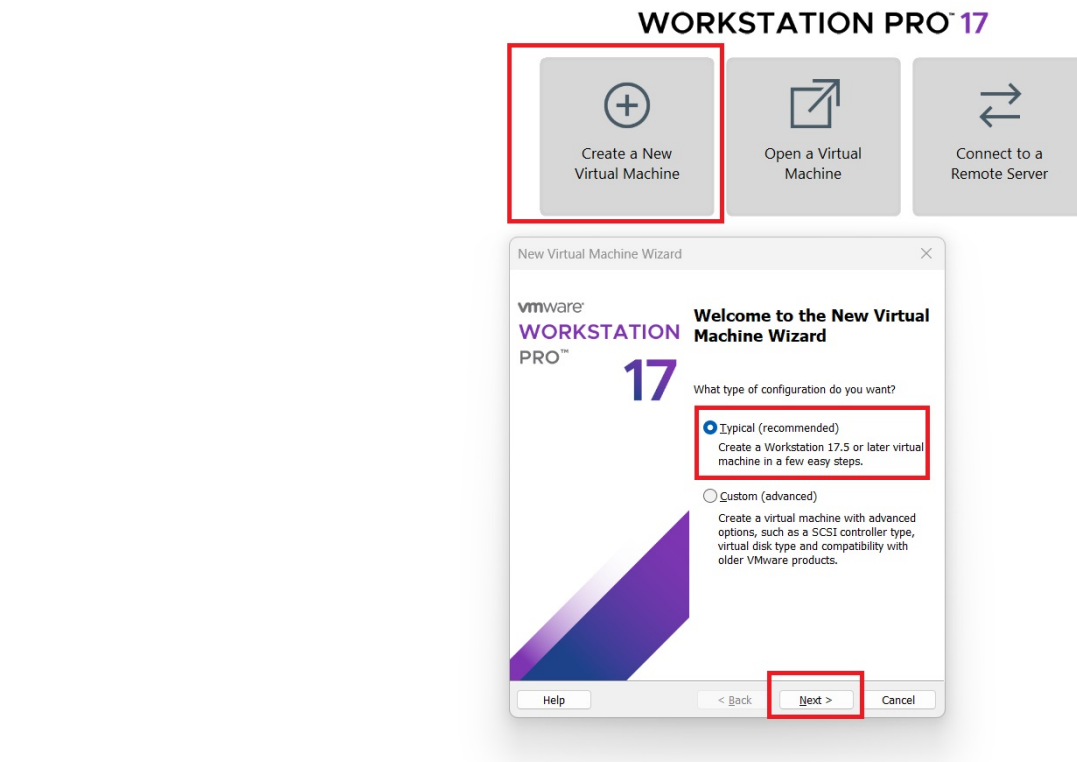


Install PfSense Firewall

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

New Virtual Machine Wizard

Guest Operating System Installation

A virtual machine is like a physical computer; it needs an operating system. How will you install the guest operating system?

Install from:

☐ Installer disc:

No drives available

☒ Installer disc image file (iso):

C:\Others\Splunk_Project\pfSense-CE-2.7.2-RELEASE

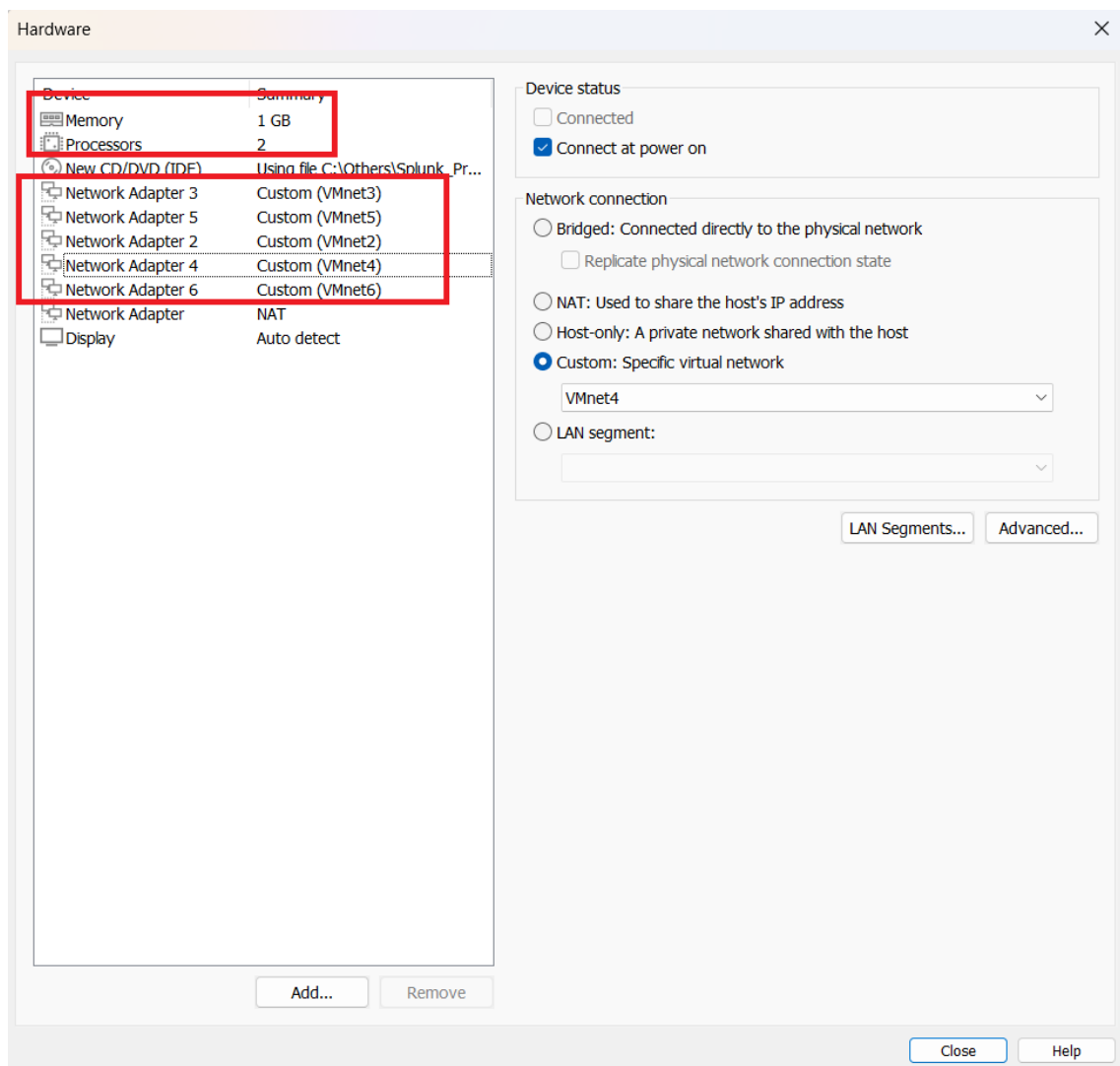
Browse...

☐ I will install the operating system later.

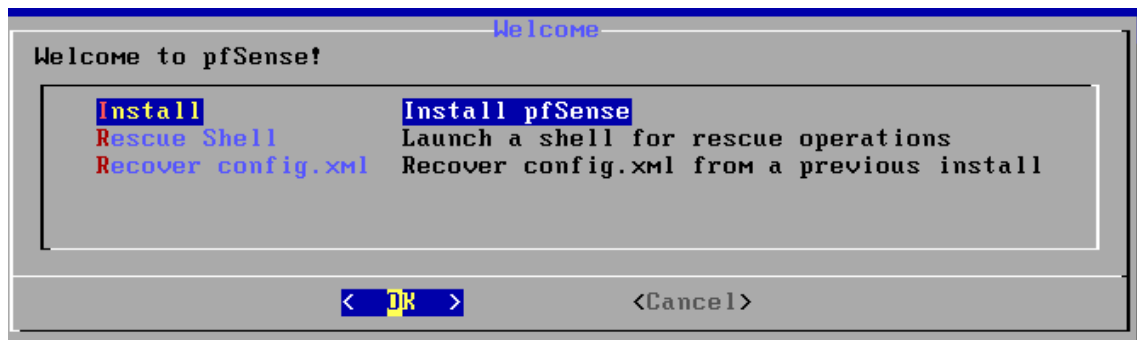
The virtual machine will be created with a blank hard disk.

Help < Back Next > Cancel

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**

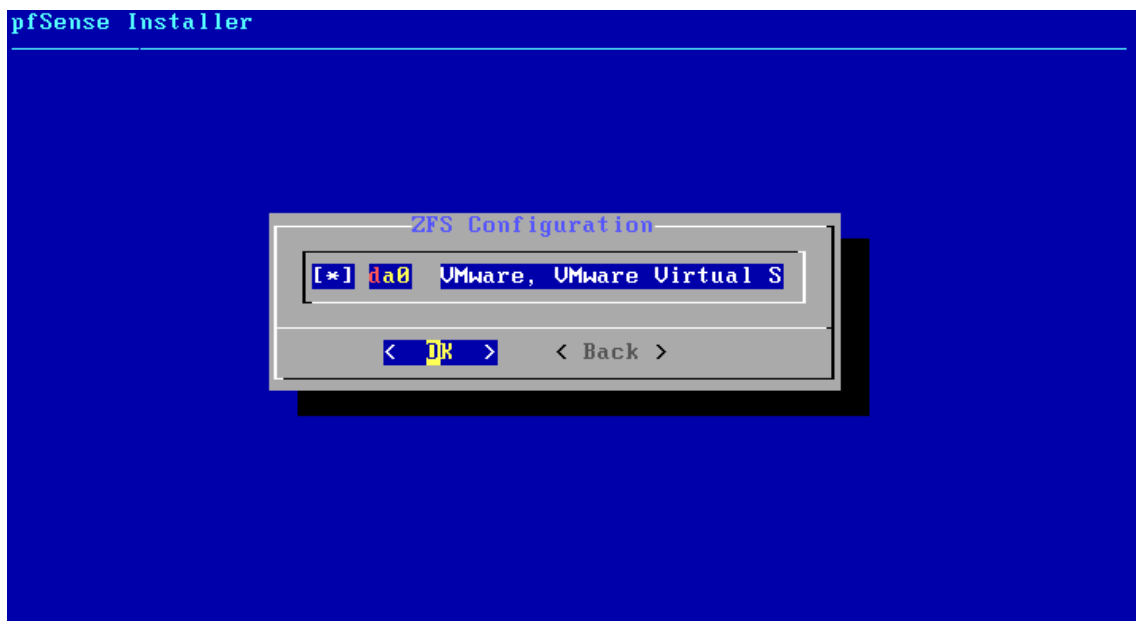


9. Choose **Auto(ZFS)** and **OK**

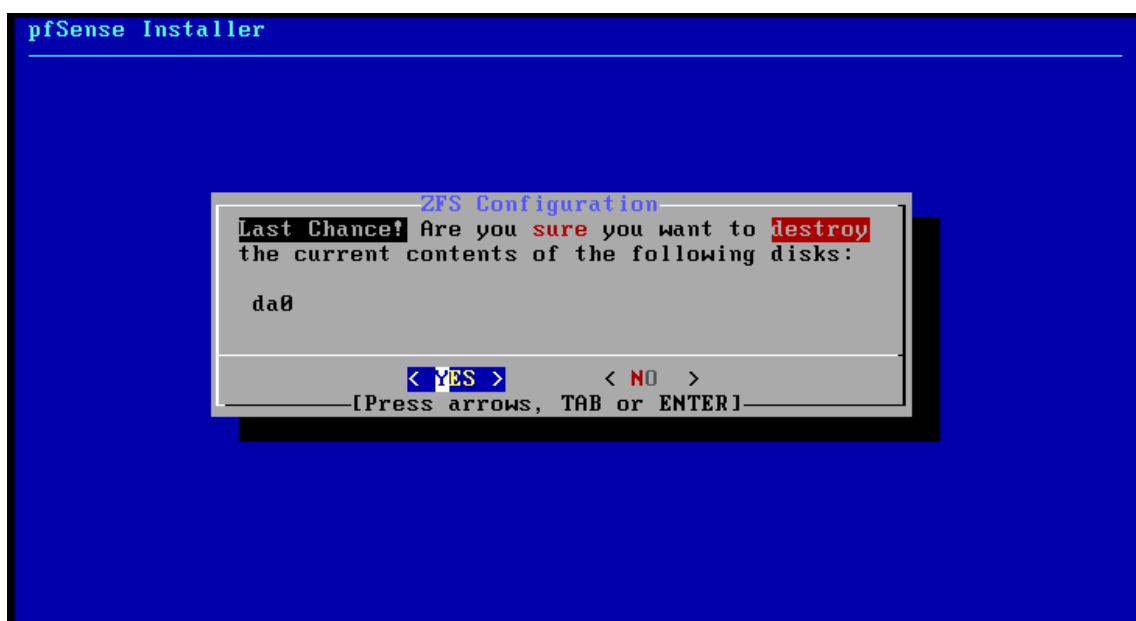
10. Choose **Install** and **OK**

11. Choose the default Stripe with no Redundancy and **OK**

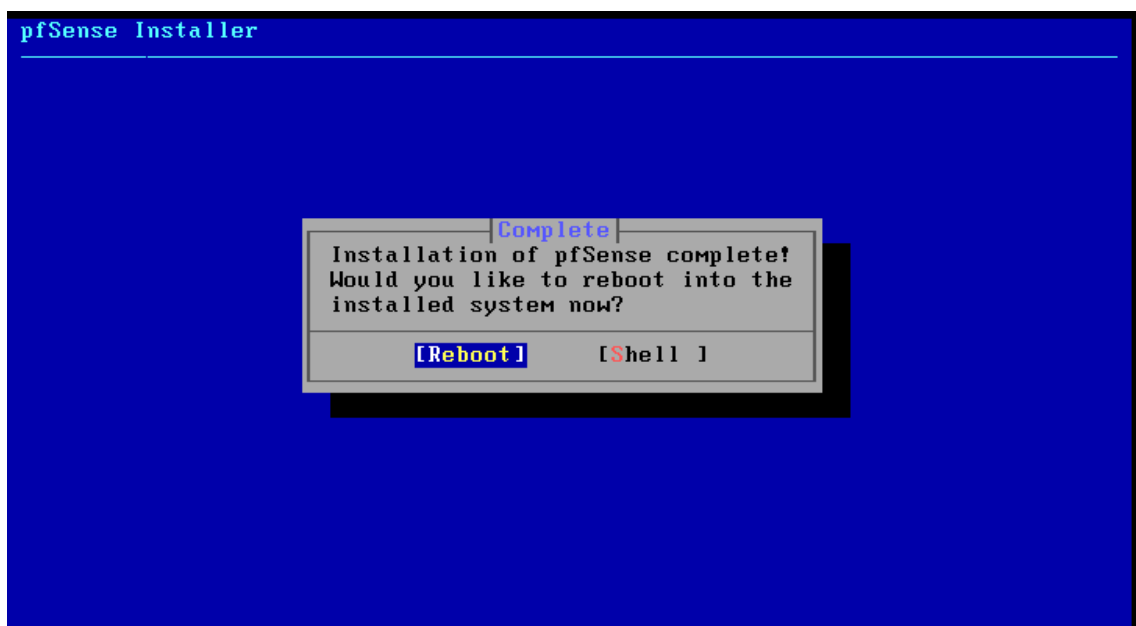
12. Use **Space bar** on your keyboard to choose da0, make sure ***** is shown, and **OK**



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.

```

done.
Starting CRON... done.
pfSense 2.7.2-RELEASE amd64 20231206-2010
Bootup complete

FreeBSD/amd64 (pfSense.home.arp) (ttyv0)

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

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: █

```

PfSense Firewall Initial Configuration

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

1. choose 1

```

done.
Starting CRON... done.
pfSense 2.7.2-RELEASE amd64 20231206-2010
Bootup complete

FreeBSD/amd64 (pfSense.home.arp) (ttyv0)

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

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: 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_algor 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.

```
http://192.168.5.254/

Press <ENTER> to continue.
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: 192.168.1.254/24
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

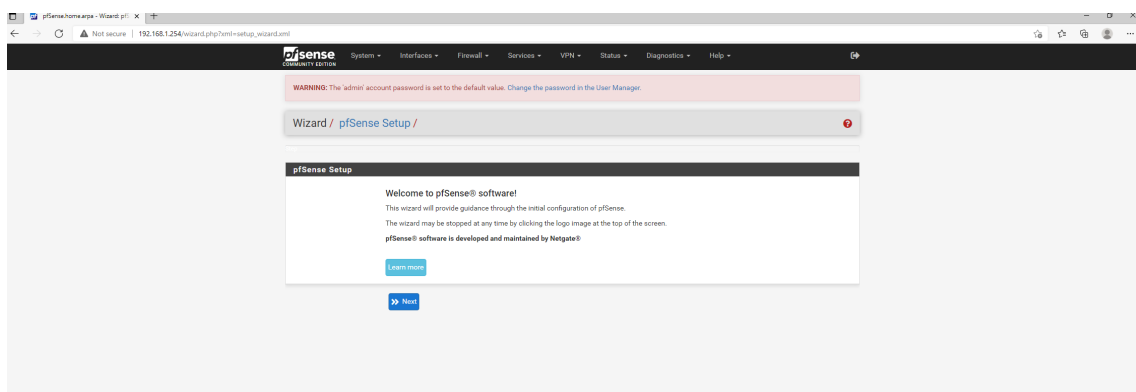
0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password
4) Reset to factory defaults  12) PHP shell + pfSense tools
5) Reboot system             13) Update from console
6) Halt system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

Enter an option: █
```

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



Wizard / pfSense Setup / Netgate® Global Support is available 24/7

Step 1 of 9

Netgate® Global Support is available 24/7

Our 24/7 worldwide team of support engineers are the most qualified to diagnose your issue and resolve it quickly, from on premises to cloud.

We offer several support subscription plans tailored to fit different environment sizes and requirements. Many companies use Netgate support because:

- Support is available 24 hours a day, seven days a week, including holidays.
- Support engineers are located around the world, ensuring that no support call is missed.
- Our support engineers hold many prestigious network engineer certificates and have years of hands-on experience

[Learn more](#)

[Next](#)

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

General Information

On this screen the general pfSense parameters will be set.

Hostname
Name of the firewall host, without domain part.
Examples: pfsense, firewall, edgefw

Domain
Domain name for the firewall
Examples: home.arpa, example.com
Do not end the domain name with '.local' as the final part (Top Level Domain, TLD). The 'local' TLD is widely used by mDNS (e.g. Avahi, Bonjour, Rendezvous, Airprint, Airplay) and some Windows systems and networked devices. These will not network correctly if the router uses 'local' as its TLD. Alternatives such as 'home.arpa', 'local.lan', or 'mylocal' are safe.
The default behavior of the DNS Resolver will ignore manually configured DNS servers for client queries and query root DNS servers directly. To use the manually configured DNS servers below for client queries, visit Services > DNS Resolver and enable DNS Query Forwarding after completing the wizard.

Primary DNS Server

Secondary DNS Server

Override DNS ☒
Allow DNS servers to be overridden by DHCP/PPP on WAN

[Next](#)

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

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.

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

System Information

Name	pfSense.test.local
User	admin@192.168.1.1 (Local Database)
System	VMware Virtual Machine Netgate Device ID: ff76e9de68b254200249
BIOS	Vendor: Phoenix Technologies LTD Version: 6.00 Release Date: Thu Nov 12 2020
Version	2.7.2-RELEASE (amd64) built on Wed Dec 6 20:10:00 UTC 2023 FreeBSD 14.0-CURRENT The system is on the latest version. Version information updated at Wed Sep 18 0:43:46 UTC 2024
CPU Type	AMD Ryzen 7 5800X 8-Core Processor 2 CPUs: 2 package(s) x 1 core(s) AES-NI CPU Crypto: Yes (inactive) QAT Crypto: No
Hardware crypto	Inactive
Kernel PTI	Disabled
MDS Mitigation	Inactive
Uptime	00 Hour 31 Minutes 46 Seconds
Current date/time	Wed Sep 18 1:14:42 UTC 2024
DNS server(s)	<ul style="list-style-type: none"> 127.0.0.1 192.168.114.2 8.8.8.8 4.4.4.4
Last config change	Wed Sep 18 1:14:02 UTC 2024
State table size	0% (332/96000) Show states
MBUF Usage	0% (3810/1000000)
Load average	0.30, 0.39, 0.32
CPU usage	2%
Memory usage	31% of 961 MiB
SWAP usage	0% of 1024 MiB

Disks

Netgate Services And Support

Contract type **Community Support**
Community Support Only

NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES

If you purchased your pfSense gateway firewall appliance from Netgate and elected **Community Support** at the point of sale or installed pfSense on your own hardware, you have access to various community support resources. This includes the [NETGATE RESOURCE LIBRARY](#).

You also may upgrade to a Netgate Global Technical Assistance Center (TAC) Support subscription. We're always on! Our team is staffed 24x7x365 and committed to delivering enterprise-class, worldwide support at a price point that is more than competitive when compared to others in our space.

- Upgrade Your Support
- Community Support Resources
- Netgate Global Support FAQ
- Official pfSense Training by Netgate
- Netgate Professional Services
- Visit Netgate.com

If you decide to purchase a Netgate Global TAC Support subscription, you **MUST** have your **Netgate Device ID (NDI)** from your firewall in order to validate support for this unit. Write down your NDI and store it in a safe place. You can purchase TAC supports [here](#).

Interfaces

WAN	↑	1000baseT <full-duplex>	192.168.114.131
LAN	↑	1000baseT <full-duplex>	192.168.1.254
OPT2	↑	1000baseT <full-duplex>	192.168.3.254
OPT3	↑	1000baseT <full-duplex>	192.168.4.254
OPT4	↑	1000baseT <full-duplex>	192.168.5.254

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

WARNING: The 'admin' account has a default value. Change the password in the User Manager.

Status / Dashboard

System Information

Name	pfSense.test.local
User	admin@192.168.1.1 (Local Database)
System	VMware Virtual Machine

Interfaces

Assignments

- WAN
- LAN
- OPT1
- OPT2
- OPT3
- OPT4

Netgate Services And Support

Contract type **Community Support**
Community Support Only

Interface	Network port	
WAN	em0 (00:0c:29:68:d6:3a)	
LAN	em1 (00:0c:29:68:d6:44)	Delete
SPAN	em2 (00:0c:29:68:d6:4e)	Delete
KALI	em3 (00:0c:29:68:d6:58)	Delete
SECONION	em4 (00:0c:29:68:d6:62)	Delete
SPLUNK	em5 (00:0c:29:68:d6:6c)	Delete

Save

Interfaces that are configured as members of a lagg(4) interface will not be shown.

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

Interface Assignments

Interface Groups

Wireless

VLANs

QinQs

PPPs



GREs

GIFs

Bridges




LAGGs

Bridge Interfaces

Interface	Members	Description	Actions
BRIDGE0	LAN		 

+ Add

Interfaces / Bridges / Edit

Bridge Configuration

Member Interfaces

WAN

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

WAN

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

pfSense COMMUNITY EDITION

- System ▾
- Interfaces ▾
- Firewall ▾**
 - Aliases
 - NAT
 - Rules
 - Schedules
 - Traffic Shaper
 - Virtual IPs
- Services ▾
- VPN ▾
- Status ▾
- Diagnostics ▾
- Help ▾

WARNING: The 'admin' account password is set to [REDACTED]. Please change the password in the User Manager.

Interfaces / Bridges

Interface Assignments Interface Groups QinQs PPPs GREs GIFs **Bridges** LAGGs

Bridge Interfaces			
Interface	Members	Description	Actions
BRIDGE0	LAN		

+ Add

WARNING: The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

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 /

Extra Options

Log ☐ Log packets that are handled by this rule
 Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the [Status: System Logs: Settings](#) page).

Description
 A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Advanced Options Display Advanced

Save

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

Floating **WAN** LAN SPAN KALI SECONION SPLUNK

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	✓ 0/1.43 MiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	✓ 0/0 B	IPv4 *	*	*	*	*	*	none			

↑ Add
↓ Add
Delete
Toggle
Copy
Save
Separator

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