Network Monitoring System (NMS)

submitted in partial fulfillment of the requirements for the degree of Bachelor of Cybersecurity in Information Technology

By:

Laith Khaled Rashed Alhawamdeh 202110384
Mohammed Ali Mohammed Obeidi 202110003
Thabet Atef Abdulaziz Aliyan 202110869
Cyrine Khalid Hamdan Alhadidi 202110089

Supervisor: Dr. Adeeb Alsaaidah

DEPARTMENT OF CYBERSECURITY
FACULTY OF INFORMATION TECHNOLOGY
AL-AHLIYYA AMMANY UNIVERSITY

Second semester – 2023/2024

Abstract:

Nowadays modern enterprise networks are overwhelmingly complex and large in scale, which means that keeping track of all the devices activities, functionality, performance, status and their incoming and outgoing traffic seems like an impossible task for the network administrator/engineer this is where our Network Monitoring System (NMS) comes in handy, this project aims to implement an all-inclusive system that ensures the networks security by constantly monitoring the networks traffic in real-time which in return helps us to identify any potential security threats and give us an insight of how the network operates, as well as provide us with real-time alerts and detailed reports in which it enables us to take the appropriate action on the spot or can even be used for later review, this system operates seamlessly and efficiently with the help of advanced tools and the implementation of well-known techniques such as anomaly detection (the detection of an unusual behavior) and packet analysis tools, the NMS can effortlessly identify various types of cyber threats such as Distributed Denial of Service (DDoS) attacks for instance, the effectiveness of our system (NMS) was deemed to be valid and successful by putting it to the test and running it on a simulated network, the tests consisted of running simulations of real-life cyber threats that may put our network at risk of being compromised, in this project we will be demonstrating that the system is capable of maintaining the confidentiality, integrity and availability of our networks resources, this documentation will be representing our development process & progress, key features, and evaluation results of the Network Monitoring System, highlighting its potential as an essential tool in the cybersecurity realm and that it can be implemented on modern enterprise networks smoothly and reliably.

Acknowledgements:

We would like to express our deepest gratitude to all those who supported and guided us throughout the course of this project, First and foremost, we extend our sincere thanks to our project supervisor, Dr. Adeeb Alsaaidah, whose invaluable guidance, insights, and encouragement were a key factor in the successful completion of this project, we are also grateful for the faculty members of the Al-Ahliyya Amman University IT department for their continuous support and for providing the necessary resources and facilities, furthermore we would also like to extend our gratitude to the graduation project unit and the discussion committee members in advance.

This project required dedication, commitment and hard work to make it possible and achievable, it truly has been an exciting, eye opening and an insightful experience for all four of us in the team, regardless of the mishaps and unfortunate events that we had to face head on as a team we were able to overcome these struggles together in a collaborative and structured manner, where each member of the team was able to contribute to this project due to the knowledge gained from our competent and extremely knowledgeable lecturers, as this project wouldn't be possible to achieve without their extensive support and expertise throughout our academic journey.

Finally, we have achieved something we are truly proud of, and we look forward to applying the knowledge and skills gained through this experience to future projects.

Table of Contents:

Chapter 1: Introduction 7

1.1. Problem definition....7

1.2. Objectives....7

1.3. Scope....8

1.4. Tools, Apps and Technology....8

1.5. Project outline....9

1.6. Contributions....10

Chapter 2: Literature Review 11

- Site-to-Site VPN....11
- Open Shortest Path First (OSPFv2)....12
- VRRP (Virtual Router Redundancy Protocol)....13
- Snort....15
- Splunk....17
- EtherChannel....18
- VLAN....18
- PAT (stands for Port Address Translation)....19
- GNS3(Graphical Network Simulator-3)....20
- VMware....20
- Using Ubuntu OS on our admins host device....21
- Using Kali Linux OS as our Pen testing host....21

Chapter 3: Network Analysis and Requirements 22

3.1. Introduction....22

3.2. Network Analysis and Requirements....24

Chapter 4: Network Design 33

4.1. General description of proposed network(s)....33

4.2. Topology....41

Chapter 5: Implementation 42

5.1. Installation....42

5.2. Administration and configuration....43

Chapter 6: Quality Analysis and Testing 63

6.1. Test case and methodology....63
6.2. Tools used for testing....63
6.3. Test Results....64
Chapter 7: Conclusions and Future Work 81
7.1 Conclusions....81
7.2 Future Work....82
7.3 Appendices....84

Table of figures:

Figure 3.2.1: Enterprise Network with Minimal Security y measures. 24
Figure 3.2.2: pfSense Firewall Setup I. 26
Figure 3.2.3: Virtual LANs (VLANs) 27
Figure 3.2.4: Network Infrastructure Recovery Strategies. 28
Figure 3.2.5: Intranet and VPN Benefits. 29
Figure 3.2.6: Challenges of Admin Placement at Access Layer. 30
Figure 3.2.7: Considerations for Admin Functions at Core Layer . 31
Figure 3.2.8: Benefits of Admin Placement at Distribution Layer 32
Figure 4.1.1: Main Branch (HQ) . 33
Figure 4.1.2: Main Branch Access Layer . 34
Figure 4.1.3: Main Branch Distribution Layer. 35
Figure 4.1.4: Main Branch Core Layer. 35
Figure 4.1.5: Second Branch (Compromised) . 36
Figure 4.1.6: Second Branch Access Layer 37
Figure 4.1.7: Second Branch Distribution Layer 37
Figure 4.1.8: Second Branch Core Layer 38
Figure 4.1.9: Web server 38
Figure 4.1.10: CIA Triad -. 39
Figure 4.2.1: Complete Network Topology. 41
Figure 5.2.1: PfSense Branch 1 CLI configurations 44
Figure 5.2.2: PfSense Branch 2 CLI configurations. 44
Figure 5.2.3: PfSense Branch 1 web gui portal 45
Figure 5.2.4: PfSense Branch 2 web gui portal 45
Figure 5.2.5: Snort interfaces. 46
Figure 5.2.6: Snort's ruleset. 46
Figure 5.2.7: Snort's rulesets scheduled updates 46
Figure 5.2.8: Snort's rulesets update 47
Figure 5.2.9: Snort's custom rulesets 47
Figure 5.2.10: Snort's IP Lists tab 48
Figure 5.2.11: Snort's Alerts tab 48
Figure 5.2.12: Snort's Alert settings 48
Figure 5.2.13: Snort's Firewall system logs 49
Figure 5.2.14: Snort's blocking rules. 49
Figure 5.2.15: VPN/IPsec configuration in HQ branch. 49
Figure 5.2.16: VPN/IPsec configuration in the second branch). 50
Figure 5.2.17: NAT overload configuration 50
Figure 5.2.18: LAN firewall rules configuration 51
Figure 5.2.19: WAN firewall rules configuration 51
Figure 5.2.20: OPT1 firewall rules configuration. 51
Figure 5.2.21: IPsec firewall rules configuration 52
Figure 5.2.22: OSPF (FRR) configuration. 52
Figure 5.2.23: OSPF configuration. 52

Figure 5.2.24: OSPF interfaces configuration 53
Figure 5.2.25: OSPF area configuration 53
Figure 5.2.26: Splunk's web GUI 53
Figure 5.2.27: Splunk's Home menu. 54
Figure 5.2.28: Splunk's server settings 54
Figure 5.2.29: Splunk's Data input settings. 55
Figure 5.2.30: Splunk's listening port 55
Figure 5.2.31: Pfsense Remote logging option 56
Figure 5.2.32: Splunk's input settings. 56
Figure 5.2.33: Splunk's input settings overview. 57
Figure 5.2.34: Splunk's input settings has been set!. 57
Figure 5.2.35: Splunk's Apps. 58
Figure 5.2.36: Splunk's search and report app. 58
Figure 5.2.37: Splunk's Snort app. 59
Figure 5.2.38: Splunk mobile feature 60
Figure 5.2.39: Splunk mobile feature QR code. 60
Figure 5.2.41: Linked mobile devices list 60
Figure 5.2.42: creating a custom mobile alert 61
Figure 5.2.43: send alerts using splunk mobile feature 62
Figure 5.2.44: Specifying the receiving user. 62
Figure 5.2.45: Specifying the visuals. 62
Figure 6.3.1: PC1 connectivity (1). 64
Figure 6.3.2: PC1 connectivity (2) 65
Figure 6.3.3: PC1 connectivity (3) 65
Figure 6.3.4: PC1 connectivity (4) 66
Figure 6.3.5: PC1 connectivity (5) 66
Figure 6.3.6: PC1 connectivity (5) 67
Figure 6.3.7: Branch 1 VPN/IPsec Setup. 68
Figure 6.3.8: Branch 2 VPN/IPsec Setup. 68
Figure 6.3.9: PC1 Ping to PC5 (Branch 2) 69
Figure 6.3.10: PC5 Ping to PC1 (Branch 1). 69
Figure 6.3.11: PC1 (Branch 1) external connectivity 70
Figure 6.3.11: Kali Linux in the second branch 70
Figure 6.3.12: Pfsense connection with the ISP in HQ 71
Figure 6.3.13: Kali Linux network settings -. 72
Figure 6.3.14: Kali Linux connectivity h. 72
Figure 6.3.15: Wireshark analyzing the ping request 73
Figure 6.3.16: Kali Linux Nmap comands 73
Figure 6.3.17: Snort Alerts. 74
Figure 6.3.18: Wireshark inspection of the TCP scan (1). 74
Figure 6.3.19: Wireshark inspection of the TCP scan (2). 75
Figure 6.3.20: Wireshark inspection of the UDP scan (1). 75
Figure 6.3.21: Wireshark inspection of the UDP scan (2)-. 76
Figure 6.3.22: Splunk search & reporting the intrusion attempt. 76
Figure 6.3.23: Splunk's send to mobile feature. 77
Figure 6.3.24: Admins handheld device (1) 77
Figure 6.3.25: Admins handheld device. 78
Figure 6.3.26: Firewall rules on the pfsense (HQ) interface. 78
Figure 6.3.27: PC1 external connectivity (before firewall rule). 79
Figure 6.3.28: Pfsense blocking firewall rule (1) 79
Figure 6.3.29: Pfsense blocking firewall rule (2). 79
Figure 6.3.30: Pfsense blocking firewall rule (3). 80
Figure 6.3.31: PC1 external connectivity (after firewall rule). 80
Figure 6.3.32: Pfsense blocking firewall rule (4). 81

Chapter 1: Introduction

In today's digital world, the security and the efficiency of network infrastructures are critical for the seamless operation of organizations, with the increasing reliance on digital communication and data exchange, the risk of cyber threats and network performance issues has increased, Network Monitoring Systems (NMS) have become an indispensable tool in the cybersecurity field, providing continuous surveillance of network activities to ensure integrity, availability, and confidentiality of network resources.

1.1. Problem definition

As modern enterprise networks grow in complexity and scale, traditional monitoring methods fall short in detecting advanced cyber threats and monitoring the networks performance effectively, as the absence of real-time monitoring and advanced anomaly detection can lead to severe security breaches that can go past us unnoticed and disrupt our operations, this project aims to address these challenges by developing a robust Network Monitoring System capable of identifying threats and performance issues in real-time.

1.2. Objectives

The primary objective of this project is to design and implement a Network Monitoring System that enhances the security and performance of network infrastructures, in which the objectives include:

- **Real-time monitoring**: in which we're going to develop a system that continuously monitors the networks traffic and the connected devices activities in order to recognize its usual pattern and behavior to gain an understanding of how the network operates and functions.

- **Security breach detecting system**: in which were going to setup an advanced firewall device that can detect and prevent external threats on our internal devices, as well as set up an IDS to identify unusual patterns that indicates a potential security breach or a network malfunction.

- **Alert Mechanism**: Create a real-time alert system that notifies network administrators of detected issues, enabling prompt response.

- **Comprehensive Reporting**: Generate detailed reports to aid in the analysis and resolution of security threats and performance problems.

1.3. Scope

This project focuses on developing and evaluating a Network Monitoring System tailored for small to medium-sized networks, the system's architecture and core components are designed to be scalable, making them applicable to diverse network configurations, the documentation covers the design methodology, implementation details, testing and validation processes, and the overall effectiveness of the NMS in enhancing network security and performance.

1.4. Tools, Apps and Technology

- **GNS3:** is an open-source network software emulator that allows the creation and simulation of a complex network topologies as if they’re running in real life.

- **VMware**: software that enables the creation of virtual machines to run multiple operating systems on a single physical machine in which we’re able to isolate our network simulator (GNS3) from our host device to keep a layer of security.

- **pfSense Firewall:** is an open-source firewall and router software distribution based on FreeBSD.

- **Snort:** is an open-source, free and lightweight intrusion detection system (IDS) software to detect emerging threats.

- **Splunk:** is a powerful platform designed for searching, analyzing, and visualizing machine generated data in real-time.

- **Wireshark:** is a network protocol analyzer that is used for detailed inspection and analysis of network traffic.

- **VPN site-to-site:** site-to-site connection establishes a secure and encrypted link between two or more networks, typically over the internet.

1.5. Project outline

To provide a clear roadmap of the project's documentation, the following outline is presented:

1. **Introduction:** This section of the documentation provides a brief intro about our project which includes; our projects solution to modern problems, objectives and aim, the scope in which the project operates in, a clear outline (roadmap), tools used throughout the project, and how our project contributes in the realm of cybersecurity.

2. **Literature review:** This section of the documentation provides an extensive and detailed review of all the necessary equipment, tools, protocols, technologies, operating systems used in our project in order to create the ideal NMS.

3. **Network analysis and requirements:** This section of the documentation provides a detailed understanding of the current

state of the network (before implementing our NMS and other security measures), in which we identify weak points in our current system and specify the requirements on how we can improve on its security posture and its overall well-being.

4. **Network design:** In this section of the documentation will be providing a topology of our network, and a clear description of our networks structure and what it consists of, and how is it going to be configured to meet our projects requirements and in which we will give a detailed plan on how to implement our NMS along with extra security measures as well as how we're able to satisfy the three major cybersecurity triads CIA.

5. **Implementation:** This section of the documentation provides a clear guide on how we we're able to configure, implement, set up and install the required tools, software and equipment.

6. **Quality analysis and testing:** This section of the documentation provides and outlines our testing plan/strategy used to evaluate the network's performance, functionality, reliability, and security

7. **Conclusion and future work:** In this section of the documentation, we will be providing the configurations implemented on our intermediary devices in the appendices, as well as cover aspects of our projects future plan.

1.6. Contributions

Our project makes several key contributions to the field of cybersecurity:

- **Innovative Anomaly Detection:** Introduces advanced algorithms that enhance the detection of unusual network patterns, improving the identification of potential security threats.

- **Incident response with an alerting system:** An NMS provides real-time alerts for detected threats, enabling security teams to respond quickly to incidents, and alerts can be customized based on severity levels and specific types of threats.

- **Comprehensive monitoring solution:** Develops a robust system that integrates real-time monitoring, alert mechanisms, and detailed reporting, providing a comprehensive approach to network security and performance management.

- **Network auditing and access control:** Monitoring systems can track user access and behavior, ensuring that only authorized personnel have access to sensitive parts of the network, this helps in enforcing and auditing access control policies.

Chapter 2: Literature Review

- **Site-to-Site VPN**

A site-to-site virtual private network (VPN): is a way to connect local area networks (LANs) in multiple locations across the public internet, in which it allows employees in different sites to securely share resources and information by encrypting the shared resource with a robust encryption algorithm as its transferred across the medium which ensures the **confidentiality** of our resources, this technology is often used by businesses or government agencies with multiple offices.

❖ **The primary benefits and uses of Site-to-Site VPN:**

Enhanced data security:

The primary benefit of a site-to-site VPN is data security, as information travels between the gateways, it is encrypted, that means that if data is intercepted by an unauthorized user while in transit between sites, it will be visible to them only as an indecipherable code.

 Streamlined resource sharing:

A site-to-site VPN enables employees in locations around the world to communicate, share resources, and securely access sensitive data, it's an excellent solution for keeping a dispersed workforce connected and productive, as long as everyone has access to the sites where the VPN gateways are established.

 Easy onboarding:

One benefit of this system is that it doesn't rely on a client/server model, instead of requiring all users on a corporate network to install specific client software on their devices, they can just connect to the VPN gateway instead, as well as using a non-client model also helps in the rare cases where particular operating systems and devices aren't compatible with VPN software.

- **Open Shortest Path First (OSPFv2)**

Open Shortest Path First Version 2 (OSPFv2): is a link-state routing protocol that uses link-state advertisements (LSAs) to update neighboring routers about a router's interface and routing info, each router maintains an identical area-topology database to determine the shortest path to any neighboring router.

❖ **The primary benefits and uses of OSPFv2:**

 Fast Convergence:

OSPFv2 quickly propagates routing changes across the network, allowing for rapid adaptation to network topology changes and ensuring minimal downtime.

 Scalability:

OSPFv2 can scale efficiently in large and complex networks by dividing them into smaller areas, this reduces routing overhead and enhances performance.

Load Balancing:

OSPFv2 supports Equal-Cost Multi-Path (ECMP), enabling load balancing across multiple paths with equal cost, thus improving bandwidth utilization and redundancy.

Enterprise Networks:

OSPFv2 is commonly used in enterprise networks to manage internal routing due to its scalability, fast convergence, and hierarchical design.

- **VRRP (Virtual Router Redundancy Protocol)**

VRRP (Virtual Router Redundancy Protocol): is a networking protocol that provides automatic backup capability for routing functions in a local area network (LAN), it allows for multiple routers on a LAN to work together in a virtual group, presenting a single virtual router as a default gateway to the hosts on the LAN.

❖ **Why VRRP instead of GLBP or HSRP**

Use Case Alignment

In small to medium networks VRRP is particularly well-suited for small to medium-sized networks where high availability is essential, but load balancing is not a primary concern, in scenarios where network stability and reliability are critical, and additional load balancing is unnecessary or handled elsewhere, VRRP is often the preferred choice, similar to HSRP.

 Simplicity:

VRRP is generally easier to configure and manage compared to HSRP and GLBP, it has a straightforward setup where one router is elected as the master and the others as backups, VRRP focuses only on redundancy without the added complexity of load balancing (like GLBP) or some of the hassle of tracking interfaces (as with HSRP), making it simpler to implement and troubleshoot.

 Reliability and Predictability:

VRRP has a clear, predictable failover process where the master router is the only active router until a failure occurs, similar to HSRP. This can make network behavior more predictable compared to GLBP's load-balancing approach.

 Network Simplicity and Performance:

a single active router handling the traffic, network paths are more consistent in VRRP and HSRP, potentially leading to lower latency and more predictable network performance compared to GLBP's load-balancing approach.

- **PfSense**

pfSense: is an open-source firewall and router software based on FreeBSD, a Unix-like operating system, it is known for its powerful features, flexibility, and ease of use, making it a popular choice for network security and routing needs.

❖ **The primary benefits and uses of pfSense:**

 Flexibility:

pfSense offers a high degree of flexibility, allowing users to customize and extend its functionality according to their specific requirements, whether you need basic firewall capabilities or more advanced security features like

Intrusion Prevention Systems (IPS) and Intrusion Detection Systems (IDS), pfSense can adapt to meet your needs, additionally, its modular architecture allows for easy integration of additional features and enhancements, making it suitable for a wide range of use cases.

Open Source:

Being open source and freely available for use pfSense provides several benefits, which can significantly reduce costs compared to proprietary firewall solutions, furthermore, the open-source nature encourages community collaboration, leading to continuous improvement and innovation in the software.

Active Community and Support:

pfSense benefits from a large and active community of users and developers who contribute to its development, provide support, and share knowledge, the availability of comprehensive documentation, including tutorials, technical guides, and troubleshooting resources, makes it easier for users to deploy and maintain pfSense effectively, additionally the pfSense support forum serves as a valuable resource for getting assistance, troubleshooting issues, and engaging with other users, furthermore, paid support options are available for organizations that require additional assistance or prefer professional support services.

- **Snort**

Snort: is an open-source network intrusion detection system (NIDS) and intrusion prevention system (IPS) developed by Cisco. It is widely used for network monitoring due to its powerful features and flexibility.

❖ **The importance of Snort:**

Intrusion Detection and Prevention:

- Real-Time Monitoring: Snort can analyze network traffic in real-time, identifying potential threats and attacks as they occur.

- Signature-Based Detection: Snort uses a comprehensive set of pre-defined rules (signatures) to detect known threats, such as malware, exploits, and unauthorized access attempts.

- Anomaly-Based Detection: It can also detect unusual patterns in network traffic that may indicate new or unknown threats, helping to identify zero-day attacks.

Comprehensive Rule Set:

- Flexible Rule Language: Snort's rule language is powerful and flexible, allowing users to write custom rules tailored to their specific network environment and security needs.

- Community and Official Rule Sets: Snort has extensive rule sets maintained by the community and by Cisco's Talos Intelligence Group, which are regularly updated to include the latest threat signatures

Versatility:

- Multiple Operating Modes: Snort can operate in different modes:

    1. Sniffer Mode: Captures and displays network packets in real-time.

    2. Packet Logger Mode: Logs packets to disk for later analysis.

    3. Network Intrusion Detection System Mode: Monitors network traffic and applies rules to detect and alert on suspicious activity

- Deployment Flexibility: Snort can be deployed on various platforms, including Linux, Windows, and macOS, making it suitable for diverse network environments

Detailed Logging and Alerts:

- Comprehensive Logging: Snort provides detailed logs of detected events, including information about the source and destination IP addresses, ports, and payload data, which are crucial for forensic analysis and incident response.

Cost-Effective:

- Open Source: As an open-source tool, Snort is free to use, which makes it a cost-effective solution for network monitoring and intrusion detection.
- Active Community Support: The active open-source community around Snort provides extensive documentation, support, and regular updates, contributing to its reliability and effectiveness.

- **Splunk**

Splunk: is a powerful platform widely used for searching, monitoring, and analyzing machine-generated big data via a web-style interface. It is particularly effective for network monitoring due to its robust features and capabilities.

❖ **The use of Splunk**

Data Ingestion and Indexing:

- Real-Time Data Ingestion: Splunk can ingest data from a wide variety of sources in real-time, including logs, metrics, events, and network traffic.

- Universal Data Parsing: Splunk's ability to handle data in various formats (e.g., CSV, JSON, XML) allows it to integrate seamlessly with numerous data sources.

Search and Analysis:

- Powerful Search Language (SPL): Splunk's Search Processing Language (SPL) enables users to search and query their data with precision, providing powerful data analysis capabilities.

- Event Correlation: Splunk can correlate events from different sources, helping identify patterns and relationships within the data, which is crucial for troubleshooting and incident response.

Dashboards and Visualization:

- Custom Dashboards: Users can create custom dashboards to visualize data through charts, graphs, and tables, providing a clear and intuitive view of network performance and issues.

- Real-Time Visualization: Splunk offers real-time visualizations, allowing users to monitor network performance and anomalies as they occur.

Alerting and Notifications:

- Real-Time Alerts: Splunk can generate real-time alerts based on predefined conditions or thresholds, helping network administrators respond to issues promptly.

- Customizable Notifications: Alerts can be configured to trigger notifications via various channels, such as email, SMS, or third-party integrations (e.g., Slack, PagerDuty).

- **EtherChannel with LACP**

EtherChannel is a Cisco technology that combines multiple physical Ethernet links into a single logical link, enhancing network performance and reliability. When used with the Link Aggregation Control Protocol (LACP), EtherChannel provides:

- **Increased Bandwidth**: Aggregates bandwidth from multiple links, e.g., four 1 Gbps links become a 4 Gbps link.
- **Load Balancing**: Distributes traffic across member links based on criteria like IP addresses or port numbers, preventing bottlenecks.
- **Redundancy and High Availability**: Ensures continuous connectivity by automatically redistributing traffic if a link fails.

LACP, an IEEE standard, offers interoperability with various vendors, dynamic link management, and flexible configuration modes, making EtherChannel a versatile and reliable solution for network optimization

- **VLAN**

Virtual LAN (VLAN): is a logical network that segments devices within a physical network, allowing administrators to group devices together based on logical criteria rather than physical location or connection. VLANs provide isolation and segmentation of network traffic, enhancing security, performance, and manageability.

❖ **Why We Use VLANs:**

 Performance Improvement:

By breaking up broadcast domains and isolating traffic, VLANs can improve network performance by reducing unnecessary traffic seen by devices.

 Security and Privacy:

VLANs enhance security by controlling access between groups of devices, allowing administrators to restrict communication between different VLANs based on security policies.

 Cost Reduction:

VLANs enable the creation of multiple logical networks on a single physical switch, reducing the need for additional hardware and infrastructure.

- **PAT (stands for Port Address Translation)**

Definition:

Port Address Translation (PAT), also known as NAT overload, is a method used in network address translation (NAT) to map multiple private IP addresses to a single public IP address by using different port numbers.

Advantages:

Conservation of public IP addresses:
PAT allows organizations to use fewer public IP addresses by multiplexing multiple private IP addresses behind a single public IP address.
Increased security:
By hiding the private IP addresses of devices behind a single public IP address, PAT helps

GNS3(Graphical Network Simulator-3)

Introduction:
GNS3, standing for Graphical Network Simulator-3, is a widely utilized network simulation platform renowned for its capacity to design, simulate, and analyze intricate network topologies within a virtual environment. This review delves into the various aspects of GNS3, highlighting its features, architecture, applications, community support, and future prospects.

Features of GNS3:

GNS3 boasts an array of features catering to network professionals and enthusiasts alike. Its emulation capability extends to a diverse range of network devices from multiple vendors, including routers, switches, and firewalls. Moreover, it supports a plethora of network protocols and technologies, facilitating comprehensive network modeling and analysis.

VMware

Introduction:
VMware has emerged as a leading provider of virtualization and cloud computing solutions, revolutionizing the way organizations deploy, manage, and scale their IT infrastructure. This literature review explores the key facets of VMware, delving into its history, technology stack, applications, impact on the industry, and future prospects.

Applications and Use Cases:

VMware's solutions find widespread application across diverse industries and use cases. From virtualizing data center environments to enabling hybrid and multi-cloud deployments, VMware's products cater to the needs of enterprises, service providers, and SMBs alike. Use cases include server consolidation, disaster recovery, desktop virtualization, and application modernization.

- **Using Ubuntu OS on our admins host device**

Security Posture:
Security is a top priority for system administrators, and Ubuntu's commitment to security is evident in its proactive approach to vulnerability management, timely security updates, and robust security features. With features like AppArmor, UFW (Uncomplicated Firewall), and secure defaults, Ubuntu provides a solid foundation for building secure and resilient IT infrastructures.

Adoption in the Enterprise:
Ubuntu's popularity among system administrators is reflected in its widespread adoption across enterprise organizations, educational institutions, government agencies, and non-profit organizations. Its affordability, scalability, and comprehensive support options make it an attractive choice for organizations seeking a reliable, cost-effective, and sustainable IT infrastructure solution.

- **Using Kali Linux OS as our Pen testing host**

❖ Using Kali Linux as a penetration testing (pen testing) host provides several advantages due to its specialized tools and environment tailored for ethical hacking and security testing purposes:

Comprehensive Toolset: Kali Linux comes pre-installed with numerous penetration testing tools, such as Metasploit, Nmap, Wireshark, Burp Suite, and many others. These tools enable a wide range of security assessments, from network scanning and vulnerability analysis to web application testing and wireless network auditing.

Ease of Use: Kali Linux is designed to be user-friendly for penetration testers and security professionals, with a menu-driven interface and organized tool categories. This facilitates efficient testing workflows and reduces the time required for tool setup and configuration.

Chapter 3: Network Analysis and Requirements

3.1. Introduction

In this section of the documentation, we will be demonstrating our current network (the humble beginning of our network), in which we will be briefly discussing the requirements needed to improve our network from the point of view of a network administrator, in which we will be gradually improving on it to make it the ideal setting/environment to implement our Network Monitoring System (NMS) and prove its importance in today's networks.

To begin with the network administrator is handed the crucial role in ensuring the smooth operation, security, and efficiency of computer networks within an organization amongst many other roles and tasks which include;

1. **Network Maintenance and Monitoring:**

- **Monitoring Performance:** regularly monitoring network performance and ensuring optimal operation of network devices such as routers, switches, firewalls.

- **Troubleshooting:** identifying and resolving network issues, including connectivity problems, slow performance, and network outages.

2. **Network Security:**

- **Firewall and Security Management:** configuring and managing firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS) and VPNs.

3. **Network Planning and Design:**

- **Designing Networks:** Designing network layouts, including physical and logical configurations, to ensure scalability, reliability, and efficient use of network resources.

- **Future Planning:** planning future network needs and planning for network expansion or upgrades to accommodate growth and new technologies.

4. Configuration and Installation:

- **Device Configuration:** Configuring network devices such as routers & switches according to organizational needs and best practices.

5. Documentation and Reporting:

- **Network Documentation:** Maintaining accurate documentation of network configurations, diagrams, policies, and procedures for reference and compliance purposes.

- **Reporting:** Generating reports on network performance & security incidents,

6. Disaster Recovery and Backup:

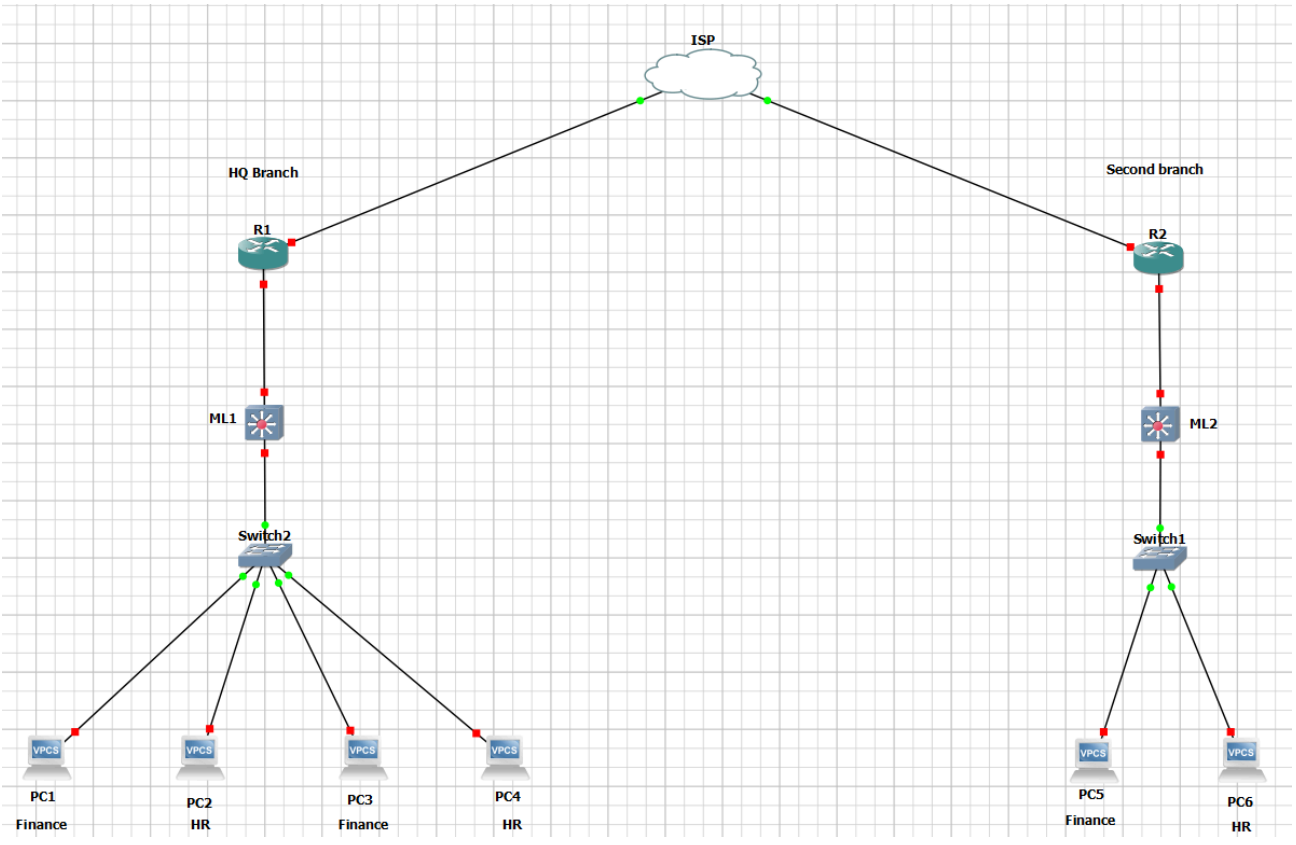
- **Backup Strategies:** Implementing and maintaining network backup strategies to ensure data integrity and recovery in case of hardware failure, natural disasters, or cyber-attacks.

In our case the network administrator was supplied with a simplified diagram of a network topology of a small to medium enterprise network that consists of 2 branches; Headquarters (HQ) branch and a branch office (Second Branch) in which he/she was instructed to take the appropriate measures to ensure the security of the 2 branches and what better way is

there to ensure its security other than being able to monitor the devices activities and implementing the proper tools and configurations to achieve that.

3.2. Network Analysis and Requirements

- The following diagram/topology represents the enterprises network with minimal to no security on the network and its operations:



- As we can see here in figure [3.2.1], we are presented with 4 Virtual PCs (to simulate a functional device of the organization) that are all connected to 1 switch which is then connected to a multilayer switch which is then connected to a router that enables the devices in the LAN network in the HQ branch to communicate with the LAN network in the second

branch through the internet (ISP) which is an unsafe method of communication between the two branches in which we will be discussing later in the documentation.

❖ Our main concerns:

1. **Unauthorized access:**

   At the first glance, we realize that there is no implementation of an IDS/firewall device that prevents any external unauthorized access into the network.

2. **VLANs:**

   we realize that the devices that operate in different offices share the same switch without proper segmentation (the use of VLANs)

3. **Recovery plan:**

   we realize that there is no recovery plan in case of bottlenecks, or a single point of failure on any of the intermediary devices (switch, multilayer switch & router) in which the network is going to suffer a severe downtime in case a SPF occurs.

4. **Method of communication:**

   we realize that the method of communication between the two branches is through the internet rather than an intranet connection.

5. **Proper administration:**

   we realize that we are lacking an administrator pc that is able to monitor the branch he/she is located on and the remote branch.

❖ The requirements to tackle these concerns:

1. Unauthorized access:

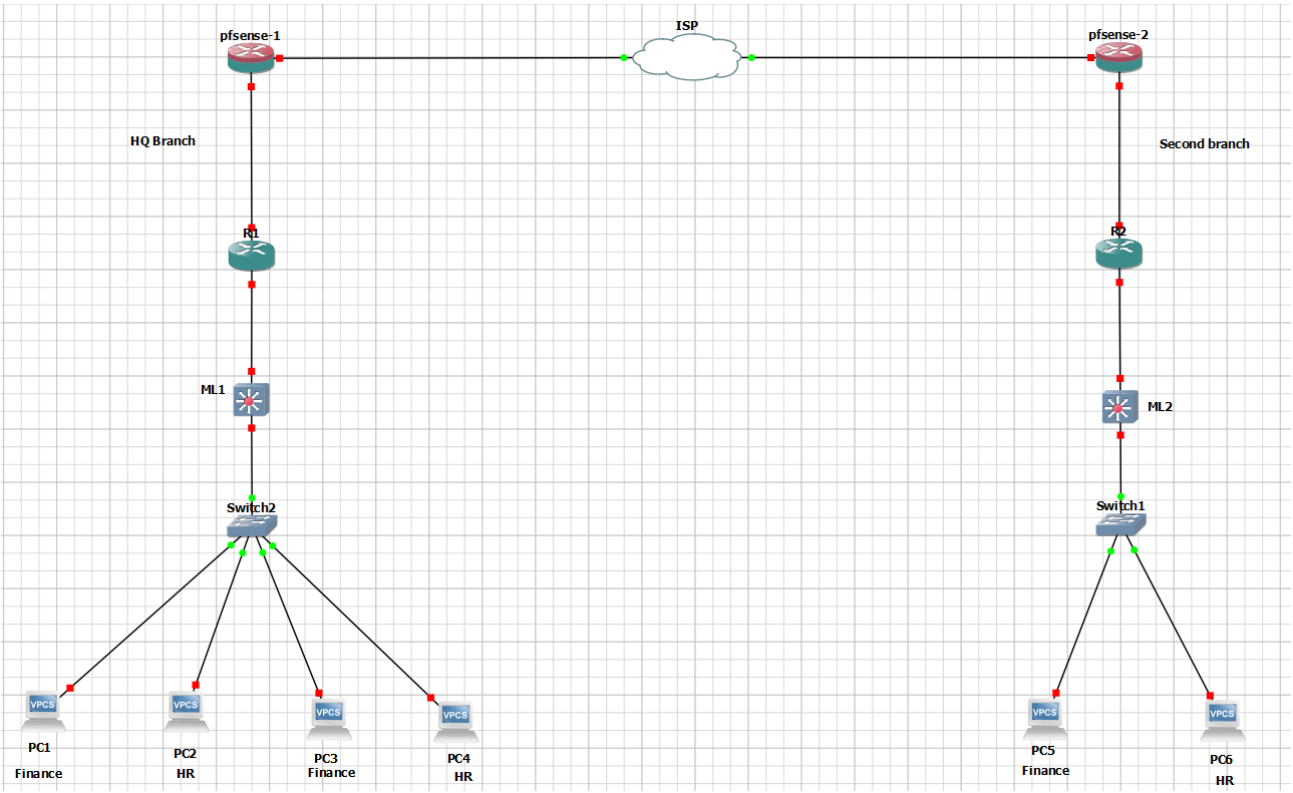


***Figure 3.2.2**: pfSense Firewall Setup - Diagram showing the setup of a pfSense firewall/router with integrated services including firewall rules, IDS (Snort), VPN site-to-site, NAT, and OSPF configuration through a Web GUI.*

- Our initial step was to setup a pfsense firewall/router, which offered us multiple features and capabilities, in which this powerful opensource appliance allowed us to integrate multiple services and features all in one device such as; applying firewall rules, an IDS

software (Snort), it also allowed us to setup a VPN site to site between the two branches, as well as setting up NAT (Network Address Translation) for our local devices (private network) in case they wanted to access the public internet, it also offered us a package which was easily accessible and downloadable which was called FRR which it enabled us to configure routing protocols such as OSPF, where all these configurations was done through a Web GUI.

- The approach we took in order to restrict unauthorized access from external threats was to configure the appropriate firewall rules.

- The second approach was to enable the IDS (snort) to detect any intrusion attempts.

2. VLANs:

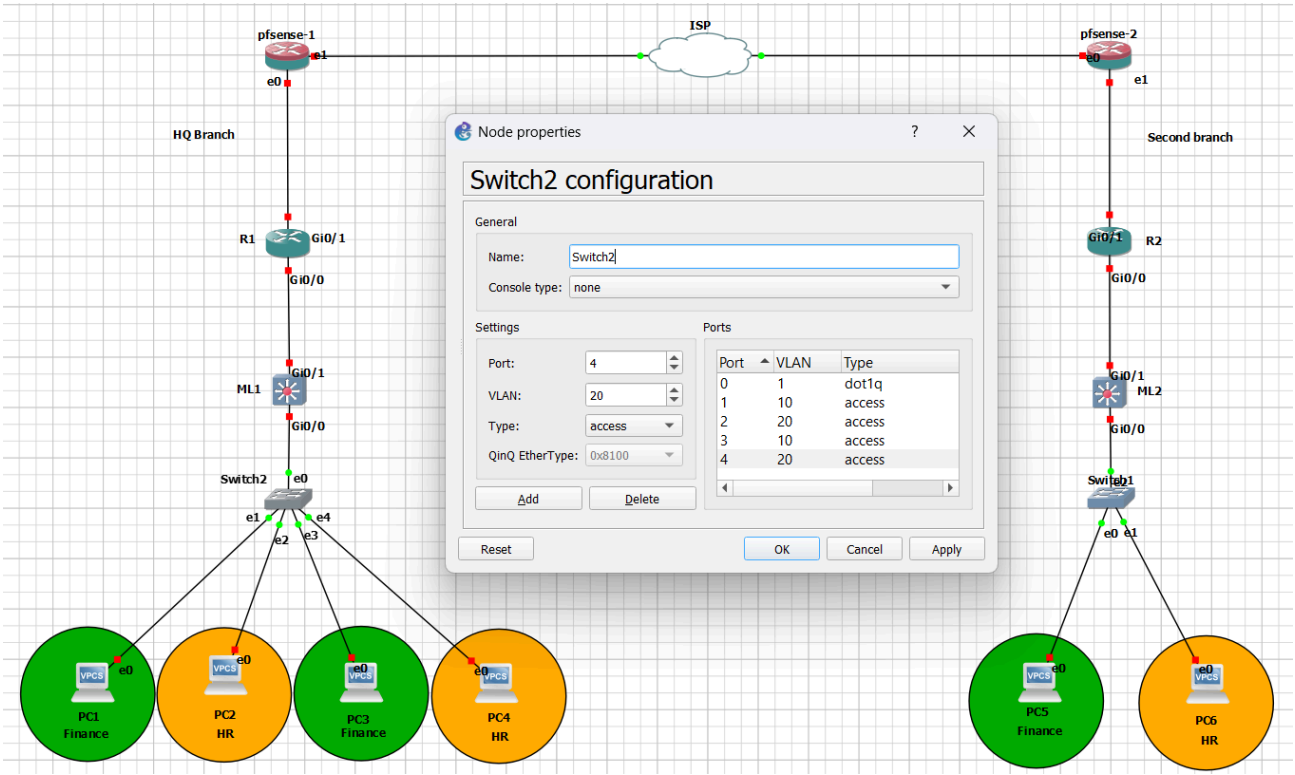


Figure 3.2.3: *Virtual LANs (VLANs) - Diagram illustrating the benefits of VLANs in enhancing security, optimizing performance, and separating data and resources within an organization's network.*

- Virtual LANs (VLANs) play a crucial role in modern network architecture by providing significant benefits in terms of security, performance enhancement, data separation, management efficiency, and operational flexibility across various departments within organizations.

- Firstly, VLAN implementation enhances security by logically segmenting a physical network into multiple virtual networks, this segmentation restricts the broadcast domain, reducing the scope of potential attacks such as eavesdropping, by isolating sensitive data or systems within dedicated VLANs, organizations can mitigate the risk of unauthorized access.
- Secondly, VLANs contribute to performance enhancement by optimizing network traffic flow, by grouping devices with similar communication requirements into the same VLAN, network administrators can prioritize traffic and allocate bandwidth more effectively, which reduces congestion ensuring that critical services receive the necessary resources for optimal performance.
- Moreover, VLANs facilitate separation of data and resources, allowing different departments or user groups to operate independently within their respective VLANs.

3. Recovery plan:

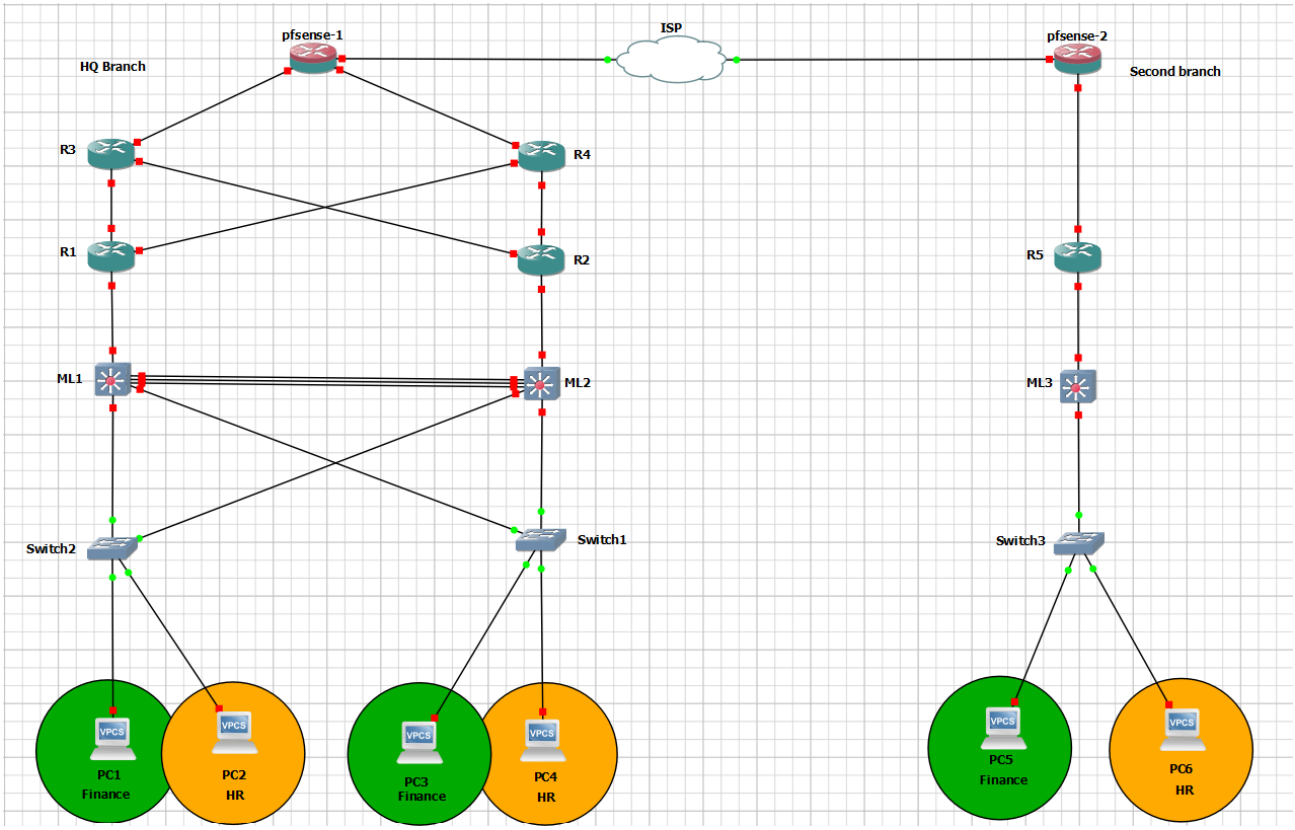


Figure 3.2.4: *Network Infrastructure Recovery Strategies - Diagram depicting the implementation of EtherChannel, VRRP, and device redundancy to enhance network availability and resilience.*

- Implementing a robust recovery plan for network infrastructure involves several strategies to ensure high availability and resilience, in our setup, we focused on EtherChannel, VRRP (Virtual Router Redundancy Protocol), and redundancy across devices to achieve these goals.

- EtherChannel was setup to aggregate (join) multiple physical links between switches into a single logical link, which increases bandwidth and providing redundancy in case of link failures, this configuration ensures that even if one link goes down, traffic can seamlessly continue through the remaining links, minimizing downtime and maintaining network stability.
- VRRP was implemented to establish a virtual IP address those multiple routers can share, this protocol enables one router to act as the master while others remain in standby mode, in case the master

router fails, a standby router takes over, ensuring continuous availability of network services without interruption.

- Redundant devices play a crucial role in our strategy by ensuring that critical network components have backups ready to take over in case of hardware failures or maintenance.

- It's important to note that our secondary branch, designated primarily for testing purposes, in which we did not have a recovery plan implemented.

4. Method of communication:

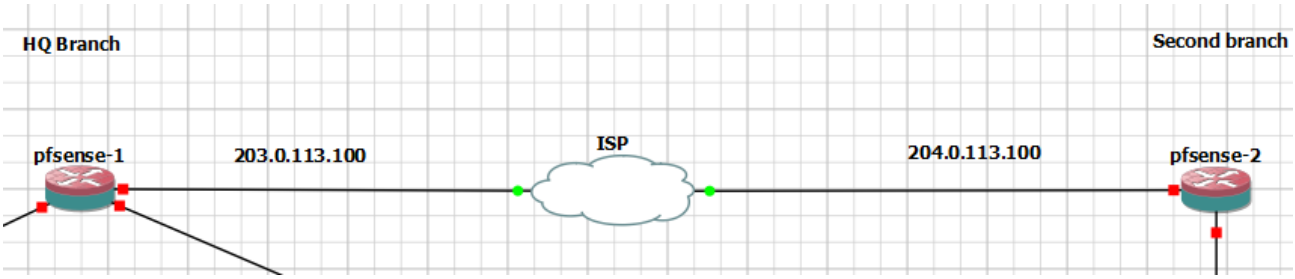


Figure 3.2.5: *Intranet and VPN Benefits - Overview highlighting the enhanced security, reliability, cost efficiency, and management benefits of using VPNs for branch-to-branch communication within an intranet setup.*

- **The difference between the internet vs intranet:** The internet is a global public network allowing universal access and communication but exposes data to external threats, as for intranets we setup private networks within organizations, which offers secure communication and resource sharing among authorized users, ensuring data confidentiality.

- **Using the intranet for branch-to-branch communication by using VPNs (virtual private networks provides:**

  - **Enhanced Security:** Internal security measures like encryption and access controls protect data from breaches and unauthorized access.
  - **Reliability:** Intranet communication offers faster, more reliable connectivity compared to the internet, crucial for efficient business operations.

- **Securing Communication:** Encrypting data over the internet ensures confidentiality and protects against unauthorized access.
- **Cost Efficiency:** Utilizing the internet for VPN connections reduces costs compared to dedicated lines.
- **Integration and Management:** VPNs integrate branch networks into a unified infrastructure, simplifying management and ensuring consistent security policies.

5. Proper administration (the Do's and Don'ts):

Why you shouldn't place the admin in the access layer:

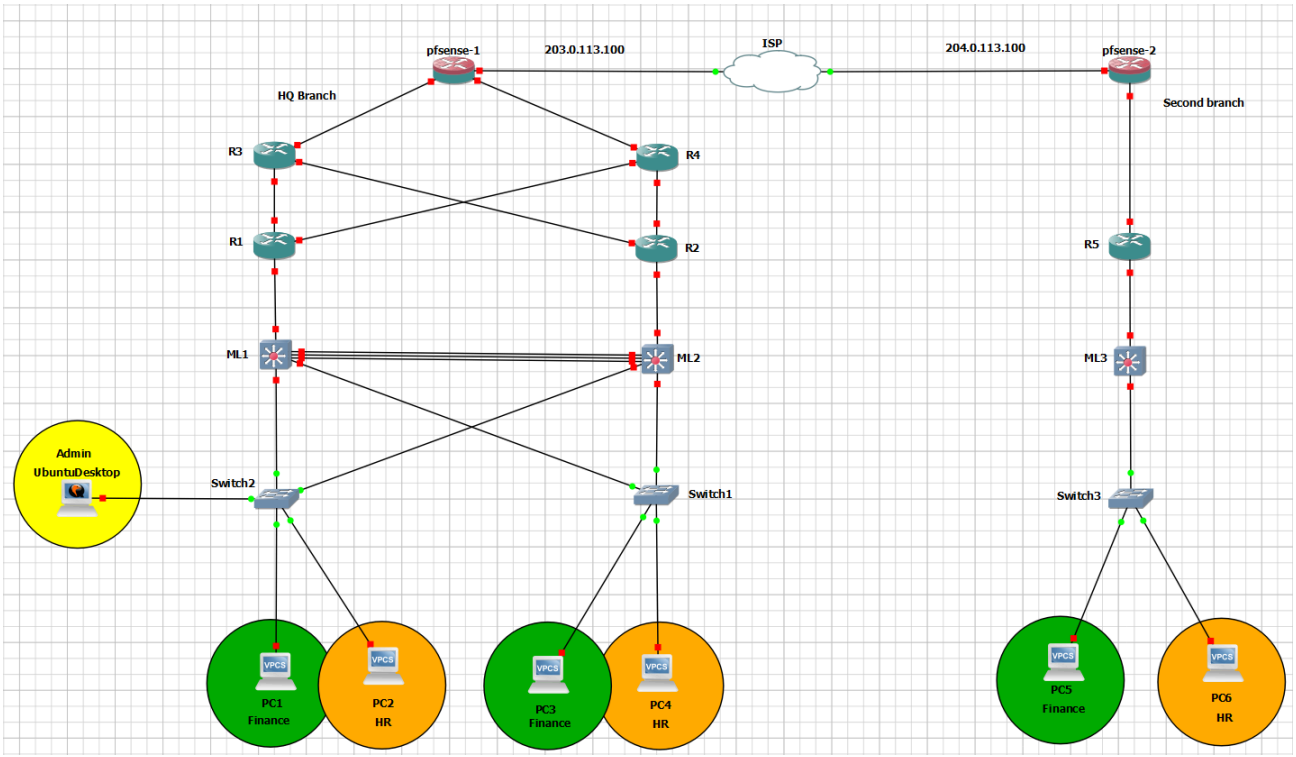


Figure 3.2.6: Challenges of Admin Placement at Access Layer - Diagram illustrating the limited visibility, security concerns, and scalability issues associated with placing administrative functions at the access layer of the network.

- **Limited Visibility:** The access layer primarily handles end-user devices and local traffic. Placing the admin here restricts visibility to only local branch traffic and does not provide oversight of traffic between branches or beyond the local network.
- **Security Concerns:** Access layer switches are vulnerable to physical access and attacks from local devices. Placing admin functions here

increases the risk of unauthorized access to monitoring tools or sensitive administrative controls.

- **Scalability Issues:** Access layer switches are typically numerous and spread across multiple locations. Managing administrative tasks across these dispersed devices can be inefficient and complex.

Why you shouldn't place the admin in the core layer:

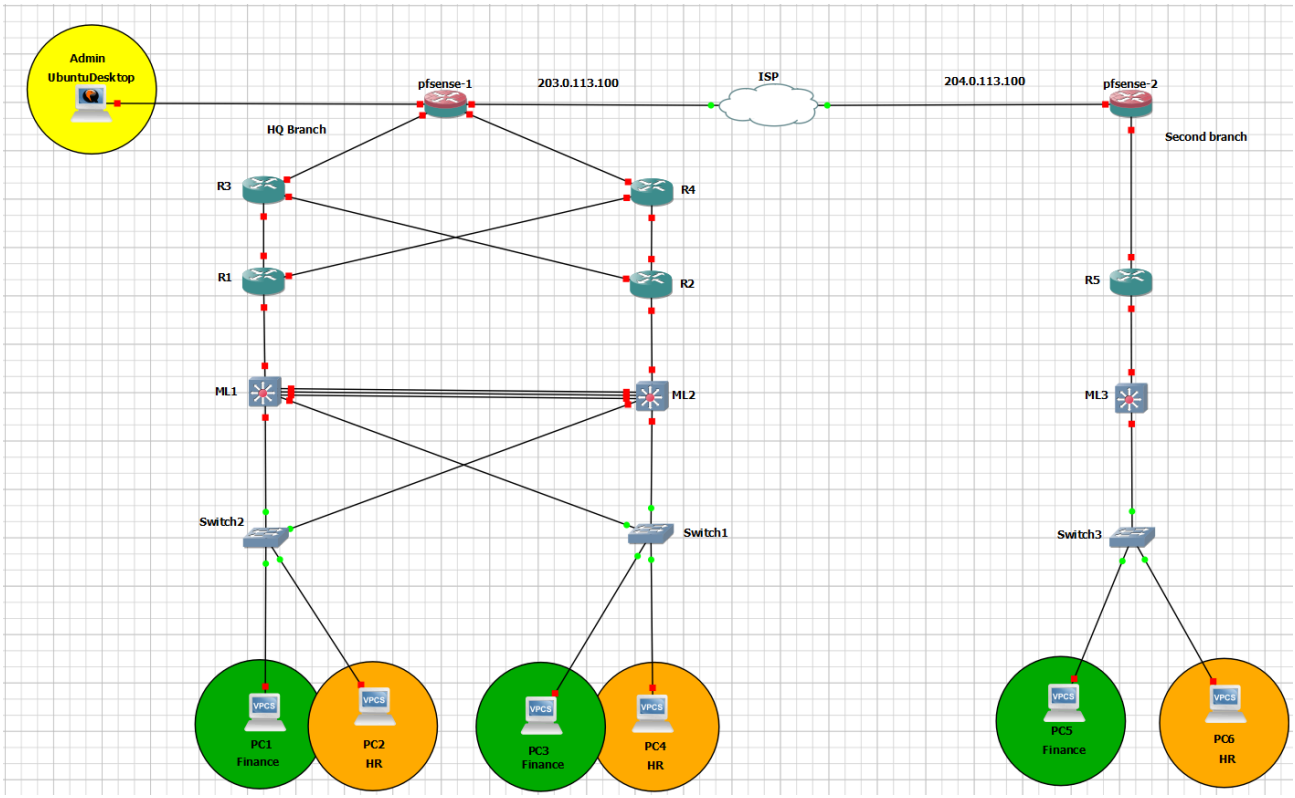


Figure 3.2.7: Considerations for Admin Functions at Core Layer - Diagram highlighting concerns such as traffic congestion, security risks, and lack of granularity when placing administrative functions or monitoring tools at the core layer of the network.

- **Traffic Congestion:** The core layer is optimized for high-speed packet forwarding and minimal latency. Introducing administrative functions or monitoring tools here could impact performance by adding processing overhead and potentially causing congestion in critical data paths.
- **Security Risks:** Core layer devices are critical to network operations and should be dedicated to efficient data forwarding. Placing admin functions here exposes monitoring tools and administrative controls to the same high-speed traffic environment, increasing the risk of security breaches or disruption.

- **Lack of Granularity:** Core layer switches typically operate at a high level, focusing on routing and switching functions. They lack the granularity required for detailed traffic monitoring and specific administrative controls at the branch level.

Why you should place the admin in the distribution layer (the ideal placement):

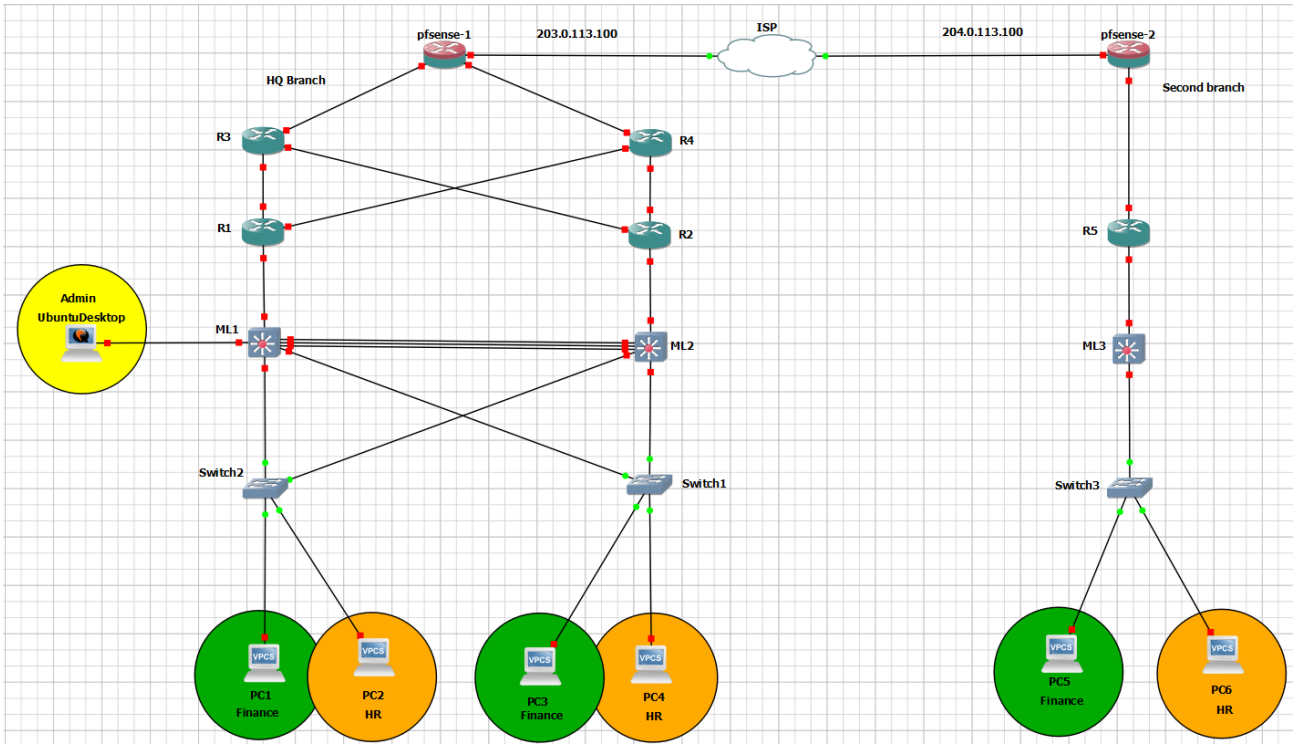


Figure 3.2.8: *Benefits of Admin Placement at Distribution Layer - Diagram illustrating the advantages of placing administrative functions at the distribution layer, including comprehensive visibility, improved security and control, efficient management,*

- **Comprehensive Visibility:** The distribution layer aggregates traffic from multiple access layer switches and provides a centralized point for monitoring. Placing admin functions here allows visibility into local branch traffic as well as traffic between branches via WAN connections.
- **Security and Control:** The distribution layer offers a balance between security and accessibility. It allows administrators to implement and enforce network-wide policies, monitor traffic flows, and apply security measures effectively across all branches.

- **Efficient Management:** By placing admin functions in the distribution layer, administrators can centrally manage monitoring tools, configure network policies, and troubleshoot issues across multiple branches. This centralization improves efficiency and reduces operational overhead compared to managing admin tasks separately at each access layer.
- **Scalability and Flexibility:** The distribution layer is designed to handle both local and inter-branch traffic efficiently. It scales well with organizational growth and adapts to changes in network topology or administrative requirements without compromising performance.

Chapter 4: Network Design

4.1. General description of proposed network(s)

In this section of the documentation, we will be describing our network in the terms of the hardware, software, and tools used in our network in order to demonstrate an efficient implementation of our Network Monitoring System on a well-adjusted environment and how were able to satisfy the 3 major cyber security triads (CIA) after implementing our NMS.

- **HQ branch:**

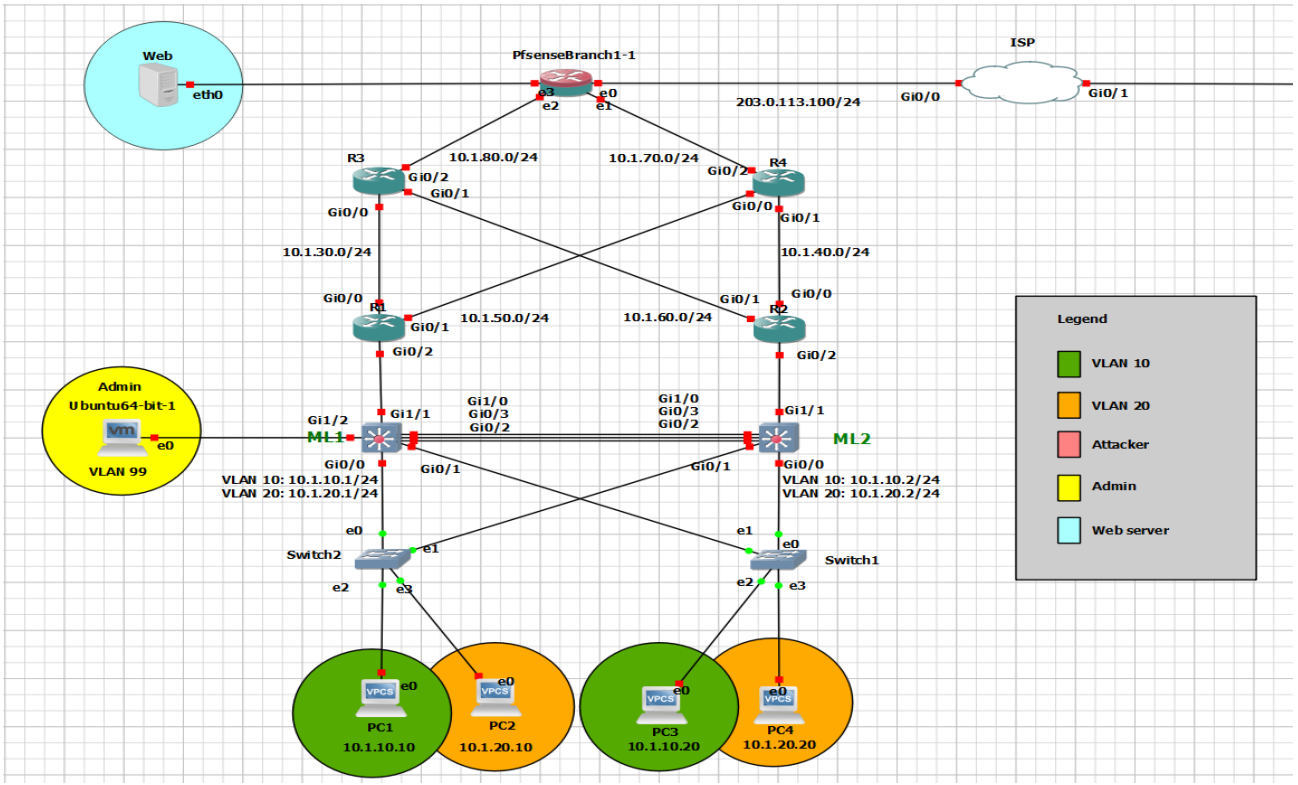


***Figure 4.1.1**: Main Branch (HQ) - Diagram of the main headquarters branch, highlighting key components and structure*

- 4x VPCS
- 2x Switches
- 2x Multilayer-switches
- 4x Routers
- 1x Pfsense (firewall & router)
- 1x Admin Virtual Machine (running on Ubuntu)
- 1x Web server

❖ HQ branch's access-layer:

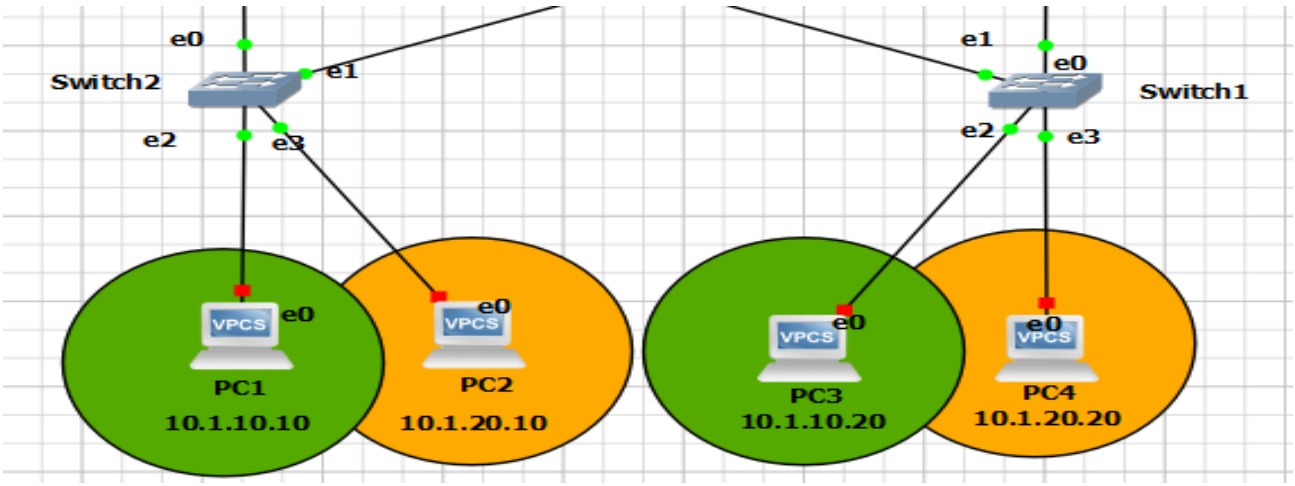


Figure 4.1.2: *Main Branch Access Layer - Detailed view of the access layer in the main branch, showing connections to end devices.*

- We used 4 VPCs and 2 switches.

- we setup 4 virtual PCs which are used to simulate real devices functionality in a simplified manner which reserves CPU utilization on our running device, in which PC1 & PC3 belong to VLAN 10, whereas PC2 & PC4 belong to VLAN 20.

- In which PC1 & PC2 are connected on a switch (Switch 2) using access mode, whereas PC3 & PC4 are connected on a separate switch (Switch 1).

❖ HQ branch's distribution-layer:

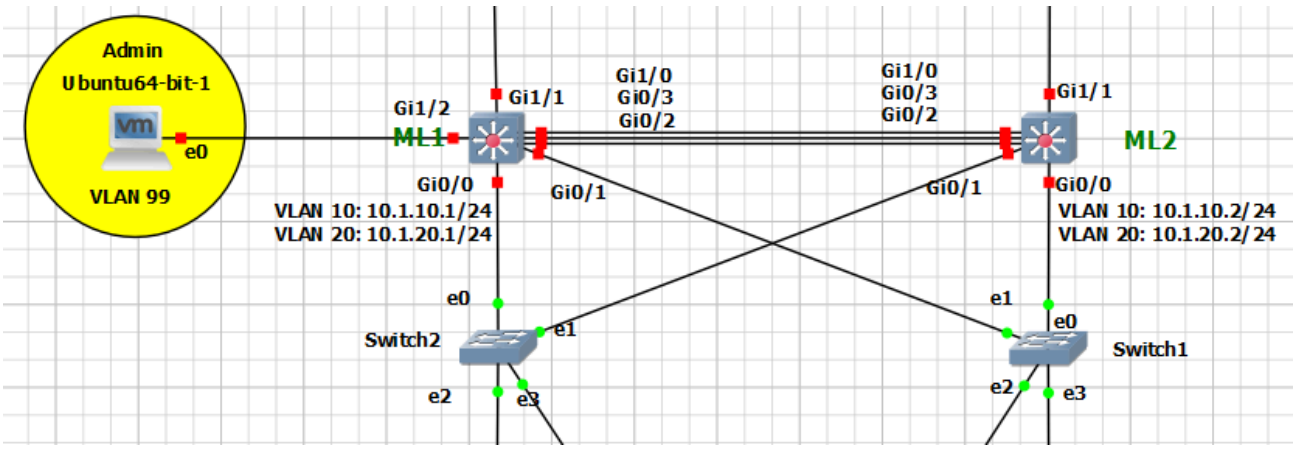


Figure 4.1.3: *Main Branch Distribution Layer - Diagram of the distribution layer in the main branch, illustrating intermediary network devices.*

- We used 2 multi-layer switches (ML1 & ML2) which are connected with one another using 3 interfaces that are used to implement EtherChannel technology between them.

- The distribution-layer is connected to the access-layer by connecting each of the multi-layer switches with each of the bottom switches (in the access-layer) using trunk mode.

- We setup the admins PC in the distribution-layer by connecting it with the multi-layer switch (ML1).

❖ HQ branch's Core-layer:

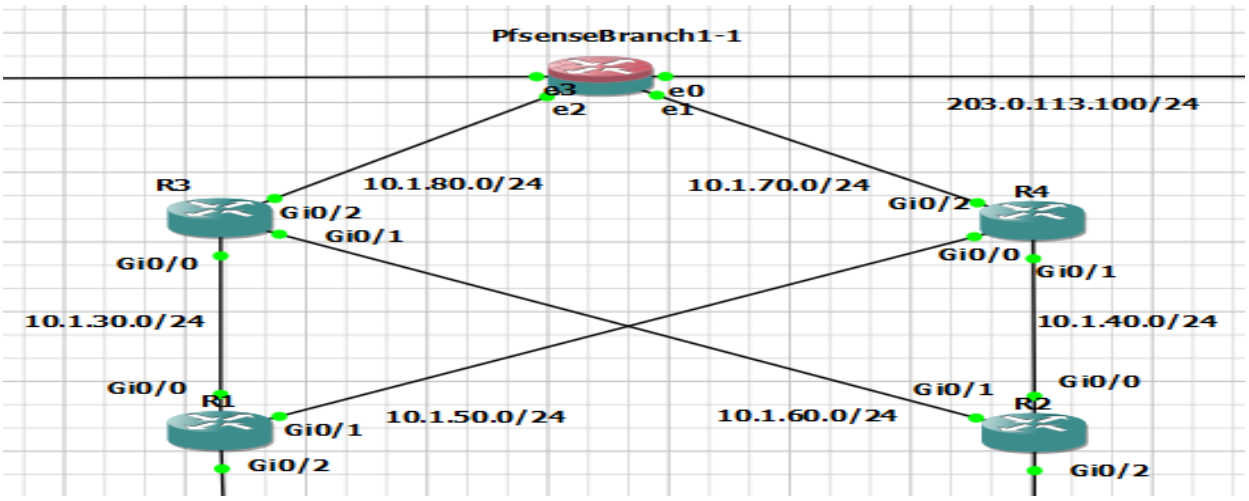


Figure 4.1.4: *Main Branch Core Layer - Schematic of the core layer in the main branch, depicting the central network infrastructure.*

- We used 4 routers (R1, R2, R3 &R4) and a pfsense firewall/router.

- R1 & R2 routers are connected to the multi-layer switches (ML1 & ML2) in the bottom layer (distribution-layer), and are also connected to R3 & R4 routers which are then both connected to the pfsense firewall/router.

- The pfsense firewall/router is connected to R3 & R4 routers, and is also connected to the ISP and the web server.

- **Second branch (compromised branch):**

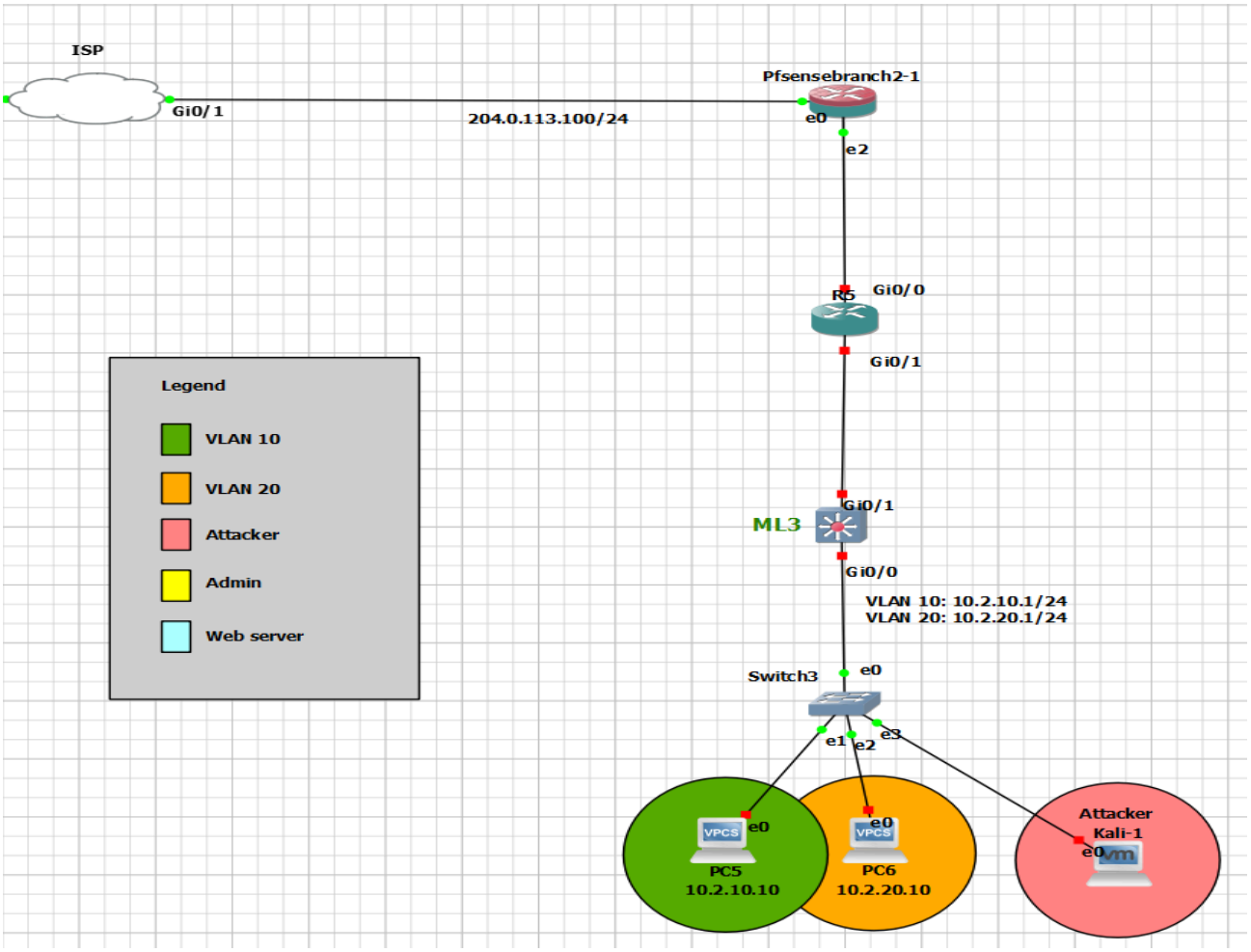


Figure 4.1.5: *Second Branch (Compromised) - Diagram of the second, compromised branch used for security testing.*

- 2x VPCS

- 1x Switches
- 1x Multilayer-switches
- 1x Routers
- 1x Pfsense (firewall & router)
- 1x Attacker's Virtual Machine (running on Kali)

❖ **Second branch's access-layer:**

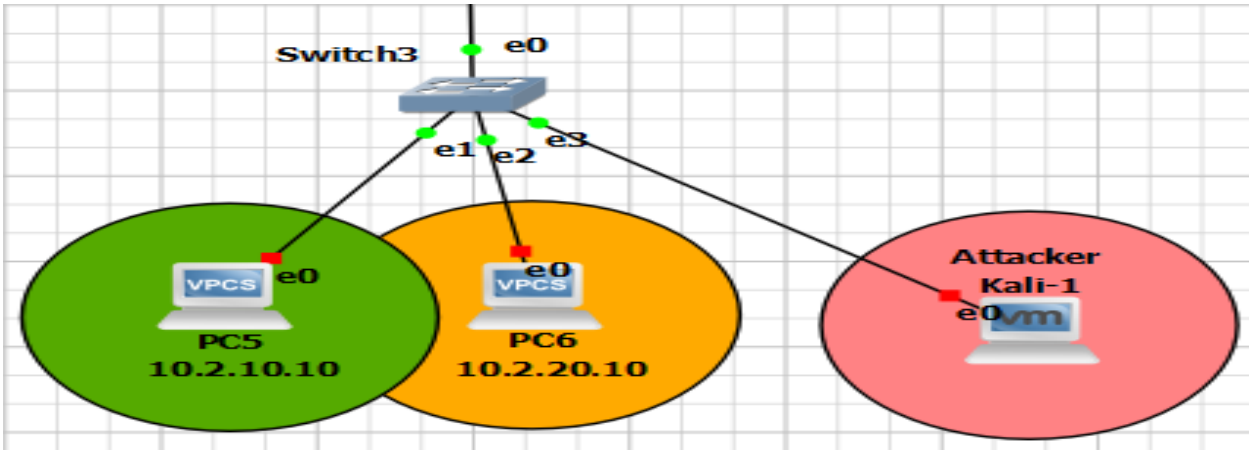


Figure 4.1.6: *Second Branch Access Layer - Detailed view of the access layer in the second branch, showing connections to end devices.*

- We have 2 VPCs and a switch
- in which PC5 and Kali Linux machine belongs to VLAN 10, whereas PC6 belongs to VLAN 20.
- The switch was configured in access mode through the ports that are connected to the PCs while the port connecting to the upper layer, we used trunk mode.
- In which were going to be simulating attacks through the kali Linux machine to demonstrate how one compromised branch can affect the other branches.

❖ **Second branch's distribution-layer:**

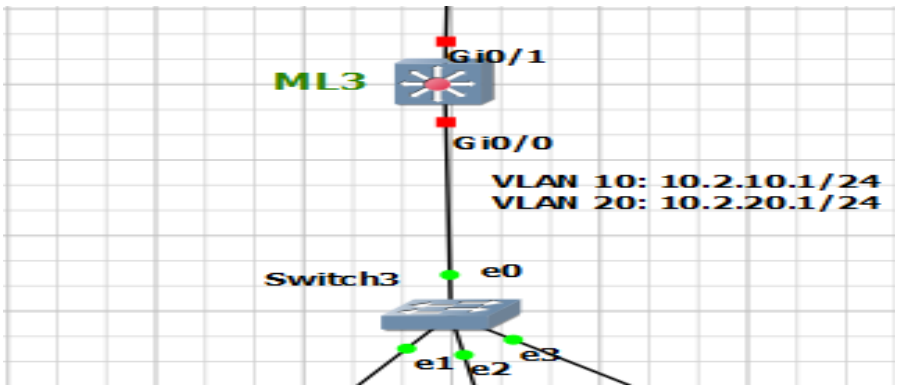


Figure 4.1.7: *Second Branch Distribution Layer - Diagram of the distribution layer in the second branch, illustrating intermediary network devices.*

- As for the distribution layer we have a multilayer switch which is connected to a switch, which connects the access layer to upper layers.

❖ Second branch's Core-layer:

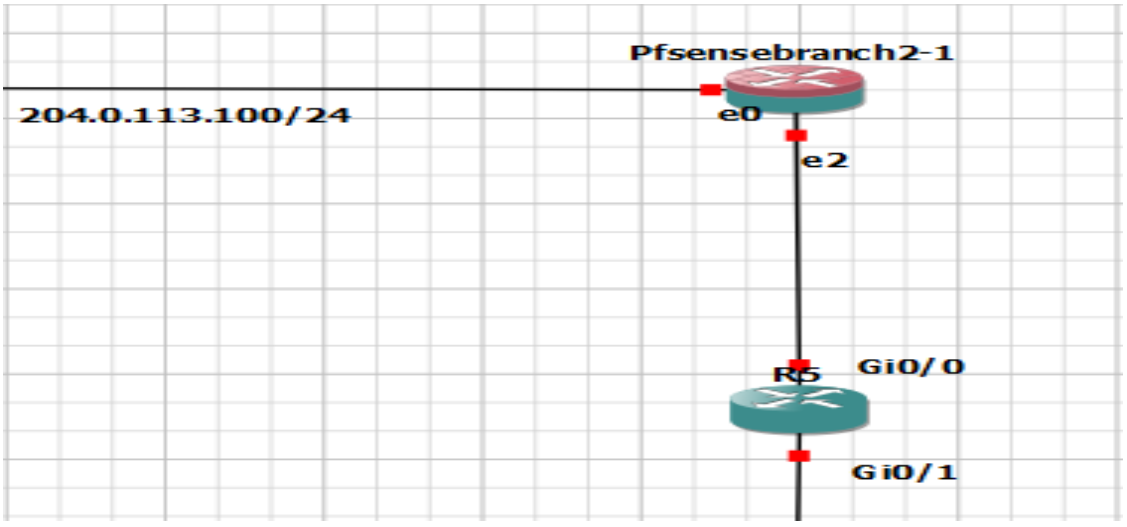


Figure 4.1.8: *Second Branch Core Layer - Schematic of the core layer in the second branch, depicting the central network infrastructure.*

- As for the core layer in branch 2, we have a pfsense firewall/router and a router
- In which the pfsense firewall/router connects the devices in the to the outside world.

Note: The web server's main purpose is to redirect the users in the network to private (local) web pages such as web login portal dedicated to local users only, the primary intention was to place a dedicated Active Directory server to authenticate authorized users but due to lack of resources on our running machine we used a web server instead.

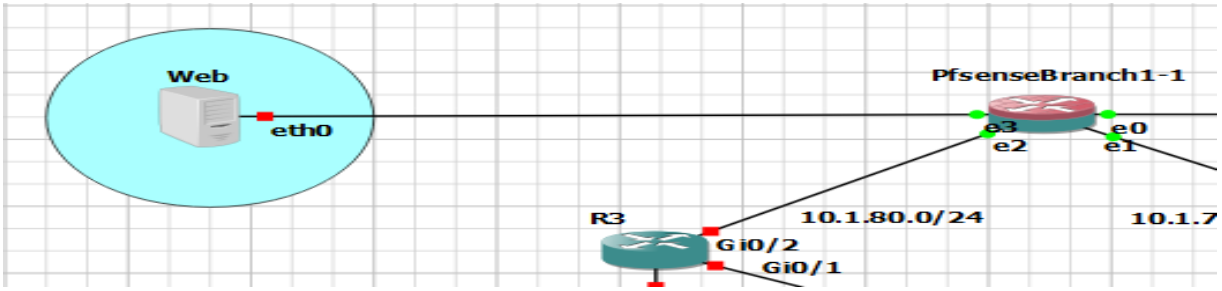


Figure 4.1.9: *Web server – web servers' purpose in the network.*

- ❖ After we have considered the main precautions when setting up our topology, and after installing all the necessary equipment to create the ideal environment for setting up an efficient Network Monitoring System (NMS) we are able to satisfy the 3 major security triads (CIA).

- We we're able to achieve the following:

1. **Confidentiality:** Ensuring that information is accessible only to those authorized to have access, this involves protecting data from unauthorized access, disclosure, or theft.

We we're able to ensure **Confidentiality** of our data by doing the following:

- **Encryption**: Using strong VPN/IPsec protocols for secure communication between Branch 1 and Branch 2.
- **Access Controls**: Strict firewall rules on pfSense at Branch 1 restrict access to authorized personnel only.
- **Intrusion Detection**: Snort on pfSense monitors and detects unauthorized access attempts or anomalies.
- **Segmentation**: VLANs isolate sensitive data within each branch, preventing unauthorized access across the network.

2. **Integrity:** ensuring that information is accurate, trustworthy, and not tampered with, it involves maintaining the consistency, accuracy, and trustworthiness of data.

We we're able to ensure **Integrity** of our data by doing the following:

- **Data Integrity**: Ensured through robust data validation mechanisms and checksums implemented at both Branch 1 and Branch 2. This ensures that data remains unaltered during transmission and storage.
- **Redundancy**: Utilizing redundant devices and protocols like EtherChannel and VRRP at critical points ensures continuous operation and minimal downtime in case of hardware failures.

- **Monitoring and Alerts**: Constant monitoring and proactive alerts from Snort IDS help in detecting and mitigating threats that could compromise data integrity.

3. **Availability:** ensuring that information and systems are accessible and usable when needed by authorized users.

We we're able to ensure **Availability** of our data by doing the following:

- **High Availability Setup**: Implemented EtherChannel for link aggregation and VRRP for router redundancy at both branches ensure uninterrupted access to network resources.
- **Load Balancing**: Optimizing traffic flow and load balancing across redundant links and devices ensure efficient resource utilization and minimize congestion.
- **Fault Tolerance**: Redundant devices and failover mechanisms at key network points guarantee seamless operation and availability of network services.

4.2. Topology

Full topology (HQ branch & Second branch)

 The following diagram represents our ideal environment to implement our Network Monitoring System (NMS).

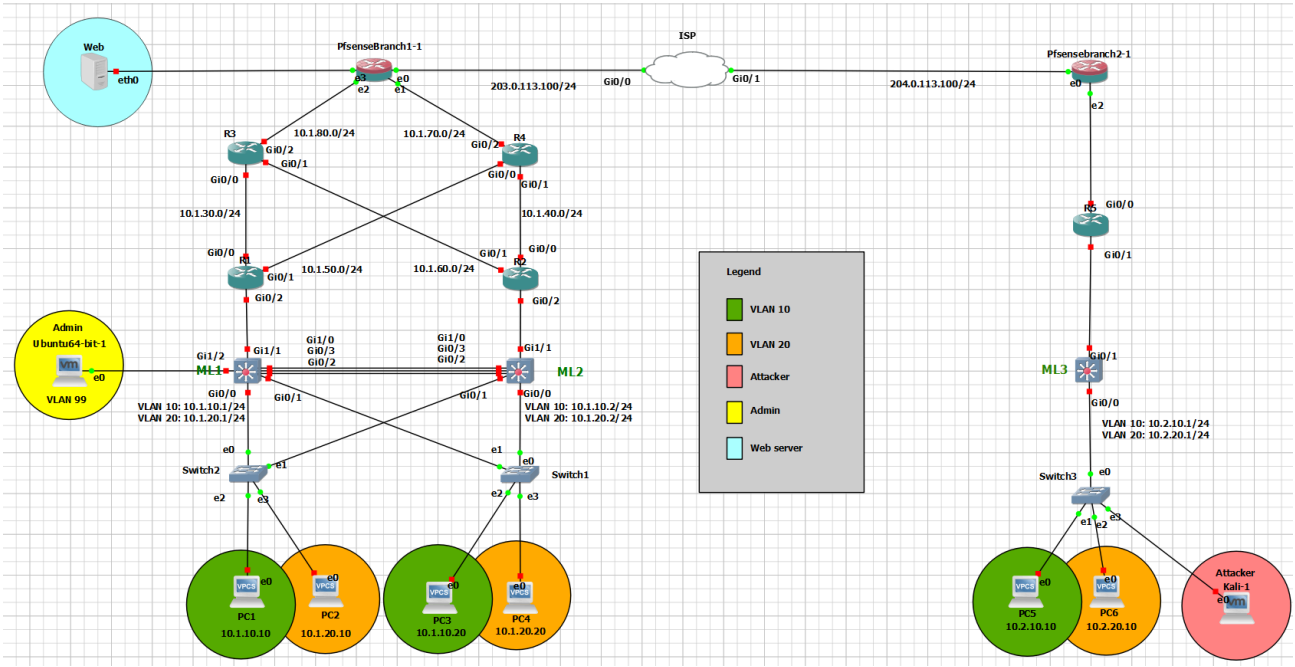


Figure 4.2.1: *Complete Network Topology - Overview of the entire network topology, including both branches and the VPN connection.*

Chapter 5: Implementation

5.1. Installation

In this section of the documentation, we're going to be mentioning all the installed software, hardware and tools along with the source of installation, in which it involved installing:

1. VMware workstation:

   Source:https://www.vmware.com/products/workstation-player/workstation-player-evaluation.html.html.html.html

2. GNS3:

   Source: https://www.gns3.com

3. Ubuntu OS:

Source: https://ubuntu.com/download/desktop

4. Kali Linux OS:

   Source: https://www.kali.org/get-kali/#kali-platforms

5. Pfsense:

   Source: https://www.pfsense.org/download/

6. The installation of Splunk:
   Source: https://www.splunk.com

7. Routers & switches images from the gns3 marketplace:

   Source: https://gns3.com/marketplace/featured

5.2. Administration and configuration

In this section of the documentation, were going to be demonstrating the appropriate configurations that was setup by the dedicated administrator in order to accomplish our NMS goals

in which we're going to be focusing the proper configuration of the following:

PfSense:

- General configuration
- Snort
- VPN/IPsec configurations
- NAT overload (PAT)
- Firewall rules configurations
- OSPF on the pfSense configuration (using FRR package)

Splunk:

- General configuration
- Receiving Snort alerts on a dedicated port
- Using the snort app & search and reporting feature
- Sending alerts to the administrator's handheld device

Note: as for the basic intermediary devices configurations they will be added towards the ending of the documentation.

❖ PfSense:

- General configuration:

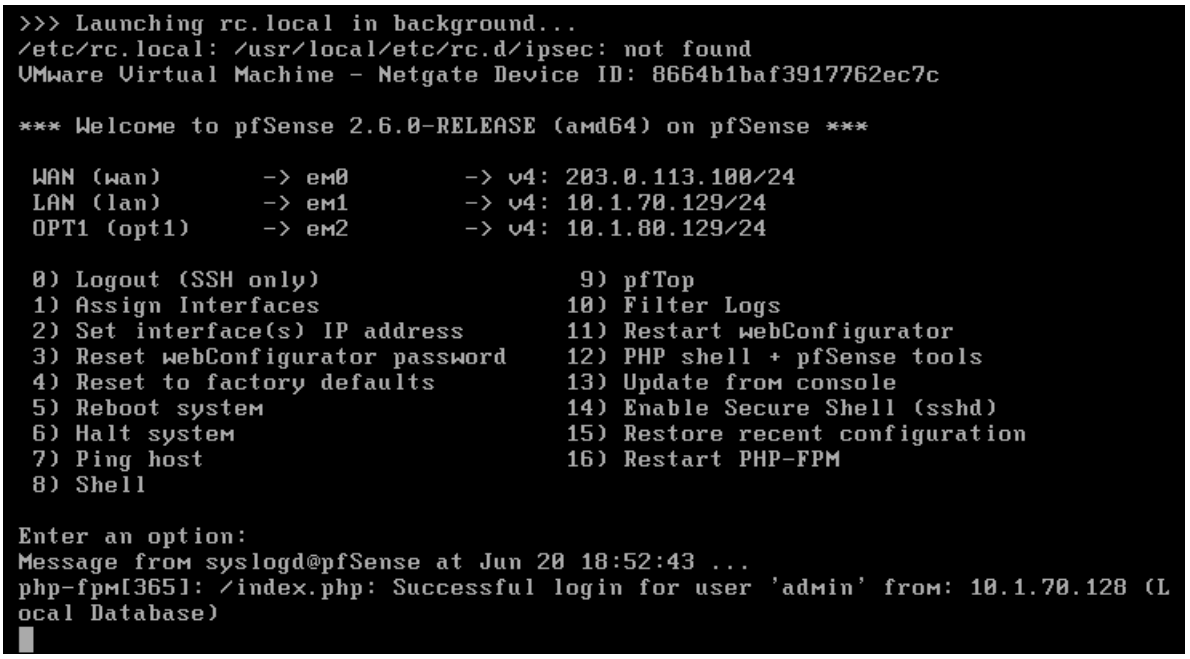


Figure 5.2.1: *PfSense Branch 1 CLI configurations – Diagram shows the ip addresses of all the connected interfaces on the pfsense in HQ branch.*

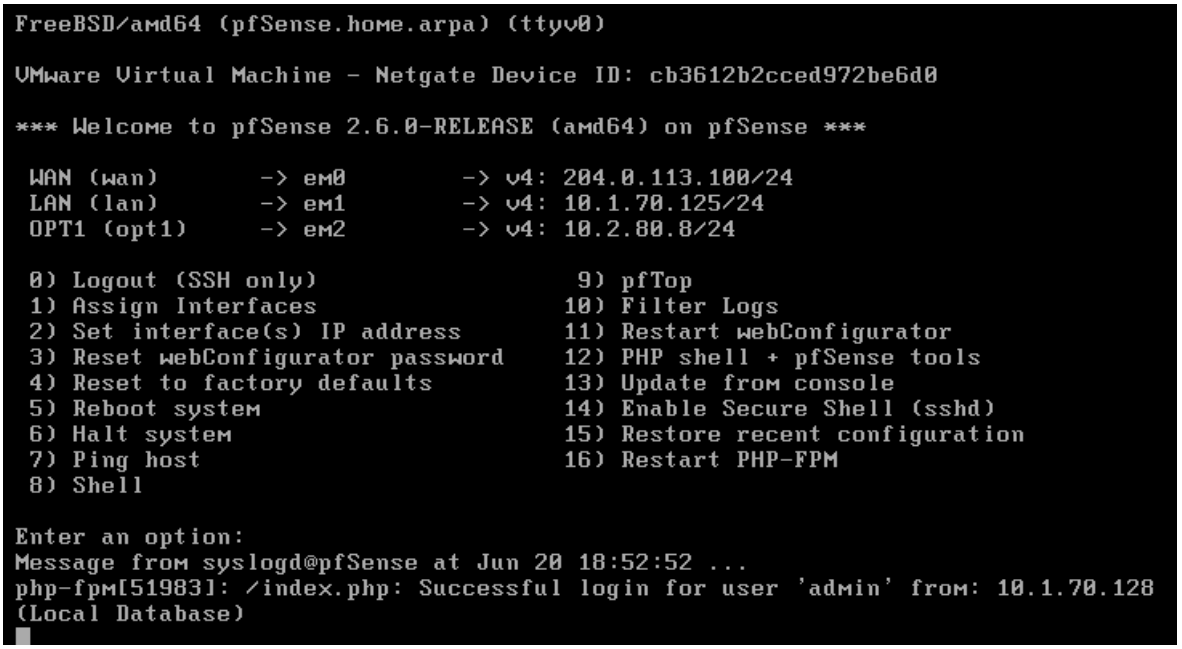


Figure 5.2.2: *PfSense Branch 2 CLI configurations – Diagram shows the ip addresses of all the connected interfaces on the pfsense in the second branch.*

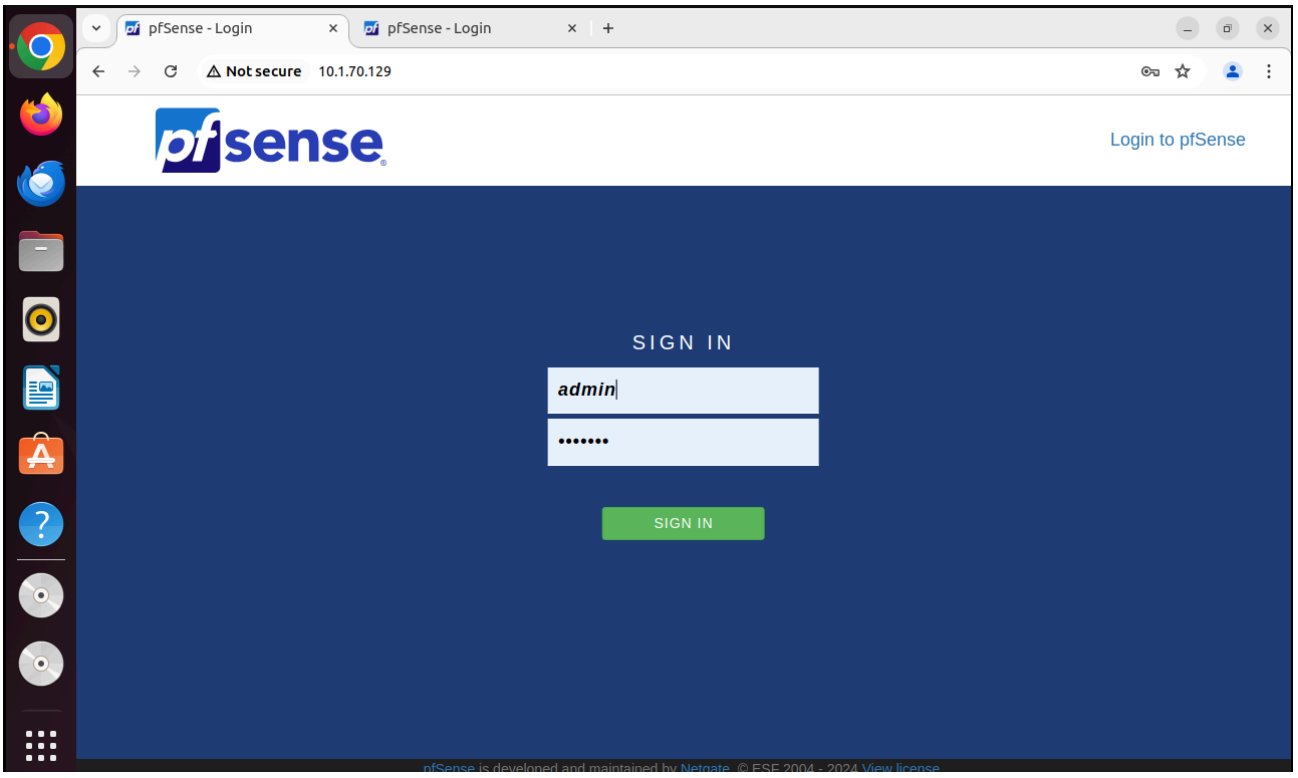


Figure 5.2.3: *PfSense Branch 1 web gui portal – Diagram shows the login portal to the pfsense in the HQ branch from the admins PC*

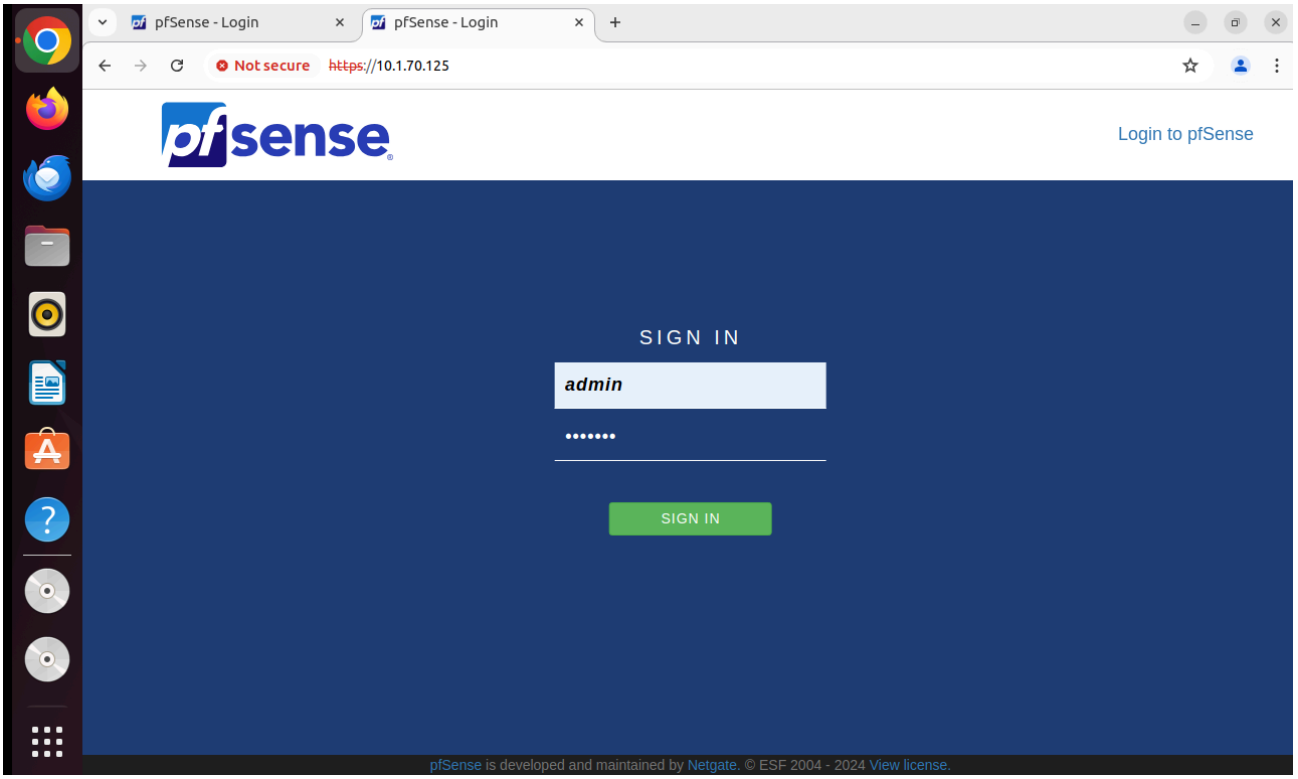


Figure 5.2.4: *PfSense Branch 2 web gui portal – Diagram shows the login portal to the pfsense in the second branch from the admins PC (remotely)*

- Snort:

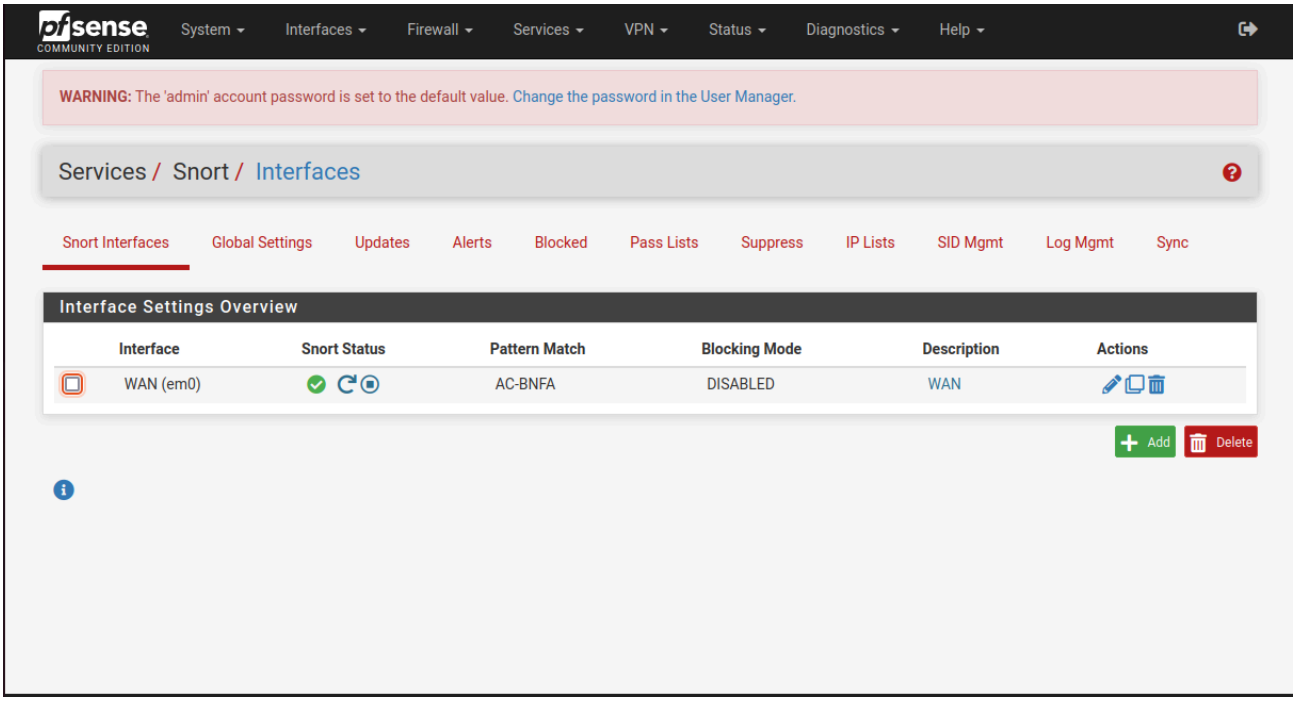


Figure 5.2.5: *Snort interfaces – Diagram shows the status of the WAN interface connected to the PfSense.*

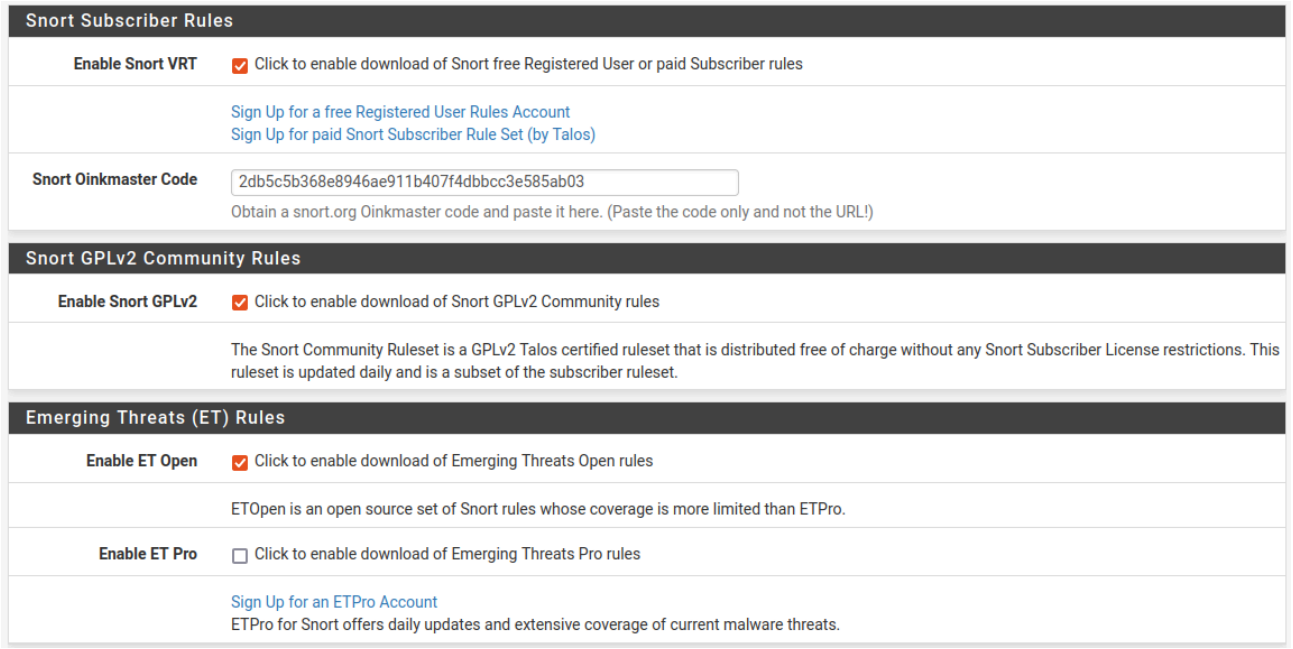


Figure 5.2.6: *Snort's ruleset – Diagram shows all the enabled preset rulesets.*

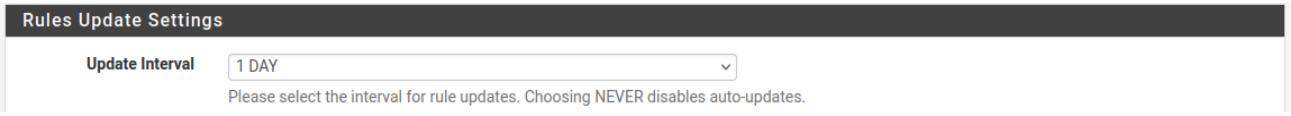


Figure 5.2.7: *Snort's rulesets scheduled updates– Diagram shows that the rulesets are scheduled for updates daily (1 day)*

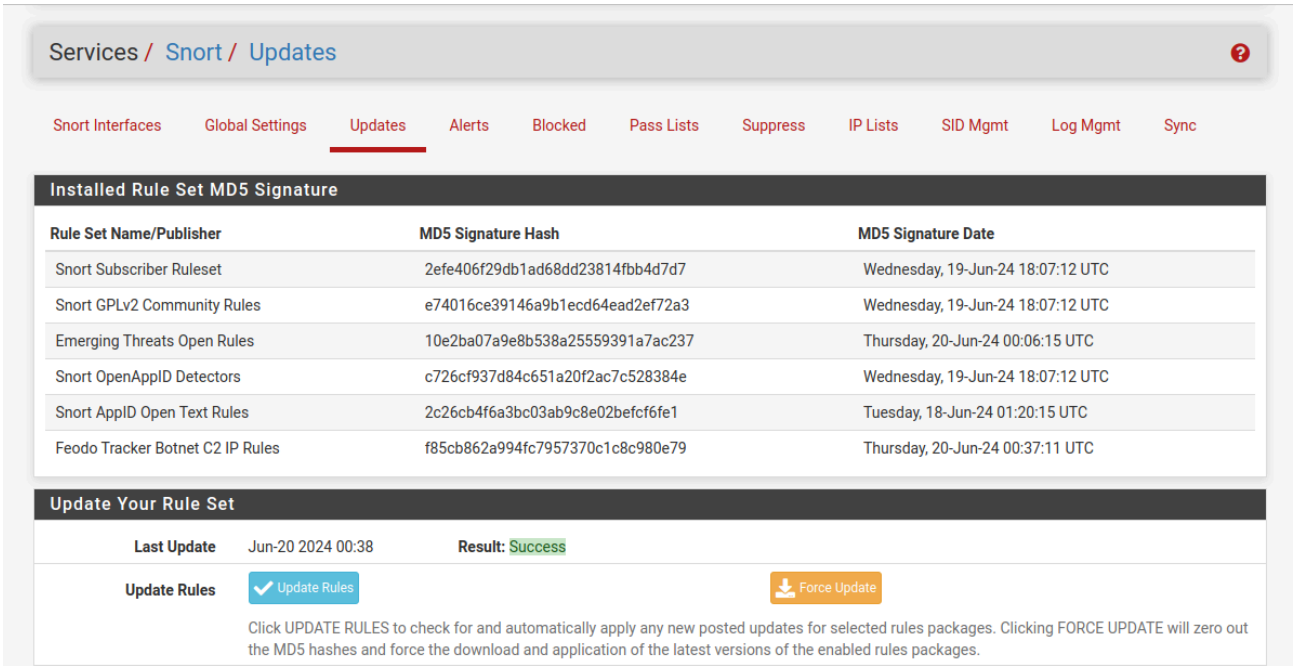


Figure 5.2.8: *Snort's rulesets update– Diagram shows that the rulesets have successfully updated (daily)*

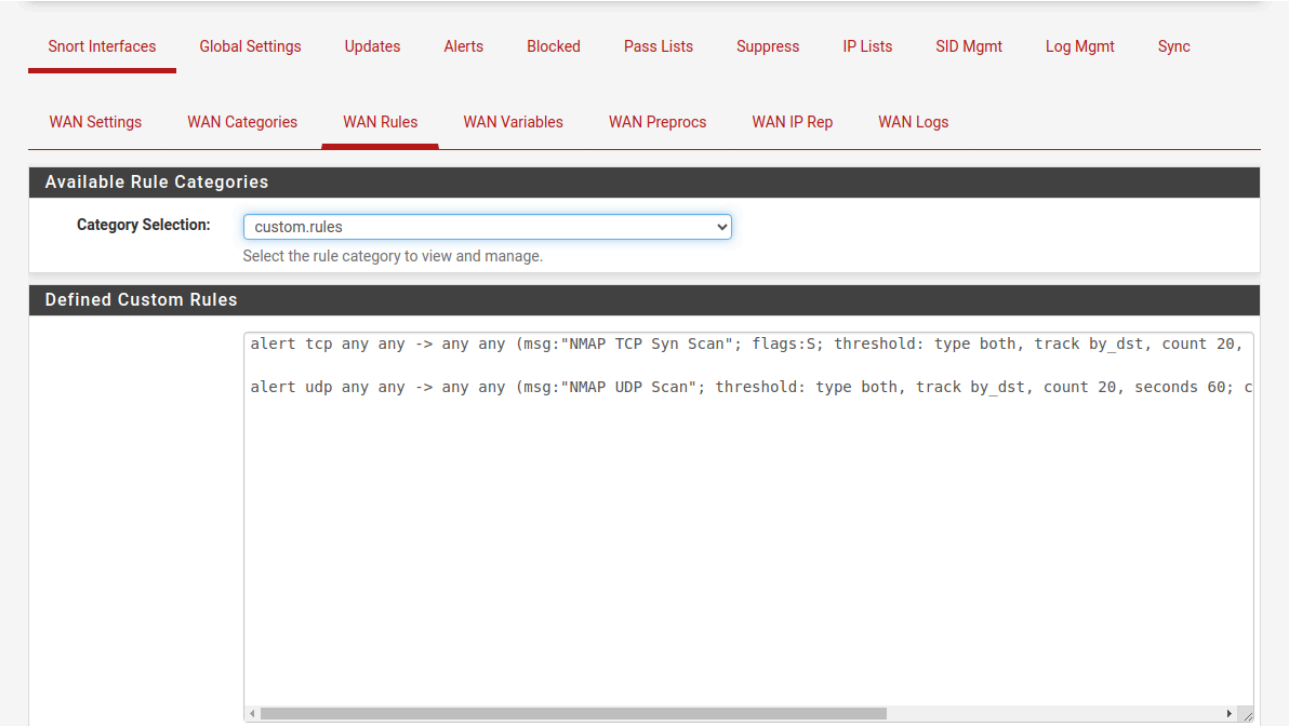


Figure 5.2.9: *Snort's custom rulesets– Diagram shows that snort enables users to set custom rules, in which it's configured to alert the user of any type of NMAP scan whether TCP/UDP.*

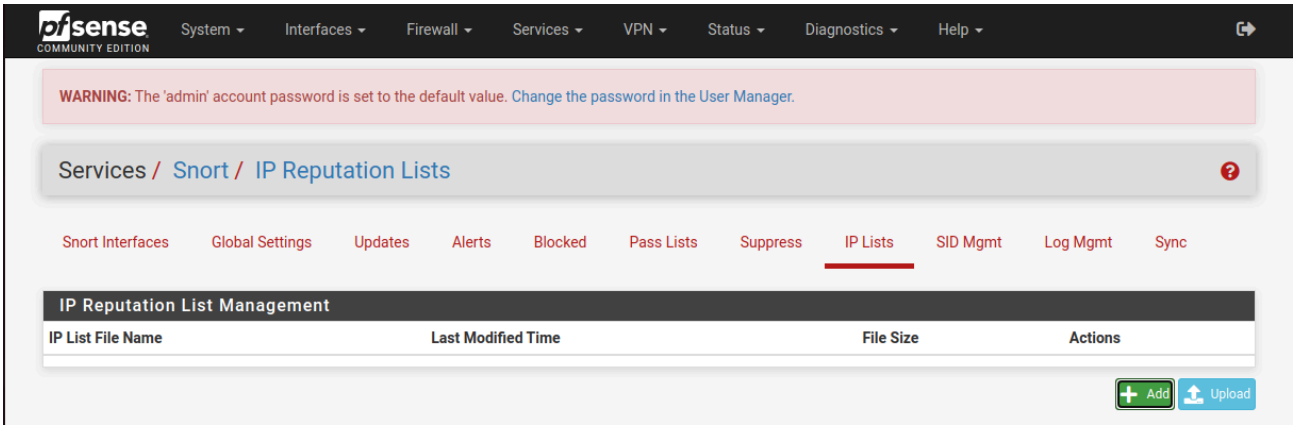


Figure 5.2.10: *Snort's IP Lists tab– Diagram shows an empty list of Ips in which Ips with bad reputations fall under.*

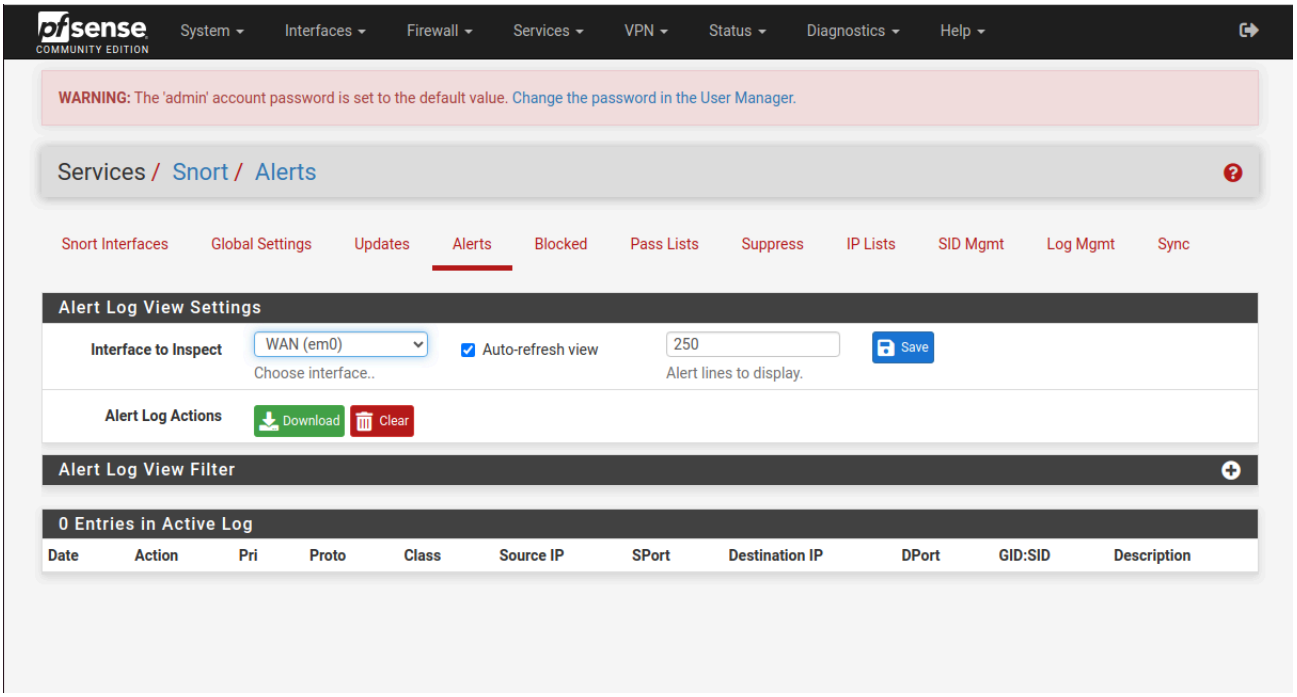


Figure 5.2.11: *Snort's Alerts tab– Diagram shows an empty list of alerts on the WAN interface indicating that no intrusion attempt took place.*

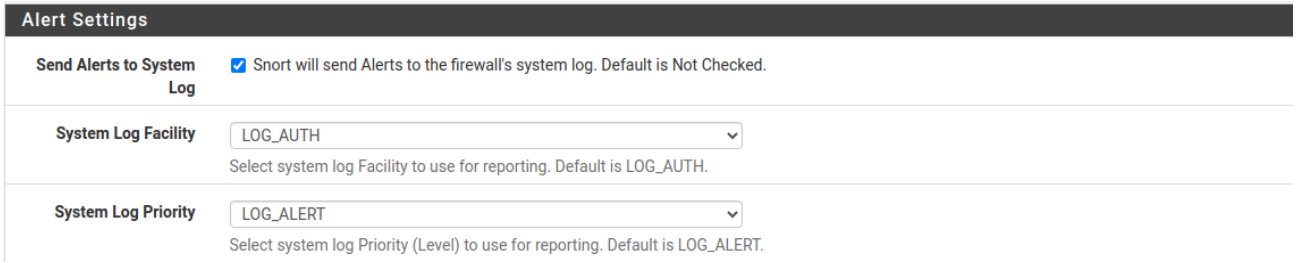


Figure 5.2.12: *Snort's Alert settings– Diagram indicates that all snort alerts get forwarded to the pfsesne's firewall system logs.*

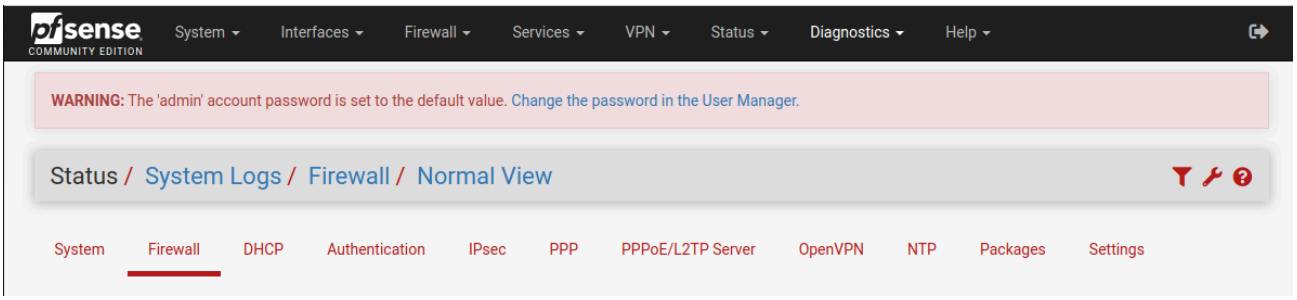


Figure 5.2.13: *Snort's Firewall system logs – Diagram indicates that all snort alerts get forwarded to this location (firewall system logs).*

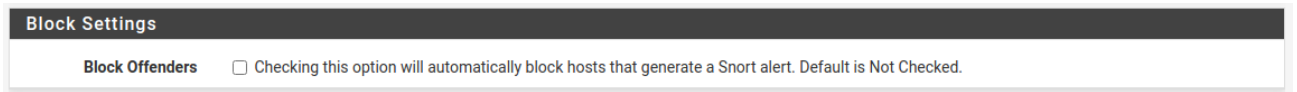


Figure 5.2.14: *Snort's blocking rules– Diagram shows that the block offenders' field have unchecked.*

Note: in figure 5.2.14 we have disabled the block offenders' field, as the main purpose of using snort in our NMS was to use the IDS (Intrusion Detection System) feature of snort for monitoring purposes, and not the IPS (Intrusion Prevention System) feature that comes along with snort, as enabling this feature prevents and automatically blocks any traffic coming from the device that triggered the system with an attack.

- **VPN/IPsec:**

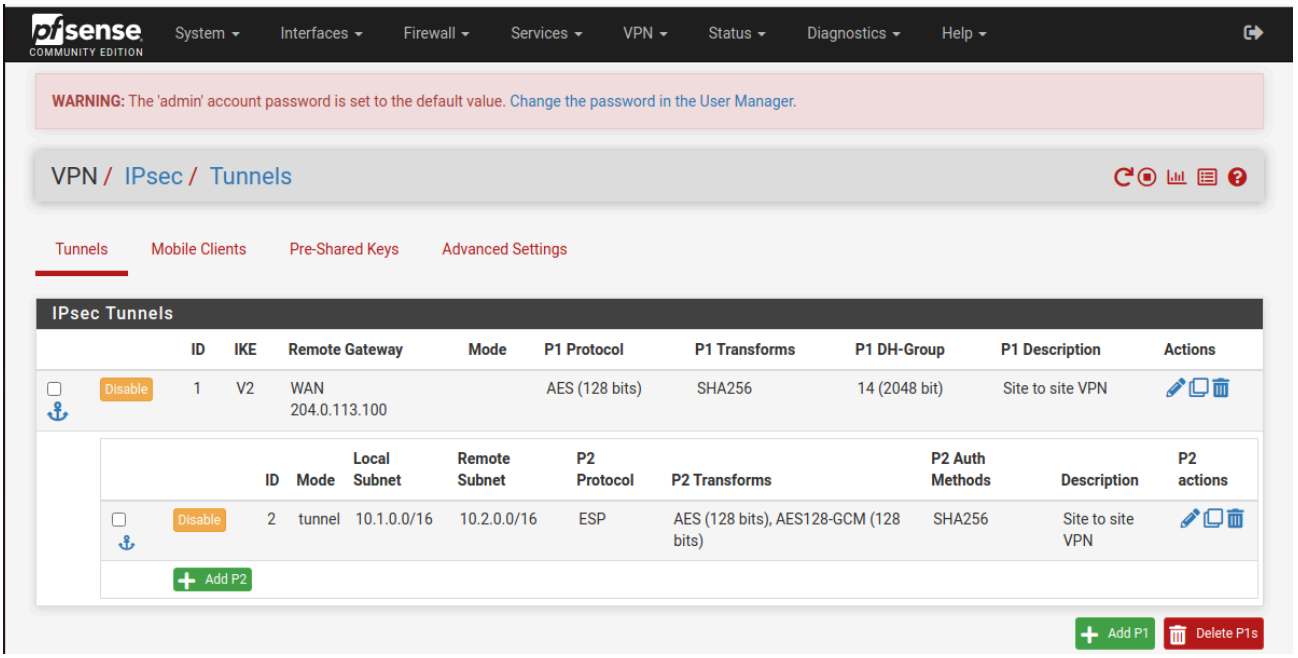


Figure 5.2.15: *VPN/IPsec configuration in HQ branch – Diagram shows the configuration of the two phases of the VPN/IPsec in the HQ branch, which specifies the encryption methods used along with the IP addresses of the remote gateway (second branch), local subnet (HQ) and remote subnet (second branch).*

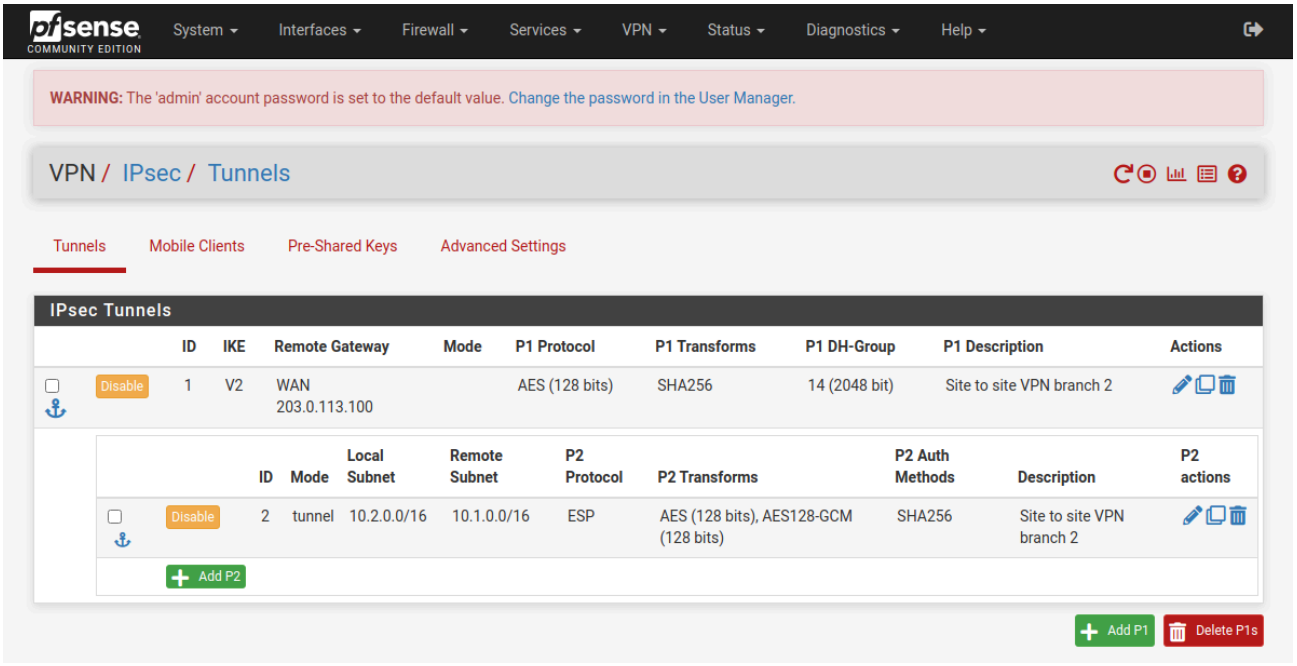


Figure 5.2.16: *VPN/IPsec configuration in the second branch – Diagram shows the configuration of the two phases of the VPN/IPsec in the second branch, which specifies the encryption methods used (identical encryption methods to HQ) along with the IP addresses of the remote gateway (HQ), local subnet (second branch) and remote subnet (HQ).*

- **NAT overload (PAT):**

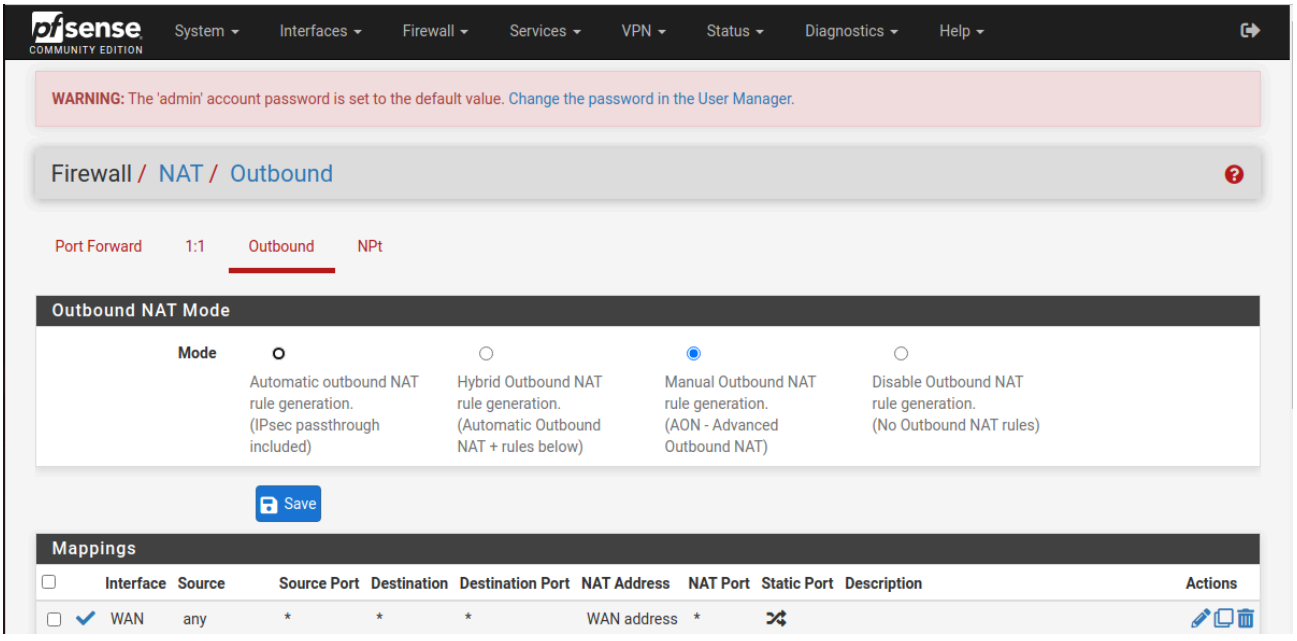


Figure 5.2.17: *NAT overload configuration – Diagram shows that the outbound NAT mode have been enabled for any device & any type of traffic passing through the WAN interface.*

- **Firewall rules:**

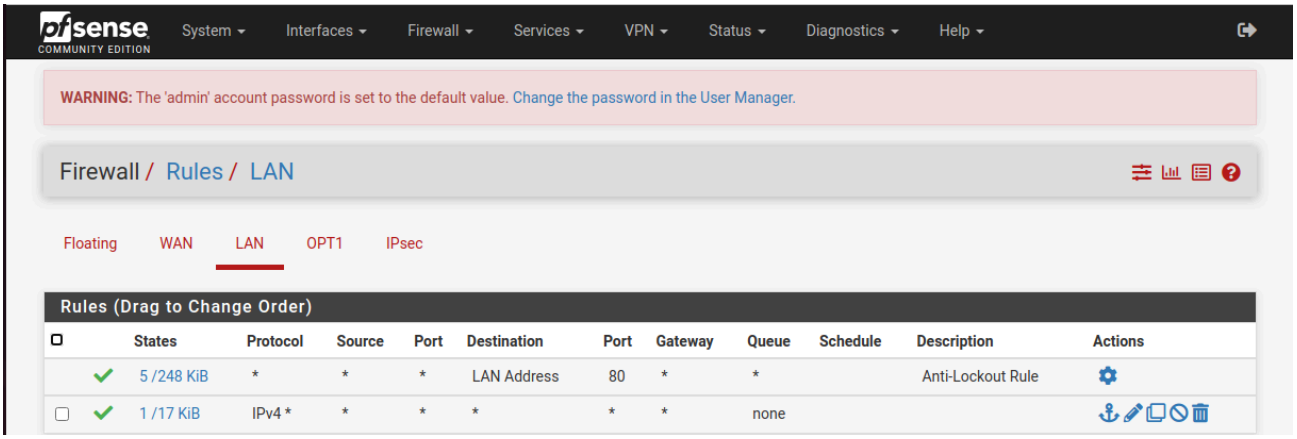


Figure 5.2.18: *LAN firewall rules configuration – Diagram shows an* ***allow any*** *firewall policy on the* ***LAN*** *interface.*

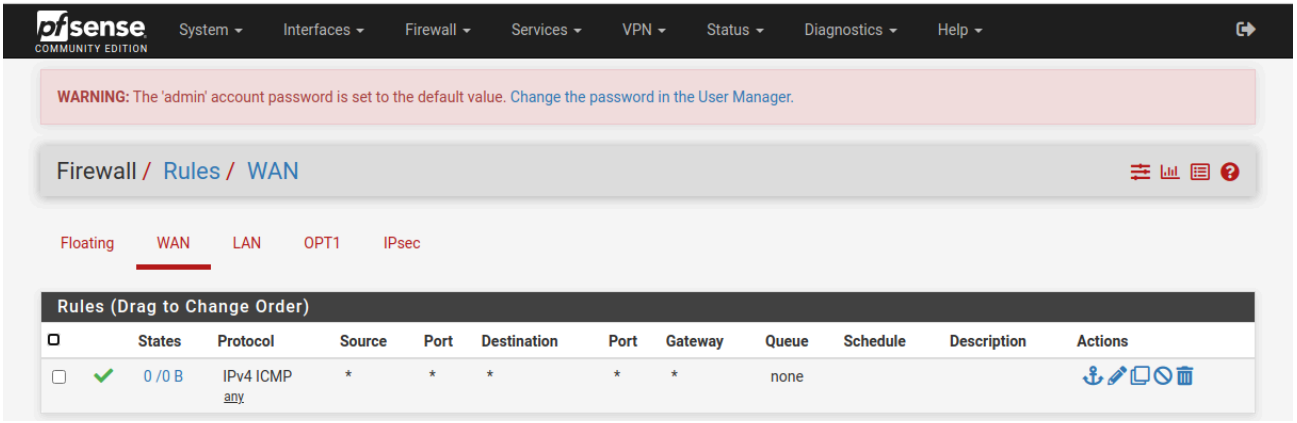


Figure 5.2.19: *WAN firewall rules configuration – Diagram shows an* ***allow ICMP traffic*** *firewall policy on the* ***WAN*** *interface.*

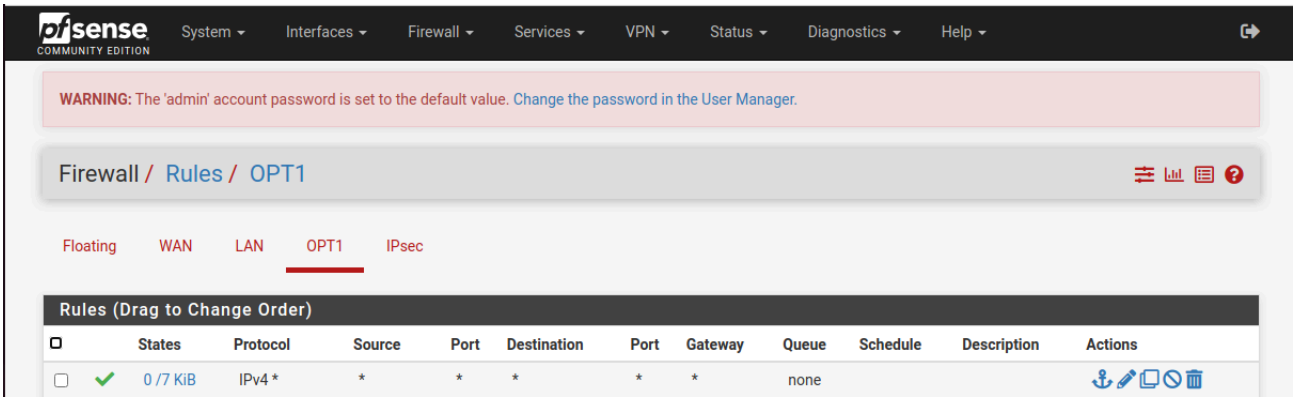


Figure 5.2.20: *OPT1 firewall rules configuration – Diagram shows an* ***allow any*** *firewall policy on the* ***OPT1*** *interface.*

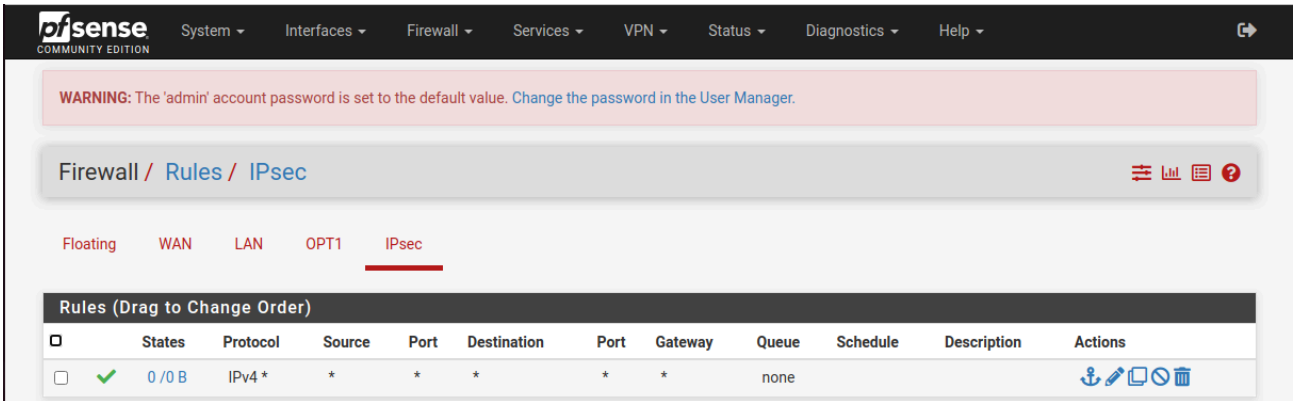


Figure 5.2.21: *IPsec firewall rules configuration – Diagram shows an* ***allow any*** *firewall policy on the* ***IPsec*** *interface.*

- **OSPF (using FRR package):**

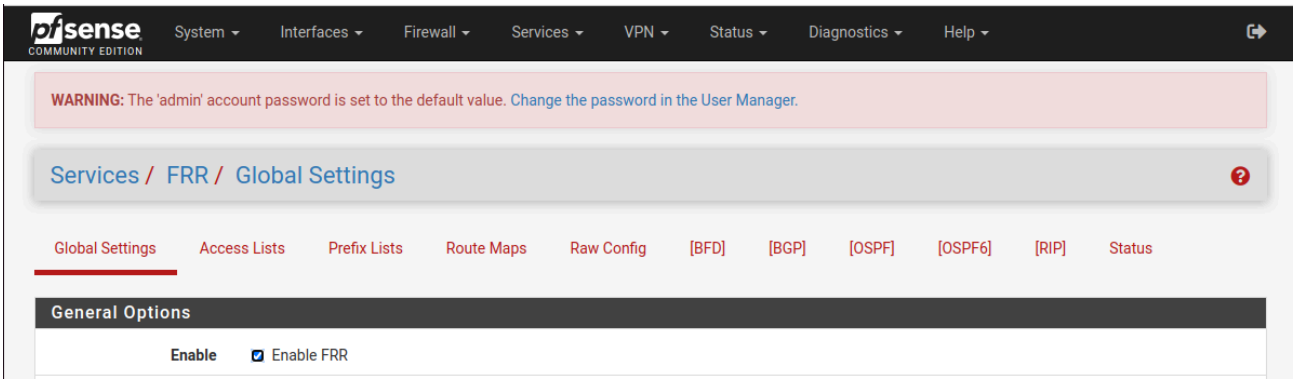


Figure 5.2.22: *OSPF (FRR) configuration – Diagram shows that the FRR service has been enabled.*

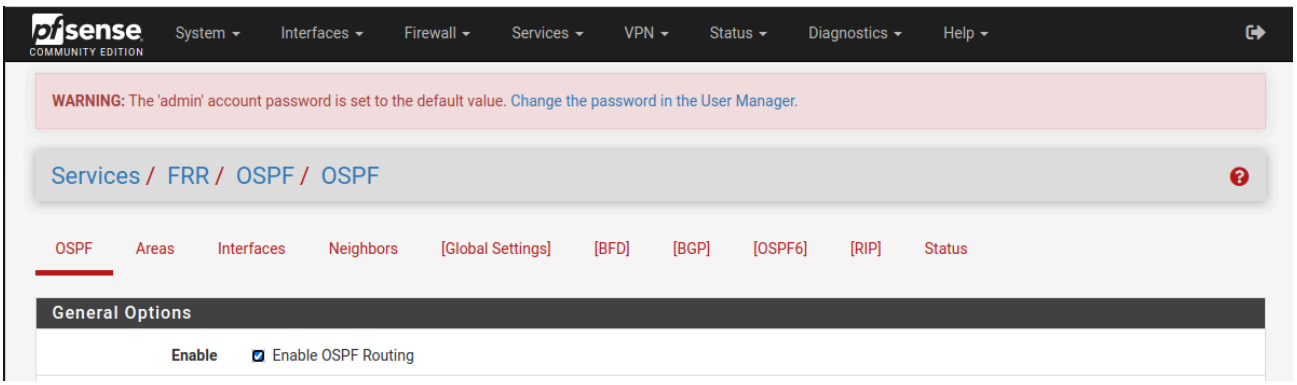


Figure 5.2.23: *OSPF configuration – Diagram shows that OSPF routing has been enabled.*

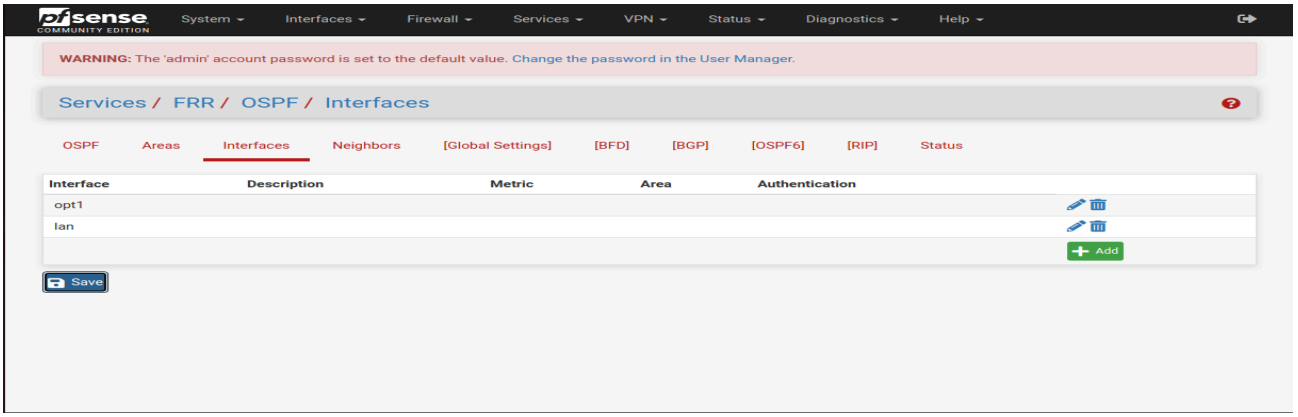


Figure 5.2.24: *OSPF interfaces configuration – Diagram shows that OSPF routing has been enabled on the* ***opt1*** *and* ***LAN*** *interfaces*

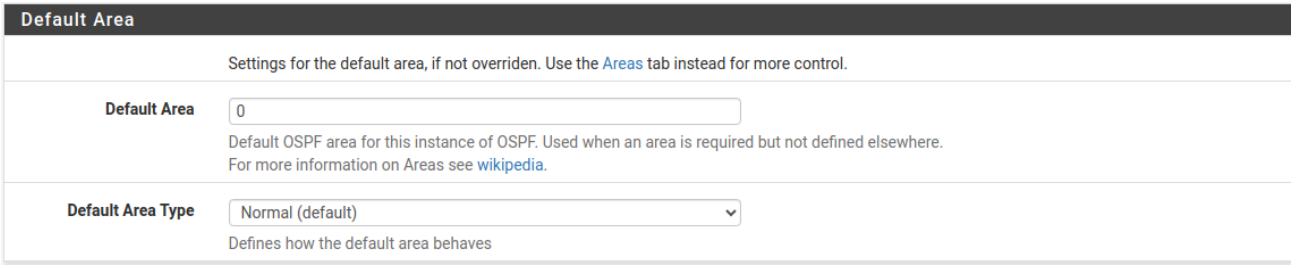


Figure 5.2.25: *OSPF area configuration – Diagram shows that OSPF operates in area 0.*

❖ Splunk:

- General configuration**:**

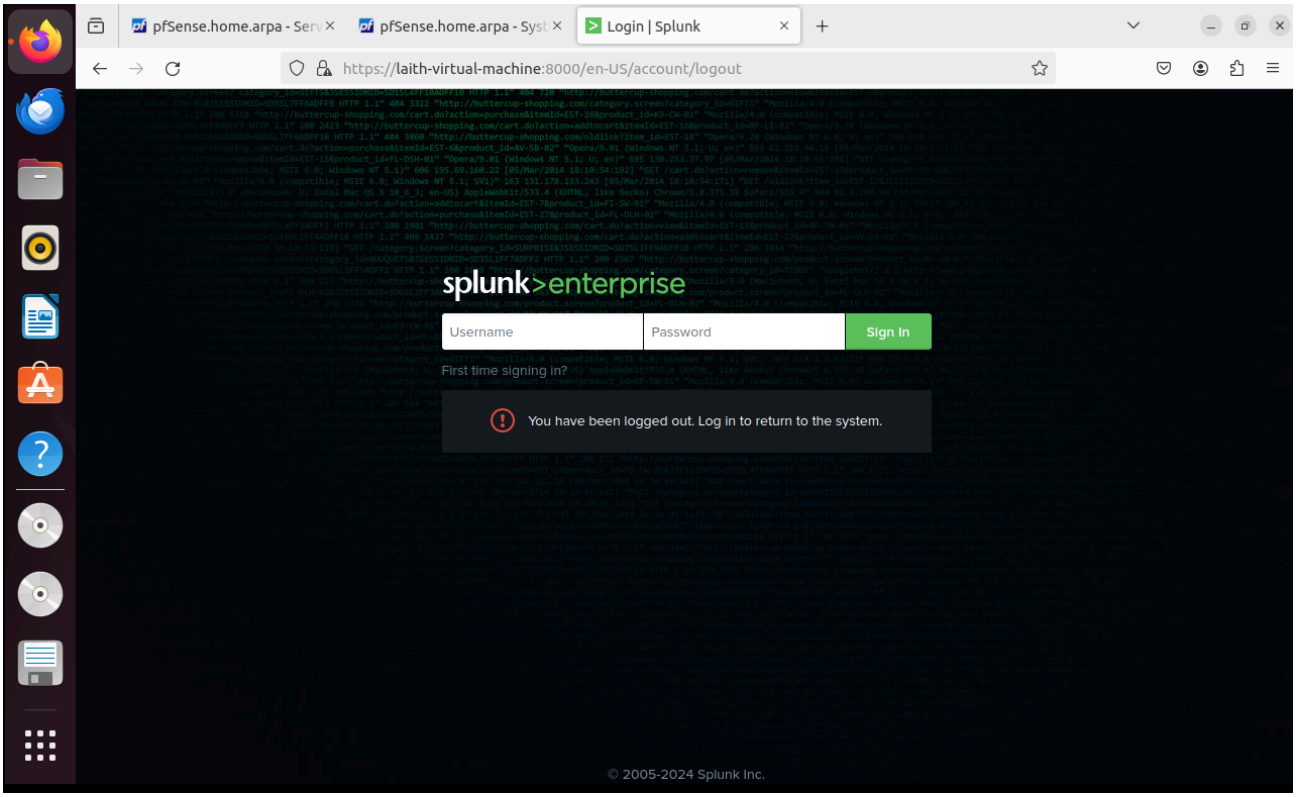


Figure 5.2.26: *Splunk's web GUI – Diagram shows Splunk's login portal from the admins PC.*

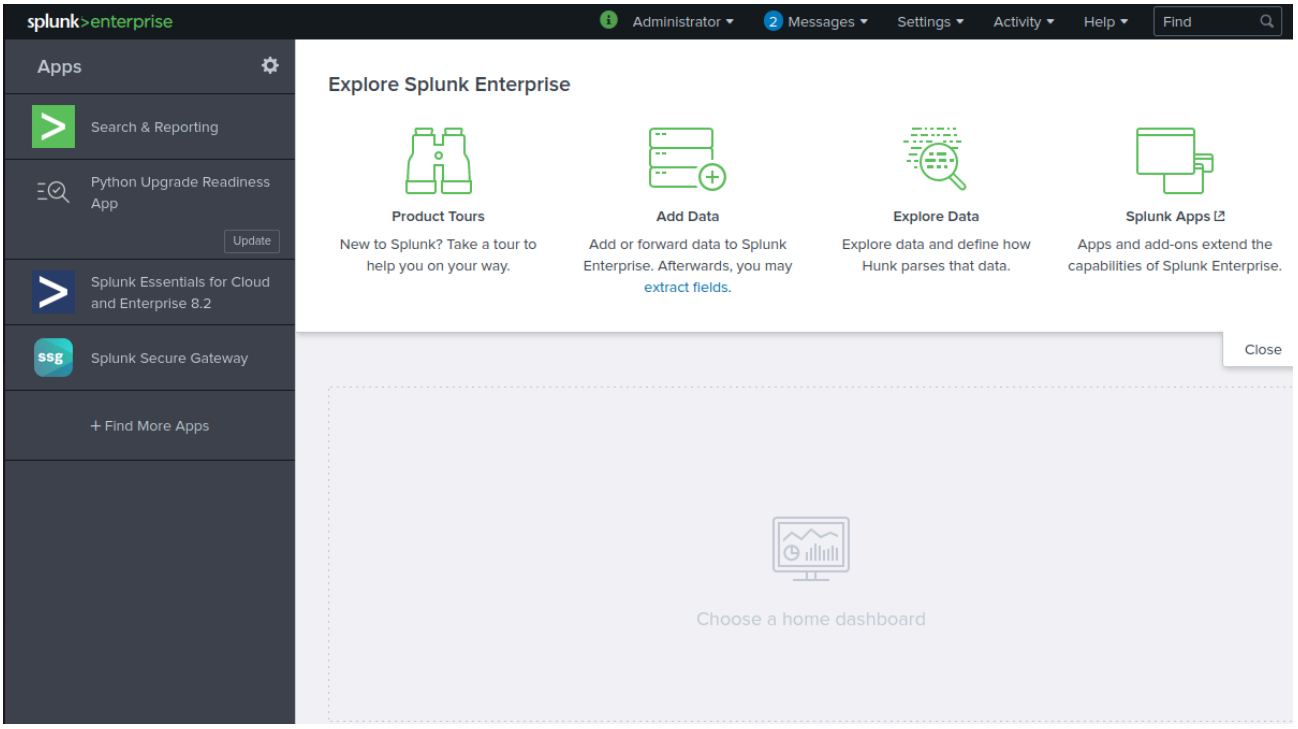


Figure 5.2.27: *Splunk's Home menu – Diagram shows Splunk's dashboard.*

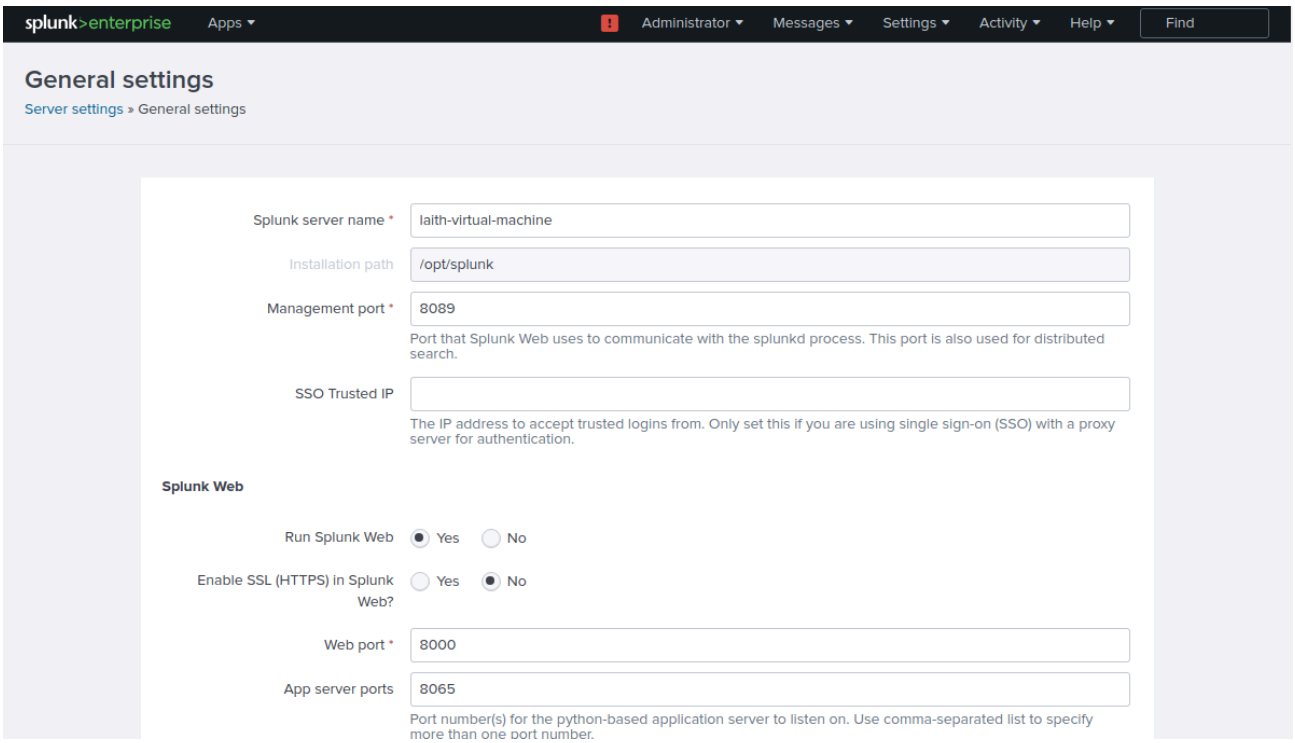


Figure 5.2.28: *Splunk's server settings – Diagram shows the name of the server and the ports dedicated to the Splunk's server, web port: 8000 indicates the port in which the web gui is accessed.*

- Receiving Snort alerts on a dedicated port:

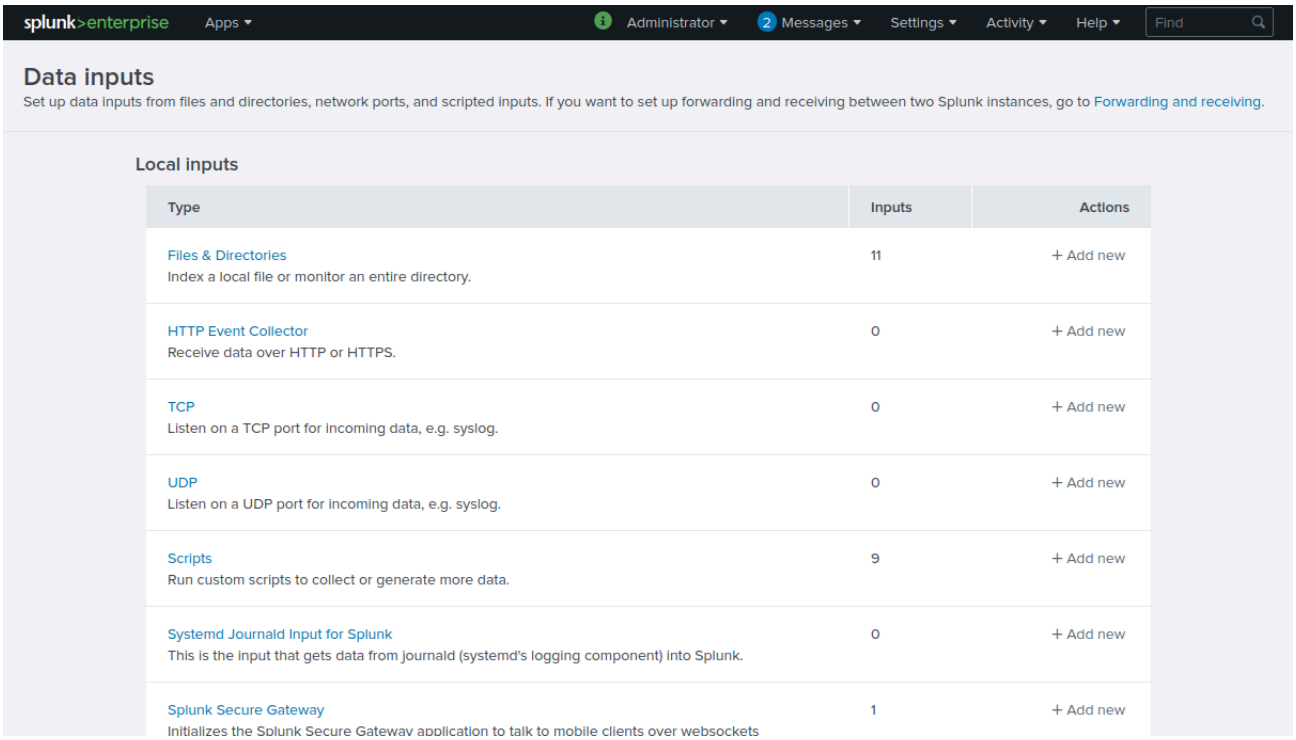


Figure 5.2.29: *Splunk's Data input settings – Diagram shows a list of data input types.*

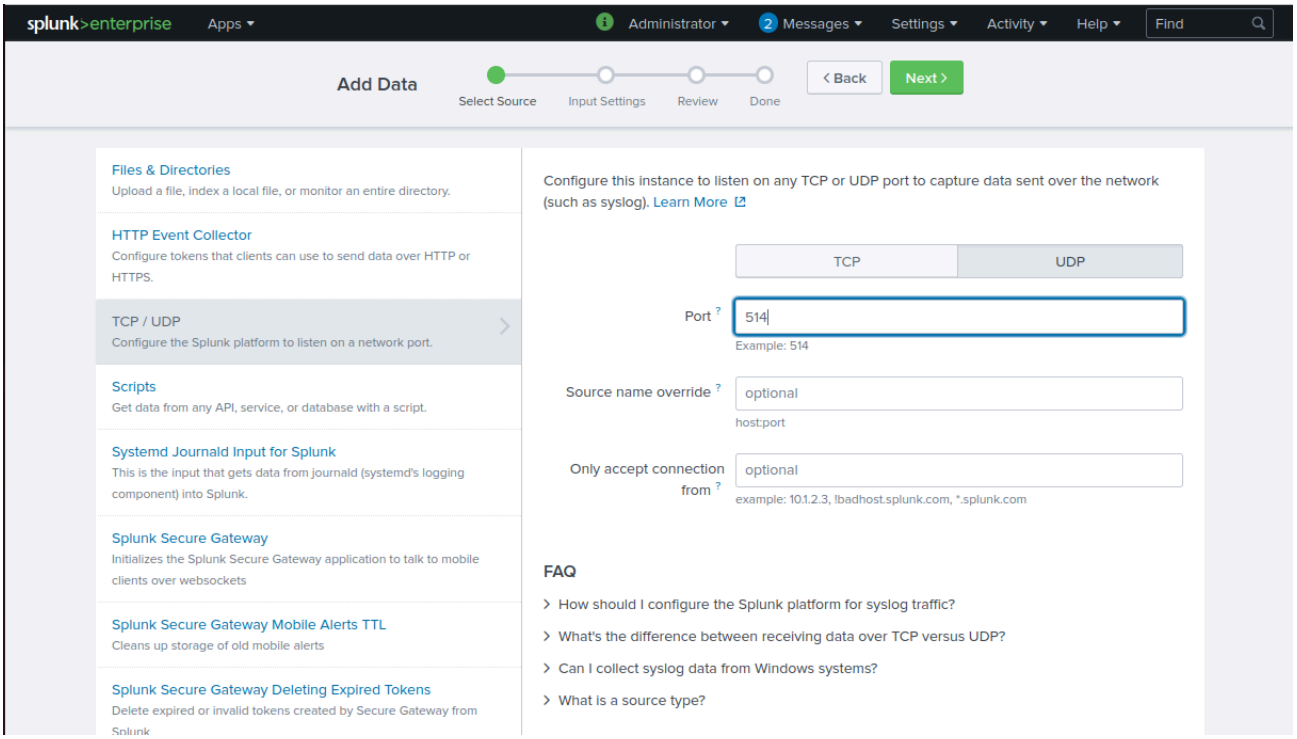


Figure 5.2.30: *Splunk's listening port – Diagram shows that Splunk is set to listen on port 514 UDP.*

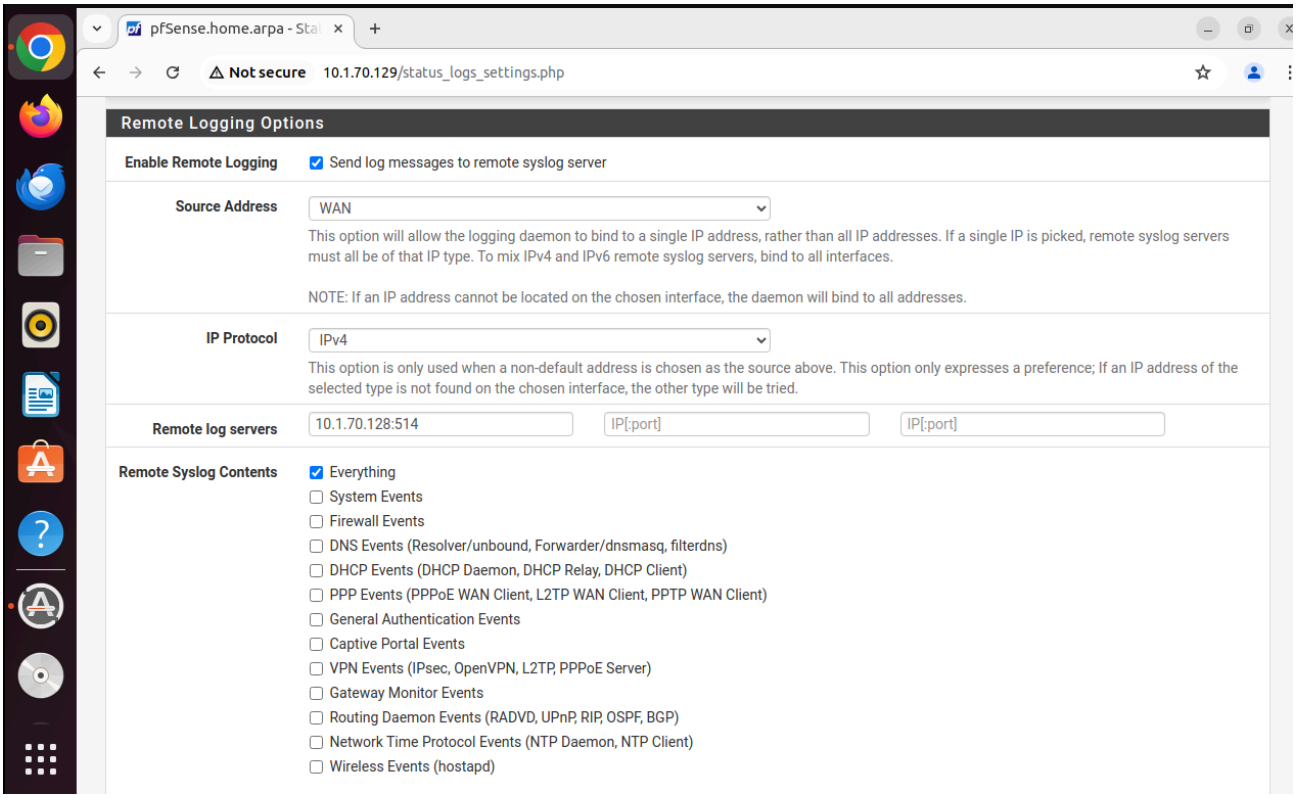


Figure 5.2.31: *Pfsense Remote logging option – Diagram shows all system logs in pfsesne (including firewall events which includes the snort logs) is forwandered to the ip address of our splunks server on the UDP port 514 which splunk will be listening on*

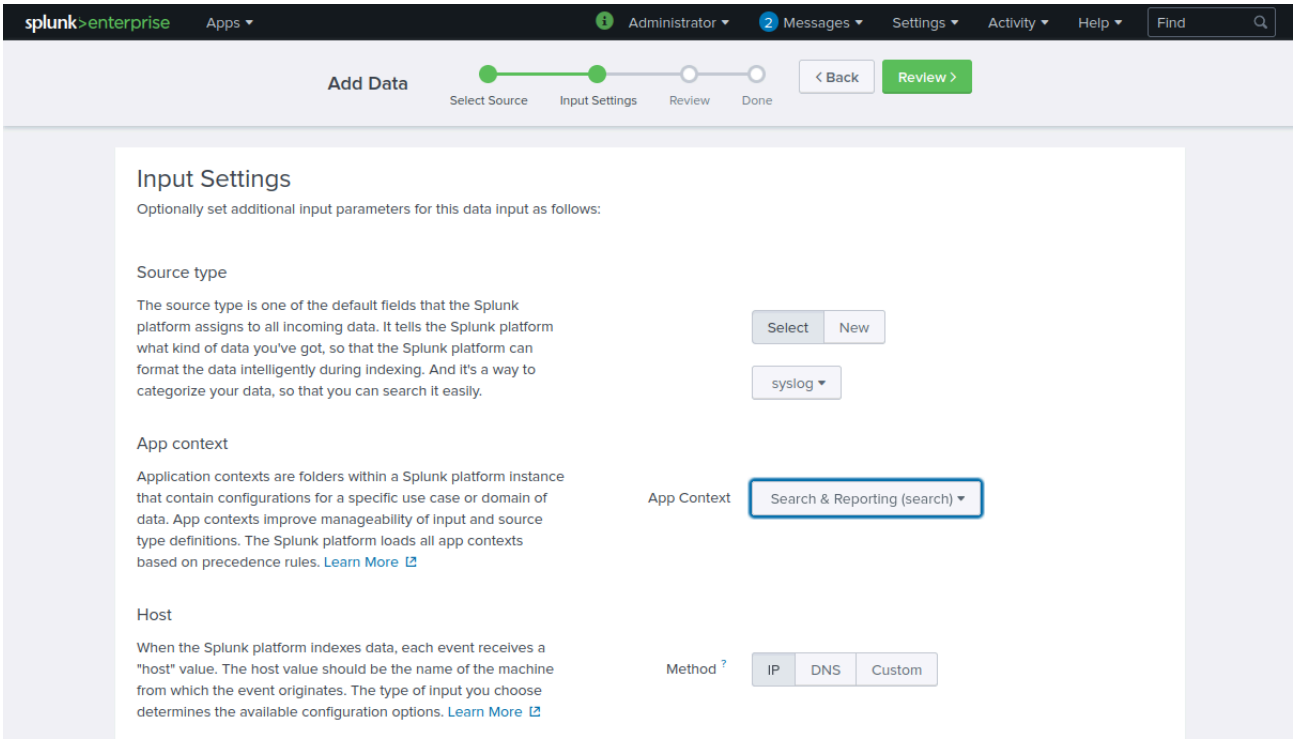


Figure 5.2.32: *Splunk's input settings – Diagram shows that Splunk is set to process and receive syslog messages using the search and reporting app.*

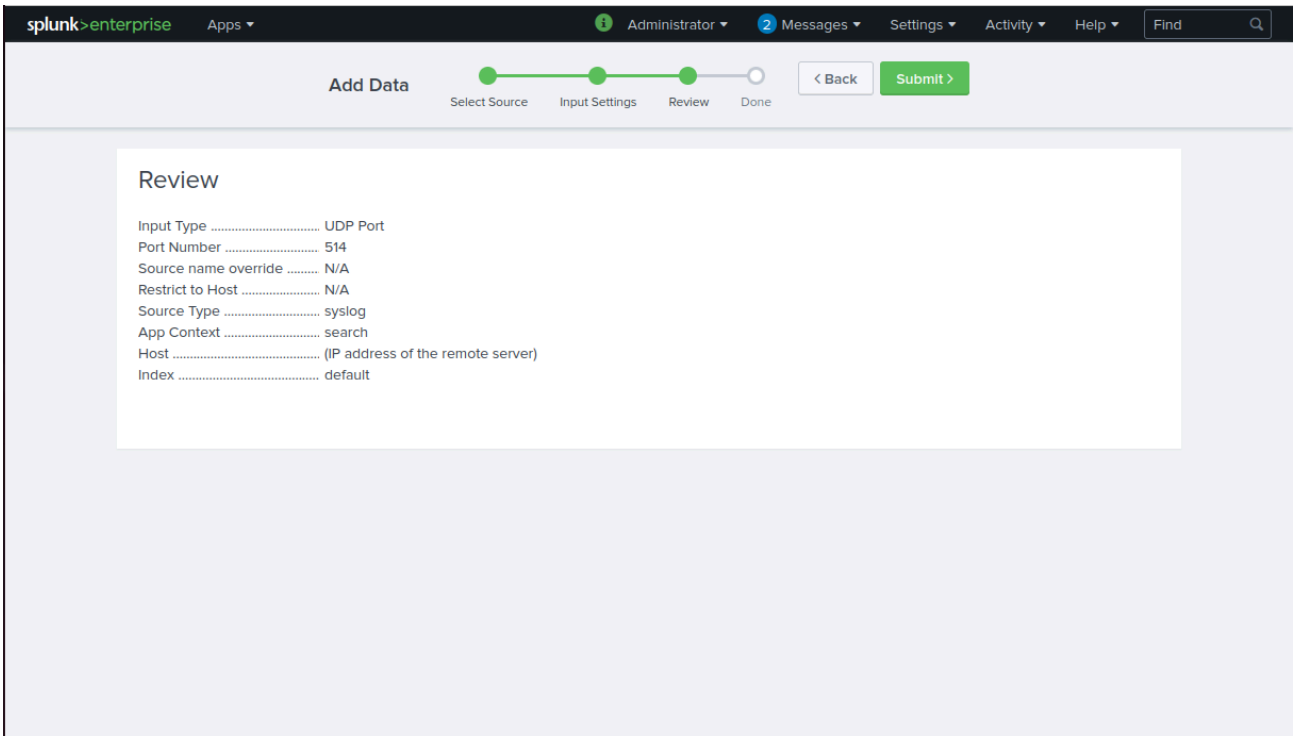


Figure 5.2.33: *Splunk's input settings overview – Diagram shows the input data settings overview.*

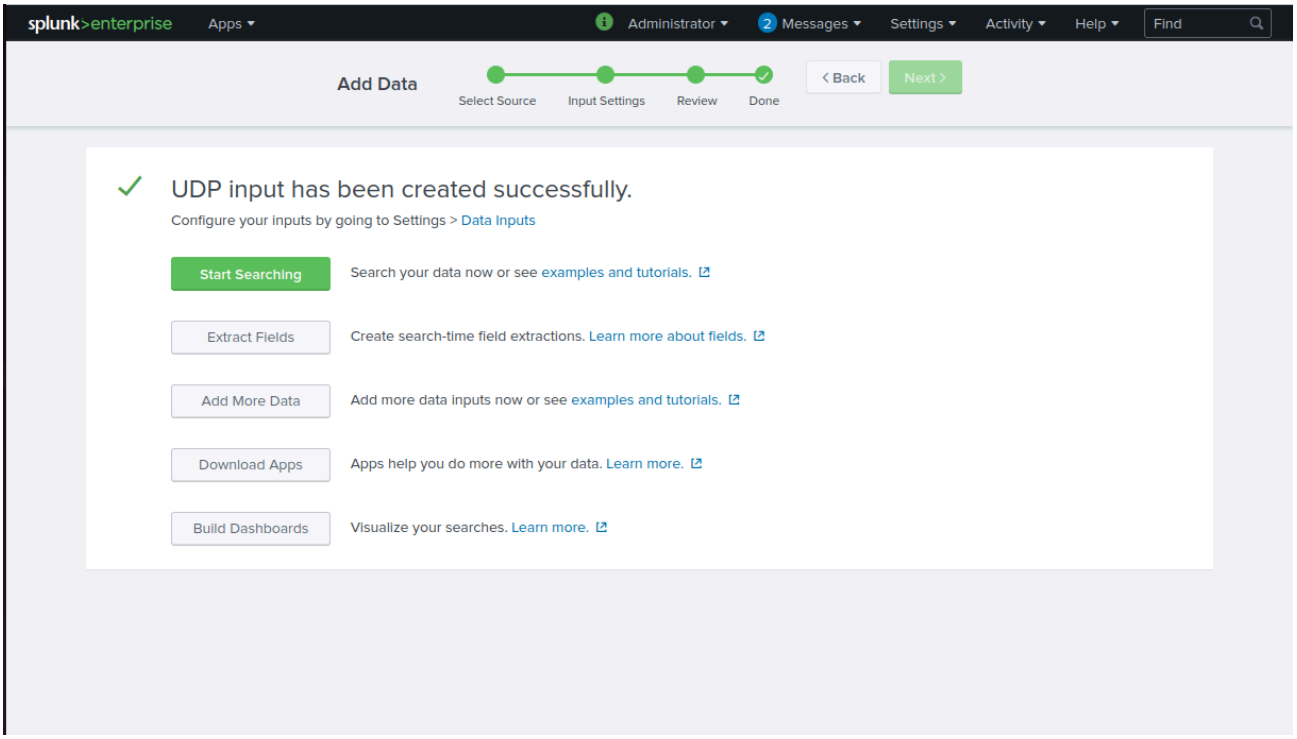


Figure 5.2.34: *Splunk's input settings has been set! – Diagram shows the input data settings are successfully set.*

- Using the snort app & search and reporting feature:

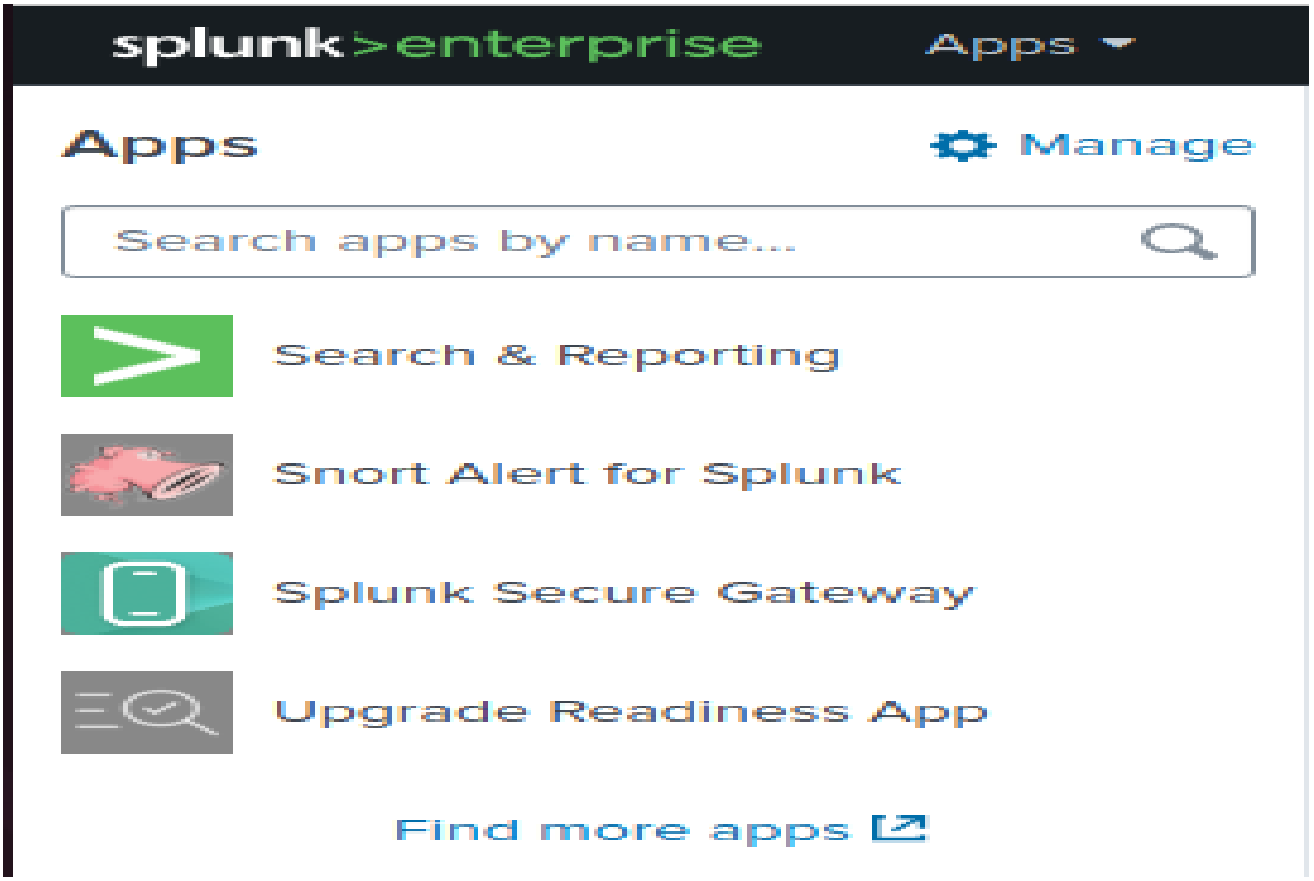


Figure 5.2.35: *Splunk's Apps – Diagram shows the available apps in splunk.*

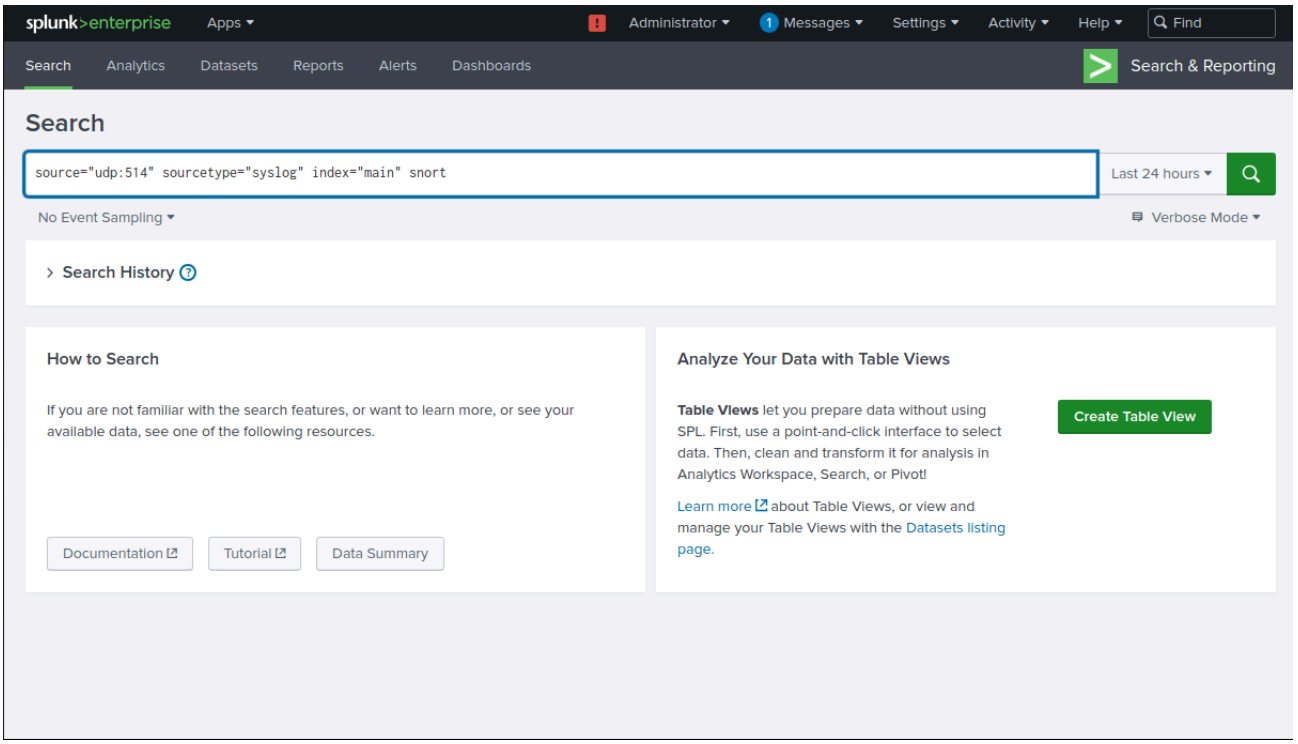


Figure 5.2.36: *Splunk's search and report app – Diagram shows the command used to filter out the logs in the search & report app.*

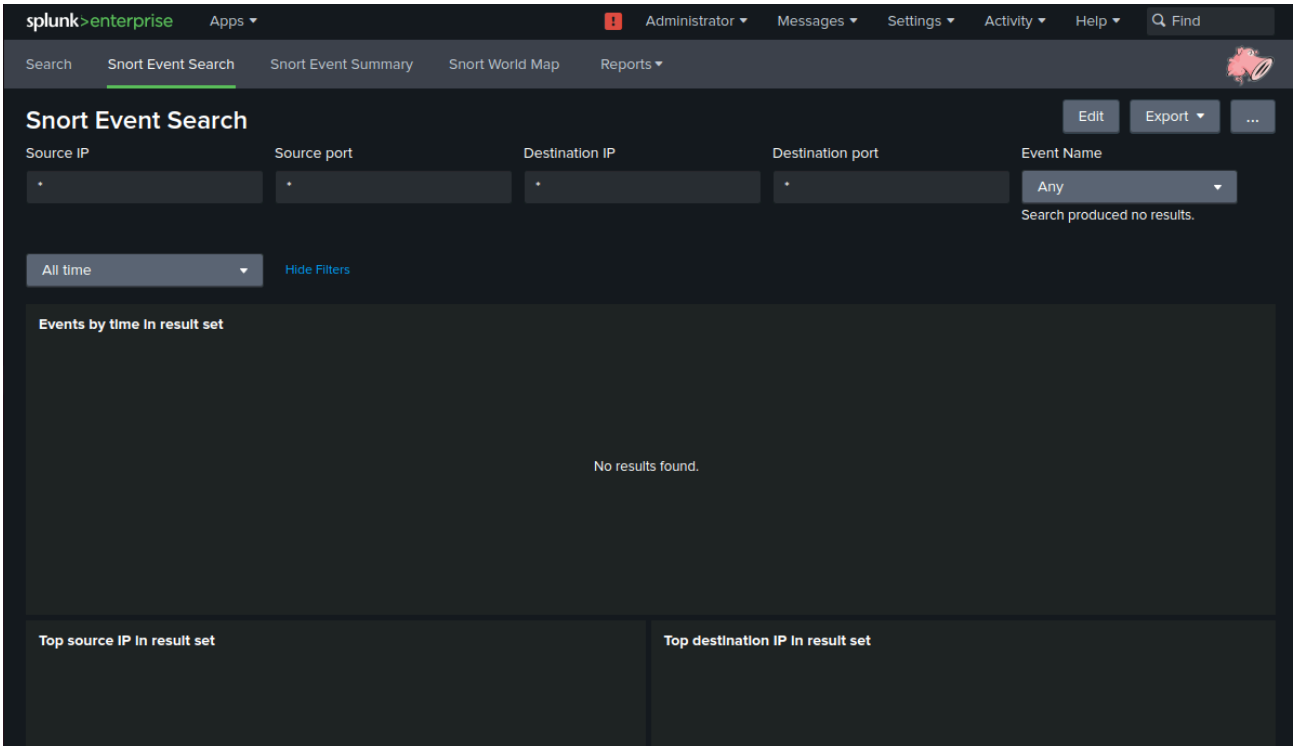


Figure 5.2.37: *Splunk's Snort app – Diagram shows the Snort app within splunk.*

- Sending alerts to the administrator's handheld device:

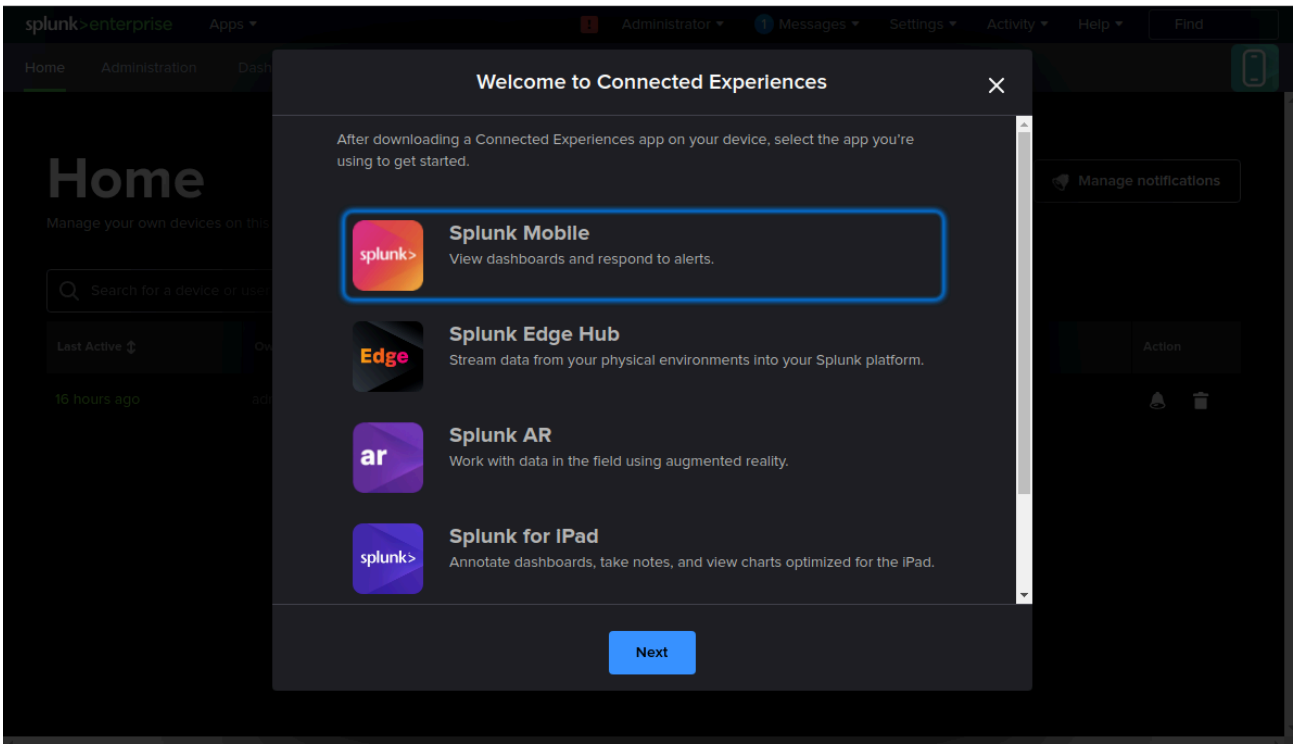


Figure 5.2.38: *Splunk mobile feature – Diagram shows as splunk's feature to review alerts using a handheld device.*

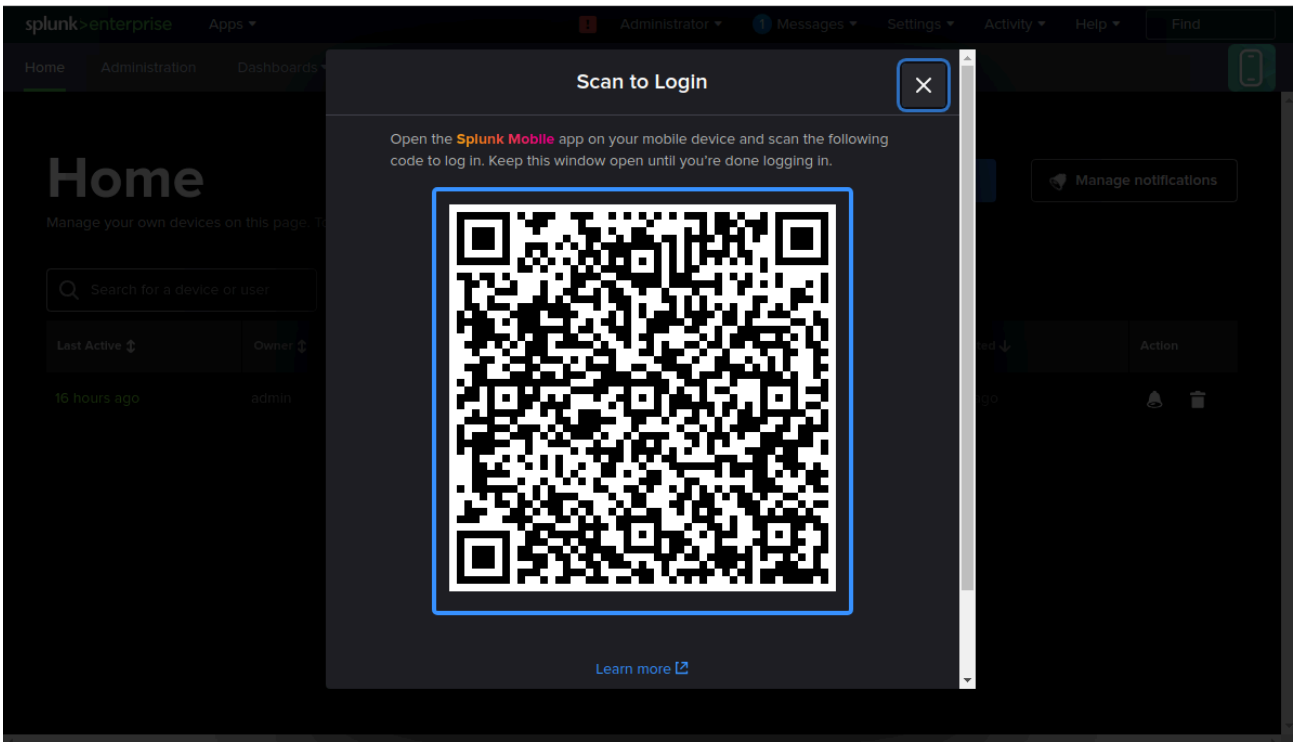


Figure 5.2.39: *Splunk mobile feature QR code – Diagram shows as splunk's feature to review alerts using a handheld device by scanning a QR code.*

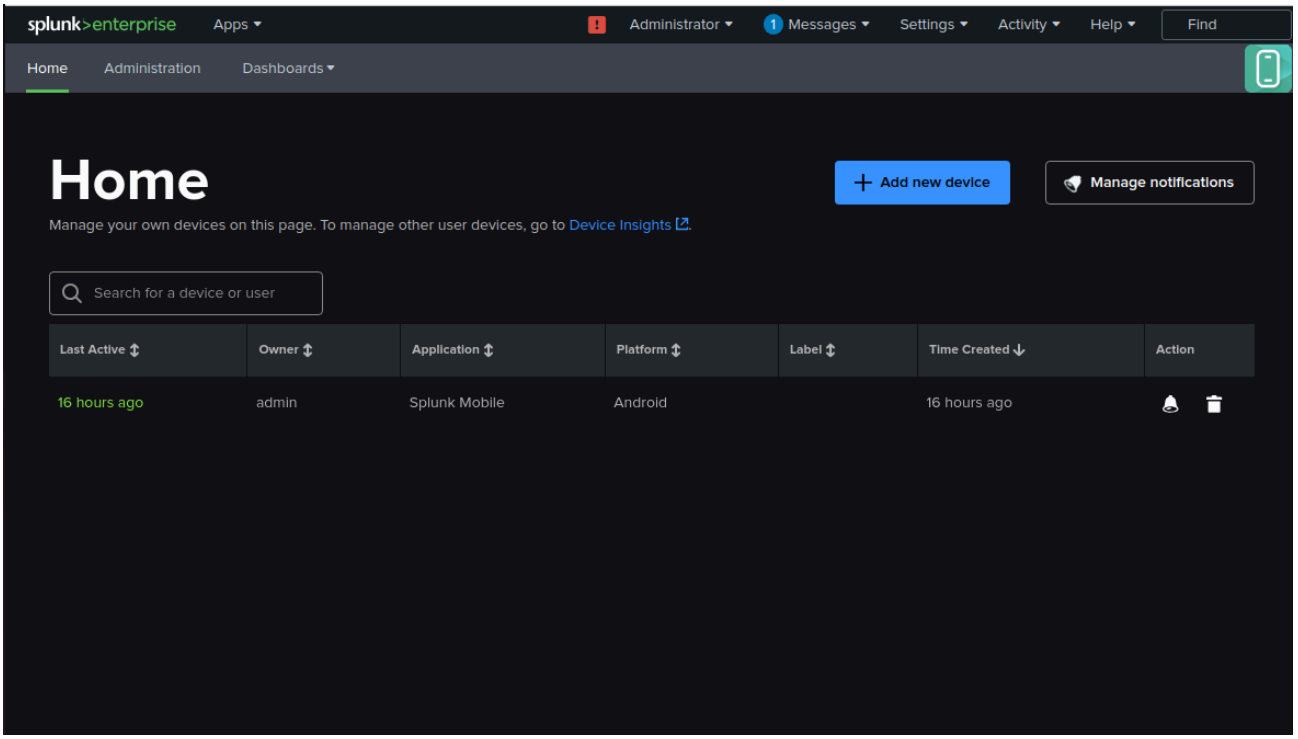


Figure 5.2.41: *Linked mobile devices list – Diagram shows list of connected devices*

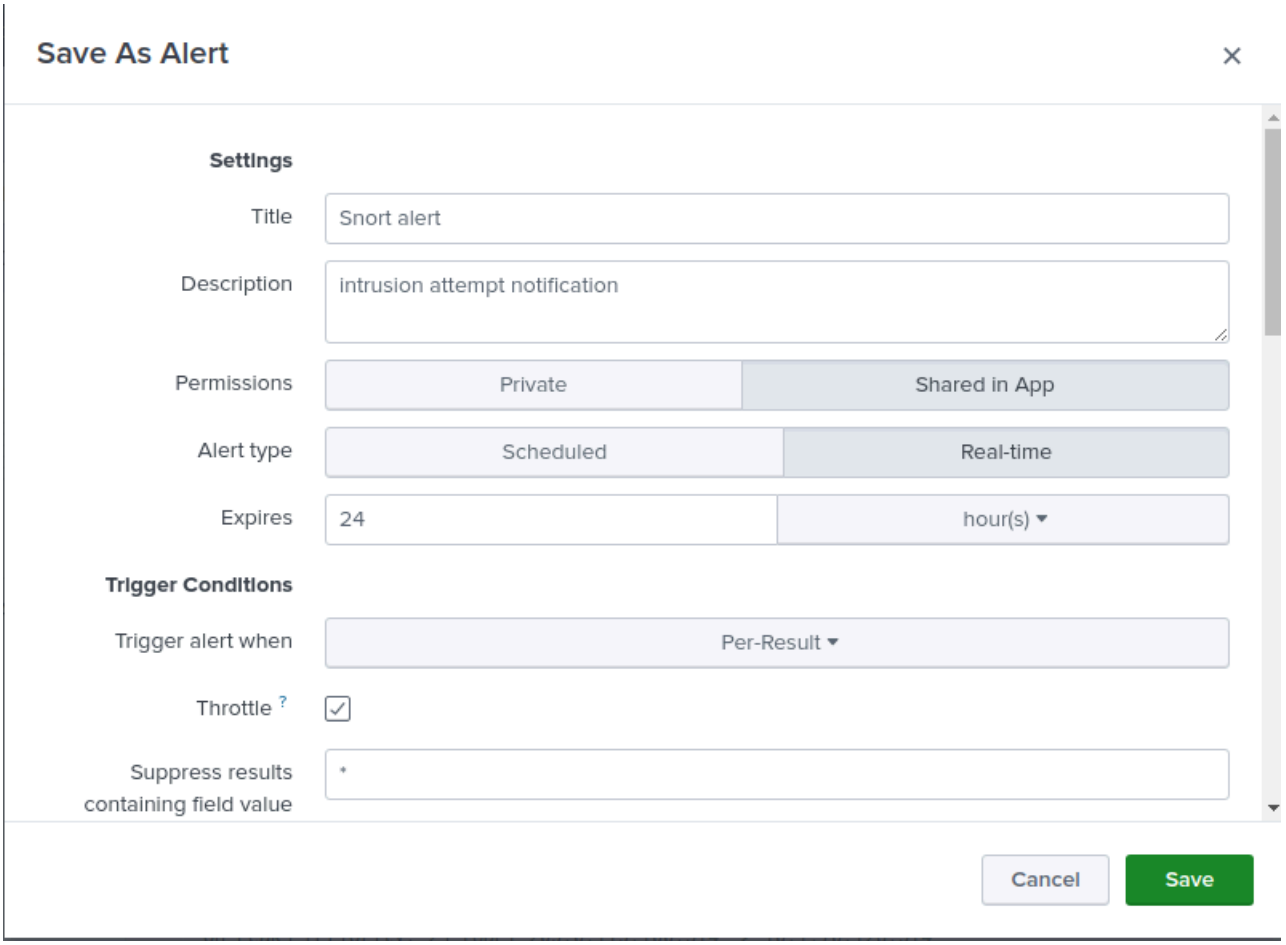


Figure 5.2.42: *creating a custom mobile alert – Diagram shows the customization of a snort that will be sent in real time which will be sent as soon as an event occurs.*

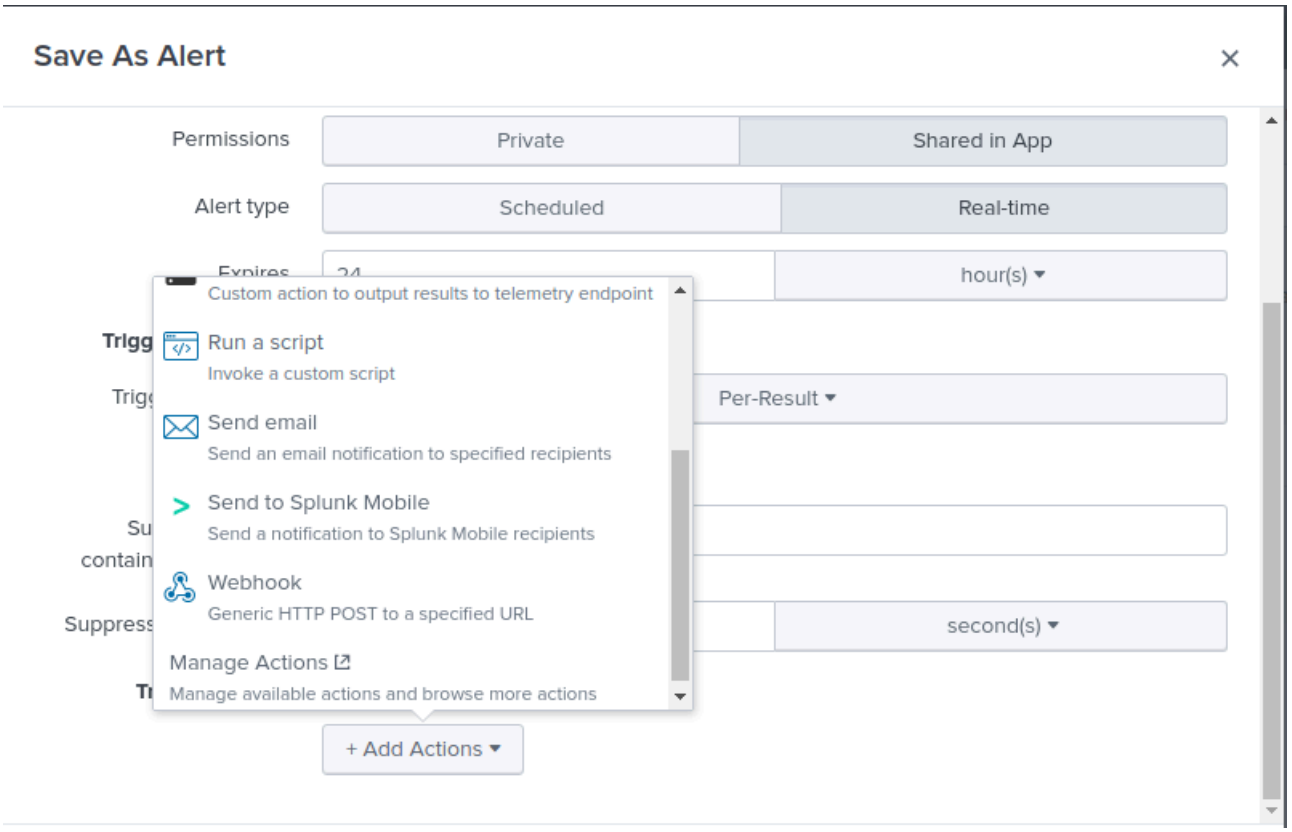


Figure 5.2.43: *send alerts using splunk mobile feature – Diagram shows a list of possible actions.*

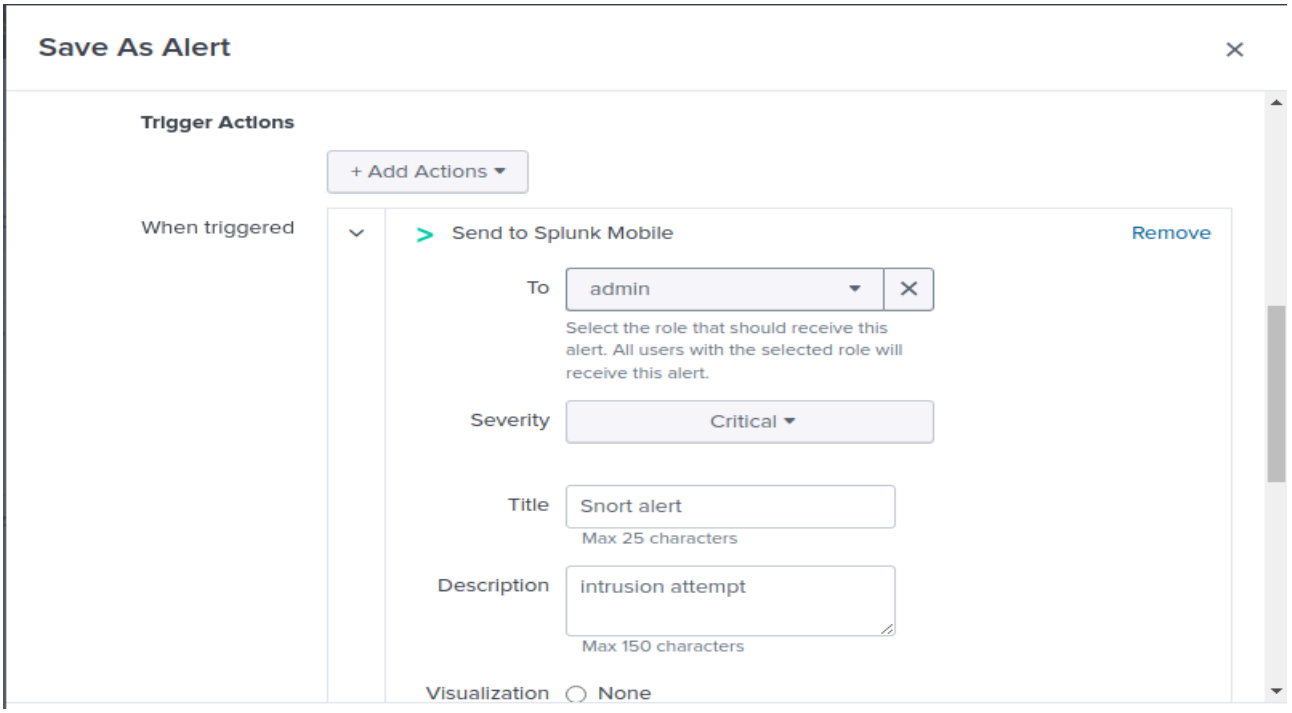


Figure 5.2.44: *Specifying the receiving user – Diagram shows that the alert will be sent in real time to the users (admins) handheld device with the indicated information.*

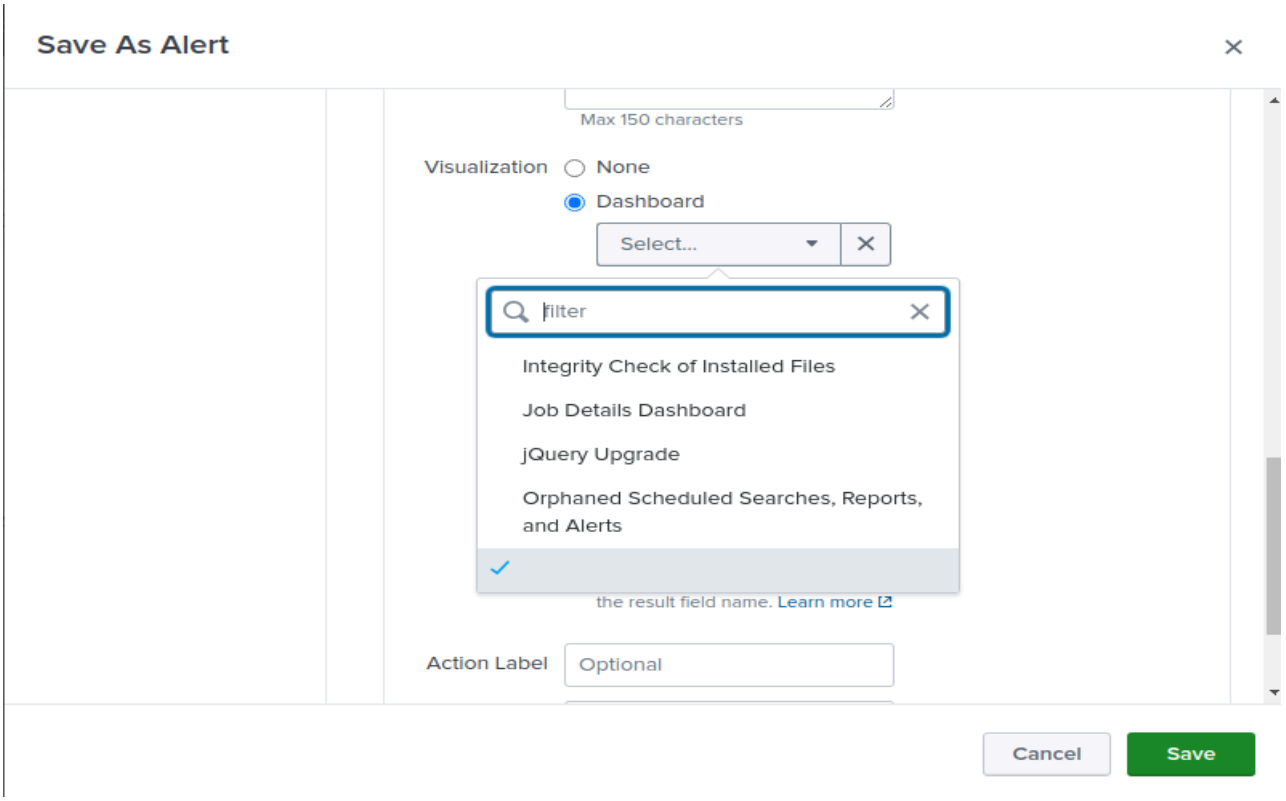


Figure 5.2.45: *Specifying the visuals – Diagram shows a list of possible visuals.*

Chapter 6: Quality Analysis and Testing

6.1. Test case and methodology

In this section of the documentation, we will be conducting the following tests:

- **Connectivity testing:** the connectivity between the devices from the 2 different branches and within the branches (internally and externally).

- **Malicious insider attack:** we will be simulating a malicious insider attack from the secondary branch (compromised branch)

- **Firewall rules:** We will be testing our firewall rules that have been set on a host.

6.2. Tools used for testing

The tools that we're going to be using during our testing phase:

- For the connectivity testing we will be using:
  - Wireshark: to capture the packets going back and forth.
  - ICMP packets: using the **ping** command on our VPCs
- For the malicious insider testing we will be using:
  - Nmap: which is an open-source network scanning tool that can be found pre-installed on a Kali Linux machine.
  - Snort: which is an open-source Intrusion Detection and Prevention System which is going to be logging any intrusion attempts.
  - Splunk: which is a software used to give a clear visual representation of the gathered logging information and generates a mobile notification to notify the admin to take an immediate action.
- For the firewall rules testing we will be using:
  - PfSense: which allows us to implement firewall rules on the dedicated interface.

6.3. Test Results

❖ Connectivity Testing:

Step 1 (Internal connectivity):

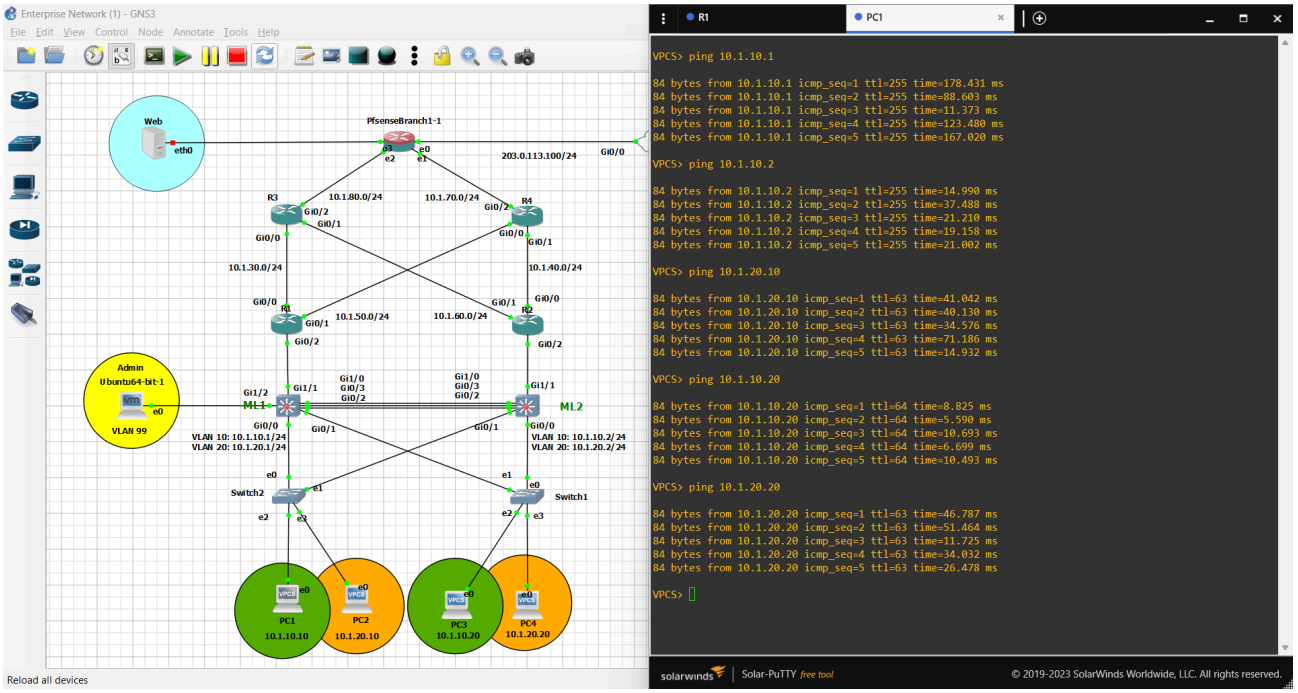


Figure 6.3.1: *PC1 connectivity (1) – Diagram shows that PC1 was able to reach all the devices within the access layer as well as the multi-layer switches.*

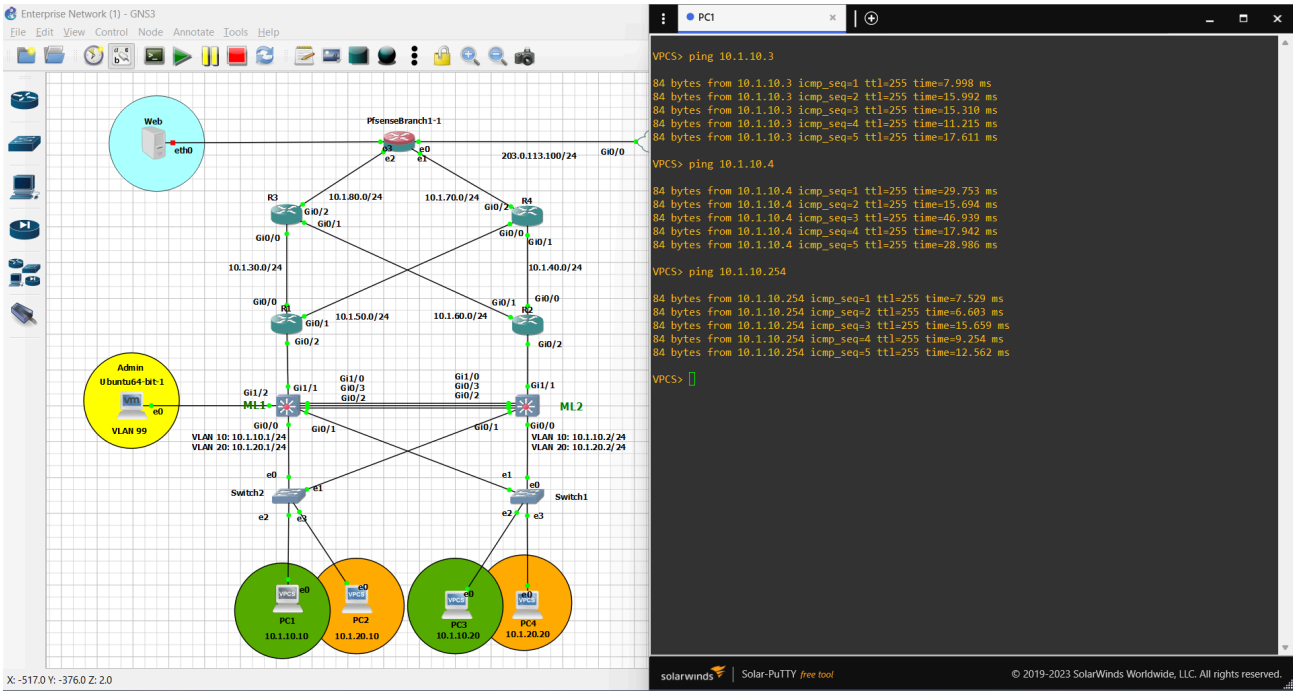


Figure 6.3.2: *PC1 connectivity (2) – Diagram shows that PC1 was able to reach its own default gateway as well as R1 & R2 interfaces (facing the internal network).*

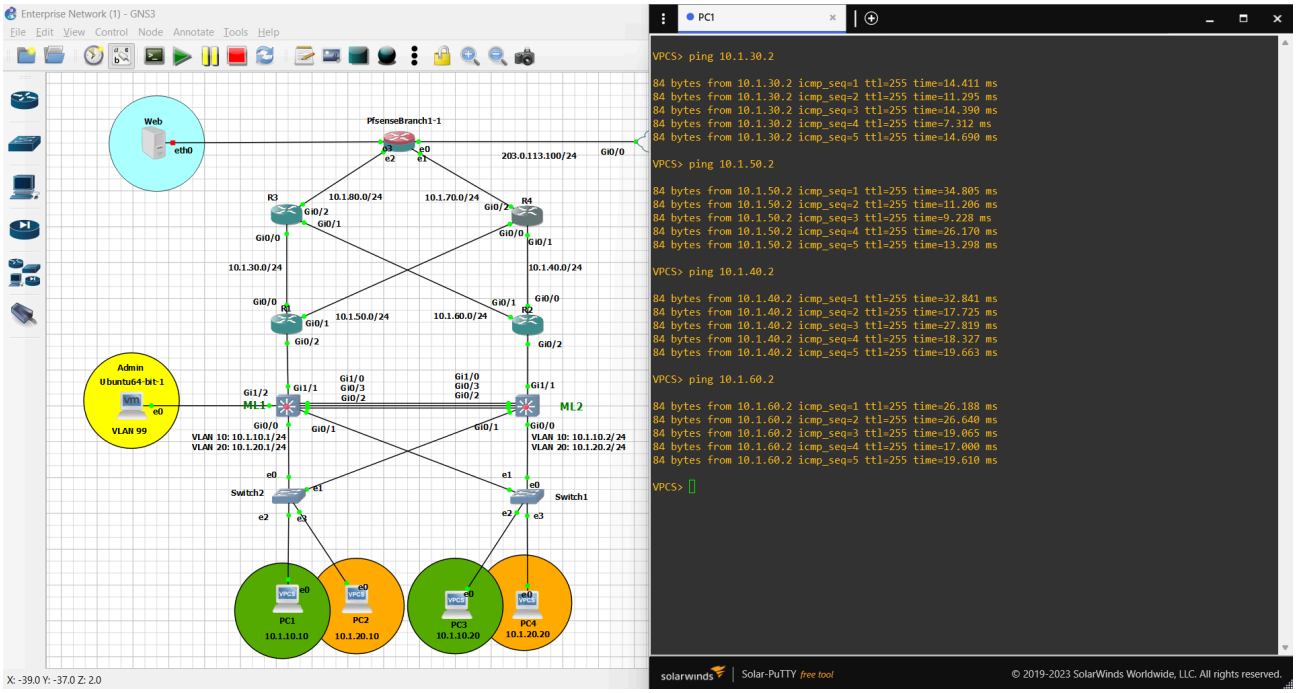


Figure 6.3.3: *PC1 connectivity (3) – Diagram shows that PC1 was able to reach R1 & R2 interfaces (facing the ISP)*

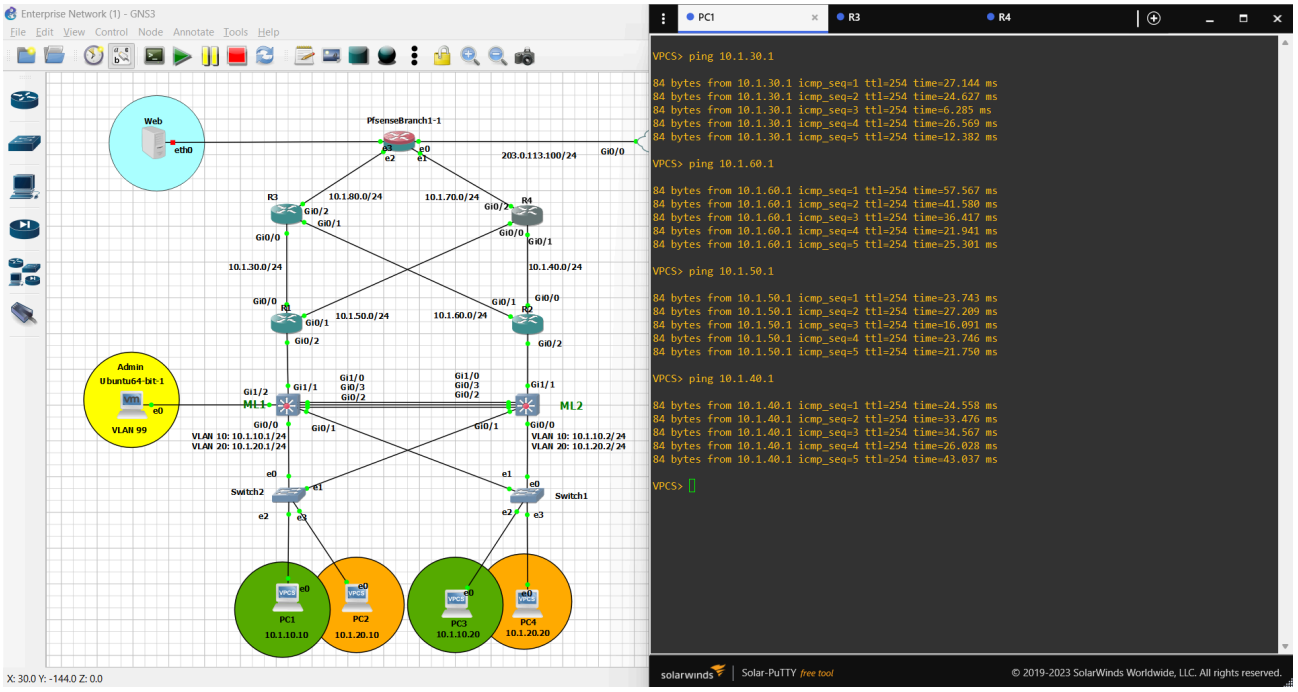


Figure 6.3.4: *PC1 connectivity (4) – Diagram shows that PC1 was able to reach R3 & R4 interfaces (facing the internal network)*

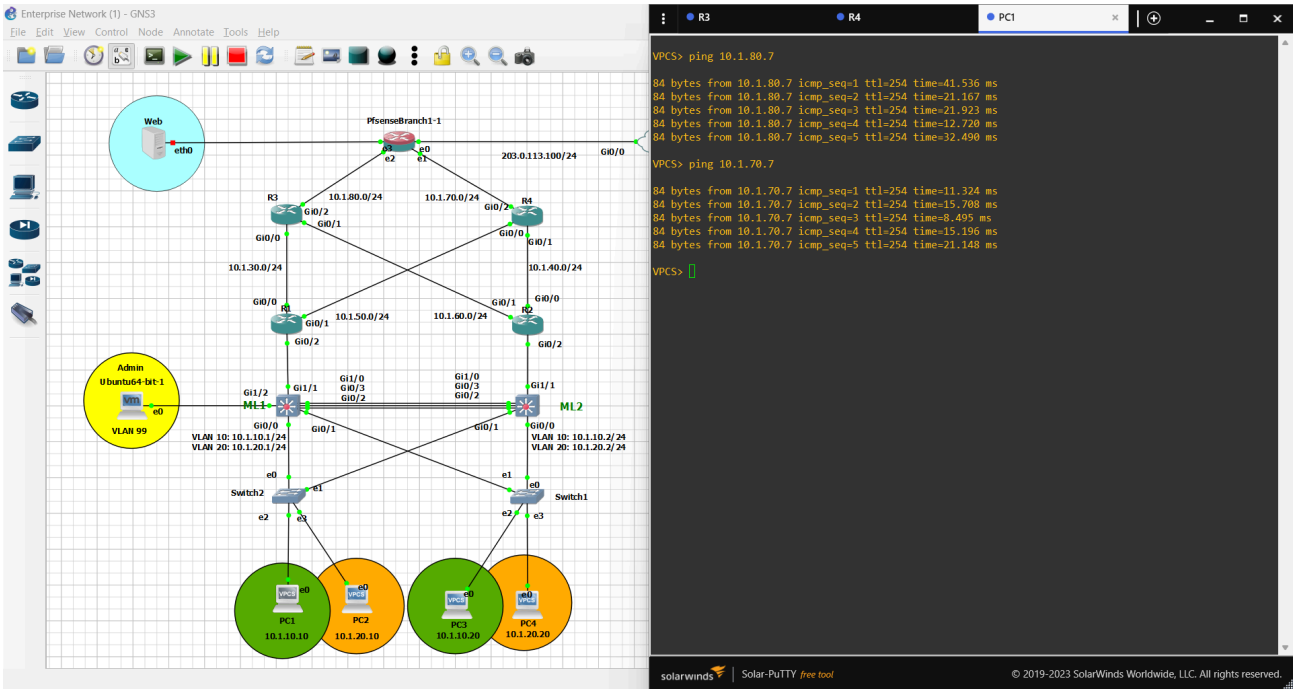


Figure 6.3.5: *PC1 connectivity (5) – Diagram shows that PC1 was able to reach R3 & R4 interfaces (facing the ISP)*

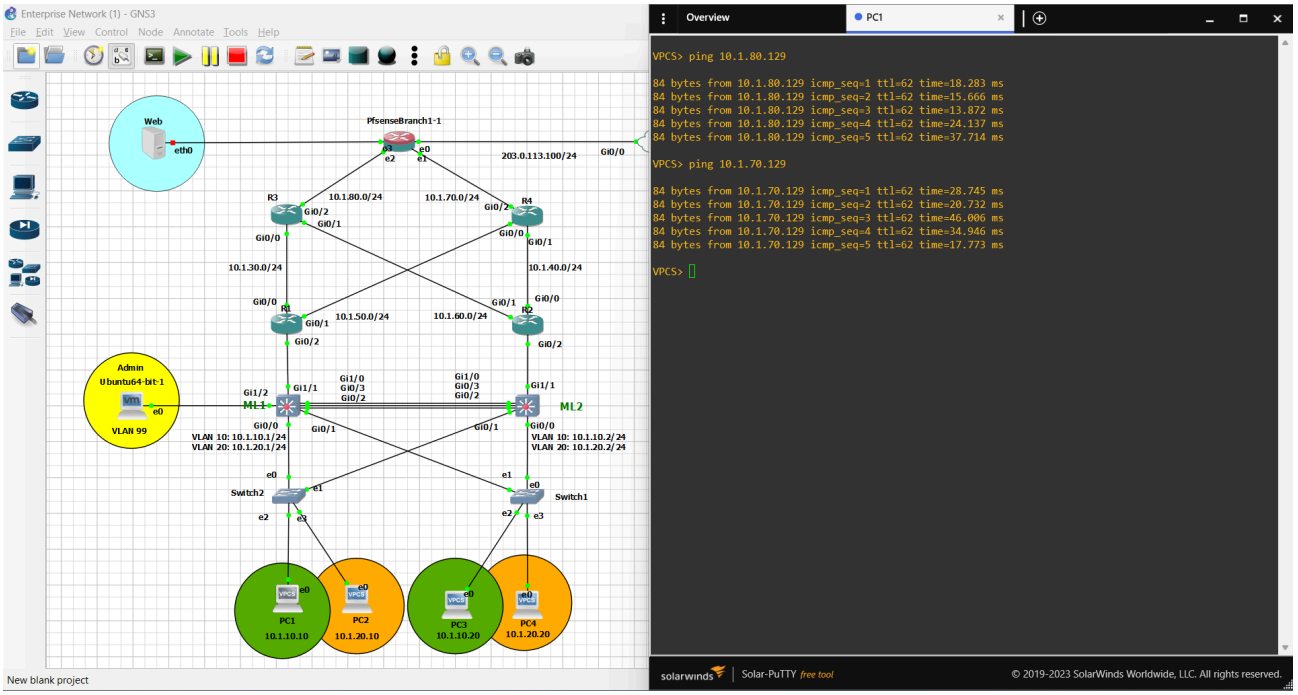


Figure 6.3.6: *PC1 connectivity (5) – Diagram shows that PC1 was able to reach the pfsense interfaces (facing the internal network)*

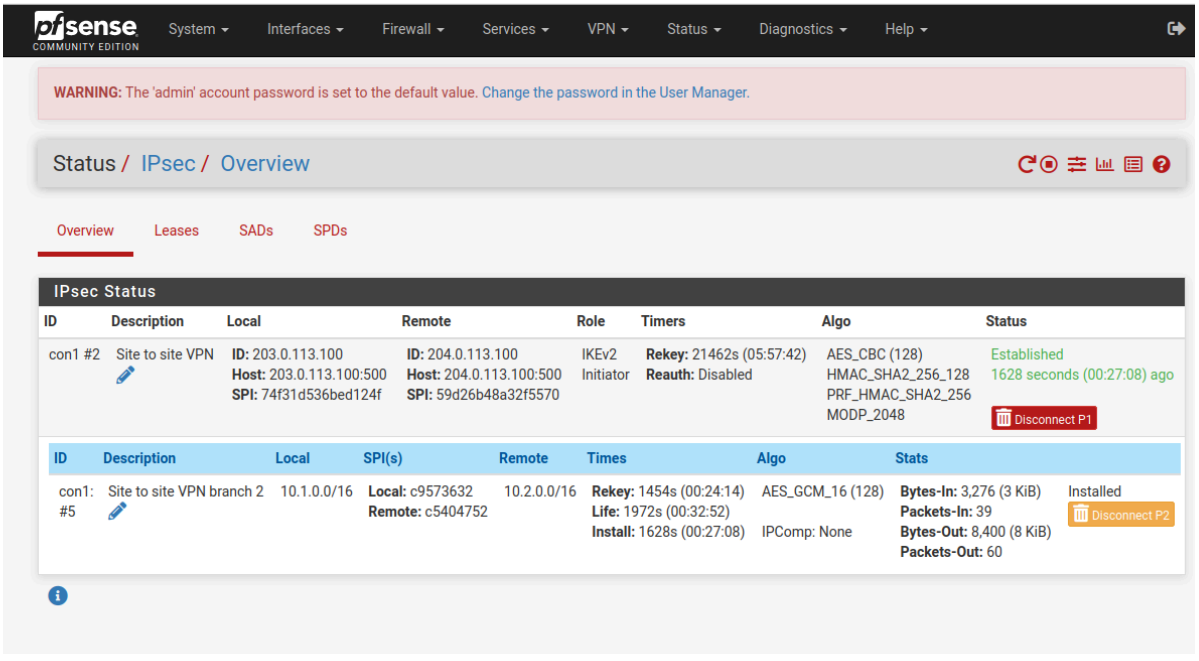
Step 2 (external connectivity):

Step 2.1 (through the intranet):

Intranet: Before we are able to communicate from branch to branch through the intranet rather than the internet, we had to establish a valid and secure connection that can only take place between the devices within the designated branches (HQ and the Secondary branch), in which we set up a secure site-to-site virtual private network (VPN) with the appropriate encryption methods using the IPsec protocol and specified the allowed devices to communicate across the VPN.

Establishing our VPN using the IPsec protocol:

Branch 1 (HQ) VPN/IPsec establishment:



Branch 2 (Second Branch) VPN/IPsec establishment:

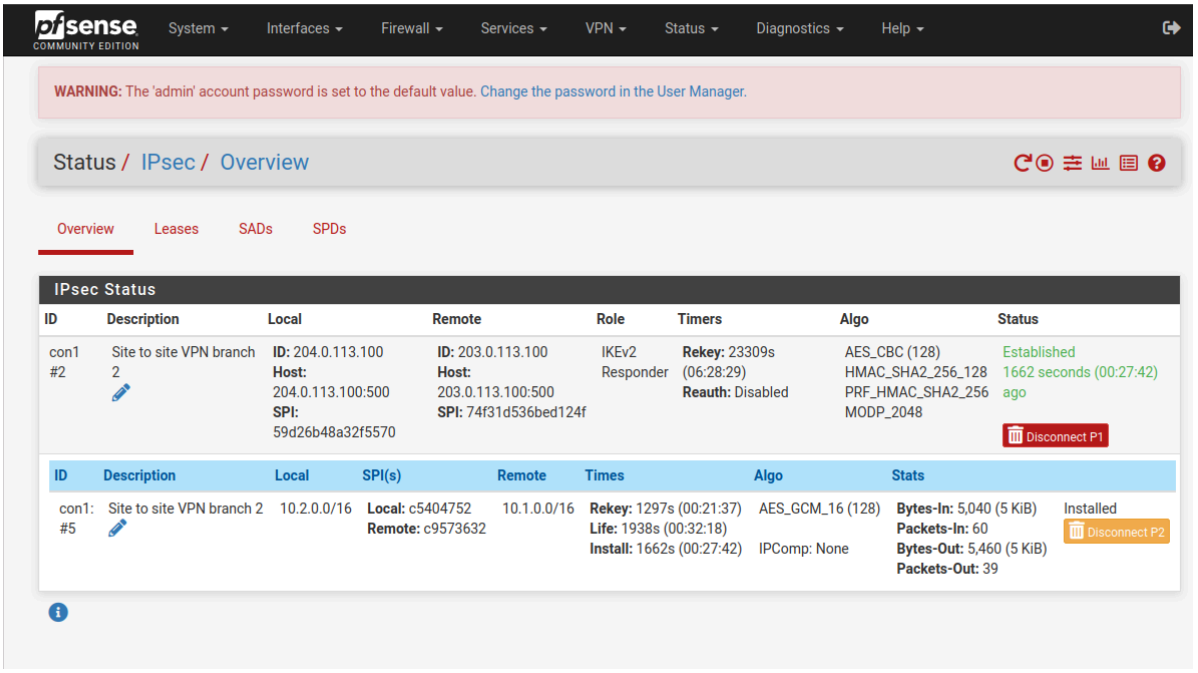


Figure 6.3.8: *Branch 2 VPN/IPsec Setup - Diagram showing the configuration of VPN/IPsec at Branch 2 for secure connectivity with Branch 1 and the broader network infrastructure.*

PC1 from branch 1 (HQ) is able to ping PC 5 in branch 2 (second branch) and vice versa:

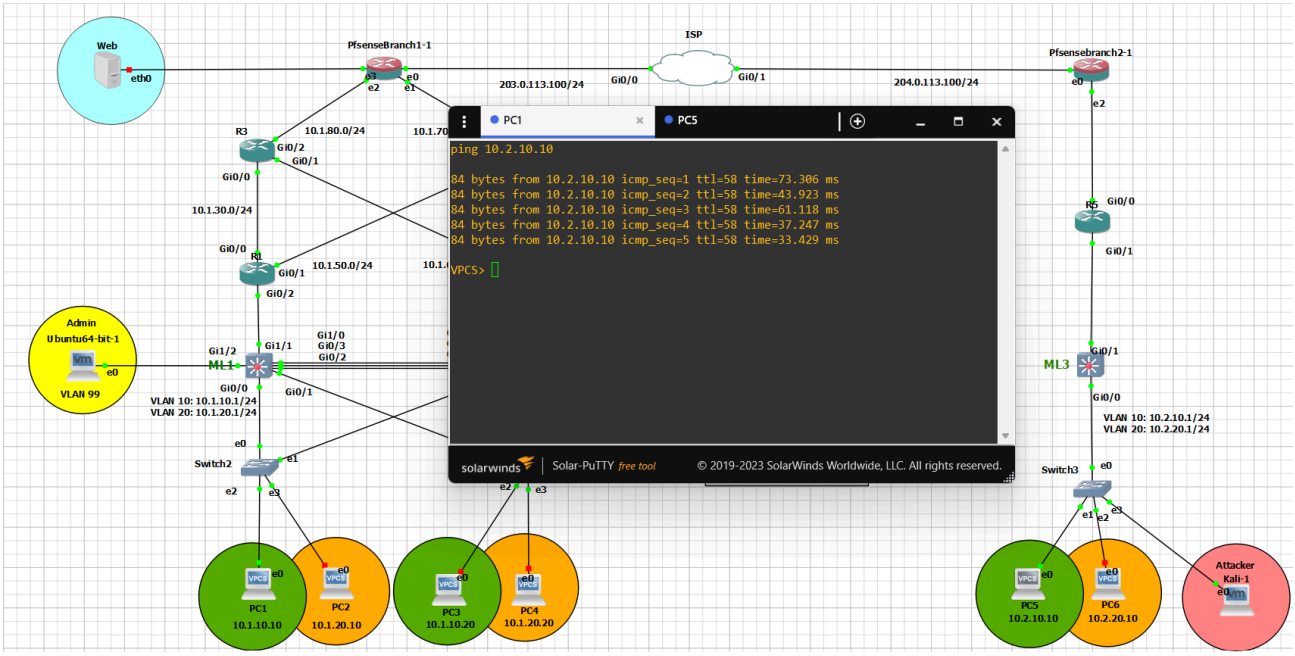


Figure 6.3.9*: PC1 Ping to PC5 (Branch 2) - Illustration showing PC1 from Branch 1 (HQ) successfully pinging PC5 in Branch 2 (Second Branch).*

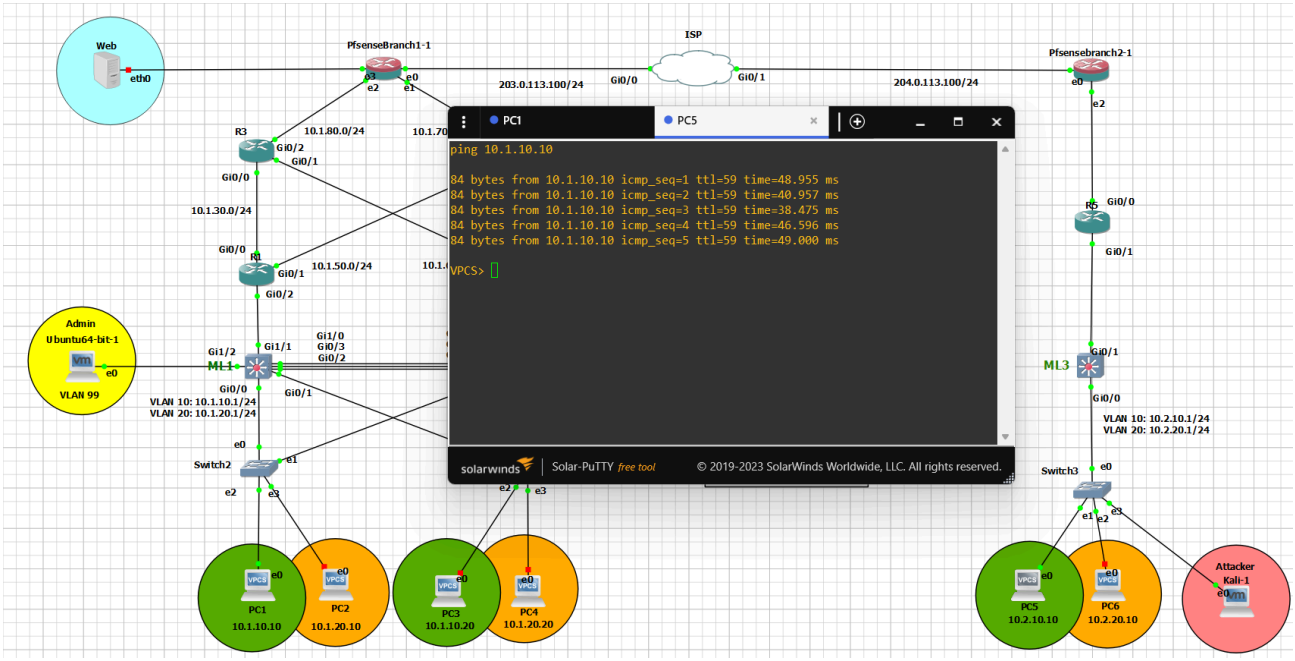


***Figure 6.3.10**: PC5 Ping to PC1 (Branch 1) - Diagram demonstrating PC5 from Branch 2 (Second Branch) successfully pinging PC1 in Branch 1 (HQ).*

Step 2.2 (through the internet):

Internet: Before were able to allow the devices within the branches to communicate with the outside world (through the internet), we configured a NAT overload (PAT) to each of the devices private IP address in which we assigned a single public IP address for each of the devices based on its unique port number thinking about communicating with the outside world.

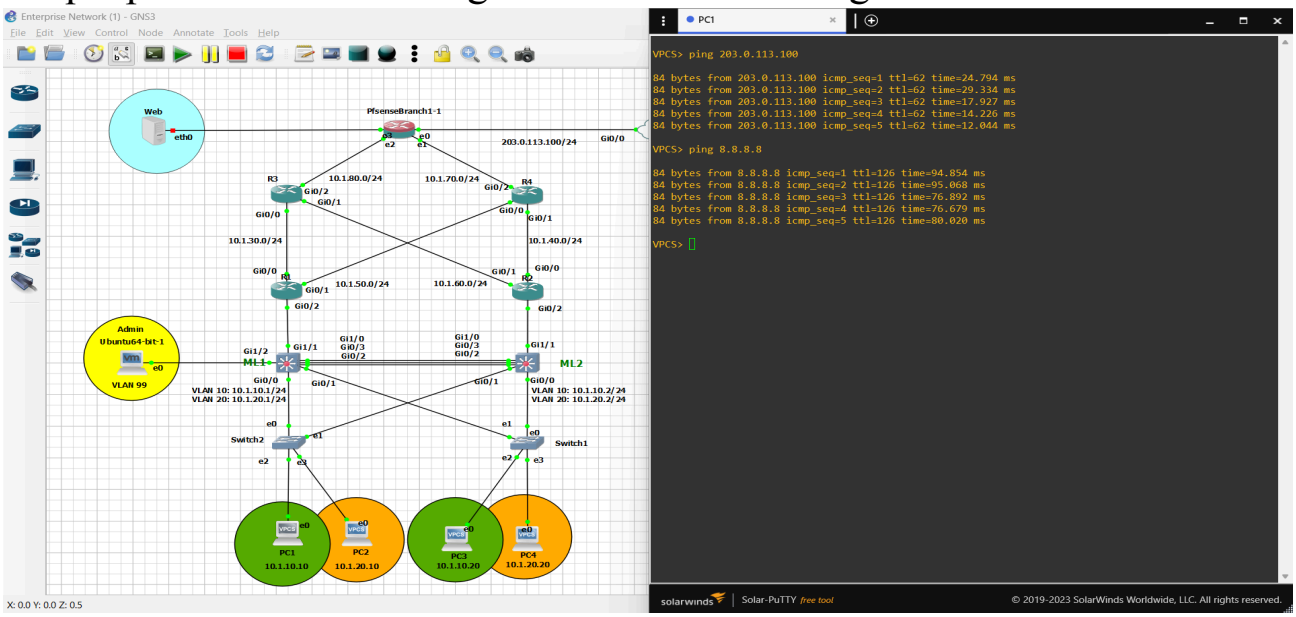


Figure 6.3.11: PC1 (Branch 1) external connectivity - Diagram demonstrating PC1 is able to reach external networks with the use of NAT overload.

❖ Malicious insider attack:

In this testing methodology we will be demonstrating the following scenario:

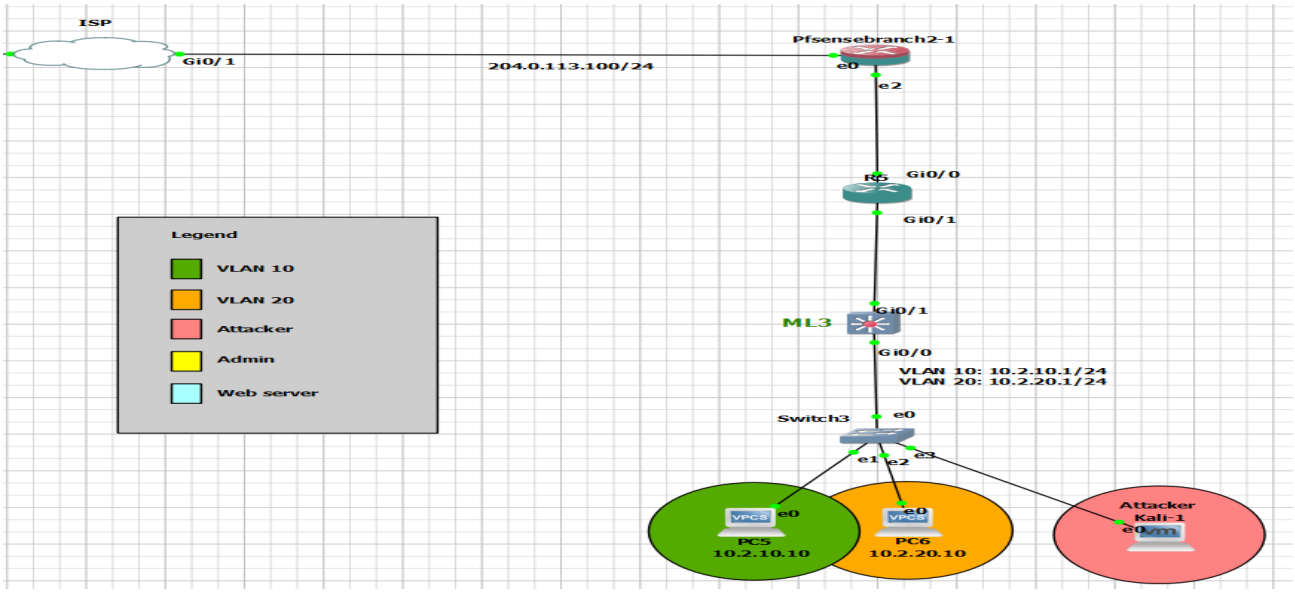


Figure 6.3.11: Kali Linux in the second branch - Diagram showing the placement of the attacker's device (Kali-1)

- The malicious insider (Kali Linux machine) was able to gain access to the second branch's switch in which he/she poses as one of the devices that belongs to VLAN 10 with IP address of 10.2.10.11.
- The pfsense in Branch 2 (second branch) wouldn't inspect any traffic coming through it from the internal network as its main role is to block any external threats, in which the traffic would pass on freely on to branch 1 (HQ) through the VPN/IPsec.

- VPN/IPsec has been configured to allow any traffic incoming from the devices in the IP range of 10.2.0.0 to be delivered to the other branch (HQ), in which the VPNs main role is to secure the communications coming from within the branches which in our scenario, traffic coming through from the malicious attacker with IP address 10.2.10.11 would certainly pass through the VPN/IPsec without any issue.

- Finally, the attacker reaches the pfsense firewall/router on its WAN interface (203.0.113.100) in the HQ branch in which the pfsense would be able to detect an intrusion attempt (with the use of snort) caused by the attacker

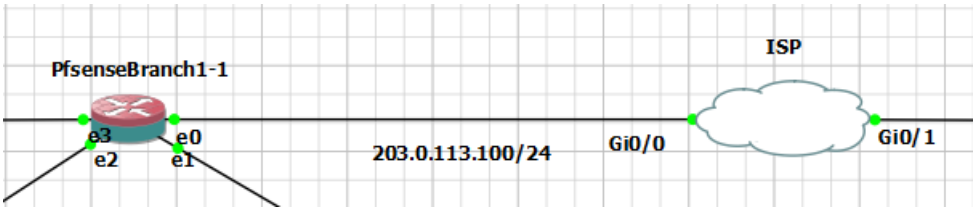


***Figure 6.3.12**: Pfsense connection with the ISP in HQ- Diagram showing the pfsense in the HQ branch connected to the ISP.*

Important note: This type of attack can be mitigated using many different approaches (example: Setting up an authentication server for the users within the branches such as an active directory server, port security on the switch & VPN restrictions), but for the sake of this scenario we would want to highlight the effectiveness of the PfSense router/firewall in the HQ branch.

Now that we've covered the aspects of how a malicious user is able to reach the WAN interface on the HQ branch, let us demonstrate the actual attack.

- Kali Linux connectivity:

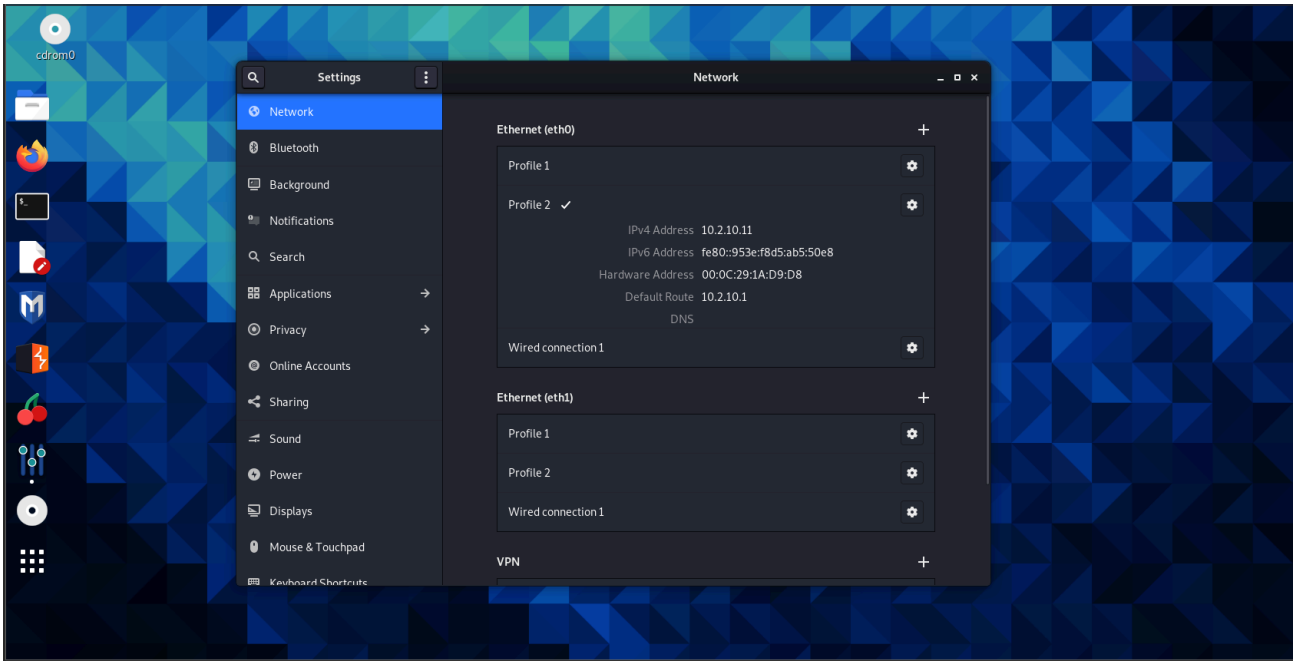


***Figure 6.3.13**: Kali Linux network settings - Diagram showing IP address of the Kali Linux device.*

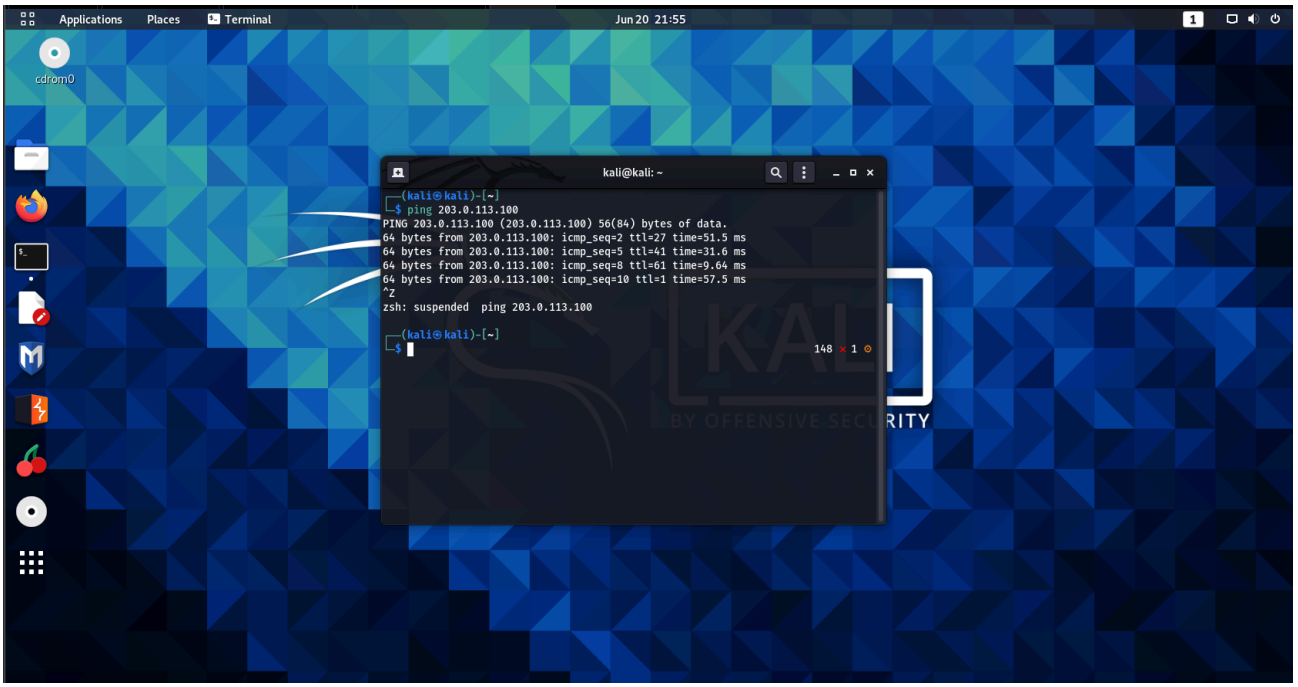


***Figure 6.3.14**: Kali Linux connectivity - Diagram showing that the Kali linux machine is able to reach the WAN interface of the pfsense in the HQ branch.*

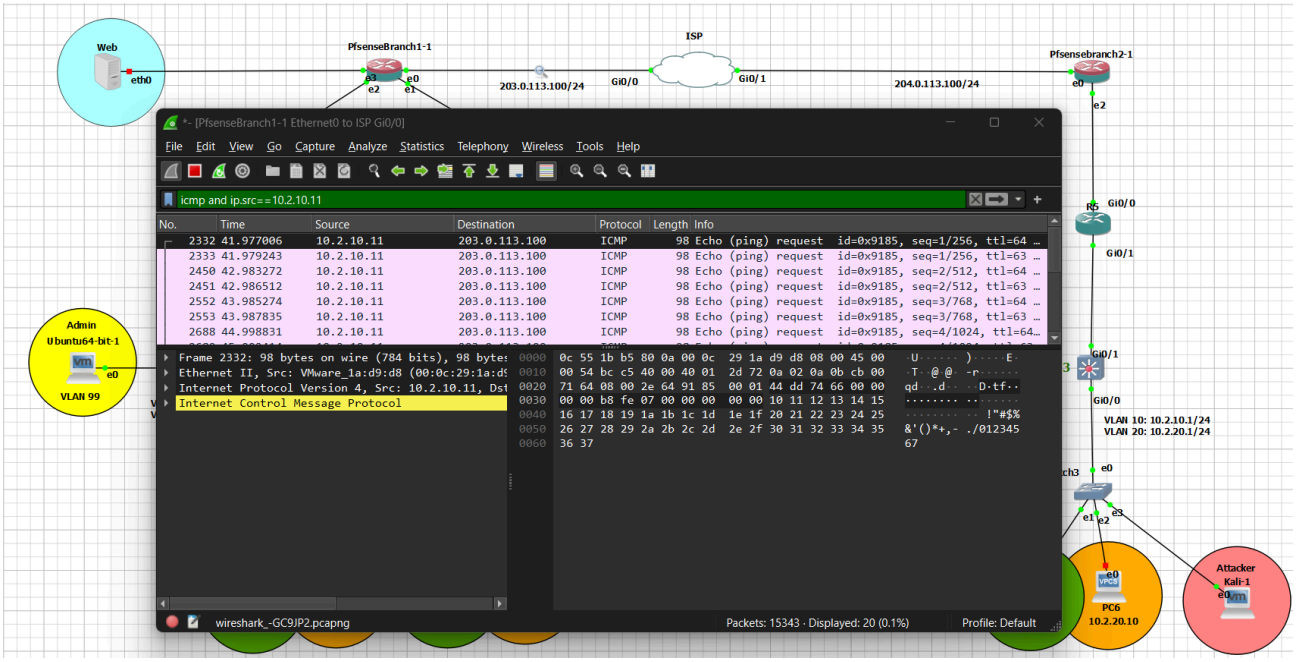


***Figure 6.3.15**: Wireshark analyzing the ping request - Diagram showing that Wireshark was able to capture the ping request sent by the kali linux user on pfsense's WAN interface.*

- Nmap:

Commands used:

sudo nmap -sS -p 1-1000 203.0.113.100
sudo nmap -sU -p 1-1000 203.0.113.100

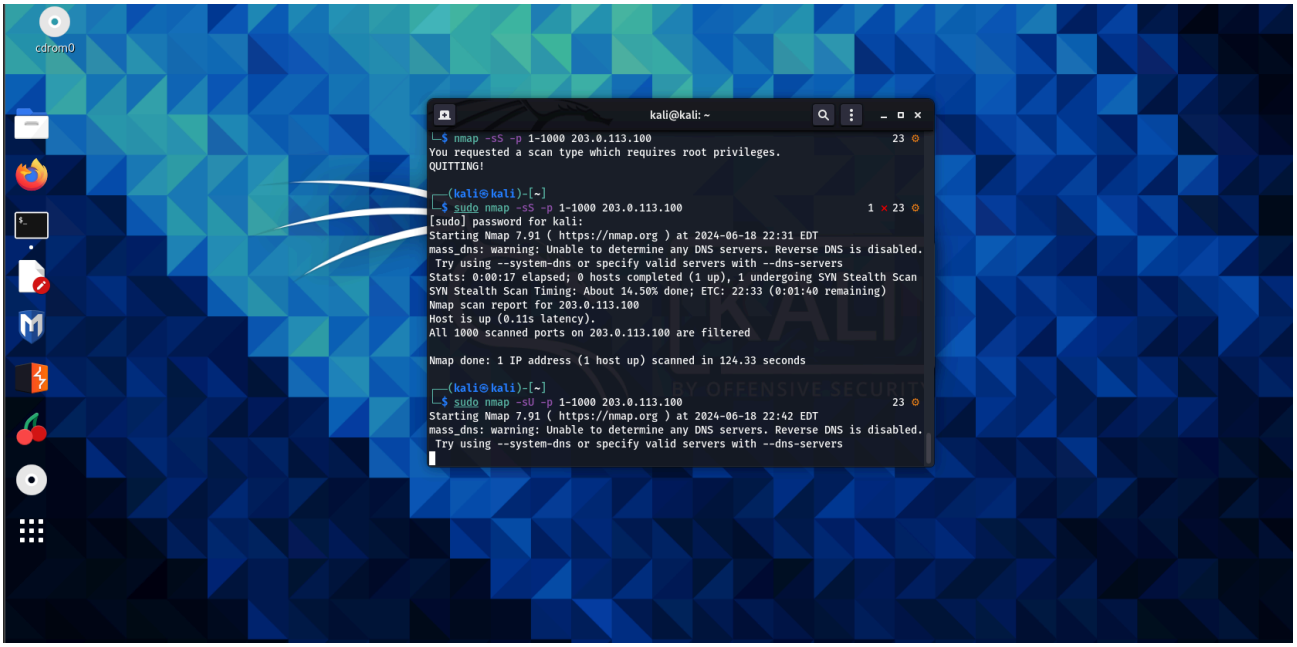


***Figure 6.3.16**: Kali Linux Nmap comands- Diagram showing that the Kali linux is performing a nmap SYN and a UDP scan to scan the ports on the pfsense WAN interface.*

- Snort and Wireshark detection

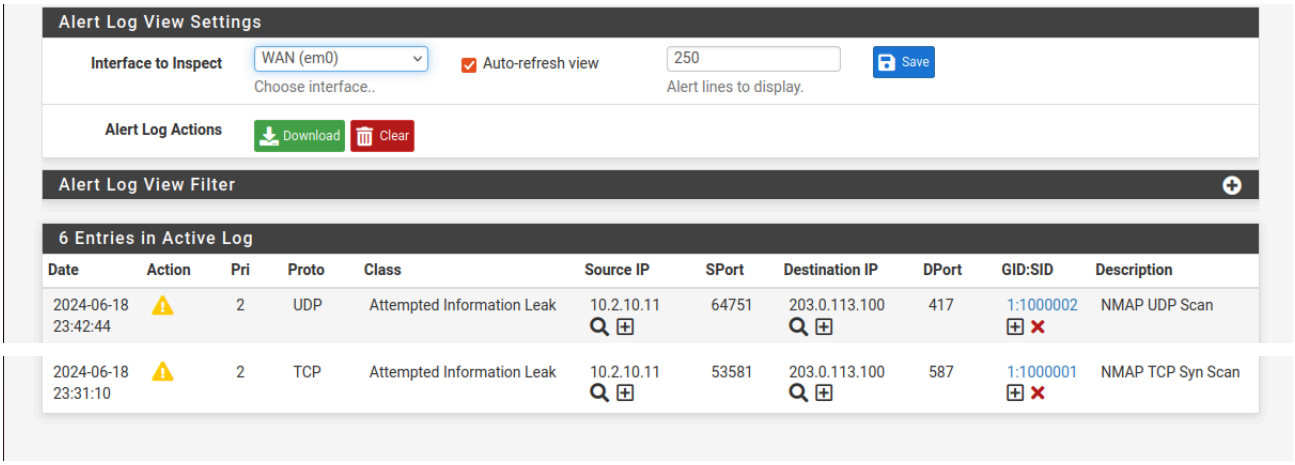


***Figure 6.3.17**: Snort Alerts - Diagram showing that snort was able to detect the intrusion attempt on the pfsense {HQ) WAN interface and displayed all the details concerning the attempt in real time (including the intruders ip address and the type of intrusion attempt).*

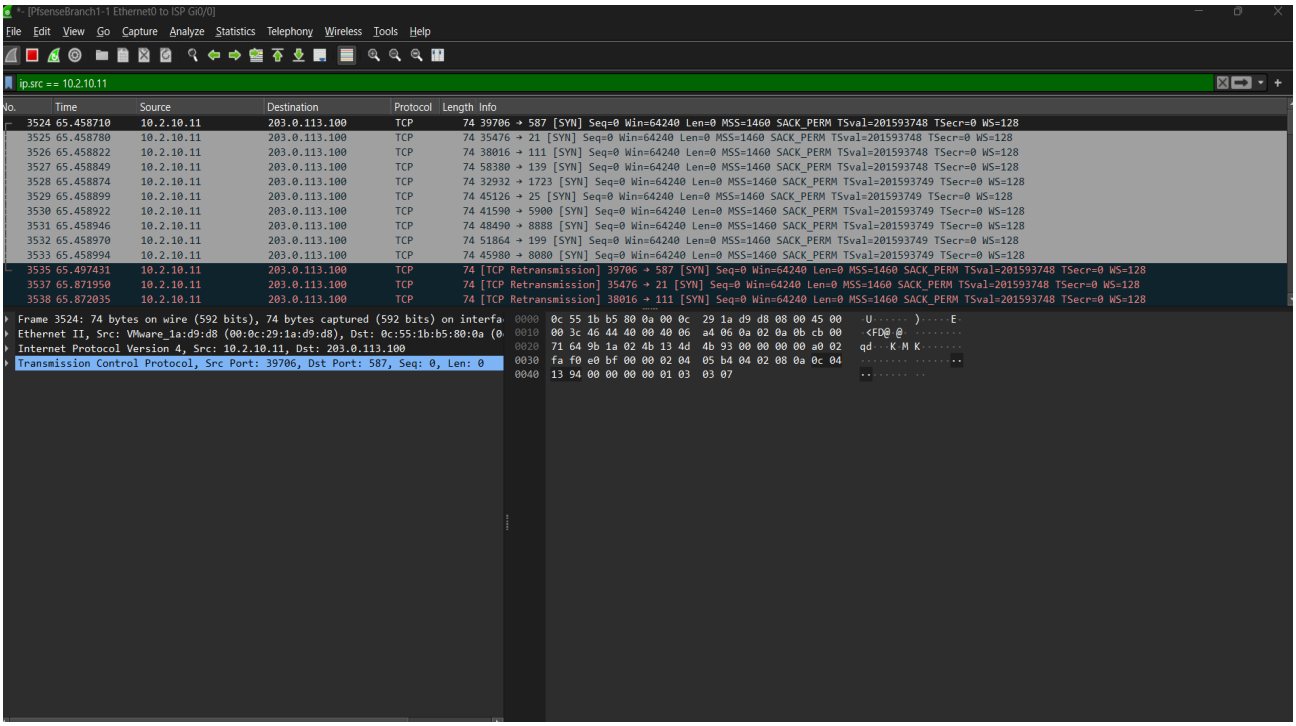


***Figure 6.3.18**: Wireshark inspection of the TCP scan (1)- Diagram showing that Wireshark was able to capture the TCP scan packets that was destined to the WAN interface.*

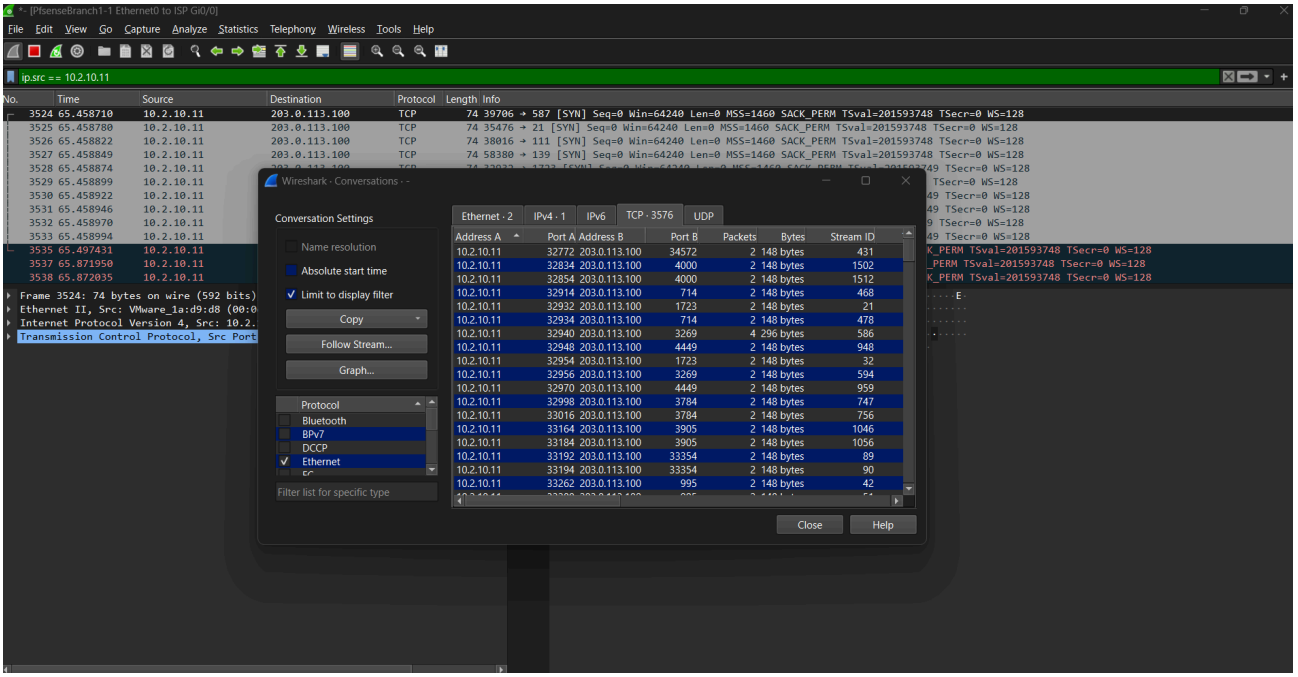


***Figure 6.3.19**: Wireshark inspection of the TCP scan (2)- Diagram showing that Wireshark is displaying the packets details.*

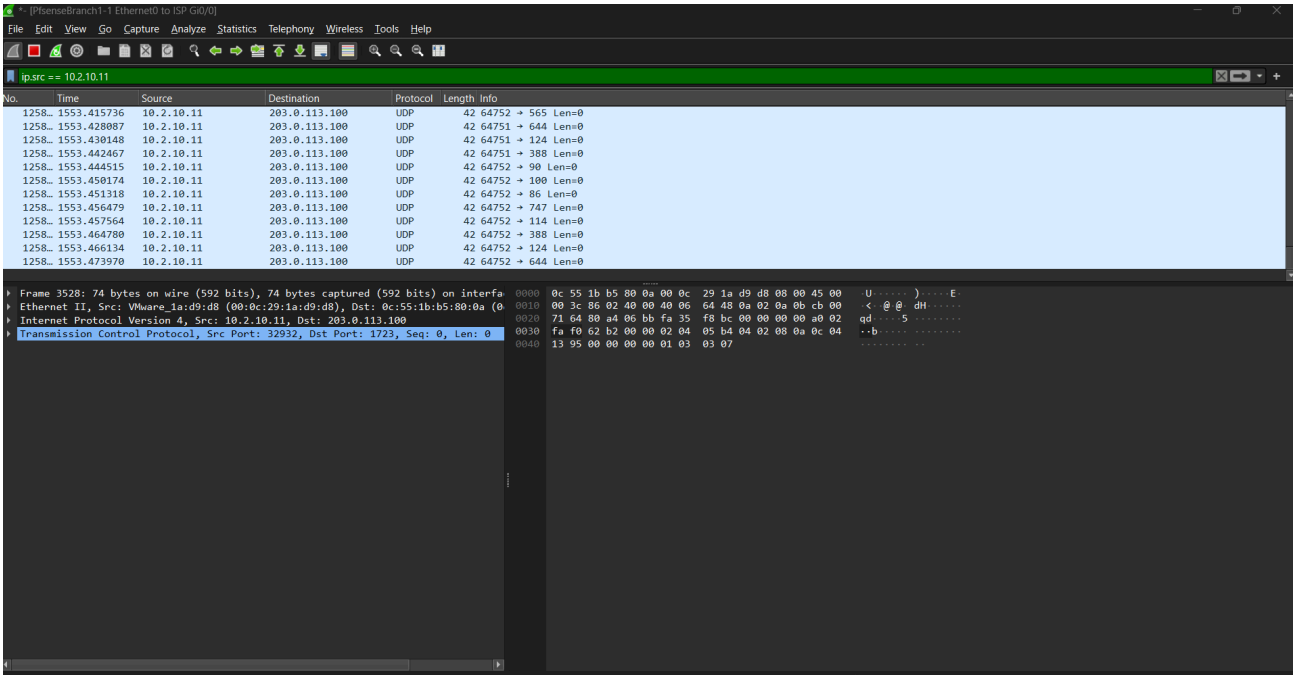


***Figure 6.3.20**: Wireshark inspection of the UDP scan (1)- Diagram showing that Wireshark was able to capture the UDP scan packets that was destined to the WAN interface.*

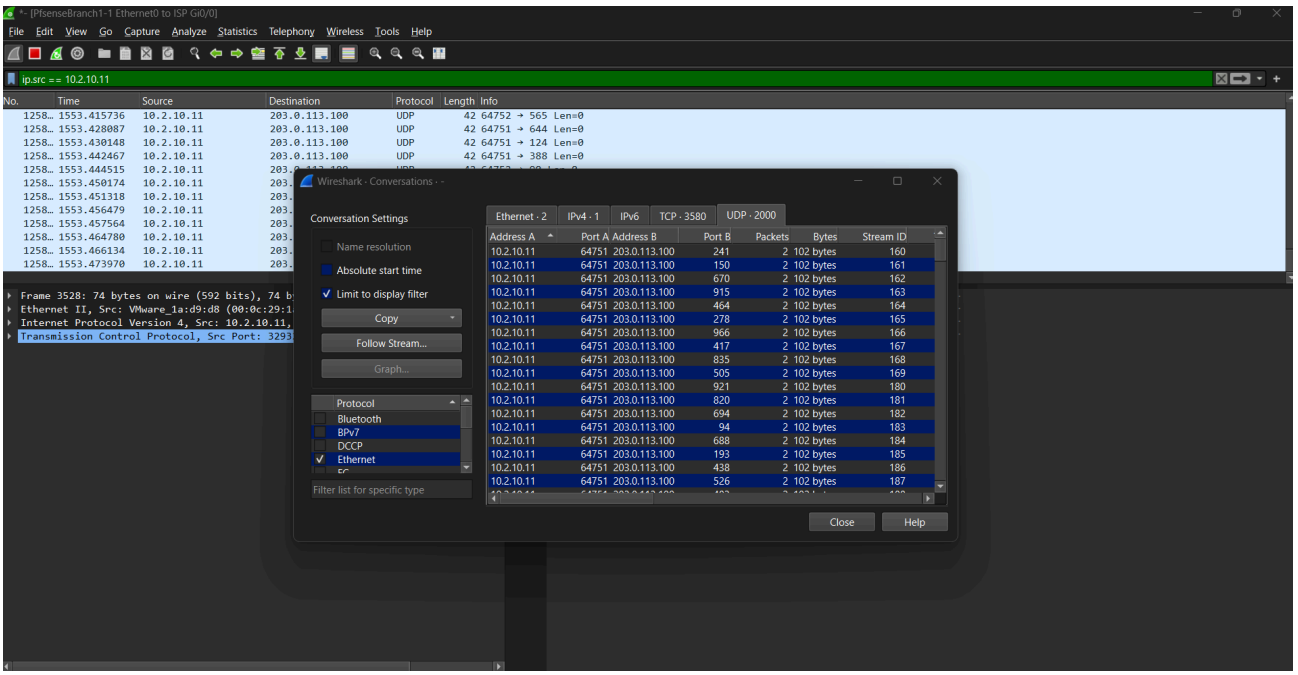


***Figure 6.3.21**: Wireshark inspection of the UDP scan (2)- Diagram showing that Wireshark is displaying the packets details.*

- Splunk**:**

- receives the snort intrusion attempts then forwards an alert notification directly to the admins handheld device to take an immediate action:

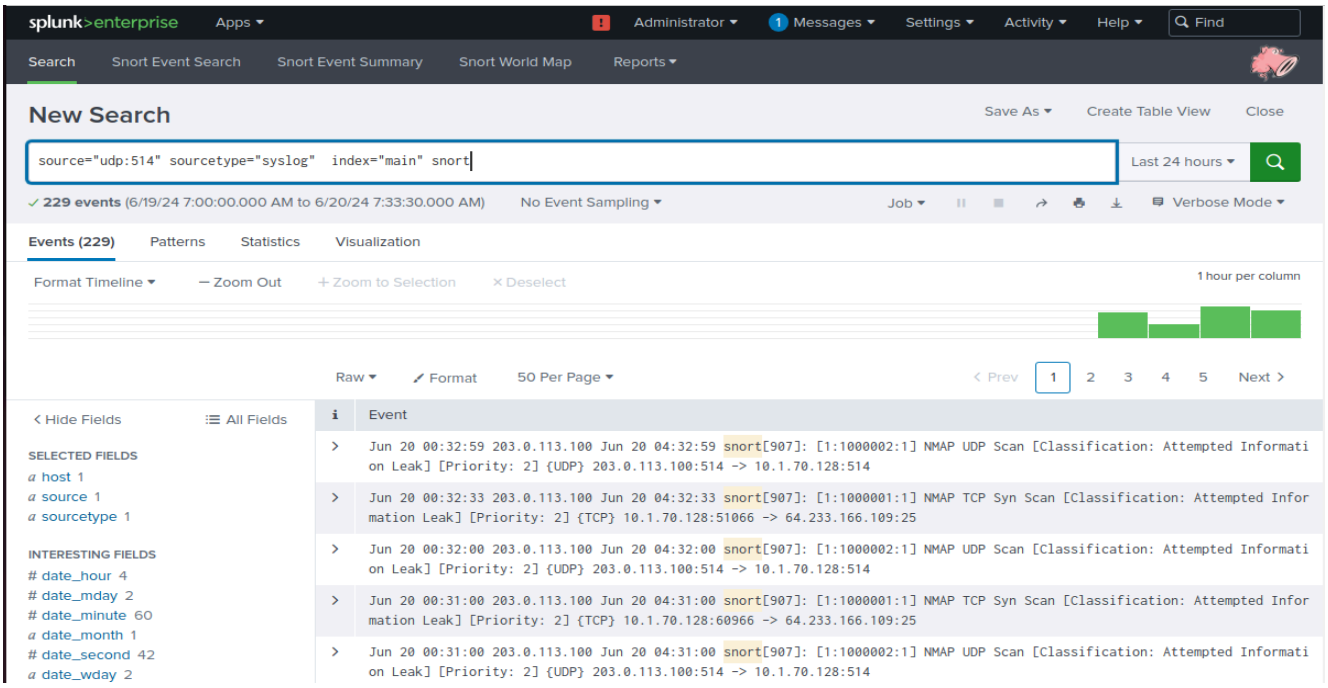


***Figure 6.3.22**: Splunk search & reporting the intrusion attempt- Diagram showing that splunk has received the syslog alerts from pfsense due to the intrusion attempt and was filtered using the appropriate command.*

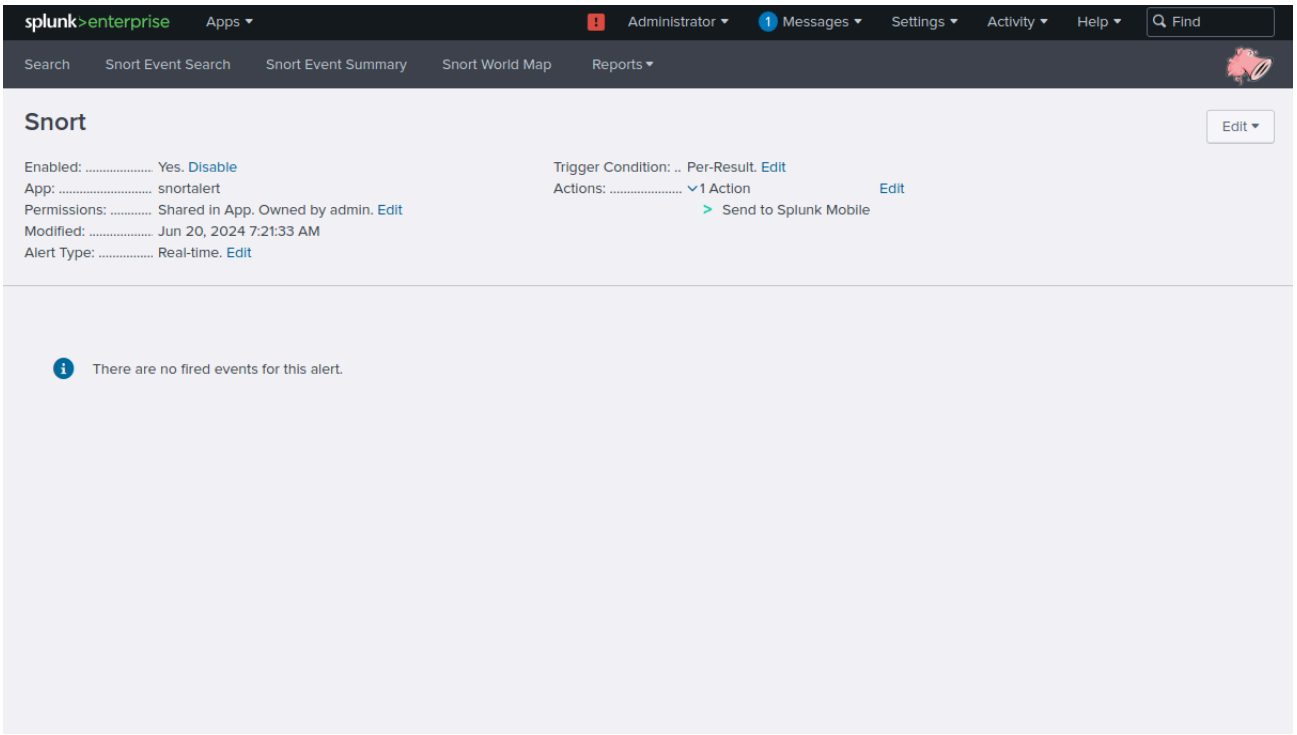


***Figure 6.3.23**: Splunk's send to mobile feature - Diagram showing that splunk has been configured to forward the intrusion attempt alerts to the admin's handheld device in real-time notifying him/her about the intrusion attempt.*

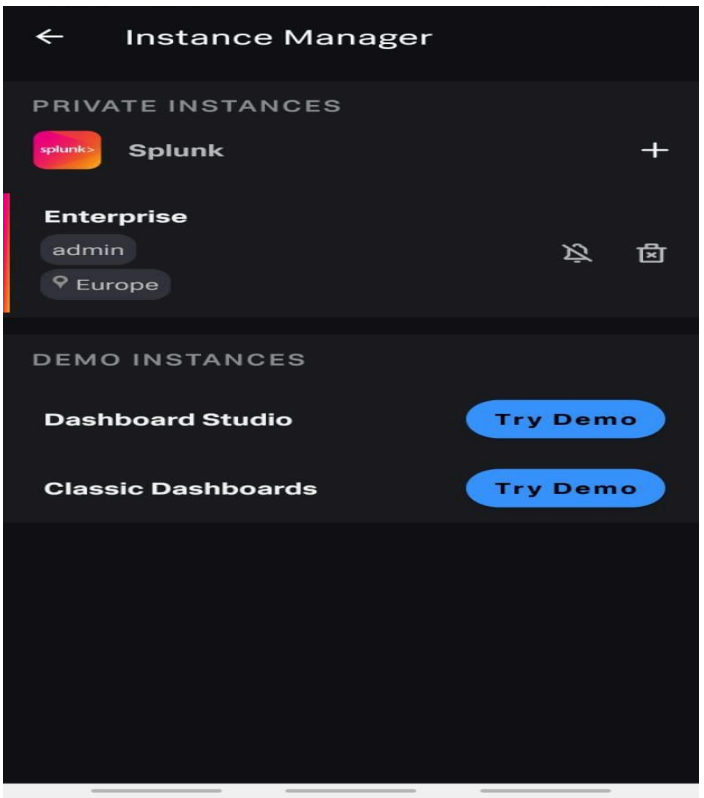


***Figure 6.3.24**: Admins handheld device (1)- Diagram showing that the splunk application on the admins handheld device has been linked with the splunk running in the network.*

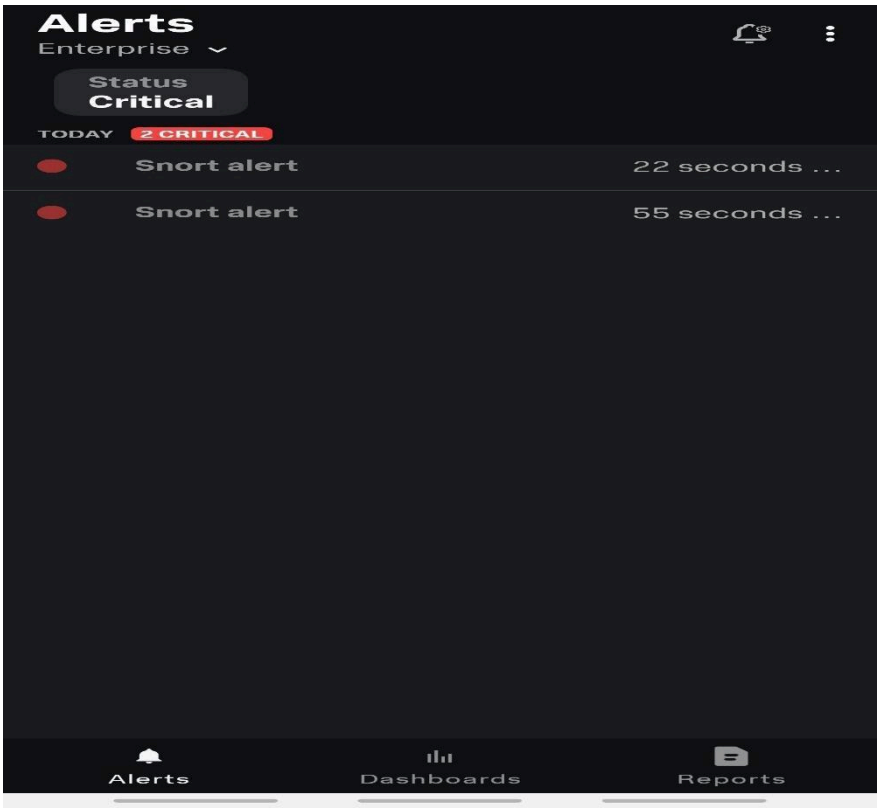


***Figure 6.3.25**: Admins handheld device - Diagram showing that the splunk application on the admins handheld device have received critical Snort alerts in real-time indicating an intrusion attempt on the network.*

❖ Firewall rules:

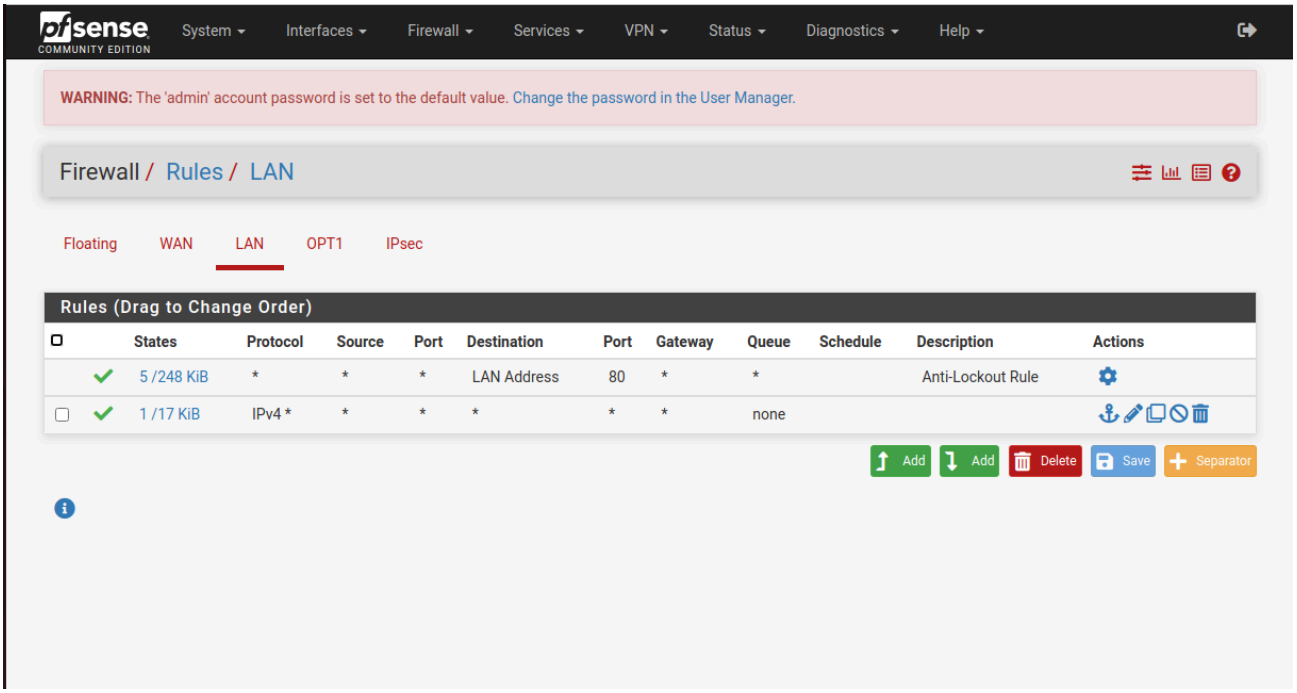


***Figure 6.3.26**: Firewall rules on the pfsense (HQ) interface - Diagram showing a list of firewall rules applied on the pfsense's LAN interface.*

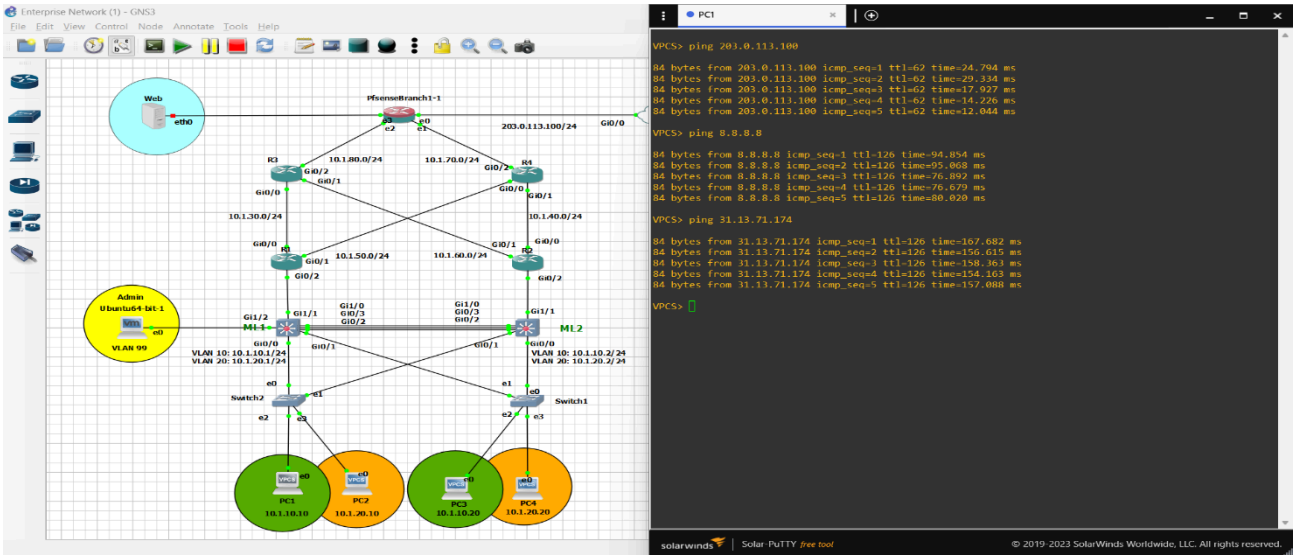


***Figure 6.3.27**: PC1 external connectivity (before firewall rule) - Diagram showing that PC1 is able to reach an external ip address (31.13.71.174) =>Instagram.com along with other external ips.*

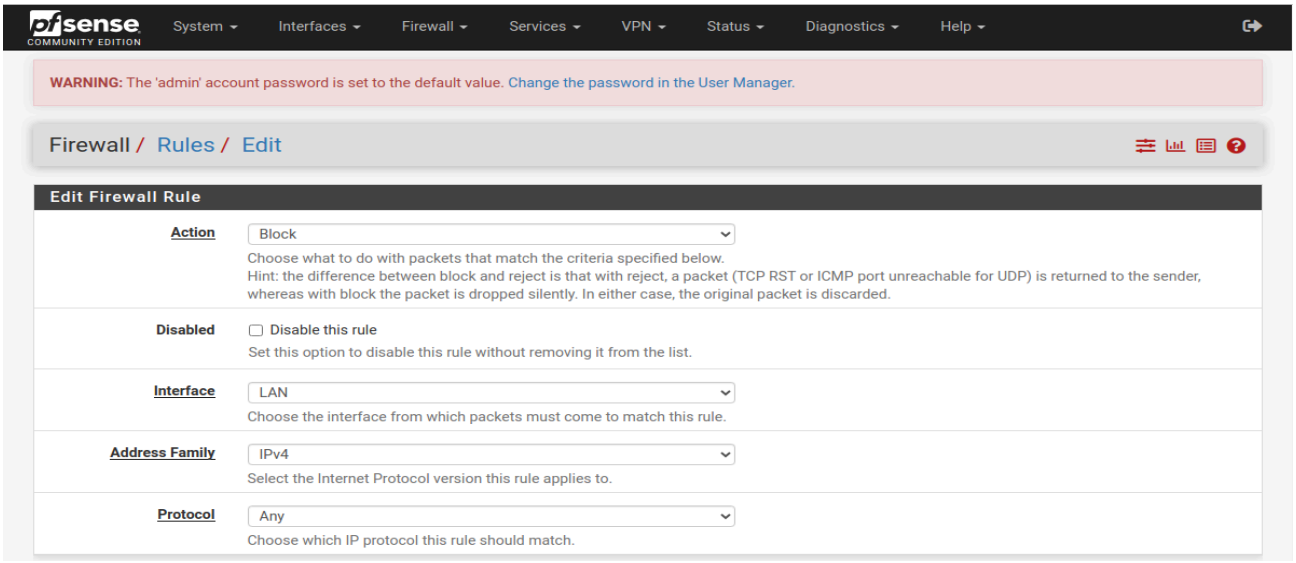


Figure 6.3.28: *Pfsense blocking firewall rule (1) - Diagram showing a firewall rule that blocks any type of protocol on the LAN interface of the pfsense.*

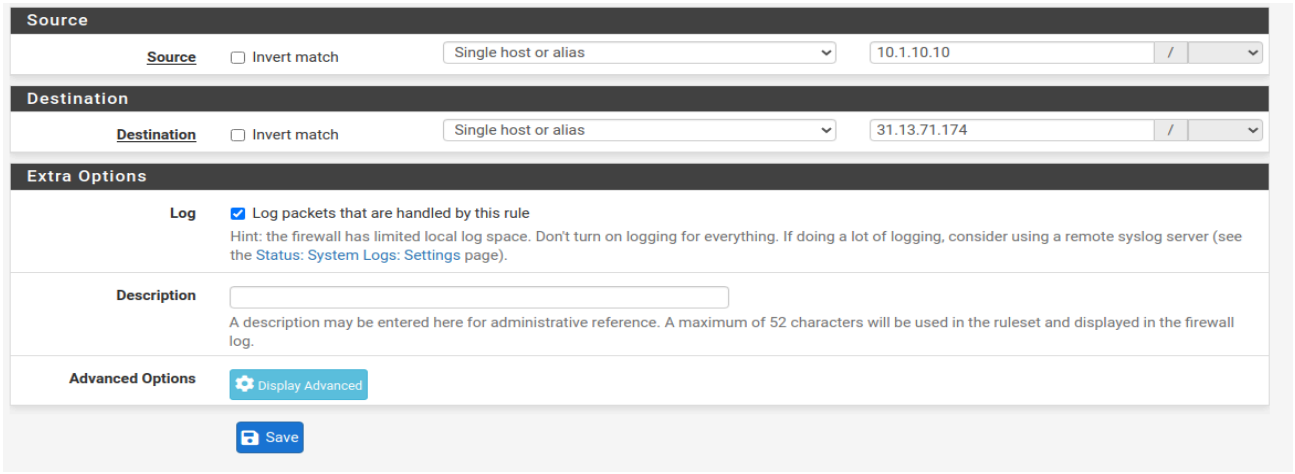


Figure 6.3.29: *Pfsense blocking firewall rule (2) - Diagram showing that the firewall rule was placed to restrict any traffic coming from the singular host (10.1.10.10) to reach a singular host (31.13.71.174) =>instagram.com.*

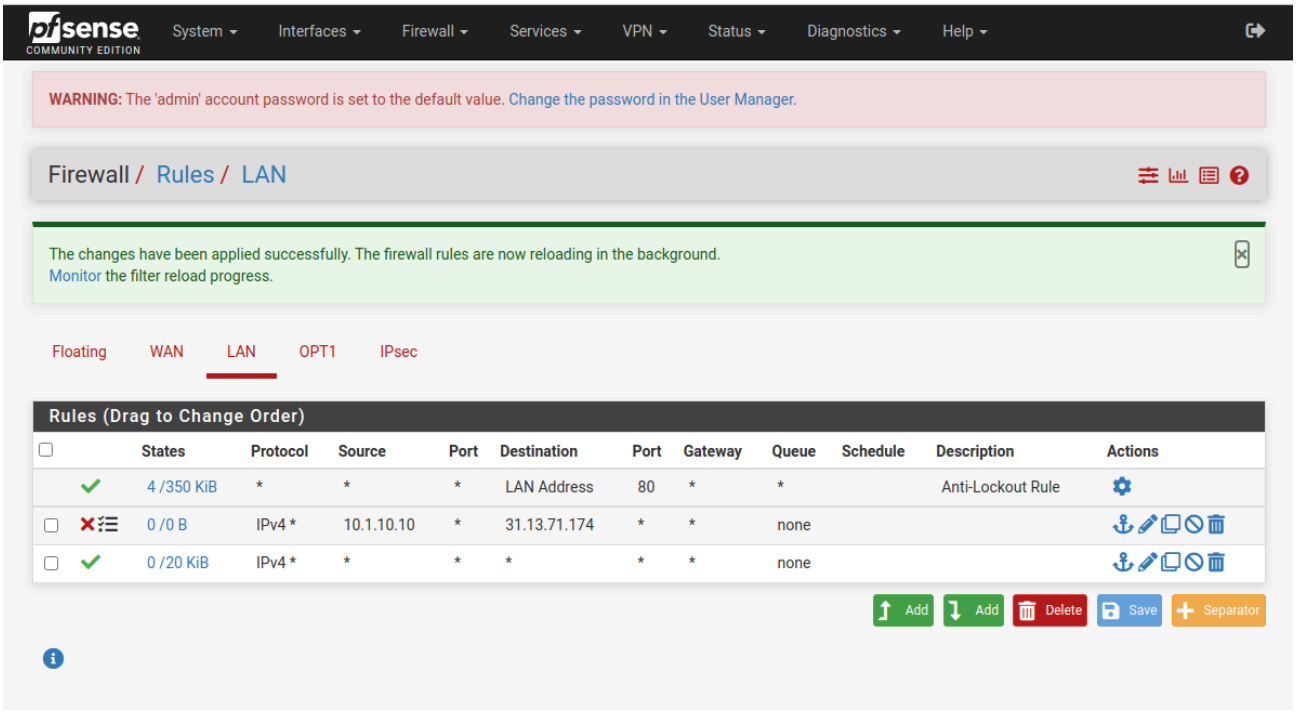


***Figure 6.3.30**: Pfsense blocking firewall rule (3) - Diagram showing a list of firewall rules on the LAN interface in which it blocks PC1 to reach 31.13.71.174(second rule on the list) but is able to reach other destinations (third rule on the list).*

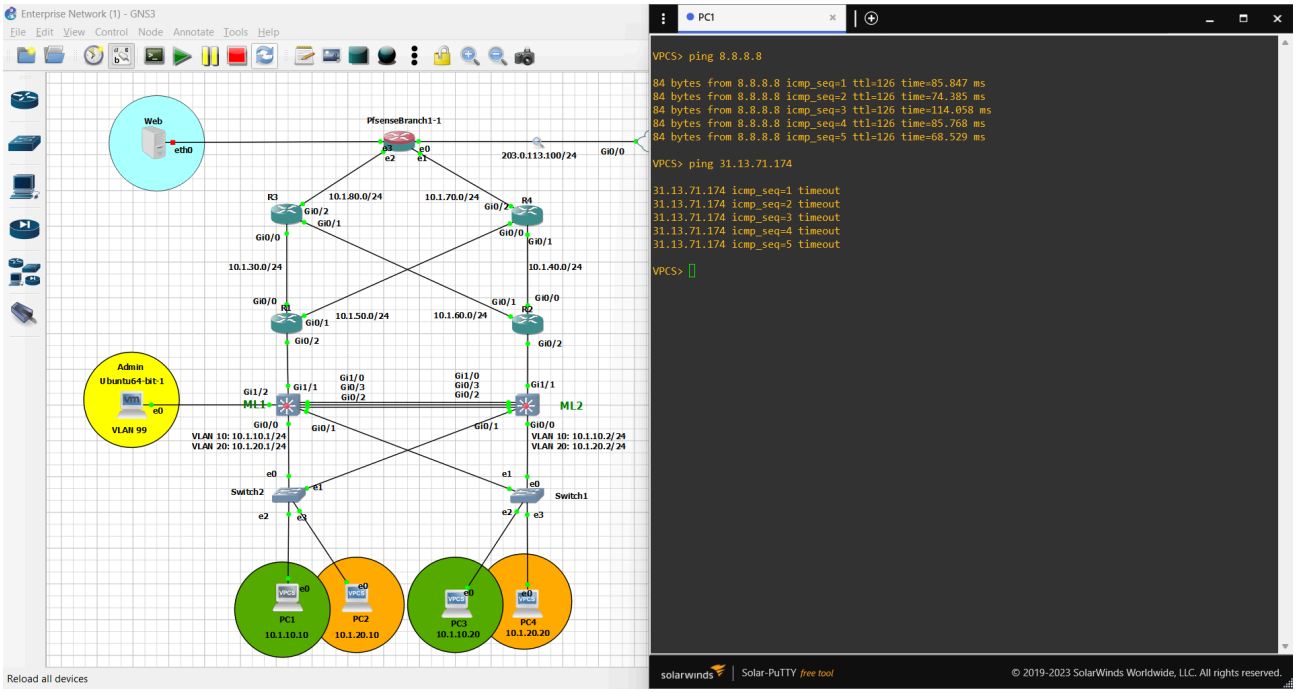


***Figure 6.3.31**: PC1 external connectivity (after firewall rule) - Diagram showing that PC1 is not able to reach an external ip address (31.13.71.174) =>Instagram.com but is able to reach other external ips.*

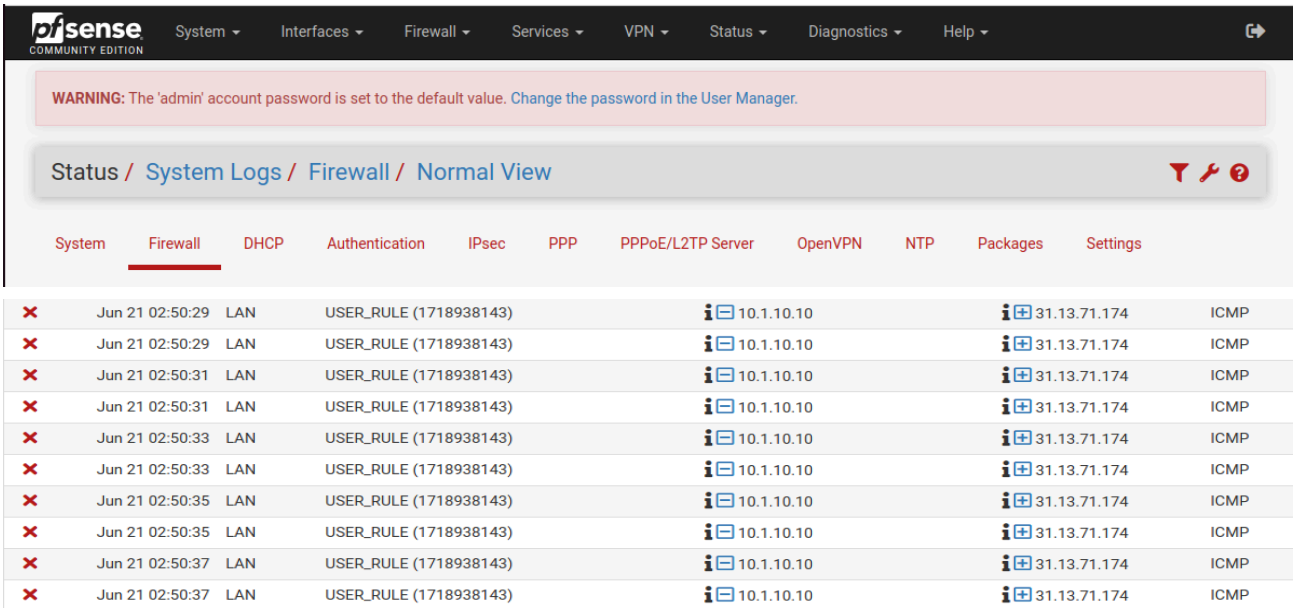


***Figure 6.3.32**: Pfsense blocking firewall rule (4) - Diagram showing a list of firewall system logs indicating that the device was restricted to access 31.13.71.174 due to a firewall policy placed on the LAN interface.*

Chapter 7: Conclusions and Future Work

7.1 Conclusions

In this project, we designed and implemented a network monitoring system aimed at enhancing security across a multi-branch organizational network. The main focus was to establish a secure VPN connection between two branches and implement an Intrusion Detection System (IDS) using pfSense firewall integrated with Snort for real-time threat detection. The key achievements and findings of this project can be summarized as follows:

1. **Network Architecture Setup**:
    - Successfully set up two network branches and established a secure VPN connection between them.
    - Implemented pfSense as a firewall on the secure branch (Branch 1) to control traffic and protect the network.
2. **Security Testing**:
    - Conducted a simulated attack using Nmap from Branch 2 (compromised branch) to test the security measures of Branch 1.

- Demonstrated that Snort, integrated with pfSense, effectively detected the Nmap scan and generated alerts for the network administrator.

3. **Effectiveness of IDS**:

   - The detection and alert capabilities of Snort were validated, confirming its efficacy in identifying and reporting network reconnaissance activities.
   - Highlighted the importance of real-time monitoring and alerting in maintaining network security.

4. **System Performance**:

   - Evaluated the performance impact of the implemented security measures on network latency and throughput.
   - Ensured that the security enhancements did not significantly degrade network performance, maintaining an acceptable level of service for users.

This project underscores the critical role of robust security mechanisms in protecting organizational networks from potential threats. The successful implementation and testing of the network monitoring system demonstrate its practicality and effectiveness in real-world scenarios.

7.2 Future Work

While this project has laid a solid foundation for network security through monitoring and detection, there are several areas for further research and improvement:

1. **Advanced Threat Detection**:

   - Implement additional IDS/IPS tools and compare their effectiveness with Snort.
   - Explore machine learning algorithms for anomaly detection to enhance the identification of sophisticated threats.

2. **Network Segmentation**:

   - Investigate the benefits of further segmenting the network to contain potential breaches and limit lateral movement of attackers.

3. **Automated Response**:

- Develop automated response mechanisms to complement the alerting system, enabling immediate mitigation actions upon threat detection.
- Integrate response automation with existing security policies and procedures.

4. **Scalability Testing**:

   - Conduct extensive scalability testing to ensure the system can handle increased network traffic and a higher number of connected devices without compromising security.

5. **User Awareness and Training**:

   - Implement regular security training and awareness programs for users to recognize and respond to potential security threats effectively.
   - Develop documentation and guidelines for network administrators to optimize the use of pfSense and Snort.

6. **Compliance and Reporting**:

   - Integrate compliance checks and reporting features to ensure adherence to industry standards and regulatory requirements.
   - Develop comprehensive reporting tools to provide insights into network security status and trends over time.

7. **Continuous Improvement**:

   - Establish a feedback loop for continuous assessment and enhancement of the security measures based on emerging threats and vulnerabilities.
   - Encourage collaboration with the cybersecurity community to stay updated with the latest security developments and best practices.

By addressing these future directions, the network monitoring system can evolve to provide even more robust protection, ensuring the integrity and security of organizational networks in an ever-changing threat landscape.

7.3 Appendices

Appendix A: Tools, Apps and Technology used within project (Name, Version, Description and Role at the project)

Name	Version	Description	Role
VMware® Workstation 17 Pro	17.5.1	Virtualization	Used to run our VMs including GNS3
GNS3	2.2.46	Emulator	Emulator that emulates our network
PfSense	2.6.0	Firewall /Router	Appliance that acts as a Firewall + Router
Ubuntu 22.04.4 LTS	Gnome version 42.9	Operating system	VM that operates the pfsense web GUI & Splunk web GUI
Kali GNU/Linux Rolling	Gnome version 3.38.3	Operating system	VM that operates hacking tools such as NMAP
Snort	4.1.6	IDS	IDS package that operates in pfSense
Splunk	9.2.1	Traffic analyzer and forwarder	Software used for traffic analyzing and forwarding
FRR	1.1.1_7	Routing	Routing package that operates in pfSense

Appendix B: List of existing network devices (passive and active components) (OS images version, model number, number of devices)

Name	OS image version	Number of devices
Multilayer switches	**vios_l2-adventerprisek9-m.vmdk.SSA.152-4.0.55. E**	**3**
Routers	**vios-adventerprisek9-m.spa.159-3.m6. qcow2**	**5**
VPCs	**VPC**	**6**
switches	**Ethernet switch**	**3**
PfSense	**pfSense-CE-2.6.0-RELEASE-amd64.iso**	**2**
Ubuntu	**ubuntu-22.04.3-desktop-amd64.iso**	**1**
Kali	**kali-linux-2021.1-installer-amd64.iso**	**1**
ISP	**vios-adventerprisek9-m.spa.159-3.m6. qcow2**	**1**

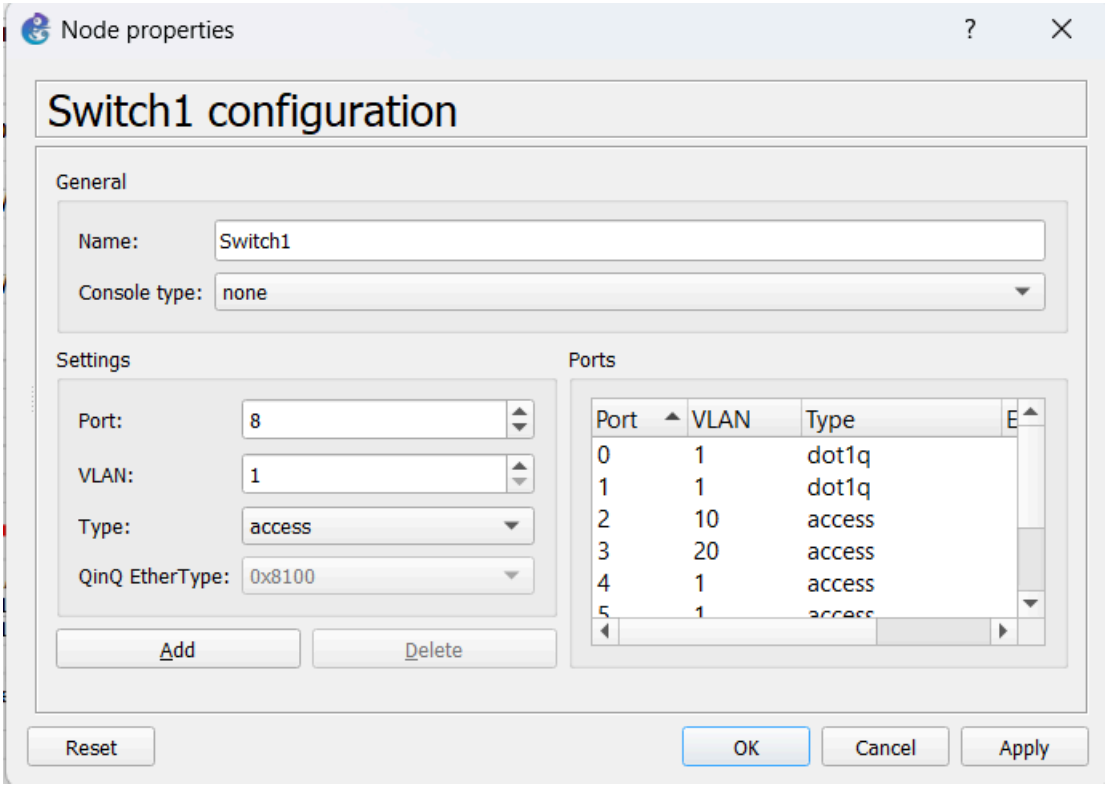
Appendix C: Configurations of existing network devices (IPs, usernames, passwords etc.…)

Name	Username	Password
Ubuntu	laith	123
Kali Linux	Kali	123
PfSense	admin	pfsense
Splunk	admin	admin12345

Device	Interface	IP address	Subnet	Default-Gateway
PC-1	NIC	10.1.10.10	255.255.255.0	10.1.10.254
PC-2	NIC	10.1.20.10	255.255.255.0	10.1.20.254
PC-3	NIC	10.1.10.20	255.255.255.0	10.1.10.254
PC-4	NIC	10.1.20.20	255.255.255.0	10.1.20.254
PC-5	NIC	10.2.10.10	255.255.255.0	10.2.10.1
PC-6	NIC	10.2.20.10	255.255.255.0	10.2.20.1
ML-1	VLAN-10	10.1.10.1	255.255.255.0	-
	VLAN-20	10.1.20.1		
ML-2	VLAN-10	10.1.10.2	255.255.255.0	-
	VLAN-20	10.1.20.2		
ML-3	VLAN-10	10.2.10.1	255.255.255.0	-
	VLAN-20	10.2.20.1		
R-1	G0/0	10.1.30.2	255.255.255.0	-
	G0/1	10.1.50.2		
	G0/2	-		
	G0/2.10	10.1.10.3		
	G0/2.20	10.1.20.3		
	VRRP 10	10.1.10.254		
	VRRP 20	10.1.20.254		
R-2	G0/0	10.1.40.2	255.255.255.0	-
	G0/1	10.1.60.2		
	G0/2	-		
	G0/2.10	10.1.10.4		
	G0/2.20	10.1.20.4		
	VRRP 10	10.1.10.254		
	VRRP 20	10.1.20.254		
R-3	G0/0	10.1.30.1	255.255.255.0	-
	G0/1	10.1.60.1		
	G0/2	10.1.80.7		
R-4	G0/0	10.1.50.1	255.255.255.0	-
	G0/1	10.1.40.1		
	G0/2	10.1.70.7		
R-5	G0/0	10.2.80.7	255.255.255.0	-
	G0/1	-		
	G0/1.10	10.2.10.3		
	G0/1.20	10.2.20.3		

❖ CLI and GUI configurations of the intermediary devices (Routers, multilayer switches & switches):

3 switches (only have access and trunk interfaces as required for the other 2 switches):



ML1+(ML2, ML3 have the same configuration with different IP addresses):

```
interface Port-channel1
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet0/0
 switchport trunk encapsulation dot1q
 switchport mode trunk
 media-type rj45
 negotiation auto
!
interface GigabitEthernet0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
 media-type rj45
 negotiation auto
!
```

```
interface GigabitEthernet0/2
 switchport trunk encapsulation dot1q
 switchport mode trunk
 media-type rj45
 negotiation auto
 channel-group 1 mode desirable
!
interface GigabitEthernet0/3
 switchport trunk encapsulation dot1q
 switchport mode trunk
 media-type rj45
 negotiation auto
 channel-group 1 mode desirable
!
interface GigabitEthernet1/0
 switchport trunk encapsulation dot1q
 switchport mode trunk
 media-type rj45
 negotiation auto
 channel-group 1 mode desirable
!
interface GigabitEthernet1/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
 media-type rj45
 negotiation auto
!
interface GigabitEthernet1/2
 switchport mode access
 media-type rj45
 negotiation auto
!

interface Vlan10
 ip address 10.1.10.1 255.255.255.0
```

```
interface Vlan20
 ip address 10.1.20.1 255.255.255.0
```

Router Configuration:
R1 (R2 have the same configuration with different IP's and OSPF, R3+R4 configured with IP's and OSPF, R5 configured with IP's as router on stick, and OSPF):

```
interface GigabitEthernet0/0
 ip address 10.1.30.2 255.255.255.0
 duplex auto
 speed auto
 media-type rj45
!
interface GigabitEthernet0/1
 ip address 10.1.50.2 255.255.255.0
 duplex auto
 speed auto
 media-type rj45
!
interface GigabitEthernet0/2
 no ip address
 duplex auto
 speed auto
 media-type rj45
!
interface GigabitEthernet0/2.10
 encapsulation dot1Q 10
 ip address 10.1.10.3 255.255.255.0
 vrrp 10 ip 10.1.10.254
 vrrp 10 priority 120
!
interface GigabitEthernet0/2.20
 encapsulation dot1Q 20
 ip address 10.1.20.3 255.255.255.0
 vrrp 20 ip 10.1.20.254
```

```
 vrrp 20 priority 120
!
router ospf 1
 network 10.1.10.0 0.0.0.255 area 0
 network 10.1.20.0 0.0.0.255 area 0
 network 10.1.30.0 0.0.0.255 area 0
 network 10.1.40.0 0.0.0.255 area 0
 network 10.1.50.0 0.0.0.255 area 0
 network 10.1.60.0 0.0.0.255 area 0
 network 10.1.70.0 0.0.0.255 area 0
 network 10.1.80.0 0.0.0.255 area 0
 network 10.2.10.0 0.0.0.255 area 0
 network 10.2.20.0 0.0.0.255 area 0
 network 10.2.80.0 0.0.0.255 area 0
!
ip route 0.0.0.0 0.0.0.0 10.1.50.1
```

References

[1] https://www.netgate.com

[2] https://forum.netgate.com

[3] https://community.splunk.com

[4] https://www.geeksforgeeks.org

[5] https://github.com

[6] https://ubuntuforums.org

[7] https://forums.kali.org