International Journal of Electrical Electronics & Computer Science Engineering
Special Issue - ICSCAAIT-2018 | E-ISSN : 2348-2273 | P-ISSN : 2454-1222
Available Online at www.ijeecse.com

Implementation of Firewall & Intrusion Detection System Using pfSense To Enhance Network Security

Deepak Kumar[1], Meenu Gupta[2]
[1]PG Scholar, CSE Department, Lingaya's University, Faridabad, Haryana, India
[2]Assistant Professor, CSE Department, Lingaya's University, Faridabad, Haryana, India

Abstract: ***This paper analyses the network security issues and threats which are increasing every day. Data centre operators, network administrator, and other data centre professionals need to comprehend the basics of security in order to safely deploy and manage networks today. Because of network and threats issue and different solutions to solve this problem this paper basically analyses about the implementation of firewall and IDS. It synthesizes the firewall and intrusion detection techniques which are being used. It explains different type of detection and prevention systems which are used for securing the network from the attacks. Main objective of this paper is to case study, analyses on network and features of pfSense and how to implement it. pfSense offers different solutions,easy rule management, Blacklisting, NAT, VPN and package system that allows to expand its services.***

Keywords*: Firewall, Types of attacks, Firewall Technologies, IDS, IDS Types, pfSense, Firewall Implementation, IDS Implementation.*

I. INTRODUCTION

Network security is a fast moving technology. Network related security issues are increasing every year at very alarming rate. With the increasing complexity of threats the security measures are also increased.

Business network and IT infrastructure need an end-to-end approach and a very strong grip on the vulnerabilities and associated protective measures to be secured from the network attacks; while such knowledge cannot thwart all attempts at network engineers to eliminate certain general problems, greatly reduce potential damage, and quickly detect breaches. Network security focuses on algorithmic aspects such as encryption and hashing techniques to secure both the large and the small enterprises because of the ever-increasing number and complexity of attacks, vigilant approaches. The basic concepts rarely change, because of which the skills generally used have is insufficient to protect computer networks. When crackers started hacking the networks and systems, security courses arose that emphasized the latest attacks. Computers networks are always connected through the fault management, fault software, abuse of resources connecting computer networks; which is the major factor behind the security problems for a network. Today security problem is the biggest issue in the field of internet developing. There is no network in the world without the loopholes. People know about "virus", "denial of service, "worms" generally. The network is vulnerable because of three failure- complexity, accident and hostile intent. Though attacks have been limited a lot these days using technologies like Firewall.

II. NETWORK SECURITY

Network security deals with protection of sensitive data on a network. It maintains the integrity of network and its data, Confidentiality of Information and availability of data or network resources. According to Cisco, Network security combines multiple layers of defences at the edge and in the network. Each network security layer implements policies and controls. Authorized users gain access to network resources, but malicious actors are blocked from carrying out exploits and threats.

An attack is any attempt for access or alter of data that is stored inside a network. Generally we categorise attacks as passive attacks and active attacks, however in an organization there are three types of attacks that can cause confidentiality and unauthorized access issues.

1) Information Theft:

It is a type of passive attack which involves stealing organization confidential data, e.g. Employee Records, accounts details

2) Information Alteration:

It is an active attack, attacker modifies organization records or create fake records that can cause damage in future.

3) Denial of Service:

It is a cyber-attack, attacker seeks to make a network resource unavailable to legitimate user. In denial of service attack, attacker flood the network server with traffic, which crashes the network server.

DOS are malicious only purpose of this type of attack is to choke the network so that no one can access it.

III. FIREWALL

A Firewall is a network security system that acts as a security wall between private network and public Internet. It protects network from unauthorized access. It act as a security guard of network gateway that checks every incoming and outgoing packets and treats them according to firewall rules. Firewall can also provide network traffic details. Firewall can block or permit a traffic, it not only prevent access but also assist in identifying security threats.

International Journal of Electrical Electronics & Computer Science Engineering
Special Issue - ICSCAAIT-2018 | E-ISSN : 2348-2273 | P-ISSN : 2454-1222
Available Online at www.ijeecse.com

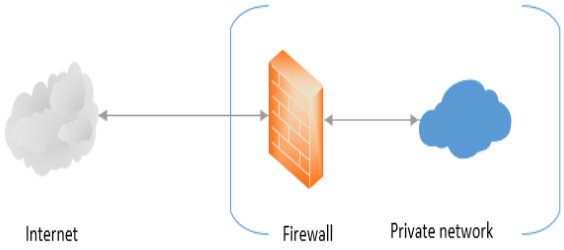

Fig. 1. Firewall

We must know firewall features and function it can perform. A firewall has these basic functions

- Manage and control Network Traffic
- Authenticate access
- Resource Protection
- Content Filtering
- Virtual private networks

1) Manage and Control Network Traffic: It is one of the most basic function of a firewall. It means firewall can manage and control network traffic whether it is incoming or outgoing. It grants or deny access based on firewall traffic rule. Firewall uses IP address and port address for creating rules.

2) Authentication Access:

Firewall does not allow unauthorized user to get access of a network. But this process can only limit the threats of unauthorized access. An expert hacker/intruder can get into the network use its IP address manually and can easily get access to all the resources that's why we need more protected way of securing the network and its resources, for verifying a user. Firewall creates login mechanism in which every trusted user has a User ID and Password. When an authorised user try to access some information then he'll be asked to verify his identity. If user input matches the database then he'll get access otherwise access permission will be denied. Firewall can also be used for assigning user rights.

3) Resource Protection:

It is most important task of firewall. Network resources are local server like web server, mail server or even proxy server that contains very sensitive data that can cause damage to an organization business.

4) Content Filtering:

Content filtering is used as a website filter technique. Basic purpose of content filtering is to block unwanted content that a user can view using browser. Firewall can block an application service or block a particular website e.g. blocking multimedia download websites or adding a filter to limit maximum file download size.

Most popular content filter technique is to use a list of keywords that administrator wants to block. Firewall can also create rules for log based access to the websites.

5) Virtual Private Network:

Virtual Private Network is a technology that is used to create a secure connection (private network) over public internet, this network is physically invisible to outside world. Implementation of VPN requires standard encryption of devices to keep network security and all network devices should support same level of encryption in order to communicate with each other.

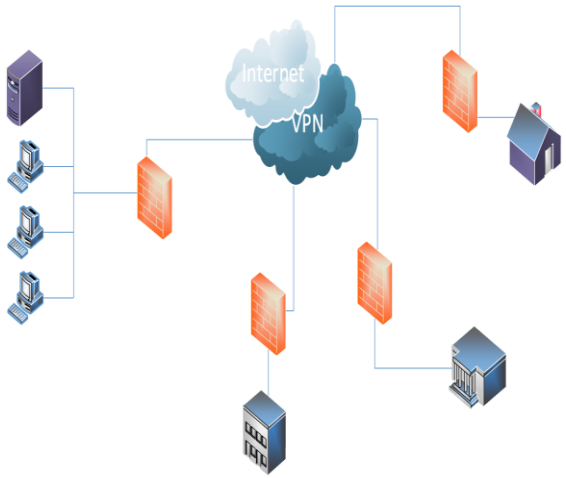

Fig. 2 An Example of VPN

6) Network Address Translator:

Network Address Translation (NAT) allows you to connect multiple computers to the Internet using a single public IP address. NAT is configured in two directions — inbound and outbound. Outbound NAT defines how outgoing traffic is translated for internet. Inbound NAT refers to incoming traffic the Internet.

Firewalls often have network address translation (NAT) functionality, and the hosts protected behind a firewall commonly have addresses in the "private address range". Firewalls often have such functionality to hide the true address of protected hosts.

IV. FIREWALL TECHNOLOGY

Firewall types and its use depends upon the size of the network and functional requirements. International Computer Security Association classifies firewall into three category: Network-level Packet Filter, Application-level Proxy Servers, Stateful Packet inspection Firewalls

1) Packet- Filter Firewall:

A firewall can be used as a packet filter. It can forward or block packets based on its source and destination IP addresses, source and destination port addresses.

A packet filter firewall is actually a router or layer3 switch that can has its own routing table and can decide if a packet can pass through its gateway or not.

But it was not very efficient because it can only work over a small network which has limited number of users or network devices. It lacks many functions which were later improved in application level firewalls.

2) Application-Level Proxy Server:

Proxy Firewall is an application gateway between local network and internet. This is an application used for verifying authenticity of individual packets. Proxy server are actually software based firewall. A network administrator configures a proxy server so that each incoming or outgoing packet can go through the proxy network. If a user sends a request, then that request is first processed by proxy server on application level. If request is legitimate then it is processed otherwise it is dropped. Proxy firewall is more secure than other firewalls and it has many functions that helps in managing the network.

3) Stateful Inspection Firewall:

It is a firewall that keep track of the state of every network connection passing through the interfaces until that particular connection is down. It maintains a table of network layer and transport layer information. If a packet does not violate firewall rules then it can pass through firewall, stateful packet firewall maintains a dynamic table about this log (Incoming and outgoing packet details). It examines every part of network packet to make sure whether to accept or deny a packet transfer.

V. INTRUSION DETECTION/ PREVENTION SYSTEM

Intrusion Detection System can be referred to as a security alarm. It alerts network administrator whenever someone try to breach into network or manages to pass through network security. Intrusion Detection System is similar to Firewall a firewall can only block unauthorised access but IDS can prevent it as well as notifies if security failure occurs.

Intrusion Prevention System is a prevention technology that detects intrusion and takes action in order to prevent the intruder. There are two types of prevention system: network based and host based. Intrusion prevention system monitors network traffic and take actions to protect network.

Intrusion Detection system can be classified into three types:

- Network based Intrusion Detection System
- Host based Intrusion Detection System
- Knowledge based Intrusion Detection System
- Behavior based Intrusion Detection System

1) Host Based Intrusion Detection System:

Host based intrusion Detection System (HIHS) uses local host machines log information to detect the intrusion. It checks through all the log files that operation system creates and analyze it. If it founds any suspicious activity then IDS treat it as an attack. HIDS are better than NIDS because it can give information about what actually happened, what operations are performed on the host on network.

2) Network Based Intrusion Detection System:

Network based intrusion Detection System (NIHS) analyzes network traffic to detect threats. Network based Intrusion system reads all incoming packets and searches for any suspicious patterns. When threat is detected it notifies Network administrator and create rule for blocking the source IP address to get access into Network.

3) Knowledge Based Intrusion Detection System:

Knowledge based or Signature based IDS references a database of past attacks logs and known system vulnerabilities to identify active intrusion attempts. It treats any situation as attack if it is similar to past attacks. It gives less false attack detection in comparison to Behavior based Intrusion Detection System.

4) Behavior-Based Intrusion Detection System:

A behavior-based or statistical anomaly–based IDS uses learned pattern of normal system activity to identify active intrusion attempts. If any activity is suspicious or not similar to the desired pattern then it will be treated as an attack and an alarm will be triggered.

VI. PFSENSE

pfSense is a free, open source customized distribution of FreeBSD O.S. specifically made for use as a Firewall, Intrusion Detection System and Router. It has many related features and a package system that allows to further expand the services provided by it without adding bloatwares and security vulnerabilities.pfSense software includes a web interface for the configuration of all its components and services. Unlike some similar GNU/Linux-based firewall distributions, there is no need for any UNIX knowledge, no need to use the command line for anything, and no need to ever manually edit any rule sets.

VII. IMPLEMENTATION OF FIREWALL

pfSense provides various firewall feature that are already integrated in it and along with basic firewall rules; squid proxy server can be used for creating a proxy firewall so that traffic can only move through this proxy socket. One of the popular technique for filtering the network packets is SquidGuard Proxy Filter.

A. Firewall Configuration using Pfsense:

pfSense offers firewall services which can be manage by set of rules and firewall logs.

1) Aliases:

Aliases can be referred to as group of IP addresses, Ports or Networks for making firewall rules easy to implement and manage. Aliases act as placeholders for real hosts, networks or ports. They can be used to minimize the number of changes that have to be made if a host, network or port changes. The name of an alias can be entered instead of the host, network or port where indicated.

Browse to *Firewall / Aliases* for creating or editing an existing alias.

2) NAT Configuration:

Browse to *Firewall / NAT* for configuring network address translation rules in Firewall.

Port Forward: In pfSense Port forward is used for accessing the admin panel over the internet. Click on add to create a port forward rule. It contains fields such as interface, protocol, destination, destination Port range, redirect target IP & redirect target port etc.

1:1 - It is used for binding internal address to external address so that traffic can move in either direction. If a 1:1 NAT entry is added for any of the interface IPs on this system, it will make this system inaccessible on that IP address. i.e. if the WAN IP address is used, any services on this system (IPsec, OpenVPN server, etc.) using the WAN IP address will no longer function.

For creating a 1:1 rule browse to *Firewall/ NAT / 1:1*and click on add button, it will lead to edit tab here user can edit or create 1:1 NAT entry. It contains fields such as interface, external subnet IP, internal IP, destination & description and save the rule.

Outbound -It manages the outgoing traffic. Browse to *Firewall / NAT / Outbound*.

pfSense offers four outbound NAT modes.

- Automatic outbound NAT rule generation.(IPsec passthrough included)
- Hybrid Outbound NAT rule generation.(Automatic Outbound NAT + rules below)
- Manual Outbound NAT rule generation.(AON - Advanced Outbound NAT)
- Disable Outbound NAT rule generation.(No Outbound NAT rules)

3) Firewall Rules:

Firewall rules controls flow of traffic, it allows or block traffic. Firewall offers two default firewall rules known as inbound or outbound rules these rules can be edit and new firewall rules can be created. Navigate to *Firewall / Rules* it will lead to WAN rule-set that already contains rules for block private networks and block bogon networks. User can create new rule by clicking on edit field. Edit Firewall Rule(Action, Disable, Interface, Address Family and Protocol) Source, Destination and extra options(log and description). LAN and floating rules can be created and manage in a same way as WAN.

4) Schedules:

Schedules are created to activate a firewall rule on certain time. Schedules can be created under *Firewall / Schedules*.

5) Monitoring Network:

Firewall Logs-Firewalls have log feature that documents how the firewall handled various types of traffic.Logs containsinformation like source and destination IP addresses, port numbers, and protocols.

Fig. 3 Firewall Logs

RRD & Traffic Graph -RRD Graphs keeps track of various bits of data about how the system performs, and then stores this data in Round-Robin Database (RRD) files. Navigate to *Status / Monitoring* in order to monitor RRD Graph.

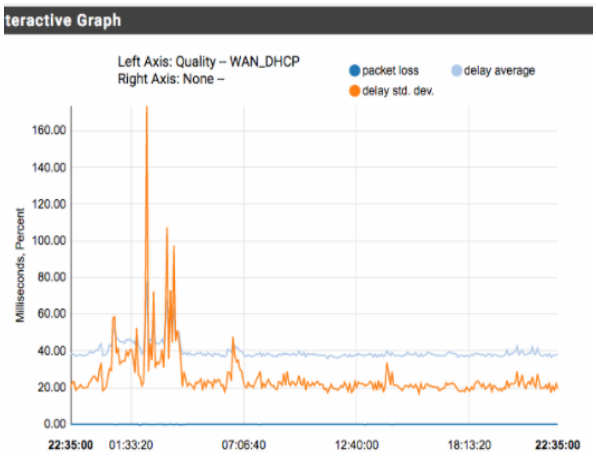

Fig. 4 RRD Graph

The traffic graph shows real-time information of all traffic flowing to and from a particular interface. It shows how much bandwidth is used by an interface.Traffic Graph helps in monitoring incoming

International Journal of Electrical Electronics & Computer Science Engineering
Special Issue - ICSCAAIT-2018 | E-ISSN : 2348-2273 | P-ISSN : 2454-1222
Available Online at www.ijeecse.com

and outgoing traffic. Traffic graph is available on status dashboard.

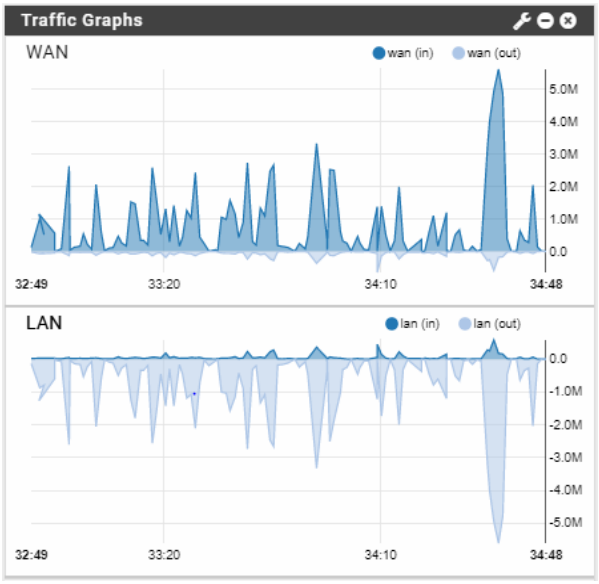

Fig. 5 Traffic Graph

B. Use of SquidGuard Proxy Filter:

SquidGuard is a URL redirector used to integrate blacklists with the Squid proxy software. Features of SquidGuard Proxy Filter

- Block access to URL or webserver that are blacklisted
- Block keywords
- Provides Blacklist and access control list feature
- Allows easy rule management for different users and provides flexibility such as blocking a list of websites for a group of hosts and allowing full network access to other host group.

Navigate to *System / Package Manager / Available Packages* and install SquidGuard Proxy Filter Package.

Browse to *Services / SquidGuard Proxy Filter* for controlling and configuring General Settings, ACL, Target Categories, Blacklist and Log etc.

Steps to configure SquidGuard Proxy Filter

- Open General settings tab, enable general, blacklist options and save.
- Open Common ACL tab and set target rules list (it contains target categories and there access mode i.e. deny or allow). Enable do not allow IP-Addresses in URL (To make sure that people do not bypass the URL filter by simply using the IP-Addresses instead of the FQDN) and log.

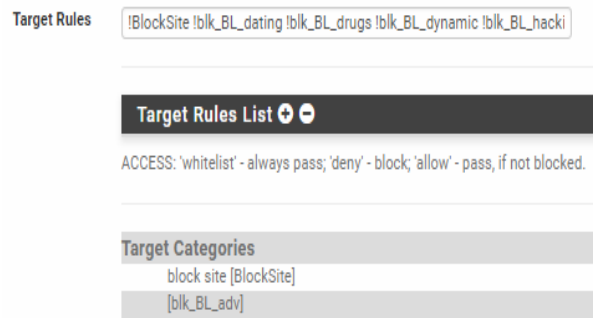

Fig. 6 Target Rules

Any blacklist archive file can also be used for updating user defined Blacklist under *Services / SquidGuard / Blacklists/*

Squid proxy sever provides real time log view of squid proxy traffic. It contains information of host IP, connection status, squid access logs and Destination address.

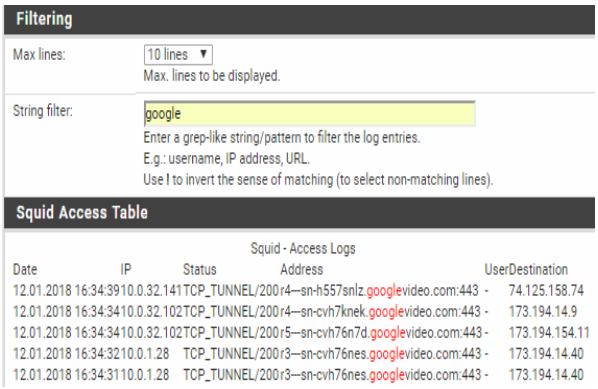

Fig. 7 Squid Proxy Real Time Logs

VIII. IMPLEMENTATION OF IDS

pfSense does not have its own IDS feature but it has package system using that other software packages can be integrated with pfSense. It uses Snort package for using IDS Services.

Snort provides IDS/IPS services. It is used for blocking and creating log information of ongoing network activity. In order to install snort on pfSense, user can locate it under *System/ Package Manager / Available package*. Search for snort and hit Install button, it will install after confirmation.

After installation user can manage snort services under *Services / Snort.*

According to pfSense documentation Snort offers VRT Rules, GPLv2 Community Rules, Emerging Threats Open Rule, Emerging Threat Pro Rules and OpenAppID Open detectors and rules for application detection. Snort VRT Rules requires paid subscription but user can also register for 30days trial. GPLv2 Community Rules and Emerging Threat Open Rule are available for free.

International Journal of Electrical Electronics & Computer Science Engineering
Special Issue - ICSCAAIT-2018 | E-ISSN : 2348-2273 | P-ISSN : 2454-1222
Available Online at www.ijeecse.com

In order to use Snort Services, user must configure the package.

1) Global Settings:

Global Settings let user choose IDS package rules, Navigate to *Services / Snort / Global Settings*

User must enable one IDS rule and set update interval, update interval is a timer that is used for checking either the package is up to date or not.

2) Snort Interfaces:

Navigate to*Services / Snort / Snort Interfaces*.Click Add button to Add an interface for implementing Snort service, this will lead to a new setting tab there user can choose an interface.

Once interface is added, user can set policies in Categories Tab under *Services / Snort / Snort Interfaces / Categories*. VRT provides three preconfigured IPS policies (Connectivity, Balanced, and Security) that makes implementation easies for user. Interface Rules can be managed under *Services / Snort / Snort Interfaces / Rules*.

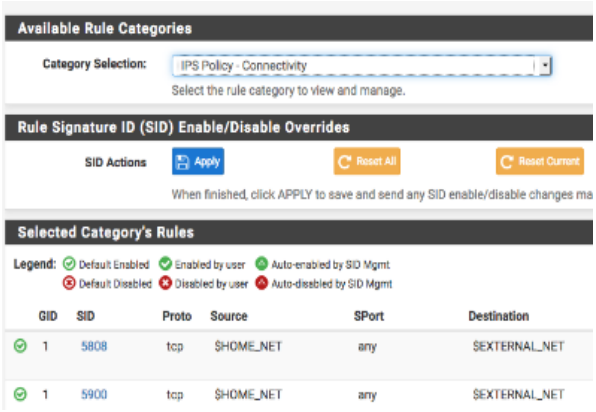

Fig. 8 Snort Rules

3) Updates:

Update Tab is useful for managing updates. It contains rules information like md5 signature hash and md5 signature date. It shows last update detail, user can update rule or force an update for downloading and enabling the rule package. User can also view or clear rule log. Path to Update Tab is *Services / Snort / Updates*.

4) Alerts:

Alert Tab contains Alert Log View Settings, Alert Log View Filter and Last Alert Log Entries. Alerts provides notification services for any faulty network events. User can limit the no. of log entries and can download or view the alert log at any time. Path to Alerts Tab is *Services / Snort / Alerts*.

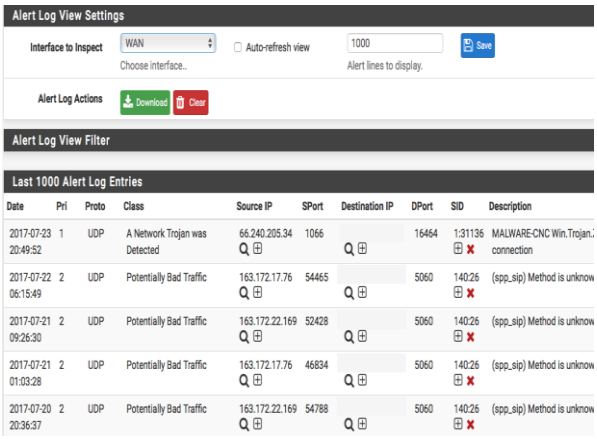

Fig. 9 Snort Alerts

5) Blocked:

Blocked Tab is used for blocking a logical address that admin does not want to allow network access. Path to Blocked Tab is *Services / Snort / Blocked*.

6) Pass List:

Pass List functions similarly as white List. It contains list of IP addresses that should not be blocked by the IDS. Navigate to *Services / Snort / Pass Lists*

User can create pass list by clicking on Add button. Pass List Edit Tab contains General Information (Name, Description), Auto Generated IP Addresses and Custom IP Addresses.

IX. CONCLUSIONS

This paper describes network security issues and how to resolve them. No network is completely secured, as the attacks are getting complex the security systems are also developing. Many different kinds of techniques are developed to detect the security issues so that we can prevent our system from all kind of attacks. In this paper I have suggested a number of network security optimization techniques that will serve to improve the quality of experience for Internet users, network security and how to implement Firewall and Intrusion Detection System. Firewalls control both incoming and outgoing network traffic. They can allow certain packets to pass through or else disable access for them. But an organisation cannot completely rely on a firewall and no protection system could make a network completely secure against attacks. If network security is breached, then it should be reported to the administrator so that necessary actions can be taken. IDS/IPS helps in parallel with firewall in order to improve network security.pfSense is one of the emerging open source platform that provides all of these services. Its installation and configuration is simple and cost effective. It is highly recommended for small and medium enterprises as it provides broad list of services, maintains network integrity and security at very less cost.

X. REFERENCES

[1] Binh Nguyen Network Security and Firewall, Helsinki Metropolia of Applied Sciences

[2] Vacca JR. Practical Internet security. USA: Springer; 2007

[3] Whitaker A, Newman D. Penetration Testing and Network Defense. Indianapolis: Cisco Press; 2006

[4] Helman, P., Liepins, G., Richards, W.: Foundations of Intrusion Detection. In: Proceedings of the IEEE Computer Security Foundations Workshop V (1992)

[5] Denning, D.: An Intrusion-Detection Model. IEEE Transactions on Software Engineering 13(2), 118-131 (1986)

[6] Young, C.: Taxonomy of Computer Virus Defense Mechanisms. In: The 10th National Computer Security Conference Proceedings (1987)

[7] Network Security First-Step: Firewalls - Donald Stoddard, Thomas M. Thomas.

[8] ISS Internet Risk Impact Summary - June 2002.

[9] JanneAnttila", Intrusion Detection in Critical Ebusiness Environment ", Presentation, 2004.

[10] Implementing a Distributed Firewall-Sotiris Loannidis, AngelosD.Keromytis, Steve M. Bellovin, Jonathan M. Smith.

[11] Kizza JM. Computer Network Security. New York: Springer Science+Business Media Inc; 2005

[12] A Review paper on pfsense – an Open source firewall introducing with different capabilities & customizationIJARIIE-ISSN(O)-2395-4396

[13] Setup Snort Package from pfSense Documentation; 18 November 2017

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

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

[16] Mamat, K, Ruzana MohamadSaad; "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.