Technical Manual: Cybersecurity Lab - Firewall

v. 2025-1

Shoaib Azad

November 24, 2025

Contents

1 Steps

1.1 Initial Configuration

1. Download the OPNsense DVD ISO image, extract the archive using a decompression utility (e.g., `bzip2`).

```
[shoaib@DBL-01 ~]$ bzip2 -d /home/shoaib/Downloads/OPNsense-25.7-dvd-amd64.iso.bz2
[shoaib@DBL-01 ~]$
```

Figure 1: `bzip2` Extraction Command.

2. Create a new Virtual Machine (VM) in VirtualBox using the FreeBSD (64-bit) type.

> Allocate a minimum of 2 VCPUs, 2 GB RAM and a 8GB VDI hard disk.

3. Create a NAT Network.
   (a) In VirtualBox, go to File > Tools > Network Manager.
   (b) Go to the `NAT Networks` tab and click Create.
   (c) Name it (e.g., `NatNetwork1`), set the IPv4 Prefix (e.g., `10.0.2.0/24`) and ensure DHCP is enabled.

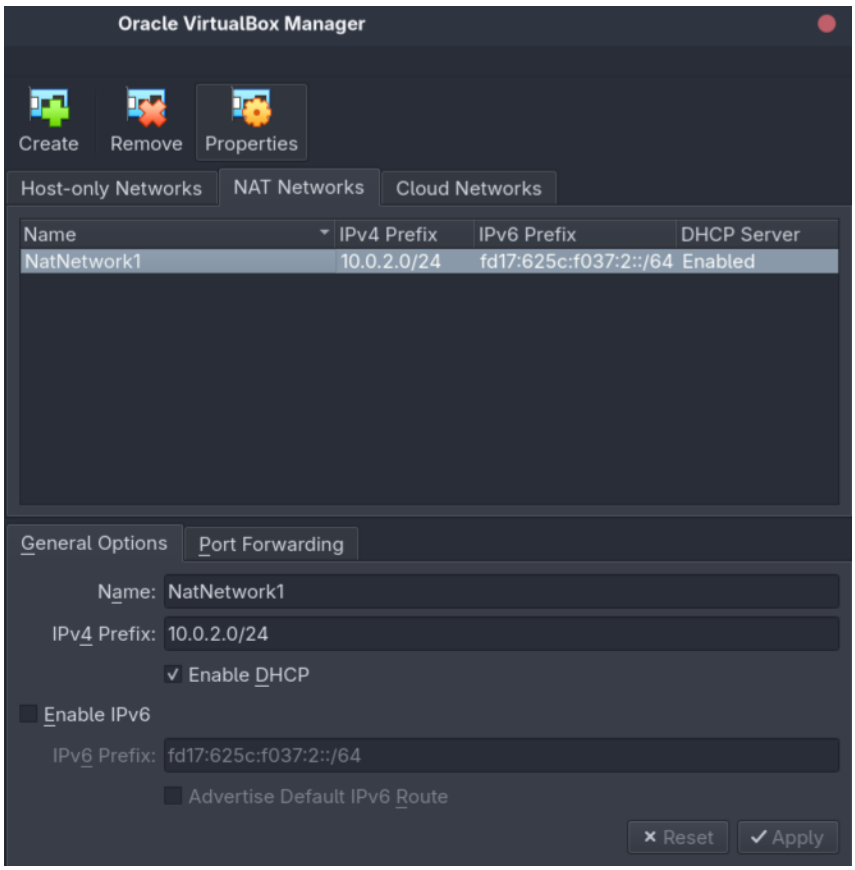

Figure 2: VirtualBox Network Manager Configuration.

4. Configure the VM's network adapters.
   (a) Set Adapter 1 to "NAT Network" (e.g., `NatNetwork1`).
   (b) Set Adapter 2 to "Internal Network" (e.g., `intnet`).

Figure 3: VM Configuration Summary.

5. Boot the VM using the OPNsense ISO, follow the setup wizard.
   (a) Select "UFS file system" installation option.
   (b) Set a strong root password.

> To launch the installer, use the default credentials at the login prompt: `installer` / `opnsense`.

6. After the installation and first reboot, login as `root` and assign the interfaces.
   (a) Enter `"1"` to access the `Assign interfaces` menu.
   (b) Enter `"n"` to skip configuring LAGGs.
   (c) Enter `"n"` to skip configuring VLANs.
   (d) Enter the name for the WAN interface (e.g., `em0`).
   (e) Enter the name for the LAN interface (e.g., `em1`).
   (f) Leave the optional interface prompt empty (press *Enter*).
   (g) Enter `"y"` to proceed and apply changes.

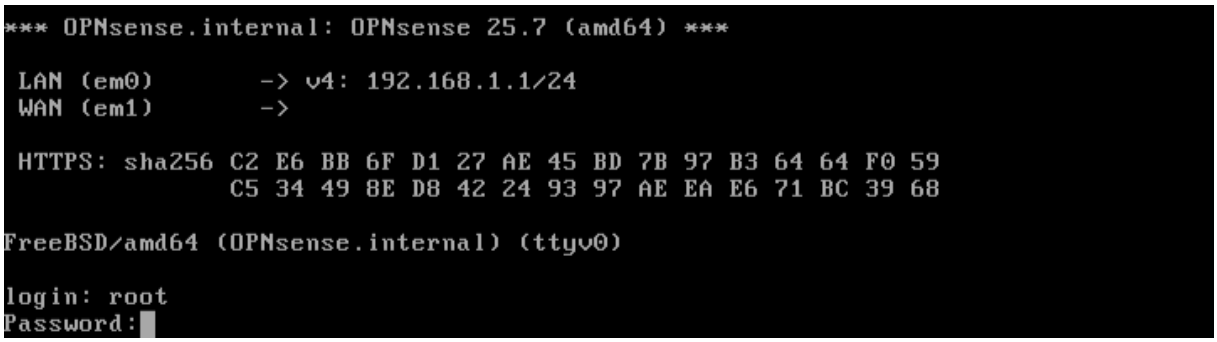

Figure 4: Console State (Before Configuration).

7. Set a static IPv4 address to the LAN interface.
   (a) Enter `"2"` to access the `Set interface IP address` menu.
   (b) Enter `"1"` to select the LAN interface.
   (c) Enter `"n"` to skip configuring the LAN interface via DHCP.
   (d) Enter your chosen static IPv4 address (e.g., `10.200.200.251`).
   (e) Enter `"24"` for the IPv4 subnet bit count (represents `255.255.255.0`).
   (f) Leave the upstream gateway prompt empty (press *Enter*).
   (g) Enter `"n"` to skip configuring IPv6 address via WAN tracking.
   (h) Enter `"n"` to skip configuring IPv6 address via DHCP6.
   (i) Leave the new LAN IPv6 address prompt empty (press *Enter*).
   (j) Enter `"n"` to skip enabling the DHCP server on the LAN interface.
   (k) Enter `"y"` to change the web GUI protocol to `HTTP`.
   (l) Enter `"y"` to restore web GUI access defaults and apply the changes.

> The `HTTP` protocol is enabled here solely for lab simplicity.

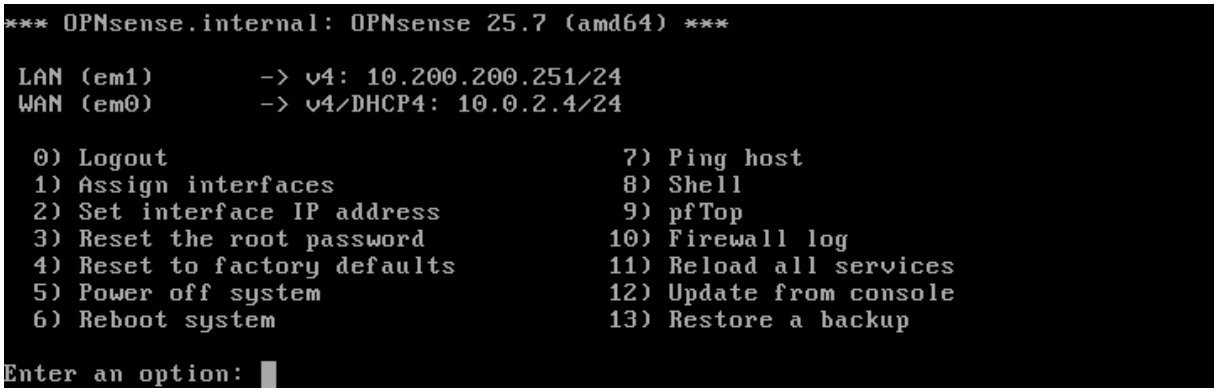

Figure 5: Console State (After Configuration).

8. Boot a client VM (connected to the same `intnet`).
   (a) Configure the client with a static IP (e.g., `10.200.200.10`).
   (b) Set the Master's IP (e.g., `10.200.200.251`) as the client's default gateway.

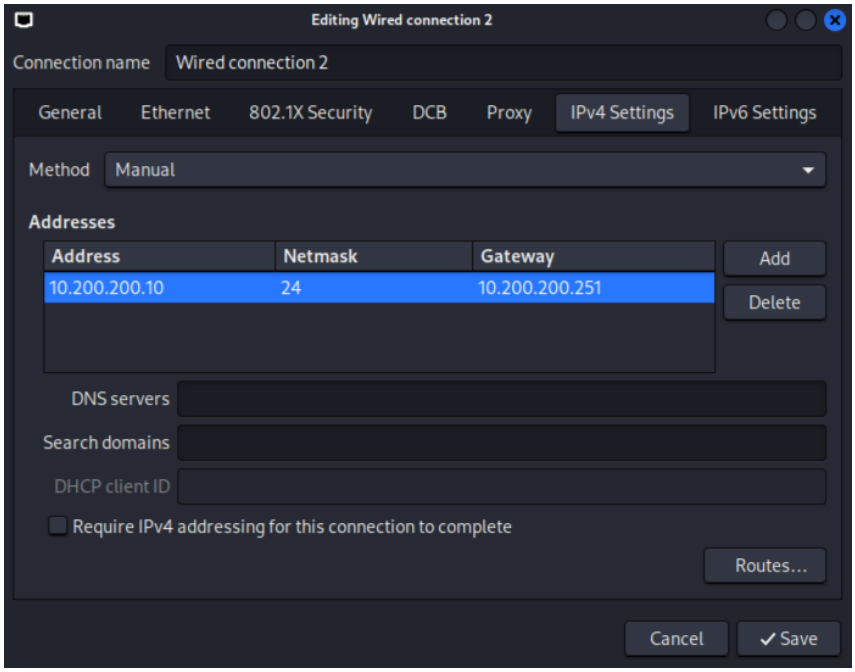

Figure 6: Client VM IPv4 Configuration.

9. Access the OPNsense Web Graphical User Interface (GUI) from the client's browser and log in.

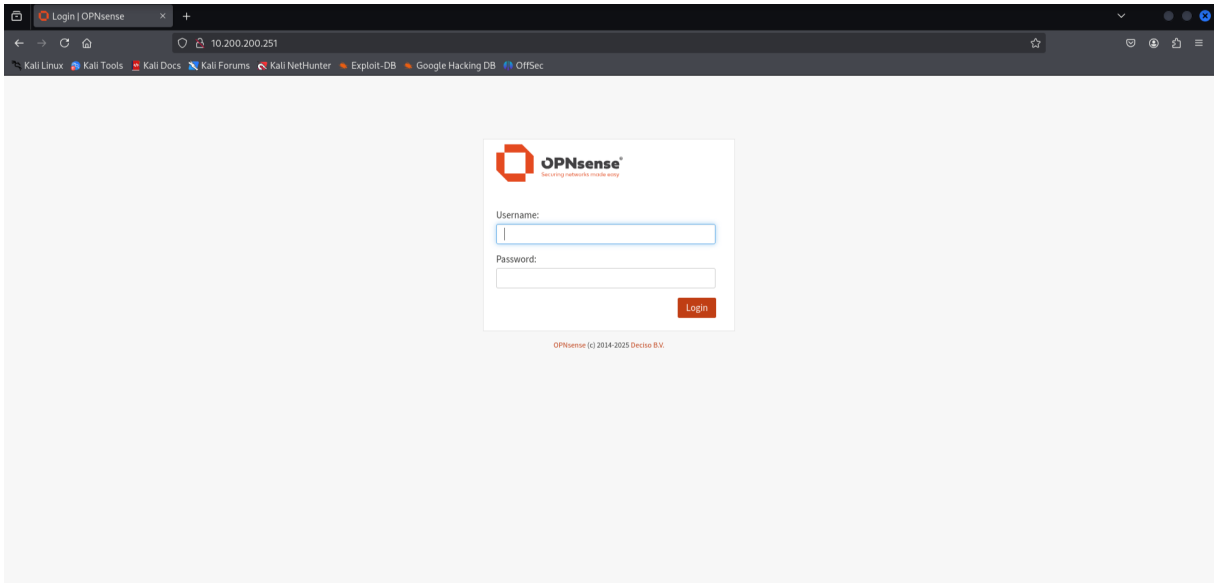

Figure 7: OPNsense Web GUI login screen.

- Use the firewall's LAN IP (e.g., `https://10.200.200.251`).

10. Update the firewall to the latest firmware.
    (a) In the OPNsense Web GUI, go to System » Firmware » Status.
    (b) Click Check for updates.
    (c) If updates are available, click Update to download and install them.

1.2 IDS/IPS Implementation

1. In the OPNsense Web GUI, go to Interfaces > Settings, ensure all hardware offloading features are disabled.

> This allows the IDS/IPS engine to correctly inspect all traffic.

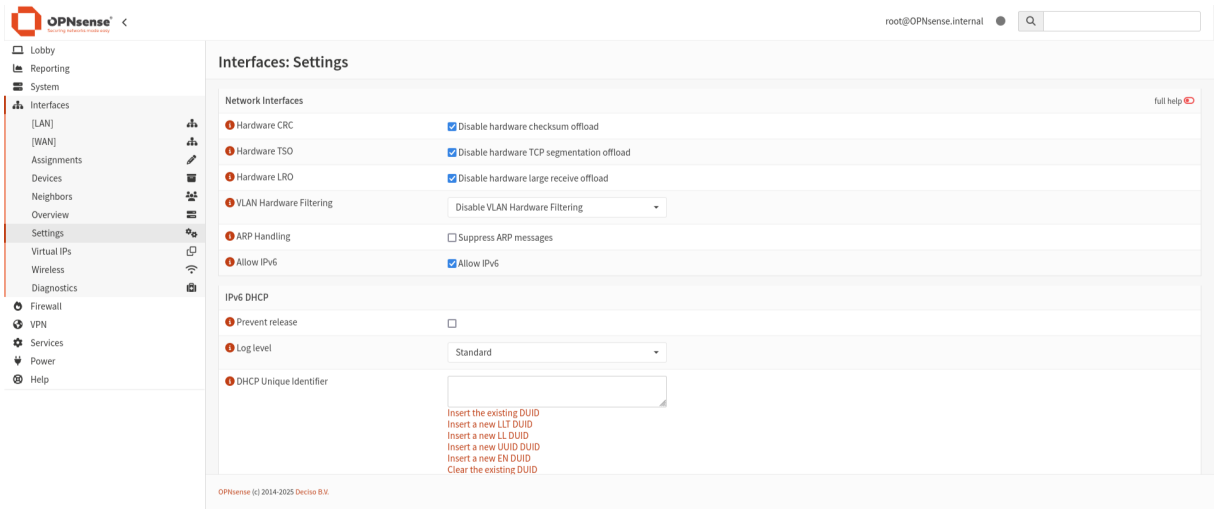

Figure 8: Disabled Hardware Offloading Features.

2. Configure the Suricata intrusion detection settings.
   (a) In the OPNsense Web GUI, go to Services > Intrusion Detection > Administration.
   (b) Toggle `Advanced Mode`.
   (c) Check `Enabled`.
   (d) Check `IPS mode`.
   (e) Check `Promiscuous mode`.
   (f) Check `Enable syslog alerts`.
   (g) Set `Interfaces` to LAN.
   (h) Set `Detect Profile` to Medium.
   (i) Set `Pattern matcher` to Hyperscan.
   (j) Define `Home networks` as the internal subnet (e.g., `10.200.200.0/24`).
   (k) Click Apply.

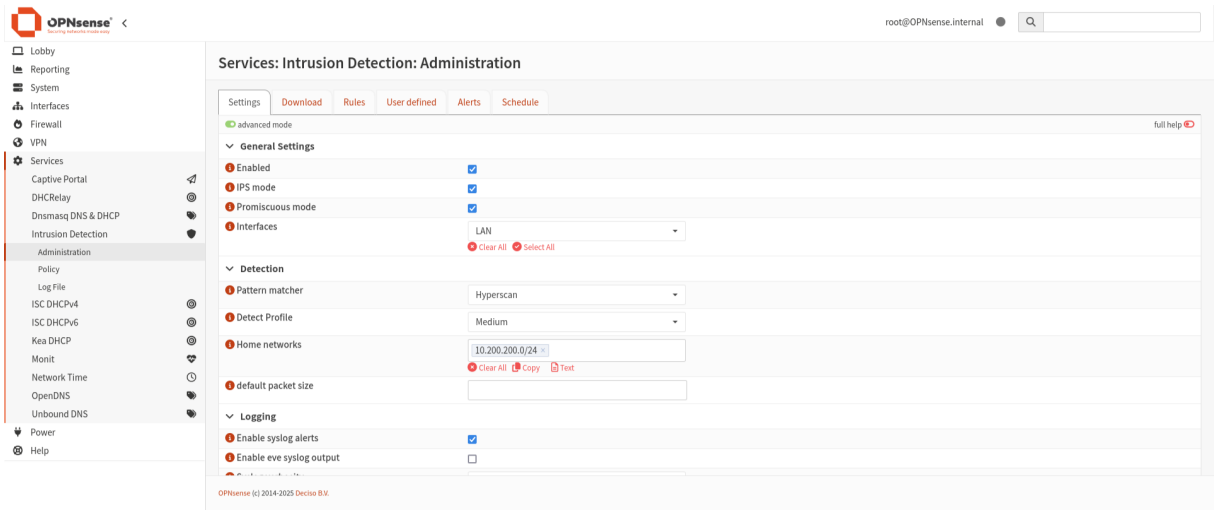

Figure 9: IDS/IPS Administration Settings.

3. Enable Secure Shell (SSH) access.
   (a) In the OPNsense Web GUI, go to System » Settings » Administration.
   (b) Check `Enable Secure Shell`.
   (c) Check `Permit root user login`.
   (d) Check `Permit password login`.

> Password login is enabled here solely for lab simplicity.

4. Develop a custom Suricata ruleset to detect a simulated attack.
   (a) On the client VM, create a .rules file (e.g., `custom_nmap.rules`).
   (b) Define the detection logic within the file.

```
alert tcp $HOME_NET any → 10.200.200.251/24 any (msg:"POSSIBLE NMAP SYNSTEALTH SCAN DETECTED"; flow:stateless;
flags:S; priority:5; threshold:type threshold, track by_src, count 50, seconds 1; classtype:attempted-recon;
sid:1234;)
```

Figure 10: Custom Rule Code Snippet.

> The rule establishes a rate-limiting threshold, alerting the system when 50 or more SYN packets originating from the internal network are detected within a single second.

5. Create a corresponding XML metadata file (e.g., `custom_nmap.xml`) on the client.

```xml
<?xml version="1.0"?>
<ruleset documentation_url="http://docs.opnsense.org/">
    <location url="http://10.200.200.10/" prefix="customnmap" />
    <files>
        <file description="Custom Nmap Detection Rules">customnmap.rules</file>
    </files>
</ruleset>
```

Figure 11: XML Code Snippet.

- This file directs OPNsense to the location of the external ruleset.

6. Install the ruleset onto the IDS/IPS engine.
   (a) Use a SFTP program (e.g., `FileZilla`), connect to the Master IP (e.g., `sftp://10.200.200.251`) using `root` credentials on port 22.
   (b) Upload the `.xml` file to the OPNsense metadata directory: `/usr/local/opnsense/scripts/suricata/metadata/rules/`.

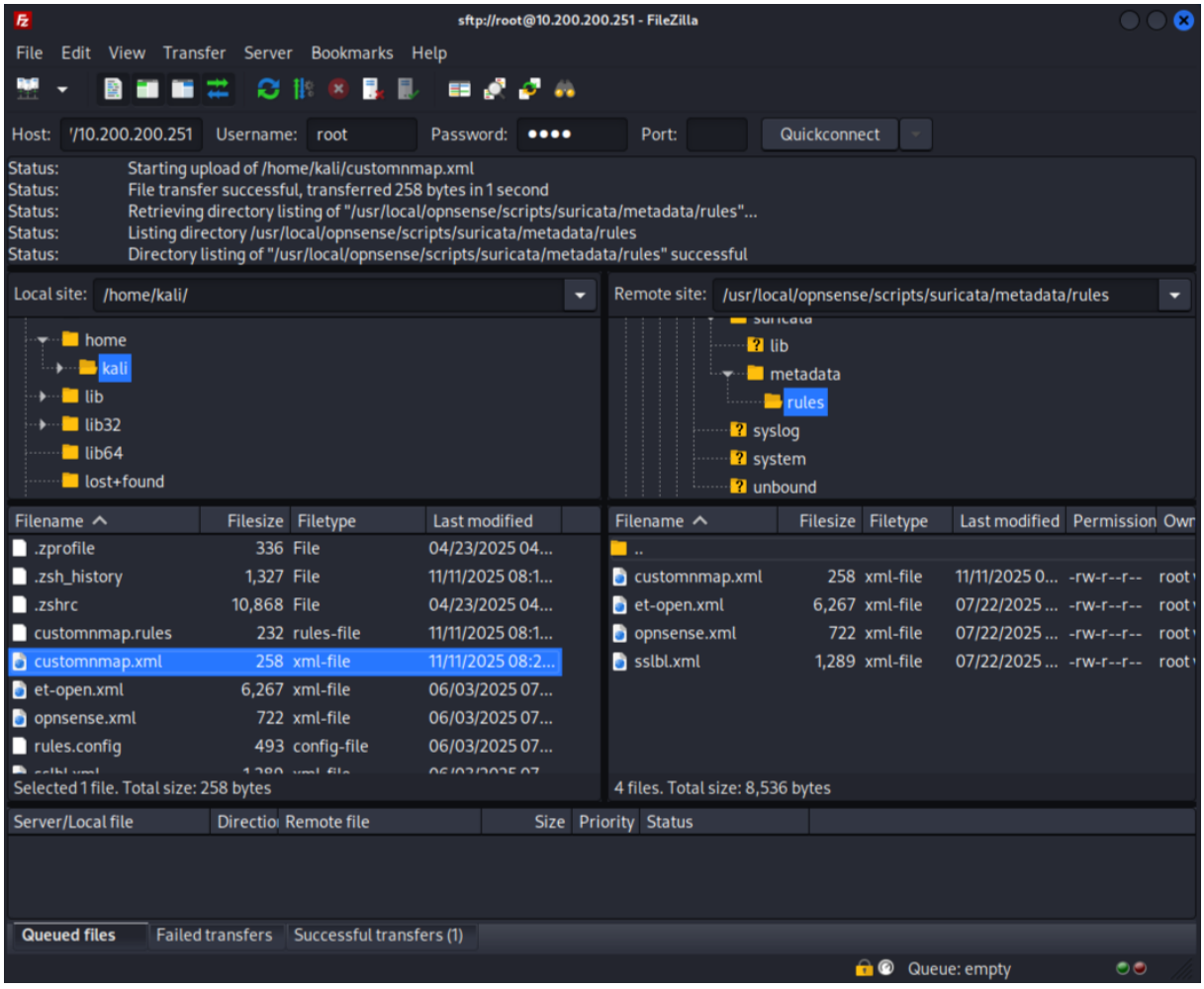

Figure 12: FileZilla SFTP transfer.

(c) Launch a terminal in the directory containing the `.rules` file.

(d) Enter "`sudo python3 -m http.server 80`".

Figure 13: Python Server Running.

The command initiates a simple web server, providing HTTP access to the `.rules` file

7. Activate the custom ruleset.

(a) In the OPNsense Web GUI, go to Services » Intrusion Detection » Administration » Download.

(b) Check the custom ruleset (e.g., `customnmap/Custom Nmap Detection Rules`).

(c) Click Download & Update Rules.

(d) Click the reload icon (top right) to apply the changes.

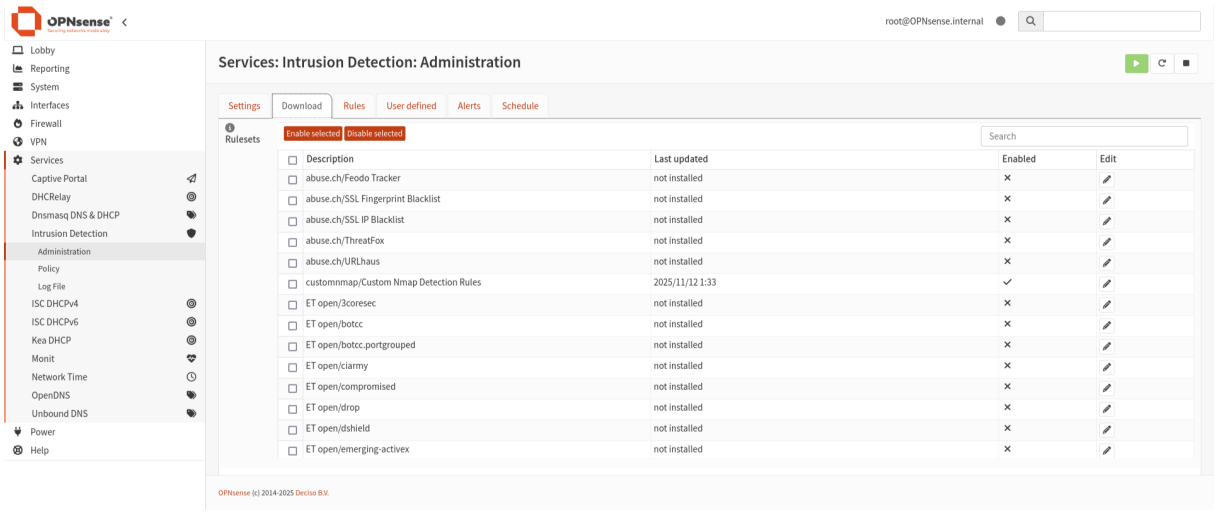

Figure 14: Enabled Custom Nmap Ruleset.

1.3 Web Policy Enforcement

1.4 High Availability Clustering

1.5 Multi-WAN Failover and Load Balancing

1.6 NGFW Deployment

2 Validation of System Continuity

1. Execute a TCP SYN Stealth Scan from the Kali VM against the firewall:
   `sudo nmap -sS -Pn -top-ports 500 10.200.200.251`

Figure 15: Kali terminal running Nmap scan.

1. Navigate to Services » Intrusion Detection » Alerts.
2. Verify that multiple alerts appear with the message **"Possible Nmap stealth scan detected"**, confirming the IPS engine is active.

Figure 16: OPNsense Alerts showing successful detection.

2.1 CARP Failover Exercise

3 Appendix: Supplementary Documentation

3.1 Host System Specifications

3.2 Virtual Environment Details

References

[1] `https://opnsense.org/`

[2] `https://www.sunnyvalley.io/zenarmor`