Opensense Firewall for Blue Teaming Homelab

Tools Needed:
Download DVD image of Opensense Firewall from :
We will be using Virtual Box as Virtualization Software (You can use anyone you prefer VMware/OracleVBox/HyperV)
THe download for Opensense Firewall will be in the format with extension .bz2
We need a archiver to extract the actual ISO to add in Virtualbox
Once Virtual box is installed we need to add OpenSense FW as a software

Steps:

- Open up Virtualbox Application
- Add New
    - Select a name for FW file (I am using OpnSense FW)
    - Select OS as FreeBSD
    - Select 2 core processor with RAM of 1GB
    - Select Hard Sisk Size as 16 Gb
        - On the network settings page we need 2 interface for Firewall to work with
        - a. NAT with configuration to Deny all Interface
        - b. Internal Network with configuration to Allows VMs in the interface (Basically this internal network interface acts as a virtualized switch) : This interface will be connected to with other VM within Virtualbox
    - Switch on the VM
        - -> We need to type installer to install the FW configuration or incase you want to run actually in live mode select root

Installing of the OPNSense and Configuration

Here we are installing

- Type installer with password opnsense as password
    - We use Default Key Map
    - We use Unix File System : UFS/UEFI Hybrid as this is stable for Homelab
    - Next we select the 16GB vbox HDD which we set earlier > Ok
    - Once the installation is complete > We need to change the server password
    - Use a desired password
    - After changing password > Select Exit and Reboot > Enter
    - Once done we need to remove the virtual disk from Device Settings in VM menu so the FW app donot restart with new installation
- Select Device > Optical Disk > REMOVE ONLY ISO DISK (DONOT REMOVE THE VDI FILE)
- Restart the Application
- Once the VM starts up login with root and the new password which you changed

OpnSense is installed and now configuration is done

- We will now Assign Interface > Select 1: Assign Interface>
- Do you configure Laggs (Link Aggregation Group): We dont need here for Homelab so we type N for no
    - Note: LAGG is basically as Link Aggregation Group which aggregate multiple network interface to form a high speed link
- Do you configure VLAN (Virtual Lan): We dont need here for homelab so we type N for no
    - Note: VLAN is basically a virtual Lan which is used to create segments in our network and switches
- Now we need to provide the interface we need to WAN interface: we will use en0 ie the interface for NAT
- Now we need to provide the interface we need to LAN interface: We will use en1 ie the interface of internalnet
    - It will provide summary of LAN AND WAN setting
        - Which we have to select yes to proceed
- And it will configure the interface for us!
- Now reboot the application

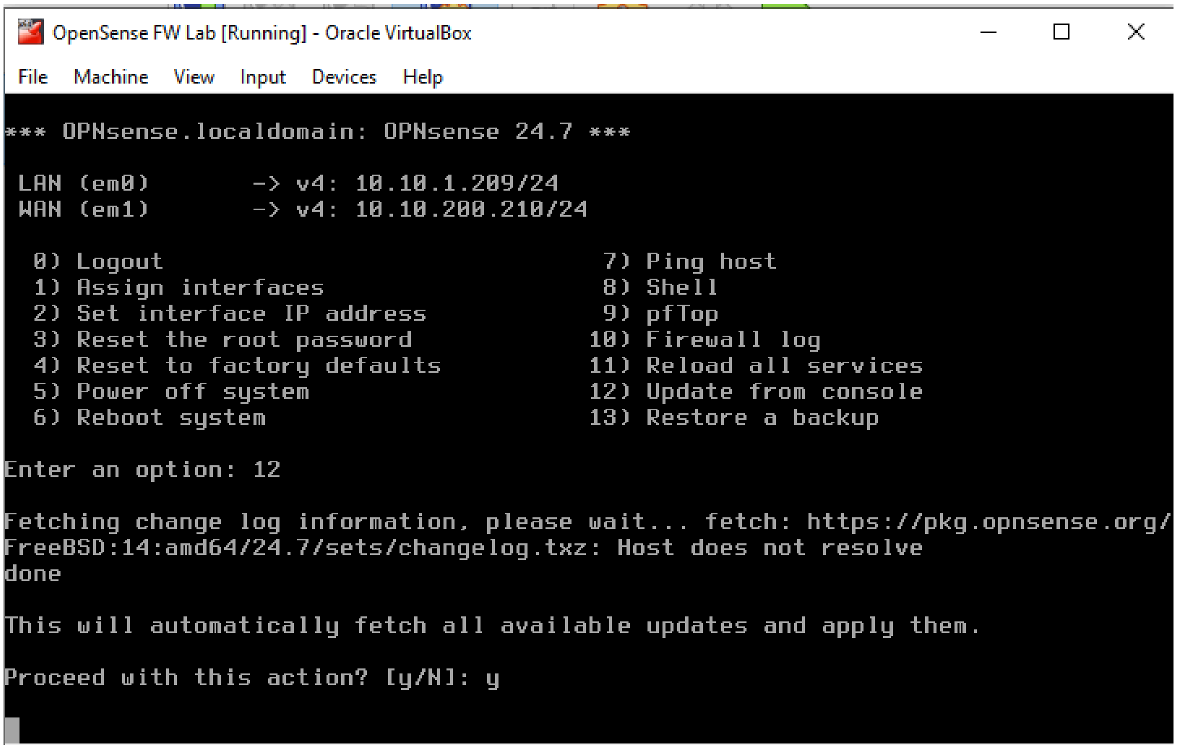
Interface for both NAT and Internal Network are set ie LAN and WAN

Setting up Interface IP to access Web GUI for OpnSense

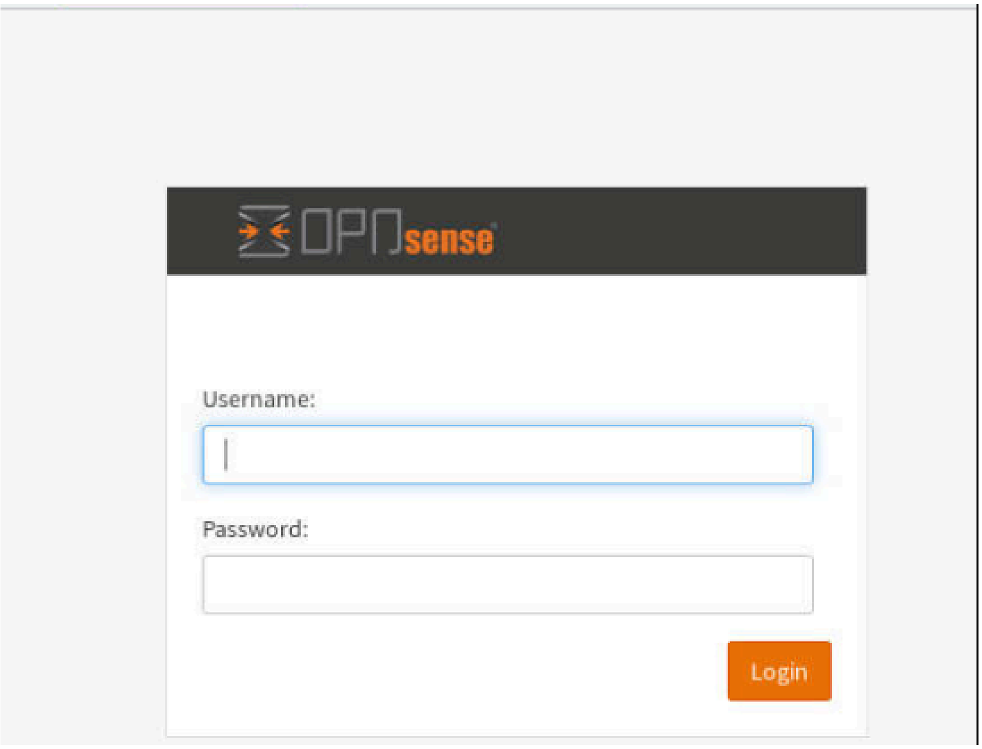
- Here we need to set interface IPs for both WAN AND LAN
- We need to set number of interface as 2
- We need DHCP not to configure automatic IPV4 address : so we select no for DHCP configuration (We will provide Static IP address)
- Set IP address related to Lab network
  Note WAN and LAN will have static IP as per your DHCP server and not Automatic: I have a DHCP configured in my ADFS lab
- So LAN IPV4 : I set to 10.20.200.254
- We need 1-32 Subnet range provided: 24 (Class C network)
    - Press Enter for LAN
        - We dont need IPV6 configured for WAN : No
        - We dont need any DHCP for IPV6 for WAN: No
        - We dont need IPV6 configured for LAN: No
        - We dont need any DHCP for IPV6 for LAN: No
        - Do you want web GUI to change HTTPS to HTTP : As this is lab environment we dont so : Yes for Production it should be No
        - We need WEB GUI access defaults: We need this so Yes

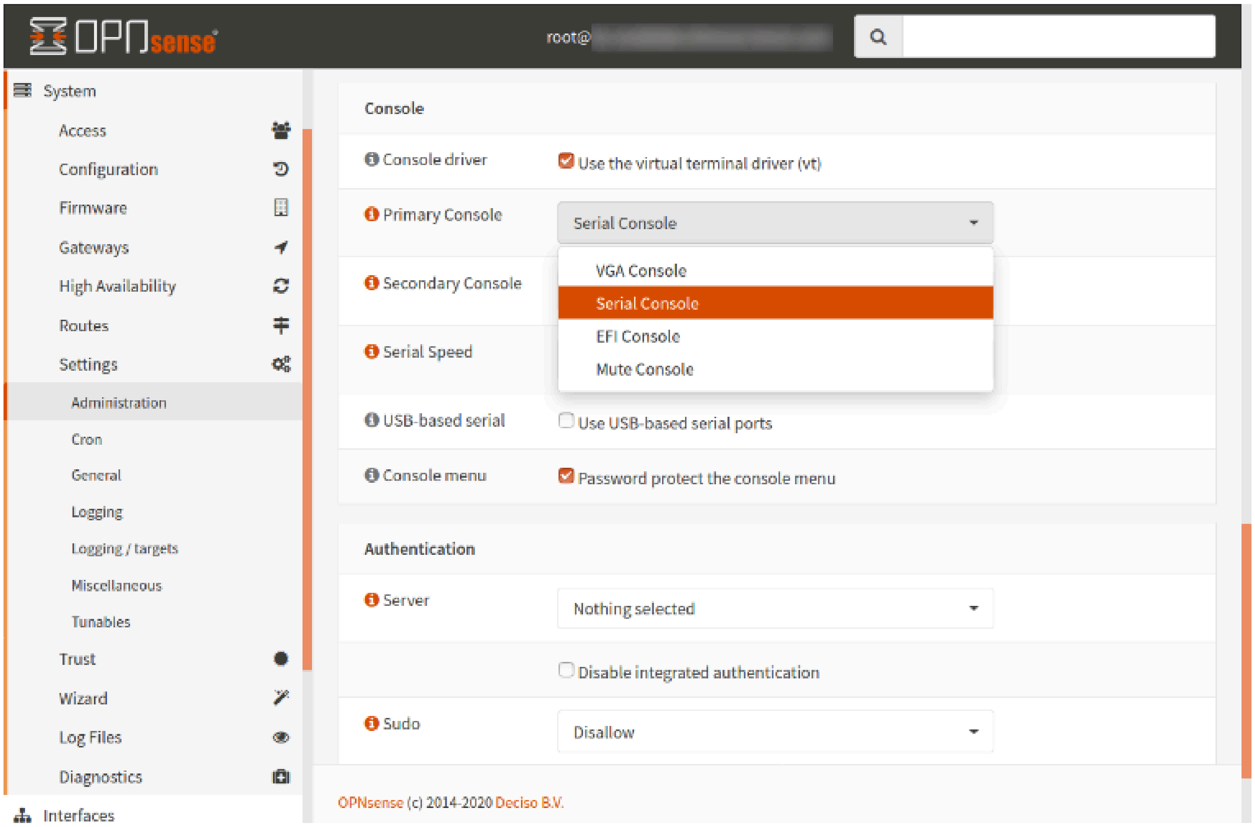
The IP configured for OpnSense Firewall is configured and provided with an IP address for Web GUI console.
username: root and Password: New Password : The GUI show we are accessing the FW

Screenshot


OpenSense FW Lab [Running] - Oracle VirtualBox
File Machine View Input Devices Help

```
*** OPNsense.localdomain: OPNsense 24.7 ***

 LAN (em0)       -> v4: 10.10.1.209/24
 WAN (em1)       -> v4: 10.10.200.210/24

  0) Logout                              7) Ping host
  1) Assign interfaces                   8) Shell
  2) Set interface IP address            9) pfTop
  3) Reset the root password            10) Firewall log
  4) Reset to factory defaults          11) Reload all services
  5) Power off system                   12) Update from console
  6) Reboot system                      13) Restore a backup

Enter an option: 12

Fetching change log information, please wait... fetch: https://pkg.opnsense.org/
FreeBSD:14:amd64/24.7/sets/changelog.txz: Host does not resolve
done

This will automatically fetch all available updates and apply them.

Proceed with this action? [y/N]: y
```





Console

Console driver: ☑ Use the virtual terminal driver (vt)

Primary Console: Serial Console

- VGA Console
- Serial Console
- EFI Console
- Mute Console

Secondary Console

Serial Speed

USB-based serial: □ Use USB-based serial ports

Console menu: ☑ Password protect the console menu

Authentication

Server: Nothing selected

□ Disable integrated authentication

Sudo: Disallow

OPNsense (c) 2014-2020 Deciso B.V.