

# PfSense Firewall initial configuration

The PfSense firewall rebooted press 1 to create the interface mappings. It will show us the valid interface available and then ask the prompt should VLANs be set up no type n.

- 1- Assign interface
- 2- Set interface's ip address
- 3- Reset webconfiguration password
- 4- And more option to 16.

```
➡ 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: 1

Valid interfaces are:

em0      00:0c:29:3b:d0:9c  (up) Intel(R) Legacy PRO/1000 MT 82545EM (Copper)
em1      00:0c:29:3b:d0:a6  (up) Intel(R) Legacy PRO/1000 MT 82545EM (Copper)
em2      00:0c:29:3b:d0:b8  (down) Intel(R) Legacy PRO/1000 MT 82545EM (Copper)
em3      00:0c:29:3b:d0:ba  (down) Intel(R) Legacy PRO/1000 MT 82545EM (Copper)
em4      00:0c:29:3b:d0:c4  (down) Intel(R) Legacy PRO/1000 MT 82545EM (Copper)
```

First I want to Assign Interface by using option 1.

```
Enter an option: 1

Valid interfaces are:

em0      00:0c:29:8c:21:9a  (up) Intel(R) Legacy PRO/1000 MT 82545EM (Copper)
em1      00:0c:29:8c:21:a4  (up) Intel(R) Legacy PRO/1000 MT 82545EM (Copper)
em2      00:0c:29:8c:21:ae  (down) Intel(R) Legacy PRO/1000 MT 82545EM (Copper)
em3      00:0c:29:8c:21:b8  (down) Intel(R) Legacy PRO/1000 MT 82545EM (Copper)
em4      00:0c:29:8c:21:c2  (down) Intel(R) Legacy PRO/1000 MT 82545EM (Copper)
em5      00:0c:29:8c:21:cc  (down) Intel(R) Legacy PRO/1000 MT 82545EM (Copper)

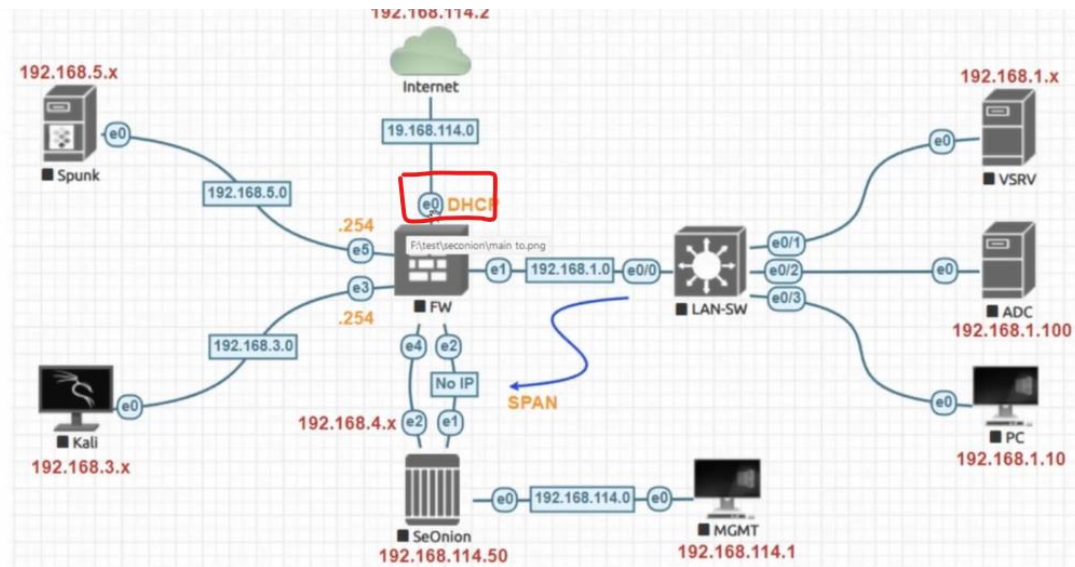
Do VLANs need to be set up first?
If VLANs will not be used, or only for optional interfaces, it is typical to
say no here and use the webConfigurator to configure VLANs later, if required.

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 em3 em4 em5 or a): em0
```

For the first interface which I want to configure at WAN as per lab set up idea.



Then also assign other interfaces that we will added during installation.

Assign second **em1** interface to **LAN** as per lab set up.

Other interface currently set as default option 1-3 that will set later.

```
(em1 em2 em3 em4 em5 a or nothing if finished): em1 → LAN
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]? y
```

After entering **y** and hitting enter, the process start and done after some time.

As it done, it will take to you start menu where options will display.

```
Writing configuration...done.
One moment while the settings are reloading... done!
VMware Virtual Machine - Netgate Device ID: e9065282468a8ced28f4

*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.114.149/24
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: 
```

Now the first step **assign interface** will **complete**.

**Move to next step now (set interface(s) IP Address)**

Select the option 2 and hit enter.

In this step, we will set up static ip to interfaces that I selected for lab setup.

IP Subnet	Network Connection	Role	PfSense Interfaces	VMware Adopter
192.168.114.0/24	NAT	WAN	EM0	Network Adopter
192.168.1.0/24	VMNet2	LAN	EM1	Network Adopter 2
No IP Address	VMNet3	SPAN	EM2	Network Adopter 3
192.168.3.0/24	VMNet4	KALI	EM3	Network Adopter 4
192.168.4.0/24	VMNet5	SECONION	EM4	Network Adopter 5
192.168.5.0/24	VMNet6	SPLUNK	EM5	Network Adopter 6

So we select the second option it will display interfaces as like show below.

Their first interface (WAN) have correct ip address but the second interface have ip address not as like our lab idea.

So we will change it.

Enter the number of em1 is **2** the hit enter.

Select ipv4 address and the subnet that is **24**.

```

8) Shell

Enter an option: 2

Available interfaces:

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

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):
>

```

Enter the subnet mask.

Enter the gateway but not needed here so press enter.

No need to set ipv6.

Enable DHCP server and set ip range start from 192.168.1.1 to 192.168.1.253.

Enable the HTTP server also and press enter.

```

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:
>

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...

```

It will complete the setup and then press enter.

First interface setup complete, other will also do as like this do that.

```

http://192.168.1.254/

Press <ENTER> to continue.
VMware Virtual Machine - Netgate Device ID: e9065282468a8ced28f4

*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.114.149/24
LAN (lan)      -> em1      -> v4: 192.168.1.254/24
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: █

```

All other interface also configure as like above.

But interface **em2** have no ip address as per lab set up.

```

The IPv4 OPT4 address has been set to 192.168.5.254/24

Press <ENTER> to continue.
VMware Virtual Machine - Netgate Device ID: e9065282468a8ced28f4

*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.114.149/24 ✓
LAN (lan)      -> em1      -> v4: 192.168.1.254/24 ✓
OPT1 (opt1)    -> em2      ->
OPT2 (opt2)    -> em3      -> v4: 192.168.3.254/24 ✓
OPT3 (opt3)    -> em4      -> v4: 192.168.4.254/24 ✓
OPT4 (opt4)    -> em5      -> v4: 192.168.5.254/24 ✓

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: █

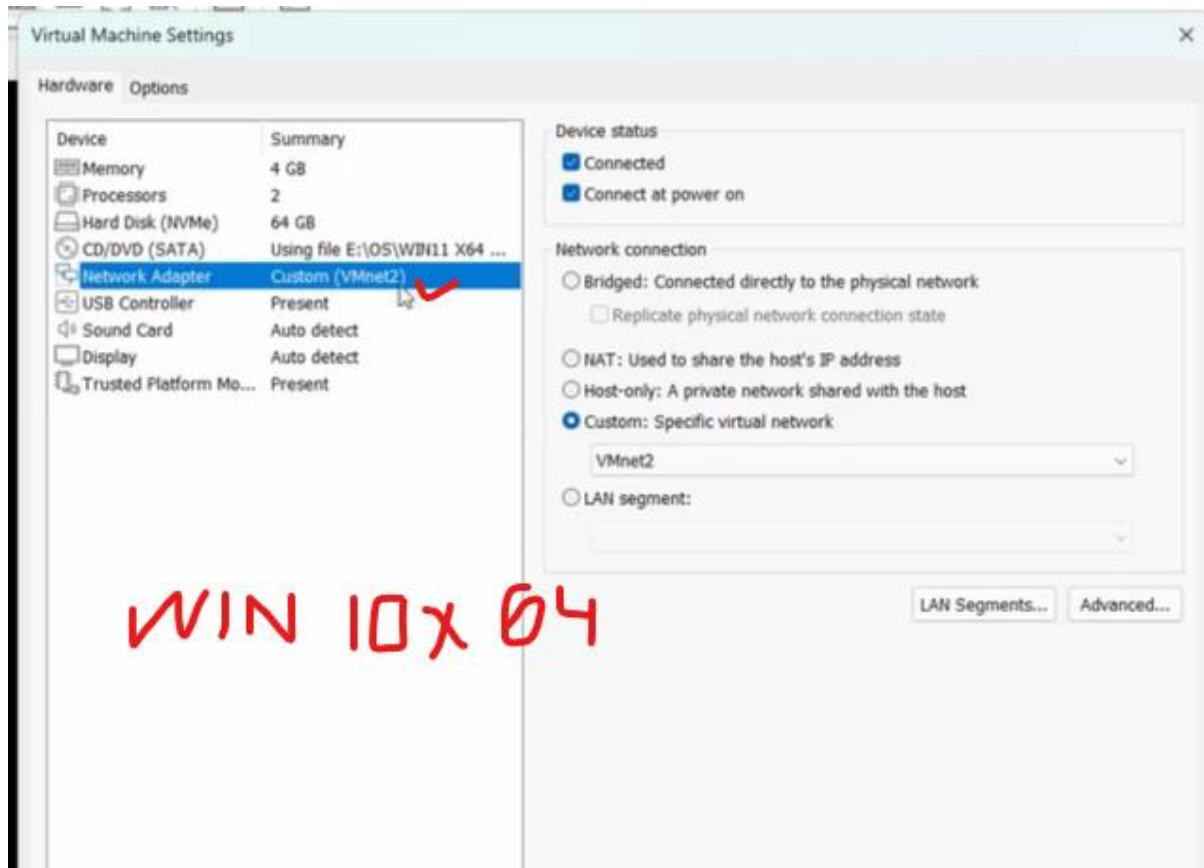
```

Now these 2 steps will complete.



### PfSense firewall configuration:

Next to create a firewall rule and naming the interface also to create bridge port. To further configure pfsense we need to access it through the web configuration at through IP address. However, we need a machine to do this from. We will use windows 10 LAN PC administrate Pfsense firewall from. Let's change Network adapter to VMnet2 LAN.

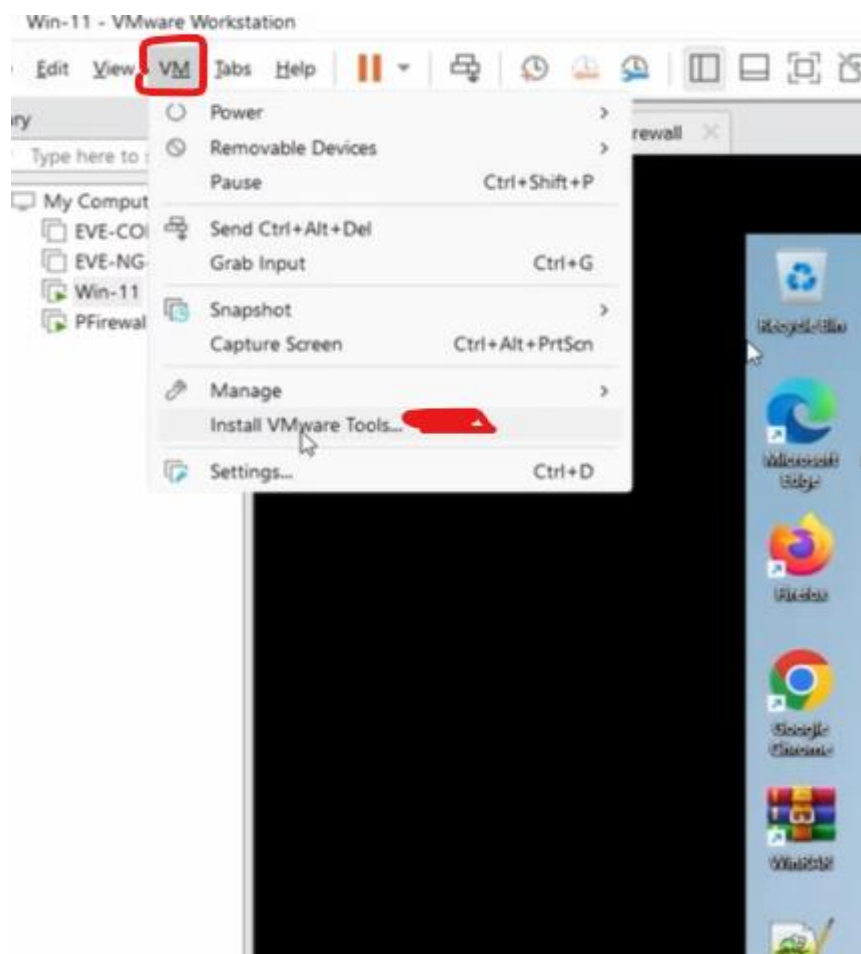


Window size is small of win 10. So, install drive to set it.



Click on VM and select install VMware Tools.

It will automatic and give full view.



If it not run automatic then go to DVD and run it manually.

The file name is **setup64** .

When it is finish then it give full screen view and also allow copy and paste.

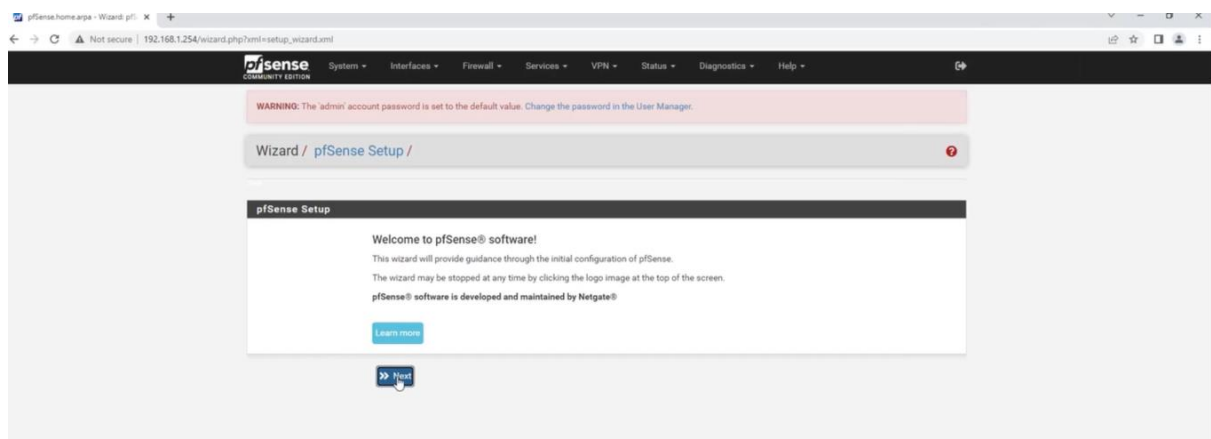
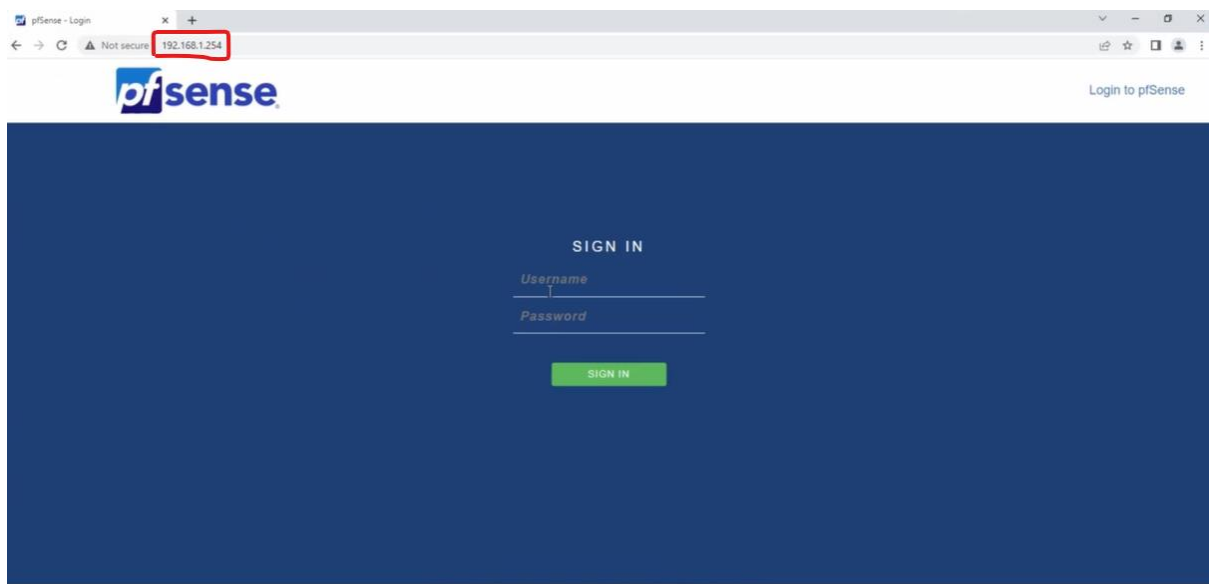
- After this check that window will get the ip from range that I selected.
- Also disable the ipv6 and also disable the firewall form window to run the firewall properly.

Now we want to access the firewall graphically form window for further configuration.

Enter the ip of LAN that assign to LAN interface in firewall, in the browser and enter.

The graphical view open on screen.

The **username** is **admin** and **password** is **pfsense** .



The firewall is open.

Here do next and then also next.



The screenshot shows the pfSense Setup Wizard at Step 2 of 9, titled "General Information". At the top, a warning message states: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." The breadcrumb trail is "Wizard / pfSense Setup / General Information". Below the title bar, a progress indicator shows "Step 2 of 9". The main section is titled "General Information" and contains the following fields:

- Hostname:** "pfSense" (with a red checkmark). Example: myserver.
- Domain:** "home.arpa" (with a red checkmark). Example: mydomain.com.
- Primary DNS Server:** "8.8.8.8" (with a red checkmark).
- Secondary DNS Server:** "1.1.1.1" (with a red checkmark).
- Override DNS:** A checked checkbox with the text "Allow DNS servers to be overridden by DHCP/PPP on WAN".

At the bottom of the form is a blue button labeled "Next".

Here set the **hostname** , **domain** **DNS server**.

Then hit next.

Time span will occur if you want to change it do.

The screenshot shows the pfSense Setup Wizard at Step 3 of 9, titled "Time Server Information". The breadcrumb trail is "Wizard / pfSense Setup / Time Server Information". Below the title bar, a progress indicator shows "Step 3 of 9". The main section is titled "Time Server Information" and contains the following fields:

- Time server hostname:** "pfsense.pool.ntp.org" (with a red checkmark). Below the field is the text "Enter the hostname (FQDN) of the time server."
- Timezone:** A dropdown menu showing "Etc/UTC".

At the bottom of the form is a blue button labeled "Next".

Hit next.

Then in next step enable the DHCP and **uncheck** the two options that shown blow:

Uncheck is necessary at WAN because at WAN have no private ip.

If no qualifying outgoing packets are transmitted for the specified number of seconds, the connection is brought down. An idle timeout of zero disables this feature.

### RFC1918 Networks

**Block RFC1918 Private Networks** ☒ Block private networks from entering via WAN  
When set, this option blocks traffic from IP addresses that are reserved for private networks as per RFC 1918 (10/8, 172.16/12, 192.168/16) as well as loopback addresses (127/8). This option should generally be left turned on, unless the WAN network lies in such a private address space, too.

### Block bogon networks

**Block bogon networks** ☒ Block non-Internet routed networks from entering via WAN  
When set, this option blocks traffic from IP addresses that are reserved (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and obviously should not appear as the source address in any packets received.

[Next](#)

hit next.

Donot change the WAN ip.

**WARNING:** The 'admin' account password is set to the default value. Change the password in the User Manager.

## Wizard / pfSense Setup / Configure LAN Interface

Step 5 of 9

### Configure LAN Interface

On this screen the Local Area Network information will be configured.

**LAN IP Address**   
Type dhcp if this interface uses DHCP to obtain its IP address.

**Subnet Mask**

[Next](#)

Hit next.

Change the admin password if you want.

## Wizard / pfSense Setup / Set Admin WebGUI Password

Step 6 of 9

### Set Admin WebGUI Password

On this screen the admin password will be set, which is used to access the WebGUI and also SSH services if enabled.

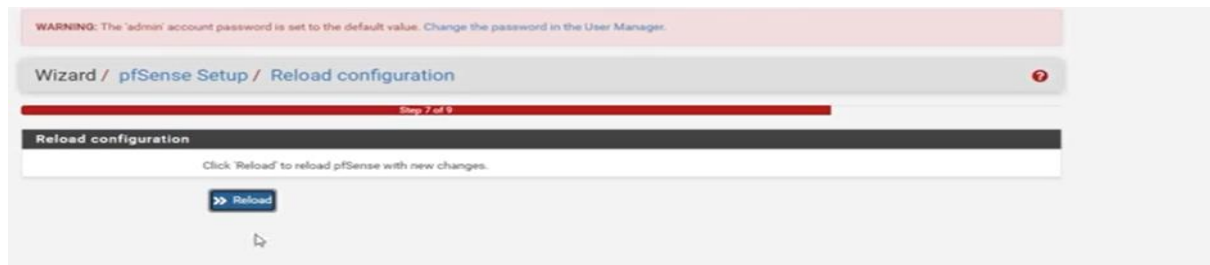
**Admin Password**

**Admin Password AGAIN**

[Next](#)

Hit next.

Then reload .

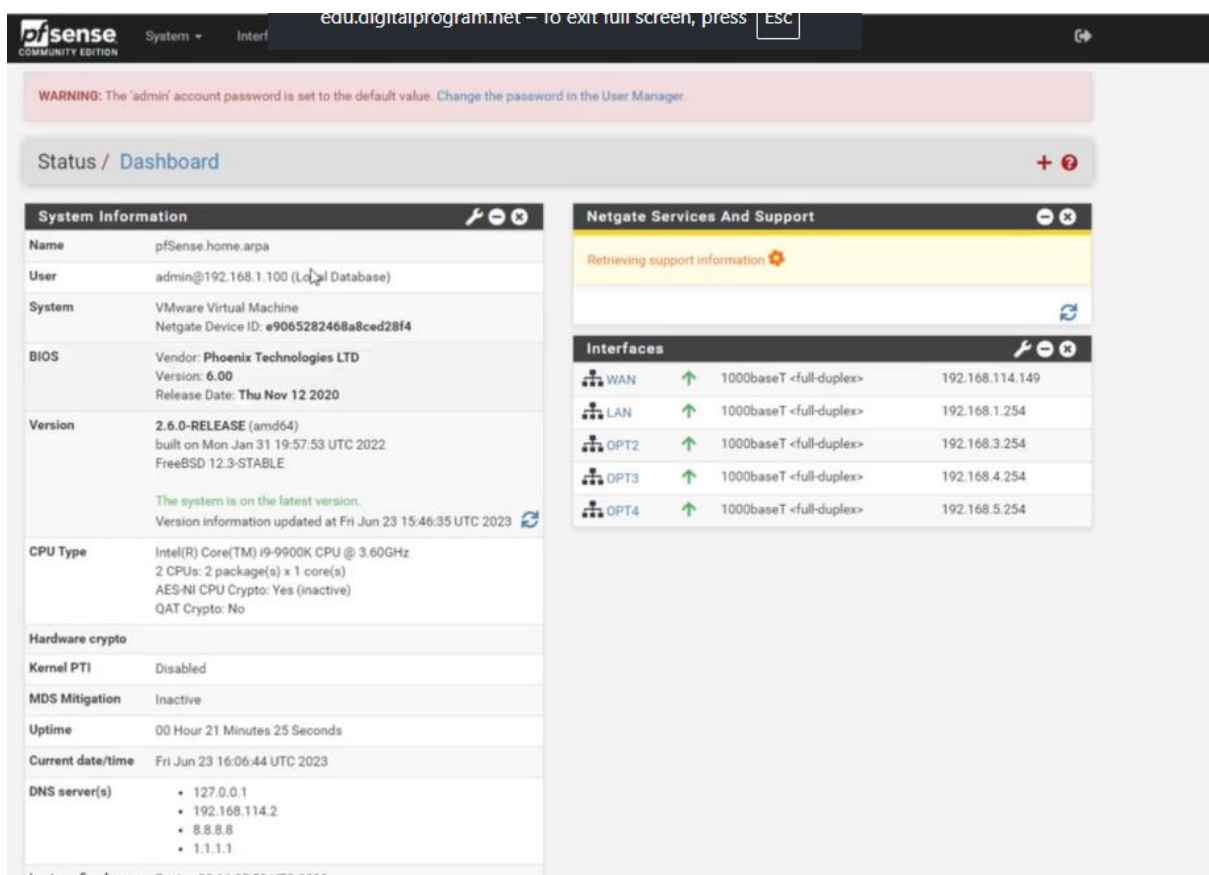


hit reload.

It will complete and in next step it will give option **finish**, hit it.

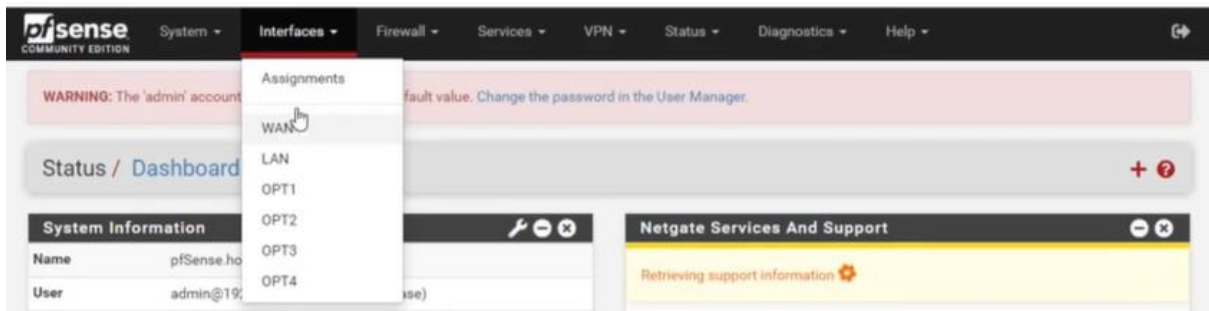
**Accept** the policy.

Then first time firewall will display.



Now we will change the name of interfaces that remains.

Go to **Interface** and select the OPT1 and change it's name and then others same.



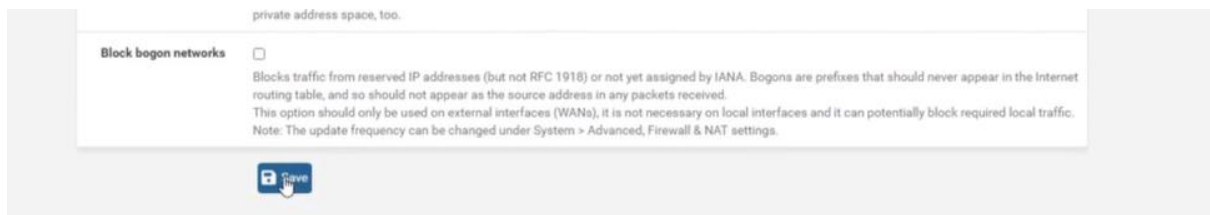
Select interface.

Give name to interfaces as like have name on below table.

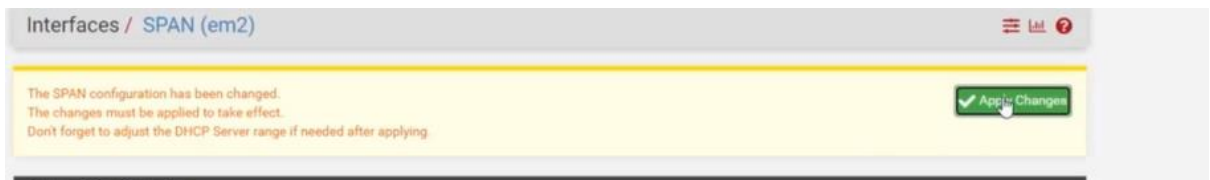
IP Subnet	Network Connection	Role	PfSense Interfaces	VMware Adaptor
192.168.114.0/24	NAT	WAN	EM0	Network Adaptor
192.168.1.0/24	VMNet2	LAN	EM1	Network Adaptor 2
No IP Address	VMNet3	SPAN	EM2	Network Adaptor 3
192.168.3.0/24	VMNet4	KALI	EM3	Network Adaptor 4
192.168.4.0/24	VMNet5	SECONION	EM4	Network Adaptor 5
192.168.5.0/24	VMNet6	SPLUNK	EM5	Network Adaptor 6

After select interface give name to it.

Then scroll down and save it.



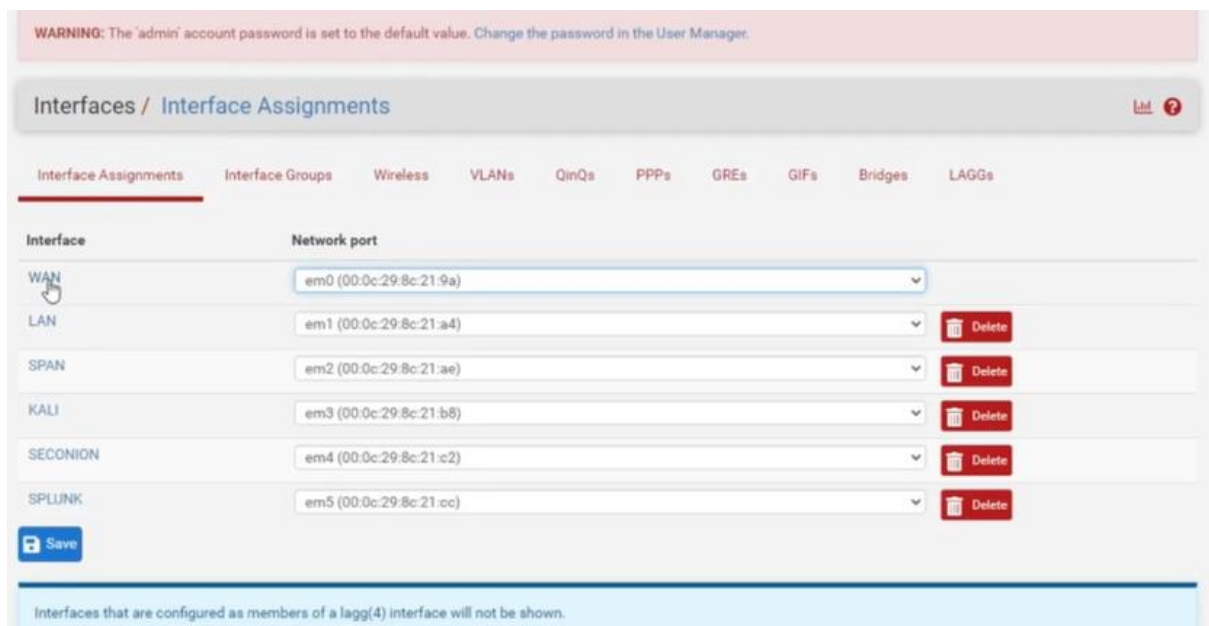
Then confirm the apply change.



First interface name change .

Do the same process for other interfaces. Give name as per lab idea shown in above table.

After it click the interface option that have in header and then assignment. You will see final result.



Interfaces name change successfully.

In firewall side name also change.

```

VMware Virtual Machine - Netgate Device ID: e9065282468a8ced28f4
*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***

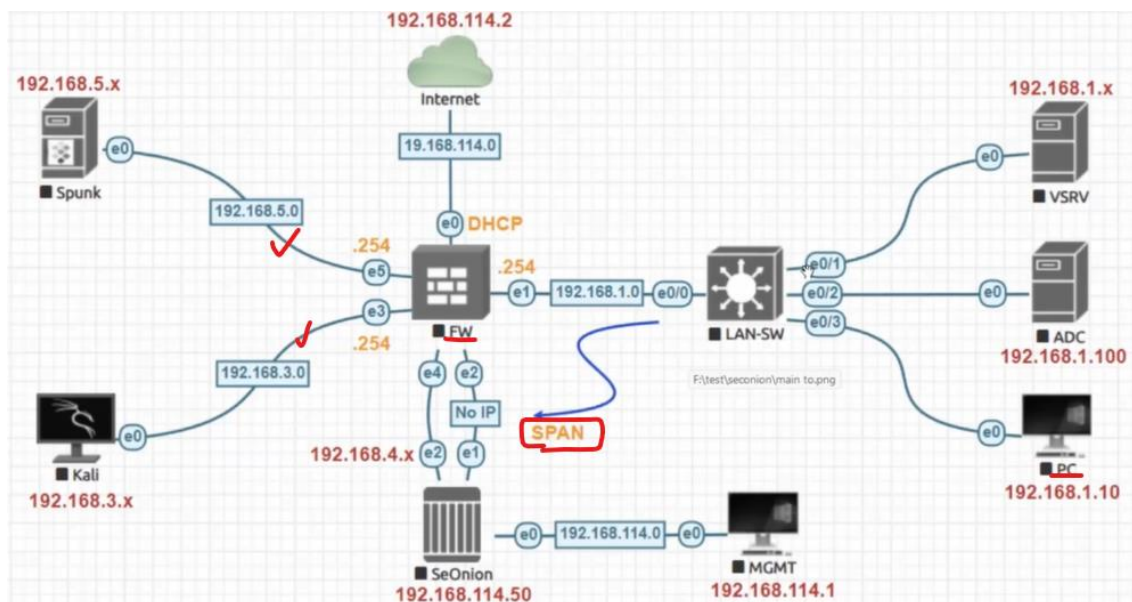
WAN (wan)      -> em0      -> v4/DHCP4: 192.168.114.149/24
LAN (lan)      -> em1      -> v4: 192.168.1.254/24
SPAN (opt1)    -> em2      ->
KALI (opt2)    -> em3      -> v4: 192.168.3.254/24
SECION (opt3)  -> em4      -> v4: 192.168.4.254/24
SPLUNK (opt4)  -> em5      -> v4: 192.168.5.254/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs

```

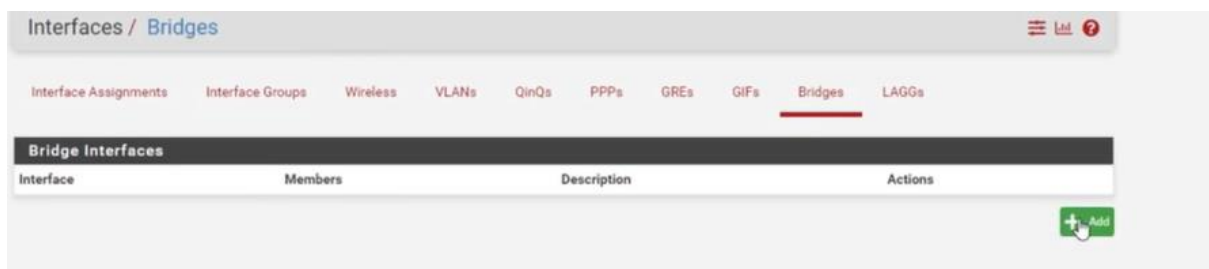
According to topology we will setup the SPAN now.  
so that LAN traffic copy also check by SECURITY ONION.

Now do it. The topology is.



Go to interface and then assignments as like above.

There have a option of BRIDGE select and then hit add to add new setup.



But for this purpose you will first enable the SPAN interface.



Interfaces / SPAN (em2)

### General Configuration

**Enable** ☒ Enable interface

**Description**   
Enter a description (name) for the interface here.

**IPv4 Configuration Type**

**IPv6 Configuration Type**

**MAC Address**   
This field can be used to modify ("spoof") the MAC address of this interface.  
Enter a MAC address in the following format: xxxxxxxxxxxx or leave blank.

**MTU**   
If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.

Then go to bridge and select the **LAN** in member traffic.

Then click advance options.

Then select SPAN in span port.

Interfaces / Bridges / Edit

### Bridge Configuration

**Member Interfaces**   
☒ LAN  
☐ SPAN  
☐ KALI  
Interfaces participating in the bridge.

**Description**

**Advanced Options** ☒ Hide Advanced

### Advanced Configuration

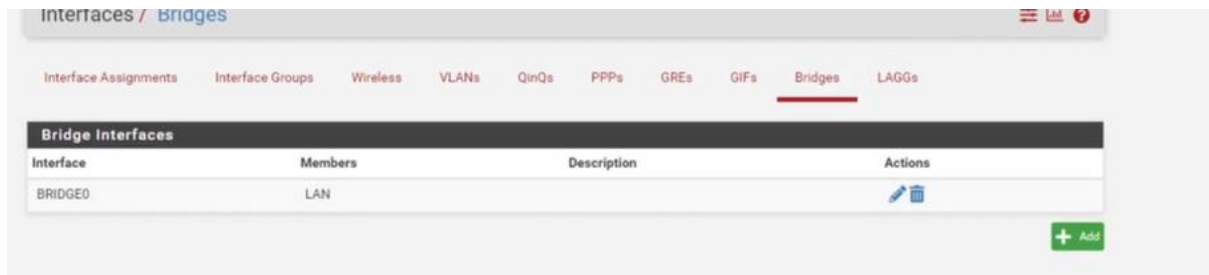
**Cache Size**   
Set the size of the bridge address cache. The default is 2000 entries.

**Cache expire time**   
Set the timeout of address cache entries to this number of seconds. If seconds is zero, then address cache entries will not be expired. The default is 1200 seconds.

**Span Port**   
☒ LAN  
☐ SPAN  
☐ KALI  
Add the interface named by interface as a span port on the bridge. Span ports transmit a copy of every frame received by the bridge. This is most useful for snooping a bridged network passively on another host connected to one of the span ports of the bridge.  
The span interface cannot be part of the bridge member interfaces.

**Edge Ports**   
☐ LAN  
☐ SPAN  
☐ KALI

Then scroll down and save the change.

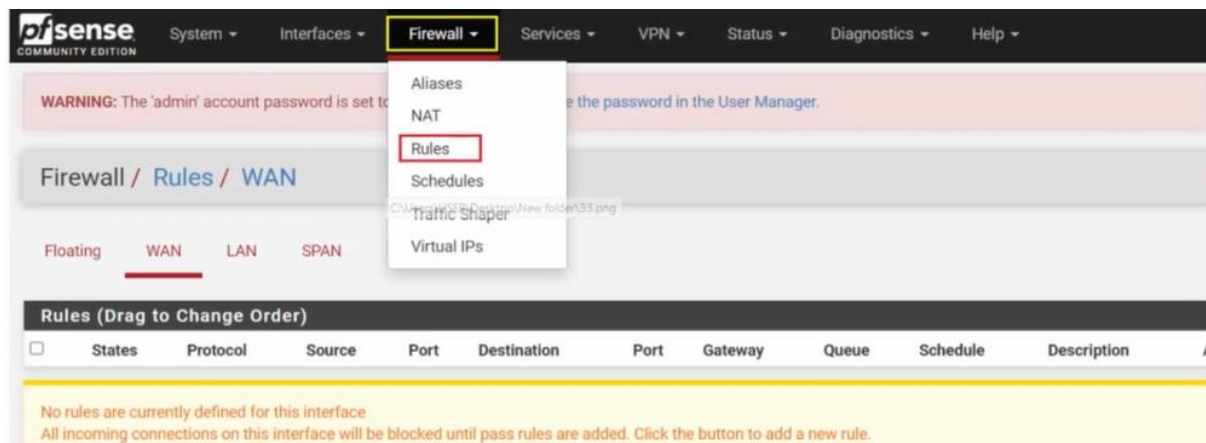


Bridge interface were created.

Create RULES for firewall traffic flow:

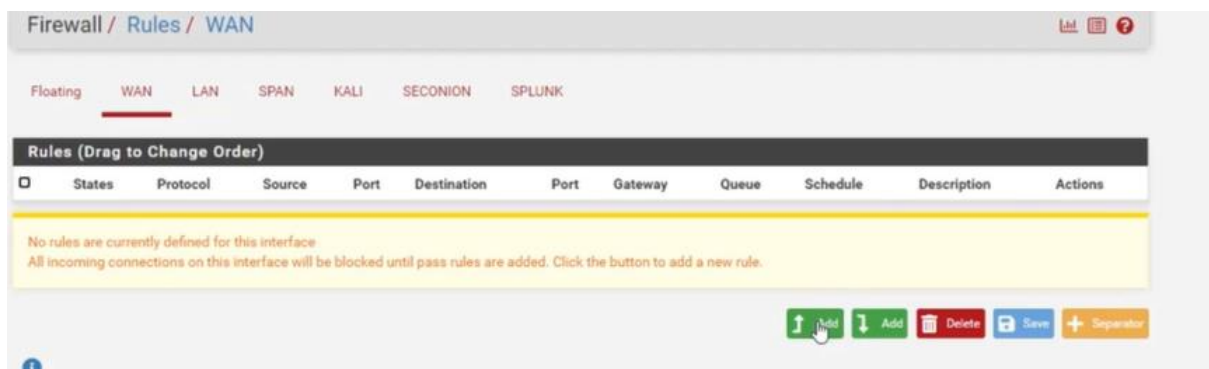
Go to Firewall and then rules.

Rules for that traffic will flow in the network.



So first is WAN , no rule have on WAN.

Click add and add rule.



Their set the ACTION to PASS.

And PROTOCOL to ANY.

Firewall / Rules / Edit

### Edit Firewall Rule

**Action** Pass ✓  
 Choose what to do with packets that match the criteria specified below.  
 Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

**Disabled** ☐ Disable this rule  
 Set this option to disable this rule without removing it from the list.

**Interface** WAN  
 Choose the interface from which packets must come to match this rule.

**Address Family** IPv4  
 Select the Internet Protocol version this rule applies to.

**Protocol** Any ✓  
 Choose which IP protocol this rule should match.

**Source**

Source ☐ Invert match any Source Address /

**Destination**

Destination ☐ Invert match any Destination Address /

Scroll down and save it.

Do same for others.

If LAN have already any rule delete it.

Set rule for ipv4 only.

At end click the apply change.

Now rules will setup .

DHCP SERVER:

Dhcp is configure and if you chack it.

Go to services option and dhcp server , you will see that it will configure.

-----complete-----