National College of Ireland

Enhancing the security of a network fabric using firewalls and load balancer

MSc Research Project
MSc Cybersecurity (MSCCYB1)

Yash Saraswat
Student ID: X20184867

School of Computing
National College of Ireland

Supervisor: Prof. (Dr) Rohit Verma

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Yash Saraswat
Student ID:	X20184867
Programme:	MSc Cybersecurity (MSCCYB1) **Year:** 2022
Module:	Research Project
Supervisor:	Prof. (Dr) Rohit Verma
Submission Due Date:	19-September-2022
Project Title:	Enhancing the security of a network fabric using firewalls and load balancer
Word Count:	6190 **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: Yash

Date: 19-September-2022

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):	

Enhancing the security of a network fabric using firewalls and load balancer

Yash Saraswat
X20184867

Abstract

The rapid change in the dynamics of attack vectors require an update in traditional firewall and load balancer policies in order to minimise the possibilities of network-compromise. This study proposes the deployment of strict security policies on next-generation firewalls cluster along with the deployment of strict redundancy policies on load balancer for ensuring the overall security of network fabric from a wide range of recent threat vectors. The security of a network fabric cannot be enhanced by traditional and hierarchical placement of internet cloud, firewall, router, and networking devices. The proposed fabric possesses the deployment of strict security policies on synchronised next-generation firewalls cluster and strict redundancy policies on load balancer is capable to defend the network resources from a wide range of incoming malicious intrusions. The proposed next-generation firewalls and load balancer policies are capable to defend the fabric from incoming intrusions. The approach is successful for detecting and blocking a broad range of attack vectors in comparison with the similar previous works in the field.

1 Introduction

Cyberattacks have been rated as the fifth top-rated risk in 2021-2022 according to Checkpoint research. Cybercrimes mostly targets the small and medium enterprises which causes unnecessary financial burden to business communities all around the world. The security of network fabric is extremely important because the disruptions in network resources degrades the business continuity cycle which leads to decreased productivity and increase financial losses. Strengthening the components of network fabric increases the overall efficiency, productivity and leads to continuous business cycles.

Research question: What techniques can be used in order to uphold the security, integrity, and availability of a network fabric?

Threat vectors mostly targets to compromise the network fabric through brute forcing security, exploiting integrity and hampering availability of network resources. A secure, integral, and available network fabric can be constructed only when the fabric is capable to detect, mitigate, thwart and block a wide of attack vectors. Therefore, our research objective was set to propose a network fabric which can detect and block a broad spectrum of incoming intrusions. In order to achieve this objective, we have opted for Next-Generation firewalls cluster possessing strict antivirus, vulnerability protection, antispyware, URL filtering, file blocking, data filtering profiles, deep packet, and payload inspection policies in order to upscale the security and integrity of network resources. Moreover, we have opted for load balancer possessing strict redundancy policies to upscale the availability of network

resources. Strict firewall and load balancer policies provides a defence mechanism to network fabric from a wide range of recent threat vectors.

The major contribution of the proposed research is to enhance and upscale the security, integrity, and availability of a network fabric in order to minimise the network disruptions caused by attack vectors. Absence of network resources imposes unnecessary financial burden which hampers the continuity of business cycles. Access of undisrupted network resources increases the productivity in business environments while the absence of network resources halts the connectivity and communication links which may lead towards the cancellation of contracts, deals or memberships.

We have used the following abbreviations throughout the report: Deep Packet Inspection as DPI, Graphical User Interface as GUI, Intrusion Detection and Prevention System as IDPS, Load balancer as LB, Management as MGMT, Next-Generation firewall(s) as NGFW(s), SQL injection as SQLi and Virtual IP as VIP. Moreover, the words policies and rules have been used interchangeably throughout the report.

The complete research report is divided into seven sections. Abstract describes the background, objectives of work and findings from the proposed research. Section 1 explains the introduction of research report which includes its background, motivation, research question and objective. Section 2 illustrates the critical analysis of previously related work. Section 3 describes the research methodology which includes the setup and procedure of proposed research. Section 4 explains the design specification, architecture, and word-based description of the proposed algorithm. Section 5 describes the final stage of research project implementation. Section 6 illustrates the evaluation and discussion of proposed network fabric. Section 7 is the last section which includes the conclusion and comments for future work.

2 Related Work

Critical analysis of reputed conference papers and journal articles from ACM, IEEE and ScienceDirect has been conducted in order to highlight the strengths and weaknesses of existing works for upholding the overall security, integrity, and availability of a network fabric. This section has been subcategorised into four sections which possesses the conference papers and journal articles of similar domain.

2.1 Security enhancement

All measurements should be taken into consideration which lead towards the security enhancement of whole network infrastructure in order to safeguard the vital network resources from malicious actors. Bhakthavatsalam and Malarkodi (Bhakthavatsalam and Malarkodi, 2016), Hamilton *et al*. (Hamilton *et al*., 2020), and Xiao, Guo and Lv (Xiao, Guo and Lv, 2021) highlighted the importance of firewalls to safeguard the network infrastructure from threat actors. Authors have proposed the usage of NGFWs to detect and block the gateway viruses and other incoming intrusions towards network infrastructure. Moreover, some preventive measures like antivirus upgradation and antispyware installation have been proposed in order to defend the system from getting compromised. The rapid change in the

dynamics of malicious payloads might allow the malwares to bypass the updated firewall, antivirus, and antispyware. In our research, we have opted for latest threat signatures along with strict security configurations of deep packet and payload inspection to instantly detect and block the incoming malicious payloads from untrusted zone towards the network infrastructure.

The importance of NGFWs over traditional firewalls have been highlighted by Neupane, Haddad and Chen (Neupane, Haddad and Chen, 2018), Khelf and Ghoualmi-Zine (Khelf and Ghoualmi-Zine, 2018), and Zaki *et al*. (Zaki *et al*., 2021). Evolution of NGFWs came into existence due to the incapabilities of traditional firewalls to detect and block advanced evasion techniques, targeted cyberattacks, web application attacks and data focused attack vectors. Conflicts in the security policies have been detected by authors at some instances which arises due to the collision of one or more security rules among each other. In our research, we have sticked upon the best practices for NGFW rules configuration and synchronisation among NGFW cluster which provides maximum security and eradicate the possibilities of potential security rule conflicts.

Wan and Xu (Wan and Xu, 2021), and Allison (Allison, 2022) opted for a cross-platform visual simulation networking tool in order to construct the network topology. The security policies which were deployed on firewall for defending topology from malicious actors included allowing/denying certain ICMP traffic along with filtering inbound ping and web network traffic. Packet filtering security policies allow the movement of data packets across the network fabric in accordance with the set of rules specifying packet header information, source IP and destination IP. On the contrary, DPI examines the content of data packets as they are supposed to pass by a checkpoint on the network. In our research, we have implemented strict security configurations on NGFWs which ensures the detection and blockage of hidden threats within the data stream, such as attempts at data exfiltration, malware, and violations of content policies.

2.2 Network fabric

A network fabric describes the network topology which contains a mesh of connections between network devices, such as routers, switches, firewalls and connecting cables that transports the data to its destination. Maraj *et al*. (Maraj *et al*., 2017), Shanmugam and Malarkodi (Shanmugam and Malarkodi, 2019), and Chapman (Chapman, 2021) conducted authorised penetration testing for verifying the security of a network fabric possessing web servers and NGFWs. Penetration testing machine was used to generate TCP and UDP flooding attacks on the web servers while monitoring server was used to record and inspect the web servers during the incoming flooding attacks. The authors have suggested the usage of NGFWs to provide a defence mechanism against significant DoS attacks. The scope of penetration testing was limited to flooding attacks only while the presence of web servers could help to test other attack vectors like SQL injection, phishing, and payload inspection. In our research, we have successfully conducted the penetration testing on network fabric through a wide range of attack vectors in order to obtain the detailed security verification results.

The behavioural patterns of two open-source firewalls have been recorded by Garcia and Hailu (Garcia and Hailu, 2021), Miloslavskaya (Miloslavskaya, 2021), and Kiratsata *et al*. (Kiratsata *et al*., 2022) in order to test and verify the security of a network fabric under security crisis. The attack vectors which were used to test the security of network included ping of death, open port exploitation, brute forcing and flooding attacks. As a result, one firewall was unable to detect while other firewall was unable to block the incoming attack vectors towards network infrastructure. The authors concluded by suggesting the usage of clustered NGFWs in order to completely thwart the incoming intrusions. In our research, we have opted for load balancing and NGFWs clustering along with strict security rules to provide a defence mechanism to network fabric against a wide range of attack vectors. Moreover, the configuration of VIP on LB using strict redundancy policies ensures the evenly distribution of connection requests among pool resources.

Blancaflor *et al*. (Blancaflor *et al*., 2020), Loureiro (Loureiro, 2021), and Zhou (Zhou, 2022) have highlighted the importance of firewall system for protecting the internal and external environment of the end-devices within the network fabric. Successful detection and blockage of virus-infected files has been taken place through pattern matching when the malicious files were injected towards LAN. The author concluded by stating the necessity of a defence mechanism which caters the blockage of wide range of malicious payloads. In our research, we have integrated latest threat signatures along with strict payload and packet inspection security rules in order to instantly detect and block the incoming malicious payloads towards network fabric.

2.3 Firewall cluster

A firewall cluster refers to high-availability and redundant pair of firewalls that work together in synchronisation. SenthilKumar and Muthukumar (SenthilKumar and Muthukumar, 2018), Singh *et al*. (Singh *et al*., 2020), and Waleed, Jamali and Masood (Waleed, Jamali and Masood, 2022) deployed threat signatures using open-source IDPS and firewall access rules using open-source firewalls in order to allow the network traffic towards respective web servers. Access rule set allows any device to connect directly with the firewall cluster which caters the passage of network traffic towards specified web servers. Authors have designed the firewall system which supports Network Address Translation (NAT), packet matching and stateful packet filtering. Stateful packet inspection evaluates packet header information only, such as port number, source, and destination IP addresses. In our research, we have opted for NGFW cluster and configured strict DPI policies which inspects wide range of data and metadata associated with individual packets flowing from untrusted zone towards trusted zone within network fabric.

The effectiveness of NGFW over stateful firewall has been compared by Soewito and Andhika (Soewito and Andhika, 2019), Daxian, Jishan and Jiujiu (Daxian, Jishan and Jiujiu, 2020) and, Liang and Kim (Liang and Kim, 2022) through a series of attack vectors like phishing and SQLi and DoS attacks on the network infrastructure of a company. Stateful firewall was unable to block the intrusions while NFGW was capable to detect and block the attack vectors that threatens the confidentiality, integrity, and availability of the network fabric. CPU utilisation of web server went high by 10% to 15% during the incursion of DoS

flooding attacks. In our research, we have configured strict security policies along with the deployment of NGFW cluster and load balancer which blocks the flooding attacks with negligible increase in the CPU utilisation of web servers. NGFW cluster enables the synchronisation between both NGFWs which gears up the secondary NGFW during the inaction or failure of primary FW in order to ensure zero downtime in NGFW service.

2.4 Load balancing

Load balancing refers to the process of distributing a set of tasks over a set of resources in order to increase the overall availability and efficiency of resources. Nenova *et al*. (Nenova *et al*., 2019), Tudosi, Balan and Potorac (Tudosi, Balan and Potorac, 2022), and Zhao, Juan and Yawen (Zhao, Juan and Yawen, 2022) proposed a system design containing NGFW cluster, IDPS and LB for detecting and blocking incoming intrusion actions. The network system was divided into two parts i.e., Trust and Untrust zone. Outside network possessing internet and other ISP configurations was placed in Untrust zone while the web servers and end-devices were placed in the engineering and administration network of Trust zone. SQLi and SYN flood DoS attacks were successfully detected and blocked after the manual addition of specific attack signatures on NFGW cluster and LB respectively. In our research, we have adapted to deployment of strict security policies on NGFWs along with strict redundancy policies on LB which completely thwarts the incoming intrusions without adding customised and specific signatures of attack vectors.

The focus of Trabelsi and Zeidan (Trabelsi and Zeidan, 2019), and Reynolds (Reynolds, 2020) was laid upon an emerging low-volume denial of firewalling attack vector called Black Nurse attack which is widely known for using specially formatted ICMP packets in order to overwhelm the CPUs of targeted firewalls. Testing of Black Nurse attack has been conducted on traditional firewalls and NGFWs in order to attain a deeper insight into the principles, dynamics, and effects of attack vector upon the impacted firewalls and network fabric. The authors have suggested the usage of firewalls possessing multiple CPU cores along with ICMP flood protection screening while specifying the minimum threshold limit. In our research, we have configured DoS protection profiles and deployed latest signatures of attack vectors along with strict security policies on NGFW cluster in order to block flooding and low-slow denial of firewalling attacks. Moreover, the load balancing of NGFW filtered traffic has been achieved through strict redundancy policies on LB which ensures the uptime of pool members for catering the incoming legitimate requests from Untrust zone.

In conclusion, the security, integrity, and availability of a network fabric cannot be achieved by defining a traditional and hierarchical network topology containing internet cloud, firewall, router, switch and other networking components. Absence of an all-rounded network fabric which possesses the capabilities of detecting and blocking a wide range of attack vectors justifies the necessity of a new solution. Our research proposes NGFW clustering, strict security policies for NGFW cluster, Python script to ensure the deployment of policies at NGFW, strict redundancy policies for LB and redundant pool resources at VIP in order to uphold the security, integrity, and availability of a network fabric. Such network fabrics are capable for providing an all-rounded defence mechanism against a wide range of threat vectors. The Table (Table 1) compares the strengths and limitations of our work with

the previously related works of our domain. Our current research on NGFW cluster and LB policies cannot ensure the detection and blockage of upcoming threat vectors. The rapid change in the dynamics of attack vectors requires a continuous and steady research of threat patterns which helps us to define the future security and redundancy policies. Therefore, the main limitation of our proposed research is the detection and blockage of future attack vectors.

Table 1: Strength and limitations of related work

Related work	Strengths	Limitations
(Bhakthavatsalam and Malarkodi, 2016)	Malicious payloads blockage	DoS, SQLi and phishing attacks blockage
(Maraj *et al*., 2017)	DoS attacks blockage	SQLi, phishing and malicious payloads blockage
(Nenova *et al*., 2019)	DoS and SQLi attacks blockage	Phishing and malicious payloads blockage
(Soewito and Andhika, 2019)	DoS, SQLi and phishing attacks blockage	Malicious payloads blockage
Our approach	DoS, SQLi, phishing and malicious payloads blockage	Future attack vectors

3 Research Methodology

The research methodology has been proposed after reviewing and referencing reputed conference papers and journal articles from ACM, IEEE and ScienceDirect. Maraj *et al*. (Maraj *et al*., 2017) conducted penetration testing on the network infrastructure possessing web server, monitoring server, two traditional firewalls and a NGFW. TCP and UDP flooding on port number 80 was executed for testing and verifying the security of network. NGFW was able to detect and block while the traditional firewalls were only able to detect the incoming flooding attacks.

The network system was divided into Trust and Untrust zones by Nenova *et al*. (Nenova *et al*., 2019). Outside network was placed in Untrust zone while engineering and administration networks were placed in Trust zone. Trust zone was built up using three firewall clusters possessing two firewalls in each cluster for providing a defence mechanism

against a wide range of attack vectors. In our research, the attack vectors which we must detect and block in order to uphold the security, integrity and availability of a network fabric is represented in the Table (Table 2).

Table 2: Description of attack vectors

S. No.	Attack vector	Description
1	High-rate DoS	Over utilises the network resources by flooding the target with traffic
2	Low and slow-rate DoS	Results in slow network resources depletion through small stream of slow traffic
3	IP spoofing	Overwhelms the network traffic resources by flooding the target by spoofing fake source IP addresses
4	SQLi	Injects malicious SQL query via the input data from client to application to retrieve database
5	Phishing	Social engineering attack for tricking individuals to reveal sensitive information, such as credentials
6	Malicious payloads	Attack components for compromising the target, such as remote code execution, privilege escalation

In our research, we have opted for NGFW cluster comprising of n1 NGFWs (where, n1 ∈ Number of NFGWs in a cluster) which are configured with strict security policies for detecting and blocking a wide range of incoming intrusions from Untrust zone. Every NGFW remains in synchronisation with each other due to the formation of firewall cluster. We have chosen to design Python script in order to ensure and validate the deployment of security policies on NGFW cluster. The flow of network traffic from Untrust zone to Trust zone is allowed to pass the NGFW cluster only when the traffic abides by all security policies. DPI and other security profiles deny/drop the threat traffic due to its failure to comply with security policies of NGFW cluster. The proposed policies for NGFW cluster are represented in the Table (Table 3).

Table 3: Proposed policies for NGFW cluster

S. No.	Name of policy	Source	Destination	Action	Profile	Description
1	Allow	Untrust zone	Trust zone	Allow	Configure and integrate strict antivirus, vulnerability protection, antispyware, URL filtering, file blocking and data filtering profiles	Allows network traffic from Untrust to Trust zone
2	LAN_WAN	Trust zone	Untrust zone	Allow		Allows network traffic from Trust to Untrust zone
3	Intra-Zone	Any	Intra	Allow		Allows network traffic from one internal zone to another internal zone

4	Inter-Zone	Any	Any	Deny	-	Denies network traffic from internal zone to external zone

The filtered traffic from NGFW cluster hits the VIP of LB. We have opted to configure and integrate the pool members with VIP in order to enable synchronisation of all n2 pool members (where, n2 ∈ Number of pool members) with each other. Least-Connection based policies have been selected for LB in order to load balance the filtered traffic using VIP. These redundant policies transfer the request from VIP to one of the pool members which possesses least number of active connection requests in order to ensure the balanced utilisation of all n2 pool resources. Finally, the permission is granted to access the web application which is locally hosted by all pool members on port 80. The flowchart of the network traffic traversal within the network fabric is illustrated in the Figure (Figure 1).

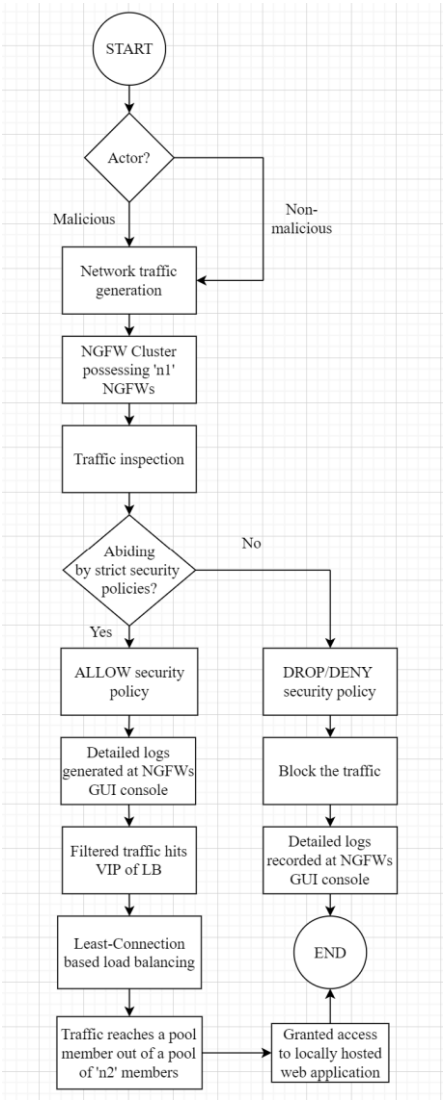

Figure 1: Flow chart of network traffic flow.

4 Design Specification

The word-based description of the proposed algorithm is illustrated as follows:

1: Initialise:
2: Set TRUST_ZONE ← TZ
3: Set UNTRUST_ZONE ← UZ
4: Set INTERNET_CLOUD ← IC
5: Set LINUX_MACHINE ← KALI
6: Set ROUTER ← RTR
7: Set SWITCH ← SWT
8: Set MANAGEMENT_CLOUD ← MGMTC
9: Set NEXT_GENERATION_FIREWALL ← NGFW
10: Set NEXT_GENERATION_FIREWALL_CLUSTER ← NGFWC
11: Set NEXT_GENERATION_FIREWALL_CLUSTER_SWITCH ← NGFWC_SWITCH
12: Set LOAD_BALANCER ← LB
13: Set POOL_MEMBER ← WIN
14: function UZ (IC, RTR, SWT, KALI) { // Defining Untrust zone
15: Integrate and configure IC, RTR and SWT // WAN configurations for catering internet
16: Configure KALI // Generates malicious & non-malicious traffic
17: Integrate KALI with SWT } // Providing internet connection in attacker's machine
18: function TZ (NGFW, NGFWC, LB, WIN) { // Defining Trust zone
19: function NGFWC () { // Defining NGFW cluster
20: Configure RTR and SWT
21: for i ← 2 to n1 do { // where n1 ∈ Number of NFGWs allowed by vendor in a cluster
22: Integrate n1 NGFW with SWT // Providing internet connection to n1 NGFWs
23: Integrate MGMTC with n1 NGFW // Accessing MGMT GUI n1 NGFWs
24: Execute NGFWC } // High-availability clustering for n1 NGFWs synchronisation
25: Commit strict security rules on NGFW cluster // Deploying security policies
26: Load Python script on NGFW API // Ensuring security rules deployment
27: Integrate NGFWC with NGFWC_SWITCH
28: function LB () { // Defining LB
29: Integrate LB with NGFWC through NGFWC_SWITCH
30: Integrate MGMTC with LB // To access MGMT GUI of LB }
31: function WIN () { // Defining pool member
32: for j ← 2 to n2 do { // where n2 ∈ Number of pool members allowed by LB vendor
33: Integrate n2 WIN with virtual IP (VIP) of LB // Synchronising n2 pool members
34: Integrate n2 WIN with NGFWC through NGFWC_SWITCH
35: Commit Least-Connection load balancing rules on LB // Deploying redundancy policies
36: Locally host the web application at port 80 for n2 WIN
37: }}} // Algorithm terminates

The network fabric has been divided into two parts i.e., Trust zone and Untrust zone. Untrust zone comprises of Linux machine, internet cloud, router, and switch while the remaining networking components constitutes the Trust zone. Linux machine has been selected to generate malicious and non-malicious network traffic while internet cloud, router

and switch possess WAN configurations for catering the internet connection within whole network fabric. Internet connection has been extended towards Linux machine through switch for allowing threat actors to launch attack vectors towards trust zone. WAN configurations on router and switch have been executed to provide internet connection on each NGFW. Each NGFW has been connected to management internet cloud in order to access their MGMT GUIs. The number of nodes allowed in a cluster varies from vendor to vendor which should be taken into consideration while defining the number of NGFWs in a cluster.

High-availability firewall clustering has been performed for synchronising all NGFWs with each other within a cluster. NFGW has been geared up with strict security policies, DoS protection profile, antivirus, vulnerability protection, antispyware, URL filtering, malware file blocking and data filtering in order to detect and block a wide range of attack vectors. Python script has been deployed on the NGFW API to validate the deployment of security policies. The NGFW cluster has been integrated with another switch for allowing the connection of NGFWs with load balancer and web servers. Load balancer has been connected to management internet cloud in order to access its MGMT GUI.

The number of pool members allowed by load balancer varies from vendor to vendor which should be taken into consideration while integrating each pool member with LB. Strict Least-Connection load balancing rules have been deployed on load balancer in order to ensure the least connection based high availability of web application which is locally hosted through common public IP of n2 pool members at port number 80. The network traffic traversal starts from internet cloud which travels from router and switch towards attacking machine and NGFW cluster. Network traffic inspection is carried out by NGFWs in accordance with the security policies which allows the clean traffic while dropping/denying the malicious traffic. Clean traffic is balanced through the redundancy policies of LB before hitting the pool members. The network fabric protype which is generated through the above algorithm is illustrated in the Figure (Figure 2).

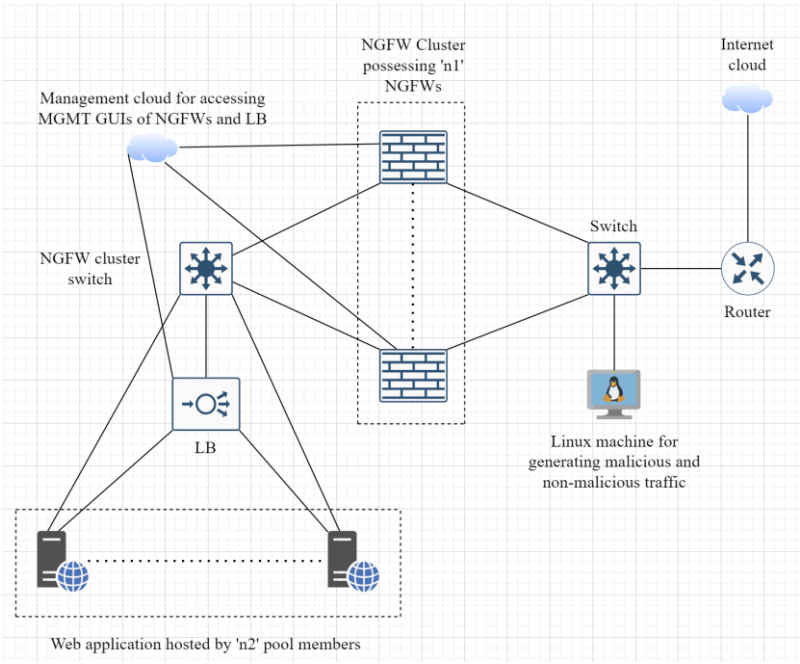

Figure 2: Network fabric prototype.

5 Implementation

The research-based implementation of the proposed network fabric has taken place by loading and configuring certain images on Emulated Virtual Environment – Next Generation (EVE-NG) 5.0.1-10 which was deployed on VMware Workstation Pro – 16.2.4. The hardware of Windows 11 Home base-machine comprises of 32.0 GB RAM, 1 TB SSD and Intel Core i7 – 10th Gen CPU. The hardware specifications for EVE-NG VM were set to 30 GB RAM, 160 GB Hard Disk (SCSI) and Bridged (Automatic) Network Adapter.

Default cloud provided by EVE-NG has been selected for the deployment of Internet and Management cloud. Kali Linux machine has been selected for generating malicious and non-malicious traffic. Single Kali has been taken into consideration for dual purposes due to hardware resources limitation. Two Palo Alto NGFWs have been selected for defining a cluster possessing n1 NGFWs. Switch 2 has been selected as NGFW cluster switch while Switch 1 has been selected as a switch which provides internet connection to Kali and NGFW cluster. Two Windows machines have been taken into consideration for defining a pool of n2 members. Private IPs of both Windows machines have been merged as one public IP i.e., 11.1.1.100/24 of Windows machines in order to make them visible outside Trust zone. The details of images which were deployed on EVE-NG VM in order to build the proposed network fabric are described in the Table (Table 4).

Table 4: List of images

S. No.	Vendor	Name and version of image	Networking component	Interface	IP address
1	Cisco	vios-15	Router	Gi0/1	192.168.101.149/22
				Gi0/0	11.1.1.10/24
		viosl2-15.5	Switch 1	Gi0/0, Gi0/1, Gi0/2, Gi0/3	-
			Switch 2	Gi0/0, Gi0/1, Gi0/2, Gi0/3, Gi1/0	-
2	Offensive Security	linux-kali-2019.3	Linux	e0	11.1.1.80/24
3	Palo Alto networks	paloalto-9.0.4	First firewall	mgmt	192.168.101.121/22
				eth1/1	High availability (HA Cluster)
				eth1/2	
				eth1/3	10.1.1.1/24
				eth1/4	11.1.1.1/24
			Second firewall	mgmt	192.168.101.122/22
				eth1/1	High availability

				eth1/2	(HA Cluster)
				eth1/3	10.1.1.1/24
				eth1/4	11.1.1.1/24
4	F5	bigip-14.1.1-0.0	Load balancer	Mgmt	192.168.101.120/22
				E1.1	10.5.5.1/24
				E1.2	10.1.1.100/24
				E1.3	10.6.6.1/24
5	Microsoft	win-10ENT	Windows 1	e0	10.5.5.10/24
				e1	10.1.1.130/24
			Windows 2	e0	10.6.6.10/24
				e1	10.1.1.50/24

The script files which were deployed on the proposed network fabric are illustrated in the Table (Table 5).

Table 5: List of script files

S. No.	Folder	Language	Version	Name	Description
1	NGFW	Python	3.9	Ensure Security Rule.py	Compiled at first Palo Alto NGFW API to ensure the deployment of security policies on NGFW cluster
2	kite	Python	3.9	mycode.py	Deployed on both Windows 10. This file is backend of web application recording roll number and name of student
		HTML	-	index.html	Deployed on both Windows 10. The file is frontend of web application

XAMPP was installed on both Windows machines in order to locally host the 'kite' folder. Port number 80 of Windows 10 public IP grants the access of web application from Untrust zone in order to ensure the privacy of Windows machines private IPs. MySQL was used to store the database details of web application. The database 'kite' possessing a table 'student' with two columns named 'roll' and 'name' was used to store the roll number and name of student. Windows machines allows a user to browse the web application along with internet. The proposed network fabric which was deployed on EVE-NG server is illustrated in the Figure (Figure 3).

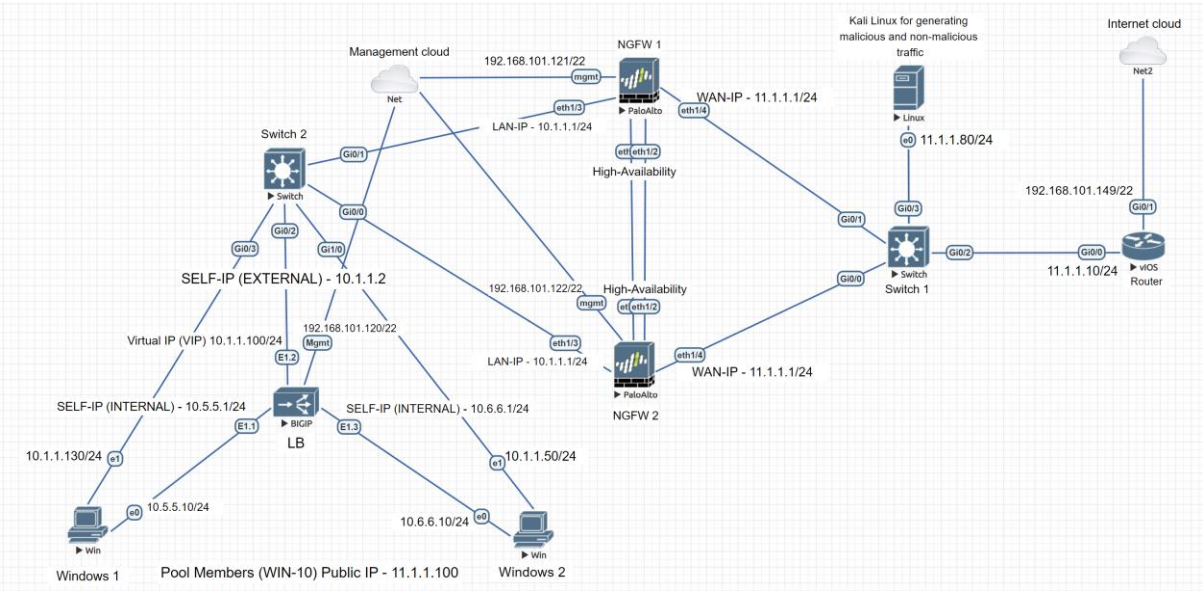

Figure 3: Proposed network fabric.

6 Evaluation

Critical evaluation of the proposed network fabric has been conducted through a series of experiments on the fabric along with well-known attack vectors in order to test the functionality and effectiveness of fabric against threat vectors. All six attack vectors were generated from Untrust zone towards Trust zone. The explanation and outcome of the research experiments have been illustrated in the following subsections.

6.1 Detection and blockage of high-rate DoS attacks

Hping3 tool was used to generate the high-rate DoS attacks from Linux machine towards victim machine i.e., web application. Malicious TCP SYN packets possessing packet count of 10,000 bytes along with data size of 10,000 bytes were flooded towards the target machine. The TCP SYN flooded packets were unable to sniff inside Trust zone because the NGFW cluster dropped the malicious packets at Untrust zone itself. The detection and blockage of high-rate DoS attacks has been represented in the Figure (Figure 4).

Type	Name	From Zone	To Zone	Source address	S... U...	Destination address	To Port	Application	Action	Severity
packet	TCP SYN with data	WAN-ZONE	WAN-ZONE	11.1.1.80		11.1.1.100	80	not-applicable	drop	informational
packet	TCP SYN with data	WAN-ZONE	WAN-ZONE	11.1.1.80		11.1.1.100	80	not-applicable	drop	informational
packet	TCP SYN with data	WAN-ZONE	WAN-ZONE	11.1.1.80		11.1.1.100	80	not-applicable	drop	informational
packet	TCP SYN with data	WAN-ZONE	WAN-ZONE	11.1.1.80		11.1.1.100	80	not-applicable	drop	informational

Figure 4: NGFW logs for high-rate DoS attacks.

6.2 Detection and blockage of low and slow-rate DoS attacks

Low and slow-rate DoS attacks on web application were generated through Linux machine using 'Slowloris' tool[1]. The web application was slowly and steadily flooded by 1000 HTTP

[1] https://github.com/gkbrk/slowloris

proxy sockets. NGFW cluster detected the threat pattern and dropped the malicious packets before entering the Trust zone. The detection and blockage of low and slow-rate DoS attacks has been illustrated in the Figure (Figure 5).

Type	Name	From Zone	To Zone	Source address	S... U...	Destination address	To Port	Application	Action	Severity
vulnerability	Slowloris HTTP Flooding Denial-of-Service Brute Force Attempt Detection	WAN-ZONE	LAN-ZONE	11.1.1.80		11.1.1.100	80	web-browsing	drop	critical
vulnerability	HTTP GET Request Without Header Detection	WAN-ZONE	LAN-ZONE	11.1.1.80		11.1.1.100	80	web-browsing	drop	informational

From Zone	To Zone	Source	Destination	From Port	To Port	Protocol	Application
WAN-ZONE	LAN-ZONE	11.1.1.80	11.1.1.100	55920	80	6	web-browsing
WAN-ZONE	LAN-ZONE	11.1.1.80	11.1.1.100	55796	80	6	web-browsing
WAN-ZONE	LAN-ZONE	11.1.1.80	11.1.1.100	55766	80	6	web-browsing
WAN-ZONE	LAN-ZONE	11.1.1.80	11.1.1.100	55898	80	6	web-browsing

Figure 5: NGFW logs for low and slow-rate DoS attacks.

6.3 Detection and blockage of IP spoofing attacks

Hping3 tool was used to generate IP spoofing attacks on web application through Linux machine. Malformed TCP SYN packets possessing packet count of 2,000 bytes along with data size of 2,000 bytes were flooded towards the target machine using spoofed source IP addresses. Spoofed IP packets were dropped at Untrust zone itself through NGFW cluster. The detection and blockage of IP spoofing attacks has been represented in the Figure (Figure 6).

Type	Name	From Zone	To Zone	Source address	S... U...	Destination address	To Port	Application	Action	Severity
packet	TCP SYN with data	WAN-ZONE	WAN-ZONE	58.89.25.161		11.1.1.100	80	not-applicable	drop	informational
packet	TCP SYN with data	WAN-ZONE	WAN-ZONE	30.233.213.72		11.1.1.100	80	not-applicable	drop	informational
packet	TCP SYN with data	WAN-ZONE	WAN-ZONE	3.253.157.214		11.1.1.100	80	not-applicable	drop	informational
packet	TCP SYN with data	WAN-ZONE	WAN-ZONE	6.104.79.40		11.1.1.100	80	not-applicable	drop	informational

Figure 6: NGFW logs for IP spoofing attacks.

6.4 Detection and blockage of SQLi attacks

SQLi attacks on web application scripts were generated through Linux machine using sqlmap tool. Data fields of HTML and Python files were rigorously injected through malicious SQL queries. NGFW cluster detected the attack pattern and dropped the maliciously crafted SQL queries before exploiting the database. The detection and blockage of SQLi attacks has been illustrated in the Figure (Figure 7).

Type	Name	From Zone	To Zone	Source address	S... U...	Destination address	To Port	Application	Action	Sev...	File Name
vulnerability	HTTP SQL Injection Attempt	WAN-ZONE	LAN-ZONE	11.1.1.80		11.1.1.100	80	web-browsing	drop	low	mycode.py
vulnerability	HTTP SQL Injection Attempt	WAN-ZONE	LAN-ZONE	11.1.1.80		11.1.1.100	80	web-browsing	drop	low	mycode.py
vulnerability	HTTP SQL Injection Attempt	WAN-ZONE	LAN-ZONE	11.1.1.80		11.1.1.100	80	web-browsing	drop	low	mycode.py
vulnerability	HTTP SQL Injection Attempt	WAN-ZONE	LAN-ZONE	11.1.1.80		11.1.1.100	80	web-browsing	drop	low	mycode.py
vulnerability	HTTP SQL Injection Attempt	WAN-ZONE	LAN-ZONE	11.1.1.80		11.1.1.100	80	web-browsing	drop	low	mycode.py
vulnerability	HTTP SQL Injection Attempt	WAN-ZONE	LAN-ZONE	11.1.1.80		11.1.1.100	80	web-browsing	drop	low	mycode.py
vulnerability	HTTP SQL Injection Attempt	WAN-ZONE	LAN-ZONE	11.1.1.80		11.1.1.100	80	web-browsing	drop	low	index.html

Figure 7: NGFW logs for SQLi attacks.

6.5 Detection and blockage of phishing attempts

'Zphisher' tool was used to generate maliciously crafted phished websites for the web application through Linux machine[2]. The phished websites were crafted using templates of famous organisations like Facebook, Google, Microsoft, and LinkedIn in order to trick anyone for revealing their sensitive information. The URLs of phished websites were blocked by NGFW cluster when the browsers of Windows machines were redirecting themselves towards compromised websites. The detection and blockage of phishing attempts has been represented in the Figure (Figure 8).

Category	URL Category List	URL	From Zone	To Zone	Source	S... U...	Destination	Applicati...	Action
PHISHING_ATTEMPT	PHISHING_ATTEMPT,web-hosting,high-risk	casio-bandwidth-potentially-trades.trycloudflare.com/	LAN-ZONE	WAN-ZONE	10.1.1.50		104.17.124.55	ssl	block-url
PHISHING_ATTEMPT	PHISHING_ATTEMPT,web-hosting,high-risk	casio-bandwidth-potentially-trades.trycloudflare.com/	LAN-ZONE	WAN-ZONE	10.1.1.50		104.17.124.55	ssl	block-url
PHISHING_ATTEMPT	PHISHING_ATTEMPT,web-hosting,high-risk	casio-bandwidth-potentially-trades.trycloudflare.com/	LAN-ZONE	WAN-ZONE	10.1.1.50		104.17.124.55	ssl	block-url
PHISHING_ATTEMPT	PHISHING_ATTEMPT,web-hosting,high-risk	casio-bandwidth-potentially-trades.trycloudflare.com/	LAN-ZONE	WAN-ZONE	10.1.1.50		104.17.124.55	ssl	block-url
PHISHING_ATTEMPT	PHISHING_ATTEMPT,web-hosting,high-risk	casio-bandwidth-potentially-trades.trycloudflare.com/	LAN-ZONE	WAN-ZONE	10.1.1.130		104.17.124.55	ssl	block-url

Type	Name	From Zone	To Zone	Source address	S... U...	Destination address	To Port	Application	Action	Severity
spyware	Suspicious TLS Evasion Found	LAN-ZONE	WAN-ZONE	10.1.1.50		74.125.193.113	443	google-base	alert	informational
spyware	Suspicious TLS Evasion Found	LAN-ZONE	WAN-ZONE	10.1.1.50		209.85.202.95	443	google-base	alert	informational

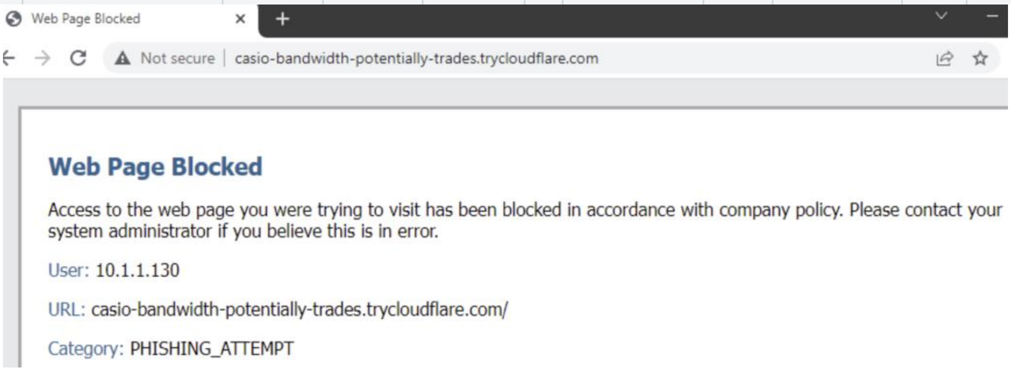

Figure 8: NGFW logs for phishing attempts.

6.6 Detection and blockage of malicious payloads (.exe and .pdf)

Malicious .exe and .pdf payloads were generated through Linux machine using Metasploit framework. The payloads were crafted using generic names, such as WindowsUpdate.exe and YashPayslip.pdf, in order to trick anyone for trusting them. NGFW cluster detected the compromised payloads and denied their accessibility on both Windows machines. The detection and blockage of malicious payloads has been illustrated in the Figure (Figure 9).

Category	File Name	F... U...	Name	From Zone	To Zone	Source address	S... U...	Destination address	To Port	Application	Action
medium-risk	YashPayslip.pdf		Adobe Portable Document Format (PDF)	LAN-ZONE	WAN-ZONE	10.1.1.130		11.1.1.80	80	web-browsing	deny
medium-risk	WindowsUpdate.exe		Microsoft PE File	LAN-ZONE	WAN-ZONE	10.1.1.130		11.1.1.80	80	web-browsing	deny
medium-risk	YashPayslip.pdf		Adobe Portable Document Format (PDF)	LAN-ZONE	WAN-ZONE	10.1.1.50		11.1.1.80	80	web-browsing	deny
medium-risk	WindowsUpdate.exe		Microsoft PE File	LAN-ZONE	WAN-ZONE	10.1.1.50		11.1.1.80	80	web-browsing	deny

[2] https://github.com/htr-tech/zphisher

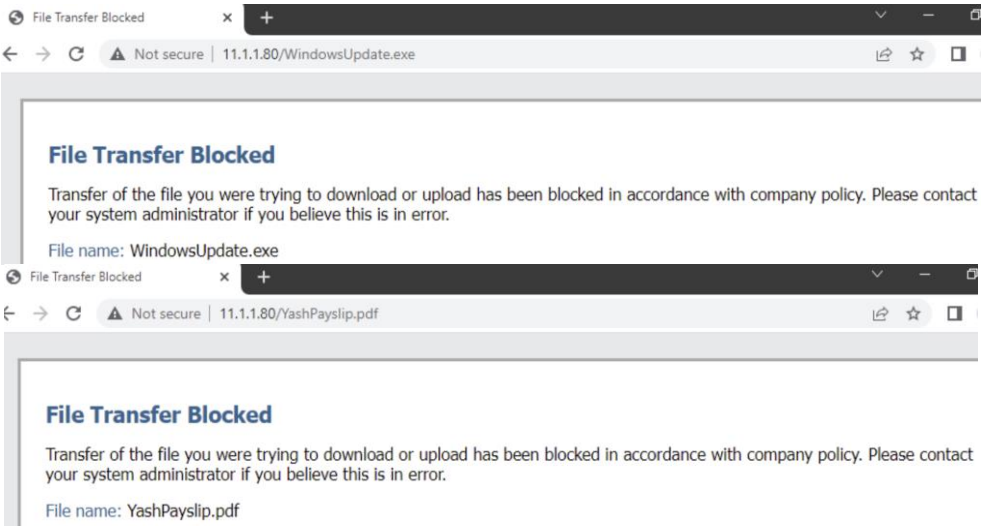

Figure 9: NGFW logs for .exe and .pdf malicious payloads.

On the other hand, the non-malicious traffic from Untrust zone towards Trust zone is allowed by NGFW cluster and LB. The Figure (Figure 10) represents the allowance of non-malicious traffic from Linux machine towards web application. The incoming connection requests are load-balanced by VIP using Least-Connection based policies which redirects the traffic towards the web application of such Windows machine which possesses the minimum number of ongoing connection requests in order eradicate the possibilities of over utilising a particular pool member.

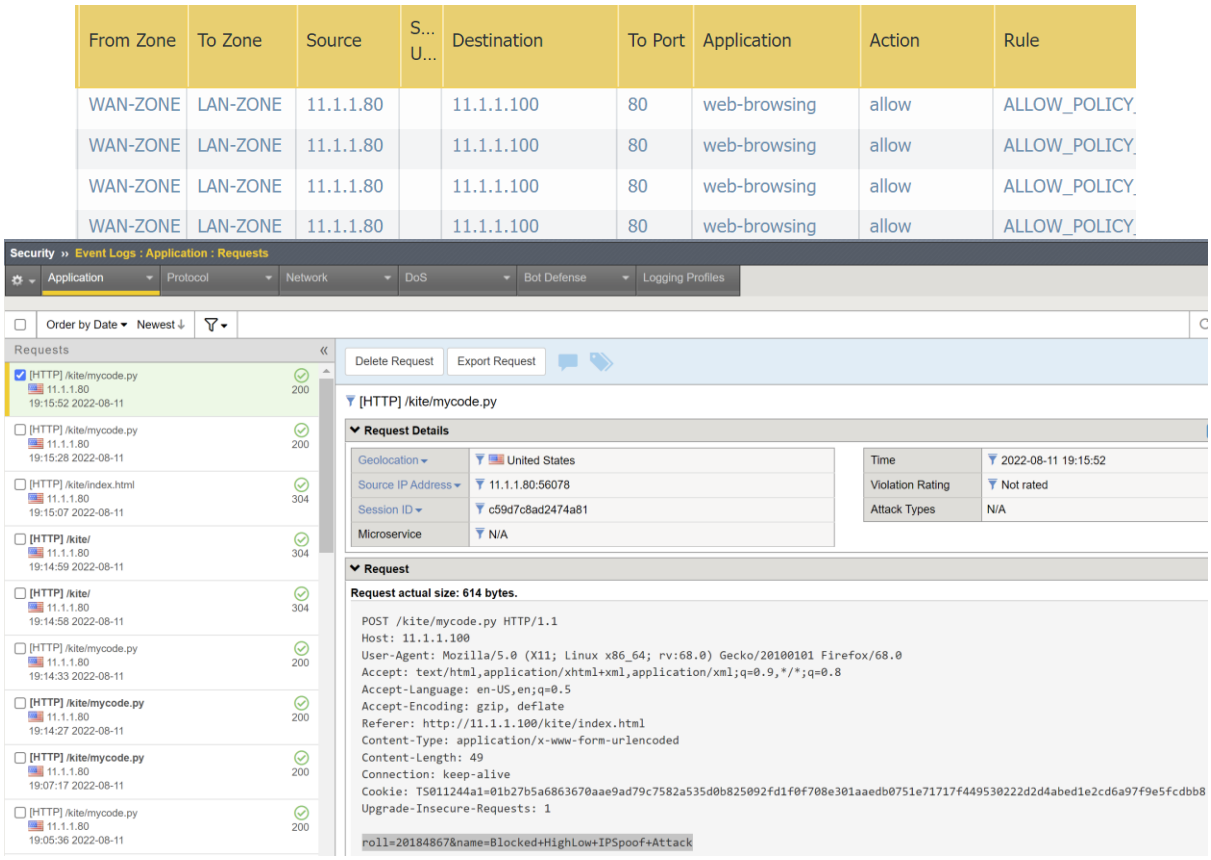

Figure 10: NGFW and LB logs for allowing non-malicious traffic.

The experimentation Table (Table 6) depicts the number of successful and unsuccessful experiments along with the rectification strategies for failed experiments.

Table 6: Experimentation table

Experiment number	Detected and blocked	Undetected	Outcome	Description
1	High-rate DoS	Low and slow-rate DoS	Unsuccessful	Small stream of low and slow-rate DoS is difficult to distinguish from normal network traffic
2	High and slow-rate DoS, IP spoofing	-	Successful	Deployed strict DoS protection policies for low stream of flooding attacks on NGFW cluster
3	High and slow-rate DoS, IP spoofing, SQLi	Phishing attempt	Unsuccessful	Browsers of pool resources were accessing few phished websites
4	High and slow-rate DoS, IP spoofing, SQLi, Phishing	-	Successful	Deployed strict URL filtering policies on NGFW cluster to carry out HTTP, HTTPS, DNS, SSL, and TLS inspection
5	High and slow-rate DoS, IP spoofing, SQLi, Phishing, Malicious .pdf payload	Malicious .exe payload	Unsuccessful	Pool resources (Win 10 machines) were presuming .exe Windows file extension as legitimate files
6	High and slow-rate DoS, IP spoofing, SQLi, Phishing, Malicious .exe and .pdf payloads	-	Successful	Deployed strict payload inspection policies on NGFW cluster to carry out inspection of .exe, .dll, .bin and .bat files

Above-mentioned attack vectors threaten the security, integrity, and availability of network resources in one or the other way. Flooding attack mainly focuses on depleting the network resources with malicious and malformed requests in order to compromise the security and availability of network infrastructure. Phishing attacks and malicious payloads mainly threatens the system security while SQLi attack focuses on distorting the database integrity.

Previous works focused on specific attack vectors that leaves the space of a network fabric which can provide a defence mechanism against a wide range of latest threat vectors. The successful detection and blockage of various threat vectors upholds the security, integrity and availability of a network fabric which helps in upscaling the overall defence capabilities of network infrastructures. In our research, we have tried to solve the problem statement

which illustrates the necessity of an all-rounded network fabric which can detect and block a wide range of recent attack vectors.

6.7 Discussion

The attack vectors which were taken into consideration in order to test the effectiveness of proposed research included flooding of network resources, SQL injections, phishing attempts, and malicious payloads. High-rate DoS attacks possessing packet count of 10,000 bytes and data size of 10,000 bytes were successfully detected and blocked at Untrust zone itself. Low and slow-rate DoS attacks possessing 1000 HTTP proxy sockets were successfully detected and blocked before hampering the Trust zone.

IP spoofing attacks possessing packet count of 2000 bytes and data size of 2000 bytes were successfully detected and blocked at Untrust zone itself. SQLi attacks were successfully detected and blocked before distorting the database of web application. Phishing attempts and Malicious payloads were successfully detected and blocked before Windows 10 pool resources tries to access them from Trust zone. Continuous improvement of security and redundancy policies of NGFW cluster and LB after rigorous experiments led to the successful evaluation of proposed network fabric. The successful detection and blockage of above-mentioned threat vectors proves the effectiveness of our proposed research in order to uphold the security, integrity, and availability of a network fabric which affirms its contribution in the field of cybersecurity.

However, the main limitation of the proposed approach is the successful detection and blockage of future attack vectors. In our proposed research, the strict NGFW cluster and LB policies were applied in accordance with the current situations, circumstances, and scenarios. Continuous research and improvement should be involved in order to provide a defence mechanism against the future threat vectors of different dynamics and patterns. The comparison of our approach with existing works is illustrated in the Table (Table 7).

Table 7: Comparing proposed solution with existing works

S. No.	Existing work	DoS		IP spoofing	SQL injection	Phishing attempt	Malicious payloads	
		High-rate	*Low and slow-rate*				*.exe*	*.pdf*
1	(Bhakthavatsalam and Malarkodi, 2016)	N/A	N/A	N/A	N/A	N/A	Yes	Yes
2	(Maraj *et al.*, 2017)	Yes	No	Yes	N/A	N/A	N/A	N/A
3	(Nenova *et al.*, 2019)	Yes	No	Yes	Yes	N/A	N/A	N/A
4	(Soewito and Andhika, 2019)	Yes	No	Yes	Yes	Yes	N/A	N/A
5	(Trabelsi and Zeidan, 2019)	Yes	Yes	Yes	N/A	N/A	N/A	N/A
6	(Kiratsata *et al.*, 2022)	Yes	No	Yes	N/A	N/A	N/A	N/A
7	Proposed solution	Yes	Yes	Yes	Yes	Yes	Yes	Yes

7 Conclusion and Future Work

The research question interrogated the techniques which can be used to uphold the security, integrity, and availability of a network fabric. The objectives of our proposed research included NGFW clustering, strict NGFW security policies, clubbing LB behind NGFW cluster and strict LB redundancy policies in order to defend the network fabric from a wide range of latest and popular threat vectors. The configuration and deployment of NGFW and LB rules took place after critically analysing the policies along with research-based evaluations which led to the successful detection and blockage of High-rate DoS, Low and slow-rate DoS, SQLi, Phishing attempts and Malicious payloads. Moreover, Python script was deployed on first NGFW in order to ensure the commitment and deployment of all security rules and configurations on NGFW cluster.

The follow-up future research project can be scaled to a large WAN using Hub-and-spoke network topology. Hub site may comprise of NGFW cluster possessing 'n1' NGFWs, load balancer and redundant 'n2' pool members which can be used to host the intranet resources of organisations or businesses. On the other hand, spoke site may comprise of various spokes which can be made using various end-devices such that each legitimate spoke can access the intranet resources with zero downtime in a safe and secure manner.

References

Allison, J. (2022) 'Simulation-based learning via Cisco Packet Tracer to Enhance the Teaching of Computer Networks', in *Proceedings of the 27th ACM Conference on on Innovation and Technology in Computer Science Education Vol. 1*. Dublin, Ireland, 08-13 July 2022, pp. 68-74, ACM. doi: 10.1145/3502718.3524739.

Bhakthavatsalam, P. K. and Malarkodi, B. (2016) 'Analysis of network infrastructure threats using SonicWALL analyser', in *2016 3rd International Conference on Devices, Circuits and Systems (ICDCS)*. Coimbatore, India, 03-05 March 2016, pp. 6–9, IEEE Xplore. doi: 10.1109/ICDCSyst.2016.7570612.

Blancaflor, E. B. *et al.* (2020) 'A Fault Tolerant and Secured Network Design for File and Application Sharing in a Mid-sized Business Environment', in *Proceedings of the 2020 5th International Conference on Cloud Computing and Internet of Things.* Okinawa, Japan, 22-24 September 2020, pp. 1-5, ACM. doi: 10.1145/3429523.3429528.

Chapman, P. (2021) 'Defending against insider threats with network security's eighth layer', *Computer fraud & security*, 2021(3), pp. 8–13, ScienceDirect. doi: 10.1016/S1361-3723(21)00029-4.

Daxian, W., Jishan, Z. and Jiujiu, Y. (2020) 'Research on intelligent Firewall for network security', in *Proceedings of the 2020 2nd International Conference on Robotics, Intelligent Control and Artificial Intelligence*. Shanghai, China, 17-19 October 2020, pp. 255-258, ACM. doi: 10.1145/3438872.3439090.

Garcia, M. and Hailu, Y. (2021) 'Security in intelligent home', *Journal of computing sciences in colleges*, 37(1), pp. 117–127, ACM. doi: 10.5555/3512469.3512483.

Hamilton, R. *et al.* (2020) 'Deep Packet Inspection in Firewall Clusters', in *2020 28th Telecommunications Forum (TELFOR).* Belgrade, Serbia, 24-25 November 2020, pp. 1–4, IEEE Xplore. doi: 10.1109/TELFOR51502.2020.9306651.

Khelf, R. and Ghoualmi-Zine, N. (2018) 'IPsec/Firewall Security Policy Analysis: A Survey', in *2018 International Conference on Signal, Image, Vision and their Applications (SIVA).* Guelma, Algeria, 26-27 November 2018, pp. 1–7, IEEE Xplore. doi: 10.1109/SIVA.2018.8660973.

Kiratsata, H. J. *et al.* (2022) 'Behaviour Analysis of Open-Source Firewalls Under Security Crisis', in *2022 International Conference on Wireless Communications Signal Processing and Networking (WiSPNET).* Chennai, India, 24-26 March 2022, pp. 105–109, IEEE Xplore. doi: 10.1109/WiSPNET54241.2022.9767176.

Liang, J. and Kim, Y. (2022) 'Evolution of Firewalls: Toward Securer Network Using Next Generation Firewall', in *2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC).* Las Vegas, NV, USA, 26-29 January 2022, pp. 0752–0759, IEEE Xplore. doi: 10.1109/CCWC54503.2022.9720435.

Loureiro, S. (2021) 'Security misconfigurations and how to prevent them', *Network security*, 2021(5), pp. 13–16, ScienceDirect. doi: 10.1016/s1353-4858(21)00053-2.

Maraj, A. *et al.* (2017) 'Testing of network security systems through DoS attacks', in *2017 6th Mediterranean Conference on Embedded Computing (MECO).* Bar, Montenegro, 11-15 June 2017, pp. 1–6, IEEE Xplore. doi: 10.1109/MECO.2017.7977239.

Miloslavskaya, N. (2021) 'A Brief Evolution of Network Protection Tools and Methods', *Procedia computer science*, 190(2021), pp. 590–596, ScienceDirect. doi: 10.1016/j.procs.2021.06.069.

Nenova, M. *et al.* (2019) 'Intrusion Detection System Model Implementation against DDOS attacks', in *2019 IEEE International Conference on Microwaves, Antennas, Communications and Electronic Systems (COMCAS).* Tel-Aviv, Israel, 04-06 November 2019, pp. 1–4, IEEE Xplore. doi: 10.1109/COMCAS44984.2019.8958346.

Neupane, K., Haddad, R. and Chen, L. (2018) 'Next Generation Firewall for Network Security: A Survey', in *SoutheastCon 2018.* St. Petersburg, FL, USA, 19-22 April 2018, pp. 1–6, IEEE Xplore. doi: 10.1109/SECON.2018.8478973.

Reynolds, R. (2020) 'It's time to rethink DDoS protection', *Network security*, 2020(1), pp. 6–8, ScienceDirect. doi: 10.1016/s1353-4858(20)30007-6.

SenthilKumar, P. and Muthukumar, M. (2018) 'A Study on Firewall System, Scheduling and Routing using pfsense Scheme', in *2018 International Conference on Intelligent Computing and Communication for Smart World (I2C2SW).* Erode, India, 14-15 December 2018, pp. 14–17, IEEE Xplore. doi: 10.1109/I2C2SW45816.2018.8997167.

Shanmugam, T. and Malarkodi, B. (2019) 'Analysis of Recent Challenges and Solutions in Network Security', in *2019 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT).* Kannur, India, 05-06 July 2019, pp. 902–907, IEEE Xplore. doi: 10.1109/ICICICT46008.2019.8993123.

Singh, A. *et al.* (2020) 'Security through Optimization Techniques of Firewall Rule Sets', in *2020 International Conference on Computation, Automation and Knowledge Management (ICCAKM).* Dubai, United Arab Emirates, 09-10 January 2020, pp. 452–455, IEEE Xplore. doi: 10.1109/ICCAKM46823.2020.9051476.

Soewito, B. and Andhika, C. E. (2019) 'Next Generation Firewall for Improving Security in Company and IoT Network', in *2019 International Seminar on Intelligent Technology and Its Applications (ISITIA).* Surabaya, Indonesia, 28-29 August 2019, pp. 205–209, IEEE Xplore. doi: 10.1109/ISITIA.2019.8937145.

Trabelsi, Z. and Zeidan, S. (2019) 'Resilence of Network Stateful Firewalls against Emerging DoS Attacks: A Case Study of the BlackNurse Attack', in *2019 IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA).* Abu Dhabi, United Arab Emirates, 03-07 November 2019, pp. 1–8, IEEE Xplore. doi: 10.1109/AICCSA47632.2019.9035323.

Tudosi, A. D., Balan, D. G. and Potorac, A. D. (2022) 'Secure network architecture based on distributed firewalls', in *2022 International Conference on Development and Application Systems (DAS).* Suceava, Romania, 26-28 May 2022, pp. 85–90, IEEE Xplore. doi: 10.1109/DAS54948.2022.9786092.

Waleed, A., Jamali, A. F. and Masood, A. (2022) 'Which open-source IDS? Snort, Suricata or Zeek', *Computer networks*, 213(2), pp. 12-23, ScienceDirect. doi: 10.1016/j.comnet.2022.109116.

Wan, B. and Xu, C. (2021) 'Application of Computer Information Technology in Internet', in *2021 4th International Conference on Information Systems and Computer Aided Education.* Dalian, China, 24-26 September 2021, pp. 2085-2089, ACM. doi: 10.1145/3482632.3484104.

Zhao, W., Juan, S. and Yawen, P. (2022) 'Design and Architecture of Local Health Platform', in *2022 2nd International Conference on Bioinformatics and Intelligent Computing.* Harbin, China, 21-23 January 2022, pp. 57-61, ACM. doi: 10.1145/3523286.3524515.

Xiao, M., Guo, M. and Lv, H. (2021) 'The Principle of Firewall Technology and Its Application in Computer Network Security', in *2021 3rd International Conference on Applied Machine Learning (ICAML).* Changsha, China, 23-25 July 2021, pp. 174–177, IEEE Xplore. doi: 10.1109/ICAML54311.2021.00044.

Zaki, M. *et al.* (2021) 'Cybersecurity Framework For Healthcare Industry Using NGFW', in *2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV).* Tirunelveli, India, 04-06 February 2021, pp. 196–200, IEEE Xplore. doi: 10.1109/ICICV50876.2021.9388455.

Zhou, L. (2022) 'Key technology research on the implementation of computer network security defense system', in *2022 3rd Asia-Pacific Conference on Image Processing, Electronics and Computers.* Dalian, China, 14-16 April 2022, pp. 658-661, ACM. doi: 10.1145/3544109.3544329.