Bachelor's Thesis (UAS)

Degree Programme in Information Technology

Internet Technology

2015

Amit Thakur

OPEN SOURCE FIREWALL IMPLEMENTATION

– Replacing traditional firewall with open source

TURUN AMMATTIKORKEAKOULU
TURKU UNIVERSITY OF APPLIED SCIENCES

BACHELOR'S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Degree Programme in Information Technology | Internet Technology

2015 | 35

Instructor: Tero Virtanen

Amit Thakur

OPEN SOURCE FIREWALL IMPLEMENTATION

– Replacing traditional firewall with open source

The prime focus of thesis is to substitute a real life solution of a router-based firewall with an open source solution having an easy, manageable, and centralized GUI and integrated built-in network extensions. The thesis compares three popular open source firewalls, namely Untangle, pfSense and Zeroshell, in order to meet security requirements. These three firewalls were installed in a VMware environment and tested for installation, stability, built-in components, security level, GUI interface administration, and resource consumption.

In conclusion, among the three mentioned firewalls, pfSense was found to be a financially effective solution because of its easy upgradability, simple web configurator, and its wide range of extension and features.

KEYWORDS:

centralized, open source, VMware, pfSense, Zeroshell, Untangle, GUI

CONTENTS

LIST OF FIGURES AND TABLES

LIST OF ABBREVIATIONS (OR) SYMBOLS

CLI	Command Line Interface
DHCP/DNS	Dynamic host configuration protocol / Domain name service
Distro	Distribution
E.g.	Example
ESXi	VMware vSphere Hypervisor
GUI	Graphical user interface
IDS/IPS	Intrusion Detection System / Intrusion Prevention System
IP	Internet Protocol
LAN/WAN	LocaL Area Network / Wide Area Network
m/r:	minimum/recommended
OSI	Open System Interconnection
TCP	Transport control protocol
UDP	User Datagram Protocol
TLS	Transport layer security
SSL	Secure socket layer
SSH	Secured shell
VPN	Virtual private network

1 INTRODUCTION

A network is defined as digital components linked in a single frame govern with a common set of rules. In the past, networks were quite easy to manage and secure. Increasing complexities in the network at community as well as enterprise level have raised questions of security. Here, users from different platforms, with different intentions, behaviors and objectives show up. Few could be normal users while others watch for network breaches to take advantage of. This led the IT specialists to work on two major issues: first to protect personal data of legitimate users and second to secure browsing interfaces for users. No protocols, software, hardware or tools can ensure 100% safety in any network. However, routers are deployed with a long list of commands and complicated configurations, aid security with configured access list, static routes, interface and login time expiry as well as VPN. Implementing new security feature on network adds extra software and tools on each additional requirement, consuming more money, time and labor.

In the practical work of this thesis, a VMware ESXi server was setup in an environment of two virtual switches and virtual desktops where open source firewalls were installed with their respective ISO uploaded to the datastore of server. Later, the server was tested for stability and reliability.

This thesis is organized in the following chapters:

Chapter 1 describes the goals of the thesis along with methodologies adopted to achieve the objectives.

Chapter 2 explains the theoretical background, elaborating a detailed overview of firewalls, their categories, firewall operational/structural methodologies and various threats and attacks.

Chapter 3 describes the practical installation and testing of the selected open source firewalls in the VMware environment. It also mentions features and drawbacks of firewalls namely Untangle, pfSense and Zeroshell.

Chapter 4 concludes the thesis with explanation of final version among three firewalls. It also explains how could free software solves the problems of enterprises as well as well as small companies.

2 FIREWALLS

Commercial business starts switching to emerging technologies such as service oriented architecture i.e. collection of services communicating with each other either using cloud computing for a sustained revenue model. Ensured round the clock uninterrupted service to the client, therefore, becomes a top priority to any organization. To accomplish this, a network needs to be secured with firewall, thus becoming an unavoidable component in network.

2.1 Concept and origin of firewall

In the past, the term ‘firewall’ referred to a blocking point between any two compartments, blocks or access points to prevent the spread of fire (Reference Dictionary 2015). The purpose of a firewall in the digital world is to provide a safe junction in order to minimize unauthorized access. Therefore, Digital Equipment Corporation (DEC) first came up with the concept of the firewall , in the late 1980s when networks were separated with routers. These devices were applied on popular and much practical lower four layers of the OSI model, i.e., Physical Layer, Data Link Layer, Network Layer and Transport Layer. The routers were defined according to IP-addresses, inspecting incoming traffic as well as outgoing traffic. The source and destination IP-address of each packet were assessed along with port numbers to acquire an entry token. The following incidents describe the chronological evolution of the firewall in the early 1980s and 1990s: (Firewall Wikipedia 2015)

- Clifford Stoll found German spies tampering with Stoll’s system
- The Morris worm, the first known large scale attack ,Although it was not malicious, had properties of propagation and affected 6000 - 60000 PCs
- In 1992, Electronic jail, designed by Bill Cheswick, was set up to observe an attacker as explained in his book “An Evening with Berferd”.

Figure 1 illustrates the timeline of firewall evolution.(PCI HISPANO 2014)

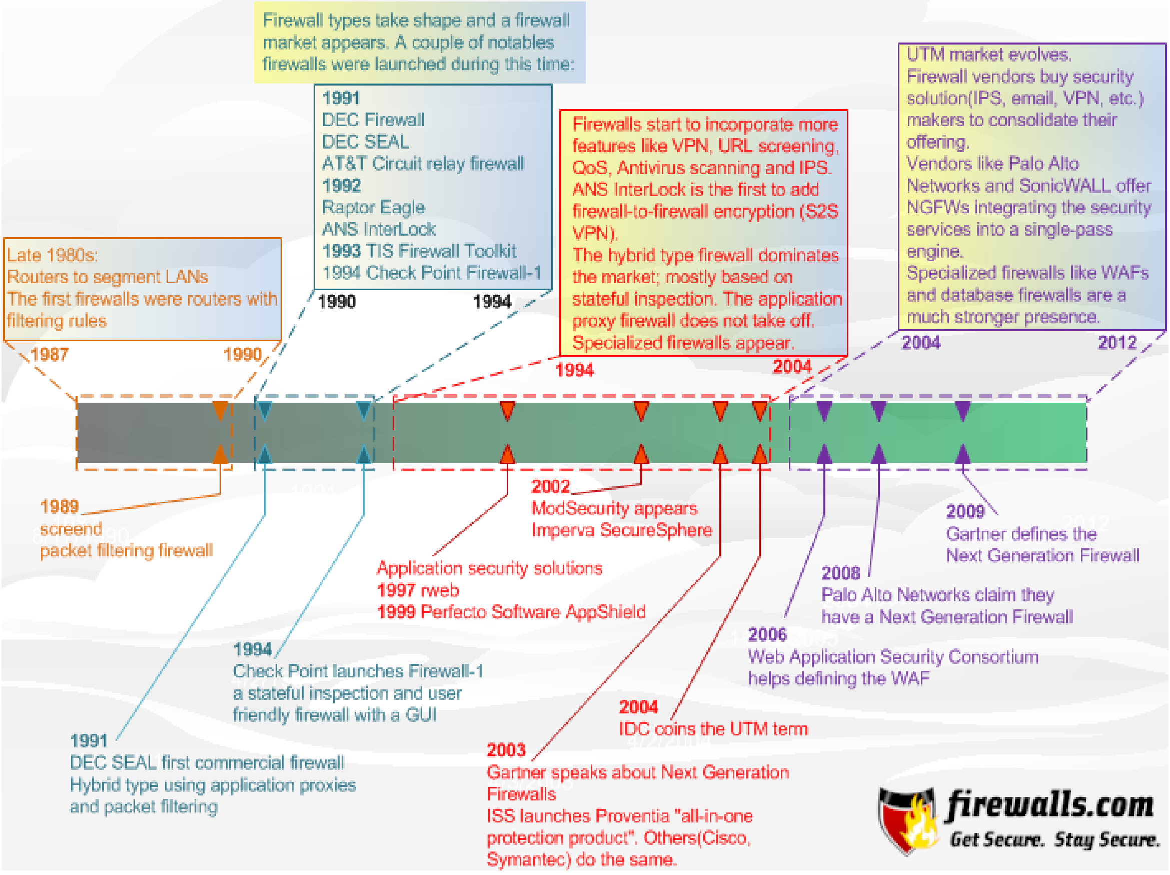

Firewall types take shape and a firewall market appears. A couple of notables firewalls were launched during this time:
1991
DEC Firewall
DEC SEAL
AT&T Circuit relay firewall
1992
Raptor Eagle
ANS InterLock
1993 TIS Firewall Toolkit
1994 Check Point Firewall-1
1990
1994
Late 1980s:
Routers to segment LANs
The first firewalls were routers with filtering rules
1987
1990
Firewalls start to incorporate more features like VPN, URL screening, QoS, Antivirus scanning and IPS. ANS InterLock is the first to add firewall-to-firewall encryption (S2S VPN).
The hybrid type firewall dominates the market; mostly based on stateful inspection. The application proxy firewall does not take off.
Specialized firewalls appear.
1994
2004
UTM market evolves.
Firewall vendors buy security solution(IPS, email, VPN, etc.) makers to consolidate their offering.
Vendors like Palo Alto Networks and SonicWALL offer NGFWs integrating the security services into a single-pass engine.
Specialized firewalls like WAFs and database firewalls are a much stronger presence.
2004
2012
1989
screend
packet filtering firewall
2002
ModSecurity appears
Imperva SecureSphere
Application security solutions
1997 rweb
1999 Perfecto Software AppShield
2009
Gartner defines the Next Generation Firewall
2008
Palo Alto Networks claim they have a Next Generation Firewall
2006
Web Application Security Consortium helps defining the WAF
1994
Check Point launches Firewall-1 a stateful inspection and user friendly firewall with a GUI
2004
IDC coins the UTM term
1991
DEC SEAL first commercial firewall
Hybrid type using application proxies and packet filtering
2003
Gartner speaks about Next Generation Firewalls
ISS launches Proventia "all-in-one protection product". Others(Cisco, Symantec) do the same.
firewalls.com
Get Secure. Stay Secure.

Figure 1. Firewall evolution timeline

There has been a wide range of firewall evolution from the beginning of the 1980s as shown in figure 1 until now. In 1980s, firewall was introduced with basic routing function, but later in 1991 it started to act as security seal as commercially produced by major companies like DEC. Era of 1994 to 2004 was major invention for features like VPN, URL screening, QoS and IPS. These features were mainly invented to improve firewall as a complete product.

2.2 Types of Firewalls

A firewall is an essential component in the network to guard against unauthenticated access to a networked computer system. Intruders are supposed to be blocked with the defined rules depending on the need of an enterprise network.

A firewall could be hardware or software installed at transition places in order to watch and alarm for incoming new risks, as well as help to monitor in order to hinder future risks. Firewalls have been categorized into following as mentioned below:

- Packet filtering firewalls
- Application level firewalls
- Hybrid firewalls

a. Packet filtering firewalls

Packet filtering firewalls are also known as traditional firewalls which evaluate packets based on the list of rules for IP-addresses and port numbers. Packets assigned with authorised IP-address and/or port numbers pass the transition point while others are rejected and dropped. The governing rules vary depending on the type of enterprise whether it is small company or multi-branch commercial enterprise, requirements like whether firewall needs to inspect traffic or need to provide VPN connection for staff users. Packet filtering has advantages like low cost and low constraints in performance, as well as complicated and more secure access policy. Packet filtering firewall inspection is illustrated in Figure 2.

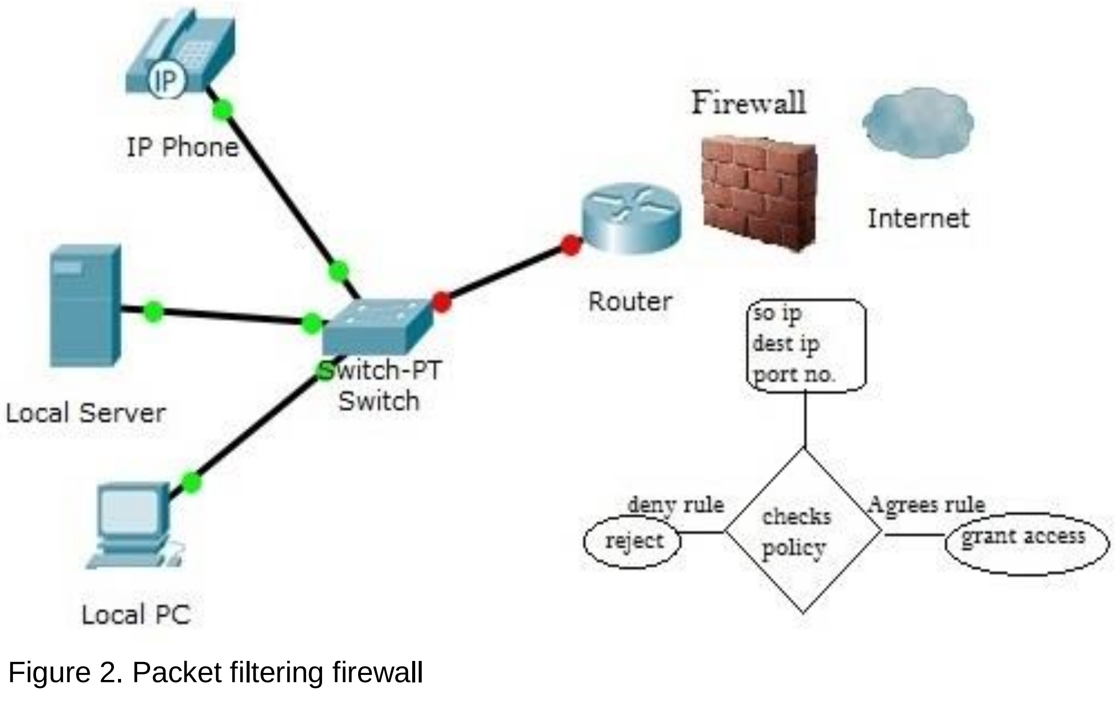


Figure 2. Packet filtering firewall

In Figure 2, Incoming packets are checked against policy which varies as per the consequences, and access is decided as per match or mismatch of policy rules.

The policy is designed based on port number and source/destination IP-address, which is evaluated every time a packet passes the firewall.

b. Application level firewalls

Application firewall is also known as proxy firewall depending on the use of it. This firewall operates at application layer of OSI model and is also known as stateful inspection firewall. This firewall is considered more practical and secure in user networks since programs and applications could be filtered on the application layer of the OSI model, even log of the traffic is tracked. This is sometimes referred to as a proxy firewall because it acts as a mediator between request and response.

Whenever there is request of connection for the server inside intranet, the mediator, i.e., proxy, checks for authorization and malicious activities, followed by opening a connection to the server. One major problem in the network could be delay and blockage of minor services and processes, thus targeted by hackers through security flaw. The application firewall is shown in Figure 3.

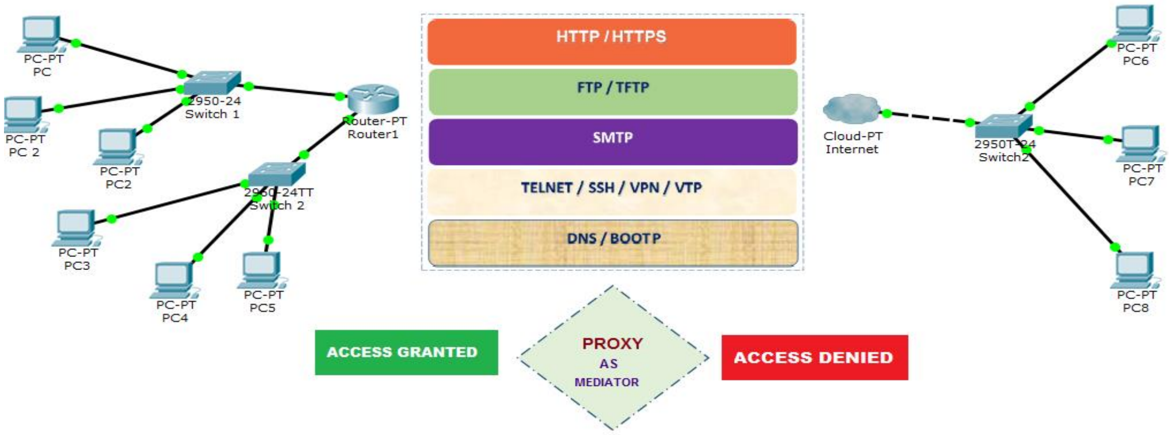


Figure 3. Application Firewall

Various application layer protocols, like World Wide Web (HTTP/HTTPS), file transfer (FTP/TFTP), mail (SMTP), remote connection (TELNET, SSH, VPN, VTP), domain service (DNS) and BOOTP gain access through the application layer of the OSI model.

Since application firewalls operate at the application layer, the application layer acquires full control on the flow of traffic.

c. Hybrid firewalls

Hybrid firewalls are also known as Next-generation firewalls. Major commercially produced firewalls have been developed to integrate the function of previously mentioned firewalls so that security could be enhanced. This minimizes risk of threat and improves performance of network. That is how concept of a hybrid firewall is introduced. It can be compared to a smartphone which integrates the functions of devices like a phone, a camera, a music player and many more.

It is possible to have built-in functions which act as:

- URL and DNS filtering
- Deep packet inspection
- Intrusion prevention/detection system
- Application Inspection and control
- SSH / SSL auditing
- QoS and bandwidth management
- VPN traffic recognition

2.3 Firewall protocols and methodologies

Firewalls, nowadays, are modified with built-in features for network requirements. Systems are configured with graphical interface administration to avoid multi-line command entries. CLI is more useful for scripting.

With customizable filtering options available for firewalls, organisations and individual customers could enable or disable the features depending on the complexity and requirements of the web traffic.

2.4 Internet threats and attacks

Most configured networks are more likely to have weak points that could be technological, configurational as well as security policy (Laorden et al. 2010). With lapse of time, qualified and technically competent network intruders exploit these weak points, using malicious codes and scripts.

Improvement in the information technology have generated numerous tools and scripts to exploit networks in order to breach and take advantage of it. Details about the progress of network attacks are explained in section 2.4.1

2.4.1 Network threats and attack examples

Before explaining the wide range of internet threats, it is essential to clarify that threats are not the same as vulnerabilities. Threats take advantage of vulnerabilities, i.e., intrusion holes to cause serious issues and crashes. Figure 4 illustrates various threats responsible for potential consequences.

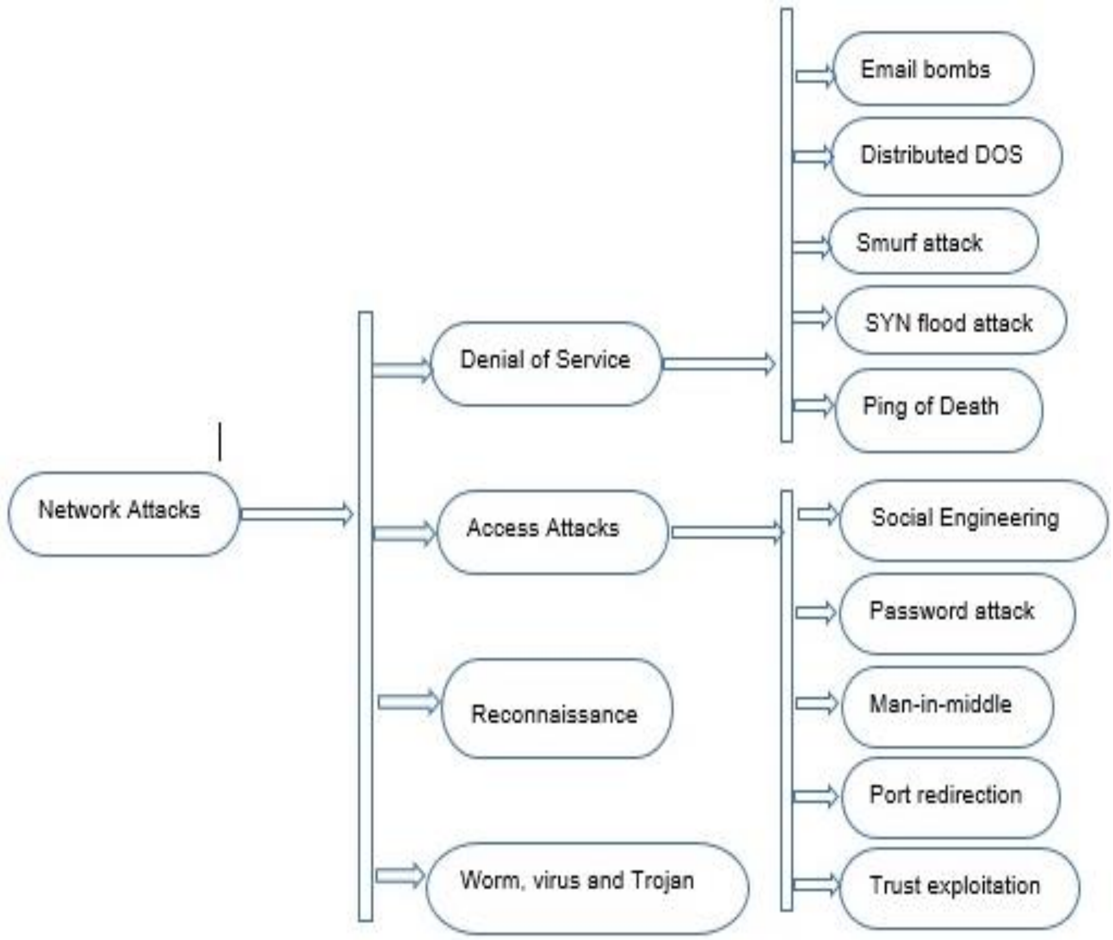


Figure 4. Different Network Attack Types

Figure 4 displays four major attacks i.e. DDOS, access attacks, reconnaissance and the last one worms and virus. Denial of Service could be in forms like Email bombs, DDOS, Smurf attack, Ping of death, all of these result to the crash of normal services. Social engineering is a kind of access attacks in which attackers try to gain potential information through different social techniques. These are explained in details later in this chapter.

According to the National Institute of Standards and Technology (NIST 2010), vulnerabilities refer to the weak and unaddressed points in the network which could be in devices or applications where attackers install malware to crash, exploit the targeted network.

Till date, various evidences of network attacks have been reported, which somehow affect performance, legitimacy, privacy, finances of organizations and individuals. Some of them are explained below:

- Denial of service (DoS as abbreviation)

The term itself explains the blockage of normal service operation in network. The intruder hacks the system using potential script and tools. This results in faulty network operations as well as disrupted network access by authorized users which results in unresponsiveness (Laorden et al. 2010).

- Access attacks

Someone with no identification and authentication in network, gains access to a network and with use of hacking script and codes, affect the systems, thus incurring poor performance, even on serious level, damaging the components and blocking regular traffic to operate (Laorden et al. 2010).

On whole, the network stops working. These activities are known as access attacks. They are of various types: Man-in-middle attacks, social engineering, port redirection, trust exploitation, phishing etc.

- Reconnaissance

Network intruders gather information about vulnerable devices and track common activities through available tools, such as nslookup and whois. This is called reconnaissance. It consists of attacks like packet sniffers, ping sweeps, Internet information queries and port scans (Laorden et al .2010).

Reconnaissance occurs as follows:

— Hackers first determine the existing network with ping sweeps.

— The port scanner technique is used to identify port numbers active on the network

- Port queries are employed to gain information about application details, version, operating system installed, number of hops to reach destination network.
- The most important and last step is to discover if any vulnerability exists in the system in order to exploit.

- Eavesdropping

Eavesdropping is a popular method of reconnaissance, achieved with tools like network snooping and packet sniffing (Laorden et al. 2010).

- Dumpster diving

A hacker gains personal and valuable information utilizing organization trash in a process of social engineering. This is known as Dumpster diving (Preetham. 2002, 40).

- Trojan, viruses and worms

Innumerable services, tools and scripts are developed by hacker communities to gain access to legitimate circle of users in order to steal private or sensitive data, affect the recovery and destruct the backbone of network architecture. In the past, it was dangerous but now this type of attack could target whole the globe within very little time. These attacks are categorized in three different forms, namely, Trojan, viruses and worms based on their nature of effect, replication and attack. Trojan refers to the malicious application which modifies data which has not been authorized. Similarly, a virus is self-replicable malicious program which affects hard disk space, CPU function as well as hard disk boot sector. A worm is also self-replicable but it depends on security failure to gain access inside computer or networks. (Laorden et al. 2010)

2.4.2 Effect and preventive measures

A survey carried out by Neustar in 2013 states that 60 percent of companies were DDoS- attacked, up from 35 percent experiencing a disruptive attack in 2012. With nearly twice as many targets, 2013 was a busy year for attackers (Neustar Annual DDoS Attacks and Impact Report 2014). Less exposure to security awareness and underestimating the ability of hackers have always put the network availability and confidential information at risk.

Most of these attacks, not only target particular departments, systems, or networks but also makes them intermediary to forward the risk of attack.

Shack News reported that a hacking community known as Lizard Squad has claimed responsibility for attacks on the PlayStation Network (PSN), Blizzard's Battle.net, Riot's League of Legends, and Grinding Gear Games' Path of Exile. (PSN 2014)

The President of Sony Online Entertainment John Smedley confirmed the news on Twitter.

"*We are under attack by a large scale ddos. Being dealt with but it will impact games until it's handled*."

— John Smedley (@j_smedley) August 24, 2014

(PSN 2014)

As per confirmation from the same group, gaming consoles provided by Microsoft and Sony were compromised through DDOS attack and took time to get them back online. The operating system in the majority of the systems are Microsoft Windows, Unix-based, Linux or Macintosh OS X. These systems use the TCP/IP protocol suite to integrate services, exchange information, update logs and audit trails. These operating systems have weak trails which are exploited by attackers to gain access which results in IP spoofing and TCP connection requests, i.e. SYN attacks.

The following are considered as consequence and effect of these system threats:

- Network-based attacks primarily focus on commercial and business platforms. Interruption in regular traffic harms daily business operations.
- Today business giants, like Microsoft and Sony, have to face damage of reputation and confidence from the customers. More likely, they have tried to re-gain trust and confidence by offering extended membership service and discounts. This might have helped up to a certain extent, but has annoyed customers who search for alternatives. Plenty of incidents over the years report that one of the prime reason of cyber-attacks is theft of information where terabytes of information is stolen and exploited to damage business reputation and operation.

- DDOS breaches in Sony Pictures have resulted in the theft of 100 terabytes of information, including budgets, payroll data, internal emails, feature files, financial information and also leaked these to public file-sharing sites such as PasteBin (Dawb C, Arik H. 2014).

No device, application, software, security policy or system administrator guarantees complete protection and security since various factors affect the guarding of the network and devices. Different tools, guides and practices are available from security vendors and suppliers. For example, Auto secure and Cisco output Interpreter from Cisco, Antiviruses, Firewall, IDS and IPS could be implemented with updated security policies (Laorden et al. 2010).

3 OPEN SOURCE FIREWALL DISTRIBUTIONS

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. These distributions are gaining popularity for their point and click interface and appeal to user community as cool gadgets with multi-platform functionality.

3.1 Distributions and Squid

Open source is often misunderstood as something that is available free of cost. Open source is something that is publicly accessible and possible to modify (Open Source 2015). In software development, open source software is a computer software whose source code is made available from the developer with open license, providing rights and obligations to manipulate or improvised and redistribute as per the need of project, having full control of it. That does not mean that it is free of cost, but rather that it is available. Since programmers who modify and sell software, provide technical support, implies that they could charge for it.

Thus, open source firewall distribution refers to similar security software available from developers with GPL v1 or v2 license, integrated with security utilities and tools designed to filter and inspect stateful packets and application layer protocols like HTTP, FTP and SMTP. Additionally, it extends to VPN, SSL and IPsec functionality. Countless firewall distributions are in use as the result of this emerging security solution. Most of them include a web proxy known as “Squid”. It helps in various ways like content filtering as well as traffic filtering. The idea of Squid generated with the concept of improving user experience by saving bandwidth from ISPs as well as scaling commercial websites without upgrading hardware. Exponential growth appears in deploying Squid in enterprise and small-scale websites.

Major commercial firewalls are offered GPLv2 for initial configuration with main security features enabled. Few might require monthly or annual subscription fee to get all features enabled.

List of firewalls available with open source license are listed below: (Distrowatch.com 2015)

- FreeBSD
- ZeroShell
- pfSense
- IPCop Firewall
- Sophos UTM
- Vyos
- Alpine Linux
- IPFire
- ClearOs
- VyOs
- FreeBSD
- ClearOS
- UntangleNG Firewall
- Devil-Linux

Besides content filtering, packet inspection and traffic assess, these firewalls are also responsible for bandwidth optimization. On a broad scale, a fully featured HTTP proxy embedded with logging environment, providing authorization and rich access control was a need in web proxy scenarios.

Popular firewalls use Squid as a proxy appliance which aids in web content filtering, security management and dynamic web activity analysis. Some of them using this proxy include Smooth wall, azeti-C, Endian Firewall, Simple Wall, Smooth Wall Guardian and pfSense. Moreover, Squid also supports HTTPS, FTP and a huge number of web protocols like SSL, TLS and many more.

3.2 Features of three open source firewalls

Firewalls and their application and features range from simple to sophisticated enterprise level. A software based solution provides safety against different intrusion implementing VPNs through tunnel mode and also serves as a platform for IPsec.

The following firewalls have been considered to compare their features, limitations and application in real environment, as part of this thesis.

1. Untangle

Untangle Unified threat management (UTM) is an OSI layer 7 application layer firewall which filters traffic based on IP-address, port number, protocol, most significantly Active Directory users and groups.

UTM is a popular commercial-grade open source complete Linux solution with built-in openVPN. It can be upgraded on hardware at a small cost. Provided with graphical interface for configuration and administration, UTM is an open source distribution with less downtime, live backup features along with zero stress of installation and configuration. Within less than 4 minutes, most of the extensions can be activated using normal resource consumption. Since configuration is done with GUI, it is quite simple to install with a clicky interface with no technical knowledge of CLI.

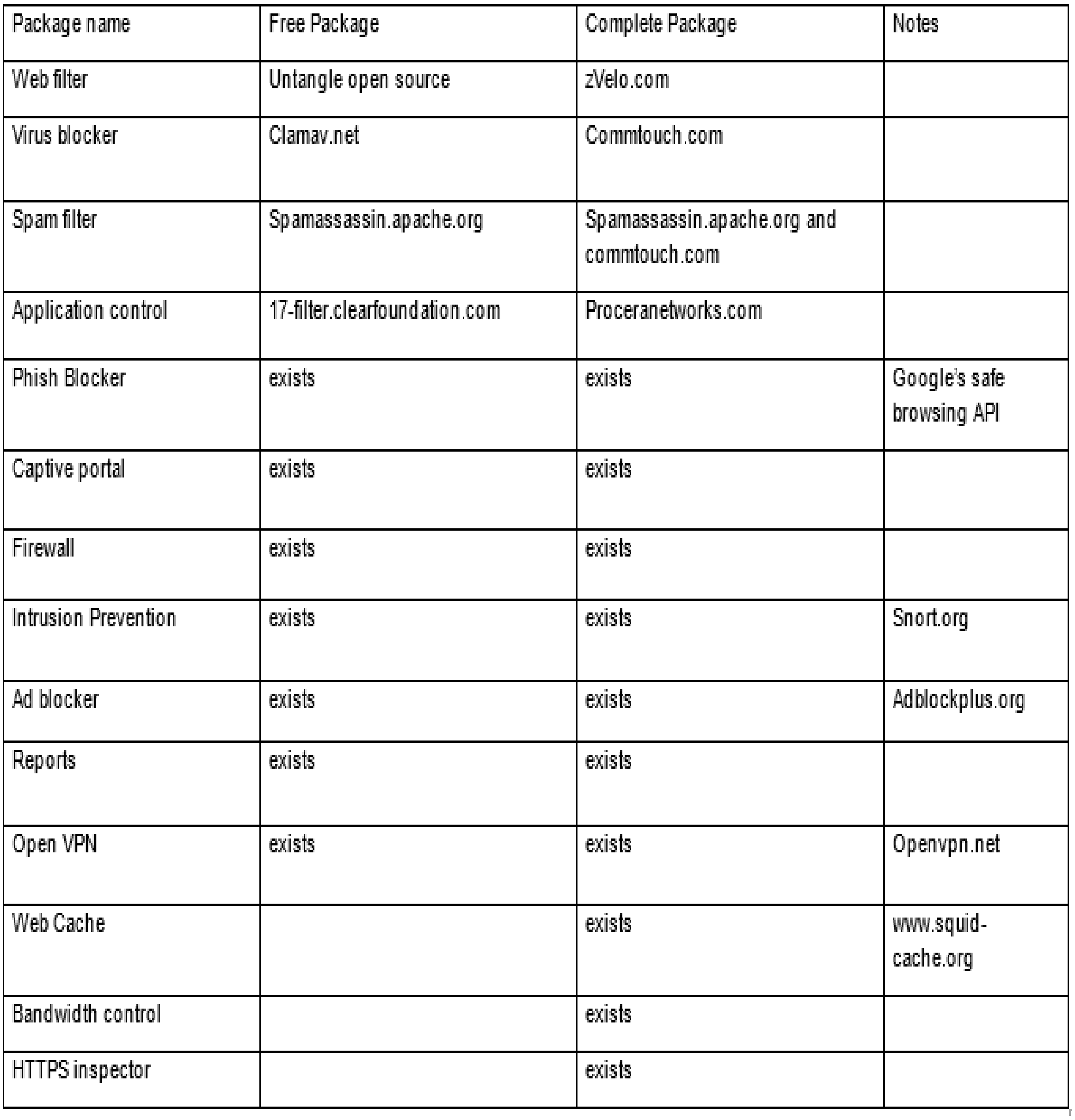
UTM supports a wide range of network applications with less resources and improved bandwidth. Apart from this, it provides modules to integrate the following network solutions:

- Firewall: UTM examines the flowing traffic at the transport layer of the OSI model and secure granting access token to the legitimate network only
- Protocol Control: Untangle has an improved version of protocol control which extends the feature to control protocol and shut down the ports if violation occurs. For example: Protocols of Skype follow similar principle.
- Attack, phish, virus, spam and spyware, malware blocker: Based on open source CalmAV, Spam Assassinblocks phish, virus and spam respectively. This prevents Distributed denial of service (DDoS) attacks and other attacks by blocking unspecified hosts, and also guards from various threats.
- OpenVPN: Users access the internet from a remote network securely with VPN provided with Untangle. It also administers protected distribution of software and encryption keys.

  In addition to these mentioned applications, Untangle supports diverse services:
- Configuration backup: It is available in the paid version and automatically backups NGFW to the cloud.

Policy Manager: This service is integrated only in paid version of Untangle.

Table 1. Services offered in different Untangle versions



Package name	Free Package	Complete Package	Notes
Web filter	Untangle open source	zVelo.com	
Virus blocker	Clamav.net	Commtouch.com	
Spam filter	Spamassassin.apache.org	Spamassassin.apache.org and commtouch.com	
Application control	17-filter.clearfoundation.com	Proceranetworks.com	
Phish Blocker	exists	exists	Google's safe browsing API
Captive portal	exists	exists	
Firewall	exists	exists	
Intrusion Prevention	exists	exists	Snort.org
Ad blocker	exists	exists	Adblockplus.org
Reports	exists	exists	
Open VPN	exists	exists	Openvpn.net
Web Cache		exists	www.squid-cache.org
Bandwidth control		exists	
HTTPS inspector		exists	

Table 1 provides information regarding packages and extension available with the Untangle released version. The free version published under public GPL and commercial version are two different releases from the official Untangle. Few services are restricted to the paid version although the majority of services and applications are accessible on the public version.

2. pfSense

pfSense is a robust firewall distribution based on the m0n0wall project. It has a web-based GUI configurator, scalable for flexible firewalling and routing with added choke for potential vulnerabilities. This firewall is easy to use for persons withoutknowledge of FreeBSD.

From the time of invention of this project, it has been considered a practical and useful solution from home networks to enterprises. The FreeBSD-based system operates at the application layer of the OSI model, supports VLAN trunking, embeds package like Asterisk for a PBX server. Above all, it is considered as the most secure because of control over the list of concurrent traffic as well as with the use of dynamic DNS services because it allows for remote desktop through dynamic IP-address.

The integrated graphical web-based configurator is a powerful interface which lets administrators configure advanced setups. It is always extensible through packages as per enterprise or individual requirement although this requires high level of customization. Some of the features describing pfSense integrity include:

- pfSense is an open source security solution without licensing fees, thus, considered as cost-effective and inexpensive network solution.
- Software upgrades are free as well.
- Since the product is FreeBSD-based, it is highly popular for its security solution, customizability and even installation is fairly easy.
- The web-based graphical interface along with the built-in command prompt provides a handy tool for configuration and administration.
- Various network supplement like failover, VPN with fast speed, NAT, DNS forwarder, port forwarding features work exceptionally efficiently.

3. Zeroshell

Linux-based Firewall solution, Zeroshell was released under GPLv2 and was created by Italian Fulvio Ricciardi. It requires a LAN to provide its security solution over the network. It does not necessarily have to be installed on hard disk, rather it works from a CDROM via which it is distributed. Thus, Zeroshell is a Live CD distribution although configuration data and setting stored in database stay on ATA, SATA, SCSI or USB. It can be obtained in two forms, either as Live CD or compact USB image.

It operates on LAN from small to large-scaled networks and acts as router, authentication server, wireless access point, VPN and many more.

Zeroshell features include:

- Deep packet inspection operates at layer 7, i.e., the application layer, ensuring security and network flow through adjusted bandwidth and priority.
- Features like packet filter, stateful packet inspection apply filters in both routing and bridging on all networks i.e. VPN, LAN, WAN, SSL etc.
- It operates through two modes: first bridge mode and router mode. It is possible to configure RIPv2 in addition to adding static routes. Regardless of configuration, it could be strengthened with modification of NAT (PNAT) through a virtual server tab.
- Network troubleshooting utilities, like ARP check, Ping, Trace path, DNS lookup, are embedded with web interface to support network troubleshooting.
- Antivirus proxies such as havp act as protectors for client traffic, behaves as a transparent proxy in either bridge or router mode

Therefore, it is considered an all-in-one security/network product for replacing traditional router, being fairly easy to understand, use, maintain and upgrade.

3.3 Installation of the three firewalls

Innumerable security breaches take place due to poor network configuration and lack of secure network plan implemented without critical analysis. In addition to these, commercial platforms are usually targeted by hackers who explore vulnerabilities in software, configuration, or hardware. Most of the time, vulnerabilities remain the easiest way to enter inside network.

In response to this issue, a project to facilitate thesis work was created with the objective of implementing a firewall which could address following issues:

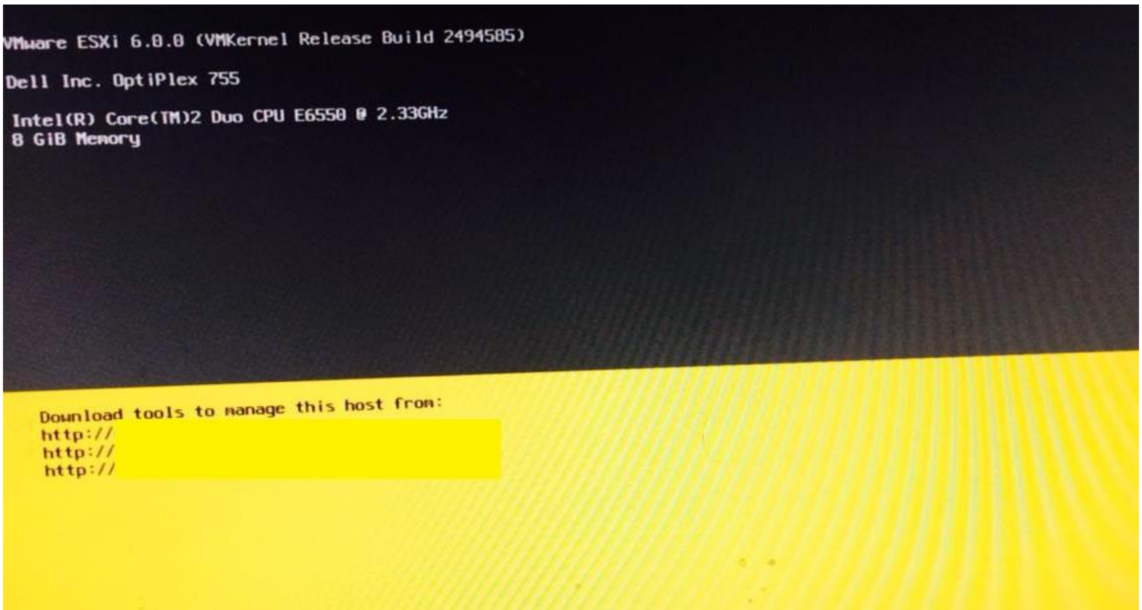
- It is free of cost
- It has an easily manageable administrative interface GUI
- It has multi-network functions, such as router, firewall, DHCP server
- It offers port forwarding, network address translation as well as DNS service
- It has an integrated built-in VPN
- It has future expansion of IPv6 support and 64 bit platforms.

Therefore, the three firewalls were tested through installation on a virtual network. This section presents the installation procedures and requirements for individual firewalls along with small overview of its tools and configuration.

Hardware and software employed for this project included :

- CPU: intel® Core™2 Duo CPU E6550 @ 2.33GHZ
- Hard disk HDD : Serial Attached ATA 2 X 160 GB = 320 GB (7200 RPM, Firmware : 4.ADA)
- Memory : 4 X 2GB = 8GB
- INTEL GIGABIT NIC
- HOST OS : VMware ESXi 6.0.0
- Remote Login Interface : VSphere client

It is easier to find a third party software which could convert ISO files into bootable USB. A software called YUMI was used in context of this project and the ISO image was downloaded from the official source and a bootable USB drive was created. Later, server system was formatted with Flash drive containing VMware ESXI 6.0.0 and within 12 minutes the VMware ESXI installation was complete as shown in Figure 5.



```
VMware ESXi 6.0.0 (VMKernel Release Build 2494585)

Dell Inc. OptiPlex 755

Intel(R) Core(TM)2 Duo CPU E6550 @ 2.33GHz
8 GiB Memory

Download tools to manage this host from:
http://
http://
http://
```

[redacted]

Figure 5. VMWare ESXi 6.0.0

In Figure 5, the VMware host interface is shown where the management IP address is visible, which could be used to gain access to it through a remote host.

After ESXi had come up, it acquired management IP-address via DHCP, which was later used for management and configuration. With login to the management IP-address from same network via desktop browser, it gained access to the VMware VSphere Client download page from where a remote login software called VSphere Client was downloaded and installed. It was a quite handy tool to give a secure remote connection to the server.

Since the testing environment was virtual, the following components were prepared for detailed installation and testing. Although system hardware was equipped with single physical NIC i.e. vmnic0, two virtual switches vswitch0 and vswitch1 were created. Virtual switch vswitch0 acted as a WAN Link port as well as Management Network and vswitch1 acted as an internal LAN.

Preferably, these two switches were configured. The same two switches were used as outbound and inbound interface for all three firewalls. Later, three selected firewalls were installed one after another as part of this thesis and at the end, one was considered the best suited firewall for the designated network. Two virtual desktops were also created, Windows Vista and Ubuntu (Linux OS), to perform testing and configuration. Windows Vista was deployed as vSwitch0 management OS while Linux OS as vswitch1.

Note: For each firewall installation, vswitch0 was used as WAN and vswitch1 was used as LAN link to verify the same working architecture.

Following three open source firewalls were installed in virtual environment and tested for their features and stability. Later, features and prices were compared.

1. Untangle

The Untangle firewall was installed as server gateway in network architecture to guard traffic, providing security, monitoring and control over the networks. It provides basic functions of routers and bridges, including security solution. It is a commercial firewall with potential security extensions.

Recommended (r) hardware requirements for the ISO boot of the Untangle server for 1 – 50 users are mentioned below: (Untangle.com 2015)

• CPU:	Atom/P4 equivalent or greater (r)
• Memory:	1GB (r)
• Hard drive:	80GB (r)
• Network cards:	2 or more

Besides these, a bootable ISO file was downloaded from the official page of Untangle i.e. https://www.Untangle.com/store/get-Untangle.

During this project, the ISO file was uploaded on server to get direct access from the datastore during installation. A new virtual machine called Untangle_pro was created to define two virtual switch ports for incoming (WAN) traffic (vswitch0) and outgoing (LAN) traffic (vswitch1). Installation was started with powering the connected virtual machine, which directs to the console. Within 10 seconds, the firewall started to reboot.

Once the virtual machine was alive, the GUI interface was accessed through the web browser with the Management IP-address. It was followed by a basic initial configuration like confirming incoming and outgoing interfaces, language changes, WAN source modification, LAN DHCP management and so on. The Untangle version used on this thesis was not commercially licensed, so it had limited features which the administrator could use after the initial registration.

Popular firewall applications, such as Web cache, Ad block, WAN balancer, DHCP, firewall, policy manager, HTTPS inspector, VPN and others become activated with initial activation. A few advanced features of the Application Lite version needs to be paid for to be activated.

Untangle was awarded InfoWorld's Best of Open Source Software Awards 2008 (Dineley D. 2008). Figure 6 is the web graphical interface for management of the Untangle firewall.

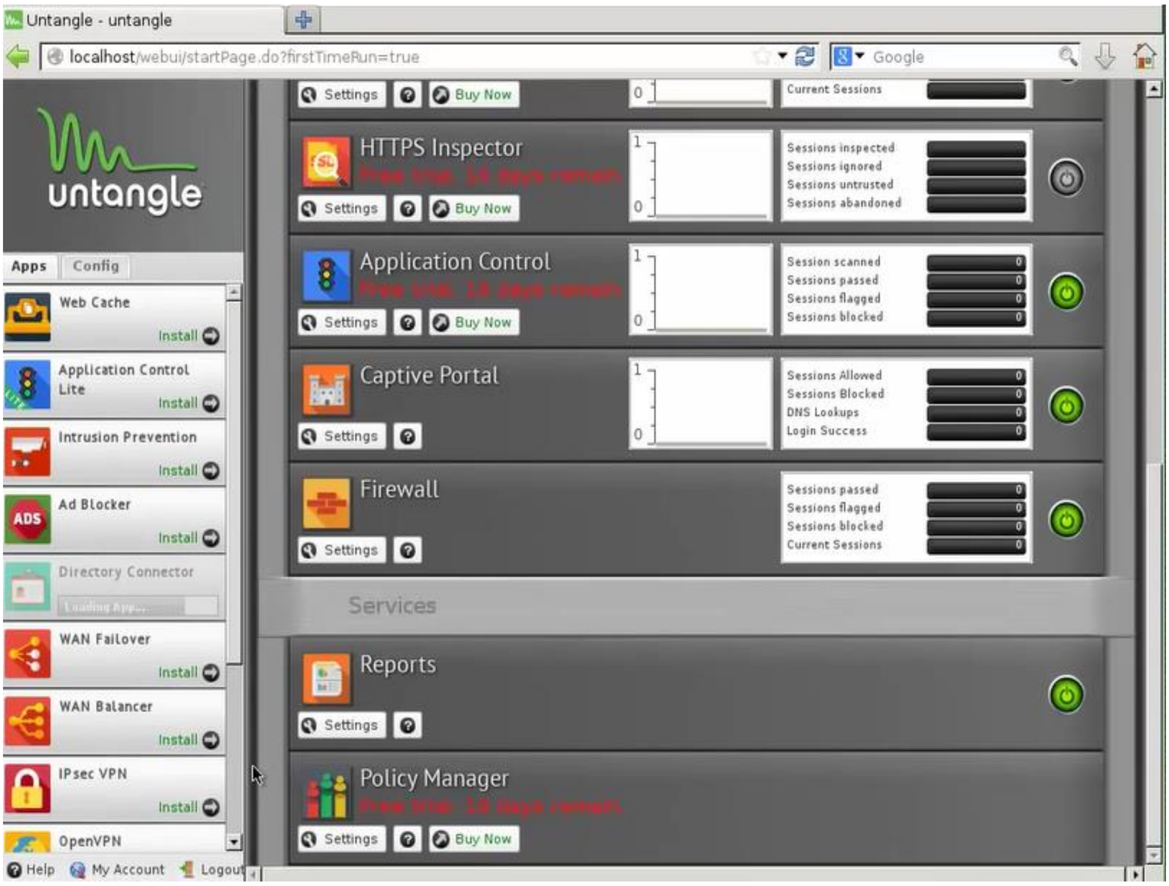


Figure 6. Web GUI interface of Untangle

Various available extensions and features are presented on the GUI interface of Untangle as shown in the figure. Some of them are free to use with registration like Firewall, Reports, web cache while advanced features are accessible only in the paid version.

Through this GUI, administrator can monitor log entries and watch network activities. This GUI helps to provide full control over the network connected with firewall. CLI interface supports basic initial configuration during installation mode. After its done, network policies could be created based on network requirements as well as guard the flow of traffic.

2. pfSense

pfSense is a free licensed router/firewall with rich web GUI. It offers easy upgrade and is supported by wide range of hardware from small LAN to school and business enterprises. Hardware requirements for day-to-day performance of pfSense do not vary and it is suitable for all kind of environments. The biggest problem is to fill the minimum requirements or otherwise it might start to slow down the system.

Here are the minimum (m) and recommended(r) requirements for installation: (Official pfSense.org 2015)

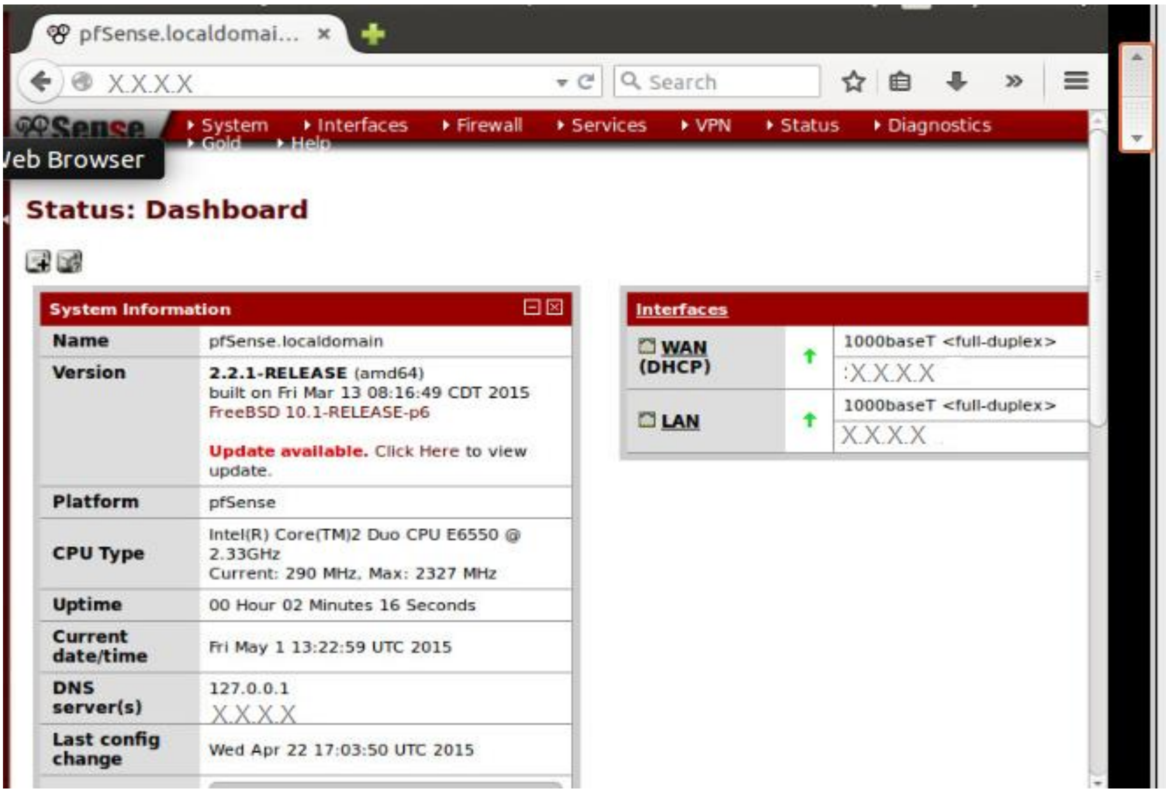
- CPU : 500MHZ(m), 1GHZ (r)
- RAM : 256MB(m), 1GB(r)
- Bootable media : CD-ROM or USB drive (m) or 1GB hard drive,
- NICs: 2(m).

The bootable ISO image of pfSense was downloaded via link https://www.pfSense.org/download/ to select the architecture and platform. Based on the architecture used, pfSense amd64 was downloaded from the official link mentioned above and uploaded to the virtual server datastore for easy access during this project.

pfSense installation is possible through a wide range of media since it is flexible with platforms, like CD-ROM, USB and Serial Console. For this project, pfSense installation was performed by uploading the ISO image of pfSense version 2.2.1 uploaded to the datastore. On the virtual server, the virtual machine named pfSense_firewall was created and two virtual switches, vswitch0 and vswitch1, were linked to incoming and outgoing traffic since pfSense required two virtual NICs, followed by powering the virtual machine. The console page shows the initial installation guided by the wizard asking for normal instructions. With initial setup, pfSense required modification for LAN and WAN network to activate the web configurator to be accessed remotely through the OS browser.

Reboot was used to restart the system, followed by opening a browser and accessing the management IP-address. The GUI page helped to control all features including apps, shields, block, filter, firewall, DHCP, VPN, IPsec, DNS, add-on, extension and automatic upgrade.

Figure 7 illustrates the graphical user interface from where administrator modify network security and channel new policies for the entire architecture.



Status: Dashboard

System Information	
Name	pfSense.localdomain
Version	**2.2.1-RELEASE** (amd64) built on Fri Mar 13 08:16:49 CDT 2015 FreeBSD 10.1-RELEASE-p6 **Update available.** Click Here to view update.
Platform	pfSense
CPU Type	Intel(R) Core(TM)2 Duo CPU E6550 @ 2.33GHz Current: 290 MHz, Max: 2327 MHz
Uptime	00 Hour 02 Minutes 16 Seconds
Current date/time	Fri May 1 13:22:59 UTC 2015
DNS server(s)	127.0.0.1 X.X.X.X
Last config change	Wed Apr 22 17:03:50 UTC 2015

Interfaces		
WAN (DHCP)	↑	1000baseT <full-duplex> X.X.X.X
LAN	↑	1000baseT <full-duplex> X.X.X.X

Figure 7. pfSense web configurator

Figure 7 illustrates the pfSense administrative interface with initial configuration where various extensions could be installed as per the needs of the network. The initial configuration page shows information about the released version of firewall with resource consumption and IP-address of WAN and LAN.

3. Zeroshell

The term Zeroshell was used because the operating system requires Zeroshell access for administrative actions. Features, like NAT/PAT, LAN/WAN configuration, DHCP, QoS, firewall, filters and so on, can be accessed using the web-based GUI. Besides these, Zeroshell supports integrated VPN and DNS functions.

For this thesis project, Zeroshell was used as a virtual router as well as a firewall in the virtual environment between internal and external switches, namely vswitch1 and vswitch0 respectively.

Minimum (m) and recommended(r) requirements for installation of Zeroshell go as follows: (Ricciardi F. 2015)

- Hard drive : 1GB(m), 2GB(r)
- CPU : Pentium I 233MHZ or equivalent (m)
- Memory: 96 MB(m)
- NIC : 2 (m)

Zeroshell works with a Live CD. It does not need to be installed on disk space, although the Installed version is more recommended since it pre-activates automatic upgrades as well as degrades to previous versions. Before installation process was started, a virtual machine named Zeroshell_firewall was created on the VMware ESXi server with the following configuration:

- Hard disk space: 2GB
- RAM : 512 MB
- NIC: vswitch0 and vswitch1 ports (vswitch0 port to communicate as WAN and vswitch1 port to work as LAN port)

Before starting virtual machine, the two different options i.e. connected and power on connected should be checked. Otherwise the machine could not load the ISO image of OS. The ISO image of Zeroshell was downloaded from the official download site (http://www.zeroshell.org/download/) and the image was extracted and uploaded to the server datastore.

The second virtual machine was connected to vswitch1. The virtual environment named Linux_OS (Ubuntu) was created for the LAN network. Gparted Partition Editor was used to create an extension named temporary. Changes were implented followed by exiting the application. Later, a new partition created and mounted.

Launching a browser in Ubuntu desktop helped to navigate the download page for Zeroshell. The ISO image file, ZeroShell-3.3.2.iso, was saved in the temporary extension. The ISO image was extracted using the *gunzip* command and the image was written to the unused hard drive using the command “ dd if = ……..” (Inet Technology Blog 2012)

Once LAN DHCP was configured and the address was acquired, the Zeroshell web GUI could be accessed using the management IP-address in the Ubuntu desktop browser and most of the settings could be accessed and modified using the same window.

3.4 Limitations and comparison of the open source firewalls

The majority of open source firewalls perform efficiently with their free versions but they do not seem easy to extend freely (Pavlina D. 2013). The choice of open source firewall depends on the requirements of the network and the organization/individual. Requirements define limitations. Few queries need be answered while implementing as such, for example, whether a firewall is a simple gateway, or is used for VPNs for remote workers or if administrator would desire to publish servers in DMZ or would like to act as Proxy, hotspot and so on. These questions need to be answered before searching for a firewall.

The majority of commercial open source firewalls come up with all these tools, which make the job of the network administrator easier. Without entering dozens of scripts, one can manage network utilities and have full control over a network, user group authentication and authorization. However, with a long list of features, firewalls have limitations, like limited configuration and even some of them remain unable to establish DMZ (demilitarized zone).

The following limitations were found on the firewalls during this project:

a) Untangle:

Although having freely available features like automatic updates, web-based GUI and easy setup and configuration, Untangle requires payment for high-end features. Besides this, it took longer to boot up and shutdown compared to the other two open source firewalls although available as both 32 bit and 64 bit version. Furthermore, Untangle does not support multipoint VPN, i.e., either VPN server or VPN client, simultaneously. Inability to setup a tunnel for all traffic from client to server right out of box shows severe limitation.

b) pfSense:

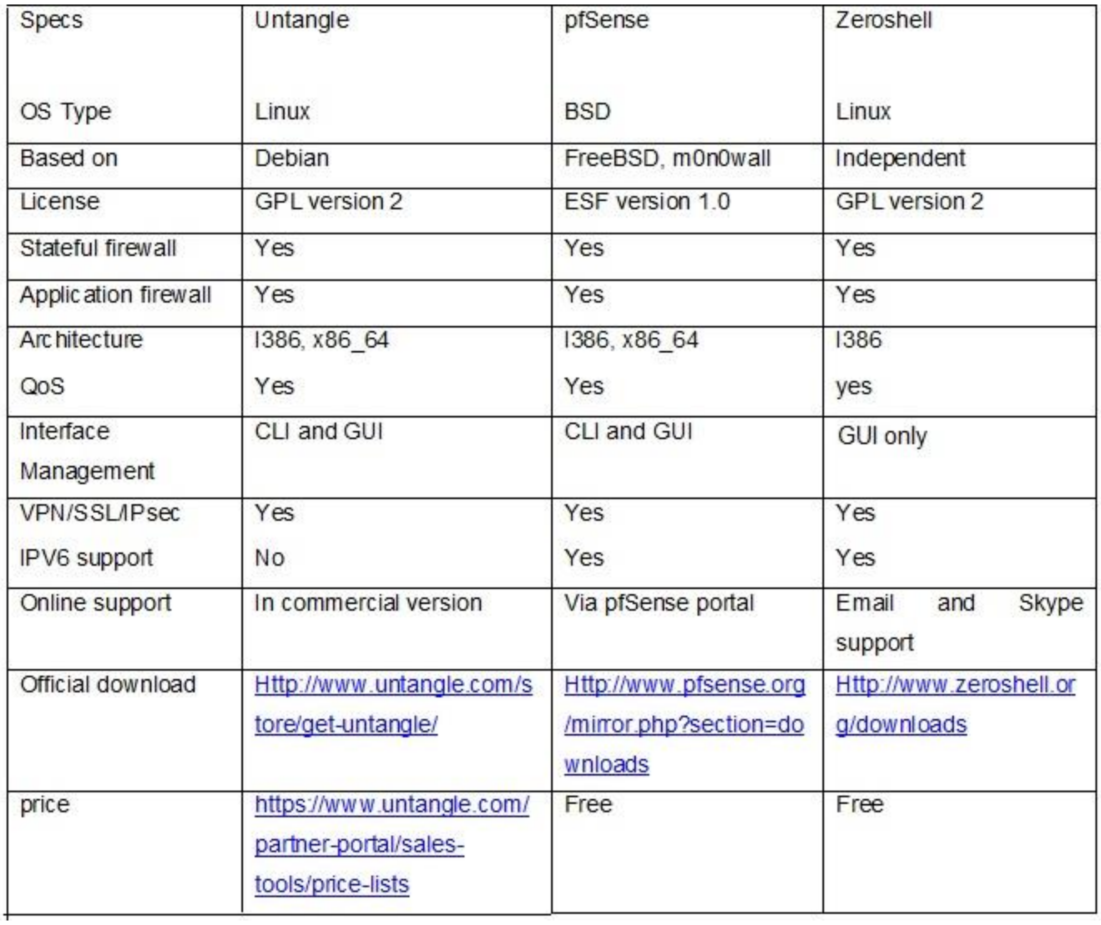
pfSense is a complete solution for today’s commercial network equipped with features, available as 32 bit and 64 bit version. It provides no support over HyperV and Xenserver. HyperV is a virtual server based on Windows environment which divides virtual machines with respect to partition. Xenserver is hypervisor released under GNU GPL version 2 and allows various computer OS to work on same hardware.

Compared to Untangle, it has a complex user interface and requires additional time in updates and upgrade.

c) Zeroshell:

Numerous modern features from wireless access point to web GUI and QoS configuration have made Zeroshell popular, still it does not appeal the most because of its user interface. It is only available as a 32 bit version. There were several similarities among the features of these three firewalls, but there were differences which have been summarized in Table 2 below.

Table 2. Firewall Comparison (Casals C. J. 2012)



Specs	Untangle	pfSense	Zeroshell
OS Type	Linux	BSD	Linux
Based on	Debian	FreeBSD, m0n0wall	Independent
License	GPL version 2	ESF version 1.0	GPL version 2
Stateful firewall	Yes	Yes	Yes
Application firewall	Yes	Yes	Yes
Architecture	I386, x86_64	I386, x86_64	I386
QoS	Yes	Yes	yes
Interface Management	CLI and GUI	CLI and GUI	GUI only
VPN/SSL/IPsec	Yes	Yes	Yes
IPV6 support	No	Yes	Yes
Online support	In commercial version	Via pfSense portal	Email and Skype support
Official download	Http://www.untangle.com/store/get-untangle/	Http://www.pfsense.org/mirror.php?section=downloads	Http://www.zeroshell.org/downloads
price	https://www.untangle.com/partner-portal/sales-tools/price-lists	Free	Free

Installation and testing of the three different firewalls in virtual environment gave conclusive idea for pfSense with features available like it is free of to install and extensions do not require any charges to upgrade. It also provides easily manageable web-based GUI to manage network functions and has reliable online support for latest version. In addition to that, pfSense also do give future expansion of IPv6 support as well as support of 64 bit platforms which meet the condition generated for the objective of the thesis. In conclusion, pfSense meets the objectives required for the thesis to implement with modern security extensions and solutions.

4 Conclusion

The purpose of this thesis was to setup a firewall solution which fits the requirements as outlined in chapter 3.3.Three firewalls were short listed, namely, Untangle, pfSense and Zeroshell, as these came up as the leading solution with a wider scope of security measures along with integrated security utilities and tools.

Analyzing and testing these three network firewalls in virtual environment i.e. VMware ESXi, pfSense indicated the most appropriate firewall since most of the features are supported by minimum hardware requirements. Some attention is required as Snort and ntop are advised not to be installed on systems having less than 1GB RAM.

Apart from these, free license services encourage the use of these firewalls.They are open source with large community of developers, who continuously make an effort to improve security and performance. Furthermore, the latest version of pfSense 2.2.2 provides support for features like IPsec, OpenVPN and HTTPS (TLS) rate above 10GBps, exceeding the normal bandwidth supported by commercial firewalls.

REFERENCES

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]

Casals Ceballos Joquim. 2012. Open Source free firewall comparison. Available at: http://www.opttic.com/content/open-source-free-firewall-comparison.[Accessed: 04.04.2015]

Chmielewski Dawb, Hesseldahl Arik. 2014. Sony Pictures Tries to Disrupt Downloads of its Stoles Files 2014. Available at: http://recode.net/2014/12/10/sony-pictures-tries-to-disrupt-downloads-of-its-stolen-files/. [Accessed: 24.03.2015].

Dineley D. 2008. Best of Open Source Software Awards 2008. Available at: http://www.infoworld.com/article/2652358/applications/applications-best-of-open-source-software-awards-2008.html. [Accesed: 13.05.2015].

Distrowatch 2015. Available at: http://distrowatch.com/search.php?category=Firewall#distrosearch. [Accessed: 23.04.2015].

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

Inet Technology Blog 2012. Creating a Zeroshell Virtual Router. Available at: http://christopherve7alb.blogspot.fi/2012/09/creating-zeroshell-virtual-router.html. [Accessed: 15.04.2015].

Laorden C, Sanz B, Alvarez G, Bringas G Paulo, A. 2010. Threat Model Approach to Threats and Vulnerabilities in On-line Social Networks. Available at: http://ptgmedia.pearsoncmg.com/images/1587131625/samplechapter/1587131625content.pdf

Neustar Annual DDoS Attacks and Impacts Report 2014. The Danger Deepens. Available at: https://www.neustar.biz/resources/whitepapers/ddos-protection/2014-annual-ddos-attacks-and-impact-report.pdf. [Accessed: 19.04.2015]

Open Source, 2015. Available at: http://opensource.com/resources/what-open-source. [Accessed: 25.03.2015].

Pavlina David. 2013. The hunt for the ultimate free open source firewall Distro. Available at: http://www.mondaiji.com/blog/other/it/10175-the-hunt-for-the-ultimate-free-open-source-firewall-distro#!kmt-start=19. [Accessed: 11.04.2015].

pfSense hardware requirements 2015. Available at: https://www.pfSense.org/hardware/#requirements. [Accessed: 03.03.2015].

Preetham. V, 2002, Internet Security and Firewalls, Course Technology / Cengage Learning, p -40.

PSN, Blizzard and Riot hit with massive DDoS attack 2014. Available at: http://www.dailydot.com/esports/psn-blizzard-riot-ddos-attack/. [Accessed: 22.03.2015]

Reference Dictionary 2015. Available at: http://dictionary.reference.com/browse/firewall [Accessed: 19.03.2015]

Ricciardi Fulvio, 2015.Hardware needed to run Zeroshell. Available at: http://www.zeroshell.org/hw/.[Accessed: 15.03.2015-10.04.2015].

Untangle hardware requirements 2015. Available at: http://wiki.untangle.com/index.php/Hardware_Requirements#Hardware_Recommendations_Table. [Accessed: 10.03.2015].