Networking Portfolio

Ethan Do

CISCO

paloalto NETWORKS

aws

Table of Contents

Windows Setup

Purpose

The purpose of this lab is to learn how to use a solid-state drive and set up an operating system & the necessary applications to succeed in the CCNP class.

Background Information

Operating systems are system software manage the computer's memory and processes, allowing user to utilize the computer's hardware resources through applications.

Windows 11 Education is the newest version of the Windows operating system and offers new productivity and security features compared to Windows 10. Compared to the Windows 11 Pro edition, Windows 11 Education allows the usage of AppLocker, persistent memory, and SMB Direct. In addition, compared to Windows 11 Home edition, Windows 11 Education allows hyper-virtualization, Resilient File System, and Group Policy. Windows 11 Education also has 36 months of servicing from its release date compared to the 24 months for the Windows Pro and Home editions.

There are several other applications needed to complete assignments.

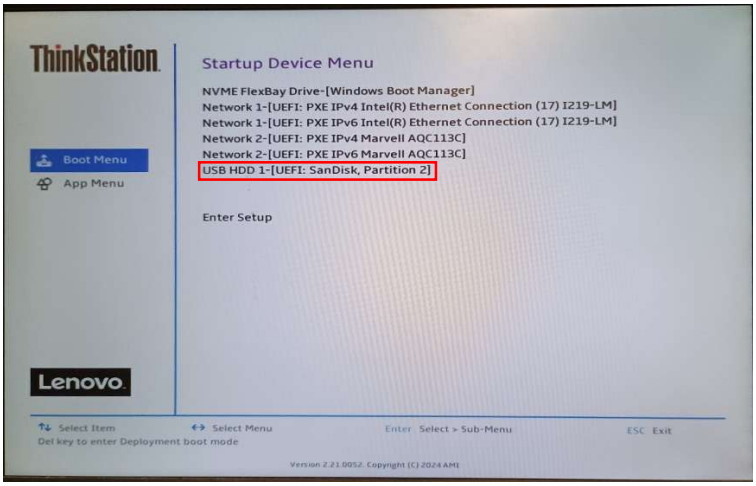
PuTTY is a free SSH and Telnet client used to connect to the console of routers, switches, and other networking devices. PuTTY or similar applications are needed in order to access and modify the configuration of networking devices.

Office 365 is a collection of productivity apps, including Word, Microsoft Teams, and OneDrive. Word and Microsoft Teams are especially useful in creating lab write-ups and the exchange of information with peers. OneDrive is used in backing up files to the cloud.

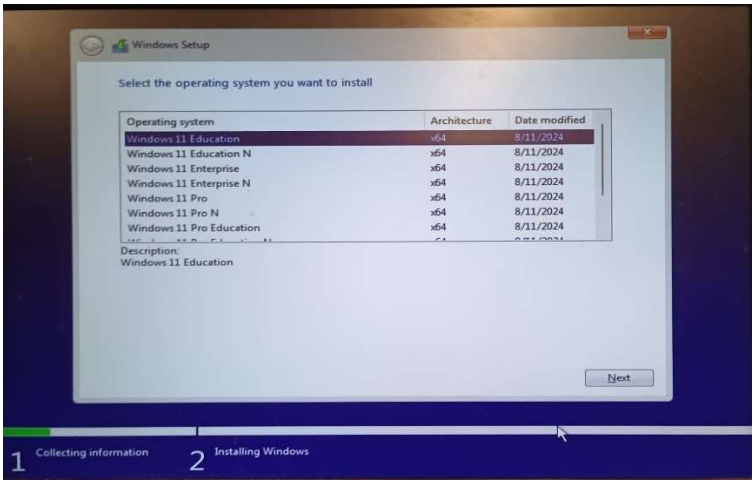
Lenovo Commercial Vantage is a tool used to make sure a device is healthy and up to date. Lenovo Commercial Vantage can also be used to download necessary security updates.

Lab Summary

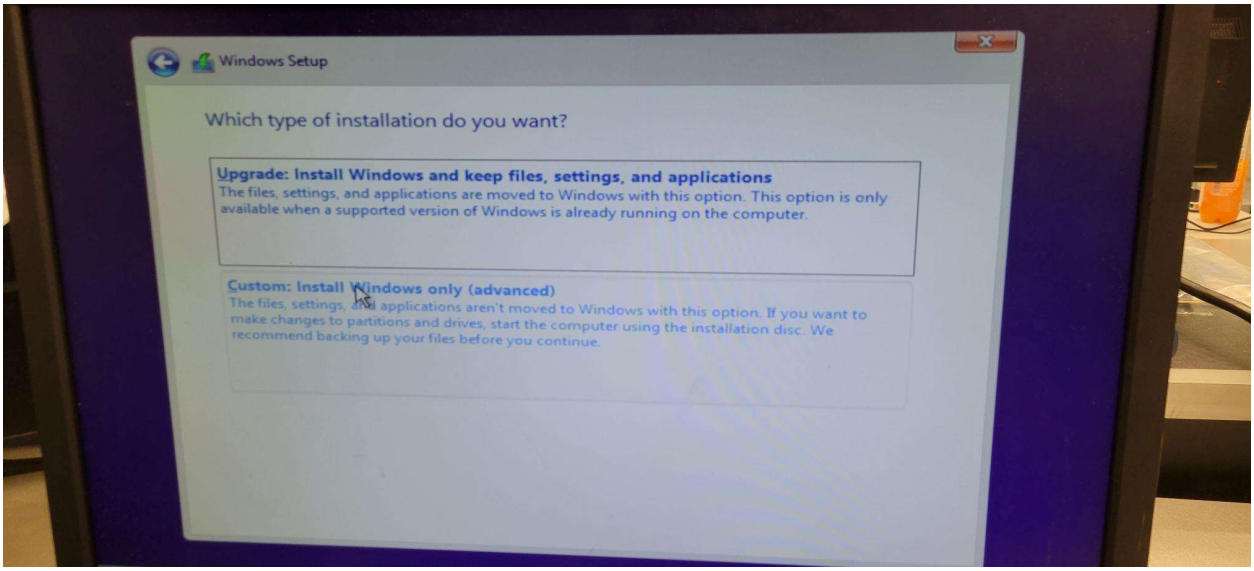
Plug in your flash drive and your USB drive containing Windows 11 Education. During bootup, press F12 until the following screen shows up. Press the option containing “USB”.



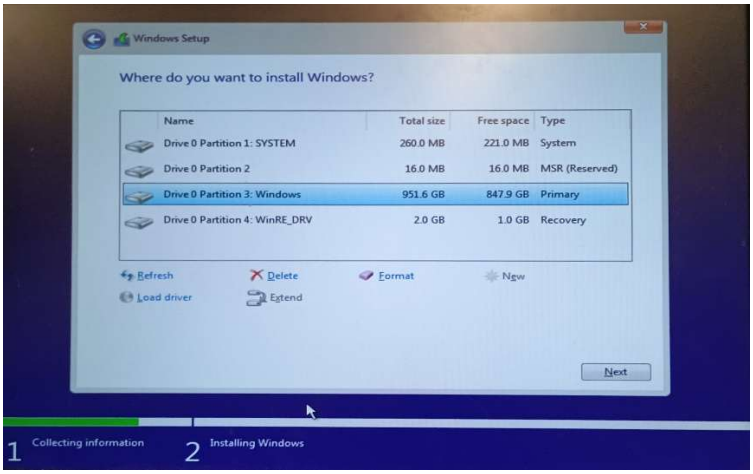
On the next screen, select Windows 11 Education, and click Next.



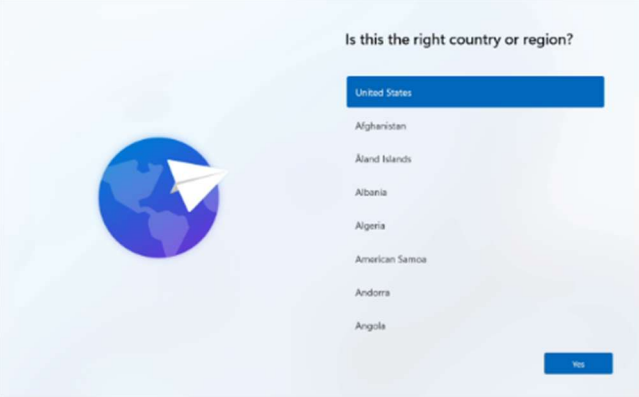
On the next screen, click Custom install.



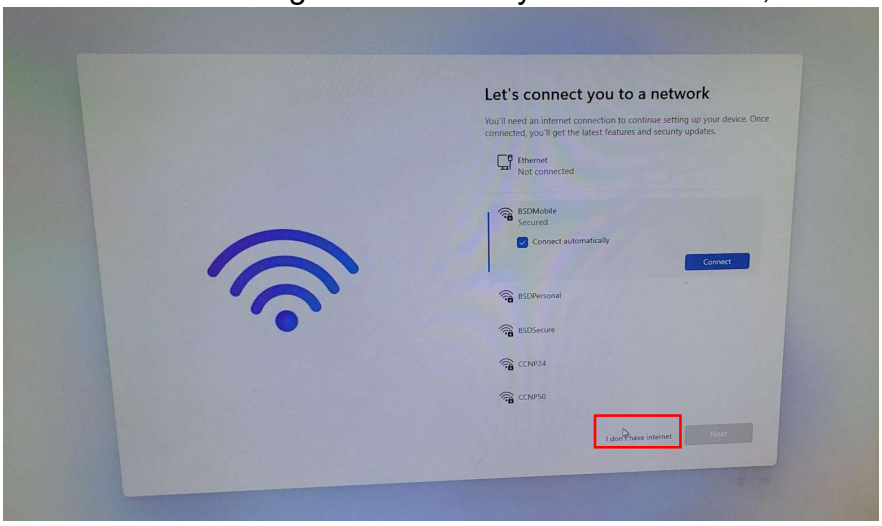
On the next screen, select the partition with a type of “Primary”, and click Next. Wait until installation is complete.



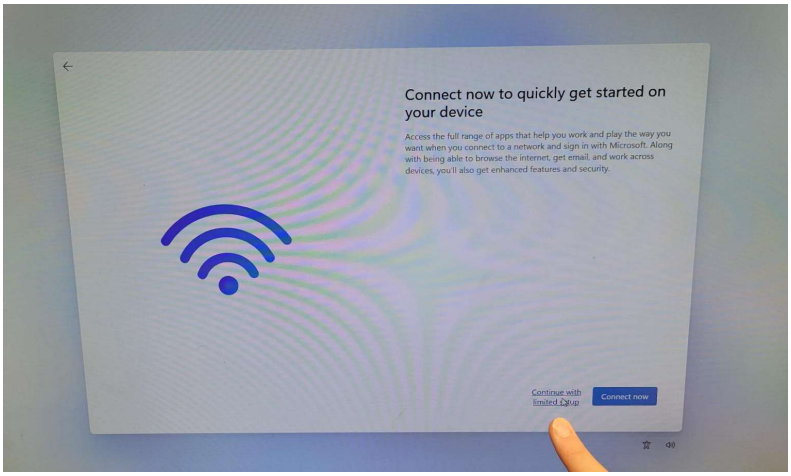
Once Windows is installed, select your country/region, keyboard layout, and second keyboard option.



On the screen stating “Lets connect you to a network”, select “I don’t have internet”.



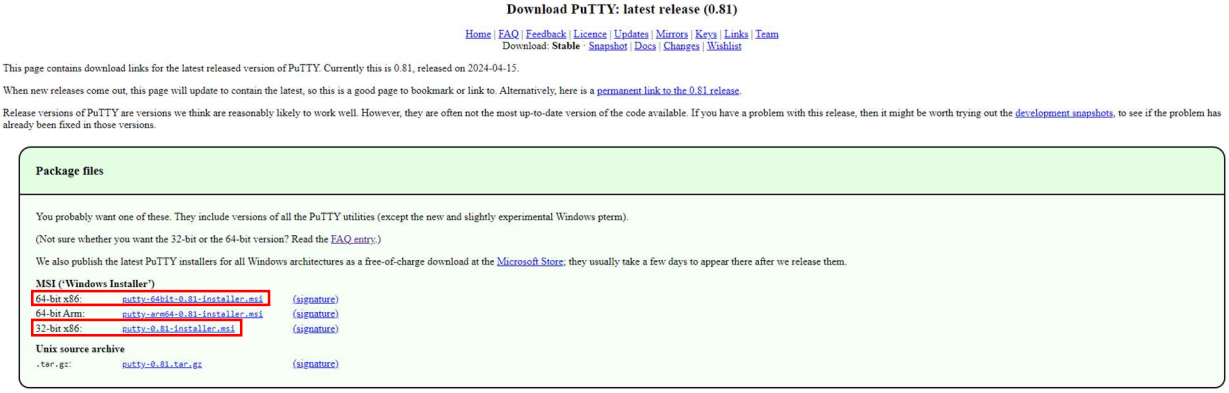
Then on the next screen, select “Continue with limited setup”. This will allow you to create a local account stored solely on your drive.



Enter the username and password you wish to use, and complete the security questions to ensure you have access to your account.

When finished with Windows installation, you will need to download PuTTY, Office 365 apps, and Lenovo Commercial Vantage.

To download PuTTY, go to https://www.putty.org/ and click on “Download Putty”. Choose the 64-bit or 32-bit version based on your needs.



Download PuTTY: latest release (0.81)

Home | FAQ | Feedback | Licence | Updates | Mirrors | Keys | Links | Team
Download: **Stable** · Snapshot | Docs | Changes | Wishlist

This page contains download links for the latest released version of PuTTY. Currently this is 0.81, released on 2024-04-15.

When new releases come out, this page will update to contain the latest, so this is a good page to bookmark or link to. Alternatively, here is a permanent link to the 0.81 release.

Release versions of PuTTY are versions we think are reasonably likely to work well. However, they are often not the most up-to-date version of the code available. If you have a problem with this release, then it might be worth trying out the development snapshots, to see if the problem has already been fixed in those versions.

Package files

You probably want one of these. They include versions of all the PuTTY utilities (except the new and slightly experimental Windows pterm).

(Not sure whether you want the 32-bit or the 64-bit version? Read the FAQ entry.)

We also publish the latest PuTTY installers for all Windows architectures as a free-of-charge download at the Microsoft Store; they usually take a few days to appear there after we release them.

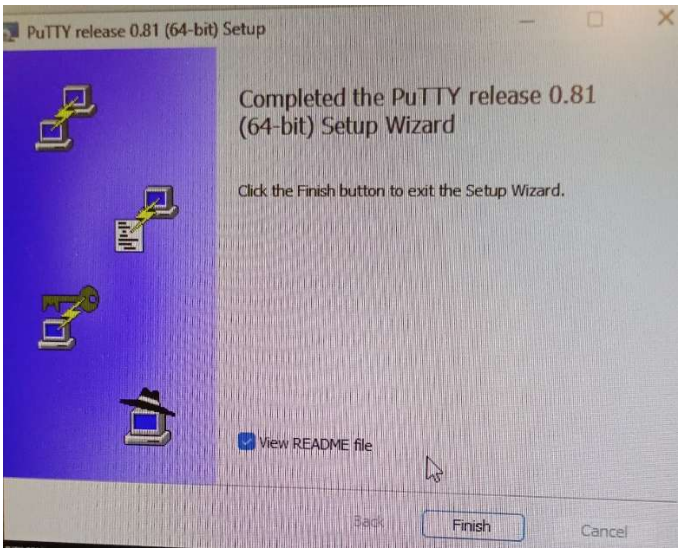
MSI ('Windows Installer')

64-bit x86:	putty-64bit-0.81-installer.msi	(signature)
64-bit Arm:	putty-arm64-0.81-installer.msi	(signature)
32-bit x86:	putty-0.81-installer.msi	(signature)

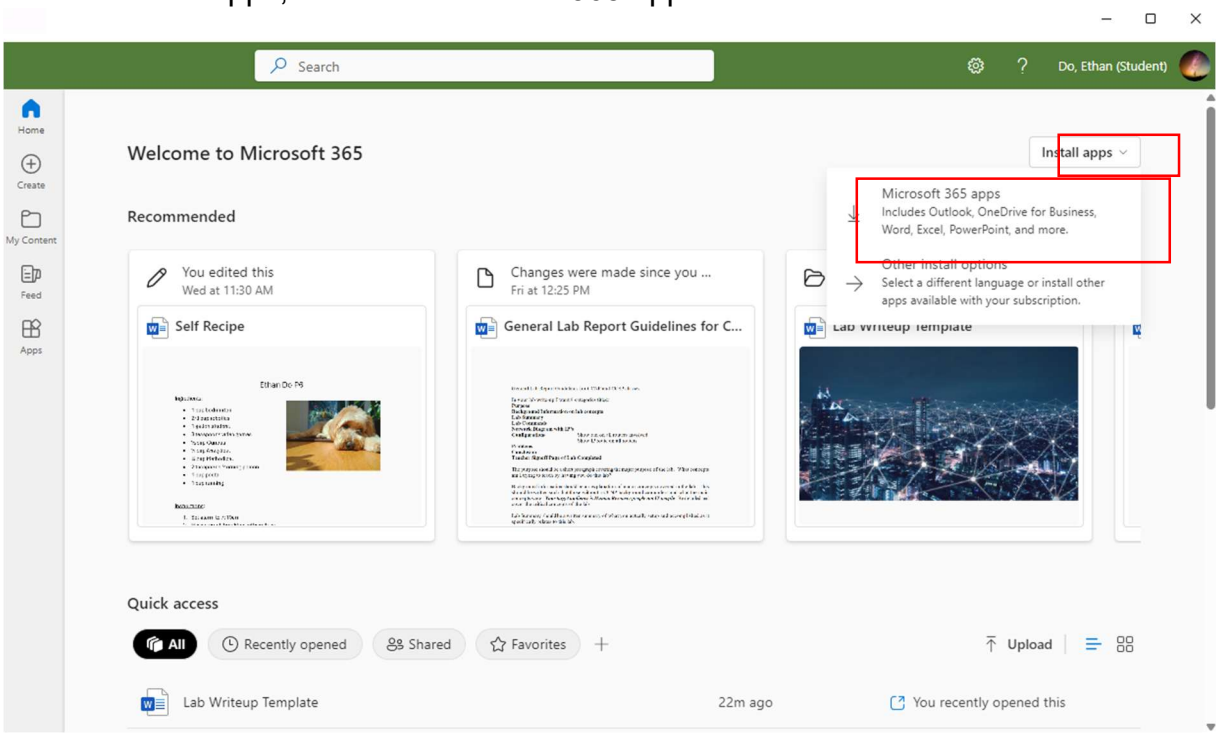
Unix source archive

.tar.gz:	putty-0.81.tar.gz	(signature)

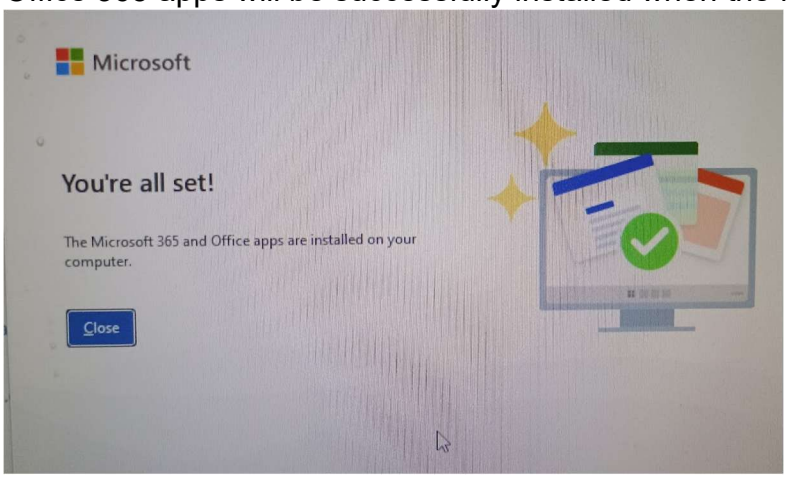
Run the downloaded file and follow the steps in the installer until you reach the following screen.



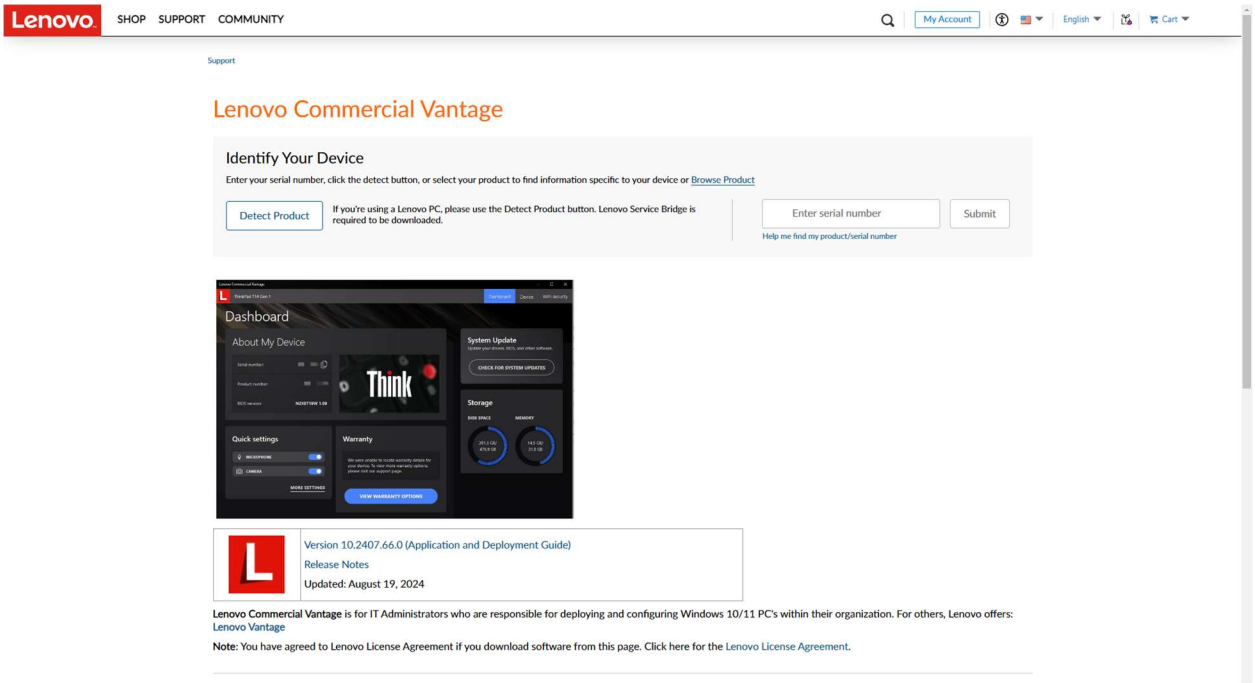
To download Office 365 apps, open Office and log into your Microsoft account. Then, click on install apps, and then Microsoft 365 apps.



Office 365 apps will be successfully installed when the following screen shows.

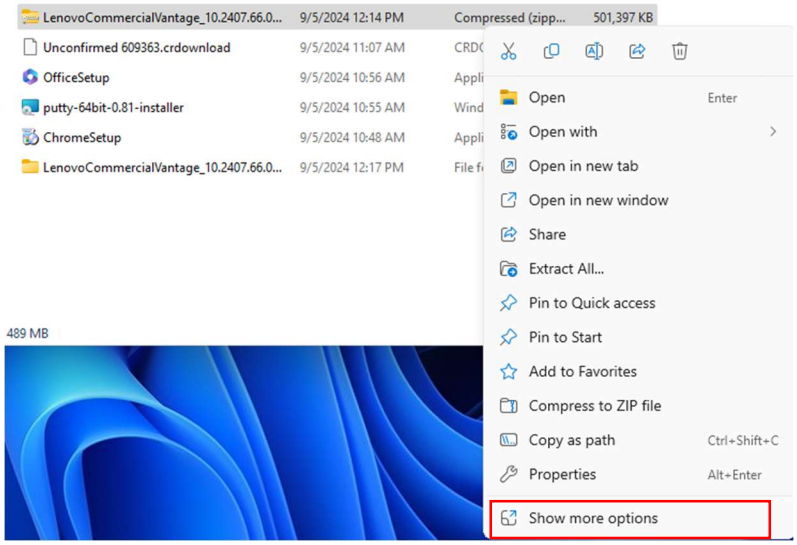


To download Lenovo Commercial Vantage, go to https://support.lenovo.com/us/en/solutions/hf003321-lenovo-vantage-for-enterprise and download the most recent version.

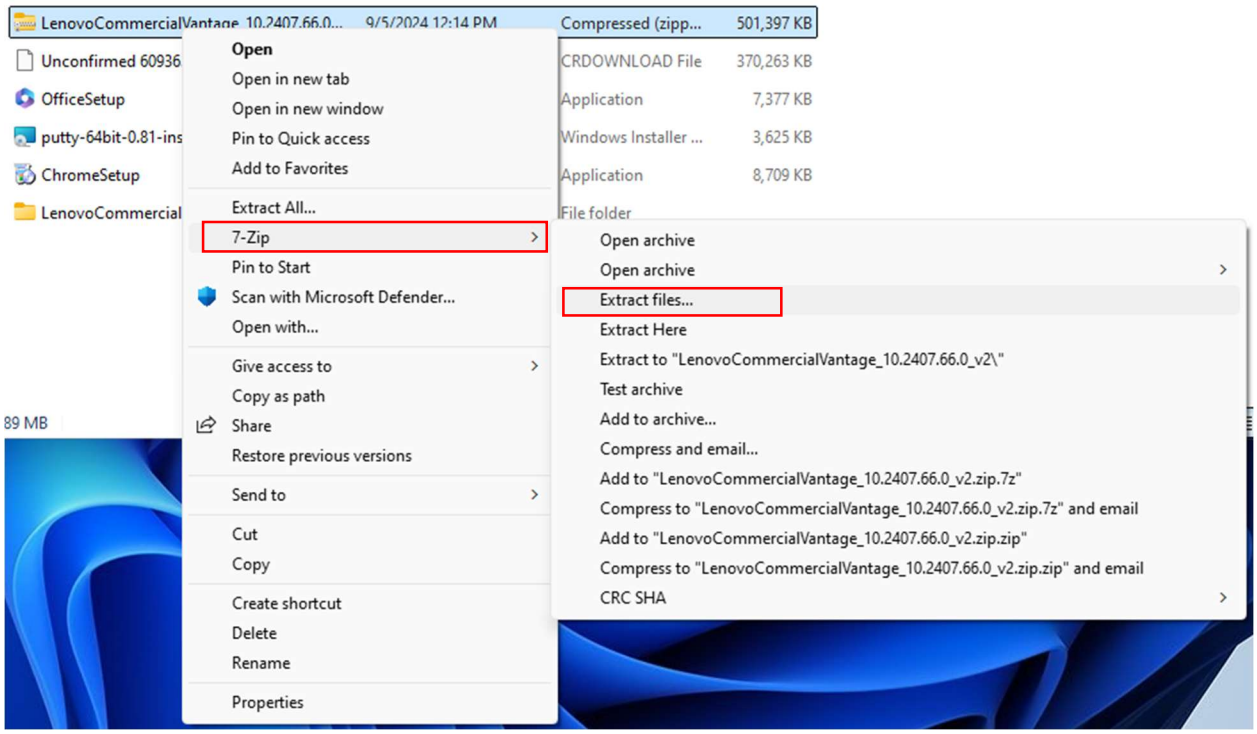


The file will be downloaded as a large zip file. To unzip it quickly, download 7-zip at https://www.7-zip.org/. Download the 64-bit version.

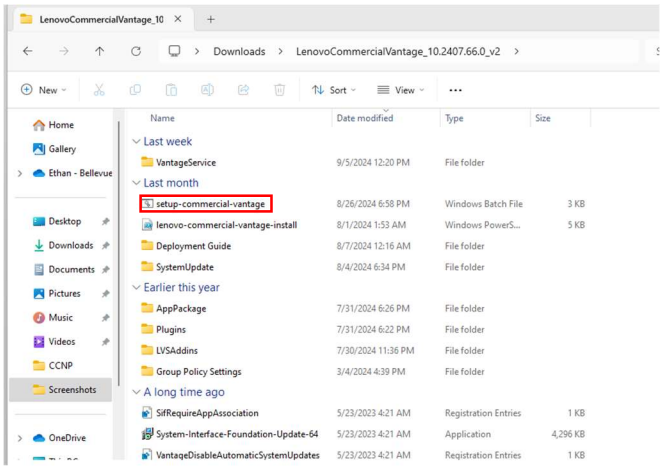
After downloading both the zip file and 7-zip, go to the downloads folder, right click on the zip file, and select “Show more options”.



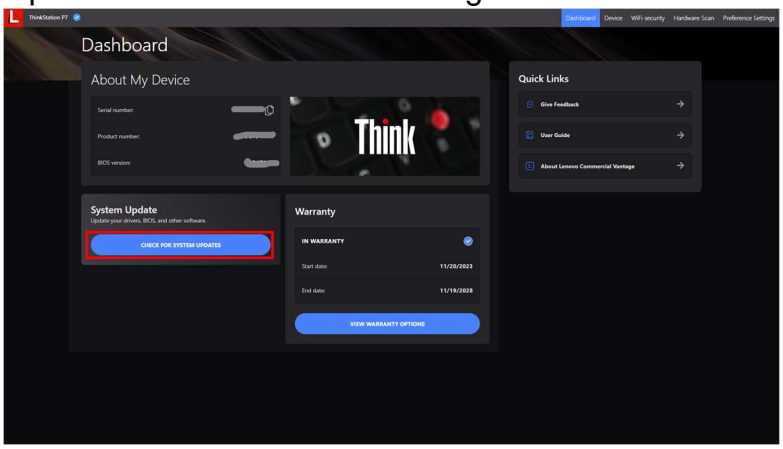
Then, click on 7-zip and extract files.



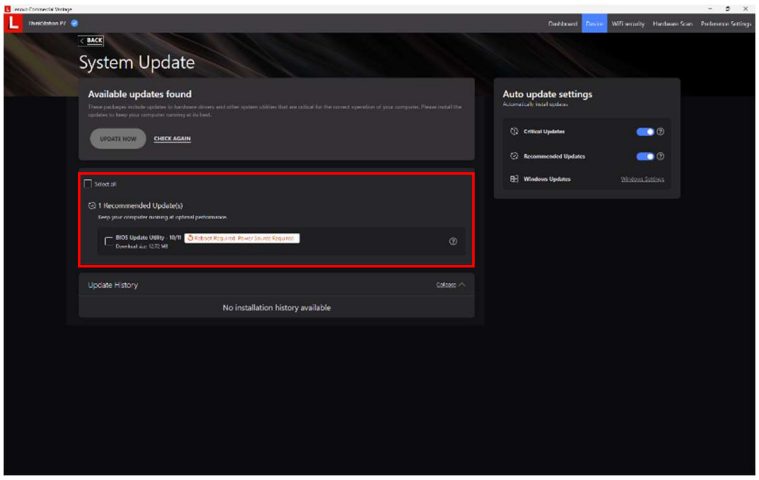
In the extracted folder, run the file “setup-commercial-vantage”. A command prompt window will open. When the window closes itself, Lenovo Commercial Vantage will be installed.



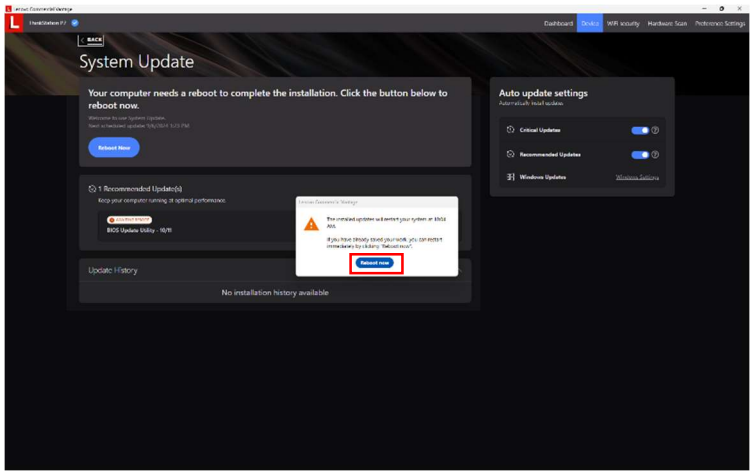
Open Lenovo Commercial Vantage. Click on “Check for System Updates”



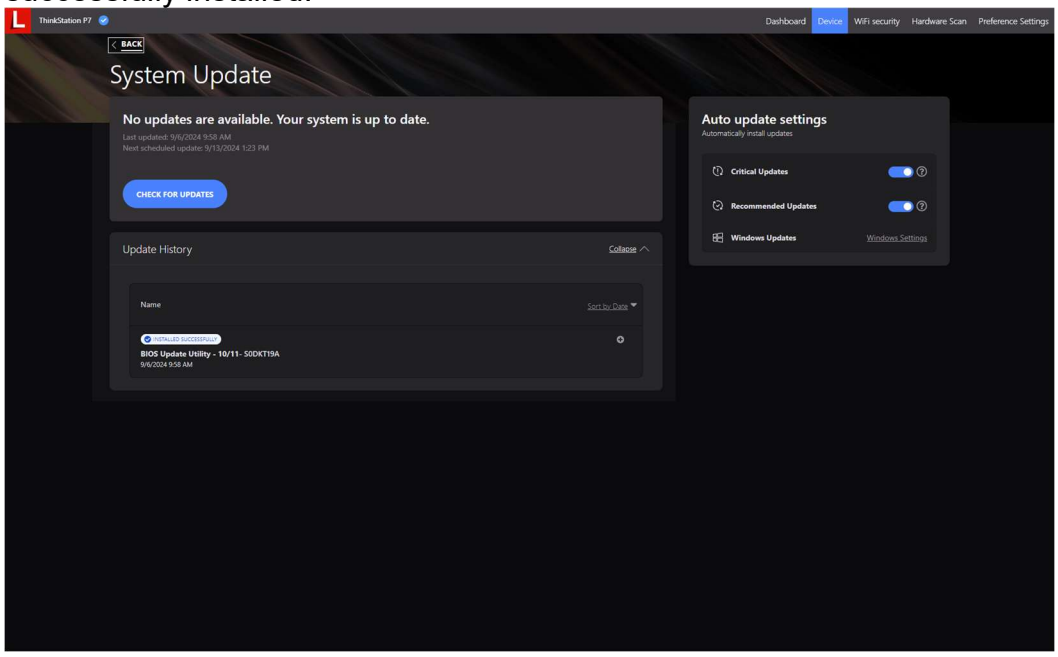
Check any of the recommended Updates and click “Update Now”.



If a restart is required, restart the computer after the update is installed.



After restarting, reopen Lenovo Commercial Vantage to make sure the update was successfully installed.



Problems

When unzipping the Lenovo commercial vantage file, the process using the native unzip function would have taken upwards of 40 minutes. To circumvent this, I downloaded 7-zip, allowing the process to take less than a minute to complete.

The desktop that I was using had trouble signing into Office. Moving to another desktop allowed me to sign in.

Conclusion

In this lab, I installed windows and the necessary apps (PuTTY, Office, Lenovo Commercial Vantage) to complete future labs in the CCNP class. I learned to setup local accounts for windows and how to secure my device.

Multi-Area OSPF

Purpose

The purpose of this lab is to review how to set up multi-area OSPF with routers and layer 3 switches.

Background Information

Routers are network devices that forward data packets between networks. Routers use routing protocols to determine where to send data packets by selecting the best path between routers.

Layer 3 switches combine the functionalities of routers and switches, supporting all switching features while providing basic routing functionalities between vlans. Routing is often faster than actual routers, but layer 3 switches often lack the advancing routing functionality of routers.

In order for a device to send and receive data packets, it must have an IP (Internet Protocol) address. IP addresses uniquely identifies devices and allow switches and routers to accurately send information. IPv4 (Internet Protocol version 4) is the most widely used version, and assigns each device a 32-bit long address. Due to only having 32 bits, there are only 4 billion unique addresses. While many are able to be “reused” through techniques like private networks, the world will quickly run out of these addresses. Thus, IPv4 (Internet Protocol version 6) was created with 128 bits, allowing 3.4 x 1038 unique addresses.

OSPF (Open Shortest Path First) is a link-state routing protocol. OSPF uses the shortest path first algorithm (SPF, also known as Dijkstra’s algorithm) to calculate the lowest cost path to send a data packet. This ensures the best use of bandwidth and allows more complex and scalable networks.

OSPFv2 is the previous version of OSPF, only working with IPv4 addresses. To implement the same connectivity with IPv6 addresses, OSPFv3, the newest version of OSPF, must be used. OSPFv2 allows configuration through network statements, interfaces, and vlans, while OSPFv3 requires the configuration of OSPF on interfaces.

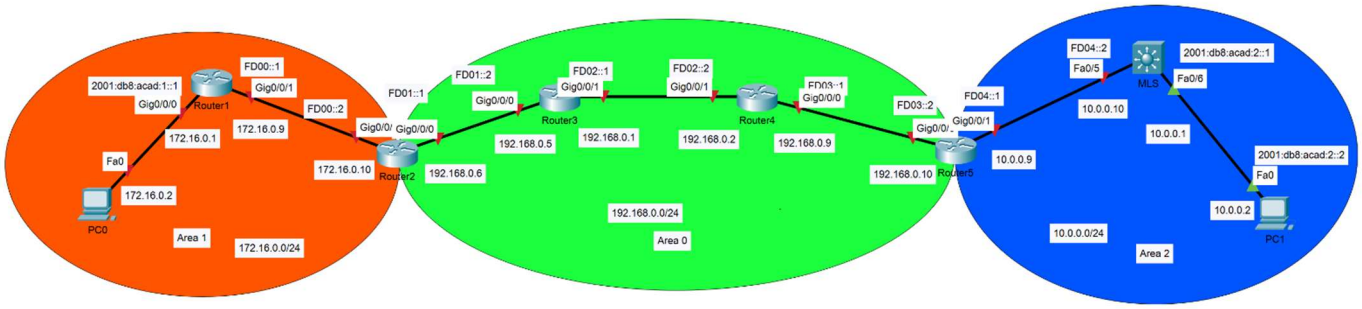
Lab Summary

In this lab, I set up multi-area OSPF for IPv4 and IPv6. Each router and layer 3 switch is given static IPv4 and IPv6 addresses and an OSPF process ID. For IPv4, each router must then specify the area ID of each network that the router is a part of. For IPv6, each interface that the router is using must be set with the correct area ID.

Lab Commands

```
ip add [IP address] [subnet mask]
router ospf [process-id]
network [network address] [wild bits] area [area-id]
ipv6 unicast-routing
ipv6 enable
ipv6 add [IPv6 address]
ipv6 router ospf [process-id]
ipv6 ospf [process-id] area [area-id]
```

Network Diagram



Configurations

Router 1

```
version 16.9
service timestamps debug datetime msec
service timestamps log datetime msec
platform qfp utilization monitor load 80
platform punt-keepalive disable-kernel-core
hostname Router1
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
login on-success log
subscriber templating
ipv6 unicast-routing
multilink bundle-name authenticated
license udi pid ISR4321/K9 sn FDO21080CTW
no license smart enable
diagnostic bootup level minimal
spanning-tree extend system-id
redundancy
 mode none
interface GigabitEthernet0/0/0
 ip address 192.168.1.1 255.255.255.0
 shutdown
 negotiation auto
 ipv6 address 2001:DB8:ACAD:F::2/64
 ipv6 ospf 1 area 0
interface GigabitEthernet0/0/1
 ip address 192.168.0.1 255.255.255.0
 shutdown
 negotiation auto
 ipv6 address 2001:DB8:ACAD:A::2/64
 ipv6 ospf 1 area 1
interface Serial0/1/0
interface Serial0/1/1
interface Service-Engine0/2/0
 no ip address
interface GigabitEthernet0
 vrf forwarding Mgmt-intf
 no ip address
 shutdown
 negotiation auto
```

```
router ospfv3 1
 router-id 0.0.0.1
 address-family ipv6 unicast
 exit-address-family
router ospf 1
 router-id 0.0.0.1
 network 192.168.0.0 0.0.0.255 area 1
 network 192.168.1.0 0.0.0.255 area 0
ip forward-protocol nd
ip http server
ip http authentication local
ip http secure-server
ip tftp source-interface GigabitEthernet0
control-plane
line con 0
 transport input none
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 login
endinterface GigabitEthernet0/0/0
 ip address 172.16.0.1 255.255.255.248
 negotiation auto
 ipv6 address 2001:DB8:ACAD:1::1/64
 ipv6 enable
 ipv6 ospf 1 area 1
interface GigabitEthernet0/0/1
 ip address 172.16.0.9 255.255.255.252
 negotiation auto
 ipv6 address FD00::1/64
 ipv6 enable
 ipv6 ospf 1 area 1
router ospf 1
 router-id 0.0.0.1
 network 172.16.0.0 0.0.0.255 area 1
ipv6 router ospf 1
 router-id 0.0.0.1
```

Router 2

```
version 15.5
service timestamps debug datetime msec
service timestamps log datetime msec
no platform punt-keepalive disable-kernel-core
hostname Router2
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

no ip domain lookup
ipv6 unicast-routing
subscriber templating
vtp domain cisco
vtp mode transparent
multilink bundle-name authenticated
license udi pid ISR4321/K9 sn FDO214328EH
spanning-tree extend system-id
redundancy
 mode none
vlan internal allocation policy ascending
interface GigabitEthernet0/0/0
 ip address 192.168.1.2 255.255.255.0
 shutdown
 negotiation auto
 ipv6 address 2001:DB8:ACAD:B::1/64
 ipv6 ospf 1 area 0
interface GigabitEthernet0/0/1
 ip address 192.168.0.2 255.255.255.0
 shutdown
 negotiation auto
 ipv6 address 2001:DB8:ACAD:A::2/64
 ipv6 ospf 1 area 1
interface Serial0/1/0
 no ip address
 shutdown
interface Serial0/1/1
 no ip address
 shutdown
interface Service-Engine0/2/0
interface GigabitEthernet0
 vrf forwarding Mgmt-intf
 no ip address
 shutdown
 negotiation auto
interface Vlan1
 no ip address
 shutdown
router ospfv3 1
 router-id 0.0.0.2
 address-family ipv6 unicast
 exit-address-family
router ospf 1
 router-id 0.0.0.2
 network 192.168.0.0 0.0.0.255 area 1
```

```
ip forward-protocol nd
no ip http server
no ip http secure-server
ip tftp source-interface GigabitEthernet0
control-plane
line con 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 login
end
```

Router 3

```
version 15.5
service timestamps debug datetime msec
service timestamps log datetime msec
no platform punt-keepalive disable-kernel-core
hostname Router3
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
no ip domain lookup
ipv6 unicast-routing
subscriber templating
multilink bundle-name authenticated
license udi pid ISR4321/K9 sn FDO214414TX
spanning-tree extend system-id
redundancy
 mode none
vlan internal allocation policy ascending
interface GigabitEthernet0/0/0
 ip address 192.168.0.5 255.255.255.252
 shutdown
 negotiation auto
 ipv6 address FD01::2/64
 ipv6 enable
 ipv6 ospf 1 area 0
interface GigabitEthernet0/0/1
 ip address 192.168.0.1 255.255.255.252
 shutdown
 negotiation auto
```

```
 ipv6 address FD02::1/64
 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
 router-id 0.0.0.3
 network 192.168.0.0 0.0.0.255 area 0
ip forward-protocol nd
no ip http server
no ip http secure-server
ip tftp source-interface GigabitEthernet0
ipv6 router ospf 1
 router-id 0.0.0.3
control-plane
line con 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 login
end
```

Router 4

```
version 16.9
service timestamps debug datetime msec
service timestamps log datetime msec
platform qfp utilization monitor load 80
```

```
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
login on-success log
subscriber templating
ipv6 unicast-routing
multilink bundle-name authenticated
license udi pid ISR4321/K9 sn FDO214811ZM
no license smart enable
diagnostic bootup level minimal
spanning-tree extend system-id
redundancy
 mode none
interface Loopback0
 ip address 4.4.4.4 255.255.255.255
interface GigabitEthernet0/0/0
 ip address 192.168.0.9 255.255.255.252
 shutdown
 negotiation auto
 ipv6 address FD03::1/64
interface GigabitEthernet0/0/1
 ip address 192.168.0.2 255.255.255.252
 shutdown
 negotiation auto
 ipv6 address FD02::2/64
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
router ospf 1
```

```
 router-id 4.4.4.4
 network 192.168.0.0 0.0.0.255 area 0
ip forward-protocol nd
ip http server
ip http authentication local
ip http secure-server
ip tftp source-interface GigabitEthernet0
control-plane
line con 0
 transport input none
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 login
end
```

Router 5

```
version 16.9
service timestamps debug datetime msec
service timestamps log datetime msec
platform qfp utilization monitor load 80
no platform punt-keepalive disable-kernel-core
hostname R5
boot-start-marker
boot system flash bootflash:isr4300-universalk9.16.09.08.SPA.bin
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 pool webuidhcp
login on-success log
subscriber templating
ipv6 unicast-routing
multilink bundle-name authenticated
license udi pid ISR4321/K9 sn FLM240607T3
no license smart enable
diagnostic bootup level minimal
spanning-tree extend system-id
redundancy
 mode none
interface Loopback0
 ip address 5.5.5.5 255.255.255.255
interface GigabitEthernet0/0/0
 ip address 192.168.0.10 255.255.255.252
```

```
 shutdown
 negotiation auto
 ipv6 address FD03::2/64
interface GigabitEthernet0/0/1
 ip address 10.0.0.9 255.255.255.0
 shutdown
 negotiation auto
 ipv6 address FD04::1/64
interface GigabitEthernet0
 vrf forwarding Mgmt-intf
 no ip address
 shutdown
 negotiation auto
router ospf 1
 router-id 5.5.5.5
 network 10.0.0.0 0.0.0.255 area 2
 network 192.168.0.0 0.0.0.255 area 0
ip forward-protocol nd
ip http server
ip http authentication local
ip http secure-server
ip tftp source-interface GigabitEthernet0
control-plane
line con 0
 transport input none
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 login
end
```

MLS

```
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
hostname MultilayerSwitch
boot-start-marker
boot-end-marker
no aaa new-model
system mtu routing 1500
ip routing
ipv6 unicast-routing
spanning-tree mode pvst
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
 no switchport
 ip address 10.0.0.10 255.255.255.252
 ipv6 address FD04::2/64
 ipv6 ospf 1 area 2
interface FastEthernet0/6
 no switchport
 ip address 10.0.0.1 255.255.255.252
 ipv6 address 2001:DB8:ACAD:2::1/64
 ipv6 ospf 1 area 2
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
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
 ip address 192.168.10.1 255.255.255.0
router ospf 1
 router-id 6.6.6.6
 log-adjacency-changes
 network 10.0.0.0 0.0.0.255 area 2
ip classless
ip http server
ip http secure-server
ipv6 router ospf 1
 router-id 6.6.6.6
 log-adjacency-changes
line con 0
line vty 0 4
 login
line vty 5 15
 login
end
```

Problems

This lab involved the usage of the Cisco Catalyst 3560, a layer 3 switch. We encountered a multitude of issues with this switch.

1. Our rack had a faulty Cisco Catalyst 3560 switch. This was indicated by a solid amber SYST light and solid green lights below it on the front panel. We had to swap out this switch in order to access the console.

2. Our new Catalyst 3560 had the IPBASE IOS image installed on it, rather than the IPSERVICES IOS image. The IPBASE image is significantly cheaper than the IPSERVICES image, but does not come with several protocols, including OSPF. Therefore, to complete this lab with the Catalyst 3560, we needed to give the switch the IPSERVICES image.
   Our first attempt to solve this was to connect our Catalyst 3560 switch (Switch A) to another Catalyst 3560 switch (Switch B) that has the IPSERVICES image. By settings up a TFTP (trivial file transfer protocol) server on Switch B, we were able to upload the IPSERVICES image file onto the server and transfer it to Switch A. However, the Catalyst 3560 does not have enough storage to have two image files on it at once. Trying to copy the file onto Switch A gave an error “Timed out”, which indicated that there wasn’t enough space. Even after deleting the original image file, we got the same error, so we concluded that we were unable to transfer the image over a tftp connection between the two switches.

   Our solution was to use a program called Tftpd64, a free and open-source application that supports among other protocols, TFTP, and can function as a TFTP client. Using this program, we were able to copy the image from Switch B onto a flash drive and then copy the image from the flash drive to Switch A. Lastly, we had to reset the boot path to make sure the switch would boot with the correct image, using the boot system [file path] command.

Conclusion

In this lab, we successfully implemented a network using multi-area OSPF, allowing connectivity across three areas. This involved the configuration of 5 routers and 1 layer 3 switch. The layer 3 switch also involved replacing the base IOS image present with one that contained the OSPF protocol.

BGP

Purpose

The purpose of this lab is to set up three autonomous systems, each with a different interior routing protocol, and connect autonomous systems with BGP.

Background Information

Autonomous Systems

The internet can be segregated into routing domains named autonomous systems (ASs), which can have their own routing information and policies. BGP, or Border Gateway Protocol, assumes that routing within an autonomous system is already complete through an Interior Gateway Protocol, such as OSPF or EIGRP.

BGP

BGP functions by assuming the network is a graph of distinct autonomous systems and provides routing information to ensure loop-free interdomain routing.

BGP is a path vector protocol, meaning that BGP routing information carries a series of AS numbers that identifies the path that information takes. This information is used to prevent loops for occurring.

Routers that run BGP are called BGP speakers. When two speakers form a connection, they are referred to as peers. When this connection forms, all BGP routes are exchanged. After this initial route exchange, updates are only sent incrementally as other network information changes.

BGP speakers establishes connections using an OPEN message, which states the version, autonomous system, hold timer, BGP identifier, and other optional parameters of the BGP speaker. Once a connection is formed, each speaker needs to send KEEPALIVE messages to ensure the connection is kept. Any updates, such as new or withdrawn routes, are sent using the UPDATE message.

Interior Gateway Protocols

An Interior Gateway Protocol manages the routing information within an AS, as opposed to BGP managing the routing information between autonomous systems. The Interior Gateway Protocols used in this lab are OSPF, IS-IS, and EIGRP.

OSPF

OSPF is a link-state routing protocol. Link-state routing protocols work on the basis that routers will exchange information, called link states, on the links and nodes in a routing domain. Rather than exchanging a routing table, routers running a link-state routing protocol will exchange information on adjacent neighbors and networks.

A link-state protocol provides several benefits – there is no hop limit a route a take, link bandwidth can be a factor in calculating the shortest path, there is better convergence in the network, and VLSM and CIDR are both supported.

OSPF operates on Layer 3, and requires IP connectivity in order to for routers to exchange OSPF information. This dependance on Layer 3 makes it more prone to attacks, and therefore often needs more security configurations to protect it. OSPF also uses areas, split into the Backbone Area (Area 0) and Standard Areas (non-area 0).

IS-IS

IS-IS is also a link-state protocol, with several differences from OSPF. IS-IS operates on Layer 2, not requiring IP connectivity, and therefore is less vulnerable to attacks. IS-IS also uses Levels in place of area, split into Level 1 and Level 2. Level 1 Routers are only aware of the topology inside of their “area”, while Level 2 Routers can handle routing between “areas”, similar to how the Backbone Area of OSPF functions.

EIGRP

EIGRP is a distance vector protocol. Distance vector protocols use a distributed computation approach in calculating the best path for a route. After each router selects a best path for each destination prefix, they send distance vectors to neighboring routers with the metrics of the selected paths. After receiving distance vectors, each router may determine a better path and update neighbors of its new path.

Older distance vector protocols, such as RIP-1, used refresh timers to check if a path was available. EIGRP, however, uses triggered updates, which propagate link failures the moment that they occur, which allows for faster convergence.

EIGRP also allows the usage of VLSM and CIDR. It also allows bandwidth, utilization, delay, and MTU in calculate of path metrics.

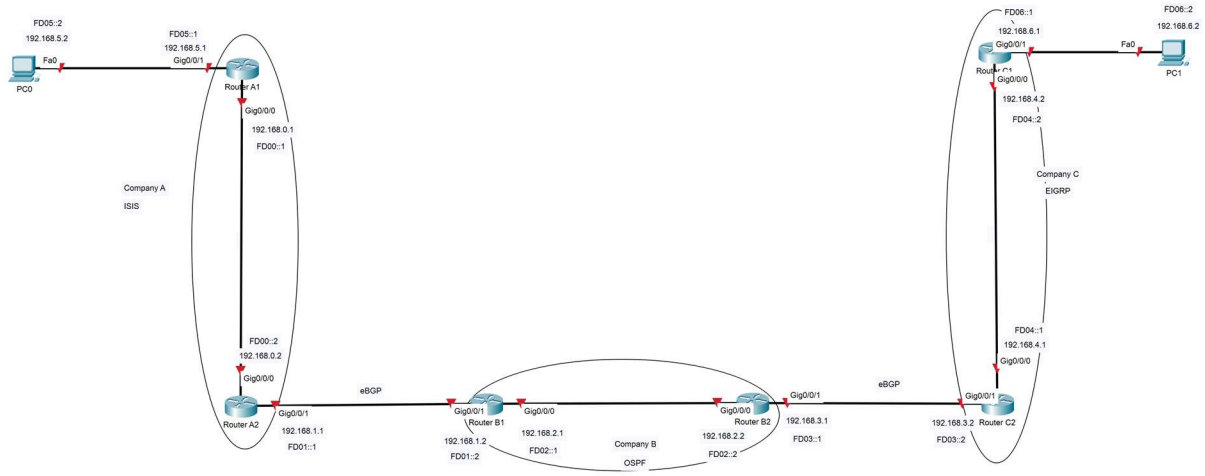
Lab Summary

In this lab, we configured three separate autonomous systems, with IS-IS, OSPF, and EIGRP each being the interior gateway protocol for one autonomous system. We then configured BGP between autonomous systems in order to distribute routes across the network.

Lab Commands

```
router isis
 net [Network Entity Title]
 is-type level-1
 metric-style narrow
 redistribute connected
 redistribute bgp [process ID]
router bgp [AS ID]
 bgp router-id [Router ID]
 neighbor [Neighbor IPv4 Address] remote-as [Neighbor AS ID]
 neighbor [Neighbor IPv6 Address] remote-as [Neighbor AS ID]
 neighbor [Neighbor IPv6 Address] update-source [Connected Interface]
 address-family ipv4
  network [network address]
  redistribute connected
  redistribute ospf [process ID] match external internal
  redistribute eigrp [ID]
  redistribute isis level-1
  neighbor [Neighbor IPv4 Address] activate
 exit-address-family
 address-family ipv6
  redistribute connected
  redistribute ospf [process ID] match external internal
  redistribute eigrp [process ID]
  redistribute isis level-1
  neighbor [Neighbor IPv6 Address] activate
router eigrp [process ID]
 default-metric 10000 100 255 1 1500
 network [network address]
 redistribute connected
 redistribute bgp [process ID]
router ospf [process ID]
 router-id 4.4.4.4
 redistribute connected subnets
 redistribute bgp 3333 subnets
 network 192.168.2.0 0.0.0.255 area 0
```

Network Diagram



Configurations

Router A1

```
version 16.9
service timestamps debug datetime msec
service timestamps log datetime msec
platform qfp utilization monitor load 80
platform punt-keepalive disable-kernel-core
hostname A1
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
login on-success log
subscriber templating
ipv6 unicast-routing
multilink bundle-name authenticated
license udi pid ISR4321/K9 sn FDO21080CTW
no license smart enable
diagnostic bootup level minimal
spanning-tree extend system-id
redundancy
 mode none
interface GigabitEthernet0/0/0
 ip address 192.168.0.1 255.255.255.0
 ip router isis
 negotiation auto
 ipv6 address FD00::1/64
 ipv6 router isis
 isis circuit-type level-1
```

```
interface GigabitEthernet0/0/1
 ip address 192.168.5.1 255.255.255.0
 ip router isis
 negotiation auto
 ipv6 address FD05::1/64
 ipv6 router isis
 isis circuit-type level-1
interface Serial0/1/0
 no ip address
 shutdown
interface Serial0/1/1
 no ip address
 shutdown
interface Service-Engine0/2/0
 no ip address
interface GigabitEthernet0
 vrf forwarding Mgmt-intf
 no ip address
 shutdown
 negotiation auto
router isis
 net 49.0001.1920.1680.0001.00
 is-type level-1
 metric-style narrow
 redistribute connected
ip forward-protocol nd
ip http server
ip http authentication local
ip http secure-server
ip tftp source-interface GigabitEthernet0
control-plane
line con 0
 transport input none
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 login
end
```

Router A2

```
version 15.5
service timestamps debug datetime msec
service timestamps log datetime msec
no platform punt-keepalive disable-kernel-core
hostname A2
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 FDO214328EH
spanning-tree extend system-id
redundancy
 mode none
vlan internal allocation policy ascending
vlan 10,20
interface GigabitEthernet0/0/0
 ip address 192.168.0.2 255.255.255.0
 ip router isis
 negotiation auto
 ipv6 address FD00::2/64
 ipv6 router isis
 isis circuit-type level-1
interface GigabitEthernet0/0/1
 ip address 192.168.1.1 255.255.255.0
 ip router isis
 negotiation auto
 ipv6 address FD01::1/64
 ipv6 router isis
 isis circuit-type level-1
interface Serial0/1/0
 no ip address
 shutdown
interface Serial0/1/1
 no ip address
 shutdown
interface Service-Engine0/2/0
 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 49.0001.1920.1680.0002.00
 is-type level-1
 redistribute connected
 redistribute bgp 2222 level-1
 address-family ipv6
  redistribute connected
  redistribute bgp 2222 level-1
```

```
 exit-address-family
router bgp 2222
 bgp router-id 2.2.2.2
 bgp log-neighbor-changes
 neighbor 192.168.1.2 remote-as 3333
 neighbor FD01::2 remote-as 3333
 neighbor FD01::2 update-source GigabitEthernet0/0/1
 address-family ipv4
  network 192.168.1.0
  redistribute connected
  redistribute isis level-1
  neighbor 192.168.1.2 activate
  no neighbor FD01::2 activate
 exit-address-family
 address-family ipv6
  redistribute connected
  redistribute isis level-1
  neighbor FD01::2 activate
 exit-address-family
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
```

Router B1

```
version 15.5
service timestamps debug datetime msec
service timestamps log datetime msec
no platform punt-keepalive disable-kernel-core
hostname B1
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
no ip domain lookup
ipv6 unicast-routing
subscriber templating
```

```
multilink bundle-name authenticated
license udi pid ISR4321/K9 sn FDO214414TX
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 ospf 1 area 0
 negotiation auto
 ipv6 address FD02::1/64
 ipv6 ospf 1 area 0
interface GigabitEthernet0/0/1
 ip address 192.168.1.2 255.255.255.0
 negotiation auto
 ipv6 address FD01::2/64
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
 router-id 3.3.3.3
 redistribute connected subnets
 redistribute bgp 3333 subnets
 network 192.168.2.0 0.0.0.255 area 0
router bgp 3333
 bgp router-id 3.3.3.3
 bgp log-neighbor-changes
 neighbor 192.168.1.1 remote-as 2222
 neighbor FD01::1 remote-as 2222
 neighbor FD01::1 update-source GigabitEthernet0/0/1
 address-family ipv4
  network 192.168.1.0
  network 192.168.2.0
```

```
  redistribute connected
  redistribute ospf 1 match external 1 external 2
  neighbor 192.168.1.1 activate
  no neighbor FD01::1 activate
 exit-address-family
 address-family ipv6
  redistribute connected
  redistribute ospf 1 match external 1 external 2
  neighbor FD01::1 activate
 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
 router-id 3.3.3.3
 redistribute connected
 redistribute bgp 3333
control-plane
line con 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 login
end
```

Router B2

```
version 16.9
service timestamps debug datetime msec
service timestamps log datetime msec
platform qfp utilization monitor load 80
platform punt-keepalive disable-kernel-core
hostname B2
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
login on-success log
subscriber templating
ipv6 unicast-routing
multilink bundle-name authenticated
license udi pid ISR4321/K9 sn FDO214811ZM
no license smart enable
diagnostic bootup level minimal
```

```
spanning-tree extend system-id
redundancy
 mode none
interface Loopback0
 ip address 4.4.4.4 255.255.255.255
interface GigabitEthernet0/0/0
 ip address 192.168.2.2 255.255.255.0
 ip ospf 1 area 0
 negotiation auto
 ipv6 address FD02::2/64
 ipv6 ospf 1 area 0
interface GigabitEthernet0/0/1
 ip address 192.168.3.1 255.255.255.252
 negotiation auto
 ipv6 address FD03::1/64
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
router ospf 1
 router-id 4.4.4.4
 redistribute connected subnets
 redistribute bgp 3333 subnets
 network 192.168.2.0 0.0.0.255 area 0
router bgp 3333
 bgp router-id 4.4.4.4
 bgp log-neighbor-changes
 neighbor fd03::2/64 peer-group
 neighbor fd03::2/64 remote-as 3
 neighbor 192.168.3.2 remote-as 3
 neighbor FD03::2 remote-as 3
 address-family ipv4
  network 192.168.2.0
  network 192.168.3.0
  redistribute connected
  redistribute ospf 1 match external 1 external 2
  neighbor 192.168.3.2 activate
```

```
  no neighbor FD03::2 activate
 exit-address-family
 address-family ipv6
  redistribute connected
  redistribute ospf 1 match external 1 external 2
  network FD02::/64
  network FD03::/64
  neighbor FD03::2 activate
 exit-address-family
ip forward-protocol nd
ip http server
ip http authentication local
ip http secure-server
ip tftp source-interface GigabitEthernet0
ipv6 router ospf 1
 router-id 4.4.4.4
 redistribute connected
 redistribute bgp 3333
control-plane
line con 0
 transport input none
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 login
end
```

Router C2

```
version 16.9
service timestamps debug datetime msec
service timestamps log datetime msec
platform qfp utilization monitor load 80
no platform punt-keepalive disable-kernel-core
hostname C2
boot-start-marker
boot system flash bootflash:isr4300-universalk9.16.09.08.SPA.bin
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 pool webuidhcp
login on-success log
subscriber templating
ipv6 unicast-routing
multilink bundle-name authenticated
license udi pid ISR4321/K9 sn FLM240607T3
no license smart enable
```

```
diagnostic bootup level minimal
spanning-tree extend system-id
redundancy
 mode none
interface Loopback0
 ip address 5.5.5.5 255.255.255.255
interface GigabitEthernet0/0/0
 ip address 192.168.4.1 255.255.255.252
 negotiation auto
 ipv6 address FD04::1/64
 ipv6 enable
 ipv6 eigrp 3
interface GigabitEthernet0/0/1
 ip address 192.168.3.2 255.255.255.252
 negotiation auto
 ipv6 address FD03::2/64
 ipv6 enable
interface GigabitEthernet0
 vrf forwarding Mgmt-intf
 no ip address
 shutdown
 negotiation auto
router eigrp 3
 default-metric 10000 100 255 1 1500
 network 192.168.3.0
 network 192.168.4.0 0.0.0.3
 redistribute connected
 redistribute bgp 3
router bgp 3
 bgp log-neighbor-changes
 neighbor fd03::1/64 peer-group
 neighbor 192.168.3.1 remote-as 3333
 neighbor FD03::1 remote-as 3333
 address-family ipv4
  redistribute connected
  redistribute eigrp 3
  neighbor 192.168.3.1 activate
  no neighbor FD03::1 activate
 exit-address-family
 address-family ipv6
  redistribute connected
  redistribute eigrp 3
  network FD03::/64
  neighbor FD03::1 activate
 exit-address-family
ip forward-protocol nd
ip http server
ip http authentication local
ip http secure-server
ip tftp source-interface GigabitEthernet0
ipv6 router eigrp 3
 eigrp router-id 5.5.5.5
```

```
 redistribute bgp 3
 redistribute connected
 default-metric 10000 100 255 1 1500=
control-plane
line con 0
 transport input none
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 login
end
```

Router C1

```
version 15.5
service timestamps debug datetime msec
service timestamps log datetime msec
no platform punt-keepalive disable-kernel-core
hostname C1
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 FDO214913GF
spanning-tree extend system-id
redundancy
 mode none
vlan internal allocation policy ascending
interface Loopback0
 ip address 6.6.6.6 255.255.255.255
interface GigabitEthernet0/0/0
 ip address 192.168.4.2 255.255.255.252
 negotiation auto
 ipv6 address FD04::2/64
 ipv6 eigrp 3
interface GigabitEthernet0/0/1
 ip address 192.168.6.1 255.255.255.252
 negotiation auto
 ipv6 address FD06::1/64
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 eigrp 3
 default-metric 10000 100 255 1 1500
 network 192.168.4.0 0.0.0.3
 network 192.168.6.0
 redistribute connected
ip forward-protocol nd
no ip http server
no ip http secure-server
ip tftp source-interface GigabitEthernet0
ipv6 router eigrp 3
 eigrp router-id 6.6.6.6
 redistribute connected
 default-metric 10000 100 255 1 1500
control-plane
line con 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 login
end
```

Problems

In configuring IS-IS, we had set both routers to Level 1 routing. However, this meant that we had to configure BGP to distribute those Level 1 routes, instead of normal IS-IS routes. Without doing so, BGP would be able to distribute routes to the other autonomous systems.

In configurating EIGRP, we did not set a default metric. When redistributing routes, EIGRP requires a metric to send with the route, unless the route is a directly connected one. This resulted in EIGRP not sending BGP routes to its autonomous system.

Conclusion

In this lab, we successfully configured a network with 3 Autonomous Systems (AS), each running a different interior routing protocol (OSPF, EIGRP, and IS-IS). Between each AS, we configured BGP to distribute routes to each AS.

IBGP

Purpose

The purpose of this lab is to learn how to set up interior Border Gateway Protocol (IBGP).

Background Information

Autonomous Systems

The internet can be segregated into routing domains named autonomous systems (ASs), which can have their own routing information and policies. BGP, or Border Gateway Protocol, assumes that routing within an autonomous system is already complete through an Interior Gateway Protocol, such as OSPF or EIGRP.

BGP

BGP functions by assuming the network is a graph of distinct autonomous systems and provides routing information to ensure loop-free interdomain routing.

BGP is a path vector protocol, meaning that BGP routing information carries a series of AS numbers that identifies the path that information takes. This information is used to prevent loops for occurring.

Routers that run BGP are called BGP speakers. When two speakers form a connection, they are referred to as peers. When this connection forms, all BGP routes are exchanged. After this initial route exchange, updates are only sent incrementally as other network information changes.

BGP speakers establishes connections using an OPEN message, which states the version, autonomous system, hold timer, BGP identifier, and other optional parameters of the BGP speaker. Once a connection is formed, each speaker needs to send KEEPALIVE messages to ensure the connection is kept. Any updates, such as new or withdrawn routes, are sent using the UPDATE message.

Interior Gateway Protocols

An Interior Gateway Protocol manages the routing information within an AS, as opposed to BGP managing the routing information between autonomous systems. The Interior Gateway Protocols used in this lab are OSPF and EIGRP.

Interior BGP

Interior BGP, or IBGP, differs from external BGP, both of which allow BGP to function. While the purpose of external BGP is to distribute routes between different ASs, IBGP shares routing information between routers in the same AS.

Other interior gateway protocols can also share routing information in an AS. The advantage of IBGP is that IBGP will is designed to share external routes learned from external BGP, while protocols like OSPF will not do this by default. Additionally, with particularly large routing tables, such as those used on the internet, protocols such as OSPF will struggle to converge in a reasonable amount of time, while this is the most common use case of BGP. BGP also allows much greater flexibility with traffic engineering than other routing protocols, with options for AS path, Local Preference, Multi-Exit Discriminator, and Next Hop Routers.

IBGP is often set up on routers that are not directly connected to each other. For this to be possible, an interior routing gateway protocol is still required within an AS so that neighbors can reach each other. In this lab, OSPF is used within Company B so that Routers B1 and B3 can be configured as interior BGP neighbors.

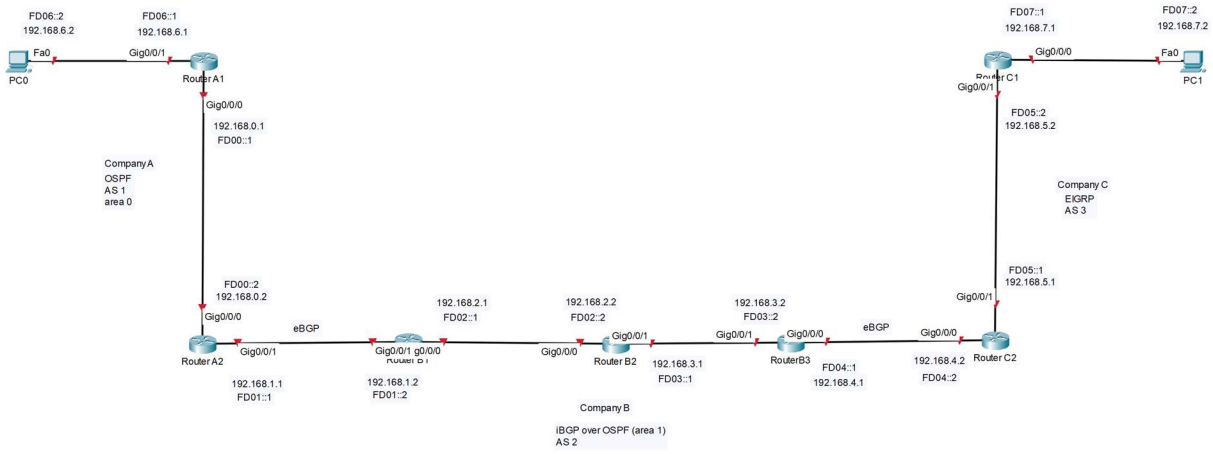
Lab Summary

Three Autonomous Systems (ASs), represented by Company A, Company B, and Company C need to be connected to one another. Each AS needs to have an interior gateway protocol to distribute routes to each router within the AS. Company A and Company B both use OSPF, while Company C uses EIGRP. Between each AS, BGP is configured to allow routing information to be distributed to each AS. For Company B, interior BGP is configured between Routers B1 and B3.

Lab Commands

```
distance bgp 20 105 1   changes the metric of iBGP to 105
```

Network Diagram



Configurations

Router A1

```
version 15.5
service timestamps debug datetime msec
service timestamps log datetime msec
no platform punt-keepalive disable-kernel-core
hostname A1
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 FDO21281AAT
spanning-tree extend system-id
redundancy
 mode none
vlan internal allocation policy ascending
interface GigabitEthernet0/0/0
 ip address 192.168.0.1 255.255.255.0
 ip ospf 1 area 0
 negotiation auto
 ipv6 address FD00::1/64
 ipv6 enable
 ipv6 ospf 1 area 0
interface GigabitEthernet0/0/1
 ip address 192.168.6.1 255.255.255.0
 ip ospf 1 area 0
 negotiation auto
 ipv6 address FD06::1/64
 ipv6 enable
 ipv6 ospf 1 area 0
interface GigabitEthernet0/1/0
 no ip address
 shutdown
 negotiation auto
interface GigabitEthernet0/1/1
 no ip address
 shutdown
 negotiation auto
interface Service-Engine0/2/0
 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
 router-id 1.1.1.1
 redistribute connected subnets
 network 192.168.0.0 0.0.0.255 area 0
ip forward-protocol nd
no ip http server
no ip http secure-server
ip tftp source-interface GigabitEthernet0
ipv6 router ospf 1
 router-id 1.1.1.1
 redistribute connected
control-plane
line con 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 login
end
```

Router A2

```
version 15.5
service timestamps debug datetime msec
service timestamps log datetime msec
no platform punt-keepalive disable-kernel-core
hostname A2
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 FDO21491LXF
spanning-tree extend system-id
redundancy
```

```
 mode none
vlan internal allocation policy ascending
interface GigabitEthernet0/0/0
 ip address 192.168.0.2 255.255.255.0
 ip ospf 1 area 0
 negotiation auto
 ipv6 address FD00::2/64
 ipv6 ospf 1 area 0
interface GigabitEthernet0/0/1
 ip address 192.168.1.1 255.255.255.0
 negotiation auto
 ipv6 address FD01::1/64
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
 router-id 2.2.2.2
 redistribute connected subnets
 redistribute bgp 1 subnets
 network 192.168.0.0 0.0.0.255 area 0
router bgp 1
 bgp log-neighbor-changes
 neighbor 192.168.1.2 remote-as 2
 neighbor FD01::2 remote-as 2
 address-family ipv4
  redistribute connected
  redistribute ospf 1
  neighbor 192.168.1.2 activate
  no neighbor FD01::2 activate
 exit-address-family
 address-family ipv6
  redistribute connected
  redistribute ospf 1
  network FD01::/64
  neighbor FD01::2 activate
 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
```

```
 router-id 2.2.2.2
 redistribute connected
 redistribute bgp 1
control-plane
line con 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 login
end
```

Router B1

```
version 15.5
service timestamps debug datetime msec
service timestamps log datetime msec
no platform punt-keepalive disable-kernel-core
hostname B1
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 FLM240607Q1
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
 shutdown
 negotiation auto
 ipv6 address FD02::1/64
 ipv6 ospf 1 area 1
interface GigabitEthernet0/0/1
 ip address 192.168.1.2 255.255.255.0
 shutdown
 negotiation auto
 ipv6 address FD01::2/64
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
 router-id 3.3.3.3
 redistribute connected subnets
 redistribute bgp 2 subnets
 network 192.168.2.0 0.0.0.255 area 1
router bgp 2
 bgp router-id 3.3.3.3
 bgp log-neighbor-changes
 neighbor 192.168.1.1 remote-as 1
 neighbor 192.168.3.2 remote-as 2
 neighbor FD01::1 remote-as 1
 neighbor FD03::2 remote-as 2
 address-family ipv4
  redistribute ospf 1 match internal external 1 external 2
  neighbor 192.168.1.1 activate
  neighbor 192.168.3.2 activate
  no neighbor FD01::1 activate
  no neighbor FD03::2 activate
  distance 105 192.168.3.2 0.0.0.0
 exit-address-family
 address-family ipv6
  redistribute connected
  redistribute ospf 1 match internal external 1 external 2
  neighbor FD01::1 activate
  neighbor FD03::2 activate
  distance bgp 20 105 1
 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
 router-id 3.3.3.3
 redistribute connected
 redistribute bgp 2
control-plane
line con 0
 stopbits 1
line aux 0
 stopbits 1
```

```
line vty 0 4
 login
end
```

Router B2

```
version 16.9
service timestamps debug datetime msec
service timestamps log datetime msec
platform qfp utilization monitor load 80
platform punt-keepalive disable-kernel-core
hostname B2
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
login on-success log
subscriber templating
vtp domain cisco
vtp mode transparent
ipv6 unicast-routing
multilink bundle-name authenticated
license udi pid ISR4321/K9 sn FLM240800D6
no license smart enable
diagnostic bootup level minimal
spanning-tree extend system-id
redundancy
 mode none
interface GigabitEthernet0/0/0
 ip address 192.168.2.2 255.255.255.0
 ip ospf 1 area 1
 shutdown
 negotiation auto
 ipv6 address FD02::2/64
 ipv6 ospf 1 area 1
interface GigabitEthernet0/0/1
 ip address 192.168.3.1 255.255.255.0
 ip ospf 1 area 1
 shutdown
 negotiation auto
 ipv6 address FD03::1/64
 ipv6 ospf 1 area 1
interface Serial0/1/0
interface Serial0/1/1
interface GigabitEthernet0
 vrf forwarding Mgmt-intf
 no ip address
 shutdown
```

```
 negotiation auto
router ospf 1
 router-id 4.4.4.4
 network 192.168.2.0 0.0.0.255 area 1
 network 192.168.3.0 0.0.0.255 area 1
ip forward-protocol nd
ip http server
ip http authentication local
ip http secure-server
ip tftp source-interface GigabitEthernet0
ipv6 router ospf 1
 router-id 4.4.4.4
control-plane
line con 0
 transport input none
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 login
end
```

Router B3

```
version 16.9
service timestamps debug datetime msec
service timestamps log datetime msec
platform qfp utilization monitor load 80
platform punt-keepalive disable-kernel-core
hostname B3
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
login on-success log
subscriber templating
vtp domain cisco
vtp mode transparent
ipv6 unicast-routing
multilink bundle-name authenticated
license udi pid ISR4321/K9 sn FLM2407011F
no license smart enable
diagnostic bootup level minimal
spanning-tree extend system-id
redundancy
 mode none
interface GigabitEthernet0/0/0
```

```
 ip address 192.168.4.1 255.255.255.252
 shutdown
 negotiation auto
 ipv6 address FD04::1/64
interface GigabitEthernet0/0/1
 ip address 192.168.3.2 255.255.255.252
 shutdown
 negotiation auto
 ipv6 address FD03::2/64
interface GigabitEthernet0/1/0
 no ip address
 shutdown
 negotiation auto
interface GigabitEthernet0/1/1
 no ip address
 shutdown
 negotiation aut
interface GigabitEthernet0
 vrf forwarding Mgmt-intf
 no ip address
 shutdown
 negotiation aut
router bgp 2
 bgp log-neighbor-changes
 redistribute connected
 neighbor 192.168.4.2 remote-as
ip forward-protocol nd
ip http server
ip http authentication local
ip http secure-server
ip tftp source-interface GigabitEthernet0
control-plane
line con 0
 transport input none
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 login
end
```

Router C2

```
version 16.9
service timestamps debug datetime msec
service timestamps log datetime msec
platform qfp utilization monitor load 80
platform punt-keepalive disable-kernel-core
hostname C2
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
login on-success log
subscriber templating
vtp domain cisco
vtp mode transparent
ipv6 unicast-routing
multilink bundle-name authenticated
license udi pid ISR4321/K9 sn FDO214420HW
license boot level appxk9
no license smart enable
diagnostic bootup level minimal
spanning-tree extend system-id
redundancy
 mode none
interface GigabitEthernet0/0/0
 ip address 192.168.4.2 255.255.255.0
 shutdown
 negotiation auto
 ipv6 address FD04::2/64
interface GigabitEthernet0/0/1
 ip address 192.168.5.1 255.255.255.0
 shutdown
 negotiation auto
 ipv6 address FD05::1/64
 ipv6 eigrp 3
interface Serial0/1/0
interface Serial0/1/1
interface GigabitEthernet0
 vrf forwarding Mgmt-intf
 no ip address
 shutdown
 negotiation auto
router eigrp 3
 default-metric 1000 100 250 100 1500
 network 192.168.5.0
 redistribute connected
 redistribute bgp 3
router bgp 3
 bgp router-id 6.6.6.6
 bgp log-neighbor-changes
 neighbor 192.168.4.1 remote-as 2
 neighbor FD04::1 remote-as 2
 address-family ipv4
  redistribute connected
  redistribute eigrp 3
  neighbor 192.168.4.1 activate
  no neighbor FD04::1 activate
 exit-address-family
```

```
 address-family ipv6
  redistribute connected
  redistribute eigrp 3
  neighbor FD04::1 activate
 exit-address-family
ip forward-protocol nd
ip http server
ip http authentication local
ip http secure-server
ip tftp source-interface GigabitEthernet0
ipv6 router eigrp 3
 eigrp router-id 6.6.6.6
 redistribute connected
 redistribute bgp 3
 default-metric 1000 100 250 100 1500
control-plane
line con 0
 transport input none
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 login
end
```

Router C1

```
version 16.9
service timestamps debug datetime msec
service timestamps log datetime msec
platform qfp utilization monitor load 80
platform punt-keepalive disable-kernel-core
hostname C1
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
login on-success log
subscriber templating
ipv6 unicast-routing
multilink bundle-name authenticated
license udi pid ISR4321/K9 sn FDO21442167
no license smart enable
diagnostic bootup level minimal
spanning-tree extend system-id
redundancy
 mode none
interface GigabitEthernet0/0/0
```

```
 ip address 192.168.7.1 255.255.255.0
 shutdown
 negotiation auto
 ipv6 address FD07::1/64
interface GigabitEthernet0/0/1
 ip address 192.168.5.2 255.255.255.0
 shutdown
 negotiation auto
 ipv6 address FD05::2/64
 ipv6 eigrp 3
interface Serial0/1/0
interface Serial0/1/1
interface GigabitEthernet0
 vrf forwarding Mgmt-intf
 no ip address
 shutdown
 negotiation auto
router eigrp 3
 default-metric 1000 100 250 100 1500
 network 192.168.5.0
 network 192.168.7.0
 redistribute connected
ip forward-protocol nd
ip http server
ip http authentication local
ip http secure-server
ip tftp source-interface GigabitEthernet0
ipv6 router eigrp 3
 eigrp router-id 7.7.7.7
 redistribute connected
 default-metric 1000 100 250 100 1500
control-plane
line con 0
 transport input none
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 login
end
```

Problems

No problems were encountered, but it took quite a bit of time to input all commands necessary to complete the lab.

Conclusion

In this lab, we successfully configured a network containing three Autonomous Systems, each running an interior routing protocol, with EBGP connecting each Autonomous System. In the middle autonomous system, iBGP was configuring to run over OSPF in order to distribute routes.

AWS Labs 1-3

Purpose

The purpose of these labs is to introduce Amazon Web Services and how they can be used to launch a Web server, along with related security, storage, and networking elements.

Background Information

Amazon Web Services (AWS) is a secure cloud platform offering a set of global cloud-based products. As a cloud computing platform, it offers on-demand access to compute, storage, networking, database, and IT management tools. In addition, customers only need to pay for the specific resources that they use, for as long as they use them, instead of needed to buy hardware for a fixed cost.

AWS operates, manages, and controls the components from the software virtualization layer to the physical security of the facilities of AWS services. AWS is responsible for the protection of all service infrastructure. Meanwhile, the customer is responsible of the encryption of data and ensuring that security credentials/logins and managed safety. The customer is also responsible for configuring security groups.

One tool that AWS offers is AWS Identity Access Management (IAM). AWS IAM allows customers to control access to various applications in the AWS Cloud. IAM is used to handle authentication and enforce authorization policies allowing users to access certain services. IAM provides granular controls over access to AWS resources, including what API calls users are allowed to make.

Within IAM, there are four components. IAM users are the people/applications defined within an AWS account, who make API calls to AWS products. Each user is defined by a unique username and a set of security credentials. IAM groups are collections of IAM users, and can be used to simplify the management of permissions for multiple users. IAM policies are documents that define what users can and cannot do within their AWS account. IAM roles are tools for temporarily granting access to specific AWS resources.

A second tool that AWS offers is AWS Virtual Private Cloud (VPC). AWS VPC provides a logically isolated section of the AWS Cloud where AWS resources can be launches. VPC provides the customer control over virtual networking resources, such is IP addresses, subnets, route tables, and network gateways. In addition, the network configuration can be customized, which both public and private subnets.

Internet gateways are scalable, redundant, and highly available VPC components that allow communication between instances in a VPC and the internet. Internet gateways provide a target in VPC route tables for internet traffic and perform NAT for instances with public IPv4 addresses.

AWS offers many compute services. Of these, Amazon Elastic Computer Cloud (EC2) provides virtual machines as Infrastructure as a Service (IaaS). EC2 provides flexibility in server management. The customer is able to choose the operating system, size, and resource capabilities of the launched servers. An operating system, such as Windows, Red Hat, Ubuntu, and Amazon Linux, is installed on the host operating system that hosts one or more virtual machines.

Amazon Machine Images (AMI) provide information that is required to launch an EC2 instance. A source AMI must be specified when launching, and includes a template for the root volume of the instance, launch permissions, and a block device mapping for the instance.

Lab Summary

In the first lab, you will first inspect pre-configured IAM policies and add users to groups using said policies. Then, you will experiment with the effects of these policies on accessing different services.

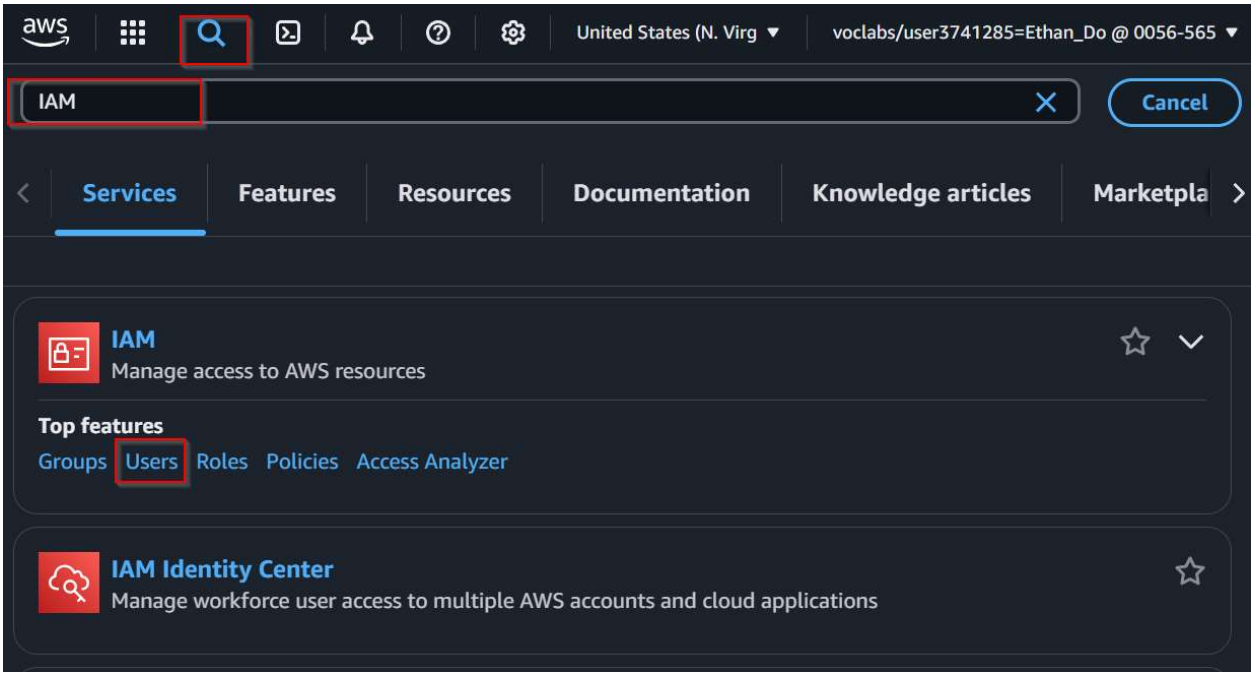
In the second lab, you will create an AWS VPC, configure subnets, and a security group, and then launch an EC2 instance using the VPC.

In the third lab, you will launch a web server through EC2, monitor the EC2 instance, modify a security group, resize the EC2 instance to scale it, and test stop protection.

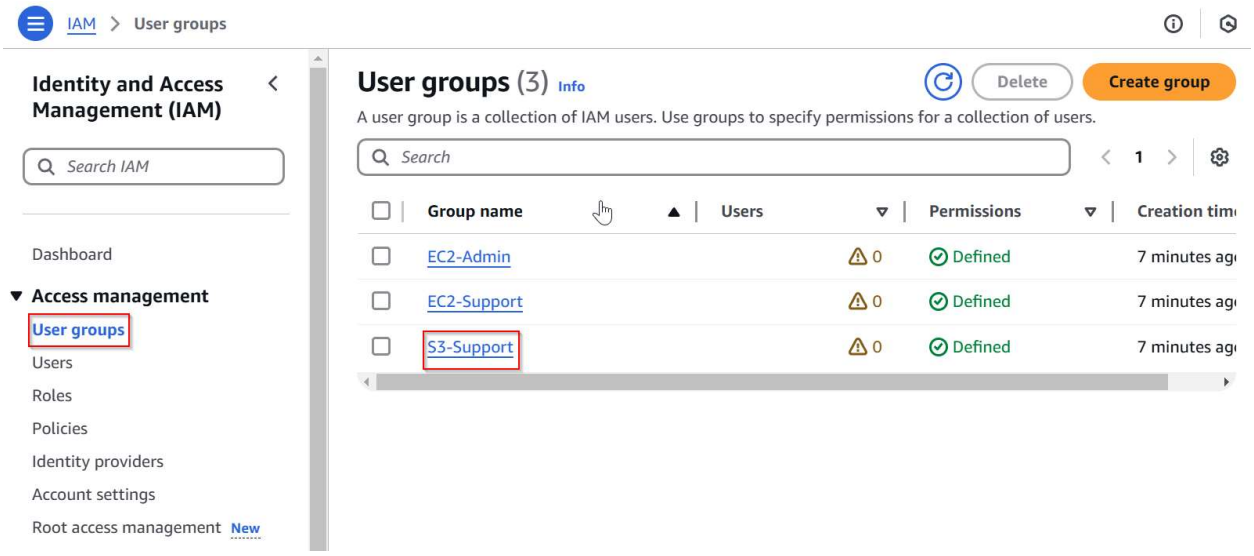
Lab Commands

Lab 1

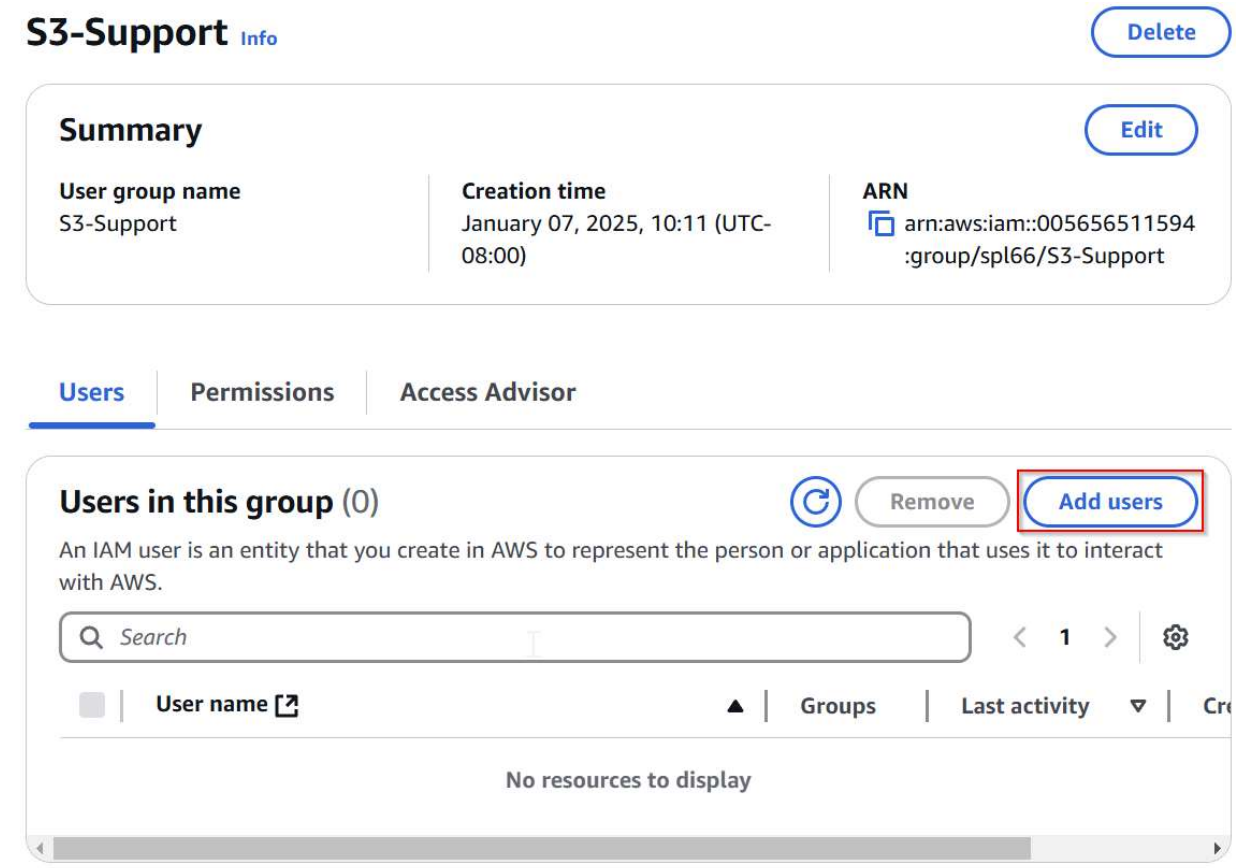
1. Search for IAM and open the Users tab.

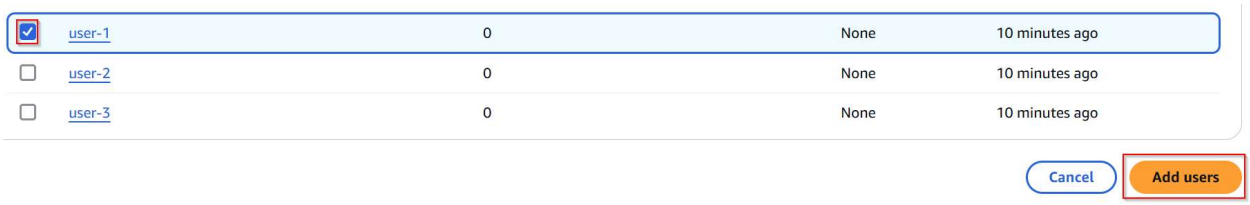


2. Choose the User groups tab and open the S3-Support group.

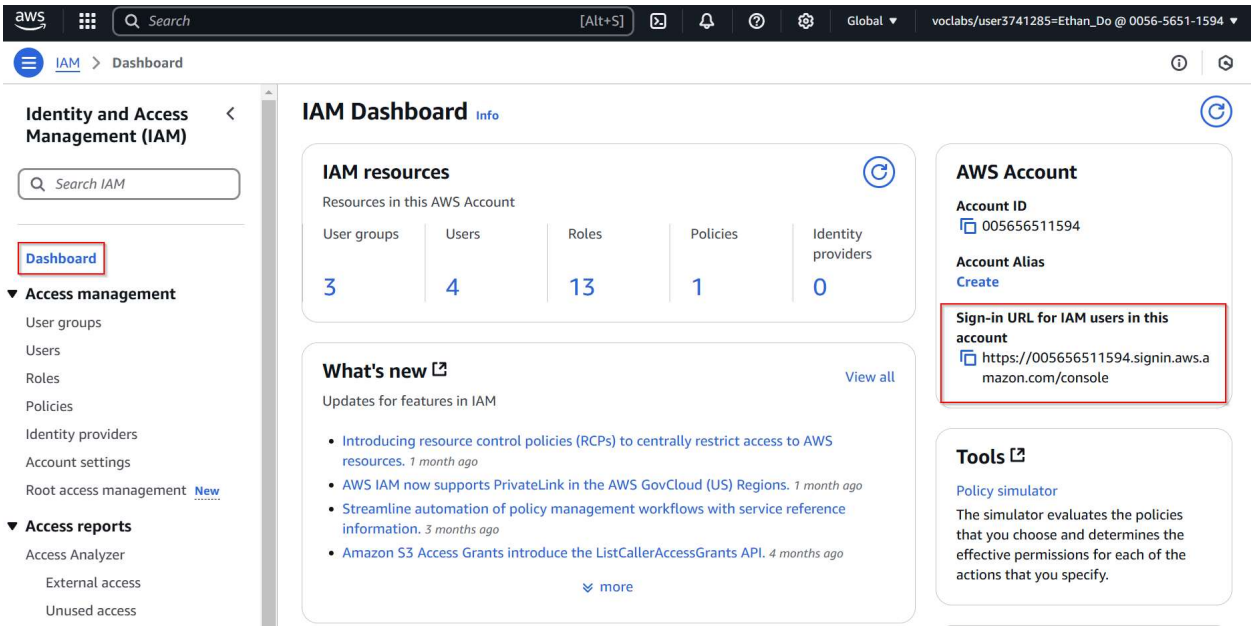


3. Click Add Users and add user-1 to the group. Similarly, add user-2 into the EC2-Support group and add user-3 to the EC2-Admin group.

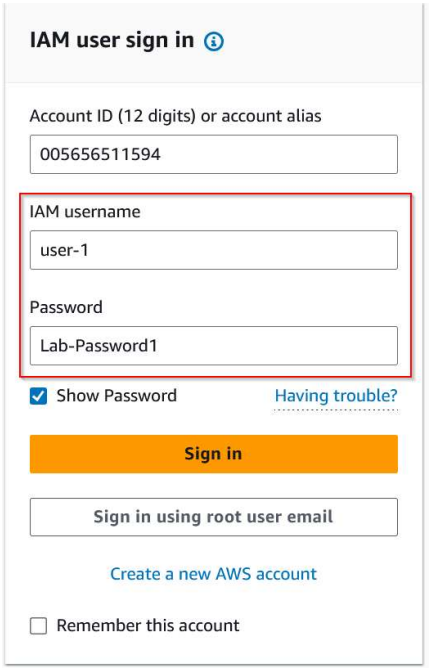




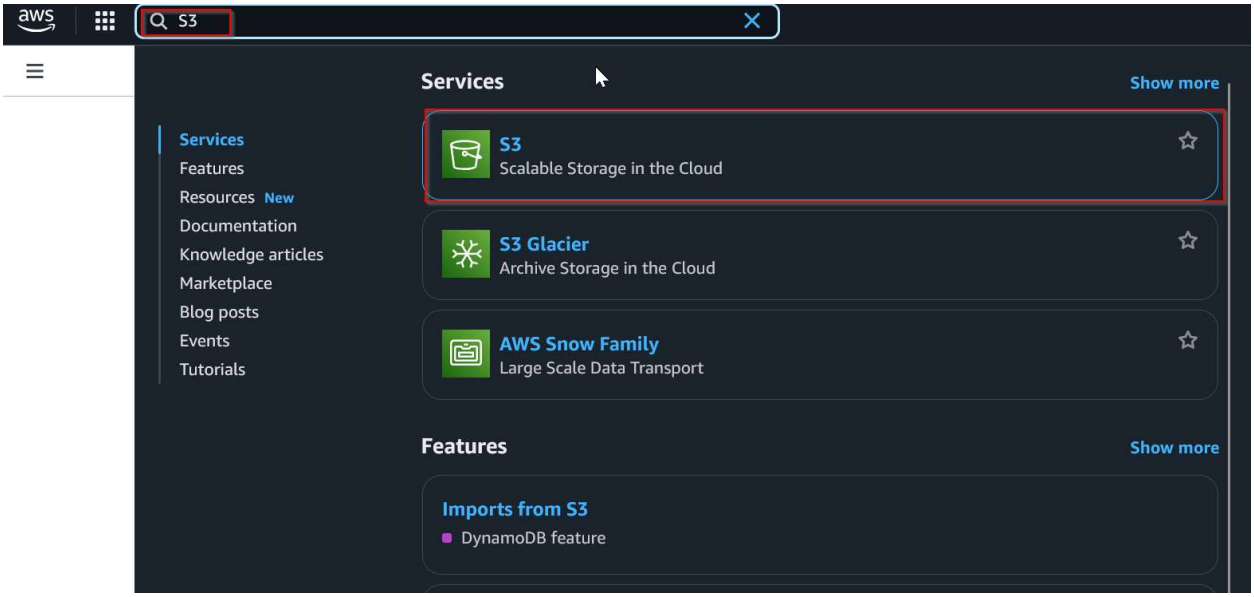
4. Open the dashboard and copy the sign-in URL for IAM users. Open a private (Incognito) window and access the URL.

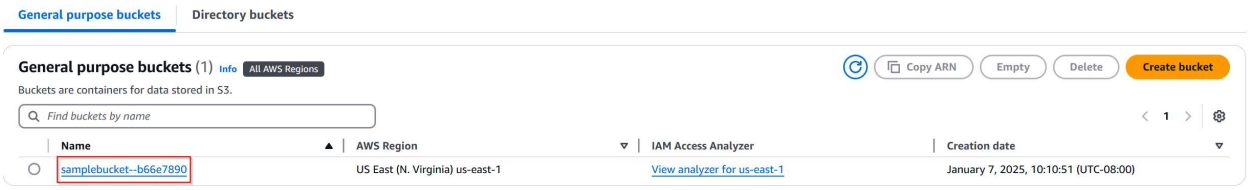


5. User user-1 for the username and Lab-Password1 for the password. The account ID will be filled in automatically.

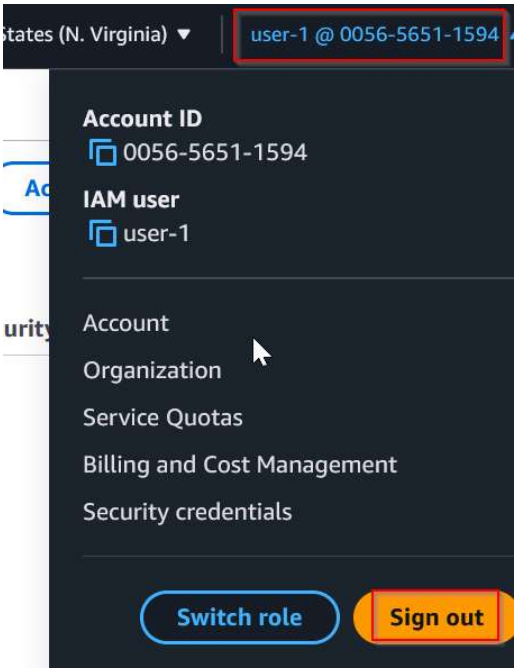


6. User the search bar to access S3. Open the bucket that appears in the account. Since user-1 is part of the S3-Support group, it is able to access S3 buckets. However, if you search up EC2 and try to view Instances, you are unable to, due to not having the permissions required.

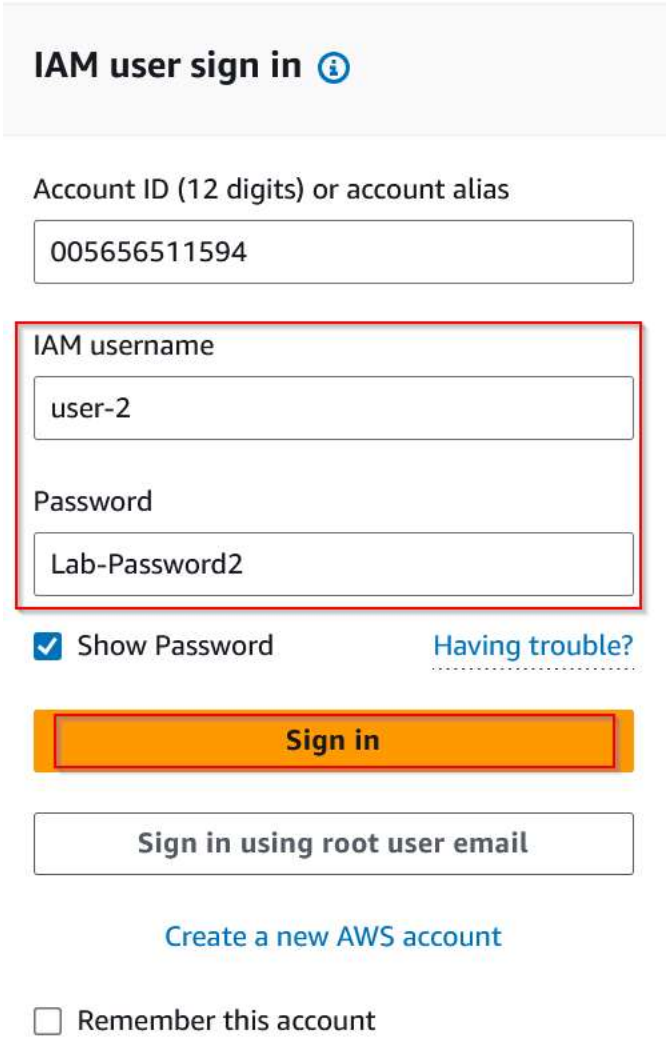




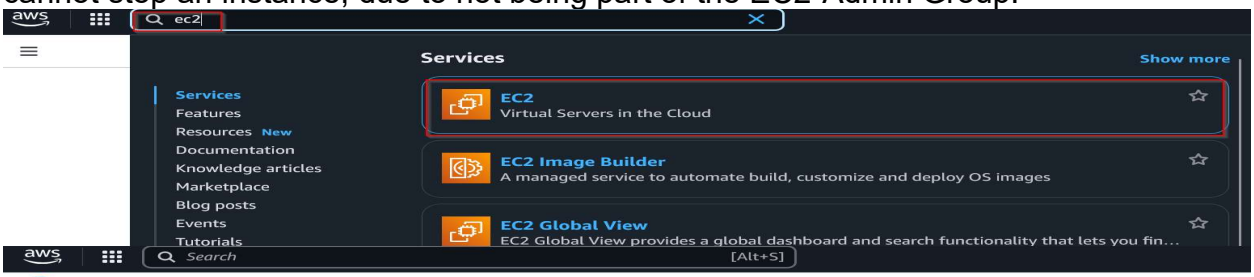
7. Now sign out.

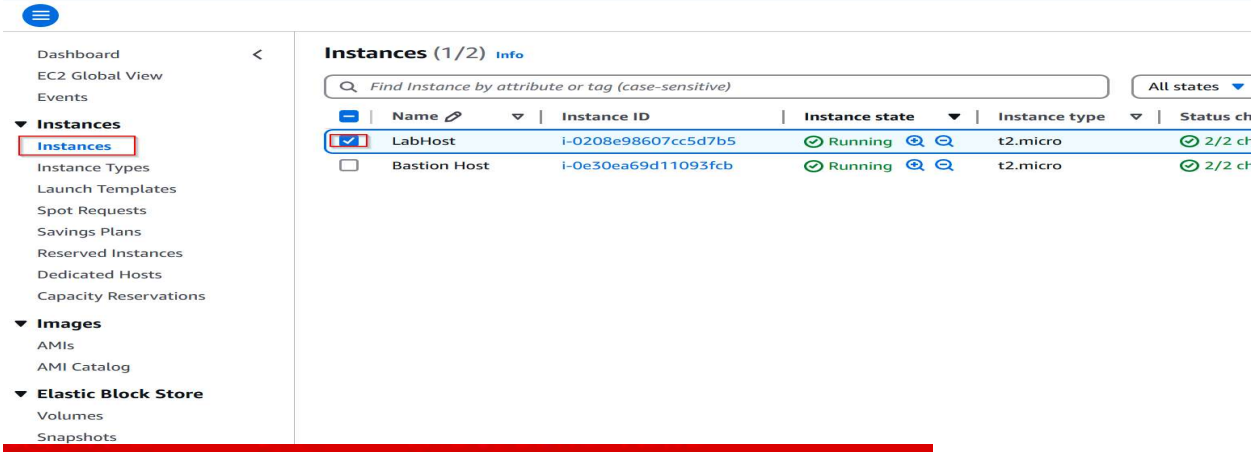


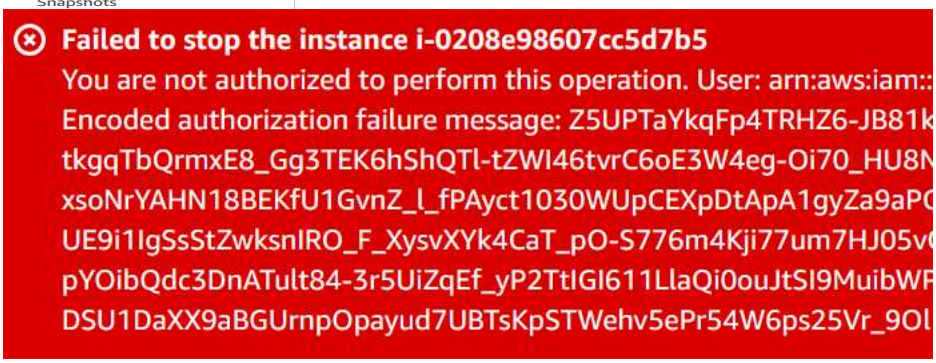
8. Sign in with user-2’s credentials by using the same link as before.



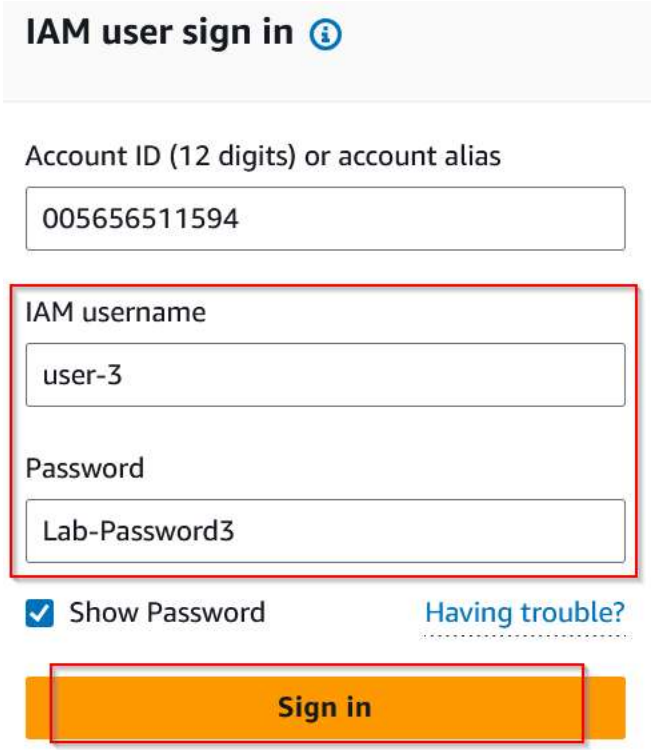
9. Search EC2 in using the search bar and choose Instances. Note that now, you are able to view instance, since user-2 is part of the EC2-Support Group. However, user-2 cannot stop an instance, due to not being part of the EC2-Admin Group.



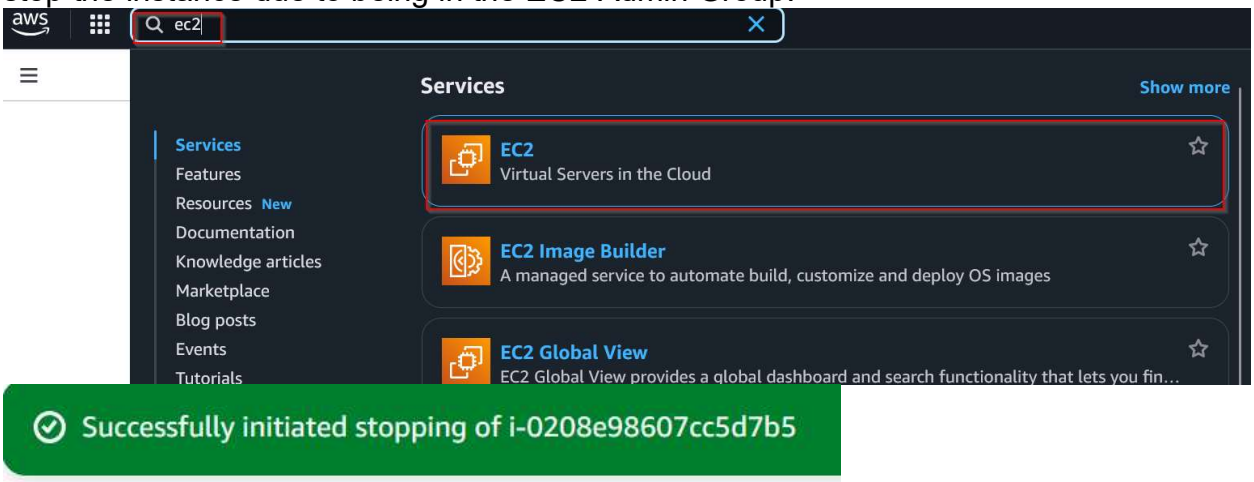




10. Using the same link, access user-3.

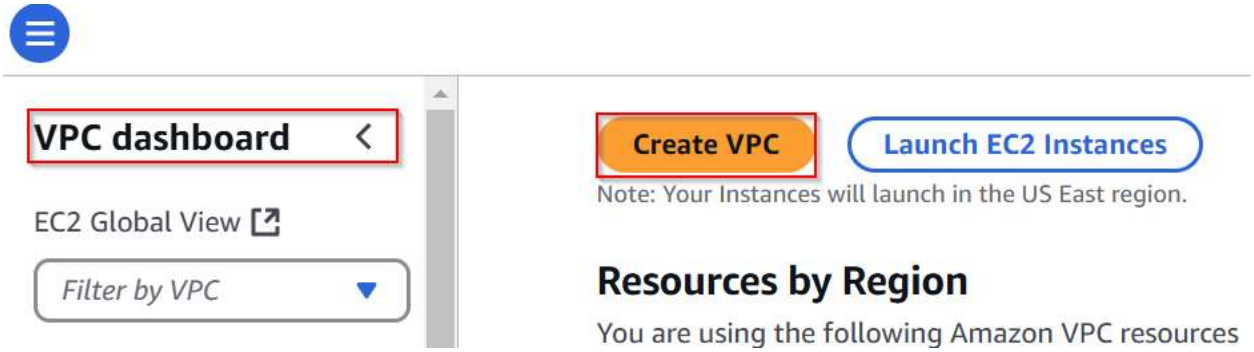


11. Access EC2 Instances and stop the instance, as before. This time, user-3 is able to stop the instance due to being in the EC2-Admin Group.



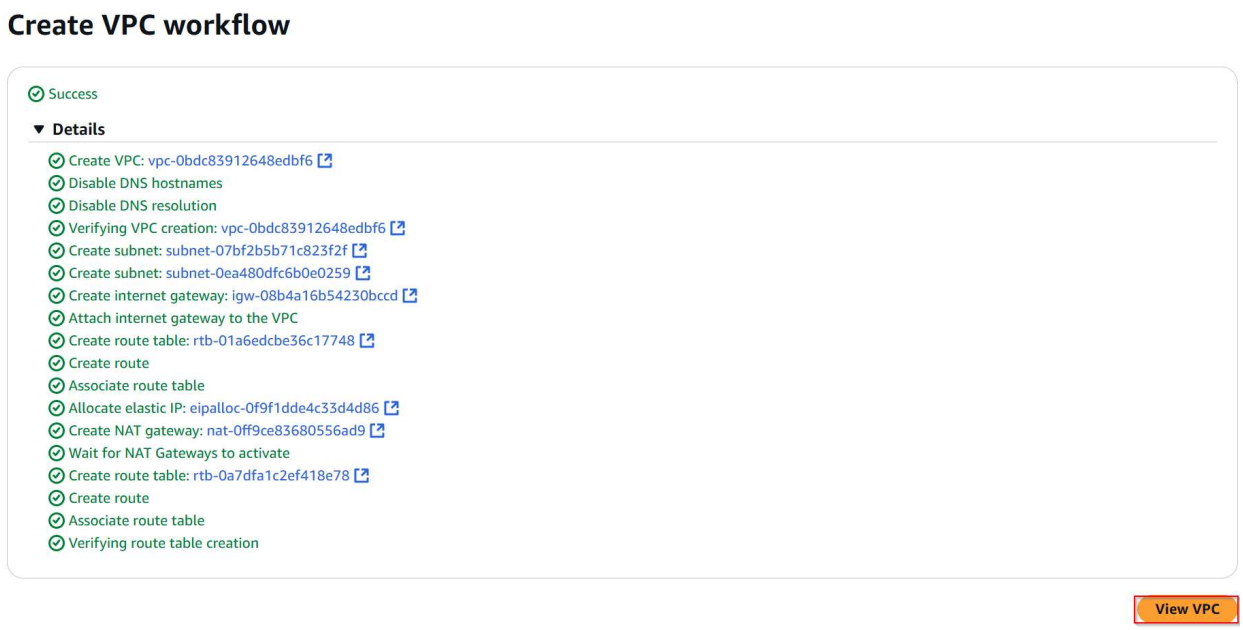
Lab 2

1. Open VPC and create a VPC in the VPC dashboard.

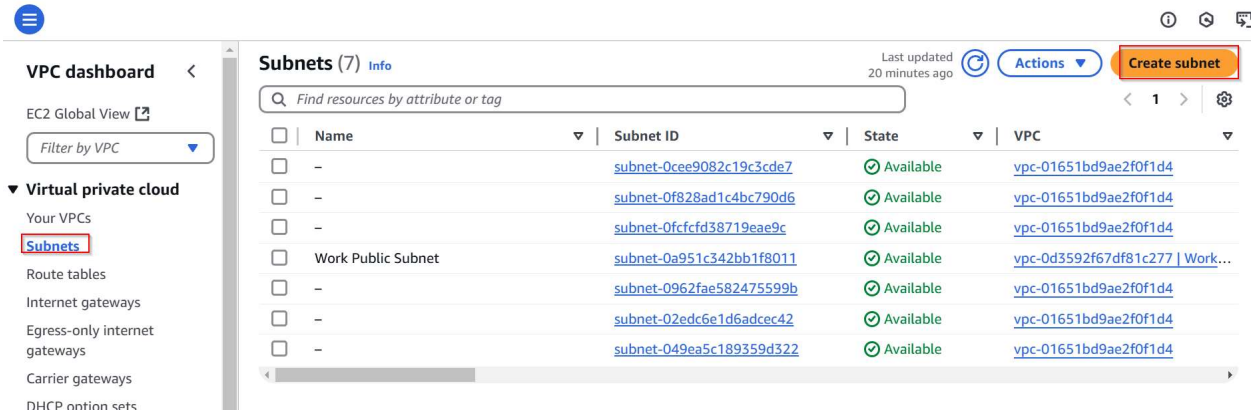


2. Configure the VPC as shown

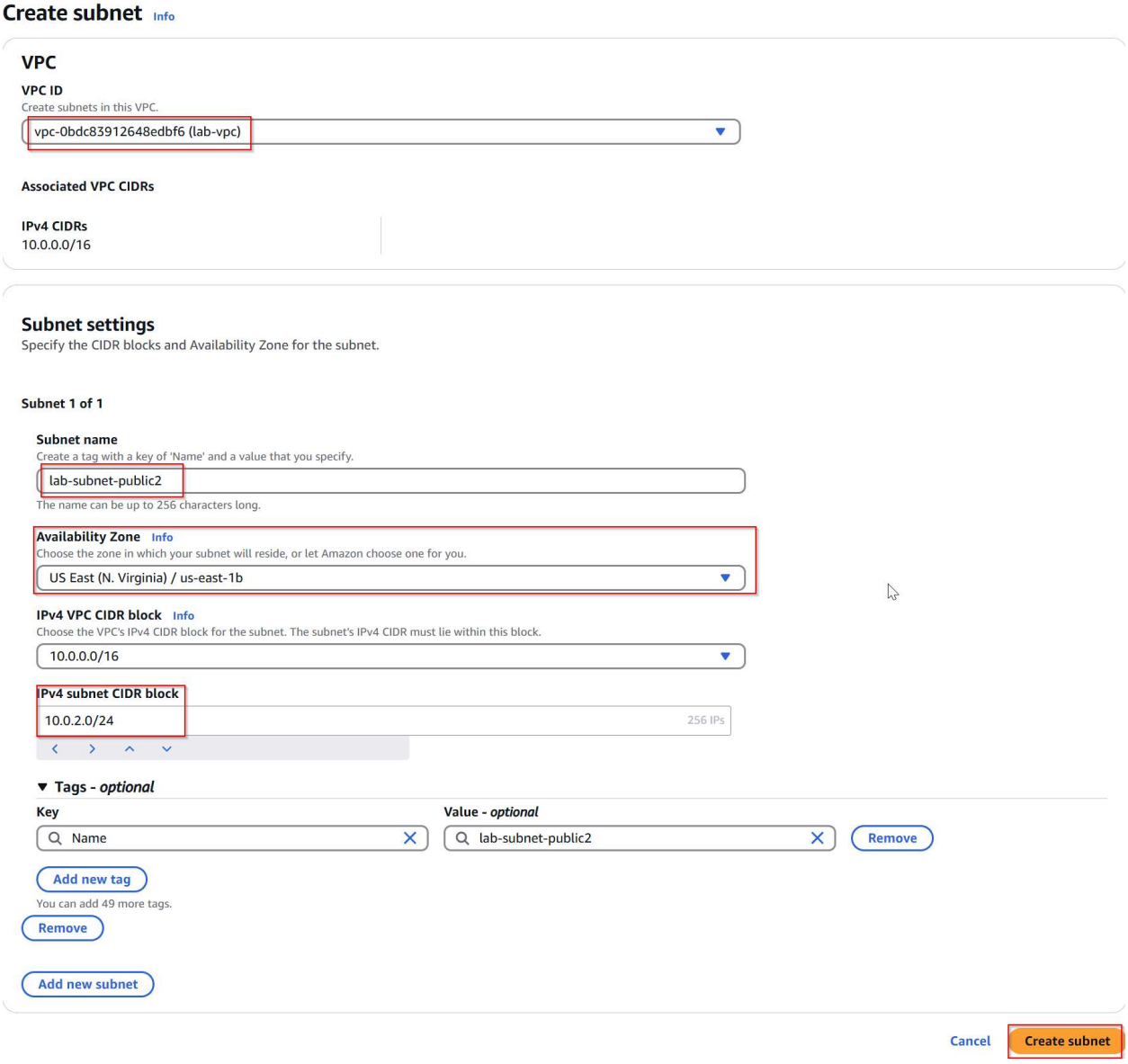
3. Click “Create VPC” and wait for all resources to be created. Click “View VPC”.



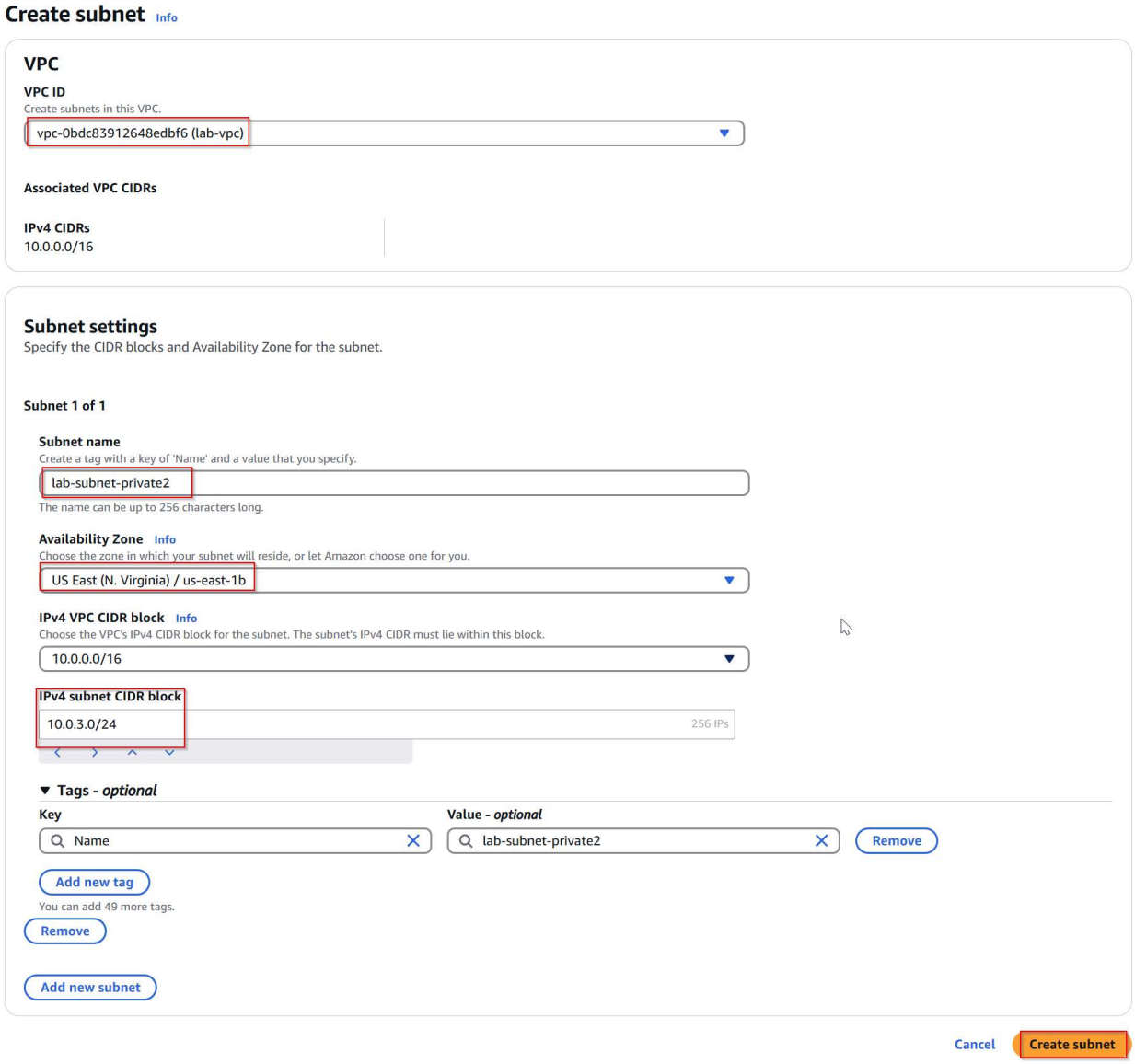
4. Click “Subnets” and “Create subnet”.



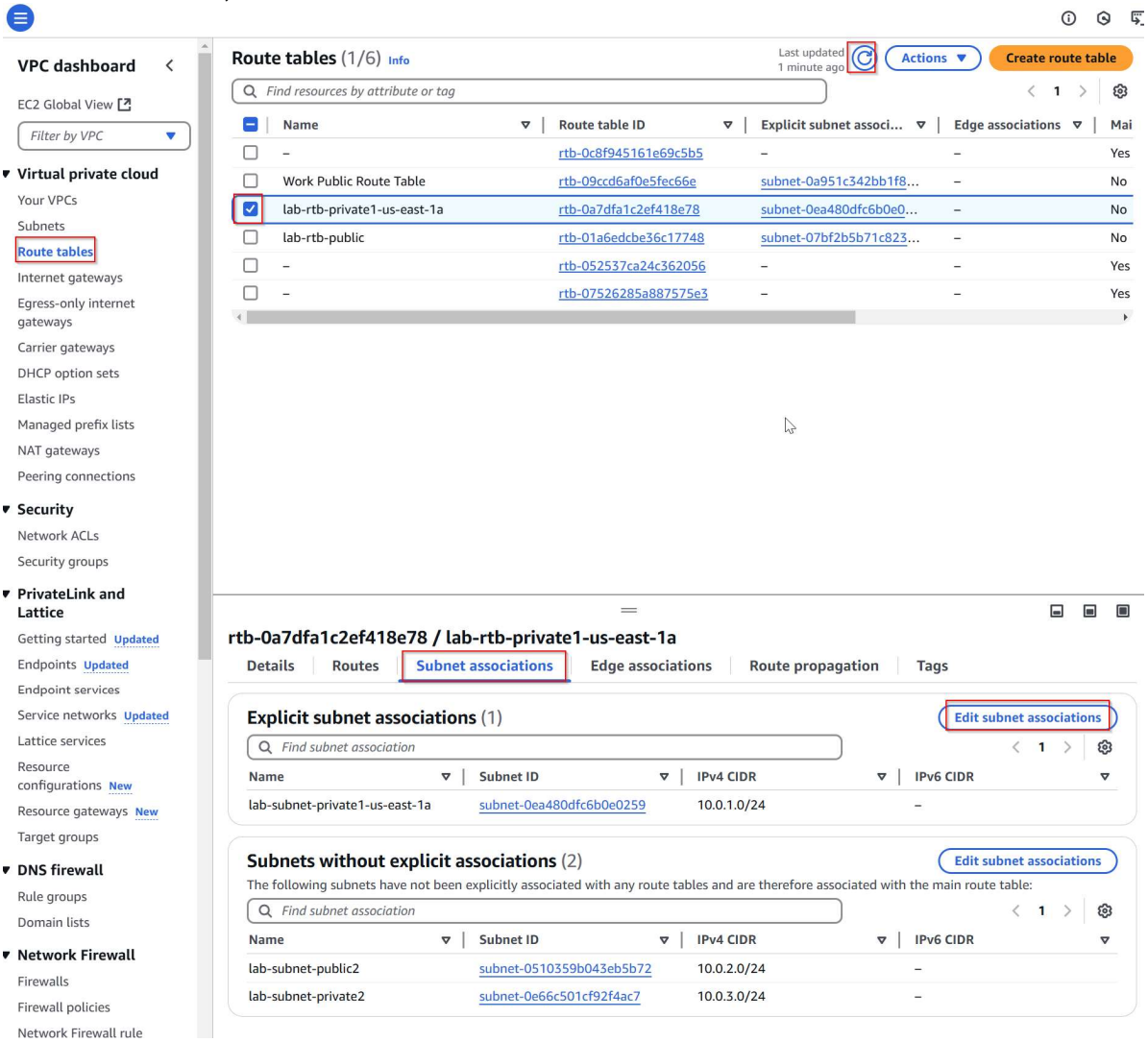
5. Configure the subnet to use lab-vpc, give it a name of lab-subnet-public2, an availability zone of us-east-1b, and an IPv4 subnet CIDR block of 10.0.2.0/24.



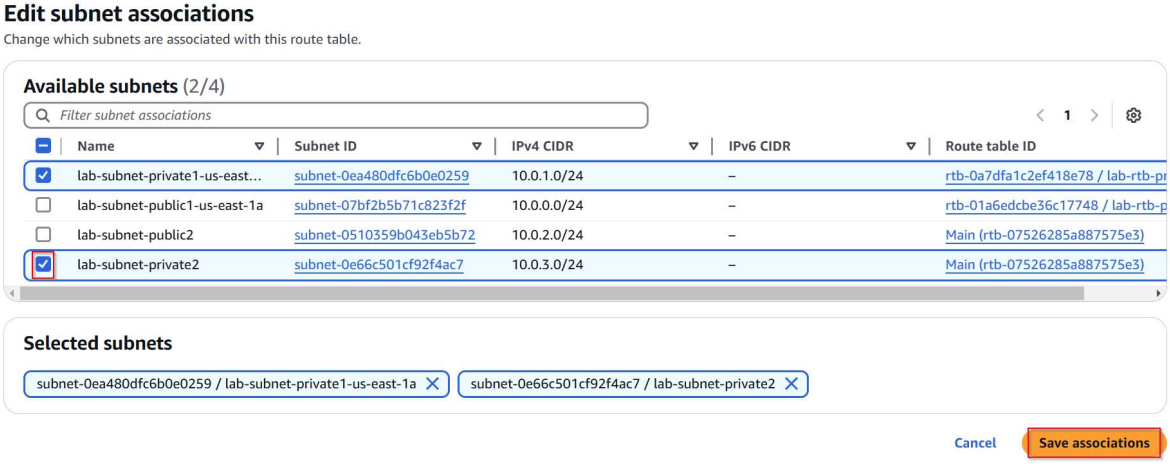
6. Configure another subnet to use lab-vpc, give it a name of lab-subnet-private2, an availability zone of us-east-1b, and an IPv4 subnet CIDR block of 10.0.3.0/24.



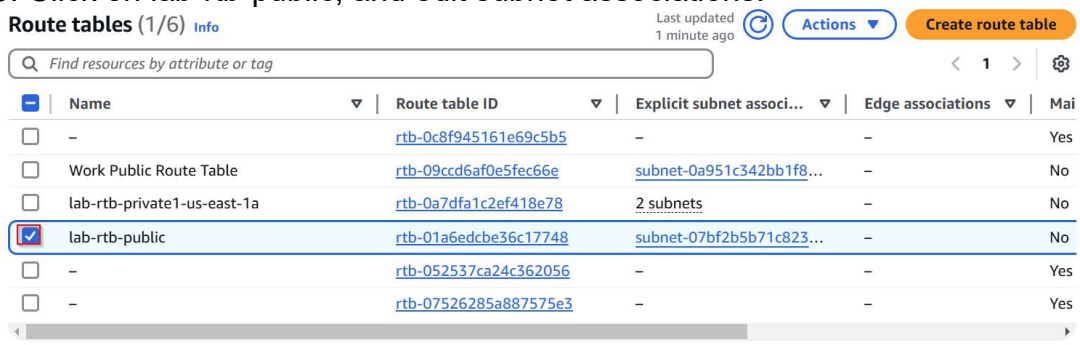
7. Click “Route Tables” and select lab-rtb-private1-us-east-1a. Choose the subnet associations tab, and click “Edit subnet associations”.

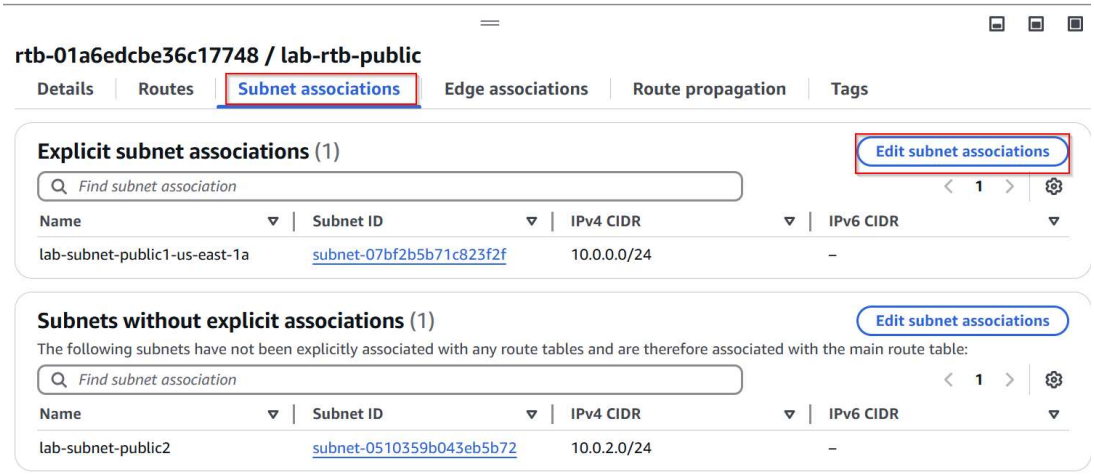


8. Select lab-subnet-private2 while keeping lab-subnet-private1-us-east-1a selected. Click “Save associations”.

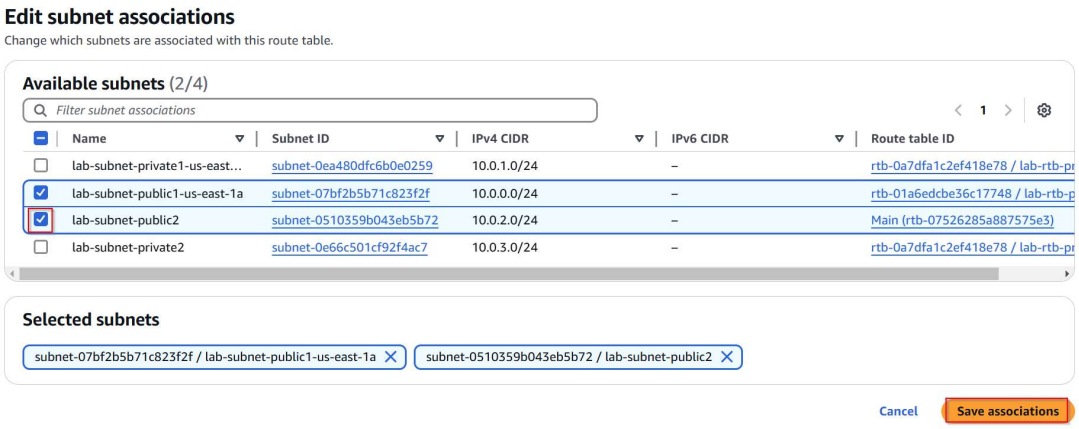


9. Click on lab-rtb-public, and edit subnet associations.

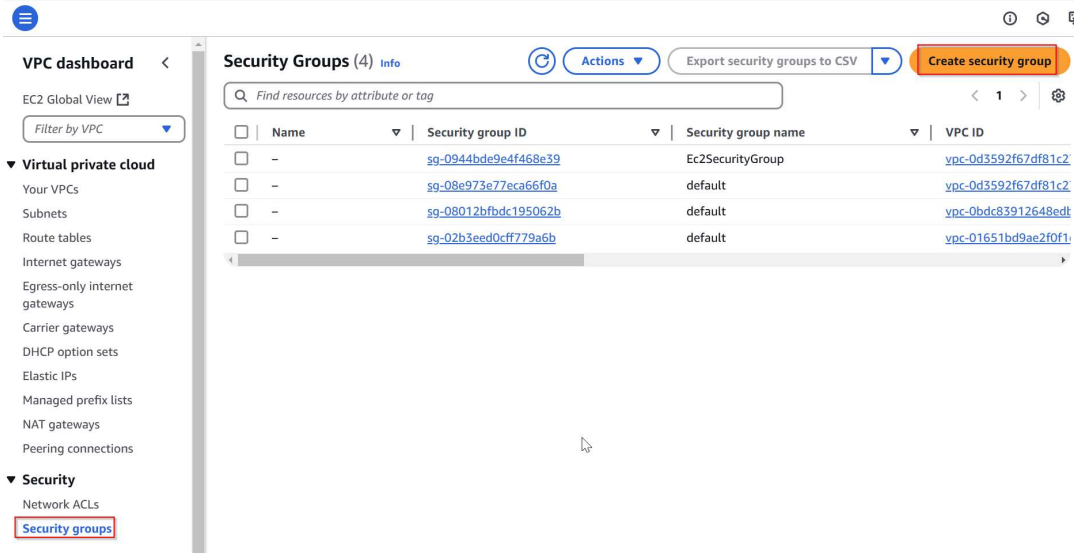


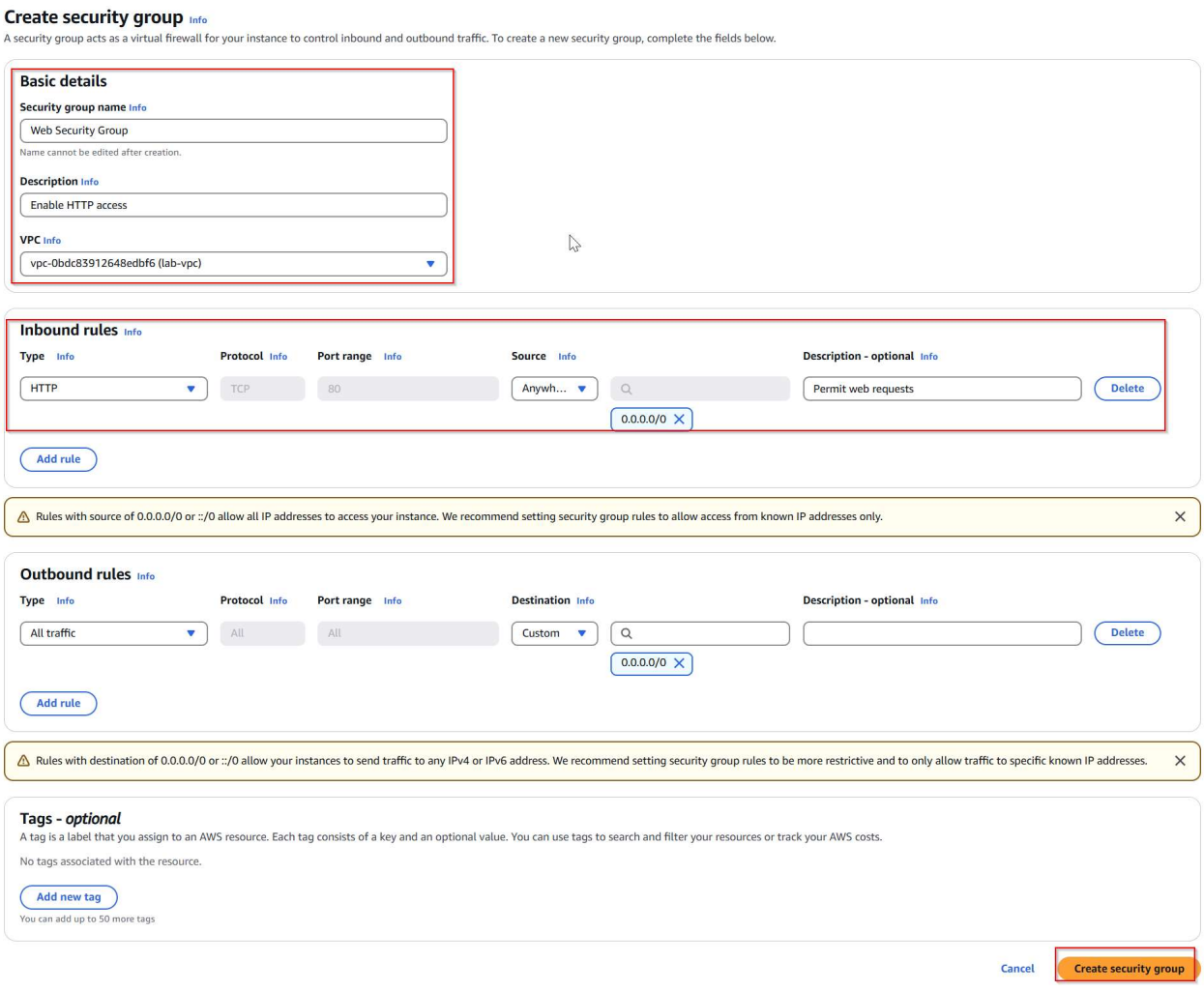


10. Select lab-subnet-public2, while leaving lab-subnet-public1-us-east-1a selected.

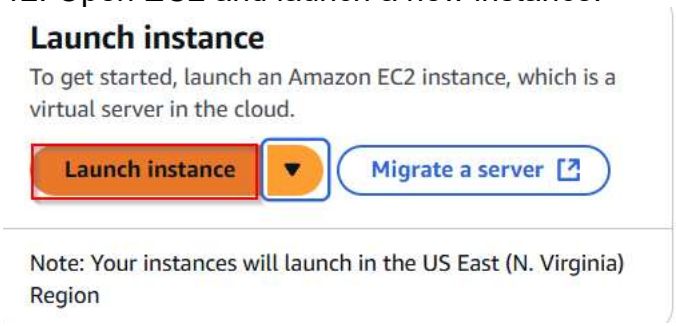


11. Select Security groups. Create a security group with the below configurations.

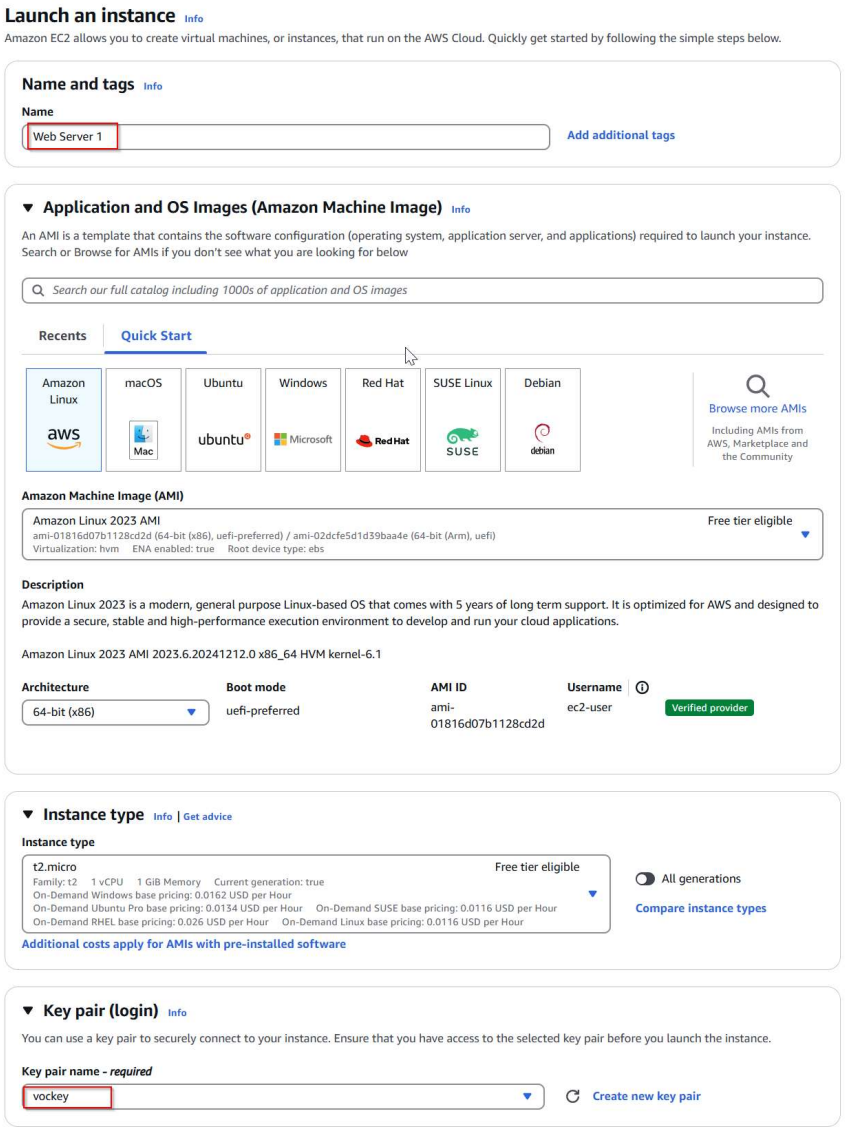


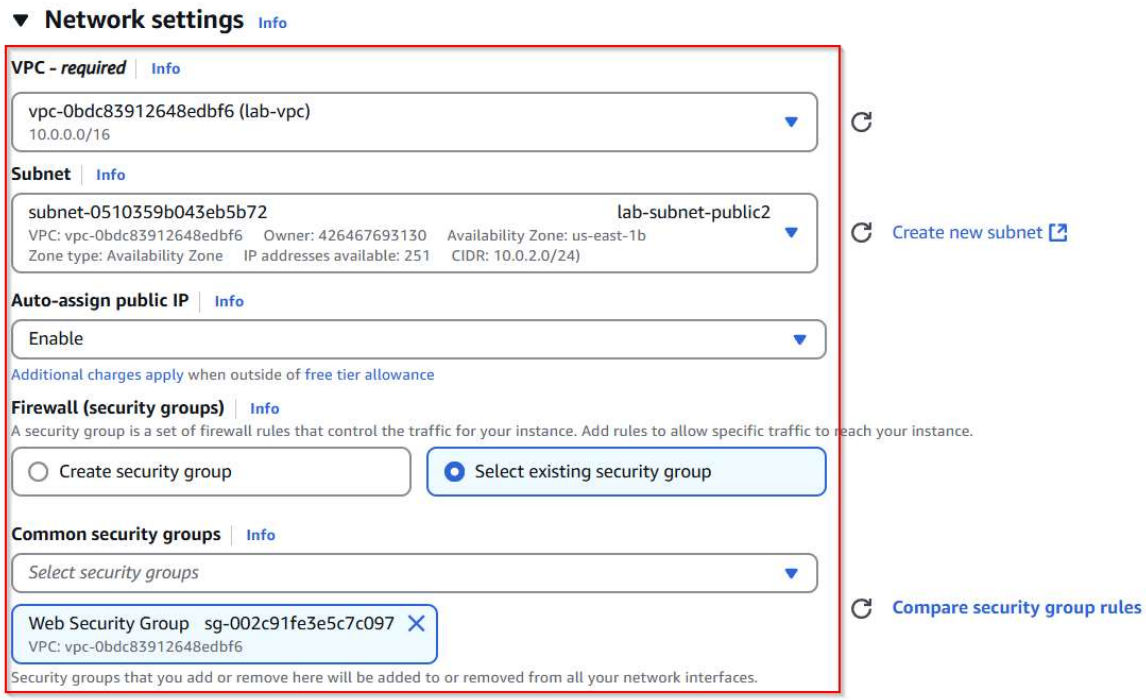


12. Open EC2 and launch a new instance.



13. Name the instance Web Serve 1. Keep the default OS and instance type. Set Key Pair to vockey. Configure the network settings and User data as shown.





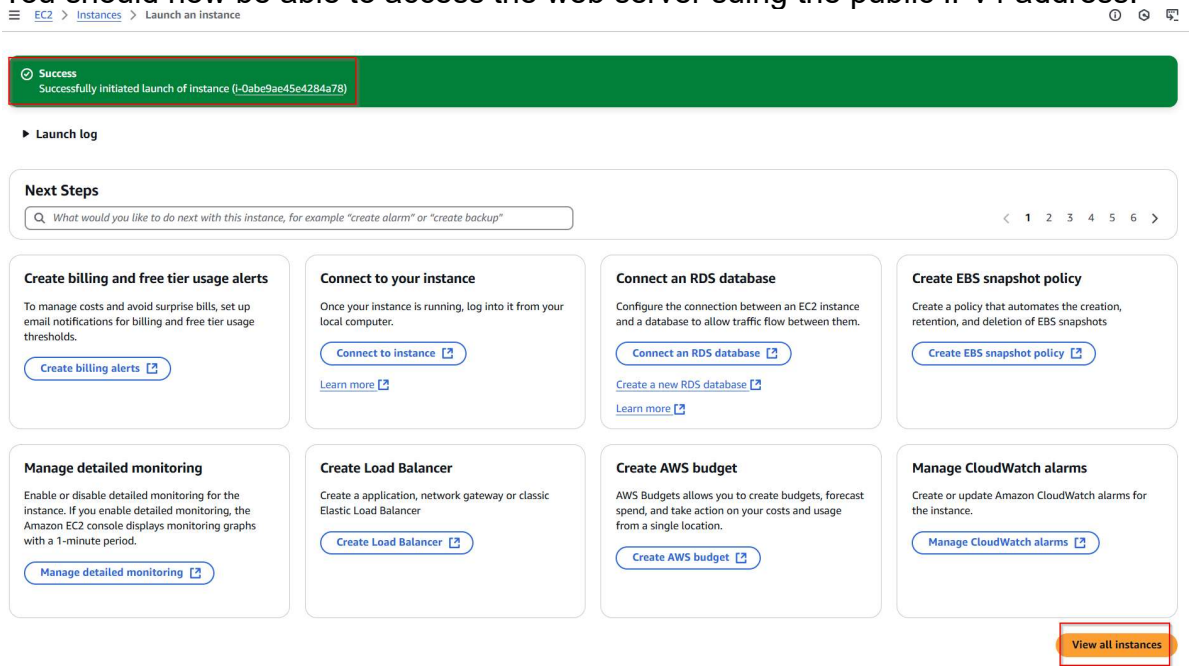
User data - *optional* Info

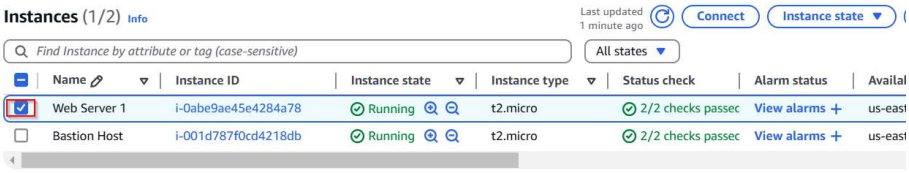
Upload a file with your user data or enter it in the field.

Choose file

```
#!/bin/bash
# Install Apache Web Server and PHP
dnf install -y httpd wget php mariadb105-server
# Download Lab files
wget https://aws-tc-largeobjects.s3.us-west-2.amazonaws.com/CUR-TF-100-ACCLFO-2/2-lab2-vpc/s3/lab-app.zip
unzip lab-app.zip -d /var/www/html/
# Turn on web server
chkconfig httpd on
service httpd start
```

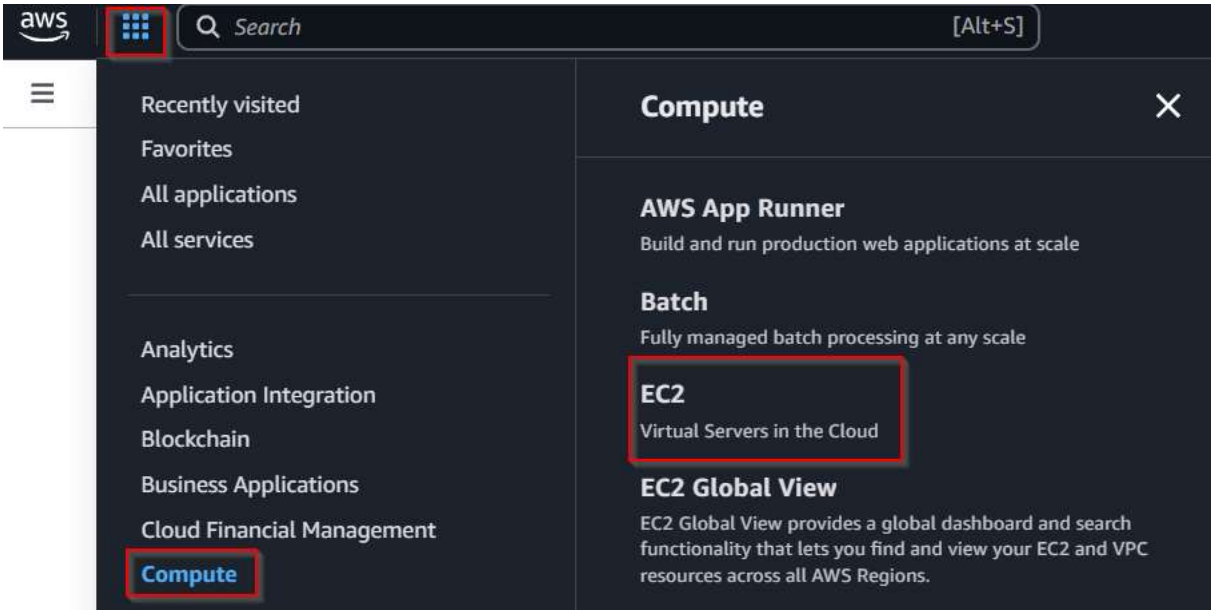
You should now be able to access the web server suing the public IPv4 address.



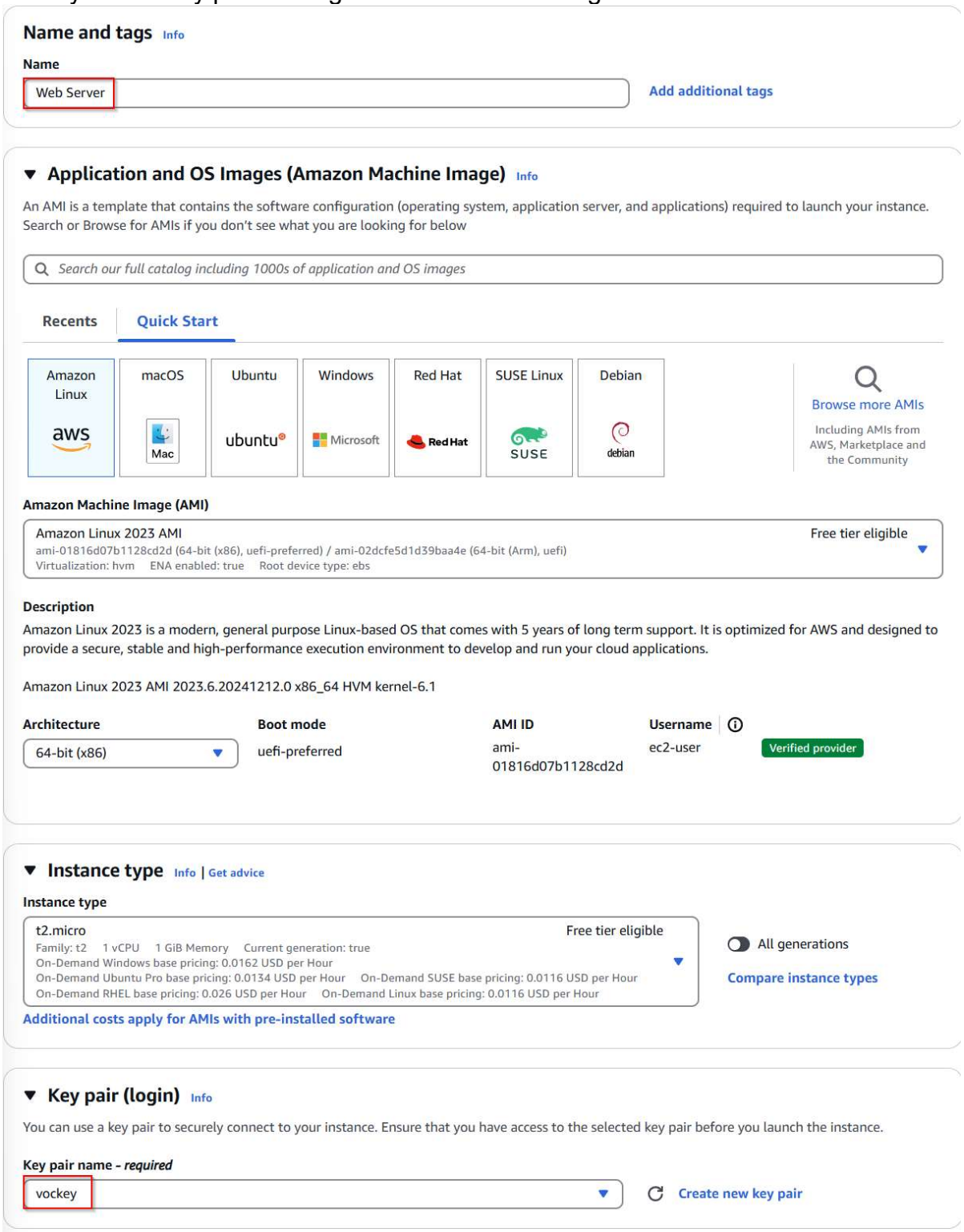


Lab 3

1. Open EC2 and launch a new instance.



2. Name the instance Web Server, keep the default OS and instance type, and use vockey as the key pair. Configure the network settings as shown below.



Network settings Info

VPC - *required* Info

vpc-00e91d20ad92b8d41 (Lab VPC)
10.0.0.0/16

Subnet Info

subnet-04c6dee46b3854c88 PublicSubnet1
VPC: vpc-00e91d20ad92b8d41 Owner: 597053808833 Availability Zone: us-east-1a
Zone type: Availability Zone IP addresses available: 1 CIDR: 10.0.1.0/28)

Create new subnet

Auto-assign public IP Info

Enable

Additional charges apply when outside of free tier allowance

Firewall (security groups) Info

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

- (•) Create security group
- ( ) Select existing security group

Security group name - *required*

Web Server security group

This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and ._-:/()#,@[]+=&;{}!$*

Description - *required* Info

Security group for my web server

Inbound Security Group Rules

No security group rules are currently included in this template. Add a new rule to include it in the launch template.

Add security group rule

▸ **Advanced network configuration**

Advanced details Info

Domain join directory Info

Select Create ne

IAM instance profile Info

Select Create ne

Hostname type Info

IP name

DNS Hostname Info

- [x] Enable IP name IPv4 (A record) DNS requests
- [ ] Enable resource-based IPv4 (A record) DNS requests
- [ ] Enable resource-based IPv6 (AAAA record) DNS requests

Instance auto-recovery Info

Select

Shutdown behavior Info

Stop

Stop - Hibernate behavior Info

Select

Termination protection Info

Enable

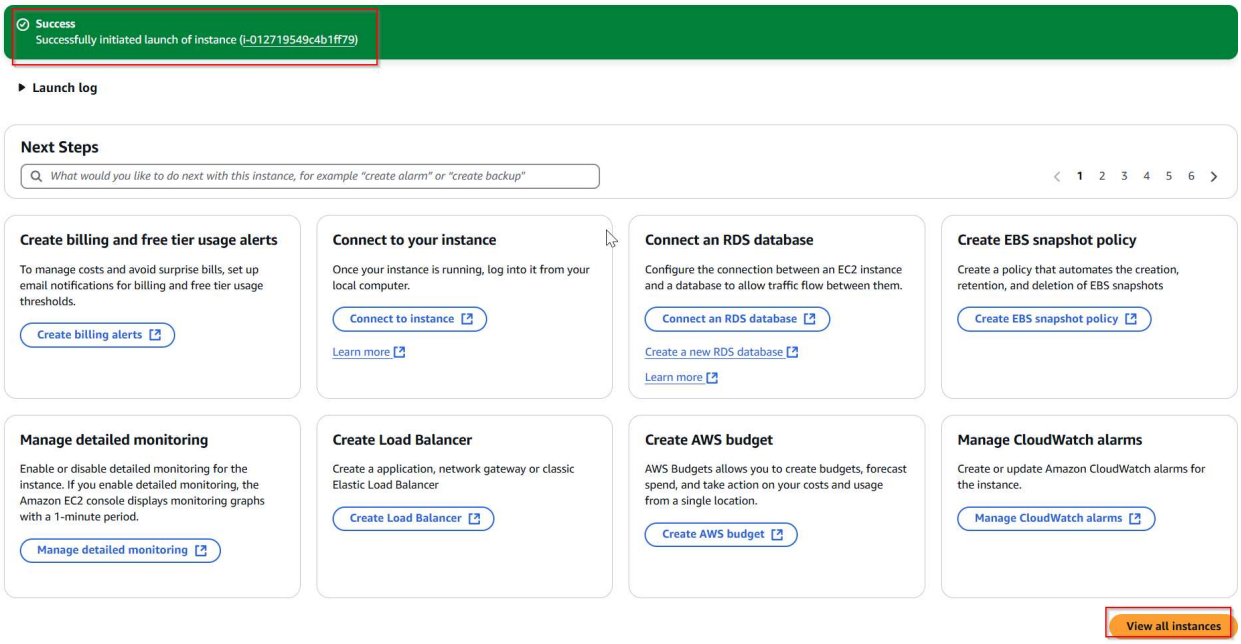
User data - *optional* Info

Upload a file with your user data or enter it in the field.

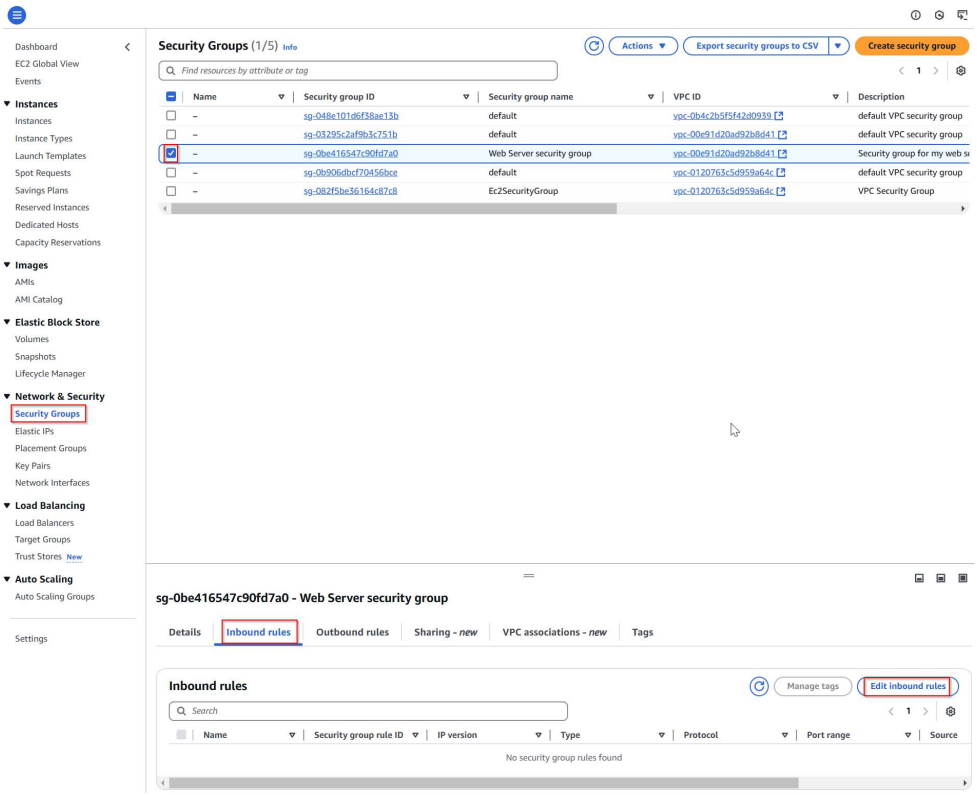
Choose file

```
#!/bin/bash
dnf install -y httpd
systemctl enable httpd
systemctl start httpd
echo '<html><h1>Hello From Your Web Server!</h1></html>' > /var/www/html/index.html
```

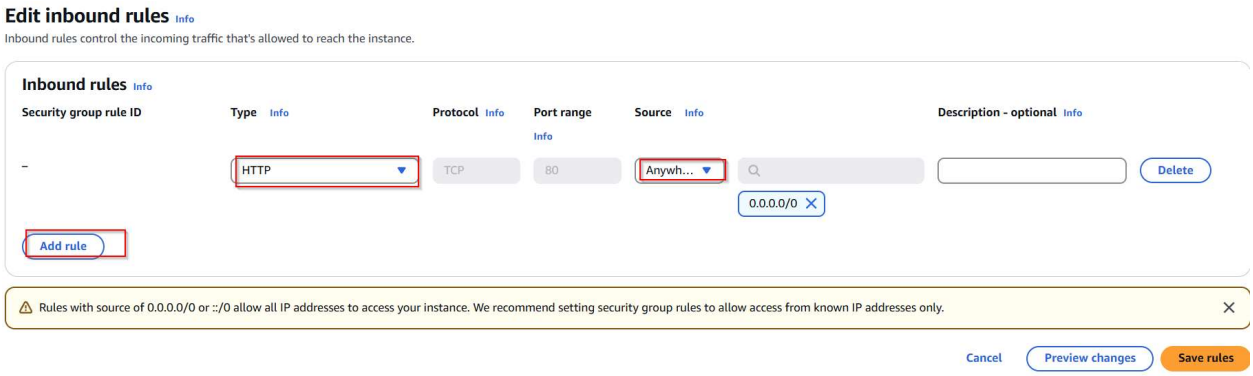
3. Once the instance has been successfully created, view all instances.



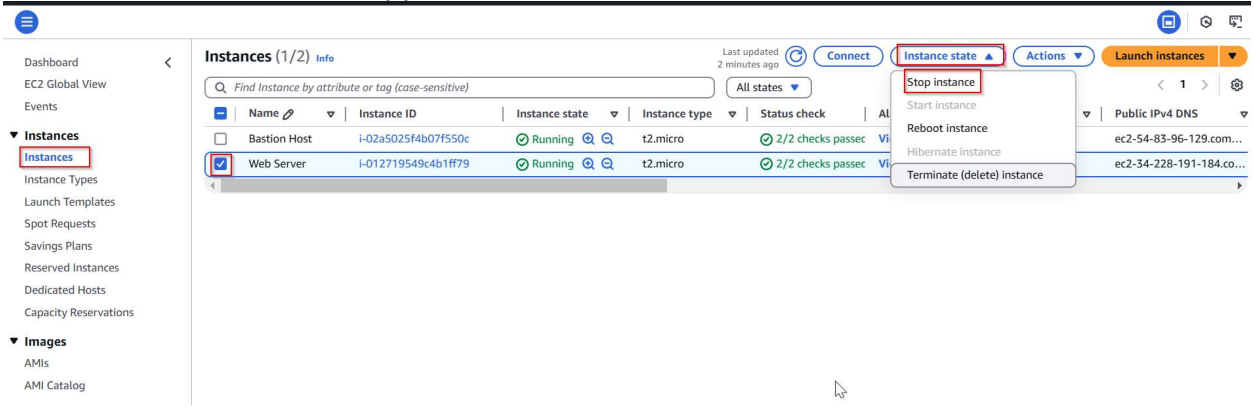
4. Click “Security Groups” and select Web Server security group. Choose the Inbound rules tab and click “Edit Inbound Rules”.



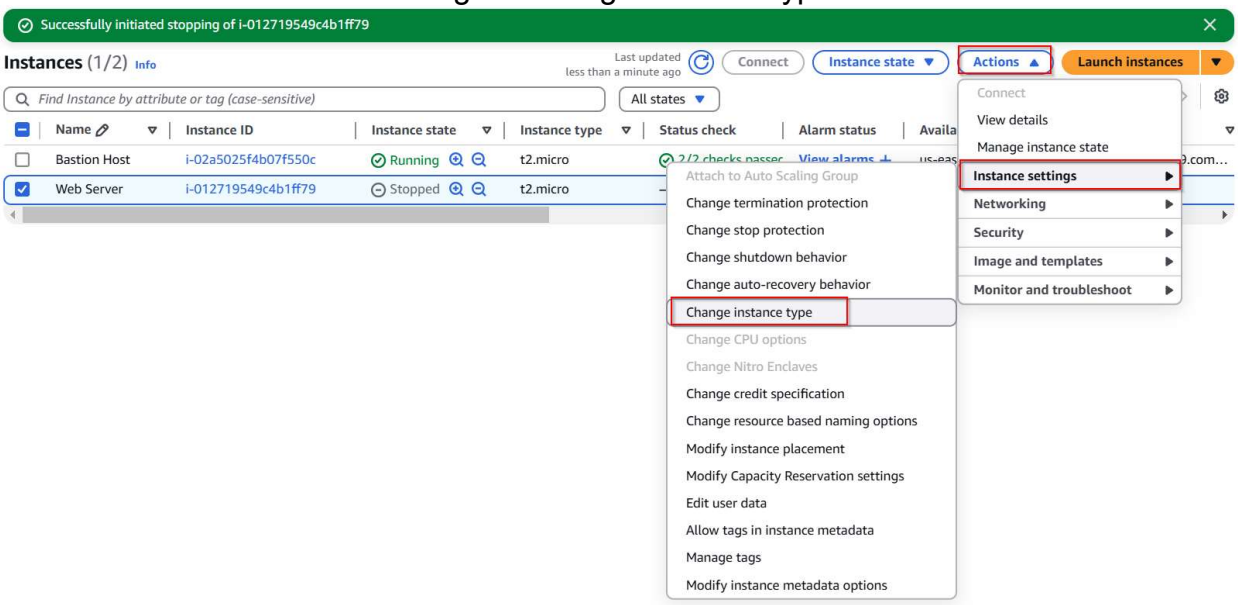
5. Add a rule and configure it to be HTTP and anywhere.



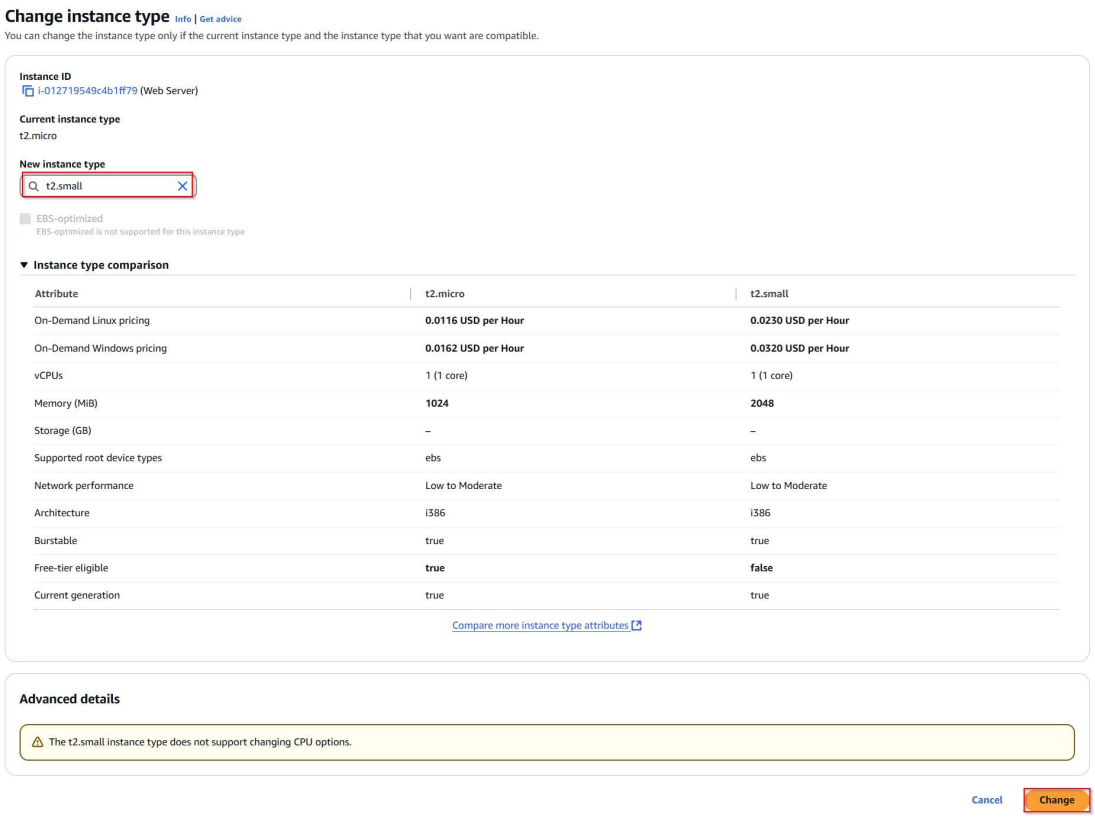
6. Choose Instances, select the Web Server instance, and select Stop instance. Wait for the instance to become stopped.



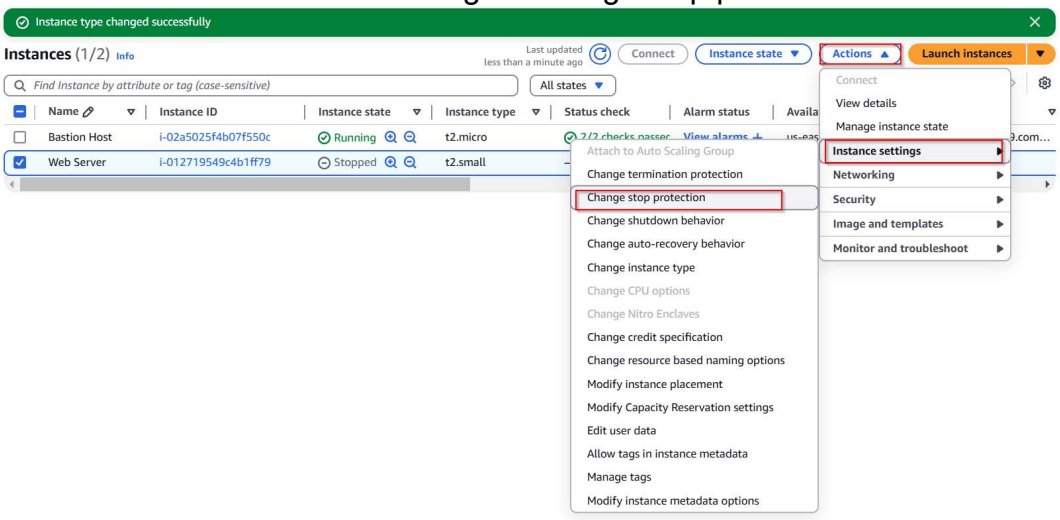
7. Click Actions > Instance settings > Change instance type.

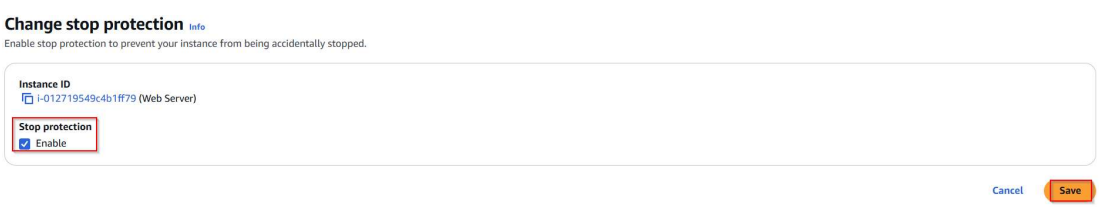


8. Change the instance to t2.small.

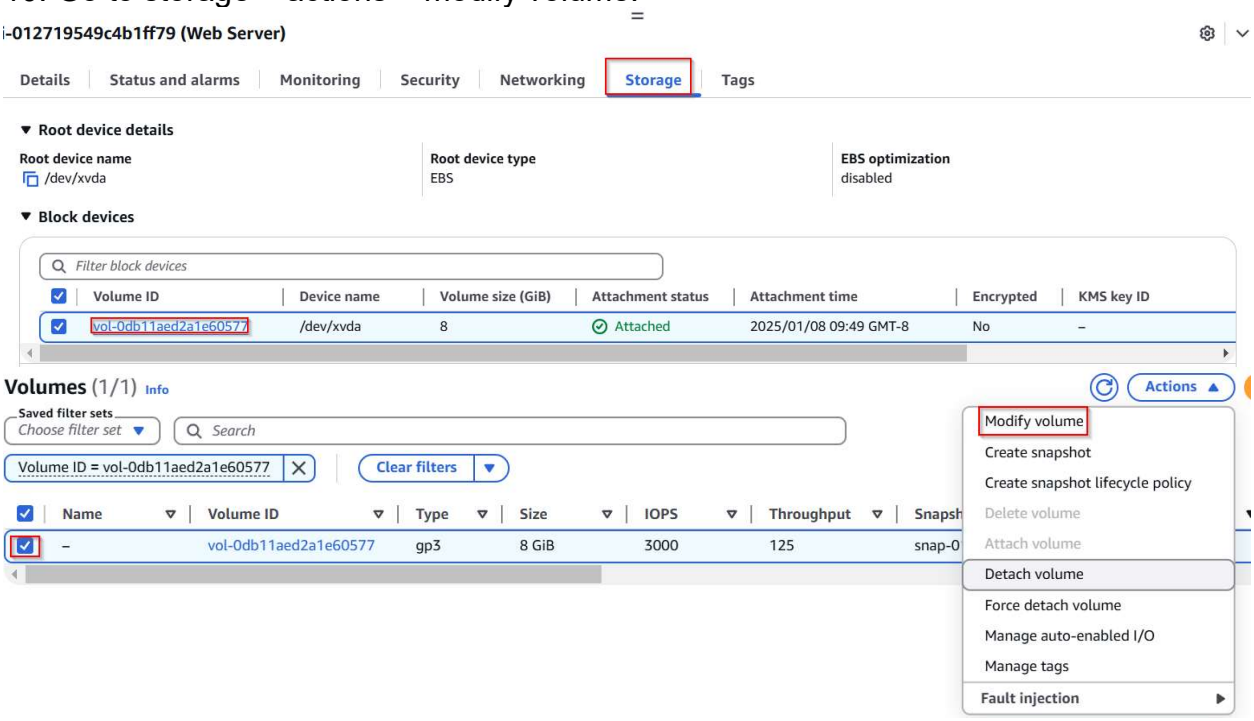


9. Go to Actions > Instance settings > change stop protection

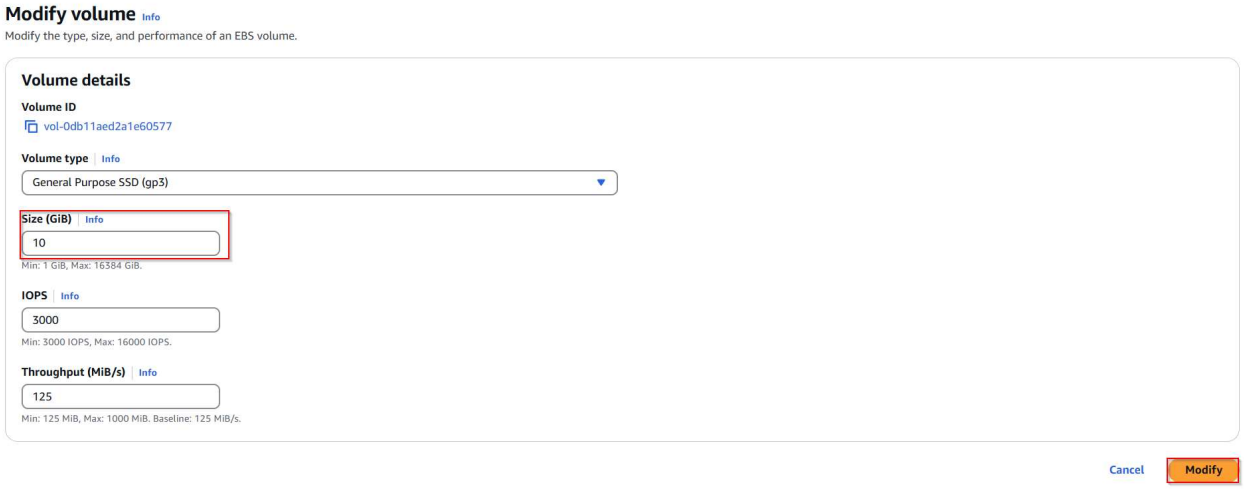




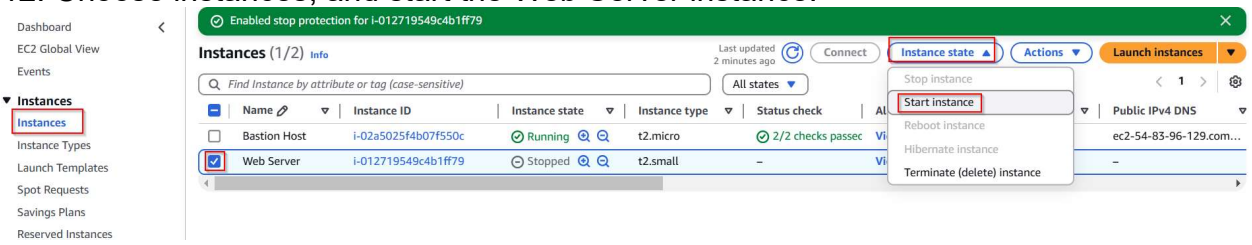
10. Go to storage > actions > modify volume.



11. Change the size to 10 and click “Modify”.



12. Choose instances, and start the Web Server instance.



Problems

In Lab 2, I had an unknown problem when trying to access the IP address of the web server. I believe that it had to do with a misconfiguration in the VPC, but even when fixed, the web server was unable to be accessed. When I restarted, the issue disappeared.

Conclusion

I successfully completed Labs 1-3 of the Amazon Web Services Academy Course. In these labs, I was introduced to the AWS IAM, built a VPC, and launched a web server.

AWS Labs 4-6

Purpose

The purpose of these labs is to gain experience with working with AWS Elastic Block Store (EBS), build a database server, and configure AWS EC2 Auto Scaling and Load Balancing.

Background Information

Amazon Web Services (AWS) is a secure cloud platform offering a set of global cloud-based products. As a cloud computing platform, it offers on-demand access to compute, storage, networking, database, and IT management tools. In addition, customers only need to pay for the specific resources that they use, for as long as they use them, instead of needed to buy hardware for a fixed cost.

Amazon Elastic Block Store (EBS) provides persistent block storage volumes for Amazon EC2 instances. Persistent storage retains data after power to the device is shot off. Every EBS volume is replicated within its availability zone to provide redundancy. Block storage allows portions of files to be updated, rather than updating the entire file when something needs to be changed. Block storage solutions are faster and use less bandwidth than object storage solutions, but will usually cost more.

Amazon EBS volumes can be backed up into files called snapshots. The first snapshot is referred to as the baseline; any future snapshots only capture the differences between the baseline and the current snapshot.

Amazon Relational Database Service (RDS) is a managed service that operates a relational database in the cloud. Managed services have some user configuration, such as setting permissions, while unmanaged services require much more user configuration for more fine-tuned control over the solution. Amazon RDS allows the customer to focus on application optimization and data, rather than the background management.

The building block of Amazon RDS is a database instance, which is an isolated environment containing multiple user-created databases. Currently, RDS allows the usage of MySQL, Amazon Aurora, Microsoft SQL, PostgreSQL, MariaDB, and Oracle. Instances can be run through Amazon Virtual Private Cloud (VPC), which allows the configuration of IP addresses, subnets, routing, and access control lists.

Amazon provides Elastic Load Balancing, which is able to distribute incoming traffic across several targets, including Amazon EC2 instances, containers, and IP address,

across multiple availability zones. Elastic Load Balancing is available to be an application load balancer, network load balancer, or classic load balancer. Application load balancers balanced HTTP and HTTPS traffic and routes traffic to targets based on the content of the request. Network Load Balancers balances TCP, UDP, and TLS traffic, and routes traffic to targets based on IP protocol data. Classic Load Balancers, or the previous generation of load balancers, handle HTTP, HTTPS, TCP, and SSL traffic.

A load balancer accepts incoming traffic from specified listeners and routes requires to registered targets. Load balancers can be configured to perform health checks, to ensure that traffic is only sent to healthy instances. Load balancers allow applications to have better availability, higher fault tolerance and be able to scale to match the demands of customers.

Amazon CloudWatch is a monitoring service and is able to monitor AWS services in real time. Alarms can be created to monitor CloudWatch metrics to send a notification or perform Amazon EC2 Autoscaling. For instance, in this lab, when an alarm is triggered for CPU load on an EC2 instance, CloudWatch notifies Auto Scaling which creates more EC2 instances.

Amazon EC2 Auto Scaling helps to maintain application availability in times of high demand. It enables the automatic addition or deletion of EC2 instances according to predefined conditions. It is also able to detect unhealthy instances and applications, and replace them without administrative intervention.

Lab Summary

In the fourth lab, you will create an Amazon EBS volume, attach the volume to an EC2 instance, create a snapshot of the volume, restore the volume from the screenshot, and attach the restored volume to an EC2 instance.

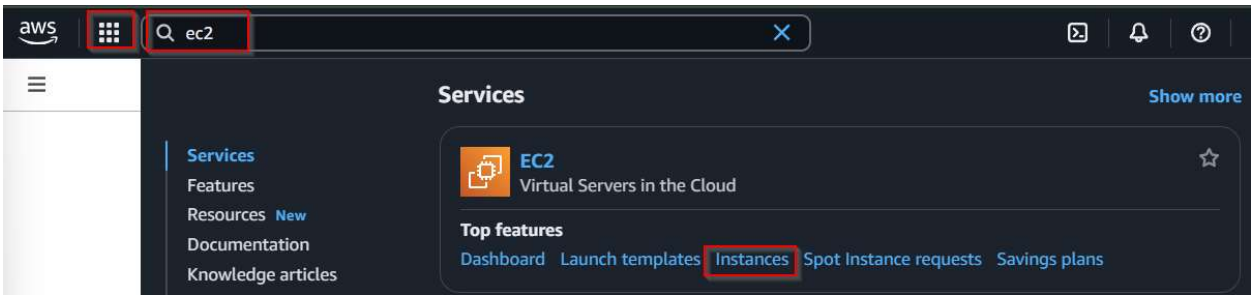
In the fifth lab, you will launch an Amazon RDS DB instance, configure it to allow connections from a web server, and test out interacting with the database from the web application.

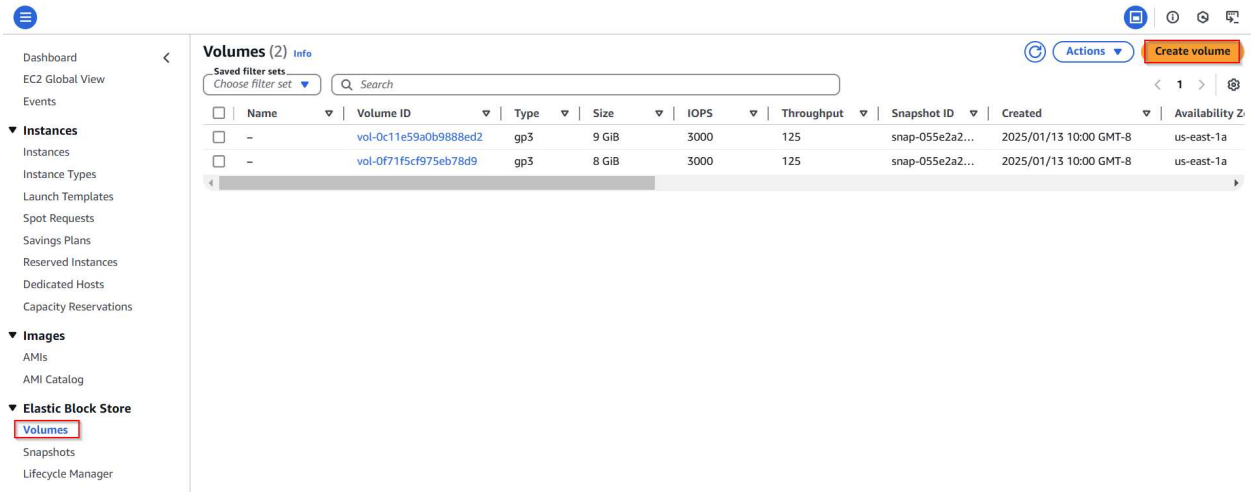
In the sixth lab, you will create an Amazon Machine Image (AMI) from a running instance, create a load balancer, create an Auto Scaling group, automatically scale new instances, and create CloudWatch alarms.

Lab Commands

Lab 4

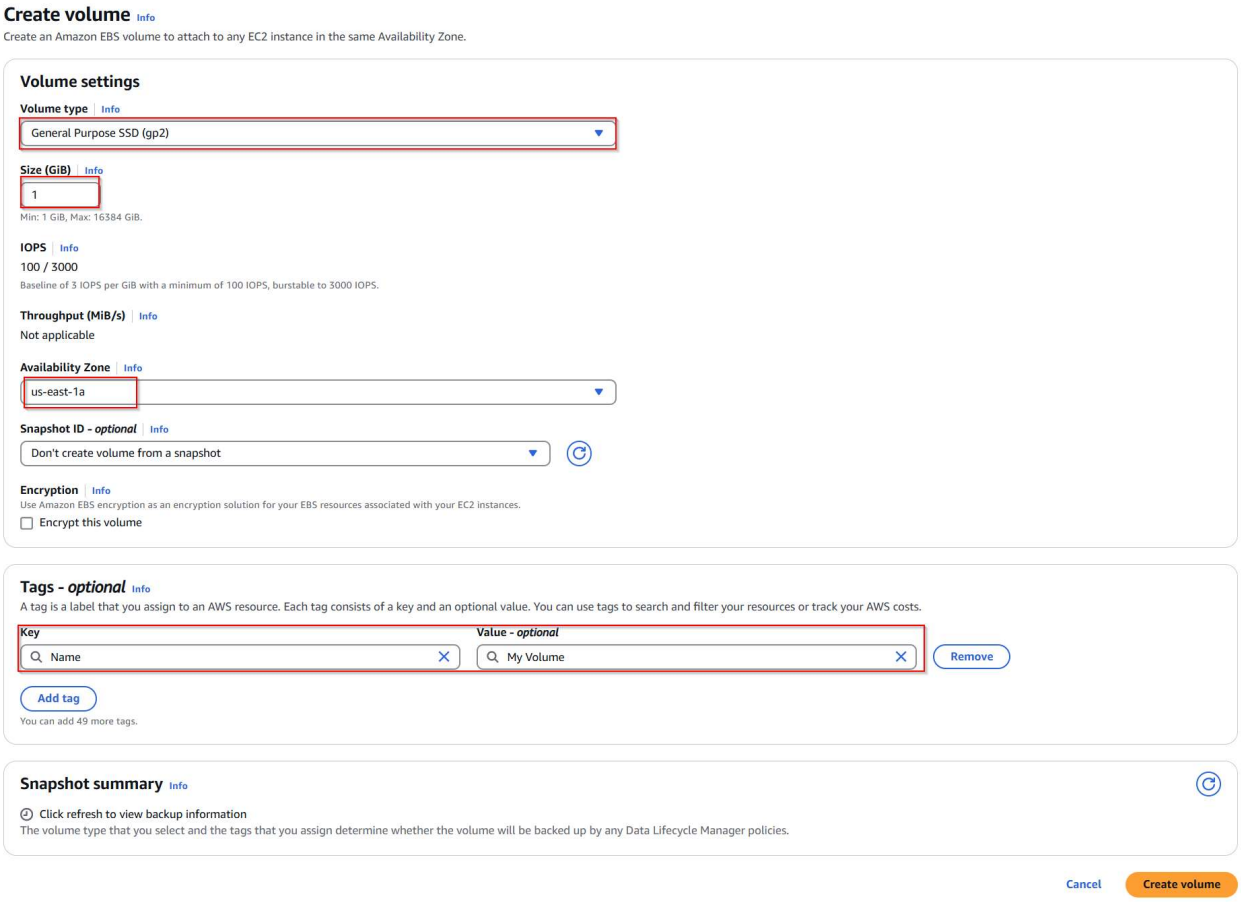
1. Navigate to EC2 Instances, and choose Volumes. Click “Create volume”.



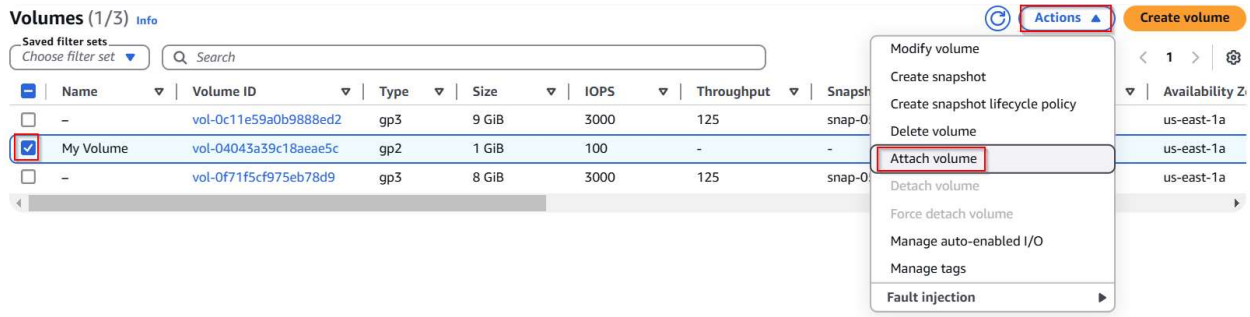


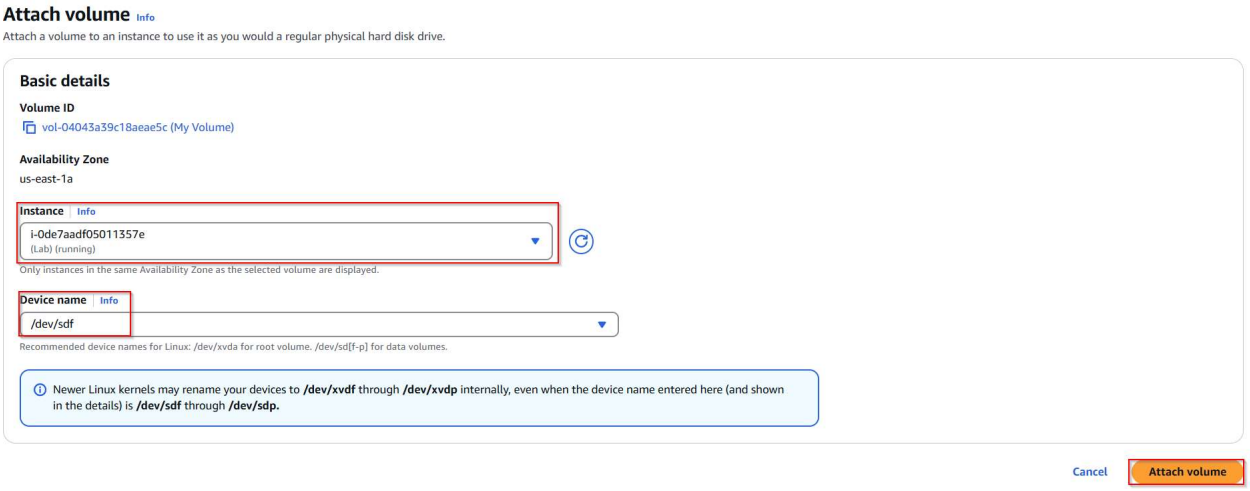
2. Configure

- Volume Type: “General Purpose SSD (gp2)”
- Size: 1
- Add a tag and enter
    - Key: Name
    - Value: My Volume.

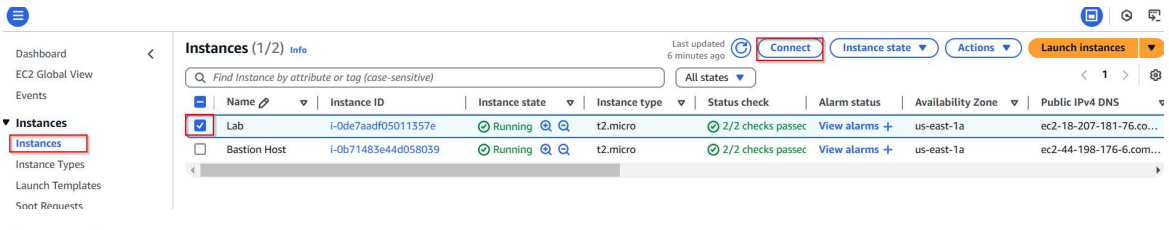


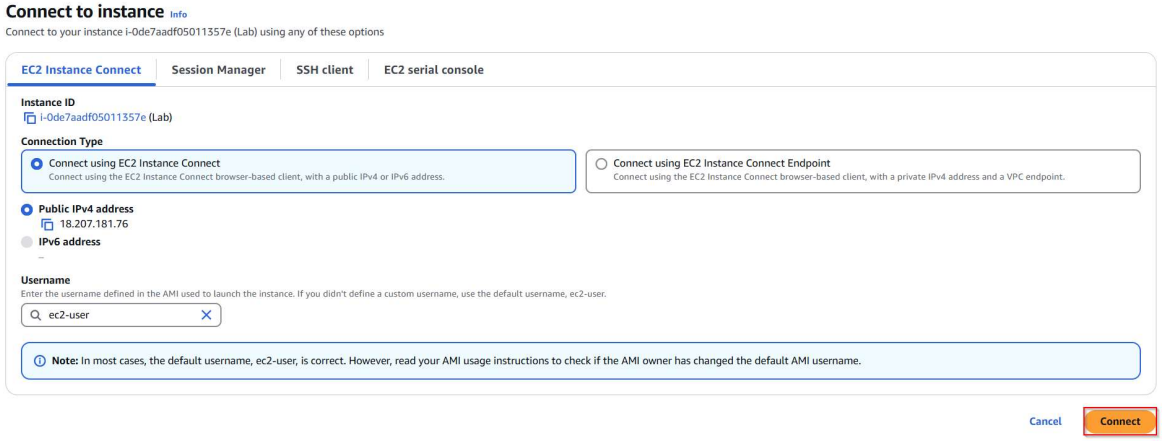
3. Select “My Volume”, and click Actions > Attach volume. Attach it to the Lab instance.





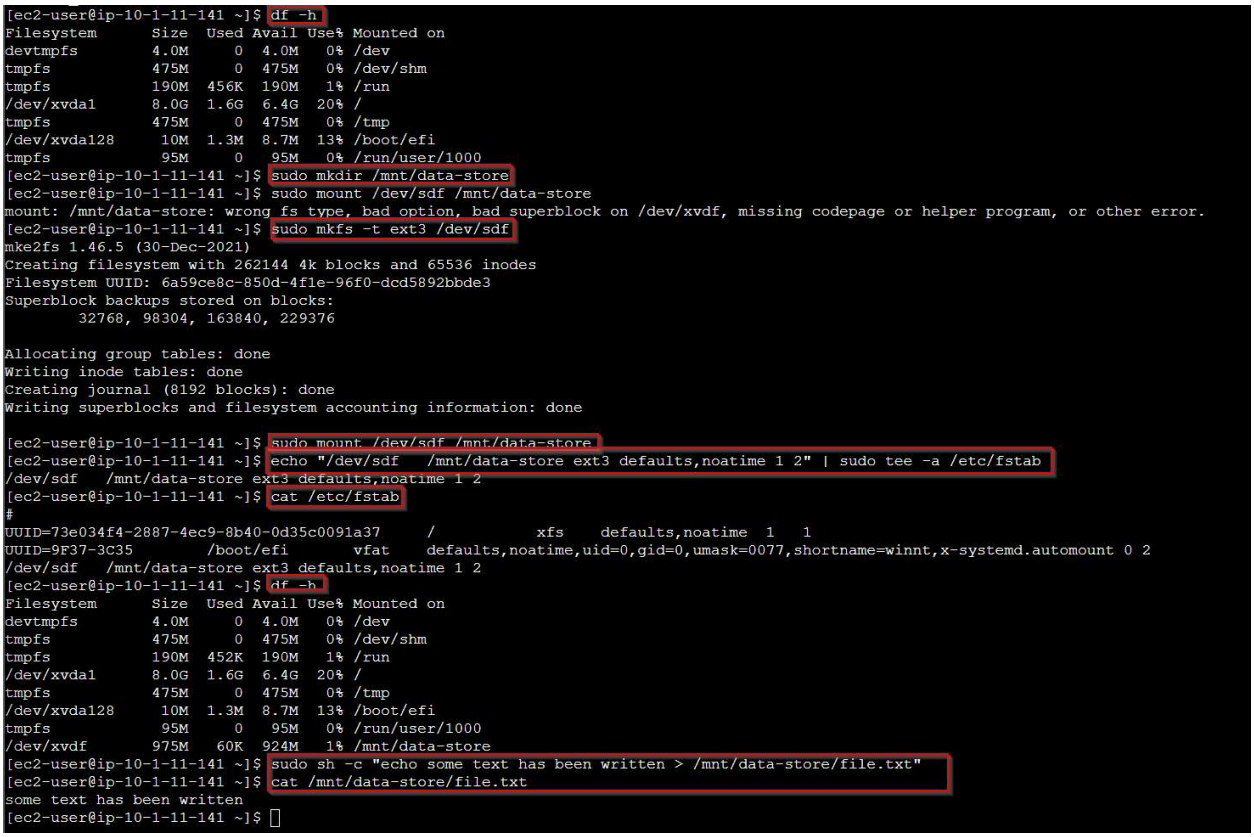
4. In the Instances tab of EC2, connect to the Lab instance. An EC2 Instance Connect terminal will open.



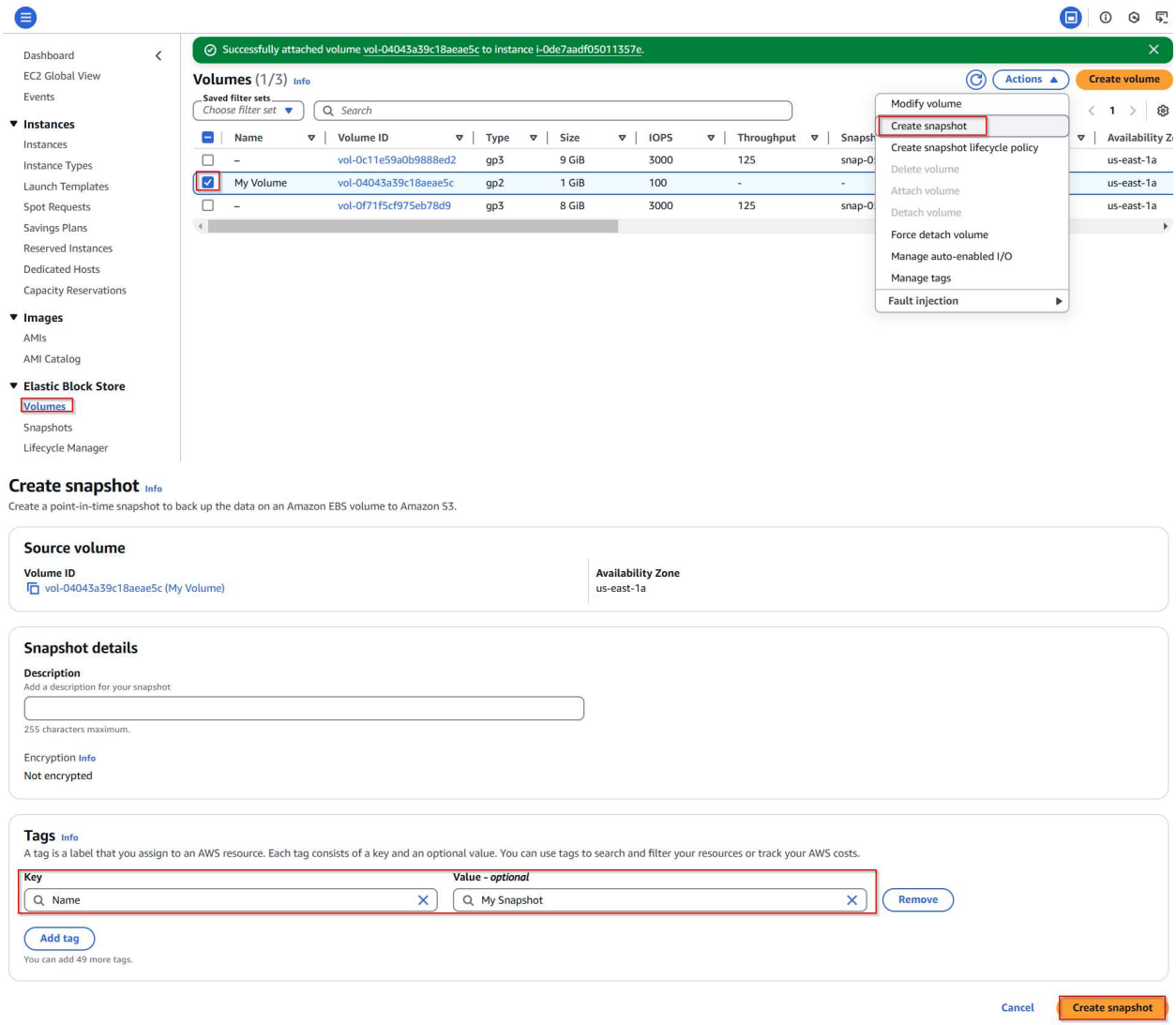


5. In the terminal, run the following commands:

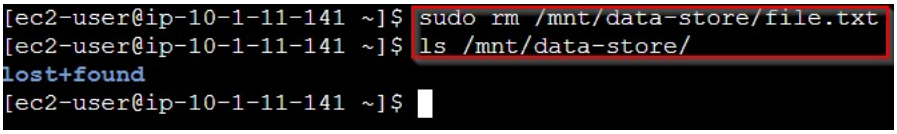
- df -h
- sudo mkfs -t ext3 /dev/sdf
- sudo mkdir /mnt/data-store
- sudo mount /dev/sdf /mnt/data-store
- echo “/dev/sdf /mnt/data-store ext3 defaults,noatime 1 2” | sudo tee -a /etc/fstab
- sudo sh -c “echo some text has been written > /mnt/data-store/file.txt”



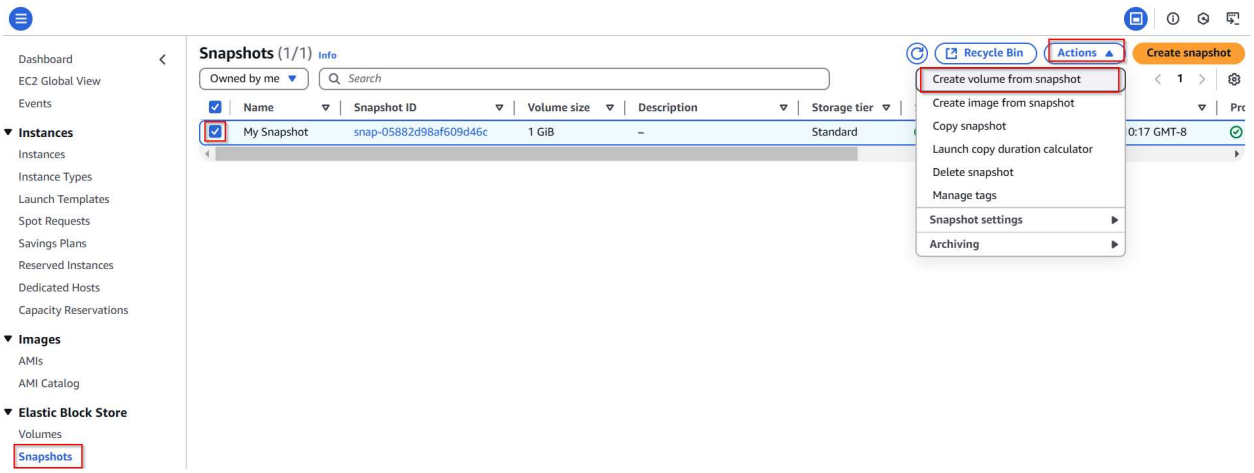
6. Navigate to EC2 > Volumes and select My Volume. Click Actions > Create snapshot. Set the key to Name and value to My Snapshot.

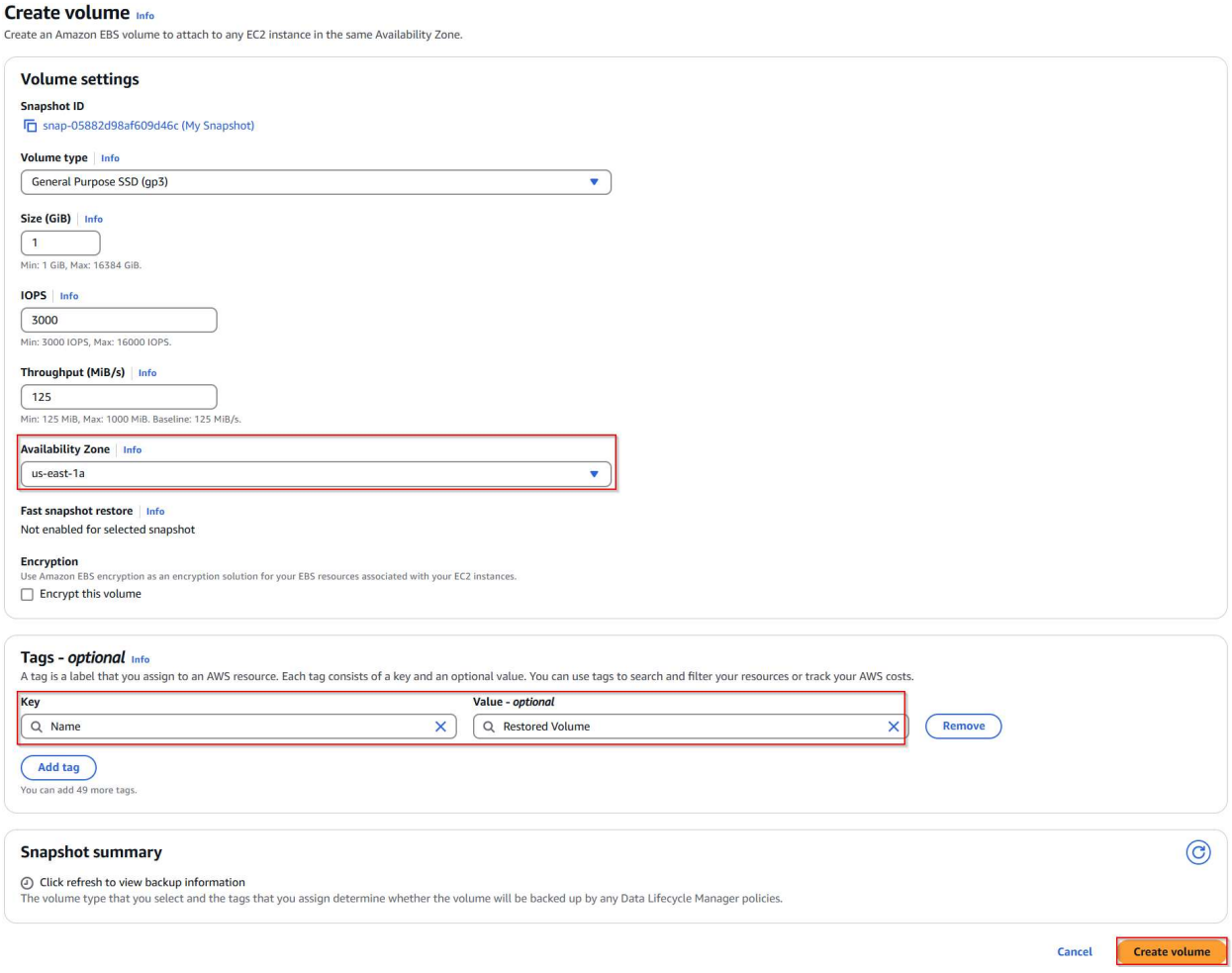


7. Delete the file previously created on the volume

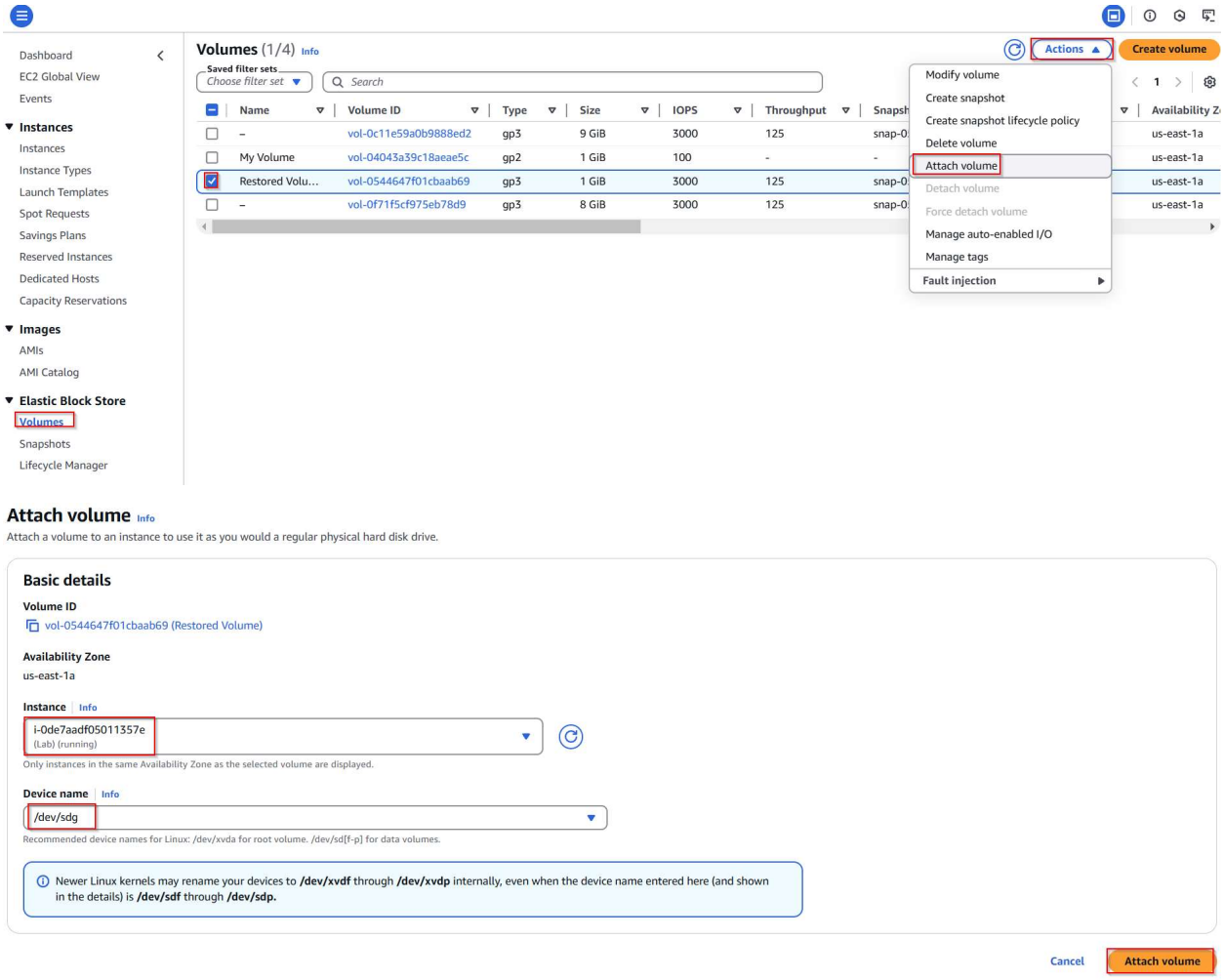


8. Navigate to Snapshots and select My Snapshot. Click Actions > Create volume from snapshot. Configure the volume as shown.





9. Navigate to Volumes and selected Restored Volume. Click Actions > Attach volume. Choose the Lab instance, and set the Device to /dev/sdg.

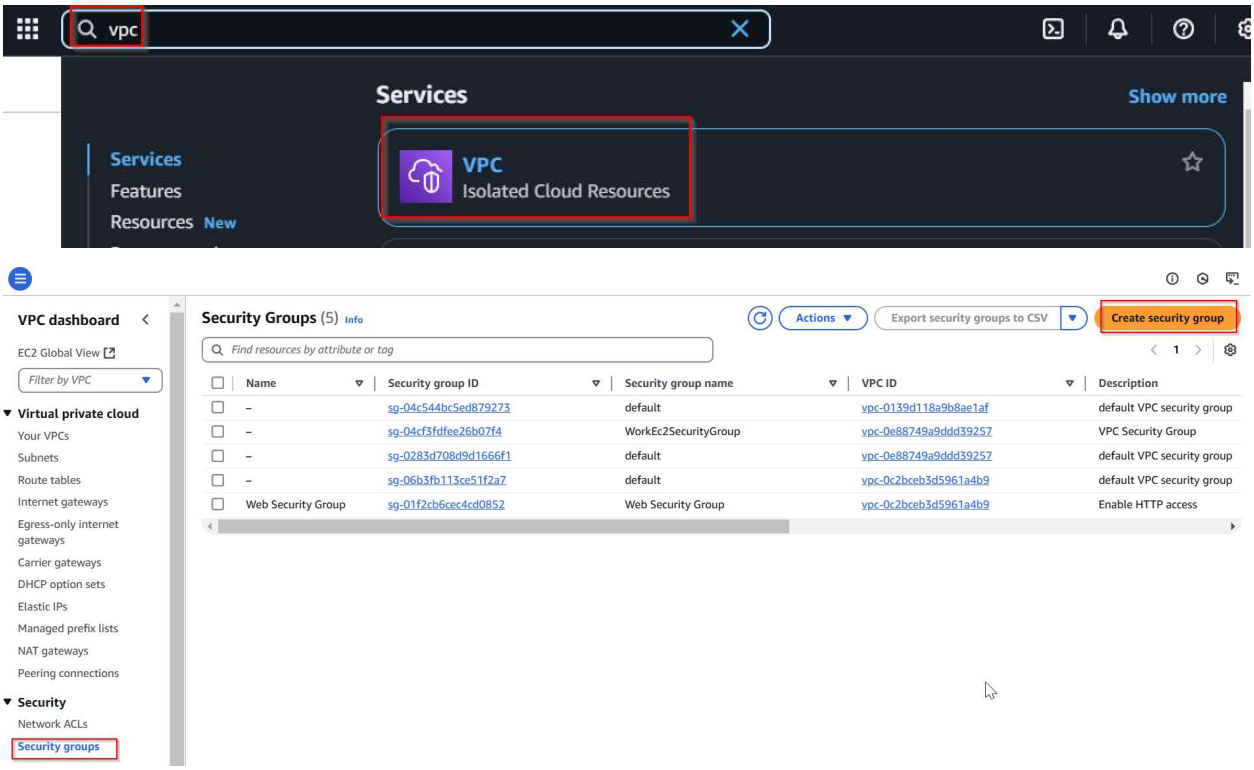


10. Mount the new volume using the below commands.

```
[ec2-user@ip-10-1-11-141 ~]$ sudo mkdir /mnt/data-store2
[ec2-user@ip-10-1-11-141 ~]$ sudo mount /dev/sdg /mnt/data-store2
[ec2-user@ip-10-1-11-141 ~]$ ls /mnt/data-store2/
file.txt  lost+found
```

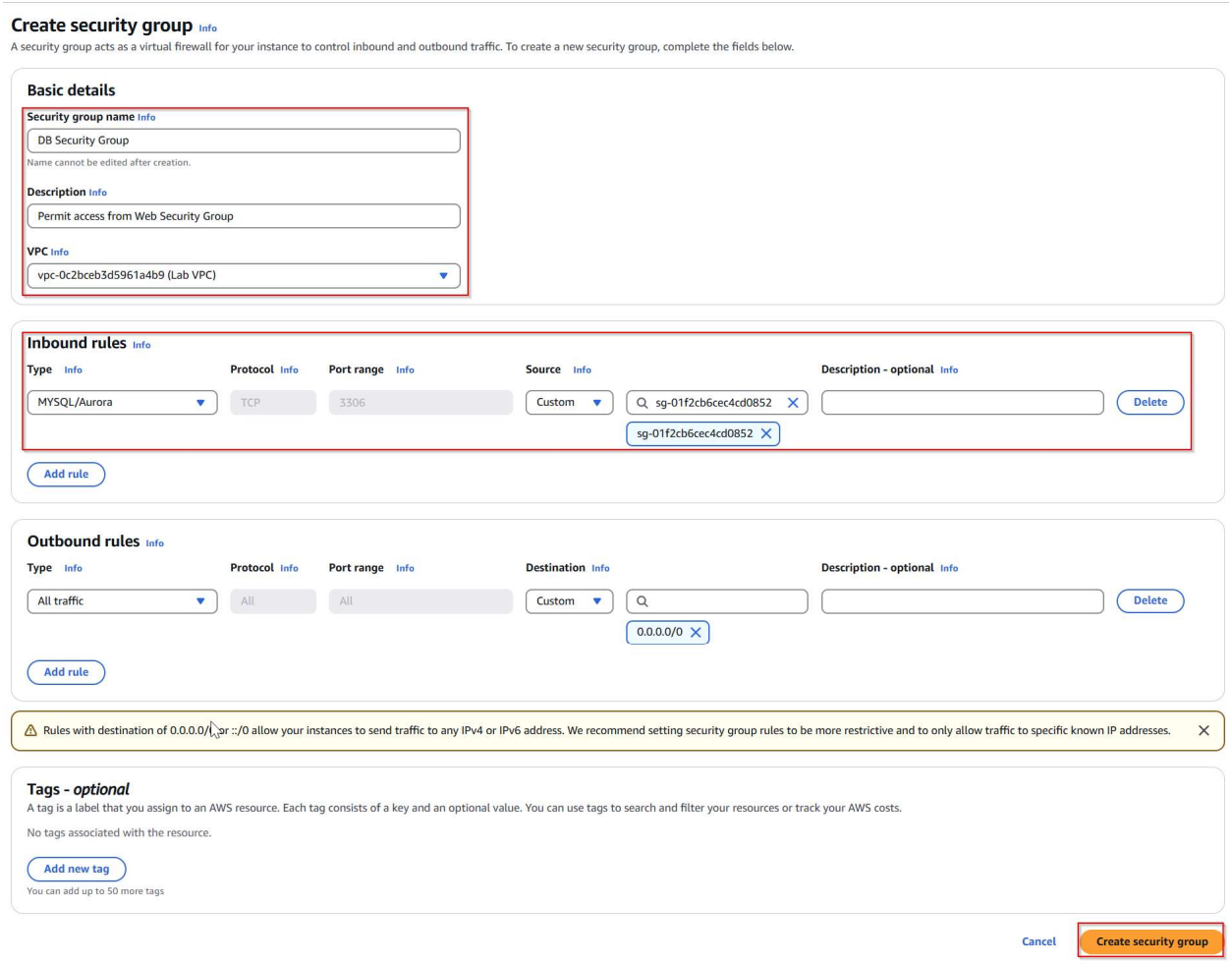
Lab 5

1. Navigate to VPC > Security Groups. Create a security group.

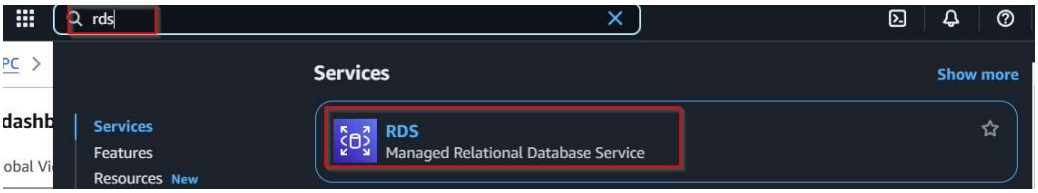


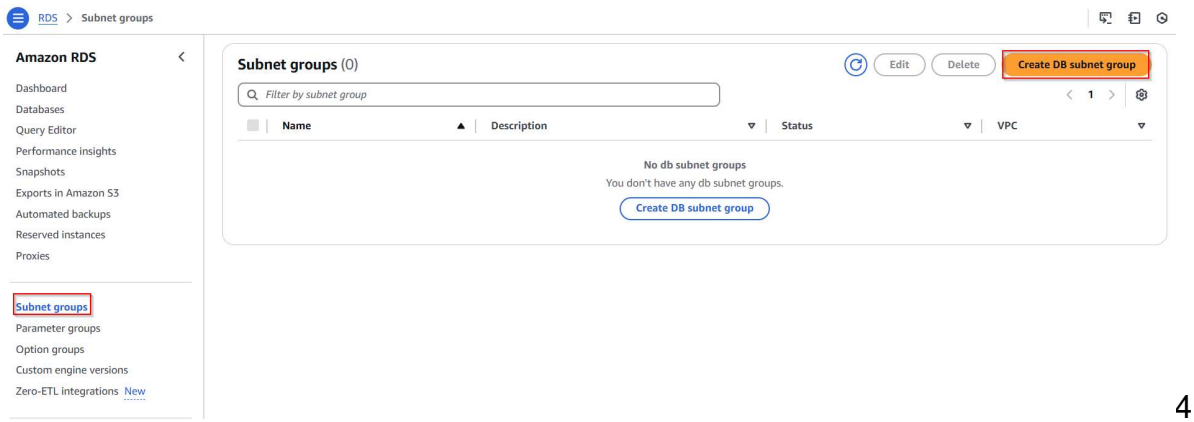
2. Configure:

- Security group name: DB Security Group
- Description: Permit access from Web Security Group
- VPC: Lab VPC
- Add a rule:
    - Type: MySQL/Aurora (3306)
    - Source: Web Security Group (type sg)



3. Navigate to RDS > Subnet groups. Create a DB Subnet Group.

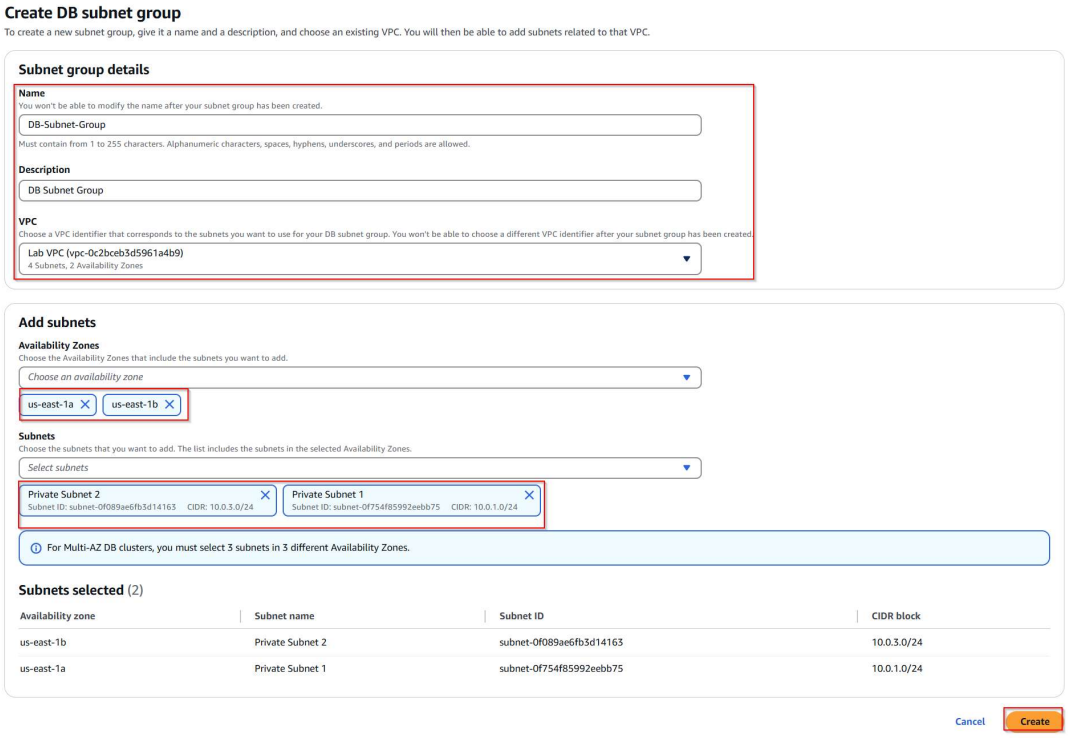




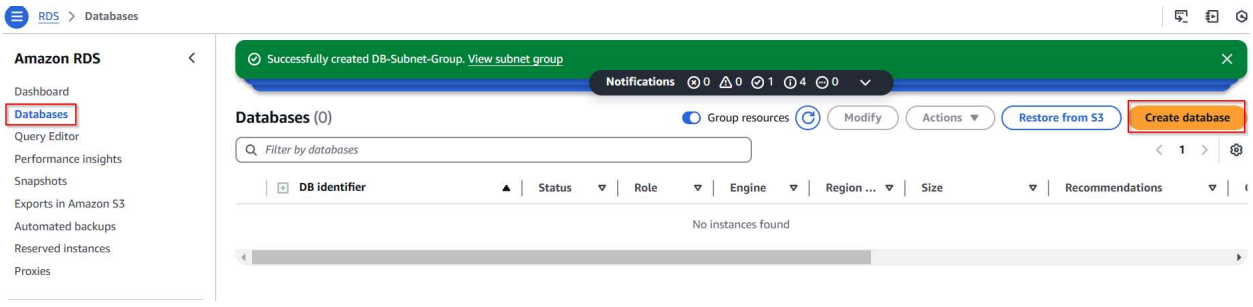
4.

4. Configure:

- Name: DB-Subnet-Group
- Descirption: DB Subnet Group
- VPC: Lab VPC
- Availability Zones: us-east-1a and us-east-1b
- Subnets: 10.0.1.0/24 and 10.0.3.0/24



5. Navigate to Databases and click Create Database.



6. Configure:

- Engine Options: MySQL
- Templates: Dev/Test
- Availability and durability: Multi-AZ DB
- Under Settings, configure:
    - DB instance identifier: lab-db
    - Master username: main
    - Credentials Management: Self managed
    - Mater password: lab-password
    - Confirm password: lab-password
- DB instance class: Burstable classes, db.t3.micro
- Storage type: General Purpose (SSD)
- Allocated storage: 20
- Connectivity: Lab VPC
- Existing VPC security groups: DB Security Group
- Uncheck Enable Enhanced monitoring
- Initial database name: lab
- Uncheck Enable automatic backups
- Uncheck Enable encryption

Create database Info

Choose a database creation method

- (•) Standard create
  You set all of the configuration options, including ones for availability, security, backups, and maintenance.
- ( ) Easy create
  Use recommended best-practice configurations. Some configuration options can be changed after the database is created.

Engine options

Engine type Info

- ( ) Aurora (MySQL Compatible)
- ( ) Aurora (PostgreSQL Compatible)
- (•) MySQL
- ( ) PostgreSQL
- ( ) MariaDB
- ( ) Oracle
- ( ) Microsoft SQL Server
- ( ) IBM Db2

Edition

(•) MySQL Community

Engine version Info

View the engine versions that support the following database features.

▼ Hide filters

- [ ] Show only versions that support the Multi-AZ DB cluster Info
  Create a A Multi-AZ DB cluster with one primary DB instance and two readable standby DB instances. Multi-AZ DB clusters provide up to 2x faster transaction commit latency and automatic failover in typically under 35 seconds.
- [ ] Show only versions that support the Amazon RDS Optimized Writes Info
  Amazon RDS Optimized Writes improves write throughput by up to 2x at no additional cost.

Engine version

MySQL 8.0.39

- [ ] Enable RDS Extended Support Info
  Amazon RDS Extended Support is a paid offering. By selecting this option, you consent to being charged for this offering if you are running your database major version past the RDS end of standard support date for that version. Check the end of standard support date for your major version in the RDS for MySQL documentation.

Templates

Choose a sample template to meet your use case.

- ( ) Production
  Use defaults for high availability and fast, consistent performance.
- (•) Dev/Test
  This instance is intended for development use outside of a production environment.
- ( ) Free tier
  Use RDS Free Tier to develop new applications, test existing applications, or gain hands-on experience with Amazon RDS. Info

Availability and durability

Deployment options Info

The deployment options below are limited to those supported by the engine you selected above.

- ○ Multi-AZ DB Cluster
  Creates a DB cluster with a primary DB instance and two readable standby DB instances, with each DB instance in a different Availability Zone (AZ). Provides high availability, data redundancy and increases capacity to serve read workloads.
- ◉ Multi-AZ DB instance
  Creates a primary DB instance and a standby DB instance in a different AZ. Provides high availability and data redundancy, but the standby DB instance doesn't support connections for read workloads.
- ○ Single DB instance
  Creates a single DB instance with no standby DB instances.

Settings

DB instance identifier Info

Type a name for your DB instance. The name must be unique across all DB instances owned by your AWS account in the current AWS Region.

lab-db

The DB instance identifier is case-insensitive, but is stored as all lowercase (as in "mydbinstance"). Constraints: 1 to 63 alphanumeric characters or hyphens. First character must be a letter. Can't contain two consecutive hyphens. Can't end with a hyphen.

▼ Credentials Settings

Master username Info

Type a login ID for the master user of your DB instance.

main

1 to 16 alphanumeric characters. The first character must be a letter.

Credentials management

You can use AWS Secrets Manager or manage your master user credentials.

- ○ Managed in AWS Secrets Manager - *most secure*
  RDS generates a password for you and manages it throughout its lifecycle using AWS Secrets Manager.
- ◉ Self managed
  Create your own password or have RDS create a password that you manage.

☐ Auto generate password
Amazon RDS can generate a password for you, or you can specify your own password.

Master password Info

••••••••••••

Password strength Neutral

Minimum constraints: At least 8 printable ASCII characters. Can't contain any of the following symbols: / ' " @

Confirm master password Info

••••••••••••

Instance configuration

The DB instance configuration options below are limited to those supported by the engine that you selected above.

DB instance class Info

▼ Hide filters

- ◯ Show instance classes that support Amazon RDS Optimized Writes Info
  Amazon RDS Optimized Writes improves write throughput by up to 2x at no additional cost.
- ◯ Include previous generation classes

- ○ Standard classes (includes m classes)
- ○ Memory optimized classes (includes r and x classes)
- ◉ Burstable classes (includes t classes)

db.t3.micro
2 vCPUs 1 GiB RAM Network: Up to 2,085 Mbps

Storage

Storage type Info

Provisioned IOPS SSD (io2) storage volumes are now available.

General Purpose SSD (gp3)
Performance scales independently from storage

Allocated storage Info

20 GiB

Minimum: 20 GiB. Maximum: 6,144 GiB

Provisioned IOPS Info

3000 IOPS

Baseline IOPS of 3,000 IOPS is included for allocated storage less than 400 GiB.

Storage throughput Info

125 MiBps

Baseline storage throughput of 125 MiBps is included for allocated storage less than 400 GiB.

To provision additional IOPS and throughput, increase the allocated storage to 400 GiB or greater.

▶ **Additional storage configuration**

Connectivity Info

Compute resource

Choose whether to set up a connection to a compute resource for this database. Setting up a connection will automatically change connectivity settings so that the compute resource can connect to this database.

- (●) Don't connect to an EC2 compute resource
  Don't set up a connection to a compute resource for this database. You can manually set up a connection to a compute resource later.
- ( ) Connect to an EC2 compute resource
  Set up a connection to an EC2 compute resource for this database.

Virtual private cloud (VPC) Info

Choose the VPC. The VPC defines the virtual networking environment for this DB instance.

Lab VPC (vpc-0c2bceb3d5961a4b9)
4 Subnets, 2 Availability Zones

Only VPCs with a corresponding DB subnet group are listed.

After a database is created, you can't change its VPC.

DB subnet group Info

Choose the DB subnet group. The DB subnet group defines which subnets and IP ranges the DB instance can use in the VPC that you selected.

db-subnet-group
2 Subnets, 2 Availability Zones

Public access Info

- ( ) Yes
  RDS assigns a public IP address to the database. Amazon EC2 instances and other resources outside of the VPC can connect to your database. Resources inside the VPC can also connect to the database. Choose one or more VPC security groups that specify which resources can connect to the database.
- (●) No
  RDS doesn't assign a public IP address to the database. Only Amazon EC2 instances and other resources inside the VPC can connect to your database. Choose one or more VPC security groups that specify which resources can connect to the database.

VPC security group (firewall) Info

Choose one or more VPC security groups to allow access to your database. Make sure that the security group rules allow the appropriate incoming traffic.

- (●) Choose existing
  Choose existing VPC security groups
- ( ) Create new
  Create new VPC security group

Existing VPC security groups

Choose one or more options

DB Security Group ×

Monitoring

☐ Enable Enhanced Monitoring
Enabling Enhanced Monitoring metrics are useful when you want to see how different processes or threads use the CPU.

▼ Additional configuration

Database options, encryption turned off, backup turned off, backtrack turned off, maintenance, CloudWatch Logs, delete protection turned off.

Database options

Initial database name Info

lab

If you do not specify a database name, Amazon RDS does not create a database.

DB parameter group Info

default.mysql8.0

Option group Info

default:mysql-8-0

Backup

☐ Enable automated backups
Creates a point-in-time snapshot of your database

Encryption

☐ Enable encryption
Choose to encrypt the given instance. Master key IDs and aliases appear in the list after they have been created using the AWS Key Management Service console. Info

Log exports

Select the log types to publish to Amazon CloudWatch Logs

☐ Audit log
☐ Error log
☐ General log
☐ Slow query log

IAM role
The following service-linked role is used for publishing logs to CloudWatch Logs.

RDS service-linked role

Maintenance

Auto minor version upgrade Info

☑ Enable auto minor version upgrade
Enabling auto minor version upgrade will automatically upgrade to new minor versions as they are released. The automatic upgrades occur during the maintenance window for the database.

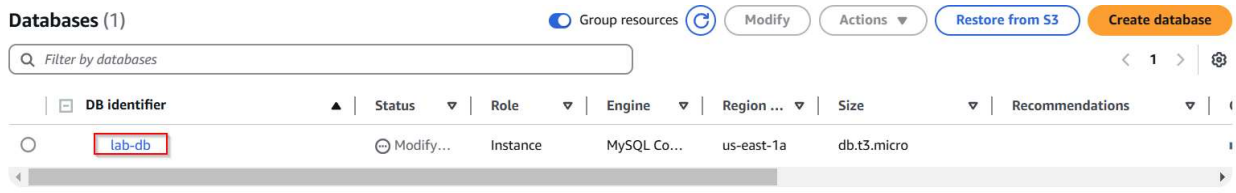
Maintenance window Info
Select the period you want pending modifications or maintenance applied to the database by Amazon RDS.

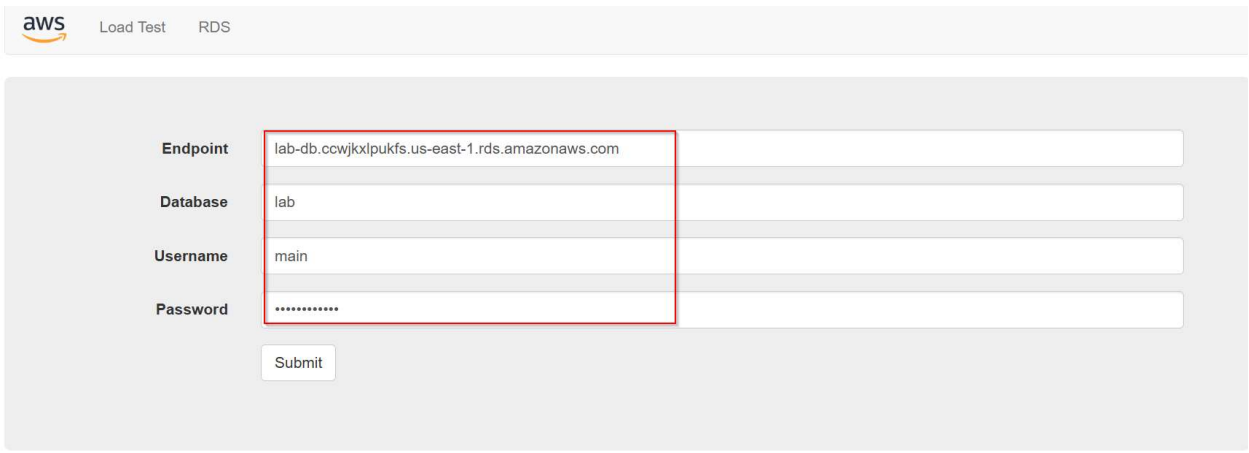
○ Choose a window
◉ No preference

Deletion protection

☐ Enable deletion protection
Protects the database from being deleted accidentally. While this option is enabled, you can't delete the database.

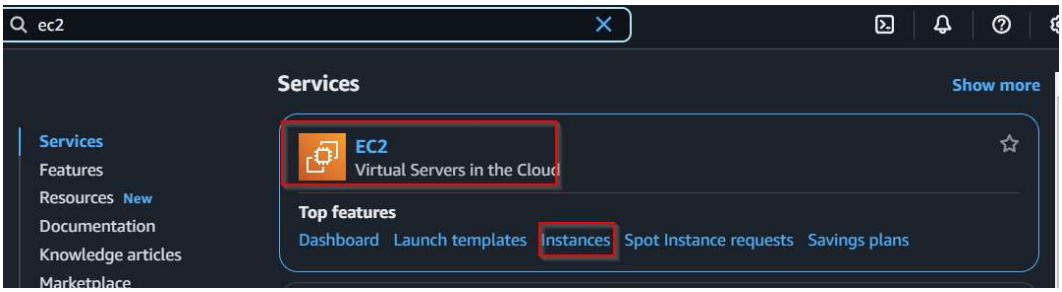
7. Wait until lab-db changes to Modifying or Available. Then, copy the Endpoint field. Access the WebServer IP address, and fill out the info below.

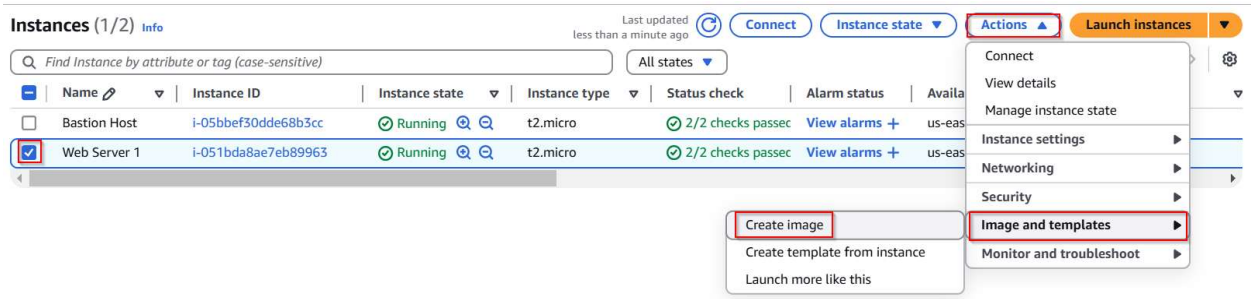




Lab 6

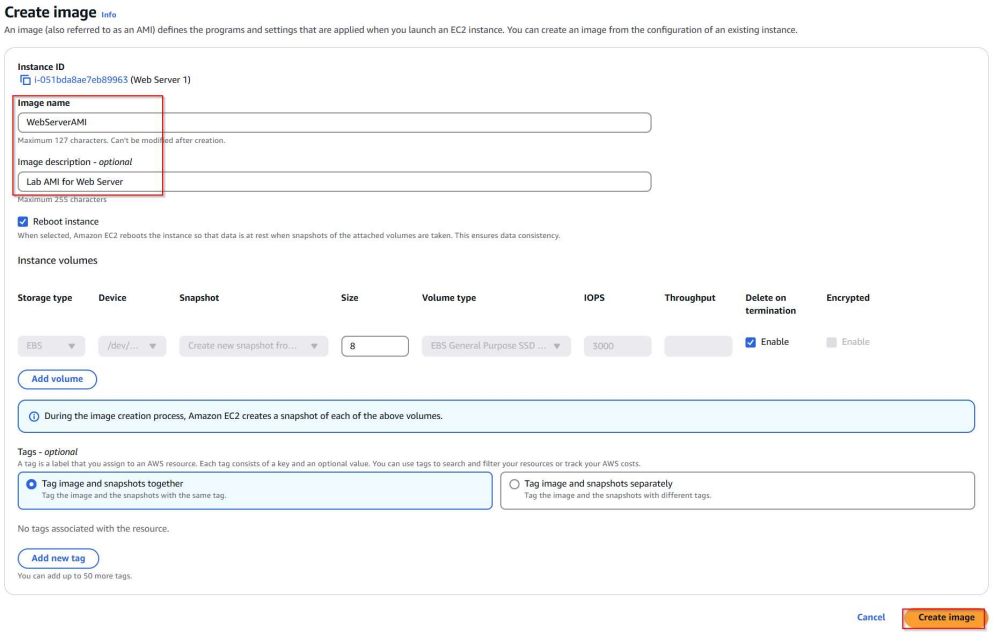
1. Navigate to EC2 > Instances. Wait until Web Server 1 displays 2/2 checks passed. Click Actions > Image and templates > Create image.



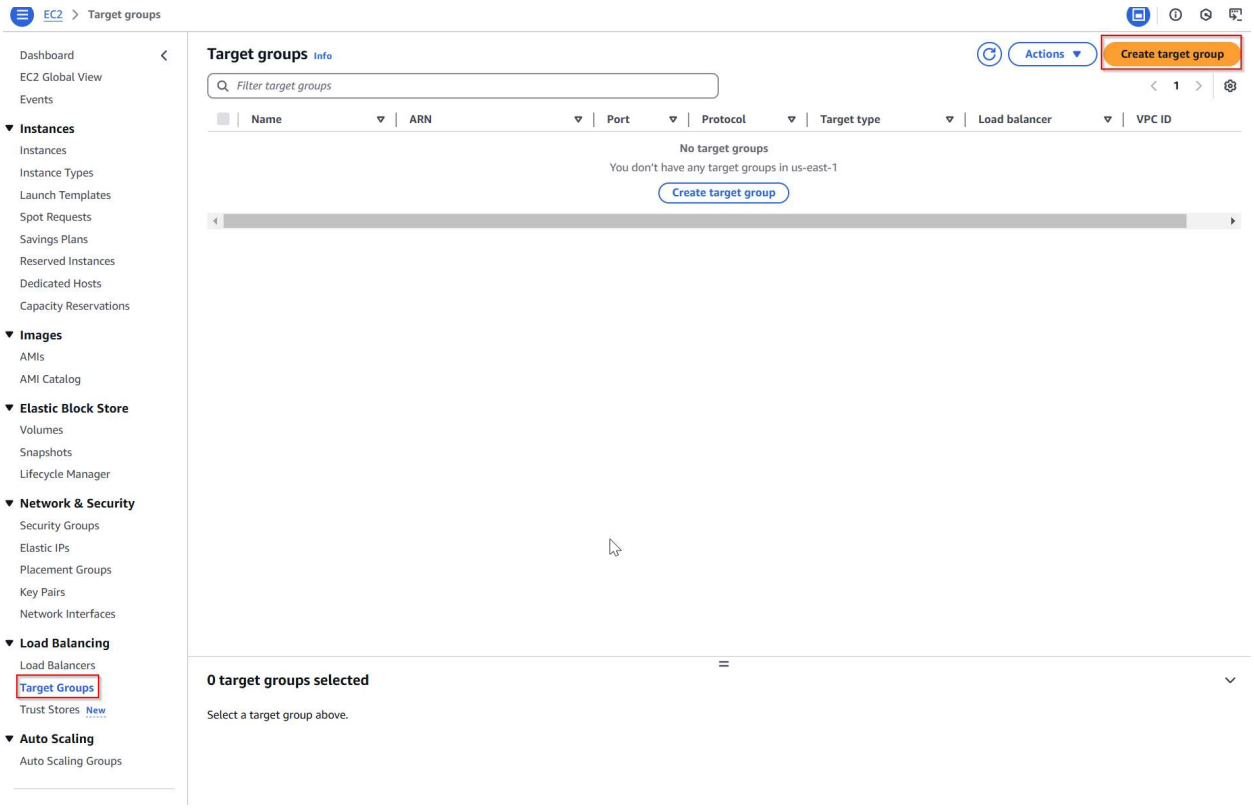


2. Configure:

- Image name: WebServerAMI
- Image description: Lab AMI for Web Server

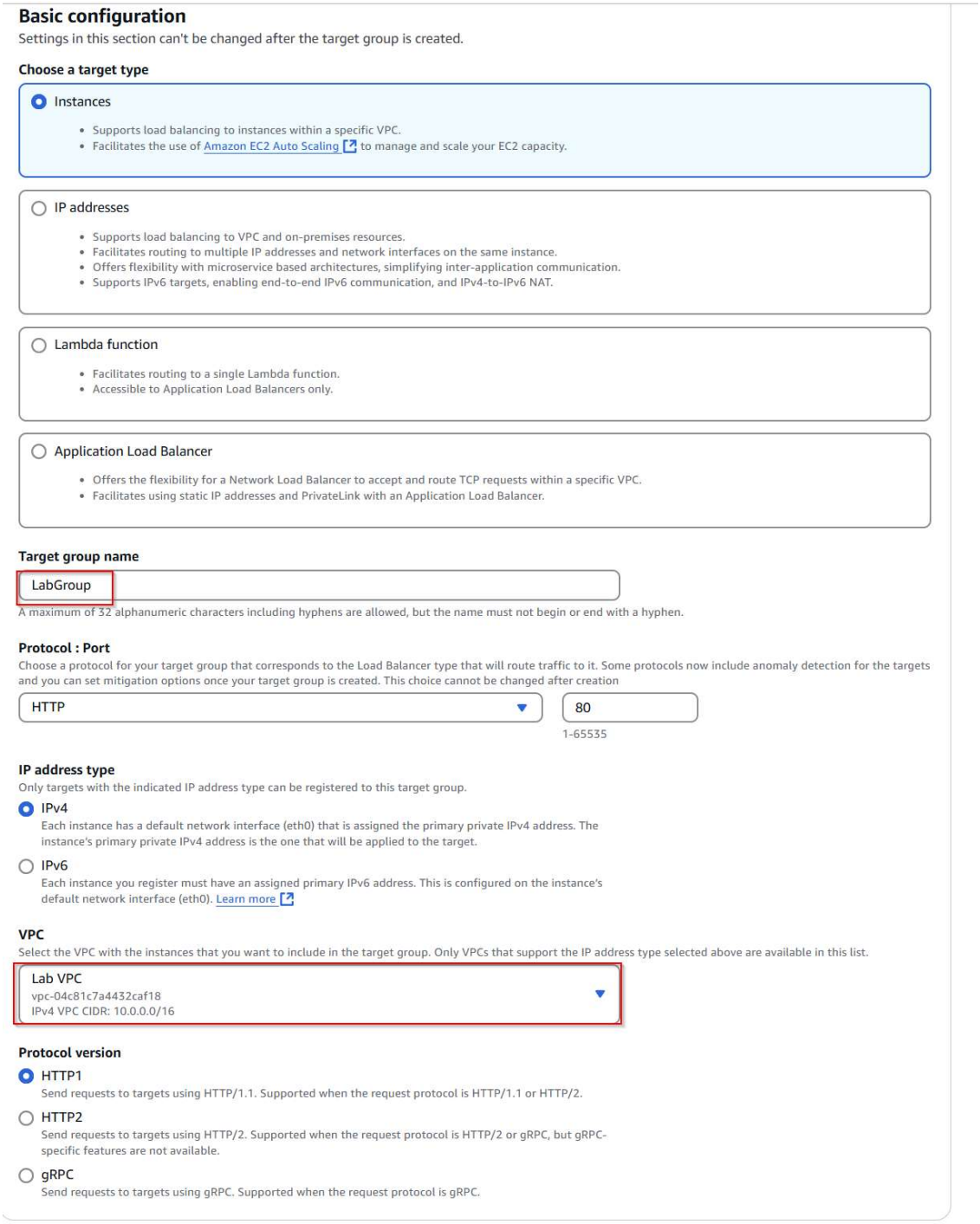


3. Navigate to Target Groups. Create a new target group

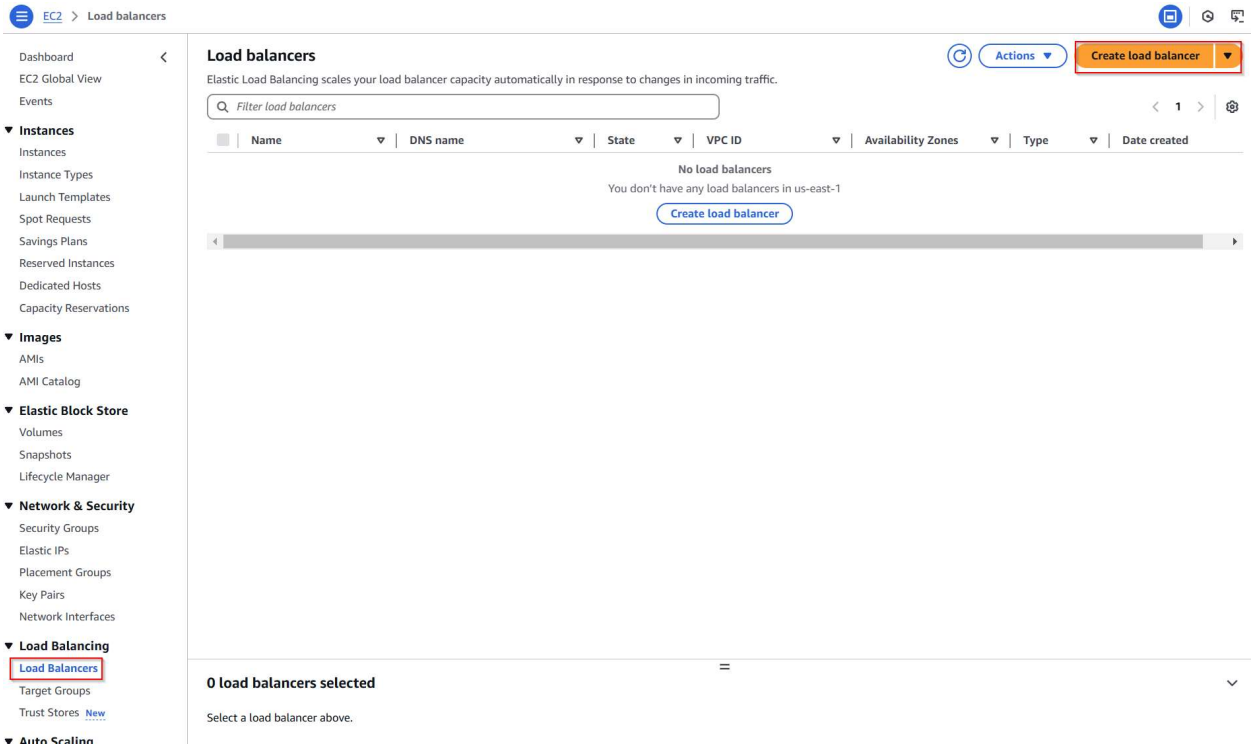


4. Configure:

- Target type: Instances
- Target group name: LabGroup
- VPC: Lab VPC

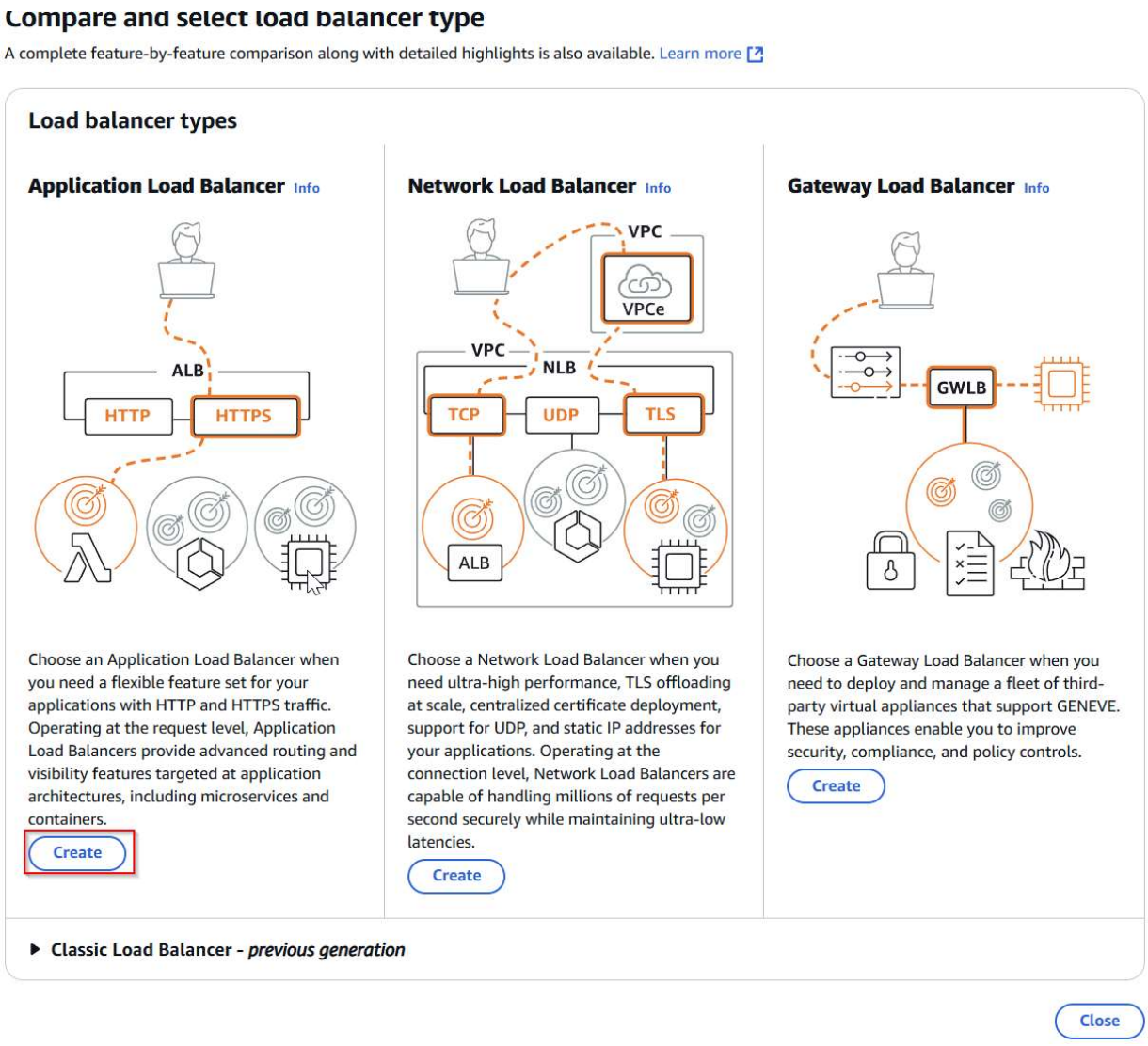


5. Navigate to Load Balances and Create a new load balancer.



6. Configure:

- Load balancer type: Application Load Balancer
- Load Balancer name: LabELB
- VPC: Lab VPC
- Choose the first two displayed Availability Zones. Select Public Subnet 1 for the first and Public Subnet 2 for the second.
- Security group: Web Security Group
- Default action: LabGroup



Create Application Load Balancer Info

The Application Load Balancer distributes incoming HTTP and HTTPS traffic across multiple targets such as Amazon EC2 instances, microservices, and containers, based on re
load balancer receives a connection request, it evaluates the listener rules in priority order to determine which rule to apply, and if applicable, it selects a target from the targ

▶ **How Application Load Balancers work**

Basic configuration

Load balancer name

Name must be unique within your AWS account and can't be changed after the load balancer is created.

LabELB

A maximum of 32 alphanumeric characters including hyphens are allowed, but the name must not begin or end with a hyphen.

Scheme | Info

Scheme can't be changed after the load balancer is created.

- (●) Internet-facing
  - Serves internet-facing traffic.
  - Has public IP addresses.
  - DNS name is publicly resolvable.
  - Requires a public subnet.
- ( ) Internal
  - Serves internal traffic.
  - Has private IP addresses.
  - DNS name is publicly resolvable.
  - Compatible with the **IPv4** and **Dualstack** IP address types.

Load balancer IP address type | Info

Select the front-end IP address type to assign to the load balancer. The VPC and subnets mapped to this load balancer must include the selected IP address types. Public IPv4 addresses have an add

- (●) IPv4
  Includes only IPv4 addresses.
- ( ) Dualstack
  Includes IPv4 and IPv6 addresses.
- ( ) Dualstack without public IPv4
  Includes a public IPv6 address, and private IPv4 and IPv6 addresses. Compatible with **internet-facing** load balancers only.

Network mapping Info

The load balancer routes traffic to targets in the selected subnets, and in accordance with your IP address settings.

VPC | Info

The load balancer will exist and scale within the selected VPC. The selected VPC is also where the load balancer targets must be hosted unless routing to Lambda or on-premises targets, or if using
VPC for your targets, view target groups. For a new VPC, create a VPC.

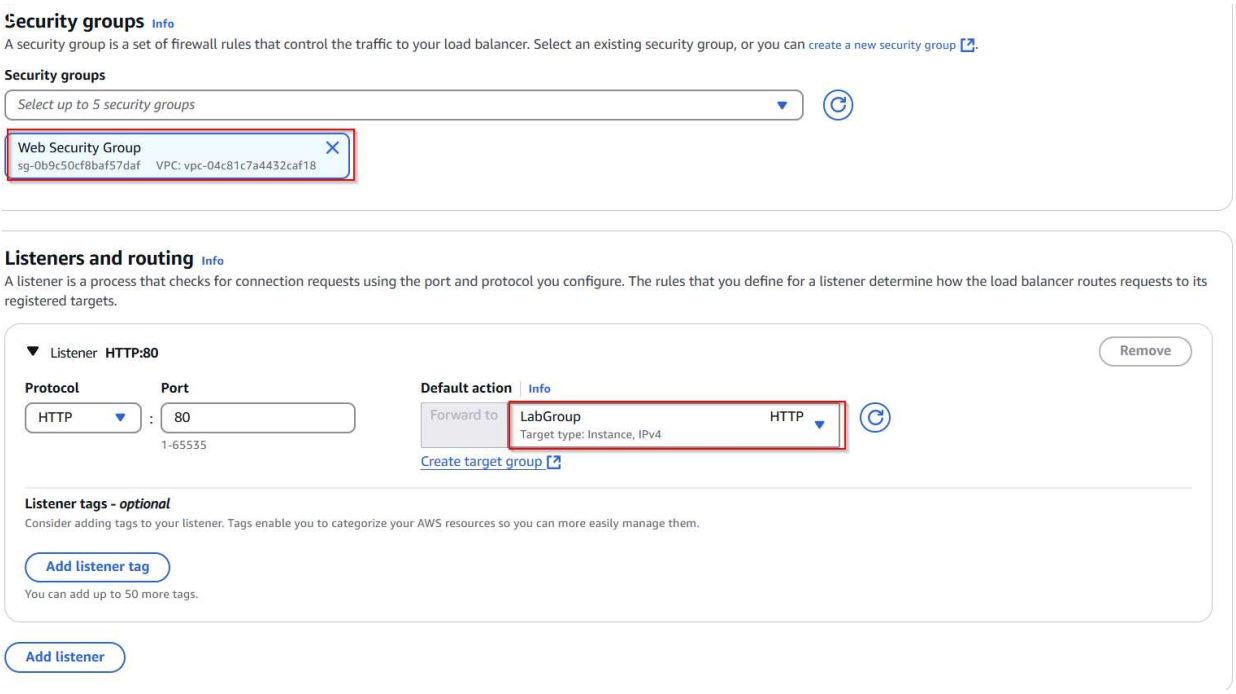
Lab VPC
vpc-04c81c7a4432caf18
IPv4 VPC CIDR: 10.0.0.0/16

Mappings | Info

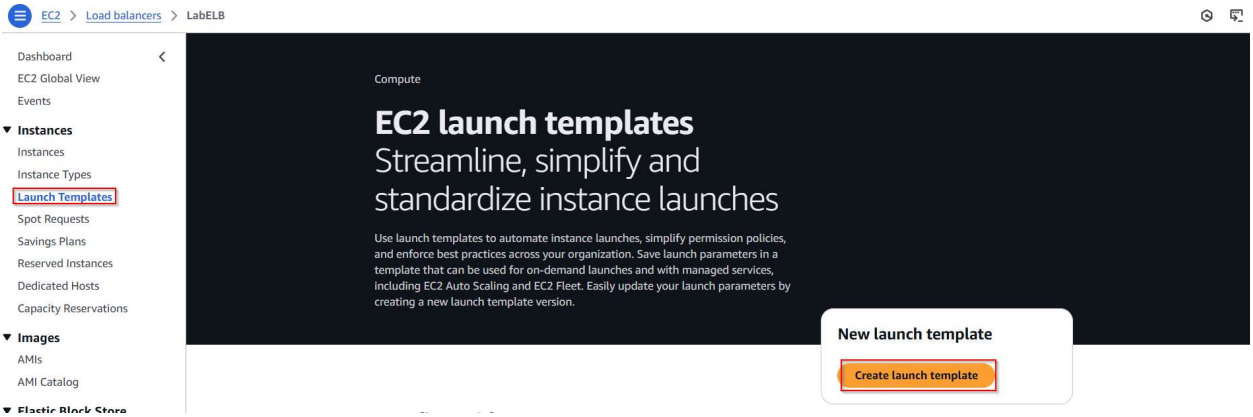
Select at least two Availability Zones and one subnet per zone. The load balancer routes traffic to targets in these Availability Zones only. Availability Zones that are not supported by the load balan
available for selection.

Availability Zones

- [x] **us-east-1a (use1-az6)**
  Subnet
  subnet-081b2e826390317e0 — Public Subnet 1
  IPv4 subnet CIDR: 10.0.0.0/24
  IPv4 address
  Assigned by AWS
- [x] **us-east-1b (use1-az1)**
  Subnet
  subnet-0104cad27fdc0763c — Public Subnet 2
  IPv4 subnet CIDR: 10.0.2.0/24
  IPv4 address
  Assigned by AWS



7. Navigate to Launch Templates and chick Create launch template.



8. Configure:

- Launch template name: LabConfig
- Check *Provide guidance to help me set up a template that I can use with EC2 Auto Scaling*.
- Amazon Machine Image: Web Server AMI
- Instance type: t2.micro
- Key pair name: vockey
- Firewall: Select existing security group
- Security group: Web Security Group
- Enable Detailed CloudWatch monitoring

Create launch template

Creating a launch template allows you to create a saved instance configuration that can be reused, shared and launched at a later time. Templates can have multiple versions.

Launch template name and description

Launch template name - *required*

LabConfig

Must be unique to this account. Max 128 chars. No spaces or special characters like '&', '*', '@'.

Template version description

A prod webserver for MyApp

Max 255 chars

Auto Scaling guidance | Info

Select this if you intend to use this template with EC2 Auto Scaling

☑ Provide guidance to help me set up a template that I can use with EC2 Auto Scaling

▶ **Template tags**

▶ **Source template**

Launch template contents

Specify the details of your launch template below. Leaving a field blank will result in the field not being included in the launch template.

▼ Application and OS Images (Amazon Machine Image) - required Info

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Search our full catalog including 1000s of application and OS images

Recents | My AMIs | Quick Start

◉ Owned by me ○ Shared with me

Browse more AMIs

Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

WebServerAMI
ami-0332f9d12c89e5cea
2025-01-13T18:56:48.000Z Virtualization: hvm ENA enabled: true Root device type: ebs Boot mode: uefi-preferred

Description

Lab AMI for Web Server

Architecture

x86_64

AMI ID

ami-0332f9d12c89e5cea

▼ Instance type Info | Get advice

Advanced

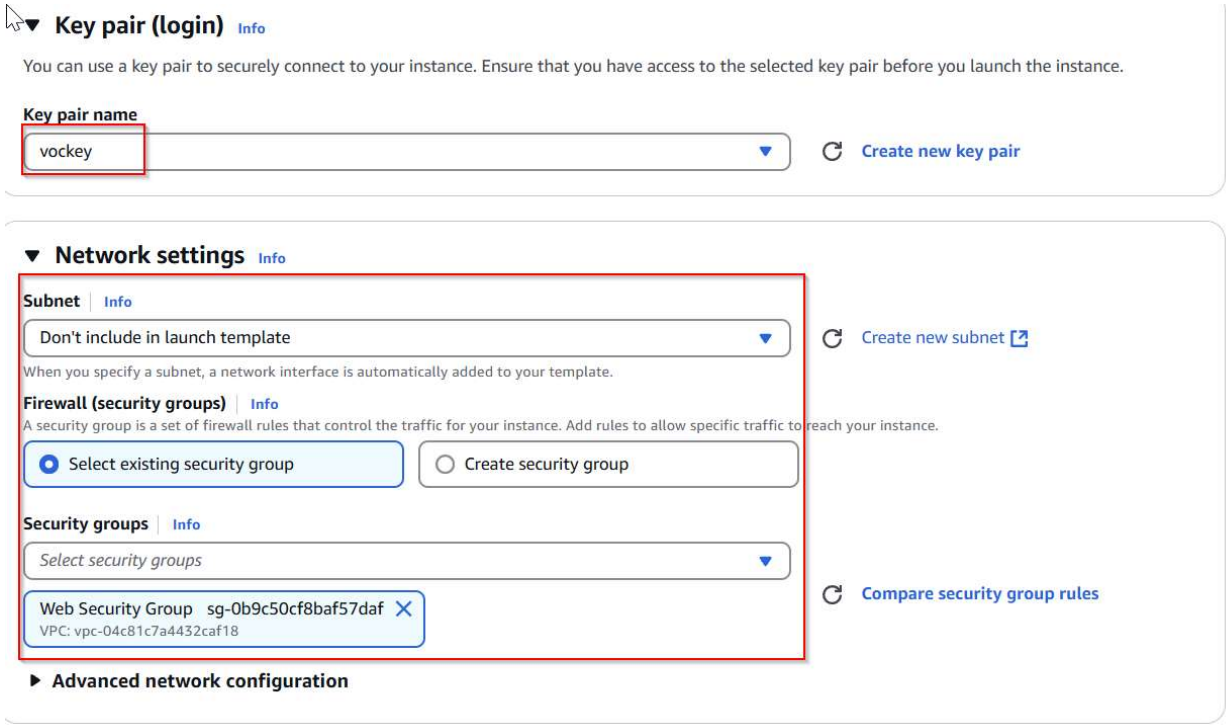
Instance type

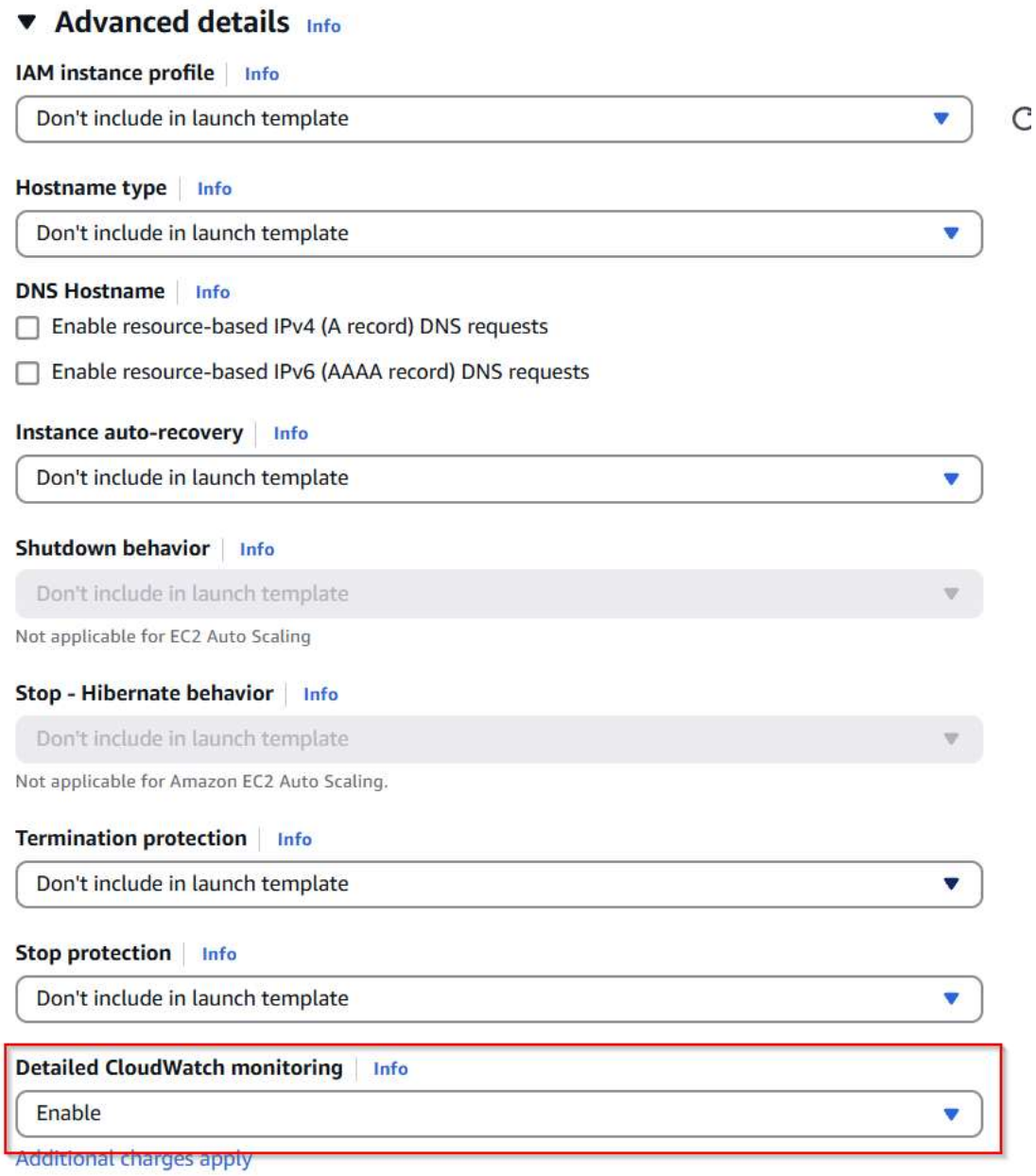
t2.micro Free tier eligible
Family: t2 1 vCPU 1 GiB Memory Current generation: true
On-Demand Windows base pricing: 0.0162 USD per Hour
On-Demand Ubuntu Pro base pricing: 0.0134 USD per Hour On-Demand SUSE base pricing: 0.0116 USD per Hour
On-Demand RHEL base pricing: 0.026 USD per Hour On-Demand Linux base pricing: 0.0116 USD per Hour

All generations

Compare instance types

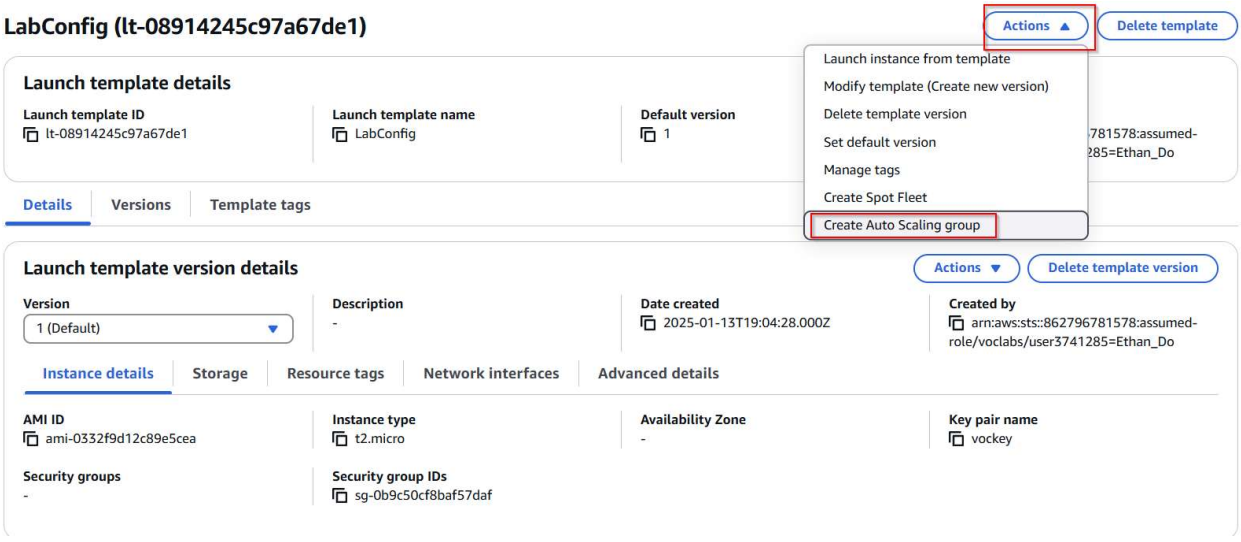
Additional costs apply for AMIs with pre-installed software


Key pair (login) Info
You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.
Key pair name
vockey
Create new key pair
Network settings Info
Subnet Info
Don't include in launch template
Create new subnet
When you specify a subnet, a network interface is automatically added to your template.
Firewall (security groups) Info
A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.
Select existing security group
Create security group
Security groups Info
Select security groups
Web Security Group sg-0b9c50cf8baf57daf
VPC: vpc-04c81c7a4432caf18
Compare security group rules
Advanced network configuration

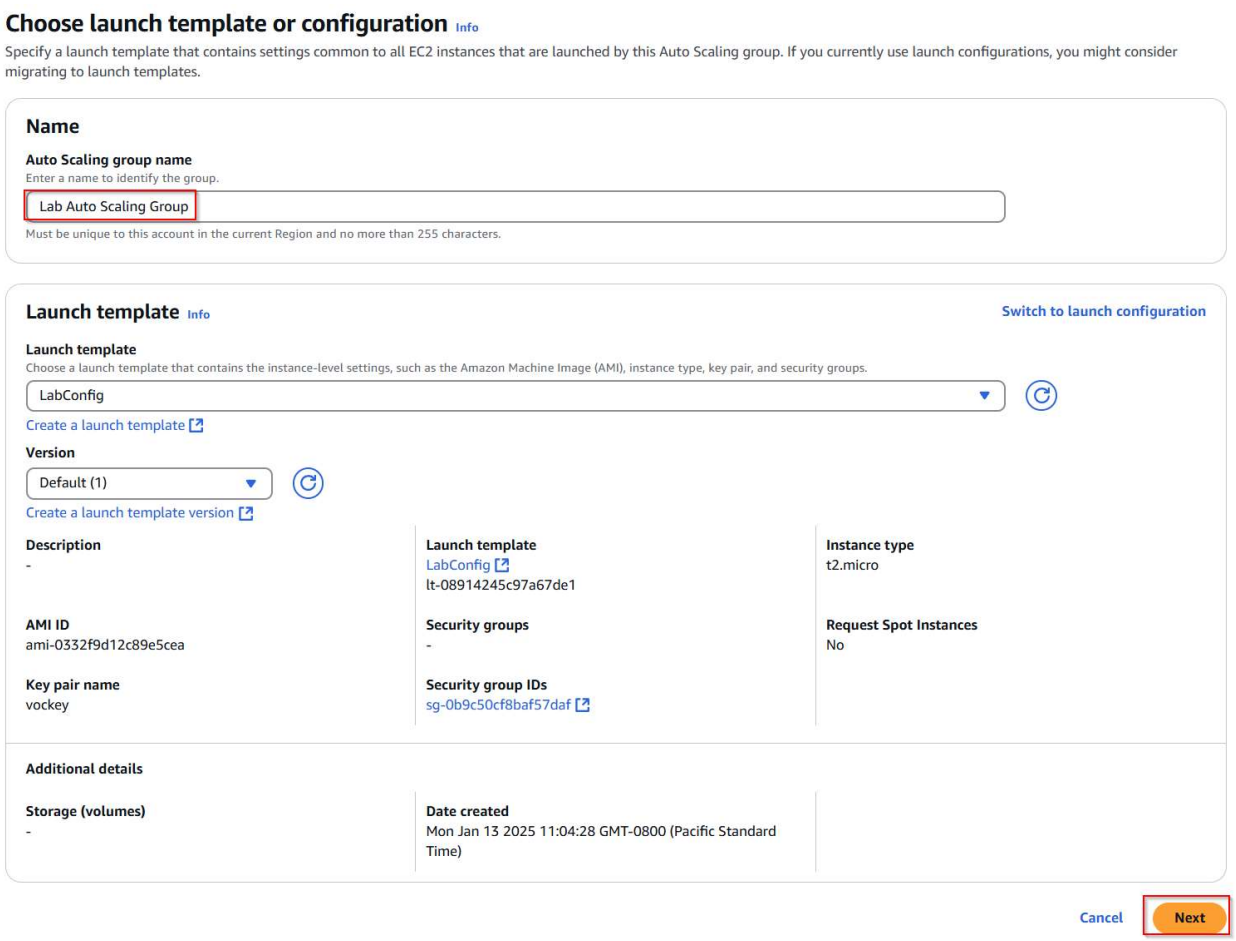


9. In the Success dialog, select the LabConfig launch template.

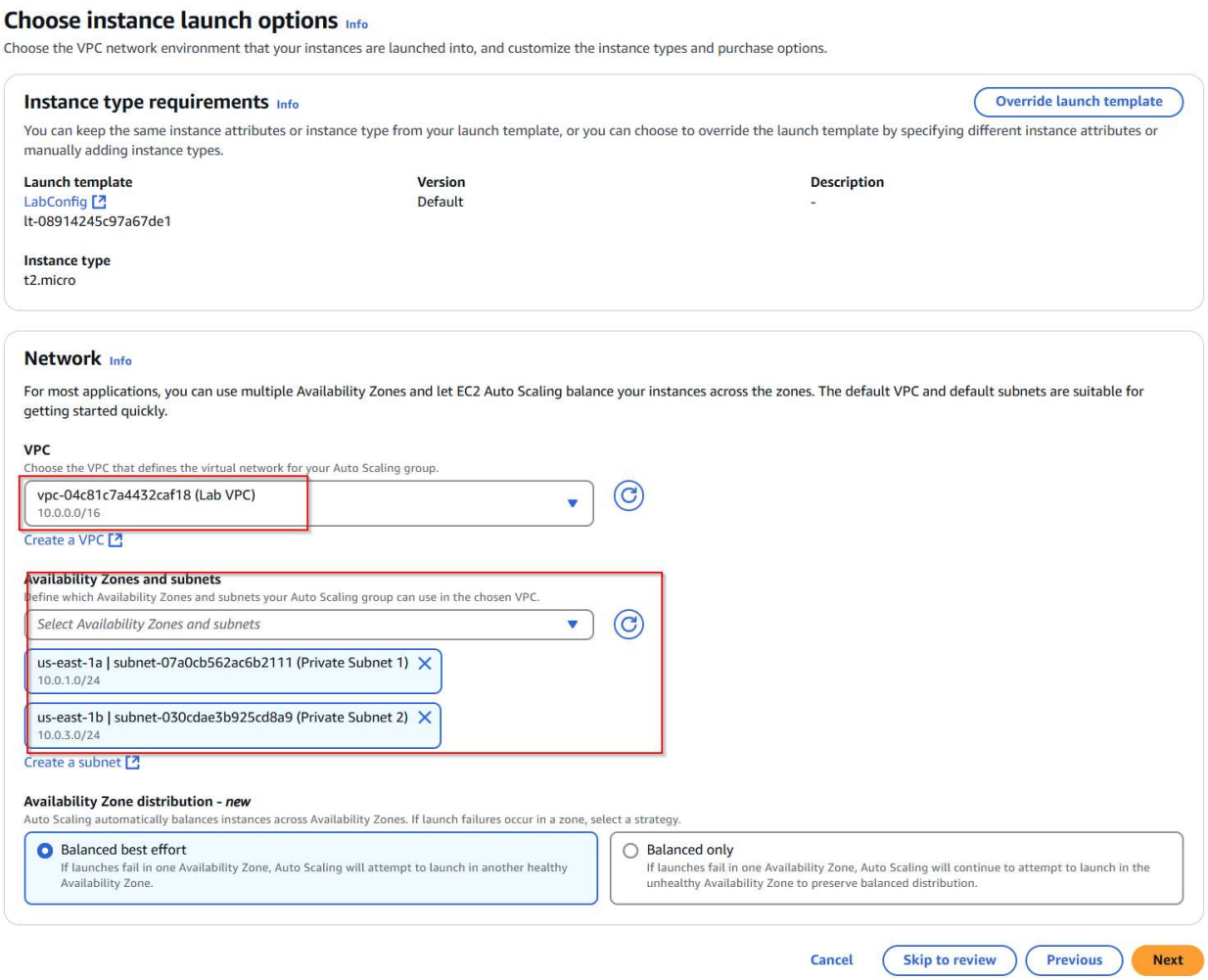
10. Click Actions > Create Auto Scaling group



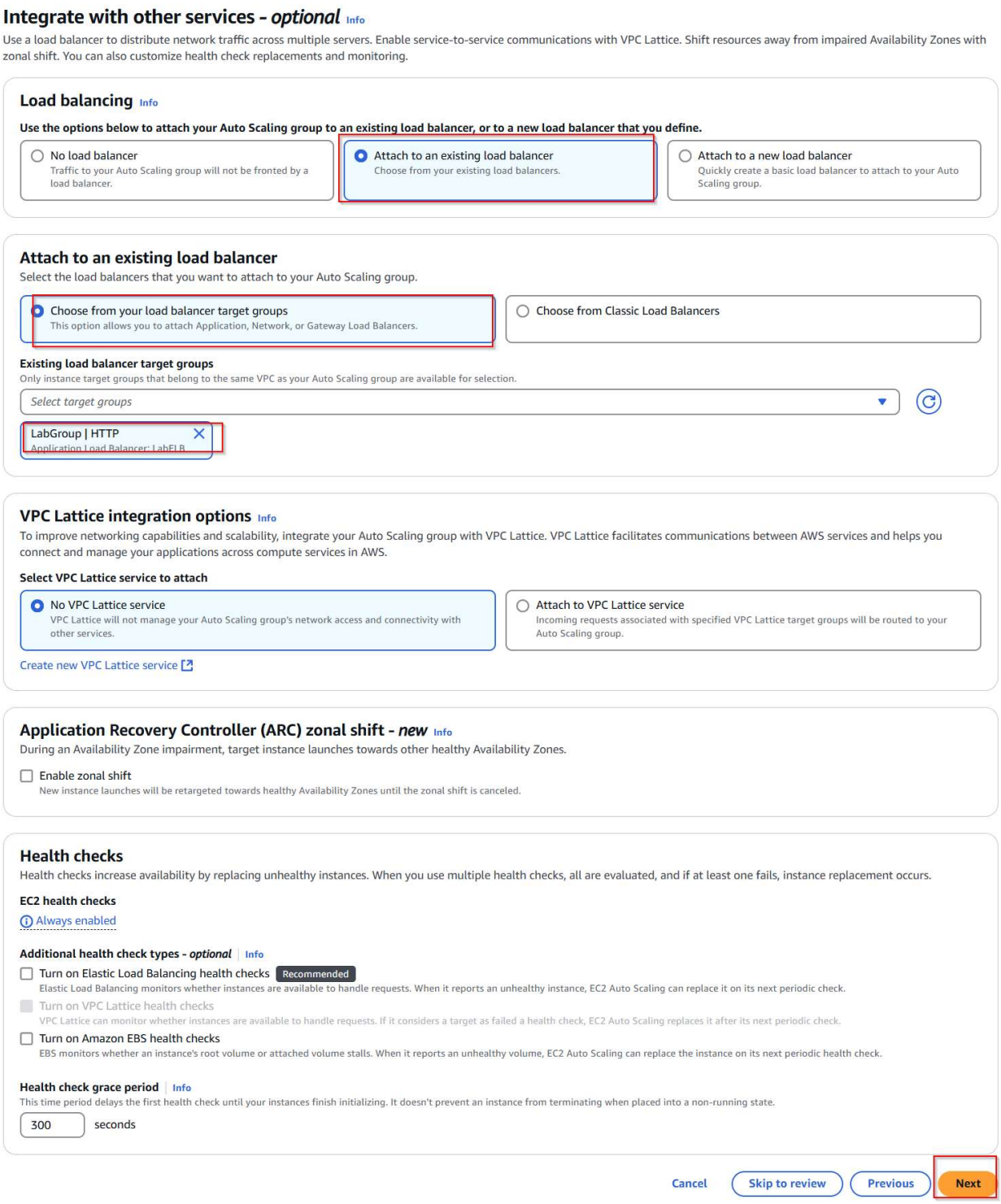
11. Configure name: Lab Auto Scaling Group.



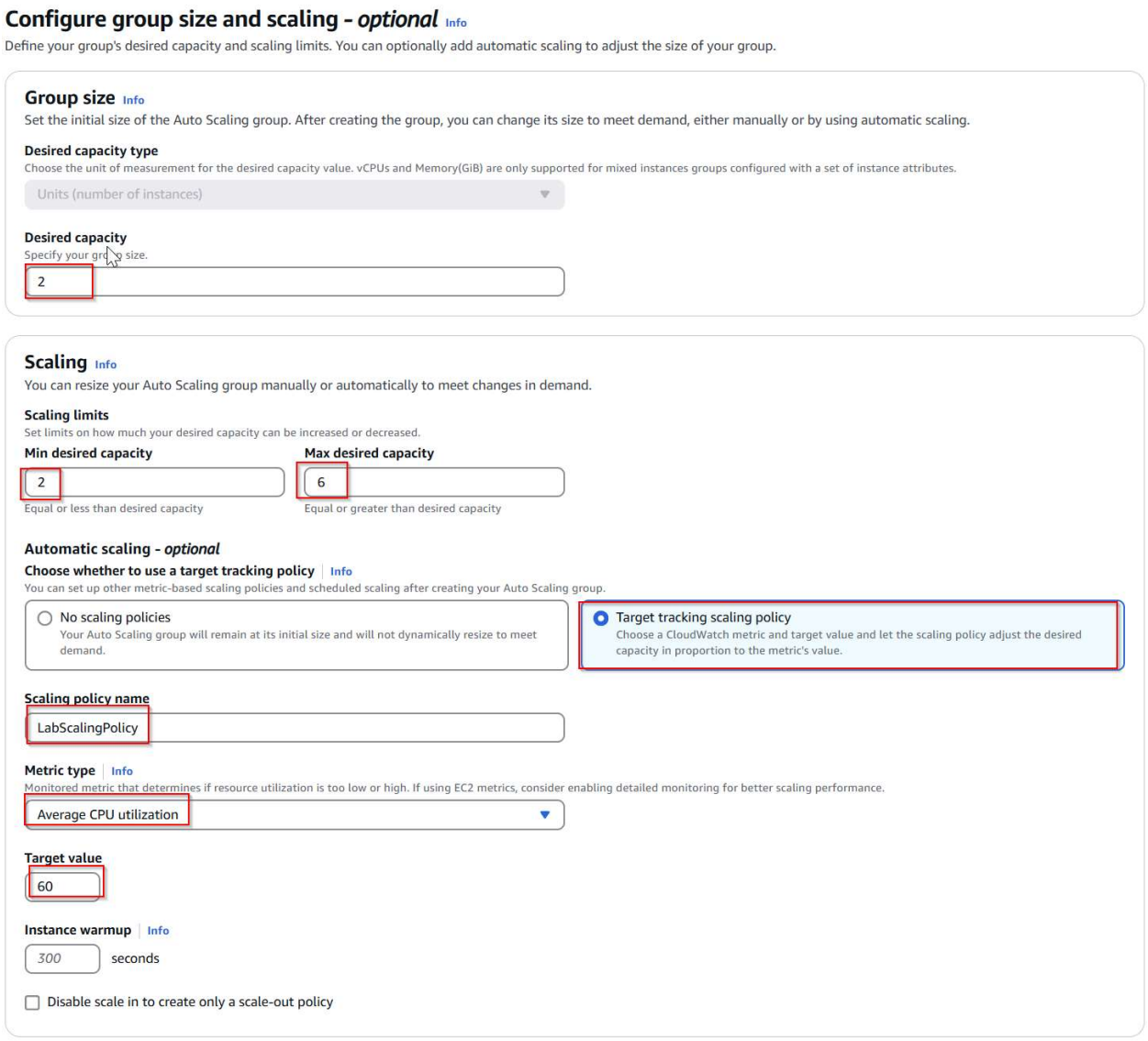
12. Configure VPC: Lab VPC, Subnets: Private Subnet 1 and Private Subnet 2.



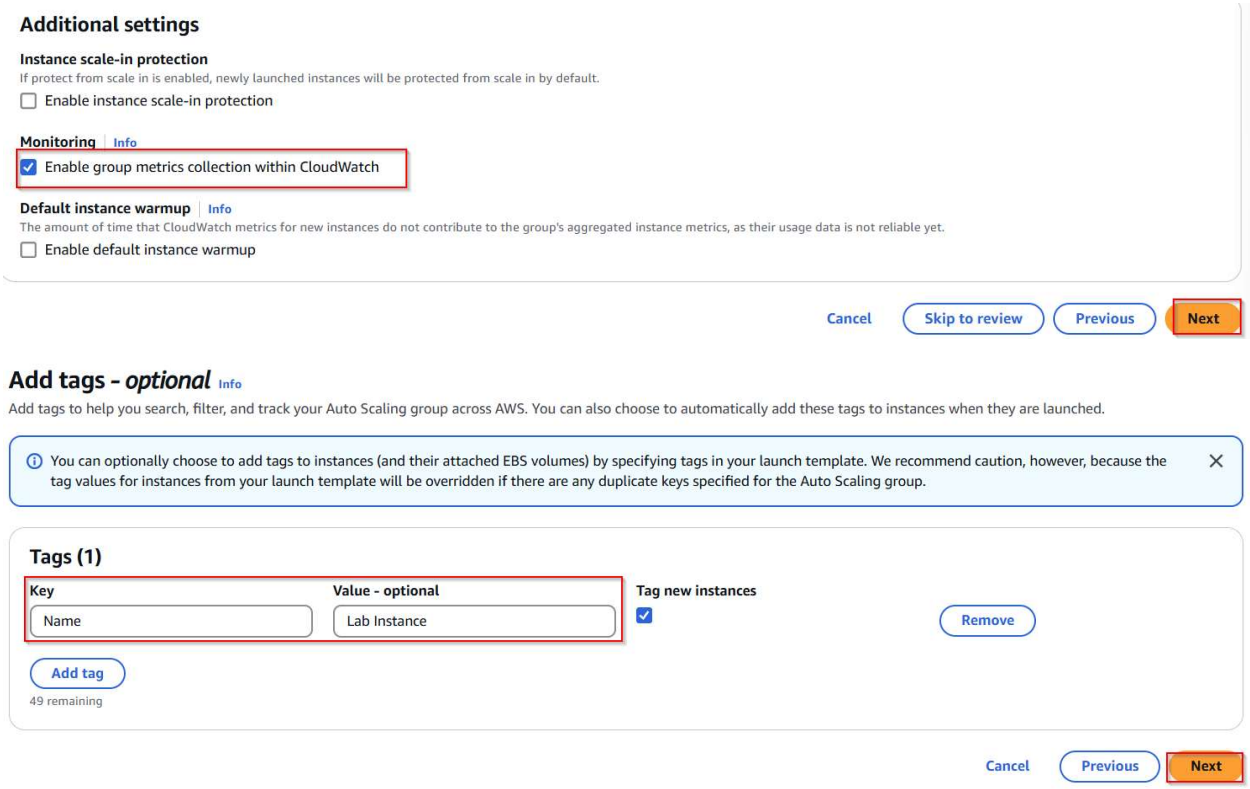
13. Configure as shown.



14. Configure as shown.



15. Configure as shown.



Problems

There were several web applications in these labs that would not work when you clicked on them; instead, you have to change the address to only use http, rather than https.

Conclusion

I successfully completed Labs 4-6 of the Amazon Web Services Academy Course. In these labs, I gained experience AWS Elastic Block Store (EBS), built a database server, and configured AWS EC2 Auto Scaling and Load Balancing.

Access Point

Purpose

The purpose of this lab is to set up an access point with three SSIDs: one with no authentication, one with WPA2 PSK, and one with WPA2 Enterprise through a RADIUS server.

Background Information

Most Wi-Fi networks use a wireless access point(s) to allow end devices to connect to the network. Access points typically connect directly to a local area network (LAN). Access points can be standalone or function through an access point controller, which provides centralized management in the case of multiple access points in order to improve efficiency and reliability.

Access points allow end devices to connect to a network through Service Set Identifiers (SSIDs), which can have a variety of authentication methods. The most basic and least secure is open authentication, which allows end devices to send an authentication to an access point and be accepted without question. Credentials are not needed, allowing anyone to connect to the network.

Other types of authentication are defined through the Wi-Fi Protected Access 2 (WPA2) protocol. The two types of authentication used within this lab are WPA2 Pre-Shared Key (WPA2 PSK) and WPA2 Enterprise.

WPA2 PSK uses a password that end devices must use in their authentication request to the network. Considered more secure than other authentication methods such as Wired Equivalent Privacy (WEP), it is one of the most common security protocols used today.

WPA2 Enterprise uses both unique usernames and passwords that end devices must use in their authentication request. WPA2 Enterprise requires the usage of a RADIUS server, which provides centralized authentication, authorization, and accounting for networks. WPA2 Enterprise also allows users to be dynamically put into VLANs.

RADIUS servers must have their own IP address and secret password set. Access points looking to use a RADIUS server for their authentication services must have both of these pieces of information in order to successfully authenticate. Since the RADIUS server requires its own secret password, it reduces the risk of data breaches.

Access points are able to broadcast in two different frequencies: 2.4GHz and 5GHz. 2.4GHz normally provides better long range capabilities and compatibility with older devices, while 5GHz provides faster speeds and is less prone to interference from other networks and devices. When putting multiple networks on the same radio, the radio

must be set to Multiple BSSID (Basic Set Service Identifier), while a single network on a radio can be set to Single BSSID.

Lab Summary

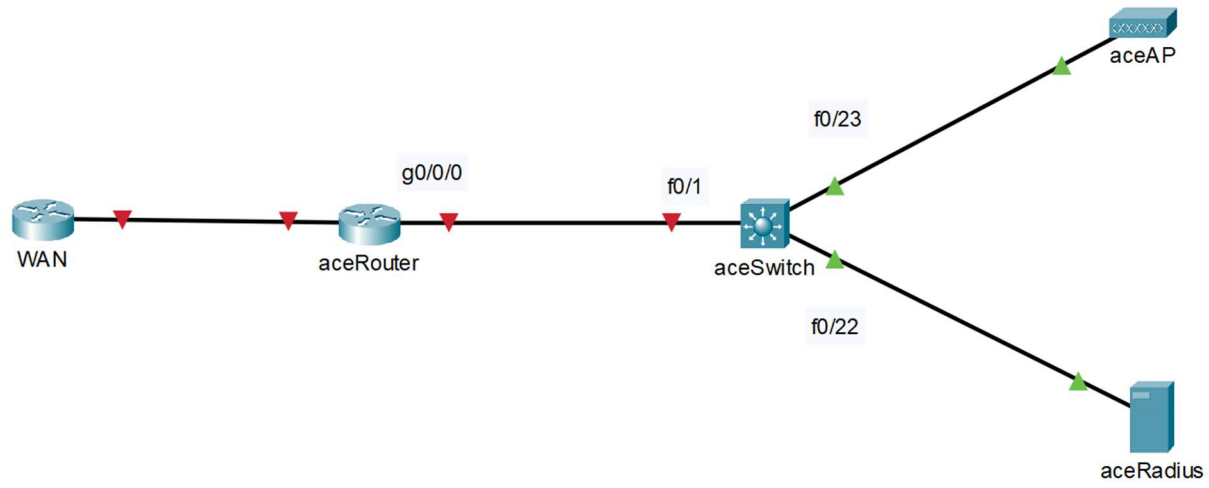
In this lab, we set up an Access Point to have three SSIDs. One has no authentication, letting anyone connect to it. One uses WPA2 PSK, requiring the user to have a password to access the network. One uses WPA2 Enterprise through RADIUS, requiring the user to have both a username and password.

A router is set up to perform DHCP and to allow traffic to go to and from the network.

A switch is set up to provide inter-VLAN routing between each of the different SSID's and the internet.

A RADIUS server is set up to provide authentication for the WPA2 Enterprise SSID.

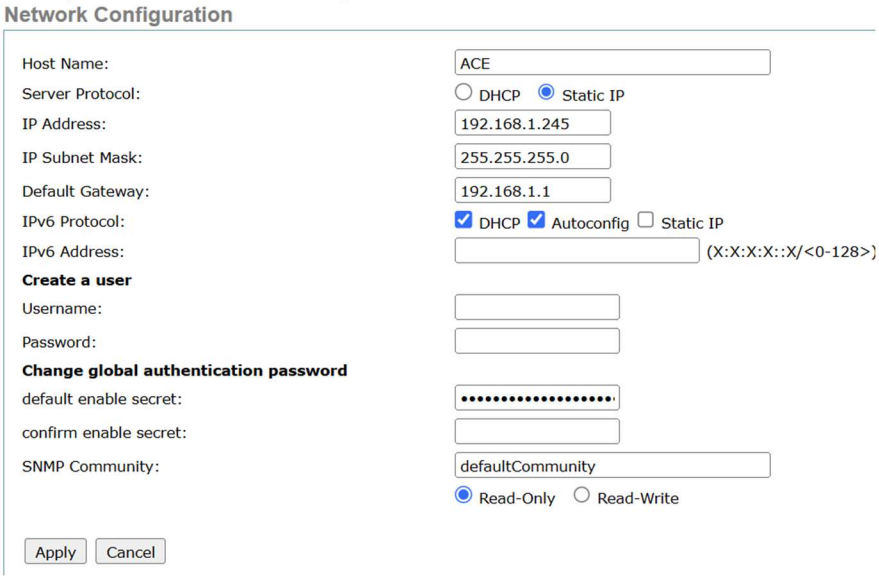
Network Diagram



Configurations

Access Point Setup

1. Connect the access point to power. Console into the access point. If the password is unknown, you will need to power cycle the access point. Once you gain access to the console, check the running configuration with `show run` and check what IP address is set up the BVI1 interface. This IP address will be the one used to access the access point's GUI.
2. Enter the IP address into a web browser. Ensure that you are using http, not https. The default will be `http://192.168.1.245`. Login using the admin credentials.
3. Setup the network configuration as follows:



Router Setup

1. Enter the following commands:

```
ip dhcp excluded-address 192.168.1.20
ip dhcp excluded-address 192.168.1.245
interface GigabitEthernet0/0/1
 ip address dhcp
 ip nat outside
ip nat inside source list 1 interface GigabitEthernet0/0/1
overload
access-list 1 permit 192.168.1.0 0.0.0.255
```

Switch Setup

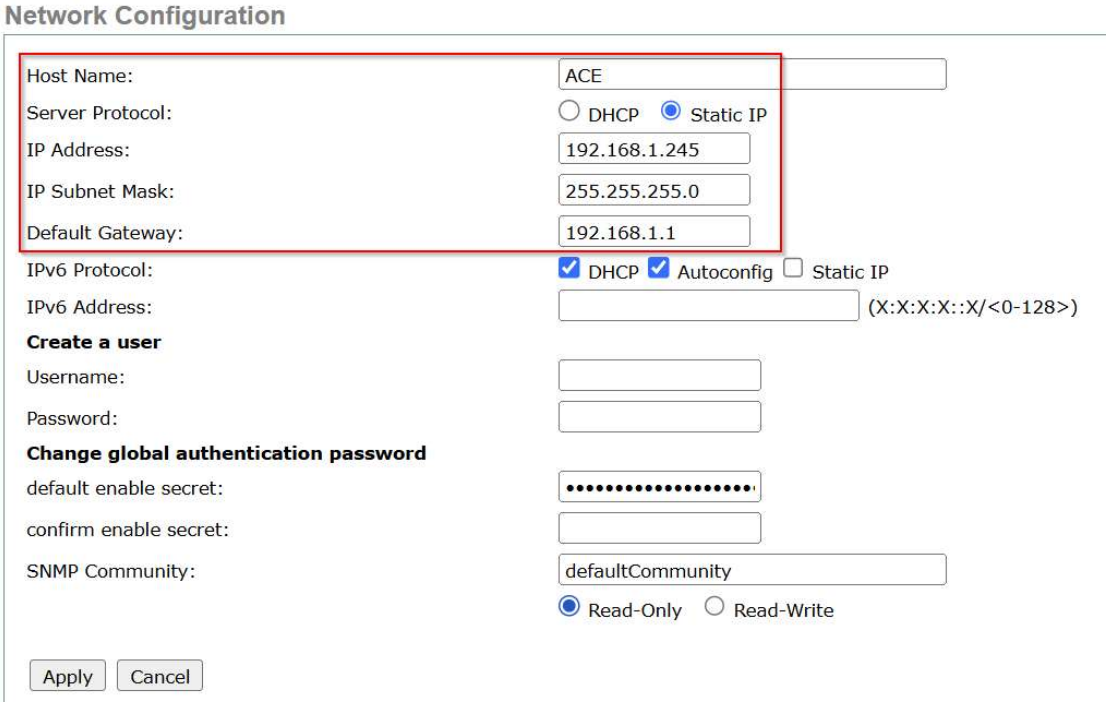
1. Enter the following commands:

```
interface FastEthernet0/1
 switchport trunk encapsulation dot1q
```

```
 switchport mode trunk
 spanning-tree portfast trunk
interface FastEthernet0/2
 switchport mode access
interface FastEthernet0/22
 switchport trunk encapsulation dot1q
 switchport mode trunk
 spanning-tree portfast trunk
interface FastEthernet0/23
 switchport trunk encapsulation dot1q
 switchport mode trunk
 spanning-tree portfast trunk
interface Vlan1
 ip address 192.168.1.2 255.255.255.0
```

Open Authentication SSID Configuration

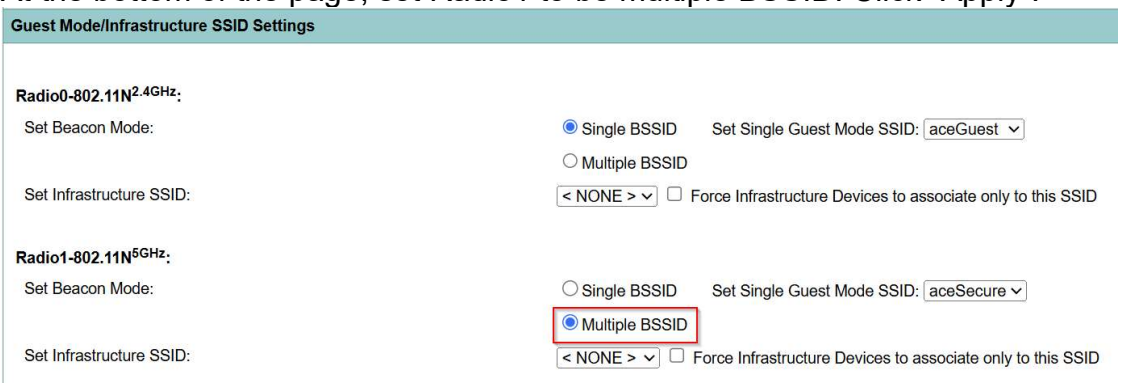
1. In the access point GUI, navigate to the express set-up page. The location will differ with different versions of the GUI, but should be located within the initial start screen.
2. Configure the SSID as shown.



3. Navigate to Security > SSID Manager. Check that for the SSID, the settings are correct. The check box for “Guest mode” must be checked in order for the SSID

to be broadcasted. Click “Apply”.

4. At the bottom of the page, set Radio1 to be multiple BSSID. Click “Apply”.



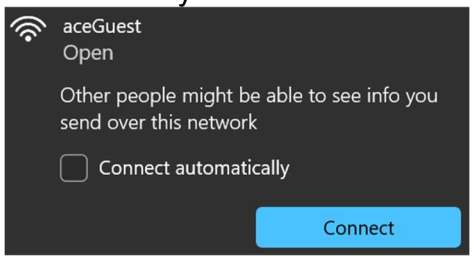
5. In the router, enter the following commands:

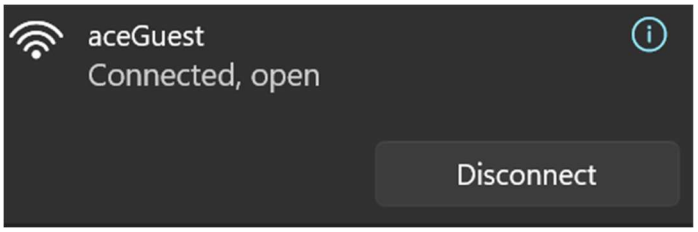
```
ip dhcp excluded-address 192.168.10.1 192.168.20.5
ip dhcp pool GUEST
 network 192.168.10.0 255.255.255.0
 dns-server 8.8.8.8
 default-router 192.168.1.1
interface GigabitEthernet0/0/0.10
 encapsulation dot1Q 10
 ip address 192.168.10.1 255.255.255.0
 ip nat inside
access-list 1 permit 192.168.10.0 0.0.0.255
```

6. In the switch, enter the following commands:

```
vlan 10
 name GUEST
```

Ensure that you are able to see and connect to your SSID.

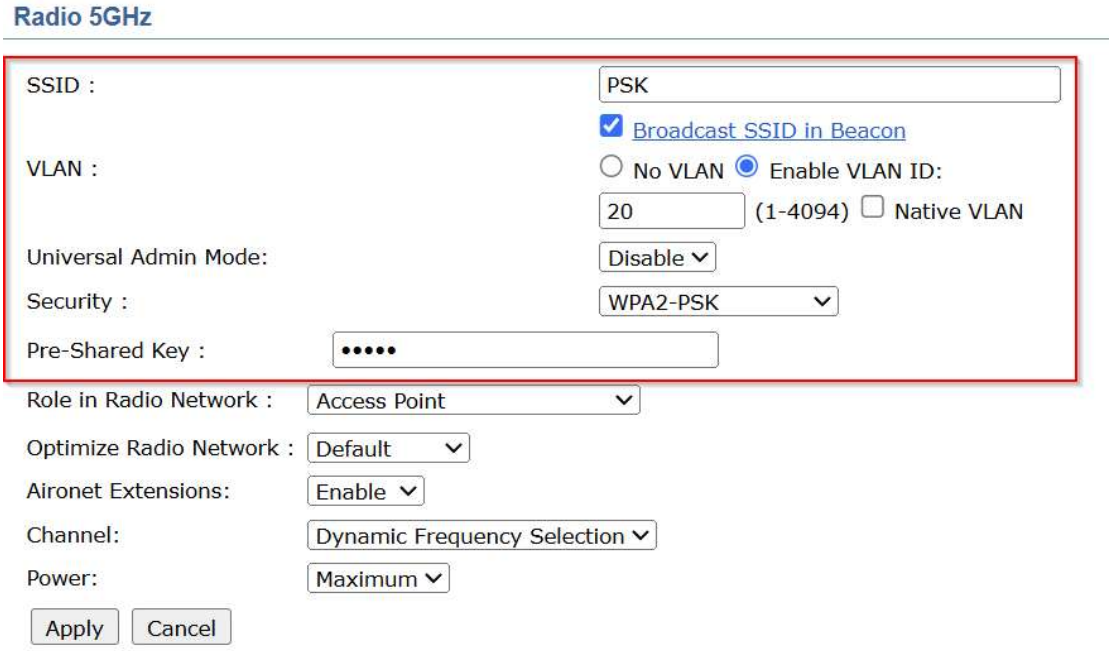




WPA2 PSK SSID Configuration

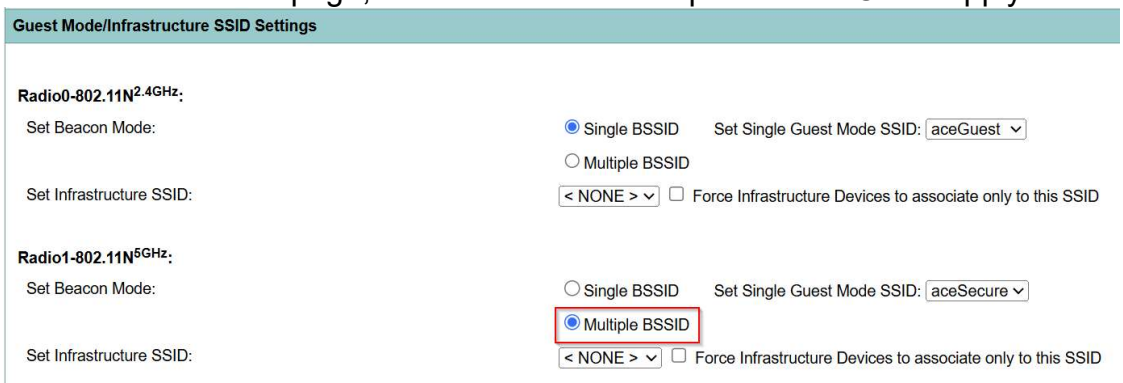
1. In the access point GUI, navigate to the express set-up page. The location will differ with different versions of the GUI, but should be located within the initial start screen.

2. Configure the SSID as shown.



3. Navigate to Security > SSID Manager. Check that for the SSID, the settings are correct. The check box for “Guest mode” must be checked in order for the SSID to be broadcasted. Click “Apply”.

4. At the bottom of the page, set Radio1 to be multiple BSSID. Click “Apply”.



5. In the router, enter the following commands:

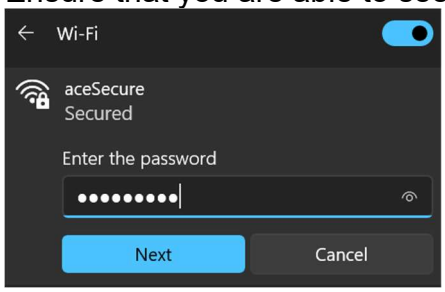
```
ip dhcp excluded-address 192.168.20.1 192.168.20.5
ip dhcp pool SECURE
 network 192.168.20.0 255.255.255.0
 dns-server 8.8.8.8
 default-router 192.168.1.1
interface GigabitEthernet0/0/0.20
```

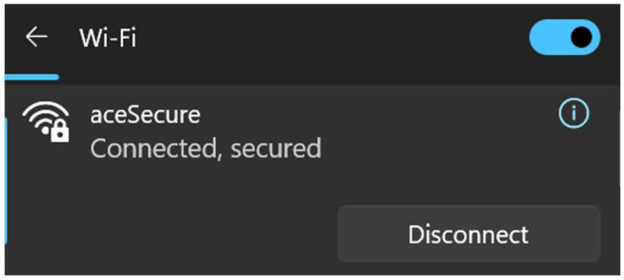
```
 encapsulation dot1Q 20
 ip address 192.168.20.1 255.255.255.0
 ip nat inside
access-list 1 permit 192.168.20.0 0.0.0.255
```

6. In the switch, enter the following commands:

```
vlan 20
 name PSK
```

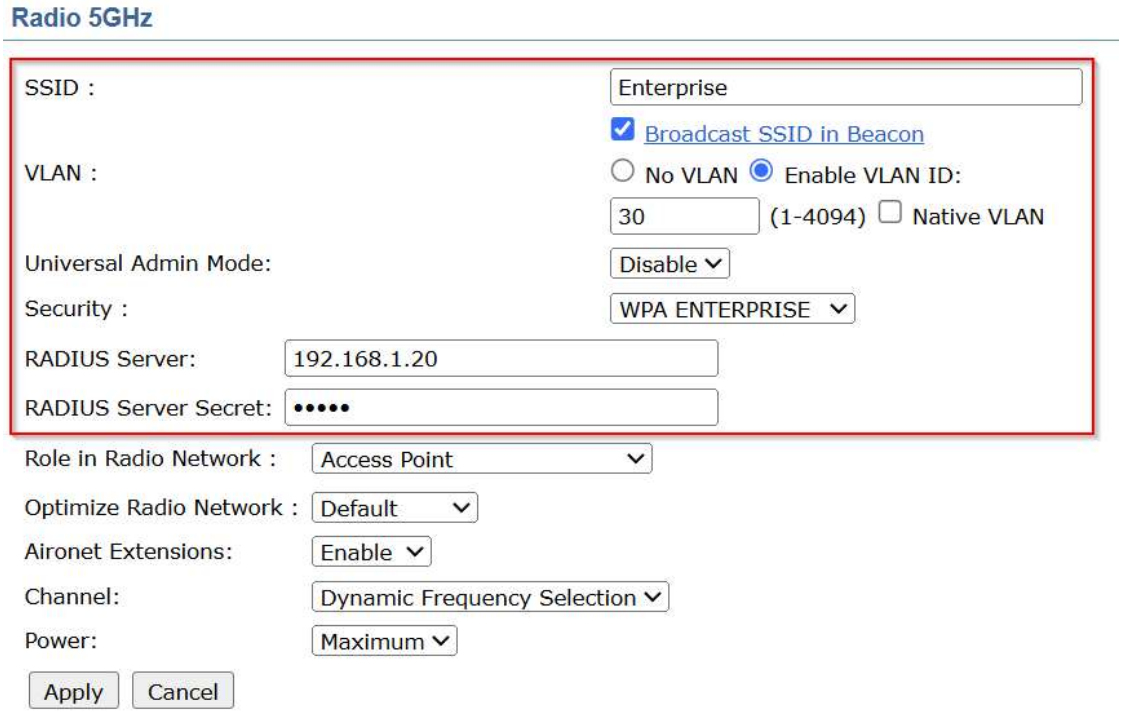
7. Ensure that you are able to see and connect to your SSID.





WPA2 Enterprise SSID Configuration

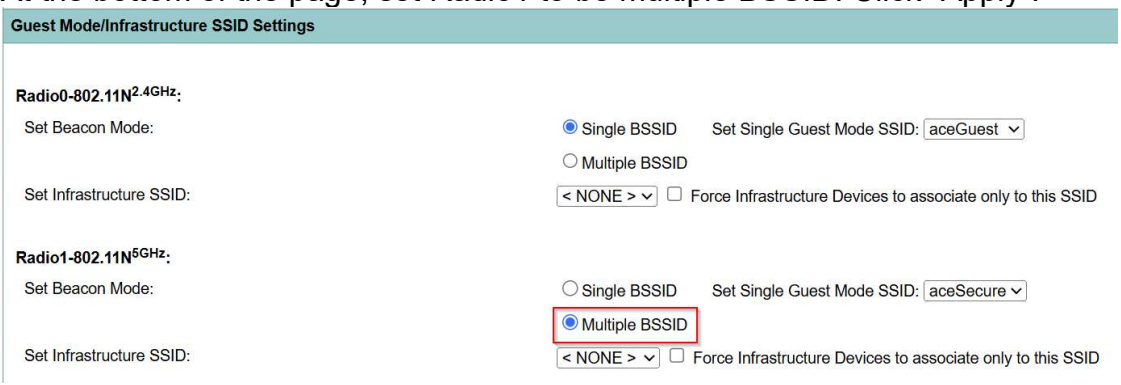
1. In the access point GUI, navigate to the express set-up page. The location will differ with different versions of the GUI, but should be located within the initial start screen.
2. Configure the SSID as shown.



3. Navigate to Security > SSID Manager. Check that for the SSID, the settings are correct. The check box for “Guest mode” must be checked in order for the SSID

to be broadcasted. Click “Apply”.

4. At the bottom of the page, set Radio1 to be multiple BSSID. Click “Apply”.



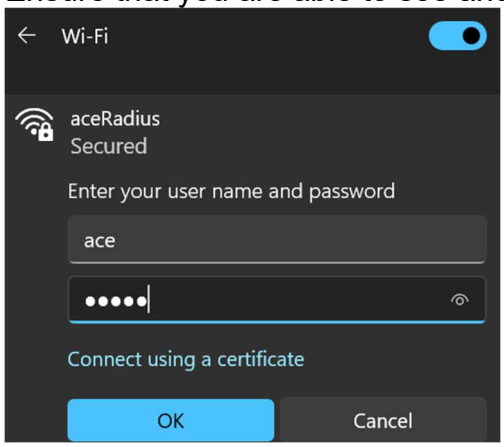
5. In the router, enter the following commands:

```
ip dhcp excluded-address 192.168.30.1 192.168.30.5
ip dhcp pool RADIUS
 network 192.168.30.0 255.255.255.0
 dns-server 8.8.8.8
 default-router 192.168.1.1
interface GigabitEthernet0/0/0.30
 encapsulation dot1Q 30
 ip address 192.168.30.1 255.255.255.0
 ip nat inside
access-list 1 permit 192.168.30.0 0.0.0.255
```

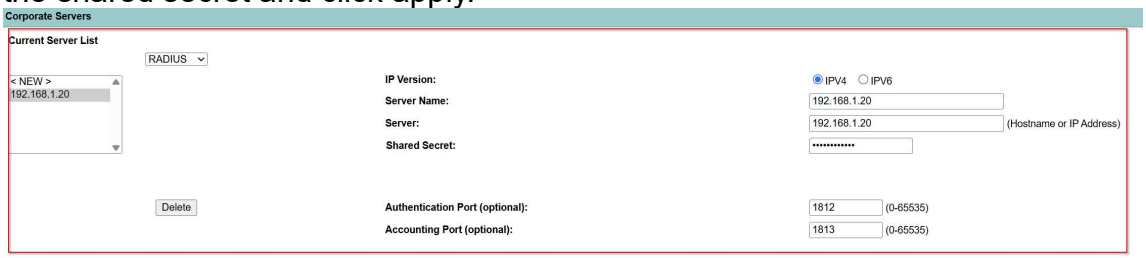
6. In the switch, enter the following commands:

```
vlan 30
 name RADIUS
```

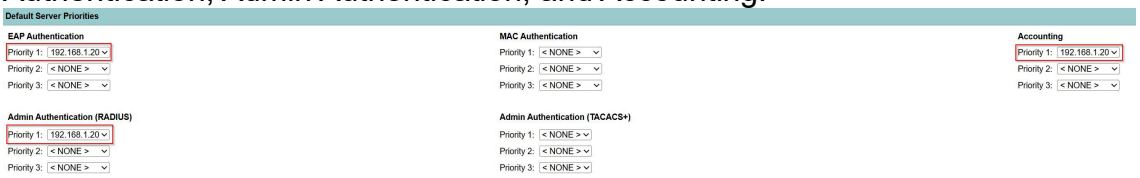
7. Ensure that you are able to see and connect to your SSID.



8. Navigate to Security > Server Management. Click on the RADIUS server. Type in the shared secret and click apply.



9. At the bottom of the page, set the RADIUS server as “Priority 1” for EAP Authentication, Admin Authentication, and Accounting.



Access Point (aceAP)

```
version 15.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
hostname ACE
logging rate-limit console 9
enable secret 5 $1$q.Mn$RQDAU5abolsVay.La2vRt1
aaa new-model
aaa group server radius rad_eap
 server name 192.168.1.20
aaa group server radius rad_mac
aaa group server radius rad_acct
 server name 192.168.1.20
aaa group server radius rad_admin
 server name 192.168.1.20
aaa group server tacacs+ tac_admin
aaa group server radius rad_pmip
aaa group server radius dummy
aaa authentication login eap_methods group rad_eap
aaa authentication login mac_methods local
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 ssid aceGuest
   vlan 10
```

```
   authentication open
   guest-mode
dot11 ssid aceRadius
   vlan 30
   authentication open eap eap_methods
   authentication network-eap eap_methods
   authentication key-management wpa
   mbssid guest-mode
dot11 ssid aceSecure
   vlan 20
   authentication open
   authentication key-management wpa version 2
   guest-mode
   mbssid guest-mode
   wpa-psk ascii 7 08701E1D5D4C53404A52
no ipv6 cef
username Cisco password 7 1531021F0725
bridge irb
interface Dot11Radio0
 no ip address
 ssid aceGuest
 antenna gain 0
 station-role root
 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 Dot11Radio0.10
 encapsulation dot1Q 10
 bridge-group 10
 bridge-group 10 subscriber-loop-control
 bridge-group 10 spanning-disabled
 bridge-group 10 block-unknown-source
 no bridge-group 10 source-learning
 no bridge-group 10 unicast-flooding
interface Dot11Radio1
 no ip address
 encryption vlan 20 mode ciphers aes-ccm
 encryption vlan 30 mode ciphers aes-ccm tkip
 ssid aceRadius
 ssid aceSecure
 antenna gain 0
 peakdetect
 dfs band 3 block
 mbssid
 channel dfs
 station-role root
 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 Dot11Radio1.20
 encapsulation dot1Q 20
 bridge-group 20
 bridge-group 20 subscriber-loop-control
 bridge-group 20 spanning-disabled
 bridge-group 20 block-unknown-source
 no bridge-group 20 source-learning
 no bridge-group 20 unicast-flooding
interface Dot11Radio1.30
 encapsulation dot1Q 30
 bridge-group 30
 bridge-group 30 subscriber-loop-control
 bridge-group 30 spanning-disabled
 bridge-group 30 block-unknown-source
 no bridge-group 30 source-learning
 no bridge-group 30 unicast-flooding
interface Dot11Radio1.201
interface GigabitEthernet0
 no ip address
 duplex auto
 speed auto
 bridge-group 1
 bridge-group 1 spanning-disabled
 no bridge-group 1 source-learning
interface GigabitEthernet0.10
 encapsulation dot1Q 10
 bridge-group 10
 bridge-group 10 spanning-disabled
 no bridge-group 10 source-learning
interface GigabitEthernet0.20
 encapsulation dot1Q 20
 bridge-group 20
 bridge-group 20 spanning-disabled
 no bridge-group 20 source-learning
interface GigabitEthernet0.30
 encapsulation dot1Q 30
 bridge-group 30
 bridge-group 30 spanning-disabled
 no bridge-group 30 source-learning
interface GigabitEthernet0.201
interface BVI1
 mac-address 44d3.ca03.7dce
 ip address 192.168.1.245 255.255.255.0
 ipv6 address dhcp
 ipv6 address autoconfig
 ipv6 enable
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 192.168.1.20
 address ipv4 192.168.1.20 auth-port 1812 acct-port 1813
 key 7 121A09160118
bridge 1 route ip
line con 0
line vty 0 4
 transport input all
end
```

Switch (aceSwitch)

```
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname aceSwitch
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
 switchport trunk encapsulation dot1q
 switchport mode trunk
 spanning-tree portfast trunk
interface FastEthernet0/2
 switchport mode access
 spanning-tree portfast
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
interface FastEthernet0/18
interface FastEthernet0/19
interface FastEthernet0/20
interface FastEthernet0/21
interface FastEthernet0/22
 switchport trunk encapsulation dot1q
 switchport mode trunk
 spanning-tree portfast trunk
interface FastEthernet0/23
 switchport trunk encapsulation dot1q
 switchport mode trunk
```

```
 spanning-tree portfast trunk
interface FastEthernet0/24
interface GigabitEthernet0/1
interface GigabitEthernet0/2
interface Vlan1
 ip address 192.168.1.2 255.255.255.0
ip classless
ip http server
ip http secure-server
ip sla enable reaction-alerts
line con 0
line vty 5 15
end
```

Router (aceRouter)

```
version 15.5
service timestamps debug datetime msec
service timestamps log datetime msec
no platform punt-keepalive disable-kernel-core
hostname aceRouter
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 192.168.1.1 192.168.1.5
ip dhcp excluded-address 192.168.10.1 192.168.10.5
ip dhcp excluded-address 192.168.20.1 192.168.20.5
ip dhcp excluded-address 192.168.30.1 192.168.30.5
ip dhcp excluded-address 192.168.1.20
ip dhcp excluded-address 192.168.1.245
!
ip dhcp pool GUEST
 network 192.168.10.0 255.255.255.0
 dns-server 8.8.8.8
 default-router 192.168.1.1
!
ip dhcp pool SECURE
 network 192.168.20.0 255.255.255.0
 dns-server 8.8.8.8
 default-router 192.168.1.1
ip dhcp pool RADIUS
 network 192.168.30.0 255.255.255.0
 dns-server 8.8.8.8
 default-router 192.168.1.1
subscriber templating
vtp domain cisco
vtp mode transparent
multilink bundle-name authenticated
license udi pid ISR4321/K9 sn FDO21281AAT
spanning-tree extend system-id
redundancy
 mode none
vlan internal allocation policy ascending
interface GigabitEthernet0/0/0
 no ip address
 negotiation auto
interface GigabitEthernet0/0/0.1
 encapsulation dot1Q 1 native
 ip address 192.168.1.1 255.255.255.0
 ip nat inside
```

```
interface GigabitEthernet0/0/0.10
 encapsulation dot1Q 10
 ip address 192.168.10.1 255.255.255.0
 ip nat inside
interface GigabitEthernet0/0/0.20
 encapsulation dot1Q 20
 ip address 192.168.20.1 255.255.255.0
 ip nat inside
interface GigabitEthernet0/0/0.30
 encapsulation dot1Q 30
 ip address 192.168.30.1 255.255.255.0
 ip nat inside
interface GigabitEthernet0/0/1
 ip address dhcp
 ip nat outside
 negotiation auto
interface GigabitEthernet0/1/0
 negotiation auto
interface GigabitEthernet0/1/1
 negotiation auto
interface Service-Engine0/2/0
 no ip address
interface GigabitEthernet0
 vrf forwarding Mgmt-intf
 no ip address
 shutdown
 negotiation auto
interface Vlan1
 no ip address
 shutdown
ip nat inside source list 1 interface GigabitEthernet0/0/1 overload
ip forward-protocol nd
no ip http server
no ip http secure-server
ip tftp source-interface GigabitEthernet0
access-list 1 permit 192.168.1.0 0.0.0.255
access-list 1 permit 192.168.10.0 0.0.0.255
access-list 1 permit 192.168.20.0 0.0.0.255
access-list 1 permit 192.168.30.0 0.0.0.255
control-plane
line con 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 login
end
```

Problems

1. Factory resetting the access point led to the access point to be stuck in the bootloader. It seemed that it was trying to load the image “flash: /c1140-k9w7-xx.153-3.JD9/c1140-k9w7-xx.153-3.JD9” and the image “flash:/ c1140-k9w7-mx.153-3.JD9/c1140-k9w7-mx.153-3.JD9”. However, the first image was too small, leading us to believe that it somehow got corrupted, and the second image didn’t exist. Instead, we found that the correct image was stored at “flash: /c1140-k9w7-mx.153-3.JD9/c1140-k9w7-xx.153-3.JD9”. To fix this, we set the BOOT environmental variable to “flash: /c1140-k9w7-mx.153-3.JD9/c1140-k9w7-xx.153-3.JD9”, and booted it through the correct image.
2. Our original topology only has one Layer 3 Switch as the networking device, as opposed to one switch and one router. This did not allow us to perform router on a stick, which allows both easier configuration and allows devices from inside the network to communicate within specific VLANs relating to their IP address.
3. There were native VLAN mismatches between the router/switch and the access point, leading to some tagged traffic to be untagged and be lost within the network, which at some points made us lose administrative access to the access point. We redid and cleaned up our VLAN settings to ensure this did not happen.
4. In our freeRADIUS configuration, we initially set up a private network in the clients.conf file. However, the correct configuration is to set a client for the access point with the IP address of the access point.
5. Using the default configuration for setting up the WPA Enterprise SSID did not set the radius server to be used. Instead, it only placed the information of the radius server within the access point. We had to manually configure the WPA Enterprise SSID to use the radius server as the default.
6. The default radius authentication and accounting ports in the access point are 1645 and 1646. However, the more common default and the default for freeRadius is 1812 and 1813. Correcting these allowed the access point to use the radius server for authentication.

Conclusion

In this lab, we successfully set up an access point to broadcast three SSIDs, each with a different authentication method. This lab had a lot of troubleshooting in relation to making sure each SSID was able to work within the network within their own VLAN. It was an excellent introduction to how access points function.

IS-IS

Purpose

The purpose of this lab is to learn how to configure IS-IS for routing across multiple areas.

Background Information

Routers are network devices that forward data packets between networks. Routers use routing protocols to determine where to send data packets by selecting the best path between routers.

The internet can be segregated into routing domains named autonomous systems (ASs), which can have their own routing information and policies. An Interior Gateway Protocol manages the routing information within an AS, as opposed to an Exterior Gateway Protocol managing the routing information between autonomous systems.

IS-IS is a link-state routing protocol that works as an interior gateway protocol. Link-state routing protocols work on the basis that routers will exchange information, called link states, on the links and nodes in a routing domain. Rather than exchanging a routing table, routers running a link-state routing protocol will exchange information on adjacent neighbors and networks.

A link-state protocol provides several benefits – there is no hop limit a route a take, link bandwidth can be a factor in calculating the shortest path, there is better convergence in the network, and VLSM and CIDR are both supported.

IS-IS allows autonomous systems to be split into “areas” for increased scalability and easier management. IS-IS can route protocols using Level 1 or Level 2. Level 1 Routing is intra-area routing, for only the other routers within the same area. Level 2 Routing is inter-area routing, and is used for routers outside the area. Interfaces can be configured as Level 1 only, Level 2 only, or both Level 1 and 2.

Compared to other interior routing protocols such as OSPF, IS-IS operates on Layer 2, not requiring IP connectivity, and therefore is less vulnerable to attacks. It does not require a “backbone” area, while OSPF uses area 0 as the backbone. Overall, IS-IS is considered to be more scalable and simpler to configure than OSPF.

IS-IS has several disadvantages, including less recent support by many services, and being more complex in terms of being Layer 2 compared to the more known Layer 3 IP routing. There is also less specific control over areas compared to OSPF and other interior gateway protocols.

Lab Summary

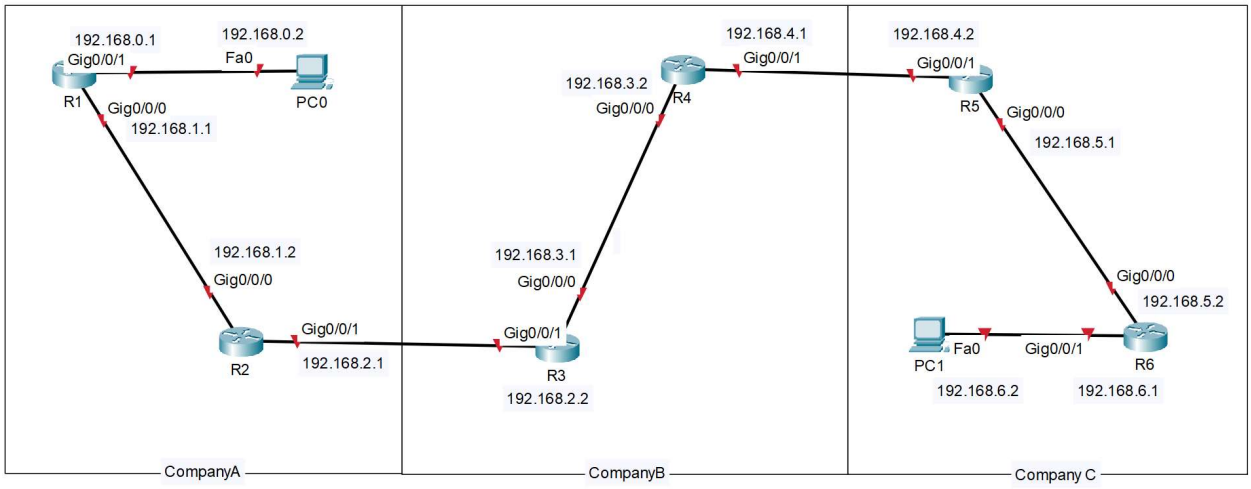
In this lab, we will configure a network consisting of six routers and two end devices within one autonomous system. The AS will be split into 3 areas, 2 routers in each area. The end devices will sit at the ends of Area A and Area C.

The routing protocol used is IS-IS, and will only be configured for IPv4.

Lab Commands

```
router isis [Area Name]
 net [Net ID]
 is-type [Level]
interface [Interface Number]
 ip router isis [Area Name]
```

Network Diagram



Configurations

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
subscriber templating
vtp domain cisco
vtp mode transparent
multilink bundle-name authenticated
license udi pid ISR4321/K9 sn FDO21281AAT
spanning-tree extend system-id
redundancy
 mode none
vlan internal allocation policy ascending
interface GigabitEthernet0/0/0
 ip address 192.168.1.1 255.255.255.0
 ip router isis companyA
 negotiation auto
interface GigabitEthernet0/0/1
 ip address 192.168.0.1 255.255.255.0
 ip router isis companyA
 negotiation auto
interface GigabitEthernet0/1/0
 no ip address
 shutdown
 negotiation auto
interface GigabitEthernet0/1/1
 no ip address
 shutdown
 negotiation auto
interface Service-Engine0/2/0
 no ip address
 shutdown
interface GigabitEthernet0
 vrf forwarding Mgmt-intf
 no ip address
 shutdown
 negotiation auto
interface Vlan1
 no ip address
 shutdown
router isis companyA
 net 49.0000.1920.1680.0001.00
```

```
 is-type level-1
 redistribute connected
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
```

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
subscriber templating
vtp domain cisco
vtp mode transparent
multilink bundle-name authenticated
license udi pid ISR4321/K9 sn FDO21491LXF
spanning-tree extend system-id
redundancy
 mode none
vlan internal allocation policy ascending
interface GigabitEthernet0/0/0
 ip address 192.168.1.2 255.255.255.0
 ip router isis companyA
 negotiation auto
interface GigabitEthernet0/0/1
 ip address 192.168.2.1 255.255.255.0
 ip router isis companyA
 negotiation auto
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 isis companyA
 net 49.0000.1920.1680.0002.00
 redistribute connected
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
```

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
subscriber templating
vtp domain cisco
vtp mode transparent
multilink bundle-name authenticated
license udi pid ISR4321/K9 sn FLM240607Q1
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 companyB
 negotiation auto
interface GigabitEthernet0/0/1
 ip address 192.168.2.2 255.255.255.0
 ip router isis companyB
 negotiation auto
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 companyB
 net 49.0000.1920.1680.0003.00
 redistribute connected
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
```

R4

```
version 16.9
service timestamps debug datetime msec
service timestamps log datetime msec
platform qfp utilization monitor load 80
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
login on-success log
subscriber templating
vtp domain cisco
vtp mode transparent
multilink bundle-name authenticated
license udi pid ISR4321/K9 sn FLM240800D6
no license smart enable
diagnostic bootup level minimal
spanning-tree extend system-id
redundancy
 mode none
interface GigabitEthernet0/0/0
 ip address 192.168.3.2 255.255.255.0
 ip router isis companyB
 negotiation auto
interface GigabitEthernet0/0/1
 ip address 192.168.4.1 255.255.255.0
 ip router isis companyB
```

```
 negotiation auto
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
router isis companyB
 net 49.0000.1920.1680.0004.00
 metric-style narrow
 redistribute connected
ip forward-protocol nd
ip http server
ip http authentication local
ip http secure-server
ip tftp source-interface GigabitEthernet0
control-plane
line con 0
 transport input none
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 login
end
```

R5

```
version 16.9
service timestamps debug datetime msec
service timestamps log datetime msec
platform qfp utilization monitor load 80
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
login on-success log
subscriber templating
vtp domain cisco
vtp mode transparent
multilink bundle-name authenticated
license udi pid ISR4321/K9 sn FLM2407011F
no license smart enable
diagnostic bootup level minimal
spanning-tree extend system-id
redundancy
```

```
 mode none
interface GigabitEthernet0/0/0
 ip address 192.168.5.1 255.255.255.0
 ip router isis companyC
 negotiation auto
interface GigabitEthernet0/0/1
 ip address 192.168.4.2 255.255.255.0
 ip router isis companyC
 negotiation auto
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
router isis companyC
 net 49.0000.1920.1680.0005.00
 metric-style narrow
 redistribute connected
ip forward-protocol nd
ip http server
ip http authentication local
ip http secure-server
ip tftp source-interface GigabitEthernet0
control-plane
line con 0
 transport input none
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 login
end
```

R6

```
version 16.9
service timestamps debug datetime msec
service timestamps log datetime msec
platform qfp utilization monitor load 80
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
```

```
login on-success log
subscriber templating
vtp domain cisco
vtp mode transparent
multilink bundle-name authenticated
license udi pid ISR4321/K9 sn FDO214420HW
license boot level appxk9
no license smart enable
diagnostic bootup level minimal
spanning-tree extend system-id
redundancy
 mode none
interface GigabitEthernet0/0/0
 ip address 192.168.5.2 255.255.255.0
 ip router isis companyC
 negotiation auto
interface GigabitEthernet0/0/1
 ip address 192.168.6.1 255.255.255.0
 ip router isis companyC
 negotiation auto
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
router isis companyC
 net 49.0000.1920.1680.0006.00
 is-type level-1
 metric-style narrow
 redistribute connected
ip forward-protocol nd
ip http server
ip http authentication local
ip http secure-server
ip tftp source-interface GigabitEthernet0
control-plane
line con 0
 transport input none
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 login
end
```

R1 Route Table

```
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, GigabitEthernet0/0/0
L        192.168.1.1/32 is directly connected, GigabitEthernet0/0/0
i L1  192.168.2.0/24 [115/20] via 192.168.1.2, 00:02:58, GigabitEthernet0/0/0
i L1  192.168.3.0/24 [115/30] via 192.168.1.2, 00:02:48, GigabitEthernet0/0/0
i L1  192.168.4.0/24 [115/40] via 192.168.1.2, 00:02:41, GigabitEthernet0/0/0
i L1  192.168.5.0/24 [115/50] via 192.168.1.2, 00:02:26, GigabitEthernet0/0/0
```

Problems

1. Wi-fi was not turned off when pinging from PC’s, causing pings to fail until it was turned off.

Conclusion

In this lab, we successfully configured IS-IS for a single autonomous system, consisting of three areas with 2 routers each. IPv4 connectivity was established from end devices from one end of the network to the other.

Layer 2 Attacks

Purpose

The purpose of this lab is to carry our three separate attacks on a Layer 2 network and then mitigate each of the attacks.

Background Information

Every device has a unique MAC (Media Access Control) address that is assigned to the device's NIC (network interface card). Each MAC address comprises of 6 groups of 2 hexadecimal digits. The first 3 groups, called the Organizationally Unique Identifier (OUI) indicate the manufacturer and the last 3 groups identify the specific device from the manufacturer.

MAC addresses are used to identify devices and frames as the basic unit of data transmission in Layer 2 networks. Layer 2 networks allow data to be transferred between connected nodes within a LAN.

There are various attacks that can be performed on a layer 2 network. The overall goal of these attacks is to disrupt services, and could be expanded to data theft or financial gain for the attacker.

3 separate attacks are performed in the lab. These attacks are MAC flooding, ARP spoofing, and DHCP starvation.

MAC Flooding

In order to know where to send data traffic, network switches have a MAC address table that records the correct mappings of MAC addresses and ports. However, these tables have a limit of how many addresses they remember. The goal of a MAC flooding attack is to overload the memory of the MAC address table. When a MAC address table is full, incoming packets to the switch are broadcasted out of every port increase of being forwarded to the correct device. This then allows the attacker to receive packets that they are not supposed to have access to.

To prevent MAC flooding, switchport security can be enabled on untrusted ports. Switchport security can be configured to limit the number of MAC addresses that are received through a single port. Excess MAC addresses are rejected and notify the switch logging system that more MAC addresses were detected.

ARP Spoofing

The ARP (address resolution protocol) table stoles mappings of IP addresses to MAC addresses. The ARP table allows a switch to translate IP address into MAC addresses in order to know where to send packets. Normally, a host will send an ARP Request

message to all other hosts on a LAN in order to find our what MAC address corresponds to a certain IP address. The correct device with that IP address responds with its own ARP Reply message, letting the original device know where to send packets. However, without configured security, nothing prevents an attacker from sending out ARP Reply messages without even being asked with an ARP Request. Devices that receive this malicious ARP Reply will update their ARP table with incorrect information. For instance, an attacker can use this to map the default gateway to their own MAC address, allowing them to receive all packets meant for the default gateway.

To prevent ARP spoofing, Dynamic ARP Inspection (DAI) should be turned on. DAI uses information in DHCP tables in order to validate incoming ARP packets. This validation compares the MAC and IP address information against information in the DHCP tables, and any inconsistent packets are automatically dropped.

DHCP Starvation

DHCP (Dynamic Host Configuration Protocol) is a network protocol that will automatically assign IP addresses to devices on a network. These IP addresses come from a DHCP pool of finite addresses. Normally, when a device joins a network, they send out a DHCP DISCOVER packet in order to contact the server and start the process of receiving a DHCP IP address.

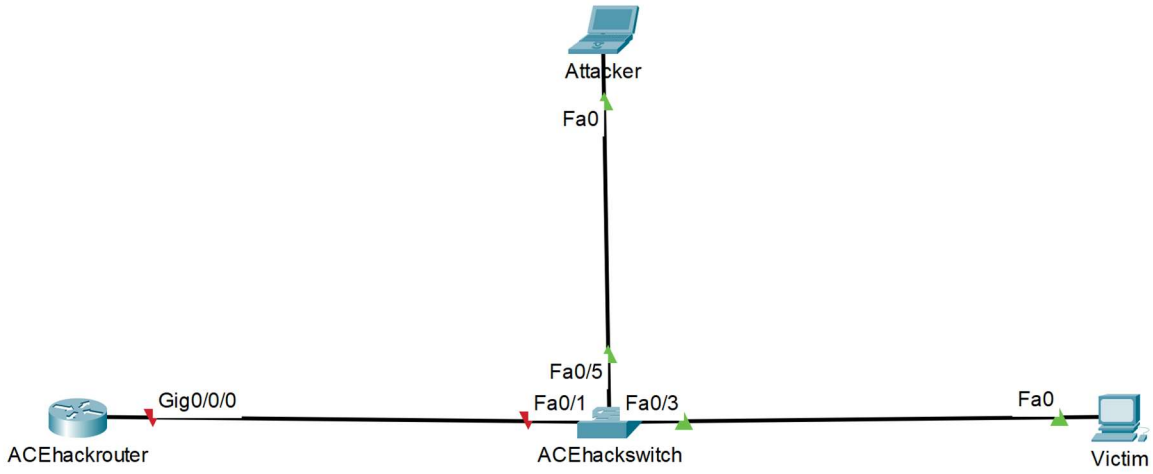
The goal of a DHCP starvation attack is to “starve” or exhaust this pool, so any new devices that join the network are unable to receive an IP address and thus unable to access the internet. A DHCP starvation attack involves sending bogus DHCP DISCOVER packets using bogus MAC addresses as the source of each request. If the DHCP server responds to these requests and hand out addresses, the pool will quickly become exhausted.

To prevent a DHCP starvation attack, the same prevention to prevent MAC flooding can be used. Since DHCP starvation attacks rely on using bogus MAC addresses, limiting the number of MAC addresses per untrusted port also prevents DHCP starvation.

Lab Summary

In this lab, we configured a Layer 2 network and then performed 3 different attacks on the network, with the goal of disrupting it and/or reading packets that are not supposed to be open. These attacks are MAC flooding, ARP spoofing, and DHCP starvation. We then set up protections against these three attacks and confirmed that they will prevent the attacks from affecting the network.

Network Diagram



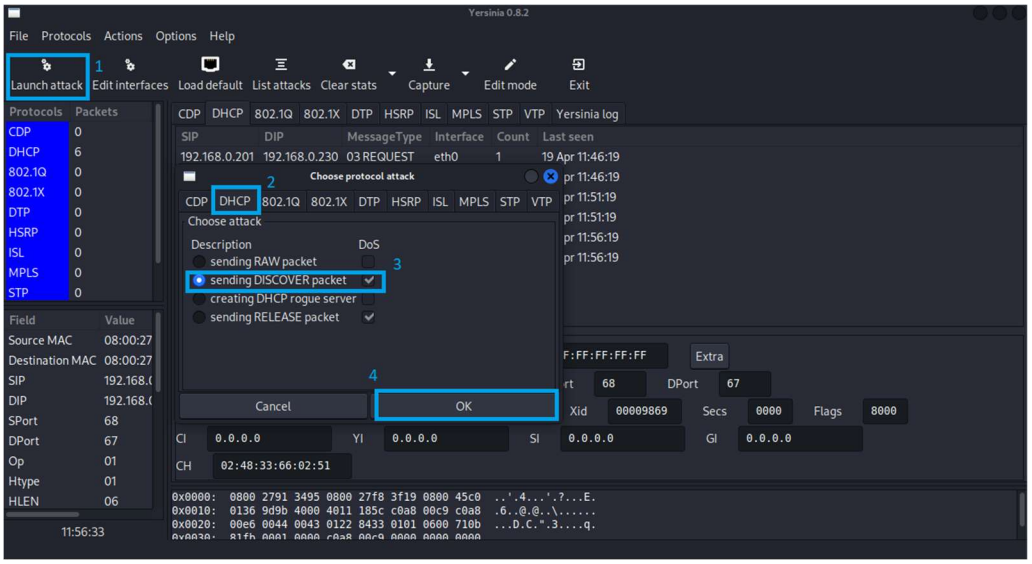
Lab Commands

Setup network

1. On the router, configure an IP address for connectivity and configure a DHCP server to distribute IP addresses.
2. Connect both the attacker and victim to the network and ensure that they can receive IP addresses.

DHCP Starvation Attack

1. On the attacker, install Yersinia
   ```
   sudo apt install yersinia
   ```
2. Disconnect the victim and attacker from the switch, and release all DHCP bindings on the router
   ```
   clear ip dhcp bindings *
   ```
3. Reconnect the attacker to gain an IP address through DHCP.
4. On the attacker, run the DHCP Discover flood attack.
   a. Bring up the Yersinia GUI
      ```
      sudo yersinia -G
      ```
   b. Click “Launch Attack” and select the DHCP Discover flood attack



5. On the router, show DHCP bindings to demonstrate the attack.
   ```
   show ip dhcp pool
   ```
6. Connect the victim to the network. Note that the PC is unable to receive an IP address.
7. To reset the network, clear DHCP bindings again.
   ```
   clear ip dhcp bindings *
   ```

DHCP Starvation Prevention

On the switch, enable port-security on all untrusted ports and set a maximum of 2 MAC addresses along with the following configurations.

```
switchport mode access
switchport port-security
switchport port-security maximum 2
```

```
switchport port-security violation restrict
switchport port-security mac-address sticky
```

ARP Spoofing Attack

1. On the attacker, install Dsniff
   `sudo apt install dsniff`
2. Connect both attacker and victim to the switch and ensure they receive IP addresses from DHCP.
3. On the router, show the arp table and record the IP and MAC addresses of both devices.
   show arp
4. On the attacker, run the ARP spoofing attack.
   a. Identify the correct interface
      ip a
   b. Run the attack
      sudo arpspoof -i [interface] -t [gateway IP] [victim IP]
5. On the router, show the arp table and note the difference in MAC addresses from before.
   show arp
6. Stop the attack with Ctrl-C on the attacker. This will automatically return the MAC addresses to normal.

ARP Spoofing Prevention

On the switch, enable DHCP snooping and ARP inspection, and set the router port to be trusted.

```
ip dhcp snooping
ip dhcp snooping vlan 1
ip arp inspection vlan 1
interface FastEthernet0/1
 ip dhcp snooping trust
 ip arp inspection trust
```

MAC Flooding Attack

1. On the attacker, install Dsniff
   `sudo apt install dsniff`
2. Connect both attacker and victim to the switch and ensure they receive IP addresses from DHCP.
3. On the router, show the mac table and note how many dynamic entries there are.
   show mac address-table dynamic
4. On the attacker, run the MAC flooding attack.
   a. Identify the correct interface
      ip a
   b. Run the attack
      sudo macof -i [interface]
5. On the router, show the mac table again.
   show mac address-table dynamic
6. Clear the mac table
   clear mac address-table dynamic

MAC Flooding Prevention

On the switch, enable port-security on all untrusted ports and set a maximum of 1 MAC address along with the following configurations.

```
switchport mode access
switchport port-security
switchport port-security maximum 1
switchport port-security violation restrict
switchport port-security mac-address sticky
```

Configurations

ACEhackswitch

```
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname ACEhackswitch
boot-start-marker
boot-end-marker
no aaa new-model
system mtu routing 1500
authentication mac-move permit
ip subnet-zero
ip dhcp snooping vlan 1
ip dhcp snooping
ip arp inspection vlan 1
spanning-tree mode pvst
spanning-tree etherchannel guard misconfig
spanning-tree extend system-id
vlan internal allocation policy ascending
interface FastEthernet0/1
 ip arp inspection trust
 spanning-tree portfast
 ip dhcp snooping trust
interface FastEthernet0/2
interface FastEthernet0/3
interface FastEthernet0/4
interface FastEthernet0/5
 switchport mode access
 switchport port-security
 switchport port-security violation restrict
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 5091.e368.6297 vlan access
 spanning-tree portfast
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
interface FastEthernet0/18
interface FastEthernet0/19
interface FastEthernet0/20
interface FastEthernet0/21
interface FastEthernet0/22
interface FastEthernet0/23
interface FastEthernet0/24
```

```
interface GigabitEthernet0/1
interface GigabitEthernet0/2
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
```

ACEhackrouter

```
version 16.9
service timestamps debug datetime msec
service timestamps log datetime msec
platform qfp utilization monitor load 80
platform punt-keepalive disable-kernel-core
hostname ACEhackrouter
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 192.168.0.0 192.168.0.9
ip dhcp pool SERVER
 network 192.168.0.0 255.255.255.0
 dns-server 8.8.8.8
 default-router 192.168.0.1
login on-success log
subscriber templating
vtp domain cisco
vtp mode transparent
multilink bundle-name authenticated
license udi pid ISR4321/K9 sn FDO21281AAT
no license smart enable
diagnostic bootup level minimal
spanning-tree extend system-id
redundancy
 mode none
interface GigabitEthernet0/0/0
 ip address 192.168.0.1 255.255.255.0
 negotiation auto
interface GigabitEthernet0/0/1
 no ip address
 negotiation auto
interface GigabitEthernet0/1/0
 no ip address
 shutdown
 negotiation auto
interface GigabitEthernet0/1/1
 no ip address
```

```
 shutdown
 negotiation auto
interface Service-Engine0/2/0
 no ip address
interface GigabitEthernet0
 vrf forwarding Mgmt-intf
 no ip address
 shutdown
 negotiation auto
ip forward-protocol nd
ip http server
ip http authentication local
ip http secure-server
ip tftp source-interface GigabitEthernet0
control-plane
line con 0
 transport input none
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 login
end
```

Problems

We had some issues downloading dsniff for running the MAC flooding and ARP spoofing onto our Linux laptop, but connecting to a different network allowed this to go through.

Conclusion

In this lab, we configured a Layer 2 network and ran three separate attacks on it with the goal of disrupting the network. We then configured protections against these attacks, and confirmed that they prevented the attacks from working. This lab was a good introduction to common prevention measures that should be configured to prevent attackers from easily disrupting a network.

PA-220 Factory Reset

Purpose

The purpose of this lab is to learn how to perform a factory reset of a Palo Alto PA-220 firewall.

Background Information

A firewall is a networking device that monitors and filters incoming and outgoing network traffic. Firewalls are necessary to prevent outside threats such as unauthorized access and malware. Firewalls normally sit on the edge of networks that connect to either the internet or other networks. Hardware-based firewalls, such as the PA-220, are useful for filtering network traffic for multiple devices and provides an additional line of defense for the network. Software-based firewalls usually sit on the user device and usually come with the operating system. They can able be installed through software vendors or an ISP. Software-based firewalls allow control over individual applications on the device, but since the firewall is located on the same device that is being protected, its ability to detect and stop malicious software can be limited. They are also less scalable than hardware-based firewalls, since each device's firewall would need to run security updates individually.

Palo Alto Networks is a cybersecurity company producing advanced firewalls. Palo Alto firewalls provide application-based policy enforcement, user identification, threat prevention, URL filtering, traffic visibility, networking versatility and speed, and malware analysis and reporting.

The PA-220 firewall is designed for small organizations or branch offices. It includes active/passive and active/active high availability, passive cooling, eight Ethernet ports, and dual power adapters. The PA-220 runs on PAN-OS® 8.0.

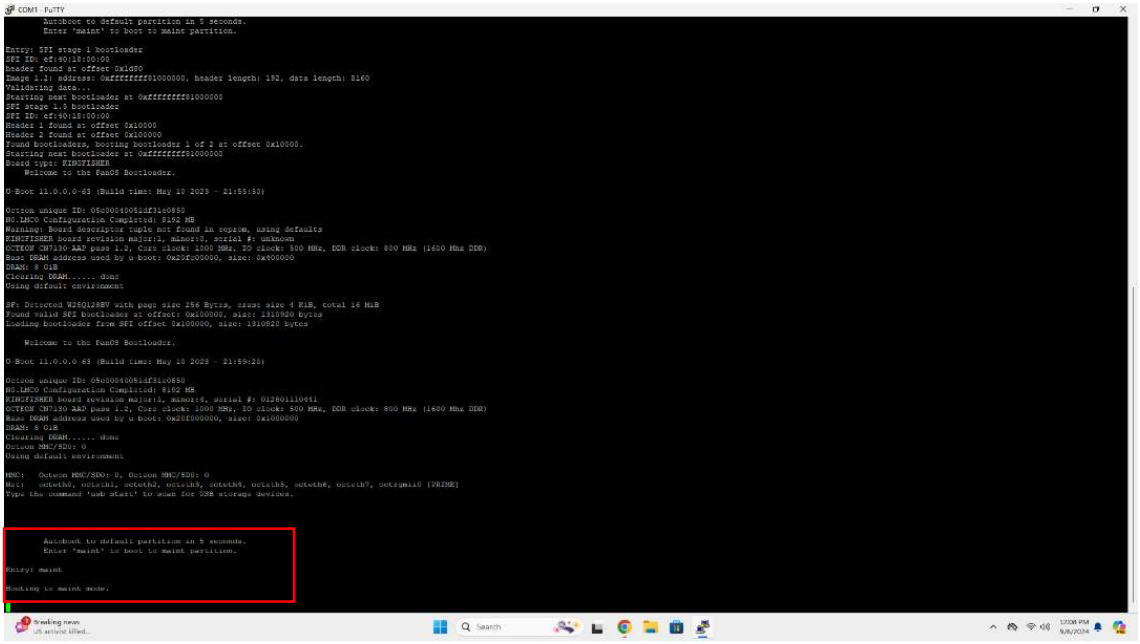
In the event of being unable to log in or receiving a PA-220 from someone else, a factory reset is needed to access the console of a PA-220. A factory reset completely wipes all data, settings, and configurations of the firewall, restoring it to its default state.

Lab Summary

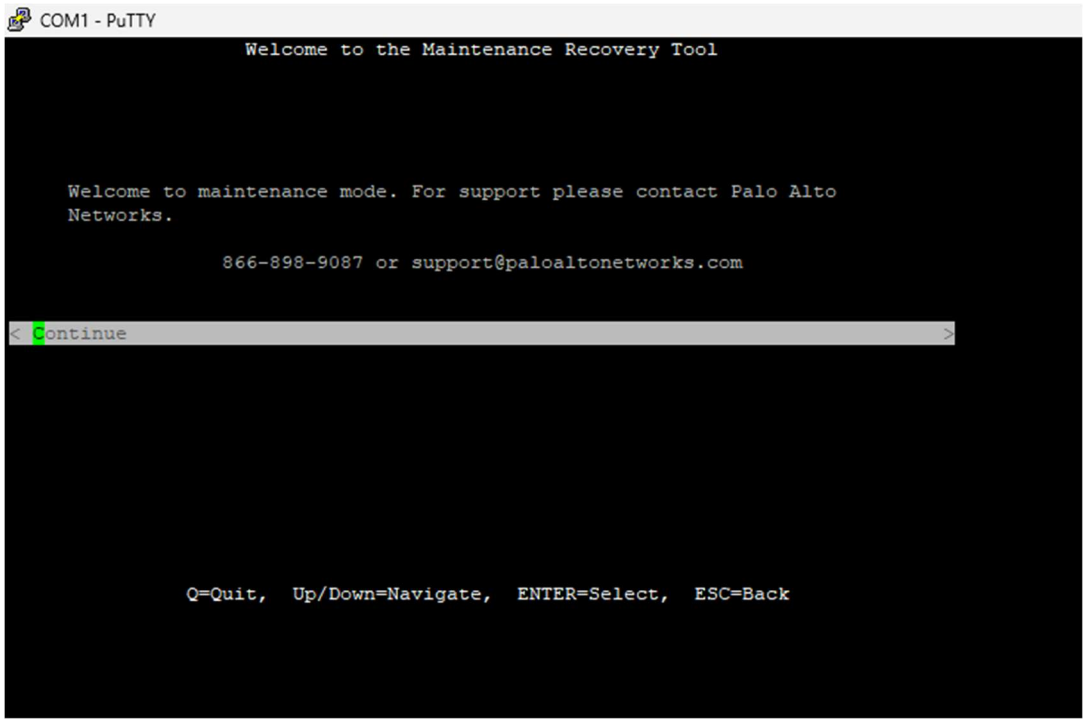
Connect your PA-220 to your computer through the console port. Open PuTTY and use COM1 as the serial line.

Connect the PA-220 to power.

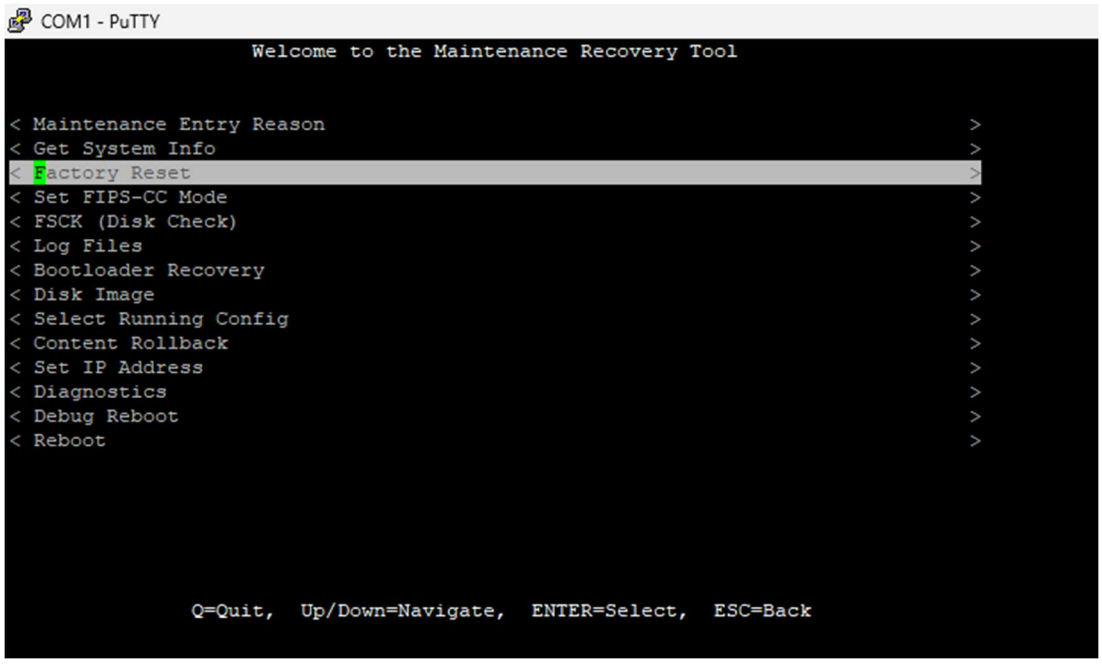
When prompted, enter “maint” to enter maintenance mode. If the firewall does not have three green lights on it yet, you will need to wait until the Maintenance Recovery Tool shows up.



In the Maintenance Recovery Tool, select “Continue”.

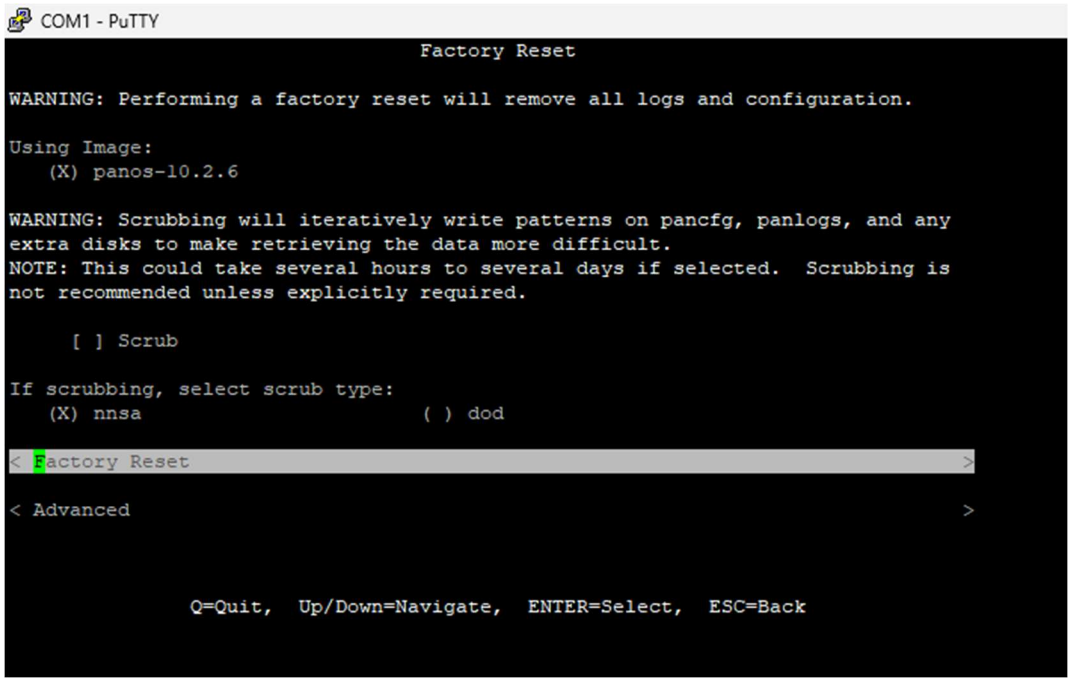


Select “Factory Reset”.

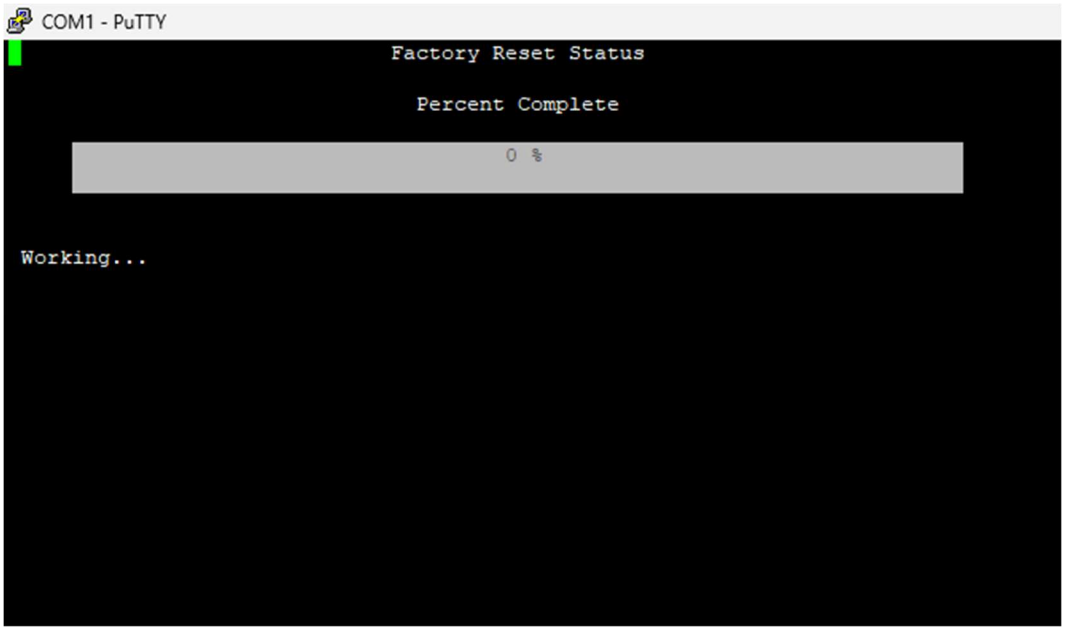


Select the image you want to reset. Do not select the Scrub option.

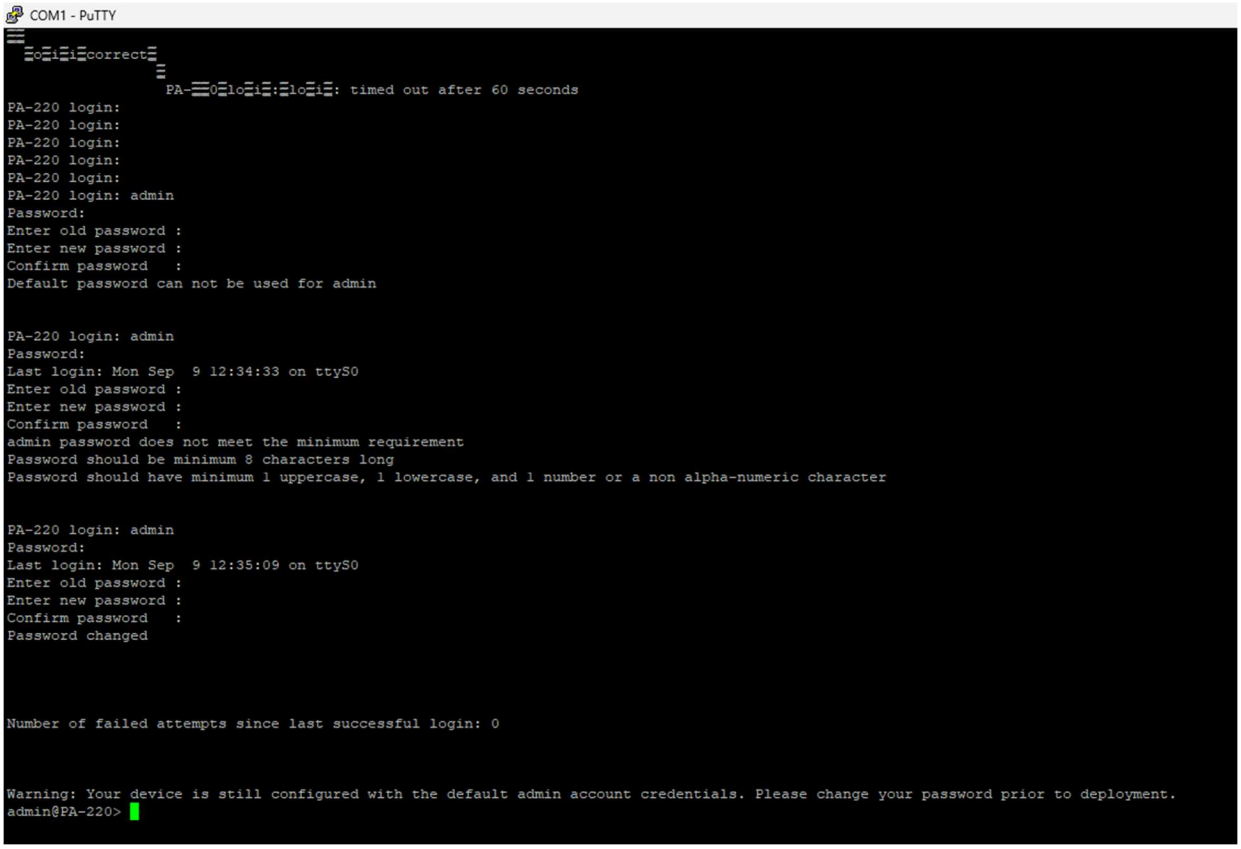
Select “Factory Reset”



The firewall will now start resetting.



After resetting, you will be prompted to log in. The default login/password is admin/admin. Change the password to something you will remember. Note that it requires 1 uppercase, 1 lowercase, and 1 number or non alpha-numeric character.



Problems

We were unaware that the firewall took a long time to boot up so when initially trying to reset the firewall, we thought that there were issues since we weren't entering the Maintenance Recovery Tool after entering "maint" into the console. In trying to fix this issue, we power cycled the firewall, which only delayed the issue.

Conclusion

In this lab, we successfully performed a factory reset on a PA-220 firewall, removing its password and adding our own password. This would be useful if we ever forget the password to a PA-220 or if we obtained a used PA-220 from someone else and need to access the console.

PA-220 SOHO Network

Purpose

The purpose of this lab is to configure a Small Office/Home Office (SOHO) network using a PA-220 firewall.

Background Information

A Small Office/Home Office (SOHO) network is designed for small businesses or individuals operating within small offices or homes. A SOHO network can be set up for much cheaper than a large corporate network, making it more suitable for small businesses or homes on a budget. Devices on a SOHO network can also share resources, such as printers or file systems, allowing greater productivity. These devices are also all easily accessible by the administrator of the network which makes is simpler for troubleshooting any problems that arise.

A SOHO network requires multiple networking devices, including a switch, router, and usually, a firewall. A switch is used to connect and communicate with all network-enabled devices, such as computers and printers. The switch forwards data packets from one device to another and ensures communication is established.

A router is used as the central networking device within a SOHO network using wired and wireless connections. They usually provide a web interface for configuration of the network. Routers can have other functions such as firewalls, VPNs, and other security features.

The PA-220 firewall is designed for small organizations or branch offices. It includes traditional routing capabilities and protocols such as OSPF and IPSec, but does not support some other protocols such as GRE or EIGRP. It includes active/passive and active/active high availability, passive cooling, eight Ethernet ports, and dual power adapters. The PA-220 runs on PAN-OS® 8.0.

As a firewall, the PA-220 is able to filter out malicious code and other cyber attacks, such as DOS. In a SOHO network, it allows users to access an outside corporate network without risk of spreading any malicious code into the network.

The PA-220 requires a security zone to be set on each interface. These security zones allow physical/virtual interfaces to be grouped together to easily set filtering on several interfaces at once. For instance, setting an Untrusted security zone and then adding all interfaces that connect to the ISP to it allows an administrator to filter any and all traffic coming from the Internet.

Each interface also requires a VLAN, which allows administrators to filter traffic to and from multiple firewalls at once.

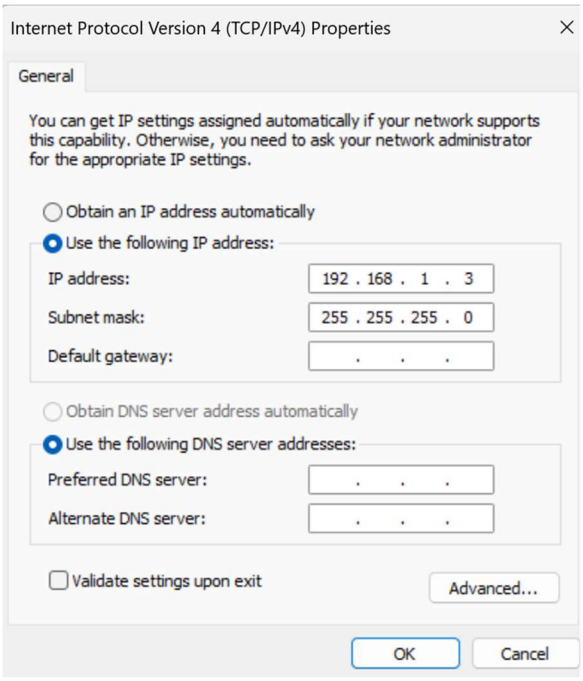
Lab Summary

In this lab, you will configure three security zones: Trust-L2, Trust-L3, and Untrust-L3, for trusted/untrusted ports. A VLAN will be created for interfaces under Trust-L2, and be given an IP Address. A DHCP pool will be created to allow the pc to gain a DHCP IP address. Security and filtering policies will be set up for future configuration.

Lab Commands

To configure the PA-220, connect your computer to the Management port on the firewall through a switch. If you do not have the password, factory reset the firewall to change the password.

Change your computer's IP address to somewhere within the 192.168.1.0/24 subnet, excluding 192.168.1.1.

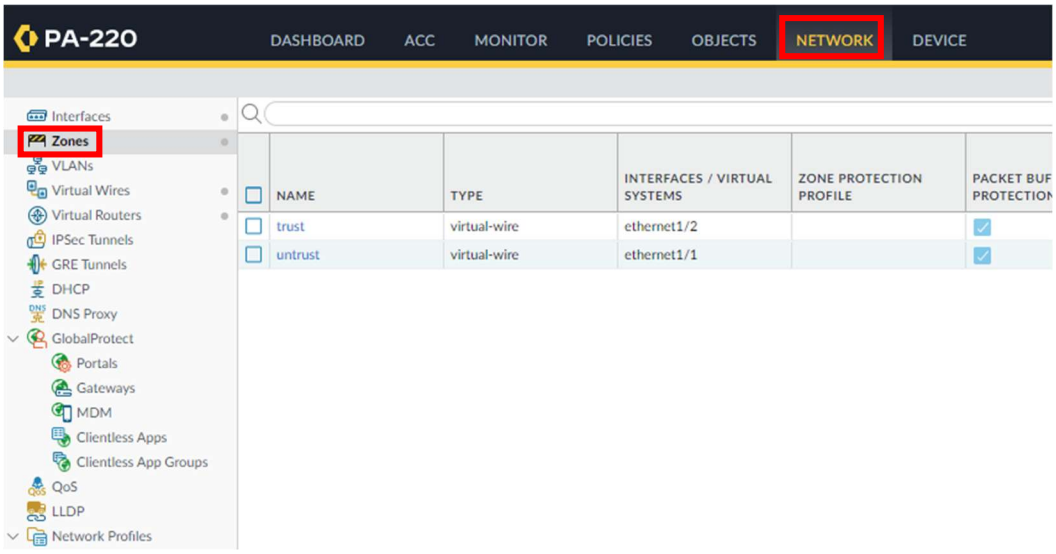


On a web browser, go to https://192.168.1.1 to access the web interface. Enter your username and password. The default username/password is admin/admin.

Security Zones Configuration

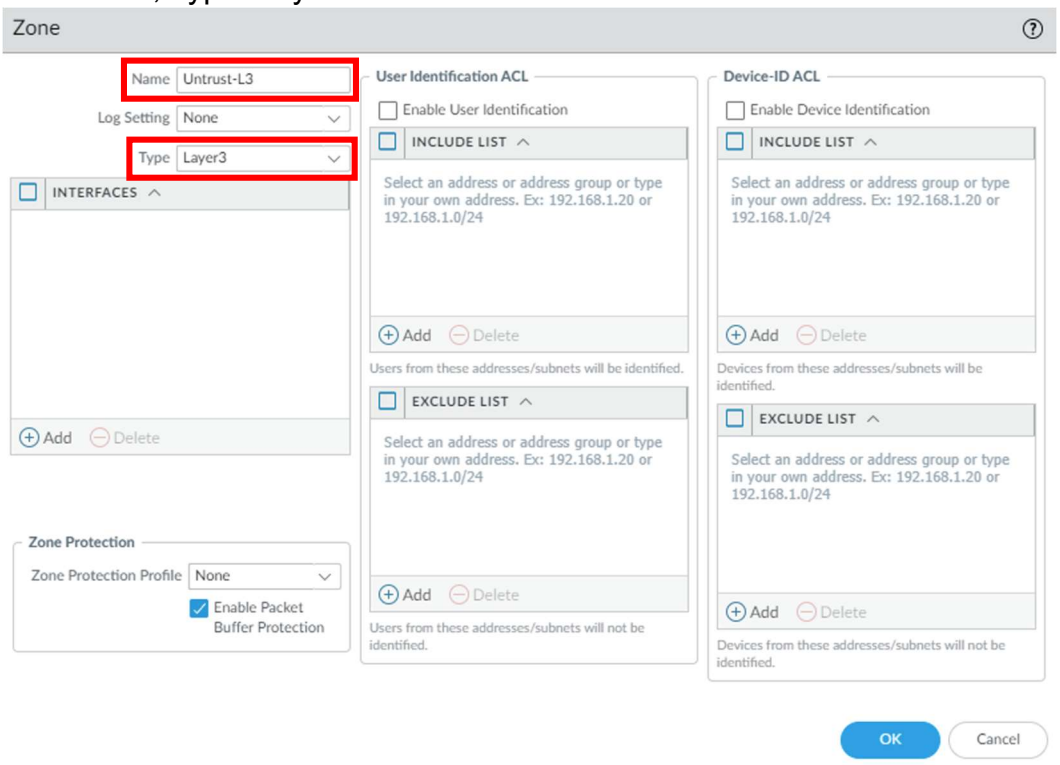
Go to Network > Virtual Wires. Select the default virtual wire and delete it.

Go to Network > Zones.

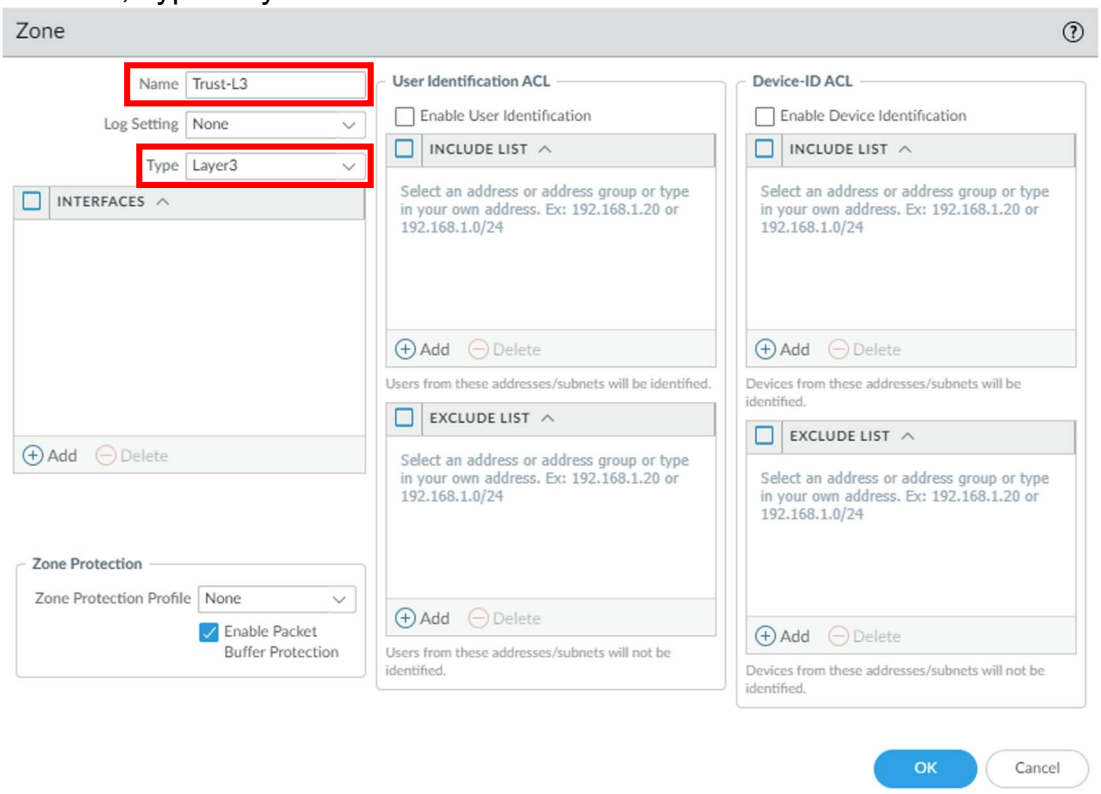


Use the “Add” button at the bottom of the web interface to create three zones:

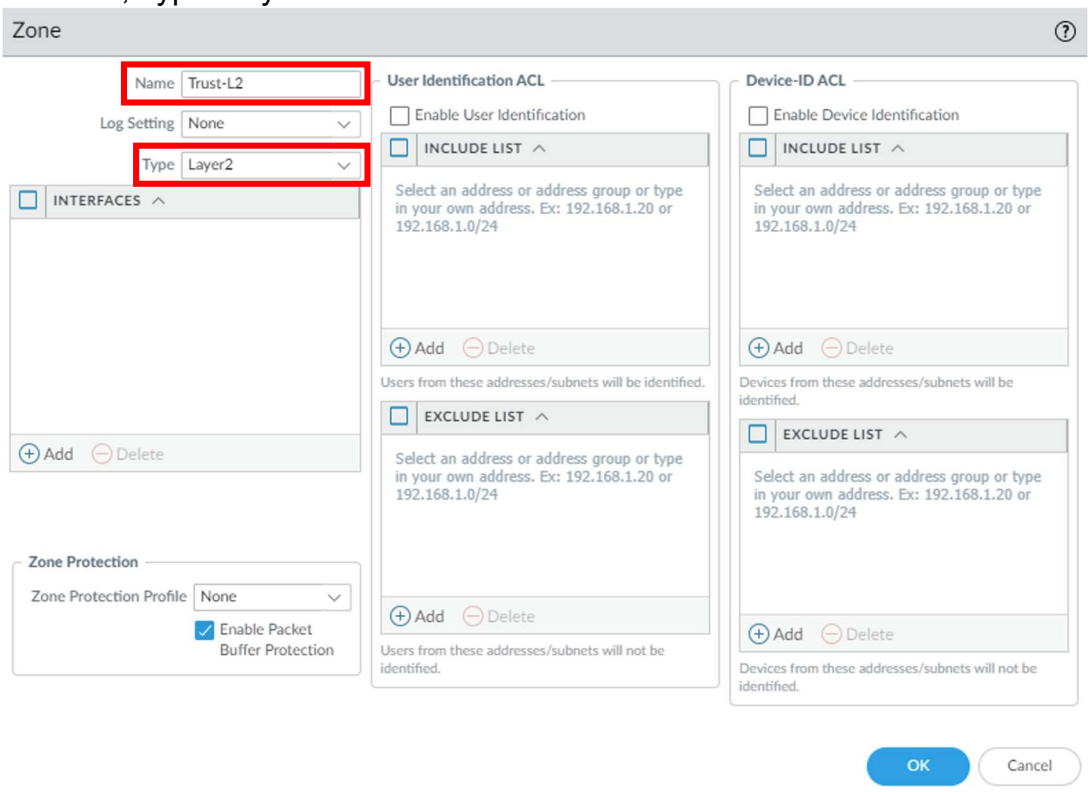
- Untrust-L3, Type: Layer3



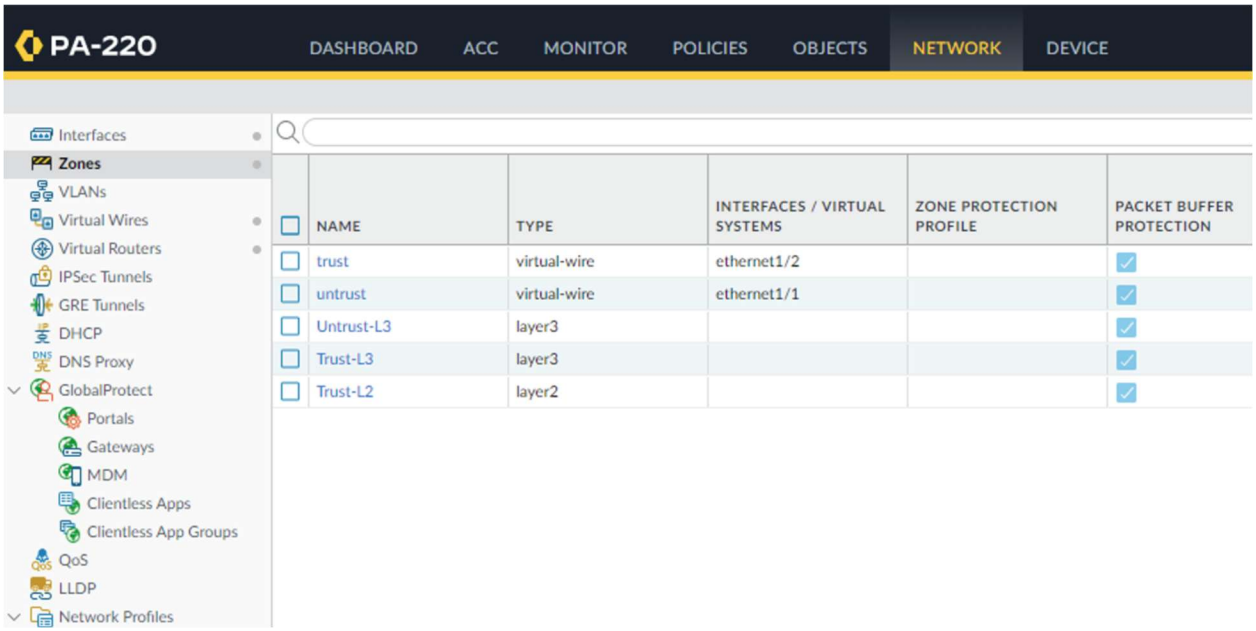
- Trust-L3, Type: Layer 3



- Trust-L2, Type: Layer 2



The result should be:

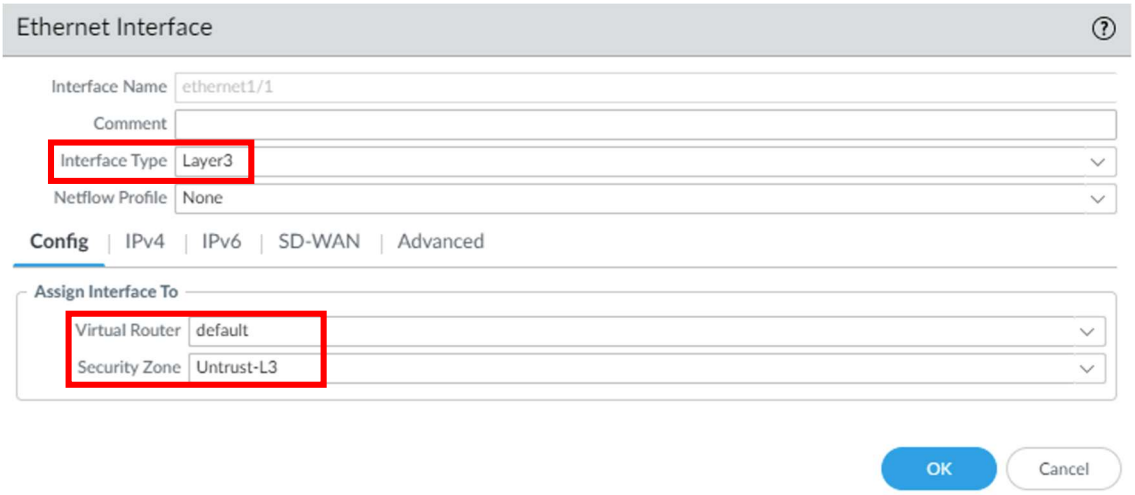


ISP Interface Configuration

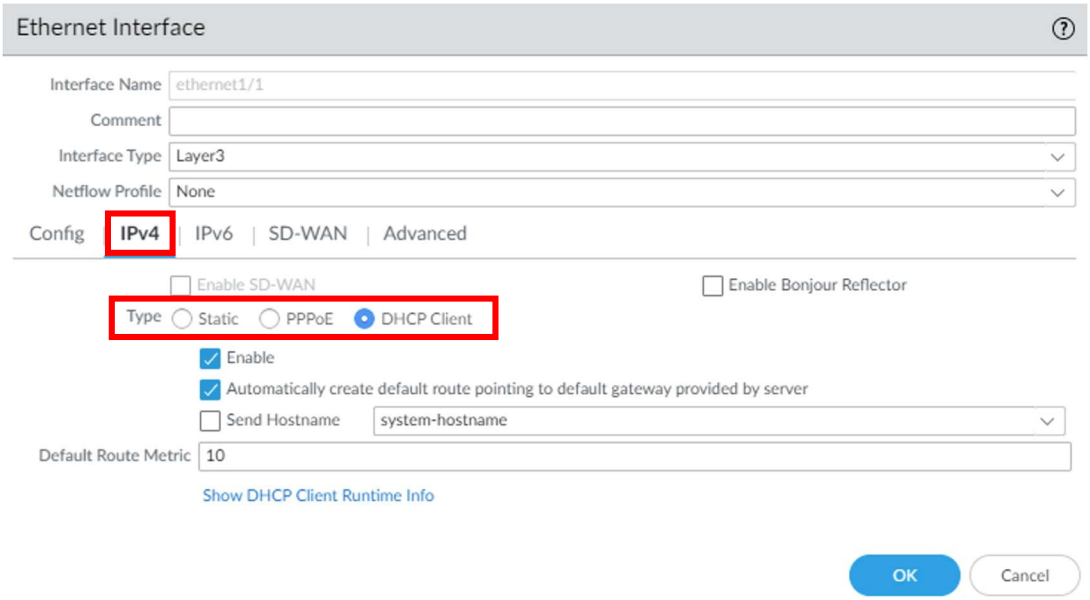
At this point, connect the firewall to the ISP modem. Any port can be used. In this example, port ethernet 1/1 is used to connect to the ISP modem.

Go to Network > Interfaces

Select ethernet 1/1 to configure the port. Set the interface type to Layer 3, set Virtual Router to default, and set the Security Zone to Untrust-L3.



Click on IPv4. If the ISP modem automatically assigns addresses, select DHCP client. A DHCP address may not be assigned until the firewall is restarted.

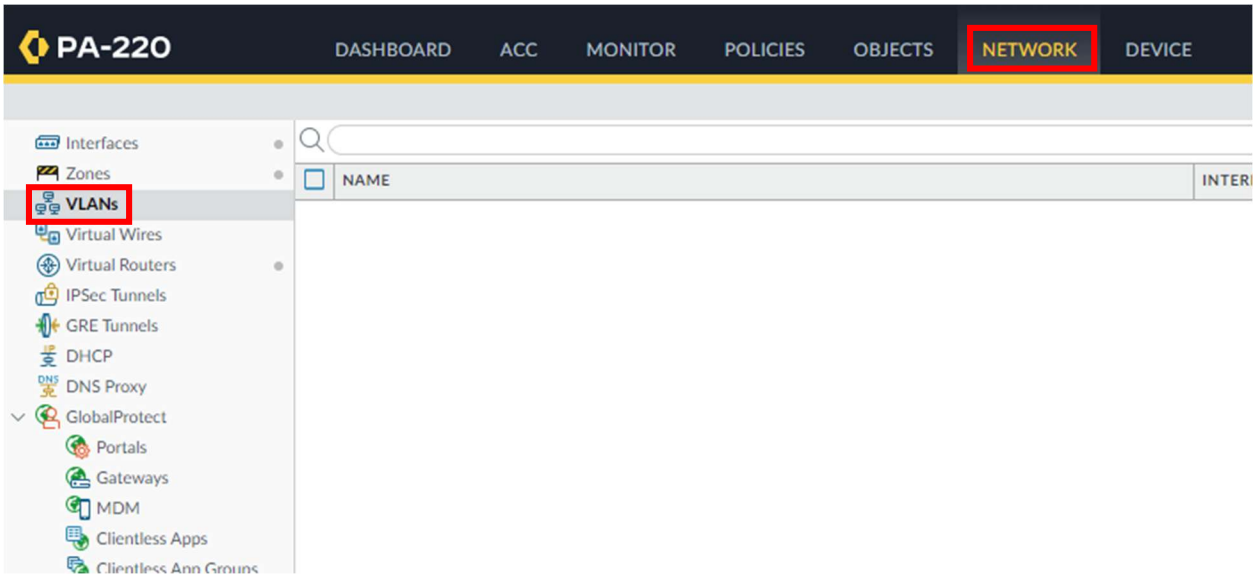


Otherwise, select Static, and add the static IP address/network mask that you would like to use. Then, go to Network > Virtual Routers > “default” > Static Routes > IPv4 and add a static route going to the ISP’s next hop address.

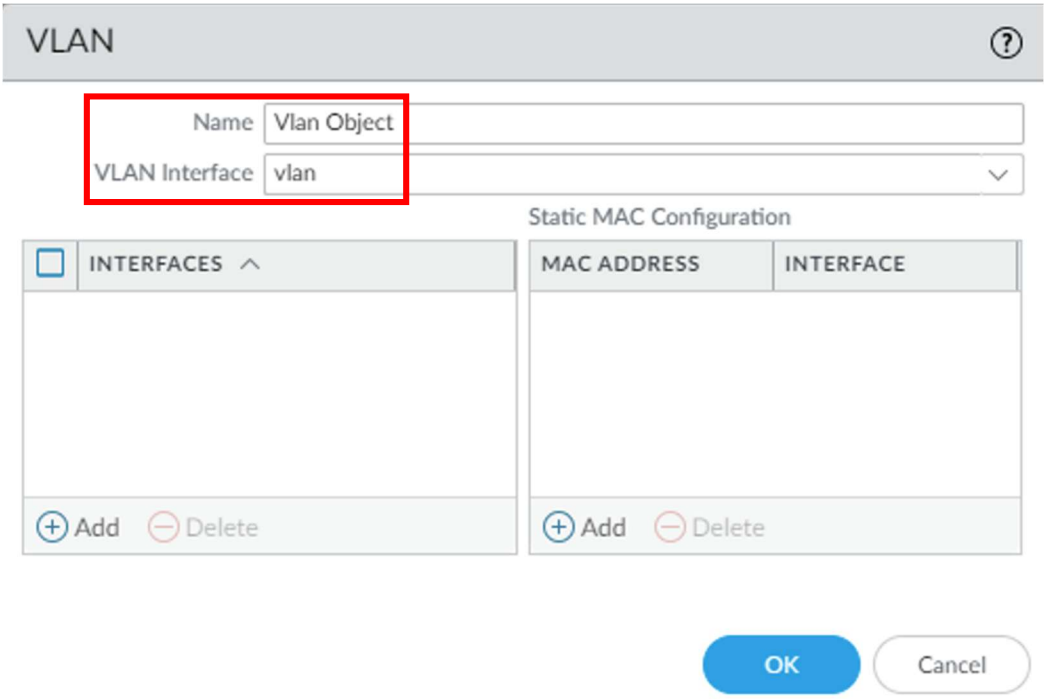
VLAN configuration

Connect the router to the ISP modem. In this example, port ethernet 1/2 is used.

Go to Network > VLANs.



Click Add at the bottom of the page to create a VLAN. Name is “Vlan Object” and set the interface to “vlan”

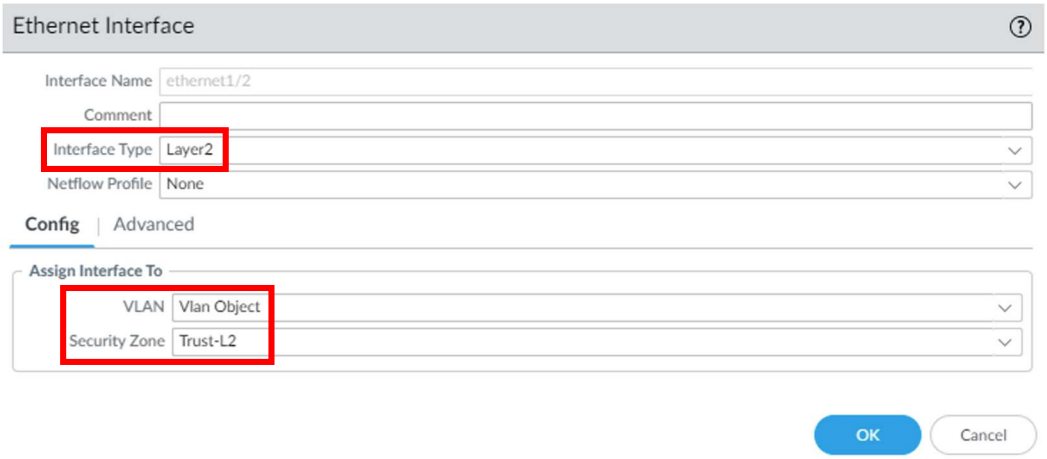


Layer 2 Configuration

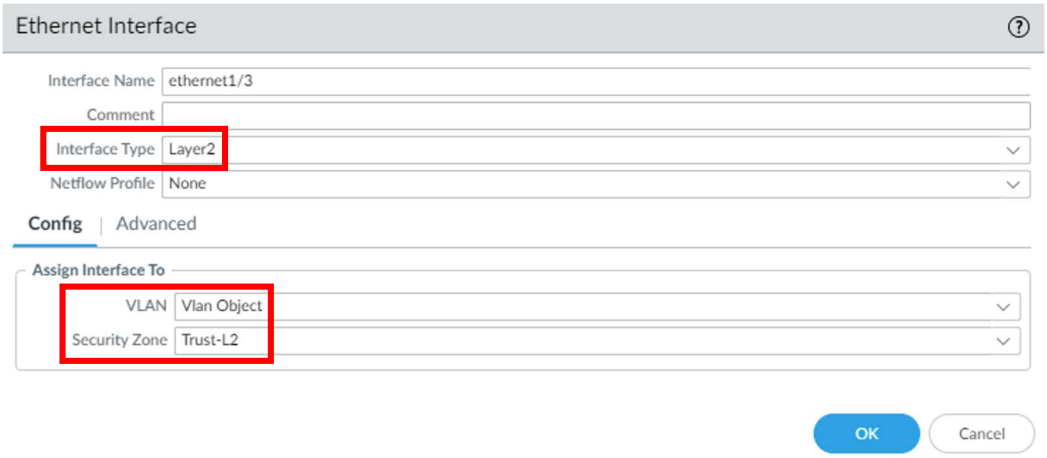
Go back to Network > Interfaces

Configure three interfaces as shown. In this example, ports 1/2, 1/3, and 1/4 are used.

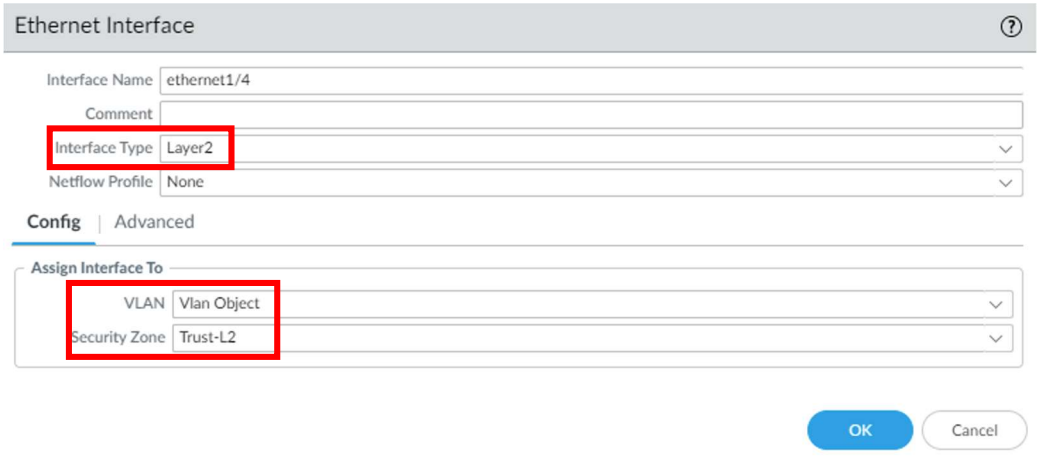
- Ethernet 1/2:



- Ethernet 1/3:



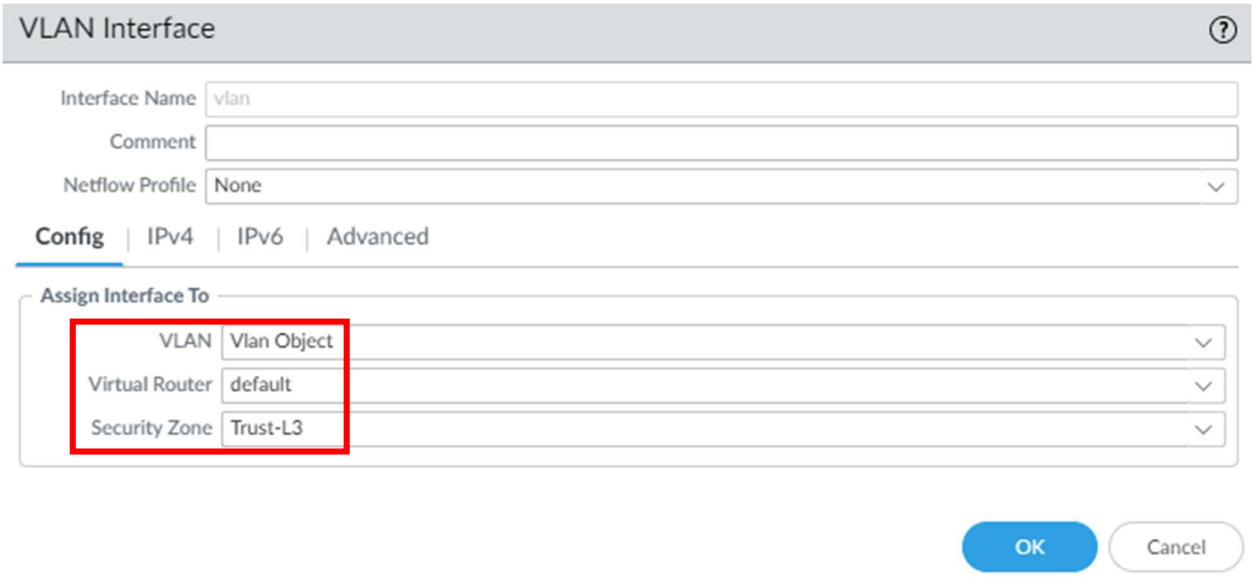
- Ethernet 1/4:

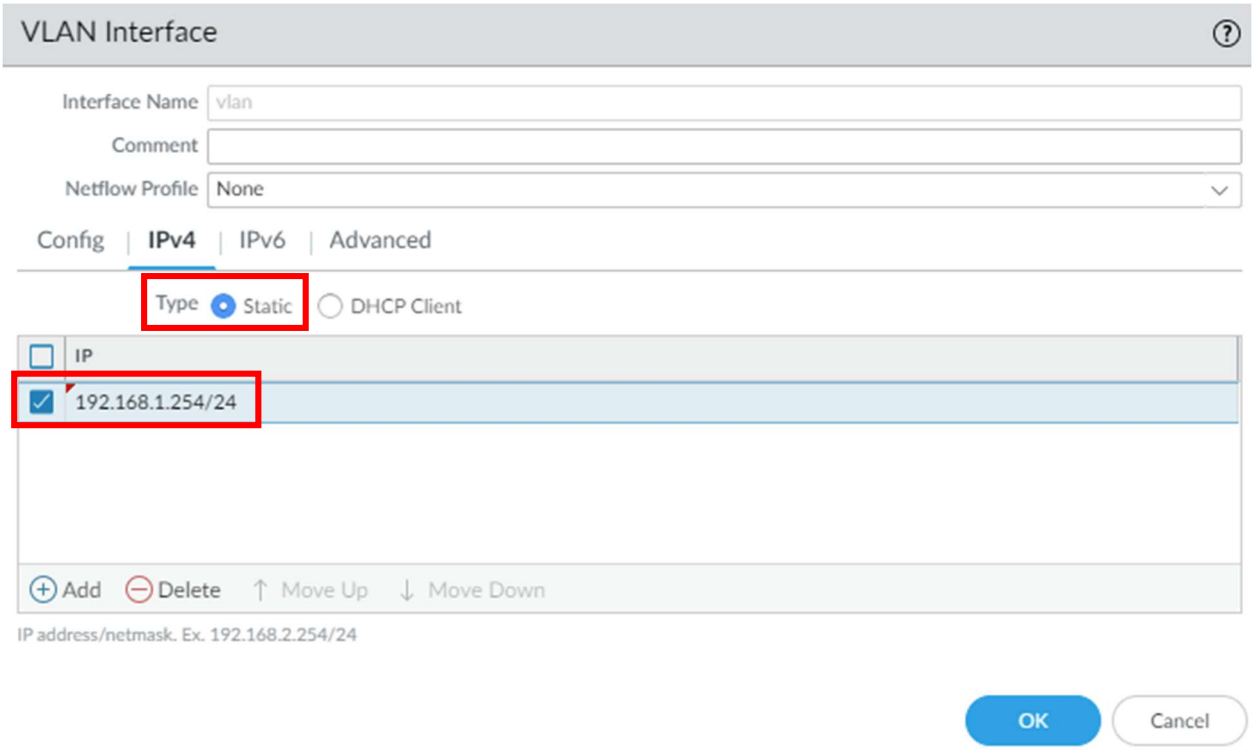


VLAN Interface Configuration

On the Interfaces page, enter the VLAN tab at the top.

Configure the VLAN interface as shown:

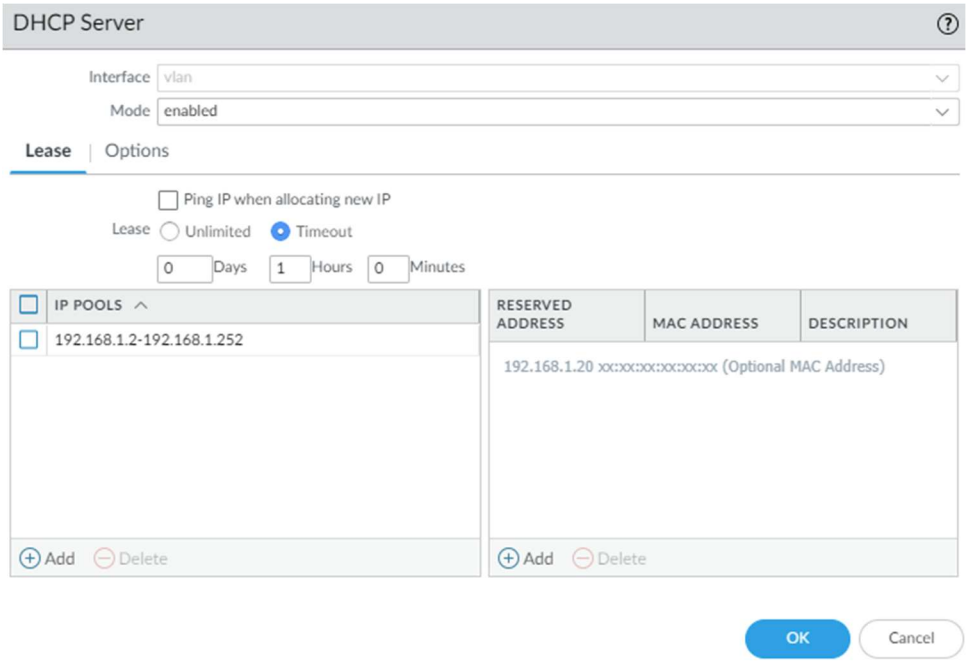


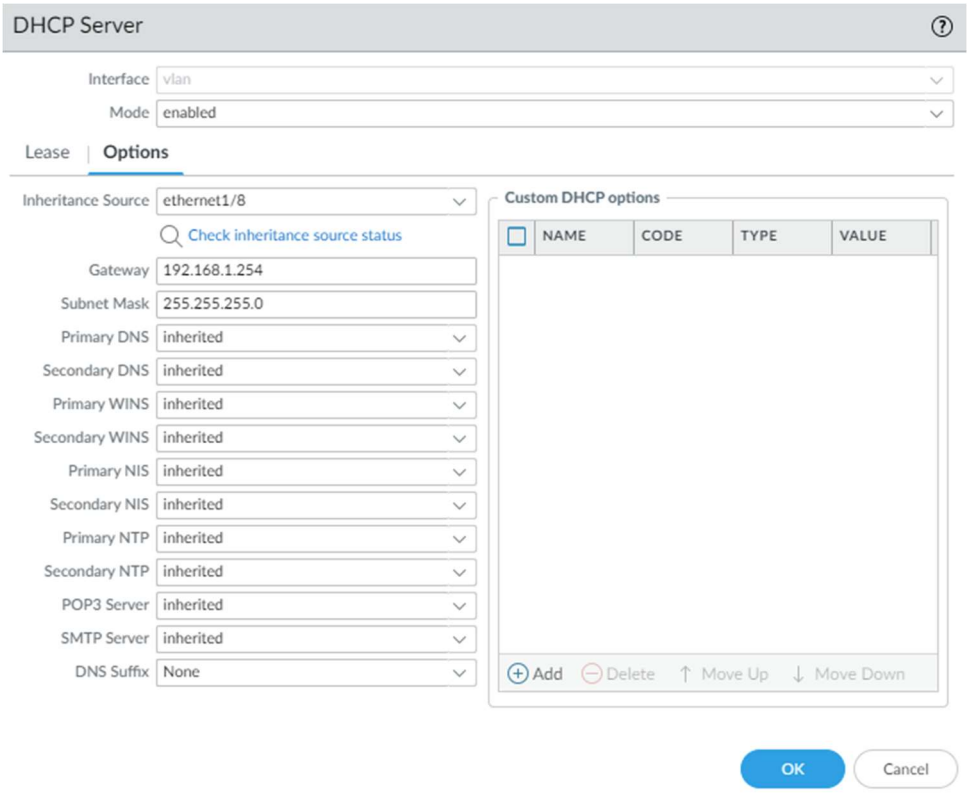


DHCP Server Configuration

Go to Network > DHCP > DHCP Server

Click “Add” at the bottom and configure the settings as shown.

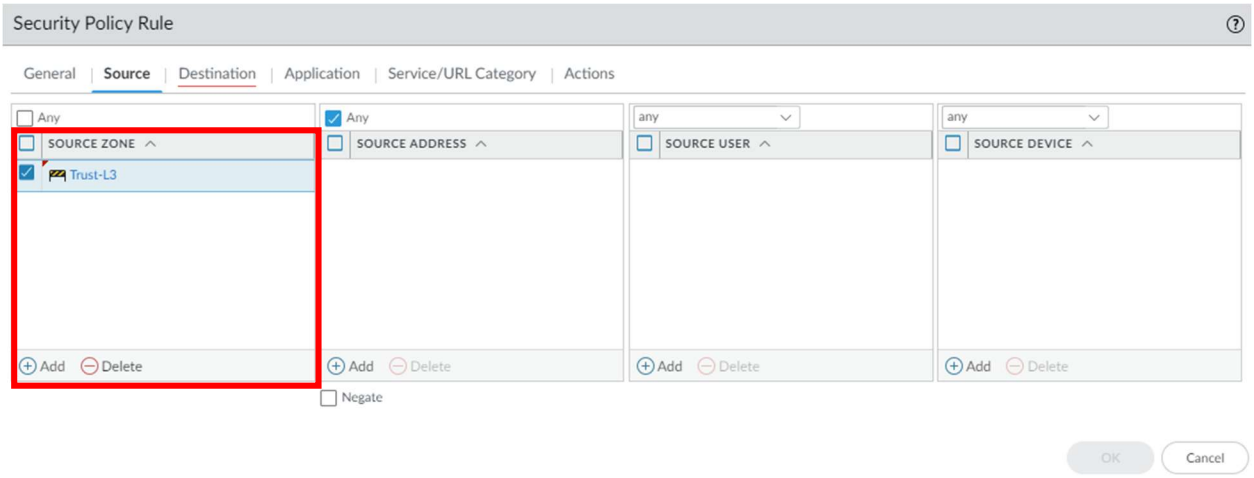


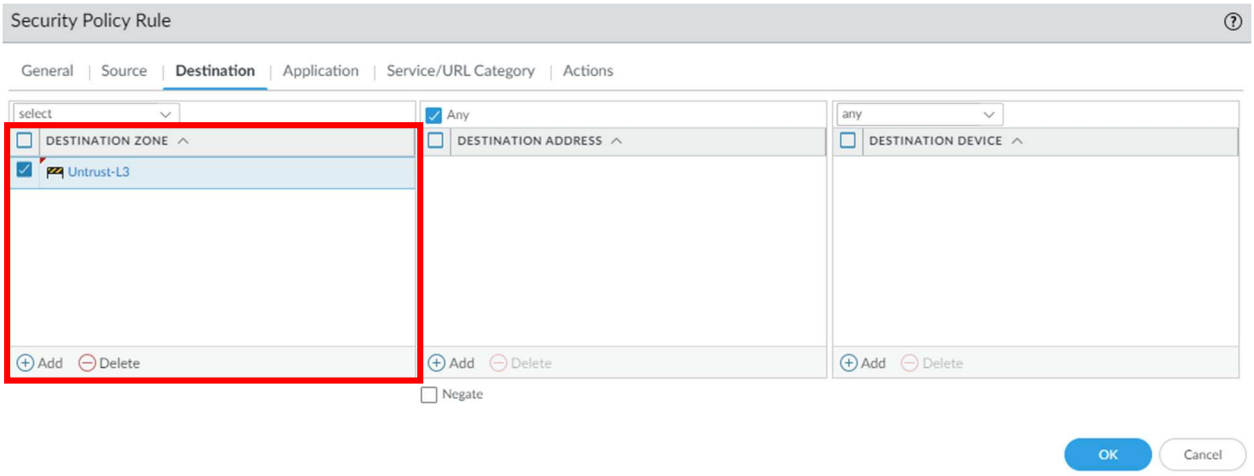


Security Profile Group Configuration

Go to Security > Policies

Click “Add” at the bottom and configure the settings as shown. Add a name of “Internet Outgoing” and a description under the “General” tab.





Under the “Actions” tab, set the “Action Setting” to “Allow”. There should now be 4 rules as shown below.

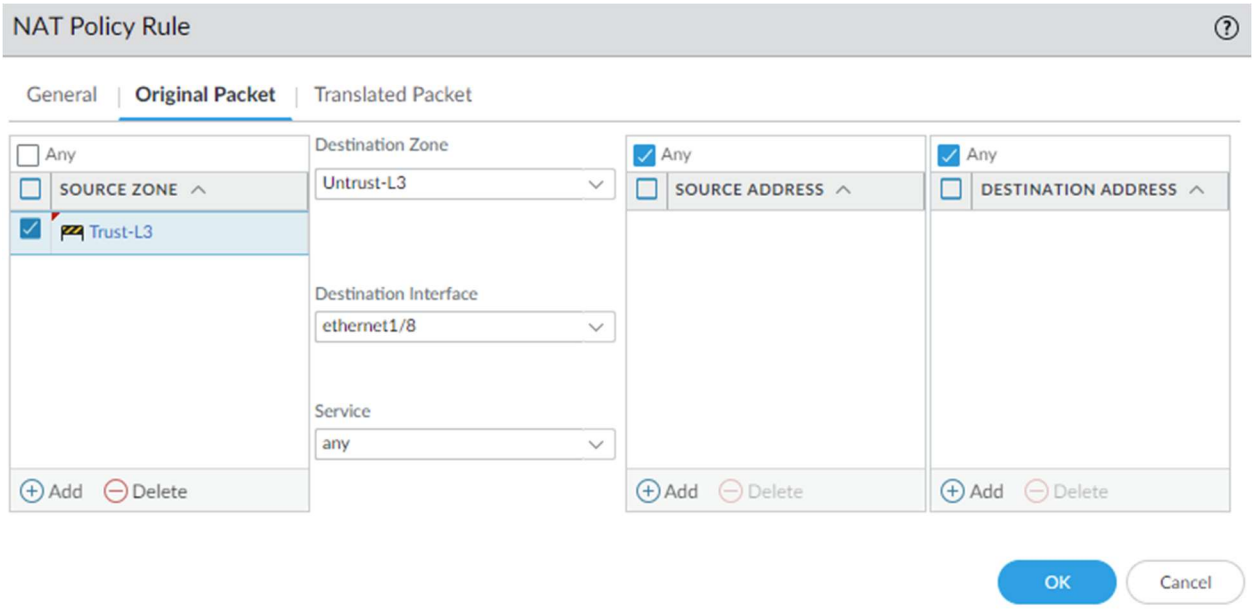
	NAME	TAGS	TYPE	Source ZONE	Source ADDRESS	Source USER	Source DEVICE	Destination ZONE	Destination ADDRESS	Destination DEVICE	APPLICATION	SERVICE	ACTION
1	rule1	none	universal	trust	any	any	any	untrust	any	any	any	any	Allow
2	Internet Outgoing	none	universal	Trust-L3	any	any	any	Untrust-L3	any	any	any	application-...	Allow
3	intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any	any	any	Allow
4	interzone-default	none	interzone	any	any	any	any	any	any	any	any	any	Deny

Outbound Internet NAT Policy Configuration

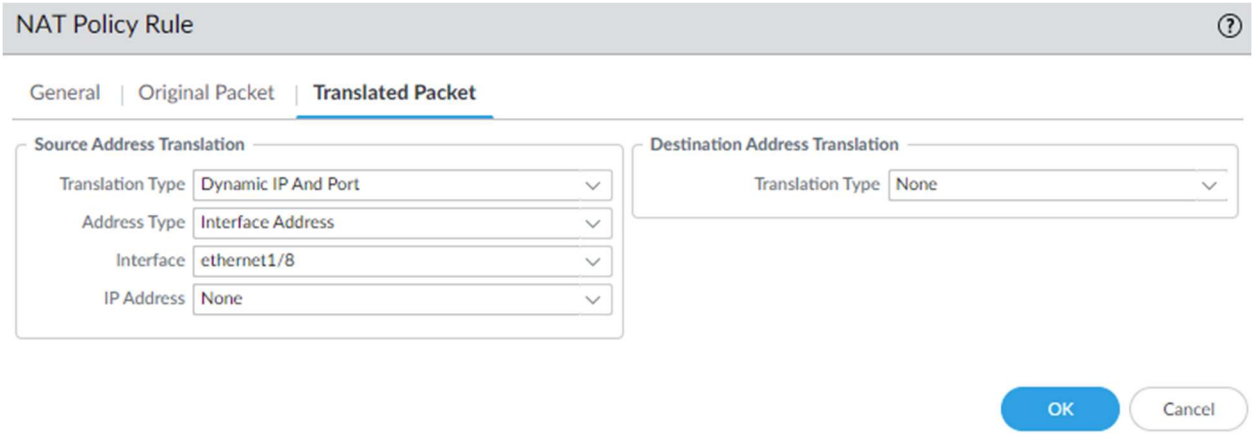
Go to Policies > NAT

Click “Add” at the bottom and configure the settings as shown. Enter the name “Internet Outgoing” and a description in the “General” tab.

For the destination interface, use the port that connects to the ISP modem. In this example, ethernet1/8 is used.



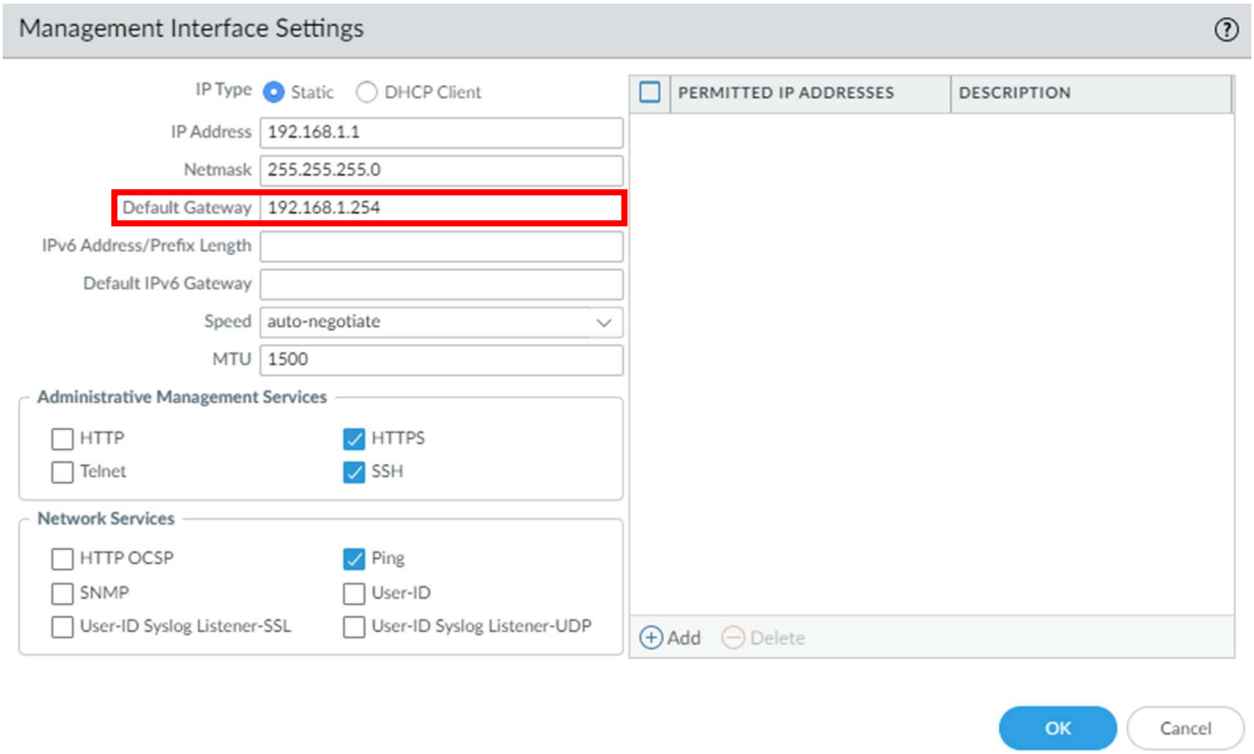
Similarly, use the port that connects to the ISP modem for the interface under “Source Address Translation”.



Management IP Configuration

Go to Device > Setup > Management

Configure the settings as shown.

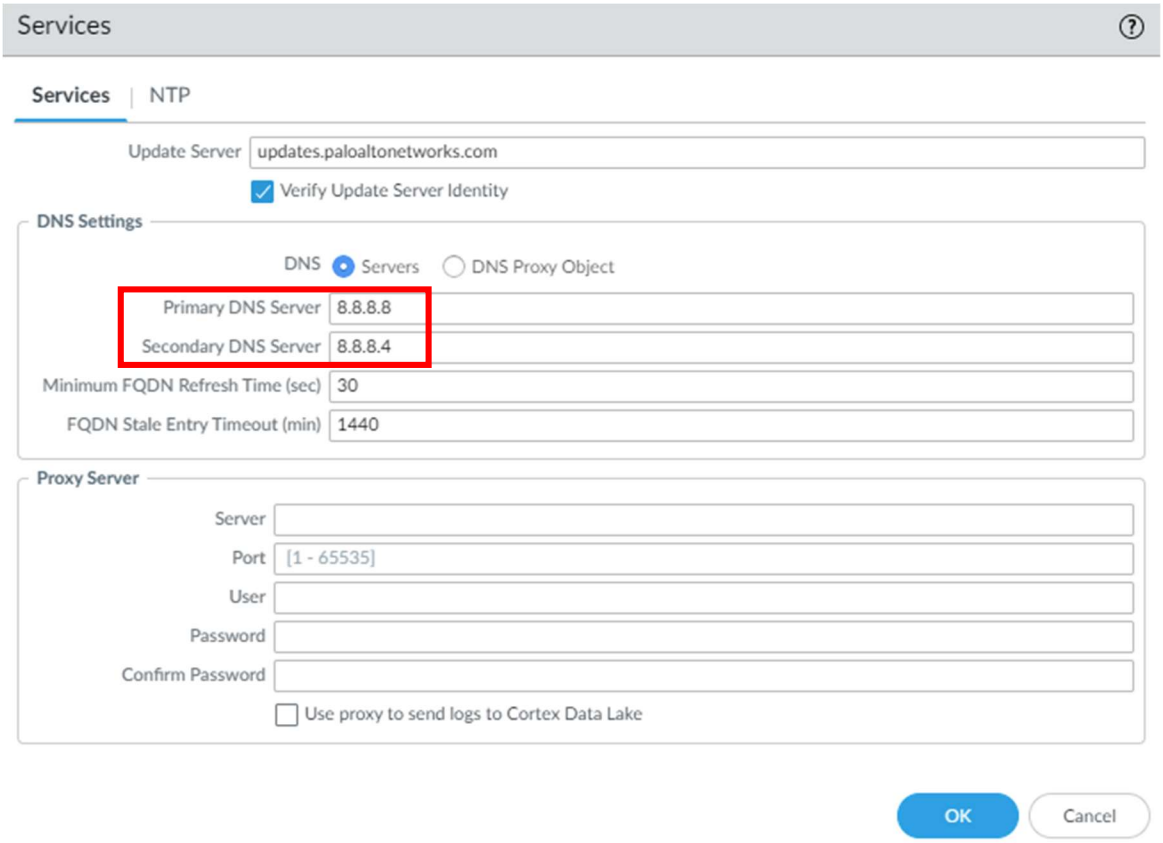


Management DNS Configuration

Go to Device > Setup > Services

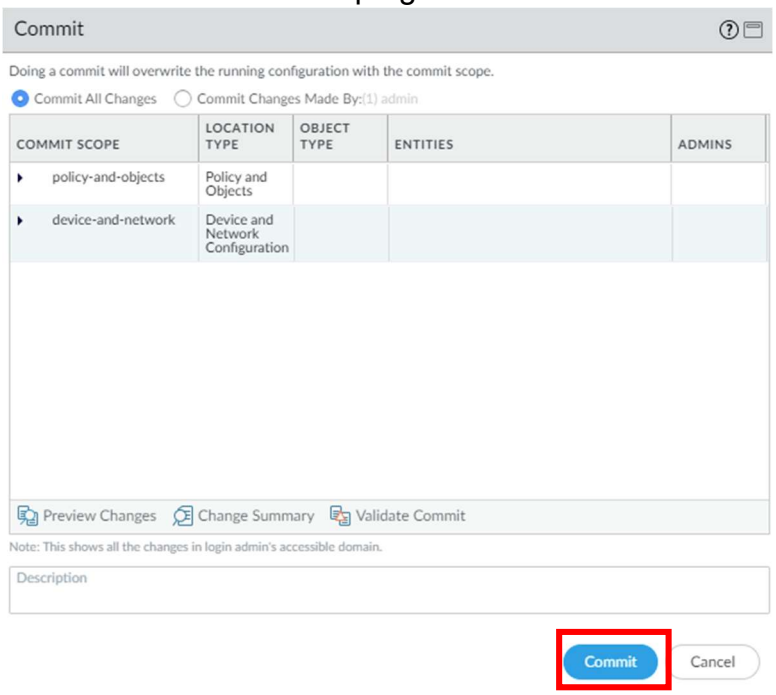
Click on the settings button on the Services section

Enter the DNS Server's IP addresses. In the example, Google's DNS IP's are used, 8.8.8.8 and 8.8.8.4.



Commit Changes

Select “Commit” in the top right of the web interface.



Do not power off the firewall until the commit is finished.

Problems

We were unable to get a DHCP address after setting the ISP interface. This was most likely due to a faulty firewall. After switching out the firewall and using committing the changes, we were able to get a DHCP address.

We were unable to commit to do a default setting in the firewall configuration. After deleting the default Virtual Wire, we were able to commit our changes.

Conclusion

In this lab, we successfully configured a firewall in a SOHO network. We were able to give to end devices through DHCP, set Security policies to enable filtering of traffic coming from the internet, and connect end devices to the internet through the firewall.

PA-220 URL Filtering

Purpose

The purpose of this lab is to set up URL filtering on a firewall suited for a student in elementary school. As such, sites inappropriate for this age group should be blocked, sites that may have some use but should be generally blocked should have an admin override, and educational sites should be unblocked.

Background Information

URL Filtering is a method used to restrict access to websites and online resources based on their URL (Uniform Resource Locator). URL filtering can be implemented by firewalls, servers, or software on devices. It is used to block access to harmful websites, restrict certain categories of content, and enforce company policies for internet use.

Whenever a user wishes to access a certain website, they must first send a request to a DNS server, which will translate the URL into an IP address. When URL filtering is enabled, a firewall can intercept this request and allow or block it from going forward. After interception, the URL will be compared to a known database of URLs and sorted in a category, such as “gaming”, “social media”, or “adult content”. Based on what the administrator has configured for the category, the firewall will allow or block the DNS request.

If the request is blocked, a safe page (such as a “Blocked” page) will be displayed, informing the user that the content they tried to access is not permitted.

The administrator may set some categories to have an administrative override. An override is useful in the case that a student may need to access a page for a project, or a teacher needs to use a site to access resources. This override has a configurable time limit.

With the introduction of HTTPS (Hypertext Transfer Protocol Secure), the firewall requires a certificate in order to properly decrypt traffic and detect that a website is within either a blocked or allowed category. In addition, the device accessing the internet through the firewall also requires a root certificate to be installed.

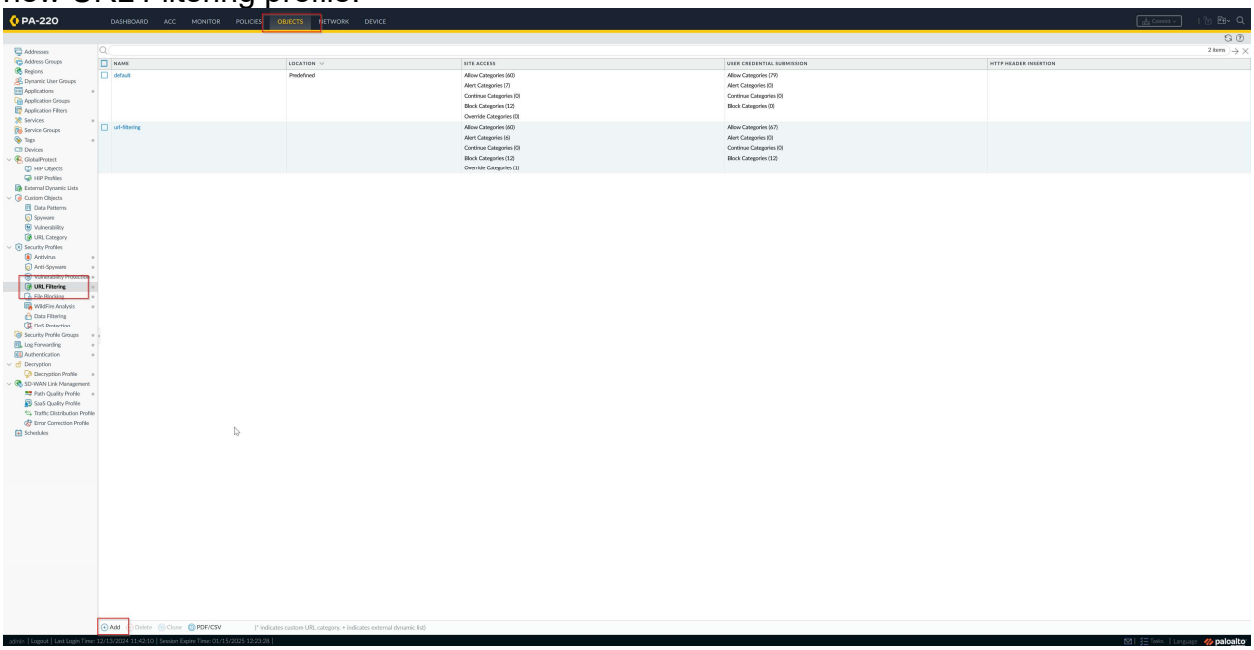
When using a PA-220 or any Palo Alto firewall, one must purchase an Advanced URL Filtering license in order to utilize URL filtering. Palo Alto, in addition to categories each URL, also assigns a risk category that indicates how likely a site will expose the user to threats. These risk categories allow administrators to block unsafe sites generally instead of blocking individual categories, which may be easier to set up, but gives the administrator less granular control. Palo Alto also allows the creation of custom URL categories consists of two or more other categories, allowing the enforcement for any webpage satisfying all of a certain number of categories.

Lab Summary

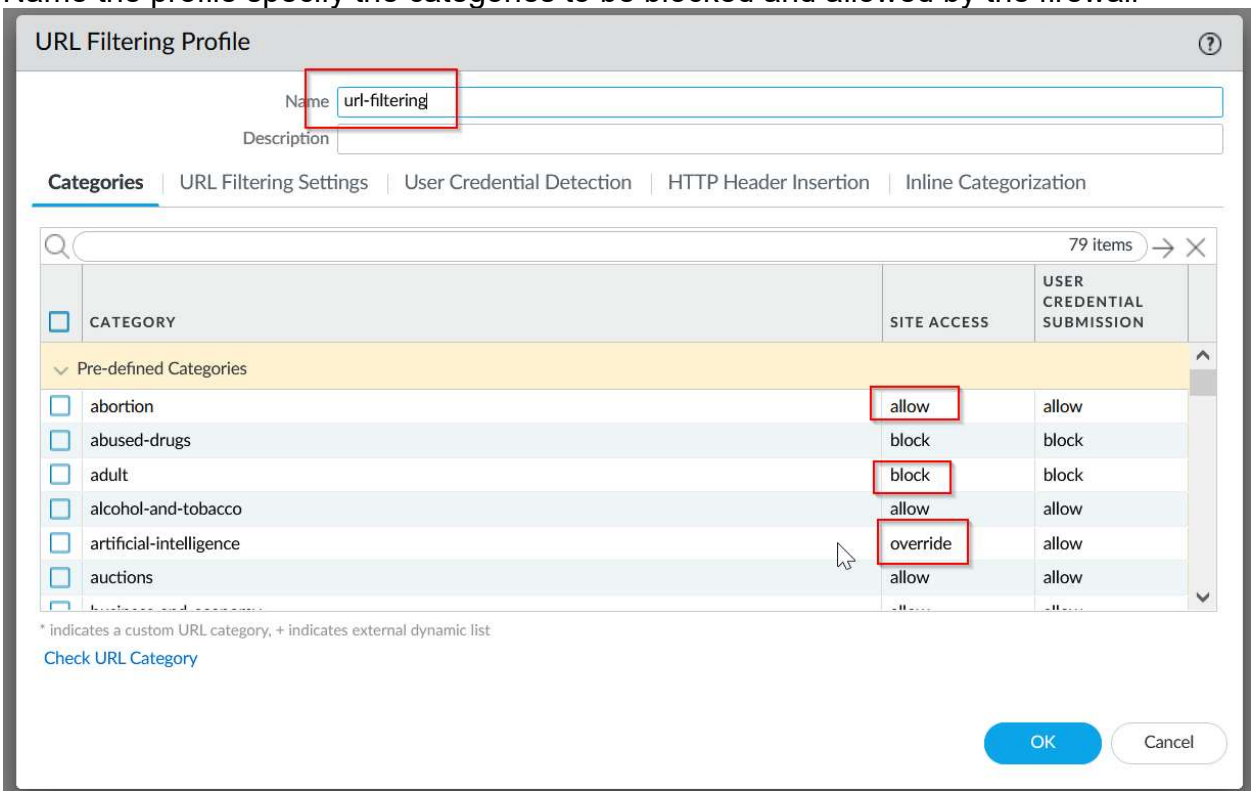
In this lab, you will configure a URL Filtering profile on a PA-220 firewall and apply the profile to traffic going through the firewall. You will also configure certificates on the firewall and an end device to allow the PA-220 to filter HTTPS traffic.

Configurations

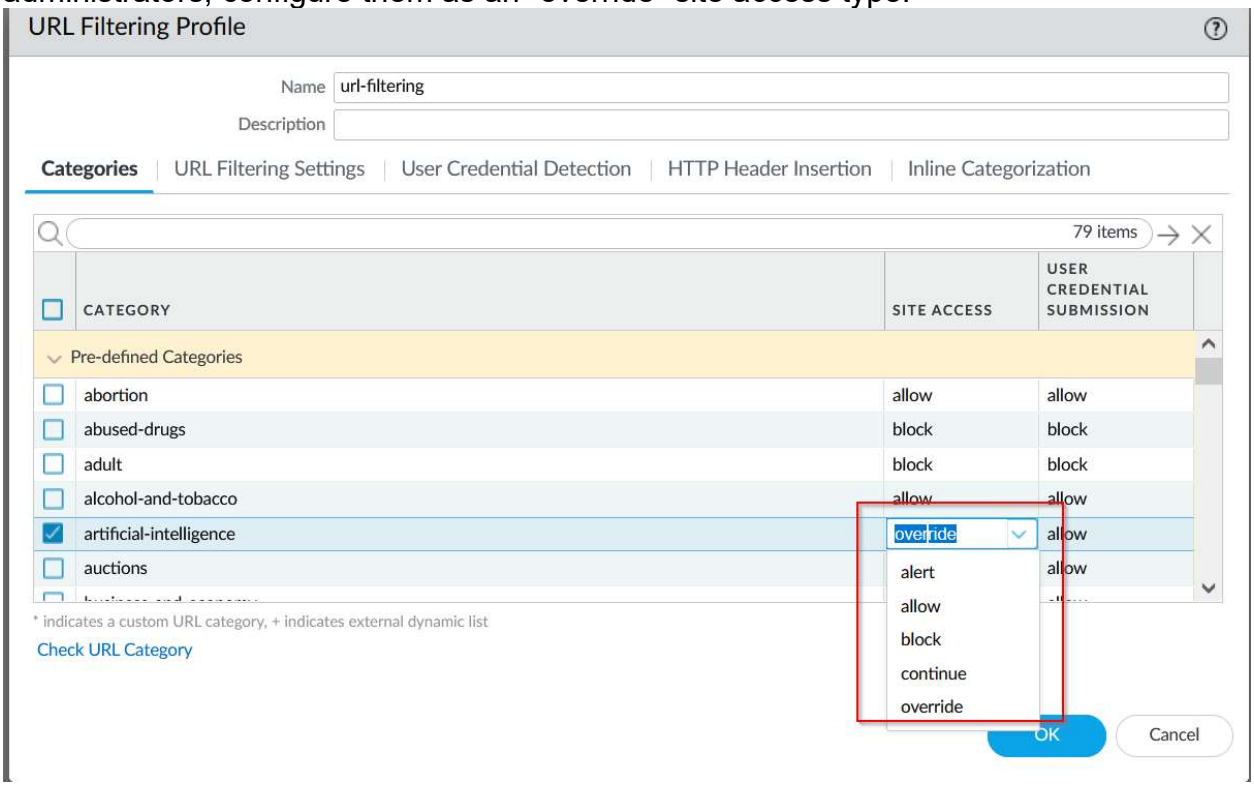
1) Navigate to Objects > Security Profiles > URL Filtering. Press Add to create a new URL Filtering profile.



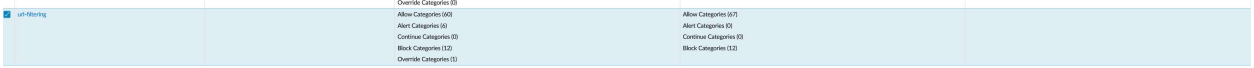
2) Name the profile specify the categories to be blocked and allowed by the firewall



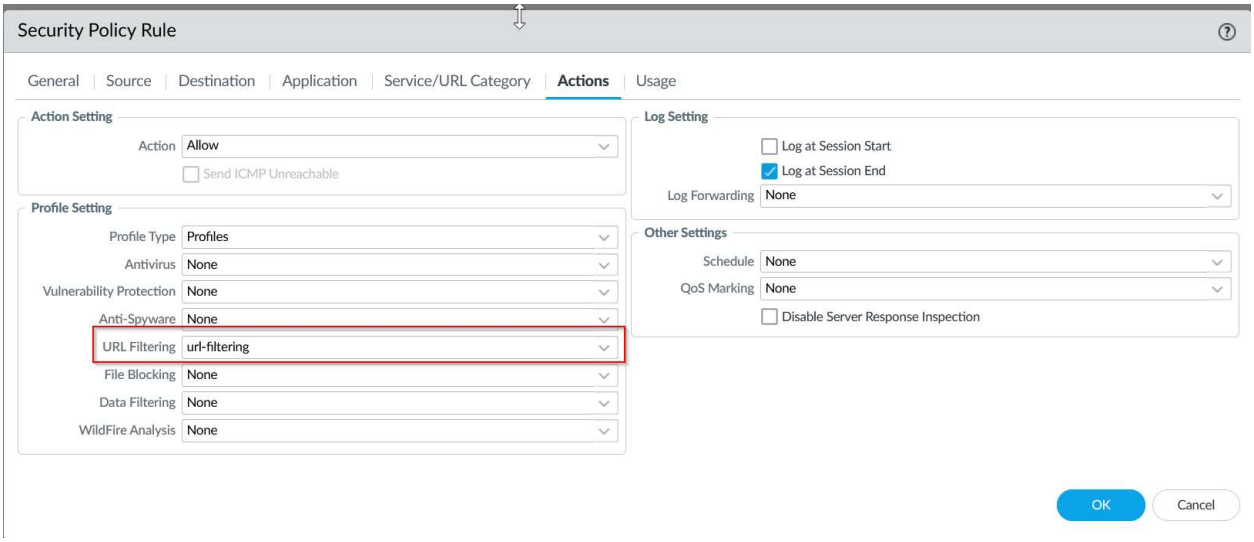
3) For categories for which there should be an override for individuals or administrators, configure them as an “override” site access type.



4) Keep the other settings the same and create the profile by pressing “Ok”.

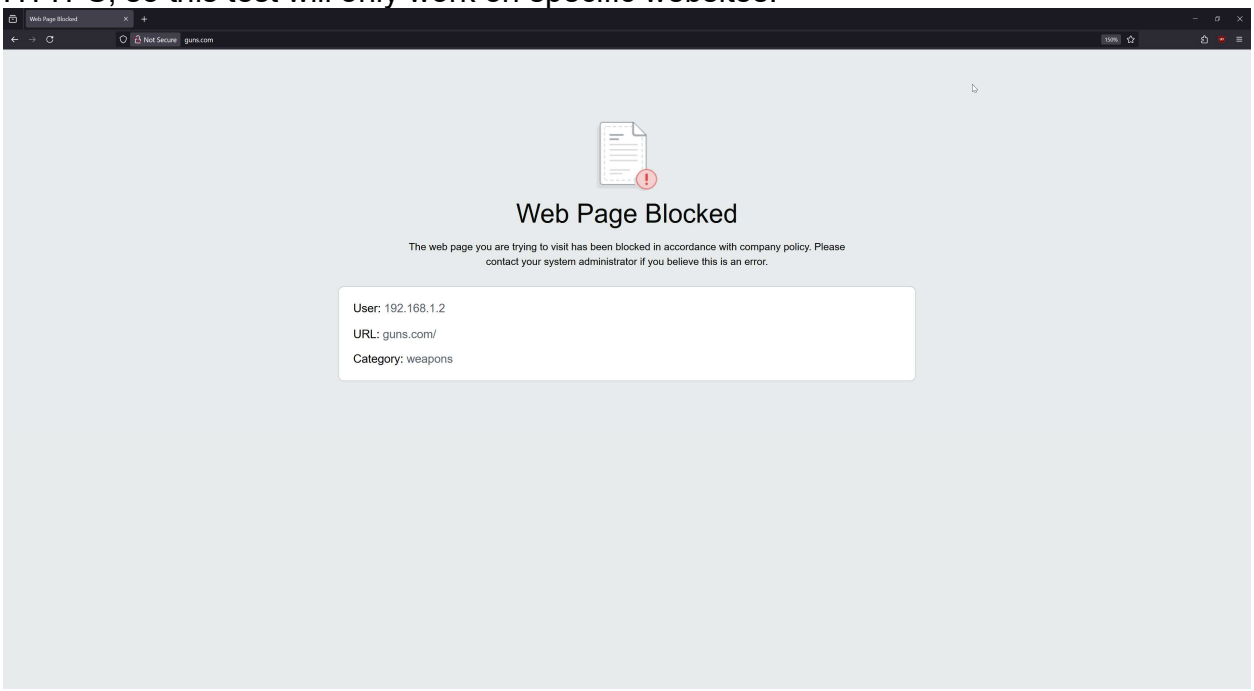


5) Navigate to Policies > Security. Apply the profile to the “outgoing” security policy to filter out websites. Go to the “Actions” section and select the profile you just created.



6) Press “Ok” and commit changes. Now, the URL Filtering should work for HTTP websites ONLY. Check that it works like a website like http://guns.com. Note that

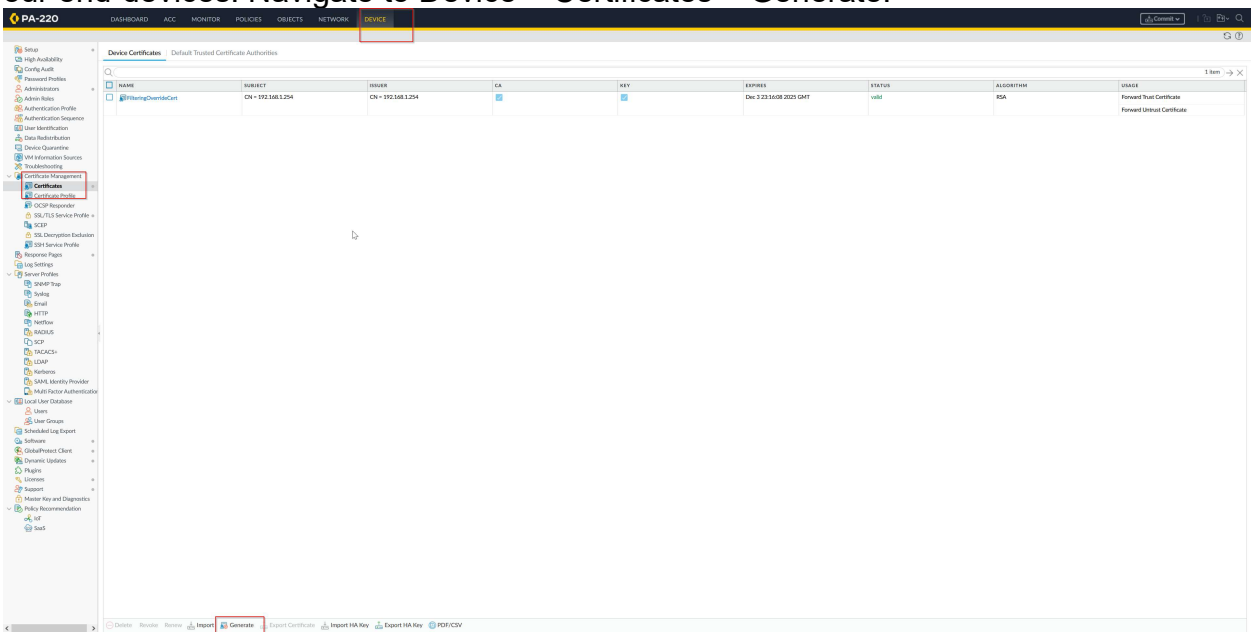
only some websites allow HTTP traffic, others will automatically redirect to HTTPS, so this test will only work on specific websites.



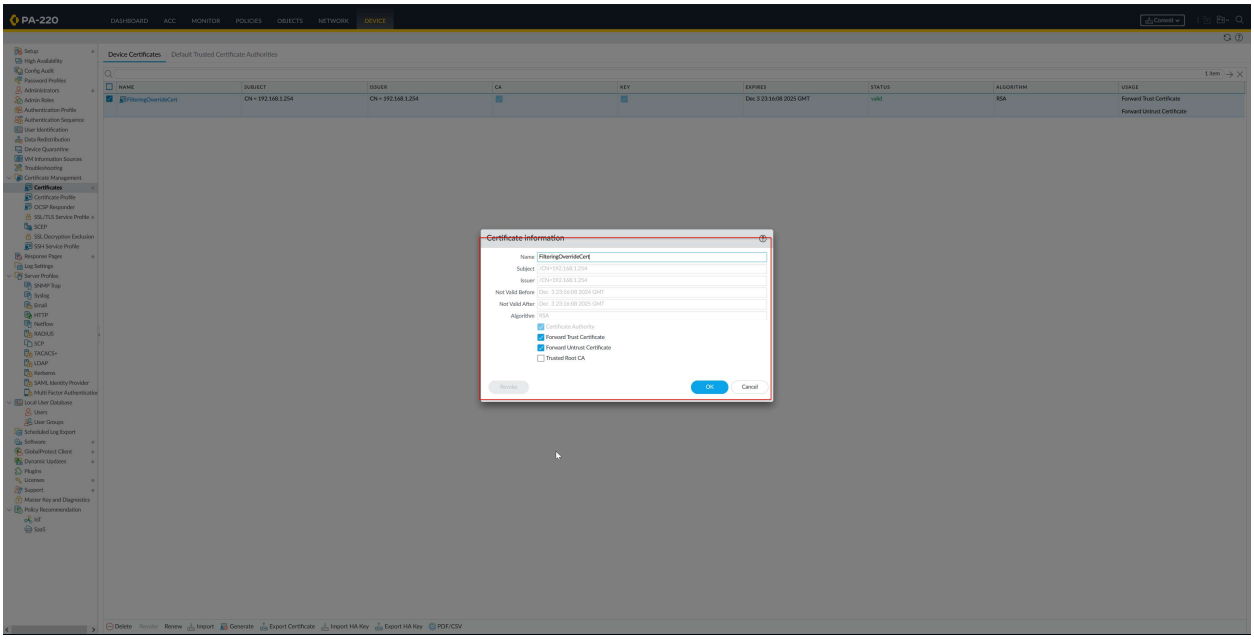
7) Certificates are needed in order to enable HTTPS filtering to work. Console into your firewall and enter this command to enable the firewall to decrypt traffic to insert the block page.

   # set deviceconfig setting ssl-decrypt url-proxy yes

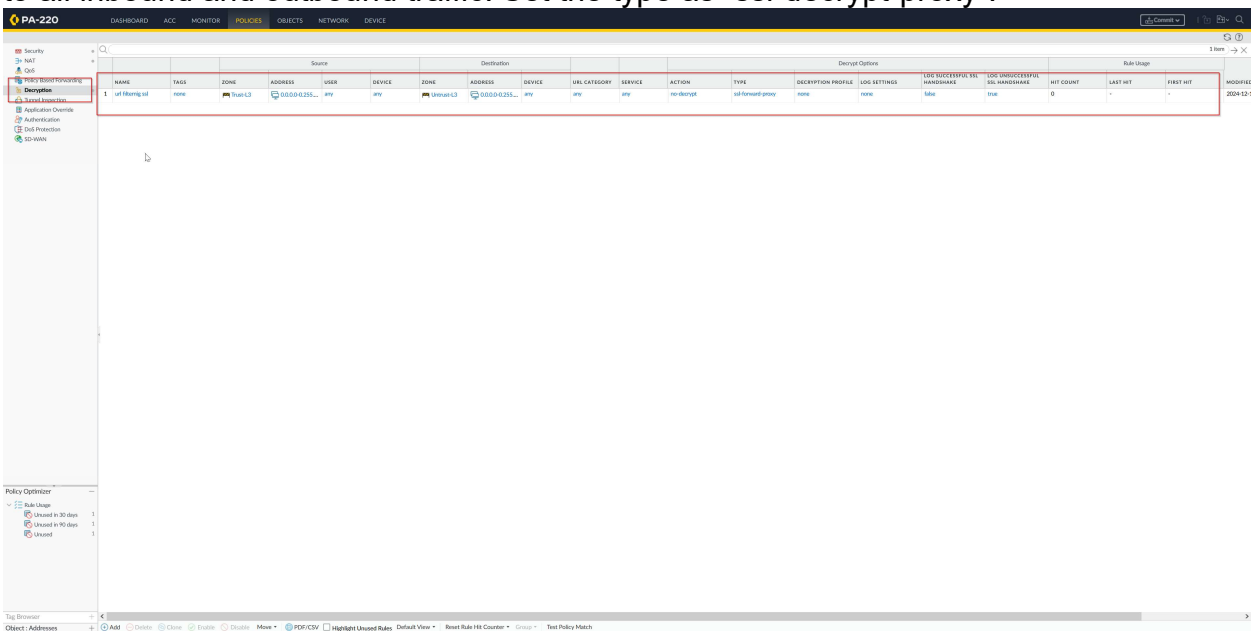
8) Certificates need to be generated for the firewall, which will be later imported into our end-devices. Navigate to Device > Certificates > Generate.



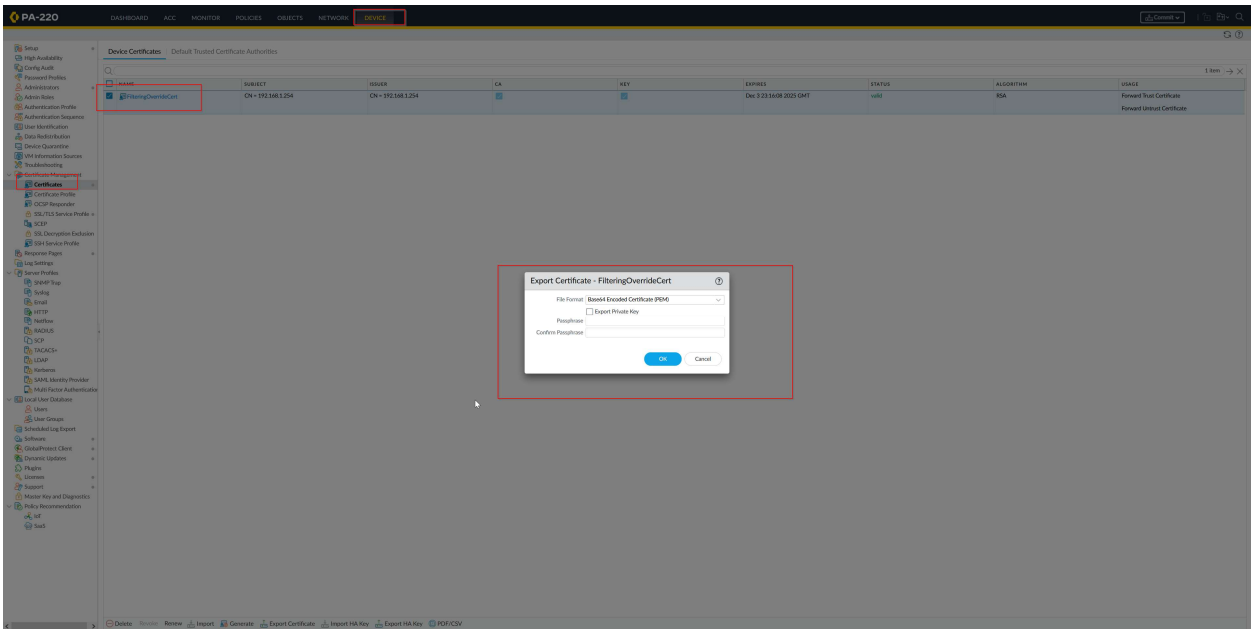
9) Set the following fields. Make sure your default gateway is configured as the correct address.



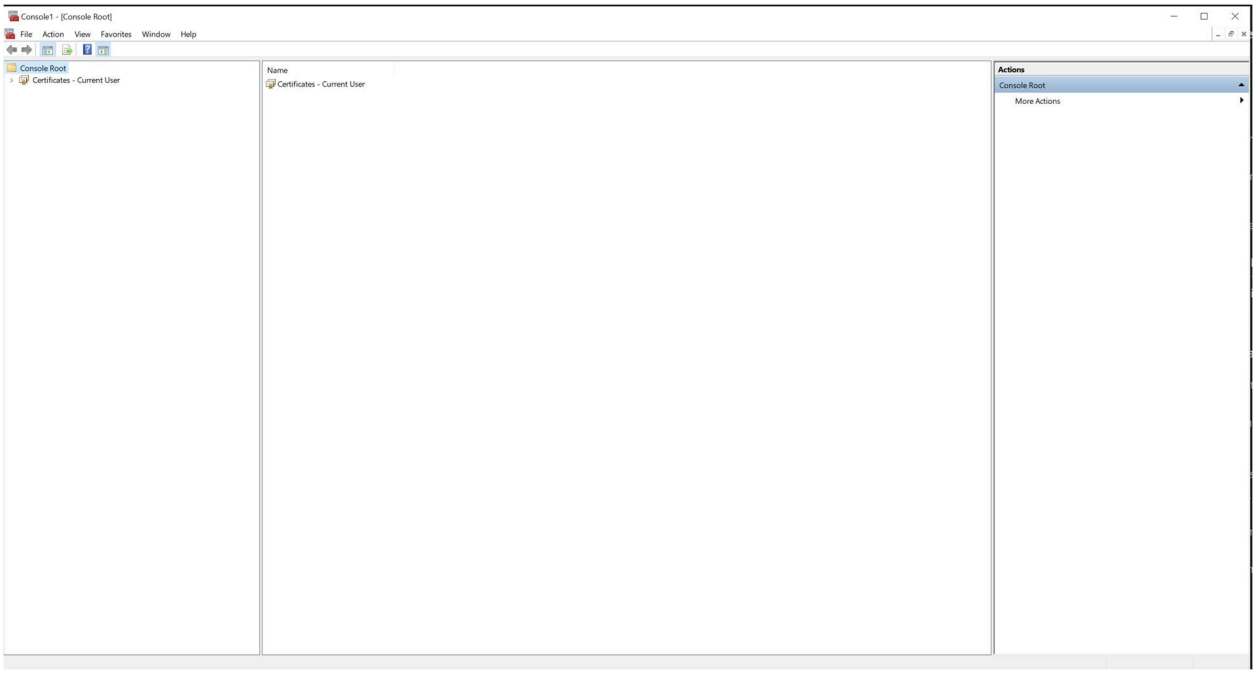
10) Navigate to Policies > Decryption and add a new policy. Make sure it is applied to all inbound and outbound traffic. Set the type as “ssl-decrypt-proxy”.



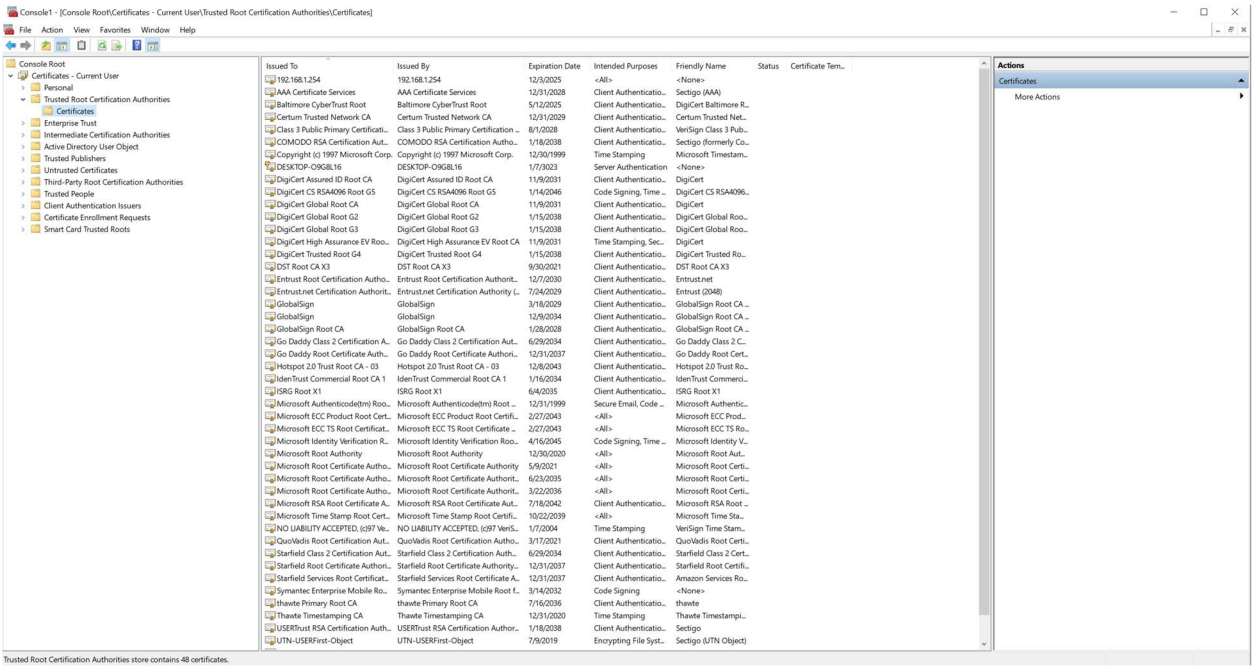
11) Finally, we need to install our Root Certificate on Windows for our end-device. Go back to Device > Certificates > Export Certificate to download the self-signed root certificate.



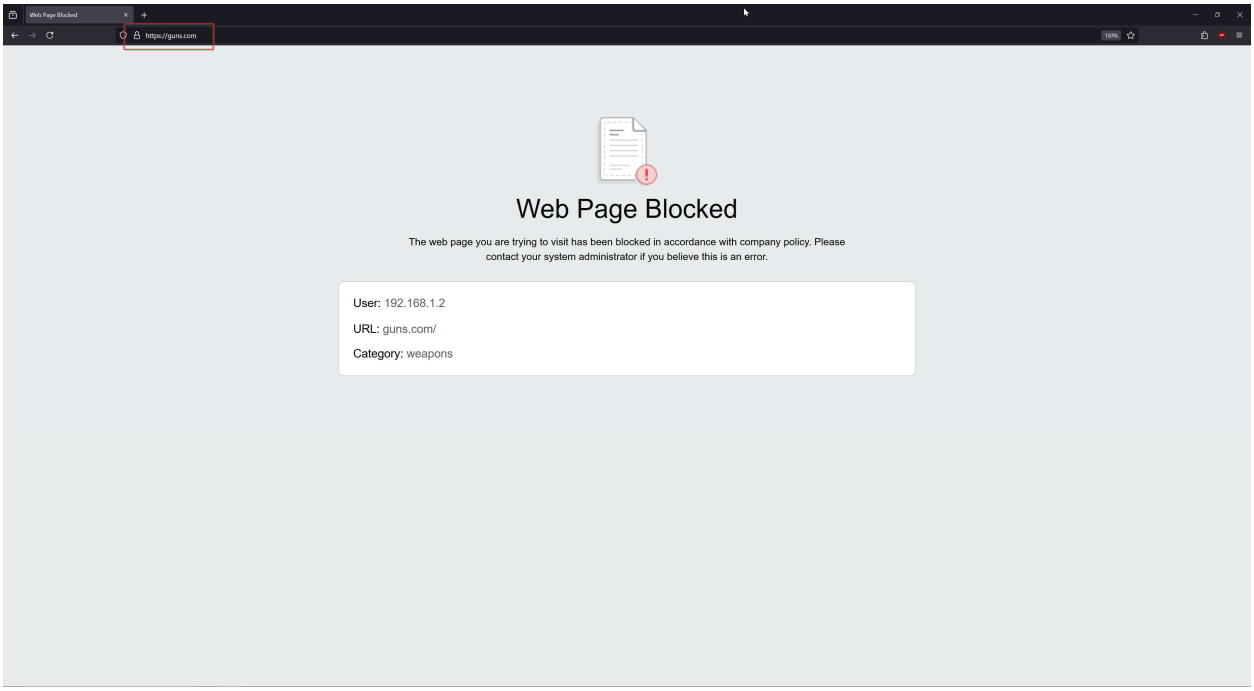
12) Install the root certificate. On Windows, this requires extra permissions. Press “Windows + r” and launch mmc, the Windows management console. Add Certificates to the menu.

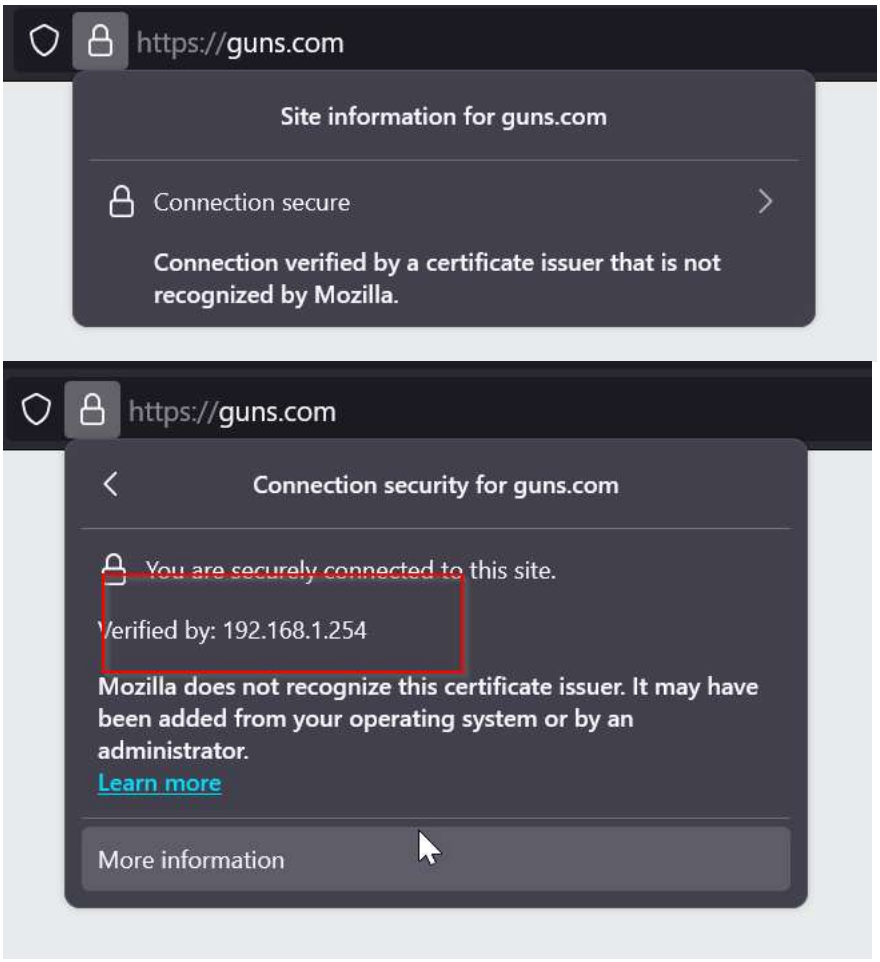


13) Navigate to the Trusted Root Certificate Authorities, and right click to add a new root certificate. Navigate to the download location of the certificate. Add the certificate.

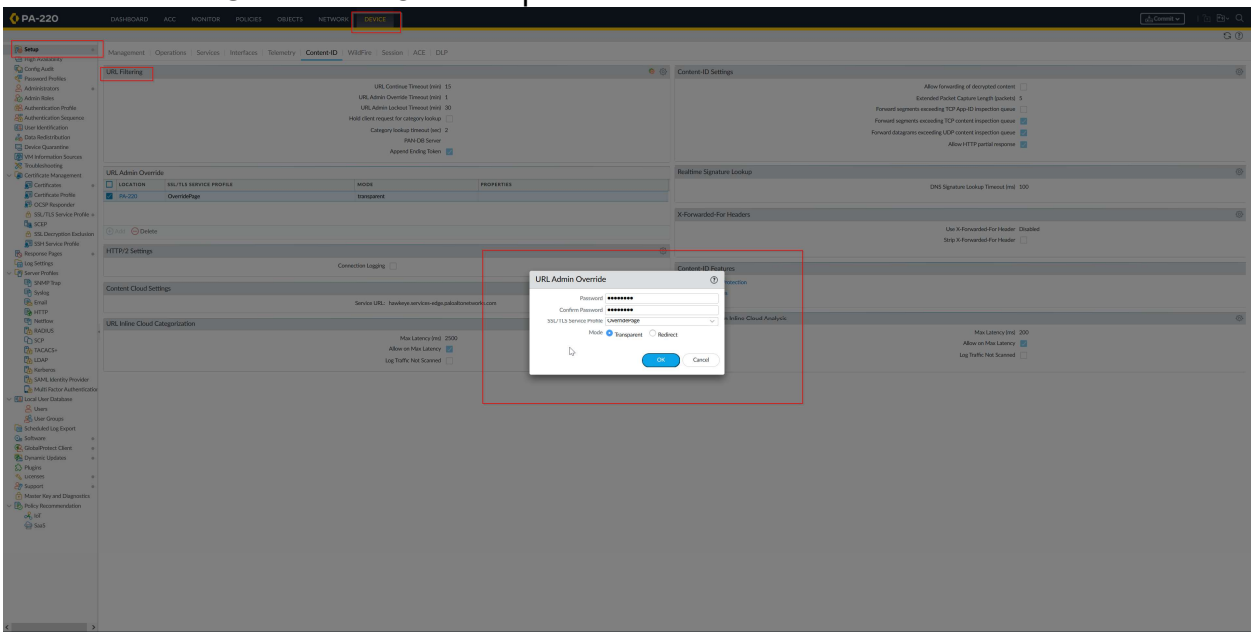


14) The root certificate should now be installed. Verify that HTTPS works with any blocked website.

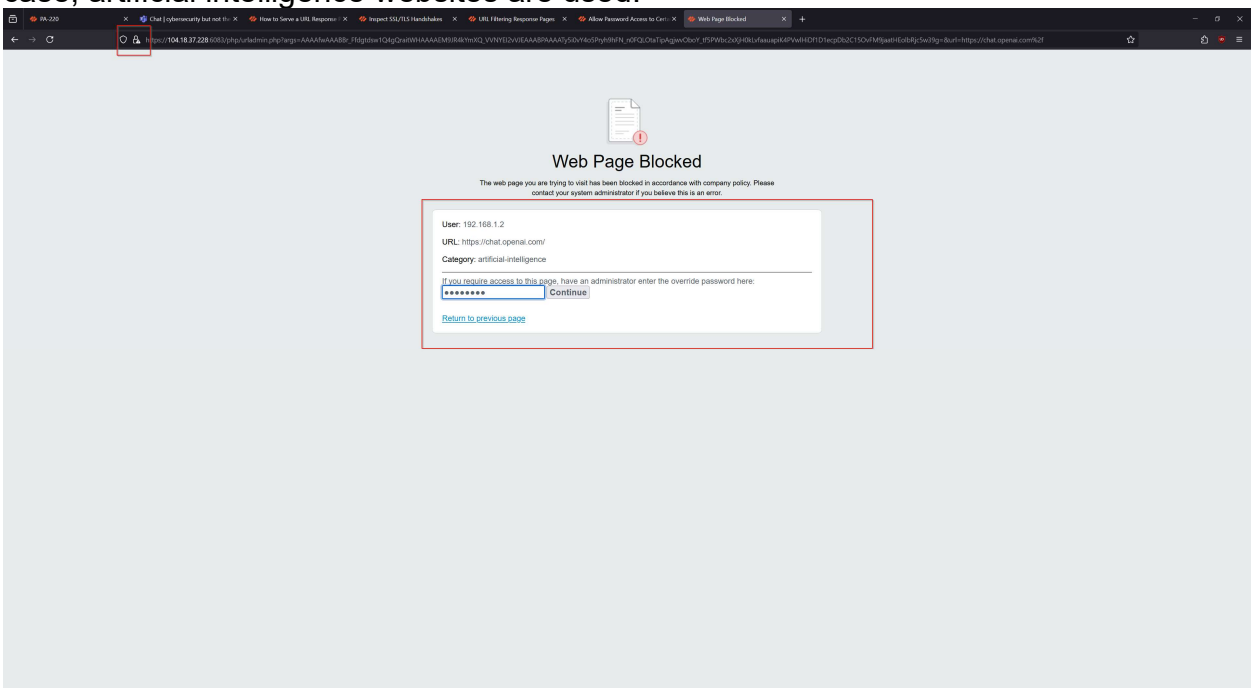




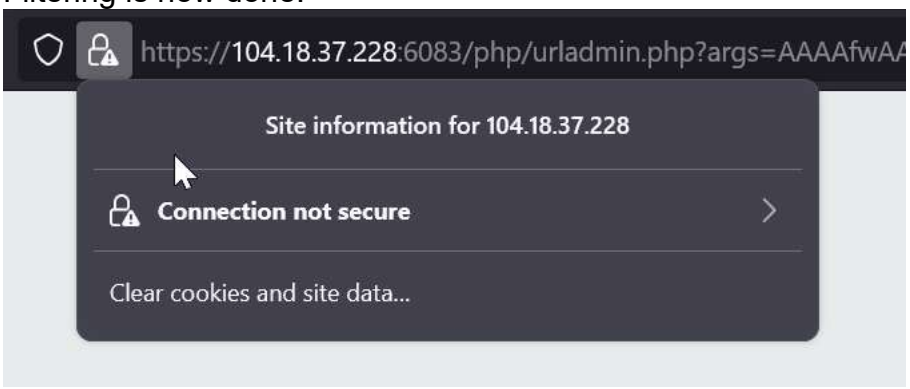
15) We can add the “override” settings now. Go to Device > Setup > URL Filtering and add a new URL Admin Override profile.

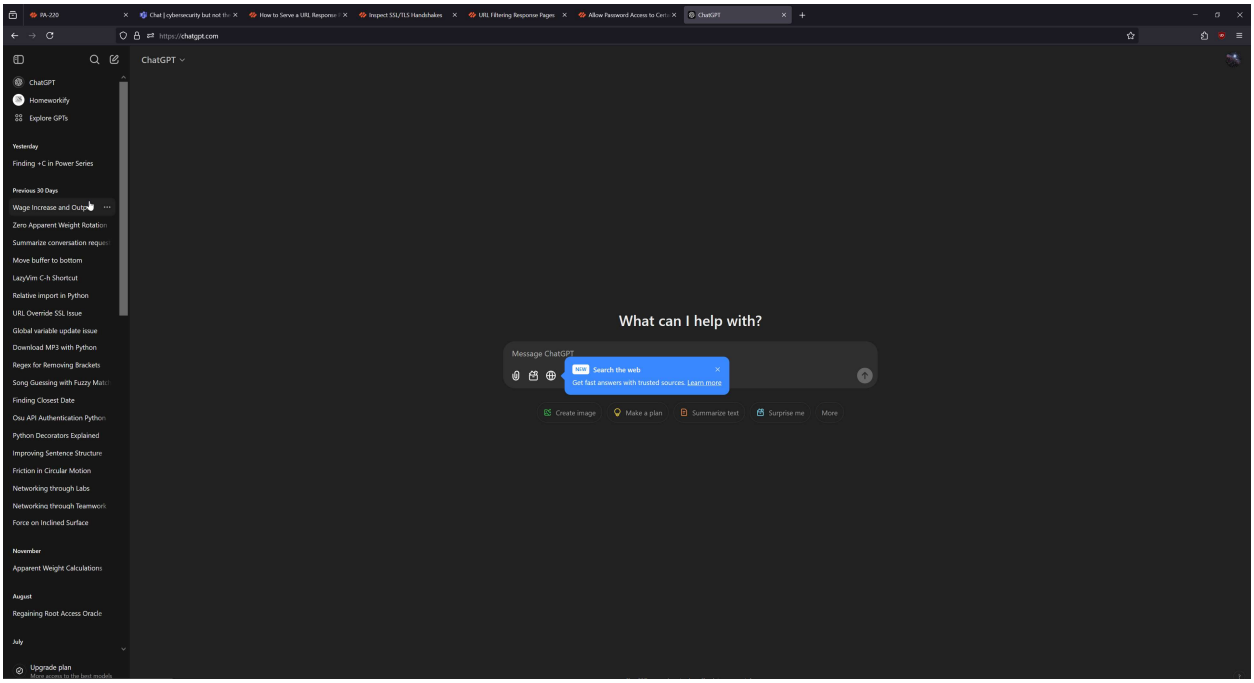


16) Verify that override works with a website that is configured to be override. In this case, artificial intelligence websites are used.



17) Note that the website is shown as “Insecure”, because our certificate is self-signed, however our browser will still allow the connection to go through. URL Filtering is now done!





Problems

(1) In configuring URL filtering, we initially did not know that configuring certificates was required for the firewall to decrypt HTTPS traffic. Thus, a lot of time was spent trying to debug why the firewall was unable to access HTTPS URLS, while being able to filter HTTP URLS.

Conclusion

In this lab, we successfully configured a PA-220 firewall to perform URL filtering on all traffic going through the firewall. In addition, we set up certificates on both the firewall and end device in order to decrypt HTTPS traffic.

PA-220 VPN

Purpose

The purpose of this lab is to set up Global Protect in order to allow one desktop to remotely connect to another desktop from another network.

Background Information

Virtual Private Networks (VPNs) virtually extend a private network into other networks that may be untrusted or need to be isolated. The goal of a VPN is to allow hosts to exchange network messages across another network and access private network, acting as if they were part of the same network. VPNs rely on tunneling protocols, which transfer network messages from one network to another. Tunneling protocols involve encapsulating and repackaging traffic data into another form, sometimes with encryption. Because of this, tunneling protocols, and thus VPNs, are able to hide the nature of the traffic run through them.

VPNs are able to be used for remote access. Remote access allows one user to access another device connected via the internet or another network and is widely used for technical troubleshooting of customer's problems. They also provide an advantage in security development, since companies are able to permit remote employees to operate from a secure computer within the companies environment.

Global Protect is Palo Alto's VPN software which allows firewall-based policies to be applied to all users, no matter what their physical location is. Global Protect is comprised of the GlobalProtect Portal, GlobalProtect Gateways, and the GlobalProtect App.

GlobalProtect Portal provides the management functions. Every endpoint receives their configuration information from the portal, including all gateways and client certificates. The portal also distributes the GlobalProtect app when accessing it through the internet. GlobalProtect Gateways help to secure traffic from GlobalProtect apps. GlobalProtect App runs on end devices and endpoints, enabling access to network resources.

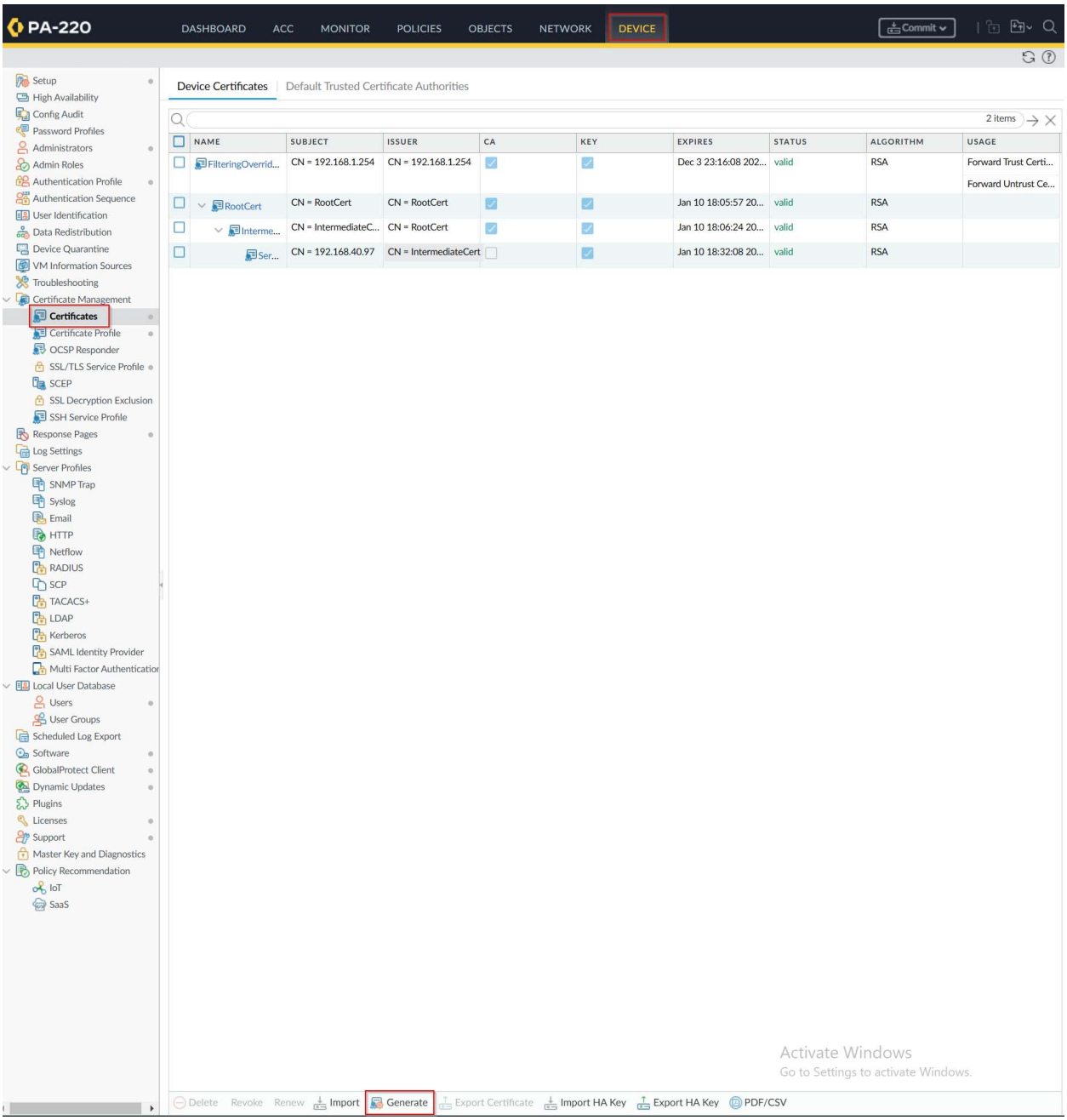
GlobalProtect can be configured to use client certificates along with user credentials in allowing access to the VPN. To authenticate an endpoint or end device, a certificate containing the correct information must be present on the device. To verify that the certificate is valid, GloablProtect Portal or Gateway checks if the client has the private key for the certificate. In addition, it checks if the certificate has the correct certificate authorities. If the certificate is the only means of entry into the VPN, the certificate must also include username in one of the fields.

Lab Summary

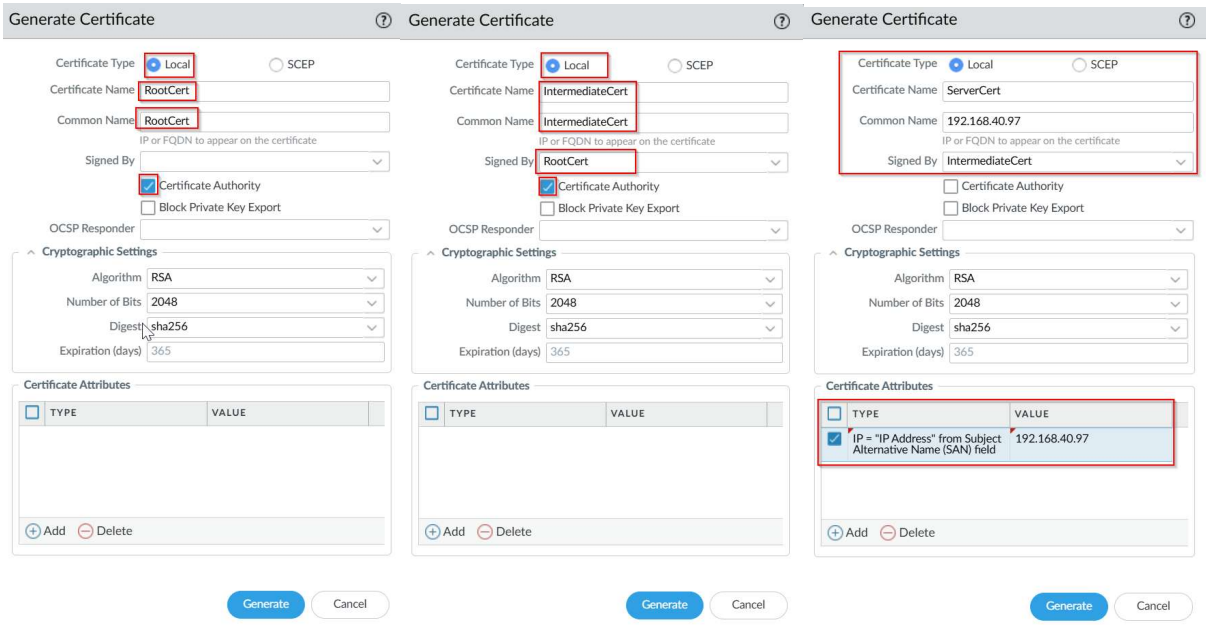
In this lab, you will configure root, intermediate, and server certificates for both a PA-220 firewall and an end device. You will configure a SSL-TSL Profile, set up interfaces for a VPN, and configure Global Protect on the firewall. Then, you will use two end devices to test out the VPN by using remote desktop from an outside end device to one inside to the network.

Configurations

1. We will first configure the required certificates for both the PA-220 firewall and end device. In the PA-220 configuration portal, navigate to Device > Certificate Management > Certificates and click Add.

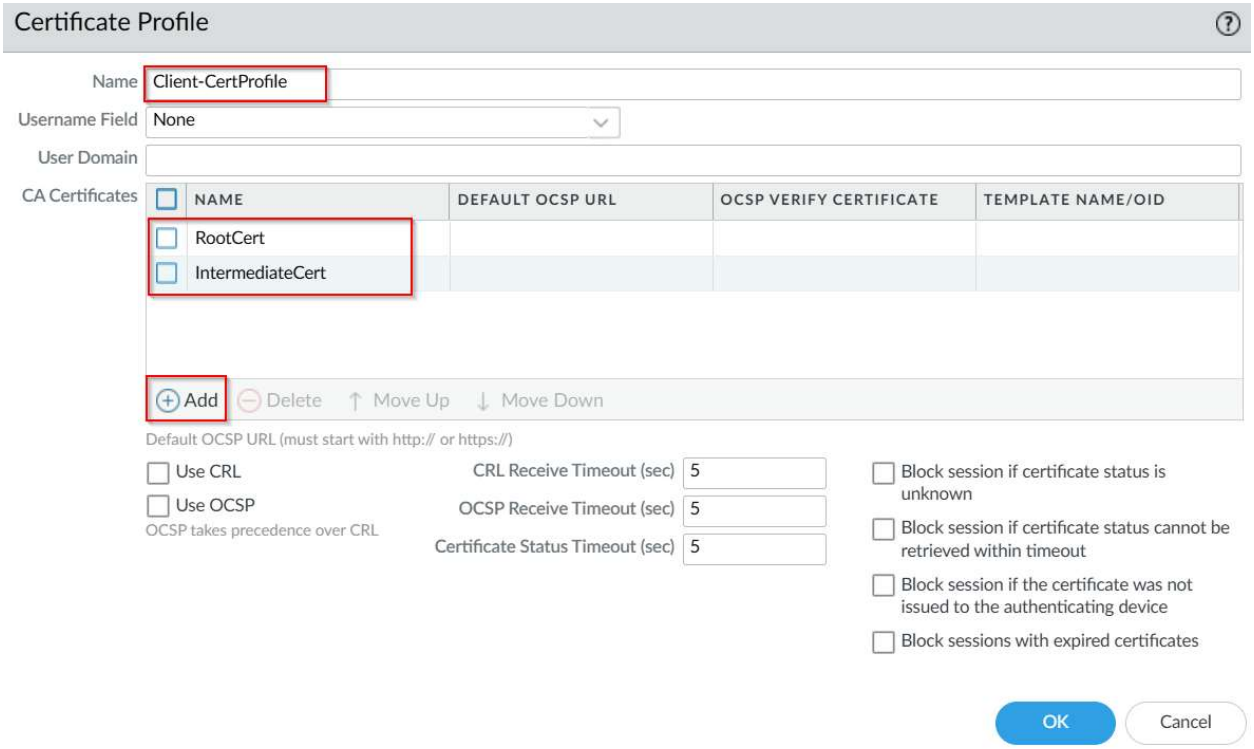


2. We need to add 3 certificates: A Root Certificate, an Intermediate Certificate, and a Server Certificate. The Root and Intermediate certificates are configured as certificate authorities. The Intermediate Certificate is signed by the Root Certificate, and the Server Certificate is signed by the Intermediate Certificate. The Server Certificate's Common Name should be the IP address of the Global Protect portal. After creating all three, export each certificate to your end device.

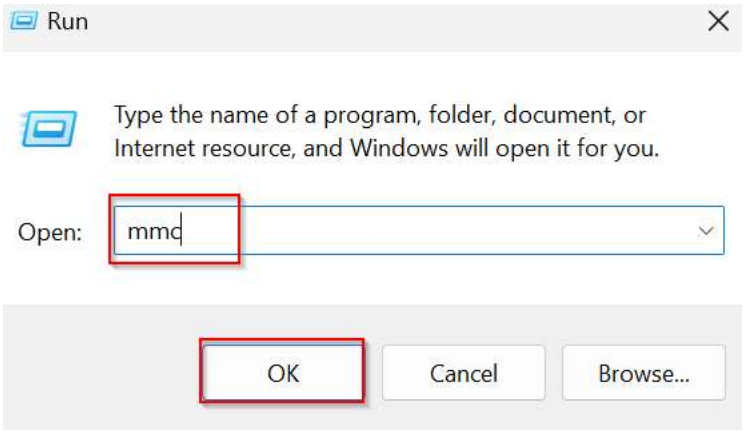


3. Navigate to Device > SSL/TLS Device Profile and click Add. Set the name to SSL-TLS-Server and the Certificate to ServerCert.

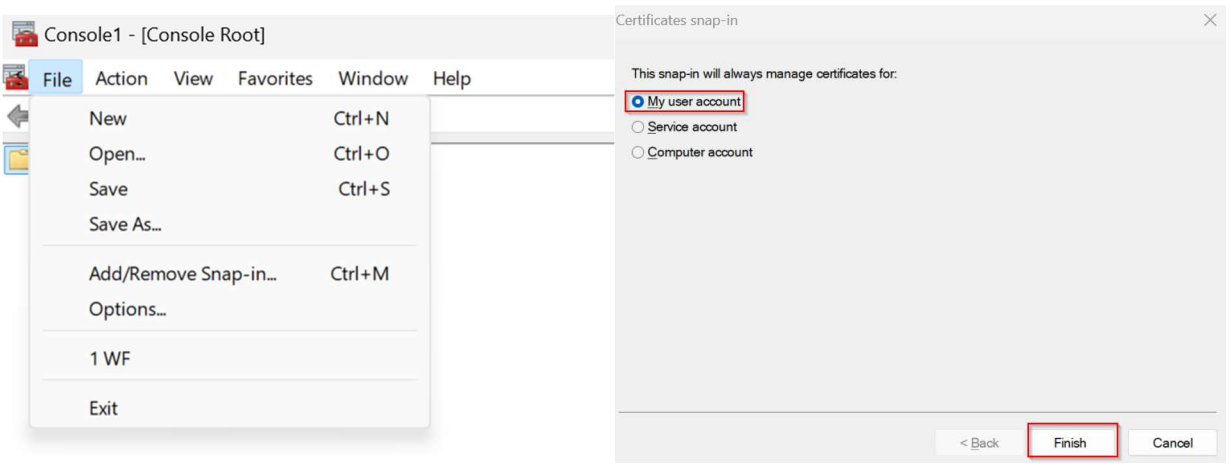
4. Navigate to Device > Certificate Management > Certificate Profile and click Add. Name the certificate profile Client-CertProfile and add both the Root and Intermediate Certificates.

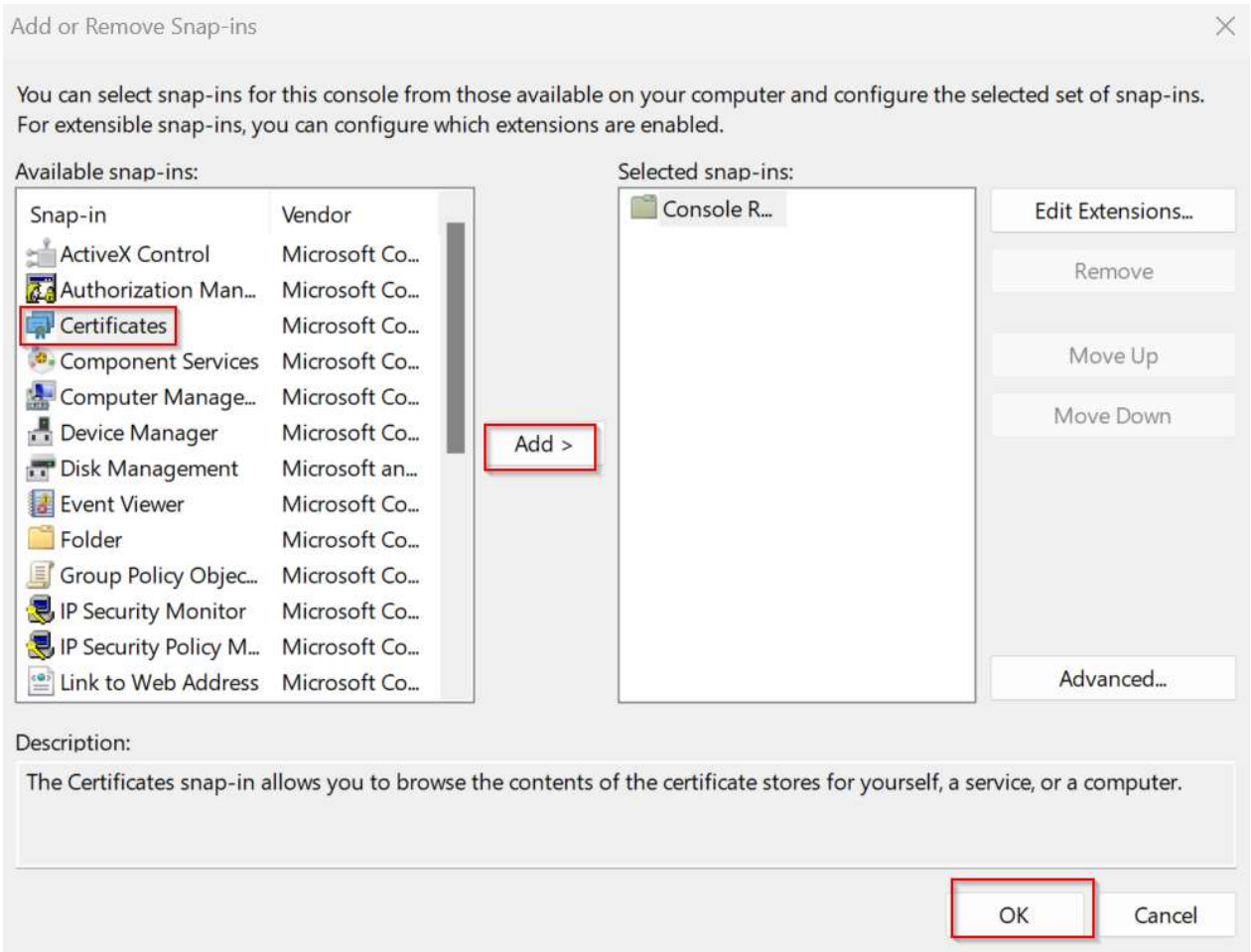


5. Now, we will add the certificates to your end device. Press WIN+R to open the Run dialog, and open “mmc”.

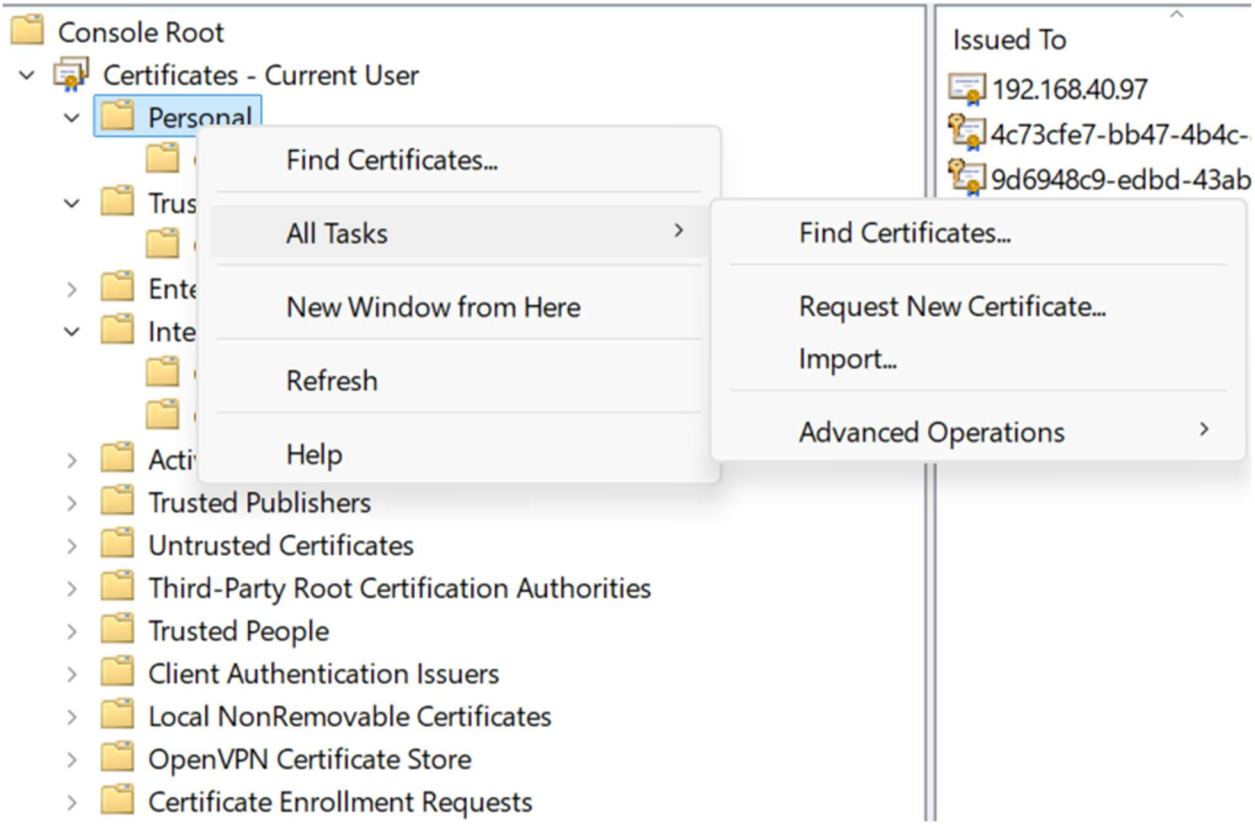


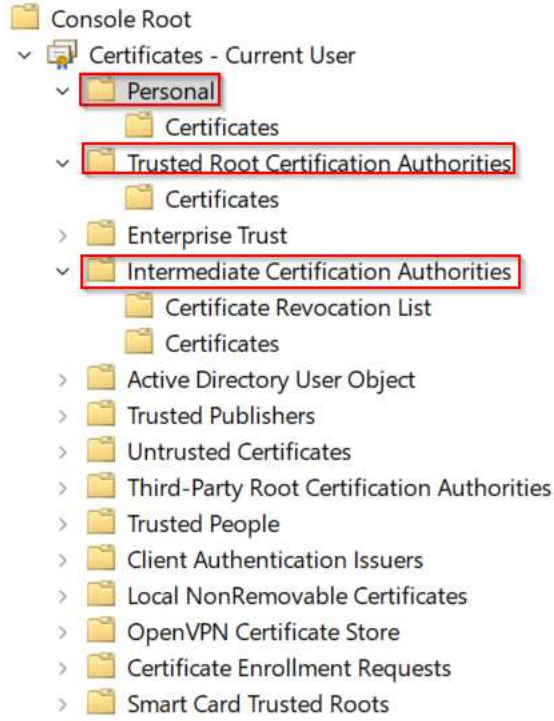
6. Navigate to File > Add/Remove Snap-in. Click on Certificates, Add, and Ok. If the dialog asks to manage certificates for your user account, service account, or computer account, select user account.



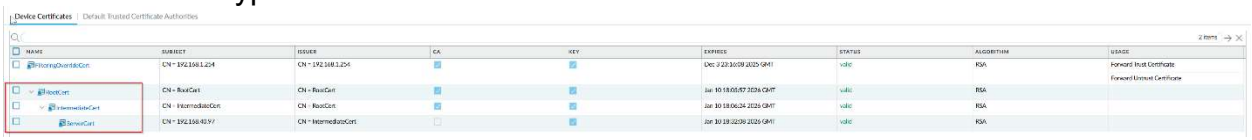


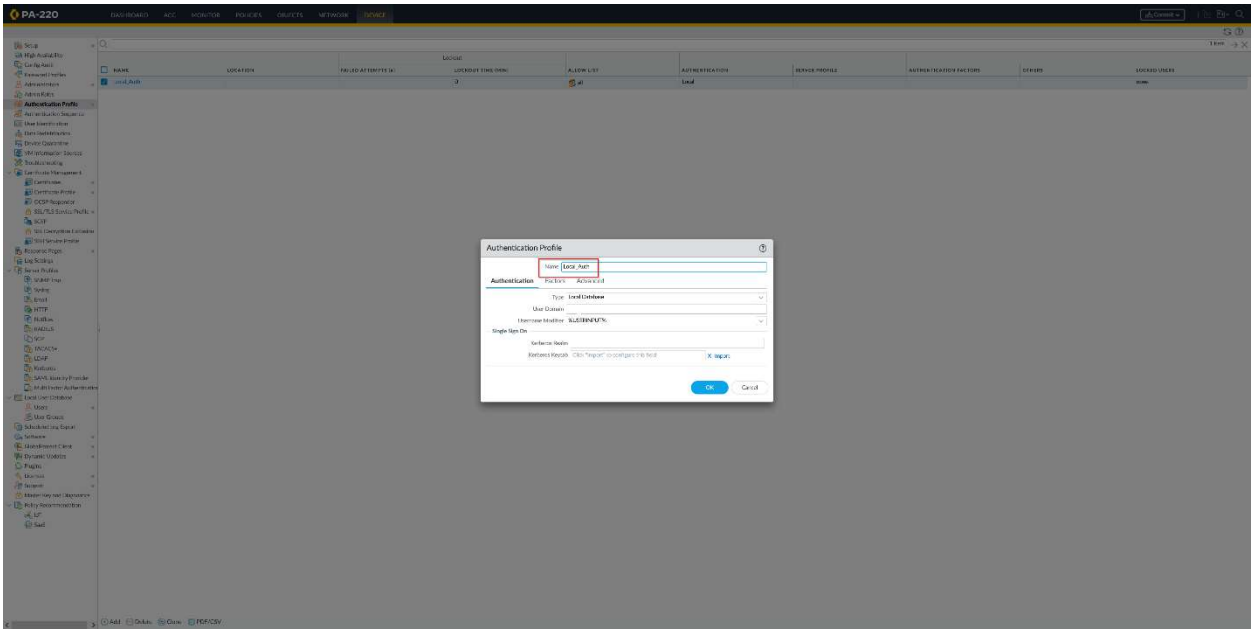
7. Import the server cert into the Personal Folder by right clicking the Personal folder > All Tasks > Import. Similarly, import the Root CA to Trusted Root Certification Authorities and import the Intermediate CA to Trusted Intermediate Certification Authorities.



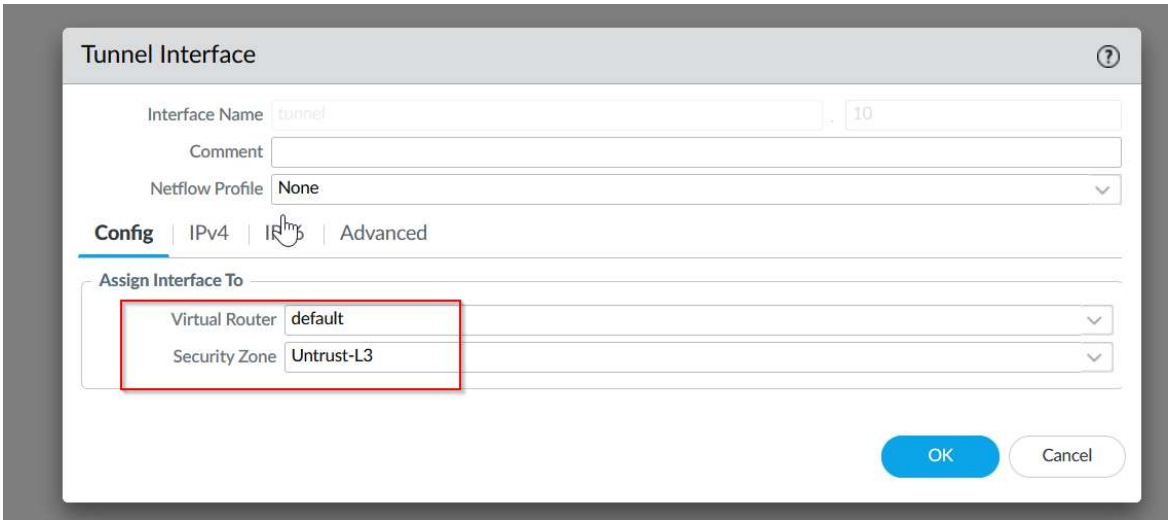


8. Now, we will start to configure GlobalProtect. Three certificates should already be generated: a root CA, an intermediate CA, and a server certificate. Navigate to Device > Authentication Profile and click Add. Name the Authentication Profile Local_Auth and ensure that the type is Local Database.

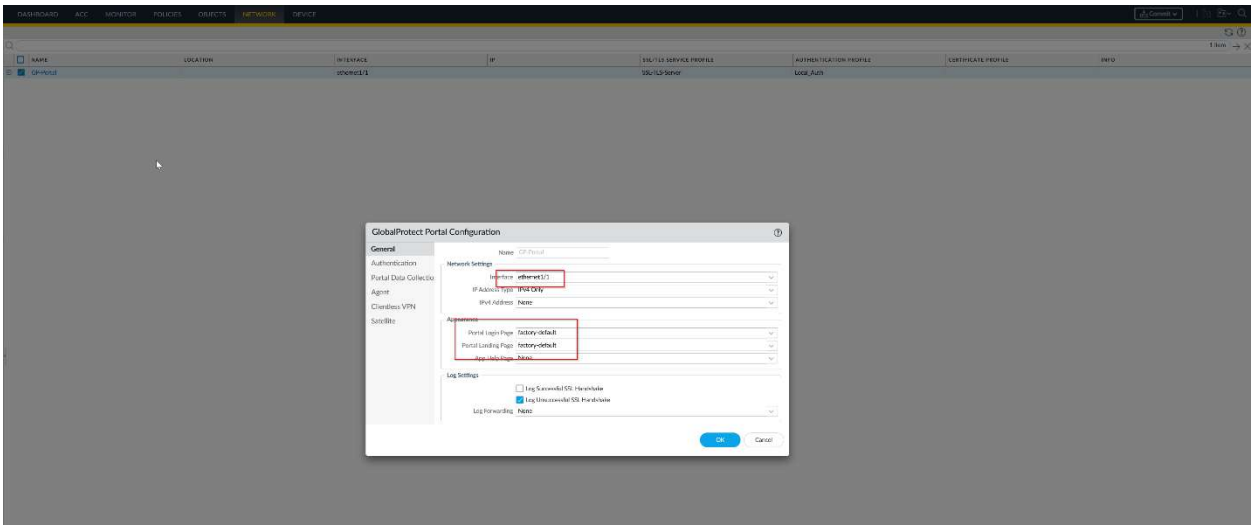


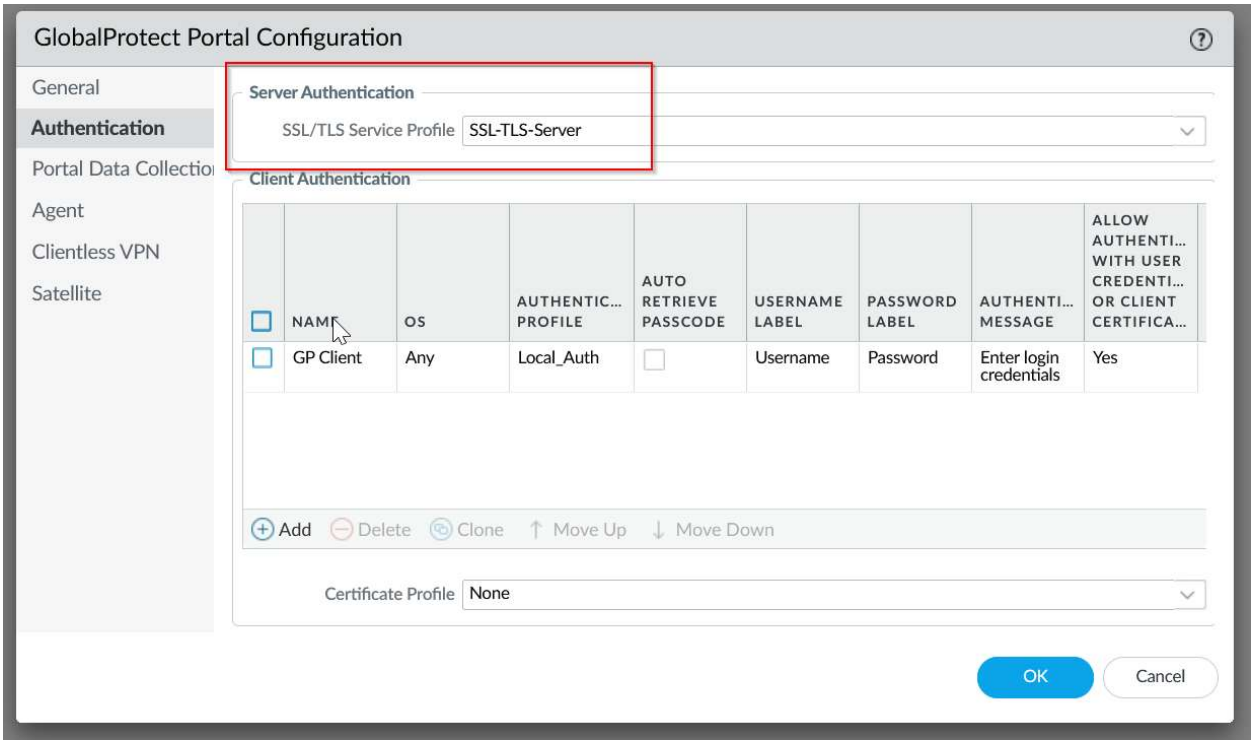


9. Navigate to Network > Interfaces > Tunnel, and add a tunnel interface. Set the interface to tunnel.10. The Security Zone should be the outward facing security zone for internet traffic, as that is where to the VPN will be allowed.

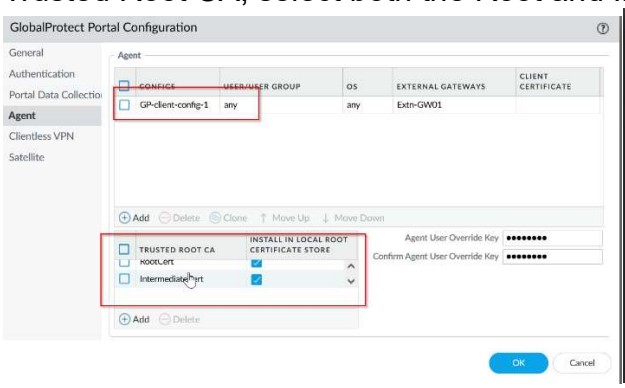


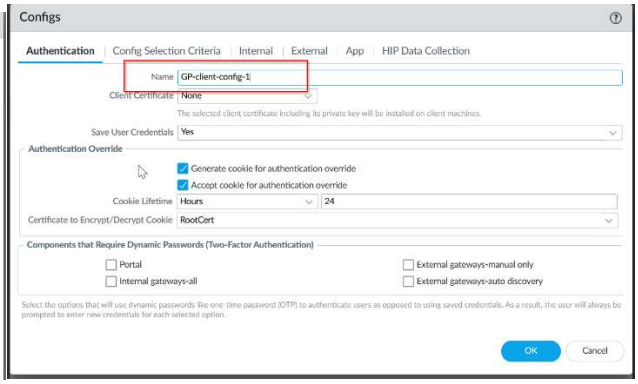
10. Now, we will configure the Global Protect Portal. Navigate to Network > GlobalProtect > Portals and click Add. Configure the name of the Portal, and make sure the interface to the outward facing interface. In the Authentication tab, set the Service Profile to SSL-TLS-Server and add Client Authentication. Set the OS to Any and Authentication Profile to Local_Auth.

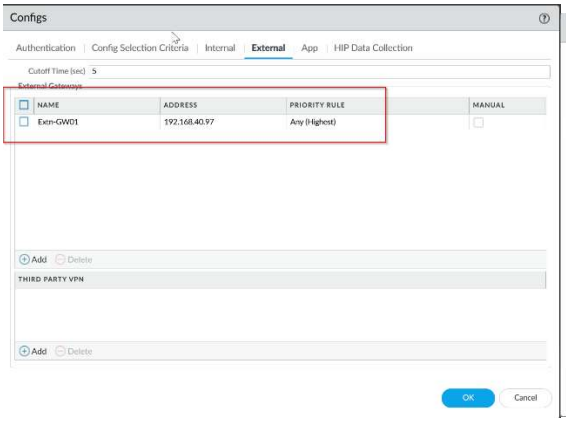


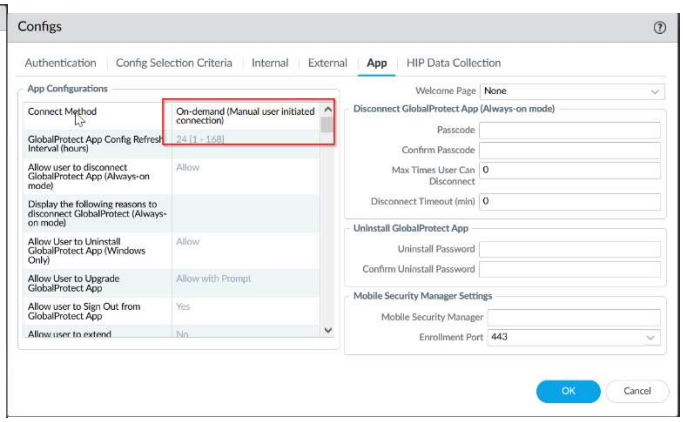


11. Navigate to the Agent tab. Add a new client config. Set the name, add an external gateway using the IP address reference in the Common Name field of the Server Cert. Then, in the “App” tab, select ‘On-demand’ on the Connect-method dropdown. Under Trusted Root CA, select both the Root and Intermediate Certificates.

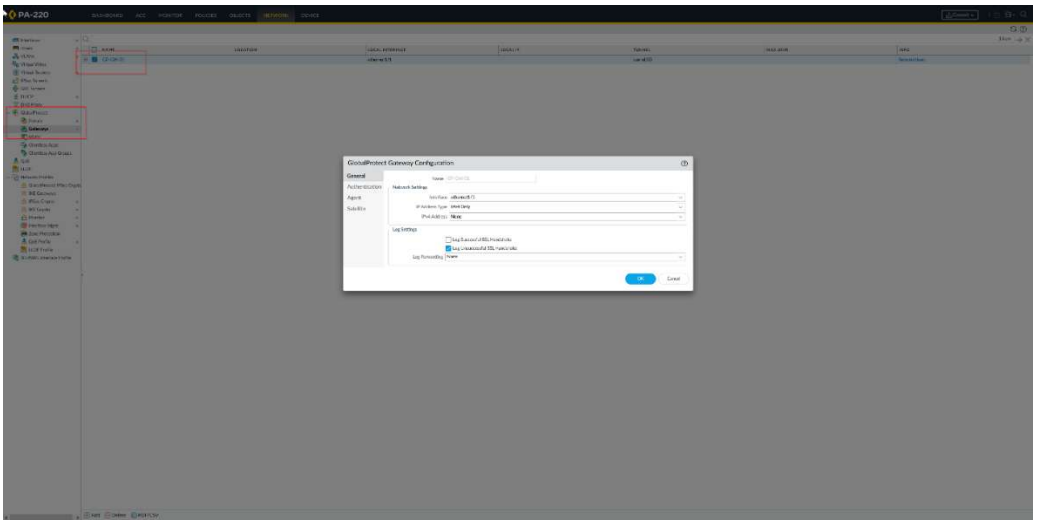




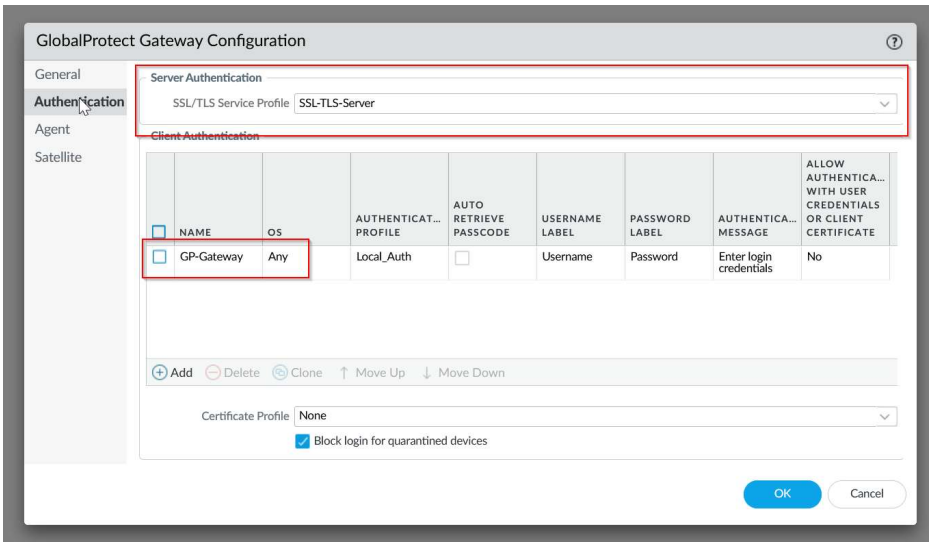


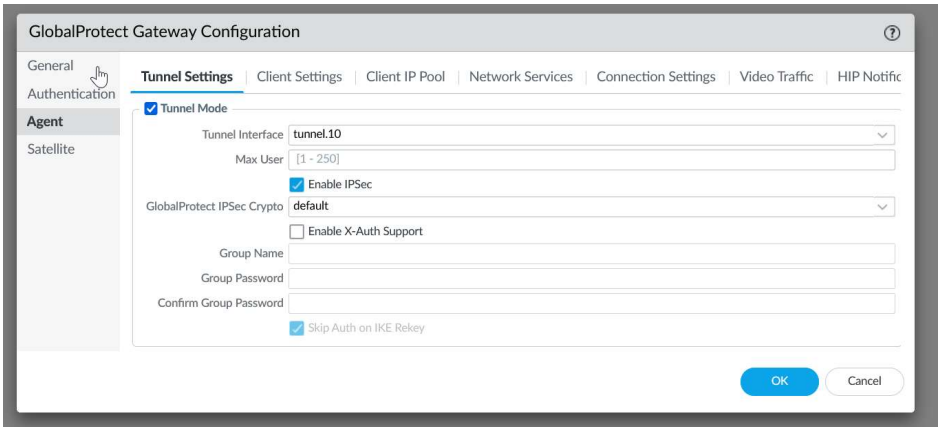


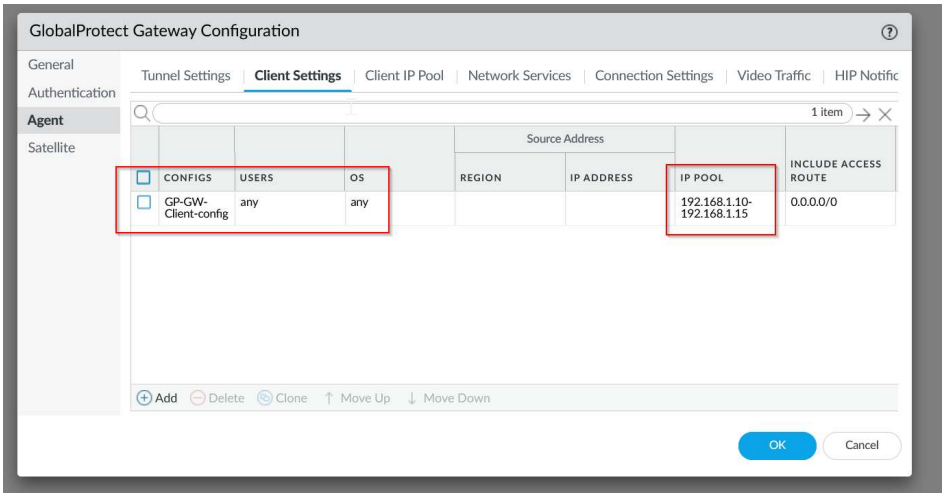
12. Now, we will configure the Global Protect Gateway. Navigate to Network > GlobalProtect > Gateways and click Add. Give the gateway a name and select the same interface as before to act as the gateway.



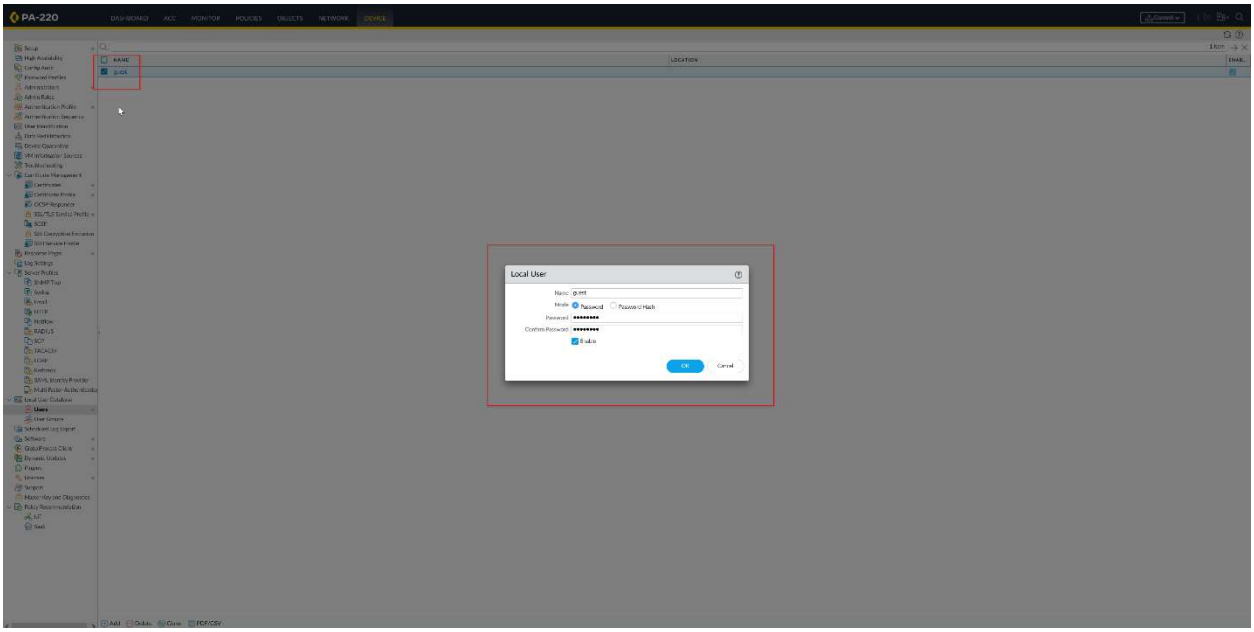
13. In the Authentication tab, select the SSL-TLS profile created. Click Add under Client Authentication. Give it a name, and select the Authentication Profile you created. In the Agent tab, select the tunnel interface you created and enable IPsec. In the Client setting tab, add a config and give it an IP pool. These are the IP addresses given to end devices when they connect to the VPN.



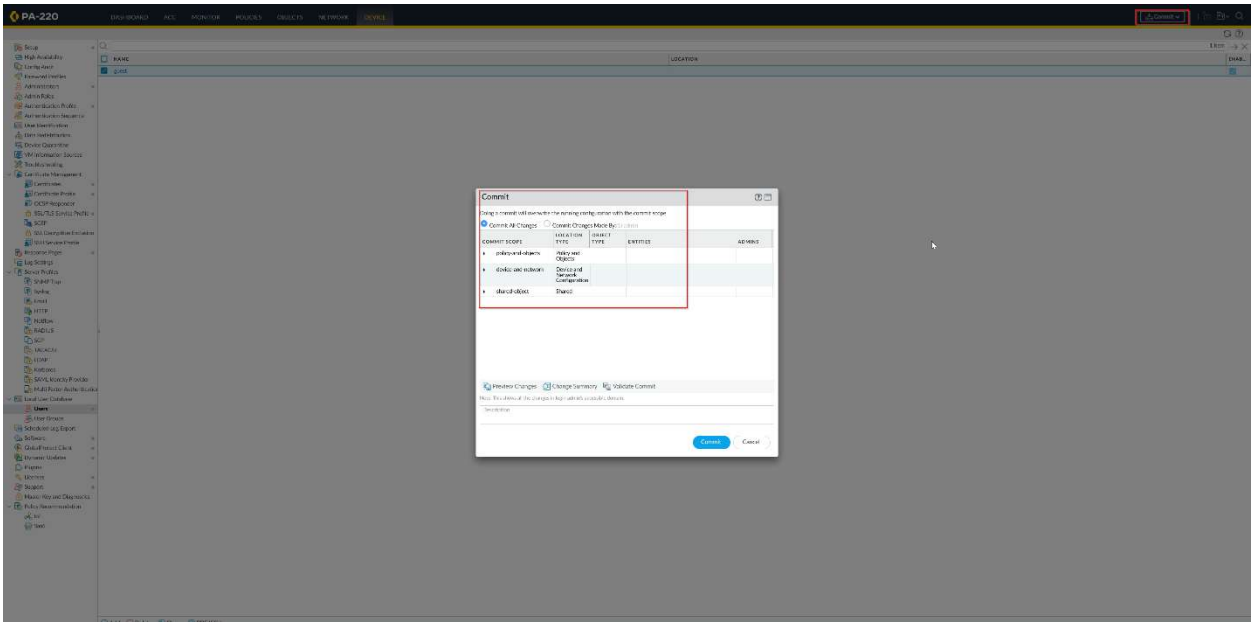




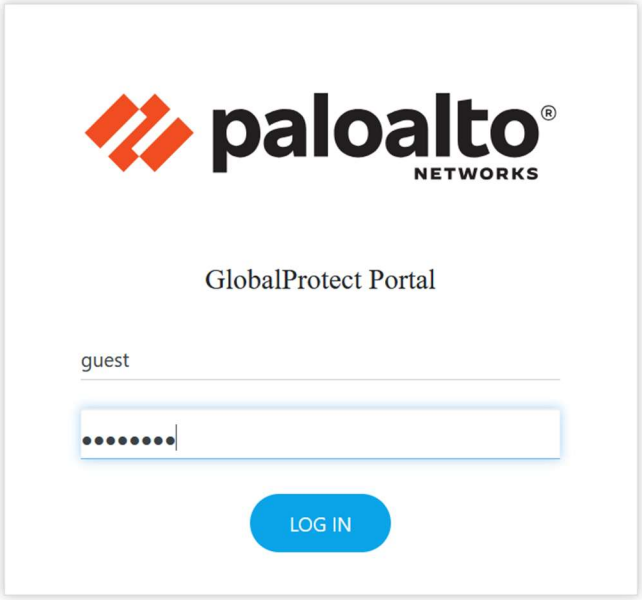
14. Navigate to Device > Local User Database > Users, and create a local user for testing.

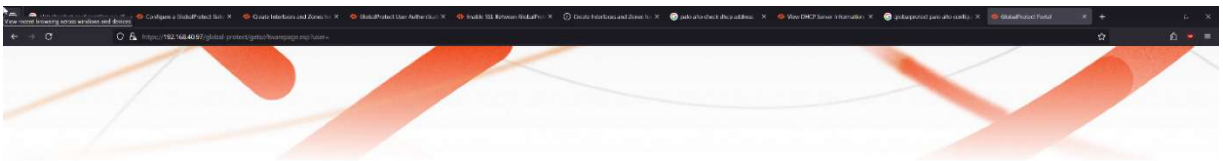


15. Commit all changes.

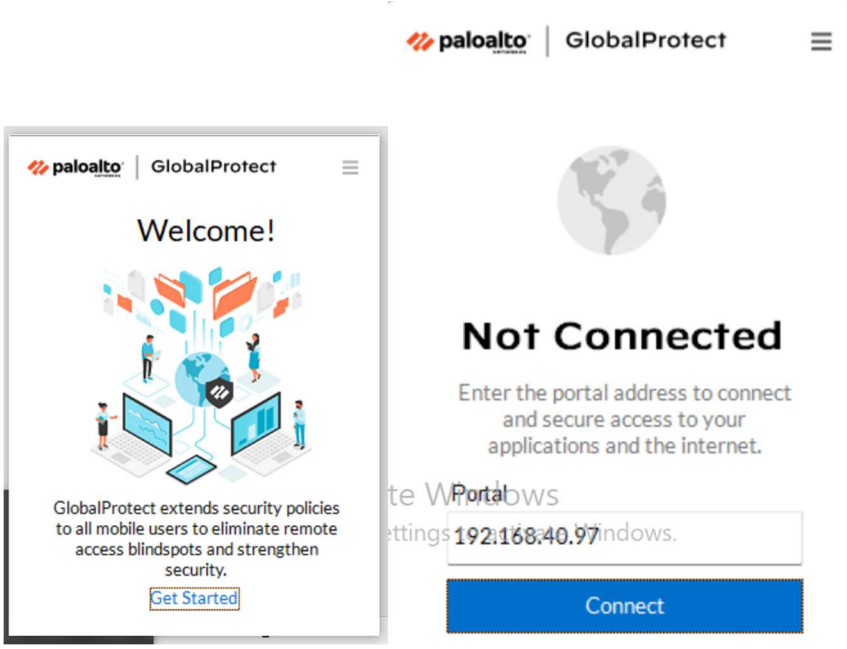


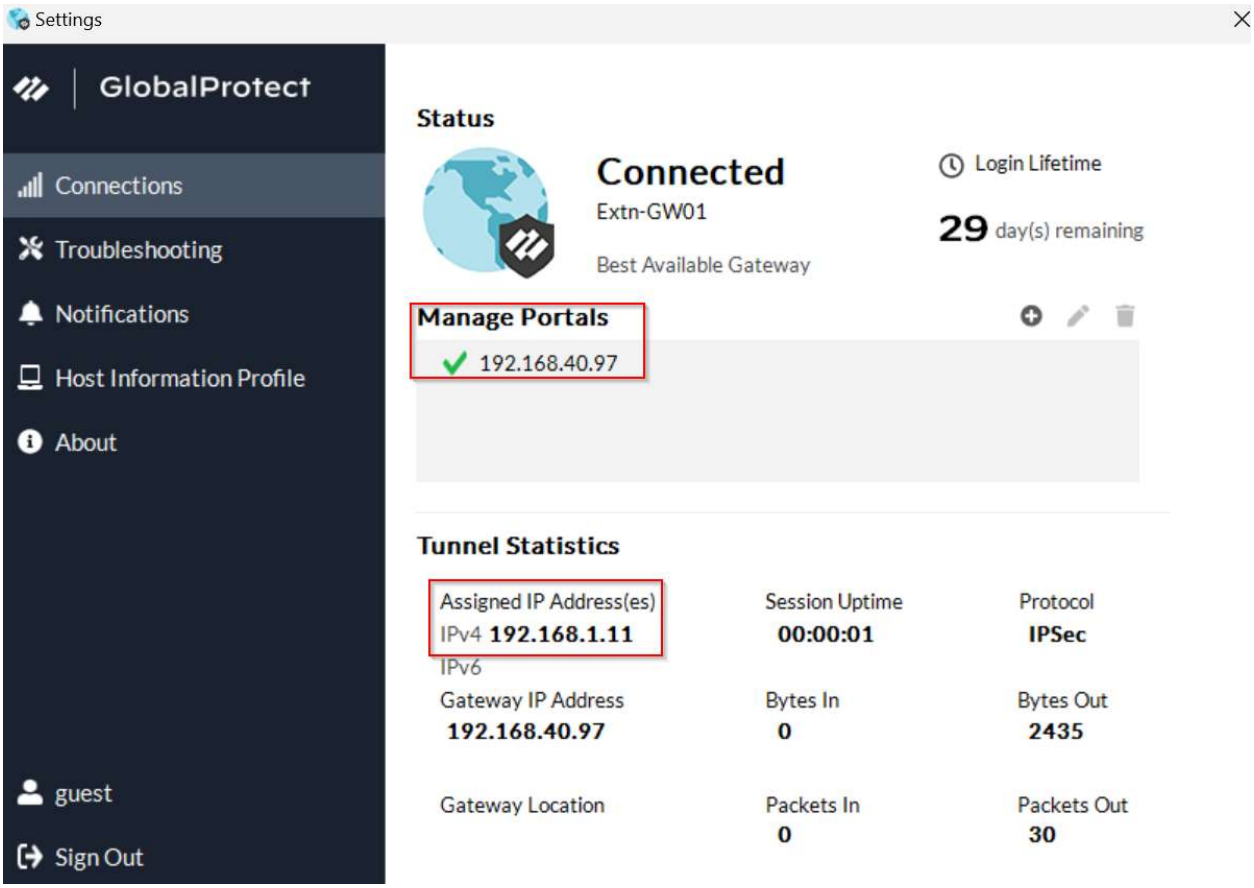
16. Navigate to the IP address of the portal you configured. Enter the local user credentials. Then, download the client for your OS. Use all defaults in the install wizard.



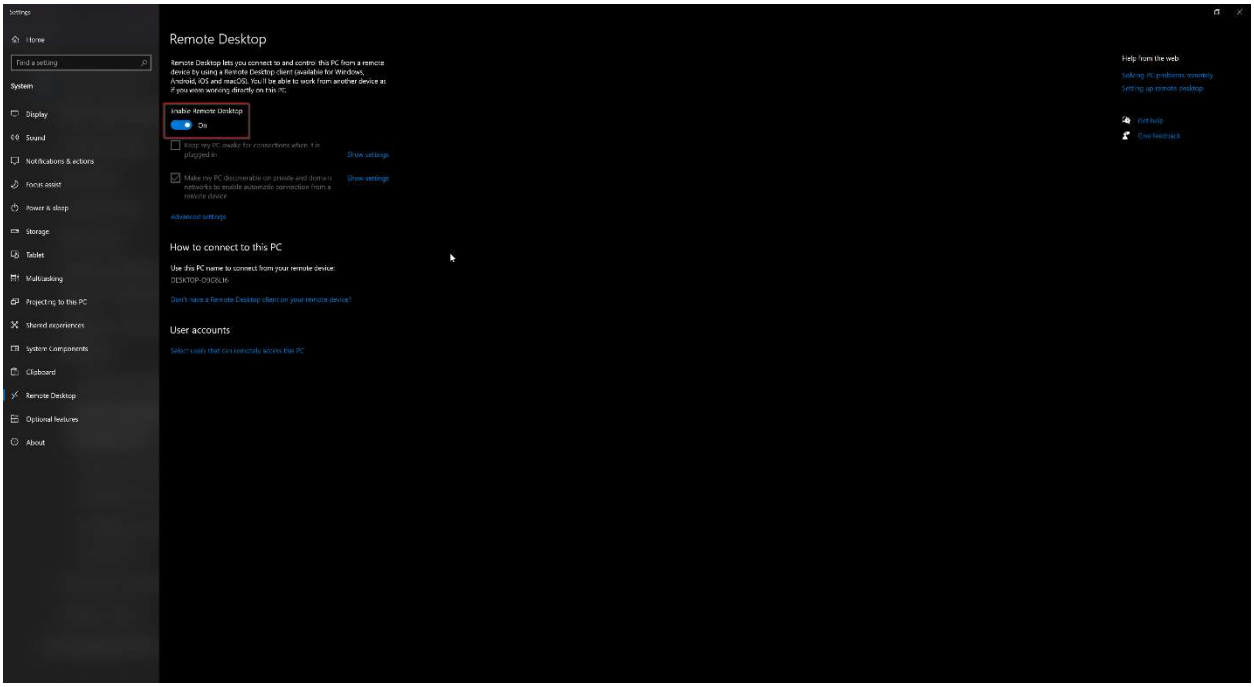


17. In the Global Protect app, click Get Started and enter the IP address of the portal. You should then be connected to the VPN and given an IP address.

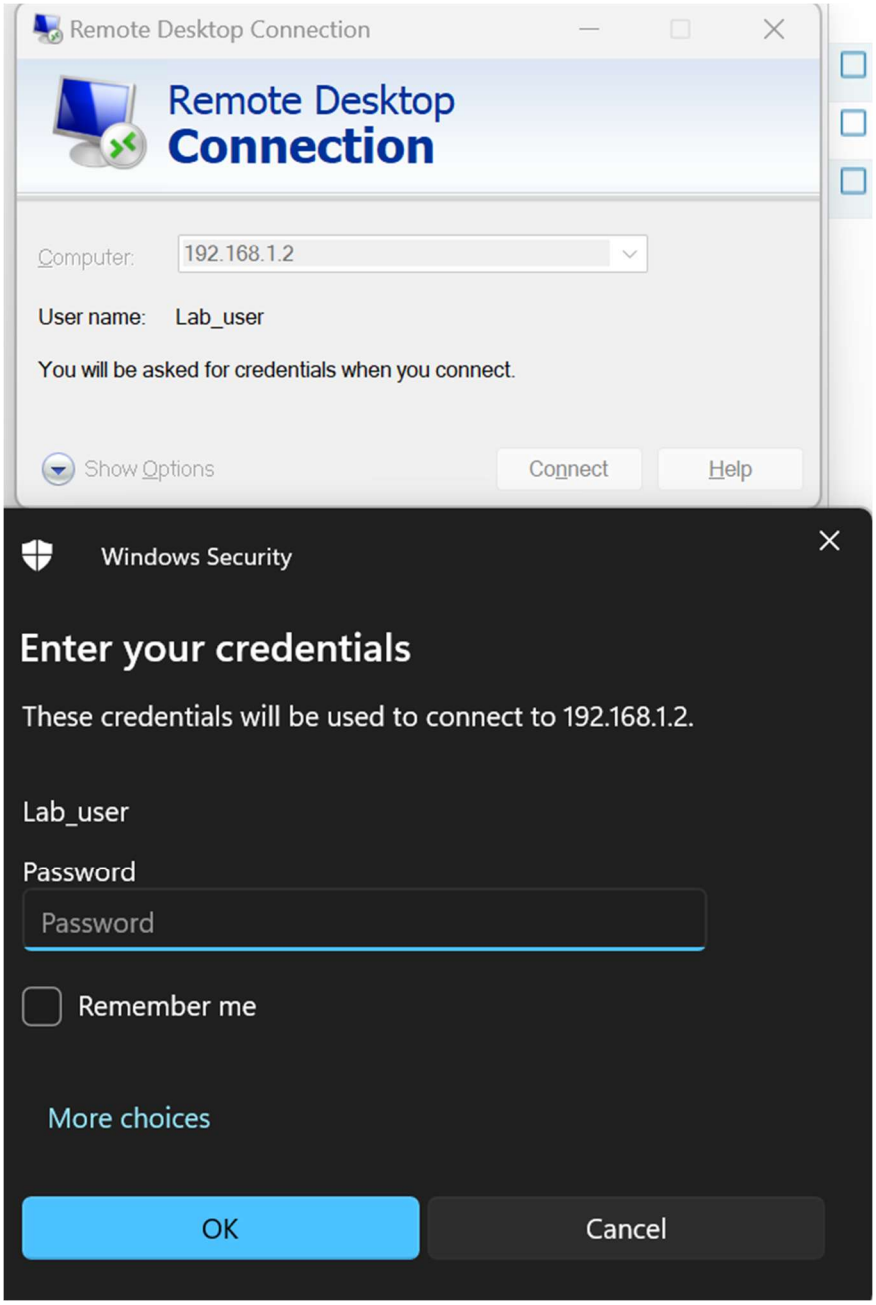




18. Now we will set up Remote Desktop to test Global Protect. Place one end device (Device A) within the network protected by the firewall, and place the end device (Device B) with the certifications outside the network. On Device A, navigate to Windows settings > System > Remote Desktop and enable remote desktop.



19. On Device B, enter the IP address of Device A and connect. Enter the credentials of Device B. You are now able to remote desktop into Device A from outside the network.



Running wireshark on Device A, we can see that it is talking to Device B, located at 192.168.1.11. This IP address was given to Device B using the GlobalProtect App. Looking at the protocol, we can see that it is running RDP (Remote Desktop), showing that we have successfully configuring GlobalProtect.

Source	Destination	Protocol	Length	Info
192.168.1.2	192.168.1.11	TLSv1.2	1279	
192.168.1.2	192.168.1.11	TLSv1.2	1109	
192.168.1.11	192.168.1.2	TLSv1.2	350	Application Data, Application Data
192.168.1.2	192.168.1.11	TLSv1.2	1287	
192.168.1.2	192.168.1.11	TLSv1.2	1279	
192.168.1.2	192.168.1.11	TLSv1.2	73	
192.168.1.2	192.168.1.11	TLSv1.2	1279	
192.168.1.2	192.168.1.11	TLSv1.2	1279	
192.168.1.2	192.168.1.11	TLSv1.2	479	
192.168.1.11	192.168.1.2	TLSv1.2	341	Application Data, Application Data
192.168.1.11	192.168.1.2	TLSv1.2	118	Application Data
192.168.1.2	192.168.1.11	RDPUDP2	54	ACK,OVERHEAD
192.168.1.2	192.168.1.11	TLSv1.2	105	Application Data
192.168.1.2	192.168.1.11	TLSv1.2	1051	
192.168.1.11	192.168.1.2	TLSv1.2	111	Application Data
192.168.1.11	192.168.1.2	TLSv1.2	97	Application Data
192.168.1.11	192.168.1.2	TLSv1.2	106	Application Data
192.168.1.2	192.168.1.11	RDPUDP2	53	ACK,OVERHEAD
192.168.1.11	192.168.1.2	TLSv1.2	97	Application Data
192.168.1.2	192.168.1.11	TCP	54	3389 → 64635 [ACK] Seq=11374 Ack=26596 Win=62692 Len=0
192.168.1.2	192.168.1.11	TLSv1.2	229	
192.168.1.11	192.168.1.2	TLSv1.2	104	Application Data
192.168.1.11	192.168.1.2	TLSv1.2	111	Application Data
192.168.1.11	192.168.1.2	TLSv1.2	104	Application Data
192.168.1.2	192.168.1.11	TCP	54	3389 → 64635 [ACK] Seq=11374 Ack=26696 Win=64000 Len=0
192.168.1.11	192.168.1.2	TLSv1.2	106	Application Data
192.168.1.2	192.168.1.11	RDPUDP2	52	ACK
192.168.1.2	192.168.1.11	TLSv1.2	1279	

Problems

1. When configuring Global Protect, we did not download and install the Global Protect App onto our firewall. Thus, when attempting to download the app from the Portal, we received a blank file. Installing the App onto our firewall fixed this issue.

Conclusion

In this lab, we successfully configured GlobalProtect for the PA-220 firewall, configuring client certificates for an end device, and performed remote desktop from one end device outside of the network into another end device protected by the firewall.

Fortinet SOHO Network

Purpose

The purpose of this lab is to configure a Small Office/Home Office (SOHO) network using a Fortinet firewall and an access point.

Background Information

A Small Office/Home Office (SOHO) network is designed for small businesses or individuals operating within small offices or homes. A SOHO network can be set up for much cheaper than a large corporate network, making it more suitable for small businesses or homes on a budget. Devices on a SOHO network can also share resources, such as printers or file systems, allowing greater productivity. These devices are also all easily accessible by the administrator of the network which makes is simpler for troubleshooting any problems that arise.

A SOHO network requires multiple networking devices, including a switch, router, and usually, a firewall. A switch is used to connect and communicate with all network-enabled devices, such as computers and printers. The switch forwards data packets from one device to another and ensures communication is established.

A router is used as the central networking device within a SOHO network using wired and wireless connections. They usually provide a web interface for configuration of the network. Routers can have other functions such as firewalls, VPNs, and other security features.

An access point is a networking device that allows end devices to connect to a wireless or wired network.

Fortinet is American cybersecurity company offering firewalls, endpoint security, and intrusion detection systems. The main firewall of Fortinet is Fortigate, a Next Generation Firewall. The model used within this lab is the Fortigate FortiWifi 40F Series, which provides simplified configurations, a wireless controller, and AI-powered security services. The 40F series firewalls run on FortiOS, an operating system made by Fortinet and the first converged networking and security operating system in the industry. FortiOS allows security and networking components to be tied together, making it much more convenient for users and administrators.

The FortiWifi 40F series has multiple use cases, including protecting network perimeters through network security policies and SSL inspection, being a secure SD-WAN, and extending security to other Fortinet networking devices.

FortiOS in conjunction with the FortiWifi 40F series firewall allows for a Fortinet access point to be plugged into the network and function without additional configuration.

Multiple things must be configured to set up a wireless network. Service Set Identifiers (SSIDs) must be configured for each network that is set up. SSIDs simply act as the name of the network and are what will show up on end devices trying to connect through them. Each network needs to have some type of authentication for them to be secure. Wi-Fi Protected Access 2 (WPA2) with Pre-Shared Key (PSK) allows a password, or PSK, to be set on a network. WPA Enterprise requires a server to contain a list of usernames and passwords that an end device needs to connect.

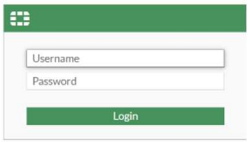
In order for end devices to access the internet, they must be given an IP address. This can be done through Dynamic Host Configuration Protocol (DHCP), while automatically gives devices an IP address from a set pool of addresses. Otherwise, end devices will need to have a static IP address.

Lab Summary

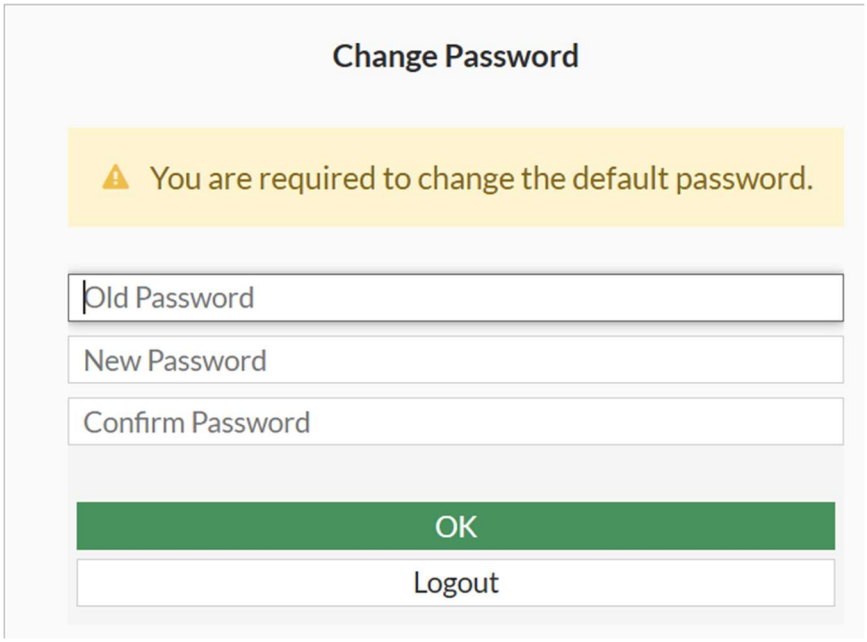
In this lab, we will set up a Fortigate firewall for a SOHO network. The firewall will be accessed and configuration through the online GUI. An administrative password will be set up. Two SSIDs are created, one using WPA2 PSK (pre-shared key), and the other used WPA Enterprise. Firewall policies are set up without any filtering, but exist for future configuration.

Configurations

1. Go to the https://192.168.1.99 to access the Fortinet GUI.

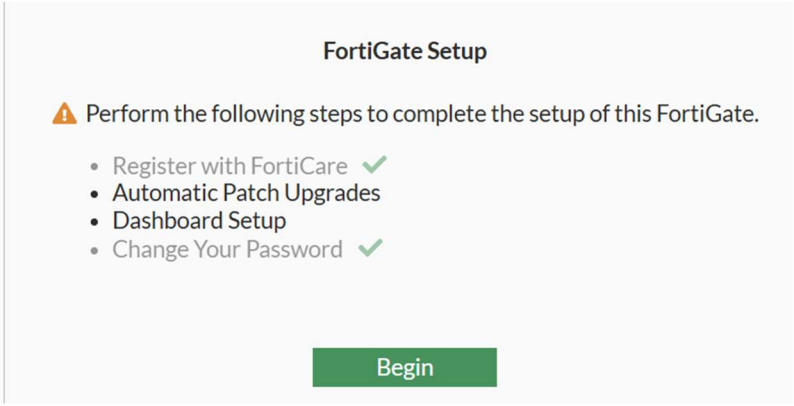


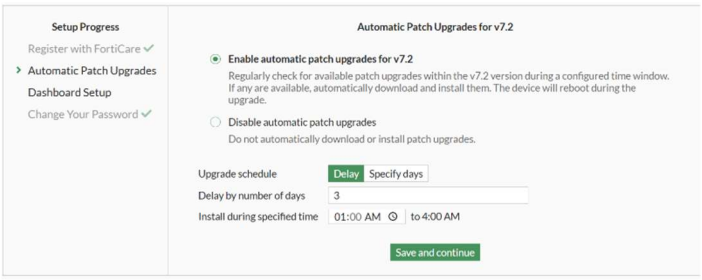
2. Put in **admin** for the username and press enter in order to set a password.

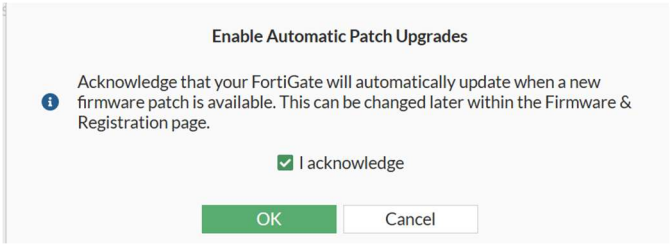


Skip the old password and put in your new password.

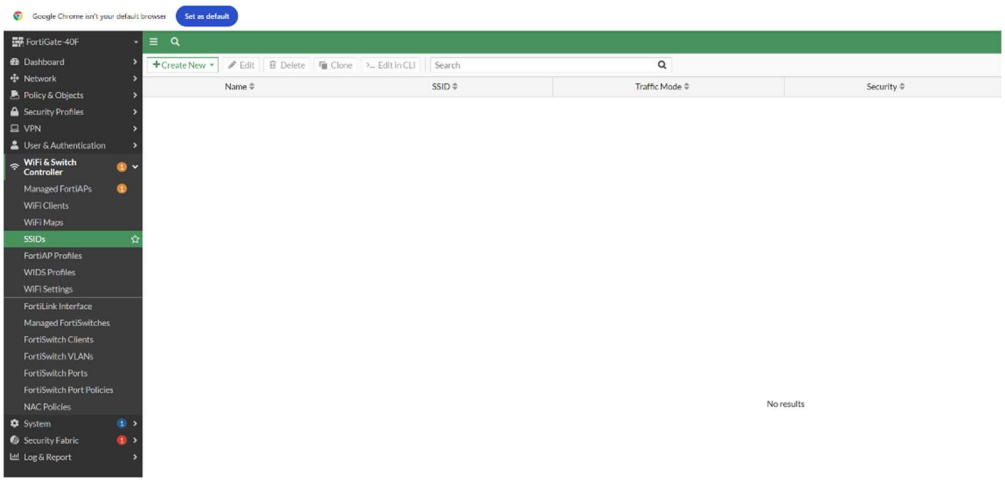
3. Once you have put in your new password, start the FortiGate setup



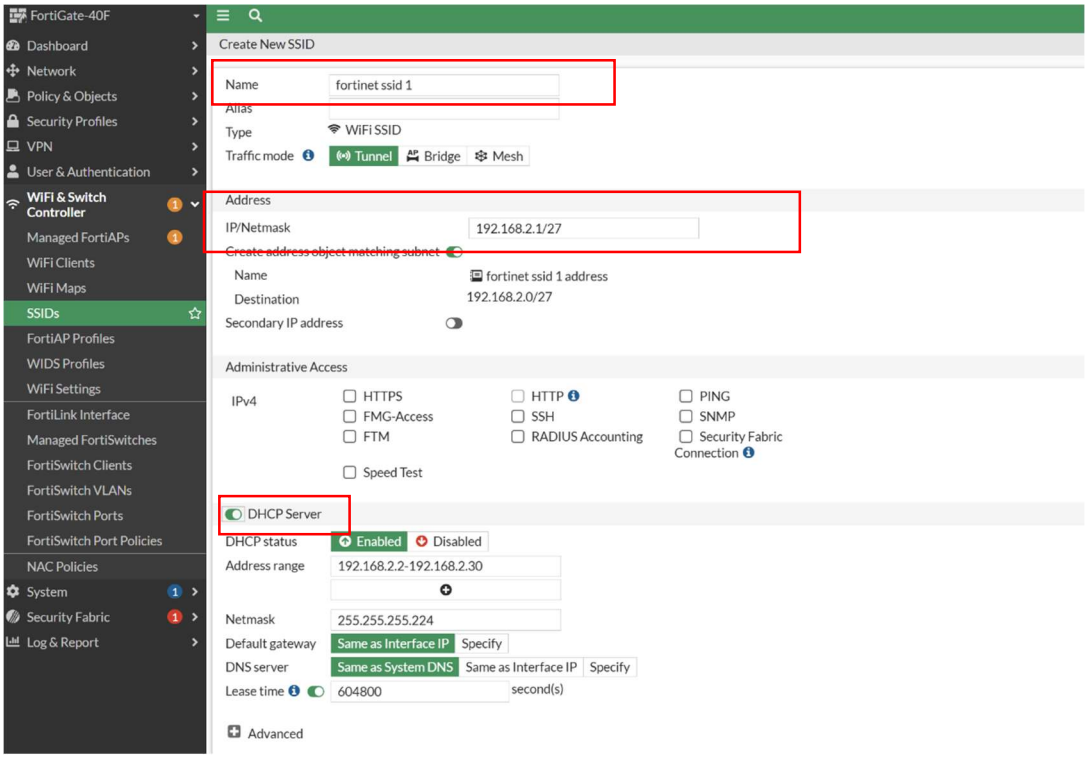




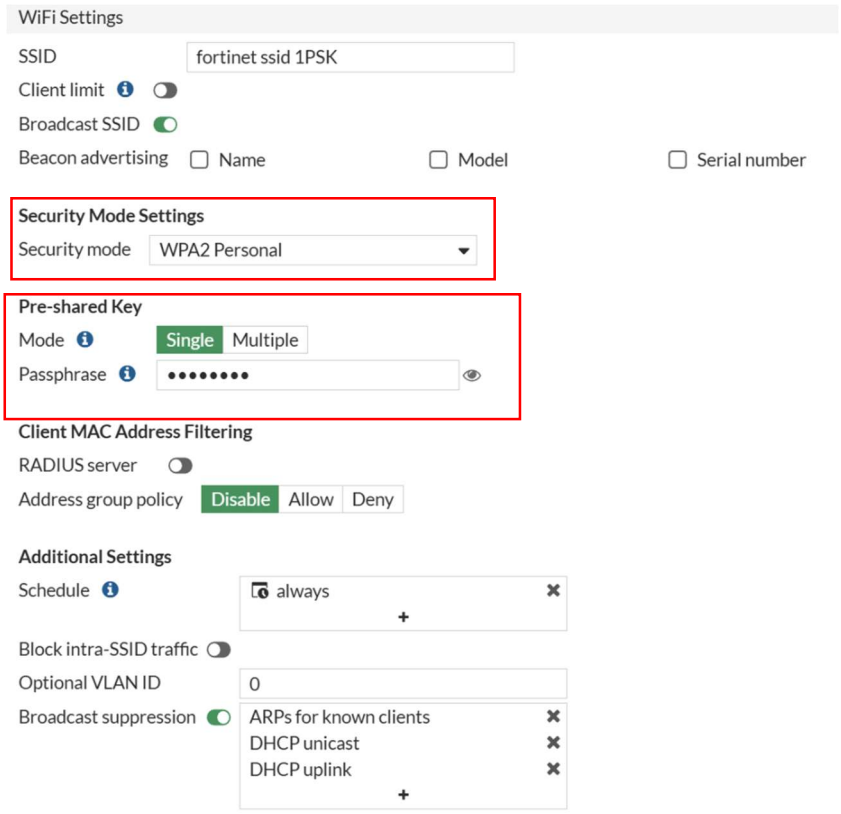
4. Once you are in the Fortigate GUI, go to **Wifi & switch controller -> SSIDs**



5. **Create** the first SSID. **Name it** and set the ip/netmask to something that isn't the LAN IP address. **Turn on the DHCP server.**



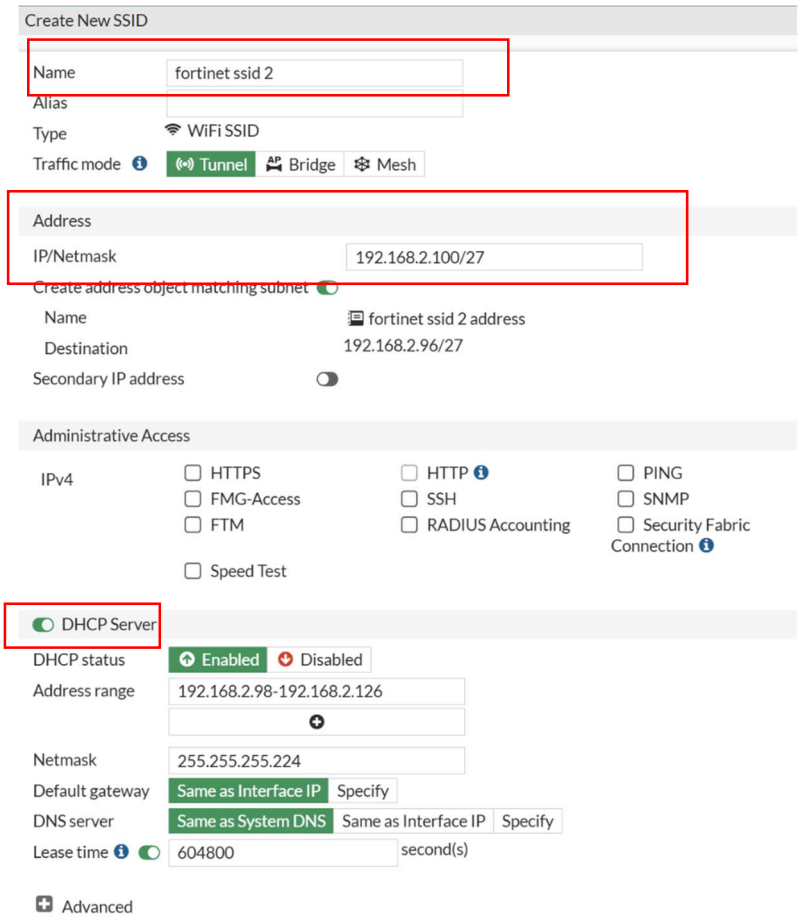
Scroll down and set the **SSID** (this is what will show up when you look for internet) along with **Set the passphrase. Ensure the security mode is WPA2 Personal.**


WiFi Settings
SSID
fortinet ssid 1PSK
Client limit
Broadcast SSID
Beacon advertising
Name
Model
Serial number
Security Mode Settings
Security mode
WPA2 Personal
Pre-shared Key
Mode
Single
Multiple
Passphrase
Client MAC Address Filtering
RADIUS server
Address group policy
Disable
Allow
Deny
Additional Settings
Schedule
always
Block intra-SSID traffic
Optional VLAN ID
0
Broadcast suppression
ARPs for known clients
DHCP unicast
DHCP uplink

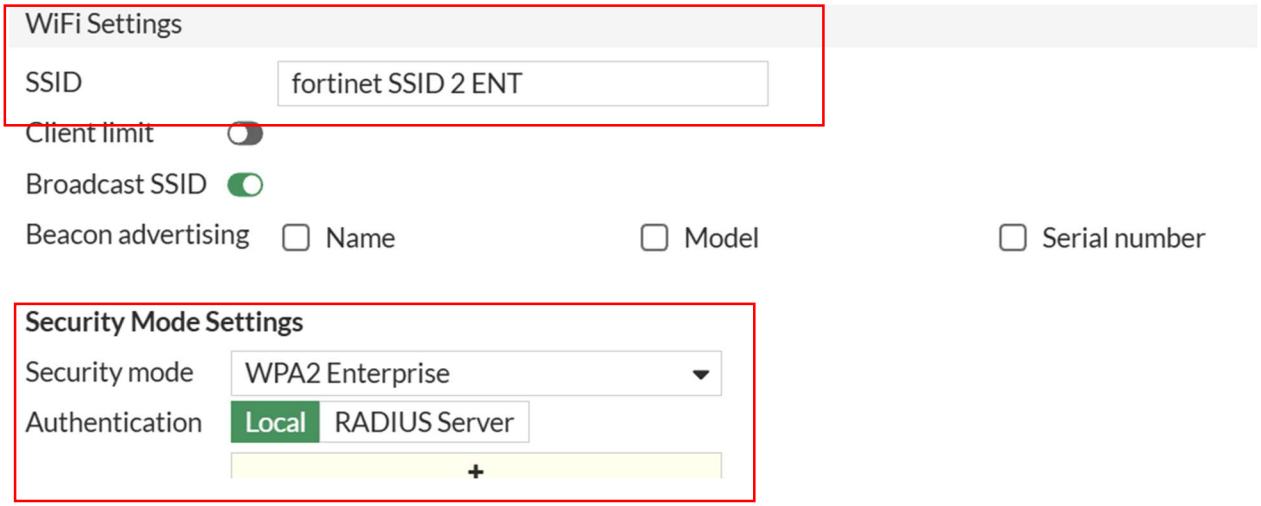
Click ok

6. Now we want to create another one.

Click **Create new**

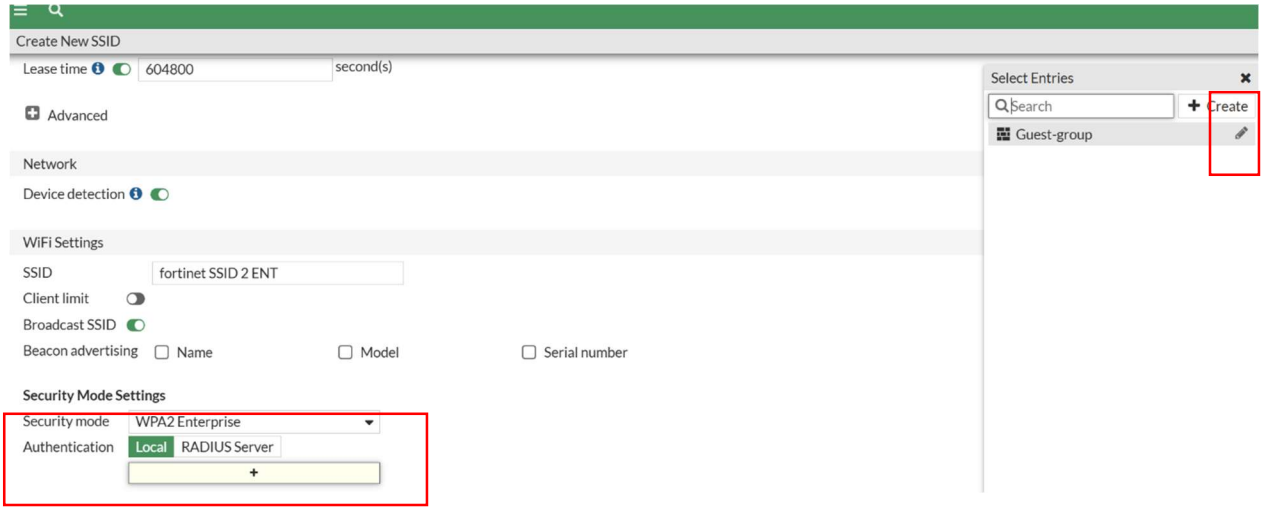


Now when we scroll down we want **Set a different name** and click **WPA2 Enterprise for the security mode**

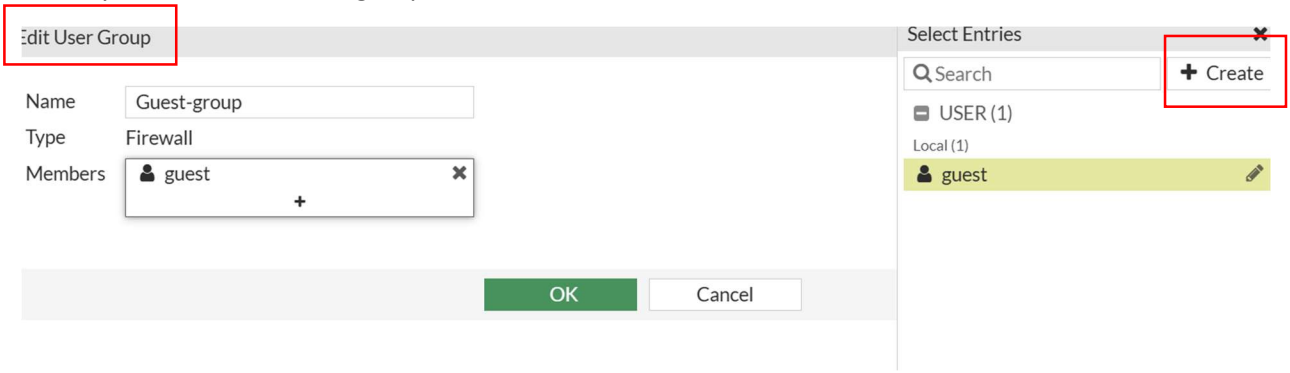


We have to **Click the plus** under authentication to create a user.

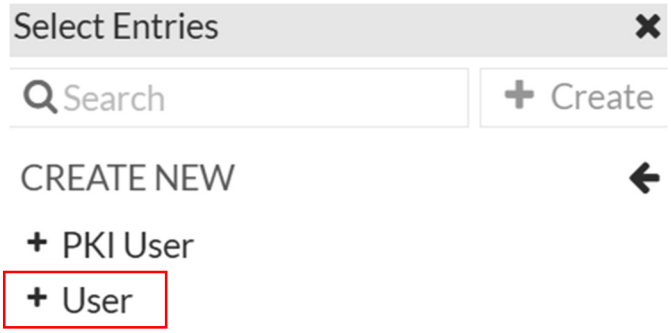
Click the pencil of the Guest-group



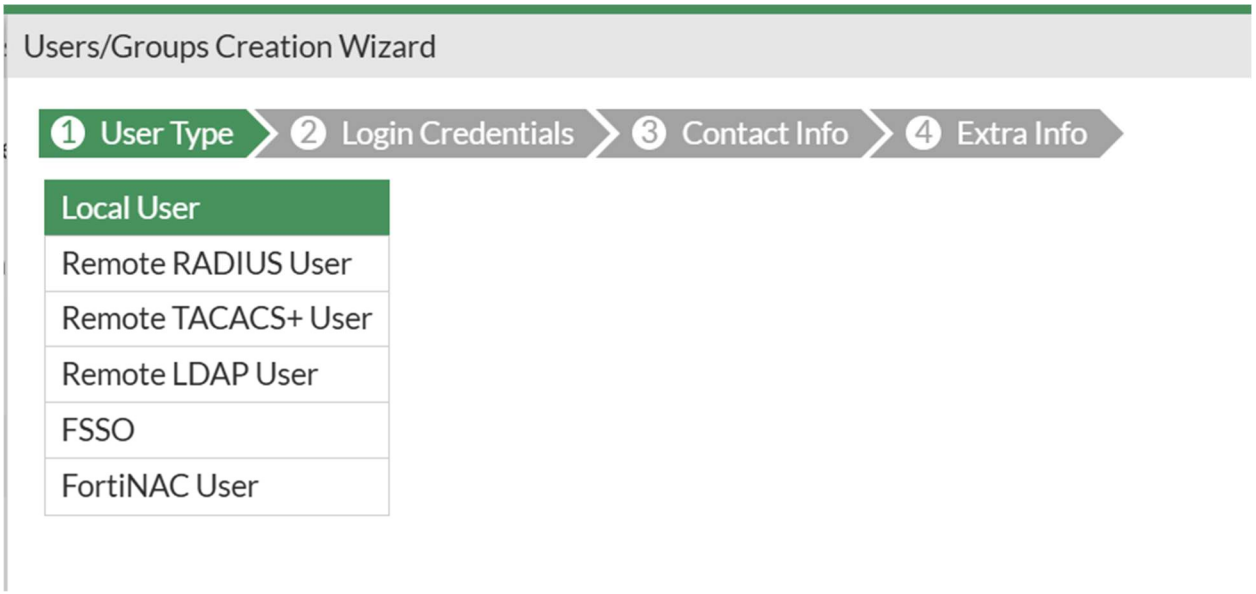
When you see the Edit user group tab **click on members and then click create**



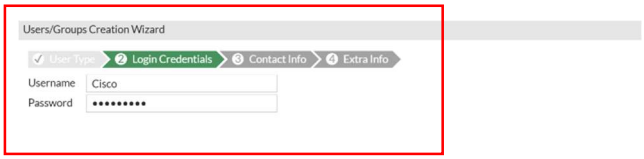
Select user.

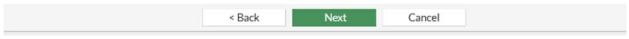


Click **Next** on this screen

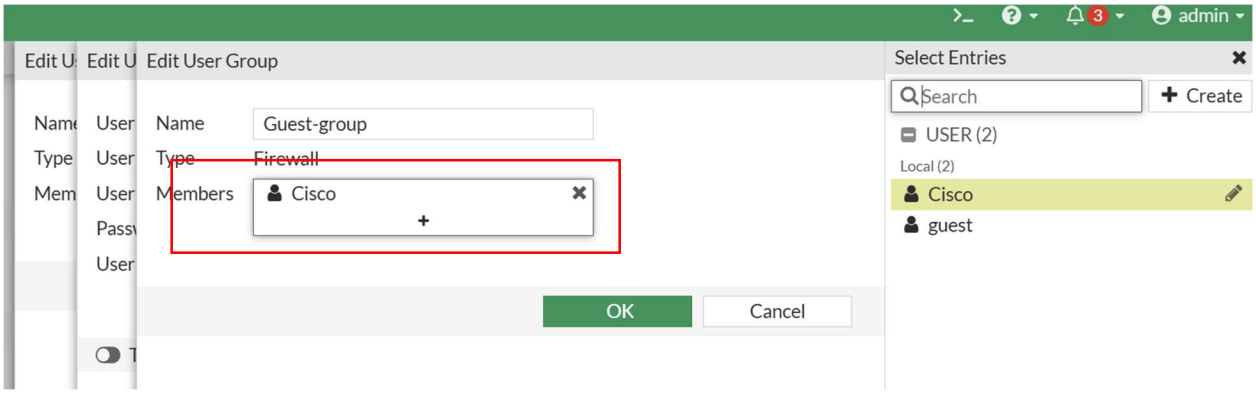


on the login credentials **made a username and password**

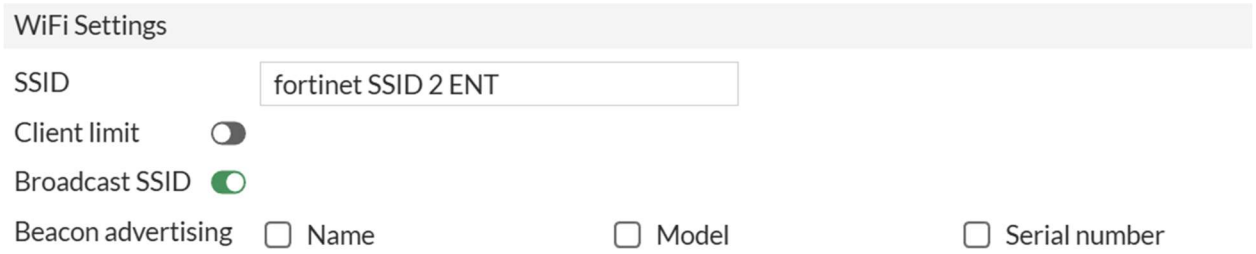


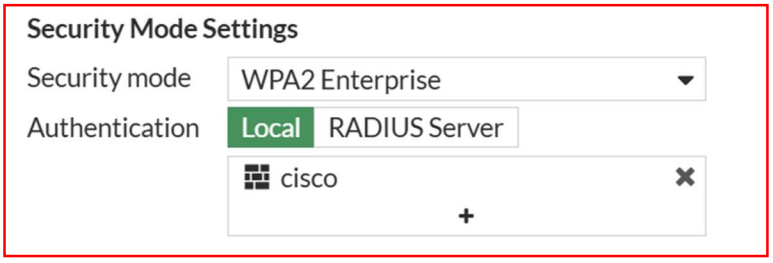


And **Click next until you get to this screen**



Put the new user we created under member and click ok until you can get to the main screen



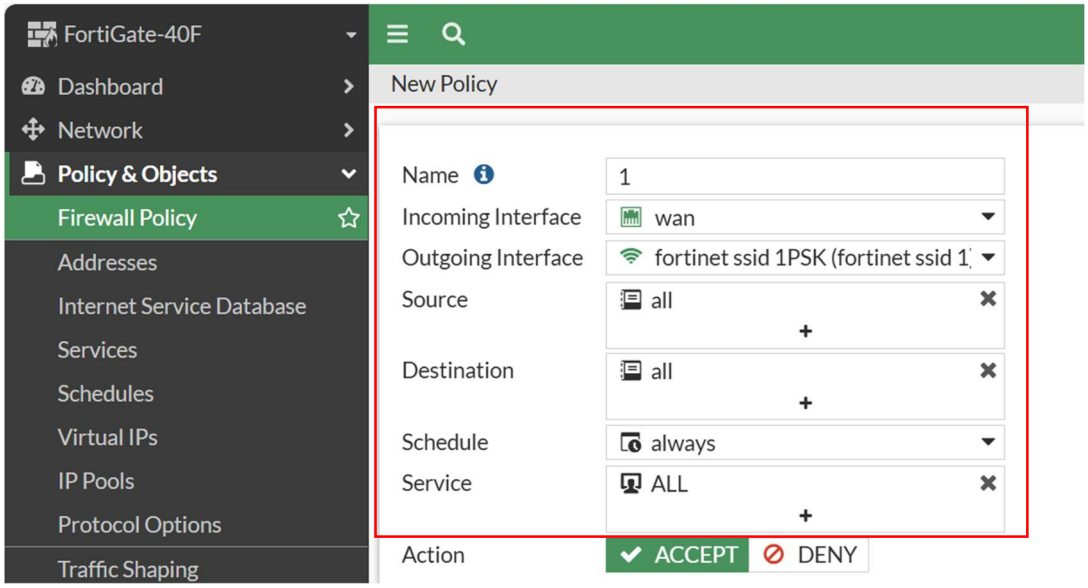


Click ok

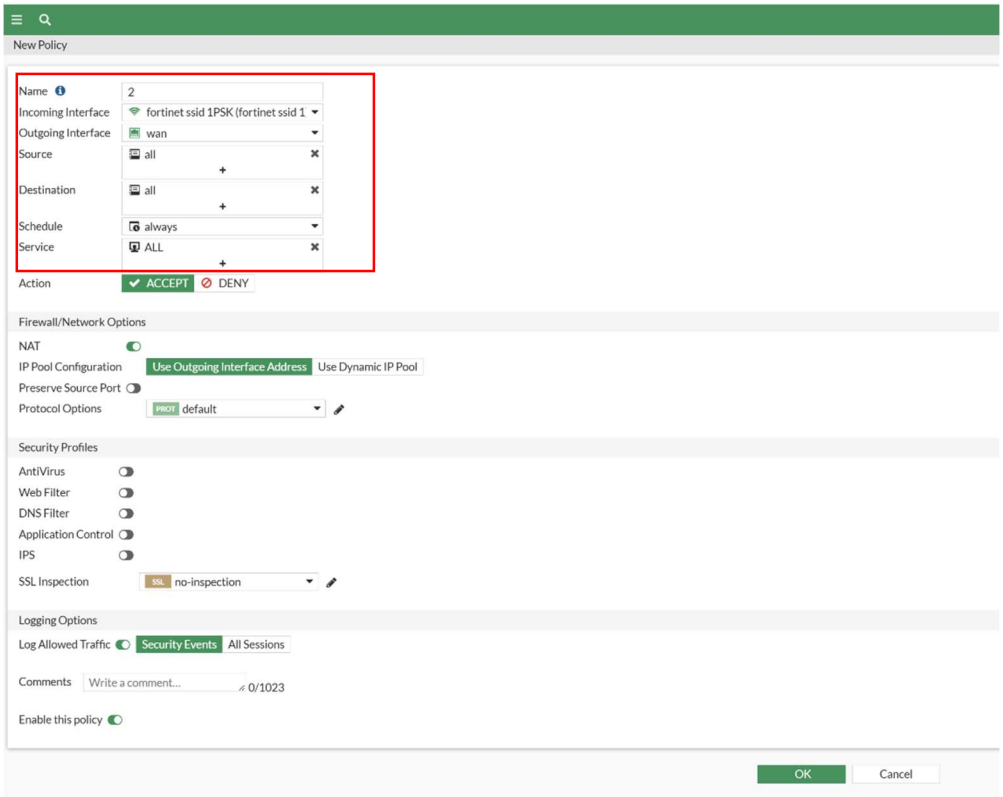
7. Go to **Policy & object -> Firewall policy**

Click create new

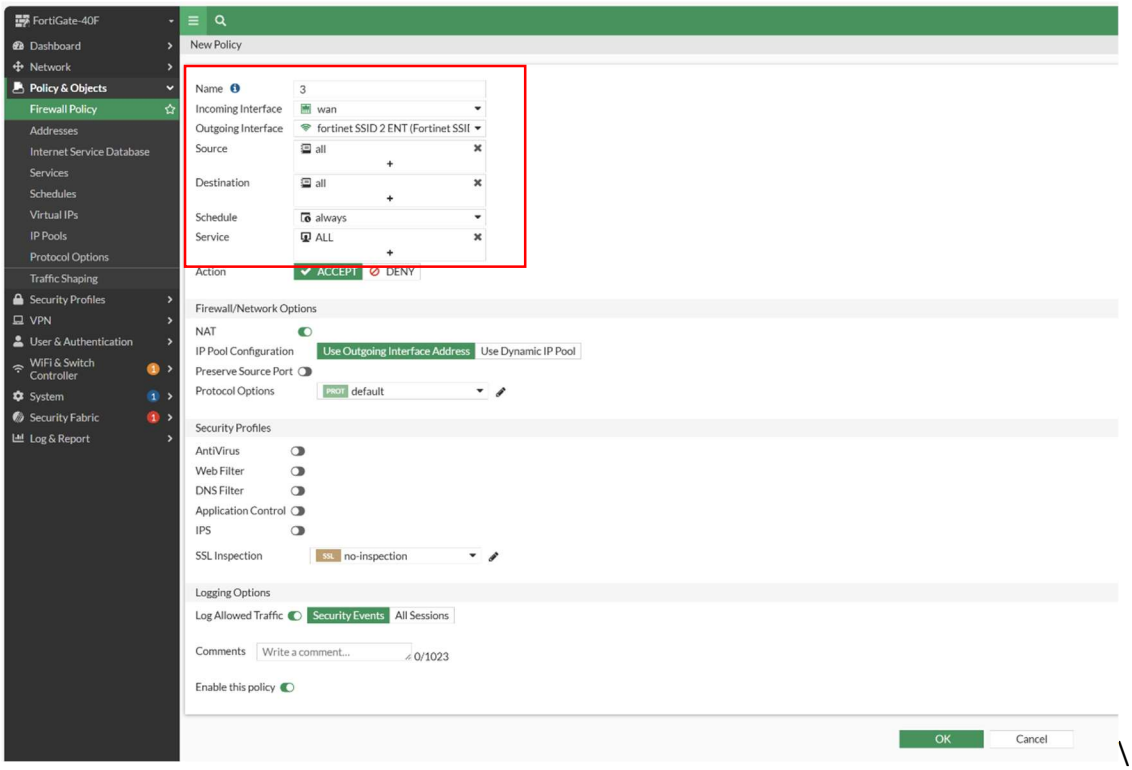
Configure as the following for the first one



For the second one do it as

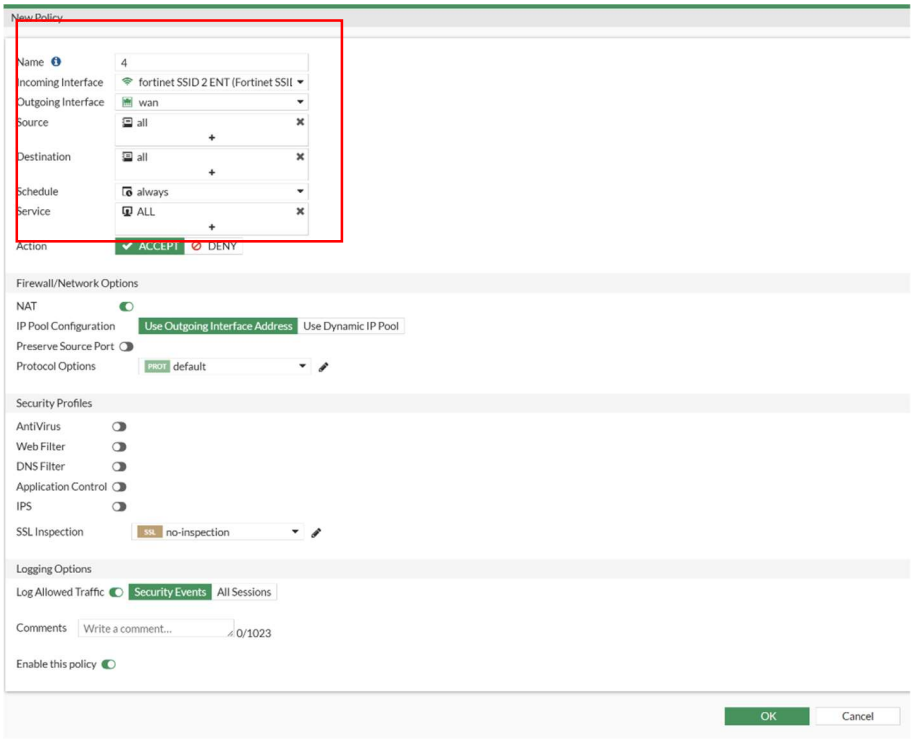


For the third one do it as following



\

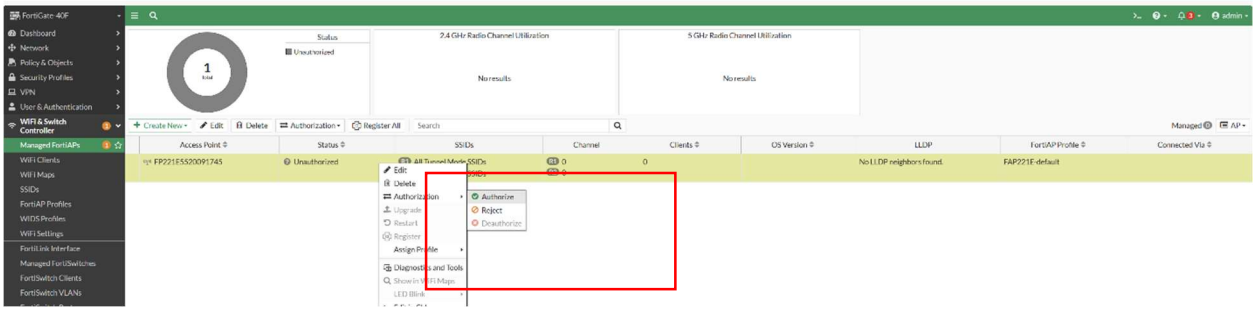
For the fourth one do it as the following



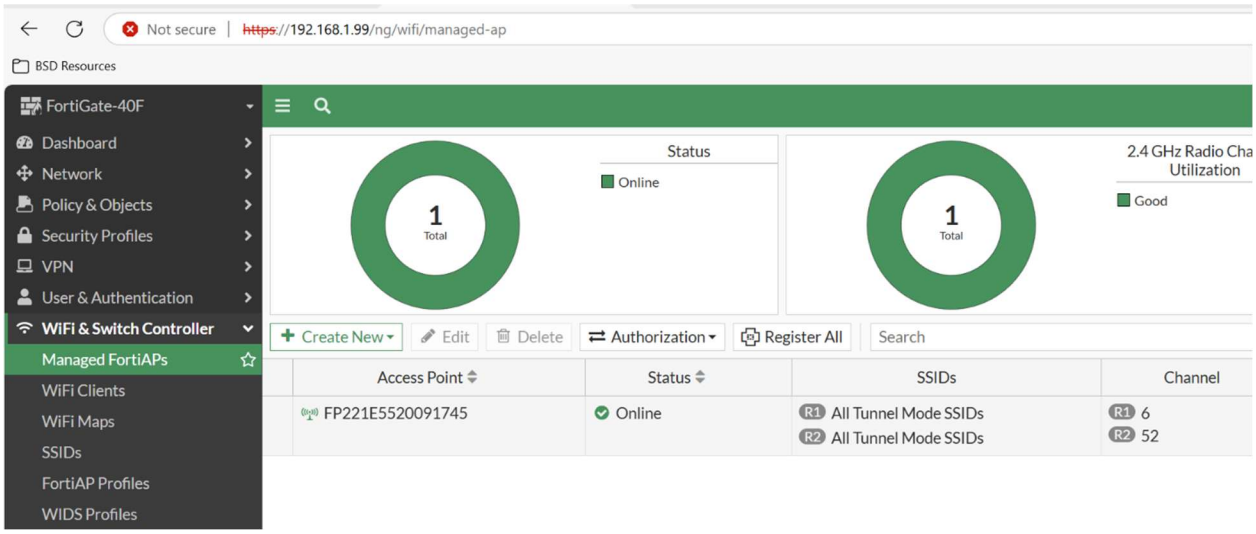
8. Now we will authorize the access point

Go to **Wifi & switch controller -> managed Fortinet aps**

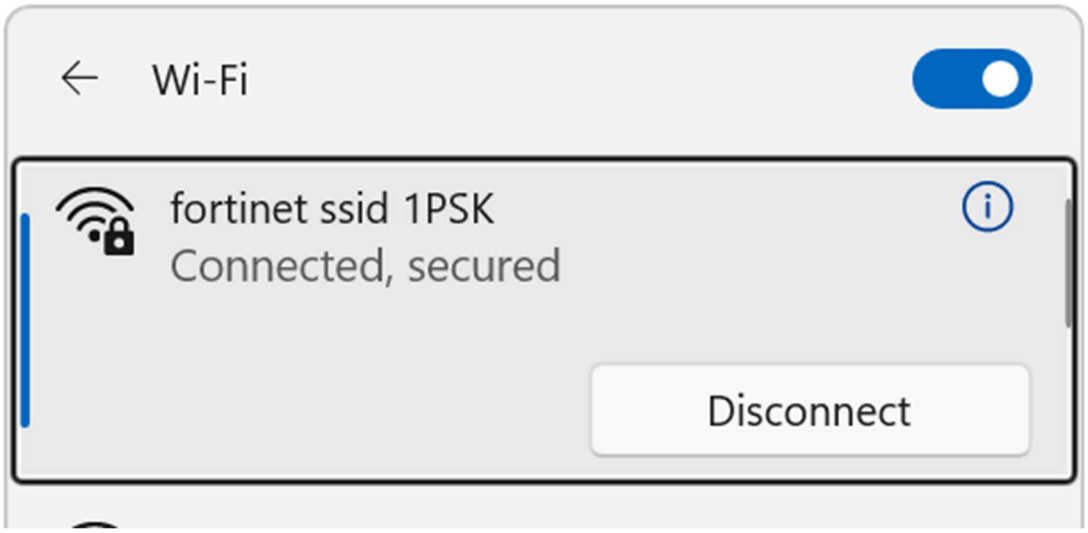
Right click on the ap and press authorize



Now we will wait for it to go online



Now that it is online you should get on a device and try to connect



Problems

1. A firewall policy was not created for all SSIDs, which caused traffic to be able to go into the network, but not out. This caused for our end devices to not be able to gain access to the internet.

Conclusion

In this lab, we successfully set up a SOHO network using a Fortinet FortiWifi 40F series firewall and a Fortinet access point. Two networks were set up, one with WPA2 PSK and one with WPA Enterprise. Firewall policies are set up without any filtering, but exist for future configuration.

Fortinet SSL VPN

Purpose

The purpose of this lab is to set up a SSL VPN using a Fortinet firewall in order to remote desktop from outside a LAN into a device inside the LAN.

Background Information

Virtual Private Networks (VPNs) virtually extend a private network into other networks that may be untrusted or need to be isolated. The goal of a VPN is to allow hosts to exchange network messages across another network and access private network, acting as if they were part of the same network. VPNs rely on tunneling protocols, which transfer network messages from one network to another. Tunneling protocols involve encapsulating and repackaging traffic data into another form, sometimes with encryption. Because of this, tunneling protocols, and thus VPNs, are able to hide the nature of the traffic run through them.

VPNs are able to be used for remote access. Remote access allows one user to access another device connected via the internet or another network and is widely used for technical troubleshooting of customer's problems. They also provide an advantage in security development, since companies are able to permit remote employees to operate from a secure computer within the companies environment.

An SSL (Secure Sockets Layer) VPN allows users to access a network and internal network utilities/directories without specialized software. SSL VPNs provide safe and secure communication for devices regardless of they are connected via public internet or another secure network. An SSL VPN utilizes the SSL or TLS protocol to encrypt traffic. It will automatically use the most secure/updated cryptographic protocol installed on the web browser used to send traffic.

SSL VPNs have two types: portal and tunnel. An SSL portal VPN allows remote users access to internal network resources through a secure web page. No VPN client is needed for a portal VPN. Once connected, users are able to access internal applications such as email, file systems, and the internet. Individual apps can be controlled by admins to permit or deny users specific permissions.

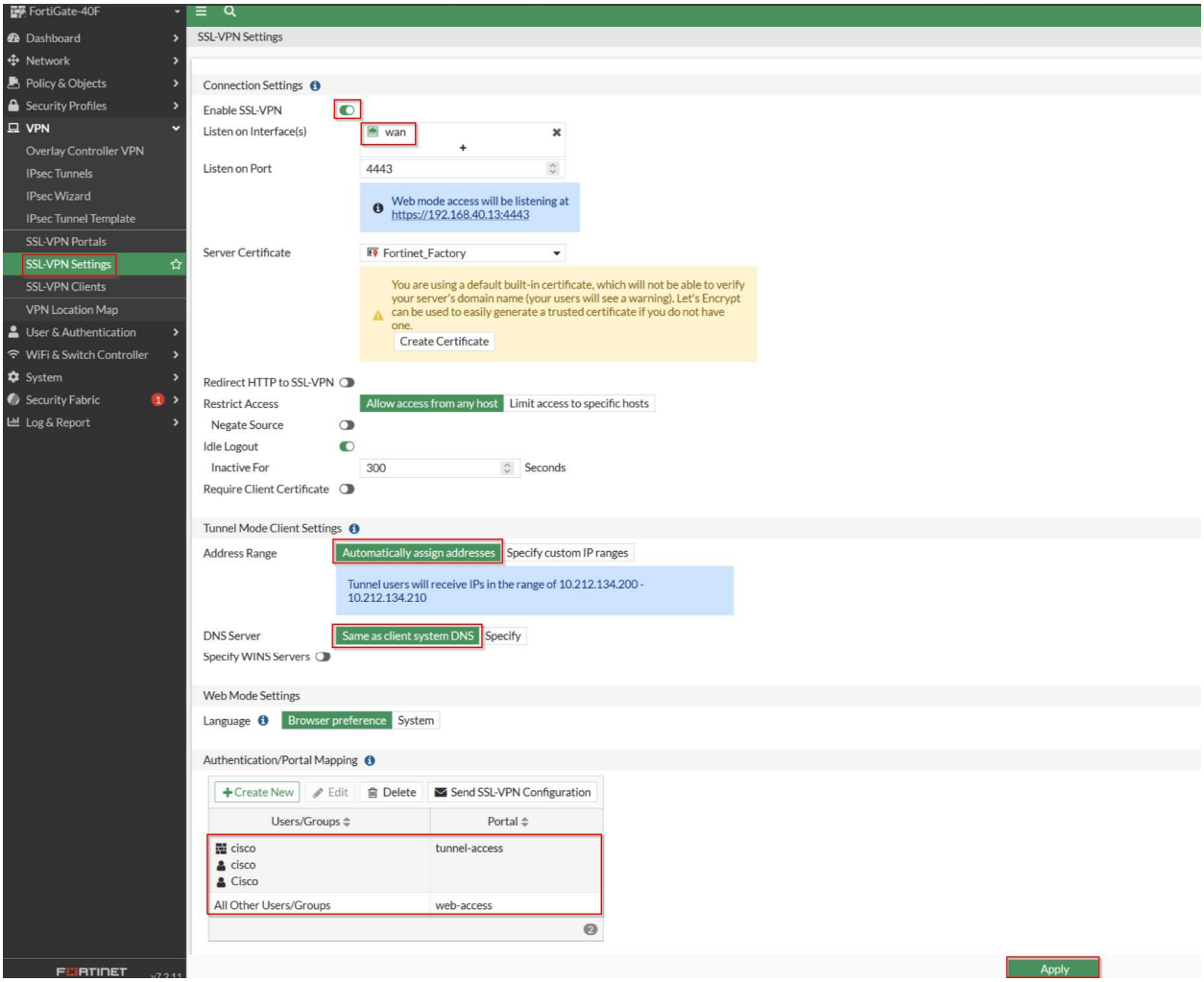
An SSL tunnel VPN provides more flexible access than an SSL portal VPN. It allows security for traffic from non-web applications, such as Outlook or remote desktop, as well as web applications. To enable tunnel functionality, a helper component needs to be installed temporarily. For Fortinet firewalls, this component is Forticlient,

Lab Summary

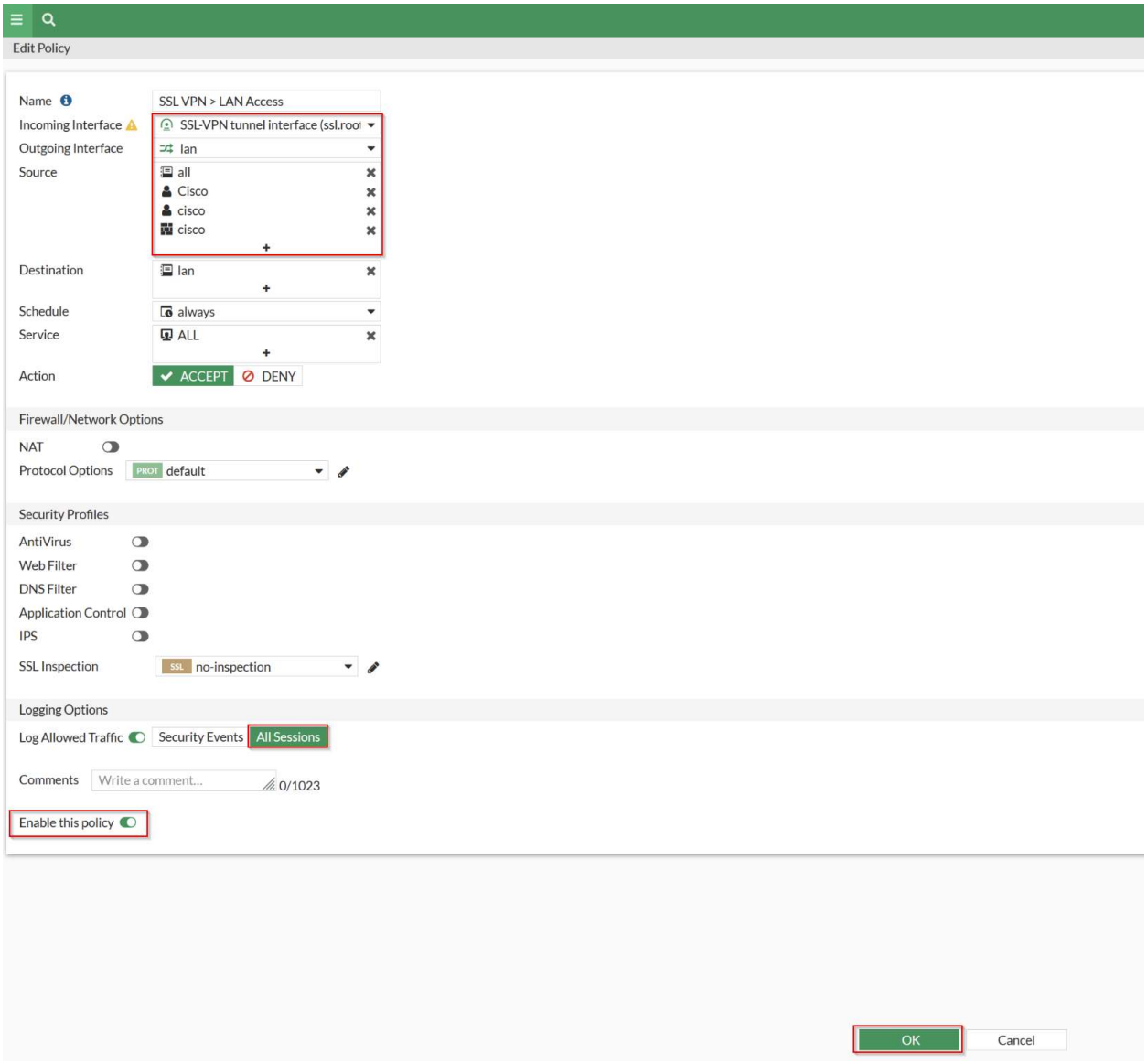
In this lab, you will configure a SSL tunnel VPN through the Fortinet firewall GUI.

Configurations

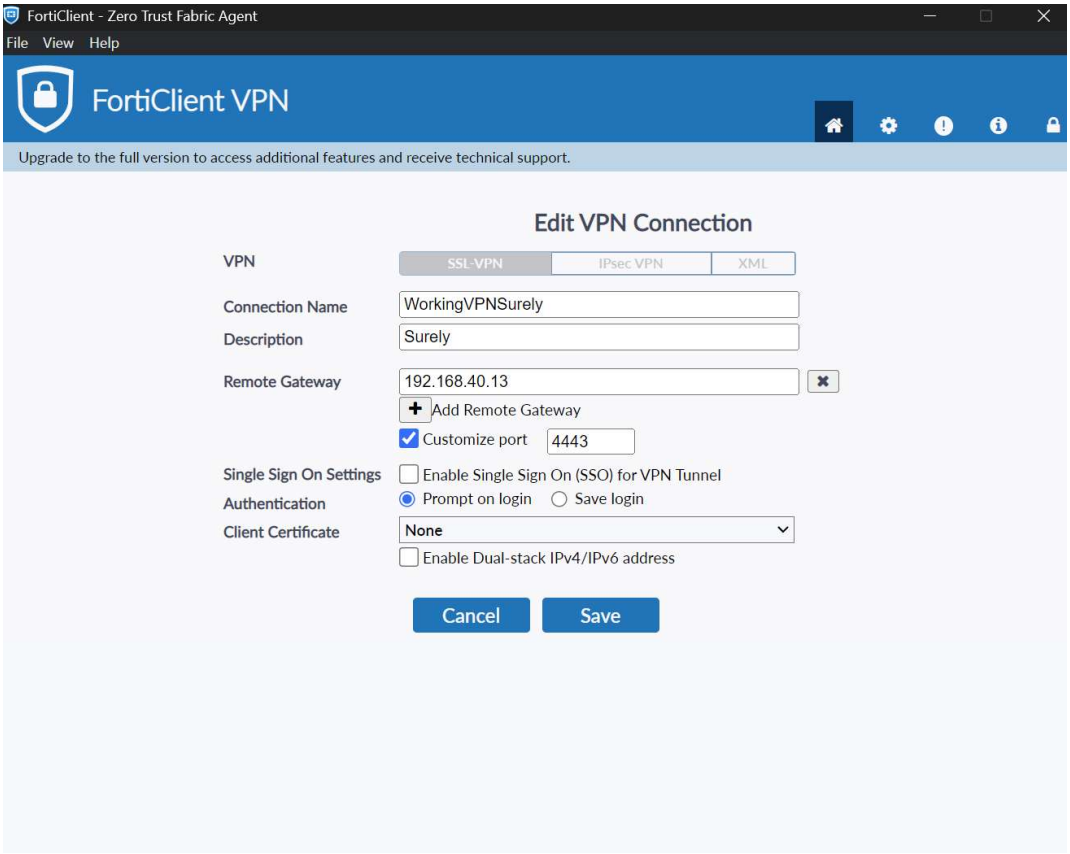
First, navigate to VPN -> SSL-VPN Settings. Enable SSL-VPN, and set it to listen on the WAN interface. Have the VPN automatically assign addresses to users and use the same DNS server as the client system. Then, add the users/groups who should have access to the VPN to the tunnel-access portal. Add all other users/groups to web-access.



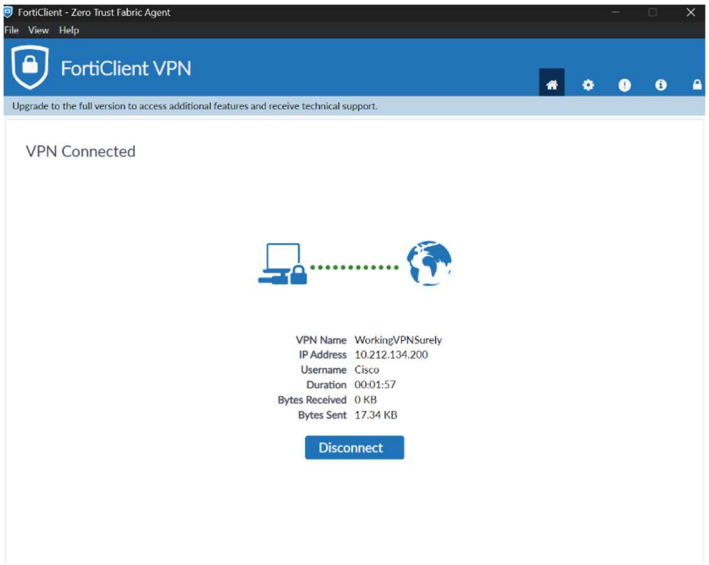
Navigate to Firewall Policy and create a new policy. Assign the incoming interface to the SSL-VPN tunnel interface and the outgoing interface to be the LAN interface. Set the source to all users that should be allowed on the VPN, and the destination as the LAN interface. Then, enable the policy.



Download Forticlient to be used as the connection to the VPN.



Set the remote gateway to be the address that web mode access is listening at during the first step. Set the port number to be the same as the web mode access. Then, save, and click connect to connect to the VPN.



Problems

1. Our inside PC did not have a default gateway due to having a static IP address. Changing the PC to use DHCP allowed it to establish connectivity with another device using the VPN.

Conclusion

In this lab, we successfully configured a Fortinet firewall to allow outside users to connect inside the network using a SSL Tunnel VPN.

Fortinet IPSec VPN

Purpose

The purpose of this lab is to set up a IPsec VPN using a Fortinet firewall in order to remote desktop from outside a LAN into a device inside the LAN.

Background Information

Virtual Private Networks (VPNs) virtually extend a private network into other networks that may be untrusted or need to be isolated. The goal of a VPN is to allow hosts to exchange network messages across another network and access private network, acting as if they were part of the same network. VPNs rely on tunneling protocols, which transfer network messages from one network to another. Tunneling protocols involve encapsulating and repackaging traffic data into another form, sometimes with encryption. Because of this, tunneling protocols, and thus VPNs, are able to hide the nature of the traffic run through them.

A site-to-site VPN is used to connect two or more separate networks over the internet. It creates a permanent, encrypted tunnel between routers/firewalls at each site, and so allow devices on either network to communicate over it, as if they were part of the same LAN. No user interaction is needed for site-to-site VPNs to function.

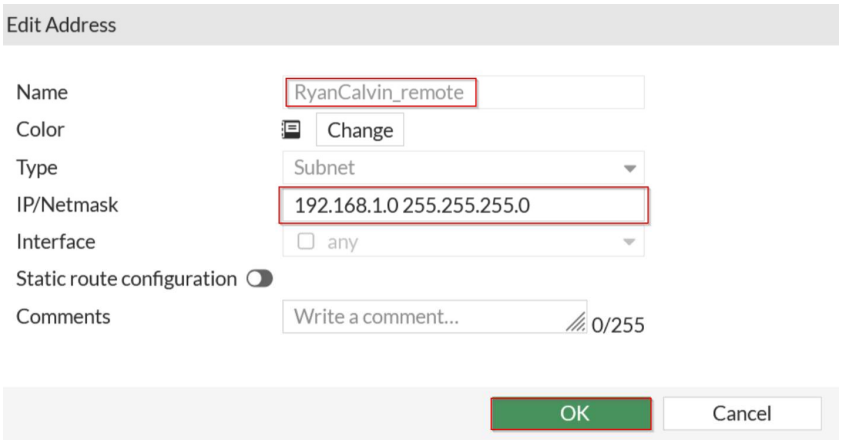
IPsec VPNs provide a private and secure connection between two points, encrypting and authenticating all IP traffic. IPsec VPNs always require a VPN client, as opposed to SSL VPNs only needing it for tunneling. IPsec VPNs also will support all IP traffic, instead of SSL working with the Application layer. However, IPsec will require a more complex setup.

Lab Summary

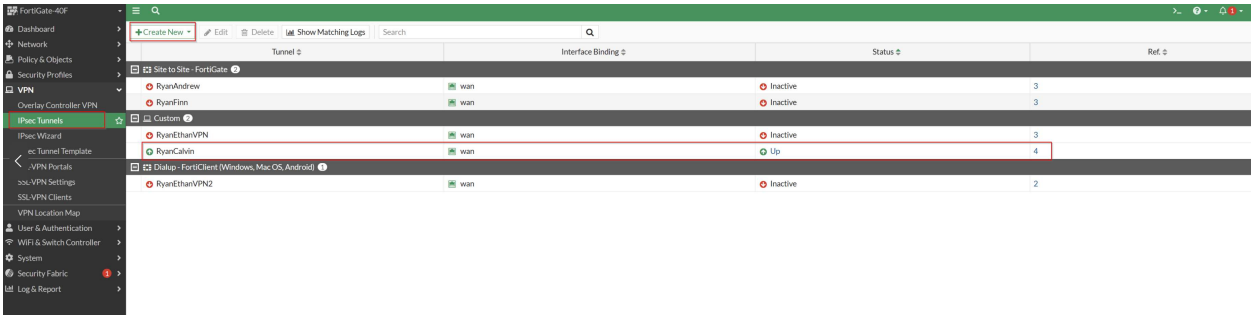
In this lab, you will configure an IPsec VPN through the Fortinet firewall GUI.

Configurations

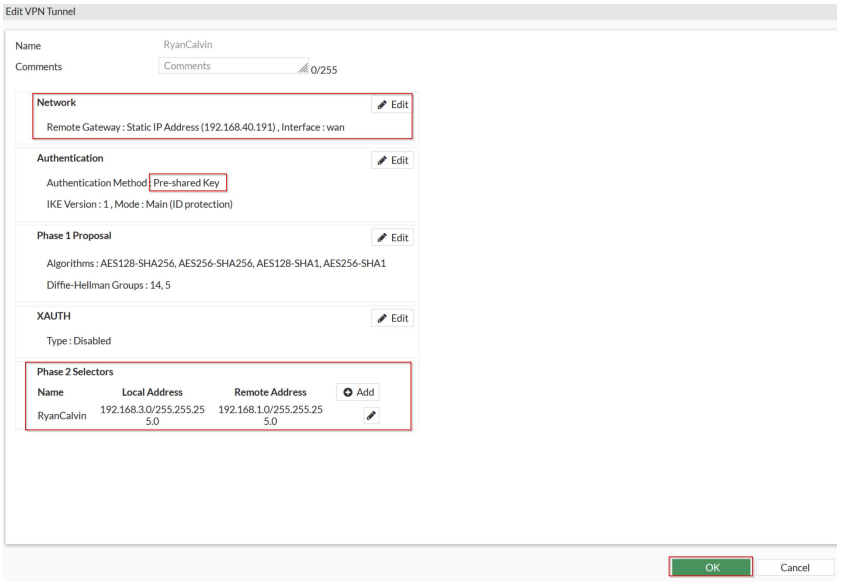
Create an address for the remote network.



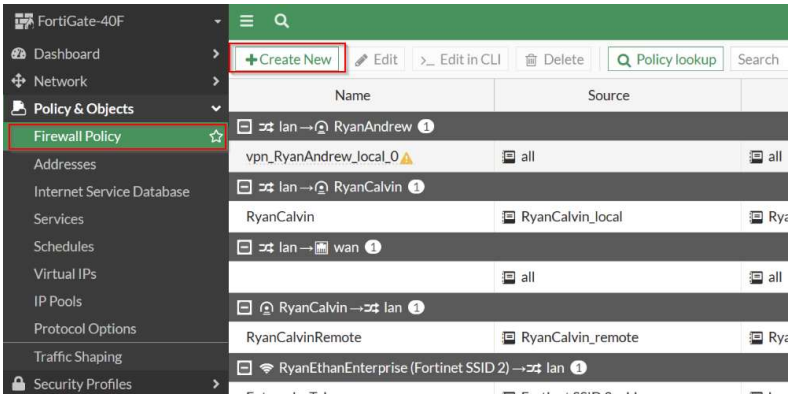
Navigate to VPN -> IPsec Tunnels and click Create New.



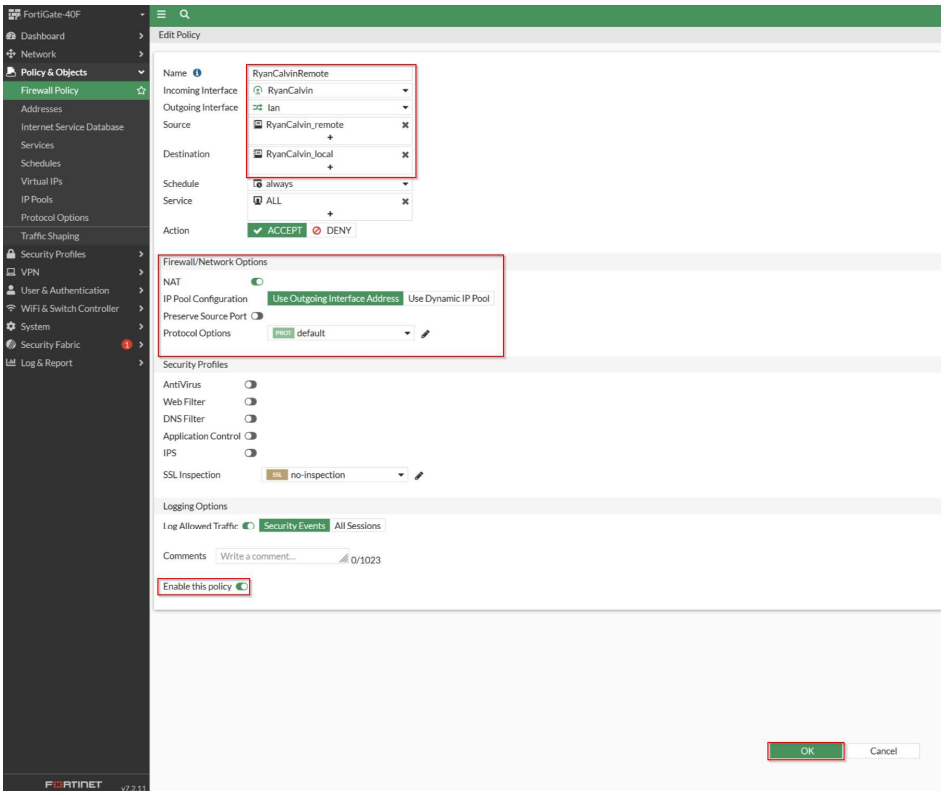
Set the remote gateway as the IP address of the remote firewall. Set authentication to Pre-shared key and create a password. Then, set the local and remote network addresses.



Navigate to Policy & Objects -> Firewall Policy, and create a new policy.



Set the incoming interface and outgoing interface as shown. Set the source address as the remote network, and the destination as the local network. Set the network to use NAT, and enable the policy.



Problems

1. When testing, we tried to use our previously configured access point in order to connect to the network. However, something had went wrong, and the access point had lost its registration. To get around this, we plugged our PC directly into the network, and was able to test from there.

Conclusion

In this lab, we successfully configured a Fortinet firewall to run an IPsec VPN from its own local network to another remote network, and was able to successfully ping and remote desktop through that VPN.