

SIGNIFICANCE OF FIREWALL AND ITS PRACTICALITY IN CORPORATE ENVIRONMENT

Dissertation submitted to Botho University

In partial fulfilment of the requirements

For the award of the degree of

Masters

In

Computer Systems Management

Submitted by

Gnana Jagathese Chelladurai

Under the Supervision and Guidance of

Dr Srinath Doss Ph.D



FACULTY OF COMPUTING

BOTHO UNIVERSITY

GABORONE

May 2019

Abstract

In recent days possible attacks on the networks has been increased and causing huge financial loss for the various organization due to lack of proper security standards. Modern networks have several services and zones like Voice, Data, ISP networks, Access control, surveillance, DMZ zones and hosting websites etc. Proper planning and access control within each zone are important to avoid network compromise. This research details on how the network can be security standards can be implemented using effective controls, in and out of each service zones. The focus of this research is intended to reduce down time and loss of service in an event of a network compromise or an external attack such as DoS, Distributed Denial of service attacks, Brute Force attack, Packet Sniffing and phishing attacks. The results confirm, when the network is structured using effective controls, in and out of each service zones will increase the security, decrease the down time and extent of compromise.

Keywords:

Segregating Network, Firewall, Security, Threats, DDoS, UTM, routing

Declaration

I **Gnana Jagathese Chelladurai** of Student identification (ID) 1817509 hereby declare that this dissertation work has been genuinely done by me. I am fully aware of Botho University Plagiarism policy and I have taken all the necessary measure to comply with the policy. Relevant sources that were used in this study, has been acknowledged.

.....

Signature

.....

Date

Acknowledgement

“To God be the glory, for the guide, protection and strength throughout my entire learning. My sincere gratitude goes to Dynagrow Company for the privilege to further my studies on master’s degree. My sincere appreciation goes to research supervisor Dr Srinath Doss for always assisting me throughout my entire study. This study couldn’t have attained its mandate without his patience, time and methodical understanding. My heartfelt thanks go my wife and friends for their support and prayers”.

Abstract

In recent days possible attacks on the networks has been increased and causing huge financial loss for the various organization due to lack of proper segregation. Modern networks have several services and zones like Voice, Data, ISP networks, Access control, surveillance, DMZ zones and hosting websites etc. Proper planning and access control within each zone are important to avoid network compromise. This research details on how the network can be segregated using effective controls, in and out of each service zones. The focus of this research is intended to reduce down time and loss of service in an event of a network compromise or an external attack such as DoS, Distributed Denial of service attacks, Brute Force attack, Packet Sniffing and phishing attacks. The results confirm, when the network is segregated using effective controls, in and out of each service zones will increase the security, decrease the down time and extent of compromise.

Table of Contents

Abstract	5
Table of Contents	6
ABBREVIATIONS AND ACRONYMS	10
List of Figures	11
1. Introduction	15
1.1 Firewall types	15
1.2 Non-public firewall	17
1.3 Personal Firewall	17
1.4 Protecting yourself with a personal Firewall	17
1.5 Firewall Design	17
1.6 Background	18
1.7 Problem Statement	19
1.8 Aim of the Study	20
1.9 Research Objective	20
1.10 Research Questions	20
1.11 Significance of the study	20
2 Literature Review	22
2.1 Introduction	22
2.2 Network Security Layers	22

2.3	Encryption	24
2.4	Packet Filtering technique	25
2.5	Virus Infection	26
2.6	Firewall Configuration	27
2.7	Port Scanning	27
2.8	IP Spoofing	28
2.9	Secure routing	29
2.10	VPNS	29
2.11	Single sign-on	30
2.12	Network Segmentation	31
3	Proposed Work	34
3.1	Proposed Architecture	34
3.1.1	Without Segregation and Firewall	34
3.1.2	With Firewall	35
3.1.3	Network With Segregation	36
3.1.4	Security Standards	37
4	Implementation	41
4.1	Anti Virus	41
4.2	Web Filtering	43
4.3	Potentially Liable	43
4.4	Potential Liable Category in Blocked state	44

4.5	Bandwidth Consuming	45
4.6	Security risk category	46
4.7	General Interest Personal	47
4.8	General Interest – Business	49
4.9	DNS filtering	50
4.10	DNS filter	50
4.11	Application control with overrides	61
4.12	Application control – Cloud IT Category	64
4.13	Application control – Collaboration category	66
4.14	Application control – Email category	68
4.15	Application control – Game category	70
4.16	Application control –General Interest category	72
4.17	Application control – Network Service category	79
4.18	Application control –P2P category	83
4.19	Application control – Proxy category	84
4.20	Application control –Remote Access category	86
4.21	Application control – Social Media category	88
4.22	Application control – Storage Backup category	90
4.23	Application control –Update category	93
4.24	Application control – Video/Audio category	94
4.25	IPS Sensor	r97

4.26	SSL Inspection	99
4.27	Logs and reports of events	100
4.28	Firewall policy summary	102
4.29	Granular Firewall Policy configuration	104
4.30	Firewall compliance and up to date definition	105
5	Recommendation from research	107
5.1	Recommendation	107
6	Conclusion and Future research	110
6.1	Conclusion	110
6.2	Future research	110
	Reference	111

ABBREVIATIONS AND ACRONYMS

OSI – Open system Interconnection
DNS – Domain Name System
IPS – Intrusion Prevention System
IDS – Intrusion Detection System
TCP – Transmission Control Protocol
IP- Internet Protocol
UDP- User Datagram Protocol
DoS – Denial of Service
DDoS- Distributed Denial of Service
VPN- Virtual Private Network
SSL- Secure Socket Layer
FTP- File Transfer Protocol
LAN- Local Area Network
VLAN- Virtual LAN
WAN- Wide Area Network
ISP- Internet Service Provider
URL- Uniform Resource Locator
SMTP- Simple mail transfer Protocol
DMZ- Demilitarized Zone

List of Figures

Fig 1: Network Security Layers

Fig 2: Firewall

Fig 3: Network with firewall

Fig 4: Virus Infection pattern

Fig 5: Firewall configuration table

Fig 6: Port Scanning

Fig 7: IP Spoofing

Fig 8: Routing Protocols

Fig 9: VPN

Fig 10: Single Sign-on

Fig 11: Segmented Network

Fig 12: Network Without Segregation and firewall

Fig 13: Network setup with firewall

Fig 14: Segregated Network Topology

Fig 15: Segregated Interfaces

Fig 16: Anti-Virus

Fig:17 Static URL Filter

Fig 18: Potentially Liable Category

Fig 19: Potential Liable Category in Blocked State

Fig 20: Bandwidth Consuming

Fig21: Security Risk Category

Fig 22: General Interest and Personal Category

Fig 23: General and Personal Interest in allowed state

Fig 24 : General Interest with Web-Based Email Blocked state

Fig 25: General Interest with Business

Fig 26: DNS Filtering

Fig 27: Fortiguard Category based filter

Fig:28 (i) Botnet C&C Category

Fig:28 (ii) Botnet C&C Category

Fig:29 Botnet - Filtering service for account validation

Fig:30 Botnet Category

Fig: 31 Edit Application server

Fig:32 Application control – Business category

Fig: 33 Application control – Cloud IT category

Fig :34 Application control – Collaboration category

Fig :35 Application control – Email category

Fig: 36 Application control – Game category

Fig: 37 Application control – General Interest category

Fig: 38 Application control – Network Service category

Fig:39 Application control – P2P category

Fig: 40 Application control – Proxy category

Fig: 41 Application control – Proxy category

Fig: 42 Application control – Remote Access category

Fig: 43 Application control – Social Media category

Fig: 44 Application control – Storage backup category

Fig:45 Application control – Storage category

Fig:46 Application control – Update category

Fig: 47 Application control – Video /Audio category

Fig:48 IPS sensor

Fig:49 Edit filter – IPS filters

Fig:50 SSL/SSH Inspection Profile

Fig 51: Logs and report of events

Fig:52 Email Service

Fig 53: Email alert Setting

Fig 54: Firewall Policy summary

Fig 55: Granular Firewall Policy configuration – with Security standards enabled

Fig 56: Firewall compliance & Up to date definitions

CHAPTER – 1

INTRODUCTION

CHAPTER-1

I INTRODUCTION

Modern networks have several services and zones like Voice, Data, ISP networks, Access control, surveillance, DMZ zones hosting websites etc., proper planning and access control from and within each zone is important to avoid compromise [1].

In this research we would research how the network can be secured using effective controls, in and out of each service zones. Generally, firewalls are made to protect in opposition to un-validated logins from external network [2][3]. Mostly firewall depends on the capacity of the firewall, it permits the valid users to pass the traffic both inbound and outbound of the network. However, physical security is like armed guard and security can be used to protect our network physically, where as the firewall secures the network from the remote logins.

Firewall is the single choke point control which grants and rejects the traffic looking into the configuration. Administrator can audit each and every connection that has passed through the firewall [4][5][6]. Firewall configuration is the key for the protecting the network, firewall policy should also match with the organization policy in-order to provide effective controls on the network. It helps in preventing the malware and wasting of the bandwidth by utilizing the unwanted service, which hampers the operation of the organization.

1.1 Two firewall types

- i. Application layer firewall
- ii. Network layer firewall

Firewalls are now not much extraordinary as we think, which purely depends on the mechanism that we use to allow and omit certain connections in the network [6][7][8]. Standards like ISO – “International Standard Organization” and OSI – “Open system Interconnect” model defines types to be includes seven layers, the place every layer gives offerings to other higher layer on the relay. The vital issue to apprehend is forwarding technique can perform interaction between the firewall. Usually it is valuable to secure the system with firewall. Most of the organizations prefer

this type of security. Protecting the network from the unauthorized user accessing the valid network and infecting the network with the can be better handled using the combination of both hardware and software-based firewall [1].

Firewalls stops the traffic from the non-public network on the internet. Each packet that flow through the protected network need to flow through the firewall for the authentication process. Based on the organization policy the packets are decided to pass through or blocked by the firewall. Firewall rules can be customized in-order to increase the security features which enables more protection for the network [9].

Firewall basically use the source, destination and port number of the incoming packet to the network. Routers are the simple layer firewall where it helps to find the packet arrival and the discard on the network. The network setup needs to be configured based on the security policy put in place which helps to secure the entire network. Filters were used to list filter the content and analyses the utilization of the services. Transparent firewall like software based helps to increase the network security [10].

Lots of sophisticated has been increased in the community layer firewalls have come to be an increasing number, and now hold interior data about the nation of connection. Most of the software layer firewall is not transparent to the end user. Update on the older version and enhancement has increased the efficiency of the software-based firewall. Cost effective way to protect the network from the intruder [11][12][13].

Community and utility layer firewall is the future which helps to grant more precious audit and grant. Checking for the malwares is the key to protect the network from the internal and external stakeholder. Firewall helps to mange data packet and manage connections. Access rules were set in order to check for the validity of the user. Packet inspection is the one of the ways to analyses the packet in the network which helps prevent the denial of service attacks. Fare adoption of firewall is the key to any organization which need to maintain the security standards as per the policy specified [14][15]. Following the effective security policy in the organization helps in increase of network security and organization security standards.

Firewalls used to enhance the protection by enabling the granular control with which type of the system function can be processes to access the network. The firewall can be used by different kinds of the signs and node condition to accept and reject. Firewall are most comfortable to operate the sounds and setup the system.

1.2 Non-public Firewall

It's miles essential to apprehend “why we want a firewall and how it allows us within the world of cozy computing”. *“We want to recognize the desires of the information safety as it helps us to recognize how a firewall may additionally deal with those wishes” [16].*

1.3 Personal Firewall

In age of the excessive-velocity net access, you electrically connect your pc to s vast network over which, until you’ve got set up a private firewall, you have limited manage and from that you have confined safety. Until recently, except you laboured for a company that furnished high pace internet get right of entry to. Like whatever, the “high-speed connection” got its personal drawbacks.” In a manner, connecting to the net through excessive-pace connection is like leaving the front door of your private home open and unlocked” [17].

1.4 Protecting yourself with a personal Firewall

So now you’ve got an idea of ways you are vulnerable each time while you are online high velocity internet connection, compared to an everyday 56kbps connection. What you now need to know is how you can protect yourself in opposition to the chance posed by means of this sort of connection.

1.5 Firewall design

Firewall design is key to any organization who depends on the security to protect the information of the organization. When the firewall software is installed precaution need to be taken based on policies set for the inbound and outbound. Considering the below figure gives a clear picture of the firewall securing the network from the internet and remote logins[18][19]. Each individual packet is monitored over the network layer and helps to decode the packet header of the all the traffics that flows in the network.

1.6. BACKGROUND

Most of the organization face various attacks on their network due to the improper planning of their network setup, mainly lack of implementation of security standards in the infrastructure. Which results in uncontrollable compromise of the network along with huge downtime [20].

A computer needs firewall to protect the software from the illegal admission to a secured private network. Several tools were available in order to provide security for the systems connected in the network such as intranet and extranet. “A firewall absolutely separates the computer from internet with a “wall of code” that will check each packet of the data as it indicates in either side of the firewall” [21].

Firewalls used to enhance the protection by enabling the granular control with which type of the system function can be processes to access the network. The firewall can be used by many types the signs and the host to grant access. Firewall are most comfortable to operate the sounds and setup the system.

What is non-public Firewall?

It's miles essential to apprehend the need for the firewall and how firewall allows incoming packet within the world of cozy computing. “We want to recognize the desires of the information safety as it helps us to recognize how a firewall may additionally deal with those wishes”[22].

What is the need for personal Firewall?

In age of the excessive-velocity net access, you electrically connect your pc to s vast network over which, until you’ve got set up a private firewall, you have limited manage and from that you have confined safety. Until recently, except you laboured for a company that furnished high pace internet get right of entry to. Like whatever, the “high-speed connection” its personal draw backs. “In a manner, connecting to the net through excessive-pace connection is like leaving the front door of your private home open and unlocked”.

- “A constant IP “- Perform smooth interloper who observed your system at the network to discovered over and over.
- “High-speed get admission” to - method that the intruder can work a good deal quicker while trying to break into your pc.
- “Continually lively connection”- way your laptop is exposed on every occasion whilst it is linked to net.

The integrity of data would be paramount in terms of securing the environment with methods which is best evolved as per best practices and industry standards. In this research, we would go through various methodologies and services, using various authentication and security controls used to secure all the various network zones in a heterogeneous environment[24].

1.7 PROBLEM STATEMENT

In the current day, data compromise and system sabotage are becoming a very common way for the perpetrators to hold ransom the victimized environments. This research deals with minimizing the damage in case of the occurrence various attack on the network, which will complete affect the network performance. This research is intended to reduce down time and loss of service in an event of a network compromise or an external attack such as DoS, Distributed Denial of service attacks, Brute Force attack, Packet Sniffing and phishing attacks. Appropriate use of security controls in the network hence the performance of the network and protecting the resources form inbound and outbound network attack. Hence, this research details on the use of firewall in the corporate environment which helps to reduce the burden of downtimes during the request for the certain services. Adopting to the best practices in industry will minimize the data compromise and helps to keep the network more secure.

1.8 AIM OF THE STUDY

The aim of this research is to make sure the best practices as per industry standards are explored, pros and cons would be discussed, to minimize the extent of exposure and data compromise.

1.9 RESEARCH OBJECTIVES

To recommend and suggest best infrastructure deployment methodologies and topologies, using the best security standards and methods available in the current industry. Focus would be more on effective implementation rather than reinventing the wheel as most standards of security are already available.

1.10 RESEARCH QUESTIONS

At the end of the literature the following research question should be asked, and we should have the answers for the following.

1. As the Goals of securing the network environment achieved?
2. As an offense (Possible attacks) been tested?
3. Does the implementation hamper user experience?
4. Have the best practices as per industry standards been followed?

1.11 SIGNIFICANCE OF THE STUDY

- ✓ The study would be used as a benchmark to design a network infrastructure, which can secure privacy, confidentiality and data integrity.
- ✓ The research would focus on a cost-effective solution with no compromise to the data security.
- ✓ The main idea behind this research would be to reduce down time and loss of service in an event of a network compromise or an external attack.

CHAPTER – II
LITERATURE REVIEW

CHAPTER - II

2. LITERATURE REVIEW

2.1 Introduction

In paper [1][2] it is discussed firewall is deployed in the internet to prevent the harmful events occurring in the network. There are different types of firewall such as application level gateway, packet filtering and circuit level switching. Basic principle will be deploying the firewall to monitor the traffic both the inbound and our mail in the networked environment. Network address translation is used limit the public IP address in our organization. Packet filtering basically used to analyse the packets then decide to pass or halt based on the Ip address of the source and destination [27].

Firewall protects the internal resource form the outside world and provides the secure manner to communicate with the internal system form the external network [2][28]. Virtual connection is used for the secure connection between the sender and receiver over the non-secure public network. It basically protects the information from the unauthorised access using the encryption algorithm and security mechanism to prevent unauthorised access to information. Mostly, tunnelling is used to transport the data by encapsulating one protocol over another protocol. It uses the public network to decrease the cost [29].

Packet filtering firewall allows or blocks the packet based on the rules set. In terms of security they can't make any dynamic decision on packets [4][30]. Dynamic decision is very difficult and challenging in the packet filtering firewall, due to this reason network may be more vulnerable. The private network resource can be access used the virtual private network with the host machine residing on the network. Advancing on the delegated access may restrict the users access the internal network. Users are given the privilege to access the resources by allocating the security credentials.

2.2 Network Security Layers

Access control service helps in handling the access permission to networked environment. VPN technology help in proving the authenticating the proxy behalf of remote users [7][31]. Hiding of

the real address of the proxy host is done by the network address translation. NAT function were used to address the IPV4 routing addressing. High security can be provided by using the increased capacity of the firewall and the configuration. TCP handshaking is used to validate the session, while considering the packet filtering only valid and authorised packet will pass through the firewall [32].

Considering an example of online examination where firewall helps to make the secure system. VPN and NAT helps to make this secure system. User with unique identification and password can authenticate the private network. PIN (personal Identification number) is used to authenticate the user [30][33].

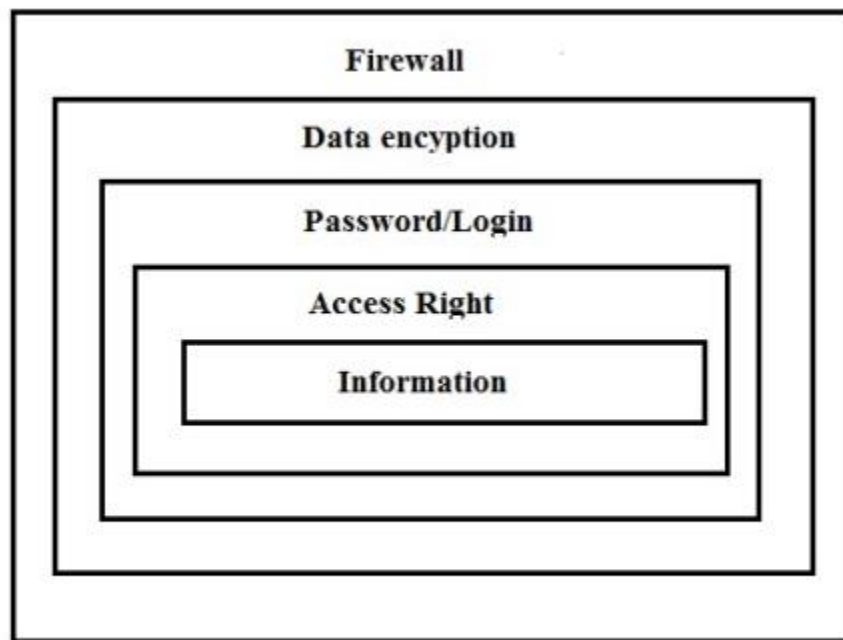


Fig 1: Network Security Layers

Network security layer consist of the information as the core followed by the access rights, password/login, data encryption and firewall. Firewall is the key component which protect the information from the external login, configuring the firewall is the very important in securing the information of the organization [37]. The above multilayered helps to handle the violating activity in the network. Most of the organization stores their information on the server and which need to be protected from the internal and external threats. From the above the figure the very inner most

layer is the access rights which determines which users can use the resources. The username and password help to provide security mechanism and it is the simplest method to verify the users.

2.3 Encryption

Data encryption is the one of the key methods to protect the information. The most popular encryption methods are public key and the private key algorithms. In terms of symmetric key, a single key is used to encrypt and decrypt the message between the sender and receiver. Whereas, public key encryption algorithm like RSA used the public and private keys. A pair of keys is used in term of public key encryption algorithms [36].

The last layer is the firewall which helps to prevent the intrusion into the network. It basically filters the unwanted traffic between the inbound and outbound traffic in the networks. Firewall is the hardware based and host based. Hardware based firewall often expensive and need configuration on the network [37]. In terms of software-based firewall, which runs on the system allows or blocks the traffic based on the rules defined.

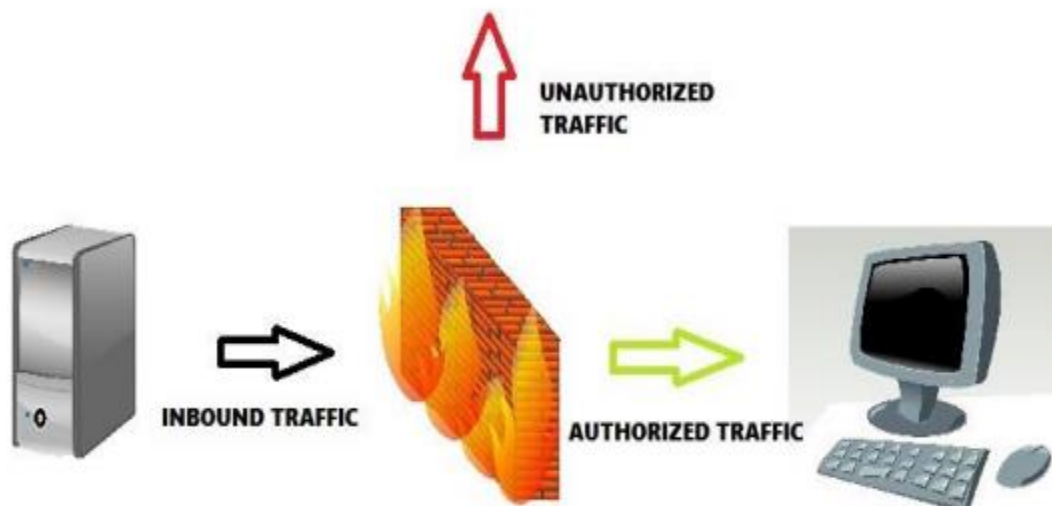


Fig 2: Firewall

Firewall allows the legitimate traffic to pass and block the unwanted traffic in the network. The above figure clearly depicts the firewall filters the unauthorized and authorized traffic in the network [39]. However, firewall can authenticate, protect, record and report etc.

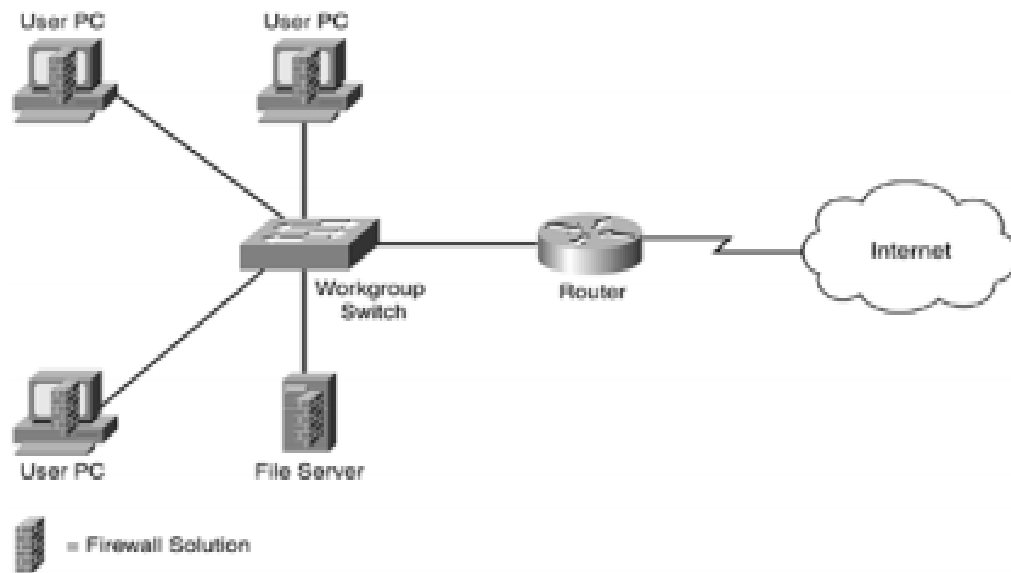


Fig 3: Network with firewall

2.4 Packet filtering technique

Securing the resource in the local network is the more challenging. Network resource residing in the intranet or FTP server etc. need to provide with the access mechanism using the proxy servers. Firewall is not only the security solution for the network related problems and network administrator need to do the network monitoring to secure the network resources. Treats to the sensitive data can come form any form of the source and mitigation methods need to be placed to avoid such situation to increase protection for the corporate information[40].

Adopting to the packet filtering technique involves the following rules. Such as

- “1. IP source address
2. IP destination address
3. Transfer protocols (TCP, UDP, ICMP, etc.)

4.TCP/UDP source port

5.TCP/UDP destination port

6.ICMP message type

7.Interface of incoming/outgoing packet”

The connection can be blocked for the invalid IP address and source. Protocols such as TELNET, SMTP and FTP mostly allowed to transfer into the local network.

2.5 Virus Infection

Malware are malicious software which affects the system and network. The virus looks for the vulnerable host and copies the code into it and infect the program. These viruses can attach to the program wherever they want in order to exploit and create the harm to the systems. Below is the figure explain about the virus infection patterns [43].

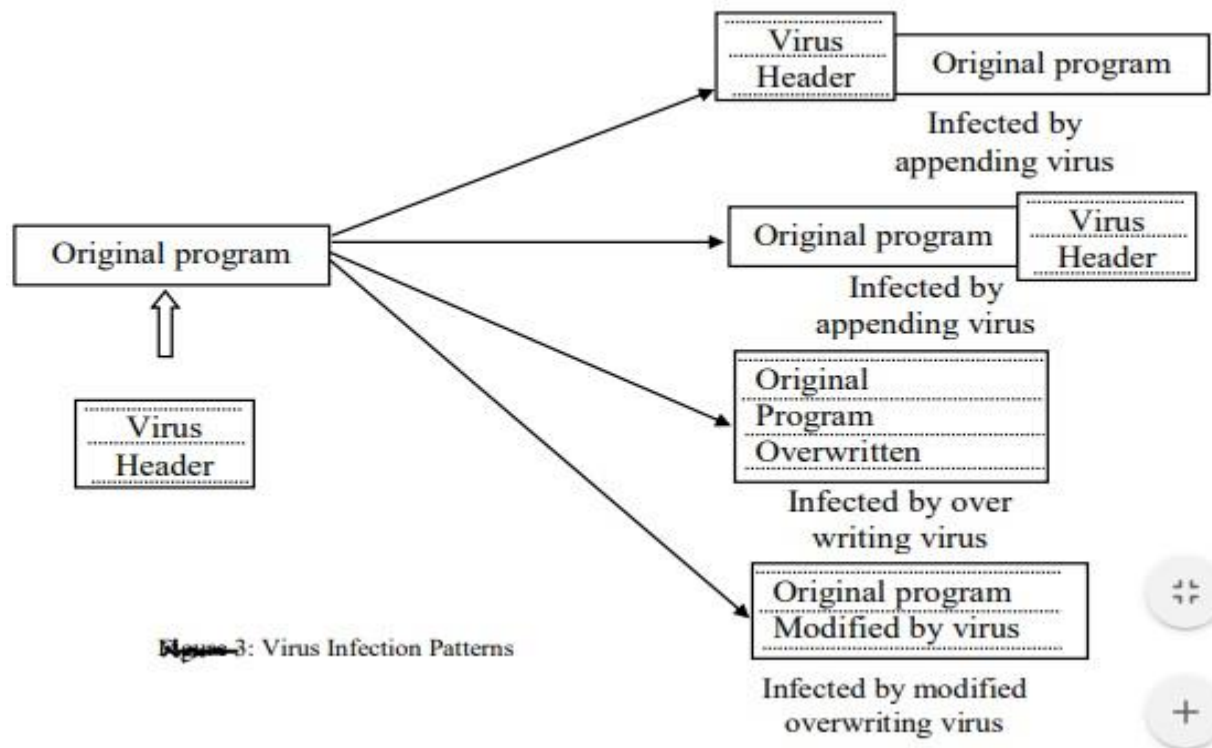


Fig 4: Virus Infection pattern

Virus header infects the original program and program gets infected by the appending virus. Once the original program is infected it can move from one system to another replicating and spreading such virus into the network.

2.6 Firewall configuration

Firewall configuration helps in putting the policies in place in order to secure the network form the external attack [44]. Administrator define the firewall policy to determine which traffic should pass through the inbound and outbound.

Rule #	Interface	Source IP	Destination IP	Destination Port	Protocol	Decision
1	0	224.168.0.0/16	192.168.0.1	25	TCP	discard
2	0	!224.168.0.0/16	192.168.0.1	!25	*	discard
3	0	*	192.168.0.1	25	TCP	accept
4	0	224.168.0.0/16	*	*	*	discard
5	*	*	*	*	*	accept

Rule #	Interface	Source IP	Destination IP	Destination Port	Protocol	Decision
1	0	!224.168.0.0/16	192.168.0.1	25	!TCP	accept
2	0	224.168.0.0/16	*	*	*	discard
3	0	*	192.168.0.1	25	TCP	ac
4	0	*	192.168.0.1	*	*	disc
5	*	*	*	*	*	accept

Fig 5: Firewall configuration table

From the above figures following rules has been set for the network environment. The configuration table consist of rules, interface, source and destination IP, destination port, protocol and decisions. Decision can be either accept or discard.

2.7 Port Scanning

Port scanning is used for understanding the port used by the user either TCP or UDP[51]. Since both the protocol uses the different ports the attacker needs to scan the port and under the inner

details [48]. It also helps to understand the protocol and operating system used by the user. Usually from the different port the remote machine tries to connect with the network. Port scanning is one of the methods where used to identify the vulnerable machine.

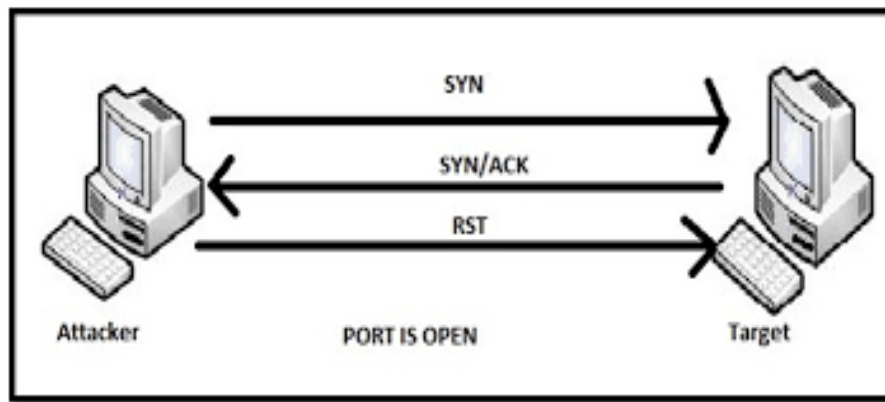


Fig 6: Port Scanning

2.8 IP Spoofing

IP Spoofing is one type of an attack, capturing the packet analyzing the header to obtain the ip address of the sender [49]. Masking the IP and transferring the packet with the forget IP address and tracking the connection to masked environment. Below Fig shows the counterfeiting of IP sender address.

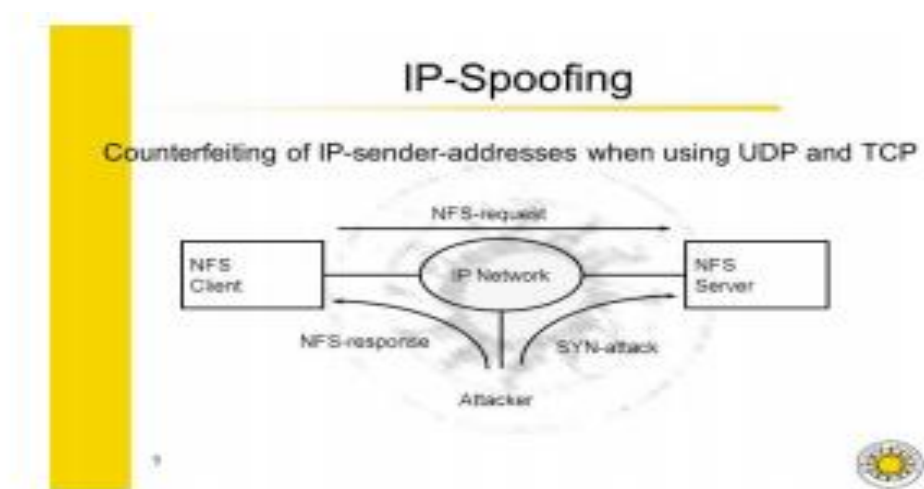


Fig 7: IP Spoofing

2.9 Secure routing

Routing is can be done on the both flat and hierarchical network [47]. There are several routing protocols with different routing strategy. Some if the routing protocols were listed in the below figure.

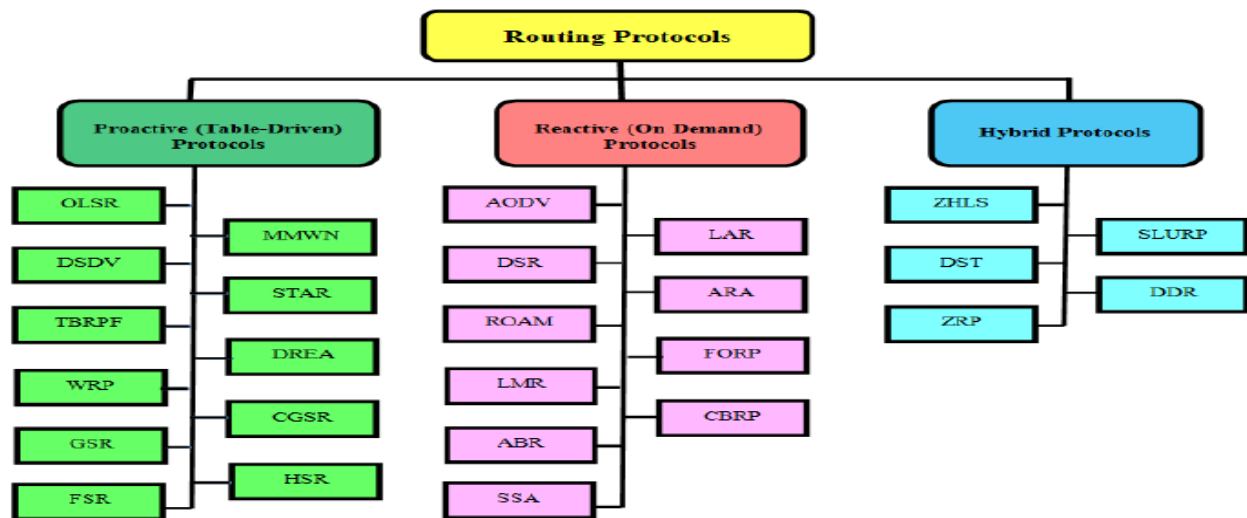


Fig 8: Routing Protocols

Routing protocols can be classified into reactive, hybrid and proactive based on the nature if the routing. These above protocols were needed to route the packets form source to the destination residing in the network layer. Updating the route and communication among the peers were very critical to provide better routing in the networks.

2.10 VPNS

Virtual Private Network allows external users to access the internal resources in the network. Security is the key for the VPN functioning were tunneling is used to create secure channel [51]. Transactions can be secured using the VPN connection and block the restricted access on the network. We can interconnection similar network over another network. Below fig. shows the VPN connection in Internet.

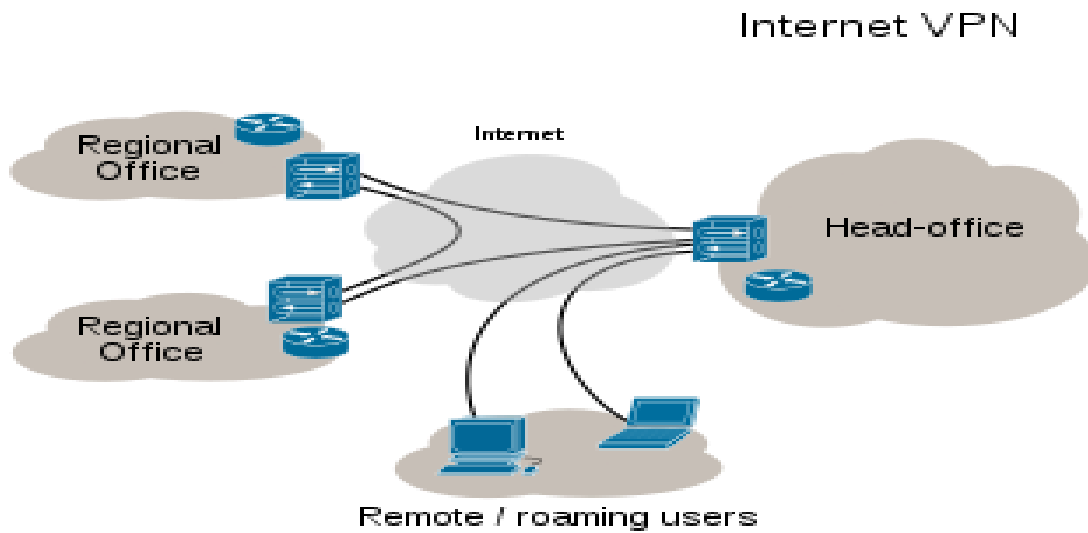


Fig 9: VPN

2.11 Single sign on

Single Sign-on helps to avoid multiple logins in the network. Single sign-on helps to access multiple application avoiding multiple login.

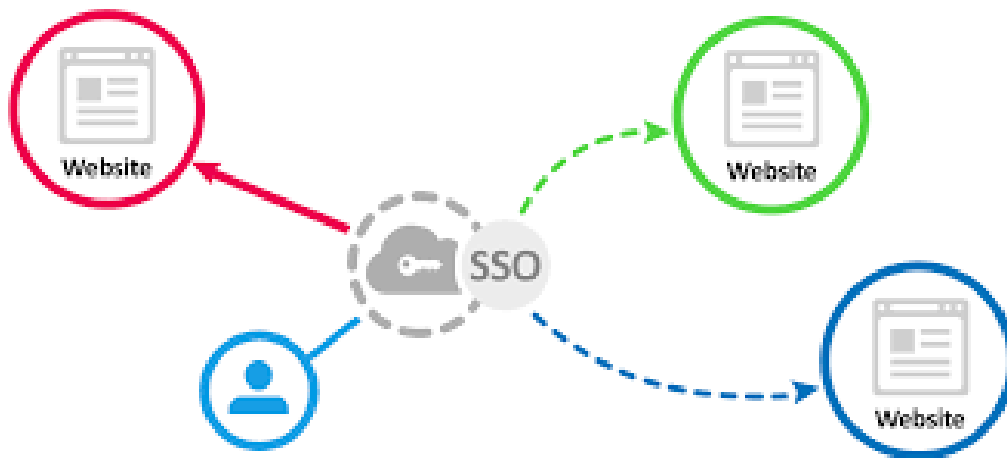


Fig 10: Single Sign-on

2.12 Network segmentation

Network segmentation associated segregation square measure extremely effective ways an organization will applied to limit the impact of a network intrusion. If enforced properly, these ways will create it considerably tougher for associate oppose to find associated gain access to organization's most sensitive information and increase the chance of sleuthing an adversary's activity in an exceeding on timely manner. Historically, network segmentation Associate in Nursing segregation has been enforced with a fringe firewall at an organization's net (or inter-organization) gateway; or a combine of firewalls close a demilitarized zone that provides a sequestered setting between utterly trustworthy[52][10].

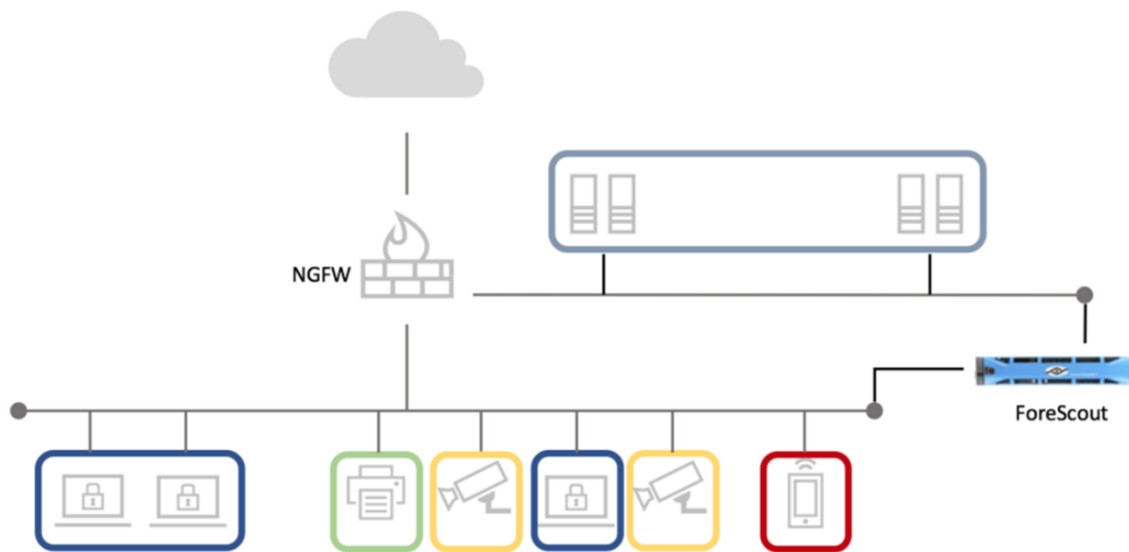


Fig 11: Segmented Network

However, merely segmentation a complete network as 'trusted' and treating it as 'flat' (i.e. the whole network as one segment) creates Associate in Nursing setting that needs solely one network intrusion for Associate in Nursing opposes to achieve widespread access. A flat network conjointly permits Associate in Nursing the opposer to pivot between hosts and services with marginal structure and restricted probability of detection [34].

With the opposing the trade craft target in the internal networks directly mistreating the techniques like in the various techniques and using various operating system, these are the common flat architecture of the network. It will not defend the organizations from up to date cyber threats. As a result, it's necessary for organizations to section the networks. The segregation sensitive data, hosts and services from atmosphere in external resources [30]. Specially the electronic mail and alternative net facilities.

Once an individual compromise a network, typically a bunch beneath the management of a Valid users suggests that of entertainment services, they'll decide to transfer round the network to find and admission sensitive info, hosts and services [47]. To reduce a network intrusion, it ought to exhaust potential for the individual to search out and admittance such info, move undiscovered round the network and take away info from the network. An individual could decide to build connections to satisfy host to additional "victimization tools and techniques" at their disposal. as an example, if AN individual has at first compromised a digital computer, they will obtain to make a foreign affiliation to a server.

In research paper [5] the author details "Map a network resource or use legitimate network administration tools to access sensitive info or execute malicious code thereon server. this is often notably common once an individual target. An organization's authentication server. Properly planned and enforced network segmentation and segregation may be a key security live to help in preventing such activities from occurring. Example mitigations embrace expressly disallowing remote desktop connections or the employment of common network administration tools from user workstations (as most users don't need such functionality), configuring servers to limit the sharing of files, and proscribing servers' ability to speak via remote connections" [11][45].

However, for the literature review several firewalls were developed both the hardware and software based. In terms of cost hardware based are high and firewall based don't poses much features like the hardware based. Using the appropriate standard increases the downtime and performance of the network. In conclusion of the literature review, corporate network needs to follow the security standards and policies which enable better services within the organization. Internal network can be protected from the remote attacks by properly configuring the firewall following the proper security features.

CHAPTER -III
PROPOSED WORK

3. PROPOSED WORK

3.1 Proposed Architecture

The diagram illustrates the network architecture for Nashua Ltd, showing connections between three locations: Nashua - Francistown, Nashua - Gaborone, and Nashua Ltd - JHB.

Connections:

- Point to Point Connection:** Direct links between Nashua - Francistown and Nashua - Gaborone, and between Nashua - Gaborone and Nashua Ltd - JHB.
- Link Used by F'Town for - Mapi email Clients AS400, VIA Gabs Data from Gabs Customer Harvester, VIA Gabs Internet Access, VIA Gabs:** A link from Nashua - Francistown to the central network.
- Link Used By Gabs For- AS400 Access (Gabs& FTN) Customer Harvester (Gabs & FTN):** A link from Nashua Ltd - JHB to the central network.

Central Network Components:

- VanGuard router:** The central hub for the network.
- Frame Relay - Modem FTN:** A link from the central router to the Nashua - Francistown location.
- Wan 2 - FTN:** A link from the central router to the Nashua - Gaborone location.
- Wan 1 - Jhb:** A link from the central router to the Nashua Ltd - JHB location.
- Frame Relay - Modem Nashua - Ltd- Jhb:** A link from the central router to the Nashua Ltd - JHB location.
- Network Switch:** A switch connected to the central router.
- IP Range - 10.11.1.0 / 24:** The central IP range.
- IP Range - 10.11.2.0 / 24:** A separate IP range for network clients.

Client and Server Details:

- Network clients - Nodes:** Includes desktop computers and laptops.
- AccPac server- Accounting application 10.11.1.5:** A server connected to the central network.
- Single server, With 2 x NIC's:** A server with two network interface cards, one for LAN access (IP 10.11.1.10) and one for internet access (IP 192.168.1.250).
- Server Roles:**
 - Directory server (For AD)
 - Email server Running exchange 2000
 - Internet sharing- proxy server
 - File server
- Internet:** Represented by a globe icon.
- ADSL - Modem For internet:** A modem connected to the internet.

34

The above shown network consist of two remote connection from two different places. It consists of two internet connections, one connection used for private browsing and other connects to the corporate network. VanGuard router has been used in the network to route packets using the frame relay internet connection. The IP ranges in all three locations are different in separate subnet. It has a server which is dedicated with several roles. Since the network has not been segmented which causes uncontrollable attack and downtime, hence affecting the business.

3.1.2 With firewall

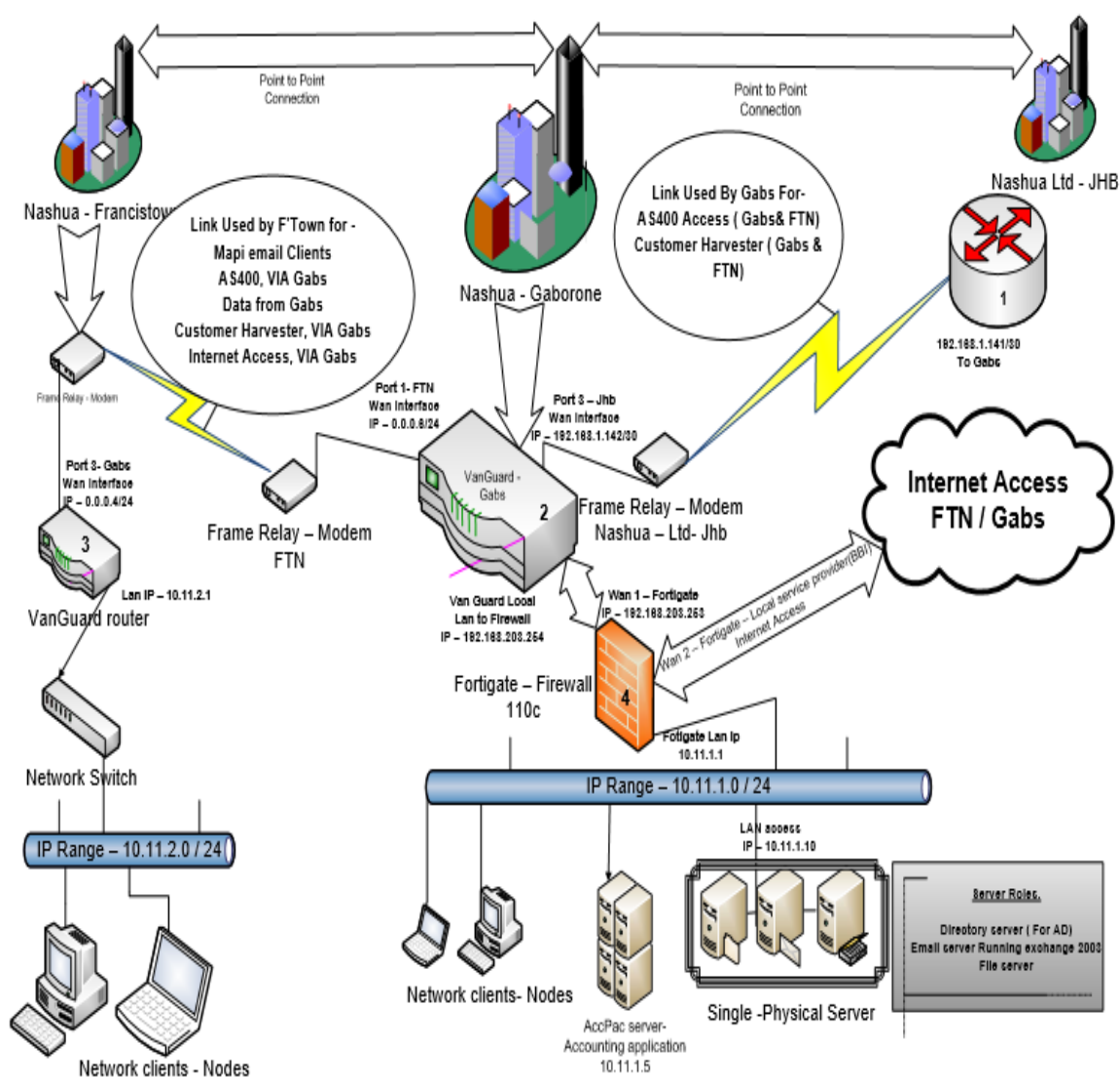


Fig 13: Network setup with firewall

The above network is with the firewall and two internet connection terminated on the firewall. The firewall also manages the connection to the branches. The firewall is fully enabled with UTM and routing polices as per the organization security policy.

3.1.3 With Segregation (Generated from System View)

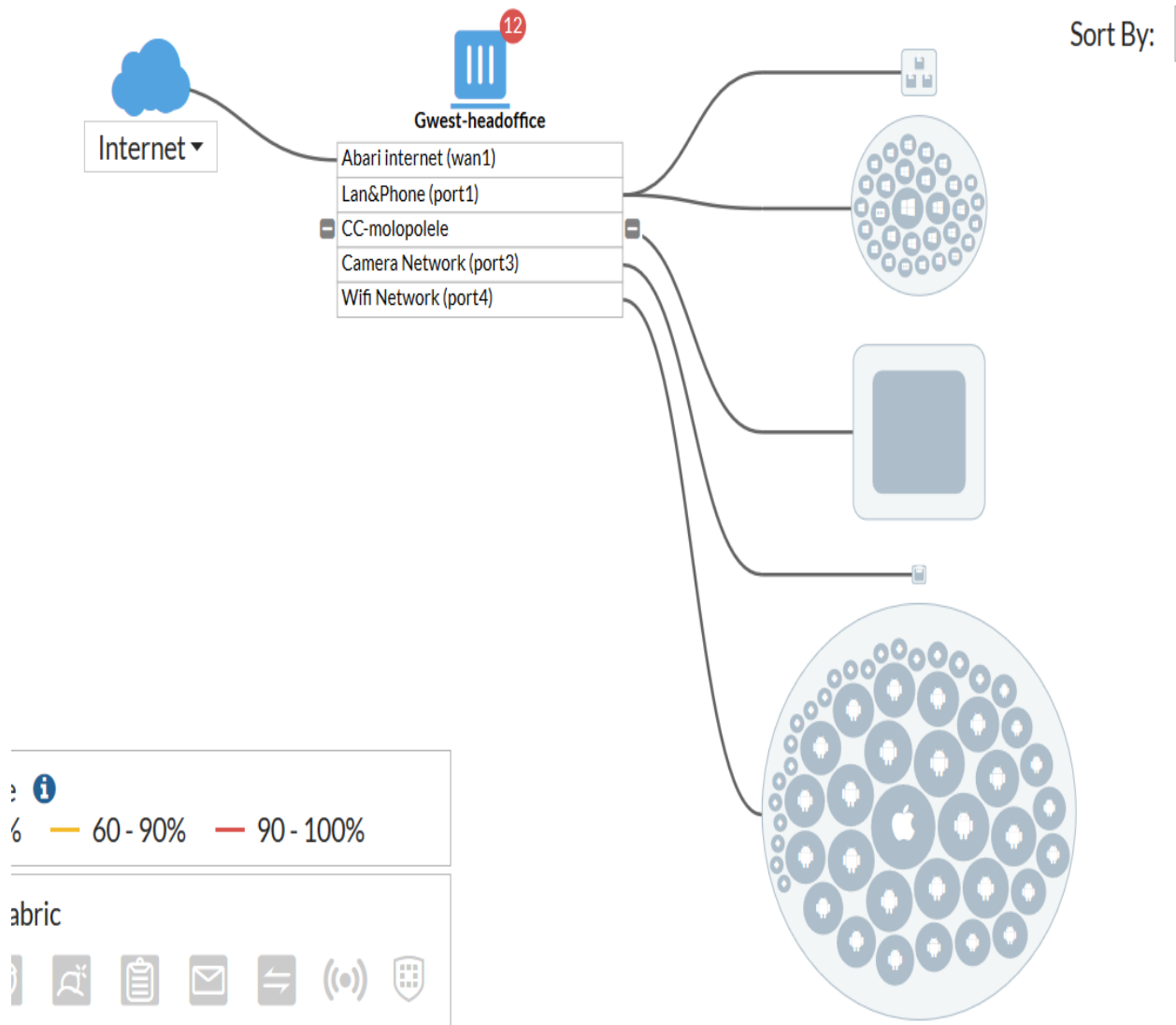


Fig 14: Segregated Network Topology

The proposed segregated network consists of various segments such as access control, VOIP, data, surveillance network. In the fig details on the various IP networks which are terminated independently.

192.168.101.X is for Data (Port 1)

192.168.102.X is for Access Control(Port 2)

192.168.103.X is for Surveillance (Port 3)

192.168.104.X is for Wifi(Port 4)

From the proposed Segregated Network system view internet is connected directly to firewall. The network is segmented using the firewall internally. The segregated network controls the access between the network segments using the firewall security policies. The above proposed firewall is a UTM enabled firewall, which enhances the security of the proposed network at the granular level. A complete network is implemented with two ISPs (Orange and Abari) , the traffic is load balanced between the two internet connection.

3.1.4 Security Standards

The proposed secured network has the following security standards:

- **Anti-virus:** Anti-virus engine scans for the threats and traffics (both in in-bound and out-bound) in the network. In addition to the scan it's also traces malware and it is more capable for virus outbreak. It also helps in network quarantine in case of virus outbreak.
- **Web Filtering:** The web filtering is category-based scan engine, which scans inbound and outbound traffic. The filtering polices can be defined by means of multiple polices as required by the organization IT policy.
- **DNS filtering:** The DNS filtering engine checks all DNS query outbound requesting external connections. The engine is a category-based standard which allows, or blocks based on the polices defined.

- **Secure routing:** The access of information amongst segments is configured using source and destination IP as required by the company IT policy. So that the communication is controlled between the segments and restricted to few trusted hosts.
- **VPNS for voice and external access:** VPNS is basically used to connect the branches to the data center. All Voice over IP (VOIP) credentials are encrypted within the IPSec VPN tunnel, which protects the network from eavesdropping and packet sniffing.
- **Single signon methodologies with secure integration using LDAP (wireless access, VPN access):** Single Signon is used for wireless and SSL VPN authentication. The single signon credentials will be same as the user log on to the network. It avoids users having multiple credentials and helps to block a user from a single location when he/she leaves the organization.
- **Content Filtering:** Content filtering is done by the firewall to manage content on internet data and key words defined by the IT policy of the organization.
- **Application Control:** It is a scan engine which scans application both inbound and outbound on each communication thread. On each communication thread the application control policies have been applied to match the allow and deny rules.
- **IPS/IDS:** Intrusion Detection and Prevention is based on the signature, which is mapped against the inbound and outbound traffic. Overrides can be added in case of false positive detection.

	▼ Status	▼ Name	▼ Members	▼ IP/Netmask	▼ Type	▼ Access	▼ Ref.
Physical (44)							
	🔴	dmz		10.10.10.1/255.255.255.0	Physical Interface	PING HTTPS HTTP FMG-Access CAPWAP	0
	🔴	ha1		0.0.0.0/0.0.0.0	Physical Interface		0
	🔴	ha2		0.0.0.0/0.0.0.0	Physical Interface		0
	🔴	mgmt		192.168.1.99/255.255.255.0	Physical Interface	PING HTTPS SSH HTTP FMG-Access	1
	🟢	port1 (Lan&Phone)		192.168.101.254/255.255.255.0	Physical Interface	PING HTTPS HTTP	86
	🟢	port2 (Access Control)		192.168.102.254/255.255.255.0	Physical Interface	PING HTTPS HTTP	2
	🟢	port3 (Camera Network)		192.168.103.254/255.255.255.0	Physical Interface	PING HTTPS HTTP	4
	🟢	port4 (Wifi Network)		192.168.104.254/255.255.255.0	Physical Interface	PING HTTPS HTTP	11
	🔴	port5		0.0.0.0/0.0.0.0	Physical Interface		0
	🔴	port6		0.0.0.0/0.0.0.0	Physical Interface		0
	🔴	port7		0.0.0.0/0.0.0.0	Physical Interface		0
	🔴	port8		0.0.0.0/0.0.0.0	Physical Interface		0
	🔴	port9		0.0.0.0/0.0.0.0	Physical Interface		0
	🔴	port10		0.0.0.0/0.0.0.0	Physical Interface		0
	🔴	port11		0.0.0.0/0.0.0.0	Physical Interface		0
	🔴	port12		0.0.0.0/0.0.0.0	Physical Interface		0
	🔴	port13		0.0.0.0/0.0.0.0	Physical Interface		0
	🔴	port14		0.0.0.0/0.0.0.0	Physical Interface		0
	🔴	port15		0.0.0.0/0.0.0.0	Physical Interface		0
	🔴	port16 (DYN-Management)		192.168.200.254/255.255.255.0	Physical Interface	PING HTTPS HTTP	0
📶	🟢	wan1 (Abari Internet)		41.79.138.114/255.255.255.252	Physical Interface	PING HTTPS HTTP FMG-Access	52
📶	🟢	wan2 (Orange Network)		0.0.0.0/0.0.0.0	Physical Interface	PING HTTPS HTTP FMG-Access	1

Fig 15: Segregated Interfaces

The above fig shows different interfaces managing each zone of the network infrastructure.

CHAPTER -IV

IMPLEMENTATION

CHAPTER – IV

4 Implementation

In this research, the proposed system has been implemented with all the corporate security standards which enables the secure network. The following has been implement using the firewall which helps to reduce the downtime and improved security. Using the following standards such as Anti-Virus, Web filtering, content filtering, Application control, IDS/IPS, Secure routing, VPNS for voice and external access, Signal sign on methodologies with secure integration using LDAP (wireless access, VPN access).

4.1 Anti-virus

Edit AntiVirus Profile

Name: default

Comments: Scan files and block viruses. 29/255

Scan Mode: Quick **Full**

Detect Viruses: **Block** Monitor

APT Protection Options

Treat Windows Executables in Email Attachments as Viruses ☒

Use Virus Outbreak Prevention Database ☒

Include Mobile Malware Protection ☒

Fig 16: Anti Virus

The above figure shows the implementation part of the securely configured anti-virus profile as per the industry standard and best practices. From the figure it is clear that it consist of scan mode which is setup for full scan which is resource intensive but a secure way to scan the traffic. The virus detection action is set to block. In additional the profile has functionalities of virus outbreak preventive method along with engines for malware scanning.

4.2 Web Filtering

Web filtering has the following filter profile. The web filter profile helps to allow and block the following category.

1. Local category
2. Potentially Liable
3. Adult / Mature content
4. Bandwidth Consuming
5. Security risk

Edit Web Filter Profile

For standard category, based filter.

Show ☐ All

Local Categories

Potentially Liable

Adult/Mature Content

Bandwidth Consuming

Security Risk

General Interest - Personal

General Interest - Business

Unrated

Static URL Filter

URL Filter ☒

+ Create

Edit

Delete

Search

URL	Type	Action	Status
team	Wildcard	Exempt	Enable
google	Wildcard	Exempt	Enable
gmail	Wildcard	Exempt	Enable

Fig:17 Static URL Filter

42

The Above figure show a effectively configured Web filter profile, the filter / restrictions are category based, each category would be explained in detail below with its sub sections , the Web filter URL filter controls the exceptions for the same for the categories and the URL 's which were blocked by the above web filter profile.

The Legends for the same are as below



Allowed Category / Subsections



Blocked Category / Subsections



Warning would be given to the user, but the Page would go through .

4.3 Potentially Liable

Potential Liable consist of following labels such as child abuse, discrimination, drug abuse, explicit violence, hacking, illegal or unethical, plagiarism and proxy avoidance. In order to achieve the security standard by checking the category listed below. Mostly the potential liability will be in the allowed state which is shown below.

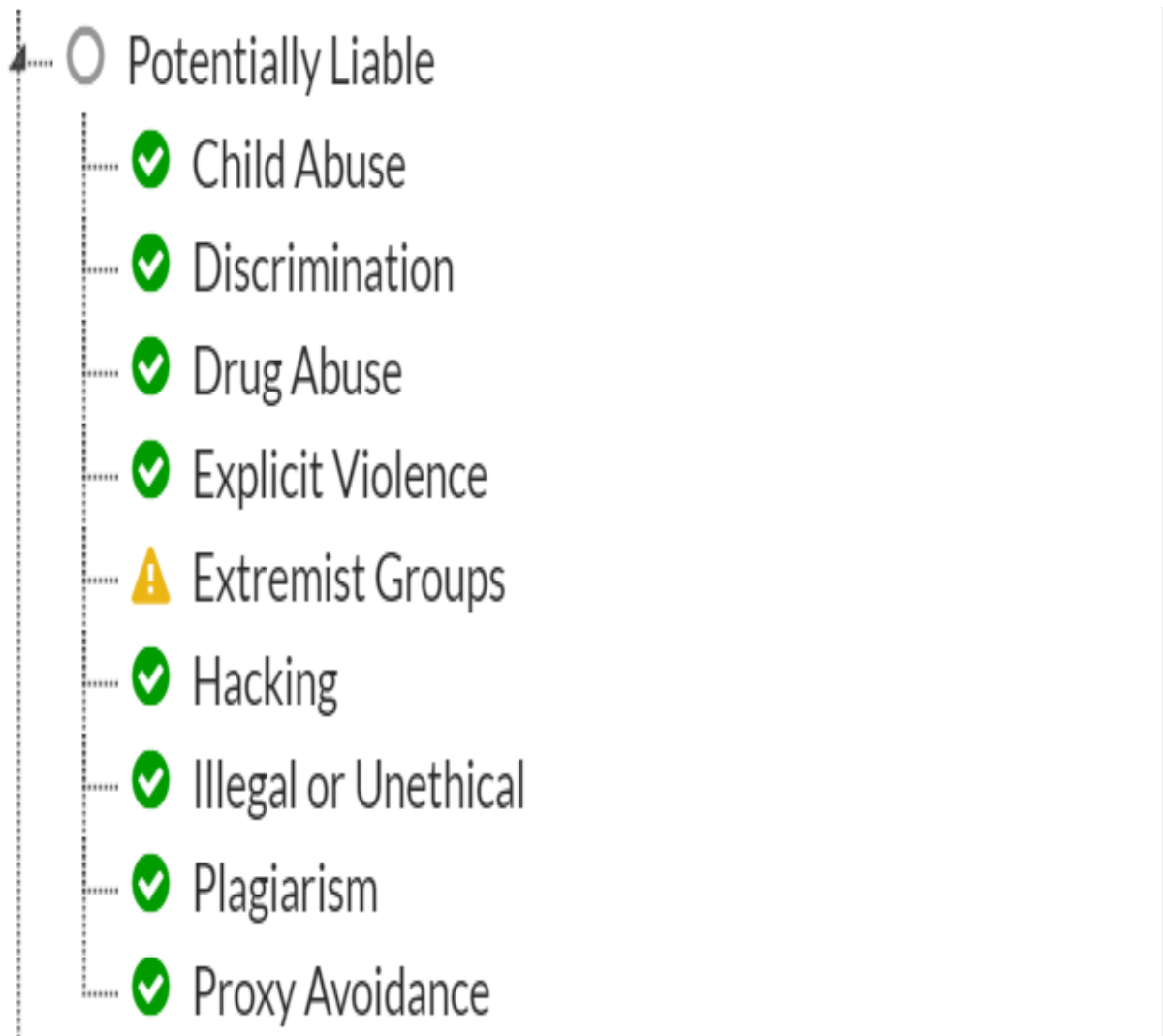


Fig 18: Potentially Liabile Category

4.4 Potential Liabile Category in Blocked State

Potential liable category shown below consist of the block state. In order to avoid the adult and mature content which is more potential source for the bandwidth consumption and vulnerable for the malware attack on the network. Categories such as abortion, alcohol, alternative beliefs, dating, Gambling, lingerie, pornography, tobacco and sex education.



Fig 19: Potential Liable Category in Blocked State

4.5 Bandwidth Consuming

Bandwidth Consuming is one of the key issues in the network, firewall configuration needs to allow and block certain category to improve the use of bandwidth. Block category consist of fire

sharing and storage, Internet Radio and Tv, Internet Telephony, Peer to Peer and streaming media and download. Video streaming usually consume huge amount of bandwidth and reduce the performance of the internet. Blocking such category will help to enhance the internet speed for processing the user request.

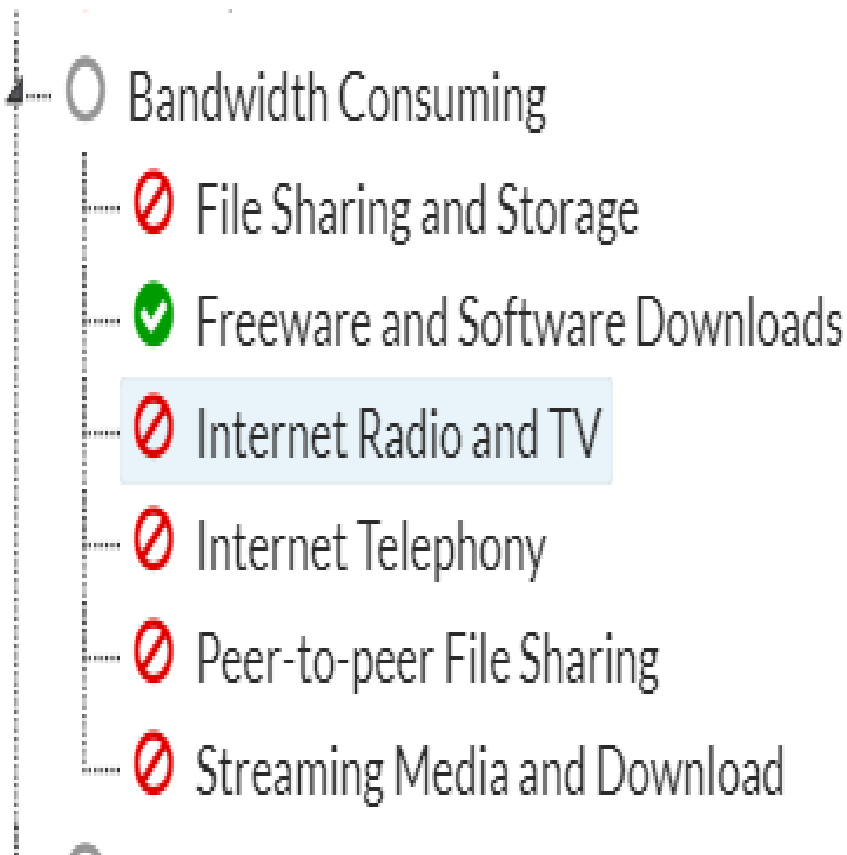


Fig 20: Bandwidth Consuming

4.6 Security Risk Category

Security risk categories are important for the corporate networks where Phishing, spam URLs, Dynamic DNS and Malicious websites. Block these categories reduced the vulnerability and threats to the network. Firewall need to be configured by blocking such category which helps to reduce the potential risk to the network. Security risks are very crucial to the organization which leads to the Zero-day attack.

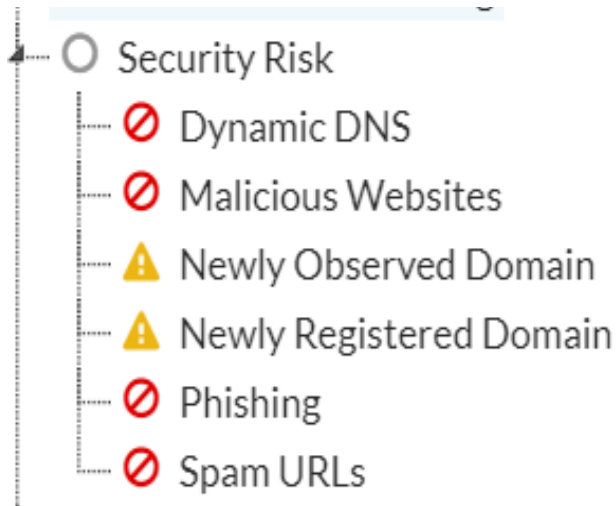


Fig21: Security Risk Category

4.7 General Interest Personal

General interest category consists of advertising, arts and culture, auction, brokerage and trading, child education, content server, digital postcards, domain parking, dynamic content, education, entertainment, folklore and games etc. Mostly in the general interest section all the categories can be opened, and it depend on the corporate requirement and standard specified to enhance the facility.



Fig 22: General Interest and Personal Category

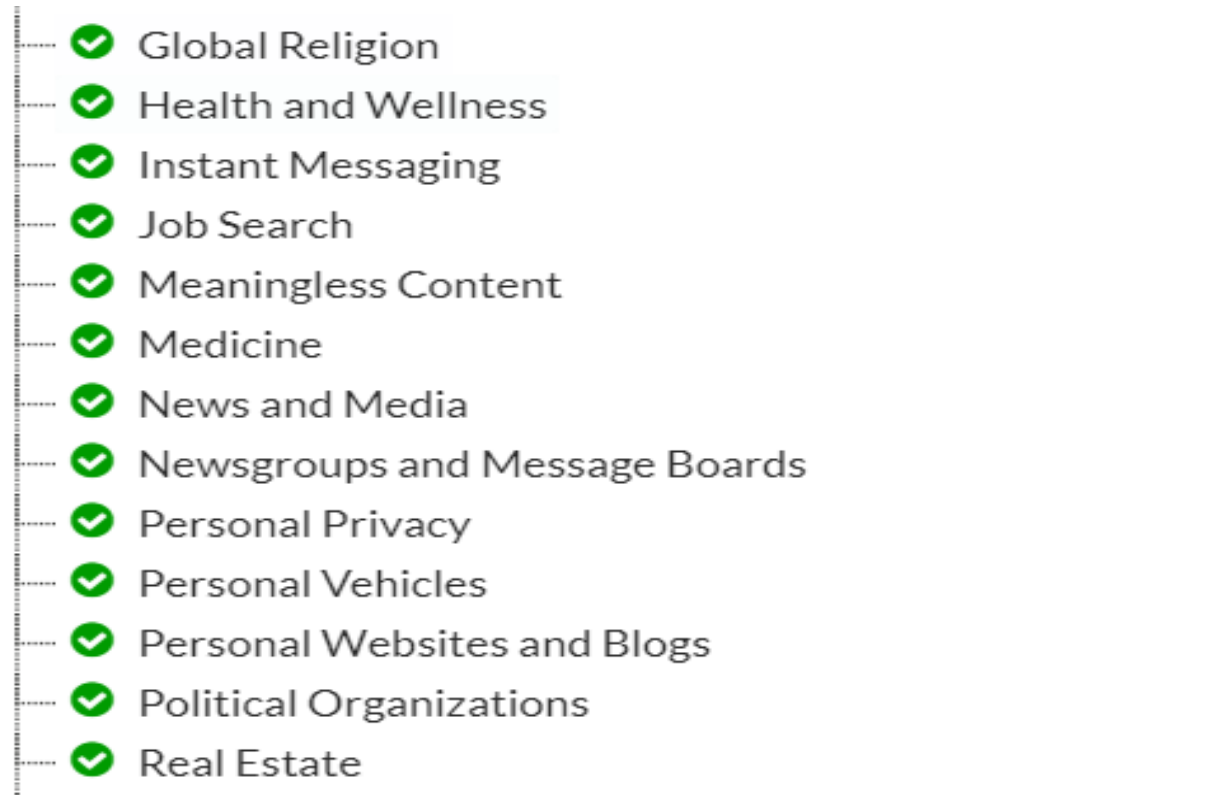


Fig 23: General and Personal Interest in allowed state

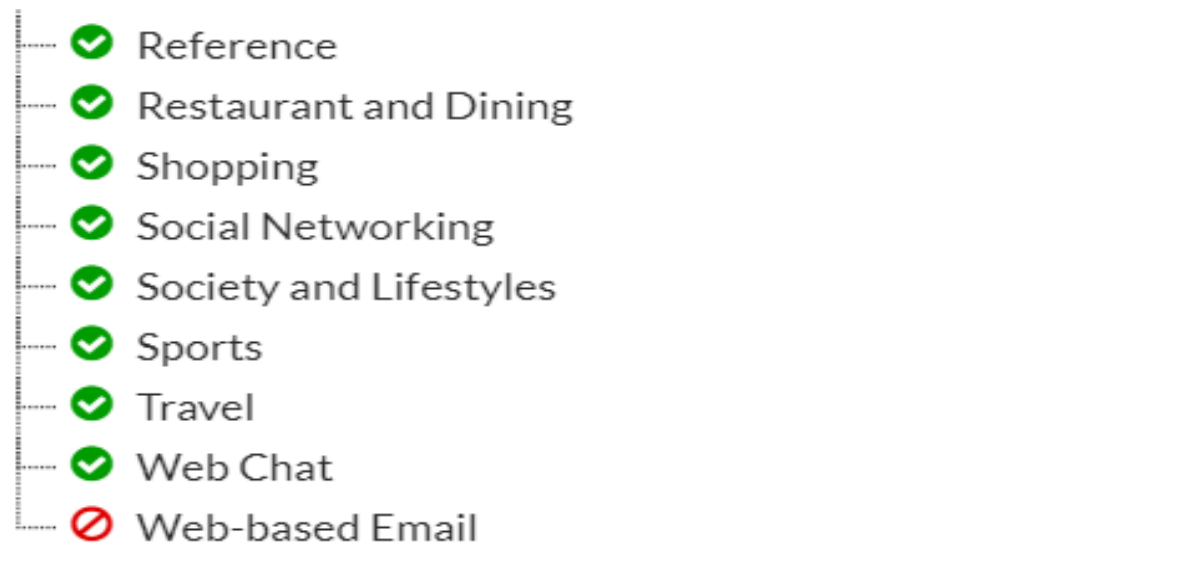


Fig 24 : General Interest with Web-Based Email Blocked state

4. 8 General Interest – Business

-
- ✓ General Interest - Business
 - ✓ Armed Forces
 - ✓ Business
 - ✓ Charitable Organizations
 - ✓ Finance and Banking
 - ✓ General Organizations
 - ✓ Government and Legal Organizations
 - ✓ Information Technology
 - ✓ Information and Computer Security
 - ✓ Online Meeting
 - ✓ Remote Access
 - ✓ Search Engines and Portals
 - ✓ Secure Websites
 - ✓ Web Analytics
 - ✓ Web Hosting
 - ✓ Web-based Applications

Fig 25: General Interest with Business

4.9 DNS filtering

The screenshot shows the 'Edit DNS Filter Profile' interface. At the top right, there is a dropdown menu set to 'default' and icons for adding, deleting, and listing profiles. The main configuration area includes:

- Name:** A text box containing 'default' with a character count of 22/255.
- Comments:** A text box containing 'Default dns filtering.' with a character count of 22/255.
- Redirect botnet C&C requests to Block Portal:** A toggle switch that is turned on (green). A blue tooltip box displays an information icon, the text '51940 domains in botnet package.', and a link to 'botnet package'.
- Enforce 'Safe search' on Google, Bing, YouTube:** A toggle switch that is turned off (grey).
- FortiGuard category based filter:** A section header with a radio button that is selected.
- Static Domain Filter:** A section header.
- Domain Filter:** A toggle switch that is turned off (grey).
- External IP Block Lists:** A toggle switch that is turned off (grey).
- Options:** A section header.
- Redirect Portal IP:** A dropdown menu set to 'Use FortiGuard Default' and a text box containing '208.91.112.55'.
- Allow DNS requests when a rating error occurs:** A toggle switch that is turned on (green).
- Log all DNS queries and responses:** A toggle switch that is turned off (grey).

At the bottom center, there is a green 'Apply' button.

Fig 26: DNS Filtering

4.10 DNS Filter

The above Figure illustrates the DNS filter profile, The DNS filter is effective in blocking the connection even before the connection is made to any site, if the site is safe the DNS query responds, otherwise the Site is blocked, this avoid unnecessary traffic inbound and outbound and

the same time reduces overhead on the firewall CPU and memory for processing sites which need not be contacted as per the IT policy of the organization.

The DNS Filter will have the below security features.

1. Domain block and override filter (exceptions)
2. IP Block list and white list (exceptions)
3. Redirect in the case of event match.
4. Blocks Botnets sites

The figures below provide some examples of BOTNET filters and subcategories which can be added to the profile, it also shares the same database as for the web filtering categories to even make it more safe and secure on the DNS queries being made.

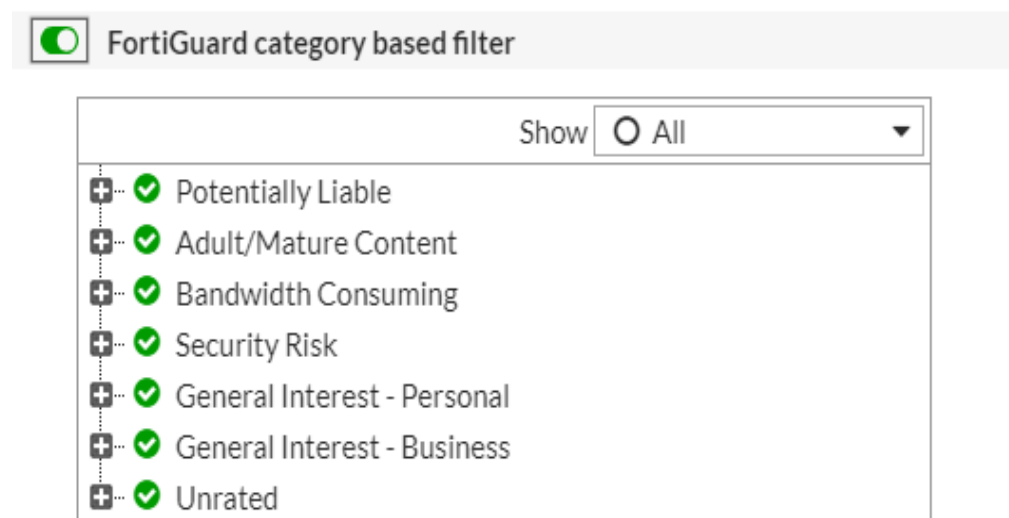


Fig 27: Fortiguard Category based filter

Category based filter consist of the following category such as potential liable, adult/mature content, bandwidth consuming, security risk, general interest such as personal and business and unrated. Each of these categories as lot of sub categories which can be configured to determine for allowing and blocking based on the security standard set by the organization.

Botnet C&C Domain Definitions	
FQDN	Name
ychynt.com	Other
bafcyhorphrblu.co.uk	Other
qwraupljqpho.co.uk	Other
4kqd3hmqgtupi3p.mustspace.us	Other
bdlife.cf	Other
resolvedari.com	Other
tc-avvora38.ru	Other
cpsc.ir	Other
pcdlldfby.cn	Other
wbaskcsxiffax.info	Other
thosewhile.net	Other
ecoshineproducts.com.au	Other
wfb-sms.xyz	Other
beur.co.kr	Other
ubhoadqxgfbkrwft.pw	Other
kewu.cfpwealthcpp.net	Other
paypal.verif-purchase-id-020318-160515.com	Other
wels-fargo.com.connect.wf-south.info	Other
247f244d.eu	Other
xleieldgatew.co.uk	Other
ciwcmzukurcixirgugkvkfjirp.biz	Other
p27dokhpz2n7nvgr.1dyzdh.top	Other
qfjhpgbefuhenjp7.1225wj.top	Other
amazon.de.fast-click05.com	Other
ecoqwegst.com	Other
ruih.co.uk	Other
aabumeyang.ml	Other
eiwkamrcushdijnzhhlfeib.info	Other
suegovariancancerace.com	Other
egitimcsitesi.com	Other
kleinaberoho.info	Other
maunzkerocuba.usa.cc	Other

Fig:28 (i) Botnet C&C Category

Botnet C&C Domain Definitions	
FQDN ↕	Name ↕
gbahhshfhe.tk	Other
rkinmndmlbzlxjveycaftxghr.org	Other
9rbk.com	Other
info1700234110700i.000webhostapp.com	Other
myappleid-cancel-order.com	Other
djwsktv/myvfo.me	Other
distanations.cn	Other
xzhacixculrmjtramaxov.info	Other
bangnice.co	Other
smaoewewe.club	Other
cuenta-verificacion.com	Other
bigg-live.com	Other
cryaaunqklsf.co.uk	Other
itau-looking.oni.cc	Other
princetontw.com	Other
debbiewhitmire.com	Other
egdrtdloyuti.co.uk	Other
vmcsihamocoqym.co.uk	Other
bledes.tk	Other
amstudiola.com	Other
student-survival-guide.co.uk	Other
ftciccbhief.co.uk	Other
euhkjbqgskmack.co.uk	Other
52uo5k3t73ypijje.xab7m0.top	Other
icloudsupportv.com	Other
loymjk0z-site.btempurl.com	Other
appleid-confirmation-appstore-purchase.com	Other
crnlorbdiiculr.co.uk	Other
fgysmnvl.cm	Other
4kqd3hmqgtupi3py12acl.bid	Other
diagnosticautomobile.fr	Other

Fig:28 (ii) Botnet C&C Category

Botnet C&C Domain Definitions	
FQDN ↕	Name ↕
dmcyqklfwcqkjveuxsfagtytam.org	Other
djjaxvor.com	Other
sslexchcert.com	Other
mobilhalksubem-tr.com	Other
account-validation.services	Other
arulhnfkcspxlccuqt.cm	Other
fubizhydztpttgedbmuglzhdy.biz	Other
mobiactif.es	Other
mobileyoga.mobi	Other
idrissukses.com	Other
yourgone.net	Other
ywdgkhl.info	Other
ijmbplinfexogedewkgavsnhy.biz	Other
cmccwlan.cn	Other
information-required.ml	Other
puzybep.com	Other
xxmnowknmdcv.pw	Other
lvauaqxfqirblruhmtuwsgem.org	Other
www.elisaart.it	Other
souzaaguiar.bid	Other
mhstolmmq.com	Other
viswavsp.com	Other
pubertilodersx.com	Other
prlnzdyxlznuoswugax.biz	Other
jstaikos.com	Other
neliti.bid	Other
gazariaaloron24.com	Other
cocktail-dress.club	Other
gadget-fanka.gq	Other
uoemautzgyydvopzltzpbcy.biz	Other
aeysop.com	Other

Fig:29 Botnet - Filtering service for account validation

Botnet C&C Domain Definitions	
FQDN	Name
dc-479b9c32c623.senoratest.cf	Other
rkwpooz.ws	Other
tlfmmymrmkbvo.co.uk	Other
menboeqhyrpvomq.0nyi6l.bid	Other
fixurprob03.xyz	Other
adobe496.000webhostapp.com	Other
sambalpuernursingcollege.org	Other
cewmhbidcemsexkc.in	Other
shripujansamagri.com	Other
unocl45trpuoefft.hyr1h3.bid	Other
notificationyourspace.cf	Other
suitupinc.com	Other
node82.btc-giveaway.info	Other
ayycxoxzstv.cn	Other
thewebhostingforum.com	Other
salimahcikupaols.id	Other
aceckwe.com	Other
rajwahaifamelema57.com	Other
gmvotoqax.pw	Other
zebxhuvsz.com	Other
adysobscfkbmvdhquoeyauxrcci.biz	Other
oe2cku7pebkpgeko.ttx0ig.top	Other
easyweb.tdcanadatrust.yousufrehman.com	Other
cenea-solaire.com	Other
inemm.cn	Other
fbmbioxrqvrcta.co.uk	Other
zippyamritsar.com	Other
mtqgcaqkpfmoveqxoffyfqscom.biz	Other
pengaluru.rent	Other
xilogrid.info	Other
icteuucvmivk.co.uk	Other

Fig:30 (i) Botnet Category

Botnet C&C Domain Definitions	
FQDN	Name
apple.itunesconnect.su	Other
appadspage.000webhostapp.com	Other
thczb.com	Other
rspvtocuzhgepntwnrswushvnrh.biz	Other
01cn.net	Other
moveintrade.com	Other
saratp.cf	Other
fkviewkavnfucagvw.pw	Other
gamingserversplus.life	Other
ymzytwgscvsmbrsxpndft.info	Other
santoantonio.portalrz.com.br	Other
pujowevo.info	Other
verificationticket.com	Other
dream55.xyz	Other
dydadp.cn	Other
latabu.ru	Other
vijayawada.biz	Other
olditis.com	Other
flertiptctdxr.co.uk	Other
xbbyextarb.info	Other
nutqauytva6213xyzf112zzz1.com	Other
citi.uverify.info	Other
capitadw.beget.tech	Other
dcfds-reason-tagum.000webhostapp.com	Other
jxw9qa3g.site	Other
hdpejeavjqm.ws	Other
asxjdp.top	Other
suntrustealrts.esy.es	Other
sarahbillheimerphotography.com	Other
nimtздеsigngroup.com	Other
saferfreedom.tk	Other

Fig: 30(ii) Botnet Category

Botnet C&C Domain Definitions	
▼ FQDN ▼	▼ Name ▼
oneillandsasso.com	Other
mnconsultants.co.tz	Other
topstockexpert.su	Other
qiinjvsf.in	Other
dnzeygmfmclgaldqojmbyorzp.org	Other
sylvacom.sml	Other
tc-ziraattbank.com	Other
cbacpartnership.org	Other
byraft.com	Other
fwuwjvqcauytebqdsojhaugpv.org	Other
sasapparel.com.au	Other
verifi74.register-aacunt21.gq	Other
refusoslou.xyz	Other
www.emitraco.com	Other
1bce05f50968121b11c98acfa7d56326.xyz	Other
inxduaimrqsyzdizbicazx.org	Other
misegundocuadro.com	Other
poemsan.info	Other
yugskcbbpxpl.pw	Other
1fq1rt4yuk04u2hwj021fu9ctu.com	Other
lykef.eu	Other
y822.com	Other
mobileif-atualiza.ml	Other
a0197915.xsph.ru	Other
integra-pharm.com	Other
qvbusbftayqcmbrmj.com	Other
pusltzlvwztrrohxxd.org	Other
85kq.com	Other
vividerenaz.com	Other
online-service-tax-return-arc.krunts.ml	Other
mygood.xyz	Other
uwtznzluilfcstmbrclnb.org	Other

Fig: 30 (iii) Botnet Category

Botnet C&C Domain Definitions	
▼ FQDN ⇅	▼ Name ⇅
xhjcptnobdtxm.co.uk	Other
ivknqssxlwjxfv.cm	Other
52uo5k3t73ypjije.ep493u.top	Other
radioonline.com	Other
inspireconsulting.ro	Other
ctadamsauthor.com	Other
dklyhdhlgobgt.co.uk	Other
tolexinesansordonnance.space	Other
mitraworm.com	Other
compowood.ru	Other
julijuli.cf	Other
dcxrqmsjwu.pw	Other
wrqjftsnyory.co.uk	Other
dkpdesigns.com	Other
niveahie.beget.tech	Other
hiyadocs.ml	Other
nrleccxwwzxh.pw	Other
agrocooperation.ru	Other
aewghfehhhiucpsduhqox.biz	Other
www.rencontreparis.org	Other
paypal.aanmelden-validerungs.tk	Other
secureweb1ppl-directmanagepaypal.m-s-c-p-pgroup.com	Other
myetherwallet-coins.space	Other
fiiqyksoeegxovi.in	Other
czlagdkpt.cn	Other
cqtuklbpwngmgilxheyporcy.org	Other
p27dokhpz2n7nvgr.1kq4l8.top	Other
centreuniversitairezenith.com	Other
doublewq.com	Other
edulineeright.download	Other
ywpspgykihvgph.co.uk	Other

Fig: 30 (iv) Botnet Category

:

Botnet C&C Domain Definitions	
FQDN	Name
w7s8v1904d.ru	Other
bigbazzarbd.com	Other
com-help-contact-100000643251657.com	Other
knwhos.ir	Other
kreoyrhpqwhjdw.co.uk	Other
rypemcidpnmjdszhxwfazx.info	Other
configuration.youthempire.com	Other
recoveryacct99002108.000webhostapp.com	Other
securityaccountcentre11042018.000webhostapp.com	Other
hhyqxojcbmxj.pw	Other
kaabkonnnect.com	Other
yxltedydgqjqrconzhtgro.info	Other
paypal.kunden-200x160-verifizierung.com	Other
staging.schoolsleuth.org	Other
kjkasdjaksdasdbe.com	Other
gjlhctmthxqcaggam.pw	Other
eyyfodmkiplv.co.uk	Other
klimark.com.pl	Other
com-customer-service.info	Other
uhzgtmjan6avtcvkrhu.littlematchagirl.com.au	Other
granthost10.icu	Other
ydfgdbwrwgpm.co.uk	Other
orderjwell.eu	Other
crush5media.com	Other
svandecka.com	Other
mnyehvjcn.ws	Other
jpfdtmbvuygyvyrebxxy.info	Other
52uo5k3t73ypjije.ovpgod.top	Other
dkwm.suwan.co.id	Other
jiqduciucqggallieq.com	Other
paypal.com.ma.cgi.bin.webscr.cmd.flow.session.ok-dul.com	Other

Fig: 30 (v) Botnet Category

:

Botnet C&C Domain Definitions	
FQDN	Name
lotihecter.com	Other
suuporrt53.confrim-fanpage111.cf	Other
rmhospitalcalicut.com	Other
guruhomeopathy.com	Other
soxkyvktatgpcqv.com	Other
ubhjipilbb.ws	Other
dqnrljrwcixqsvsqdahhmvxoin.org	Other
gregorian.club	Other
disablepage2017.cf	Other
matjournal.com	Other
pvgaroc.org.tw	Other
cykjmnbvtibx.co.uk	Other
gadpbajzplqfmwhlzaqyxb.org	Other
xiazailou.co	Other
saldodeofertas.tk	Other
halkbankasiceponlinesube.com	Other
bockrc.ws	Other
lrkjllyllajrlotzrscadeealkv.org	Other
amskrupajal.org	Other
soudagarminerals.com	Other
bl7.000webhostapp.com	Other
windirectodaserra.co.uk	Other
djlrvukfmjnnqxy.tw	Other
lzbxgjrplvcupfqslduzrg.biz	Other
zoygroup.com	Other
pechodin.com	Other
paypal.login.myaccount.secure.myaccloginsecid.com	Other
zinrop.com	Other
suknsokhuwduvruo.info	Other
pvcgymbeljvtttdtmxbl.info	Other
contratosdemarkting.com	Other
rusmond.com	Other

Fig:30 (vi) Botnet Category

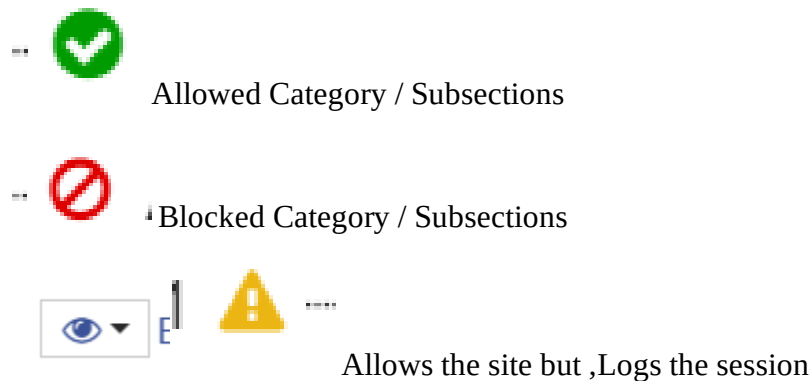
Botnet C&C Domain Definitions	
FQDN	Name
sdtjeqtbstix.co.uk	Other
hmajxlyb.net	Other
pmenboeqhyrpvomq.xneyvm.top	Other
nextime.top	Other
rsgarmentsinc.com	Other
safety.microsoft.com.www.wnxzl.ddsmdslxz7yw.trade	Other
aldaypill.com	Other
ajpylvvgvdrcbl.co.uk	Other
news-medias.ru	Other
vrympoqs5ra34nfo.torhelper.pl	Other
7aisngyh91e-cpsess0671158385-id.tallercastillocr.com	Other
teamok.000webhostapp.com	Other
gudanglagu4shared.website	Other
ejmhoeufrkkoj.co.uk	Other
vbxdugdsrkrir.co.uk	Other
leadnever.net	Other
concerncibc.com	Other
icf-fx.kz	Other
autoconexion.com	Other
fcngqff.ws	Other
7hjlw.xyz	Other
lamerpamer.org	Other
leadskit.ru	Other
santanetibeempresarial.com	Other
wfbank.trade	Other
usrfxecthkwolwtuvgv.pw	Other
bcocivgolhw.cn	Other
njbqlifyfatdewsqgdpzuovc.biz	Other
com-verifyaccountupdateappstore.info	Other
supermercadosbandeirante.com.br	Other
secure.apple.appleid.info.momcpum.com.my	Other

Fig: 30 (vii) Botnet Category

4.11 Application control with overrides

The Below figure show a effectively configured Application control profile, the filter / restrictions are category based, each category would be explained in detail below with its sub sections , the application control overrides controls the exceptions for the same for the categories and the categories which were blocked by the below application control profile.

The Legends for the same are as below



Edit Application Sensor Staff-LAN-DYN

▼ All Categories

Business (140, ☁ 6)	Cloud.IT (45)	Collaboration (252, ☁ 10)
Email (78, ☁ 12)	Game (84)	General.Interest (224, ☁ 7)
Mobile (3)	Network.Service (329)	P2P (59)
Proxy (166)	Remote.Access (82)	Social.Media (118, ☁ 31)
Storage.Backup (162, ☁ 17)	Update (49)	Video/Audio (150, ☁ 14)
VoIP (24)	Web.Client (23)	Unknown Applications

Application Overrides

[+ Add Signatures](#) [Edit Parameters](#) [Delete](#)

Application Signature	Category	Action
Kaspersky.Update	Update	Monitor ▼
MS.Windows.Update	Update	Monitor ▼
RDP	Remote.Access	Monitor ▼
RDP.over.HTTPS	Remote.Access	Monitor ▼

Fig: 31 Edit Application server

Below are some detailed examples of each category , which were used to strengthen the security , each subcategory is being displayed in detail for reference along with their risk ratings

☐ Select All

☒ Category: Business

☒ All
 Cloud
 Selected: 0 / 208

Name	Category	Technology	Popularity	Risk
Hubspot	Business	Browser-Based, Client-Server	★★★★★	
IBM.DB2	Business	Client-Server	★★★★☆	
Insightly	Business	Browser-Based	★★★★☆	
Insightly_File.Download	Business	Browser-Based	★★★★☆	
Insightly_File.Upload	Business	Browser-Based	★★★★☆	
Jobvite	Business	Browser-Based	★★★★☆	
JotForm	Business	Browser-Based, Client-Server	★★★★☆	
Kanban.Tool	Business	Browser-Based	★★★★☆	
Kaseya	Business	Client-Server	★★★★☆	
Load.Impact	Business	Browser-Based, Client-Server	★★★★☆	
LucidChart	Business	Browser-Based	★★★★☆	
Magento	Business	Browser-Based	★★★★☆	
Market-Q	Business	Browser-Based	★★★★☆	
Mavenlink	Business	Browser-Based	★★★★☆	
Mavenlink_Post	Business	Browser-Based	★★★★☆	
MaxDB	Business	Client-Server	★★★★☆	
Maximizer.CRM	Business	Browser-Based	★★★★☆	
Memcached	Business	Client-Server	★★★★☆	
Micros	Business	Client-Server	★★★★☆	
Microsoft.Office.Macro.Embedded.Document	Business	Browser-Based	★★★★★	
MongoDB	Business	Client-Server	★★★★☆	
Moodle	Business	Browser-Based	★★★★★	

Fig:32 (i) Application control – Business category

☐ Select All ☒ Category: Business Add Filter ✕ All Cloud Selected: 0 / 20				
Name ▲	Category ▲	Technology ▲	Popularity ▲	Risk ▲
Acronis.Snap.Deploy	Business	Client-Server	★★★★☆	
Act!	Business	Browser-Based	★★★★☆	
ActiveCampaign	Business	Browser-Based	★★★★☆	
ActiveCampaign_File.Upload	Business	Browser-Based	★★★★☆	
ADP	Business	Browser-Based	★★★★☆	
AirWatch.MDM	Business	Client-Server	★★★★☆	
Alibaba	Business	Browser-Based	★★★★☆	
Apache.Cassandra	Business	Client-Server	★★★★☆	
Applane.CRM	Business	Client-Server	★★★★☆	
Atlassian.JIRA	Business	Browser-Based	★★★★☆	
AutoDesk.360	Business	Browser-Based	★★★★☆	
AutoDesk.360.Upload	Business	Browser-Based	★★★★☆	
Autodesk.Buzzsaw	Business	Browser-Based, Client-Server	★★★★☆	
Baidu.PC.Faster	Business	Client-Server	★★★★☆	
BambooHR	Business	Browser-Based	★★★★☆	
BambooHR_File.Download	Business	Browser-Based	★★★★☆	
BambooHR_File.Upload	Business	Browser-Based	★★★★☆	
Base.CRM	Business	Browser-Based, Client-Server	★★★★☆	
Blinksale	Business	Browser-Based	★★★★☆	
Brightpearl	Business	Browser-Based	★★★★☆	
Bugzilla	Business	Browser-Based	★★★★☆	
Censhare	Business	Client-Server	★★★★☆	

Fig:32 (ii) Application control – Business category

Select All

Category: Business

Add Filter

All

Cloud

Selected: 0 / 208

Name	Category	Technology	Popularity	Risk
 Scotty	Business	Browser-Based	★★★★☆	
 ServiceDesk.Plus	Business	Browser-Based	★★★★☆	
 Shopify	Business	Browser-Based	★★★★★	
 Sicoobnet	Business	Client-Server	★★★★☆	
 SignNow	Business	Browser-Based	★★★★☆	
 Silent.Circle	Business	Client-Server	★★★★☆	
 Sprout.Social	Business	Browser-Based	★★★★☆	
 SQL.Navigator	Business	Client-Server	★★★★☆	
 Student.Planner	Business	Client-Server	★★★★☆	
 Sugar.CRM	Business	Browser-Based	★★★★☆	
 Sybase	Business	Client-Server	★★★★☆	
 Tableau	Business	Client-Server	★★★★☆	
 Tencent.Beacon	Business	Client-Server	★★★★★	
 Time.Warner.Cable	Business	Browser-Based	★★★★☆	
 Tonghuashun	Business	Client-Server	★★★★☆	
 TrendMicro.Earthagent	Business	Client-Server	★★★★☆	
 Uber	Business	Client-Server	★★★★★	
 Univision_Financial.Info	Business	Browser-Based	★★★★☆	
 UserVoice	Business	Browser-Based	★★★★★	
 UserVoice_File.Download	Business	Browser-Based	★★★★☆	
 UserVoice_File.Upload	Business	Browser-Based	★★★★☆	
 vend	Business	Client-Server	★★★★☆	

Fig: 32 (iii) Application control – Business category

4.12 Application control – Cloud IT category

This category controls the flow of application in the internet link. The below figure shows the various categories using this standard for Cloud IT category.

☐ Select All	☒ Category: Cloud.IT	Add Filter	☒ All Cloud	Selected: 0/2
Name	Category	Technology	Popularity	Risk
 Amazon.Alexa	Cloud.IT	Client-Server	★★★★★	
 Amazon.AWS	Cloud.IT	Browser-Based	★★★★★	
 Amazon.AWS_EC2	Cloud.IT	Browser-Based	★★★★★	
 Amazon.AWS_S3	Cloud.IT	Browser-Based	★★★★★	
 Amazon.AWS_S3.Download	Cloud.IT	Browser-Based	★★★★★	
 Amazon.AWS_S3.Upload	Cloud.IT	Browser-Based	★★★★★	
 Amazon.CloudFront	Cloud.IT	Browser-Based	★★★★★	
 Any.Do	Cloud.IT	Client-Server	★★★★☆	
 AppScale	Cloud.IT	Client-Server	★★★☆☆	
 Arvix	Cloud.IT	Browser-Based, Client-Server	★★★★☆	
 AT&T.Synaptic	Cloud.IT	Browser-Based	★★★★★	
 Cloudify.Co	Cloud.IT	Browser-Based	★★★☆☆	
 Cloudmark	Cloud.IT	Client-Server	★★★☆☆	
 Cradlepoint.Netcloud	Cloud.IT	Client-Server	★★★☆☆	
 Engine.Yard.Cloud	Cloud.IT	Browser-Based	★★★☆☆	
 Fortiguard.Search	Cloud.IT	Browser-Based	★★★★★	
 Godaddy	Cloud.IT	Browser-Based	★★★★★	
 Google.Cloud.Platform	Cloud.IT	Browser-Based	★★★☆☆	
 Google.Cloud.Platform_App.Engine	Cloud.IT	Browser-Based	★★★☆☆	
 Google.Cloud.Platform_BigQuery	Cloud.IT	Browser-Based	★★★☆☆	
 Google.Cloud.Platform_Bigtable	Cloud.IT	Browser-Based	★★★☆☆	
 Google.Cloud.Platform_Cloud.Launcher	Cloud.IT	Browser-Based	★★★☆☆	

Fig: 33(i) Application control – Cloud IT category

 Google.Cloud.Platform_Container.Engine	Cloud.IT	Browser-Based	★★★★☆	
 Google.Cloud.Platform_Dataflow	Cloud.IT	Browser-Based	★★★★☆	
 Google.Cloud.Platform_Dataproc	Cloud.IT	Browser-Based	★★★★☆	
 Google.Cloud.Platform_Datastore	Cloud.IT	Browser-Based	★★★★☆	
 Google.Cloud.Platform_Endpoints	Cloud.IT	Browser-Based	★★★★☆	
 Google.Cloud.Platform_Genomics	Cloud.IT	Browser-Based	★★★★☆	
 Google.Cloud.Platform_Networking	Cloud.IT	Browser-Based	★★★★☆	
 Google.Cloud.Platform_Pub.Sub	Cloud.IT	Browser-Based	★★★★☆	
 Google.Cloud.Platform_Shell	Cloud.IT	Browser-Based	★★★★☆	
 Google.Cloud.Platform_SQL	Cloud.IT	Browser-Based	★★★★☆	
 Google.Cloud.Platform_Storage	Cloud.IT	Browser-Based	★★★★☆	
 Google.Cloud.Print	Cloud.IT	Browser-Based	★★★★☆	
 Google.Stackdriver	Cloud.IT	Browser-Based	★★★★☆	
 Meraki.Cloud.Controller	Cloud.IT	Client-Server	★★★★☆	
 Microsoft.Azure	Cloud.IT	Browser-Based, Client-Server	★★★★☆	
 Mimecast	Cloud.IT	Client-Server	★★★★☆	
 Panda.Antivirus	Cloud.IT	Client-Server	★★★★☆	
 Razor	Cloud.IT	Client-Server	★★★★☆	
 TrendMicro.OfficeScan	Cloud.IT	Client-Server	★★★☆☆	
 TrendMicro.WFBS	Cloud.IT	Client-Server	★★★★★	
 Twilio	Cloud.IT	Browser-Based	★★★★☆	
 webMethods.AgileApps.Cloud	Cloud.IT	Browser-Based	★★★★☆	

Fig: 33 (ii) Application control – Cloud IT category

4.13 Application control – Collaboration category

This category controls the flow of application in the internet link. The below figure shows the various categories using this standard for Collaboration category.

☐ Select All	☒ Category: Collaboration	Add Filter	☒ All Cloud	Selected: 0 / 208
Name ▲	Category ▼	Technology ▼	Popularity ▼	Risk ▼
Adobe.Connect	Collaboration	Browser-Based	★★★★☆	
Adobe.Connect_Meeting.Chat	Collaboration	Browser-Based, Client-Server	★★★★☆	
Adobe.Connect_Meeting.Share.Document.Upload	Collaboration	Browser-Based	★★★★☆	
Adobe.Connect_Meeting.Share.My.Screen	Collaboration	Browser-Based	★★★★☆	
Adobe.Connect_Meeting.Share.Whiteboard	Collaboration	Browser-Based	★★★☆☆	
Adobe.Online.Office	Collaboration	Browser-Based	★★★★☆	
AIM	Collaboration	Client-Server	★★★★★	
AnyMeeting	Collaboration	Browser-Based, Client-Server	★★★★☆	
Apple.Messages	Collaboration	Client-Server	★★★★★	
Atlassian.Confluence	Collaboration	Browser-Based	★★★★☆	
Baidu.Hi	Collaboration	Client-Server	★★★★☆	
Baidu.Hi_Audio.Video.Chat	Collaboration	Client-Server	★★★☆☆	
Baidu.Hi_File.Transfer	Collaboration	Client-Server	★★★☆☆	
Beamyourscreen	Collaboration	Browser-Based	★★★★☆	
Blackboard.Collaborate	Collaboration	Browser-Based	★★★★☆	
Bloomfire	Collaboration	Browser-Based	★★★★☆	
Bluejeans	Collaboration	Browser-Based	★★★★☆	
Camfrog	Collaboration	Client-Server	★★★★☆	
CGI.IRC	Collaboration	Browser-Based	★★★☆☆	
Chatango	Collaboration	Browser-Based	★★★★★	
Chikka	Collaboration	Client-Server	★★★★☆	
Cisco.Spark	Collaboration	Browser-Based, Client-Server	★★★★☆	

Fig :34 (i) Application control – Collaboration category

 CVS	Collaboration	Client-Server	★★★★☆	
 Digsby	Collaboration	Client-Server	★★★★☆	
 Discord	Collaboration	Browser-Based, Client-Server	★★★★☆	
 Disqus	Collaboration	Browser-Based	★★★★★	
 Docker	Collaboration	Client-Server	★★★★☆	
 Docker_Pull.Blob	Collaboration	Client-Server	★★★★☆	
 Docker_Pull.Manifest	Collaboration	Client-Server	★★★★☆	
 Docker_Push.Blob	Collaboration	Client-Server	★★★★☆	
 Docker_Push.Manifest	Collaboration	Client-Server	★★★★☆	
 DreamBox	Collaboration	Browser-Based	★★★★☆	
 Drupal	Collaboration	Browser-Based	★★★☆☆	
 Facebook_Messenger.Image.Transfer	Collaboration	Client-Server	★★★★☆	
 Facebook_Messenger.Video.Transfer	Collaboration	Client-Server	★★★★☆	
 Facebook_Messenger.Voice.Message	Collaboration	Client-Server	★★★★☆	
 Facebook_Messenger.VoIP.Call	Collaboration	Client-Server	★★★★☆	
 FC2	Collaboration	Browser-Based	★★★★★	
 Fetion	Collaboration	Client-Server	★★★★☆	
 FireChat	Collaboration	Client-Server, Peer-to-Peer	★★★☆☆	
 First.Class	Collaboration	Client-Server	★★★★☆	
 Fring	Collaboration	Browser-Based	★★★★☆	
 Fronter	Collaboration	Browser-Based	★★★★☆	
 Fuze.Meeting	Collaboration	Browser-Based	★★★★☆	

Fig :34 (ii) Application control – Collaboration category

4.14 Application control – Email category

This category controls the flow of application in the internet link. The below figure shows the various categories using this standard for email category.

☐ Select All

☒ Category: Email

☒ All
 Cloud
 Selected: 0 / 208

Name	Category	Technology	Popularity	Risk
1und1.Mail	Email	Browser-Based	★★★★☆	
126.Mail	Email	Browser-Based	★★★★☆	
AIM.Webmail	Email	Browser-Based	★★★★☆	
AIM.Webmail_Attachment	Email	Browser-Based	★★★☆☆	
Comcast.Webmail	Email	Browser-Based	★★★☆☆	
Cox.Webmail	Email	Browser-Based	★★★★☆	
Daum.Mail	Email	Browser-Based	★★★★☆	
Daum.Mail_Attachment	Email	Browser-Based	★★★☆☆	
Daum.Mail_Send	Email	Browser-Based	★★★★☆	
FastMail	Email	Browser-Based	★★★★☆	
Gmail	Email	Browser-Based	★★★★★	
Gmail_Attachment	Email	Browser-Based	★★★★☆	
Gmail_Attachment.Download	Email	Browser-Based	★★★☆☆	
Gmail_Attachment.Upload	Email	Browser-Based	★★★☆☆	
Gmail_Chat	Email	Browser-Based	★★★★☆	
Gmail_G.Suite	Email	Browser-Based	★★★★☆	
Gmail_Personal	Email	Browser-Based	★★★★★	
Gmail_Send.Message	Email	Browser-Based	★★★★★	
GMTP	Email	Network-Protocol	★★★☆☆	
GMX.Webmail	Email	Browser-Based	★★★☆☆	
Horde.Webmail	Email	Browser-Based	★★★★☆	
Hushmail	Email	Browser-Based	★★★★☆	

Fig :35 (i) Application control – Email category

Name 	Category 	Technology 	Popularity 	Risk 
 Livedoor.Webmail	Email	Browser-Based	★★★★☆	
 Mail.Ru	Email	Browser-Based	★★★★★	
 Mail.Ru_Mail	Email	Browser-Based	★★★★☆	
 Mailchimp	Email	Browser-Based	★★★★★	
 Mailchimp_File.Upload	Email	Browser-Based	★★★★☆	
 Mailjet	Email	Browser-Based	★★★★☆	
 Microsoft.Exchange.Server	Email	Client-Server	★★★★★	
 Microsoft.Outlook	Email	Browser-Based	★★★★★	
 Microsoft.Outlook.Office.365	Email	Browser-Based	★★★★★	
 Microsoft.Outlook.Web.App	Email	Browser-Based	★★★★★	
 Microsoft.Outlook_Attachment	Email	Browser-Based	★★★★☆	
 Microsoft.Outlook_Attachment.Download	Email	Browser-Based	★★★★☆	
 Microsoft.Outlook_Attachment.Upload	Email	Browser-Based	★★★★☆	
 Microsoft.Outlook_Read.Message	Email	Browser-Based	★★★★☆	
 Microsoft.Outlook_Send.Message	Email	Browser-Based	★★★★☆	
 Nate.Mail	Email	Browser-Based	★★★★☆	
 Nate.Mail_Attachment.Download	Email	Browser-Based	★★★★☆	
 Nate.Mail_Attachment.Upload	Email	Browser-Based	★★★★☆	
 Nate.Mail_Send	Email	Browser-Based	★★★★☆	
 Naver.Mail	Email	Browser-Based	★★★★☆	
 Naver.Mail_Attachment	Email	Browser-Based	★★★★☆	
 Naver.Mail_Send	Email	Browser-Based	★★★★☆	

Fig: 35 (ii) Application control – Email category

4.15 Application control – Game category

This category controls the flow of application in the internet link. The below figure shows the various categories using this standard for game category.

☐ Select All ☒ Category: Game Add Filter ✕ All Cloud Selected: 0 / 20				
Name	Category	Technology	Popularity	Risk
Addicting.Games	Game	Browser-Based	★★★★☆	
Aion	Game	Client-Server	★★★★☆	
Anipop	Game	Client-Server	★★★★★	
Apple.Game.Center	Game	Client-Server	★★★★★	
Armagetron	Game	Client-Server	★★☆☆☆	
Armor.Games	Game	Browser-Based	★★★★☆	
Battle.Net	Game	Browser-Based	★★★★★	
Chinagames	Game	Client-Server	★★☆☆☆	
Clash.Of.Clans	Game	Client-Server	★★★★★	
Combat.Arms	Game	Client-Server	★★☆☆☆	
Craz3.Match	Game	Client-Server	★★★★★	
DC.Universe.Online	Game	Client-Server	★★★★☆	
DOFUS	Game	Client-Server	★★☆☆☆	
Draw.Free	Game	Client-Server	★★★★☆	
Dungeon.And.Fighter	Game	Client-Server	★★★★☆	
EA.FIFA	Game	Browser-Based	★★★★☆	
Epic.Games	Game	Client-Server	★★★★☆	
Evony	Game	Browser-Based	★★☆☆☆	
FarmVille	Game	Browser-Based	★★★★☆	
Fortnite	Game	Client-Server	★★★★★	
Garena	Game	Client-Server	★★★★☆	
Guild.Wars	Game	Client-Server	★★☆☆☆	

Fig: 36 (i) Application control – Game category

Name	Category	Technology	Popularity	Risk
PUBG	Game	Client-Server	★★★★★	■□□□□
QQ.HLDDZ	Game	Client-Server	★★★★★	■□□□□
QQ_Games	Game	Client-Server	★★★★★	■□□□□
Quake	Game	Client-Server	★★★☆☆	■□□□□
Rift	Game	Client-Server	★★★★★	■□□□□
Riot.Games	Game	Client-Server	★★★★★	■□□□□
ROBLOX	Game	Browser-Based, Client-Server	★★★☆☆	■□□□□
Runes.Of.Magic	Game	Browser-Based	★★★☆☆	■□□□□
RuneScape	Game	Client-Server	★★★★★	■□□□□
Second.Life	Game	Client-Server	★★★★★	■□□□□
Sina.Game	Game	Browser-Based	★★★★★	■□□□□
Sploder	Game	Browser-Based	★★★☆☆	■□□□□
Starcraft.Broodwar	Game	Client-Server	★★★☆☆	■□□□□
Steam	Game	Client-Server	★★★★★	■□□□□
Street.Basketball	Game	Client-Server	★★★☆☆	■□□□□
Super.Mario.Run	Game	Client-Server	★★★★★	■□□□□
Tales.Runner	Game	Browser-Based	★★★☆☆	■□□□□
Terraria	Game	Client-Server	★★★☆☆	■□□□□
Tibia	Game	Client-Server	★★★☆☆	■□□□□
Unreal.Engine	Game	Client-Server	★★★☆☆	■□□□□
Valve.Games	Game	Client-Server	★★★★★	■□□□□
WAR2Glory	Game	Browser-Based	★★★☆☆	■□□□□

Fig: 36 (ii) Application control – Game category

Warcraft	Game	Client-Server	★★★★★	■□□□□
WeGame	Game	Client-Server	★★★★★	■□□□□
Wordfeud	Game	Browser-Based	★★★★★	■□□□□
World.Of.Tanks	Game	Browser-Based	★★★★★	■□□□□
World.Of.Warcraft	Game	Client-Server	★★★★★	■□□□□
Xbox	Game	Browser-Based	★★★★★	■□□□□
Xbox.HTTP	Game	Browser-Based	★★★☆☆	■□□□□
XYQ	Game	Client-Server	★★★☆☆	■□□□□
Y8	Game	Browser-Based	★★★★★	■□□□□
Yahoo.Sports	Game	Client-Server	★★★★★	■□□□□
Zhengtu	Game	Client-Server	★★★☆☆	■□□□□
Zynga.Games	Game	Browser-Based	★★★☆☆	■□□□□

Fig: 36 (iii) Application control – Game category

4.16 Application control – General Interest category

This category controls the flow of application in the internet link. The below figure shows the various categories using this standard for general Interest category.

☐ Select All	☒ Category: General.Interest	<input checked="" type="button" value="Add Filter"/>	☒ All	Cloud	Selected: 0 / 208
Name	Category	Technology	Popularity	Risk	
 ActiveSync	General.Interest	Client-Server	★★★★★	■■■■■	
 Adobe.Web	General.Interest	Browser-Based	★★★★☆	■■■■■	
 Airport.Utility.mDNS	General.Interest	Client-Server	★★★★☆	■■■■■	
 Akamai.Client	General.Interest	Browser-Based, Client-Server	★★★★★	■■■■■	
 Alexa.Toolbar	General.Interest	Browser-Based	★★★★☆	■■■■■	
 Allstate	General.Interest	Browser-Based	★★★★☆	■■■■■	
 Amazon.Ads	General.Interest	Browser-Based	★★★★☆	■■■■■	
 Amazon.AWS_Console	General.Interest	Browser-Based	★★★★☆	■■■■■	
 Amazon.Mobile	General.Interest	Client-Server	★★★★☆	■■■■■	
 Amazon.Services	General.Interest	Browser-Based	★★★★★	■■■■■	
 Aol.AOL.Search	General.Interest	Browser-Based	★★★★☆	■■■■■	
 AOL.Toolbar	General.Interest	Browser-Based	★★★★☆	■■■■■	
 APC.Powerchute	General.Interest	Client-Server	★★★★☆	■■■■■	
 Apple.Maps	General.Interest	Client-Server	★★★★☆	■■■■■	
 Apple.News	General.Interest	Client-Server	★★★★☆	■■■■■	
 Apple.Push.Notification	General.Interest	Client-Server	★★★★★	■■■■■	
 Apple.Services	General.Interest	Client-Server	★★★★★	■■■■■	
 Apple.Store	General.Interest	Client-Server	★★★★☆	■■■■■	
 Ask.Fm	General.Interest	Client-Server	★★★★☆	■■■■■	
 AT&T.Connect	General.Interest	Browser-Based	★★★★☆	■■■■■	
 AzureWatch	General.Interest	Browser-Based	★★★★☆	■■■■■	
 Babylon	General.Interest	Browser-Based	★★★★★	■■■■■	

Fig: 37 (i) Application control – General Interest category

BBC	General.Interest	Browser-Based	★★★★★	■■■■■
Big.Brother	General.Interest	Client-Server	★★★★☆	■■■■■
Bing.Bar	General.Interest	Browser-Based	★★★★☆	■■■■■
Bing.Maps	General.Interest	Browser-Based	★★★★☆	■■■■■
Bing.Search	General.Interest	Browser-Based	★★★★★	■■■■■
Bing.Search_Image	General.Interest	Browser-Based	★★★★☆	■■■■■
Bing.Search_Safe.Search.Off	General.Interest	Browser-Based	★★★★☆	■■■■■
Bing.Search_Search.Phrase	General.Interest	Browser-Based	★★★★☆	■■■■■
Bitcoin.Cryptocurrency.Miner	General.Interest	Client-Server	★★★★☆	■■■■■
Bitly	General.Interest	Browser-Based	★★★★★	■■■■■
Blackberry.World	General.Interest	Client-Server	★★★★☆	■■■■■
Blogger	General.Interest	Browser-Based	★★★★★	■■■■■
Bloomberg	General.Interest	Browser-Based	★★★★★	■■■■■
BOINC	General.Interest	Client-Server	★★★★☆	■■■■■
Chrome.Bookmark.Sync	General.Interest	Browser-Based	★★★★☆	■■■■■
Chrome.Microphone	General.Interest	Browser-Based	★★★★☆	■■■■■
Chrome.Webstore	General.Interest	Browser-Based	★★★★☆	■■■■■
Citrix.ICA	General.Interest	Client-Server	★★★★☆	■■■■■
CNN	General.Interest	Browser-Based	★★★★★	■■■■■
Computrace	General.Interest	Client-Server	★★★★☆	■■■■■
Conduit.Toolbar	General.Interest	Browser-Based	★★★★★	■■■■■
CPUminer.Cryptocurrency.Miner	General.Interest	Client-Server	★★★★☆	■■■■■

Fig: 37 (ii) Application control – General Interest category

	Craigslist	General.Interest	Browser-Based	★★★★★	
	Daum.Shopping	General.Interest	Browser-Based	★★★★☆	
	Dealio.Toolbar	General.Interest	Browser-Based	★★★★☆	
	Dell.Kace	General.Interest	Browser-Based	★★★★☆	
	Dell.Service	General.Interest	Browser-Based, Client-Server	★★★★★	
	Dell.SupportAssist	General.Interest	Client-Server	★★★★☆	
	Distcc	General.Interest	Client-Server	★★★★☆	
	Distributed.Net	General.Interest	Client-Server	★★★★☆	
	Download.Accelerator.Plus	General.Interest	Client-Server	★★★★☆	
	DuckDuckGo.Search	General.Interest	Browser-Based	★★★★☆	
	DuckDuckGo.Search_Safe.Off	General.Interest	Browser-Based	★★★★☆	
	Duolingo	General.Interest	Browser-Based	★★★★☆	
	eBay.Desktop	General.Interest	Client-Server	★★★★☆	
	eBay.Toolbar	General.Interest	Browser-Based	★★★★☆	
	EndNote	General.Interest	Client-Server	★★★★☆	
	Ethereum.Cryptocurrency.Miner	General.Interest	Client-Server	★★★★☆	
	Eventbrite	General.Interest	Browser-Based	★★★★☆	
	Evernote	General.Interest	Browser-Based	★★★★★	
	Evernote_File.Download	General.Interest	Browser-Based, Client-Server	★★★★★	
	Evernote_File.Upload	General.Interest	Browser-Based, Client-Server	★★★★★	
	Evernote_Login	General.Interest	Browser-Based, Client-Server	★★★★★	
	FeedReader	General.Interest	Client-Server	★★★★☆	

Fig: 37 (iii) Application control – General Interest category

	Flipp	General.Interest	Client-Server	★★★★★	
	FortiGuard.DDNS	General.Interest	Client-Server	★★★★★	
	Free.Download.Manager	General.Interest	Client-Server	★★★★☆	
	FSAE	General.Interest	Client-Server	★★★★☆	
	FunWebProducts	General.Interest	Browser-Based	★★★★☆	
	Gawker	General.Interest	Browser-Based	★★★★☆	
	GKrellM	General.Interest	Client-Server	★★★★☆	
	GO.Global	General.Interest	Client-Server	★★★★☆	
	Google.Accounts	General.Interest	Browser-Based	★★★★☆	
	Google.Ads	General.Interest	Browser-Based	★★★★★	
	Google.Calendar	General.Interest	Browser-Based	★★★★★	
	Google.Calendar_G.Suite	General.Interest	Browser-Based	★★★★☆	
	Google.Calendar_Personal	General.Interest	Browser-Based	★★★★★	
	Google.Calendar_Post	General.Interest	Browser-Based	★★★★★	
	Google.Cloud.Messaging	General.Interest	Client-Server	★★★★☆	
	Google.Earth	General.Interest	Client-Server	★★★★★	
	Google.FeedBurner	General.Interest	Browser-Based	★★★★☆	
	Google.Finance	General.Interest	Browser-Based	★★★★★	
	Google.Keep	General.Interest	Browser-Based	★★★★☆	
	Google.Maps	General.Interest	Browser-Based	★★★★★	
	Google.Maps_Street.View	General.Interest	Browser-Based	★★★★☆	
	Google.Play	General.Interest	Browser-Based	★★★★☆	

Fig:37 (iv) Application control – General Interest category

 Google.Push.Notification	General.Interest	Client-Server	★★★★★	
 Google.Search	General.Interest	Browser-Based	★★★★★	
 Google.Search_Image	General.Interest	Browser-Based	★★★★★	
 Google.Search_Mobile.Voice	General.Interest	Browser-Based	★★★★☆	
 Google.Search_Safe.Off	General.Interest	Browser-Based	★★★★★	
 Google.Search_Search.Phrase	General.Interest	Browser-Based	★★★★★	
 Google.Search_Video	General.Interest	Browser-Based	★★★★☆	
 Google.Services	General.Interest	Browser-Based	★★★★★	
 Google.Toolbar	General.Interest	Browser-Based	★★★★☆	
 Google.Translate	General.Interest	Browser-Based	★★★★★	
 Google.Login	General.Interest	Browser-Based	★★★☆☆	
 Google.Login.G.Suite	General.Interest	Browser-Based	★★★☆☆	
 Google.Login.Personal	General.Interest	Browser-Based	★★★☆☆	
 Gepser	General.Interest	Browser-Based	★★★☆☆	
 Haiwangxing	General.Interest	Client-Server	★★★☆☆	
 HFS.File.Server	General.Interest	Browser-Based	★★★☆☆	
 Hootsuite	General.Interest	Browser-Based	★★★★☆	
 HP.ePrint	General.Interest	Client-Server	★★★★☆	
 HTS	General.Interest	Client-Server	★★★☆☆	
 HTTP.Download.Accelerator	General.Interest	Browser-Based	★★★★★	
 HTTrack	General.Interest	Client-Server	★★★★☆	
 Huffington.Post	General.Interest	Browser-Based	★★★★★	

Fig: 37 (v) Application control – General Interest category

 iRods	General.Interest	Client-Server	☆☆☆☆☆	
 JavaRMI	General.Interest	Client-Server	☆☆☆☆☆	
 JavaRMI_Call	General.Interest	Client-Server	☆☆☆☆☆	
 JavaRMI_Stream	General.Interest	Client-Server	☆☆☆☆☆	
 John.Deere	General.Interest	Browser-Based	☆☆☆☆☆	
 Kakao.Accounts	General.Interest	Browser-Based	☆☆☆☆☆	
 Kiwoom.Hero	General.Interest	Client-Server	☆☆☆☆☆	
 LeBonCoin	General.Interest	Browser-Based, Client-Server	☆☆☆☆☆	
 LiveTV.Toolbar	General.Interest	Browser-Based	☆☆☆☆☆	
 Loglogic.MX	General.Interest	Client-Server	☆☆☆☆☆	
 MapQuest	General.Interest	Browser-Based	☆☆☆☆☆	
 McAfee.SiteAdvisor	General.Interest	Browser-Based	☆☆☆☆☆	
 Microsoft.Silverlight	General.Interest	Browser-Based	☆☆☆☆☆	
 Microsoft.Store	General.Interest	Client-Server	☆☆☆☆☆	
 MinerGate.Cryptocurrency.Miner	General.Interest	Client-Server	☆☆☆☆☆	
 Mipony	General.Interest	Client-Server	☆☆☆☆☆	
 MLB.com	General.Interest	Client-Server	☆☆☆☆☆	
 Monero.Cryptocurrency.Miner	General.Interest	Client-Server	☆☆☆☆☆	
 MS.Firewall.ISA.Client	General.Interest	Client-Server	☆☆☆☆☆	
 MSN.Money	General.Interest	Browser-Based	☆☆☆☆☆	
 Nagios	General.Interest	Browser-Based	☆☆☆☆☆	
 Naver.Map	General.Interest	Browser-Based	☆☆☆☆☆	

Fig: 37 (vi) Application control – General Interest category

 Naver.Search	General.Interest	Browser-Based	☆☆☆☆☆	
 NetFlow	General.Interest	Client-Server	☆☆☆☆☆	
 NetIQ	General.Interest	Client-Server	☆☆☆☆☆	
 NetSupport.School	General.Interest	Client-Server	☆☆☆☆☆	
 New.York.Times	General.Interest	Browser-Based	☆☆☆☆☆	
 NZBVortex	General.Interest	Client-Server	☆☆☆☆☆	
 Paros.Tool	General.Interest	Client-Server	☆☆☆☆☆	
 PeerGuardian	General.Interest	Client-Server	☆☆☆☆☆	
 Pepperplate	General.Interest	Client-Server	☆☆☆☆☆	
 Progress.OpenEdge	General.Interest	Client-Server	☆☆☆☆☆	
 Propalms.TSE	General.Interest	Client-Server	☆☆☆☆☆	
 Qfer	General.Interest	Browser-Based, Client-Server	☆☆☆☆☆	
 QNAP.Web.Portal	General.Interest	Client-Server	☆☆☆☆☆	
 RabbitMQ	General.Interest	Client-Server	☆☆☆☆☆	
 Rakuten.Toolbar	General.Interest	Browser-Based	☆☆☆☆☆	
 Rapportive	General.Interest	Browser-Based	☆☆☆☆☆	
 Realtor.Com	General.Interest	Browser-Based	☆☆☆☆☆	
 Rstatd	General.Interest	Client-Server	☆☆☆☆☆	
 RT.Noticias	General.Interest	Browser-Based	☆☆☆☆☆	
 Rusers	General.Interest	Client-Server	☆☆☆☆☆	
 SAP.Diagnostic	General.Interest	Client-Server	☆☆☆☆☆	
 SAP.Message.Server	General.Interest	Client-Server	☆☆☆☆☆	

Fig: 37 (vii) Application control – General Interest category

 StumbleUpon.Toolbar	General.Interest	Browser-Based	★★★★★	
 Swyxxware.CDS	General.Interest	Client-Server	★☆☆☆☆	
 Symantec.Sysnt.Center	General.Interest	Client-Server	★☆☆☆☆	
 Tencent.Services	General.Interest	Browser-Based	★★★★★	
 Texthelp	General.Interest	Browser-Based	★★★★☆	
 TFN	General.Interest	Network-Protocol	★☆☆☆☆	
 TgCom24	General.Interest	Browser-Based	★★★★☆	
 Toad	General.Interest	Client-Server	★☆☆☆☆	
 Track.It	General.Interest	Client-Server	★☆☆☆☆	
 TradeStation	General.Interest	Client-Server	★☆☆☆☆	
 Truecaller	General.Interest	Browser-Based, Client-Server	★☆☆☆☆	
 UEFA	General.Interest	Browser-Based	★★★★☆	
 UNIStim	General.Interest	Client-Server	★☆☆☆☆	
 Univision	General.Interest	Browser-Based	★★★★☆	
 Usenet.Net	General.Interest	Browser-Based	★☆☆☆☆	
 Washington.Post	General.Interest	Browser-Based	★★★★★	
 Waze	General.Interest	Client-Server	★★★★☆	
 WeatherBug	General.Interest	Browser-Based	★★★★★	
 WebConnect	General.Interest	Client-Server	★☆☆☆☆	
 Webshots	General.Interest	Browser-Based	★★★★☆	
 Wget	General.Interest	Client-Server	★★★★★	
 Windows.CRL.Request	General.Interest	Browser-Based	★★★★★	

Fig: 37 (viii) Application control – General Interest category

Name	Category	Technology	Popularity	Risk
Windows.Phone.Store	General.Interest	Browser-Based	☆☆☆☆☆	■■■■■
WinPcap.Rpcapd	General.Interest	Client-Server	☆☆☆☆☆	■■■■■
WinSCP	General.Interest	Client-Server	☆☆☆☆☆	■■■■■
Wordfast.Anywhere	General.Interest	Browser-Based	☆☆☆☆☆	■■■■■
Wunderlist	General.Interest	Browser-Based, Client-Server	☆☆☆☆☆	■■■■■
X.Font.Server	General.Interest	Client-Server	☆☆☆☆☆	■■■■■
XWare	General.Interest	Client-Server	☆☆☆☆☆	■■■■■
YaCy	General.Interest	Peer-to-Peer	☆☆☆☆☆	■■■■■
Yahoo.Account_Login	General.Interest	Browser-Based	☆☆☆☆☆	■■■■■
Yahoo.Accounts	General.Interest	Browser-Based	☆☆☆☆☆	■■■■■
Yahoo.Calendar	General.Interest	Browser-Based	☆☆☆☆☆	■■■■■
Yahoo.Finance	General.Interest	Browser-Based	☆☆☆☆☆	■■■■■
Yahoo.Japan.Box	General.Interest	Client-Server	☆☆☆☆☆	■■■■■
Yahoo.News	General.Interest	Browser-Based	☆☆☆☆☆	■■■■■
Yahoo.Notepad	General.Interest	Browser-Based	☆☆☆☆☆	■■■■■
Yahoo.Search	General.Interest	Browser-Based	☆☆☆☆☆	■■■■■
Yahoo.Search_Safe.Moderate.Level	General.Interest	Browser-Based	☆☆☆☆☆	■■■■■
Yahoo.Search_Safe.Off	General.Interest	Browser-Based	☆☆☆☆☆	■■■■■
Yahoo.Services	General.Interest	Browser-Based	☆☆☆☆☆	■■■■■
Yahoo.Toolbar	General.Interest	Browser-Based	☆☆☆☆☆	■■■■■
Yandex	General.Interest	Browser-Based	☆☆☆☆☆	■■■■■
Yandex.Maps	General.Interest	Browser-Based, Client-Server	☆☆☆☆☆	■■■■■

Fig: 37 (ix) Application control – General Interest category

Yahoo.Accounts	General.Interest	Browser-Based	☆☆☆☆☆	■■■■■
Yahoo.Calendar	General.Interest	Browser-Based	☆☆☆☆☆	■■■■■
Yahoo.Finance	General.Interest	Browser-Based	☆☆☆☆☆	■■■■■
Yahoo.Japan.Box	General.Interest	Client-Server	☆☆☆☆☆	■■■■■
Yahoo.News	General.Interest	Browser-Based	☆☆☆☆☆	■■■■■
Yahoo.Notepad	General.Interest	Browser-Based	☆☆☆☆☆	■■■■■
Yahoo.Search	General.Interest	Browser-Based	☆☆☆☆☆	■■■■■
Yahoo.Search_Safe.Moderate.Level	General.Interest	Browser-Based	☆☆☆☆☆	■■■■■
Yahoo.Search_Safe.Off	General.Interest	Browser-Based	☆☆☆☆☆	■■■■■
Yahoo.Services	General.Interest	Browser-Based	☆☆☆☆☆	■■■■■
Yahoo.Toolbar	General.Interest	Browser-Based	☆☆☆☆☆	■■■■■
Yandex	General.Interest	Browser-Based	☆☆☆☆☆	■■■■■
Yandex.Maps	General.Interest	Browser-Based, Client-Server	☆☆☆☆☆	■■■■■
Yandex.Search	General.Interest	Browser-Based	☆☆☆☆☆	■■■■■
Yandex.Search_Image	General.Interest	Browser-Based	☆☆☆☆☆	■■■■■
Yandex.Search_Safe.Off	General.Interest	Browser-Based	☆☆☆☆☆	■■■■■
Yandex.Search_Video	General.Interest	Browser-Based	☆☆☆☆☆	■■■■■
Youdao	General.Interest	Client-Server	☆☆☆☆☆	■■■■■
ZbigZ	General.Interest	Browser-Based	☆☆☆☆☆	■■■■■
ZCash.Cryptocurrency.Miner	General.Interest	Client-Server	☆☆☆☆☆	■■■■■
ZeroNet	General.Interest	Browser-Based, Peer-to-Peer	☆☆☆☆☆	■■■■■
Zhihu	General.Interest	Browser-Based	☆☆☆☆☆	■■■■■

Fig: 37 (x) Application control – General Interest category

Add signatures				
☐ Select All ☒ Category: Mobile Add Filter <input checked="" type="button" value="All"/> Cloud Selected: 0 / 2085 				
Name	Category	Technology	Popularity	Risk
Android	Mobile	Client-Server	★★★★★	
Apple.iPad	Mobile	Client-Server	★★★★★	
Apple.iPhone	Mobile	Client-Server	★★★★★	

Fig: 37 (xi) Application control – General Interest category

4.17 Application control – Network Service category

This category controls the flow of application in the internet link. The below figure shows the various categories using this standard for network service category.

☐ Select All ☒ Category: Network.Service Add Filter <input checked="" type="button" value="All"/> Cloud Selected: 0 / 208 				
Name	Category	Technology	Popularity	Risk
3PC	Network.Service	Network-Protocol	★★★★☆	
9PFS	Network.Service	Network-Protocol	★★★★☆	
A.N	Network.Service	Network-Protocol	★★★★☆	
Active.Directory	Network.Service	Network-Protocol	★★★★★	
AFP	Network.Service	Network-Protocol	★★★★☆	
AH	Network.Service	Network-Protocol	★★★★☆	
AMQP	Network.Service	Network-Protocol	★★★★★	
Applicability.Statement.2	Network.Service	Network-Protocol	★★★☆☆	
ARGUS	Network.Service	Network-Protocol	★★★★☆	
ARIS	Network.Service	Network-Protocol	★★★★☆	
Aruba.PAPI	Network.Service	Network-Protocol	★★★★☆	
AS2	Network.Service	Network-Protocol	★★★★☆	
Atom.Publishing.Protocol	Network.Service	Network-Protocol	★★★★★	
AX.25	Network.Service	Network-Protocol	★★★★☆	
BBN.RCC.MON	Network.Service	Network-Protocol	★★★★☆	
BFD	Network.Service	Network-Protocol	★★★☆☆	
BGP	Network.Service	Network-Protocol	★★★★☆	
BICC	Network.Service	Network-Protocol	★★★☆☆	
BlackBerry.Enterprise	Network.Service	Network-Protocol	★★★★★	
BNA	Network.Service	Network-Protocol	★★★★☆	
BOOTP	Network.Service	Network-Protocol	★★★★★	
BR.SAT.MON	Network.Service	Network-Protocol	★★★★☆	

Fig: 38 (i) Application control – Network Service category

DICOM_C.Store.Request	Network.Service	Network-Protocol	★★★★☆	
DICOM_N.Action.Request	Network.Service	Network-Protocol	★★★★☆	
DICOM_N.Create.Request	Network.Service	Network-Protocol	★★★★☆	
DICOM_N.Get.Request	Network.Service	Network-Protocol	★★★★☆	
DICOM_N.Set.Request	Network.Service	Network-Protocol	★★★★☆	
Discard	Network.Service	Network-Protocol	★★★★☆	
DLSw.RPN	Network.Service	Network-Protocol	★★★★☆	
DLSw.WPN	Network.Service	Network-Protocol	★★★★☆	
DNS	Network.Service	Network-Protocol	★★★★★	
DNS_Dynamic.Update	Network.Service	Network-Protocol	★★★★★	
DNS_Request.ANY.Record	Network.Service	Network-Protocol	★★★★★	
DNS_Zone.Transfer	Network.Service	Network-Protocol	★★★★☆	
DSR	Network.Service	Network-Protocol	★★★★☆	
DTLS	Network.Service	Network-Protocol	★★★★☆	
Echo	Network.Service	Network-Protocol	★★★★★	
EGP	Network.Service	Network-Protocol	★★★★☆	
EIGRP	Network.Service	Network-Protocol	★★★★☆	
Eklogin	Network.Service	Network-Protocol	★★★★☆	
EMCON	Network.Service	Network-Protocol	★★★★☆	
ENCAP	Network.Service	Network-Protocol	★★★★☆	
EPMD	Network.Service	Network-Protocol	★★★★☆	
ESP.IP	Network.Service	Network-Protocol	★★★★☆	

Fig:38 (ii)Application control – Network Service category

IDRP	Network.Service	Network-Protocol	★★★★☆	
IFMP	Network.Service	Network-Protocol	★★★★☆	
IGMP	Network.Service	Network-Protocol	★★★★☆	
IGP	Network.Service	Network-Protocol	★★★★☆	
IKE	Network.Service	Network-Protocol	★★★★☆	
IL	Network.Service	Network-Protocol	★★★★☆	
IP.In.IP	Network.Service	Network-Protocol	★★★★☆	
IP.Multicast	Network.Service	Network-Protocol	★★★★☆	
IP.Within.IP	Network.Service	Network-Protocol	★★★★☆	
IPComp	Network.Service	Network-Protocol	★★★★☆	
IPCU	Network.Service	Network-Protocol	★★★★☆	
Iperf	Network.Service	Client-Server	★★★★☆	
IPFix	Network.Service	Network-Protocol	★★★★☆	
IPLT	Network.Service	Network-Protocol	★★★★☆	
IPMI	Network.Service	Network-Protocol	★★★★☆	
IPP	Network.Service	Network-Protocol	★★★★☆	
IPPC	Network.Service	Network-Protocol	★★★★☆	
IPv6.Frag	Network.Service	Network-Protocol	★★★★☆	
IPv6.ICMP	Network.Service	Network-Protocol	★★★★★	
IPv6.In.IP	Network.Service	Network-Protocol	★★★★★	
IPv6.NoNxt	Network.Service	Network-Protocol	★★★★☆	
IPv6.Opts	Network.Service	Network-Protocol	★★★★☆	

Fig: 38 (iii)Application control – Network Service category

Mobile.IP	Network.Service	Network-Protocol	★★★★☆	
Mobility.Header	Network.Service	Network-Protocol	★★★★☆	
Mount	Network.Service	Network-Protocol	★★★★☆	
MPLS.In.IP	Network.Service	Network-Protocol	★★★★☆	
MPTCP	Network.Service	Network-Protocol	★★★★☆	
MQTT	Network.Service	Network-Protocol, Client-Server	★★★★☆	
MS.DFSR	Network.Service	Client-Server	★★★★☆	
MS.DTC	Network.Service	Client-Server	★★★★☆	
MS.FRS	Network.Service	Client-Server	★★★★☆	
MS.RPC	Network.Service	Client-Server	★★★★☆	
MS.RPC_UUID	Network.Service	Client-Server	★★★★☆	
MSDP	Network.Service	Network-Protocol	★★★★☆	
MSRP	Network.Service	Network-Protocol	★★★★☆	
MTP	Network.Service	Network-Protocol	★★★★☆	
Multicast.DNS	Network.Service	Network-Protocol	★★★★☆	
Multimedia.Message	Network.Service	Client-Server	★★★★☆	
MUX	Network.Service	Network-Protocol	★★★★☆	
NARP	Network.Service	Network-Protocol	★★★★☆	
NAT.PMP	Network.Service	Network-Protocol	★★★★☆	
NCP	Network.Service	Network-Protocol	★★★★☆	
NDMP	Network.Service	Network-Protocol	★★★★☆	
NetBIOS.DGM	Network.Service	Network-Protocol	★★★★☆	

Fig: 38 (iv)Application control – Network Service category

QUIC	Network.Service	Network-Protocol	★★★★☆	
Quote.Of.The.Day	Network.Service	Network-Protocol	★★★★☆	
RADIUS	Network.Service	Network-Protocol	★★★★☆	
RAP	Network.Service	Network-Protocol	★★★★☆	
RDT	Network.Service	Network-Protocol	★★★★☆	
Reliable.Data.Protocol	Network.Service	Network-Protocol	★★★★☆	
RIP	Network.Service	Network-Protocol	★★★★☆	
RIPng	Network.Service	Network-Protocol	★★★★☆	
RLP	Network.Service	Network-Protocol	★★★★☆	
RMCP	Network.Service	Network-Protocol	★★★★☆	
RMI.IIOP	Network.Service	Network-Protocol	★★★★☆	
RPC.Over.HTTP	Network.Service	Network-Protocol	★★★★☆	
RSS	Network.Service	Browser-Based	★★★★☆	
RSVP	Network.Service	Network-Protocol	★★★★☆	
RSVPE2E.IGNORE	Network.Service	Network-Protocol	★★★★☆	
RVD	Network.Service	Network-Protocol	★★★★☆	
Rwho	Network.Service	Network-Protocol	★★★★☆	
S1AP	Network.Service	Network-Protocol	★★★★☆	
SAT.EXPAK	Network.Service	Network-Protocol	★★★★☆	
SAT.MON	Network.Service	Network-Protocol	★★★★☆	
SCC.SP	Network.Service	Network-Protocol	★★★★☆	
SCPS	Network.Service	Network-Protocol	★★★★☆	

Fig: 38 (v)Application control – Network Service category

 SRP	Network.Service	Network-Protocol	★★★★☆	
 SSCOMCE	Network.Service	Network-Protocol	★★★★☆	
 SSH	Network.Service	Network-Protocol	★★★★★	
 SSH.Over.HTTP	Network.Service	Client-Server	★★★★☆	
 SSH.Over.SOCKS	Network.Service	Client-Server	★★★★☆	
 SSL	Network.Service	Network-Protocol	★★★★★	
 SSL_SSLv2	Network.Service	Network-Protocol	★★★★★	
 SSL_SSLv3	Network.Service	Network-Protocol	★★★★★	
 SSL_TLSv1.0	Network.Service	Network-Protocol	★★★★★	
 SSL_TLSv1.1	Network.Service	Network-Protocol	★★★★★	
 SSL_TLSv1.2	Network.Service	Network-Protocol	★★★★★	
 SSL_TLSv1.3	Network.Service	Network-Protocol	★★★★★	
 ST	Network.Service	Network-Protocol	★★★★☆	
 STOMP.Protocol	Network.Service	Network-Protocol	★★★★☆	
 STP	Network.Service	Network-Protocol	★★★★☆	
 STUN	Network.Service	Network-Protocol	★★★★★	
 SUN.ND	Network.Service	Network-Protocol	★★★★☆	
 Sun.RPC	Network.Service	Client-Server	★★★★★	
 Sun.RPC_Program.Number	Network.Service	Client-Server	★★★★☆	
 swIpe	Network.Service	Network-Protocol	★★★★☆	
 Syslog	Network.Service	Network-Protocol	★★★★★	
 Systat	Network.Service	Network-Protocol	★★★★☆	

Fig: 38 (vi)Application control – Network Service category

 WB.EXPAK	Network.Service	Network-Protocol	★★★★☆	
 WB.MON	Network.Service	Network-Protocol	★★★★☆	
 WCCPV1	Network.Service	Network-Protocol	★★★★☆	
 WCCPV2	Network.Service	Network-Protocol	★★★★☆	
 WebDAV	Network.Service	Network-Protocol	★★★★★	
 WebSocket	Network.Service	Browser-Based	★★★★★	
 WHOIS	Network.Service	Network-Protocol	★★★★☆	
 Windows.File.Sharing	Network.Service	Client-Server	★★★★★	
 Windows.File.Sharing_Create.Directory	Network.Service	Client-Server	★★★★☆	
 Windows.File.Sharing_Create.File	Network.Service	Client-Server	★★★★☆	
 Windows.File.Sharing_Delete.Directory	Network.Service	Client-Server	★★★★☆	
 Windows.File.Sharing_Delete.File	Network.Service	Client-Server	★★★★☆	
 Windows.File.Sharing_Open.Directory	Network.Service	Client-Server	★★★★★	
 Windows.File.Sharing_Print.File	Network.Service	Client-Server	★★★★★	
 Windows.File.Sharing_Read.Executable.File	Network.Service	Client-Server	★★★★★	
 Windows.File.Sharing_Read.File	Network.Service	Client-Server	★★★★★	
 Windows.File.Sharing_Write.Executable.File	Network.Service	Client-Server	★★★★☆	
 Windows.File.Sharing_Write.File	Network.Service	Client-Server	★★★★★	
 WINS	Network.Service	Network-Protocol	★★★★☆	
 WLCCP	Network.Service	Network-Protocol	★★★★☆	
 WSN	Network.Service	Network-Protocol	★★★★☆	
 X11	Network.Service	Network-Protocol	★★★★☆	

Fig: 38 (vii)Application control – Network Service category

4.18 Application control – P2P category

This category controls the flow of application in the internet link. The below figure shows the various categories using this standard for P2P category.

☐ Select All	Category: P2P	All	Cloud	Selected: 0 / 20
Name	Category	Technology	Popularity	Risk
ABC	P2P	Peer-to-Peer	★★★★☆	■■■■■
ANts.P2P	P2P	Peer-to-Peer	★★★★☆	■■■■■
Arctic.Torrent	P2P	Peer-to-Peer	★★★★☆	■■■■■
Ares	P2P	Peer-to-Peer	★★★★★	■■■■■
Ares.Chat.Join	P2P	Peer-to-Peer	★★★★★	■■■■■
Baidu.Music	P2P	Peer-to-Peer	★★★★★	■■■■■
Baidu.P2P	P2P	Peer-to-Peer	★★★★☆	■■■■■
BBCP	P2P	Peer-to-Peer	★★★★☆	■■■■■
Bitcoin	P2P	Client-Server, Peer-to-Peer	★★★★☆	■■■■■
Bitcomet.HTTP.Seed	P2P	Peer-to-Peer	★★★★★	■■■■■
Bitsnoop	P2P	Browser-Based	★★★★☆	■■■■■
BitTorrent	P2P	Peer-to-Peer	★★★★★	■■■■■
Cabos	P2P	Peer-to-Peer	★★★★☆	■■■■■
Cacaoweb	P2P	Peer-to-Peer	★★★★☆	■■■■■
CTorrent	P2P	Peer-to-Peer	★★★★☆	■■■■■
Direct.Connect	P2P	Peer-to-Peer	★★★★☆	■■■■■
eMule	P2P	Peer-to-Peer	★★★★★	■■■■■
ExtraTorrent	P2P	Peer-to-Peer	★★★★☆	■■■■■
FileGuri	P2P	Peer-to-Peer	★★★★★	■■■■■
FlashGet	P2P	Peer-to-Peer	★★★★★	■■■■■
Freenet	P2P	Peer-to-Peer	★★★★☆	■■■■■
FrostWire	P2P	Peer-to-Peer	★★★★☆	■■■■■

Fig:39 (i) Application control – P2P category

Name	Category	Technology	Popularity	Risk
TorrentSpy	P2P	Peer-to-Peer	★★★★☆	■■■■■
Torrentz	P2P	Browser-Based	★★★★☆	■■■■■
TOTOROSA	P2P	Peer-to-Peer	★★★★☆	■■■■■
Trin00	P2P	Peer-to-Peer	★★★★☆	■■■■■
Tudou.Speedup	P2P	Peer-to-Peer	★★★★☆	■■■■■
VeryCD	P2P	Browser-Based	★★★★☆	■■■■■
Vuze	P2P	Peer-to-Peer	★★★★★	■■■■■
WinMX	P2P	Peer-to-Peer	★★★★★	■■■■■
Winny	P2P	Peer-to-Peer	★★★★☆	■■■■■

Fig:39 (ii) Application control – P2P category

4.19 Application control – Proxy category

This category controls the flow of application in the internet link. The below figure shows the various categories using this standard for proxy category.

☐ Select All	Category: Proxy	All	Cloud	Selected: 0 / 208
Name	Proxy	Technology	Popularity	Risk
ActMobile.VPN	Proxy	Client-Server	★★★★☆	██████
Amaze.VPN	Proxy	Client-Server	★★★★☆	██████
AnonymoX	Proxy	Client-Server	★★★★☆	██████
AnonyTun	Proxy	Client-Server	★★★★☆	██████
AppVPN	Proxy	Client-Server	★★★★☆	██████
ASProxy	Proxy	Browser-Based	★★★★☆	██████
Astrill	Proxy	Client-Server	★★★★☆	██████
Atom.VPN	Proxy	Client-Server	★★★★☆	██████
AutoHideIP	Proxy	Client-Server	★★★★☆	██████
Avira.Phantom.VPN	Proxy	Client-Server	★★★★☆	██████
Bestline.VPN	Proxy	Client-Server	★★★★☆	██████
Betternet.VPN	Proxy	Client-Server	★★★★☆	██████
Blockless.Proxy.VPN	Proxy	Client-Server	★★★★☆	██████
BlueSurface	Proxy	Client-Server	★★★★☆	██████
Browsec	Proxy	Client-Server	★★★★☆	██████
CGIProxy	Proxy	Browser-Based	★★★★☆	██████
Cisco.VPN.Client	Proxy	Client-Server	★★★★☆	██████
Cloud.VPN	Proxy	Client-Server	★★★★☆	██████
Cow.VPN	Proxy	Browser-Based	★★★★☆	██████
CProxy	Proxy	Client-Server	★★★★☆	██████
Croxy.Proxy.VPN	Proxy	Client-Server	★★★★☆	██████
CyberGhost.VPN	Proxy	Client-Server	★★★★☆	██████

Fig: 40 (i) Application control – Proxy category

Name	Category	Technology	Popularity	Risk
HeaderTun.VPN	Proxy	Client-Server	★★★★☆	■■■■■
Hexatech.VPN	Proxy	Client-Server	★★★★☆	■■■■■
Hi.VPN	Proxy	Client-Server	★★★★☆	■■■■■
Hide.Ali.IP	Proxy	Client-Server	★★★★☆	■■■■■
Hide.me.VPN	Proxy	Browser-Based, Client-Server	★★★★☆	■■■■■
Hide.My.IP	Proxy	Client-Server	★★★★☆	■■■■■
Hideman.VPN	Proxy	Client-Server	★★★★☆	■■■■■
HideMe.Free.VPN	Proxy	Client-Server	★★★★☆	■■■■■
HMA.Pro.VPN	Proxy	Client-Server	★★★★☆	■■■■■
Hola.Unblocker	Proxy	Client-Server	★★★★☆	■■■■■
HoSPProxy	Proxy	Client-Server	★★★★☆	■■■■■
Hotspot.Shield	Proxy	Client-Server	★★★★☆	■■■■■
Hotspot.VPN	Proxy	Client-Server	★★★★☆	■■■■■
HotVPN	Proxy	Client-Server	★★★★☆	■■■■■
Hoxc.VPN	Proxy	Client-Server	★★★★☆	■■■■■
HTTP.Tunnel	Proxy	Client-Server	★★★★☆	■■■■■
I2P	Proxy	Client-Server	★★★★☆	■■■■■
Iodine	Proxy	Client-Server	★★★★☆	■■■■■
IP.Shield	Proxy	Client-Server	★★★★☆	■■■■■
Ivacy	Proxy	Client-Server	★★★★☆	■■■■■
JonDo	Proxy	Browser-Based	★★★★☆	■■■■■
Just.Proxy.VPN	Proxy	Client-Server	★★★★☆	■■■■■

Fig: 40 (ii) Application control – Proxy category

Name	Category	Technology	Popularity	Risk
Puff	Proxy	Client-Server	★★★★☆	■■■■■
Puffin	Proxy	Browser-Based	★★★★☆	■■■■■
Pure.VPN	Proxy	Client-Server	★★★★☆	■■■■■
Raha.VPN	Proxy	Client-Server	★★★★☆	■■■■■
Rus.VPN	Proxy	Client-Server	★★★★☆	■■■■■
SaferVPN	Proxy	Client-Server	★★★★☆	■■■■■
SecurityKiss	Proxy	Client-Server	★★★★☆	■■■■■
Seed4.Me.VPN	Proxy	Client-Server	★★★★☆	■■■■■
Setup.VPN	Proxy	Client-Server	★★★★☆	■■■■■
Shadowsocks	Proxy	Client-Server	★★★★☆	■■■■■
Skyfire	Proxy	Client-Server	★★★★☆	■■■■■
SkyVPN	Proxy	Client-Server	★★★★☆	■■■■■
skyZIP	Proxy	Browser-Based	★★★★☆	■■■■■
Snap.VPN	Proxy	Client-Server	★★★★☆	■■■■■
Socks2HTTP	Proxy	Client-Server	★★★★☆	■■■■■
SOCKS4	Proxy	Network-Protocol	★★★★☆	■■■■■
SOCKS5	Proxy	Network-Protocol	★★★★☆	■■■■■
Speedify	Proxy	Client-Server	★★★★☆	■■■■■
Spotflux	Proxy	Client-Server	★★★★☆	■■■■■
SSTP	Proxy	Network-Protocol	★★★★☆	■■■■■
Star.VPN	Proxy	Client-Server	★★★★☆	■■■■■
SuperVPN.Android	Proxy	Client-Server	★★★★☆	■■■■■

Fig: 41 (iii) Application control – Proxy category

Name ↕	Category ↕	Technology ↕	Popularity ↕	Risk ↕
 VPN.Go	Proxy	Client-Server	★★★★☆	
 VPN.Master	Proxy	Client-Server	★★★★☆	
 VPN.Monster	Proxy	Client-Server	★★★★☆	
 VPN.Robot	Proxy	Client-Server	★★★★☆	
 WASEL.Pro	Proxy	Client-Server	★★★★☆	
 Wi.Free	Proxy	Client-Server	★★★★☆	
 WindScribe	Proxy	Client-Server	★★★★☆	
 WireGuard	Proxy	Client-Server	★★★★☆	
 Wuma.VPN	Proxy	Client-Server	★★★★☆	
 XiaoMing.VPN	Proxy	Client-Server	★★★★☆	
 Yoga.VPN	Proxy	Client-Server	★★★★☆	
 Your.Freedom	Proxy	Client-Server	★★★★☆	
 Zapyo	Proxy	Browser-Based	★★★★☆	
 ZenMate	Proxy	Browser-Based	★★★★★	
 Zero.VPN	Proxy	Client-Server	★★★★☆	
 ZPN.Connect	Proxy	Client-Server	★★★★☆	

Fig: 41 (iv) Application control – Proxy category

4.20 Application control – Remote Access category

This category controls the flow of application in the internet link. The below figure shows the various categories using this standard for remote access category.

☐ Select All	Category: Remote.Access	All	Cloud	Selected: 0 / 208
Name	Category	Technology	Popularity	Risk
Adobe.Connect_Meeting.Remote.Control	Remote.Access	Browser-Based	☆☆☆☆☆	■■■■■
AeroAdmin	Remote.Access	Client-Server	☆☆☆☆☆	■■■■■
AirDroid	Remote.Access	Client-Server	☆☆☆☆☆	■■■■■
Alpemix	Remote.Access	Client-Server	☆☆☆☆☆	■■■■■
Ammyy.Admin	Remote.Access	Client-Server	☆☆☆☆☆	■■■■■
AnyDesk	Remote.Access	Client-Server	☆☆☆☆☆	■■■■■
Anyplace.Control	Remote.Access	Client-Server	☆☆☆☆☆	■■■■■
Apple.Remote.Desktop	Remote.Access	Client-Server	☆☆☆☆☆	■■■■■
Back.Orifice	Remote.Access	Client-Server	☆☆☆☆☆	■■■■■
Bomgar	Remote.Access	Client-Server	☆☆☆☆☆	■■■■■
Chrome.Remote.Desktop	Remote.Access	Client-Server	☆☆☆☆☆	■■■■■
Citrix.Receiver	Remote.Access	Client-Server	☆☆☆☆☆	■■■■■
Citrix.Services_Netviewer	Remote.Access	Browser-Based	☆☆☆☆☆	■■■■■
ConnectWise.Automate	Remote.Access	Client-Server	☆☆☆☆☆	■■■■■
ConnectWise.Automate_Remote.Control	Remote.Access	Client-Server	☆☆☆☆☆	■■■■■
CrazyRemote	Remote.Access	Client-Server	☆☆☆☆☆	■■■■■
DameWare	Remote.Access	Client-Server	☆☆☆☆☆	■■■■■
DeskShare	Remote.Access	Client-Server	☆☆☆☆☆	■■■■■
Ericom.AccessNow	Remote.Access	Client-Server	☆☆☆☆☆	■■■■■
FastViewer	Remote.Access	Client-Server	☆☆☆☆☆	■■■■■
FixMe.IT	Remote.Access	Client-Server	☆☆☆☆☆	■■■■■
GoToAssist	Remote.Access	Client-Server	☆☆☆☆☆	■■■■■

Fig: 42 (i) Application control – Remote Access category

Name	Category	Technology	Popularity	Risk
RDP	Remote.Access	Client-Server	☆☆☆☆☆	■■■■■
RDP.over.HTTPS	Remote.Access	Client-Server	☆☆☆☆☆	■■■■■
Remote.Manipulator.System	Remote.Access	Client-Server	☆☆☆☆☆	■■■■■
RemotelyAnywhere	Remote.Access	Client-Server	☆☆☆☆☆	■■■■■
RemotePC	Remote.Access	Client-Server	☆☆☆☆☆	■■■■■
Rexec	Remote.Access	Client-Server	☆☆☆☆☆	■■■■■
Rlogin	Remote.Access	Client-Server	☆☆☆☆☆	■■■■■
Rsh	Remote.Access	Client-Server	☆☆☆☆☆	■■■■■
Rsupport.RemoteCall	Remote.Access	Client-Server	☆☆☆☆☆	■■■■■
Rsupport.RemoteView	Remote.Access	Browser-Based	☆☆☆☆☆	■■■■■
ScreenConnect	Remote.Access	Client-Server	☆☆☆☆☆	■■■■■
Screenhero	Remote.Access	Client-Server	☆☆☆☆☆	■■■■■
ShowMyPC	Remote.Access	Client-Server	☆☆☆☆☆	■■■■■
Solarwinds.Take.Control	Remote.Access	Client-Server	☆☆☆☆☆	■■■■■
Splashtop	Remote.Access	Client-Server	☆☆☆☆☆	■■■■■
Spy.Agent	Remote.Access	Client-Server	☆☆☆☆☆	■■■■■
Supremo	Remote.Access	Client-Server	☆☆☆☆☆	■■■■■
Synergy	Remote.Access	Client-Server	☆☆☆☆☆	■■■■■
TeamViewer	Remote.Access	Client-Server	☆☆☆☆☆	■■■■■
TeamViewer_CallReceive	Remote.Access	Client-Server	☆☆☆☆☆	■■■■■
TeamViewer_CallRequest	Remote.Access	Client-Server	☆☆☆☆☆	■■■■■
Telnet	Remote.Access	Client-Server	☆☆☆☆☆	■■■■■

Fig: 42 (ii) Application control – Remote Access category

4.21 Application control – Social Media category

This category controls the flow of application in the internet link. The below figure shows the various categories using this standard for social media category.

☐ Select All Category: Social.Media All Cloud Selected: 0 / 208				
Name	Category	Technology	Popularity	Risk
2ch	Social.Media	Browser-Based	★★★★☆	■ ■ ■ ■ ■
2ch_Post	Social.Media	Browser-Based	★★★★☆	■ ■ ■ ■ ■
5ch	Social.Media	Browser-Based	★★★★☆	■ ■ ■ ■ ■
5ch_Post	Social.Media	Browser-Based	★★★★☆	■ ■ ■ ■ ■
After.School	Social.Media	Client-Server	★★★★☆	■ ■ ■ ■ ■
Apple.Daily	Social.Media	Client-Server	★★★★★	■ ■ ■ ■ ■
Badoo	Social.Media	Browser-Based	★★★★★	■ ■ ■ ■ ■
Baidu.Tieba	Social.Media	Browser-Based	★★★★☆	■ ■ ■ ■ ■
Bubbly	Social.Media	Client-Server	★★★★☆	■ ■ ■ ■ ■
Care2	Social.Media	Browser-Based	★★★★☆	■ ■ ■ ■ ■
Circle.Of.Moms	Social.Media	Browser-Based	★★★★☆	■ ■ ■ ■ ■
Cyworld	Social.Media	Browser-Based	★★★★☆	■ ■ ■ ■ ■
Daum.Blog	Social.Media	Browser-Based	★★★★☆	■ ■ ■ ■ ■
Daum.Cafe	Social.Media	Browser-Based	★★★★☆	■ ■ ■ ■ ■
DeviantArt	Social.Media	Browser-Based	★★★★★	■ ■ ■ ■ ■
Dlisted	Social.Media	Browser-Based	★★★★☆	■ ■ ■ ■ ■
Eyejot	Social.Media	Browser-Based	★★★★☆	■ ■ ■ ■ ■
Facebook	Social.Media	Browser-Based	★★★★★	■ ■ ■ ■ ■
Facebook_AppName	Social.Media	Browser-Based	★★★★☆	■ ■ ■ ■ ■
Facebook_Apps	Social.Media	Browser-Based	★★★★☆	■ ■ ■ ■ ■
Facebook_Chat	Social.Media	Browser-Based	★★★★☆	■ ■ ■ ■ ■
Facebook_File.Download	Social.Media	Browser-Based	★★★★☆	■ ■ ■ ■ ■

Fig: 43(i) Application control – Social Media category

Name 	Category 	Technology 	Popularity 	Risk 
 Houseparty	Social.Media	Client-Server	★★★★★	
 FTTT	Social.Media	Browser-Based	★★★★☆	
 Imgur.File.Upload	Social.Media	Browser-Based	★★★★☆	
 Instagram	Social.Media	Client-Server	★★★★★	
 Instagram_File.Upload	Social.Media	Client-Server	★★★★★	
 Instagram_Login	Social.Media	Client-Server	★★★★★	
 Instagram_Post	Social.Media	Client-Server	★★★★★	
 Instagram_Video	Social.Media	Client-Server	★★★★★	
 Jodel	Social.Media	Client-Server	★★★★☆	
 KakaoStory	Social.Media	Browser-Based	★★★★☆	
 Keek	Social.Media	Client-Server	★★★★☆	
 LinkedIn	Social.Media	Browser-Based	★★★★★	
 LinkedIn_File.Download	Social.Media	Browser-Based	★★★★☆	
 LinkedIn_File.Upload	Social.Media	Browser-Based	★★★★☆	
 LinkedIn_Login	Social.Media	Browser-Based	★★★★☆	
 LinkedIn_Message	Social.Media	Browser-Based	★★★★☆	
 LinkedIn_Post	Social.Media	Browser-Based	★★★★☆	
 Livejournal	Social.Media	Browser-Based	★★★★★	
 Mail.Ru_Moimir	Social.Media	Browser-Based	★★★★☆	
 Marvel	Social.Media	Browser-Based	★★★★☆	
 Meetup	Social.Media	Browser-Based	★★★★★	
 Meetup_Email	Social.Media	Browser-Based	★★★★☆	

Fig:43 (ii) Application control – Social Media category

Name ▲	Category ▼	Technology ▼	Popularity ▼	Risk ▼
Reddit_Post	Social.Media	Browser-Based	★★★★★	
Renren	Social.Media	Browser-Based	★★★★☆	
Renren_Apps	Social.Media	Browser-Based	☆☆☆☆☆	
Renren_Posting	Social.Media	Browser-Based	☆☆☆☆☆	
Sarahah	Social.Media	Browser-Based, Client-Server	★★★★☆	
Sina.Services	Social.Media	Browser-Based	★★★★★	
Sina.Weibo	Social.Media	Browser-Based	★★★★★	
Sina.Weibo_Post	Social.Media	Browser-Based	★★★★☆	
Snapchat	Social.Media	Client-Server	★★★★★	
Sohu	Social.Media	Browser-Based	★★★★★	
Tapatalk	Social.Media	Browser-Based	★★★★☆	
Taringa	Social.Media	Browser-Based	★★★★☆	
Tellagami	Social.Media	Client-Server	☆☆☆☆☆	
Tencent.Weibo	Social.Media	Browser-Based	★★★★★	
Tencent.Weibo_Login	Social.Media	Browser-Based	★★★★☆	
Tencent.Weibo_Publish.Message	Social.Media	Browser-Based	☆☆☆☆☆	
Tianya.BBS	Social.Media	Browser-Based	★★★★☆	
Tinder	Social.Media	Client-Server	★★★★★	
To.Be.Honest	Social.Media	Client-Server	★★★★★	
Trippy	Social.Media	Browser-Based	☆☆☆☆☆	
Tuenti	Social.Media	Client-Server	★★★★☆	
Tumblr	Social.Media	Browser-Based	★★★★★	

Fig: 43 (iii) Application control – Social Media category

4.22 Application control – Storage Backup category

This category controls the flow of application in the internet link. The below figure shows the various categories using this standard for storage backup category.

Select All		Category: Storage.Backup	All Cloud	Selected: 0 / 2085
Name	Category	Technology	Popularity	Risk
4shared	Storage.Backup	Browser-Based, Client-Server	★★★★★	■■■■■
4shared_File.Download	Storage.Backup	Browser-Based, Client-Server	★★★★☆	■■■■■
4shared_File.Upload	Storage.Backup	Browser-Based, Client-Server	★★★★☆	■■■■■
360.Yunpan	Storage.Backup	Browser-Based, Client-Server	★★★★☆	■■■■■
360.Yunpan_File.Download	Storage.Backup	Browser-Based, Client-Server	★★★☆☆	■■■■■
360.Yunpan_File.Upload	Storage.Backup	Browser-Based, Client-Server	★★★☆☆	■■■■■
360.Yunpan_Login	Storage.Backup	Browser-Based, Client-Server	★★★☆☆	■■■■■
Accellion	Storage.Backup	Client-Server	★★★★☆	■■■■■
Acrobat.Cloud	Storage.Backup	Browser-Based	★★★★★	■■■■■
Acrobat.Cloud_Download	Storage.Backup	Browser-Based	★★★☆☆	■■■■■
Acrobat.Cloud_Upload	Storage.Backup	Browser-Based	★★★☆☆	■■■■■
ADFS	Storage.Backup	Network-Protocol	★★★☆☆	■■■■■
Adobe.Creative.Cloud	Storage.Backup	Browser-Based	★★★★☆	■■■■■
Adobe.Creative.Cloud_File.Download	Storage.Backup	Browser-Based	★★★☆☆	■■■■■
Adobe.Creative.Cloud_File.Upload	Storage.Backup	Browser-Based	★★★☆☆	■■■■■
Adobe.Send.Track	Storage.Backup	Browser-Based	★★★☆☆	■■■■■
ADrive	Storage.Backup	Browser-Based, Client-Server	★★★★☆	■■■■■
AFS	Storage.Backup	Client-Server	★★★☆☆	■■■■■
Amazon.Cloud.Drive	Storage.Backup	Browser-Based	★★★★☆	■■■■■
Amazon.Cloud.Drive_File.Download	Storage.Backup	Browser-Based	★★★☆☆	■■■■■
Amazon.Cloud.Drive_File.Upload	Storage.Backup	Browser-Based	★★★☆☆	■■■■■
Amazon_Login	Storage.Backup	Browser-Based	★★★☆☆	■■■■■

Fig: 44 (i) Application control – Storage backup category

Name	Category	Technology	Popularity	Risk
Cubby	Storage.Backup	Client-Server	★★★★☆	■■■■■
CVSup	Storage.Backup	Client-Server	★★★☆☆	■■■■■
Diino	Storage.Backup	Browser-Based	★★★☆☆	■■■■■
Dropbox	Storage.Backup	Browser-Based	★★★★★	■■■■■
Dropbox.Lan.Sync.Discovery.Protocol	Storage.Backup	Client-Server	★★★★☆	■■■■■
Dropbox_File.Download	Storage.Backup	Browser-Based	★★★☆☆	■■■■■
Dropbox_File.Edit	Storage.Backup	Browser-Based	★★★☆☆	■■■■■
Dropbox_File.Upload	Storage.Backup	Browser-Based	★★★☆☆	■■■■■
Dropbox_Login	Storage.Backup	Browser-Based	★★★☆☆	■■■■■
Droplr	Storage.Backup	Browser-Based, Client-Server	★★★☆☆	■■■■■
Droplr_Download	Storage.Backup	Browser-Based, Client-Server	★★★☆☆	■■■■■
Droplr_Link	Storage.Backup	Browser-Based, Client-Server	★★★☆☆	■■■■■
Droplr_Preview	Storage.Backup	Browser-Based, Client-Server	★★★☆☆	■■■■■
Droplr_Upload	Storage.Backup	Browser-Based, Client-Server	★★★☆☆	■■■■■
DropSend	Storage.Backup	Browser-Based, Client-Server	★★★★☆	■■■■■
DropSend_File.Upload	Storage.Backup	Browser-Based, Client-Server	★★★☆☆	■■■■■
Druva.InSync	Storage.Backup	Browser-Based, Client-Server	★★★☆☆	■■■■■
eFolder	Storage.Backup	Browser-Based, Client-Server	★★★★☆	■■■■■
Egnyte	Storage.Backup	Browser-Based	★★★★☆	■■■■■
Egnyte_File.Download	Storage.Backup	Browser-Based	★★★☆☆	■■■■■
Egnyte_File.Upload	Storage.Backup	Browser-Based	★★★☆☆	■■■■■
ElephantDrive	Storage.Backup	Browser-Based, Client-Server	★★★☆☆	■■■■■

Fig: 45 (ii) Application control – Storage backup category

☐ Select All	☒ Category: Storage.Backup	Add Filter	☒ All Cloud	Selected: 0 / 208
Name	Category	Technology	Popularity	Risk
 iCloud_Login	Storage.Backup	Browser-Based	★★★★☆	
 Insync	Storage.Backup	Client-Server	★★★★☆	
 Insync_File.Download	Storage.Backup	Client-Server	★★★★☆	
 InterSystems.Cache	Storage.Backup	Client-Server	★★★★☆	
 JDI.Backup	Storage.Backup	Client-Server	★★★★☆	
 Jianguoyun	Storage.Backup	Client-Server	★★★★☆	
 Jianguoyun_Download	Storage.Backup	Client-Server	★★★★☆	
 Jianguoyun_Upload	Storage.Backup	Client-Server	★★★★☆	
 JumboMail	Storage.Backup	Browser-Based	★★★★☆	
 KT.Ucloud	Storage.Backup	Browser-Based	★★★★☆	
 KT.Ucloud_Download	Storage.Backup	Browser-Based	★★★★☆	
 KT.Ucloud_Upload	Storage.Backup	Browser-Based	★★★★☆	
 LastPass	Storage.Backup	Client-Server	★★★★☆	
 Letty	Storage.Backup	Client-Server	★★★★☆	
 Mail.Ru_Cloud	Storage.Backup	Client-Server	★★★★☆	
 MediaFire	Storage.Backup	Browser-Based	★★★★★	
 MediaFire_File.Download	Storage.Backup	Browser-Based	★★★★☆	
 MediaFire_File.Upload	Storage.Backup	Browser-Based	★★★★☆	
 Mega	Storage.Backup	Browser-Based	★★★★☆	
 Mendeley	Storage.Backup	Browser-Based	★★★★☆	
 Mozy	Storage.Backup	Client-Server	★★★★☆	
 Naver.Cloud	Storage.Backup	Browser-Based	★★★★☆	

Fig: 45 (iii) Application control – Storage backup category

Name ▲	Category ▲	Technology ▲	Popularity ▲	Risk ▲
 Sina.Vdisk_File.Upload	Storage.Backup	Client-Server	★★★★☆	
 Slideshare	Storage.Backup	Browser-Based	★★★★★	
 Slideshare_File.Download	Storage.Backup	Browser-Based	★★★★☆	
 Slideshare_File.Upload	Storage.Backup	Browser-Based	★★★★☆	
 SOS.Online.Backup	Storage.Backup	Client-Server	★★★★☆	
 SpiderOak	Storage.Backup	Browser-Based	★★★★☆	
 Studiopass	Storage.Backup	Browser-Based, Client-Server	★★★★☆	
 SugarSync	Storage.Backup	Browser-Based, Client-Server	★★★★☆	
 SugarSync_File.Download	Storage.Backup	Browser-Based, Client-Server	★★★★☆	
 SugarSync_File.Upload	Storage.Backup	Browser-Based, Client-Server	★★★★☆	
 Symform	Storage.Backup	Client-Server	★★★★☆	
 Synology.DSM	Storage.Backup	Browser-Based, Client-Server	★★★★☆	
 TeamDrive	Storage.Backup	Browser-Based, Client-Server	★★★★☆	
 TeamDrive_Upload	Storage.Backup	Client-Server	★★★★☆	
 Totodisk	Storage.Backup	Browser-Based	★★★★☆	
 Ulozto	Storage.Backup	Browser-Based	★★★★☆	
 Veritas.Backup.Exec	Storage.Backup	Client-Server	★★★★☆	
 Veritas.NetBackup	Storage.Backup	Client-Server	★★★★☆	
 WatchDox	Storage.Backup	Browser-Based	★★★★☆	
 WebHard	Storage.Backup	Browser-Based	★★★★☆	
 WeTransfer	Storage.Backup	Browser-Based	★★★★☆	
 WeTransfer_File.Download	Storage.Backup	Browser-Based	★★★★☆	

Fig:45 (iv) Application control – Storage backup category

4.23 Application control – Update category

This category controls the flow of application in the internet link. The below figure shows the various categories using this standard for update category.

☐ Select All

x Category: Update
 x All Cloud
 Selected: 0 / 208!

Name	Category	Technology	Popularity	Risk
360.Safeguard.Update	Update	Client-Server	★★★★★	
Adobe.Update	Update	Client-Server	★★★★★	
ALTools.Update	Update	Client-Server	★★★★☆	
ALYac.Update	Update	Client-Server	★★★☆☆	
Apple.Software.Update	Update	Client-Server	★★★★★	
Apt-Get	Update	Client-Server	★★★★★	
Avast.Update	Update	Client-Server	★★★★★	
AVG.Update	Update	Client-Server	★★★★★	
Avira.Update	Update	Client-Server	★★★★★	
Bitdefender.Update	Update	Client-Server	★★★★☆	
Chrome.Update	Update	Browser-Based	★★★★★	
Dell.Update	Update	Client-Server	★★★☆☆	
Driver.Booster.Update	Update	Client-Server	★★★☆☆	
Duba.Update	Update	Client-Server	★★★★☆	
Firefox.Update	Update	Client-Server	★★★★★	
Flexera.PSI	Update	Client-Server	★★★★☆	
FortiClient	Update	Client-Server	★★★★☆	
InstallAnywhere.Update	Update	Client-Server	★★★☆☆	
Intel.Resource.Download	Update	Client-Server	★★★★★	
iTunes_Update	Update	Client-Server	★★★★☆	
Java.Update	Update	Client-Server	★★★★☆	
Kaspersky.Update	Update	Client-Server	★★★★★	

Fig:46 Application control – Update category

4.24 Application control – Video /Audio category

This category controls the flow of application in the internet link. The below figure shows the various categories using this standard.

☐ Select All	Category: Video/Audio	All	Cloud	Selected: 0 / 208
Name	Category	Technology	Popularity	Risk
1kxun	Video/Audio	Client-Server	★★★★☆	■■■■■
8tracks	Video/Audio	Browser-Based, Client-Server	★★★★☆	■■■■■
ABC.Com	Video/Audio	Browser-Based	★★★★☆	■■■■■
Adobe.Flash.Media.Playback	Video/Audio	Client-Server	★★★★☆	■■■■■
Air.Video	Video/Audio	Client-Server	★★★★☆	■■■■■
Airtime	Video/Audio	Browser-Based	★★★★☆	■■■■■
AllMusic	Video/Audio	Browser-Based	★★★★☆	■■■■■
Amazon.Music	Video/Audio	Browser-Based, Client-Server	★★★★☆	■■■■■
Amazon.Video	Video/Audio	Browser-Based	★★★★☆	■■■■■
AP.Archive	Video/Audio	Browser-Based	★★★★☆	■■■■■
Apple.Daily.Video	Video/Audio	Browser-Based	★★★★☆	■■■■■
aTube.Catcher	Video/Audio	Client-Server	★★★★☆	■■■■■
Baidu.Player	Video/Audio	Peer-to-Peer	★★★★☆	■■■■■
Baofeng	Video/Audio	Peer-to-Peer	★★★★☆	■■■■■
BBC.iPlayer	Video/Audio	Browser-Based	★★★★☆	■■■■■
Bigo.Live	Video/Audio	Client-Server	★★★★☆	■■■■■
Brightcove	Video/Audio	Browser-Based	★★★★☆	■■■■■
Cienradios	Video/Audio	Browser-Based	★★★★☆	■■■■■
CNLive	Video/Audio	Browser-Based, Client-Server	★★★★☆	■■■■■
CNN.Video	Video/Audio	Browser-Based	★★★★☆	■■■■■
CNTV	Video/Audio	Browser-Based	★★★★☆	■■■■■
Comedy.Central	Video/Audio	Browser-Based	★★★★☆	■■■■■

Fig: 47 (i) Application control – Video /Audio category

Name	Category	Technology	Popularity	Risk
iTunes_Podcast	Video/Audio	Client-Server	★★★★☆	■■■■■
iTunes_Select.Play	Video/Audio	Client-Server	★★★★☆	■■■■■
iTunes_Store	Video/Audio	Browser-Based	★★★★☆	■■■■■
Jango	Video/Audio	Browser-Based	★★★★☆	■■■■■
Kboing.Music	Video/Audio	Client-Server	★★★★☆	■■■■■
KeyholeTV	Video/Audio	Client-Server	★★★★☆	■■■■■
Kodi	Video/Audio	Client-Server	★★★★☆	■■■■■
Ku6	Video/Audio	Browser-Based	★★★★☆	■■■■■
Kugou	Video/Audio	Peer-to-Peer	★★★★☆	■■■■■
Kuwo.Music	Video/Audio	Browser-Based	★★★★☆	■■■■■
Last.FM	Video/Audio	Browser-Based	★★★★☆	■■■■■
LeTV	Video/Audio	Browser-Based	★★★★☆	■■■■■
Livestream	Video/Audio	Browser-Based	★★★★☆	■■■■■
MediaMonkey	Video/Audio	Client-Server	★★★★☆	■■■■■
MelOn	Video/Audio	Browser-Based	★★★★☆	■■■■■
Metacafe	Video/Audio	Browser-Based	★★★★☆	■■■■■
Miro	Video/Audio	Client-Server	★★★★☆	■■■■■
MMSH	Video/Audio	Network-Protocol	★★★★☆	■■■■■
MPEG.TS	Video/Audio	Network-Protocol	★★★★☆	■■■■■
Napster	Video/Audio	Browser-Based	★★★★☆	■■■■■
Naver.Livestream	Video/Audio	Browser-Based	★★★★☆	■■■■■
NBA.Video	Video/Audio	Browser-Based	★★★★☆	■■■■■

Fig: 48 (ii) Application control – Video /Audio category

Name	Category	Technology	Popularity	Risk
SHOUTcast	Video/Audio	Client-Server	★★★★☆	■ ■ ■ ■ ■
Showtime.Anytime	Video/Audio	Browser-Based, Client-Server	★★★★☆	■ ■ ■ ■ ■
Sina.Video	Video/Audio	Browser-Based	★★★★☆	■ ■ ■ ■ ■
Sky.Go	Video/Audio	Client-Server	★★★☆☆	■ ■ ■ ■ ■
Slacker	Video/Audio	Browser-Based	★★★★☆	■ ■ ■ ■ ■
Sling.TV	Video/Audio	Browser-Based	★★★★★	■ ■ ■ ■ ■
Smilebox	Video/Audio	Client-Server	★★★★☆	■ ■ ■ ■ ■
Sohu.TV	Video/Audio	Browser-Based	★★★★☆	■ ■ ■ ■ ■
Songr	Video/Audio	Client-Server	★★★☆☆	■ ■ ■ ■ ■
Soribada	Video/Audio	Browser-Based	★★★☆☆	■ ■ ■ ■ ■
SoundCloud	Video/Audio	Client-Server	★★★★★	■ ■ ■ ■ ■
Spotify	Video/Audio	Client-Server	★★★★★	■ ■ ■ ■ ■
Stitcher	Video/Audio	Client-Server	★★★★☆	■ ■ ■ ■ ■
Stream.Media	Video/Audio	Browser-Based	★★★★★	■ ■ ■ ■ ■
Streambox	Video/Audio	Client-Server	★★★☆☆	■ ■ ■ ■ ■
SuperLivePro	Video/Audio	Client-Server	★★★☆☆	■ ■ ■ ■ ■
SVT.Play	Video/Audio	Browser-Based	★★★★☆	■ ■ ■ ■ ■
Tagoo	Video/Audio	Browser-Based	★★★☆☆	■ ■ ■ ■ ■
TED	Video/Audio	Browser-Based, Client-Server	★★★★☆	■ ■ ■ ■ ■
Tencent.Video	Video/Audio	Browser-Based	★★★★★	■ ■ ■ ■ ■
TikTok	Video/Audio	Client-Server	★★★★☆	■ ■ ■ ■ ■
Time.Warner.Cable_Video	Video/Audio	Browser-Based	★★★★☆	■ ■ ■ ■ ■

Fig: 49 (iii) Application control – Video /Audio category

Name	Category	Technology	Popularity	Risk
YouTube	Video/Audio	Browser-Based	★★★★★	■ ■ ■ ■ ■
YouTube.Downloader.YTD	Video/Audio	Client-Server	★★★★★	■ ■ ■ ■ ■
YouTube_Channel.Access	Video/Audio	Browser-Based	★★★★★	■ ■ ■ ■ ■
YouTube_Channel.ID	Video/Audio	Browser-Based	★★★★★	■ ■ ■ ■ ■
YouTube_Comment.Posting	Video/Audio	Browser-Based	★★★☆☆	■ ■ ■ ■ ■
YouTube_HD.Streaming	Video/Audio	Browser-Based	★★★★★	■ ■ ■ ■ ■
YouTube_Search.Safety.Mode.Off	Video/Audio	Browser-Based	★★★★☆	■ ■ ■ ■ ■
YouTube_Search.Video	Video/Audio	Browser-Based	★★★★☆	■ ■ ■ ■ ■
YouTube_Video.Access	Video/Audio	Browser-Based	★★★★★	■ ■ ■ ■ ■
YouTube_Video.Embedded	Video/Audio	Browser-Based	★★★★★	■ ■ ■ ■ ■
YouTube_Video.Play	Video/Audio	Browser-Based	★★★☆☆	■ ■ ■ ■ ■
YouTube_Video.Upload	Video/Audio	Browser-Based	★★★☆☆	■ ■ ■ ■ ■
Zattoo	Video/Audio	Browser-Based	★★★☆☆	■ ■ ■ ■ ■
Zune	Video/Audio	Client-Server	★★★☆☆	■ ■ ■ ■ ■

Fig: 49 (iv) Application control – Video /Audio category

4.25 IPS sensor

IPS sensor signature are shown below, can be setup with block or quarantine actions. The sensor signature can be modified to block the network activity based on its behavior.

Edit IPS Sensor				protect_client			
Enable	Signature	Threshold	Duration (seconds)	Track By	Action	Block Duration (min)	
☐	Apache.Tomcat.HTTP2.DoS	50	2	Any	 Block	None	
☐	Cisco.Adaptive.Security.Appliance.SIP.Handling.DoS	100	1	Any	 Block	None	
☐	Digium.Asterisk.Chan.skinny.SCCP.Memory.Exhaustion.DoS	100	10	Any	 Block	None	
☐	Digium.Asterisk.INVITE.TCP.Connection.Close.DoS	5	1	Any	 Block	None	
☐	DotNetNuke.Padding.Oracle.Attack	1000	5	Any	 Block	None	
☐	FTP.Login.Brute.Force	200	10	Any	 Block	None	
☐	Flexense.HTTP.Server.HTTP.Header.DoS	20	1	Any	 Block	None	
☐	FreeBSD.TCP.Reassembly.DoS	10	2	Any	 Block	None	
☐	IMAP.Login.Brute.Force	60	10	Any	 Block	None	
☐	MS.Active.Directory.LDAP.Packet.Handling.DoS	100	1	Any	 Block	None	
☐	MS.IIS.HTTP2.SETTINGS.FRAME.DoS	200	5	Any	 Block	None	
☐	MS.OWA.Brute.Force	15	1	Any	 Block	None	
☐	MS.RDP.Connection.Brute.Force	2000	1	Any	 Block	None	
☐	MS.SMB.CVE-2019-0633.Remote.Code.Execution	20	5	Any	 Block	None	

Fig:50 IPS sensor

Edit Filter ✕					
✕ Target: client + Add Filter ✕					
Name ⬇	Severity ⬇	Target ⬇	OS ⬇		
Adobe.Acrobat.CVE-2018-15985.Memory.Corruption		Server, Client	Windows, Linux, MacOS	TCP, HTTP, FT	^
Adobe.Acrobat.CVE-2018-15986.Memory.Corruption		Server, Client	Windows, Linux, MacOS	TCP, HTTP, FT	
Adobe.Acrobat.CVE-2018-15987.Memory.Corruption		Server, Client	Windows, Linux, MacOS	TCP, HTTP, FT	
Adobe.Acrobat.CVE-2018-15991.Memory.Corruption		Server, Client	Windows, Linux, MacOS	TCP, HTTP, FT	
Adobe.Acrobat.CVE-2018-15992.Memory.Corruption		Server, Client	Windows, Linux, MacOS	TCP, HTTP, FT	
Adobe.Acrobat.CVE-2018-15993.Memory.Corruption		Server, Client	Windows, Linux, MacOS	TCP, HTTP, FT	
Adobe.Acrobat.CVE-2018-15994.Memory.Corruption		Server, Client	Windows, Linux, MacOS	TCP, HTTP, FT	
Adobe.Acrobat.CVE-2018-15995.Memory.Corruption		Server, Client	Windows, Linux, MacOS	TCP, HTTP, FT	
Adobe.Acrobat.CVE-2018-15996.Memory.Corruption		Server, Client	Windows, Linux, MacOS	TCP, HTTP, FT	
Adobe.Acrobat.CVE-2018-16001.Out.of.Bounds.Read		Server, Client	Windows, Linux, MacOS	TCP, HTTP, FT	
Adobe.Acrobat.CVE-2018-16002.Out.of.Bounds.Read		Server, Client	Windows, Linux, MacOS	TCP, HTTP, FT	⌵
<< < 1 /71 > >> [Total: 3530]					

Severity ⬇	Target ⬇	OS ⬇	Service ⬇	Action ⬇
	Server	Windows	TCP, FTP	Block
	Server	Windows	TCP, HTTP	Block
	Server	Linux	TCP, HTTP	Block
	Client	Windows	TCP, HTTP	Block
	Server	Windows	TCP	Block
	Server, Client	Windows	TCP, HTTP, FTP, SMTP, POP3, IMAP, NNTP	Block
	Server	Other	TCP, HTTP	Block
	Server, Client	All	TCP	Block
	Server	All	UDP, DNS	Block
	Client	All	TCP	Block
	Server, Client	Windows	TCP, SMTP, HTTP	Block
	Server	All	TCP, HTTP	Block
	Server	Windows, Linux, BSD, Solaris, MacOS	TCP, HTTP	Block
	Server	Linux, BSD	TCP, HTTP	Block
	Server	Linux, BSD	TCP, HTTP	Block
	Server	Linux	TCP, HTTP	Block
	Server	Windows	TCP	Block
	Server	Linux, BSD	TCP, HTTP	Block
	Client	Windows	TCP, HTTP	Block
	Server	All	TCP, HTTP	Block
	Server	Windows	TCP, HTTP	Block

Fig:50 Edit filter – IPS filters

The Above Figures demonstrates , the IPS sensors , which are signature based and can be applied to the firewall rules , internally and externally , the action field displays the action in case of the event match to the rule.

4.26 SSL inspection

Edit SSL/SSH Inspection Profile

The default profile is read only.

Name

certificate-inspection

Comments

Read-only SSL handshake inspection profile.

43/255

SSL Inspection Options

Enable SSL Inspection of

Multiple Clients Connecting to Multiple Servers

Protecting SSL Server

Inspection Method

SSL Certificate Inspection

Full SSL Inspection

CA Certificate

Fortinet_CA_SSL

Download Certificate

Protocol Port Mapping

Inspect All Ports

☐

HTTPS

☒

443

SSH Inspection Options

SSH Deep Scan

☐

Fig:51 SSL/SSH Inspection Profile

The above figure, displays the security features that is enabled on the traffic which is SSL enabled , the SSL traffic is checked using certificate inspection , Sites with invalid certificates can be allowed as exceptions.

4.27 Logs and reports of events

The setup is capable of the below Log and events , to monitor the operations of the network , it is important the logs are check periodically and any anomalies are acted upon with due care , along with the monitoring we can setup automated email alerts based on the type of the event , where an email would be triggered without human intervention , below is the figure which display the events with which alerts can be triggered to the IT administrator.

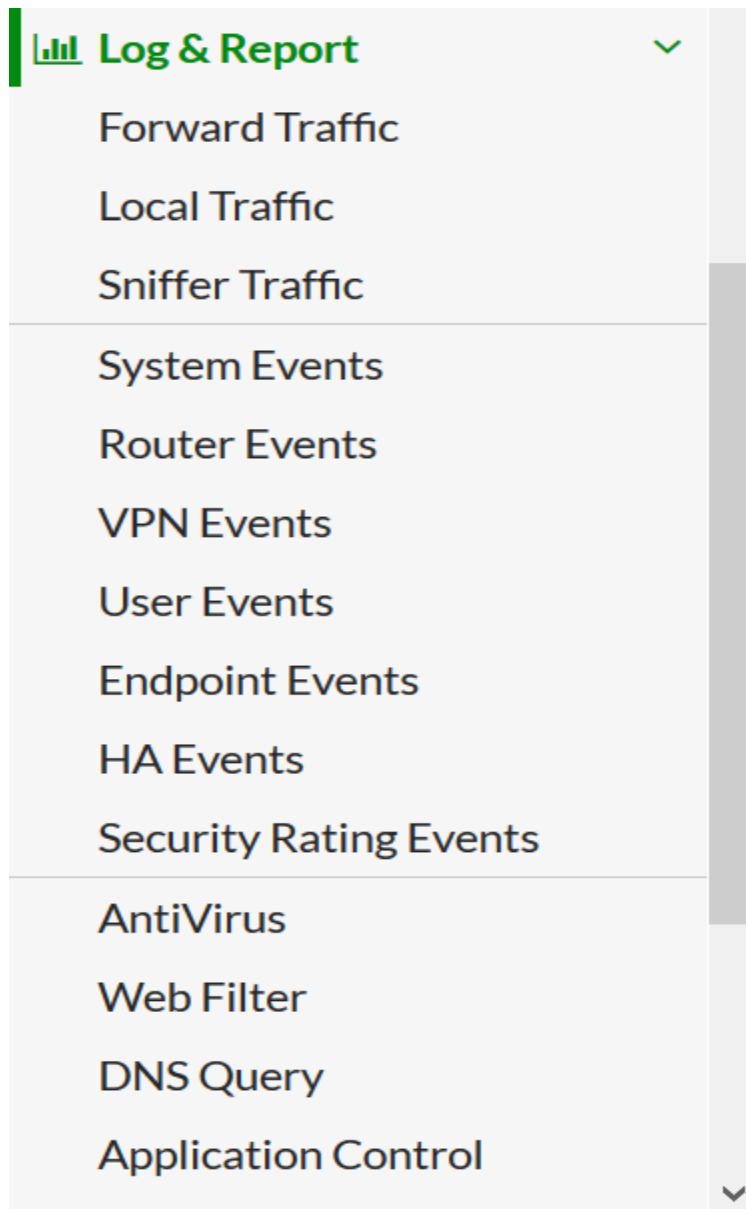
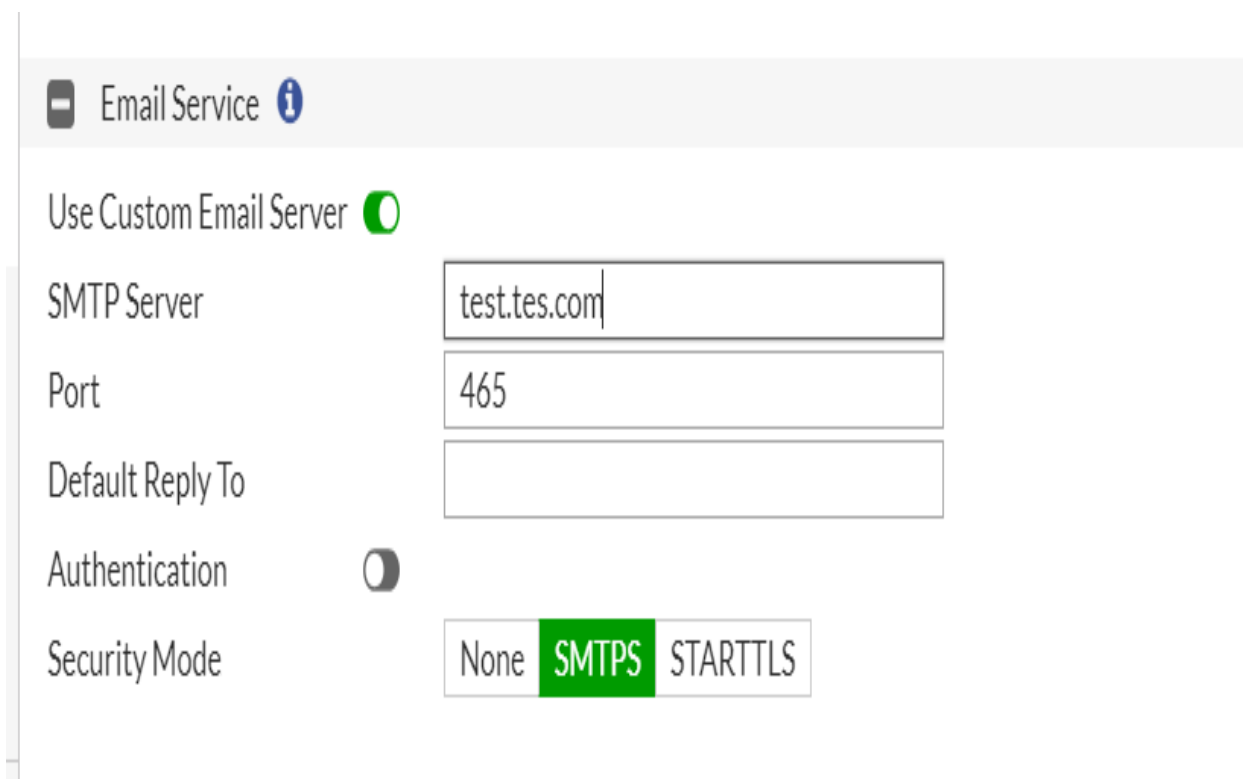


Fig 52: Logs and report of events

The below figure email alert system, for the security events. Which consist of following fields such as SMTP server, Port , default reply to, authentication and security mode. In this implementation port 465 is used as the SMTP for communication.



The screenshot shows a configuration window titled "Email Service" with a minus icon and an information icon. It contains several settings:

- Use Custom Email Server:** A toggle switch that is turned on (green).
- SMTP Server:** A text input field containing "test.tes.com".
- Port:** A text input field containing "465".
- Default Reply To:** An empty text input field.
- Authentication:** A toggle switch that is turned off (grey).
- Security Mode:** A selection box with three options: "None", "SMTPS" (which is highlighted in green), and "STARTTLS".

Fig:53 Email Service

The alert can be set up for security, which as intrusion detection, web filter, policy denied traffic. Administrative setup consist of disk usage, administrative login, configuration change, authentication and HA status change.

Email Alert Settings

Enabled ☒

From

To

+

Alert parameter

Events

Severity

Interval

5

Security

Intrusion detected

Virus detected

Web Filter blocked traffic

Policy denied traffic

Administrative

Disk usage exceeds

FortiGuard renewal due within

Administrator login/logout

Configuration change

Firewall authentication failure

HA status change

Fig 54: Email alert Setting

4.28 Firewall Policy summary

Below is the figure which displays the summary of the firewall policies , the directions are internal to internal & internal to external (WAN – internet facing) and vice versa , each policy can be enables with the security standards discussed above in a granular method .

ID	Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
Abari internet (wan1) → Camera Network (port3) 1										
31	camera	all	Camera	always	ALL	✓ ACCE...	✓ Ena...	AV default SSL certificate-in:	U...	73.81 Mf
Abari internet (wan1) → Lan&Phone (port1) 3										
32	Rdp	all	Cellcity Wk	always	RDP	✓ ACCE...	✓ Ena...	AV default IPS high_security SSL certificate-in:	U...	4.16 Gf
33	sql-mon...	Blueke	SQL-MON-	always	SQL-M	✓ ACCE...	✓ Ena...	AV default IPS high_security SSL certificate-in:	U...	0 f
34	pabx	all	PABX	always	ALL	✓ ACCE...	✓ Ena...	AV default IPS high_security SSL certificate-in:	U...	22.17 Mf
Lan&Phone (port1) → Abari internet (wan1) 3										
35	Exeption...	cc-sap CC-ser CC_SA Except SAP se	all	always	ALL	✓ ACCE...	✓ Ena...	AV default WEB DYN-Prevelig DNS default APP DYN-Prevelig +2	U...	110.66 Gf
36	STaff-Lan	all	all	always	ALL	✓ ACCE...	✓ Ena...	AV default WEB Staff-LAN-D DNS default APP Staff-LAN-D +2	U...	65.16 Gf
42	Deny	all	all	always	ALL	✗ DENY			✓ All	0 f
Wifi Network (port4) → Abari internet (wan1) 2										
40	exceptio...	Wirele	all	always	ALL	✓ ACCE...	✓ Ena...	AV default WEB DYN-Prevelig DNS default APP DYN-Prevelig +2	U...	80.53 Gf
41	Wireless...	all	all	always	ALL	✓ ACCE...	✓ Ena...	AV default	U...	117.59 Gf

Fig 55: Firewall Policy summary

4.29 Granular Firewall Policy configuration – with Security standards enabled.

Below is the figure which demonstrates a policy with all security standards, discussed above each of the standard is enabled after it is being created as a profile.

Edit Policy

Name ⓘ

Preveliged-Lan

Incoming Interface

DYNAGROW LAN (lan1)

Outgoing Interface

BBI internet (wan)

Source

jags pc - lan

+

Destination

all

+

Schedule

always

Service

ALL

+

Action

✓ ACCEPT

✗ DENY

📖 LEARN

Firewall / Network Options

NAT

☒

IP Pool Configuration

Use Outgoing Interface Address

Use Dynamic IP Pool

Security Profiles

AntiVirus

☒

AV

DYN-Common

✎

Web Filter

☐

Application Control

☒

APP

Preveliged

✎

Proxy Options

☒

PRX

default

✎

SSL Inspection

☒

SSL

certificate-inspection

✎

Logging Options

Log Allowed Traffic

☒

Security Events

All Sessions

Comments

Write a comment...

0/1023

OK

Cancel

Fig 56: Granular Firewall Policy configuration – with Security standards enabled

104

4.30 Firewall compliance & Up to date definitions

It is important that the subscription on the device is active, as every day new threats are evolving and being spread across the internet, it is paramount that the firewall is up to date with the new updates, below is the figure which demonstrates the device compliance and the date of the release of the relevant updates.

Hardware Version	✔ Advanced hardware - expires on 2020/02/25	
Enhanced Support	✔ 24x7 support - expires on 2020/02/25	
Firmware & General Updates	✔ Licensed - expires on 2020/02/25	
Application Control Signatures	🕒 Version 14.00605	⊕ Upgrade Database
Device & OS Identification	🕒 Version 1.00074	
Internet Service Database Definitions	🕒 Version 5.00575	
Intrusion Prevention	✔ Licensed - expires on 2020/02/25	
IPS Definitions	🕒 Version 14.00605	⊕ Upgrade Database
IPS Engine	🕒 Version 4.00029	
Malicious URLs	🕒 Version 2.00183	
AntiVirus	✔ Licensed - expires on 2020/02/25	
AV Definitions	🕒 Version 68.00217	⊕ Upgrade Database

Fig 57: Firewall compliance & Up to date definitions

CHAPTER – V
RECOMMENDATION

CHAPTER - 5

5.1 Recommendation

From the research, the following recommendation should be taken into consideration before designing a infrastructure for any corporate network.

1. Select a suitable firewall based on security requirements
2. Configuring the security standards as per the best practices
3. Monitoring of security events and recording using syslogs server
4. Use single sign-on wherever possible
5. Use web filtering by blocking all and allowing what is needed
6. Use Application filtering by blocking all and allowing what is needed
7. Use DNS filtering by blocking all and allowing what is needed
8. Use IPS filtering by blocking all and allowing what is needed
9. Segregate important areas of the network
10. Use proxy-based packet scanning rather than flow based
11. Use SSL inspection
12. Update the firewall firmware for performance and accuracy
13. Use VPNs for remote access
14. Use vulnerability scanning tools on the network frequently

- 15. Monitor bad logon attempt to the firewall
- 16. Setup automated network isolation in the event of system compromise detection
- 17. Restrict access to the firewall configuration only from trusted host
- 18. Manage separate login credential for the firewall administrator with segregation of duty

CHAPTER – VI
CONCLUSION AND FUTURE RESEARCH

CHAPTER - 6

6. Conclusion and Future research

6.1 Conclusion

In this research, a secure network environment has been created using the firewall security standard based on the company security policy. It is paramount that the security standards are optimized based on the security guideline as per the best practices and industry standards. This research has been carried out in the real time environment to prove the robustness of the environment against malware attacks and system compromise event, hence reducing the downtime and loss of data integrity.

It is evident from the implementation that the current firewall setup configuration can safeguard network environment incase of system breaches and compromise. The security standards such as web filtering, content filtering, DNS filtering, application control, IPS and network segregation play a major role in securing the environment against any possible attack on the network.

6.2 Future research

In order for the security standard to work effectively it is important that the definitions are regularly updated to secure the network against nature of Zero-day attack. This research can be further carried by implementing network segregation in conjunction with the security standard discussed in the above research.

“References

- [1] Imran et al., "Role of Firewall Technology in Network Security", International Journal of Innovations & Advancement in Computer Science, Vol. 4, Issue.12, (2016).
- [2] Taluja, Sachin, and Pradeep Kumar, “Network Security Using IP Firewalls”, International Journal of Advanced Research in Computer Science and Software Engineering Vol.2, Issue: 8 ,2012
- [3] Malik and Pal , ” Impact of Firewall and VPN for WLAN”, International Journal of Advanced Research in Computer Science and Software Engineering, 2013.
- [4] Bhanot, Amit, and Leena Jain., “Implementing Network Security Policies: Packet Filtering Mechanism”. International Journal of Emerging Trends and Technology in computer Science, Vol 2, No..3 ,2013
- [5] V, Selvi, Sankar R, and Umarani R. “The Design and Implementation of On-Line Examination Using Firewall Security”. IOSR Journal of Computer Engineering, Vol. 16, No.6 ,2016.
- [6] Sharma, Bhisham, and Karan Bajaj. "Packet Filtering Using IP Tables in Linux". IJCSI International Journal of Computer Science Issues 8.4 (2011): 6. Print. [06.02.2016].
- [7] Gaud, J.V., and Bartere, M.M., “Data Security Based on LAN Using Distributed Firewall”, International Journal of Computer Science and Mobile Computing (IJCSMC), Vol. 3, Issue. 3, March 2014.
- [8] Bhovare, S. R., and Chaudhari, B. K., “A Survey on Data Security Provided in Local Network Using Distributed Firewall”. International Journal of Research in Advent Technology, Vol. 2, No. 4, April 2014.
- [9] Warade, S. J., Tijare, P. A., & Sawalkar, S. N., “Data Security in Local Network using Distributed Firewall: A Review”. International Journal of Computer Applications (0975-8887), National Conference on Emerging Trends in Computer Technology (NCETCT-2014), pp: 19-21.
- [10] S. M. Goodreau, J. A. Kitts, and M. Morris, “Birds of a feather, or friend of a friend? Using exponential random graph models to investigate adolescent social networks,” Demography, vol. 46, No. 1, pp. 103–125, 2009.
- [11] E. D. Kolaczyk, Statistical Analysis of Network Data: Methods and Models, Springer, 1st edition, 2010.

- [12] K. Dombrowski, B. Khan, K. McLean et al., “A re-examination of connectivity trends via exponential random graph modeling in two IDU risk networks,” *Substance Use and Misuse*, vol. 49, 2012.
- [13] R. Curtis, S. R. Friedman, A. Neaigus, B. Jose, M. Goldstein, and G. Ildefonso, “Street-level drug markets: network structure and HIV risk,” *Social Networks*, vol. 17, no. 3-4, pp. 229–249, 1995.
- [14] Robert, “Simulation of truncated normal variables,” *Statistics and Computing*, vol. 5, pp. 121–125, 1995.
- [15] Goodreau, “Assessing the effects of human mixing patterns on human immunodeficiency virus-1 interhost phylogenetics through social network simulation,” *Genetics*, vol. 172, no. 4, pp. 2033–2045, 2006.
- [16] Des Jarlais, K. Arasteh, and S. R. Friedman, “HIV among drug users at beth israel medical center, new york city, the first 25 years,” *Substance Use and Misuse*, vol. 46, no. 2-3, pp. 131–139, 2011.
- [17] Friedman, R. Curtis, A. Neaigus, B. Jose, and D. C. D. Jarlais, *Social Networks, Drug Injectors’ Lives, and HIV/AIDS*, Springer, 1st edition, 2010.
- [18] Canghong Zhang, “Based on network security firewall technology, Information technology, Chinese new technology new product”, 2009.
- [19] Rui Wang. Haibo Lin, “Network security and firewall technology”, Tsinghua university publishing house, in 2000
- [20] Kuang Chu, “Network security and firewall technology”, Chongqing university publishing house, 2005
- [21] Rizwan rehman, et al, “Malware threats and mitigation strategies: A survey”; *Journal of Theoretical and Applied Information Technology*; 31st July 2011. Vol. 29 No.2.
- [22] Robert Moskovitch, “Detecting unknown malicious code by applying classification techniques on OpCode patterns”, Springer-Verlag “<http://link.springer.com/article/10.1186%2F2190-8532-1-1>” 2012.\.
- [23] Wildlist Organization, “Virus descriptions of viruses in the wild”. Online publication, 2000. <http://www.fsecure.com/virusinfo/wild.html>.
- [24] Yuval Elovici, et al, “Applying Machine Learning Techniques for Detection of Malicious Code in Network Traffic”. Vol:40, No.2, 2014.

- [25] ArunLakhotia ,AdityaKapoor , Eric Uday , “Are Metamorphic Viruses Really Invincible ? Part 2” , Virus Bulletin, January 2005.
- [26] Robin Sharp, An Introduction to Malware, Spring 2012. Retrieved on April, 10, 2013 http://orbit.dtu.dk/fedora/objects/orbit:82364/datastreams/file_4918204/content
- [27] A. H. Sung, J. Xu, P. Chavez and S. Mukkamala: Static Analyzer of Vicious Executables (SAVE), Proceedings of the 20th Annual Computer Security Applications Conference (ACSAC’04), IEEE
- [28].J.Rabek, R.Khazan, S.Lewandowski and R.Cunningham. Detection of injected, dynamically generated, and obfuscated malicious code. In Proceedings of the 2003 ACM Workshop on Rapid Malcode, pages 76–82, 2003.
- [29] G. McGraw and G. Morrisett. Attacking malicious code: A report to the infosec research council. IEEE Software, 17(5):33–44, 2000
- [30] Muazzam , ”Data Mining Methods for Malware Detection”: University of Central Florida, 2008.
- [31] T. Almeida, A. Yamakami, and J. Almeida, “Evaluation of approaches for dimensionality reduction applied with naive bayes antispam filters,” in Proceedings of the 8th IEEE International Conference on Machine Learning and Applications, Miami, FL, USA, December2009, pp. 1–6.
- [32] K. Schneider, “On word frequency information and negative evidence in naive bayes text classification,” in Proceedings of the 4th Inter-national Conference on Advances in Natural Language Processing, Alicante, Spain, October 2004, pp. 474–485.
- [33] D. Losada and L. Azzopardi, “Assessing multivariate bernoulli modelsfor information retrieval,” ACM Transactions on Information Systems, vol. 26, no. 3, pp. 1–46, June 2008.
- [34] J. Carpinter and R. Hunt, “Tightening the net: A review of current and next generation spam filtering tools,” Computers and Security, vol. 25, no. 8, pp. 566–578, 2006.
- [35] G. Cormack and T. Lynam, “Online supervised spam filter evaluation,” ACM Transactions on Information Systems, vol. 25, no. 3, pp. 1–11, 2007.
- [36] T. Almeida, A. Yamakami, and J. Almeida, “Filtering spams using the minimum description length principle,” in Proceedings of the 25th ACM Symposium On Applied Computing, Sierre, Switzerland, March 2010, pp. 1–5.
- [37] NIST Special Publication (SP) 800-45 Version 2, Guidelines on Electronic Mail Security (<http://csrc.nist.gov/publications/PubsSPs.html>)

- [38] NIST SP 800-94, Guide to Intrusion Detection and Prevention Systems (IDPS) (<http://csrc.nist.gov/publications/PubsSPs.html>).
- [39] NIST SP 800-52, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations and NIST SP 800-113, Guide to SSL VPNs (<http://csrc.nist.gov/publications/PubsSPs.html>).
- [40] NIST SP 800-114, User's Guide to Securing External Devices for Telework and Remote Access (<http://csrc.nist.gov/publications/PubsSPs.html>).
- [41] NIST SP 800-84, Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities, which is available at <http://csrc.nist.gov/publications/PubsSPs.html#800-84>.
- [42] S. Bellovin and W. Cheswick, "Network firewalls," Communications Magazine, IEEE, vol. 32, no. 9, pp. 50–57, Sept 1994.
- [43] M. Gouda and A. Liu, "A model of stateful firewalls and its properties," in Dependable Systems and Networks, 2005. DSN 2005. Proceedings. International Conference on, June 2005, pp. 128–137.
- [44] K. Ingham and S. Forrest, "A history and survey of network firewalls," University of New Mexico, Tech. Rep, 2002.
- [45] A. Atlasis, "Attacking ipv6 implementation using fragmentation," BlackHat Europe, 2012.
- [46] K. K. Frederick, "Abnormal ip packets," <http://www.symantec.com/connect/articles/abnormal-ip-packets>, Accessed: 2014-08-09.
- [47] M. Gouda and X.-Y. Liu, "Firewall design: consistency, completeness, and compactness," in Distributed Computing Systems, 2004. Proceedings. 24th International Conference on, 2004, pp. 320–327.
- [48] A. Liu and M. Gouda, "Diverse firewall design," Parallel and Distributed Systems, IEEE Transactions on, vol. 19, no. 9, pp. 1237–1251, Sept 2008.
- [49] A. Wool, "A quantitative study of firewall configuration errors," Computer, vol. 37, no. 6, pp. 62–67, June 2004.
- [51] "Trends in firewall configuration errors: Measuring the holes in swiss cheese," Internet Computing, IEEE, vol. 14, no. 4, pp. 58–65, July 2010.
- [52] D. Newman, "Bencharking Terminology for Firewall Performance," RFC 2647, August 1999."

“Books:

“[1] Kahate, A. Cryptography and Network Security. ISBN-13: 978- 0-07-064823-4, ISBN-10:0-07-64823-9, McGraw Hill Higher Education.

[2] Forouzan, B. A., & Mukhopadhyay, D. Cryptography and Network Security. ISBN-13:978-0-07-70208-0, ISBN-10: 0-07- 070208-X, Mc Graw Hill Higher Education.

[3] Stallings, W. Cryptography and Network Security Principles and Practices. ISBN-978-81-775-8774-6.

[4] Tanenbaum, A. S., Watherall, D. J. Computer Networks. ISBN13: 978-0132126953, ISBN-10: 0132126958, 5 th Edition, Paperback, 2010, pp: 34-39”."