



UNIFIED THREAT MANAGEMENT (UTM): A COMPARATIVE STUDY

AHMAD AYID AHMAD AHMAD

JULY 2017

UNIFIED THREAT MANAGEMENT (UTM): A COMPARATIVE STUDY

A THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF NATURAL AND APPLIED
SCIENCES OF
ÇANKAYA UNIVERSITY

BY
AHMAD AYID AHMAD AHMAD

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE
DEGREE OF
MASTER OF SCIENCE


IN

THE DEPARTMENT OF
MATHEMATICS
INFORMATION TECHNOLOGY PROGRAM

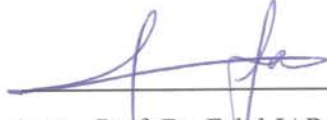
JULY 2017

Title of the Thesis: **Unified Threat Management (UTM): A Comparative Study**
Submitted by **Ahmad Ayid Ahmad AHMAD**


Approval of the Graduate School of Natural and Applied Sciences, Çankaya University.


Prof. Dr. Can ÇOGUN (U)
Director

I certify that this thesis satisfies all the requirements as a thesis for the degree of Master of Science.


Assoc. Prof. Dr. Fahd JARAD
Head of Department

This is to certify that we have read this thesis and that in our opinion it is fully adequate, in scope and quality, as a thesis for the degree of Master of Science.


Assist. Prof. Dr. Sibel ÖZYER
Supervisor

Examination Date: 18.07.2017

Examining Committee Members

Assist. Prof. Dr. Sibel ÖZYER (Çankaya Univ.)


Assist. Prof. Dr. Tolga PUSATLI (Çankaya Univ.)

Assist. Prof. Dr. Tolga MEDENİ (Yıldırım Beyazıt Univ.)



STATEMENT OF NON-PLAGIARISM PAGE

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, Last Name : Ahmad , AHMAD
Signature : 
Date : 18.07.2017

ABSTRACT

UNIFIED THREAT MANAGEMENT (UTM): A COMPARATIVE STUDY

AHMAD, Ahmad Ayid Ahmad
M.S., Information Technology Department
Supervisor: Assist Prof. Dr. Sibel ÖZYER

July 2017, 90 pages

Network security has been the foremost need of the technologically advanced world, when considering the implications in the business environment. It has been affirmed that the business enterprises have intensively become susceptible to the data theft or data breaching attacks over the internet; thus, credibility of the processes has been affected. Businesses that lack in being considerate towards the competitive needs of the strategies tend to face declining performance. It leads to the assertion that the decision making process of the businesses must be based on the deployment of continuous improvement prospects.

In this thesis, we assessed the business stance of an Imaginary Organisation that led to the assertion that the current network infrastructure of traditional firewall needs to be upgraded. The existing traditional firewall has been disabled to standing against security threats such as Denial of Service, SQL injection, email viruses ..etc. Therefore, the study has been proposed to the migration plan of an Imaginary

Organisation network that serve 200 users with developed security services. The plan has been presented to the UTM as advanced features security solution.

In order to select the best UTM that satisfied the demands of an Imaginary Organization security requirements, a comparison study among four commercial UTMs has been held. This study achieved by using a virtual lab that consistent from a multi virtual machines that was used as a test environment. The four UTMs have been assessed based on the attributes of visions, execution, ease of use, web-interfaces, device performance, throughput capacity, intrusion prevention system features along with the guaranteed elements of security and many other factors.

The experimental work includes installation and test of the software's such as SONICWALL, SOPHOS XG Firewall, WarchGuard, and Palo Alto Networks. The researcher also analyses the impacts of Gartner's reviews along with testing lab result to come out with conclusions that the UTM device called SOPHOS XG Firewall was the best tested device based on study criteria. This device provides the most significant security features affordably. SOPHOS XG Firewall provides the security features such as email protection, Unknown Application Identification, along with the element of Full-Featured Web Application Firewall that able to prevent SQL injection attacks and Denial of service ..etc which traditional firewalls and other UTMs may not be capable of doing. Moreover, the study has presented details in this regard, along with the clearly articulated recommendations as well.

Keywords: Unified Threat Management, Network Security, Advanced Threat Protection.

ÖZ

BİRLEŞTİRİLMİŞ TEHDİT YÖNETİMİ (BTY): KARŞILAŞTIRMALI BİR ÇALIŞMA

AHMAD, Ahmad Ayid Ahmad
Yüksek Lisans, Bilgi Teknolojileri Anabilim Dalı
Tez Yöneticisi: Yrd. Doç. Dr. Sibel ÖZYER

Temmuz 2017, 90 sayfa

İş ortamındaki etkileri göz önüne alındığında, ağ güvenliği teknolojik olarak gelişmiş dünyanın önde gelen ihtiyacı olmuştur. İşletme teşebbüslerinin internet üzerinden veri hırsızlığına veya veri ihlallerine karşı duyarlı hale geldiği doğrulandı; böylece, süreçlerin güvenilirliği etkilenmiştir. Stratejilerin rekabetçi ihtiyaçlarına karşı düşüncesinden yoksun olan işletmeler, düşen performansla karşı karşıyadır. Bu, işletmelerin karar verme sürecinin sürekli gelişim umutlarının yaygınlaştırılmasına dayalı olması gerektiği iddiasına yol açmaktadır.

Bu tezde, geleneksel güvenlik duvarının mevcut ağ altyapısının yükseltilmesi gerektiği iddiasına neden olan hayali bir organizasyonun iş tutumunu değerlendirdik. Mevcut geleneksel güvenlik duvarı hizmet reddi, SQL enjeksiyonu, e-posta virüsleri gibi güvenlik tehditlerine karşı durmak için devre dışı bırakılmıştır. Bu nedenle, çalışma, gelişmiş güvenlik hizmetleri olan 200 kullanıcıya hizmet eden hayali bir organizasyon ağının göç planını önermiştir. Plan, BTY' yi gelişmiş özellikler güvenlik çözümü olarak sunmuştur.

Hayali organizasyon güvenlik gereksinimlerinin taleplerini karşılayan en iyi BTY' yi seçmek için, dört ticari BTY arasında bir karşılaştırma çalışması yapılmıştır. Bu çalışma, bir test ortamı olarak kullanılan çok sanal makinelerden tutarlı bir sanal laboratuvarı kullanarak gerçekleştirildi. Dört BTY; vizyonlar, uygulama, kullanım kolaylığı, web arayüzleri, cihaz performansı, verim kapasitesi, saldırı önleme sistemi özellikleri ve güvenlik unsurları ile diğer pek çok faktörün özelliklerine dayanılarak değerlendirildi.

DeneySEL çalışma, SONICWALL, SOPHOS XG Firewall, WarchGuard ve Palo Alto Networks gibi yazılımların kurulumunu ve test edilmesini içerir. Araştırmacı ayrıca Gartner'ın incelemelerinin etkilerini laboratuvar test sonuçlarıyla birlikte analiz ederek SOPHOS XG Firewall adlı BTY cihazının çalışma ölçütlerine dayalı en iyi test edilmiş cihaz olduğu sonucuna varmıştır. Bu cihaz, en önemli güvenlik özelliklerini uygun fiyatla sağlar. SOPHOS XG Güvenlik Duvarı; e-posta koruması, Bilinmeyen Uygulama Tanımlama ve ayrıca SQL enjeksiyon saldırılarını ve Hizmet Reddini engelleyebilen Tam Özellikli Web Uygulaması Güvenlik Duvarı ögesiyle birlikte, geleneksel güvenlik duvarları ve diğer BTY' lerin yapamayacağı durumları sağlar. Ayrıca; çalışma, açık bir şekilde ifade edilen tavsiyelerle birlikte bu konuda ayrıntılar sunmuştur.

Anahtar Kelimeler: Birleştirilmiş Tehdit Yönetimi (BTY), Ağ Güvenliği, Gelişmiş Tehdit Koruması.

ACKNOWLEDGEMENTS

First of all, I would like to thank my god ALLAH who support me and supplied me with power and faithful to comprehensive with this hot topic. I love you with all my heart, my Lord.

I wish to express my deep gratitude and appreciation to my supervisor Assist. Prof. Dr. Sibel ÖZYER, for her guidance, advice, support throughout the entire thesis, and her teaching of the methodologies for good scientific research.

I would like to present my thanks to family, especially sweetheart, my mother, my brothers, and my sisters who supported me all the time.

Lastly, I would like to thank all the staff in our department at Cankaya University who supported me throughout academic courses, especially for the coordinate of the information technology program Assist. Prof. Dr. Tolga PUSATLI.

TABLE OF CONTENTS

STATEMENT OF NON PLAGIARISM.....	iii
ABSTRACT.....	iv
ÖZ.....	vi
ACKNOWLEDGEMENTS.....	viii
TABLE OF CONTENTS.....	ix
LIST OF FIGURES.....	xii
LIST OF TABLES.....	xiv
LIST OF ABBREVIATIONS.....	xv
CHAPTERS:	
1. INTRODUCTION.....	1
1.1. Introduction.....	1
1.2. Background.....	1
1.3. Problem Statement.....	3
1.4. Contribution and Objectives of The Study	4
1.5. Significance the Study.....	4
1.6. Thesis Structure.....	5
2. LITERATURE REVIEW.....	6
2.1. Introduction.....	6
2.2. Security Needs in the Business Environment and the Technological Challenges.....	6
2.3 Potential Sources of Attacks on the Vulnerable Business Network.....	8
2.3.1 Email Viruses.....	9
2.3.1.1 Landscape of Inbound Threats.....	10
2.3.1.2 Landscape of Outbound Risks.....	11
2.3.2 File Based Threats.....	11
2.3.3 Application Attacks.....	12
2.3.3.1 Spyware Infection.....	13
2.4 Traditional Network Security and its Inefficacies.....	14

2.4.1	Anti-virus as a Security Tool.....	15
2.4.2	Integration of Firewall.....	17
2.4.3	Deep Packet Inspection and Intrusion Prevention.....	17
2.5	Unified Threat Management - UTM System.....	18
2.5.1	Categorisation of UTM Systems.....	19
2.5.1.1	Equipment Types.....	19
2.5.1.2	Technical Architecture Type.....	19
2.5.1.3	Integrated Technologies Type.....	19
2.6	Performance Analysis of a Unified Threat Management System.....	21
2.7	Next Generation Firewalls (NGFW).....	23
2.8	Performance Comparison of UTM and NGFW.....	24
3.	RESEARCH METHODOLOGY.....	25
3.1	Introduction.....	25
3.2	Oracle VM Virtual Box.....	26
3.3	UTM Solutions Used in the Study.....	27
3.3.1	SONICWALL Unified Threat Management Solution.....	27
3.3.2	SOPHOS Unified Threat Management Solution.....	29
3.3.3	WatchGuard Unified Threat Management Solution.....	30
3.3.4	Palo Alto Networks.....	32
4.	EXPERIMENTAL WORK	36
4.1	Introduction.....	36
4.2	Migration Plan.....	36
4.2.1	PDCA - Plan-Do-Check-Act.....	37
4.3	Next-Generation Firewall (NGFW).....	38
4.3.1	Essential Aspects.....	38
4.3.2	Awareness regarding the Contextual Aspects.....	39
4.3.3	Implications of UTM Functionality.....	39
4.3.4	Advantages of NGFW-UTM.....	39
4.4	Current Network of an Imaginary Organisation.....	40
4.5	Future Network for an Imaginary Organisation.....	41
4.6	Requirements of the Proposed System.....	43

4.7	Implications based on Comparison of Features.....	43
4.7.1	Platform Testing.....	44
4.7.2	Initial Configuration/Ease of Installation.....	44
4.7.2.1	Palo Alto Network.....	45
4.7.2.2	SONICWALL.....	45
4.7.2.3	SOPHOS.....	47
4.7.2.4	WatchGuard.....	50
4.7.3	Web Interface.....	52
4.7.3.1	Palo Alto Networks.....	52
4.7.3.2	SONICWALL.....	54
4.7.3.3	SOPHOS.....	58
4.7.3.4	WatchGuard.....	61
4.8	Comparison of the Devices based on Magic Quadrant of Gartner.....	62
4.9	Comparison of the Devices based on Virtual Box environment	68
4.10	Comparing the Capability of Gartner's Recommended Device "SOPHOS" with others.	70
4.10.1	SOPHOS XG vs., Dell SONICWALL.....	71
4.10.2	SOPHOS XG vs. WatchGuard.....	73
4.10.3	SOPHOS XG vs. Palo Alto Networks.....	74
4.11	Discussion.....	76
5.	CONCLUSION AND FUTURE WORK.....	78
5.1	Findings	79
5.2	Limitations	80
5.3	Future studies	80
5.4	Conclusion	80
	REFERENCES.....	82
	APPENDICES.....	90
	A. CURRICULUM VITAE.....	90

LIST OF FIGURES

FIGURES

Figure 1 Virus attacks through Emails [12].	10
Figure 2 File Transfer Threats [34].	12
Figure 3 Application attacks through servers [36].	13
Figure 4 Spyware Infections [14].	14
Figure 5 Traditional security framework of Network [40].	15
Figure 6 Proposed Topology	42
Figure 7 Hierarchal structure of IP interface for Palo Alto [69]	45
Figure 8 consol connection port [70]	46
Figure 9 Initial Configuration [70].	47
Figure 10 The configuration details of SOPHOS [71].	48
Figure 11 basic setup GUI of SOPHO [71].	49
Figure 12 Sophos LAN setting [71]	50
Figure 13 setup GUI of WatchGuard [72]	51
Figure 14 WatchGuard network setting [72].	52
Figure 15 Alo palo network control center[69].	53
Figure 16 Web-interface of PAN [73].	54
Figure 17 Accepted browsers for SONICWALL [74].	55
Figure 18 SONICWALL installation steps[74]	56
Figure 19 SONICWALL anti-virus enabling [74]	57
Figure 20 SONICWALL monitor [74].	58
Figure 21 SOPHOS control center (Author, reference)	59
Figure 22 SOPHOS email protection (Author, reference)	60
Figure 23 WatchGuard control center [72]	61
Figure 24 WatchGuard management elements [72].	62
Figure 25 Gartner Magic Quadrant - ENDPOINT PROTECTION [75]	66

Figure 26 Gartner Magic Quadrant UNIFIED THREAT MANAGEMENT [75]....	67
Figure 27 SOPHOS XG vs., Dell SONICWALL [77].....	72
Figure 28 SOPHOS XG vs. WatchGuard [76].....	74
Figure 29 SOPHOS XG vs. Palo Alto Networks [78]	76



LIST OF TABLES

TABLES

Table 1	Comparison of the devices	69
Table 2	Compare SOPHOS XG vs., Dell SONICWALL.....	71
Table 3	Compare SOPHOS XG vs. WatchGuard.....	73
Table 4	Compare SOPHOS XG vs. Palo Alto Network.....	74



LIST OF ABBREVIATIONS

ALG	Application Layer Gateway
APTs	Advanced Prsistant Threat
AS	Anti spam
ATP	Advanced Threat Protection
AV	Anti viruse
AWS	Amazon Web Service
CLI	Command Line Interface
DLP	Data loss prevention
FTP	File Transfer Protocol
HTTPS	Hyper Text Transfer Protocol Secure
HW	Hardware
IaaS	Infrastructure as a Service
ICT	Information and Communications Technology
IPS	Intrusion Prevenation System
LAN	Local Area Connection
MAPP	Microsoft Active Protections Program
NAT	Network Adress Translation
NAT	Network Address Translating
NetBIOS	Network Basic Input/Output System
NGFW	Next Ganeration Firewall
PDCA	Plan-Do-Check-Act
Qos	Quality of Service
SSL	Secure Sockets Layer
SW	Software
VPN	Virtual Private Network

CHAPTER 1

INTRODUCTION

1.1 Introduction

This section presents the basic background information that is relevant to the topic under consideration. The provision of secure network has been the foremost need of business to sustain its position in the marketplace. Since the entire business framework of the business is network-based, there are extreme threats of data theft or certain other virus-related concerns. Multiple traditional firewalls and other security applications have long been used as a defense mechanism against these security threats. However, today's modern technology have disregarded these security applications as a reliable source that eventually demands proficient and intensely secure networking systems [1,2,3,4 and 6]. In this regard, the approach of unifying multiple threat management entities has been deployed in different frameworks, yielding different security levels to the businesses. Accordingly, this section presents the problem focus, along with the formulated objectives and the adopted methodology as well.

1.2 Background

The rapid advancements in the internet technology have generated the challenges of data security, as the hackers or the attackers have also acquired potential skills of virus or malicious attacks to gain access to the network [1,2,3,4,5 and 6]. This particular prospect has been a major issue for the enterprises, government agencies, or even educational institutions, as the loss of data eventually causes intensive damage to the entire business model, regardless of the business sector. The success of a business primarily depends on the growth of the revenues, along with the secure

networking to prevent certain losses. Regardless of the nature or the size of the business, damage to the data security results in severe loss to the reputation of the business in the marketplace that is not acceptable within the intensely competitive business environment. It is mainly due to the loss of potential customer loyalty as the element of customer satisfaction is greatly affected due to the vulnerabilities of the data security system [7,8,9 and 10].

The network of the business remains susceptible to the malicious attacks of data that is mainly caused by the communication modes of e-mails, file transferring systems, and even the contents integrated within the applications on server. It reflects that the network is vulnerable to the security threats that eventually cost the business severe monetary losses. Besides, the businesses even have to face the lawsuits or certain other liabilities from the stakeholders' side [11]. In this regard, [7] has contended that the businesses focus on the assurance of making the entire IT environment secure; however, it is also observed that the business enterprises have been prioritising other economic prospects over the assurance of secure networking. Here, the situation gets even more adverse as the malicious attacks are facilitated; thus, disrupting the overall reputation of the business. Consequently, it is established that the businesses tend to be more vulnerable to the security threats due to their less responsiveness towards the security frameworks that is reflected from the deployment of traditional firewalls or other security applications, whose efficacies have been disregarded with respect to the intensity of the malicious attacks over the internet [1,2,3,5 and 12].

It has been recognized that the businesses must have the insightful knowledge of the cyber essentials when operating in the network-based environment. There needs to be no chance of any unauthorized or unintended access to the company's data as it may lead to data theft, data manipulation, or even destruction of the data. It needs to be the prime objective of an enterprise to have a secure business network, as it eventually generates potential commercial opportunities.

[9] has asserted that the internet world cannot be regarded as absolutely safe that is aligned with the incessant advancements in the technology. In this regard, the deployment of a Unified Threat Management - UTM System has been affirmed as the potential technique of mitigating the vulnerabilities of the business networks.

UTM is a combined security framework that facilitates intrusion detection, filters the content against malicious data, manages the spam content integrated within the applications, and handles the anti-virus duties as well [13,14,15,16,17 and 18]. Therefore, it is affirmed that the UTM system provides all time security needs of the computer network; thus, mitigating all the shortcomings of the individual security solutions [18,19,20,21 and 22]. This research explores the implications of UTM system with respect to the security needs of the business networks.

1.3 Problem Statement

Security concerns have also been there since the use of internet technology within the business processes. The data or the information of the enterprises is of utmost value to the success of the business, which demands intensive measures of ensuring the integrity and confidentiality of the data. However, this prospect of assurance has been challenging against the advancing pace of technology that has disregarded the security potential of anti-virus or anti-spam tools alone. The extent of hacking attacks or data theft activities of the actors involved demands exceptionally strong defense mechanism. The defensive system needs to have ensured security at all the levels as the competitiveness of the businesses greatly depends on the satisfied service delivery to the consumers.

Traditional security network system used many devices to stand against network threads. The disadvantages of this approach include high hardware cost, multi vender problems, upgrade problems, availability and the cost of management as this process required more expert employees.

This thesis studied and analyzed the security system of an Imaginary organization, where the an Imaginary Organization security system based on a traditional firewall. This firewall contended to have inefficiencies of inspecting the packets received in terms of malicious codes or malwares. Besides, this firewall is also inefficient in comprehending the objective or agenda of the end-users over the server. Also an Imaginary Organization suffers from advanced threats such as denial of service and email viruses .etc. However, we presented the UTM as a best solution for upgrade the existed security system of an Imaginary Organization.

1.4 Contribution and Objectives of The Study

The study has evaluated the security potential of Unified Threat Management system for the sustained competitiveness of a business in this environment of increasingly vulnerable technology. The study entails the element of value innovation with respect to the business needs of risk management and enhanced productivity. Besides, the prospects of reduced operating costs, workforce mobilization, enhanced competitive advantage, increased traffic and bandwidth, and real-time growth are also recognized in relation to the use of UTM system over the network [13,14,15,16,17 and 18].

The study aims exploring the security potential of Unified Threat Management - UMT against the malicious attacks or data theft activities over the network. In order to achieve this aim, certain objectives have been formulated to make the research plan effectively directed towards success. The proceeding section presents the listed objectives of the study:

- To explore the security needs of the business networks
- To explore the importance and benefits of UTM pertaining to the security needs of the network
- To study the working of UTM
- To compare the available UTM frameworks with respect to the network defense layer
- To study the importance of Next Generation Firewalls (NGFW)
- To analyze the performance of UTM and NGFW

1.5 Significance the Study

The significance of the study is associated with the focused objectives of UTM "Unified Threat Management" in the networking world. Insightful knowledge has been gained regarding the potential benefits of UTM system over the individual level security or anti-virus systems. The prospects of lowest, It is obvious that using one device is the lowest price of using several devices ownership cost in terms of

licensing needs, deployment aspects, and consistent security performance have been affirmed with respect to the credibility of UTM [13,14,15,16,17 and 18]. Besides, significant knowledge of the real-time automation of network security has also been gained. The study also provides analysis of multiple vendor approach of security functions for different servers or appliances.

1.6 Thesis Structure

- Chapter 1 - Introduction: This section presents the relevant background context of the research problem, along with the problem statement, aim and objectives, significance of the study, and the adopted method as well.
- Chapter 2 - Literature Review: In this section, the researcher has presented the relevant literature of the topic under consideration. It is regarded as an important section of the entire study as it entails the descriptive details of the main areas of the research.
- Chapter 3 - Research Methodology: The adopted research method and its constituents are discussed in this section, depending on the nature of the study.
- Chapter 4 - Discussion and Analysis: In this section, the acquired findings and the associated discussion is presented.
- Chapter 5 - Conclusion and Recommendations: This section encompasses the concluding remarks based on the analysis of the acquired findings. In addition to this, it also presents certain recommendations pertaining to the future work.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

This section presents the literary support of the topic under consideration. The networks of enterprises are always vulnerable to the threats of spyware or viruses that eventually damages the data files, and in most of the cases, the entire network is collapsed. These vulnerabilities to the data security cannot be disregard as the success needs of the organizations are aligned with the customer satisfaction [7,9 and 10]. If the data of the customers or the information of the businesses is not protected against the hacking attacks, the businesses are deemed to loss their competitiveness. Accordingly, the proceeding section presents the description of the security needs in the business environment, the associated technological challenges, limitations of the individual security tools, and the security potential of the system of Unified Threat Management in this regard.

2.2 Security Needs in the Business Environment and the Technological Challenges

According to the study of [8] , if the security measures of a business operating on the network are improper or inadequate, the business ultimately encounters failure. The prospect of losing data cannot be disregarded as it governs the credibility of the enterprise system of valuing its clients and their needs. The data present on the network, whether it belongs to the staff. The potential clients or the organizational processes, needs to be align with the prospects of integrity and confidentiality at all the levels.

According to the study of [10] the businesses are customer-focused that demands the entire data management system to be aligned with the assurance of facilitating confidentiality to the respective customers. The study of [9] has regarded the secure systems' assurance of the business as the success factor for the business, as it directs the attainment of customer satisfaction and loyalty. On the other hand, having poor quality of network system leads the business towards definite failure. Considering the worst-case scenario of inadequacies of meeting the data security needs of the customers, the businesses have to face even obligatory challenges as lawsuits, since the data is actually customers' "Personally Identifiable Information". The data theft may result in crime-related activities, making the customers suffer for no reason [24,25 and 26]. Therefore, the situation ultimately results in lost loyalty of the potential customers, along with the loss of competitive position in the market.

According to the study of [19], the data management platforms of the businesses are vulnerable to the challenges of ICTs that is eventually the result of advancements in all the sectors of technology [11,19]. There are certain conditions entailing the concerned prospects with respect to the attacks:

- Unauthorized data access, in terms of manipulating the data logs, and hacking the user sessions or accounts
- Vulnerabilities of the Application Program Interfaces that are accessible to the developers
- Malicious activities of inbound and outbound tasks
- The vulnerabilities of the shared platforms being accessed across the enterprise

According to the study of [19], the main reason of enhanced vulnerabilities of the computers over the shared networks is the lacking of being responsive to the security needs of the data, as the system is anticipated as an isolated region that has no accessibility for others. The hosting of these virtual machines is carried out on servers that are called hypervisors; thus, these hypervisors are prone to the hacking attacks. These hypervisors represent the potential vulnerabilities against the DDoS, buffer overflows, viruses, Trojans, spyware, and other malicious activities. Since the attackers are the professional hackers they might have certain access-related permission or rights over the network of the business; thus, the needs of securing the

individual level systems are ascertained as the system in such cases needs not to be targeted from outside, but the threats may be injected from a folder.

The study of [22] has emphasized the needs of deploying security measures over the networks. It has been asserted based on the fact that the internet world has been experiencing increasing speed of cyber-attacks. The more a business requires technological integration for the attainment of competitive advantage, the more its success prospects are vulnerable to the increasing cyber-attacks. Hackers have access of the automated tools or that attacks are carried out in a hybrid manner that reflects that the strength potential of the hackers in the technological environment of business [22]. Accordingly, it has been noted that the susceptible infrastructure of the business networks seems to support the unpredictability of the threats as the business entities are observed to avoid the concerns of security, compromising it based on the constraints of cost-investment, time and other resource allocations.

2.3 Potential Sources of Attacks on the Vulnerable Business Network

The study of [23] has contended that the attackers are not concerned with the nature of the business or the respective industry, what the attackers target are the potential vulnerabilities of the network systems. The advancements in the technological domains have strengthened the hackers or the attackers to exploit the vulnerabilities of the computer networks. General elements of the enterprise networks are observed to be potentially susceptible to the data theft attempts of the hackers, like Windows, Internet Explorers and others. Certain automated tools are always in-line to exploit any vulnerability posed by the system [12,23]. This particular hacking or attacking phenomenon is facilitated by the internet service that is the basic need of the business networks. It has been contended that all the computers that are connected on the networks are prone to the hacking attacks.

The computer systems that are networked have the prospects of being used as "Spam Relays", as the spammers or internet, hackers are observed to send a number of spam emails that is carried out by masking their appearance as a credible source. The same computers over the network may also be used by the hackers as somewhat illegal repository of files. Besides, it is also affirmed that these hackers are proficient in

breaching even the potentially secure networks of the enterprises [12,23]. The study of [12] has asserted that the networks are the potential targets of the rivals, in order to damage the integrity of the business model. There are certain cases that involve hiring the professional hackers to track the networking of a particular business over the internet. These hackers or attackers already have a number of infected computers that are collectively used to exploit the targeted business websites. These computers having the infected content visit the website at the same time, resulting in increased traffic over the website. It results in making the server busy to respond to the needs of its potential customers, as the deceived requests disrupt the prioritising system of the business network [11]. The proceeding section presents the vulnerabilities of the potential elements of communication over the network.

2.3.1 Email Viruses

Emails have long been the primary mode of communication among the research and technical professionals. Almost 100 billion email messages are swapped among the corporate users on daily basis, which reflects the significance of email towards the businesses. Being the central element of businesses, the security concern is of utmost significance for the emails. In this regard, it is noteworthy that only massive campaigns of spamming are not concerning, but these malware or spam are just a part of outbound risks and inbound threats [27,28].

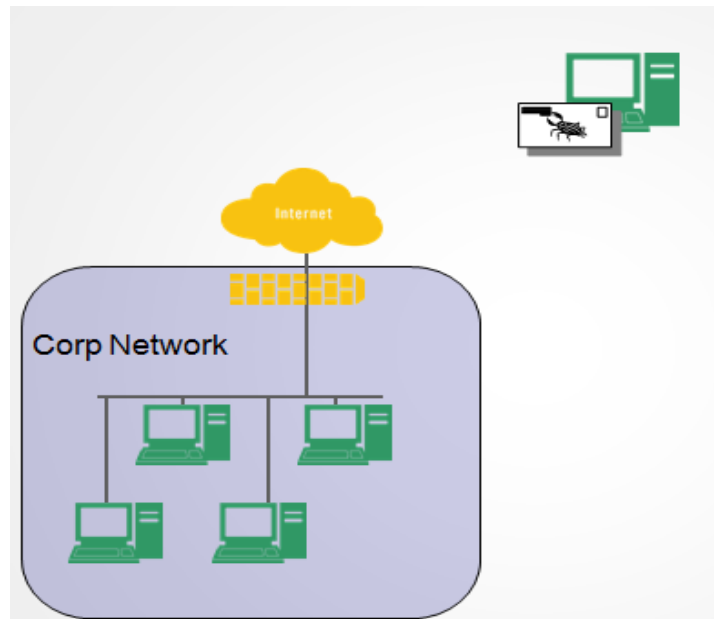


Figure 1 Virus attacks through Emails [12].

2.3.1.1 Landscape of Inbound Threats

The attacks through emails have turned out to be more complex as the professional hackers have established their personalized malware along with the kits of installing malware as well. These professional hackers sell out those spam networks as DoS " Denial of Service " attacks. DDoS is a network cyber attacks designed to overwhelm the victim server by huge number of service requests until the system crash that prevent legal users from access to the service. Besides, these attacks are further supported by the spammers' offered test programs of anti-spamming that are basically the malicious links. It reflects that these attacks have been carried out in a targeted manner. It is facilitated by acquiring the information from the social media websites that is floated to the target through phishing mails [29]. There are web-links in these mails that direct the targets towards the hosting websites that have exploiting kits. Most importantly, the exposure to threats has also increased due to the users' accessibility of the HTML content over multiple devices. In these cases, the company firewall or any other security plan does not protect the content as the avenues of HTML are prone to the blended attacks; thus, blurring the segmented layers of security [30].

2.3.1.2 Landscape of Outbound Risks

Unfortunately, the advancements in the technological world have instilled same level of advancements in the hacking attempts as well. The communication mode of emails has been the most preferred source of sharing the sensitive data of the enterprises and even the information of the employees or the customers that is personally identifiable [31,32]. Therefore, it is highly emphasized that the information that is personally identifiable or PII needs to be encrypted within the mail body [24,25 and 26]. If left unencrypted, the emails of the business result in damaging the brand equity along with losing customer trust. In order to cope with the challenges, The world's largest network company and a strong competitor to these devices it was Cisco , [33] , [33] has presented the protection protocols that have scalability and flexibility in ensuring the compliance at outbound level and capabilities of encryption as well. The entire system needs to be aligned with the infrastructure potential of dealing with the oppressive aspects of content.

In addition to the email viruses, there are certain other sources of threats as well, that are described in the section below:

2.3.2 File Based Threats

These threats are associated with the internet-downloaded files that are easily infected by the malicious codes or viruses over the internet. Its influences have been adverse at all the levels as file sharing or transferring is a common mode of data transfer. If data is being transferred through USBs or other storage devices, these devices are easily infected once the malicious code is inserted [34,35]. Later on, all the files stored or transferred on to the media get affected with the virus instantly. Additionally, the advanced mechanisms of sharing large files within the legitimate corporations have been the shareware sites, certain instant messaging applications, compromised servers, and definitely the emails as well.

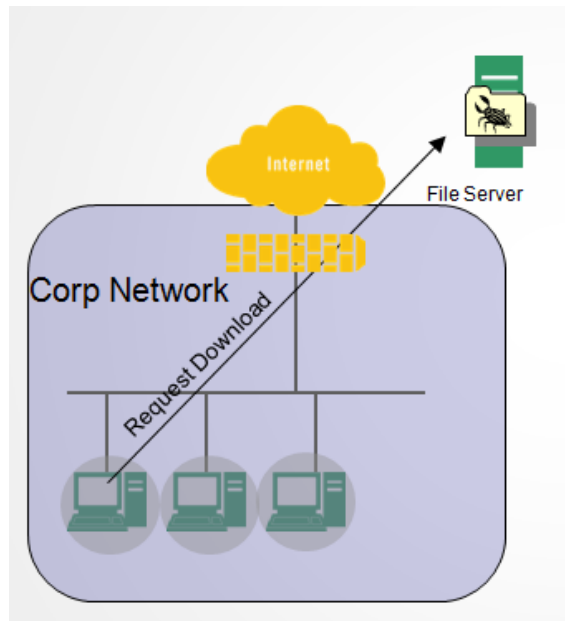


Figure 2 File Transfer Threats [34].

2.3.3 Application Attacks

These attacks to the network security are powered over the servers of the business that are used as a source of interconnectivity across the organization. These servers are usually unpatched along with the concerned scenario of avoiding updating needs. Once the server is targeted, the attackers or the hackers send malicious codes as buffer overflow that finds its way to the targets' computers. These malicious codes can also have the prospects of DDoS attacks that in turn results in crashing the entire computer with losing all the datasets [36,37]. As a result, the entire server remains affected due to inefficiencies of update system. Therefore, any potential new user of the same server also gets infected with the threat.

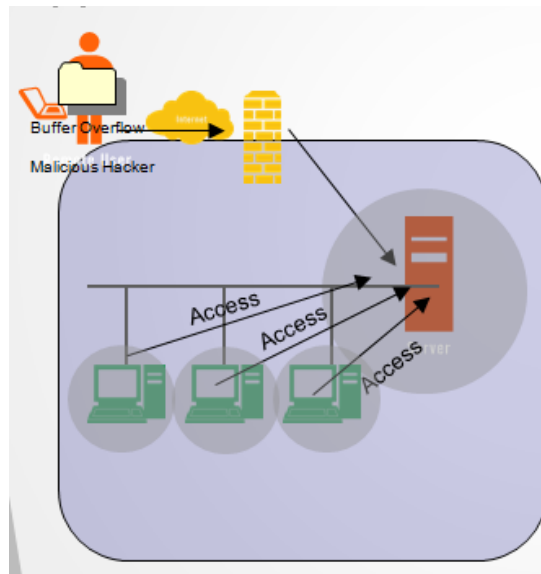


Figure 3 Application attacks through servers [36].

2.3.3.1 Spyware Infection

These infections are injected through diverse sources, inclusive of the following:

- Downloading programs;
Kazaa / screensavers / windows utilities, and
Download managers / file sharing sw / demo software
- Trojans that are delivered or downloaded in e-mail
- In free, banner ad-based software - Popups
- The most notorious enabler of Spyware is Microsoft's ActiveX module

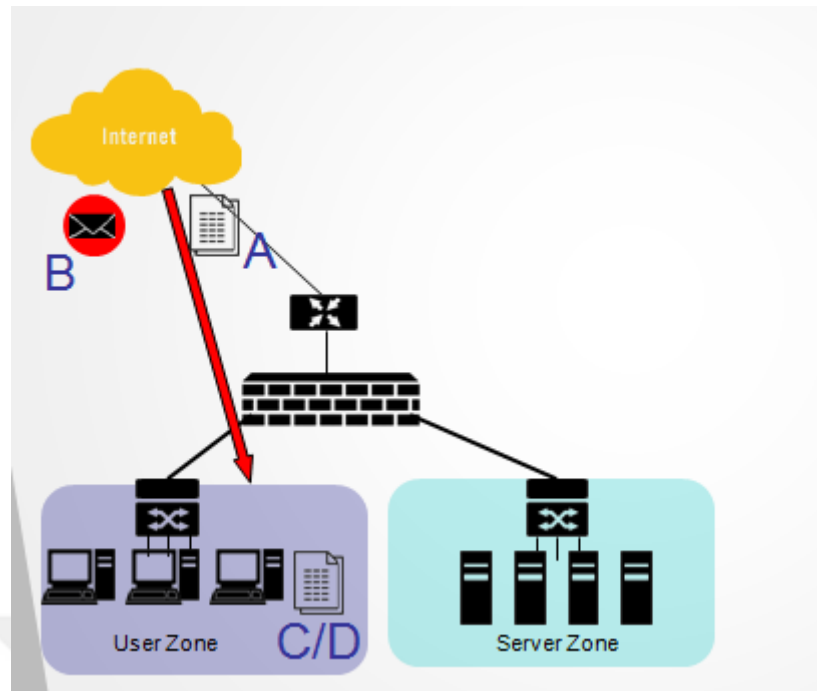


Figure 4 Spyware Infections [14].

2.4 Traditional Network Security and its Inefficacies

The computer networks have always been susceptible to the viruses or hacking attacks that eventually damage the entire data content. Regardless of the recognized impacts of the virus attacks on the entire business framework, organizations are observed to have less or slack readiness in terms of security measures. The LANs are the most vulnerable to the security challenges that have been dramatically increasing with the evolution of internet [38,39]. [40] has documented these threats as the intellectual method of data leakage, data theft or data manipulation as well. It has resulted generating concerned situations across the organizations and even the government that needs the deployment of the most efficacious solutions in the most effective manner. However, the traditional measures are somehow unsuccessful in meeting the expected level of security in a sustained manner.

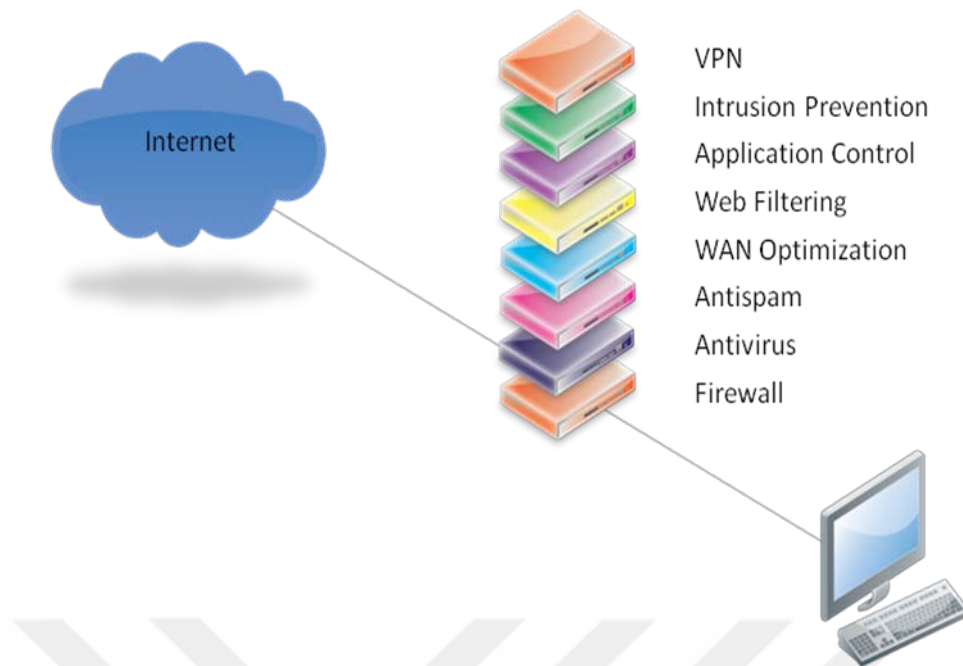


Figure 5 Traditional security framework of Network [40].

It has been established that the organizations deploying different measures of security tend to have significant knowledge of the essentials of security. However, it is also noted that the deployment of a particular solution facilitates only specific service delivery, rather than governing the security of the entire system against all types of attacks or virus threats. For instance, the figure above represents the connectivity of internet and user's computer with an integrated Firewall system. Even though it is going to provide security against the malware or certain hacking attacks, yet the system is not proficient enough to deal with the added elements of content filtering, intrusion prevention, application control or others [13]. Having a unified system seems the most important need of the time; however, the proceeding section presents the respective inefficacies of the traditional security approaches in an individual manner.

2.4.1 Anti-virus as a Security Tool

Anti-virus is disregarded as a potential security tool for the business network. These products are not designed in accordance with the multi-faceted security threats of today's networking. These anti-virus products can be an essential element of the

defensive mechanism against the security threats, but it can never be an entire security system on individual level [33,41]. The main reasons of inefficacious anti-virus system are listed as:

- The system is capable of dealing with the formerly highlighted and recorded threats. It works based on the unique patterns that are encrypted within its coding. It is regarded as "Virus Signature" that is basically the governing potential of the tool against threats. Having no potential of tracing the malicious codes in its signature makes it ineffective on the respective threats. As a result, the advancing appearance of threats in an unpredictable manner can never be traced, unless recognized as the signature of the tool.
- Anti-virus tools are observed to be effective only on the recognized versions of the threats. In this regard, it is ineffective on certain polymorphic viruses that are written in a manner to fool the defensive system of signatures.
- In this regard, the technological world has noted certain security measures among the vendors. For instance, if a particular malicious entry is observed over the internet through the appearance of Vulnerability window. The system of anti-virus initiates spotting and analyzing the virus to define a signature for it; meanwhile, the virus is on its way. If the appropriate signature is formulated, the virus gets stopped, and the signature is floated across the distributors. However, not all the vendors are efficient enough that results in infected computer systems far before the formulation of the signature.
- Most importantly, anti-virus is influential over the viruses that reflects its inefficacy of being a potential defensive system. The internet world has numerous forms of threats or attacks, including the severe threats of botnet attacks, key loggers, drive-by downloading, root kits, and others as well. Not these all prospects are spotted with the limited potential of anti-virus solutions [33,41].

Consequently, it leads to the assertion that the security needs of the today's computer networks demand layered defensive mechanism.

2.4.2 Integration of Firewall

Firewalls serve as the security tool over the business networks by means of closing the superfluous ports over the servers, along with applying certain routing rules pertaining to the spotted requests of DDoS. Nonetheless, these firewalls are contended to have inefficacies of inspecting the packets received in terms of malicious codes or malwares. Besides, these firewalls are also inefficient in comprehending the objective or agenda of the end-users over the server [34,42]. It is asserted that if a port is granted accessibility permission, there are certain chances of letting the malicious codes enter the server that are basically disguised as authentic traffic; yet, these are the basic tools of hackers to intrude into the servers of business dealings without letting the target realize, unless damage has been caused. Therefore, the deployment of firewalls as an individual security solution seems not a vigilant attempt of securing the business network.

2.4.3 Deep Packet Inspection and Intrusion Prevention

It facilitates the security element of filtering the content of packets of the information. This particular inspection is carried out at the application layer of the system. This security solution has expertise of dealing with the threats associated with the content of the packets, including the processes of spotting, identifying, classifying, rerouting, or even blocking certain data packets over the servers. These tools provide peer-to-peer security in terms of data transfer and communication across the online networks [43,44]. However, there are certain limitations that ascertain the avoidance of implementing an individual level security framework of Deep Packet Inspection. This security solution is inefficient in dealing with the extreme cases of buffer overflow, certain malware detection, and the DDoS attacks as well. It has also been asserted that this particular security approach disrupts the performance of existing measures of firewalls or anti-virus solutions within the system [13]. There are periodic update needs associated with the sustainability of these solutions that tend to affect the credibility of its optimal performance.

Consequently, it results in decreased speed of the system that is unacceptable with respect to the competitive needs of the marketplace.

2.5 Unified Threat Management - UTM System

UTM is regarded as the mostly adopted comprehensive solution, which has been the primary defensive gateway against the treat-related concerns of the organizations. Theoretically, it is the evolutionary form of traditional security tool of Firewall as an all-inclusive solution, which is potentially capable of facilitating the business network in different aspects. There are the essential constituents of firewalling, antivirus, intrusion detection systems, anti-spam, content filters, VPNs and other load balancing elements as well, that are unified to deliver comprehensive protection to the network [18,19,20,21 and 22].

UTM acquired the acceptance as the most efficient security system since 2004. The potential of UTM is governed from its widely adopted implementation even in the virtual world. Therefore, the technology of UTM system is affirmed to have the attribute of mature enough to deal with the security needs of the large-enterprises as well. With respect to the security needs of the elements of the enterprise system, diverse products are integrated within a single framework in a unified manner that eventually manages the entire security related activities of the business sensitive data, and even the personally identifiable information of the involved stakeholders of the business domain [18,19,20 and 22]. According to the study of [18], UTM system facilitates the security needs in terms of yielding faster updates related to the dynamically changing environment of the internet world. The prospects of threats or malicious attacks have increased with the increasing advancement in the technology of internet. UTM system makes it a success to eliminate the appearing False Positives over the networks of the businesses.

2.5.1 Categorization of UTM Systems

2.5.1.1 Equipment Types

Considering the type of equipments, UTM is categorized as Loosely-coupled UTM and Tightly-coupled UTM. If the UTM is tightly-coupled, all the instilled security functions are provided by the same vendor, while there are different or multiple vendors of the security related functions in Loosely-coupled UTM. There is a significant role of the management of the UTM components and the configuration patterns as well.

2.5.1.2 Technical Architecture Type

On the other hand, UTM is also categorised based on the technical architecture into three types.

- At first, the architecture of UTM is Firewall based, along with certain other security components. However, the addition of new elements makes the performance efficiency of the system declined.
- Secondly, the architecture of UTM is IPS-based (Intrusion Prevention System), which includes an integrated framework of security tools in a unified manner.
- With respect to the third type, the architecture is regarded as Unity Threat Management as it facilitates ideal performance with its adjustable functions [20,45].

2.5.1.3 Integrated Technologies Type

Regardless of the architectural prospects of UTM, the typical technologies of five types are instilled within the UTM systems.

- Complete Content Protection - CCP

This technology makes the UTM performance improved as compared to the impacts of deep packet inspection and state detection. It is based on the fact that it has the potential of real-time restructuring the data into objects in between the network layer

and the application layer of the Gigabit Ethernet. Moreover, these restructured objects are scanned along with being analyzed by means of the library feature of dynamic update [20,45].

- Application Specific Integrated Circuit -ASIC

This particular technological element performs efficiently than general CPU in terms of magnitude that is attained based on the solidification of the special optimizing algorithm. Accordingly, it yields efficient feature matching rather than security prospects [20,45].

- Customized Operating System

The customized prospect integrated with respect to the operating systems facilitates the UTM systems with streamlined operations. The firewall performs efficiently, and the speeding up module makes the content filtering and hardware accelerating performance enhanced as well. Accordingly, pipeline managing is also performed in an efficient manner in terms of intelligent queuing [20,45].

- Close Pattern Recognition Language - CPRL

It facilitates the protection of the content in a comprehensive manner by means of accelerating the calculation programs. As a result, the entire processing efficiency of the UTM against the threats or malicious attacks is significantly improved [20,45].

- Dynamic Threat Prevention System - DTPS

It primarily facilitates improved accuracy of detecting the threats within the systems that are usually unknown. It is carried out on the basis of the accumulated performance procedure of testing and tracking all the security links, along with the heuristic scanning and detection engine's anomaly checking as well [20,45].

2.6 Performance Analysis of a Unified Threat Management System

According to the research of [46], UTM systems are observed to have certain performance flaws. The observations reflected that the integration of multiple security tools or solution in a stringent manner could not yield productive and proficient outcomes. There is a need of optimized integration of the security tools at system-level to ensure the high-performance delivery of UTM. In this regard, the study has proposed a processing scheme based on the integration of the protocols; in terms of analyzing the Free Scale MPC8572E network processor. As a result, the performance outcomes of the UTM have been increasingly efficient as compared to the outcomes of the stringent integration of the security components.

The study of [22] has studied the essentials of UTM, focusing on the technical constraints of UTM based on its multi-core technology. The deployment of multi-core UTM is regarded as the most efficient technology, if the constraints are mitigated that is ensured by the deployment of SonicWall Solution of UTM. The notable constraints are:

- The system's architectural inabilities of dealing with the multiple processes of multi-core UTM

In this regard, the operating system architecture is needed to be changed and developed in terms of adding the management elements of memory, timer, and file-functioning.

- Difficult Scheduling of UTM services

In this regard, it is ensured that the system is capable of dealing with the intelligent scheduling of parallel service while executing the UTM system in parallel mode. In serial mode of performance, the prospects of bottleneck are mitigated by allocating the resource in accordance with the resource occupancy of the system.

- Efficient detection at application layer

During parallel mode of processing, there is a definite bottleneck appearance in performance of the security solutions instilled within the UTM system. Even for single threat detection, the entire system is involved that ascertains the increased resource consumption. Therefore, the efficient detection seems dubious that needs to be improved.

- Alignment of the performance of the multi-core elements with the deployed platforms and software design

The performance efficiency of the multi-core UTM systems is greatly dependent on the quality service delivery of its constituents [22]. However, it has always been a concerned situation to deploy the proportional products range within the entire framework in relation to the credibility of the software.

With respect to the successful implementation of UTM for the purpose of secure networks, the study of [11] has asserted that there is a significant role of the strategic alignment of the implementation policies with the ICT governance. Being a technological solution, UTM system offers incredible advantages to the security related concerns; however, efficient approaches of the deployment need to be considered to enhance and sustain the performance outcomes.

The study of [19] has explored the security challenges of the cloud in terms of determining the potential efficacy of the UTM in meeting the security needs of the cloud. With respect to the management of the data, the performance of cloud is regarded as the most efficient one. However, the technological vulnerabilities have influenced the performance of the cloud as well; thus, the needs of security solutions are ascertained at all the levels [47,48,49 and 50]. In this regard, [19] have analysed the implications of UTM system in mitigating the security related concerns of the cloud. The interface of UTM was positioned as the primary interface while accessing the data on the cloud. The interface of the UTM entailed multiple interfaces, based on firewall infrastructure of UTM system. However, the database traffic over the cloud was observed not to be aligned with the UTM system, as certain delays in queuing the requests were observed. As a result, it has been established that certain cases of bottlenecks are also observed with UTM Systems as it is potentially applicable for small and medium sized enterprise networks.

On the contrary, the study of [45], has presented a holistic approach of assessing the credibility of UTM systems in delivery security of the business networks. The holistic approach of NAC-UTM (Network Access Control) reflects that it is capable of securing the intranet topologies, along with governing the throughput outcome of the UTM systems. It has been evaluated that the system is aligned with the security needs of the networking. Considering the case of hackers using fake IP addresses or

login credentials due to certain configuration errors, the NAC-UTM promptly spots the changed or manipulated IP address and report to the respective authority to deal with the false positive. However, it has also been established that the system demands the configuration decisions to be based on intelligent system.

2.7 Next Generation Firewalls (NGFW)

Next Generation Firewalls represent the concept that is based on the extension of the traditional firewall systems. With the traditional firewalls, the network system is always vulnerable to the threats of data theft, data breach or data manipulation, as the recent advanced level of expertise has raised the level of attackers' potential. In such circumstances of ensuring the technological security needs of the businesses, there is a definite need of the most advanced levels of protecting Firewalls [1,2,3,6 and 23], like Next Generation Firewalls - NGFWs. These firewalls (NGFWs) being regarded as next-generation are observed to have significantly improved performance as compared to the traditional firewalls. There are additional elements of packet filtering, Virtual Private Networks, Intrusion detection, URL blocking and multiple other security essentials of the network.

According to [51], NGFWs are the security systems against the sophisticated attacks over the networks. These firewalls have the added potential of security policies implications at all the levels, including the application layer, the protocol and port levels. These firewalls systems (NGFWs) encompass the capabilities of firewall for the entire enterprise system, intrusion prevention and the controlling essentials required at application level. As compared to the traditional firewalls, these NGFWs are proficient in terms of added value of decision-making capabilities as well. The firewalls are capable of comprehending the volume of web traffic that is the main source of malicious attacks or hacking attempts of the users. Accordingly, it gets easier to take decisions of either blocking or allowing the traffic flow, considering the prospects of exploitation vulnerabilities of the web traffic [51,52].

2.8 Performance Comparison of UTM and NGFW

Observing the performance matrix of both the UTM (Unified Threat Management) and NGFW (Next Generation Firewall), it is noted that the prime purpose of both the systems is to secure the entire business network against the hacking attempts of data theft, data manipulation, or even the collapse of the entire network. However, certain notable differences are still there that make the implementation of the respective system varying based on varied objectives of the business. At first, the UTM systems are affirmed to serve the security needs of the network in an inclusive manner. The system entails all the essentials of firewalls, Intrusion prevention, anti-spamming, anti-virus, and other essential of content filtering, blocking traffics, and others. However, with respect to the performance efficacy of NGFW, it is noted that these solutions are mostly having specific objectives with respect to the needs of deployment. It reflects that the system of UTM provides the security in the most efficient manner that is in accordance with the sustenance of a business network.

In accordance with the report of [53], it has been established that the NGFWs are not UTMs, as UTMs facilitate the needs of streamlined installation of the security system that is flexible in terms of concurrent updates of the security tools in an inclusive setting. With respect to the infrastructure prospects of NGFWs, it is affirmed that these systems offer no maintenance or update related functionalities. Accordingly, it makes the NGFWs context-specific, while UTMs have the advantage of adopting to levels of the security required. The deployment of NGFWs is not feasible for small and medium sized businesses as these business sectors entail potential chances of demanding the business entities to respond to the uncertainties prevailing due to the advancements. Therefore, UTMs are the most preferred security solutions for the business enterprises, aiming at the attainment of significant amount of competitive advantage in the respective sector [53,54]. Most importantly, these UTM solutions facilitate the businesses in terms of securing their competitiveness within the marketplace, as the data breaching is mitigated, malicious attempts of the hackers are promptly detected and blocked at all the levels.

CHAPTER 3

RESEARCH METHODOLOGY

3.1 Introduction

The chapter is aimed at discussing the methodology that was adopted for the successful accomplishment of the research objectives; in this account, diverse efficient technologies were used by the researcher. In particular, “Oracle’s virtual box” was used by the researcher to establish the virtual or computer-generated environment for testing the security potential of multiple open source UTM systems. It is significant to bring into the notice that the computer system that was used in this regard had the certain specifications, i.e., Core i7 processor (CPU) with 8GB RAM. These setting had remarkably assisted the researcher in evaluating the performance potential of diverse software solutions of UTM. In this regard, the researcher had put the focus on particular attributes of UTM that include, VPN (Virtual Private Network), application filters, content filters, firewalls, and intrusion detection systems. The detailed representation of the systems and software that were used in testing the performance attributes of UTM are discussed in the proceeding sections. In particular, the solutions that are described in the below manuscript include SONICWALL unified threat management solution, SOPHOS unified threat management solution, and WatchGuard unified threat management solution, and Palo Alto Network Solutions. In addition to this, the platform that was used for creating virtual environment, i.e., Oracle VM VirtualBox is also discussed in the following section.

3.2 Oracle VM Virtual Box

Oracle VM Virtual Box is an open and free source hypervisor for x86 computers that are currently being manufactured by Oracle Corporation. One of the greatest qualities of Oracle VM Virtual Box is that it can be installed on multiple host operating systems including Open Solaris, Solaris, Windows, OS X, and Linux. In particular, the recent report of [55] has revealed that Oracle VM Virtual Box is nothing more than the cross-platform virtualization software that facilitates its users to extend the capability of their computer systems; thereby, enabling them to run multiple operate systems, simultaneously. It has been established that Oracle VM Virtual Box is specifically designed for IT developers and professionals, as it is ideal for deploying, demonstrating, developing, and testing solutions across multiple platforms on a single machine [56]. One of the noteworthy characteristics of Oracle VM Virtual Box is that it is compatible with diverse systems, i.e., Oracle Solaris systems, Linux, Mac OS X, and Windows.

In the current study, the researcher had adopted Oracle VM Virtual Box because it is easy to install, user-friendly, and light in weight. Apart from this, the researcher also had to perform a test on different UTM software; therefore, there was a need for highly efficient and flexible system [56]. Therefore, the researcher had chosen Oracle VM Virtual Box to feasibly install and run diverse software to assess their performance in providing fool-proof security on a corporate level. It has already been mentioned that the researcher had to carry out tests on diverse UTM software; therefore, there was a need to create isolated environments to adequately analyze the performance of each of the selected UTMs [55]. In such circumstances, the researcher had found Oracle VM Virtual Box as the most optimal options, as it offers an opportunity to the professionals to closely examine the attributes of their desired software, in an isolated and high-performance environment.

It is significant to bring into the notice that regardless of providing diverse efficient performance parameters, Oracle VM Virtual Box also incorporates various shortcomings. In this regard, one of the biggest issues is associated with the resource overhead due to the full OS layer. This feature has considerable impacts on the performance of the system. In addition to this, Oracle VM Virtual Box do not has

centralized management features that directly limits the number of hosts; thereby, restricting its capability to be deployed in the large sized infrastructures. In addition to this, it is also observed that this platform is only applicable or compatible with very few numbers of third-party applications and tools [56]. However, the intensity and impacts of these limitations are not greater than the inclusive features and efficient performance outcomes of Oracle VM Virtual Box.

3.3 UTM Solutions Used in the Study

In a world crowded with competition and struggle for survival depends on several factors including performance, price reliability and quality of service as well, there are many unique security products that have been characterized in recent years at the level of the community and the widespread global networks, and have recorded a very significant presence in the hearts of users. Besides, these solutions have won the acclaim of specialized criticisms as mention on Gartner Magic Quadrant for Enterprise Network Firewalls [www.gartner.com]. The selected ones include the following:

- SONICWALL
- SOPHOS
- WatchGuard
- Palo Alto Network

3.3.1 SONICWALL Unified Threat Management Solution

SonicWall has developed and offered a high-tech unified threat management solution to the small-to-medium sized enterprises. The software solution is aimed at providing effective security and considerably high levels of performance characteristics to the businesses. The researcher had adopted and utilized the UTM solution, provided by SonicWall, as it is dedicated to simplify security management while delivering comprehensive protection without affecting the performance of the network [57]. Another reason that was involved in selecting SonicWall provided UTM for this research includes the inclusiveness of the solution. It is due to the fact that SonicWall

UTM gathers all features that are individually used by the organizations and businesses, like application control systems, SSL VPN, URL/content filtering, intrusion prevention, anti-spam, anti-malware, and gateway antivirus.

Unified threat management solution, provided by SonicWall, provides comprehensive security to the businesses and enterprises. It is due to the fact that it integrates all fundamental components that are essential for ensuring fool-proof security. Some of the most prominent components that are assimilated within the SonicWall's UTM solution include anti-spam services, enforced client antivirus, intrusion prevention, gateway antivirus, application control, and content or URL filtering on the highly affordable platform [58].

Besides providing comprehensive security, SonicWall provided UTM also enables the enterprises and businesses to ensure thorough protection and security, while boosting their overall efficiency and performance. One of the greatest reasons that had led the researcher to opt this software solution includes its capability of assessing the traffic, at the same time, across all ports without establishing latency [57]. In this regard, the software makes use of the deep packet inspection technology. Some of the prominent features that show its high-performance capability of this solution include its ability to scan files without caching, regardless of their size [58]. Moreover, the solution is also found to be capable enough to manage hundreds of thousands of synchronized downloads.

Apart from this, the solution also offers an opportunity to the businesses to get remote access and getting benefited from the wireless connectivity. It is due to the fact that the solution provides VPN (Virtual Private Network) access for the devices running on different operating systems, regardless of facing security issues [58]. It is because; UTM filters security related risks from wireless traffic and VPN; thereby, ensuring the integrity and confidentiality of the traffic entering and leaving the network.

3.3.2 SOPHOS Unified Threat Management Solution

SOPHOS provided unified threat management solution was another software based solution that was adopted by the researcher to examine its relevance in protecting organization assets (network, information, etc.). It has been established from the recent report of Sophos [59] that Sophos UTM is one of the most efficient options for simplifying the IT security of an organization without facing any complexity or issue that are often encountered during the utilization of multiple-point solutions. One of the greatest reasons behind the adoption of Sophos based UTM solution was its capability of utilizing multi-layered security technological tools that include the web and email filtering, VPN, IPS, and ATP (Advanced Threat Protection). It is significant to bring into the notice that all of these features combine the simplest admin interface of the industry. Moreover, this solution also offers an opportunity to the organizations and businesses to ensure the trouble-free and cost effective management and installation of the solution. Apart from this, the researcher had also preferred to adopt this solution as it offers complete control to the organizations to prioritise, shape, allow, and block applications [61]. Another commendable feature of Sophos UTM is its regular automatic updates and its true application identification that is backed by a next-generation firewall (i.e., seven layer inspection).

Sophos provided UTM services also play an inevitable and indispensable role in restricting and combating the sophisticated attacks that are impractical to be managed by the firewall. It is due to the fact that UTM combines diverse technological tools for the sake of blocking and identifying the outgoing traffic to control and command hosts. Furthermore, the solution also offers configurable flood protection and intrusion protection system against DoS (denial of service attacks) [60]. Sophos UTM also offers an opportunity to the businesses to stop viruses and spam; thereby, securing the sensitive data from being disclosed or misused. In the contemporary era, wireless connectivity is one of the most desirable aspects of the organizations [61]. Though wireless connectivity helps the organizations feasibly performing their day-to-day tasks, but wireless technology also pose diverse security-related threats to the organizations. In such circumstances, the adoption of Sophos UTM is found to be one of the most effective solutions for the organizations that are intended to protect

their integrity from undesirable security issues. This efficient UTM solution has the capability of setting up the wireless hotspot by the help of using backend SMS, vouchers, or authentication. Additionally, some of the other characteristics qualities of this solution are related to providing protection to the web, web server, and sandbox.

In the context of providing security to the web, the Sophos UTM software plays a commendable role in limiting the utilization of the undesired applications. This feature results in increasing the efficiency and overall performance of the business [61]. Apart from this, the software based solution, provided by Sophos also contributes in protecting the integrity of the web server. It is usually done by the technique of reverse proxy authentication. This characteristic quality offers an added security layer to the applications and network of the enterprises. Along with this characteristic quality, Sophos provided UTM services also holds undeniable importance in preventing the hacking incidents that are performed through cookie tampering, directory traversal, cross-site scripting, and SQL injection [61]. In precise words, the UTM solution that is provided by Sophos is one of the best solutions for the organizations that are intended to protect their networks from unintended security attacks [60].

3.3.3 WatchGuard Unified Threat Management Solution

The third UTM solution that was adopted by the researcher to test its relevance in providing strong and robust security was WatchGuard based UTM solution. It has been established that the solution offers exclusive security to the businesses and organization from the security related issues that are faced by the businesses. These include DDoS/DoS attacks, blended threats, Trojan attacks, viruses, spams, SQL injections, and worms. The researcher had made the selection of this software solution, as it offers additional capabilities that include URL filtering, intrusion prevention, spyware prevention, gateway antivirus, and spam blocking [62]. In addition to this, WatchGuard UTM offers several other security related benefits to the organizations that mainly include: logging capabilities, monitoring, as well as

integrated management for the sake of streamlining the maintenance and deployment of the solution.

It has been established that the WatchGuard provided UTM solution integrate powerful security subscription to offer fool-proof security from malware and unintended security risks. One of the commendable and noteworthy aspects of WatchGuard provided UTM is that it has the capability of managing all security related features by using the single intuitive console. This solution possesses centralized reporting and logging features for providing integrated security features [62].

The researcher had found it appropriate to adopt and use the UTM solution, provided by WatchGuard, as it allows the users to manage multiple appliances or devices from a central location. Moreover, it is also observed that the operations or functionality of the system is dependent on interactive real-time logging and monitoring capabilities. Additionally, the solution also has great significance in eradicating the need of using diverse interfaces [62]. Instead of it, this UTM software solution makes use of a single intuitive interface for managing and installing all security related aspects of the organizational network.

When the capabilities and characteristic qualities of WatchGuard UTM we reanalyzed, it was revealed that, it offers an opportunity to the businesses to ensure the protection of their network infrastructure from emerging and new threats. In more precise words, it can be affirmed that WatchGuard UTM enables the organizations to secure or protect their network by blocking web-based exploits, blended threats, Trojans, worms, viruses, as well as spyware. One of the most notable features of the solution is that it is dependent on highly intelligent architecture for the sake of securing the network and optimizing the overall network performance [62]. While highlighting all of these performance capabilities of WatchGuard UTM, it is important to note that information security practices do not affect the normal performance attributes of the network. In other words, the security related practices do not disturb the IT activities, like compliance reporting, auditing, and log file management.

It has been recognized from the analysis of the study of [63] that the prominent features offered by WatchGuard provided UTM include DLP (Data leakage

prevention), email security, web content security, gateway antivirus, IPS (intrusion prevention system), as well as state-of-the-art and highly strong firewall. Therefore, on the basis of these findings, it can be affirmed that WatchGuard provided UTM plays a substantial role in providing robust and unbreakable (to some extent) security to the entire network of the organization; thereby, protecting the confidential information from being leaked or mistreated.

3.3.4 Palo Alto Networks

Primarily, Palo Alto Networks (henceforth, PAN) are not termed as UTM, but depending on the equivalent integrated functionalities PAN has been adopted as a UTM based device. These devices are basically facilitating the performance outcomes of NFGWs in terms of assurance of controlled visibility over the users, the used applications, and the content being used across those applications, based on the implication of certain policies. Accordingly, it offers three technological implications of User-ID, App-ID, and Content-ID, which incorporate the prospects of network security.

App-ID:

This category is a five-stage process that eventually classifies the application traffic that is being generated within PAN's operating system. Below is the description of the stages involved in App-ID execution:

1. The traffic is assessed in terms of the policy check that evaluates either traffic can be permitted at source/destination. If the policy does not permit, the traffic request is dropped eventually.
2. The application is detected on the basis of the signature that turns out to be a unique session. Besides, the standard of the ports is also assessed by means of the identified port-number.
3. If there is any detection of SSH or SSL encryption, the decryption of traffic takes place based on the decryption policy.
4. Decoders are also there within the policies of App-ID that are destined to determine the use of tunnelling applications like BitTorrent over HTTP. Besides, port

mapping is also carried out for FTP and NAT traversal. It turns out to be ALG-functionality that is incorporated with the NGFW prospect of PAN.

5. For the applications that are not identified through protocol and signature analysis, behavioral or heuristics analysis is carried out.

User-ID:

Directory services are integrated within the network of PAN's NGFW, in order to map the users over the network and the respective policies as well. Afterwards, the device maps the user with the IP address for the enforcement of policies.

1. In order to monitor the service, a user-ID agent is required across the integrated PAN-OS or some window-based server. Primarily, the details of log-in events are noted on the domain controllers or MS Exchange Servers. The login events might be Kerberos ticker renewals or grants and the print or file server connections. Accordingly, there is a need of correct configuration of logging details that are required across the target devices.

2. If the enterprise environment is observed to have regular changes in IP addresses, client probing is crucial. Probing is carried out by means of WMI - Windows Management Instrumentation. Accordingly, there are certain limits to probing as well, since NetBIOS probing demands external User-ID agent. Probing takes place every 20 minutes, validating the IP authenticity of the users. Even if there is a certain detection of an IP address with no User-ID, probing makes it easier to map the newly generate User-ID with the IP address in a prompt manner.

3. Recognizing the users- mapping across a virtualized environment, there is a distinguishing source-port that makes it possible to use the same IP address by multiple users. However, the element of user-to-address mapping is not present that requires PAN's agent to be deployed across the target device for being a mediator.

4. Syslog is identical to server monitoring that is regarded as the most effective approach for NAC "Network Access Control" mechanisms within a networking environment.

5. Log-in attempts from the users are enforced to access web-based services by means of the security mechanism of Captive Portal. It depends on the web browsers being used by the users.

6. More specifically, if there is a need of directly mapping the users based on VPNs, Global Protect serves the intended aspect when integrated with User-ID.

Content-ID:

It refers to the general functionality offered by PAN in terms of DLP, Control, and Command detection, URL-filtering, and anti-malware services. As its name suggests, it tends to identify the patterns within the content of the traffic across the databases of private Malware and Susceptibility research, WildFire, Microsoft Active Protections Program - MAPP, and custom signatures as well.

1. Basically, threat prevention is ensured with respect to the enforcement of security policies.

2. If there is any potential unknown Malware attack, WildFire is integrated with the automatic detection and creation of the signatures in a virtual environment. Multiple files are executable under WildFire or accessible that keeps the suspicious activities observable. Once identified as malicious, URL is added to the file and thus updated to the database of PAN. Clients of WildFire are facilitated with signature generation in merely 5 minutes, while threat prevention-subscribed clients receive the updates to the antivirus every 24-48 hours.

3. Besides, WildFire is facilitated in two formats of cloud-based and hosted environment, like the private data remains intact to the private networks and other detected threats are headed to the public clouds. Even email links are also analysed with WildFire. Below are the supported files listed:

- Android Application Package files - APF files
- Java Archive - JAR
- Portable Document Format - PDF
- Adobe and embedded flash files content
- Portable Executable files inclusive of .dll, .exe, and .FON.
- HTTP/HTTPS links
- MS-Office files

The firewall of PAN is manageable locally and even centrally, requiring Panorama for accessing the centralized system of security. Even though PAN is not genuinely a UTM system, its firewall implications are contended to present the notions of being a

strategic infrastructure component of network security. PAN is affirmed to mitigate the limitations of traditional firewalls that are observed to classify the traffic based on certain protocols and ports' dependency. These limitations used to result in ease for the internet users to by-pass the security system in terms of using SSL, and non-standardized ports, and hopping ports as well [64,65,66 and 67]. The report of [68] has elaborated the visibility attribute of PAN in facilitating the administration needs of network security. The elements governing the visibility of PAN include the following:

Application Command Centre - ACC: The business needs of keeping the network performance and the associated element aligned with security are facilitated by ACC. ACC is based on the graphical illustrations that present information regarding the overall network activity. The reported activities include URL categories, applications, data and threats, in particular. Even a new application entry is also accessed with all its details of users, features, and the instilled security rules as well. ACC tool of PAN enables the administrators to make increasingly informed decisions regarding the policies of security.

App-Scope: PAN is integrated with the provision of user-customizable and dynamic view of the applications being used, the traffic over the network and the extent or probability of threat activities in a real-time environment.

Log Viewer: There are real-time filters that facilitate the prompt forensic analysis of all the sessions over the network. Accordingly, the analysis is presented in report format as well, which enhances the credibility of the PAN's functionality.

CHAPTER 4

EXPERIMENTAL WORK

4.1 Introduction

The study is focused comparing the network security devices of SONICWALL, SOPHOS, WatchGuard, and PAN's PA-series, alongside the challenging assessment of the best-suited device application for an Imaginary Organisation's future network. In order to acquire the best study outcomes, the researcher has ensured the assessment of the network requirements of an Imaginary Organisation, so that the best solution can be implemented to acquire the desired outcomes. Consequently, recognising the needs of migrating the existing infrastructure with the new proposed one, the platform of migration is based on the best-practice implementation plan regarding the resources. The Company's existing framework, and the implementation of the selected security solutions have been assessed and compared on the basis of ease and accessibility; thus, mitigating the prospects of any possible human error. As mentioned above, the proposed solutions have been tested based on the Oracle Virtual Box environment.

4.2 Migration Plan

The traditional firewall systems that are functional within an Imaginary Organisation are anticipated to be upgraded from the port-based environment to the contemporary application-aware security framework. In this regard, the process of planning involved at every stage is essentially carries out to avoid errors. Therefore, PDCA cycle has been completed successfully.

4.2.1 PDCA - Plan-Do-Check-Act

PDCA implementation facilitates the success of a project in a structured and planner manner. PDCA entails the attribute of cycling multiple times throughout the stages deployment, if required to enhance the outcomes. Below is the migration planning of an Imaginary Organisation's network, in terms of the first cycle implementation of PDCA.

Plan: At first, the process of auditing requirements of the current firewall settings is carried out that includes the essentials of configuration, policies and services, along with the identification of general concerns of security.

Do: Afterwards, the former services and policies are then converted into the new proposed platform. It is followed by the implementation of the new features.

Check: Once the features of the new solution are implemented, the performance delivery is tested.

Act: Accordingly, decisions regarding any possible changes or adding any new details is taken based on the preceding stage.

Once the preparation phase is completed, PDCA is then employed for the implementation phase of the proposed solution, which is described below:

Plan: Planning regarding the actual migration and testing of the implementation in physical terms is carried out.

Do: The security framework is then implemented.

Check: The new implementation undergoes testing in correspondence with the intended objectives.

Act: Changes are made accordingly, if needed.

Even though the potential of PDCA cycle is greatly synced with the security needs of the an Imaginary Organisation; however, the study has directed its focus across the first stage of the preparation stage of the migration plan. As a result, the planning stage has led to the generation of the most favourable options of enhanced network security.

4.3 Next-Generation Firewall (NGFW)

Based on the reviewed aspects of NGFW, it has been established that NGFW fosters the increasingly advanced features of security in an integrated manner. The implications of NGFW are not widespread across the industry that instils the aspect of different interpretations of NGFW.

4.3.1 Essential Aspects

NGFW is entitled to have the following features essentially:

1. It has been recognised that Integrated IPS is the basic featured element, but with enhanced performance outcomes as compared to the traditional firewalls. It has been identified that the IPS requirements of NGFW need not to be based on stand-alone perspectives, as practiced in traditional firewall settings. Both the firewall and IPS outcomes are anticipated to be attained in an integrated manner, resulting a single packet outflow in terms of rules' enforcement of IPS's input through firewalls.
2. Awareness regarding the use of best-practice applications is crucial that requires the inspection of the application layer. If the enterprise's network is capable of determining the applications needed for controlling the traffic across the application layers in a granular manner, potential opportunities of enhanced security are ascertained.
3. Extra intelligence is also demanded for implementing the rules on the basis of the information from the external sources, like *Active Directory*.
4. NGFW ensures centralised management that is the prime need of an enterprise network system.
5. The information regarding a secure network needs to be accessed at administration level that seems feasible if the system offers easy-to-read tables and graphs regarding the entire processing. It is referred as logging that instils the focused aspects of Graphical User Interface in a well-structured manner. Typical firewalls are observed to overlook this logging management, but NGFW recognises the benefits of troubleshooting, and monitoring of the

threats across the network as well. The centralised management is capable of monitoring the details of applications in use, along with the users as well.

4.3.2 Awareness regarding the Contextual Aspects

NGFW has application awareness as its core element that incorporates the needs of IPS functionality in a feasible, compatible, and accessible manner. It has been established that even though application awareness was misinterpreted in terms of avoiding its importance towards the system's needs of security, its potential has now been improved in terms of context awareness. Context awareness includes all the details of applications that are installed and being used across the enterprise.

4.3.3 Implications of UTM Functionality

UTM and NGFW have the major difference of integration that is much advanced than the technological collocation for the throughput of multi-gigabit information across the system; moreover, even the security breadth is not impeached. Previously, the main concerns were about the internet connectivity only, rather than being concerned about the security of the network. It has been due to the increasing cloud technology that brought in the challenges of security. It has been comprehended that the functionalities of UTM in an integrated manner with NGFW are somewhat varying, depending on the service providers.

4.3.4 Advantages of NGFW-UTM

NGFW are not innately UTMs, but the implications and the resulting performance outcomes are contended to be of similar or equivalent nature to a considerable extent. High throughput is expected along with the element of advanced protection in terms of activated layer of application. Even its single device is appropriate to fulfil the networking needs of the entire enterprise, requiring reduced and simpler management; thus, entailing the prospects of scalability. Below is the

discussion regarding the devices to be deployed to meet the security needs of an Imaginary Organisation's network.

4.4 Current Network of an Imaginary Organisation

The targeted office at an Imaginary Organisation is noted to have typical firewalls' network connectivity and security deployed across the domain that is observed to be of Juniper's type. Currently, the offered services at an Imaginary Organisation's office include the domain controlling for the environment of Active Directory, and mail service management through MS Lync Server. The section below presents the current performance outcomes of an Imaginary Organisation's network system:

Juniper SSG140

An Imaginary Organisation has employed the system of Juniper SSG-140 that is running over the ScreenOS (Operating system). Even though SSG140 has certain features as NGFW, its efficacy in terms of the performance is not up to the mark. It has IPS integration, but the signatures generation and inspection is limited that in turns limits the performance as well. These IPS facilitations are referred as IPS Lite, when compared to the NGFW's offered full IPS. IPS is referred as the essential element of a UTM system that employs protocol detection of anomaly based and protocol signatures that are stateful. These services or protocols are available on paid-terms, along with having different provisions in different packages. It has been noted that Juniper has taken the decision of moving its operating system from ScreenOS to JunOS; thus, presenting the perspective of ending the subscription offered for ScreenOS. Moreover, there is another gateway security providing service as Blue Coat ProxySG that entails the security elements of anti-malware, SSL proxy, application awareness, user-ID integration, and prevention of data loss. This particular device has been the need due to the unavailability of this particular gateway security with SSG-140.

4.5 Future Network for an Imaginary Organisation

The above discussed functionalities at an Imaginary Organisation's office clearly indicate that the office has the need of upgraded network infrastructure to mitigate the potential limitations. It has been decided that the company's network infrastructure is going to be transformed into an enterprise model that would offer high prospects of scalability, flexibility, and availability. The upgraded system designed to serve 200 users with advanced security services . The upgraded service plan intends to offer the packaged areas as:

- File Server
- Active Directory
- Print Server
- Pulse Server
- Finance System
- Sales System
- FTP-Server
- Service Desk System

It has been anticipated that the new migrated infrastructure at an Imaginary Organisation will have on-site hosted services. Below are the topology details regarding the migrated option for an Imaginary Organisation in terms of improved infrastructure of the network.

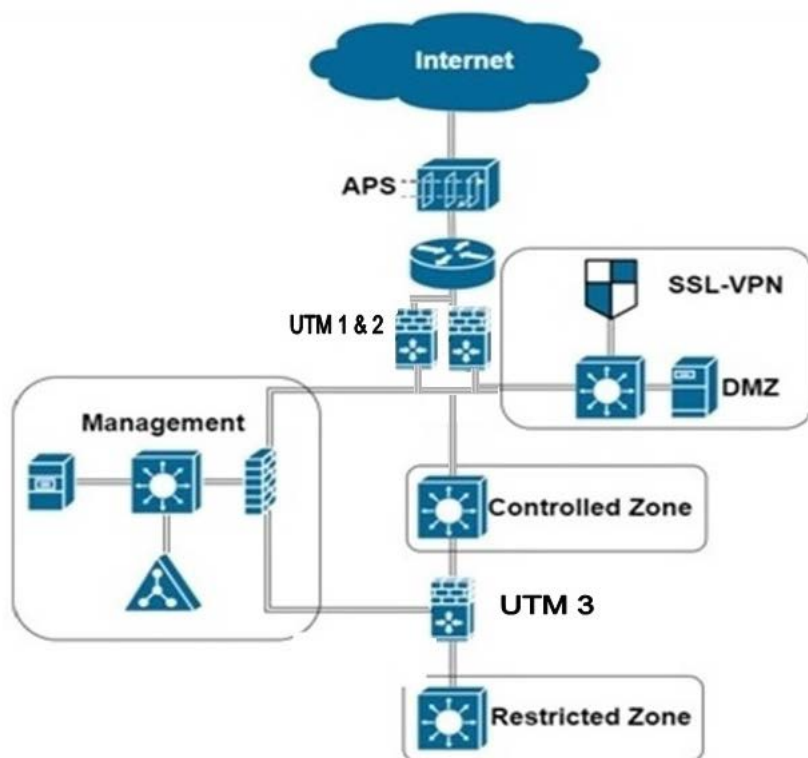


Figure 6 Proposed Topology

The devised topology for enhanced network security at an Imaginary Organisation has couple of security zones that are newly introduced. Logically, the entire network is going to have segmented into four regions that is illustrated in the figure above. All the zones are affirmed to have distinct policies of the integrated element of the devices installed across the domain. Below is the detailed functionality of the proposed system:

Controlled Zone: It represents the basic network that would be operational, internally. Employees, print-servers and the printers, and service desk system are the essentials of this particular zone.

DMZ: It is going to incorporate the shared resources all across the domain. The shared connection in between the internal network and the internet service will be focused in this zone, including the web-server, and SSL-VPN server.

Management Zone: Syslog and Active Directory are anticipated to be included in this domain.

Restricted Zone: It has been tagged as being restricted due to the data incorporation of high sensitivity that cannot be left uncontrolled. The FTP and File server, Finance and Sales system, and all backup data logs will be stored here in this restricted zone.

4.6 Requirements of the Proposed System

With respect to the data management aspects of the new infrastructure, the concerns of UTM selection need proper consideration. Accordingly, the basic requirements are affirmed to be facilitated as:

Increasingly high availability: In this regard, three UTMs have been employed within the proposed topology. As a result, high availability is anticipated throughout the setup. Where UTM1 and UTM2 placed in parallel to increase the availability and the scalability of the network.

Increased Application Visibility: Being focused on sales and finance areas of business, security needs are crucial to the entire system of the enterprise. Therefore, the application awareness is regarded as the utmost need.

Increased Context Awareness: Aligned with the prospect of application awareness, the system is also sensitive to the context awareness needs of the applications being used all across the network.

High throughput: IPS integration is activated that ensures high throughput at all the levels.

4.7 Implications based on Comparison of Features

In order to assess the credibility of the network security solution for an Imaginary Organisation, comparison matrix proposed by SANS Institute has been deployed that focuses the assessment of NGFWs in a real-world environment. The assessment has been based on the following aspects:

- Ease of use

- Installation aspects
- User interface or Management Console
- Attacks detection capability
- High availability
- Accuracy
- High throughput
- Support mechanism
- Pricing

4.7.1 Platform Testing

Typically, network configuration is carried out through CLI "Command Line interface", but the advancing technologies have resulted in complex or challenging situations for configuration. Therefore, it has been recognised that there is a need of visual platform that would provide all the performance measures regarding the configuration in an accurate and appropriate manner. For the integration of NGFWs and UTMs, the configuration needs are complex, when considered from the perspective of multi-stage implications of network security. Besides, there is another element that is critical to the deployment of challenging security solutions, which is identified to be the assurance of control and visibility of the applications. Even though web-interfaces have long been there to facilitate this particular need of system integration, yet the implications of user-friendly aspects of GUI have not been deployed in an efficient manner. Based on these notions, the performance efficacy of the solutions has been assessed, in terms of the deployed infrastructures.

4.7.2 Initial Configuration/Ease of Installation

The initial configuration of the selected devices seems somewhat identical, in terms of the most important perspective of ease and accessibility. Once mounted and powered, the offered choices of the devices are configured through the CLI or web-interface. The above-mentioned system of Oracle VM Virtual box is connected with the CLI configuration of the devices. In order to configure through the web-interface,

the computer is connected across the web-server through the IP-address configuration by means of the Ethernet connectivity.

4.7.2.1 Palo Alto Network

Networking in Palo Alto Network Solutions is carried out in a top-hierarchical manner

Figure 7, which moves down to interfaces available that leads to the IP address.

PAN-OS	<pre>set network interface ethernet ethernet1/1 layer3 ip 1.1.1.1/24</pre>
--------	--


```
network {
  interface {
    ethernet {
      ethernet1/1 {
        layer3 {
          ip {
            1.1.1.1/24;
          }
        }
      }
    }
  }
}
```

Figure 7 Hierarchical structure of IP interface for Palo Alto [69]

We normally use CLI command such as set network interface , to set up the network configuration of the devices then we will access it using web browser, This is a relatively difficult process to prepare in its general form.

4.7.2.2 SONICWALL

At first, a management session is initiated by means of CLI. The CONSOLE port of the device is attached with the null cable of model that is connected to the serial port of the computer at the other end (Figure 8).

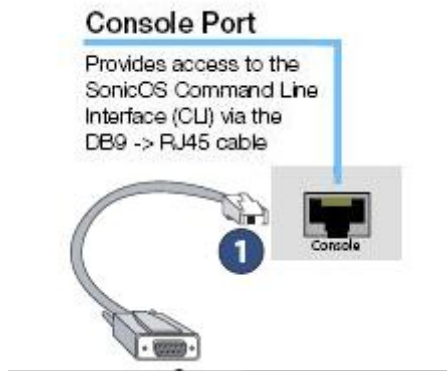


Figure 8 console connection port [70]

It is followed by launching the application of terminal emulation, which ensures the connectivity of the serial port with the appliances. It has been recommended that the freeware program of SONICWALL as "Treaterm Pro" offers stable output capturing from the sessions of CLI. Figure 9 show the obtaining information process of Initial Configuration.

Obtain Configuration Information

Please record and keep for future reference the following setup information:

Registration Information

Serial Number:	Record the serial number found on the bottom panel of your SonicWALL appliance.
Authentication Code:	Record the authentication code found on the bottom panel of your SonicWALL appliance.

Networking Information

LAN IP Address: _____	Select a static IP address for your SonicWALL appliance that is within the range of your local subnet. If you are unsure, you can use the default IP address (192.168.168.168).
Subnet Mask: _____	Record the subnet mask for the local subnet where you are installing your SonicWALL appliance.
Ethernet WAN IP Address: _____	Select a static IP address for your Ethernet WAN. <i>This setting only applies if you are already using an ISP that assigns a static IP address.</i>

Administrator Information

Admin Name:	Select an administrator account name. (default is <i>admin</i>)
Admin Password:	Select an administrator password. (default is <i>password</i>)

Obtain Internet Service Provider (ISP) Information

Record the following information about your current Internet service:

If you connect using	Please record
DHCP	<i>No information is usually required.</i> Some providers may require a Host name: _____
Static IP	IP Address: _____ Subnet Mask: _____ Default Gateway: _____ Primary DNS: _____ DNS 2 (optional): _____ DNS 3 (optional): _____

 **Note:** *if you are not using one of the network configurations above, refer to <<http://www.sonicwall.com/us/support.html>>.*

Figure 9 Initial Configuration [70]

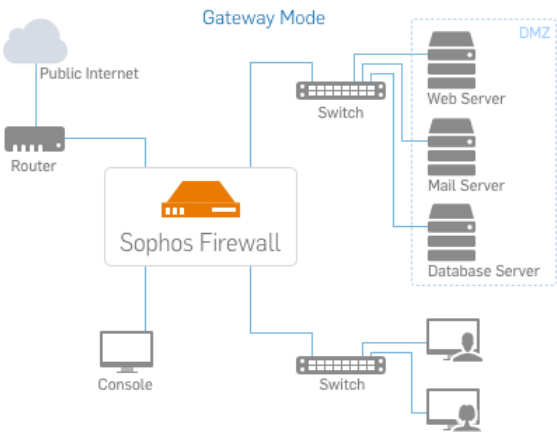
4.7.2.3 SOPHOS

The configuration details of SOPHOS are illustrated in the figures below. These illustrations offer considerably easy of accessibility, if the administrators or users are potentially aligned with the technological implications associated with the deployment of SOPHOS in terms of its UTM/NGFW attributes (Figure 10).

Deployment Mode is the way you want your Sophos Firewall to be positioned in the network.

Please refer the Network Diagrams to choose the deployment mode from the following options:

- Bridge Mode
- Gateway Mode



Progress bar with steps: Deployment Mode (selected), Zone & Network, Access, Email, Date & Time, Summary. Navigation buttons: < > Skip

Figure 10 The configuration details of SOPHOS [71]

Figure 11 represents the basic setup that is required for system configuration:

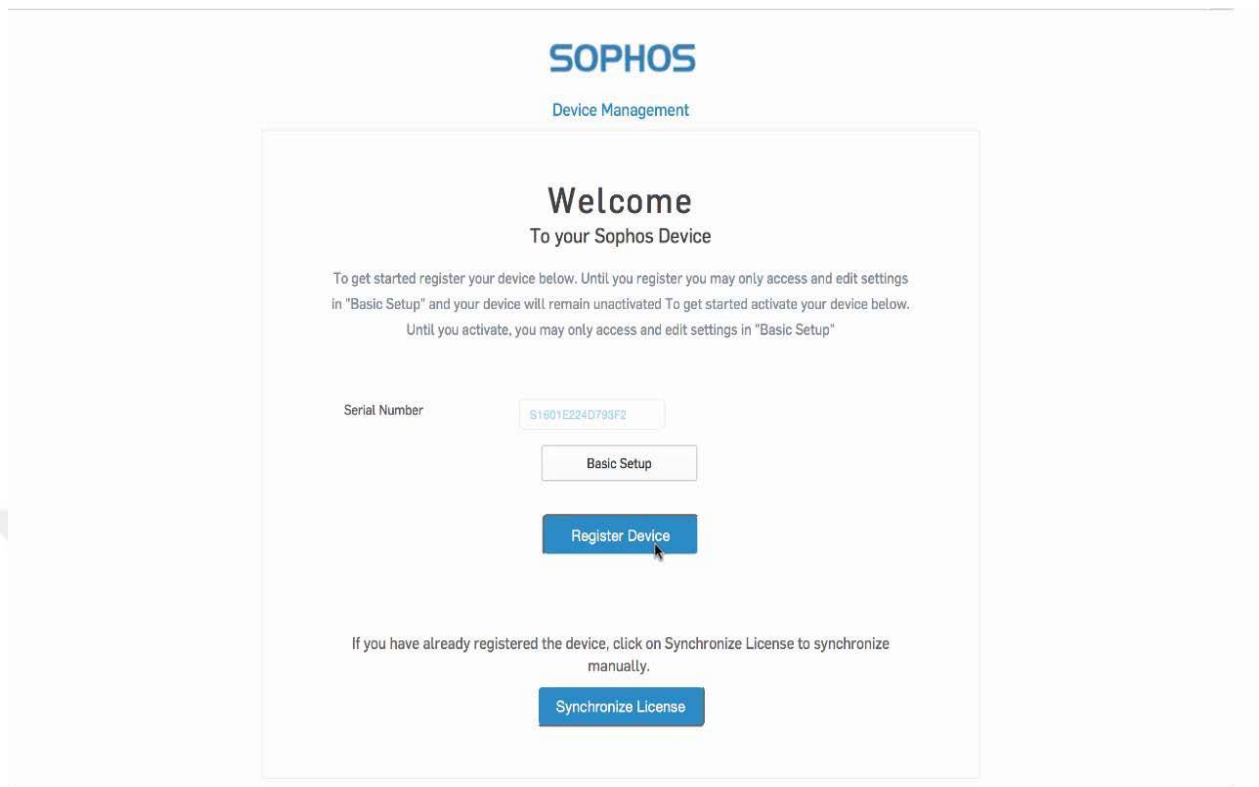


Figure 11 basic setup GUI of SOPHO [71]

Figure 12 shows initial level LAN settings required for the connectivity are:

Port Configuration

<input checked="" type="radio"/> PortA <input type="radio"/> PortB <input type="radio"/> PortC	<input type="radio"/> Obtain an IP from DHCP <input type="radio"/> Obtain an IP from PPPoE <input checked="" type="radio"/> Use Static IP	IP Address <input type="text" value="172.16.16.1"/> Subnet Mask <input type="text" value="255.255.255.0"/> Zone <input type="text" value="LAN"/>
--	---	--

Zone & Network allows you to configure the interfaces on your device, including your DNS settings.

You can select the method of IP assignment as DHCP, PPPoE or Static IP. Before doing this, you must gather the required information of your network schema.

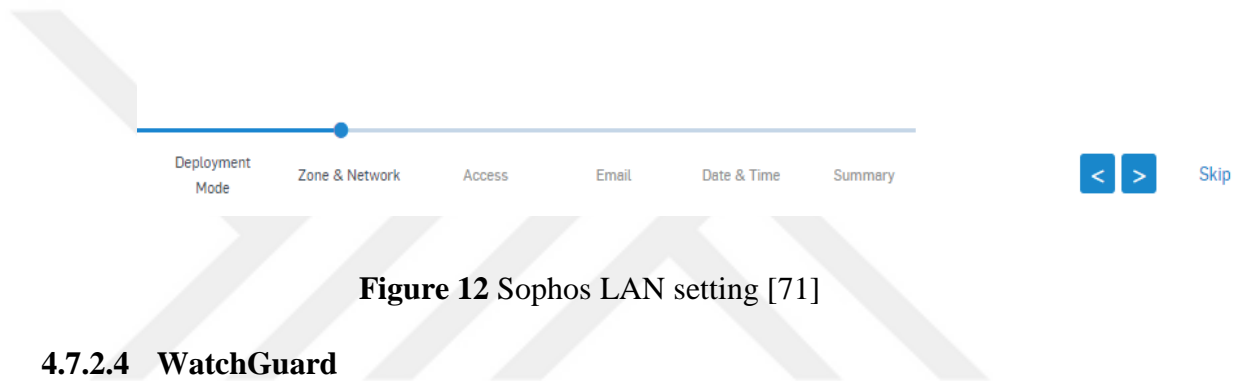


Figure 12 Sophos LAN setting [71]

4.7.2.4 WatchGuard

With respect to the ease of initiation, WatchGuard offers considerable preferences. However, its essentials seem complex to some extent. Figure 13 show the primary devices network setting when you entitial installing the device in our own virtual lab

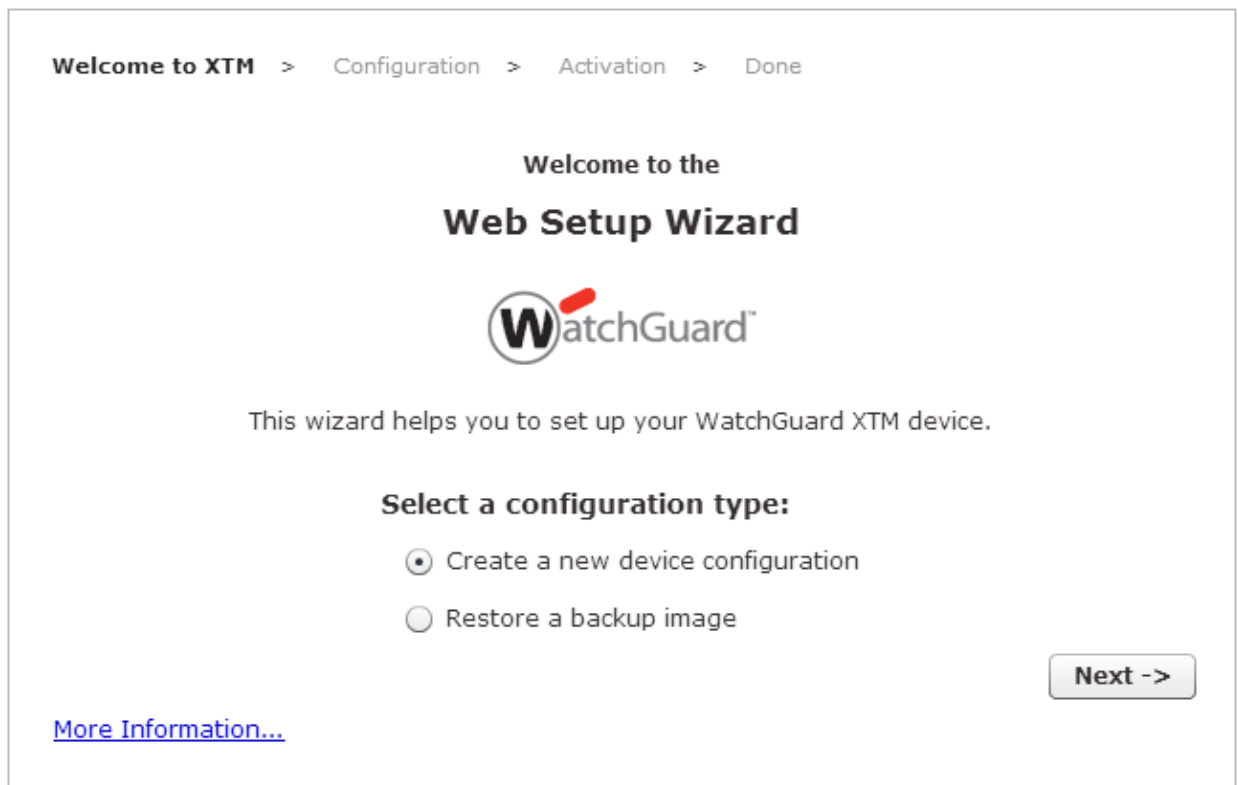


Figure 13 setup GUI of WatchGuard [72]

Figure 14 shows the configuration window for network setting so we can configure the device to meet your network setting in our own virtual lab

The screenshot displays the 'Network Configuration' window for a WatchGuard device. The 'Network Type' is set to 'Single Interface Mode'. The 'Eth0' interface configuration is as follows:

Field	Value
IP Address	192.168.54.60
Subnet Mask	255.255.255.0
Default Gateway	192.168.54.254
Primary DNS	192.168.130.131
Secondary DNS	4.2.2.2
Hostname	wgtraining.local
DNS Search Order	wgtraining.net watchguard.net

Below the fields, there is an information icon and a note: "If you enter more than one domain in the DNS Search Order, each domain name must be separated by a space. The search list is limited to six domains and a total of 256 characters." A 'Next >' button is located at the bottom right of the configuration area. A 'Route Configuration' button is visible at the bottom of the window.

Figure 14 WatchGuard network setting [72]

4.7.3 Web Interface

The web-interfaces of the proposed solutions are compared on the basis of the configuration aspects, mainly highlighting the security features. Accordingly, the comparison is carried out on subjective basis.

4.7.3.1 Palo Alto Networks

The dashboard of PAN is noted to have tunnels, interface configurations, and zones' details as well. Besides, it also has policies feature that facilitates the encryption or decryption of the policies regarding QoS rules, NAT rules, and DoS protection. Even the database of the applications is also visibly configurable that has application filters, URL filters, anti-viruses, and file blocking options as well. Moreover, there is another tab of monitoring the traffic logs, threat logs, and applications usage across the domain (Figure 15).

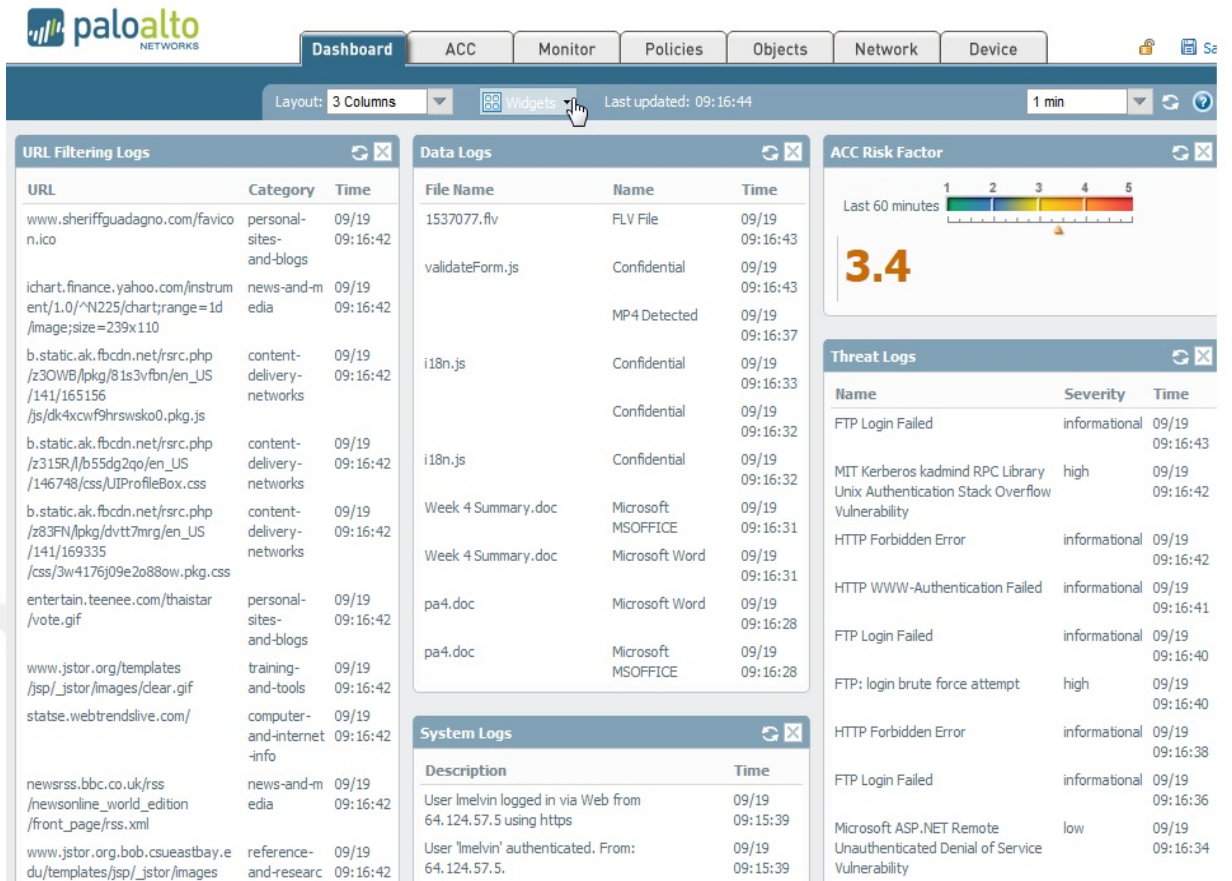


Figure 15 Alo palo network control center[69]

The web-interface of PAN is noted to have certain details regarding the logs and system information. It is easy to be configured as illustrated in the figure below. The layout is having the feature of being customised to any position by just dragging across the interface (Figure 16).

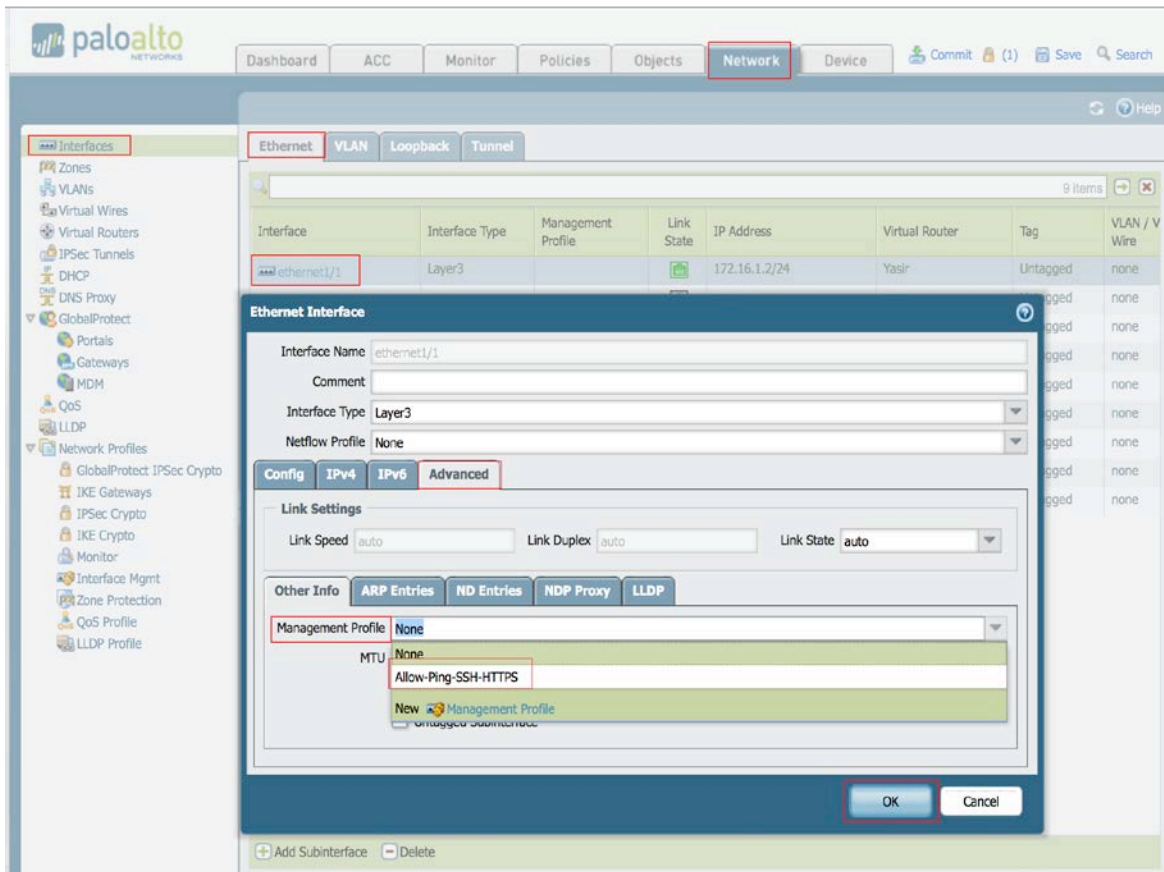


Figure 16 Web-interface of PAN [73]

4.7.3.2 SONICWALL


Secure network access is ensured across the entire network topology by means of reliable connectivity. Connecting to the SONICWALL interface automatically provides IP address to the device. Initially, there is an access need towards the interface of SONICWALL management.

The accepted browsers listed, in Figure 17 which facilitate interconnectivity,

Initial Setup

This section provides initial configuration instructions for connecting your SonicWALL NSA 2400. Follow these steps if you are setting up **scenario A, B, or C**.

This section contains the following subsections:

	Accepted Browser	Browser Version Number
	Internet Explorer	6.0 or higher
	Firefox	2.0 or higher
	Netscape	9.0 or higher
	Opera	9.10 or higher for Windows
	Safari	2.0 or higher for MacOS

System Requirements

Before you begin the setup process, check to verify that you have:

- An Internet connection
- A Web browser supporting Java Script and HTTP uploads

Connecting the WAN Port

1. Connect one end of an Ethernet cable to your Internet connection.
2. Connect the other end of the cable to the **X1 (WAN)** port on your SonicWALL NSA Series appliance.

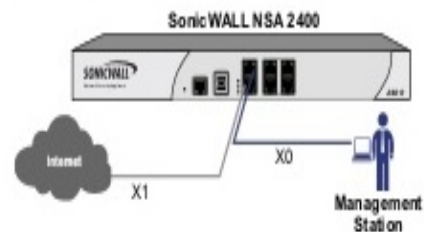


Figure 17 Accepted browsers for SONICWALL [74]

The device installation or deployment takes place as shown in Figure 18 . These rules are selected based on the prospect of deployment scenario

Selecting a Deployment Scenario

Before continuing, select a deployment scenario that best fits your network scheme. Reference the table below and the diagrams on the following pages for help in choosing a scenario.

Current Gateway Configuration	New Gateway Configuration	Use Scenario
No gateway appliance	Single SonicWALL NSA as a primary gateway.	A - NAT/Route Mode Gateway
	Pair of SonicWALL NSA appliances for high availability.	B - NAT with State Sync Pair
Existing Internet gateway appliance	SonicWALL NSA as replacement for an existing gateway appliance.	A - NAT/Route Mode Gateway
	SonicWALL NSA in addition to an existing gateway appliance.	C - Layer 2 Bridge Mode
Existing SonicWALL gateway appliance	SonicWALL NSA in addition to an existing SonicWALL gateway appliance.	B - NAT with State Sync Pair

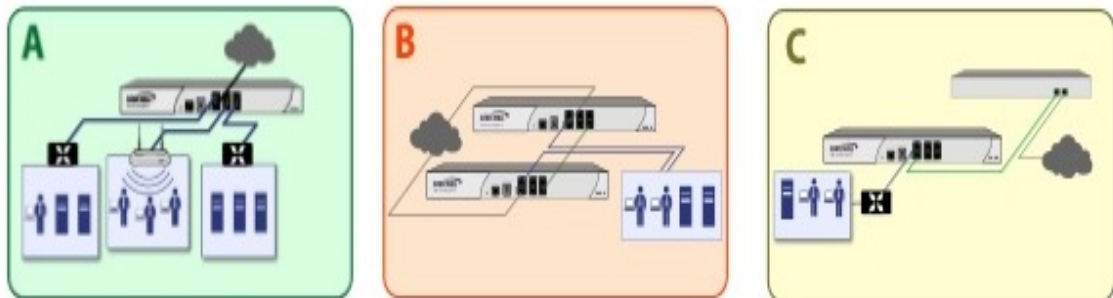


Figure 18 SONICWALL installation steps[74]

Figure 19 is the illustration of gateway anti-virus enabling, Even advanced settings regarding the gateway are also facilitated as below image , Moreover, the intrusion prevention system offered by SONICWALL is represented as:

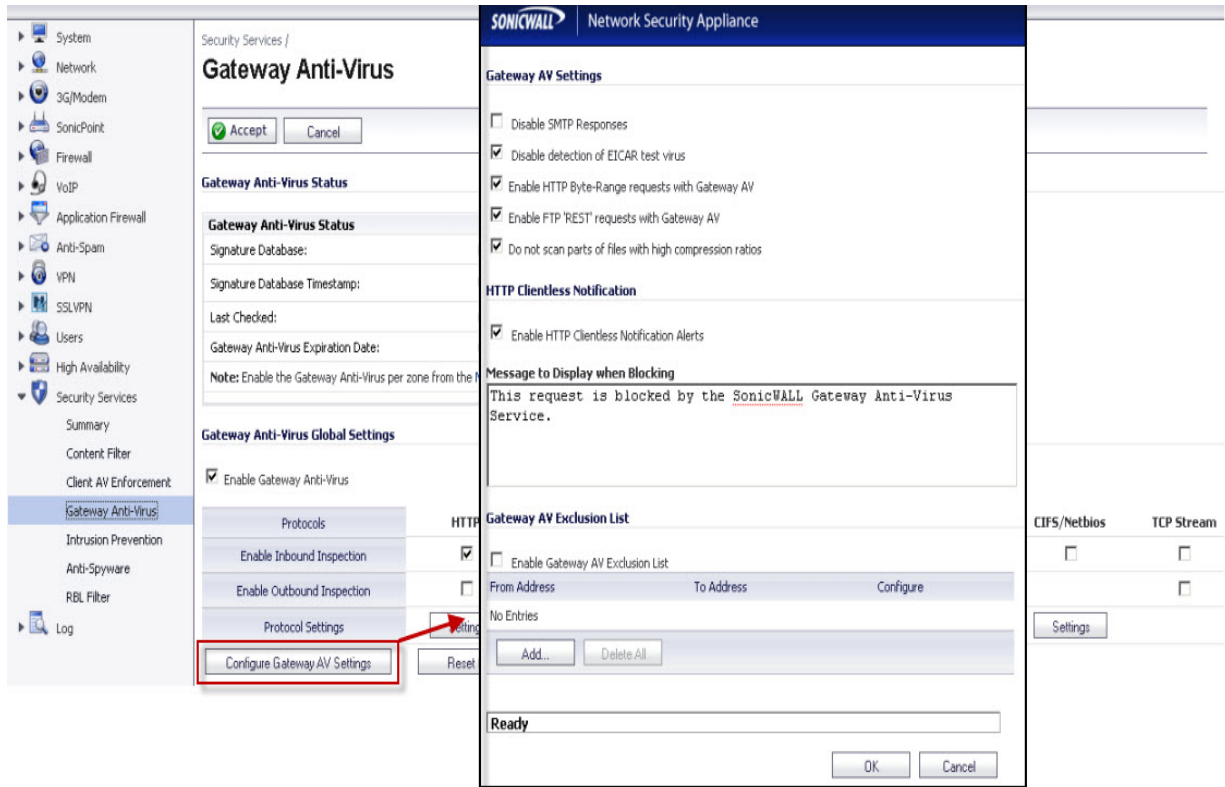


Figure 19 SONICWALL anti-virus enabling [74]

Besides, the diagnostic aspects are also facilitated in a user-friendly setting, Figure 20 is the representation of the real-time monitoring of the traffic across the applications:



Figure 20 SONICWALL monitor [74]

4.7.3.3 SOPHOS

The web interface aspects of SOPHOS solution of UTM/NGFW is observed to be quite appealing from the administrators'/ users'/ point of view. Every detail that is required or needs to be provided, is clearly represented within the interface of the solution; thus, ensuring that the designing of SOPHOS is potentially aligned with the ease of accessibility that is regarded as the eminent aspect of security solutions.

The software also offers a strong , nice , rich dashboard that can help system admin to easy manage their own device with one page(Figure 21)

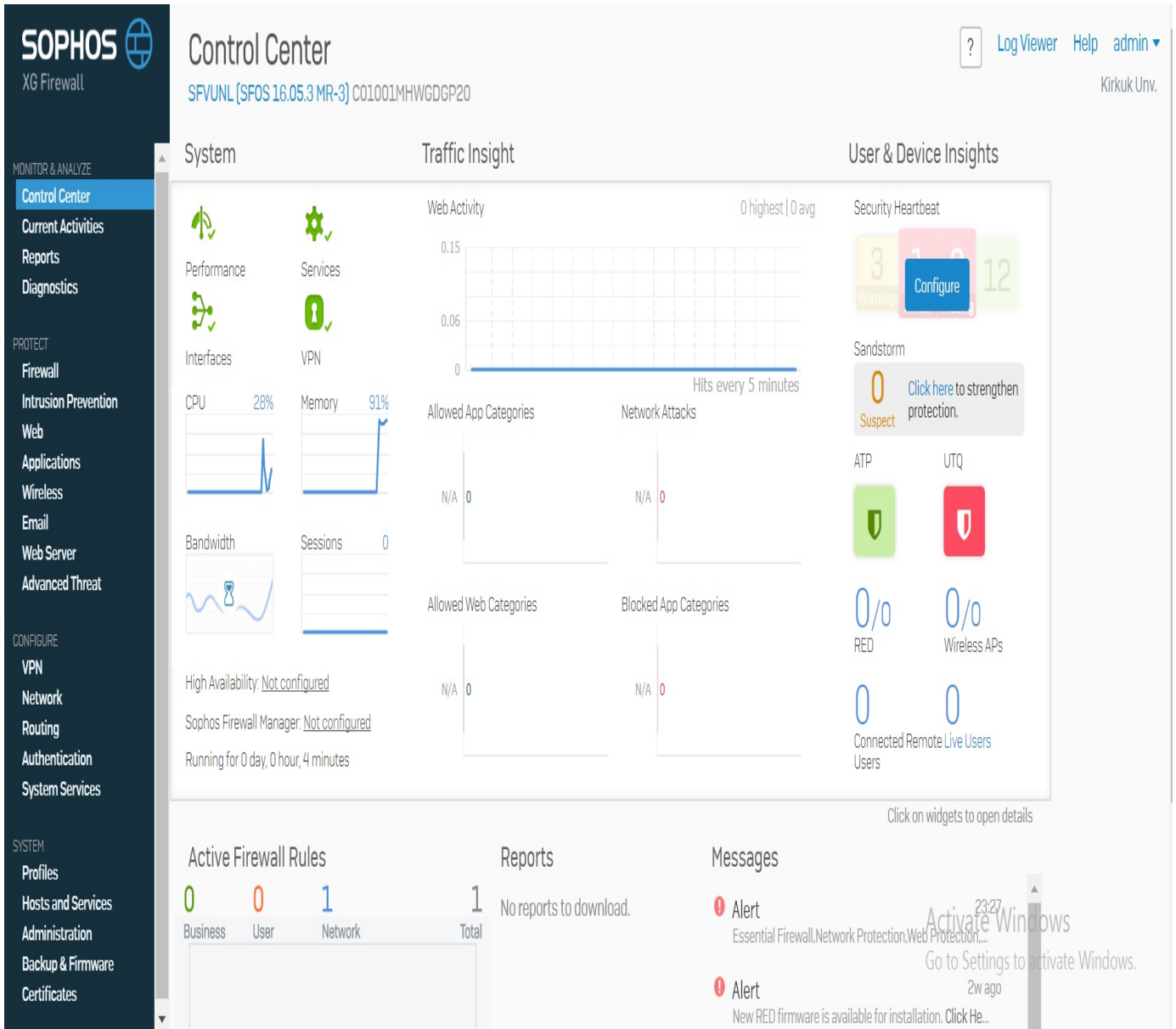


Figure 21 SOPHOS control center (Author, reference)

The software also offers threat protection in an advanced manner, providing protection across web-access and email and reporting system as well (Figure 22)

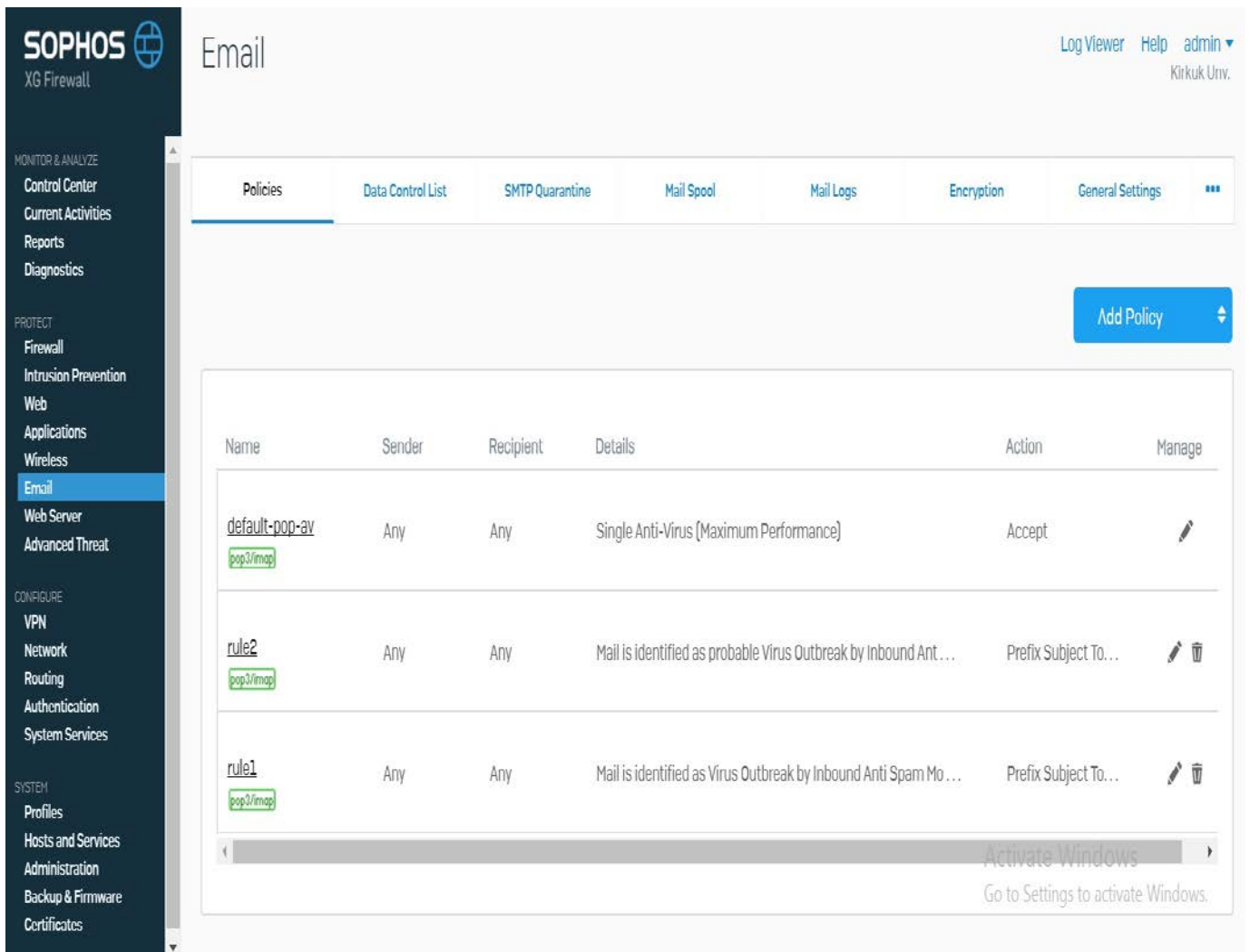


Figure 22 SOPHOS email protection (Author, reference)

The reports are simplified, concise and easily customizable. The manager can access the required information in a short time. A filter can also be created within the same report .

Sophos XG Firewall provides unprecedented visibility into your network, users, and applications directly from the all-new control center. You also get rich on-box reporting and the option to add Sophos iView for centralized reporting across multiple firewalls.

4.7.3.4 WatchGuard

Undoubtedly, the web-interface of WatchGuard is well-organized that is regarded as the basic element of an internet-based software solution. The Front Panel page shows basic information about your device, your network, and network traffic. Moreover From the Dashboard, you can see real-time information about your Firebox or XTM device on these pages (Figure 23)

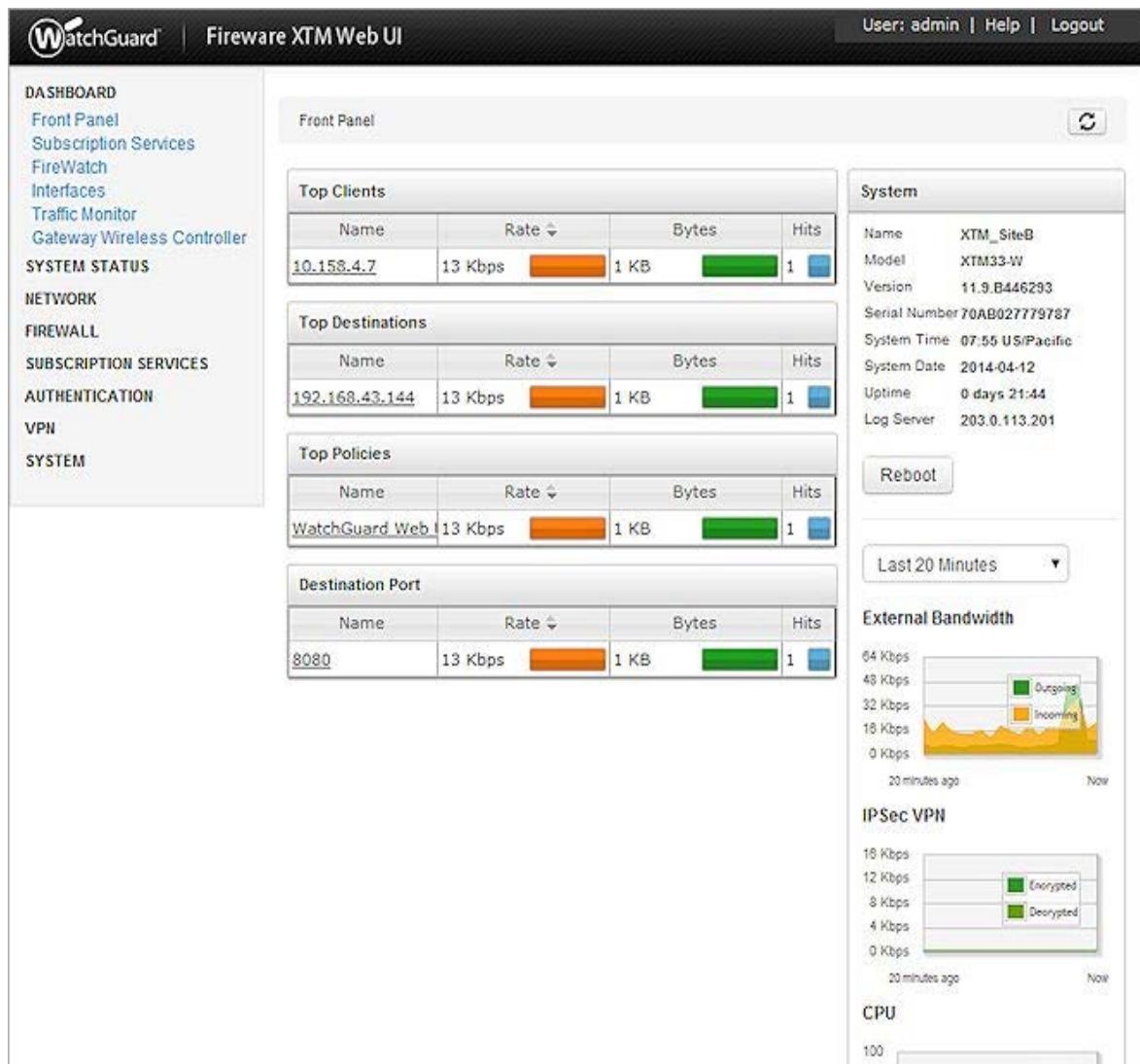


Figure 23 WatchGuard control center [72]

Figure 24 shows web-interface of the software solution, representing that each and every element is managed efficiently, you can use the Dashboard to browse the System Status pages as well.

The screenshot shows the WatchGuard Fireware XTM Web UI. The top navigation bar includes the WatchGuard logo, the title 'Fireware XTM Web UI', and user information 'User: admin | Help | Logout'. The left sidebar contains a 'DASHBOARD' menu with various system status and network management options. The main content area is titled 'ARP Table' and features a table with the following data:

IP Address	Hardware Type	Flags	HW Address	Device
10.0.40.2	0x1	0x2	00:90:7f:b0:00:8e	eth3
10.0.50.2	0x1	0x2	00:90:7f:b0:01:39	br0
192.168.43.125	0x1	0x2	90:b1:1c:92:dd:0b	eth0
192.168.42.242	0x1	0x2	00:21:70:12:e5:54	eth0
192.168.42.201	0x1	0x2	d4:be:d9:90:ee:86	eth0
192.168.43.30	0x1	0x2	00:21:70:13:0f:2e	eth0
192.168.42.127	0x1	0x2	18:03:73:4c:d8:de	eth0
192.168.42.171	0x1	0x2	00:25:64:eb:b0:84	eth0
192.168.43.60	0x1	0x2	a4:ba:db:eb:85:d8	eth0
192.168.43.91	0x1	0x2	b8:ca:3a:9d:c6:31	eth0
192.168.42.131	0x1	0x2	78:2b:cb:ad:4f:6f	eth0
192.168.43.48	0x1	0x2	00:25:64:eb:b1:0d	eth0
192.168.42.207	0x1	0x2	a4:ba:db:f6:c4:62	eth0
192.168.43.152	0x1	0x2	00:e0:81:c3:e9:4c	eth0
192.168.42.208	0x1	0x2	90:b1:1c:70:1f:7b	eth0
192.168.42.186	0x1	0x2	b8:ac:6f:a9:99:c1	eth0
192.168.43.98	0x1	0x2	18:03:73:33:2f:8f	eth0
192.168.43.92	0x1	0x2	00:25:64:ce:a0:5b	eth0

Figure 24 WatchGuard management elements [72]

The interface that you use to connect to WatchGuard SSL Web UI is different depending on the deployment method you used for your device.

4.8 Comparison of the Devices based on Magic Quadrant of Gartner

It has been acknowledged that the early firewalls have been effective in securing the IT networks against basic threat attempts of exploiting the network. In this regard, these firewall systems had lower layers of stacking that provided basic level of packet filtering and routing across the ports, along with the basic inspection of protocols for managing the forwarding or dropping of traffic across the IT infrastructure of the business enterprise. However, the current technical environment

has brought in certain revolutions by means of exploiting the potential susceptibilities of the servers and applications. Accordingly, it has been recognised that the secure business activities demand the integration of certain intrusion prevention systems, anti-spam, web-filters, WAF - Web Application Firewalls, and the assurance of remote access in the form of centralised management through VPNs. Consequently, the advanced and upgraded security network has resulted in the evolution of UTM as the potential product of network security in a consolidated form [71].

Even firewall technology has also received high level of advancement that is reflected from the stacking layers to be over seven for the ascertained management of application traffic. These firewalls have evolved in terms of adding multiple security technologies regarding threat prevention. Besides, it has also been affirmed that the firewalls (Next Generation Firewalls) are now capable of detecting and managing the traffic on the basis of application in use or the potential users, rather than the typical mode of traffic type [71]. With the advancements appearing in the IT-security sector, it has been contended that the landscape of threats has also acquired the notions of being ever evolving, such as the threats of *botnet malwares*, and *ransomware* are the eminent and the most challenging ones. These identified threats have been referred as APTs (or Advanced Persistent Threats), and are potentially capable of affecting the entire system with the instant creation of zero-day malwares that are detected by the signature-based systems, once the threat attempt is successful. Its severity is evident from the statistics of the affected businesses with these botnets or APTs, since 83% of the organisations are affirmed to be affected [76].

Such a susceptible situation of the IT network has been the prime cause of deploying prompt and adequate security measures across the business environment, since the rate of affected businesses seems alarming. It has led to the recognition of integrating innovative technologies of identifying the potential chances of malicious attacks, without being reliant over traditional signature-based anti-virus applications. As a result, it has been noted that even the small and medium sized businesses are capable of integrating the technology of Sandboxing that was previously affordable only for large enterprises. Besides, it has also been acknowledged that the security system must be integrated and centralised rather than being independent and isolated.

Moreover, the detection of malwares or botnets must be proficient enough in avoiding the system to be affected.

Even though increasingly efficient firewall products have been developed, the system is contended to be extensively complicated with loose integration and poor compliance towards the required solutions. Resultantly, these systems have caused the management to suffer in terms of managing the massive amount of data logs; thus, increasing the management burden to unsustainable levels. The responses of different IT administrators in this regard have reflected that the firewalls are quite time consuming in collection information of the threats. Besides, these firewalls lack in visibility into risks and threats, along with being complex due to multiple features that are mostly not user-friendly [76].

On the basis of these market trends, the adopted devices for the network security of an Imaginary Organisation have been assessed based on their potential credibility in terms of the assurance of *Endpoint Protection* and *Unified Threat Management*. The comparison has been based on the Gartner Magic Quadrant to get the leading firewall solution/vendor in the market. The Gartner research process that incorporates the collaborative efforts of the analysts and researchers, who are proficient in respective areas of expertise. Primarily, five-stage process is deployed that entails the essentials of the analysis being independent and fair (Figure 25). The analysis is focused on the essential areas of assurance of visionary aspects and the competence in terms of execution. The vendors involved in the assessment are categorised as:

Visionaries: Having good vision, but capability scoring is low, along with potentially good insights of future market. However, execution is observed to meet failure.

Leaders: The potential of having a good vision with significant competence in the current and future market

Niche Players: Both the assessment criteria are observed to have low scores

Challengers: These are the vendors that are at lower level in terms of being visionary, but have good potential of being capable of meeting the challenges of the future market

Based on this particular implication of Gartner's strategic analysis, figures below illustrates the preferred vendor to be adopted for an Imaginary Organisation. The assessment of Gartner reflects the most important finding for this particular study that Palo Alto Network as a security solution could not acquire presence over the magic quadrants of Gartner, neither in terms of end-protection nor as potentially a UTM. Therefore, it eventually eradicates the device of PAN from the choices for an Imaginary Organisation. In the same manner, WatchGuard has been positioned as Visionary for being UTM, but its effectiveness for being a potential solution of end protection has not been affirmed. Therefore, WatchGuard also loses its chances of being adopted as a potential security solution at an Imaginary Organisation.

Likewise, the device of SONICWALL has been affirmed as *Challenger* on the magic quadrant of Gartner, in terms of facilitating UTM services; however, the element of end protection is noted to be missing or avoided within the service package of SONICWALL. As a result, the comparison has led to the preferred selection of SOPHOS as the potential solution for UTM needs and the end protection needs of the IT security of an Imaginary Organisation, since it has been affirmed as a competent leader in both the areas.

:



Figure 25 Gartner Magic Quadrant - ENDPOINT PROTECTION [75]

Sophos now days still keeping maintains advanced positions in the global rankings as shown in the Figure 26 , again in 2016 Sophos takes place in "Magic Quadrant for Unified Threat Management." as a "Leaders" , the analysis was based on an assessment of a company's ability to execute and completeness of vision, This position is shared by three competing companies, But the thing that distinguishes the Sophos company which are it is only company take a "Leaders" positions in three different security product which are Mobile Data Protection , Endpoint Protection Platforms and Unified Threat Management (UTM).



Figure 26 Gartner Magic Quadrant UNIFIED THREAT MANAGEMENT [75]

Sophos company is always a forerunner in hardware development and information security development sometimes faster than the evolution of the Network security business, some financial statistics for 2016 showed ratios of 27.5 % in Network security business which is well above the reported market growth of 7%. For the same period, Most of the growth in the company is for products of next-generation firewall (NGFW) and UTM.

Sophos Placed in the Leader’s Quadrant of Gartner’s 2016 Unified Threat Management Magic Quadrant for Fifth Consecutive Year, according to the Gartner’s report, compiled by [75], it has been affirmed that SOPHOS offers extensive security with its multiple packages and series of security solutions. SOPHOS offers virtual devices that are integrated on the platform of AWS IaaS, with competitive endpoint products. It facilitates with synchronized security assurance with its single

dashboard, along with multi-lingual management console. Recently, SOPHOS has acquired recognition in terms of developing SFOS (SOPHOS Firewall Operating System) for the UTMs of SOPHOS XG-Series. Besides, the platform support has also been extended to MS Azure Stack and Azure Cloud. It is also affirmed to have IPsec module and email security attributes as well that are in essence of dealing with the dynamic tunnelling.

4.9 Comparison of the Devices Based on Virtual Box Environment

After reviewing many previous relevant studies, a Unified threat management (UTM) and a comparison conducted among a group of commercial software was done in this study, We have been working on a virtual environment through the use of a host operating system as virtual servers with full installation of four devices have been assessed based on the attributes of visions, execution, ease of use, web-interfaces, device performance , throughput capacity , intrusion prevention system featuers along with the guaranteed elements of security and many other factor. The test environment include installation and testion of SONICWALL, SOPHOS XG Firewall, WarchGuard, and Palo Alto Networks.

In order to accomplish the objectives of the study, the researcher has used Oracle's Virtual box to create the virtual environment as the research setting for assessing the security potential of Unified Threat Management system. The specifications of the computer used for running the software solutions included Core i7 processor (CPU) with 8GB RAM, based on Windows 10 platform. The selected UTM solutions are:

- SONICWALL
- SOPHOS
- WarchGuard
- Palo Alto Networks

The researcher also analysis and carrying the impacts of Gartner's reviews along with testing lab result to came out with conclusions that shown in Table1. The table shows the existance of security features in each tested UTM software.

Table1: Comparison of the Devices

Firewall Comparison Features		SOPHOS XG Firewall	WatchGuard Firebox	SonicWALL NSA	Palo Alto Networks
Next-Gen Firewall and ATP	FastPath Packet Optimization	✓			
	Dual AV Engines	✓			
	Intrusion Prevention System	✓	✓	✓	✓
	Application Control	✓	✓	✓	✓
	Web Protection and Control	✓	✓	✓	✓
	User and App Risk Assessment & Visibility	✓			✓
	HTTPS Filtering	✓	✓	✓	✓
	Advanced Threat Protection	✓	✓	✓	✓
	Sandboxing	✓	✓	✓	✓
Synchronized Security 	Identify Compromised Host, User, & Process	✓			
	Compromised System Isolation	✓			
	Unknown Application Identification	✓			✓

UTM & Deployment	Full-Featured Web Application Firewall	✓		+1Box	
	Email AV, AS, Encryption & DLP	✓	+1Box	+1Box	+1Box
	Full Historical Reporting	✓	+1Box	+1Box	+1Box
	Plug-and-Play Remote Office Security (RED)	✓			
	Flexible Deployment (HW, SW, VM, IaaS)	✓	No SW/IaaS	No SW/IaaS	No SW/IaaS
	Price	Average to low	High	Average	Very High

4.10 Comparing the Capability of Gartner's Recommended Device "SOPHOS" with others

Gartner has once again named Sophos as a Leader in the Magic Quadrant for Unified Threat Management – for the fifth year in a row. Sophos is now one of only three vendors in the Leader’s Quadrant, There are many reason Behind this progress and maintain this high level

- Sophos keep it simple. it is easy to deploy, manage, and use.
- With Sophos you will get lightning speed. All sophos appliances are engineered for speed.
- Everything’s on one box. With Sophos you will get all the latest next-gen firewall features plus much more. No need to buy extra hardware.

- Reporting's built in. Detailed reports come as standard, stored locally on the built-in solid-state drive.
- Sophos constantly innovating. And consistently enhance their own technology and they have an outstanding roadmap.

Below section are the most important point that can be comparing Sophos with other Devices in same level.

4.10.1 SOPHOS XG vs., Dell SONICWALL

SonicWALL is noted to be under multiple stages of acquisition that might have affected its credibility or it could be contended that the acquisitions have been due to potential flaws in serving the business needs. However, SonicWALL seems to offer significant level of competition to SOPHOS products, when compared in terms of facilitating the business needs of UTM and NGFW Functionality.

Table 2 Compare SOPHOS XG vs., Dell SONICWALL

COMPETITIVE STANCE		
Competitors	SonicWALL UTMs	SOPHOS UTMs
Products	TZ Series	SOPHOS XG
Description	<ul style="list-style-type: none"> • Facilitating the UTM needs of small businesses dealing in retail, • Serving the remote accessibility needs of businesses 	
Product	NSA Series	SOPHOS XG
Description	<ul style="list-style-type: none"> • Facilitating the needs of NGFWs for large corporate sectors, distributed networks, and small to medium sized enterprises 	
Strengths of SonicWALL		
<ul style="list-style-type: none"> • Comparative range of products or packages for all sizes of customers or business • Competitive pricing • Competitive performance ratio 		

Weaknesses of SonicWALL
<ul style="list-style-type: none"> • Too many options or features tend to yield confusing impression among the IT administrators, as reported by Gartner • Potential impacts of repeated acquisitions
Competitive Strengths of SOPHOS
<ul style="list-style-type: none"> • A single source facilitating all the security needs • Effective shielding against advanced threats • No need of on-site technical expertise

	Sophos	Dell SonicWALL
Unified Policy Model	✓	✗
User Threat Quotient (UTQ)	✓	✗
Synchronized Security	✓	✗
Built-in WAF	✓	✗
Free Central Management	✓	✗
Remote Ethernet Device	✓	✗
Built-in Email Security	✓	✗
Selective SSL Scanning	✓	✗

Figure 27 SOPHOS XG vs., Dell SONICWALL [77]

It has been established that SOPHOS XG Firewall tends to be the preferred one, since it serves both the needs of UTM and end protection in terms of its NGFW features. Moreover, the potential weaknesses of SonicWALL (as mentioned above) leads to disregarding it, with respect to the security needs of an Imaginary Organisation.

4.10.2 SOPHOS XG vs. WatchGuard

WatchGuard UTMs are owned as private vendors that are in market since 1993. These security solutions have been serving the security needs of email gateways, and facilitating the businesses with remotely manageable APs. There has been a recent adoption of threat detection technology of "*Hexis Cyber Solutions' HawkEye G*".

Table 3 Compare SOPHOS XG vs. WatchGuard

COMPETITIVE STANCE		
Competitors	WatchGuard UTMs	SOPHOS UTMs
Products	Firebox T10, T30, T50, T70, M200 & M300	SOPHOS XG
Description	<ul style="list-style-type: none"> Facilitating the UTM needs of small businesses dealing in retail, Serving the remote accessibility needs of businesses 	
Product	M400, M440, M500, M4600 & M5600	SOPHOS XG
Description	<ul style="list-style-type: none"> Facilitating the needs of UTMs for medium to large corporate sectors 	
Strengths of WatchGuard		
<ul style="list-style-type: none"> Potentially strong brand image Competitive pricing Efficient performance ratio Potential winners of price-sensitive contracts Integrated cloud-based services - "<i>WatchGuard Dimension</i>" Sandboxing as APT Blocker 		
Weaknesses of WatchGuard		
<ul style="list-style-type: none"> Limited scope of innovations Confusing centralised management Limited preference across the enterprises Certain lacking in configuration aspects, based on the complex settings 		

Competitive Strengths of SOPHOS	
<ul style="list-style-type: none"> • Flexibility of sizing the solution for multiple issues • Easy to configure with unlimited storage due to Microsoft Azure pack services • Synchronised security at all the levels 	

	Sophos	WatchGuard
Single UI to fully configure the Firewall	✓	✗
Simple product line up	✓	✗
All features on all boxes	✓	✗
Unified Policy Model	✓	✗
User Threat Quotient (UTQ)	✓	✗
Granular Logging and Reporting	✓	✗
Full featured Synchronized Security	✓	✗

Figure 28 SOPHOS XG vs. WatchGuard [76]

Consequently, it is evidently validated that the single device of SOPHOS is equivalent to multiple devices of WatchGuard, in order to deal with the intended needs of security. Moreover, the centralised management is the eminent attribute of SOPHOS that keeps in a favoured security solution.

4.10.3 SOPHOS XG vs. Palo Alto Networks

Palo Alto Network is observed to be serving the business security needs of firewalls since 2007. The eminence of these security solutions lies in the

Table 4 Compare SOPHOS XG vs. Palo Alto Networks

COMPETITIVE STANCE		
Competitors	Palo Alto Networks	SOPHOS UTM's
Products	PA-200 and PA-500 series	SOPHOS XG
Description	<ul style="list-style-type: none"> • Facilitating the UTM needs of small businesses 	

	dealing in retail, <ul style="list-style-type: none"> • Serving the remote accessibility needs of businesses 	
Product	PA-3000 and PA-5000 series	SOPHOS XG
Description	<ul style="list-style-type: none"> • Facilitating the needs of NGFWs for large corporate sectors, distributed networks, and small to medium sized enterprises 	
Strengths of Palo Alto Networks		
<ul style="list-style-type: none"> • Potentially granular in terms of application monitoring and control technology • Attractive features of User-ID, App-ID, and Content-ID • Facilitating the security needs of large data centres and enterprises • Competent NGFW with innovative features 		
Weaknesses of Palo Alto Networks		
<ul style="list-style-type: none"> • Cannot be regarded as a real UTM • Lacks in wireless facility, and potential flaws in email protection • Flaws in integration of technology across endpoint services • Expensive • Not effective central management 		
Competitive Strengths of SOPHOS		
<ul style="list-style-type: none"> • Easy to access and configure • Adaptable across all business sizes • Facilitates large enterprises, in particular 		

	Sophos	Palo Alto Networks
All-in-One Protection	✓	✗
User Threat Quotient (UTQ)	✓	✗
Synchronized Security	✓	✗
Built-in Email Security	✓	✗
Granular Logging and Reporting	✓	✗
Built-in WAF	✓	✗
Remote Ethernet Device	✓	✗
User Portal	✓	✗

Figure 29 SOPHOS XG vs. Palo Alto Networks [78]

Accordingly, SOPHOS security solutions are comparatively favourable even against Palo Alto Networks that were previously regarded as Leaders. However, the incessant advancements in SOPHOS performance outcomes have made SOPHOS to be recognised as potential leader among the vendors of security solutions, which is in accordance with the Gartner's Magic Quadrant results.

4.11 Result and Discussion

Considering the findings acquired within this study, it has also been established that SOPHOS seems more feasible with respect to the needs of an Imaginary Organisation's office migration plan. It has been stated based on the fact that SOPHOS XG Firewall is proficient in all the respective areas that are considered as preferable for an improved network performance. The rest options that have been considered as a potential choice for an Imaginary Organisation have been disregarded based on their stance in the market that eventually makes their long-term credibility dubious. The business needs of an Imaginary Organisation cannot be directed towards a risky approach, since the adversities of the consequences would be unacceptable. The other devices of UTM/NGFW are noted to be a bit complex that demands expertise among the administrators or potential users. If there are certain lacking in potential required for accessing the solutions, the anticipated outcomes would not be achieved. Therefore, SOPHOS is much better over the other solutions, as it offers both the UTM and NGFW functionalities in a uniquely

innovative manner. SOPHOS is affirmed to be compatibly feasible for the management and control of evolving nature of threats across the business networks. SOPHOS turns out to be the only vendor, ensuring the security facilitation in the business areas of email protection, Unknown Application Identification, along with the element of Full-Featured Web Application Firewall that able to prevent SQL injection attacks and Denial of service ..etc which traditional firewalls and other UTMs may not be capable of doing [71] . Other features are explained in table1 .



CHAPTER 5

CONCLUSION AND RECOMMENDATIONS

The study has focused the most challenging impact of technological implications that are increasing incessantly, as the world of technology is advancing. Within the business environment, the technological advancements are rapidly being deployed, as the business enterprises are entirely directed towards the attainment of competitive edge within the marketplace.

The deployment of technology has been resulting in effective outcomes, if managed appropriately. It has been asserted based on the fact that the rate of technological advancements has eventually increased the risks of data security; thus, affecting the performance efficiency of the organisations. Recognising this particular aspect, the researcher has assessed the business needs of secure network, by means of considering the case study of an Imaginary Organisation. An Imaginary Organisation's office has been assumed to be in need of improved levels of network security, since the existing framework has been noted to be less proficient as technologically demanded. Moreover, the existing infrastructure is also noted to be near to being obsolete that requires prompt implication of improved security system.

Based on this particular scenario, the researcher has formulated the objectives of presenting the implication of UTM as the preferred solution to serve 200 users with advanced security services. In this regard, the researcher has thoroughly explored the security requirements within a business network, focusing on the business needs of sustained success. Accordingly, the importance of UTM/NGFW has also been explored in terms of performance criteria.

5.1 Findings

We found the business stance of an Imaginary Organisation within the current network infrastructure of traditional firewall needs to be upgraded. Since the existing traditional firewall disabled to standing against security threats such as Denial of service, SQL injection, email viruses ..etc.

The researcher has assessed the selected solutions of SONICWALL UTM Devices, SOPHOS UTM Devices, Watch guard UTM Devices, and Palo Alto Networks as the potential UTM devices. These devices have been assessed to be presented as potential proposition to an Imaginary Organisation, as a potential choice to improve the network security.

Considering the security needs of the businesses, the study of these devices and the relevant security aspects has led to the conclusion that the decision of migrating from one infrastructure to another one demands extensive analysis of the market situation and the credibility of the selected solution as well. If the current infrastructure at an Imaginary Organisation is considered, it has been noted that the system lacks in visionary approach to some extent. It has been based on the fact that the company's deployed system is near to EoL "End of Life" that eventually affects the performance efficacy of the business.

Besides, it is also contended that the decision-making process at the managerial layer has not been efficient enough to better plan the future of the organisation. However, the leadership has then decided to migrate to some feasible software solution in terms of advancing the existing infrastructure of the company.

At this stage, the management has carried out PDCA testing vigilantly, whose planning stage has been the prime focus of this particular study. The PDCA cycle has led to the assertions that the company is seriously in need of advanced security system, particularly in the areas of sales and finances. The analysis has been carried out in a considerable manner to emphasise the long-term credibility of the selected solution; thus, mitigating the prospects of potential failure as currently being experienced due to the obsolescence of the existing framework of an Imaginary Organisation.

5.2 Limitations

The use of virtual machine considers the main limitation of our study. Obviously, the measurements that depends on the UTM performance are influenced if hardware or virtual software used. Likewise, the use of virtual machines needs a computer with high requirements to simulate real attacks and provide a high effectiveness. Therefore, the deployment of real UTM devices in a real network will detected the variation of the system. We expect this approach to give more precise results for the study.

5.3 Future studies

Recognising the implications of SOPHOS for the business upgrading needs of an Imaginary Organisation, the study also proposes certain recommendation of improving the potential outcomes of the SOPHOS deployment. It has been recommended that the consequences of this particular migration would be further enhanced, if the implications of SOPHOS are further studied, in terms of extensive research. Eventually, it would be a potential direction for future research as well, if the researchers study the SOPHOS in details, without compromising any possible aspect due to the constraints of timing or even costs.

5.4 Conclusion

The study has been established that SOPHOS UTM tends to be the preferred one, since it serves both the needs of UTM and end protection in terms of its NGFW features based on experimental work. SOPHOS turns out to be the only vendor, ensuring the security facilitation in the business areas of Email Protection, Unknown Application Identification, along with the element of Full-Featured Web Application Firewall that able to prevent SQL injection attacks and Denial of Service. Moreover, the potential weaknesses of another solutions (as mention below) leads to disregarding it, with respect to the security needs of an Imaginary Organisation.

Even though, four choices have been made, but the assessment based on findings and Gartner's approaches affirmed that not all the new or innovative solutions are practical to be implemented across all the organisations. Care needs to be taken while making decisions in this regard, since the nature of the business, and the respective needs of security tend to have diverse impacts and different feasibilities with respect to the software solutions available in the market.

The solutions of SONICWALL UTM, WatchGuard UTM, and Palo Alto Network could have been regarded as the most preferred ones, since these are the potentially competitive vendors in the market. However, it has also been recognized that the interfaces, accessibility and other vision and execution related attributes make these options less preferable. If these solutions are potentially efficacious within the recent times, there are potential chances that the rapidly changing technology and the advancements in technology would eventually leave these solutions obsolete or less proficient when compared with the new arrivals.

Based on Gartner report, These solutions are either Challengers (SONICWALL) or Visionaries (WatchGuard); thus, minimum chances are there to select any one of them for the business security needs of an Imaginary Organisation. Therefore, the remaining software solution of SOPHOS has been presented as the preferred choice for the security needs of an Imaginary Organisation's network.

SOPHOS has been ranked as leaders among the categories of Gartner's assessment; thus, affirming the visionary and executing related implications of the security solution. Besides, even the findings have also affirmed that SOPHOS security solutions are potentially easy to use, since the stage of initiating its usage or its configuration is readily accessible and user-friendly as well. More specifically, the entire web interface of SOPHOS is affirmed to have the feasibility and accessibility notions that in turns validates its preference as the infrastructure for migration of an Imaginary Organisation.

Finally, The proposed topology for enhanced network security at an Imaginary Organisation has couple of security zones that are newly introduced. Consequently , high availability is anticipated throughout the setup. Where UTM1 and UTM2 placed in parallel to increase the availability and the scalability of the network and UTM3 assigned for restricted zone.

REFERENCES

1. **Thomas, T.M. and Stoddard, D., (2011).** *"Network security first-step"*. Cisco Press.
2. **Bari, M.F., Boutaba, R., Esteves, R., Granville, L.Z., Podlesny, M., Rabbani, M.G., Zhang, Q. and Zhani, M.F., (2013).** *"Data center network virtualization: A survey"*. IEEE Communications Surveys & Tutorials, 15(2), pp.909-928.
3. **Shahriar, H. and Zulkernine, M., (2012).** *"Mitigating program security vulnerabilities: Approaches and challenges"*. ACM Computing Surveys (CSUR), 44(3), p.11.
4. **Johari, R. and Sharma, P., (2012), May.** *"A survey on web application vulnerabilities (SQLIA, XSS) exploitation and security engine for SQL injection"*. In Communication Systems and Network Technologies (CSNT), 2012 International Conference on (pp. 453-458). IEEE.
5. **Reitblatt, M., Foster, N., Rexford, J., Schlesinger, C. and Walker, D., (2012).** *"Abstractions for network update"*. In Proceedings of the ACM SIGCOMM 2012 conference on Applications, technologies, architectures, and protocols for computer communication (pp. 323-334). ACM.
6. **Benton, K., Camp, L.J. and Small, C., (2013), August.** *"Open flow vulnerability assessment"*. In Proceedings of the second ACM SIGCOMM workshop on Hot topics in software defined networking (pp. 151-152). ACM.
7. **Gorgievski, M.J., Ascalon, M.E. and Stephan, U., (2011).** *"Small business owners' success criteria, a values approach to personal differences"*. Journal of Small Business Management, 49(2), pp.207-232.
8. **Lacey, D., (2011).** *"Managing the Human Factor in Information Security: How to win over staff and influence business managers"*. John Wiley & Sons.
9. **Baltzan, P. (2012).** *"Business driven technology"*. McGraw-Hill/Irwin.
10. **Gambardella, A. and McGahan, A.M., (2010).** *"Business-model innovation: General purpose technologies and their implications for industry structure"*. Long range planning, 43(2), pp.262-271.

11. **Alinaghian, R., Rahman, A. A., & Ibrahim, R. (2011).** *"Information and communication technology (ICT) policy; significances, challenges, issues and future research framework"*. Australian Journal of Basic and Applied Sciences, 5(12), 963-969.
12. **Ciampa, M., (2012).** *"Security+ guide to network security fundamentals"*. Cengage Learning
13. **Stiawan, D., Abdullah, A.H. and Idris, M.Y., (2010), June.** *"The trends of intrusion prevention system network"*. In Education Technology and Computer (ICETC), 2010 2nd International Conference on (Vol. 4, pp. V4-217). IEEE.
14. **Aven, T., (2007).** *"A unified framework for risk and vulnerability analysis covering both safety and security"*. Reliability engineering & System safety, 92(6), pp.745-754.
15. **Chen, D. and Zhao, H., (2012).** *"Data security and privacy protection issues in cloud computing"*. In Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on (Vol. 1, pp. 647-651). IEEE.
16. **Qi, Y., Yang, B., Xu, B. and Li, J., (2007), June.** *"Towards system-level optimization for high performance Unified Threat Management"*. In Networking and Services, 2007. ICNS. Third International Conference on (pp. 7-7). IEEE.
17. **Jørgensen, T.H. and Simonsen, G., (2002).** *"Prospects of a unified management system"*. Corporate social responsibility and environmental management, 9(2), pp.91-98.
18. **Ali, S., Al Lawati, M. H., & Naqvi, S. J. (2012, September).** *"Unified Threat Management System Approach for Securing SME's Network Infrastructure"*. In e-Business Engineering (ICEBE), 2012 IEEE Ninth International Conference on (pp. 170-176). IEEE.
19. **Al-Aqrabi, H., Liu, L., Xu, J., Hill, R., Antonopoulos, N., & Zhan, Y. (2012, April).** *"Investigation of IT security and compliance challenges in Security-as-a-Service for Cloud Computing"*. In Object/Component/Service-Oriented Real-Time Distributed Computing Workshops (ISORCW), 2012 15th IEEE International Symposium on (pp. 124-129). IEEE.

- 20. Krishnakumar, L. and Varughese, N.M., (2013), December.** *"High speed classification of vulnerabilities in cloud computing using collaborative network security management"*. In Advanced Computing and Communication Systems (ICACCS), 2013 International Conference on (pp. 1-6). IEEE.
- 21. Deng, F., Luo, A., Zhang, Y., Chen, Z., Peng, X., Jiang, X. and Peng, D., (2008), November.** *"TNC-UTM: A holistic solution to secure enterprise networks"*. In Young Computer Scientists, 2008. ICYCS 2008. The 9th International Conference for (pp. 2240-2245). IEEE.
- 22. Liu, H. and Zheng, L., (2010), November.** *"Application and Research on Active Protection for Campus Network Based On Multi-Cores UTM"*. In Multimedia Information Networking and Security (MINES), 2010 International Conference on (pp. 589-592). IEEE.
- 23. Dumitras, T. and Shou, D., (2011), April.** *"Toward a standard benchmark for computer security research: The Worldwide Intelligence Network Environment (WINE)"*. In Proceedings of the First Workshop on Building Analysis Datasets and Gathering Experience Returns for Security (pp. 89-96). ACM.
- 24. Krishnamurthy, B. and Wills, C.E., (2009), August.** *"On the leakage of personally identifiable information via online social networks"*. In proceedings of the 2nd ACM workshop on Online social networks (pp. 7-12). ACM.
- 25. Schwartz, P.M. and Solove, D.J., (2011).** *"The PII problem: Privacy and a new concept of personally identifiable information"*. NYUL rev., 86, p.1814.
- 26. Hotaling, A., (2007).** *"Protecting personally identifiable information on the internet: Notice and consent in the age of behavioural targeting"*. CommLaw Conspectus, 16, p.529.
- 27. Yang, L.X. and Yang, X., (2014).** *"The spread of computer viruses over a reduced scale-free network"*. Physica A: Statistical Mechanics and Its Applications, 396, pp.173-184.
- 28. Herath, T., Chen, R., Wang, J., Banjara, K., Wilbur, J. and Rao, H.R., (2014).** *"Security services as coping mechanisms: an investigation into user intention to adopt an email authentication service"*. Information systems journal, 24(1), pp.61-84.

- 29. Steer, J., (2014).** *"The gaping hole in our security defences"*. Computer Fraud & Security, 2014(1), pp.17-20.
- 30. Muthuramalingam, S., Thangavel, M. and Sridhar, S., (2016).** *"A Review on Digital Sphere Threats and Vulnerabilities"*. In Combating Security Breaches and Criminal Activity in the Digital Sphere (pp. 1-21). IGI Global.
- 31. Rhodes-Ousley, M., (2013).** *"Information security the complete reference"*. McGraw Hill Professional.
- 32. Johnson, M., (2016).** *"Cyber Crime, Security and Digital Intelligence"*. Routledge.
- 33. Cisco. (2013).** *"Mitigating Email Virus Attacks"*, White Paper [Online] Available at http://www.cisco.com/c/en/us/products/collateral/security/email-security-appliance/white_paper_c11-728635.pdf , [accessed 17 April 2017].
- 34. Chen, P., Desmet, L. and Huygens, C., (2014).** *"A study on advanced persistent threats"*. In IFIP International Conference on Communications and Multimedia Security (pp. 63-72). Springer Berlin Heidelberg
- 35. Taylor, R.W., Fritsch, E.J. and Liederbach, J., (2014).** *"Digital crime and digital terrorism"*. Prentice Hall Press.
- 36. Khari, M. and Sangwan, P., (2016), March.** *"Web-application attacks: A survey"*. In Computing for Sustainable Global Development (INDIACom), 2016 3rd International Conference on (pp. 2187-2191). IEEE.
- 37. Marforio, C., Masti, R.J., Soriente, C., Kostianen, K. and Capkun, S., (2015).** *"Personalized security indicators to detect application phishing attacks in mobile platforms"*. arXiv preprint arXiv:1502.06824.
- 38. Hashizume, K., Rosado, D.G., Fernández-Medina, E. and Fernandez, E.B., (2013).** *"An analysis of security issues for cloud computing"*. Journal of Internet Services and Applications, 4(1), p.5.
- 39. Jing, Q., Vasilakos, A.V., Wan, J., Lu, J. and Qiu, D., (2014).** *"Security of the Internet of Things: perspectives and challenges"*. Wireless Networks, 20(8), pp.2481-2501.

- 40. Liang, C. and Yu, F.R., (2015).** *"Wireless network virtualization: A survey, some research issues and challenges"*. IEEE Communications Surveys & Tutorials, 17(1), pp.358-380.
- 41. Kim, D.W., Yan, P. and Zhang, J., (2015).** *"Detecting fake anti-virus software distribution webpages"*. Computers & Security, 49, pp.95-106.
- 42. Jeong, J., Kim, H. and Park, J., (2014).** *"Requirements for security services based on software-defined networking"*. IETF draft-jeong-i2nsf-sdn-securityservices-00.
- 43. Lin, Y.D., Lin, P.C., Prasanna, V.K., Chao, H.J. and Lockwood, J.W., (2014).** *"Guest Editorial Deep Packet Inspection: Algorithms, Hardware, and Applications"*. IEEE Journal on Selected Areas in Communications, 32(10), pp.1781-1783.
- 44. Bremler-Barr, A., Harchol, Y., Hay, D. and Koral, Y., (2014), December.** *"Deep packet inspection as a service"*. In Proceedings of the 10th ACM International on Conference on emerging Networking Experiments and Technologies (pp. 271-282). ACM.
- 45. Fan, Y., Li, D., Xie, Y., Xu, B. and Wang, H., (2012), January.** *"A Holistic Protection Based on Network Access Control"*. In Intelligent System Design and Engineering Application (ISDEA), 2012 Second International Conference on (pp. 975-978). IEEE.
- 46. Chao, Y., Bingyao, C., Jiaying, D., & Wei, G. (2009, December).** *"The research and implementation of UTM"*. In Wireless Mobile and Computing (CCWMC 2009), IET International Communication Conference on (pp. 389-392). IET.
- 47. Takabi, H., Joshi, J.B. and Ahn, G.J., (2010).** *"Security and privacy challenges in cloud computing environments"*. IEEE Security & Privacy, 8(6), pp.24-31.
- 48. Ren, K., Wang, C. and Wang, Q., (2012).** *"Security challenges for the public cloud"*. IEEE Internet Computing, 16(1), pp.69-73.
- 49. Subashini, S. and Kavitha, V., (2011).** *"A survey on security issues in service delivery models of cloud computing"*. Journal of network and computer applications, 34(1), pp.1-11.

- 50. Feng, D.G., Zhang, M., Zhang, Y. and Xu, Z., (2011).** *"Study on cloud computing security"*. Journal of software, 22(1), pp.71-83.
- 51. Zapechnikov, S., Miloslavskaya, N. and Tolstoy, A., (2015), September.** *"Modeling of next-generation firewalls as queuing services"*. In Proceedings of the 8th International Conference on Security of Information and Networks (pp. 250-257). ACM.
- 52. Frahim, J., Santos, O. and Ossipov, A., (2014).** *"Cisco ASA: All-in-one Next-generation Firewall, IPS, and VPN Services"*. Cisco Press.
- 53. Maddumala, M. N., & Kumar, V. (2016, June).** *"Efficient Design of Firewall Temporal Policies"*. In Computer Software and Applications Conference (COMPSAC), 2016 IEEE 40th Annual (Vol. 2, pp. 449-454). IEEE.
- 54. Roy, S., (2015), December.** *"Mitigating the Dark Silicon Phenomenon on Next-Generation Network Processor Architectures"*. In Nanoelectronic and Information Systems (iNIS), 2015 IEEE International Symposium on (pp. 124-124). IEEE.
- 55. Oracle. (2015)."** *Oracle VM VirtualBox. Oracle"*, retrieved from, <http://www.oracle.com/us/technologies/virtualization/oraclevm/oracle-vm-virtualbox-ds-1655169.pdf> ,[accessed 17 April 2017].
- 56. Van Surksum, K., (2017).** *"Release: Oracle VM VirtualBox 4.3. Red, 2016"*.
- 57. SonicWall. (2010).** *"The SonicWALL Network Security Appliance Series"*. Sonic, retrieved from, http://www.telict.be/doc/DS_NSA_Series_A4.pdf, [accessed 20 April 2015].
- 58. SonicWall. (2017).** *"Unified threat management. SonicWall"*, retrieved from, <https://www.sonicwall.com/solutions/unified-threat-management/> , [accessed 20 April 2015].
- 59. SOPHOS, (2014).** *"SOPHOS UTM Software Appliances"*, Retrieved from, <https://www.sophos.com/en-us/medialibrary/PDFs/documentation/sophosutmsoftwarewebadminqsgen.pdf?la=en> ,[accessed 25 April 2017].

- 60. Sophos. (2014).** *"Sophos UTM. Sophos"*, retrieved from, <https://www.sophos.com/en-us/medialibrary/PDFs/factsheets/sophosutmoverviewdsna.pdf?la=enc>, [accessed 25 April 2017].
- 61. Shbair, W.M., Cholez, T., Goichot, A. and Chrisment, I., (2015), May.** *"Efficiently bypassing SNI-based HTTPS filtering"*. In Integrated Network Management (IM), 2015 IFIP/IEEE International Symposium on (pp. 990-995).IEEE.
- 62. WatchGuard, (2014).** *"Use the WatchGuard Access Point Web UI"*, Retrieved from, https://www.watchguard.com/help/docs/wsm/xtm_11/en-us/content/en-us/wireless/ap_web-ui_c.html , [accessed 01 May 2017].
- 63. Rodriguez, C. n.d. Understanding Unified Threat Management (UTM) and Next-Generation Firewalls (NGFWs): A Frost & Sullivan Analysis** **Chris Rodriguez Senior Industry Analyst, Information and Network Security Sponsored by WatchGuard Advancing Network Defenses both Now and in the Future for Mid-Size Organizations.** *"Watchguard"*, retrieved from, https://www.watchguard.com/docs/analysis/FS_Article_WatchGuard_052814_CM.pdf , [accessed 20 April 2017].
- 64. Zuk, N., Wang, S., Leung, S.W. and Gong, F., Palo Alto Networks, Inc., (2011).** *"Packet classification in a network security device"*. U.S. Patent 8,009,566.
- 65. Van der Schaar, M. and Chou, P.A. eds., (2011).** *"Multimedia over IP and wireless networks: compression, networking, and systems"*. Academic Press.
- 66. Kim, H., Schlansker, M., Santos, J.R., Tourrilhes, J., Turner, Y. and Feamster, N., (2012), October.** *"Coronet: Fault tolerance for software defined networks"*. In Network Protocols (ICNP), 2012 20th IEEE International Conference on (pp. 1-2). IEEE.
- 67. Bharali, A., Ithal, R. and Chen, Y.Z., Palo Alto Networks, Inc., (2013).** *"Using geographical information in policy enforcement"*. U.S. Patent 8,566,900.
- 68. Palo Alto Networks, (2010).** *"Palo Alto Networks Next-Generation Firewall Overview"*.

- 69. Palo Alto Networks, (2017).** " *Palo Alto Networks Inc*", Retrieved from, <https://www.paloaltonetworks.com/documentation/70/pan-os/pan-os/device-management/use-the-web-interface> , [accessed 17 April 2017].
- 70. SONICWALL, (2017).** " *How to login to the SonicWALL UTM appliance using the Command Line Interface (CLI) (SW6180)*", SONICWALL, Retrieved from, <https://support.sonicwall.com/kb/sw6180> , [accessed 20 Apr. 2017].
- 71. SOPHOS, (2017).** " *Solution Brief: XG Firewall, SOPHOSBrief Document*".
- 72. WatchGuard, (2017).** " *Navigation WatchGuard WebCentre*", Retrieved from, http://www.watchguard.com/help/docs/fireware/11/en-US/Content/en-US/webcenter/webcenter_navigate_wsm.html , [accessed 01 May 2017].
- 73. Palo Alto ,(2017).** " *Palo Alto Networks* " , Retrieved from https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/frame-maker/70/pan-os/pan-os.pdf , [accessed 10 May 2017].
- 74. SonicWall. (2017).** " *Unified threat management. SonicWall*", retrieved from, <https://www.sonicwall.com/solutions/unified-threat-management/> , [accessed 20 April 2017].
- 75. D'Hoinne, J., Hils, A., and Kaur, R., (2016).** " *Magic Quadrant for Unified Threat Management*", Retrieved from, <http://www.gartner.com/home> , [accessed 17 April 2017].
- 76. SOPHOS Group, (2017).** " *Battlecard: Sophos XG Firewall vs WatchGuard UTM's*".
- 77. SOPHOS Group, (2016).** " *Battlecard: Sophos XG Firewall vs Dell SonicWALL*".
- 78. SOPHOS Group, (2016a).** " *Battlecard: Sophos XG Firewall vs Palo Alto Networks NGFWs*".

CURRICULUM VITAE

PERSONAL INFORMATION

Surname, Name: Ahmad Ayid Ahmad

Date and Place of Birth: 02 February 1982, Iraq/ Kirkuk

Marital Status: Single

Phone: +9647701328946

Email: Ahmadayid@yahoo.com

EDUCATION

Degree	Institution	Year of Graduation
M.Sc.	Çankaya University, Mathematics and Computer science Dept. / Information Technology program, Ankara, Turkey	2017
B.Sc.	College Of Technology Kirkuk /Software Engineering Dep.	2005
High School	Alhaweja High School Kirkuk, Iraq.	2001

WORK EXPERIENCE

Year	Place	Enrollment
2011-now	Kirkuk University	Teacher
2006-2011	NGO Organizations	IT

LANGUAGES

Language	Speaking	Reading	Writing
Arabic	Native	Native	Native
English	V.Good	V.Good	V.Good
Turkish	B1	B1	B1