

ENHANCED NETWORK SECURITY USING NEXT GENERATION FIREWALLS(NGFW)

By

Kazi Talim

ID: 183-31-258

This Report Presented in Partial Fulfillment of the Requirements for the Degree of Master of
Science in Electronics and Telecommunication Engineering (M.Sc. in ETE).

Supervised By

Md. Taslim Arefin

Associate Professor and Head

Department of ETE



Department of Electronics and Telecommunication Engineering
Daffodil International University
Dhaka, Bangladesh

The thesis titled "Enhancing Network Security Using Next Generation Firewalls (NGFW)_Case of Fortinet Firewall" submitted by Kazi Talim, ID No. 183-31-258, Department of Electronics and Telecommunication Engineering, Daffodil International University, has been accepted as satisfactory for the partial fulfillment of certain requirements his education of M.Sc. in Electronics and Telecommunication Engineering and approved concerning its style, value and contents.


BOARD OF EXAMINERS



1. Md. Taslim Arefin

Chairman

Associate Professor and Head
Department of ETE, DIU




2. Professor Dr. A. K. M. Fazlul Haque

Member

Professor & Associate Dean
Department of ETE, DIU

(Internal Examiner)




3. Engr. Md. Zahirul Islam

Member

Assistant Professor
Department of ETE, DIU

(Internal Examiner)



4. Dr. Engr. M. Quamruzzaman

Member

Professor
Department of ETE, DIU

(Internal Examiner)



5. Dr. Saeed Mahmud Ullah

Member

Associate Professor

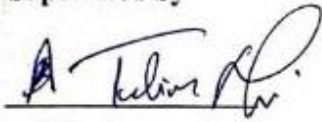
(External Examiner)

Department of ETE, University of Dhaka

DECLARATION

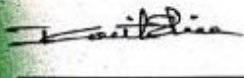
I hereby declare that, this project has been done by me under the supervision of **Md. Taslim Arefin, Associate Professor and Head, Department of ETE, Daffodil International University.** It is also declared that this thesis and any part of it has not been submitted elsewhere for the award of any degree or diploma.

Supervised by



Md. Taslim Arefin
Associate Professor and Head
Department of ETE, DIU

Submitted by



Kazi Talim
ID: 183-31-258
Department of ETE, DIU

LIST OF TABLES:

Table 5.1	: Next-Generation Firewalls Comparison	36
Table 6.1	: List of Tools and devices for Implementation and application. .	41
Table 6.2	: Firewall access security parameters	42
Table 6.3	: Performance Enhancement Report	68

LIST OF FIGURES:

Figure: 1.1	Architecture of Enterprise Network	5
Figure: 2.1	Most common Network Security Threats	10
Figure: 2.2	Active Attack	13
Figure: 2.3	Passive Attack	14
Figure: 2.4	Operation of a DDoS attack	15
Figure: 2.5	Statistics of phishing attacks	16
Figure: 2.6	Overview of SQL Injection Attack	17
Figure: 2.7	Fortinet Threat Landscape Index (top) and sub-indices for Botnets, Exploits, and Malware	19
Figure: 2.8	Most prevalent exploits, malware, and botnets for Q1 2019	19
Figure: 2.9	Five most targeted content management systems in Q1 2019	20
Figure: 2.10	Threat landscape report in Q1 2019	20
Figure: 2.11	Types of informations can be gained through data leakage	21
Figure: 3.1	Security Attack Cycle	29
Figure: 3.2	Role of a Next-Generation-Firewall	29
Figure: 4.1	Existing (experimental) Network Model of an Enterprise Network	30
Figure: 4.2	The working process of Fortinet firewall	32
Figure: 4.3	Authentication and Security process of Fortinet firewall	32
Figure: 4.4	Proposed Secured Network Model	33
Figure: 5.1	Community recommendations of NGFW	37
Figure: 5.2	FortiGate 300E Firewall	38
Figure: 6.1	Layers of security	42

Figure: 6.2	Access port customization	43
Figure: 6.3	SSH default port login restricted	44
Figure: 6.4	SSH secured login with port customization	44
Figure: 6.5	Web login port security	45
Figure: 6.6	Role based administrator (Read User)	45
Figure: 6.7	Compromised Host automation rule	47
Figure: 6.8	Automatically Ban IP addresses of compromised hosts	47
Figure: 6.9	Protocol authentication (RDP)	48
Figure: 6.10	Port Forwarding in FortiGate Firewall	49
Figure: 6.11	Service declaration in Port Forwarding policy	50
Figure: 6.12	Policy For Direct Internet Traffic without authorization	51
Figure: 6.13	Experimental Avg. Internet Traffic of an Enterprise Network.	52
Figure: 6.14	IP-Sec VPN tunnel (step-1)	53
Figure: 6.15	IP-Sec VPN tunnel (step-2)	53
Figure: 6.16	IP-Sec VPN tunnel (step-3)	54
Figure: 6.17	SSL-VPN configuration	55
Figure: 6.18	SSL-VPN web login page	55
Figure: 6.19	SSL-VPN web session	56
Figure: 6.20	Packet Capture of PPTP VPN (Unencrypted)	56
Figure: 6.21	Packet Capture of SSL-VPN (Encrypted)	57
Figure: 6.22	DoS Protection in fortinet firewall	58

Figure: 6.23	UDP flood prevented based on DoS Policy	58
Figure: 6.24	Web filtering configuration in firewall	59
Figure: 6.25	Unrated sites are automatically blocked	60
Figure: 6.26	Overrides required blocking websites to access	60
Figure: 6.27	Updated IPS signatures from global security database	61
Figure: 6.28	Intrusion detected and blocked immediately	62
Figure: 6.29	Logical view of whole network	62
Figure: 6.30	All active sessions are visible and under control of administrator	63
Figure: 6.31	Previous bandwidth utilization & CPU usages without firewall. .	63
Figure: 6.32	Resource utilization with optimized bandwidth using firewall. . .	64
Figure: 6.33	Avg. latency during regular usages before firewall integration . . .	65
Figure: 6.34	Avg. latency & packet drop during pick usages	65
Figure: 6.35	Avg. latency during regular usages after firewall integration	66
Figure: 6.36	Avg. latency & packet drop during pick usages	66
Figure: 6.37	Avg. page load time difference after incorporating firewall	67
Figure: 6.38	Ookla speed test result from user PC after incorporating firewall	67
Figure: 6.39	Enhancing Network Performance using NGFW	68
Figure: 6.40	Enhancing network security and operational management using NGFW	69

TABLE OF CONTENTS:

DECLARATION	iii
ACKNOWLEDGEMENT	xi
ABSTRACT	xii
1 INTRODUCTION	1
1.1 FIREWALL CONCEPT	1
1.2 ENTERPRISE NETWORK	3
1.3 WORK SCOPE	6
1.4 METHODOLOGY	7
1.5 AIMS & OBJECTIVES.....	8
2 THREAT & ATTACK ANALYSIS	9
2.1 MOST COMMON NETWORK THREATS	9
2.1.1 COMPUTER VIRUS	10
2.1.2 TROJAN HORSE	11
2.1.3 ROOTKIT	11
2.1.4 COMPUTER WORM	12
2.1.5 ADWARE AND SPYWARE	12
2.2 MOST COMMON SECURITY ATTACKS	13
2.2.1 ACTIVE ATTACK	13
2.2.2 PASSIVE ATTACK	14
2.2.3 DoS AND DDoS ATTACK	14

2.2.4	PHISHING ATTACK	16
2.2.5	SQL INJECTION ATTACK	17
2.2.6	MAN-IN-THE MIDDLE ATTACK	18
2.3	THREAT LANDSCAPE	19
2.4	DATA LEAKAGE IS A PROBLEM	21
2.5	IT'S HIGH TIME TO FIX THE FIREWALL	22
3	EVALUATION OF FIREWALL	23
3.1	LITERATURE REVIEW	23
3.2	BASIC CONCEPTS OF A FIREWALL	24
3.3	HARDWARE FIREWALLS	26
3.4	SOFTWARE FIREWALLS	26
3.5	HOST BASED VS NETWORK BASED FIREWALLS	27
3.6	TYPES OF FIREWALLS	27
3.7	THE NEXT GENERATION FIREWALL	28
4	PROBLEM STATEMENT AND PROPOSED SOLUTION	29
4.1	PROBLEM STATEMENT	30
4.2	PROPOSED NETWORK MODEL	31
5	FIREWALL PERFORMANCE AND FEATURES	35
5.1	NEXT GENERATION FIREWALLS COMPARISON	35
5.2	FORTINET FIREWALL PERFORMANCE & FEATURES	38
5.2.1	FEATURES	39
5.2.2	PERFORMANCE	39
5.2.3	CAPACITY	39
6	SECURITY ENHANCEMENT AND RESULT	40
6.1	SECURING THE FIREWALL ACCESS	41
6.2	SECURITY AUTOMATION	46

6.3	PROTOCOL AUTHENTICATION	48
6.4	PORT FORWARDING SECURITY	49
6.5	DEFAULT DENY POLICY FOR UNTRACKET TRAFFIC	51
6.6	SECURE VPN	52
6.7	SECURING THE DoS ATTACK	57
6.8	WEB SECURITY	59
6.9	INTRUSION PREVENTION SYSTEM (IPS)	61
6.10	NETWORK VISIBILITY & PERFORMANCE COMPARISON	62
6.11	FINAL RESULT	68
7	CONCLUSION	70
7.1	RECOMMENDATION & CONCLUSION	70
7.2	FUTURE WORK	71
7.3	REFERENCES	72
7.4	APPENDIX-A	74

ACKNOWLEDGEMENT

First and important my heartfelt and sincere gratitude goes to Almighty Allah who has enabled me to successfully complete my entire thesis. I would first like to thank my thesis advisor **Md. Taslim Arefin** who was always open whenever I ran into a trouble spot or had a question about my research work or writing. He consistently allowed this thesis to be my own work, and also advised me in the right the direction whenever he thought I needed it. Finally, I must express my very profound gratitude to my parents and to my friends and for providing me with unfailing support and continuous encouragement throughout my years of study and through the process of master and this thesis. This accomplishment would not have been possible without them. This thesis is dedicated to my family, who have been most understanding during the process of writing. Thank you.

ABSTRACT

This thesis described about the necessity, deployment considerations, performance evaluation and the possible outcomes of using the next-generation firewalls (NGFW) in an enterprise network environment. A firewall is the most important component for any system considering their information security because it's the first line of defense against every known and unknown security attacks. Security threats come with a big deal to any enterprise network, these threats always try to penetrate into system's confidentiality, integrity, and availability. Firewalls are designed to provide security against these threats, however, it can be more effective by timely implementation and fine-tuning of the configurations according to the network requirement. In this thesis, we have described how the security threats are vulnerable to systems with their possible impacts. We also differentiated between different types of firewalls based on their features and capacities which could help anyone to choose the optimal one for any network environment. And, finally we have also showed how to better handle these firewalls to mitigate the impact of latest security attacks without considering network performance using Next-Generation firewall technologies. Our proposed network model using NGFW improved a lot of segments of an existing network which was previously running without a firewall. Our experimental results could give a clear idea about how much improvement could be gained in network performance and security by using our recommended Next-generation firewalls.

CATEGORIES:

Computer network and information security.

GENERAL TERM:

Security

KEYWORDS:

Network Security, Information Security, Firewall, Traffic, Attacks, Throughput, Intrusion detection/prevention.

CHAPTER 1

INTRODUCTION

1.1 FIREWALL CONCEPT

In this modern era of technology, the use of computer systems in personal and commercial sectors makes it possible together and share information with each other using the internet. Thoughts are not hidden inside now, it's global on the internet world. Now, we can do many banking operations, academic activities or shopping via the internet. Many companies are presenting themselves on the internet where their data should keep safe from any type of attack. Here comes the concept of network security.

TCP/IP was primarily developed to ensure reliable communications between different networks. At that time, security was not a concern at all. The internet was not so vast covering very specific small networks. In that sense, the base technologies behind this network contained many insecurities, most of which continue to exist today. A decent number of well-reputed attacks already take place on sensitive private networks originated from the internet. Finally, security is the biggest concern nowadays. Organizations need to conduct their business in such a secure manner to protect their data and resources from internal, or external attacks.

To secure a private network the organization first needs to deploy some security policies based on a business strategy and their privacy requirements. For example, any financial organization like a bank cannot consider their security policies as a publicly accessible network like social sites. A network security policy defines which connections are allowed between the privates and external networks and the actions to take in the event of any security breach. A firewall has a

great role to perform this task here. A firewall placed between the private network and the Internet enforces the security policy by controlling what connections can be established between the two networks in a secure manner. All network traffic must pass through the firewall, which ensures that only permitted traffic passes based on applied policies. The primary objective of using a firewall is to protect unwanted access to or from any private network. [1]

Things to keep in mind that, a firewall is nothing but a machine that performs based on your applied policies. The common difference between a firewall and a router is that “By default, all allow for a router & by default all deny in case of the firewall”. A firewall only allows traffic mentioned in your policies. It should not be forgotten that firewall itself also is open to security attacks. Any problem with the operation of the firewall, due to malfunction or hacking could be disastrous to other less protected systems on the Internal network.

The research will focus on answering the following questions:

-Types of security threats and attacks.

- What potential risks and security attacks encourage the enterprise network to adopt firewall systems as well as what consideration to keep in mind during choosing a suitable firewall based on business requirement?

-What is the significance of performance and security features that can be delivered by firewalls in any enterprise network?

-Deployment considerations, fine-tuning process with risk management recommendations.

1.2 ENTERPRISE NETWORK:

An enterprise network is a network which helps to connect associates PCs and related gadgets crosswise over offices and workgroup systems. An enterprise network decreases correspondence conventions, encouraging framework, and gadget interoperability, and also enhanced interior and outside enterprise data management. This venture also called a corporate network.

The key motivation of an enterprise network is to eliminate different client and workgroups. All method should be able to communicate with each other and provide and recover data. Also, physical process and devices should be able to maintain and give favorable performance, reliability, and security. Enterprise computing models are developed for this purpose, facilitating the exploration and improvement of established enterprise communication protocols and strategies. [2]

In scope, an enterprise network may include local and wide area networks (LAN/WAN), depending on operational and departmental requirements. An enterprise network can incorporate all process, including Windows and Apple workstation and operating systems (OS), UNIX systems, mainframes and related devices like smartphones and tablets. A closely incorporated enterprise network effectively joins and uses different device and system communication protocols. [2]

Enterprise network Includes different kind of service and server. In this service there are both public and private access. For example, web-based services could be accessed by different clients from various networks, they can also get into other services like database services. Users from Internet, internal network, and branches networks can access their e-mail and FTP accounts. For security purpose, access to database servers is restricted from internal network, it should not be obtain from public network. EN contains various networks, each network has its function, users, devices, and technology. [2]

Securing servers of the enterprise network are essential, they must be available and secure. Enterprise network has various needs, it needs availability, scalability, security, and mobility.

Users at any time and from anywhere should be able to connect to services hosted at enterprise network. There are different techniques that should be implemented within the enterprise network to maintain availability. Unavailability of services damage enterprise prestige, it accommodates its business. Fast recover will avoid service unavailability, a business cannot tolerate failure, and it costs many. Various technology and mechanisms are used to defeat this shortcut, failover technology is such one. It becomes harder to maintain availability as more services are distributed in an enterprise network. Accelerated growth in an enterprise network is critical, enterprise network should be able to connect more branches networks. WAN devices such as routers should be range enough to connect new branches, we need not change the whole infrastructure of the enterprise network. In addition, enterprise network requires a scalable wireless network, so it can connect new wireless sites. Scalability permits continuation without the need to change enterprise network infrastructure.

Today most users have smartphones like android, iPhone, these phones require a wireless connection. Enterprise network should support mobility for wireless devices in order to enable mobile users to access enterprise network service from anywhere and at any time. There are different wireless technologies that can be used in an enterprise network. Wi-Fi is a wireless technology that intends to connect user inside enterprise network, they usually used for the indoor connection. It may be possible to use Wi-Fi to connect branches networks but it still limited in the distance that it covers. On the other hand, WiMAX is used to connected branches networks of large distance, it needs more equipment and devices than Wi-Fi. WiMAX connects both sites and remote users to the enterprise network. Giving a protected enterprise network is not an easy job, it needs more efforts, money, and devices. We cannot figure the enterprise network without security, it will be a big problem.

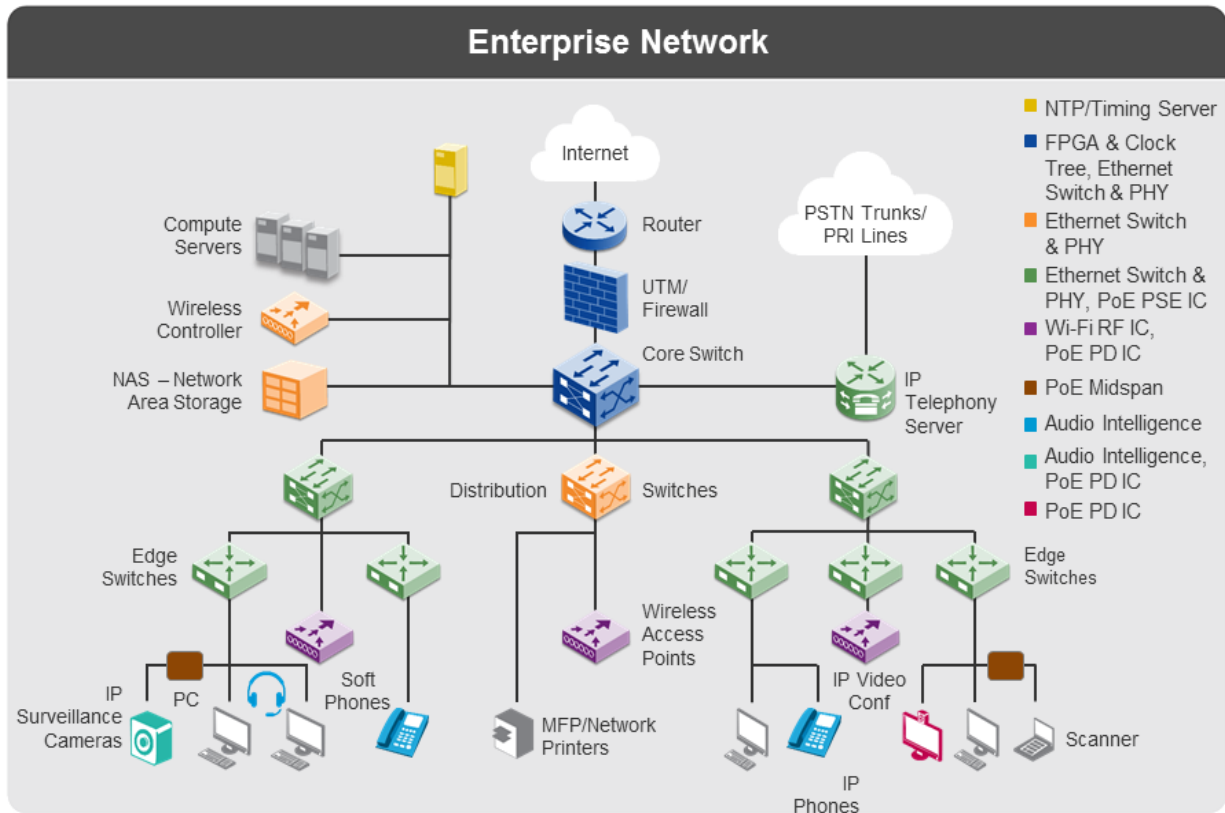


Figure: 1.1 – Architecture of Enterprise Network

So, Enterprise network management is an important task that administrators should care about it. According to the diagram (figure: 1.1), analysis and collecting information from different networking devices and users is necessary for monitoring and controlling EN. Most monitoring devices use SNMP protocol to collect information about network devices, they may also need to enable syslog service as well. Authors in proposed an Enhancing Enterprise Network Management using SMART, they try to make management of heterogeneous devices flexible and reliable. The paper utilized mobile agent technology for enterprise network in order to plan a hierarchical network management structure. It aims to manage 4 dynamic evolving network components using distributed network management, flexible coordination and runtime topology discovery.

Based on the importance of Enterprise network security, we chose this master thesis topic to study regarding solutions about enhancing computer security. No absolute safety solution is

possible, in order to secure the information over a network, we need to construct multiple layers of protection. A firewall is the outmost layer of the system. In this paper, we will briefly elaborate on the concept of Network security of an enterprise network, how it can be done in the past. And with the emergence and increasing use of internet how security threats are pointed to our devices is also studied. The goal of this thesis is to study the basic concepts of a firewall, threats to computer network security, firewall topologies, how they work and deployment of open source firewall products. And finally a secure network model of an enterprise network.

1.3 WORK SCOPE:

First, we put firewall concepts into a network system, the necessity of firewalls, describes how they work and how to classify their types. Looking closer to a typical firewall configuration gives us more ideas on how the components work together simultaneously to provide the desired level of data security.

To choose from several vendors, a comparison table gives us an overview which gets best matched with our requirements. Feedback from the managers of enterprise systems and international security forums gives us confirmation on our selection.

In the second part, we will describe the deployment considerations along with network configurations. Fine-tuning of network configurations resulting best possible performance which enhanced overall network security.

By the end of this study, we give some recommendations on how to better handle these Next-Generation Firewalls and suggest for the best utilization of their endless features to protect our valuable data. The final part covers what we have done and raised some questions for future investigations.

1.4 METHODOLOGY:

Hardware requirements for this thesis	: Fortinet Firewall and Physical Server
Software requirements	: Forti OS & Forti-Analyzer
Network environment and users	: Experience the changes of configurations

Theoretical analysis of current threats and attacks gives an answer to define the requirement behind the firewall into a network system. Understanding of network requirements to ensure the best possible information security can take place during the selection of firewalls from available suppliers. Firewall's features and a detail comparison chart always helps to select the best-desired device for any network. Need a physical or VM based Fortinet device to experiment with the outputs by varying different configuration parameters. This fine-tuning process always helps us to achieve the desired values. UTM features of NGFW supports to minimize the security issues and perform the required filtering using their updated global security database. Excluding the UTM features, firewalls are just like a traditional router that can't perform against any security attacks. In this thesis study, a Fortinet firewall including the latest UTM features (Web filter, Antivirus, IPS, Application filter) gives us the experimental values and we will use Forti-Analyzer to explore the network traffic and security threats.

1.5 AIMS & OBJECTIVES:

Our main target is to implement secured enterprise level network to ensure data security without considering network performance. To defend against latest network threats & attacks and to mitigate the existing solution vulnerabilities, we are introducing Next-Generation firewall technologies to be incorporated with the existing system. The specific objectives of our thesis study belongs to as follows –

- To examine the pattern and impact of different network security threats and attacks
- To acquire sound knowledge for designing an better handling of enterprise level networks
- To explore firewall technology and their advanced security features
- How to select the best firewall considering business requirement and network compatibility
- Examine the deployment process and their best possible usages in production network
- To give you recommendation on firewall configurations to get best possible performance
- To show you how the implementation of firewalls can upgrade your existing network in a most secured manner

CHAPTER 2

THREAT & ATTACK ANALYSIS

2.1 MOST COMMON NETWORK THREATS

Since the internet was created in the 1960's thousands of researchers were working for creating a reliable network. From those early days, several network attacks forced them to think twice about implementing network security. In that small era of internet, no one suspected that from the very few numbers of internet users, they would turn against each other.

In the 1980s, a hacker meant to people that you belong to an exclusive group. We had a club at that time named "Chaos Computer Club" in Germany and Legion of Doom in the USA, both are still widely renowned hacker groups. The term "hacker" was introduced in the 1960s, at MIT's artificial intelligence labs, which was referring to a specialized group of people working and programming in FORTRAN.

The 1970s saw a number of phreaking attempts. One notable case involved a friend of Joe Joy bubbles dubbed "Captain Crunch," who devised a way to make free long-distance calls.

But today we're going back to basics — exploring and explaining the most common network security threats you may encounter while online. [3]

SECURITY THREATS

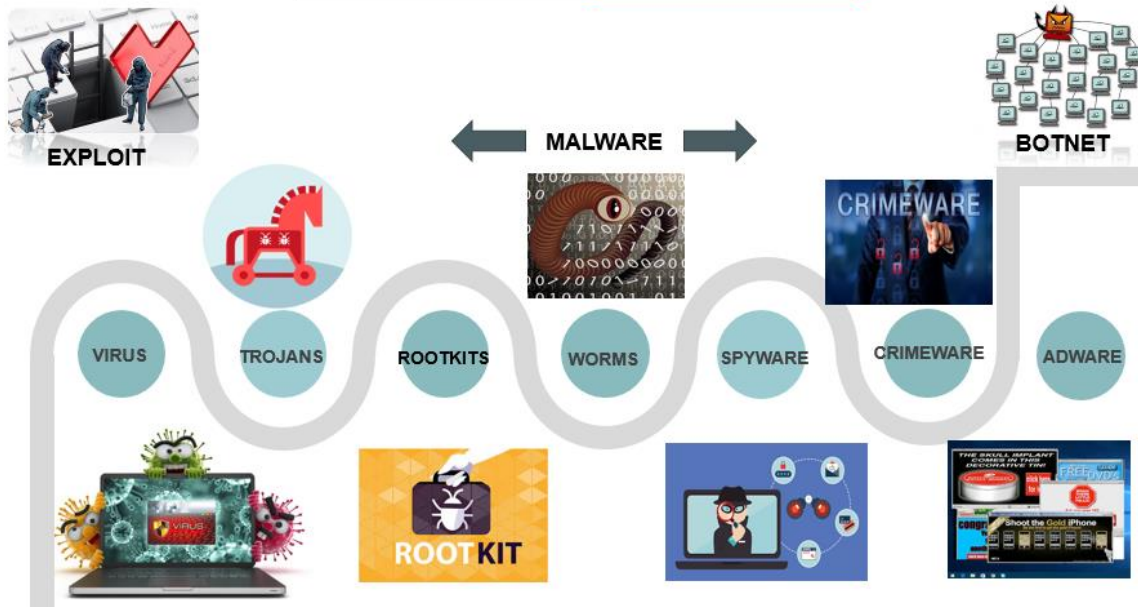


Figure: 2.1 – Most common Network Security Threats

2.1.1 Computer virus

Computer viruses are very similar to a pieces of software that are intentionally designed to spread from one computer to another. Almost all the viruses keep themselves hidden into an executable files that may come into your computer by some unauthorized files download or from infected sources. That means viruses are not able to spread into your system, unless any user execute those files by themselves.

Viruses often originates on the internet and spreads by downloading the infected files from the internet. It can also spreads by peer to peer file sharing or even through email attachment. Statistics show that, approximately 33% of home computers are affected with some type of malware, where more than a half of them are affected by viruses.

2.1.2 Trojan horse

A Trojan horse or “Trojan” is a malicious bit of attacking code or software capable of misleading users for running it willingly, by hiding behind a legitimate program that we regularly use in common scenarios.

Trojans not only steal our data, but they can also give access to cyber crooks into our system. Trojans are usually used to gain access to our computer's financial and personal information. Trojans can spread often by an email from someone we know, and when anyone clicks on the email and the included attachment, we've immediately downloaded the linked malware to our computer. Trojans also can spread when we click on a false advertisement.

Once inside any computer, that Trojan horse can record your passwords by logging keystrokes, hijacking the webcam, also may stealing any sensitive data we may have on our computer.

2.1.3 Rootkit

The name Rootkit derived from the concept of root access in the operating system UNIX which allow to change files and settings. Rootkit is a collection of software tools that is capable to activate remote control even administrative level access over a computer system or networks. Once remote access is obtained, the rootkit can perform multiple malicious actions on that computer. Rootkit is very tough to identify and remove for its concealing behavior.

Rootkits are installed by hiding behind any legitimate software. After getting permission by any user, those software's can make changes into our OS. Thus rootkits are installed itself in our computer and waits for the hacker to activate it. Other ways of rootkit spreading include phishing emails, unrated or malicious links, infected files, and downloading software from suspicious websites.

2.1.4 Computer worm

Worms can replicate themselves and spread themselves into multiple computers causing major damages. Network worm often use computer networks to spread, slowing down network traffic and enforce security failure of out dated systems. A virus needs support from a host file to stay and need execution to perform but worm is a standalone software that doesn't need human help to be executed. The best practice to keep our computer safe from worms by keeping our operating system clean, downloading regular patches, updates and ensuring our computer is protected by any updated anti-virus software. [4]

2.1.5 Adware and spyware

Adware is a kind of software that supports advertisement. Adware usually comes with bundle when download any other software's which is designed to recover the development cost of the original software. By this way, developers are able to provide the software for free and also get their development cost from the adware. Adware often designed to collect user's data like which website we visited.

The adware clause is often hidden in the related User Agreement, but it can be checked by carefully reading anything we accept while installing any software.

Spyware working architecture is exactly similar to adware. The only difference is it usually installed on our computer without our acknowledgement.

2.2 MOST COMMON SECURITY ATTACKS

Networks are most effective subject to attacks from different malicious sources. The principal classifications of Attacks can be from two classes:

- Active attack
- Passive attack

2.2.1 Active Attack

The attacker always tries to directly break into secured systems while the communication is ongoing during an active attack. Viruses, worms, or Trojan horses are the agents for a successful attack. Active attacks include attempts which can break protection features and able to steal or modify private information. Unauthorized attacker monitors, listens and also modifies the data packet in the communication channel known as an active attack.

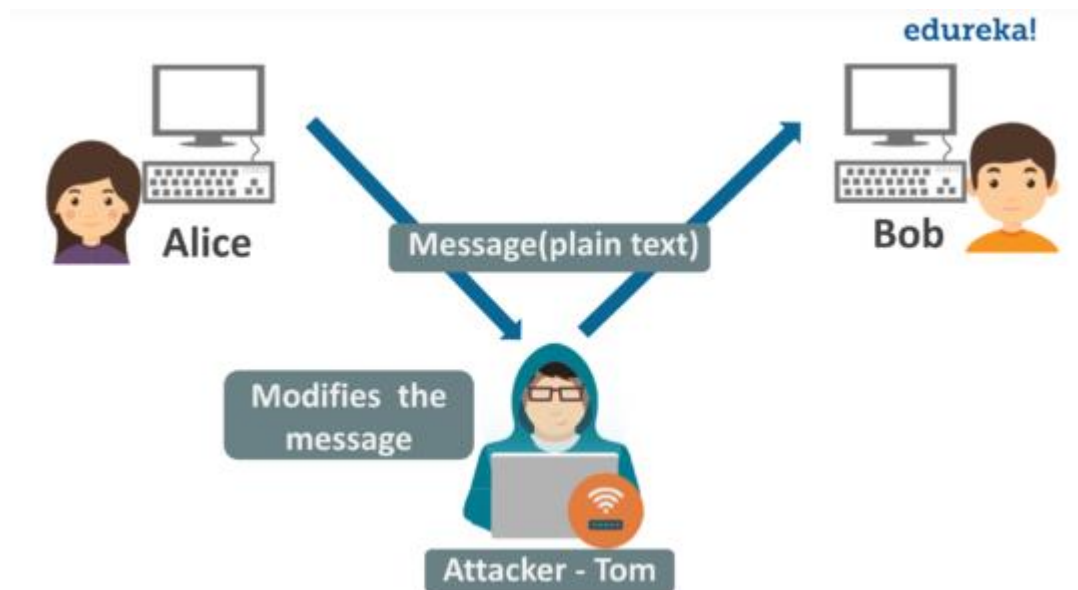


Figure: 2.2 – Active Attack

2.2.2 Passive Attack

A passive attack only monitors unencrypted traffic and searches for sensitive contents like passwords or credit card information that can be utilized in different sorts of future assaults. Passive attack includes traffic analysis, observing of unencrypted traffic, decoding pitifully scrambled traffic, and catching authentication data, for example, pin codes or passwords.

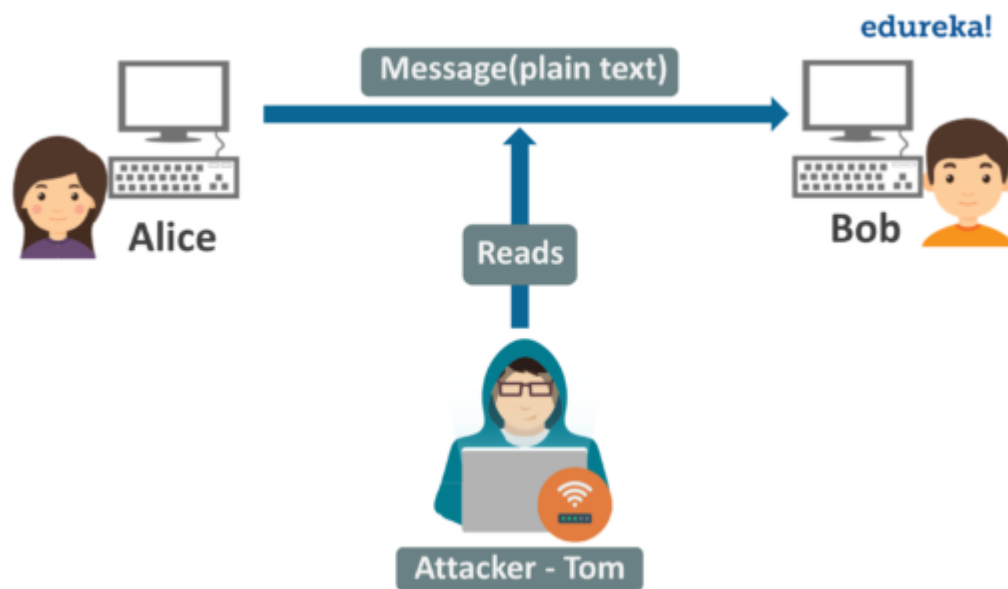


Figure: 2.3 – Passive Attack

2.2.3 DOS and DDOS attack

Sometimes we may be waiting impatiently for the online release of a product, that we eagerly waiting to purchase. At the final moment, we keep refreshing the page and waiting for the moment when the product goes live and we can order. And, during the final try by refreshing the page, it shows something like “Service Unavailable” or some error code.

Or, on the day of any vital result published on a national website, everyone is trying to access the site within the same time period, then the site then goes overloaded. [6]

The second example is general and very practical with the condition. But, there are a lot of cases like these where a website's server gets overloaded with traffic and simply crashes during critical business hours. This scenario often happens to a website due to a huge amount of malicious traffic overloaded to the specific site by the attackers. When a website has that huge amount of broadcast traffic, it's quite impossible to serve its original content to the legitimate visitors.

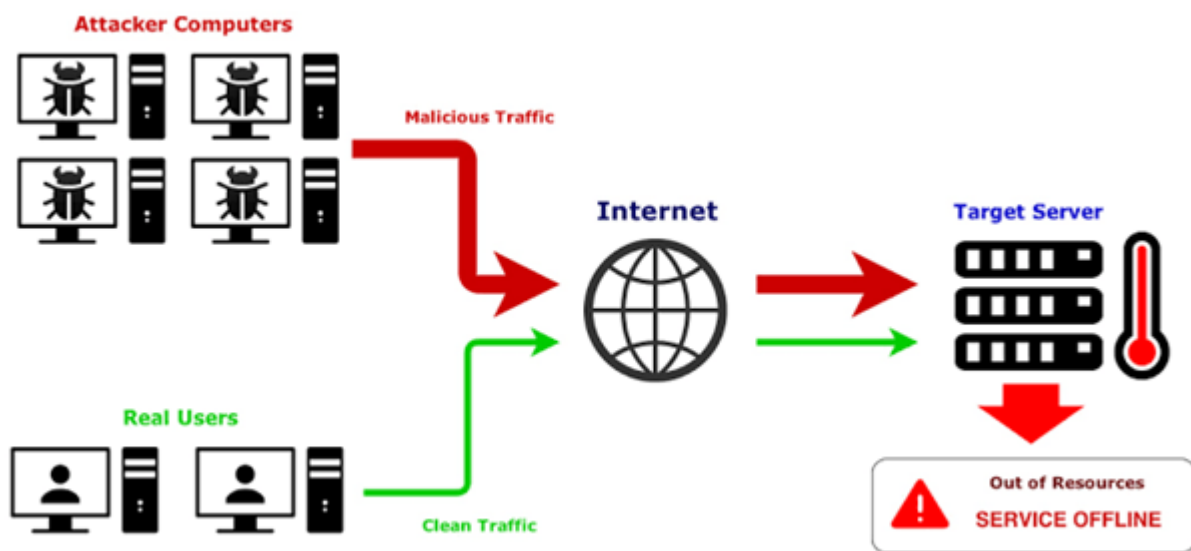


Figure: 2.4 – Operation of a DDoS attack

As the attack comes from so many different IP addresses simultaneously, a DDoS attack is much more difficult for the victim to locate and defend against in real-time.

2.2.4 Phishing

Phishing is a kind of social engineering with the target of getting users sensitive data such as credit card information, secret passwords or important financial data. The pattern of this attack mostly come as instant messages or phishing emails which actually designed to appear legitimate to the users. [7]

This kind of phishing messages or mails can also obtain personal informations by approaching like it sent from a bank, asking to verify your identity by providing some private information. [8]



Figure: 2.5 – Statistics of phishing attacks

2.2.5 SQL Injection attack

Many servers storing data for websites using SQL programming language. With the continuous up-gradation of technology, network security threats have also been advanced which leading us to the threat like SQL injection attacks nowadays.

SQL injection attacks are well designed to target data-driven applications by exploiting the available security vulnerabilities in the application's software. Malicious codes are used to collect confidential data, modify and even destroy that original data. Nowadays it is treated as a dangerous privacy issue for data confidentiality of any business applications.

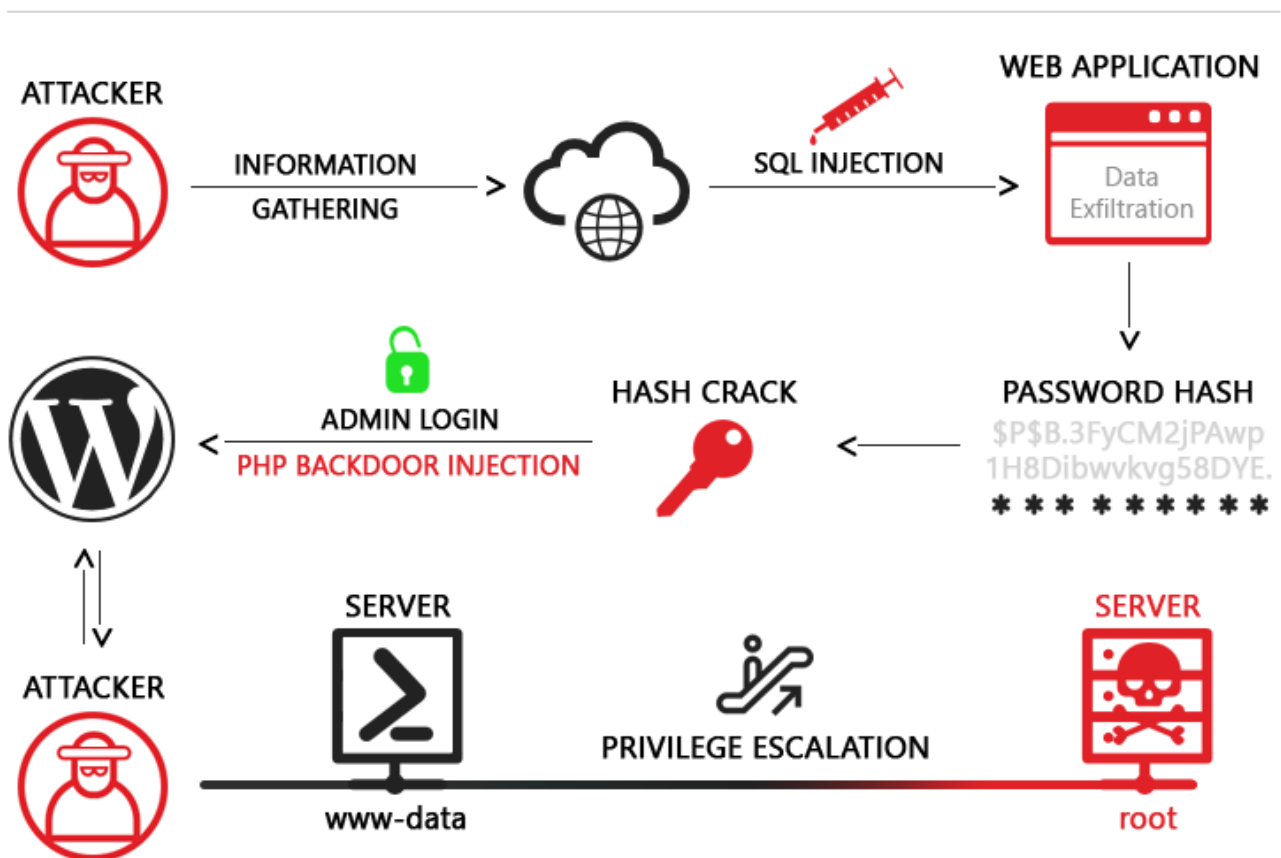


Figure: 2.6 – Overview of SQL Injection Attack

2.2.6 Man-in-the-middle attacks

Man-in-the-middle attacks are one of the most common cybersecurity attacks where the attacker eavesdrop during the communication between two authentic users. By this attack, attacker can listen to the communication already running which should be private in normal cases.

For an example, a man-in-the-middle attack happens when the attacker wants to intercept an ongoing communication between two users. Let's assume user X and Y are on a running communication over the network. At first, user X sends their public key to user Y, but the attacker intercepts the communication and sends a forged message to person Y, representing his identity as original user X. Instead of getting it as attacker's public key, user Y believes that the message comes from user X and as a result encrypts the message with the attacker's public key and send back to user X. During this, attacker again intercepts the message and re-encrypts it by the public key that was previously provided by user X. Finally, when the message is transferred back to person X, he believes it comes from person Y, and by this way an attacker stands in the middle that eavesdrops the communication between two targets. Below are just some of the types of MITM attacks:

- DNS spoofing
- HTTPS spoofing
- IP spoofing
- ARP spoofing
- SSL hijacking
- Wi-Fi hacking

2.3 THREAT LANDSCAPE

First quarter of 2019, exhibits more volatility than previous quarters (especially for malware), but the extent of those shifts is not unprecedented. Overall, the Index rose a little over 1% during the quarter to close at 1017. [9]

Below are few statistical references from fortinet site to understand the current threat scenario –

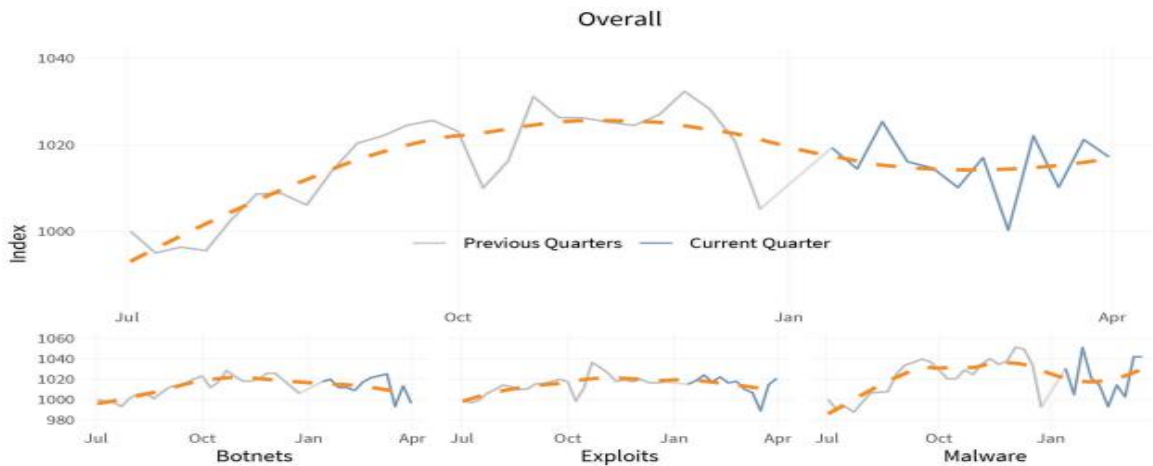


Figure 2.7: Fortinet Threat Landscape Index (top) and sub-indices for Botnets, Exploits, and Malware

Exploit Targets		Malware Families		Botnets	
1.	MS IIS	1.	MSOffice/CVE_2017_11882	1.	ZeroAccess
2.	ThinkPHP	2.	W32/Agent	2.	Andromeda
3.	Apache Struts	3.	JS/ProxyChanger	3.	H-Worm
4.	D-Link 2750B	4.	W32/Kryptik	4.	Conficker
5.	MS Windows	5.	Riskware/Refresh	5.	Sora
6.	Netcore Netis	6.	Riskware/Coinhive	6.	Emotet
7.	DASAN GPON	7.	W32/STRAT_Gen	7.	XorDDoS
8.	WebRTC	8.	Android/Hiddad	8.	Necurs
9.	Apache Tomcat	9.	Riskware/Generic	9.	AAEH
10.	Linksys	10.	Android/Generic	10.	Torpig

Figure 2.8: Most prevalent exploits, malware, and botnets for Q1 2019.

In March this year, we had reports of a Russian threat group compromising hundreds of WordPress and Joomla websites even using the sites to distribute ransom ware and phishing pages. [9]

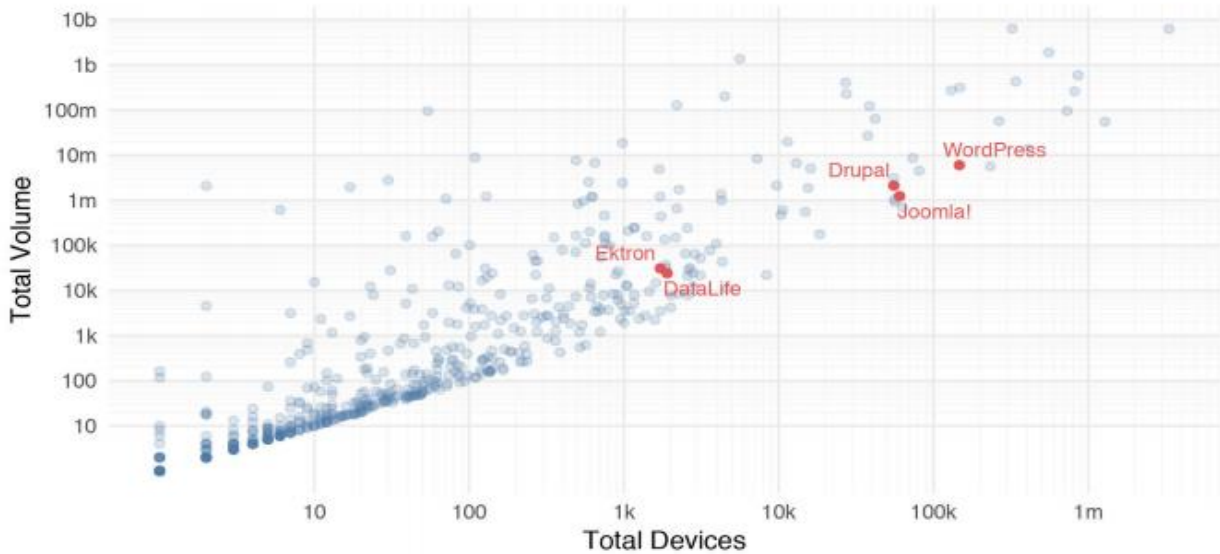


Figure 2.9: Five most targeted content management systems in Q1 2019.

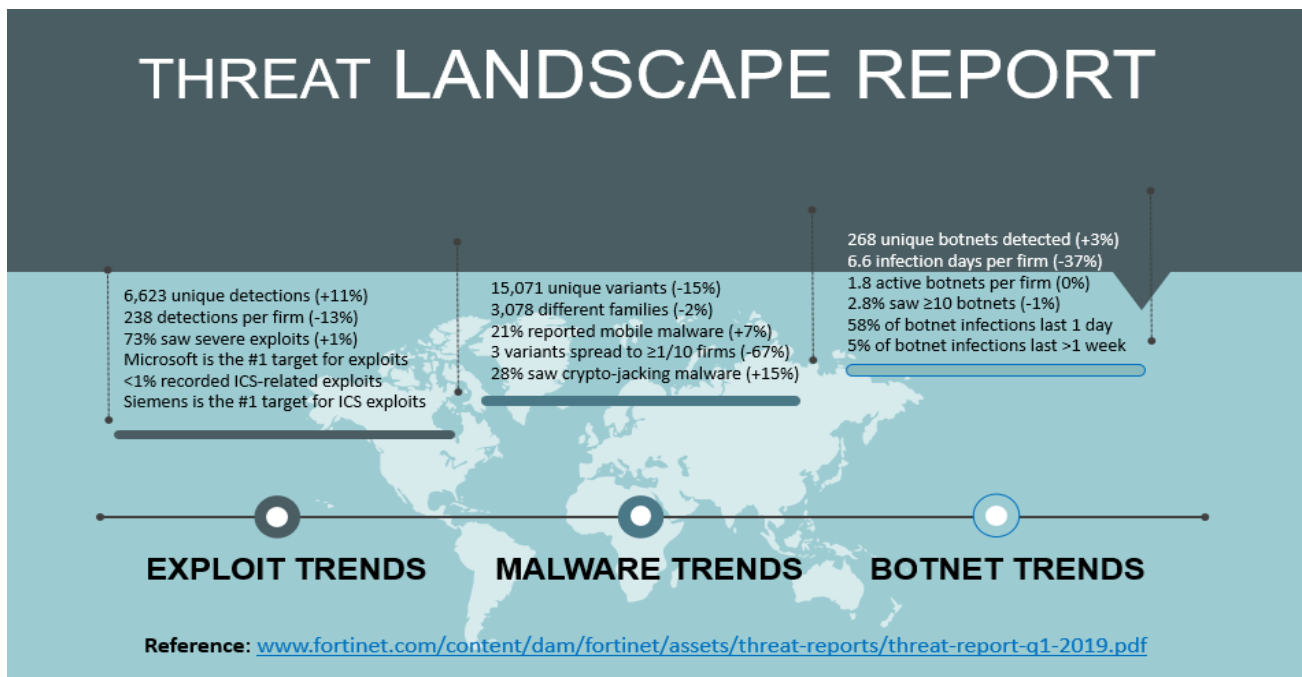


Figure 2.10: Threat landscape report in Q1 2019

2.4 DATA LEAKAGE IS A PROBLEM

One of the biggest problem for any public or private organization is data leakage. There are thousands of examples of accidental and intentional data leakage which randomly make newspaper's headlines. The firewall can sit in the perfect location to prevent these kind of data leakage because of seeing all traffic traversing different networks and network segments for an organization. Unfortunately, previous legacy port and protocol-based firewalls can't do anything to protect applications, users, or contents from current patterns of data leakage. [10]

To effectively address data leakage with a firewall solution, organizations should have -

- Gain proper control over the used applications on their network
- Scan the applications for vulnerability, update their firmware and ensure patch management
- Should have enough idea about which users are using different applications and why?
- Implement strong control policies to prevent accidental or intentional data leakage

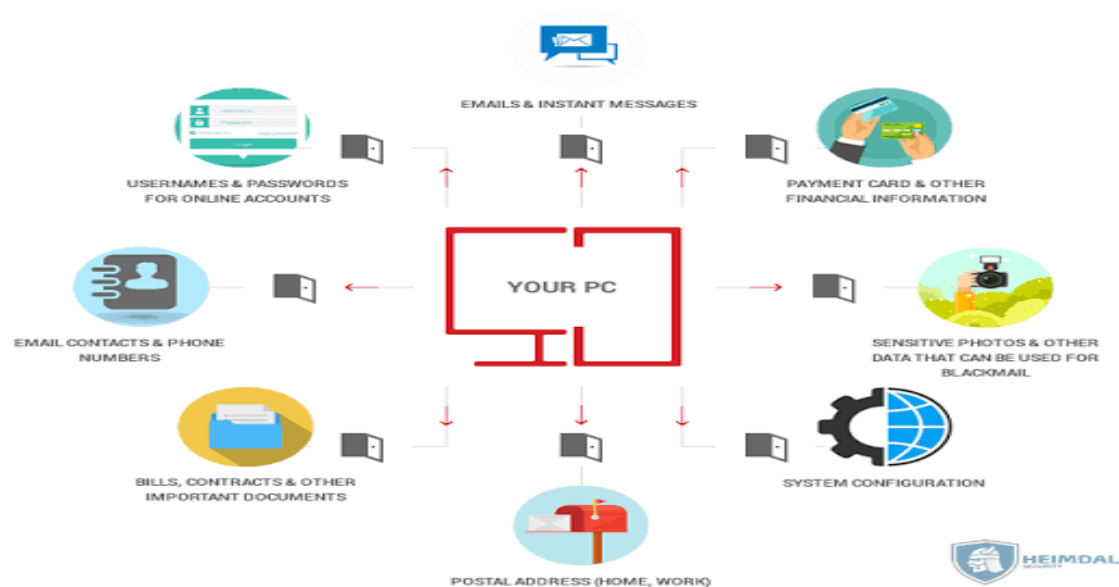


Figure: 2.11 – Types of informations can be gained through data leakage

2.5 IT'S HIGH TIME TO FIX THE FIREWALL

We should have noticed that, nobody gets excited anymore about a firewall anymore nowadays. There was a time, when the single most important security device in any commercial network was firewall. We need to know, what actually happened here and what are those big changes that make this happen?

Few years ago, most of the firewalls did a pretty good job of controlling traffic with ensuring security in and out of maximum corporate networks. That's because application traffic was usually well behaved and specified like –

E-mail traffic would typically flow through port 25,

FTP was assigned to port 20,

Web surfing usually done through port 80

That time policy and rule means “ports + protocols = applications” and as a result, firewall had everything under control with its characteristics. Blocking a port simply meant blocking an application during the time. Very plain and simple rule was applicable for traffic shaping. But, the Internet has never really been so decent and simple from time to time till date. Nowadays, 70 percent or more of the traffic on your corporate network is internet traffic. And it's not just port 80 means Web surfing anymore. Typically, 20 to 30 percent of it is encrypted SSL traffic on port 443 but what about the rest? As a result, most of the new threats can go through your existing firewall undetected because it's still playing by rules that don't exist anymore in this modern era.

So, it's high time to change your existing traditional firewall to support application level security by deploying Next-Generation firewalls in your commercial network.

CHAPTER 3

EVALUATION OF FIREWALL

3.1 LITERATURE REVIEW

Firewalls have a set of rules, responsible for granting access into and out over the network through the device. These rules are the key element to control any kind of traffic flow. The firewall is responsible for acting as a point of demarcation or a traffic warden within the network as every communication needs to flow from it and this is the area where traffic is given access or access is rejected. Point to be noted that, rules will work according to first match.

Previous discussions of distributed firewall architectures can be classified as two main types:

- 1) Architectures that employ centralized policy management with end-point enforcement and
- 2) Defense in depth architectures.

A well-known work discussing distributed firewalls was given by Bellovin [11]

There has been a massive & continuous change in firewall technology for maintaining the dynamic changing needs of network security. Established initially as an approach to allow or restrict external accessibility to specific resources of the network, current capability is enjoyed by firewalls to enforce policies of network security, internet activity of logging and security of business exposure to external threats [12]. Firewalls can be defined as extremely effective for effective authentication of users, enforce policies of network society and activity of internet and logging. Enterprises consider the utilization of firewalls as the defense of network perimeter for making efficient decisions of security and protecting the valuable hosts from external attacks on a private network. Need to keep in mind that,

firewalls are not effective in protecting the hosts in connection with internet network without being involved with the enterprise firewall. The use of internet without any authentication and reliability resulting expose of the host or user to any unwanted security attacks.

A firewall can successfully complement anti-virus solutions with the dynamic settlement of active rules on the basis of malware type. Even though deployment of firewalls can take place as a hardware or any software appliances. These systems have the ability of performing real-time introspection of every network traffic without affecting the throughput. A major combination of activated rules consistently filtering data packets finally affects the network performance and causing a bottlenecks. In future, firewalls should be able to differentiate between legitimate and illegitimate traffic for identifying and plugging any new threats automatically. The capabilities of anti-malware scanning are not beyond the firewalls capabilities in the current era, but the present performance of network affects the crucial needs of running an enterprise. While developing a secure network, the following needs to be considered.

- Accessibility – authorized users are provided the means to communicate to and from a particular network.
- Confidentiality – Information in the network remains private, Discloser should not be easily possible.
- Authentication – Ensure the users of the network are, the user must be the person who they say they are.
- Integrity – Ensure the message has not been modified in transit, the content must be same as they are sent.
- Non-repudiation – Ensure the user does not refute that he used the network.
-

3.2 BASIC CONCEPTS OF A FIREWALL

A firewall is completely as like as human skin. Skin, which does not truly kill foreign hostile bodies, it simply obstructs them to access.

Properly configured and deployed firewall operates as a shield around any network just as skin on a human body. A firewall executes by acting on traffic based on its configured policy. A policy is made by of a set of rules. A rule is an action which is taken on traffic that fit a certain predefined criteria. A single rule is comprised of four basic elements, they are –

Source

- From where the incoming traffic is coming from considering below terms -
- Single IP or multiple source IP addresses
- One or more networks by calculating their network ID and subnet mask
- Combination of IP addresses including their Network addresses

Destination

- Indicates where the originated traffic is going to considering below terms -
- Single IP or multiple destination IP addresses
- One or more networks by calculating their network ID and subnet mask
- A combination of IP addresses as well as their Network addresses

Service

- Service defines which protocol is used by the traffic considering below terms -
- Either, one or more destination TCP ports
- Or, one or more destination UDP ports
- Combination of destination TCP and UDP ports both
- Source port can be limited to a certain range, but it is generally left wide open. It is the destination port which is primarily specified.

Action

- Administrator can choose from the following options when all the above conditions matches –
- Reject the network traffic
- Drop the transmitted traffic

- Permit/Allow the legitimate traffic
- Encrypt the traffic flow where IPSEC VPN is capable inside firewalls

3.3 HARDWARE FIREWALL

Hardware firewalls are generally integrated with the router which sits between a computer and the Internet. They always use packet filtering by default, which means they always scan the every packet headers to determine their actual source, destination addresses and also check with the existing user list defined access policy to make an allow or deny decision. Key advantages of hardware firewall are specified as follows –

1. **Speed:** Hardware firewalls always gives faster response times, so it can handle more capacity of traffic loads.
2. **Security:** A firewall with its own operating system inside is less effected from security attacks. This reduces the security risk and hardware firewalls have enhanced security controls as well.
3. **No Interference:** As the hardware firewall is an isolated network component, it can be managed in better way, as a result it does not load or slowdown other running applications.

3.4 SOFTWARE FIREWALL

Software firewalls are just like an OS usually installed on individual server environment. They are able to intercept each and every connection request over the network and then determine whether the request is valid or not. Software firewall process those requests by utilizing the server resources. Apart from some performance related limitations, the software firewall has a vast amount of advantages. Key advantages of software firewall are mentioned as below -

1. Comparing with the hardware firewalls, software firewalls are easier to configure and setup.
2. Using software firewall, we can restrict some specific application from the Internet. This makes the software firewall more flexible to use.
3. Software firewall allows users full control over their Internet traffic through a simple user friendly interface that requires little or no knowledge to execute.

3.5 HOST-BASED VS NETWORK-BASED FIREWALL

A host-based firewall designed to be installed on last end individual computers only. The applied policy will affect only the traffic passed through the computer.

On the other hand, a network-based firewall is designed to deploy at a specified point in the network path and protects all the computers and other network component from internal or external security issues. But, a network-based firewall cannot protect one computer from another on the same network, or any computer from itself which can be performed by anti-virus software where host based firewalls are superior.

3.6 TYPES OF FIREWALLS

A firewall is a network security framework intended to keep unapproved access to or from a private network. Firewalls can be actualized as both equipment and software, or a mix of both. But the problem arises when we don't know which firewall we have to use. So to solve this problem we are making a classification so that we can select which firewall we have used according to our utilization. For the most part, firewalls are of three sorts. [12]

1. Circuit Level firewalls

2. Application level firewall
3. Packet filtering firewall

3.7 THE NEXT GENERATION FIREWALL

The Next-Generation Firewall (NGFW) comes with the solution of current network security issues. Starting with a blank slate, next-generation firewalls (NGFW) can classify traffic by the application's identity in order to enable proactive tracking, session's visibility and administrative control of all kinds of applications including Web 2.0, Enterprise 2.0, and legacy running on any kind of enterprise network.

As shown in below (figure: 3.2) a firewall always stands between the host and the internet to protect the identity of the host. Attacker has to face the layers of defends, when we use any network firewall in front of an enterprise system. Nowadays, the essential functional requirements of an effective next-generation firewall include the ability to –

- Identify applications specified by their port, protocol, evasive techniques, or SSL encryption before doing anything else
- Provide visibility of each sessions, policy-based control over running applications, including individual functions based on requirement
- Accurately track end users identity and subsequently use identity information as an attribute for policy control of those users over the entire network
- Provide real-time data protection against available network threats, including those operating at the application layer eventually
- Integrate traditional firewall system and network intrusion prevention capabilities to ensure best possible security

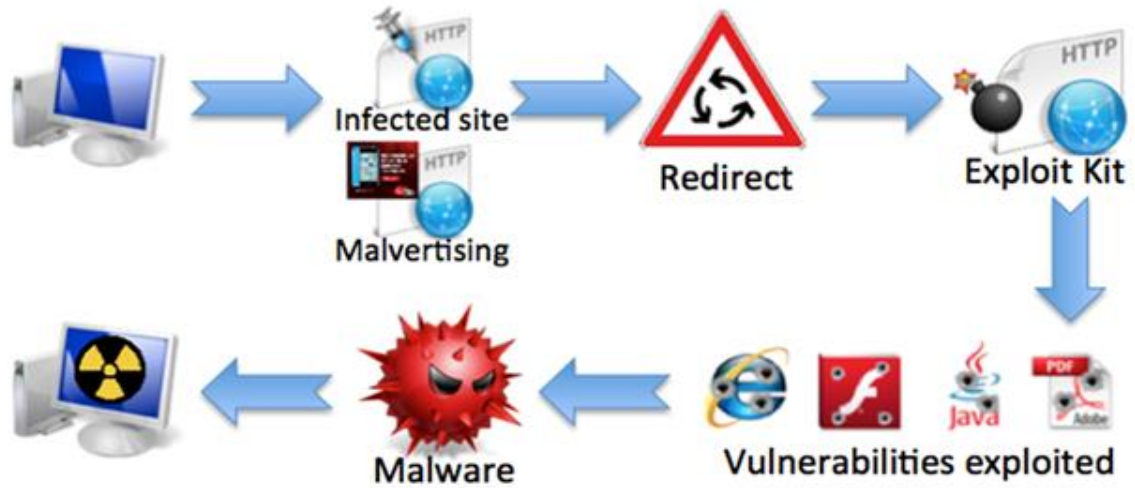


Figure 3.1: Security Attack Cycle

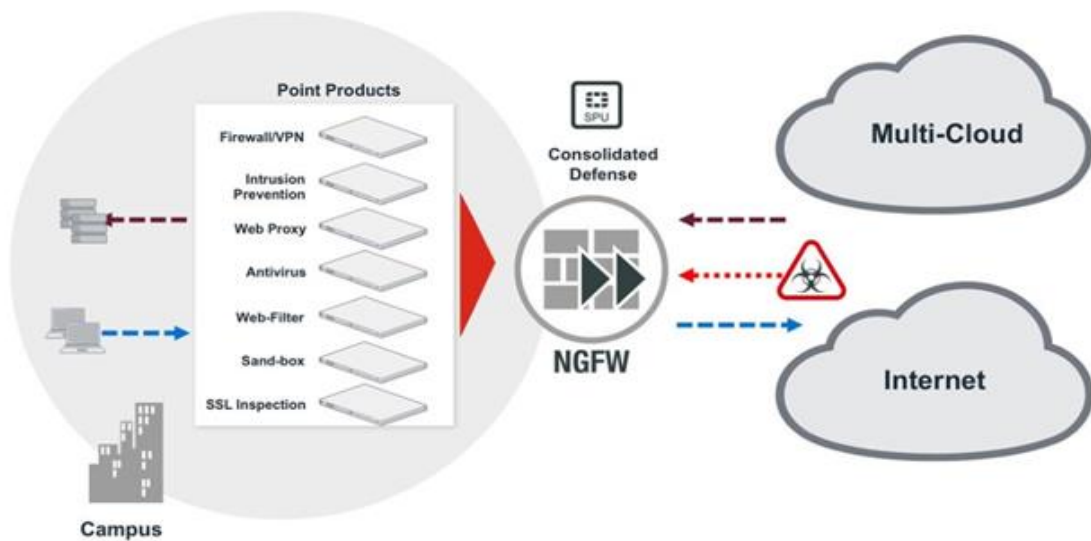


Figure 3.2: Role of a Next-Generation-Firewall

CHAPTER 4

PROBLEM STATEMENT AND PROPOSED SOLUTION

4.1 PROBLEM STATEMENT

A security architects think that how to provide major threat protection for their enterprises or any other platform including intrusion prevention, DoS attack, web filtering, anti-malware and various types of application control, will face a major complexity to hurdle managing these point products as well as no integration and lack of visibility. A prediction and Gartner estimates that by 2019, 80% of enterprise traffic will be encrypted and 50% of attacks targeting enterprise will be hidden in encrypted traffic. FortiGate Next Generation Firewall utilizes purpose-built security processors and threat intelligence security services from FortiGuard labs to deliver top-rated protection and high performance including encrypted traffic.

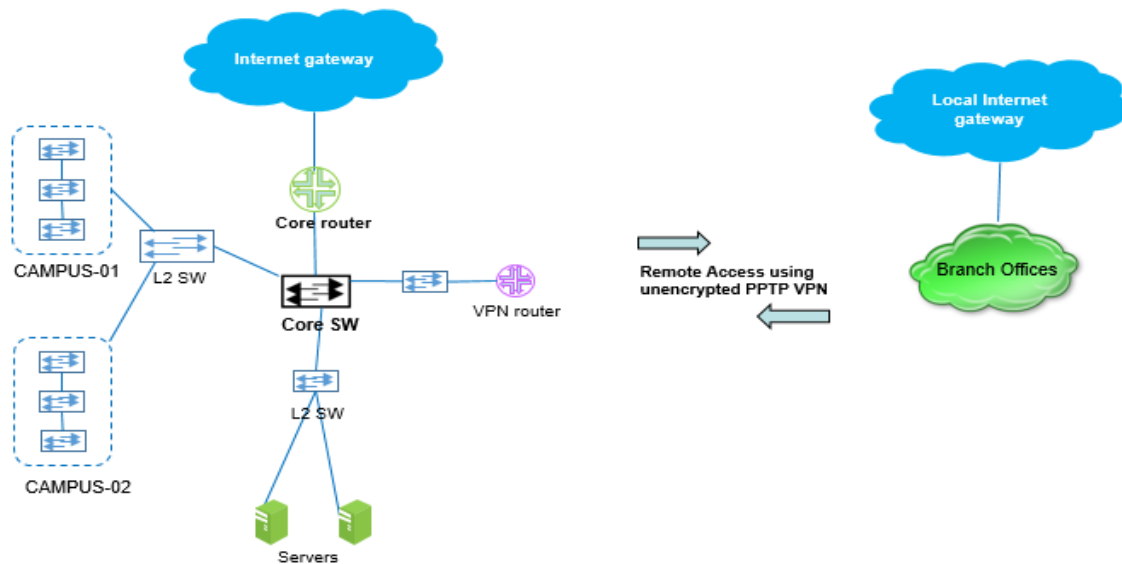


Figure 4.1: Existing (experimental) Network Model of an Enterprise Network

On the above network model (Figure: 4.1), everything will be running fine according to the business requirement but the thing is, there is nothing inside the network to protect against security attacks. Without active protection multiple crucial attacks can perform over this type of networks like,

- IP Spoofing
- Insider Intrusion
- Masquerade attack
- DDoS Attack

To defend these active threats NGFW has a proactive role based on their features and license. When the LAN is associated with another LAN or the Internet and turns into a WAN, the majority of that changes. The organization does not recognize what physical securities have been made to whatever remains of the WAN, just its little bit. On account of an Internet association, they have no clue who may endeavor to get to their LAN. The whole risk display changes. Not unreasonably any of the dangers from the LAN-just condition have left, yet a lot more have been included. One can think about the danger profile for a LAN similar to a subset of the risk profile for a WAN.

4.2 PROPOSED NETWORK MODEL

We will deploy Fortinet firewall and evaluate the result after deployment over an existing enterprise network environment. In the below diagram (figure: 4.2 & 4.3) the working mechanism and authentication system of our proposed fortinet firewall OS.

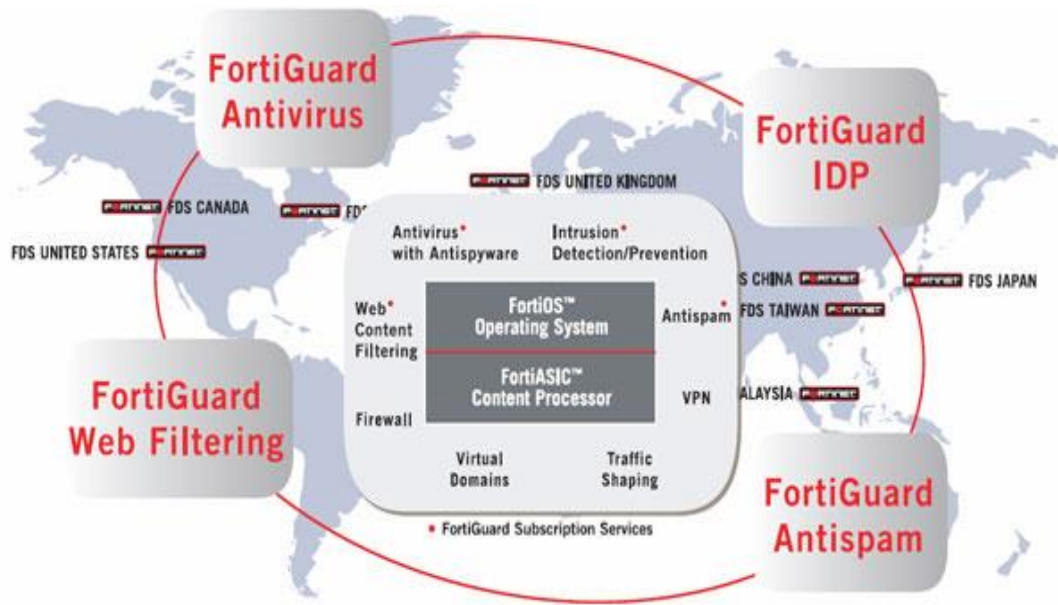


Figure 4.2: The working process of Fortinet firewall

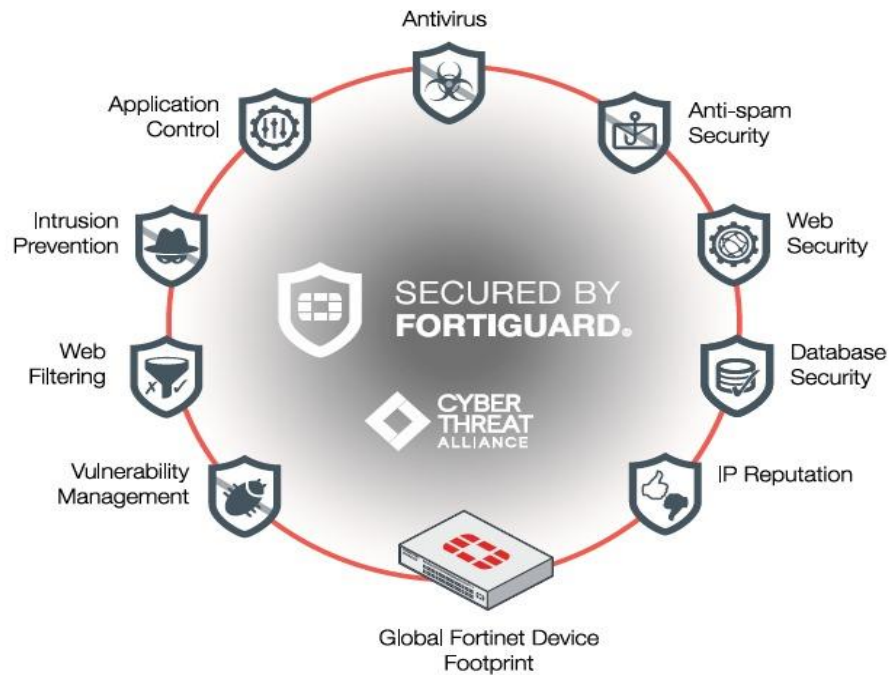


Figure 4.3: Authentication and Security process of Fortinet firewall

Security measures are appropriate or not depend on the threat profile that helps us to understand network management for a self-connected LAN network, Here no need to have network management protocol encryption or special authentication for those protocols, Network administrator does not want his network management protocols to traverse without the special authentication of internet protocols, So for any system first step is to identify the threat and then apply threat prevention policy to ensure security protection.

To avail these kind of security protections we are proposing a new model of enterprise network using a NGFW (Fortinet FG-300E) in front of the network.

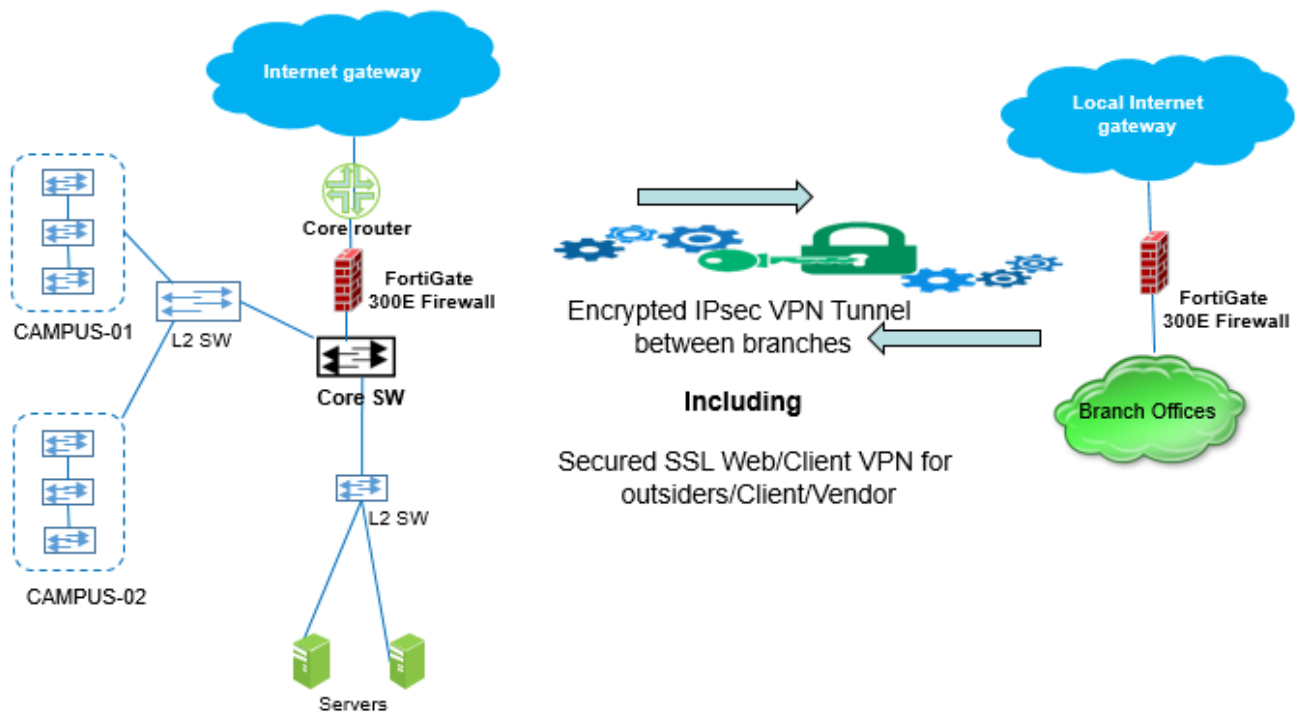


Figure 4.4: Proposed Secured Network Model

The proposed model will overcome most of the security issues of an enterprise network. Here are those probable improved part of the model given below:

- User authentication.
- Multilevel Protection.
- Protocol authentication.
- Forti View of all active sessions.
- Access policy.
- Network Traffic Encryption.
- Traffic scanning & filtering
- Virus, Intrusion, Spam filtering
- High Data Security and more.

In our coming chapter, we will briefly elaborate how the implementation of this diagram can upgrade overall network performance, specially the security parameters to protect our private data.

CHAPTER 5

FIREWALL PERFORMANCE AND FEATURES

5.1 NEXT GENERATION FIREWALLS COMPARISON

To select from different firewall models we have to define some essential parameters by which we can measure and select our suitable one. We are preparing one comparison table between several firewall models considering one medium size enterprise network requirement focusing but not limited to –

- 500 users (Avg. 300+ con-current users)
- Exchange mail server v2016
- Active directory, File server, Web server, DNS server and some service oriented servers
- Business applications like- ERP, Ticketing system, Leave management system, Tally, Escalation tools etc.
- Office surveillance system like- CC Camera, Access Control System
- LAN, Wi-Fi, IP-phone service for end users

Considering above scenario, we will compare some renowned NGFW's to get the most suitable one for the described network –

Table 5.1: Next-Generation Firewalls Comparison

Features	Experimental Requirement	Eudemon200E-N5	Fortigate300E	SRX 1500
Interfaces	2x 10 GE ports, 8x GE RJ45 Ports, 4x SFP	Support	2x GE mgt, 16 GE RJ45 Ports,16 GE SFP	16x1GE(12 RJ-45)+ 4x10G
Firewall Throughput	5 Gbps	8	32	9
Throughput (with all features and load)	2 Gbps	2	3 [Threat Protection]	5
Firewall Policies	2,000	20,000	10,000	16,000
IPsec VPN Throughput	3 Gbps	3	20	4
Gateway-to-Gateway IPsec VPN Tunnels	1,000	4,000	2,000	2000 (Total IPsec)
Client-to-Gateway IPsec VPN Tunnels	5,000	4,000	50,000	2000(Total IPsec)
High Availability Configurations	Active/Passive, Clustering	Active-Active, Active-Standby	Active-Active, Active-Passive, Clustering	Yes
Wireless Controller Mode	Yes/Not	not	Built-in	No
Redundant Power Supply	Internal and DC power preferred	Supported	Optional Redundant Power	Yes

NGFW	Support -Yes/No	Yes	Yes-license included	Yes
VPN License	Required-Yes/No	Required	No license required	Yes
IP and Sys Log	Minimum 2 month logs	Supported	Required Tool	Yes
Memory (DRAM)	1 GB	4	16	16
Storage	100 GB	No default Storage	2 x 240	100
User must change password at VPN 1stlogon	MD5 or SHA	SHA	Depends on: Windows AD, LDAP, RADIUS...etc.	No

We also compared the user community recommendation to avail the users feedback based on the performance and satisfaction –

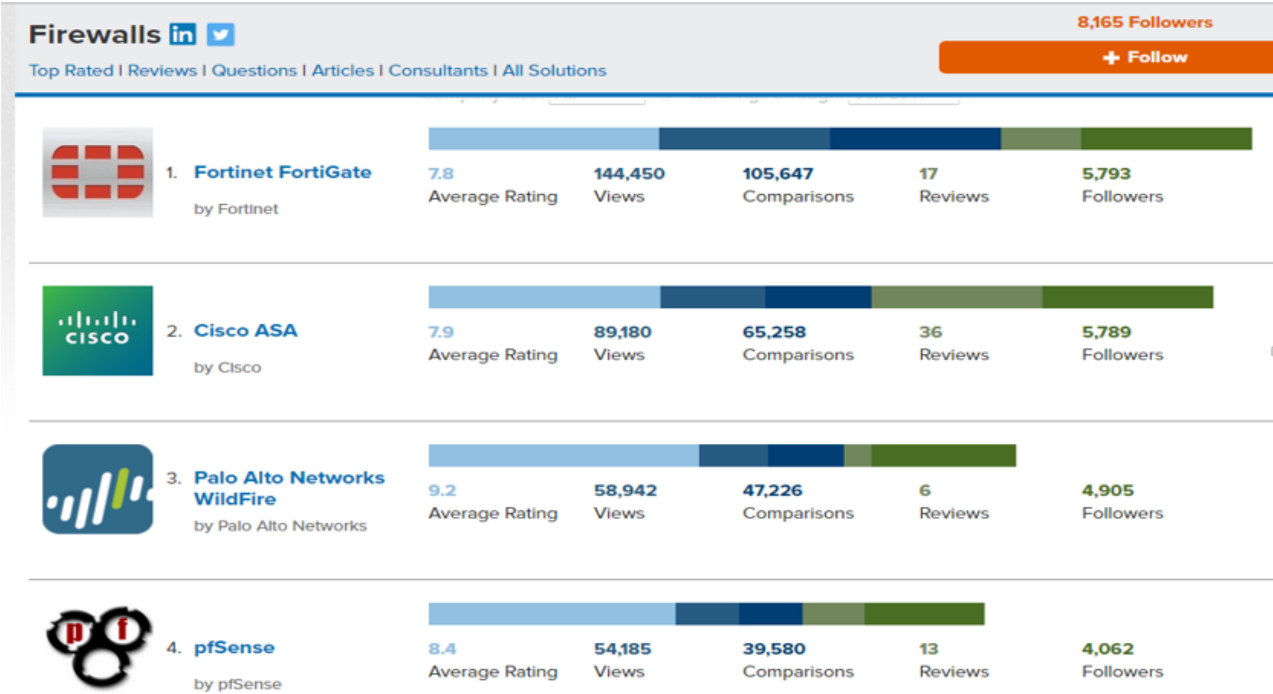


Figure 5.1: Community recommendations of NGFW

5.2 FORTINET FIREWALL PERFORMANCE & FEATURES



Figure 5.2: FortiGate 300E Firewall

Interfaces and modules	2 USB, 1 RJ45 Console, 2x GE mgt, 16 GE RJ45 Ports, 16 GE SFP
Redundant power supply	Optional Redundant Power supply with FRPS
Nominal Voltage	AC 120/230 V
Power Consumption Operational	80 Watt
Remote Management Protocol	CLI, HTTP
Network / Transport Protocol	IPsec, SCTP, TCP/IP, UDP/IP
Data Link Protocol	Ethernet, Fast Ethernet, Gigabit Ethernet
Encryption Algorithm	256-bit AES, 256-bit SHA, SSL, TLS 1.2
Height (Rack Units)	1 m
Built-in Devices	LED panel
Dimensions (WxDxH)	17 in x 15 in x 1.8 in
Weight	16.09 lbs

5.2.1 Features

CAPWAP support, High Availability, IPv4 support, IPv6 support, Intrusion Prevention System (IPS), SSL inspection, URL filtering, VPN support, anti-malware protection, anti-virus protection, checksum offload support, content filtering, firewall protection, manageable, routing, switching [16]

5.2.2 Performance

IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP)	: 32 / 32 / 20 Gbps
IPv6 Firewall Throughput (1518 / 512 / 64 byte, UDP)	: 32 / 32 / 20 Gbps
Firewall latency (64-byte UDP)	: 3 μ s
VPN throughput (512-bit IPSec)	: 20 Gbps
VPN throughput (SSL)	: 2.5 Gbps
SSL inspection throughput	: 6.8 Gbps
Application control (AVC) throughput	: 7 Gbps
IPS throughput (enterprise traffic mix)	: 5 Gbps
NGFW throughput	: 3.5 Gbps
CAPWAP throughput	: 5 Gbps
Threat protection throughput	: 3 Gbps

5.2.3 Capacity

Concurrent TCP sessions	: 4000000
New TCP sessions per second	: 300000
Firewall policies	: 10000
Gateway to gateway IPSec VPN Tunnels	: 2000
Client to gateway IPSec VPN tunnels	: 50000
Concurrent SSL VPN users	: 500
Virtual domains	: 10
Maximum number of registered endpoints	: 600

CHAPTER 6

SECURITY ENHANCEMENT AND RESULT

This chapter mainly focused on our target study that we want to implement and enhance our security model of our proposed system of an enterprise network. Fortinet is the next generation firewall as its deployment in a big networking sector or any local large will add a tremendous security which is really a better options for enhancing security. [18] We are using physical fortiGate 300E firewall in a practical corporate enterprise network to enhance the network security of the organization. Here we will describe the process and will show the practical result of implementation –

Firstly, we have to ensure physical and environmental security for the firewall system to prevent any kind of physical damage. Some crucial points to keep in mind for the deployment is –

- Hardware should be properly mount in data center environment (Where applicable)
- Acceptable temperature
- Stable power system
- Power backup in case of commercial power failure
- Industry level cabling and tagging
- Access control system to prevent unauthorized physical access
- CC Camera surveillance system for proactive monitoring
- Backup plan of hardware

Below table shows the devices and installed software's that we have used during the experimental session –

Table 6.1: List of Tools and devices for Implementation and application

Device Name	Specification	Installed Tools
Firewall	Fortinet -FortiGate 300E Physical Box	FortiOS v6.2.1 build0932 (GA), Forti-Analyzer (VM)
Router	MikroTik Router- CCR1036- 12G-4S (Layer3 device, Gigabit port, SFP port, High speed)	MikroTik RouterOS 6.43.8
Cisco Switch	Manageable Layer-2 device	Real Production Network
Host PC – PC1 (Local)	CPU: Core i5, 1.8 GHz	PuTTY, Winbox, Wireshark, Xshell
Host PC – PC2 (Local)		
Host PC – PC3 (Remote)		

6.1 SECURING THE FIREWALL ACCESS

In the second phase, we will implement access level security to protect against the first layer of security attacks. The first layer of attack inside any network will be getting access inside the network components.

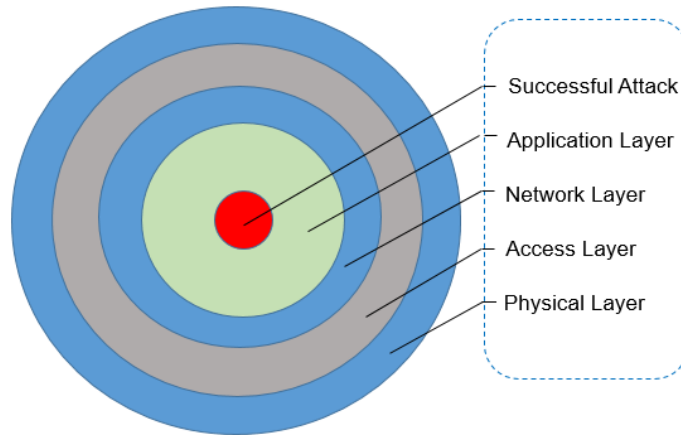


Figure 6.1: Layers of security

To penetrate the security layers firstly the attacker has to break the security of physical or access layer to get access inside the network system. Access level security is applicable for any network appliances like firewall, router, switch, server, computer etc. So, primarily we have to ensure best possible security against getting unauthorized access over these components. The access policy we have defined in our firewall system to protect the access level security described below –

Table 6.2: Firewall access security parameters

Category	Process	Result
Console login password	Set strong and secured password	Unauthorized physical access can be prevented by securing the console login
MGT port security	Set customized IP address & strong and secured password for management access	Customized IP with secured password
Administrative port customization	Customized secured port for HTTP, HTTPS, Telnet, SSH access	Without having the actual port information, remote access will not be possible
Secure remote login	Enable SSH login instead of Telnet	Remote login sessions will be encrypted and secured
Role-based access	Set administrator profile based on role and expertise	Prevent any kind of unwanted logical activities

Idle timeout	Maintain standard idle timeout for each login sessions	After the predefined period of time, users will be automatically logged out from the system
TCP port scan	Block TCP port scanning option	Which ports are running inside a network system will be invisible
UDP flooding	Block UDP flooding option	Will prevent UDP traffic overflow
Password policy	Standard password policy - letter, number, upper-case, lower-case, special character, end of life etc.	Will ensure more security
Secure SNMP	Secret community string, only responsive to the predefined hosts	Outsiders will not be able to get your SNMP data
Network Time Protocol (NTP)	Use local NTP or Fortinet site	All of your running services & logs will match the same time
Alert notification	Set alert notifications for device access, reboot, configuration change etc.	Will get instant notification over mail when anyone access the device or change any type of configurations and more
Trusted source	Define trusted source for device access	Users from only the trusted sources will be able to access the firewall

Now, after customizing the administrative access ports if any hacker attempt to login into the firewall without having the knowledge of ports, access will be denied. For example –

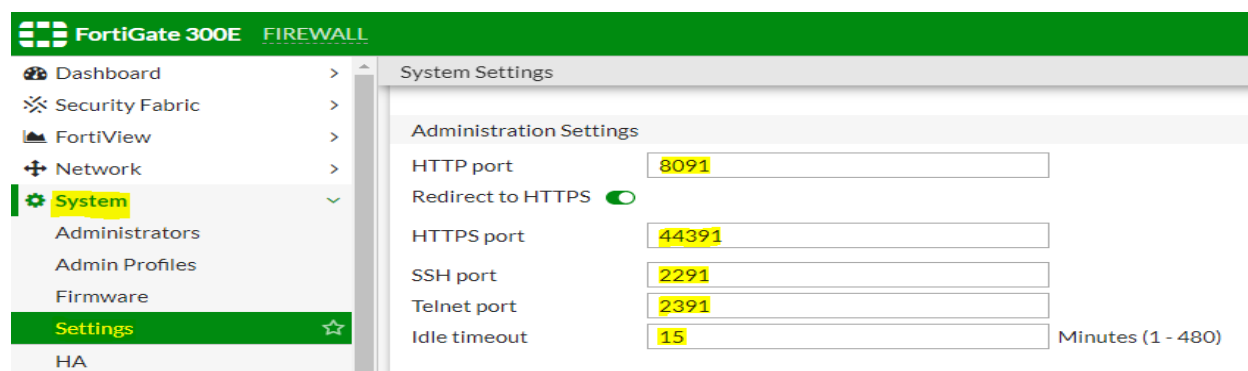


Figure 6.2: Access port customization

We have customized all the administrative access default ports like –

HTTP 80 > 8091 (HTTP to secured HTTPS redirection enabled)

HTTPS 443 > 44391

SSH 22 > 2291

Telnet 23 > 2391

Also, specified the idle timeout based on requirement and security standard.

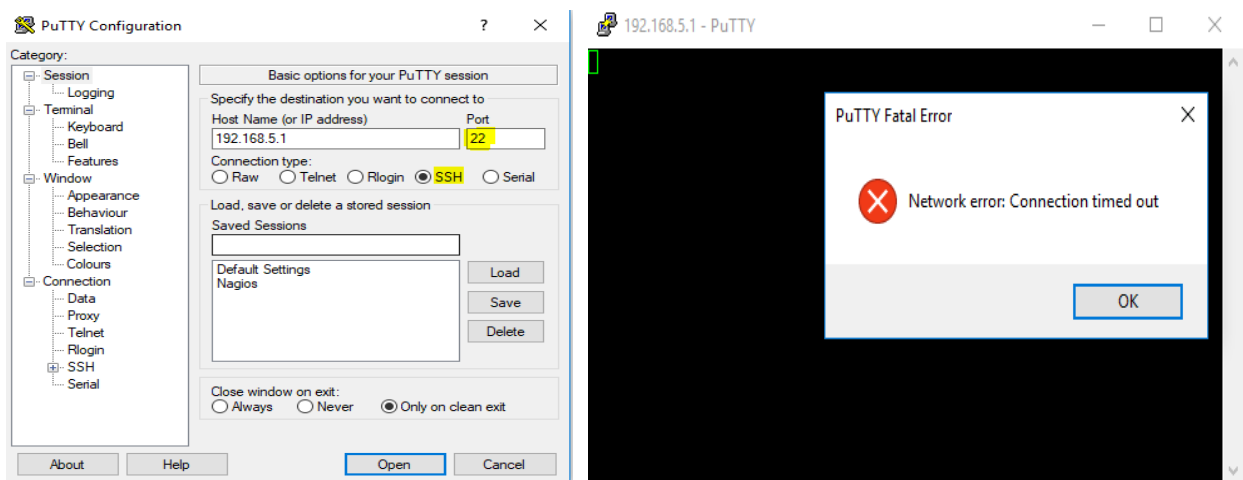


Figure 6.3: SSH default port login restricted

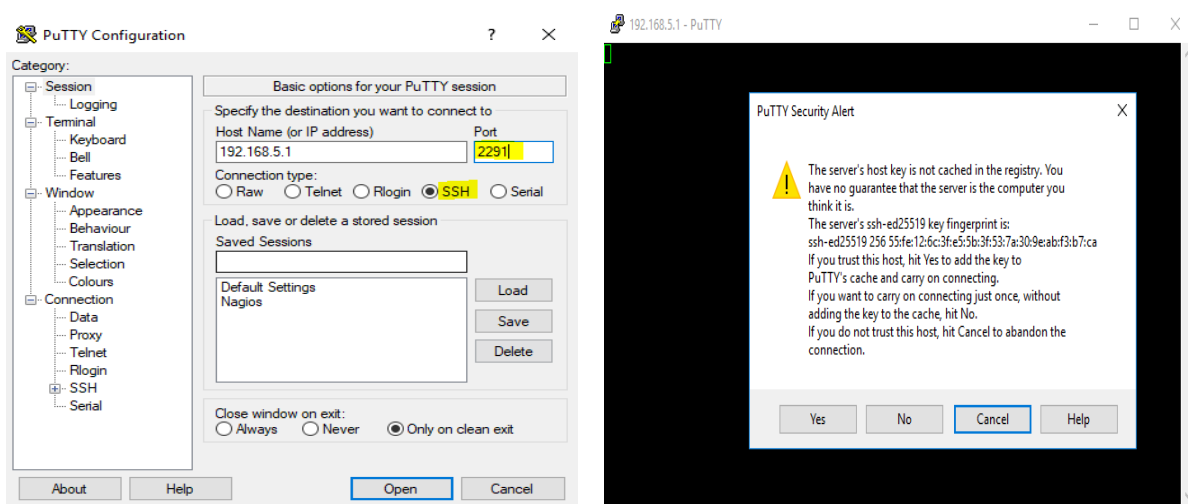


Figure 6.4: SSH secured login with port customization

We found the same result for web/SSH access when port customization is configured. This will reduce the chance of unauthorized access to our device.

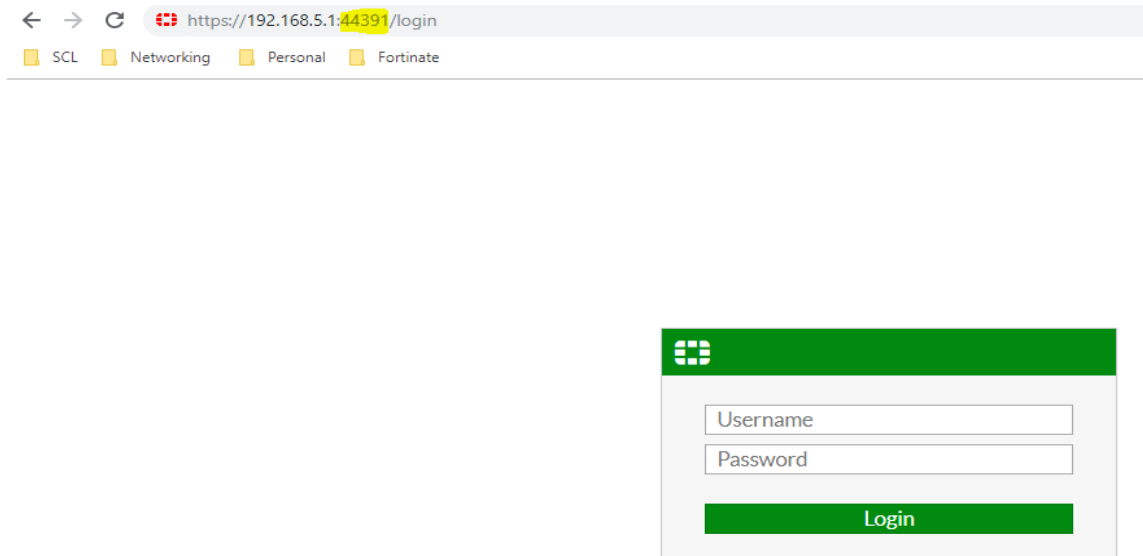


Figure 6.5: Web login port security

Role based administrator setting is another vital point for securing the authorization. Read users can see all the existing configurations but not able to modify any part of these.

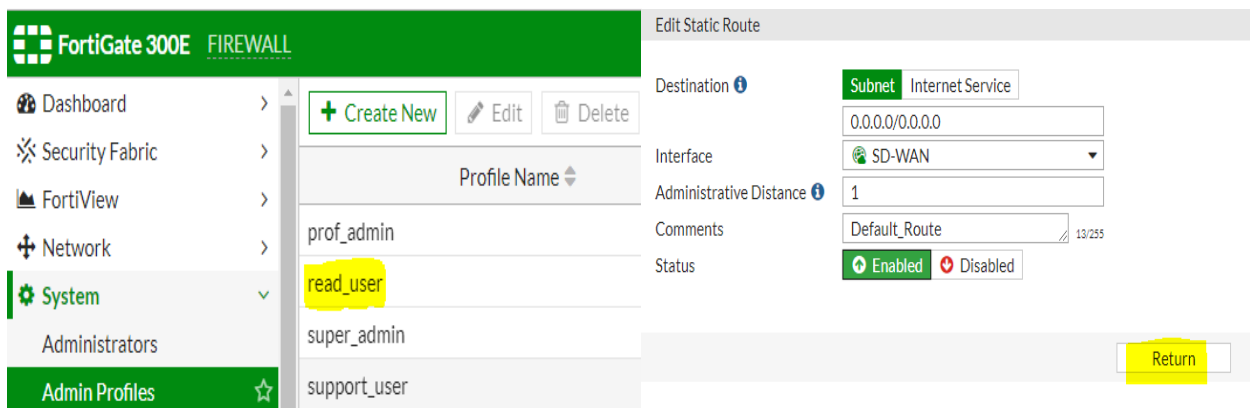


Figure 6.6: Role based administrator (Read User)

6.2 SECURITY AUTOMATION

Under fortinet security fabric we can enable various security automation features where administrator just have to set the rules and firewall automatically play the defender role when any error occurs based on policy. For example, when any kind of configuration change occurs or any error occurring in your firewall, you will get instant notification. Moreover, if any host got compromised during or after office hours you can set rule for automatically Ban the IP address of that host.

While we enable IP Ban for compromised host's option, we found that weather any unappropriated activities take pace immediately that host will be banned according to the given rule. Firewall treats any host as compromised for below reasons –

- Visit to any malicious site
- Broadcast traffic
- Global upload (large data)
- Ransomware attack
- Huge con-current sessions

As described, we have enabled some automation policies like –

- Email alert for any kind of configuration changes, device login, device reboot etc.
- Automatically Ban IP addresses of compromised hosts
- Scheduled update/reboot etc.

After enabling the “Automatically Ban IP addresses of compromised hosts” feature we found something exciting. Whenever any host in the entire network was involved with any kind of malicious activities, immediately firewall banned the IP address of that host without administrator's engagement as shown in below figure: 6.8

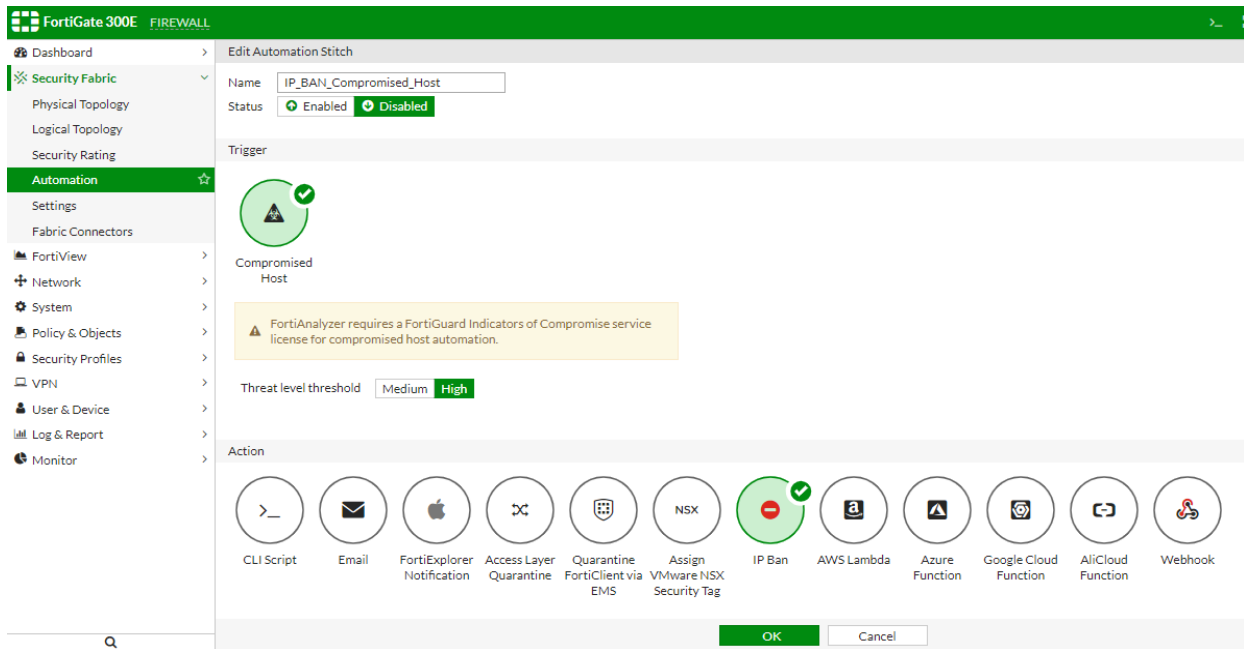


Figure 6.7: Compromised Host automation rule

Details	Device	Source	Expires
Banned IP 11			
162.220.161.2		IPS	12 minute(s) and 1 second(s)
5.188.86.10		Administrative	26 day(s) and 8 hour(s)
185.153.197.13		IPS	12 minute(s) and 1 second(s)
193.188.22.17		IPS	8 minute(s) and 15 second(s)
130.61.62.31		IPS	30 minute(s) and 56 second(s)
13.76.7.33		IPS	38 minute(s) and 13 second(s)
129.213.38.52		IPS	26 minute(s) and 12 second(s)
139.60.160.153		IPS	38 minute(s) and 14 second(s)
139.60.160.197		IPS	38 minute(s) and 14 second(s)
163.172.107.202		IPS	12 minute(s) and 3 second(s)
23.91.75.219		IPS	12 minute(s) and 2 second(s)

Figure 6.8: Automatically Ban IP addresses of compromised hosts

6.3 PROTOCOL AUTHENTICATION

Direct Internet traffic that a hacker send malicious virus and different kind of direct attack through third party software like uTorrent, Bit torrent and many other open source software in our window operating system with the permission of access firewall without unknowing of mind. So defend against these kind of attacks, we have to enable “Protocol Authentication” system.

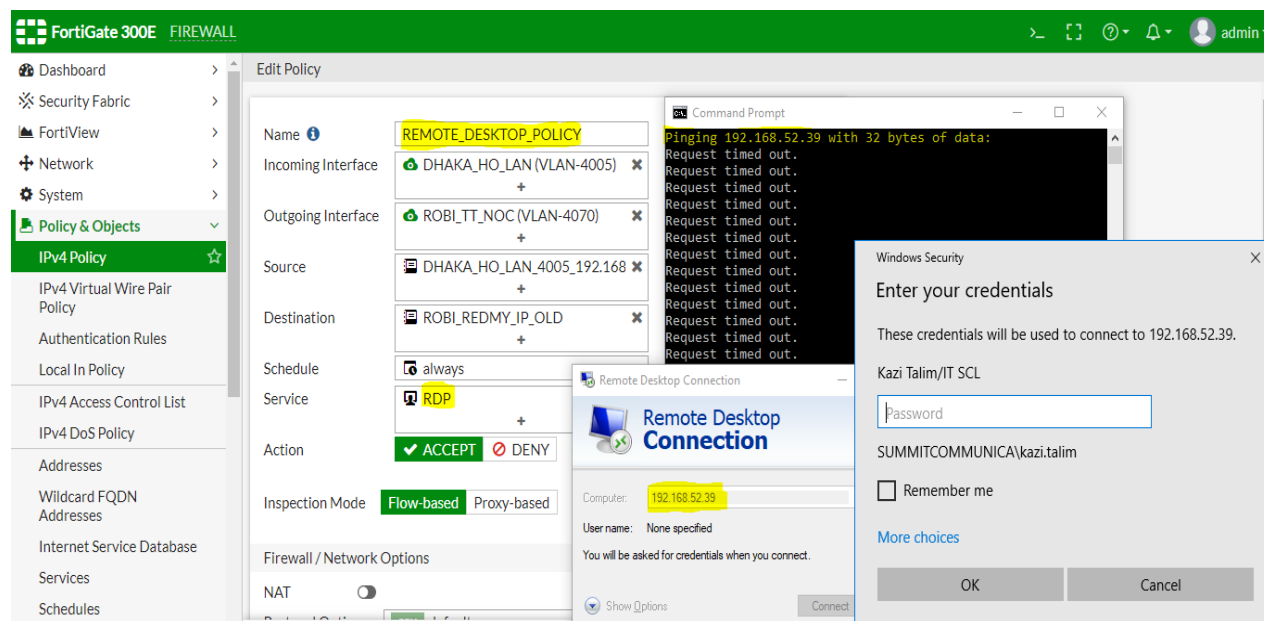


Figure 6.9: Protocol authentication (RDP)

In our practical experiment, when we set protocol authentication like, **RDP allow only** – we can't even ping the IP but required service (RDP) is running smoothly with most secured manner as you can see in figure: 6.9.

This is very important to protect your network from hacking attempts. When we use protocol authentication for each and every running services, it is very difficult for anyone to perform security attacks on target. Specially, when any important servers like your mail server or company web server hosted in public IP, Protocol authentication is very important factor on that

case. For applying protocol authentication, we have to know about all running services inside any particular application.

6.4 PORT FORWARDING SECURITY

Port forwarding on router or firewall or any kind Device which control or monitor traffic in the internet which are allows a port address enter to it. Port forwarding plays an important role to secure vulnerable port of potential devices form attackers and hackers to keep safe our important data. With port forwarding the internal port of a router or firewall along with an IP address can be changed where port number forwarded to unknown port for Incoming. This is tricky way to secure and put a privacy on firewall to protect our Data. To activate first we have to create virtual IP address mentioning the mapped port identity.

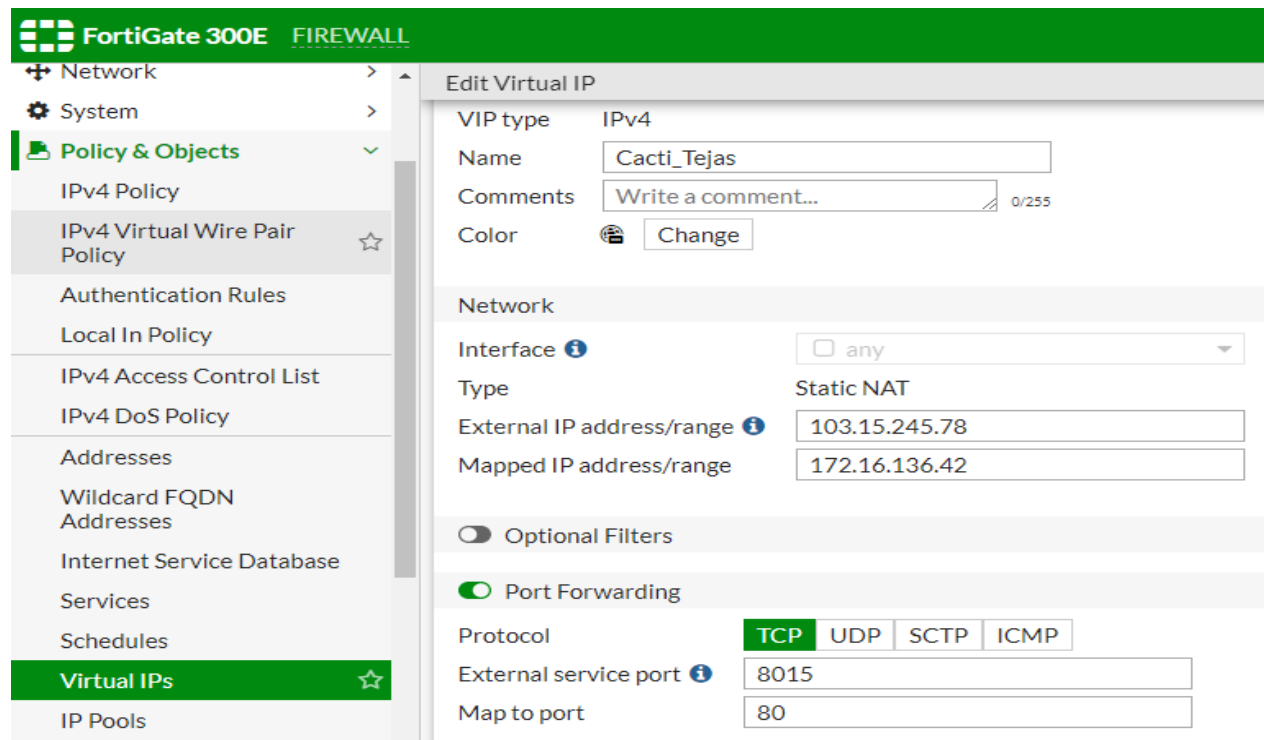


Figure 6.10: Port Forwarding in FortiGate Firewall

In This firewall we forwarded TCP port 8015 to 80 with the Private IP mapping with public IP as it given form Internet Service provider. Port Forwarding or port mapping is part of Network Address translation (NAT) where it is applicable. One major thing to keep in mind that, **when use any port forward service we used specific service (Protocol type) for secured communication.**

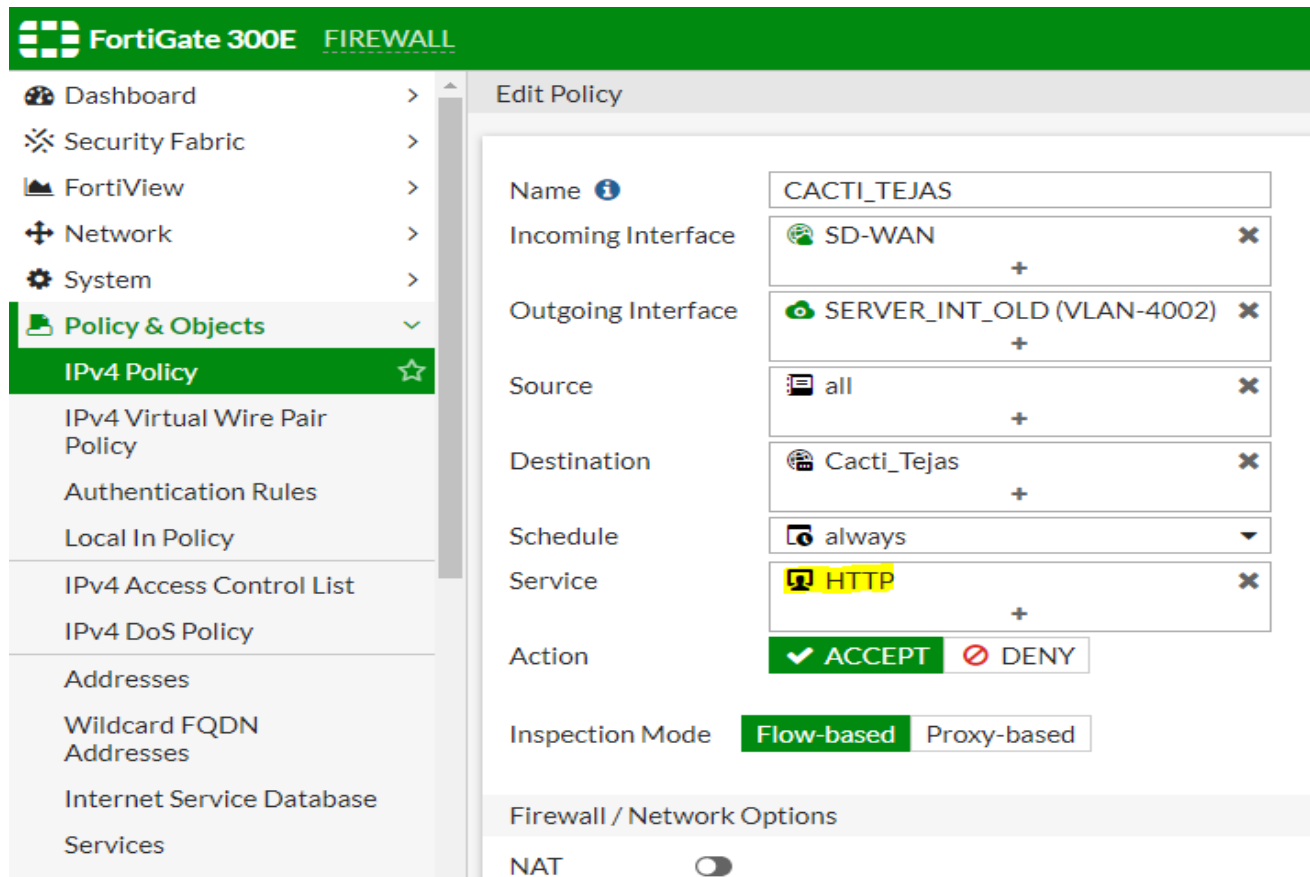


Figure 6.11: Service declaration in Port Forwarding policy

Here we used HTTP service to be allowed of the mapped local ip address using the port forward service. As a result, any other access or port attacks will be blocked by this policy.

6.5 DEFAULT DENY POLICY FOR UNTRACKET TRAFFIC

Figure 6.12 shows that policy applied for direct Internet Traffic for remove malicious attack from different ports, open source software and create strong zone for protect valuable data from attackers.

The image consists of two screenshots from the FortiGate 300E Firewall management interface. The top screenshot shows a table of policies. The bottom screenshot shows the 'Edit Policy' configuration for the 'Implicit Deny' policy.

ID	Name	From	To	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
0	Implicit Deny	any	any	all	all	always	ALL	DENY			Enabled	2.82 GB

Edit Policy Configuration:

- Incoming Interface: any
- Outgoing Interface: any
- Source: all
- Destination: all
- Action: ACCEPT, DENY (selected)
- Log Violation Traffic:

Statistics:

- ID: 0
- Last used: 0 second(s) ago
- First used: 93 day(s) ago
- Hit count: 36,970,537
- Active sessions: 1
- Total bytes: 2.82 GB
- Current bandwidth: 1.48 kB/s

Figure 6.12: Policy For Direct Internet Traffic without authorization

By default Policy ID: 0 (Implicit Deny) is a characteristic feature of firewall system. In a router “**Everything is allowed until we manually create block rule**” but in firewall system the policy is completely reverse like “**Everything is denied until we create allow rule**”

That means any traffic can pass through the firewall based on our allowed policy only and for the untracked traffic, the default policy is always denied. In a medium to large scale enterprise

network the consumed internet traffic volume is quite high where this default deny policy has a great role for securing the overall network performance.

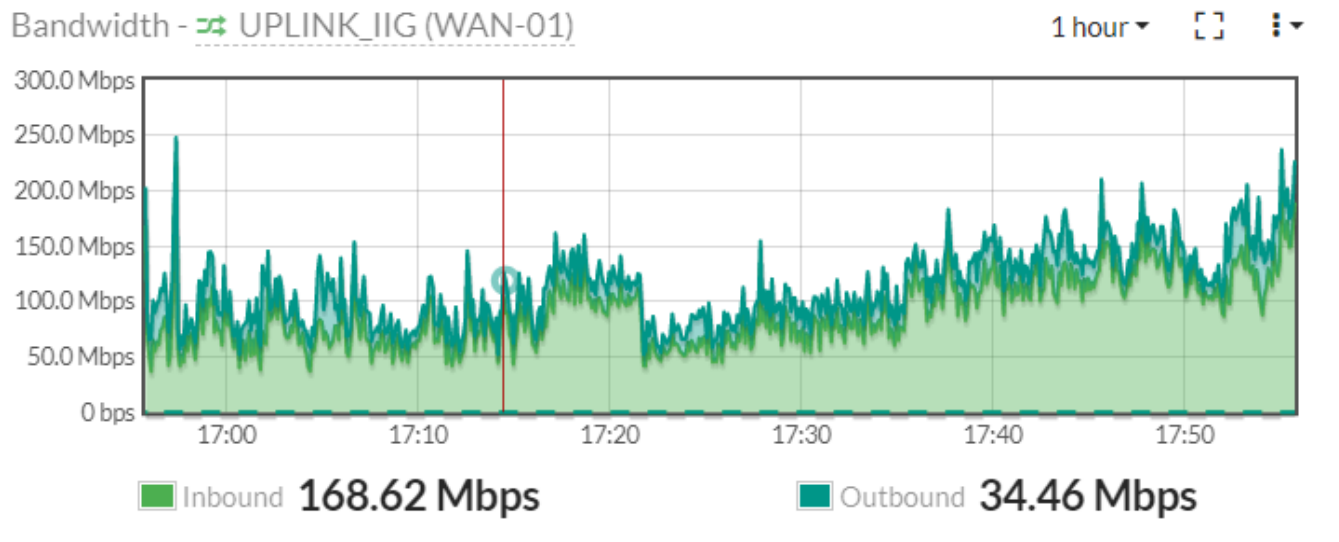


Figure 6.13: Experimental Avg. Internet Traffic of an Enterprise Network

6.6 SECURE VPN

Fortinet Next-Generation-Firewall offers secured IP-sec VPN tunnels as well as SSL-VPN (both Web & Client) for remote users. In our proposed network model (Figure 5.4) we have established IP-Sec VPN tunnel with branch offices with head office for encrypted communication of data. For setting up IP-Sec VPN tunnel forinet offers just few simple steps –

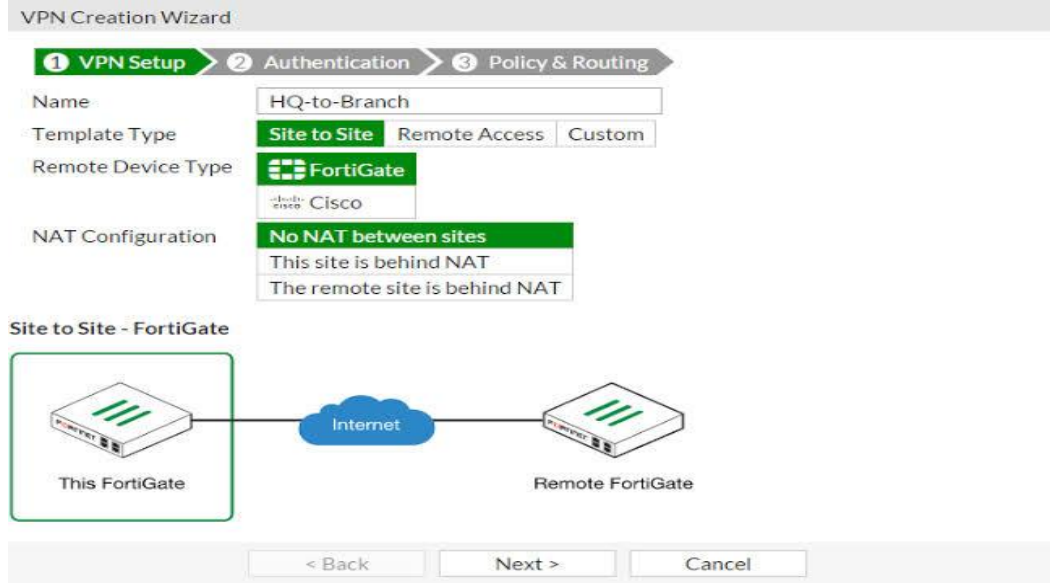


Figure 6.14: IP-Sec VPN tunnel (step-1)

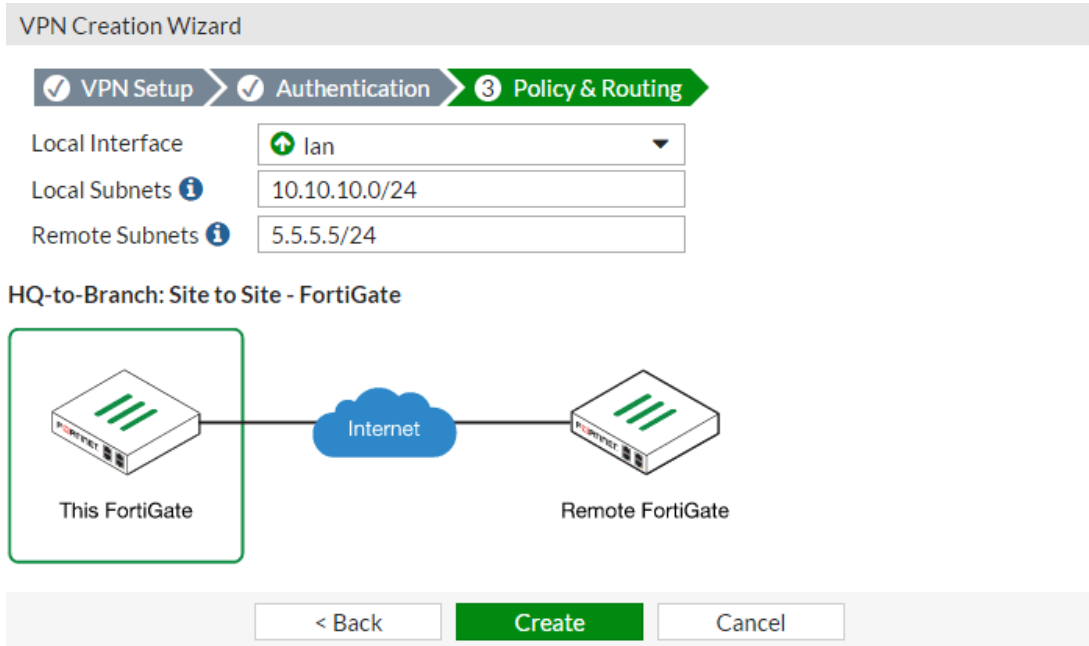


Figure 6.15: IP-Sec VPN tunnel (step-2)

VPN Creation Wizard

VPN Setup
 2 Authentication
 3 Policy & Routing

Remote Device: IP Address Dynamic DNS

IP Address:

Outgoing Interface:

Detected via routing lookup.

Authentication Method: Pre-shared Key Signature

Pre-shared Key:

HQ-to-Branch: Site to Site - FortiGate

Figure 6.16: IP-Sec VPN tunnel (step-3)

Fortinet also offers SSL-VPN (both Web & Client version) for secured remote user's communication. This is secured and also less CPU intensive as these VPN only allows secured tunnel between source and destination rather than encryption of all traffic.

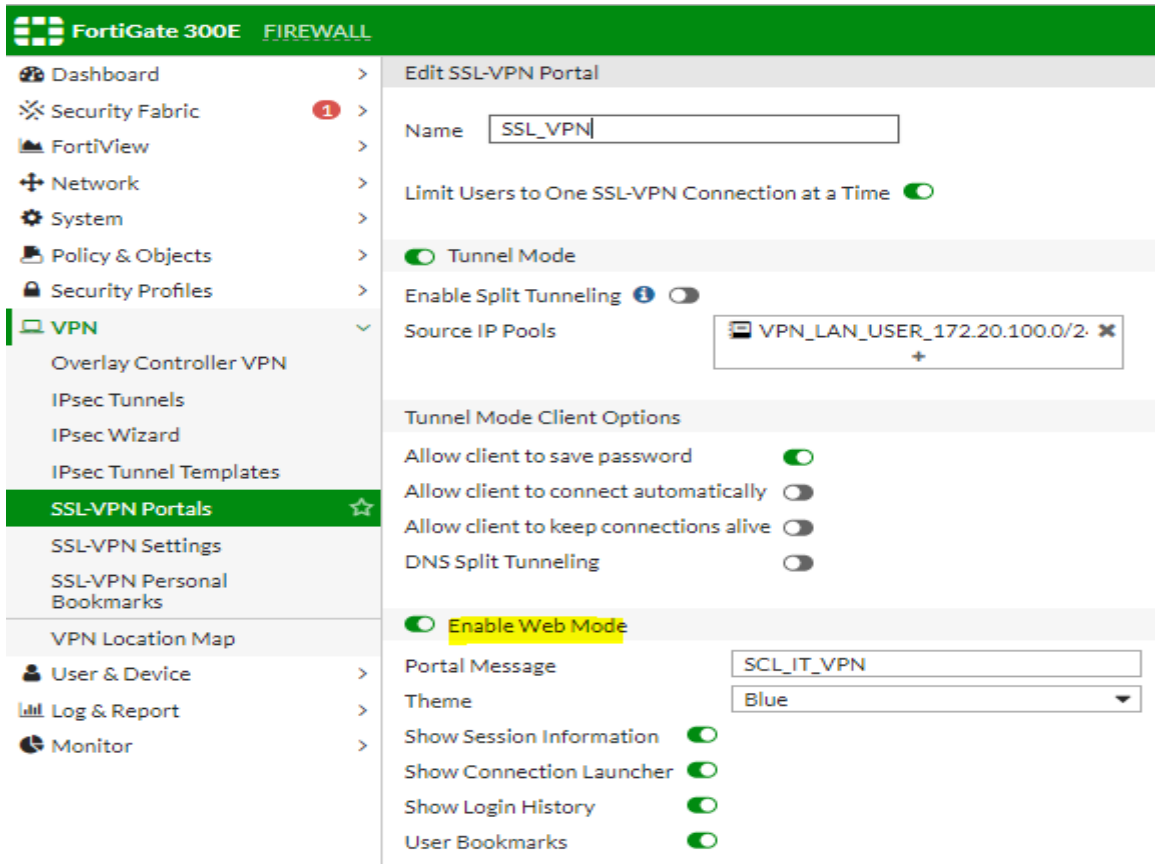


Figure 6.17: SSL-VPN configuration

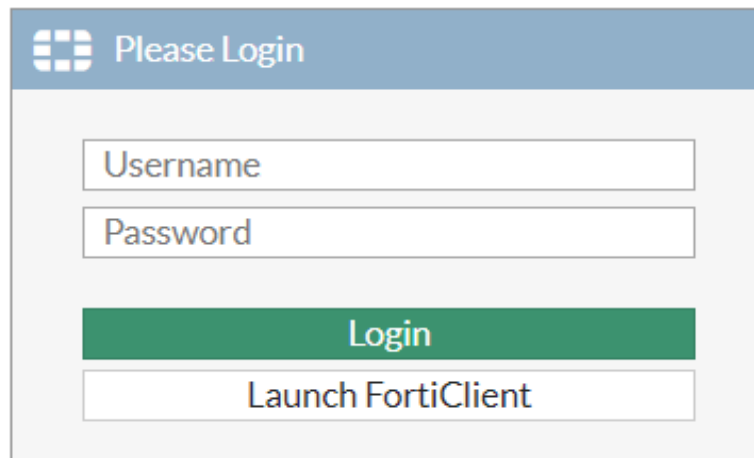


Figure 6.18: SSL-VPN web login page

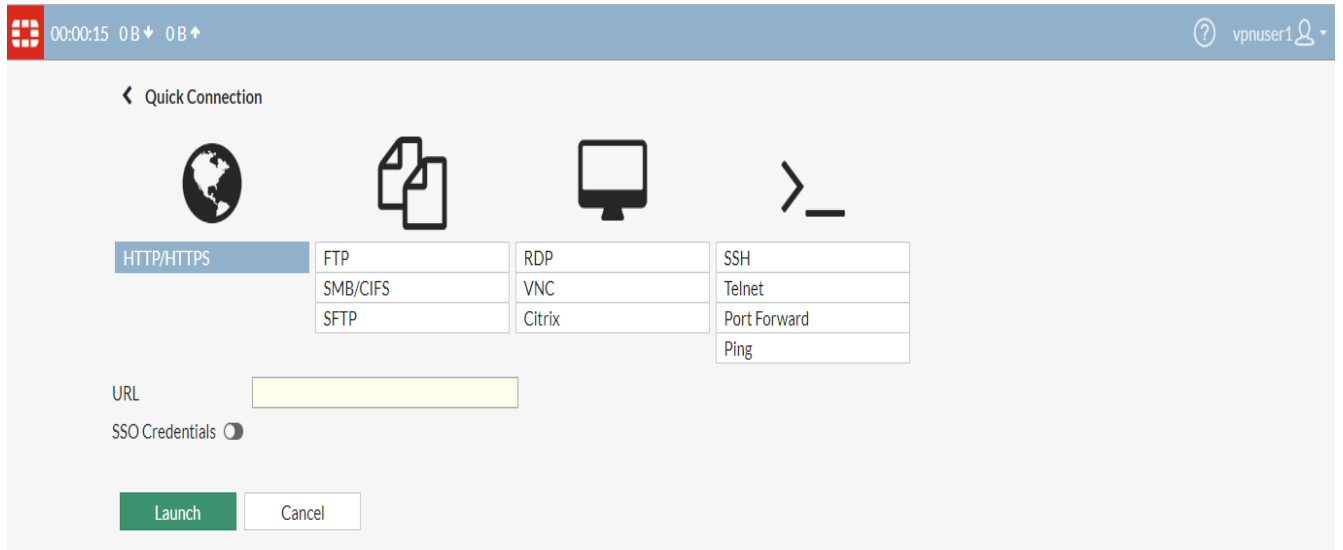


Figure 6.19: SSL-VPN web session

After enabling VPN service, we have captured network traffic of both PPTP and SSL-VPN using Wireshark software. For IP-Sec or SSL-VPN if anyone capture your data during transmission though he will not be able to trigger out the actual data shared between the authentic users due to the data encryption technique. The below pictures (figure: 6.20) will clarify the whole scenario to us —

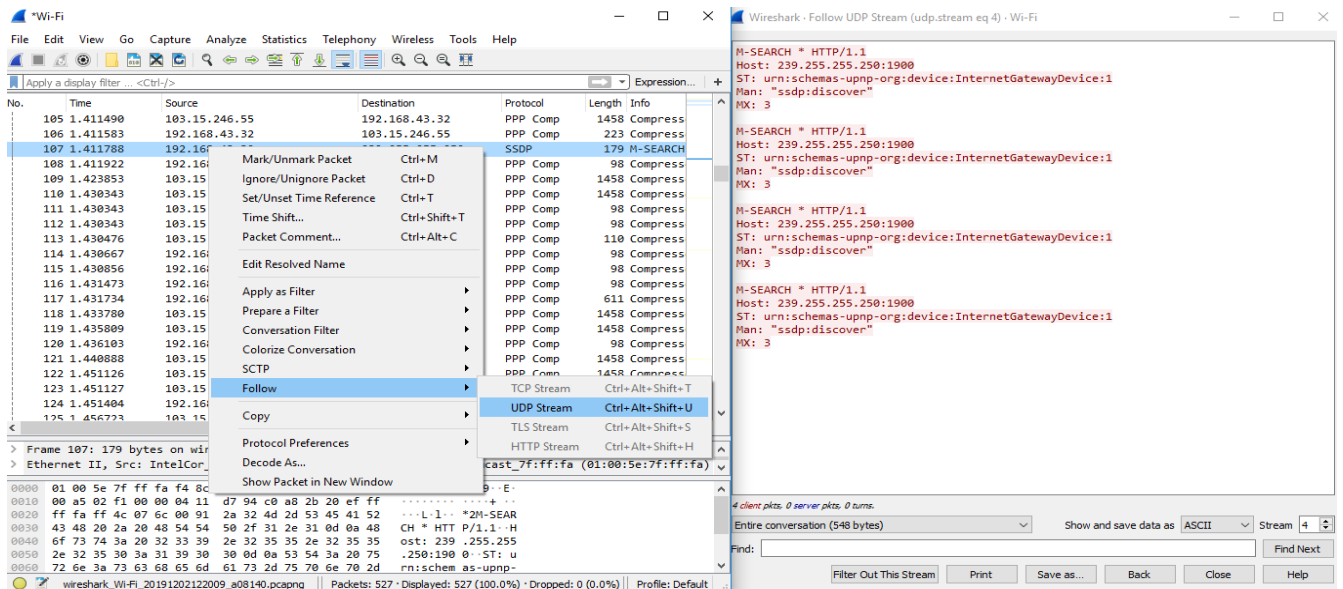


Figure 6.20: Packet Capture of PPTP VPN (Unencrypted)

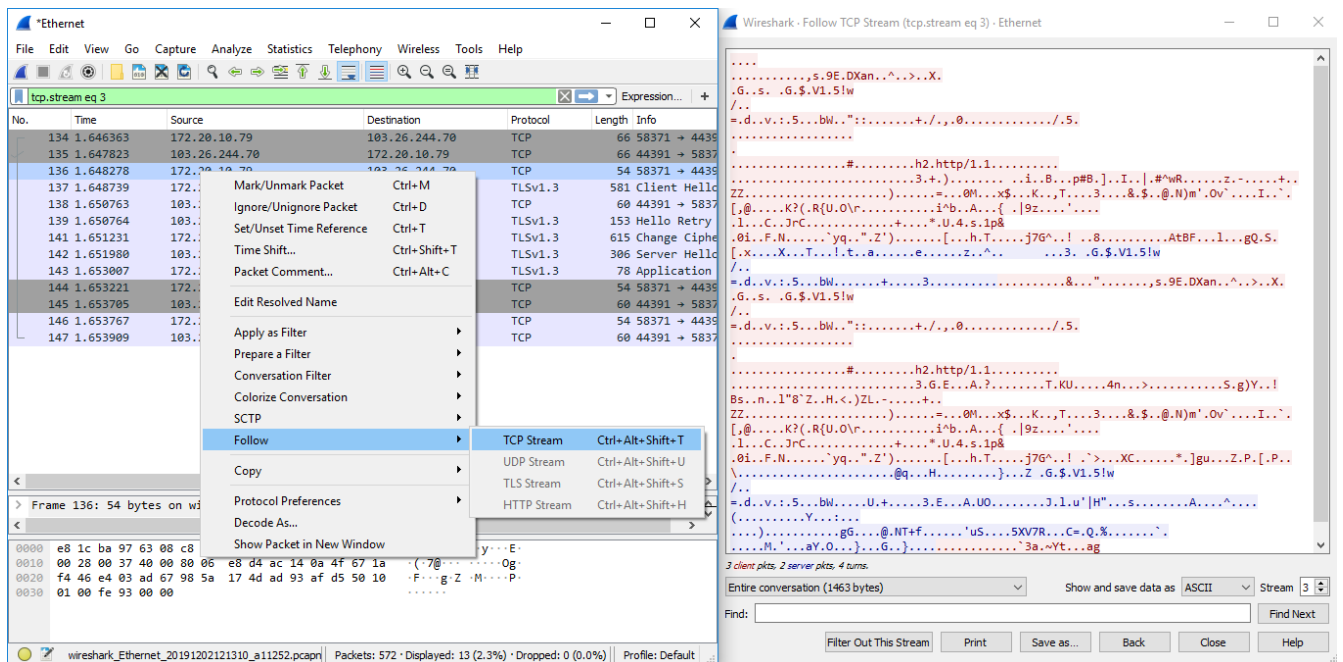


Figure 6.21: Packet Capture of SSL-VPN (Encrypted)

In this way, we can protect our data communication using encrypted VPN service offered by fortinet firewall.

6.7 SECURING THE DoS ATTACK

Though DoS solution is a very big deal and most expensive one, fortinet firewall offers basic protection against DoS attack. By defining standard DoS policy we can have control over common DoS attacks. To define this policy we should have enough knowledge about the average and highest active sessions in our production network. We can control up to how much sessions can be generated in our network using this policy to prevent broadcast session which is the key element of DoS attack.

FortiGate 300E FIREWALL

Dashboard >
 Security Fabric >
 FortiView >
 Network >
 System >
Policy & Objects >
 IPv4 Policy
 IPv4 Virtual Wire Pair Policy
 Authentication Rules
 Local In Policy
 IPv4 Access Control List
IPv4 DoS Policy ☆
 Addresses
 Wildcard FQDN Addresses
 Internet Service Database
 Services
 Schedules
 Virtual IPs
 IP Pools
 Protocol Options
 Traffic Shapers

Edit DoS Policy

L3 Anomalies

Name	Status	Logging	Pass	Block	Action	Threshold
ip_src_session	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Pass	Block		5000
ip_dst_session	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Pass	Block		5000

L4 Anomalies

Name	Status	Logging	Pass	Block	Action	Threshold
tcp_syn_flood	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Pass	Block	Proxy	2000
tcp_port_scan	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Pass	Block		1000
tcp_src_session	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Pass	Block		5000
tcp_dst_session	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Pass	Block		5000
udp_flood	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Pass	Block		12000
udp_scan	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Pass	Block		2000
udp_src_session	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Pass	Block		5000
udp_dst_session	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Pass	Block		5000

Figure 6.22: DoS Protection in fortinet firewall

FortiGate 300E FIREWALL

Dashboard >
 Security Fabric >
 FortiView >
 Network >
 System >
 Policy & Objects >
 Security Profiles >
 VPN >
 User & Device >
Log & Report >
 Forward Traffic
 Local Traffic
 Sniffer Traffic
 Events
 AntiVirus
 Web Filter
 DNS Query
 Application Control
 Intrusion Prevention
Anomaly ☆
 FortiGate Cloud Reports

Add Filter

Date/Time	Severity	Source	Protocol	U...	Action	Count	Attack Name
2019/12/02 12:49:37	■■■■■	54.36.115.66	17		clear_session	87	udp_flood
2019/12/02 12:35:40	■■■■■	52.184.39.253	17		clear_session	6,562	udp_flood
2019/12/01 20:11:40	■■■■■	172.217.163.161	17		clear_session	1,802	udp_flood
2019/12/01 19:39:06	■■■■■	182.79.148.206	17		clear_session	4,376	udp_flood
2019/12/01 19:37:17	■■■■■	182.79.143.143	17		clear_session	1,430	udp_flood
2019/12/01 16:49:00	■■■■■	172.217.163.193	17		clear_session	10,437	udp_flood
2019/12/01 16:44:59	■■■■■	182.79.143.145	17		clear_session	7,397	udp_flood
2019/12/01 16:44:23	■■■■■	182.79.143.145	17		clear_session	13,578	udp_flood
2019/12/01 03:28:13	■■■■■	180.149.234.6	17		clear_session	8,047	udp_flood
2019/12/01 03:27:41	■■■■■	180.148.214.18	17		clear_session	10,490	udp_flood
2019/12/01 03:27:09	■■■■■	172.217.160.131	17		clear_session	16,680	udp_flood
2019/12/01 03:26:41	■■■■■	180.149.234.6	17		clear_session	10,769	udp_flood
2019/12/01 03:26:10	■■■■■	180.149.234.6	17		clear_session	7,692	udp_flood
2019/12/01 03:25:38	■■■■■	103.78.226.249	17		clear_session	11,587	udp_flood
2019/12/01 03:25:08	■■■■■	27.147.235.111	17		clear_session	2,838	udp_flood
2019/12/01 03:23:39	■■■■■	27.147.168.204	17		clear_session	602	udp_flood
2019/12/01 03:20:59	■■■■■	118.179.70.164	17		clear_session	1,896	udp_flood

Figure 6.23: UDP flood prevented based on DoS Policy

But, these are not enough to fight against latest DoS attacks but can protect us till a moderate level. Network experts are still working for upgrading the DoS/DDoS solutions by their best possible effort.

6.8 WEB SECURITY

We have configured fortinet category based web filtering for untrusted sites and got the desired blocking result as shown in figure: 6.25 from the web filter log analysis.

The screenshot displays the FortiGate 300E Firewall configuration interface for editing a Web Filter Profile named 'WEB_FILTER'. The profile is configured with FortiGuard category based filtering. The 'Block' action is selected for various categories including Gambling, Nudity and Risk, Pornography, Dating, Weapons (Sales), Marijuana, Sex Education, Alcohol, and Tobacco. The 'Allow' action is selected for Internet Telephony. The 'Security Risk' category is also highlighted with a 'Block' action.

Name	Action
Gambling	Block
Nudity and Risk	Block
Pornography	Block
Dating	Block
Weapons (Sales)	Block
Marijuana	Block
Sex Education	Block
Alcohol	Block
Tobacco	Block
Alternative Beliefs	Block
Abortion	Block
Other Adult Materials	Block
Advocacy Organizations	Block
Internet Telephony	Allow
Security Risk (6)	Block
Malicious Websites	Block
Phishing	Block
Spam URLs	Block
Dynamic DNS	Block
Newly Observed Domain	Block
Newly Registered Domain	Block
General Interest - Personal (35)	Block

Figure 6.24: Web filtering configuration in firewall

Date/Time	U...	Source	Action	URL	Category D...	Sent / Received
2019/11/28 13:10:34		37.6.60.202	blocked	103.15.246.57/	Unrated	185 B / 0 B
2019/11/28 12:03:58		103.74.120.201	blocked	103.15.246.58/wp-login.php	Unrated	183 B / 0 B
2019/11/28 12:03:58		103.74.120.201	blocked	103.15.246.57/wp-login.php	Unrated	183 B / 0 B
2019/11/28 12:02:41		78.186.254.130	blocked	103.15.246.58/	Unrated	191 B / 0 B
2019/11/28 10:23:15		129.213.20.205	blocked	103.15.246.57/imp/test.php	Unrated	156 B / 0 B
2019/11/28 10:23:15		129.213.20.205	blocked	103.15.246.57/phpmyadmin/setup.php	Unrated	164 B / 0 B
2019/11/28 10:23:14		129.213.20.205	blocked	103.15.246.57/myadmin/scripts/setup.php	Unrated	169 B / 0 B
2019/11/28 10:23:14		129.213.20.205	blocked	103.15.246.57/_phpmyadmin/scripts/setu...	Unrated	173 B / 0 B
2019/11/28 10:23:12		129.213.20.205	blocked	103.15.246.57/pma/scripts/setup.php	Unrated	165 B / 0 B
2019/11/28 10:23:12		129.213.20.205	blocked	103.15.246.57/phpmyadmin/scripts/_setu...	Unrated	173 B / 0 B
2019/11/28 10:23:11		129.213.20.205	blocked	103.15.246.57/mysql/scripts/setup.php	Unrated	167 B / 0 B
2019/11/28 10:23:10		129.213.20.205	blocked	103.15.246.57/MyAdmin/scripts/setup.php	Unrated	169 B / 0 B
2019/11/28 10:23:10		129.213.20.205	blocked	103.15.246.57/scripts/setup.php	Unrated	161 B / 0 B
2019/11/28 10:21:06		202.201.163.21	blocked	103.15.246.58/manager/html	Unrated	138 B / 0 B
2019/11/28 10:21:06		202.201.163.21	blocked	103.15.246.57/manager/html	Unrated	138 B / 0 B
2019/11/28 08:37:53		150.109.50.64	blocked	103.15.246.57/	Unrated	182 B / 0 B

Figure 6.25: Unrated sites are automatically blocked

On the other hand, if we need to allow any particular website which is already listed in category based blocking list, fortinet also allow it's administrator to overrides the web rating category. In the below picture we have overridden some business websites which were in blocking list of firewall and we can access those sites without any hiccup.

URL	Override Category	Original Category	Status
Advertising (3)			
ibtbid.net	Advertising	Malicious Websites	Enabled
ibtbid.net/fadlah-khan-director-summit-communications-ltd	Advertising	Malicious Websites	Enabled
icentre-bd.com	Advertising	Phishing	Enabled

Figure 6.26: Overrides required blocking websites to access

6.9 INTRUSION PREVENTION SYSTEM (IPS)

Fortinet offers market leading IPS system for high level intrusion protection. IPS is very important nowadays based on current threats and attacks statistics. Traditional firewalls only check source, destination and protocol information from their header whereas intrusion can be send with the body of original content. Deep scan of whole message is must needed to detect this kind of malicious contents. Here comes the concept of intrusion prevention system which is a kind of technology that can scan the whole message and able to detect as well as block the malicious part.

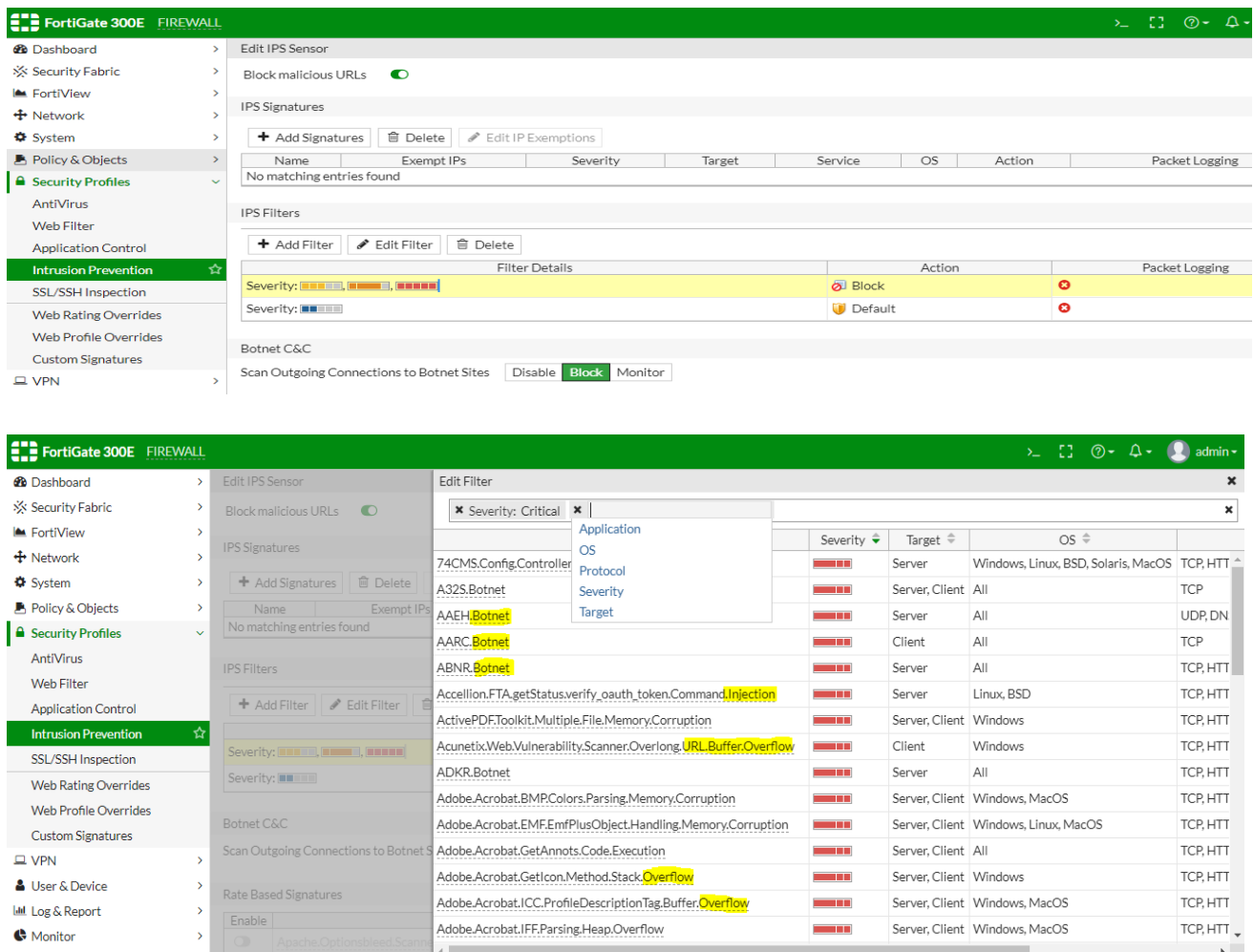


Figure 6.27: Updated IPS signatures from global security database

Date/Time	Severity	Source	Protocol	U...	Action	C...	Attack Name
2019/11/28 12:40:48	Medium	49.150.105.140	6		dropped		MS.SMB.Server.Trans.Peeking.Data.Information.Disclosure
2019/11/28 12:40:28	Critical	49.150.105.140	6		dropped		Backdoor.DoublePulsar
2019/11/28 12:40:04	Medium	49.150.105.140	6		dropped		MS.SMB.Server.Trans.Peeking.Data.Information.Disclosure
2019/11/28 12:38:51	Critical	123.22.191.253	6		dropped		Backdoor.DoublePulsar
2019/11/28 12:38:26	Medium	123.22.191.253	6		dropped		MS.SMB.Server.Trans.Peeking.Data.Information.Disclosure
2019/11/28 12:38:06	Critical	123.22.191.253	6		dropped		Backdoor.DoublePulsar
2019/11/28 12:37:41	Medium	123.22.191.253	6		dropped		MS.SMB.Server.Trans.Peeking.Data.Information.Disclosure
2019/11/28 12:37:29	Critical	36.82.230.230	6		dropped		Backdoor.DoublePulsar
2019/11/28 12:37:07	Critical	27.74.243.201	6		dropped		Backdoor.DoublePulsar
2019/11/28 12:37:05	Medium	36.82.230.230	6		dropped		MS.SMB.Server.Trans.Peeking.Data.Information.Disclosure
2019/11/28 12:36:45	Critical	36.82.230.230	6		dropped		Backdoor.DoublePulsar
2019/11/28 12:36:43	Medium	27.74.243.201	6		dropped		MS.SMB.Server.Trans.Peeking.Data.Information.Disclosure
2019/11/28 12:36:31	Critical	101.255.16.26	6		dropped		Backdoor.DoublePulsar
2019/11/28 12:36:23	Critical	27.74.243.201	6		dropped		Backdoor.DoublePulsar
2019/11/28 12:36:20	Medium	36.82.230.230	6		dropped		MS.SMB.Server.Trans.Peeking.Data.Information.Disclosure
2019/11/28 12:36:06	Medium	101.255.16.26	6		dropped		MS.SMB.Server.Trans.Peeking.Data.Information.Disclosure

Figure 6.28: Intrusion detected and blocked immediately

6.10 NETWORK VISIBILITY & PERFORMANCE COMPARISON

Each and every single active sessions are visible even we can control those sessions using the fortinet Next-Generation-Firewall as shown in below pictures (fig. 6.29 & fig. 6.30)

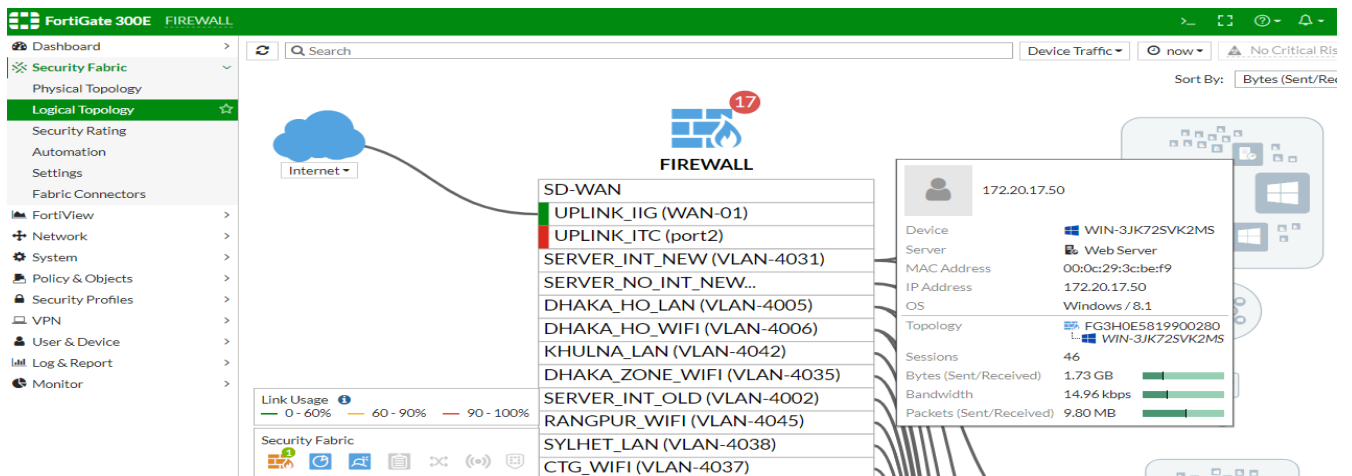


Figure 6.29: Logical view of whole network

Source	Device	Destination	Application	Protocol	Source Port	Destination Port
172.20.9.243	android-bd0f61a9cbb686f3	216.58.197.34	TCP/443	TCP	48928	443
172.20.17.185	fa:9f:70:f9:6e:b9	172.30.1.227	UDP/161	UDP	47695	161
m.saleheen - 172.20.9.116	SCL-L200636	216.58.196.162	UDP/443	UDP	56016	443
172.20.17.185	fa:9f:70:f9:6e:b9	172.30.33.134	UDP/161	UDP	55519	161
sudipta.chakma - 172.20.9.107	SCL-L200448	172.20.17.15	TCP/443	TCP	59069	443
172.20.17.193	a6:a3:a8:54:64:22	172.30.1.46	UDP/161	UDP	47071	161
172.20.17.193	a6:a3:a8:54:64:22	172.30.1.78	UDP/161	UDP	47039	161
172.20.9.74	ac:ed:5c:bcbf:79	172.20.18.13	TCP/3389	TCP	49804	3389
kazlibozle - 192.168.5.75	SCL-300109	172.20.18.13	UDP/53	UDP	59321	53
172.20.17.185	fa:9f:70:f9:6e:b9	172.30.1.246	UDP/161	UDP	46783	161
172.20.17.185	fa:9f:70:f9:6e:b9	172.30.7.14	UDP/161	UDP	45263	161
172.20.9.74	ac:ed:5c:bcbf:79	172.20.17.16	TCP/443	TCP	51501	443
192.168.5.251	00:0c:29:97:ed:60	172.20.16.38	UDP/161	UDP	60051	161
172.20.8.139	Android	74.125.68.188	TCP/5228	TCP	46153	5228
172.20.10.13	OnePlus6	157.240.23.54	TCP/5222	TCP	38998	5222
172.20.9.3	HUAWEL_nova_2i-584fe60270	216.58.197.46	TCP/443	TCP	47312	443
naznin.dina - 192.168.11.66	18:5e:0f:92:ed:c0	172.20.18.13	UDP/53	UDP	53081	53

Figure 6.30: All active sessions are visible and under control of administrator

Previously we were using MikroTik router (CCR 1036-12G-4S) in production network without advanced Next-Generation- Firewall UTM features (Anti-virus, anti-spam, IPS, application control) and during pick hours the device performance shows in figure 6.31



Figure 6.31: Previous bandwidth utilization & CPU usages without firewall

We found 550Mbps bandwidth utilization during pick hours with almost 97% of CPU usages (pick) without any firewall system. Within this 550Mbps consumed bandwidth, a huge amount goes for personal use like, Facebook, YouTube even intentional or unintentional malicious activities like, torrent file download, global upload, session broadcasting etc.

Based on this experience, we applied appropriate usages policy and security profile using fortinet fortiGate-300E firewall to restrict unusual usages and to protect from different security issues. After successful deployment we found almost 50% of consumed traffic dropped using firewall policy involving social media & unofficial traffic. During several speed test sessions, we also found satisfactory result including CPU & Memory utilization ratio as shown in figure: 6.32

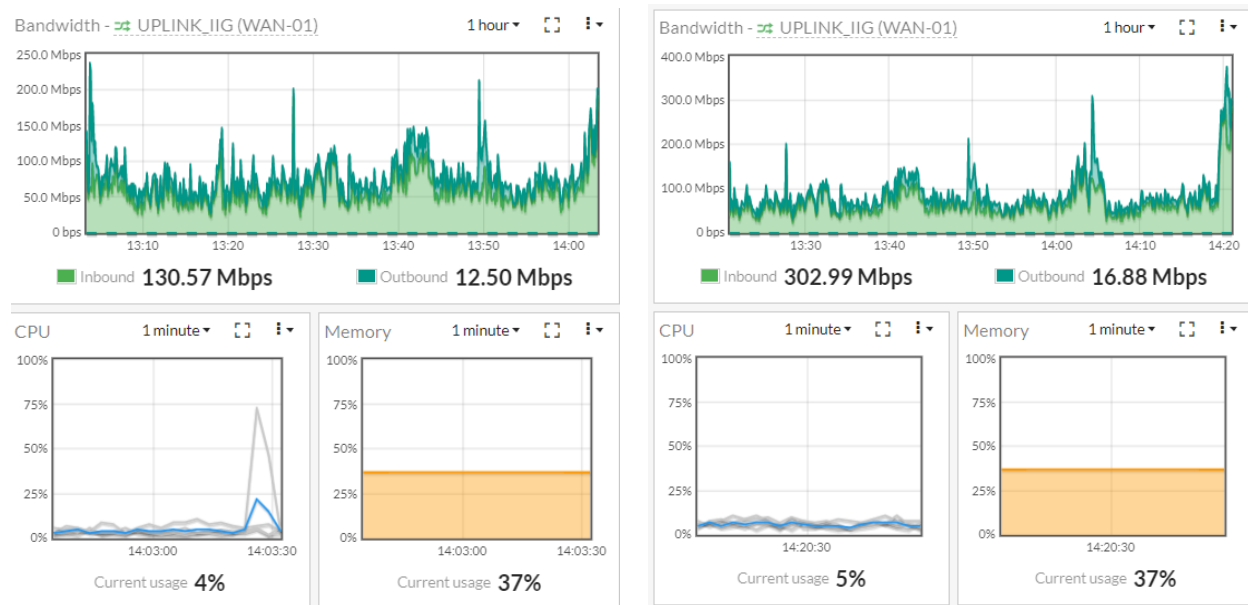
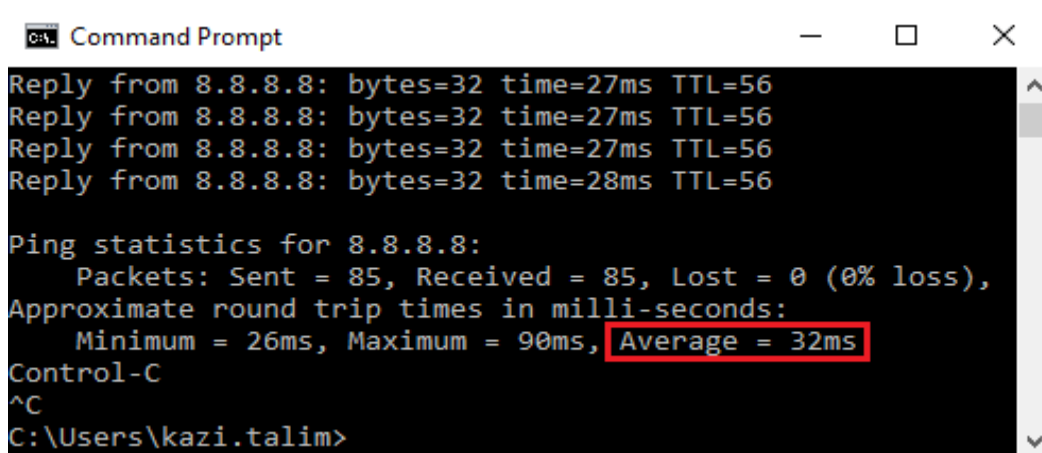


Figure 6.32: Resource utilization with optimized bandwidth using firewall

By this thesis study, we have discarded unusual network traffic from an enterprise network and applied standard security policies to defend against latest security risks. We have practically examined the performance throughout a month and didn't find any hiccup inside the entire

network. Let's check the network performance comparison before and after introducing the NGFW in the existing network –

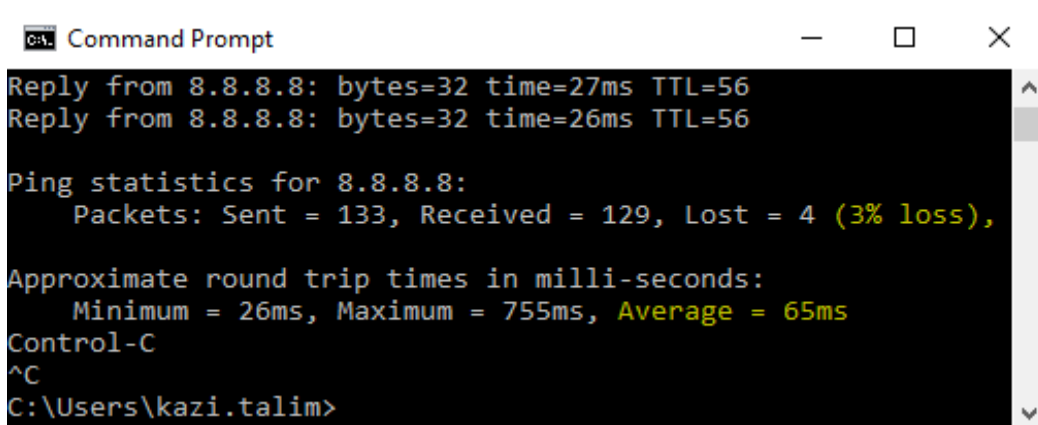
Before Firewall Integration:



```
CA: Command Prompt
Reply from 8.8.8.8: bytes=32 time=27ms TTL=56
Reply from 8.8.8.8: bytes=32 time=27ms TTL=56
Reply from 8.8.8.8: bytes=32 time=27ms TTL=56
Reply from 8.8.8.8: bytes=32 time=28ms TTL=56

Ping statistics for 8.8.8.8:
    Packets: Sent = 85, Received = 85, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 26ms, Maximum = 90ms, Average = 32ms
Control-C
^C
C:\Users\kazi.talim>
```

Figure 6.33: Avg. latency during regular usages before firewall integration

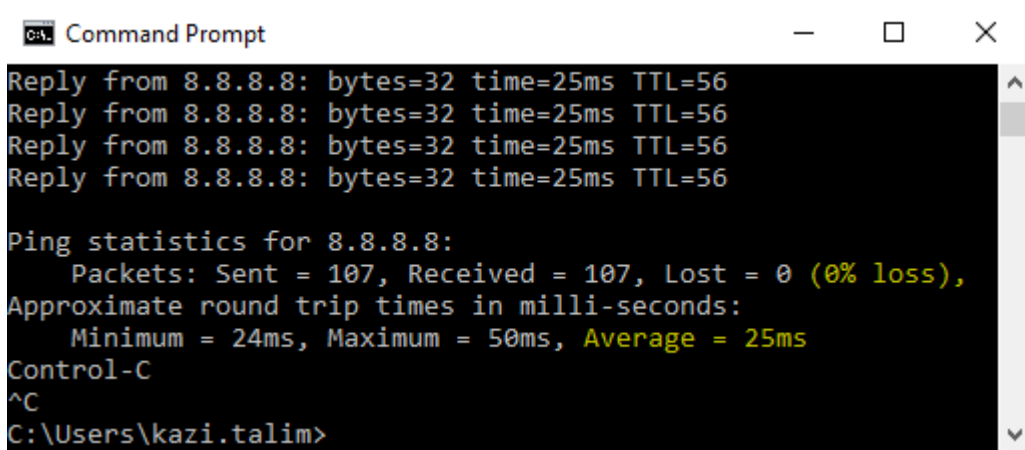


```
CA: Command Prompt
Reply from 8.8.8.8: bytes=32 time=27ms TTL=56
Reply from 8.8.8.8: bytes=32 time=26ms TTL=56

Ping statistics for 8.8.8.8:
    Packets: Sent = 133, Received = 129, Lost = 4 (3% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 26ms, Maximum = 755ms, Average = 65ms
Control-C
^C
C:\Users\kazi.talim>
```

Figure 6.34: Avg. latency & packet drop during peak usages

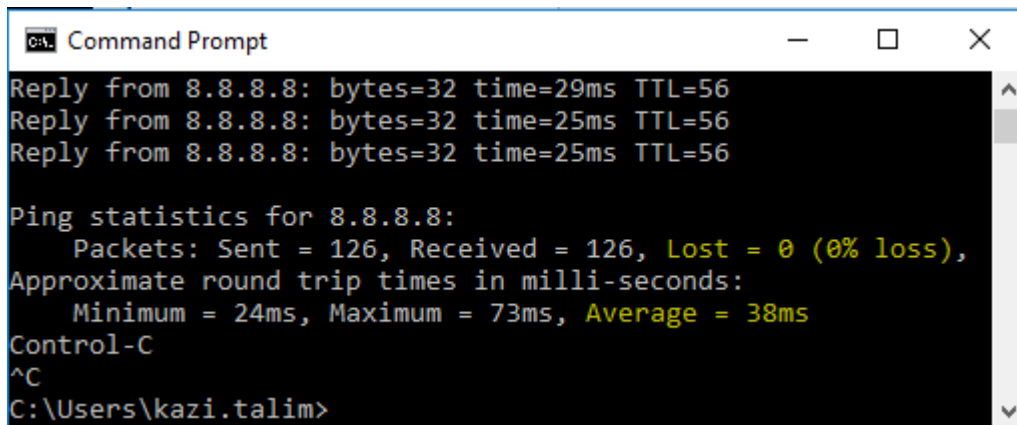
After Firewall Integration:



```
Command Prompt
Reply from 8.8.8.8: bytes=32 time=25ms TTL=56
Reply from 8.8.8.8: bytes=32 time=25ms TTL=56
Reply from 8.8.8.8: bytes=32 time=25ms TTL=56
Reply from 8.8.8.8: bytes=32 time=25ms TTL=56

Ping statistics for 8.8.8.8:
    Packets: Sent = 107, Received = 107, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 24ms, Maximum = 50ms, Average = 25ms
Control-C
^C
C:\Users\kazi.talim>
```

Figure 6.35: Avg. latency during regular usages after firewall integration



```
Command Prompt
Reply from 8.8.8.8: bytes=32 time=29ms TTL=56
Reply from 8.8.8.8: bytes=32 time=25ms TTL=56
Reply from 8.8.8.8: bytes=32 time=25ms TTL=56

Ping statistics for 8.8.8.8:
    Packets: Sent = 126, Received = 126, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 24ms, Maximum = 73ms, Average = 38ms
Control-C
^C
C:\Users\kazi.talim>
```

Figure 6.36: Avg. latency & packet drop during pick usages

Another essential parameter for enterprise is web-browsing where we also get optimized result in page loading time. Lower page loading time can effectively increase the production hours as we often need to browse different websites to collect data or store our contents. Below figures 6.37 will elaborate the difference in page loading time after incorporating firewall in the network –

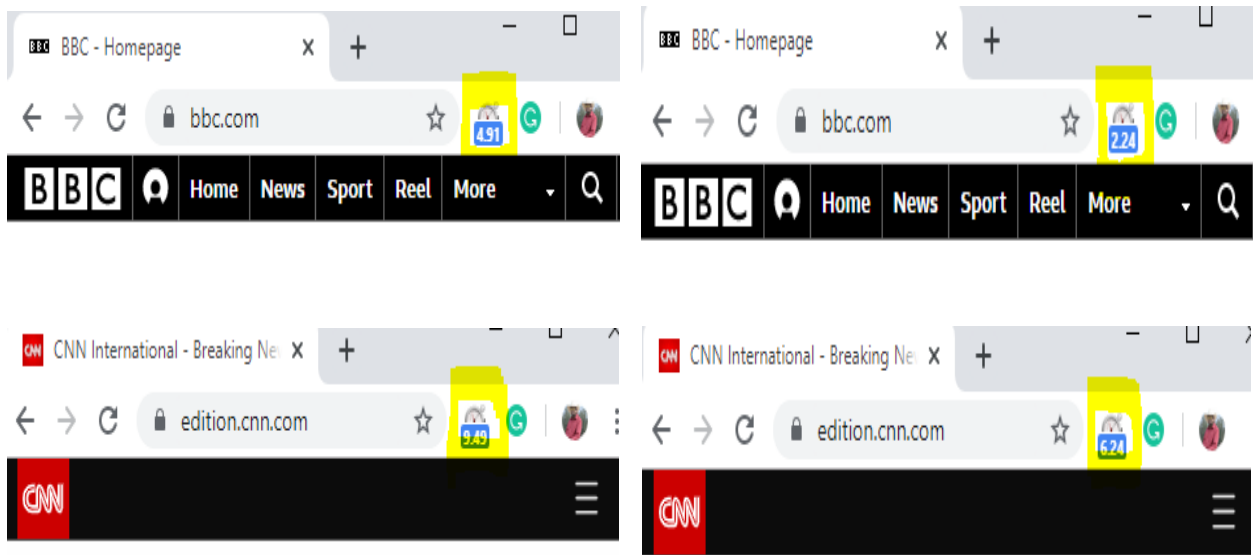
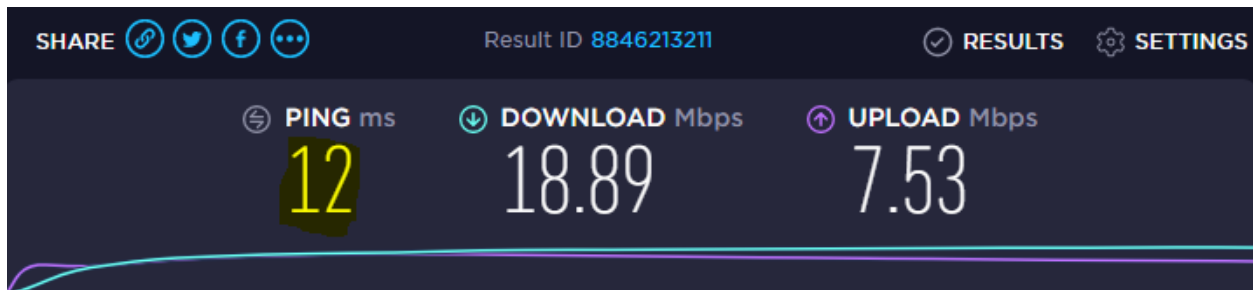


Figure 6.37: Avg. page load time difference after incorporating firewall

We have also found satisfactory result while checking internet speed from users PC after firewall integration inside office network. Reference values are shown in below figure 6.38 –

Before Firewall Deployment:



After Firewall Deployment:

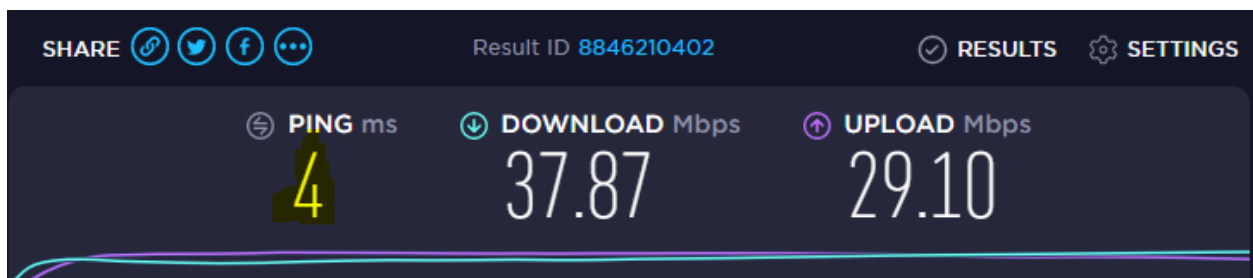


Figure 6.38: Ookla speed test result from user PC after incorporating firewall

6.11 FINAL RESULT

By the deployment of our proposed network model, overall network performance changed a lot according to the expectation. We have taken essential parameters for measurement that an enterprise usually needs according to their production requirement. Our final result shows in the below table and the analytical graph will show you how much we have enhanced the overall network performance by using the fortinet next-generation firewall in our existing system.

Table 6.3: Performance Enhancement Report

Measurement Category	Existing Network	Proposed Network	% of Enhancement (Experimental Approx. value)
Avg. Latency in Regular Usages	32ms	25ms	20%
Avg. Packet Drop at Pick Usages	3%	0%	100%
Avg. Page Load Time	9s	6s	30%
Speed Test	18Mbps	37Mbps	50%
Protection Level	Layer-5	Layer-7	30%
Secure VPN	Unencrypted	Encrypted	100%
UTM (Anti-virus, Web-filter, IPS)	None	Secured	100%
Traffic monitoring	Manual	Automated	50%
Log & Reporting	Very Limited	Advanced & analytical	80%

Graphical representation of **enhancing overall network performance** using Next-Generation Firewall – (Approx. Value)

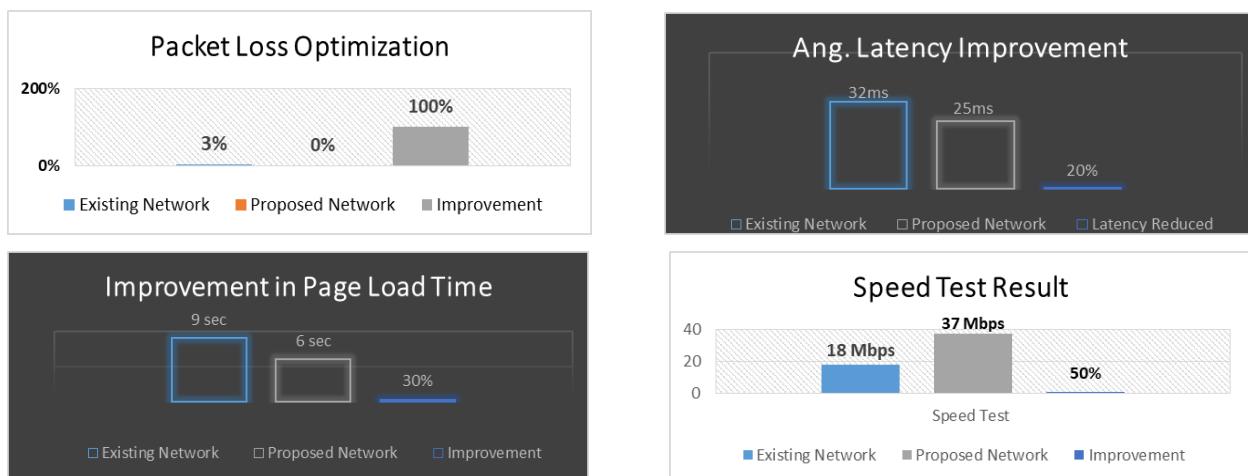


Figure 6.39: Enhancing overall network performance using NGFW

Graphical representation of **enhancing network security and operational management** using Next-Generation Firewall –

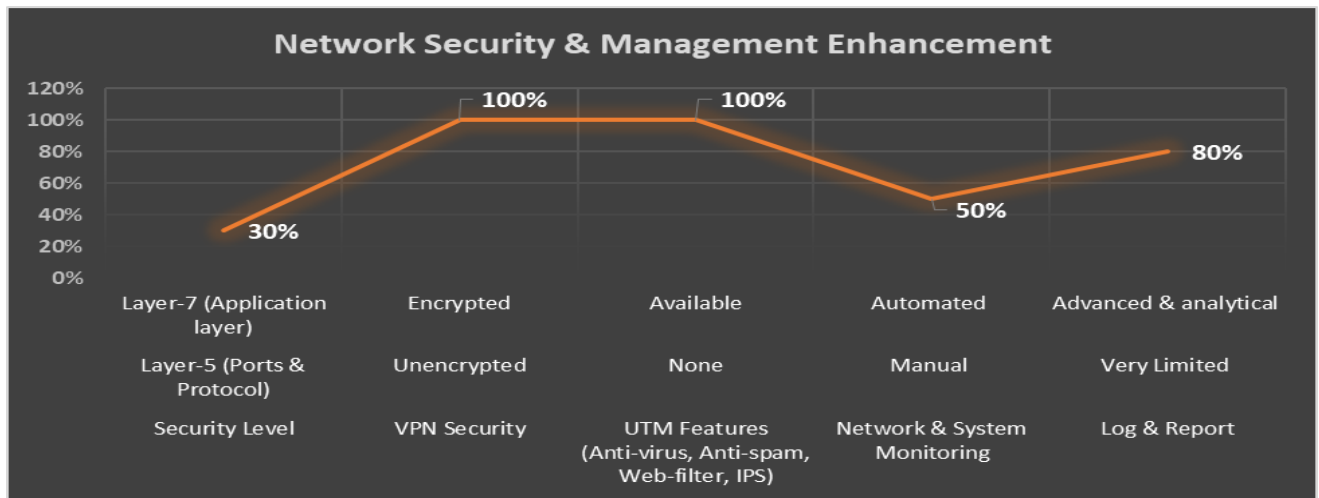


Figure 6.40: Enhancing network security and operational management using NGFW

CHAPTER 7

CONCLUSION

7.1 RECOMMENDATION & CONCLUSION

One of the best things about a firewall is that it stops unauthorized identity on the outside from logging onto a computer in your private network. Considering current security threat analysis, commercial networks are highly recommended to introduce with Next Generation Firewalls to protect their sensitive data and any kind of unwanted network access.

Basically, an enterprise network attacked by many threats like external and internal threats. Also, attacks came from different layers. To prevent this attack enterprise network uses different devices like VPN, firewall.

Firewall is used for filtering the traffic which comes from the internal or external network. A firewall can be either hardware based or host based. Different firewall used in a different layer. Based on the network criteria firewall is implemented in the network. Virtual Private Network (VPN) is used to connect to different networks which are located in the different area for securing data. VPN creates a tunnel to secure private network from the public network. Basically, an enterprise network creates by interconnects different LAN and WAN. Also, there are different requirements of enterprise network such as availability, security, redundancy, reliability, scalability. These requirements make enterprise network reliable.

Security threats become a big challenge to create an enterprise network. This enterprise network is affected by different threats like IP spoofing, Phishing attack, DoS attack, spyware attack etc.

The proposed solution using NGFW gives a better solution to prevent those attacks. As an enterprise network security issue is critical we deployed firewall and VPN to protect the network. But there is no guarantee that the proposed NGFW can detect the new attacks coming near future. The proposed security model using NGFW only detect the common listed and current dynamic attacks to secure our enterprise network.

7.2 FUTURE WORK

According to our performance evaluation in above discussion we found a lots of improvement in network performance, security and resource utilization as well. One of the main purpose of the module is to provide enough information about different types of threats, attacks and intrusions before they occur. And, during selecting and deploying a firewall this module will help you to take your decision in an efficient manner.

But, still a lot to do specially in network security portion. Our proposed solution can give intermediate level of security against latest security attacks but really not sufficient especially in case of DDoS type attacks. We will try to use the firewalls from other vendors such as Cisco ASA, Juniper, Palo Alto, Check point etc. in near future which will help us to understand their advantages over each other. We will also need an advanced wireless security module to protect the enterprise wireless network in this era of wireless technology. In our future work, we will try to cover all those security area for the betterment of entire information and communication community.

7.3 REFERENCES

- [1] J. E. Canavan, *Fundamentals of Network Security*. Norwood, MA, USA: Artech House, Inc., 2001, p. 153-155.
- [2] Khaled W. Alnaji "Developing Security-Enhanced Model For Enterprise Network" Islamic University – Gaza Palestine 1435H (2014)
- [3] Mr. Sachin Taluja¹, Prof. Rajeshwar Lal Dua² "Survey on Network Security, Threats & Firewalls" Volume 1, Issue 7, September 2012 ISSN: 2278 – 1323
- [4] Zou, C., Towsley, D., Weibo, G., A Firewall Network System for Worm Defense in Enterprise Networks, Technical Report: TR-04-CSE-01, University of Massachusetts, Amherst, 2004
- [5] K. Ingham and S. Forrest, "A history and survey of network firewalls," University of New Mexico, Tech. Rep, 2002.
- [6] Tasnuva Mahjabin, Yang Xiao, Guang Sun "A survey of distributed denial-of-service attack, prevention, and mitigation techniques" Available:
<https://journals.sagepub.com/doi/full/10.1177/1550147717741463>
- [7] J. Hong, "The state of phishing attacks," *Commun. ACM*, vol. 55, no. 1, pp. 74–81, Jan. 2012. [Online]. Available: <http://doi.acm.org.focus.lib.kth.se/10.1145/2063176.2063197>
- [8] R. Dhamija, J. D. Tygar, and M. Hearst, "Why phishing works," pp. 581–590, 2006. [Online]. Available: <http://doi.acm.org/10.1145/1124772.1124861>
- [9] <https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/threat-report-q1-2019.pdf>

- [10] Next-Generation Firewalls For Dummies, ISBN: 978-0-470-939550. Available: https://www.csuc.cat/sites/default/files/docs/ngfw_for_dummies_ebook.pdf
- [11] Ioannidis, S., Keromytis, A.D., Bellovin, S.M., Smith, J.M., Implementing a Distributed Firewall, In Proceedings of Computer and Communications Security (2000), CCS'00 pp. 190-1999
- [12] Monali S. Gaigole, Prof. M. A. Kalyankar "The Study of Network Security with Its Penetrating Attacks and Possible Security Mechanisms" IJCSMC, Vol. 4, Issue. 5, May 2015, pg.728 – 735.
- [13] Axelsson, S., Intrusion Detection Systems: A Survey and Taxonomy, Technical Report, pp. 99-115, Dept. of Computer Engineering, Chalmers University of Technology, Sweden, March 2000
- [14] S. Alabady, "Design and Implementation of a Network Security Model for Cooperative Network," Int. Arab J. e-Technol., vol. 1, pp. 26-36, 2009.
- [15] Best Practice by Fortinet Document Library, Available: <https://docs.fortinet.com/document/fortigate/6.2.0/best-practices/587898/best-practices>
- [16] Data-Sheets by Fortinet, available: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_300E.pdf
- [17] Network Access Control [December 19 2018 4PM] is available here <https://www.esecurityplanet.com/network-security/network-access-control.html>
- [18] FortiGate: Next Generation Firewall (NGFW) (November 12 2018 9.24PM) is Available Here <https://www.fortinet.com/products/next-generation-firewall.html>

7.4 APPENDIX-A

LIST OF ABBREVIATIONS

ACL	Access Control List
API	Application Programming Interface
ARP	Address Resolution Protocol
ATP	Advanced Threat Protection
BER	Bit-Error-Rate
CLI	Command Line Interface
CPU	Central Processing Unit
DDoS	Distributed Denial of Service
DMZ	Demilitarized Zone
DNS	Domain Name System
DoS	Denial of Service
ICMP	Internet Control Message Protocol
IDS	Intrusion-Detection System
IP	Internet Protocol
IPS	Intrusion Prevention System
LAN	Local Area Network
MAC	Media Access Control
MAN	Metropolitan Area Network
NAT	Network Address Translation
NGFW	Next Generation Firewall
NIC	Network Interface Controller
OS	Operating System
QoS	Quality of Service

RAM	Random Access Memory
SAAS	Software as a Service
SDN	Software Defined Network
SDWAN	Software Defined Wide Area Network
SLA	Service Level Agreement
SNMP	Simple Network Management Protocol
SSL	Secure Socket Layer
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UTM	Unified Threat Management
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
VRRP	Virtual Router Redundancy Protocol
VSG	Virtual Security Gateway
WAN	Wide Area Network
WLAN	Wireless Local Area Network