Network security and firewall

Swetha SS
Assistant Professor Dept of CSE, St. Martin's Engineering College, Secunderbad
G Pushpa Rajitha
Assistant Professor Dept of CSE, St. Martin's Engineering College, Secunderbad
Ankita Sharma
Assistant Professor Dept of CSE, St. Martin's Engineering College, Secunderbad
G Rama Krishna
Assistant Professor Dept of CSE, St. Martin's Engineering College, Secunderbad

Abstract:-Computer and network security are challenging topics. Internet security is the practice of protecting and preserving private resource and information on internet. Network security concerns with concept of design a secured network. Securing a network involves applying policies and procedures to protect different network devices from unauthorized access. with the advent of internet , security becomes major concern. Itself internet structure allowed many threats to occur.

Keywords:- firewall , network security, firewall rules, firewall rule parameter, network security mechanism .

I. Introduction

Network security is an important task that must be seriously considered at the designing of network. Network security means to the policies and procedures followed by the network administrator to protect network device against the threat and as well as to unauthorized user must be prevented from accessing the network[1]. A firewall establishes a barrier between a trusted, secure internal network and another network (e.g., the Internet) that is not assumed to be secure and trusted. For the purpose of internet security, this paper proposes the solution that handles security problems on computer network with the help of firewalls[2]. Network firewalls are devices or systems that control the flow of traffic between networks employing different security postures. The network traffic flow is controlled according to a firewall policy. The filtering decision is based on a firewall policy defined by network administrator. For each type of network traffic, there are one or more different rules. Every network packet, which arrives at firewall, must be checked against defined rules until first matching rule is found. The packet will be then allowed or banned access to the network, depending on the action specified in the matching rule.

II. Firewall

Firewalls are a great way of protecting your computer against internet viruses. One of the main advantages of a firewall is that it can be configured to provide a great deal of security; it can even protect multiple systems simultaneously. However, filtering done by a software's firewall can degrade your system's performance. Internet hubs on the other hand repeat all traffic therefore, it takes more time to get its traffic onto a particular network.

Hardware and software firewall: Firewalls can be either hardware or software but the ideal firewall configuration will consist of both.
In addition to limiting access to your computer and network, a firewall is also useful for allowing remote access to a private network through secure authentication certificates and logins. Hardware firewalls can be purchased as a stand-alone product but are also typically found in broadband routers, and should be considered an important part of your system and network set-up. Most hardware firewalls will have a minimum of four network ports to connect other

computers, but for larger networks, business networking firewall solutions are available. Software firewalls are installed on your computer (like any software) and you can customize it; allowing you some control over its function and protection features. A software firewall will protect your computer from outside attempts to control or gain access your computer.[3]

III. Network security

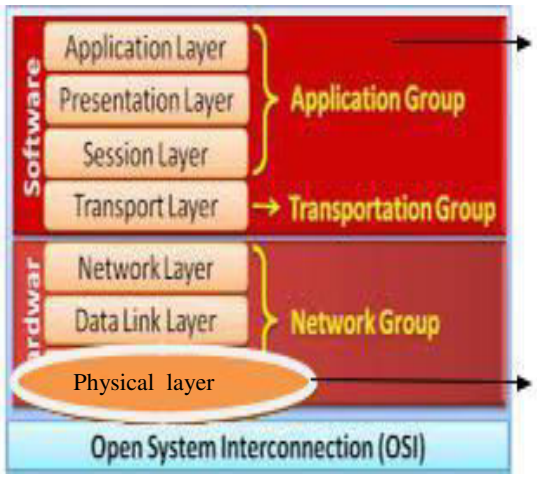
Network security is not concern about the security of computer but also securing of data on communication channel. A good hacker makes target to communication channel, steal data and decrypt it and reinsert the false message.
When developing a network, following things are considered as:

1. **Access :-**authorized user can get accessibility.
2. **Confidentiality**:-information in network remain private.
3. **Authentication:-**ensurethatuser of network are who they pretend
4. **Integrity:-**ensure that data remain unchanged.
5. **Non-repudiation:-**ensure that user does not refute.

Differentiating Data Security and Network Security:

Data security means protecting a data from destructive forces and the unwanted actions of unauthorized users.[4]

Data security



Network security

(Figure: OSI layer)[5]

Network security consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, misuse and modification.[6]

IV. Password mechanism

Password are a way by which identify user and authenticate .but unfortunately there are many way by which password can compromised.
For Example, someone wanting to gain access can listen for a username password as an authorized user gains access over a public network.
Good password procedures include the following:

- Do use a password with mixed-case alphabetic.
- Do use a password with non-alphabetic characters (digits or punctuation).
- Do use a password that is easy to remember, so you don't have to write it down
- Do not use your login name in any form
- Do not use your first, middle, or last name in any form.
- Do not use other information easily obtained about you.
- Do not use a password of all digits or all

the same letter.

- Do not use a word contained in English or foreign language dictionaries

Encryption, Authentication, and Integrity:

Firewall system is a combination of hardware and software configuration that sits between the company's network and internet, controlling into and out of the network. Encryption can be followed as:

- Coding of data through the algorithms
- A method of ensuring the data

There are many encryption techniques like as DES , RSA etc.

Encryption mechanism rely on keys or password. The longer password hard to break. There two kinds of mechanism are used for encryption purpose as:

- Private key
- Public key

Private-key encryption uses the same key to encode and decode the data. Public-key encryption uses one key to encode the data and another to decode the data. The name public key comes from a unique property of this type of encryption mechanism—namely, one of the keys can be public without compromising the privacy of the message or the other key. In fact, usually a trusted recipient, perhaps a remote office network gateway, keeps a private key to decode data as it comes from the main office. VPNs employ encryption to provide secure transmissions over public networks such as the Internet[7]-[18].

V. Firewall rules

Different firewalls usually provide different rule logic with different parameters. But some basic elements are common to all. They all allow an action to be defined allowing or banning specific network traffic. Also, all of them allow checking for most important elements in packets like IP addresses, ports and protocol. Software for firewall rule optimization (FIRO) was originally developed for ip firewalls firewall command tool. One of the most important functionalities of ip firewalls firewall is stateful inspection. Stateful inspection automatically opens only the ports necessary for internal packets to access the Internet. It only allows transfer of packets which are defined in firewall rules and which are part of established connections.

V. Firewall Rule Parameters

Each rule identifies specific type of network traffic. In order to enable this identification parameters for identification of specific network packets must be set for each rule. FIRO provides optimizing procedure which is based on these parameters:

• IP addresses – it can be destination or Source IP address; also, it can be written as a single IP, network IP or IP range,

• Ports - it can be destination or source Port; also, it can be written as a single port, port range or port array,

• Protocol – it can be referred to TCP, UDP, and ICMP or all together,

• Interface – it can be incoming or outgoing interface,

• TTL (Time To Live) field residing in the IP headers,

• Tos (Type of Service) field residing in the IP headers,

• Length of packet,

• MAC source address,

•Syn flag – identification of new connection,

• ICMP type,

• Limit – maximum number of packets in time interval.

Although FIRO allows use of all parameters, in real environment commonly used parameters are: source and destination IP addresses, destination port which defines service or application, and protocol[16].

VI. Conclusions

The Firewall which works as the gateway for the network should be configured in such a way that it should not allow unauthorized users entering the network or accessing the information. Network audit information such as log messages and network monitoring tool's record will also help in securing the network by providing information about the network access.

Network security is an important area that gaining attention as the internet expands. The security threats and internet protocol were analyzed to determine the necessary security technology. The security technology is mostly software based, but many common hardware devices are used.

References

[1] Enhancing Network Security in Linux Environment, Technical Report, IDE1202,February 2012

[2]firewall-Wikipedia, the free encyclopediaen.wikipedia.org/wiki/firewall

[3]firewall-Wikipedia, the free encyclopediaen.wikipedia.org/wiki/firewall

[4] data security-en.wikipedia.org/wiki/Data_security

[5] OSI layer image-https://www.google.co.in/url?sa=i&rct=j&q=&esrc=s&source=images&cd=&cad=rja&docid=pTKgIps8puE5zM&tbnid=3gyuiZVe70sLkM:&ved=0CAQQjB0&url=http%3A%2F%2Fopentutorial.hpage.in%2Fosi-model_96532353.html&ei=5J8HU8D9CI6FrgfX3IDACQ&bvm=bv.61725948,d.bmk&psig=AFQjCNGOqH_qfX5hZlgiWa0iObpxnobQcw&ust=1393094885303433

[6] network security-en.wikipedia.org/wiki/Network_security

[7] Treese, G. W. and Wolman, A. X through the Firewall and Other Application Relays.

[8] I. Akyildiz, et al., "AdaptNet: An Adaptive Protocol Suite for the Next-Generation Wireless Internet," IEEE Communications Magazine, March 2004, pp. 128-139.

[9] H. Balakrishnan et al., "A comparison of mechanisms for improving TCP performance over wireless links," IEEE/ACM Trans. on Networking, Vol. 5, pp. 756-776 (December 1999).

[10]M. Chiani, E. Milani, and R. Verdone, "A Semi-Analytical Approach for Performance Evaluation of TCP-IP Based Mobile Radio Links," Proc. GlobeCom 2000.

[11]Hiroshi Yoshimura et al, "Future Photonic Transport Networks Based on WDM Technologies", Vol 37, No 2, pp 74-81, February 1999.

[12]E. Lowe, "Current European WDM Deployment Trends", IEEE Communications Magazine, Feburary 1998, pp. 46-50.

[13] J. P. Ryan, R. H. Kent, "WDM: North American Deployment Trends", IEEE 153 Communications Magazine, Feburary 1998, pp. 40-44.