**IMPORTANT OF FIREWALLS IN AN ORGANIZATION**

**BY**

**USMAN ADAMU**

**ST/CS/ND/19/052**

**A SEMINAR PRESENTED TO THE DEPARTMENT OF COMPUTER SCIENCE, SCHOOL OF SCIENCE AND TECHNOLOGY, FEDERAL POLYTECHNIC MUBI, ADAMAWA STATE, NIGERIA**

**NOVEMBER, 2021**

**IMPORTANT OF FIREWALLS IN AN ORGANIZATION**

**BY**

**USMAN ADAMU**

**ST/CS/ND/19/052**

**A SEMINAR PRESENTED TO THE DEPARTMENT OF COMPUTER SCIENCE, SCHOOL OF SCIENCE AND TECHNOLOGY, FEDERAL POLYTECHNIC MUBI, ADAMAWA STATE, NIGERIA**

**IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF HIGHER NATIONAL DIPLOMA(HND)NATIONAL,DIPLOMA(ND) IN COMPUTER SCIENCE**

**NOVEMBER, 2021**

**Abstract**

*The increasing complexity of networks, and the need to make them more open due to the growing emphasis on and attractiveness of the Internet as a medium for business transactions, mean that networks are becoming more and more exposed to attacks, both from without and from within. The search is on for mechanisms and techniques for the protection of organization from such attacks. One of the protective mechanisms under serious consideration is the firewall. A firewall protects a network by guarding the points of entry to it. Firewalls are becoming more sophisticated by the day, and new features are constantly being added, so that, in spite of the criticisms made of them and developmental trends threatening them, they are still a powerful protective mechanism. This article provides an overview of firewall technologies in an organization.*

**INTRODUCTION**

Today's networks change and develop on a regular basis to adapt to new business situations, such as organisations, acquisitions, outsourcing, mergers, joint ventures, and strategic partnerships. Amos (2013) the increasing degree to which internal networks are connected to the Internet. The increased complexity and openness of the network thus caused makes the question of security more complicated and necessitates the development of sophisticated security technologies. The best way of ensuring interface security is the use of a firewall.

A Firewall is a computer, router or other communication device that filters access to the protected network. Cheswick and Bellovin (2005), define a firewall as a collection of components or a system that is placed between two networks and possesse. the following properties:

1. All traffic from inside to outside, and vice-versa, must pass through it.
2. Only authorised traffic, as defined by the local security policy, is allowed to pass through it.
3. The firewall itself is immune to penetration.

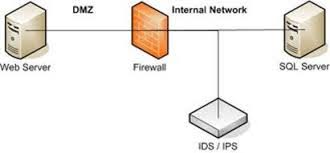


Figure: Firewall Schematics

Such traditional network firewalls prevent unauthorised access and attacks by protecting the points of entry into the network. A gateway is a machine or set of machines that provides relay services complementing the filters. Another term illustrated in the figure is "demilitarised zone or DMZ".

**FIREWALLS**

Firewalls is the first defense of network which is placed outside the network to monitor the traffic in such a way that only authorized data can flow inside the network and rest should be dropped Dowd(2007) firewalls outside as the configuration rules is given in the firewalls by administrators. Though there are some other schemes also for firewalls but we have given here basic and simple one which is mostly used by organizations. The packets filter firewalls is mainly stand on the packet allow rules e.g. So it checks only that whatever we have blocked should be dropped outside or whatever we permit should be allowed in the network. The big benefit of this firewall is it’s easy to configure and work on it as whereas the drawback is that it drop and allow the packets but not provide the log file facility so it’s tough to know the threat point. Marianne (2004)Proxy Server is like a sharing (Virtual) machine. which is having capacity to read the security instruction. what to allow and deny and accordingly it provide the service to the client The Stateful Packet filtering also causes security by passing through network layer It maintains the status for each session also but it is not a complete solution in term of firewalls.

**IMPORTANT OF FIREWALLS IN ANOGANIZATION.**

Avinashi (2011) Firewalls are the first line of defence in protecting against unauthorized access. They are important for blocking unwanted content, helping prevent malicious files such as worms, viruses and malware and creating a secure network which protects every device within that network environment.

While they cannot detect viruses and malware, they can prevent infected traffic gaining access in the first place. However, it is still important to have an up-to-date antivirus and anti-malware installed to prevent threats and malware attacks.

**Hardware Firewall**

John and Amos (2004) A Hardware Firewall is a device that typically sits between your devices and the internet that filters out network traffic. An example would be the internet router that you are running. Most modern-day routers will have a built-in firewall which filters traffic. The router would be considered a hardware Firewall, although they lack a lot of configuration options that a dedicated firewall server would.

If set up properly, your organization can disable software/application firewalls and solely rely on the hardware firewall, however it requires proper configuration and maintenance, hence it may not be feasible or practical for an organization with few devices connected to the network or one without a proper IT department.

**Software Firewall**

The software or Application Firewall is installed on individual devices and can block incoming and outgoing traffic at the application level. It differs from the hardware firewall in that it is a process running on your devices, John (2014) it takes processing power to run. It also require installation, updating and maintenance on every device running it, which also means that you will be required to buy multiple copies and install and configure them individually.

You can employ both hardware and software Firewalls, if configured properly there will be no compatibility problems between the two and will provide an extra layer of protection to your network and your devices.

**BENEFITS OF FIREWALLS IN AN ORGANIZATION**

Charles (2007), understanding the benefits of firewall security is the first step needed. It helps your organization grow safely in the ever-changing digital age. Even if your business only relies on technology and networks for a small piece of your operations, it is still equally important that you take proactive steps to keep things protected.

**1. Monitors Network Traffic**

All of the benefits of firewall security start with the ability to monitor network traffic. By monitoring and analyzing network traffic, firewalls leverage preestablished rules and filters to keep your systems protected

**2. Stops Virus Attacks**

Nothing can shut your digital operations down faster and harder than a virus attack. With hundreds of thousands of new threats developed every single day, it is vital that you put the defenses in place to keep your systems healthy.

**3. Prevents Hacking**

Unfortunately, the trend of businesses moving more toward digital operations invites thieves and bad actors to do the same. With the rise of data theft and criminals holding systems hostage, firewalls have become even more important, as they prevent hackers from gaining unauthorized access to your data, emails, systems, and more.

**ADVANTAGES AND DISADAVANTAGES**

**ADVANTAGE**

**Versatility:** The ability to consistently upgrade and adapt your network security in real time provides a lot of flexibility and versatility to your IT team. Additionally, you can more easily control the flow of data and users if your business changes the way it operates.

**Intelligence Port Control:** The smarter your security system, the more effective you can count on it to operate.

**Consistent Network Speed:** As mentioned, traditional firewalls can bog down your systems more and more as you increase the breadth of your protections.

**DISADVANTAGES**

**Application Awareness Limitations:** Organization firewalls lack the ability to go as deep as NGFWs, especially when it comes to applications.

**Issues with Network Speed**

Speed is an issue. Many organization firewalls create a bottleneck at the data inspection points, which can slow down your operation and cost you money.

**3. Logistical Drawbacks**

Many organization firewalls are not capable of adapting to the changing aspect of company systems and operations.

**CONCLUSION**

In this effort we have made an attempt firstly to assess the organization belief of majority of management of organization in context of firewall deployment and its operations. Then the important and benefits of the firewall are discussed. All through the survey followed by analysis it was the major point that there is lack of expertise about the functioning of firewalls in an organization.

**RECOMMENDATION**

After you have completed your firewall system setup, you need to administer and manage it on an ongoing basis. One of the weakest links in your security setup is the people maintaining it: People are prone to making errors. Therefore, your security solution should be simple enough for your administrators to make changes to it and to troubleshoot it, yet still meet the objectives outlined in your company's security policy.

Even in this situation, configuration errors will be made in your firewall system. Therefore, before any changes are made to the firewall system, it is important that you back them up before the changes are made. After changes are made, it is of the utmost importance that you always test changes in your firewall system.

**REFERENCES**

Dowd, M. Mary, J. (2007) firewalls outside as the configuration rules is given in the firewalls by administrators. *IEEE Journal of Symposium on Security and Privacy, 02(07)*

Amos, E. (2003) the increasing degree to which internal networks are connected to the Internet: *Journal of Security Architecture Blueprint, Arctec Group, LLC, 03(03)*

Cheswick, A. Bellovin, E. (2005).define a firewall as a collection of components or a system that is placed between two networks and possesse. the following properties: *Journal of IBM Service Management,04(05).*

Marianne, I. (2004)Proxy Server is like a sharing (Virtual) machine. *Journal of Harrington Network Security 04(04)*

Avinashi, A. (2001) Firewalls are the first line of defence in protecting against unauthorized access. *IEEE Internet of Things Journal, 05(01)*

John, T. Amos, M. (2004) A Hardware Firewall is a device that typically sits between your devices and the internet that filters out network traffic.*Journal of ACM Transactions on firewalls Networks,06(04).*

John,T. (2004) it takes processing power to run. *Journal of Computers, IEEE 07(04)*

Charles(2007) Understanding the benefits of firewall security is the first step needed. *Network Security Journal of US, 08(07).*