Nimble Troubleshooting and Firewall Configuration

MINT 709 - Capstone Project

by
Prabin Joshi

Master of Science in Internetworking

Department of Computing Science

University of Alberta

Supervisor

Dr. Mike MacGregor

Table of Contents

Table of Figures

1. Introduction

Despite significant advances in technology and its widespread application in our society, many still do not have access to the Internet. This is primarily due to approaches taken for infrastructure rollout or failure to connect more sparsely populated areas [4]. As per Wakoma, Nimble uses the concept of a wireless mesh network to create a decentralized network infrastructure that is portable and, most importantly, an offline-first network. In the present world, the concept of portable wireless infrastructure helps to build communities that don't; have access to proper wired infrastructure. A wireless mesh network has a rich interconnection among devices, and it adopts a self-form, self-heal approach, which means that if one node fails to operate, the rest of the nodes or devices can still communicate with each other either directly or through intermediate nodes [5]. As there are a growing number of challenges in the deployment of wired infrastructure due to geographical issues, etc., wireless technology is needed to reach every corner of the world and keep people connected. Wakoma is trying to solve this problem by enabling communities to build their infrastructure that works offline and connects back to the Internet [4].

The Nimble network is an open-source network that can be built and deployed locally [6]. Users connected to the Nimble network can have access to a lot of services, such as video, voice, and text chat, video streaming and downloading, file sharing, eLearning module and website building and learning, collaborative spreadsheet and document creation, eBook reading, gaming, and much more, completely offline [4]. All these features can be accessed entirely offline and help people to stay connected with each other. The users on the Nimble network can easily connect to the Internet by plugging it into the network. Nimble units are portable and can be moved around or left in place to grow sustainable and scalable networks [6]. Over time, Nimble increases Internet demand and access by making it relevant, practical, and affordable to local communities [4].

1.1 SCOPE OF THE PROJECT

The Nimble Troubleshooting and Firewall Configuration course is designed to provide users with no prior experience in Nimble implementation with a general understanding of its structure and technical aspects. The course offers comprehensive coverage of the different services and devices used to create a complete Nimble, covering fundamental to moderate complexity topics and providing hands-on practical demonstrations of modules to equip users with the experience needed to successfully configure, monitor, and upgrade their Nimble.

1.2 PURPOSE OF THE PROJECT

The goal of this project is to equip users with the fundamental knowledge necessary to operate the Nimble. This course offers hands-on implementation of technology concepts supported by interactive short video vignettes. By focusing on the application of Intranet technology with an offline-first network and implementation modules, users gain the technical knowledge to independently implement the Nimble, enabling large-scale deployment for remote smaller communities and providing a strong infrastructure for building a community wireless mesh network. The bundled solution of Nimble and the hands-on modules provides end users with easy access to resources and timely configuration, enabling them to utilize the full range of features that Nimble has to offer.

2. MODULE DESCRIPTIONS

The Nimble Troubleshooting and Firewall Configuration course consists of 11 modules focused on policy implementation, configuration, monitoring, and backup, as well as topics focused on how to stay secure and how the activity of users is monitored on a day-to-day basis. Figure 1 shows the block diagram representation of Nimble with the functions of each component. The functions of each individual component help in the application of the offline first network by integrating together to perform as a bundled solution. Such solutions help remote communities by being portable as well as eliminating the great need for the Internet and, at the same time, allowing individuals living in those communities to access the services locally without the need for expensive Internet plans. The offline first ideology uses the services run locally on Nimble to provide an offline way of communicating with people without the need for the Internet [1]. The services can be used for various communication services like video chat, messaging, streaming, etc.

Figure 2 represents a data flow diagram of Nimble. It explains how Nimble works and how it is connected to provide various services to end users. It uses colour-coded symbols to help end users understand the workflow of Nimble. This Nimble unit consists of devices like routers, switches, servers, access points, etc., to facilitate the offline first ideology. The platform used to run the Nimble services is an open-source project called ‘Lokal’, developed by Wakoma Incorporated and available on GitHub as ‘GitHub-Wakoma’. It is designed to be platform-agnostic and serves as an open-source solution to connect various open-source services and applications. The ‘Lokal’ platform allows content creation, curation, and sharing without relying on the Internet. Branded as ‘Lokal Services Global Impact’, the platform operates on the philosophy of making a positive impact. It is compatible with online and offline environments due to its compatibility with a range of hardware and operating systems.

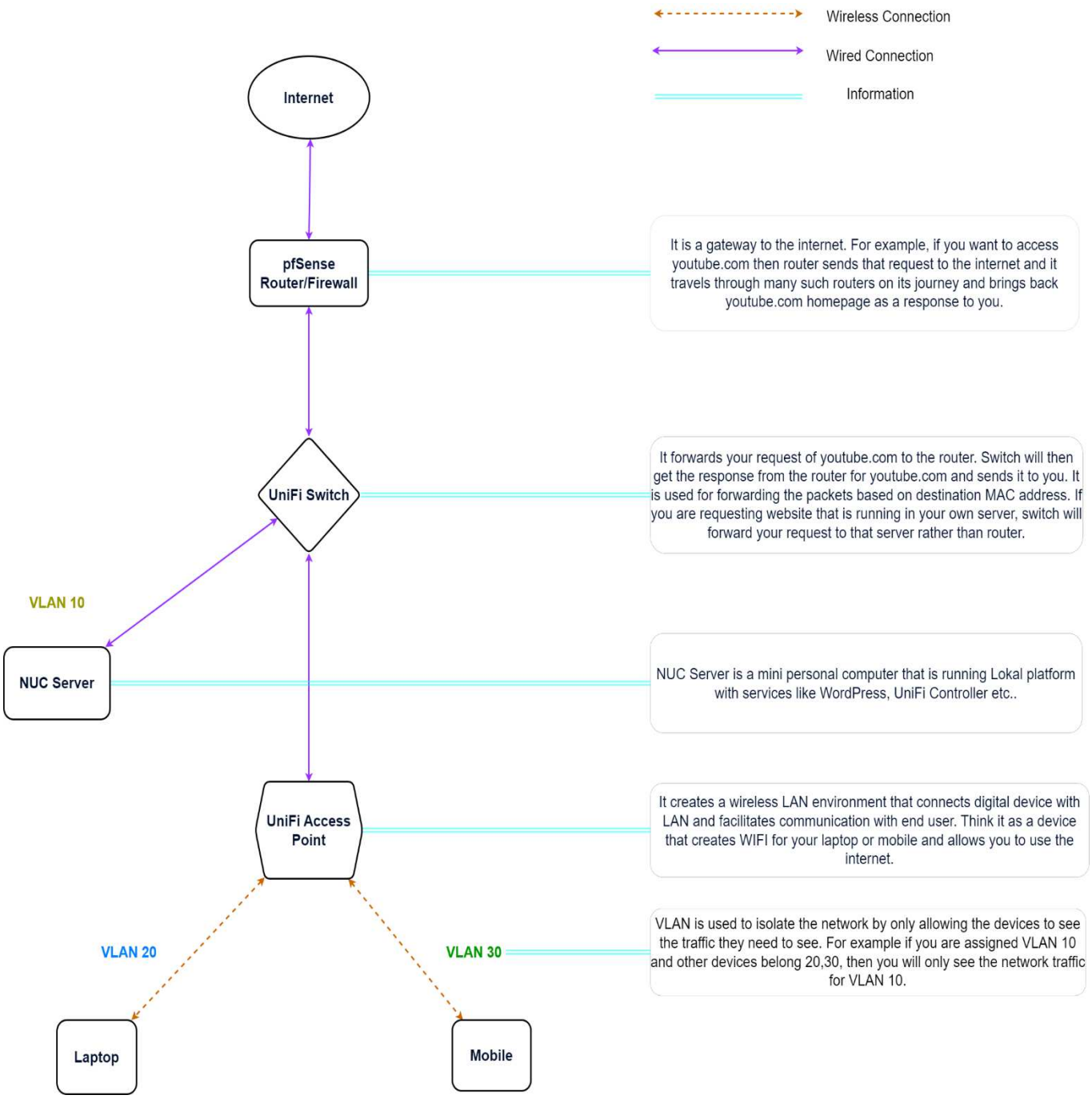

Figure 1: Block Diagram of Nimble and its Roles

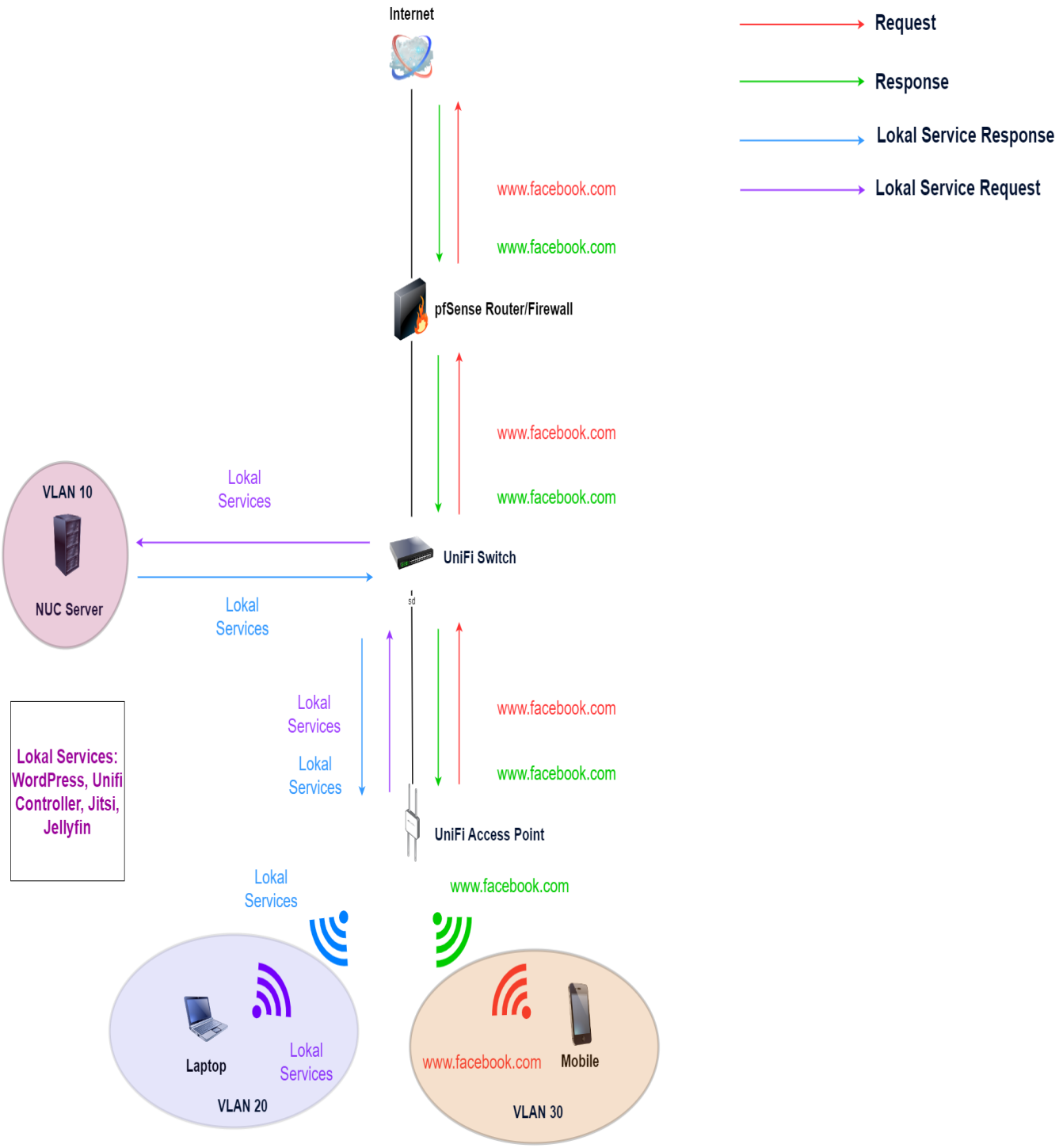

Figure 2: Data Flow of Nimble

As a customizable open-source software and service platform, ‘Lokal’ enables communities and organizations to produce, consume, and interact both online and offline. The ‘Lokal’ platform prioritizes offline functionality, offering a wide range of services, including video and audio calls, messaging, music, e-learning, e-books, network monitoring, Wikipedia, file-sharing, social networking, wireless network management, media streaming, and more. Platform installation is straightforward, requiring only a single line of code. Currently, the ‘Lokal’ platform runs on modern Linux OS, specifically Ubuntu, and is an ideal solution for remote communities with unreliable Internet connections.

This course consists of 11 fundamental modules focused on providing the end-user with hands-on experience in Nimble operation. A general overview of the topic, along with technical implementation, is provided to give users fundamental skills and hands-on training to use Nimble on their own. The module list is as follows:

- Understanding and Implementing User and Group Policy Management
- Implementing VLAN on Nimble.
- Understanding Port Forwarding and its Implementation.
- Monitoring Nimble with pfTop.
- Connecting Nimble to the Internet.
- Restricting Websites Access with Nimble.
- Creating a Network on UniFi.
- Restricting Device Access with Nimble.
- Implementing Firewall Policy on UniFi.
- Create and Restore Backup on Nimble.
- Knowledge Sharing on Security and Monitoring.

2.1 Understanding and Implementing User and Group Policy Management

This module is designed to provide users with an understanding of how to manage users and groups on Nimble. Policy-level management of users and groups determines who should have access to what resources and this module defines such policies. A general understanding of access management policies involves dividing a group of people into various subgroups based on their access rights, as well as defining policies based on roles. Examples of this are given in the figures below.

By the end of this module, users will be able to describe and complete tasks related to creating users and groups and assigning privileges based on the requirements. They will also be able to demonstrate measurable and observable output while understanding the concept of different privilege rules.

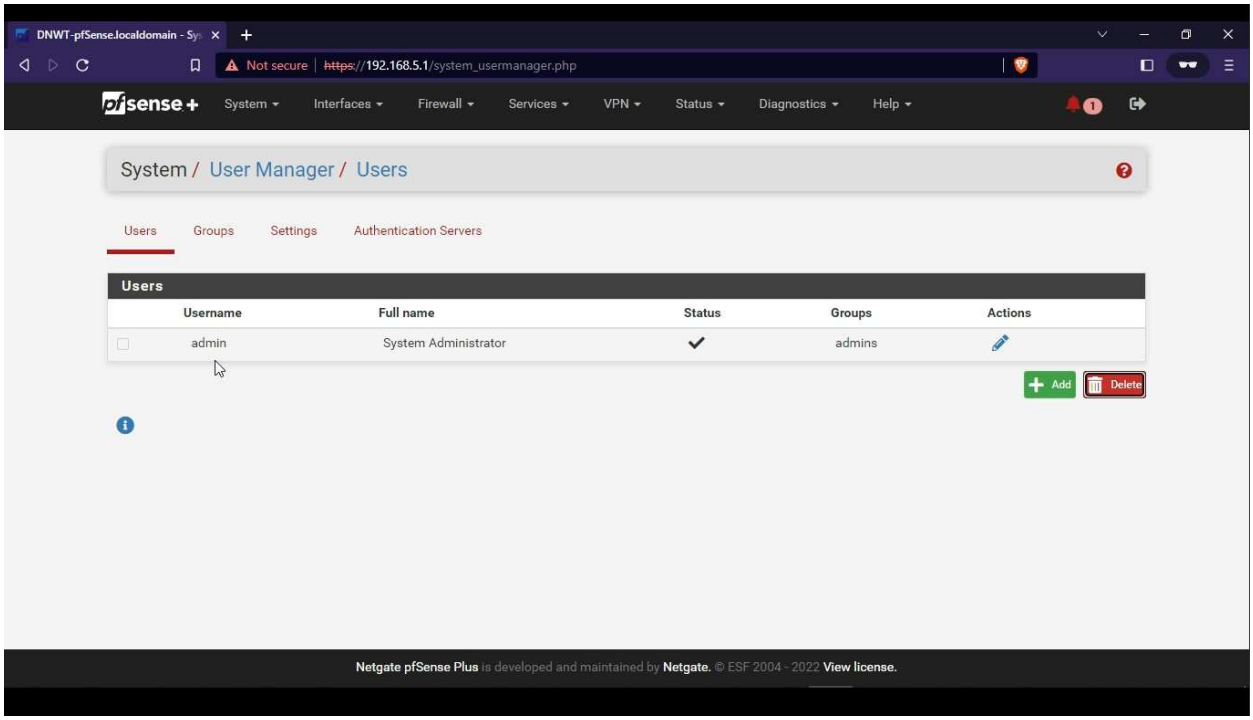

Figure 3: User Manager

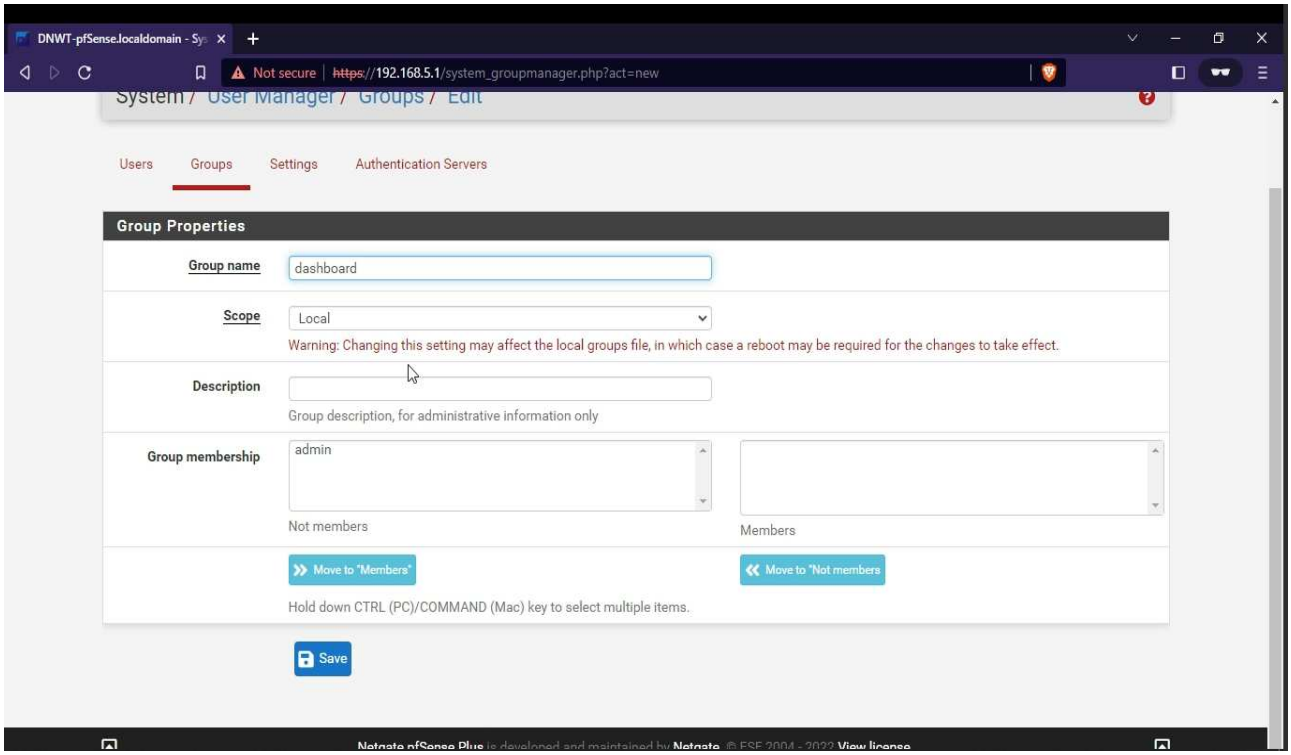

Figure 4: Group Manager

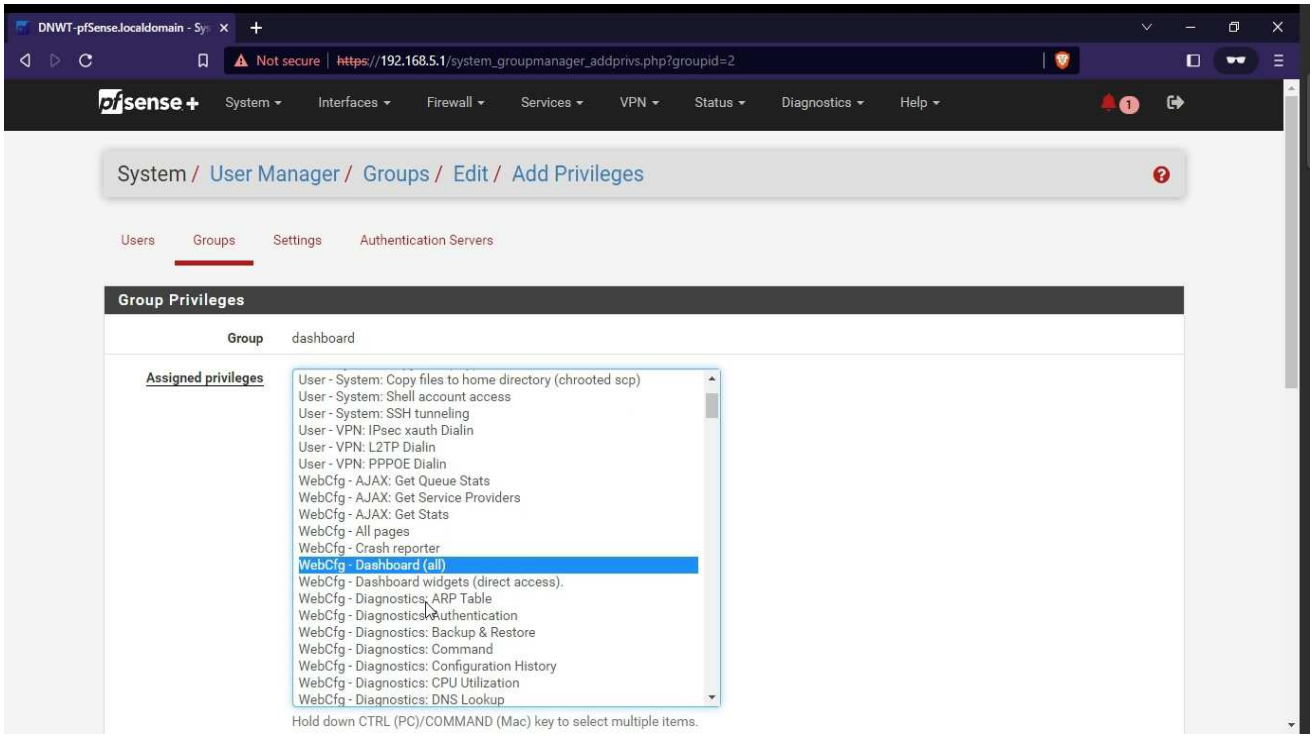

Figure 5: Privilege Management.

2.1.1 Motivation

The motivation of this module is to provide users with simplified approaches to implementing policies and maintaining access rights. In addition, the module aims to equip users with the skills and knowledge necessary to train others on policy design and monitoring. By the end of this module, users will have a better understanding of the importance of having policies in place and be able to perform real-world test cases through hands-on demonstrations.

2.1.2 Learning Objectives

After completing this module, users should be able to execute the following tasks:

a. Create, update, and delete Users, Groups.
b. Understand the privilege access management.
c. Grant access to users and groups based on roles.
d. Define policy for groups.

2.2 Implementing VLAN on Nimble

This module gives users with the knowledge and skills to implement VLAN on Nimble. It covers concepts related to the configuration and implementation of VLAN in Nimble. VLANs allow a switch to act like many switches, which means that one switch can handle many different networks or groups of computers that are unable to talk to each other. This helps to divide a big network into smaller parts for better organization and security. When switches are connected, computers on the same VLAN can be on different switches and still communicate. A single port on a device can also be used to talk to computers on different VLANs. The module provides a hands-on demo on creating VLANs, assigning them to interfaces, implementing firewall policies, and IP address assignments. The snapshots can be found in the figures below.

By the end of this module, users will be able to describe VLAN and its terminologies. They will also gain ideas on configuring interfaces and proper VLAN assignments. They will be able to implement firewall policies along with managing a pool of IP addresses with the introduction of a DHCP server and its benefits.

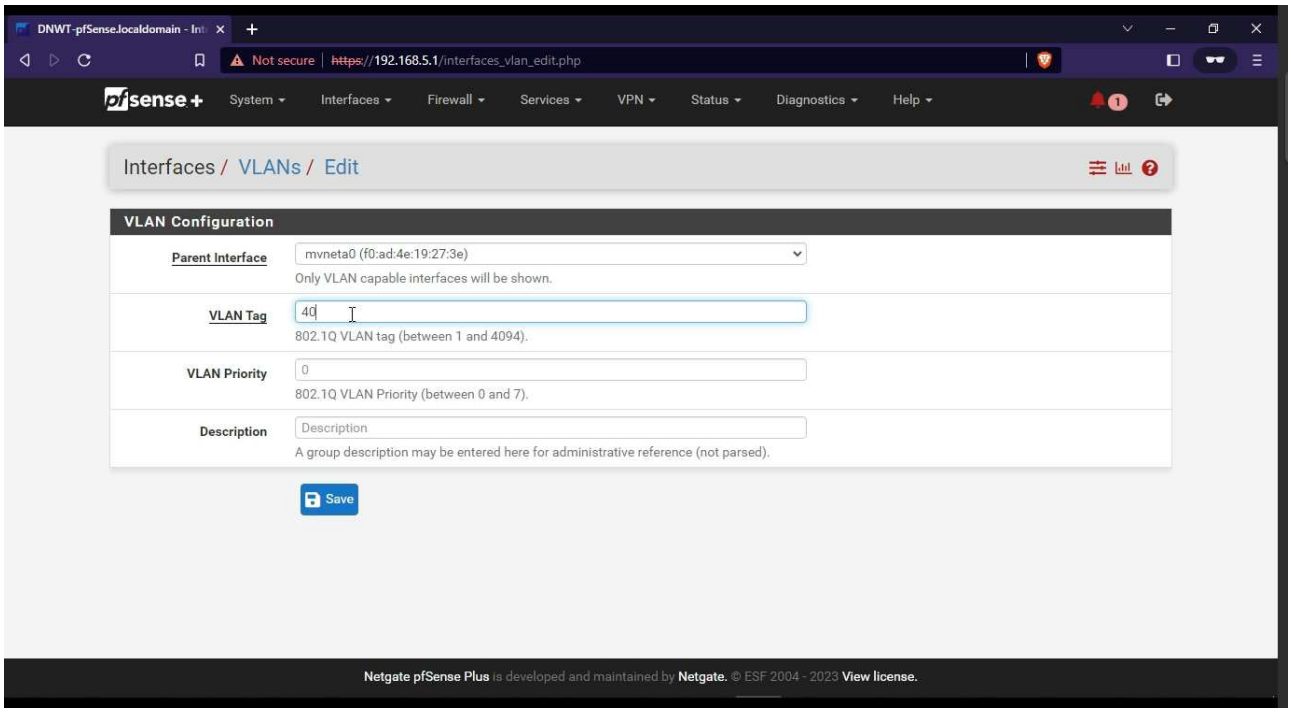

Figure 6: Creating a VLAN

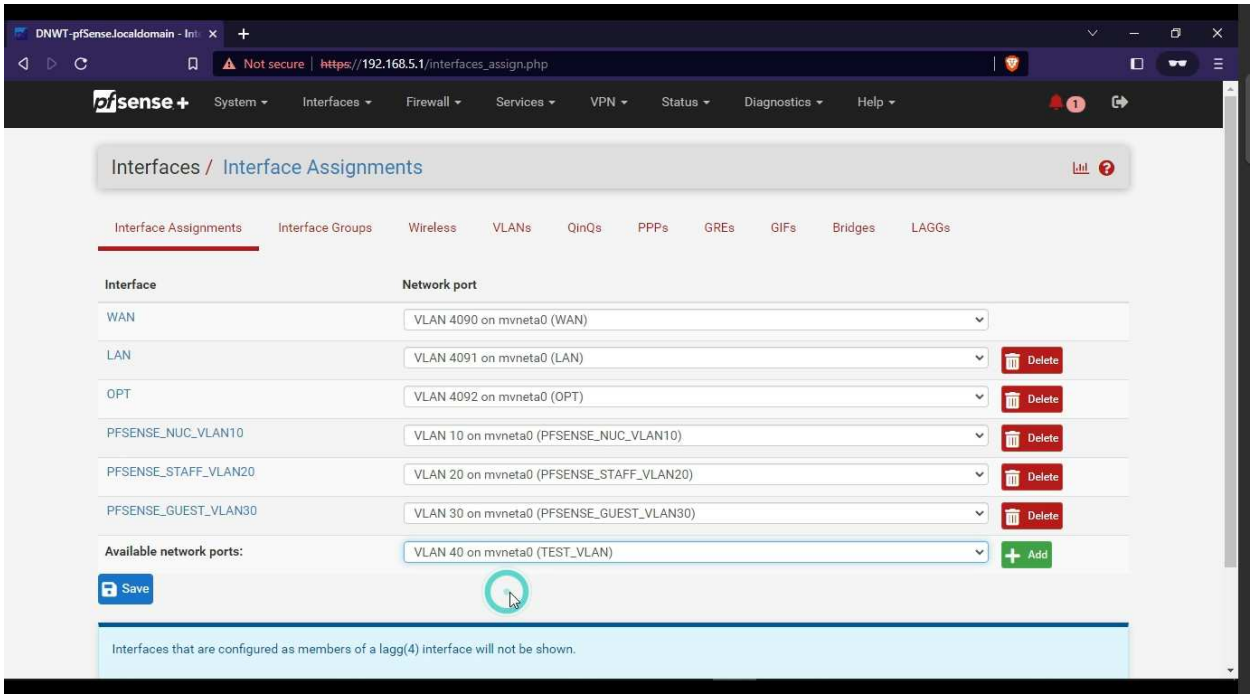

Figure 7: Interface Assignment

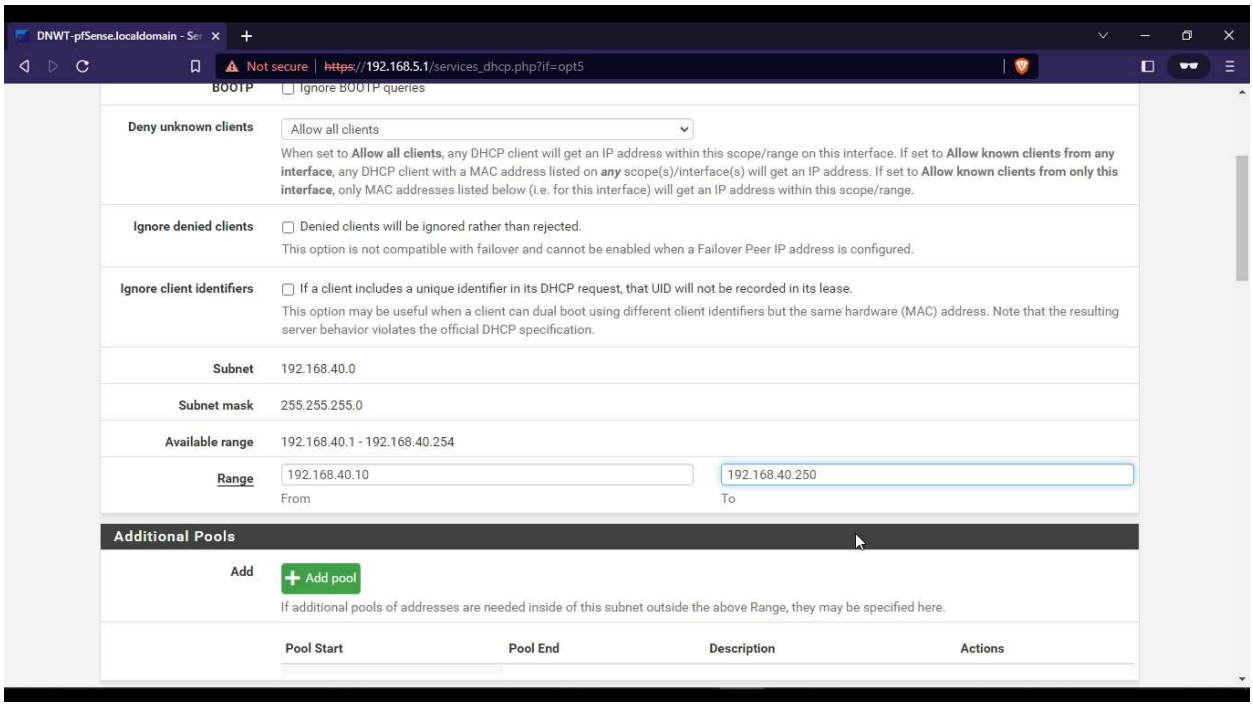

Figure 8: DHCP Server IP Pool

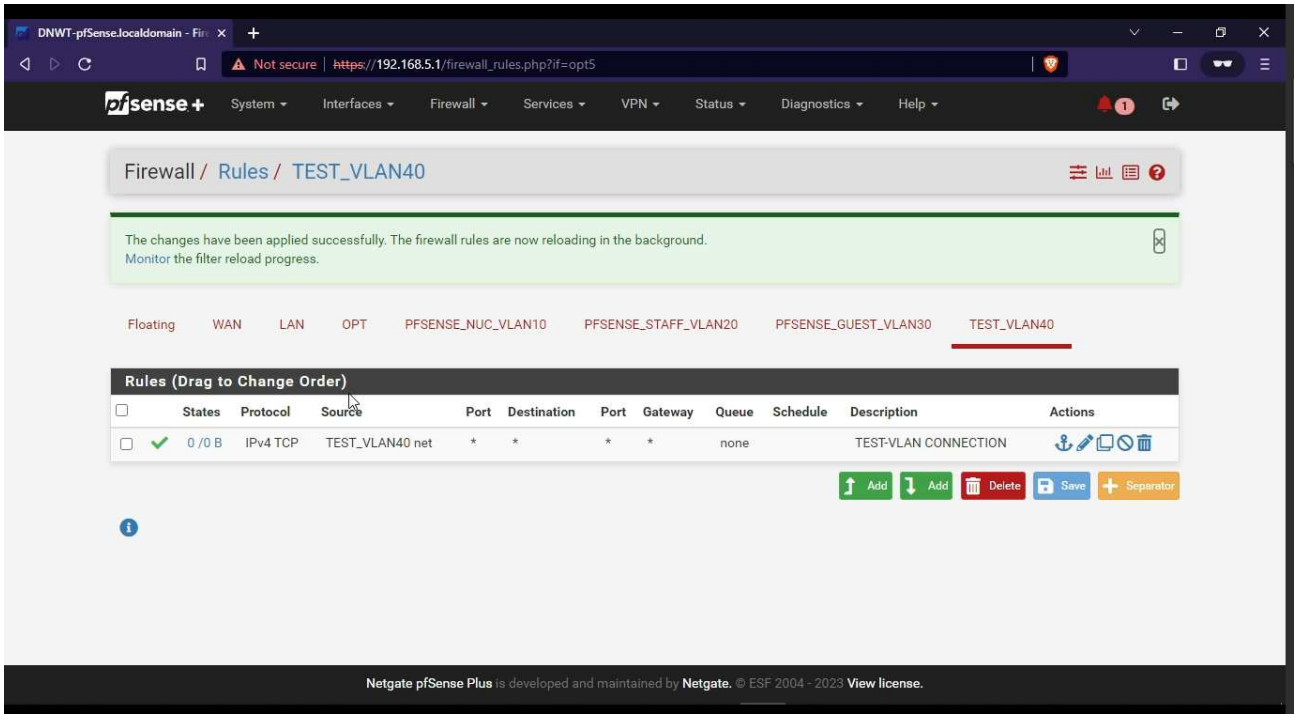

Figure 9: Firewall Rules

2.2.1 Motivation

The motivation of this module is to provide users with knowledge of using VLAN and its implementation. The main goal of this module is to help users understand the significance of VLAN in managing network traffic and how it can be used to improve the performance of the Nimble network. By providing a comprehensive overview of the VLAN concept and its implementation, this module will enable users to successfully integrate VLAN in the Nimble network and configure firewall rules to enhance the flow of network traffic.

2.2.2 Learning Objectives

After completing this module, users should be able to execute the following tasks:

a. Creating VLANs and assigning appropriate VLAN tags.
b. Understanding the concept of VLAN and basic VLAN terminologies.
c. Configuring interfaces and proper VLAN assignments.
d. Implementing Firewall rules and policies.
e. Selecting an appropriate pool of IP addresses.

2.3 Understanding Port Forwarding and its Implementation.

This module provides the user with the basic concept of Port Forwarding. It covers concepts related to the implementation of port forwarding in Nimble. This will guide users to understand why it is required and how to implement that in Nimble. Port Forwarding is a technique that will help external devices access devices or computer services on a private network. Port forwarding is a way to connect a device on your private network (like your home network) to the Internet. This allows other people on the Internet to access things on your device, like a game or a website. Port forwarding maps an "Internet door" (called a port) to your device so that when someone knocks on that door, it goes directly to your device. However, this can also be dangerous if not set up properly, as someone could access your device without your permission. An example of this concept is provided with the hands-on demo. The snapshots can be found in the figures below.

By the end of this module, users will be able to get hands-on experience with port forwarding and understand its implementation. Users will also gain ideas on choosing appropriate ports as per the standards and rules in place for the use of ports for private and public use. They will be able to implement port forwarding to connect with devices behind a different network.

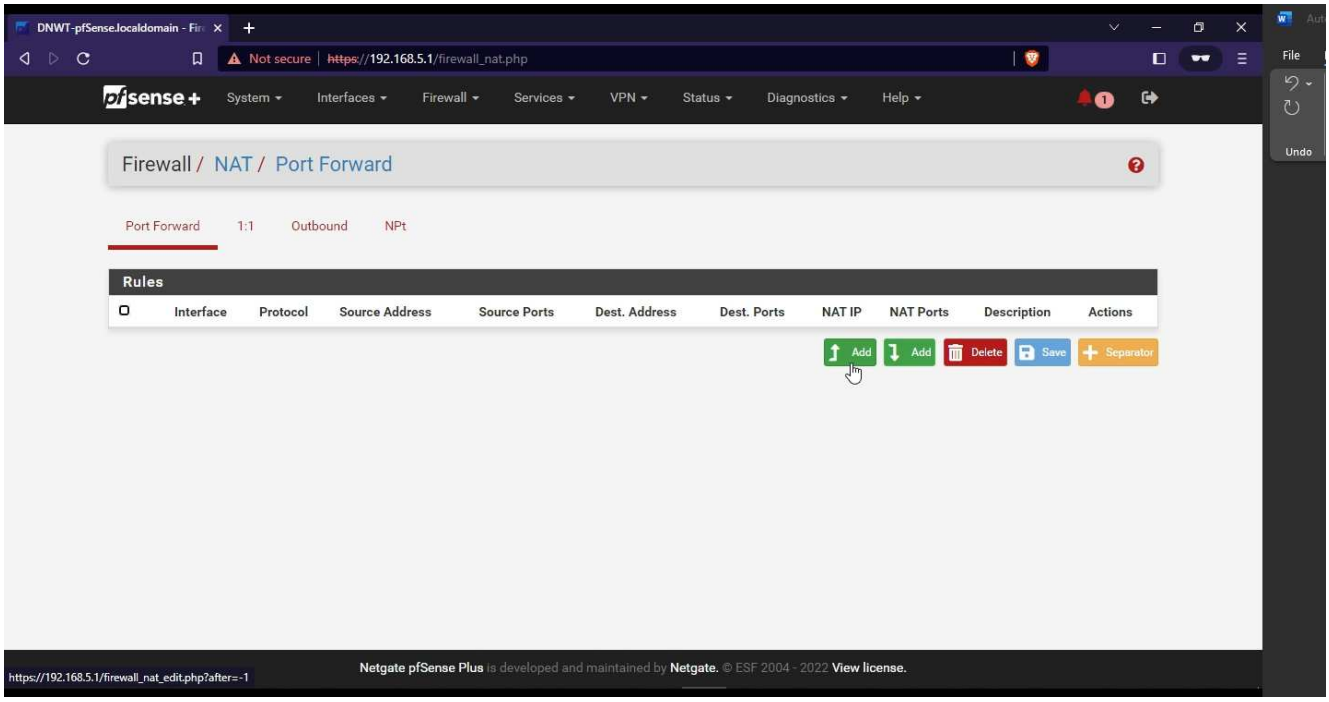

Figure 10: Port Forwarding in Nimble

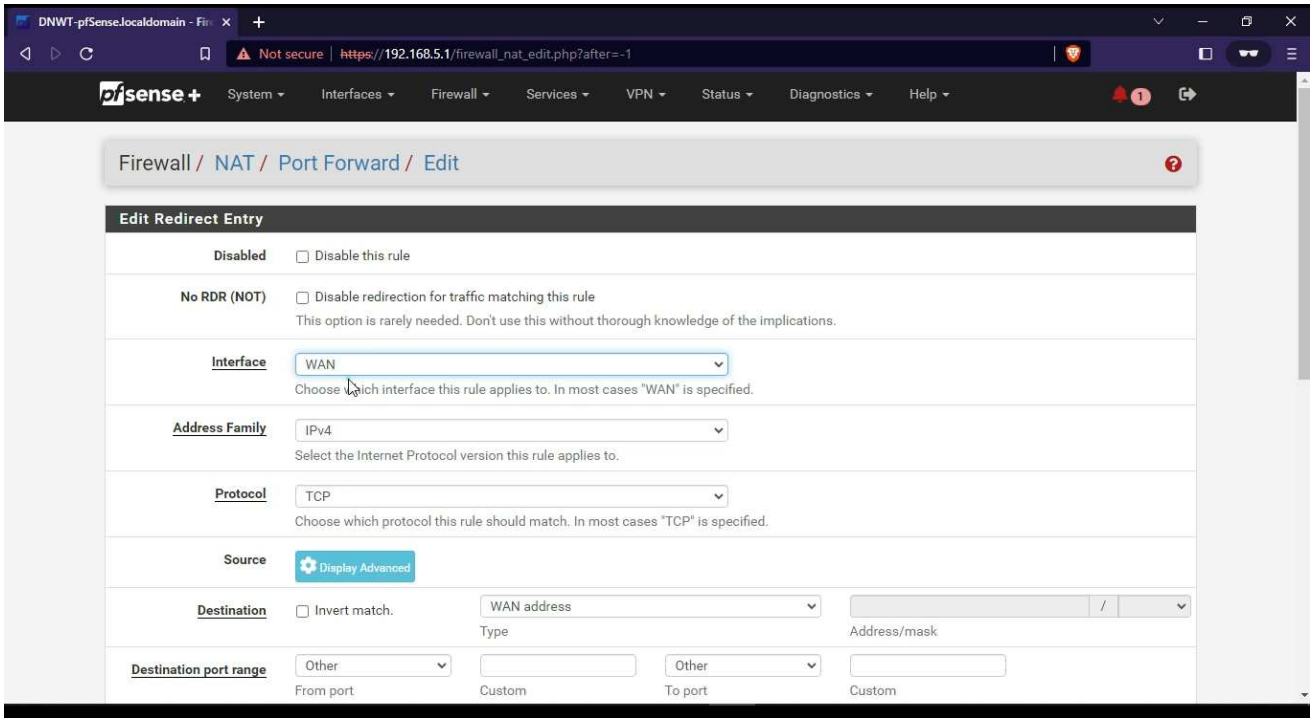

Figure 11: Configuring Port Forwarding

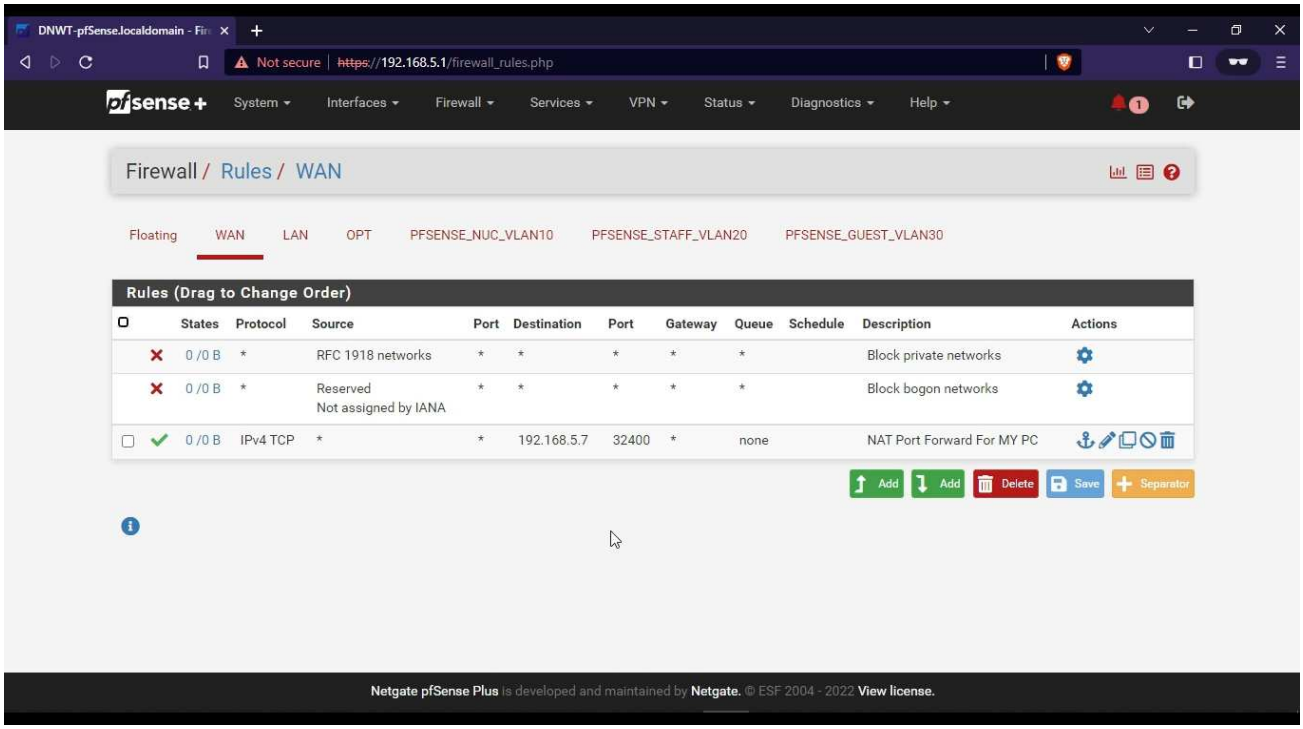

Figure 12: Firewall Policy

2.3.1 Motivation

The motivation behind this module is to provide users with the knowledge and skills to use port forwarding and its implementation. The module will help users understand why and when we use port forwarding and how it can help gain access to services or devices located behind a different private network. This module will enable users to plan which services to connect using port forwarding, as well as gain the necessary skills to integrate it into the Nimble network.

2.3.2 Learning Objectives

After completing this module, users should be able to perform the following tasks:

a. Understand the concept of Port Forwarding.
b. Understand the concept of NAT.
c. Implement Port Forwarding on Nimble.

2.4 Monitoring Nimble with pfTop

In this module, users will learn how to monitor Internet activity on a Nimble network and use tools such as pfTop to gain insights into network traffic. Through the use of visuals, users will learn to quickly make sense of network activity and respond to any issues that arise. Specifically, users will be trained in using pfTop, a network traffic monitoring and statistics plugin in pfSense, to analyze and monitor network traffic in Nimble. The module will guide users through the process and provide snapshots of the tools used. By the end of the module, users will be able to:

a. Use pfTop to monitor the traffic.
b. Use filter expression to analyze the traffic and makes changes as required.

2.4.1 Motivation

The motivation of this module is to provide users with knowledge of pfTop and its implementation in Nimble. This module will help users to gain insights into their network traffic and its statistics. Users will learn how to implement the pfTop plugin through the pfSense portal to analyze their network traffic.

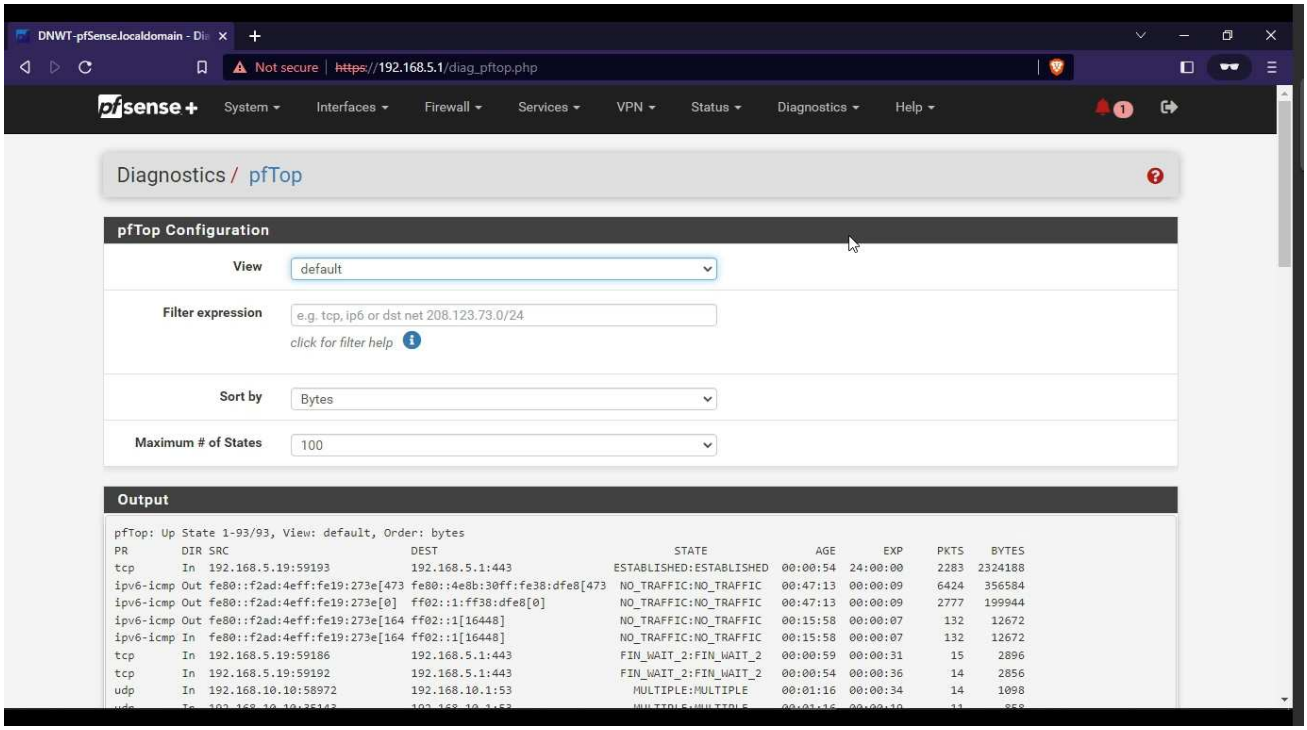

Figure 13: pfTop Configuration

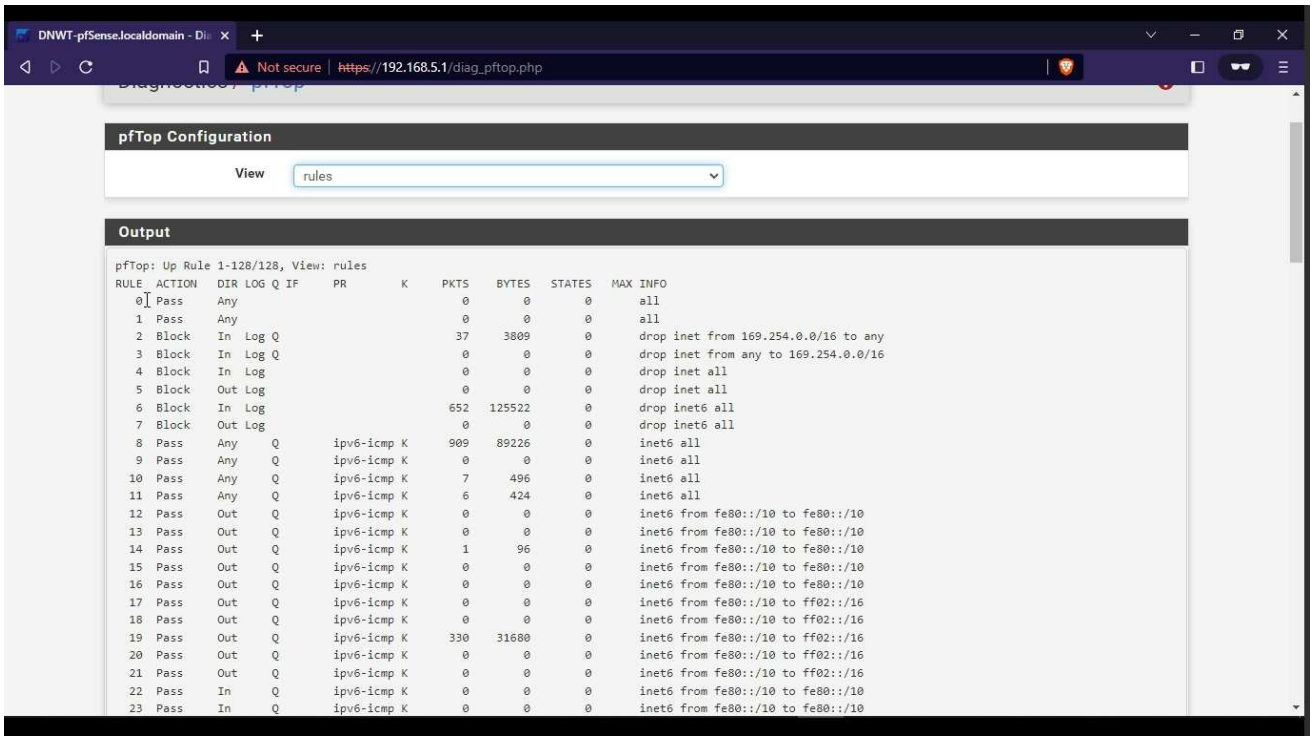

Figure 14: pfTop Rules Monitoring

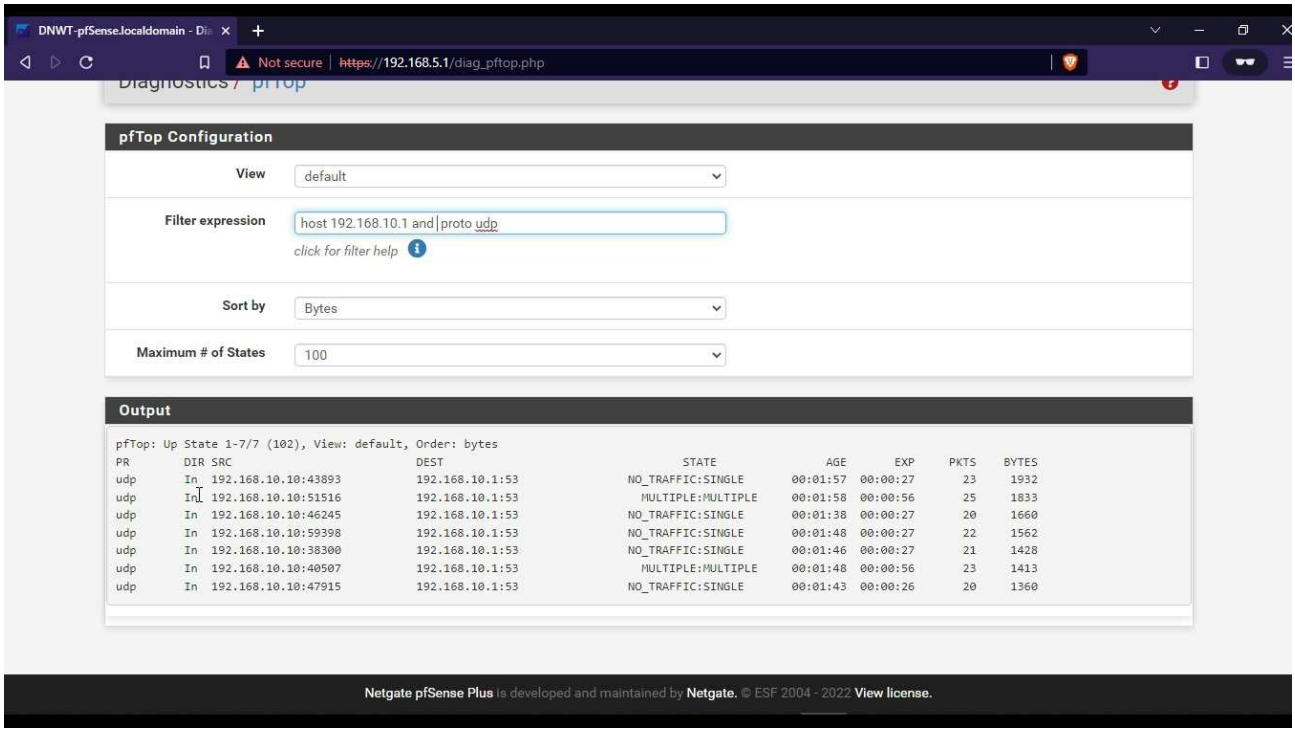

Figure 15: Using Filter Expression on pfTop.

2.4.2 Learning Objectives

After completing this module, users will be able to analyze the network traffic and rules using pfTop. Users will be able to use filter expressions to perform extensive analysis of the generated traffic. They will also be able to monitor firewall rules and take necessary actions as required.

2.5 Connecting Nimble to the Internet

While the Nimble ideology is based on an offline-first network, this module provides users with the knowledge needed to connect Nimble to the Internet, should they choose to do so. Nimble is a solution designed to provide offline communication, eliminating the need for the Internet. However, for users who want to take advantage of the Internet connectivity, this module provides guidance on how to set up and configure a connection. With a focus on remote communities, Nimble is deployed to work in both online and offline modes. The snapshot of the tools and process is given in the figures below. This module will help users to do the following tasks:

a. Connecting Nimble to the Internet.

b. Monitoring the Connections and Implementing WAN firewall policy.

Figure 16: Netgate Router Ports Overview.

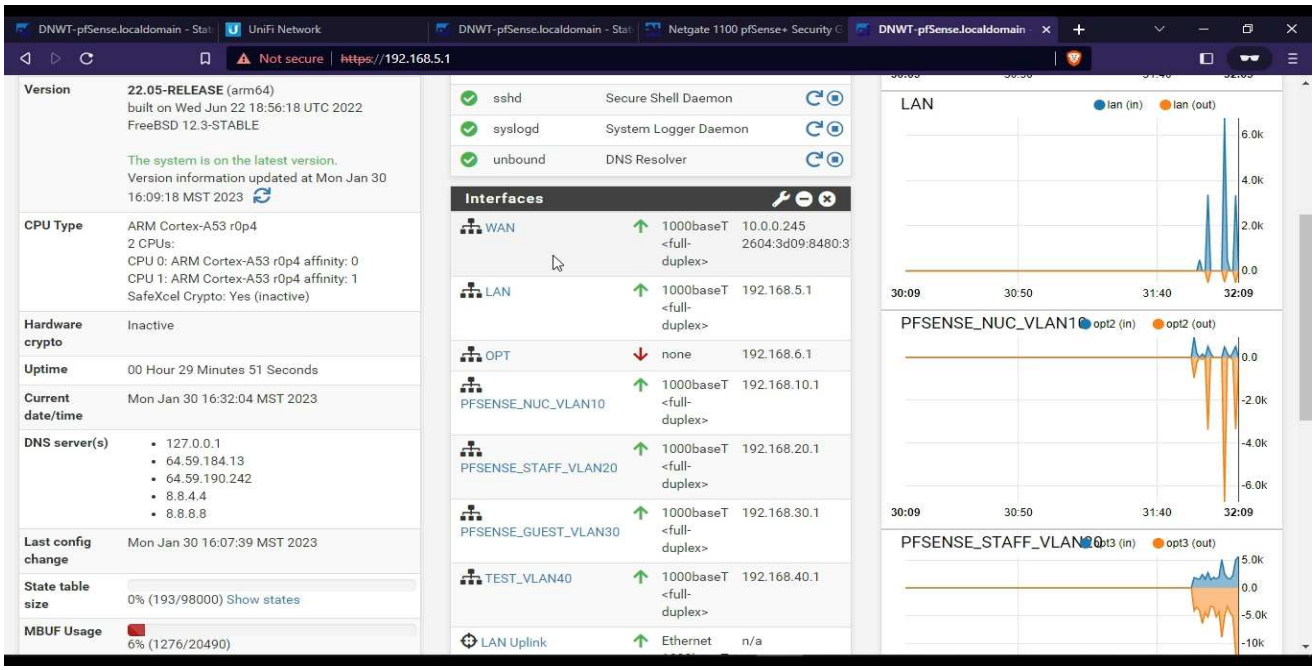

Figure 17: Connection Monitoring

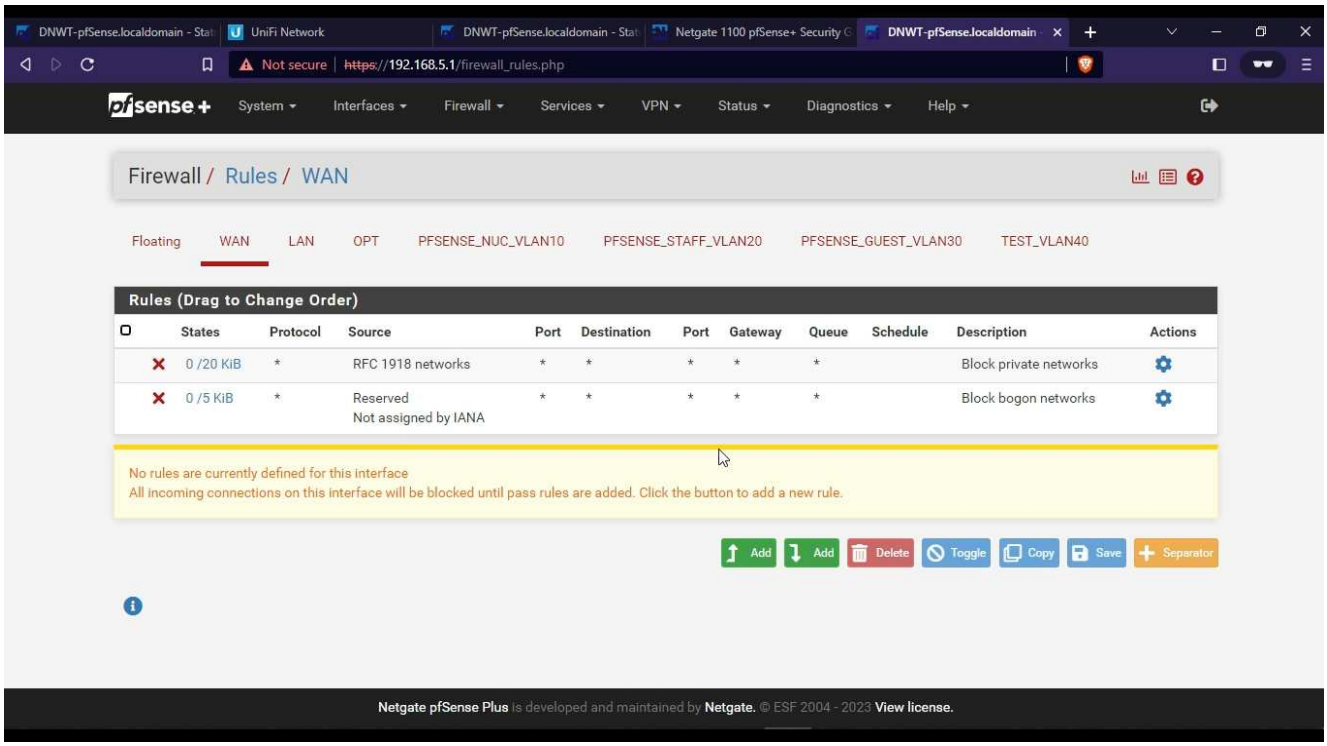

Figure 18: Firewall Policy for WAN

2.5.1 Motivation

The motivation of this module is to help users with connecting the Nimble to the Internet. It will provide guidance on the necessary steps to be taken and rules to be followed while emphasizing the associated risks of transitioning from an offline-first network to an open Internet approach.

2.5.2 Learning Objectives

After completing this module, users will have hands-on experience with the process required to connect to the Internet and gain insights into the standards used for IP addresses to make such a connection. Additionally, users will learn about applying appropriate firewall policies to facilitate connections with the outside network.

2.6 Restricting Websites Access with Nimble

Restricting user's Internet access can increase productivity and protect your network from viruses and malicious content found on some websites. There are various ways to perform this operation, such as allowing access to all URLs except the ones you block or blocking all URLs and only allowing specific websites to enter your network. In this module, we focus on allowing all websites and blocking only specific websites from entering your network. The snapshot of this demo is given in the figures below.

After completing this module, users will have hands-on experience with the concept of aliases, as well as defining firewall rules to protect their network from external interference. Users will also gain ideas on the advantages of applying these policies to better protect their network and facilitate URL management on the network.

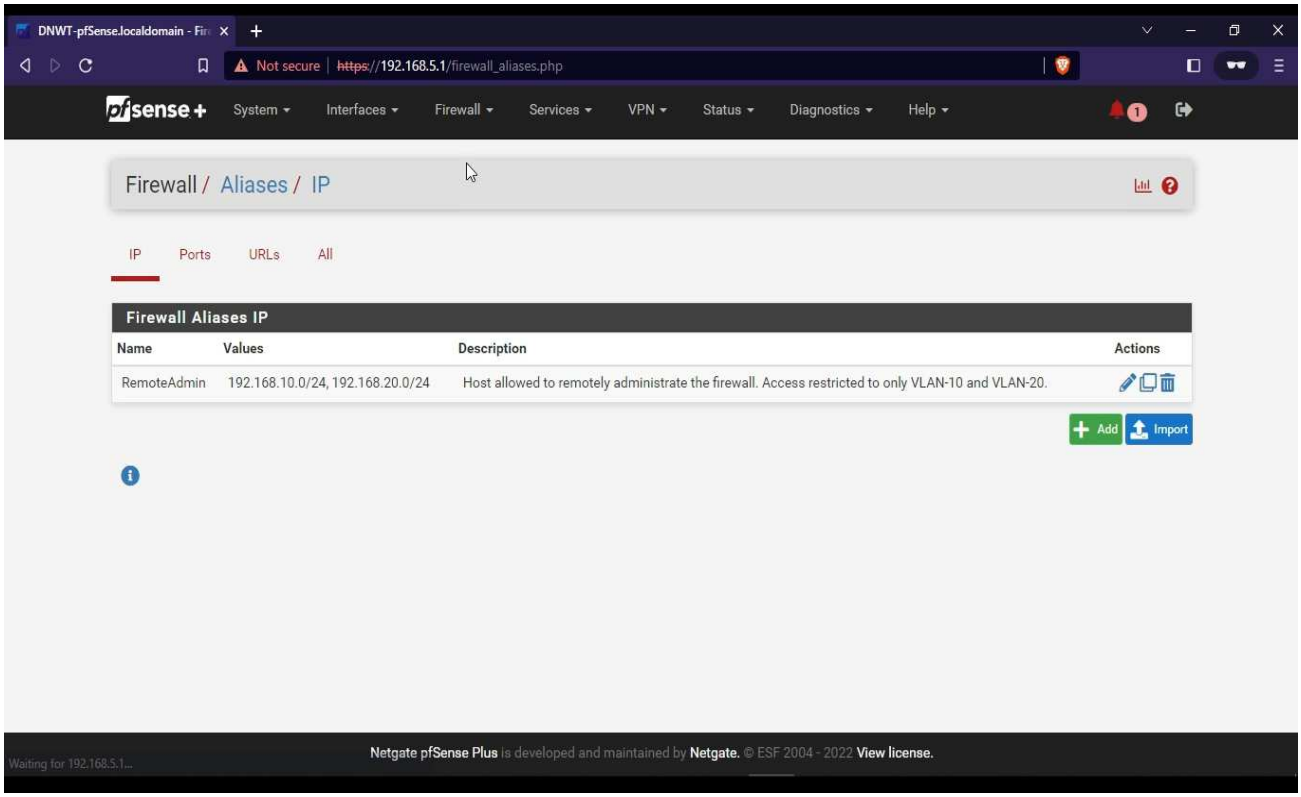

Figure 19: Firewall Aliases

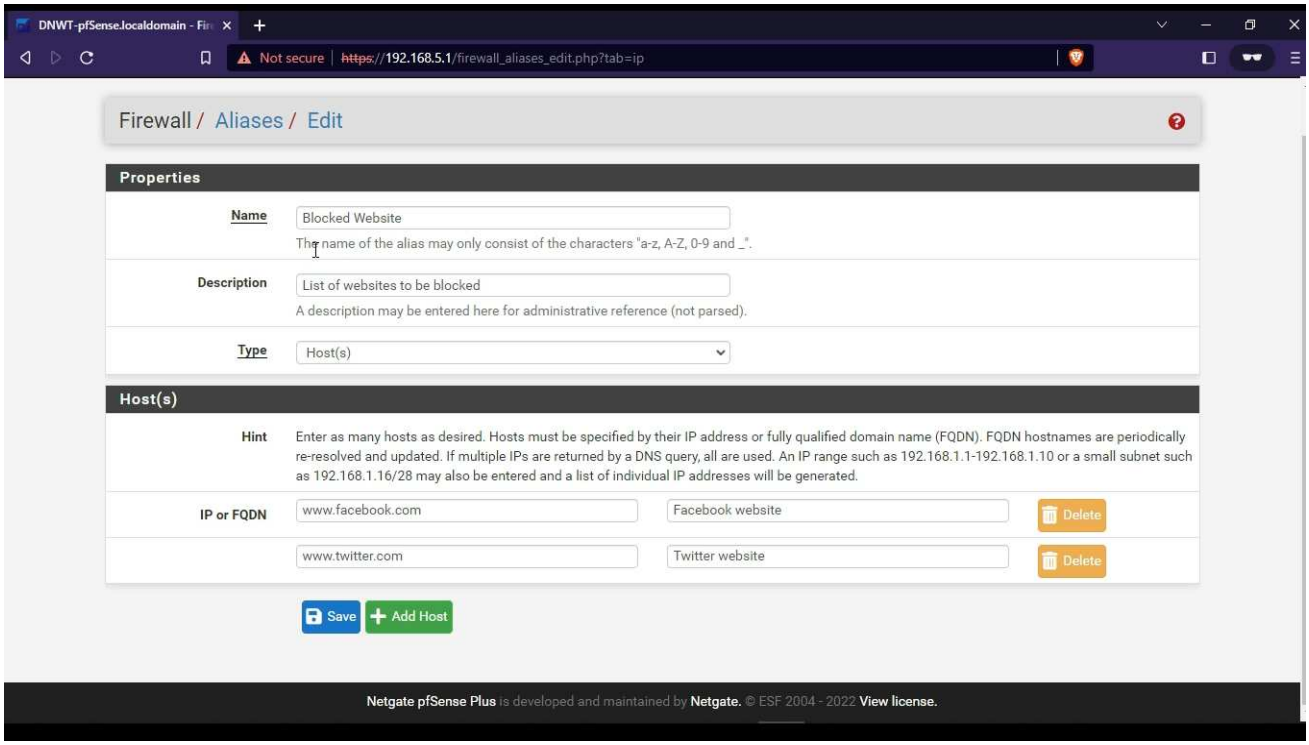

Figure 20: Host Addition

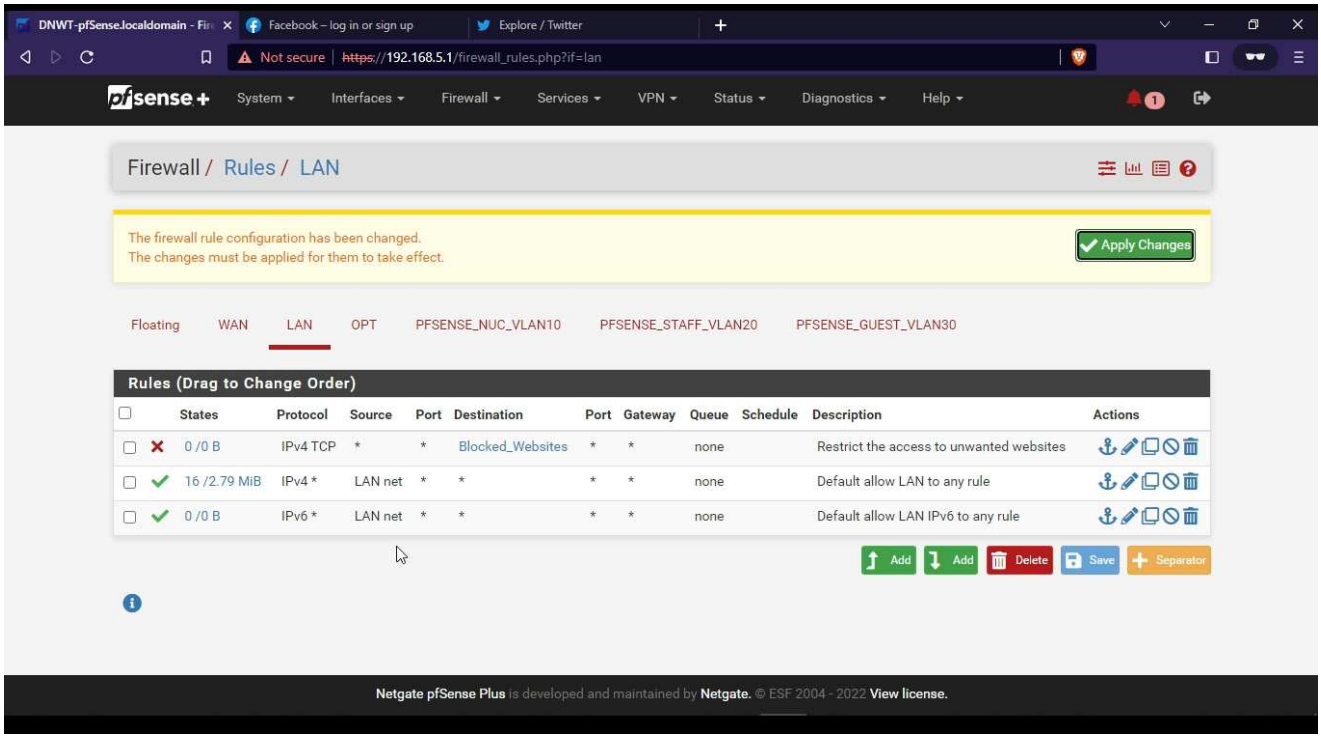

Figure 21: Firewall Rules

2.6.1 Motivation

The motivation of this module is to help users block unwanted websites from their network. This module will help users understand the security aspects of their network by keeping it safe from malicious websites and increasing productivity. Restricting certain websites from entering the network is important to increase the safety and security of the network.

2.6.2 Learning Objectives

Users will be able to perform the following tasks:

a. Defining the websites that need to be blocked from entering the network.
b. Understanding aliases and their implementation.
c. Defining firewall policy to block the websites.

2.7 Creating a Network on UniFi

This module provides knowledge on how to create networks on UniFi devices using a platform called as UniFi controller. All UniFi equipment can be managed using a single interface, which

offers intuitive configuration options as well as robust device control and monitoring.[1]. The controller, also referred to as UniFi Network Application hosts the feature allowing users to control UniFi devices like Switch, Aps, etc. In this module, we will learn about creating networks and assigning the networks to wireless services. The snapshot of the demo is given in the figures below. Users will be able to perform the following tasks:

a. Creating networks using UniFi network application.
b. Creating Wireless SSID using UniFi controller.
c. Managing the networks using the controller.
d. Managing the network based on AP groups.

2.7.1 Motivation

The motivation of this module is to help users to provide a hands-on demo to create networks using UniFi controllers on UniFi devices. This module aims to equip users with the knowledge required to implement and maintain networks on these devices and troubleshoot any problems related to network creation using UniFi Network Application.

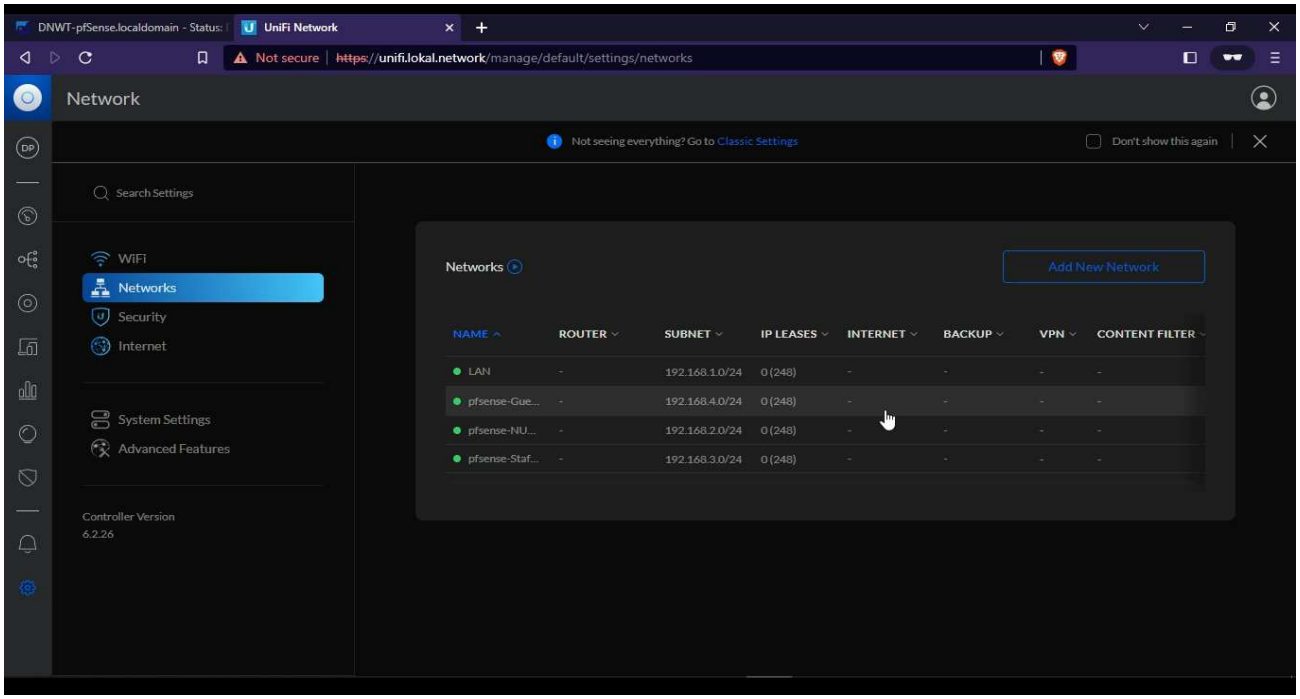

Figure 22: Creating a Network using UniFi Controller

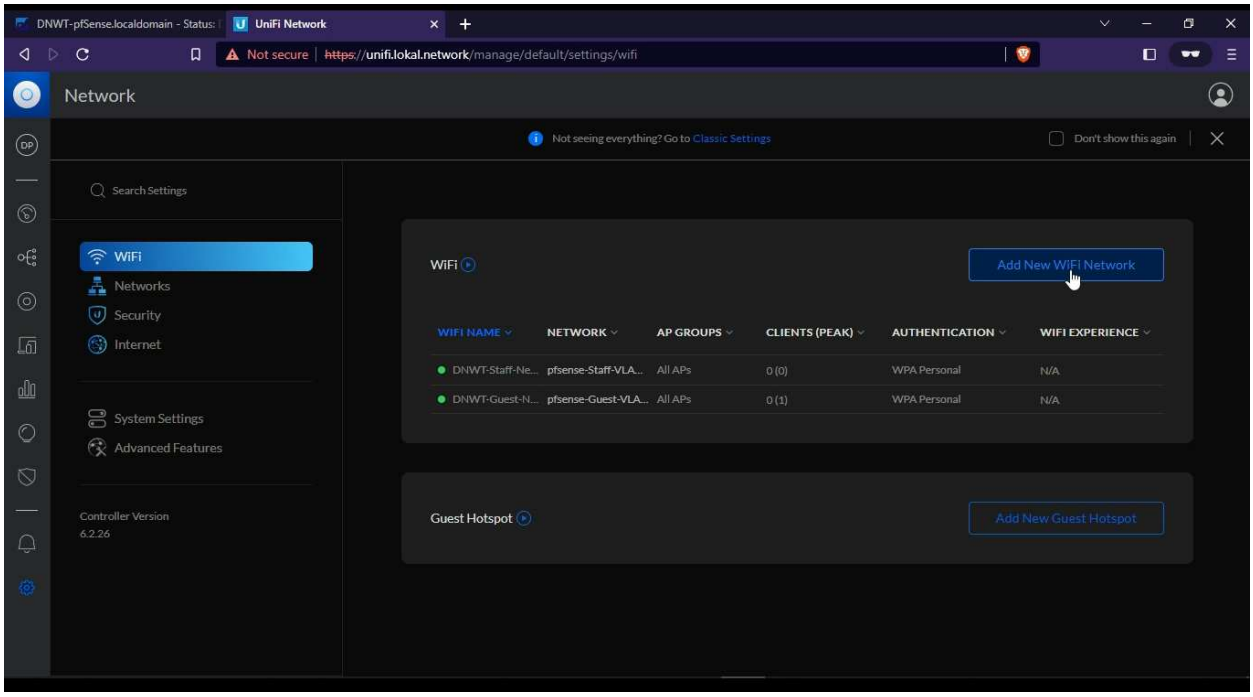

Figure 23: Creating Wi-Fi Network.

2.7.2 Learning Objectives

After completing this module, users will understand how to use the controller to configure networks for UniFi devices. Users will also be able to maintain their networks depending on their use cases.

2.8 Restricting Device Access with Nimble

Nimble does not offer the option to restrict access for a device attempting to connect to the network or to block it using MAC addresses. Instead, Nimble uses logical addresses to restrict access, and this module will guide users through the process of implementing this concept. It is important to note that blocking a particular IP address may not necessarily restrict the device from connecting to the network. As logical addresses can change, unlike physical addresses, users may need to block a pool of IP addresses or an entire subnet of IP addresses. Additionally, a device may still connect by switching the connection, so monitoring traffic is essential to ensure proper network management. This module will provide hands-on experience for restricting a specific IP address. The snapshot of the demo is included in the figures below.

After completing this module, users will possess the skills required to manage their network access rules and control device connections to their network. They will also be able to filter good and bad traffic using logical addresses and protect their network from unwanted access.

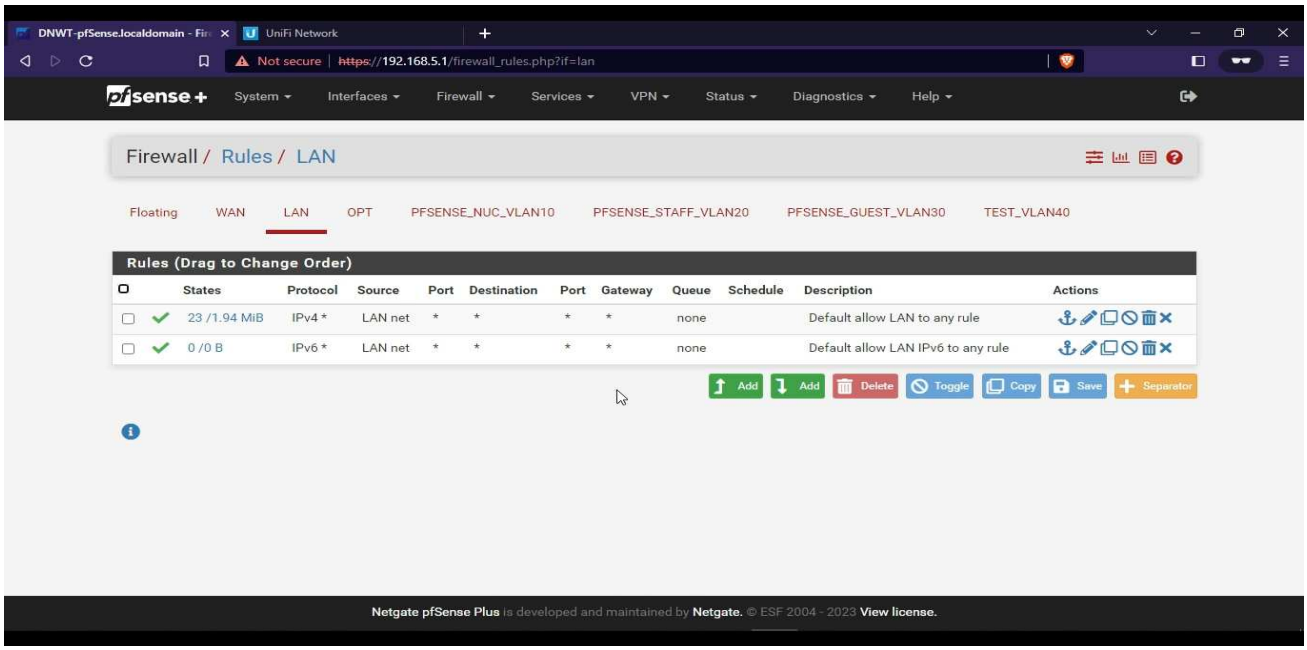

Figure 24: Firewall Rules

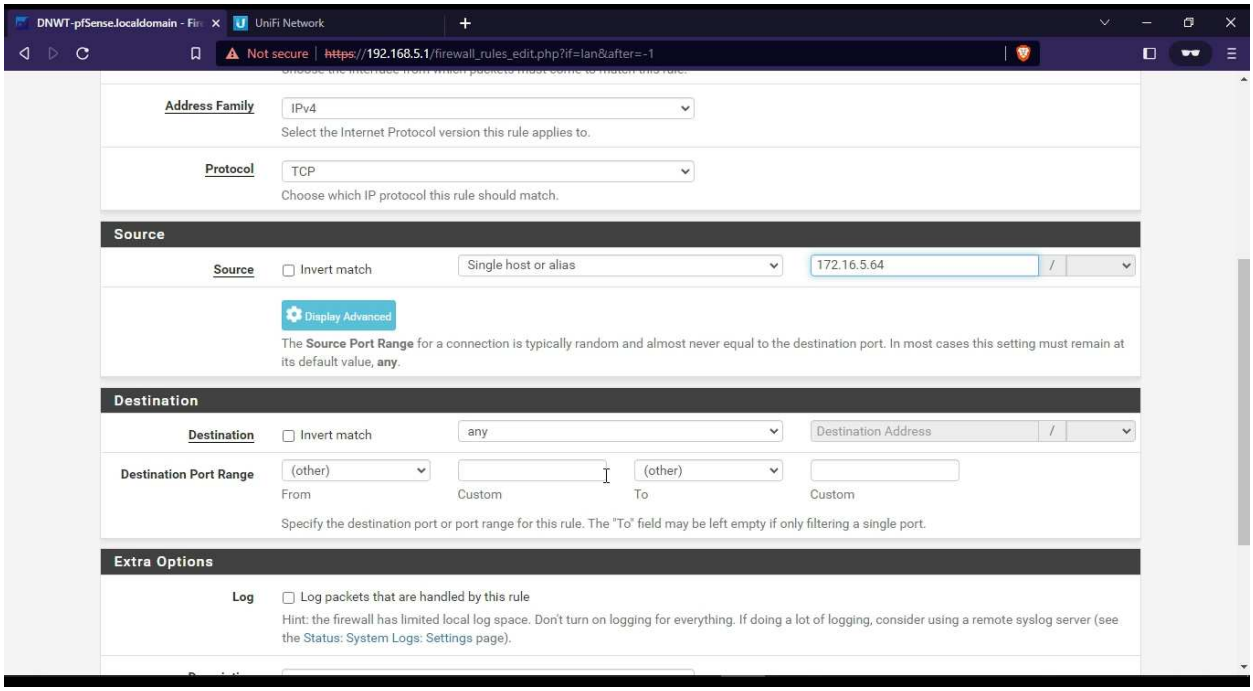

Figure 25: Restriction using Logical Address.

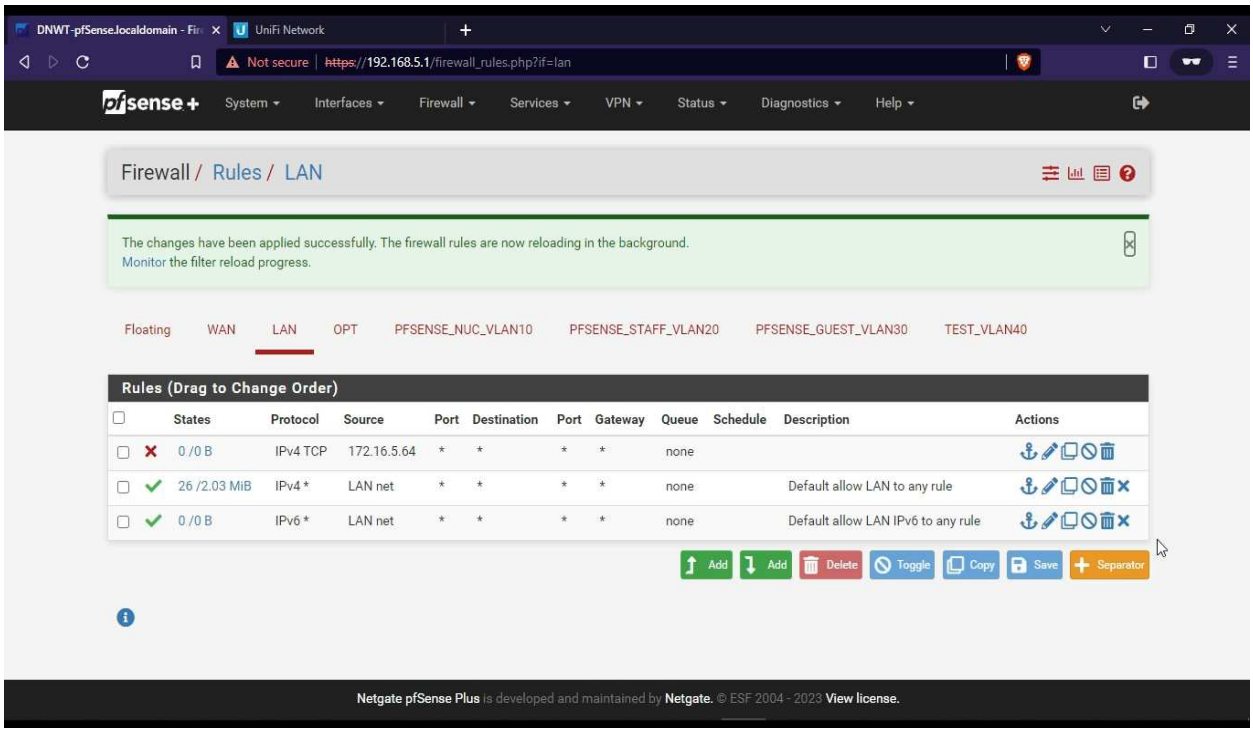

Figure 26: Active Firewall Policy

2.8.1 Motivation

The motivation of this module is to help users with the knowledge and hands-on demo to block unwanted devices from their network or devices trying to connect to their network using logical addresses. Providing users with the technical information necessary to execute this policy. Also provides users to manage their network access rules.

2.8.2 Learning Objectives

Users will be able to perform the following tasks:

a. Use of firewalls to restrict devices.
b. Understand the concept of logical address and physical address.
c. Implement a firewall policy to protect network infrastructure.

2.9 Implementing Firewall Policy on UniFi

This module provides knowledge on how to create firewall rules on UniFi devices using a platform called UniFi Controller. All UniFi equipment can be managed using a single interface, which offers intuitive configuration options as well as robust device control and monitoring [1]. The controller, also referred to as UniFi Network Application hosts the feature that allows users to control UniFi devices such as switches and access points. In this module, we will learn about creating firewall rules and implementing them on UniFi devices through UniFi Controller. The snapshot of the demo is given in the figures below. After completing this module, users will have the necessary skills to create, manage, and monitor firewall rules in their UniFi-managed networks. They will also understand the difference between established and invalid states.

2.9.1 Motivation

This module aims to provide users with a hands-on demonstration of how to create networks on UniFi devices using the UniFi controller. It will equip users with the necessary knowledge and skills to implement, maintain, and troubleshoot their networks using the UniFi Network Application.

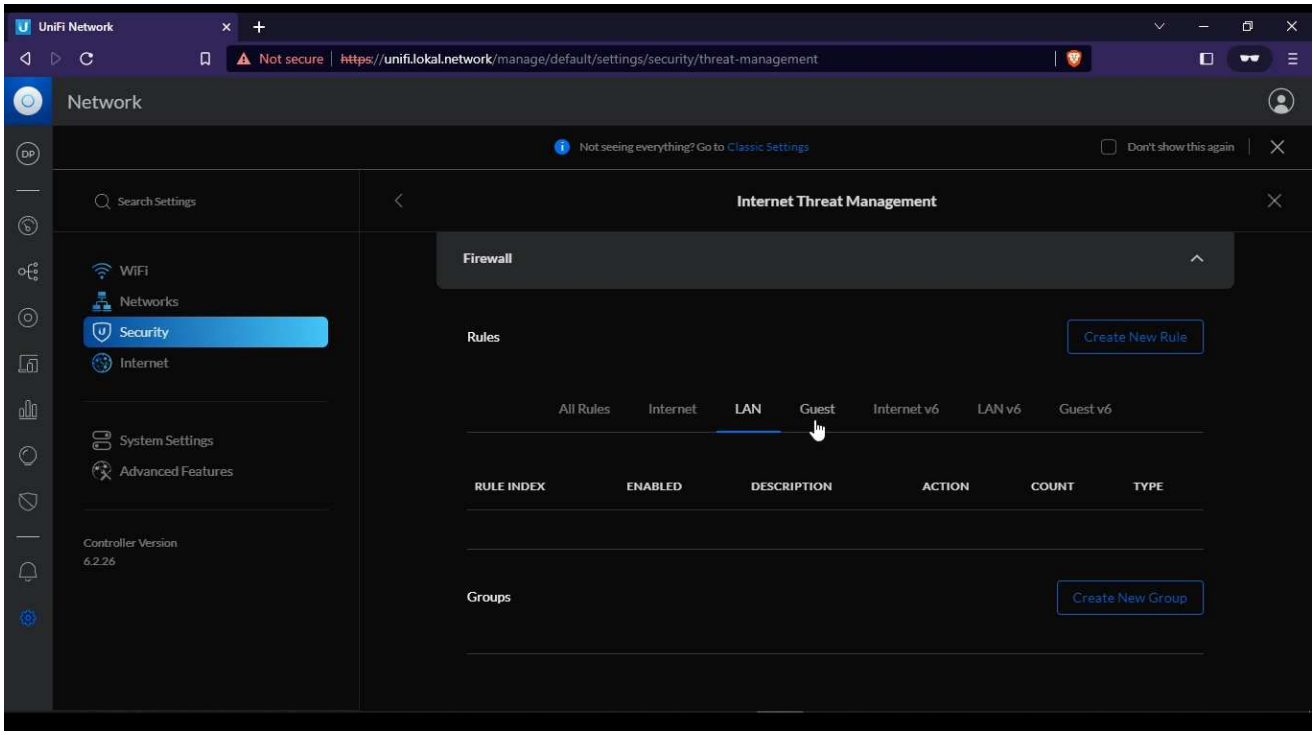

Figure 27: Implementation of Firewall rules on UniFi devices

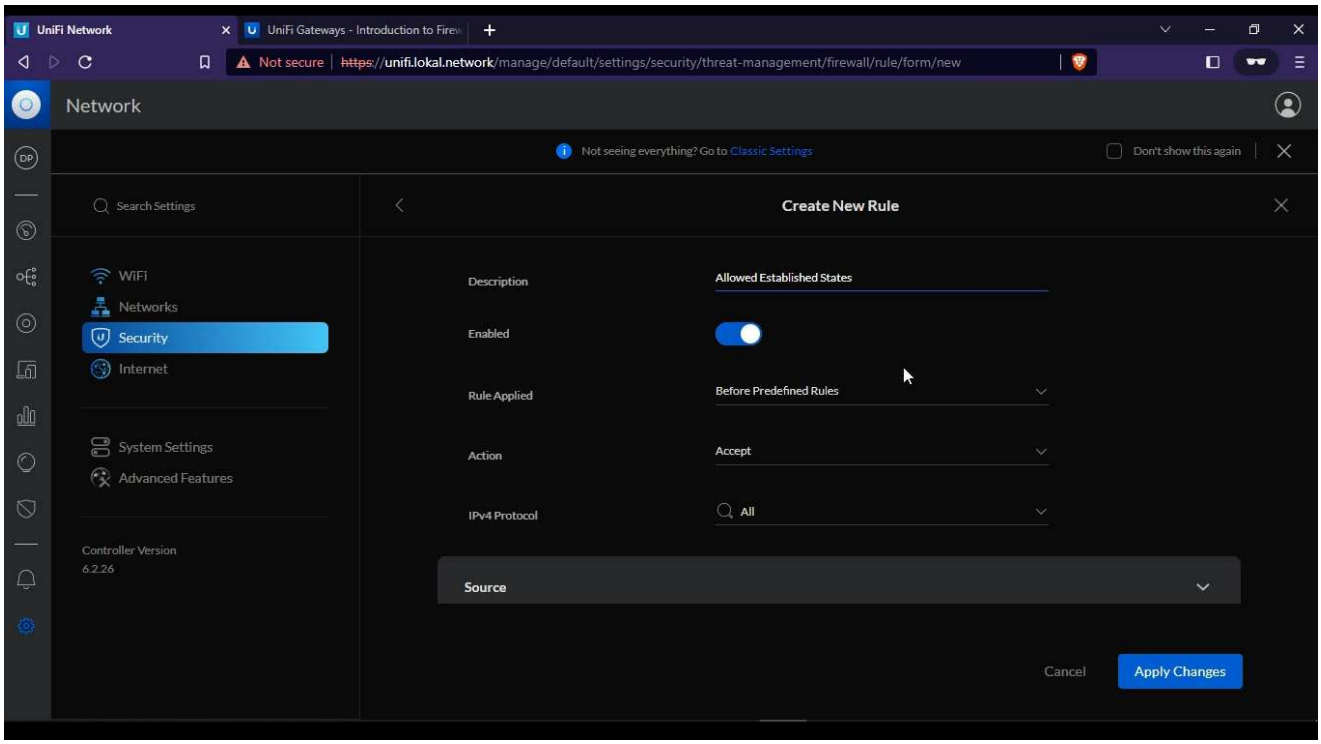

Figure 28: Creating Firewall Rule

2.9.2 Learning Objectives

Users will be able to perform the following tasks:

a. Creating firewall rules using the UniFi network application.
b. Implementing firewall policies for different internal and external interfaces.
c. Monitoring the policy using the controller.
d. Understanding the concept of established and invalid states.

2.10 Create and Restore Backup on Nimble

The critical aspect of every deployment is the planning and response for failover. If a live system goes down, it hampers the overall operation and possibly may result in loss of data or the devices getting crashed. It is important to be able to have a backup in place and restore it in case a failure occurs. This module will help users in this scenario with a hands-on demonstration and the technical skills required to perform this operation. Backup and restore is done with the pfSense router and a snapshot of which is given in the figures below.

After completing this module, users will be able to restore their network device from a hard reset and regain their data using previously stored backup information. They will also be able to recover their device from any misconfiguration using the backup file.

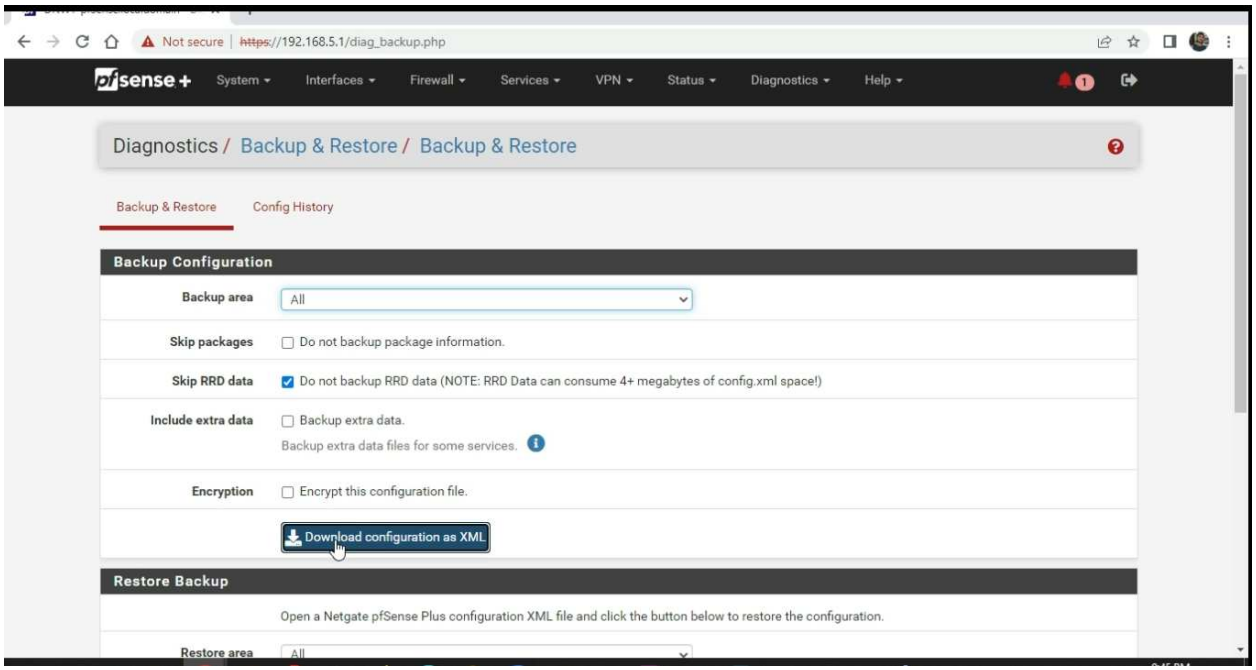

Figure 29: Creating Backup

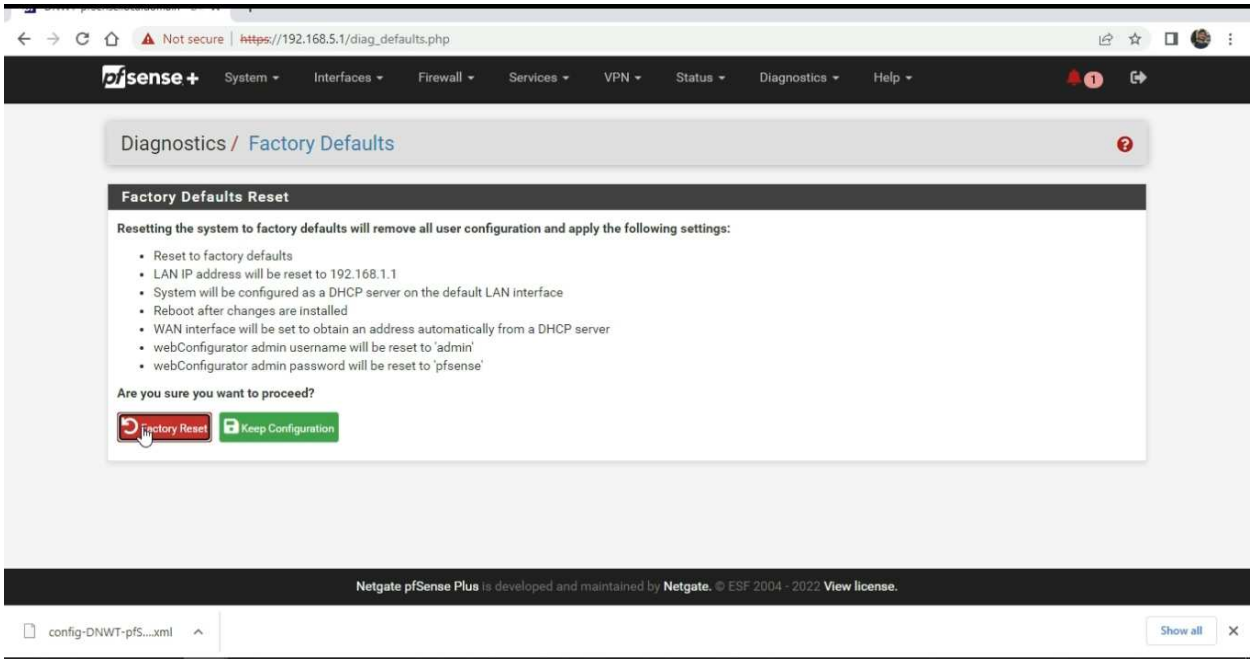

Figure 30: Factory Reset

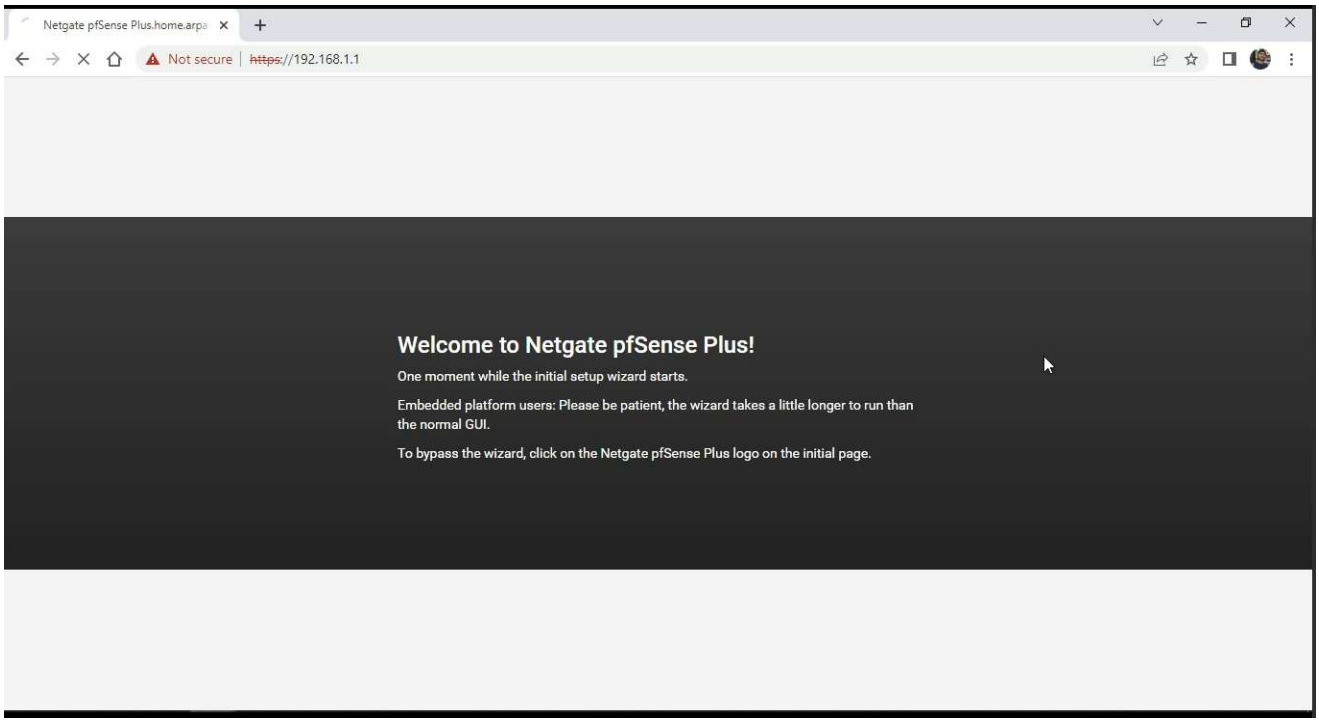

Figure 31: Reset Process

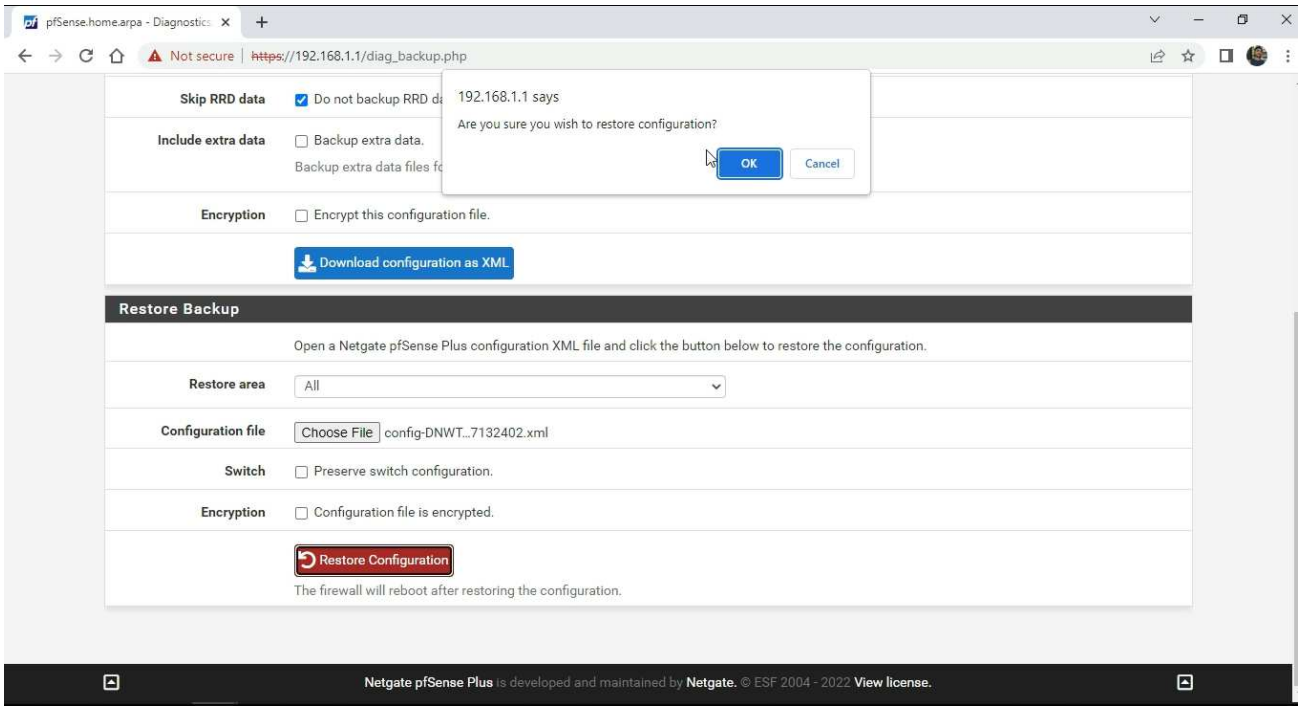

Figure 32: Restoring Backup

2.10.1 Motivation

The motivation of this module is to assist users with maintaining a backup of their network device and restoring it in case of failure. These skills will provide users with the technical knowledge necessary to recover successfully from an event. This module provides a hands-on demonstration to share knowledge on restoring their network from potential data loss.

2.10.2 Learning Objectives

Users will be able to perform the following tasks:

a. Create the backup file.
b. Resetting the device.
c. Restore the device using the backup file.

2.11 Knowledge Sharing on Security and Monitoring

The module is designed to provide users with knowledge about security and the fact that they are not anonymous on the Internet. It is more of a knowledge-sharing module than an implementation module that shows users, through a hands-on demo, how they can be tracked and have their activities monitored by external parties. The module provides a general overview of data traffic monitoring and how to remain secure and protected from unwanted parties. The snapshot is included in the figures below.

Upon completing the module, users will be able to understand how to keep their network secured and protect their privacy. They will also gain knowledge on how they can be tracked by external parties. This will help build a solid foundation for being aware of such situations and taking necessary actions when appropriate.

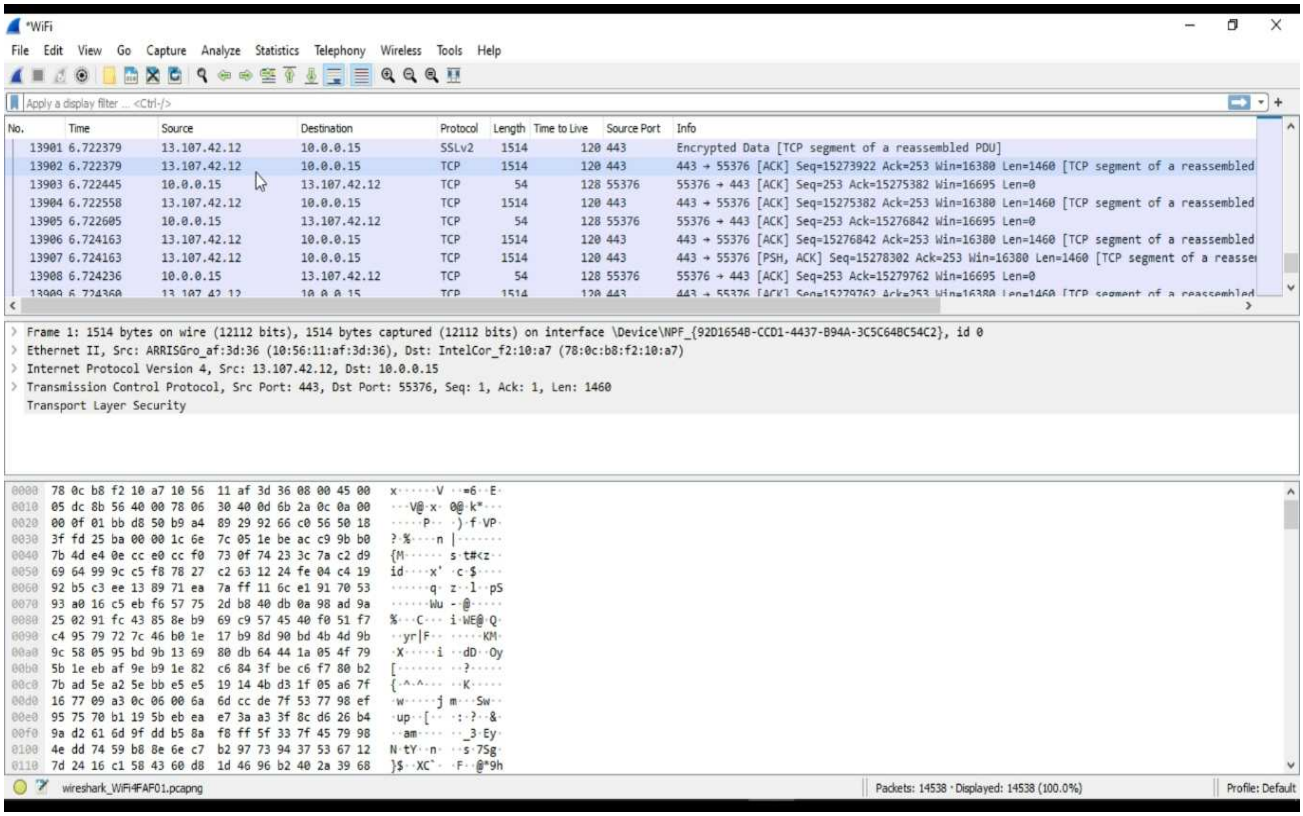

Figure 33: Capturing Traffic

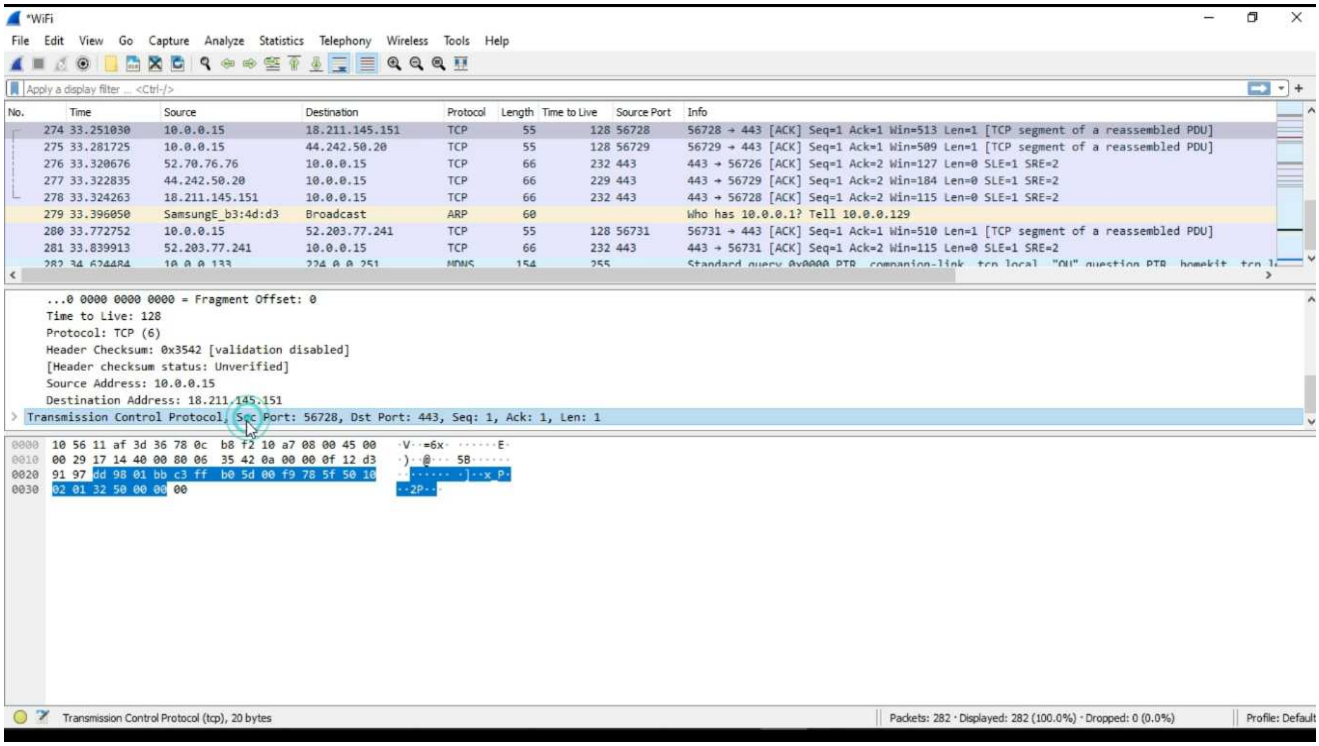

Figure 34: Analyzing the Traffic.

2.11.1 Motivation

The motivation of this module is to help guide users about the importance of understanding real-world scenarios and protecting information from third parties. Providing users with information on how they can be monitored and tracked.

2.11.2 Learning Objectives

Users will be able to perform the following tasks:

a. Gain knowledge of Traffic Monitoring
b. Learn about implementing security practices.

3. CONCLUSIONS

To conclude, this Nimble course uses short video vignettes to provide users with both knowledge and hands-on experience with various platforms. The idea of using videos to share information with end users provides additional resources for them to gain an in-depth understanding of Nimble, making it an effective way to enrich the user's learning experience. This method can help supplement key concepts of Nimble, provide real-life examples, and demonstrate problem-solving techniques. Users can learn about Nimble and gain technical expertise at their own pace, with the course providing a common platform for learning about different concepts used in Nimble. This interactive learning experience provides users with more efficient processing and memory recall.

The key observations from producing this course on Nimble are that it provides clarification for difficult concepts, including relevant content for the learning goals of each module, highlighting key information from specific topics, and communicating the learning objectives and motivation for each topic. This form of communication helps to build a stronger and more skilled community to operate Nimble successfully.

4. REFERENCES

1. Taneja, A., "Intranet and its application 'Community Networks' to overcome Digital Divide"2022. [Online]. Available: https://doi.org/10.7939/r3-rby4-a929.
2. Virtual LANs (VLANs) Netgate, "pfSense Documentation," 19 Jan 2021. [Online] Available: https://docs.netgate.com/pfsense/en/latest/vlan/index.html.
3. Why Videos are important in Education. 2023. [Online] Available: https://www.nextthoughtstudios.com/video-production-blog/2017/1/31/why-videos-are-important-in-education.
4. "IEEE CTU Summit 2021- Wakoma Nimble," Wakoma (2021, January 21). [Online] Available: https://www.youtube.com/watch?v=wjBn3O5Ksgg.
5. "Wireless Mesh Network", Wikipedia. [Online]. Available: https://en.wikipedia.org/wiki/Wireless_mesh_network
6. "Nimble," Wakoma. [Online] Available: https://wakoma.co/nimble/.