*International Journal of*
*Emerging Research in Management &Technology*
*ISSN: 2278-9359 (Volume-3, Issue-10)*

**Research Article** | **October 2014**

# Network Security: A Literature Review

**Amandeep Kumar**
Assistant Professor, CSE
SLIET, Longowal, India

**Harmandeep Singh**
Assistant Professor, CSE
SLIET, Longowal, India

***Abstract-***

***Paper discusses about basics of network security . The paper starts with the introduction to network security problem and then it analyzes the computer network security features and the main threats to the network security. After that solutions to the network security problem are discussed. In actual there are very large number of solutions exists but we have discussed mainly three solutions namely firewall technologies, the intrusion detection and prevention technology. And in the end of this paper I have discussed the integration technique which can be used to integrate different techniques to improve the real-time check, accuracy and recovery ability of the network security system.***

***Keywords- Security, Threats, Firewalls, Integrity, Confidentiality, Authorized***

## I. INTRODUCTION

The fast development of the modern Internet technology and information technology cause the individual, enterprise, school and government department joining the Internet, Which cause more illegal users to attack and destroy the network by using the fake websites, fake mail, Trojan horse and backdoor virus at the same time. The target of the attacks and intrusion on the network are computers, so once the intruders succeed, it will cause thousands of network computers in a paralyzed state. By this way, the intruders steal massive information to seek user's benefits. In addition, some invaders with ulterior motives look upon the military and government department as the target which cause enormous threats for the social and national security [1][2].

Besides the problems of the network, the defense measures we usually take also have their own shortcoming; security event is facing other challenge, for example:

- From security event was discovered to be controlled, the basic approach is taken manually and is difficult to control in time.
- The unknown security event and the network virus are unable to guard against.
- The mis-operation and network data destruction which caused by internal personnel, the spread of network virus, the Trojan horse.
- The safety equipments work dispersedly which are unable to coordinate the management. They only can form the simple point defense.

## II. COMPUTER NETWORK SECURITY

### *A. Network Security*

As we have already discussed that the fast development of the modern Internet technology and information technology cause the individual, enterprise, school and government department joining the Internet, Which cause more illegal users to attack and destroy the network by using the fake websites, fake mail, Trojan horse and backdoor virus at the same time. So we need some type of security to protect our networks from such malicious users.

Network security mainly consists of the technologies and the processes that are deployed to protect internal networks from external threats. The primary goal of network security is to provide controls along the network perimeter which allow access to the internal network and only let traffic pass if that traffic is authorized, valid, and of acceptable risk.

One thing should always be kept in mind that network security controls cannot completely eliminate the risk. The goal is to minimize risk as much as possible and to avoid unnecessary or excessive risk [2].

### *B. Characteristics of Network Security*

Network security has the following four basic characteristics:

1. **Data Integrity:** it means the data can not be changed without the authorization that is, only people who can be allowed can modify data, and can determine whether data has been modified.
2. **The confidentiality of the data:** this states that data can not be leaked to unauthorized users for their use. Data encryption is used to achieve this goal. By encrypting the data in transmission and use it can be protected from illegal access by third parties.
3. **Data availability:** it states that data is not available to all the users at all the time. It means that only authorized users can access and use the data and data is made available only on demand.
4. **Data controllable:** that can control the flow of information and the behavior patterns within the mandate, such as access to data, communication and content with the control. System must be able to control who can access the

system or network data, and how to access at the same time, be able to authenticate users on the network, and record the network activity of all users.

### *C. Main Threats to Network Security*

From a technical point of view, the network insecurity, on the one hand because of all the resources through a network share, on the other hand its technology is open. In general, network security threats are the following [2]:

1. **Inadvertent human error:** improper use of operators, security configuration vulnerabilities, user with poor security awareness, choosing inadvertently a password will pose a threat to network security.
2. **Man-made malicious attacks:** such attacks are divided into two kinds: one is the active attacks, its purpose is to tamper with the information contained in the system, or to change the system's state and operation in variety of ways and to destroy it validity, integrity and authenticity; the other is a passive attack, it does not affect the normal work of the network, intercept and theft information, strong threat confidentiality of the system.
3. **"Back door" of networking software and loopholes:** all network software can not be 100% free from vulnerabilities which are a prime target for hacker attacks. Thus due to their own vulnerability the corresponding system and application software are targeted by the hackers.
4. **Non-authorized access:** the use of network or computer resources without their consent is seen as a non-authorized access. Mainly in the following forms: the illegal users by impersonating the identity access the network for illegal operation; authorized users in lawful manner operate and so on.

## III. SOLUTION OF NETWORK SECURITY PROBLEM

### *A. Firewalls*

Firewalls may be defined as the network devices used to restrict traffic passing between networks. A fire wall can consist of hardware and software, or even several components working together. Firewalls are mainly used to implement security policies which govern the flow of traffic between two or more networks.

As a traditional security technology, the main function of firewall is to strengthen the visit restrictions between the networks and prevent the exterior network user from entering into the internal network by illegal method. If an intruder want access to the target computer; first of all, it must pass through firewall. By setting the visit rules to filtrate the visits which are not safely, it may enhance the network security enormously and reduce the risk of host.

Limitations of Firewalls are:

1. Firewall cannot prevent attacks coming from Intranet.
2. The access control policy of firewall is static, and can not adapt itself to the change of the attack from outside.
3. Filtering rules of firewall are usually very simple, so firewall cannot prevent attacks coming from application layer, and cannot prevent viruses also.

### *B. Types of firewalls*

There are mainly five types of firewalls and are given below:

1. Simple packet filter
2. State full inspection filter
3. Application proxy
4. Hybrid firewalls
5. Personal firewalls

Now we will explain all these type of firewalls one by one.

#### *i. Simple packet filter):*

Simple packet filters selectively controls the flow of packets in/out of a network or between networks. Control is based and enforced through a series of rules. These rules are based on information stored in the IP and TCP/UDP/ICMP headers.

Rule criteria can be based on the following characteristics of the IP packet:

- Source and/or destination addresses
- Protocol including TCP, UDP, ICMP, or all IP
- TCP or UDP source and/or destination ports
- ICMP message type
- TCP flags, especially ACK (to distinguish a new connection from a reply to an established connection )

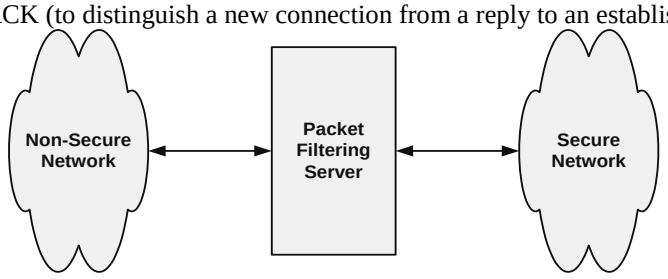


Figure-1 Simple packet filter firewall

 

***ii. Stateful inspection filter)*:**

When a packet arrives on the outside interface, it could be one of the two things:

- A packet intended to start a new connection originating from the outside. This is risky because the packet may be inappropriate or malicious.
- A packet that is replying to the request initiated from inside. This is less likely to present a risk and more likely to be legitimate.

Both a brand new packet and a reply packet both appear similar because both have source IPs from the outside, destination IPs for inside, and appear to external interface. The only difference is in the TCP flag bit, that is:

- New traffic has SYN while return traffic for exiting connections has ACK.
- TCP flags can be crafted or manipulated so these are not good ways to track state.
- UDP, ICMP and other protocols do not have the flags.

Thus stateful inspection should be used whenever there is a need to differentiate between an incoming return/reply packet for an outgoing connection and an incoming packet for an incoming connection. This type of firewalls extracts state related information from the application layer, such as the FTP PORT, command that defines the data channel port and open that port for the life of the connection.

The stateful inspection filters maintain tables to track the state of each packet. The state tables stores source address, destination address, source port, destination port, and connection expiration time limit. Any packets that match a connection in the table is considered part of the same connection. Packets that did not match an existing connection in the table are considered new and are added to the table (assuming that the connection passes the filtering rules which have been defined).

***iii. Application Proxy):***

Application proxy firewalls are those firewalls that understand and are able to interpret information in the data part of the network packets, including commands at the application protocol level. Application proxy firewalls break the client server model. Each connection between client and server actually requires two connections: one between client and firewall and another between firewall and server.

Application-level proxy processes run on the firewall to interpret the application data contained in the network packets. Proxies can analyze application-level commands and filter out security vulnerabilities, such as HTTP content type, detection of viruses in mail messages, etc. proxies rewrite packets before sending them along to internal nodes.

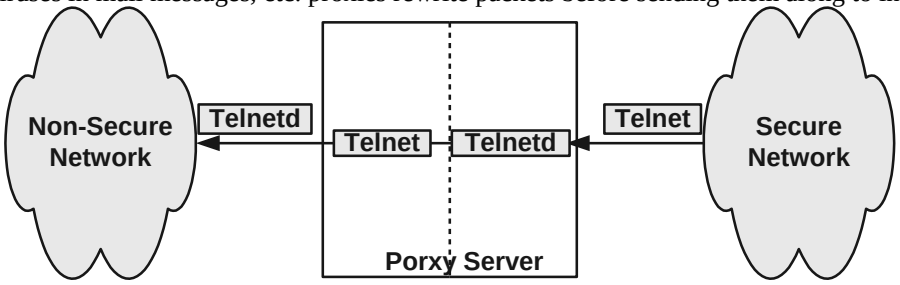


Figure-2 Application Proxy firewall

**Advantages of proxy firewalls**

- Such type of firewalls enable filtering based on the entire network packet. Application layer vulnerabilities can be detected (e.g.. CGIs or HTTP parms, viruses etc. )
- Provide authentication capability (IDs/passwords, certificates, etc. that are passed in the data part of the packet)
- Provide more detailed logging by including application layer information (e.g., not just IP address of the web server, but URLs as well)
- Prevent direct connection to the inside, the connection is broken at the firewall.
- Reconstruct the network packets, prevents malformed packet attacks.

**Disadvantages of proxy firewalls**

- Poor performance – application proxies are slow because all packets have to be processed up the full TCP/IP stack.
- Only a limited number of common services have proxy agents available.

***iv. Hybrid Firewall)s:***

Most firewalls are hybrid and contain features of several different types of firewalls. Few combinations are given below:

- Some simple packet filters contain limited state functions, and even more. For example, Cisco routers can perform limited state tracking for TCP using reflexive ACLs. In addition, an optional firewall feature set is available.
- Stateful inspection firewall also provides some limited proxy support for authentication and basic filtering. For example, Firewall-1 contains security servers for HTTP, SMTP, and FTP.

 

- Proxy firewalls have packet filtering capabilities for protocols that are not proxiable. For example, Symantec Raptor firewall offers simple filtering rules on tuples.

***v. Personal Firewall)s:***

- Workers may be connected to corporate networks from their home PCs by:
  - High-bandwidth mechanism – DSL, cable modems
  - VPNs for remote connections.

- What happen if home PCs are compromised and used as launching point for attacks on the corporate networks?
- This is why companies have to consider about the personal firewalls as a part of their total security solutions.
- Personal firewalls can software products that protect a particular desktop machine, or they can hardware applications that protect a home network.
- They perform a variety of functions:
- Packet filtering based on port and source address
- Logging and alerting of attacks
- They sometimes allow for remote management. This feature enables a company to centrally manage and administer rule sets.

***B. Intrusion Detection Technology***

***i. What is an intrusion?***

An intrusion is a security event in which someone attempts access to systems or information that they would not normally be allowed to see. This behavior can be quite similar, whether this person is entering (or trying to enter) from outside a network, or a legitimate local user misusing access privileges. Similarly, Denial of Service attacks, which render a system or service unavailable, are another common type of attack commonly called an "intrusion."

***ii. Intrusion Detection System:***

It refers to the intrusion detection and real-time monitoring of the reporting system, mainly by the sensor, analyzer, manager, and user interface component. It gather information from a different source systems and networks (including the internal network information and network information from the outside), and then according to known attack patterns of the information analyzed to check whether there are signs of invasion. It can completely track the user's activities, identifying users who violate security policy activities; to provide expert system, automatic configuration of the system consistency check and diagnosis, monitoring and analysis of data packets to identify the same pattern with the known activities of the invasion. According to the object monitoring system, intrusion detection systems can be divided into network-based intrusion detection and host-based intrusion detection [3][5].

**Host-Based**: which monitors the characteristics of a single host and the events occurring within that host, for suspicious activity.

**Network-Based**: which monitors network traffic for particular network segments or devices and analyzes the network and application of protocol activity to identify suspicious activity.

**Hybrid**: In this type both kinds of IDS can be used simultaneously.

**Network Behavior Analysis (NBA)**: which 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 (e.g., a client system providing network services for other systems)

An IDS uses one or both of the following techniques to detect intrusions:

- **Signature detection**—the IDS scan packets or audit logs to look for specific signatures (sequences of commands or events) that were previously determined to indicate a given attack's presence.
- **Anomaly detection**—the IDS use its knowledge of behavior patterns that might indicate malicious activity and analyzes past activities to determine whether observed behaviors are normal.

***iii. ID System Components***

The functionality of an IDS can be logically distributed into three components: sensors, analyzers, and a user interface.

**• Sensors**

Sensors are responsible for collecting data. The input for a sensor may be any part of a system that could contain evidence of an intrusion. Example types of input to a sensor are network packets, log files, and system call traces. Sensors collect and forward this information to the analyzer.

**• Analyzers**

Analyzers receive input from one or more sensors or from other analyzers. The analyzer is responsible for determining if an intrusion has occurred. The output of this component is an indication that an intrusion has occurred. The output may include evidence supporting the conclusion that an intrusion occurred. The analyzer may provide guidance about what actions to take as a result of the intrusion.

**• User interface**

The user interface to an IDS enables a user to view output from the system or control the behavior of the system. In some systems, the user interface may equate to a "manager," "director," or "console" component.

 

***iv. Architecture***

The example of typical architecture is shown in figure. The *sensors/agents* components monitor and analyze activities. A *management server* is a centralized device that receives information from the sensors or agents and manages them. A *database server* is a repository for event information recorded by sensors, agents, and/or management servers. A *console* is a program that provides an interface for the IDS's users and administrators .

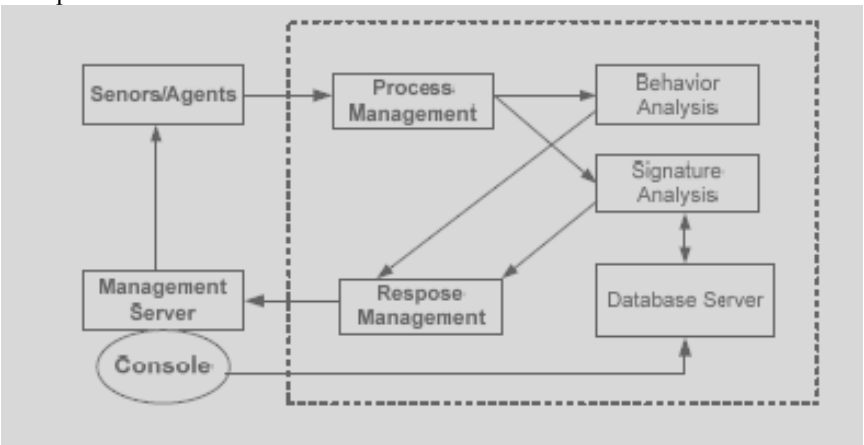


Figure-3 Architecture of IDS

***v. Intrusion prevention technology:***

IPS is known as a new technology which is developed after the intrusion detection technology; it inherits all the advantages of intrusion detection intrusion prevention adds a module which is able to response the intrusion on its own initiative. It makes use of marks left by the intruders to effectively discover the illegal intrusion from external or internal. Once discovered the aggressive behavior, it will cut off the connections actively. It is an extremely important part in network security.

***vi. Characteristics of IPS***

IPS is a system in which firewall is tightly coupled with IDS, and it can react to the changes of the network environment, IPS can find out intrusion action and prevent them, it is one of the promising technologies of the network security.

IPS is not roughly combining IDS with isolation of firewall. In order to improve on network security, IPS should satisfy the following conditions:

- IPS should run on a reliable and stable platform and should be one part of the communication link.
- IPS based network should be supported by special hardware
- More exact and intelligent are to be employed to enhance the detection ability.
- IPS should become one part of the network applications, detect attack in real time, isolate intrusion in real time, and protect network actively.

On the basis of objects IPS protects and methods it uses, IPS is divided into three classes:

- IPS based host (HIPS)
- IPS based network (NIPS)
- Distributed IPS (DIPS)

Compared with IDS, NIPS has two new features: In-line and traffic isolation. It means IPS is placed in sole path which all traffic of the network detected must pass through, unlike IDS detecting traffic bypassed as shown below in the figure. IPS has suspicious traffic, which is impossible for IDS.

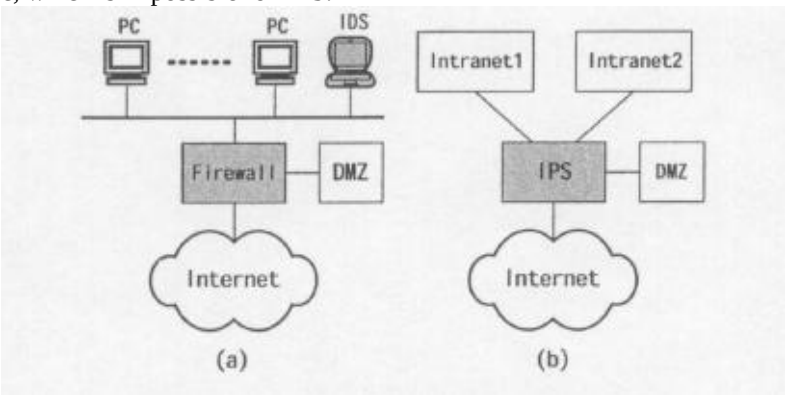


Figure-4 (a) Firewall and IDS (b) NIPS

iv Recent Development in Network Security by using Integration of Network Security Technology

 

***A. Comparison of network security technology***

The comparison of the different network security techniques is given in the following table with explanation:

***i. The source of defensible intrusion***

Firewall can only deal with the attacks which come from the external network. As the definition of firewall, it is a method which separates the internal and external work. The data which the firewall rules allow will be able to enter the internal network, at the same time the data which not allowed will be isolated in the exterior. Intrusion detection technology can not only guard against the external network attack, but also providing a real-time monitoring with internal attacks and mis-operation by collecting the security logs, audit data and computer system information.

Intrusion prevention technology can also guard against the external network attack and provide a real-time monitoring with internal attacks and mis-operation.

TableI. Comparison of key technologies [1].

| performance | technologies | | |
|---|---|---|---|
| | *firewall* | *intrusion detection* | *intrusion prevention* |
| The source of defensible intrusion | external network | external and internal network | External and internal network |
| Real-time | lower | low | high |
| Accuracy | lower | low | high |
| sphere of action | link layer, network layer, transport layer | link layer, network layer, transport layer | link layer, network layer, transport layer, application Layer |

***ii. Real-time***

As an important tool to prevent from the internal attacks, firewall rules are set well in advance, and only provide a coarse-grained check in real-time filtering, for unknown security case it can do nothing. Therefore, its real-time is low. Intrusion detection technology is a supplement of firewall, which makes up the insufficiency of firewall. The intrusion detection technology sends out the warning and informs the administrator to take action when it discovered the attacks, so there is a time gap difference between discovering the attack and taking measures. Therefore, its real-time is relatively poor. Intrusion prevention technology adds the active defense function to the intrusion detection technology. Not only can it detect known and unknown security event, but also controlling and defending actively. Therefore, it has the strong real-time.

***iii. Accuracy***

All the behaviors want to visit the network have to pass through the firewall, therefore, the setting rules of the visit rules is extremely important. The common firewall rules are a kind of coarse-grained detection, which could intercept completely the known attack and reduce the rate of false alarm, but easily "allowed to pass" actually the unknown attack. Thus it causes the rate of missing report high. Intrusion detection technology provides a fine-grained detection. It sends out alarm frequently which makes the administrator to spend more time on analyzing data, but most of them are mis-information, therefore most of manpower is wasted and the rate of missing report does not so high correspondingly. The high rate of missing report and false report is still a serious problem of intrusion detection technology.

There are two types of detection methods for intrusion prevention technology, one is anomaly detection, and the other one is pattern match. The first method detects the uniformity with the behavior of the current user and the normal behavior which has established to judge whether the behavior is an illegal intrusion. This will cause a high rate of false alarm and low rate of missing report. The latter extracts a model of intrusion. Once the behavior matches the model, it will be blocked. The rate of false alarm is low, but for the unknown intrusion, it could not discover promptly, the missing report rate is high. At present, the intrusion prevention technology has used more types of detection methods to judge the unknown and known attack to an extreme.

 

***B. The integration of network security technologies***

Via the analysis of the network problems and comparison of security technologies, it is not difficult to find that each kind of technologies has its own flaw. The single technology has been unable to meet the attacks and intrusion which emerge one after another. The direction of security technology development is to integrate, coordinate and centralized management.

The linkage of firewall and intrusion detection technology discover the external intrusion and internal abnormity to a great extent, however the duty of intrusion detection is to detect the threat and notify the administrator to take action, rather than intercepting intrusion on own initiatives. Therefore, the real-time of the merging is not very high.

Firewall focuses on access control; intrusion prevention technology focuses on discovering the intrusion signal, monitoring the network and controlling the intrusion timely. If integrating them, the advantage of the two technologies will play out fully, the performance of network security system will be enhanced enormously.

One integrative model of firewall and intrusion prevention technology is proposed as shown in figure-1.Firewall section intercepts the exterior intrusion completely which is not right to the rules, the behavior which across the firewall has to be detected again by the intrusion prevention system, when the illegal behavior is found, the progress starts the active response module to cut off the attacks and notify the firewall to make the dynamic modification immediately. At the same time, the intrusion prevention system placed behind the firewall can detect the network security log, audit data and system information in real time, once discovered the abnormal behavior, it informs the active response module to take action as soon as possible. So the integration can play a good safeguard role to the internal network and provide a high real time by taking action actively, thus achieving the goal of the overall security control.

In this model, the firewall places between the exterior network and internal network, intercepting the known intrusion the maximally. Intrusion prevention system acts as the second defense line behind the firewall. When firewall leaves out the intrusion, the fine-grained detection module of intrusion prevention system will cut off the intrusion in time and notify the firewall to modify the relevant rules. When the same intrusion attacks again, the firewall will be able to deal with the intrusion immediately providing a high real time, this helps to solve the problem of missing report caused by the coarse grained of firewall and false report caused by fine-grained of intrusion detection.

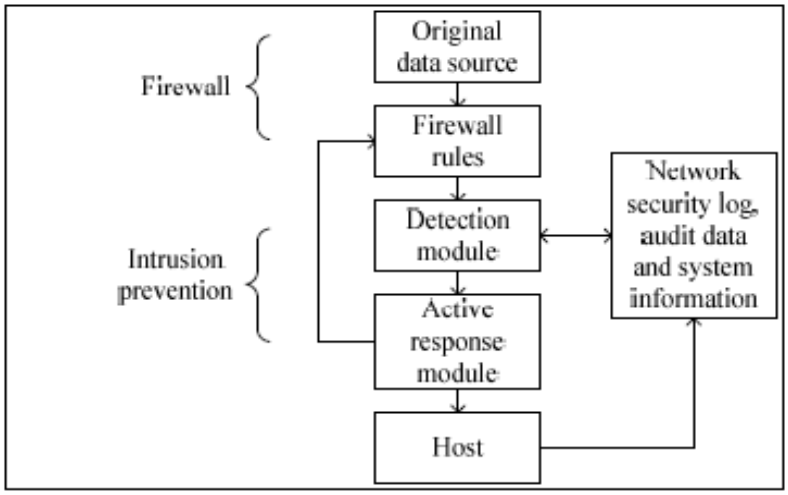


Figure-5. The integrative model of Firewall and Intrusion Prevention technology [1].

Most of all, according to host-based intrusion prevention and network-based intrusion prevention, we can build a defense system for guarding against distributed attacks. In this system, the outer makes up of border firewall and network based intrusion prevention, the inner makes up of host firewall and host-based intrusion prevention, and this forms the defense units for borders and host on their own. Each defensive unit achieves integration through the firewall technology and the intrusion prevention technology.

Based on the firewall technology and intrusion prevention technology, the defense system not only to adapt to the change of the network environment, but also provide the multi-level protection, greatly enhancing the real time and accuracy of the network security system.

## VII. CONCLUSION

Due to the increasing innovation of network attacks technologies and the changing network environment, the network attacks and intrusion is growing at very high rate, showing a character of complication and distribution. Therefore, the network security technologies also must improve the performance in many respects.

This can be done by examining the deficiencies and advantages of the existing network security techniques and the integrating the different techniques to develop perfect network security techniques.

## REFERENCES

[1] Zhijie Liu Xiaoyao Xie, *Member* , *IEEE* ,School of Mathematics and Computer Science and Zhen Wang, Key Laboratory of Information Computing Science of Guizhou Province , Guizhou Normal University Guiyang , China, The Research of Network Security Technologies.

 

[2] The Research of Firewall Technology in Computer Network Security, 2009 Second Asia-Pacific Conference on Computational Intelligence and Industrial Applications by Xin Vue, Wei Chen, Yantao Wang, College of Computer and Information Engineering Heilongjiang Institute of Science and Technology Harbin, China.

[3] The Evolution of Intrusion Detection Technology, an ISS Technical White Paper, Updated August 29, 2001.

[4] Intrusion Prevention System Design, by Xinyou Zhang, college of computer science and engineering, University of electronic science and technology of China and Chengzhong Li, Wenbin Zheng. School of computer and communication engineering, China.

[5] Intrusion Detection: A Survey, The Third International Conference on Systems and Networks Communications, F.Sabahi, IEEE Member School of Computer Engineering, Azad University, Arak, Iran, A.Movaghar, IEEE Senior Member School of Computer Engineering, Sharif University of Technology, Tehran, Iran

 