PORTFOLIO

By Alvin Chow

Table Of Content

Window Format and Install(P.3)

Palo Alto Factory Reset (P.12)

SOHO Configuration Palo Firewall (P.20)

Multi-area OSPF lab (P.30)

Exterior Border Gateway Protocol (P.58)

Interior BGP lab (P.81)

Palo Alto URL filtering (P.105)

Palo Alto Remote Access VPN Lab (P.114)

Amazon Cloud Foundation Lab 1-3 (P.127)

Amazon Cloud Foundation Lab 4-6 (P.154)

Fortinet SOHO with Wireless WPA2-PSK and WPA2-Enterprise (P.171)

Fortinet SSL VPN Remote Access Lab (P.180)

Cisco Multiple Wireless SSID with Access Point, WPA2 PSK, WPA2-ent (P.187)

Layer 2 Attacks and Mitigations (P.201)

IS-IS Integrated Services to Integrated Services Lab (P.208)

FortiGate IPSec Site to Site VPN Lab (P.226)

Lab1: Window Format and Install

By Alvin Chow

Purpose: Set up and downloaded the application onto the personal hard drive, and computer driver for the lab during this school year, learned more about what driver and application to set up a computer for networking lab uses.

Background information: Lab computer is Lenovo ThinkStation P5 this computer used ntel Xenon W5-2455X processor, which has a processing speed of 3.20 GHz and can go up to 4.60 GHz. The desktops also come with an NVIDIA RTX A4500 graphics card as well as 32 GB of DDR5 RAM (4800 MHz processing speed). It also comes with a 1000W power supply, Bluetooth, and Wi-fi. In this lab, we updated the Window Version to Window 11 Education.

For the normal networking lab computer, first, you need some driver to ensure the normal use of the computer, so we downloaded the application called Lenovo Service Bridge to make sure we downloaded the correct driver for the computer.

After that, we downloaded Lenovo Commercial Vantage for some future updates for the computer system and let the future updates more easily. This application also enables personal configuration preferences. Lenovo is a global technology powerhouse, ranked at 217 in the Fortune Global 500, Building onsuccess as the world's number one PC maker, Lenovo is expanding its research into growth areas to advance "New IT" technologies (client, edge, cloud, network, and intelligence)

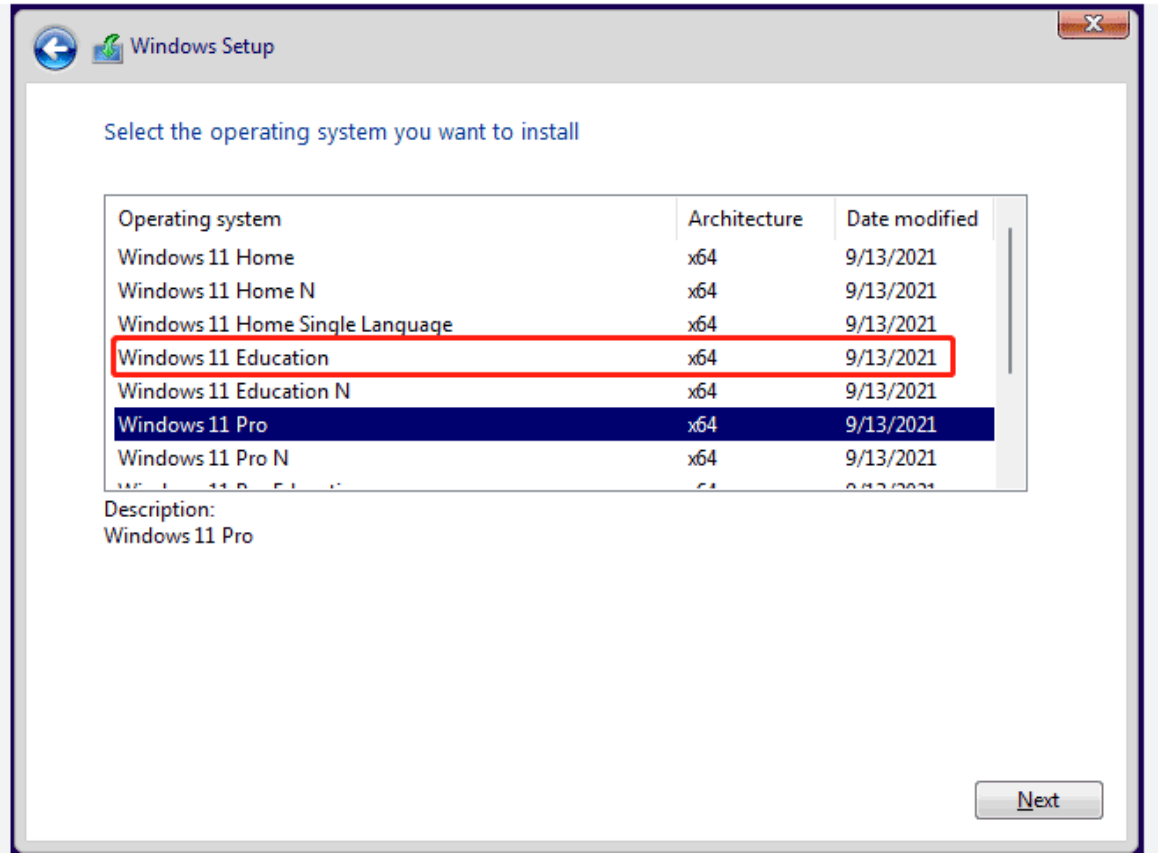
Then, we need to have some terminal application for the lab uses for example command prompt for window, but we prefer the application called Putty because PuTTY is a free and open-source terminal emulator, network file transfer application, and serial console for Windows platforms. It allows you to connect to remote computers or devices using various protocols such as secure socket shell (SSH), Telnet, and Serial.

Sometimes if we have some problem in our lab, we usually capture some traffic of the network, so, we downloaded Wireshark because Wireshark is a widely used, open-source network analyzer that can capture and display real-time details of network traffic, For Example from your computer to your home office or the internet. Packet is the name given to a discrete unit of data in a typical Ethernet network. Wireshark is the most often-used packet sniffer in the world.

For the Lab report, we downloaded Office 365 because we prefer to use Word to write the lab report. After all, Office 365 is a product family of productivity software, collaboration and cloud-based services owned by Microsoft. It encompasses online services such as Outlook.com, OneDrive, Microsoft Teams, programs formerly marketed under the name Microsoft Office (including applications such as Word, Excel, PowerPoint, and Outlook.)

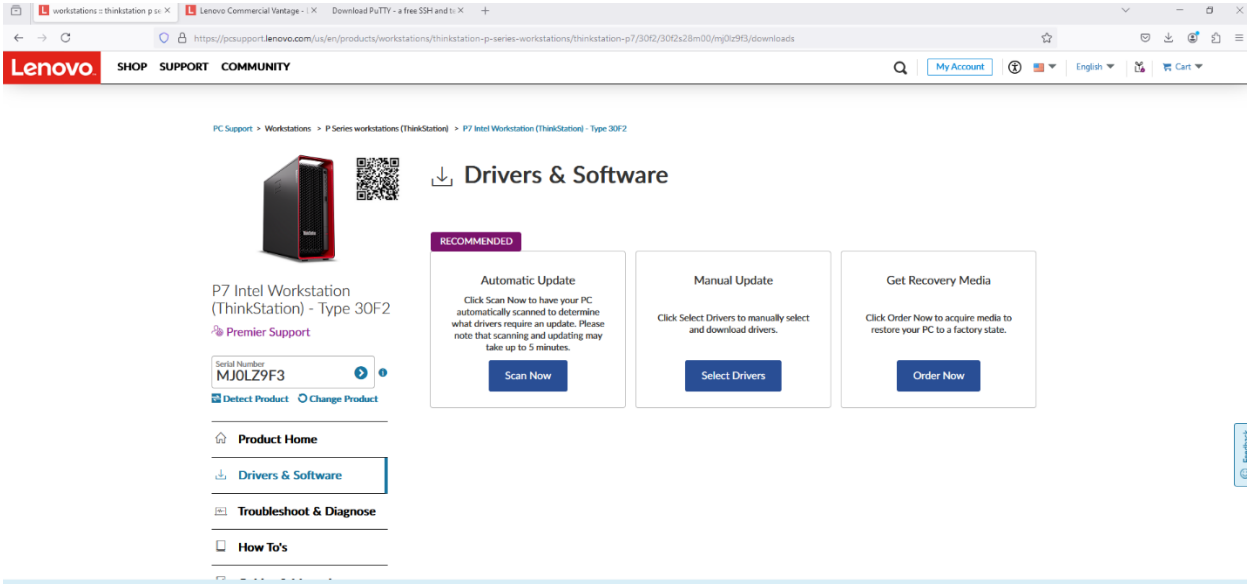
Lab summary: Step by step guide

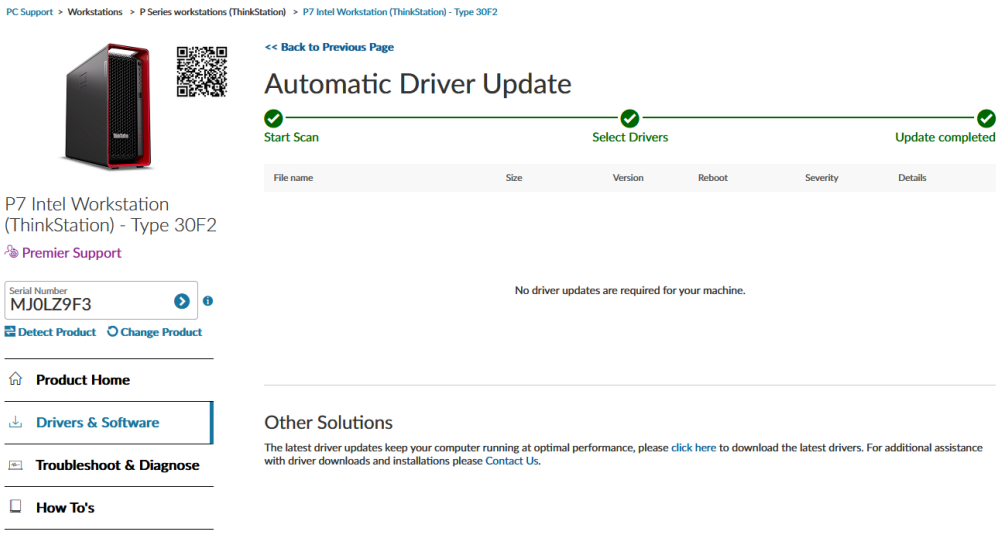
Steps 1: Using USB to download Window 11 Education



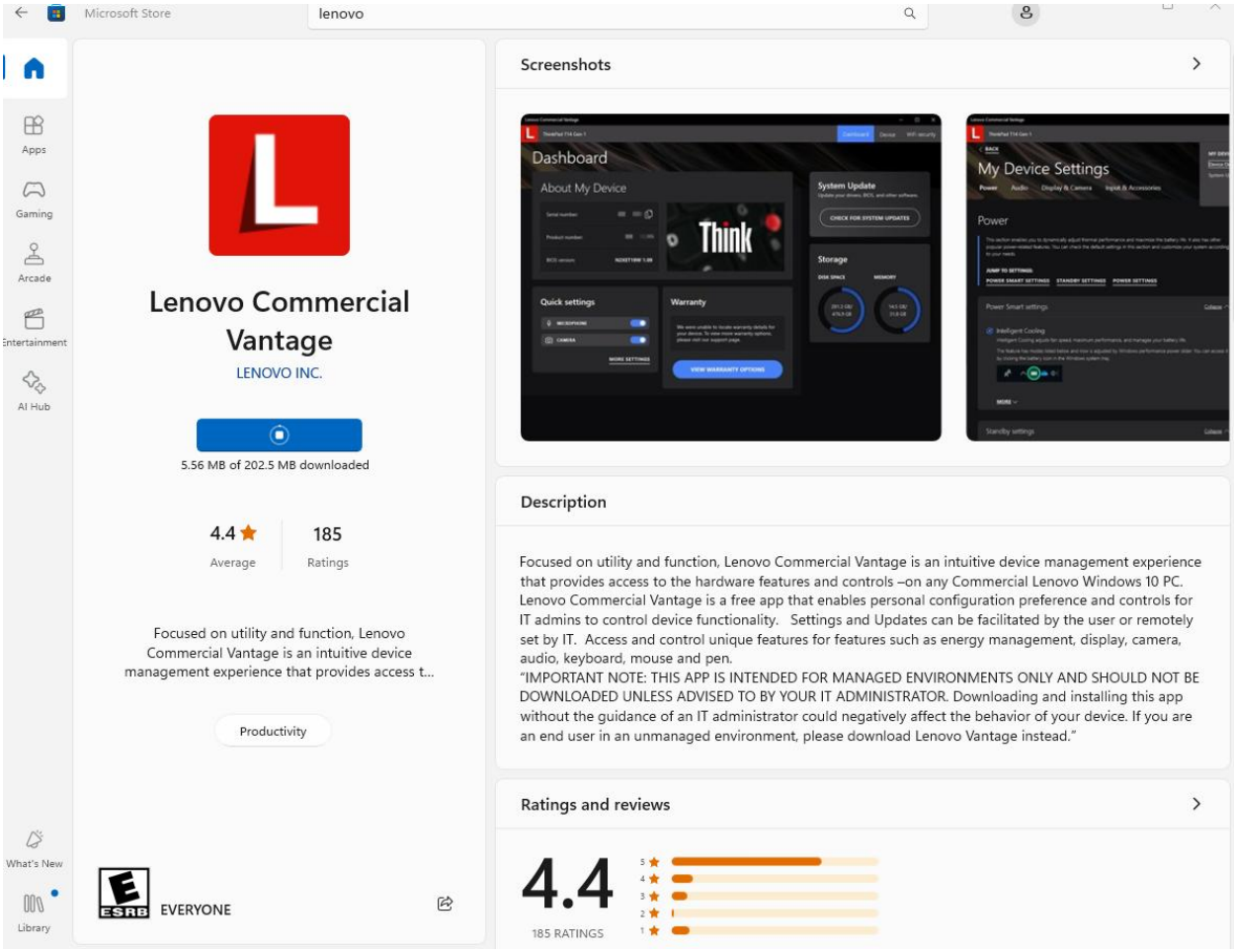
Steps 2: install driver for Lenovo Computer, first go to Lenovo support page, let it scan for your serial number,

Steps 3: Lenovo website will suggest that you download the application called Lenovo Service Bridge. This is for getting your serial number. After you get your serial number, The Website should suggest the driver that you need to install for your computer, click on the recommended one and it should start downloading the driver that the computer needs.

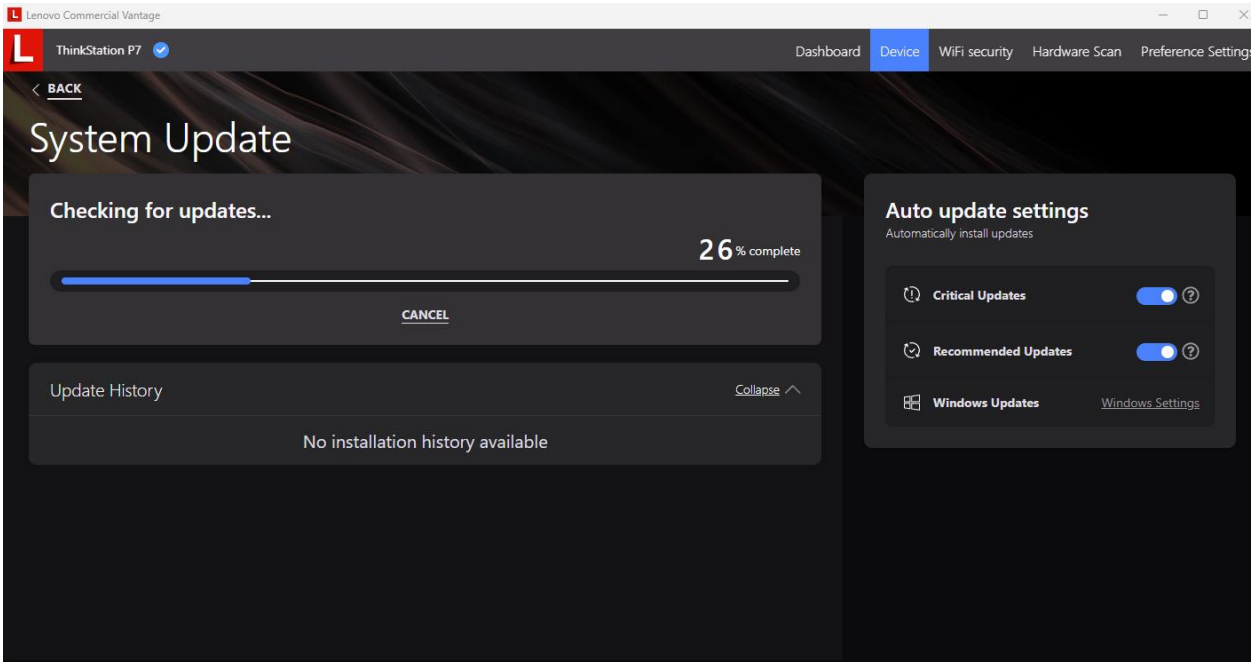


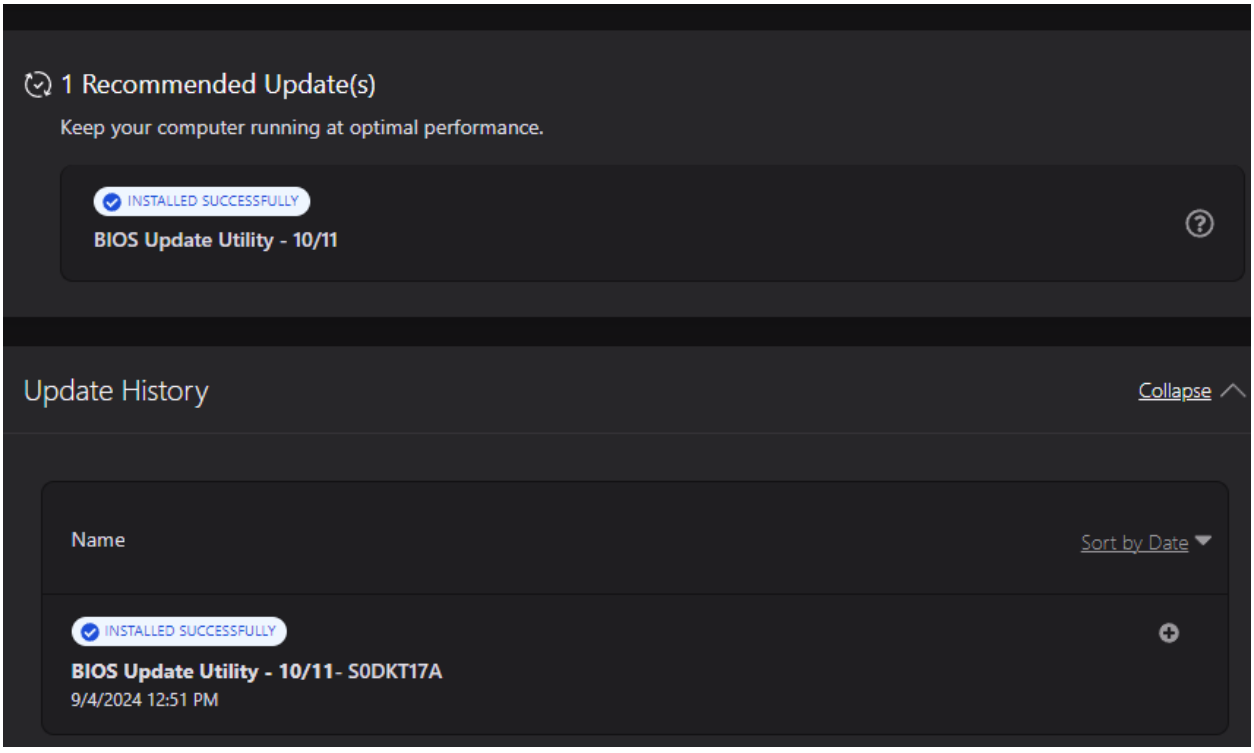


Steps4: Download Lenovo Commerical Vantage, first go to Microsoft store, then search for Lenovo Commerical Vantage, after you find it, click download to install the application.

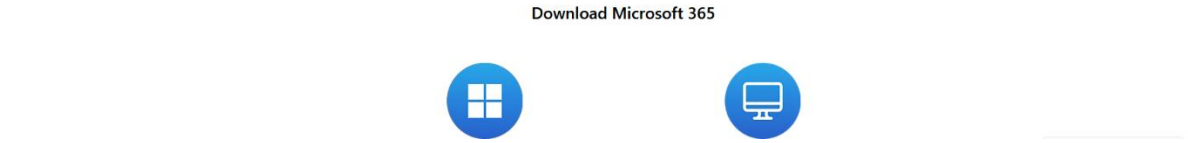


Steps5: After Lenovo Commercial Vantage was installed, check for any update for the Bios. For my computer, I have some Bios update, so I update all the Bios setting to Newest Version



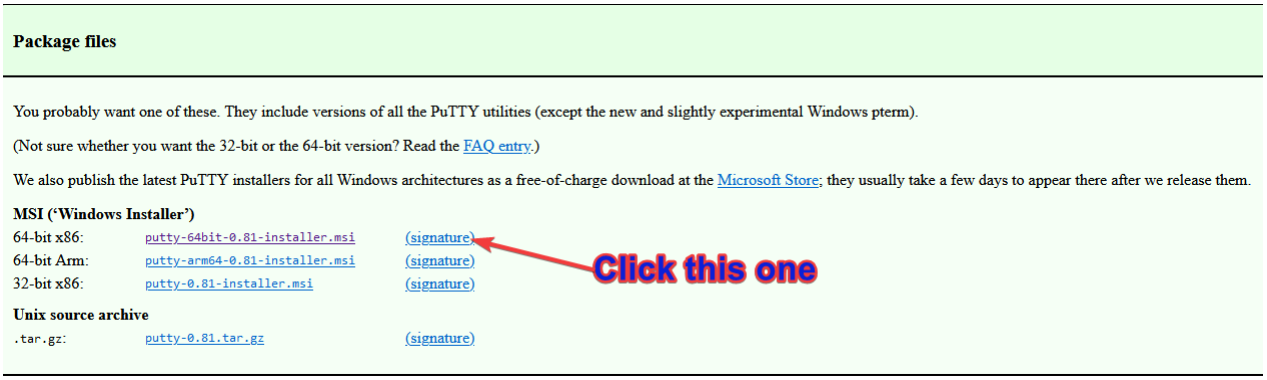


Steps 6: Install Office 365 for lab report, first go to www.microsoft.com/en-us/microsoft-365/download-office Click on the download button

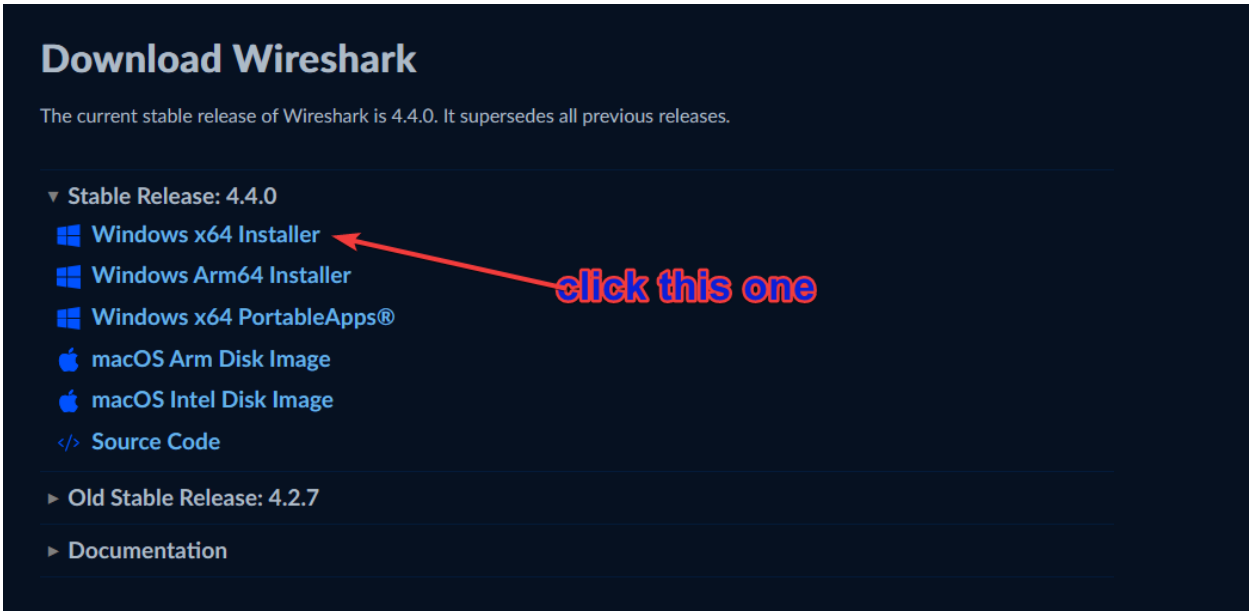


Steps 7: click on the office Setup.exe to install Office 365, after click on it, it will start downloading Office, Then wait for it to finish install, after it installed, use your office 365 account to login.

Steps 8: Download PuTTY and wireshark (optional), first go to https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html and



After the installer download, run the installer and it should auto install PuTTY. For Wireshark, go to this website https://www.wireshark.org/download.html and



It will automatically download wireshark, when wireshark suggest you to download other applications, it is optional to download.

Problem: In this lab, I only faced one problem, which was that I could not find the actual Lenovo Commerical Vantage application in website, after I asked my classmates, they showed me I could Download it from the Microsoft store.

Conclusion: In this lab, I set up my hard drive and I downloaded the application that I needed for future lab. For example, PuTTY for configure router, switch and firewall, Wireshark for capture traffic to find the problem inside the network, Lenovo Driver and commerical Vantage for normal uses of the computer, Office 365 allow us to write to lab report more easily. I learn more about how to set up a labs uses computers .

Lab 1: Factory reset and update admin password for Paloalto PA-220 firewall

By Alvin Chow

Purpose: Learn how to remove all saved config on the PA-220 firewall by doing a factory reset and learn how to set up a new admin password to prevent some unwanted user login to the Firewall, we factory reset the firewall for future Cybersecurity lab uses.

Background information:

The Palo Alto Networks® PA-220 next-generation firewall is designed for small organizations or branch offices. This firewall included passive cooling to reduce noise and power consumption, eight Ethernet ports, and dual power adapters for power redundancy. The PA-220 firewall enables to secure the organization through advanced visibility and control of applications, users, and content.

Palo Alto Networks (Palo Alto) provides cybersecurity services to enterprises, government, and service providers. This company's products and services portfolio include firewall and software, panorama, support and maintenance services, security management solutions, and virtual system upgrades.

Lab Summary:

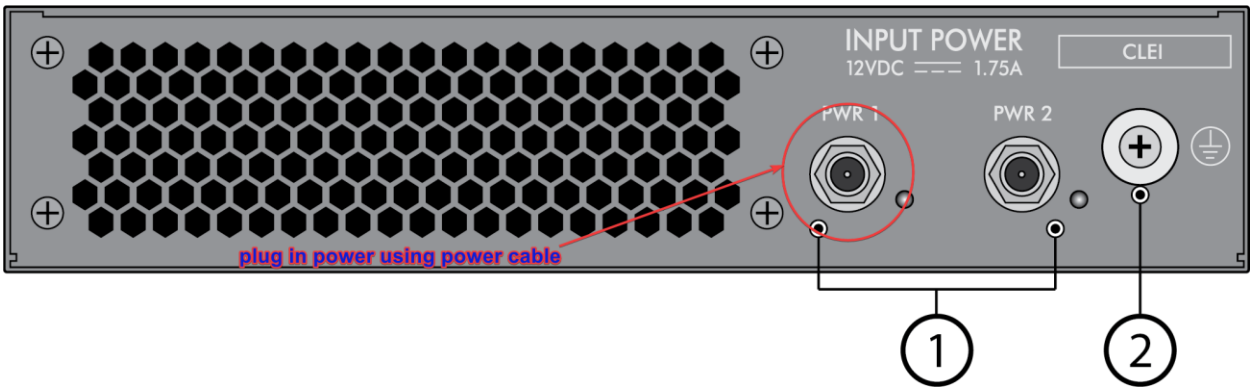
First When we received the Firewall that have some config already save on the firewall and we don't have any login credentials to login.

First, when we power it on, first we try to get into maintenance mode and find the Factory Reset option, then we confirm to use the most updated image Operation System version for the firewall and wait for it to factory reset and reboot the firewall again after factory reset.

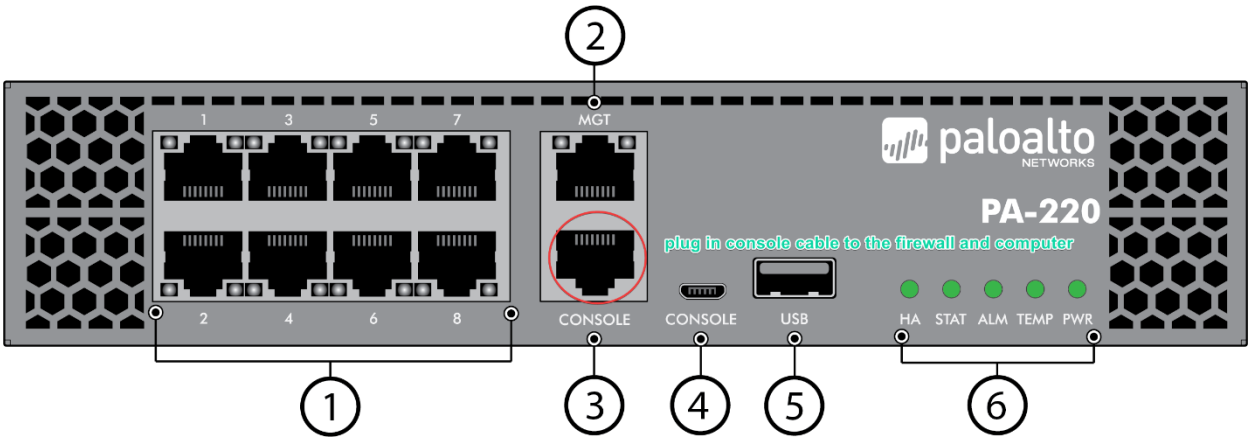
After the Factory reset, we login using default admin password and changed default admin password, then save the configuration, so we can continue to use this firewall for future labs.

Lab Commands:

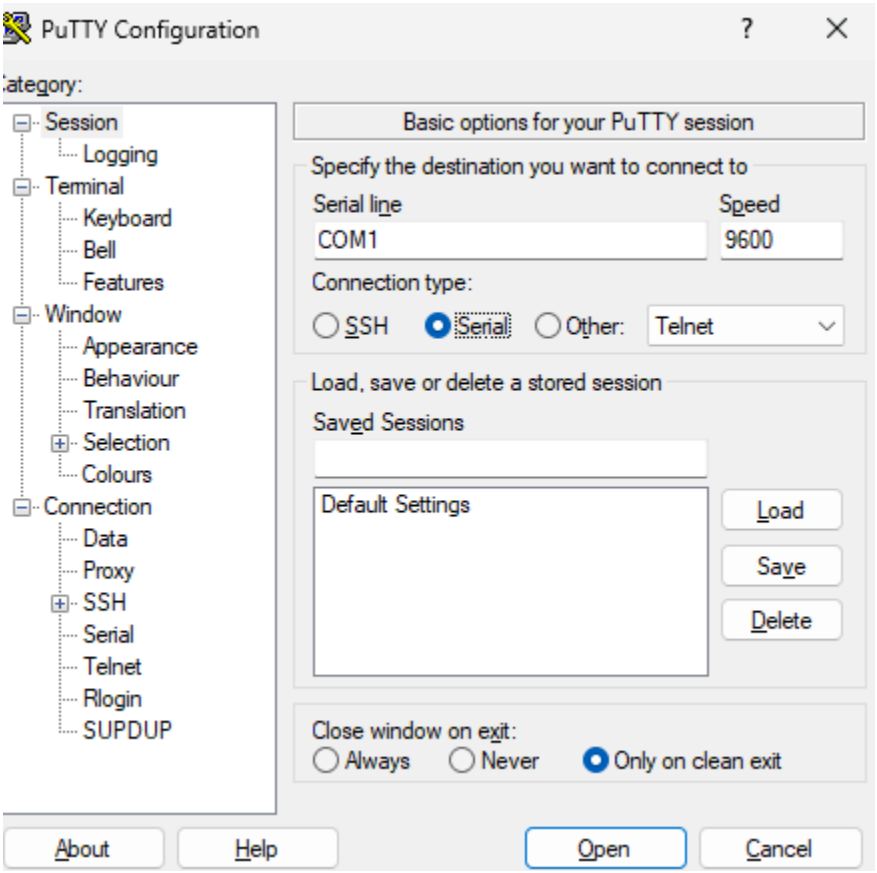
Steps 1: plug in power to the firewall.



Steps 2: plug in console cable to firewall and computer.



Steps 3: Open up PuTTY for access firewall command line, then enter the correct Serial line for your computer



Steps 4: When we accessed the command line of the firewall and when the “enter maint to boot in maintenance screen” pop up, we enter the command “maint” so I can trying go to

maintenance mode for factory reset.

```
        Autoboot to default partition in 5 seconds.
        Enter 'maint' to boot to maint partition.

Entry: maint

Booting to maint mode.
```

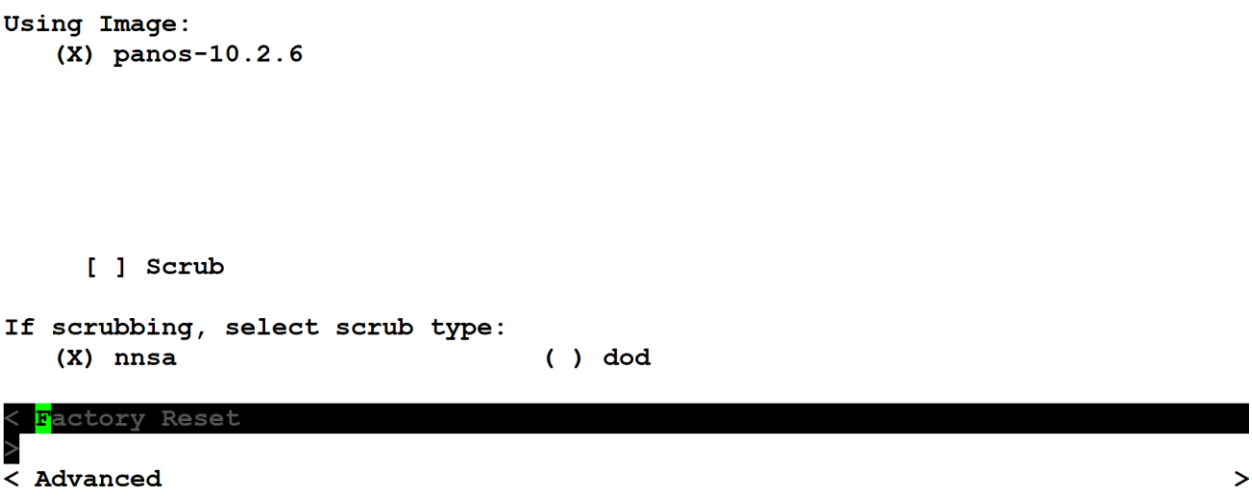
```
    Welcome to maintenance mode. For support please contact Palo Alto
    Networks.

                866-898-9087 or support@paloaltonetworks.com

< Continue
>
```

Steps 5: After the Welcome Screen pop up, we click continue to enter the Maintenance mode menu.

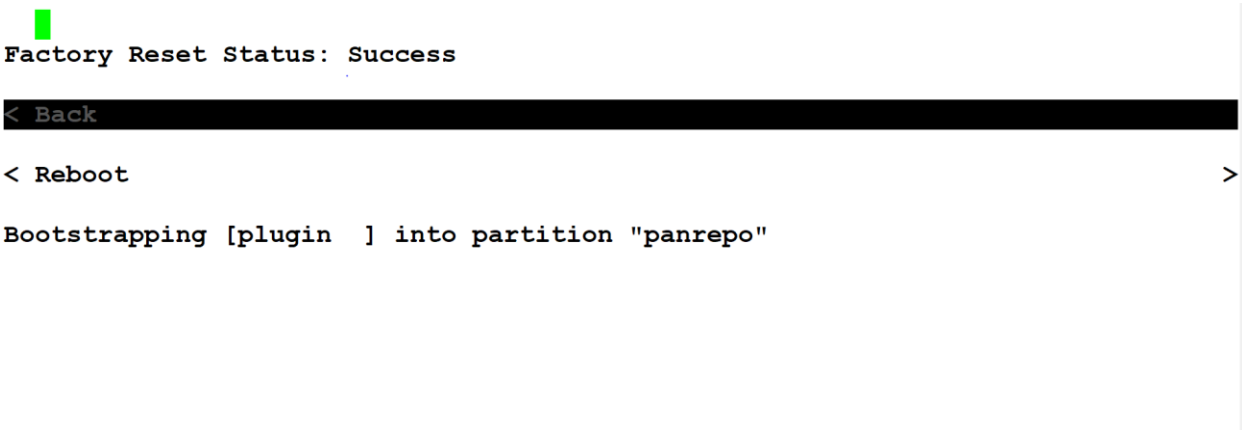
```
< Maintenance Entry Reason
>
```

```
< Maintenance Entry Reason
< Get System Info
< Factory Reset
> Set FIPS-CC Mode                                                    >
< FSCK (Disk Check)                                                  >
< Log Files                                                          >
< Bootloader Recovery                                                >
< Disk Image                                                         >
< Select Running Config                                              >
< Content Rollback                                                   >
< Set IP Address                                                     >
< Diagnostics                                                        >
< Debug Reboot                                                       >
< Reboot                                                             >
```

Steps 6: After we see the Maintenance mode menu, we click factory Reset for starting Factory Reset of the Firewall.



Steps 7: We need to make sure the firewall used panos version 10.2 because this is the newest firewall OS image for PA-220 and we need to click Factory Reset to start the factory reset.



Steps 8: When Firewall complete the factory reset, we need to click the Reboot option to let the firewall Reboot after factory reset.

Steps 9: After the firewall rebooted, we needs to let the firewall accept default admin/admin password, first it should only show “220 login”, after few attempts using default password it will change to “PA-HDF” login, then try to login using default password again for few times, after that, it will change to PA-220 login.

```
PA-220 login: admin
Password:
Last login: Fri Sep  6 12:16:01 on ttyS0
Enter old password :
Enter new password :
Confirm password   :
Password changed



Number of failed attempts since last successful login: 0


Warning: Your device is still configured with the default admin account credent
ials. Please change your password prior to deployment.
```

Steps 10: after we used the default password to login, it will let us change the admin password, we need to enter the default password for the old password, then you can enter any password that fulfill the requirements.

```
admin@PA-220>
admin@PA-220>
```

Steps 11: After we login to PA-220 using the admin password, we still need change the admin password again.

Steps 12: First, we go to configure mode, then enter the command “set mgt-config user admin password”, then we can enter the new admin password, and enter it again to confirm. Finally, we need to commit it for saving the configuration.

```
admin@PA-220>
admin@PA-220> configure
Entering configuration mode
[edit]
admin@PA-220# set mgt-config users admin password
Enter password   :
Confirm password :

[edit]
admin@PA-220# comit
Unknown command: comit
[edit]
admin@PA-220# commit


Server error : Commit job was not queued since auto-commit nc
[edit]
admin@PA-220# commit force
```

Problems: First, we didn’t know we needed to change the password again after we login to the firewall, Second, we forgot to save the configuration by using the “commit” command after we entered the “set mgt-config user admin password” we cannot log in to the firewall next day, so we need to do the factory reset again. This causes us to waste a lot of time waiting for factory reset and Reboot.

Conclusion: In this lab We got a Palo Alto PA-220 firewall that has saved configuration inside, we learned how to factory reset by going to maintain mode to remove all saved configurations and set up a new admin password to prevent unwanted users from login the firewall.

PA-220 SOHO Network set up

By Alvin Chow

Purpose: In this lab, we learned more about how to do some basic config by setting up the SOHO network using Palo alto PA-220 firewall, we learned more about why and how to set up Zones, how to change interface types, how to allow or blocked traffic, how to set up DHCP server and how to let LAN traffic go to internet by setting up NAT translation.

Background info: The Palo Alto Networks® PA-220 next-generation firewall is designed for small organizations or branch offices. This firewall included passive cooling to reduce noise and power consumption, eight Ethernet ports, and dual power adapters for power redundancy. The PA-220 firewall enables to secure the organization through advanced visibility and control of applications, users, and content.

Palo Alto Networks (Palo Alto) provides cybersecurity services to enterprises, government, and service providers. This company's products and services portfolio include firewall and software, panorama, support and maintenance services, security management solutions, and virtual system upgrades.

SOHO, which stands for Small Office/Home Office, refers to a network designed for small businesses and individuals operating within limited physical workspaces, such as homes or small offices.

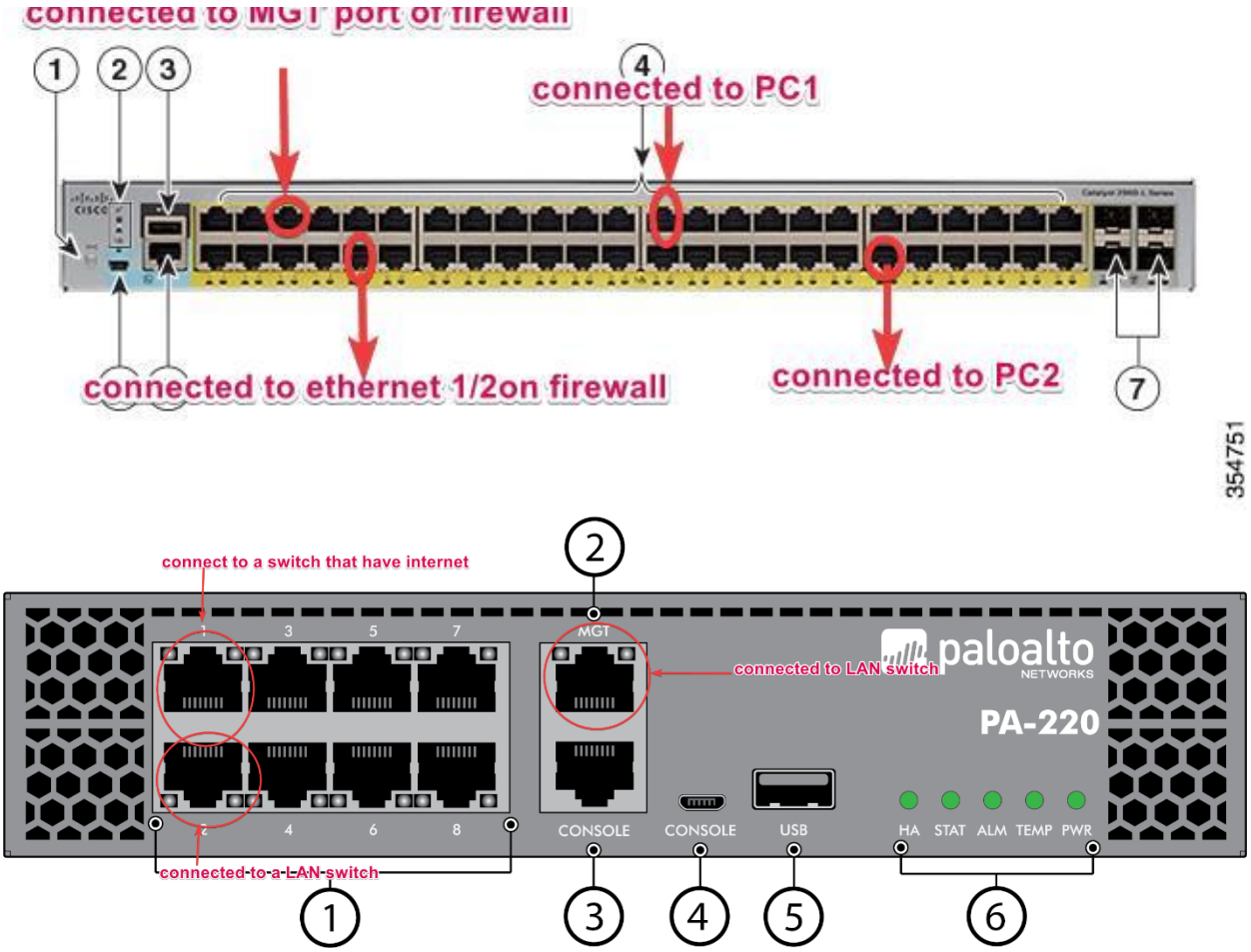
NAT stands for network address translation. It's a way to let multiple private ip addresses inside a local network to a public IP address that used for allowing information to reach internet.

Security zones are a good way to group the physical and virtual interfaces on the firewall to control and log. An interface on the firewall must be assigned to a security zone before the interface can process traffic. Zones also prevent uncontrolled traffic flow into your network.

DHCP is a client/server protocol that automatically provides an ip address to the host and other configuration information such as the subnet mask and default gateway to the users within that network

Lab summary:

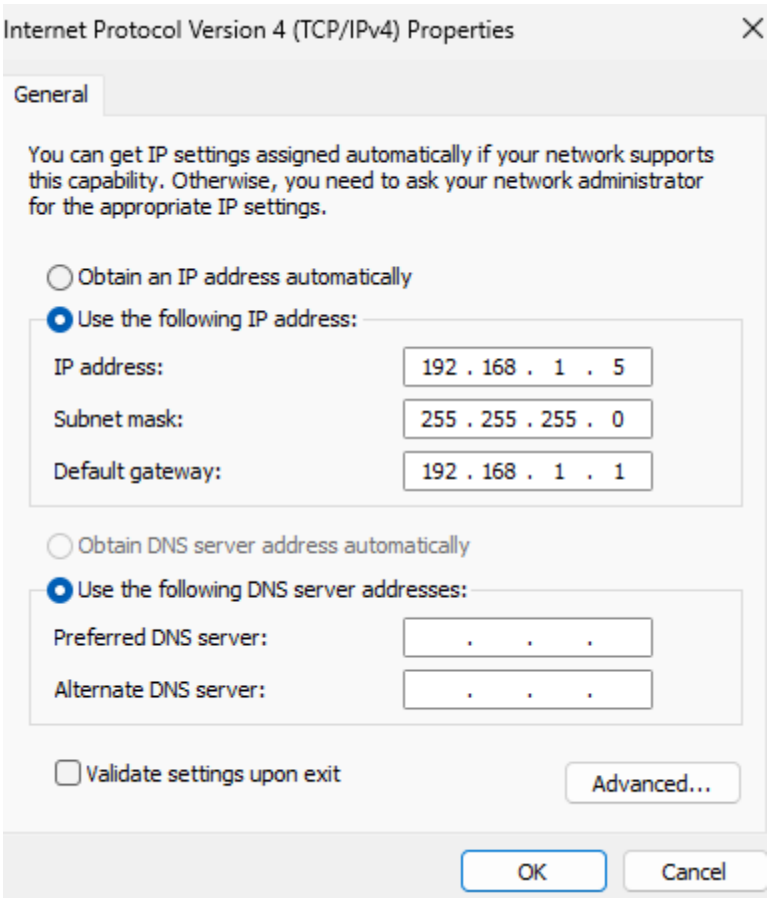
Steps 1**:** First, I connected my ethernet 1/1 to the switch that connected to internet, this act like my WAN port, then I connected my ethernet1 /2 to the switch, that act like my LAN port, then I connect my MGT port to switch and I connected both of my pc to the LAN switch.



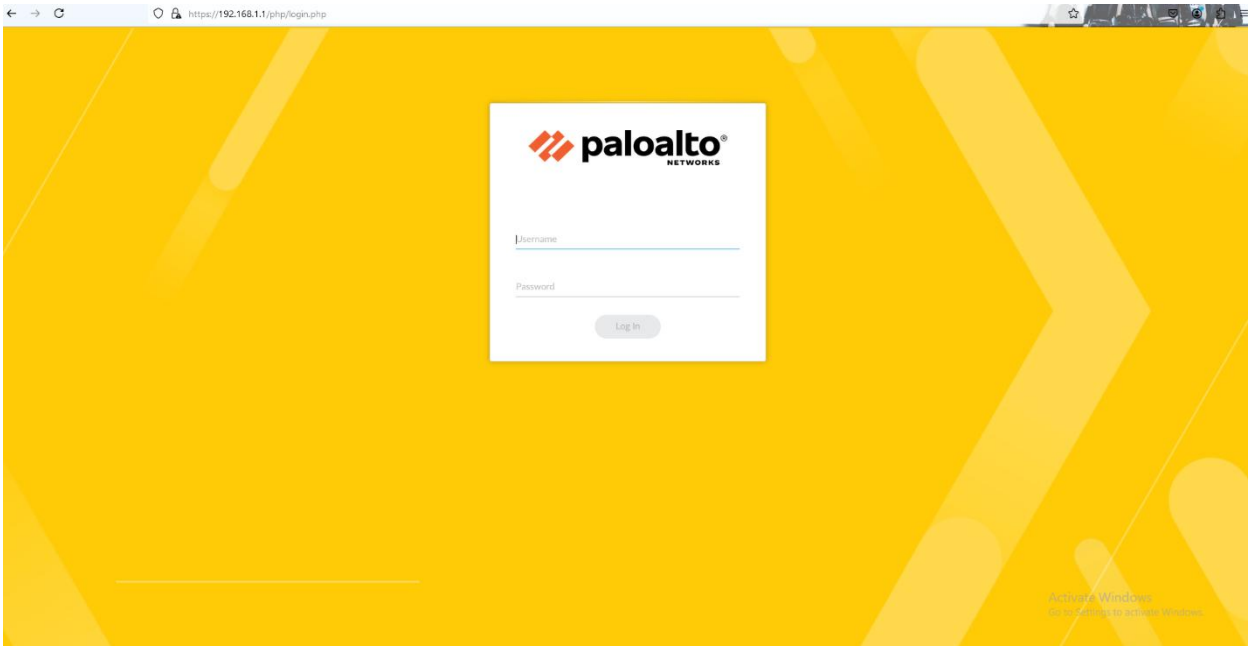
Steps 2: access firewall GUI interface

You need to have console accress to your firewall, then type in this command, this help you set up the management port ip and you can save the config.

```
admin@PA-220# set deviceconfig system ip-address 192.168.1.1 netmask 255.255.25
.0

[edit]
admin@PA-220# commit
```

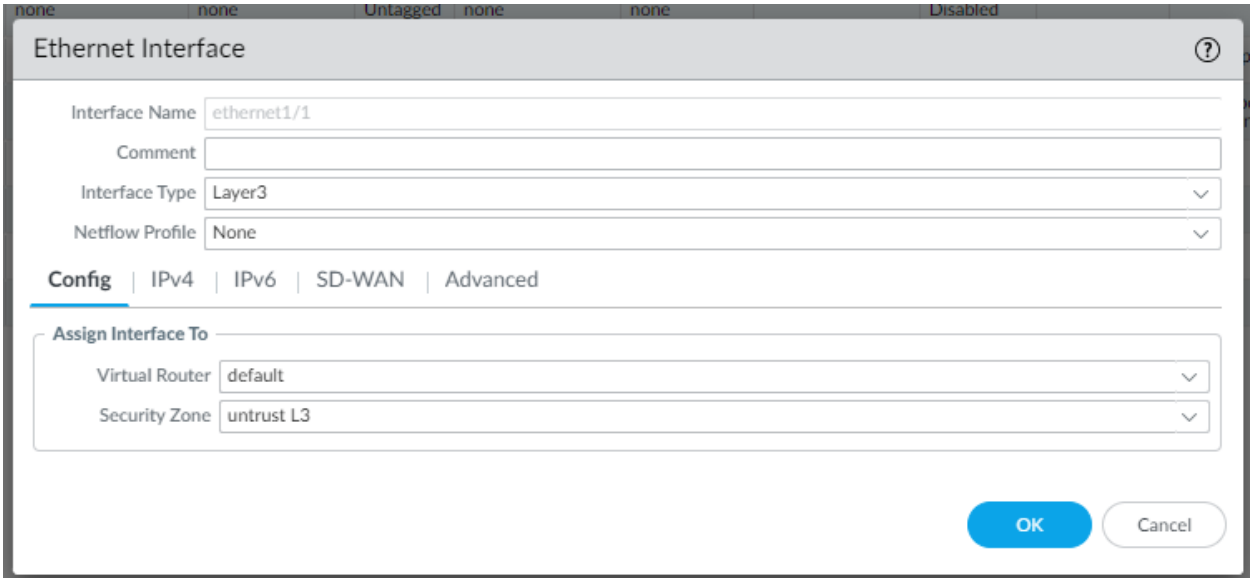


Then you need to set up static ip on your computer that on the same subnet as the firewall. After that, you can access to the web GUI using the ip that you set up on mgt port.



Steps 3: remove all the unused stuff, for example virtual wire, then commit every change that you made on the firewall.

Steps 4: In this lab, we use ethernet 1/1 to be the WAN port so this is the setting of the interface



First we change to interface type to Layer 3, then we put this interface at untrust L3 zones, because internet information is not trustable.

Steps 5: In this lab, my group choose to set up a layer 3 interface instead of multiple layer 2 and vlan interface, because we think it is more easier to do, first we change to interface type to layer 3 and set up the static ip of 192.168.2.1 for that interface that connect to our LAN switch, and this is a trust port because it is where all the users located.

INTERFACE	INTERFACE TYPE	MANAGEMENT PROFILE	LINK STATE	IP ADDRESS	VIRTUAL ROUTER	TAG	VLAN / VIRTUAL-WIRE	SECURITY ZONE	SD-WAN INTERFACE PROFILE	UPSTREAM NAT	FEATURES	COMMENT
ethernet1/1	Layer3			Dynamic-DHCP Client	default	Untagged	none	untrust L3		Disabled		
ethernet1/2	Layer3			none	none	Untagged	none	none		Disabled		
ethernet1/3	Layer3			192.168.2.1/24	default	Untagged	none	trust L3		Disabled		trusted port

Steps 6: Put all the interface to correct zone, In this lab, we put ethernet 1/1 to be untrust L3, then we put 1/3 to be trust L3

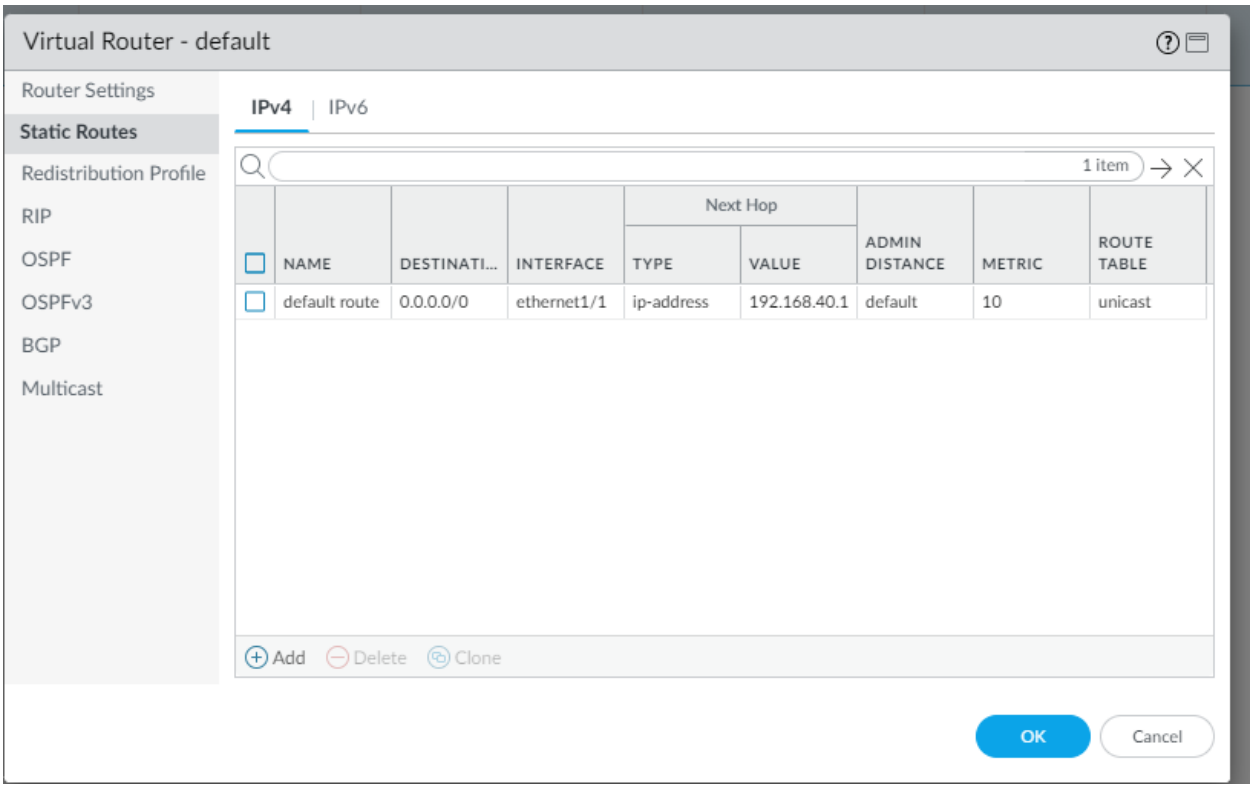
NAME	TYPE	SYSTEMS	PROFILE	PROTECTION	LOG SETTING	ENABLED	INCLUDED NETWORKS	EXCLUDED NETWORKS	ENABLED	INCLUDED NETWORKS	EXCLUDED NETWORKS
trust L2	layer2						any	none		any	none
trust L3	layer3	ethernet1/3 ethernet1/4 ethernet1/5 ethernet1/6 vlan					any	none		any	none
untrust	virtual-wire						any	none		any	none
untrust L3	layer3	ethernet1/1					any	none		any	none

Steps 7: We need to set up DHCP server for all the hosts that connected to the LAN switch, we prefer to save first 10 usable ip address to be static, for example we save 192.168.2.1 to be the ip of the ethernet 1/3 interface, we set the gateway to be 192.168.2.1 because this is

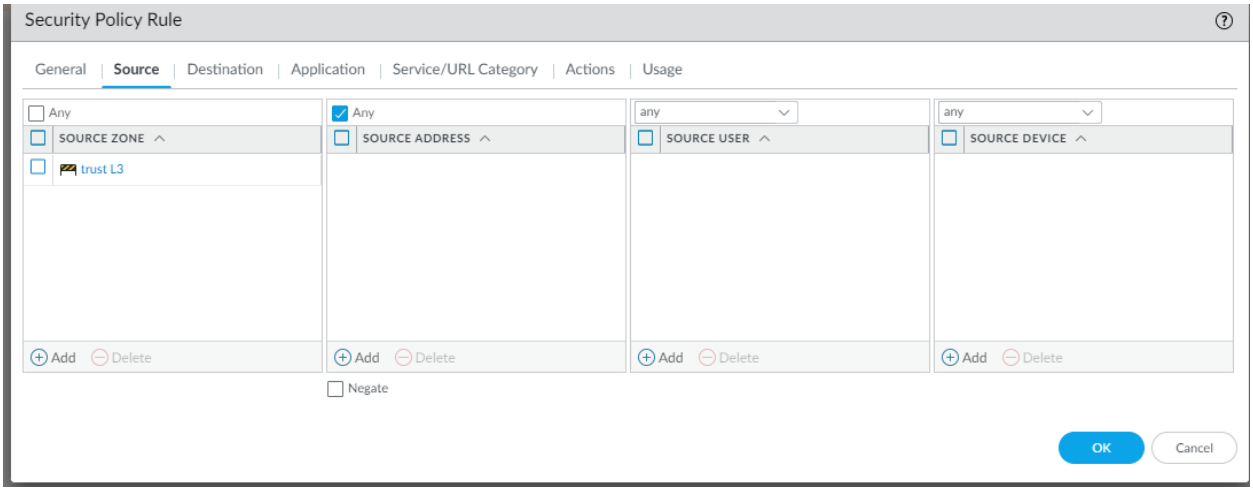
the port that act like default gateway of the LAN and we use the DNS setting of the WAN port to the LAN users DNS.

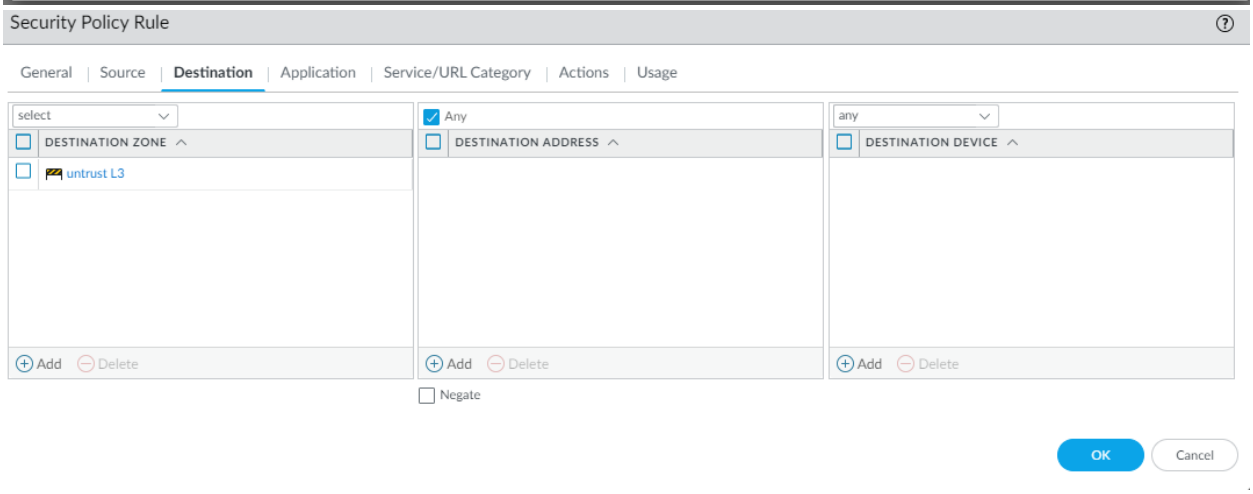
INTERFACE	MODE	PROBE IP	OPTIONS	IP POOLS	RESERVED
ethernet1/3	enabled		View Inherited Settings Lease: Unlimited DNS: inherited,inherited Gateway: 192.168.2.1	View Allocation 192.168.2.10-192.168.2.210	

Steps 8: When we trying reach internet, we need to set up a default route, the destination is 0.0.0.0/0 and the outgoing interface is ethernet 1/1 and we know the next hop ip by checking the DHCP client status on ethernet 1/1.

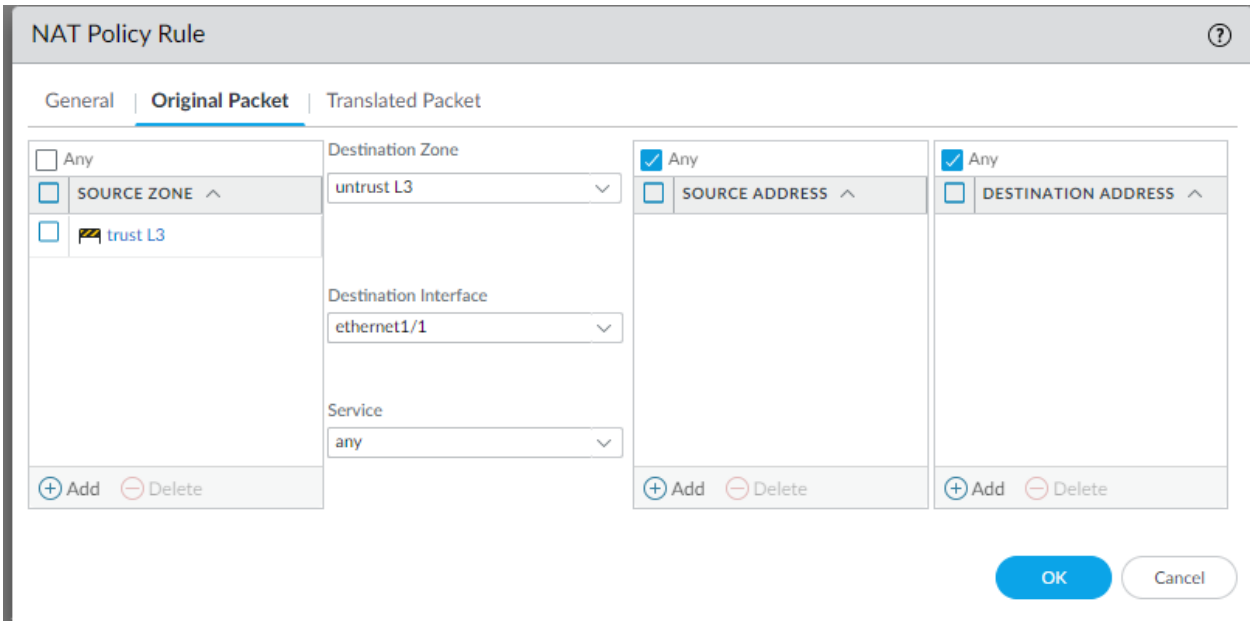


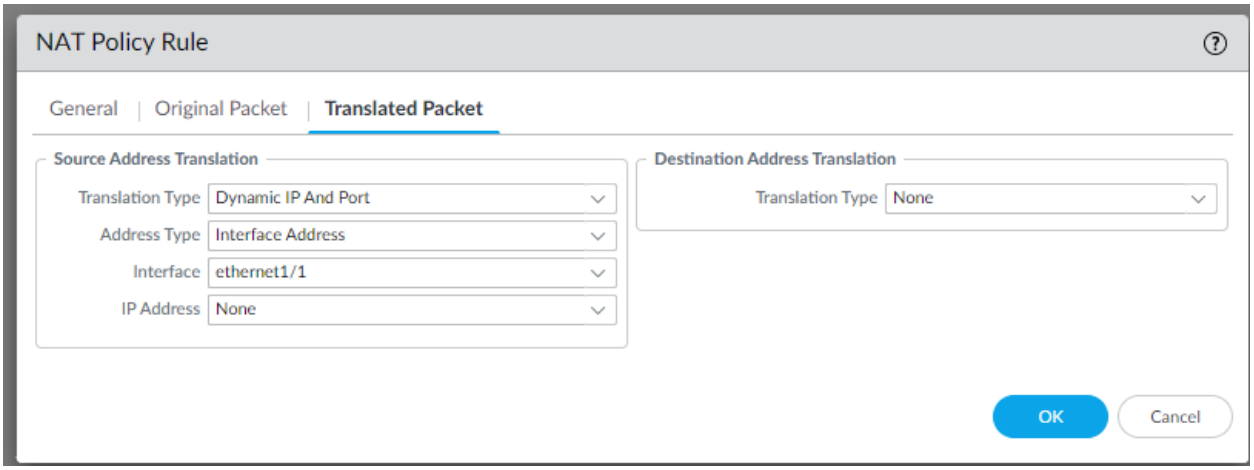
Steps 9: Allow traffic from trust zone to untrust zone, first go to policies and ad rule on security, we need to choose source to be trust L3 and destination is untrust L3, because it trying to reach internet which is untrust zone



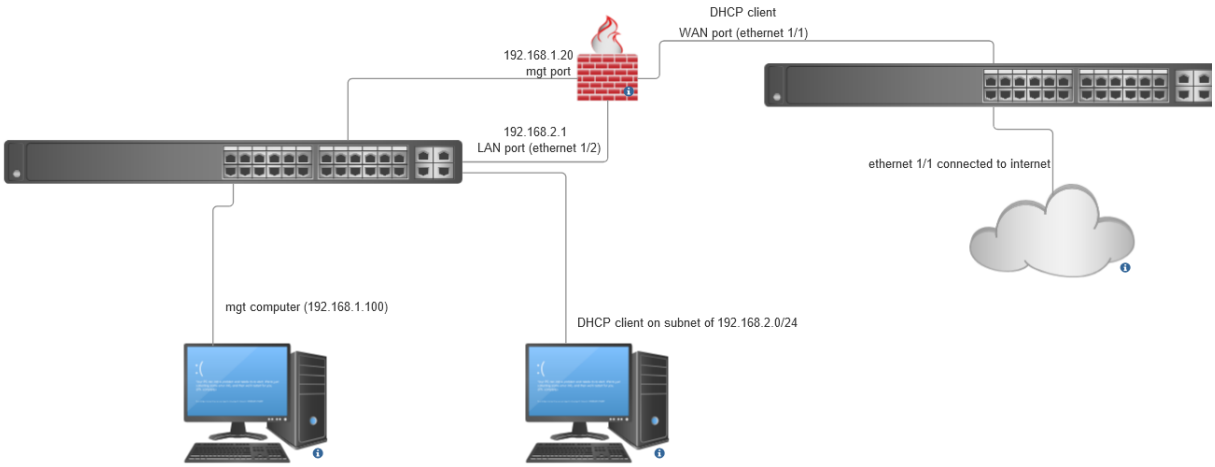


Steps 10: In this steps, we needs to set up the NAT rules for reaching internet, go to policies and click NAT, set the original Packet to this, source is trust L3, destination to untrust L3 by WAN port, then set the translation type to my dynamic IP and Port because we only got one “public ip” and we translate the packet to be ethernet 1/1 interface ip with port number.


NAT Policy Rule
General
Original Packet
Translated Packet
Any
SOURCE ZONE
trust L3
Add
Delete
Destination Zone
untrust L3
Destination Interface
ethernet1/1
Service
any
Any
SOURCE ADDRESS
Add
Delete
Any
DESTINATION ADDRESS
Add
Delete
OK
Cancel


NAT Policy Rule
General
Original Packet
Translated Packet
Source Address Translation
Translation Type
Dynamic IP And Port
Address Type
Interface Address
Interface
ethernet1/1
IP Address
None
Destination Address Translation
Translation Type
None
OK
Cancel

Network diagram:



Problems: At the start of the lab, we don't know we need to remove the virtual wire, so we cannot commit any changes and our cabling also is not correct, so we cannot commit any changes, after we use switch and connect all the pc to the switch, everything is working. Second problem that we faced is we cannot access to internet using our "WAN port", because the switch that we connected to don't have any internet access, so we cannot do dhcp request to get the WAN port working, we fix it by cable to other port on the wall and the "WAN switch" is working fine.

Conclusion: In this lab, we learned more about some basic config by making the firewall that can filter traffic also can route traffic to internet by setting a default static route to WAN port and NAT translation at WAN port, we also learned palo alto firewall use zones to isolate the trusted traffic and untrusted traffic. We also learn how to set a interface ip and DHCP server that allow user can get ip automatically and allow users can reach internet without any problems.

Mult Area OSPF Lab

By Alvin Chow

Purpose: In this lab, we learned how to configure Mult area OSPF with required using 5 routers and one mult-layers switch (layer 3 switch). In this lab we refresh our brain of how to config a Cisco router and a Switch, this lab also help us help to set up OSPF and help us design the network that fulfilled the requirement.

Background information: Open shortest path first (OSPF) is a routing protocol for internet, it uses link state routing algorithm, and it is a interior gateway protocol. It functions y determine the shortest path to the destination and it calculated base on bandwidth, delay and cost.

Cisco is the worldwide technology leader for making network device Since 1984. Cisco specializes in networking hardware, software, telecommunications equipment, and high-technology services. The company is best known for development of internet protocol based networking solutions, including routers, switches, and cybersecurity products.

Cisco 4321 router designed for small to medium-sized branch offices. It offers a balance of performance and features, supporting secure connectivity, advanced routing, and a range of services such as voice and video.

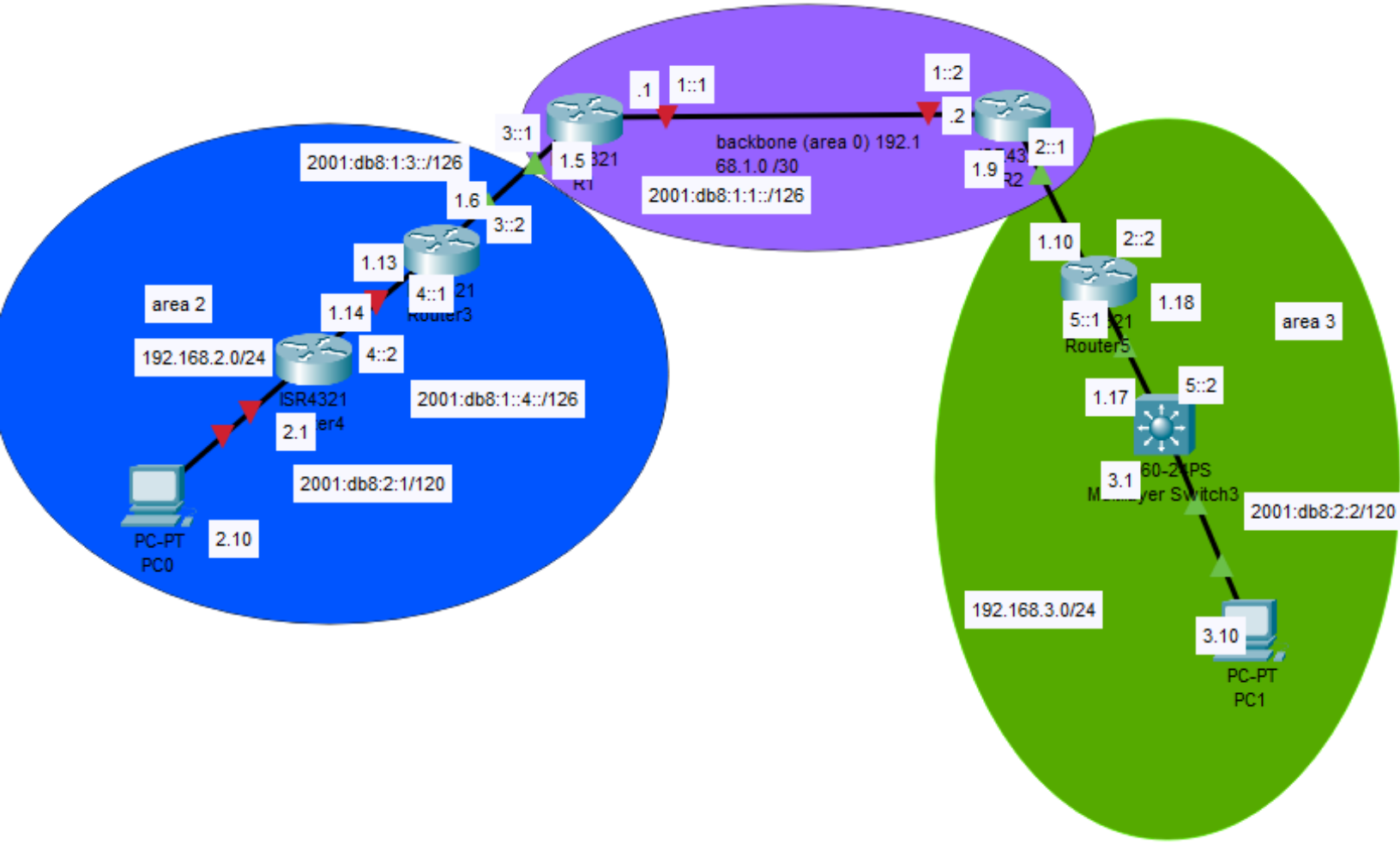
The Cisco 3560 switch is a Layer 3, managed switch designed for enterprise networks. It has some advanced function such as VLAN support, Qos and enhanced security protocols. With support for both IPv4 and IPv6, so this a good device for enterprise networks.

Layer 2 and Layer 3 switch, layer 2 is good for local routing that don't need vlan routing, layer 2 forward traffic based on the MAC address(physical address), Every device have different MAC address, so layer 2 switch can forward traffic based on MAC address, but layer 3 switch can forward traffic based on ip or MAC address, but is require more configuration for layer 3 switches. Overall the main different between layer 2 and layer 3 switch is layer 2 devices on forward traffic based on MAC address, but layer 3 switch can forward traffic based on MAC or ip address, which is good for enterprise network.

Lab summary: First, me and my partner decided to use 192.168.1.0/24 to be the management ip subnet, then for not wasting ip, we use /30 for every router connected to every router and switch, this can make us have good amount of ip for future uses. Then we used R1 and R2 to be the backbone router, R3 and R4 to be on their own area, then R5 and Multilayer switch on the same area. We decided to use area 2 and 3 because on our host subnet, we use 192.168.2.0/24 and 192.168.3.0/24 because we don't know how many hosts we have on the host subnet. For ipv6, we decided to use 2001:db8:1 to be our management device ip, then we used 2001:db8:2 and 2001:db8:3 to be our host subnet ip

address and we use same area number as the ipv4 because we think it can help us to find problems easier.

Network Diagram:



Lab commands:

no switchport, this is the command for multilayer switch to enable layer 3 function.

ip address and subnet mask, this command used for setting up the static ip for the layer 3 interface.

router ospf and process id, this command let us to enter config routing mode, which can let us to enter network for setting up ospf on that interface.

network, network ip and wildcard mask, this let us to start ospf for that interface.

Ipv6 unicast routing, this command let us to start ipv6 function on router and switch.

Ipv6 address and the subnet prefix, this let us set up the ipv6 address for the layer 3 interface.

Ipv6 ospf process id area number, this command let us to run ipv6 ospf on that interface.

Configurations:

R1 config:

version 15.5

service timestamps debug datetime msec

service timestamps log datetime msec

no platform punt-keepalive disable-kernel-core

hostname R1

boot-start-marker

boot-end-marker

vrf definition Mgmt-intf

address-family ipv4

exit-address-family

address-family ipv6

exit-address-family

no aaa new-model

ipv6 unicast-routing

subscriber templating

vtp domain cisco

vtp mode transparent

multilink bundle-name authenticated

```
license udi pid ISR4321/K9 sn FDO214421BY
spanning-tree extend system-id
redundancy
mode none
vlan internal allocation policy ascending
interface GigabitEthernet0/0/0
ip address 192.168.1.1 255.255.255.252
negotiation auto
ipv6 address 2001:DB8:1:1::1/126
ipv6 enable
ipv6 ospf 10 area 0
interface GigabitEthernet0/0/1
ip address 192.168.1.5 255.255.255.252
negotiation auto
ipv6 address 2001:DB8:1:3::1/126
ipv6 enable
ipv6 ospf 10 area 2
interface Serial0/1/0
no ip address
shutdown
interface Serial0/1/1
no ip address
shutdown
interface GigabitEthernet0/2/0
no ip address
shutdown
```

```
negotiation auto
interface GigabitEthernet0/2/1
no ip address
shutdown
negotiation auto
interface GigabitEthernet0
vrf forwarding Mgmt-intf
no ip address
shutdown
negotiation auto
interface Vlan1
no ip address
shutdown
router ospf 10
network 192.168.1.0 0.0.0.3 area 0
network 192.168.1.4 0.0.0.3 area 2
ip forward-protocol nd
no ip http server
no ip http secure-server
ip tftp source-interface GigabitEthernet0
ipv6 router ospf 10
control-plane
line con 0
stopbits 1
line aux 0
stopbits 1
```

```
R1#show ipv6 route
IPv6 Routing Table - default - 10 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, I1 - ISIS L1, I2 - ISIS L2
       IA - ISIS interarea, IS - ISIS summary, D - EIGRP, EX - EIGRP external
       ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2, a - Application
C   2001:DB8:1:1::/126 [0/0]
     via GigabitEthernet0/0/0, directly connected
L   2001:DB8:1:1::1/128 [0/0]
     via GigabitEthernet0/0/0, receive
OI  2001:DB8:1:2::/126 [110/2]
     via FE80::B6A8:B9FF:FE47:92C0, GigabitEthernet0/0/0
C   2001:DB8:1:3::/126 [0/0]
     via GigabitEthernet0/0/1, directly connected
L   2001:DB8:1:3::1/128 [0/0]
     via GigabitEthernet0/0/1, receive
O   2001:DB8:1:4::/126 [110/2]
     via FE80::B6A8:B9FF:FE01:AE51, GigabitEthernet0/0/1
OI  2001:DB8:1:5::/126 [110/3]
     via FE80::B6A8:B9FF:FE47:92C0, GigabitEthernet0/0/0
O   2001:DB8:2:1::/120 [110/3]
     via FE80::B6A8:B9FF:FE01:AE51, GigabitEthernet0/0/1
OI  2001:DB8:2:2::/120 [110/4]
     via FE80::B6A8:B9FF:FE47:92C0, GigabitEthernet0/0/0
L   FF00::/8 [0/0]
     via Null0, receive
```

line vty 0 4

login

end

R2:

```
R1(config)#do show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is not set

      192.168.1.0/24 is variably subnetted, 6 subnets, 2 masks
C        192.168.1.0/30 is directly connected, GigabitEthernet0/0/0
L        192.168.1.1/32 is directly connected, GigabitEthernet0/0/0
C        192.168.1.4/30 is directly connected, GigabitEthernet0/0/1
L        192.168.1.5/32 is directly connected, GigabitEthernet0/0/1
O IA     192.168.1.8/30
           [110/2] via 192.168.1.2, 00:09:50, GigabitEthernet0/0/0
O IA     192.168.1.16/30
           [110/3] via 192.168.1.2, 00:09:50, GigabitEthernet0/0/0
O IA  192.168.3.0/24 [110/4] via 192.168.1.2, 00:09:50, GigabitEthernet0/0/0
```

```
version 15.5
service timestamps debug datetime msec
service timestamps log datetime msec
no platform punt-keepalive disable-kernel-core
hostname R2
boot-start-marker
boot-end-marker
vrf definition Mgmt-intf
address-family ipv4
exit-address-family
address-family ipv6
exit-address-family
no aaa new-model
ipv6 unicast-routing
subscriber templating
multilink bundle-name authenticated
license udi pid ISR4321/K9 sn FDO214420QQ
license accept end user agreement
license boot level securityk9
spanning-tree extend system-id
redundancy
mode none
vlan internal allocation policy ascending
interface GigabitEthernet0/0/0
ip address 192.168.1.2 255.255.255.252
negotiation auto
```

ipv6 address 2001:DB8:1:1::2/126

ipv6 enable

ipv6 ospf 10 area 0

interface GigabitEthernet0/0/1

ip address 192.168.1.9 255.255.255.252

negotiation auto

ipv6 enable

ipv6 ospf 10 area 3

interface Serial0/1/0

no ip address

shutdown

interface Serial0/1/1

no ip address

shutdown

interface GigabitEthernet0

vrf forwarding Mgmt-intf

no ip address

shutdown

negotiation auto

interface Vlan1

no ip address

shutdown

router ospf 10

network 192.168.1.0 0.0.0.3 area 0

network 192.168.1.8 0.0.0.3 area 3

ip forward-protocol nd

```
no ip http server
no ip http secure-server
ip tftp source-interface GigabitEthernet0
ipv6 router ospf 10
control-plane
line con 0
stopbits 1
line aux 0
stopbits 1
line vty 0 4
login
end
```

```
R2(config)#do show IPV6 route
IPv6 Routing Table - default - 8 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE - Destination
       NDr - Redirect, O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1
       OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       a - Application
C   2001:DB8:1:1::/126 [0/0]
     via GigabitEthernet0/0/0, directly connected
L   2001:DB8:1:1::2/128 [0/0]
     via GigabitEthernet0/0/0, receive
O   2001:DB8:1:2::/126 [110/1]
     via GigabitEthernet0/0/1, directly connected
OI  2001:DB8:1:3::/126 [110/2]
     via FE80::B6A8:B9FF:FE01:B510, GigabitEthernet0/0/0
OI  2001:DB8:1:4::/126 [110/3]
     via FE80::B6A8:B9FF:FE01:B510, GigabitEthernet0/0/0
O   2001:DB8:1:5::/126 [110/2]
     via FE80::6EDD:30FF:FEB6:6031, GigabitEthernet0/0/1
O   2001:DB8:2:2::/120 [110/3]
     via FE80::6EDD:30FF:FEB6:6031, GigabitEthernet0/0/1
L   FF00::/8 [0/0]
     via Null0, receive
R2(config)#
```

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is not set

      192.168.1.0/24 is variably subnetted, 7 subnets, 2 masks
C        192.168.1.0/30 is directly connected, GigabitEthernet0/0/0
L        192.168.1.2/32 is directly connected, GigabitEthernet0/0/0
O IA     192.168.1.4/30
           [110/2] via 192.168.1.1, 00:44:03, GigabitEthernet0/0/0
C        192.168.1.8/30 is directly connected, GigabitEthernet0/0/1
L        192.168.1.9/32 is directly connected, GigabitEthernet0/0/1
O IA     192.168.1.12/30
           [110/3] via 192.168.1.1, 00:28:07, GigabitEthernet0/0/0
O        192.168.1.16/30
           [110/2] via 192.168.1.10, 00:44:59, GigabitEthernet0/0/1
R2(config)#
```

R3:

version 15.5

service timestamps debug datetime msec

service timestamps log datetime msec

```
no platform punt-keepalive disable-kernel-core
hostname R3
boot-start-marker
boot-end-marker
vrf definition Mgmt-intf
address-family ipv4
exit-address-family
address-family ipv6
exit-address-family
no aaa new-model
ipv6 unicast-routing
subscriber templating
vtp domain cisco
vtp mode transparent
multilink bundle-name authenticated
license udi pid ISR4321/K9 sn FDO214420HY
license boot level securityk9
spanning-tree extend system-id
redundancy
mode none
vlan internal allocation policy ascending
vlan 10,20
interface GigabitEthernet0/0/0
ip address 192.168.1.13 255.255.255.252
negotiation auto
ipv6 address 2001:DB8:1:4::1/126
```

ipv6 enable

ipv6 ospf 10 area 2

interface GigabitEthernet0/0/1

ip address 192.168.1.6 255.255.255.252

negotiation auto

ipv6 address 2001:DB8:1:3::2/126

ipv6 enable

ipv6 ospf 10 area 2

interface Serial0/1/0

no ip address

interface Serial0/1/1

no ip address

interface GigabitEthernet0

vrf forwarding Mgmt-intf

no ip address

negotiation auto

interface Vlan1

no ip address

router ospf 10

network 192.168.1.4 0.0.0.3 area 2

network 192.168.1.12 0.0.0.3 area 2

ip forward-protocol nd

no ip http server

no ip http secure-server

ip tftp source-interface GigabitEthernet0

ipv6 router ospf 10

control-plane

line con 0

stopbits 1

line aux 0

stopbits 1

line vty 0 4

login

end

```
S3(config)#do  show ipv6 route
IPv6 Routing Table - Default - 10 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, D - EIGRP, EX - EIGRP external
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
OI  2001:DB8:1:1::/126 [110/3]
     via FE80::6EDD:30FF:FEB6:6030, FastEthernet0/1
O   2001:DB8:1:2::/126 [110/2]
     via FE80::6EDD:30FF:FEB6:6030, FastEthernet0/1
OI  2001:DB8:1:3::/126 [110/4]
     via FE80::6EDD:30FF:FEB6:6030, FastEthernet0/1
OI  2001:DB8:1:4::/126 [110/5]
     via FE80::6EDD:30FF:FEB6:6030, FastEthernet0/1
C   2001:DB8:1:5::/126 [0/0]
     via FastEthernet0/1, directly connected
L   2001:DB8:1:5::2/128 [0/0]
     via FastEthernet0/1, receive
OI  2001:DB8:2:1::/120 [110/6]
     via FE80::6EDD:30FF:FEB6:6030, FastEthernet0/1
C   2001:DB8:2:2::/120 [0/0]
     via FastEthernet0/16, directly connected
L   2001:DB8:2:2::1/128 [0/0]
     via FastEthernet0/16, receive
L   FF00::/8 [0/0]
     via Null0, receive
S3(config)#
```

```
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is not set

      192.168.1.0/24 is variably subnetted, 5 subnets, 2 masks
O IA     192.168.1.0/30
           [110/2] via 192.168.1.5, 00:10:46, GigabitEthernet0/0/1
C        192.168.1.4/30 is directly connected, GigabitEthernet0/0/1
L        192.168.1.6/32 is directly connected, GigabitEthernet0/0/1
O IA     192.168.1.8/30
           [110/3] via 192.168.1.5, 00:10:46, GigabitEthernet0/0/1
O IA     192.168.1.16/30
           [110/4] via 192.168.1.5, 00:10:46, GigabitEthernet0/0/1
O IA  192.168.3.0/24 [110/5] via 192.168.1.5, 00:10:46, GigabitEthernet0/0/1
R3#
```

R4:

```
version 15.5
service timestamps debug datetime msec
service timestamps log datetime msec
no platform punt-keepalive disable-kernel-core
hostname R4
boot-start-marker
boot-end-marker
vrf definition Mgmt-intf
address-family ipv4
exit-address-family
address-family ipv6
exit-address-family
no aaa new-model
ipv6 unicast-routing
subscriber templating
vtp domain cisco
vtp mode transparent
multilink bundle-name authenticated
license udi pid ISR4321/K9 sn FDO21491LXV
license accept end user agreement
license boot level securityk9
spanning-tree extend system-id
redundancy
mode none
```

```
vlan internal allocation policy ascending
vlan 2
name v2
vlan 3
name v3
vlan 4
name v4
vlan 10,20
interface GigabitEthernet0/0/0
ip address 192.168.1.14 255.255.255.252
negotiation auto
ipv6 address 2001:DB8:1:4::2/126
ipv6 enable
ipv6 ospf 10 area 2
interface GigabitEthernet0/0/1
ip address 192.168.2.1 255.255.255.0
negotiation auto
ipv6 address 2001:DB8:2:1::1/120
ipv6 enable
ipv6 ospf 10 area 2
interface Serial0/1/0
interface Serial0/1/1
interface GigabitEthernet0
vrf forwarding Mgmt-intf
no ip address
shutdown
```

```
negotiation auto
interface Vlan1
no ip address
shutdown
router ospf 10
network 192.168.1.12 0.0.0.3 area 2
network 192.168.2.0 0.0.0.255 area 2
ip forward-protocol nd
no ip http server
no ip http secure-server
ip tftp source-interface GigabitEthernet0
ipv6 router ospf 10
control-plane
line con 0
stopbits 1
line aux 0
stopbits 1
line vty 0 4
login
```

end

```
R4(config)#do show ipv6 route
IPv6 Routing Table - default - 10 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE - Destination
       NDr - Redirect, O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1
       OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       a - Application
OI  2001:DB8:1:1::/126 [110/3]
     via FE80::B6A8:B9FF:FE01:AE50, GigabitEthernet0/0/0
OI  2001:DB8:1:2::/126 [110/4]
     via FE80::B6A8:B9FF:FE01:AE50, GigabitEthernet0/0/0
O   2001:DB8:1:3::/126 [110/2]
     via FE80::B6A8:B9FF:FE01:AE50, GigabitEthernet0/0/0
C   2001:DB8:1:4::/126 [0/0]
     via GigabitEthernet0/0/0, directly connected
L   2001:DB8:1:4::2/128 [0/0]
     via GigabitEthernet0/0/0, receive
OI  2001:DB8:1:5::/126 [110/5]
     via FE80::B6A8:B9FF:FE01:AE50, GigabitEthernet0/0/0
C   2001:DB8:2:1::/120 [0/0]
     via GigabitEthernet0/0/1, directly connected
L   2001:DB8:2:1::1/128 [0/0]
     via GigabitEthernet0/0/1, receive
OI  2001:DB8:2:2::/120 [110/6]
     via FE80::B6A8:B9FF:FE01:AE50, GigabitEthernet0/0/0
L   FF00::/8 [0/0]
     via Null0, receive
R4(config)#
```

```
Gateway of last resort is not set

      192.168.1.0/24 is variably subnetted, 6 subnets, 2 masks
O IA     192.168.1.0/30
           [110/3] via 192.168.1.13, 00:01:46, GigabitEthernet0/0/0
O        192.168.1.4/30
           [110/2] via 192.168.1.13, 00:01:46, GigabitEthernet0/0/0
O IA     192.168.1.8/30
           [110/4] via 192.168.1.13, 00:01:46, GigabitEthernet0/0/0
C        192.168.1.12/30 is directly connected, GigabitEthernet0/0/0
L        192.168.1.14/32 is directly connected, GigabitEthernet0/0/0
O IA     192.168.1.16/30
           [110/5] via 192.168.1.13, 00:01:46, GigabitEthernet0/0/0
      192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.2.0/24 is directly connected, GigabitEthernet0/0/1
L        192.168.2.1/32 is directly connected, GigabitEthernet0/0/1
O IA  192.168.3.0/24 [110/6] via 192.168.1.13, 00:01:46, GigabitEthernet0/0/0
R4#
```

R5:

version 15.5

service timestamps debug datetime msec

service timestamps log datetime msec

no platform punt-keepalive disable-kernel-core

hostname R5

boot-start-marker

```
boot-end-marker
vrf definition Mgmt-intf
address-family ipv4
exit-address-family
address-family ipv6
exit-address-family
no aaa new-model
ipv6 unicast-routing
subscriber templating
vtp domain cisco
vtp mode transparent
multilink bundle-name authenticated
license udi pid ISR4321/K9 sn FDO21400XZX
spanning-tree extend system-id
redundancy
mode none
vlan internal allocation policy ascending
interface GigabitEthernet0/0/0
ip address 192.168.1.18 255.255.255.252
negotiation auto
ipv6 address 2001:DB8:1:5::1/126
ipv6 enable
ipv6 ospf 10 area 3
interface GigabitEthernet0/0/1
ip address 192.168.1.10 255.255.255.252
negotiation auto
```

```
ipv6 address 2001:DB8:1:2::2/126
ipv6 enable
ipv6 ospf 10 area 3
interface Serial0/1/0
no ip address
shutdown
interface Serial0/1/1
no ip address
shutdown
interface GigabitEthernet0
vrf forwarding Mgmt-intf
no ip address
shutdown
negotiation auto
interface Vlan1
no ip address
shutdown
router ospf 10
network 192.168.1.8 0.0.0.3 area 3
network 192.168.1.16 0.0.0.3 area 3
ip forward-protocol nd
no ip http server
no ip http secure-server
ip tftp source-interface GigabitEthernet0
ipv6 router ospf 10
control-plane
```

line con 0

stopbits 1

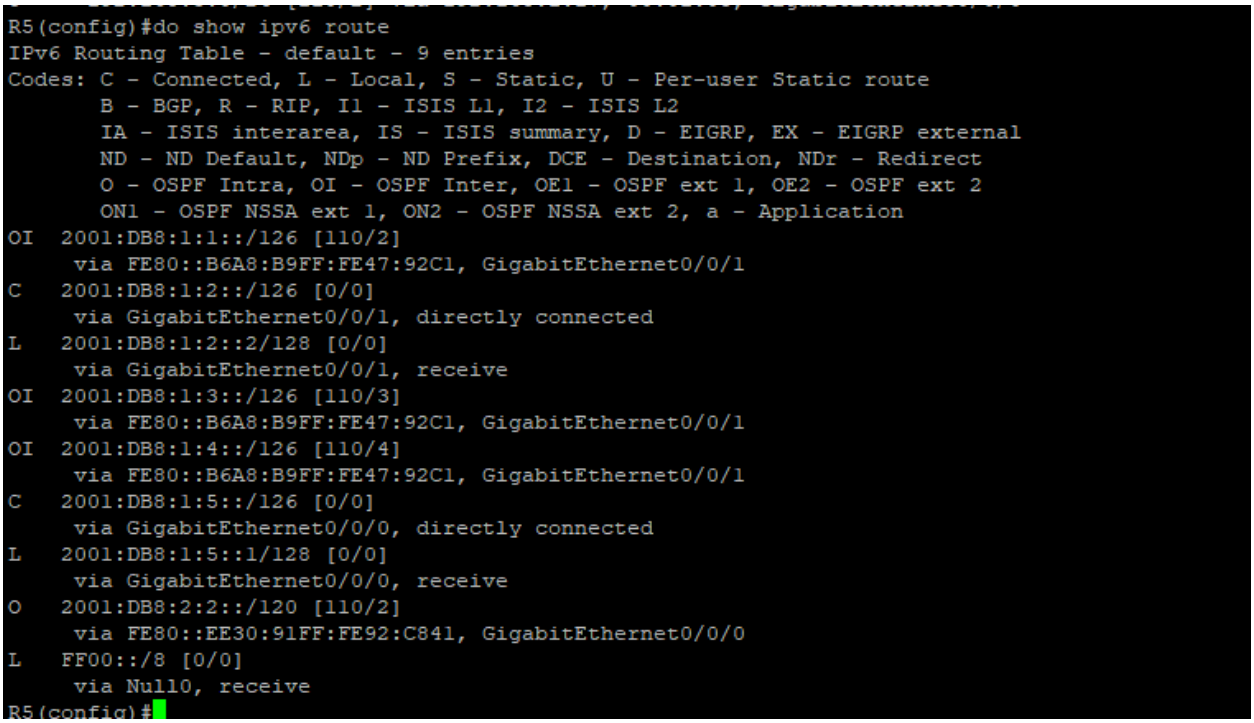
line aux 0

stopbits 1

line vty 0 4

login

end



```
R5(config)#do show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is not set

      192.168.1.0/24 is variably subnetted, 7 subnets, 2 masks
O IA     192.168.1.0/30
           [110/2] via 192.168.1.9, 00:56:41, GigabitEthernet0/0/1
O IA     192.168.1.4/30
           [110/3] via 192.168.1.9, 00:55:54, GigabitEthernet0/0/1
C        192.168.1.8/30 is directly connected, GigabitEthernet0/0/1
L        192.168.1.10/32 is directly connected, GigabitEthernet0/0/1
O IA     192.168.1.12/30
           [110/4] via 192.168.1.9, 00:39:59, GigabitEthernet0/0/1
C        192.168.1.16/30 is directly connected, GigabitEthernet0/0/0
L        192.168.1.18/32 is directly connected, GigabitEthernet0/0/0
O IA  192.168.2.0/24 [110/5] via 192.168.1.9, 00:07:01, GigabitEthernet0/0/1
O     192.168.3.0/24 [110/2] via 192.168.1.17, 00:01:05, GigabitEthernet0/0/0
R5(config)#
```

S3:

version 12.2

no service pad

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

hostname S3

boot-start-marker

boot-end-marker

no aaa new-model

system mtu routing 1500

authentication mac-move permit

ip subnet-zero

ip routing

ipv6 unicast-routing

spanning-tree mode pvst

spanning-tree etherchannel guard misconfig

spanning-tree extend system-id

vlan internal allocation policy ascending

interface FastEthernet0/1

no switchport

ip address 192.168.1.17 255.255.255.252

ipv6 address 2001:DB8:1:5::2/126

ipv6 enable

ipv6 ospf 10 area 3

interface FastEthernet0/2

interface FastEthernet0/3

interface FastEthernet0/4

interface FastEthernet0/5

interface FastEthernet0/6

interface FastEthernet0/7

interface FastEthernet0/8

interface FastEthernet0/9

interface FastEthernet0/10

interface FastEthernet0/11

interface FastEthernet0/12

interface FastEthernet0/13

interface FastEthernet0/14

interface FastEthernet0/15

interface FastEthernet0/16

no switchport

ip address 192.168.3.1 255.255.255.0

ipv6 address 2001:DB8:2:2::1/120

ipv6 enable

ipv6 ospf 10 area 3

interface FastEthernet0/17

interface FastEthernet0/18

interface FastEthernet0/19

interface FastEthernet0/20

interface FastEthernet0/21

interface FastEthernet0/22

interface FastEthernet0/23

interface FastEthernet0/24

interface FastEthernet0/25

interface FastEthernet0/26

interface FastEthernet0/27

interface FastEthernet0/28

interface FastEthernet0/29

interface FastEthernet0/30

interface FastEthernet0/31

interface FastEthernet0/32

interface FastEthernet0/33

interface FastEthernet0/34

interface FastEthernet0/35

interface FastEthernet0/36

interface FastEthernet0/37

interface FastEthernet0/38

interface FastEthernet0/39

interface FastEthernet0/40

interface FastEthernet0/41

interface FastEthernet0/42

interface FastEthernet0/43

interface FastEthernet0/44

interface FastEthernet0/45

interface FastEthernet0/46

interface FastEthernet0/47

interface FastEthernet0/48

interface GigabitEthernet0/1

interface GigabitEthernet0/2

interface GigabitEthernet0/3

interface GigabitEthernet0/4

interface Vlan1

no ip address

shutdown

router ospf 10

log-adjacency-changes

network 192.168.1.16 0.0.0.3 area 3

network 192.168.3.0 0.0.0.255 area 3

ip classless

ip http server

ip http secure-server

ip sla enable reaction-alerts

ipv6 router ospf 10

log-adjacency-changes

line con 0

line vty 5 15

end

```
S3(config)#do  show ipv6 route
IPv6 Routing Table - Default - 10 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, D - EIGRP, EX - EIGRP external
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
OI  2001:DB8:1:1::/126 [110/3]
     via FE80::6EDD:30FF:FEB6:6030, FastEthernet0/1
O   2001:DB8:1:2::/126 [110/2]
     via FE80::6EDD:30FF:FEB6:6030, FastEthernet0/1
OI  2001:DB8:1:3::/126 [110/4]
     via FE80::6EDD:30FF:FEB6:6030, FastEthernet0/1
OI  2001:DB8:1:4::/126 [110/5]
     via FE80::6EDD:30FF:FEB6:6030, FastEthernet0/1
C   2001:DB8:1:5::/126 [0/0]
     via FastEthernet0/1, directly connected
L   2001:DB8:1:5::2/128 [0/0]
     via FastEthernet0/1, receive
OI  2001:DB8:2:1::/120 [110/6]
     via FE80::6EDD:30FF:FEB6:6030, FastEthernet0/1
C   2001:DB8:2:2::/120 [0/0]
     via FastEthernet0/16, directly connected
L   2001:DB8:2:2::1/128 [0/0]
     via FastEthernet0/16, receive
L   FF00::/8 [0/0]
     via Null0, receive
S3(config)#
```

```
     192.168.1.0/30 is subnetted, 5 subnets
O       192.168.1.8 [110/2] via 192.168.1.18, 00:00:08, FastEthernet0/1
O IA    192.168.1.12 [110/5] via 192.168.1.18, 00:00:08, FastEthernet0/1
O IA    192.168.1.0 [110/3] via 192.168.1.18, 00:00:08, FastEthernet0/1
O IA    192.168.1.4 [110/4] via 192.168.1.18, 00:00:08, FastEthernet0/1
C       192.168.1.16 is directly connected, FastEthernet0/1
O IA 192.168.2.0/24 [110/6] via 192.168.1.18, 00:00:08, FastEthernet0/1
C    192.168.3.0/24 is directly connected, FastEthernet0/16
S3(config)#
```

Problems: In this lab, we faced about one problem, which is we don't quite understand how much router we need to use, we quickly fix that by asking other classmate for the requirements of the lab, so we need to restart the lab for fulfill the requirement of the lab. Sometimes we misconfigured some network statement for the OSPF, so the OSPF is not working at that subnet, which make us cannot reach the end device, but we quickly fix that by checking running configure, check the ip route and find out we entered the wrong network ip, so the OSPF is not working for that subnet, we fixed that problem by entering the right network ip and correct wildcard mask, after that, the end device can reach another end device.

Conclusion: In this lab, we practice how to set up Mult area OSPF, it helped us remember how to do some basic configure on a Cisco router and a multilayer switch, we learned more about how to set up OSPF for ipv6 and how to configure a multilayer switch. Overall, this lab helped us to remember how to do some basic configure on Cisco devices, and improved our problem-solving technique, which can prepare us for future job situation when we need to set up OSPF network and when we facing some problem when we setting up a network.

Exterior Border Gateway Protocol

By Alvin Chow

Purpose: In this lab, we learned to configure EBGP to connect 3 different company that using different routing protocol, included EIGRP, OSPF and RIP. This lab help us understand how the current internet work by ISP connect to other ISP and how to set up other type of routing protocol.

Background Information:

eBGP (External Border Gateway Protocol) is a way for different networks on the Internet to share routing information, which can help every request to get to their destination. It helps routers find the best paths for sending data between all networks. eBGP works at the edge of a network, connecting it to others border router that have different routing protocol. It uses TCP to ensure reliable communication. Key features include tracking the path data takes to avoid loops and using different attributes to decide which route is best.

RIP (Routing Information Protocol) is a simple routing protocol used in small to medium-sized networks to manage routes. It helps routers share information about the best paths for data transmission, using hop count as its metric with a maximum limit of 15 hops. Routers send updates about their routing tables every 30 seconds to keep information current. There are two main versions: RIP version 1 (RIPv1), which doesn't support subnetting, and RIP version 2 (RIPv2), which includes features like route tagging and multicast updates. While easy to configure, RIP can be slow to respond to changes and may not be efficient for larger networks compared to more advanced protocols like OSPF or BGP.

Open shortest path first (OSPF) is a routing protocol for internet, it uses link state routing algorithm, and it is an interior gateway protocol. It functions y determine the shortest path to the destination and it calculated based on bandwidth, delay and cost.

EIGRP (Enhanced Interior Gateway Routing Protocol) is a routing protocol used in networks to help routers share information about the best paths for sending data. It combines features of two types of protocols for faster updates and better scalability. EIGRP uses a calculation that considers bandwidth, delay, load to find the best route. Routers send hello packets to discover nearby routers and keep their information up to date. It adapts quickly to changes in the network, which helps reduce downtime when connections go up or down. EIGRP also supports Variable Length Subnet Masking, it allowing for better use of IP addresses. Additionally, it can work with different types of network protocols, making it a good choice for large and complex networks.

Lab Summary: First, me and my partner designed to use 192.168.1.0/24 to be the connection ip between router, then we decided to use /30 for point-to-point connection between router. For ipv6 we decided to use. For ipv6, we decided to use 2001:db8:1 to be

our management device ip, then we used 2001:db8:2 and 2001:db8:3 to be our host subnet ipv6 address. We decided to use 3 routing protocol for each company and use EBGP to share all the routing information between company. We use OSPF, EIGRP and RIP for the internal routing process.

For the EBGP, we chose AS 1 to be the AS for the company that using EIGRP, then we chose AS 2 to be the AS for company that using RIP, for company that using OSPF, we assign AS 3 to that company. For the border router at company A, we redistribute EIGRP route into BGP, which can share the route of company A to other company. For the border router at company B, we redistribute rip route into BGP, which can let company A and C know the route inside company B. For company C, we distribute OSPF route into BGP. After company A border router learn the BGP route for all network, we distribute BGP route into EIGRP route, which can make internal device of company A know all the route to every network. For company B, we redistribute the BGP route that learn from company A and B into RIP route, which can make all router within Company B know the route to every network. For company C, we redistribute the route that we learn from company B into OSPF, which can make all router of Company C know all the route to other company.

Lab command:

Ip address : ip address and subnet mask, this help us set a static ip for that interface.

Ipv6 unicast routing, it let router can do ipv6 routing.

Ipv6 eigrp/ospf process-number, this command let us to put routing protocol to the interface that we want.

Ipv6 rip enable, this command enable rip to that internet for ipv6

Router eigrp/bgp/ospf process number/AS number, this command can let us configure routing protocol.

Router Rip, this command let us configure RIP for that router

Neighbor ip address/ipv6 address remotes-as As number, this command can let us set up the neighbor ip for BGP, it can help neighbor establish the connection for exchange route.

Neighbor ip/ipv6 address next-hop-self, this command set the BGP route next hop to be that routing, which can help other device know how to reach that subnet.

Network network ip wildcard mask, this command let us configure the interface that we want to put in routing protocol.

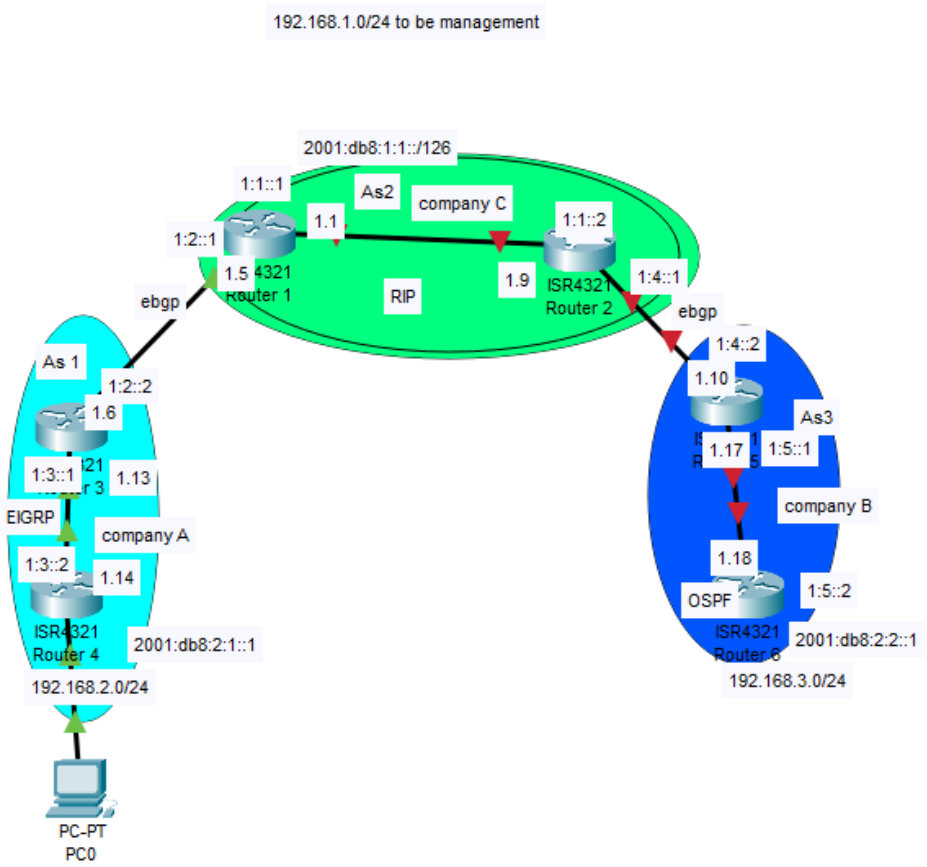
Redistribute connected, this command let us to Redistribute the connected route into BGP

Redistribute ospf/bgp/eigrp process number/ AS-number metric, it can redistribute BGP route into internal routing protocol or redistribute internal route to BGP to let other router learn the learn

Redistribute rip metric number, it can redistribute rip route

no bgp default ipv4-unicast, it let us can configure ipv4 and ipv6 for BGP

Lab Topology:



Configurations:

R1 configure:
version 15.5
service timestamps debug datetime msec
service timestamps log datetime msec
no platform punt-keepalive disable-kernel-core
hostname R
boot-start-marker
boot-end-marker
vrf definition Mgmt-intf
address-family ipv4
exit-address-family

address-family ipv6
exit-address-family
no aaa new-model
ipv6 unicast-routing
subscriber templating
vtp domain cisco
vtp mode transparent
multilink bundle-name authenticated
license udi pid ISR4321/K9 sn FDO214421BY
spanning-tree extend system-id
Redundancy
mode none
vlan internal allocation policy ascending
interface GigabitEthernet0/0/0
ip address 192.168.1.5 255.255.255.252
negotiation auto
ipv6 address 2001:DB8:1:2::1/126
ipv6 enable
ipv6 rip 1 enable
interface GigabitEthernet0/0/1
ip address 192.168.1.1 255.255.255.252
negotiation auto
ipv6 address 2001:DB8:1:1::1/126
ipv6 enable
ipv6 rip 1 enable
interface Serial0/1/0
no ip address
shutdown
interface Serial0/1/1
no ip address
shutdown
interface GigabitEthernet0/2/0
no ip address
shutdown
negotiation auto
interface GigabitEthernet0/2/1
no ip address
shutdown
negotiation auto
interface GigabitEthernet0
vrf forwarding Mgmt-intf
no ip address
shutdown
negotiation auto
interface Vlan1
no ip address
shutdown
router rip

```
redistribute connected
redistribute bgp 2 metric 10
network 192.168.1.0
neighbor 192.168.1.2
router bgp 2
bgp log-neighbor-changes
no bgp default ipv4-unicast
neighbor 2001:DB8:1:2::2 remote-as 1
neighbor 192.168.1.6 remote-as 1
address-family ipv4
network 192.168.1.4 mask 255.255.255.252
redistribute connected
redistribute rip
neighbor 192.168.1.6 activate
exit-address-family
address-family ipv6
redistribute connected
redistribute rip 1
neighbor 2001:DB8:1:2::2 activate
neighbor 2001:DB8:1:2::2 next-hop-self
exit-address-family
ip forward-protocol nd
no ip http server
no ip http secure-server
ip tftp source-interface GigabitEthernet0
ipv6 router rip 1
redistribute connected
redistribute bgp 2 metric 10
control-plane
line con 0
stopbits 1
line aux 0
stopbits 1
line vty 0 4
login
```

end

```
      192.168.1.0/24 is variably subnetted, 7 subnets, 2 masks
C        192.168.1.0/30 is directly connected, GigabitEthernet0/0/1
L        192.168.1.1/32 is directly connected, GigabitEthernet0/0/1
C        192.168.1.4/30 is directly connected, GigabitEthernet0/0/0
L        192.168.1.5/32 is directly connected, GigabitEthernet0/0/0
R        192.168.1.8/30
           [120/1] via 192.168.1.2, 00:00:04, GigabitEthernet0/0/1
B        192.168.1.12/30 [20/0] via 192.168.1.6, 00:11:13
R        192.168.1.16/30
           [120/10] via 192.168.1.2, 00:00:04, GigabitEthernet0/0/1
B     192.168.2.0/24 [20/3072] via 192.168.1.6, 00:10:43
R     192.168.3.0/24 [120/10] via 192.168.1.2, 00:00:04, GigabitEthernet0/
R1(config)#
```

```
IPv6 Routing Table - default - 11 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, I1 - ISIS L1, I2 - ISIS L2
       IA - ISIS interarea, IS - ISIS summary, D - EIGRP, EX - EIGRP external
       ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2, a - Application
R   200:DB8:1:4::/126 [120/11]
     via FE80::B6A8:B9FF:FE47:92C1, GigabitEthernet0/0/1
C   2001:DB8:1:1::/126 [0/0]
     via GigabitEthernet0/0/1, directly connected
L   2001:DB8:1:1::1/128 [0/0]
     via GigabitEthernet0/0/1, receive
C   2001:DB8:1:2::/126 [0/0]
     via GigabitEthernet0/0/0, directly connected
L   2001:DB8:1:2::1/128 [0/0]
     via GigabitEthernet0/0/0, receive
B   2001:DB8:1:3::/126 [20/0]
     via FE80::B6A8:B9FF:FE01:AE50, GigabitEthernet0/0/0
R   2001:DB8:1:4::/126 [120/2]
     via FE80::B6A8:B9FF:FE47:92C1, GigabitEthernet0/0/1
R   2001:DB8:1:5::/126 [120/11]
     via FE80::B6A8:B9FF:FE47:92C1, GigabitEthernet0/0/1
B   2001:DB8:2:1::/120 [20/3072]
     via FE80::B6A8:B9FF:FE01:AE50, GigabitEthernet0/0/0
R   2001:DB8:2:2::/120 [120/11]
     via FE80::B6A8:B9FF:FE47:92C1, GigabitEthernet0/0/1
L   FF00::/8 [0/0]
     via Null0, receive
R1(config)#
```

R2 configure:

version 15.5
service timestamps debug datetime msec
service timestamps log datetime msec
no platform punt-keepalive disable-kernel-core
hostname R2
boot-start-marker

```
boot-end-marker
vrf definition Mgmt-intf
address-family ipv4
exit-address-family
address-family ipv6
exit-address-family
no aaa new-model
ipv6 unicast-routing
subscriber templating
multilink bundle-name authenticated
license udi pid ISR4321/K9 sn FDO214420QQ
license accept end user agreement
license boot level securityk9
spanning-tree extend system-id
redundancy
mode none
vlan internal allocation policy ascending
interface GigabitEthernet0/0/0
ip address 192.168.1.9 255.255.255.252
negotiation auto
ipv6 address 2001:DB8:1:4::1/126
ipv6 rip process1 enable
interface GigabitEthernet0/0/1
ip address 192.168.1.2 255.255.255.252
negotiation auto
ipv6 address 2001:DB8:1:1::2/126
ipv6 rip process1 enable
interface Serial0/1/0
no ip address
shutdown
interface Serial0/1/1
no ip address
shutdown
interface GigabitEthernet0
vrf forwarding Mgmt-intf
no ip address
shutdown
negotiation auto
interface Vlan1
no ip address
shutdown
router rip
redistribute bgp 2 metric 10
network 192.168.1.0
neighbor 192.168.1.1
router bgp 2
bgp log-neighbor-changes
no bgp default ipv4-unicast
```

```
neighbor 2001:DB8:1:4::2 remote-as 3
neighbor 192.168.1.10 remote-as 3
address-family ipv4
redistribute rip
neighbor 192.168.1.10 activate
neighbor 192.168.1.10 next-hop-self
exit-address-family
address-family ipv6
redistribute connected
redistribute rip process1
neighbor 2001:DB8:1:4::2 activate
neighbor 2001:DB8:1:4::2 next-hop-self
exit-address-family
ip forward-protocol nd
no ip http server
no ip http secure-server
ip tftp source-interface GigabitEthernet0
ipv6 router rip process1
redistribute connected
redistribute bgp 2 metric 10
control-plane
line con 0
stopbits 1
line aux 0
stopbits 1
line vty 0 4
login
```

end

R3 configure:

```
Gateway of last resort is not set

      192.168.1.0/24 is variably subnetted, 7 subnets, 2 masks
C        192.168.1.0/30 is directly connected, GigabitEthernet0/0/1
L        192.168.1.2/32 is directly connected, GigabitEthernet0/0/1
R        192.168.1.4/30
           [120/1] via 192.168.1.1, 00:00:07, GigabitEthernet0/0/1
C        192.168.1.8/30 is directly connected, GigabitEthernet0/0/0
L        192.168.1.9/32 is directly connected, GigabitEthernet0/0/0
R        192.168.1.12/30
           [120/10] via 192.168.1.1, 00:00:07, GigabitEthernet0/0/1
B        192.168.1.16/30 [20/0] via 192.168.1.10, 00:08:11
R     192.168.2.0/24 [120/10] via 192.168.1.1, 00:00:07, GigabitEthernet0/0/1
B     192.168.3.0/24 [20/2] via 192.168.1.10, 00:07:21
R2(config)#
```

```
IPv6 Routing Table - default - 11 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE - Destination
       NDr - Redirect, O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1
       OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       a - Application
B   200:DB8:1:4::/126 [20/0]
     via FE80::6EDD:30FF:FEB6:6030, GigabitEthernet0/0/0
C   2001:DB8:1:1::/126 [0/0]
     via GigabitEthernet0/0/1, directly connected
L   2001:DB8:1:1::2/128 [0/0]
     via GigabitEthernet0/0/1, receive
R   2001:DB8:1:2::/126 [120/2]
     via FE80::B6A8:B9FF:FE01:B511, GigabitEthernet0/0/1
R   2001:DB8:1:3::/126 [120/11]
     via FE80::B6A8:B9FF:FE01:B511, GigabitEthernet0/0/1
C   2001:DB8:1:4::/126 [0/0]
     via GigabitEthernet0/0/0, directly connected
L   2001:DB8:1:4::1/128 [0/0]
     via GigabitEthernet0/0/0, receive
B   2001:DB8:1:5::/126 [20/0]
     via FE80::6EDD:30FF:FEB6:6030, GigabitEthernet0/0/0
R   2001:DB8:2:1::/120 [120/11]
     via FE80::B6A8:B9FF:FE01:B511, GigabitEthernet0/0/1
B   2001:DB8:2:2::/120 [20/2]
     via FE80::6EDD:30FF:FEB6:6030, GigabitEthernet0/0/0
L   FF00::/8 [0/0]
     via Null0, receive
R2(config)#
```

version 15.5
service timestamps debug datetime msec
service timestamps log datetime msec
no platform punt-keepalive disable-kernel-core
hostname R3
boot-start-marker
boot-end-marker
vrf definition Mgmt-intf

```
address-family ipv4
exit-address-family
address-family ipv6
exit-address-family
no logging console
no aaa new-model
ipv6 unicast-routing
subscriber templating
vtp domain cisco
vtp mode transparent
multilink bundle-name authenticated
license udi pid ISR4321/K9 sn FDO214420HY
license boot level securityk9
spanning-tree extend system-id
redundancy
 mode none
vlan internal allocation policy ascending
vlan 10,20
interface GigabitEthernet0/0/0
ip address 192.168.1.6 255.255.255.252
negotiation auto
ipv6 address 2001:DB8:1:2::2/126
ipv6 enable
ipv6 eigrp 1
interface GigabitEthernet0/0/1
ip address 192.168.1.13 255.255.255.252
negotiation auto
ipv6 address 2001:DB8:1:3::1/126
ipv6 enable
ipv6 eigrp 1
interface Serial0/1/0
no ip address
interface Serial0/1/1
no ip address
interface GigabitEthernet0
vrf forwarding Mgmt-intf
no ip address
negotiation auto
interface Vlan1
no ip address
router eigrp 1
network 192.168.1.4 0.0.0.3
network 192.168.1.12 0.0.0.3
redistribute bgp 1 metric 100000 10 255 1 1500
redistribute connected
router bgp 1
bgp log-neighbor-changes
no bgp default ipv4-unicast
```

```
neighbor 2001:DB8:1:2::1 remote-as 2
neighbor 192.168.1.5 remote-as 2
address-family ipv4
redistribute connected
redistribute eigrp 1
neighbor 192.168.1.5 activate
neighbor 192.168.1.5 next-hop-self
exit-address-family
address-family ipv6
redistribute connected
redistribute eigrp 1
neighbor 2001:DB8:1:2::1 activate
neighbor 2001:DB8:1:2::1 next-hop-self
exit-address-family
ip forward-protocol nd
no ip http server
no ip http secure-server
ip tftp source-interface GigabitEthernet0
ipv6 router eigrp 1
redistribute bgp 1 metric 10000 10 255 1 1500
redistribute connected
control-plane
line con 0
stopbits 1
line aux 0
stopbits 1
line vty 0 4
login
end
```

```
Gateway of last resort is not set

      192.168.1.0/24 is variably subnetted, 7 subnets, 2 masks
B        192.168.1.0/30 [20/0] via 192.168.1.5, 00:08:41
C        192.168.1.4/30 is directly connected, GigabitEthernet0/0/0
L        192.168.1.6/32 is directly connected, GigabitEthernet0/0/0
B        192.168.1.8/30 [20/1] via 192.168.1.5, 00:08:10
C        192.168.1.12/30 is directly connected, GigabitEthernet0/0/1
L        192.168.1.13/32 is directly connected, GigabitEthernet0/0/1
B        192.168.1.16/30 [20/10] via 192.168.1.5, 00:05:34
D     192.168.2.0/24
           [90/3072] via 192.168.1.14, 00:07:05, GigabitEthernet0/0/1
B     192.168.3.0/24 [20/10] via 192.168.1.5, 00:04:44
R3(config)#
```

```
IPv6 Routing Table - default - 11 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE - Destination
       NDr - Redirect, O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1
       OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       a - Application
B   200:DB8:1:4::/126 [20/11]
     via FE80::B6A8:B9FF:FE01:B510, GigabitEthernet0/0/0
B   2001:DB8:1:1::/126 [20/0]
     via FE80::B6A8:B9FF:FE01:B510, GigabitEthernet0/0/0
C   2001:DB8:1:2::/126 [0/0]
     via GigabitEthernet0/0/0, directly connected
L   2001:DB8:1:2::2/128 [0/0]
     via GigabitEthernet0/0/0, receive
C   2001:DB8:1:3::/126 [0/0]
     via GigabitEthernet0/0/1, directly connected
L   2001:DB8:1:3::1/128 [0/0]
     via GigabitEthernet0/0/1, receive
B   2001:DB8:1:4::/126 [20/2]
     via FE80::B6A8:B9FF:FE01:B510, GigabitEthernet0/0/0
B   2001:DB8:1:5::/126 [20/11]
     via FE80::B6A8:B9FF:FE01:B510, GigabitEthernet0/0/0
D   2001:DB8:2:1::/120 [90/3072]
     via FE80::521C:B0FF:FE2D:7101, GigabitEthernet0/0/1
B   2001:DB8:2:2::/120 [20/11]
     via FE80::B6A8:B9FF:FE01:B510, GigabitEthernet0/0/0
L   FF00::/8 [0/0]
     via Null0, receive
R3(config)#
```

R4 Configure:

version 15.5
service timestamps debug datetime msec
service timestamps log datetime msec
no platform punt-keepalive disable-kernel-core
hostname R4
boot-start-marker
boot-end-marker
vrf definition Mgmt-intf
address-family ipv4
exit-address-family
address-family ipv6

```
exit-address-family
no aaa new-model
ipv6 unicast-routing
subscriber templating
vtp domain cisco
vtp mode transparent
multilink bundle-name authenticated
license udi pid ISR4321/K9 sn FDO21491LXV
license accept end user agreement
license boot level securityk9
spanning-tree extend system-id
redundancy
mode none
vlan internal allocation policy ascending
vlan 2
name v2
vlan 3
name v3
vlan 4
name v4
vlan 10,20
interface GigabitEthernet0/0/0
ip address 192.168.2.1 255.255.255.0
negotiation auto
ipv6 address 2001:DB8:2:1::1/120
ipv6 enable
ipv6 eigrp 1
interface GigabitEthernet0/0/1
ip address 192.168.1.14 255.255.255.252
negotiation auto
ipv6 address 2001:DB8:1:3::2/126
ipv6 enable
ipv6 eigrp 1
interface Serial0/1/0
no ip address
shutdown
interface Serial0/1/1
no ip address
shutdown
interface GigabitEthernet0
vrf forwarding Mgmt-intf
no ip address
shutdown
negotiation auto
interface Vlan1
no ip address
shutdown
router eigrp 1
```

```
network 192.168.1.12 0.0.0.3
network 192.168.2.0
ip forward-protocol nd
no ip http server
no ip http secure-server
ip tftp source-interface GigabitEthernet0
ipv6 router eigrp 1
control-plane
line con 0
stopbits 1
line aux 0
stopbits 1
line vty 0 4
login
```

end

```
R4(config)#do show ipv6 route
IPv6 Routing Table - default - 11 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE - Destination
       NDr - Redirect, O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1
       OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       a - Application
EX  200:DB8:1:4::/126 [170/258816]
     via FE80::B6A8:B9FF:FE01:AE51, GigabitEthernet0/0/1
EX  2001:DB8:1:1::/126 [170/258816]
     via FE80::B6A8:B9FF:FE01:AE51, GigabitEthernet0/0/1
D   2001:DB8:1:2::/126 [90/3072]
     via FE80::B6A8:B9FF:FE01:AE51, GigabitEthernet0/0/1
C   2001:DB8:1:3::/126 [0/0]
     via GigabitEthernet0/0/1, directly connected
L   2001:DB8:1:3::2/128 [0/0]
     via GigabitEthernet0/0/1, receive
EX  2001:DB8:1:4::/126 [170/258816]
     via FE80::B6A8:B9FF:FE01:AE51, GigabitEthernet0/0/1
EX  2001:DB8:1:5::/126 [170/258816]
     via FE80::B6A8:B9FF:FE01:AE51, GigabitEthernet0/0/1
C   2001:DB8:2:1::/120 [0/0]
     via GigabitEthernet0/0/0, directly connected
L   2001:DB8:2:1::1/128 [0/0]
     via GigabitEthernet0/0/0, receive
EX  2001:DB8:2:2::/120 [170/258816]
     via FE80::B6A8:B9FF:FE01:AE51, GigabitEthernet0/0/1
L   FF00::/8 [0/0]
     via Null0, receive
R4(config)#
```

```
Gateway of last resort is not set

      192.168.1.0/24 is variably subnetted, 6 subnets, 2 masks
D EX     192.168.1.0/30
           [170/28416] via 192.168.1.13, 00:05:39, GigabitEthernet0/0/1
D        192.168.1.4/30
           [90/3072] via 192.168.1.13, 00:05:39, GigabitEthernet0/0/1
D EX     192.168.1.8/30
           [170/28416] via 192.168.1.13, 00:05:39, GigabitEthernet0/0/1
C        192.168.1.12/30 is directly connected, GigabitEthernet0/0/1
L        192.168.1.14/32 is directly connected, GigabitEthernet0/0/1
D EX     192.168.1.16/30
           [170/28416] via 192.168.1.13, 00:04:03, GigabitEthernet0/0/1
      192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.2.0/24 is directly connected, GigabitEthernet0/0/0
L        192.168.2.1/32 is directly connected, GigabitEthernet0/0/0
D EX  192.168.3.0/24
           [170/28416] via 192.168.1.13, 00:03:13, GigabitEthernet0/0/1
R4(config)#
```

R5 Config:

version 15.5
service timestamps debug datetime msec
service timestamps log datetime msec
no platform punt-keepalive disable-kernel-core
hostname R5

```
boot-start-marker
boot-end-marker
vrf definition Mgmt-intf
address-family ipv4
exit-address-family
address-family ipv6
exit-address-family
no aaa new-model
ipv6 unicast-routing
subscriber templating
vtp domain cisco
vtp mode transparent
multilink bundle-name authenticated
license udi pid ISR4321/K9 sn FDO21400XZX
spanning-tree extend system-id
redundancy
mode none
vlan internal allocation policy ascending
interface GigabitEthernet0/0/0
ip address 192.168.1.10 255.255.255.252
negotiation auto
ipv6 address 200:DB8:1:4::2/126
ipv6 address 2001:DB8:1:4::2/126
ipv6 ospf 1 area 1
interface GigabitEthernet0/0/1
ip address 192.168.1.17 255.255.255.252
negotiation auto
ipv6 address 2001:DB8:1:5::1/126
ipv6 ospf 1 area 1
interface Serial0/1/0
no ip address
shutdown
interface Serial0/1/1
no ip address
shutdown
interface GigabitEthernet0
vrf forwarding Mgmt-intf
no ip address
shutdown
negotiation auto
interface Vlan1
no ip address
shutdown
router ospf 1
```

```
redistribute bgp 3 subnets
network 192.168.1.8 0.0.0.3 area 1
network 192.168.1.16 0.0.0.3 area 1
router bgp 3
bgp log-neighbor-changes
no bgp default ipv4-unicast
neighbor 2001:DB8:1:4::1 remote-as 2
neighbor 192.168.1.9 remote-as 2
address-family ipv4
redistribute ospf 1
neighbor 192.168.1.9 activate
neighbor 192.168.1.9 next-hop-self
exit-address-family
address-family ipv6
redistribute connected
redistribute ospf 1 match internal external 1 external 2
neighbor 2001:DB8:1:4::1 activate
neighbor 2001:DB8:1:4::1 next-hop-self
exit-address-family
ip forward-protocol nd
no ip http server
no ip http secure-server
ip tftp source-interface GigabitEthernet0
ipv6 router ospf 1
redistribute connected
redistribute bgp 3 metric 10
control-plane
line con 0
stopbits 1
line aux 0
stopbits 1
line vty 0 4
login
end
```

```
      192.168.1.0/24 is variably subnetted, 7 subnets, 2 masks
B        192.168.1.0/30 [20/0] via 192.168.1.9, 00:03:42
B        192.168.1.4/30 [20/1] via 192.168.1.9, 00:03:12
C        192.168.1.8/30 is directly connected, GigabitEthernet0/0/0
L        192.168.1.10/32 is directly connected, GigabitEthernet0/0/0
B        192.168.1.12/30 [20/10] via 192.168.1.9, 00:02:27
C        192.168.1.16/30 is directly connected, GigabitEthernet0/0/1
L        192.168.1.17/32 is directly connected, GigabitEthernet0/0/1
B     192.168.2.0/24 [20/10] via 192.168.1.9, 00:01:57
O     192.168.3.0/24 [110/2] via 192.168.1.18, 00:00:01, GigabitEthernet0/0/1
R5(config)#do show ipv6 route
IPv6 Routing Table - default - 12 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, I1 - ISIS L1, I2 - ISIS L2
       IA - ISIS interarea, IS - ISIS summary, D - EIGRP, EX - EIGRP external
       ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2, a - Application
C   200:DB8:1:4::/126 [0/0]
     via GigabitEthernet0/0/0, directly connected
L   200:DB8:1:4::2/128 [0/0]
     via GigabitEthernet0/0/0, receive
B   2001:DB8:1:1::/126 [20/0]
     via FE80::B6A8:B9FF:FE47:92C0, GigabitEthernet0/0/0
B   2001:DB8:1:2::/126 [20/2]
     via FE80::B6A8:B9FF:FE47:92C0, GigabitEthernet0/0/0
B   2001:DB8:1:3::/126 [20/11]
     via FE80::B6A8:B9FF:FE47:92C0, GigabitEthernet0/0/0
C   2001:DB8:1:4::/126 [0/0]
     via GigabitEthernet0/0/0, directly connected
L   2001:DB8:1:4::2/128 [0/0]
     via GigabitEthernet0/0/0, receive
C   2001:DB8:1:5::/126 [0/0]
     via GigabitEthernet0/0/1, directly connected
L   2001:DB8:1:5::1/128 [0/0]
     via GigabitEthernet0/0/1, receive
B   2001:DB8:2:1::/120 [20/11]
     via FE80::B6A8:B9FF:FE47:92C0, GigabitEthernet0/0/0
O   2001:DB8:2:2::/120 [110/2]
     via FE80::521C:B0FF:FE2D:6801, GigabitEthernet0/0/1
L   FF00::/8 [0/0]
     via Null0, receive
R5(config)#

      192.168.1.0/24 is variably subnetted, 7 subnets, 2 masks
B        192.168.1.0/30 [20/0] via 192.168.1.9, 00:03:42
B        192.168.1.4/30 [20/1] via 192.168.1.9, 00:03:12
C        192.168.1.8/30 is directly connected, GigabitEthernet0/0/0
L        192.168.1.10/32 is directly connected, GigabitEthernet0/0/0
B        192.168.1.12/30 [20/10] via 192.168.1.9, 00:02:27
C        192.168.1.16/30 is directly connected, GigabitEthernet0/0/1
L        192.168.1.17/32 is directly connected, GigabitEthernet0/0/1
B     192.168.2.0/24 [20/10] via 192.168.1.9, 00:01:57
O     192.168.3.0/24 [110/2] via 192.168.1.18, 00:00:01, GigabitEthernet0/0/1
R5(config)#
```

R6 Configure:

version 15.5
service timestamps debug datetime msec
service timestamps log datetime msec
no platform punt-keepalive disable-kernel-core
hostname R6
boot-start-marker
boot-end-marker

```
vrf definition Mgmt-intf
address-family ipv4
exit-address-family
address-family ipv6
exit-address-family
no aaa new-model
ipv6 unicast-routing
subscriber templating
vtp domain cisco
vtp mode transparent
multilink bundle-name authenticated
license udi pid ISR4321/K9 sn FDO21491FHX
spanning-tree extend system-id
Redundancy
mode none
vlan internal allocation policy ascending
interface GigabitEthernet0/0/0
ip address 192.168.3.1 255.255.255.0
negotiation auto
ipv6 address 2001:DB8:2:2::1/120
ipv6 enable
ipv6 ospf 1 area 1
interface GigabitEthernet0/0/1
ip address 192.168.1.18 255.255.255.252
negotiation auto
ipv6 address 2001:DB8:1:5::2/126
ipv6 enable
ipv6 ospf 1 area 1
interface GigabitEthernet0/1/0
no ip address
shutdown
negotiation auto
interface GigabitEthernet0/1/1
no ip address
shutdown
negotiation auto
interface GigabitEthernet0
vrf forwarding Mgmt-intf
no ip address
shutdown
negotiation auto
interface Vlan1
no ip address
shutdown
router ospf 1
network 192.168.1.16 0.0.0.3 area 1
network 192.168.3.0 0.0.0.255 area 1
ip forward-protocol nd
```

no ip http server
no ip http secure-server
ip tftp source-interface GigabitEthernet0
ipv6 router ospf 1
control-plane
line con 0
stopbits 1
line aux 0
stopbits 1
line vty 0 4
login
end

```
R6(config)#do show ipv6 route
IPv6 Routing Table - default - 11 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, I1 - ISIS L1, I2 - ISIS L2
       IA - ISIS interarea, IS - ISIS summary, D - EIGRP, EX - EIGRP external
       ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2, a - Application
O   200:DB8:1:4::/126 [110/2]
     via FE80::6EDD:30FF:FEB6:6031, GigabitEthernet0/0/1
OE2 2001:DB8:1:1::/126 [110/10]
     via FE80::6EDD:30FF:FEB6:6031, GigabitEthernet0/0/1
OE2 2001:DB8:1:2::/126 [110/10]
     via FE80::6EDD:30FF:FEB6:6031, GigabitEthernet0/0/1
OE2 2001:DB8:1:3::/126 [110/10]
     via FE80::6EDD:30FF:FEB6:6031, GigabitEthernet0/0/1
O   2001:DB8:1:4::/126 [110/2]
     via FE80::6EDD:30FF:FEB6:6031, GigabitEthernet0/0/1
C   2001:DB8:1:5::/126 [0/0]
     via GigabitEthernet0/0/1, directly connected
L   2001:DB8:1:5::2/128 [0/0]
     via GigabitEthernet0/0/1, receive
OE2 2001:DB8:2:1::/120 [110/10]
     via FE80::6EDD:30FF:FEB6:6031, GigabitEthernet0/0/1
C   2001:DB8:2:2::/120 [0/0]
     via GigabitEthernet0/0/0, directly connected
L   2001:DB8:2:2::1/128 [0/0]
     via GigabitEthernet0/0/0, receive
L   FF00::/8 [0/0]
     via Null0, receive
R6(config)#
```

```
      192.168.1.0/24 is variably subnetted, 6 subnets, 2 masks
O E2     192.168.1.0/30
           [110/1] via 192.168.1.17, 00:01:36, GigabitEthernet0/0/1
O E2     192.168.1.4/30
           [110/1] via 192.168.1.17, 00:01:36, GigabitEthernet0/0/1
O        192.168.1.8/30
           [110/2] via 192.168.1.17, 00:01:36, GigabitEthernet0/0/1
O E2     192.168.1.12/30
           [110/1] via 192.168.1.17, 00:01:36, GigabitEthernet0/0/1
C        192.168.1.16/30 is directly connected, GigabitEthernet0/0/1
L        192.168.1.18/32 is directly connected, GigabitEthernet0/0/1
O E2  192.168.2.0/24 [110/1] via 192.168.1.17, 00:01:36, GigabitEthernet0/0/1
      192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.3.0/24 is directly connected, GigabitEthernet0/0/0
L        192.168.3.1/32 is directly connected, GigabitEthernet0/0/0
R6(config)#
```

Problem: In this lab, we faced two main problem, the first one is for the EIGRP redistribution, we don't know we need to put metric for it, which cause only border router know all the route to every subnets, but all the internal don't know the route to other network that not in the internal network, we solved this problem by looking at cisco forum to find out we need to add metric for redistribution. For ipv6, we configure the wrong ipv6 address for one interface on the border router, which cause all the ping to that company not working, first we thought that is a redistribution problem, but that is a normal ipv6 address problem, to solve this problem, we solve this by looking at cisco forum, it suggest us to check the bgp status, we find out bgp is not working, then we do show run, and find out the ipv6 address is wrong, it should be 2001 instead of 200.

Conclusion: In this lab, we learned how to set up EBGP to connect multiple company that using different internal routing protocol together, it helped us understand how current internal working by some ISP connect together, so everyone can reach internet. we learned more about how to set up redistribution and set up routing protocol. Overall, this lab helped us learn more about how different routing protocol works and improved our problem-solving technique, which can prepare us for future job situation when we need to set up BGP for connection to ISP or other company.

Interior BGP Lab

By Alvin Chow

Purpose: In this lab, we learned to configure IBGP to connect 3 different branch that using different routing protocol, included EIGRP and OSPF. This lab helps us understand how the company with different branch connect each other and how to set up other type of routing protocol.

Background information:

Border Gateway Protocol (BGP) is a set of rules that manages how data is routed across the internet. BGP is responsible for selecting the best path for data to travel by evaluating all available routes. BGP is essential for the internet's global routing system and is used by both the internet and service provider private networks. BGP enables communication between networks by exchanging routing information between autonomous systems (ASes). ASes are networks managed by a single enterprise or service provider. BGP is important for maintaining the internet working.

IBGP is used to exchange routing information between routers within the same autonomous system. Its primary purpose is to maintain consistent routing across all routers in the AS, ensuring that they share information about the best paths to reach every networks. iBGP operates differently from eBGP, which is used to exchange routes between different ASes. IBGP provides loop-free inter-router communication, ensures all routers are aware of each other, and enables efficient data transmission.

Open shortest path first (OSPF) is a routing protocol for internet, it uses link state routing algorithm, and it is an interior gateway protocol. It functions determine the shortest path to the destination, and it calculated based on bandwidth, delay and cost.

EIGRP (Enhanced Interior Gateway Routing Protocol) is a routing protocol used in networks to help routers share information about the best paths for sending data. It combines features of two types of protocols for faster updates and better scalability. EIGRP uses a calculation that considers bandwidth, delay, load to find the best route. Routers send hello packets to discover nearby routers and keep their information up to date. It adapts quickly to changes in the network, which helps reduce downtime when connections go up or down. EIGRP also supports Variable Length Subnet Masking, it allowing for better use of IP addresses. Additionally, it can work with different types of network protocols, making it a good choice for large and complex networks.

Lab summary: First, me and my partner designed to use 192.168.1.0/24 to be the connection ip between router, then we decided to use /30 for point-to-point connection between router and I decided to use 192.168.2.0/24 amd 192.168.3.0/24 to be the host subnet . For ipv6, we decided to use 1: for management and 2: to be host subnets. We decided to use 2 routing protocol for each company and use IBGP to share all the routing

information between branches. We use OSPF and EIGRP for the internal routing process. For IBGP we used AS 1 and the branch that using EIGRP to redistribute into BGP and learn from IBGP and redistribute back to EIGRP. For the branches that using OSPF, we redistribute the route into IBGP and after it learned the route from IBGP, it redistribute back to OSPF

Lab Commands: Ip address : ip address and subnet mask, this help us set a static ip for that interface.

Ipv6 unicast routing, it let router can do ipv6 routing.

Ipv6 eigrp/ospf process-number, this command let us to put routing protocol to the interface that we want.

Router eigrp/bgp/ospf process number/AS number, this command can let us configure routing protocol

Neighbor ip address/ipv6 address remotes-as As number, this command can let us set up the neighbor ip for BGP, it can help neighbor establish the connection for exchange route.

Neighbor ip/ipv6 address next-hop-self, this command set the BGP route next hop to be that routing, which can help other device know how to reach that subnet.

Network network ip wildcard mask, this command let us configure the interface that we want to put in routing protocol.

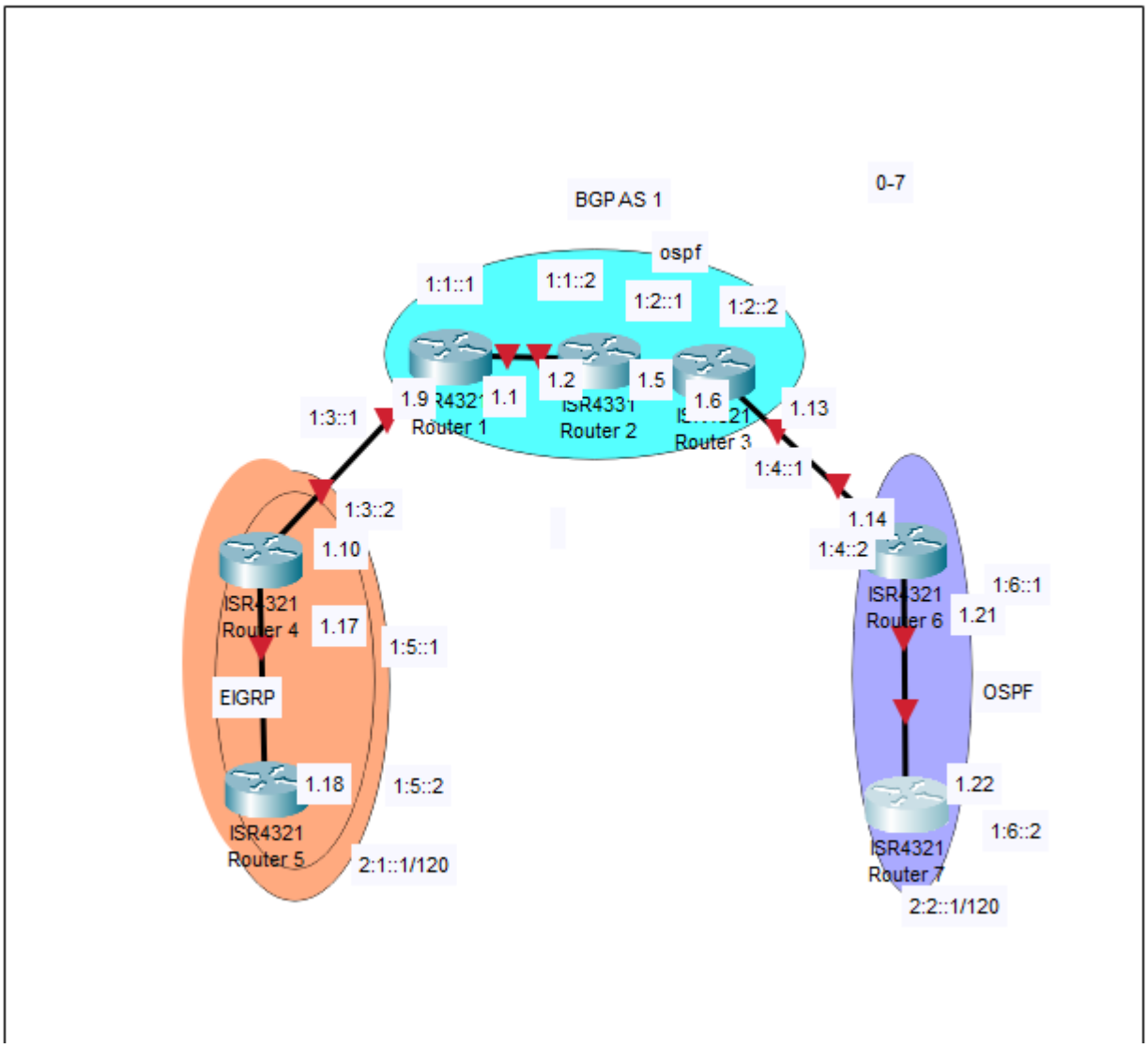
Redistribute connected, this command let us to Redistribute the connected route into BGP

Redistribute ospf/bgp/eigrp process number/ AS-number metric, it can redistribute BGP route into internal routing protocol or redistribute internal route to BGP to let other router learn the learn

no bgp default ipv4-unicast, it let us can configure ipv4 and ipv6 for BGP

BGP redistribute internal, this allow IBGP working

Lab Topology:



Configuration:

R1: version 15.5
service timestamps debug datetime msec
service timestamps log datetime msec
no platform punt-keepalive disable-kernel-core
hostname R1
boot-start-marker
boot-end-marker
vrf definition Mgmt-intf
address-family ipv4
exit-address-family
address-family ipv6
exit-address-family
no aaa new-model

```
ipv6 unicast-routing
subscriber templating
vtp domain cisco
vtp mode transparent
multilink bundle-name authenticated
license udi pid ISR4321/K9 sn FDO214421BY
spanning-tree extend system-id
redundancy
mode none
vlan internal allocation policy ascending
interface GigabitEthernet0/0/0
ip address 192.168.1.9 255.255.255.252
negotiation auto
ipv6 address 1:3::1/126
ipv6 enable
ipv6 ospf 1 area 0
interface GigabitEthernet0/0/1
ip address 192.168.1.1 255.255.255.252
negotiation auto
ipv6 address 1:1::1/126
ipv6 enable
ipv6 ospf 1 area 0
interface Serial0/1/0
no ip address
shutdown
interface Serial0/1/1
no ip address
shutdown
interface GigabitEthernet0/2/0
no ip address
shutdown
negotiation auto
interface GigabitEthernet0/2/1
no ip address
shutdown
negotiation auto
interface GigabitEthernet0
vrf forwarding Mgmt-intf
no ip address
shutdown
negotiation auto
interface Vlan1
no ip address
shutdown
router ospf 1
redistribute connected subnets
```

```
redistribute bgp 1 subnets
network 192.168.1.0 0.0.0.3 area 0
network 192.168.1.8 0.0.0.3 area 0
router bgp 1
bgp log-neighbor-changes
no bgp default ipv4-unicast
neighbor 1:3::2 remote-as 1
neighbor 192.168.1.10 remote-as 1
address-family ipv4
bgp redistribute-internal
redistribute connected
redistribute ospf 1 match internal external 1 external 2
neighbor 192.168.1.10 activate
neighbor 192.168.1.10 next-hop-self
exit-address-family
address-family ipv6
redistribute connected
redistribute ospf 1 match internal external 1 external 2
bgp redistribute-internal
neighbor 1:3::2 activate
neighbor 1:3::2 next-hop-self
exit-address-family
ip forward-protocol nd
no ip http server
no ip http secure-server
ip tftp source-interface GigabitEthernet0
ipv6 router ospf 1
redistribute connected
redistribute bgp 1 metric 10
control-plane
line con 0
stopbits 1
line aux 0
stopbits 1
line vty 0 4
login
end
```

```
      192.168.1.0/24 is variably subnetted, 8 subnets, 2 masks
C        192.168.1.0/30 is directly connected, GigabitEthernet0/0/1
L        192.168.1.1/32 is directly connected, GigabitEthernet0/0/1
O        192.168.1.4/30
           [110/2] via 192.168.1.2, 00:05:48, GigabitEthernet0/0/1
C        192.168.1.8/30 is directly connected, GigabitEthernet0/0/0
L        192.168.1.9/32 is directly connected, GigabitEthernet0/0/0
O        192.168.1.12/30
           [110/3] via 192.168.1.2, 00:05:48, GigabitEthernet0/0/1
B        192.168.1.16/30 [200/0] via 192.168.1.10, 00:05:52
O IA     192.168.1.20/30
           [110/4] via 192.168.1.2, 00:05:48, GigabitEthernet0/0/1
B     192.168.2.0/24 [200/3072] via 192.168.1.10, 00:05:52
      192.168.3.0/30 is subnetted, 1 subnets
O IA     192.168.3.0 [110/5] via 192.168.1.2, 00:05:48, GigabitEthernet0/0/1
R1#show ipv6 route
IPv6 Routing Table - default - 11 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, I1 - ISIS L1, I2 - ISIS L2
       IA - ISIS interarea, IS - ISIS summary, D - EIGRP, EX - EIGRP external
       ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2, a - Application
C   1:1::/126 [0/0]
     via GigabitEthernet0/0/1, directly connected
L   1:1::1/128 [0/0]
     via GigabitEthernet0/0/1, receive
O   1:2::/126 [110/2]
     via FE80::B6A8:B9FF:FE47:92C1, GigabitEthernet0/0/1
C   1:3::/126 [0/0]
     via GigabitEthernet0/0/0, directly connected
L   1:3::1/128 [0/0]
     via GigabitEthernet0/0/0, receive
OI  1:4::/126 [110/3]
     via FE80::B6A8:B9FF:FE47:92C1, GigabitEthernet0/0/1
B   1:5::/126 [200/0]
     via 1:3::2
OI  1:6::/126 [110/4]
     via FE80::B6A8:B9FF:FE47:92C1, GigabitEthernet0/0/1
B   2:1::/120 [200/3072]
     via 1:3::2
OI  2:2::/120 [110/5]
     via FE80::B6A8:B9FF:FE47:92C1, GigabitEthernet0/0/1
L   FF00::/8 [0/0]
     via Null0, receive
```

R2:

version 15.5
service timestamps debug datetime msec
service timestamps log datetime msec
no platform punt-keepalive disable-kernel-core
hostname R2
boot-start-marker
boot-end-marker
vrf definition Mgmt-intf
address-family ipv4
exit-address-family

```
address-family ipv6
exit-address-family
no aaa new-model
ipv6 unicast-routing
subscriber templating
multilink bundle-name authenticated
license udi pid ISR4321/K9 sn FDO214420QQ
license accept end user agreement
license boot level securityk9
spanning-tree extend system-id
redundancy
mode none
vlan internal allocation policy ascending
interface GigabitEthernet0/0/0
ip address 192.168.1.5 255.255.255.252
negotiation auto
ipv6 address 1:2::1/126
ipv6 enable
ipv6 ospf 1 area 0
interface GigabitEthernet0/0/1
ip address 192.168.1.2 255.255.255.252
negotiation auto
ipv6 address 1:1::2/126
ipv6 enable
ipv6 ospf 1 area 0
interface Serial0/1/0
interface Serial0/1/1
interface GigabitEthernet0
vrf forwarding Mgmt-intf
no ip address
shutdown
negotiation auto
interface Vlan1
no ip address
shutdown
router ospf 1
network 192.168.1.0 0.0.0.3 area 0
network 192.168.1.4 0.0.0.3 area 0
ip forward-protocol nd
no ip http server
no ip http secure-server
ip tftp source-interface GigabitEthernet0
ipv6 router ospf 1
control-plane
line con 0
stopbits 1
line aux 0
stopbits 1
```

line vty 0 4
login
end

```
      192.168.1.0/24 is variably subnetted, 8 subnets, 2 masks
C        192.168.1.0/30 is directly connected, GigabitEthernet0/0/1
L        192.168.1.2/32 is directly connected, GigabitEthernet0/0/1
C        192.168.1.4/30 is directly connected, GigabitEthernet0/0/0
L        192.168.1.5/32 is directly connected, GigabitEthernet0/0/0
O        192.168.1.8/30
           [110/2] via 192.168.1.1, 00:04:23, GigabitEthernet0/0/1
O        192.168.1.12/30
           [110/2] via 192.168.1.6, 00:18:07, GigabitEthernet0/0/0
O E2     192.168.1.16/30
           [110/1] via 192.168.1.1, 00:04:23, GigabitEthernet0/0/1
O IA     192.168.1.20/30
           [110/3] via 192.168.1.6, 00:13:47, GigabitEthernet0/0/0
O E2  192.168.2.0/24 [110/1] via 192.168.1.1, 00:04:23, GigabitEthernet0/0/1
      192.168.3.0/30 is subnetted, 1 subnets
O IA     192.168.3.0 [110/4] via 192.168.1.6, 00:13:05, GigabitEthernet0/0/0
R2#show ipv6 route
IPv6 Routing Table - default - 11 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE - Destinatior
       NDr - Redirect, O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1
       OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       a - Application
C   1:1::/126 [0/0]
     via GigabitEthernet0/0/1, directly connected
L   1:1::2/128 [0/0]
     via GigabitEthernet0/0/1, receive
C   1:2::/126 [0/0]
     via GigabitEthernet0/0/0, directly connected
L   1:2::1/128 [0/0]
     via GigabitEthernet0/0/0, receive
O   1:3::/126 [110/2]
     via FE80::B6A8:B9FF:FE01:B511, GigabitEthernet0/0/1
OI  1:4::/126 [110/2]
     via FE80::B6A8:B9FF:FE01:AE50, GigabitEthernet0/0/0
OE2 1:5::/126 [110/10]
     via FE80::B6A8:B9FF:FE01:B511, GigabitEthernet0/0/1
OI  1:6::/126 [110/3]
     via FE80::B6A8:B9FF:FE01:AE50, GigabitEthernet0/0/0
OE2 2:1::/120 [110/10]
     via FE80::B6A8:B9FF:FE01:B511, GigabitEthernet0/0/1
OI  2:2::/120 [110/4]
     via FE80::B6A8:B9FF:FE01:AE50, GigabitEthernet0/0/0
L   FF00::/8 [0/0]
     via Null0, receive
```

R3:

version 15.5
service timestamps debug datetime msec
service timestamps log datetime msec
no platform punt-keepalive disable-kernel-core
hostname R3
boot-start-marker

```
boot-end-marker
vrf definition Mgmt-intf
address-family ipv4
exit-address-family
address-family ipv6
exit-address-family
no aaa new-model
ipv6 unicast-routing
subscriber templating
vtp domain cisco
vtp mode transparent
multilink bundle-name authenticated
license udi pid ISR4321/K9 sn FDO214420HY
license boot level securityk9
spanning-tree extend system-id
redundancy
mode none
vlan internal allocation policy ascending
vlan 10,20
interface GigabitEthernet0/0/0
ip address 192.168.1.6 255.255.255.252
negotiation auto
ipv6 address 1:2::2/126
ipv6 enable
ipv6 ospf 1 area 0
interface GigabitEthernet0/0/1
ip address 192.168.1.13 255.255.255.252
negotiation auto
ipv6 address 1:4::1/126
ipv6 enable
ipv6 ospf 1 area 2
interface Serial0/1/0
no ip address
interface Serial0/1/1
no ip address
interface GigabitEthernet0
vrf forwarding Mgmt-intf
no ip address
negotiation auto
interface Vlan1
no ip address
router ospf 1
redistribute bgp 1 subnets
network 192.168.1.4 0.0.0.3 area 0
network 192.168.1.12 0.0.0.3 area 0
router bgp 1
bgp log-neighbor-changes
no bgp default ipv4-unicast
```

```
neighbor 1:4::2 remote-as 1
neighbor 192.168.1.14 remote-as 1
address-family ipv4
bgp redistribute-internal
redistribute connected
redistribute ospf 1 match internal external 1 external 2
neighbor 192.168.1.14 activate
neighbor 192.168.1.14 next-hop-self
exit-address-family
address-family ipv6
redistribute connected
redistribute ospf 1
bgp redistribute-internal
neighbor 1:4::2 activate
neighbor 1:4::2 next-hop-self
exit-address-family
ip forward-protocol nd
no ip http server
no ip http secure-server
ip tftp source-interface GigabitEthernet0
ipv6 router ospf 1
control-plane
line con 0
stopbits 1
line aux 0
stopbits 1
line vty 0 4
login
end
```

```
      192.168.1.0/24 is variably subnetted, 8 subnets, 2 masks
O        192.168.1.0/30
           [110/2] via 192.168.1.5, 00:12:43, GigabitEthernet0/0/0
C        192.168.1.4/30 is directly connected, GigabitEthernet0/0/0
L        192.168.1.6/32 is directly connected, GigabitEthernet0/0/0
O        192.168.1.8/30
           [110/3] via 192.168.1.5, 00:09:50, GigabitEthernet0/0/0
C        192.168.1.12/30 is directly connected, GigabitEthernet0/0/1
L        192.168.1.13/32 is directly connected, GigabitEthernet0/0/1
O E2     192.168.1.16/30
           [110/1] via 192.168.1.5, 00:09:50, GigabitEthernet0/0/0
O IA     192.168.1.20/30
           [110/2] via 192.168.1.14, 00:19:23, GigabitEthernet0/0/1
O E2  192.168.2.0/24 [110/1] via 192.168.1.5, 00:09:50, GigabitEthernet0/0/0
      192.168.3.0/30 is subnetted, 1 subnets
O IA     192.168.3.0 [110/3] via 192.168.1.14, 00:18:42, GigabitEthernet0/0/1
R3#show ipv6 route
IPv6 Routing Table - default - 11 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE - Destination
       NDr - Redirect, O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1
       OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       a - Application
O   1:1::/126 [110/2]
     via FE80::B6A8:B9FF:FE47:92C0, GigabitEthernet0/0/0
C   1:2::/126 [0/0]
     via GigabitEthernet0/0/0, directly connected
L   1:2::2/128 [0/0]
     via GigabitEthernet0/0/0, receive
O   1:3::/126 [110/3]
     via FE80::B6A8:B9FF:FE47:92C0, GigabitEthernet0/0/0
C   1:4::/126 [0/0]
     via GigabitEthernet0/0/1, directly connected
L   1:4::1/128 [0/0]
     via GigabitEthernet0/0/1, receive
OE2 1:5::/126 [110/10]
     via FE80::B6A8:B9FF:FE47:92C0, GigabitEthernet0/0/0
O   1:6::/126 [110/2]
     via FE80::521C:B0FF:FE2D:6801, GigabitEthernet0/0/1
OE2 2:1::/120 [110/10]
     via FE80::B6A8:B9FF:FE47:92C0, GigabitEthernet0/0/0
O   2:2::/120 [110/3]
     via FE80::521C:B0FF:FE2D:6801, GigabitEthernet0/0/1
L   FF00::/8 [0/0]
     via Null0, receive
```

R4:

version 15.5
service timestamps debug datetime msec
service timestamps log datetime msec
no platform punt-keepalive disable-kernel-core
hostname R4
boot-start-marker
boot-end-marker
vrf definition Mgmt-intf
address-family ipv4
exit-address-family

```
address-family ipv6
exit-address-family
no aaa new-model
ipv6 unicast-routing
subscriber templating
vtp domain cisco
vtp mode transparent
multilink bundle-name authenticated
license udi pid ISR4321/K9 sn FDO21491LXV
license accept end user agreement
license boot level securityk9
spanning-tree extend system-id
redundancy
mode none
vlan internal allocation policy ascending
vlan 2
name v2
vlan 3
name v3
vlan 4
name v4
vlan 10,20
interface GigabitEthernet0/0/0
ip address 192.168.1.10 255.255.255.252
negotiation auto
ipv6 address 1:3::2/126
ipv6 enable
ipv6 eigrp 1
interface GigabitEthernet0/0/1
ip address 192.168.1.17 255.255.255.252
negotiation auto
ipv6 address 1:5::1/126
ipv6 enable
ipv6 eigrp 1
interface Serial0/1/0
no ip address
shutdown
interface Serial0/1/1
no ip address
shutdown
interface GigabitEthernet0
vrf forwarding Mgmt-intf
no ip address
shutdown
negotiation auto
interface Vlan1
no ip address
shutdown
```

```
router eigrp 1
network 192.168.1.8 0.0.0.3
network 192.168.1.16 0.0.0.3
redistribute connected
redistribute bgp 1 metric 100 1 255 1 1500
router bgp 1
bgp log-neighbor-changes
no bgp default ipv4-unicast
neighbor 1:3::1 remote-as 1
neighbor 192.168.1.9 remote-as 1
address-family ipv4
bgp redistribute-internal
redistribute connected
redistribute eigrp 1
neighbor 192.168.1.9 activate
neighbor 192.168.1.9 next-hop-self
exit-address-family
address-family ipv6
redistribute connected
redistribute eigrp 1
bgp redistribute-internal
neighbor 1:3::1 activate
neighbor 1:3::1 next-hop-self
exit-address-family
ip forward-protocol nd
no ip http server
no ip http secure-server
ip tftp source-interface GigabitEthernet0
ipv6 router eigrp 1
redistribute bgp 1 metric 10000 10 255 1 1500
redistribute connected
control-plane
line con 0
stopbits 1
line aux 0
stopbits 1
line vty 0 4
login
end
```

```
      192.168.1.0/24 is variably subnetted, 8 subnets, 2 masks
B        192.168.1.0/30 [200/0] via 192.168.1.9, 00:11:19
B        192.168.1.4/30 [200/2] via 192.168.1.9, 00:11:16
C        192.168.1.8/30 is directly connected, GigabitEthernet0/0/0
L        192.168.1.10/32 is directly connected, GigabitEthernet0/0/0
B        192.168.1.12/30 [200/3] via 192.168.1.9, 00:11:16
C        192.168.1.16/30 is directly connected, GigabitEthernet0/0/1
L        192.168.1.17/32 is directly connected, GigabitEthernet0/0/1
B        192.168.1.20/30 [200/4] via 192.168.1.9, 00:11:16
D     192.168.2.0/24
           [90/3072] via 192.168.1.18, 00:27:21, GigabitEthernet0/0/1
      192.168.3.0/30 is subnetted, 1 subnets
B        192.168.3.0 [200/5] via 192.168.1.9, 00:11:16
R4#show ipv6 route
IPv6 Routing Table - default - 11 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE - Destination
       NDr - Redirect, O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1
       OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       a - Application
B   1:1::/126 [200/0]
     via 1:3::1
B   1:2::/126 [200/2]
     via 1:3::1
C   1:3::/126 [0/0]
     via GigabitEthernet0/0/0, directly connected
L   1:3::2/128 [0/0]
     via GigabitEthernet0/0/0, receive
B   1:4::/126 [200/3]
     via 1:3::1
C   1:5::/126 [0/0]
     via GigabitEthernet0/0/1, directly connected
L   1:5::1/128 [0/0]
     via GigabitEthernet0/0/1, receive
B   1:6::/126 [200/4]
     via 1:3::1
D   2:1::/120 [90/3072]
     via FE80::6EDD:30FF:FEB6:6031, GigabitEthernet0/0/1
B   2:2::/120 [200/5]
     via 1:3::1
L   FF00::/8 [0/0]
     via Null0, receive
```

R5:

version 15.5
service timestamps debug datetime msec
service timestamps log datetime msec
no platform punt-keepalive disable-kernel-core
hostname R5
boot-start-marker
boot-end-marker
vrf definition Mgmt-intf
address-family ipv4
exit-address-family
address-family ipv6
exit-address-family

```
no aaa new-model
ipv6 unicast-routing
subscriber templating
vtp domain cisco
vtp mode transparent
multilink bundle-name authenticated
license udi pid ISR4321/K9 sn FDO21400XZX
spanning-tree extend system-id
redundancy
mode none
vlan internal allocation policy ascending
interface GigabitEthernet0/0/0
ip address 192.168.2.1 255.255.255.0
negotiation auto
ipv6 address 2:1::1/120
ipv6 enable
ipv6 eigrp 1
interface GigabitEthernet0/0/1
ip address 192.168.1.18 255.255.255.252
negotiation auto
ipv6 address 1:5::2/126
ipv6 enable
ipv6 eigrp 1
interface Serial0/1/0
no ip address
shutdown
interface Serial0/1/1
no ip address
shutdown
interface GigabitEthernet0
vrf forwarding Mgmt-intf
no ip address
shutdown
negotiation auto
interface Vlan1
no ip address
shutdown
router eigrp 1
network 192.168.1.16 0.0.0.3
network 192.168.2.0
ip forward-protocol nd
no ip http server
no ip http secure-server
ip tftp source-interface GigabitEthernet0
ipv6 router eigrp 1
control-plane
line con 0
stopbits 1
```

line aux 0
stopbits 1
line vty 0 4
login
end

```
      192.168.1.0/24 is variably subnetted, 7 subnets, 2 masks
D EX     192.168.1.0/30
           [170/25600512] via 192.168.1.17, 00:12:24, GigabitEthernet0/0/1
D EX     192.168.1.4/30
           [170/25600512] via 192.168.1.17, 00:12:21, GigabitEthernet0/0/1
D        192.168.1.8/30
           [90/3072] via 192.168.1.17, 00:15:15, GigabitEthernet0/0/1
D EX     192.168.1.12/30
           [170/25600512] via 192.168.1.17, 00:12:21, GigabitEthernet0/0/1
C        192.168.1.16/30 is directly connected, GigabitEthernet0/0/1
L        192.168.1.18/32 is directly connected, GigabitEthernet0/0/1
D EX     192.168.1.20/30
           [170/25600512] via 192.168.1.17, 00:12:21, GigabitEthernet0/0/1
      192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.2.0/24 is directly connected, GigabitEthernet0/0/0
L        192.168.2.1/32 is directly connected, GigabitEthernet0/0/0
      192.168.3.0/30 is subnetted, 1 subnets
D EX     192.168.3.0
           [170/25600512] via 192.168.1.17, 00:12:21, GigabitEthernet0/0/1
R5#show ipv6 route
IPv6 Routing Table - default - 11 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, I1 - ISIS L1, I2 - ISIS L2
       IA - ISIS interarea, IS - ISIS summary, D - EIGRP, EX - EIGRP external
       ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2, a - Application
EX  1:1::/126 [170/258816]
     via FE80::521C:B0FF:FE2D:7101, GigabitEthernet0/0/1
EX  1:2::/126 [170/258816]
     via FE80::521C:B0FF:FE2D:7101, GigabitEthernet0/0/1
D   1:3::/126 [90/3072]
     via FE80::521C:B0FF:FE2D:7101, GigabitEthernet0/0/1
EX  1:4::/126 [170/258816]
     via FE80::521C:B0FF:FE2D:7101, GigabitEthernet0/0/1
C   1:5::/126 [0/0]
     via GigabitEthernet0/0/1, directly connected
L   1:5::2/128 [0/0]
     via GigabitEthernet0/0/1, receive
EX  1:6::/126 [170/258816]
     via FE80::521C:B0FF:FE2D:7101, GigabitEthernet0/0/1
C   2:1::/120 [0/0]
     via GigabitEthernet0/0/0, directly connected
L   2:1::1/128 [0/0]
     via GigabitEthernet0/0/0, receive
EX  2:2::/120 [170/258816]
     via FE80::521C:B0FF:FE2D:7101, GigabitEthernet0/0/1
L   FF00::/8 [0/0]
     via Null0, receive
```

R6:

version 15.5
service timestamps debug datetime msec

```
service timestamps log datetime msec
no platform punt-keepalive disable-kernel-core
hostname R6
boot-start-marker
boot-end-marker
vrf definition Mgmt-intf
address-family ipv4
exit-address-family
address-family ipv6
exit-address-family
no aaa new-model
ipv6 unicast-routing
subscriber templating
vtp domain cisco
vtp mode transparent
multilink bundle-name authenticated
license udi pid ISR4321/K9 sn FDO21491FHX
spanning-tree extend system-id
redundancy
mode none
vlan internal allocation policy ascending
interface GigabitEthernet0/0/0
ip address 192.168.1.21 255.255.255.252
negotiation auto
ipv6 address 1:6::1/126
ipv6 enable
ipv6 ospf 1 area 2
interface GigabitEthernet0/0/1
ip address 192.168.1.14 255.255.255.252
negotiation auto
ipv6 address 1:4::2/126
ipv6 enable
ipv6 ospf 1 area 2
interface GigabitEthernet0/1/0
no ip address
shutdown
negotiation auto
interface GigabitEthernet0/1/1
no ip address
shutdown
negotiation auto
interface GigabitEthernet0
vrf forwarding Mgmt-intf
no ip address
shutdown
negotiation auto
interface Vlan1
no ip address
```

```
shutdown
router ospf 1
redistribute bgp 1 subnets
network 192.168.1.12 0.0.0.3 area 0
network 192.168.1.20 0.0.0.3 area 2
router bgp 1
bgp log-neighbor-changes
no bgp default ipv4-unicast
neighbor 1:4::1 remote-as 1
neighbor 192.168.1.13 remote-as 1
address-family ipv4
bgp redistribute-internal
redistribute connected
redistribute ospf 1 match internal external 1 external 2
neighbor 192.168.1.13 activate
neighbor 192.168.1.13 next-hop-self
exit-address-family
address-family ipv6
redistribute connected
redistribute ospf 1
bgp redistribute-internal
neighbor 1:4::1 activate
neighbor 1:4::1 next-hop-self
exit-address-family
ip forward-protocol nd
no ip http server
no ip http secure-server
ip tftp source-interface GigabitEthernet0
ipv6 router ospf 1
control-plane
line con 0
stopbits 1
line aux 0
stopbits 1
line vty 0 4
login
end
```

```
      192.168.1.0/24 is variably subnetted, 8 subnets, 2 masks
O        192.168.1.0/30
           [110/3] via 192.168.1.13, 00:17:52, GigabitEthernet0/0/1
O        192.168.1.4/30
           [110/2] via 192.168.1.13, 00:24:43, GigabitEthernet0/0/1
O        192.168.1.8/30
           [110/4] via 192.168.1.13, 00:14:59, GigabitEthernet0/0/1
C        192.168.1.12/30 is directly connected, GigabitEthernet0/0/1
L        192.168.1.14/32 is directly connected, GigabitEthernet0/0/1
O E2     192.168.1.16/30
           [110/1] via 192.168.1.13, 00:14:59, GigabitEthernet0/0/1
C        192.168.1.20/30 is directly connected, GigabitEthernet0/0/0
L        192.168.1.21/32 is directly connected, GigabitEthernet0/0/0
O E2  192.168.2.0/24 [110/1] via 192.168.1.13, 00:14:59, GigabitEthernet0/0/1
      192.168.3.0/30 is subnetted, 1 subnets
O        192.168.3.0 [110/2] via 192.168.1.22, 00:23:51, GigabitEthernet0/0/0
R6#show ipv6 route
IPv6 Routing Table - default - 11 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, I1 - ISIS L1, I2 - ISIS L2
       IA - ISIS interarea, IS - ISIS summary, D - EIGRP, EX - EIGRP external
       ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2, a - Application
OI  1:1::/126 [110/3]
     via FE80::B6A8:B9FF:FE01:AE51, GigabitEthernet0/0/1
OI  1:2::/126 [110/2]
     via FE80::B6A8:B9FF:FE01:AE51, GigabitEthernet0/0/1
OI  1:3::/126 [110/4]
     via FE80::B6A8:B9FF:FE01:AE51, GigabitEthernet0/0/1
C   1:4::/126 [0/0]
     via GigabitEthernet0/0/1, directly connected
L   1:4::2/128 [0/0]
     via GigabitEthernet0/0/1, receive
OE2 1:5::/126 [110/10]
     via FE80::B6A8:B9FF:FE01:AE51, GigabitEthernet0/0/1
C   1:6::/126 [0/0]
     via GigabitEthernet0/0/0, directly connected
L   1:6::1/128 [0/0]
     via GigabitEthernet0/0/0, receive
OE2 2:1::/120 [110/10]
     via FE80::B6A8:B9FF:FE01:AE51, GigabitEthernet0/0/1
O   2:2::/120 [110/2]
     via FE80::B6A8:B9FF:FE01:BEA0, GigabitEthernet0/0/0
L   FF00::/8 [0/0]
     via Null0, receive
```

R7:

version 15.5
service timestamps debug datetime msec
service timestamps log datetime msec
no platform punt-keepalive disable-kernel-core
hostname R7
boot-start-marker
boot-end-marker
vrf definition Mgmt-intf
address-family ipv4

```
exit-address-family
address-family ipv6
exit-address-family
no aaa new-model
ipv6 unicast-routing
subscriber templating
vtp domain cisco
vtp mode transparent
multilink bundle-name authenticated
license udi pid ISR4321/K9 sn FDO214420G3
spanning-tree extend system-id
redundancy
mode none
vlan internal allocation policy ascending
vlan 10,20
interface GigabitEthernet0/0/0
ip address 192.168.1.22 255.255.255.252
negotiation auto
ipv6 address 1:6::2/126
ipv6 enable
ipv6 ospf 1 area 2
interface GigabitEthernet0/0/1
ip address 192.168.3.1 255.255.255.252
negotiation auto
ipv6 address 2:2::1/120
ipv6 enable
ipv6 ospf 1 area 2
interface Serial0/1/0
no ip address
shutdown
interface Serial0/1/1
no ip address
shutdown
interface GigabitEthernet0
vrf forwarding Mgmt-intf
no ip address
shutdown
negotiation auto
interface Vlan1
no ip address
shutdown
router ospf 1
network 192.168.1.20 0.0.0.3 area 2
network 192.168.3.0 0.0.0.3 area 2
ip forward-protocol nd
no ip http server
no ip http secure-server
ip tftp source-interface GigabitEthernet0
```

ipv6 router ospf 1
control-plane
line con 0
stopbits 1
line aux 0
stopbits 1
line vty 0 4
login
end

```
      192.168.1.0/24 is variably subnetted, 7 subnets, 2 masks
O IA     192.168.1.0/30
           [110/4] via 192.168.1.21, 00:18:59, GigabitEthernet0/0/0
O IA     192.168.1.4/30
           [110/3] via 192.168.1.21, 00:24:59, GigabitEthernet0/0/0
O IA     192.168.1.8/30
           [110/5] via 192.168.1.21, 00:16:07, GigabitEthernet0/0/0
O IA     192.168.1.12/30
           [110/2] via 192.168.1.21, 00:24:59, GigabitEthernet0/0/0
O E2     192.168.1.16/30
           [110/1] via 192.168.1.21, 00:16:02, GigabitEthernet0/0/0
C        192.168.1.20/30 is directly connected, GigabitEthernet0/0/0
L        192.168.1.22/32 is directly connected, GigabitEthernet0/0/0
O E2  192.168.2.0/24 [110/1] via 192.168.1.21, 00:16:02, GigabitEthernet0/0/0
      192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.3.0/30 is directly connected, GigabitEthernet0/0/1
L        192.168.3.1/32 is directly connected, GigabitEthernet0/0/1
R7#show ipv6 route
IPv6 Routing Table - default - 11 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, I1 - ISIS L1, I2 - ISIS L2
       IA - ISIS interarea, IS - ISIS summary, D - EIGRP, EX - EIGRP external
       ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2, a - Application
OI  1:1::/126 [110/4]
     via FE80::521C:B0FF:FE2D:6800, GigabitEthernet0/0/0
OI  1:2::/126 [110/3]
     via FE80::521C:B0FF:FE2D:6800, GigabitEthernet0/0/0
OI  1:3::/126 [110/5]
     via FE80::521C:B0FF:FE2D:6800, GigabitEthernet0/0/0
O   1:4::/126 [110/2]
     via FE80::521C:B0FF:FE2D:6800, GigabitEthernet0/0/0
OE2 1:5::/126 [110/10]
     via FE80::521C:B0FF:FE2D:6800, GigabitEthernet0/0/0
C   1:6::/126 [0/0]
     via GigabitEthernet0/0/0, directly connected
L   1:6::2/128 [0/0]
     via GigabitEthernet0/0/0, receive
OE2 2:1::/120 [110/10]
     via FE80::521C:B0FF:FE2D:6800, GigabitEthernet0/0/0
C   2:2::/120 [0/0]
     via GigabitEthernet0/0/1, directly connected
L   2:2::1/128 [0/0]
     via GigabitEthernet0/0/1, receive
L   FF00::/8 [0/0]
     via Null0, receive
```

Problem: The only big problem that we faced is we don't know we need `bgp redistribute-internal` command and we find the solution for this problem at cisco forum.

Conclusion: In this lab, we learned how to set up IBGP to connect multiple branch that using different internal routing protocol together. We learned more about how to set up redistribution and how to set up different routing protocol. Overall, this lab helped us learn more about how different routing protocol works and improved our problem-solving technique, which can prepare us for future job situation when we need to set up IBGP for company connect multiple branch.

PA-220 URL filtering lab

By Alvin Chow

Purpose: The purpose of the URL filtering lab is learn how to filter and block the website based on what elementary school based on they want students can access. We learned how to filter traffic based on that category, then we can block the whole category. We also learned how to set up override for some websites that admin need to access.

Background info: The Palo Alto Networks® PA-220 next-generation firewall is designed for small organizations or branch offices. This firewall included passive cooling to reduce noise and power consumption, eight Ethernet ports, and dual power adapters for power redundancy. The PA-220 firewall enables to secure the organization through advanced visibility and control of applications, users, and content.

Palo Alto Networks (Palo Alto) provides cybersecurity services to enterprises, government, and service providers. This company's products and services portfolio include firewall and software, panorama, support and maintenance services, security management solutions, and virtual system upgrades.

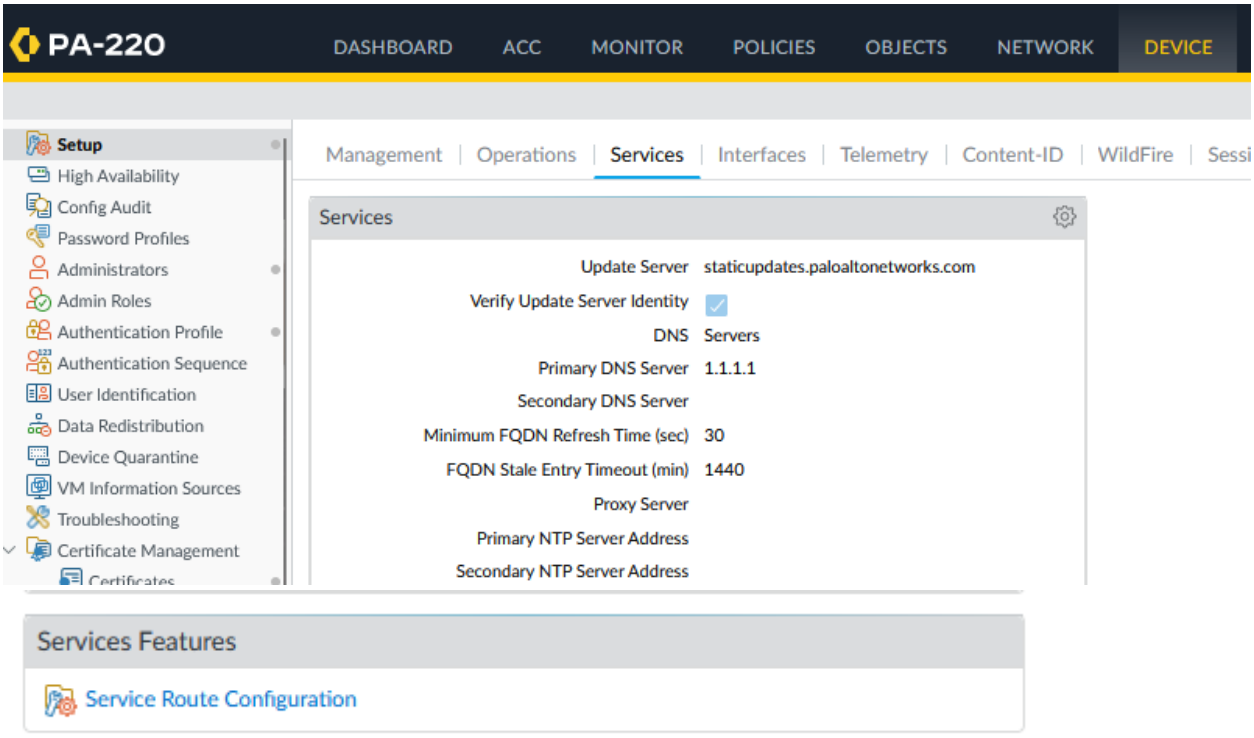
URL (Uniform Resource Locator) is the web address used to identify a resource on the internet. It is a reference that enables users to access websites, files, or services. A typical URL includes several parts, including the **protocol** (such as HTTP or HTTPS), the **domain name, then** an optional **port number**, and the **path** to the specific resource. URLs can also include **query parameters** to pass information to the server. In summary URL can help directs web browsers to the correct server.

URL filtering is a method used to control access to websites by checking and restrict the URLs users try to visit. It works by comparing URLs to predefined lists, such as blacklists or whitelists. URL filtering is commonly used in businesses, schools, and homes for many different purposes, such as improving security by blocking malicious sites, enhancing productivity by restricting access to non-work-related content, and ensuring compliance with organizational policies. It can be implemented through firewalls, network devices, or web filtering software to manage web traffic effectively.

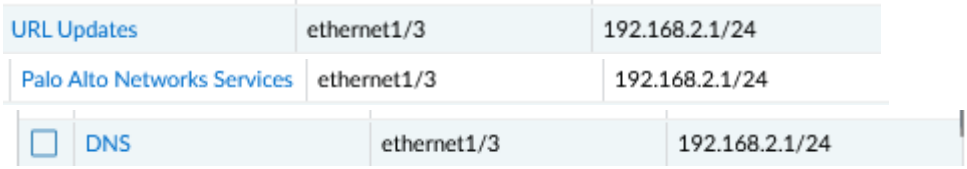
Lab summary: Step by Step guide setting this up.

Steps 1: Get the license for the PA-220 Firewall. Based on last lab, our firewall can reach internet by doing NAT translation and make the policies to allow traffic to reach internet. First, we need to get license for download software and get URL database update. We did this by changing the Palo alto Update Server and service route.

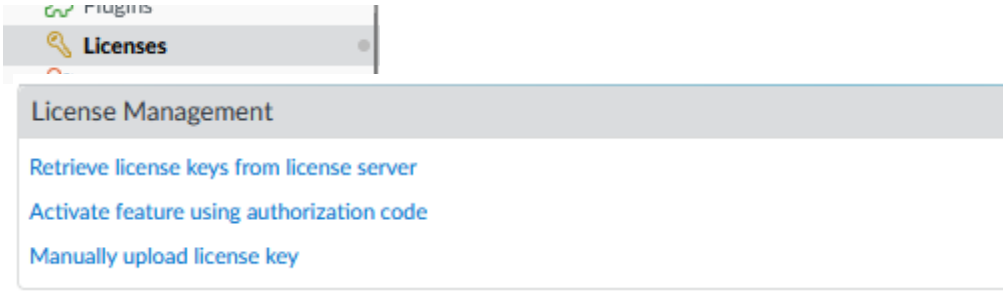
We access the web GUI by enter the mgt port ip which is 192.168.1.20, we can do it by changing our host IP to 192.168.1.0/24 subnets. Then, we can change the Update Server to staticupdate.paloaltonetworks.com by going to device than set up, this is the only server that we tested can get license from. Then we changed the DNS to 1.1.1.1 which is the DNS server that hosted by Cloudflare. After that we changed the DNS, Palo alto update, URL update route using the LAN port which is 192.168.2.0/24 instead of the MGT port. We clicked Service Route Configuration to change it.



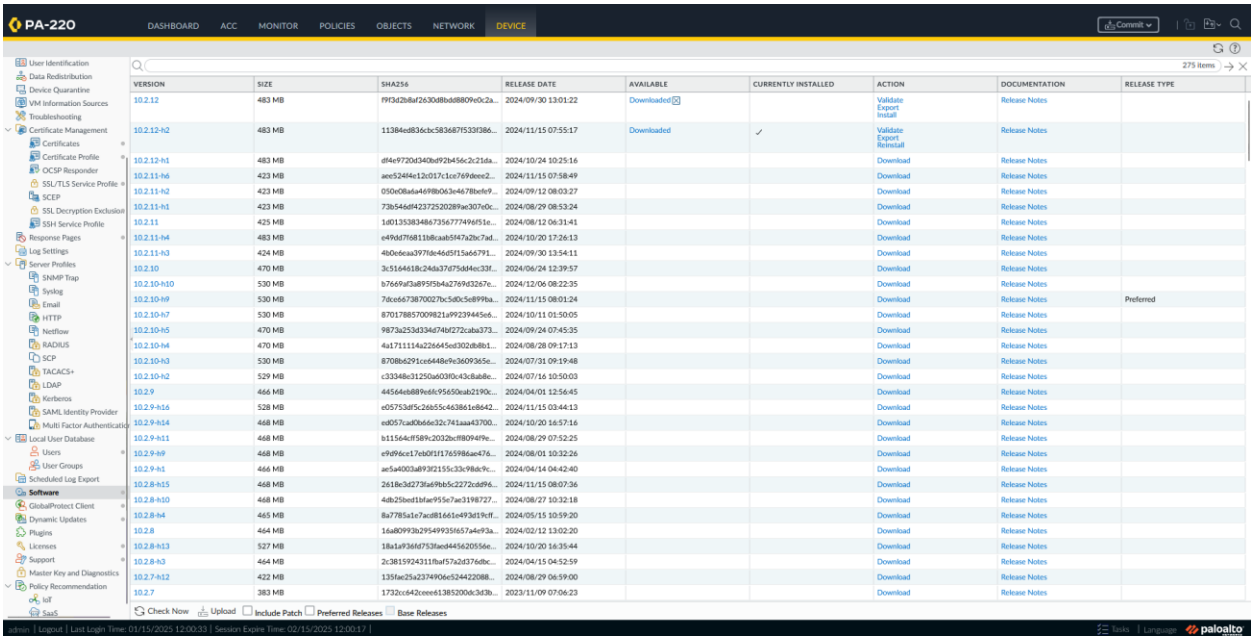
Then we find DNS, Palo alto update, URL update and change it to LAN port



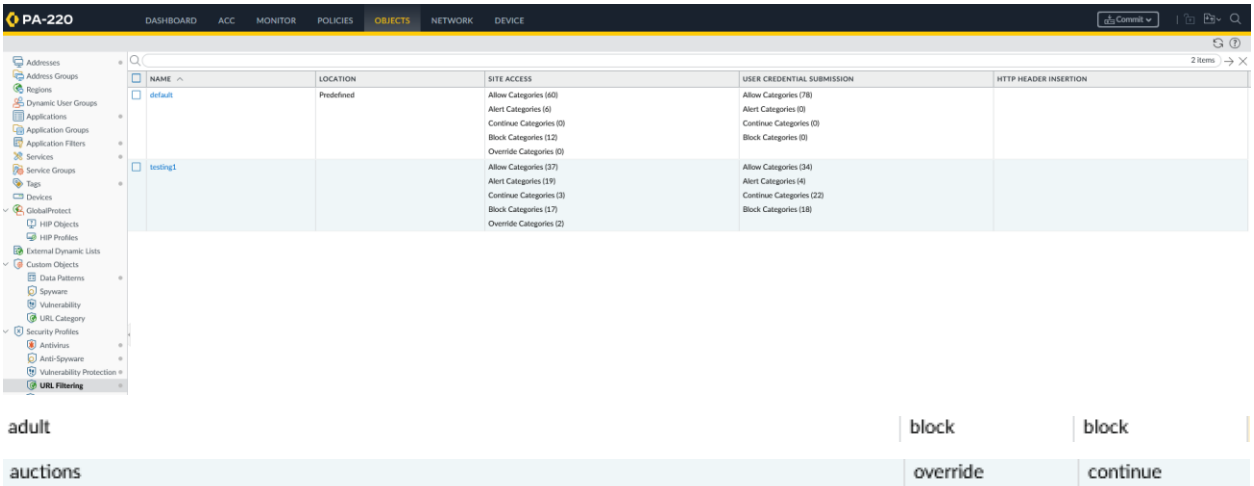
Steps 2: get license by going to license page and click retrieve license key from license server by clicking license tab.



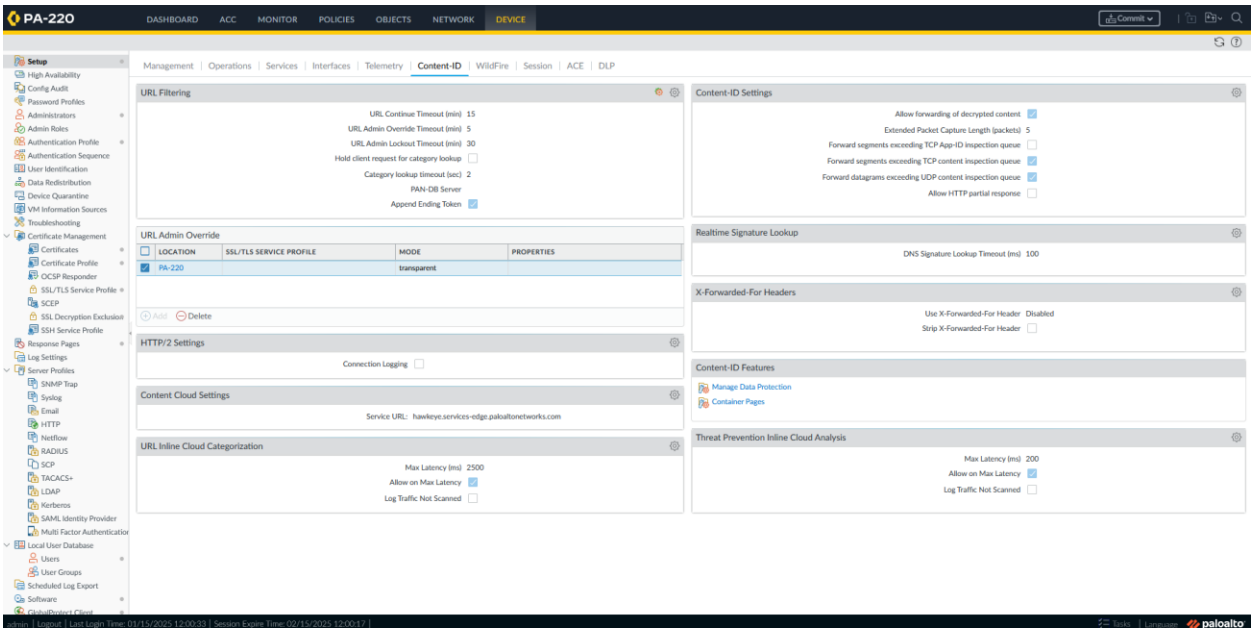
Steps 3: Download and install the software version 10.2.12-h2, first go to software tab, then uncheck preferred release and base release, then download and install 10.2.12.



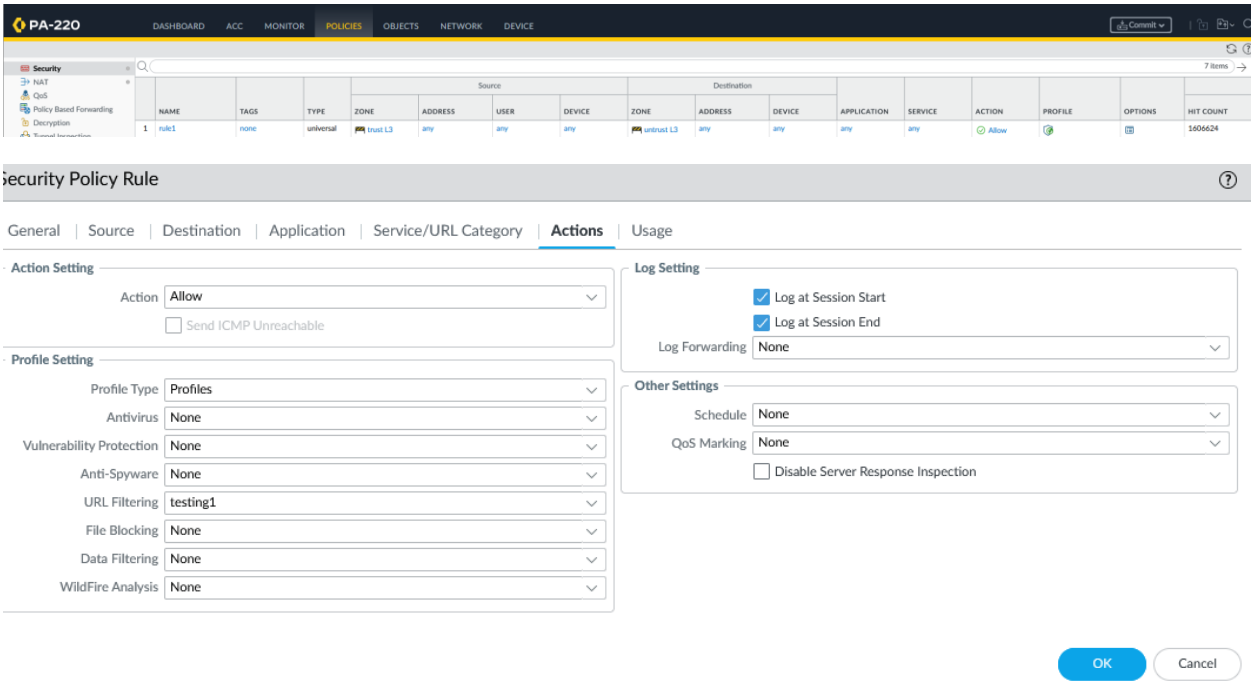
Steps 4: Create or duplicate the URL filter and change the category you want to override or block, first go to object than click URL filtering, then you can create a new filtering or duplicate the default one, then go to the category you want to block and override then change it. That are four option that you can choose including allow, that allow user to that access category without any logs, second one is alert, it allow user to access that category but with log, third one is continue, it create a page that ask user do they want to continue to the site, the last one is override, it allow user to access that category when they entered the password. The last one is blocked, it doesn't allow user to reach any website that is that category and generate a log for it.



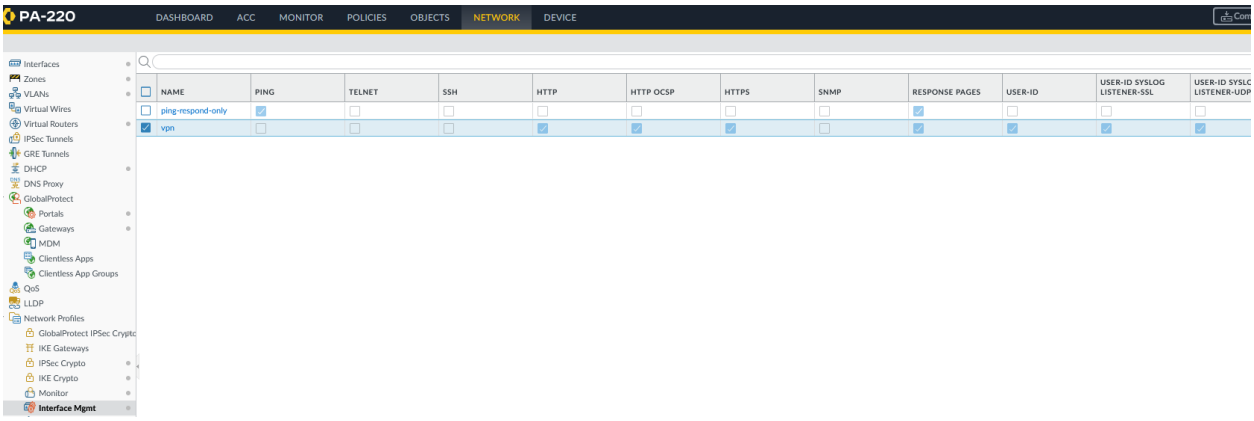
Steps 5: Add password to admin override, you can change the admin override password the anything you want by going back to device tag, then click content-id, you can add URL admin override and set the mode to transparent.

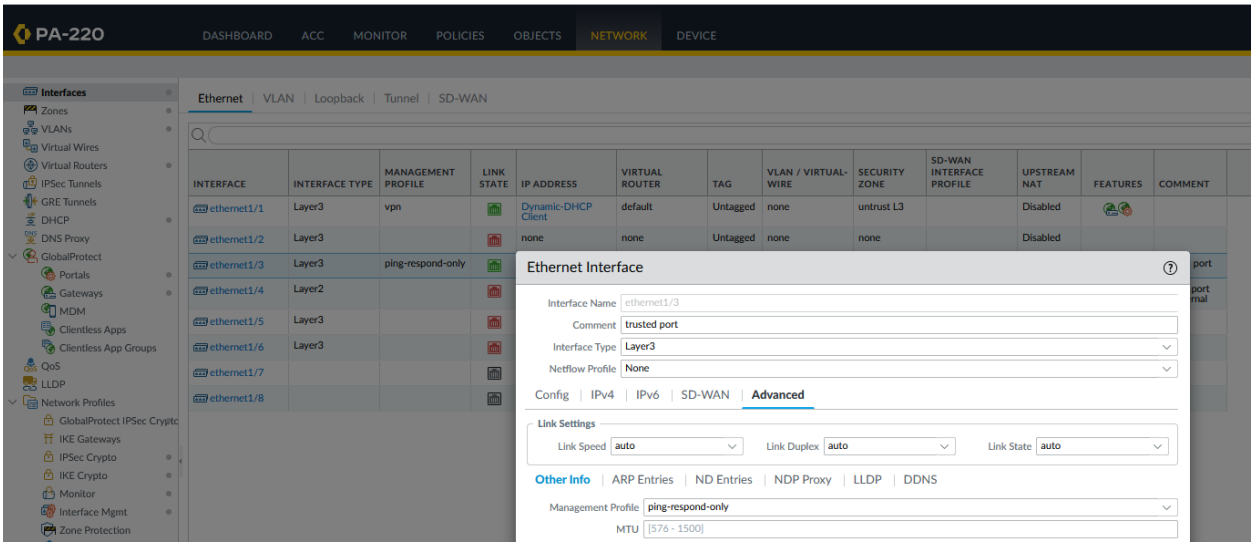


Steps 6: You need to add the URL filter list to the security rule that make your internal to reach internet then click on it, go to action tab, change profile types to profiles and add your URL filtering.

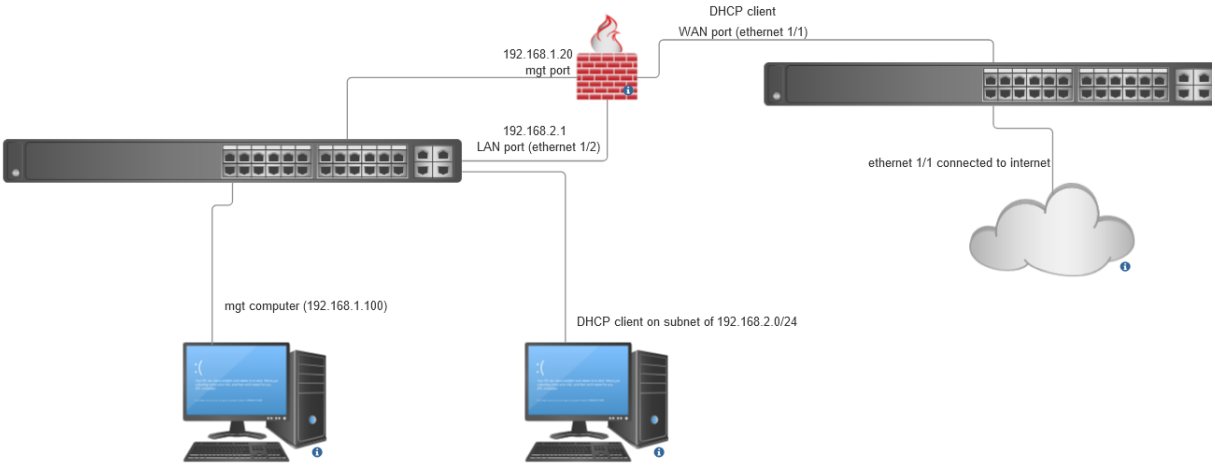


Steps 7: create a mgt profile that allow response page and all it to Lan interface, go to network than interface mgt and create the new profile, you need to check the response page, than go back to interface and click on your LAN interface and go to advanced than you can add the profile that you created.





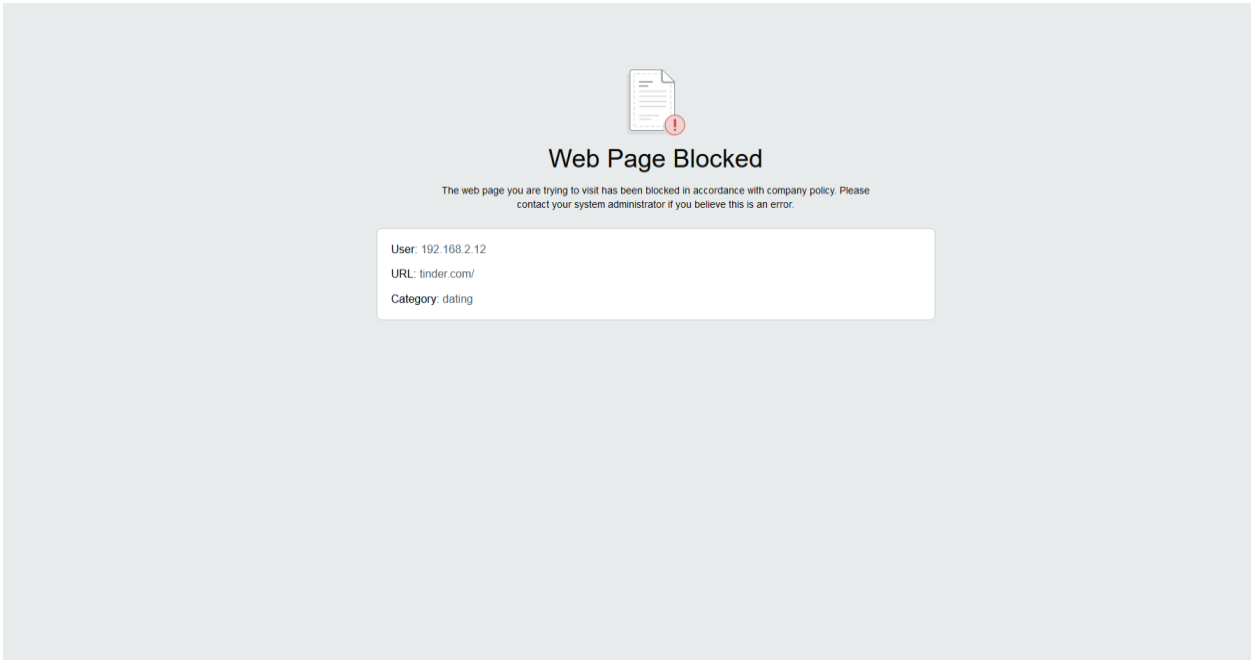
Network diagram:

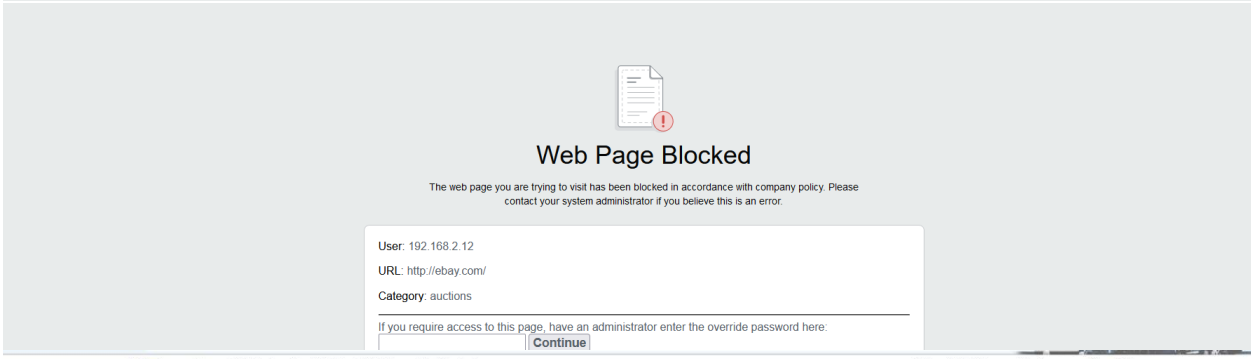


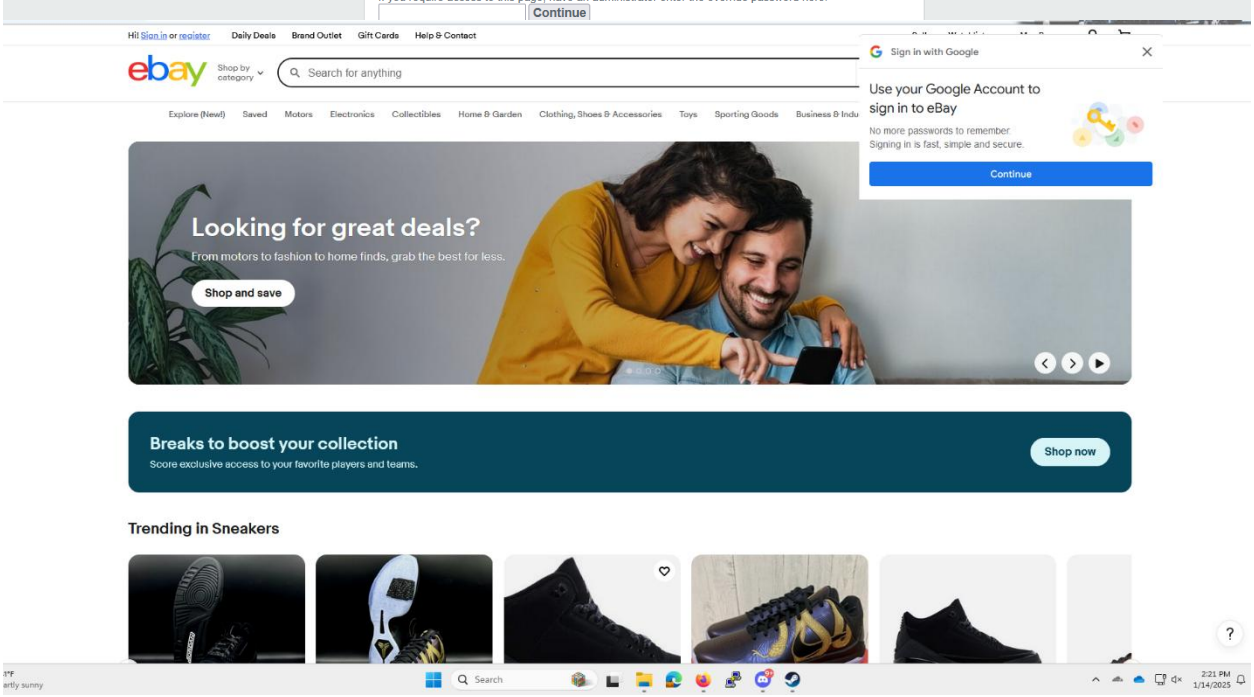
Problems: In this lab, we only faced two problem the first one is we don't know what mode to use to admin override, there is two mode you can select, we used redirect at the beginning but it not working, we fix this by asking other people that finished the lab. The second problem is the response page don't load up when we requesting the website that we override it, we fix this issue by searching YouTube and find out we need to clear our cookie before we try it.

Conclusion: In this lab, we learned how to get license for PA-220 and learned how to set up URL filtering and setting up URL admin override, one main problem that we spent more time on is find out which URL override mode we need to use and how to make the response page show up. We also learned more about how PA-220 works and how to configure it to fulfilled the requirement of a elementary school

Result of URL filtering and override:







GlobalProtect VPN Lab

By Alvin Chow

Purpose: In this lab, we learned how to set up global protect VPN, it is a secure way that allow user to connect to internal firewall network by creating a tunnel with IPSEC encryption. During this lab, we learned about how to configure GlobalProtect portal and gateway, setting up user authentication. We learned more about IPSEC encryption, which can ensure data that transmitted between user device and internal network remain private.

Background info: The Palo Alto Networks® PA-220 next-generation firewall is designed for small organizations or branch offices. This firewall included passive cooling to reduce noise and power consumption, eight Ethernet ports, and dual power adapters for power redundancy. The PA-220 firewall enables to secure the organization through advanced visibility and control of applications, users, and content.

Palo Alto Networks (Palo Alto) provides cybersecurity services to enterprises, government, and service providers. This company's products and services portfolio include firewall and software, panorama, support and maintenance services, security management solutions, and virtual system upgrades.

GlobalProtect is a VPN solution offered by Palo Alto Networks that provides secure remote access to an organization's internal network. It uses IPsec encryption to create a secure tunnel between a user's device and the corporate network, ensuring that sensitive data is protected while transmitted over the internet. It can be configured through the Palo Alto Networks firewall, it has integration with existing security policies. This VPN solution is designed to support remote work by ensuring secure access to internal resources from anywhere.

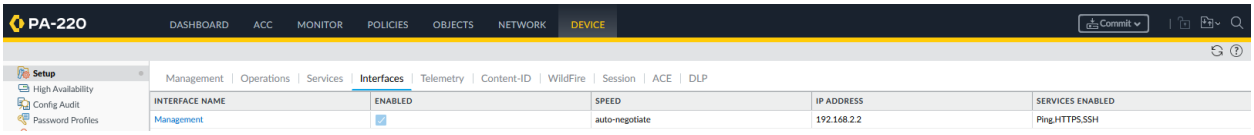
A **VPN (Virtual Private Network)** is a technology that creates a secure, encrypted connection over a public network, it allows users to access a private network remotely. By extending a private network across a public network, a VPN enables devices to send and receive data like they were directly connected to the private network, it can protect the data from potential threats. It provides key features like encryption to secure sensitive information, and remote access for employees or users to connect securely to internal networks.

I**Psec (Internet Protocol Security)** is a suite of protocols designed to secure communications over an IP network by encrypting and authenticating data exchanged between devices, such as routers, firewalls, or VPN gateways. Operating at the network layer, IPsec ensures the confidentiality, integrity, and authenticity of data. It achieves this through encryption to protect data from unauthorized access and authentication to verify the identity of communicating devices and maintain data integrity. IPsec can operate in two modes: **Transport Mode**, where only the data payload is encrypted, and **Tunnel Mode**,

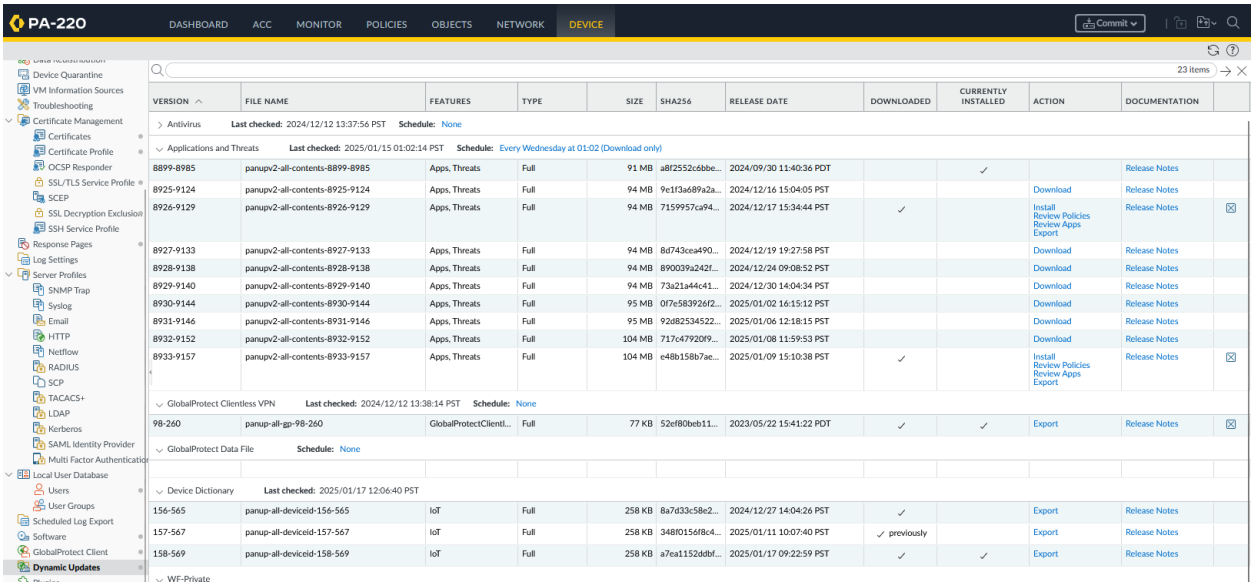
where the entire IP packet, including the header, is encrypted and encapsulated. This make IPSEC is often use in VPN service.

Lab summary: Steps by Steps guide how to setup GlobalProtect.

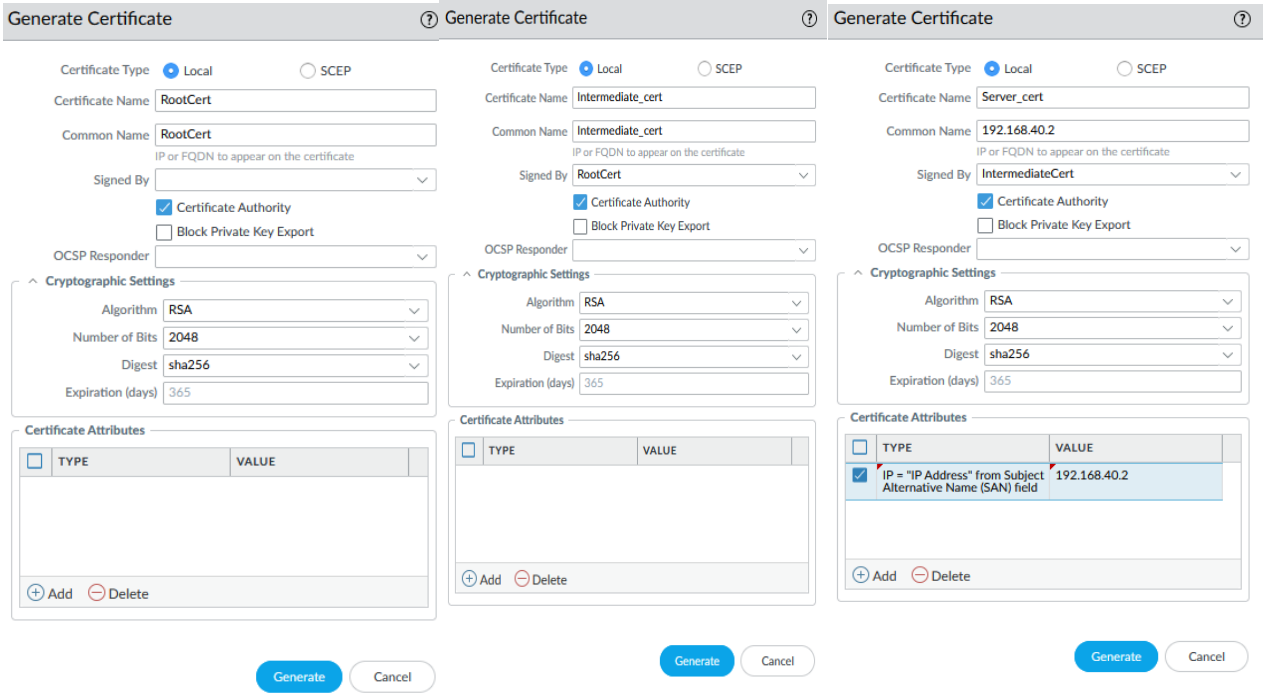
Steps 1: Before we do anything, we changed our mgt port from 192.168.1.0/24 network to 192.168.2.0/24 network, this can allow DHCP client can easily access management GUI by typing 192.168.2.2. We changed it by going to device, setup, interface than click on management and change the IP address and default gateway.



Steps 2: download and install global protect to the firewall. Based on last name we already got the license for the firewall to set up URL filtering, so we only need to download and install GlobalProtect Clientless VPN at device, dynamic updates, than click download, wait for it to download, then click install

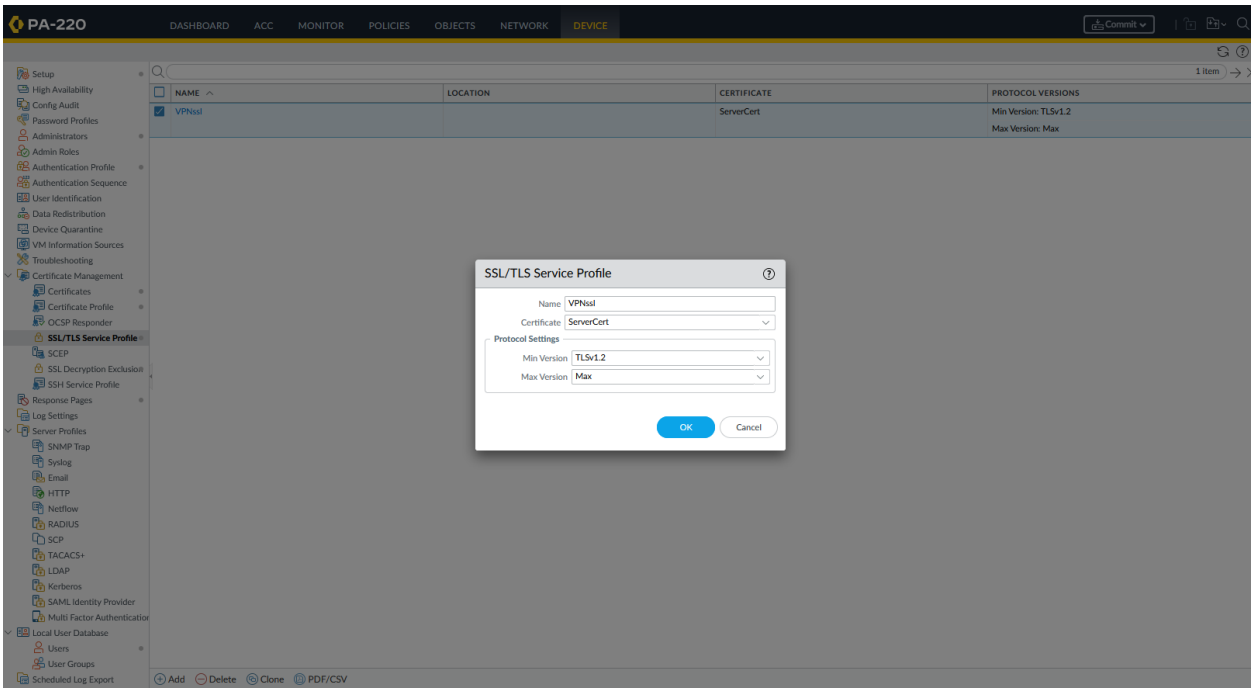


Steps 3: create certificate for firewall, first go to device, then certificates, we need to make 3 certificate, the first one is RootCert, second one is Intermediate Cert, last one is Server Cert, we create the Certificate like this

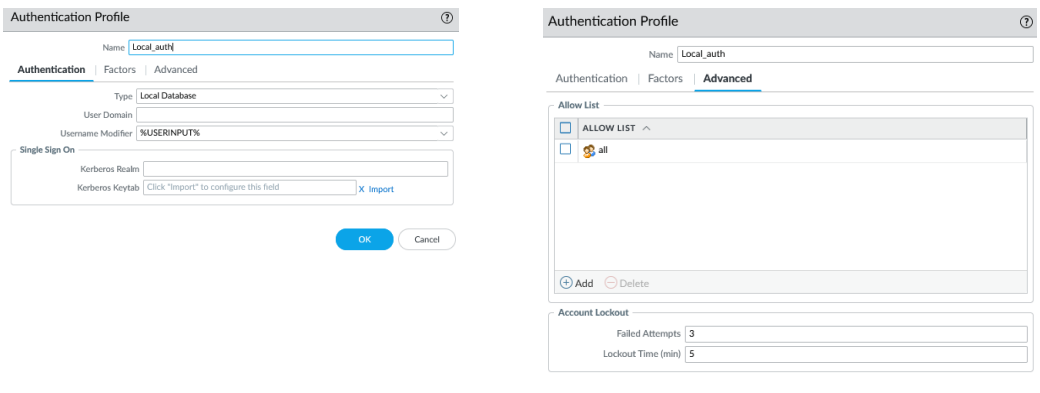


For Server Cert, you need to use your Wan port for the Common Name and certificate Attributes.

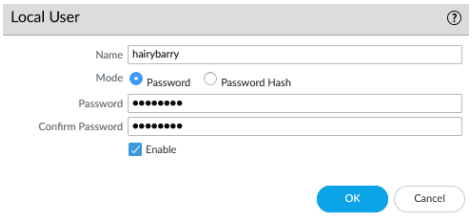
Steps 4: Then You need to create SSL/TLS service profile, you can create it at Device, then click SSL/TLS Service Profile, after that click add, name can be any name you want, Certificate you need to use your Server Cert, you can use any version for it.



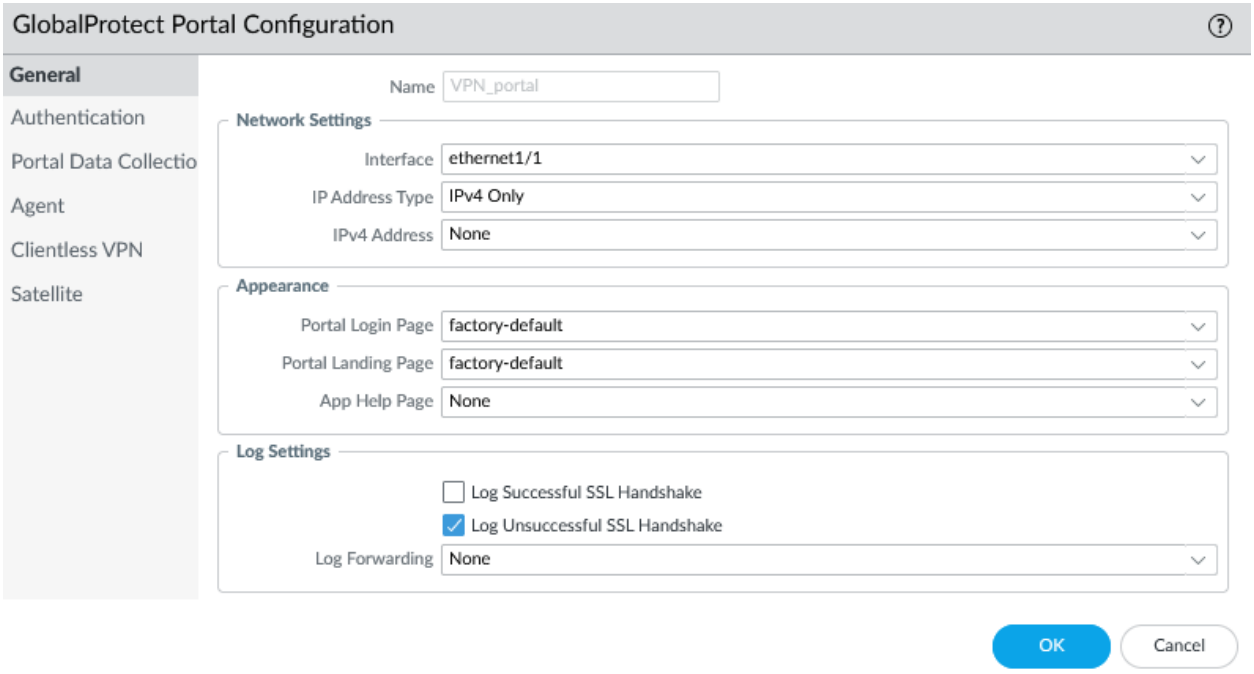
Steps 5: You need to create a new authentication profile, you can name it any name, but authentication type need to be local Database and the advanced allow list need to be all.



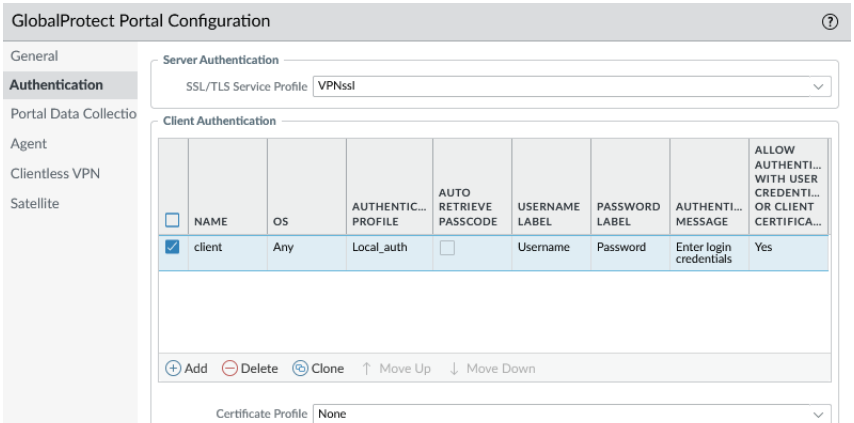
Steps 6: go to Users than create a new local user, the name is the username you want to be and the password is the password you can remember and use it later.



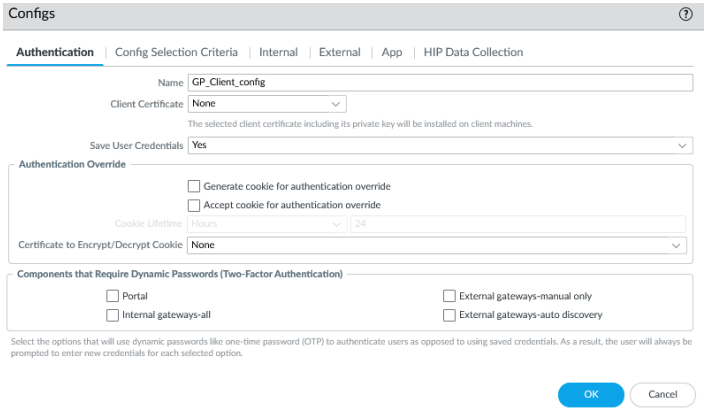
Steps 7: You need to create a new portal, first go to device, then find portals and click on it, you need to create a new portal by clicking add at bottom left corner, you can name is whatever you want, interface need to using you WAN interface, address type is IPV4 only, than for the IPV4 address, if you have static ipv4 address you can use it, if not just leave it None.

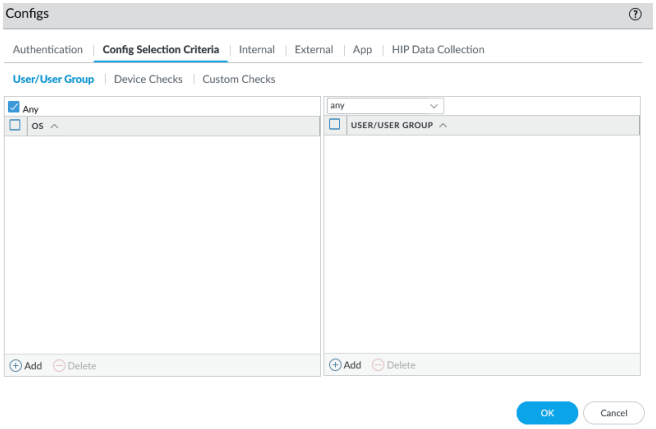


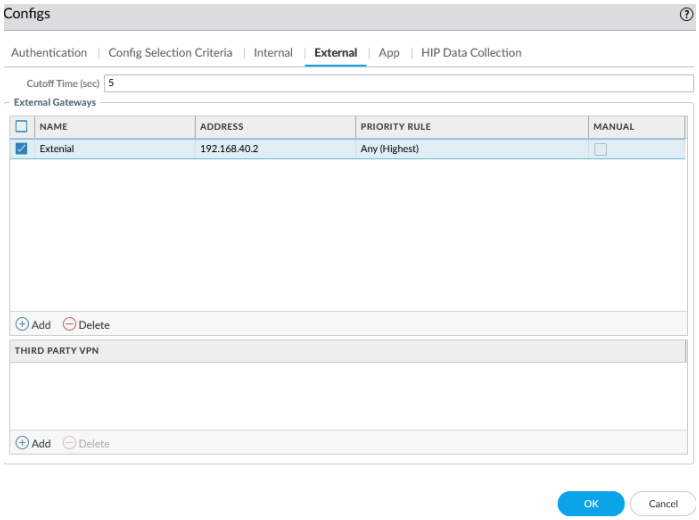
Steps 8: Than go to authentication tab, use the SSL/TLS Service Profile, you created before, than add new client Authentication, use any name you want, authentication use the one you created before, than change the Allow authentication with User Credentials or Client Certificate to Yes.

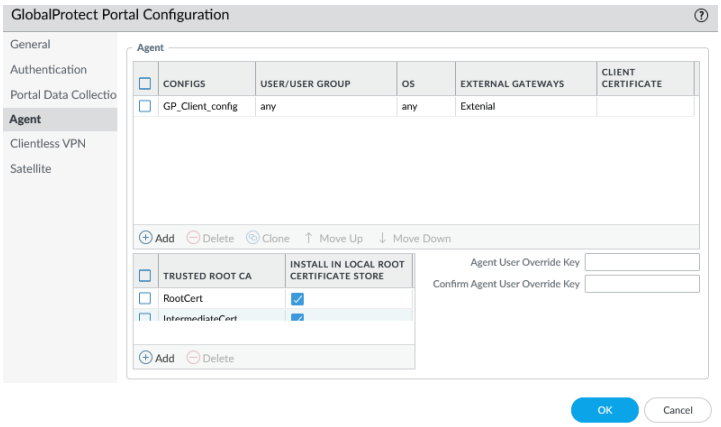


Steps 9: Go to Agent tab, create a new agent, name whatever you want, go to config selection Criteria, click Any OS, go the external, create new external Gateway, name is whatever you want, set the address to be your WAN port and priority Rule is Any. Then you need to add Trusted Root CA, first one is RootCert, the second one is Intermediate Cert, and you need to click checked on Install In Local Root Certifciate Store.

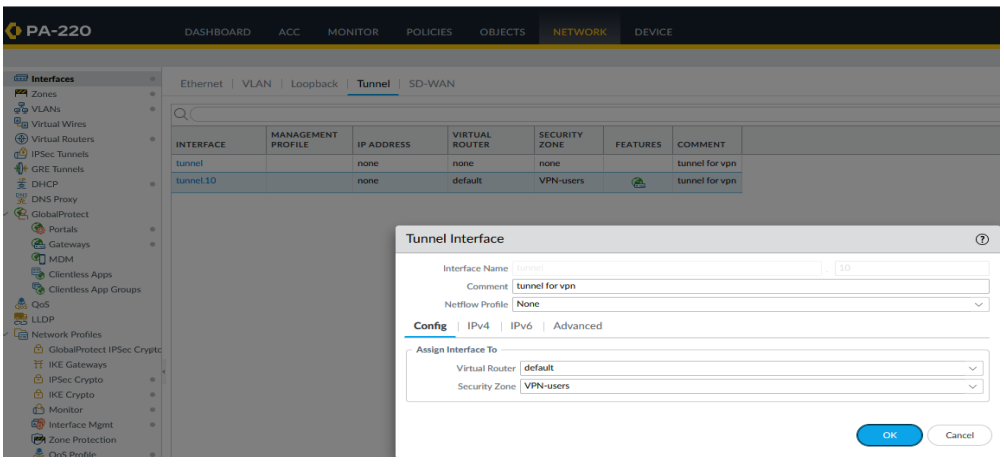




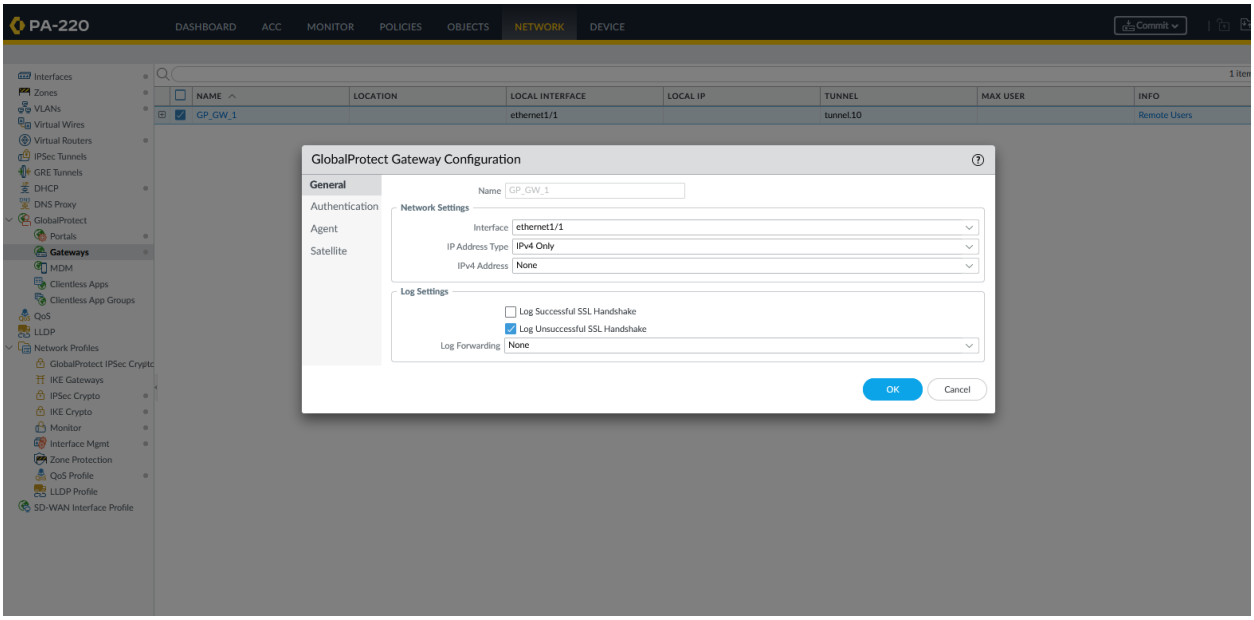




Steps 10: Before we set up the gateway go back to network, interface, then click on Tunnel, add two, you can just leave the first tunnel and the second tunnel you can name is tunnel.10, then assign interface to default virtual Router and create a new security Zone called VPN user.

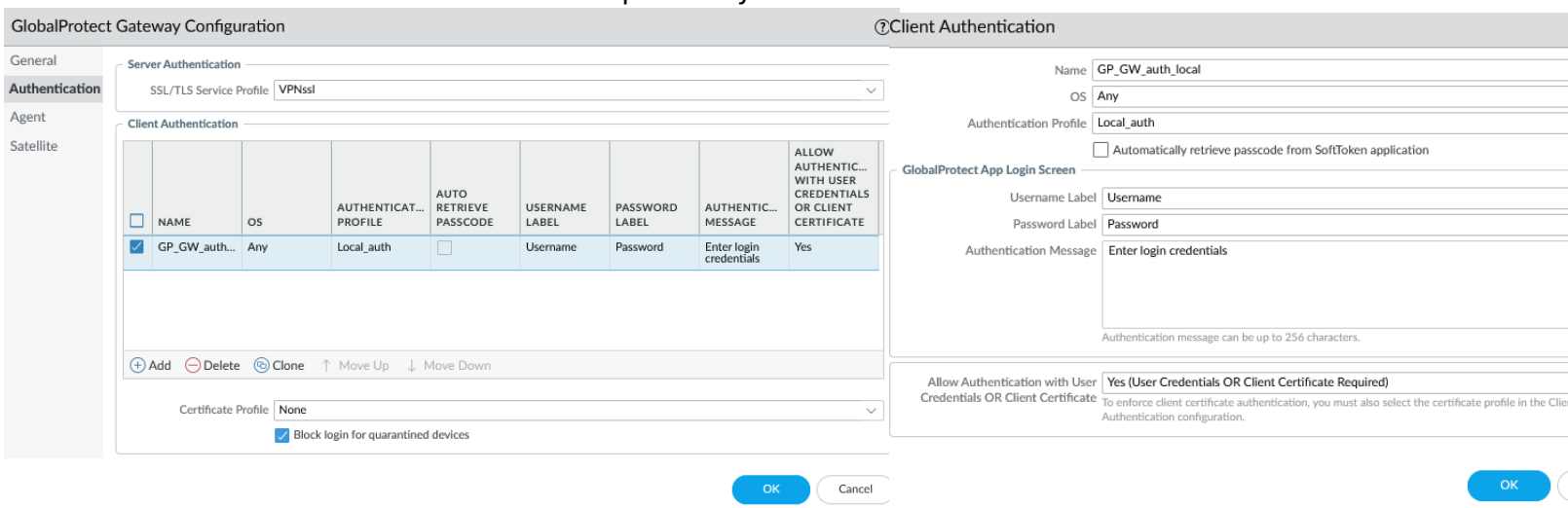


Steps 11: Then click on global protect Gateways, add the new gateway and name it, you need to use your WAN interface for it, if you have static WAN port ip, you can use your static on the ipv4 address

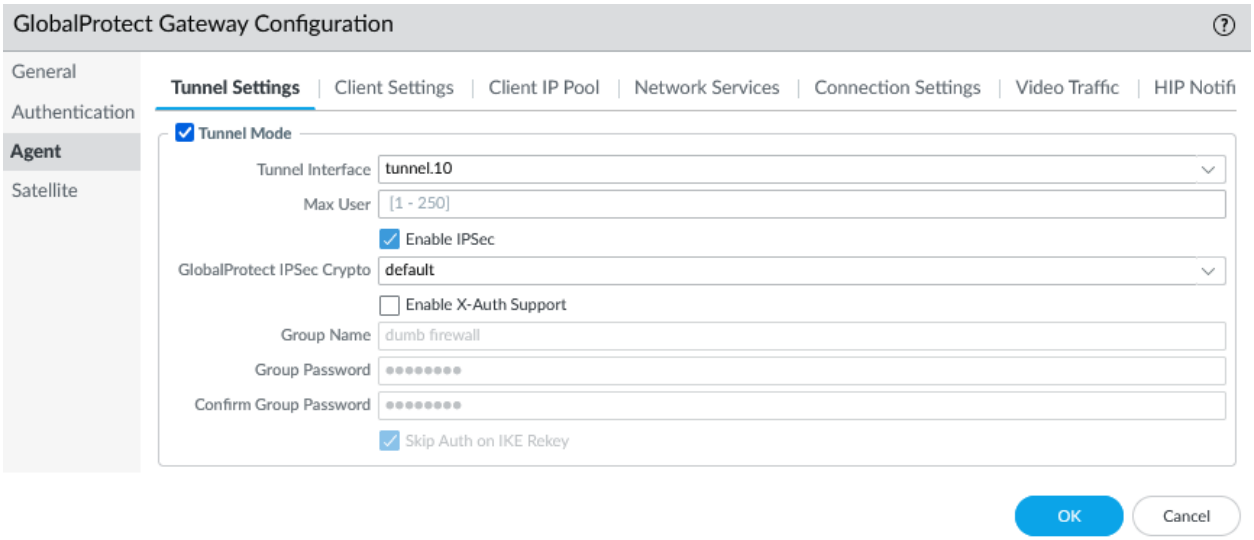


Steps 12:

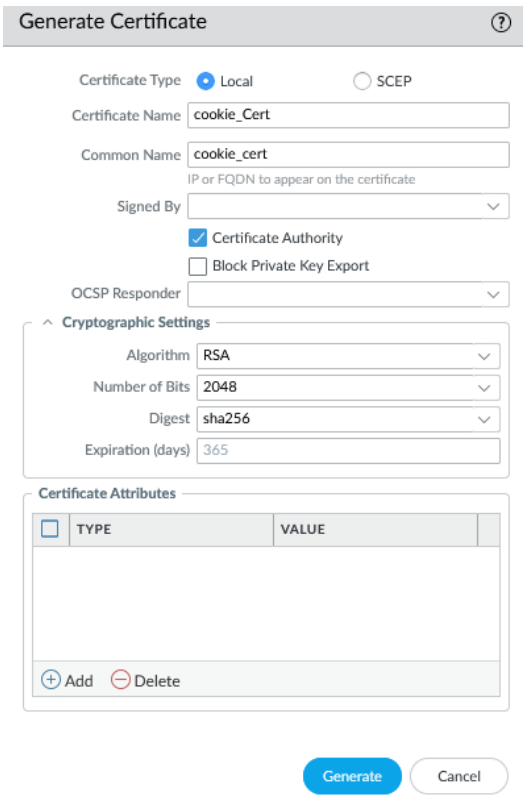
Click on authentication tab, use the SSL/TLS Service profile than you created, then add new client authentication, name is whatever you want, OS need to be any, use the authentication profile that you created before and change the allow authication with user credential OR client Certificate required to yes.

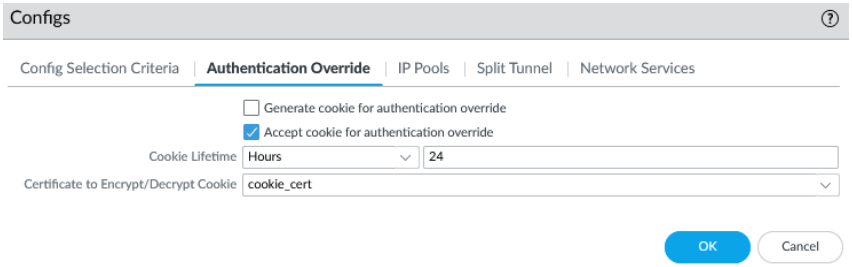


Steps 13: click on agent, then tunnel settings, enable tunnel mode, use the tunnel.10 to be your tunnel interface, enable IPSec, it can give you extra security.

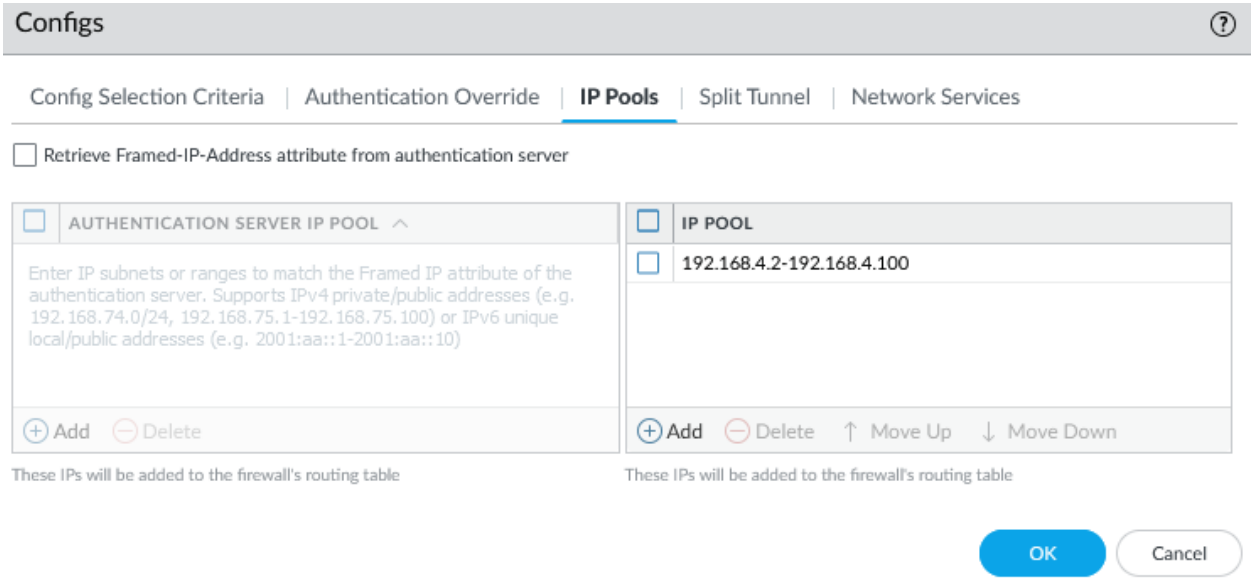


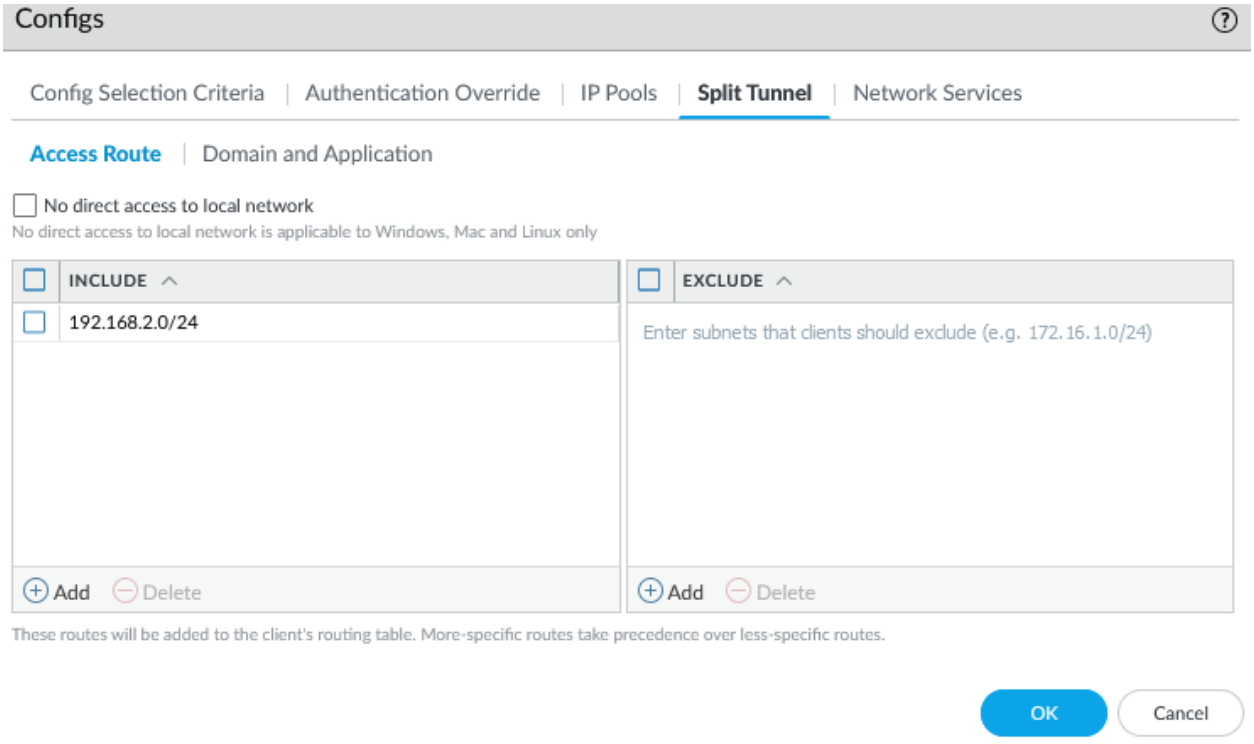
Steps 14: click on client settings, then create a new configs, name is whatever you want, click on any OS. Than go to authentication override tab, click on accept cookie, and create new certificate to Encrypt/Decrypt cookie, use any name for certificate name and common name than click on Certificate authority.





Steps 15: click on IP Pools, make the ip range that you want to use for your VPN users. Then click on split Tunnel enter 0.0.0.0/0 which is all the traffic from vpn user will go to vpn first or only enter the internal subnet of your firewall.



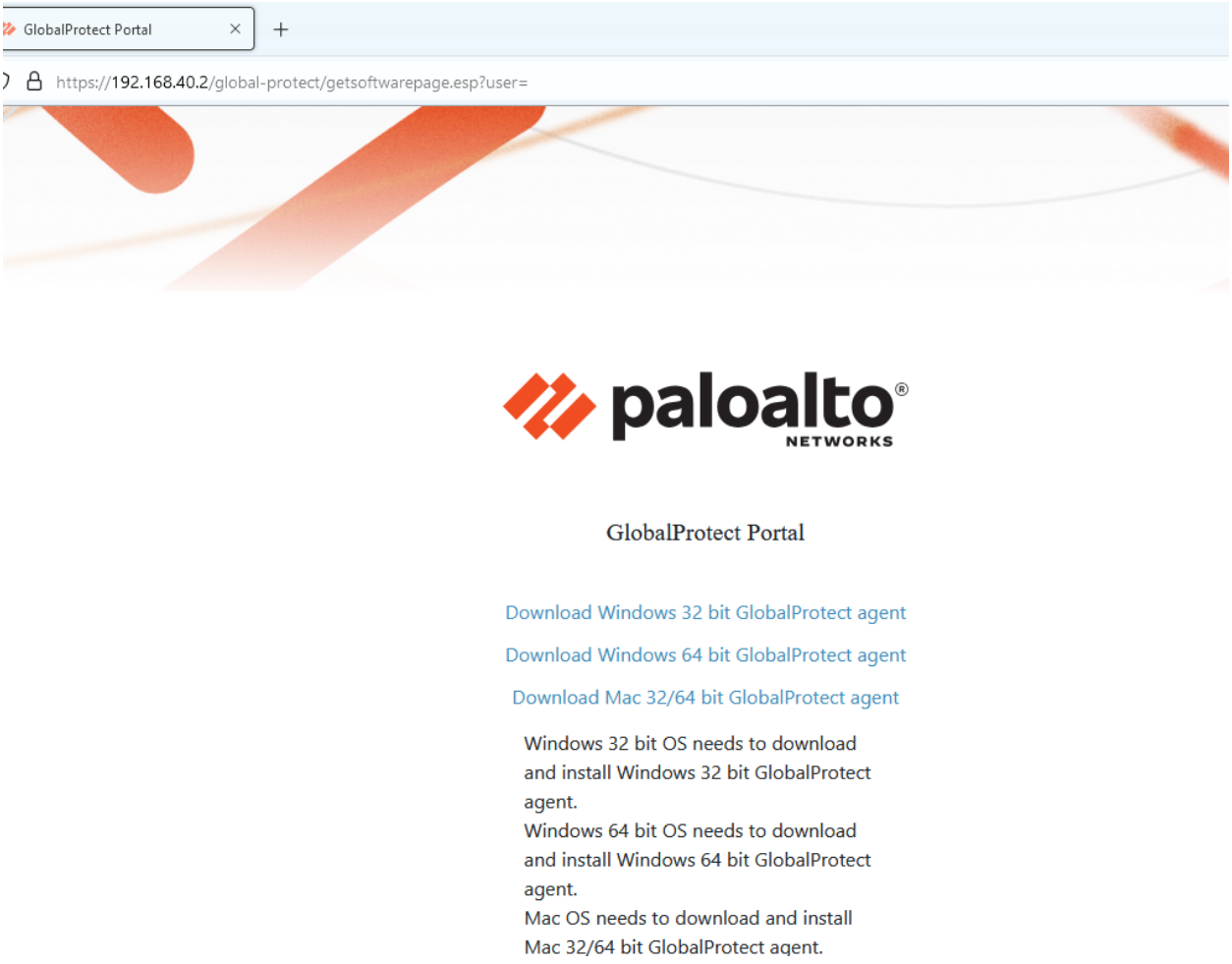


Steps 16: click on policies, than security create 3 new rule like this, the first on is allow VPN user to untrust which can send back the traffic outside the firewall network, the second one is VPN to internal, and the last one is allow portal traffic from untrust L3 to VPN users zone.

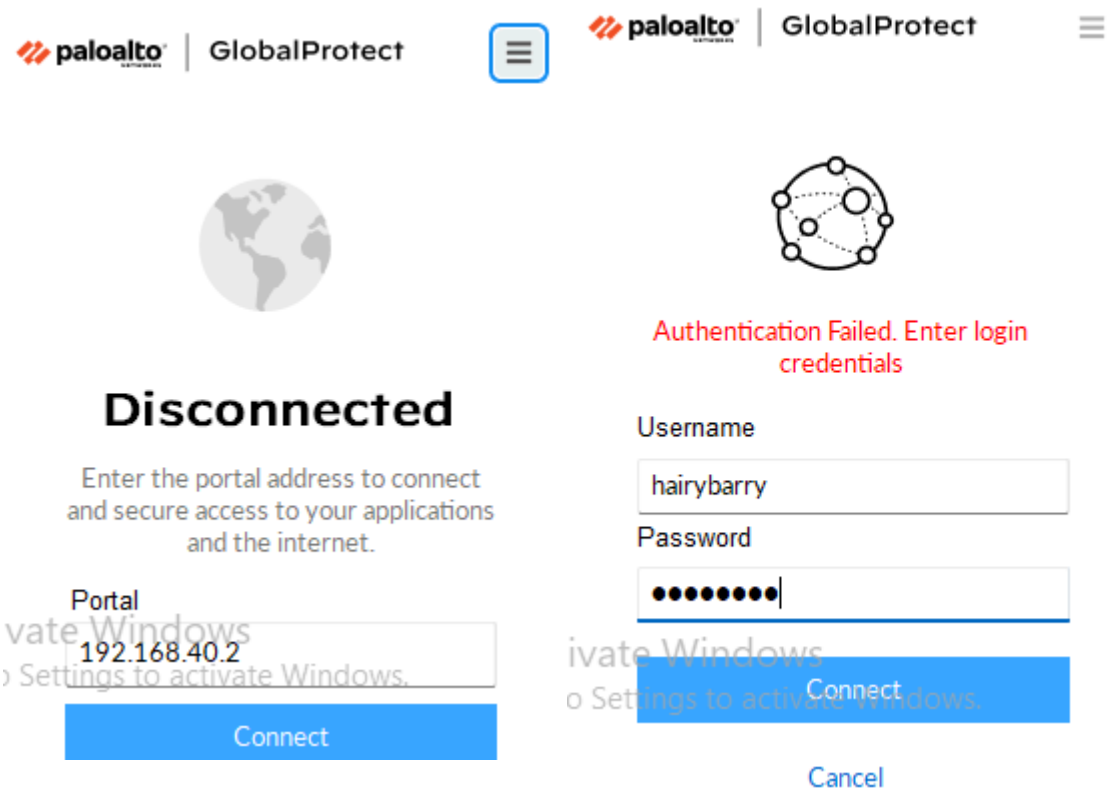
2	vpn_to_trust	none	universal	VPN-users	any	any	any	untrust L3	any	any	any	any	Allow	none
3	vpn_to_internal	none	universal	VPN-users	any	any	any	trust L3	any	any	any	any	Allow	none
4	allow_portal_traffic	none	universal	untrust L3	any	any	any	VPN-users	any	any	any	any	Allow	none

Steps 17: click on NAT, add the VPN user to source zone is allow the VPN traffic Nat and go back to VPN user.

Steps 18: go to your wan interface ip on browser than enter your WAN ip, it should show like this, click download depends on your system.

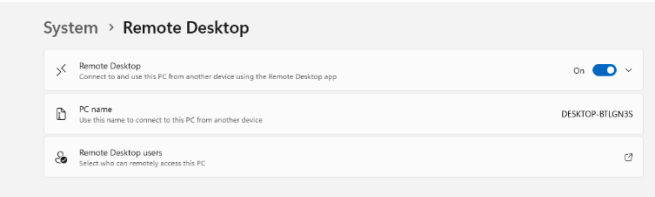


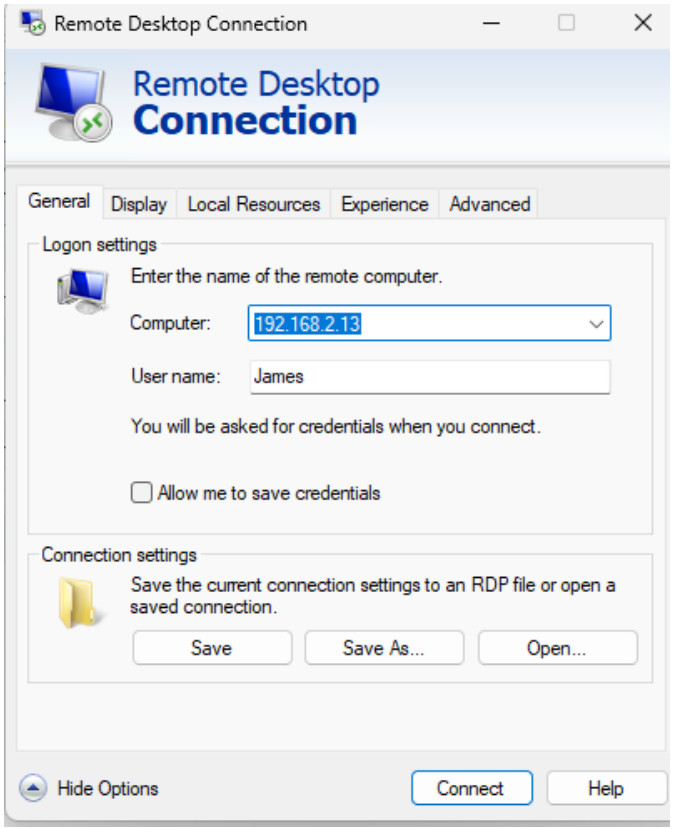
Steps 19: enter your wan ip, enter the username and password that you set on authentication profile and click connect. If you config correctly, it should working.



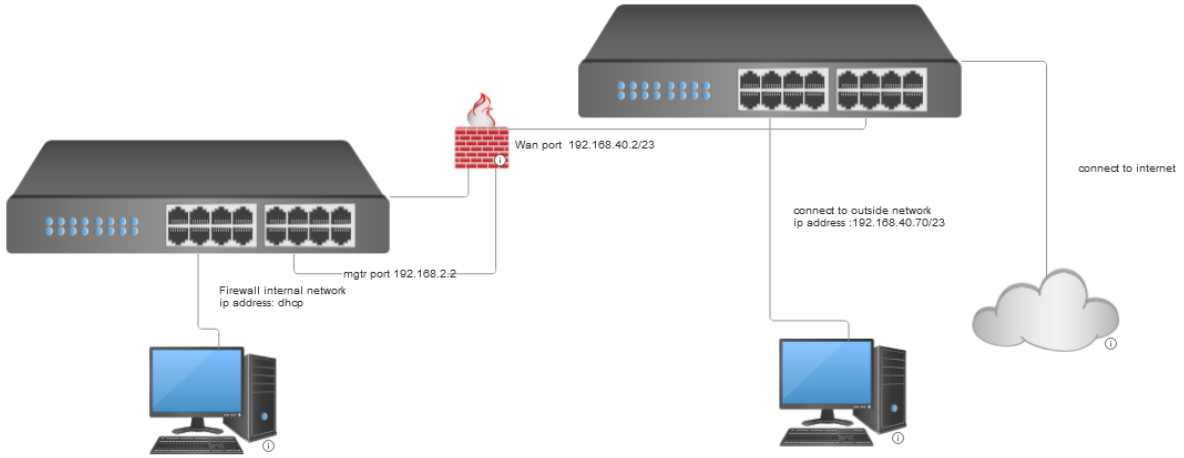
Steps 20: enable remote desktop on setting, go to setting, then remote desktop tab, enable it.

Then go to remote desktop application enter the internal ip address for your target computer and the username, then click connect





Network diagram:



Problems: We only faced one big problem, it is we don't know which interface should be the outside network to connect, we find it out by try and face some error then one classmate told us need to be on the 192.168.40.0/23 network.

Conclusion: In this lab, we learned how to set up global protect VPN by configuring global protect portal with gateway, then we learned how to use window remote desktop, which sometime can be useful for network management.

Wireshark capture:

```
Data (132 bytes)
    Data […]: ac7629090000706c19cb14ca532b2587b48ee9ae9e14974f7cd7603cbcdcb7c0c5073ab7708a022a
    [Length: 132]
```

346	6.028590	192.168.40.42	96.7.158.104	TLSv1.2	346 Application Data
347	6.050910	96.7.158.104	192.168.40.42	TLSv1.2	1300 Application Data
348	6.059206	192.168.40.42	96.7.158.104	TLSv1.2	346 Application Data
349	6.084981	96.7.158.104	192.168.40.42	TLSv1.2	1300 Application Data

10	0.029279	192.168.4.5	192.168.2.2	TCP	54 64107 → 443 [ACK] Seq=1873 Ack=1447 Win=262400 Len=0
11	0.033480	192.168.4.5	192.168.2.2	TLSv1.2	171 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Messa
12	0.040053	192.168.2.2	192.168.4.5	TLSv1.2	336 New Session Ticket, Change Cipher Spec, Encrypted Handshake Messag
13	0.041592	192.168.4.5	192.168.2.2	TLSv1.2	1083 Application Data
14	0.083069	192.168.2.2	192.168.4.5	TCP	60 443 → 64107 [ACK] Seq=1729 Ack=3019 Win=23168 Len=0
15	0.261836	192.168.2.2	192.168.4.5	TLSv1.2	651 Application Data
16	0.315425	192.168.4.5	192.168.2.2	TCP	54 64107 → 443 [ACK] Seq=3019 Ack=2326 Win=261376 Len=0
17	5.006155	192.168.4.5	192.168.2.2	TLSv1.2	1083 Application Data
18	5.009090	192.168.2.2	192.168.4.5	TCP	60 443 → 64107 [ACK] Seq=2326 Ack=4048 Win=26112 Len=0

AWS lab 1 -3

By Alvin Chow

Purpose: The purpose of those lab provides us hands-on experiences with AWS, which make me understand the core services like EC2, S3, IAM. Those labs also make me understand how to configure, deploy and manage it. By working through tasks like real workplace situations, it can help me prepare for it.

Background Information:

AWS is a leading cloud computing platform that allows businesses and individuals to rent computing resources like servers, storage, and databases over the internet instead of owning physical hardware. It offers flexibility, cost savings, and scalability, letting users pay only for what they use. AWS provides hundreds of tools and services, making it a one-stop solution for hosting websites, running apps, storing data, and more, all managed securely through a web interface.

AWS S3, S3 is AWS's cloud storage service designed to store and retrieve any amount of data, like documents, images, or videos. Think of it as a giant, secure online hard drive. Files are stored in "buckets," and you can control who accesses them using permissions. S3 is popular for hosting static websites, backing up data, or even storing logs. Its durability and accessibility make it a go-to choice for businesses needing reliable storage.

EC2 (Elastic Compute Cloud), EC2 lets you rent virtual servers (called "instances") in the cloud. These servers can run applications, websites, or software, just like a physical computer. You choose the operating system, memory, and CPU, and you can scale up or down instantly to handle traffic spikes. EC2 is ideal for tasks like hosting a web app, running simulations, or testing software without buying expensive hardware.

IAM(Identity and Access Management, IAM is AWS's security service for managing who or *what* can access resources in your AWS account. It lets you create users, groups, and roles, for example, developer and user assign fine-grained permissions for example, Allow read-only access to S3. Security features include multi-factor authentication (MFA), password policies, and temporary credentials for third-party apps.

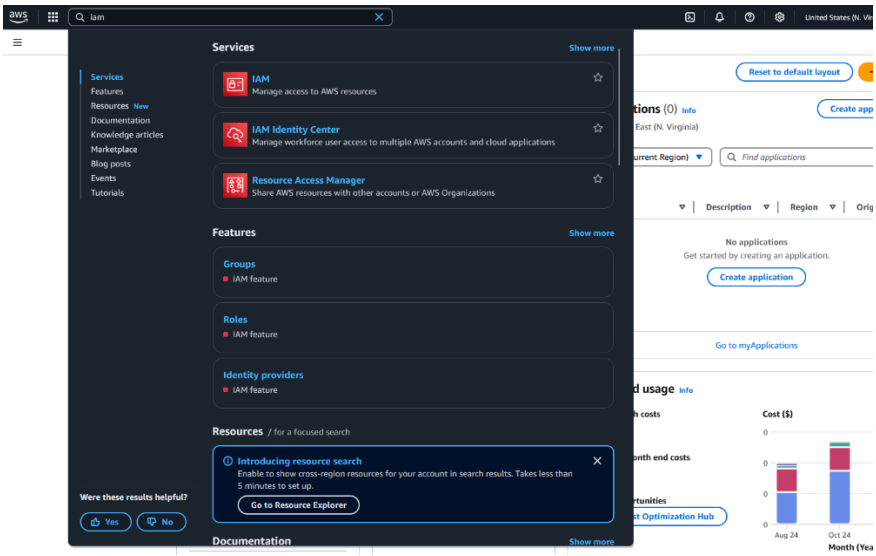
VPC(Virtual Private Cloud),VPC lets you create a private, isolated network within AWS, similar to a traditional data center but in the cloud. You define subnets (public/private), route tables, and firewalls to control traffic flow. For example, you might place a database in a private subnet and a web server in a public subnet. VPC also supports VPN connections to link your AWS cloud with other servers, it also has tools like NAT gateways for secure internet access. By isolating resources, VPC adds layers of security and compliance, critical for sensitive workloads.

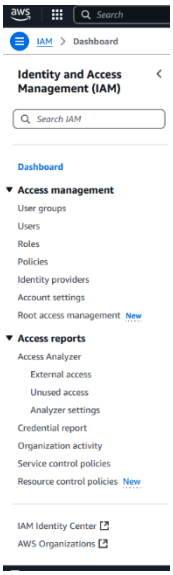
Lab summary: Step by step guide of lab 1-3

Lab 1:

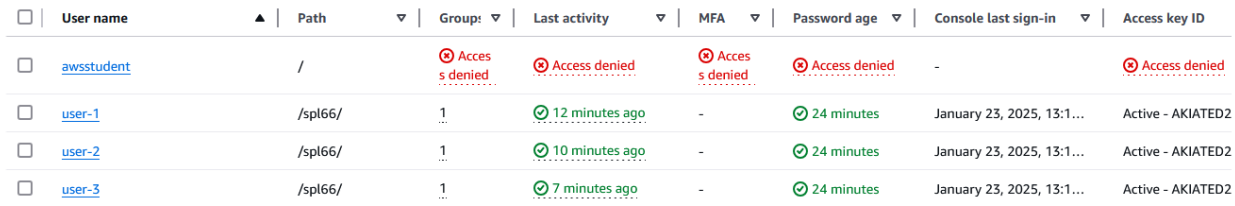
Steps 1: Click on start Lab to start to Lab and wait it turn green, then click on the link of AWS ▶ Start Lab AWS

Steps 2: In the search box, search for IAM to open IAM console, then click on users



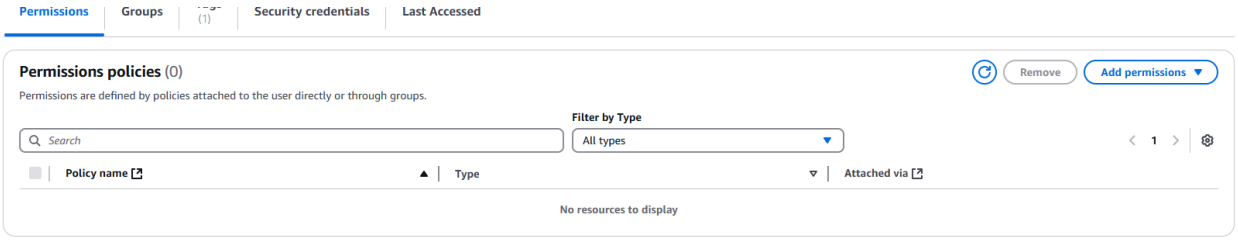


Steps 3: check is there 3 users created, then click on user 1

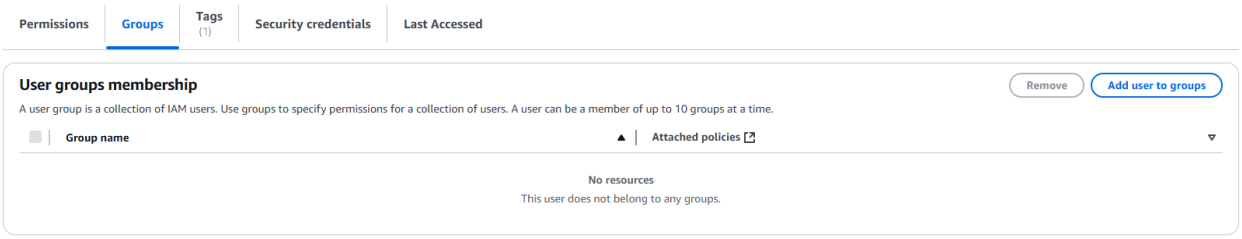


User name	Path	Groups	Last activity	MFA	Password age	Console last sign-in	Access key ID
awsstudent	/	Access denied	Access denied	Access denied	Access denied	-	Access denied
user-1	/spl66/	1	12 minutes ago	-	24 minutes	January 23, 2025, 13:1...	Active - AKIATED2
user-2	/spl66/	1	10 minutes ago	-	24 minutes	January 23, 2025, 13:1...	Active - AKIATED2
user-3	/spl66/	1	7 minutes ago	-	24 minutes	January 23, 2025, 13:1...	Active - AKIATED2

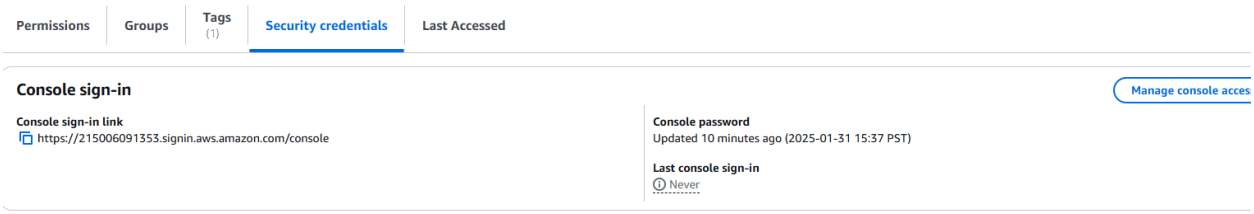
Steps 4: you can see there are no permissions for users 1



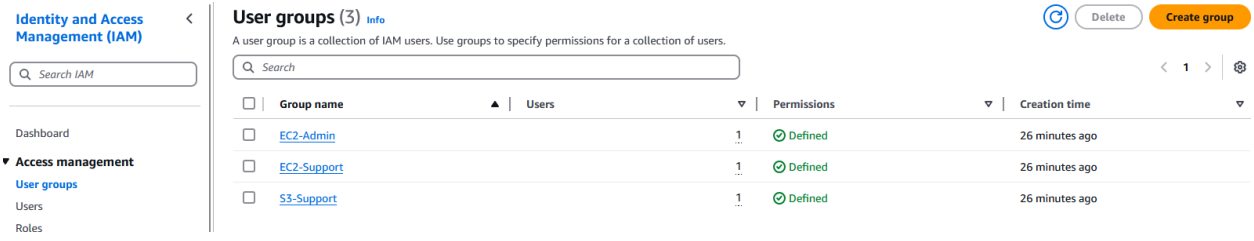
Steps 5: click on Groups tab, you can see user 1 is not in any group



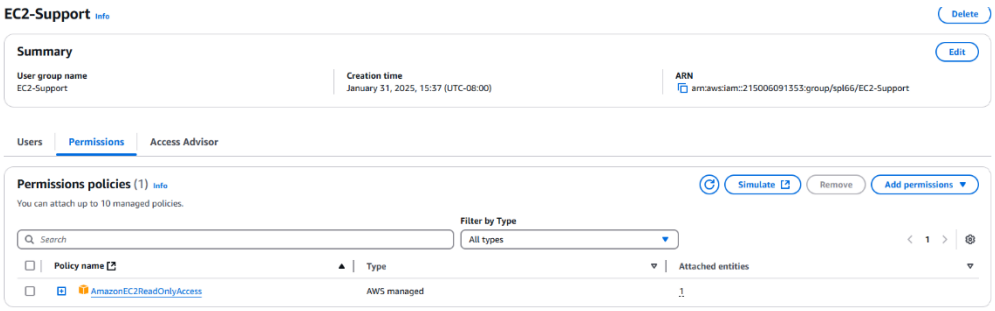
Steps 6: click on Security credentials and see user one is assigned a Console password



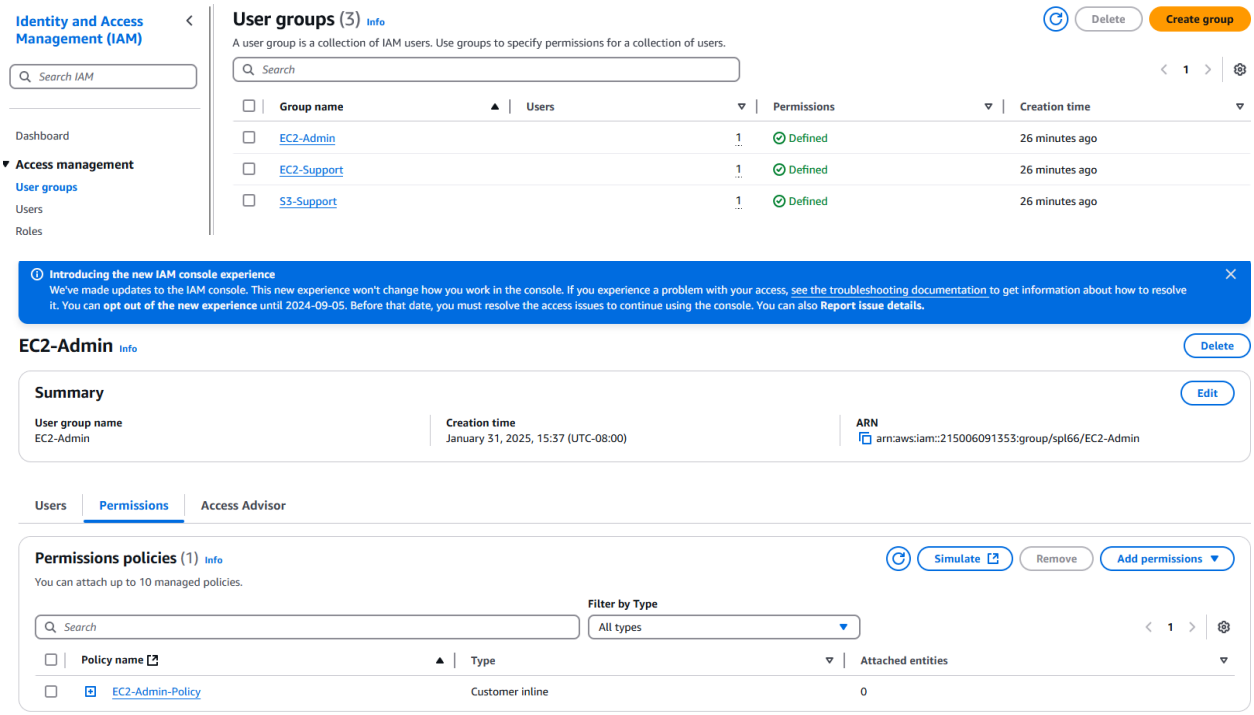
Steps 7: click on User groups, then you should see there are 3 user groups already created, then click on the EC2-Support group link



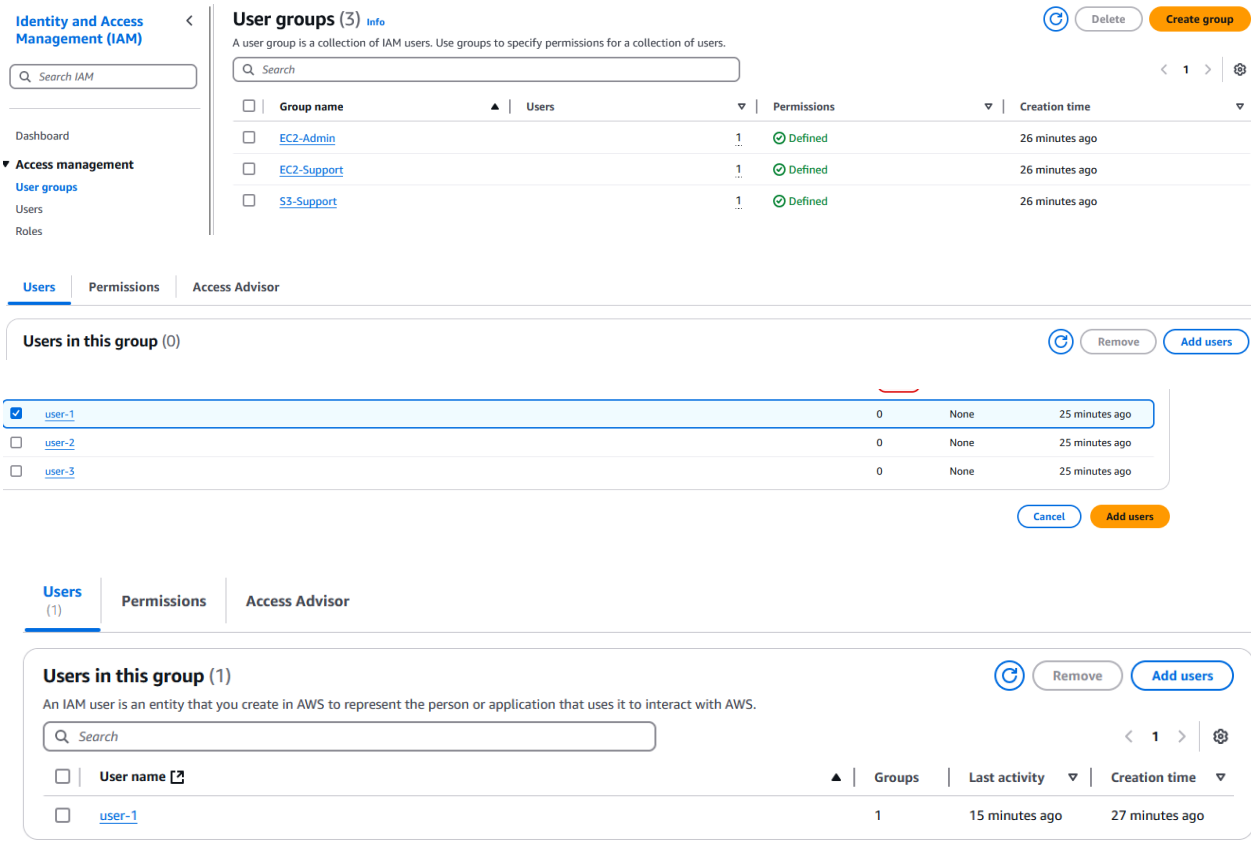
Steps 8: After you clicked on the EC2-Support, then click on Permission, you should see the AmazonEC2ReadOnlyAccess, then click on the plus button to see more detail of the permissions.



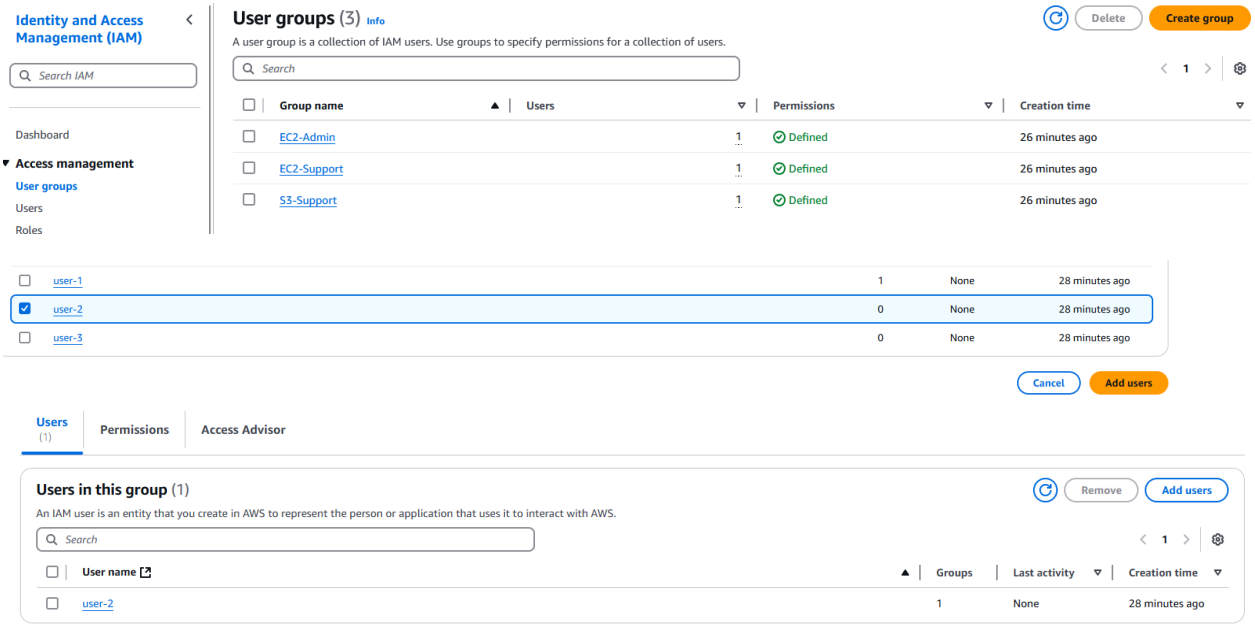
Steps 9: go back to User groups, then click on EC2-Admin link to check the permissions there



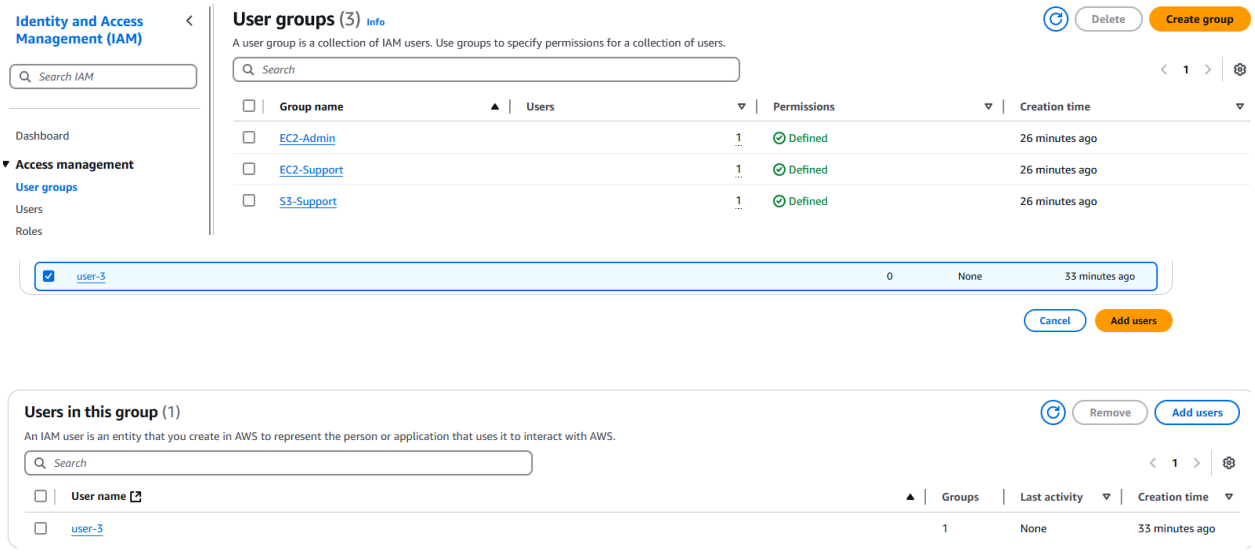
Steps 10: go back to user group, choose S3-support, then click add user, check on user-1 than click add user, and you should see user-1 added to this group



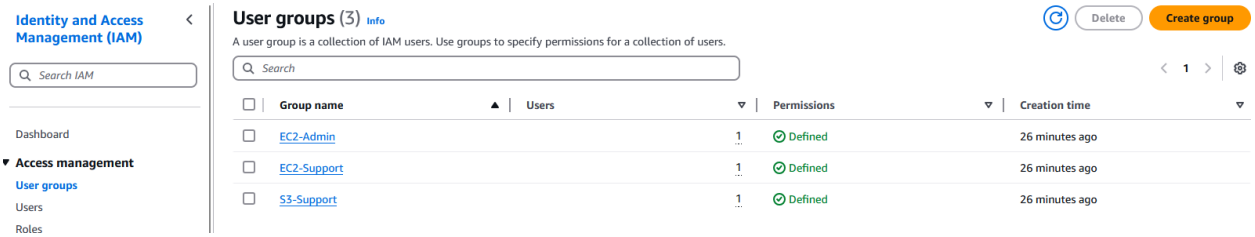
Steps 11: go back to user group click on EC2-support, click add user than add user 2 to that group, then user 2 should be in EC2-support group



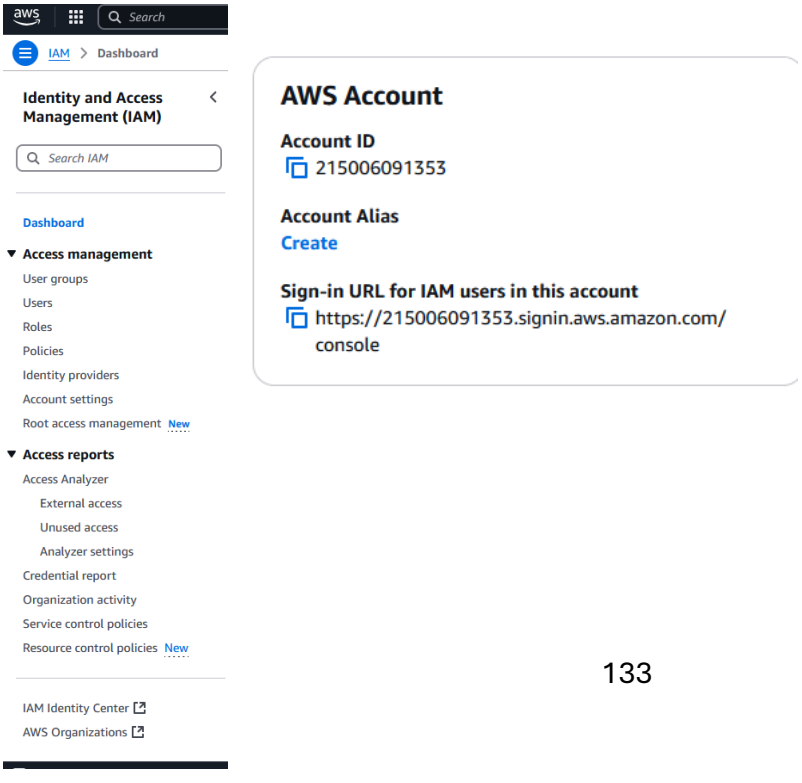
Steps 12: add user 3 to the EC2-Admin Group, go back to user group click on EC2-admin, click add user than add user 3 to that group, then user 3 should be in EC2-admin group



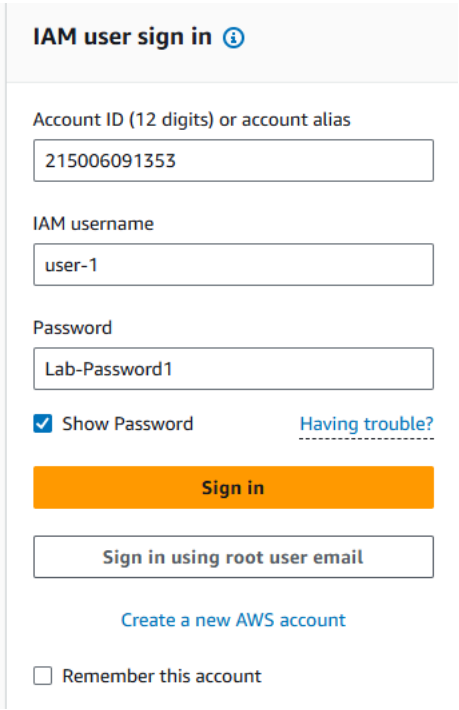
Steps 13: go back to user group, you should see each group with one user in that group.



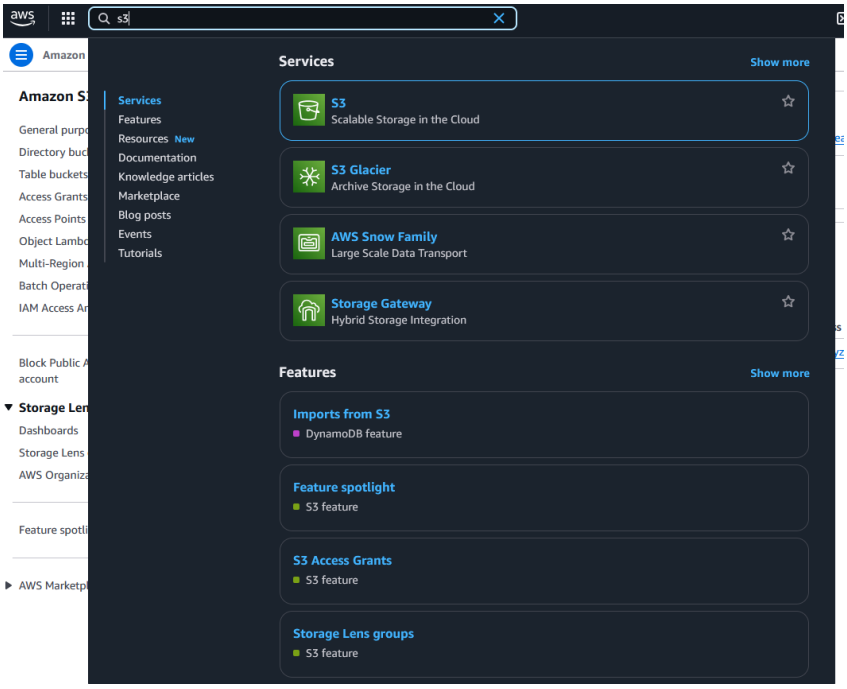
Steps 14: click on IAM dashboard and you should see this, copy the url of the sign-in URL for IAM users in this account

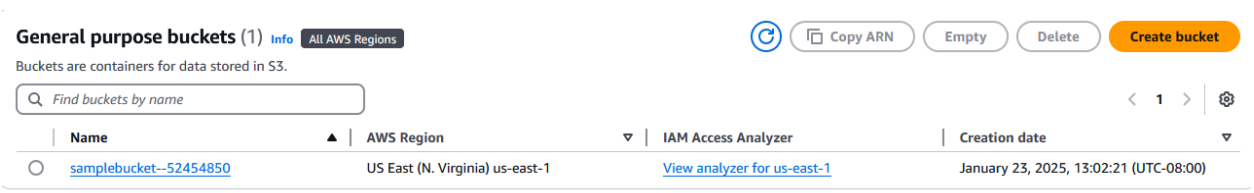


Steps 15: User-1 sign in, paste the link that you copied and login as user 1

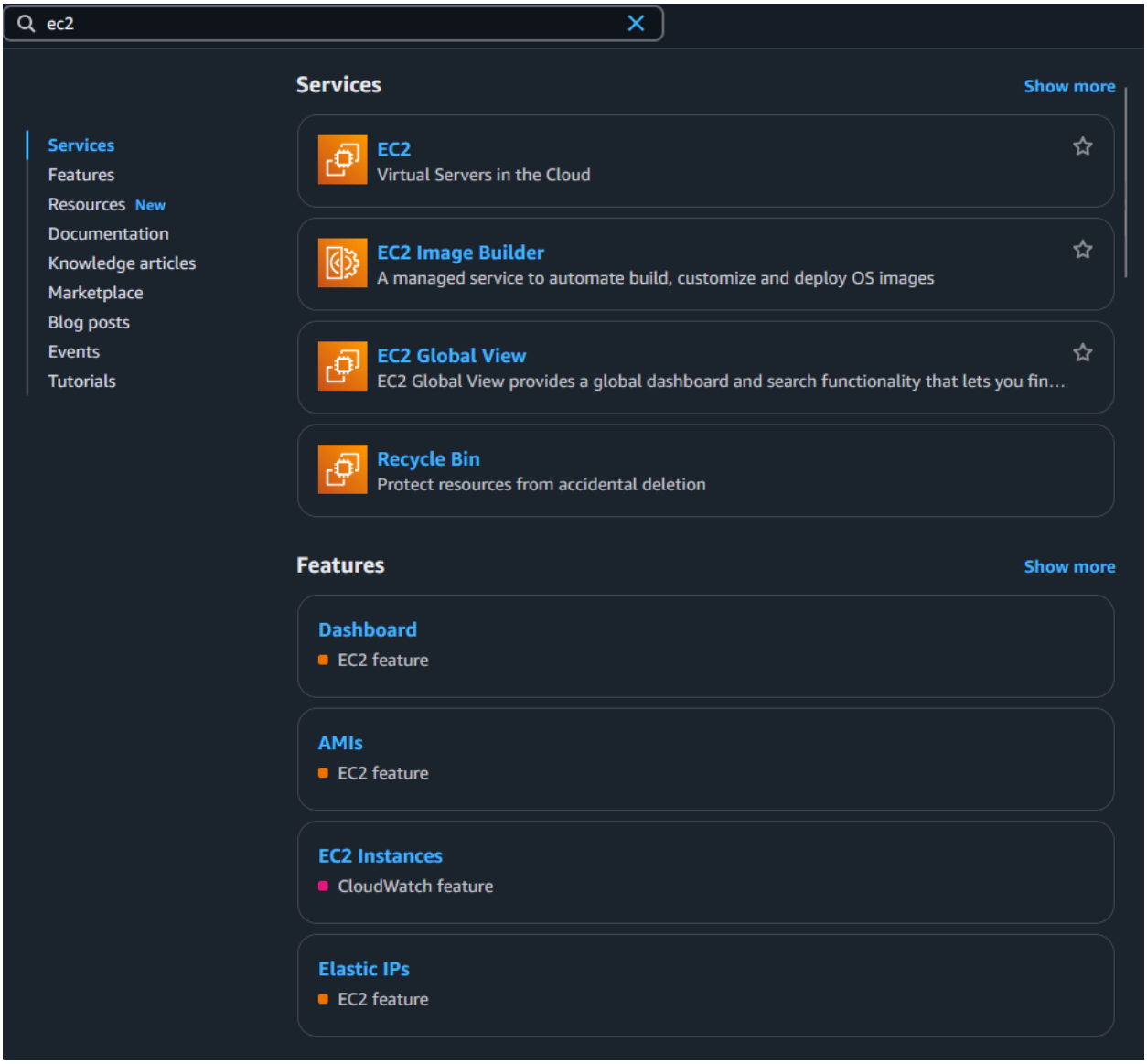


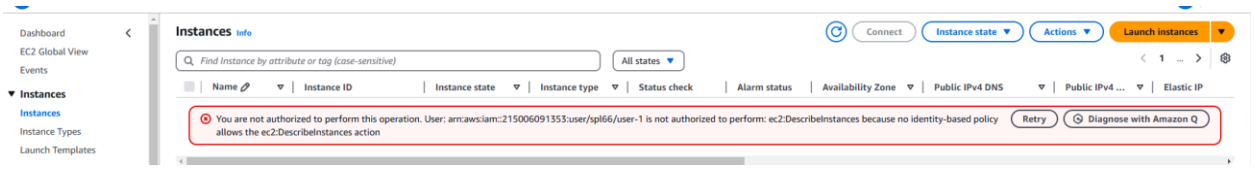
Steps 16: search up S3 and should see the Bucket because user1 added to the group that can view the buckets



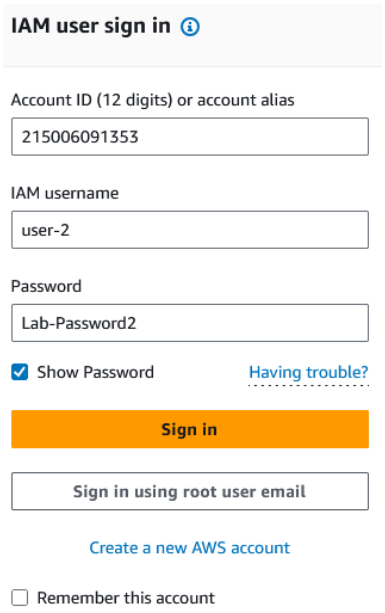


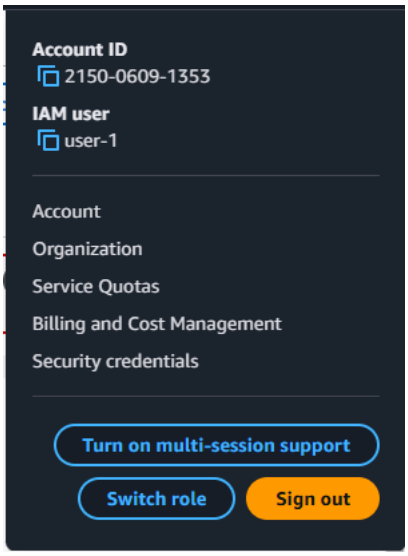
Steps 17: go to EC2 dashboard than click on instances, should see the message are not authorized to view the instances



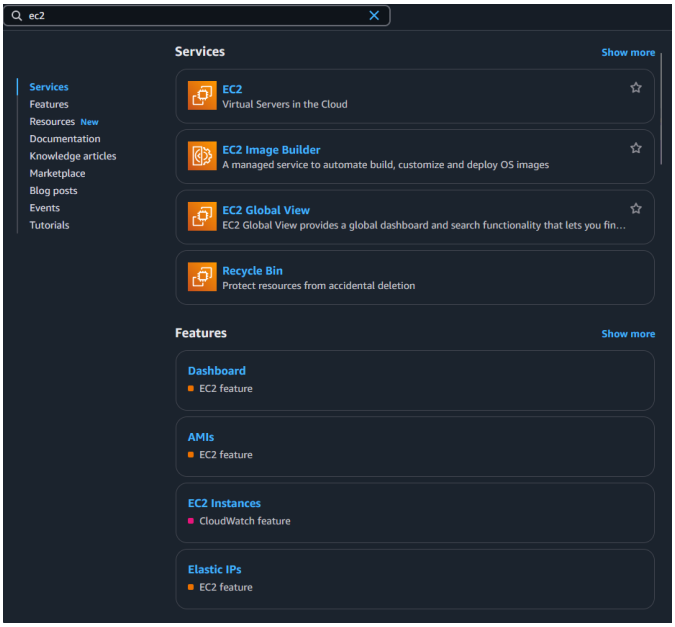


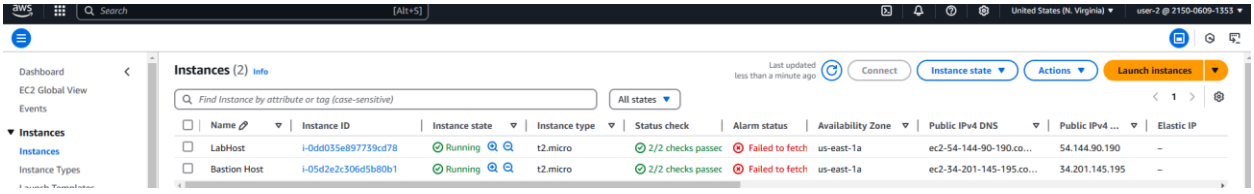
Steps 18: sign out user 1 and sign in user 2

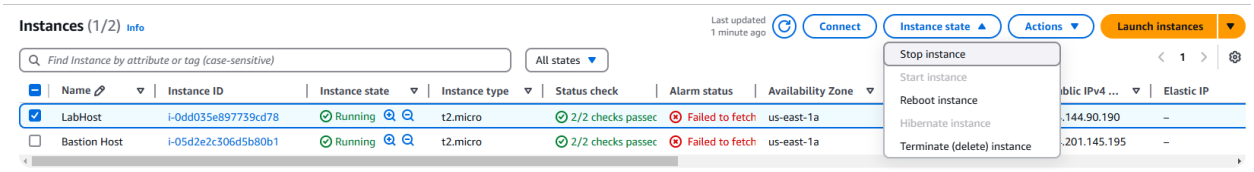


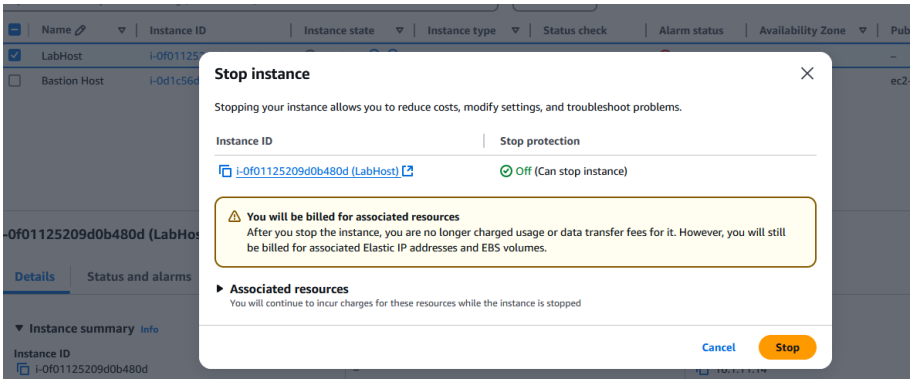


Steps 19: search up ec2, then go to instances, then trying to stop the instance, error message should pop up like this

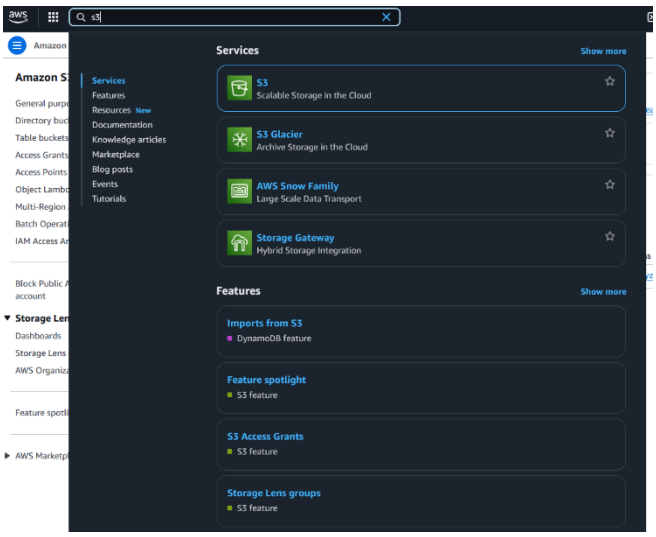


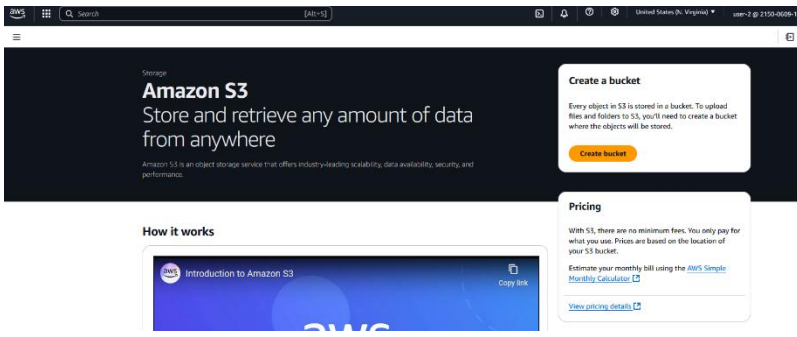




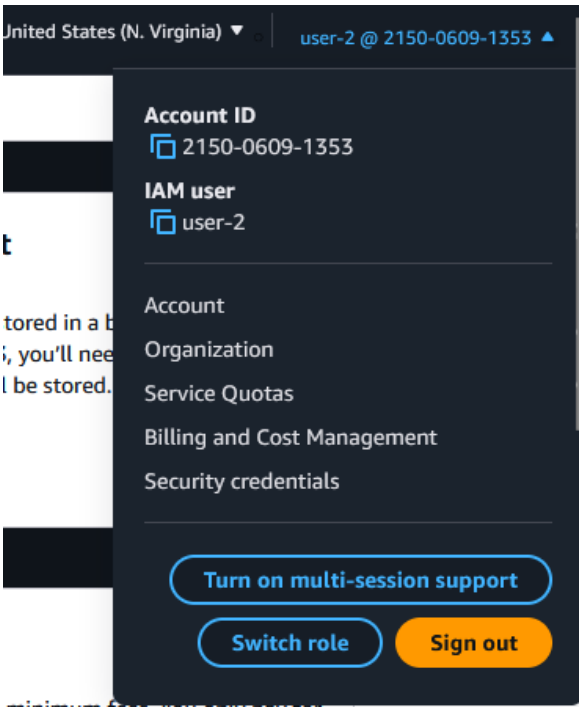


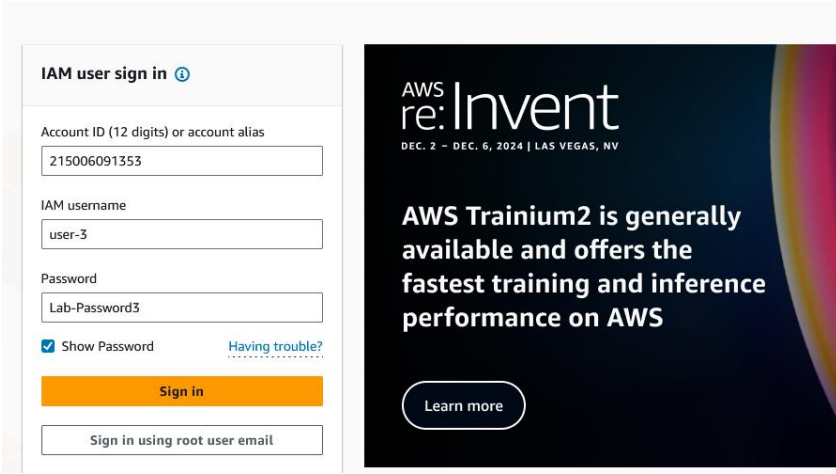
Steps 20: search up S3 then should nothing show up like this because user 2 don't have access to it



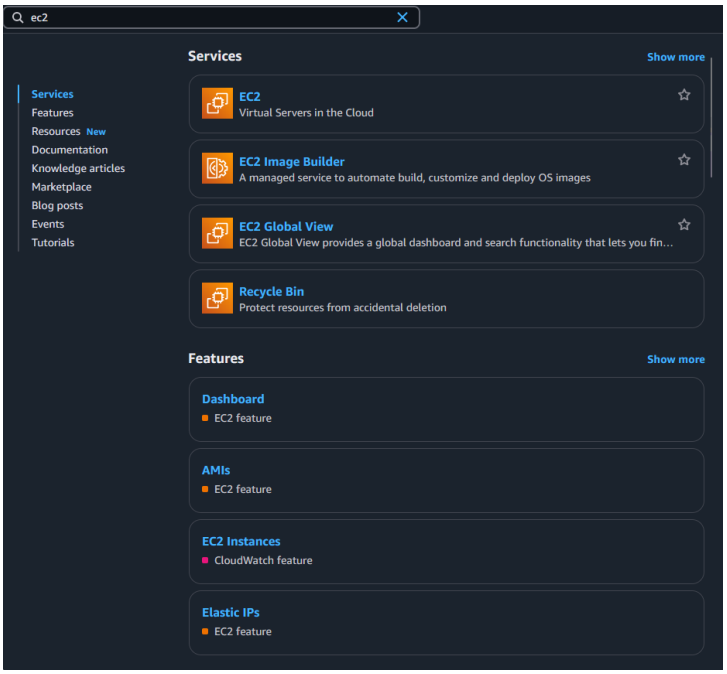


Steps 21: sign out user 2 and sign in user 3

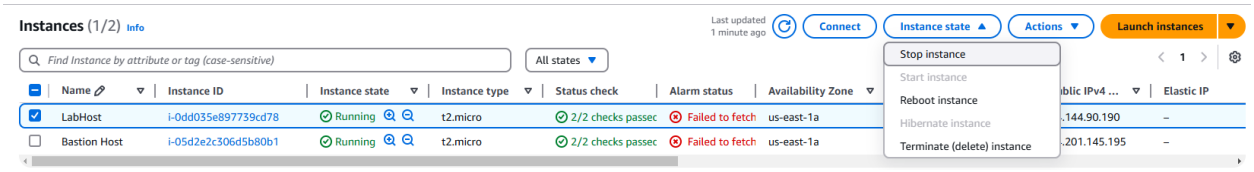


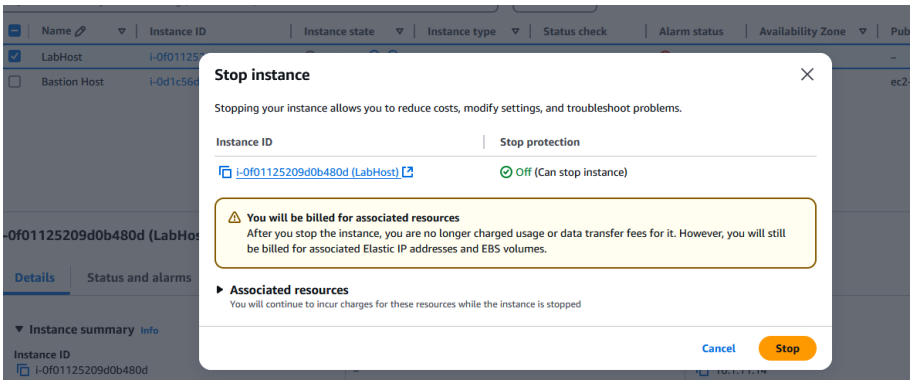


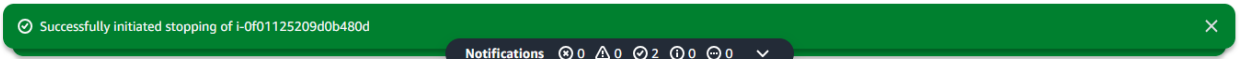
Steps 22: Search up EC2 than click on instances



Steps 23: try to stop the instance, but this time it did not show any error there.





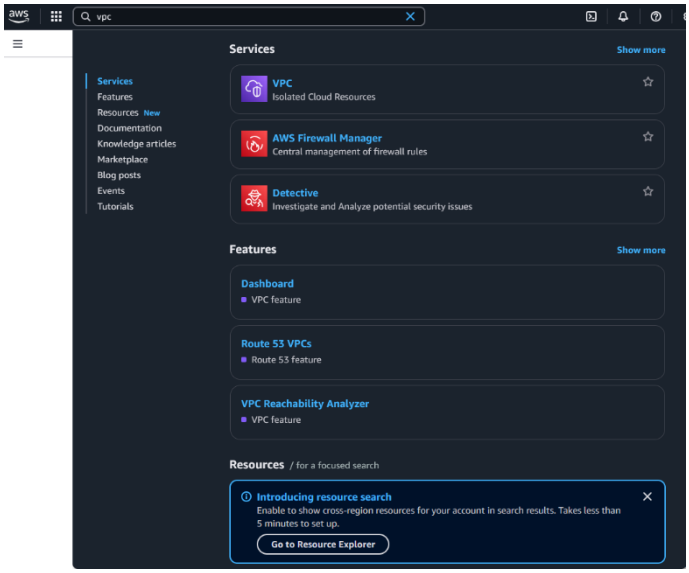


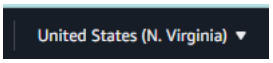
Steps 24: You can close all window than click submit, check for submission report, then you can ■ End Lab

Lab2:

Steps 1: Click on start Lab to start to Lab and wait it turn green, then click on the link of AWS ▶ Start Lab AWS

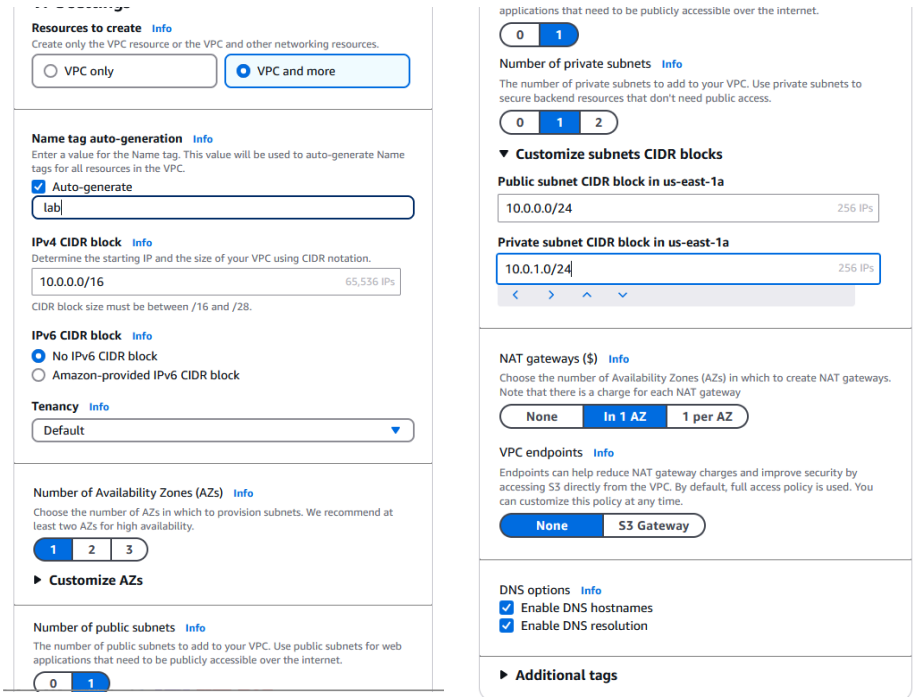
Steps 2: search up VPC than open VPC console



Steps 3: make sure it is N. Virginia 

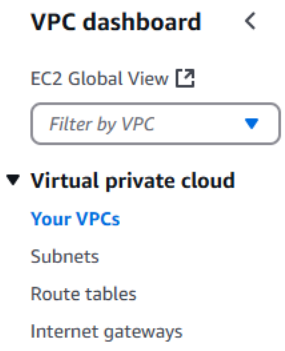
Steps 4: click on create VPC 

, then follow the setting based on the screen shot, click on VPC and more, keep auto generate selected, but change the value from project to lab, keep the IPv4 CIDR block set to 10.0.0.0/16, number of Availability Zones choose 1, for the number of public subnet and private, keep the 1 settings, expand the customize subnet CIDR blocks section, change the public subnet CIDR block in us-east-1a to 10.0.0.0/24, then private subnet CIDR block to 10.0.1.0/24, set NAT gateways to In 1 AZ, select VPC endpoints to None, keep both DNS hostnames and DNS resolution enabled



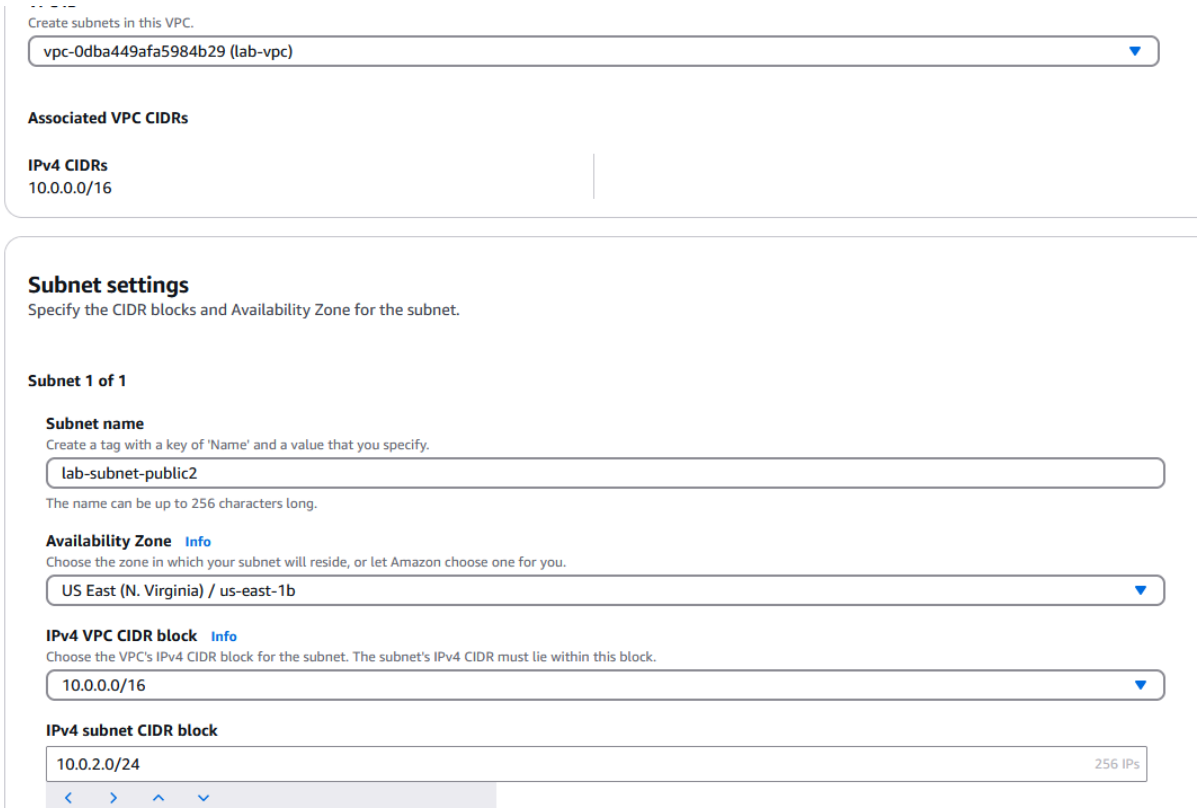
Steps 5: choose create VPC, and wait until all resources are created, then click 

Steps 6: choose subnet located at the top left of the web page

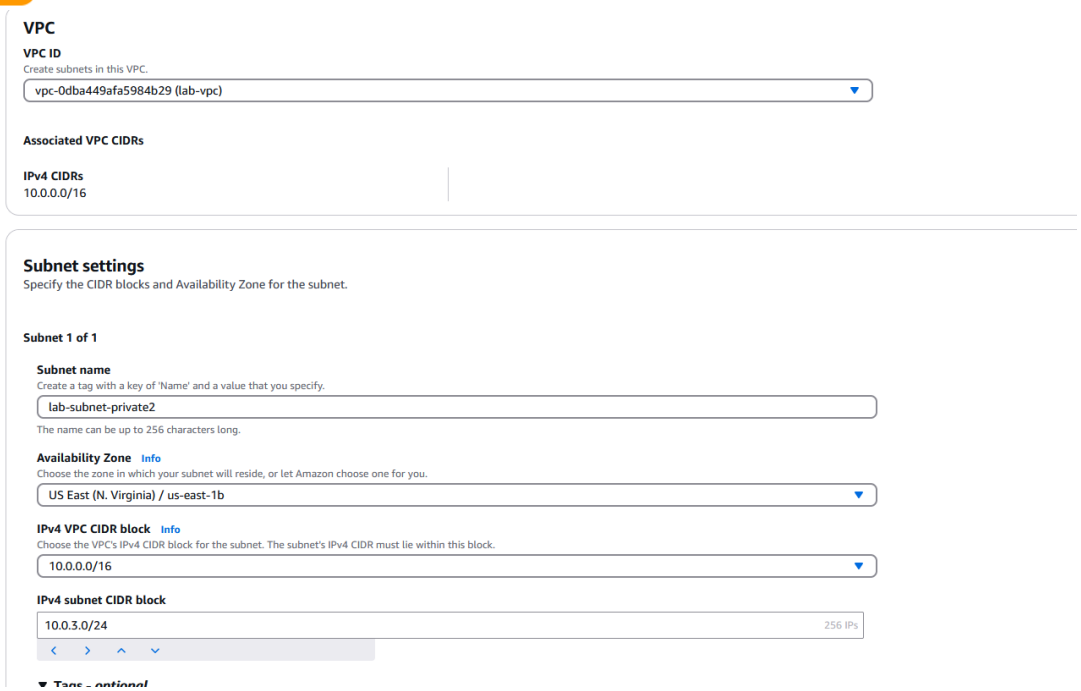


Steps 7: Then click on Create subnet, VPC ID, lab-VPC, select from the menu, subnet name lab-subnet-public2, availability Zone, us-east-1b, ipv4 CIDR block 10.0.2.0/24, then click

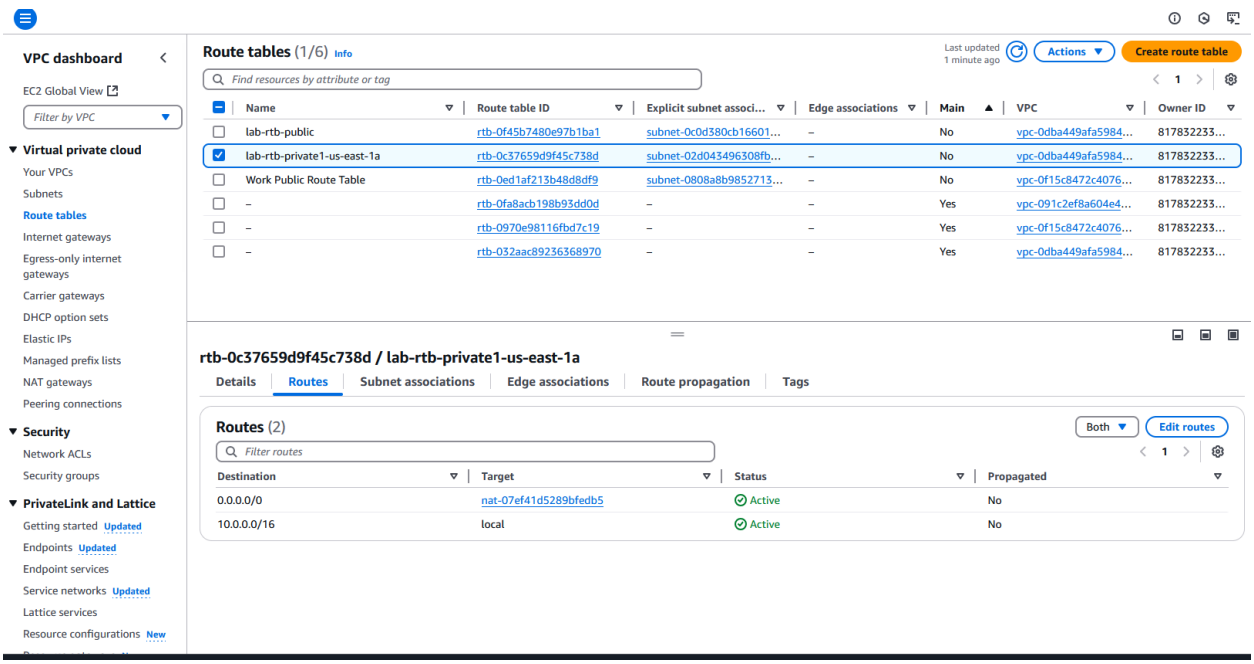
Create subnet



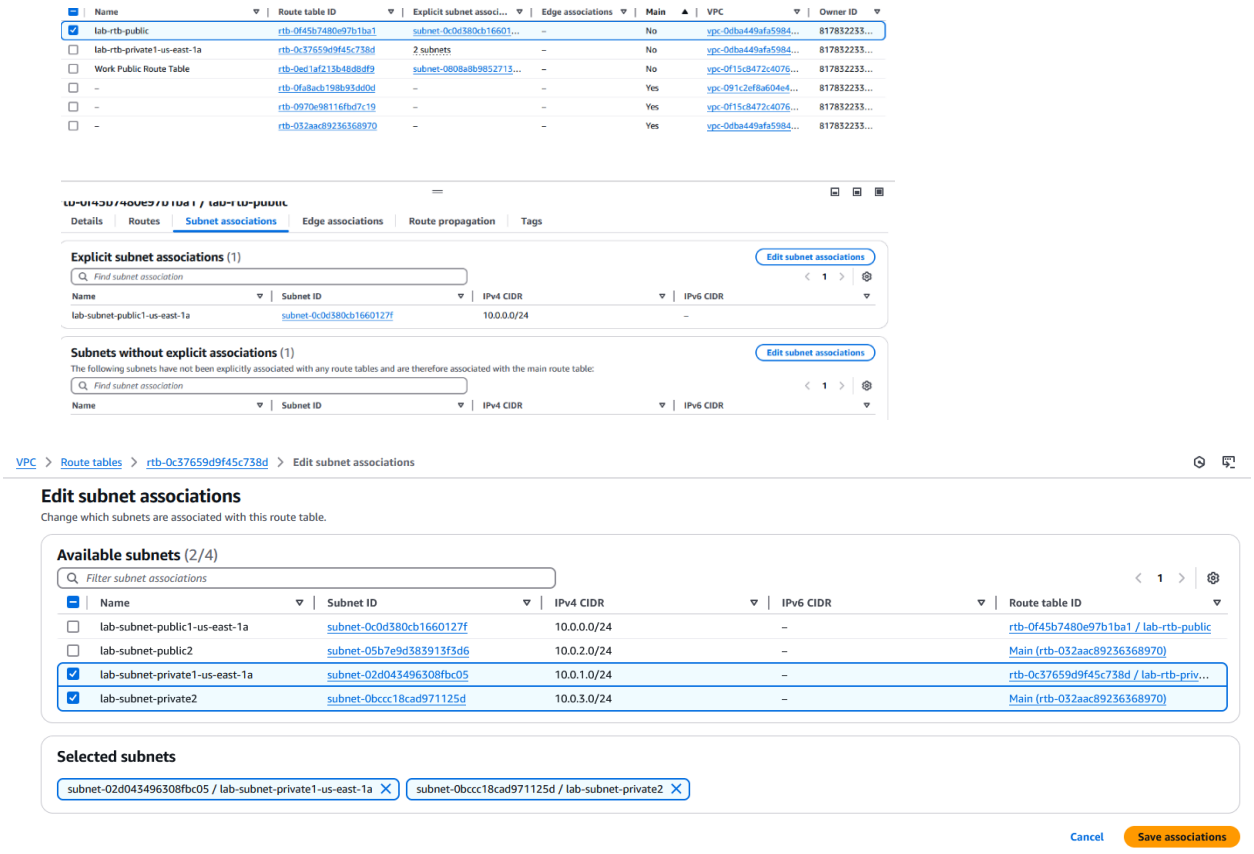
Steps 8: click on Create subnet again, VPC ID, lab-VPC, select from the menu, subnet name lab-subnet-private2, availability Zone, us-east-1b, ipv4 CIDR block 10.0.3.0/24, then click Create subnet



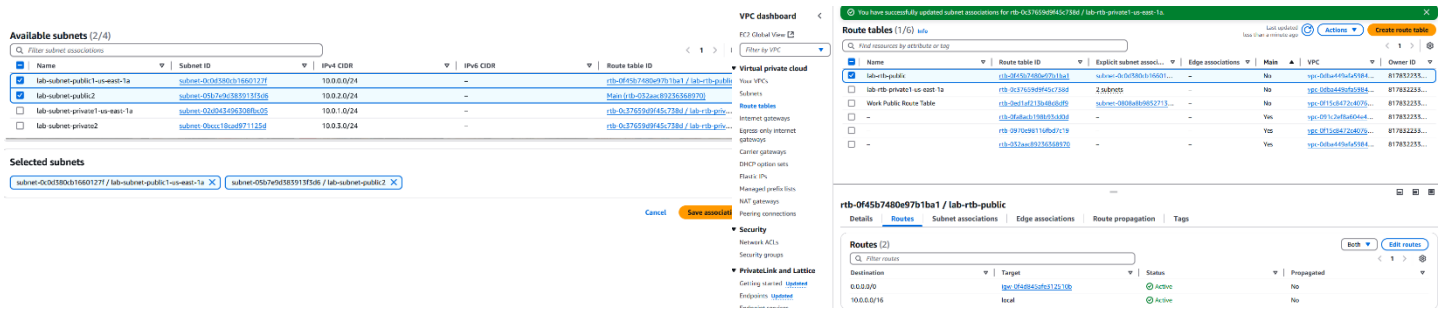
Steps 9: click on route tables and check on lab-rtb-private1-us-east-1a, then click on route and check all internet go to internet is NATed



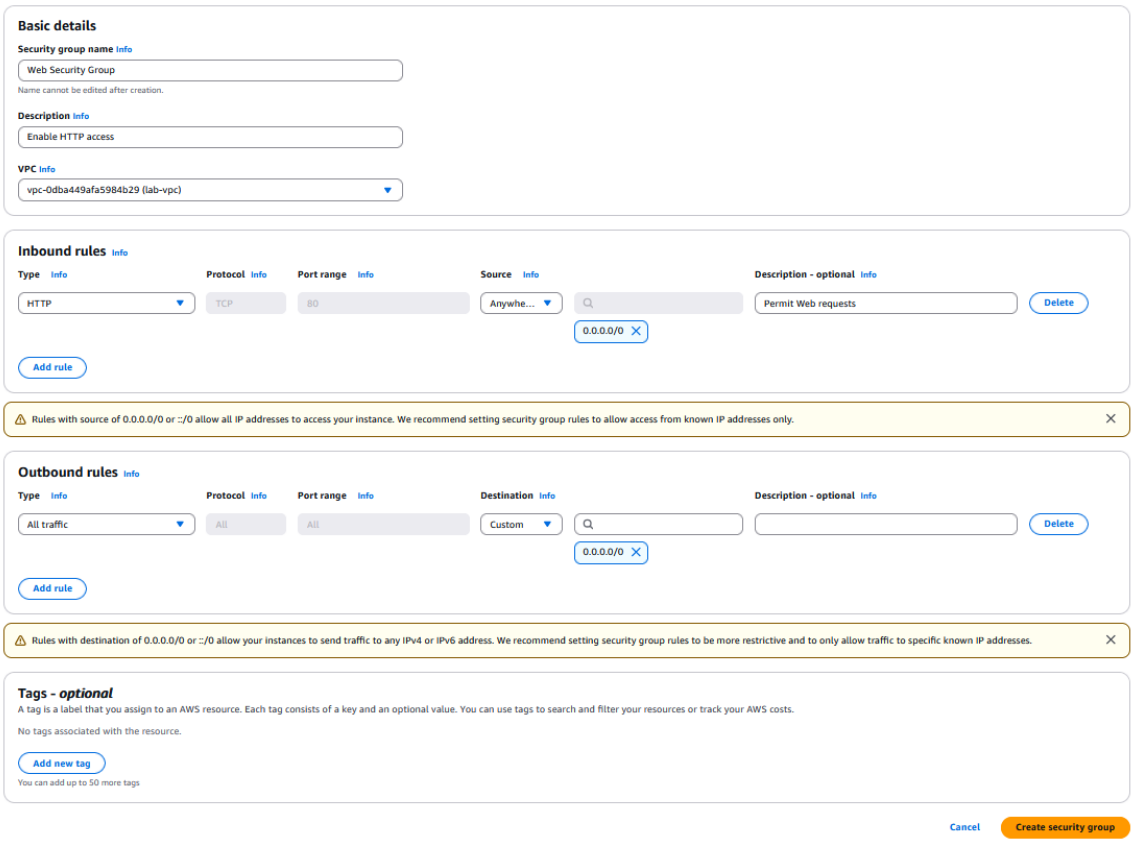
Steps 10: choose the subnet associations tab, then choose edit subnet associations, leave lab-subnet-private1-us-east-1a selected, but also select lab-subnet-private2, then choose **Save associations**



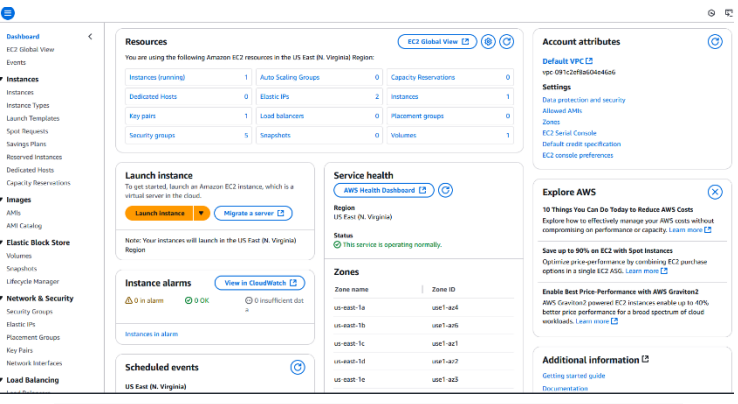
Steps 11: select the lab-rtb-public route table, check the route 0.0.0.0/0 is set to target igw-xxxxxx, which is internet gateway, choose the subnet associations tab, then choose edit subnet associations, then select both subnet-public and choose **Save associations**

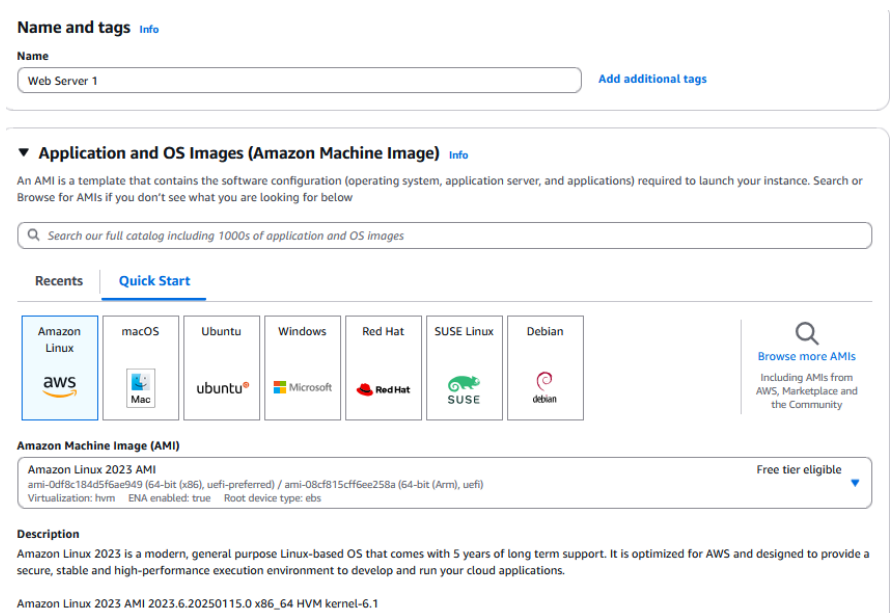


Steps 12: click on security groups, then choose **Create security group**, configure like the screenshot below, name is Web Security Group, description enable HTTP access, vpc choose lab-vpc, In the Inbound rules pane, choose add rule, type http, source anywhere-ipv4, description permit web requests, then choose **Create security group**

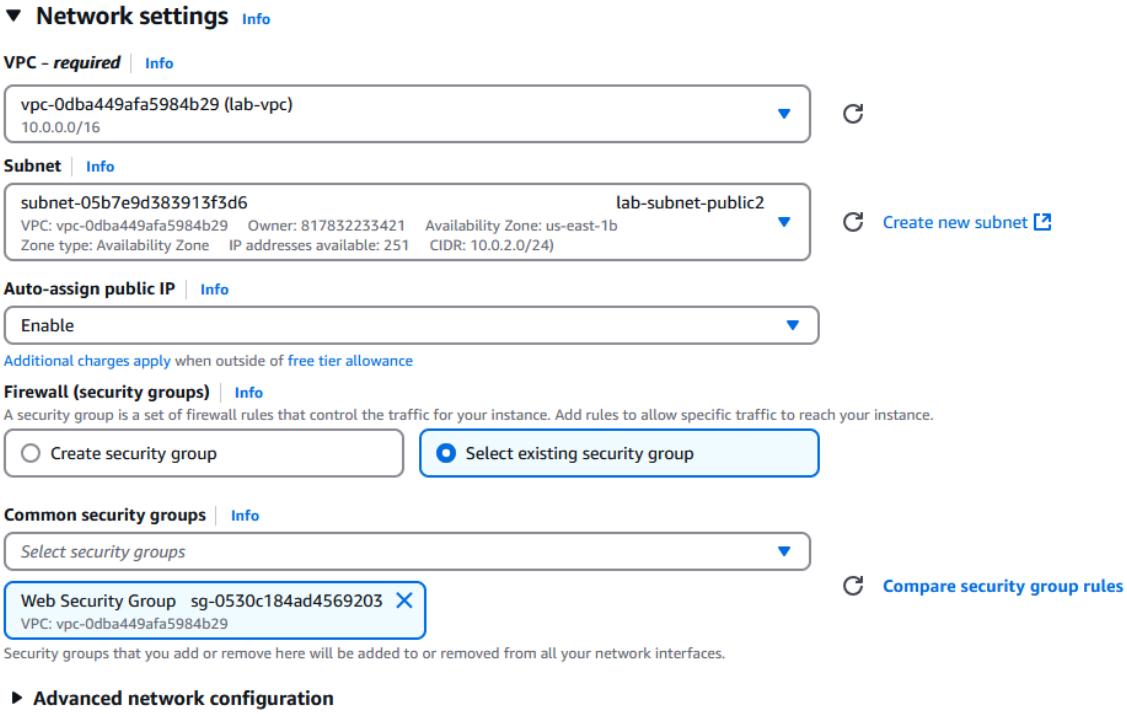


Steps 13: search EC2 and open EC2 console, then click on launch instance, name it Web Server 1, keep the default Amazon Linux selected, also keep the default Amazon Linux 2023 AMI selected, keep the default t2.micro selected, then choose vockey at key pair

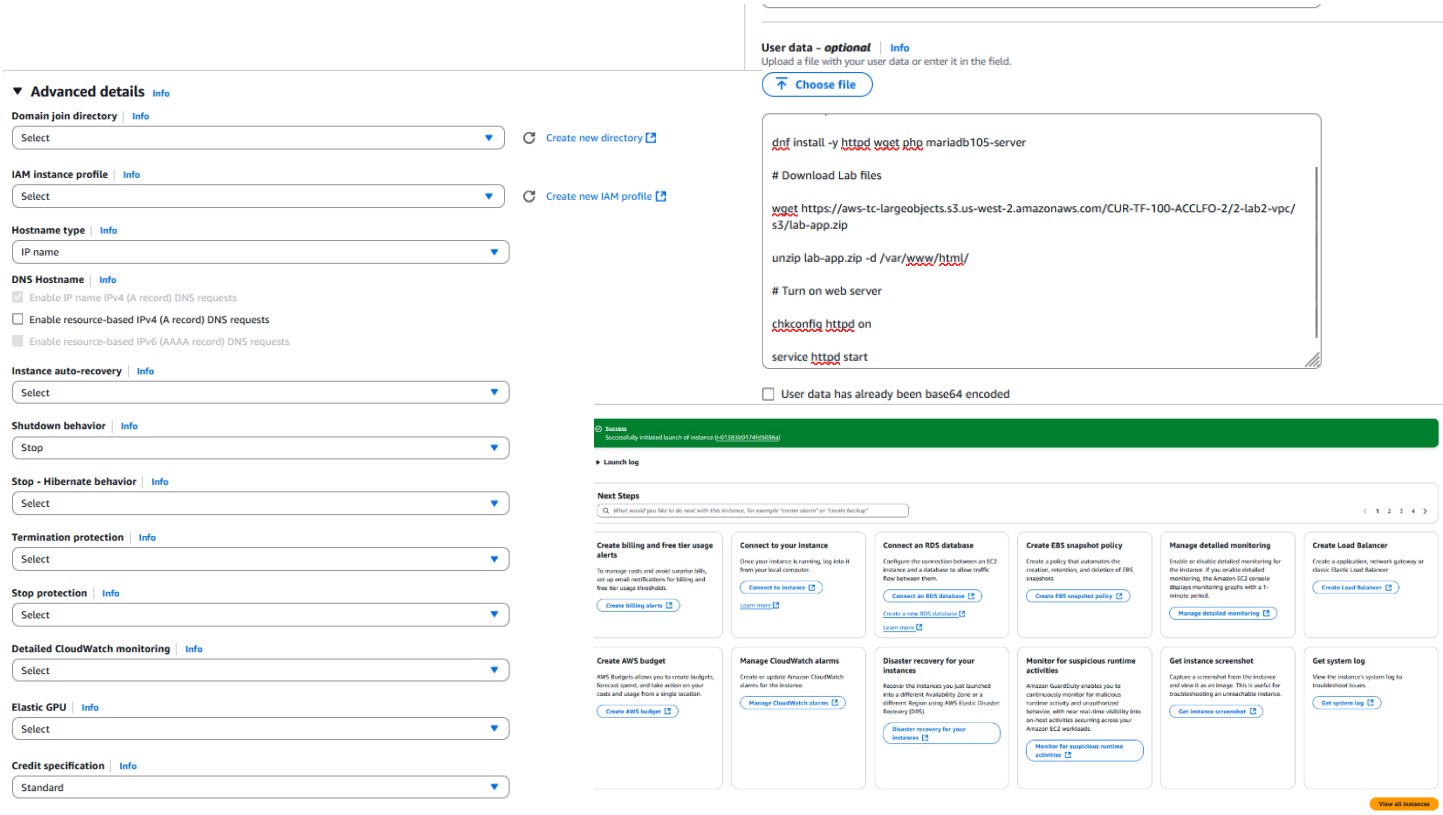




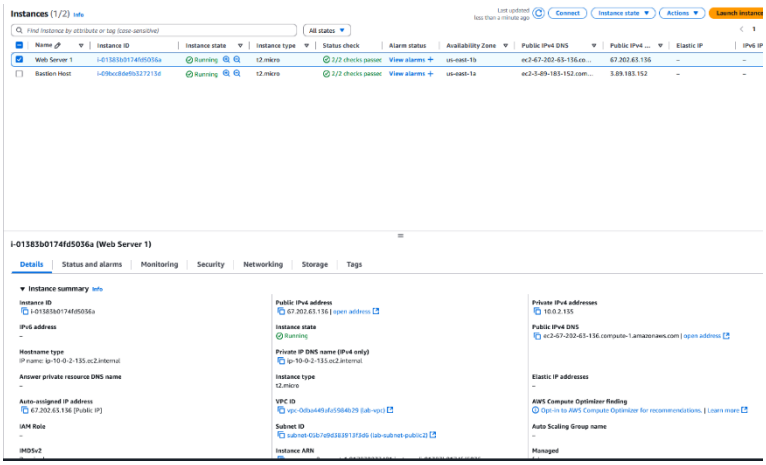
Steps 14: expand network setting, follow the screenshot for the configuration, choose the lab-vpc, subnet to lab-subnet-public2, enable auto assign public ip, choose select existing security group, for common security group, select web security group.

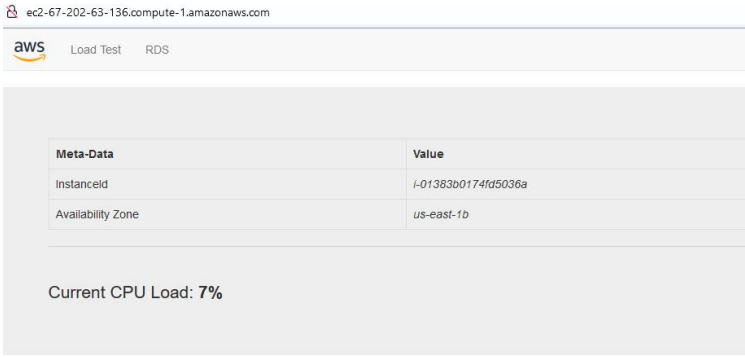


Steps 15: Expand Advanced detail panel, scroll to bottom then copy and paste the code shown into User data box, then click **Launch instance** , you will see a success message, then click on view all instances

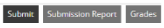


Steps 16: Wait until Web Server 1 show 2/2 checks passed, then select web Server 1, copy public ipv4 DNS, paste it on new browser tab, then the result should be looks like this





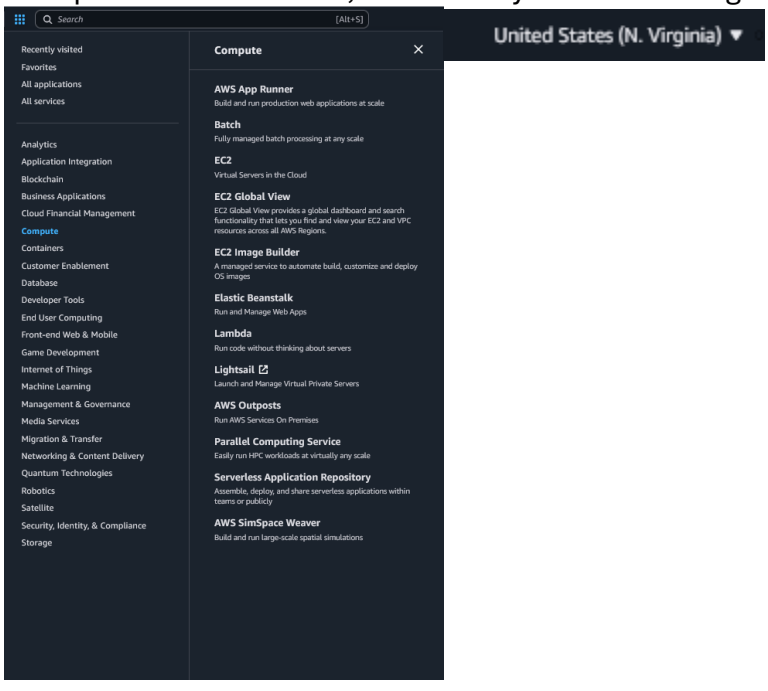
Steps 17: You can close all window than click submit, then check for submission report, then ■ End Lab



Lab 3:

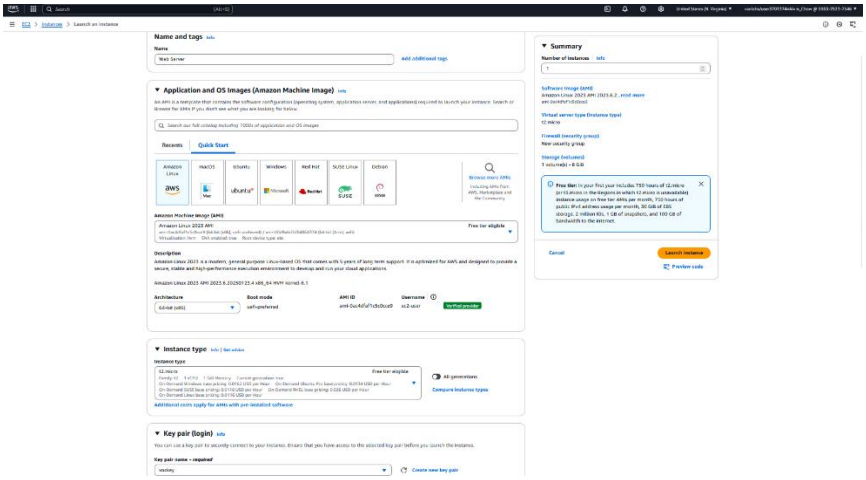
Steps 1: Click on start Lab to start to Lab and wait it turn green, then click on the link of AWS ▶ Start Lab AWS

Steps 2: search for EC2, make sure you are in N. Virginia region

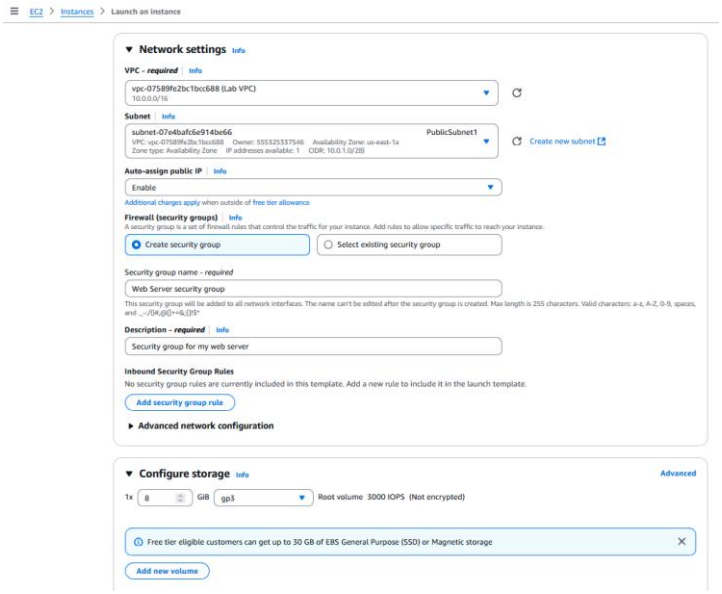


Steps 3: Choose the Launch instance menu and select Launch instance

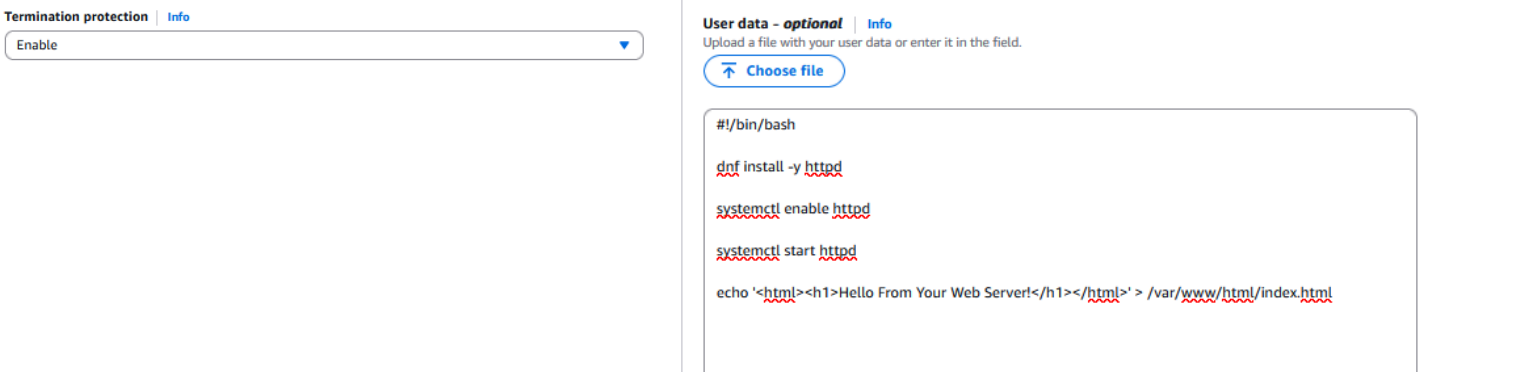
Steps 4: Follow the setting of the screenshot, first name is Web Server, then keep the default Amazon Linux 2023 AMI selected, then keep the default t2.micro selected, for key parir name choose vockey



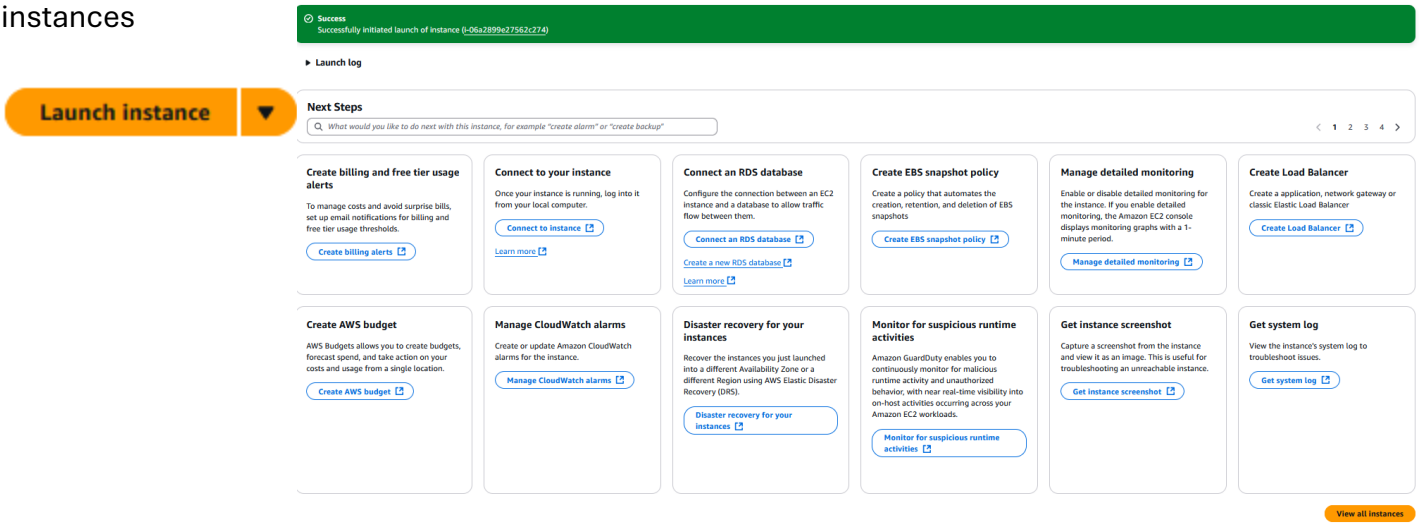
Steps 5: next to network settings choose edit, for vpc, select Lab VPC, keep the default subnet, under security groups, choose create security group and name is Web Server security group, description Security group for my web server, under Inbound security group rules, remove any existing rules. Then keep the default settings of configure storage section



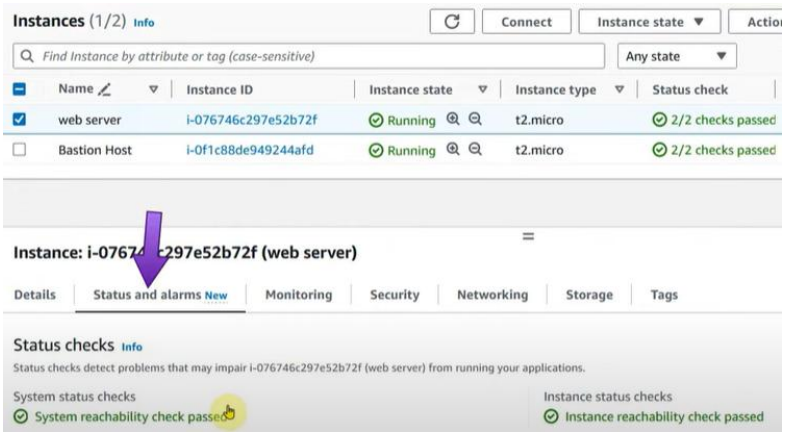
Steps 6: Expand Advanced details, enable termination protection, scroll to the bottom of the page and copy and paste the code into User data box

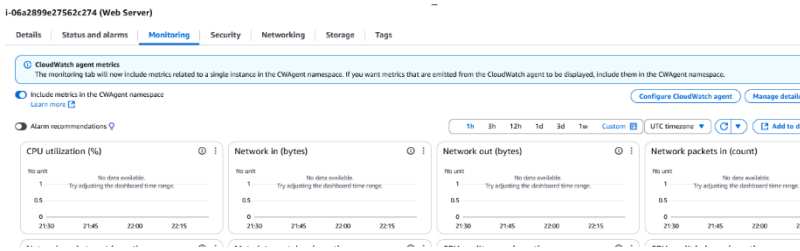


Steps 7: click on launch instance and should see successful message, that choose view all instances

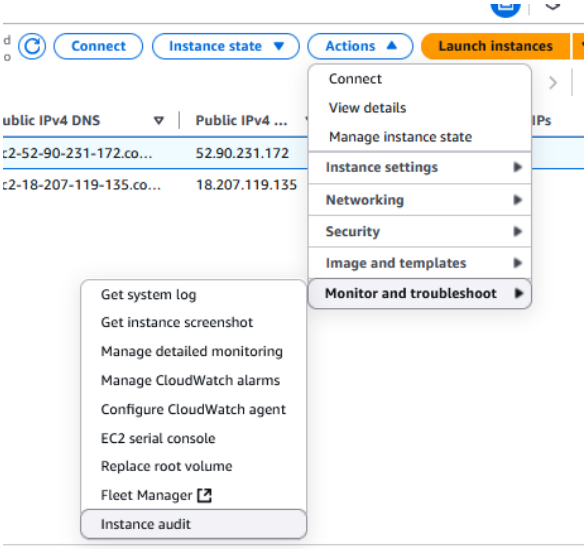


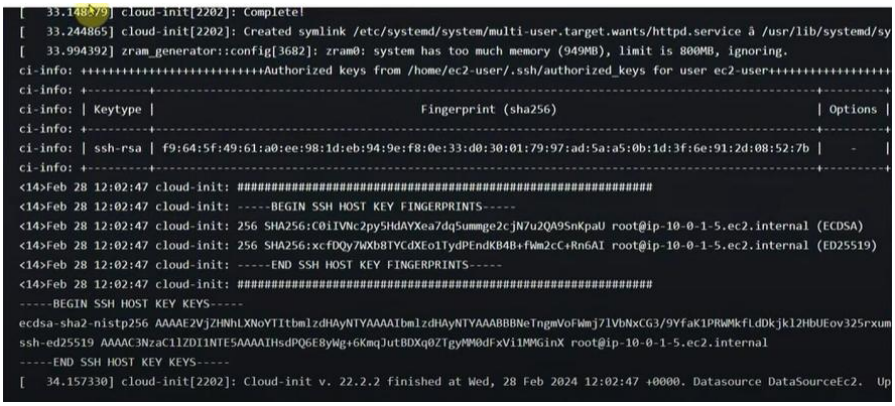
Steps 8: check that instance that go to status and alarms, make sure it pass all the system check, then go to monitoring, you should see this



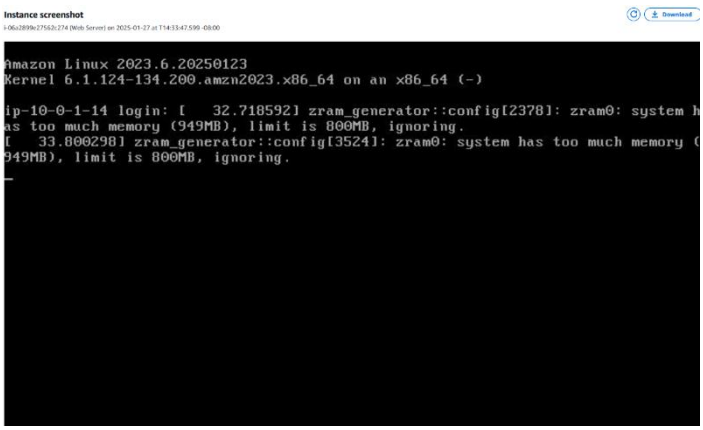


Steps 9: click on actions, then monitor and troubleshoot and select get system log

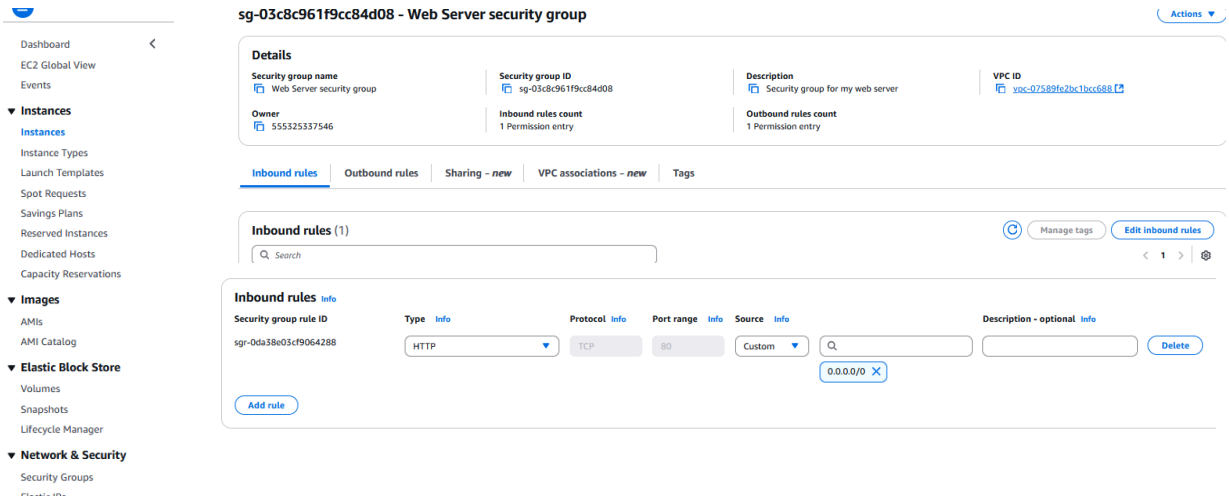




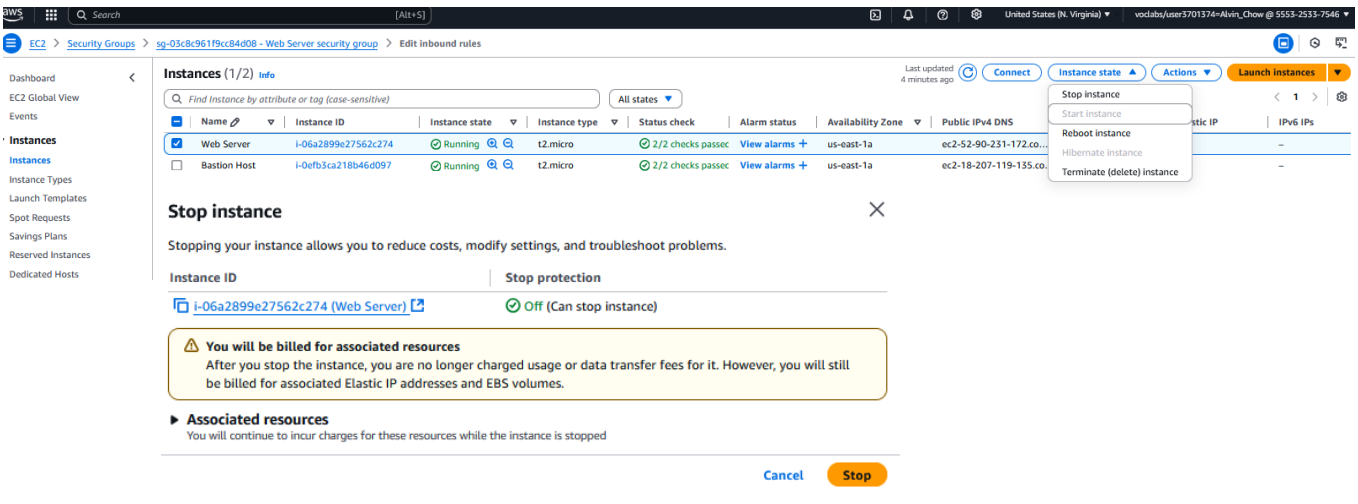
Steps 10: go back to instance list, in the actions menu, select Monitor and troubleshoot, and get instance screenshot



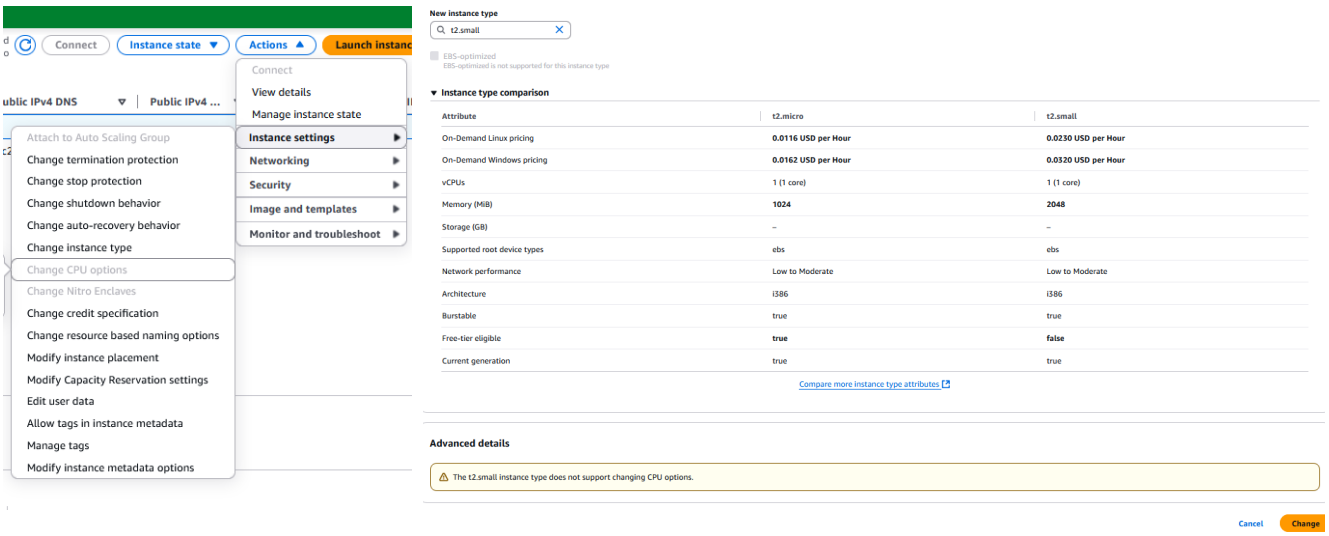
Steps 11: back to instance list, then in the left navigation pane, choose security groups, select Web Server security groups, choose the inbound rules tab, choose edit inbound rules and set the type to be HTTP, source anywhere-IPv4, then choose saves rules



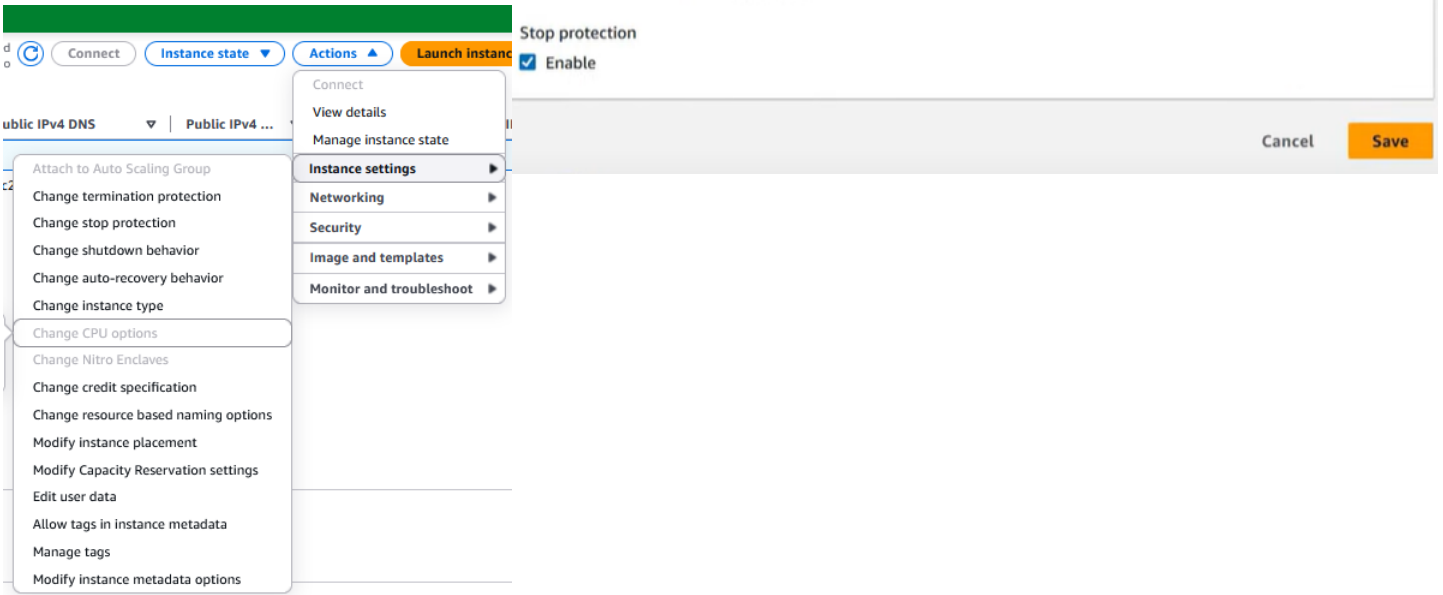
Steps 12: back to instance list and select the Web Server instance, in the Instance state menu, select Stop instance, choose Stop



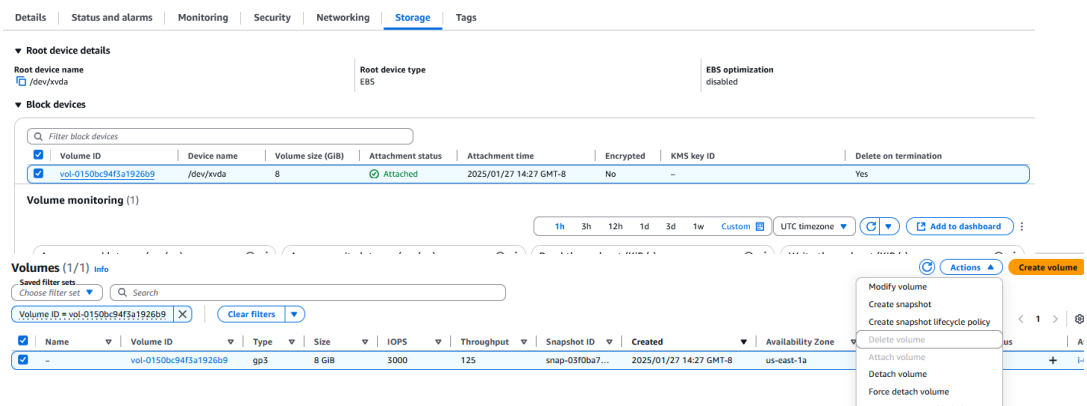
Steps 13: In the action menu, select Instance settings, then change instance type to t2.small then click change



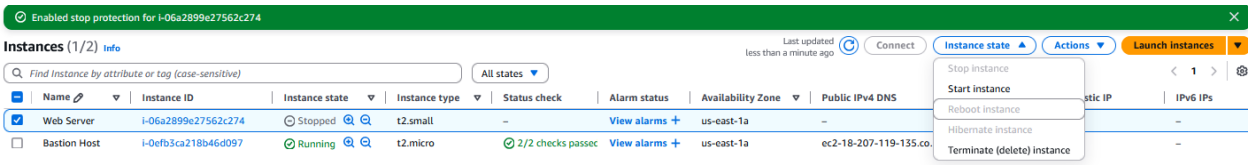
Steps 14: back to instance list, select web server instance, in action menu, select Instance setting, change stop protection select enable, then save



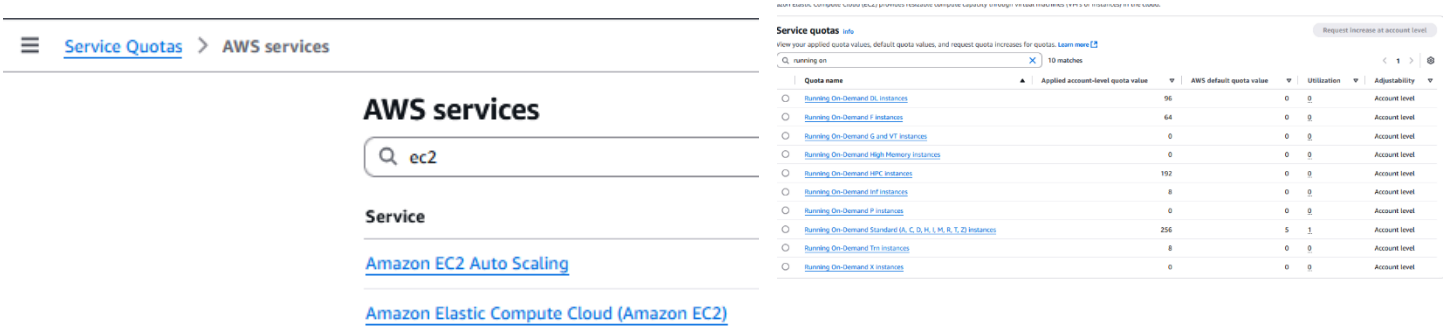
Steps 15: With the Web Server instance still selected, choose the storage tab, select the name of the Volume ID, then go to action menu select modify volume, change the size to 10, choose modify, then choose it again to confirm and increase the size of the volume



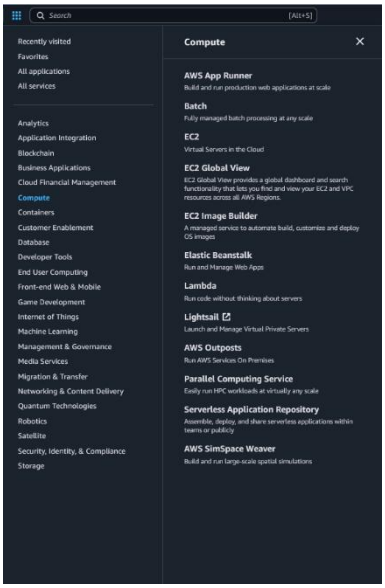
Steps 16: go back to instance tab and select Web Server instance and start it

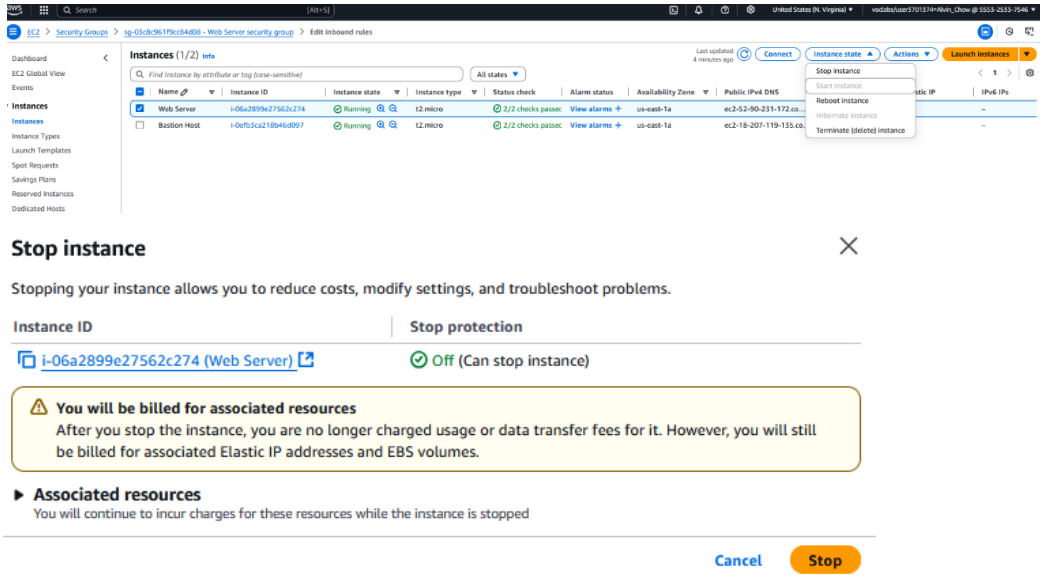


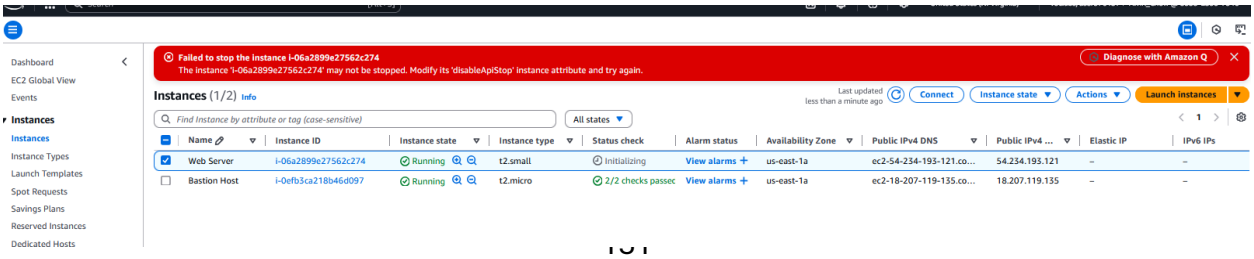
Steps 17: Search up Service Quotas in the search box, choose AWS Service, then service ec2 and choose Amazon Elastic Compute Cloud, then on Service Quotas, search running on -demand, and observer list of service that match the criteria



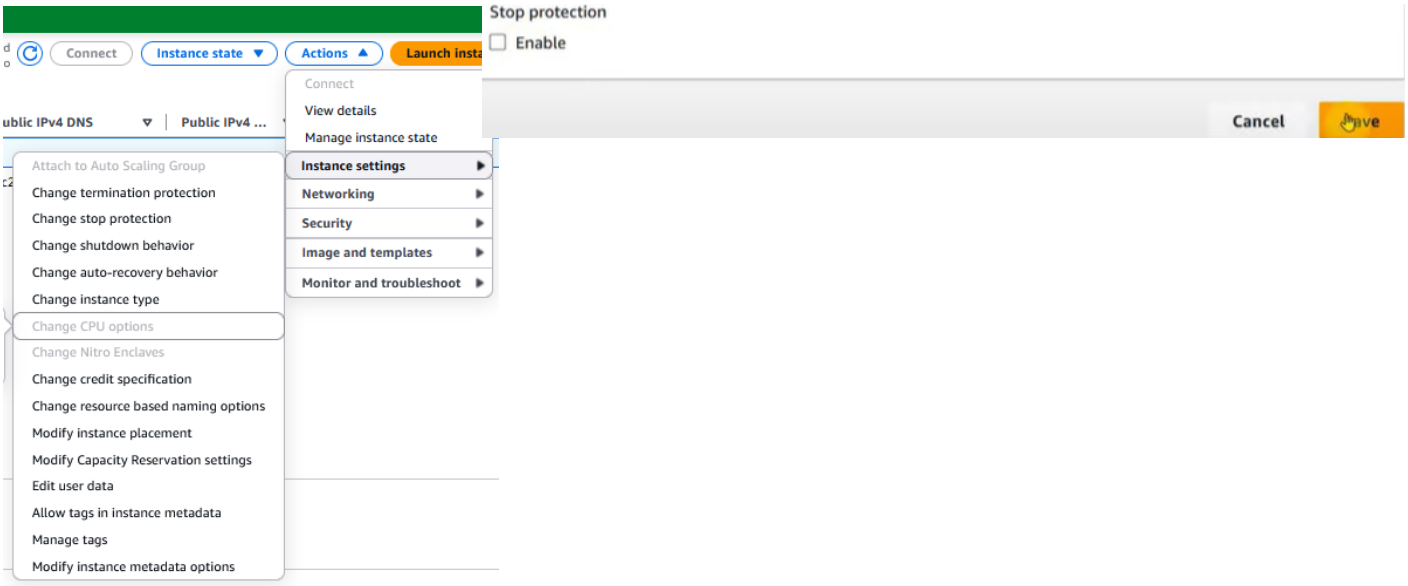
Steps 18: go back to Ec2 console, then click instances, select Web Server instance, select stop instance then choose stop and it should show failed because the stop protection enabled



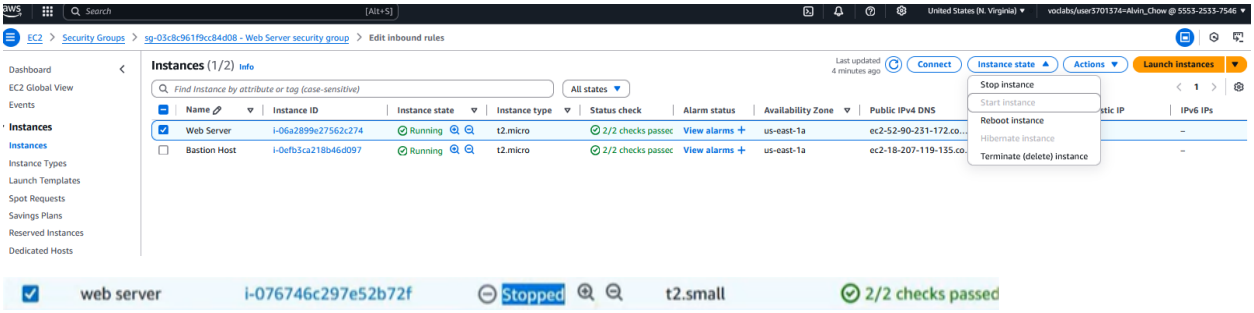




Steps 19: In the Actions menu select Instance settings, change stop protection, and remove the check next to enable, then click save



Steps 20: Now you can go back to instances and go to instance state menu, select stop instances choose stop, it should be successfully stopped



Steps 21: You can close all window than click submit, then check for submission report, then ■ End Lab

Problem: In these three labs, I did not faced any problems because I followed the instructions of the lab and it working fine.

Conclusion: In this lab, I learned more about how AWS works by setting it up, those lab also made us understand more about the core services like EC2, S3, IAM and VPC, Now I learned how to configure, deploy and manage it. By working through tasks like real workplace situations, it can help me prepare for future working situations.

AWS Lab 4-6

By Alvin Chow

Purpose: The purpose of these labs is to provide hands-on experience with AWS, helping me understand core services such as Amazon EBS, VPS, RDS DB, AMI, load balancers, launch templates, auto scaling, and Amazon CloudWatch alarms. These labs teach me how to configure, deploy, and manage these cloud components in a normal environment. By working through tasks that similar to real-world scenarios, I know more about those topics, which can prepare me for a future career in cloud computing.

Background information:

Amazon EBS is a high-performance block storage service designed for use with Amazon EC2 instances. It provides high-availability storage that remains independent of the lifecycle of an EC2 instance. With features like dynamic volume resizing, snapshot capabilities for backups, and encryption options, EBS is a reliable choice for a wide range of applications.

Amazon EC2 provides resizable compute capacity in the cloud, enabling users to launch virtual servers on demand. It offers many instance types for different workloads, from general-purpose computing to high-performance tasks. EC2's flexible pricing options, such as On-Demand, Reserved, and Spot Instances, allow organizations to optimize costs while scaling their infrastructure.

Amazon RDS is a managed database service that simplifies the process of setting up, operating, and scaling relational databases in the cloud. It supports popular database engines such as MySQL, PostgreSQL, Oracle, and SQL Server, automating tasks like backups, patching, and replication. By offloading these operational burdens, RDS allows developers to focus on application logic while ensuring high availability and scalability for database workloads.

An Amazon Machine Image is a pre-configured template that contains the information required to launch an EC2 instance. This includes the operating system, application server, applications, and necessary settings. AMIs help ensure consistency across multiple instances, making it easier to scale environments or replicate server configurations reliably and rapidly.

In AWS, an Elastic Load Balancer automatically distributes incoming application traffic across multiple EC2 instances or other targets. This service enhances fault tolerance and scalability by ensuring that no single instance bears too much load, while also improving the overall availability of applications by routing traffic only to healthy instances. It supports various types—including Application, Network, and Classic Load Balancers—to suit different application needs.

Launch templates are configuration resources that define the settings required to launch EC2 instances. They bundle parameters such as the AMI, instance type, key pair, security groups, and storage options, and support versioning so that multiple configurations can be maintained.

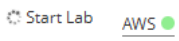
Amazon Auto Scaling automatically adjusts the number of EC2 instances in response to real-time demand changes. It ensures that applications have the right amount of capacity to maintain performance while minimizing costs during low-traffic periods. By using policies that trigger scaling actions based on metrics like CPU utilization or network load, Auto Scaling helps maintain optimal application performance and availability.

Amazon CloudWatch is a monitoring service for AWS resources and applications, and its alarms allow you to track specific metrics over time. By setting threshold-based alarms, you can automatically trigger notifications or corrective actions, such as scaling events or instance replacement.

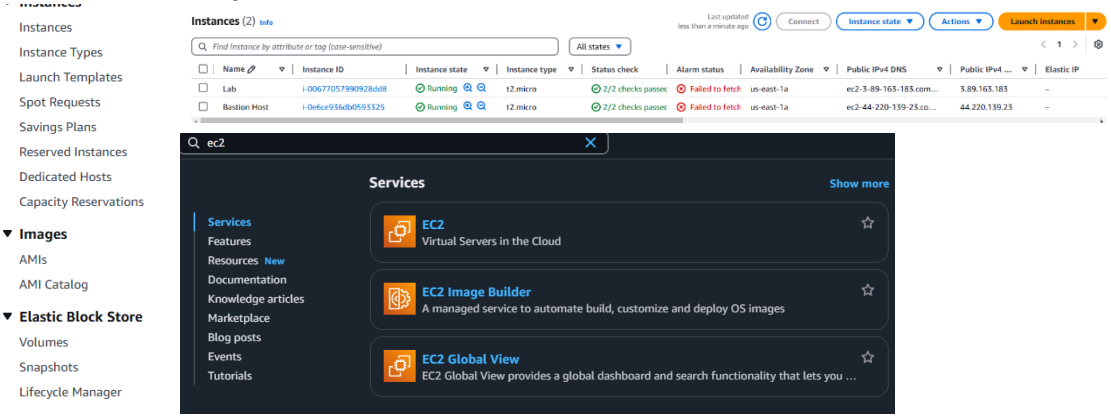
Lab Summary: Step by step guide to finish lab 4-6

Lab 4:

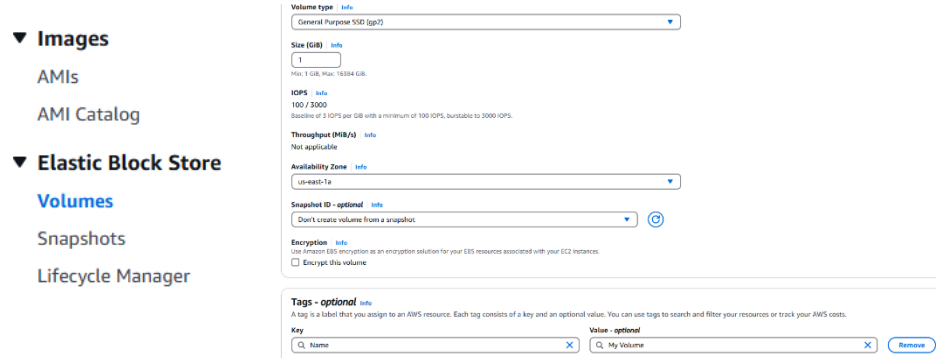
Step 1: click on start lab and wait for AWS line to turn green, then click on the link



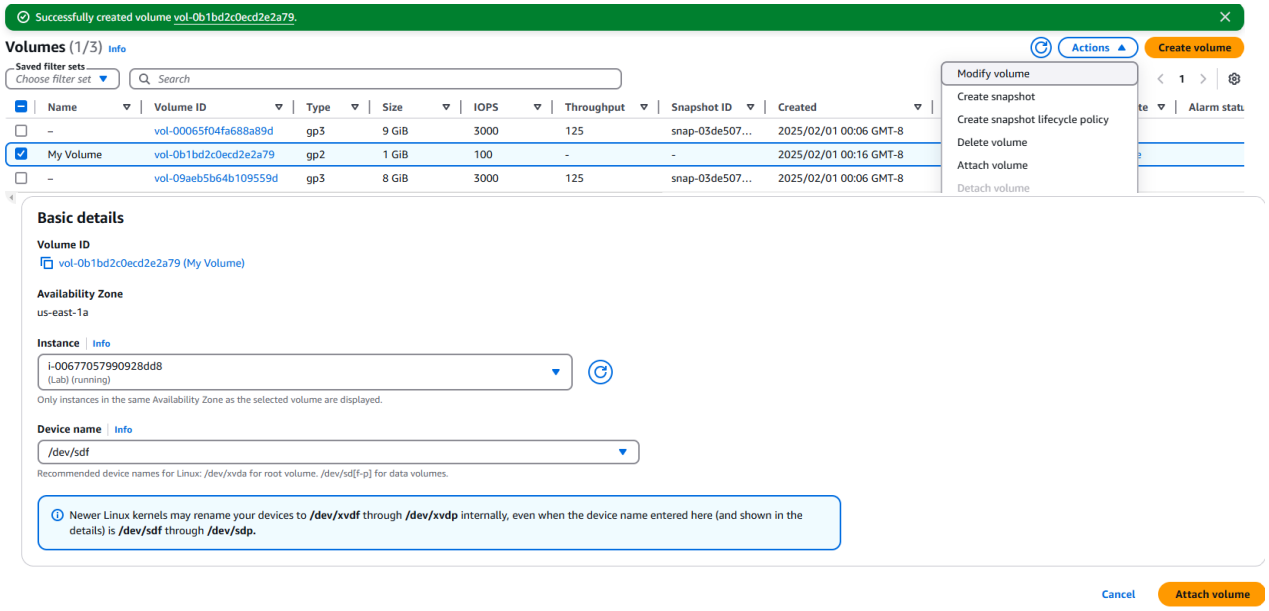
Step 2: Search up EC2 and go to the dashboard, then go to instance, there are one instances already created.



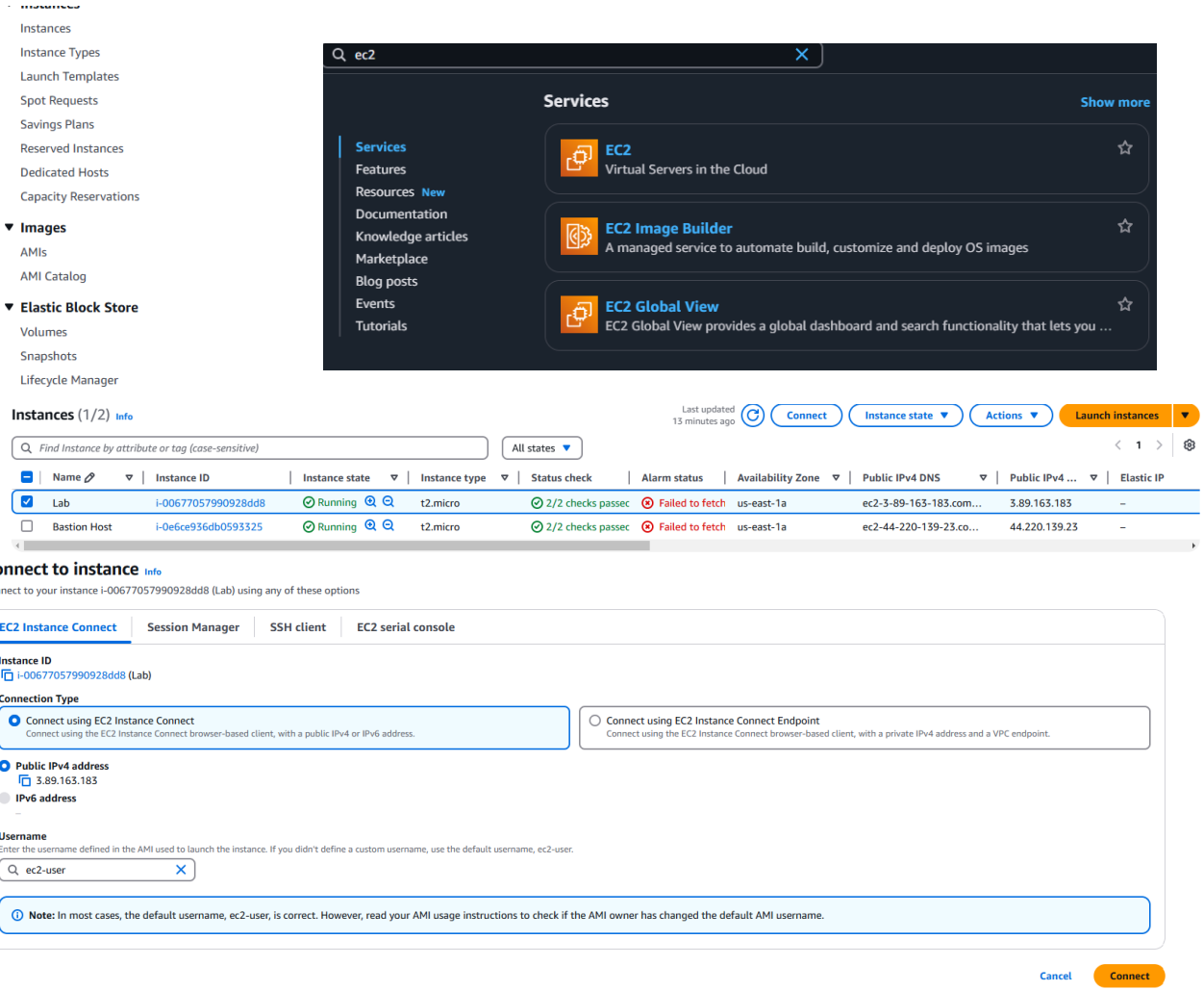
Steps 3: go to Volumes, then click on Create volume, Volume type is gp2, size set it to 1, Avaliability zone set it same as your instance, than click on add tag, name it Name and Value is My Volume, then scroll down add click on create volume



Steps 4: If it successfully created it should looks like the screenshot, then click on actions, then attach volume, choose the lab instance, set the device name to /dev/sdf, and click attach volume



Steps 5: search ec2 then click on instances, select the Lab Instance then choose connect, then click connect again on EC2 Instance connect



Steps 6: it should bring you to new tab after you clicked connect type the command **df-h**, you should see something like this, then type the command **sudo mkfs -t ext3 /dev/sdf**, to create an ext3 file system on the new volume

```
[ec2-user@ip-10-1-11-82 ~]$ df -h
Filesystem      Size  Used Avail Use% Mounted on
devtmpfs        4.0M     0  4.0M   0% /dev
tmpfs           475M     0  475M   0% /dev/shm
tmpfs           190M  452K  190M   1% /run
/dev/xvda1      8.0G  1.6G  6.4G  20% /
tmpfs           475M     0  475M   0% /tmp
/dev/xvda128     10M  1.3M  8.7M  13% /boot/efi
tmpfs            95M     0   95M   0% /run/user/1000
```

```
mke2fs 1.46.5 (30-Dec-2021)
Creating filesystem with 262144 4k blocks and 65536 inodes
Filesystem UUID: 9946ceb3-842a-47d0-80b9-6565b46eb5d7
Superblock backups stored on blocks:
        32768, 98304, 163840, 229376

Allocating group tables: done
Writing inode tables: done
Creating journal (8192 blocks): done
Writing superblocks and filesystem accounting information: done
```

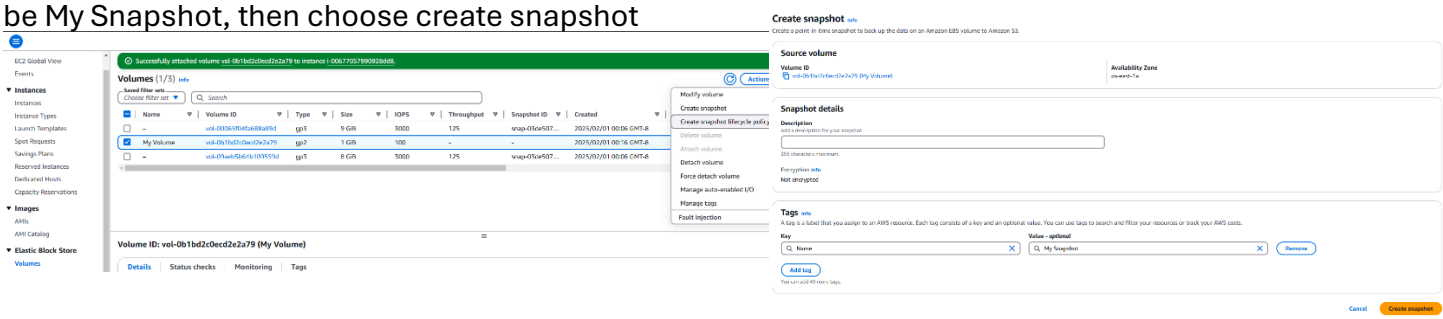
Steps 7: Type the command **sudo mkdir /mnt/datastore**, this command create a directory for mounting the new storage volume, **type sudo mount /dev/sdf /mnt/data-store** to mount the new volume, to configure the Linux instance to mount this volume whenever the instance is started, you will need to add a line to */etc/fstab*. Run the command **echo "/dev/sdf /mnt/data-store ext3 defaults,noatime 1 2" | sudo tee -a /etc/fstab** to do it

Steps 8: to view the configuration file to see the setting on the last command by **cat /etc/fstab**, then you can type **df -h** to view the available storage again. On you mounted volume, create a file and add some text to it by typing **sudo sh -c "echo some text has been written > /mnt/data-store/file.txt"**. You can verify that the text has been written by typing **cat /mnt/data-store/file.txt**

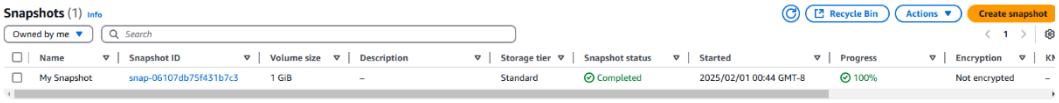
```
some text has been written
```

```
#
UUID=9d0c119b-7697-47bd-99a8-48ecf6e02f0d     /           xfs    defaults,noatime  1   1
UUID=1883-E9E2        /boot/efi       vfat    defaults,noatime,uid=0,gid=0,umask=0077,shortname=winnt,x-systemd.automount 0 2
/dev/sdf   /mnt/data-store ext3 defaults,noatime 1 2
[ec2-user@ip-10-1-11-82 ~]$ df -h
Filesystem      Size  Used Avail Use% Mounted on
devtmpfs        4.0M     0  4.0M   0% /dev
tmpfs           475M     0  475M   0% /dev/shm
tmpfs           190M  452K  190M   1% /run
/dev/xvda1      8.0G  1.6G  6.4G  20% /
tmpfs           475M     0  475M   0% /tmp
/dev/xvda128     10M  1.3M  8.7M  13% /boot/efi
tmpfs            95M     0   95M   0% /run/user/1000
/dev/xvdf       975M   60K  924M   1% /mnt/data-store
```

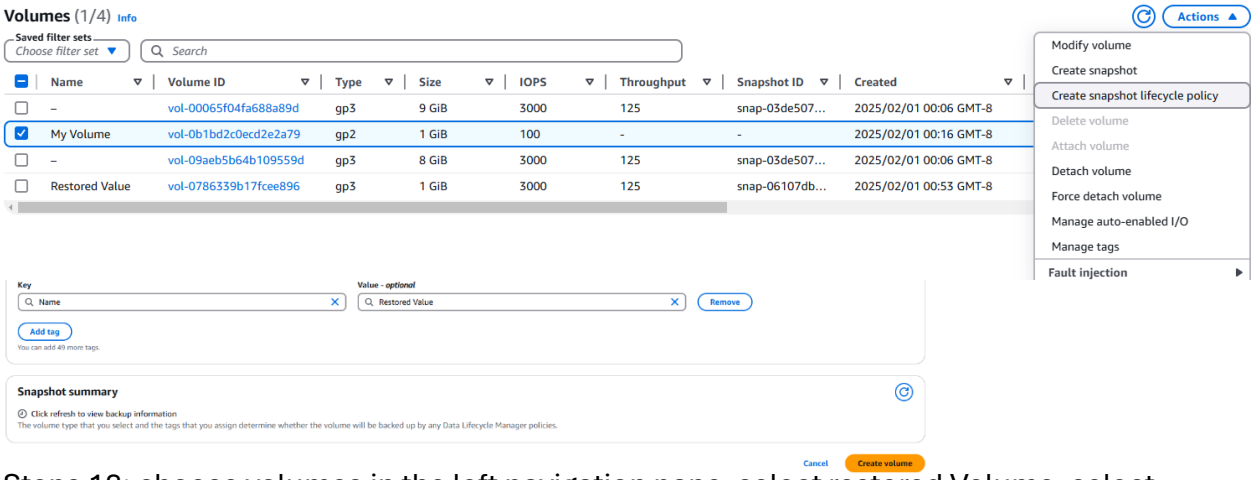
Steps 9: go back to EC2 console, choose Volume and select My Volume, In the Actions menu, select Create snapshot, choose add tag then configure key to be Name and Value to be My Snapshot, then choose create snapshot



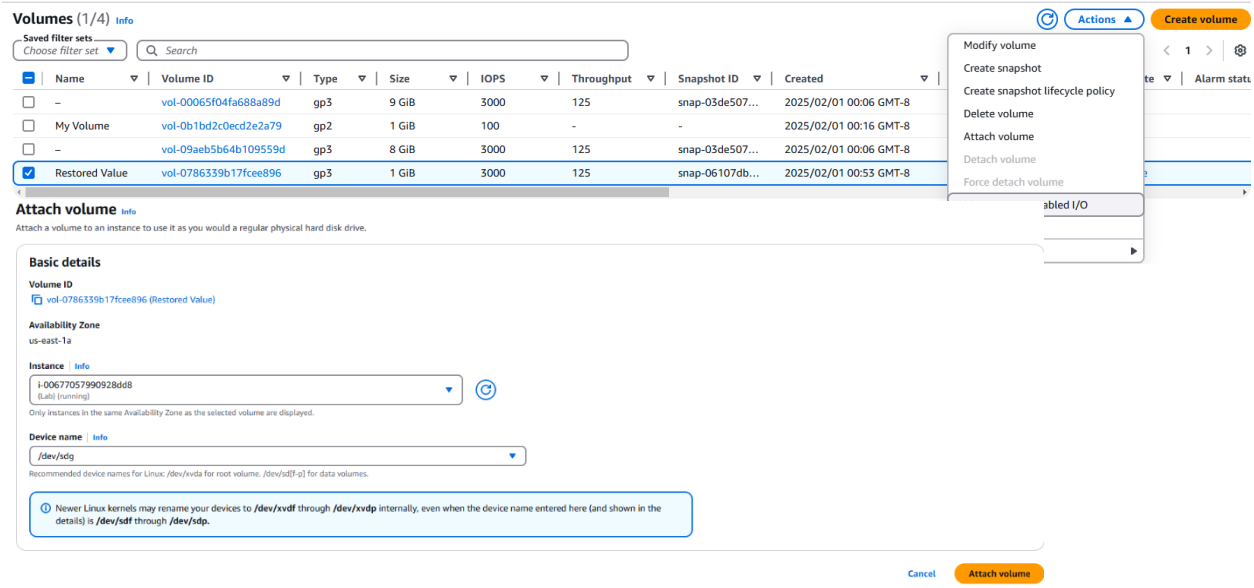
Steps 10: choose Snapshot, at first it will show pending, but it will change to complected, then go back to the console cli of the instance, type the command **sudo rm /mnt/data-store/file.txt**, verify that the file has been deleted by typing **ls /mnt/data-store/**



Steps 11: Go back to EC2 console, select My Snapshot, in action menu, select create volume from snapshop, for availability zone, select the same availability zone that you used earlier, choose add tag then configure key to be Name, value to be Restored Volume, then choose Create volume



Steps 13: choose volumes in the left navigation pane, select restored Volume, select Restored Volume, in actions menu select Attach volume, choose the Instance field , then select the Lab instance, note that the device field set to /dev/sdg, choose attach volume



Steps 14: Go back to CLI of the instance type **sudo mkdir /mnt/data-store2** to Create a directory for mounting the new storage volume. Mount the new volume by **sudo mount /dev/sdg /mnt/data-store2**, verify that volume you mounted has the file that you created earlier by typing **ls /mnt/data-store2/** and there are still have the file.txt

```
[ec2-user@ip-10-1-11-8]
file.txt  lost+found
```

Steps 15: click submit than ■ End Lab

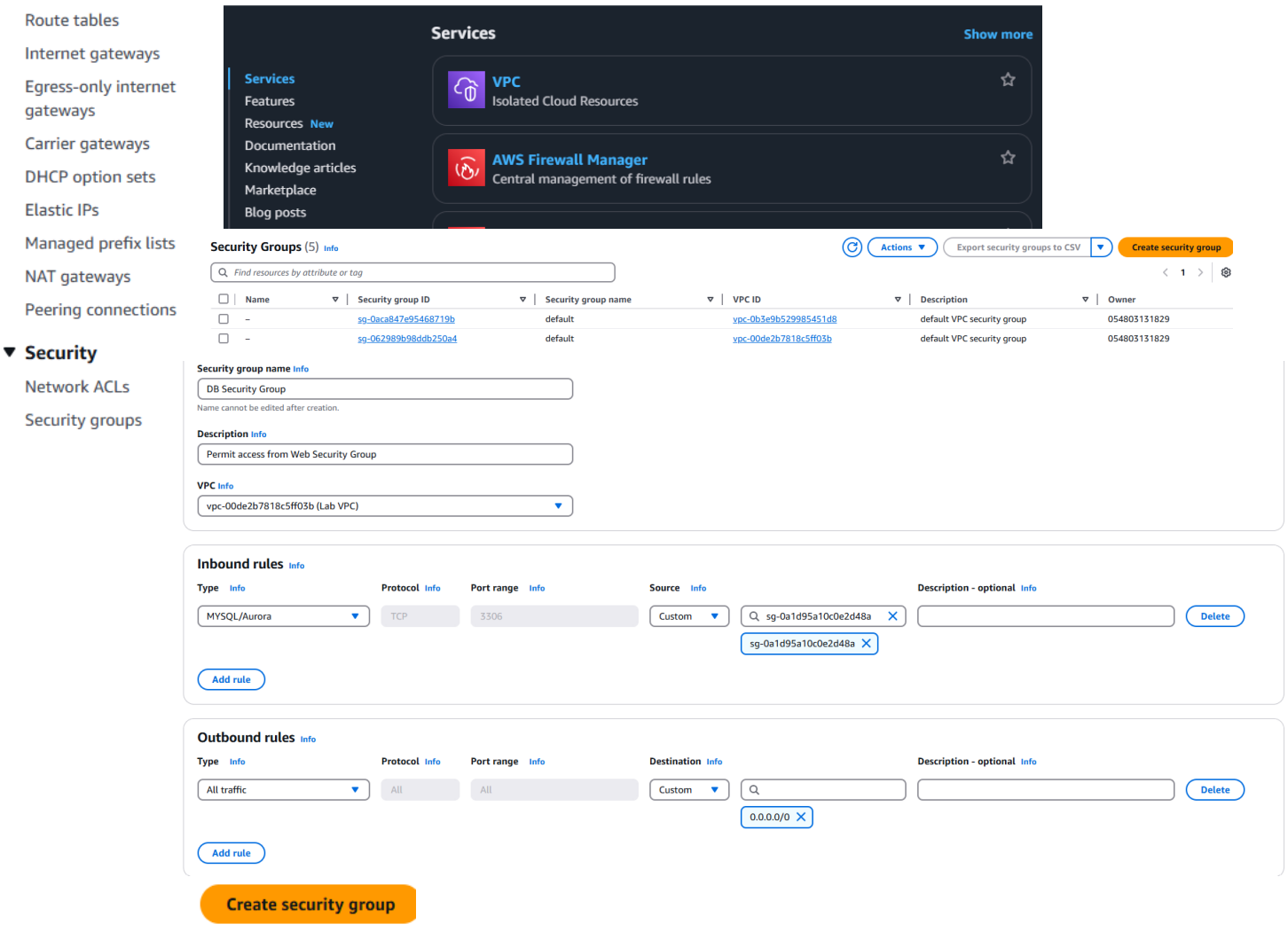
Submit | Submission Report | Grades

Lab 5:

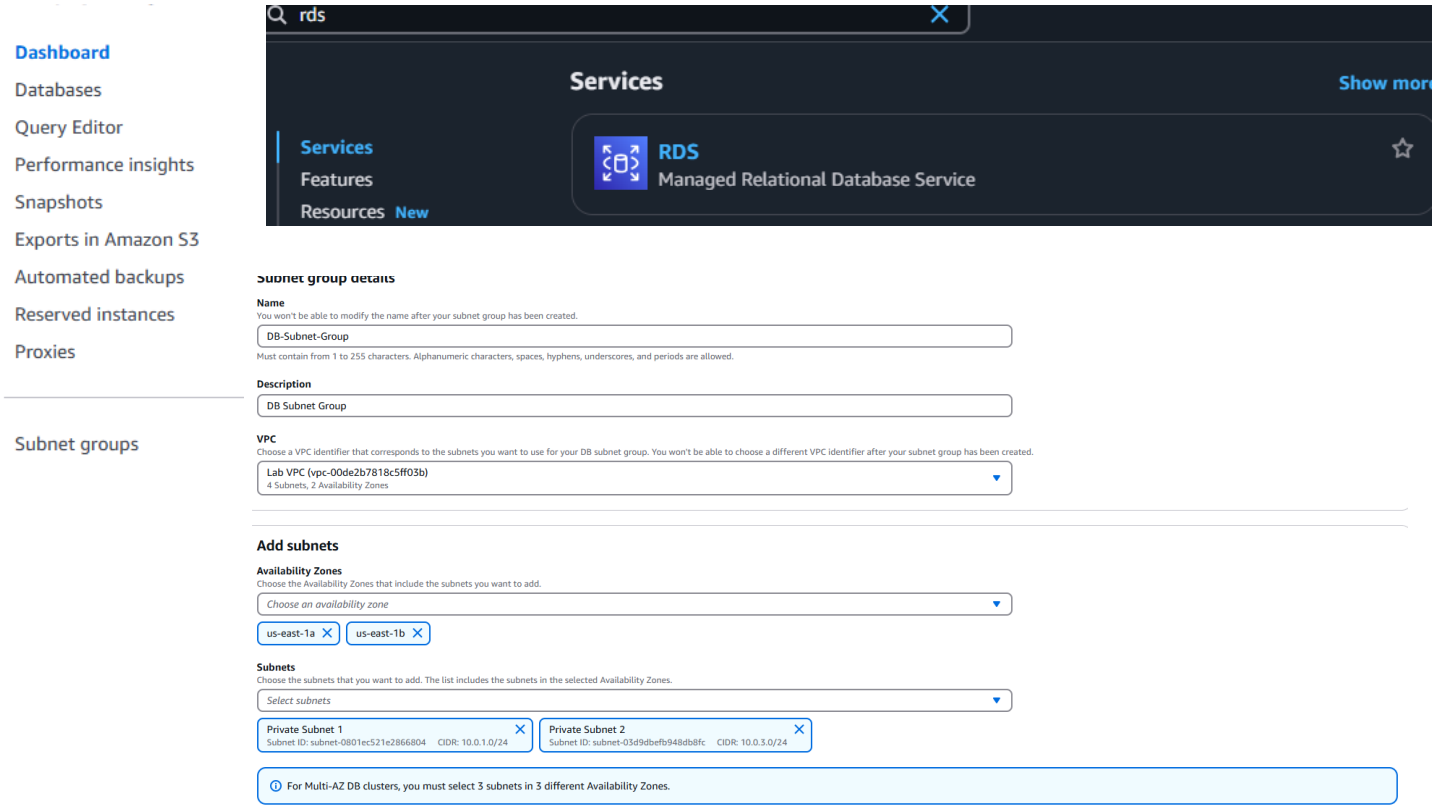
Step 1: click on start lab and wait for AWS line to turn green, then click on the link

Start Lab AWS

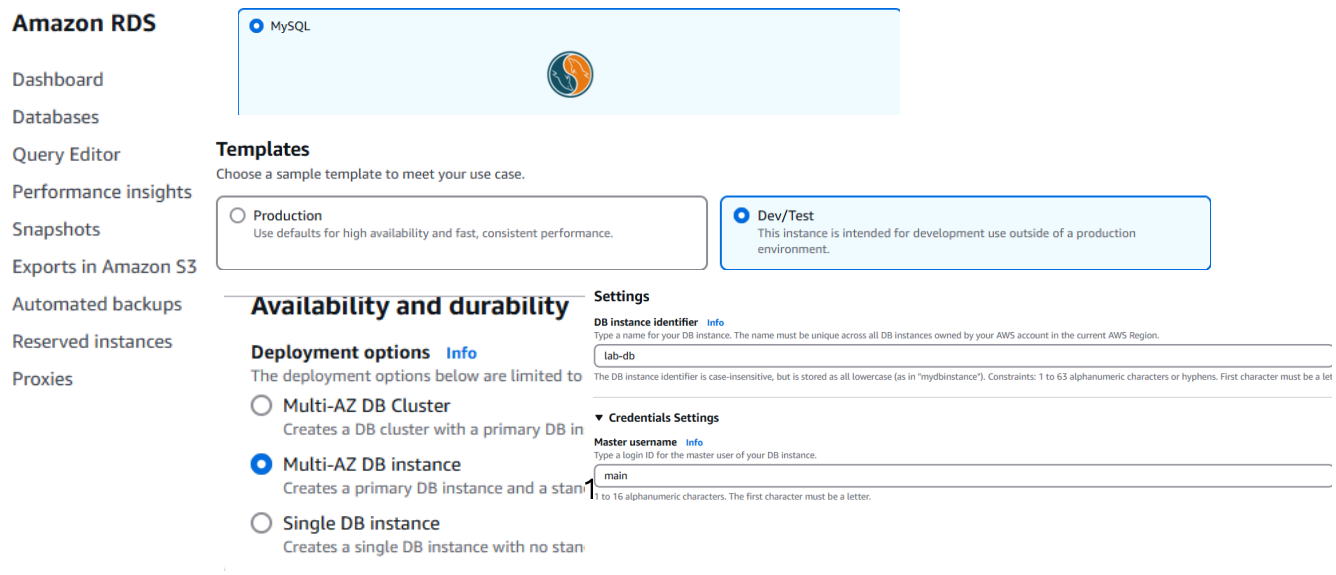
Step 2: search for VPC, then go to security group, then create security group, follow the security group name to be DB Security Group, Description is about Permit access from Web Security Group, VPC need to choose Lab VPC, add new inbound rule, type is MYSQL/Aurora, then type sg on source then selected Web Security Group, then click create security group



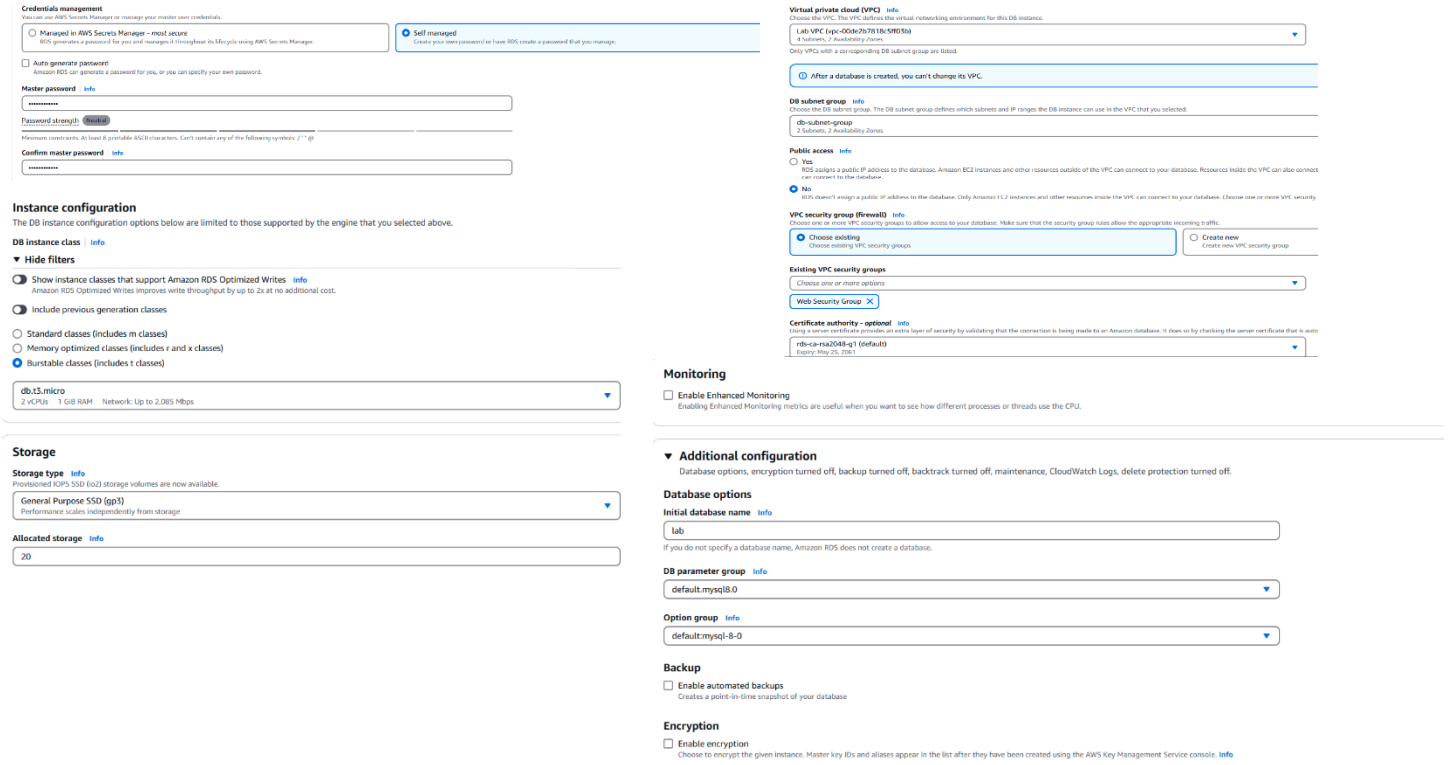
Steps 3: go to Service, then type RDS, in the left navigation pane, choose subnet groups, click on create DB subnet group, name to be DB-Subnet-Group, Description to be DB Subnet Group, then select Lab VPC, scroll down to the add subnets section, expand the list under availability Zones, select us-east-1a and us-east-1b, expand the list under subnets and choose 10.0.1.0/24 and 10.0.3.0/24, then choose create



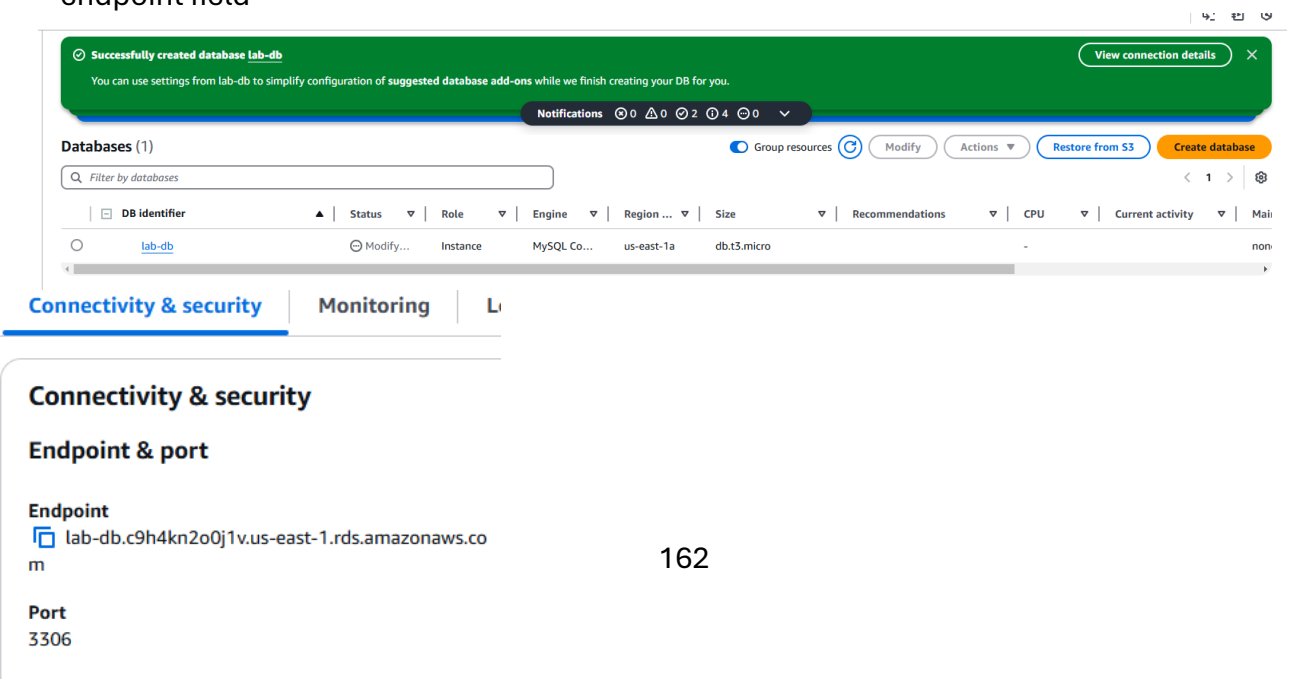
Steps 4: click on databases, choose create database, then, select MySQL, choose Dev/test, under availability and durability, choose Multi-AZ DB instance, under settings, config DB instance identifier to be lab-db, master username to be main,



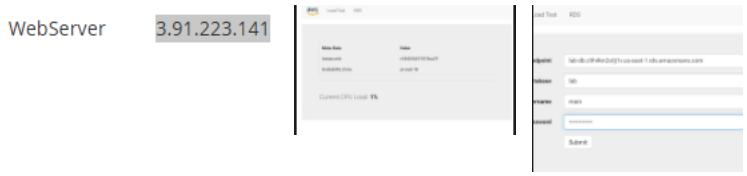
Step 4.5: Credentials management need to choose self managed, than enter password lab-password and reenter it at confirm master password. Instance configure to be Burstable classes, then allocated storage to be 20 GiB, under connectivity configure Lab VPC, under existing VPC security groups, choose DB Security Group, Deselect default, scroll down to monitoring, uncheck enable Enhanced Monitoring, expand Additional configurations, initial database name to be lab, uncheck both enable encryption, and automated backups, then click create database



Steps 5: click on the lab-db scroll down to the connectivity and security and copy the endpoint field



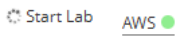
Steps 6: click on AWS Details , then find the Web Server ip, go to the website by entering the ip for your WebServer, than go to RDS and enter the endpoint, then Database, Username and password, for me I only can reach that website and enter the credentials, but I cannot edit any information because there are no respond after I entered my credentials.



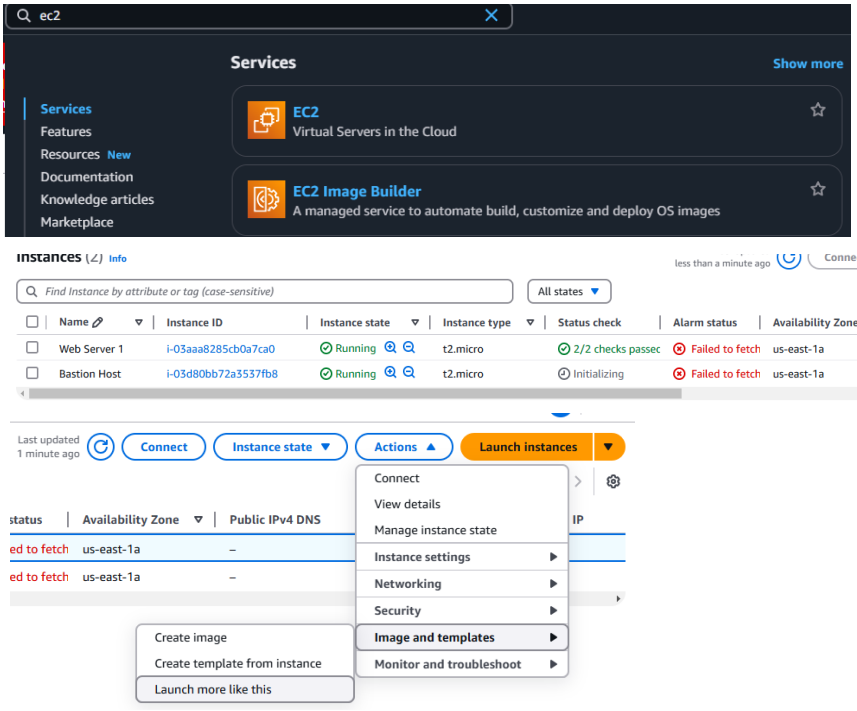
Steps 7: click submit than End Lab

Lab 6:

Step 1: click on start lab and wait for AWS line to turn green, then click on the link

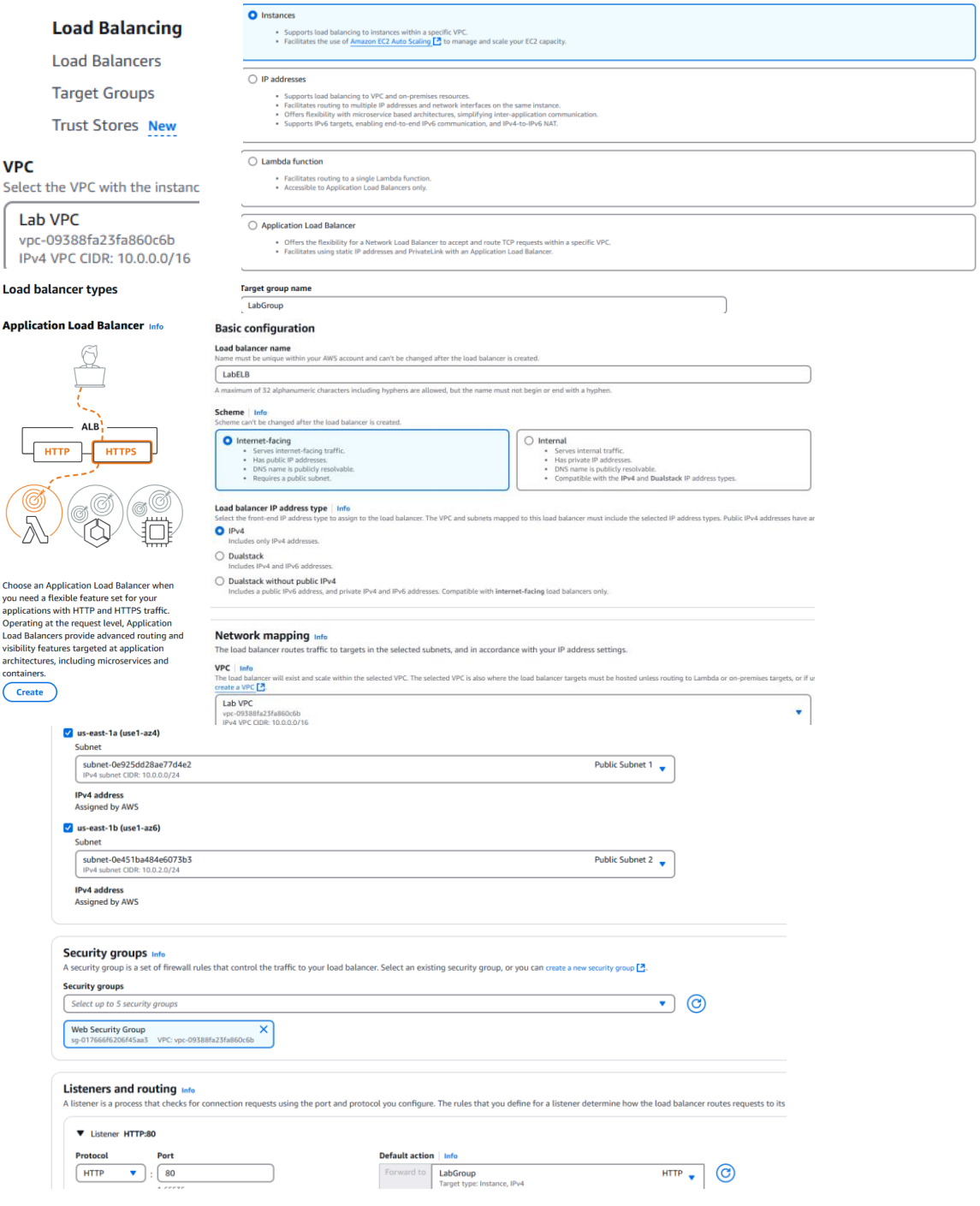


Step 2: search for Ec2 and go to instances, make sure web Server 1 is working, click on actions, choose image and templates, than choose create image

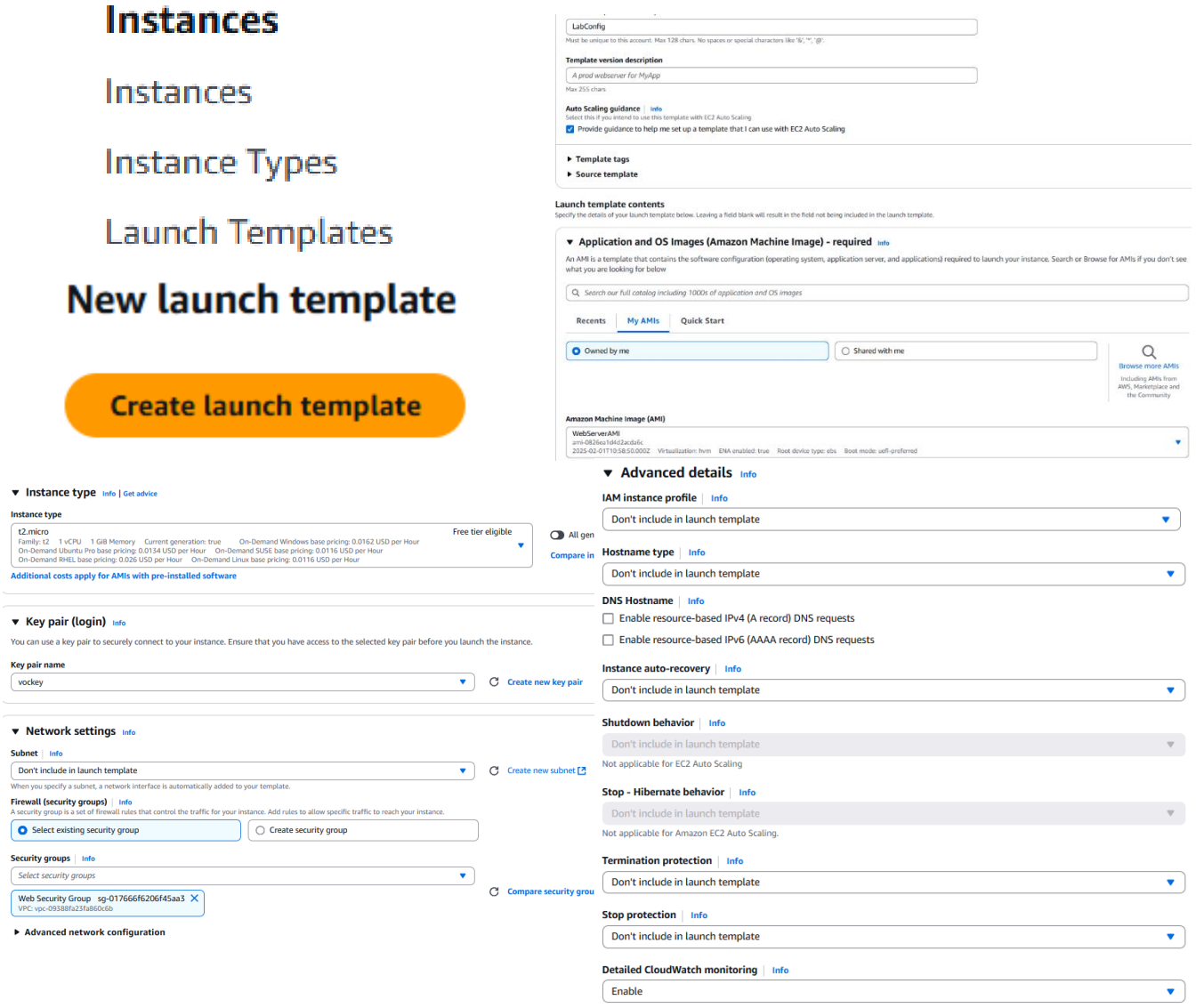


Step 3: Make the image name to be WebServerAMI and the description about Lab AMI for Web Server, then choose create image

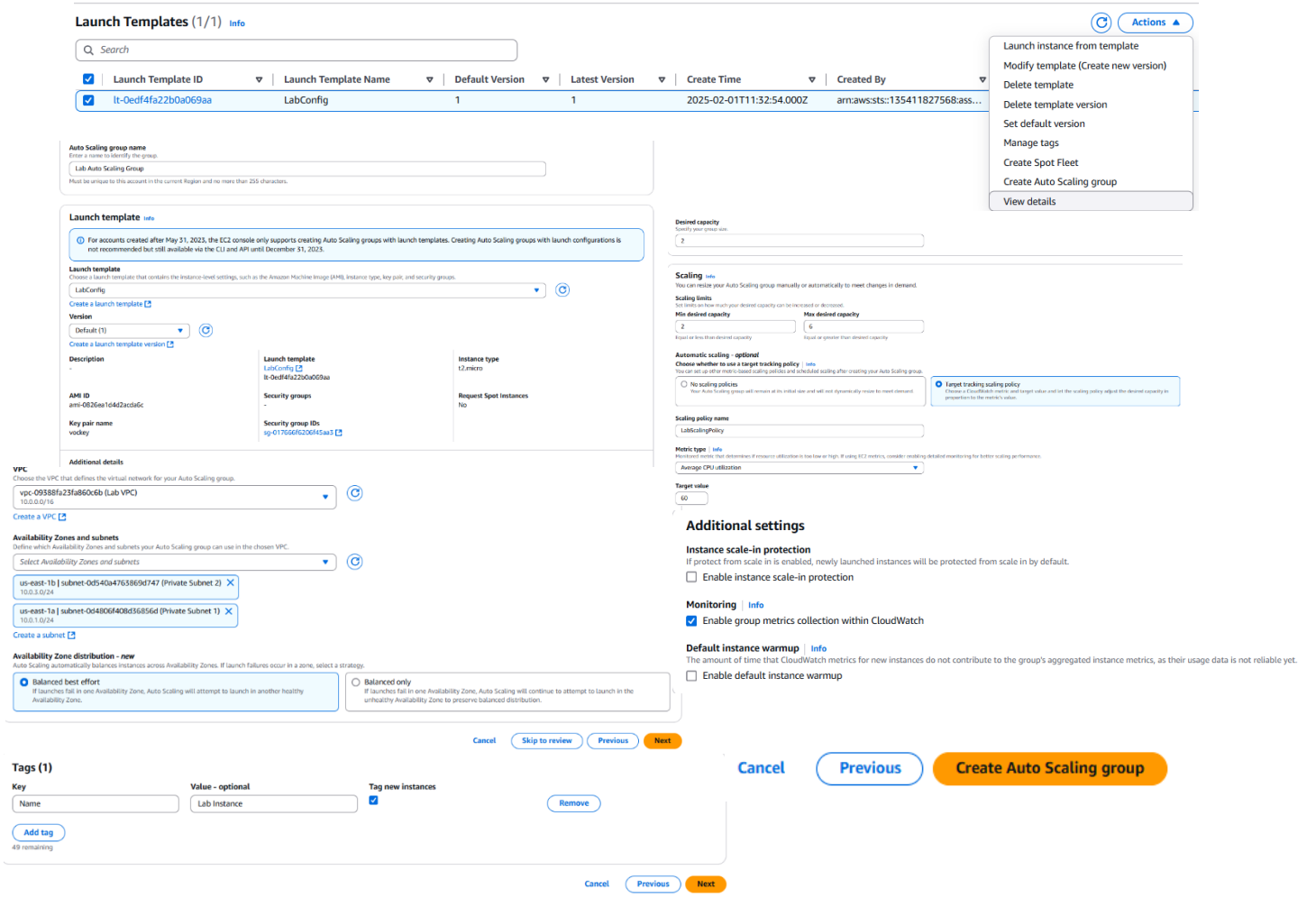
Step 4: choose target group, click create target group , choose a target type to be instances, target group name to be LabGroup, select Lab VPC from the VPC drop-down menu, click on next , review the settings than click Create target group, click on Load Balancers at the left navigation pane, click on create load balancer, choose application load balancer, Under Load Balancer name enter Lab ELB, scroll down to the Network mapping, for vpc choose Lab VPC, check all availaility Zones, select public subnet 1 and 2, go down to security group check Web security group and uncheck default, add the LabGroup to the default action than click



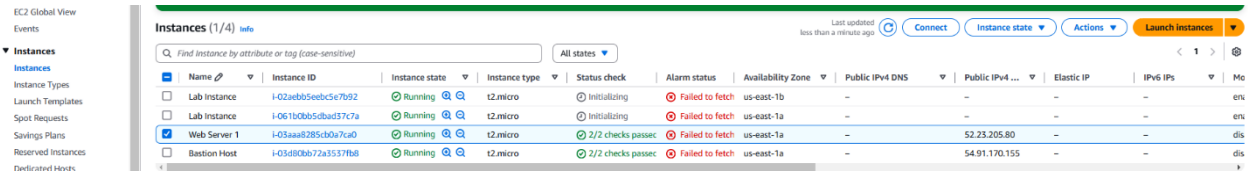
Steps 5: In the left navigation pane, choose Launch Templates and choose Create launch template, launch template name to be LabConfig, under Auto Scaling guidance, select provide guidance to help me set up a template, In application and OS image, choose My AMIs. AMI choose Web Server AMI, Instance type choose t2.micro, key pair name choose vockey, firewall(security group) choose select existing security group, check web Security Group, scroll down to the Detailed Cloudwatch monitoring setting, select enable, at the end choose Create launch Templates



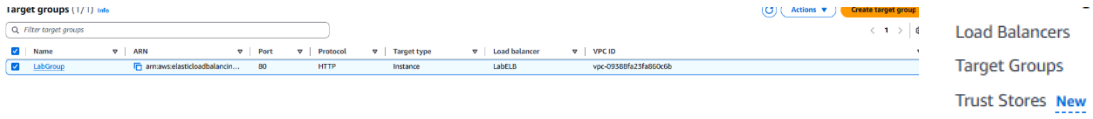
Step 7: go back to launch templates, click on the one we just created, go to action and choose create auto scaling group, enter the name Lab Auto Scaling Group then click next, choose Lab VPC, select Private subnet 1 and 2 and click next, click attach to an existing load balancer, choose LabGroup, and click Next, set desired capacity to 2, min desired capacity to 2, max desired capacity to 6, select target tracking scaling policy, name is LabScalingPolicy, set the metric type to average CPU utilization, set target value to 60, and select enable group metrics collection within CloudWatch, then hit next, hit next again, click on add tag, key to be name and value to be Lab Instance and hit next and scroll down and click on Create Auto Scaling group

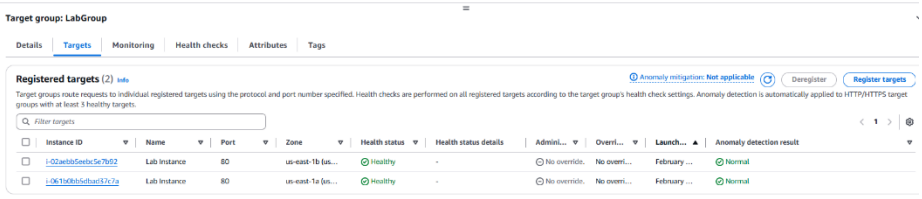


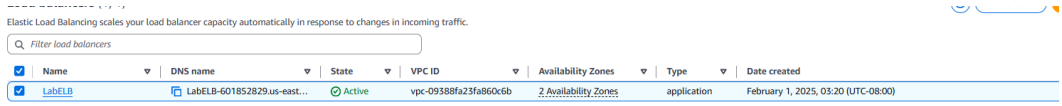
Step 8: When you click on Instances, it should have 2 more instances called Lab Instance

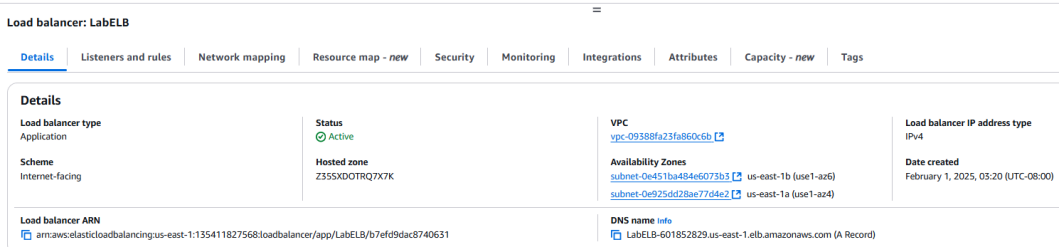


Step 9: click on Target Group, click on LabGroup, choose the target tab, there should have 2 targets, then choose load balancers, select that load balancers, copy the DNS name

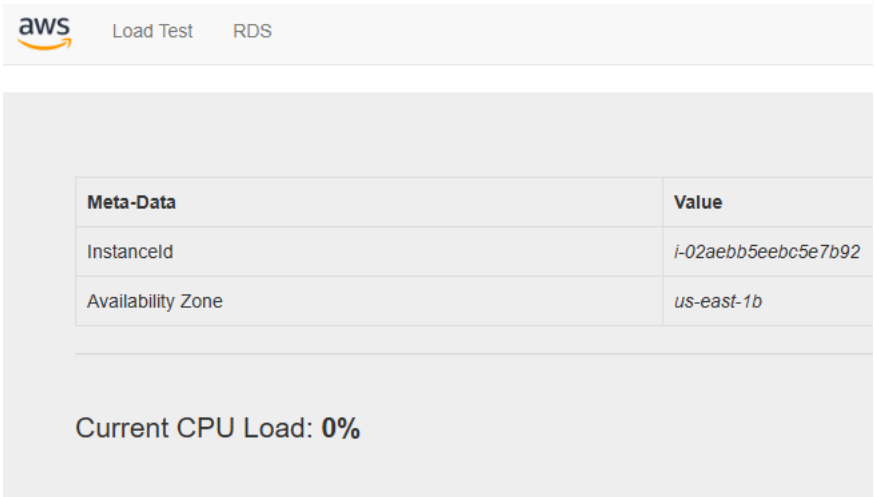




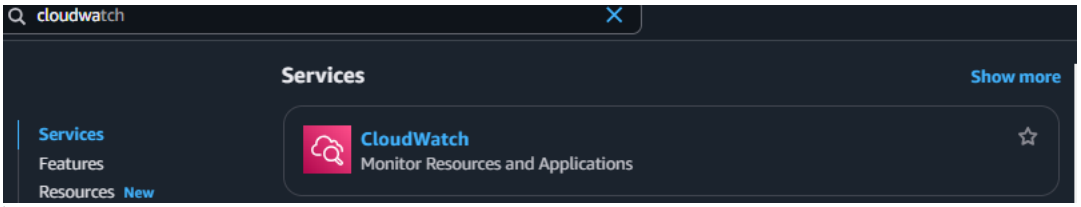




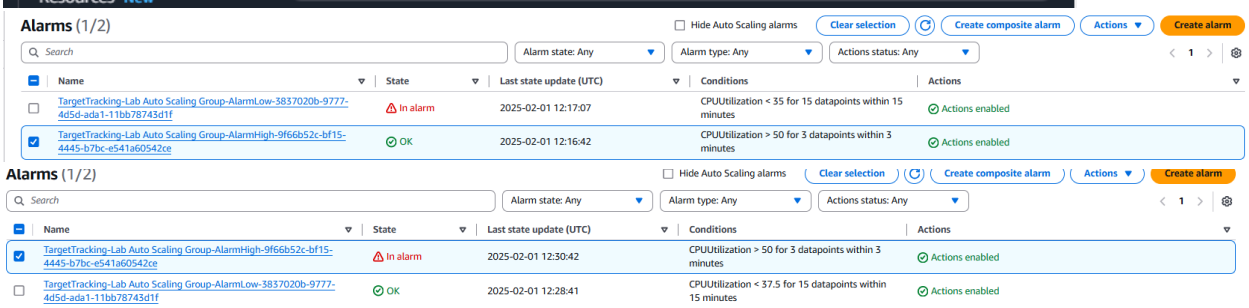
Step 10: paste the DNS name to browser and connected to the web server



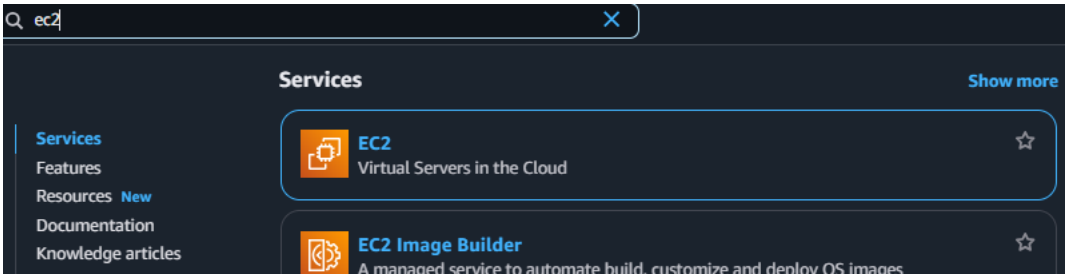
Step 11: search for cloudwatch, choose all alarm in alarm tab, there are two alarms, click on load test on your web server and wait until alarm high from ok turn to in alarm

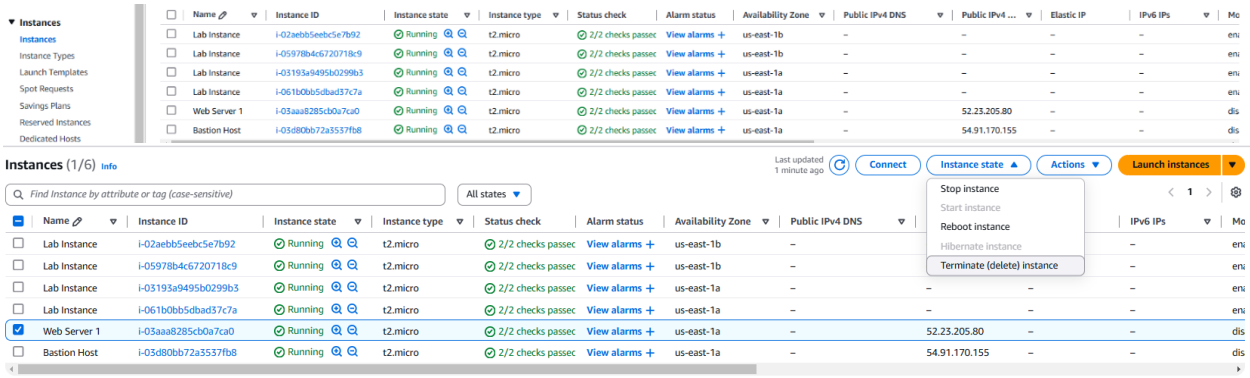


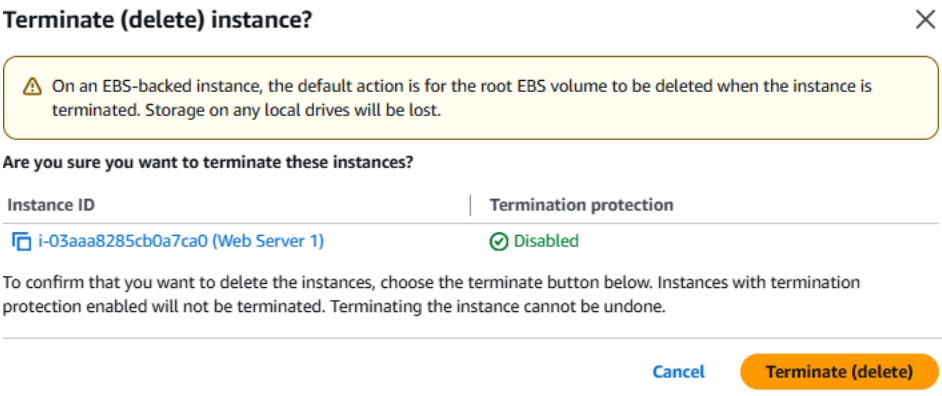
Load Test

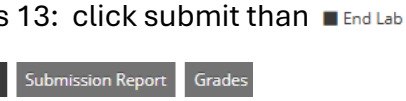


Step 12: go back to EC2 and noticed that are two more instance, selected Web Server 1, then click terminate it and confirm terminate it







Steps 13: click submit than 

Problems: For these three labs, the only problems I faced is I cannot connect to the RDS and change the information there, after I entered my credentials, there are no response and redirected me back to the login page, so I cannot do the part that add, editing and removing contacts at the database.

Conclusion: In conclusion, these labs help me know more about AWS and cloud computing. In these labs, I learned more about EBS, VPS, RDS DB, AMI, load balancers, launch templates, auto scaling and cloudWatch alarms. By doing this lab, I knew more about AWS and it can help me prepare for future job situations.

Fortinet SOHO with wireless WPA2-PSK and Enterprise

By Alvin Chow

Purpose: In this lab, we learn how to config a Fortinet FortiGate 40f for SOHO environment, we learned how to secure and manage network traffic effectively. We also learn how to set up a Fortinet AP by create and set up 2 SSID, one is for WPA-2 PSK and one is for WPA-2 Enterprise. This lab gave us hand-on experience with both FortiGate firewall and Fortinet AP.

Background Info:

Fortinet is a global cybersecurity company that provides a wide range of security solutions designed to protect networks, data, and devices. Known for its high-performance security appliances, Fortinet specializes in next-generation firewalls, secure wireless solutions, intrusion prevention systems, and secure access products. Fortinet's flagship product, the FortiGate firewall, is widely used across various industries to safeguard networks from cyber threats.

The FortiGate 40F is a compact yet powerful next-generation firewall designed for small office and home office environments. It offers advanced security features such as intrusion prevention, VPN support, antivirus, web filtering, and application control. The device is known for its high-performance throughput and ease of management, making it an ideal solution for small businesses looking to protect their network with enterprise-grade security.

The Fortinet Access Point is designed to provide secure, high-performance wireless connectivity. Fortinet APs are seamlessly integrated with FortiGate firewalls, allowing for centralized management and robust security features. They support various wireless standards, including WPA2-PSK and WPA2-Enterprise, providing flexible options for securing wireless networks based on different security needs. These APs are perfect for businesses looking for secure and scalable wireless networking solutions.

WPA2-PSK is a wireless security protocol that uses a shared password (or passphrase) for authentication. It is simple to set up and ideal for home or small office environments.

WPA2-Enterprise offers a more advanced and secure method of authentication. It uses a RADIUS server or local database for user authentication, providing unique credentials for each user. This allows for better control over who accesses the network, making it ideal for business or organizational environments where security, monitoring, and individual access management are priorities.

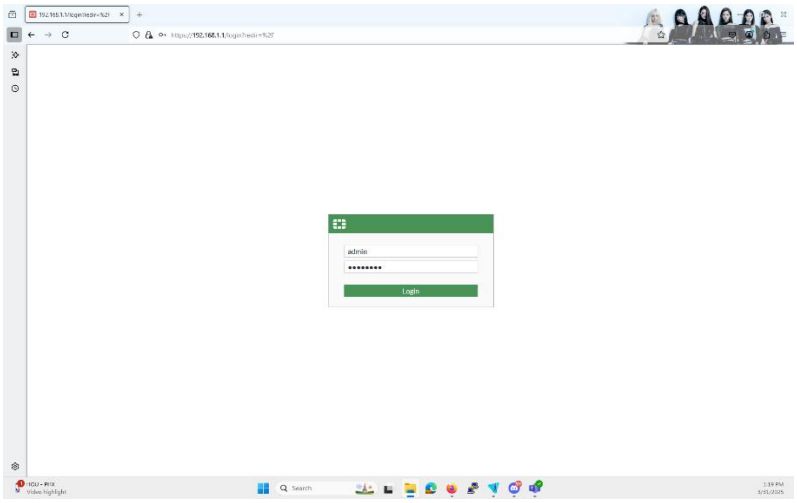
Lab Summary: Step by Step guide of config it

1. We put 2 ethernet cable on the firewall, one on the WAN port and one on the LAN port, then my LAN port is connect to a POE switch, because we need a POE switch

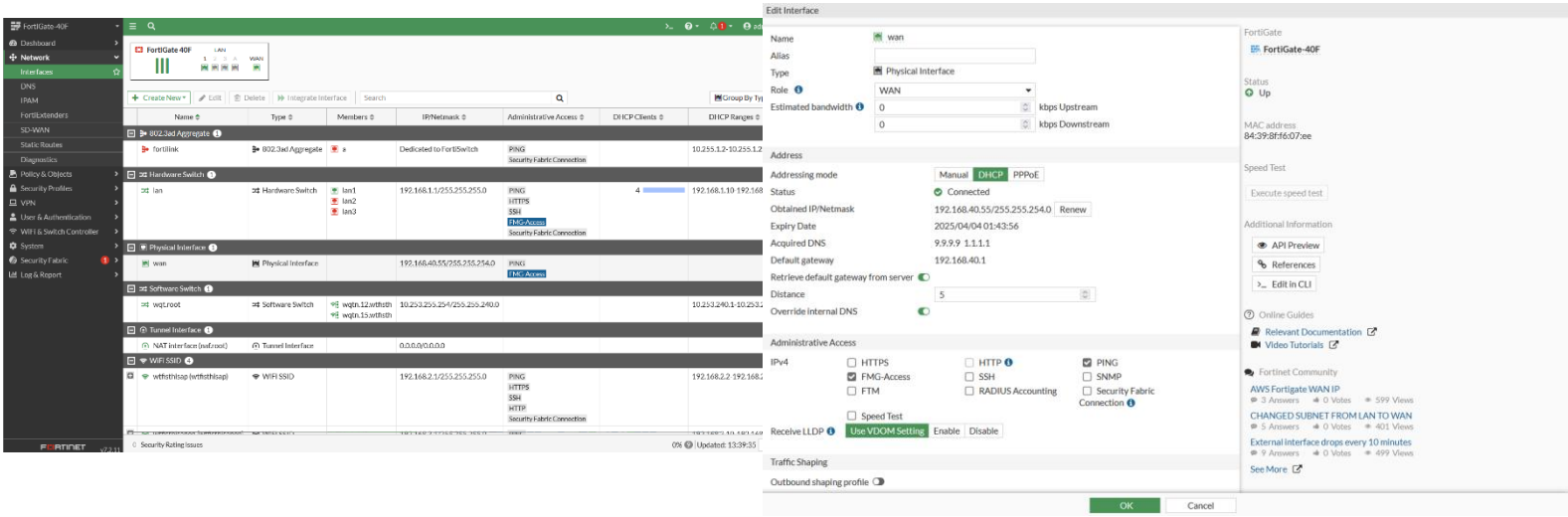
to power the AP, the WAN port is connected to the CCNP network, then connect a pc to POE switch

2. When we received the firewall, it already have the username and password on it, so we don't need to factory reset it, and we noticed we got the IP address from the DHCP server.

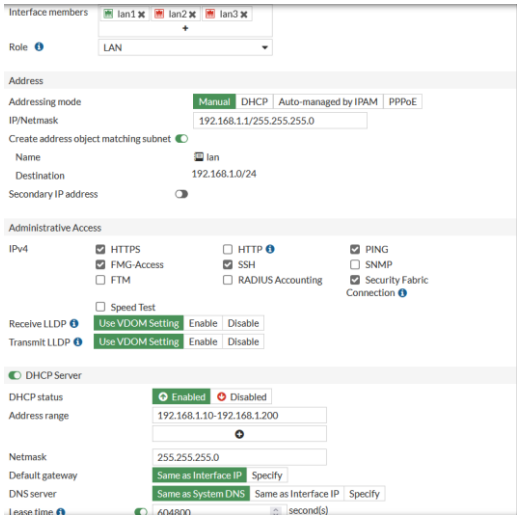
3. Then we enter the ip address of the default gateway, then it bring us to the login page, then we using the password that on the firewall and we login to the firewall.

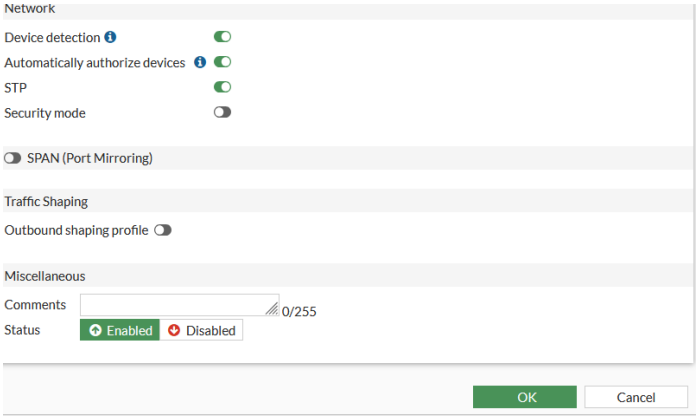


4. Then we go to interface tab and click on WAN, change it to DHCP, then save it

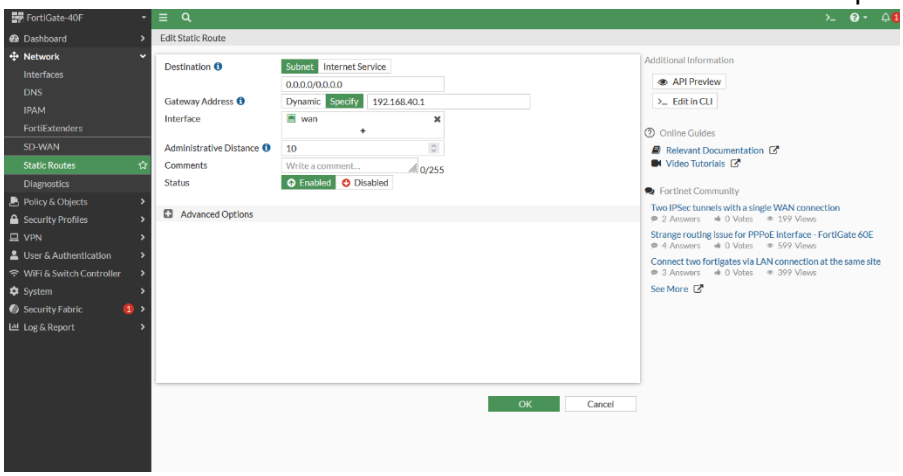


5. Go back to the interfaces list, go to LAN port and set it like this, make sure the security Fabric connection is turn on, enable dhcp server, set the address range that set it like the screenshot, then, scroll down and enable Device detection and automatically authorize devices.

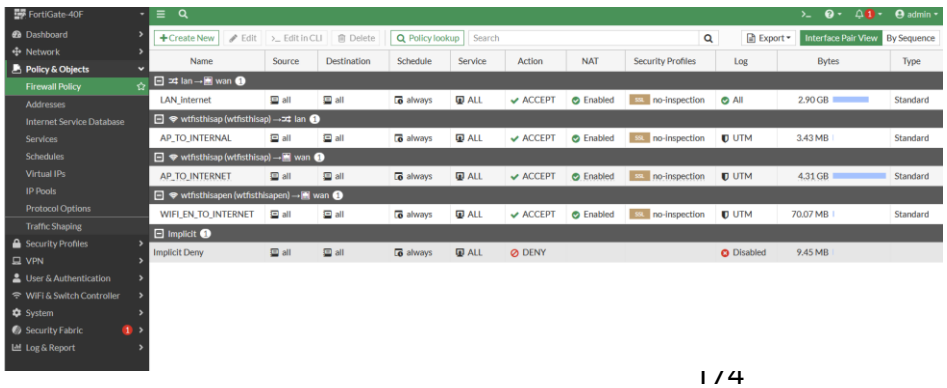


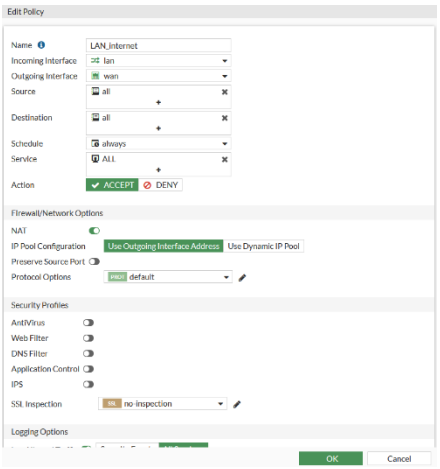


6. Go to static route, set destinations to 0.0.0.0 and the gateway address to 192.168.40.1 because we know that is our next hop address

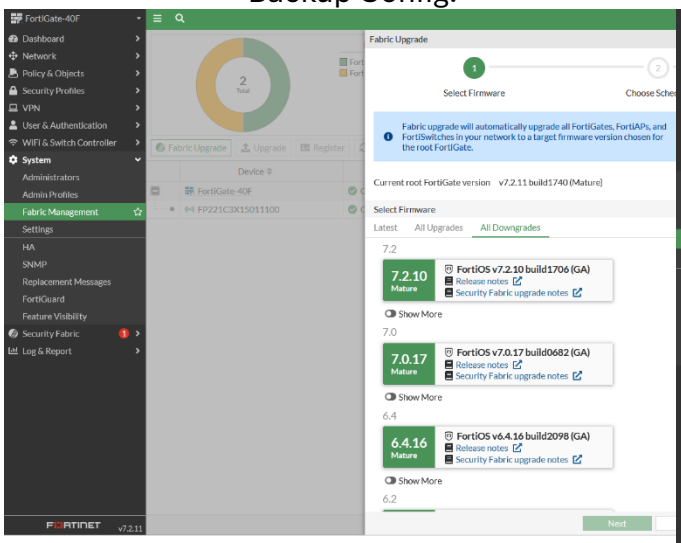


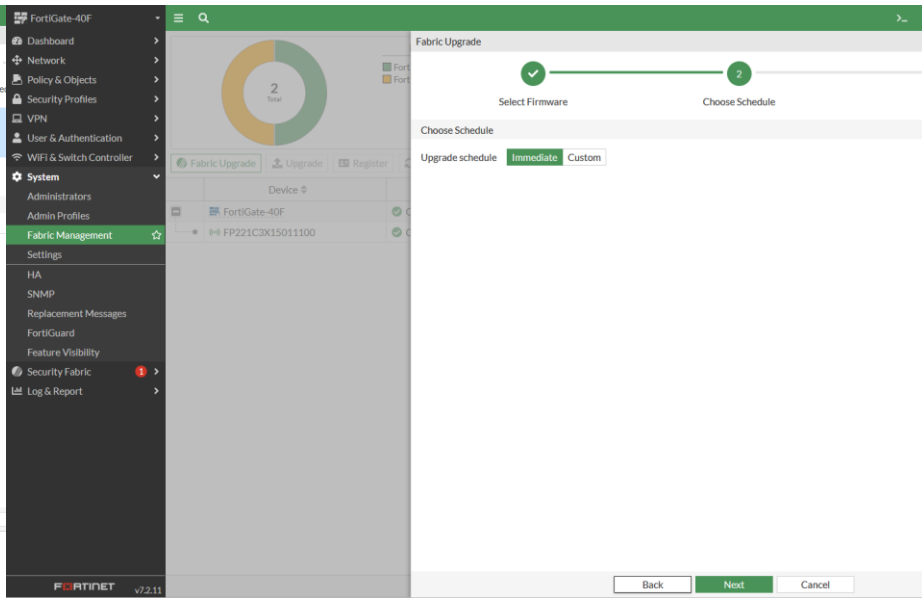
7. Go to policy and create on for LAN to internet, edit that one, set it like the screenshot

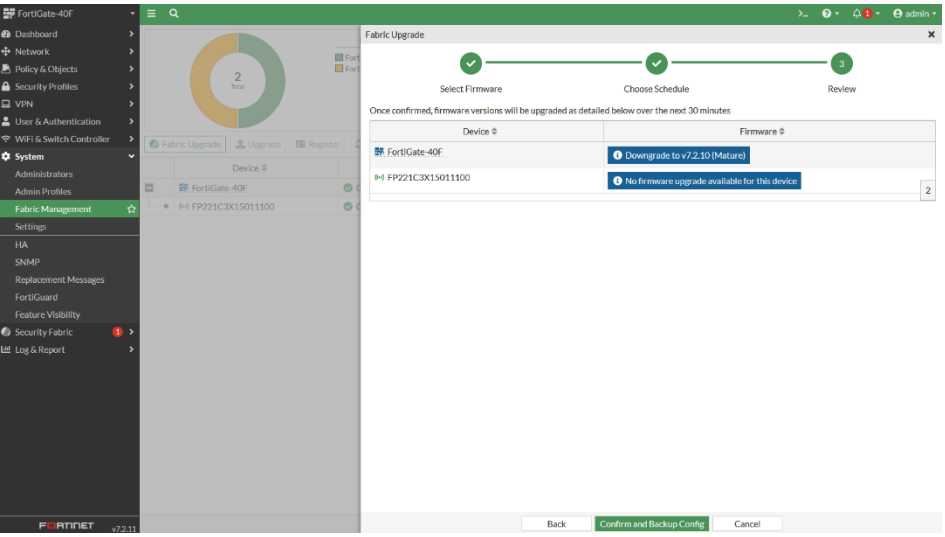




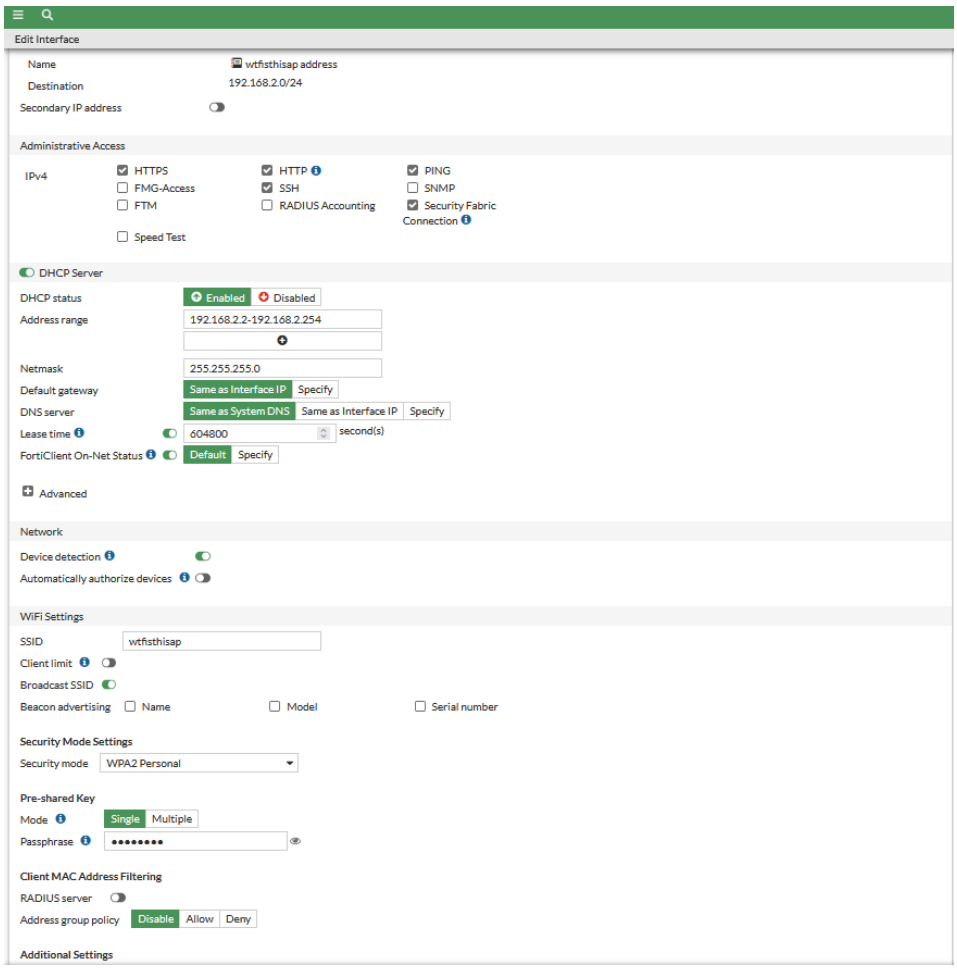
8. Then we noticed the FortiGate firewall cannot find the ap then we noticed the firewall is on version 7.4, which make it cannot found the ap. First we go to settings, fabric management, then click fabric update, click on all downgrades tab, then select firmware version 7.2, click next, click next again, then click confirm and Backup Config.



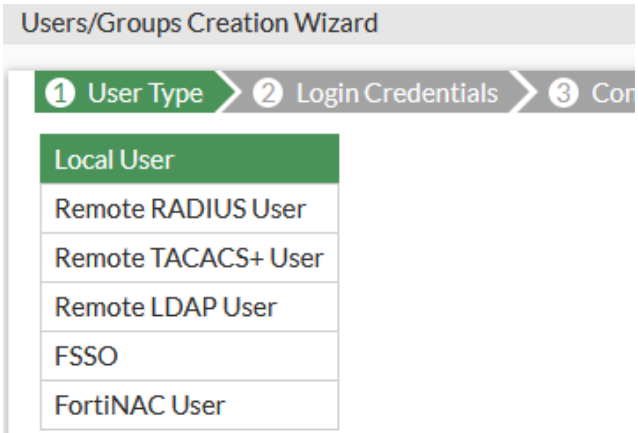


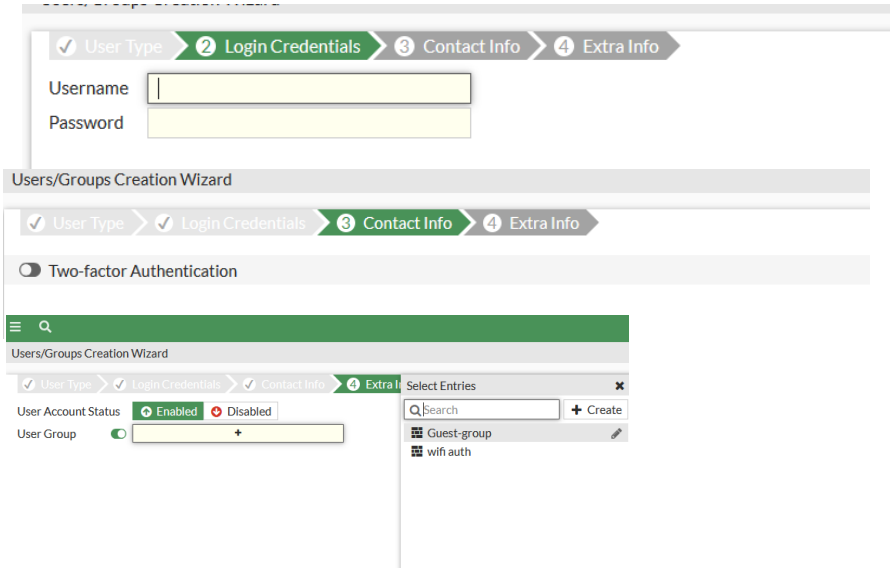


9. After the firewall downgrade it, you can go to wifi and switch controller tab, your ap should be there, click on SSIDS tab create new SSID name is whatever you want, then you can follow this set up, enable DHCP server, set up address range, default gateway that click on broadcast SSID set it to WPA2-Personal and enter the Pre-shared key.

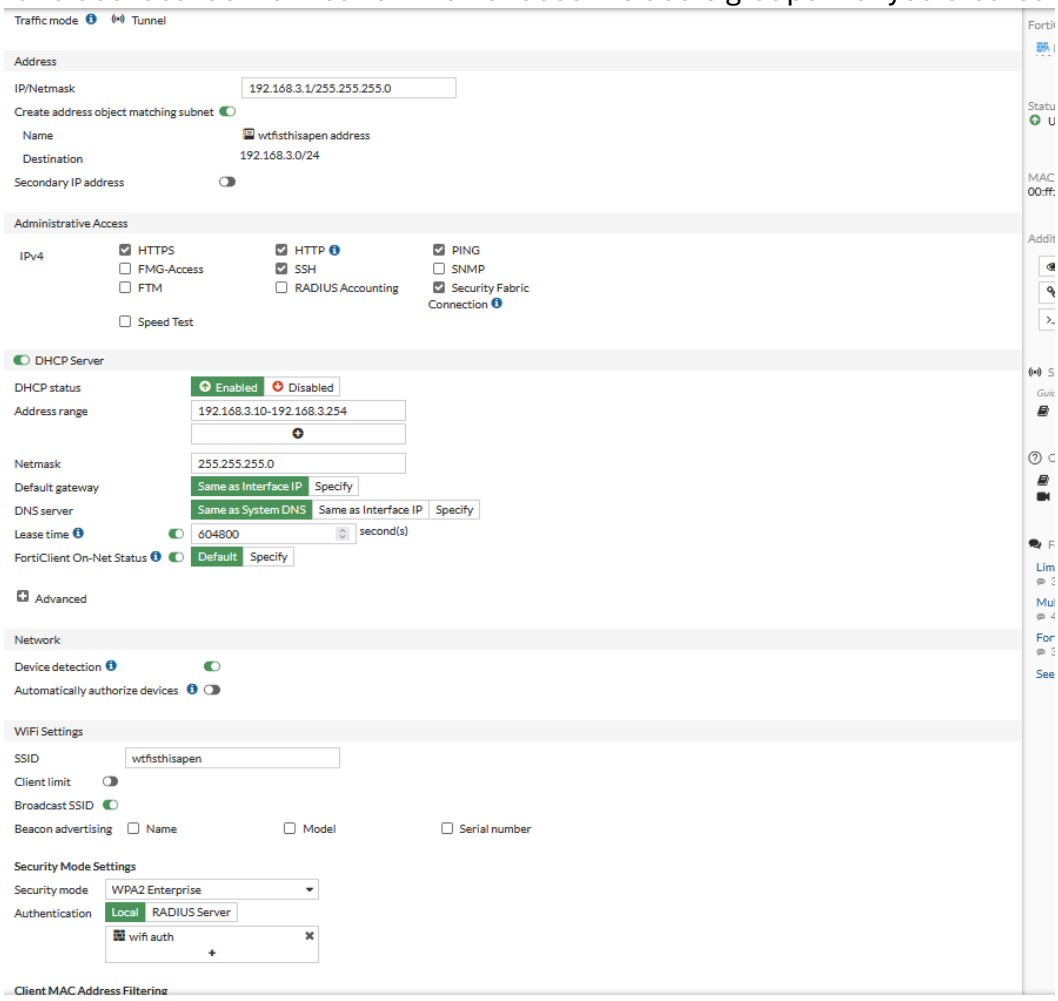


10. Go to User and Authentication, click on User definition create one new user, set it to local user, enter the username and password, click next, disable 2fa, then set it to a User group by create new one by click on create, enter the name and set it to firewall type, and click create, then click submit to create users.

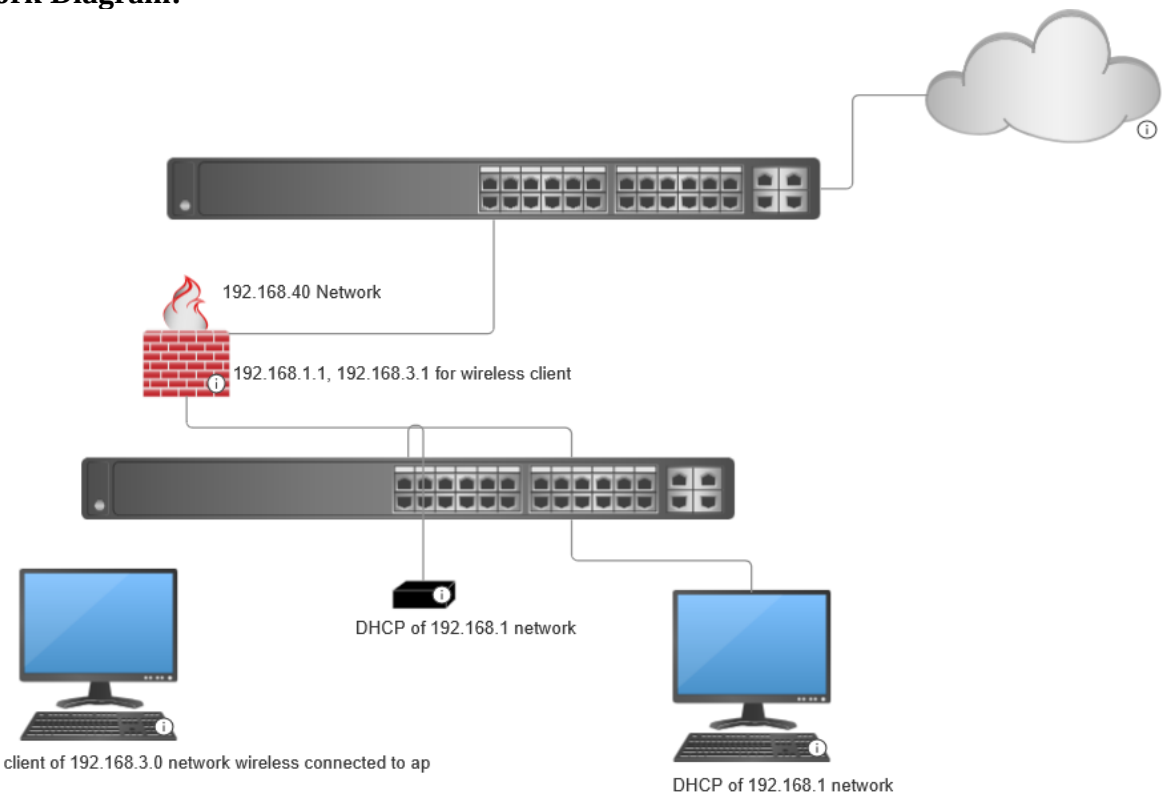




11. Go Back to SSID create the new SSID, enter the name, ip address then enable DHCP, then enter the SSID, broadcast it, set the security mode to WPA2-Enterprise and use local authentication then choose the users groups that you created.



Network Diagram:



Problems: The only big problem that we have is the firewall cannot discover any ap when we trying to config the SSIDs. Then we asked classmate that finish the lab, they told us the firewall need to be on 7.2 version firmware, after we downgrade the firewall, everything is working.

Conclusion: In this lab, we learned how to config the FortiGate firewall with the Fortinet ap, we also learned more about how to config the wireless access point with the firewall act like a wireless LAN controller. In this lab we config the firewall for the SOHO environment which can give me opportunity to learn how to config for my home lab network.

Fortinet SSL VPN Remote Access Lab

By Alvin Chow

Purpose: The purpose of this lab is set up FortiGate SSL remote access which is useful when you trying to access your company data at any location. This is important because it helped us prepare for future job situations, where we need to set up SSL VPN for the organization.

Background info:

A FortiGate firewall is a network firewall developed by Fortinet. It provides advanced protection against cyber threats by combining traditional firewall capabilities with additional features such as VPN support, antivirus, and web filtering. FortiGate devices are widely used in both enterprise and small business environments to protect the networks from unauthorized access and attacks.

A VPN is a service that creates a secure, encrypted connection between your device and a remote server, masking your IP address and protecting your internet traffic. This is useful when using public Wi-Fi networks, it can prevent hackers from intercepting your data.

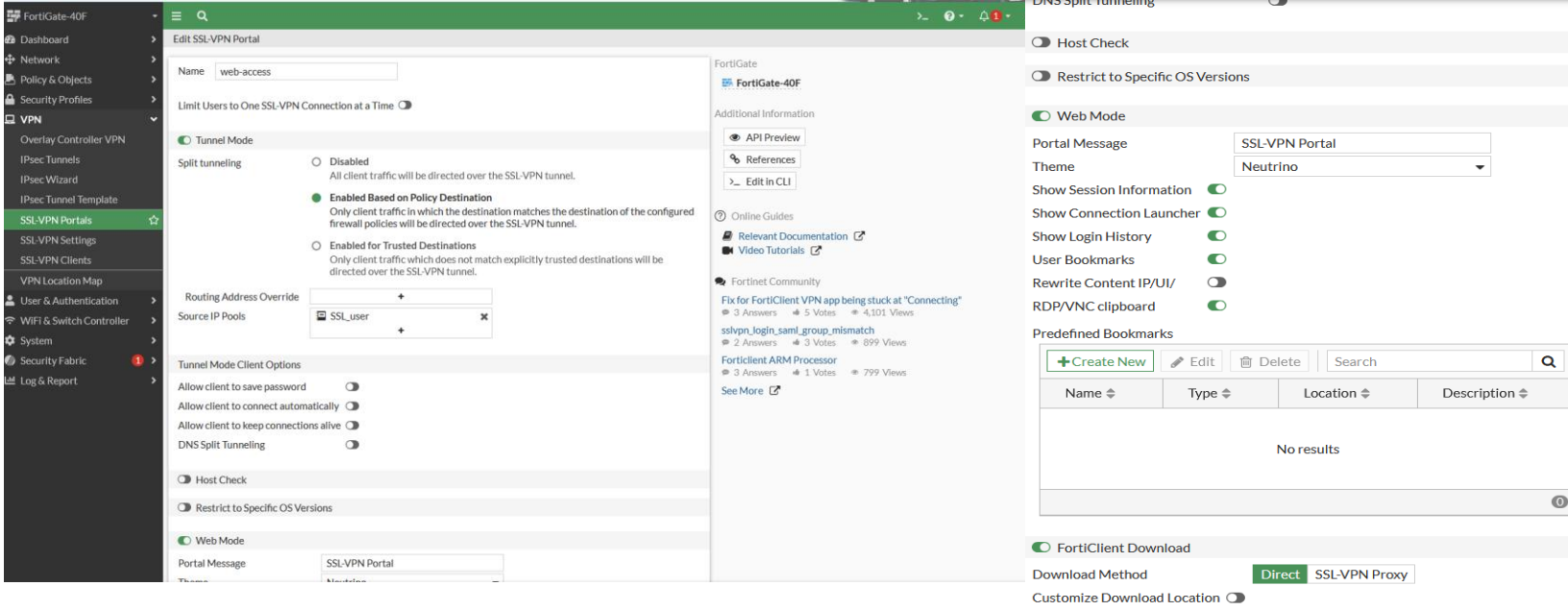
An SSL VPN is a type of VPN that uses the SSL protocol (now mostly using TLS) to secure internet traffic. Unlike traditional VPNs that may require client software, SSL VPNs can be accessed through a standard web browser, making them more convenient for remote access. They are commonly used by organizations to allow employees to securely connect to internal networks from remote locations.

Remote desktop is a technology that allows a user to control a computer from a remote location. This is achieved by transmitting the computer's screen image to the remote device and sending back the user's inputs (keyboard and mouse). It's widely used for technical support, remote work, and accessing files and applications.

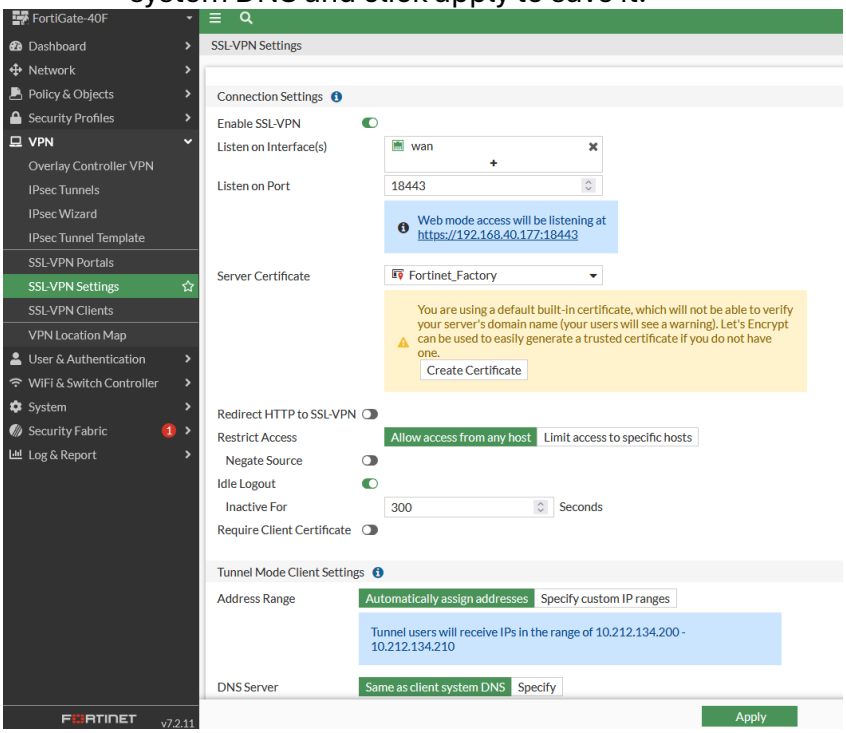
Remote access refers to the ability to connect to a computer or network from a distant location. This can be achieved through various methods, including VPNs and remote desktop software. Remote access is essential for telecommuting, IT support, and accessing resources when away from the office.

Lab summary:

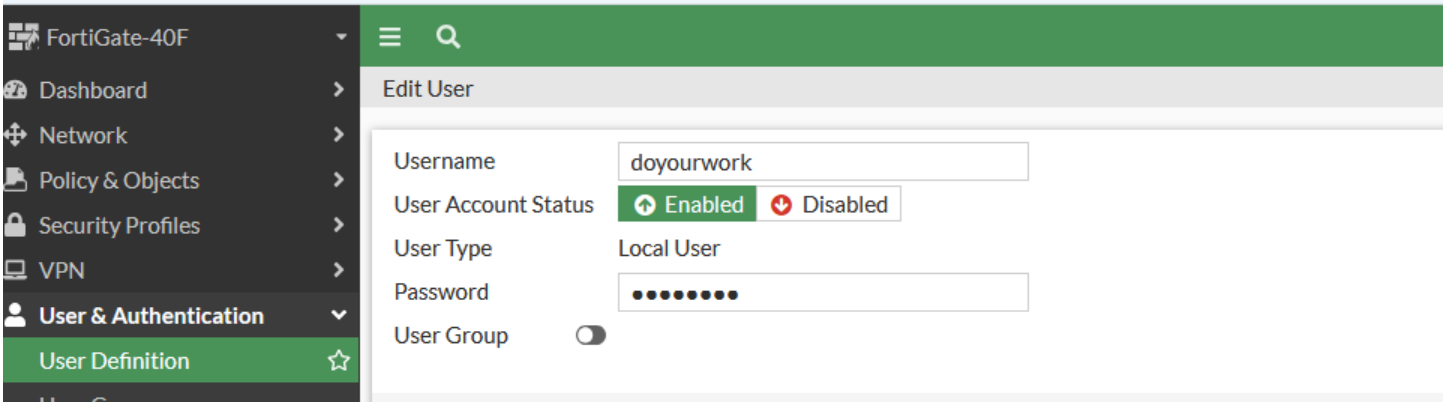
1. Go to SSL-VPN Portal tab, create a new portal name is whatever you want, enable tunnel mode, add the ip range, name is as SSL_user, assign a subnet to it, then enable Web Mode and enable FortiClient Download



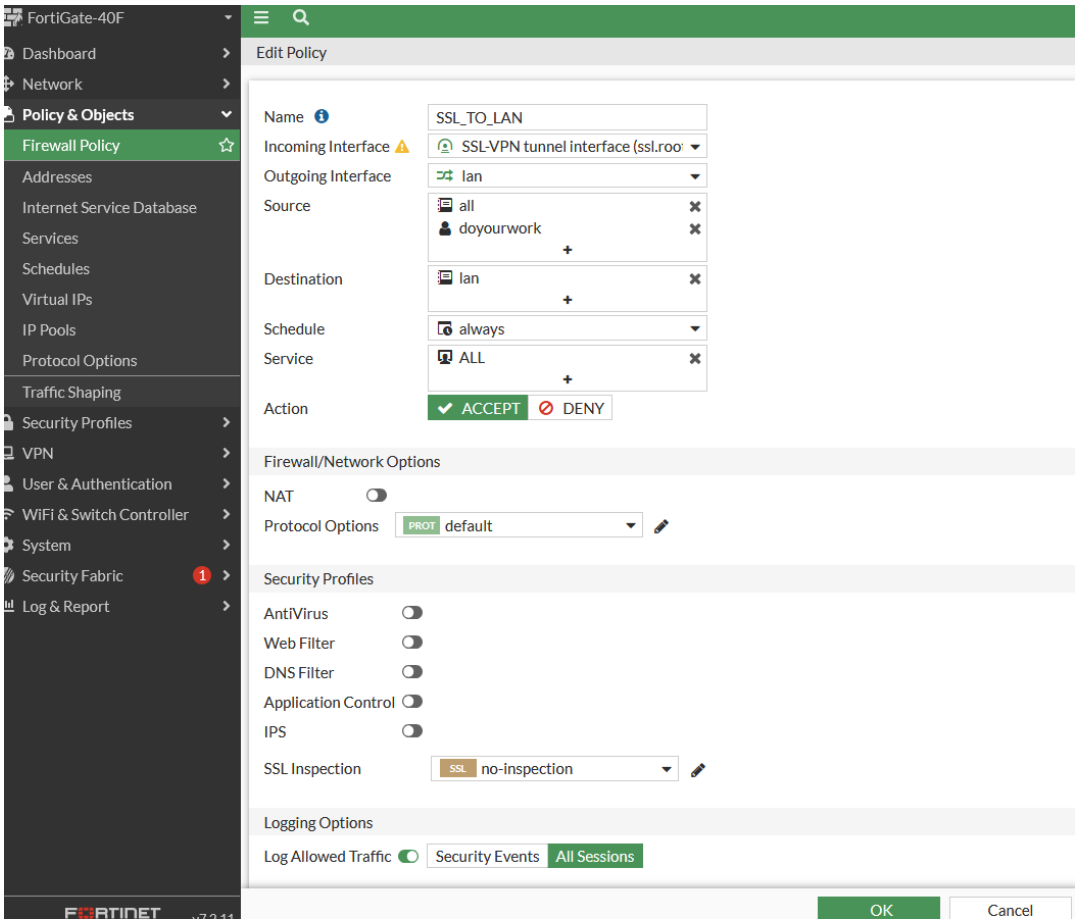
2. Go to SSL-VPN settings, enable SSL-VPN, listen on the WAN interface, use the default Fortinet_Factory Certificate, select Auto assign address and same as client system DNS and click apply to save it.



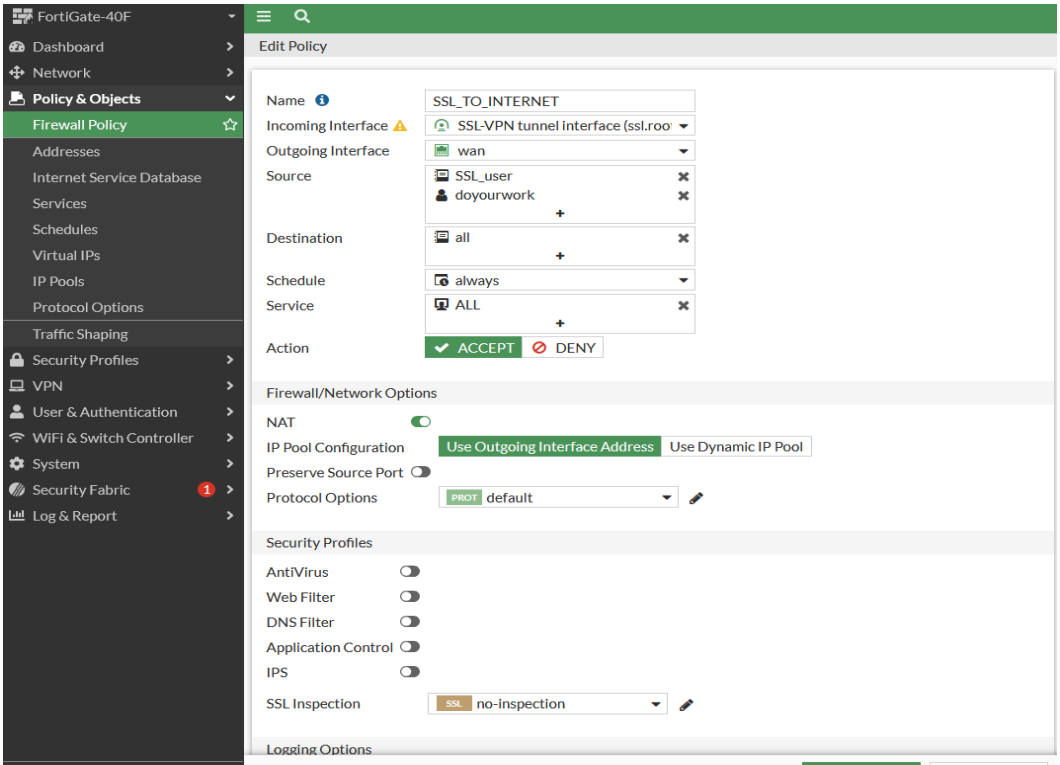
3. Go to User and Authentication, create a new local users, enter the Username and Password



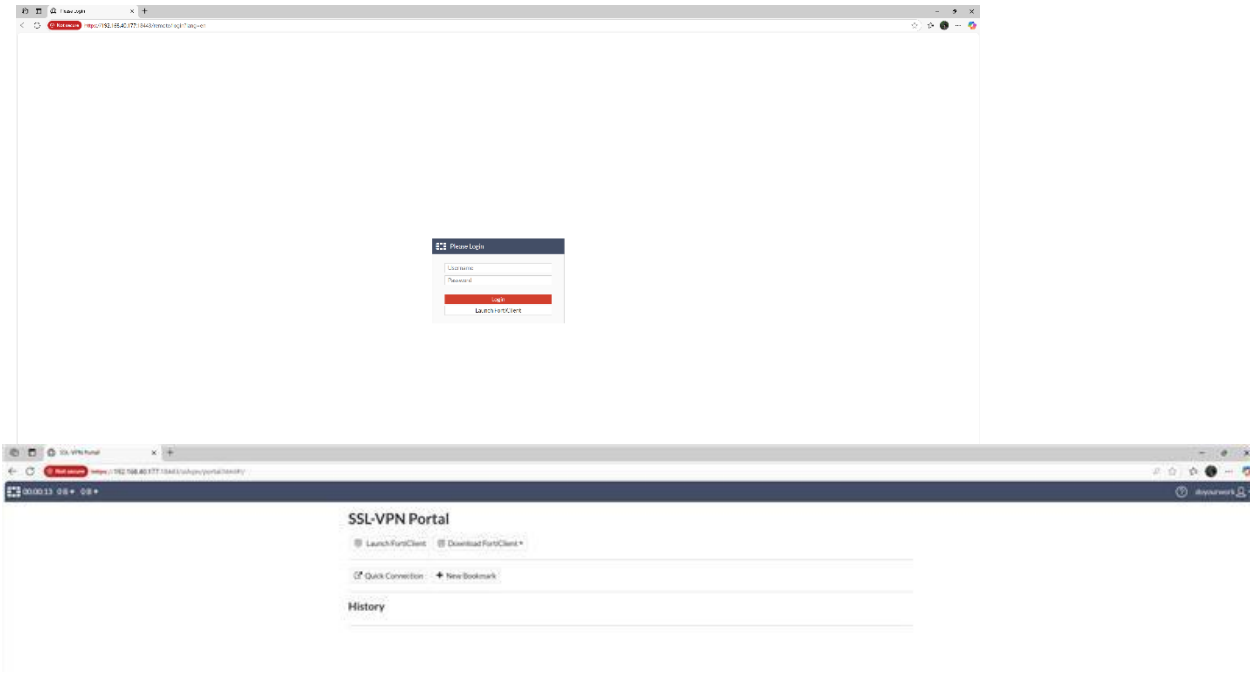
4. Go to Firewall Policy, create a new policy, Incoming Interface set it as SSL-VPN tunnel interface and Outgoing Interface to LAN, Source is All, with only the user that you created and Destination is the Lan interface. Then disable NAT and click create



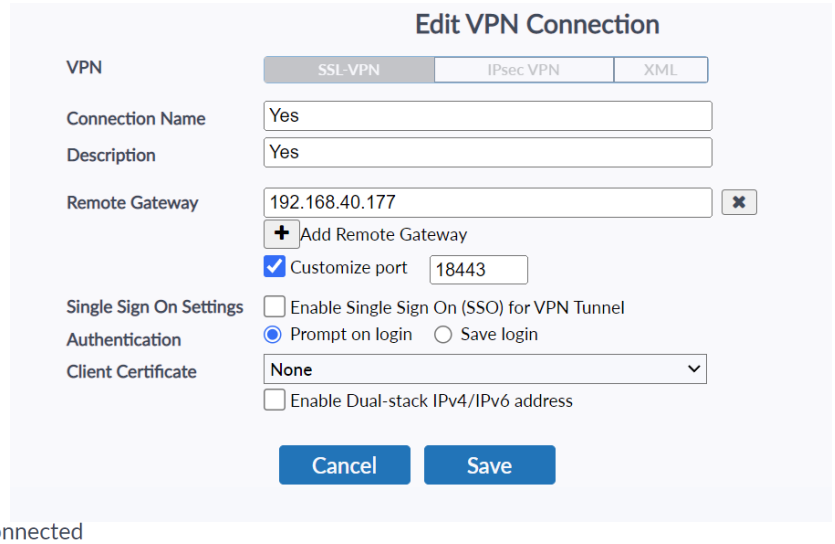
5. Duplicate the previous step, but enable NAT and change to outgoing Interface and destination to WAN

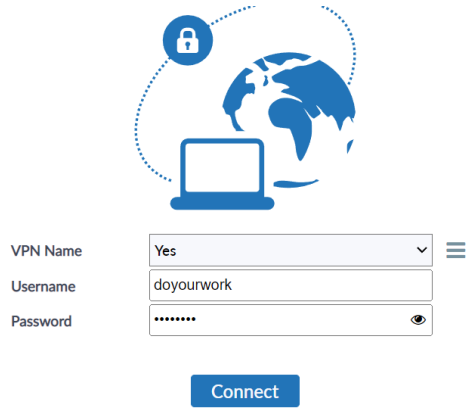


6. Go to your firewall WAN IP address with the port that you specific for SSL-VPN, login and client on Download FortClient

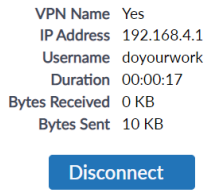


7. Enter your VPN Wan port IP with the port number that you used for SSL_VPN then click connect, then save



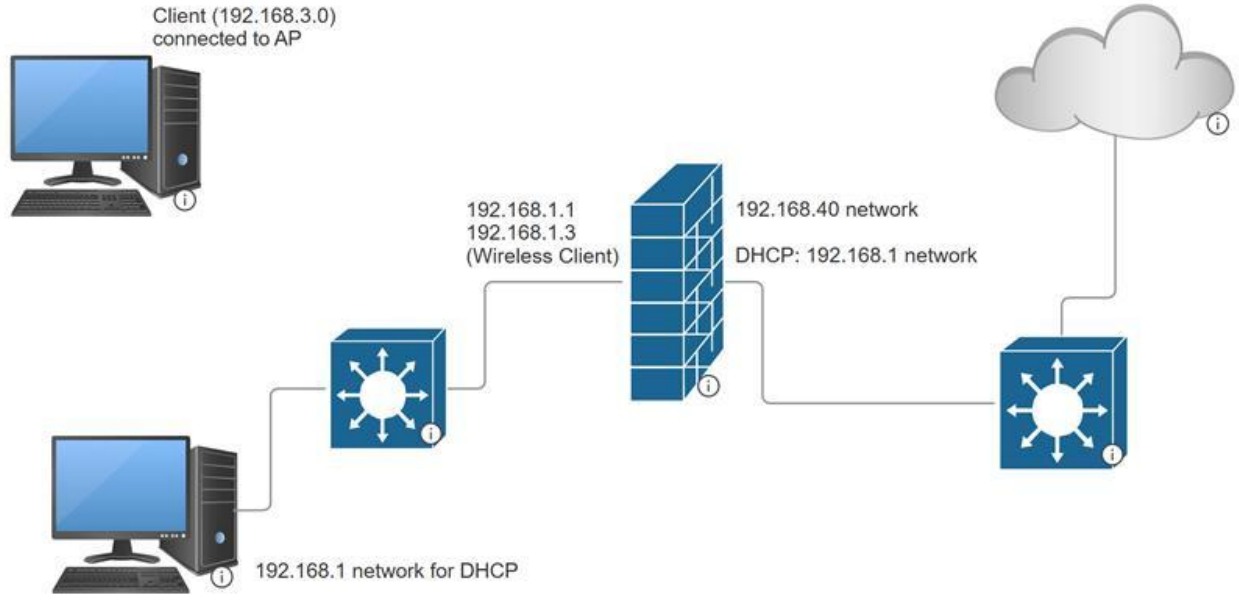


VPN Connected



8. Go to Remote Desktop, enter the target Client IP and click connect.

Network Diagram:



Problems: In this lab, we only facing one problem which is the Forticlient version changed when we doing the lab, and it removed the VPN connection on the old version, we fix it by going back to the portal and reinstall the newest version of for Forticlient.

Conclusion: In this lab, we learned how to set up Fortinet SSL Remote Access, we set up Fortinet SSL remote access by creating a SSL portal and user, one thing that no going well is the version of Forticlient changed, so we need to reinstall Forticlient, we learned more about how different type of VPN works, which can prepare us for future job situation.

CCNP Multiple Wireless SSID with Access Point- WPA2 PSK, WPA2-Ent

By Alvin Chow

Purpose: In this we learned how to convert a lightweight ap to standalone, then we learned how to set it up. Then we learned more on how to set up a radius VM, which is requirement of the lab of doing WPA2-Enterprise. We also practice how to set up router on a stick which can be called inter vlan routing and connect our networks to internet.

Background info:

"Router on a Stick" is a network configuration where a single router interface is used to route traffic between multiple VLANs. This can be done by configuring the router interface as a trunk link, allowing it to handle traffic for multiple VLANs using 802.1Q tagging. It's a cost-effective solution for inter-VLAN routing in small to medium-sized networks.

Network Address Translation (NAT) is a technique used to modify IP address information in packet headers while they are in transit across a routing device. NAT allows multiple devices on a local network to share a single public IP address for accessing external networks, conserving the limited number of available public IP addresses.

An Access Point (AP) is a device that allows wireless devices to connect to a wired network using Wi-Fi. It acts as an interface between the wired network and wireless clients, enabling mobility and flexibility in network access. APs are commonly used in homes, offices, and public spaces to provide wireless connectivity.

The Cisco Aironet 1042N is a dual-band 802.11n wireless access point designed for enterprise environments. It supports data rates up to 300 Mbps and. This device operates on both 2.4 GHz and 5 GHz bands, offering flexibility in deployment. It includes features like WPA2 security, Power over Ethernet (PoE) support, and is wall or ceiling mountable. The AP is managed via a web-based interface or command-line interface, making it suitable for small to medium-sized businesses seeking reliable wireless connectivity.

WPA2 PSK (Pre-Shared Key) is a wireless security protocol where all users share the same password to access the network. It's simple to configure but less secure for larger environments. WPA2 Enterprise, on the other hand, uses a RADIUS server for authentication, providing unique credentials for each user, which enhances security and is suitable for enterprise networks.

A RADIUS (Remote Authentication Dial-In User Service) server is a network protocol that provides centralized Authentication, Authorization, and Accounting (AAA) management for users who connect and use a network service. It is commonly used in enterprise environments for managing access to network resources.

A Virtual Local Area Network (VLAN) is a logical grouping of devices within a network, segmented by function, department, or project, regardless of their physical location.

VLANs improve network efficiency, enhance security by isolating traffic, and simplify management by grouping users with similar needs.

The Native VLAN is the default VLAN assigned to a trunk port on a switch. Frames belonging to the Native VLAN are sent untagged, meaning they don't have an 802.1Q VLAN tag. This is important for compatibility with devices that don't support VLAN tagging. Typically, VLAN 1 is used as the Native VLAN, but this can be changed for security reasons.

DHCP is a network protocol that automates the assignment of IP addresses and other network configuration details to devices on a TCP/IP network. When a device connects to the network, it sends a DHCPDISCOVER message to locate a DHCP server. The server responds with a DHCPOFFER, and the device requests the offered IP address via DHCPREQUEST. The server then acknowledges with a DHCPACK, completing the process. This dynamic assignment simplifies network management by reducing manual configuration and minimizing IP address conflicts. DHCP is essential in large-scale networks, enabling efficient use of IP resources and accommodating changes in network topology without manual intervention.

Lab summary: First, we configure router, we configure a DHCP server which can handle all VLAN IP assignment to every VLAN, then we change the interface that connected to 40 networks to DHCP, which allow it to get an IP address from the 40 network. Then we set the default route and NAT to the 40 networks which allow all traffic can reach internet

Then we set up the switch, we set up VLAN 3 to be native VLAN, VLAN 4 used for PSK authentication, VLAN 5 used for open authentication, then VLAN 6 used for radius server authentication. We set up f0/30 to be the AP interface, we set it as a trunk port and allow VLAN 3-6 traffic, We also the f0/40 port as the access port for vlan 3, it used for configure the AP and the radius server and we used f0/33 to connect to the router.

After that we found the image of c1040 N standalone AP firmware, Then we install the TFTP server on the PC, boot the AP to ROMMON mode, set up the IP of AP, load the standalone image, then boot it up.

Then we access the CLI interface, set up 4 vlan, create 3 SSID and set up the encryption method. We used VM to set up the radius server, first we download the Ubuntu image, set the connection as bridged interface, load it up on the VM, install free radius package, change the clients and users list, then we link the ap to the radius server. Then we tested it, all SSID working.

Lab command

VLAN 3,4,5,6, used it for create some vlan

Interface f0/30, 40, used for config the interface

Switchport trunk encapsulation dot1q, set the trunk encapsulation, allow multiple VLAN over a single link

switchport trunk native vlan 3, used VLAN 3 as native VLAN

switchport trunk allowed vlan 3-6, limits the allowed VLAN on the trunks.

Ip dhcp excluded-address, specific IP address to be excluded from the DHCP pool

Ip dhcp pool, define a DHCP address pool for specific VLAN

Network specifies the network address and subnet mask for the DHCP pool

Default router specifies the default gateway IP address for DHCP clients

DNS-server used for specifies the DNS server IP for DHCP clients

Ip nat inside source list, config NAT to translate address from specified access control list to the IP address of an interface

Ip access-list standard, define a standard ACL to permit or deny traffic based on source IP

encapsulation dot1Q 6, config 802.1Q encapsulation for vlan tagging

Ip address, assignments an IP and subnet mask to the interface

Ip nat inside/outside, specific the interface as part of inside or outside network for NAT

Interface g0/0/0.3, used for creating sub interface for inter vlan routing

Ip route 0.0.0.0 0.0.0.0 192.168.40.1, this set up a default route to the 40 networks

aaa group server radius rad_eap**,** Defines a RADIUS server group named "rad_eap" for EAP authentication.

dot11 vlan-name enterprise vlan 6 Associates the SSID "enterprise" with VLAN 6.

dot11 ssid ap_ent, Defines the SSID "ap_ent" with WPA2-EAP authentication using the "eap_methods3" method and assigns it to VLAN 6.

interface Dot11Radio0 Enters the configuration mode for the 2.4 GHz radio interface.

encryption mode ciphers aes-ccm, Sets the encryption mode to AES-CCM for secure wireless communication.

interface Dot11Radio0.3, Creates a subinterface for VLAN 3 with 802.1Q encapsulation and bridges it to bridge group 1.

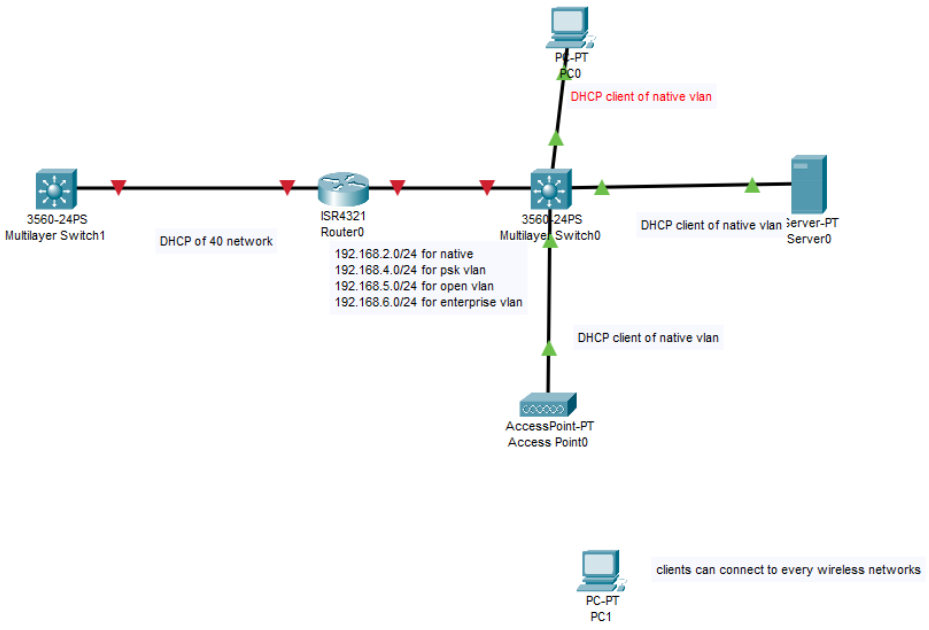
interface BVI1, Configures a Bridge Virtual Interface (BVI) for the bridged VLANs, allowing routing between them.

ip default-gateway 192.168.2.1, Sets the default gateway for the AP to 192.168.2.1.

ip radius source-interface BVI1**,** Specifies that RADIUS requests originate from the BVI1 interface.

radius server radius_vlan6**,** defines a RADIUS server named "radius_vlan6" with its IP address and shared secret for authentication.

Network Diagram:



Configuration:

Router:

```
version 15.5
service timestamps debug datetime msec
service timestamps log datetime msec
no platform punt-keepalive disable-kernel-core
hostname Router
boot-start-marker
boot-end-marker
vrf definition Mgmt-intf
address-family ipv4
```

```
 exit-address-family
 address-family ipv6
 exit-address-family
no aaa new-model
ip dhcp excluded-address 192.168.2.1
ip dhcp excluded-address 192.168.3.1
ip dhcp excluded-address 192.168.4.1
ip dhcp excluded-address 192.168.5.1
ip dhcp excluded-address 192.168.6.1
ip dhcp excluded-address 192.168.2.10
ip dhcp excluded-address 192.168.2.11
ip dhcp pool vlan3
 network 192.168.2.0 255.255.255.0
 default-router 192.168.2.1
 dns-server 1.1.1.1
ip dhcp pool vlan4
 network 192.168.4.0 255.255.255.0
 default-router 192.168.4.1
 dns-server 1.1.1.1
ip dhcp pool vlan5
 network 192.168.5.0 255.255.255.0
 default-router 192.168.5.1
 dns-server 1.1.1.1
ip dhcp pool vlan6
 network 192.168.6.0 255.255.255.0
 default-router 192.168.6.1
 dns-server 1.1.1.1
subscriber templating
vtp domain cisco
vtp mode transparent
multilink bundle-name authenticated
license udi pid ISR4321/K9 sn FDO214421BY=
spanning-tree extend system-id
redundancy
 mode none
vlan internal allocation policy ascending
interface GigabitEthernet0/0/0
 no ip address
 negotiation auto
interface GigabitEthernet0/0/0.3
 encapsulation dot1Q 1 native
 ip address 192.168.2.1 255.255.255.0
 ip nat inside
interface GigabitEthernet0/0/0.4
 encapsulation dot1Q 4
 ip address 192.168.4.1 255.255.255.0
 ip nat inside
interface GigabitEthernet0/0/0.5
 encapsulation dot1Q 5
 ip address 192.168.5.1 255.255.255.0
 ip nat inside
interface GigabitEthernet0/0/0.6
```

```
 encapsulation dot1Q 6
 ip address 192.168.6.1 255.255.255.0
 ip nat inside
interface GigabitEthernet0/0/0.20
interface GigabitEthernet0/0/1
 ip address dhcp
 ip nat outside
 negotiation auto
interface Serial0/1/0
interface Serial0/1/1
interface GigabitEthernet0/2/0
 no ip address
 shutdown
 negotiation auto
interface GigabitEthernet0/2/1
 no ip address
 shutdown
 negotiation auto
interface GigabitEthernet0
 vrf forwarding Mgmt-intf
 no ip address
 shutdown
 negotiation auto
interface Vlan1
 no ip address
 shutdown
ip nat inside source list NAT_LAN interface GigabitEthernet0/0/1
overload
ip forward-protocol nd
no ip http server
no ip http secure-server
ip tftp source-interface GigabitEthernet0
ip route 0.0.0.0 0.0.0.0 192.168.40.1
ip access-list standard NAT_LAN
 permit 192.168.2.0 0.0.0.255
 permit 192.168.4.0 0.0.0.255
 permit 192.168.5.0 0.0.0.255
 permit 192.168.6.0 0.0.0.255
control-plane
line con 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 login
end
```

Switch:

```
version 12.2
```

```
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname Switch
boot-start-marker
boot-end-marker
no aaa new-model
system mtu routing 1500
authentication mac-move permit
ip subnet-zero
spanning-tree mode pvst
spanning-tree etherchannel guard misconfig
spanning-tree extend system-id
vlan internal allocation policy ascending
interface FastEthernet0/1
interface FastEthernet0/2
interface FastEthernet0/3
interface FastEthernet0/4
interface FastEthernet0/5
interface FastEthernet0/6
interface FastEthernet0/7
interface FastEthernet0/8
interface FastEthernet0/9
interface FastEthernet0/10
interface FastEthernet0/11
interface FastEthernet0/12
interface FastEthernet0/13
interface FastEthernet0/14
interface FastEthernet0/15
interface FastEthernet0/16
interface FastEthernet0/17
 switchport access vlan 3
 switchport mode access
interface FastEthernet0/18
interface FastEthernet0/19
interface FastEthernet0/20
interface FastEthernet0/21
interface FastEthernet0/22
interface FastEthernet0/23
interface FastEthernet0/24
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 3
 switchport trunk allowed vlan 3-6
 switchport mode trunk
interface FastEthernet0/25
interface FastEthernet0/26
interface FastEthernet0/27
interface FastEthernet0/28
interface FastEthernet0/29
interface FastEthernet0/30
 switchport trunk encapsulation dot1q
```

```
 switchport trunk native vlan 3
 switchport trunk allowed vlan 3-6
 switchport mode trunk
interface FastEthernet0/31
 switchport access vlan 3
 switchport mode access
interface FastEthernet0/32
interface FastEthernet0/33
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 3
 switchport trunk allowed vlan 3-6
 switchport mode trunk
interface FastEthernet0/34
interface FastEthernet0/35
interface FastEthernet0/36
interface FastEthernet0/37
interface FastEthernet0/38
interface FastEthernet0/39
interface FastEthernet0/40
 switchport access vlan 3
 switchport mode access
interface FastEthernet0/41
interface FastEthernet0/42
interface FastEthernet0/43
interface FastEthernet0/44
interface FastEthernet0/45
interface FastEthernet0/46
interface FastEthernet0/47
interface FastEthernet0/48
 switchport access vlan 4
 switchport mode access
interface GigabitEthernet0/1
interface GigabitEthernet0/2
interface GigabitEthernet0/3
interface GigabitEthernet0/4
interface Vlan1
 no ip address
ip classless
ip http server
ip http secure-server
ip sla enable reaction-alerts
line con 0
line vty 5 15
end
```

AP:

```
version 15.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
hostname ap
```

```
logging rate-limit console 9
enable secret 5 $1$zwxp$r6eRN/WDBk2si/2VOJtFd0
aaa new-model
aaa group server radius rad_eap
aaa group server radius rad_mac
aaa group server radius rad_acct
aaa group server radius rad_admin
aaa group server tacacs+ tac_admin
aaa group server radius rad_pmip
aaa group server radius dummy
aaa group server radius rad_eap3
 server name radius_vlan6
aaa authentication login eap_methods group rad_eap
aaa authentication login mac_methods local
aaa authentication login eap_methods3 group rad_eap3
aaa authorization exec default local
aaa accounting network acct_methods start-stop group rad_acct
aaa session-id common
no ip source-route
no ip cef
dot11 pause-time 100
dot11 syslog
dot11 vlan-name enterprise vlan 6
dot11 vlan-name management vlan 3
dot11 vlan-name open vlan 5
dot11 vlan-name psk vlan 4
dot11 ssid ap_ent
   vlan 6
   authentication open eap eap_methods3
   authentication key-management wpa version 2
   mbssid guest-mode
dot11 ssid ap_open
   vlan 5
   authentication open
   mbssid guest-mode
dot11 ssid ap_psk
   vlan 4
   authentication open
   authentication key-management wpa version 2
   guest-mode
   mbssid guest-mode
   wpa-psk ascii 7 02250D4808095E731F
no ipv6 cef
username admin privilege 15 secret 5 $1$ItvP$nRrnZmReg1RDcpFdNJhKn/
bridge irb
interface Dot11Radio0
 no ip address
 encryption mode ciphers aes-ccm
 encryption vlan 4 mode ciphers aes-ccm
 encryption vlan 6 mode ciphers aes-ccm
 ssid ap_ent
 ssid ap_open
```

```
 ssid ap_psk
 antenna gain 0
 mbssid
 station-role root
interface Dot11Radio0.3
 encapsulation dot1Q 3 native
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 spanning-disabled
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
interface Dot11Radio0.4
 encapsulation dot1Q 4
 bridge-group 4
 bridge-group 4 subscriber-loop-control
 bridge-group 4 spanning-disabled
 bridge-group 4 block-unknown-source
 no bridge-group 4 source-learning
 no bridge-group 4 unicast-flooding
interface Dot11Radio0.5
 encapsulation dot1Q 5
 bridge-group 5
 bridge-group 5 subscriber-loop-control
 bridge-group 5 spanning-disabled
 bridge-group 5 block-unknown-source
 no bridge-group 5 source-learning
 no bridge-group 5 unicast-flooding
interface Dot11Radio0.6
 encapsulation dot1Q 6
 bridge-group 6
 bridge-group 6 subscriber-loop-control
 bridge-group 6 spanning-disabled
 bridge-group 6 block-unknown-source
 no bridge-group 6 source-learning
 no bridge-group 6 unicast-flooding
interface Dot11Radio0.41
interface Dot11Radio0.51
interface Dot11Radio1
 no ip address
 encryption mode ciphers aes-ccm
 encryption vlan 4 mode ciphers aes-ccm
 encryption vlan 6 mode ciphers aes-ccm
 ssid ap_ent
 ssid ap_open
 ssid ap_psk
 antenna gain 0
 peakdetect
 dfs band 3 block
 mbssid
 channel dfs
 station-role root
```

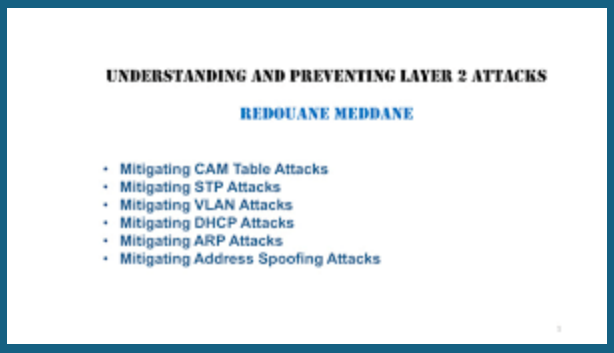
```
interface Dot11Radio1.3
 encapsulation dot1Q 3 native
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 spanning-disabled
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
interface Dot11Radio1.4
 encapsulation dot1Q 4
 bridge-group 4
 bridge-group 4 subscriber-loop-control
 bridge-group 4 spanning-disabled
 bridge-group 4 block-unknown-source
 no bridge-group 4 source-learning
 no bridge-group 4 unicast-flooding
interface Dot11Radio1.5
 encapsulation dot1Q 5
 bridge-group 5
 bridge-group 5 subscriber-loop-control
 bridge-group 5 spanning-disabled
 bridge-group 5 block-unknown-source
 no bridge-group 5 source-learning
 no bridge-group 5 unicast-flooding
interface Dot11Radio1.6
 encapsulation dot1Q 6
 bridge-group 6
 bridge-group 6 subscriber-loop-control
 bridge-group 6 spanning-disabled
 bridge-group 6 block-unknown-source
 no bridge-group 6 source-learning
 no bridge-group 6 unicast-flooding
interface GigabitEthernet0
 no ip address
 duplex auto
 speed auto
interface GigabitEthernet0.3
 encapsulation dot1Q 3 native
 bridge-group 1
 bridge-group 1 spanning-disabled
 no bridge-group 1 source-learning
interface GigabitEthernet0.4
 encapsulation dot1Q 4
 bridge-group 4
 bridge-group 4 spanning-disabled
 no bridge-group 4 source-learning
interface GigabitEthernet0.5
 encapsulation dot1Q 5
 bridge-group 5
 bridge-group 5 spanning-disabled
 no bridge-group 5 source-learning
interface GigabitEthernet0.6
```

```
 encapsulation dot1Q 6
 bridge-group 6
 bridge-group 6 spanning-disabled
 no bridge-group 6 source-learning
interface GigabitEthernet0.41
interface GigabitEthernet0.51
interface BVI1
 mac-address 0007.7db6.1687
 ip address 192.168.2.10 255.255.255.0
 ipv6 address dhcp
 ipv6 address autoconfig
 ipv6 enable
ip default-gateway 192.168.2.1
ip forward-protocol nd
ip http server
no ip http secure-server
ip http help-path
http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag
ip radius source-interface BVI1
radius-server attribute 32 include-in-access-req format %h
radius server radius_vlan6
 address ipv4 192.168.2.67 auth-port 1812 acct-port 1813
 key 7 030A540C0702245F411B1C090417
bridge 1 route ip
line con 0
line vty 0 4
 transport input all
end
```

Problem: In this lab we have about 3 big problems the first one is the ap cannot get any IP from the DHCP server, we fix it by using the native vlan 3 to get ip. We fix it by searching Cisco forum and find the solution for that. The second problem that we have is the Radius server is not working, we fix it by uninstall the FreeRadius, then install it back and config it again. The last big problem that we have is we don't know why only one SSID broadcast, we fix it by using multiple guess mode and all SSID can be broadcast.

Conclusion: In this we learned how to convert a lightweight ap to standalone, then we learned how to set it up. We also learned more on how to set up a radius VM and did some basic configuration. We also practice how to set up router on a stick which can be called inter vlan routing and we can prepare for the future job situation, and we practice connect our networks to internet by setting up default route and NAT.

Layer 2 Attack and Mitigations



UNDERSTANDING AND PREVENTING LAYER 2 ATTACKS

REDOUANE MEDDANE

- Mitigating CAM Table Attacks
- Mitigating STP Attacks
- Mitigating VLAN Attacks
- Mitigating DHCP Attacks
- Mitigating ARP Attacks
- Mitigating Address Spoofing Attacks

By Alvin Chow

Purpose: The purpose of this lab is to learn how a Layer 2 attack works, such as MAC flooding, ARP spoofing and STP Manipulation Attacks, and then use Cisco switch security features like port security, DHCP snooping, and dynamic ARP inspection—to detect and prevent these attacks.

Background info:

Layer 2 attacks is about the data link layer got attack. Layer 2 is responsible for switching and MAC address forwarding. Common attacks include MAC flooding, ARP spoofing, and DHCP spoofing. These attacks can lead to traffic interception, network disruption, or unauthorized access.

Kali Linux is a specialized Linux system designed for penetration testing and ethical hacking. It includes tools like ettercap, macof, and yersinia, which is useful for simulate Layer 2 attacks to test the network defenses.

Dynamic ARP Inspection can prevents ARP spoofing by intercepting and verifying ARP packets. It compares ARP requests and replies, then compare DHCP snooping database and only permits valid bindings. This can protects against man-in-the-middle (MITM) attacks.

BPDU Guard helps prevent rogue switches from access port become root bridge to cause STP fails. It disables a port immediately if it receives a Bridge Protocol Data Unit (BPDU), which should only come from other switches. This can protects the network topology.

Port security allows administrators to limit which MAC addresses can connect to a specific switch port. It can restrict the number of allowed devices and take actions like shutting down the port if a violation occurs. The sticky MAC feature learns the MAC addresses dynamically on a port and stores them in the running configuration. This can be useful for prevent attack like mac flooding.

Lab Summary:

First we installed Kali Linux on a VM, We changed the network type to bridged connection, then we find the mac address table have the VM mac address. Then we started the Mac flooding attack using macof, we prevent it happened by doing sticky mac-address and set the maximum mac address to be 2 for the port that connected to a Host. After that we launched ARP spoofing attack by using arpspoof, and we noticed the arp table changed on the victim PC. We prevent it using DHCP snooping and arp inspection. At the end, we launched the STP Manipulation Attacks and we noticed the root bridge of STP changed to the host port, we prevent it by using BPDU guard.

Lab Commands:

Macof -i eth0, this command allow us to launch MAC flooding attack.

Arpspoof -i eth0 192.168.1.1 192.168.1.99, this command allow us to launch Arp poisoning attack.

Switchport port-security maximum 2, this command set the max 2 mac address on that port

Switchport port-security mac-address sticky, this command allow the switch learn the mac address

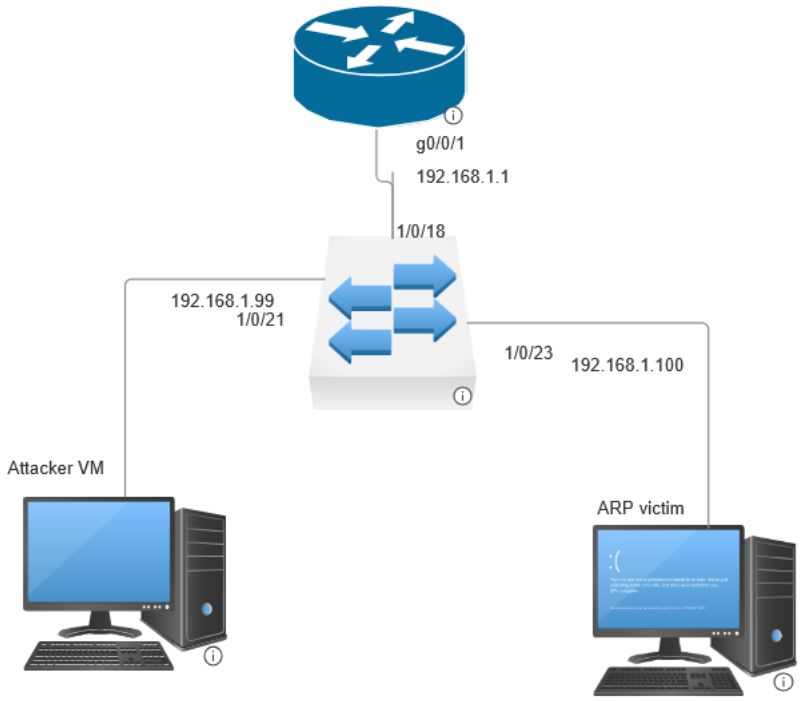
Spanning-tree bpduguard enable, this command enable BPDU guard to prevent STP attack.

Ip arp inspection vlan 1, this command inspect all the arp traffic from VLAN1

Ip dhcp snooping, this command enable dhcp snooping which created a table to bind mac-address to a ip

Ip dhcp snooping vlan 1, this command check do vlan 1 traffic match the binding ip and the MAC address to prevent ARP poisoning.

Network Diagram:



Configurations:

```
 version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname Switch
boot-start-marker
boot-end-marker
!
no aaa new-model
system mtu routing 1500
ip arp inspection vlan 1
ip dhcp snooping vlan 1
ip dhcp snooping
vtp domain CCNP
vtp mode transparent
spanning-tree mode pvst
spanning-tree extend system-id
vlan internal allocation policy ascending
vlan 2
 name data
vlan 3
 name voice
interface FastEthernet1/0/1
interface FastEthernet1/0/2
interface FastEthernet1/0/3
interface FastEthernet1/0/4
interface FastEthernet1/0/5
interface FastEthernet1/0/6
interface FastEthernet1/0/7
interface FastEthernet1/0/8
interface FastEthernet1/0/9
interface FastEthernet1/0/10
interface FastEthernet1/0/11
interface FastEthernet1/0/12
interface FastEthernet1/0/13
interface FastEthernet1/0/14
interface FastEthernet1/0/15
interface FastEthernet1/0/16
interface FastEthernet1/0/17
interface FastEthernet1/0/18
interface FastEthernet1/0/19
interface FastEthernet1/0/20
interface FastEthernet1/0/21
switchport mode access
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security mac-address sticky 04d9.c8ba.261c
switchport port-security mac-address sticky 7e9e.a874.1ebb
interface FastEthernet1/0/22
interface FastEthernet1/0/23
interface FastEthernet1/0/24
switchport mode access
spanning-tree bpduguard enable
interface GigabitEthernet1/0/1
interface GigabitEthernet1/0/2
interface GigabitEthernet1/1/1
interface GigabitEthernet1/1/2
interface Vlan1
no ip address
shutdown
ip http server
ip http secure-server
```

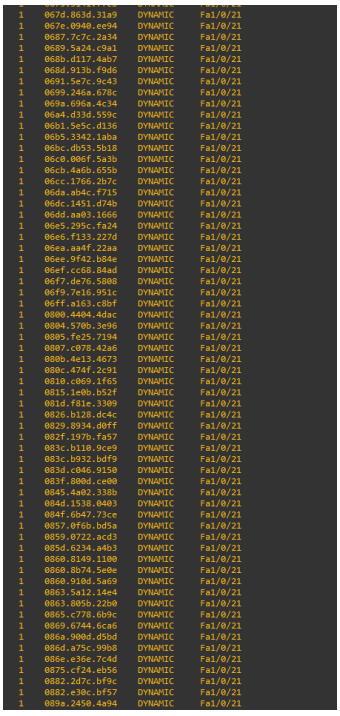
```
logging esm config
line con 0
line vty 5 15
end
```

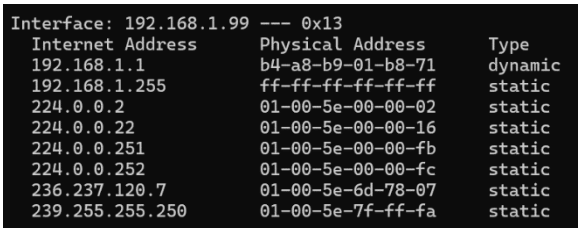
Problems: In this lab one problem that we faced is we cannot install yersinia on the VM, we fix this issue by getting another group laptop that have yersinia install.

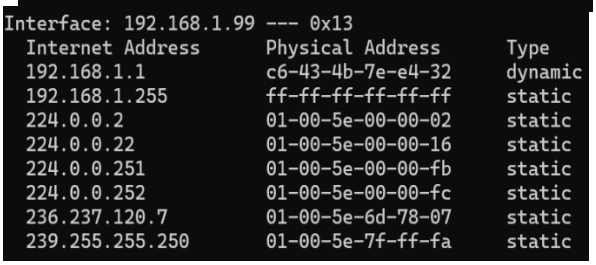
Conclusion:

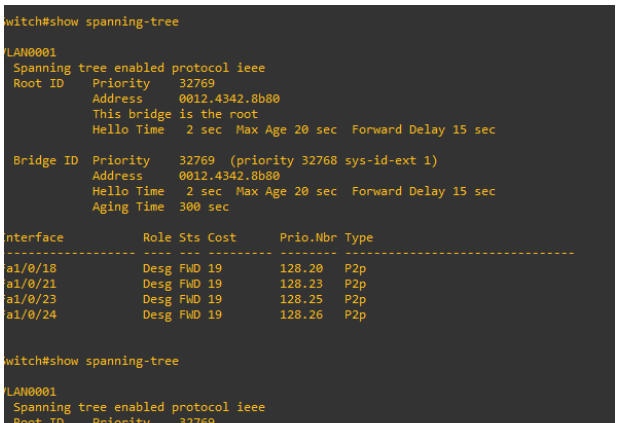
This lab show how Layer 2 attacks such as ARP spoofing, MAC flooding, and DHCP spoofing can affect network security. By simulating these attacks using Kali Linux, we gained hands-on experience in understanding the risks of those vulnerability. Then we applied Cisco security features, including DHCP snooping, ARP Inspection, BPDU Guard, and port security, those features can effectively detect and prevent these threats. Overall, this lab show it is important to securing the data link layer in enterprise.

Proof of attack and mitigations:

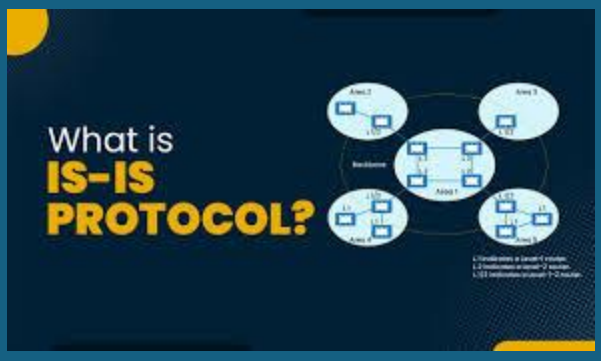








ISIS Routing Protocol Lab



By Alvin Chow

Purpose: The purpose of this lab is to learn another routing protocol. My partner and I simulated a network and configured it using the IS-IS routing protocol. This helped us understand how IS-IS works in a network environment. We also get some hands-on experience in network configuration and troubleshooting.

Background info: The Intermediate System to Intermediate System (IS-IS) routing protocol is a link-state interior gateway protocol designed for efficient data routing within a network. Unlike OSPF, IS-IS operates at the data link layer, making it independent of IP addressing and capable of supporting multiple network layer protocols, including IPv4 and IPv6. It used hierarchical structure with level 1 router for inter area routing and level 2 router for Mult area. It used SPF algorithm to determine optimal paths.

ISIS design allows efficient management of large network, it operating at the data link layer, which make ISIS can support multiple network layer. It used SPF algorithm, which mean ISIS can quickly recalculate the routers if the network changes.

ISIS hierarchical structure and use of NSAP address make the initial configuration and troubleshooting more complex compared to other routing protocol like OSPF.

Lab Summary: In this lab, me and my partner used 6 router and we make it 3 area, we used /30 for point-to-point router and used /24 if the network is connected to users network. Then we used 49.0001 for first area, then 49.0002 for second area and the last one I used 49.0003 for third area.

Lab Command:

router isis: This enable isis on the router

net 49.0001.0000.0000.0004.00: This assignment a NET address to the router. NET address is important in ISIS for identify routers and establishing adjacencies.

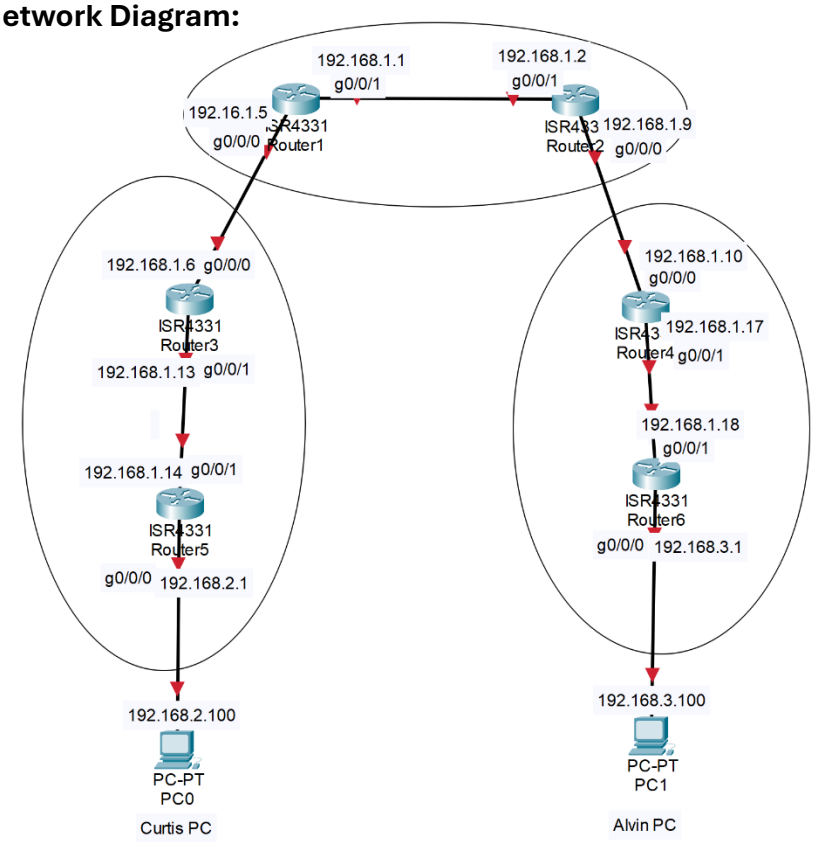
ip router isis/ ipv6 router isis: This command attach the interface to ISIS protocol\

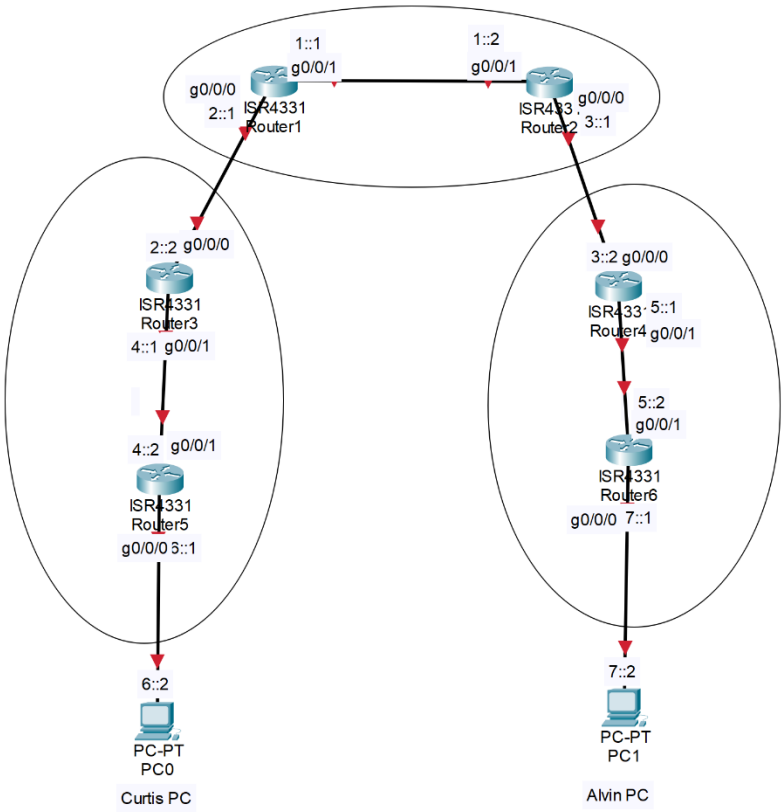
is-type level-1: This made router become level 1 router

is-type level-1-2: This made router become level 1 and level 2 router

is-type level-2: This made router become level 2 router.

Network Diagram:





Configuration:

R1:
```
version 15.5
service timestamps debug datetime msec
service timestamps log datetime msec
no platform punt-keepalive disable-kernel-core
hostname R1
boot-start-marker
boot-end-marker
vrf definition Mgmt-intf
 address-family ipv4
 exit-address-family
 address-family ipv6
 exit-address-family
no aaa new-model
ipv6 unicast-routing
subscriber templating
vtp domain cisco
vtp mode transparent
multilink bundle-name authenticated
license udi pid ISR4321/K9 sn FDO214421BY
spanning-tree extend system-id
redundancy
 mode none
vlan internal allocation policy ascending
interface GigabitEthernet0/0/0
 ip address 192.168.1.5 255.255.255.252
 ip router isis
 negotiation auto
 ipv6 address 2::1/64
 ipv6 enable
 ipv6 router isis
interface GigabitEthernet0/0/1
 ip address 192.168.1.1 255.255.255.252
 ip router isis
 negotiation auto
 ipv6 address 1::1/64
 ipv6 enable
 ipv6 router isis
interface Serial0/1/0
interface Serial0/1/1
interface GigabitEthernet0/2/0
 no ip address
 shutdown
 negotiation auto
interface GigabitEthernet0/2/1
 no ip address
 shutdown
 negotiation auto
```

```
interface GigabitEthernet0
 vrf forwarding Mgmt-intf
 no ip address
 shutdown
 negotiation auto
interface Vlan1
 no ip address
 shutdown
router isis
 net 49.0001.0000.0000.0001.00
 is-type level-2-only
ip forward-protocol nd
no ip http server
no ip http secure-server
ip tftp source-interface GigabitEthernet0
control-plane
line con 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 login
end
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B -
BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS
level-2
       ia - IS-IS inter area, * - candidate default, U - per-user
static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l -
LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from
PfR

Gateway of last resort is not set

      192.168.1.0/24 is variably subnetted, 7 subnets, 2 masks
C        192.168.1.0/30 is directly connected, GigabitEthernet0/0/1
L        192.168.1.1/32 is directly connected, GigabitEthernet0/0/1
C        192.168.1.4/30 is directly connected, GigabitEthernet0/0/0
L        192.168.1.5/32 is directly connected, GigabitEthernet0/0/0
i L2     192.168.1.8/30
           [115/20] via 192.168.1.2, 00:07:18, GigabitEthernet0/0/1
i L2     192.168.1.12/30
           [115/20] via 192.168.1.6, 00:08:10, GigabitEthernet0/0/0
i L2     192.168.1.16/30
           [115/30] via 192.168.1.2, 00:07:18, GigabitEthernet0/0/1
```

```
i L2  192.168.2.0/24 [115/30] via 192.168.1.6, 00:08:10,
GigabitEthernet0/0/0
i L2  192.168.3.0/24 [115/40] via 192.168.1.2, 00:07:13,
GigabitEthernet0/0/1
IPv6 Routing Table - default - 10 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, I1 - ISIS L1, I2 - ISIS L2
       IA - ISIS interarea, IS - ISIS summary, D - EIGRP, EX - EIGRP
external
       ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr -
Redirect
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF
ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2, a - Application
C   1::/64 [0/0]
     via GigabitEthernet0/0/1, directly connected
L   1::1/128 [0/0]
     via GigabitEthernet0/0/1, receive
C   2::/64 [0/0]
     via GigabitEthernet0/0/0, directly connected
L   2::1/128 [0/0]
     via GigabitEthernet0/0/0, receive
I2  3::/64 [115/20]
     via FE80::B6A8:B9FF:FE47:92C1, GigabitEthernet0/0/1
I2  4::/64 [115/20]
     via FE80::B6A8:B9FF:FE01:AE50, GigabitEthernet0/0/0
I2  5::/64 [115/30]
     via FE80::B6A8:B9FF:FE47:92C1, GigabitEthernet0/0/1
I2  6::/64 [115/30]
     via FE80::B6A8:B9FF:FE01:AE50, GigabitEthernet0/0/0
I2  7::/64 [115/40]
     via FE80::B6A8:B9FF:FE47:92C1, GigabitEthernet0/0/1
L   FF00::/8 [0/0]
     via Null0, receive
```

R2:

```
version 15.5
service timestamps debug datetime msec
service timestamps log datetime msec
no platform punt-keepalive disable-kernel-core
hostname R2
boot-start-marker
boot-end-marker
vrf definition Mgmt-intf
address-family ipv4
 exit-address-family
address-family ipv6
 exit-address-family
no aaa new-model
ipv6 unicast-routing
subscriber templating
vtp domain cisco
```

```
vtp mode transparent
multilink bundle-name authenticated
license udi pid ISR4321/K9 sn FDO214420QQ
license accept end user agreement
license boot level securityk9
spanning-tree extend system-id
redundancy
 mode none
vlan internal allocation policy ascending
interface GigabitEthernet0/0/0
 ip address 192.168.1.9 255.255.255.252
 ip router isis
 negotiation auto
 ipv6 address 3::1/64
 ipv6 enable
 ipv6 router isis
interface GigabitEthernet0/0/1
 ip address 192.168.1.2 255.255.255.252
 ip router isis
 negotiation auto
 ipv6 address 1::2/64
 ipv6 enable
 ipv6 router isis
interface Serial0/1/0
 no ip address
 shutdown
interface Serial0/1/1
 no ip address
 shutdown
interface GigabitEthernet0
 vrf forwarding Mgmt-intf
 no ip address
 shutdown
 negotiation auto
interface Vlan1
 no ip address
 shutdown
router isis
 net 49.0001.0000.0000.0002.00
 is-type level-2-only
ip forward-protocol nd
no ip http server
no ip http secure-server
ip tftp source-interface GigabitEthernet0
control-plane
line con 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 login
end
```

```
Gateway of last resort is not set
      192.168.1.0/24 is variably subnetted, 7 subnets, 2 masks
C        192.168.1.0/30 is directly connected, GigabitEthernet0/0/1
L        192.168.1.2/32 is directly connected, GigabitEthernet0/0/1
i L2     192.168.1.4/30
           [115/20] via 192.168.1.1, 00:08:43, GigabitEthernet0/0/1
C        192.168.1.8/30 is directly connected, GigabitEthernet0/0/0
L        192.168.1.9/32 is directly connected, GigabitEthernet0/0/0
i L2     192.168.1.12/30
           [115/30] via 192.168.1.1, 00:08:43, GigabitEthernet0/0/1
i L2     192.168.1.16/30
           [115/20] via 192.168.1.10, 00:08:43, GigabitEthernet0/0/0
i L2  192.168.2.0/24 [115/40] via 192.168.1.1, 00:08:43,
GigabitEthernet0/0/1
i L2  192.168.3.0/24 [115/30] via 192.168.1.10, 00:08:43,
GigabitEthernet0/0/0
C   1::/64 [0/0]
     via GigabitEthernet0/0/1, directly connected
L   1::2/128 [0/0]
     via GigabitEthernet0/0/1, receive
I2  2::/64 [115/20]
     via FE80::B6A8:B9FF:FE01:B511, GigabitEthernet0/0/1
C   3::/64 [0/0]
     via GigabitEthernet0/0/0, directly connected
L   3::1/128 [0/0]
     via GigabitEthernet0/0/0, receive
I2  4::/64 [115/30]
     via FE80::B6A8:B9FF:FE01:B511, GigabitEthernet0/0/1
I2  5::/64 [115/20]
     via FE80::521C:B0FF:FE2D:7100, GigabitEthernet0/0/0
I2  6::/64 [115/40]
     via FE80::B6A8:B9FF:FE01:B511, GigabitEthernet0/0/1
I2  7::/64 [115/30]
     via FE80::521C:B0FF:FE2D:7100, GigabitEthernet0/0/0
L   FF00::/8 [0/0]
     via Null0, receive
R3: Building configuration...


Current configuration : 1590 bytes
 Last configuration change at 21:44:53 UTC Fri Apr 25 2025

version 15.5
service timestamps debug datetime msec
service timestamps log datetime msec
no platform punt-keepalive disable-kernel-core
hostname R3
boot-start-marker
boot-end-marker
vrf definition Mgmt-intf
 address-family ipv4
```

```
 exit-address-family
address-family ipv6
 exit-address-family
no aaa new-model
ipv6 unicast-routing
subscriber templating
vtp domain cisco
vtp mode transparent
multilink bundle-name authenticated
license udi pid ISR4321/K9 sn FDO214420HY
license boot level securityk9
spanning-tree extend system-id
redundancy
 mode none
vlan internal allocation policy ascending
vlan 10,20
interface GigabitEthernet0/0/0
 ip address 192.168.1.6 255.255.255.252
 ip router isis
 negotiation auto
 ipv6 address 2::2/64
 ipv6 enable
 ipv6 router isis
interface GigabitEthernet0/0/1
 ip address 192.168.1.13 255.255.255.252
 ip router isis
 negotiation auto
 ipv6 address 4::1/64
 ipv6 enable
 ipv6 router isis
interface Serial0/1/0
 no ip address
interface Serial0/1/1
 no ip address
interface GigabitEthernet0
 vrf forwarding Mgmt-intf
 no ip address
 negotiation auto
interface Vlan1
 no ip address
router isis
 net 49.0002.0000.0000.0003.00
ip forward-protocol nd
no ip http server
no ip http secure-server
ip tftp source-interface GigabitEthernet0
control-plane
line con 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
```

```
 login
end
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B -
BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS
level-2
       ia - IS-IS inter area, * - candidate default, U - per-user
static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l -
LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from
PfR

Gateway of last resort is not set

      192.168.1.0/24 is variably subnetted, 7 subnets, 2 masks
i L2     192.168.1.0/30
           [115/20] via 192.168.1.5, 00:09:00, GigabitEthernet0/0/0
C        192.168.1.4/30 is directly connected, GigabitEthernet0/0/0
L        192.168.1.6/32 is directly connected, GigabitEthernet0/0/0
i L2     192.168.1.8/30
           [115/30] via 192.168.1.5, 00:08:07, GigabitEthernet0/0/0
C        192.168.1.12/30 is directly connected, GigabitEthernet0/0/1
L        192.168.1.13/32 is directly connected, GigabitEthernet0/0/1
i L2     192.168.1.16/30
           [115/40] via 192.168.1.5, 00:08:07, GigabitEthernet0/0/0
i L1  192.168.2.0/24 [115/20] via 192.168.1.14, 00:40:15,
GigabitEthernet0/0/1
i L2  192.168.3.0/24 [115/50] via 192.168.1.5, 00:08:02,
GigabitEthernet0/0/0
IPv6 Routing Table - default - 10 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE -
Destination
       NDr - Redirect, O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext
1
       OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       a - Application
I2  1::/64 [115/20]
     via FE80::B6A8:B9FF:FE01:B510, GigabitEthernet0/0/0
C   2::/64 [0/0]
     via GigabitEthernet0/0/0, directly connected
L   2::2/128 [0/0]
     via GigabitEthernet0/0/0, receive
I2  3::/64 [115/30]
     via FE80::B6A8:B9FF:FE01:B510, GigabitEthernet0/0/0
```

```
C   4::/64 [0/0]
     via GigabitEthernet0/0/1, directly connected
L   4::1/128 [0/0]
     via GigabitEthernet0/0/1, receive
I2  5::/64 [115/40]
     via FE80::B6A8:B9FF:FE01:B510, GigabitEthernet0/0/0
I1  6::/64 [115/20]
     via FE80::6EDD:30FF:FEB6:6031, GigabitEthernet0/0/1
I2  7::/64 [115/50]
     via FE80::B6A8:B9FF:FE01:B510, GigabitEthernet0/0/0
L   FF00::/8 [0/0]
     via Null0, receive
```

R4:

```
version 15.5
service timestamps debug datetime msec
service timestamps log datetime msec
no platform punt-keepalive disable-kernel-core
hostname R4
boot-start-marker
boot-end-marker
vrf definition Mgmt-intf
address-family ipv4
 exit-address-family
address-family ipv6
 exit-address-family
no aaa new-model
ipv6 unicast-routing
subscriber templating
vtp domain cisco
vtp mode transparent
multilink bundle-name authenticated
license udi pid ISR4321/K9 sn FDO21491LXV
license accept end user agreement
license boot level securityk9
spanning-tree extend system-id
redundancy
 mode none
vlan internal allocation policy ascending
vlan 2
 name v2
vlan 3
 name v3
vlan 4
 name v4
vlan 10,20
interface GigabitEthernet0/0/0
 ip address 192.168.1.10 255.255.255.252
 ip router isis
 negotiation auto
 ipv6 address 3::2/64
 ipv6 enable
 ipv6 router isis
```

```
interface GigabitEthernet0/0/1
 ip address 192.168.1.17 255.255.255.252
 ip router isis
 negotiation auto
 ipv6 address 5::1/64
 ipv6 enable
 ipv6 router isis
interface Serial0/1/0
 no ip address
 shutdown
interface Serial0/1/1
 no ip address
 shutdown
interface GigabitEthernet0
 vrf forwarding Mgmt-intf
 no ip address
 shutdown
 negotiation auto
interface Vlan1
 no ip address
 shutdown
router isis
 net 49.0001.0000.0000.0004.00
 net 49.0003.0000.0000.0004.00
ip forward-protocol nd
no ip http server
no ip http secure-server
ip tftp source-interface GigabitEthernet0
control-plane
line con 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 login
end


Gateway of last resort is not set

      192.168.1.0/24 is variably subnetted, 7 subnets, 2 masks
i L2     192.168.1.0/30
           [115/20] via 192.168.1.9, 00:08:01, GigabitEthernet0/0/0
i L2     192.168.1.4/30
           [115/30] via 192.168.1.9, 00:08:01, GigabitEthernet0/0/0
C        192.168.1.8/30 is directly connected, GigabitEthernet0/0/0
L        192.168.1.10/32 is directly connected, GigabitEthernet0/0/0
i L2     192.168.1.12/30
           [115/40] via 192.168.1.9, 00:08:01, GigabitEthernet0/0/0
C        192.168.1.16/30 is directly connected, GigabitEthernet0/0/1
L        192.168.1.17/32 is directly connected, GigabitEthernet0/0/1
```

```
i L2  192.168.2.0/24 [115/50] via 192.168.1.9, 00:08:01,
GigabitEthernet0/0/0
i L1  192.168.3.0/24 [115/20] via 192.168.1.18, 00:08:55,
GigabitEthernet0/0/1


IPv6 Routing Table - default - 10 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE -
Destination
       NDr - Redirect, O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext
1
       OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       a - Application
I2  1::/64 [115/20]
     via FE80::B6A8:B9FF:FE47:92C0, GigabitEthernet0/0/0
I2  2::/64 [115/30]
     via FE80::B6A8:B9FF:FE47:92C0, GigabitEthernet0/0/0
C   3::/64 [0/0]
     via GigabitEthernet0/0/0, directly connected
L   3::2/128 [0/0]
     via GigabitEthernet0/0/0, receive
I2  4::/64 [115/40]
     via FE80::B6A8:B9FF:FE47:92C0, GigabitEthernet0/0/0
C   5::/64 [0/0]
     via GigabitEthernet0/0/1, directly connected
L   5::1/128 [0/0]
     via GigabitEthernet0/0/1, receive
I2  6::/64 [115/50]
     via FE80::B6A8:B9FF:FE47:92C0, GigabitEthernet0/0/0
I1  7::/64 [115/20]
     via FE80::521C:B0FF:FE2D:6801, GigabitEthernet0/0/1
L   FF00::/8 [0/0]
     via Null0, receive
```

R5: Building configuration...

```
Current configuration : 1554 bytes
! Last configuration change at 21:15:41 UTC Fri Apr 25 2025
version 15.5
service timestamps debug datetime msec
service timestamps log datetime msec
no platform punt-keepalive disable-kernel-core
hostname R5
boot-start-marker
boot-end-marker
vrf definition Mgmt-intf
address-family ipv4
 exit-address-family
```

```
address-family ipv6
 exit-address-family
no aaa new-model
ipv6 unicast-routing
subscriber templating
vtp domain cisco
vtp mode transparent
multilink bundle-name authenticated
license udi pid ISR4321/K9 sn FDO21400XZX
spanning-tree extend system-id
redundancy
 mode none
vlan internal allocation policy ascending
interface GigabitEthernet0/0/0
 ip address 192.168.2.1 255.255.255.0
 ip router isis
 negotiation auto
 ipv6 address 6::1/64
 ipv6 enable
 ipv6 router isis
interface GigabitEthernet0/0/1
 ip address 192.168.1.14 255.255.255.252
 ip router isis
 negotiation auto
 ipv6 address 4::2/64
 ipv6 enable
 ipv6 router isis
interface Serial0/1/0
 no ip address
 shutdown
interface Serial0/1/1
 no ip address
 shutdown
interface GigabitEthernet0
 vrf forwarding Mgmt-intf
 no ip address
 shutdown
 negotiation auto
interface Vlan1
 no ip address
 shutdown
router isis
 net 49.0002.0000.0000.0005.00
 is-type level-1
ip forward-protocol nd
no ip http server
no ip http secure-server
ip tftp source-interface GigabitEthernet0
control-plane
line con 0
 stopbits 1
line aux 0
```

```
 stopbits 1
line vty 0 4
 login
end
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B -
BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS
level-2
       ia - IS-IS inter area, * - candidate default, U - per-user
static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l -
LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from
PfR

Gateway of last resort is 192.168.1.13 to network 0.0.0.0

i*L1  0.0.0.0/0 [115/10] via 192.168.1.13, 00:10:07,
GigabitEthernet0/0/1
      192.168.1.0/24 is variably subnetted, 3 subnets, 2 masks
i L1     192.168.1.4/30
           [115/20] via 192.168.1.13, 00:41:29, GigabitEthernet0/0/1
C        192.168.1.12/30 is directly connected, GigabitEthernet0/0/1
L        192.168.1.14/32 is directly connected, GigabitEthernet0/0/1
      192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.2.0/24 is directly connected, GigabitEthernet0/0/0
L        192.168.2.1/32 is directly connected, GigabitEthernet0/0/0
IPv6 Routing Table - default - 7 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, I1 - ISIS L1, I2 - ISIS L2
       IA - ISIS interarea, IS - ISIS summary, D - EIGRP, EX - EIGRP
external
       ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr -
Redirect
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF
ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2, a - Application
I1  ::/0 [115/10]
     via FE80::B6A8:B9FF:FE01:AE51, GigabitEthernet0/0/1
I1  2::/64 [115/20]
     via FE80::B6A8:B9FF:FE01:AE51, GigabitEthernet0/0/1
C   4::/64 [0/0]
     via GigabitEthernet0/0/1, directly connected
L   4::2/128 [0/0]
     via GigabitEthernet0/0/1, receive
C   6::/64 [0/0]
     via GigabitEthernet0/0/0, directly connected
L   6::1/128 [0/0]
```

```
     via GigabitEthernet0/0/0, receive
L   FF00::/8 [0/0]
     via Null0, receive
```

R6:

```
0version 15.5
service timestamps debug datetime msec
service timestamps log datetime msec
no platform punt-keepalive disable-kernel-core
hostname R6
boot-start-marker
boot-end-marker
vrf definition Mgmt-intf
address-family ipv4
 exit-address-family
address-family ipv6
 exit-address-family
no aaa new-model
ipv6 unicast-routing
subscriber templating
vtp domain cisco
vtp mode transparent
multilink bundle-name authenticated
license udi pid ISR4321/K9 sn FDO21491FHX
spanning-tree extend system-id
redundancy
 mode none
vlan internal allocation policy ascending
interface GigabitEthernet0/0/0
 ip address 192.168.3.1 255.255.255.0
 ip router isis
 negotiation auto
 ipv6 address 7::1/64
 ipv6 enable
 ipv6 router isis
interface GigabitEthernet0/0/1
 ip address 192.168.1.18 255.255.255.252
 ip router isis
 negotiation auto
 ipv6 address 5::2/64
 ipv6 enable
 ipv6 router isis
interface GigabitEthernet0/1/0
 no ip address
 shutdown
 negotiation auto
interface GigabitEthernet0/1/1
 no ip address
 shutdown
 negotiation auto
interface GigabitEthernet0
 vrf forwarding Mgmt-intf
 no ip address
```

```
 shutdown
 negotiation auto
interface Vlan1
 no ip address
 shutdown
router isis
 net 49.0003.0000.0000.0006.00
 is-type level-1
ip forward-protocol nd
no ip http server
no ip http secure-server
ip tftp source-interface GigabitEthernet0
control-plane
line con 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 login
end


i*L1  0.0.0.0/0 [115/10] via 192.168.1.17, 00:07:20,
GigabitEthernet0/0/1
      192.168.1.0/24 is variably subnetted, 3 subnets, 2 masks
i L1     192.168.1.8/30
           [115/20] via 192.168.1.17, 00:08:18, GigabitEthernet0/0/1
C        192.168.1.16/30 is directly connected, GigabitEthernet0/0/1
L        192.168.1.18/32 is directly connected, GigabitEthernet0/0/1
      192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.3.0/24 is directly connected, GigabitEthernet0/0/0
L        192.168.3.1/32 is directly connected, GigabitEthernet0/0/0


IPv6 Routing Table - default - 7 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, I1 - ISIS L1, I2 - ISIS L2
       IA - ISIS interarea, IS - ISIS summary, D - EIGRP, EX - EIGRP
external
       ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr -
Redirect
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF
ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2, a - Application
I1  ::/0 [115/10]
     via FE80::521C:B0FF:FE2D:7101, GigabitEthernet0/0/1
I1  3::/64 [115/20]
     via FE80::521C:B0FF:FE2D:7101, GigabitEthernet0/0/1
C   5::/64 [0/0]
     via GigabitEthernet0/0/1, directly connected
L   5::2/128 [0/0]
     via GigabitEthernet0/0/1, receive
```

```
C   7::/64 [0/0]
     via GigabitEthernet0/0/0, directly connected
L   7::1/128 [0/0]
     via GigabitEthernet0/0/0, receive
L   FF00::/8 [0/0]
     via Null0, receive
```

Problems: In this lab, we has some problem to find out why after we changed the idea, all route is not working, we fix it by looking at cisco forum and noticed we need some router be on layer 1-2 and some need to be on layer 2**.**

Conclusion: In this lab, we learned how to config ISIS with 3 different area, we faced some problem due to we don't know much about this routing protocol. We solved this by scrolling cisco forum and found out we needs some router be layer 1 and 2 and some need to be layer 2 router. Overall this lab give us some hand on experience with configure ISIS routing protocol, which can be useful for future job situation.

Fortinet IPsec Site-to-Site VPN Lab

Port

By Alvin Chow

Purpose: In this lab, we learned how to configure an IPsec Site-to-Site VPN. We get hands-on experience in setting up a site-to-site VPN, which can be helpful in future job situations, especially in network administration or cybersecurity roles. In this lab, we also learned more about how VPNs function to securely connect remote networks over the internet. This experience makes us understand more network security concepts.

Background information:

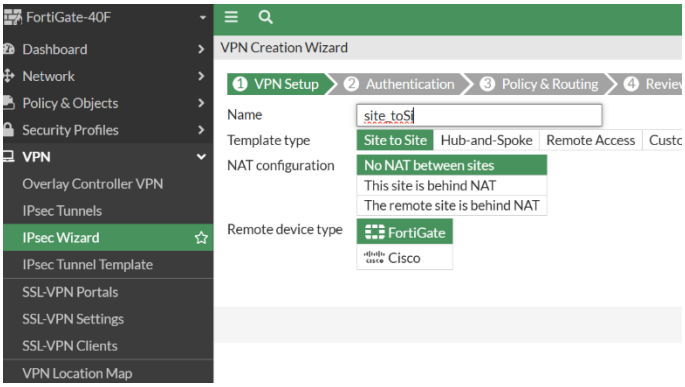
IPsec (Internet Protocol Security), IPsec is a protocol used to secure Internet Protocol (IP) communications by authenticating and encrypting each IP packet in a communication session. It operates at the network layer and supports data confidentiality, data integrity, and authentication between. IPsec is widely used to create secure Virtual Private Networks, by creating IPsec tunnel, it is useful for connecting remote sites or users over the internet.

A Site-to-Site VPN is a type of VPN connection used to securely connect two or more separate networks, most of it is between a branch office and a headquarters. This setup allows company resources to be shared between the sites, this function make them looks like on same local network. Site-to-Site VPNs commonly use IPsec to create encrypted tunnels, which can ensure secure communication between networks.

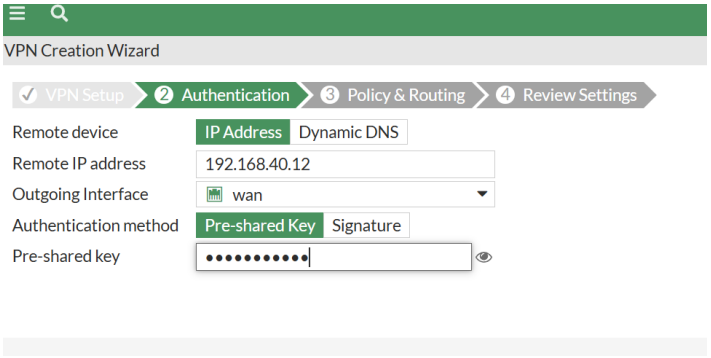
FortiGate firewall is a firewall that developed by Fortinet. These firewalls offer a wide range of security features including web filtering, antivirus, and VPN support. FortiGate devices are commonly used in enterprise environments and it known for easy to configuration. FortiGate firewalls support both IPsec and SSL VPNs and they are widely used to implement Site-to-Site VPNs because they have strong encryption and advanced routing features.

Lab Summary:

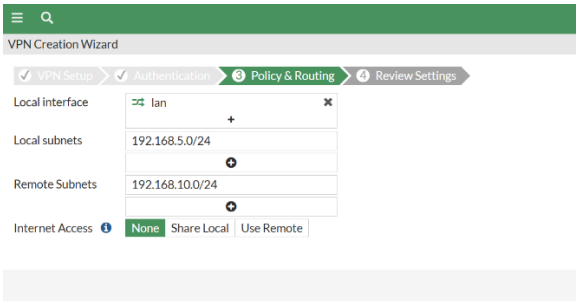
1. Make sure your local network IP is different to your remote local network. Then go to IPsec Wizard, name it, set it to Site to Site, NAT configuration is determined by your network, than the Remote device type is FortiGate. Then click next



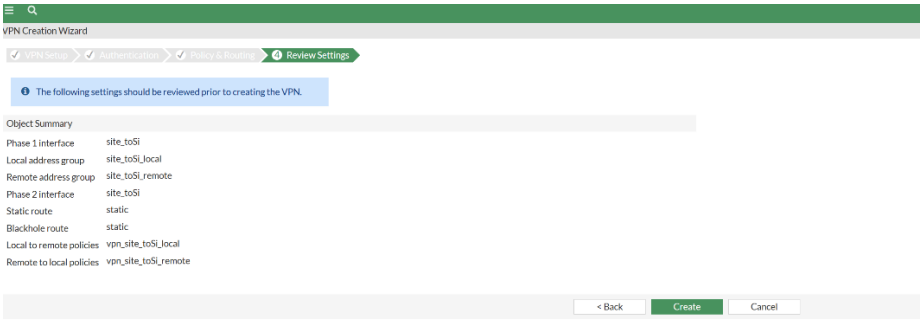
2. Enter your Remote Network WAN IP, set the authentication method as PSK and enter the PSK you going to use what authenticate for the connection. Then click next



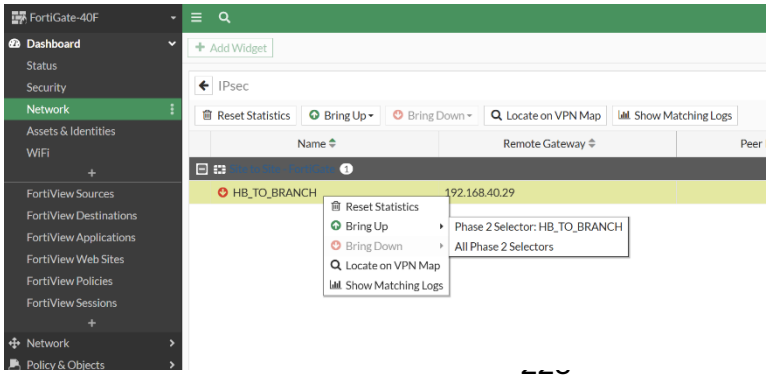
3. On the Local interface, set it to your LAN network, then enter the Remote Local subnets, on the Internet Access tab, you can choose the one that fit your needs. Then click next



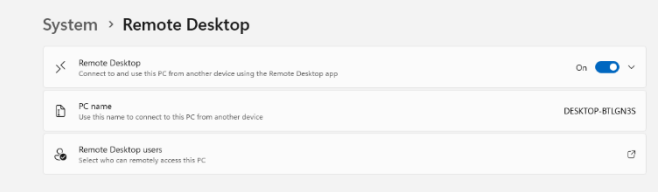
4. Make sure everything is correct then click create.

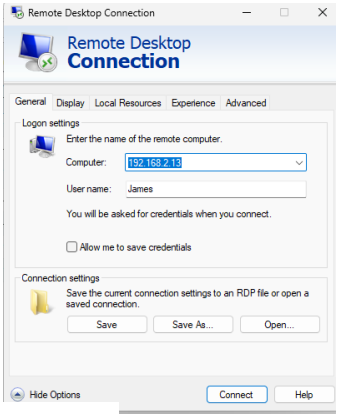


5. Repeat steps 1-4 on others site, remember the change the remote host WAN IP and the remote local subnets.
6. Go to Dashboard, Network, IPSec, then click bring up your IPsec site-to-site

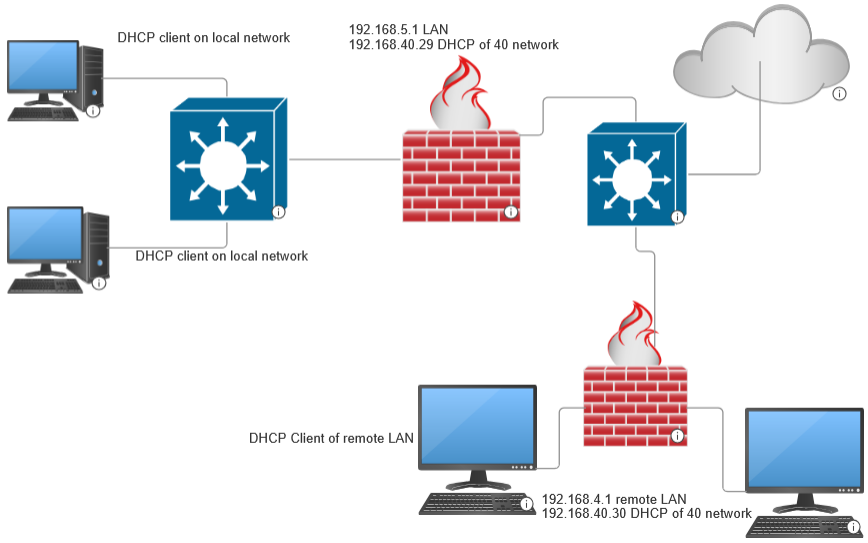


7. Turn on RDP on window setting and enter the IP of the computer on remote subnet.





Network Diagram:



Problems: In this lab, the main problem that we faced is we don't know we need to Bring up the IPsec on network tab, which make us waste sometime to troubleshoot it, we fixed it by looking at Fortinet forum.

Conclusion: In this lab we learned more about different between site-to-site VPN and remote access VPN, we also learned how to set up Site-to-Site VPN that using IPsec, one thing that did not go well that is we don't know we need to bring up the site-to-site connection. By learning many types of VPN and how to set it up, which can prepare for future job situation.