Instituto Tecnológico de Morelia

Computer Science Engineering

SECURITY IN SERVICES
PRACTICE 1

REPORT: ESTABLISHMENT OF A LABORATORY WITH NETWORK SERVICES (VMs)

BY:

RODRIGO VEGA LINARES

Morelia, Michoacán, Mexico. February 29th, 2024

Table of Contents:

Introduction ***3***

Problem Statement ***4***

Research & Development ***5***

Research **5**

Development **8**

Network Topology – "Dia" Diagram **8**

Results/Summary ***14***

Additional Topic – Firewalls **38**

Table 1 – Top 10 Firewalls 38

Table 2 – Firewalls: Pros vs Cons 38

Conclusion ***39***

References ***40***

Introduction

This report outlines and explains the establishment of a structured network incorporating WAN, LAN and DMZ segments, achieved through the implementation of the “pfSense” firewall to oversee and regulate the network management. Additionally, the process of implementing main network services, including a web server, storage server, radius server, network clients and name server, will be described. For the web server “Wordpress Bitnami” is being used, “TrueNAS Scale” serves as the storage server, “pfSense” functions as the RADIUS server, “Kali Linux” is utilized for the network clients and either “TrueNAS or Wordpress Bitnami” could be used for the name server.

The implementation of common network services in servers (VMs), creates a laboratory environment that serves as a platform for conducting subsequent vulnerability assessments and analysis using the capabilities of “Kali Linux”.

Glossary:

Below is a glossary with some terms and concepts related to virtualization.

- **Baremetal:** Running an operating system directly on hardware without using virtualization technology.
- **Paravirtualization:** Approach where the guest operating system is modified prior to installation inside a VM. Allowing it to work more efficiently with the hypervisor, resulting in better performance.
- **VM (Virtual Machine):** Virtual representation or emulation of a physical computer. They are referred to as guest while the physical machine they run on is the host.
- **KVM (Kernel-based Virtual Machine):** Linux kernel that enables the virtualization of hardware, turning the host operating system into a hypervisor.
- **QEMU:** Is an open-source emulator and virtualizer, used for development and testing purposes.
- **Hypervisor:** Software that allows multiple operating systems (VMs) to run sharing the resources of a single physical machine.

- **Services virtualization:** Simulating real services for testing purposes, ensuring software reliability and performance.
- Server Pools: Collection of servers grouped together to distribute workloads, enhance efficiency, and improve resource utilization.
- High availability: Ensuring uninterrupted system operation by minimizing downtime through redundancy and failover mechanisms.
- Container: Lightweight, portable, and scalable packaging of software that include code, libraries and dependencies, able to run in any environment.
- Multithreading: Execution of multiple threads or tasks concurrently within a single process, improving program efficiency on multi-core processors.

Problem Statement

Nowadays, modern companies are increasingly vulnerable to cyberattacks that exploit network services, such as code injection, buffer overflow and authentication bypass. These vulnerabilities pose a significant threat, as they can result in data breaches, financial losses and reputational damage. Addressing this problem requires the creation of a secure and controlled environment dedicated to perform vulnerability assessments on these services, ultimately aiming to identify and mitigate potential security risks.

Network services play a critical role, by enabling communication, connection and resource management in clouds environments, as well as in the application maintenance and development. In this manner, companies can select the network services that best align with their specific infrastructure needs.

Research & Development

Research

In this section, general concepts related to the practice will be described.

Perimeter Firewall

“A network perimeter firewall is a secured boundary providing the main defense of a private network and other public networks, such as the internet. The firewall detects and protects the network against unwanted traffic, potentially dangerous code, and intrusion attempts” (*VMware*, 2023).

The firewall act as a gatekeeper, positioned between a company’s network and external untrusted networks, controlling the traffic flow through the implementation of the next methods:

- **Static Packet Filtering:** “Method of filtering traffic based on the packet header addressing information. This is commonly used in larger organizations to prevent banned websites from being accessed (e.g., social media)” (*VMware*, 2023).
- **Proxy Services:** Acts as an intermediary between the internal network and external networks (internet), it prevents direct packet transfers from either side of the firewall, enhancing security by making it harder for intruders to determine the location of the network from the packet.
- **Stateful Inspection:** Logs outgoing traffic and permits only the return of traffic matching an initial request. This safeguards against external networks threats like IP spoofing and network scanning.

Firewall rules: Instructions within a firewall that dictate how the firewall should handle incoming and outgoing traffic, determining whether to block or allow communication based on factors such as IP address, ports, protocols and services. Some recommended practices are documenting the rules across multiple devices, implementing a deny by

default policy, monitoring firewall logs, grouping firewall rules, configuring application-level controls, implementing least-privileged access (access to minimum privileges to perform tasks) and blocking certain ports.

NAT rules: Enable traffic flow between private and public networks by translating private IP addresses to routable, public IP addresses.

Common network services

- **Virtual Networks:** Network environment where all devices communicate through software and wireless technology rather than physical hardware connections.
- **Load balancers:** “Device that sits between the user and the server group and acts as an invisible facilitator, ensuring that all resource servers are used equally” (*AWS*, n.d.).
- **DNS (Domain Name System):** Translates human readable domain names to machine readable IP addresses.
- **RADIUS Server:** “Is a client-server protocol and software that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service” (*TechTarget*, 2021).
- **Web Server:** Hardware and software that uses HTTP/HTTPS to respond to clients requests made over the World Wide Web.
- **Content Delivery:** “Method of providing web-based media over a particular medium, such as the Internet or television broadcast channels” (*Optimizely*, 2021).
- **Gateway:** “Network node used in telecommunications that connects two networks with different transmission protocols together” (*TechTarget*, 2019).
- **Network monitor:** “Provides the information that network administrators need to determine, in real time, whether a network is running optimally” (*Cisco*, 2023).
- **IaaS:** “Cloud computing model that provides on-demand access to computing resources such as servers, storage, networking, and virtualization” (*Google*, n.d.).
- **PaaS:** Cloud computing model offering a flexible, scalable platform to develop, run and manage apps, delivered by a third-party service provider.

- **SaaS:** Delivery model enabling users to access and utilize cloud-based applications via the internet eliminating the need for software installation and maintenance.

Network Segments

LAN (local area network): “Collection of devices connected together in one physical location, such as a building, office, or home. A LAN can be small or large, ranging from a home network with one user to an enterprise network with thousands of users and devices in an office or school” (*Cisco*, 2023).

WAN (wide area network): “Form of telecommunication networks that can connect devices from multiple locations and across the globe” (*CompTia*, 2019). It connects multiple LANs and allows them to communicate with each other.

DMZ (demilitarized zone): “Perimeter network that protects and adds an extra layer of security to an organization’s internal local-area network from untrusted traffic” (*Fortinet*, n.d.). It allows an organization to access the internet while maintaining their LAN secure, by storing external-facing services, resources and servers within.

Development

Network Topology – “Dia” Diagram

In this section, the network topology being implemented in the laboratory will be presented and explained, as shown in Figure 1.

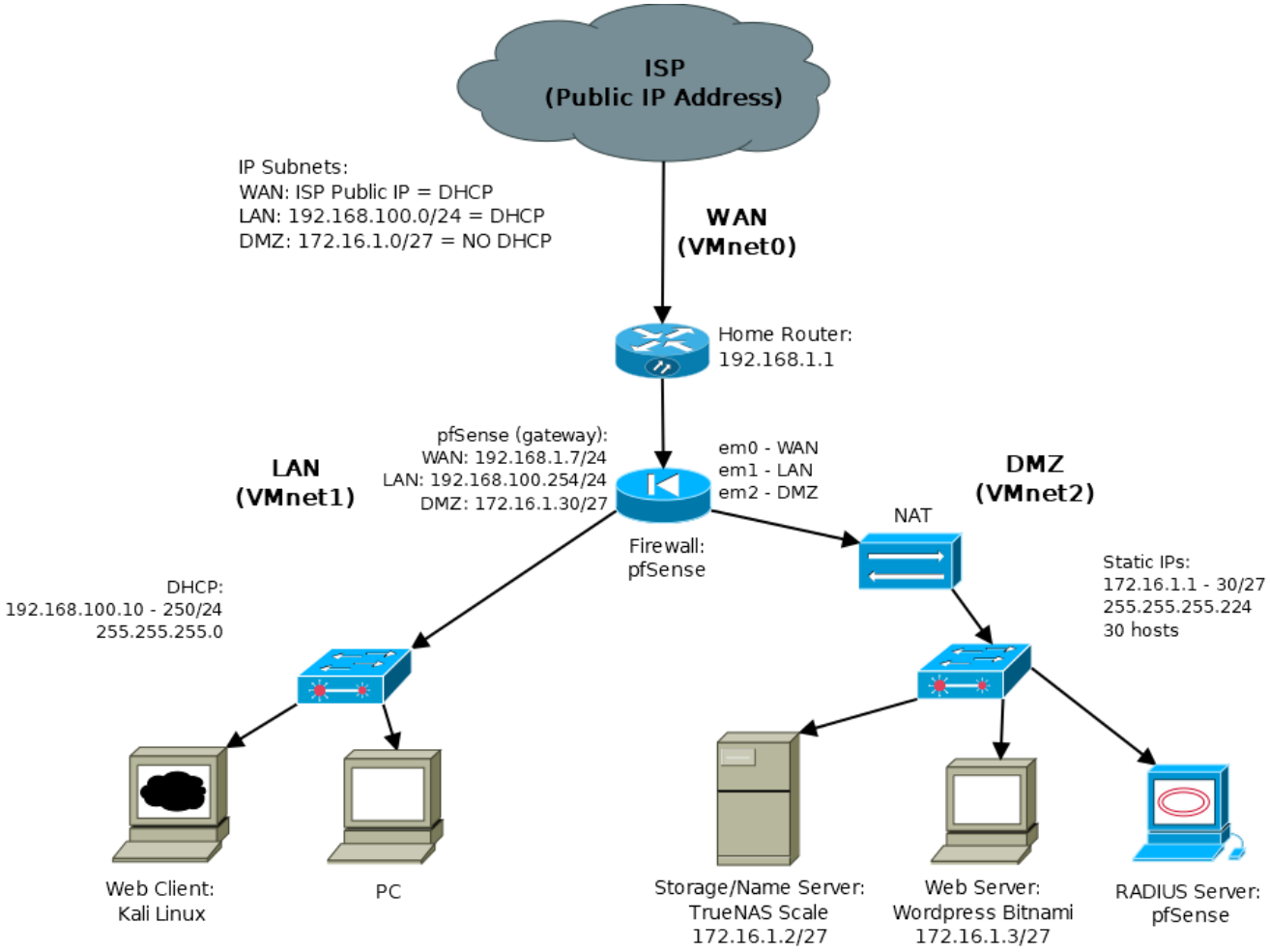

Figure 1.Laboratory Network Topology.

The network begins with the ISP, which uses a public IP address, it then connects to the home router, forming the WAN. The router is then linked to the pfSense firewall, responsible for traffic monitoring, NAT and RADIUS authentication (represented in the DMZ segment). It then further segregates into LAN and DMZ segments. Notably, the firewall utilizes interface em0 as WAN with the IP automatically assigned by the home router, em1 as LAN with a static IP of 192.168.100.254 and em2 as DMZ with a static IP

of 172.16.1.30. This configuration positions pfSense as the gateway between LAN and DMZ segments.

The LAN segment includes a Kali Linux web client and a PC, which could be running any operating system. DHCP is employed within this segment, using an IP address range of 192.168.100.10 to 192.168.100.250 with a /24 subnet.

In the DMZ, there is a TrueNAS Scale for storage and name service, alongside a WordPress Bitnami serving as the web server. In this segment, DHCP is not being utilized for connectivity, instead the storage/name server has a static IP of 172.16.1.2, and the web server is assigned the IP 172.16.1.3.

The laboratory is described in three phases, and each one will now be explained.

Phase 1

In this phase, the main network services are established, justifying their use and describing a summary of the installation and changes implemented.

- Wordpress Bitnami is employed as the web server for its simplicity in installation and configuration, making the setup process straightforward. The virtual machine is downloaded from the official Bitnami page and imported into VMware Workstation. It is using VMNet1, with 20GB of hard disk and 3GB of RAM. A static IP address, set to 172.16.1.2, is configured following the documentation. A crontab is implemented to reset the network service and retrieve the configured static IP address upon every machine boot. Screenshots are provided as shown in Figure 2-8.

- TrueNAS Scale is utilized as the storage and name server due to its scalability and user-friendly nature. The ISO is downloaded from the official page, and a new VM is created with 10GB of RAM, 20GB hard disk for installation and three 30GB hard disk for a RAIDZ1. A pool is created with the RAIDZ1 set up, leaving 53GB. The web GUI interface port is changed from 80 to 8080.

- iSCSI Configuration:
  - A 40GB Zvol is added inside the pool.
  - iSCSI service configuration involves adding a portal, a target, an extent and an associated target.
  - A dataset with a capacity of 10GB is added.
- SMB share configuration:
  - A dataset is added inside the pool, utilizing the remaining capacity (expected to be 3GB).
  - A local group and a local user are added.
  - The SMB service is set to start automatically.
  - An SMB Share is created and the ACL is edited to add the local group.
  - Testing is conducted by accessing from a LAN client to the DMZ.

Screenshots illustrating the configurations are provided in Figure 9-25.

- pfSense acts as the RADIUS server due to the availability of packages that extend its capabilities beyond being solely a firewall. The ISO is downloaded from the official page and a new VM is created. It uses 20GB hard disk and 4GB of RAM, with three network adapters (VMnet0, VMnet1 and VMnet3). From the web GUI, the DNS server is configured for LAN and OPT1 (DMZ) address pool ranges. The address pool range for LAN is 192.168.100.10 to 192.168.100.245, and for OPT1 (DMZ) is 172.16.1.5 to 172.16.1.29. Aliases are added, for ports 443 and 80, named “Web”, and for IP address 172.16.1.2 for TrueNAS and 172.16.1.3 for WordPress. Screenshots are provided as shown in Figure 26-39.

- Kali Linux act as the network client since the purpose is to test the laboratory in the future, and any client could potentially attack the network at any moment. It usually operates on VMNet1 (LAN). It has 50GB for the hard disk and 8GB of RAM.

Phase 2

In this phase, the design of the network by services is carried out, separating the network by traffic type.

The following settings depict how it is implemented in “Virtual Network Editor” of VMware Workstation:

- WAN network: Belongs to VMnet0, with the network connection type set to bridged (connecting machines directly to the external network). It uses the NIC (network interface card) identified as "Intel(R) Wi-Fi 6 AX201" in this laboratory and it obtains the IP address from the router.
- LAN network: Belongs to VMnet1, with the type set to bridged, using the ethernet port/adapter, named "Realtek PCIe GbE Family Controller" in this laboratory.
- DMZ network: Belongs to VMnet2, with the type set to host-only (connecting machines internally in a private network). It has no DHCP, as a result, the subnet IP is 172.16.1.0/27. Additionally, the option "connect a host virtual adapter to this network" is enabled, making all the servers in the DMZ accessible from the host machine (Windows), such as TrueNAS Scale and the web server WordPress Bitnami.

Screenshots are provided as shown in Figure 40-42.

Phase 3

In this phase, the configuration of the perimeter firewall pfSense is established, including the assignment of interfaces, IP address allocation, and definition of policies/rules.

- The first task involves the assignment of interfaces through the pfSense console. Interface em0 is designated for the WAN network segment, em1 for the LAN segment, and em2 for the OPT1 (DMZ) segment.
- The allocation of IP addresses is performed via the pfSense console. The LAN network is assigned IP address of 192.168.100.254 with a /24 subnet, utilizing DHCP with a range of 192.168.100.10 to 192.168.100.250. The DMZ network is assigned IP address of 172.16.1.30 with a /27 subnet, without the implementation of DHCP. The IP addresses are pinged both internally and using google DNS 8.8.8.8 to verify proper functionality.
- Defining firewall rules is accomplished through the pfSense WebGUI, specifically within the “Firewall/Rules” section.
    - The LAN segment comprises six rules, excluding “Anti-Lockout Rule”:

        - First rule allows traffic from LAN to DMZ. It has the protocol IPv4 TCP, source LAN subnets, any port, and destination OPT1 subnets on port 8080 intended for TrueNAS.
        - Second rule allows traffic from LAN to DMZ, using protocol IPv4 TCP, source LAN subnets, any port, and destination OPT1 subnets on port 445 (SMB).
        - Third rule allows traffic from LAN to DMZ, using protocol IPv4 TCP, source LAN subnets, any port, and destination OPT1 subnets on port 80 (this rule is already included in sixth rule).
        - Fourth rule allows traffic from LAN to WAN using protocol IPv4 TCP/UDP, source LAN subnets, any port, and destination “This Firewall (self)” WAN address on port 53 (DNS).
        - Fifth rule, similar to the fourth, blocks traffic from LAN to WAN, preventing DNS injection or unauthorized external DNS resolution.
        - Sixth rule facilitates internal navigation, allowing traffic from LAN to any destination. It uses protocol IPv4 TCP, source LAN subnets, any port, and “any” destination on specific ports (80 and 443) using “Web” alias.
    - The DMZ (OPT1) segment incorporates three rules:
        - The first permits DNS traffic from DMZ to WAN, utilizing IPv4 TCP/UDP protocol, with source OPT1 subnets, any port, and destination “any” on port 53 (DNS).
        - The second permits internet navigation traffic from DMZ to WAN with similar configurations but exclusively using TCP protocol, and destination ports specified using the “Web” alias for port 80 and 443.
        - The third permits ICMP protocol for executing “ping” commands, which are solely used to test connectivity. It uses IPv4 IMCP protocol, allowing traffic from source OPT1 subnets on any port to any destination and port.
    - The WAN segment has no manually created rules, as they are automatically generated when selecting the option “create new associated filter rule” in the port forwarding section.

- In the section “Firewall/NAT/Port Forward” two port forwarding rules are established. Important to note the selection of the “create new associated filter rule” option for both rules, ensuring the creation of corresponding WAN rules.
  - The first rule enables NAT translation from WAN to DMZ, allowing access to the web server. This rule utilizes the WAN interface, TCP protocol, with the source set to “any”, source port to “any”, and destination “This Firewall (self)” WAN address on ports 80 and 443, using “Web” alias, with NAT IP of 172.16.1.3, and the same “Web” alias for the NAT Ports.
  - The second rule is similar to the previous, allowing access to the storage/name server. The destination ports and NAT ports change to 8080, along with the NAT IP to 172.16.1.2.

Screenshots are provided as shown in Figure 43-59.

Phase 4

In this phase, the functionality of the services is tested.

- WAN to DMZ: Access from the host machine (Windows 11) to the storage/name server (TrueNAS Scale) and the web server (WordPress Bitnami) works successfully. Typing http://192.168.1.7:8080 in a browser translates with NAT, to access 172.168.1.2, and when entering http://192.168.1.7:80 it translates to 172.16.1.3. Thus, any source IP address in the WAN can access these servers.
- WAN to LAN: No rules or configurations have been implemented.
- LAN to WAN: The LAN network has successfully established a connection to the internet, allowing navigation in the IPv4 protocol on ports 53, 443 and 80. Testing was conducted using the web client (Kali Linux).
- LAN to DMZ: Access is functional for the storage/name server (TrueNAS Scale) when entering http://172.16.1.2:8080/ in a browser and also for WordPress when accessing http://172.16.1.3. Testing was conducted using the web client (Kali Linux).
- DMZ to LAN: No rules or configurations have been implemented.

- DMZ to WAN: The implemented rules function successfully, allowing both the storage/name server (TrueNAS) and web server (WordPress) to access the internet via ports 53, 80 and 443. This facilitates the ability to update software. Testing was performed using the console terminal (CLI) for both VMs.

Screenshots are provided as shown in Figure 60-66.

Results/Summary

In this section evidence of phase 1,2,3 and 4 of the development employment of the laboratory will be showed. In this section only a summary or most important screenshots will be provided to not flood the report with every single step.

Phase 1

In this phase, screenshots of the installation and setup of main network services are displayed.

Figure 2. WordPress Bitnami.

Figure 3. WordPress Bitnami - Login.

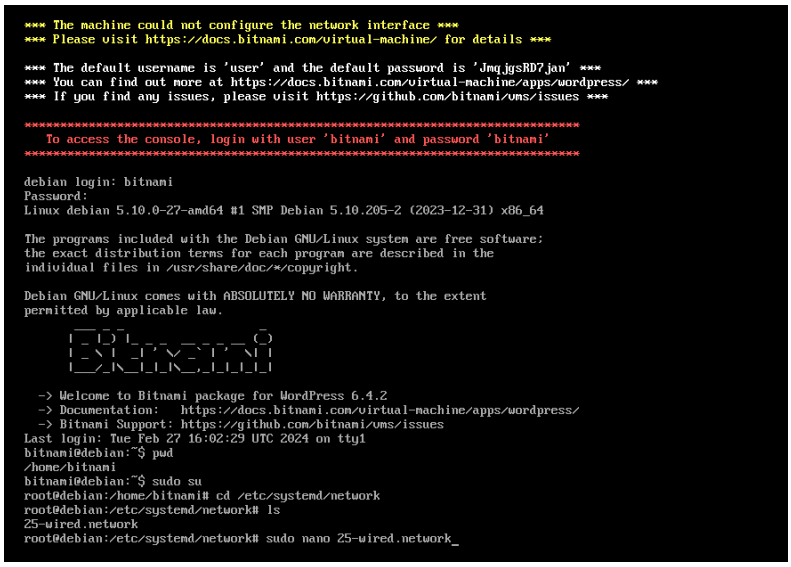

Figure 4. WordPress Bitnami - Setting Static IP.

Figure 5. WordPress Bitnami - Setting Static IP.

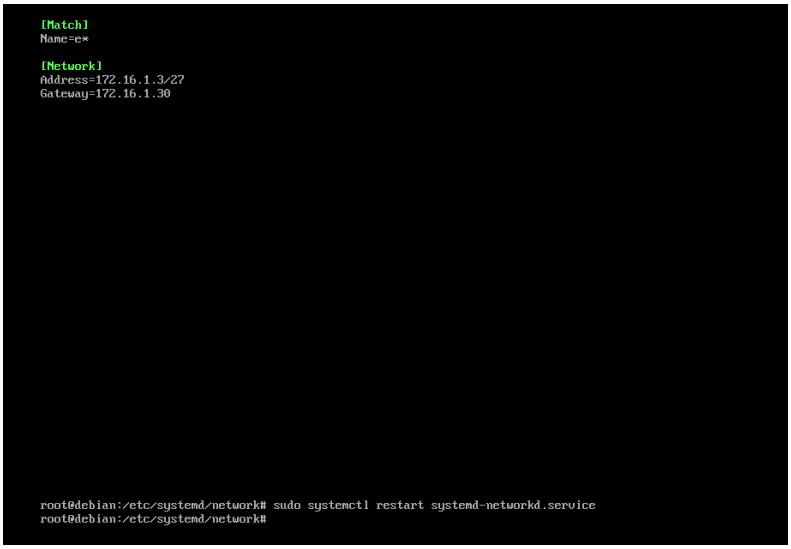

Figure 6. WordPress Bitnami - Setting Static IP.

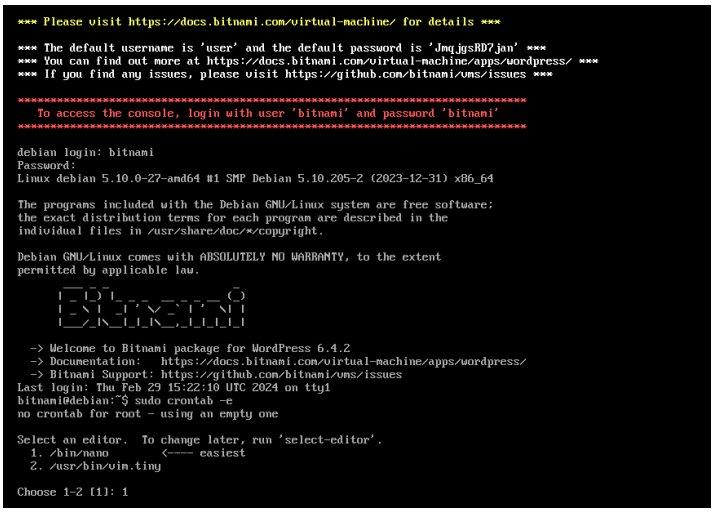

Figure 8. WordPress Bitnami - Cronjob

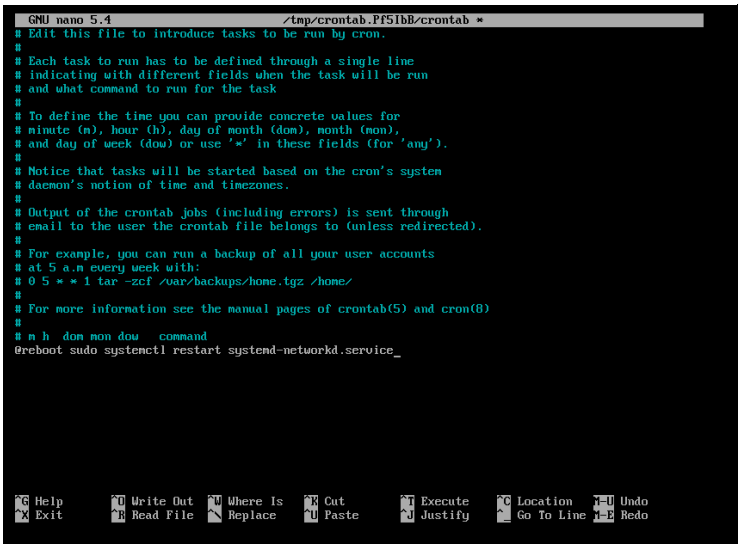

Figure 7. WordPress Bitnami - Cronjob.

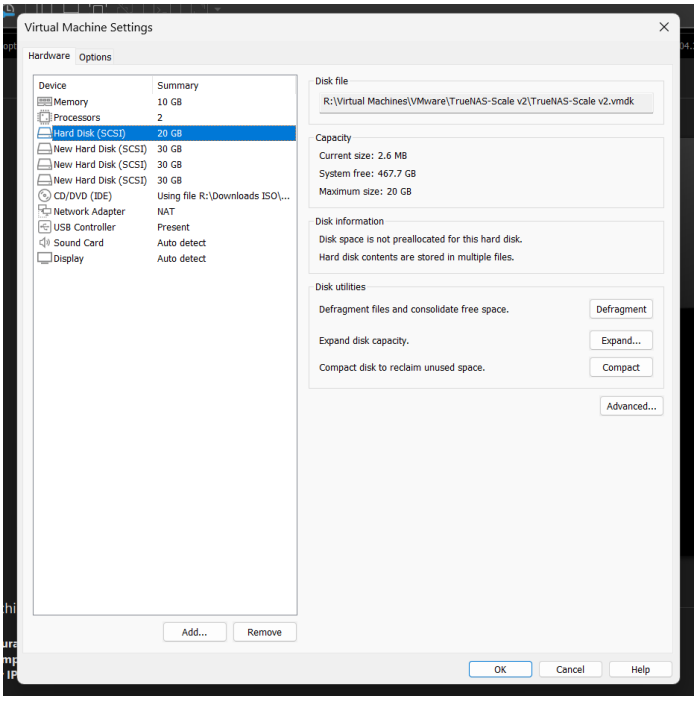

Figure 9. TrueNAS Scale - VM Settings.

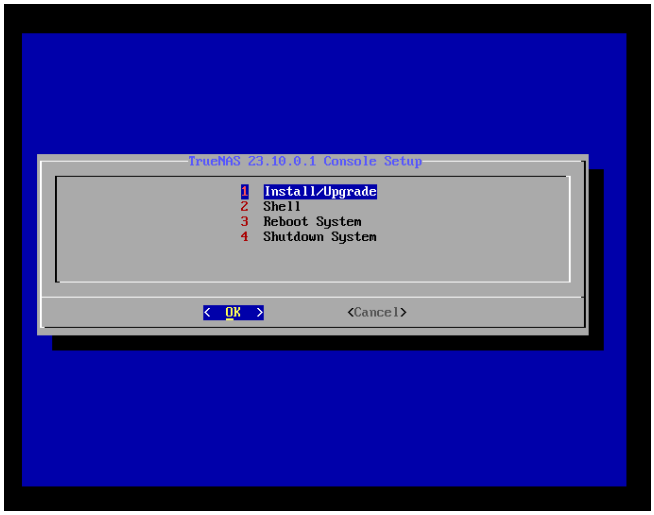

Figure 10. TrueNAS Scale - Installation.

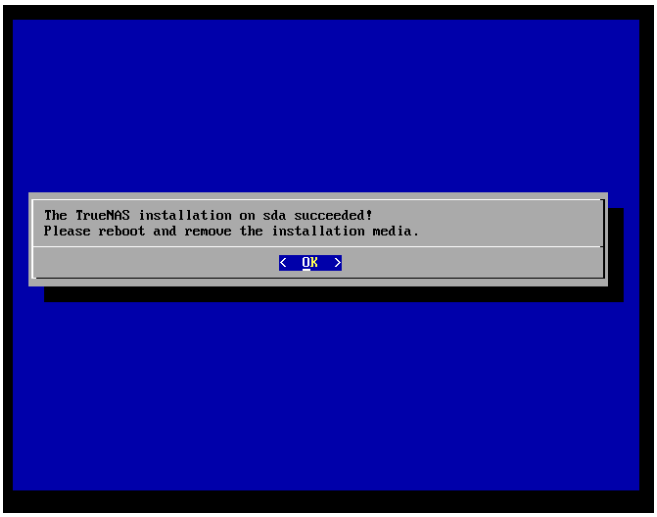

Figure 11. TrueNAS Scale - Installation.

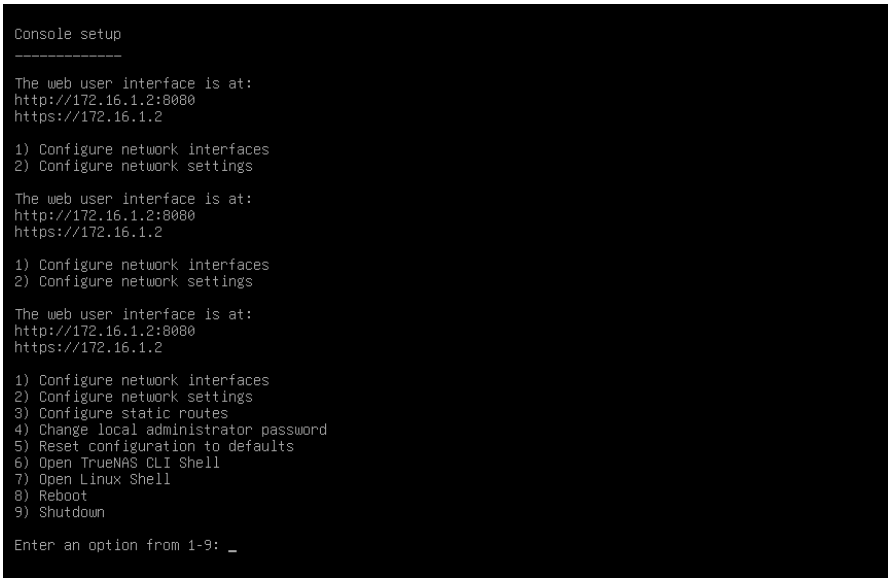

Figure 12. TrueNAS Scale - Console.

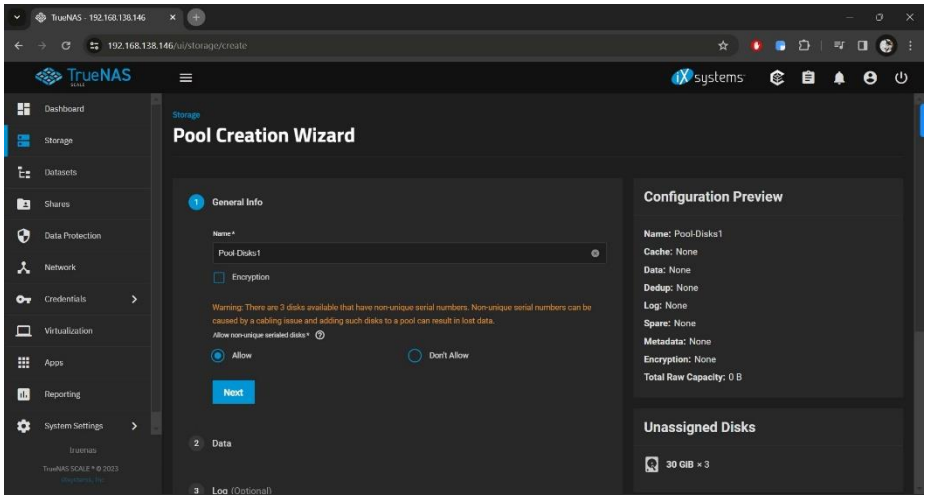

Figure 15. TrueNAS Scale - Adding Pool.

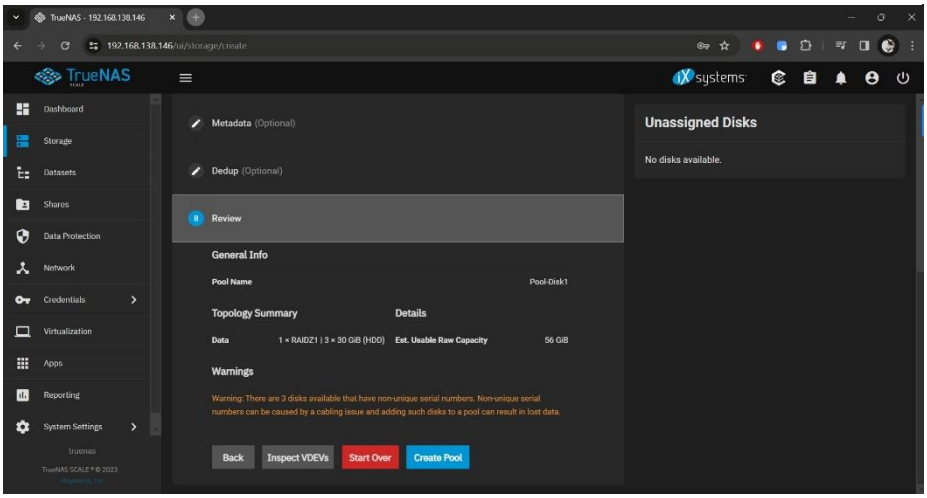

Figure 14. TrueNAS Scale - Adding Pool.

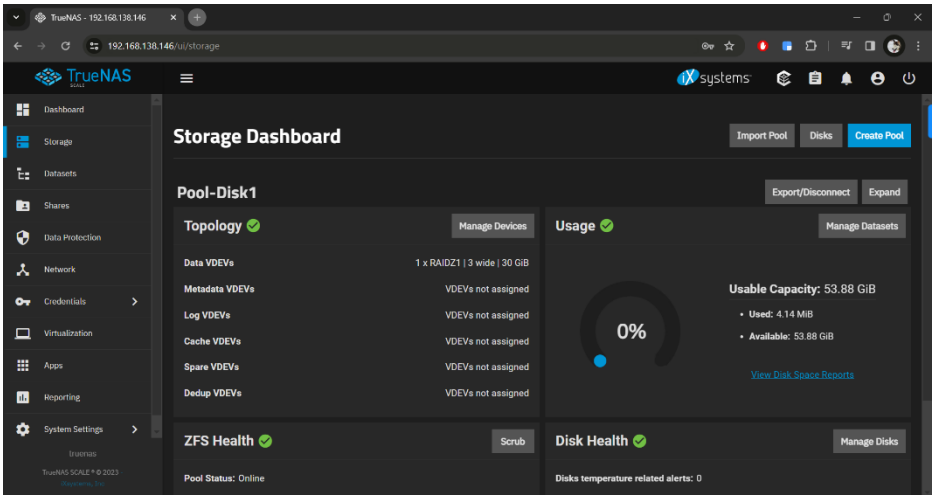

Figure 13. TrueNAS Scale - Adding Pool.

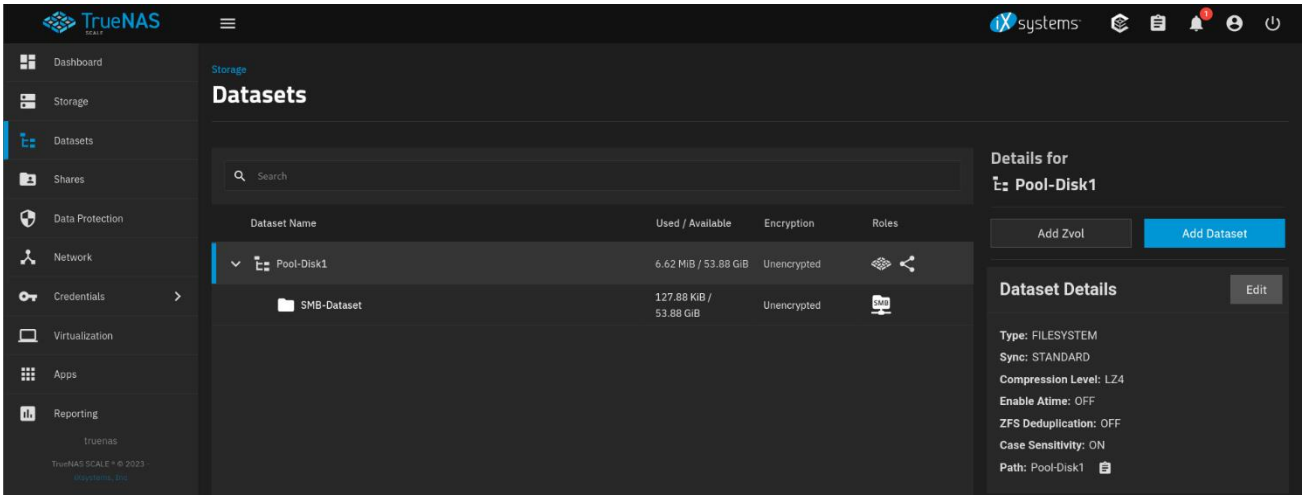

Figure 16. TrueNAS Scale - SMB Share.

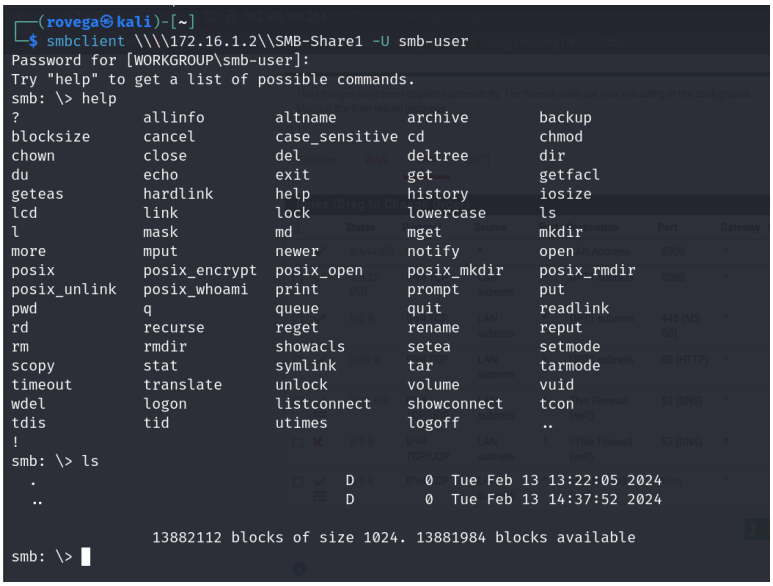

Figure 17. Kali Linux - Testing SMB Share - LAN to DMZ.

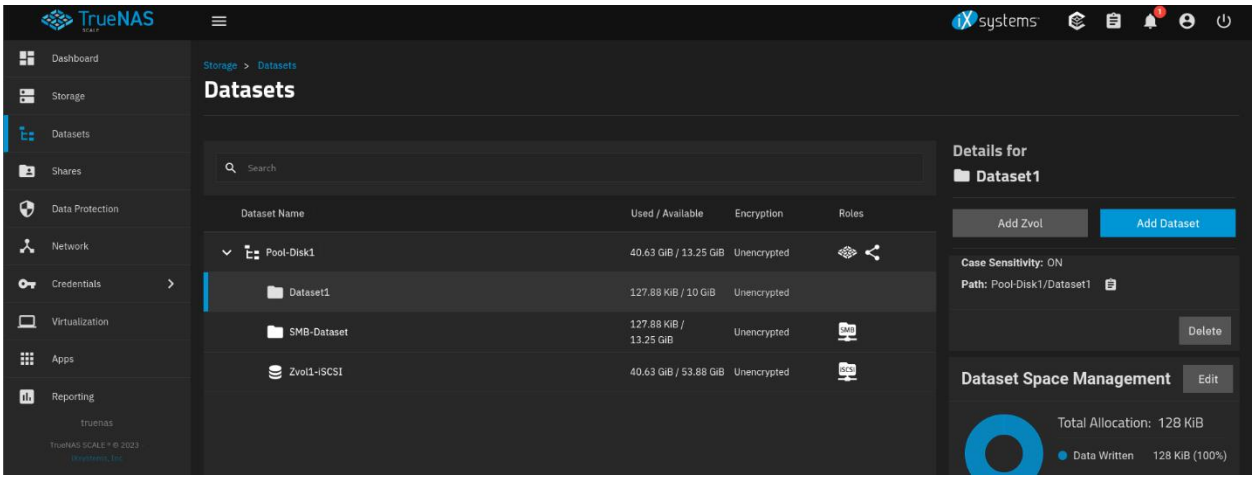

Figure 18. TrueNAS Scale - iSCI & Dataset.

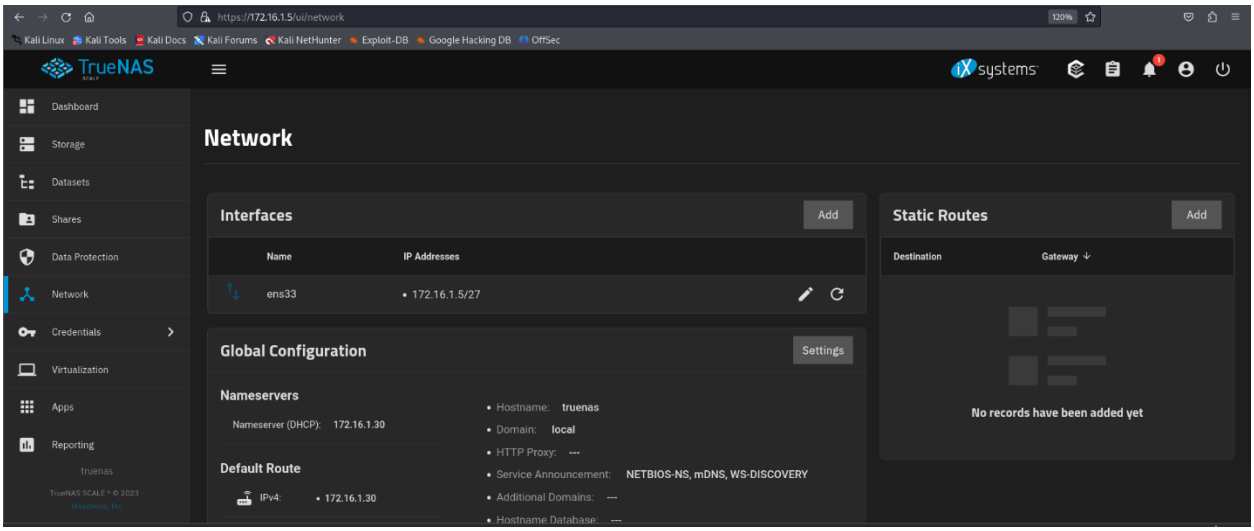

Figure 19. TrueNAS Scale - Static IP Adress.

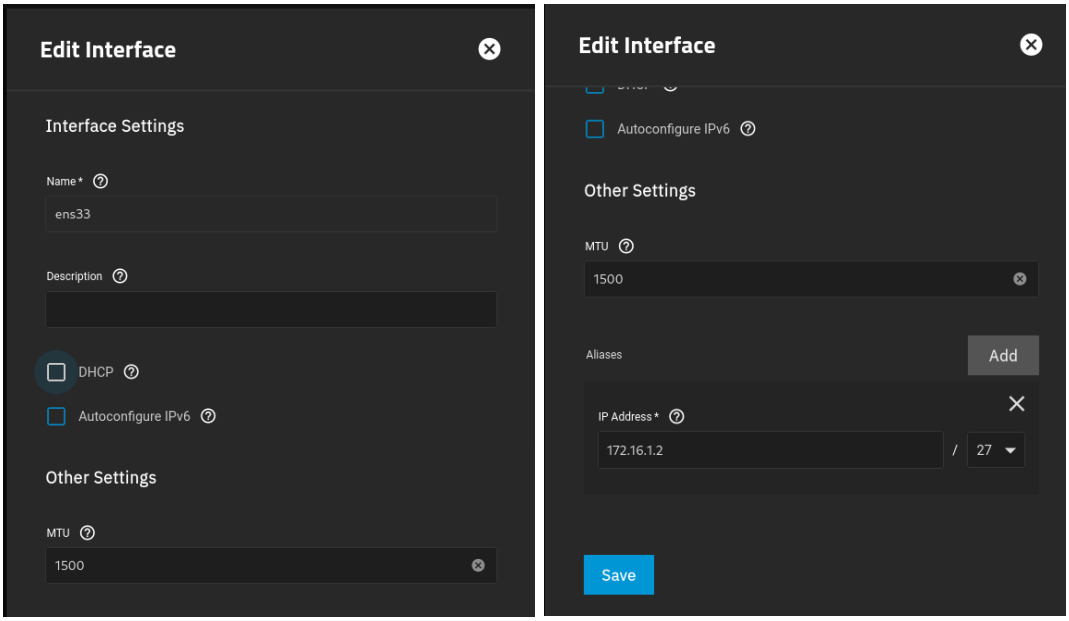

Figure 20. TrueNAS Scale - Static IP Adress.

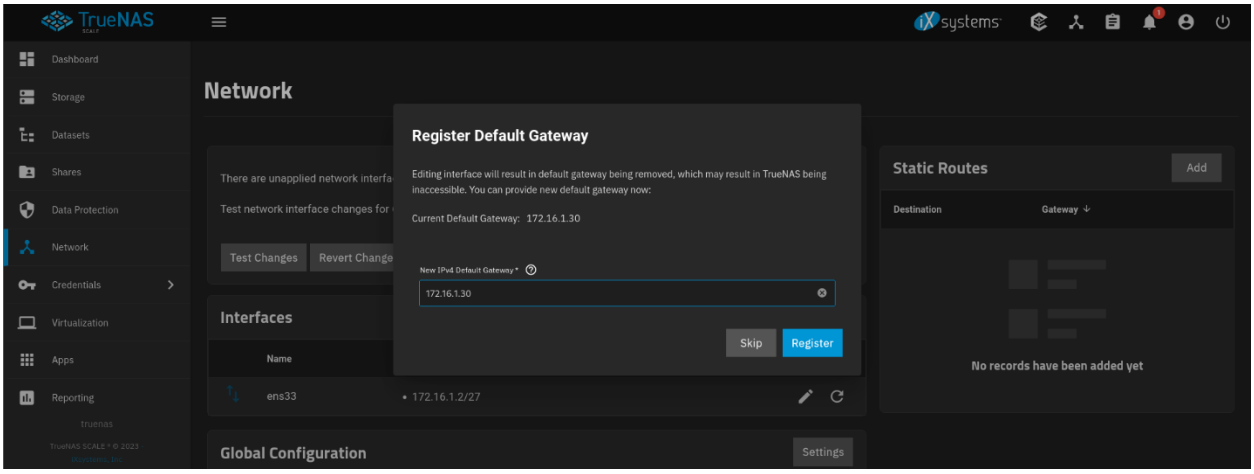

Figure 21. TrueNAS Scale - Static IP Adress.

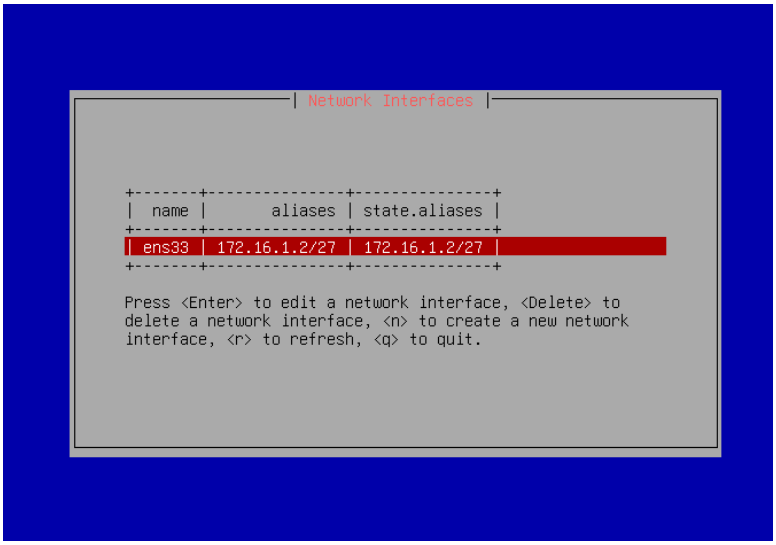

Figure 24. TrueNAS Scale - Static IP Adress.

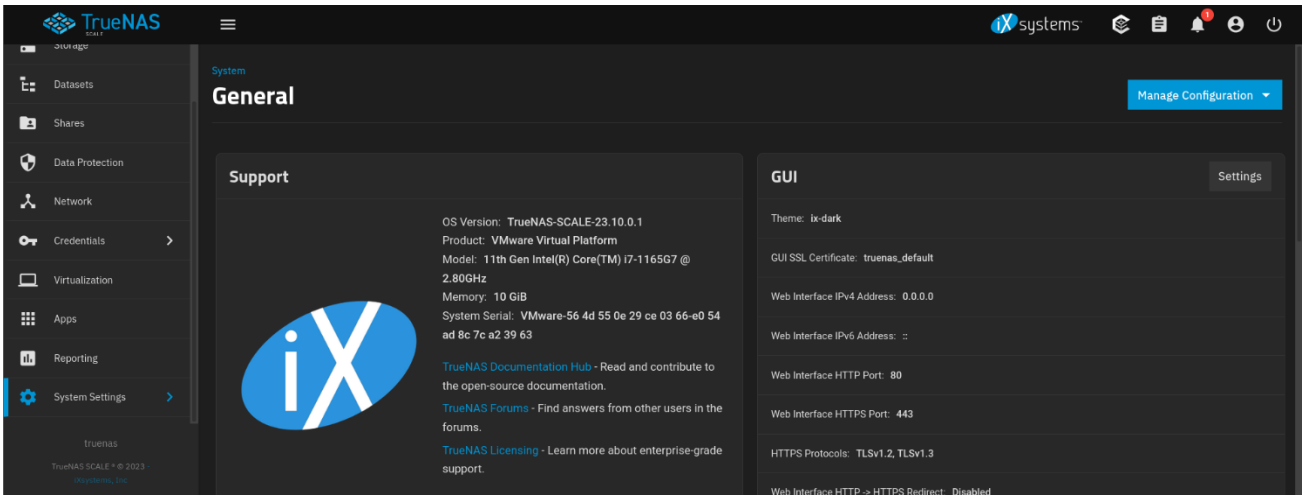

Figure 23. TrueNAS Scale - Changing Web GUI Port.

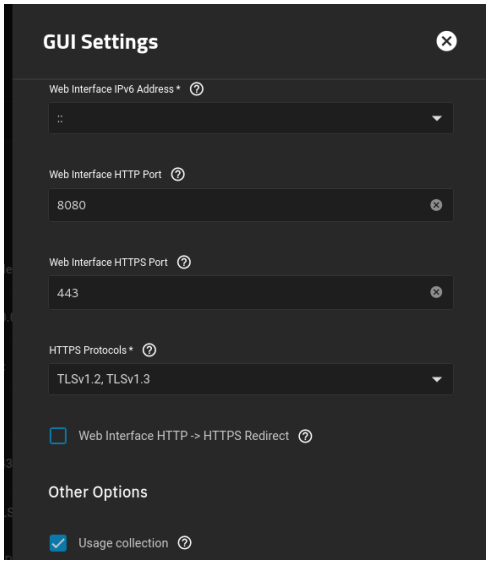

Figure 22. TrueNAS Scale - Changing Web GUI Port.

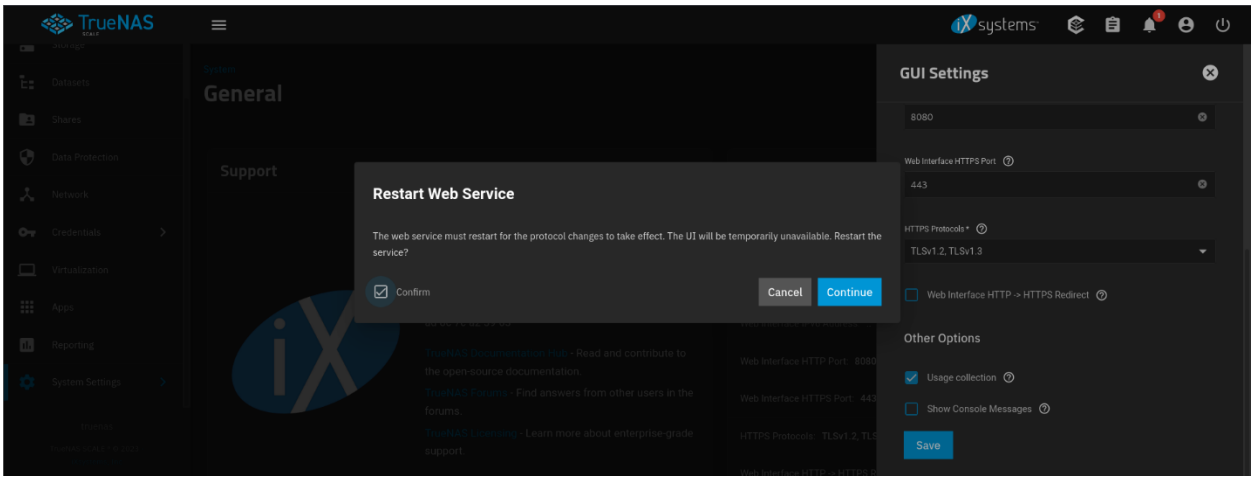

Figure 27. TrueNAS Scale - Changing Web GUI Port.

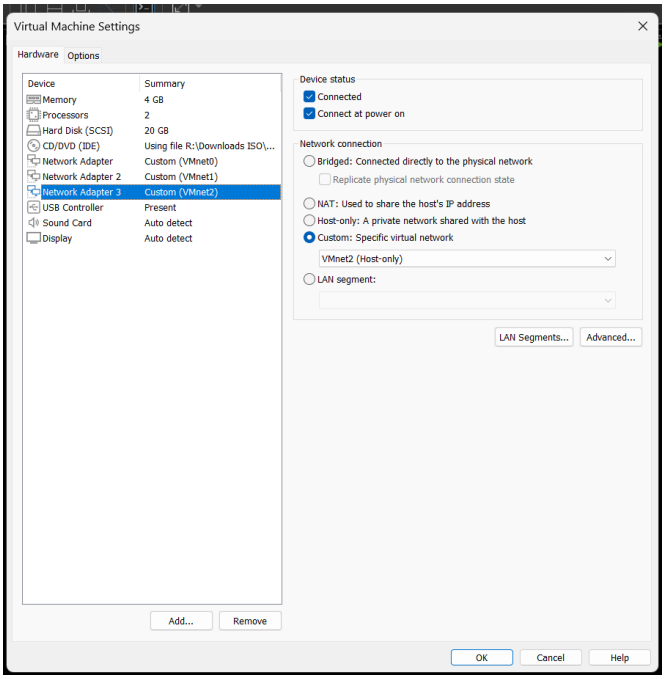

Figure 26. pfSense - VM Settings.

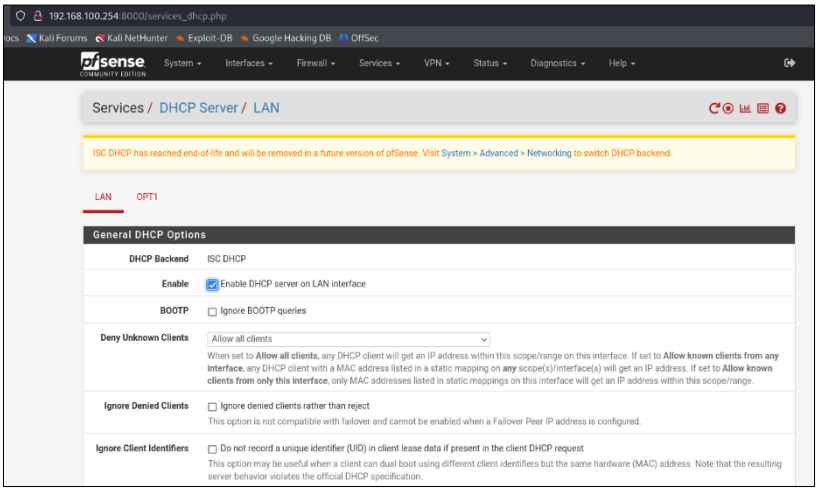

Figure 25. pfSense - DHCP Server LAN.

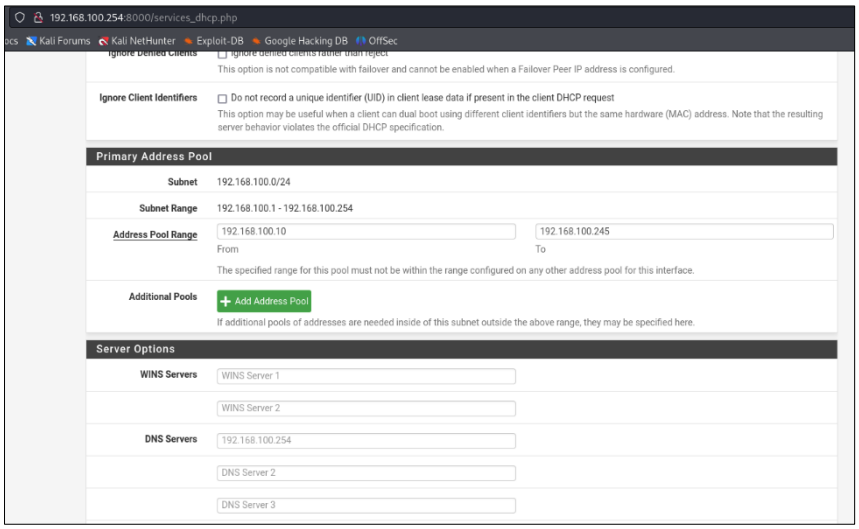

Figure 30. pfSense - DHCP Server LAN.

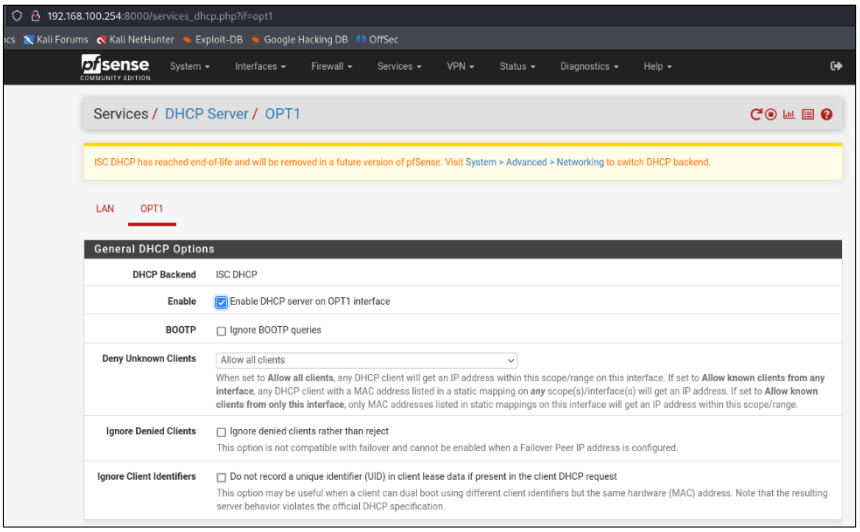

Figure 29. pfSense - DHCP Server DMZ.

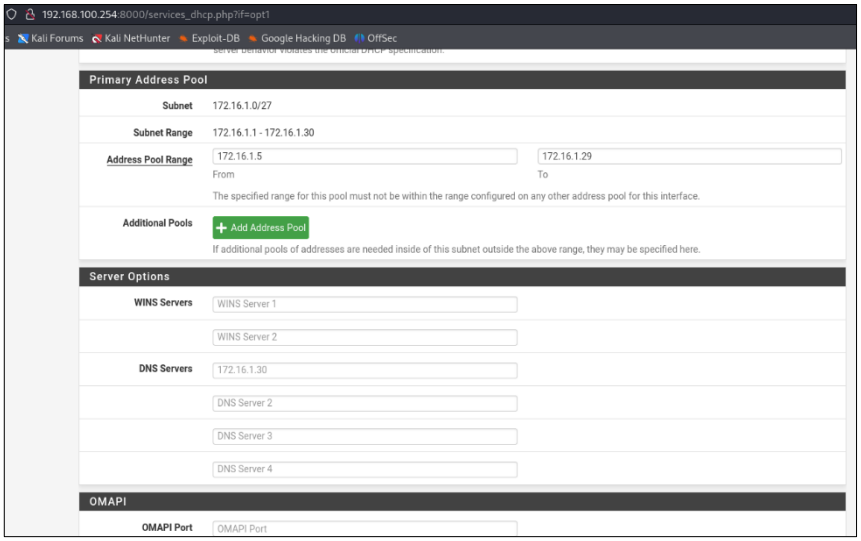

Figure 28. pfSense - DHCP Server DMZ.

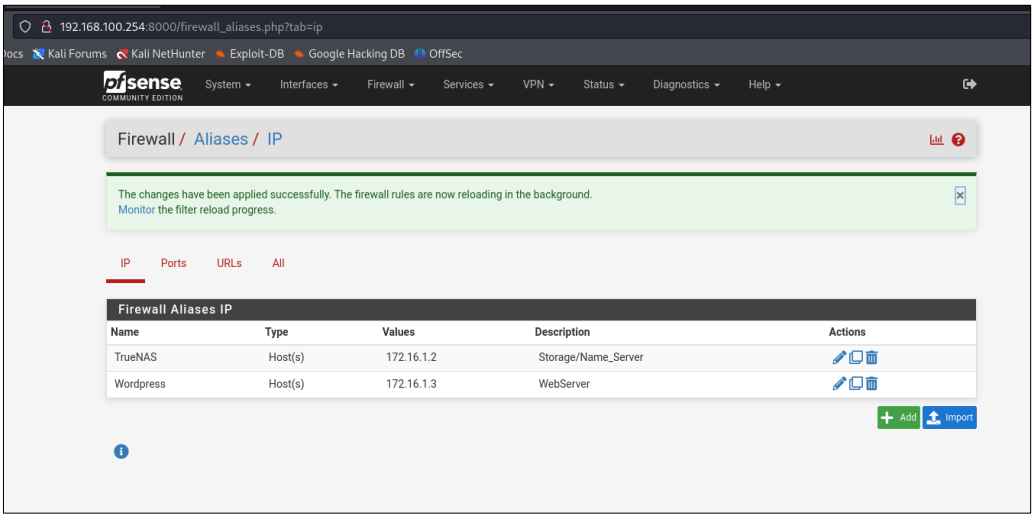

Figure 31. pfSense - Aliases IP.

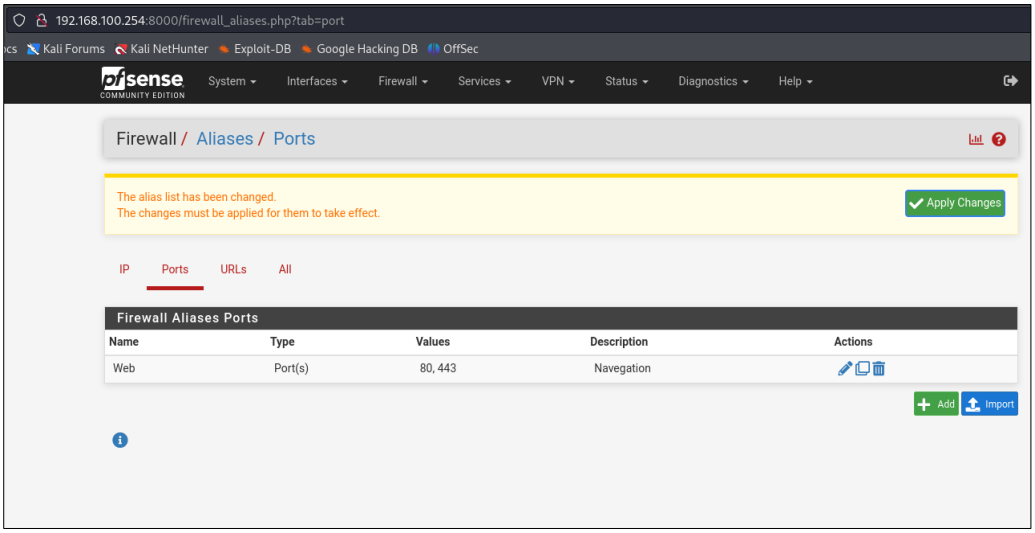

Figure 32. pfSense - Aliases Ports.

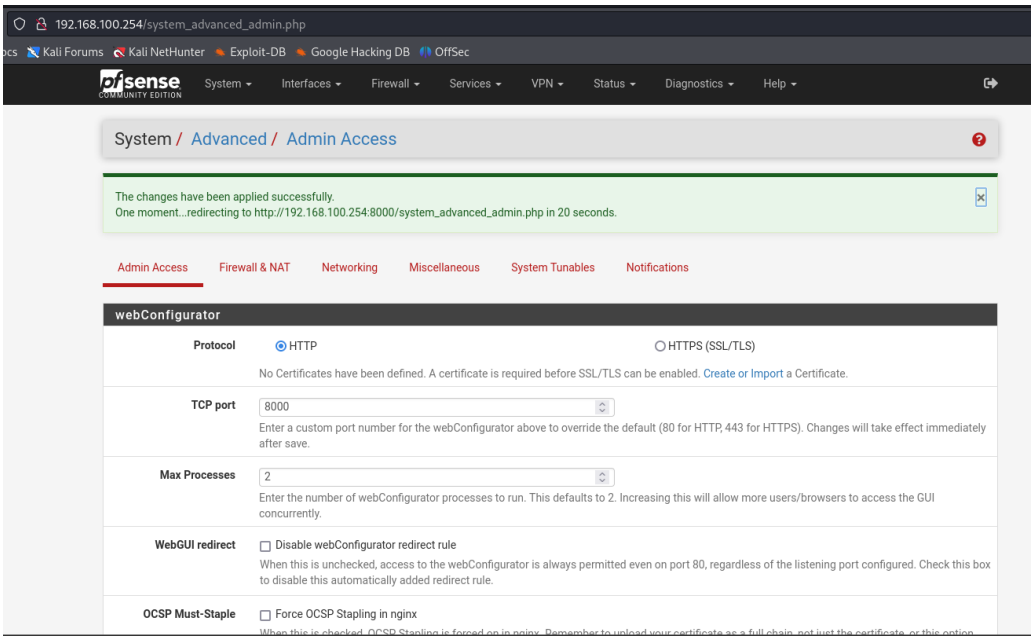

Figure 33. pfSense - Changing Admin Access Port.

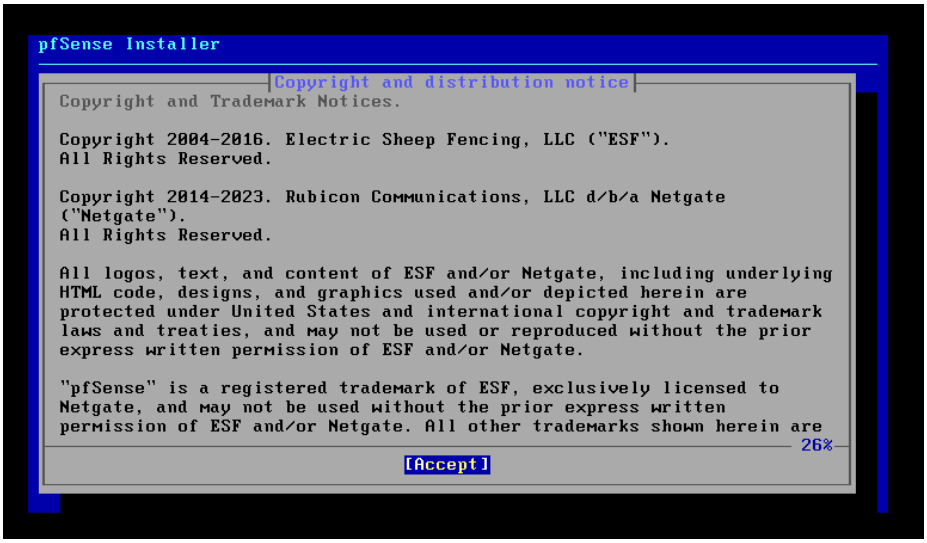

Figure 34. pfSense - Installation.

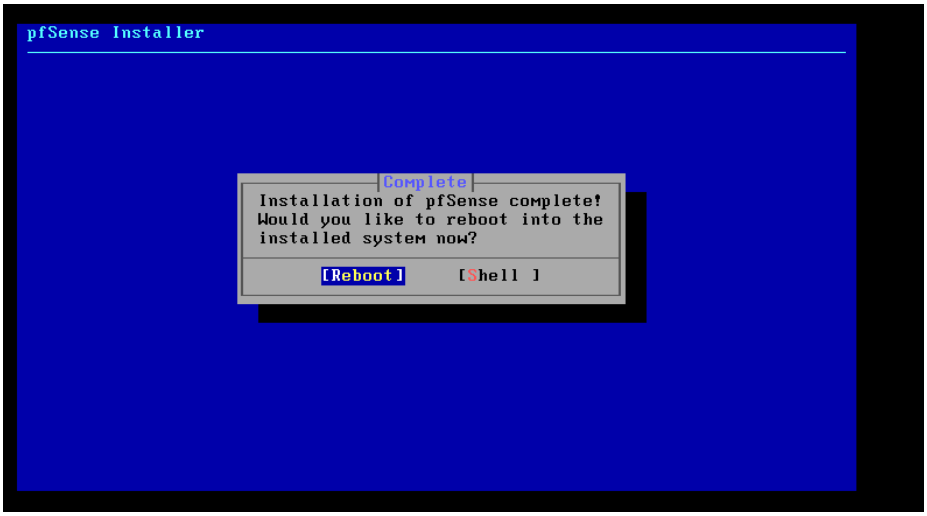

Figure 35. pfSense - Installation.

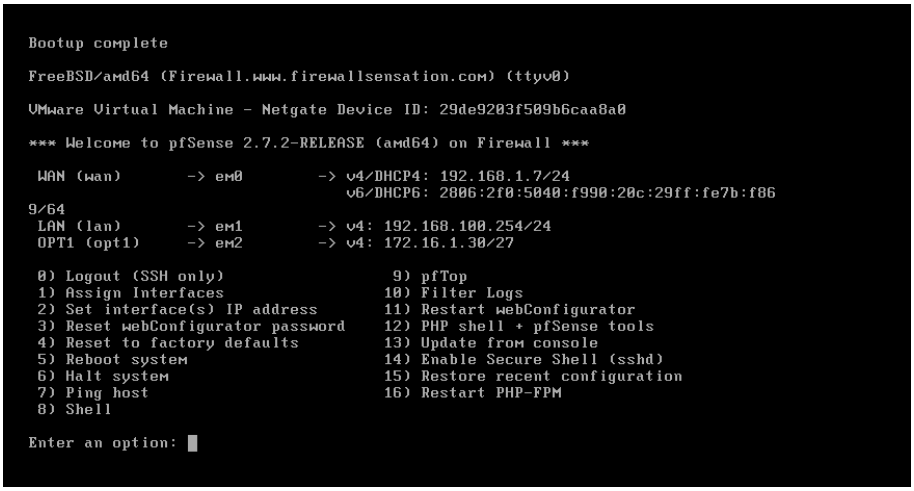

Figure 36. pfSense - Console.

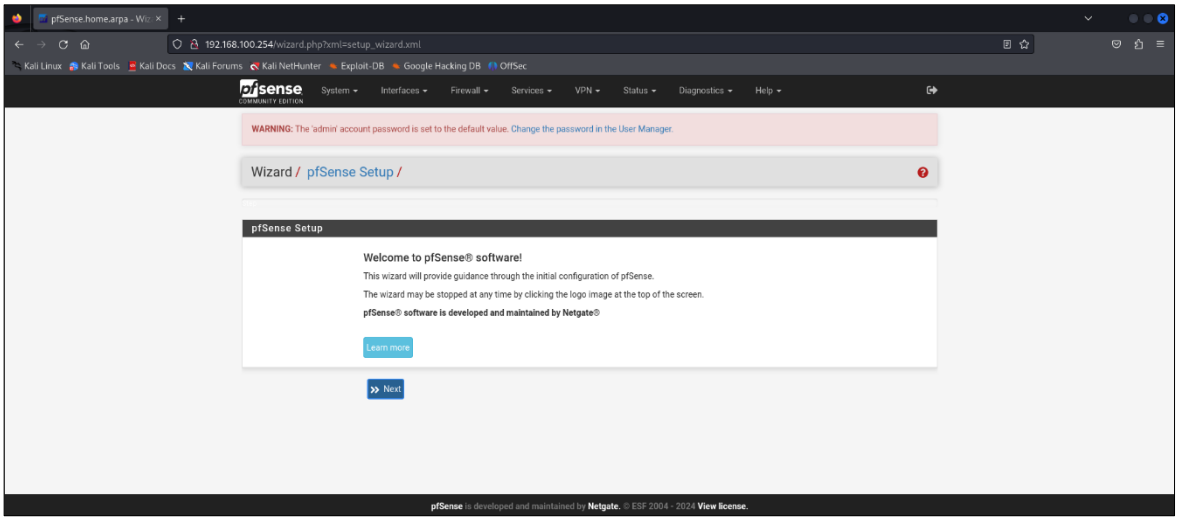

Figure 37. pfSense - Setup.

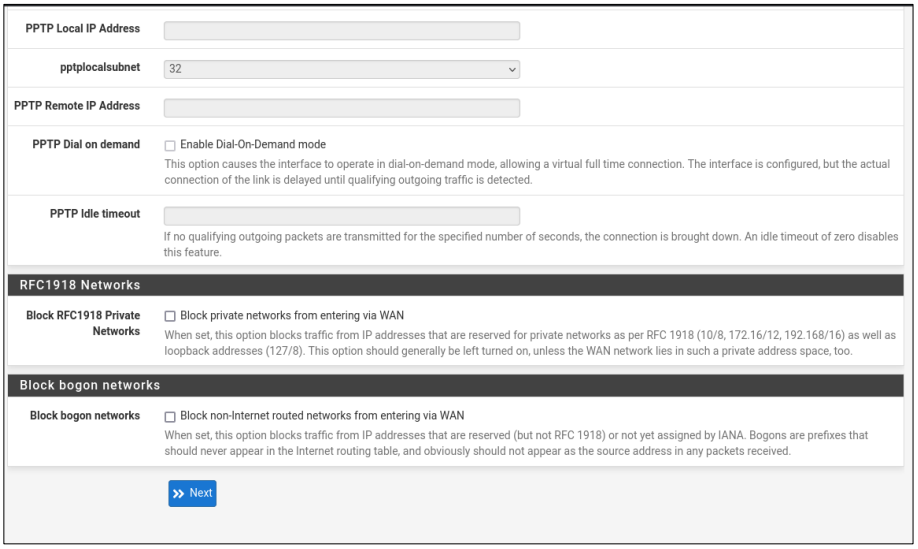

Figure 38. pfSense - Setup Important Options.

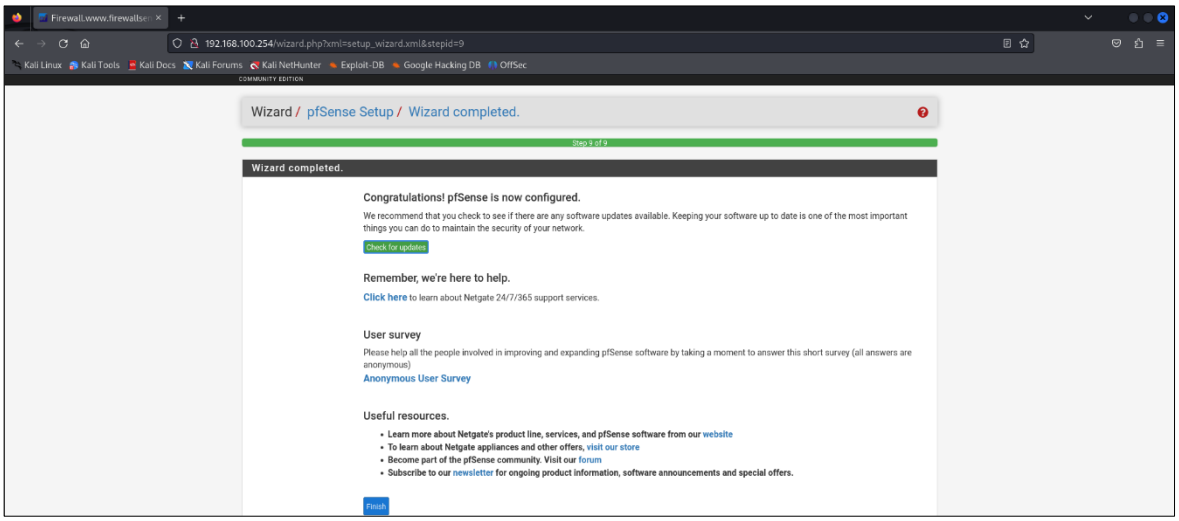

Figure 39. pfSense - Setup.

Phase 2

In this phase, screenshots of the VMware Workstation virtual network editor interfaces are presented.

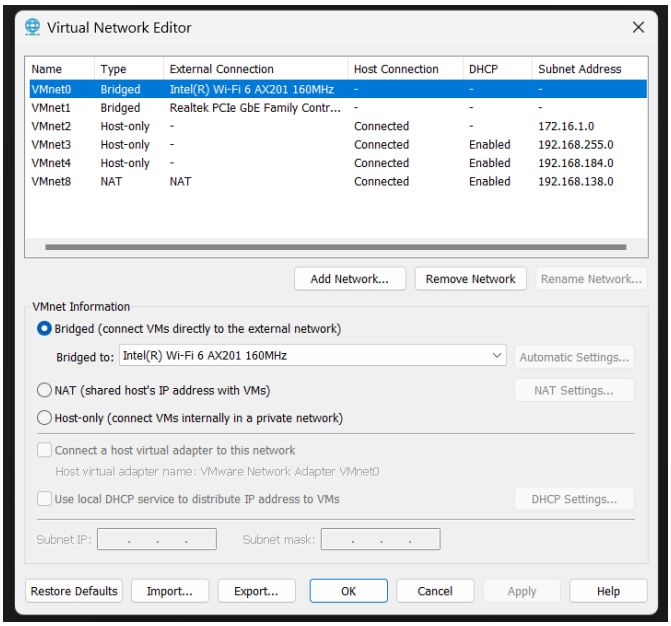

Figure 40.Virtual Network Editor - WAN.

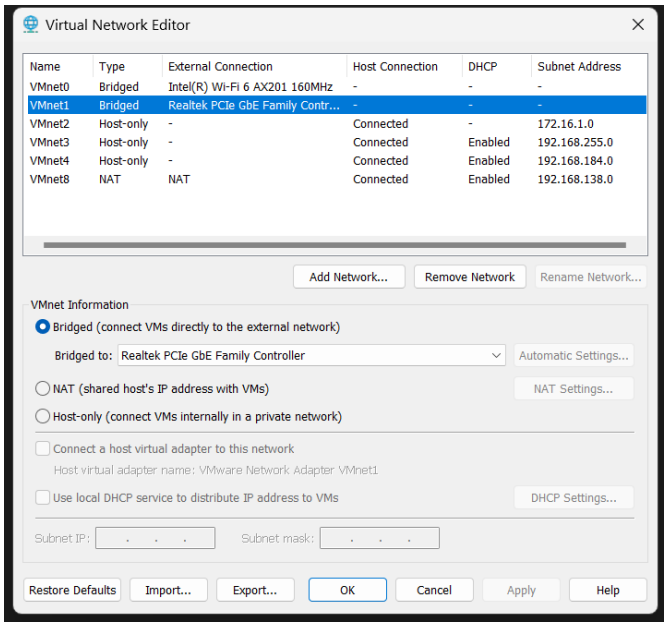

Figure 41.Virtual Network Editor - LAN.

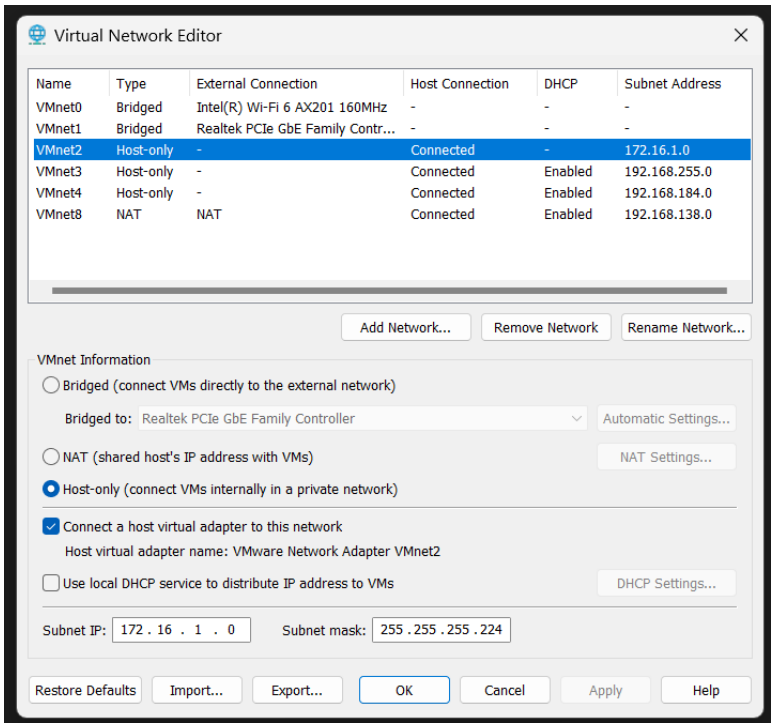

Figure 42.Virtual Network Editor - DMZ.

Phase 3

In this phase, screenshots of the assignment of interfaces, firewall rules, and port forwarding are showcased.

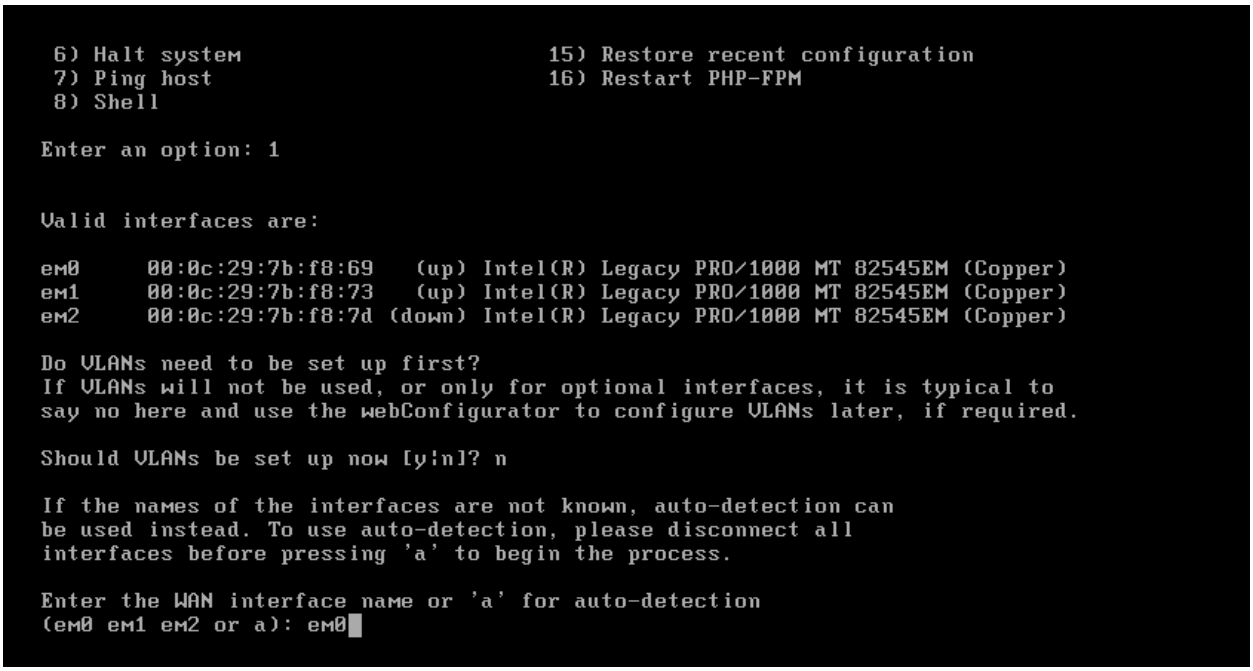

Figure 43.pfSense - Assignment of interfaces.

```
say no here and use the webConfigurator to configure VLANs later, if required.

Should VLANs be set up now [y|n]? n

If the names of the interfaces are not known, auto-detection can
be used instead. To use auto-detection, please disconnect all
interfaces before pressing 'a' to begin the process.

Enter the WAN interface name or 'a' for auto-detection
(em0 em1 em2 or a): em0

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(em1 em2 a or nothing if finished): em1

Enter the Optional 1 interface name or 'a' for auto-detection
(em2 a or nothing if finished): em2

The interfaces will be assigned as follows:

WAN  -> em0
LAN  -> em1
OPT1 -> em2

Do you want to proceed [y|n]? y
```

Figure 45.pfSense - Assignment of interfaces.

```
 7) Ping host                          16) Restart PHP-FPM
 8) Shell

Enter an option: 2

Available interfaces:

1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static)
3 - OPT1 (em2)

Enter the number of the interface you wish to configure: 2

Configure IPv4 address LAN interface via DHCP? (y/n) n

Enter the new LAN IPv4 address.  Press <ENTER> for none:
> 192.168.100.254

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new LAN IPv4 subnet bit count (1 to 32):
> 24
```

Figure 44.pfSense - IP address allocation – LAN.

```
> 192.168.100.254

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new LAN IPv4 subnet bit count (1 to 32):
> 24

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Configure IPv6 address LAN interface via DHCP6? (y/n) y

Do you want to enable the DHCP server on LAN? (y/n) y
Enter the start address of the IPv4 client address range: 192.168.100.10
Enter the end address of the IPv4 client address range: 192.168.100.250
Disabling IPv6 DHCPD...

Do you want to revert to HTTP as the webConfigurator protocol? (y/n) y

Please wait while the changes are saved to LAN...
 Reloading filter...
```

Figure 46.pfSense - IP address allocation – LAN.

```
For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Configure IPv6 address LAN interface via DHCP6? (y/n) y

Do you want to enable the DHCP server on LAN? (y/n) y
Enter the start address of the IPv4 client address range: 192.168.100.10
Enter the end address of the IPv4 client address range: 192.168.100.250
Disabling IPv6 DHCPD...

Do you want to revert to HTTP as the webConfigurator protocol? (y/n) y

Please wait while the changes are saved to LAN...
 Reloading filter...
 Reloading routing configuration...
 DHCPD...
 Restarting webConfigurator...

The IPv4 LAN address has been set to 192.168.100.254/24


The IPv6 LAN address has been set to dhcp6

Press <ENTER> to continue.
```

Figure 47.pfSense - IP address allocation – LAN.

```
 7) Ping host                          16) Restart PHP-FPM
 8) Shell

Enter an option: 2

Available interfaces:

1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static, dhcp6)
3 - OPT1 (em2)

Enter the number of the interface you wish to configure: 3

Configure IPv4 address OPT1 interface via DHCP? (y/n) n

Enter the new OPT1 IPv4 address.  Press <ENTER> for none:
> 172.16.1.30

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new OPT1 IPv4 subnet bit count (1 to 32):
> 27
```

Figure 48.pfSense - IP address allocation – DMZ.

```
Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new OPT1 IPv4 subnet bit count (1 to 32):
> 27

For a WAN, enter the new OPT1 IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Configure IPv6 address OPT1 interface via DHCP6? (y/n) n

Enter the new OPT1 IPv6 address.  Press <ENTER> for none:
>

Do you want to enable the DHCP server on OPT1? (y/n) n
Disabling IPv4 DHCPD...
Disabling IPv6 DHCPD...

Please wait while the changes are saved to OPT1...
 Reloading filter...
 Reloading routing configuration...
 DHCPD...
```

Figure 49.pfSense - IP address allocation – DMZ.

```
For a WAN, enter the new OPT1 IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Configure IPv6 address OPT1 interface via DHCP6? (y/n) n

Enter the new OPT1 IPv6 address.  Press <ENTER> for none:
>

Do you want to enable the DHCP server on OPT1? (y/n) n
Disabling IPv4 DHCPD...
Disabling IPv6 DHCPD...

Please wait while the changes are saved to OPT1...
 Reloading filter...
 Reloading routing configuration...
 DHCPD...

The IPv4 OPT1 address has been set to 172.16.1.30/27
You can now access the webConfigurator by opening the following URL in your web
browser:
                http://172.16.1.30/

Press <ENTER> to continue.
```

Figure 50.pfSense - IP address allocation – DMZ.

```
               http://172.16.1.30/

Press <ENTER> to continue.
VMware Virtual Machine - Netgate Device ID: 29de9203f509b6caa8a0

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

 WAN (wan)       -> em0        -> v4/DHCP4: 192.168.1.12/24
                                  v6/DHCP6: 2806:2f0:5040:f990:20c:29ff:fe7b:f86
9/64
 LAN (lan)       -> em1        -> v4: 192.168.100.254/24
                                  v6/DHCP6: 2806:2f0:5040:f990::2/128
 OPT1 (opt1)     -> em2        -> v4: 172.16.1.30/27

 0) Logout (SSH only)                  9) pfTop
 1) Assign Interfaces                 10) Filter Logs
 2) Set interface(s) IP address       11) Restart webConfigurator
 3) Reset webConfigurator password    12) PHP shell + pfSense tools
 4) Reset to factory defaults         13) Update from console
 5) Reboot system                     14) Enable Secure Shell (sshd)
 6) Halt system                       15) Restore recent configuration
 7) Ping host                         16) Restart PHP-FPM
 8) Shell

Enter an option: 7
```

Figure 51.pfSense - Testing with ping.

```
 1) Assign Interfaces                 10) Filter Logs
 2) Set interface(s) IP address       11) Restart webConfigurator
 3) Reset webConfigurator password    12) PHP shell + pfSense tools
 4) Reset to factory defaults         13) Update from console
 5) Reboot system                     14) Enable Secure Shell (sshd)
 6) Halt system                       15) Restore recent configuration
 7) Ping host                         16) Restart PHP-FPM
 8) Shell

Enter an option: 7


Enter a host name or IP address: 192.168.100.254

PING 192.168.100.254 (192.168.100.254): 56 data bytes
64 bytes from 192.168.100.254: icmp_seq=0 ttl=64 time=0.286 ms
64 bytes from 192.168.100.254: icmp_seq=1 ttl=64 time=0.105 ms
64 bytes from 192.168.100.254: icmp_seq=2 ttl=64 time=0.335 ms

--- 192.168.100.254 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.105/0.242/0.335/0.099 ms

Press ENTER to continue.
```

Figure 52.pfSense - Testing with ping.

```
 1) Assign Interfaces               10) Filter Logs
 2) Set interface(s) IP address     11) Restart webConfigurator
 3) Reset webConfigurator password  12) PHP shell + pfSense tools
 4) Reset to factory defaults       13) Update from console
 5) Reboot system                   14) Enable Secure Shell (sshd)
 6) Halt system                     15) Restore recent configuration
 7) Ping host                       16) Restart PHP-FPM
 8) Shell

Enter an option: 7


Enter a host name or IP address: 172.16.1.30

PING 172.16.1.30 (172.16.1.30): 56 data bytes
64 bytes from 172.16.1.30: icmp_seq=0 ttl=64 time=0.669 ms
64 bytes from 172.16.1.30: icmp_seq=1 ttl=64 time=0.295 ms
64 bytes from 172.16.1.30: icmp_seq=2 ttl=64 time=0.338 ms

--- 172.16.1.30 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.295/0.434/0.669/0.167 ms

Press ENTER to continue.
```

Figure 53.pfSense - Testing with ping.

```
 1) Assign Interfaces               10) Filter Logs
 2) Set interface(s) IP address     11) Restart webConfigurator
 3) Reset webConfigurator password  12) PHP shell + pfSense tools
 4) Reset to factory defaults       13) Update from console
 5) Reboot system                   14) Enable Secure Shell (sshd)
 6) Halt system                     15) Restore recent configuration
 7) Ping host                       16) Restart PHP-FPM
 8) Shell

Enter an option: 7


Enter a host name or IP address: 192.168.1.12

PING 192.168.1.12 (192.168.1.12): 56 data bytes
64 bytes from 192.168.1.12: icmp_seq=0 ttl=64 time=0.246 ms
64 bytes from 192.168.1.12: icmp_seq=1 ttl=64 time=0.261 ms
64 bytes from 192.168.1.12: icmp_seq=2 ttl=64 time=0.075 ms

--- 192.168.1.12 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.075/0.194/0.261/0.084 ms

Press ENTER to continue.
```

Figure 54.pfSense - Testing with ping.

```
 1) Assign Interfaces               10) Filter Logs
 2) Set interface(s) IP address     11) Restart webConfigurator
 3) Reset webConfigurator password  12) PHP shell + pfSense tools
 4) Reset to factory defaults       13) Update from console
 5) Reboot system                   14) Enable Secure Shell (sshd)
 6) Halt system                     15) Restore recent configuration
 7) Ping host                       16) Restart PHP-FPM
 8) Shell

Enter an option: 7


Enter a host name or IP address: 8.8.8.8

PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: icmp_seq=0 ttl=57 time=70.208 ms
64 bytes from 8.8.8.8: icmp_seq=1 ttl=57 time=44.504 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=57 time=19.373 ms

--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 19.373/44.695/70.208/20.754 ms

Press ENTER to continue.
```

Figure 55.pfSense - Testing with ping.

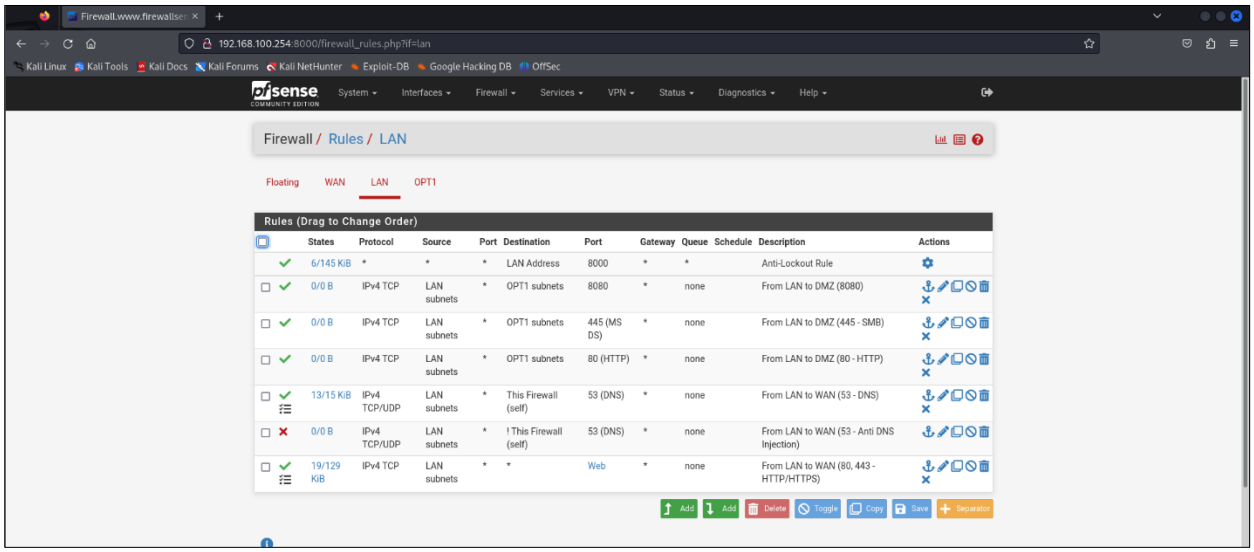

Figure 56. pfSense Web GUI - LAN Rules.

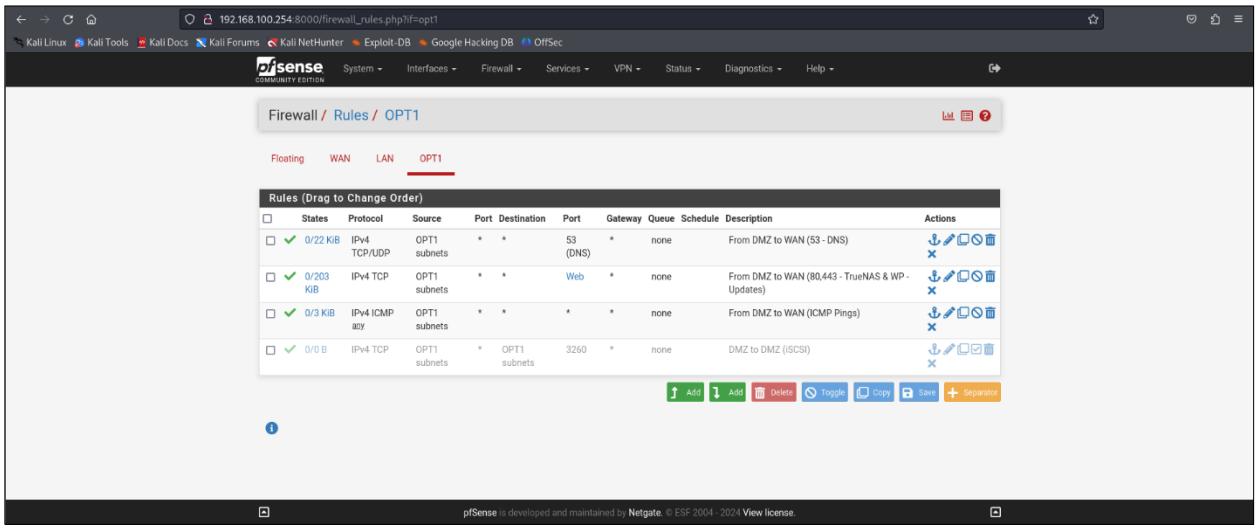

Figure 57. pfSense Web GUI - DMZ Rules.

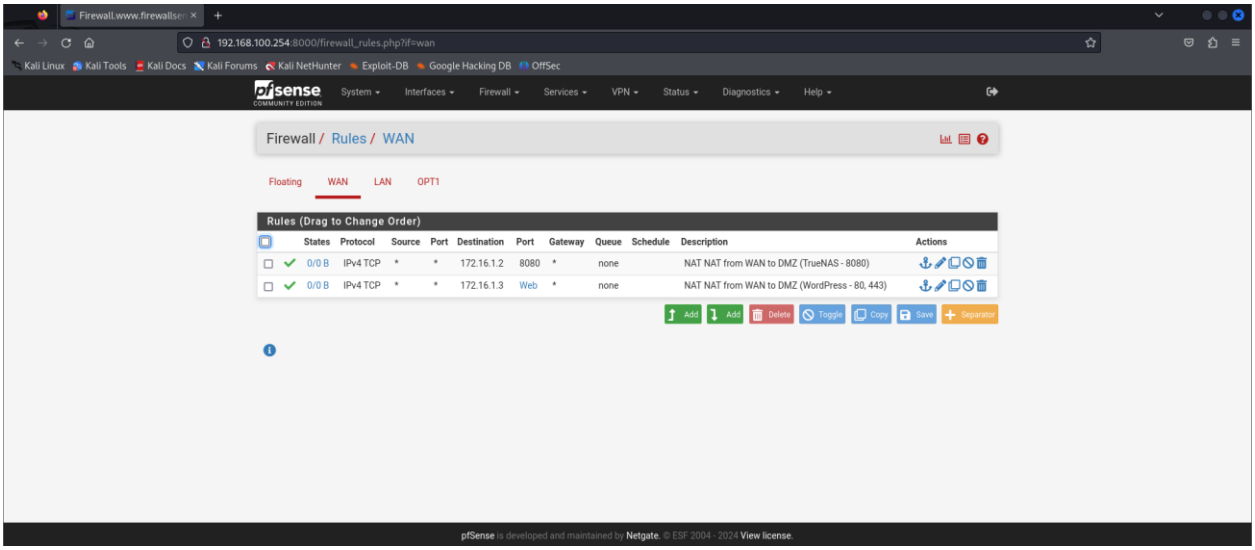

Figure 58. pfSense Web GUI - WAN Rules.

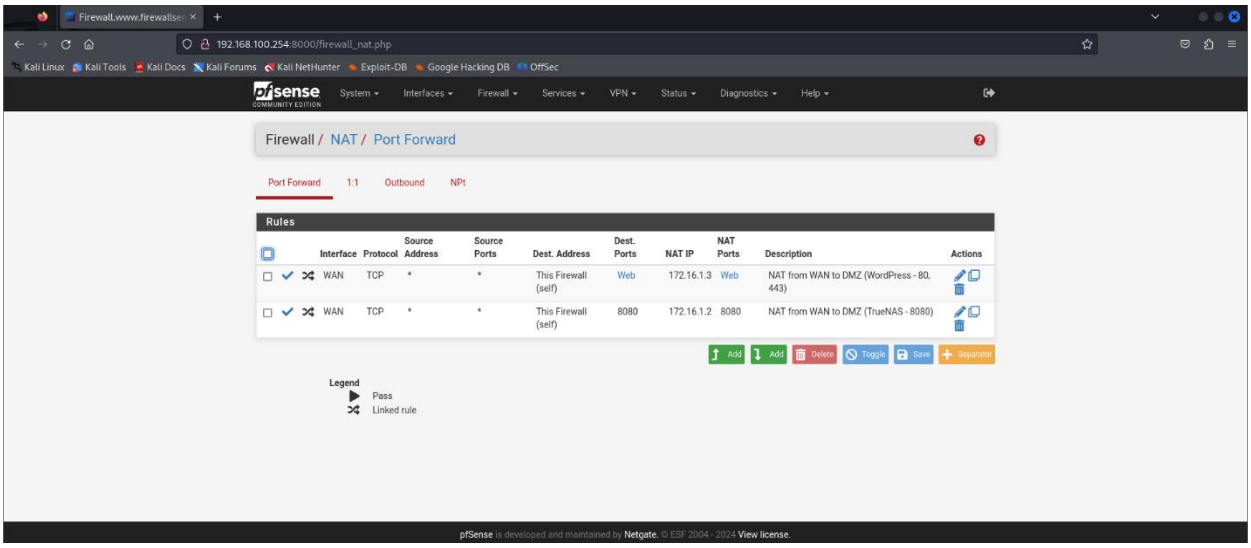

Figure 59. pfSense Web GUI - NAT Port Forward Rules.

Phase 4

In this phase, screenshots demonstrating the functionality between the services in the network segments are provided.

WAN to DMZ:

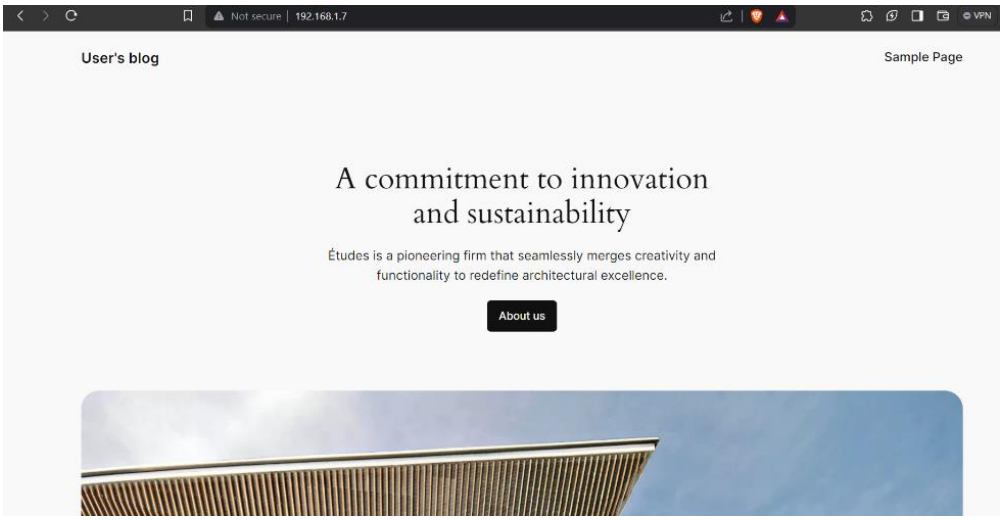

Figure 60. Local host (Windows 11) - WAN to DMZ - WordPress Port 80.

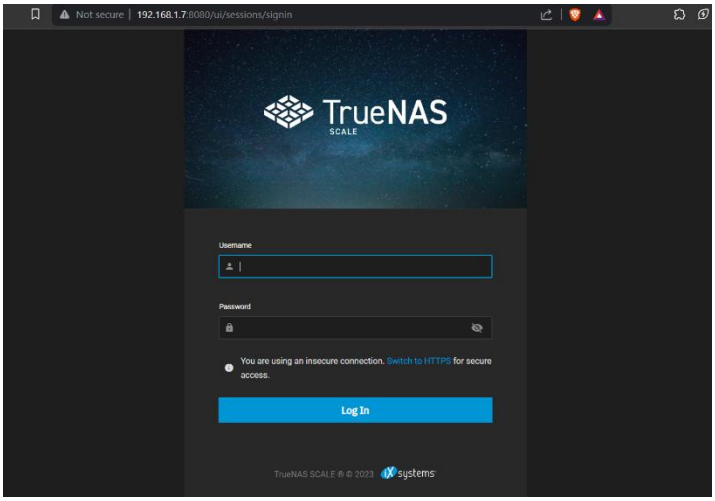

Figure 61. Local host (Windows 11) - WAN to DMZ – TrueNAS Port 8080.

LAN to WAN:

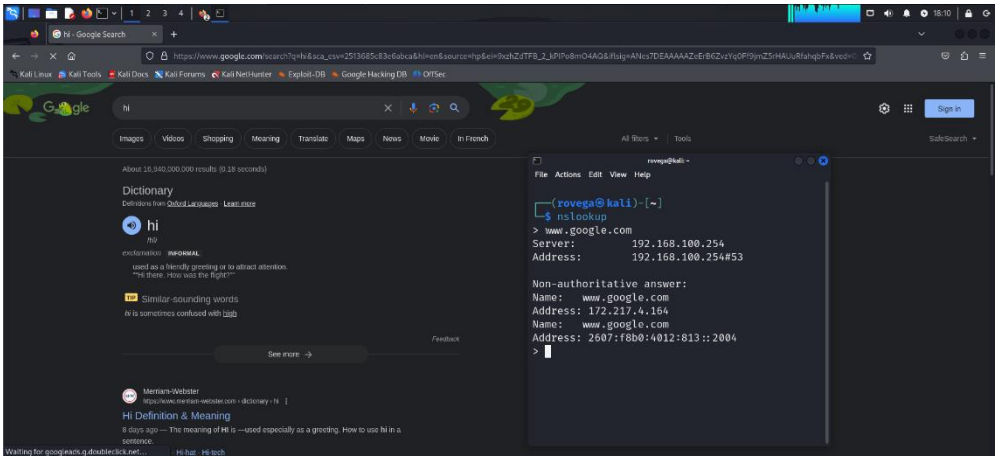

Figure 62. Kali Linux (Web Client) - LAN to WAN – Navigating Internet.

LAN to DMZ:

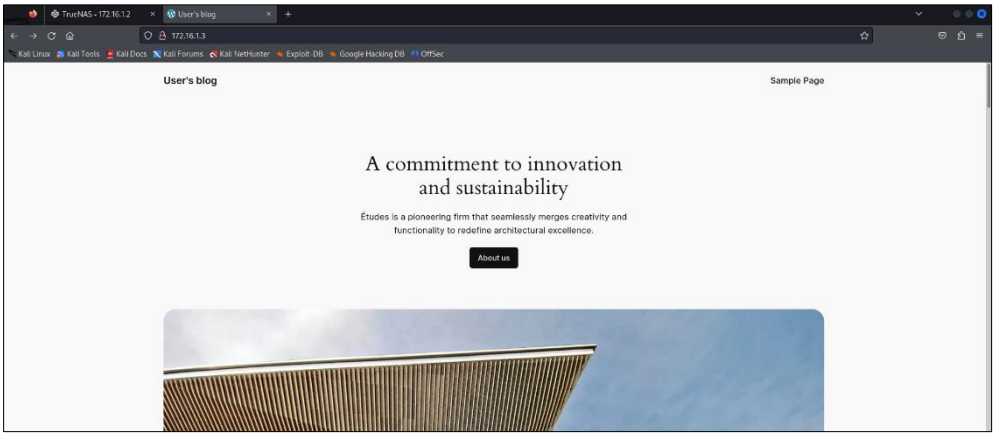

Figure 63. Kali Linux (Web Client) - LAN to DMZ – WordPress Port 80.

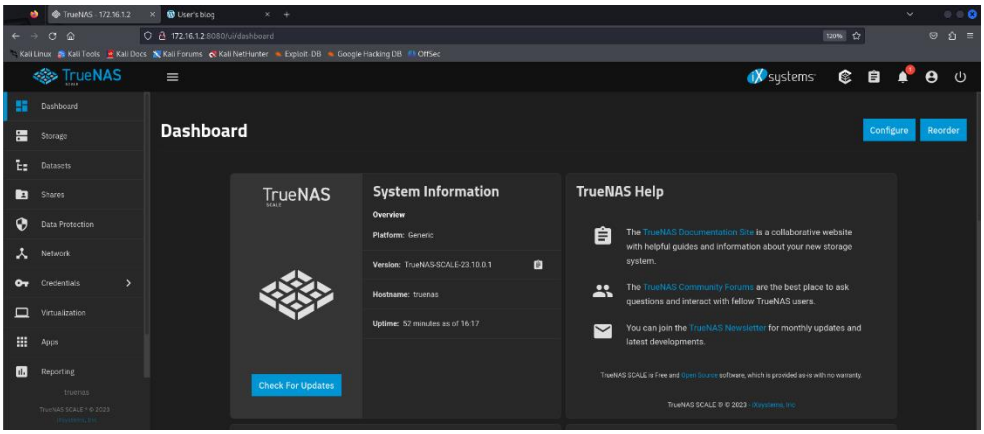

Figure 64. Kali Linux (Web Client) - LAN to DMZ – TrueNAS Port 8080.

DMZ to WAN:

```
*** You can find out more at https://docs.bitnami.com/virtual-machine/apps/wordpress/ ***
*** If you find any issues, please visit https://github.com/bitnami/vms/issues ***

********************************************************************************
   To access the console, login with user 'bitnami' and password 'bitnami'
********************************************************************************

debian login: bitnami
Password:
Linux debian 5.10.0-27-amd64 #1 SMP Debian 5.10.205-2 (2023-12-31) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
      ___ _ _                                  _
     | _ |_) |_ _ _  __ _ _ __  ___ _____ (_)
     | _ \ |  _| ' \/ _` | '  \/ -_)  _  | |
     |___/_|\__|_|_|\__,_|_|_|_\___|_| |_|_|

  -> Welcome to Bitnami package for WordPress 6.4.2
  -> Documentation:   https://docs.bitnami.com/virtual-machine/apps/wordpress/
  -> Bitnami Support: https://github.com/bitnami/vms/issues
Last login: Tue Mar 12 19:05:56 UTC 2024 on tty1
bitnami@debian:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=56 time=36.5 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=56 time=20.7 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=56 time=18.4 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=56 time=47.1 ms
^C
--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 18.436/30.684/47.144/11.781 ms
bitnami@debian:~$
```

Figure 65. WordPress Bitnami - DMZ to WAN – Ping.

```
2) Configure network settings
3) Configure static routes
4) Change local administrator password
5) Reset configuration to defaults
6) Open TrueNAS CLI Shell
7) Open Linux Shell
8) Reboot
9) Shutdown

Enter an option from 1-9: 7


Warning: the supported mechanisms for making configuration changes
are the TrueNAS WebUI, CLI, and API exclusively. ALL OTHERS ARE
NOT SUPPORTED AND WILL RESULT IN UNDEFINED BEHAVIOR AND MAY
RESULT IN SYSTEM FAILURE.

root@truenas[~]# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=56 time=18.1 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=56 time=18.4 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=56 time=23.7 ms
^C
--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 18.058/20.078/23.739/2.593 ms
root@truenas[~]# nslookup
> www.google.com
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
Name:   www.google.com
Address: 142.251.34.4
Name:   www.google.com
Address: 2607:f8b0:4012:813::2004
> _
```

Figure 66. TrueNAS - DMZ to WAN – Ping & nslookup.

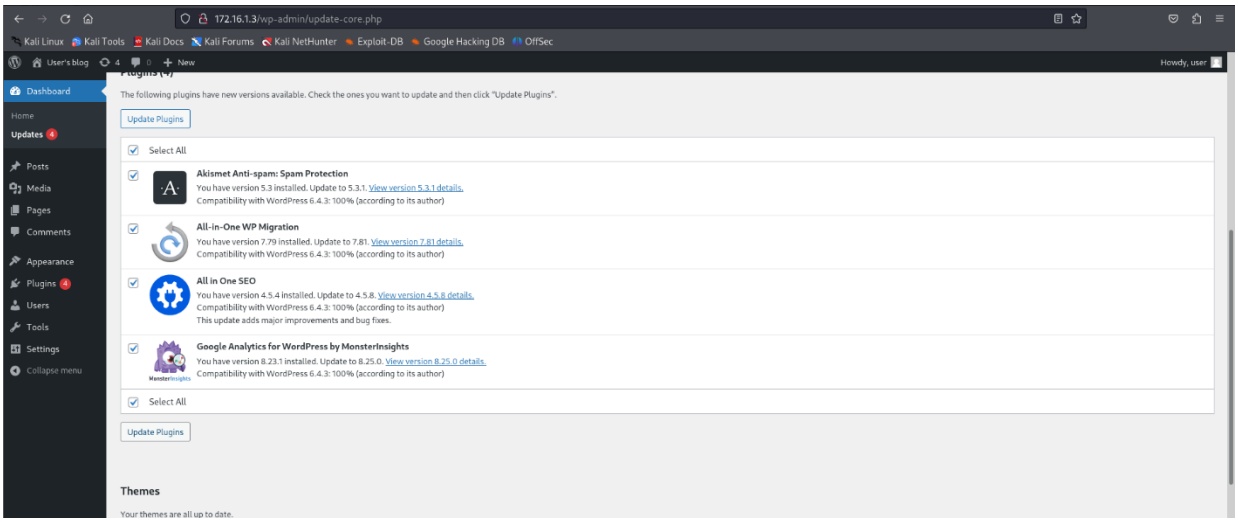

Figure 67. WordPress Admin - Updating Plugins.

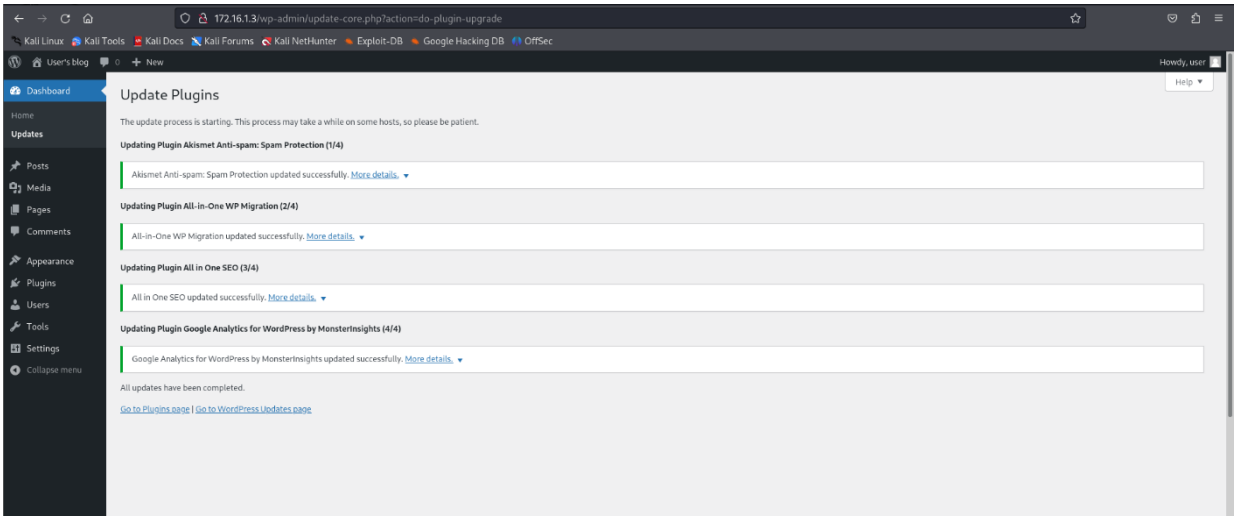

Figure 68. WordPress Admin - Updating Plugins.

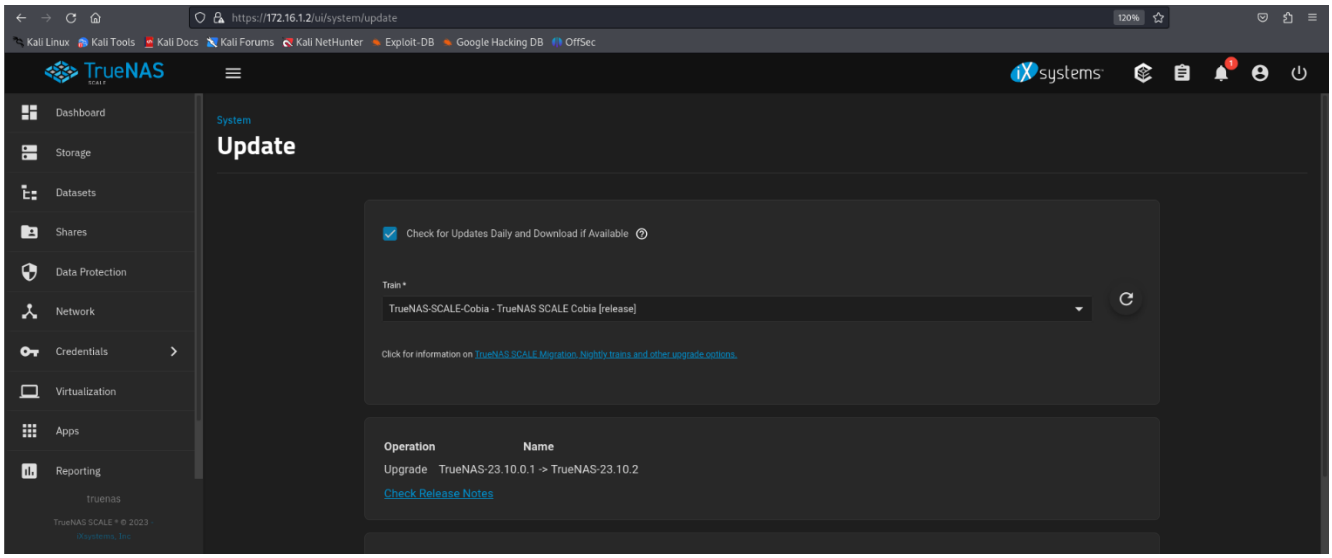

Figure 69. TrueNAS Web GUI - Checking for updates.

Additional Topic – Firewalls

Table 1 – Top 10 Firewalls

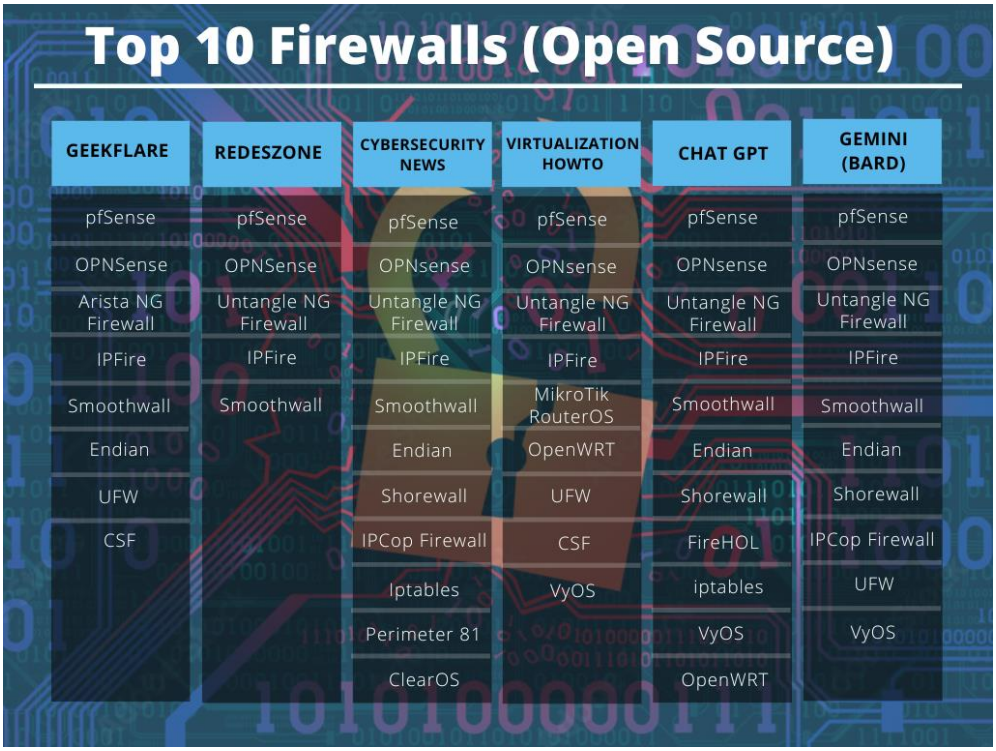

Figure 70. Table - Top 10 Firewalls.

Table 2 – Firewalls: Pros vs Cons

Table 1. Top 5 Firewalls - Pros vs Cons.

	pfSense	OPNSource	Untangle	IPFire	Endian
F - Functionality	1	1	1	1	1
U - Usability	1	0.5	1	0.5	1
R - Reliability	1	0.5	1	1	0.5
P - Performance	1	1	1	0.5	0.5
S - Supportability	0.5	1	0.5	0.5	0
Integrity	1	1	0.5	1	1
Security	0.5	1	1	1	1
Portability	0.5	0.5	0.5	1	0.5
Reusability	0.5	0.5	0.5	1	1
Cost	FREE	FREMIUM	FREMIUM	FREE	FREMIUM
TOTAL	7/9	7/9	7/9	7.5/9	6.5/9

Conclusion

In conclusion, the implementation of this laboratory has provided me with valuable insights into configuring and setting up a firewall across multiple network segments and services. Several challenges were encountered during the process, requiring the use of cronjobs. One challenge involved addressing an issue in TrueNAS, ensuring the server functioned correctly on port 8080. Another cronjob was employed in WordPress to restart the network service, ensuring the proper application of the static IP address. The comprehension of port forwarding rules presented its own set of difficulties, particularly in understanding the source and destination parameters.

While there is room for improvement in terms of connectivity and security practices for the services, I am satisfied with the achieved results and the successful communication within the network, despite the RADIUS server not being implemented in pfSense firewall and the DNS server as well. The overall network performance meets the specified requirements.

The implemented network topology showcases a solid foundation for how companies should configure and secure a basic network to mitigate attacks or vulnerabilities.

Additional Topic:

Regarding the firewall tables, we can easily corroborate from multiple sources to determine which firewall is the best fit based on factors such as the cost, as well as criteria like FURPS, and most importantly user reviews. This allows us to make informed decisions about the most suitable choice for a company and its needs.

References

TrueNAS - SMB:

SpaceRex. (2023, January 4). How to create a SMB Share in TrueNAS SCALE - The basics [Video]. YouTube. https://www.youtube.com/watch?v=DeXNFUzpeFI

TrueNAS - iSCSI Storage:

Virtualizacion y Redes. (2020, December 20). 19. Curso de Vmware 6.7 - Configuracion de Freenas, Iscsi y NFS [Video]. YouTube. https://www.youtube.com/watch?v=hgAKpZWYeBI

pfSense Firewall Rules:

Airline Hydraulics. (2021, August 19). Port forwarding, IP masquerading, and 1-1 NAT explained | Industrial Wi-Fi Setup Part 11 | FL WLAN [Video]. YouTube. https://www.youtube.com/watch?v=yfQKXpRcxxA

Glossary

What is a Hypervisor? - Hypervisor Explained - AWS. (n.d.). Amazon Web Services, Inc. https://aws.amazon.com/what-is/hypervisor/#:~:text=A%20hypervisor%20is%20a%20software,individual%20virtual%20machines%20as%20required.

Sheldon, R. (2024, March 18). paravirtualization. IT Operations. https://www.techtarget.com/searchitoperations/definition/paravirtualization

QEMU. (n.d.). https://www.qemu.org/

What is a virtual machine (VM)? | IBM. (n.d.). https://www.ibm.com/topics/virtual-machines

What is KVM? - Kernel-Based Virtual Machine Explained - AWS. (n.d.). Amazon Web Services, Inc. https://aws.amazon.com/what-

is/kvm/#:~:text=Kernel%2Dbased%20Virtual%20Machine%20(KVM,computer%20within%20another%20physical%20computer.

Wikipedia contributors. (2024, February 8). Kernel-based virtual machine. Wikipedia. https://en.wikipedia.org/wiki/Kernel-based_Virtual_Machine

Moore, N. (2023, December 6). service virtualization. IT Operations. https://www.techtarget.com/searchitoperations/definition/service-virtualization#:~:text=Service%20virtualization%20helps%20these%20teams,and%20shared%20responsibility%20for%20quality.

Server pools. (n.d.). https://docs.vmware.com/en/VMware-NSX-Advanced-Load-Balancer/22.1/Configuration_Guide/GUID-B59BC312-750E-4A80-82CD-9D6CB1F09835.html

What is high availability? (2023, October 5). Cisco. https://www.cisco.com/c/en/us/solutions/hybrid-work/what-is-high-availability.html#:~:text=High%20availability%20means%20that%20an,with%20minimal%20or%20zero%20downtime.

What is a Container? | Docker. (n.d.). Docker. https://www.docker.com/resources/what-container/

Wikipedia contributors. (2024a, January 3). Multithreading (computer architecture). Wikipedia. https://en.wikipedia.org/wiki/Multithreading_(computer_architecture)

Research

Perimeter firewall. (2023, March 16). VMware. https://www.vmware.com/topics/glossary/content/perimeter-firewall.html

Sophos Ltd. (n.d.). NAT rules - Sophos Firewall. https://docs.sophos.com/nsg/sophos-firewall/18.5/Help/en-us/webhelp/onlinehelp/AdministratorHelp/RulesAndPolicies/NATRules/index.html

Abdullahi, A. (2023, September 19). What are firewall rules? definition, types, and best practices. Enterprise Networking Planet. https://www.enterprisenetworkingplanet.com/security/firewall-rules/

Watts, S. (n.d.). What is a Virtual Network? BMC Blogs. https://www.bmc.com/blogs/virtual-network/#:~:text=A%20virtual%20network%20is%20a,addition%20to%20numerous%20other%20benefits.

What is Load Balancing? - Load Balancing Algorithm Explained - AWS. (n.d.). Amazon Web Services, Inc. https://aws.amazon.com/what-is/load-balancing/#:~:text=A%20load%20balancer%20is%20a,resource%20servers%20are%20used%20equally.

What is DNS? – Introduction to DNS - AWS. (n.d.). Amazon Web Services, Inc. https://aws.amazon.com/route53/what-is-dns/#:~:text=DNS%2C%20or%20the%20Domain%20Name,example%2C%20192.0.2.44).

Loshin, P. (2021, September 30). RADIUS (Remote Authentication Dial-In User Service). Security. https://www.techtarget.com/searchsecurity/definition/RADIUS#:~:text=RADIUS%20(Remote%20Authentication%20Dial%2DIn%20User%20Service)%20is%20a,the%20requested%20system%20or%20service.

Gillis, A. S. (2020, July 22). web server. WhatIs. https://www.techtarget.com/whatis/definition/Web-server

What is content delivery? (2021, July 7). Optimizely. https://www.optimizely.com/optimization-glossary/content-delivery/

Lewis, S., & Burke, J. (2019, June 6). gateway. IoT Agenda. https://www.techtarget.com/iotagenda/definition/gateway

What is network monitoring? (2023, July 4). Cisco. https://shorturl.at/koLTZ

What is IaaS (Infrastructure as a Service)? | Google Cloud. (n.d.). Google Cloud. https://cloud.google.com/learn/what-is-iaas

What is IaaS (Infrastructure as a Service)? | Google Cloud. (n.d.). Google Cloud. https://cloud.google.com/learn/what-is-iaas

What is SaaS? Software as a Service | Microsoft Azure. (n.d.). https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-saas#:~:text=Software%20as%20a%20service%20(SaaS,from%20a%20cloud%20service%20provider.

What is WAN | Wide Area Network Definition | Computer Networks | CompTIA. (n.d.). CompTIA. https://www.comptia.org/content/guides/what-is-a-wide-area-network

What is a LAN? (2023, September 6). Cisco. https://www.cisco.com/c/en/us/products/switches/what-is-a-lan-local-area-network.html#:~:text=A%20local%20area%20network%20(LAN,in%20an%20office%20or%20school.

What is a DMZ network and why would you use it? | Fortinet. (n.d.). Fortinet. https://www.fortinet.com/resources/cyberglossary/what-is-dmz