ISSN: 2321-7782 (Online)

Volume 2, Issue 11, November 2014

International Journal of Advance Research in Computer Science and Management Studies

Research Article / Survey Paper / Case Study

Available online at: www.ijarcsms.com

Factors for Selecting Firewall with Comparative Study

Deepika Sekhawat[1]
Department of Computer Science & Engineering
JECRC University
Jaipur, India

Vaibhav Bhatnagar[2]
Department of IT & Computer System
JECRC University
Jaipur, India

Abstract: Nowadays firewall plays a vital role to secure a computer network. There are some basic points that should be considered while implementing a firewall in a particular network. In this paper we have taken three firewalls as an example to understand which firewall satisfies the factor. This paper will be a assist for a Network Administrator for selecting a firewall.

Key Words: Application layer firewall, MAC Level filtering, network Layer firewall, proxy firewall, tarpit.

I. Introduction

Our data on different servers or computers are needed to be secure to maintain the privacy, confidentiality and data Integrity. Firewall is the best way to apply security in a particular network. A firewall is a software system or a hardware that provide security to our network system. It acts as a gatekeeper to control the incomings and outgoings of the network on the basis of applied rule sets. It maintains a barricade to our private LAN (Local Area Network) to unsecure or distrusted WAN (Wide Area Network) the internet. [1]

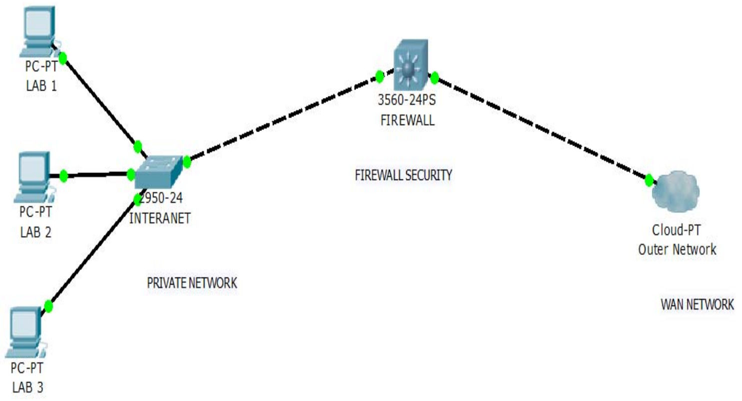

Figure 1: General View of Firewall

II. Categories of Firewall

There are mainly two broad categories of firewall

1. **Hardware Firewall**:

The hardware firewalls can be directly purchased as separate device typically found in broadband routers and can be essential part of the network setup. The hardware firewall does not require huge configuration, little configuration can be sufficient for them.

2. **Software Firewall**:

Software firewall is generally for individual PCs, laptops, basically for home users. It can be easy installed in the system just like any software. It can give protection from different viruses, Torzons and different e-worms. It can be easily configured for file and printer sharing, it can also incorporate privacy controls and other web filtering.[2]

III. Different Types of Firewalls

Depending upon the state, communication is intercepted and the place of communication the firewall can be classified as

1. Network layer Firewall:

A network layer firewall is also called packet filtering firewall that operates on low level of TCP/IP protocol. It does not allow packet who does not fit on set of rules applied by the Network Administrator. It can also be subdivided into two parts

A. **Statefull:** A statefull firewall maintains the information about current session and uses this information for speed packet processing. Any network connection has some properties like current stage of session or connection, source and destination address, TCP or UDP port number etc. A statefull firewall matches the property of new packet if it does not match evaluate it from the ruleset connection, and if matches it passes without further processing.

B. **Stateless:** A stateless firewall is faster for simple filter and requires less time for look up new session and it also require less memory.

2. Application layer Firewall:

As the name indicates, it works on the application layer of TCP/IP protocol suit. It blocks the packet usually without acknowledged by the sender. It blocks the packet on the basis of process, not on the basis of filtering connection on the ports. Processes use prompts to make the rulesets. Since there are ample of software available, it has more complex rulesets for standard services.

3. *Proxies:*

Basically it is also kind of application but it acts as an intermediate between sender and receiver. Sender and receiver conduct the session through this proxy firewall. Proxy firewall breaks the two sessions into four party sessions. To understand this mechanism we can take an example, if can user in a LAN connected with internet want to access that particular website. Any incoming packet is proceeds through that web server before forwarded through that particular user.

4. Network Address Translation:

Many firewalls have features of NAT where a host's private IP address is protected by the firewall as defined in the RFC. It hides the true IP address of the host.[3]

IV. Factor for Selecting Firewall

In this paper we have taken three firewalls, which will help us to understand which firewall should be useful for implement in a network. The firewalls are

1) Wingate: Multi-protocol proxy server, email server and the internet gateway management system for windows.[4]

2) Utangle: A network software and appliance company, provides the most complete multi-function firewall and Internet management application suite available**.**[5]

3) IPFire: Focus on security, stability and ease of use. A variety of add-ons can be installed with a single click, to add more features to the base system.[6]

The factors are:

I. **License:** It is the permission to use a particular firewall which is provided by the vendor of firewall. As far as our firewalls have concern IPFire and Utangle are GPL, that means they are General Public License, they are free which guarantee the end user for modify, share and use, but Wingate is proprietary not freely available.

II. **Cost:** If organization which we are going to implement is low in budget then IPFire is most suitable. If organization can afford Wingate is recommended by the experts. Utangle has both the versions free (Cost less) and paid.

III. **Supported Operating System:** All the firewall are made to support different operating system, suppose if we are using Linux based operating systems IPFire and Utangle will be available. Wingate is exclusively for Microsoft based operating systems.

IV. **MAC level filtering:** Generally firewall filter the packet with the help of logical address i.e. IP address, but in order to provide more security some firewall can also do filtering on the basis of physical address i.e. the MAC address (Media Access Control). IPFire & Wingate provide MAC address filtering but Utangle does not provide this facility. These two firewalls are more secure than Utangle.

V. **Tarpit:** It is also known as Teergrube. It is a facility on a firewall that intentionally delays the incoming connection or the packets. It is a defensive technique used against the computer worms. Because of low response rate it makes the sending process impractical for spammers. Only Utangle provide this facility. IPFire and Wingate unfortunately do not provide it.

VI. **Configurations:** Configuration a firewall will be easy if done with the help of Graphical User Interface. It becomes user friendly to configure it. Wingate is fully GUI based, it does not provide configuration with the command line, while Utangle and IPFire provide the both the options.

VII. **Remote Access:** Once a firewall is configured there may be a requirement to reconfigure or edit the rulesets. It can be done with the remote login servers like web (HTTPS), SSH (Secure **shell)** and can be done by proprietary user interface. SSH is more secure then HTTPS. IPFire can remotely be access with both HTTPS and SSH. Wingate can only be accessed with the help of SSH only. Utangle has dedicated proprietary user interface.

VIII. **Open Source:** A firewall is open source that means it is modified because its code is publically accessible. It is more convenient because company can modify according to the different situations. Since Wingate is the product of Microsoft it is not open source. Utangle and IPFire are Linux based so they are open source.

IX. **Domestic Use:** Some firewall can also be used for domestic or home purpose. Only Wingate does not provide this facility because it is only server based. Utangle and IPFire can be used as domestic purpose.

X. **Support of IPV6:** Implementation of IPV6 have many advantages over IPV4 like Effective routing, easy network configurations and provide more security. Unfortunately Wintage and Utangle do not support the IPV6 addressing. IPV6 is supported only by IPFire.

V. CONCLUSION

As we analyzed that these are some that these are some basic factors that should be considered while selecting a firewall of a network. A single firewall does not accomplish all the factors, and even though all factors are not altogether seen in a single network. It is fully depend upon the wisdom of Network Administrator to take decision which firewall is suitable for a particular network. However these factors can help out a Network Administrator to maintain a network secure by using these three firewalls.

References

1. www.microsoft.com/security/pc-security/**firewalls**
2. www.intego.com
3. http://searchnetworking.techtarget.com
4. www.**wingate**.com
5. www.**untangle**.com
6. www.**ipfire**.org