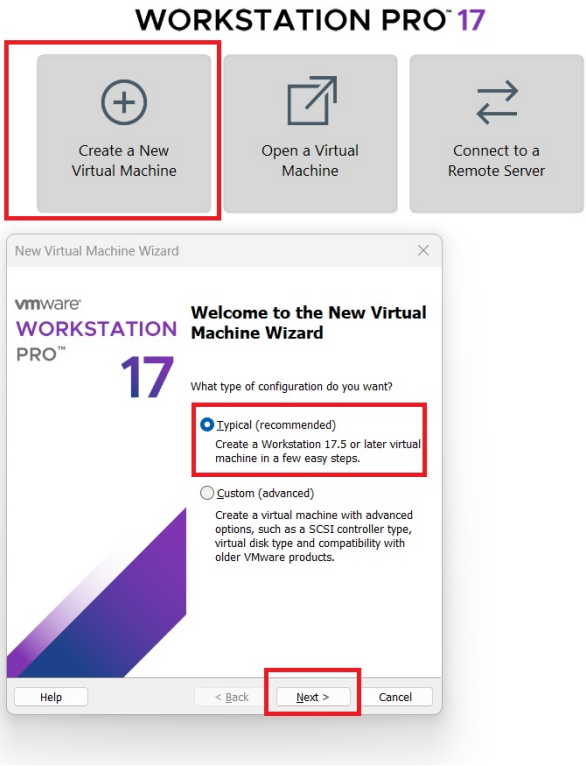
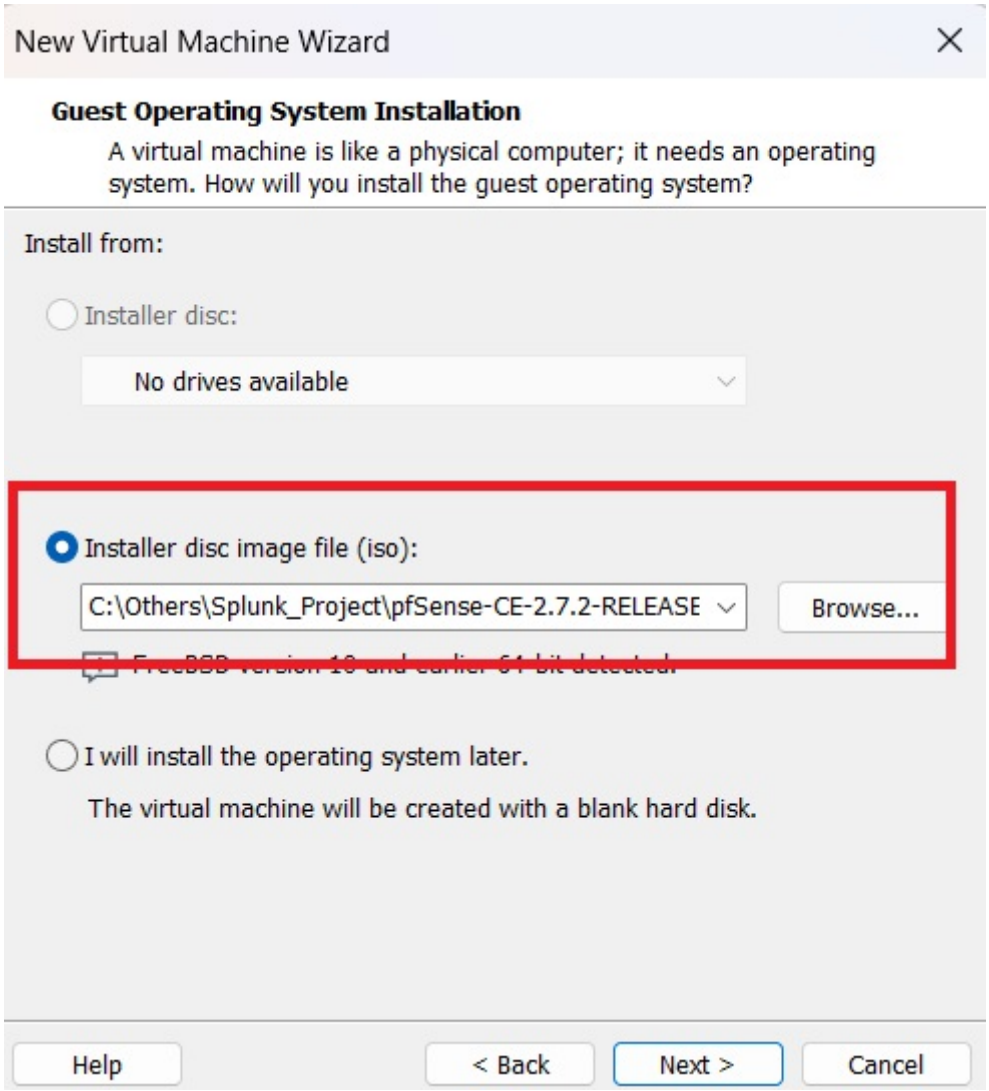
Install PfSense Firewall

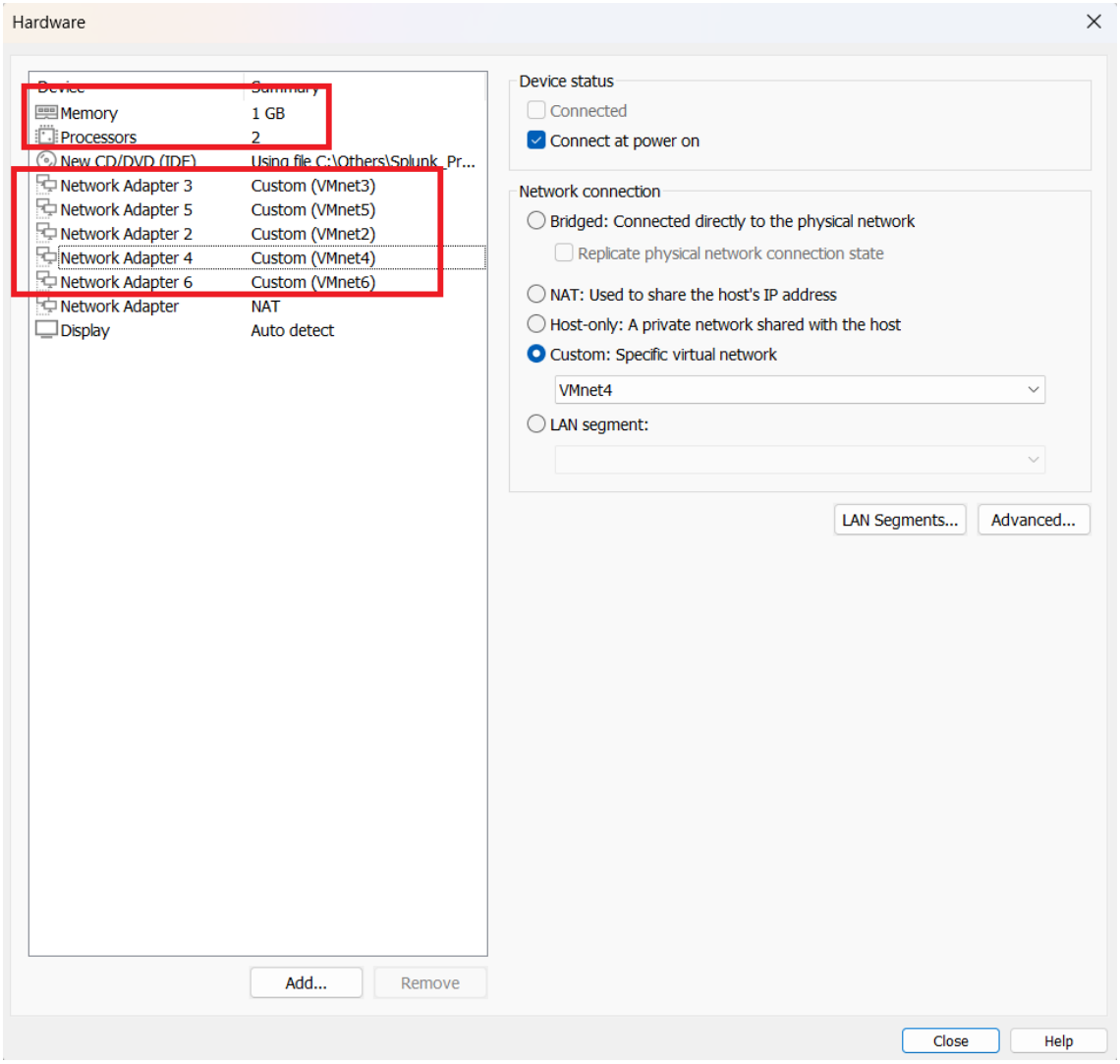
1. Download PfSense Firewall **.iso**, my version is **2.7.2 amd64**
2. Unzip file and Create a New Virtual Machine



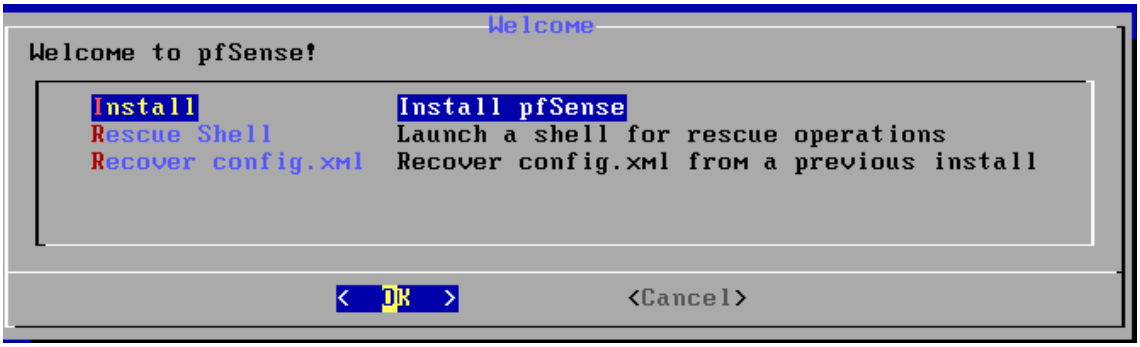
3. Browse for the pfSense.iso and Next



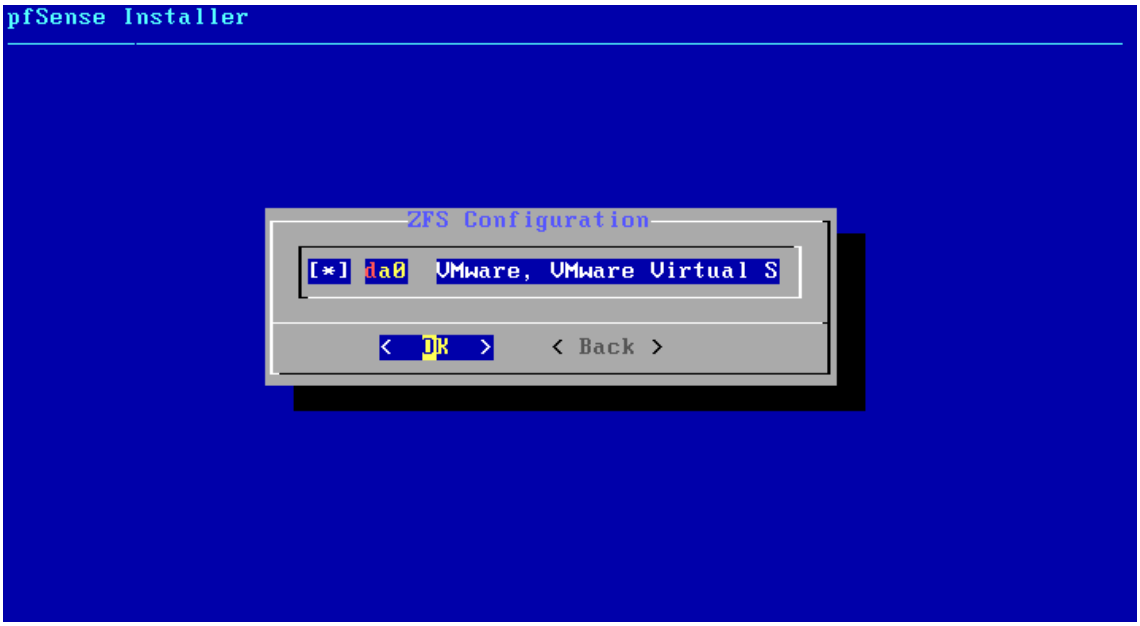
4. Rename it if necessary, and Next
5. Maximum disk size 20GB is enough, select **Store virtual disk as a single file** and Next
6. Click customize hardware
7. Change **Memory** and **Processors**, Add additional **Network Adapter** and configure them as the following capture. These network adapters function as network interfaces, allowing PfSense and other connected hosts to communicate with each other.



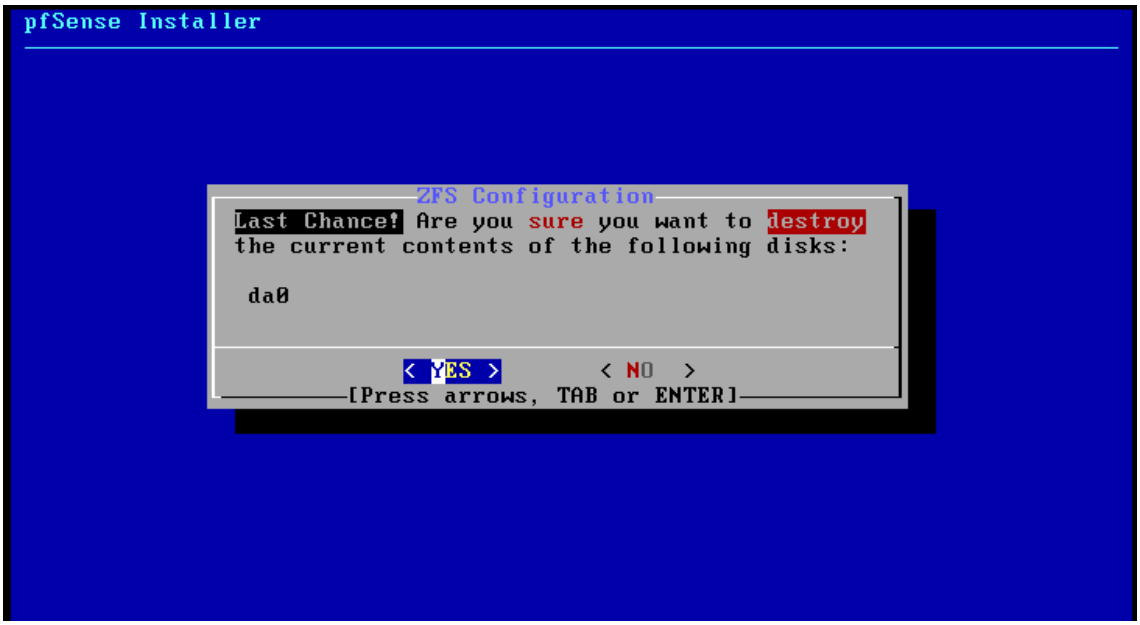
8. **Accept**, **Install** and **OK**



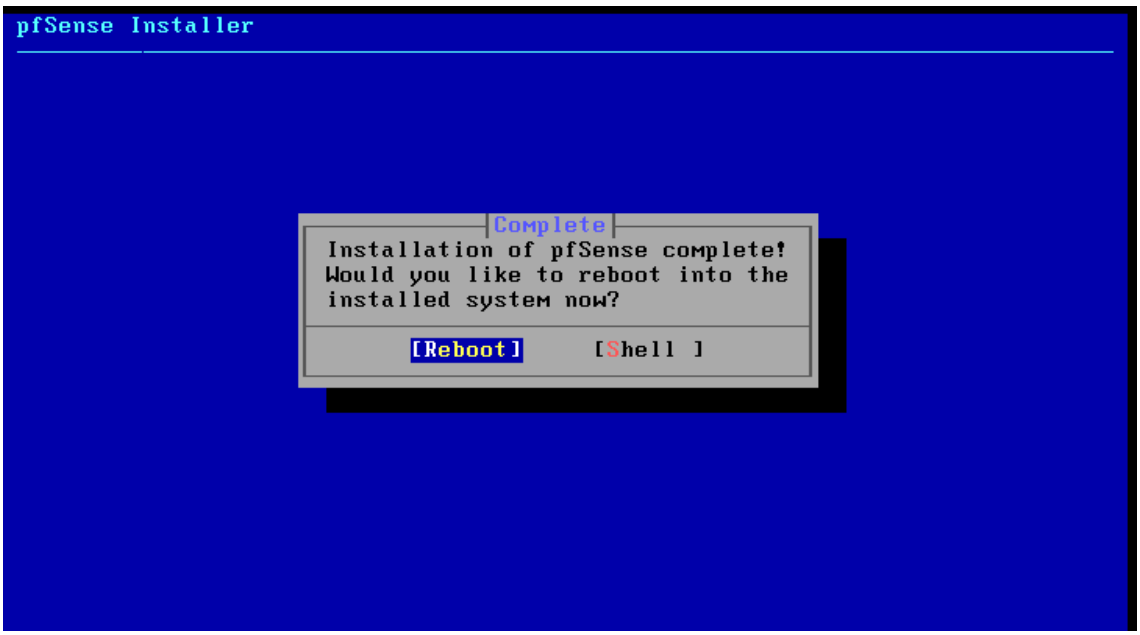
9. Choose **Auto(ZFS)** and **OK**
10. Choose **Install** and **OK**
11. Choose the default Stripe with no Redundancy and **OK**
12. Use **Space bar** on your keyboard to choose da0, make sure ***** is shown, and **OK**



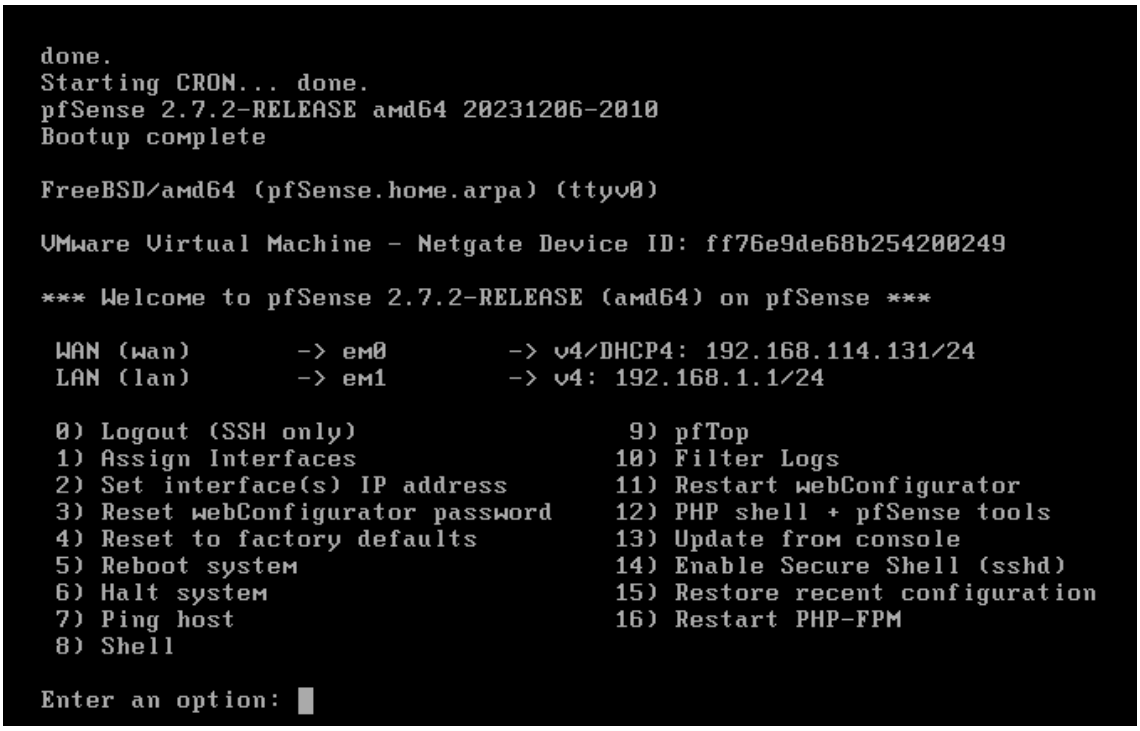
13. Choose **YES**



14. **Reboot**



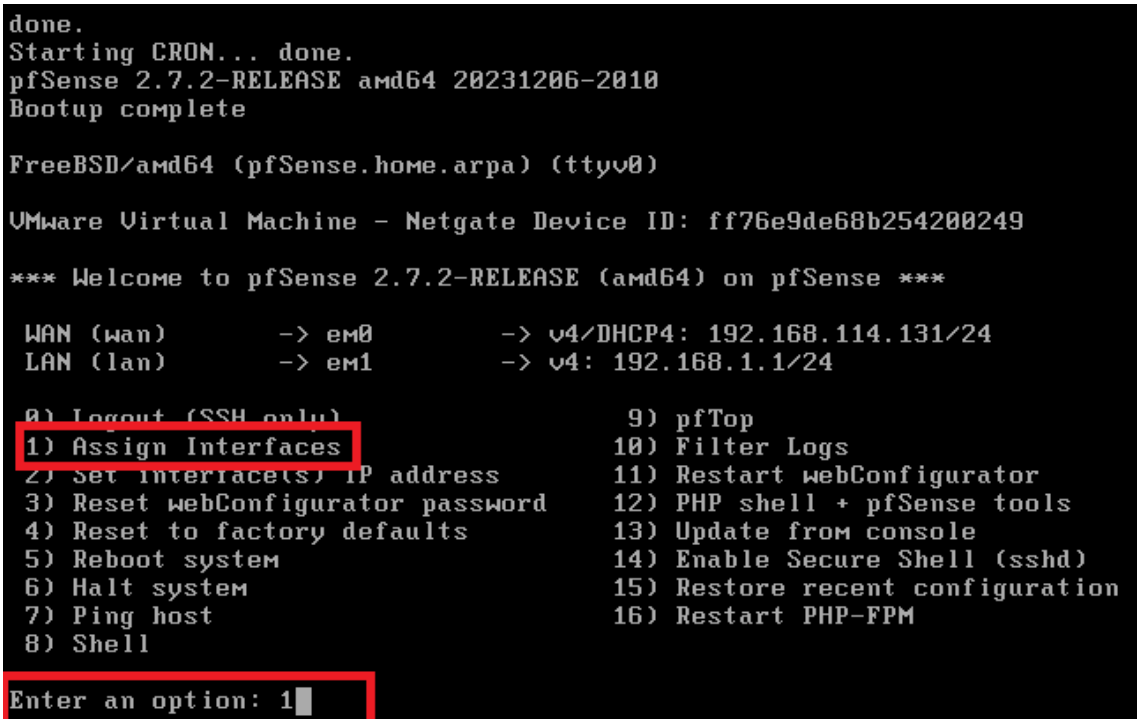
15. After all done, you will get your em0 with IP 192.168.114.x/24 and em1 192.168.1.1/24 by default.



PfSense Firewall Initial Configuration

In this initial configuration, main object is to create interfaces and IP mapping for each subnet.

1. choose **1**



2. choose **n**

3. For the WAN interface, named **em0**, the rest configuration as shown in the following capture. Then input **y**

```
NOTE: this enables full Firewalling/NAT mode.
(em1 em2 em3 em4 em5 a or nothing if finished): em1

Enter the Optional 1 interface name or 'a' for auto-detection
(em2 em3 em4 em5 a or nothing if finished): em2

Enter the Optional 2 interface name or 'a' for auto-detection
(em3 em4 em5 a or nothing if finished): em3

Enter the Optional 3 interface name or 'a' for auto-detection
(em4 em5 a or nothing if finished): em4

Enter the Optional 4 interface name or 'a' for auto-detection
(em5 a or nothing if finished): em5

The interfaces will be assigned as follows:

WAN  -> em0
LAN  -> em1
OPT1 -> em2
OPT2 -> em3
OPT3 -> em4
OPT4 -> em5

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

4. choose **2**

```
Writing configuration...done.
One moment while the settings are reloading... done!
VMware Virtual Machine - Netgate Device ID: ff76e9de68b254200249

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

 WAN (wan)       -> em0        -> v4/DHCP4: 192.168.114.131/24
 LAN (lan)       -> em1        -> v4: 192.168.1.1/24
 OPT1 (opt1)     -> em2        ->
 OPT2 (opt2)     -> em3        ->
 OPT3 (opt3)     -> em4        ->
 OPT4 (opt4)     -> em5        ->

 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: 2
```

5. First set interface **2 - LAN**

```
1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static)
3 - OPT1 (em2)
4 - OPT2 (em3)
5 - OPT3 (em4)
6 - OPT4 (em5)

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:
> 192.168.1.254

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:
>
```

Enable webConfigurator protocol to access this firewall through browser

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

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

Do you want to enable the DHCP server on LAN? (y/n) y
Enter the start address of the IPv4 client address range: 192.168.1.1
Enter the end address of the IPv4 client address range: 192.168.1.253
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... S

The IPv4 LAN address has been set to 192.168.1.254/24
You can now access the webConfigurator by opening the following URL in your web
browser:
                http://192.168.1.254/

Press <ENTER> to continue.
```

6. Same way to set interface IP Address for OPT2(em3), OPT3(em4), OPT4(em5), the reason to skip OPT1(em2) is because interface em2 is to receive logs via SPAN port
7. **OPT2(em3)**

```
1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static)
3 - OPT1 (em2)
4 - OPT2 (em3)
5 - OPT3 (em4)
6 - OPT4 (em5)

Enter the number of the interface you wish to configure: 4

Configure IPv4 address OPT2 interface via DHCP? (y/n) n

Enter the new OPT2 IPv4 address.  Press <ENTER> for none:
> 192.168.3.254

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 OPT2 IPv4 subnet bit count (1 to 32):
> 24

For a WAN, enter the new OPT2 IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>
```

```
Configure IPv4 address OPT2 interface via DHCP? (y/n) n

Enter the new OPT2 IPv4 address.  Press <ENTER> for none:
> 192.168.3.254

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 OPT2 IPv4 subnet bit count (1 to 32):
> 24

For a WAN, enter the new OPT2 IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Configure IPv6 address OPT2 interface via DHCP6? (y/n) n

Enter the new OPT2 IPv6 address.  Press <ENTER> for none:
>

Do you want to enable the DHCP server on OPT2? (y/n) y
Enter the start address of the IPv4 client address range: 192.168.3.1
Enter the end address of the IPv4 client address range: 192.168.3.253
```

8. **OPT3(em4)**

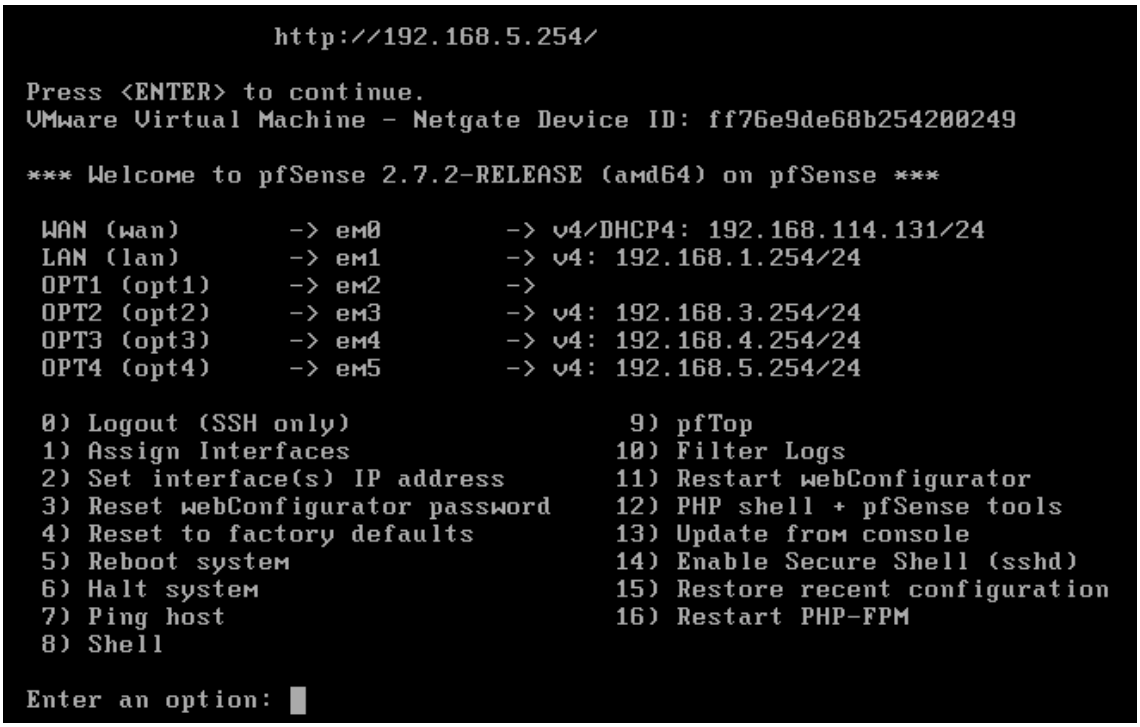
```
Configure IPv4 address OPT3 interface via DHCP? (y/n) n

Enter the new OPT3 IPv4 address.  Press <ENTER> for none:
> 192.168.4.254

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 OPT3 IPv4 subnet bit count (1 to 32):
> 24

For a WAN, enter the new OPT3 IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Configure IPv6 address OPT3 interface via DHCP6? (y/n) n

Enter the new OPT3 IPv6 address.  Press <ENTER> for none:
>

Do you want to enable the DHCP server on OPT3? (y/n) y
Enter the start address of the IPv4 client address range: 192.168.4.1
Enter the end address of the IPv4 client address range: 192.168.4.253
```

```
>

Configure IPv6 address OPT3 interface via DHCP6? (y/n) n

Enter the new OPT3 IPv6 address.  Press <ENTER> for none:
>

Do you want to enable the DHCP server on OPT3? (y/n) y
Enter the start address of the IPv4 client address range: 192.168.4.1
Enter the end address of the IPv4 client address range: 192.168.4.253
Disabling IPv6 DHCPD...

Please wait while the changes are saved to OPT3...[fib_algo] inet.0 (bsearch4#26
) rebuild_fd_flm: switching algo to radix4_lockless

 Reloading filter...
 Reloading routing configuration...
 DHCPD...

The IPv4 OPT3 address has been set to 192.168.4.254/24
You can now access the webConfigurator by opening the following URL in your web
browser:
                http://192.168.4.254/

Press <ENTER> to continue.
```

9. **OPT4(em5)**

```
Configure IPv4 address OPT4 interface via DHCP? (y/n) n

Enter the new OPT4 IPv4 address.  Press <ENTER> for none:
> 192.168.5.254

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 OPT4 IPv4 subnet bit count (1 to 32):
> 24

For a WAN, enter the new OPT4 IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Configure IPv6 address OPT4 interface via DHCP6? (y/n) n

Enter the new OPT4 IPv6 address.  Press <ENTER> for none:
>

Do you want to enable the DHCP server on OPT4? (y/n) y
Enter the start address of the IPv4 client address range: 192.168.5.1
Enter the end address of the IPv4 client address range: 192.168.5.253
```

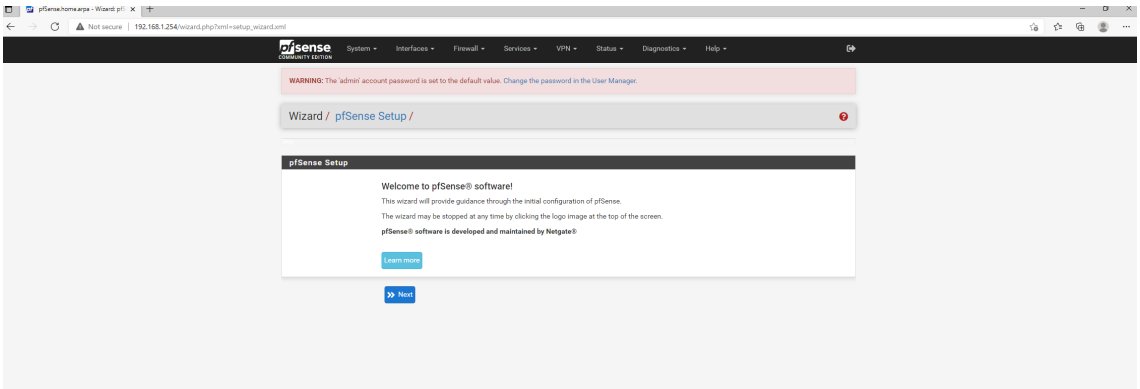
10. em0 is the WAN adapter with IP received via DHCP, em1 is the LAN adapter with IP 192.168.1.254, then leave em2 which is on SPAN Port it will be configured as a span port to allow us to monitor traffic using security onion. em3 which is on KALI will be assigned IP 192.168.4.254, em4 which is on Security Onion will be assigned 192.168.4.254 IP Address and finally em5 which will be connected to Splunk and IP Address will be assigned 192.168.5.254.



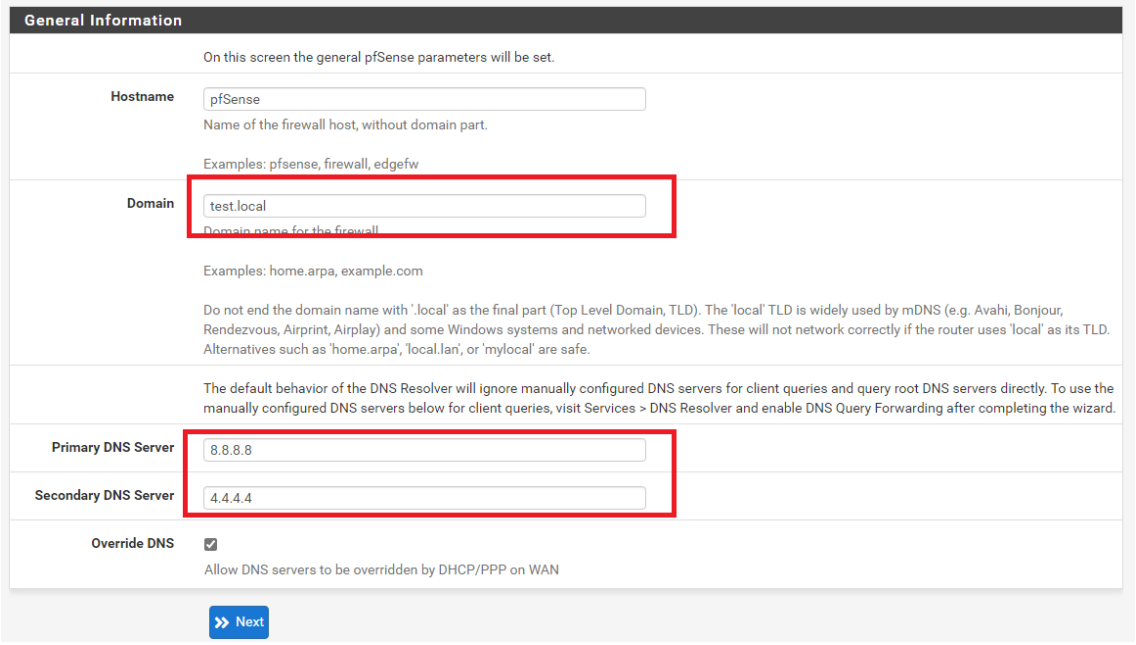
PfSense Firewall Configuration

Windows 10 is connected to PfSense Interface LAN(em1), so now can use Windows 10 to access the PfSense web portal via the link: http://192.168.1.254, default username is **admin**, default password is **pfsense**

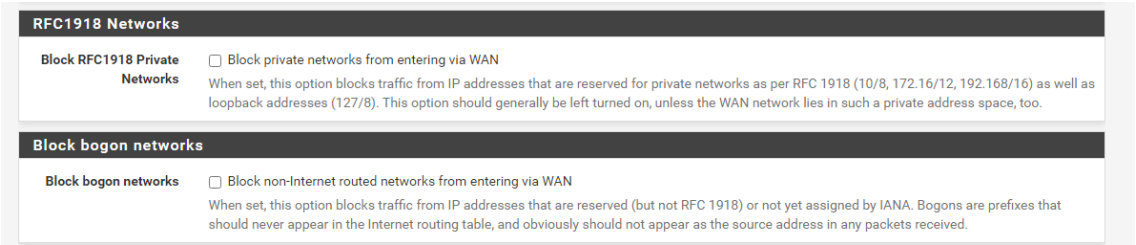
1. pfSense Setup



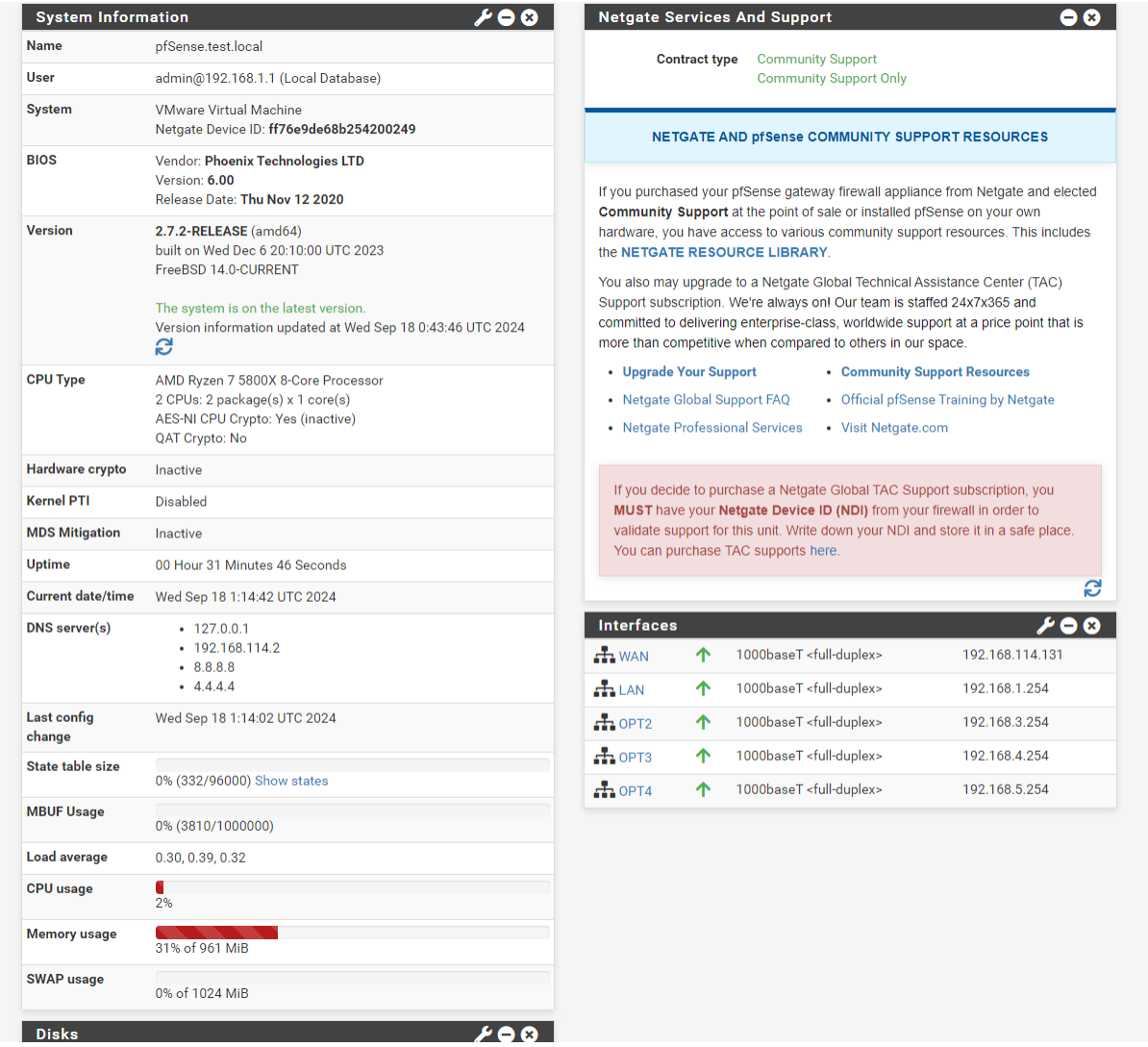
Here, if change domain name to others, has to remember it, cuz this domain name will be used afterwards.



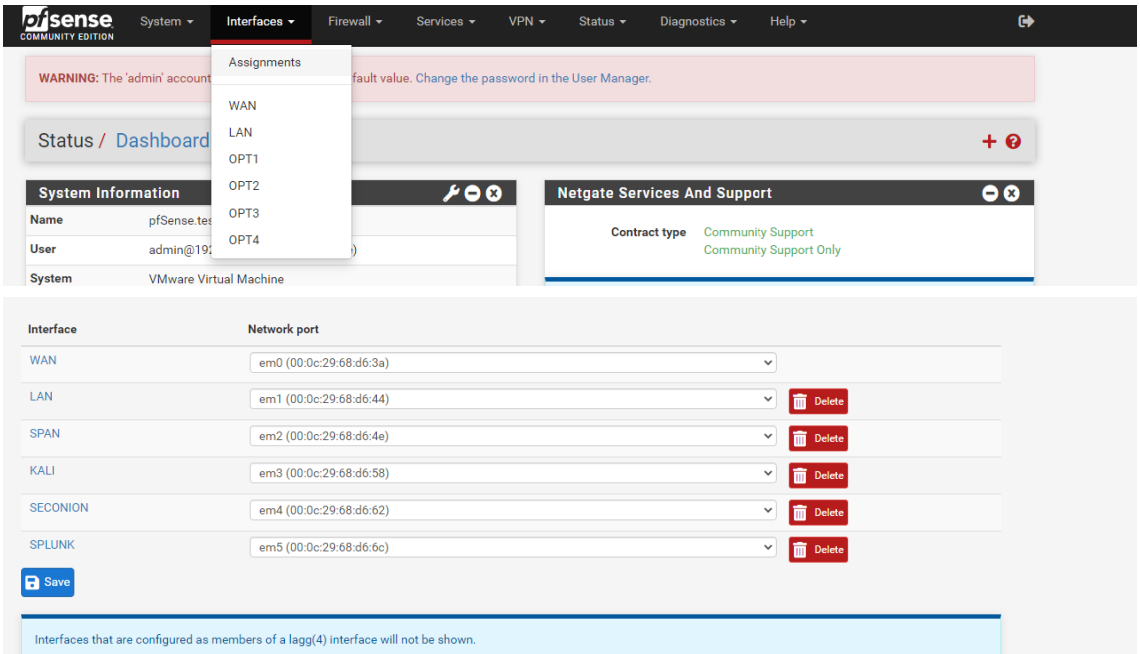
At step 4, uncheck **Block RFC1918 Private Networks** and **Block bogon Networks** options



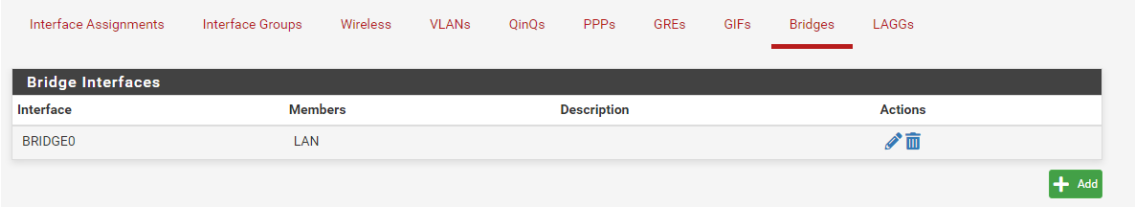
At step 6, no need to change default password. After all done, here is what it should looks like

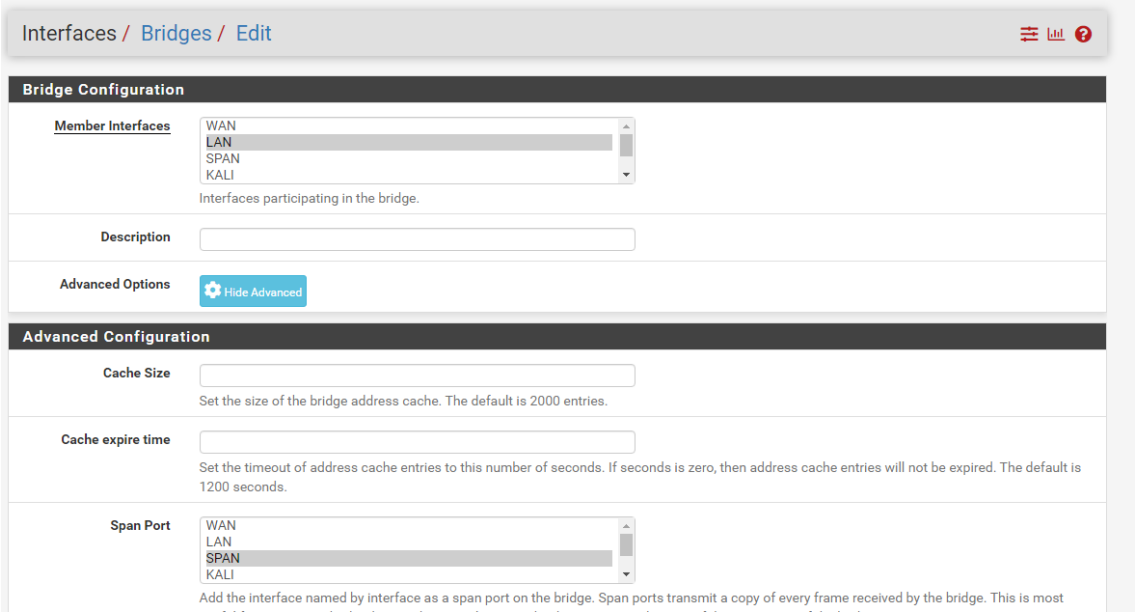


2. Navigate to Interfaces -> Assignments, enable Interfaces for OPT1, OPT2, OPT3, OPT4, and then rename

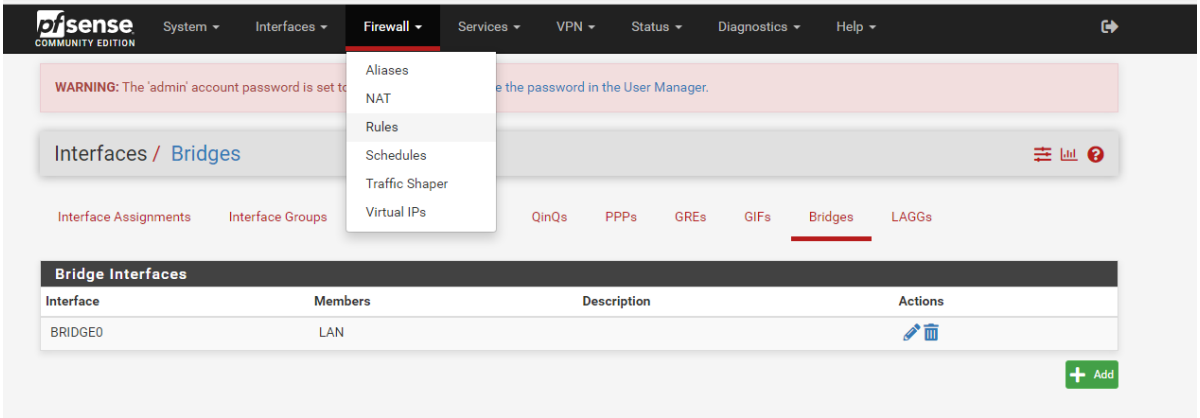


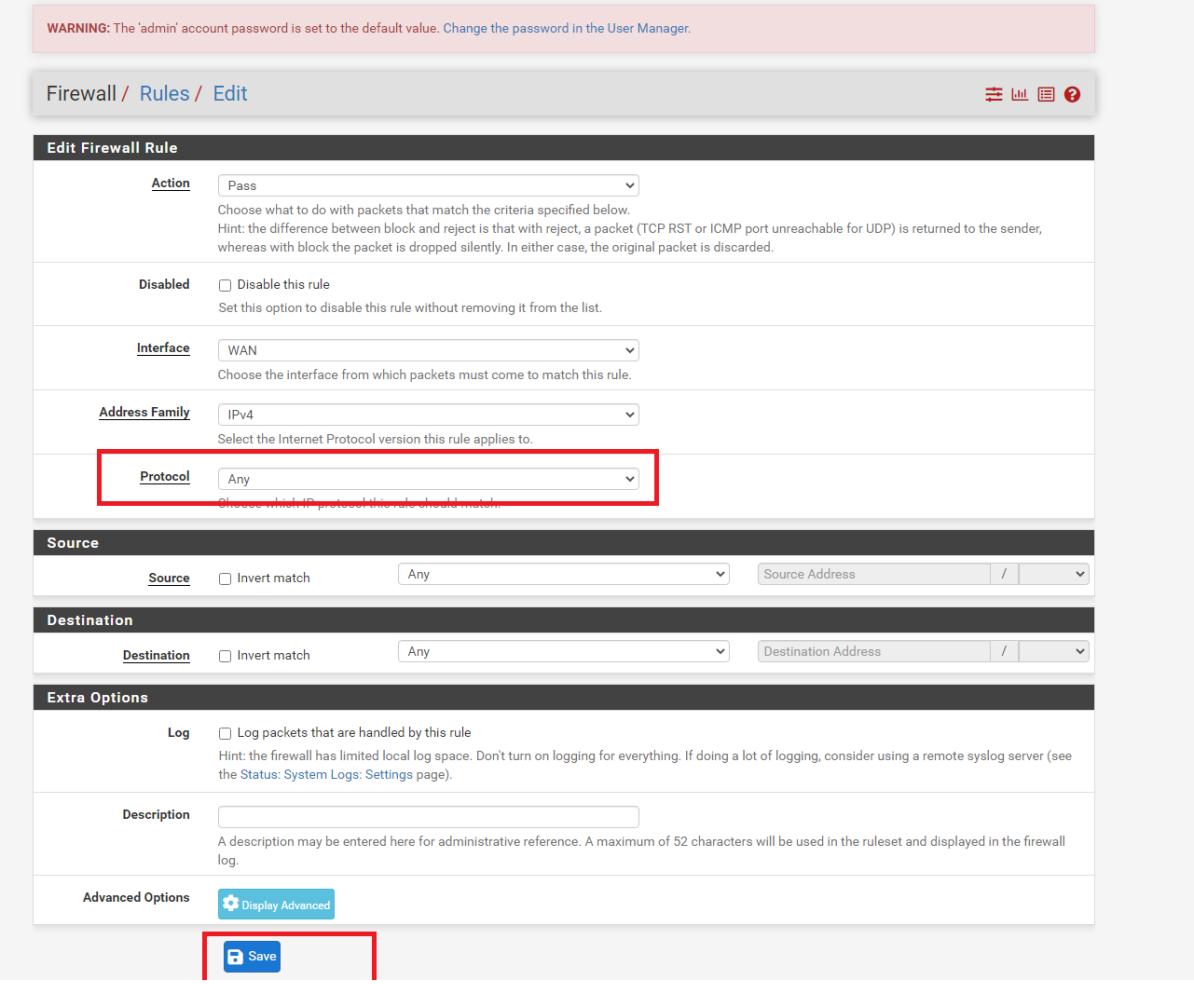
3. Go to Bridges-> Add, this step is to configure LAN traffic copy that will be forwarded to SPAN.



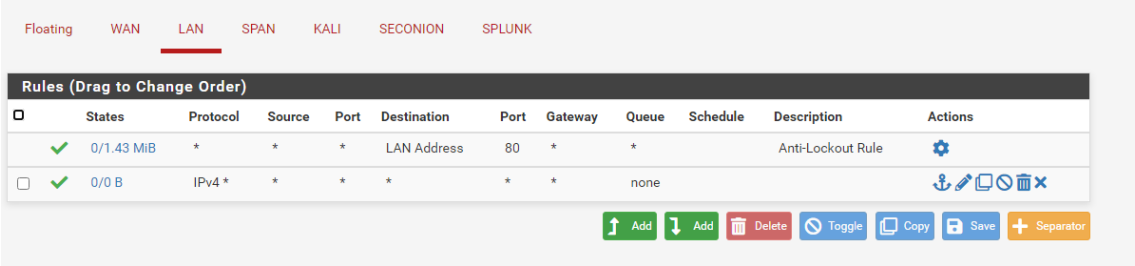


4. Navigate to Firewall->Rules, under WAN, select Add, select Protocol to **Any**





5. Go to LAN, delete two rules and create a same rule as WAN



6. For SPAN, KALI, SECONION, SPLUNK, do same as WAN, don't forget **Apply Changes**