Services and features available with pfSense to secure your Organizational Network

Jamyang Tashi, Associate Lecturer
Department of Information Technology, Jigme Namgyel Engineering College,
Royal University of Bhutan, Bhutan.

ABSTRACT

This is a white paper that would help the readers and the System Administrator to get some knowledge on the pfSense, open-source software that can be easily deployed in any of the network systems. The paper presents the reader with important aspects of using the pfSense in the network and its benefits. The pfSense contains different varieties of features that can be installed, configured, and implemented in any scale of the network. The paper briefly explained the features and advantages of using pfSense from user credentials to authenticate and protect the resources in the network in terms of its confidentiality, integrity, and availability of the services to the user. The pfSense provides an easy way to set up any features required for an organization. Most features are available for free use, however, if users want to have their network a more secure and complex one, there are features the user can subscribe and download module and plugins.

Keywords: pfSense, Open Source, Security, Network, Authentication, Features

I. INTRODUCTION

Every organization has the IT resources to be protected from different kind of threats. There is not even a single organization that uses internet for sharing the resources and it the responsibility of the network administrator to secure the resources. Since, information in many organizations acts as the main resources it should maintain confidentiality, integrity and availability at all times, the concept of hybrid security – physical and logical security. Therefore, the pfSense is a firewall distribution that will secure your resources in the network. It is based on the FreeBSD operating system with a custom kernel and it also includes third party free software packages for additional functionality (Mamat et al., 2017).

According to the production description, pfSense software is able to provide the functionality of commercial firewall and it also replaced every commercial firewall such as Check Point, Cisco PIX, Cisco ASA, Juniper, Sonicwall, Netgear, Watchguard, Astaro etc. While discussing on the configuration, it can be configured and upgraded through a web-based interface, and requires no knowledge of the underlying FreeBSD system to manage. pfSense is mostly installed and configured wo work as a firewall to protect the system and server, wireless access point to provide wireless connectivity to the clients, IP assignment as a role of DHCP server, mapping and translation of IP address as the role of DNS server, and also VPN endpoint. pfSense supports wide variety of installation and it can also be installed as of third-party packages like Snort or Squid using the package manager.

pfSense is also an Enterprise-Grade open-source firewall. It has lots of features that are usually available on high priced firewalls of proprietary nature. There are no licensing issues and has every feature that top brand name firewalls offer. It provides great stability unless a hardware problem occurs and performance is great.

This study on pfSense will help an organization to optimize their network performance. pfSense if configured correctly is more secured that any other expensive firewalls available in the market today. Basic features such as captive portal can be configured to authenticate users before accessing the Internet. You can also configure pfSense to be used as VPN end station that uses encryption and other security measures to send data privately and securely through a wide area network (WAN) such as the Internet. (Aryeh*et* al., 2016)

pfSense is remarkably full-featured and very fast firewall that is built on FreeBSD, using the stellar pf packet filter. The interface for the user is as good as if not better than many expensive commercial offerings, and you can always

dig under the covers if you like. It supports Point-to-Point Tunneling Protocol (PPTP), Layer 2 Tunneling Protocol (L2TP), Internet Protocol Security (IPsec), and Virtual Private Networks (VPN). It can handle multi-WAN configurations, and it offers Quality of Service, extremely detailed performance data collection and graphing, load balancing, captive portal, DHCP services, and all kinds of other capabilities. (Jones et al., 2019).

According to Nahid Kausar Shaikh, pfsense is created on the FreeBSD operating system with a custom kernel and includes third party free software packages for additional functionality. The pfSense software provides most functions and features similar to a common commercial firewall. Since it provides a similar functionality with the pfSense, it has successfully replaced some of the commercial firewall around the world, including Check Point, Cisco PIX, Cisco ASA, and more, with its advance features and reliability. The pfSense has proved its advantage over other firewall and is now widely used in Small Office Home Office (SOHO) environments and Small and Medium Business (SMB) environments.

The help desk support analyst at an energy/utility company with 6500 employees has stated that they have installed pfSense across three sites where it is configured on the Virtual Private Network (VPN) and firewalls between their branch office at different geographical locations. With the implementation of VPN, communication between end devices is secured ensuring security, privacy protection, restricted access, better connectivity, and so on. It has also reduced cost drastically and has outperformed its expectations. (Arunwan et al., 2016).

According to Senior System Administrator, Samir Ramazanov stated that "We like pfsense mostly for being able to use BSD compiled software inside it. It is fast, flexible, powerful and full of features, such as easy proxy filter, and clustering along with an easy and well-developed web-based interface". The study also mentioned that before using pfsense he always had problems with internet connection for the user, he also had no idea what users were downloading and had no statistics on the quality of the internet.

II. BENEFITS OF PFSENSE

The first advantage of using the pfSense is that it has many features which are very rich, robust, and very flexible. Besides this, it also has an essential firewall feature in addition to many additional features for network routing, remote connectivity, diagnostics, and reporting, etc. It is also an extensible platform where users do not need to have to settle for the functionality provided with pfSense. The users have the right and freedom to write their own plugins and add-ons.

With all the enterprise-grade features and security pfSense provides, it is unbelievable that it is made free to all the users who wish to use it and also made it an open-source product which the users have been enjoying the biggest benefit. The user can download it from the pfSense website at https://www.pfsense.org/download/, and install it without much difficulty. Similarly, if you want to protect your network organization much complex way then the user will have an option to purchase the licensed version that will support a more complex way of securing your network organization. But those features are all left up to the users as optional.

Many users have found that pfSense is very adaptable and flexible. If you are working in an organization, you can use pfSense to protect your network. At the same time if you are working in an enterprise business, you can still use pfSense to protect various parts of your work.

It supports up to on very minimal computer configuration to very large and sophisticated computers which made this product more scalable. The user can also expand the resources of pfSense infrastructure with the expansion of your network. Considering those benefits and advantages, many of the pfSense features helps to promote the product and that makes the system administrator, network administrator, security enthusiastic and an individual to embrace the pfSense.

III. FEATURES OF pfSENSE

The following are the most common features and services the user can integrated in the network at the time of installation and configuration of the network.

1. Firewall

A firewall is a security device that controls the inbound and outbound network traffic of an enterprise to the internet. It also filters source and destination IP addresses, source and destination ports for TCP and UDP traffic. It can be used to prevent intrusions and provide a secure data exchange between internal and external users of the shadow.

Filtering source, target IP, protocol, target portal, restricting connections with rule base, approving or blocking data packs transition according. directing for each rule on a policy basis, and normalization of packaging are some of the activities done by the firewall.

2. Network Address Translation

Network Address Translation is the translation of an Internet Protocol address used within one network to a different IP address known within another network. Generally, directing ports, address transformation on the IPs and networks, reflecting of address transformation, providing to local network devices that have an external IP address to connect servers that have a local IP address are some of the activities managed by the Network Address Translation.

3. Captive Portal

Captive portal is a technique that forces HTTP clients on a network to see a special web page (usually for an authentication purpose) before using the internet normally. A captive portal turns a web browser into an authentication device. Captive Portal service is used on public-access networks that require a user to view and interact with before being granted. This service can also use on corporate networks as well to make an extra security layer. With captive portal service, you can customize the following services.

- Restricting maximum concurrent connections from a client's IP.
- Idle timeout: Logging of users that's status value is idle.
- Hard timeout: Logging off all clients for a specific timeline.
- Logon Pop-up windows: After establishing a connection log off-screen could be set as a pop-up screen.
- URL redirection: After a successful authorization users can redirect to a certain URL address.
- HTTP or HTTPS: User Authorization can be done via http or https portal page.
- File manager: Provides different pages or /and pictures uploading to Portal Page.

4. Virtual Private Network

Virtual Privet Network extends a private network across a public network such as the internet. It enables a computer to send and receive data across a shared or public networks as it is directly connected to the private network. The pfSense software offers three options for VPN connectivity, IPsec, OpenVPN, and PPTP.

- IPSec; - IPsec allows connectivity with any device supporting standard IPsec. This is the most commonly used for site-to-site connectivity to offer pfSense installation, other source firewalls and mostly commercial firewall solutions. It can also be used for mobile connectivity.
- OpenVPN: - OpenVPN is an open-source software application that implements virtual private network (VPN) techniques for creating secure point-to-point or site-to-site connections in routed or bridge configurations and remote access facilities. It uses a custom security protocol that utilize SSL/TLS for key exchange. It is capable of traversing network address translator (NATs) and firewalls. It also allows peers to authenticate each other using a pre-shared secret key, certificates or username and password. OpenVPN is a flexible, powerful SSL VPN solution supporting a wide range of client's operating systems.
- PPPoE Server:- The pfSense software offers a PPPoE server which means local User database can be used for authentication and RADIUS authentication with optional accounting is also supported.

5. Domain Name System

The DNS is a server that will resolve IP address to name and name to IP address. DNS is implemented using the concept of DNS server and DNS clients. There is concept of DNS zone such as primary, secondary, forward lookup and reverse lookup zone while discussing about the DNS database.

6. Proxy

The Proxy will act as an intermediary for requests from clients seeking resources from other servers. The connection is done where a client connects to the proxy server, requesting some services such as establishing the connection, accessing the files, web pages or other resources available in the proxy server.

7. Dynamic Host Configuration Protocol

DHCP is a services protocol that assigns a unique IP address to devices to devices, then releases and renews this address as devices leave and re-join the network. This helps in automatic IP assignment in the network that will

reduce the human error. This protocol eases the job of the network administrator or system administrator tremendously.

8. Multi-WAN

Multi-WAN functionality enables the use of multiple Internet connections, with load balancing or failover for improved Internet availability and bandwidth usage distribution.

9. Server Load Balancing

Server load balancing is used to distribute the load between multiple servers. This is commonly used with a web server, mail servers, and others. The server that fails to respond to ping or request or TCP port connections is removed from the pool.

10. Reporting and monitoring

The pfSense supports two graphs, RRD Graphs, and SVG graphs. The RRD graphs in the pfSense software maintain historical information. it maintains historical information about:

- CPU utilization
- Total throughput
- Firewall states
- Individual throughput for all interface
- Packets per second rates for all interface
- WAN interface gateway ping response times, and
- Traffic shaper queues on a system with traffic shaping enabled

IV. LOGICAL WORKING PRINCIPLES – AUTHENTICATION

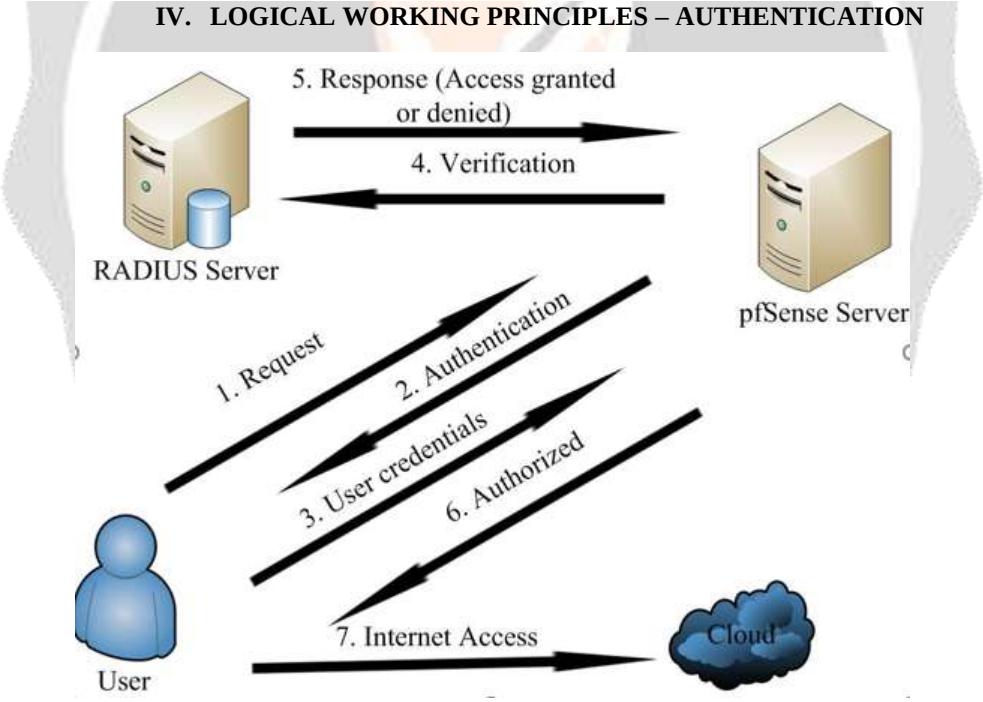

Figure 1- User Authentication Process

There are different types of authentication process for the pfSense with different sevices features implementation. The below is the working principles in the authentication process using the captive portal.

1. **Request**: As any user tries to access the internet from any of the available clients, it sends the request to the internet or web server through browser.

2. **Authentication**: Before the request is accepted by the internet or browser, the pfSense which is an operating system with configured captive portal will ask for user credentials. The captive portal displays captive portal login page asking to enter user credentials.
3. **User Credentials**: The user has to provide username and password that is provided by the administrator.
4. **Verification**: As soon as the user provides the username and password, pfSense forwards the verification to RADIUS server which checks its database for that particular user name and password.
5. **Response** (Positive and Negative): After verifying the username and password, it gives back the response to the pfsense. Here positive response is given if the username and password are correct allowing the user to browse and access the internet. It gives negative response if the username and password provided by the username is incorrect thus denying user to access the internet.
6. **Authorized**: After the user has been given the right to browse and access the internet, the user is authorized, meaning it has the right and permission to browse and access the internet.
7. **Browse**: Only after the user has been authorized, the user has a right to browse the internet.

V. THE BASIC NETWORK DIAGRAM

The diagram below gives the user an idea of how pfSense plays a dynamic role in the network. The ISP Modem or Router connects the pfSense to the internet and similarly, the networking switch connects pfSense to various user's computers.

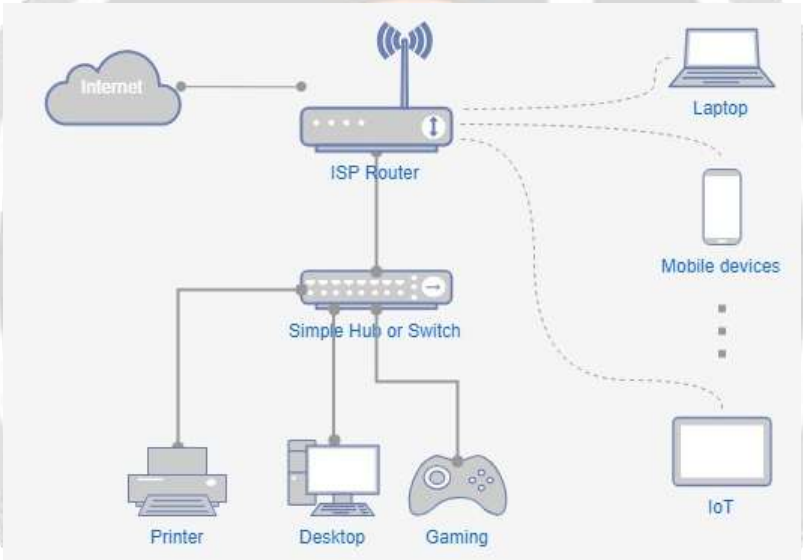

Fig 2- Basic Network Architecture

In this diagram or scenario, pfSense acts as a DHCP server that will assign the IP address to all the user computers in the network, a Firewall to filter the incoming and outgoing packets, and NAT to do the address translation to the outside network. Therefore, it plays a distinct role simultaneously.

- The DHCP Relay Agent feature in the pfSense server serves the DHCP service for all client computers in the network.
- The Firewall feature filters the requests and responses sends by the source and destination IPs in the network, and source and destination ports. It also confines simultaneous connections on a per rules basis.
- In the NAT port forwarders, it includes a range of IPs and the use of multiple public IPs. It also forwards one-to-one NAT for individual IPs or multiple subnets in the network.
- The Multi-WAN functions in the given diagram enables the use of multiple internet connections in the network with failover, and usage distribution, and load balancing. This enables the user to accomplish redundancy across multiple ISP connections. It is also not limited to that, and not only that, you can distribute the traffic from your internal network to the internet to numerous links in a load-balanced fashion.

As a VPN server, pfSense offers two different options for VPN connectivity in the network:

- IPsec allows connectivity with any of the networking devices supporting standard IPsec. Most importantly, this is mostly used in configuring the site-to-site connectivity to other pfSense installations and almost all other firewall solutions like Cisco, Juniper, and so on. This is also used for mobile and remote client connectivity in the network.
- The second in the diagram is OpenVPN. its powerful SSL VPN solution and it is very flexible, which supports a wide range of client operating systems. Let's assume that the computers are on different sites. The user can use IPsec VPN to connect them both together.

VI. CONCLUSION

As covered up in the write-up, this paper was to help readers know the key benefits of using the pfSense in their network organization in securing the resources. pfSense is used for different purposes based on the features user uses and many studies were carried out to check the functionality, reliability, and feasibility of its features to meet the requirement and expectations of the organization and its clients. pfSense feature, Captive Portal asks for the user credentials from the user to access the Internet services and thus enables the network administrators to keep track of users who are currently logged into their network. This ensures a fair amount of bandwidth distribution among all the users in an organization and improves network performance.

Since pfSense is open source and freely available it is the best firewall solution for small and medium business industries. Easy configuration using a customizable graphical user interface is an added advantage of using pfSense. Most of the industries today prefer high-end single functionality firewalls in their network for information security which is very expensive and difficult to configure and manage. Implementing pfSense will provide better security over external threats and information transferred over the internet is protected as it provides Virtual Private Network (VPN) functionality that can be configured easily.

VII. REFERENCES

[1]. Buechler, C. & Ullrich, S. (2008*). "*pfsense TurorialBSDCan". Retrived August 2, 2021. Available at https://www.bsdcan.org/2008/schedule/attachments/66_pfSenseTutorial.pdf
Mamat, K, Ruzana Mohamad Saad (2017); "A Review paper on pfsense – an Open source firewall introducing with different capabilities & customization". Retrieved on August 25, 2021.

[2]. Felix Larbi Aryeh, M Asante, A. E. Y. Danso (2018); "Securing Wireless Network Using pfSense Captive Portal with Radius Authentication – A Case Study at UMaT". Retrived on August 25, 2021. Available at http://www2.umat.edu.gh/gjt/index.php/gjt/article/view/21

[3]. Jones, J., & Chou, T. (2019), An Infrastructure Supporting a Game-Based Learning System for Information Security Topics Paper presented at 2019 CIEC, New Orleans, LA. https://peer.asee.org/31524

[4]. K.N. Shaikh., P. Dhawale., & S. Agrawal (2018). "A Survey on Network Firewall Solutions", Retrieved on July 23, 2021. Available at https://www.apsitjournals.com/apsitjoun/Article%202/A%20Survey%20on%20Network%20Firewall%20Solutions.pdf

[5]. M. Arunwan, T. Laong and K. Atthayuwat, "Defensive performance comparison of firewall systems," *2016 Management and Innovation Technology International Conference (MITicon)*, 2016, pp. MIT-221-MIT-224, doi: 10.1109/MITICON.2016.8025212.

[6]. pfSense Plus Logo White (nd), "The world's leading open-source driven firewall, router, and VPN solution for network edge and cloud secure networking". Retrieved on August 27, 2021. Available at https://www.netgate.com/pfsense-features

[7]. pfSense (nd). "Open Source Security", Retrieved on June 30, 2021. Available at https://www.pfsense.org/