detect an attack can occur when an IDS does not have adequate or comprehensive intrusion detection mechanisms in place. It also occurs when new attacks are created and then missed by poorly implemented detection mechanisms [15]. While it is virtually impossible to detect every attack, the goal of any system should be to minimize the number of undetected attacks.

Detected bad traffic: Identifying "real attacks" as an attack. This is the ideal result of an IDS. The ability to detect bad traffic with speed and reliability is referred to as intrusion detection accuracy. All other functions of the system hinge on this capability [15]. The more accurate the system, the more you can trust its abilities. A system must have proven accuracy before enabling it to take the necessary actions (such as dropping the connection) to secure the network.

Identifying good traffic as an attack: False alarm or false positive. This is the most troublesome and time-consuming aspect of IDS solutions. It occurs when the

IDS sees something in legitimate and benign traffic that makes it believe there is an attack [15]. It is detrimental because each and every alarm needs to be investigated in order to determine whether an attack was successful and assess any resulting damage. Every moment spent investigating a false positive reduces the time available to investigate real threats. The result is that false positives can erode trust in the product; sometimes causing real attack alarms to be overlooked (the "crying wolf" effect). Most IDSs can be tuned to try to reduce the occurrence of false positives, however, the tuning process is often long and involved, sometimes taking weeks to accomplish [15]. In addition, because of the management design of current IDSs, tuning is often an all or nothing approach. This means that security managers must choose whether or not to look for a certain attack. If, in the interest of reducing false positives, the detection of certain attacks is turned completely "off," those attacks will be able to go by the IDS completely undetected.

Nevertheless, false positives are not the result of poor software design by IDS vendors. As Stefan Axelsson demonstrated in his 1999 ACM presentation, [16] there are some fundamental mathematical constraints that make false positives endemic to the whole paradigm of real-time signature (pattern) recognition. Deviations from baseline norms can be caused by a variety of factors, many of them innocuous. So, false positives are inherently part of signature-based intrusion detection schemes or any other type of anomaly detection system.

Identifying good traffic as good traffic: An ideal result of intrusion detection mechanisms, identifying good traffic for what it is good traffic [15]. Users should be aware that most of the existing IDSs are not difficult to by-pass if the attacker is knowledgeable. In addition, users should be aware that IDSs generate voluminous logs that must be examined carefully if the IDS is to be effective [4].

B. The advantages and disadvantages of IDSs are summarized below :

Advantages

- The deployment of network-based IDSs has little performance impact upon an existing network,
- Host-based IDSs are able to monitor events local to a host,
- IDSs can allow security managers, regardless of their level of security expertise, to track security problems on their systems, initiating incident handling procedures [14].

Disadvantages

- IDSs have a tendency to generate "false positives". That is, they frequently generate alerts about an attack when none is taking place,
- The only way to eliminate false positives would be to tune the system down to the point where it would also ignore real attacks – yielding "false negatives" – an obviously unacceptable approach,
- IDSs are extremely administration-intensive. Highly skilled security professionals must constantly tune the system, update signatures, analyze alerts to determine if they are real or false, and then respond with appropriate remedial action,
- An IDS must be closely monitored and continually fine-tuned to the usage patterns and vulnerabilities discovered in its deployed environment. Such maintenance typically consumes a fair amount of administrative resources and effort,
- A substantial amount of time may pass between the attack and the remediation, allowing the attacker to do irreversible damage in the meantime,
- Any IDS system that relies exclusively on documented attack profiles will be vulnerable to new, as-yet-undocumented attacks.

C. Types of intrusion detection system

There exist various IDS products in the market today. These products are categorized in several ways according to their different characteristics [17] are Detection method, Behavior Based (Misuse detection), Knowledge Based (Anomaly detection), Audit source location, Host log files (Host based), Network Packets (Network based), Behavior on detection, Passive and Active.

*Detection Method***:** The detection method describes the characteristics of the analyzer [17]. When the intrusion-detection system uses information about the normal behavior of the system it monitors, we qualify it as misuse detection. When the intrusion-detection system uses information about the attacks, we qualify it as anomaly detection.

Misuse Detection IDS: Knowledge-based intrusion-detection techniques apply the knowledge accumulated about specific attacks and system vulnerabilities. The intrusion-detection system contains information about these vulnerabilities and looks for attempts to exploit them. When such an attempt is detected, an alarm is triggered. In other words, any action that is not explicitly recognized as an attack is considered acceptable. Essentially, the IDS looks for a specific attack that has already been documented. Like a virus detection system, misuse detection software is only as good as the database of attack signatures that it uses to compare packets against. Therefore, the accuracy of misuse intrusion detection systems is considered good. However, their completeness requires that their knowledge of attacks be updated regularly.

Misuse detection provides various benefits. One of the first benefits is that the signature definitions are modeled on known intrusive activity. Furthermore, the user can examine the signature database, and quickly determine which intrusive activity the misuse detection system is programmed to alert on. Another benefit is that the misuse detection system begins protecting your network immediately upon installation. One final benefit is that the system is easy to understand. When an alarm fires, the user can relate this directly to a specific type of activity occurring on the network.

Along with the numerous benefits, misuse detection systems also have their share of drawbacks. One of the biggest problems is maintaining state information for signatures in which the intrusive activity encompasses multiple discrete events (that is, the complete attack signature occurs in multiple packets on the network) [18]. Another drawback is that your misuse detection system

must have a signature defined for all of the possible attacks that an attacker may launch against your network. This leads to the necessity for frequent signature updates to keep the signature database of your misuse detection system up-to-date. One final problem with misuse detection systems is that someone may set up the misuse detection system in their lab and intentionally try to find ways to launch attacks that bypass detection by the misuse detection system.

Anomaly Detection IDS: Anomaly detection techniques assume that an intrusion can be detected by observing a deviation from normal or expected behavior of the system or the users [17]. The model of normal or valid behavior is extracted from reference information collected by various means. The security manager defines the baseline, or normal, state of the network's traffic load, breakdown, protocol, and typical packet size. The intrusion-detection system later compares this model with the current activity. If a deviation is observed, an alarm is generated. In other words, anything that does not correspond to a previously learned behavior is considered intrusive. Therefore, the intrusion-detection system might be complete, but its accuracy is a difficult issue. The anomaly detection technique is as good as its normal model definition.

Anomaly detection systems offer several benefits. First, they can detect insider attacks or account theft very easily. If a real user or someone using a stolen account starts performing actions that are outside the normal user profile, it generates an alarm. Second, because the system is based on customized profiles, it is very difficult for an attacker to know with certainty what activity he can do without setting off an alarm. Probably the largest benefit, however, is that intrusive activity is not based on specific traffic that represents known intrusive activity (as in a misuse IDS). An anomaly detection system can potentially detect an attack the first time it is used [17]. The intrusive activity generates an alarm because it deviates from normal activity, not because someone configured the system to look for a specific stream of traffic. Like every IDS, anomaly detection systems also suffer from several drawbacks. The first obvious drawback is that the system must be trained to create the appropriate user profiles. During the training period to define what normal traffic looks like on your network, the network is not protected from attack. Just defining "normal" is a challenge in itself [17]. Maintenance of the profiles can also become time-consuming. Nevertheless, the biggest drawback to anomaly detection is probably the complexity of the system and the difficulty of associating an alarm with the specific event that triggered the alarm. Furthermore, you have no guarantee that a specific attack will even generate an alarm. If the intrusive activity is too close to normal user activity, then the attack will go unnoticed. It is also difficult to know which attacks will set off alarms unless actually test the attacks against the network using various user profiles [18].

Author described that 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. Based on constructing firewall with Iptables in the environment of Linux OS, the respective characters of firewall and IDS are analyzed. Then, the viewpoint of integrating firewall and IDS to realize the network security is proposed and the application and algorithm of intrusion detection are systematically analyzed and designed [19]. Authors provide the first formal definition and theoretical analysis and safety in firewall policy development [20]. They show that naïve development approaches can easily create a temporary security hole by permitting illegal traffic or interrupt service by rejecting legal traffic deployment. They defined safe and most-efficient deployments, and introduce the shuffling theorem as a formal basis for constructing deployment algorithms and providing their safety. They also presented efficient algorithms for constructing most-efficient deployments in popular policy editing languages; a safe deployment is not always possible. Scientists presented a series of three efficient algorithms for discovering all functional discrepancies between two given firewall policies: a construction algorithm, a shaping algorithm, and a comparison algorithm. [21] The algorithms can be used to perform firewall policy change impact analysis as well. Firewall policies often need to be changed, as networks evolve, and new threats emerge. Many firewall policy errors are caused by the unintended side effects of policy changes. Their algorithms can be used directly to compute the impact of firewall policy changes by computing the functional discrepancies between the policy before changes and the policy after changes. Researchers described that in open source Linux, users can simply use the basic grammatical rules to complete add, delete, insert the rules. And after all the rules are generated script can be retained [22]. Netfilter or IPtables structure can be a little mouse suitable for the establishment of their own packet filtering firewall, in order to achieve their own aims and needs. Author presented the background of introducing of the personal firewall, the development of domestic and foreign personal firewall, the security problem of network and the technology of computer firewall [23]. Then, analyzed thoroughly the technology of the capturing of network data under the operation system of Windows and introduces overall frame about the operation system of Windows as well as structural drawing about the network system of Windows. The paper further explains the design of the project and the implementation of all modules in detail, illuminates the testing and analysis of performance of program. For the development, they adopted the software designing methodology of structurization and modularization which improves the transplantation and agility of the system. Scientists designed an intrusion prevention system (IPS) based on Snort and Netfilter [24]. The policy control module of the system was written in Multi-thread technologies. They optimized the algorithm of IDS and rule set of firewall to improve system

efficiency. The system can modify the attack source by dynamically modifying the firewall rules according to IDS. They have reconfigured the firewall using the result of IDS which enhances the level of security in a network. Researchers represent an innovative policy anomaly management framework for firewalls, adopting a rule-based segmentation technique to identify policy anomalies and derive effective anomaly resolutions [25]. They proposed a grid-based representation technique, providing an intuitive cognitive sense about policy anomaly. They also discussed a proof-of-concept implementation of a visualization-based firewall policy analysis tool called Firewall Anomaly Management Environment (FAME). They have also demonstrated how efficiently anomalies in firewall policies can be discovered and resolved through their proposed method. Authors proposed a new design of firewall which consists of two parts: (1) Single Domain Decision Firewall (SDD) – a new firewall rule management policy that is certainly not conflicts, and (2) the Binary Tree Firewall (BTF) – a data structure and an algorithm to fast check the firewall rules [26]. The performance of firewall depends on its rule management. The performance may be increased by reducing the firewall anomalies. The result of their study has shown that the new design can fix conflicting anomaly and increase the speed of firewall rule checking.

V. Conclusion

The network security in today's world is a major concern because of increasing threats from malicious users. Therefore, designing a correct network security policy is a challenging task. To design filtering rules to formulate a sound firewall security policy and implement intrusion detection system to capture network packets and detect attacks to fulfill this gap.

Acknowledgment

I am grateful to School of Electrical Engineering and Information Technology, College of Agricultural Engineering and Technology, Punjab Agricultural University, Ludhiana to provide the facilities and financial assistance for writing this article. I am also very thankful to my advisor Dr. O.P Gupta, Associate Professor who encouraged to write this article by providing the valuable suggestions.

References

[1] D. Brent Chapman and Elizabeth D. Zwicky. *Building Internet Firewalls*, (O'RIELLY), ISBN 1 56592 -124-0, First Edition, November 1995.

[2] J. P. Wack and L. J. Carnahan. "*Keeping Your Site Comfortably Secure: An Introduction to Internet Firewalls*", NIST Special Publication 800-100 U.S. Department of Commerce, 1995.

[3] WEB_1 2005. Check Point Software Technologies Ltd. "Stateful Firewall Technology Products and Solutions", 08/11/2005. (http://www.checkpoint.com/products/technology)

[4] NIST (National Institute of Standards and Technology). "Guidelines on Firewalls and Firewall Policy". January 2002.

[5] W. A. Shay. "Firewall", University of Wisconsin-Green Bay. 2000

[6] NA (Network Associates). "Intrusion Prevention: Myths, Challenges, and Requirements", April 2003. (http://www.networkassociates.com/)

[7] CNAPC (Cisco Certified Network Associate Curriculum). http://std.cnap.ege.edu.tr

[8] WEB_3 2005. "TCP/IP Protocol Suite", 05/04/2005. http://burks.bton.ac.uk/burks/pcinfo/hardware/ethernet/tcpip.htm

[9] W. Stalling. *Network Security Essentials Applications and Standards*, (Prentice Hall), 2002, pp. 345.

[10] Anita K. Jones and Robert S. Sielken. "Computer System Intrusion Detection: A Survey", Department of Computer Science University of Virginia, 2000.

[11] D. G. Gómez. "Sistemas de Detección de Intrusiones: Capítulo 4". July 2003.http://www.dggomez.arrakis.es/secinf/ids/html/cap01.htm

[12] R. Bace. "Intrusion Detection". Macmillan Technical Publishing, 2000.

[13] WEB_7 2002. "Intrusion Detection System". 29.10.2002. (http://www.webopedia.com/tem/I/intrusion_detection_system.html) http://www.infosecurity.org.cn/content/ids/intru_detec_ter_2.htm

[14] R. Bace and P. Mell. "Intrusion Detection Systems". NIST Special Publication, 2001.

[15] OneSecure. "Intrusion Detection and Prevention Protecting Your Network From Attacks Allowed By The Firewall", 2001.

[16] S. Axelsson. "The Base-Rate Fallacy and its Implications for the Difficulty of Intrusion Detection". In Proceedings of the 6th ACM Conference on Computer and Communications Security. pp. 1-7. November 2-4, 1999.

[17] H. Debar, M. Dacier and A. Wespi. "Towards a taxonomy of intrusion-detection systems", *Computer Networks*. 31 1999, pp. 805–822.

[18] E. Carter, "Intrusion Detection Systems", 15.02.2002, http://www.informit.com/.

[19] Z. Jia, S. Liu and G. Wang. Research and Design of NIDS Based on Linux Firewall, *2006 1st International Symposium on Pervasives Computing and Applications, IEEE,* 2006

[20] C. Z. Zhang, M. Winslett and C. A. Gunter. On the Safety and Efficiency of Firewall Policy Deployment, *2007 IEEE Symposium on Security and Privacy (SP'07)*.

[21] A. X. Liu and M. G. Gouda. Diverse Firewall Design, *IEEE Transactions on Parallel and Distributed Systems*, **19**, No. 9, September 2008.

[22] F. Ying-lan, H. Bing and L. Ye-bai. The Design and Realization of the packet Filter Firewall based on Linux, *International Conference on Industrial and Information Systems, IEEE*, 2009.

[23] Z. Yu. The Program Design of Network Firewall Based on Windows, *International Conference on Machine Vision and Human-machine Interface*, *IEEE*, 2010.

[24] Jianrong. A Design and Implement of IPS based on Snort, *Seventh International Conference on Computational Intelligence and Security, IEEE,* 2011.

[25] H. Hu, G. Ahn and K. Kulkarni. Detecting and Resolving Firewall Policy Anomalies, *IEEE Transactions on Dependable and Secure Computing*, **9**, No. 3, May/June 2012.

[26] S. Khummanee, A. Khumseela and S. Puangpronpitag. Towards a New Design of Firewall: Anomaly Elimination and Fast Verifying of Firewall Rules, *10th International Joint Conference on Computer Science and Software Engg. (JCSSE),* 2013.

Author's Profile

Hemdeep Kaur Bimbraw

is pursuing M. Tech in Computer Science from School of Electrical Engineering and Information Technology, College of Agricultural Engineering and Technology at Punjab Agricultural University, Ludhiana for the session of 2012-13and 2013-14. The degree includes course and research work whereby she has scored OGPA 8.0. Currently she is involved in research work and this paper is an attempt to present her line of work.

Dr. O. P. Gupta

is Associate Professor Cum Head, School of Electrical Engineering and Information Technology, College of Agricultural Engineering and Technology at Punjab Agricultural University, Ludhiana. Under his valuable guidance, Hemdeep Kaur Bimbraw has been able to successfully conduct her study.