

LAB 6 GUIDANCE

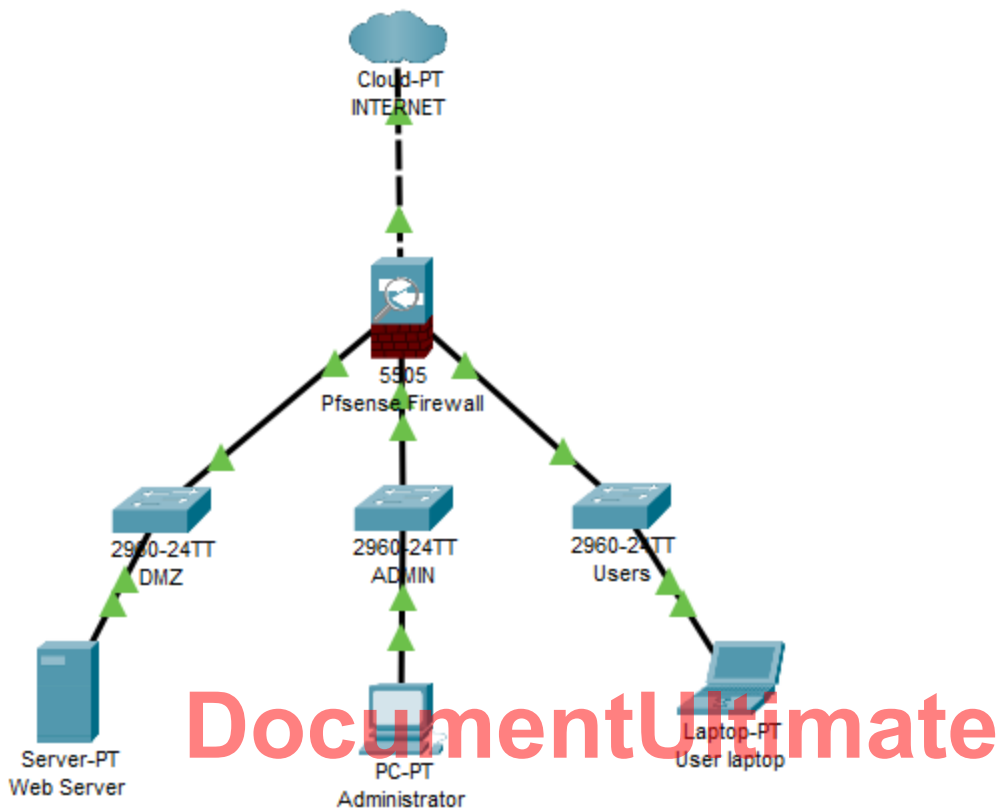
Contents

I. Requirement	2
II. Preparing networks	2
III. Create VMs.....	4
IV. Install OS	12
V. Configure the Pfsense firewall	25
VI. Install and configure web server	36
VII. Test your firewall rules	37

DocumentUltimate

I. Requirement

1. Use your virtualization application to create the below network



2. In the DMZ, you have a Web server, it will serve on port 80, 443 and 22 (for SSH)
3. Use NAT on Pfsense firewall to expose the Web server to Internet. Your web server must be configured with static IP address.
4. Create some policies on Pfsense to restrict the traffic from Internet and LAN to protect your web server and data, as below description:
 - + Allow traffic from Internet to access web server on port 443 only
 - + Allow traffic from Users on LAN to access web server on port 443 and 80
 - + Allow administrators access web server on port 443, 80, and 22
 - + Deny any other port

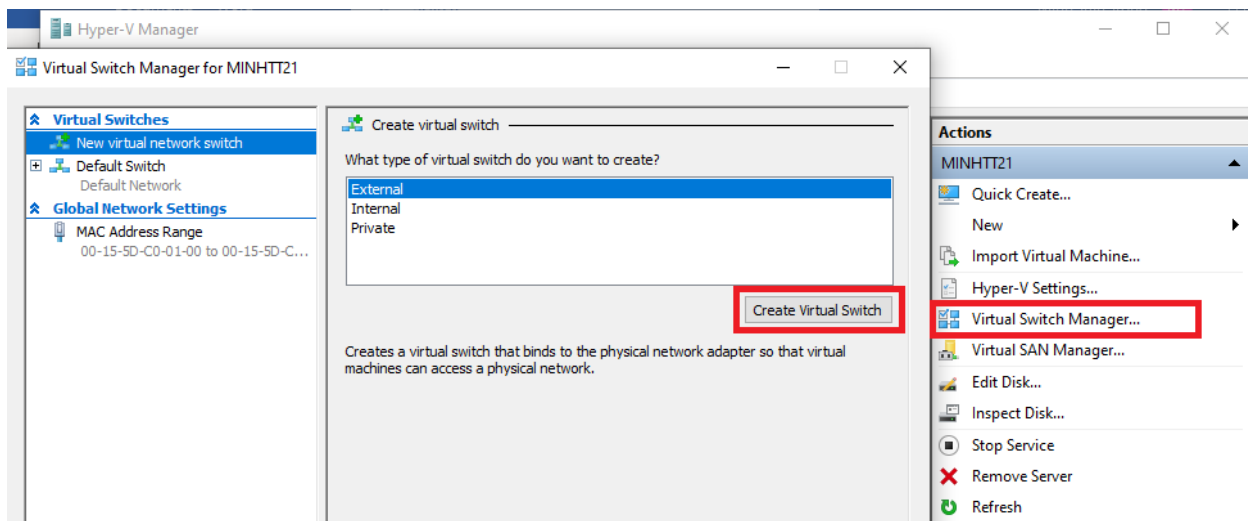
II. Preparing networks

We need 4 networks (4 switches):

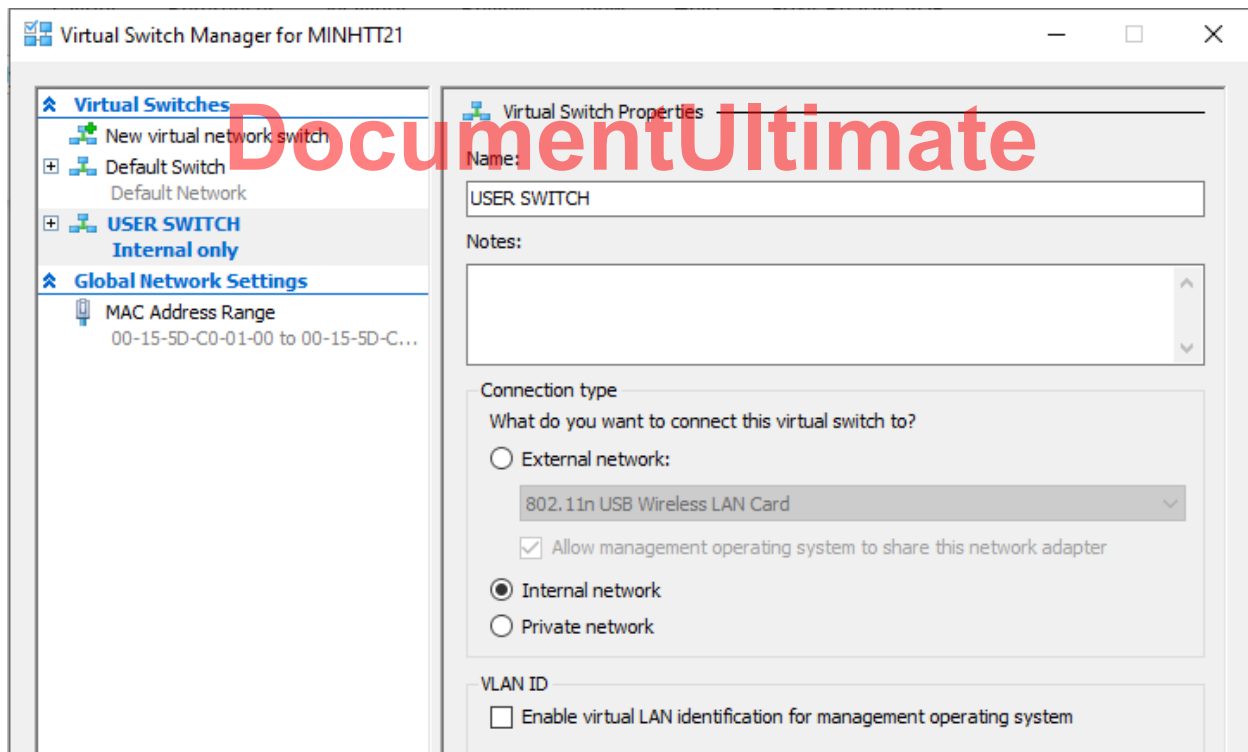
- 01 External network (or NAT network, or Default Switch): for connecting firewall to Internet
- 01 Internal network: for users' PC

- 02 Private network (host only network): for DMZ and ADMIN

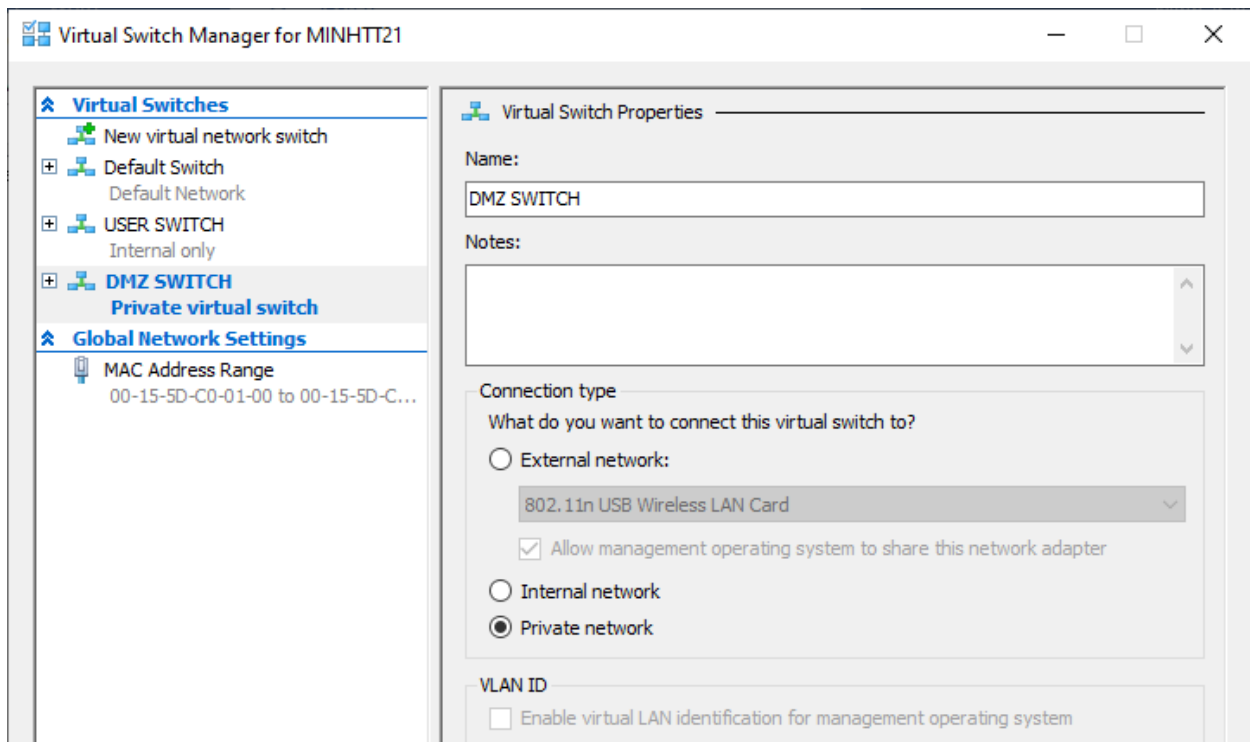
Go to Virtual Switch Manager to Create Virtual Switch



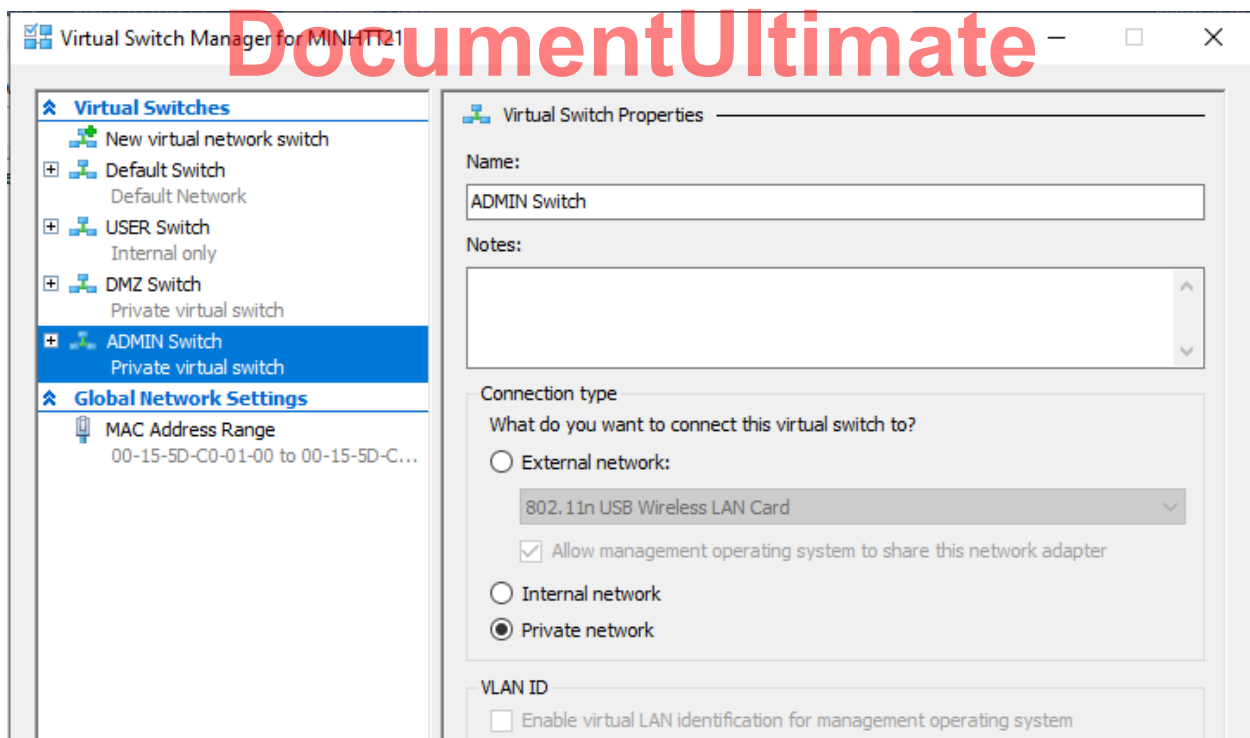
Create USER SWITCH



Create DMZ SWITCH

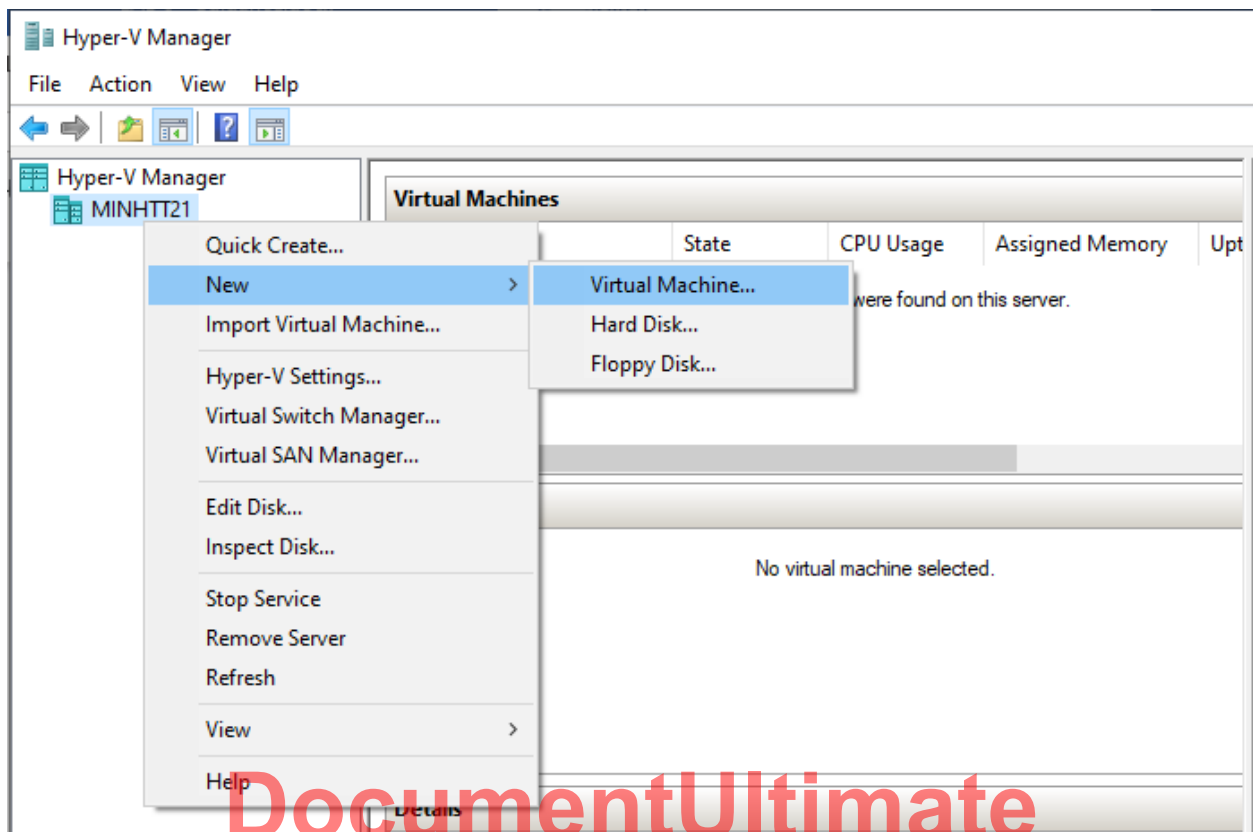


Create ADMIN Switch



III. Create VMs

Right click at the Computer Name > New > Virtual Machine



Create the VM for Pfsense firewall

The screenshot shows the 'New Virtual Machine Wizard' window with the 'Specify Name and Location' step selected. The left sidebar lists the steps: 'Before You Begin', 'Specify Name and Location' (highlighted), 'Specify Generation', 'Assign Memory', 'Configure Networking', 'Connect Virtual Hard Disk', 'Installation Options', and 'Summary'. The main area contains instructions to choose a name and location. The 'Name' field is set to 'Pfsense'. The 'Location' field is set to 'F:\VMs', with a 'Browse...' button next to it. A checkbox 'Store the virtual machine in a different location' is checked. A warning icon and text state: 'If you plan to take checkpoints of this virtual machine, select a location that has enough free space. Checkpoints include virtual machine data and may require a large amount of space.' At the bottom, there are buttons for '< Previous', 'Next >' (highlighted), 'Finish', and 'Cancel'.

New Virtual Machine Wizard

Specify Name and Location

Before You Begin
Specify Name and Location
Specify Generation
Assign Memory
Configure Networking
Connect Virtual Hard Disk
Installation Options
Summary

Choose a name and location for this virtual machine.


The name is displayed in Hyper-V Manager. We recommend that you use a name that helps you easily identify this virtual machine, such as the name of the guest operating system or workload.

Name:

You can create a folder or use an existing folder to store the virtual machine. If you don't select a folder, the virtual machine is stored in the default folder configured for this server.

☒ Store the virtual machine in a different location

Location:

 If you plan to take checkpoints of this virtual machine, select a location that has enough free space. Checkpoints include virtual machine data and may require a large amount of space.

< Previous Next > Finish Cancel

Click Next, then select **Generation 1**

Pfsense firewall we can use minimum memory at 1024 MB (1 GB)

The screenshot shows the 'Assign Memory' step of the 'New Virtual Machine Wizard'. The left sidebar highlights 'Assign Memory'. The main area contains instructions to specify the amount of memory to allocate. The 'Startup memory' field is set to '1024' MB. A checkbox 'Use Dynamic Memory for this virtual machine.' is checked. An information icon and text state: 'When you decide how much memory to assign to a virtual machine, consider how you intend to use the virtual machine and the operating system that it will run.'


Assign Memory

Before You Begin
Specify Name and Location
Specify Generation
Assign Memory
Configure Networking
Connect Virtual Hard Disk
Installation Options
Summary

Specify the amount of memory to allocate to this virtual machine. You can specify an amount from 32 MB through 251658240 MB. To improve performance, specify more than the minimum amount recommended for the operating system.

Startup memory: MB

☒ Use Dynamic Memory for this virtual machine.

 When you decide how much memory to assign to a virtual machine, consider how you intend to use the virtual machine and the operating system that it will run.

At Configure network window, you can select the Default switch

Configure Networking

Each new virtual machine includes a network adapter. You can configure the network adapter to use a virtual switch, or it can remain disconnected.

Connection: **Default Switch**

Not Connected
Default Switch
USER Switch
DMZ Switch
ADMIN Switch

Create Virtual Hard Disk , Pfsense does not need large hard disk space, so we create a 20GB disk

Connect Virtual Hard Disk

A virtual machine requires storage so that you can install an operating system. You can specify the storage now or configure it later by modifying the virtual machine's properties.

☒ Create a virtual hard disk
Use this option to create a VHDX dynamically expanding virtual hard disk.

Name: Pfsense.vhdx

Location: F:\VMs\Pfsense Virtual Hard Disks Browse...

Size: 20 GB (Maximum: 64 TB)

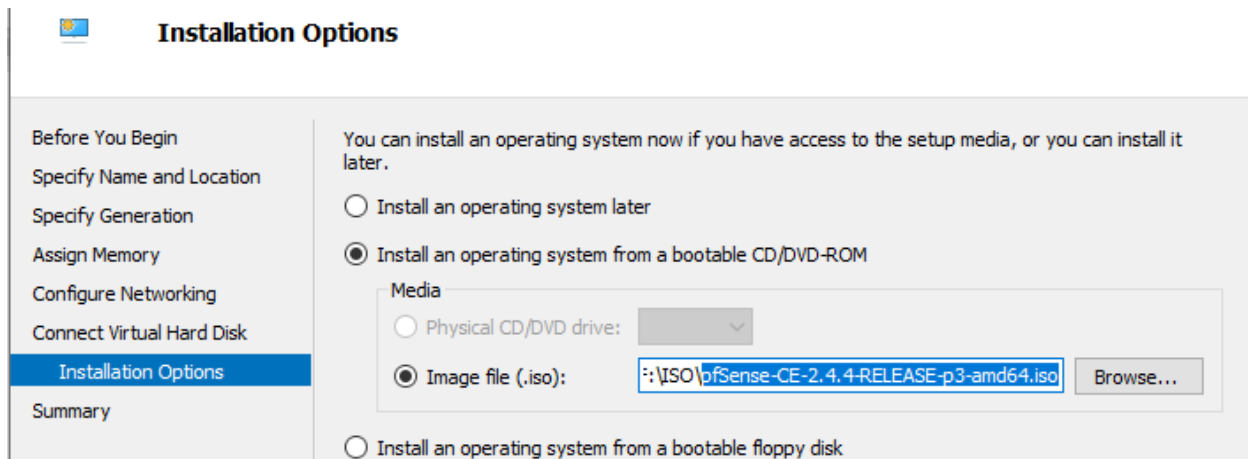
☐ Use an existing virtual hard disk
Use this option to attach an existing virtual hard disk, either VHD or VHDX format.

Location: C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks\ Browse...

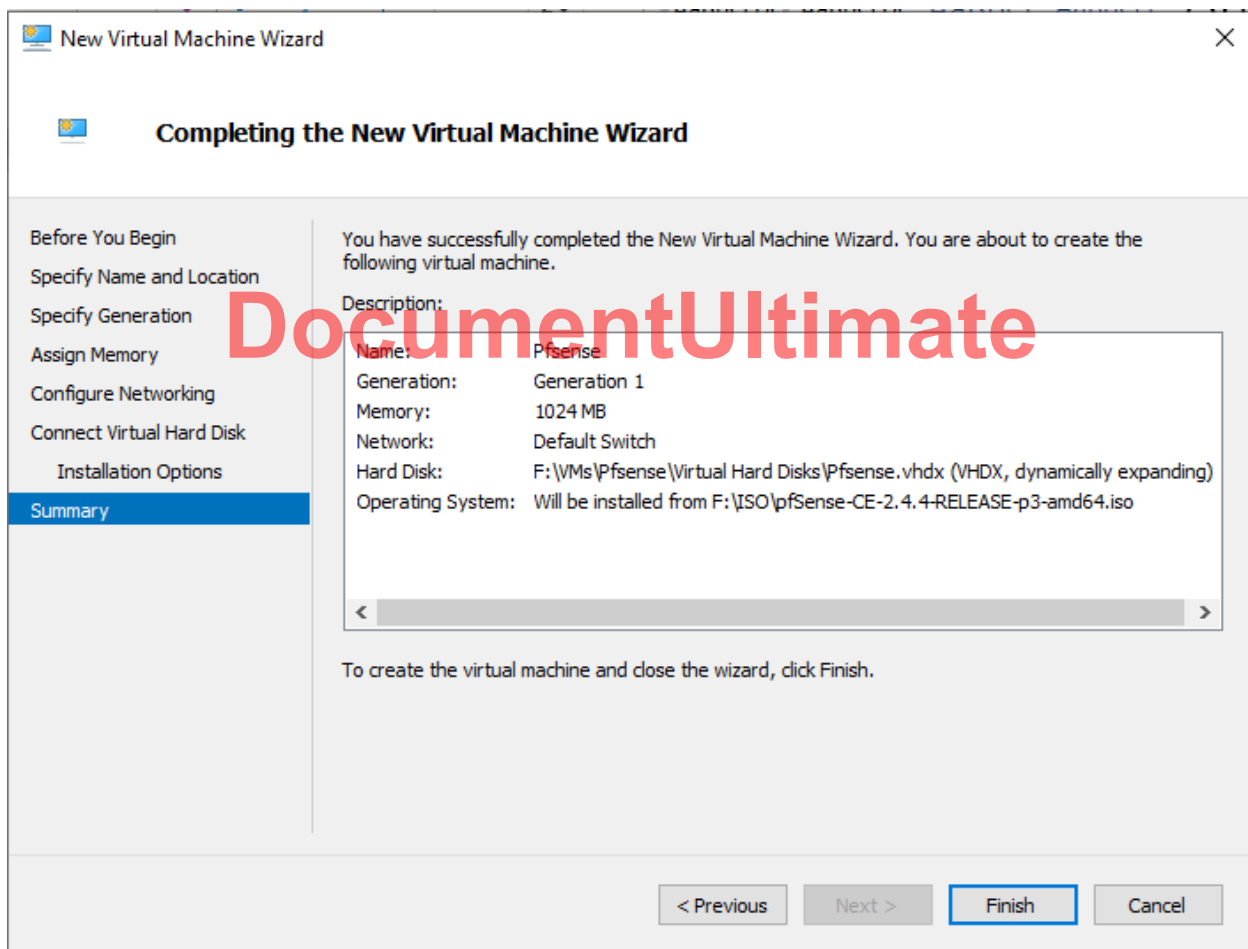
☐ Attach a virtual hard disk later
Use this option to skip this step now and attach an existing virtual hard disk later.

< Previous Next > Finish Cancel

At Installation Options windows, select the options as below

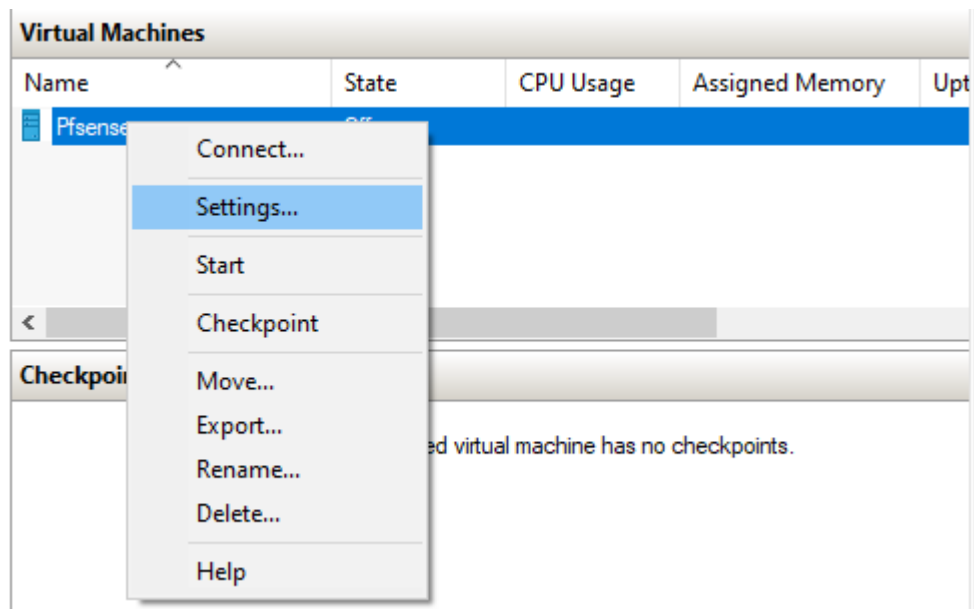


Finishing

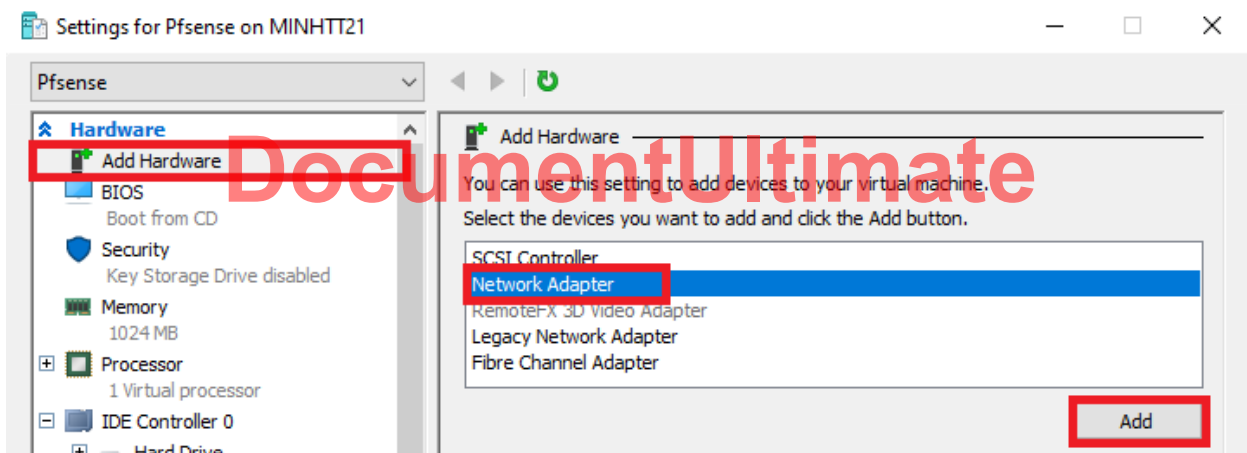


We need add more network interface (NIC) for PfSense VM

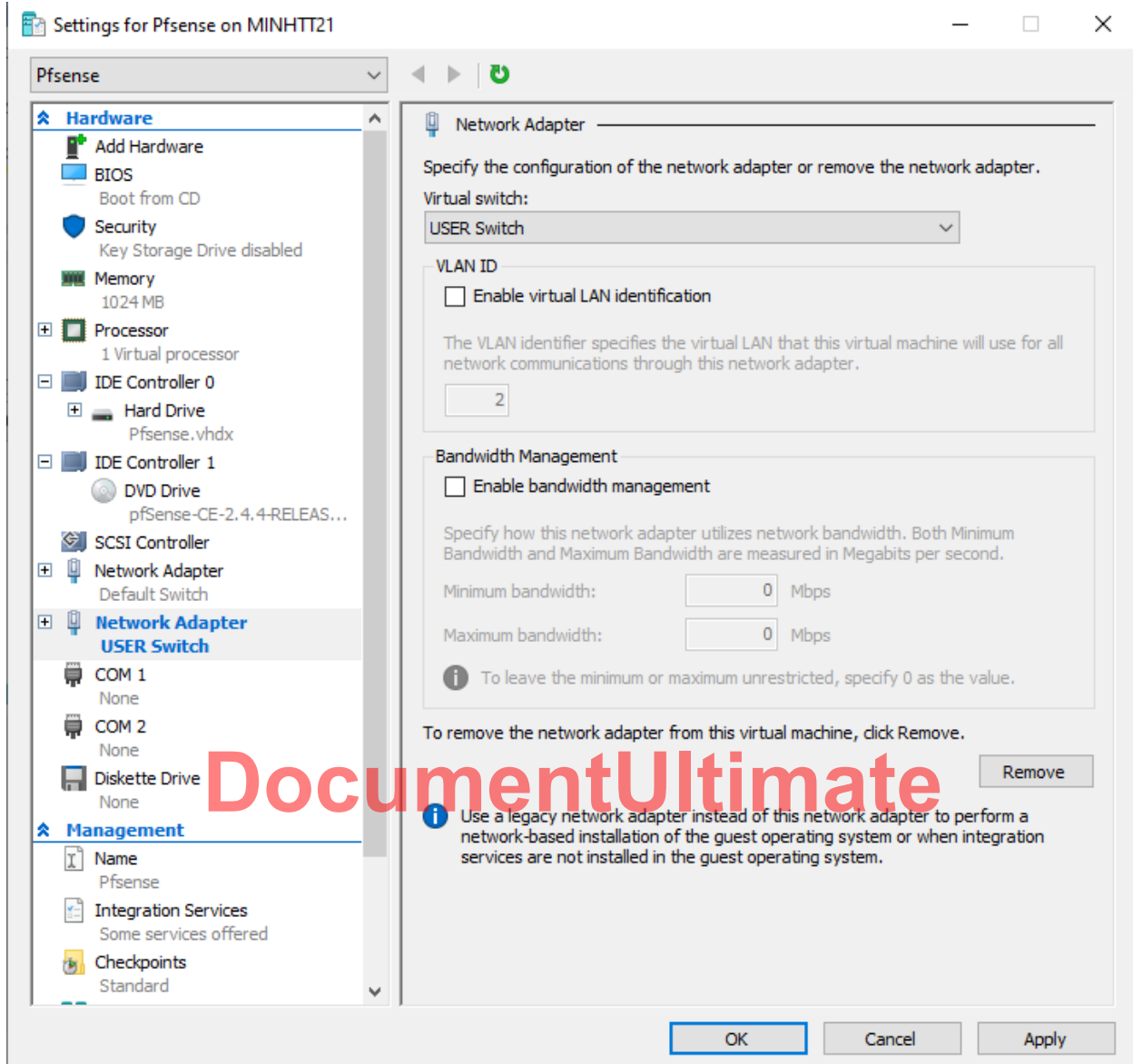
Go to PfSense settings...



Click Add Hardware, select Network Adapter then Add button



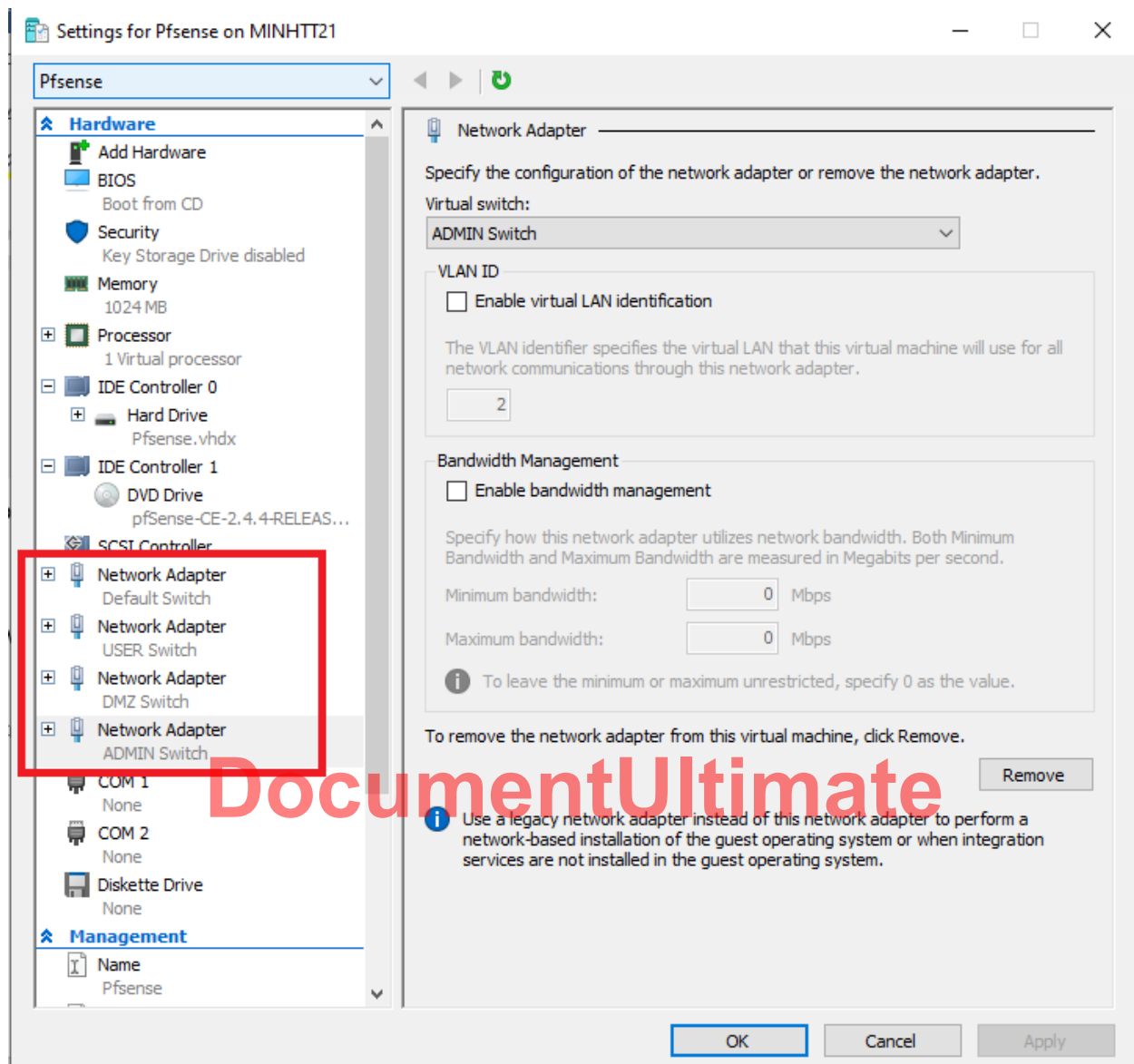
Select the USER Switch for 2nd Network



Do the same for

- DMZ Switch for 3rd Network
- ADMIN Switch for 4th Network

We got:



Create the VM for Web server

Do the same procedure of PfSense creation, but with the below configuration

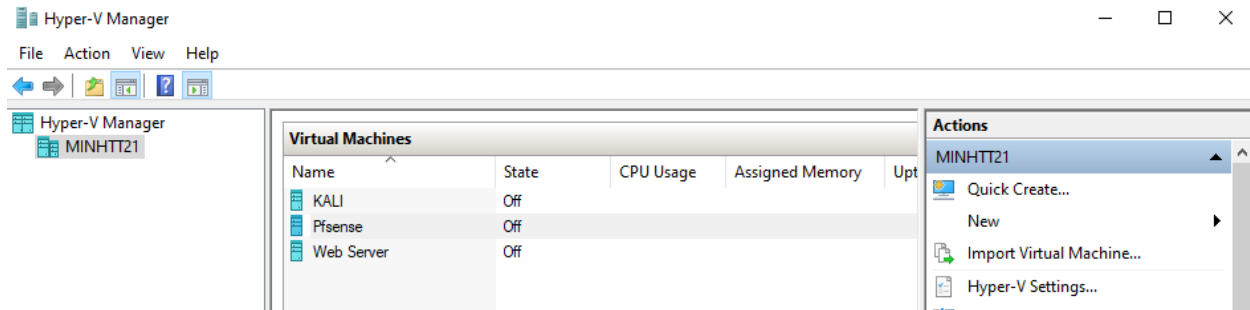
Memory for Web server: 2048 MB

Hard disk: 40 GB

Network: connect to DMZ Switch

Create the VM for ADMIN, the same as web server but this machine has a network connecting to ADMIN Switch

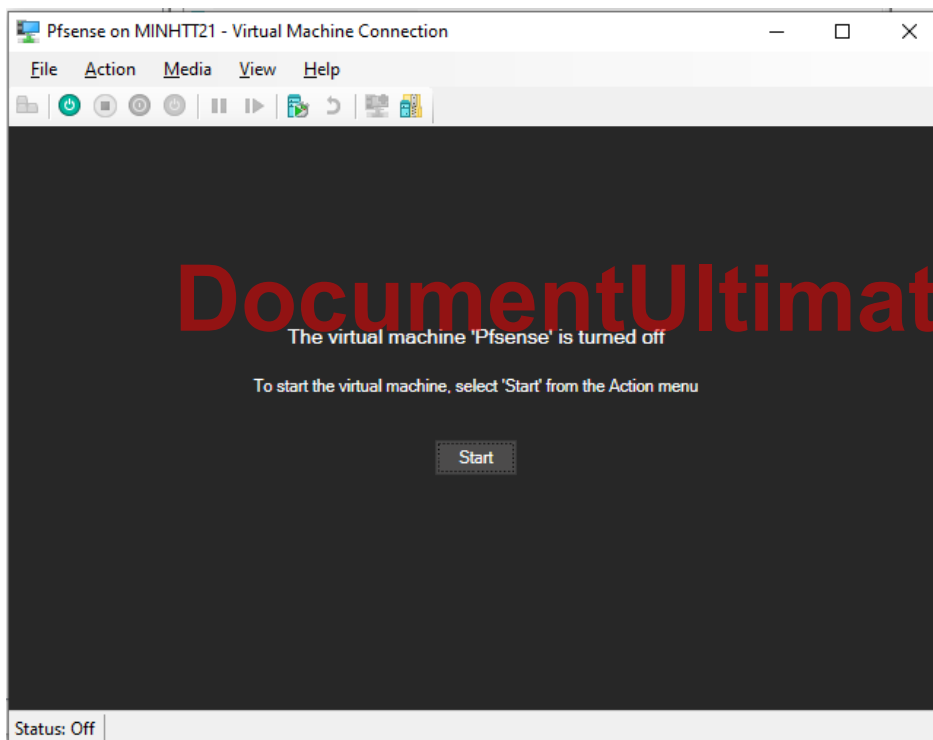
We got:



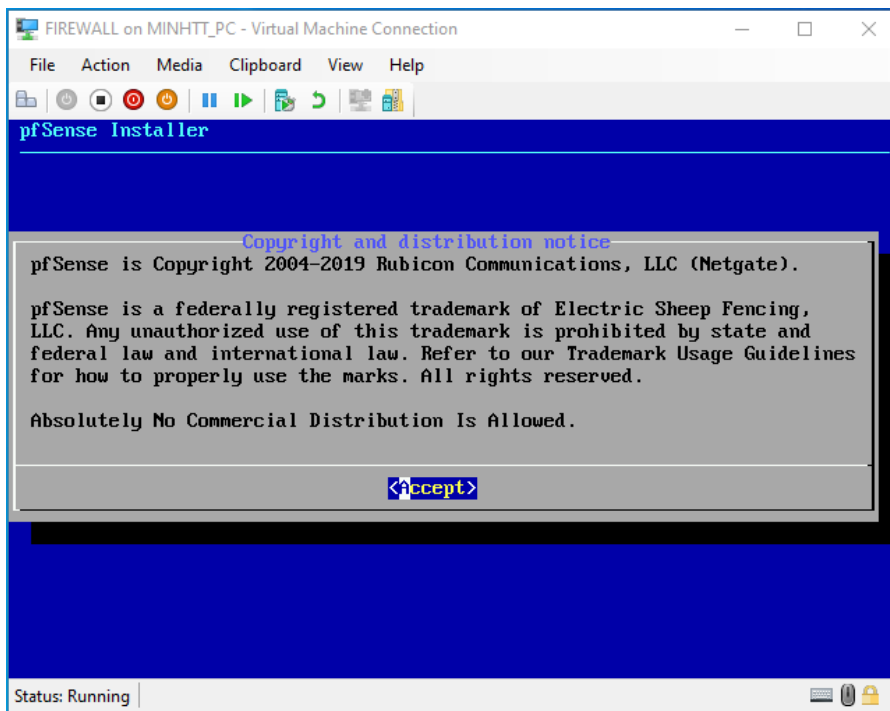
IV. Install OS

1. Install Pfsense

Connect to the Firewall monitor: Right click on Pfsense VM and select connect.



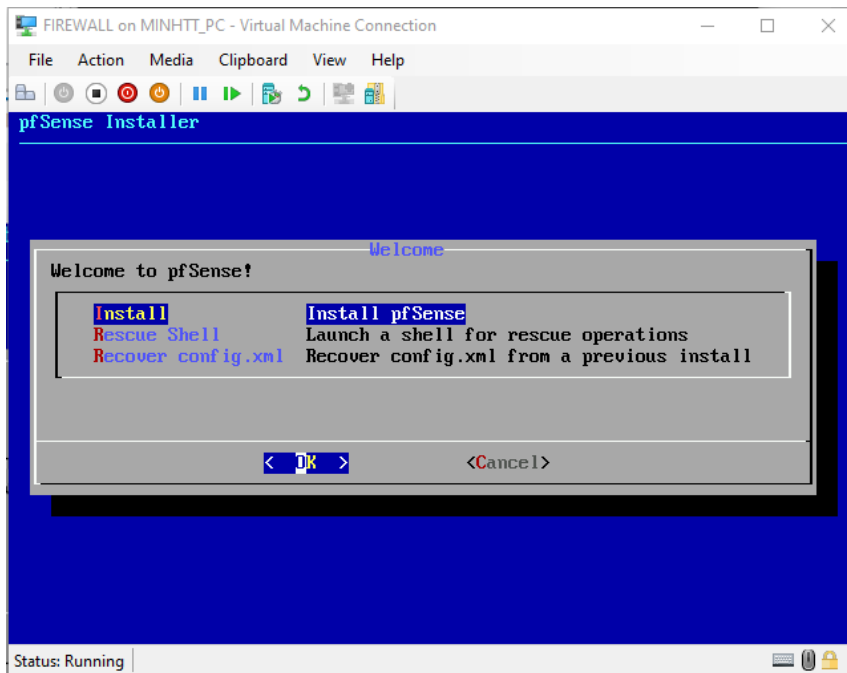
Click the Start button to Power on the Pfsense machine



Press Enter for <Accept>

DocumentUltimate

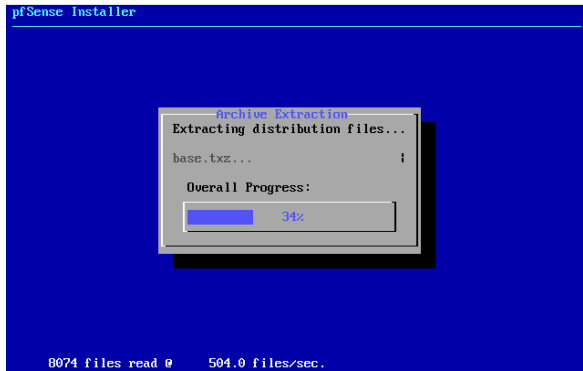
Then as below screen, press Enter for <OK> to install Pfsense on VM



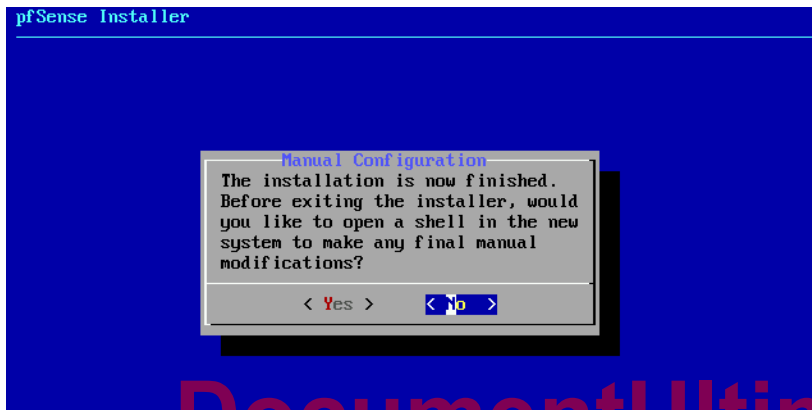
Press Enter for <Select> at "Continue with default keymap"



Press Enter for **Auto (UFS)**, then Install will run



At this screen, select **NO**



DocumentUltimate

At the last finishing screen, you should eject your ISO out of CDROM-Drive first, then select **Reboot**

After reboot, select NO (n) at VLAN setup requirement

```
Structured Extended Features3=0xbc000000<IBPB,STIBP,ARCH_CAP,SSBD>
XSAVE Features=0x1<XSAVEOPT>
Hypervisor: Origin = "Microsoft Hv"
Done.
..... done.
Initializing..... done.
Starting device manager (devd)...done.
Loading configuration.....done.
Updating configuration.....done.
Warning: Configuration references interfaces that do not exist: em0 em1

Network interface mismatch -- Running interface assignment option.

Valid interfaces are:

bn0      00:15:5d:c0:01:01 (down) Hyper-V Network Interface
bn1      00:15:5d:c0:01:02 (down) Hyper-V Network Interface
bn2      00:15:5d:c0:01:03 (down) Hyper-V Network Interface
bn3      00:15:5d:c0:01:04 (down) Hyper-V Network Interface

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
```

Select the 1st Interface for WAN (hn0)

```
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
(hn0 hn1 hn2 hn3 or a): hn0
```

The 2nd Interface for Users network (hn1)

```
Enter the WAN interface name or 'a' for auto-detection
(hn0 hn1 hn2 hn3 or a): hn0

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(hn1 hn2 hn3 a or nothing if finished): hn1
```

The 3rd Interface for DMZ (hn2) and the 4th Interface for Administrator network (hn3)

```
Enter the WAN interface name or 'a' for auto-detection
(hn0 hn1 hn2 hn3 or a): hn0

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(hn1 hn2 hn3 a or nothing if finished): hn1

Enter the Optional 1 interface name or 'a' for auto-detection
(hn2 hn3 a or nothing if finished): hn2

Enter the Optional 2 interface name or 'a' for auto-detection
(hn3 a or nothing if finished): hn3
```

Remember that, we can change these interface assignment later!

After answer yes (y) at asking for processing, we get


```
Pfsense on MINHTT21 - Virtual Machine Connection
File Action Media Clipboard View Help
pfSense 2.4.4-RELEASE (Patch 3) amd64 Wed May 15 18:53:44 EDT 2019
Bootup complete

FreeBSD/amd64 (pfSense.localdomain) (ttyv0)
Hyper-V Virtual Machine - Netgate Device ID: 75eea8bc900e43adccb1

*** Welcome to pfSense 2.4.4-RELEASE-p3 (amd64) on pfSense ***

WAN (wan)      -> hn0      -> v4/DHCP4: 172.28.6.106/20
LAN (lan)      -> hn1      -> v4: 192.168.1.1/24
OPT1 (opt1)    -> hn2      ->
OPT2 (opt2)    -> hn3      ->

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

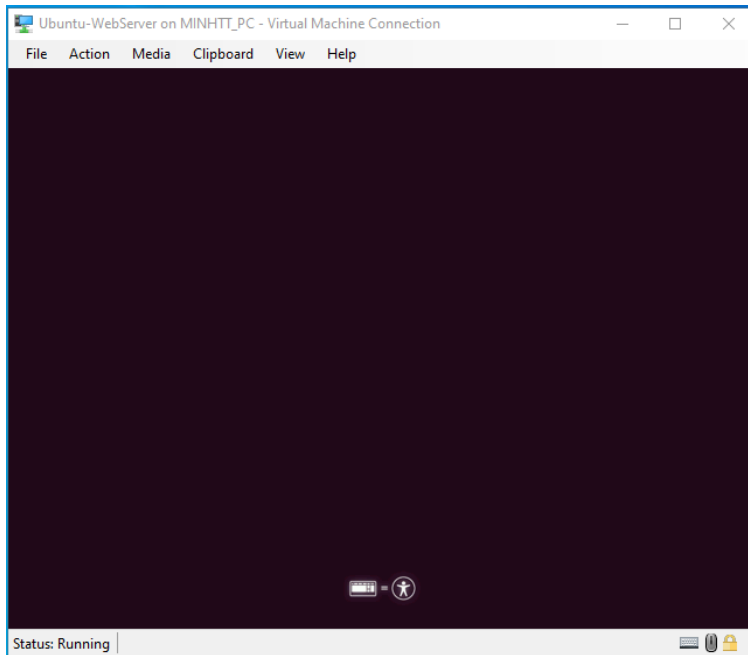
Enter an option:
Status: Running
```

2. Install Web server

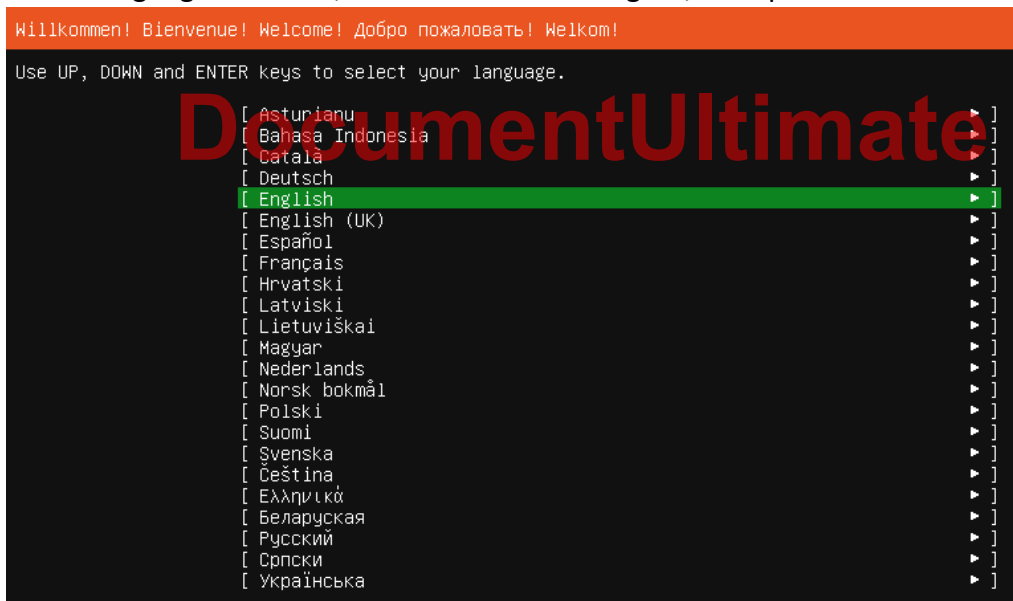
We can use any kind of OS to create a web server in the DMZ.

At this guidance, we will use the Ubuntu 20.04.

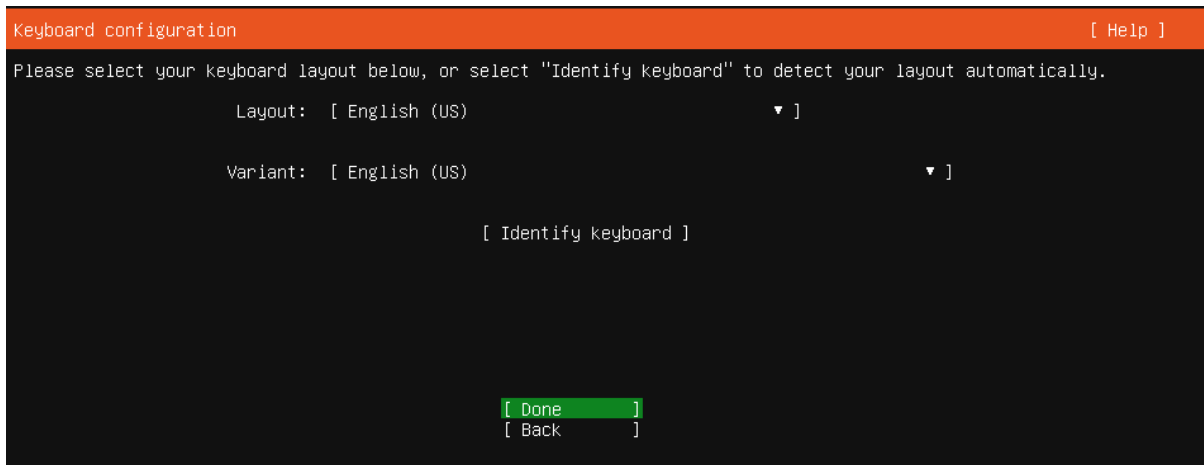
Start your machine



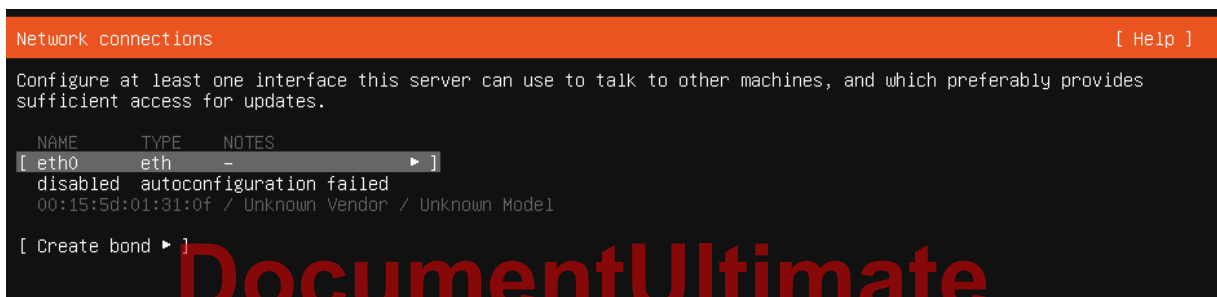
At the language selection, we should use the English, then press Enter



At the keyboard configuration, also use English (US) key type and Done



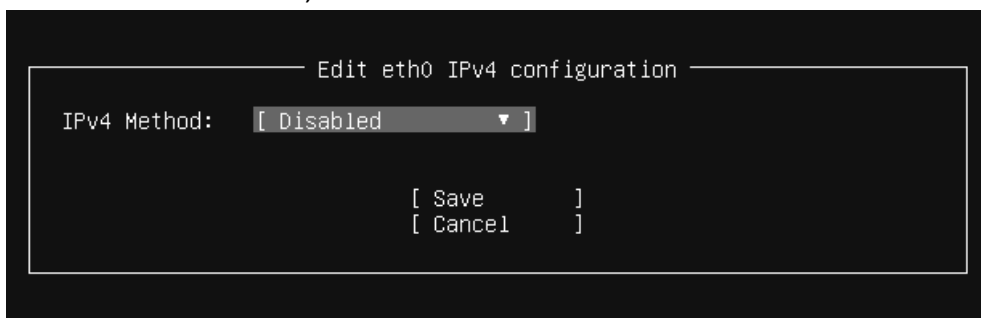
At the Network Configuration, use the up/down arrow keys to move the pointer to your network interface as below



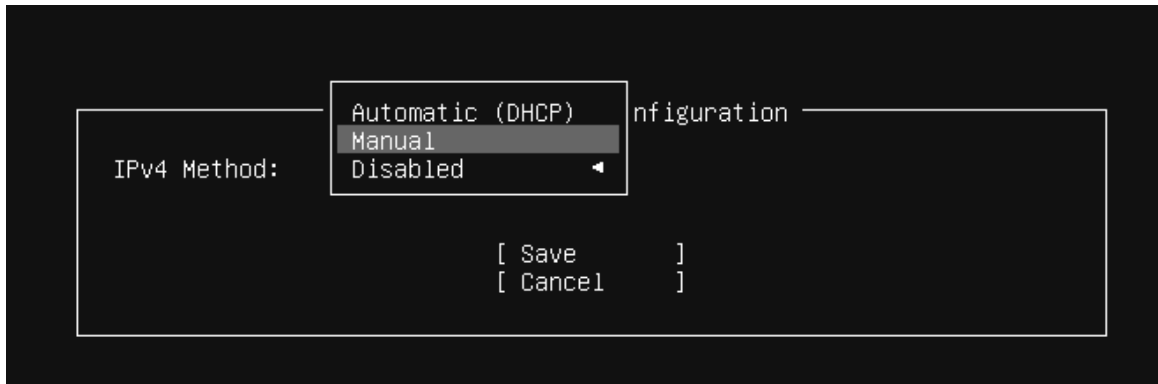
Press Enter, select **Edit IPv4**



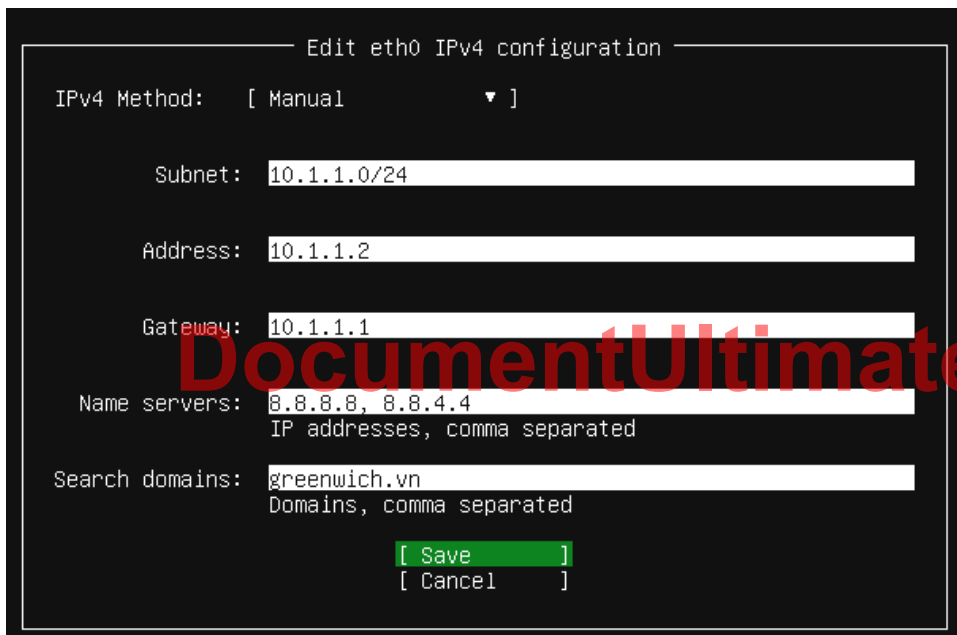
Press Enter at Edit IPv4, we have the edit screen



At IPv4 Method, press Enter then select the **Manual**

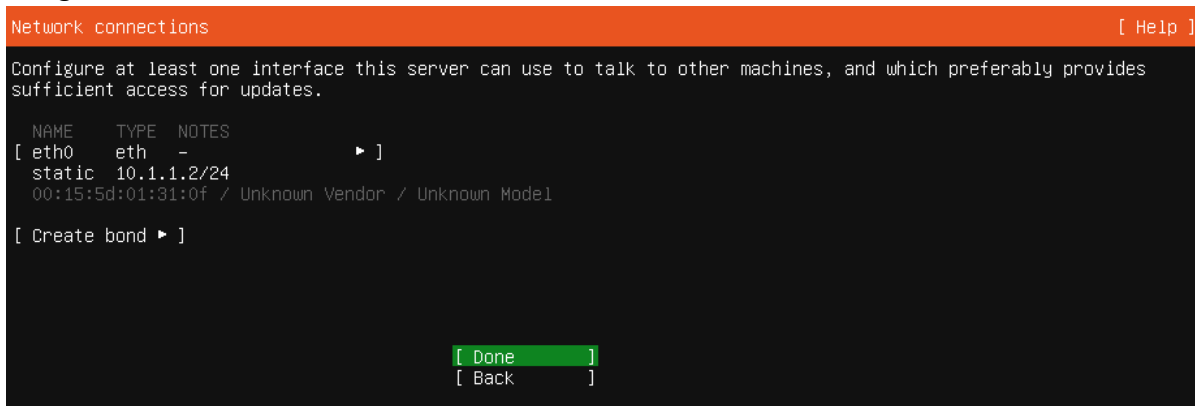


We will set static IP for this web server



Move the pointer to Save and press Enter.

We get the below screen



Move the pointer to Done then press Enter

At the Guided Storage Configuration, we also use the default setting as below

Move your pointer to Done and press Enter
Next screen, review your partitions and just Done

```

Storage configuration
FILE SYSTEM SUMMARY
  MOUNT POINT      SIZE      TYPE      DEVICE TYPE
[ /                20.000G   new ext4   new LVM logical volume ▶ ]
[ /boot            1.000G   new ext4   new partition of local disk ▶ ]

AVAILABLE DEVICES

  DEVICE                                TYPE                                SIZE                                ▶ ]
[ ubuntu-vg (new)                        LVM volume group                    38.996G
  free space                            18.996G

[ Create software RAID (md) ▶ ]
[ Create volume group (LVM) ▶ ]

USED DEVICES

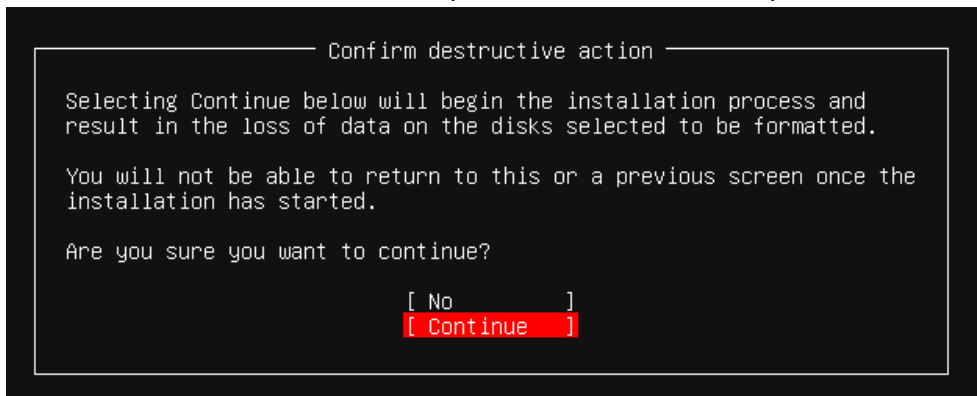
  DEVICE                                TYPE                                SIZE                                ▶ ]
[ ubuntu-vg (new)                        LVM volume group                    38.996G
  ubuntu-lv      new, to be formatted as ext4, mounted at /    20.000G ▶ ]

[ 3600224806d35e23bd67c210eab1b5864    local disk                    40.000G ▶ ]
  partition 1    new, bios_grub                                1.000M ▶ ]
  partition 2    new, to be formatted as ext4, mounted at /boot 1.000G ▶ ]
  partition 3    new, PV of LVM volume group ubuntu-vg          38.997G ▶ ]

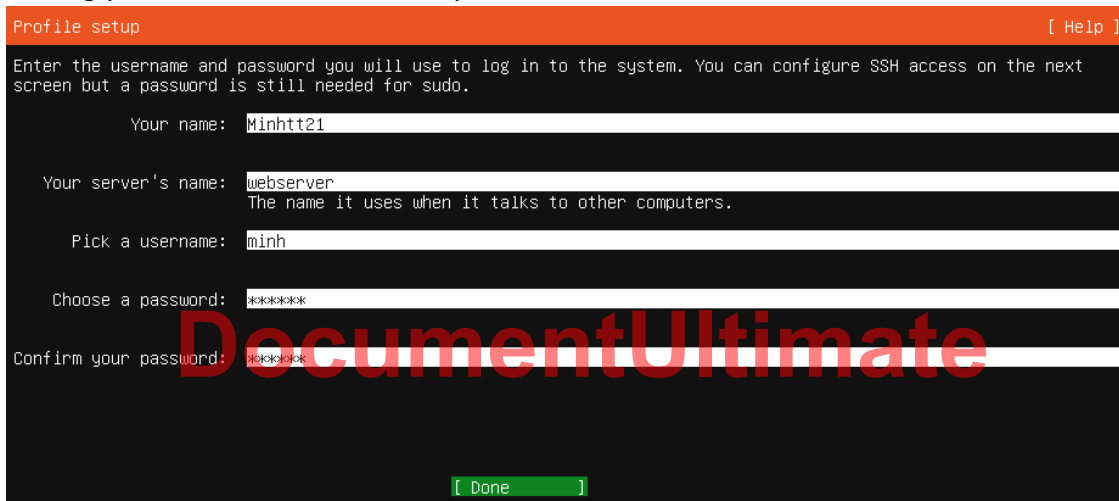
[ Done ]
[ Reset ]
[ Back ]

```

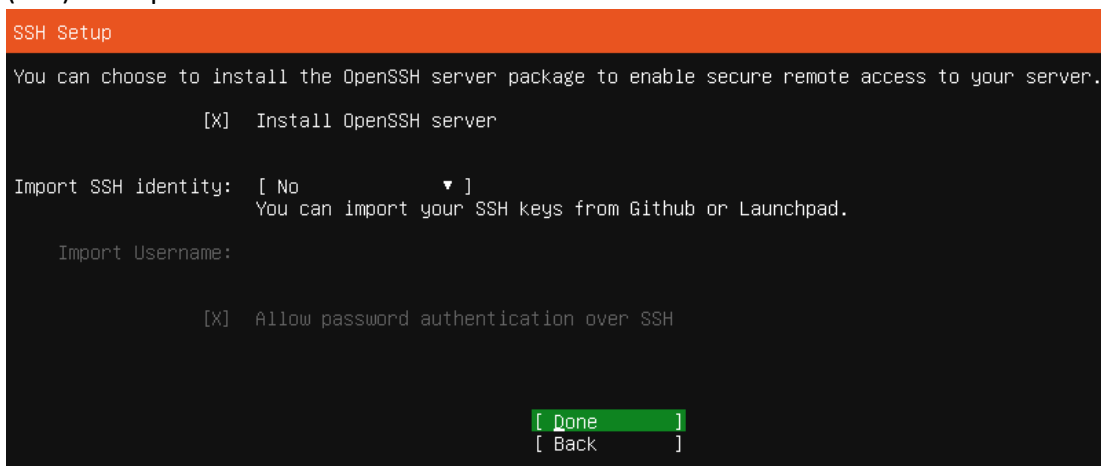
At confirmation screen, move the pointer to Continue and press Enter



Setting your name, username and password then Done



At SSH setup screen, move the pointer to **Install SSH Server** option, use Space key to select (tick) this option. Then Done.



System will be installed. Just wait until it finishes.

```
installing system
  curtin command install
    preparing for installation
    configuring storage
      running 'curtin block-meta simple'
      curtin command block-meta
        removing previous storage devices
        configuring disk: disk-sda
        configuring partition: partition-0
        configuring partition: partition-1
        configuring format: format-0
        configuring partition: partition-2
        configuring lvm_volgroup: lvm_volgroup-0
        configuring lvm_partition: lvm_partition-0
        configuring format: format-1
        configuring mount: mount-1
        configuring mount: mount-0
    writing install sources to disk
      running 'curtin extract'
      curtin command extract
        acquiring and extracting image from cp:///media/filesystem
    configuring installed system
      running '/snap/bin/subiquity.subiquity-configure-run'
      running '/snap/bin/subiquity.subiquity-configure-apt /snap/subiquity/1966/usr/bin/python3 true'
      curtin command apt-config
      curtin command in-target
    running 'curtin curthooks'
      curtin command curthooks
        configuring apt configuring apt
        installing missing packages
        configuring iscsi service
        configuring raid (mdadm) service
        installing kernel |
```

DocumentUltimate

[View full log]

Complete and reboot

```
Installation complete! [ Help ]

Finished install!

removing previous storage devices
configuring disk: disk-sda
configuring partition: partition-0
configuring partition: partition-1
configuring format: format-0
configuring partition: partition-2
configuring lvm_volgroup: lvm_volgroup-0
configuring lvm_partition: lvm_partition-0
configuring format: format-1
configuring mount: mount-1
configuring mount: mount-0
writing install sources to disk
running 'curtin extract'
curtin command extract
acquiring and extracting image from cp:///media/filesystem
configuring installed system
running '/snap/bin/subiquity.subiquity-configure-run'
running '/snap/bin/subiquity.subiquity-configure-apt /snap/subiquity/1966/usr/bin/python3 true'
curtin command apt-config
curtin command in-target
running 'curtin curthooks'
curtin command curthooks
configuring apt configuring apt
installing missing packages
configuring iscsi service
configuring raid (mdadm) service
installing kernel
setting up swap
apply networking config
writing etc/fstab
configuring multipath
updating packages on target system
configuring pollinate user-agent on target
updating initramfs configuration
configuring target system bootloader
installing grub to target devices
finalizing installation
running 'curtin hook'
curtin command hook
executing late commands
final system configuration
configuring cloud-init
installing openssh-server
restoring apt configuration
downloading and installing security updates

[ View full log ]
[ Reboot ]
```

Login after reboot

```
Ubuntu 20.04.1 LTS webserver tty1

webserver login: minh
Password: _
```


Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by applicable law.

To run a command as administrator (user "root"), use "sudo <command>". See "man sudo_root" for details.

```
minh@webserver:~$  
minh@webserver:~$  
minh@webserver:~$ _
```

Check IP address of web server

```
minh@webserver:~$  
minh@webserver:~$  
minh@webserver:~$ ip addr  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1/8 scope host lo  
        valid_lft forever preferred_lft forever  
    inet6 ::1/128 scope host  
        valid_lft forever preferred_lft forever  
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000  
    link/ether 00:15:5d:01:31:0f brd ff:ff:ff:ff:ff:ff  
    inet 10.1.1.2/24 brd 10.1.1.255 scope global eth0  
        valid_lft forever preferred_lft forever  
    inet6 fe80::215:5dff:fe01:310f/64 scope link  
        valid_lft forever preferred_lft forever  
minh@webserver:~$
```

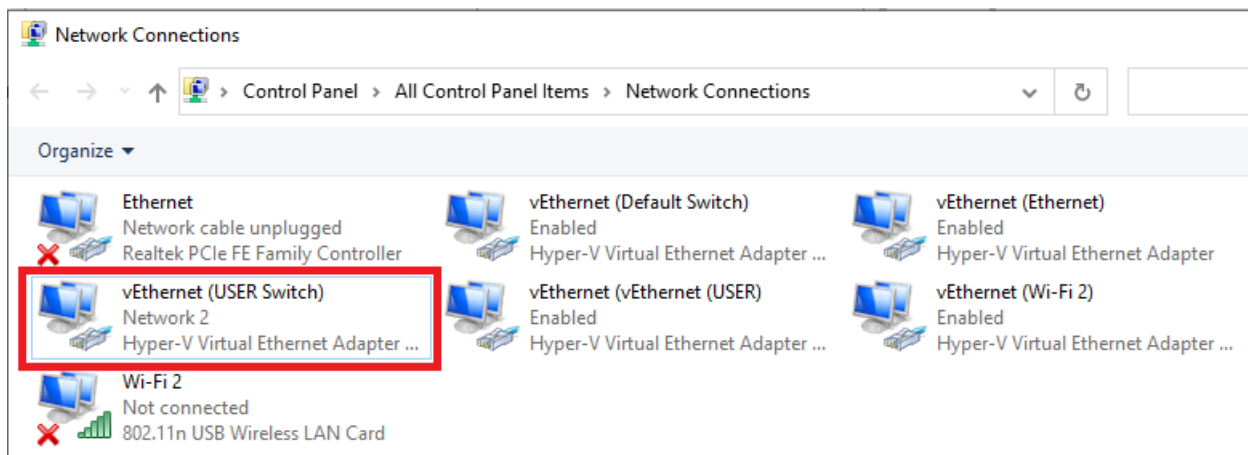
Test ping to gateway of DMZ

DocumentUltimate

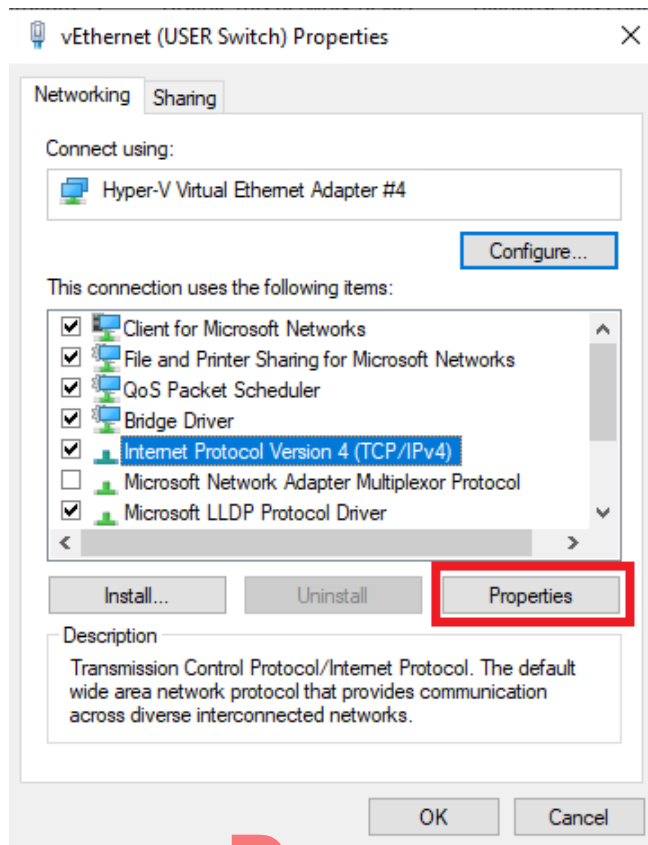
3. Install Kali Linux for Administrator's PC

V. Configure the Pfsense firewall

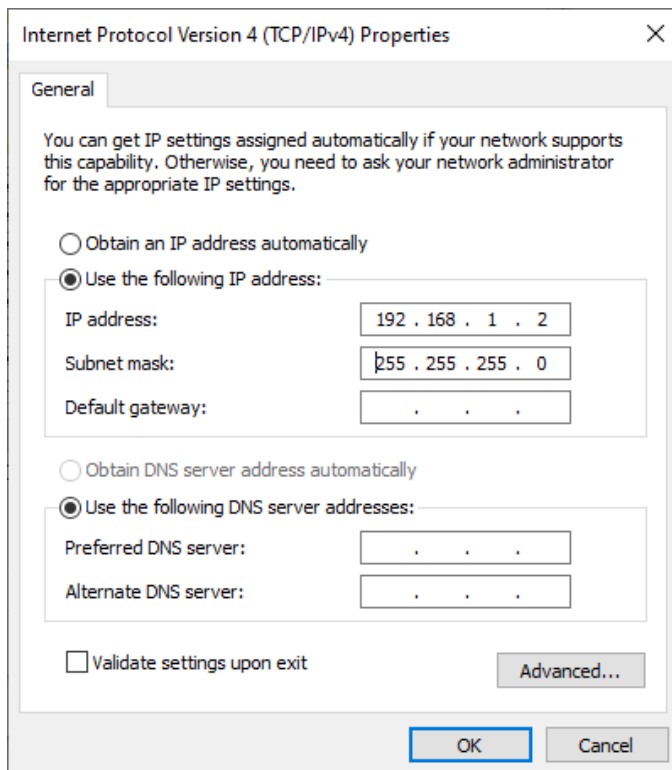
1. Setting the virtual interface on your REAL computer (laptop) that connecting to USER Switch



Right click and select Properties



Set the static IP in the same subnet of LAN Network on Pfsense. You can change the LAN IP address later.



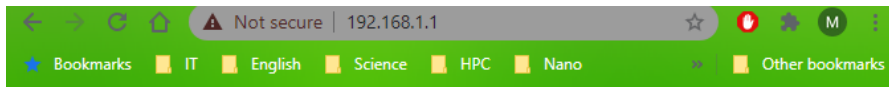
Make sure you can reach the the LAN interface by the ping command on your real computer (laptop).

```
C:\Users\minht>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

2. Use your browser to open the PfSense web console (use the LAN IP 192.168.1.1 for the URL)



Your connection is not private

Attackers might be trying to steal your information from **192.168.1.1** (for example, passwords, messages, or credit cards). [Learn more](#)

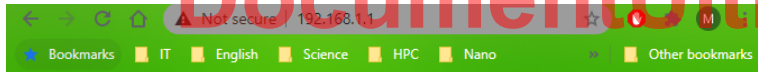
NET::ERR_CERT_AUTHORITY_INVALID

☐ Help improve security on the web for everyone by sending [URLs of some pages you visit, limited system information, and some page content](#) to Google. [Privacy policy](#)

Advanced

Back to safety

Because we have no certificate for the HTTPS on this page, so don't worry, just click **Advanced** and then **Proceed**.



SIGN IN

admin

.....

SIGN IN

3. Login your Pfsense with admin/pfsense for username/password
You can follow the Wizard to configure your firewall
Or you just ignore the wizard and go to the menu bar on the top to configure the Pfsense.
Below is the wizard steps
Next and then fill some information

Wizard / pfSense Setup / General Information ?

Step 2 of 9

General Information

On this screen the general pfSense parameters will be set.

Hostname
EXAMPLE: myserver

Domain
EXAMPLE: mydomain.com

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

Next at the WAN configuration (use the default setting)

The configuration of LAN (you can change the subnet as your wish)

Configure LAN Interface

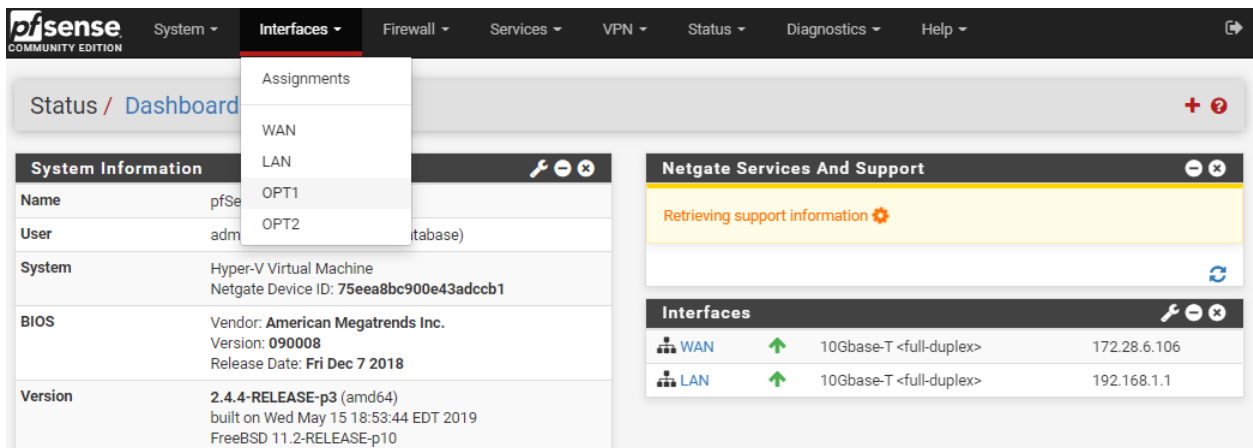
On this screen the Local Area Network information will be configured.

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

Subnet Mask

» Next

4. Rename the interface for easy remember them



The OPT1 will be DMZ (below image, I have cropped the important information about the subnet mask of DMZ interface, it should be /24, see the next image for the same)

Interfaces / OPT1 (hn2)

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: xx:xx:xx:xx:xx:xx or leave blank.

MTU
If this field is blank, the adapter's default MTU will be used. This is typically 1500.




MSS
If a value is entered in this field, then MSS clamping for TCP connections to this interface will be enabled.

Speed and Duplex
Explicitly set speed and duplex mode for this interface.
WARNING: MUST be set to autoselect (automatically negotiate speed) unless you know what you are doing.

Static IPv4 Configuration

IPv4 Address

The OPT2 will be ADMIN

Interfaces / OPT2 (hn3)   

General Configuration

Enable	<input checked="" type="checkbox"/> Enable interface
Description	<input type="text" value="ADMIN"/> <small>Enter a description (name) for the interface here.</small>
IPv4 Configuration Type	<input type="text" value="Static IPv4"/>
IPv6 Configuration Type	<input type="text" value="None"/>
MAC Address	<input type="text" value="xxxxxxxxxxxx"/> <small>This field can be used to modify ("spoof") the MAC address of this interface. Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.</small>
MTU	<input type="text"/> <small>If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.</small>
MSS	<input type="text"/> <small>If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect.</small>
Speed and Duplex	<input type="text" value="Default (no preference, typically autoselect)"/> <small>Explicitly set speed and duplex mode for this interface. WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.</small>

Static IPv4 Configuration

IPv4 Address	<input type="text" value="10.1.1.1"/> / <input type="text" value="24"/>
--------------	---

DO NOT forget to tick at Enable Interface, Save and Apply Changes buttons

5. NAT configuration

Here we will use the overlapping NAT

NAT will be used for Web server, mapping the private IP of web server (10.1.1.2) to the WAN's IP and mapping the HTTPS port (on web server) to outside HTTPS port.

Go to Firewall > NAT, then click Add button

Edit Redirect Entry

Disabled ☐ Disable this rule

No RDR (NOT) ☐ Disable redirection for traffic matching this rule
This option is rarely needed. Don't use this without thorough knowledge of the implications.

Interface WAN
Choose which interface this rule applies to. In most cases "WAN" is specified.

Protocol TCP
Choose which protocol this rule should match. In most cases "TCP" is specified.

Source Display Advanced

Destination ☐ Invert match. WAN address Type Address/mask

Destination port range HTTPS From port Custom HTTPS To port Custom
Specify the port or port range for the destination of the packet for this mapping. The 'to' field may be left empty if only mapping a single port.

Redirect target IP 10.1.1.2
Enter the internal IP address of the server on which to map the ports.
e.g.: 192.168.1.12

Redirect target port HTTPS Port Custom
Specify the port on the machine with the IP address entered above. In case of a port range, specify the beginning port of the range (the end port will be calculated automatically).
This is usually identical to the "From port" above.

Description NAT for Web server
A description may be entered here for administrative reference (not parsed).

Then click Save button

Firewall / NAT / Port Forward

The NAT configuration has been changed.
The changes must be applied for them to take effect. Apply Changes

Port Forward 1:1 Outbound NPT

Rules												
	Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions		
<input type="checkbox"/>	<input checked="" type="checkbox"/>		WAN	TCP	*	*	WAN address	443 (HTTPS)	10.1.1.2	443 (HTTPS)	NAT for Web server	

Add Add Delete Save Separator

Legend
 Pass
 Linked rule

And Do Not forget to click Apply Changes button

Go to the Firewall > Rules, we can see :

Firewall / Rules / WAN

Floating WAN LAN DMZ ADMIN

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	0/606 B	*	RFC 1918 networks	*	*	*	*	*		Block private networks	
<input checked="" type="checkbox"/>	0/0 B	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	
<input type="checkbox"/>	0/0 B	IPv4 TCP	*	*	10.1.1.2	443 (HTTPS)	*	none		NAT NAT for Web server	

Add Add Delete Save Separator

The NAT rules was created for Web server.

The NAT for web server means: accept any TCP/IPv4 session from any IP (outside) to Web server on port 443 (HTTPS)

6. Configure the Rules (firewall policies)

Now, at the menu Firewall > Rules we can create any policy we want to protect our network on any interface.

REMEMBER: firewall will manage session of any connection, this mean that firewall will check for the first packet of any initiation session then remember the policy of this session in memory until the session finishes.

As the LAB requirements, we can create some rules on the DMZ network as below
Go to the DMZ, then click Add (with down arrow, you can change the order of rules by dragging them)

pfSense
COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

Firewall / Rules / DMZ

Floating WAN LAN DMZ ADMIN

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<p>No rules are currently defined for this interface</p> <p>All incoming connections on this interface will be blocked until pass rules are added. Click the button to add a new rule.</p>											

Add Add Delete Save Separator

Now the first rule, we allow any computer in the DMZ network can reach outside network (or reach the Internet). This means that any session that initiates by any computer in DMZ will pass the firewall check. This rule is optional so that your servers can download any update or patch packet from software supplier.

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

DMZ

▼

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

DMZ net

▼

Source Address

/

▼

Destination

Destination

☐ Invert match

any

▼

Destination Address

/

▼





Save the rule and we have:

Firewall / Rules / DMZ

The changes have been applied successfully. The firewall rules are now reloading in the background.
Monitor the filter reload progress.

FloatingWANLANDMZADMIN

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓	1 / 16 KiB	IPv4 *	DMZ net	*	*	*	*	none		   

Do not forget click apply changes

Create the rule: *Allow any Administrator PC (source) connect to Web server (Destination, a host with IP 10.1.1.2) on SSH port (22)*

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	<input type="checkbox"/> Disable this rule Set this option to disable this rule without removing it from the list.
Interface	DMZ
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	TCP
Choose which IP protocol this rule should match.	

Source

Source	<input type="checkbox"/> Invert match	ADMIN net	Source Address	/	
---------------	---------------------------------------	-----------	----------------	---	--

[Display Advanced](#)

The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, **any**.

Destination

Destination	<input type="checkbox"/> Invert match	Single host or alias	10.1.1.2	/	
--------------------	---------------------------------------	----------------------	----------	---	--

Destination Port Range

From	To
SSH (22)	SSH (22)

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

And the rules table as below

Firewall / Rules / DMZ

The changes have been applied successfully. The firewall rules are now reloading in the background.
[Monitor](#) the filter reload progress.

Floating

WAN

LAN

DMZ

ADMIN

Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 1 / 16 KiB	IPv4 *	DMZ net	*	*	*	*	none			
<input type="checkbox"/>	✓ 0 / 0 B	IPv4 TCP	ADMIN net	*	10.1.1.2	22 (SSH)	*	none			

It is similar for other rules.

Firewall / Rules / DMZ

The changes have been applied successfully. The firewall rules are now reloading in the background.
Monitor the filter reload progress.

Floating

WAN

LAN

DMZ

ADMIN

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓	0/16 KiB	IPv4 *	DMZ net	*	*	*	none			
<input type="checkbox"/>	✓	0/0 B	IPv4 TCP	ADMIN net	*	10.1.1.2	80 (HTTP)	*	none		
<input type="checkbox"/>	✓	0/0 B	IPv4 TCP	ADMIN net	*	10.1.1.2	22 (SSH)	*	none		
<input type="checkbox"/>	✓	0/0 B	IPv4 TCP	ADMIN net	*	10.1.1.2	443 (HTTPS)	*	none		
<input type="checkbox"/>	✓	0/0 B	IPv4 TCP	LAN net	*	10.1.1.2	80 (HTTP)	*	none		
<input type="checkbox"/>	✓	0/0 B	IPv4 TCP	LAN net	*	10.1.1.2	443 (HTTPS)	*	none		

↑ Add

↓ Add

Delete

Save

Separator

VI. Install and configure web server

1. Install Apache2

Reference: <https://www.digitalocean.com/community/tutorials/how-to-install-the-apache-web-server-on-ubuntu-20-04>

Run the command:

```
$ sudo apt install apache2
```

```
minh@webserver:~$ sudo apt install apache2
[sudo] password for minh:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  apache2-bin apache2-data apache2-utils libapr1 libaprutil1 libaprutil1-dbd-sqlite3 libaprutil1-ldap libjansson4 liblua5.2-0 ssl-cert
Suggested packages:
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom www-browser openssl-blacklist
The following NEW packages will be installed:
  apache2 apache2-bin apache2-data apache2-utils libapr1 libaprutil1 libaprutil1-dbd-sqlite3 libaprutil1-ldap libjansson4 liblua5.2-0 ssl-cert
0 upgraded, 11 newly installed, 0 to remove and 0 not upgraded.
Need to get 1,864 kB of archives.
After this operation, 8,080 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://archive.ubuntu.com/ubuntu focal/main amd64 libapr1 amd64 1.6.5-1ubuntu1 [91.4 kB]
Get:2 http://archive.ubuntu.com/ubuntu focal/main amd64 libaprutil1 amd64 1.6.1-4ubuntu2 [84.7 kB]
Get:3 http://archive.ubuntu.com/ubuntu focal/main amd64 libaprutil1-dbd-sqlite3 amd64 1.6.1-4ubuntu2 [10.5 kB]
Get:4 http://archive.ubuntu.com/ubuntu focal/main amd64 libaprutil1-ldap amd64 1.6.1-4ubuntu2 [8,736 B]
Get:5 http://archive.ubuntu.com/ubuntu focal/main amd64 libjansson4 amd64 2.12-1build1 [28.9 kB]
Get:6 http://archive.ubuntu.com/ubuntu focal/main amd64 liblua5.2-0 amd64 5.2.4-1.1build3 [106 kB]
Get:7 http://archive.ubuntu.com/ubuntu focal/main amd64 apache2-bin amd64 2.4.41-4ubuntu3 [1,179 kB]
74% [7 apache2-bin 1,146 kB/1,179 kB 97%] 1,962 B/s 3min 17s
Get:8 http://archive.ubuntu.com/ubuntu focal/main amd64 apache2-data all 2.4.41-4ubuntu3 [159 kB]
Get:9 http://archive.ubuntu.com/ubuntu focal/main amd64 apache2-utils amd64 2.4.41-4ubuntu3 [83.3 kB]
Get:10 http://archive.ubuntu.com/ubuntu focal/main amd64 apache2 amd64 2.4.41-4ubuntu3 [95.5 kB]
Get:11 http://archive.ubuntu.com/ubuntu focal/main amd64 ssl-cert all 1.0.39 [17.0 kB]
Fetched 1,864 kB in 13s (147 kB/s)
Preconfiguring packages ...
Selecting previously unselected package libapr1:amd64.
(Reading database ... 70848 files and directories currently installed.)
Preparing to unpack .../00-libapr1_1.6.5-1ubuntu1_amd64.deb ...
Unpacking libapr1:amd64 (1.6.5-1ubuntu1) ...
Selecting previously unselected package libaprutil1:amd64.
Preparing to unpack .../01-libaprutil1_1.6.1-4ubuntu2_amd64.deb ...
Unpacking libaprutil1:amd64 (1.6.1-4ubuntu2) ...
^[[SSelecting previously unselected package libaprutil1-dbd-sqlite3:amd64.
Preparing to unpack .../02-libaprutil1-dbd-sqlite3_1.6.1-4ubuntu2_amd64.deb ...
Unpacking libaprutil1-dbd-sqlite3:amd64 (1.6.1-4ubuntu2) ...
Selecting previously unselected package libaprutil1-ldap:amd64.
Preparing to unpack .../03-libaprutil1-ldap_1.6.1-4ubuntu2_amd64.deb ...
Unpacking libaprutil1-ldap:amd64 (1.6.1-4ubuntu2) ...
Progress: [ 16%] [#####]
```

Check Ubuntu firewall for this app (Optional: if the Ubuntu firewall is active)

```
$ sudo ufw app list
```

```
minh@webserver:~$ sudo ufw app list
Available applications:
  Apache
  Apache Full
  Apache Secure
  OpenSSH
minh@webserver:~$
```

Allow Apache service on Ubuntu firewall

```
$ sudo ufw allow 'Apache'
```

```
minh@webserver:~$ sudo ufw allow 'Apache'
Rules updated
Rules updated (v6)
minh@webserver:~$
```

You can verify the change by typing:

```
$ sudo ufw status
```

2. Configure web server

Check with the systemd init system to make sure the service is running by typing:

```
$ sudo systemctl status apache2
```

```
minh@webserver:~$ sudo systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: enabled)
   Active: active (running) since Thu 2020-11-26 03:08:28 UTC; 14min ago
     Docs: https://httpd.apache.org/docs/2.4/
    Main PID: 1664 (apache2)
      Tasks: 55 (limit: 2205)
     Memory: 5.1M
    CGroup: /system.slice/apache2.service
            └─1664 /usr/sbin/apache2 -k start
              └─1666 /usr/sbin/apache2 -k start
                └─1667 /usr/sbin/apache2 -k start

Nov 26 03:08:28 webserver systemd[1]: Starting The Apache HTTP Server...
Nov 26 03:08:28 webserver apachectl[1663]: AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.0.1
Nov 26 03:08:28 webserver systemd[1]: Started The Apache HTTP Server.
lines 1-15/15 (END)
```

Or

```
$ netstat -nca | grep :80
```

```
minh@webserver:~$ netstat -nca | grep :80
tcp6      0      0 :::80          :::*           LISTEN
tcp6      0      0 :::80          :::*           LISTEN
tcp6      0      0 :::80          :::*           LISTEN
tcp6      0      0 :::80          :::*           LISTEN
tcp6      0      0 :::80          :::*           LISTEN
tcp6      0      0 :::80          :::*           LISTEN
```

VII. Test your firewall rules

1. Test connection session from WAN to DMZ

You can use your real machine (laptop) or Kali Linux VM

Setting the correct IP address of the virtual interface that connect to Default Switch of Hyper-V

Use the nmap to scan port to make sure that you can see the 443 port only.

2. Test connection session from USER network to DMZ

Similar to the 1st test above

3. Test connection session from ADMIN network to DMZ

Similar to the 1st test above

Test SSH, you can use the Kali Linux to SSH to Web Server. Before this, you should enable the SSH service on web server first.

4. Try to change the order of rules or try with some incorrect configuration

5. Conclusion

DocumentUltimate