A Review paper on pfsense – an Open source firewall introducing with different capabilities & customization

[1] Krupa C. Patel, [2] Dr. Priyanka Sharma
[1] Student M.Tech(Cyber Security), [2] Professor(IT)
[1.2] Department of Information Technology
[1.2] Raksha Shakti University, Gujarat-Ahmedabad, India.

ABSTRACT

Network Security is a crucial aspect in network management with many formation around the world spend millions each year to safeguard valuable corporate data and information. Many companies use firewalls and encryption mechanisms as security diamention. Although there are many types of firewalls and encryption mechanisms in the market, not all are suitable for Small and Medium Enterprises (SMEs). For SMEs, these operations might be an overkill, both financially and functionally. For proper and centralized control and management, range of security features need to be integrated into unified security package One of the most efficient solution will be carried out by an open source firewall. In this paper we are carried out a case study of different existing features of an open source pfSense, a firewall on FreeBSD operating system such as, a comprehensive network security solution which integrates all of the security services such as firewall, URL filtering, virtual private networking etc in a single appliance, Captive Portal and Active Directory for managing user authentication for wireless network, analyse the logs to make network infrastructure more secure, layer 7 capabilities providing a powerful solution to control traffic based on application patterns and lastly used as a tool with other different open source tool will work well together in detecting and disabling network attacks.

Keywords: *Network security, pfsense, open source, Securing, Wireless, Network, Authentication, and access logs*

I. INTRODUCTION

In this 21st century, the internet has become a powerful tool for all regardless of age. Its purpose varies among users. Some see it as a reliable source of getting information and making a business transaction. Others also use it as an intermediate to connect to different people across the globe on social networks, play online games, upload and download music and videos, etc. The traditional security solutions individual is becoming increasingly in adequate to protect infrastructures from newer threats. Defense efforts must be unified to provide comprehensive protection against continually changing network and cyber threats.

Many companies use firewalls and encryption mechanisms as a security measure (BhavyaDaya, 2013). Although there are many types of firewalls and encryption mechanisms in the market, not all are relevant for small companies such as the *Small and Medium Enterprises* (SMEs). For SMEs, these applications might be an overkill, both financially and functionally. Open source firewall distributions are a new set of security distribution, replaced with graphical interface, compared to the traditional command line interface (CLI), fully operational with cost-effective features and upgrading firmware. There are lot many open source firewalls are available in current scenario.

Table 1: Comparision of three Open Source Firewall

Firewall	Untangle	Pfsense	Ipfire
Os type	Linux/NanoBSD-based appliance firewall distribution	FreeBSD-based appliance firewall distribution	Linux/NanoBSD-based appliance firewall distribution
License	GPL Version 2	ESF version 1.0	GPL

Stateful firewall	Yes	Yes	Yes
Application firewall	Yes	Yes	Yes
Architecture	I386, x86_64	I386, x86_64	I386, x86_64
QoS	Yes	Yes	Yes
Interface Management	CLI and GUI	CLI and GUI	CLI and GUI
VPN/SSL/IPsec	Yes	Yes	Yes
IPV6 support	No	Yes	Yes (Since IPFire 3)
Official download	https://www.untangle.com/get-untangle/	https://www.pfsense.org/download/	http://www.ipfire.org/download
Price	https://www.untangle.com/partner-portal/sales-tools/price-lists	Free	Free

By comparing all open source firewall, pfSense meets the objectives required for this paper to implement with modern security extensions and solutions.

II. THE PFSENSE PLATFORM

pfSense is a customized FreeBSD distribution, primarily oriented to be used as a firewall and router. It started as a fork of the m0n0wall project. m0n0wall was mainly directed towards embedded hardware installations. pfSense, on the other hand, it is mainly focused on full PC installations, despite the fact that pfSense also offers solutions for embedded hardware. It consists of many base features, and can be extended with the package system, including “one touch” installations.

pfSense is currently a viable replacement for commercialfirewalling/routing packages, including many features foundon commercial products (Cisco Pix, SonicWall, WatchGuard).The list of features, among others, include the following: firewall, routing, QoS differentiation, NAT, Redundancy, Load Balancing, VPN, Report and Monitoring, Real Time information,and a Captive Portal. It is fully prepared for highthroughput scenarios (over 500 Mbps), as long as high endserver class hardware is used.

PfSense uses a single XML file, called config.xml, which stores the configuration of all services available in the pfSense machine. The code responsible for the operation of the distinct pfSense services is essentially written in PHP, which makes easy to extend the current code base, improving existing features or adding new ones.

III. LITRACURE REVIEW

A. Implementing UTM based on pfsense platform

Defense efforts must be unified to provide comprehensive protection against frequently changing network and cyber threats. UTM generally refers to a security appliance that consolidates a wide range of essential network security functions into a single device. UTM brings the following network security technologies in to a single platform: Firewall, Anti-spam, Anti-virus, URL filtering, Virtual Private Network (VPN).

Two types of UTM are used: A. Hardware/Appliance based UTM; B. Software/Appliance based UTM.

In this paper, we implemented UTM based on pfsense rather than hardware/software Appliance, two main factors contributed to this reasoning. First, this approach can be cost-effective than hardware/software based. The second factor is the stability of it, makes less failure for our network. The main objective behind our solution was to mitigate bandwidth as well as the cost. The basic idea is that when a user visits a web site, the content of the page are cached on a proxy server. The next time that person visits that web page content does not have to be downloaded because it already exists in the cache. And using squidGuard on WAN interface to filter URL address. Squid3 proxy server caching the web supporting HTTP, HTTPS, FTP and etc.it caches all IP subnet with high range of users with low error ratio.

Implementation results shows optimization of bandwidth having graph with 20MB bandwidth and 600 active-users, and minimizing required resources as squid3 proxy continuously caching on pfsense, on the other hand a lot of services is running on pfsense but CPU usage is low.

As a conclusion, pfsense is a powerful open source UTM with many advanced features and services that demonstrates a good performance in a big organization , it reduces complexity and costs, easy to manage with high reliability but need some proper and easy way that was based on user.

B. Securing Wireless Network Using pfSense Captive Portal with RADIUS Authentication – A Case Study at UMaT*

In a WLAN, communication and data transfer use radio transmission, which is open to all users. For that it uses WEP, WPA/TKIP, WPA2 chronologically. However, some researchers have uncovered a vulnerability in the WPA2, which is the strongest for Wi-Fi encryption and authentication currently standardized and available. Hence, to improve the security of WLAN, a new secure mechanism called Captive Portal has been introduced which uses a webpage to authenticate users.

In order to use pfSense Captive Portal for UMaT wireless network, pfSense has to be installed on a server and configured with one LAN interface to assign an IP to the appliance. The LAN interface has to be assigned a static IP address and default gateway. Every user on pfSense LAN has to pass through this default gateway before he/she reaches WAN network.

By using the experiment setup, weinvestigate the following:

1. How to configure pfSense Captive Portal?
2. How to configure RADIUS server?
3. How to set the policy and securitymechanism?
4. How to manage user credential?

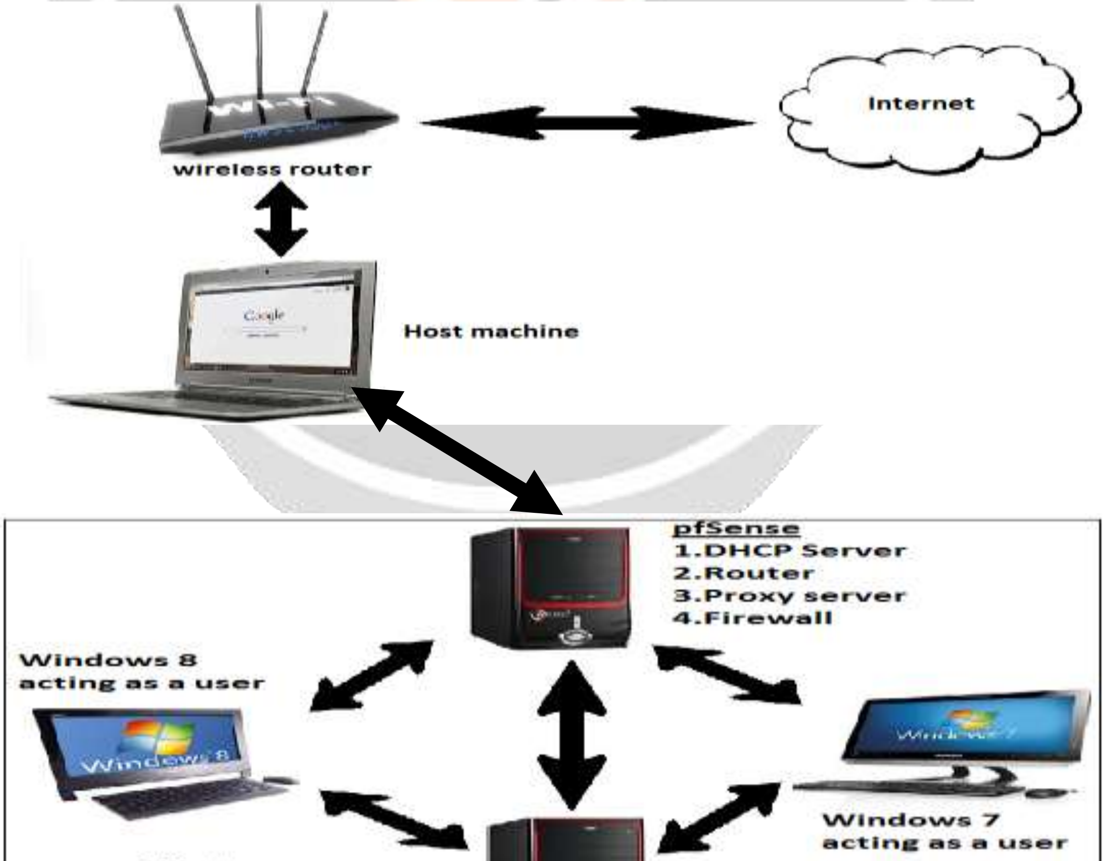

Fig- 1: setup

Result and discussions shows how to configure and implement all the above questions. As This paper aims at disabling concurrent logins for Captive Portal, hence, provision was made by generating vouchers for guest or visitors to the university to also have access to the internet.

The experiment conducted demonstrated how to achieve the configuration of pfSense Captive Portal and a local RADIUS server for authenticated users on a wireless network and secure their credentials. A user connected to the wireless network is assigned an IP address by the Dynamic Host Configuration Protocol in the pfSense and any web request from the user is redirected to the Captive Portal page. This paper sort to find a simple way to incorporate already existing users in an AD to communicate with the Captive Portal instead of manually entering details into the pfSense local user account. The approach used by Mamat and Ruzana (2013) will be difficult for large organisations. In the future to enhance the level of security at the OSI reference model layer 7 by protecting a range of attacks against web applications and also to allow for HTTP traffic monitoring, logging, and real-timeanalysis.

C. Network security with open source firewall

Information technology changes regularly and it is very important to protect our systems and network infrastructure from compromising. So the main purpose of this educational research is to test the weaknesses of the secure and unsecured environments .

The aim of this research is to analyse the system logs that are generated in the virtual environment (Which is secure with pfsense firewall). The method used in this research is 'Whitebox Testing'. Whitebox testing is the part of the penetration testing
The tools & script used in this testing are,

1. Nmap (Network Mapper)
2. traceroute
3. tcptraceroute
4. NmapFirewalk Script
5. XPROBE2
6. ARMITAGE

They do information gathering, scanning of system, generate log with above tool in addition to that they shows results of with pfsense firewall result and without firewall result.

After the white box testing , from the pfsense firewall logs we can understand that attacking pattern of a hacker or intruder . Also we can find out the behaviour of attack . How, by analysing those protocols, flags – ,ack, fin , ports and the ports number . Even administrator, security expert can study these attacking pattern from the logs and he can protect its own network infrastructure or after studying this type of virtual environments , he can redefine his secure physical infrastucture. In short this whole research helps us to upgrade our network security with the help of open source firewall.
Future research includes,

- This research helps in the logical and practical implementation of the firewall security to make network environments more secure .
- This research helps administrator to understand the attack.
- He can analyse and trace attacker with the help of firewall logs.
- It helps to make your system more secure and network infrastructure more secure.
- It helps students to understand how things are actually going behind the scenes.
- We can test different types of attacks on virtual environment.
- The logs analysis helps network administrator to understand what happen when an attack is done. Like Ddosattack , Decoy attack etc. Without breaking any cyber law .
- Also we can analyse the log and see which Tcp ports are used during the attacks so that in future we can close that ports .

D. Open Source Versus Commercial Firewalls: Functional Comparison*

This paper performs an experiment to compare two firewall alternatives with the capability of deploying Virtual Private Networks (VPNs) over the Internet, one being *an* open source software solution **and** the other being a proprietary commercial product. This research provides analysis to the current security debate between "open source" and "security-by-obscurity" solutions.
Two specific firewall solutions are compared highlighting corresponding security risks:
(1) a firewall constructed using only open source software available for the Linux operating s.wtem and

(2) a commercial jrewall solution from Cisco using the Cisco 10s firewall feature set

Comparison of Firewall Alternatives are based on network level filtering, application level filtering and VPN capabilities.

Experimental Resultsshows that the Linux firewall has consistently higher transaction throughput rates for rule sets varying from 0 to 200 rules and for packet sizes of both 1 and 128 bytes. So it concluded that Linux firewall has superior transaction rate performance and application-level filtering capabilities. The Cisco 10s firewall is functionally superior for network level filtering, VPN capabilities. Ultimately, the most effective firewall solution may be a combination of both application level and network level packet filtering. This experiment demonstrate a basis for future experiments building toward general conclusions between open source implementations versus general commercial implementations.

E. L7 Classification and Policing in the pfSense Platform

The traditional way to organize traffic entering a network domain is usually based on network and transport data fields, e.g. service class marks, source and/or destination IP addresses and ports. Although in many cases this type of classification provides a good compromise between simplicity and efficacy. In this context, performing traffic classification and policing at the application layer (layer 7 or L7 in short) can be a convenient solution to conquer these limitations. In L7 classification, user traffic can be identified based on an application pattern.

Examples of related work on L7 classification include IPCop Firewall and Bandwidth Arbitrator . Although IPCop can support classification by application protocol, it does not allow the definition of shaping policies, only accepting blocking policies. In the present work, we study and tackle the L7 classification paradigm for the pfSense platform. Although pfSense already includes support for traffic classification at application layer, it does not introduce that capacity to the user.

In this context, we have established the following goals: i) to develop mechanisms to control the classification component in the application protocol, consolidating them in the platform through a graphical interface; ii) to define and implement user-friendly wizards to clarify the configuration of QoS rules; iii) to plan and develop a test platform which allows testing multiple patterns of applications simultaneously, and to measure the performance (e.g. response time) of the classification module based on the application layer.

After the implementation, It is concluded that pfSense has now another shaping mechanism, that puts it on par with a extent amount of commercial solutions, and it also has now a fully integrated GUI that grant the end user to easily leverage the layer 7 capabilities that ipfw-classifyd provides to the pfSense platform. The only current drawback in that ipfw-classifyd is not currently fully operational due to ongoing improvements.
As future work, we think there is still some room for improvement. In particular, performing L7 inspection directly in kernel land would be very essential and should be faced as a top goal. This would avoid the overhead introduced by the context switch between kernel and user land, that is crucial to divert IP packets from the kernel to ipfw-classifyd or to other application for that purpose.

F. Design of a Network Security Tool Using Open-Source Applications

Many companies use firewalls and encryption mechanisms as a security measure. Although there are many types of firewalls and encryption mechanisms in the market, not all are suitable for small companies such as the *Small and Medium Enterprises* (SMEs). For SMEs, these applications might be an overkill, both financially and functionally. This paper proposes the design of Network Defender, a network security tool, based on open source applications.

Network Defender is composed of four components namely *Firewall*, *Network Intrusion Detection*, *Vulnerability Scanner* and *Exploit Tool*. The value of this design was demonstrated by the implementation of Network Defender using *PfSense*, *Snort, Nmap* and *Metasploit*. Test results show that all four components work well together in detecting and disabling network attacks. The usage of Metasploit also enable reverse attacks to be carried out.
Test results show that all components work well together in detecting and disabling network attacks.

Future work include the inclusion of other tools and applications such as SMS alerts and centralized database to better equipped *Network Defender* against attacks. It is hoped that this study has provided a cheaper alternative to SMEs in guarding their network.

Table 2: Summarization of literature survey

Sr. No	Name	Advantages	Disadvantages
1	Implementing UTM based on pfsense platform	It consolidates a wide range of essential network security functions into a single device	It needs some proper and easy way that was based on user.
2	Securing Wireless Network Using pfSense Captive Portal with RADIUS Authentication – A Case Study at UMaT*	It improves the security of WLAN,Captive Portal has been introduced which uses a webpage to authenticate users.	It will be difficult for large organisations.
3	NETWORK SECURITY WITH OPENSOURCE FIREWALL	By using penetration testing approach,attacking pattern of a hacker or intruder and behaviour of the attack can be understood	All the tools used in testing are not included in pfsense platform.
4	Open Source Versus Commercial Firewalls: Functional Comparison*	Open source provides more or less similar function to commercial firewall	Somewhat implementation needed in open source firewall.
5	L7 Classification and Policing in the pfSense Platform	It allows the end user to easily leverage the layer 7 capabilities that ipfw-classifyd provides to the pfSense platform.	The current drawback in that ipfw-classifyd is not currently fully operational due to ongoing improvements.
6	Design of a Network Security Tool Using Open-Source Applications	*PfSense, Snort,Nmap*and*Metasploit,*all components work well together in detecting and disabling network attacks.	There are some room for improvement for adding more functionality needed to secure network by obsecurity.

IV. CONCLUSION

All through the examination work, outrageous investigation of the firewall, it is inferred that for little to medium size business an open source firewall gives the best chance to secure their system from various digital dangers. Despite all other open source firewall, pfSense demonstrated the most suitable firewall since the majority of the elements are upheld by least equipment prerequisites and in addition free permit administrations empower the utilization of these firewall. Pfsense gives incredible functionalities and elements. It gives secured association through hostage entryway. It utilizes all techniques IP based. Encourage execution is to enhance this as client based.

V. REFERENCES

[1]. Ed Tittel, Unified Threat Management for Dummies, copyright 2012 by John Wiley & Sons, Inc., Hoboken, New Jersey

[2]. K RAJESH, “HARDWARE Vs. SOFTWARE UTM AND OPEN SOURCE UTM”

[3]. VIVEK GITE, Debian, “Ubuntu Linux: Install squidGuard web Filter plugin for squid3 x to block unwanted sites”, unpublished

[4]. Anon., (2011), “Cisco” *www.linksysbycisco.com?EU?en?learningcenter/HowtoSecureYourNetwork* , Accessed: 27th February, 2016.

[5]. Danen, V. (2009), “Tech Republic”, *http://www.techrepublic.com/blog/linux-and-opensource/diy-pfsense-firewall-system-beatsothers-for-features-reliability-and-security,*Accessed: 17th March, 2016.

[6]. Mamat, K, Ruzana Mohamad Saad; “Home Wireless Network Security Using pfSense Captive Portal”, *Proceedings of 8th International Conference on IT in Asia 2013 (CITA'13) {IEEE/SCOPUS/ISI},* Accessed:12th April, 2016.

[7]. Stahie, S. (2014), “Softpedia”, *http://news.softpedia. com/news/PfSense-2-1-1-Firewall-Distro-Can-Replace-Any-Commercial-Alternative-436111.shtml,* Accessed: 21stFebruary, 2016.

[8]. Lee Allen , Advanced Penetration Testing for Highly Secured Environments: The Ultimate Security Guide,Packt Publishing , www.packetpub.com

[9]. www.wikipedia.org

[10]. ShakeelAli,TediHariyanto, Backtrack 4 : Assuring Security by Penetration Testing , Packt Publishing www.packetpub.com

[11]. “TIS Firewall Toolkit Configuration and Administration,” Trusted Infomation Systems, Inc.

[12]. pfSense Project. URL: http://www.pfsense.com/, 2004.

[13]. A. Seddik-Ghaleb, Y. Ghamri-Doudane, and S.-M. Senouci. Emulating End-to-End Losses and Delays for Ad Hoc Networks. Communications, 2007. ICC apos; 07. IEEE International Conference, 24-28:3224–3231,June 2007.

[14]. BhavyaDaya, 2013. “Network Security: History, Importance, and Future”. University of Florida Department of Electrical and Computer Engineering. http://web.mit.edu/~bdaya/www/Network%20Security.pdf.

[15]. BSD Perimeter LLC, 2004-2011. PfSense. http://www.PfSense.org/.

[16]. Firewall (computing), 2013.http://en.wikipedia.org/wiki/Firewall_%28computing%29.

[17]]. Network Working Group of the IETF, 2013. “The Secure Shell (SSH) Authentication Protocol”. http://en.wikipedia.org/wiki/Secure_shell.

[18]. Acosta, David. 2014. PCI DSS engineering controls part II: Firewall (Firewall), PCI HISPANO. Available at :http://www.pcihispano.com/controles-tecnicos-de-pci-dss-parte-ii-cortafuegos-firewall/. [Accessed : 19.05.2015]

[19]. Firewall (Computing) 2015 Available at: http://en.wikipedia.org/wiki/Firewall_(computing) [Accessed at : 03.06.2015]