National College of Ireland

Using Redundancy of Perimeter Firewall to Increase the Availability of Business Resources

MSc Research Project
MSc Cybersecurity (MSCCYB)

Rohan Yele
Student ID: X21203971

School of Computing
National College of Ireland

Supervisor: Prof. Mr. Michael Pantridge

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Rohan Yele		
Student ID:	X21203971		
Programme:	MSc Cybersecurity (MSCCYB1)	**Year:**	2023
Module:	Research Project		
Lecturer:	Prof. Mr. Michael Pantridge		
Submission Due Date:	18/09/2023		
Project Title:	Using Redundancy of Perimeter Firewall to Increase the Availability of Business Resources		
Word Count:	5168	**Page Count:**	19

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature:	Rohan Yele
Date:	18/09/2023

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Using Redundancy of Perimeter Firewall to Increase the Availability of Business Resources

Rohan Yele
X21203971
MSCCYB1
National College of Ireland

Abstract

The security of an organization's network infrastructure is critical for the success of its operations, and single points of failure in the network can pose significant risks to the organization. This research project aims to investigate the risks associated with single points of failure in an organization's infrastructure and the importance of redundancy, with a specific focus on the service availability and role of firewall redundancy in supporting business security architecture. The project will use simulation-based experiments to evaluate the effectiveness of service availability and firewall redundancy and improving the security and reliability of an organization's infrastructure. This will help organizations ensure the continuity of their critical business processes in the event of a security breach or any hardware link or system failures. The proposed research will provide valuable insights into the practical challenges and benefits of providing resource reliability and service availability by implementing firewall redundancy in real-world security scenarios and offer recommendations for its implementation. The results of this research can be used by organizations to improve the availability, security and reliability of their network infrastructure and ensure the protection of their critical business data.

Keywords: Availability; Firewall; Perimeter; Reliability; Redundancy; Security

1. Introduction

Availability is an important CIA traid in the information systems; if the service is not available to the public then it will be difficult for any organisation to generate revenue from it. In today's world, any disruption to network services can lead to significant down time therefore, it is important to identify and mitigate the risk associated with single point of failure. In this section, we are focusing on such availability of the services using the secured perimeter device, which is a firewall. Firewalls helps to safeguard internal environment form the external public threats such as any kind of malware or any application layer attacks, it also helps to block or prevent any access to a particular user or their IP address, thus preventing from the attackers and their attempts to compromise network (Waqar, et al., 2017).

Firewall is the perimeter device; it works on layer 3, layer 4 and layer 7 of an OSI (Open System interconnection) model. It has the ability to allow, block redirect or discard the traffic and acts as a barrier between trusted network and untrusted network. All the users or systems present within the LAN are in control of the organisation comes under trusted and the entire public user outside of the LAN comes under untrusted (Imran, et al., 2015) (S. -d. & E. , 2017) (P. , et al., 2006). Devices kept at perimeter are prone to external as well as internal attacks, attacks such as denial of service(DOS), which fully utilize the resources and once reached a maximum capacity it may face any hardware issues and cause hardware corrupt or system shutdown (Konikiewicz1 & Markowski, 2017).

To avoid this single point of failure, a replica firewall is added in the network with the same configuration as of the previous one. Bringing both the devices in sync with the help of high availability

feature in the firewalls, which transfers the current session information between both the firewalls. Session information is the information of the traffic going through the firewall. Creating a replica of firewall in the environment gives the Organisation a second backup to manage threat-full events, where firewalls will be securing the perimeters in a High availability mode and one of the device being the master and other being the slave. Both the devices share real time information of the sessions that has been created in the master so that in case of failure slave can take the place of master automatically until the master comes up and/or the threat is resolved. This model overcomes the limitation of failsafe network to avoid network being hampered and provide services continuity.

The contribution of this work is significant, as it will provide insights into the practical challenges and benefits of providing continuity of the services and securing and implementing firewall redundancy in real world scenarios. Additionally, the proposed research will also provide recommendations for any such implementation, which later can be used by an organization to improve the security and reliability of their network architecture and ensure protection and continuity of their critical business services. The benefits of this proposed solution are service continuity, reliability of resource, reduced downtime of network infrastructure and ensure the protection of their critical business data.

Problem Statement

The major issue is with the availability of the services provided by an organization; if the devices are not available then the services will not be available. Firewall is the first line of defense and have a higher importance in securing a network fabric hence providing redundancy in firewalls will increase the chances of availability of the Business resources.

Research Question:

What is the need of redundancy in the security infrastructure and how firewall supports business security architecture with redundancy?

2. Related Work

Critical analysis of reputed papers were conducted, in order to highlight strength and weakness of existing related work. This section will provide an overview of research in Network redundancy, Firewall redundancy implementation of GNS3 and virtual environments.

2.1 Reliability

Recently, modern society has become highly dependent on communication networks, including Internet, for various functions ranging from infrastructural utilities such as electricity, water, social and economic aspects such as telecommunications, education, business and commerce. As these are present on the Internet, it is crucial to ensure reliability and availability of these networks, (Waqar, et al., 2017) proposed modeling and analysis techniques that can be used to study the reliability of communication networks. Along with the increasing growth of computer networks, security threats multiplies and accordingly improving and enhancing the network security devices and methods become a necessity

2.2 Redundancy

The importance of reliability is highlighted by (Cisco Press, 2014) by adding redundancy, as it is important to keep the network reliable and available to the end users. In this, the LAN redundancy is achieved by various layer 2 and layer three devices such as switches and routers and if one device fails, other device will help continue the work. This article also explains spanning tree protocol and layer-3 redundancy implementation (Cisco Press, 2014) helps achieve the organization service continuity.

The diagram below shows the redundant architecture of the complete business where each and every communicating device has a redundant partner which helps in communication, thus ruling out the single point of failure concept.

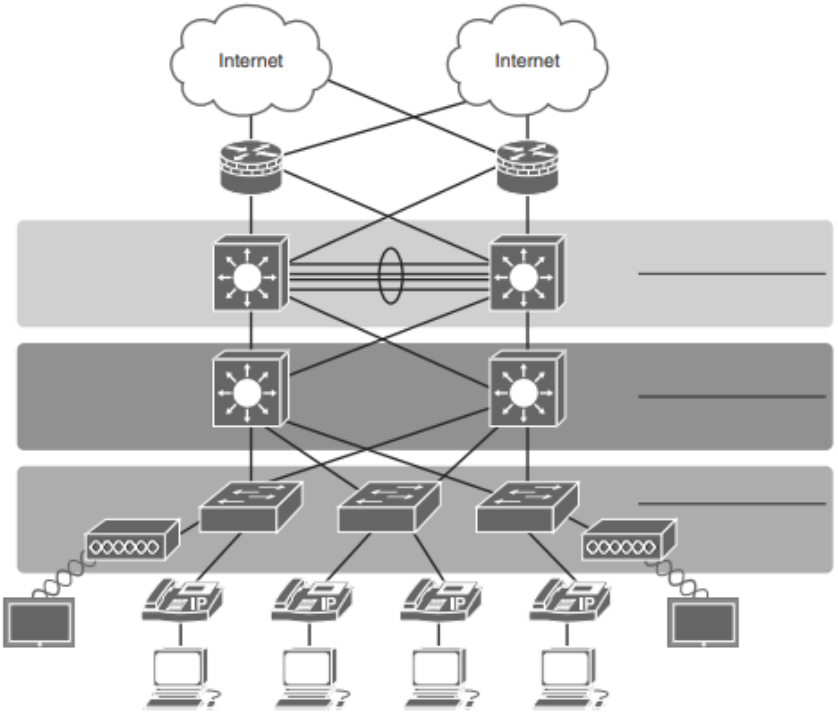

Figure 1: LAN Redundancy with hierarchical design model (Cisco Press, 2014).

The importance of reliability and availability of the switches router and devices are highlighted by (Waqar, et al., 2017) and (Zhu, et al., 2016), Here, it work until the layer 3 of the OSI model, but not above layer 3, such as firewalls, IPS, IDS web application firewalls and many more. Implementation of security requires a device working on higher levels such as layer 3 and above which is represented by (Imran, et al., 2015) (Xin , et al., 2009) (P. , et al., 2006).

The significance of redundancy in firewalls and its support for the security architecture of businesses is highlighted by (A., 2019). By evaluating the performance of first hop redundancy protocols in industrial network environments, the study sheds light on the importance of redundancy in maintaining network availability and reliability. By leveraging redundant firewalls and effective first hop redundancy protocols, organizations can enhance the security and resilience of their computer networks.

2.3 Firewall Technologies

Based on the previous research on LAN redundancy also (Imran, et al., 2015) and (Xin , et al., 2009) represented the firewalls technologies and its working. These papers analyze network security using the firewall technology based on variable firewall principles with its advantages and disadvantages also increasing the security provided by the organization. As the attacks are emerging on the daily basis and also to cope with loss of confidential data, virus spreading and avoid attackers by blocking or restricting access however this research was limited to single firewall and edge devices.

Here as there is only one firewall deployed and also being the single point of failure, which does not, helps business with service availability also we cannot deploy hardware firewalls, as it will incur charges to purchase the device. This above paper was focusing on the hardware firewall, its type, but it was not implemented in fault tolerant mode in real world scenario. Implementing redundancy measures in firewalls is a crucial aspect of building a secure and reliable business network infrastructure (W, et al., 2019).

2.4 Firewall Load Balancing

It is the process of distributing the traffic over a set of resources in order to increase the overall availability and efficiency of the resources. (S, et al., 2001) Highlights about the usage of load balancer kept in before firewall pairs to balance the traffic load between the firewalls and make the services and resources available. Clustering technologies similar to the server technologies used in the Firewall load balancing technique. Different approaches, such as L4/2 and L7/2 clustering, used to tie servers together. FLB devices acted as gateways between network traffic and firewalls, similar to server clusters, balancing connection requests. Leading vendors like Cisco and F5 Networks developed FLB devices alongside server load balancing solutions. Software-based balancers, like the UNL solution, offered flexibility, while hardware-based devices provided superior performance butt it cost extra implementation and configurational overhead for load balancers as well.

2.5 Firewall Cluster

It consists a pair of firewall that refers to redundant pair, which work together in synchronization. (S, et al., 2001)published a paper which shows the firewall in pairs but not synchronized with each other they are only used to load balance the traffic whereas (P. , et al., 2006) and (Sararwat, 2022) has performed the cluster of firewalls in an High availability mode(HA) and they were in sync of each other. Any changes done on active firewall was updated to the backup firewall. Access rules were used to allow for communication of traffic from inside zone to outside zone. Natting, Packet filtering and state-full packet inspection is performed where the traffic is flowing from trusted to untrusted network, but the failover scenarios as well as the continuity of the service is not proven to create fault tolerant network in this research.

Hence, in our research, we have configured strict policies on the firewall to secure our organization from external threats to avoid any services being hampered provided by that organization. In addition, we are trying to prove how high availability of the firewalls will help the business to provide continuity for their services.

Table 1: Strength and Limitation of the Related Work

Related work	Strengths	Limitations
(W, et al., 2019)	Reliability of Communication Networks	Broader perspective not limited to particular Communicating device
(Cisco Press, 2014)	Lan Redundancy	No security devices Involved
(Zhu, et al., 2016)	Real Time Fault-tolerance	Applicable for task allocation and message transmission
(Iman , et al., 2013)	Role of Firewall technology	Redundancy
(Xin , et al., 2009)	Firewall Applications in network security	Limited to edge devices
(A., 2019)	Performance evaluation of redundancy protocols	Focused on performance of three different protocols for redundancy
(Stoitsov & Shotlekov, 2016).	Network Topology implementation with GNS3	Implementation of only routers and switches but not Firewalls
(S, et al., 2001)	Firewall Sandwich configuration	Focused on traffic Load balancing
(P. , et al., 2006)	Designing Stateful network equipment's	Focused on kernels and process architecture
(Sararwat, 2022)	Securing Firewalls in HA from external attacks	Focused on different types of attacks and securing from the external threats
Our Approach	Service continuity using Firewall redundancy and securing the firewalls in HA	Creating huge amount of traffic using DOS or DDOS to create firewall failover and Future attack vectors

3. Research Methodology

As per analysing previous studies and methods, we observed that each method has advantages for its own wellbeing and corresponding limitations, however summarising this might not help in creating a redundant nature for devices supporting L3 and above layers. To overcome this, we are proposing service continuity using firewall redundancy to ensure security and services to be available all the time. Therefore, in case of failure of the security hardware another replica should be present without hampering the production environment and the live traffic.

The proposed research aims to investigate the risks associated with a single point of failure in an organization's infrastructure and the need for redundancy, with a specific focus on how to provide service availability and resource reliability to support business security architecture with firewall redundancy. The research implemented using a combination of literature review, case studies, and simulation-based

experiments. As discussed in the previous section about the redundancy, we are proposing a new approach with simple network architecture including servers, switches, users and external public user, for ensuring security with reliability and High availability with the help of firewalls.

The proposed research will also include the development of a High availability plan that will outline the steps that an organization can take to ensure the continued operation of its critical business processes in the event of a failure or outage.

The network possessing web servers, Linux servers, DNS, Routers, switches and two Next generation firewalls (NGFW). Here, we are using ASA firewalls that has security levels 0-100 and traffic flow from higher level to lower levels so, inside zone has higher security level (100) and outside zone has lower security level (0) and DMZ ha security level of 50 and we can also create a customised zones with customised security level. Outside network is placed in Outside zone and internal network is placed in Inside zone also management zone is created for having management access of the firewalls.

In our research, we have opted for ASA NGFW cluster as the image size is small, it requires less space and boots faster as compared to Palo alto (Sararwat, 2022) and with 2 firewalls in a cluster which are configured with strict security policies for detecting and blocking any malicious traffic from an untrust /Outside zone. The NGFW are configured in an HA mode so the data is synchronised between them. The synchronization of data includes any incremental configurational changes and the current traffic status and the heart beat signals. The flow of traffic from trust zone to untrust zone is allowed but not in reverse by default. The default policy of the firewall is to deny the traffic and access list can be used to allow traffic from particular source to destination.

Table 2: Proposed Access Lists

S. No.	Name of policy	Source	Destination	Action	Description
1	ICMP_Allow	Outside zone, Inside Zone	Inside Zone, Outside zone	Allow	Allows network traffic from Outside to Inside zone and vice versa to verify the connectivity (Later it can be deleted)
2	Inside to outside	inside zone to outside zone	Outside Zone	Allow	Allows network traffic from Inside to outside zone
3	Management to inside	Mgmt zone	Inside Zone	Allow	Allows network traffic from mgmt zone to another internal zone

4. Design Specification

The Network Fabric is divided into 3 parts Trust zone, Untrust Zone and the Management zone. Untrust zone or the Outside zone comprises of the router and a Linux based Firefox machine while trust zone/ Inside zone comprises of all the internal organisational devices that needs to be secured such as User segment and the Server segments, User segment in turn consists of two Linux desktop (kali Linux and a firefox-ubuntu image). The server segment consist of DNS server, router, switch, Ubuntu and a WordPress server. In addition, both the firewalls are configured with the management interface using a switch so that the SSH access of both the firewalls can be taken from the management interface.

HA clustering is performed for synchronizing all the NGFWs with each other. These ASA uses ip-proto-105 & ip-proto-8 for High availability. Failure is detected by sending hello messages at regular interval on all the interfaces if one of the interface is down then firewall is forced to inform the status to the partner and change the state. The firewall is connected towards the internal network-using switch, which then later connects to a router, server and various user end devices. Router is added to segregate the server segment from the user segment.

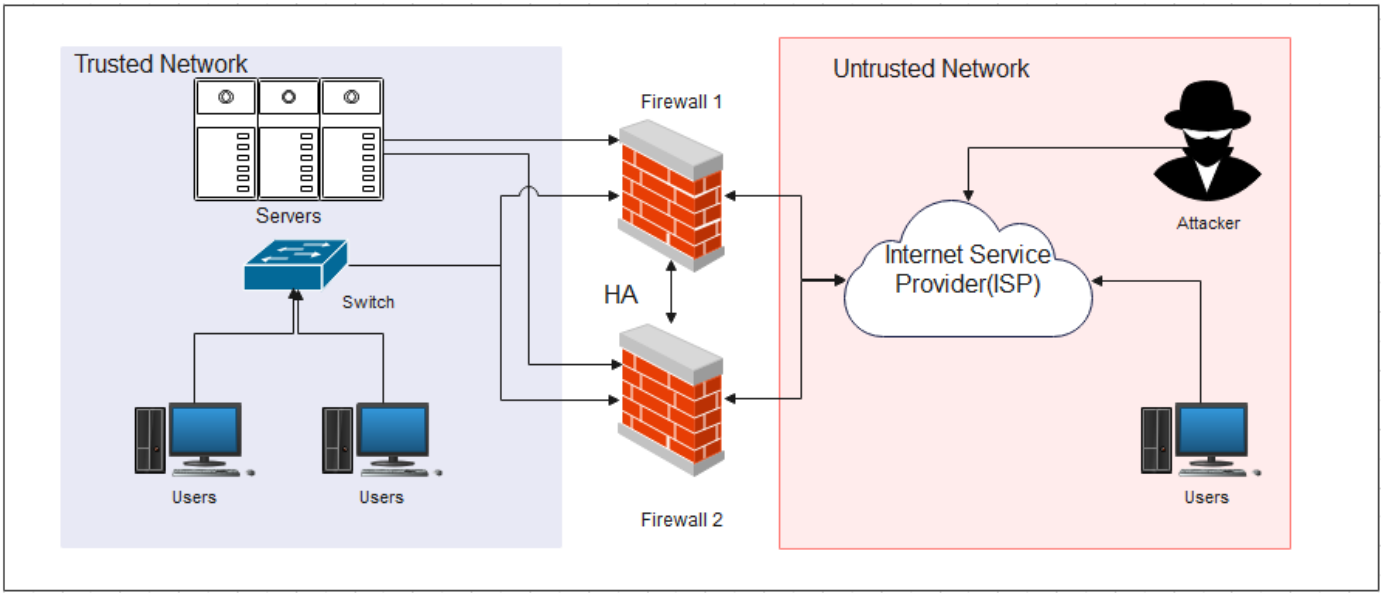

Figure 2 Proposed Architecture.

5. Implementation

Problems and solutions on virtual network topologies are depicted with a simulation environment called GNS3 (Stoitsov & Shotlekov, 2016) (D. T. Vojnak, 2019). The implementation of network fabric done by using GNS3 virtual environment, which is a network simulator and loading of certain images on the virtual

environment such as Cisco ASAv 10.1.0, Cisco 3725 routers, GNS provided basic switches, kali Linux and Ubuntu based desktops, DNS server and a WordPress server.

The GNS3 is integrated with VMware workstation Virtualised environment to run the firewalls and Linux servers on it. The hardware configuration of ASAv is 3 GB ram and 8 ports of 1 GBPS link each, Linux server was running with 4 GB ram and 80 GB of SSD drive with 2 ports and intel i5 8th Generation. The Gns3 Environment is also integrated with the Docker containers to download WordPress and DNS server images. A DNS server is created for having a hostname-ip mapping within the environment, a simple WordPress server is placed in the server segment. A separate router R2 is added to keep the networks of User and Server Segment variable.

Agni 1 and Agni 2 are the Cisco ASAv 992 image of the firewall and are placed at the perimeter of the organisation. In Outside network an attacker is present using kali Linux with 4 GB ram and 80 GB SSD and performing a denial of service attack from the outside zone. Default cloud was created for the internet access in the virtual environment using the loopback adapter and the DNS server is created for the name lookups. A WordPress server is also hosted on the server segment to make it look like a simple simulated organisation.

Table 3: List of Devices and Images

S. No.	Vendor		Name and version of image	Networking component	Interface	IP address
1	Cisco	Agni-1	asav9.9(2)	Firewall	Ge 0/0	192.168.140.10
					Ge 0/1	192.168.2.10
					Ge 0/2	192.168.45.10
					Ge 0/6 (Failover)	10.1.1.1
					Man 0/0	10.1.0.10
2		Agni-2				
					Ge 0/0	192.168.140.11
					Ge 0/1	192.168.2.11
					Ge 0/2	192.168.45.11
					Ge 0/6 (Failover)	10.1.1.2
					Man 0/0	10.1.0.11
3		R2	c3725-adventerprisek9-mz.124-15.T14.image	Router	Fe 0/0	192.168.140.12
					Fe 0/1	172.20.19.12
4		R1			Fe 0/0	192.168.2.1
					Fe 0/1	192.168.146.11
5	Docker	WrodPress-1	WordPress	Web server	eth0	172.20.19.15
6		Ubuntu-1	Ubuntu	Linux server	eth0	172.20.19.16

7	Linux	DNS-1	Dns	DNS Server	eth0	172.20.19.100
8		Attacker	Kali Linux 2021.3	Edge Device	eth1	192.168.146.15
9		User Desktop	linux-tinycore	Edge Device	eth0	192.168.140.9
10		MGMT	linux-tinycore	Edge Device	eth0	10.1.0.12

11	Gns3	PC1	BSD	Edge Device	eth0	192.168.140.8
12		Cloud1	Cloud	Cloud	VMnet8	192.168.146.1
13-17		Switch 1, Switch 2, Switch 3, Switch 4, Switch 5	Switch	Access Switch	eth0, eth1, eth2, eth3, eth4	N/A

Python script Goldeneye were used to create denial of service attack at some level to see how the firewall is handling the traffic and how the firewall blocks the unknown traffic

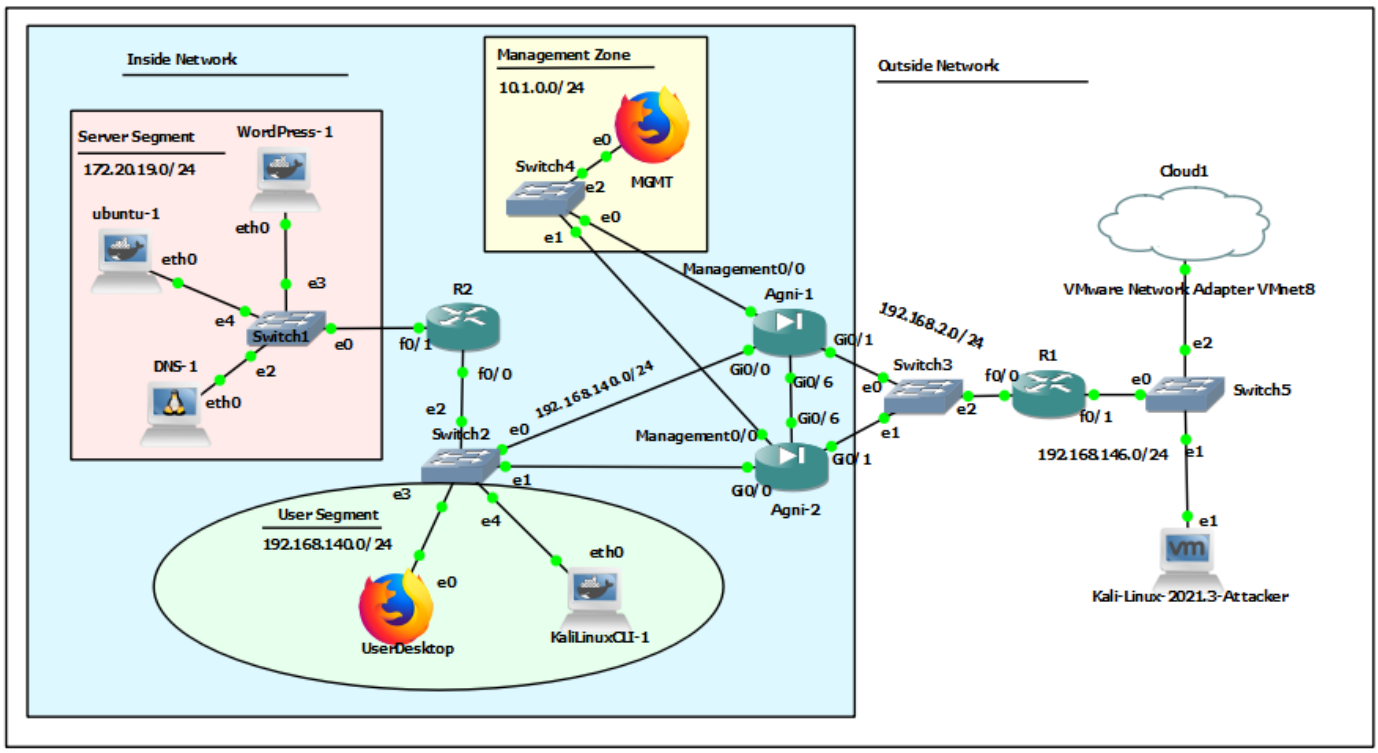

Figure 3: Network Fabric

6. Evaluation

Critical Evaluation is conducted through a series of experiments using the simulated environments. The simulation-based experiment are done to measure the service availability and effectiveness of firewall redundancy in improving the security and reliability of an organization's infrastructure. As per analysis of (Sararwat, 2022) for enhancing security in network using Firewalls and load balancers. Here the study was

done on all the security aspects for securing the environment with redundancy and firewall hardening, based on that the network security is evaluated.

Using this evaluation method as a benchmark for our proposed methods, we implement our proposed theory. The qualitative evaluation based on the real time traffic observed in the scenarios, which is used to provide insight into the practical challenges and benefits of providing service availability and implementing firewall redundancy and security policies in real-world environment. The attack vector generated are from an outside zone interface of the firewall where a port 443 and 80 is open for the public access which acts as the services provided by an organisation.

6.1 Detection and blocking of DOS attacks

Denial of service attack done on the outside interface of the firewall through an attack vector using kali Linux. Here, Goldeneye script are used to generate huge amount of TCP traffic. It is used for performing attack on the firewall through a router; the motive of this evaluation is to avoid any service being hampered due to such types of attack thus avoiding any services being disrupted.

Goldeneye is an open source tool from GitHub, used to perform denial of service attack. This tool allows a single machine to takedown another machines webserver by using legitimate HTTP traffic. It makes a complete handshake of TCP connection and requires only few hundred requests at regular intervals and for long-term.

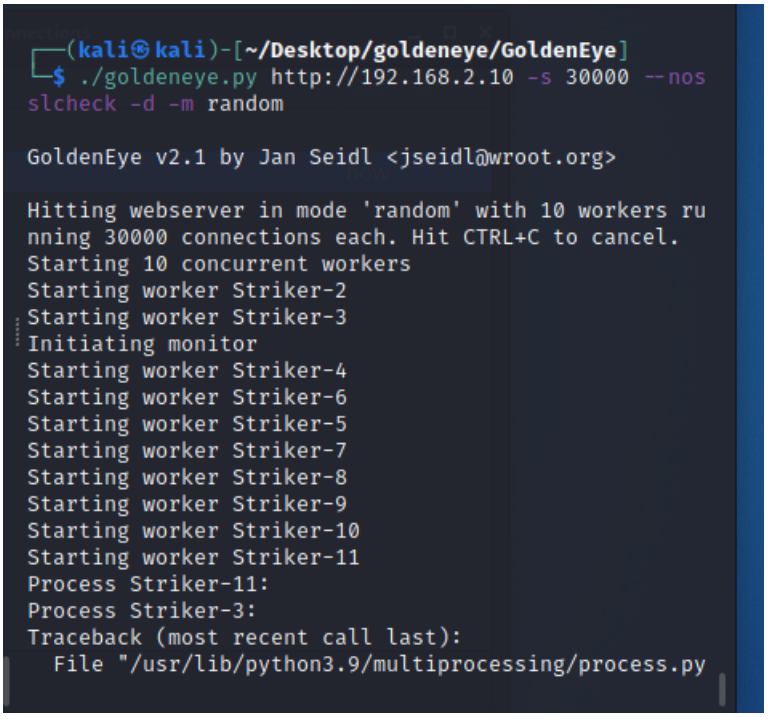

Figure 4: DDOS using GoldenEye

As we can see that, the command uses the python script with port number 80 with default 10 workers, creating 30,000 socket connections on the target address. The attack is done on the outside interface of the firewall creating huge amount of traffic and flooding on port 80 as shown below in the image of firewall packet capture and the CPU peaks to 100% resource utilization.

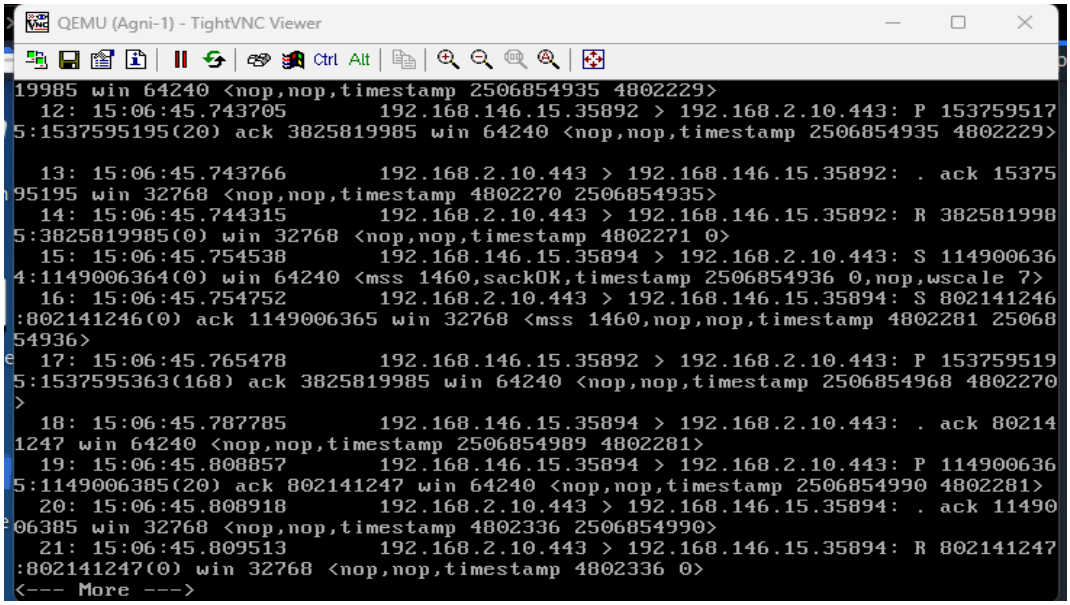

Figure 5: Before Implementation of security policies

```
Agni-1# sh cpu usage
CPU utilization for 5 seconds = 56%; 1 minute: 100%; 5 minutes: 72%

Virtual platform CPU resources
------------------------------
Number of vCPUs              :     1
Number of allowed vCPUs      :     0
vCPU Status                  :  Noncompliant: Over-provisioned
Agni-1# _
```

Figure 6: CPU Utilization

After Implementation of threat detection and security policies by applying DOS rate limiting the traffic from the attacker, the traffic is getting dropped as well as shunned to block the attack from that ip for a particular time as shown below,

```
  16: 09:18:29.057354 c201.0711.0000 0cff.9931.9f02 0x0800 Length: 74
      192.168.146.15.55620 > 192.168.2.10.80: S [tcp sum ok] 3325728120:3325
20(0) win 64240 <mss 1460,sackOK,timestamp 3917899922 0,nop,wscale 7> (DF) (
63, id 57218) Drop-reason: (shunned) Packet shunned

  17: 09:18:29.057415 c201.0711.0000 0cff.9931.9f02 0x0800 Length: 74
      192.168.146.15.55624 > 192.168.2.10.80: S [tcp sum ok] 2341528240:2341
40(0) win 64240 <mss 1460,sackOK,timestamp 3917899922 0,nop,wscale 7> (DF) (
63, id 45993) Drop-reason: (shunned) Packet shunned

  18: 09:18:29.057476 c201.0711.0000 0cff.9931.9f02 0x0800 Length: 74
      192.168.146.15.55626 > 192.168.2.10.80: S [tcp sum ok] 466658685:46665
(0) win 64240 <mss 1460,sackOK,timestamp 3917899922 0,nop,wscale 7> (DF) (tt
, id 51932) Drop-reason: (shunned) Packet shunned

  19: 09:18:29.057492 c201.0711.0000 0cff.9931.9f02 0x0800 Length: 74
      192.168.146.15.55628 > 192.168.2.10.80: S [tcp sum ok] 1318373552:1318
52(0) win 64240 <mss 1460,sackOK,timestamp 3917899922 0,nop,wscale 7> (DF) (
63, id 34019) Drop-reason: (shunned) Packet shunned

  20: 09:18:29.132653 c201.0711.0000 0cff.9931.9f02 0x0800 Length: 74
      192.168.146.15.55630 > 192.168.2.10.80: S [tcp sum ok] 2770159015:2770
15(0) win 64240 <mss 1460,sackOK,timestamp 3917899922 0,nop,wscale 7> (DF) (
63, id 38071) Drop-reason: (shunned) Packet shunned
_
```

Figure 7: After Implementation of Security policy against DOS

The Event per second list is also shown below, representing the total attack events that has been detected per second on the interface of the firewall for an amount of 10 minutes to 1 hour.

```
Top          Name    Id     Average(eps)    Current(eps) Trigger      Total events
  10-min Sent attack:
  10-min Recv attack:
01           HTTP    80              0              0      22                57
02          HTTPS   443              0              0      23                35
  1-hour Sent byte:
01          HTTPS   443           1537              0       0           5534945
02           ICMP *  1               2              0       0              8608
  1-hour Sent pkts:
01          HTTPS   443             10              0       0             37731
02           ICMP *  1               0              0       0                95
  1-hour Recv byte:
  1-hour Recv pkts:
Top          Name    Id     Average(eps)    Current(eps) Trigger      Total events
                            Average(eps)    Current(eps) Trigger      Total events
Top 10 protected servers under attack (sorted by average rate)
Monitoring window size: 30 mins    Sampling interval: 30 secs
Agni-1(config)#
```

Figure 8: Blocked Dos Events per second

6.2 Detection and blocking of traffic from unknown sources

The firewall uses stateful inspection and remembers the session traffic flowing through the firewall and if the traffic is not terminated then after the stipulated time the firewall discards the traffic. This evaluation was done to show the security policies working in the firewall and are in place to prevent from such type of attacks. Hping3 and metaslpoit tool was used to generate a high rate SYN attack on the interface of the firewall to utilize the bandwidth and create unnecessary fake sessions on the firewall.

```
┌──(kali㉿kali)-[~/Desktop/goldeneye/GoldenEye]
└─$ sudo hping3 192.168.2.10 -q -n -d 120 -S -p 443 --flood --rand-source
[sudo] password for kali:
HPING 192.168.2.10 (eth0 192.168.2.10): S set, 40 headers + 120 data bytes
hping in flood mode, no replies will be shown
```

Figure 9: Hping3 attack

```
msf6 auxiliary(dos/tcp/synflood) > set RHOSTS 192.168.2.10
RHOSTS ⇒ 192.168.2.10
msf6 auxiliary(dos/tcp/synflood) > exploit
[*] Running module against 192.168.2.10

[*] SYN flooding 192.168.2.10:80 ...
```

Figure 10: Metasploit attack

After starting the command, the connection requests on the firewall started increasing.

Figure 11: Connection list while the Hping3 attack

Before the actual implementation of security policies, the firewall was opening the packet, handling the traffic and waiting for the reply from the sender. This was causing unnecessary memory and bandwidth usage as follows,

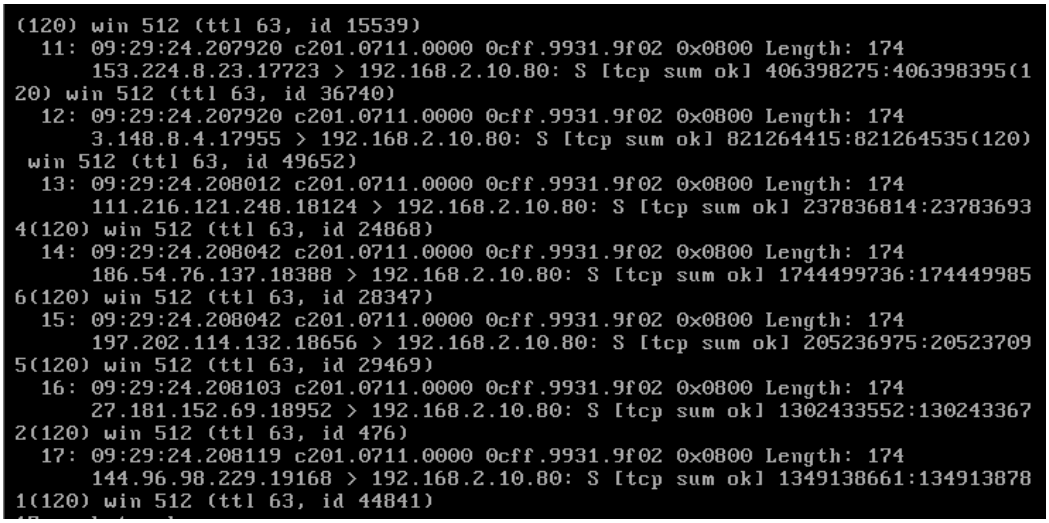

Figure 12: Before Implementation of Security Policies

Our approach was to add rate-limiting feature and access list also using threat detection monitoring system on the firewall that eliminates unnecessary utilization of the resources and the session is not in time-wait state, nor waiting for a reply from the sender thus saving the firewall resource for legitimate traffic.

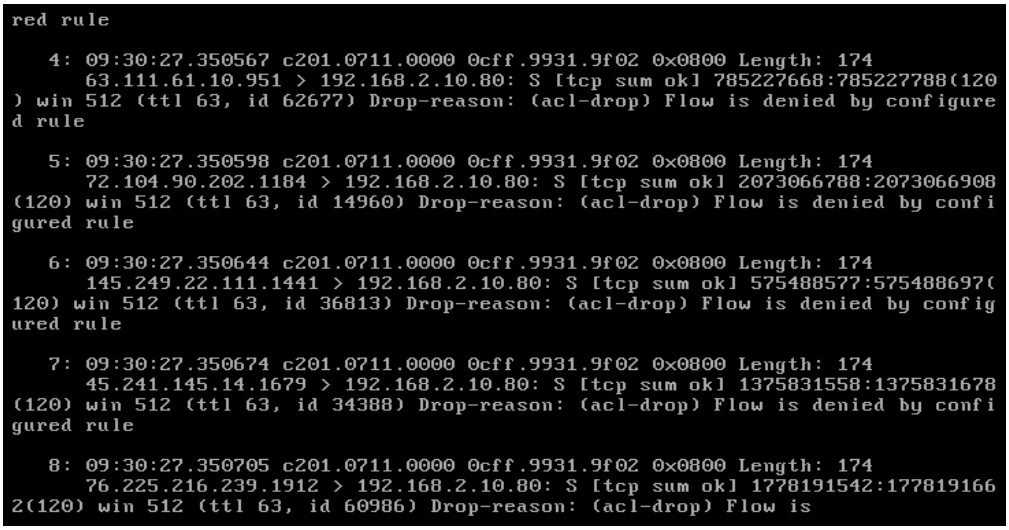

Figure 13: After enabling Threat detection

6.3 Link failure

Created a scenario by manually failing one of the link connecting to the firewall and the management switch and making the firewall to inform the state change to the partner and forcing itself to failover and change the state Standby and the standby device will become active. Here Agni-1 is active firewall and Agni-2 is standby firewall, so after the state change the Agni-2 firewall becomes active and the Agni-1 becomes standby.

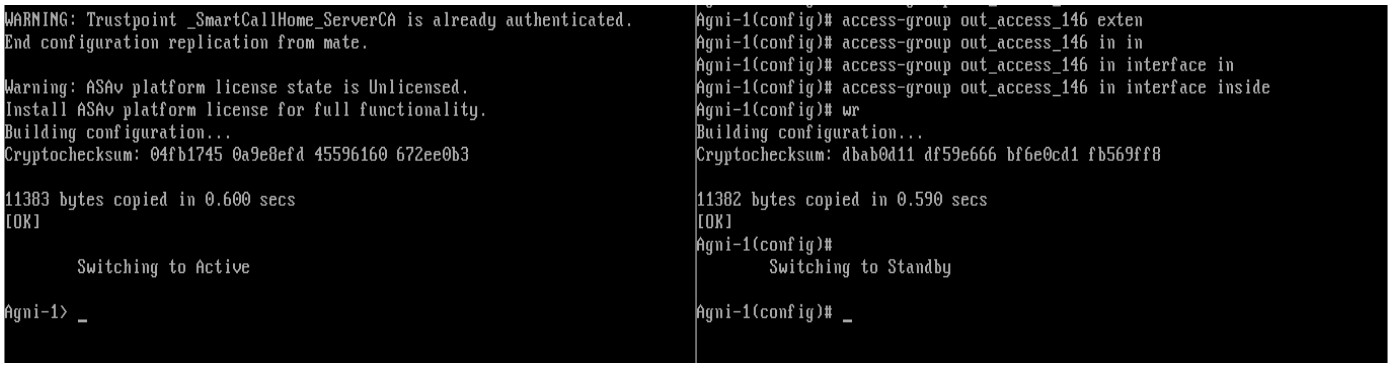

Figure 14: Failover of the Firewalls

The below is the status of the firewall that was changed to standby Ready once the interface came up, but for gaining the Active status again needs to be performed manually.

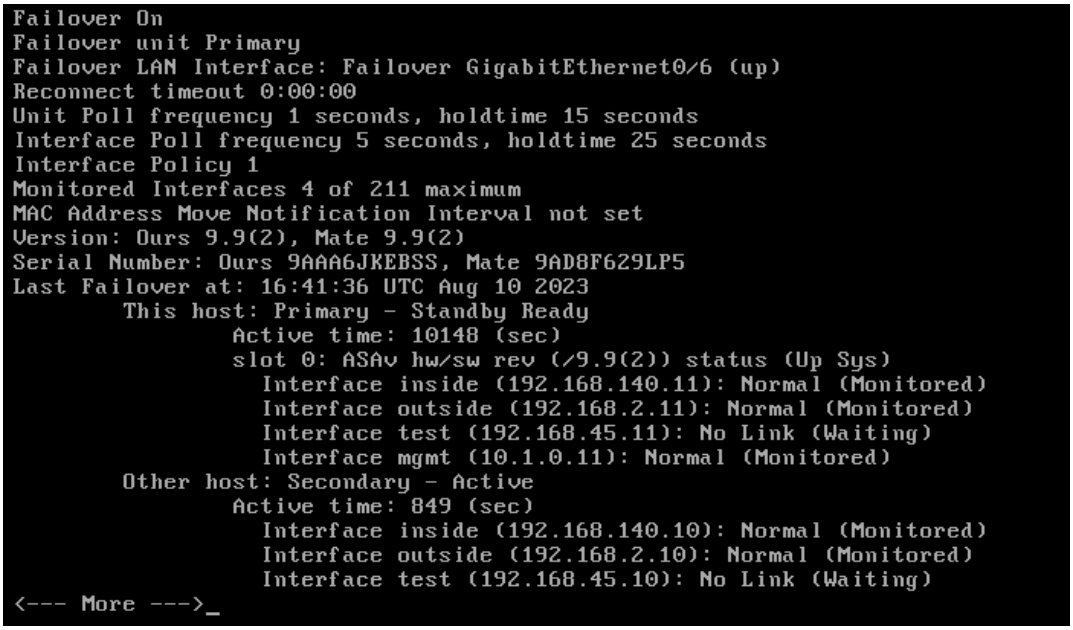

Figure 15: Status of the previously active firewall after failover

We can also see that during the failover activity the connection from inside network to outside network is not much hampered thus we can prove that the redundancy of the firewall can help achieve service continuity without hampering the traffic flow thus allowing the organisation to maintain the service availability and resource reliability.

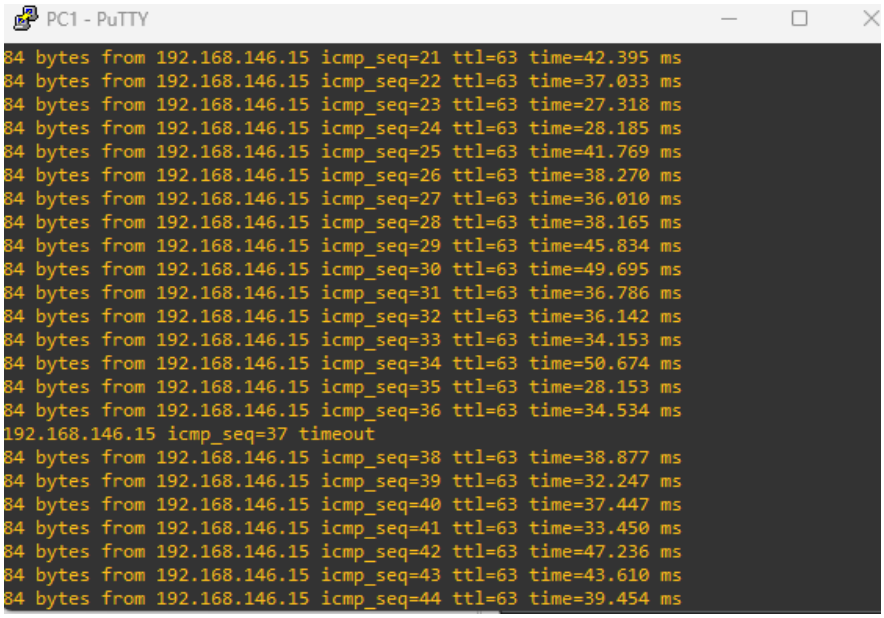

Figure 16: Traffic scenario during the failover event

7. Discussions

The attack vector was taken into consideration in order to propose an effective research including flooding in to the network and utilizing the resources. A denial of service attack of type SYN flood and HTTP flood was performed with more than 10,000 packet counts. The attacks such as goldeneye script, metasploit and hping3 were used to attack on outside interface of the firewall.

The attack was also done by changing the source ip address of the attacker system were the traffic from different source ip addresses were created to hide the attacker. Here, sync floods were also created with to see if the attack is being dropped by the firewall security policies or not, to highlight that the firewall is working under the strict security policies.

However, the main limitation of the proposed approach is that the amount of traffic generated by the attack vector is not sufficient for the firewall interface of one GBPS to shut down or cause any link failure. Hence, to create a failover scenario, manual failover is created by shutting the interface down and making the firewall to switch the state and the standby firewall gaining the active state. Thus providing continuity of the services provided by an organisation by resource availability and continually processing the traffic.

8. Conclusion and Future work

The research questions and interrogates the technique of reliability security feature and the availability of the network traffic. The objective and purpose of the research was providing the organization with resource availability, strict security policies and creating a small infrastructure keeping end devices in mind. The configuration and deployment of the NGFW took place after critically analysing the policies and research based evaluations, which led to successful detection and blocking the attacks and also providing service continuity for a business.

Overall, this research project aims to provide valuable insights into the risks associated with single points of failure in an organization's infrastructure and the importance of redundancy, specifically focusing on Service availability using firewall redundancy in supporting business security architecture.

The follow-up future research project can be performed considering creation of security context in firewalls-in-HA and also deployment of the web servers and web application firewalls and generating such amount of traffic that can enable the attack vector to cause failure in the firewall interface causing failover by attacking the port.

9. References

A., Z., 2019. *Performance Evaluation of First Hop Redundancy Protocols for a Computer Networks of an Industrial Enterprise.* Vladivostok, Russia,, s.n.

Cisco Press, 2014. *ptgmedia.pearsoncmg.com.* [Online] Available at: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://ptgmedia.pearsoncmg.com/images/9781587133442/samplepages/158713344x.pdf

[Accessed 11 04 2023].

D. T. Vojnak, B. S. Đ. V. V. T. a. S. M. Š., 2019. *Performance Comparison of the type-2 hypervisor VirtualBox and VMWare Workstation.* Belgrade, Serbia, s.n., pp. 1-4.

Iman , K., Maryam, . K. & Ali , S., 2013. A Survey on Security Issues in Firewalls: A New Approach for Classifying Firewall Vulnerabilities. *International Journal of Engineering Research and Applications (IJERA) ISSN:*, 3(2), pp. 585-591.

Imran, M., Algamdi, D. A. & Bilal, A., 2015. Role of firewall Technology in Network Security. *International Journal of Innovations & Advancement in Computer Science IJIACS*, 4(12), pp. 3-6.

Konikiewicz1, W. & Markowski, M., 2017. Analysis of Performance and Efficiency of Hardware and Software Firewalls.. *Journal of Applied Computer Science Methods. 9. 10.1515,* Volume 0003, pp. 49-63.

P. , N., L. , L. & R. M. , G., 2006. *High availability support for the design of stateful networking equipments.* Vienna, Austria,, First International Conference on Availability, Reliability and Security (ARES'06).

S. -d., K. & E. , H., 2017. *Overview of firewalls: Types and policies: Managing windows embedded firewall programmatically,.* Monastir, Tunisia, 2017 International Conference on Engineering & MIS (ICEMIS).

Sararwat, Y., 2022. *Enhancing the security of a network fabric using firewalls and load balancer.* [Online] Available at: https://norma.ncirl.ie/6053/

[Accessed 08 07 2023].

S, G., R, K. & Yuping, Z., 2001. *An unavailability analysis of firewall sandwich configurations.* USA, Proceedings Sixth IEEE International Symposium on High Assurance Systems Engineering. Special Topic: Impact of Networking,.

Stoitsov, G. & Shotlekov, I., 2016. Sample network topologies for educational purposes implemented with GNS3. *MATTER: International Journal of Science and Technology,* 04(07), pp. 106-115.

Waqar, A., Osman , H., Usman , P. & Junaid , Q., 2017. Reliability modeling and analysis of communication network. *Network and Computer Applications,* Volume 78, pp. 191-215.

W, Y., Z, X. & Z, D., 2019. *A High-reliability Network Architecture Based on Parallel Redundancy Protocol.* Toronto, ON, Canada, 14th International Conference on Computer Science & Education (ICCSE).

Xin , Y., Wei , C. & Yantao , W., 2009. The research of firewall technology in computer network security. *Asia-Pacific Conference on Computational Intelligence and Industrial Applications (PACIIA),* Volume 2, pp. 421-424.

Zhu, . X. et al., 2016. Fault-Tolerant Scheduling for Real-Time Scientific Workflows with Elastic Resource Provisioning in Virtualized Clouds. *IEEE Transactions on Parallel and Distributed Systems,* Volume 27, pp. 3501-3517.