RESEARCH ARTICLE OPEN ACCESS

Firewall Selection and Placement

Azhar Ushmani

ABSTRACT
This article is part of a project that focuses on the importance of firewalls in organizations and their role in protecting servers from outside attacks. The internet is a primary source of cyber-attacks, making it crucial for network administrators to establish criteria for blocking unauthorized access. This part of the project aimed to select a firewall that is both secure and easy to manage to support the organization's operations effectively. The chosen firewall should ensure that remote access does not compromise the organization's servers, and the organization will use both personal and commercial firewalls for maximum protection. A demilitarized zone will be created to separate the internal network from the internet and prevent attacks on the organization's servers. This zone will use multiple firewalls, and authentication will be required at various levels to ensure network security. The project will use the pfSense firewall due to its ease of management and capacity to work with VPN connections. The company must also train its administrators to manage the commercial firewall effectively or outsource this task. Finally, the default firewall configurations will be changed to prevent attacks.
Keywords: -Cybersecurity, firewalls, commercial firewall, protection, pfSense firewall

I. INTRODUCTION

Nowadays, nearly all businesses utilize the internet to communicate better with their customers and partners. However, this also raises concerns about the safety of the network and computer systems. The issue of internet security has become a significant problem, and it appears that simply preventing malicious activities will not benefit everyone. Therefore, this study investigates the usage of firewalls to safeguard the internet by examining various technologies and firewall types and how they can aid in protecting the internet. The study suggests that firewalls have played a crucial role in averting widespread security threats on the internet. As a result, implementing firewalls could potentially improve the efficiency and safety of the internet.

Bourgeois et al. (2019) note that firewalls are essential to an organization since they protect a company's servers by blocking the outside packets that fail to meet specific criteria. The network administrators specify these criteria in an organization to ensure the safety of their network from unauthorized actors from outside the organization. The internet is usually the primary source of attacks, especially from those accessing a company's web services, since the attackers target the web servers to penetrate the organization's network. This project concerns selecting a firewall and placing it where the organization benefits from it by stopping all potential attacks from entering the organization. The security considerations include the organization's population and infrastructure in the organization. However, the most crucial consideration will be the operational environment since most of the company's staff will operate remotely, with a higher risk to the organization.

The link between the organization and the remote workers will be the internet which poses many threats to the organization. The internet could be described as the attackers' space since many malicious actors seek any opportunity to compromise organizations (Schoenfield, 2015). Understanding this effect will help the corporation deploy effective strategies to help it handle the threats in its operational environment. The company will begin by replacing the old firewall. It will also separate the internal network from the external network minimizing the attack surface since the web servers will be in a separate region where the company can detect ad eliminate the attacks before they affect its operations.

II. FIREWALL SELECTION

The company will consider the selected firewall's security and ease of managementto support its security and deliver to the users effectively. Once such a firewall is available, it will be easy for the company to drive secure operations and become more competitive in itsoperational environment. The

firm will use a commercial and a personal firewall to drive its operations since the two will provide these critical considerations to an effective and secure organization. A personal firewall is designed for personal use. Therefore, it is easy to manage and ensure that the organization is secure.

The commercial firewall could require additional skills to ensure the company is in a reliable position to deliver to its customers. The selected firewall should ensure that the remote access does not compromise the database servers in the organization through access by the attackers who attempt access to the organization when the users access it using the remote desktop protocol. A personal firewall ensures easy usage and protects the organization from potential attacks. However, the company must tune it to serve the needs at the corporate level. The selected firewall will be the pf sense firewall since it is easy to manage due to its lower skill level requirements. This firewall will work in line with the VPN connections to the organization since it also has an in-built VPN functionality (Stewart & Kinsey, 2019).

The company is also growing and needs solutions that address its capacity. This case will require a commercial firewall to manage its large size and make it more competitive in its operational environment. The challenge is that the company must train the administrators to use the latest versions of the commercial firewall to ensure they professionally manage the organization's security. Alternatively, the organization could outsource the skill for configuration, and then the administrators will maintain the firewalls. Besides, the administrator must configure the windows firewall on the windows servers and workstations to ensure all the computers are secure from attackers outside the company's environment.

III. DEVELOPING A DEMILITARIZED ZONE

A demilitarized zone ensures the organization separates its internal environment from the internet, ensuring the threats do not affect its internal servers. The company will require an additional web server since its client base has increased, and there will be more requests to access its services from the internet. The essence of an additional web server is for load balancing to ensure the load is not on a single web server and maintain that the organization responds to all the users timely. This status will increase the users' satisfaction with the organization's services since there will be faster response times, and clients will get the services they want faster and satisfactorily.

The web servers will be close to the external environment, but multiple firewalls will be around them. The first firewall will be at the organization's perimeter to monitor and authorize the requests from the internet and ensure only the authentic ones pass to the web servers. Schoenfield (2015) notes that sophisticated attackers targeting the organization will find a way to compromise them. In this case, the web server will be an attack surface. Therefore, an additional firewall will be between the web and application servers. To filter what comes from the web servers. Lastly, since the application servers are not immune, the last firewall will face the internal servers to ensure that the potential attacks that pass to the application servers do not enter the organization's servers (Schoenfield, 2015).

IV. AUTHENTICATION

Authentication at multiple levels will ensure that the company's network is secure from attacks. The users will be authenticated by the VPN and the machines they will access. Besides, the administrator will also activate the tunneling mode to increase the security provided by the communication channel (Solomon, 2019). It is vital to change the default configurations to ensure the attackers do not compromise them when deploying firewalls.

V. CONCLUSION

The selection of a firewall is crucial for organizations to protect their servers from unauthorized access by outside actors. The internet is a common source of attacks, and organizations must deploy effective strategies to handle the threats in their operational environment. To drive secure operations and become more competitive, companies should consider the selected firewall's security and ease of management. Using personal and commercial firewalls can provide adequate protection for the organization, and the selected firewall should ensure that remote access does not compromise database

servers. Developing a demilitarized zone with multiple firewalls can ensure that internal servers are separated from the internet and protected from potential attacks. Authentication at multiple levels is also essential to ensure the network's security. By implementing these measures, organizations can safeguard their operations from potential threats and ensure their customers receive satisfactory services.

REFERENCES

Bourgeois, David T.; Smith, James L.; Wang, Shouhong; and Mortati, Joseph, "Information Systems for Business and Beyond" (2019). *Open Textbooks*. 1.https://digitalcommons.biola.edu/open-textbooks/1

Schoenfield, B. S. (2015). *Securing systems: Applied security architecture and threat models*. CRC Press.

Solomon, M. G. (2019). *Security Strategies in Windows Platforms and Applications*. Jones & Bartlett Learning.

Stewart, J. M., & Kinsey, D. (2021). *Network Security, Firewalls, and VPNs* (3rd ed.). Jones & Bartlett Learning.