Republic of Yemen

University of Science & Technology

Faculty of Computing and IT

Department of Cybersecurity and Networking

CUSTOMIZING NEXT-GENERATION FIREWALL FUNCTIONALITIES FOR ENVIRONMENT-SPECIFIC SECURITY NEEDS

A project report submitted in partial fulfillment of the requirements for the Degree of Bachelor of Cybersecurity and Networking

SUBMITTED BY

Omar Muawadh

Hossam Al-Dalali

Khalil Al-Dbiani

Amgad Almaazabi

SUPERVISOR

Dr. Redhwan Qasem Shaddad

2025م - 1446هـ

بسم الله الرحمن الرحيم

In the name of Allah, the Most Gracious, the Most Merciful

قَالَ اللهُ -عَزَّ وَجَلَّ-:

﴿فَتَعَالَى اللَّهُ الْمَلِكُ الْحَقُّ ۗ وَلَا تَعْجَلْ بِالْقُرْآنِ مِن قَبْلِ أَن يُقْضَىٰ إِلَيْكَ وَحْيُهُ ۖ وَقُل رَّبِّ زِدْنِي عِلْمًا﴾ [طه : 114]

Allah, the Almighty, said:

Then High above all be Allah, the True King. And be not in haste (O Muhammad SAW) with the Quran before its revelation is completed to you, and say: "My Lord! Increase me in knowledge."

Republic of Yemen

University of Science & Technology

Faculty of Computing and IT

Department of Cybersecurity and Networking

PROJECT APPROVAL STATEMENT

The project committee hereby approves the graduation project titled “**Customizing Next-Generation Firewall Functionalities for Environment-Specific Security Needs**” submitted by the students:

1. Hossam Al-Dalali
2. Omar Muawadh
3. Khalil Al-Dbiani
4. Amgad Almaazabi

has been accepted as part of the Bachelor’s degree program requirements.

Head of Computer Department

Dr. Radwan Al-Dailami

Program Coordinator

Dr. Redhwan Shaddad

Projects Committee Coordinator

Dr. Fahd Al-Qasim

Date: / / 2025

Republic of Yemen

University of Science & Technology

Faculty of Computing and IT

Department of Cybersecurity and Networking

DECLARATION OF AUTHENTICITY

We, the project team behind “**Customizing Next-Generation Firewall Functionalities for Environment-Specific Security Needs**” affirm that all theoretical and practical content presented in this project is the result of our own efforts, except for the referenced materials attributed to reviewers. Furthermore, we confirm that this work has not been submitted to any other academic or scientific institution.

Project Team

Signature

1. Hossam Al-Dalali
2. Omar Muawadh
3. Khalil Al-Dbiani
4. Amgad Almaazabi

Supervisor

Dr. Redhwan Shaddad

DEDICATION

First and foremost, praises and thanks be to Allah. We extend our heartfelt and profound gratitude to our supervisor, **Dr. Redhwan Shaddad**, and our esteemed teachers, **Dr. Fahd Al-Qasm, Dr. Hajar Al-Suhbani, and Eng. Balqis Alwa,** for their valuable guidance and unwavering support throughout this project. Their mentorship has been instrumental not only in the successful completion of this work but also throughout our entire academic journey at the University. We would also like to express our deepest gratitude to our **parents**, whose endless love, encouragement, and sacrifices have been a constant source of strength and inspiration throughout our lives and studies.

ABSTRACT

Network security is essential for safeguarding data integrity, confidentiality, and maintaining reliable operations as cyber threats continue to grow in complexity. This project focuses on strengthening network security by customizing Next-Generation Firewall (NGFW) functionalities to meet the specific security needs of various IT environments, including LAN, Cloud, and Data Center infrastructures. NGFWs offer advanced features beyond traditional firewalls, such as intrusion prevention, application control, and deep packet inspection; however, activating all these features simultaneously can burden network resources, leading to performance issues. The project aims to address these challenges by developing tailored configurations that balance security and performance while adhering to organizational policies. Using simulations, the project demonstrates how properly customized NGFWs enhance threat detection and operational efficiency, with results across different environments revealing how optimized configurations can minimize resource consumption while effectively mitigating risks. Key findings highlight that environment-specific NGFW customization improves traffic management, threat prevention, and system responsiveness, providing a practical framework for organizations to enhance their cybersecurity posture while maintaining efficient network performance.

ARABIC ABSTRACT

تُعد أمان الشبكات ضرورية لحماية سلامة البيانات وسريتها وضمان استمرارية العمليات بكفاءة، خاصة مع تزايد تعقيد التهديدات السيبرانية. يركز هذا المشروع على تعزيز أمن الشبكات من خلال تخصيص وظائف الجدار الناري من الجيل التالي (NGFW) لتلبية الاحتياجات الأمنية الخاصة بمختلف بيئات تقنية المعلومات، بما في ذلك الشبكات المحلية (LAN)، والحوسبة السحابية، ومراكز البيانات. توفر الجدران النارية الحديثة ميزات متقدمة تتجاوز تلك الموجودة في الجدران التقليدية، مثل منع التسلل، والتحكم في التطبيقات، وفحص الحزم العميق؛ ومع ذلك، فإن تفعيل جميع هذه الميزات في الوقت نفسه قد يُثقل موارد الشبكة، مما يؤدي إلى مشكلات في الأداء. يهدف المشروع إلى معالجة هذه التحديات من خلال تطوير إعدادات مخصصة توازن بين الأمان والأداء مع الالتزام بسياسات المؤسسة. ومن خلال عمليات المحاكاة، يُظهر المشروع كيف يُمكن أن تؤدي تخصيصات الجدار الناري المصممة بشكل صحيح إلى تحسين اكتشاف التهديدات والكفاءة التشغيلية. كما تكشف النتائج عبر البيئات المختلفة كيف يمكن أن تقلل التكوينات المحسّنة من استهلاك الموارد مع التخفيف الفعّال للمخاطر. وتُبرز النتائج الرئيسية أن التخصيص المحدد لبيئة الجدار الناري يُحسّن إدارة حركة المرور، ويمنع التهديدات، ويُعزز استجابة النظام، مما يوفر إطارًا عمليًا للمؤسسات لتعزيز وضعها في مجال الأمن السيبراني مع الحفاظ على أداء شبكي فعّال.

TABLE OF CONTENTS

FRONT MATTER

CHAPTER ONE: INTRODUCTION

CHAPTER TWO: LITERATURE REVIEW

CHAPTER THREE: METHODOLOGY

CHAPTER FOUR: IMPLEMENTATION AND RESULTS

CHAPTER FIVE: CONCLUSIONS AND RECOMMENDATIONS

REFERENCES

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

ACC ------------------------ Application Command Center

App-ID -------------------- Application Identification

DMZ ----------------------- Demilitarized Zone

DPI ------------------------- Deep Packet Inspection

GNS3 ---------------------- Graphical Network Simulator-3

HA -------------------------- High Availability

IDS ------------------------- Intrusion Detection System

IPS ------------------------- Intrusion Prevention System

LAN ------------------------ Local Area Network

MFA ----------------------- Multi-Factor Authentication

ML ------------------------- Machine Learning

NAT ------------------------ Network Address Translation

NGFW --------------------- Next- Generation Firewall

OSPF ---------------------- Open Shortest Path First

PAFW --------------------- Palo Alto Firewall

PAN ------------------------ Palo Alto Networks

PAT ------------------------ Port Address Translation

SDN ------------------------ Software Defined Networks

SSL ------------------------- Secure Sockets Layer

TLS ------------------------ Transport Layer Security

User-ID -------------------- User Identification

UTM ----------------------- Unified Threat Management

VPN ------------------------ Virtual Private Network

WAF ----------------------- Web Application Firewall

CHAPTER ONE

INTRODUCTION

1.1. Introduction

In today's interconnected world, networks form the backbone of communication, fueling innovation and efficiency across sectors. With the rise in cyber threats, protecting these networks is more important than ever. Next-Generation Firewalls (NGFWs) are essential in securing network integrity, offering advanced security features beyond those of traditional firewalls. This project highlights the role of NGFWs in enhancing network defenses and explores their practical applications across diverse IT environments.

NGFWs operate seamlessly within three primary environments: data centers, cloud infrastructures, and local networks. In data centers, NGFWs manage high traffic volumes, ensuring efficient data flow while protecting against sophisticated threats. In cloud settings, NGFWs provide scalable security solutions that adapt to dynamic workloads and virtual resources [1]. In local networks, they offer tailored protections to safeguard organizational data and maintain network performance.

However, deploying NGFWs presents challenges. Inefficiencies may occur from uninspected data transmission or the failure to perform key functions. Activating all features indiscriminately can lead to excessive load, slowing network performance. Additionally, poor design and configuration may introduce vulnerabilities that compromise the firewall's effectiveness [2].

This project emphasizes the importance of aligning NGFW capabilities with organizational policies to prevent unauthorized data access, tailoring security features to specific needs based on the environment, and implementing configurations based on expert guidance. Using GNS3 simulations, this study demonstrates how effectively deployed NGFWs can enhance both network security and operational efficiency [3].

1.2. Motivations and Importance

In recent years, the cybersecurity landscape has grown increasingly complex, with threats becoming more sophisticated and difficult to detect. Traditional firewalls, which primarily focus on basic filtering, are no longer sufficient to counter these evolving challenges [4]. As a result, organizations are motivated to adopt Next-Generation Firewalls (NGFWs) to address the limitations of conventional security measures. NGFWs offer a more comprehensive approach by combining features such as intrusion prevention, application control, and deep packet inspection, which are essential to confront today's diverse threat landscape effectively.

The deployment of NGFWs also stems from the need for robust security tailored to specific network environments. Each setting—whether a data center, cloud infrastructure, or enterprise network—has distinct performance and security requirements. Activating all NGFW features at once may place an excessive burden on system resources, potentially causing inefficiencies or operational issues.

By adopting a flexible, environment-specific approach to NGFW implementation, organizations can better align their security measures with their unique needs. Tailoring NGFW functionalities improves adaptability and responsiveness, supporting an enhanced security posture and optimized network performance [3]. Developing a framework for NGFW customization also provides a valuable guide for organizations, helping them implement and refine network security strategies that are both effective and efficient. This framework serves as a blueprint for achieving a balanced and proactive defense across various operational contexts.

1.3. Problem Statement

The main problem in this project is managing the balance between comprehensive security and optimal performance in Next-Generation Firewalls (NGFWs). While NGFWs offer advanced functionalities like intrusion prevention, deep packet inspection, and application control, enabling all features simultaneously can lead to feature overload, overwhelming network resources and causing significant performance degradation. This overload strains processing power and bandwidth, slowing down network operations and affecting critical response times. Additionally, inadequate traffic inspection, especially in traditional firewall configurations, may allow malicious content to bypass security defenses if not properly configured. Lastly, configuration vulnerabilities arising from poorly designed policies or inconsistencies can create exploitable security gaps, leaving networks exposed to various threats.

1.4. Objectives

The objectives of this project are centered around enhancing the security posture of IT environments through the effective implementation of Next-Generation Firewalls (NGFWs). Key goals include identifying specific security needs of various environments, evaluating different types of NGFWs, and developing customized configurations that address unique risks. Additionally, the project aims to provide organizations with insights into best practices for NGFW deployment and management, ensuring they remain resilient against evolving cyber threats. Ultimately, the project seeks to create a robust framework that supports continuous improvement in security measures.

This project aims to:

- Develops and customize NGFW functionalities to meet the specific security needs of various IT environments, prioritizing essential features to avoid performance degradation due to feature overload.
- Enhance network security by implementing NGFWs to protect data from unauthorized access across data centers, cloud infrastructures, and local networks.
- Simulate and test NGFW deployments, assessing their effectiveness and performance in diverse conditions to ensure practical and real-world applicability.

1.5. Scope of Study

The project focuses on designing and customizing Next-Generation Firewall (NGFW) functionalities to meet the security needs of three primary environments: cloud, data centers, and local networks. This is achieved using the GNS3 platform to simulate network environments and test firewall performance, emphasizing features such as traffic monitoring, application control, and threat prevention. The scope is limited to virtualization-based simulations and does not include testing in real-world environments or advanced enterprise integrations, while considering resource constraints and evolving security threats.

1.6. Project Methodology

The methodology adopted for this project followed a structured and systematic approach to ensure comprehensive analysis and successful implementation. It began with the adoption of the project idea, followed by gathering general information to establish a foundational understanding of the subject. Key problems and objectives were then identified to guide the research direction. A detailed study of IT environments and network visibility was conducted, leading to the identification of solution mechanisms. Theoretical background and previous studies were reviewed to build a robust knowledge base and identify gaps.

The weaknesses and security requirements for the three IT environments were thoroughly analyzed, and these environments were depicted in detailed diagrams for clarity. The project then moved into the configuration and execution phase, where the proposed solutions were implemented. Rigorous review and testing were conducted to ensure functionality and reliability. Finally, comprehensive documentation was prepared to capture all aspects of the project.

Throughout the process, the methodology adhered to the principles of preparation, planning, design, implementation, operation, and optimization, ensuring a holistic and efficient approach to achieving the project's goals.

1.7. Project Contents Overview

1. Literature Review

This chapter will cover the concept of firewalls, their historical development from inception to the present, as well as their benefits, types, and the various environments in which they are utilized, such as cloud networks, data centers, and local networks. The project will also discuss four studies similar to our current project, outlining the benefits and limitations of each study, the differences between their results and ours, and how our study could provide additional solutions or alternatives.

2. Methodology

The project will focus on three main environments: cloud environments, data centers, and local networks. This section will highlight the common vulnerabilities faced by each environment and the main security requirements for each to ensure high performance and security effectiveness. This section will review companies currently manufacturing firewall devices and their role in securing these different environments.

3. Implementation and Results

Firewalls (NGFW) will be implemented across the three environments, with customized configurations and programming tailored to the specific needs of each. Performance tests will then be conducted on the firewalls to assess the effectiveness of these customizations and evaluate their efficiency in handling threats and achieving optimal performance.

4. Recommendations and Conclusions

This section outlines key recommendations, conclusions, and future directions for enhancing the customization and performance of Next-Generation Firewalls (NGFWs). It proposes suggestions for further studies to address evolving threats, including AI-driven attacks and the challenges of complex environments like IoT and Industrial Control Systems.

CHAPTER TWO

LITERATURE REVIEW

2.1. Introduction

In this chapter, the project reviews the fundamental concepts of advanced firewalls and discuss their evolution from the first generation to modern firewalls, focusing on advanced features such deep packet inspection, application awareness, and encrypted data decryption. This project also examines the different types of firewalls and their roles in enhancing integrated defense strategies [4].

In this context, four previous studies on the same topic will be utilized. These studies highlight the advantages of modern firewalls, best practices, and the challenges organizations face in building a secure network architecture based on advanced firewall technologies.

2.2. Key Features of Palo Alto Firewall

The firewall's security relies on a set of advanced technologies that work in perfect harmony. **App-ID** enables precise application identification through protocol analysis, decryption, and application signatures. Meanwhile, **Content-ID** scans content to detect sensitive data, such as credit card numbers and security vulnerabilities, protecting users against viruses and spyware. Additionally, **User-ID** maps users to IP addresses, enabling the enforcement of security policies based on user roles and access levels.

In Figure (2.1), Palo Alto Firewall offers an innovative and comprehensive solution for network security, thanks to its unique ability to identify and deeply inspect SSL-encrypted traffic and applications. This capability provides a high level of control, allowing specific application functions to be managed without entirely blocking them, ensuring seamless workflow while maintaining security policies [18].

One of Palo Alto's most remarkable innovations is its **Single Pass Parallel Processing (SP3) Architecture**. This design ensures that packets are processed only once across all layers of protection, enabling simultaneous execution of application identification, security checks, and networking operations. This approach minimizes latency and maximizes performance, ensuring all operations are carried out efficiently without reprocessing the same packet.

The system’s advanced architecture enhances operational efficiency by separating the control plane from the data plane. The control plane handles configurations, reporting, and logs without interfering with data traffic, while the data plane focuses on forwarding traffic and enforcing security policies. This separation allows for seamless system updates without disrupting ongoing operations, ensuring business continuity.

Furthermore, Palo Alto leverages cloud computing capabilities to deliver proactive protection. If a new threat is identified within one subscriber’s network, all connected networks are automatically updated in real-time, providing robust defense against known and unknown threats. The use of multiple processors and parallel processing further ensures high performance and minimal delay in handling traffic.

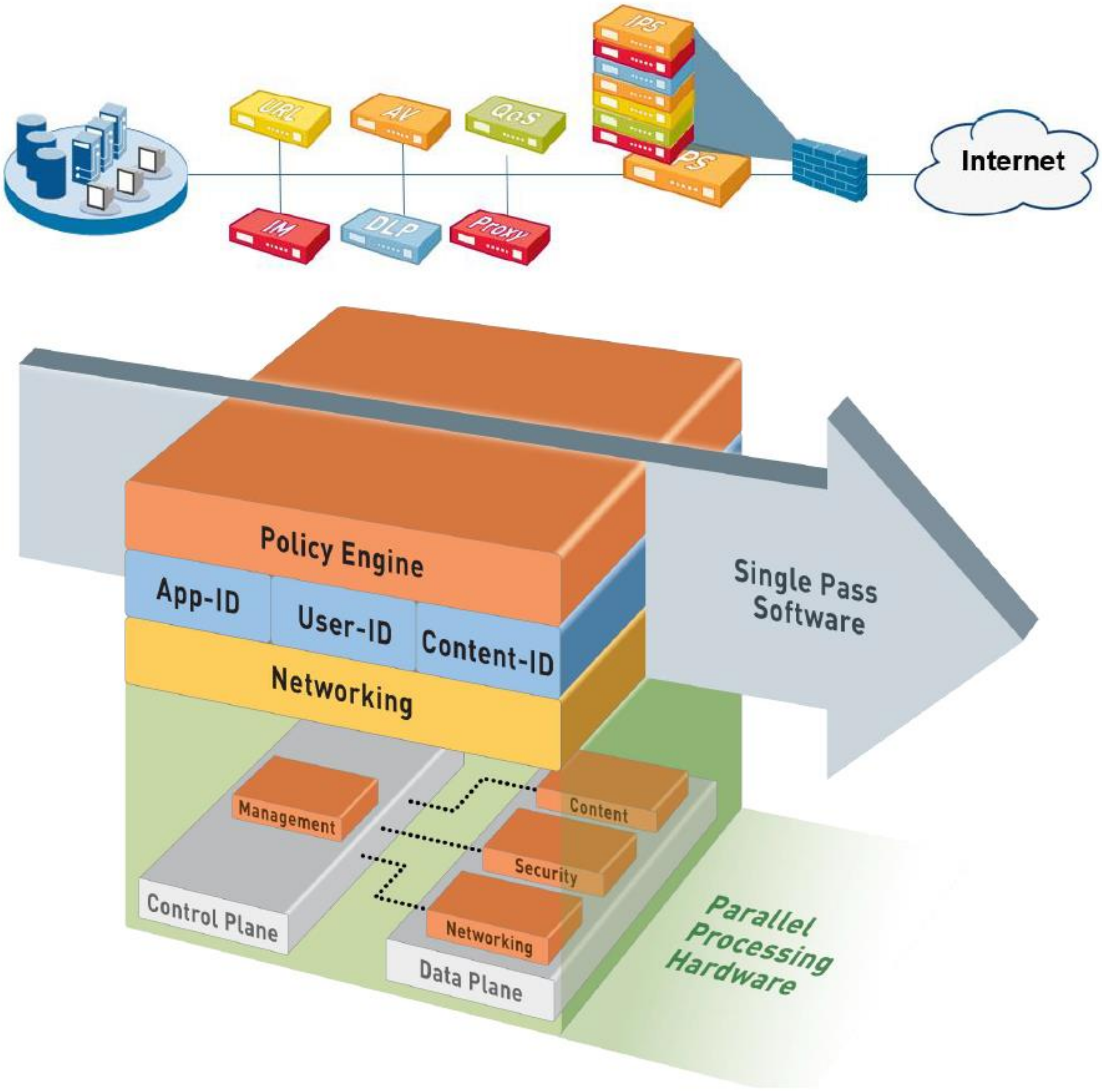


Figure. 2.1. Key Features form

2.3. NGFWs and Leading Companies in Manufacturing

A Next-Generation Firewall (NGFW) is an advanced security solution that builds on traditional packet filtering by integrating features like intrusion prevention, deep packet inspection (DPI), application control, and threat intelligence. It offers enhanced visibility into application traffic, enabling real-time threat detection and comprehensive policy enforcement to address modern cybersecurity challenges [1]. The firewall industry has evolved significantly since the 1980s, with pioneers like Cisco, Check Point, and Palo Alto Networks driving advancements from basic packet filters to sophisticated NGFWs, incorporating tools such as IDS/IPS, VPN concentrators, and network monitoring systems.

- Today, the leading companies in NGFW manufacturing are:

- **Cisco Systems:** Renowned for its routers, switches, and comprehensive network security solutions.
- **Palo Alto Networks:** Specializes in NGFWs, cloud security, and endpoint protection, with a strong focus on machine-learning-driven defense.
- **Fortinet**: Provides NGFWs, secure SD-WAN, and endpoint security, emphasizing integrated, high-performance security solutions.
- **Check Point**: Known for NGFWs, threat prevention, and unified security management solutions.

2.4. Theoretical background about NGFW

In the early days of technology, the absence of digital devices meant there was little need for information protection. However, as networks expanded, cyber threats increased, leading to the development of firewalls. Starting in the 1980s, firewalls evolved from simple barriers to advanced Next-Generation Firewalls (NGFWs). “Charles Backman played a key role in early intrusion detection and prevention, and his work gained traction when Cisco supported his efforts” [3]. Today, companies like Palo Alto Networks continue to innovate with features like machine learning. The development of firewalls can be traced through four key stages.

2.4.1. First Generation: Packet Filtering Firewalls

In the late 1990s, the first-generation packet-filtering firewalls introduced a shift in network security by filtering packets based on header information like IP addresses, protocols, and ports [4], as shown in Figure (2.2). However, these firewalls were stateless, analyzing [3]. each packet in isolation, which made them vulnerable to spoofing and session hijacking. Their static rule sets couldn't adapt to new threats, highlighting the need for more advanced technologies. This led to the development of the next generation of firewalls, incorporating features like stateful inspection for enhanced security.

2.4.2. Second Generation: Stateful Firewalls

In the early 2000s, stateful firewalls emerged as the second generation of firewall technology, operating at the transport layer and tracking active connections as shown in Figure (2.2) Unlike basic packet filters, they monitored entire sessions through a state table, improving detection of unauthorized access and attacks. However, stateful firewalls couldn't inspect packet content, leaving them vulnerable to advanced threats. This limitation drove the development of application firewalls and Unified Threat Management (UTM) systems, which integrated multiple security functions for better protection [4].

2.4.3. Third Generation: Next-Generation Firewalls

Introduced by Palo Alto Networks in 2008, Next-Generation Firewalls (NGFWs) revolutionized network security by operating across all OSI layers as seen in Figure (2.2) and providing advanced features like Deep Packet Inspection (DPI), application awareness, and integrated Intrusion Prevention Systems (IPS) [5]. They could detect applications regardless of port, inspect encrypted traffic, and block malicious content, addressing concerns about data leaks and breaches. However, their advanced capabilities added complexity in deployment and management, requiring precise configurations and adjustments to minimize performance impacts like latency. NGFWs brought network security in line with modern, evolving internet traffic and threats [1, 4].

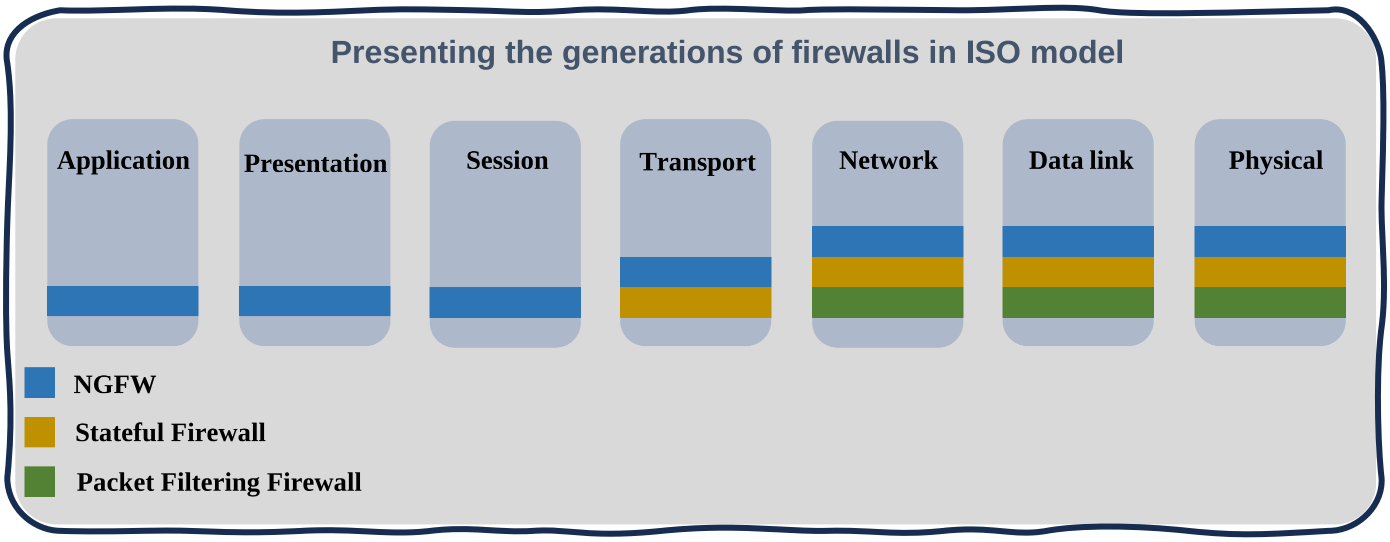


Figure. 2.2. Firewalls in ISO model

2.4.4. Fourth Generation: Machine Learning-Powered NGFWs

In 2020, Palo Alto Networks introduced the first ML-powered next-generation firewall (NGFW), offering proactive, real-time zero-day protection. This firewall uses machine learning to analyze network traffic patterns, identifying anomalies that may indicate new cyberattacks, without relying on known threat signatures. With advanced device visibility and behavioral anomaly detection, ML-powered NGFWs excel in securing IoT devices by dynamically adapting security policies based on continuous traffic analysis. They also simplify security management by recommending policy updates, ensuring rapid response to emerging threats and reducing administrative effort, allowing organizations to maintain a strong, adaptive security posture. [8]

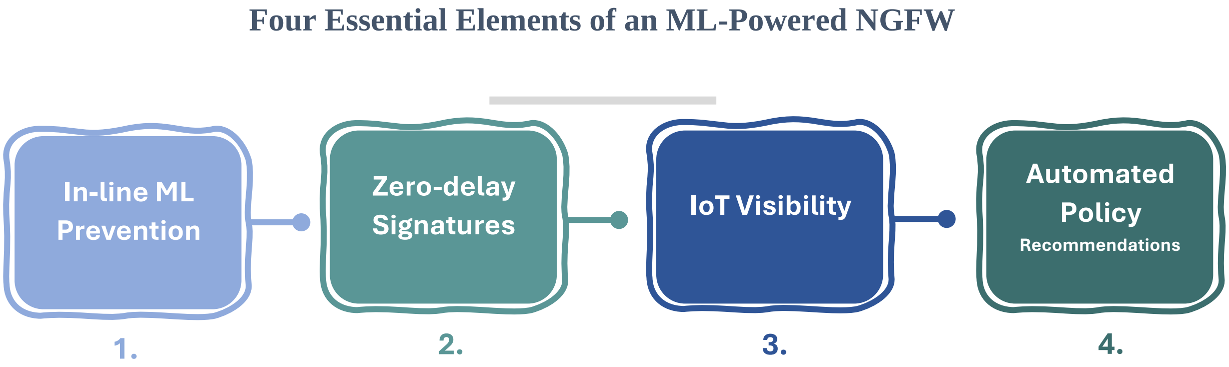


Figure. 2.2. Essential Elements of ML-

2.5. Types of Next-Generation Firewalls (NGFWs)

The project explores various types of Next-Generation Firewalls (NGFWs) that cater to a wide range of organizational needs and security requirements. NGFWs can be categorized based on their deployment methods, such as hardware-based, software-based, and cloud-based solutions. Each type offers distinct features and capabilities, enabling organizations to select the most suitable option for their specific IT environments. By examining the advantages and limitations of each type, the project aims to provide a comprehensive understanding of how different NGFWs can effectively protect against modern cyber threats while ensuring optimal performance. There are several types of Next-Generation Firewalls (NGFWs) [8]. each suited to specific security needs:

- **Software-Based NGFW:** Installed like any application, without specialized hardware. They integrate easily with cybersecurity tools like intrusion prevention systems and VPNs, providing detailed network control and visibility.
- **Hardware-Based NGFW:** Physical devices that monitor all network traffic without adding latency. Positioned outside the internal network, they offer comprehensive protection.
- **Cloud-Based NGFW:** Hosted by cloud providers as a subscription service, ideal for organizations needing scalable security without managing hardware.
- **Unified Threat Management (UTM) NGFW:** Combines multiple security features into one device, making it a simple all-in-one solution for small to medium-sized businesses.

2.6. Last studies

This section within this project reviews recent projects and findings related to Next-Generation Firewalls (NGFWs) and their effectiveness in various IT environments. By examining contemporary studies, this project highlights the advancements in NGFW technologies, illustrating how they address emerging cyber threats and enhance security protocols. These studies provide valuable insights into best practices, challenges, and innovative approaches that can inform the customization and deployment of NGFWs. Ultimately, this analysis aims to contribute to the broader understanding of NGFW applications and their role in fortifying network defenses.

2.6.1. Title: “Analysis and Evaluation of Network and Application Security Based on Next Generation Firewall” [10]

This study aims to enhance network security at the Atomic Energy Project Establishment (AERE) in Savar, part of the Bangladesh Atomic Energy Commission (BAEC), by utilizing a Cisco-based Next-Generation Firewall (NGFW). The AERE network, which integrates both wired and wireless systems, requires effective traffic management and protection from cyber threats.

The NGFW improves security through various features. It uses network segmentation via VLANs to streamline traffic monitoring and control, while integrated IDS/IPS systems detect and block threats through rule-based mechanisms. Content and URL filtering restrict access to harmful websites, and sandboxing identifies and blocks malicious files during uploads or downloads. The firewall also decrypts traffic for inspection and includes Web Application Firewall (WAF) capabilities to strengthen security. Wireless security is enhanced by a Wireless Intrusion Detection and Prevention System (WIDPS), protecting against unauthorized access. Additionally, port forwarding is used to secure vulnerable ports by mapping public IP addresses to private ones, improving overall network resilience. The analysis of the network security measures revealed several key results. First, network traffic monitoring effectively tracks IP usage to manage bandwidth and identify high-traffic applications. Intrusion prevention measures are documented and used to block intrusion attempts, with statistical insights into the types of attacks. File and URL filtering processes ensure safe internet access by blocking malware. Finally, proactive malware detection and mitigation efforts, including port scanning, help safeguard the network from potential threats.

2.6.2. Title: “Enterprise Network: Security Enhancement and Policy Management Using Next-Generation Firewall (NGFW)” [11]

The study addresses the challenges enterprises face in balancing security needs with the need for business information sharing, emphasizing how traditional security controls often fail to mitigate emerging cyber threats. It highlights the necessity for a more adaptive and robust security system and proposes a security model utilizing a Next-Generation Firewall (NGFW) with tailored policies to enhance network protection. The project explores various cybersecurity threats, including IP spoofing, insider intrusion, DDoS attacks, and masquerade attacks, and their impact on organizational networks. It stresses the importance of securing both trusted and untrusted networks (LAN/WAN) and suggests deploying NGFW policies for better threat management. The study uses Fortinet FortiGate firewall models to demonstrate the effectiveness of these policies in a simulated environment, employing GNS3 for network topology simulation to address identified security gaps.

The proposed security system leverages FortiGate Firewalls with advanced features such as IPsec VPN, port forwarding, and internet traffic filtering to enhance security. Policy integration focuses on direct internet traffic management, secure port forwarding, and IPsec VPN configuration to strengthen both internal and external network security. Additionally, monitoring tools such as WinMTR and free bandwidth monitoring software are used to evaluate network performance, bandwidth utilization, and security improvements.

The evaluation of the system shows that the NGFW setup effectively mitigates vulnerabilities like DoS attacks and unauthorized port scanning, improves bandwidth utilization, and increases CPU efficiency. The model also proves to be cost-effective compared to traditional ASA firewalls, making it a viable solution for enterprises looking to enhance their cybersecurity posture.

2.6.3. **Title: “Synergizing Next-Generation Firewalls and Defense-in-Depth Strategies in a Dynamic Cybersecurity Landscape”** [12]

This study explores the integration of Next-Generation Firewalls (NGFWs) into Defense-in-Depth (DiD) cybersecurity strategies, evaluating their effectiveness in defending against modern cyber threats. NGFWs provide advanced capabilities beyond traditional firewalls, such as SSL/TLS decryption, application awareness, and deep packet inspection (DPI), all of which enhance the DiD approach by strengthening detection, prevention, and response to cyber risks. The project uses a qualitative simulation within a virtual network environment, focusing on Palo Alto’s NGFW (PAN-OS 10.1). It demonstrates the firewall's role in segmenting security zones and supporting SSL/TLS decryption, application awareness, and DPI. Through various case studies, the NGFW is tested in configurations that include blocking specific applications like Facebook and YouTube, decrypting SSL/TLS traffic, and implementing file-blocking policies to prevent data loss.

Key findings from the study show that the NGFW’s SSL Forward Proxy effectively inspects encrypted traffic, selectively decrypting it based on URL categories to maintain a balance between security and privacy. It emphasizes the need for customized decryption policies to ensure user privacy and compliance. The study also highlights how the NGFW’s App-ID technology allows for application awareness, enabling the firewall to block specific applications without relying on IP or port configurations, thereby improving policy enforcement. Furthermore, through DPI, the NGFW inspects packet content for data loss prevention and malware protection, with testing showing its success in blocking unauthorized file downloads, demonstrating DPI’s value in enforcing data governance and mitigating risks.

However, the study also identifies challenges, including the issue of false positives and alert fatigue, where the high volume of alerts from NGFWs and DiD layers may overwhelm security teams, potentially causing real threats to be missed. It also notes the cost considerations of NGFW deployment, which can be expensive due to licensing, training, and support, posing a challenge for smaller organizations. A cost-benefit analysis is recommended to ensure that security investments are balanced with budget constraints.

2.6.4. Title: “Toward a Modern Secure Network Based on Next-Generation Firewalls: Recommendations and Best Practices” [13]

This study addresses gaps in existing project by focusing on proprietary industrial solutions, specifically Fortinet’s FortiGate and FortiWeb, which are widely used in corporate environments. Unlike much of the existing literature that either relies on open-source NGFWs or lacks comprehensive best practices, this study proposes a secure architecture tailored for multi-site campuses. The study's key objectives include proposing a secure architecture suited for multi-site environments, providing configuration recommendations for NGFW services, and conducting penetration testing to validate the architecture's security effectiveness.

The network security architecture has several components that create a layered defense. The Frontend NGFW acts as the primary defense, filtering traffic between the internet and the internal network. It includes firewall policies that control resource access by segmenting traffic based on user groups, such as students and staff, and High Availability (HA) configurations to ensure continuity during hardware failures. VPN settings are also incorporated to secure connections across campus sites. The backend NGFW provides additional internal segmentation, manages traffic between network zones, and offers features like application control and logs for detailed traffic analysis.

An Intrusion Prevention System (IPS) monitors network traffic, detecting known and novel threats through both signature-based and behavioral analysis. A Load Balancer is used to distribute incoming traffic across multiple servers to ensure optimal application performance. A Web Application Firewall (WAF) further protects web applications by detecting and blocking malicious traffic, providing an additional layer of defense against web-based attacks. These components work together to form a multi-layered security framework that enhances network defense and operational efficiency. The architecture was validated through a testbed setup that included dual front-end firewalls in an Active-Active HA configuration, an IPS, a load balancer, LDAP and log servers, a backend firewall, and a Web Application Firewall (WAF). The architecture was assessed using the Firewall Inspection Test script, with results showing that malware threats were effectively blocked across the entire setup, confirming the robustness of the proposed security framework.

2.7. Environment Risks

The identification and analysis of environmental risks are essential components of this study, focusing on the various threats faced by different IT environments. Each environment presents unique vulnerabilities that can be exploited by cyber attackers, ranging from insider threats to external malware. This study aims to assess these risks comprehensively, allowing for the development of tailored security measures that effectively mitigate potential dangers. By understanding the specific risks associated with each environment, organizations can enhance their security strategies and protect critical data and resources.

And the project will focus on the following environments:

2.7.1. Cloud Environment Risks

1. **Attacks on Cloud-Based IT Platforms:** Emerging risks like model data poisoning, and unauthorized access necessitate strong access control and data encryption.
2. **Software Supply Chain Risks:** As organizations increasingly rely on third-party services, they become vulnerable to security threats originating from these external vendors. These risks include inadequate security controls, or malicious tampering in the supply chain.
3. **Cloud-Native Malware:** Targeted malware for cloud platforms requires regular updates, active detection systems, controlled access, and data backups for effective defense [7].

2.7.2. Data Center Environment Risks

1. **Insider Threats:** Managed through stringent access controls and activity monitoring to mitigate risks from privileged misuse.
2. **Ransomware Attacks:** Countered with disaster recovery plans, dynamic firewall strategies, and user awareness training.
3. **Data Center Theft:** Physical protection with surveillance, access restrictions, and onsite personnel.
4. **Supply Chain Attacks:** Mitigated with thorough third-party vetting and data encryption.
5. **Network Intrusion:** Contained using intrusion detection and segmentation.
6. **Physical Security Tampering:** Defended with redundant, independent security systems.
7. **Continuous Training:** Essential for adapting to new threat tactics [7].

2.7.3. LAN Environment Risks

1. **Malware Infiltration:** Malicious software, such as viruses, worms, and ransomware, can enter the network through infected websites, email attachments, or compromised devices, potentially leading to data corruption or unauthorized access.

2. **Phishing Attacks**: Users may be targeted by phishing schemes designed to steal credentials, financial information, or sensitive data by masquerading as legitimate entities or trusted sources.

3. **Insider Threats**: Users within the organization, either intentionally or accidentally, may misuse their access privileges, leading to unauthorized data exposure, policy violations, or other harmful actions.

4. **Unauthorized Application Access**: Unapproved applications or risky software can operate on the network, introducing vulnerabilities and exposing the LAN to data leaks or unmonitored activity.

5. **Data Exfiltration**: Sensitive data, such as personal information or intellectual property, is at risk of being transferred out of the network by attackers or insiders, leading to data breaches and loss of confidential information.

6. **DNS-Based Attacks**: Malicious actors may exploit the Domain Name System (DNS) to direct users to fraudulent websites or to establish command-and-control communication channels for malware [7].

CHAPTER THREE

METHODOLOGY

3.1. Introduction

This Chapter focuses on the experimental approach used to test and configure firewalls in three distinct environments: cloud, local network, and data center environments. These environments have unique security needs, and the project aims to demonstrate the optimal firewall configurations for each to ensure robust protection without overburdening the network or misusing resources. The simulation of these environments is conducted using the GNS3 platform, which offers high-fidelity simulations and integrates effectively with VMware to enhance load management and performance with virtual devices. This chapter provides a detailed overview of the network setups, including their schematics, and discusses the customization of firewall settings tailored to the specific requirements of each environment.

3.2. Justification for Choosing GNS3

The GNS3 simulation environment was selected for this project due to its realism and widespread adoption in academic and professional settings. GNS3 provides highly accurate virtual network and device simulations, ensuring results that closely mimic real-world scenarios and are practically applicable. It supports a wide range of network systems and firewalls, including Palo Alto NGFW. GNS3 is highly flexible, enabling the design of multi-layered networks with capabilities to perform advanced operations like traffic decryption, threat prevention, and policy customization. Additionally, GNS3 reduces the costs associated with physical hardware and offers a robust community of support, facilitating problem-solving and efficient project execution, making it an ideal choice for achieving the objectives of this project.

3.3. Selecting the Optimal Next-Generation Firewall (NGFW)

Choosing the right Next-Generation Firewalls (NGFWs) is a critical decision in enhancing the security posture of modern IT environments. This project emphasizes the importance of selecting NGFWs based on specific organizational needs, such as data throughput requirements, deployment contexts, and unique security challenges. The selection process is designed to ensure that organizations can effectively address current and emerging threats in their respective environments [28].

Palo Alto Networks’ NGFWs are recognized for their advanced features, making them a top choice for organizations seeking comprehensive and reliable security solutions:

- **Advanced Threat Detection:** Palo Alto Firewalls utilize behavioral analysis and machine learning to detect advanced threats with speed and precision, ensuring protection against unknown and emerging cyber risks.
- **Centralized Management & Flexibility:** The Panorama management tool provides centralized visibility and control, allowing security teams to monitor and respond to threats effectively across diverse network environments.
- **App-ID Technology:** Capable of identifying and managing over 3,000 applications, ensuring precise traffic inspection, application control, and encrypted traffic analysis (SSL/TLS decryption) regardless of port or protocol.
- **Different collection categories by argument:** The PA-Series models (PA-3220, PA-5250, PA-5280) offer substantial processing power, and the same for the other categories.
- **Comprehensive Security Framework:** By combining AI-driven threat detection, centralized management, and advanced application control**.**

3.4. Palo Alto FW Selection Criteria and Deployment Approach

Palo Alto Firewall (PAFW) is determined by several factors, including the organization’s size, data throughput requirements, intended applications, and deployment environment. Modern ML-powered NGFWs provide industry-leading performance and security across a range of environments, from small branch offices to expansive data centers.

For example, smaller environments such as local networks can utilize entry-level models like the PA-400R, PA-400, or PA-1400 Series, while mid-to-large data centers benefit from more robust models, such as the PA-5400 or PA-3400 Series. For cloud deployments, mid-to-high-end options like the PA-5450, PA-7000, and PA-7500 Series offer optimal protection [10]. This project will use the PAN VM-Series Firewall Version 10.1.0 to simulate NGFW performance, providing a realistic representation of current advanced firewall capabilities.

3.5. Solution Mechanisms

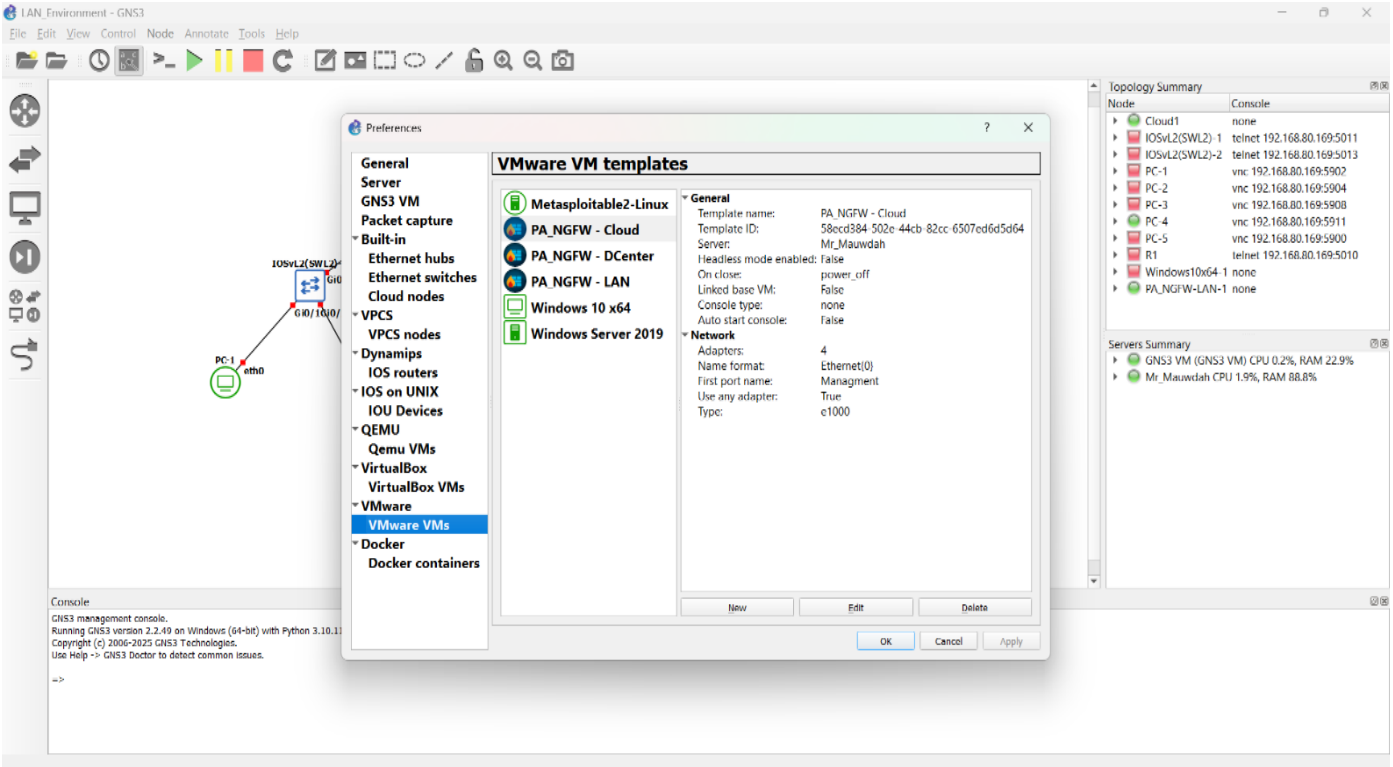
The project employs advanced tools and techniques to strengthen security measures and improve system performance. This approach includes assessing specific security needs and implementing customized configurations. The primary objective is to develop a resilient framework capable of tackling current cybersecurity challenges while adapting to emerging digital threats. Table (3.1) shows the tools used for environment simulation, explaining their selection criteria and intended purpose in customizing the NGFW.

Table 3.1. Solution Mechanisms

Tools	**Purpose**	**Advantages**
GNS3	Simulate network environments for NGFW deployment testing	GNS3 offers flexibility in designing and testing network configurations, with real-time feedback that enables thorough evaluation of NGFW implementations
VMware	Host GNS3 virtual machines to create stable, virtualized network environments	VMware provides a reliable and scalable platform for running complex network simulations, ensuring optimal performance and effective resource management
Palo-alto: PAN VM-Series Firewall Version 10.1.0	Essential for enhancing network security through advanced threat protection and application control	It uses Machine Learning and provides features that are crucial for enabling organizations to implement robust security measures and adapt effectively to evolving cyber threats.
Network Devices	Facilitate communication between various network components in the simulated environment	Switches and routers are crucial for creating realistic network topologies, ensuring accurate simulation of real-world networking conditions

3.6. Initial preparation for the implementation of network plans

This section outlines the foundational steps involved in setting up the network simulation environment using GNS3 and VMware. It details the configuration of virtual devices, network interfaces, and security components to ensure seamless integration and effective network management. The figures provided illustrate key configuration interfaces and settings that are essential for implementing the network plans, emphasizing the customization of virtual machines and the deployment of a Next-Generation Firewall (NGFW) for enhanced network protection.



General
Template name: PA_NGFW - Cloud
Template ID: 58ecd384-502e-44cb-82cc-6507ed6d5d64
Server: Mr_Mauwdah
Headless mode enabled: False
On close: power_off
Linked base VM: False
Console type: none
Auto start console: False

Network
Adapters: 4
Name format: Ethernet{0}
First port name: Managment
Use any adapter: True
Type: e1000

Node	Console
Cloud1	none
IOSvL2(SWL2)-1	telnet 192.168.80.169:5011
IOSvL2(SWL2)-2	telnet 192.168.80.169:5013
PC-1	vnc 192.168.80.169:5902
PC-2	vnc 192.168.80.169:5904
PC-3	vnc 192.168.80.169:5908
PC-4	vnc 192.168.80.169:5911
PC-5	vnc 192.168.80.169:5900
R1	telnet 192.168.80.169:5010
Windows10x64-1	none
PA_NGFW-LAN-1	none

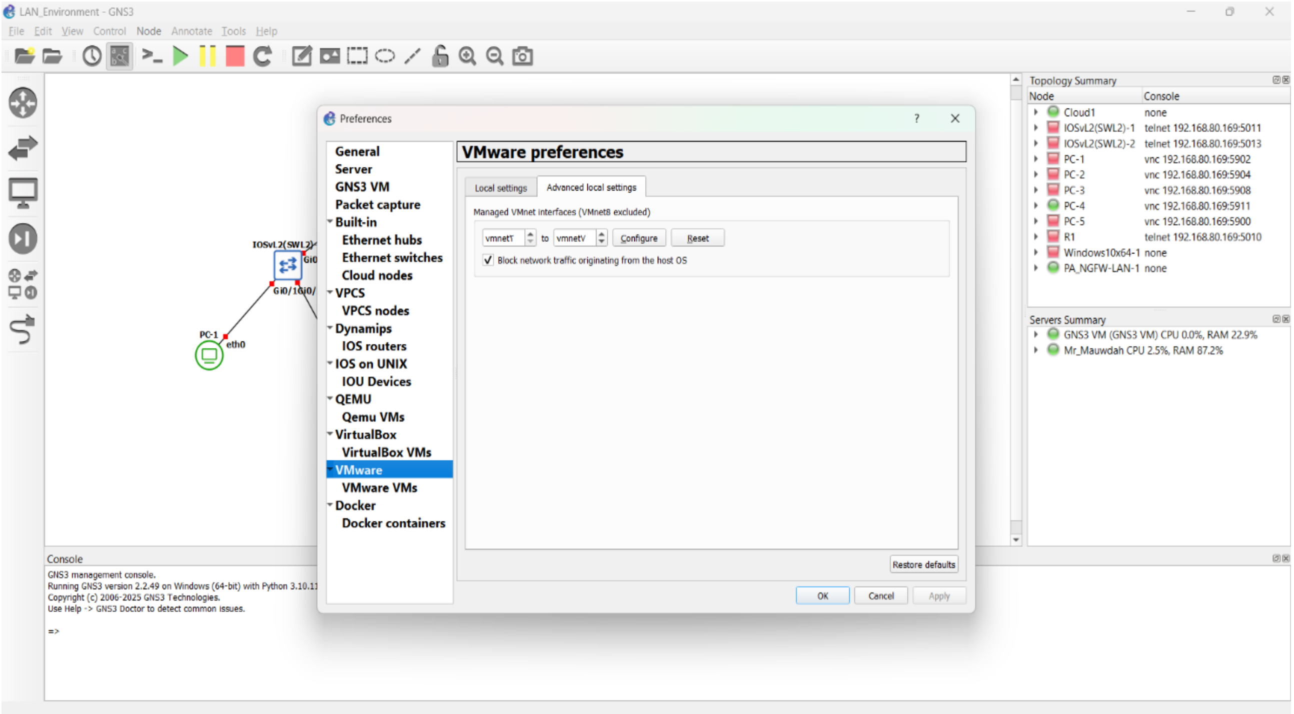
GNS3 VM (GNS3 VM) CPU 0.2%, RAM 22.9%
Mr_Mauwdah CPU 1.9%, RAM 88.8%

```
GNS3 management console.
Running GNS3 version 2.2.49 on Windows (64-bit) with Python 3.10.11
Copyright (c) 2006-2025 GNS3 Technologies.
Use Help -> GNS3 Doctor to detect common issues.

=>
```

Figure. 3.1. Add Virtual Machines

- Figure (3.1) illustrates the GNS3 settings interface for adding device emulators via VMware. It features a "VMware VMs" list for configuring virtual machines, displaying details such as the model’s name and system type. These settings help to add new VMs that exist in VMware and customize them for seamless integration into the GNS3 environment, enhancing the simulation experience.

-



VMware preferences

Managed VMnet interfaces (VMnet8 excluded)

vmnet١ to vmnet٧

☑ Block network traffic originating from the host OS

Topology Summary

Node	Console
Cloud1	none
IOSvL2(SWL2)-1	telnet 192.168.80.169:5011
IOSvL2(SWL2)-2	telnet 192.168.80.169:5013
PC-1	vnc 192.168.80.169:5902
PC-2	vnc 192.168.80.169:5904
PC-3	vnc 192.168.80.169:5908
PC-4	vnc 192.168.80.169:5911
PC-5	vnc 192.168.80.169:5900
R1	telnet 192.168.80.169:5010
Windows10x64-1	none
PA_NGFW-LAN-1	none

Servers Summary

GNS3 VM (GNS3 VM) CPU 0.0%, RAM 22.9%

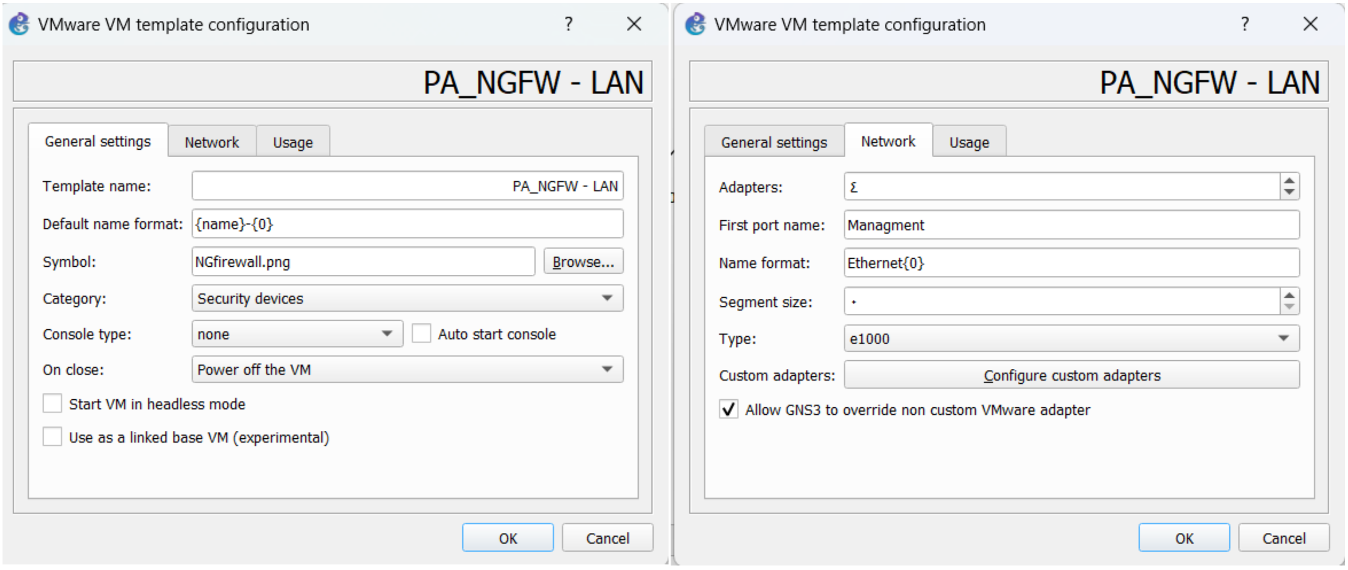
Mr_Mauwdah CPU 2.5%, RAM 87.2%

Console

```
GNS3 management console.
Running GNS3 version 2.2.49 on Windows (64-bit) with Python 3.10.11
Copyright (c) 2006-2025 GNS3 Technologies.
Use Help -> GNS3 Doctor to detect common issues.

=>
```

Figure. 3.2. Add Interfaces

- Figure (3.2) illustrates the VMware settings interfaces designed for adding or managing Interface for virtual machines. The menu includes the "VMware VMs" option, allowing users to customize network adaptors related to ports. These configurations help to manage and ensure effective communication between virtual machines in VMware and within the GNS3 internal network.


VMware VM template configuration
?
General settings
Network
Usage
Browse...
OK
Cancel
VMware VM template configuration
?
General settings
Network
Usage
Configure custom adapters
OK
Cancel

PA_NGFW - LAN

Template name: PA_NGFW - LAN

Default name format: {name}-{0}

Symbol: NGfirewall.png

Category: Security devices

Console type: none ☐ Auto start console

On close: Power off the VM

☐ Start VM in headless mode

☐ Use as a linked base VM (experimental)

PA_NGFW - LAN

Adapters: ٤

First port name: Managment

Name format: Ethernet{0}

Segment size: ٠

Type: e1000

Custom adapters: Configure custom adapters

☑ Allow GNS3 to override non custom VMware adapter

Figure. 3.3. Edit Virtual Machines

- Figure (3.3) In the virtual machine settings for "PA_NGFW - LAN," the device has been categorized under Security Devices to designate it as a Next-Generation Firewall (NGFW) specialized in network protection. Additionally, four network adapters have been configured to meet diverse network requirements. The first adapter is dedicated to the management, ensuring full administrative control over the device, while the other adapters are allocated for the Local Area Network (LAN), Wide Area Network (WAN), and Demilitarized Zone (DMZ). The e1000 adapter type was selected for its compatibility and ease of integration with various systems. Furthermore, the option to allow GNS3 to override non-custom VMware adapter settings has been enabled to provide flexibility in configuration and seamless integration with virtual networking environments.

3.7. Environments customization

The customization of environments is a crucial aspect of this project, aimed at tailoring Next-Generation Firewall (NGFW) functionalities to meet the specific security needs of different IT settings, including cloud infrastructures, data centers, and local networks. By analyzing the unique risks and requirements of each environment, the project develops targeted configurations that enhance security without compromising performance. This approach not only improves the effectiveness of the security measures implemented but also ensures a more efficient use of resources, ultimately leading to a robust and resilient network infrastructure. All types explain the most important firewall customizations to protect against the potential attacks [22].

3.7.1. Cloud Next Generation firewall customization needs

To ensure efficient operation and implement critical security measures using the Palo Alto NGFW, the following functions are recommended:

- **Access Control and User Identification (User-ID):** Enforces strict access policies to prevent unauthorized entry and manage permissions, particularly to mitigate risks like unauthorized access and model data poisoning in cloud IT platforms.

- **Data Encryption (SSL Decryption):** Decrypts and inspects encrypted traffic, ensuring that sensitive data is protected while still allowing inspection of potentially harmful content, essential for both access control and supply chain security.
- **Advanced URL Filtering:** Monitors and restricts access to harmful or unapproved URLs, helping control exposure to phishing, malware, and malicious sites that could compromise cloud data or applications.
- **Centralized Monitoring and Logging (Strata Logging Service):** Provides centralized log storage and monitoring to facilitate continuous assessment and quick response to any suspicious activity, ensuring constant oversight in the cloud environment [12].

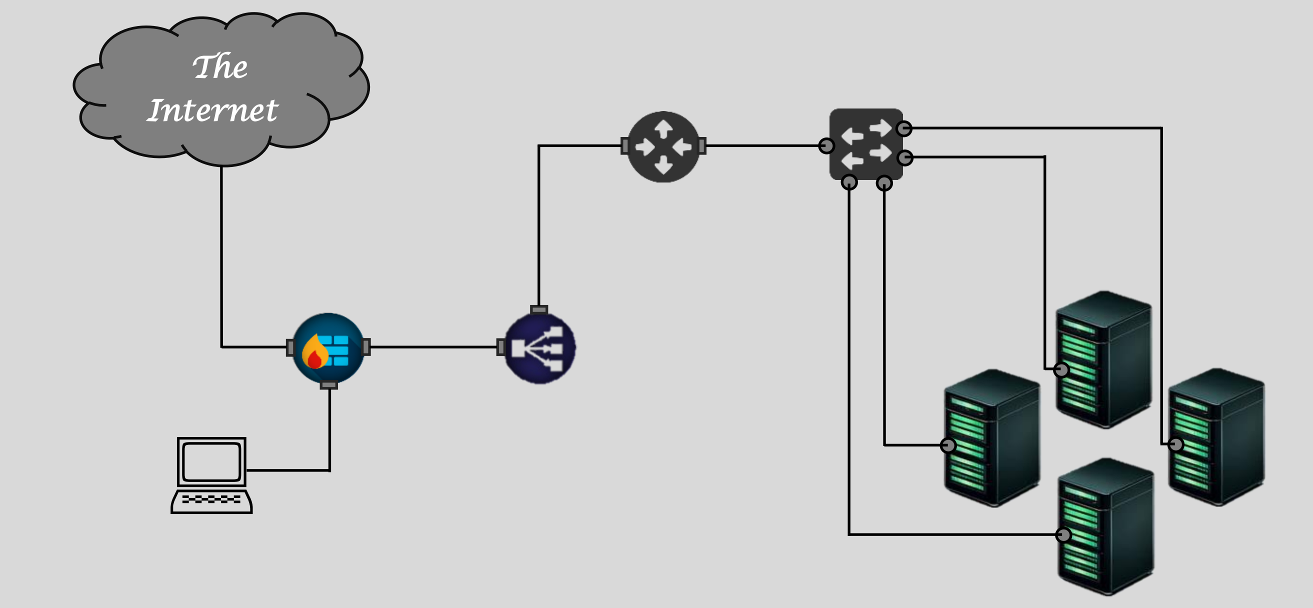


Figure. 3.4. Cloud Diagram

- In Figure (3.4), the firewall is positioned between the secure network (cloud) and the unsecured network (Internet). This placement enables it to inspect incoming data flow to the secure network and block any suspicious activity. Additionally, a load balancer is included to reduce excessive pressure on the servers, enhancing performance and improving response times. Is illustrated in the network diagram, which depicts a typical cloud environment and the customized firewall setup applied in the project.

3.7.2. Data Center Next Generation firewall customization needs

To ensure efficient operation and implement critical security measures using the Palo Alto NGFW, the following functions are recommended:

- **User Identification and Access Control:** Enforce strict access policies to manage insider threats, monitoring privileged access and tracking user activities to quickly identify unauthorized actions.
- **Threat Prevention:** Implement antivirus, anti-spyware, and vulnerability protection to prevent malware, particularly ransomware, includes integrating regular updates for real-time protection.
- **DNS Security and URL Filtering:** Apply DNS security and URL filtering to restrict malicious web access and block phishing sites, reducing the likelihood of ransomware delivery and unauthorized communication with malicious servers [15].
- **Segmentation and (App-ID):** Utilize traffic segmentation and deep packet inspection to isolate sensitive workloads and ensure that only authorized traffic flows through critical areas. This reduces exposure to potential intrusions and improves detection accuracy.
- **Physical Security Integration:** Coordinate firewall policies with physical security measures by integrating access controls and video surveillance data where possible. This adds a layer of security against physical security tampering and equipment theft [12].

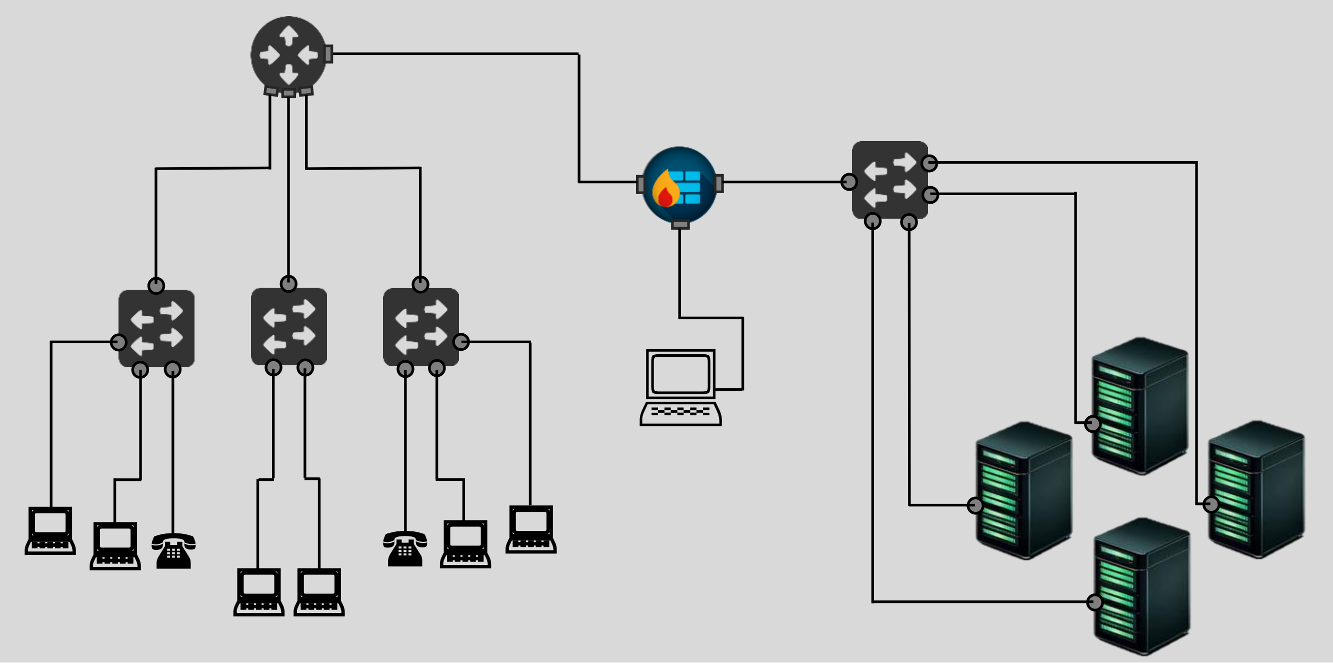


Figure. 3.5. Data Center Diagram

- The diagram in Figure (3.5), you can observe that the firewall is positioned between the secured network (Data Center) and the unsecured network (LAN). This placement allows it to inspect incoming stream data to the secure network and block any suspicious activity. The network diagram shows a data center environment with customized firewall configurations applied in the project.

3.7.3. LAN Next Generation firewall customization needs

To ensure efficient operation and implement critical security measures using the Palo Alto NGFW, the following functions are recommended:

- **URL Filtering:** Controls web access by blocking access to malicious or unapproved websites, reducing the risk of phishing attacks and preventing access to potentially harmful web content.
- **User Identification (User-ID):** Maps IP addresses to individual user identities, enabling policies that restrict access based on user roles and activity. This helps enforce strict access control within the LAN.
- **DNS Security:** Provides protection against DNS-based threats by identifying and blocking connections to malicious domains, preventing command-and-control attacks and limiting malware spread.
- **Application Control (App-ID):** Identifies and manages applications on the network, allowing or blocking application usage based on predefined security policies. This is critical in preventing unauthorized or risky applications from operating within the LAN [12].

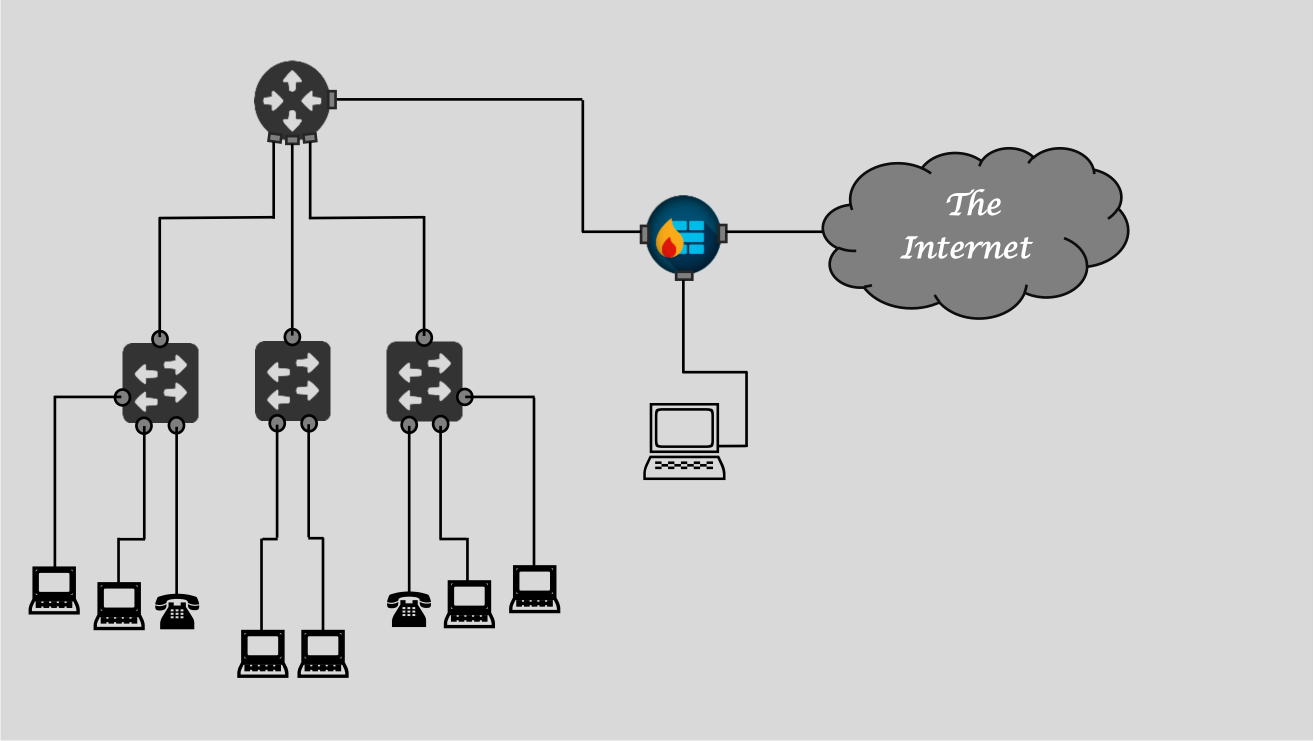


Figure. 3.6. LAN Diagram

- The diagram in Figure (3.6), you can observe that the firewall is positioned between the secure network (LAN) and the unsecure network (Internet). This placement allows it to inspect incoming stream data to the secure network and block any suspicious activity The network diagram depicts a typical LAN environment with these NGFW customizations implemented in this project.

Note: Note: All of the above diagrams illustrate realistic or near-realistic environments akin to those used in actual implementations, these diagrams were adapted after studying diagrams found in the following studies: [3,6,11,12]. However, the environments featured in this project will be presented through images in Chapter Four. These environments have been streamlined to convey the basic concepts while ensuring compatibility with the limited RAM capacity of the lab machine, which cannot support all of the devices mentioned.

3.8. Project Contributions

The project contributions of this project focus on developing tailored security solutions for various IT environments, including cloud, data centers, and local networks. By customizing Next-Generation Firewall (NGFW) functionalities, the project enhances performance and efficiency, enabling organizations to strengthen their cybersecurity posture. Additionally, it introduces a performance monitoring framework that facilitates continuous assessment and improvement, ensuring optimal resource management. Overall, the findings underscore the importance of balancing security and performance to create resilient and adaptive network infrastructures [17].

1. Developing tailored security solutions for each environment to meet their unique requirements (cloud, data centers, and local networks).
2. Improving performance and efficiency by customizing the firewall for each environment, reducing response time, and enhancing threat detection.
3. Creating a performance monitoring framework using specialized tools, enabling continuous assessment and improvement.
4. Enhancing security by increasing the effectiveness of threat detection through algorithm improvements and customized security rules [14].
5. Better resource management to ensure efficient use of bandwidth and processing load in each environment.
6. Providing a guideline for firewall implementation that helps engineers and network managers configure firewalls properly for each environment.
7. Balancing security and performance to offer high protection without significantly impacting network efficiency.
8. Enhancing scalability and adaptability to changing technologies to meet future needs.

CHAPTER FOUR

IMPLEMENTATION AND RESULTS

4.1. Introduction

In this chapter, we transition from theoretical frameworks and methodological planning to practical implementation, where concepts take shape in real-world execution. This section focuses on customizing the functionalities of Next-Generation Firewalls (NGFWs) according to the specific security requirements of the targeted environments: cloud, data centers, and local networks. It highlights the importance of translating security principles into practical solutions through the use of simulation technologies, such as GNS3 and VMware, to develop virtual environments that reflect the challenges faced by real-world systems.

The implementation in this chapter is not merely a technical validation but an experiment that demonstrates how a well-structured set of configurations and customizations can enhance network performance while minimizing security risks. The final results are presented through analytical diagrams and performance indicators, showcasing how security can be reinforced without compromising system efficiency. Additionally, this chapter underscores the value of collaboration between technology and human expertise in building dynamic and adaptive security systems capable of responding to future challenges.

4.2. Implementation

This section of the project focuses on implementing Next-Generation Firewall (NGFW) customizations across different environments, including cloud, data centers, and local networks. Using the GNS3 and VMware simulation platforms, firewall configurations are deployed and optimized to meet the specific security needs of each environment. The implementation aims to evaluate the efficiency of these customizations in enhancing security and performance while ensuring a balance between protection and network efficiency.

4.2.1. LAN Environment

The Local Area Network (LAN) environment is a fundamental component of modern network architecture, connecting a group of devices within a limited geographic area, such as offices or homes. LANs are characterized by high data transfer speeds, facilitating effective communication between devices and enhancing business productivity. In the context of our project, the focus is on how to customize Next-Generation Firewall (NGFW) settings to meet specific security needs within the local network environment, ensuring data protection and optimizing overall network performance [19].

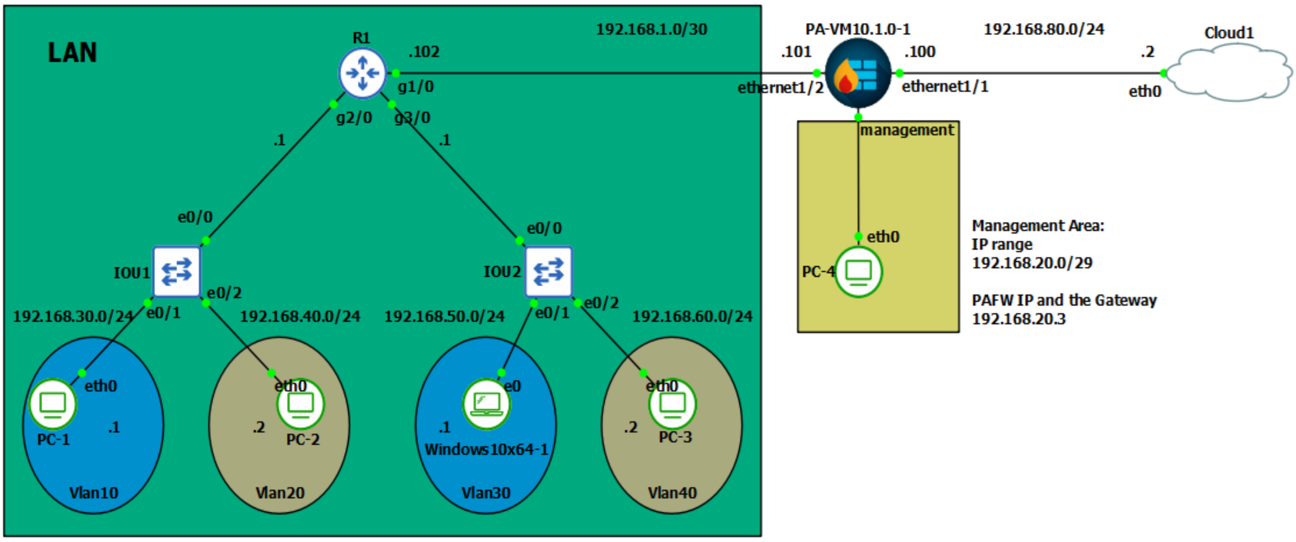


Figure. 4.1. LAN Executive diagram

- Figure (4.1) show the network topology created in GNS3, showcasing a Local Area Network (LAN) environment segmented into different zones. It includes various devices such as PCs, switches, a router, and a firewall (Palo Alto VM), with connections to a management network and WAN.

4.2.2. Key Components of the LAN Diagram

Designing the network architecture is essential for tailoring Next-Generation Firewalls (NGFWs) to achieve optimal security and operational efficiency. The network diagram in this project illustrates the key components of the network, highlighting devices, access points, and the segmentation of the network into distinct security zones.

As shown in Figure (4.1), multiple IP address ranges are utilized. The subsequent tables present these IP addresses along with their corresponding subnet masks and gateways, organized by zones:

1. **Management Zone:**

Table (4.1) Ip addresses for Management Zone

Device/Component	IP Address	Gateway	Subnet Mask
PC-4 (eth0)	192.168.20.5	192.168.20.2	255.255.255.248
Palo Alto (Mgmt. Port)	192.168.20.3	192.168.20.2	255.255.255.248

This zone is dedicated to network administration devices such as firewalls and management PCs. It provides centralized control over security policies, ensuring the network remains protected against unauthorized access. Static IPs are used in this zone for stability and precise security configurations.

2. **WAN Zone (Wide Area Network):**

Table (4.2) Ip addresses for WAN Zone

Device/Component	IP Address	Gateway	Subnet Mask
Cloud1 (Eth0)	192.168.80.2	192.168.80.1	255.255.255.0
Palo Alto FW (Eth1/1)	192.168.80.100	192.168.80.2	255.255.255.0

Acts as the gateway between the internal network and the internet, routing data through the firewall. The firewall filters traffic, blocks potential threats, and applies security measures like Network Address Translation (NAT) to hide internal devices from direct exposure.

3. **LAN Zone (Local Area Network):**

Table (4.3) Ip addresses for LAN Zone

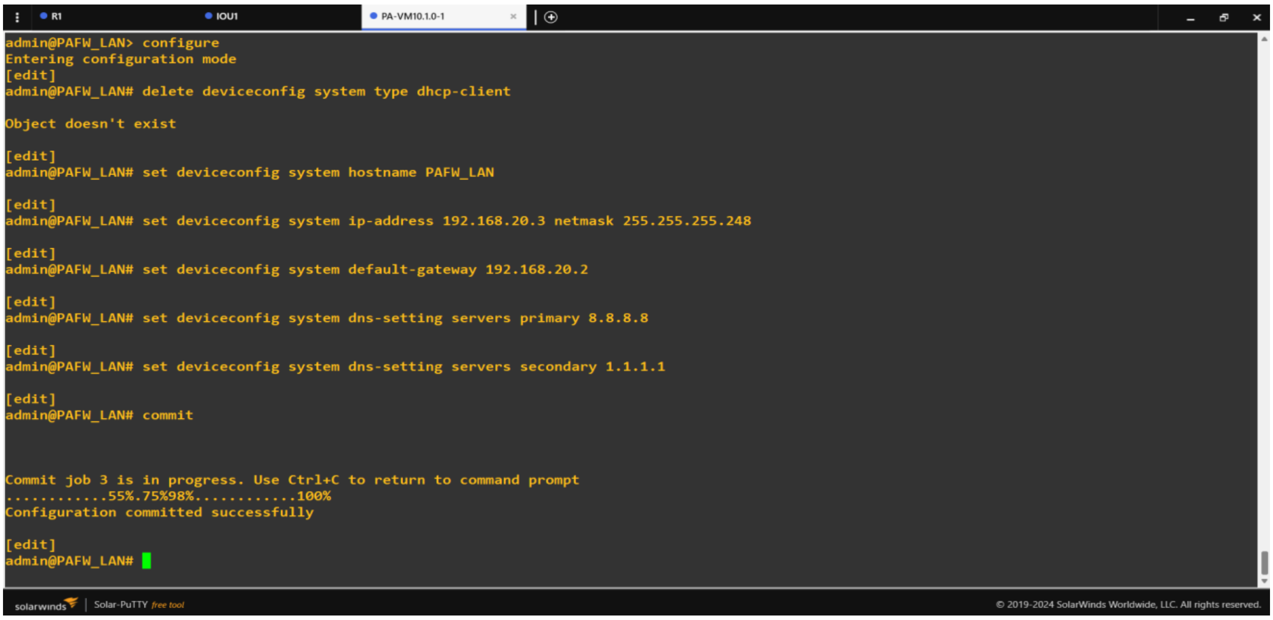
Device/Component	IP Address	Gateway	Subnet Mask
Router_R1 (g1/0) Router_R1 (g2/0.10) Router_R1 (g1/0.20)	192.168.1.102 192.168.30.1 192.168.40.1	______ ______ ______	255.255.255.252 255.255.255.0 255.255.255.0

Device/Component	IP Address	Gateway	Subnet Mask
Router_R1 (g3/0.40) Router_R1 (g3/0.40)	192.168.50.1 192.168.60.1	______ ______	255.255.255.0 255.255.255.0
Palo Alto FW (eth1/2)	192.168.1.101	______	255.255.255.252
PC-1 (VLAN10)	192.168.30.2	192.168.30.1	255.255.255.0
PC-2 (VLAN20)	192.168.40.2	192.168.40.1	255.255.255.0
Windows10x64 (VLAN30)	192.168.50.2	192.168.50.1	255.255.255.0
PC-3 (VLAN40)	192.168.60.2	192.168.60.1	255.255.255.0

This zone consists of user devices, printers, and internal servers. It is segmented into VLANs to separate traffic based on function, such as isolating administrative devices from general users, enhancing performance, and security.

Note:

The number of IP addresses is reduced and manually assigned to the management network by dividing the range into subnets using a /29 mask. This enhances security by limiting the available address space and reducing the risk of unused or unauthorized IP addresses. The gateway for each host in the management network is the IP address of the firewall interface within the same network. However, in the LAN area, IP addresses are dynamically distributed using DHCP to simplify management and scalability. In the WAN area, the firewall prevents devices from obtaining IP addresses via NAT to maintain a higher level of security and prevent any Dynamic IP assignment.

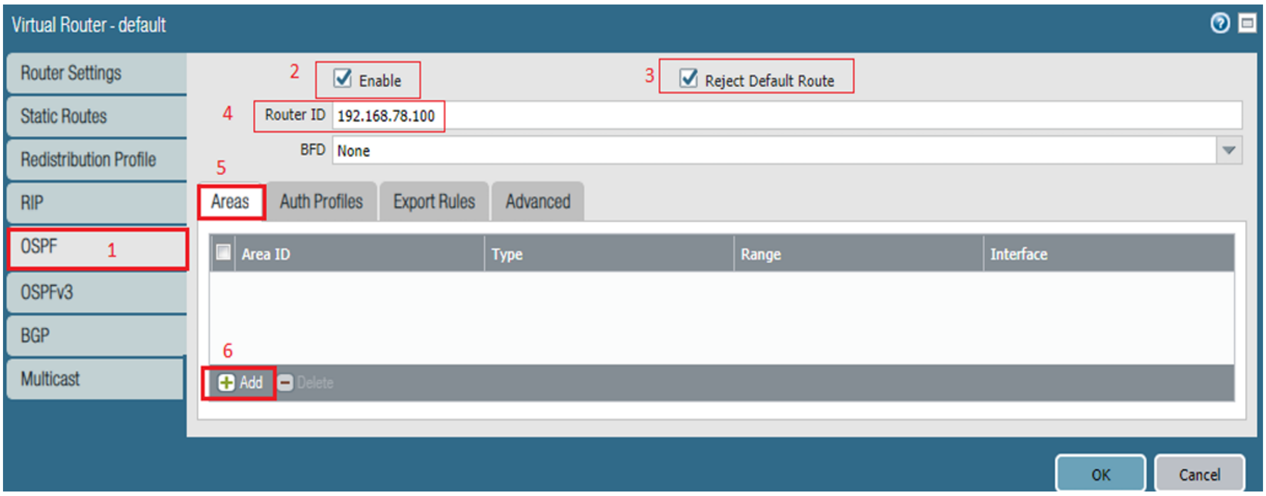


```
admin@PAFW_LAN> configure
Entering configuration mode
[edit]
admin@PAFW_LAN# delete deviceconfig system type dhcp-client

Object doesn't exist

[edit]
admin@PAFW_LAN# set deviceconfig system hostname PAFW_LAN

[edit]
admin@PAFW_LAN# set deviceconfig system ip-address 192.168.20.3 netmask 255.255.255.248

[edit]
admin@PAFW_LAN# set deviceconfig system default-gateway 192.168.20.2

[edit]
admin@PAFW_LAN# set deviceconfig system dns-setting servers primary 8.8.8.8

[edit]
admin@PAFW_LAN# set deviceconfig system dns-setting servers secondary 1.1.1.1

[edit]
admin@PAFW_LAN# commit


Commit job 3 is in progress. Use Ctrl+C to return to command prompt
...........55%.75%98%...........100%
Configuration committed successfully

[edit]
admin@PAFW_LAN#
```

Figure. 4.2. Basic config for PAFW

4.2.3. Configuring Palo Alto Firewall

This section presents all the configurations applied to the LAN network, which serve as the foundation for setting up the remaining environments in a similar manner. Figure (4.2) illustrates the process of setting up a Palo Alto Firewall) PAFW (using the CLI via Solar-PuTTY .Initially ,the DHCP deletion command was executed in order to activate IP static ,deactivate dynamics ,and enter configuration mode to make the necessary adjustments .The device name is set to be" PAFW_LAN ," then the IP address of the management interface is set as "192.168.20.3" with the subnet mask ."255.255.248"After that ,a virtual gateway with the address "192.168.20.2" is configured ,as well as the primary and secondary DNS servers are set up ,where the primary server is set "8.8.8.8" and



☑ Enable

☑ Reject Default Route

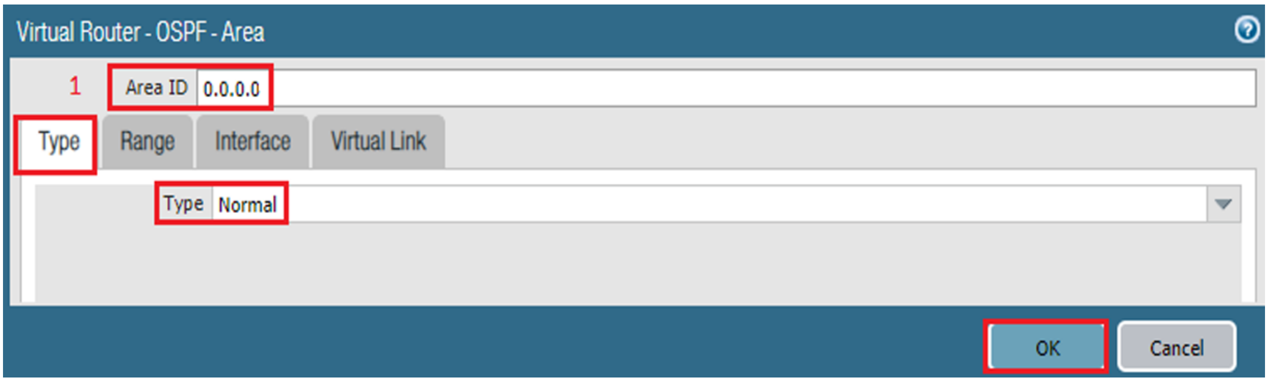
Router ID 192.168.78.100

BFD None

Figure. 4.3. Configure OSPF in F.W

the secondary server ."1.1.1.1" Finally ,modifications were applied using the command" commit ," and the success of the configuration was confirmed .This setting is used to properly secure the administration area and connect the firewall to the network.

- Figure (4.3) show Select OSPF from the menu on the left. Select Enable to enable the OSPF protocol. Select Reject Default Route if you do not want to learn any default routes through OSPF. Enter the Route ID, then press add in areas section.

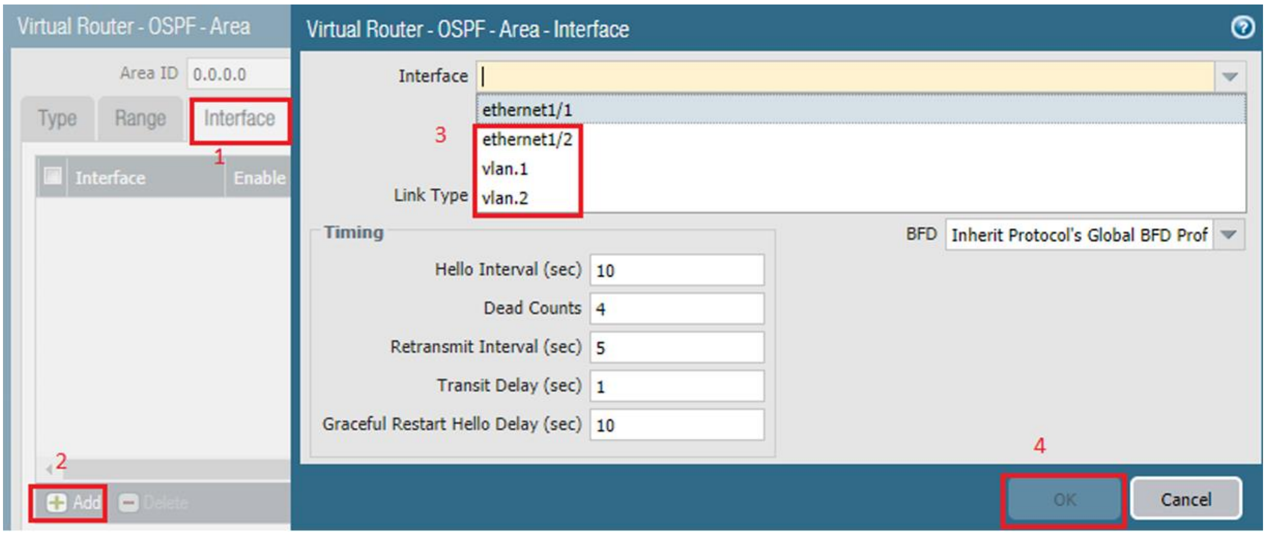


Area ID 0.0.0.0

Type Normal

Figure. 4.4. Area ID

- Figure (4.4) show Enter an Area ID for the area. This is the identifier that each neighbor must accept to be part of the same area. Area ID 0.0.0.0 is the same as Cisco’s Area 0. On the Type tab, select Normal then press OK.



Area ID 0.0.0.0

Interface |

Hello Interval (sec) 10

Dead Counts 4

Retransmit Interval (sec) 5

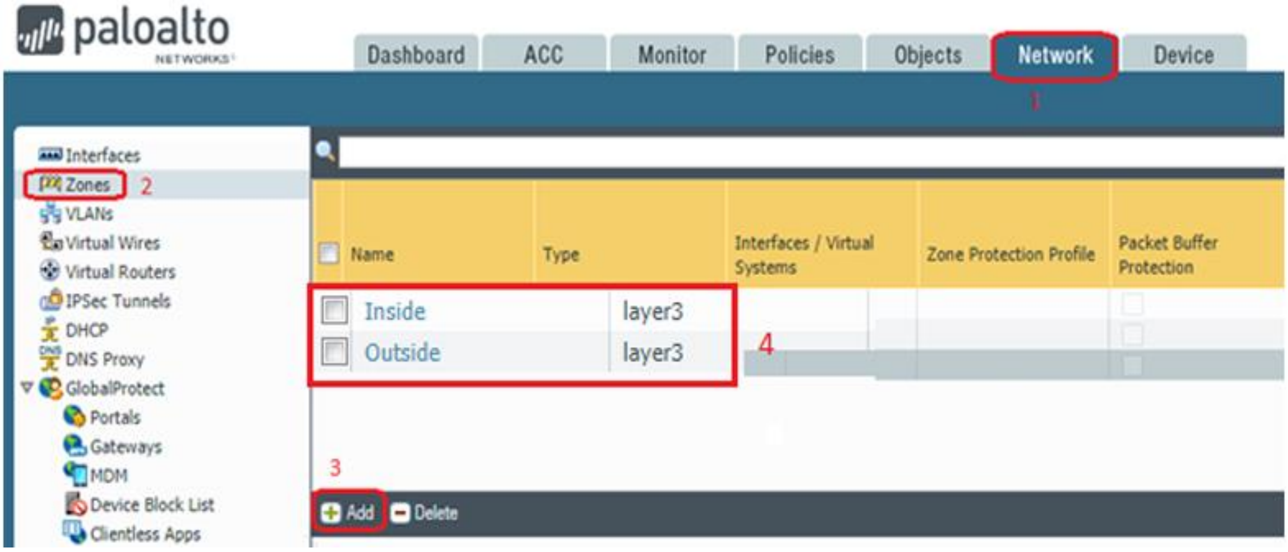
Transit Delay (sec) 1

Graceful Restart Hello Delay (sec) 10

BFD Inherit Protocol's Global BFD Prof

Figure. 4.5. Add Interface

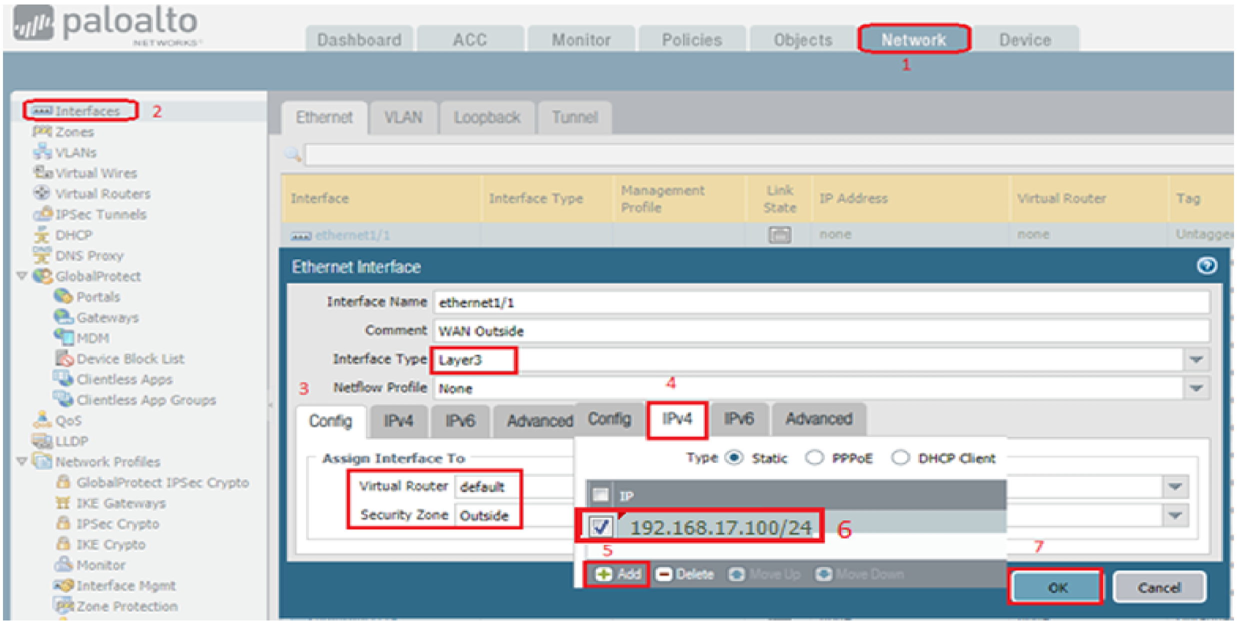
- Figure (4.5) show Select Interface tab and click add. Interface—Select an interface from the drop-down. Click OK.



Name	Type	Interfaces / Virtual Systems	Zone Protection Profile	Packet Buffer Protection
☐ Inside	layer3			☐
☐ Outside	layer3			☐

Figure. 4.6. Create Zones

- **Create Zones:** Figure (4.6) show configure two zones' names Inside and Outside. Go to Network> Zone>Add, Give the name Inside, select Type to be Layer3 and click OK. Create the same way other Zone Outside.



Interface Name: ethernet1/1

Comment: WAN Outside

Interface Type: Layer3

Netflow Profile: None

Assign Interface To

Virtual Router: default

Security Zone: Outside

Type ● Static ○ PPPoE ○ DHCP Client

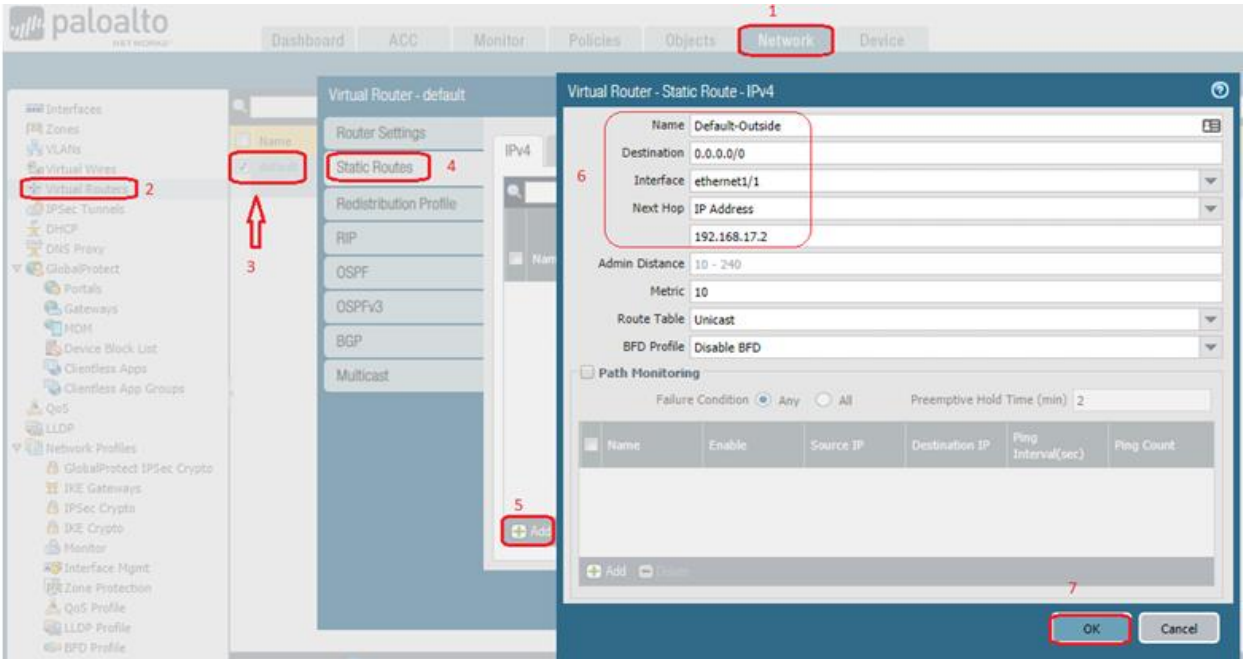
☐ IP

☑ 192.168.17.100/24

Figure. 4.7. Configure Interfaces

- **Configure Interfaces:** Figure (4.7) show Go to Network > Interfaces Click on ethernet1/1 interface change Interface Type: Layer3, set Virtual Router: default, set Security Zone: Outside, Click on IPv4 tab Assign IP Address: 192.168.17.100/24 and Click OK. Go to Network>Interfaces Click on ethernet1/2 interface change Interface Type: Layer3, set Virtual

Router: default, set Security Zone: Inside , Click on IPv4 tab Assign IP Address: 192.168.78.100/24 and Click OK.

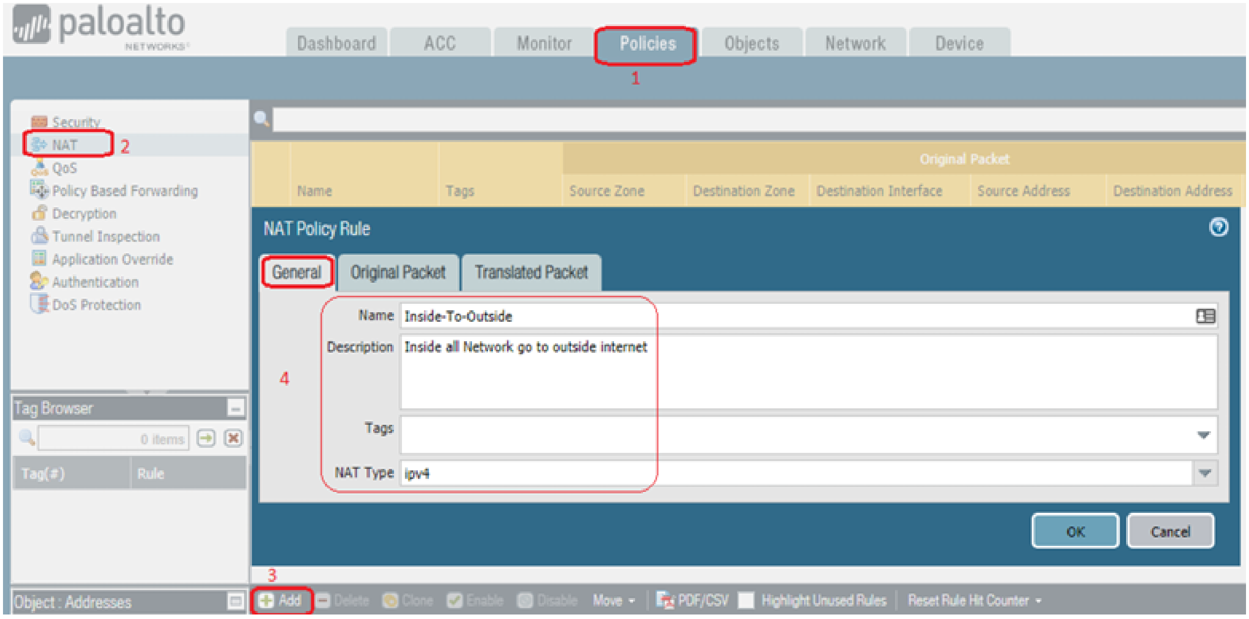


Virtual Router - Static Route - IPv4

Name: Default-Outside
Destination: 0.0.0.0/0
Interface: ethernet1/1
Next Hop: IP Address
192.168.17.2
Admin Distance: 10 - 240
Metric: 10
Route Table: Unicast
BFD Profile: Disable BFD
□ Path Monitoring
Failure Condition ● Any ○ All
Preemptive Hold Time (min) 2

Figure. 4.8. Configure Routing

- **Configure Routing:** Figure (4.8) show Each interface must be given virtual router. Network > Virtual Router > default we will add static routing. Static Routes > IPv4 > Add we will go by choosing interface > ethernet1/1 (as Outside), put 192.168.17.2 as the next hop due to our topology.



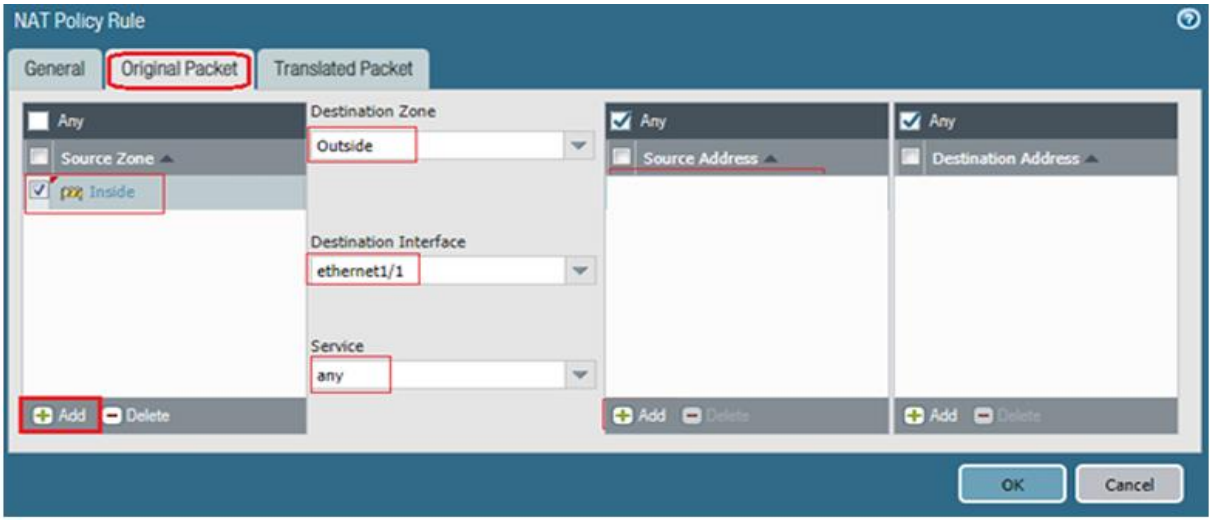
NAT Policy Rule

General | Original Packet | Translated Packet

Name: Inside-To-Outside
Description: Inside all Network go to outside internet
Tags:
NAT Type: ipv4

Figure. 4.9. Configure NAT

- **Nating Policy:** Figure (4.9) show the configure NAT using Dynamic IP and Port to NAT my Inside LAN 192.168.78.0/24 to 192.168.17.100 IP address of WAN.Going to Policies > NAT > Add. Let’s name it Inside-To-Outside.



☐ Any

Source Zone

☑ Inside

Destination Zone: Outside

Destination Interface: ethernet1/1

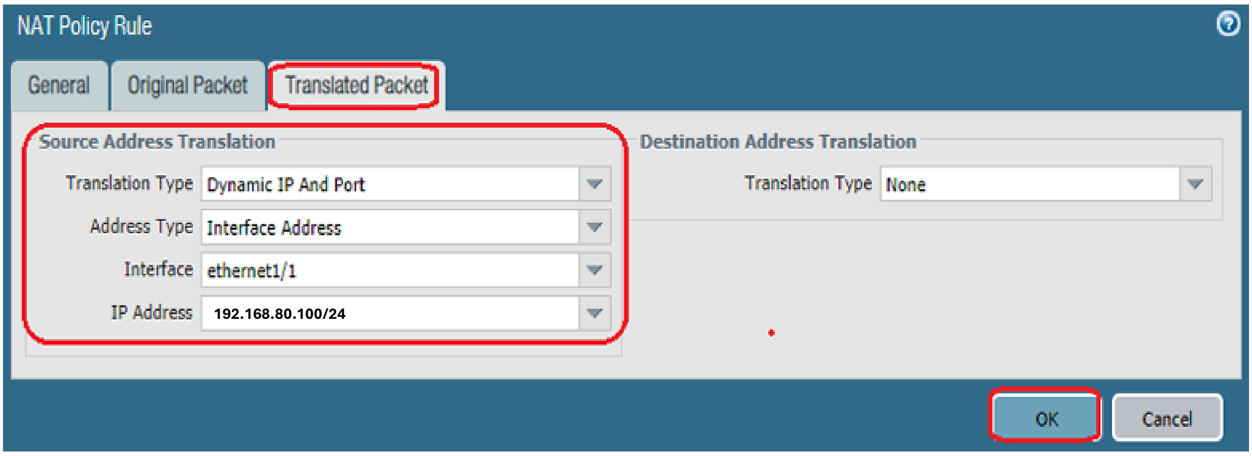
Service: any

☑ Any — Source Address

☑ Any — Destination Address

Figure. 4.10. Nating Between Zones

- Figure (4.10) show Go to Original Packet and fill since, traffic coming from Inside (192.168.1.102 is in Inside) then destination zone Outside (since 192.168.80.100/24 is going to Internet), destination interface is ethenret1/1 outgoing Interface. Set Service to any.



Source Address Translation

Translation Type: Dynamic IP And Port

Address Type: Interface Address

Interface: ethernet1/1

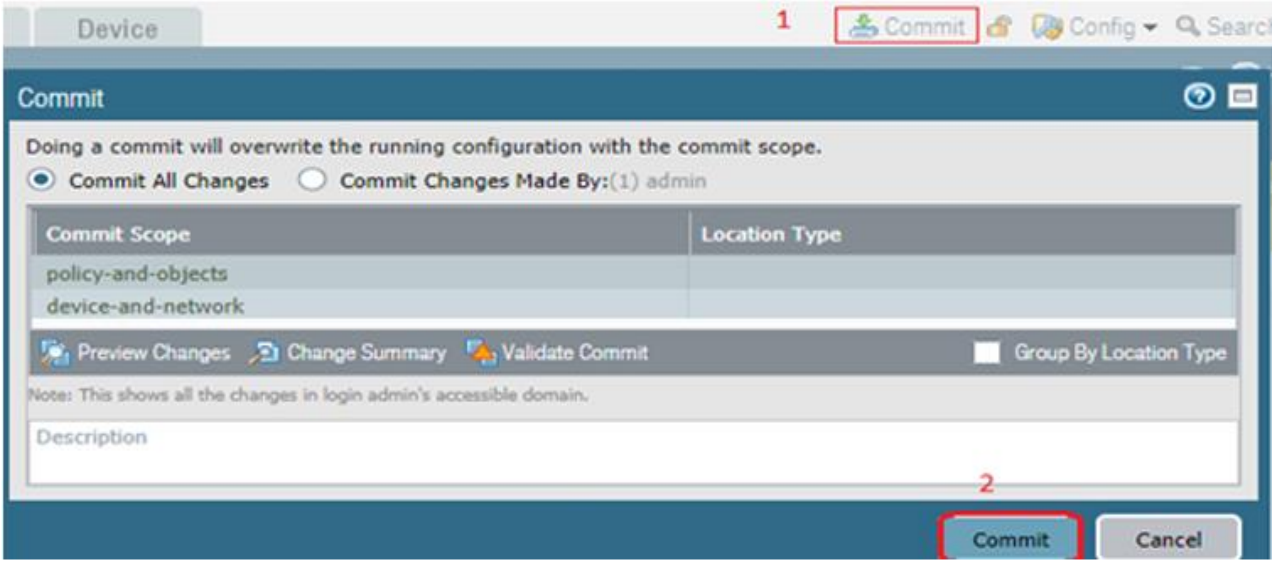
IP Address: 192.168.80.100/24

Destination Address Translation

Translation Type: None

Figure. 4.11. Configure Dynamic IP And Port

After specifying the general information, the next crucial step is to define the translation type as Dynamic IP and port, which will be connected to the destination zone, designated as the external zone, through the ethernet1/1 port. Once the configuration is complete, click [OK] to apply the settings as shown in Figure (4.11).



Doing a commit will overwrite the running configuration with the commit scope.

● Commit All Changes ○ Commit Changes Made By:(1) admin

Commit Scope	Location Type
policy-and-objects	
device-and-network	

□ Group By Location Type

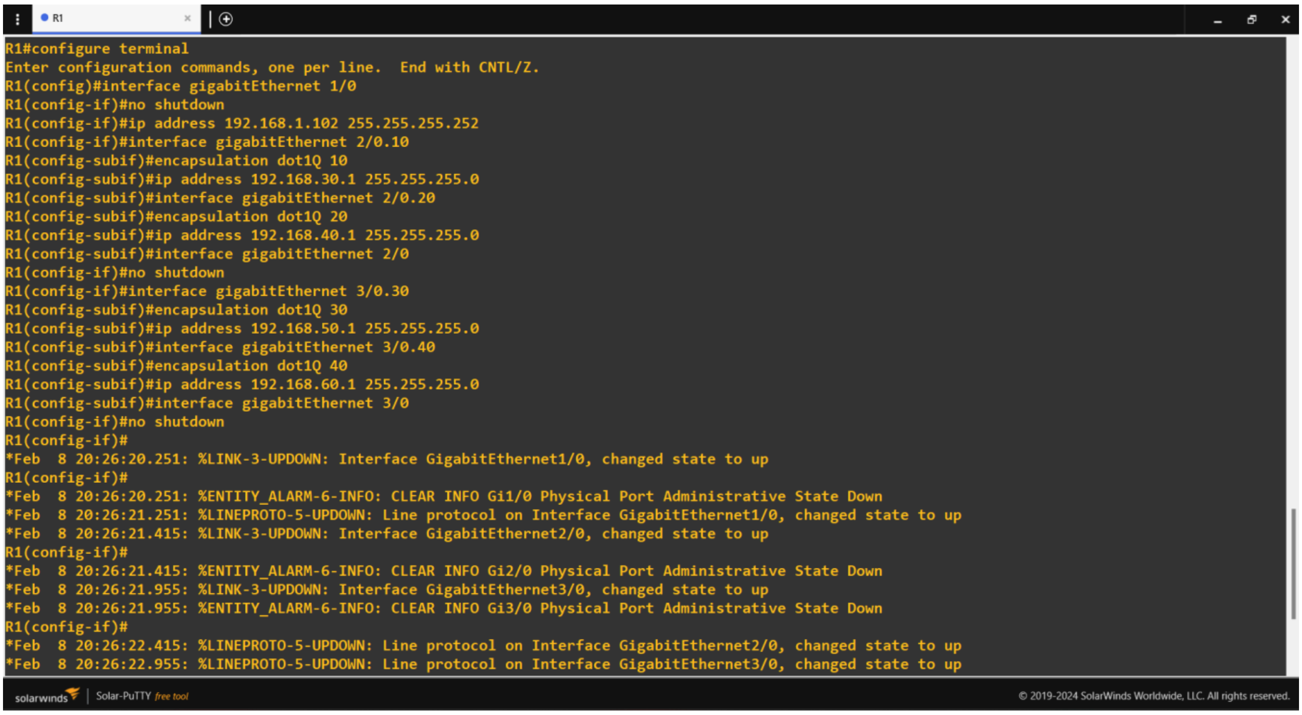
Note: This shows all the changes in login admin's accessible domain.

Figure. 4.12. Save Changes

- **Commit Changes:** Figure (4.12) show Commit the Changes by Clicking Commit on top right corner to save the configuration.

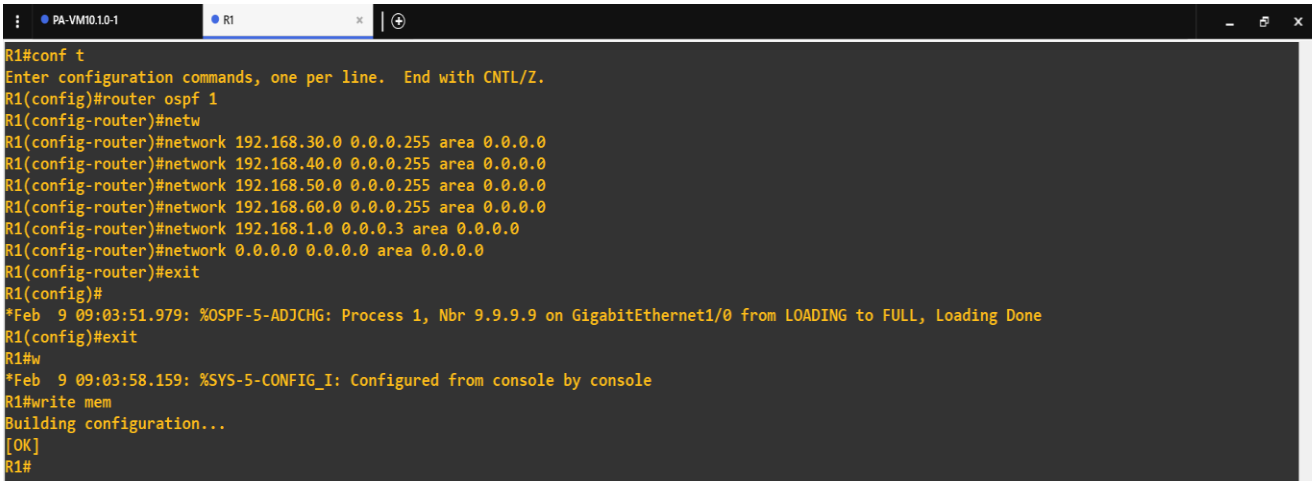
4.2.4. Configuring the network components

- Figure (4.13) illustrates the configuration of Router1. The router has multiple sub interfaces configured using dot1q, each corresponding to a specific VLAN. IP addresses are assigned to each sub interface to act as default gateways for VLANs 10, 20, 30, and 40. The router is used to enable inter-VLAN routing, allowing communication between the different virtual networks.



```
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface gigabitEthernet 1/0
R1(config-if)#no shutdown
R1(config-if)#ip address 192.168.1.102 255.255.255.252
R1(config-if)#interface gigabitEthernet 2/0.10
R1(config-subif)#encapsulation dot1Q 10
R1(config-subif)#ip address 192.168.30.1 255.255.255.0
R1(config-subif)#interface gigabitEthernet 2/0.20
R1(config-subif)#encapsulation dot1Q 20
R1(config-subif)#ip address 192.168.40.1 255.255.255.0
R1(config-subif)#interface gigabitEthernet 2/0
R1(config-if)#no shutdown
R1(config-if)#interface gigabitEthernet 3/0.30
R1(config-subif)#encapsulation dot1Q 30
R1(config-subif)#ip address 192.168.50.1 255.255.255.0
R1(config-subif)#interface gigabitEthernet 3/0.40
R1(config-subif)#encapsulation dot1Q 40
R1(config-subif)#ip address 192.168.60.1 255.255.255.0
R1(config-subif)#interface gigabitEthernet 3/0
R1(config-if)#no shutdown
R1(config-if)#
*Feb  8 20:26:20.251: %LINK-3-UPDOWN: Interface GigabitEthernet1/0, changed state to up
R1(config-if)#
*Feb  8 20:26:20.251: %ENTITY_ALARM-6-INFO: CLEAR INFO Gi1/0 Physical Port Administrative State Down
*Feb  8 20:26:21.251: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0, changed state to up
*Feb  8 20:26:21.415: %LINK-3-UPDOWN: Interface GigabitEthernet2/0, changed state to up
R1(config-if)#
*Feb  8 20:26:21.415: %ENTITY_ALARM-6-INFO: CLEAR INFO Gi2/0 Physical Port Administrative State Down
*Feb  8 20:26:21.955: %LINK-3-UPDOWN: Interface GigabitEthernet3/0, changed state to up
*Feb  8 20:26:21.955: %ENTITY_ALARM-6-INFO: CLEAR INFO Gi3/0 Physical Port Administrative State Down
R1(config-if)#
*Feb  8 20:26:22.415: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet2/0, changed state to up
*Feb  8 20:26:22.955: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet3/0, changed state to up
```

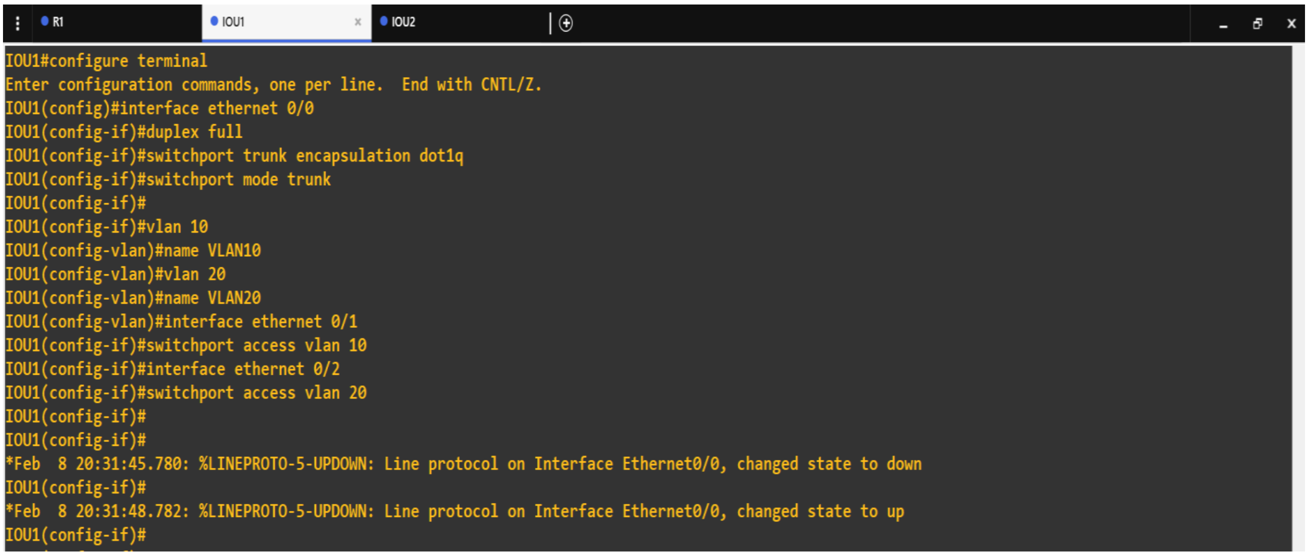
Figure. 4.13. Config Router1



```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#router ospf 1
R1(config-router)#netw
R1(config-router)#network 192.168.30.0 0.0.0.255 area 0.0.0.0
R1(config-router)#network 192.168.40.0 0.0.0.255 area 0.0.0.0
R1(config-router)#network 192.168.50.0 0.0.0.255 area 0.0.0.0
R1(config-router)#network 192.168.60.0 0.0.0.255 area 0.0.0.0
R1(config-router)#network 192.168.1.0 0.0.0.3 area 0.0.0.0
R1(config-router)#network 0.0.0.0 0.0.0.0 area 0.0.0.0
R1(config-router)#exit
R1(config)#
*Feb  9 09:03:51.979: %OSPF-5-ADJCHG: Process 1, Nbr 9.9.9.9 on GigabitEthernet1/0 from LOADING to FULL, Loading Done
R1(config)#exit
R1#w
*Feb  9 09:03:58.159: %SYS-5-CONFIG_I: Configured from console by console
R1#write mem
Building configuration...
[OK]
R1#
```

Figure. 4.14. Config OSPF Routing

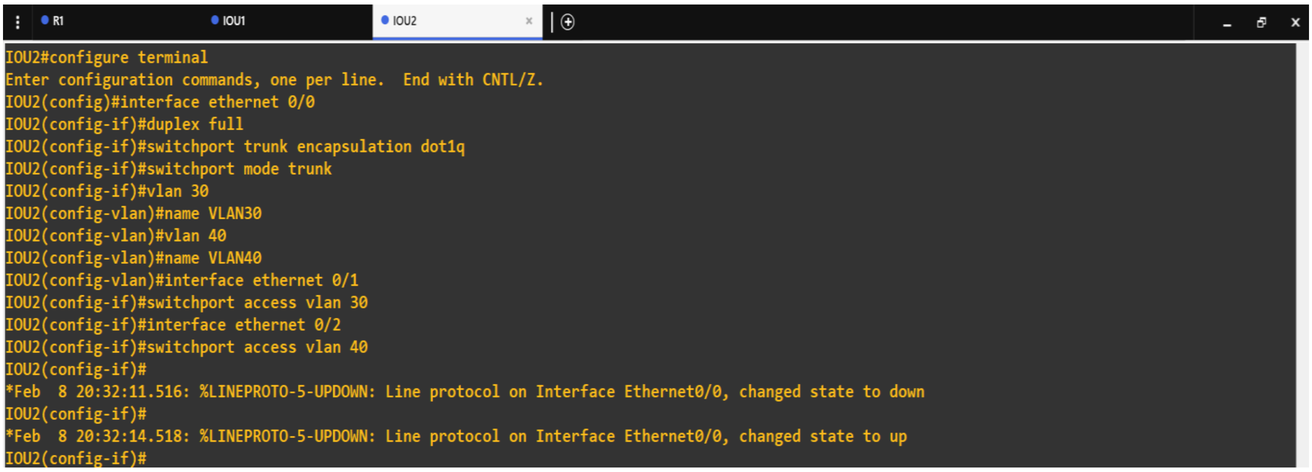
- Figure (4.14) shows the command-line interface of a router, where commands are being entered to configure OSPF routing. It shows the commands used to set up the subnet and define areas for the OSPF protocol. It also indicates that the loading process was successful, these steps are essential to ensure effective communication between devices in the network and enhance routing efficiency.



```
IOU1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
IOU1(config)#interface ethernet 0/0
IOU1(config-if)#duplex full
IOU1(config-if)#switchport trunk encapsulation dot1q
IOU1(config-if)#switchport mode trunk
IOU1(config-if)#
IOU1(config-if)#vlan 10
IOU1(config-vlan)#name VLAN10
IOU1(config-vlan)#vlan 20
IOU1(config-vlan)#name VLAN20
IOU1(config-vlan)#interface ethernet 0/1
IOU1(config-if)#switchport access vlan 10
IOU1(config-if)#interface ethernet 0/2
IOU1(config-if)#switchport access vlan 20
IOU1(config-if)#
IOU1(config-if)#
*Feb  8 20:31:45.780: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to down
IOU1(config-if)#
*Feb  8 20:31:48.782: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to up
IOU1(config-if)#
```

Figure. 4.15. Config Switch1

- Figure (4.15) shows the configuration for Switch1. The Ethernet 0/0 interface is set as a trunk port using the dot1q protocol, allowing traffic from all VLANs to pass through. VLANs 10 and 20 are created and named "VLAN10" and "VLAN20," respectively. Additionally, Ethernet ports 0/1 and 0/2 are configured as access ports associated with VLANs 10 and 20, respectively.

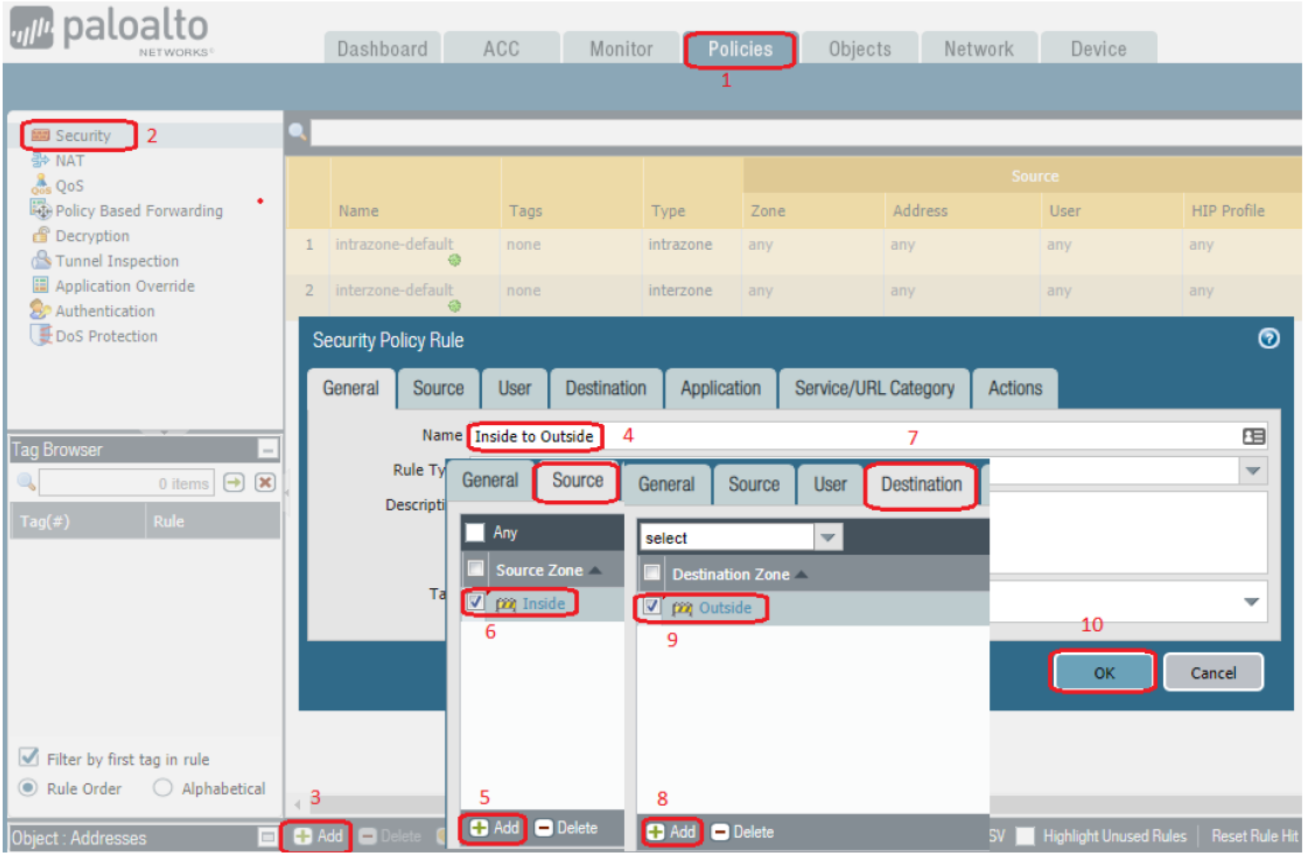


```
IOU2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
IOU2(config)#interface ethernet 0/0
IOU2(config-if)#duplex full
IOU2(config-if)#switchport trunk encapsulation dot1q
IOU2(config-if)#switchport mode trunk
IOU2(config-if)#vlan 30
IOU2(config-vlan)#name VLAN30
IOU2(config-vlan)#vlan 40
IOU2(config-vlan)#name VLAN40
IOU2(config-vlan)#interface ethernet 0/1
IOU2(config-if)#switchport access vlan 30
IOU2(config-if)#interface ethernet 0/2
IOU2(config-if)#switchport access vlan 40
IOU2(config-if)#
*Feb  8 20:32:11.516: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to down
IOU2(config-if)#
*Feb  8 20:32:14.518: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to up
IOU2(config-if)#
```

Figure. 4.16. Config Switch2

- These settings are used to segment the network into isolated sub-networks._Figure (4.16) show the displays the configuration for Switch2. Similar to Switch1, the Ethernet 0/0 interface is set as a trunk port using dot1q. VLANs 30 and 40 are created and named "VLAN30" and "VLAN40." Ethernet ports 0/1 and 0/2 are configured as access ports assigned to VLANs 30 and 40, respectively. These configurations aim to separate traffic between different virtual networks.

Note: The process of establishing connectivity between the firewall and devices, configuring inter-network communication, and implementing the initial setup for both the cloud and data center environments follows the same steps applied in the local network environment. Given this similarity, the same configuration procedures were not repeated for the remaining environments to avoid redundancy. Instead, the focus was placed on environment-specific customizations and security policies tailored to each use case.



Name: Inside to Outside

Figure. 4.17. Create Polices

- Figure (4.17) illustrates the steps for creating a **Security Policy Rule** in **Palo Alto NGFW**. The process begins by navigating to the **"Policies"** tab and selecting **"Security"** from the side menu to create a new rule. Next, the **"Add"** button is clicked to create the rule, and a name is assigned, such as **"Inside to Outside"**, to indicate traffic moving from the internal network to the internet. The **Source Zone** is then selected as **Inside** and added to the rule, followed by switching to the **"Destination"** tab and adding the **Destination Zone (Outside)**, representing the internet or external networks. Finally, the settings are saved by clicking **"OK"**.

Note: This approach will be followed when **creating security policies for all three environments (Local Network, Cloud Environment, and Data Center)**. The policies will be configured based on the specific security requirements of each environment, such as controlling data flow between internal and external networks, enforcing security filters, and utilizing features like **App-ID, User-ID, and Threat Prevention** to ensure robust protection.

4.2.5. Cloud Environment

The cloud environment is an essential part of modern digital infrastructure, providing access to computing and storage resources over the internet. This environment allows organizations to host applications and data flexibly and saleably, enhancing operational efficiency while reducing costs. In the context of our project, we focus on how to customize Next-Generation Firewall (NGFW) settings to protect these cloud resources from potential threats, ensuring data security and business continuity [26].

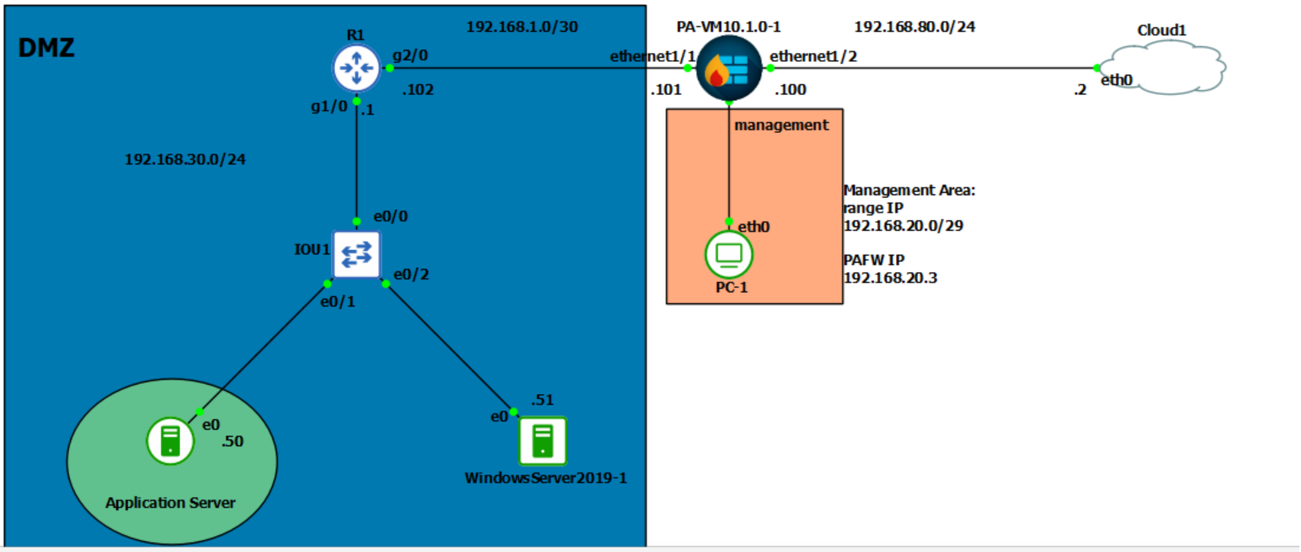


Figure. 4.18. Cloud Environment diagram

- Figure (4.18) illustrates a network configuration featuring an application server located in a DMZ, enhancing security by isolating it from the internal network. The server is connected to a router (R1) via an Ethernet interface, with specific IP addresses assigned. Additionally, the diagram shows a management PC (PC-1) utilizing an IP address for network administration, facilitating the monitoring and management of resources in the connected cloud environment.

4.2.6. Key Components of the Cloud Diagram

Network segments such as the DMZ (Demilitarized Zone) provide an extra security layer for public-facing services. The management area is responsible for administrative control, while cloud connectivity enables seamless integration with external networks. Together, these components establish a robust cloud infrastructure that balances security, accessibility, and performance [27].

As shown in Figure (4.18), multiple IP address ranges are utilized. The subsequent tables present these IP addresses along with their corresponding subnet masks and gateways, organized by zones:

1. **Management Zone:**

Table (4.4) Ip addresses for Management Zone

Device/Component	IP Address	Gateway	Subnet Mask
Palo Alto (Mgmt. Port)	192.168.20.3	192.168.20.2	255.255.255.248
PC-1 (eth0)	192.168.20.5	192.168.20.2	255.255.255.248

This zone manages cloud resources, including security configurations, firewall policies, and server administration. It ensures compliance with security protocols such as encryption and intrusion prevention, maintaining a stable and secure cloud environment.

2. **Cloud Zone:**

Table (4.5) Ip addresses for Cloud Connection Zone

Device/Component	IP Address	Gateway	Subnet Mask
PA-VM (eth1/2)	192.168.80.100	192.168.80.2	255.255.255.0
Cloud1 (eth0)	192.168.80.2	192.168.80.1	255.255.255.0

It connects the on-premises infrastructure to cloud services like AWS or Azure. Secure protocols such as VPNs and IPsec encrypt data transmissions, mitigating the risk of interception or breaches.

3. **DMZ Zone:**

Table (4.6) Ip addresses for DMZ Zone

Device/Component	IP Address	Gateway	Subnet Mask
Router_R1 (g2/0)	192.168.1.102	______	255.255.255.252

Device/Component	IP Address	Gateway	Subnet Mask
Router_R1 (g1/0)	192.168.30.1	______	255.255.255.0
PA-VM (eth1/1)	192.168.1.101	______	255.255.255.252
Application Server (e0)	192.168.30.50	192.168.30.1	255.255.255.0
Windows Server 2019-1 (e0)	192.168.30.51	192.168.30.1	255.255.255.0

This intermediate zone hosts public-facing services such as web and application servers. Strict access policies, port restrictions, and continuous monitoring are enforced to prevent cyberattacks from compromising the internal network.

4.2.7. Data Center Environment

The data center environment is a crucial element of modern information technology, used for centralized data storage and processing. These centers provide a robust and reliable infrastructure that supports the operation of various applications and services. In the context of our project, we

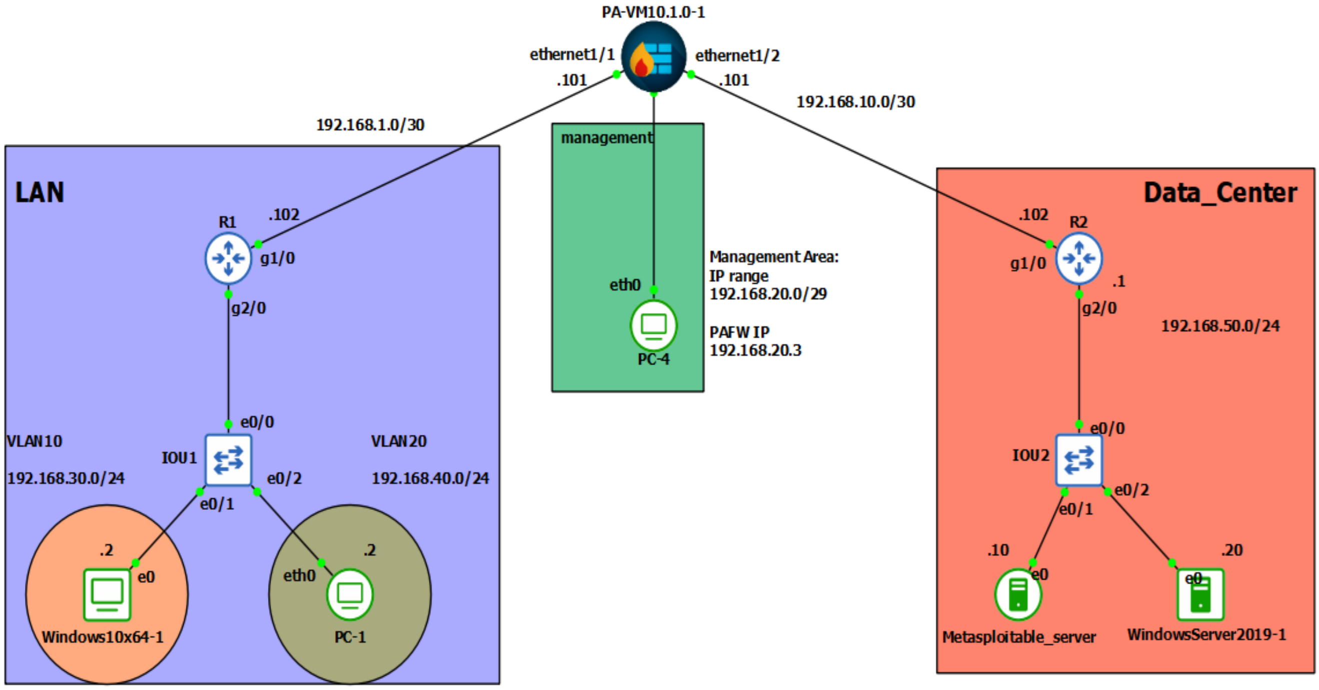


Figure. 4.19. Data Center diagram

focus on how data centers integrate with Next-Generation Firewalls (NGFW) to enhance security and protect data from increasing threats, ensuring business continuity and information integrity [21].

- Figure (4.19) illustrates a network configuration that includes a Local Area Network (LAN) and a data center. The LAN connects to a router (R1), which includes devices like a PC (PC-1) and a Windows server. The router connects to a management device (PA-WH) via Ethernet interfaces, with specific IP addresses assigned. The diagram also shows the data center containing a Windows server and an exploitable server, reflecting how resources are organized in a secure and efficient environment.

4.2.8. Key Components of the Data Center Diagram

The key components of the data center diagram represent the essential elements that ensure high performance and security within the data center environment. This includes the firewall, which acts as a security barrier to protect data and control traffic between different networks. Routers and switches play a crucial role in directing data and ensuring efficient communication between servers and devices within the center. Additionally, the **LAN** zone provides internal connectivity, while the **Data-center** zone secures public-facing services and enhances protection against external threats. These components work together to establish a well-balanced data center environment that prioritizes both security and operational efficiency. As shown in Figure 4.19, multiple IP address ranges are utilized. The subsequent tables present these IP addresses along with their corresponding subnet masks and gateways, organized by zones:

1. **Management Zone:**

Table (4.7) Ip addresses for Core Network Zone

Device/Component	IP Address	Gateway	Subnet Mask
PC-4 (eth0)	192.168.10.5	192.168.20.2	255.255.255.248
PA-VM (Mgmt. Port)	192.168.20.3	192.168.20.2	255.255.255.248

This zone houses administrative devices that oversee data center operations, including firewalls and monitoring servers. Strict access control policies ensure only authorized personnel can make security modifications.

2. **Data Center Zone:**

Table (4.8) Ip addresses for Data Center Zone

Device/Component	IP Address	Gateway	Subnet Mask
Router_R2 (g2/0) Router_R2 (g1/0)	192.168.50.1 192.168.10.102	_____ _____	255.255.255.0 255.255.255.252
Metasploitable_Server (e0)	192.168.50.10	192.168.50.1	255.255.255.0
Windows Server 2019-1 (e0)	192.168.50.20	192.168.50.1	255.255.255.0

Hosts servers containing critical applications and databases. Network segmentation and security measures like Intrusion Detection Systems (IDS) and Advanced Threat Protection (ATP) are deployed to safeguard sensitive data.

3. **LAN Zone:**

Table (4.9) Ip addresses for LAN Zone

Device/Component	IP Address	Gateway	Subnet Mask
R1 (g1/0) R1 (g2/0.10) R1 (g2/0.20)	192.168.1.102 192.168.30.1 192.168.40.1	_____ _____ _____	255.255.255.252 255.255.255.0 255.255.255.0
Windows10x64-1 (e0)	192.168.30.2	192.168.30.1	255.255.255.0
PC-1 (eth0)	192.168.40.2	192.168.40.1	255.255.255.0

Facilitates user access to data center resources, ensuring that permissions are assigned based on departmental needs. IT teams may have direct access, while general users interact with data through controlled applications.

4.3. Results

The results of this project demonstrated that customizing Next-Generation Firewall (NGFW) functionalities based on specific environmental needs enhances threat detection efficiency and improves network performance. Through the simulation of three environments (cloud, data centers, and local networks) using GNS3, findings showed that proper configuration reduces resource consumption and strengthens cybersecurity defenses. The results also highlighted the importance of balancing security and performance to maintain a secure and resilient network infrastructure.

1. **Effectiveness of NGFW Customization**

Simulation results using GNS3 and VMware demonstrated that customizing Next-Generation Firewall (NGFW) functionalities based on the specific environment (cloud, data centers, local networks) significantly improved performance while reducing unnecessary resource utilization.

2. **Achieving Security Objectives**

Security was enhanced against major threats, including malware attacks, phishing attempts, and internal data leaks, while also minimizing the risk of network downtime.

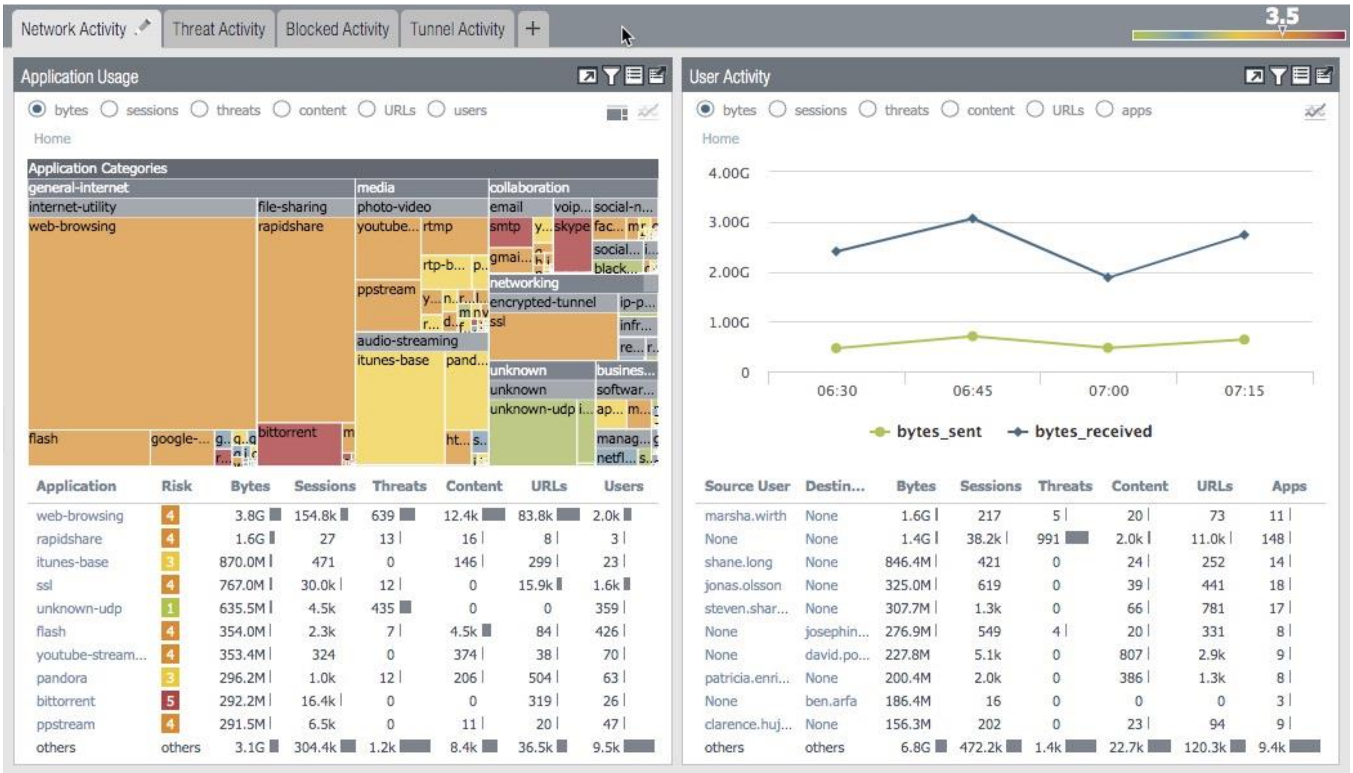
3. **Performance Analysis**

Customized firewalls exhibited high efficiency in detecting advanced threats, such as encrypted malware and malicious websites, while maintaining optimal data transmission performance.

4. **Application Command Center which gives Roya a credit**

The Application Command Center (ACC) provides a comprehensive visual overview of network traffic trends and historical data. In this project, the ACC interface is used to monitor overall network risk levels, identify threats from high-risk and frequently used applications, and assess application categories with the most detected threats. Users can analyze traffic patterns over various timeframes, including the past hour, day, week, month, or a custom-defined period [13].

Risk levels are categorized from 1 (lowest) to 5 (highest), reflecting an application's security risk based on factors like file-sharing capabilities, potential for misuse, or attempts to bypass firewall protections. Within the WebGUI, the Dashboard tab displays the ACC Risk Factor, offering insight into network threat activity over the past 60 minutes. Elevated risk levels can be investigated by accessing the main ACC interface to pinpoint the source of increased threat activity [29].



Application	Risk	Bytes	Sessions	Threats	Content	URLs	Users
web-browsing	4	3.8G	154.8k	639	12.4k	83.8k	2.0k
rapidshare	4	1.6G	27	13	16	8	3
itunes-base	3	870.0M	471	0	146	299	23
ssl	4	767.0M	30.0k	12	0	15.9k	1.6k
unknown-udp	1	635.5M	4.5k	435	0	0	359
flash	4	354.0M	2.3k	7	4.5k	84	426
youtube-stream...	4	353.4M	324	0	374	38	70
pandora	3	296.2M	1.0k	12	206	504	63
bittorrent	5	292.2M	16.4k	0	0	319	26
ppstream	4	291.5M	6.5k	0	11	20	47
others	others	3.1G	304.4k	1.2k	8.4k	36.5k	9.5k

Source User	Destin...	Bytes	Sessions	Threats	Content	URLs	Apps
marsha.wirth	None	1.6G	217	5	20	73	11
None	None	1.4G	38.2k	991	2.0k	11.0k	148
shane.long	None	846.4M	421	0	24	252	14
jonas.olsson	None	325.0M	619	0	39	441	18
steven.shar...	None	307.7M	1.3k	0	66	781	17
None	josephin...	276.9M	549	4	20	331	8
None	david.po...	227.8M	5.1k	0	807	2.9k	9
patricia.enri...	None	200.4M	2.0k	0	386	1.3k	8
None	ben.arfa	186.4M	16	0	0	0	3
clarence.huj...	None	156.3M	202	0	23	94	9
others	others	6.8G	472.2k	1.4k	22.7k	120.3k	9.4k

Figure. 4.20. ACC results

Additionally, the Top Applications widget, when enabled, highlights applications with the highest session counts. Each block's size represents the relative number of sessions (hovering over a block reveals the session count), while the block color indicates the associated security risk—ranging from green (low risk) to red (high risk) [29]. Clicking on a block provides detailed information about the selected application, including a breakdown of its activity within the ACC.

- Each widget includes the following components:

1. View: Sort and organize data using selectable options.
2. Graph: Visualize data through various graphical formats, depending on the widget.
3. Table: Access detailed data that underpins the graphical displays.
4. Actions: Expand the view, apply local filters, navigate to logs, or export data for further analysis.

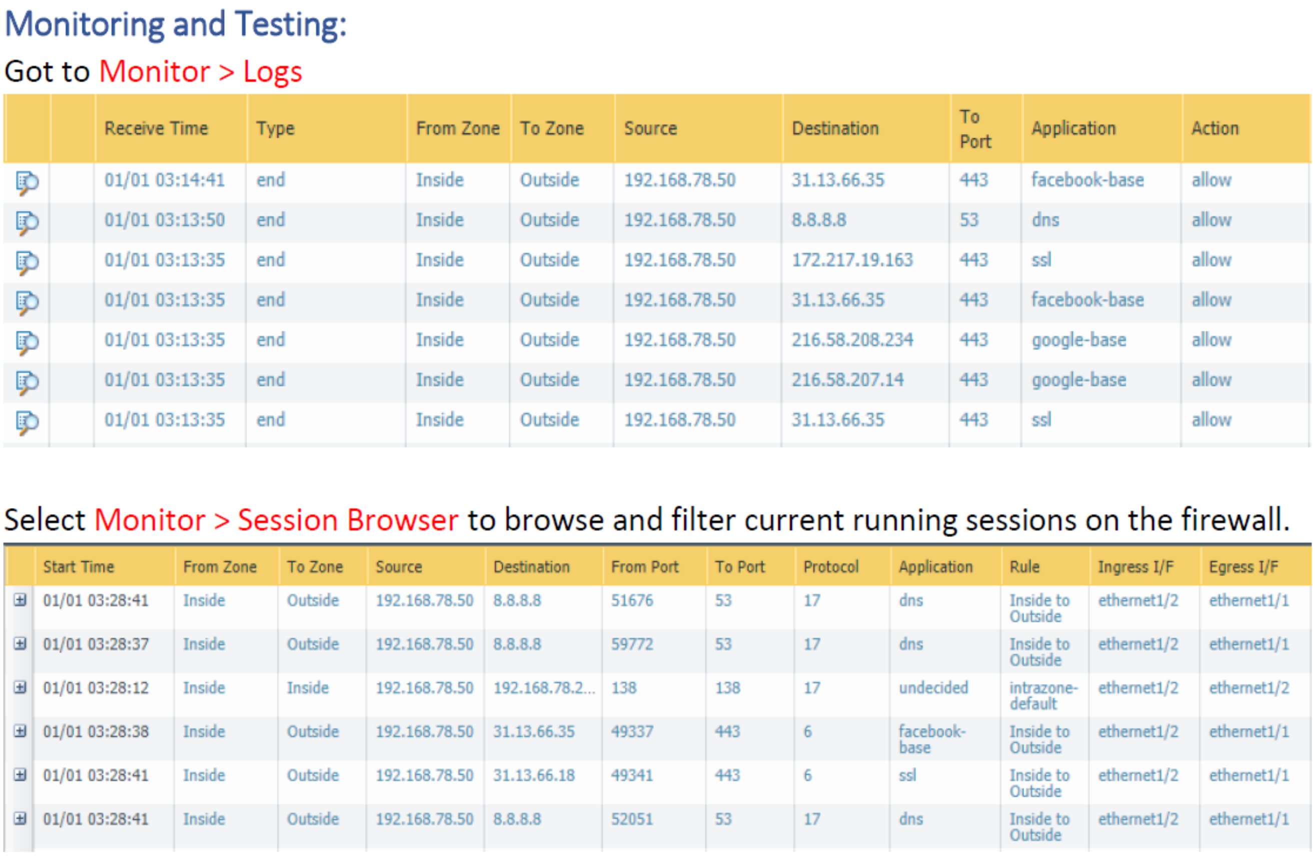
As it showed in Figure (4.20) of the interface is attached to demonstrate the ACC layout and functionality.

The three environments—LAN, Cloud, and Data Center—were thoroughly examined to assess their network activity and security performance. The evaluation process involved simulating each environment using the GNS3 platform, with the PAN VM-Series Firewall deployed to monitor and analyze traffic patterns. For the LAN environment, internal network communications, device interactions, and local application usage were observed. In the Cloud environment, data transmissions to and from cloud-based services were monitored to evaluate external access and threat exposure. The Data Center environment was assessed by simulating high-volume data transfers, server communications, and external client access.

Network activity data from all three environments was collected and analyzed using the Application Command Center (ACC), which provided real-time insights into traffic trends, risk levels, and detected threats. The results, as previously displayed in the Network Activity section, include detailed information on high-risk applications, top communication sources, and potential vulnerabilities within each environment. By leveraging the ACC's visual analytics and customizable filters, it was possible to drill down into specific traffic flows, identify abnormal behaviors, and assess how effectively the Next-Generation Firewall (NGFW) mitigated potential threats in different network scenarios.

5. Monitoring and Testing

Through the research findings, we achieved better visibility and monitoring of logs, which contributed to reducing false alarms and improving the system's response to actual threats. Additionally, data was recorded in multiple locations and categorized based on types, risk levels, and associated logs, enhancing the efficiency of security analysis and decision-making for network protection.



Monitoring and Testing:

Got to Monitor > Logs

Receive Time	Type	From Zone	To Zone	Source	Destination	To Port	Application	Action
01/01 03:14:41	end	Inside	Outside	192.168.78.50	31.13.66.35	443	facebook-base	allow
01/01 03:13:50	end	Inside	Outside	192.168.78.50	8.8.8.8	53	dns	allow
01/01 03:13:35	end	Inside	Outside	192.168.78.50	172.217.19.163	443	ssl	allow
01/01 03:13:35	end	Inside	Outside	192.168.78.50	31.13.66.35	443	facebook-base	allow
01/01 03:13:35	end	Inside	Outside	192.168.78.50	216.58.208.234	443	google-base	allow
01/01 03:13:35	end	Inside	Outside	192.168.78.50	216.58.207.14	443	google-base	allow
01/01 03:13:35	end	Inside	Outside	192.168.78.50	31.13.66.35	443	ssl	allow

Select Monitor > Session Browser to browse and filter current running sessions on the firewall.

Start Time	From Zone	To Zone	Source	Destination	From Port	To Port	Protocol	Application	Rule	Ingress I/F	Egress I/F
01/01 03:28:41	Inside	Outside	192.168.78.50	8.8.8.8	51676	53	17	dns	Inside to Outside	ethernet1/2	ethernet1/1
01/01 03:28:37	Inside	Outside	192.168.78.50	8.8.8.8	59772	53	17	dns	Inside to Outside	ethernet1/2	ethernet1/1
01/01 03:28:12	Inside	Inside	192.168.78.50	192.168.78.2...	138	138	17	undecided	intrazone-default	ethernet1/2	ethernet1/2
01/01 03:28:38	Inside	Outside	192.168.78.50	31.13.66.35	49337	443	6	facebook-base	Inside to Outside	ethernet1/2	ethernet1/1
01/01 03:28:41	Inside	Outside	192.168.78.50	31.13.66.18	49341	443	6	ssl	Inside to Outside	ethernet1/2	ethernet1/1
01/01 03:28:41	Inside	Outside	192.168.78.50	8.8.8.8	52051	53	17	dns	Inside to Outside	ethernet1/2	ethernet1/1

Figure. 4.21. Monitoring and Testing

- Figure (4.21) illustrates the steps for **monitoring and testing** traffic on the **Palo Alto firewall** through the **Monitor** section. First, navigate to **Monitor > Logs** to view **traffic logs**, which display the connections between networks, including **time received, session type, source zone, destination zone, source and destination IP addresses, used ports, application, and action taken (allow or deny)**. It can be noted that all connections in the log have been allowed, such as **DNS, SSL, and Facebook-base** traffic.

Additionally, **Monitor > Session Browser** can be used to view active sessions on the firewall and filter data based on criteria such as **source and destination zones, ports, protocols, applications, applied rules, and interfaces used**. This provides a comprehensive view of data traffic across the firewall, helping administrators in **analyzing activity, detecting threats, and effectively tuning security policies**.

4.4. Traffic Risk Assessment and Performance Metrics

Effective network security requires continuous monitoring and assessment of traffic to detect and mitigate potential threats. This section explores key security metrics used to evaluate traffic risk and enhance overall network performance. By analyzing various indicators, such as data flow rate, packet inspection, abnormal connection attempts, and behavioral analysis, organizations can identify suspicious activities and respond proactively. Additionally, advanced threat intelligence and deep packet inspection (DPI) play a crucial role in uncovering hidden threats and preventing unauthorized access. The following metrics provide a structured approach to assessing network security and optimizing firewall performance.

4.4.1. Impact of Palo Alto NGFW Customization on Security and Performance

1. Traffic Risk Assessment - Palo Alto NGFW

To evaluate the impact of Palo Alto NGFW customization on network security, a risk assessment was conducted before and after implementing its security features. The table below presents the percentage distribution of different risk levels, demonstrating how App-ID and Threat Prevention significantly reduce high and critical risks, thereby enhancing overall security.

Table (4.10) Traffic Risk Assessment

Risk Level	Before Palo Alto NGFW Customization	After Palo Alto NGFW Customization
Low	35%	75%
Medium	40%	18%
High	15%	5%
Critical	10%	2%

Note: App-ID and **Threat Prevention** in **Palo Alto NGFW** reduce high and critical risks by up to **80%**, significantly improving overall security.

2. Performance Metrics - Palo Alto NGFW

Optimizing NGFW settings improves not only security but also network performance and efficiency. The following table compares key performance metrics before and after customizing Palo Alto NGFW, highlighting improvements in response time, packet processing rate, latency, and supported concurrent sessions due to SP3 (Single-Pass Parallel Processing) technology.

Table (4.11) Performance Metrics

Metric	Before Palo Alto NGFW Customization	After Palo Alto NGFW Customization
Response Time (ms)	100	45
Packet Processing Rate (Gbps)	3.5	5.2
Latency (ms)	60	25
Supported Concurrent Sessions	500K	1.2M

Note: SP3 (Single-Pass Parallel Processing) technology in Palo Alto NGFW accelerates deep packet inspection without performance degradation, reducing latency by **58%**.

3. Threat Analysis - Palo Alto NGFW

An essential measure of firewall effectiveness is its ability to detect and block threats across different environments. The table below outlines the number of threats detected before customization and the number successfully blocked after applying advanced security features like WildFire, DNS Security, and URL Filtering, achieving a high success rate in threat mitigation.

Table (4.12) Threat Analysis

Environment	Detected Threats Before Customization	Blocked Threats After Customization	Success Rate (%)
Local Network (LAN)	3,200	3,000	93%

Environment	Detected Threats Before Customization	Blocked Threats After Customization	Success Rate (%)
Cloud Environment	5,500	5,200	95%
Data Center	8,000	7,800	97.5%

Note: Features like **WildFire, DNS Security, and URL Filtering** in PAFW enhance advanced threat detection, achieving a **97.5%** threat-blocking success rate in data center environments.

4.5. Traffic Risk Classification

Traffic Risk Classification is a crucial component in customizing Next-Generation Firewalls (NGFWs) to ensure an effective response to cyber threats. This classification analyzes network behavior and assesses the risk level of traffic, ranging from low-risk normal activities to critical attacks requiring immediate action. This project aims to enhance risk classification mechanisms to improve threat detection accuracy and reduce false alarms, ultimately optimizing firewall performance and strengthening network security [23].

Traffic is categorized based on its risk level to determine the appropriate security response showed in Table (4.13).

Table (4.13) Traffic Risk Classification

Risk Level	Description	Action Taken
Low	Normal activity or unintentional errors.	Allow traffic and log the event.
Medium	Suspicious activity, such as a slight increase in failed login attempts.	Alert administrators and monitor traffic.
High	Repeated login attempts or unusual traffic patterns.	Temporarily block the connection and investigate.
Critical	Confirmed attack, such as malware downloads or data exfiltration.	Immediately block the connection, alert security teams, and initiate incident response.

Note: The firewall actively monitors and inspects network traffic to detect suspicious activities and categorize them based on their severity, ranging from critical threats to low-risk activities. The firewall prioritizes addressing the most severe threats immediately and efficiently, ensuring robust security by focusing its efforts where they are needed most. This approach enhances network protection by mitigating high-risk threats promptly while maintaining overall system integrity.

4.6. Challenges

Customizing Next-Generation Firewalls (NGFWs) presents several challenges in balancing security and performance. Enabling all security features can lead to excessive resource consumption, impacting network efficiency. Additionally, configuration complexity, simulation limitations, and ongoing update costs pose obstacles to effective security implementation. This project aims to analyze these challenges and propose solutions to optimize NGFW customization without compromising network performance [24].

- **Challenges faced in the project:**

1. **Complexity of Customization**

   Tailoring firewall functionalities to meet the specific needs of each environment required extensive effort to define precise system requirements.

2. **Simulation Limitations**

   Simulated environments do not fully replicate the complexities of real-world networks, which may impact the comprehensiveness of the results.

3. **Cost of Updates and Maintenance**

   Next-Generation Firewall technologies demand continuous investment in software updates and hardware maintenance to ensure optimal security and performance.

4. **Account Creation Restrictions**

   The inability to create an account with the firewall manufacturer to obtain an activation key resulted in the inability to access certain functionalities.

CHAPTER FIVE

CONCLUSIONS AND RECOMMENDATIONS

5.1. Introduction

This chapter outlines the key conclusions drawn from the project, along with recommendations and potential areas for future research. It highlights the importance of Next-Generation Firewall (NGFW) customization in enhancing network security across different environments while maintaining operational efficiency. The findings emphasize the need for tailored configurations to optimize threat detection and resource utilization. Additionally, recommendations are provided to further improve NGFW performance, and future research directions are suggested to explore advanced security solutions and emerging technologies.

5.2. Conclusions

With the rise of cyber threats, Next-Generation Firewalls (NGFWs) have become essential for network security, but their effectiveness relies on proper customization for different environments. This project aims to enhance NGFW performance by tailoring configurations for cloud, data center, and local network environments, ensuring maximum protection without compromising efficiency. The conclusions highlight that proper customization improves threat detection and optimizes resource utilization, while poor configuration can introduce security vulnerabilities. Therefore, providing a practical framework for NGFW customization is crucial to helping organizations build more secure and reliable digital environments.

This project led to the following key findings:

1. NGFW functions can be customized to achieve an optimal balance between high security performance and network efficiency.
2. The simulations conducted demonstrated the capability of NGFW to enhance data protection and reduce cyberattacks targeting cloud environments, data centers, and local networks.
3. Well-designed customization strategies help reduce resource strain and improve real-time threat response.

Despite the limitations of simulation environments, the project successfully delivered a prototype that can be further developed into an effective cybersecurity management tool.

5.3. Recommendations

This chapter provides recommendations for enhancing NGFW customization in light of the study and analysis conducted, such as leveraging artificial intelligence for automated security policies and improving integration with other security systems. The key conclusions of the study emphasize the importance of balancing security and performance to ensure effective network protection.

1. Enhancing Customization Based on Environment

- Develop software tools that integrate artificial intelligence and machine learning to enable automatic customization of NGFW functions based on the nature of data traffic in each environment (cloud, data centers, local networks) [25].
- Adopt flexible solutions that allow dynamic reallocation without requiring system restarts.

2. For Licensing and Activation of NGFW Functions

To fully utilize the advanced capabilities of the Next-Generation Firewall (NGFW) and ensure optimal security customization, it is essential to acquire the necessary licenses and activation keys from the firewall manufacturer. Many advanced NGFW features, such as intrusion prevention systems (IPS), deep packet inspection (DPI), threat intelligence, and cloud-based security enhancements, require valid subscriptions and licensing agreements.

3. Strengthening Cloud Security

- Activate advanced threat intelligence features to analyze cloud-based threats in real time.
- Implement multi-factor authentication (MFA) systems to ensure secure access to cloud resources.

4. Improving Local Network Efficiency

- Implement network segmentation policies to minimize the risk of threat propagation within local networks.
- Enhance intrusion detection systems (IDS) by integrating them with NGFW.

5. Continuous Education and Training

- Provide ongoing training programs for IT teams on the latest firewall technologies and customization techniques.

- Develop standardized operational guidelines to facilitate NGFW management across different environments.

6. **Conducting Future Studies**

- Expand project to cover more complex environments, such as Internet of Things (IoT) networks and industrial networks.
- Assess the impact of firewall technologies in countering evolving threats, including malicious artificial intelligence.

5.4. Future studies

Next-Generation Firewalls (NGFWs) play a crucial role in strengthening network security, but with the rapid advancement of cyberattack techniques, it is essential to reconsider their functionality and ways to enhance their performance. Future studies open the door to exploring new technologies and innovative methods to improve NGFW efficiency, not only in terms of security but also in their integration with other security systems and ease of management. Upcoming project will also focus on making these systems smarter and more responsive to evolving threats, ensuring that networks remain secure without compromising performance or adding operational complexity [20].

- **The future studies of this project are:**

1. Integrating Next-Generation Firewalls (NGFWs) with artificial intelligence and machine learning technologies to enhance real-time threat detection and response [16].
2. Examining the impact of automating dynamic security policies on reducing operational overhead and improving overall network performance.
3. Analyzing the application of NGFWs in complex environments such as Internet of Things (IoT) networks and Industrial Control Systems (ICS) to address unique security challenges.
4. Exploring the evolution of cyber threats, including AI-driven attacks, and developing effective strategies to counter them using NGFWs.
5. Evaluating the effectiveness of modern encryption technologies when integrated with NGFWs to enhance data protection during transmission and storage.

REFERENCES

[1] Sharma, Himanshu. "Next-Generation Firewall in the Cloud: Advanced Firewall Solutions to the Cloud." *ESP Journal of Engineering & Technology Advancements (ESP-JETA)* 1, no. 1 (2021): 98-111.

[2] Neupane, Kishan, Rami Haddad, and Lei Chen. "Next generation firewall for network security: a survey." In *SoutheastCon 2018*, pp. 1-6. IEEE, 2018.

[3] Patel, Udit. "THE ROLE OF NEXT-GENERATION FIREWALLS IN MODERN NETWORK SECURITY: A COMPREHENSIVE ANALYSIS." *INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN ENGINEERING AND TECHNOLOGY (IJARET)* 15, no. 4 (2024): 135-154.

[4] Saraswat, Yash. "Enhancing the security of a network fabric using firewalls and load balancer." PhD diss., Dublin, National College of Ireland, 2022.

[5] PaloaltoNetworks. (2024, August 5). History of Firewalls. Retrieved from https://www.paloaltonetworks.com/cyberpedia/history-of-firewalls.

[6] Tounsi, Wiem, and Helmi Rais. "A survey on technical threat intelligence in the age of sophisticated cyber-attacks." *Computers & security* 72 (2018): 212-233.

[7] Humanize. (2024, April 19). Next-Generation Firewall (NGFW): Types & Benefits. Retrieved from https://www.humanize.security/blog/cyber-awareness/next-generation-firewall-types-and-benefits.

[8] PaloaltoNetworks. (2024, October 1). The latest ML-Powered NGFWs bring industry-leading performance and security to emerging use cases. Retrieved from https://www.paloaltonetworks.com/network-security/next-generation-firewall-hardware.

[9] Islam, Md Shamimul, Mohammed Asraf Uddin, Dr Md Dulal Hossain, Dr Md Shakil Ahmed, and Dr Md Golam Moazzam. "Analysis and evaluation of network and application security based on next generation firewall." *International Journal of Computing and Digital Systems* 13, no. 1 (2023).

[10] Arefin, Md Taslim, Md Raihan Uddin, Nawshad Ahmad Evan, and Md Raiyan Alam. "Enterprise network: Security enhancement and policy management using next-generation firewall (NGFW)." In *Computer Networks, Big Data and IoT: Proceedings of ICCBI 2020*, pp. 753-769. Springer Singapore, 2021.

[11] Lei, Sun. "Synergizing next-generation firewalls and defense-in-depth strategies in a dynamic cybersecurity landscape." In *International Conference on Computer Network Security and Software Engineering (CNSSE 2024)*, vol. 13175, pp. 143-149. SPIE, 2024.

[12] Lamdakkar, Oussama, Ismail Ameur, Mohamed Mbarek Eleyatt, Fabien Carlier, and Lahcen Ait Ibourek. "*Toward a modern secure network based on next-generation firewalls: recommendations and best practices*." *Procedia Computer Science* 238 (2024): 1029-1035.

[13] Palo-Alto Company. "PAN-OS Administrator's Guide." Subscriptions You Can Use with the Firewall, 68-71, 2024.

[14] Thu, Sai Lwin. "Evaluation of the Next Generation Firewall with Breach and Attack Simulation." In *Conference on Innovative Technologies in Intelligent Systems and Industrial Applications*, pp. 253-271. Cham: Springer Nature Switzerland, 2023.

[15] Rabiul Hasan, Mohammad. "*Safeguarding of Financial Organization from Cyber-Attack using Next Generation Firewall (NGFW), Security Information & Event Management (SIEM) and Honeypot*." PhD diss., Dublin Business School, 2024.

[16] Kallepalli, Karthik, and Umair B. Chaudhry. "*Intelligent Security: Applying Artificial Intelligence to Detect Advanced Cyber Attacks*." In Challenges in the IoT and Smart Environments: A Practitioners' Guide to Security, Ethics and Criminal Threats, pp. 287-320. Cham: Springer International Publishing, 2021.

[17] " Noor, Asim, Noshina Tariq, Farrukh Aslam Khan, and Muhammad Ashraf. "24 Evolution of Next-Generation Firewall System for Secure." *Securing the Digital Realm: Advances in Hardware and Software Security, Communication, and Forensics* (2025): 263.

[18] Brar, Manbir Kaur, Bhupinder Kaur, Gurvinder Singh, Pardeep Kumar Jindal, and Sonal Sood. "Traditional firewall vs. next-generation firewall: A review." In *AIP Conference Proceedings*, vol. 3121, no. 1. AIP Publishing, 2024.

[19] Pavlović, Milan, Marija Zajeganović, and Milan Milivojević. "*Implementation of Next-Generation Firewalls in Modern Networks*".

[20] Bodipudi, Akilnath. "*Effective Firewall Review And Network Optimization by Data-Driven & Holistic approach*." Journal of Technological Innovations 5, no. 2 (2024).

[21] Sozol, Md Shariar, Md Minhazul Islam, Md Mostafizur Rahman, Md Arafath Uzzaman, Md Zamshed, and Golam Mostafa Saki. "*Building an Impenetrable Vault: Advanced Cybersecurity Strategies for Database Servers*." (2024).

[22] Kampa, Thomas, Christian Klaus Müller, and Daniel Großmann. "*Interlocking IT/OT security for edge cloud-enabled manufacturing*." *Ad Hoc Networks* 154 (2024): 103384.

[23] Oudina, Zina, Ahmed Dib, Mohamed Amine Yakoubi, and Makhlouf Derdour. "*Comprehensive Risk Classification and Mitigation in the Petroleum Cyber-Physical Systems of the Oil and Gas Industry*." International Journal of Safety & Security Engineering 14, no. 1 (2024).

[24] Shantilawati, Irma, Jihan Zanubiya, Fajriannoor Fanani, Henrik Jensen, Shofiyul Millah, and Ninda Lutfiani. "*Challenges in securing data and networks from modern cyber threats*." International Journal of Cyber and IT Service Management 4, no. 2 (2024): 88-96.

[25] Chowdhury, Dhiman Deb. "*Innovations in Network Security: Embracing a Security First Approach*." In Future of Networks: Modern Communication Infrastructure, pp. 259-312. Cham: Springer Nature Switzerland, 2025.

[26] Sugunaraj, Niroop, Shree Ram Abayankar Balaji, Barathwaja Subash Chandar, Prashanth Rajagopalan, Utku Kose, David Charles Loper, Tanzim Mahfuz et al. "*Distributed Energy Resource Management System (DERMS) Cybersecurity Scenarios, Trends, and Potential Technologies: A Review*." IEEE Communications Surveys & Tutorials (2025).

[27] Xun, Ang Ting, Lim Alan Zhe En, Lim Tze Shen, Ang Ning Xin, Wong Hee Soon, Wong Zi Jun, Harish Ramachandra et al. "*Building Trust in Cloud Computing: Strategies for Resilient Security*." (2025).

[28] TechTarget. 2024. "*How to Select and Implement a Next-Gen Firewall*." TechTarget SearchSecurity, January 2024. Accessed February 12, 2025. https://www.techtarget.com/searchsecurity/buyershandbook/How-to-select-and-implement-a-next-gen-firewall.

[29] Palo-Alto Company. "*Palo Alto Networks PCNSE Study Guide: Early Access*". Global, 2019.