ITI EC3 Task

Documentation Cloud Task

Supervision

Dr.Mohammed Adly

Monitors

Eng. Mai Mostafa

Eng. Ekram Abd-Elwhab

By

Ahmed Hussein Saleh

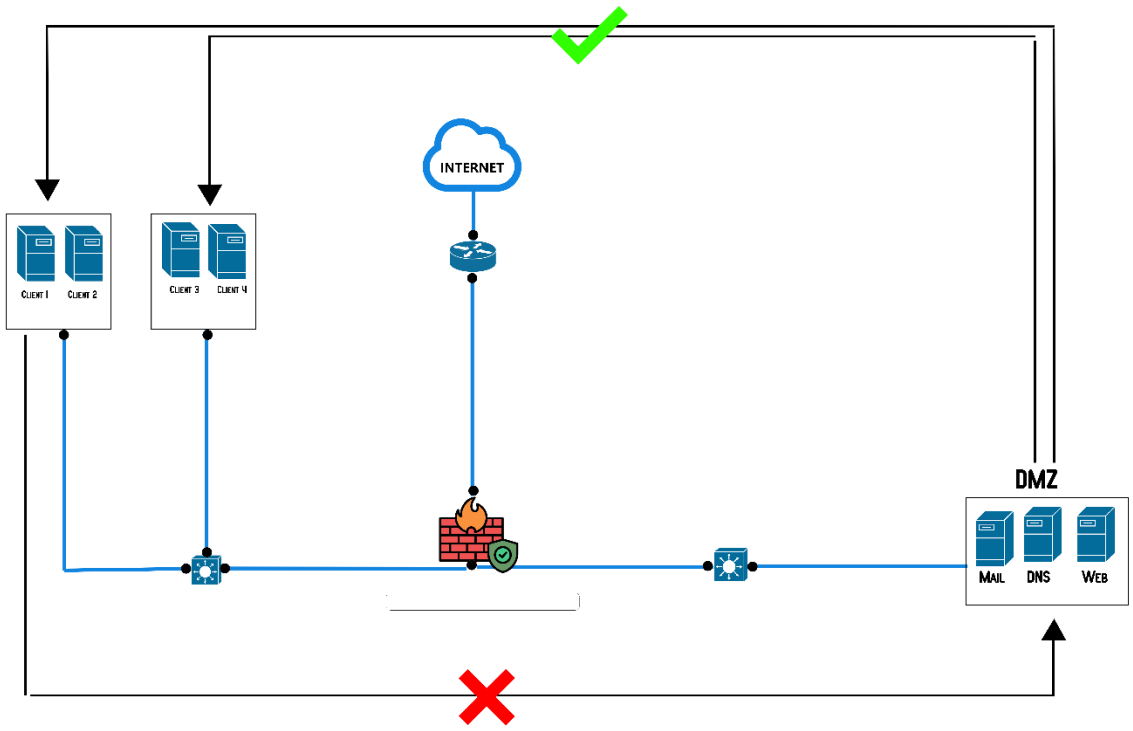
Amir Mohammed Saleh

ITI EC3 Task

Content Table

ITI EC3 Task

We want to implement this topology



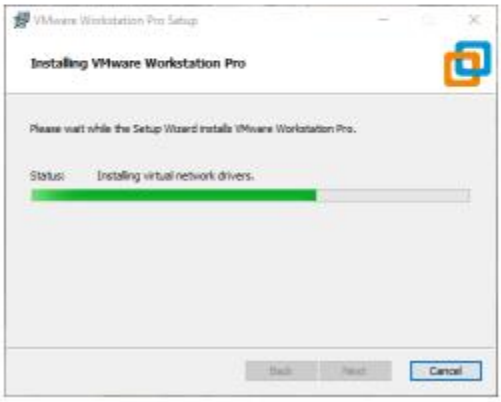
Requirements :

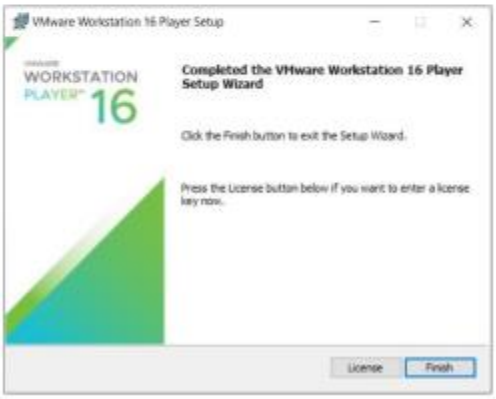
1- Work on any virtualization environment
2- Install on DMZ servers (DNS – WebMail)
3- Install Router as vm
4- Install 2 Switch (Layer 3 or layer2) as vm
5- Install 4 Clients on the left side to access web server and mail server
6- Configure router and firewall to access the internet
7- Separate the topology into 6 Networks
8- Configuration on firewall
    - Allow any host or server can access the internet
    - Allow any server from the right side can ping or communicate any host from the left side
    - Allow any server from the right side to log to the firewall and make changes on configuration on specific ports and deny any hosts from wan or lan
    - Allow the host to access only the web server and mail server on a specific port
    - Deny not reject any host go ping on server or firewall or router

ITI EC3 Task

- **The first step**
  Preparing work environment (Download VMWare WorkStaion and install it)
  - Install VMware Workstation

    You can download it from the official site VMware link https://www.vmware.com/
  - Double click on icon VMware Work station





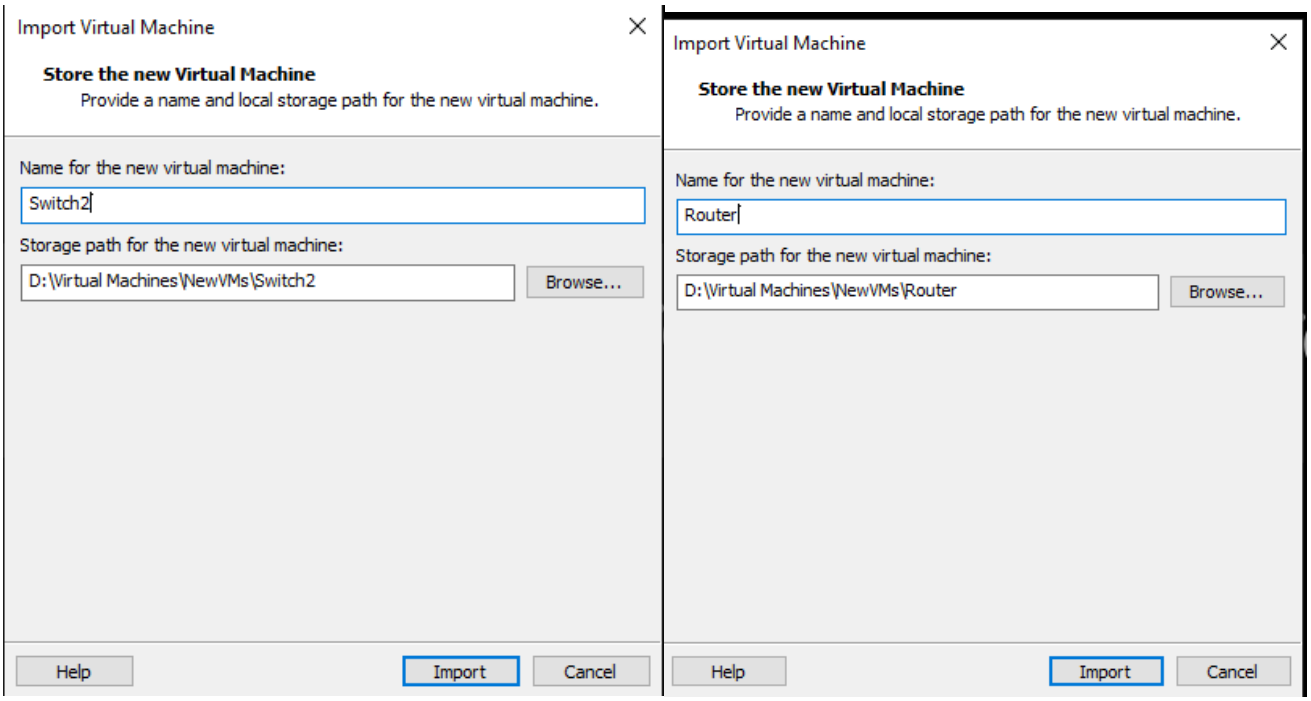
- **Second Step Download Machines as iso** from the Official Site
  1- **Router (Cisco V1000)**
  2- **Switch (Arouba Switch Layer3)**
  3- **Firewall (PfSense)**
  4- **Windows Server 2019**
  5- **Install ubuntu**
  6- **Windows 10**
  7- **Windows 7**

ITI EC3 Task

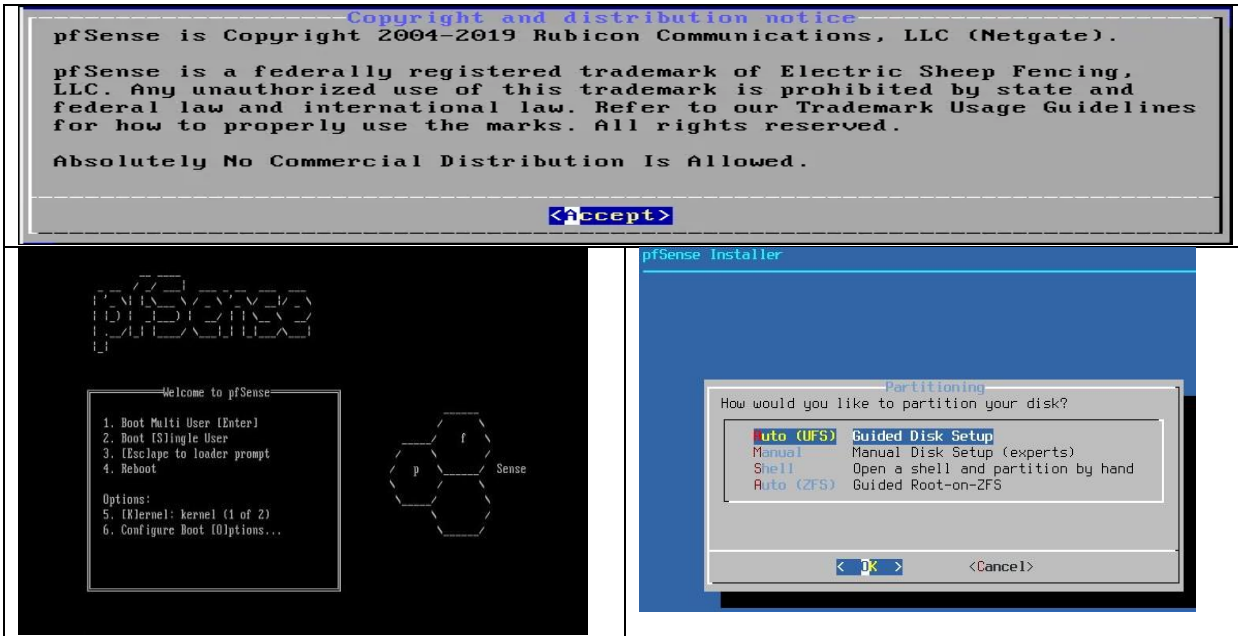
- **The third step install Machiens as VMs on Vmware Workstation v17.2**

1- Router Cisco has Pre Installed just import it or install it on VMware

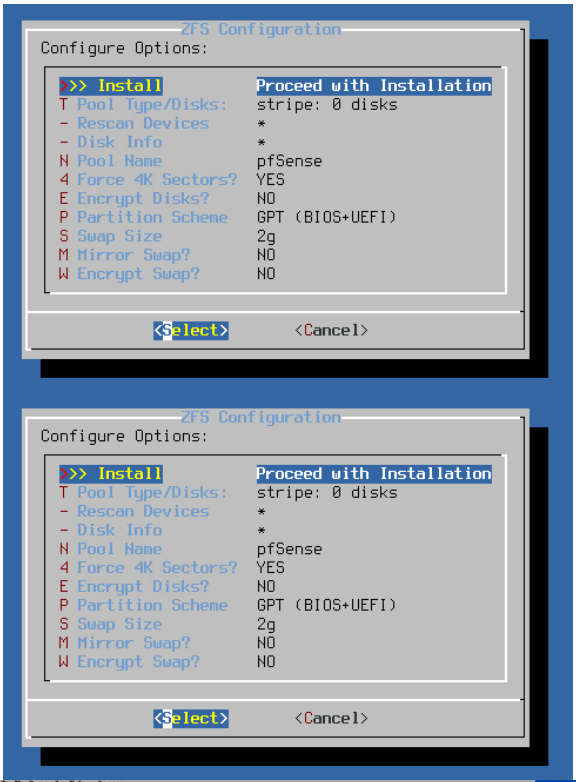
2- Arouba Switch Is preInstalled just import it or install it on VMware



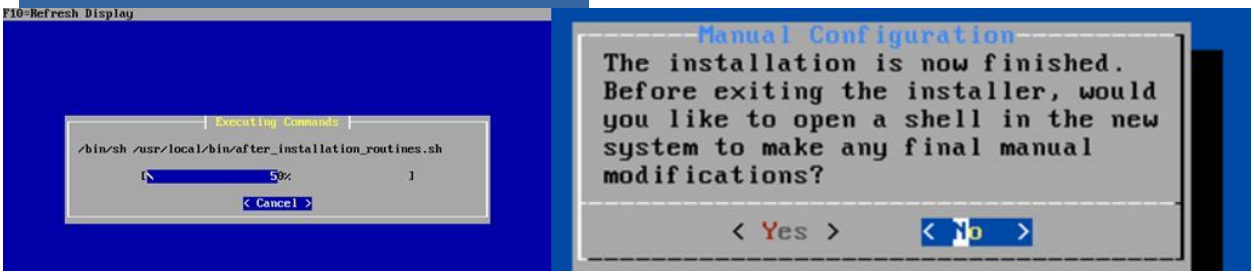
3- install PfSense iso Img

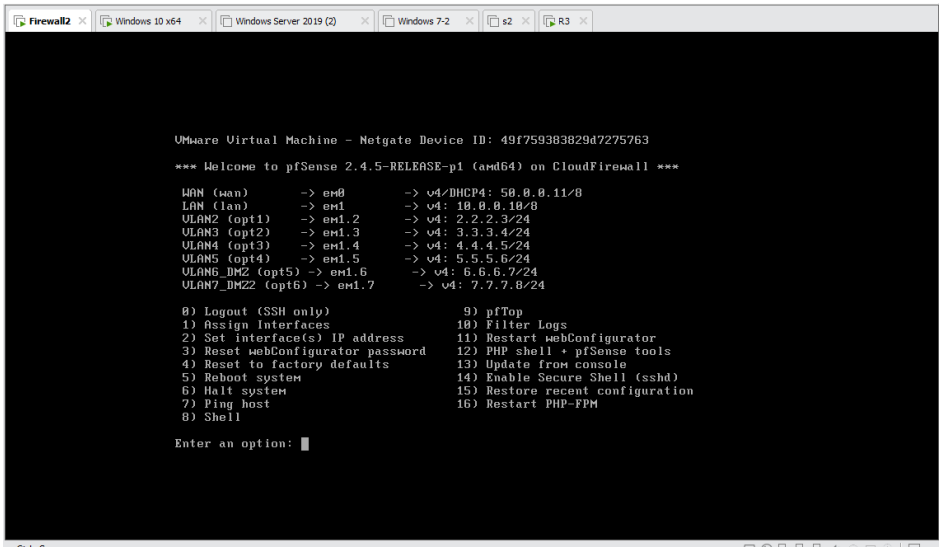


ITI EC3 Task


ZFS Configuration
Configure Options:
>>> Install Proceed with Installation
T Pool Type/Disks: stripe: 0 disks
- Rescan Devices *
- Disk Info *
N Pool Name pfSense
4 Force 4K Sectors? YES
E Encrypt Disks? NO
P Partition Scheme GPT (BIOS+UEFI)
S Swap Size 2g
M Mirror Swap? NO
W Encrypt Swap? NO
<Select> <Cancel>
ZFS Configuration
Configure Options:
>>> Install Proceed with Installation
T Pool Type/Disks: stripe: 0 disks
- Rescan Devices *
- Disk Info *
N Pool Name pfSense
4 Force 4K Sectors? YES
E Encrypt Disks? NO
P Partition Scheme GPT (BIOS+UEFI)
S Swap Size 2g
M Mirror Swap? NO
W Encrypt Swap? NO
<Select> <Cancel>

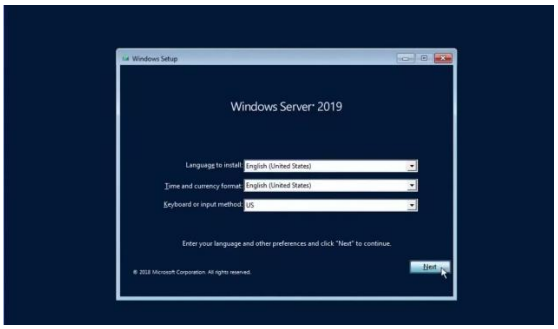

freebsd12.0 on QEMU/KVM
File Virtual Machine View Send Key
pfSense Installer
Copyright and distribution notice
pfSense is Copyright 2004-2020 Rubicon Communications, LLC (Netgate).
pfSense is a federally registered trademark of Electric Sheep Fencing, LLC. Any unauthorized use of this trademark is prohibited by state and federal law and international law. Refer to our Trademark Usage Guidelines for how to properly use the marks. All rights reserved.
Absolutely No Commercial Distribution Is Allowed.
<Accept>
pfSense Installer
Keymap Selection
The system console driver for pfSense defaults to standard "US" keyboard map. Other keymaps can be chosen below.
>>> Continue with default keymap
-> Test default keymap
( ) Armenian phonetic layout
( ) Belarusian Codepage 1131
( ) Belarusian Codepage 1251
( ) Belarusian ISO-8859-5
( ) Belgian ISO-8859-1
( ) Belgian ISO-8859-1 (accent keys)
( ) Brazilian Z75 Codepage 850
( ) Brazilian Z75 ISO-8859-1
( ) Brazilian Z75 ISO-8859-1 (accent keys)
( ) Bulgarian (BDS)
<Select> <Cancel>
[Press arrows, TAB or ENTER]

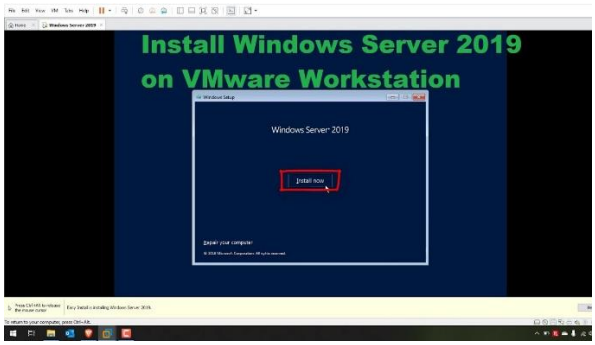

F10=Refresh Display
Executing Commands
/bin/sh /usr/local/bin/after_installation_routines.sh
50%
< Cancel >
Manual Configuration
The installation is now finished.
Before exiting the installer, would you like to open a shell in the new system to make any final manual modifications?
< Yes >
< No >

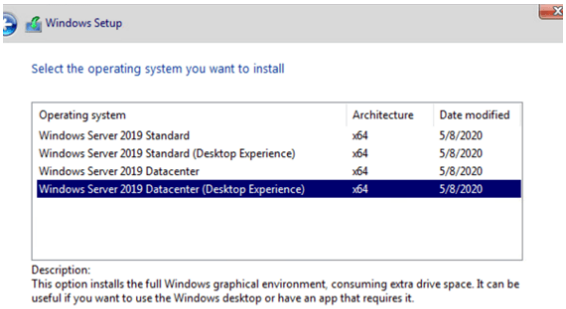

Firewall2
Windows 10 x64
Windows Server 2019 (2)
Windows 7-2
s2
R3
VMware Virtual Machine - Netgate Device ID: 49f759383829d7275763
*** Welcome to pfSense 2.4.5-RELEASE-p1 (amd64) on CloudFirewall ***
WAN (wan) -> em0 -> v4/DHCP4: 50.0.0.11/8
LAN (lan) -> em1 -> v4: 10.0.0.10/8
VLAN2 (opt1) -> em1.2 -> v4: 2.2.2.3/24
VLAN3 (opt2) -> em1.3 -> v4: 3.3.3.4/24
VLAN4 (opt3) -> em1.4 -> v4: 4.4.4.5/24
VLAN5 (opt4) -> em1.5 -> v4: 5.5.5.6/24
VLAN6_DMZ (opt5) -> em1.6 -> v4: 6.6.6.7/24
VLAN7_DMZ2 (opt6) -> em1.7 -> v4: 7.7.7.8/24
0) Logout (SSH only)
1) Assign Interfaces
2) Set interface(s) IP address
3) Reset webConfigurator password
4) Reset to factory defaults
5) Reboot system
6) Halt system
7) Ping host
8) Shell
9) pfTop
10) Filter Logs
11) Restart webConfigurator
12) PHP shell + pfSense tools
13) Update from console
14) Enable Secure Shell (sshd)
15) Restore recent configuration
16) Restart PHP-FPM
Enter an option:

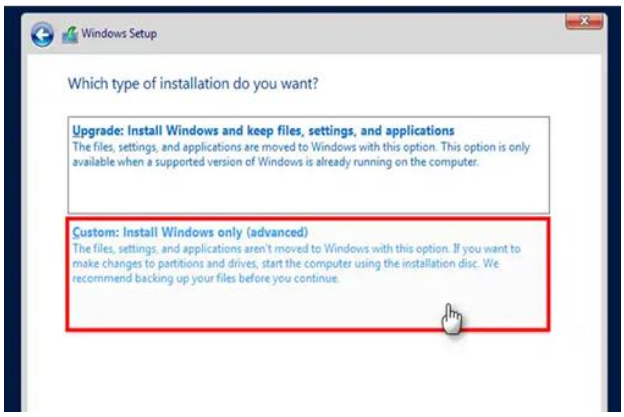
ITI EC3 Task

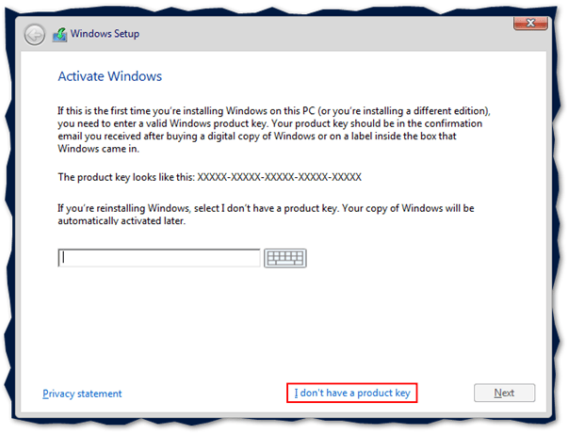
4- install Windows server 2019

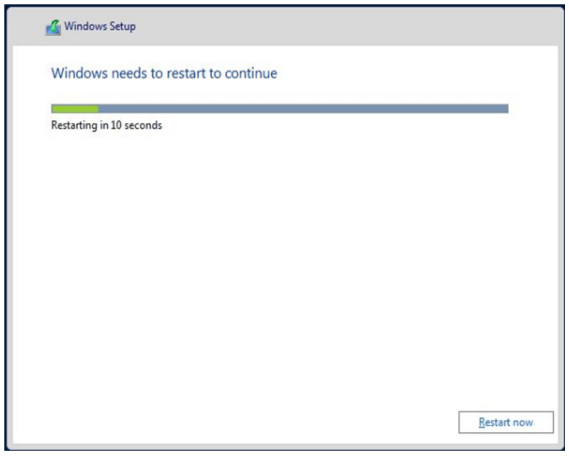






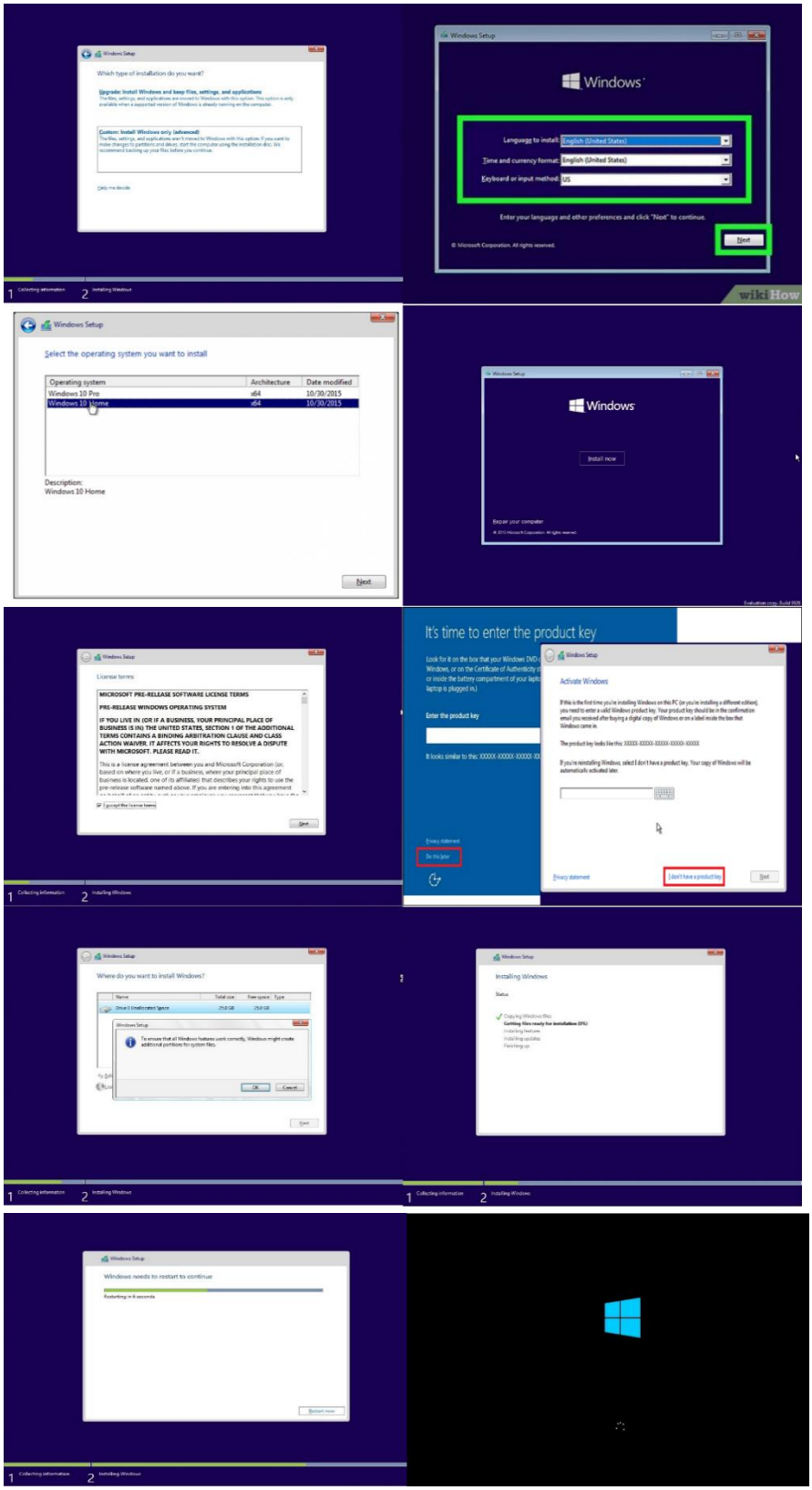






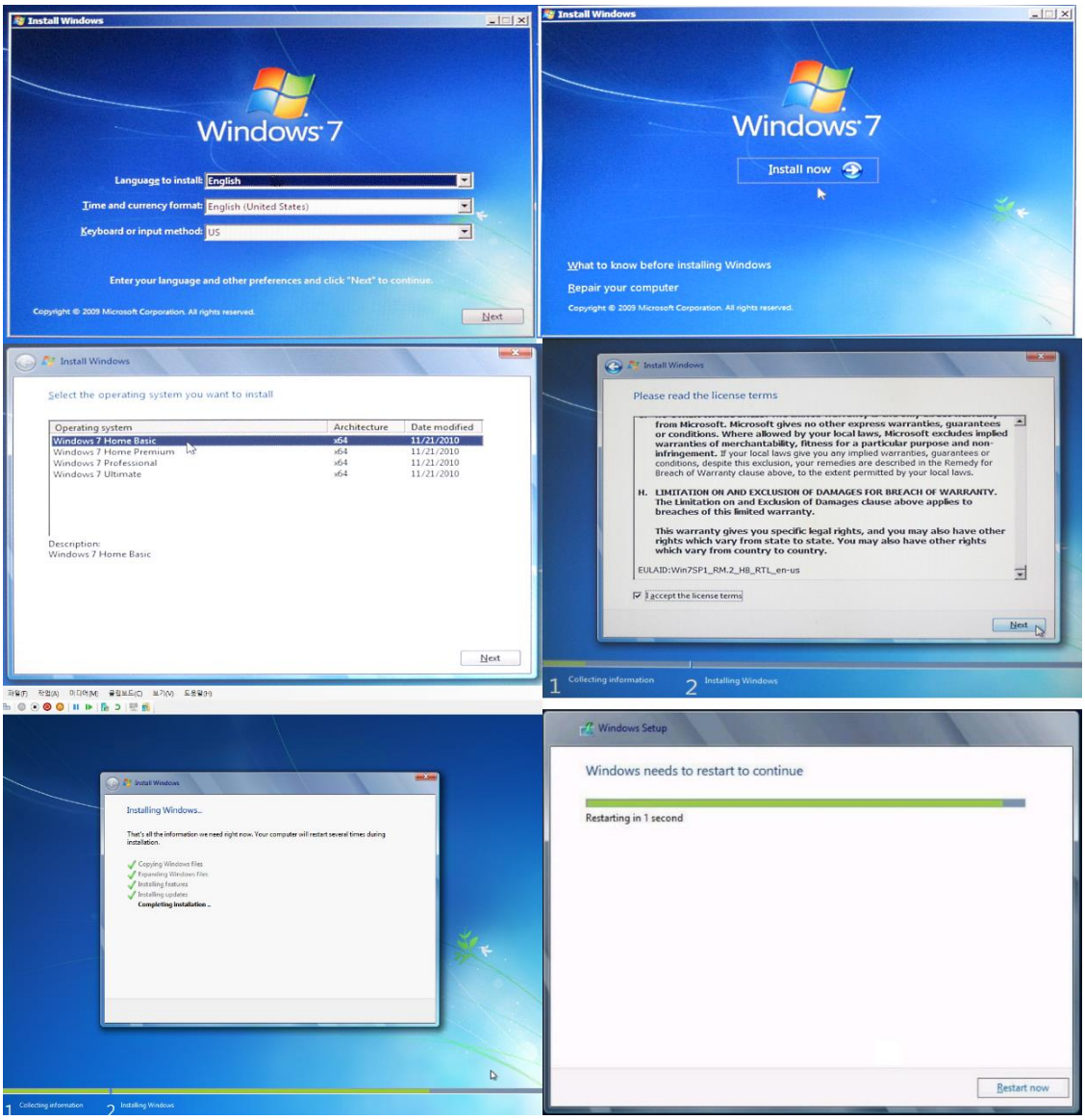
ITI EC3 Task

8- INSTALL WINDOWS 10



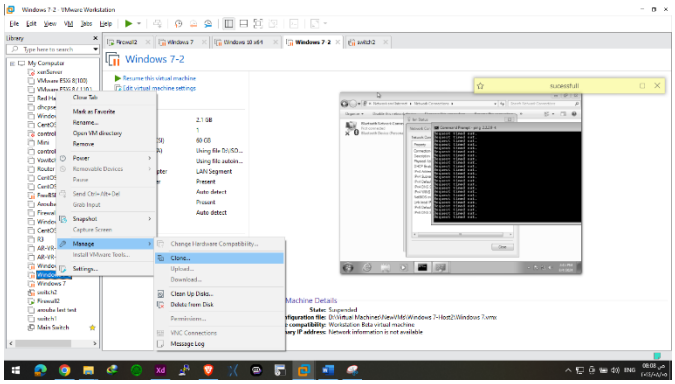
ITI EC3 Task

9- Install Windows 7 and clone it to be 2 Machines



ITI EC3 Task

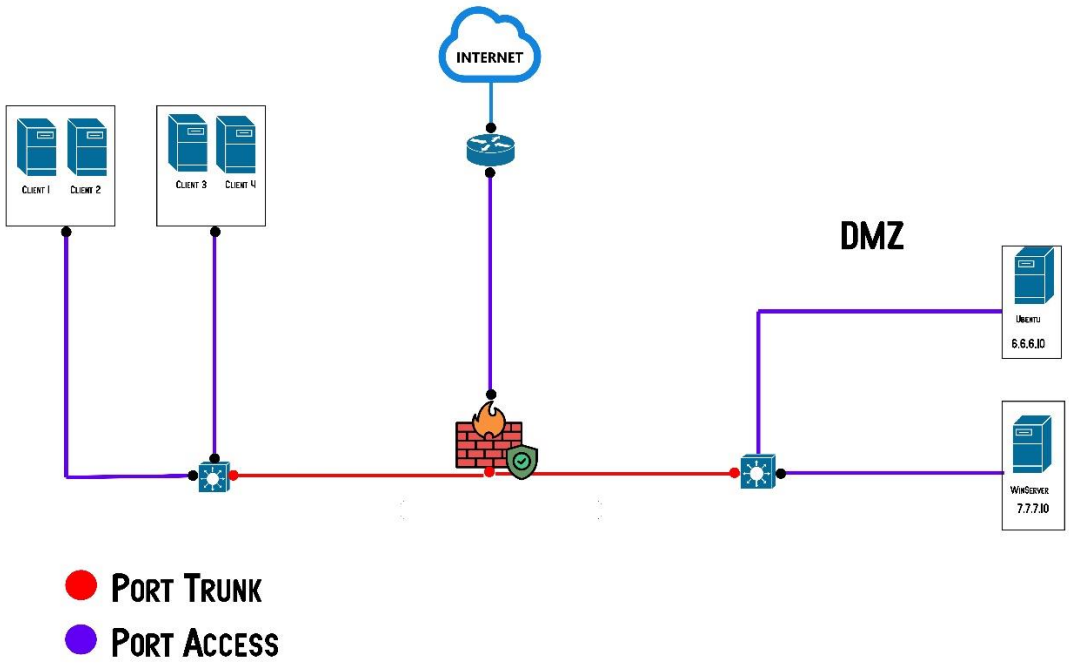
- **Clone Windows 7 on Vmware to act as 2 machine**



We will install 2 Server on Different Vlans

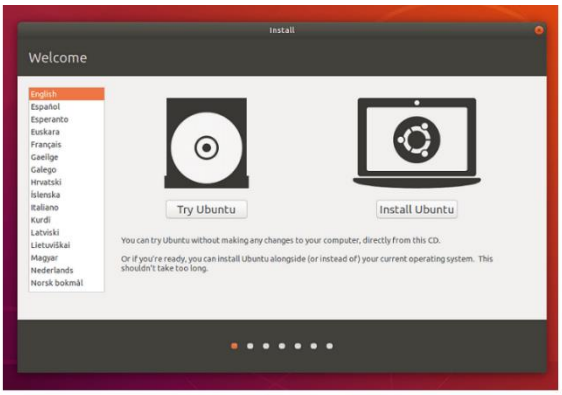
- vlan 6.6.6.6 Ubuntu Desktop
  Server Ip 6.6.6.10
- vlan 7.7.7.7 Windows server
  Windows Server 7.7.7.10

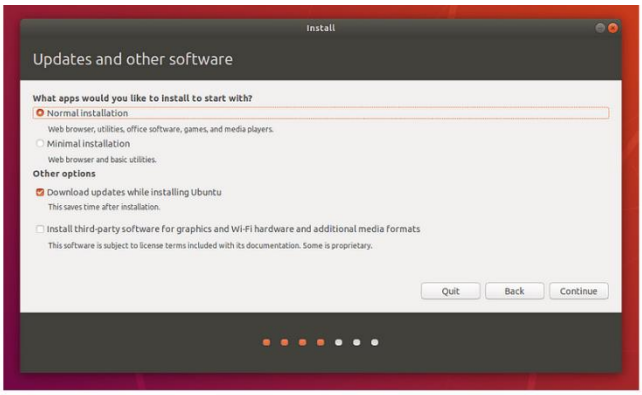
we will continue all work on the Windowsows server

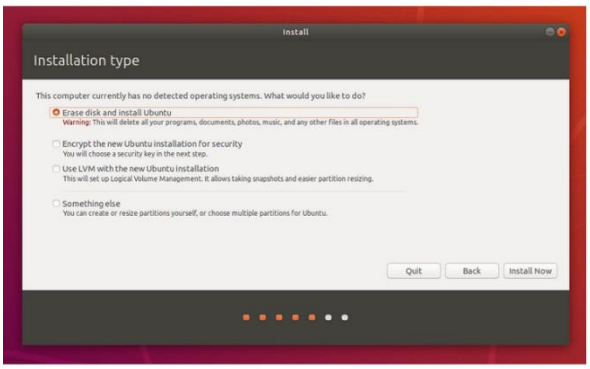


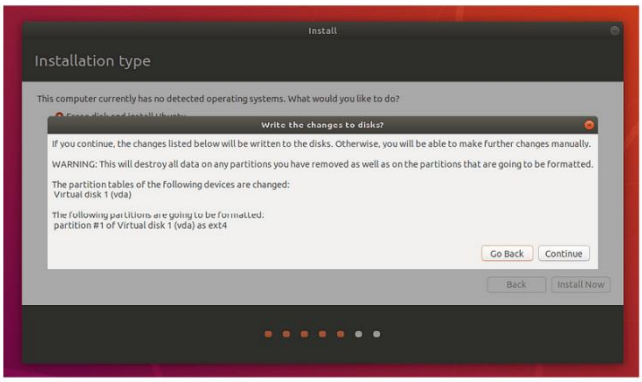
ITI EC3 Task

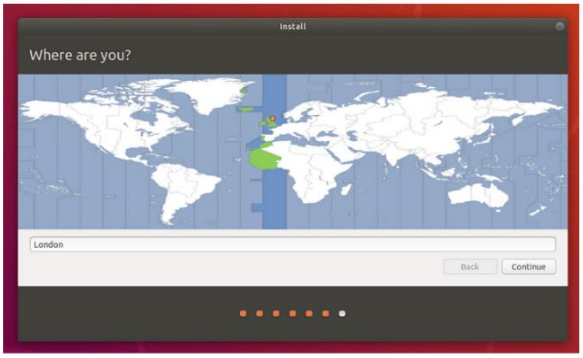
10-Install Ubuntu to act as a Mail Server

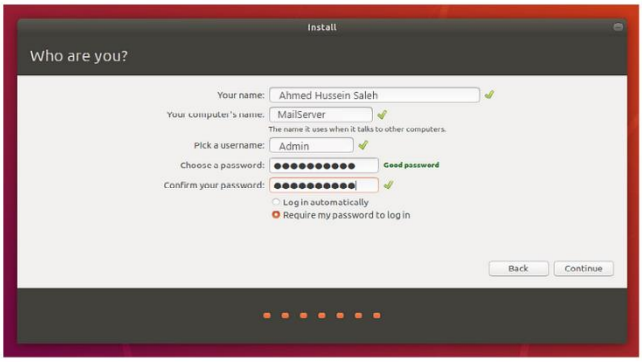


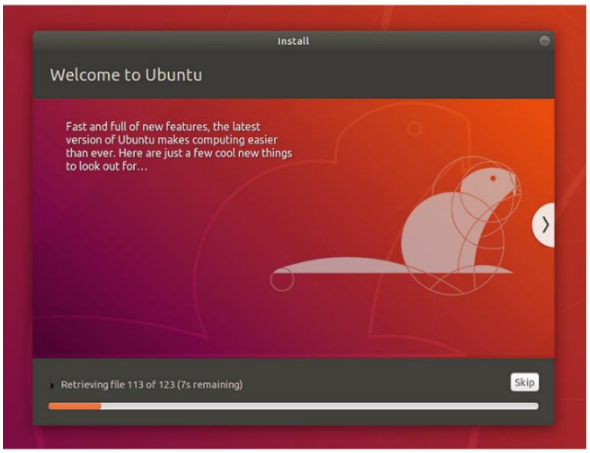


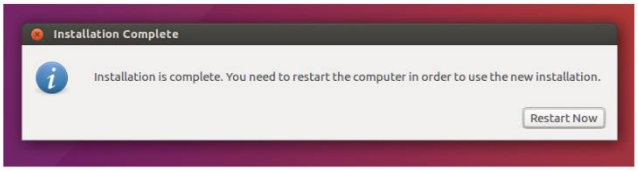












ITI EC3 Task

Configuring the DNS Server for An Ubuntu Mail Server:

Just follow this step-by-step guide, and you shouldn't have any problems setting up the configuration!

1. Log In and Update Your Server

Open terminal

- apt-get update

2. Install Bind

To configure a DNS server that will use Postfix we'll need an additional tool – Bind. Let's install it first:

- sudo apt install bind9

3. Configure /var/cache/db.test

At this point, we must take into account that the IP address of our Ubuntu machine is **7.7.7.100**, it is necessary to replace it with the IP address where we will perform the installation. For this example, we'll use mail.test.com as a FQDNS.

So, now it is necessary to create a new zone for our example. To do this, create a new file with the zone information.

- sudo nano /var/cache/bind/db.test

Then, add the following:

```
$ORIGIN test.com.
$TTL 1D
@       IN SOA    ns1 root(
            1 ;serial
            1D ;refresh
            2H ;retry
            2W ;expire
            5H ;minimum
);
@       IN       NS ns1
ns1     IN       A 7.7.7.100
mail    IN       A 7.7.7.100
@       IN       MX 5 mail
```

Remember, we must replace the IP address with that of your server, and change the domain to the one you wish to use. Press **CTRL+O** to save the changes and **CTRL+X** to close the nano editor.

4. Add a New Zone to Bind the Configuration

Before enabling the newly created zone it is necessary to check the configuration of the file.

```
sudo named-checkzone test.com. /var/cache/bind/db.test
```

Now we can add our new zone to the Bind zone configuration file. To do this, run the following command:

```
sudo nano /etc/bind/named.conf.default-zones
```

And add the new zone:

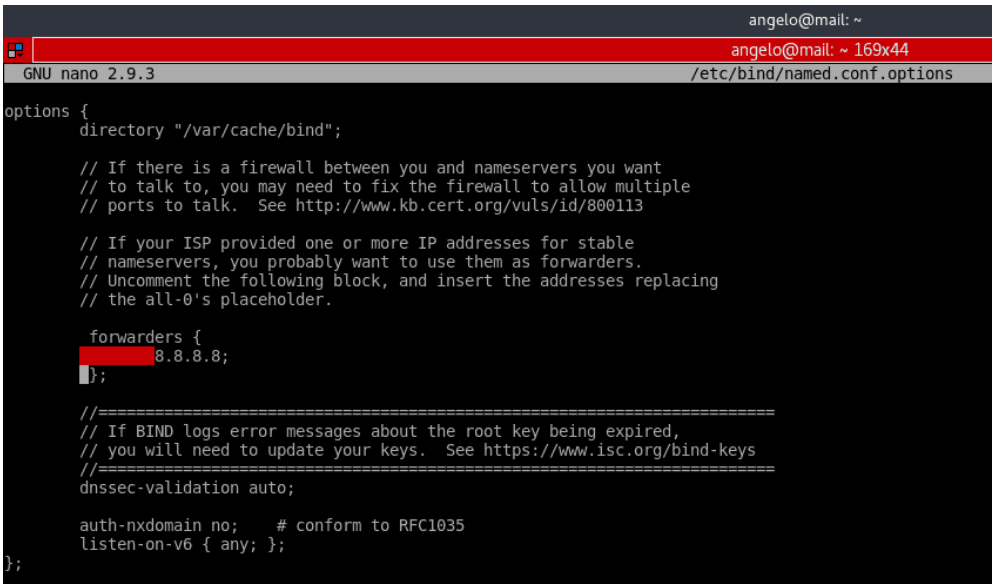
```
zone "test.com." {
    type master;
    file "db. test";
};
```

Again, **CTRL+O** to save the changes and **CTRL+X** to close it.

5. Configure /etc/bind/named.conf.options

Now, in the file **/etc/bind/named.conf.options** it is necessary to uncomment the forwarders line and include the Google DNS – **8.8.8.8**. For that simply remove the **//** symbols as shown in the screenshot below.

```
sudo nano /etc/bind/named.conf.options
```



6. Restart Bind

Now, we have to restart the bind9 service. You can do it with one of two commands:

```
sudo systemctl reload bind9
```

or

```
sudo systemctl restart bind9
```

ITI EC3 Task

How to Install and Setup Mail Server on Ubuntu

We're almost there, your Ubuntu email server is ready to come online. Here's what you should do:

1. Install Postfix Email Server

Now it is time to install Postfix. Postfix is an email server written in C. Its main feature is the speed of execution and open-source nature. Install it with the following command:

```
sudo apt install postfix
```

During installation, we will be asked to configure the package. On the first screen, choose the option Internet Site.

Then, we have to enter the name of the server. In this case **test.com**.

Postfix is very flexible and allows extensive configuration, but for this tutorial, we'll fix it with the default configuration.

2. Add User

Then, we have to add our user to the group mail:

```
sudo usermod -aG mail $(whoami)
```

After that, we have to create the users and add them to the mail group so they can send and receive mail. I'll add Gabriel:

```
sudo useradd -m -G mail -s /bin/bash/ gabriel
```

Then, we need to set a password to the newly created user:

```
sudo passwd Gabriel
```

ITI EC3 Task

Test the Ubuntu Mail Server

Now to prove what we just did. We will send and receive an email from the terminal. To do this, we will install the mailutils package:

sudo apt install mailutils

Next, we send an email to the other email account user named gabriel. Type in the subject and the message. After that, press **CTRL+D** to finish. To start writing an email enter the following command:

```
mail gabriel@test.com
```

Now we can log into another user and check the mail utility.

There, after running the **mail** command, we will see the email we just sent to the other test user. To access the email just write the number of the mail, in this case, **1**.

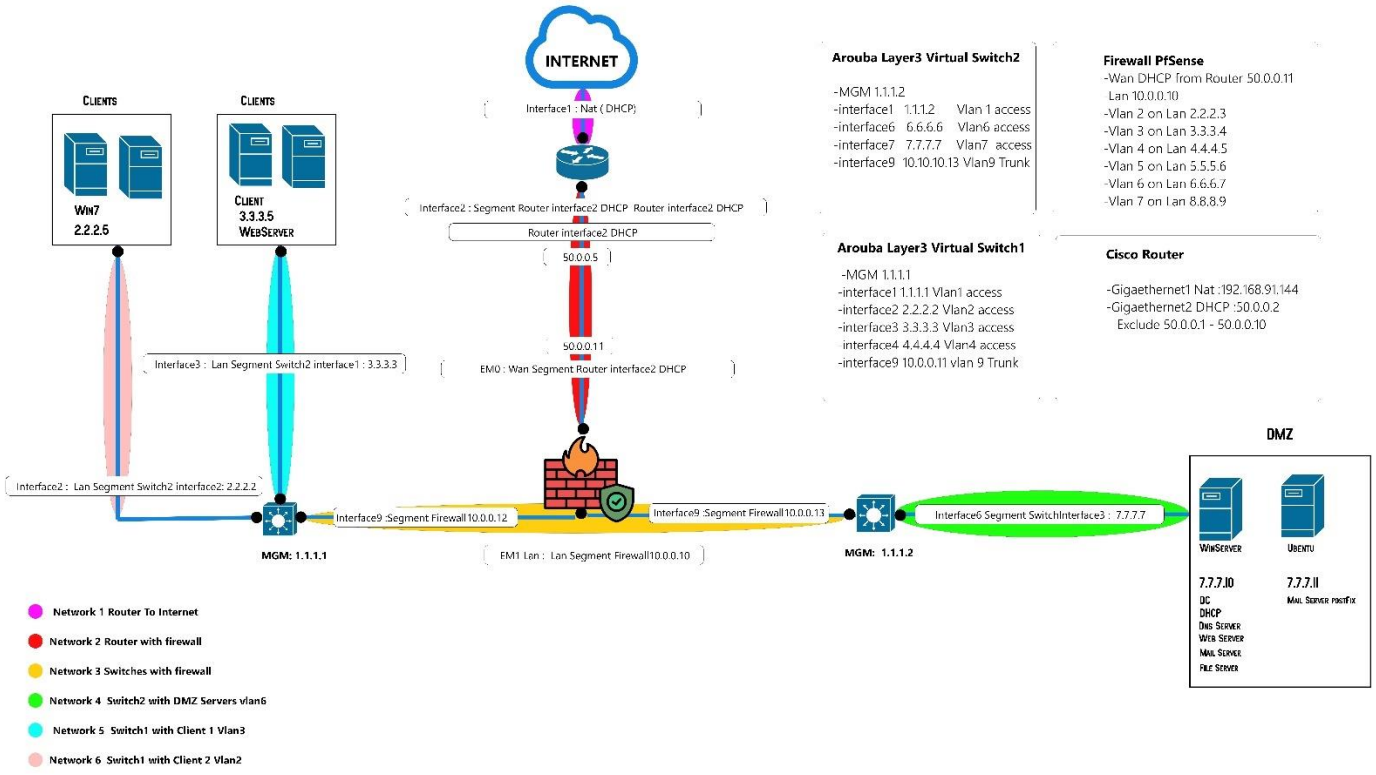
To test outbound emails from this user, just try another email address:

```
mail angelo@test.com
```

That's it! You're sending emails from your very own email server on Ubuntu.

ITI EC3 Task

Network Desing and subnetting



We will devide the topology into 6 networks

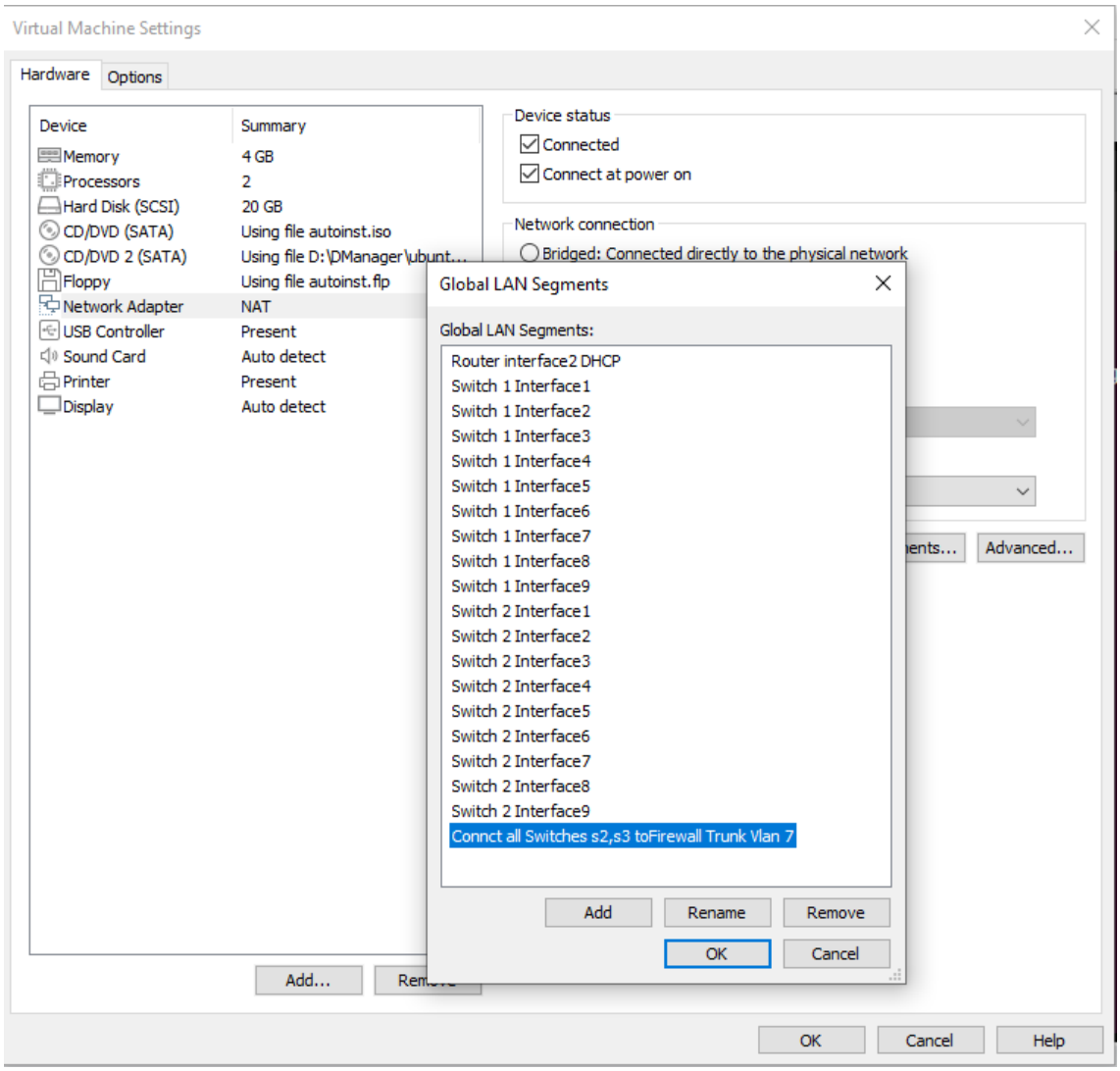
- **Network 1 Router To Internet (NAT 192.168.91.200)**
- **Network 2 Router with firewall (DHCP from Router 50.0.0.0)**
- **Network 3 Switches with firewall Vlan 9 in switches and interface 2 Lan on Firewall**
- **Network 4 Switch2 interface6 with DMZ Servers vlan6 Trunk**
- **Network 5 Switch1 with Client 1 Vlan3 access**
- **Network 6 Switch1 with Client 2 Vlan2 access**

ITI EC3 Task

Configuration Devices

1- Vmware WorkStaion Setting

-LAN segment on Network Adapters



We just want to create these LAN segments to isolate networks from each other and connect devices to specific networks or host

What are LAN Segments?

ITI EC3 Task

LAN Segments

- LAN Segments can be thought of as an isolated network environment. Any VMs in the segment can talk to each other but not to the outside world. It is like having the VMs on an isolated switch. Only by setting up some routing appliance or VM can external access be achieved. More on this later.

- DHCP is not available in the segment either, so any VMs joined to the segment will not receive an IP address unless you set up a DHCP server on a VM in the segment.

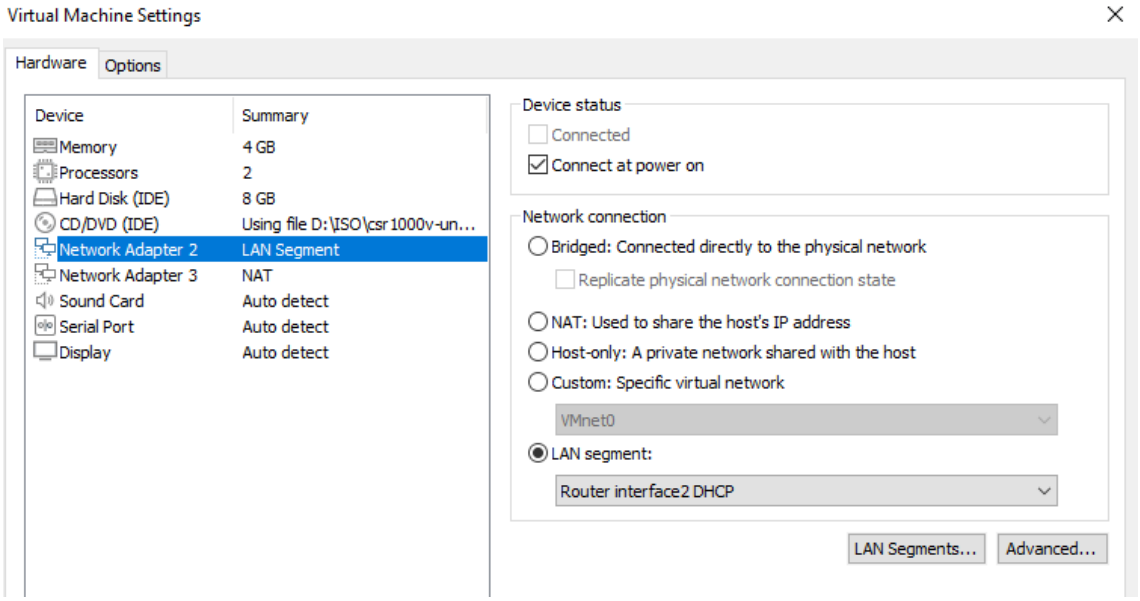
  Benefits and Drawbacks of LAN Segments
  I've gone over much of this in the post but to summarize the benefits of LAN Segments:

  - Provides a nice isolated network environment
  - Over 20 available LAN Segments (then again if you have over 20 Virtual Networks you may want to rethink your layout)
  - Easy to identify the network you are using
  - This is a tenuous one but if you are using Workstation on a computer you do not have admin rights on you can create/modify/delete LAN Segments without Admin rights. To edit Virtual Networks you do require Admin rights

ITI EC3 Task

Router Configuration

- We will add 2 network adapters to this machine router



- **the first one is configured as NAT to receive dhcp ip to connect to the internet**

```
Router >enable
Router  #   configure terminal
Router (Config)   interface Gigaethernet1
Router (config-if)   IP address dhcp
Router (config-if)   no sh
Router (Config)   end
Router >
```

- **the second step config interface** *Gigaethernet2* **as lan segment named "Router interface2 DHCP"**

```
Router >enable
Router  #   configure terminal
Router (Config)#   interface Gigaethernet1
Router (config-if ) #   ip address 50.0.0.5 255.0.0.0
Router (config-if)#   no sh
Router (config-if)#   end
Router >
```

ITI EC3 Task

- **the third step config dhcp Server IPs**

```
Router>enable
Router#configure terminal
Router(config)# ip dhcp pool firewall
Router(config)# network 50.0.0.0 255.0.0.0
Router(config)#  default-router 50.0.0.5
Router(config)# ip dhcp excluded-address 50.0.0.1 50.0.0.10
Router#exit
Router#end
Router>wr
Router>
```

Show interfaces

```
Router>show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet2       50.0.0.5        YES NVRAM  up                    up
GigabitEthernet3       192.168.91.141  YES DHCP   up                    up
Router>
```

Show dhcp pool

```
Router#show ip dhcp pool

Pool pool0 :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 16777214
 Leased addresses               : 0
 Excluded addresses             : 10
 Pending event                  : none
 1 subnet is currently in the pool :
 Current index        IP address range                    Leased/Excluded/Total
 50.0.0.1             50.0.0.1         - 50.255.255.254    0      / 10     / 16777
214
Router#_
```

Test Connectivity with the Internet

```
Router#ping 8.8.8.8 r 50
Type escape sequence to abort.
Sending 50, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (50/50), round-trip min/avg/max = 41/42/52 ms
Router#_
```

ITI EC3 Task

Switch 1 Configuration

- Lan segment configuration into VMWare

We will add 10 network adapter and Connect each card to its parallel

Just imagine it as a physical switch

Network adapter1 => Switch 1 interface1

Network adapter2 => Switch 1 interface2

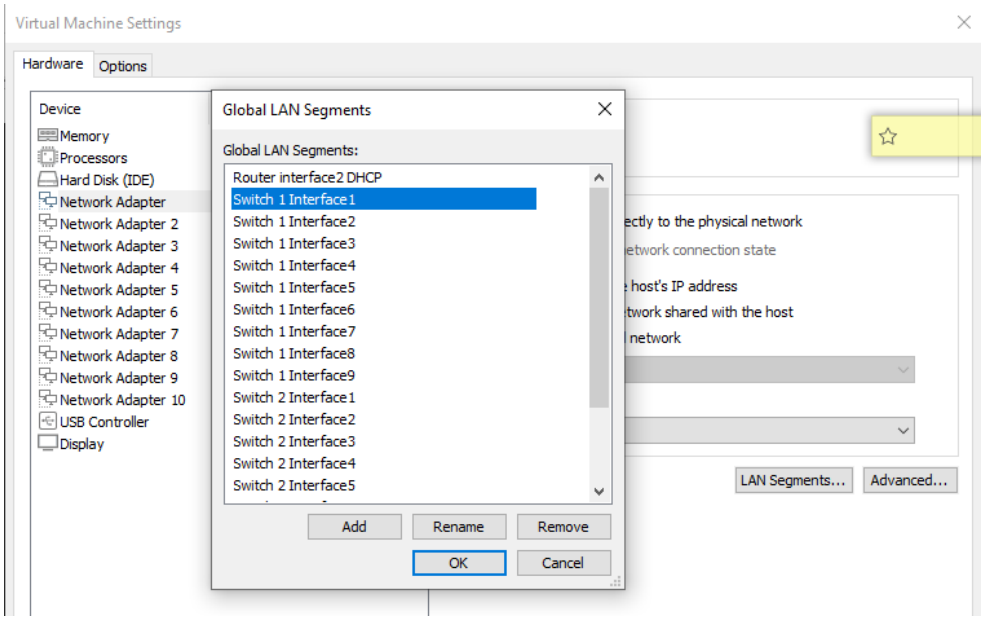
Network adapter3 => Switch 1 interface3

.

.

.

etc



- assign IP to management interface

```
Switch1(config)# interface mgmt
Switch1(config-if-mgmt)# no shutdown
Switch1(config-if-mgmt)# ip static 1.1.1.1/24
Switch1(config-if-mgmt)# default-gateway 192.168.91.2 (Nat Gateway)
```

- create vlans access connected to client 1 and client 2

```
switch(config)# valn1
```

```
switch(config)# interface vlan 1
```

ITI EC3 Task

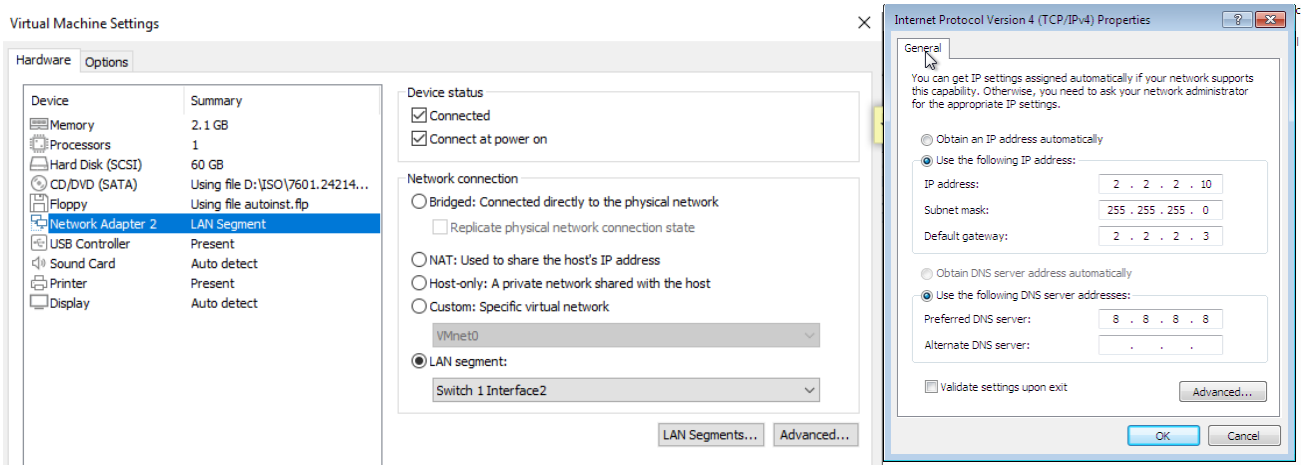
```
switch (config-if-vlan)# ip add 1.1.1.1 255.255.255.0

ip add 1.1.1.1 255.255.255.0 ip add 1.1.1.1 255.255.255.0ip add 1.1.1.1
255.255.255.00ip add 1.1.1.1 255.255.255.0ip add 1.1.1.1 255.255.255.0

switch config-if-vlan)#exit


switch(config)# valn2

switch(config)# interface vlan 2

switch(config-if-vlan)# ip add 2.2.2.2 255.255.255.0

switch(config-if-vlan)#exit


switch(config)# valn3

switch(config)# interface vlan 3

switch(config-if-vlan)# ip add 3.3.3.3 255.255.255.0

switch(config-if-vlan)#exit


switch(config) #interface 1/1/2

switch(config-if) #switchport access vlan 2

switch(config-if) #exit


switch(config) #interface 1/1/3

switch(config-if) #switchport access vlan 3

switch(config-if) #exit
```

- Create vlan trunk connect to Firewall

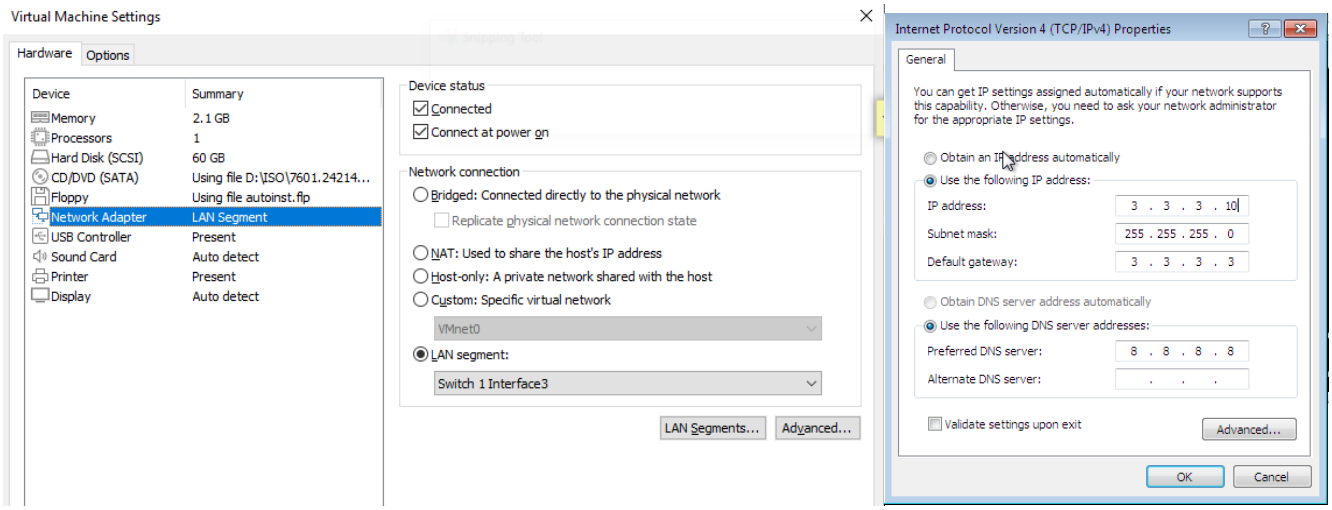
```
switch(config)# valn10

switch(config-if)# vlan trunk allowed all

switch(config)# interface vlan 10

switch (config-if-vlan)# ip address 10.0.0.12 255.255.255.0

switch (config-if-vlan)#exit



switch(config) #interface 1/1/9

switch(config-if) #switchport access vlan 10

switch(config-if) #exit
```

ITI EC3 Task

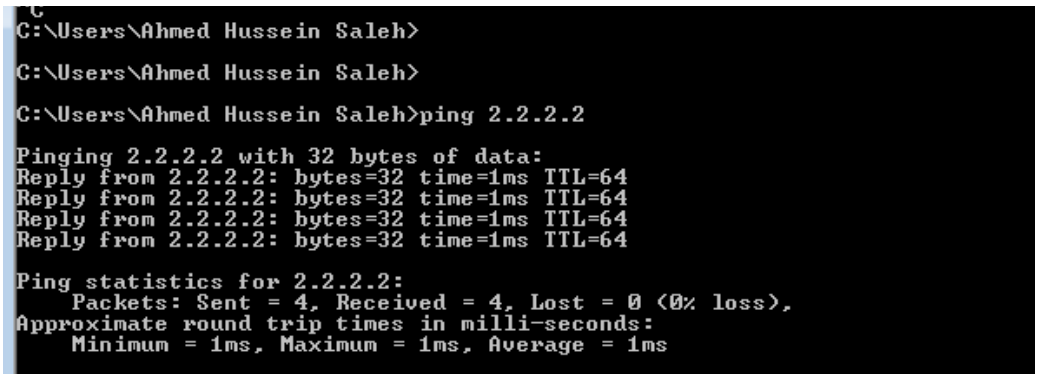
- Client 1 Configuration



- Client 2 Configuration

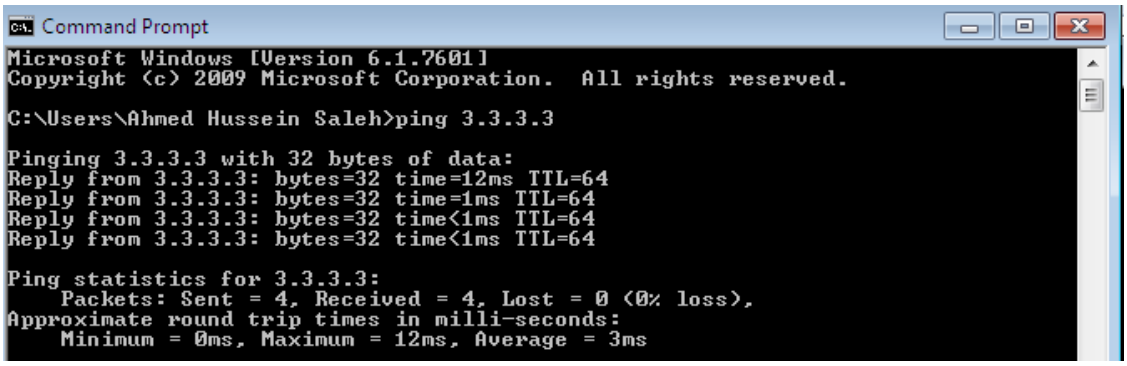


- check connectivity client 1 with switch 1

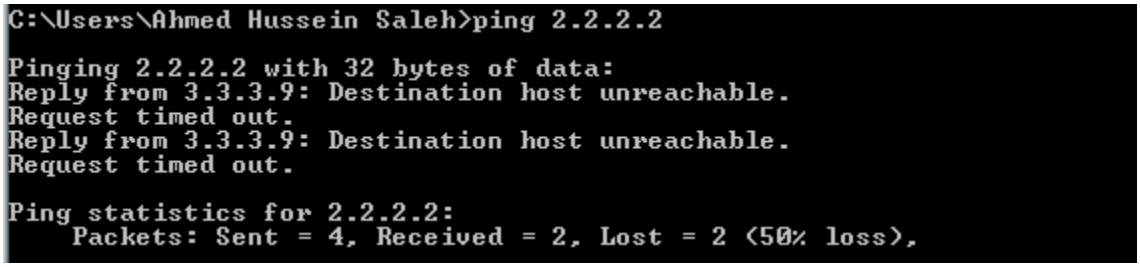


ITI EC3 Task

- check connectivity client 2 with switch 2



- check vlans is isolated



ITI EC3 Task

Swich2 Configuration to DMZ Servers

- Lan segment configuration into VMWare

We will add 10 network adapter and Connect each card to its parallel

Just imagine it as a physical switch just to imagin it as physical switch

Network adapter1 => Switch2 interface1

Network adapter2 => Switch2 interface2

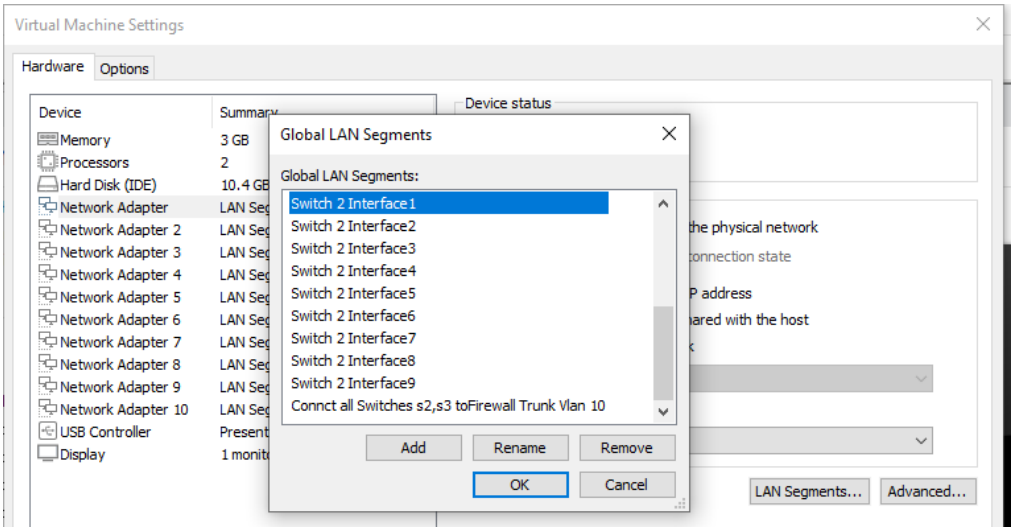
Network adapter3 => Switch 2 interface3

.

.

.

etc



- Assign IP to the management interface

```
Switch2(config)# interface mgmt
Switch2(config-if-mgmt)# no shutdown
Switch2(config-if-mgmt)# ip static 1.1.1.2/24
Switch2(config-if-mgmt)# default-gateway 192.168.91.2 (Nat Gateway)
```

- create VLAN access connected to client 1 and client 2

```
switch2(config)# valn1

switch2(config)# interface vlan 1

switch2(config-if-vlan)# ip address 1.1.1.2 255.255.255.0

switch2(config-if-vlan)#exit


switch2(config)# valn6
```

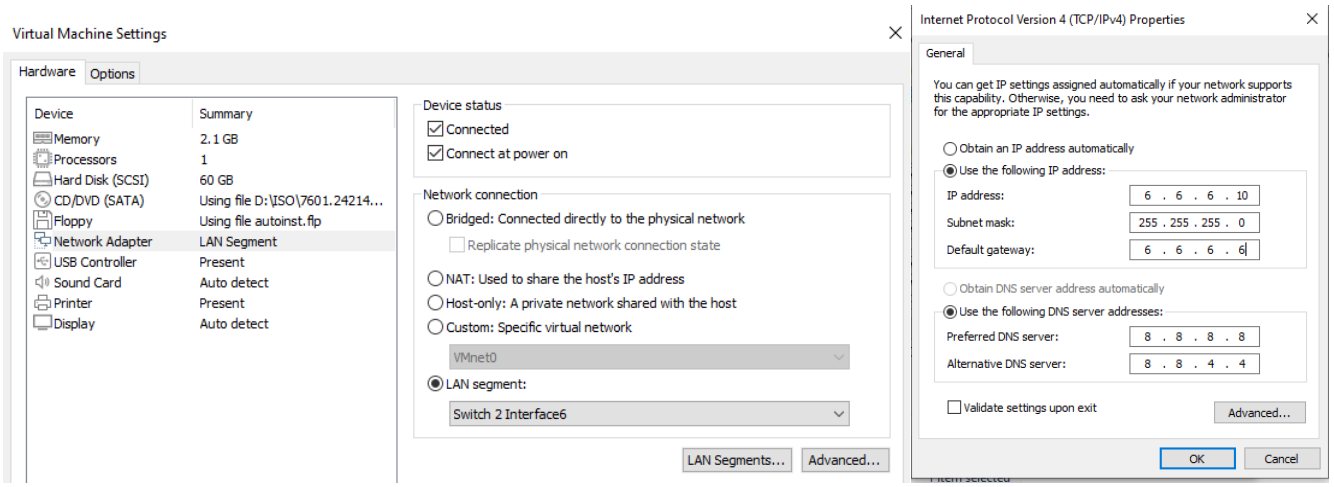
```
switch2(config)# interface vlan 6
switch2(config-if-vlan)# ip add 6.6.6.6 255.255.255.0
switch2(config-if-vlan)#exit

switch2(config)# valn7
switch2(config)# interface vlan 7
switch2(config-if-vlan)# ip add 7.7.7.7 255.255.255.0
switch2(config-if-vlan)#exit

switch(config) #interface 1/1/6
switch(config-if) #switchport access vlan 6
switch(config-if) #exit

switch(config) #interface 1/1/7
switch(config-if) #switchport access vlan 7
switch(config-if) #exit
```

- Create vlan10 trunk connect to Firewall

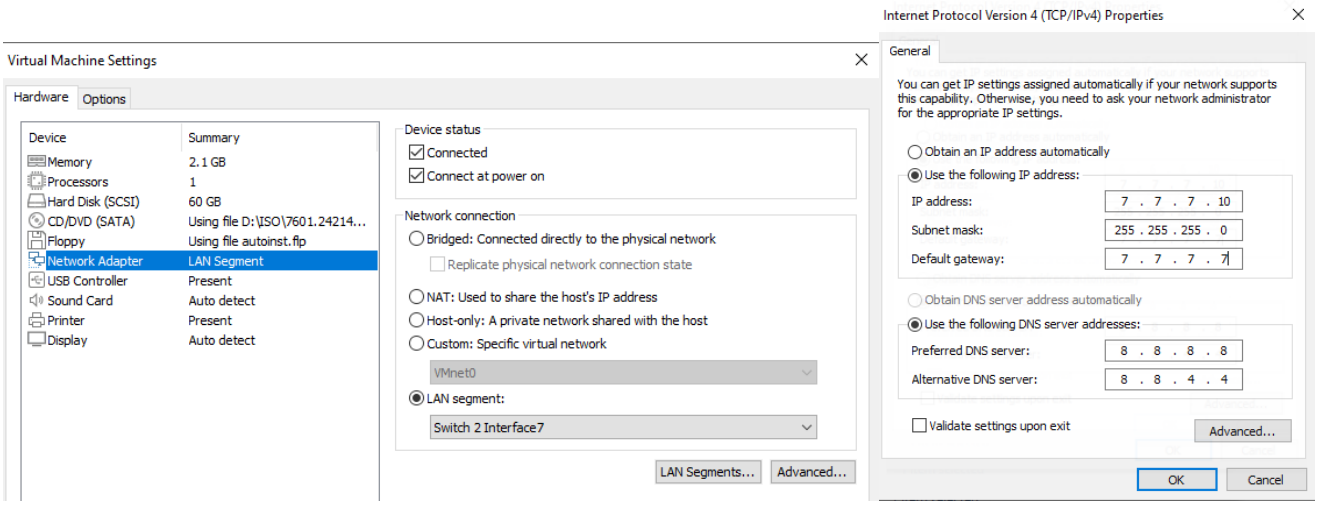
```
switch(config)# valn10
switch(config-if)# vlan trunk allowed all
switch(config)# interface vlan 10
switch(config-if-vlan)# ip address 10.0.0.13 255.255.255.0
switch(config-if-vlan)#exit

switch(config) #interface 1/1/9
switch(config-if) #switchport access vlan 10
switch(config-if) #exit
```

ITI EC3 Task

- **Server 1 Configuration**

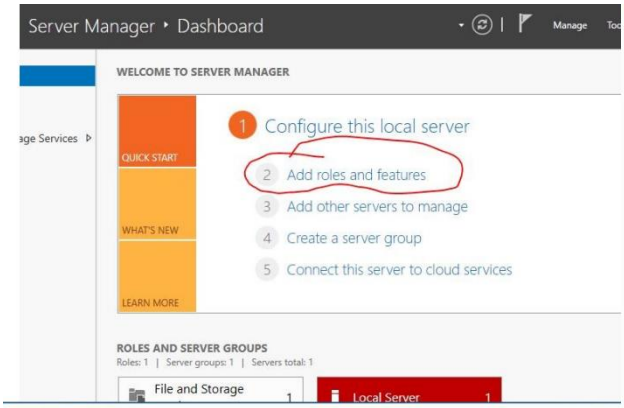


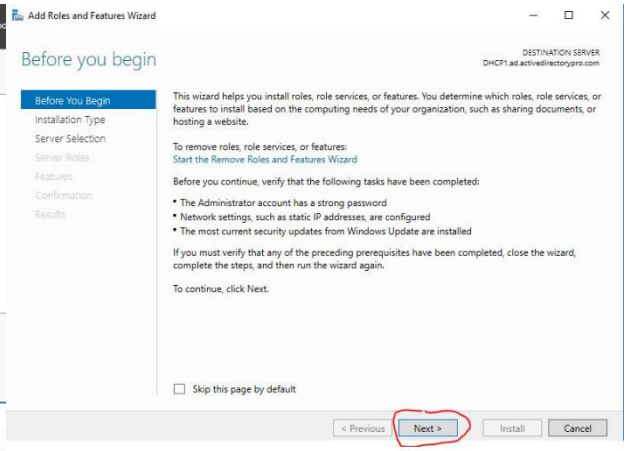
- Server2 configuration

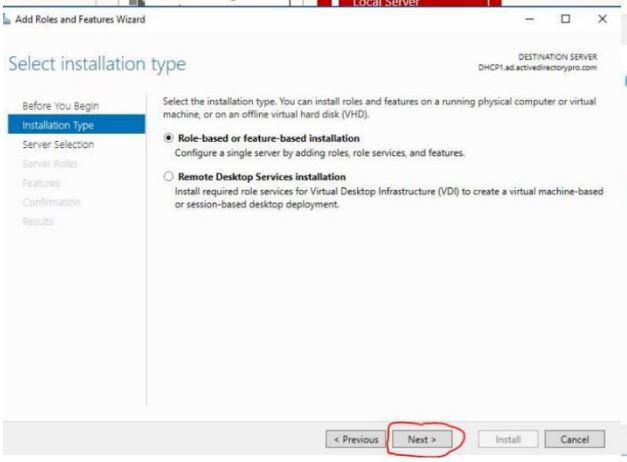


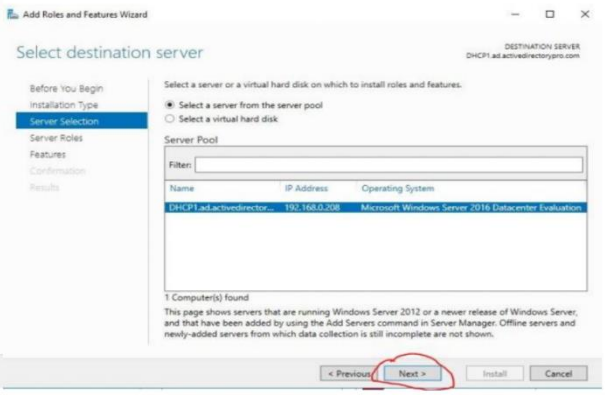
ITI EC3 Task

- Install Domain Controller, DNS Server, and DHCP Server

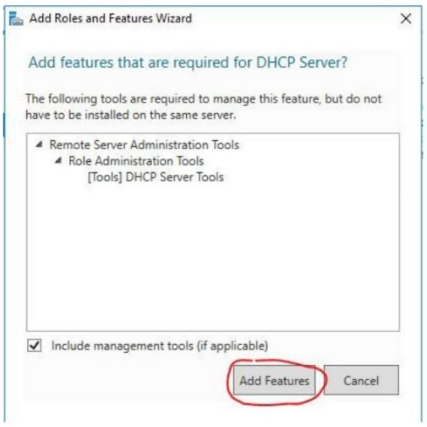


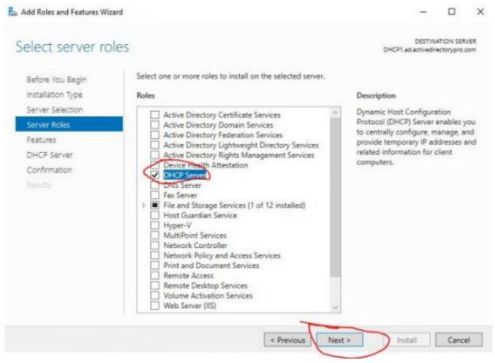


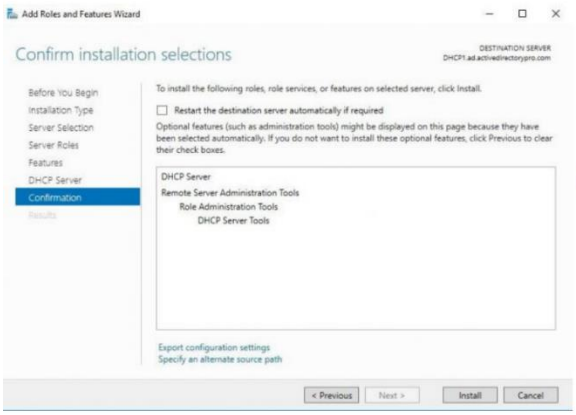


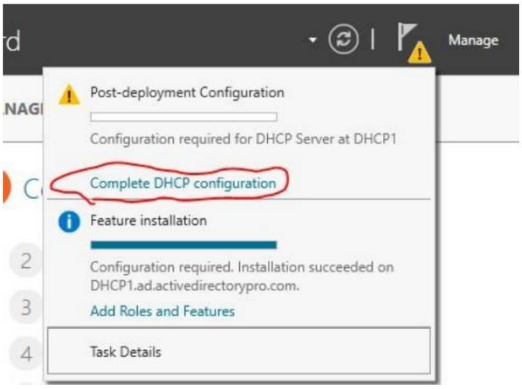


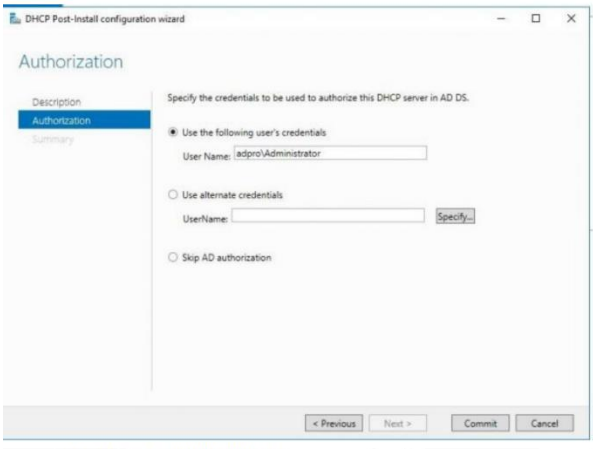
ITI EC3 Task

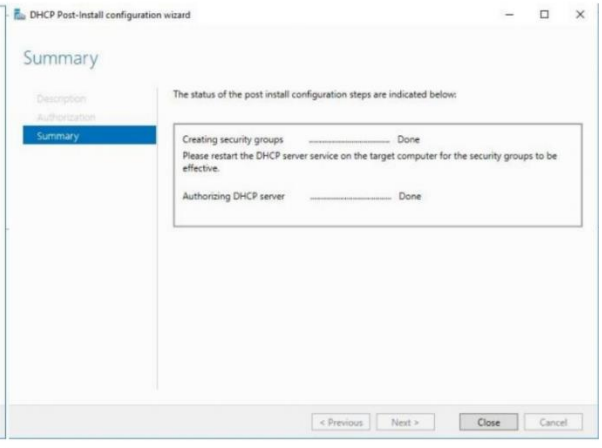

Add Roles and Features Wizard
Add features that are required for DHCP Server?
The following tools are required to manage this feature, but do not have to be installed on the same server.
Remote Server Administration Tools
Role Administration Tools
[Tools] DHCP Server Tools
Include management tools (if applicable)
Add Features
Cancel

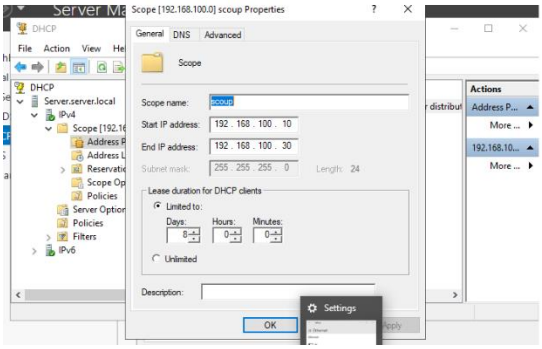

Add Roles and Features Wizard
Select server roles
Before You Begin
Installation Type
Server Selection
Server Roles
Features
DHCP Server
Confirmation
Results
Select one or more roles to install on the selected server.
Roles
Active Directory Certificate Services
Active Directory Domain Services
Active Directory Federation Services
Active Directory Lightweight Directory Services
Active Directory Rights Management Services
Device Health Attestation
DHCP Server
DNS Server
Fax Server
File and Storage Services (1 of 12 installed)
Host Guardian Service
Hyper-V
MultiPoint Services
Network Controller
Network Policy and Access Services
Print and Document Services
Remote Access
Remote Desktop Services
Volume Activation Services
Web Server (IIS)
Description
Dynamic Host Configuration Protocol (DHCP) Server enables you to centrally configure, manage, and provide temporary IP addresses and related information for client computers.
< Previous
Next >
Install
Cancel

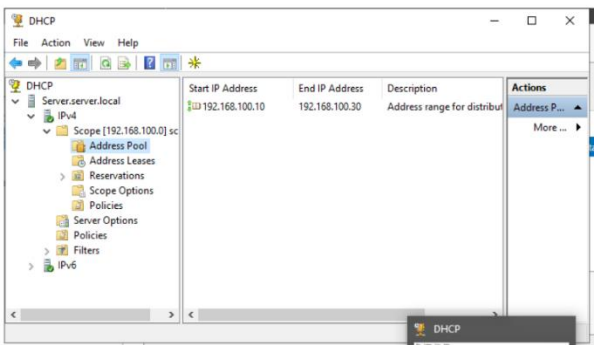

Add Roles and Features Wizard
Confirm installation selections
DESTINATION SERVER
DHCP1.ad.activedirectorypro.com
Before You Begin
Installation Type
Server Selection
Server Roles
Features
DHCP Server
Confirmation
Results
To install the following roles, role services, or features on selected server, click Install.
Restart the destination server automatically if required
Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.
DHCP Server
Remote Server Administration Tools
Role Administration Tools
DHCP Server Tools
Export configuration settings
Specify an alternate source path
< Previous
Next >
Install
Cancel


Manage
Post-deployment Configuration
Configuration required for DHCP Server at DHCP1
Complete DHCP configuration
Feature installation
Configuration required. Installation succeeded on DHCP1.ad.activedirectorypro.com.
Add Roles and Features
Task Details


DHCP Post-Install configuration wizard
Authorization
Description
Authorization
Summary
Specify the credentials to be used to authorize this DHCP server in AD DS.
Use the following user's credentials
User Name: adpro\Administrator
Use alternate credentials
UserName:
Specify...
Skip AD authorization
< Previous
Next >
Commit
Cancel

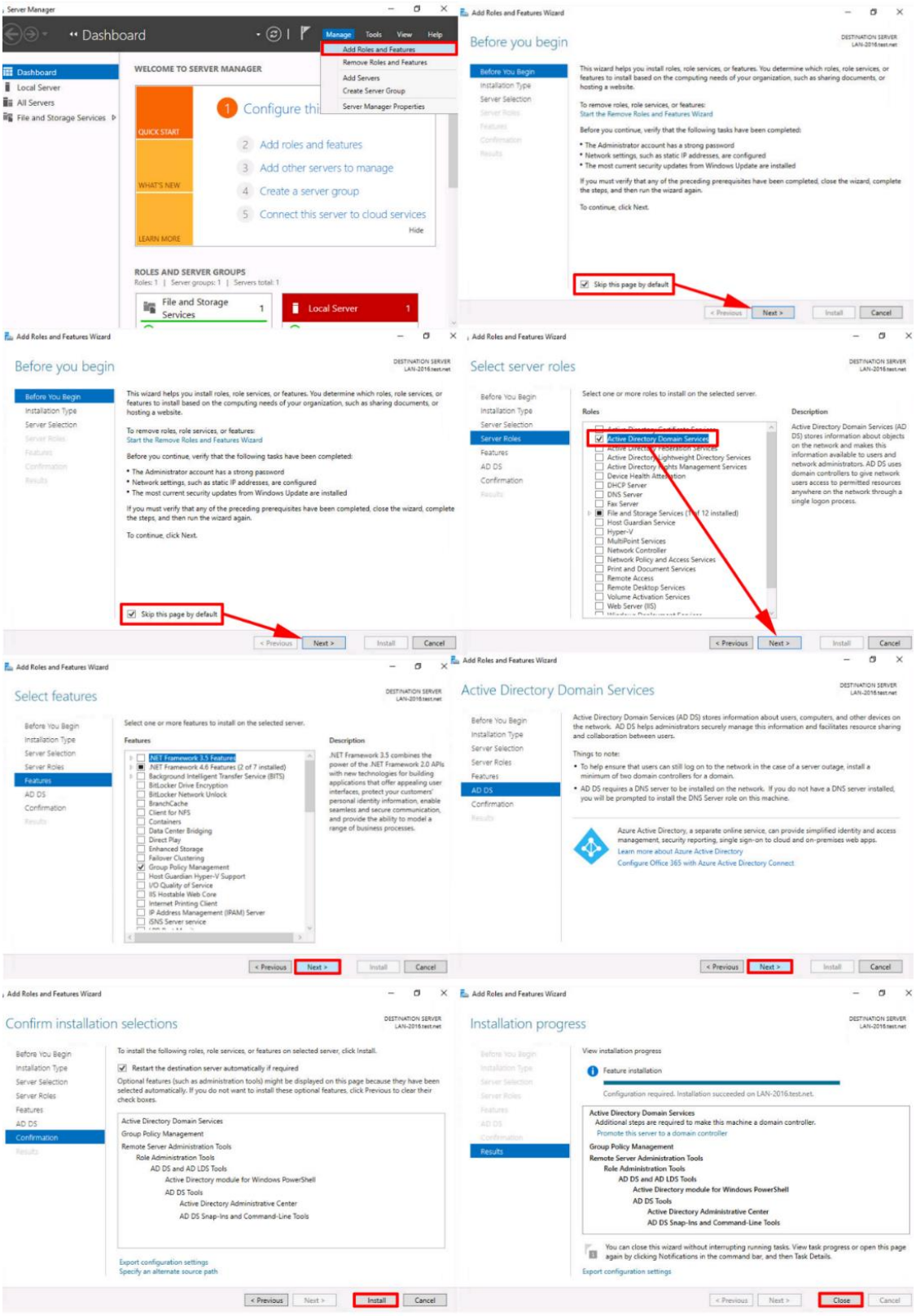

DHCP Post-Install configuration wizard
Summary
Description
Authorization
Summary
The status of the post install configuration steps are indicated below:
Creating security groups ..... Done
Please restart the DHCP server service on the target computer for the security groups to be effective.
Authorizing DHCP server ..... Done
< Previous
Next >
Close
Cancel


Scope [192.168.100.0] scoup Properties
General
DNS
Advanced
Scope
Scope name:
scoup
Start IP address:
192 . 168 . 100 . 10
End IP address:
192 . 168 . 100 . 30
Subnet mask:
255 . 255 . 255 . 0
Length: 24
Lease duration for DHCP clients
Limited to:
Days:
Hours:
Minutes:
Unlimited
Description:
OK
Settings
DHCP
File
Action
View
Server.server.local
IPv4
Scope [192.168.100.0] sc
Address Pool
Address Leases
Reservations
Scope Options
Policies
Server Options
Policies
Filters
IPv6
Start IP Address
End IP Address
Description
192.168.100.10
192.168.100.30
Address range for distribut
Actions
Address P...
More ...


DHCP
File
Action
View
Help
DHCP
Server.server.local
IPv4
Scope [192.168.100.0] sc
Address Pool
Address Leases
Reservations
Scope Options
Policies
Server Options
Policies
Filters
IPv6
Start IP Address
End IP Address
Description
192.168.100.10
192.168.100.30
Address range for distribut
Actions
Address P...
More ...
DHCP

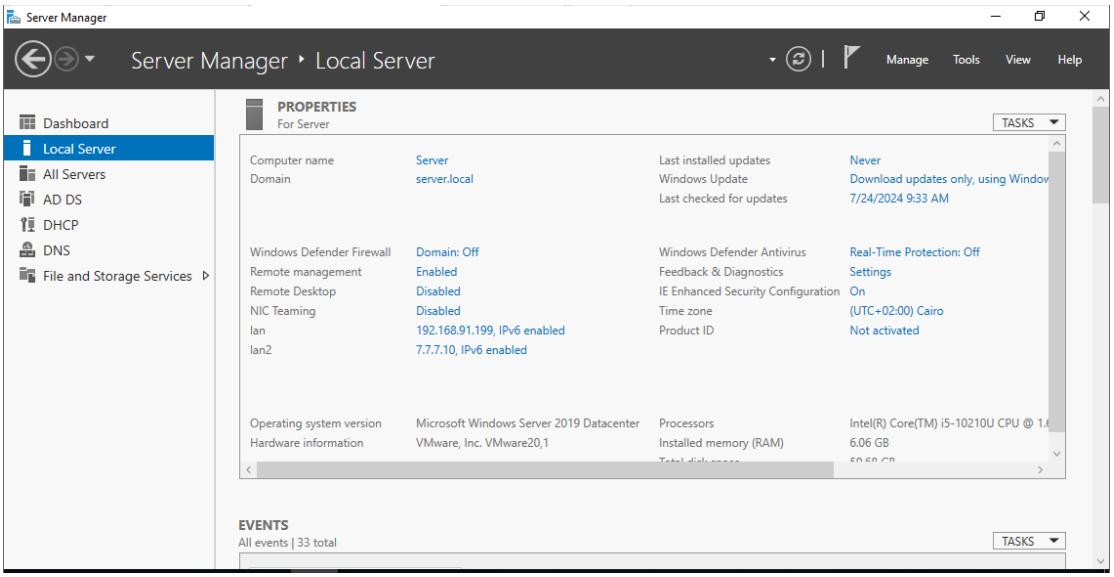
ITI EC3 Task

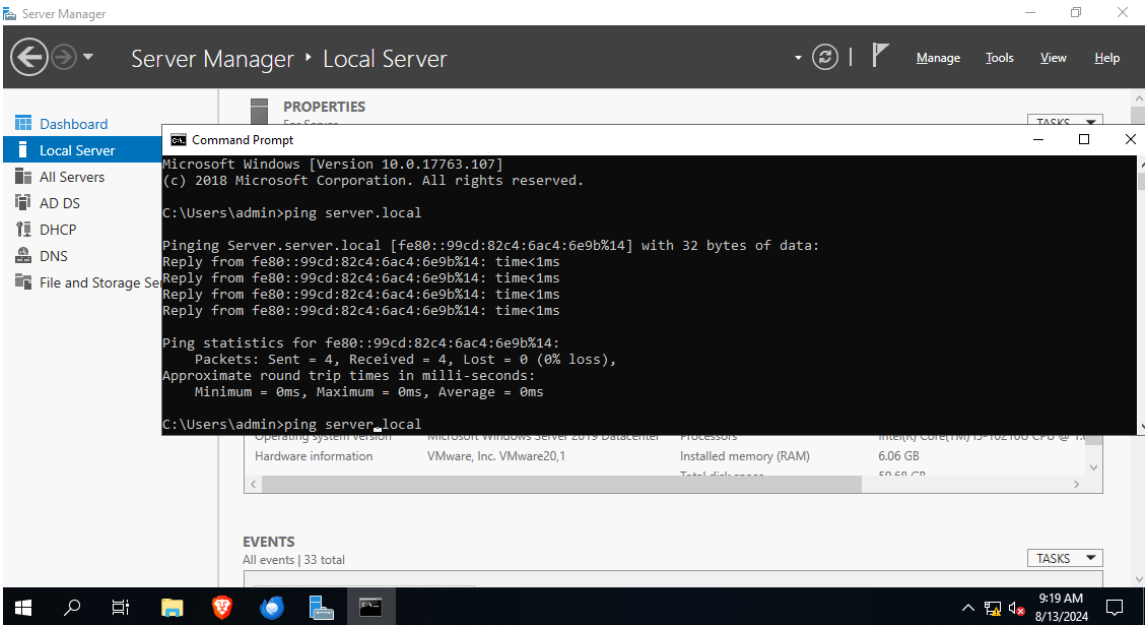
- **install Domain Controller and DNS server**



ITI EC3 Task

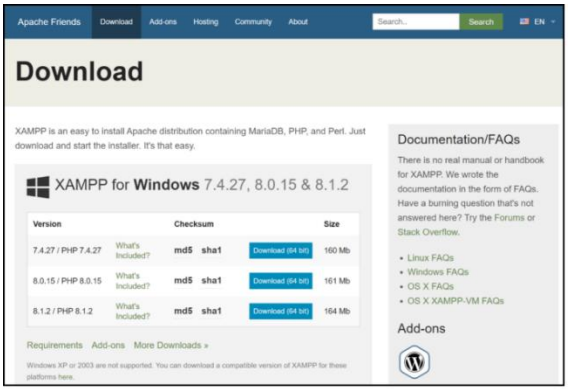
- In conclusion, installing Windows Server with Active Directory Domain Services (AD DS), DNS, and DHCP provides a robust foundation for network management. AD DS facilitates centralized user and resource management within a domain, DNS ensures reliable name resolution, and DHCP automates IP address allocation. Together, these components enhance network efficiency, security, and ease of administration, forming a cohesive infrastructure for both small and large organizations.

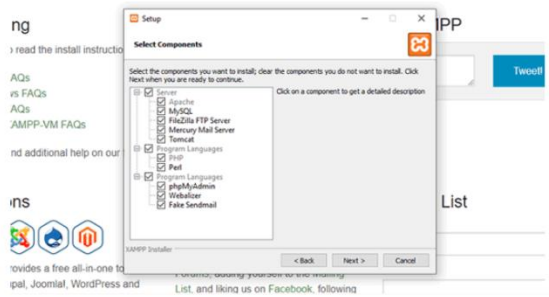


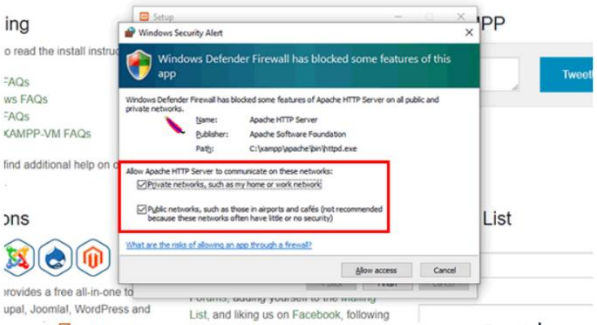


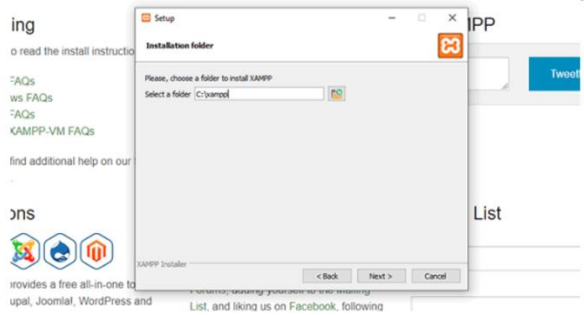
ITI EC3 Task

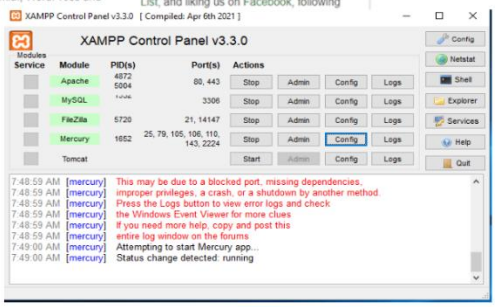
- **Install xamp on Windows server including:**
  - Mail server (port 110)
  - webserver (port 80)
  - database server SQL (3305)
  - ftp Server (port 21)











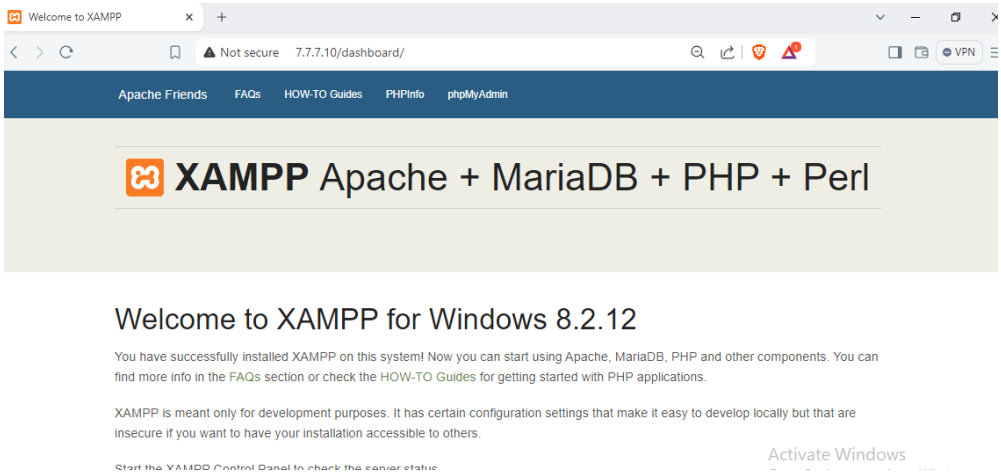
ITI EC3 Task

- To test the web server open the browser and write http://7.7.7.10 from your server

  It will be open

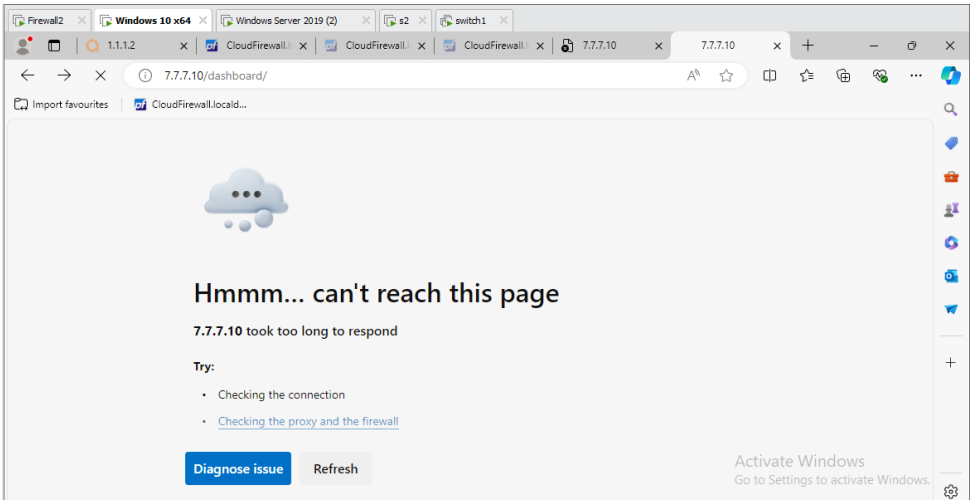
- To test from another host on the vlan write http://7.7.7.10

  It will be open



- To test from another host on another vlan write http://7.7.7.10

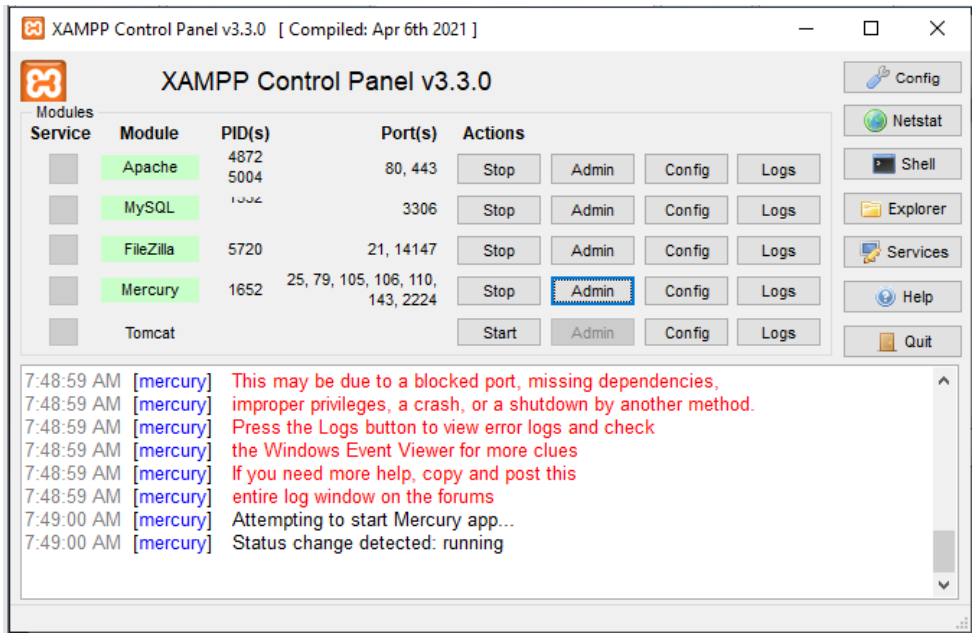
  It will be not open !! why?



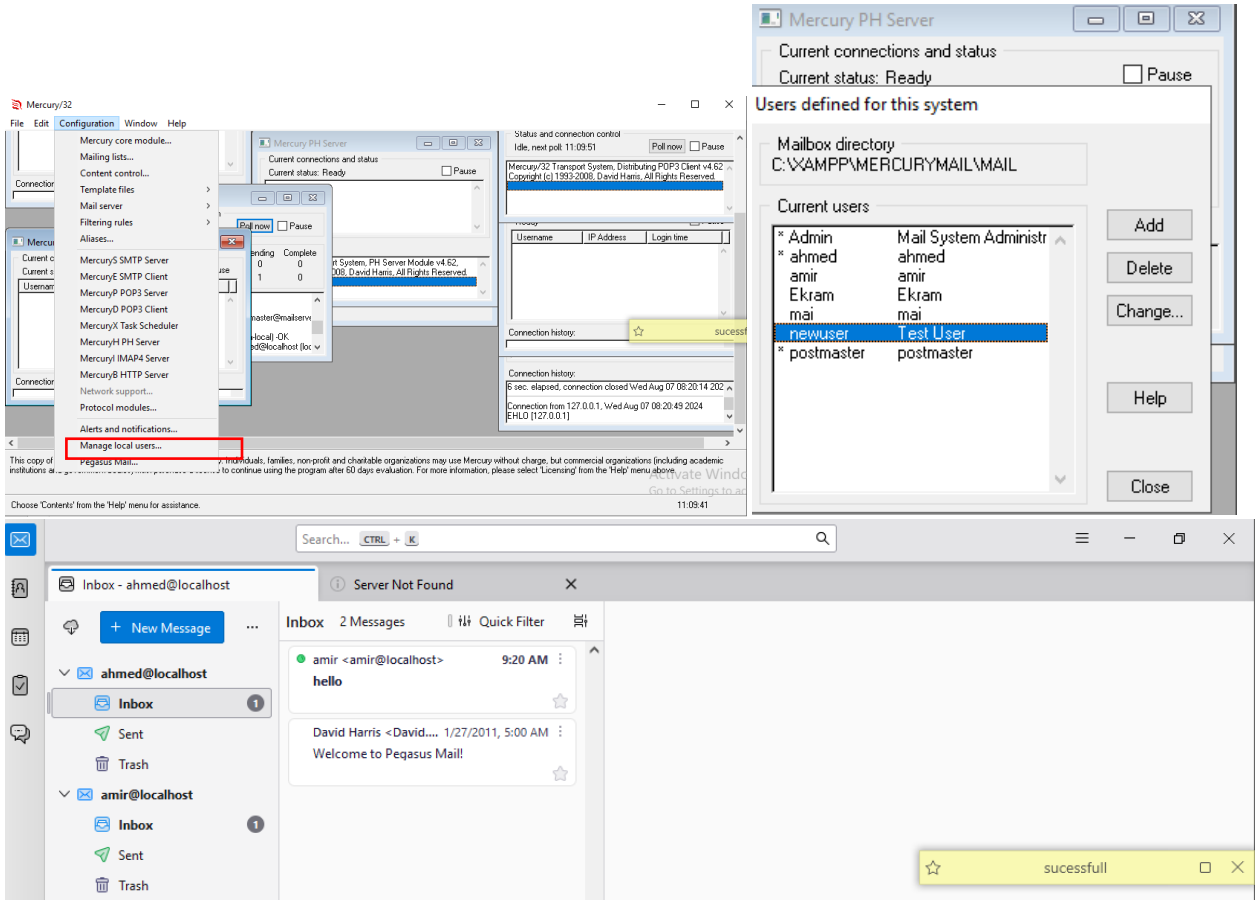
Because the firewall by default blocked it, we must add a rule to permit it.to permit.

ITI EC3 Task

- **Configure mail server**



- Add local email to test

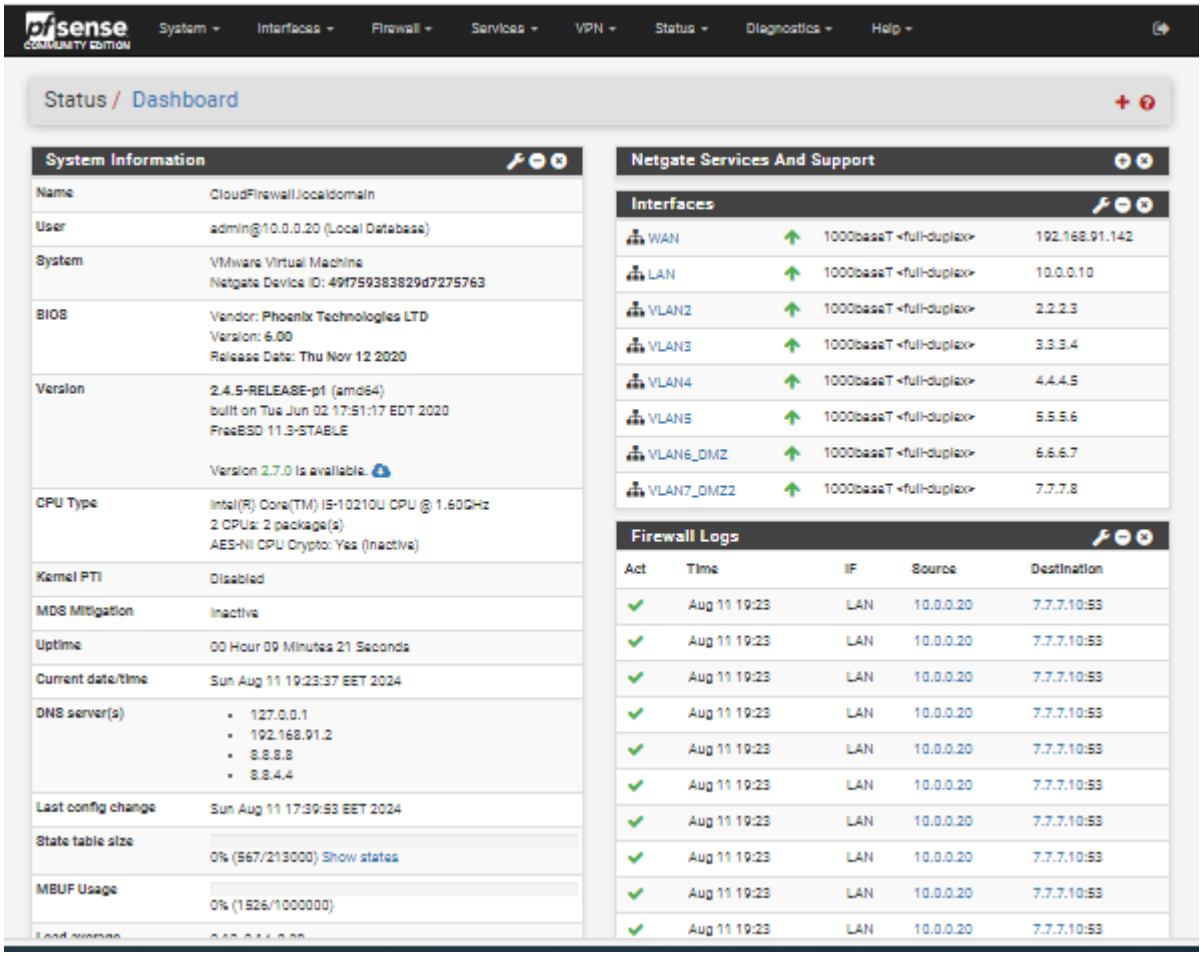


ITI EC3 Task

Firewall Rules Configuration

What are firewall rules?

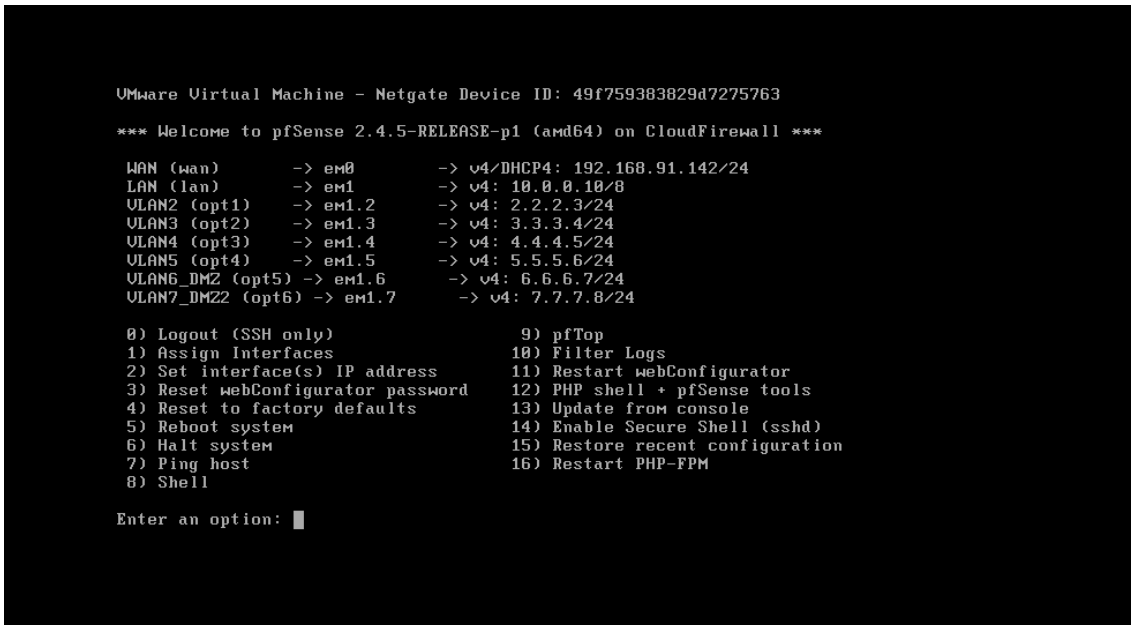
Add the rule designed to block the domains by placing them at the top of the list using the button with an upward-facing arrow. Opt for the action “block”, designate the interface as “WAN”, and choose the protocol “any”. For the source, select “Network”, and for the destination, choose “Single host or alias,” then input the alias “block domains.”



ITI EC3 Task

What are firewall rules priorities?

1- Floating
2- Wan
3- Lans

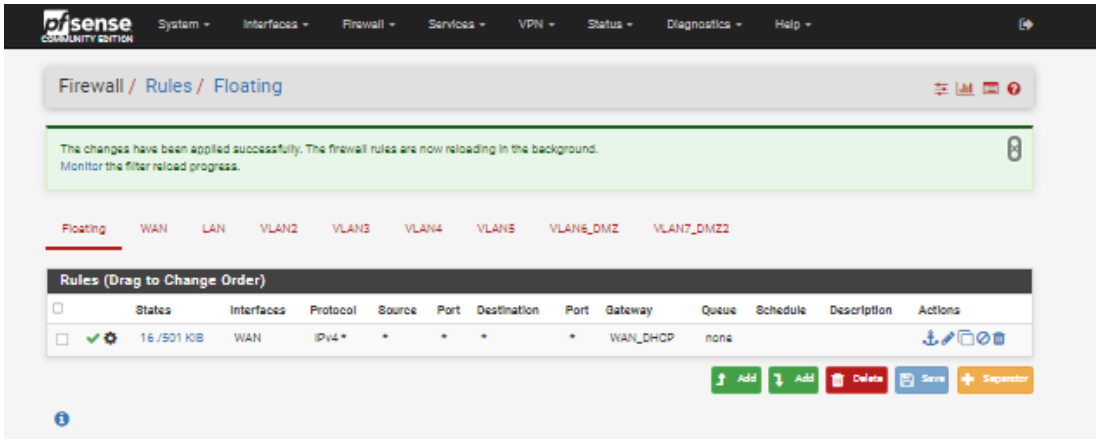


firewall processing order?

1. inbound quick rules, first match wins, and skips step 2
    1. quick floating inbound
    2. quick nic1 inbound
2. inbound non-quick rules, the last match wins
    1. non-quick floating inbound
    2. non-quick nic1 inbound
3. outbound quick rules, first match wins, and skips step 4
    1. quick floating outbound
    2. quick nic2 outbound
4. outbound non-quick rules, the last match wins
    1. non-quick floating outbound
    2. non-quick nic2 outbound

ITI EC3 Task

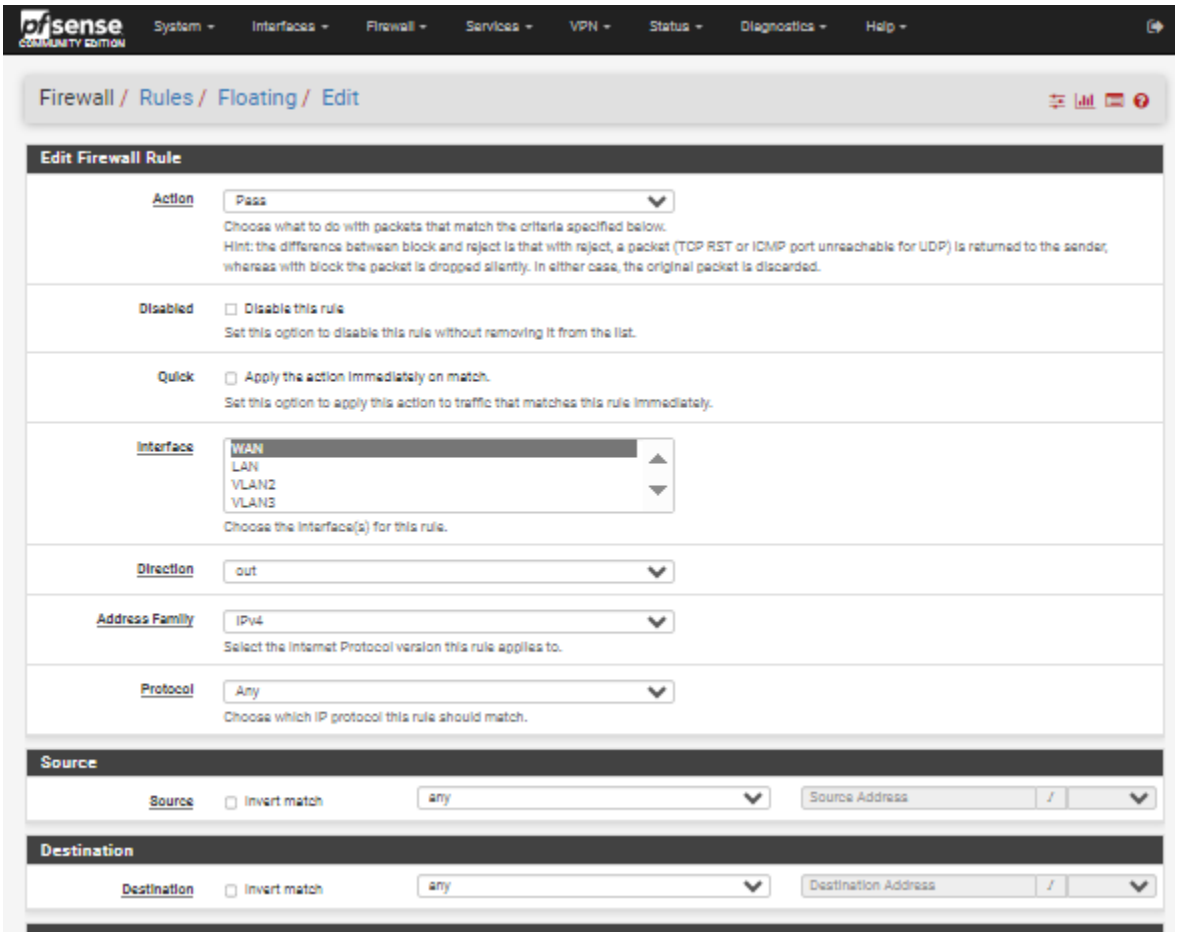
The packet can go through if and only if neither inbound rules (step 1&2) nor outbound rules (step 3&4) block it. Is that an accurate description?
Again I am still new to this and sampling both pfsense and opnsense, apologies for the mix-up..



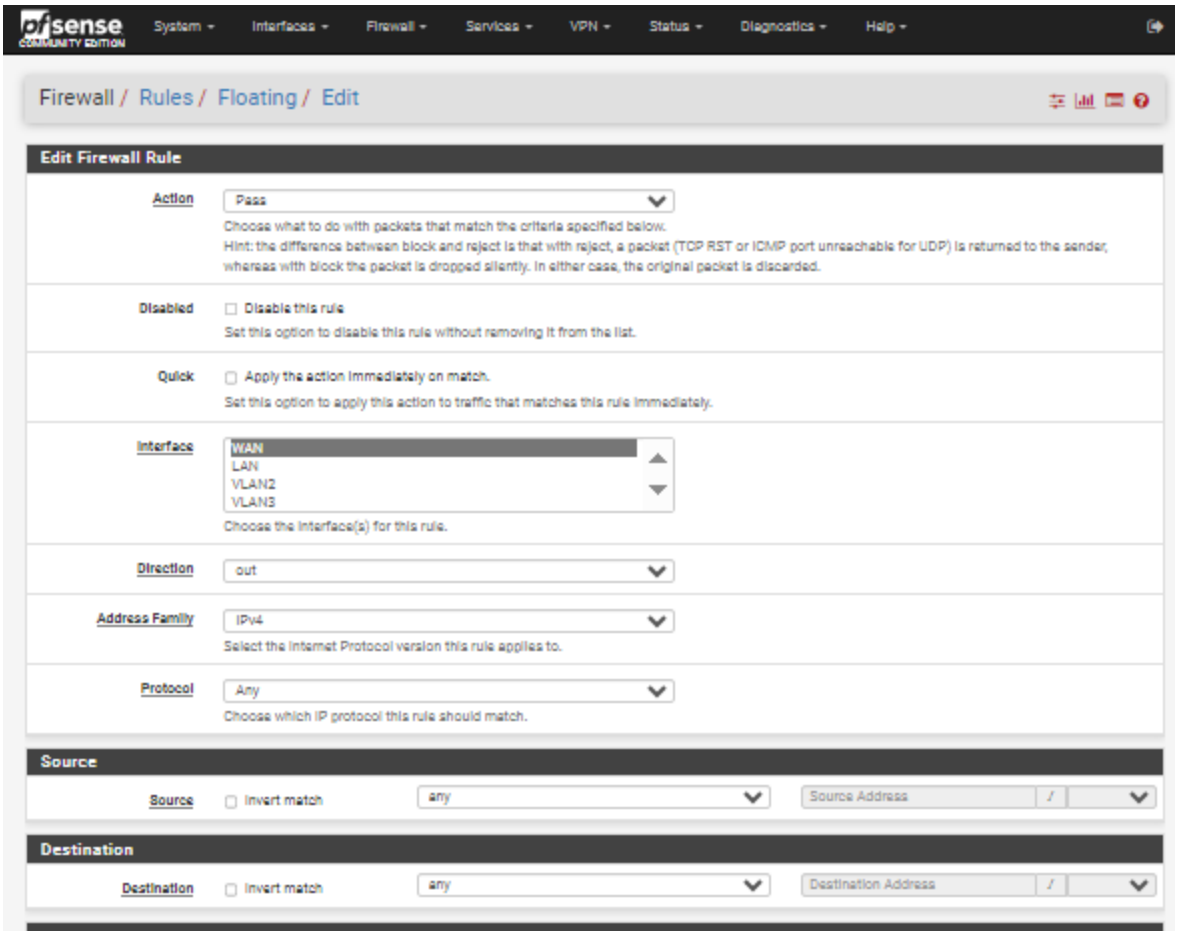
- Any rule on floating will overwrite any rule
- Any rule on wan will overwrite any rule on LAN
- any rule on lan will overwrite any rule on vlan

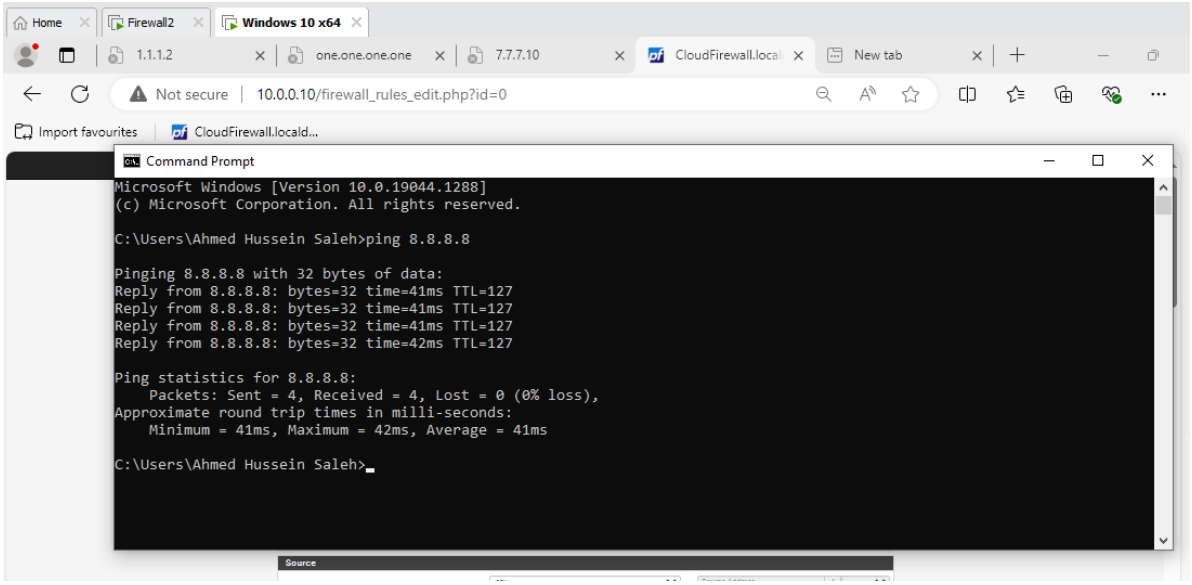
ITI EC3 Task

The next Step is (adding a role to access the internet on floating)



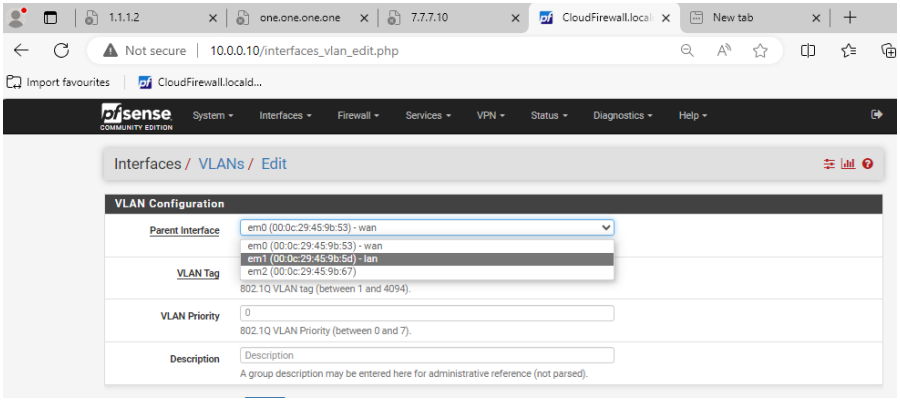
ITI EC3 Task

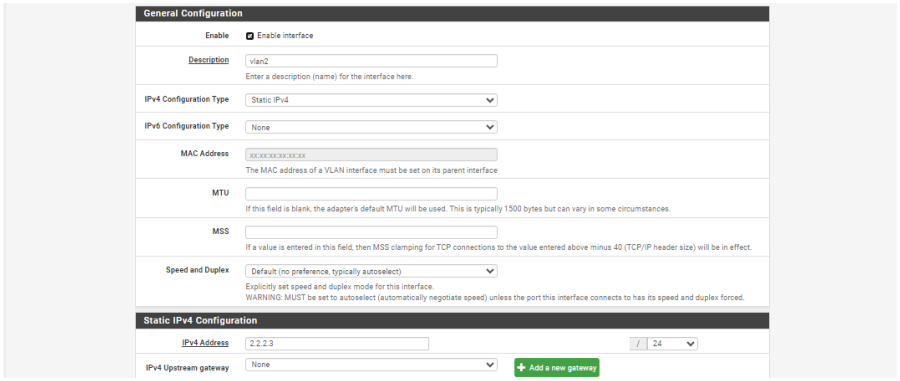

pfsense
COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Firewall / Rules / Floating / Edit
Edit Firewall Rule
Action
Pass
Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (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.
Quick
Apply the action immediately on match.
Set this option to apply this action to traffic that matches this rule immediately.
Interface
WAN
LAN
VLAN2
VLAN3
Choose the interface(s) for this rule.
Direction
out
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

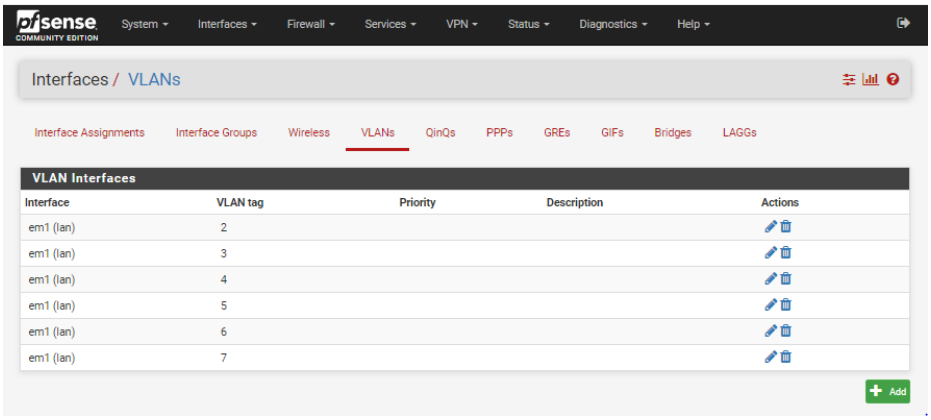

Home
Firewall2
Windows 10 x64
1.1.1.2
one.one.one.one
7.7.7.10
CloudFirewall.local
New tab
Not secure
10.0.0.10/firewall_rules_edit.php?id=0
Import favourites
CloudFirewall.locald...
Command Prompt
Microsoft Windows [Version 10.0.19044.1288]
(c) Microsoft Corporation. All rights reserved.
C:\Users\Ahmed Hussein Saleh>ping 8.8.8.8
Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=41ms TTL=127
Reply from 8.8.8.8: bytes=32 time=41ms TTL=127
Reply from 8.8.8.8: bytes=32 time=41ms TTL=127
Reply from 8.8.8.8: bytes=32 time=42ms TTL=127
Ping statistics for 8.8.8.8:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 41ms, Maximum = 42ms, Average = 41ms
C:\Users\Ahmed Hussein Saleh>
Source

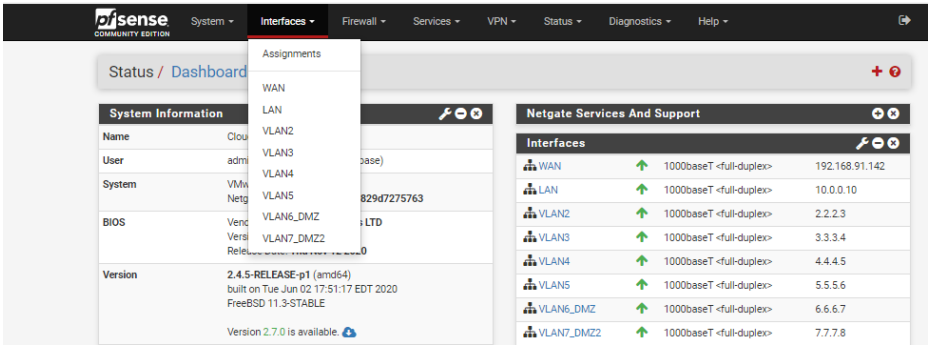
ITI EC3 Task

Create vlans on the firewall with lan interface(trunk with interface 1/1/9) on switches









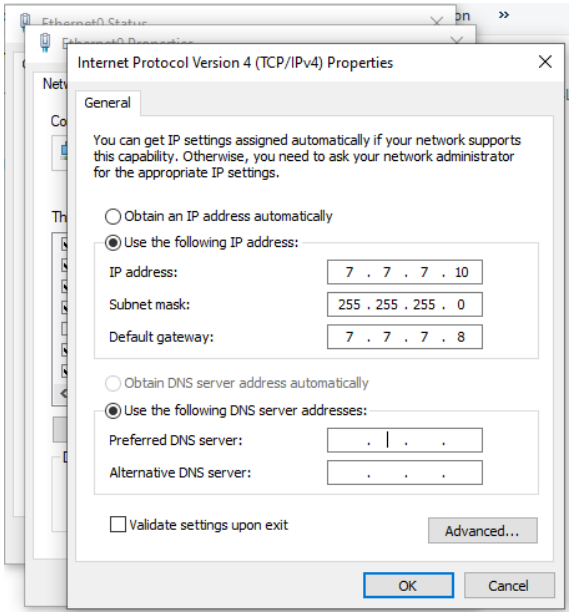
ITI EC3 Task

Last step change any gateway on hosts for every vlan configuration

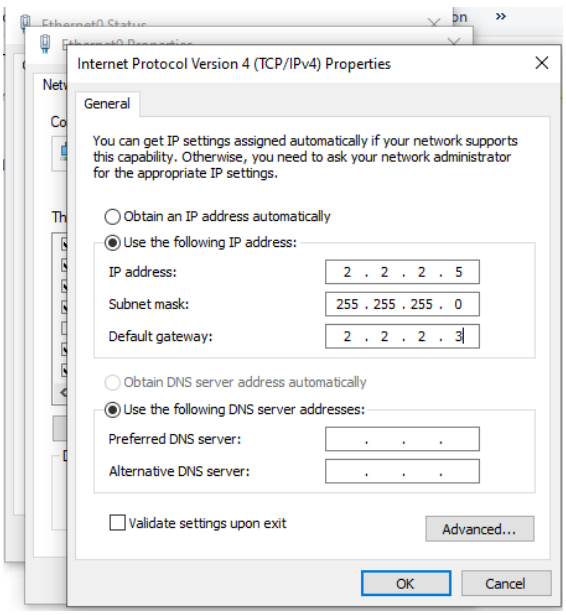
- Any network on 2.2.2.0 the gateway will be 2.2.2.3
- Any network on 3.3.3.0 the gateway will be 2.2.2.4
- Any network on 4.4.4.0 the gateway will be 2.2.2.5
- Any network on 5.5.5.0 the gateway will be 2.2.2.6
- Any network on 6.6.6.0 the gateway will be 2.2.2.7
- Any network on 7.7.7.0 the gateway will be 2.2.2.8
- Any network on 10.0.0.0 the gateway will be 10.0.0.10 Firewall Trunk port

Example:-

Windows Server2



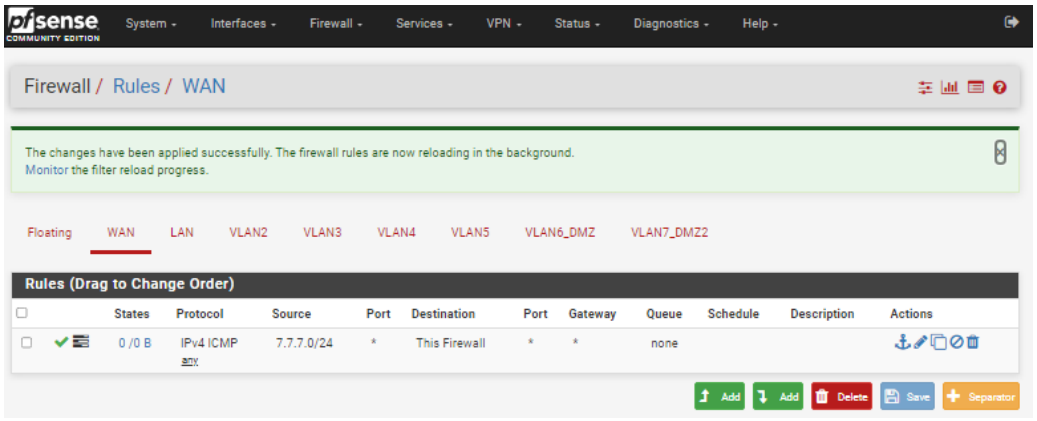
Client 2

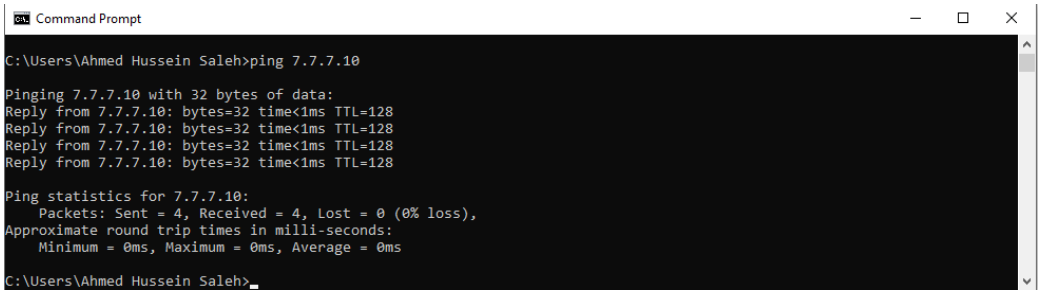


ITI EC3 Task

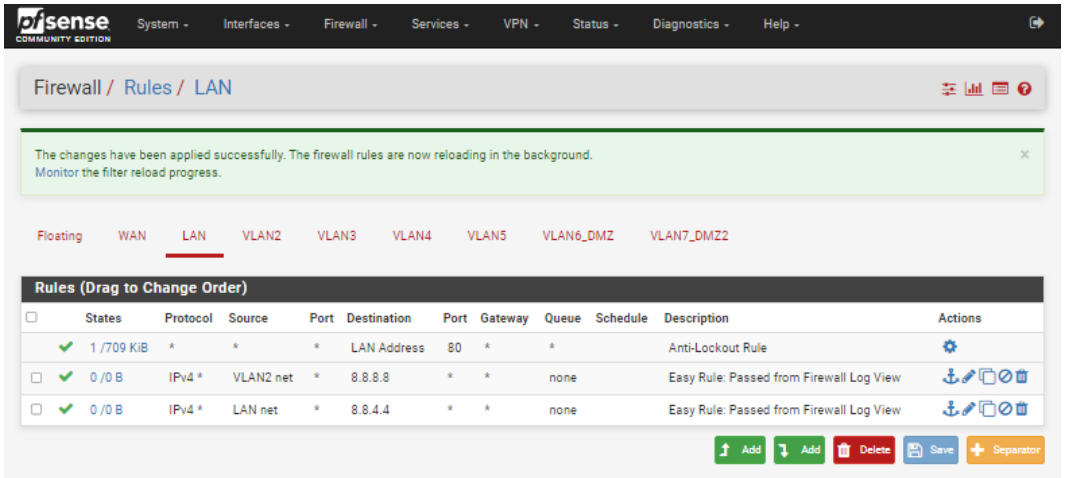
Create Rules

- Any host on network 7.7.7.0 DMZ Servers Can ping firewall IP using protocol ICMP on Wan



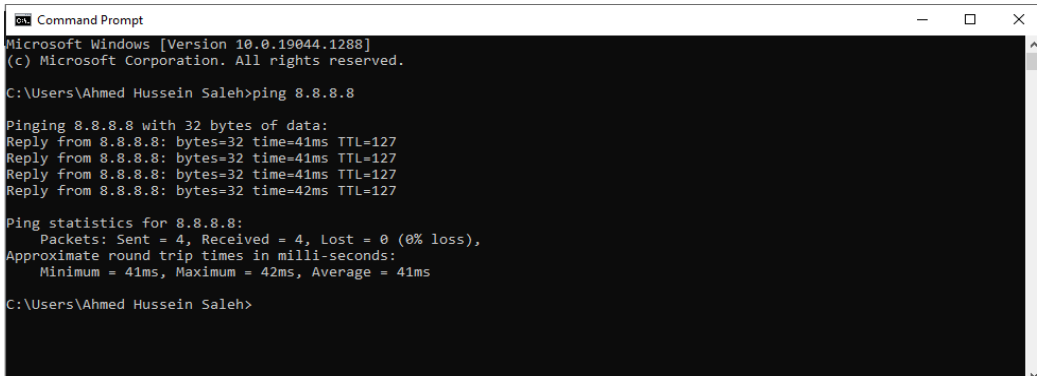


- any host Connected with firewall network 10.0.0.0 Can access the internet with any protocol with any port Within also floating rules



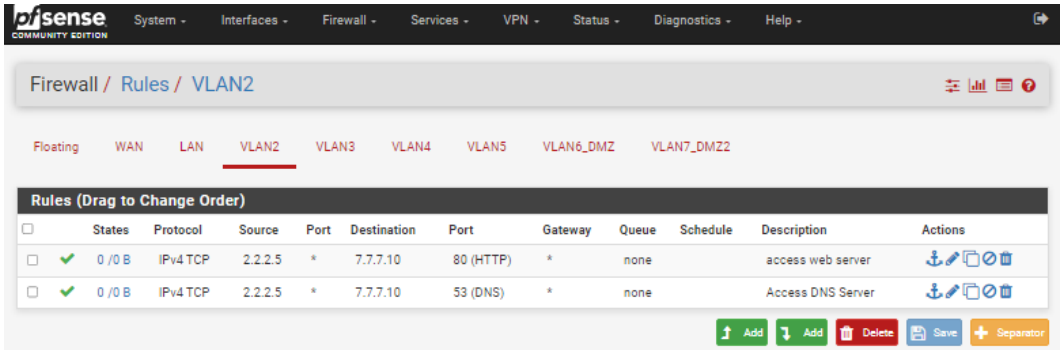
ITI EC3 Task

- Tes internet connction



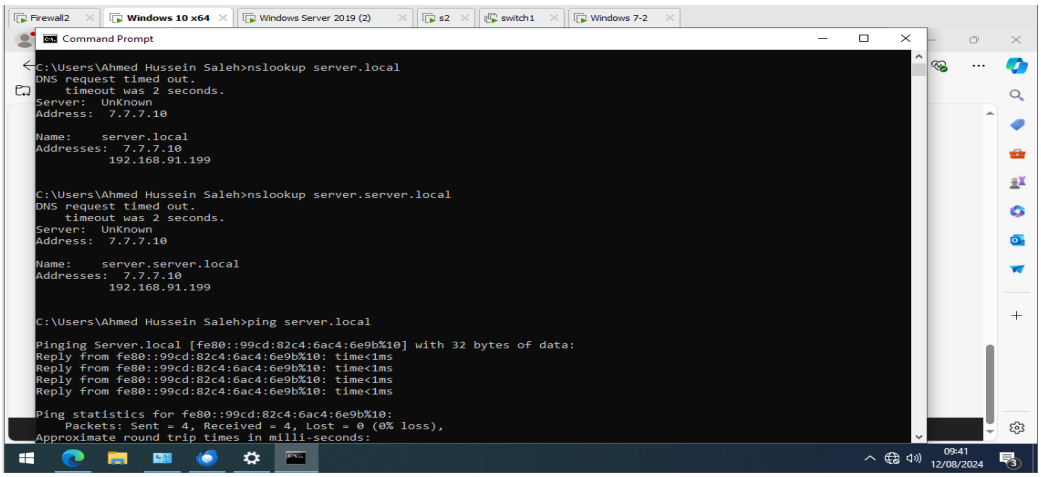
- host with ip 2.2.2.5 Can access webServer with protocol TCP on Port 80

- host with ip 2.2.2.5 Can access DNS Server with protocol TCP on Port 53

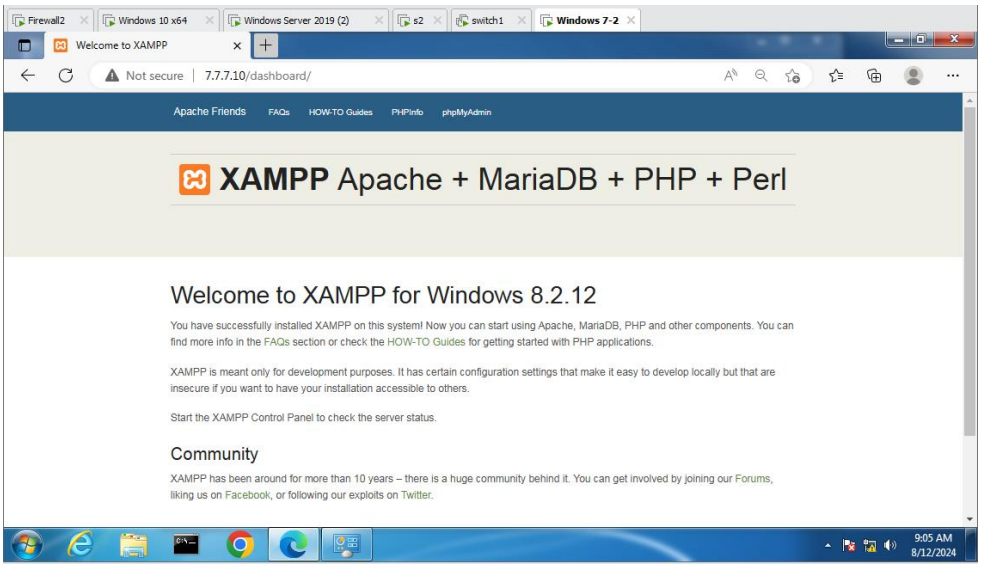


- Test DNS server

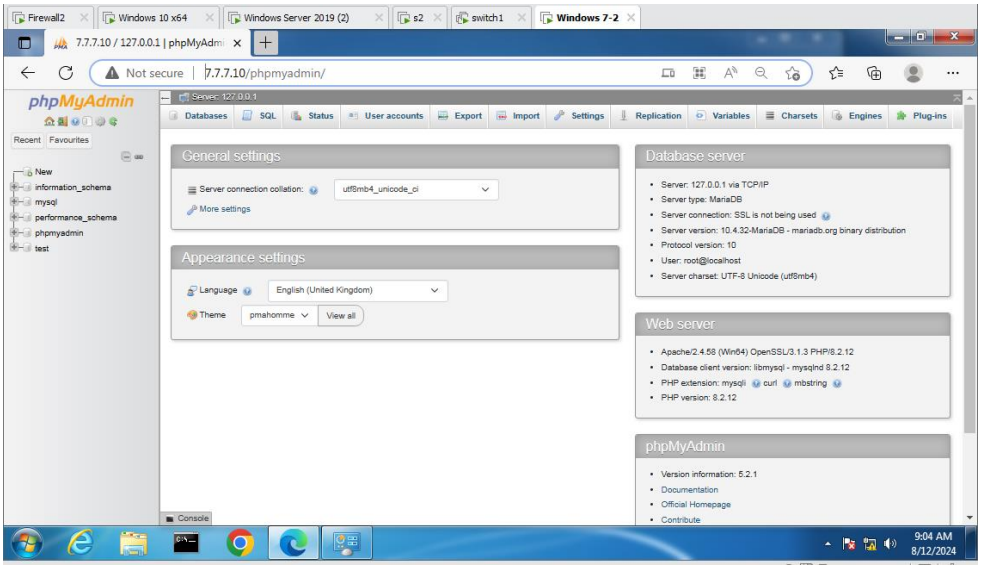
ITI EC3 Task



- Test Access WebServer and Database server



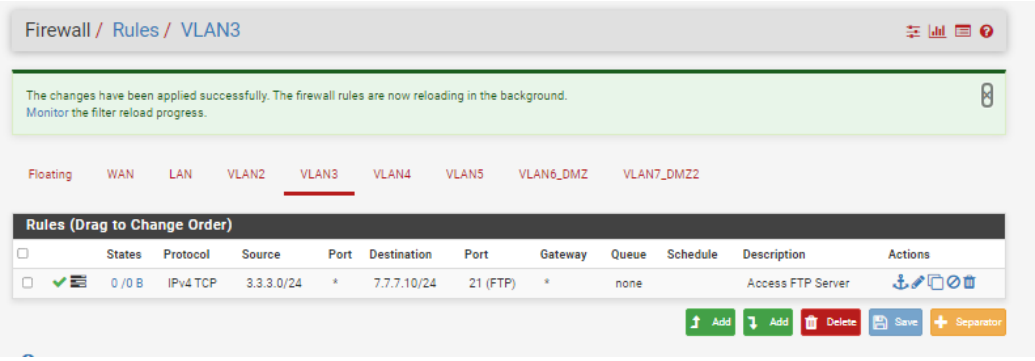
ITI EC3 Task



- Show Logs On the Firewall

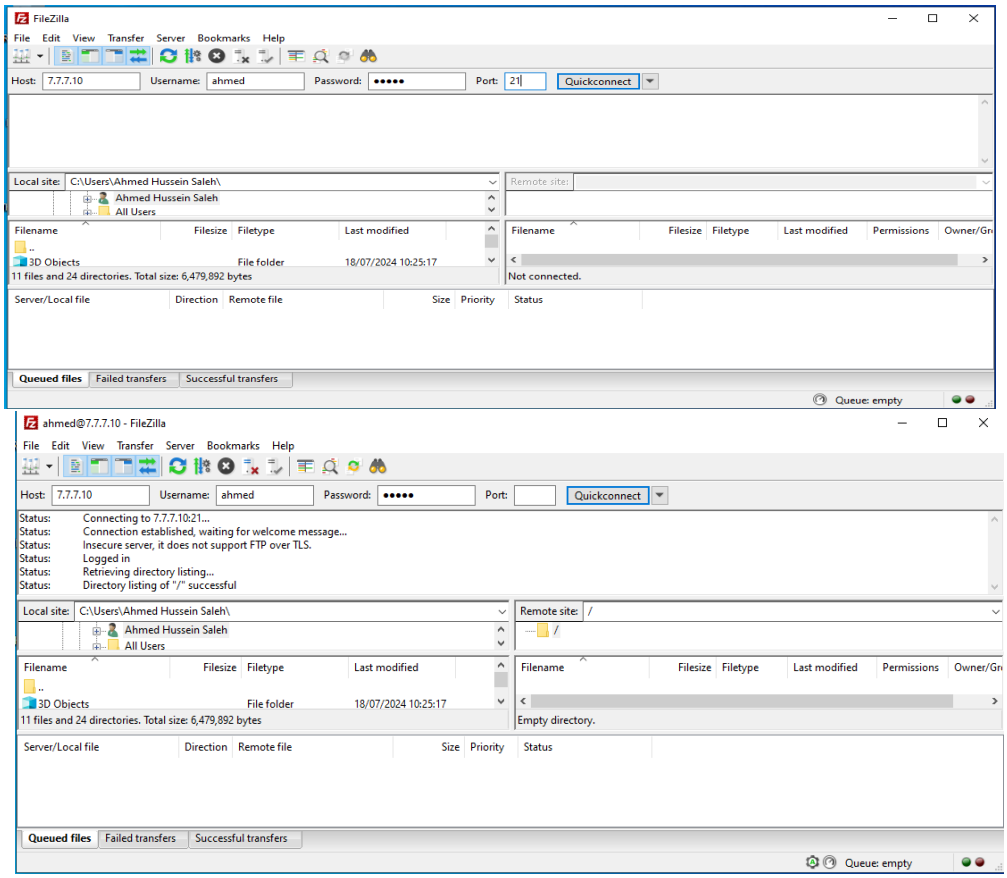
✔	Aug 11 17:10:55	VLAN2	USER_RULE (1722958698)	2.2.2.5:49176	7.7.7.10:80	TCP:S
✔	Aug 11 17:11:00	VLAN2	USER_RULE (1722958698)	2.2.2.5:49177	7.7.7.10:80	TCP:S
✔	Aug 11 17:11:00	VLAN2	USER_RULE (1722958698)	2.2.2.5:49178	7.7.7.10:80	TCP:S
✔	Aug 11 17:11:00	VLAN2	USER_RULE (1722958698)	2.2.2.5:49179	7.7.7.10:80	TCP:S
✔	Aug 11 17:11:00	VLAN2	USER_RULE (1722958698)	2.2.2.5:49180	7.7.7.10:80	TCP:S
✔	Aug 11 17:11:11	VLAN2	USER_RULE (1722958698)	2.2.2.5:49181	7.7.7.10:80	TCP:S
✔	Aug 11 17:11:31	LAN	USER_RULE (1722962762)	2.2.2.5:49182	7.7.7.10:80	TCP:S
✔	Aug 11 17:11:32	LAN	USER_RULE (1722962762)	2.2.2.5:49183	7.7.7.10:80	TCP:S
✔	Aug 11 17:11:32	LAN	USER_RULE (1722962762)	2.2.2.5:49184	7.7.7.10:80	TCP:S
✔	Aug 11 17:11:32	VLAN2	USER_RULE (1722958698)	2.2.2.5:49185	7.7.7.10:80	TCP:S
✔	Aug 11 17:11:53	VLAN2	USER_RULE (1722958698)	2.2.2.5:49186	7.7.7.10:80	TCP:S
✔	Aug 11 17:11:54	VLAN2	USER_RULE (1722958698)	2.2.2.5:49187	7.7.7.10:80	TCP:S

- Any host on network 3.3.3.0 Can access the FTP Server using protocol FTP On Port 21



- Test Fileserver (Filezilla)

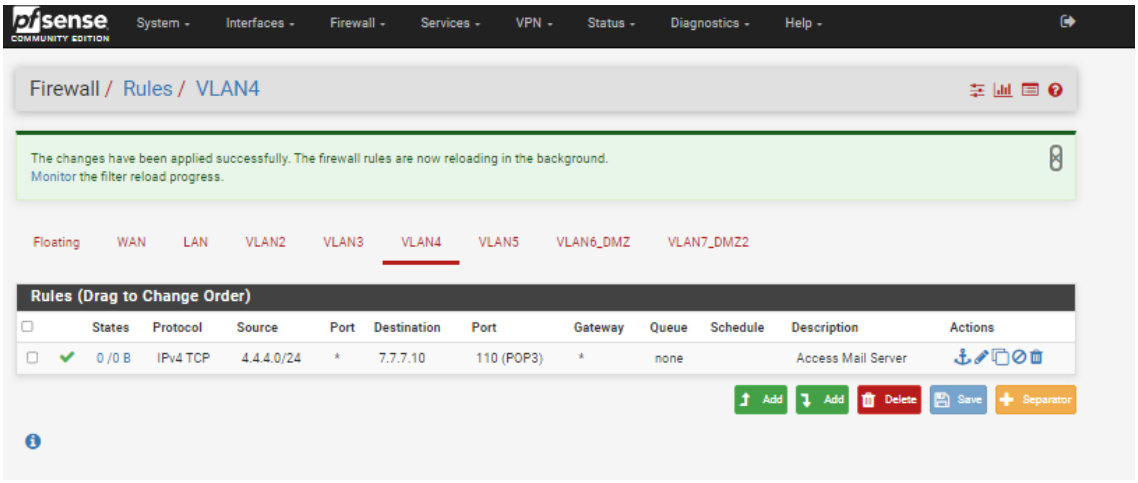
ITI EC3 Task



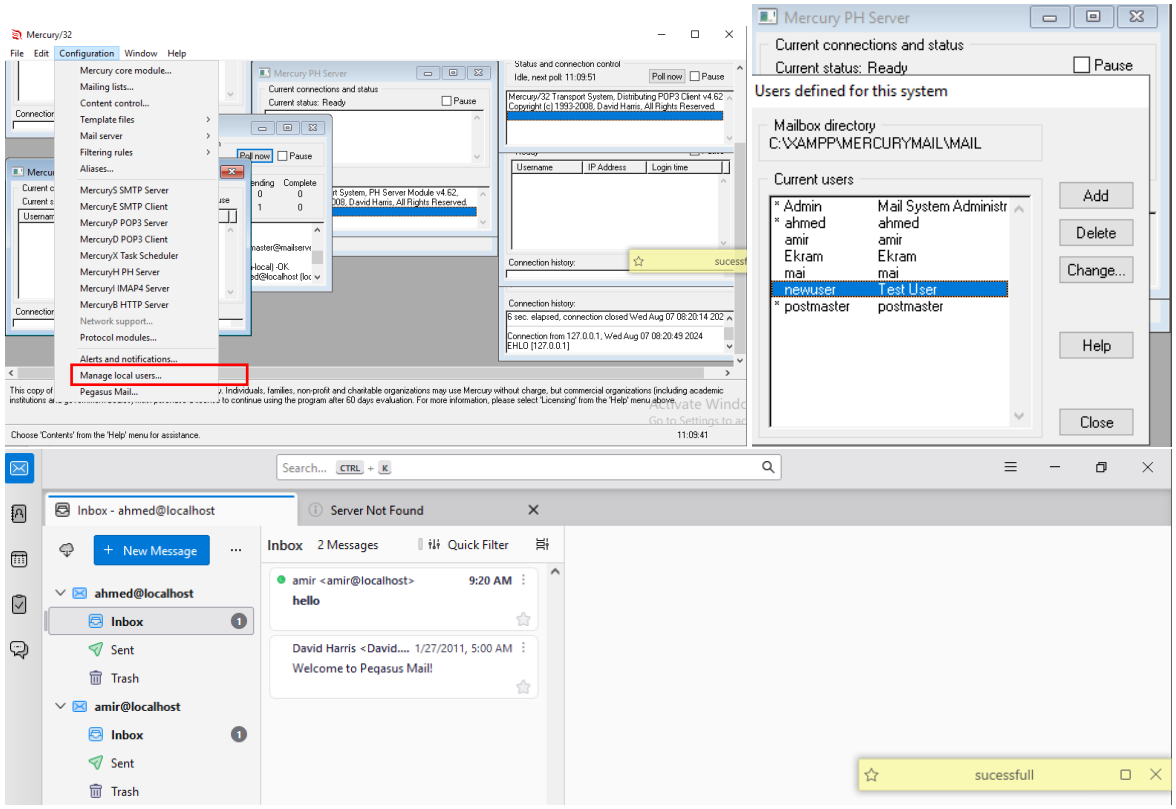
- Now can create folders and files under the rules we established in Filezillailla

- **Configure mail server**
  - Any host on network 4.4.4.0 Can access Mail Server using protocol POP3 On Port 110
    - If you want another protocol Such as SNMP 465 you can add a rule like this just change the port

ITI EC3 Task



Add local email to test



Conclusion and Summary

In this project, we successfully implemented a comprehensive network and server virtualization environment with specific configurations and security measures. The setup included a range of components and configurations, ensuring a cloud and

secure network infrastructure. Here is a summary of the steps undertaken and the outcomes achieved:

1. Virtualization Environment Setup (VmWare WorkStation):
    - We began by establishing a virtualization environment “VMware WorkStation ”, which serves as the foundation for hosting various network components and services.
2. DMZ Servers Installation (Windows Server – Ubuntu server):
    - We deployed DNS, Web, and Mail servers within the DMZ (Demilitarized Zone). These servers are essential for providing web and email services while ensuring they are isolated from the internal network for enhanced security.
3. Router Installation (Cisco):
    - A virtual router was installed to manage traffic between different network segments and to provide routing capabilities within the environment.
4. Switch Installation (Arouba Switches):
    - Two virtual switches were configured, with one operating at Layer 3 and the other at Layer 3, to handle routing and switching functions respectively.
5. Client Installation:
    - Four virtual clients were set up on the left side of the network to interact with the Web and Mail servers. These clients were used to test connectivity and access services.
6. Router and Firewall Configuration:
    - The router and firewall were configured to facilitate internet access and secure the network. This involved setting up rules and policies to manage and control traffic effectively.

ITI EC3 Task

7. Network Segmentation:
    - The network topology was divided into six distinct networks to organize traffic and improve security and performance.
8. Firewall Configuration:
    - Specific firewall rules were implemented to meet the following requirements:
        - Internet Access: Allowed any host or server to access the internet.
        - Communication Between Networks: Enabled servers on the right side of the topology to ping and communicate with hosts on the left side.
        - Firewall Access: Permitted servers on the right side to log in to the firewall and make configuration changes on specific ports, while denying any access from WAN or LAN hosts.
        - Restricted Host Access: Allowed hosts to access only the Web and Mail servers on specified ports.
        - Ping Restrictions: Denied any ping requests to the servers, firewall, or router from hosts.

ITI EC3 Task

Achievements

- Enhanced Security: By segmenting the network and configuring firewall rules, we ensured that only authorized traffic could flow between different segments and to/from the internet.
- Improved Management: The virtualized environment facilitated easier management and configuration of network components and services.
- Functional Testing: The setup was tested to confirm that all specified access controls and restrictions were functioning as intended, ensuring that the network operates securely and efficiently.

Recommendations

- Regular Monitoring: Continuous monitoring of network traffic and firewall logs is recommended to detect and respond to any potential security threats.
- Update Policies: Periodic review and updating of firewall policies and network configurations will help adapt to new security challenges and changes in network requirements.
- Backup and Recovery: Implementing regular backups of the firewall and router configurations can help quickly restore operations in case of failure or misconfiguration.

In conclusion, the successful implementation of this network environment demonstrates the effectiveness of virtualization and careful configuration in creating a secure and manageable network infrastructure. The design and policies put in place ensure that both functionality and security requirements are met, providing a solid foundation for further network operations and improvements.

ITI EC3 Task

References

- https://www.arubanetworks.com
- https://www.pfsense.org/
- https://www.vmware.com/
- https://www.cisco.com/
- https://www.microsoft.com/en-us/software-download/windows10
- https://www.arubanetworks.com/techdocs/hardware/DocumentationPortal/Content/ArubaTopics/Switches/1430.htm
- https://www.cisco.com/c/en/us/td/docs/routers/access/800M/software/800MSCG/routconf.html
- https://medium.com/
- https://openai.com/index/chatgpt/