



Networking Portfolio

Ethan Do

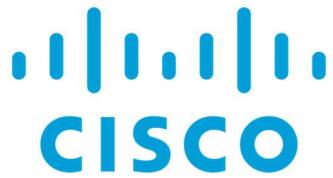


Table of Contents

Windows Setup.....	3
Multi-Area OSPF.....	15
BGP.....	29
iBGP.....	45
AWS Labs 1-3.....	60
AWS Labs 4-6.....	88
Access Point.....	125
IS-IS.....	144
Layer 2 Attacks.....	157
PA-220 Factory Reset.....	167
PA-220 SOHO Network.....	174
PA-220 URL Filtering.....	192
PA-220 VPN.....	204
Fortinet SOHO Network.....	222
Fortinet SSL VPN.....	238
Fortinet IPSec VPN.....	245

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.

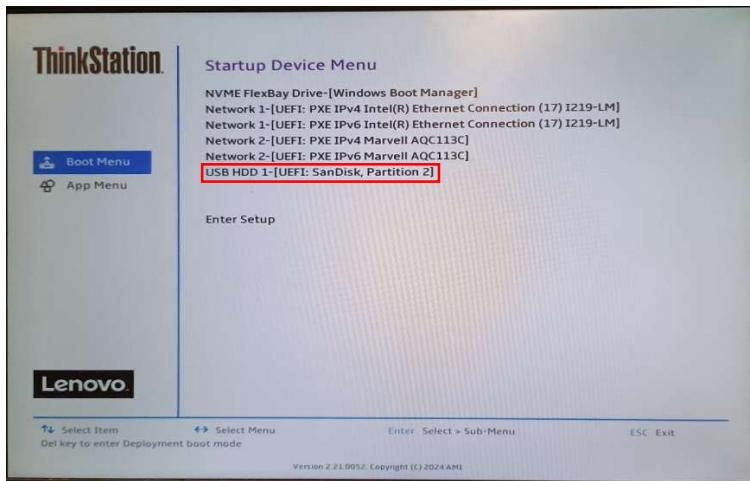
PuTTY is a free SSH and Telnet client used to connect to the console of routers, switches, and other networking devices. PuTTY or similar applications are needed in order to access and modify the configuration of networking devices.

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.

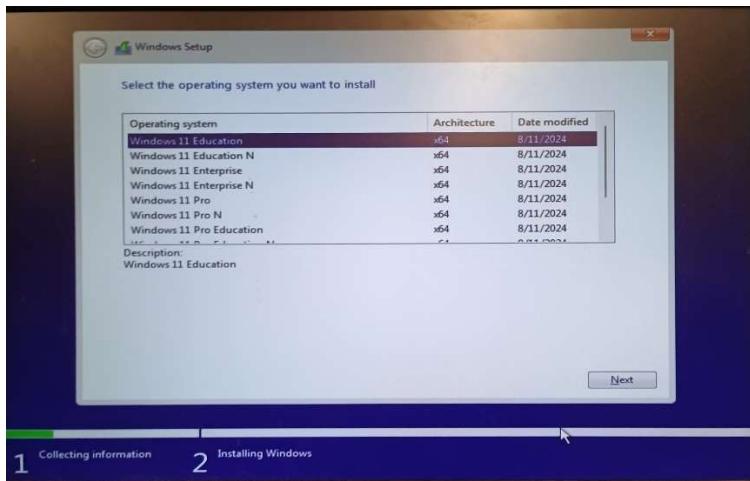
Lenovo Commercial Vantage is a tool used to make sure a device is healthy and up to date. Lenovo Commercial Vantage can also be used to download necessary security updates.

Lab Summary

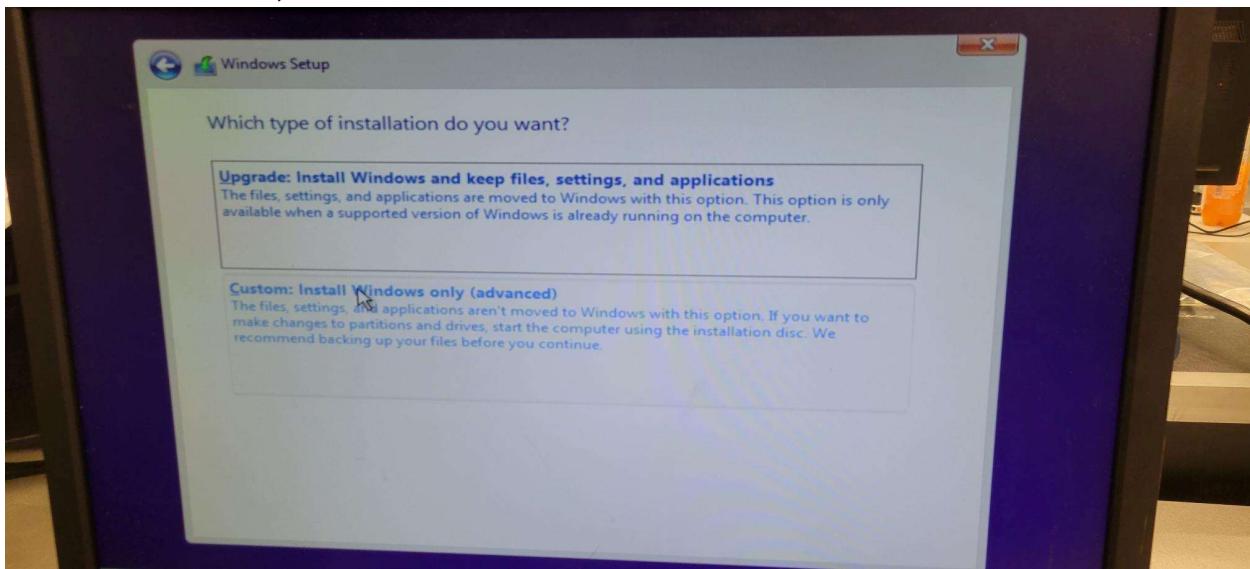
Plug in your flash drive and your USB drive containing Windows 11 Education. During bootup, press F12 until the following screen shows up. Press the option containing “USB”.



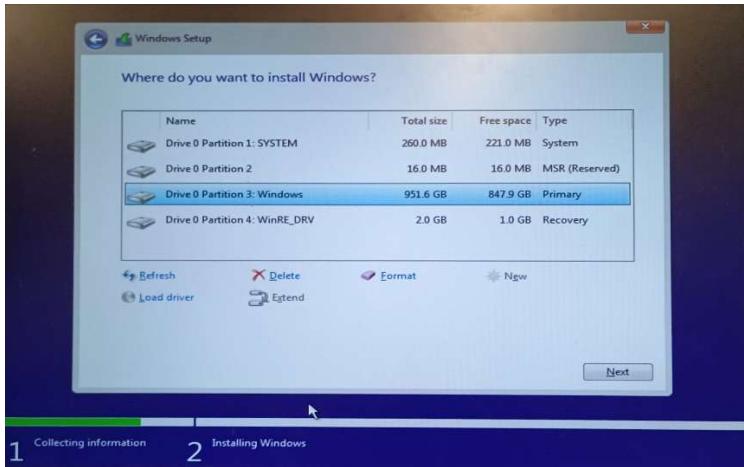
On the next screen, select Windows 11 Education, and click Next.



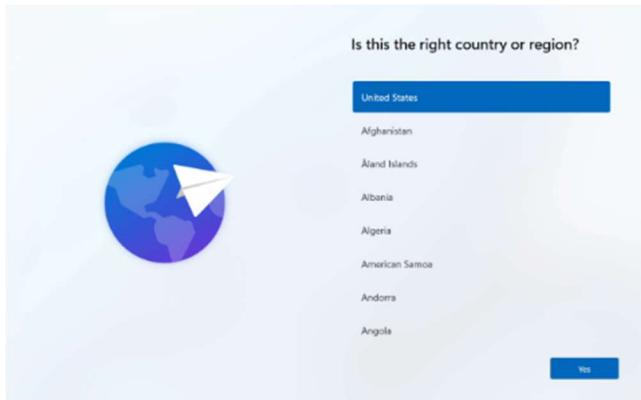
On the next screen, click Custom install.



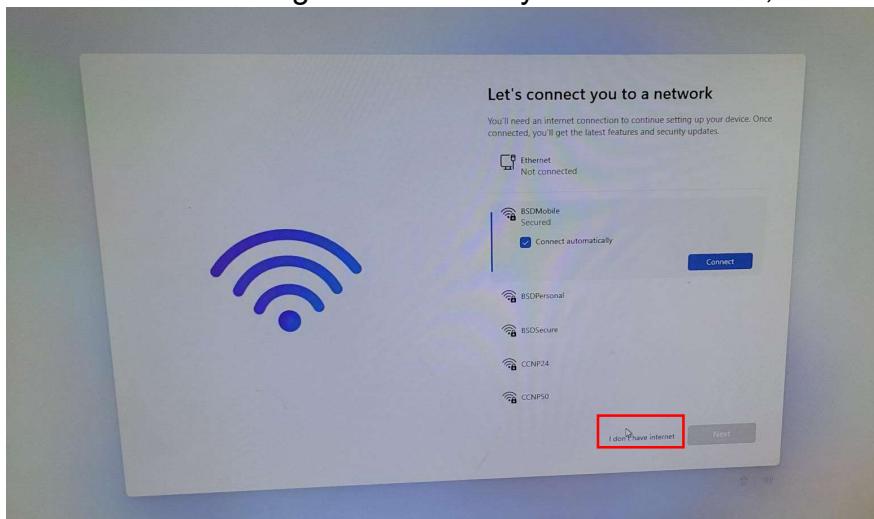
On the next screen, select the partition with a type of “Primary”, and click Next. Wait until installation is complete.



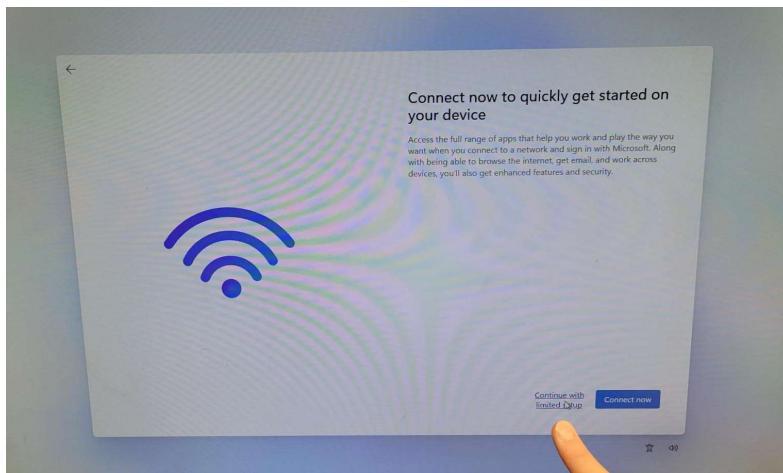
Once Windows is installed, select your country/region, keyboard layout, and second keyboard option.



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.

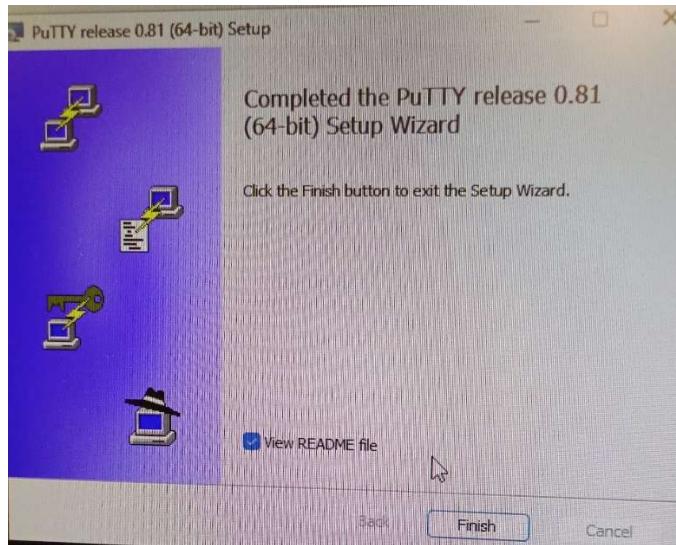
Download PuTTY: latest release (0.81)

[Home](#) | [FAQ](#) | [Feedback](#) | [Licence](#) | [Updates](#) | [Mirrors](#) | [Keys](#) | [Links](#) | [Team](#)
Download: [Stable](#) | [Snapshot](#) | [Docs](#) | [Changes](#) | [Wishlist](#)

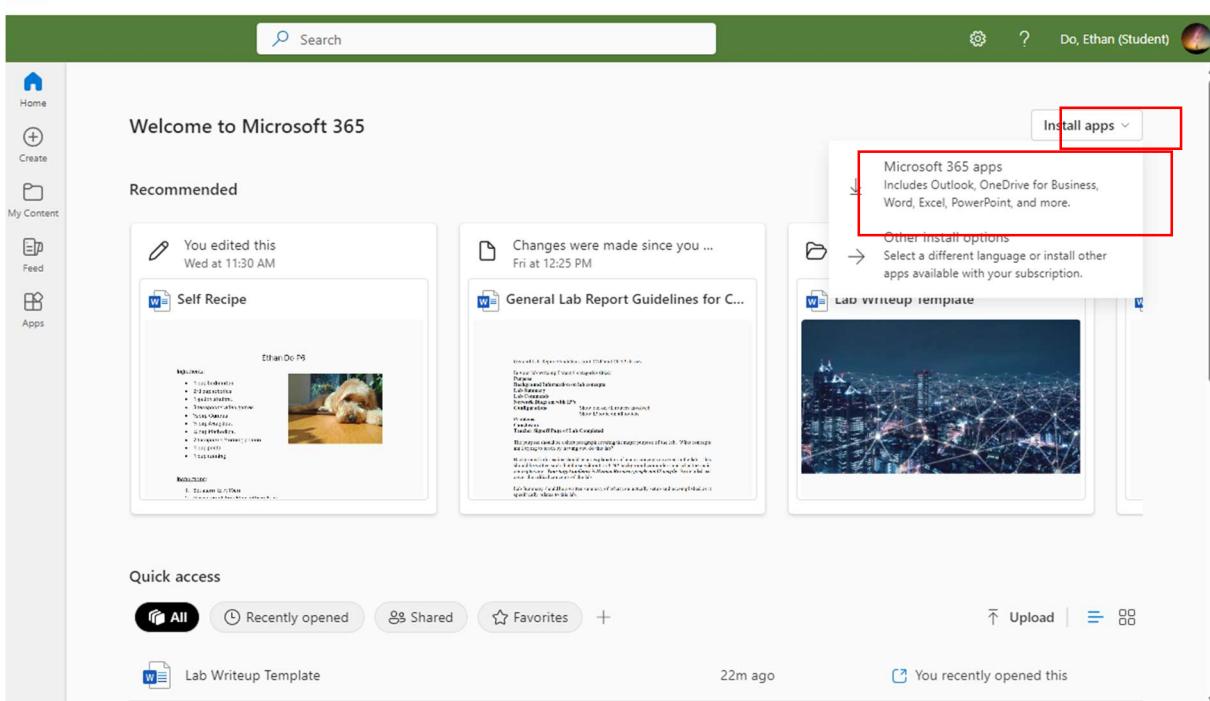
This page contains download links for the latest released version of PuTTY. Currently this is 0.81, released on 2024-04-15.
When new releases come out, this page will update to contain the latest, so this is a good page to bookmark or link to. Alternatively, here is a [permanent link to the 0.81 release](#).
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-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)

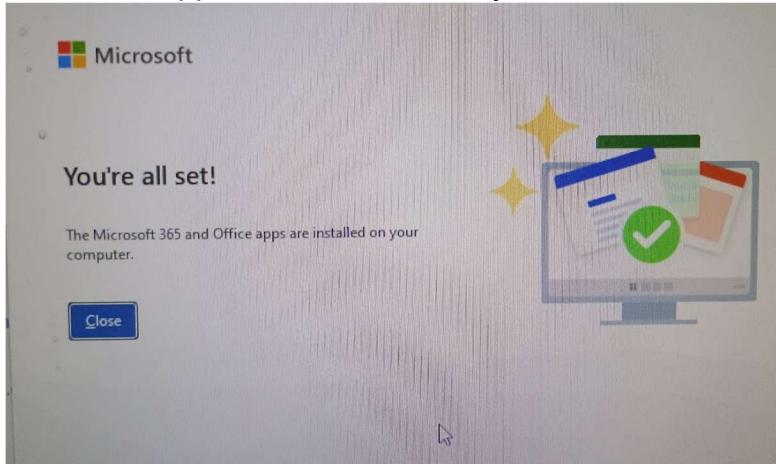
Run the downloaded file and follow the steps in the installer until you reach the following screen.



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.

Lenovo | SHOP SUPPORT COMMUNITY

Support

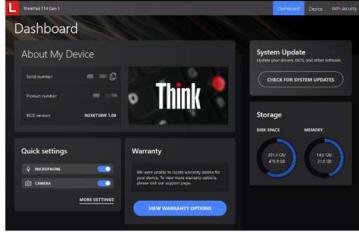
Lenovo Commercial Vantage

Identify Your Device

Enter your serial number, click the detect button, or select your product to find information specific to your device or [Browse Product](#)

[Detect Product](#) If you're using a Lenovo PC, please use the Detect Product button. Lenovo Service Bridge is required to be downloaded.

Enter serial number [Submit](#) [Help me find my product/serial number](#)



Version 10.2407.66.0 (Application and Deployment Guide)
Release Notes
Updated: August 19, 2024

Lenovo Commercial Vantage is for IT Administrators who are responsible for deploying and configuring Windows 10/11 PC's within their organization. For others, Lenovo offers: [Lenovo Vantage](#)

Note: You have agreed to Lenovo License Agreement if you download software from this page. Click here for the [Lenovo License Agreement](#).

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.

7-ZIP

7-Zip is a file archiver with a high compression ratio.

Download 7-Zip 24.08 (2024-08-11) for Windows x64 (64-bit):

Link	Type	Windows	Size
Download	.exe	64-bit x64	1.6 MB

Download 7-Zip 24.08 for another Windows platforms (32-bit x86 or ARM64):

Link	Type	Windows	Size
Download	.exe	32-bit x86	1.3 MB
Download	.exe	64-bit ARM64	1.5 MB

License

7-Zip is free software with open source. The most of the code is under the [GNU GPL](#) license. Some parts of the code are under the BSD 3-clause license. Also there is unRAR license restriction for some parts of the code. Read [7-Zip License](#) information.

You can use 7-Zip on any computer, including a computer in a commercial organization. You don't need to register or pay for 7-Zip.

The main features of 7-Zip

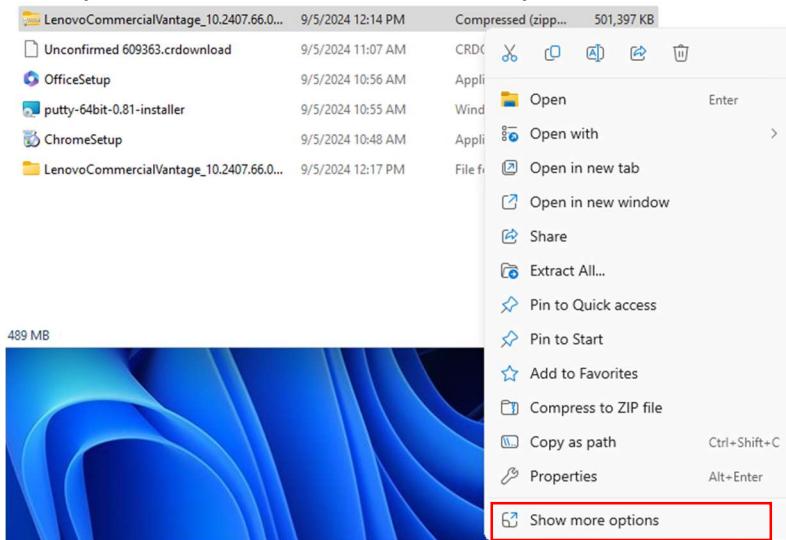
- High compression ratio in [7z format](#) with [LZMA](#) and [LZMA2](#) compression
- Supported formats:
 - Packaging and unpacking: 7z, XZ, BZIP2, GZIP, TAR, ZIP and WIM
 - Unpacking only: AMFS, AR, ARJ, CAB, CHM, CPIO, CramFS, DMG, EXT, FAT, GPT, HFS, IHEX, ISO, LZH, LZMA, MBR, MSI, NSIS, NTFS, QCOW2, RAR, RPM, SquashFS, UDF, UEFI, VDI, VHD, VHDX, VMDK, XAR and Z.
- For ZIP and GZIP formats, 7-Zip provides a compression ratio that is 2-10 % better than the ratio provided by PKZip and WinZip
- Strong AES-256 encryption in 7z and ZIP formats
- Self-extracting capability for 7z format
- Integration with Windows Shell
- Powerful File Manager
- Powerful command line version
- Plugin for FAR Manager
- Localizations for 87 languages

7-Zip works in Windows 11 / 10 / 8 / 7 / Vista / XP / 2022 / 2019 / 2016 / 2012 / 2008 / 2003 / 2000.

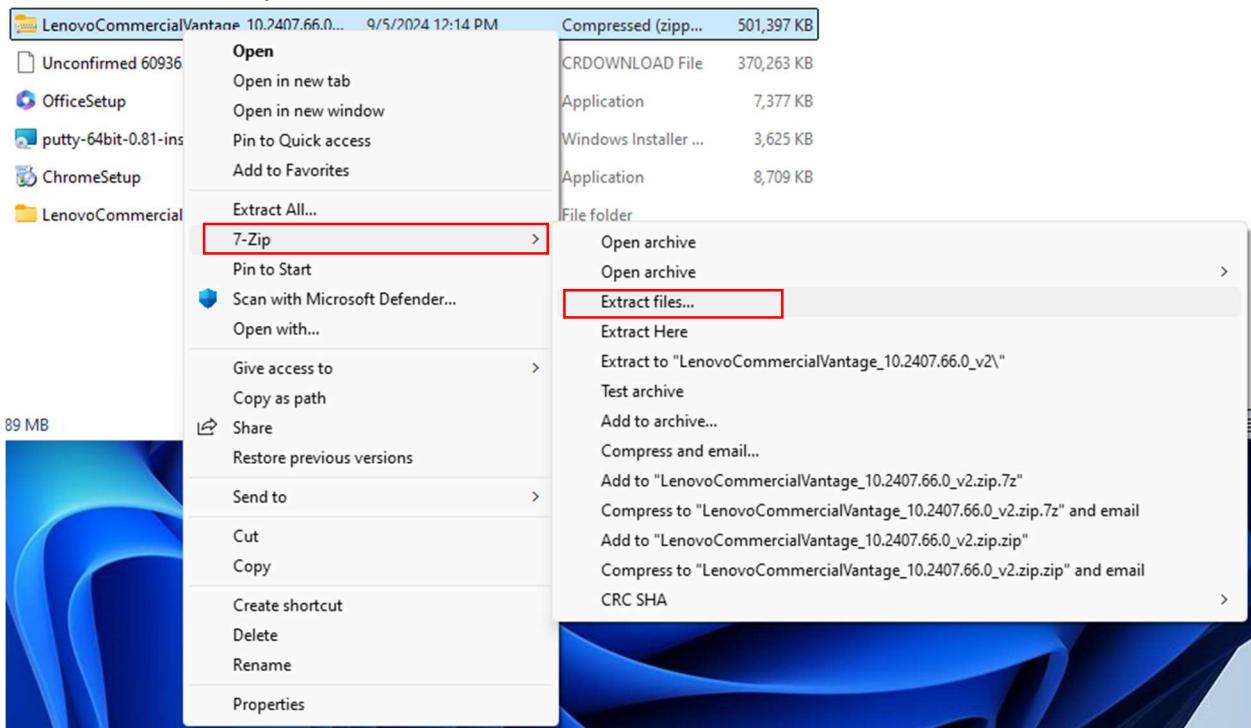
On [7-Zip's SourceForge Page](#) you can find a forum, bug reports, and feature request systems.

Copyright (C) 2024 Igor Pavlov.

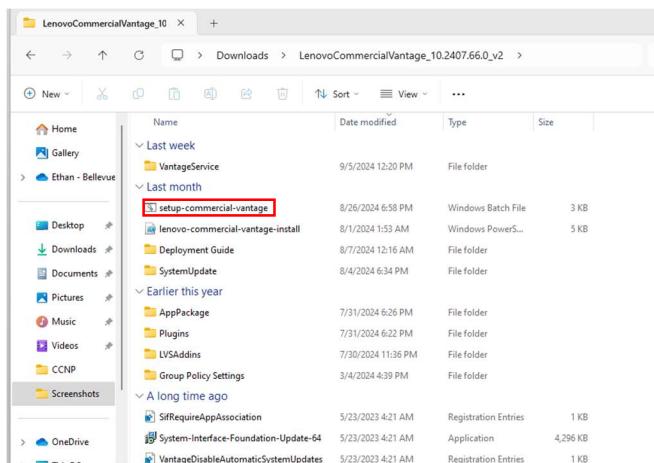
After downloading both the zip file and 7-zip, go to the downloads folder, right click on the zip file, and select “Show more options”.



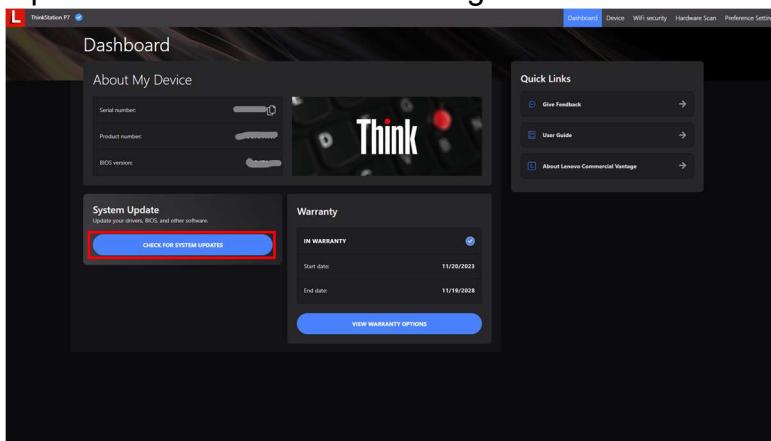
Then, click on 7-zip and extract files.



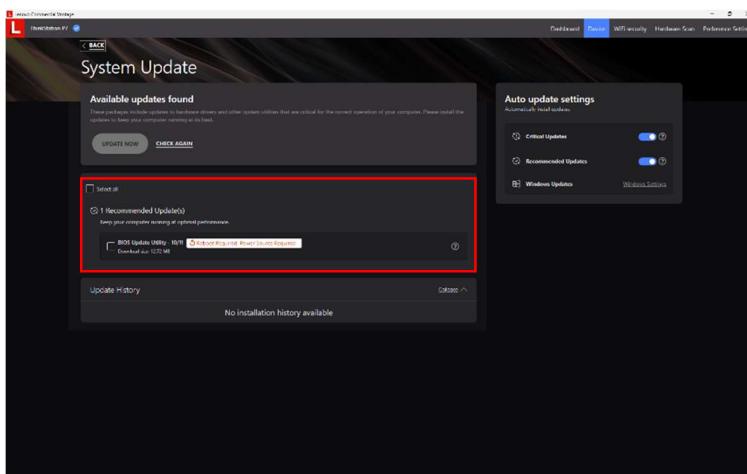
In the extracted folder, run the file “setup-commercial-vantage”. A command prompt window will open. When the window closes itself, Lenovo Commercial Vantage will be installed.



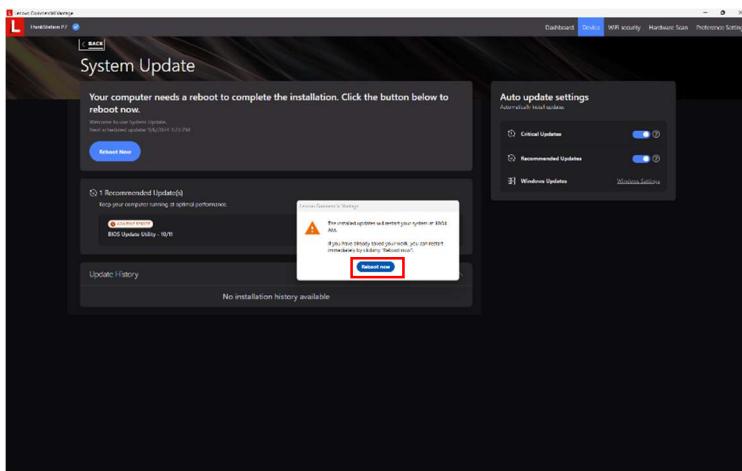
Open Lenovo Commercial Vantage. Click on “Check for System Updates”



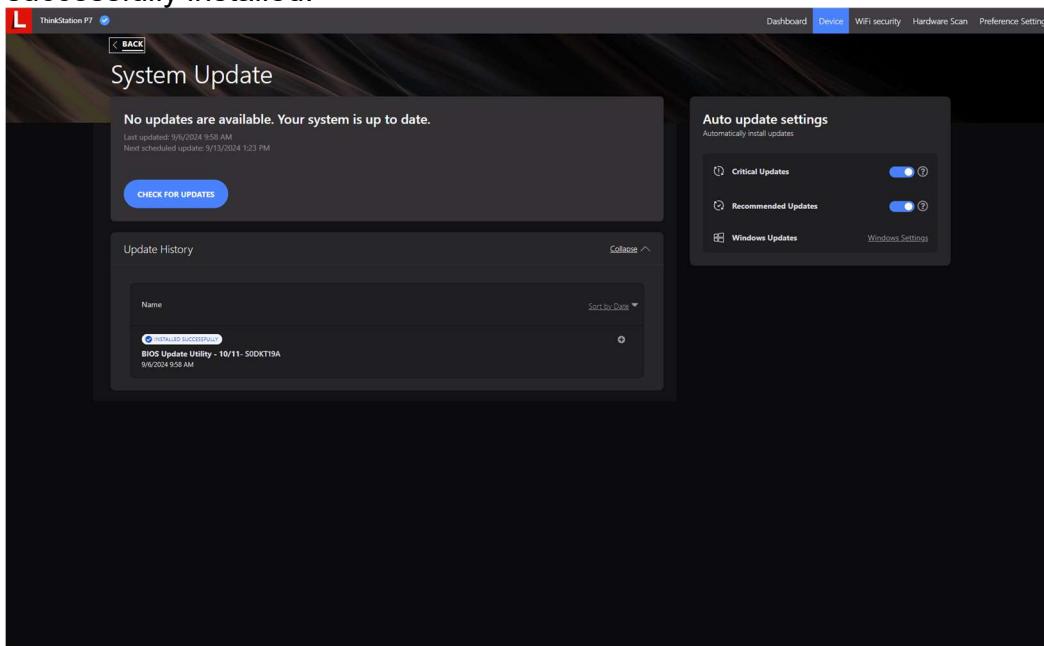
Check any of the recommended Updates and click “Update Now”.



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 3.4×10^{38} 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.

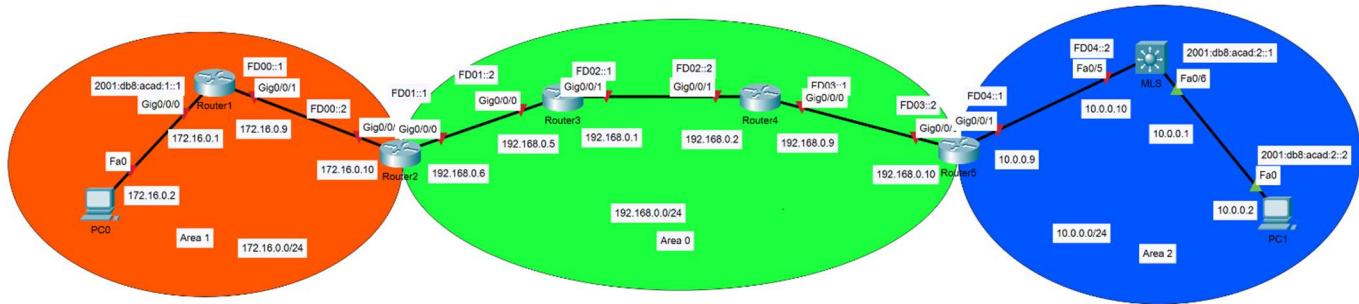
Lab Summary

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 setting 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 from 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 establish 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 takes, 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 for routers to exchange OSPF information. This dependence 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.

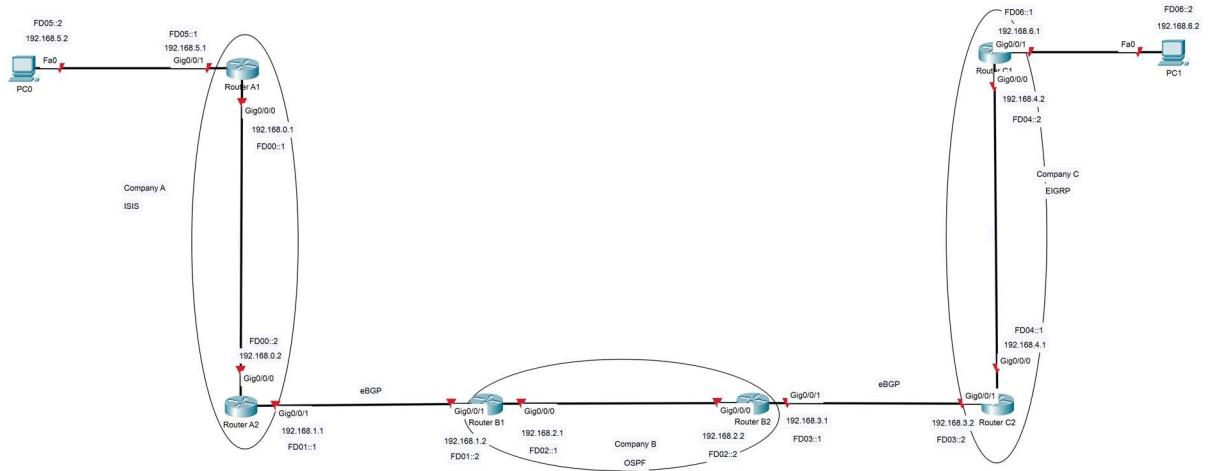
Lab Summary

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 configuring 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 from 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 establish 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 be 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.

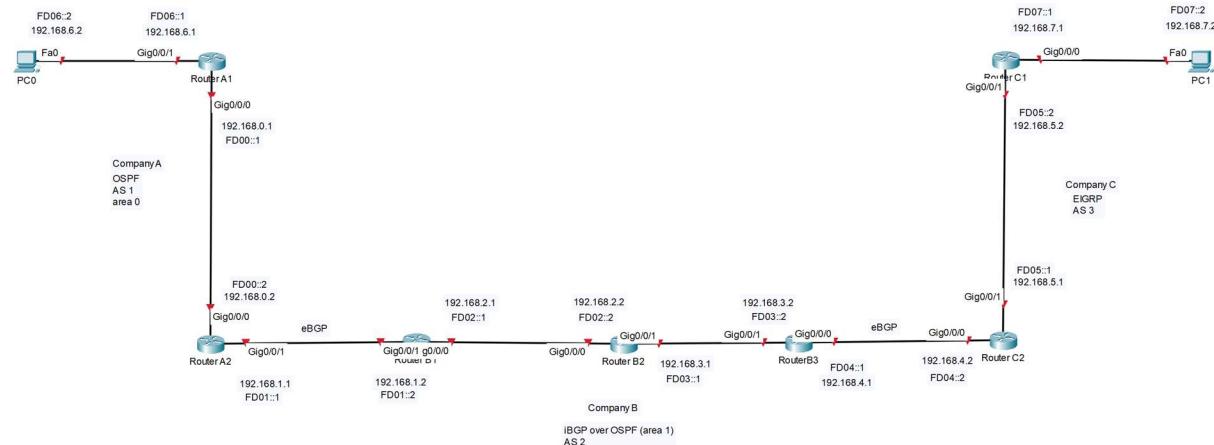
Lab Summary

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 launched. VPC provides the customer control over virtual networking resources, such as 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.

The screenshot shows the AWS Lambda search interface. The search bar at the top has 'IAM' typed into it and is highlighted with a red box. Below the search bar, there are tabs for Services, Features, Resources, Documentation, Knowledge articles, and Marketplace. The 'Services' tab is currently selected and highlighted with a blue underline. Under the Services tab, there are two main sections: 'IAM' and 'IAM Identity Center'. The 'IAM' section is expanded, showing 'Manage access to AWS resources' and a 'Top features' section with tabs for Groups, **Users**, Roles, Policies, and Access Analyzer. The 'Users' tab is also highlighted with a red box. The 'IAM Identity Center' section is collapsed, showing its name and a brief description. The overall interface is dark-themed.

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

The screenshot shows the AWS IAM User groups page. On the left, there is a navigation sidebar for 'Identity and Access Management (IAM)' with a 'User groups' tab highlighted with a red box. The main area displays a table titled 'User groups (3)'. The table has columns for Group name, Users, Permissions, and Creation time. There are three entries: 'EC2-Admin', 'EC2-Support', and 'S3-Support'. The 'S3-Support' entry is highlighted with a red box. The table includes standard AWS UI elements like sorting arrows, a search bar, and pagination controls.

Group name	Users	Permissions	Creation time
EC2-Admin	⚠ 0	Defined	7 minutes ago
EC2-Support	⚠ 0	Defined	7 minutes ago
S3-Support	⚠ 0	Defined	7 minutes ago

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.

S3-Support Info

Delete

Edit

Summary

User group name S3-Support

Creation time January 07, 2025, 10:11 (UTC-08:00)

ARN arn:aws:iam::005656511594 :group/spl66/S3-Support

Users **Permissions** **Access Advisor**

Users in this group (0)

An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.

Add users (highlighted with a red box)

<input type="checkbox"/>	User name	Groups	Last activity	Create date
<input checked="" type="checkbox"/>	user-1	0	None	10 minutes ago
<input type="checkbox"/>	user-2	0	None	10 minutes ago
<input type="checkbox"/>	user-3	0	None	10 minutes ago

Cancel **Add users** (highlighted with a red box)

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

The screenshot shows the AWS IAM Dashboard. On the left, there's a sidebar with 'Identity and Access Management (IAM)' and several navigation links like 'Dashboard', 'Access management', 'Access reports', and 'Access analyzer'. The main area is titled 'IAM Dashboard' and contains sections for 'IAM resources' (User groups: 3, Users: 4, Roles: 13, Policies: 1, Identity providers: 0), 'What's new' (with a list of recent changes), and 'Tools' (Policy simulator). A red box highlights the 'Sign-in URL for IAM users in this account' section, which displays the URL <https://005656511594.signin.aws.amazon.com/console>.

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

The screenshot shows the 'IAM user sign in' page. It has fields for 'Account ID (12 digits) or account alias' (containing '005656511594'), 'IAM username' (containing 'user-1'), and 'Password' (containing 'Lab-Password1'). These three fields are all highlighted with a red border. Below the password field are checkboxes for 'Show Password' (checked) and 'Having trouble?'. A large orange 'Sign in' button is at the bottom, along with links for 'Sign in using root user email', 'Create a new AWS account', and a 'Remember this account' checkbox.

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.

The screenshot shows the AWS Services page. A search bar at the top has "S3" typed into it. Below the search bar, there's a sidebar with links like "Services", "Features", "Resources", etc. The main content area shows three services: "S3 Scalable Storage in the Cloud", "S3 Glacier Archive Storage in the Cloud", and "AWS Snow Family Large Scale Data Transport". The "S3" service card is highlighted with a red border. At the bottom, there's a "Features" section titled "Imports from S3" which includes a "DynamoDB feature".

The screenshot shows the "General purpose buckets" page. It lists one bucket: "samplebucket-b66e7890". The bucket details show it was created on January 7, 2025, at 10:10:51 (UTC-08:00). There are buttons for "Copy ARN", "Empty", and "Delete", along with a "Create bucket" button. The "Name" field contains "samplebucket-b66e7890".

7. Now sign out.

The screenshot shows the "Account" page. The top navigation bar shows "States (N. Virginia)" and the user "user-1 @ 0056-5651-1594". The main content area displays account information: "Account ID" (0056-5651-1594), "IAM user" (user-1), and other account settings like "Organization", "Service Quotas", "Billing and Cost Management", and "Security credentials". At the bottom, there are "Switch role" and "Sign out" buttons. The "Sign out" button is highlighted with a red border.

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

IAM user sign in

Account ID (12 digits) or account alias

IAM username

Password

Show Password

[Having trouble?](#)

 **Sign in**

[Sign in using root user email](#)

[Create a new AWS account](#)

Remember this account

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.

Services

EC2 Virtual Servers in the Cloud

EC2 Image Builder A managed service to automate build, customize and deploy OS images

EC2 Global View EC2 Global View provides a global dashboard and search functionality that lets you fin...

Dashboard <

EC2 Global View

Events

Instances

Instances

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances

Dedicated Hosts

Capacity Reservations

Images

AMIs

AMI Catalog

Elastic Block Store

Volumes

Snapshots

Instances (1/2) [Info](#)

Find Instance by attribute or tag (case-sensitive)

All states ▾

Name	Instance ID	Instance state	Instance type	Status
<input checked="" type="checkbox"/> LabHost	i-0208e98607cc5d7b5	Running	t2.micro	2/2 cfl
<input type="checkbox"/> Bastion Host	i-0e30ea69d11093fcb	Running	t2.micro	2/2 cfl

✖ Failed to stop the instance i-0208e98607cc5d7b5

You are not authorized to perform this operation. User: arn:aws:iam:::Encoded authorization failure message: Z5UPTaYkqFp4TRHZ6-JB81ktkgqTbQrmxE8_Gg3TEK6hShQTL-tZWI46tvrC6oE3W4eg-Oi70_HU8NxsoNrYAHN18BEKfU1GvnZ_l_fPAyct1030WUpCEXpDtApA1gyZa9aPCUE9i1lgSsStZwksnIRO_F_XysvXYk4CaT_pO-S776m4Kji77um7HJ05vpYOibQdc3DnATult84-3r5UiZqEf_yP2TtIGI611LlaQi0ouJtSI9MuibWFDsu1DaXX9aBGUrnpOpayud7UBTsKpSTWehv5ePr54W6ps25Vr_9OI

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

IAM user sign in ⓘ

Account ID (12 digits) or account alias
005656511594

IAM username
user-3

Password
Lab-Password3

Show Password [Having trouble?](#)

Sign in

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.

The screenshot shows the AWS Management Console with a dark theme. In the top navigation bar, the 'aws' logo, a grid icon, a search bar containing 'ec2', and a close button are visible. On the left, a sidebar menu includes 'Services' (selected), 'Features', 'Resources New', 'Documentation', 'Knowledge articles', 'Marketplace', 'Blog posts', 'Events', and 'Tutorials'. The main content area is titled 'Services' and lists three services: 'EC2 Virtual Servers in the Cloud' (selected and highlighted with a red box), 'EC2 Image Builder' (a managed service to automate build, customize and deploy OS images), and 'EC2 Global View' (provides a global dashboard and search functionality). A green success message at the bottom states: 'Successfully initiated stopping of i-0208e98607cc5d7b5'.

Lab 2

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

The screenshot shows the AWS VPC Dashboard. At the top right, there are two buttons: "Create VPC" (highlighted with a red box) and "Launch EC2 Instances". Below these buttons, a note says "Note: Your Instances will launch in the US East region." To the left, there's a "VPC dashboard" section with a "Filter by VPC" dropdown. On the right, there's a "Resources by Region" section with a note "You are using the following Amazon VPC resources".

Create VPC Info

A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as:

VPC settings

Resources to create Info
Create only the VPC resource or the VPC and other networking resources.

VPC only VPC and more

Name tag auto-generation Info
Enter a value for the Name tag. This value will be used to auto-generate Name tags for all resources in the VPC.

Auto-generate
lab

IPv4 CIDR block Info
determine the starting IP and the size of your VPC using CIDR notation.

10.0.0.0/16 65,536 IPs

CIDR block size must be between /16 and /28.

IPv6 CIDR block Info
 No IPv6 CIDR block Amazon-provided IPv6 CIDR block

Tenancy Info
Default

NAT gateways (\$) Info
Choose the number of Availability Zones (AZs) in which to create NAT gateways.
Note that there is a charge for each NAT gateway.

None In 1 AZ 1 per AZ

VPC endpoints Info
Endpoints can help reduce NAT gateway charges and improve security by accessing S3 directly from the VPC. By default, full access policy is used. You can customize this policy at any time.

None S3 Gateway

DNS options Info
 Enable DNS hostnames Enable DNS resolution

Additional tags

Create VPC

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

Create VPC workflow

Success

▼ Details

- ✓ Create VPC: vpc-0fdc83912648edbf6 []
- ✓ Disable DNS hostnames
- ✓ Disable DNS resolution
- ✓ Verifying VPC creation: vpc-0fdc83912648edbf6 []
- ✓ Create subnet: subnet-07bf2b5b71c823f2f []
- ✓ Create subnet: subnet-0ea480dfc6b0e0259 []
- ✓ Create internet gateway: igw-08b4a16b5423bccd []
- ✓ Attach internet gateway to the VPC
- ✓ Create route table: rtb-01a6edcbe36c17748 []
- ✓ Create route
- ✓ Associate route table
- ✓ Allocate elastic IP: eipalloc-0f9f1dde4c33d4d86 []
- ✓ Create NAT gateway: nat-0ff9ce83680556ad9 []
- ✓ Wait for NAT Gateways to activate
- ✓ Create route table: rtb-0a7dfa1c2ef418e78 []
- ✓ Create route
- ✓ Associate route table
- ✓ Verifying route table creation

View VPC

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

VPC dashboard <

EC2 Global View []

Filter by VPC ▾

Virtual private cloud

Your VPCs

Subnets

Route tables

Internet gateways

Egress-only internet gateways

Carrier gateways

DHCP option sets

Subnets (7) Info

Last updated 20 minutes ago

Actions ▾ Create subnet

<input type="checkbox"/>	Name	Subnet ID	State	VPC
<input type="checkbox"/>	-	subnet-0cee9082c19c3cde7	✓ Available	vpc-01651bd9ae2f0f1d4
<input type="checkbox"/>	-	subnet-0f828ad1c4bc790d6	✓ Available	vpc-01651bd9ae2f0f1d4
<input type="checkbox"/>	-	subnet-0fcfcfd38719eae9c	✓ Available	vpc-01651bd9ae2f0f1d4
<input type="checkbox"/>	Work Public Subnet	subnet-0a951c342bb1f8011	✓ Available	vpc-0d3592f67df81c277 Work...
<input type="checkbox"/>	-	subnet-0962fae582475599b	✓ Available	vpc-01651bd9ae2f0f1d4
<input type="checkbox"/>	-	subnet-02edc6e1d6adcec42	✓ Available	vpc-01651bd9ae2f0f1d4
<input type="checkbox"/>	-	subnet-049ea5c189359d322	✓ Available	vpc-01651bd9ae2f0f1d4

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.

[Create subnet](#) Info

VPC

VPC ID
Create subnets in this VPC.

Associated VPC CIDRs

IPv4 CIDRs
10.0.0.0/16

Subnet settings
Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 1

Subnet name
Create a tag with a key of 'Name' and a value that you specify.

The name can be up to 256 characters long.

Availability Zone Info
Choose the zone in which your subnet will reside, or let Amazon choose one for you.

IPv4 VPC CIDR block Info
Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.

IPv4 subnet CIDR block
 256 IPs

Tags - optional

Key	Value - optional
<input type="text" value="Name"/> 	<input type="text" value="lab-subnet-public2"/> Remove

[Add new tag](#)
You can add 49 more tags.
[Remove](#)

[Add new subnet](#)

[Cancel](#) **Create subnet**

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.

Create subnet [Info](#)

VPC

VPC ID

Create subnets in this VPC.

vpc-0bdc83912648edbf6 (lab-vpc)

Associated VPC CIDRs

IPv4 CIDRs

10.0.0.0/16

Subnet settings

Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 1

Subnet name

Create a tag with a key of 'Name' and a value that you specify.

lab-subnet-private2

The name can be up to 256 characters long.

Availability Zone [Info](#)

Choose the zone in which your subnet will reside, or let Amazon choose one for you.

US East (N. Virginia) / us-east-1b

IPv4 VPC CIDR block [Info](#)

Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.

10.0.0.0/16

IPv4 subnet CIDR block

10.0.3.0/24

256 IPs

▼ Tags - optional

Key

Name X

Value - optional

lab-subnet-private2 X

[Remove](#)

[Add new tag](#)

You can add 49 more tags.

[Remove](#)

[Add new subnet](#)

[Cancel](#)

Create subnet

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

The screenshot shows the AWS VPC dashboard with the "Route tables" section selected. A specific route table, "lab-rtb-private1-us-east-1a", is highlighted with a red box. The "Subnet associations" tab is active, and a red box highlights the "Edit subnet associations" button. The table below lists subnet associations:

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
lab-subnet-private1-us-east-1a	subnet-0ea480dfc6b0e0259	10.0.1.0/24	-

Below this, another section titled "Subnets without explicit associations" lists two subnets:

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
lab-subnet-public2	subnet-0510359b043eb5b72	10.0.2.0/24	-
lab-subnet-private2	subnet-0e66c501cf92f4ac7	10.0.3.0/24	-

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

Edit subnet associations

Change which subnets are associated with this route table.

The screenshot shows the "Edit subnet associations" dialog. The "Available subnets" section lists four subnets, with "lab-subnet-private2" selected (highlighted with a red box). The "Selected subnets" section shows the selected subnet:

subnet-0ea480dfc6b0e0259 / lab-subnet-private1-us-east-1a	subnet-0e66c501cf92f4ac7 / lab-subnet-private2
---	--

At the bottom right are "Cancel" and "Save associations" buttons.

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

Route tables (1/6) Info						
		Route table ID	Explicit subnet associ...	Edge associations	Actions	Create route table
<input type="text"/> Find resources by attribute or tag						
<input type="checkbox"/>	Name	rtb-0c8f945161e69c5b5	-	-	Yes	
<input type="checkbox"/>	Work Public Route Table	rtb-09cc6af0e5fec66e	subnet-0a951c342bb1f8...	-	No	
<input type="checkbox"/>	lab-rtb-private1-us-east-1a	rtb-0a7dfa1c2ef418e78	2 subnets	-	No	
<input checked="" type="checkbox"/>	lab-rtb-public	rtb-01a6edcbe36c17748	subnet-07bf2b5b71c823f...	-	No	
<input type="checkbox"/>	-	rtb-052537ca24c362056	-	-	Yes	
<input type="checkbox"/>	-	rtb-07526285a887575e3	-	-	Yes	

rtb-01a6edcbe36c17748 / lab-rtb-public

- [Details](#) | [Routes](#) | [Subnet associations](#) Subnet associations
- [Edge associations](#) | [Route propagation](#) | [Tags](#)

Explicit subnet associations (1)				Edit subnet associations
<input type="text"/> Find subnet association				< 1 >
Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	
lab-subnet-public1-us-east-1a	subnet-07bf2b5b71c823f2f	10.0.0.0/24	-	

Subnets without explicit associations (1)				Edit subnet associations
The following subnets have not been explicitly associated with any route tables and are therefore associated with the main route table:				< 1 >
Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	
lab-subnet-public2	subnet-0510359b043eb5b72	10.0.2.0/24	-	

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

Edit subnet associations

Change which subnets are associated with this route table.

Available subnets (2/4)					
<input type="text"/> Filter subnet associations					
<input type="checkbox"/>	Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
<input type="checkbox"/>	lab-subnet-private1-us-east...	subnet-0ea480dfc6b0e0259	10.0.1.0/24	-	rtb-0a7dfa1c2ef418e78 / lab-rtb-pr...
<input checked="" type="checkbox"/>	lab-subnet-public1-us-east-1a	subnet-07bf2b5b71c823f2f	10.0.0.0/24	-	rtb-01a6edcbe36c17748 / lab-rtb-p...
<input checked="" type="checkbox"/>	lab-subnet-public2	subnet-0510359b043eb5b72	10.0.2.0/24	-	Main (rtb-07526285a887575e3)
<input type="checkbox"/>	lab-subnet-private2	subnet-0e66c501cf92f4ac7	10.0.3.0/24	-	rtb-0a7dfa1c2ef418e78 / lab-rtb-pr...

Selected subnets

[subnet-07bf2b5b71c823f2f / lab-subnet-public1-us-east-1a X](#) [subnet-0510359b043eb5b72 / lab-subnet-public2 X](#)

[Cancel](#) Save associations

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

VPC dashboard

Security Groups (4) Info

Create security group

Name	Security group ID	Security group name	VPC ID
-	sg-0944bde9e4f468e39	Ec2SecurityGroup	vpc-0d3592f67df81c2
-	sg-08e973e77eca6610a	default	vpc-0d3592f67df81c2
-	sg-08012bfbd195062b	default	vpc-0bdc83912648edb6
-	sg-02b3eed0cff779a6b	default	vpc-01651bd9ae2f0f1

Create security group Info

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

Basic details

Security group name Info
Web Security Group
Name cannot be edited after creation.

Description Info
Enable HTTP access

VPC Info
vpc-0bdc83912648edb6 (lab-vpc)

Inbound rules Info

Type Info: HTTP **Protocol** Info: TCP **Port range** Info: 80 **Source** Info: Anywhere... **Description - optional** Info: Permit web requests **Delete**

Add rule

⚠ Rules with source of 0.0.0.0/0 or ::/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

Outbound rules Info

Type Info: All traffic **Protocol** Info: All **Port range** Info: All **Destination** Info: Custom **Description - optional** Info: 0.0.0.0/0 **Delete**

Add rule

⚠ Rules with destination of 0.0.0.0/0 or ::/0 allow your instances to send traffic to any IPv4 or IPv6 address. We recommend setting security group rules to be more restrictive and to only allow traffic to specific known IP addresses.

Tags - optional

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

No tags associated with the resource.

Add new tag

You can add up to 50 more tags

Create security group

12. Open EC2 and launch a new instance.

Launch instance

To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.

Launch instance



Migrate a server

Note: Your instances will launch in the US East (N. Virginia) Region

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.

Launch an instance

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags

Name

Web Server 1

Add additional tags

▼ Application and OS Images (Amazon Machine Image)

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

Quick Start



Browse more AMIs
Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

Amazon Linux 2023 AMI

ami-01816d0761128cd2d (64-bit (x86), uefi-preferred) / ami-02dcfe5d1d39baa4e (64-bit (Arm), uefi)
Virtualization: hvm ENA enabled: true Root device type: ebs

Free tier eligible

Description

Amazon Linux 2023 is a modern, general purpose Linux-based OS that comes with 5 years of long term support. It is optimized for AWS and designed to provide a secure, stable and high-performance execution environment to develop and run your cloud applications.

Amazon Linux 2023 AMI 2023.6.20241212.0 x86_64 HVM kernel-6.1

Architecture

64-bit (x86)

Boot mode

uefi-preferred

AMI ID

ami-01816d07b1128cd2d

Username

ec2-user

▼ Instance type | Get advice

Instance type

t2.micro

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

Free tier eligible

All generations

[Compare instance types](#)

[Additional costs apply for AMIs with pre-installed software](#)

▼ Key pair (login)

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 - required

vockey

Create new key pair

▼ Network settings [Info](#)

VPC - required [Info](#)

vpc-0bdc83912648edbf6 (lab-vpc)
10.0.0.0/16

Subnet [Info](#)

subnet-0510359b043eb5b72 lab-subnet-public2
VPC: vpc-0bdc83912648edbf6 Owner: 426467693130 Availability Zone: us-east-1b
Zone type: Availability Zone IP addresses available: 251 CIDR: 10.0.2.0/24



[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

[Compare security group rules](#)

Common security groups [Info](#)

Select security groups

Web Security Group sg-002c91fe3e5c7c097
VPC: vpc-0bdc83912648edbf6

Security groups that you add or remove here will be added to or removed from all your network interfaces.

► Advanced network configuration

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 using the public IPv4 address.

EC2 > Instances > Launch an instance

Success
Successfully initiated launch of instance (i-0abe9ae45e4284a78)

Launch log

Next Steps

What would you like to do next with this instance, for example "create alarm" or "create backup"

1 2 3 4 5 6

Create billing and free tier usage alerts	Connect to your instance	Connect an RDS database	Create EBS snapshot policy
To manage costs and avoid surprise bills, set up email notifications for billing and free tier usage thresholds.	Once your instance is running, log into it from your local computer.	Configure the connection between an EC2 instance and a database to allow traffic flow between them.	Create a policy that automates the creation, retention, and deletion of EBS snapshots
Create billing alerts	Connect to instance Learn more	Connect an RDS database Create a new RDS database Learn more	Create EBS snapshot policy

Manage detailed monitoring	Create Load Balancer	Create AWS budget	Manage CloudWatch alarms
Enable or disable detailed monitoring for the instance. If you enable detailed monitoring, the Amazon EC2 console displays monitoring graphs with a 1-minute period.	Create a application, network gateway or classic Elastic Load Balancer	AWS Budgets allows you to create budgets, forecast spend, and take action on your costs and usage from a single location.	Create or update Amazon CloudWatch alarms for the instance.
Manage detailed monitoring	Create Load Balancer	Create AWS budget	Manage CloudWatch alarms

[View all instances](#)

Instances (1/2) [Info](#)

Last updated 1 minute ago [Connect](#) [Instance state](#) (All states)

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Available
<input checked="" type="checkbox"/> Web Server 1	i-0abe9ae45e4284a78	Running Details Logs	t2.micro	2/2 checks passed	View alarms +	us-east-1
<input type="checkbox"/> Bastion Host	i-001d787f0cd4218db	Running Details Logs	t2.micro	2/2 checks passed	View alarms +	us-east-1

i-0abe9ae45e4284a78 (Web Server 1)

Details Status and alarms Monitoring Security Networking Storage Tags

Instance summary [Info](#)

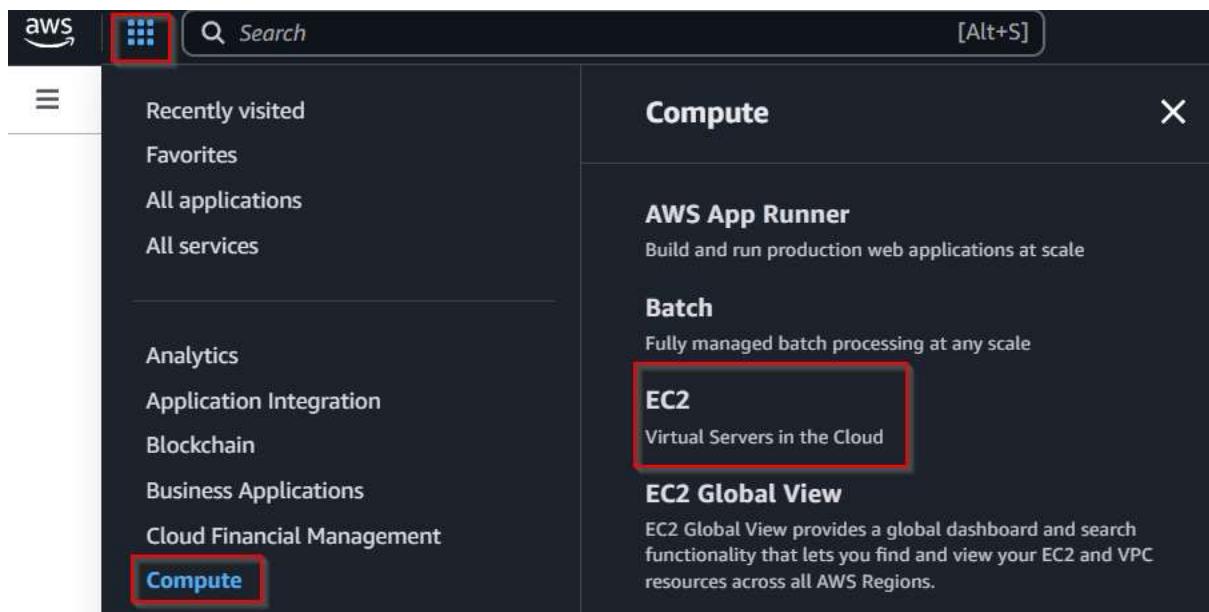
Instance ID i-0abe9ae45e4284a78

Public IPv4 address [54.197.13.42](#) | [open address](#)

Private IPv4 addresses [10.0.2.17](#)

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.

Name and tags [Info](#)

Name
 [Add additional tags](#)

Application and OS Images (Amazon Machine Image) [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.

[Recents](#) [Quick Start](#)

[Browse more AMIs](#)
Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

Amazon Linux 2023 AMI [Free tier eligible](#) [View details](#)

ami-01816d07b1128cd2d (64-bit (x86), uefi-preferred) / ami-02dcfe5d1d39baa4e (64-bit (Arm), uefi)
Virtualization: hvm ENA enabled: true Root device type: ebs

Description
Amazon Linux 2023 is a modern, general purpose Linux-based OS that comes with 5 years of long term support. It is optimized for AWS and designed to provide a secure, stable and high-performance execution environment to develop and run your cloud applications.

Amazon Linux 2023 AMI 2023.6.20241212.0 x86_64 HVM kernel-6.1

Architecture	Boot mode	AMI ID	Username
64-bit (x86)	uefi-preferred	ami-01816d07b1128cd2d	ec2-user Verified provider

Instance type [Info](#) | [Get advice](#)

Instance type

t2.micro [Free tier eligible](#) [View details](#)

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](#)

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 - required

[Create new key pair](#)

▼ 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 new](#)

IAM instance profile [Info](#)

Select

[Create new](#)

Hostname type [Info](#)

IP name

DNS Hostname [Info](#)

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.

Success
Successfully initiated launch of instance (i-012719549c4b1ff79)

Launch log

Next Steps

Q. What would you like to do next with this instance, for example "create alarm" or "create backup"?

Create billing and free tier usage alerts
To manage costs and avoid surprise bills, set up email notifications for billing and free tier usage thresholds.
[Create billing alerts](#)

Connect to your instance
Once your instance is running, log into it from your local computer.
[Connect to instance](#) [Learn more](#)

Connect an RDS database
Configure the connection between an EC2 instance and a database to allow traffic flow between them.
[Connect an RDS database](#) [Create a new RDS database](#) [Learn more](#)

Create EBS snapshot policy
Create a policy that automates the creation, retention, and deletion of EBS snapshots.
[Create EBS snapshot policy](#)

Manage detailed monitoring
Enable or disable detailed monitoring for the instance. If you enable detailed monitoring, the Amazon EC2 console displays monitoring graphs with a 1-minute period.
[Manage detailed monitoring](#)

Create Load Balancer
Create a application, network gateway or classic Elastic Load Balancer.
[Create Load Balancer](#)

Create AWS budget
AWS Budgets allows you to create budgets, forecast spend, and take action on your costs and usage from a single location.
[Create AWS budget](#)

Manage CloudWatch alarms
Create or update Amazon CloudWatch alarms for the instance.
[Manage CloudWatch alarms](#)

[View all instances](#)

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

Security Groups (1/5) Info

Find resources by attribute or tag

Name	Security group ID	Security group name	VPC ID	Description
sg-048e101d6f38ae13b	default	vpc-004c2b5f5f42d0930	vpc-004c2b5f5f42d0930	default VPC security group
sg-03295c2af9b3c751b	default	vpc-00e91d20ad92b8d41	vpc-00e91d20ad92b8d41	default VPC security group
<input checked="" type="checkbox"/> sg-0be416547c90fd7a0	Web Server security group	vpc-00e91d20ad92b8d41	vpc-00e91d20ad92b8d41	Security group for my web server
sg-0b906dbfcf70456bce	default	vpc-0120763c5d959a64c	vpc-0120763c5d959a64c	default VPC security group
sg-082f5be36164c87c8	Ec2SecurityGroup	vpc-0120763c5d959a64c	vpc-0120763c5d959a64c	VPC Security Group

sg-0be416547c90fd7a0 - Web Server security group

Details [Inbound rules](#) Outbound rules Sharing - new VPC associations - new Tags

Inbound rules

Search

Name	Security group rule ID	IP version	Type	Protocol	Port range	Source
No security group rules found						

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

Edit inbound rules [Info](#)

Inbound rules control the incoming traffic that's allowed to reach the instance.

Inbound rules Info	Type Info	Protocol Info	Port range	Source Info	Description - optional Info
-	<input type="button" value="Add rule"/>	HTTP	TCP	80	Anywhere... Info
					0.0.0.0/0 X

⚠ Rules with source of 0.0.0.0/0 or ::/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

[Cancel](#) [Preview changes](#) [Save rules](#)

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.

Change instance type [Info](#) | [Get advice](#)

You can change the instance type only if the current instance type and the instance type that you want are compatible.

Instance ID
i-012719549c4b1ff79 (Web Server)

Current instance type
t2.micro

New instance type
 [X](#)

EBS-optimized
EBS-optimized is not supported for this instance type

▼ Instance type comparison

Attribute	t2.micro	t2.small
On-Demand Linux pricing	0.0116 USD per Hour	0.0230 USD per Hour
On-Demand Windows pricing	0.0162 USD per Hour	0.0320 USD per Hour
vCPUs	1 (1 core)	1 (1 core)
Memory (MiB)	1024	2048
Storage (GB)	-	-
Supported root device types	ebs	ebs
Network performance	Low to Moderate	Low to Moderate
Architecture	i386	i386
Burstable	true	true
Free-tier eligible	true	false
Current generation	true	true

[Compare more instance type attributes](#)

Advanced details

The t2.small instance type does not support changing CPU options.

[Cancel](#) [Change](#)

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

Instance type changed successfully

Instances (1/2) [Info](#)

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Available
Bastion Host	i-02a5025f4b07f550c	Running	t2.micro	2/2 checks passed	View alarms	Yes
Web Server	i-012719549c4b1ff79	Stopped	t2.small	0/2 checks passed	View alarms	No

Last updated less than a minute ago [Connect](#) [Instance state](#) [Actions](#) [Launch instances](#)

Actions ▾

- View details
- Manage instance state
- Instance settings** [Edit](#)
- Networking
- Security
- Image and templates
- Monitor and troubleshoot

Change stop protection

Change shutdown behavior

Change auto-recovery behavior

Change instance type

Change CPU options

Change Nitro Enclaves

Change credit specification

Change resource based naming options

Modify instance placement

Modify Capacity Reservation settings

Edit user data

Allow tags in instance metadata

Manage tags

Modify instance metadata options

Change stop protection [Info](#)

Enable stop protection to prevent your instance from being accidentally stopped.

Instance ID
i-012719549c4b1ff79 (Web Server)

Stop protection [Enable](#)

[Cancel](#) [Save](#)

10. Go to storage > actions > modify volume.

i-012719549c4b1ff79 (Web Server)

Details | Status and alarms | Monitoring | Security | Networking | **Storage** | Tags

Root device details

Root device name: /dev/xvda | Root device type: EBS | EBS optimization: disabled

Block devices

Volume ID	Device name	Volume size (GiB)	Attachment status	Attachment time	Encrypted	KMS key ID
vol-0db11aed2a1e60577	/dev/xvda	8	Attached	2025/01/08 09:49 GMT-8	No	-

Volumes (1/1) Info

Name	Volume ID	Type	Size	IOPS	Throughput	Snapshots
-	vol-0db11aed2a1e60577	gp3	8 GiB	3000	125	snap-0

Actions

- Modify volume (highlighted)
- Create snapshot
- Create snapshot lifecycle policy
- Delete volume
- Attach volume
- Detach volume
- Force detach volume
- Manage auto-enabled I/O
- Manage tags
- Fault injection

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

Modify volume

Modify the type, size, and performance of an EBS volume.

Volume details

Volume ID: vol-0db11aed2a1e60577

Volume type: General Purpose SSD (gp3)

Size (GiB): 10 (highlighted)

IOPS: 3000

Throughput (MiB/s): 125

Actions

Cancel | **Modify**

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

Enabled stop protection for i-012719549c4b1ff79

Instances (1/2) Info

Name	Instance ID	Instance state	Instance type	Status check	Actions
Bastion Host	i-02a5025f4b07f550c	Running	t2.micro	2/2 checks passed	Stop instance Start instance (highlighted) Connect Launch instances All states Public IPv4 DNS: ec2-54-83-96-129.com...
Web Server	i-012719549c4b1ff79	Stopped	t2.small	-	Stop instance Start instance Reboot instance Hibernate instance Terminate (delete) instance Public IPv4 DNS: -

Actions

- Start instance (highlighted)
- Stop instance
- Reboot instance
- Hibernate instance
- Terminate (delete) 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 traffic 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.

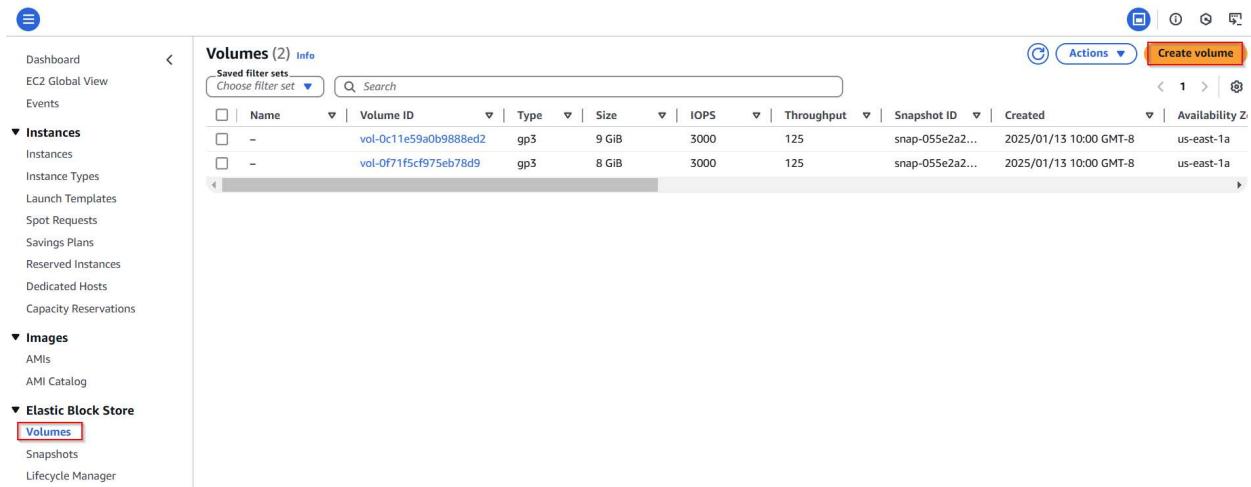
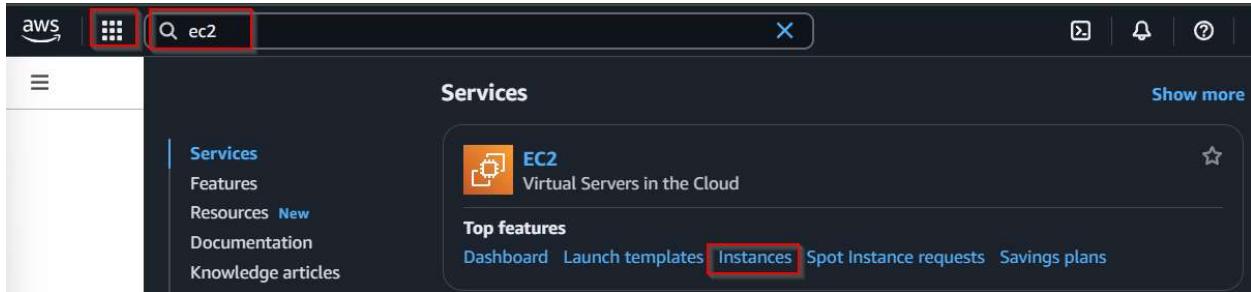
In the fifth lab, you will launch an Amazon RDS DB instance, configure it to allow connections from a web server, and test out interacting with the database from the web application.

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.

Create volume [Info](#)

Create an Amazon EBS volume to attach to any EC2 instance in the same Availability Zone.

Volume settings

Volume type [Info](#)
General Purpose SSD (gp2)

Size (GiB) [Info](#)
1
Min: 1 GiB, Max: 16384 GiB.

IOPS [Info](#)
100 / 3000
Baseline of 3 IOPS per GiB with a minimum of 100 IOPS, burstable to 3000 IOPS.

Throughput (MiB/s) [Info](#)
Not applicable

Availability Zone [Info](#)
us-east-1a

Snapshot ID - optional [Info](#)
Don't create volume from a snapshot [↻](#)

Encryption [Info](#)
Use Amazon EBS encryption as an encryption solution for your EBS resources associated with your EC2 instances.
 Encrypt this volume

Tags - optional [Info](#)

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key [Value - optional](#)
Name [X](#) Value - optional [X](#) Remove [Add tag](#)
You can add 49 more tags.

Snapshot summary [Info](#) [↻](#)

Click refresh to view backup information
The volume type that you select and the tags that you assign determine whether the volume will be backed up by any Data Lifecycle Manager policies.

[Cancel](#) [Create volume](#)

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

The screenshot shows the AWS Lambda Volumes page. A context menu is open over the row for 'My Volume'. The 'Actions' menu is visible, with 'Attach volume' highlighted. The 'Basic details' section of the 'Attach volume' dialog is shown, with the 'Instance' dropdown set to 'i-0de7aadf05011357e (Lab) (running)' and the 'Device name' dropdown set to '/dev/sdf'. The 'Attach volume' button is highlighted in orange at the bottom right of the dialog.

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

The screenshot shows the AWS EC2 Instances tab. The 'Instances' section is selected, showing two instances: 'Lab' (running, t2.micro, 2/2 checks passed) and 'Bastion Host' (running, t2.micro, 2/2 checks passed). The 'Connect' button for the 'Lab' instance is highlighted. The 'Connect to instance' dialog is open, showing the 'EC2 Instance Connect' tab selected. It displays the instance ID 'i-0de7aadf05011357e (Lab)', connection type options ('Connect using EC2 Instance Connect' and 'Connect using EC2 Instance Connect Endpoint'), and a public IP address '18.207.181.76'. The 'Username' field is set to 'ec2-user'. A note at the bottom states: 'Note: In most cases, the default username, ec2-user, is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI username.' The 'Connect' button is highlighted in orange at the bottom right of the dialog.

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"

```
[ec2-user@ip-10-1-11-141 ~]$ df -h
Filesystem      Size  Used Avail Use% Mounted on
/devtmpfs        4.0M   0    4.0M  0% /dev
tmpfs           475M   0   475M  0% /dev/shm
tmpfs          190M  456K  190M  1% /run
/dev/xvda1       8.0G  1.6G  6.4G  20% /
tmpfs           475M   0   475M  0% /tmp
/dev/xvda128     10M  1.3M  8.7M  13% /boot/efi
tmpfs           95M   0   95M  0% /run/user/1000
[ec2-user@ip-10-1-11-141 ~]$ sudo mkdir /mnt/data-store
[ec2-user@ip-10-1-11-141 ~]$ sudo mount /dev/sdf /mnt/data-store
mount: /mnt/data-store: wrong fs type, bad option, bad superblock on /dev/xvdf, missing codepage or helper program, or other error.
[ec2-user@ip-10-1-11-141 ~]$ sudo mkfs -t ext3 /dev/sdf
mke2fs 1.46.5 (30-Dec-2021)
Creating filesystem with 262144 4k blocks and 65536 inodes
Filesystem UUID: 6a59ce8c-850d-4f1e-96f0-dcd5892bbde3
Superblock backups stored on blocks:
      32768, 98304, 163840, 229376

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

[ec2-user@ip-10-1-11-141 ~]$ sudo mount /dev/sdf /mnt/data-store
[ec2-user@ip-10-1-11-141 ~]$ echo "/dev/sdf /mnt/data-store ext3 defaults,noatime 1 2" | sudo tee -a /etc/fstab
[ec2-user@ip-10-1-11-141 ~]$ cat /etc/fstab
#
UUID=73e034f4-2887-4ec9-8b40-0d35c0091a37      /          xfs  defaults,noatime 1  1
UUID=9f37-3c35      /boot/efi      vfat  defaults,noatime,uid=0,gid=0,umask=0077,shortname=winnt,x-systemd.automount 0 2
/dev/sdf  /mnt/data-store ext3 defaults,noatime 1 2
[ec2-user@ip-10-1-11-141 ~]$ df -h
Filesystem      Size  Used Avail Use% Mounted on
/devtmpfs        4.0M   0    4.0M  0% /dev
tmpfs           475M   0   475M  0% /dev/shm
tmpfs          190M  452K  190M  1% /run
/dev/xvda1       8.0G  1.6G  6.4G  20% /
tmpfs           475M   0   475M  0% /tmp
/dev/xvda128     10M  1.3M  8.7M  13% /boot/efi
tmpfs           95M   0   95M  0% /run/user/1000
/dev/xvdf        975M  60K  924M  1% /mnt/data-store
[ec2-user@ip-10-1-11-141 ~]$ sudo sh -c "echo some text has been written > /mnt/data-store/file.txt"
[ec2-user@ip-10-1-11-141 ~]$ cat /mnt/data-store/file.txt
some text has been written
[ec2-user@ip-10-1-11-141 ~]$
```

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

The screenshot shows the AWS EC2 Volumes page. A success message at the top says "Successfully attached volume vol-04043a39c18aeae5c to instance i-0de7aadf05011357e." The "Volumes (1/3) Info" table has one row selected, "My Volume". The "Actions" menu for this volume is open, with "Create snapshot" highlighted. The "Create snapshot" dialog is displayed below, containing fields for "Source volume" (set to "vol-04043a39c18aeae5c (My Volume)"), "Availability Zone" (set to "us-east-1a"), "Snapshot details" (with a "Description" field containing "My Snapshot" and an "Encryption" field set to "Not encrypted"), and "Tags" (containing a single tag "Name: My Snapshot"). The "Create snapshot" button is at the bottom right of the dialog.

7. Delete the file previously created on the volume

```
[ec2-user@ip-10-1-11-141 ~]$ sudo rm /mnt/data-store/file.txt
[ec2-user@ip-10-1-11-141 ~]$ ls /mnt/data-store/
lost+found
[ec2-user@ip-10-1-11-141 ~]$ 
```

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

The screenshot shows the AWS EBS Create Volume wizard. On the left, a sidebar navigation includes: Dashboard, EC2 Global View, Events, Instances (selected), Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Capacity Reservations, Images (AMIs, AMI Catalog), and Elastic Block Store (Volumes, Snapshots - selected). The main area displays the 'Snapshots (1/1) Info' table with one entry: 'My Snapshot' (snap-05882d98af609d46c, 1 GiB, Standard). A context menu is open over this row, with the 'Create volume from snapshot' option highlighted. The 'Create volume' wizard steps are visible:

- Volume settings**: Includes fields for Snapshot ID (selected), Volume type (General Purpose SSD (gp3)), Size (1 GiB), IOPS (3000), Throughput (125 MiB/s), Availability Zone (us-east-1a), Fast snapshot restore (disabled), and Encryption (checkbox for Encrypt this volume).
- Tags - optional**: A table for adding tags with columns Key (Name) and Value - optional (Restored Volume). An 'Add tag' button and a note about adding more tags are present.
- Snapshot summary**: Summary information including a refresh link, a note about backup policies, and a note about the volume type and tags determining backup status.

At the bottom right of the wizard are 'Cancel' and 'Create volume' buttons.

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

The screenshot shows the AWS Management Console interface. On the left, there's a navigation sidebar with sections like Dashboard, EC2 Global View, Events, Instances, Images, and Elastic Block Store. Under Elastic Block Store, 'Volumes' is selected, indicated by a red box. The main area displays a table titled 'Volumes (1/4) Info' with columns: Name, Volume ID, Type, Size, IOPS, Throughput, and Snapshot. There are four entries: 'vol-0c11e59a0b9888ed2' (gp3, 9 GiB, 3000 IOPS, 125 throughput), 'My Volume' (gp2, 1 GiB, 100 IOPS, - throughput), 'Restored Volu...' (gp3, 1 GiB, 3000 IOPS, 125 throughput), and 'vol-0f71f5cf975eb78d9' (gp3, 8 GiB, 3000 IOPS, 125 throughput). A context menu is open over the 'Restored Volu...' row, with 'Actions' highlighted. The 'Attach volume' option is also highlighted with a red box. Below this, the 'Attach volume' dialog is shown. It has tabs for 'Basic details', 'Instance', and 'Device name'. In 'Basic details', the 'Volume ID' is 'vol-0544647f01cbaab69 (Restored Volume)', 'Availability Zone' is 'us-east-1a', and 'Instance' dropdown shows 'i-0de7aaddf05011357e (Lab (running))' with a red box around it. In 'Device name', the 'Device name' dropdown shows '/dev/sdg' with a red box around it. A note at the bottom says 'Newer Linux kernels may rename your devices to /dev/xvdf through /dev/xvdp internally, even when the device name entered here (and shown in the details) is /dev/sdf through /dev/sdp.' At the bottom right of the dialog are 'Cancel' and 'Attach volume' buttons, with 'Attach volume' highlighted with a red box.

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.

The screenshot shows the AWS VPC dashboard. At the top, there is a search bar with 'vpc' typed into it. Below the search bar, there is a 'Services' section with a 'VPC' icon and the text 'Isolated Cloud Resources'. This entire section is highlighted with a red box. On the left side, there is a sidebar with various options under 'Virtual private cloud' and 'Security'. Under 'Security', the 'Security groups' option is selected and highlighted with a red box. The main area displays a table titled 'Security Groups (5) Info' with the following data:

Name	Security group ID	Security group name	VPC ID	Description
-	sg-04c544bc5ed879273	default	vpc-0139d118a9b8ae1af	default VPC security group
-	sg-04cf3fdfee26b07f4	WorkEc2SecurityGroup	vpc-0e88749a9ddd39257	VPC Security Group
-	sg-0283d708d9d1666f1	default	vpc-0e88749a9ddd39257	default VPC security group
-	sg-06b3fb113ce51f2a7	default	vpc-0c2bceb3d5961a4b9	default VPC security group
Web Security Group	sg-01f2cb6cec4cd0852	Web Security Group	vpc-0c2bceb3d5961a4b9	Enable HTTP access

At the top right of the table, there is a 'Create security group' button. The entire screenshot is framed by a large red box.

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)

Create security group Info

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

Basic details

Security group name Info
DB Security Group
Name cannot be edited after creation.

Description Info
Permit access from Web Security Group

VPC Info
vpc-0c2bceb3d5961a4b9 (Lab VPC)

Inbound rules Info

Type	Protocol	Port range	Source	Description - optional
MySQL/Aurora	TCP	3306	Custom	Q, sg-01f2cb6cec4cd0852 <input type="button" value="Delete"/> sg-01f2cb6cec4cd0852 <input type="button" value="Delete"/>

Add rule

Outbound rules Info

Type	Protocol	Port range	Destination	Description - optional
All traffic	All	All	Custom	Q, 0.0.0.0/0 <input type="button" value="Delete"/> 0.0.0.0/0 <input type="button" value="Delete"/>

Add rule

⚠ Rules with destination of 0.0.0.0/0 or ::/0 allow your instances to send traffic to any IPv4 or IPv6 address. We recommend setting security group rules to be more restrictive and to only allow traffic to specific known IP addresses.

Tags - optional

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

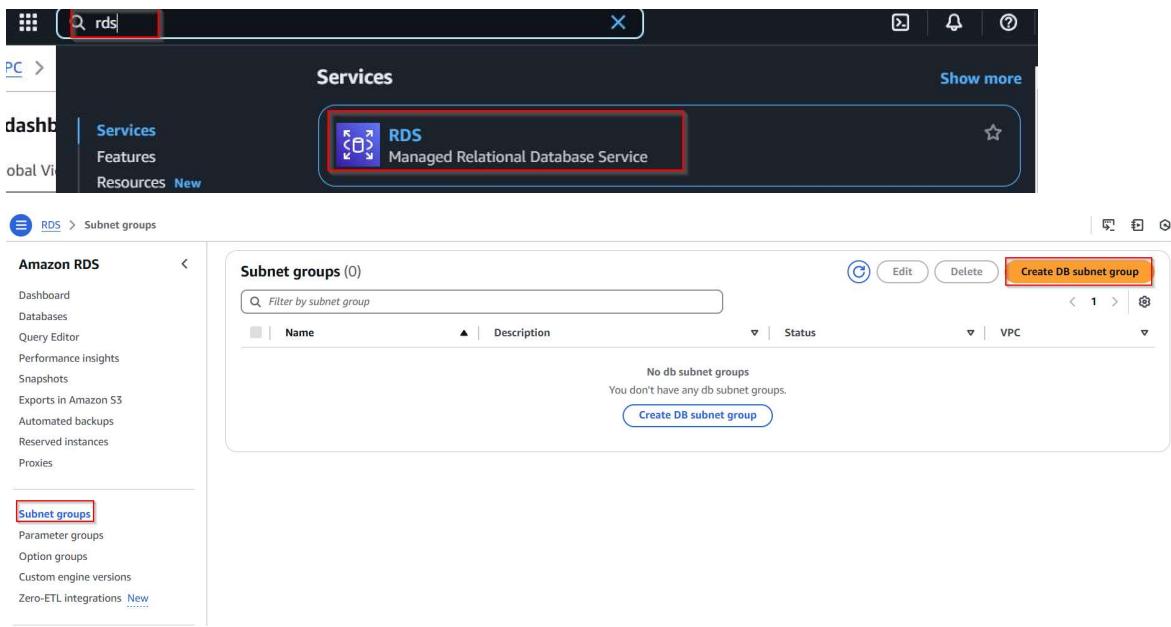
No tags associated with the resource.

Add new tag

You can add up to 50 more tags

Create security group

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



The screenshot shows the AWS RDS Subnet groups page. At the top, there is a search bar with 'rds' typed into it. Below the search bar, the 'Services' section is visible, with the 'RDS' icon and text 'Managed Relational Database Service' highlighted with a red box. The main content area is titled 'Subnet groups (0)' and contains a table header with columns: Name, Description, Status, and VPC. A message below the table states 'No db subnet groups' and 'You don't have any db subnet groups.' A prominent orange button labeled 'Create DB subnet group' is located at the bottom right of the table area. On the left sidebar, under 'Amazon RDS', the 'Subnet groups' link is also highlighted with a red box. The overall interface is dark-themed.

4.

4. Configure:

- Name: DB-Subnet-Group
- Description: 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

Create DB subnet group

To create a new subnet group, give it a name and a description, and choose an existing VPC. You will then be able to add subnets related to that VPC.

Subnet group details

Name
You won't be able to modify the name after your subnet group has been created.
DB-Subnet-Group

Must contain from 1 to 255 characters. Alphanumeric characters, spaces, hyphens, underscores, and periods are allowed.

Description
DB Subnet Group

VPC
Choose a VPC identifier that corresponds to the subnets you want to use for your DB subnet group. You won't be able to choose a different VPC identifier after your subnet group has been created.
Lab VPC (vpc-0c2be0b3d5d961a4b9)
4 Subnets, 2 Availability Zones

Add subnets

Availability Zones
Choose the Availability Zones that include the subnets you want to add.
Choose an availability zone
us-east-1a X us-east-1b X

Subnets
Choose the subnets that you want to add. The list includes the subnets in the selected Availability Zones.
Select subnets
Private Subnet 2 Subnet ID: subnet-0f089ae6fb3d14163 CIDR: 10.0.3.0/24 **Private Subnet 1** Subnet ID: subnet-0f754f85992eebb75 CIDR: 10.0.1.0/24

(i) For Multi-AZ DB clusters, you must select 3 subnets in 3 different Availability Zones.

Subnets selected (2)				
Availability zone	Subnet name	Subnet ID	CIDR block	
us-east-1b	Private Subnet 2	subnet-0f089ae6fb3d14163	10.0.3.0/24	
us-east-1a	Private Subnet 1	subnet-0f754f85992eebb75	10.0.1.0/24	

Create

5. Navigate to Databases and click Create Database.

RDS > Databases

Amazon RDS

- Dashboard
- Databases**
- Query Editor
- Performance insights
- Snapshots
- Exports in Amazon S3
- Automated backups
- Reserved instances
- Proxies

Successfully created DB-Subnet-Group. View subnet group

Databases (0)

Create database

No instances found

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



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 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.

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.

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

► Additional storage configuration

Connectivity [Info](#) C

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.

i 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 X

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 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.

Databases (1)

Group resources Modify Actions ▾ Restore from S3 Create database

Filter by databases

DB identifier	Status	Role	Engine	Region ...	Size	Recommendations
lab-db	Modifying	Instance	MySQL Co...	us-east-1a	db.t3.micro	

aws Load Test RDS

Endpoint: lab-db.ccwjxlpukfs.us-east-1.rds.amazonaws.com

Database: lab

Username: main

Password: *****

Submit

Address Book

Last name	First name	Phone	Email	Admin
Add Contact				
Doe	Jane	010-110-1101	janed@someotheraddress.org	Edit Remove
Johnson	Roberto	123-456-7890	robertoj@someaddress.com	Edit Remove

Lab 6

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

The screenshot shows the AWS EC2 Instances page. There are two instances listed: 'Bastion Host' and 'Web Server 1'. 'Web Server 1' is selected, indicated by a checked checkbox. The status for 'Web Server 1' is 'Running' with '2/2 checks passed'. The 'Actions' menu is open, and the 'Create image' option is highlighted with a red box. Other options in the Actions menu include 'View details', 'Manage instance state', 'Instance settings', 'Networking', 'Security', 'Image and templates', and 'Monitor and troubleshoot'.

2. Configure:

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

Create image info

An image (also referred to as an AMI) defines the programs and settings that are applied when you launch an EC2 instance. You can create an image from the configuration of an existing instance.

Instance ID
i-051bda8ae7eb89963 (Web Server 1)

Image name
WebServerAMI
Maximum 127 characters. Can't be modified after creation.

Image description - optional
Lab AMI for Web Server
Maximum 255 characters

Reboot instance
When selected, Amazon EC2 reboots the instance so that data is at rest when snapshots of the attached volumes are taken. This ensures data consistency.

Instance volumes

Storage type	Device	Snapshot	Size	Volume type	IOPS	Throughput	Delete on termination	Encrypted
EBS	/dev/...	Create new snapshot fro...	8	EBS General Purpose SSD ...	3000		<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable

Add volume

During the image creation process, Amazon EC2 creates a snapshot of each of the above volumes.

Tags - optional
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Tag image and snapshots together
Tag the image and the snapshots with the same tag.

Tag image and snapshots separately
Tag the image and the snapshots with different tags.

No tags associated with the resource.

Add new tag
You can add up to 50 more tags.

Create image

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

The screenshot shows the AWS EC2 Target Groups page. On the left, there's a navigation sidebar with sections like Dashboard, EC2 Global View, Events, Instances, Images, Elastic Block Store, Network & Security, Load Balancing, Auto Scaling, and a section for Target Groups which is highlighted with a red box. The main content area is titled "Target groups Info" and contains a table header with columns: Name, ARN, Port, Protocol, Target type, Load balancer, and VPC ID. Below the header, it says "No target groups" and "You don't have any target groups in us-east-1". A prominent orange "Create target group" button is located at the bottom of this section. The URL in the browser bar is [https://console.aws.amazon.com/ec2/v2/home?region=us-east-1#TargetGroups:](#)

4. Configure:

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

Basic configuration

Settings in this section can't be changed after the target group is created.

Choose a target type

Instances

- Supports load balancing to instances within a specific VPC.
- Facilitates the use of [Amazon EC2 Auto Scaling](#) to manage and scale your EC2 capacity.

IP addresses

- Supports load balancing to VPC and on-premises resources.
- Facilitates routing to multiple IP addresses and network interfaces on the same instance.
- Offers flexibility with microservice based architectures, simplifying inter-application communication.
- Supports IPv6 targets, enabling end-to-end IPv6 communication, and IPv4-to-IPv6 NAT.

Lambda function

- Facilitates routing to a single Lambda function.
- Accessible to Application Load Balancers only.

Application Load Balancer

- Offers the flexibility for a Network Load Balancer to accept and route TCP requests within a specific VPC.
- Facilitates using static IP addresses and PrivateLink with an Application Load Balancer.

Target group name

LabGroup

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

Protocol : Port

Choose a protocol for your target group that corresponds to the Load Balancer type that will route traffic to it. Some protocols now include anomaly detection for the targets and you can set mitigation options once your target group is created. This choice cannot be changed after creation

HTTP

▼

80

1-65535

IP address type

Only targets with the indicated IP address type can be registered to this target group.

IPv4

Each instance has a default network interface (eth0) that is assigned the primary private IPv4 address. The instance's primary private IPv4 address is the one that will be applied to the target.

IPv6

Each instance you register must have an assigned primary IPv6 address. This is configured on the instance's default network interface (eth0). [Learn more](#)

VPC

Select the VPC with the instances that you want to include in the target group. Only VPCs that support the IP address type selected above are available in this list.

Lab VPC

vpn-04c81c7a4432caf18

IPv4 VPC CIDR: 10.0.0.0/16

Protocol version

HTTP1

Send requests to targets using HTTP/1.1. Supported when the request protocol is HTTP/1.1 or HTTP/2.

HTTP2

Send requests to targets using HTTP/2. Supported when the request protocol is HTTP/2 or gRPC, but gRPC-specific features are not available.

gRPC

Send requests to targets using gRPC. Supported when the request protocol is gRPC.

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

The screenshot shows the AWS EC2 console with the 'Load balancers' section selected. The left sidebar includes links for Dashboard, EC2 Global View, Events, Instances, Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Capacity Reservations, Images, AMIs, AMI Catalog, Elastic Block Store, Volumes, Snapshots, Lifecycle Manager, Network & Security, Security Groups, Elastic IPs, Placement Groups, Key Pairs, Network Interfaces, Load Balancing (with 'Load Balancers' highlighted), Target Groups, Trust Stores (New), and Auto Scaling. The main content area is titled 'Load balancers' and displays a message: 'Elastic Load Balancing scales your load balancer capacity automatically in response to changes in incoming traffic.' Below this is a search bar labeled 'Filter load balancers' and a table header with columns: Name, DNS name, State, VPC ID, Availability Zones, Type, and Date created. A message 'No load balancers' is displayed, followed by 'You don't have any load balancers in us-east-1'. A prominent orange 'Create load balancer' button is located at the bottom of the table area.

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

Compare and select load balancer type

A complete feature-by-feature comparison along with detailed highlights is also available. [Learn more](#)

Load balancer types

Application Load Balancer	Network Load Balancer	Gateway Load Balancer
Choose an Application Load Balancer when you need a flexible feature set for your applications with HTTP and HTTPS traffic. Operating at the request level, Application Load Balancers provide advanced routing and visibility features targeted at application architectures, including microservices and containers. Create	Choose a Network Load Balancer when you need ultra-high performance, TLS offloading at scale, centralized certificate deployment, support for UDP, and static IP addresses for your applications. Operating at the connection level, Network Load Balancers are capable of handling millions of requests per second securely while maintaining ultra-low latencies. Create	Choose a Gateway Load Balancer when you need to deploy and manage a fleet of third-party virtual appliances that support GENEVE. These appliances enable you to improve security, compliance, and policy controls. Create

▶ [Classic Load Balancer - previous generation](#)

[Close](#)

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 rules. When a 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 targets defined in the rule.

► 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 additional cost.

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 a 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 balancer are not available for selection.

Availability Zones

us-east-1a (use1-az6)

Subnet

subnet-081b2e826390317e0
IPv4 subnet CIDR: 10.0.0.0/24

Public Subnet 1



IPv4 address

Assigned by AWS

us-east-1b (use1-az1)

Subnet

subnet-0104cad27fdc0763c
IPv4 subnet CIDR: 10.0.2.0/24

Public Subnet 2



IPv4 address

Assigned by AWS

Security groups [Info](#)

A security group is a set of firewall rules that control the traffic to your load balancer. Select an existing security group, or you can [create a new security group](#).

Security groups

Select up to 5 security groups

Web Security Group [Info](#) [X](#) [C](#)

sg-0b9c50cf8baf57daf VPC: vpc-04c81c7a4432caf18

Listeners and routing [Info](#)

A listener is a process that checks for connection requests using the port and protocol you configure. The rules that you define for a listener determine how the load balancer routes requests to its registered targets.

▼ Listener HTTP:80

Protocol: HTTP Port: 80 1-65535

Default action | [Info](#) Forward to: LabGroup Target type: Instance, IPv4 [HTTP](#) [C](#)

Create target group [C](#)

Listener tags - optional

Consider adding tags to your listener. Tags enable you to categorize your AWS resources so you can more easily manage them.

[Add listener tag](#)

You can add up to 50 more tags.

[Add listener](#)

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

[EC2](#) > [Load balancers](#) > LabELB

Dashboard EC2 Global View Events

▼ Instances Instances Instance Types [Launch Templates](#) Spot Requests Savings Plans Reserved Instances Dedicated Hosts Capacity Reservations

▼ Images AMIs AMI Catalog

▼ Elastic Block Store

Compute

EC2 launch templates

Streamline, simplify and standardize instance launches

Use launch templates to automate instance launches, simplify permission policies, and enforce best practices across your organization. Save launch parameters in a template that can be used for on-demand launches and with managed services, including EC2 Auto Scaling and EC2 Fleet. Easily update your launch parameters by creating a new launch template version.

New launch template [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

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

Free tier eligible

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 

When you specify a subnet, a network interface is automatically added to your template.

 Create new subnet 

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

 Compare security group rules

Security groups Info

Select security groups 

Web Security Group sg-0b9c50cf8ba5f57daf 

VPC: vpc-04c81c7a4432caf18

Advanced network configuration

▼ Advanced details [Info](#)

IAM instance profile | [Info](#)

Don't include in launch template ▾ C

Hostname type | [Info](#)

Don't include in launch template ▾

DNS Hostname | [Info](#)

Enable resource-based IPv4 (A record) DNS requests

Enable resource-based IPv6 (AAAA record) DNS requests

Instance auto-recovery | [Info](#)

Don't include in launch template ▾

Shutdown behavior | [Info](#)

Don't include in launch template ▾

Not applicable for EC2 Auto Scaling

Stop - Hibernate behavior | [Info](#)

Don't include in launch template ▾

Not applicable for Amazon EC2 Auto Scaling.

Termination protection | [Info](#)

Don't include in launch template ▾

Stop protection | [Info](#)

Don't include in launch template ▾

Detailed CloudWatch monitoring | [Info](#)

Enable ▾

Additional charges apply

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

 **Success**
Successfully created [LabConfig\(lt-08914245c97a67de1\)](#).

10. Click Actions > Create Auto Scaling group

The screenshot shows the AWS Lambda Launch Configuration page for 'LabConfig'. In the top right corner, there is a 'Actions' button with a dropdown menu. The 'Create Auto Scaling group' option is highlighted with a red box. The main page displays 'Launch template details' for 'LabConfig' with version 1 selected. Below this, there are tabs for 'Details', 'Versions', and 'Template tags'. The 'Launch template version details' section shows the configuration for version 1, including instance type t2.micro, AMI ami-0332f9d12c89e5cea, and security group sg-0b9c50cf8baf57daf.

11. Configure name: Lab Auto Scaling Group.

The screenshot shows the 'Choose launch template or configuration' step of the 'Create Auto Scaling group' wizard. The 'Name' section is active, showing the 'Auto Scaling group name' field with the value 'Lab Auto Scaling Group' highlighted with a red box. Below it is a note: 'Must be unique to this account in the current Region and no more than 255 characters.' The 'Launch template' section shows 'LabConfig' selected from a dropdown. The 'Additional details' section includes fields for 'Storage (volumes)' and 'Date created' (Mon Jan 13 2025 11:04:28 GMT-0800 (Pacific Standard Time)). At the bottom right, there are 'Cancel' and 'Next Step' buttons, with 'Next Step' highlighted with a red box.

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

Choose instance launch options Info

Choose the VPC network environment that your instances are launched into, and customize the instance types and purchase options.

Instance type requirements Info

You can keep the same instance attributes or instance type from your launch template, or you can choose to override the launch template by specifying different instance attributes or manually adding instance types.

Launch template

LabConfig  lt-08914245c97a67de1

Version

Default

Description

-

[Override launch template](#)

Instance type

t2.micro

Network Info

For most applications, you can use multiple Availability Zones and let EC2 Auto Scaling balance your instances across the zones. The default VPC and default subnets are suitable for getting started quickly.

VPC

Choose the VPC that defines the virtual network for your Auto Scaling group.

vpc-04c81c7a4432caf18 (Lab VPC)

10.0.0.0/16



[Create a VPC](#) 

Availability Zones and subnets

Define which Availability Zones and subnets your Auto Scaling group can use in the chosen VPC.

Select Availability Zones and subnets

10.0.1.0/24



us-east-1a | subnet-07a0cb562ac6b2111 (Private Subnet 1) 

10.0.1.0/24

us-east-1b | subnet-030cdae3b925cd8a9 (Private Subnet 2) 

10.0.3.0/24

[Create a subnet](#) 

Availability Zone distribution - new

Auto Scaling automatically balances instances across Availability Zones. If launch failures occur in a zone, select a strategy.

Balanced best effort

If launches fail in one Availability Zone, Auto Scaling will attempt to launch in another healthy Availability Zone.

Balanced only

If launches fail in one Availability Zone, Auto Scaling will continue to attempt to launch in the unhealthy Availability Zone to preserve balanced distribution.

[Cancel](#)

[Skip to review](#)

[Previous](#)

[Next](#)

13. Configure as shown.

Integrate with other services - optional Info

Use a load balancer to distribute network traffic across multiple servers. Enable service-to-service communications with VPC Lattice. Shift resources away from impaired Availability Zones with zonal shift. You can also customize health check replacements and monitoring.

Load balancing Info

Use the options below to attach your Auto Scaling group to an existing load balancer, or to a new load balancer that you define.

- No load balancer
Traffic to your Auto Scaling group will not be fronted by a load balancer.
- Attach to an existing load balancer
Choose from your existing load balancers.
- Attach to a new load balancer
Quickly create a basic load balancer to attach to your Auto Scaling group.

Attach to an existing load balancer

Select the load balancers that you want to attach to your Auto Scaling group.

- Choose from your load balancer target groups
This option allows you to attach Application, Network, or Gateway Load Balancers.
- Choose from Classic Load Balancers

Existing load balancer target groups

Only instance target groups that belong to the same VPC as your Auto Scaling group are available for selection.

Select target groups ▼ 

- LabGroup | HTTP X
- Application Load Balancer: LabFLB

VPC Lattice integration options Info

To improve networking capabilities and scalability, integrate your Auto Scaling group with VPC Lattice. VPC Lattice facilitates communications between AWS services and helps you connect and manage your applications across compute services in AWS.

Select VPC Lattice service to attach

- No VPC Lattice service
VPC Lattice will not manage your Auto Scaling group's network access and connectivity with other services.
- Attach to VPC Lattice service
Incoming requests associated with specified VPC Lattice target groups will be routed to your Auto Scaling group.

Create new VPC Lattice service 

Application Recovery Controller (ARC) zonal shift - new Info

During an Availability Zone impairment, target instance launches towards other healthy Availability Zones.

Enable zonal shift

New instance launches will be retargeted towards healthy Availability Zones until the zonal shift is canceled.

Health checks

Health checks increase availability by replacing unhealthy instances. When you use multiple health checks, all are evaluated, and if at least one fails, instance replacement occurs.

EC2 health checks

Always enabled

Additional health check types - optional Info

- Turn on Elastic Load Balancing health checks Recommended
Elastic Load Balancing monitors whether instances are available to handle requests. When it reports an unhealthy instance, EC2 Auto Scaling can replace it on its next periodic check.
- Turn on VPC Lattice health checks
VPC Lattice can monitor whether instances are available to handle requests. If it considers a target as failed a health check, EC2 Auto Scaling replaces it after its next periodic check.
- Turn on Amazon EBS health checks
EBS monitors whether an instance's root volume or attached volume stalls. When it reports an unhealthy volume, EC2 Auto Scaling can replace the instance on its next periodic health check.

Health check grace period Info

This time period delays the first health check until your instances finish initializing. It doesn't prevent an instance from terminating when placed into a non-running state.

300 seconds

Cancel

Skip to review

Previous

Next

14. Configure as shown.

Configure group size and scaling - optional Info

Define your group's desired capacity and scaling limits. You can optionally add automatic scaling to adjust the size of your group.

Group size Info

Set the initial size of the Auto Scaling group. After creating the group, you can change its size to meet demand, either manually or by using automatic scaling.

Desired capacity type

Choose the unit of measurement for the desired capacity value. vCPUs and Memory(GiB) are only supported for mixed instances groups configured with a set of instance attributes.

Units (number of instances)



Desired capacity

Specify your group's size.

2

Scaling Info

You can resize your Auto Scaling group manually or automatically to meet changes in demand.

Scaling limits

Set limits on how much your desired capacity can be increased or decreased.

Min desired capacity

2

Equal or less than desired capacity

Max desired capacity

6

Equal or greater than desired capacity

Automatic scaling - optional

Choose whether to use a target tracking policy | Info

You can set up other metric-based scaling policies and scheduled scaling after creating your Auto Scaling group.

No scaling policies

Your Auto Scaling group will remain at its initial size and will not dynamically resize to meet demand.

Target tracking scaling policy

Choose a CloudWatch metric and target value and let the scaling policy adjust the desired capacity in proportion to the metric's value.

Scaling policy name

LabScalingPolicy

Metric type | Info

Monitored metric that determines if resource utilization is too low or high. If using EC2 metrics, consider enabling detailed monitoring for better scaling performance.

Average CPU utilization



Target value

60

Instance warmup | Info

300 seconds

Disable scale in to create only a scale-out policy

15. Configure as shown.

Additional settings

Instance scale-in protection
If protect from scale in is enabled, newly launched instances will be protected from scale in by default.
 Enable instance scale-in protection

Monitoring | [Info](#)
 Enable group metrics collection within CloudWatch

Default instance warmup | [Info](#)
The amount of time that CloudWatch metrics for new instances do not contribute to the group's aggregated instance metrics, as their usage data is not reliable yet.
 Enable default instance warmup

[Cancel](#) [Skip to review](#) [Previous](#) [Next](#)

Add tags - optional [Info](#)
Add tags to help you search, filter, and track your Auto Scaling group across AWS. You can also choose to automatically add these tags to instances when they are launched.

(1) You can optionally choose to add tags to instances (and their attached EBS volumes) by specifying tags in your launch template. We recommend caution, however, because the tag values for instances from your launch template will be overridden if there are any duplicate keys specified for the Auto Scaling group. [X](#)

Tags (1)

Key	Value - optional
Name	Lab Instance

Tag new instances [Remove](#)

[Add tag](#)
49 remaining

[Cancel](#) [Previous](#) [Next](#)

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

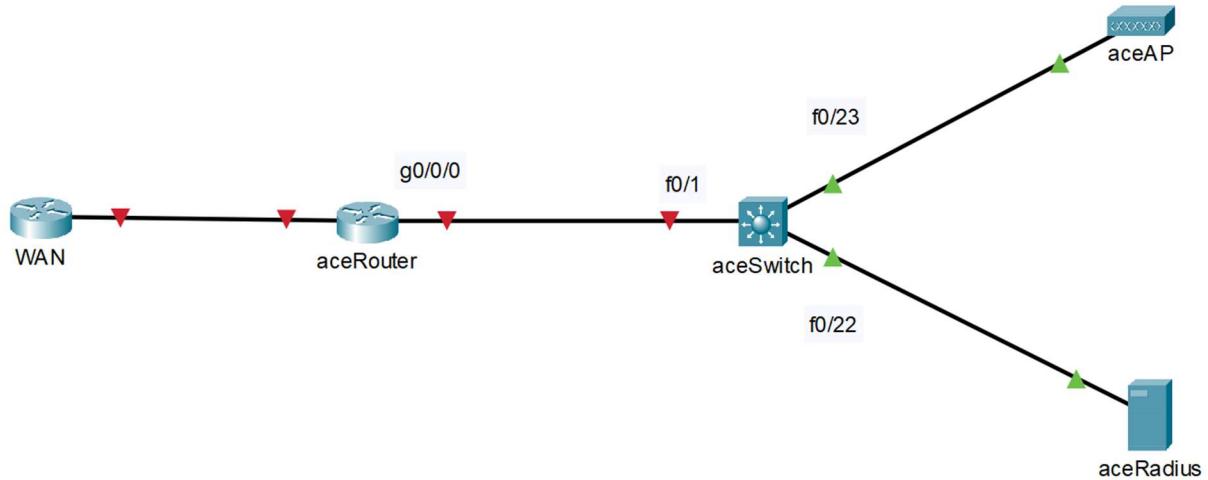
In this lab, we set up an Access Point to have three SSIDs. One has no authentication, letting anyone connect to it. One uses WPA2 PSK, requiring the user to have a password to access the network. One uses WPA2 Enterprise through RADIUS, requiring the user to have both a username and password.

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:

Network Configuration

Host Name:	ACE
Server Protocol:	<input type="radio"/> DHCP <input checked="" type="radio"/> Static IP
IP Address:	192.168.1.245
IP Subnet Mask:	255.255.255.0
Default Gateway:	192.168.1.1
IPv6 Protocol:	<input checked="" type="checkbox"/> DHCP <input checked="" type="checkbox"/> Autoconfig <input type="checkbox"/> Static IP
IPv6 Address:	(X:X:X::X:<0-128>)
Create a user	
Username:	
Password:	
Change global authentication password	
default enable secret:	*****
confirm enable secret:	
SNMP Community:	defaultCommunity
<input checked="" type="radio"/> Read-Only <input type="radio"/> Read-Write	
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

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
```

```

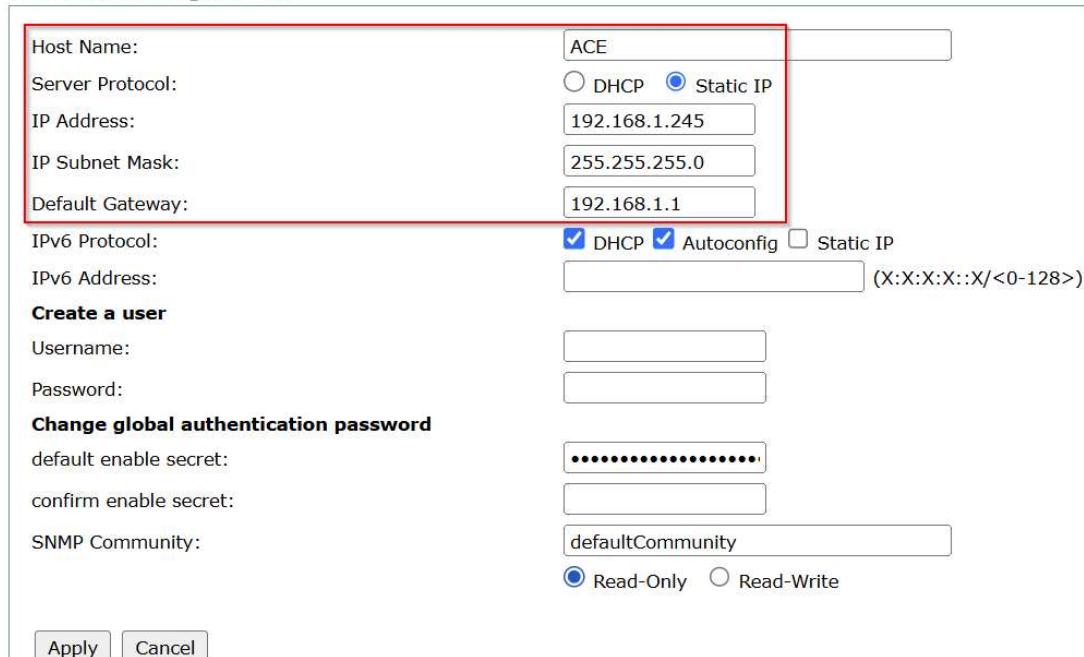
switchport mode trunk
spanning-tree portfast trunk
interface FastEthernet0/2
  switchport mode access
interface FastEthernet0/22
  switchport trunk encapsulation dot1q
  switchport mode trunk
  spanning-tree portfast trunk
interface FastEthernet0/23
  switchport trunk encapsulation dot1q
  switchport 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.

Network Configuration



The screenshot shows the 'Network Configuration' section of a network setup interface. A red box highlights the following fields:

- Host Name: ACE
- Server Protocol: DHCP Static IP
- IP Address: 192.168.1.245
- IP Subnet Mask: 255.255.255.0
- Default Gateway: 192.168.1.1

Below these, there are other fields and options:

- IPv6 Protocol: DHCP Autoconfig Static IP
- IPv6 Address: (X:X:X:X::X/<0-128>)
- Create a user
- Username: [empty field]
- Password: [empty field]
- Change global authentication password**
- default enable secret: [redacted]
- confirm enable secret: [redacted]
- SNMP Community: defaultCommunity
- Read-Only Read-Write

At the bottom are 'Apply' and 'Cancel' buttons.

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”.

Multiple BSSID Beacon Settings

Multiple BSSID Beacon

Set SSID as Guest Mode

Set DataBeacon Rate (DTIM): DISABLED (1-100)

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

Guest Mode/Infrastructure SSID Settings

Radio0-802.11N^{2.4GHz}:

Set Beacon Mode:

Single BSSID Set Single Guest Mode SSID: aceGuest ▾

Multiple BSSID

Set Infrastructure SSID:

<NONE> ▾ Force Infrastructure Devices to associate only to this SSID

Radio1-802.11N^{5GHz}:

Set Beacon Mode:

Single BSSID Set Single Guest Mode SSID: aceSecure ▾

Multiple BSSID

Set Infrastructure SSID:

<NONE> ▾ Force Infrastructure Devices to associate only to this SSID

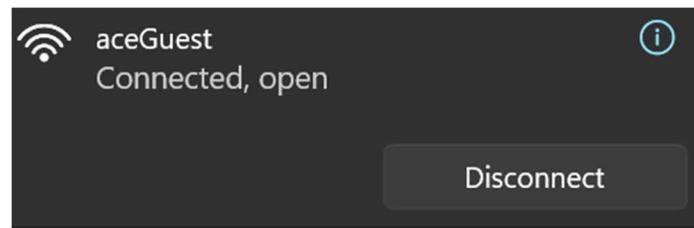
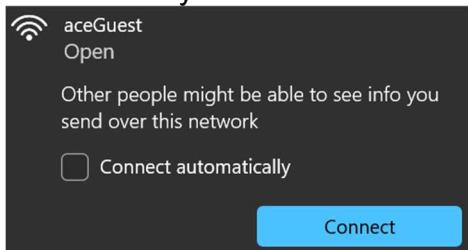
- In the router, enter the following commands:

```
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
```

- 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

- 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.

Radio 5GHz

SSID :	PSK
	<input checked="" type="checkbox"/> Broadcast SSID in Beacon
VLAN :	<input type="radio"/> No VLAN <input checked="" type="radio"/> Enable VLAN ID: 20 (1-4094) <input type="checkbox"/> Native VLAN
Universal Admin Mode:	Disable
Security :	WPA2-PSK
Pre-Shared Key :	*****
Role in Radio Network :	Access Point
Optimize Radio Network :	Default
Aironet Extensions:	Enable
Channel:	Dynamic Frequency Selection
Power:	Maximum
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

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”.

Multiple BSSID Beacon Settings

Multiple BSSID Beacon

Set SSID as Guest Mode

Set DataBeacon Rate (DTIM): DISABLED (1-100)

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

Guest Mode/Infrastructure SSID Settings

Radio0-802.11N^{2.4GHz}:

Set Beacon Mode:

Single BSSID Set Single Guest Mode SSID: aceGuest

Multiple BSSID

Set Infrastructure SSID:

<NONE> Force Infrastructure Devices to associate only to this SSID

Radio1-802.11N^{5GHz}:

Set Beacon Mode:

Single BSSID Set Single Guest Mode SSID: aceSecure

Multiple BSSID

Set Infrastructure SSID:

<NONE> Force Infrastructure Devices to associate only to this SSID

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
```

```

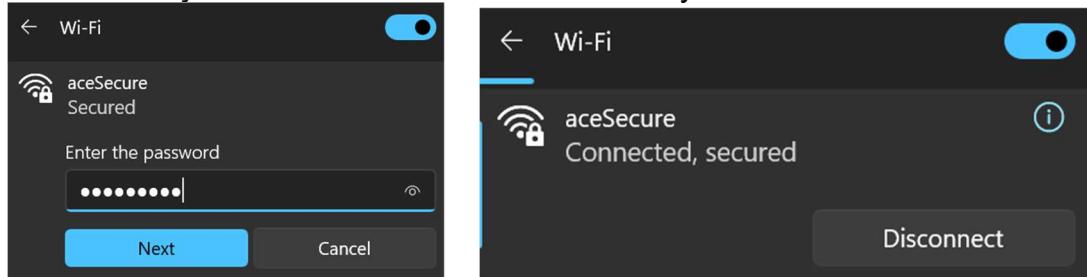
encapsulation dot1Q 20
ip address 192.168.20.1 255.255.255.0
ip nat inside
access-list 1 permit 192.168.20.0 0.0.0.255

```

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.

Radio 5GHz

SSID :	Enterprise
	<input checked="" type="checkbox"/> Broadcast SSID in Beacon
VLAN :	<input type="radio"/> No VLAN <input checked="" type="radio"/> Enable VLAN ID: 30 (1-4094) <input type="checkbox"/> Native VLAN
Universal Admin Mode:	Disable
Security :	WPA ENTERPRISE
RADIUS Server:	192.168.1.20
RADIUS Server Secret:	*****
Role in Radio Network :	Access Point
Optimize Radio Network :	Default
Aironet Extensions:	Enable
Channel:	Dynamic Frequency Selection
Power:	Maximum
<input type="button"/> Apply <input type="button"/> Cancel	

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”.

Multiple BSSID Beacon Settings

Multiple BSSID Beacon

Set SSID as Guest Mode

Set DataBeacon Rate (DTIM): DISABLED (1-100)

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

Guest Mode/Infrastructure SSID Settings

Radio0-802.11N^{2.4GHz}:

Set Beacon Mode:

Single BSSID Set Single Guest Mode SSID: aceGuest ▾

Multiple BSSID

Set Infrastructure SSID:

< NONE > Force Infrastructure Devices to associate only to this SSID

Radio1-802.11N^{5GHz}:

Set Beacon Mode:

Single BSSID Set Single Guest Mode SSID: aceSecure ▾

Multiple BSSID

Set Infrastructure SSID:

< NONE > Force Infrastructure Devices to associate only to this SSID

- 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
```

- In the switch, enter the following commands:

```
vlan 30
  name RADIUS
```

- 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.

Corporate Servers

Current Server List

RADIUS

IP Version: IPv4 IPv6

Server Name: 192.168.1.20

Server: 192.168.1.20 (Hostname or IP Address)

Shared Secret:

Delete

Authentication Port (optional): 1812 (0-65535)

Accounting Port (optional): 1813 (0-65535)

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

Default Server Priorities		
EAP Authentication	MAC Authentication	Accounting
Priority 1: 192.168.1.20	Priority 1: <NONE>	Priority 1: 192.168.1.20
Priority 2: <NONE>	Priority 2: <NONE>	Priority 2: <NONE>
Priority 3: <NONE>	Priority 3: <NONE>	Priority 3: <NONE>
Admin Authentication (RADIUS)	Admin Authentication (TACACS+)	
Priority 1: 192.168.1.20	Priority 1: <NONE>	
Priority 2: <NONE>	Priority 2: <NONE>	
Priority 3: <NONE>	Priority 3: <NONE>	

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
vIan 30
authentication open eap eap_methods
authentication network-eap eap_methods
authentication key-management wpa
mbssid guest-mode
dot11 ssid aceSecure
vIan 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 takes, 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

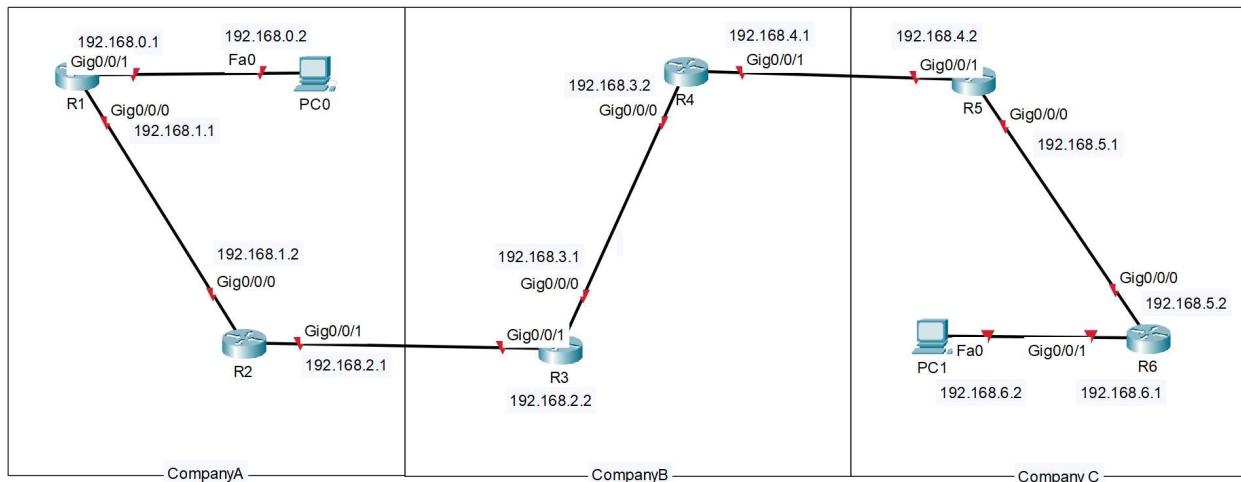
In this lab, we will configure a network consisting of six routers and two end devices within one autonomous system. The AS will be split into 3 areas, 2 routers in each area. The end devices will sit at the ends of Area A and Area C.

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 instead 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 steals 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 out 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.

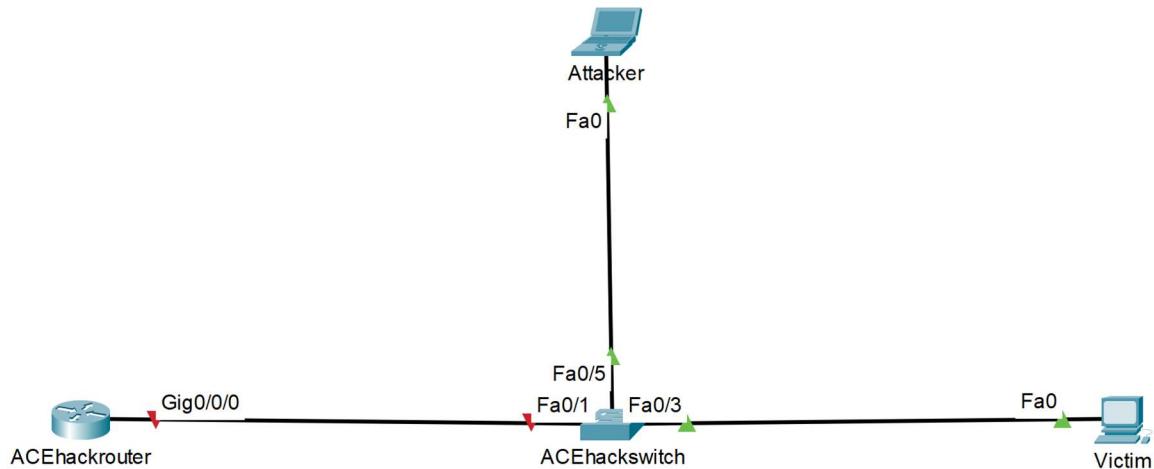
The goal of a DHCP starvation attack is to “starve” or exhaust this pool, so any new devices that join the network are unable to receive an IP address and thus unable to access the internet. A DHCP starvation attack involves sending bogus DHCP DISCOVER packets using bogus MAC addresses as the source 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



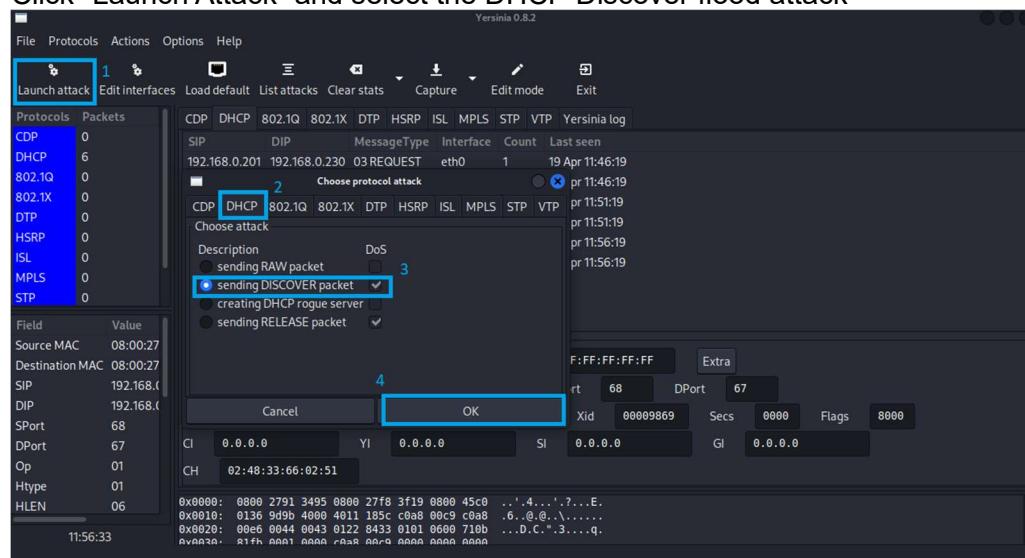
Lab Commands

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 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”.

COM1 - PuTTY

```
Welcome to the Maintenance Recovery Tool

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

866-898-9087 or support@paloaltonetworks.com

< Continue >

Q=Quit, Up/Down=Navigate, ENTER=Select, ESC=Back
```

Select “Factory Reset”.

COM1 - PuTTY

```
Welcome to the Maintenance Recovery Tool

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

>
>
>
>
>
>
>
>
>
>
>
>
>
>
>
>
>
```

Q=Quit, Up/Down=Navigate, ENTER=Select, ESC=Back

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



```
COM1 - PuTTY
Factory Reset

WARNING: Performing a factory reset will remove all logs and configuration.

Using Image:
(X) panos-10.2.6

WARNING: Scrubbing will iteratively write patterns on pancfg, panlogs, and any
extra disks to make retrieving the data more difficult.
NOTE: This could take several hours to several days if selected. Scrubbing is
not recommended unless explicitly required.

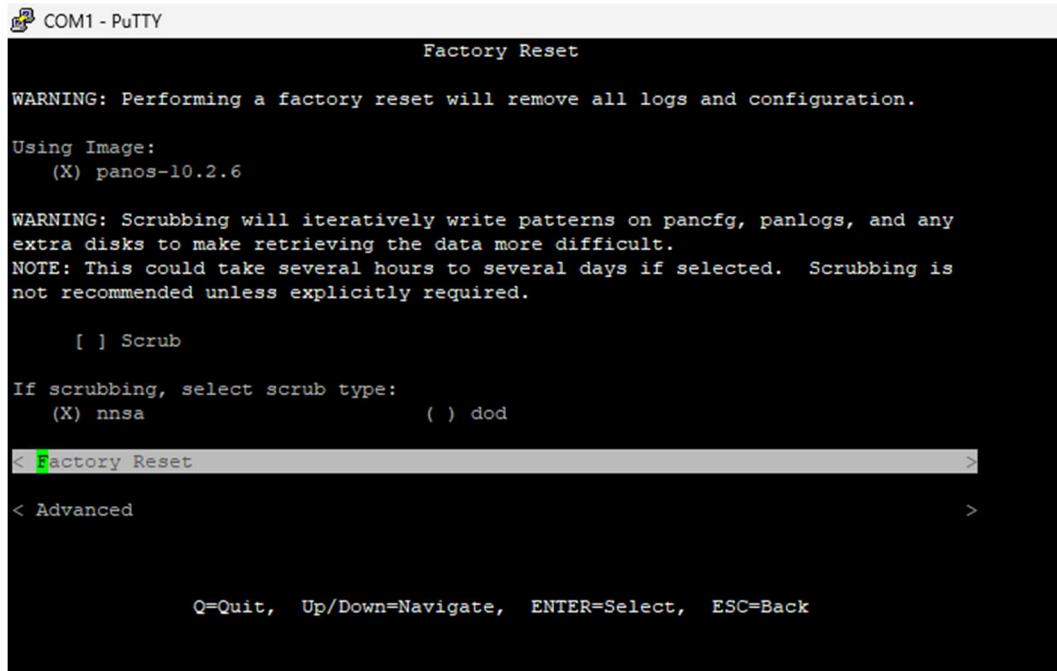
[ ] Scrub

If scrubbing, select scrub type:
(X) nnsa           ( ) dod

< Factory Reset          >
< Advanced             >

Q=Quit, Up/Down=Navigate, ENTER=Select, ESC=Back
```

Select “Factory Reset”



```
COM1 - PuTTY
Factory Reset

WARNING: Performing a factory reset will remove all logs and configuration.

Using Image:
(X) panos-10.2.6

WARNING: Scrubbing will iteratively write patterns on pancfg, panlogs, and any
extra disks to make retrieving the data more difficult.
NOTE: This could take several hours to several days if selected. Scrubbing is
not recommended unless explicitly required.

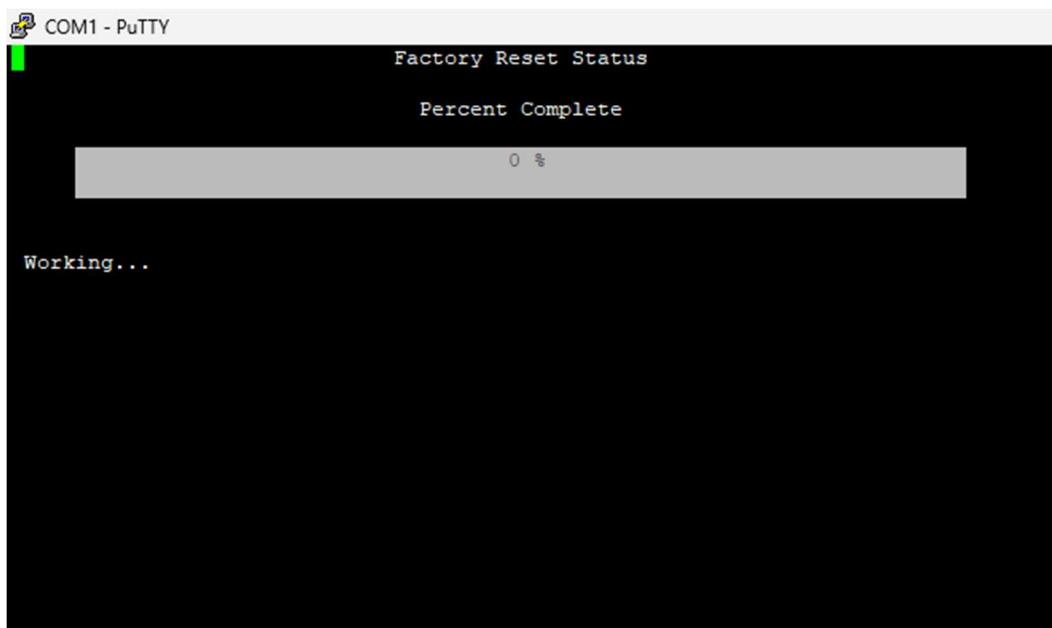
[ ] Scrub

If scrubbing, select scrub type:
(X) nnsa           ( ) dod

< Factory Reset          >
< Advanced             >

Q=Quit, Up/Down=Navigate, ENTER=Select, ESC=Back
```

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.

A screenshot of a PuTTY terminal window titled "COM1 - PuTTY". The session starts with a series of failed login attempts: "PA-220 login: admin" followed by several "incorrect" messages and a timeout message "PA-220 login: timed out after 60 seconds". It then shows a password reset process: "Enter old password :" followed by "admin", "Enter new password :" followed by "admin", "Confirm password :" followed by "admin", and a warning that "Default password can not be used for admin". This is followed by another set of login attempts where the password "admin" is rejected due to being too simple ("admin password does not meet the minimum requirement"). Finally, a successful login is shown: "PA-220 login: admin", "Password:", "Last login: Mon Sep 9 12:35:09 on ttys0", and "Password changed". The session ends with a warning message: "Warning: Your device is still configured with the default admin account credentials. Please change your password prior to deployment." and the prompt "admin@PA-220>".

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 it 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.

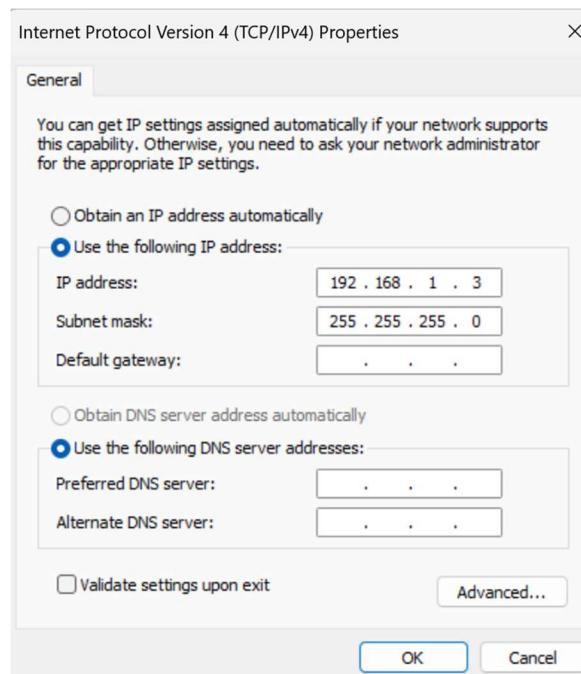
Lab Summary

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.

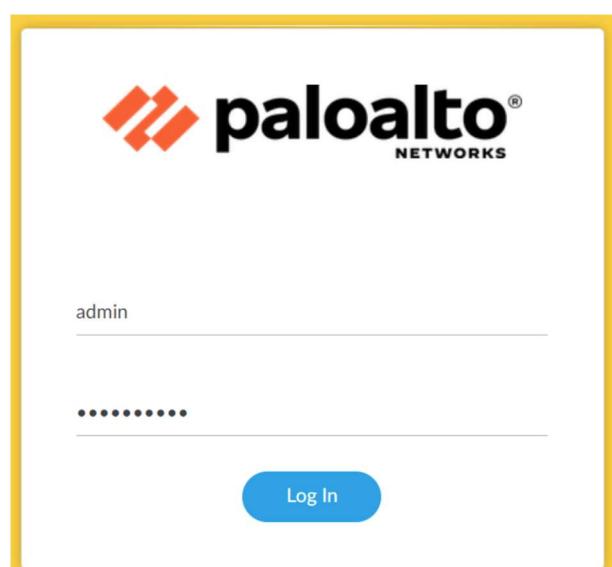
Lab Commands

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.

NAME	TYPE	INTERFACES / VIRTUAL SYSTEMS	ZONE PROTECTION PROFILE	PACKET BUF PROTECTION
trust	virtual-wire	ethernet1/2		<input checked="" type="checkbox"/>
untrust	virtual-wire	ethernet1/1		<input checked="" type="checkbox"/>

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

- Untrust-L3, Type: Layer3

Name: Untrust-L3
Log Setting: None
Type: Layer3

INTERFACES

Zone Protection
Zone Protection Profile: None
Enable Packet Buffer Protection:

User Identification ACL
Enable User Identification:
INCLUDE LIST: Add Delete
Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24
Users from these addresses/subnets will be identified.
EXCLUDE LIST: Add Delete
Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24
Users from these addresses/subnets will not be identified.

Device-ID ACL
Enable Device Identification:
INCLUDE LIST: Add Delete
Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24
Devices from these addresses/subnets will be identified.
EXCLUDE LIST: Add Delete
Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24
Devices from these addresses/subnets will not be identified.

OK Cancel

- Trust-L3, Type: Layer 3

Zone

Name: Trust-L3

Type: Layer3

INTERFACES: (+) Add (-) Delete

Zone Protection: Zone Protection Profile: None, Enable Packet Buffer Protection checked

User Identification ACL: INCLUDE LIST (checked)

Device-ID ACL: INCLUDE LIST (checked)

OK Cancel

- Trust-L2, Type: Layer 2

Zone

Name: Trust-L2

Type: Layer2

INTERFACES: (+) Add (-) Delete

Zone Protection: Zone Protection Profile: None, Enable Packet Buffer Protection checked

User Identification ACL: INCLUDE LIST (checked)

Device-ID ACL: INCLUDE LIST (checked)

OK Cancel

The result should be:

The screenshot shows the PA-220 network configuration interface. The top navigation bar includes links for DASHBOARD, ACC, MONITOR, POLICIES, OBJECTS, NETWORK (which is highlighted in yellow), and DEVICE. On the left, a sidebar menu lists various network components: Interfaces, Zones (selected), VLANs, Virtual Wires, Virtual Routers, IPSec Tunnels, GRE Tunnels, DHCP, DNS, DNS Proxy, GlobalProtect (expanded to show Portals, Gateways, MDM, Clientless Apps, Clientless App Groups, QoS, LLDP), and Network Profiles. The main content area displays a table for managing Zones. The table has columns for NAME, TYPE, INTERFACES / VIRTUAL SYSTEMS, ZONE PROTECTION PROFILE, and PACKET BUFFER PROTECTION. Five zones are listed: trust (virtual-wire, ethernet1/2, checked), untrust (virtual-wire, ethernet1/1, checked), Untrust-L3 (layer3, checked), Trust-L3 (layer3, checked), and Trust-L2 (layer2, checked).

NAME	TYPE	INTERFACES / VIRTUAL SYSTEMS	ZONE PROTECTION PROFILE	PACKET BUFFER PROTECTION
trust	virtual-wire	ethernet1/2		<input checked="" type="checkbox"/>
untrust	virtual-wire	ethernet1/1		<input checked="" type="checkbox"/>
Untrust-L3	layer3			<input checked="" type="checkbox"/>
Trust-L3	layer3			<input checked="" type="checkbox"/>
Trust-L2	layer2			<input checked="" type="checkbox"/>

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.

Ethernet Interface

Interface Name: ethernet1/1

Comment:

Interface Type: Layer3

Netflow Profile: None

Config | IPv4 | IPv6 | SD-WAN | Advanced

Assign Interface To

Virtual Router: default

Security Zone: Untrust-L3

OK Cancel

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.

Ethernet Interface

Interface Name: ethernet1/1

Comment:

Interface Type: Layer3

Netflow Profile: None

Config | **IPv4** | IPv6 | SD-WAN | Advanced

Type: Static PPPoE DHCP Client

Enable SD-WAN Enable Bonjour Reflector

Enable Automatically create default route pointing to default gateway provided by server

Send Hostname: system-hostname

Default Route Metric: 10

Show DHCP Client Runtime Info

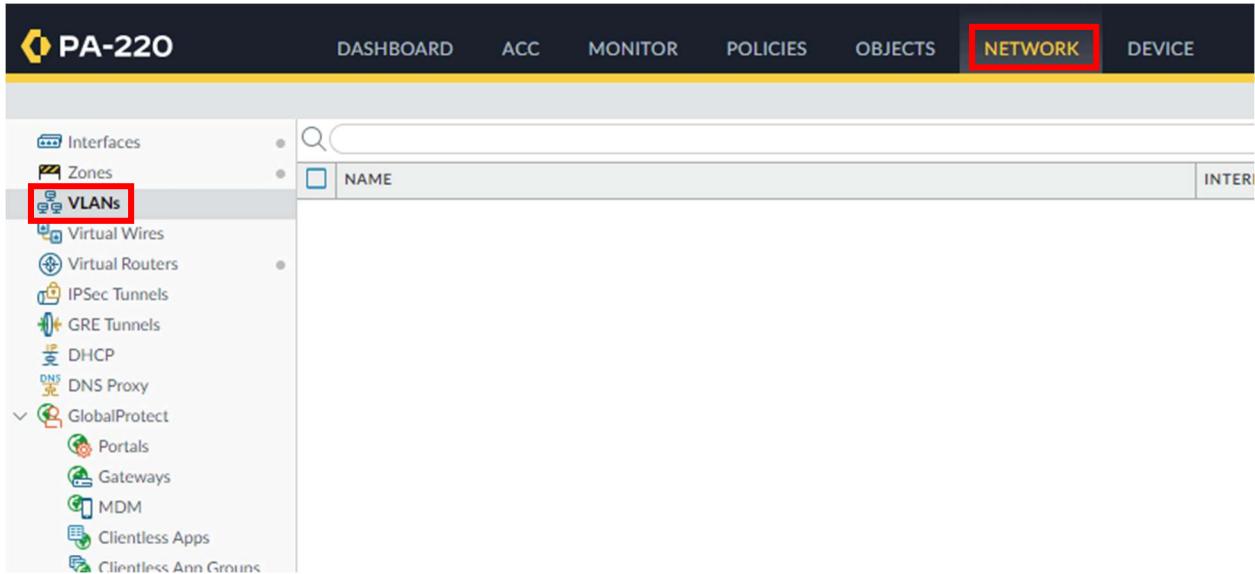
OK Cancel

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”

The screenshot shows the "VLAN" configuration dialog. At the top, it says "VLAN" and has a help icon. Below that, there are two input fields: "Name" (containing "Vlan Object") and "VLAN Interface" (containing "vlan"). Both of these fields are highlighted with a red box. Below the fields is a section titled "Static MAC Configuration" with two tables: "INTERFACES" and "MAC ADDRESS". Each table has a header row with "INTERFACE" and "MAC ADDRESS" respectively. At the bottom, there are "Add" and "Delete" buttons for both tables, and "OK" and "Cancel" buttons at the very bottom.

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 Interface

Interface Name	ethernet1/2
Comment	
Interface Type	Layer2
Netflow Profile	None

Config | Advanced

Assign Interface To

VLAN	Vlan Object
Security Zone	Trust-L2

OK Cancel

- Ethernet 1/3:

Ethernet Interface

Interface Name	ethernet1/3
Comment	
Interface Type	Layer2
Netflow Profile	None

Config | Advanced

Assign Interface To

VLAN	Vlan Object
Security Zone	Trust-L2

OK Cancel

- Ethernet 1/4:

Ethernet Interface

Interface Name	ethernet1/4
Comment	
Interface Type	Layer2
Netflow Profile	None

Config | Advanced

Assign Interface To

VLAN	Vlan Object
Security Zone	Trust-L2

OK Cancel

VLAN Interface Configuration

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

Configure the VLAN interface as shown:

VLAN Interface

Interface Name:

Comment:

Netflow Profile:

Config | IPv4 | IPv6 | Advanced

Assign Interface To

VLAN	<input type="text" value="Vlan Object"/>
Virtual Router	<input type="text" value="default"/>
Security Zone	<input type="text" value="Trust-L3"/>

OK **Cancel**

VLAN Interface

Interface Name:

Comment:

Netflow Profile:

Config | IPv4 | IPv6 | Advanced

Type: Static DHCP Client

<input type="checkbox"/> IP
<input checked="" type="checkbox"/> 192.168.1.254/24

+ Add **- Delete** **↑ Move Up** **↓ Move Down**

IP address/netmask. Ex. 192.168.2.254/24

OK **Cancel**

DHCP Server Configuration

Go to Network > DHCP > DHCP Server

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

DHCP Server

Interface: <input type="text" value="vlan"/>	Mode: <input type="text" value="enabled"/>									
Lease Options										
<input type="checkbox"/> Ping IP when allocating new IP										
Lease: <input type="radio"/> Unlimited <input checked="" type="radio"/> Timeout										
0 <input type="text"/> Days 1 <input type="text"/> Hours 0 <input type="text"/> Minutes										
<table border="1"><tr><th colspan="3">IP POOLS</th></tr><tr><td><input type="checkbox"/></td><td>192.168.1.2-192.168.1.252</td><td></td></tr><tr><td colspan="3">+ Add - Delete</td></tr></table>		IP POOLS			<input type="checkbox"/>	192.168.1.2-192.168.1.252		+ Add - Delete		
IP POOLS										
<input type="checkbox"/>	192.168.1.2-192.168.1.252									
+ Add - Delete										
<table border="1"><thead><tr><th>RESERVED ADDRESS</th><th>MAC ADDRESS</th><th>DESCRIPTION</th></tr></thead><tbody><tr><td>192.168.1.20</td><td>xx:xx:xx:xx:xx:xx</td><td>(Optional MAC Address)</td></tr></tbody></table>		RESERVED ADDRESS	MAC ADDRESS	DESCRIPTION	192.168.1.20	xx:xx:xx:xx:xx:xx	(Optional MAC Address)			
RESERVED ADDRESS	MAC ADDRESS	DESCRIPTION								
192.168.1.20	xx:xx:xx:xx:xx:xx	(Optional MAC Address)								
+ Add - Delete										
OK Cancel										

DHCP Server

Interface: <input type="text" value="vlan"/>	Mode: <input type="text" value="enabled"/>															
Lease Options																
Inheritance Source: <input type="text" value="ethernet1/8"/>	Check inheritance source status															
Gateway: <input type="text" value="192.168.1.254"/>																
Subnet Mask: <input type="text" value="255.255.255.0"/>																
Primary DNS: <input type="text" value="inherited"/>																
Secondary DNS: <input type="text" value="inherited"/>																
Primary WINS: <input type="text" value="inherited"/>																
Secondary WINS: <input type="text" value="inherited"/>																
Primary NIS: <input type="text" value="inherited"/>																
Secondary NIS: <input type="text" value="inherited"/>																
Primary NTP: <input type="text" value="inherited"/>																
Secondary NTP: <input type="text" value="inherited"/>																
POP3 Server: <input type="text" value="inherited"/>																
SMTP Server: <input type="text" value="inherited"/>																
DNS Suffix: <input type="text" value="None"/>																
<table border="1"><tr><th colspan="5">Custom DHCP options</th></tr><tr><th><input type="checkbox"/></th><th>NAME</th><th>CODE</th><th>TYPE</th><th>VALUE</th></tr><tr><td colspan="5">+ Add - Delete ↑ Move Up ↓ Move Down</td></tr></table>		Custom DHCP options					<input type="checkbox"/>	NAME	CODE	TYPE	VALUE	+ Add - Delete ↑ Move Up ↓ Move Down				
Custom DHCP options																
<input type="checkbox"/>	NAME	CODE	TYPE	VALUE												
+ Add - Delete ↑ Move Up ↓ Move Down																
OK Cancel																

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.

Security Policy Rule

General | **Source** | Destination | Application | Service/URL Category | Actions

<input type="checkbox"/> Any <input type="checkbox"/> SOURCE ZONE ^ <input checked="" type="checkbox"/> Trust-L3	<input checked="" type="checkbox"/> Any <input type="checkbox"/> SOURCE ADDRESS ^	any <input type="checkbox"/> SOURCE USER ^	any <input type="checkbox"/> SOURCE DEVICE ^
<input type="button" value="+ Add"/> <input type="button" value="Delete"/>	<input type="button" value="+ Add"/> <input type="button" value="Delete"/>	<input type="button" value="+ Add"/> <input type="button" value="Delete"/>	<input type="button" value="+ Add"/> <input type="button" value="Delete"/>
<input type="checkbox"/> Negate			

OK Cancel

Security Policy Rule

General | Source | **Destination** | Application | Service/URL Category | Actions

select <input type="checkbox"/> DESTINATION ZONE ^ <input checked="" type="checkbox"/> Untrust-L3	<input checked="" type="checkbox"/> Any <input type="checkbox"/> DESTINATION ADDRESS ^	any <input type="checkbox"/> DESTINATION DEVICE ^
<input type="button" value="+ Add"/> <input type="button" value="Delete"/>	<input type="button" value="+ Add"/> <input type="button" value="Delete"/>	<input type="button" value="+ Add"/> <input type="button" value="Delete"/>
<input type="checkbox"/> Negate		

OK Cancel

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

	NAME	TAGS	TYPE	Source				Destination				APPLICATION	SERVICE	ACTION
				ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE				
1	rule1	none	universal	<input checked="" type="checkbox"/> trust	any	any	any	<input checked="" type="checkbox"/> untrust	any	any	any	any	any	<input checked="" type="checkbox"/> Allow
2	Internet Outgoing	none	universal	<input checked="" type="checkbox"/> Trust-L3	any	any	any	<input checked="" type="checkbox"/> Untrust-L3	any	any	any	any	<input checked="" type="checkbox"/> application-...	<input checked="" type="checkbox"/> Allow
3	intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any	any	any	any	<input checked="" type="checkbox"/> Allow
4	interzone-default	none	interzone	any	any	any	any	any	any	any	any	any	any	<input checked="" type="checkbox"/> 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.

NAT Policy Rule

General | Original Packet | Translated Packet

<input type="checkbox"/> Any <input type="checkbox"/> SOURCE ZONE ^ <input checked="" type="checkbox"/> Trust-L3	Destination Zone Untrust-L3	<input checked="" type="checkbox"/> Any <input type="checkbox"/> SOURCE ADDRESS ^	<input checked="" type="checkbox"/> Any <input type="checkbox"/> DESTINATION ADDRESS ^
	Destination Interface ethernet1/8		
	Service any		
+ Add Delete	+ Add Delete	+ Add Delete	OK Cancel

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

NAT Policy Rule

General | Original Packet | Translated Packet

Source Address Translation Translation Type Dynamic IP And Port Address Type Interface Address Interface ethernet1/8 IP Address None	Destination Address Translation Translation Type None
OK Cancel	

Management IP Configuration

Go to Device > Setup > Management

Configure the settings as shown.

Management Interface Settings

	PERMITTED IP ADDRESSES	DESCRIPTION
<input type="checkbox"/>		

IP Type Static DHCP Client

IP Address

Netmask

Default Gateway

IPv6 Address/Prefix Length

Default IPv6 Gateway

Speed

MTU

Administrative Management Services

<input type="checkbox"/> HTTP	<input checked="" type="checkbox"/> HTTPS
<input type="checkbox"/> Telnet	<input checked="" type="checkbox"/> SSH

Network Services

<input type="checkbox"/> HTTP OCSP	<input checked="" type="checkbox"/> Ping
<input type="checkbox"/> SNMP	<input type="checkbox"/> User-ID
<input type="checkbox"/> User-ID Syslog Listener-SSL	<input type="checkbox"/> User-ID Syslog Listener-UDP

[\(+\) Add](#) [\(-\) Delete](#)

[OK](#) [Cancel](#)

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.

Services (?)

Services | NTP

Update Server: updates.paloaltonetworks.com Verify Update Server Identity

DNS Settings

DNS Servers DNS Proxy Object

Primary DNS Server: 8.8.8.8
Secondary DNS Server: 8.8.8.4

Minimum FQDN Refresh Time (sec): 30

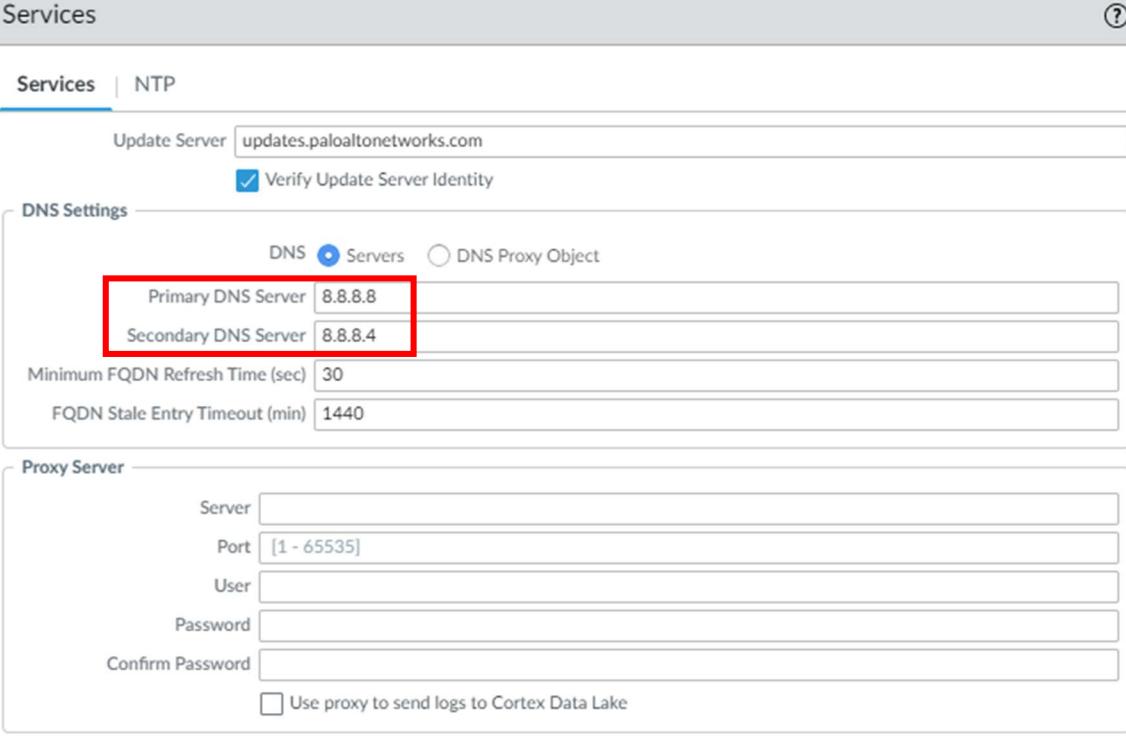
FQDN Stale Entry Timeout (min): 1440

Proxy Server

Server:
Port: [1 - 65535]
User:
Password:
Confirm Password:

Use proxy to send logs to Cortex Data Lake

OK Cancel



Commit Changes

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

The screenshot shows a web-based configuration interface for committing changes. At the top, there is a header with a 'Commit' button and help/sync icons. Below the header, a message states: "Doing a commit will overwrite the running configuration with the commit scope." There are two radio buttons: one selected for "Commit All Changes" and another for "Commit Changes Made By: (1) admin". A table follows, with columns: COMMIT SCOPE, LOCATION TYPE, OBJECT TYPE, ENTITIES, and ADMINS. Two rows are listed: "policy-and-objects" (Policy and Objects) and "device-and-network" (Device and Network Configuration). At the bottom of the main area are three buttons: "Preview Changes", "Change Summary", and "Validate Commit". A note below the preview buttons says: "Note: This shows all the changes in login admin's accessible domain." At the very bottom is a "Description" input field and a row with "Commit" and "Cancel" buttons, where the "Commit" button is highlighted with a red box.

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 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 which 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.

The screenshot shows the Palo Alto Networks PA-220 interface. The left sidebar contains a tree view of objects like Addresses, Regions, Application Groups, and Security Profiles. Under Security Profiles, 'URL Filtering' is selected and highlighted with a red box. The main pane shows a table for creating a new URL Filtering profile. The table has columns for NAME, LOCATION, SITE ACCESS, USER CREDENTIAL SUBMISSION, and HTTP HEADER INSERTION. A row for 'url-filtering' is being created, with the 'NAME' field set to 'url-filtering'. The 'LOCATION' dropdown is set to 'Prefixed'. The 'SITE ACCESS' section lists categories: Allow Categories (6), Alert Categories (7), Continue Categories (3), Block Categories (12), and Override Categories (1). The 'USER CREDENTIAL SUBMISSION' and 'HTTP HEADER INSERTION' sections also list various categories. At the bottom of the table, there are tabs for 'Add', 'Edit', 'PDF/CSV', and 'Cancel'.

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

The screenshot shows the 'URL Filtering Profile' configuration dialog. The 'Name' field is set to 'url-filtering' and is highlighted with a red box. The 'Description' field is empty. Below the name, there are tabs for 'Categories', 'URL Filtering Settings', 'User Credential Detection', 'HTTP Header Insertion', and 'Inline Categorization'. The 'Categories' tab is selected and highlighted with a blue bar. It displays a table of pre-defined categories under 'Pre-defined Categories'. The table has columns for 'CATEGORY', 'SITE ACCESS', and 'USER CREDENTIAL SUBMISSION'. The categories listed are: abortion, abused-drugs, adult, alcohol-and-tobacco, artificial-intelligence, and auctions. The 'SITE ACCESS' column contains actions: allow, block, block, allow, override, and allow. The 'USER CREDENTIAL SUBMISSION' column contains actions: allow, block, block, allow, allow, and allow. A note at the bottom left says '* Indicates a custom URL category, + indicates external dynamic list'. At the bottom right are 'OK' and 'Cancel' buttons.

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

CATEGORY	SITE ACCESS	USER CREDENTIAL SUBMISSION
abortion	allow	allow
abused-drugs	block	block
adult	block	block
alcohol-and-tobacco	allow	allow
<input checked="" type="checkbox"/> artificial-intelligence	override	allow
auctions	allow	allow

* indicates a custom URL category, + indicates external dynamic list
Check URL Category

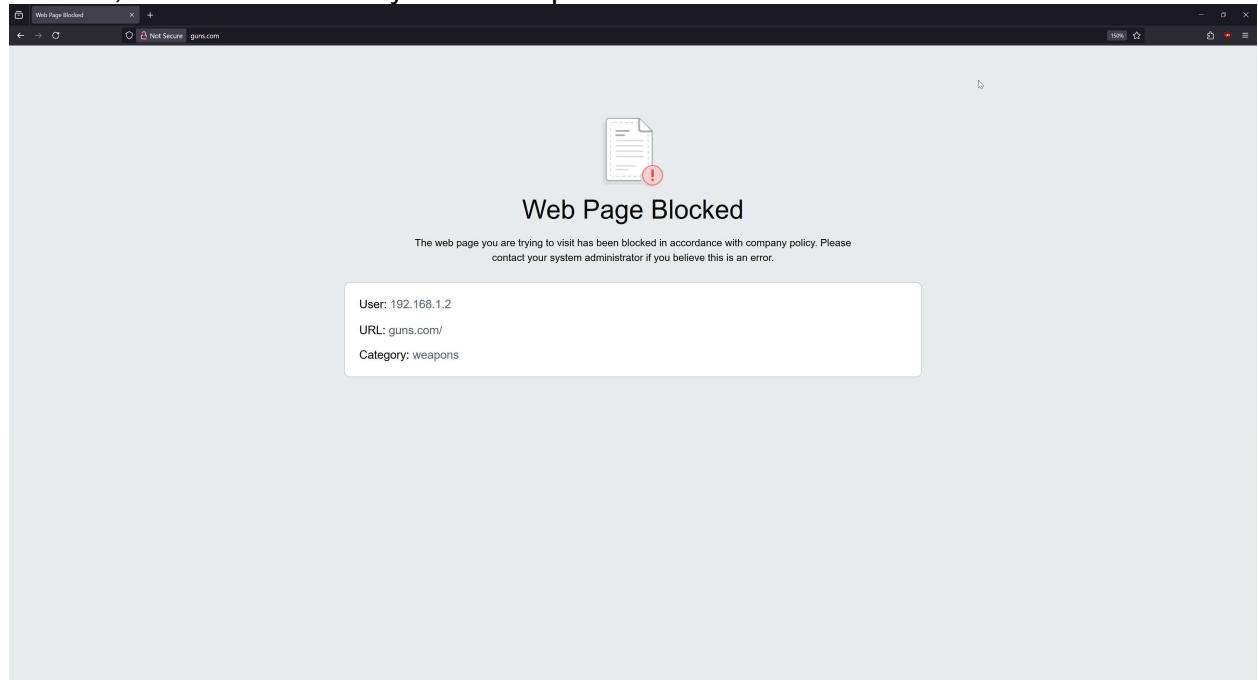
- 4) Keep the other settings the same and create the profile by pressing “Ok”.

- 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.

Action Setting	Log Setting
Action: Allow <input type="checkbox"/> Send ICMP Unreachable	<input type="checkbox"/> Log at Session Start <input checked="" type="checkbox"/> Log at Session End Log Forwarding: None
Profile Setting	Other Settings
Profile Type: Profiles Antivirus: None Vulnerability Protection: None Anti-Spyware: None URL Filtering: url-filtering (highlighted with a red box)	Schedule: None QoS Marking: None <input type="checkbox"/> Disable Server Response Inspection

- 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.

NAME	SUBJECT	ISSUER	CA	KEY	EXPIRES	STATUS	ALGORITHM	VMWARE
FilteringOverrideCert	CN=192.168.1.254	CN=192.168.1.254			Dec 22 16:08 2025 GMT	valid	RSA	Forward Trust Certificate Forward Unsigned Certificate

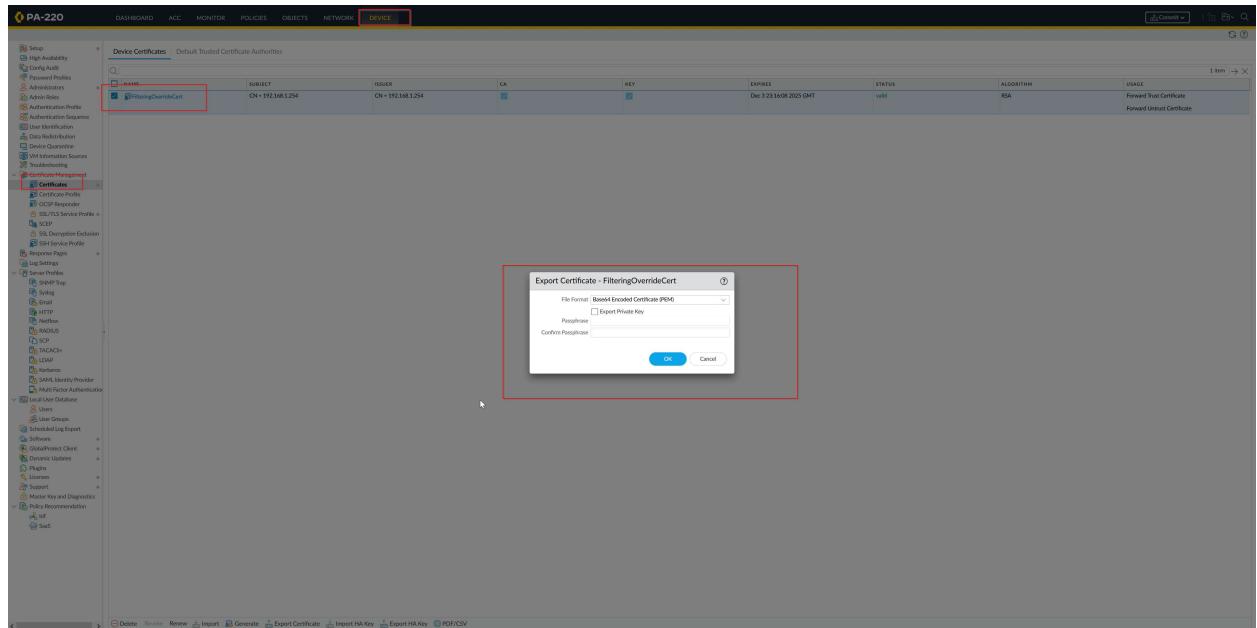
- 9) Set the following fields. Make sure your default gateway is configured as the correct address.

The screenshot shows the 'Device Certificates' section of the PA-220 interface. A certificate named 'FilteringOverrideCert' is listed in the table. A modal window titled 'Certificate Information' is open, displaying details about the certificate. The certificate's name is 'FilteringOverrideCert', subject is 'CN=192.168.1.254', issuer is 'CN=192.168.1.254', and it has an RSA algorithm. The status is 'valid' and it expires on Dec 9 23:59:00 2025 (GMT). The usage is 'Forward Trust Certificate'. The modal also shows the certificate's validity period from Nov 23 14:00 2024 (GMT) to Dec 9 23:59:00 2025 (GMT). The 'OK' button is highlighted.

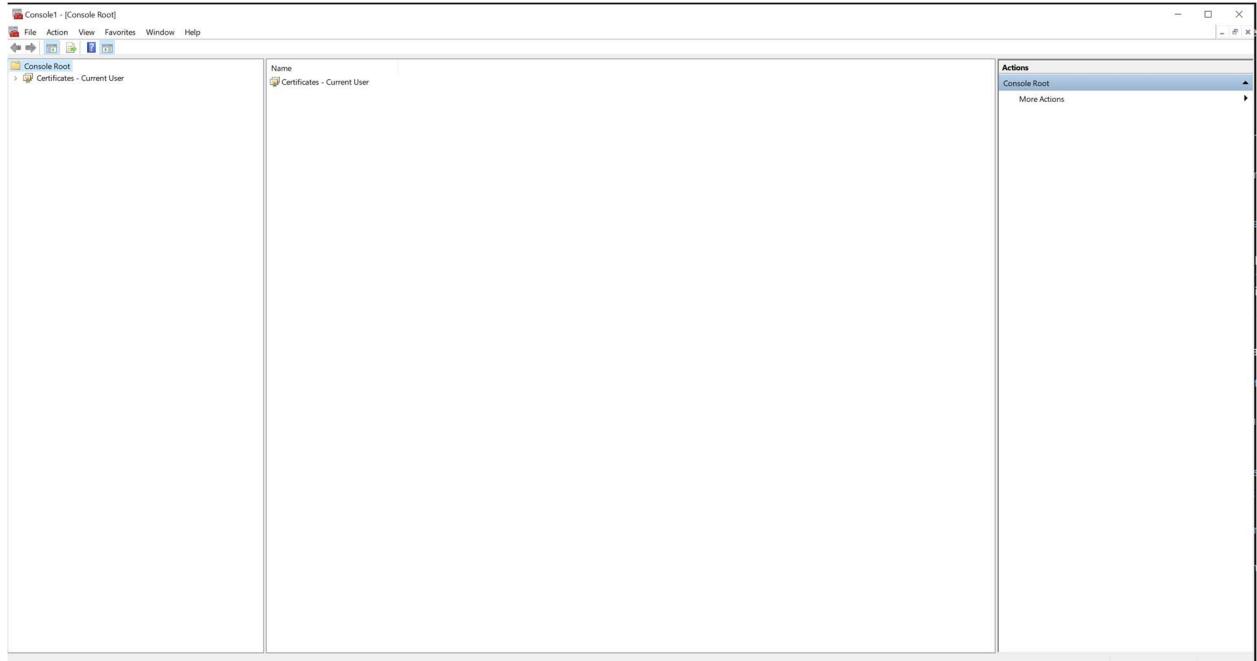
- 10) Navigate to Policies > Decryption and add a new policy. Make sure it is applied to all inbound and outbound traffic. Set the type as "ssl-decrypt-proxy".

The screenshot shows the 'Decryption' section of the PA-220 interface. A new policy named 'ssl-forwarding' is listed in the table. The policy details are: Source is 'Any' and Destination is 'Any'. Deny Options include 'LOG SUCCESSFUL SSL HANDSHAKE' and 'LOG UNSUCCESSFUL SSL HANDSHAKE'. Rule Usage shows 0 hits. The policy was modified on 2024-11-21. The 'ssl-forwarding' policy is highlighted with a red box.

- 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.

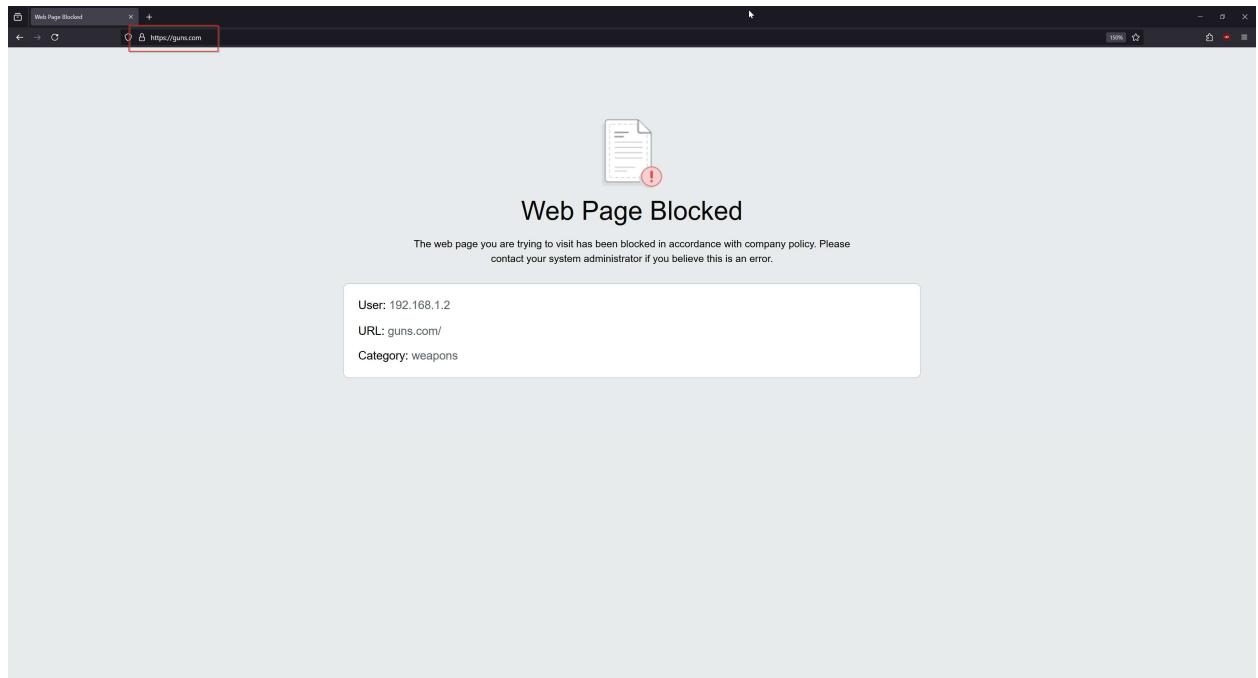


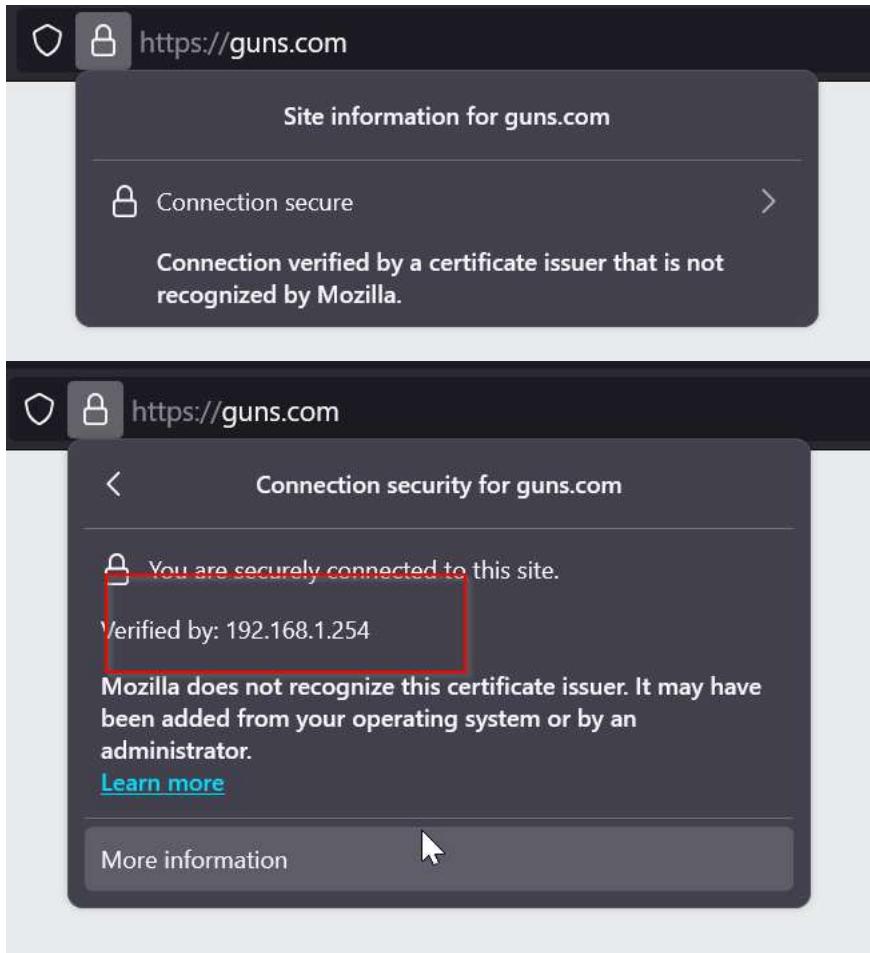
- 12) Install the root certificate. On Windows, this requires extra permissions. Press "Windows + r" and launch mmc, the Windows management console. Add Certificates to the menu.



- 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.

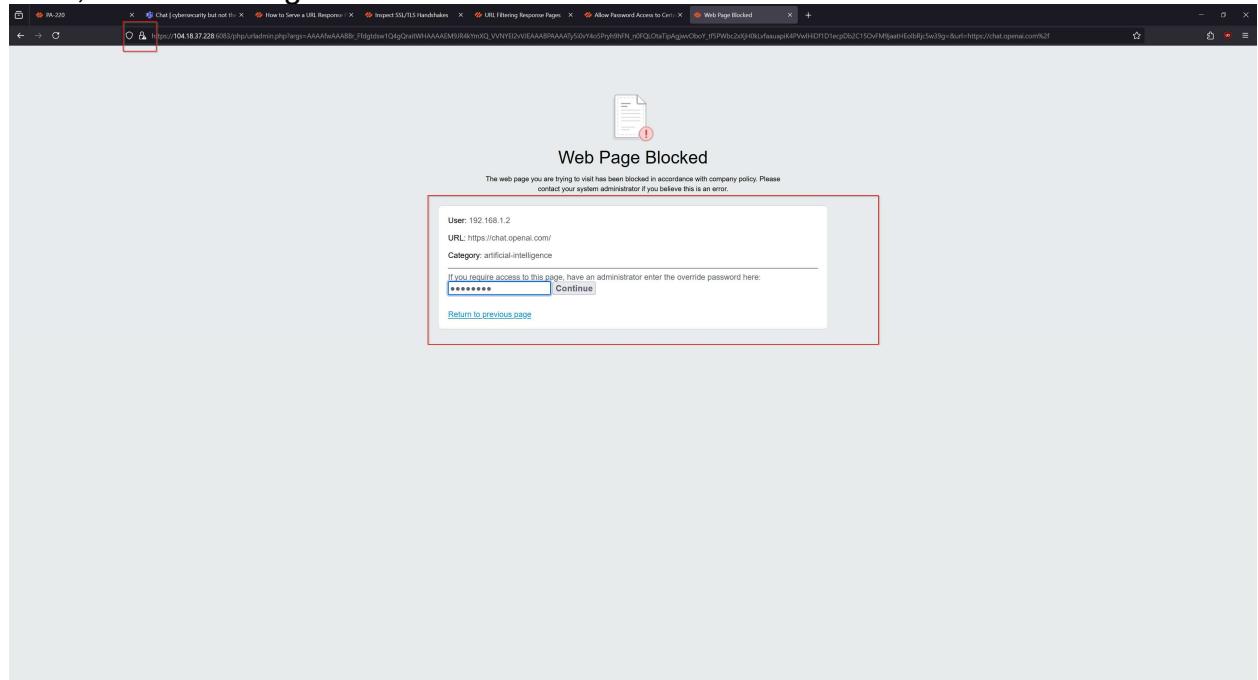




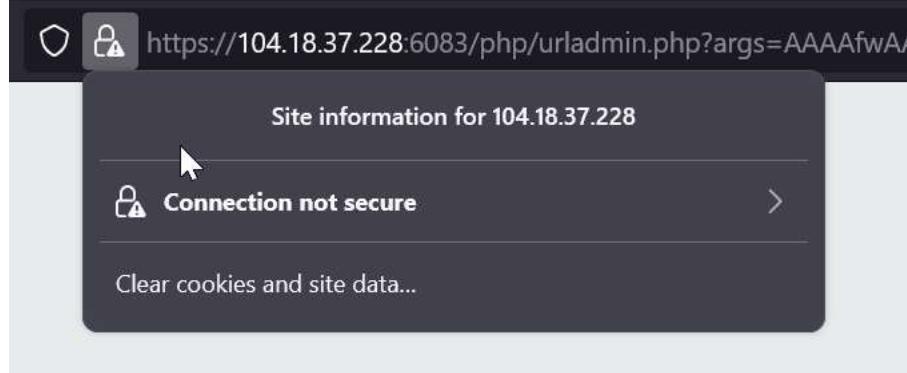
- 15) We can add the “override” settings now. Go to Device > Setup > URL Filtering and add a new URL Admin Override profile.

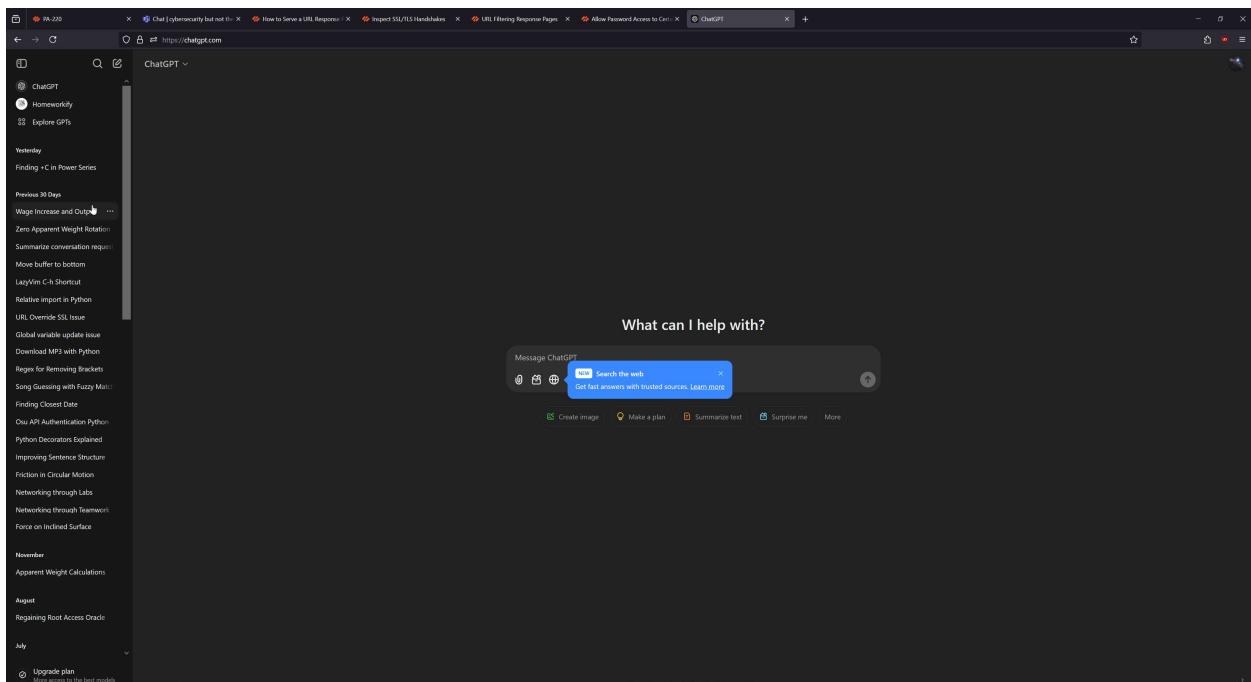
The screenshot shows the PA-220 device configuration interface under the 'DEVICE' tab. On the left, the 'Setup' menu is expanded, showing various sections like Management, Operations, Services, Interfaces, Telemetry, Content-ID, WiFi/Fire, Session, ACE, and DLP. In the center, the 'URL Filtering' section is selected. A 'URL Admin Override' dialog box is open, prompting for a 'Password', 'Confirm Password', 'Username' (set to '350/113 Service Points'), and 'Mode' (set to 'Transparent'). The 'OK' button is visible at the bottom of the dialog. The background shows other configuration tabs like Content-ID Settings, Realtime Signature Lookup, X-Forwarded-For Headers, and Content-ID Analytics.

- 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, GlobalProtect 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.

The screenshot shows the PA-220 configuration interface. The top navigation bar includes links for DASHBOARD, ACC, MONITOR, POLICIES, OBJECTS, NETWORK, and DEVICE. The DEVICE tab is selected and highlighted with a red box. Below the navigation is a toolbar with Commit, Undo, Redo, and Search icons. The left sidebar contains a tree view of configuration categories, with 'Certificates' under 'Certificate Management' also highlighted with a red box. The main content area is titled 'Device Certificates | Default Trusted Certificate Authorities'. It displays a table with two items:

NAME	SUBJECT	ISSUER	CA	KEY	EXPIRES	STATUS	ALGORITHM	USAGE
FilteringOverrid...	CN = 192.168.1.254	CN = 192.168.1.254	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Dec 3 23:16:08 202...	valid	RSA	Forward Trust Certi... Forward Untrust Ce...
RootCert	CN = RootCert	CN = RootCert	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Jan 10 18:05:57 20...	valid	RSA	
Intermediate...	CN = IntermediateC...	CN = RootCert	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Jan 10 18:06:24 20...	valid	RSA	
Ser...	CN = 192.168.40.97	CN = IntermediateCert	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Jan 10 18:32:08 20...	valid	RSA	

At the bottom of the page, there are buttons for Delete, Revoke, Renew, Import, Generate (highlighted with a red box), Export Certificate, Import HA Key, Export HA Key, and PDF/CSV.

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.

The image shows three separate 'Generate Certificate' dialog boxes, each with a red border around its main content area. Each dialog has fields for Certificate Type (Local), Certificate Name, Common Name, Signed By, OCSP Responder, Cryptographic Settings (Algorithm RSA, Number of Bits 2048, Digest sha256, Expiration 365 days), and Certificate Attributes (a table with columns TYPE and VALUE). The 'Signed By' dropdown is set to 'RootCert' for the first two and 'IntermediateCert' for the third. The 'Common Name' field is set to 'RootCert' for the first, 'IntermediateCert' for the second, and '192.168.40.97' for the third. The 'Certificate Attributes' table includes a row where 'IP = "IP Address" from Subject Alternative Name (SAN) field' is checked and '192.168.40.97' is entered in the 'Value' column. Each dialog has a 'Generate' and 'Cancel' button at the bottom.

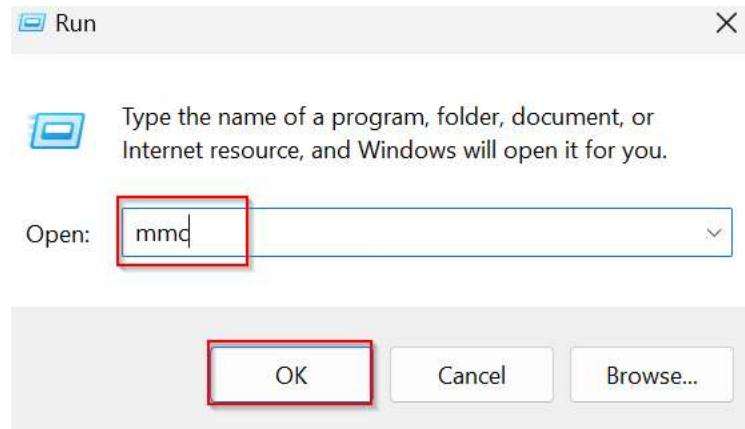
3. Navigate to Device > SSL/TLS Device Profile and click Add. Set the name to SSL-TLS-Server and the Certificate to ServerCert.

The image shows the 'SSL/TLS Service Profile' dialog. It has fields for 'Name' (SSL-TLS-Server) and 'Certificate' (ServerCert), both with red borders. Below these are 'Protocol Settings' with 'Min Version' (TLSv1.0) and 'Max Version' (Max), also with red borders. At the bottom are 'OK' and 'Cancel' buttons.

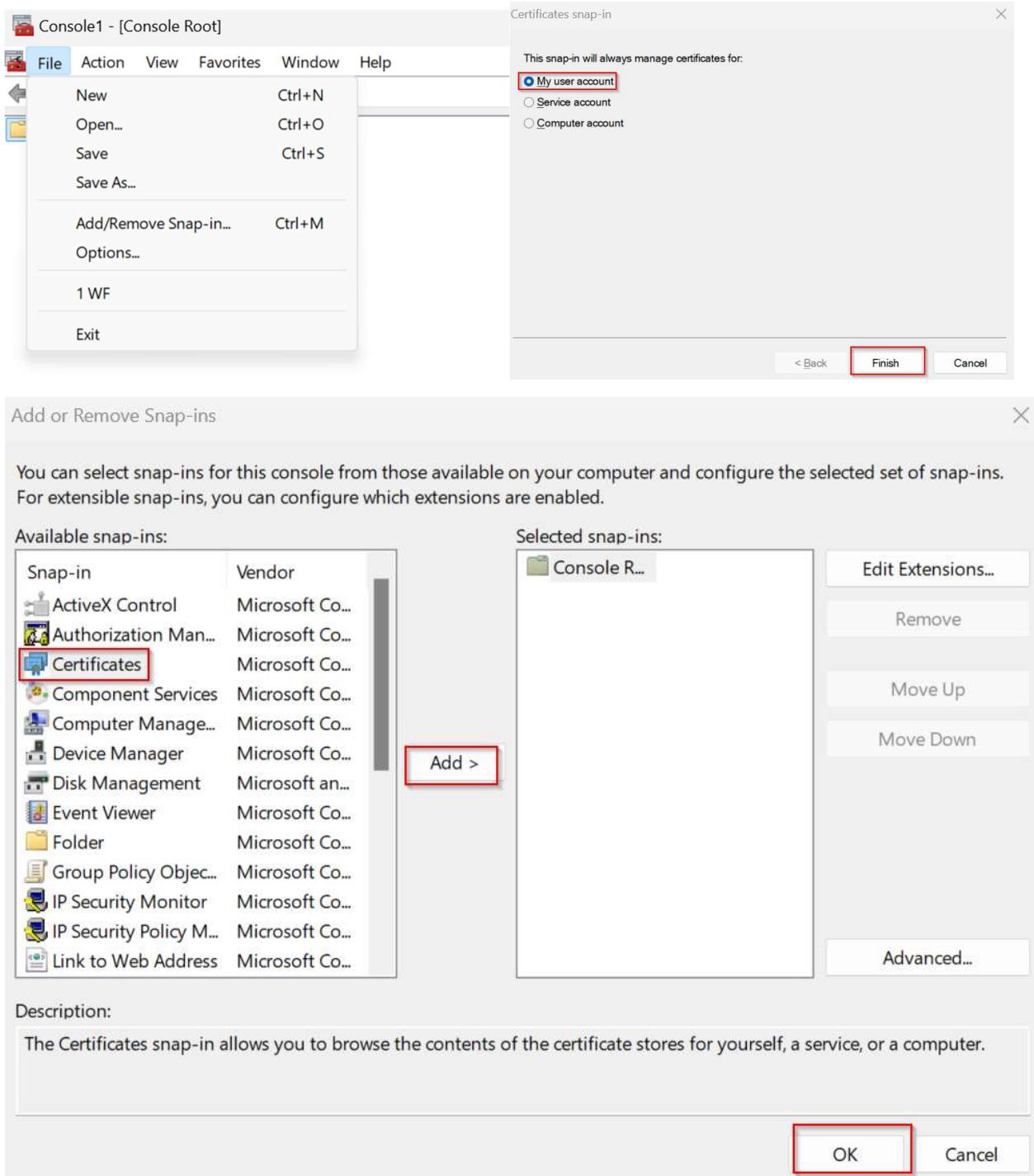
4. Navigate to Device > Certificate Management > Certificate Profile and click Add. Name the certificate profile Client-CertProfile and add both the Root and Intermediate Certificates.

NAME	DEFAULT OCSP URL	OCSP VERIFY CERTIFICATE	TEMPLATE NAME/OID
RootCert			
IntermediateCert			

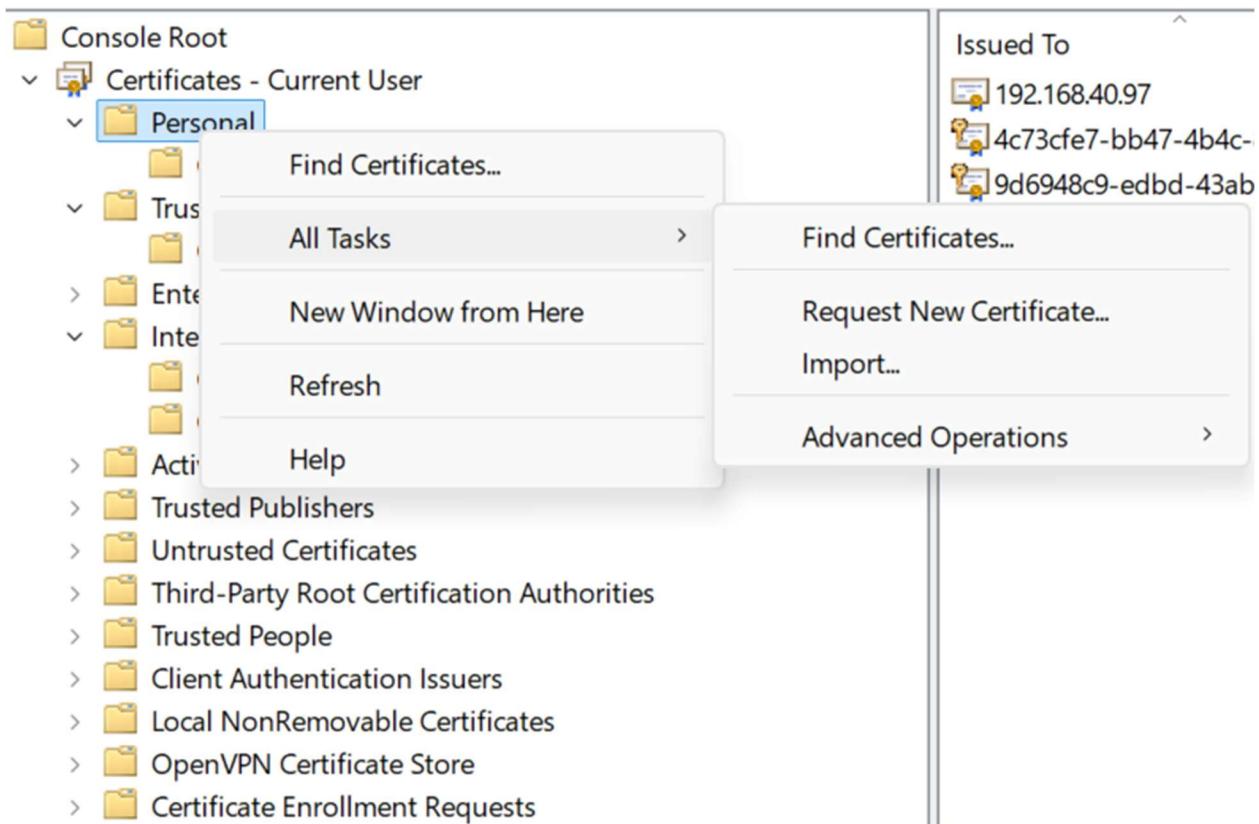
5. Now, we will add the certificates to your end device. Press WIN+R to open the Run dialog, and open "mmc".



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.

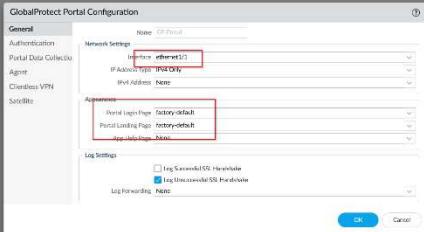
NAME	SUBJECT	ISSUER	CA	KEY	EXPIRES	STATUS	ALGORITHM	USAGE
CN=RootCert	CN=192.168.1.254	CN=192.168.1.254			Dec 22 23:59:59 2025 GMT	valid	RSA	Forward Trust Certificate
CN=RootCert	CN=RootCert	CN=RootCert			Jan 18 00:07:30 2024 GMT	valid	RSA	Forward Trust Certificate
CN=IntermediateCert	CN=RootCert	CN=RootCert			Jan 30 00:06:24 2023 GMT	valid	RSA	Forward Trust Certificate
CN=ServerCert	CN=IntermediateCert	CN=RootCert			Jan 30 19:32:09 2025 GMT	valid	RSA	Forward Trust Certificate

NAME	LOCATION	FAILED ATTEMPTS	LOCKOUT TIME (HRS)	ALLOW LIST	AUTHENTICATION	SERVICE PROFILE	AUTHENTICATION FACTORS	DETAILS	LOCKED USERS
Local_Auth					Local				

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 the VPN will be allowed.

Virtual Router	default
Security Zone	Untrust-L3

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.



GlobalProtect Portal Configuration

General

Name: GP Portal

Network Settings:

- Interface: Internet/0/0
- IP Address Type: IP4 Only
- IPv4 Address: None

Log Settings:

- Log SuccessfulSSL Handshake:
- Log UnsuccessfulSSL Handshake:
- Log Forwarding: None

Authentication

SSL/TLS Service Profile: SSL-TLS-Server

Client Authentication

	NAM	OS	AUTHENTIC... PROFILE	AUTO RETRIEVE PASSCODE	USERNAME LABEL	PASSWORD LABEL	AUTHENTI... MESSAGE	ALLOW AUTHENTI... WITH USER CREDENTI... OR CLIENT CERTIFI...
<input type="checkbox"/>	GP Client	Any	Local_Auth	<input type="checkbox"/>	Username	Password	Enter login credentials	Yes

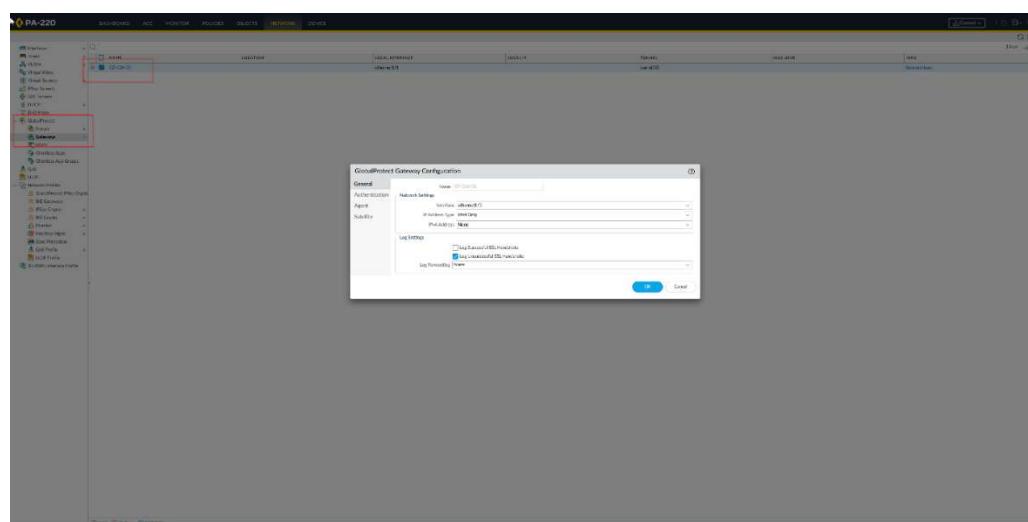
Certificate Profile: None

Buttons: OK, Cancel

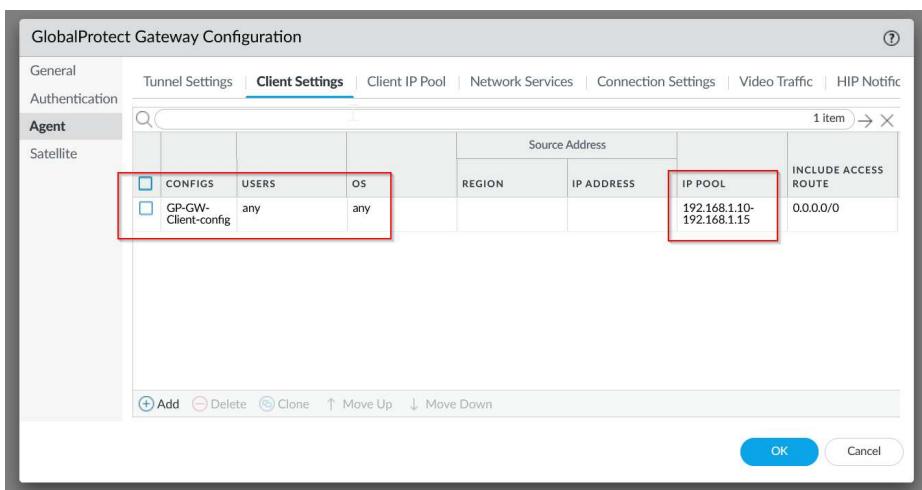
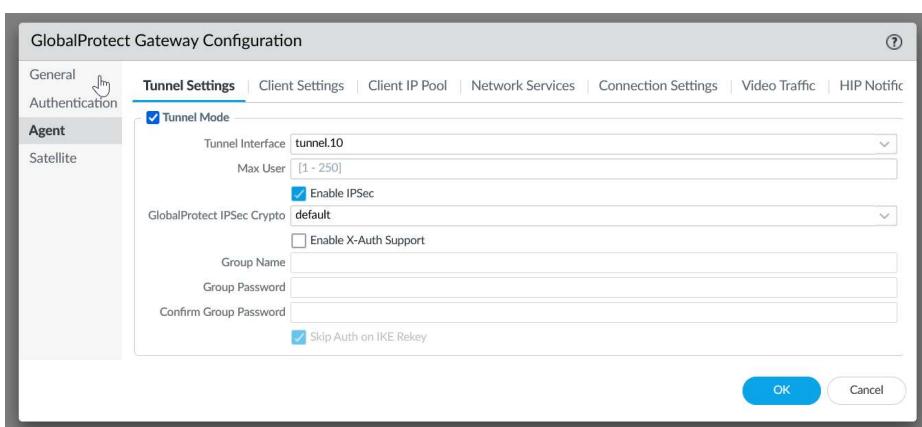
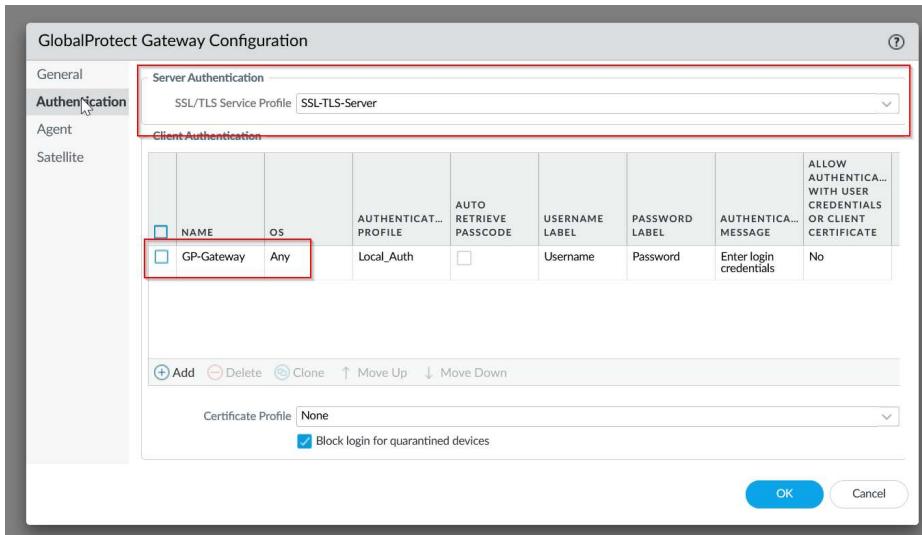
11. Navigate to the Agent tab. Add a new client config. Set the name, add an external gateway using the IP address reference in the Common Name field of the Server Cert. Then, in the “App” tab, select ‘On-demand’ on the Connect-method dropdown. Under Trusted Root CA, select both the Root and Intermediate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

The screenshot shows two overlapping configuration windows. The left window is 'GlobalProtect Portal Configuration' with the 'Agent' tab selected. It displays a table of client configurations, one of which is highlighted with a red box. Below the table is a section for certificate installation, also highlighted with a red box. The right window is titled 'Configs' and has the 'App' tab selected. It shows various app configuration options. A specific section under 'App Configurations' is highlighted with a red box, showing the 'Connect Method' dropdown set to 'On-demand (Manual user initiated connection)'.

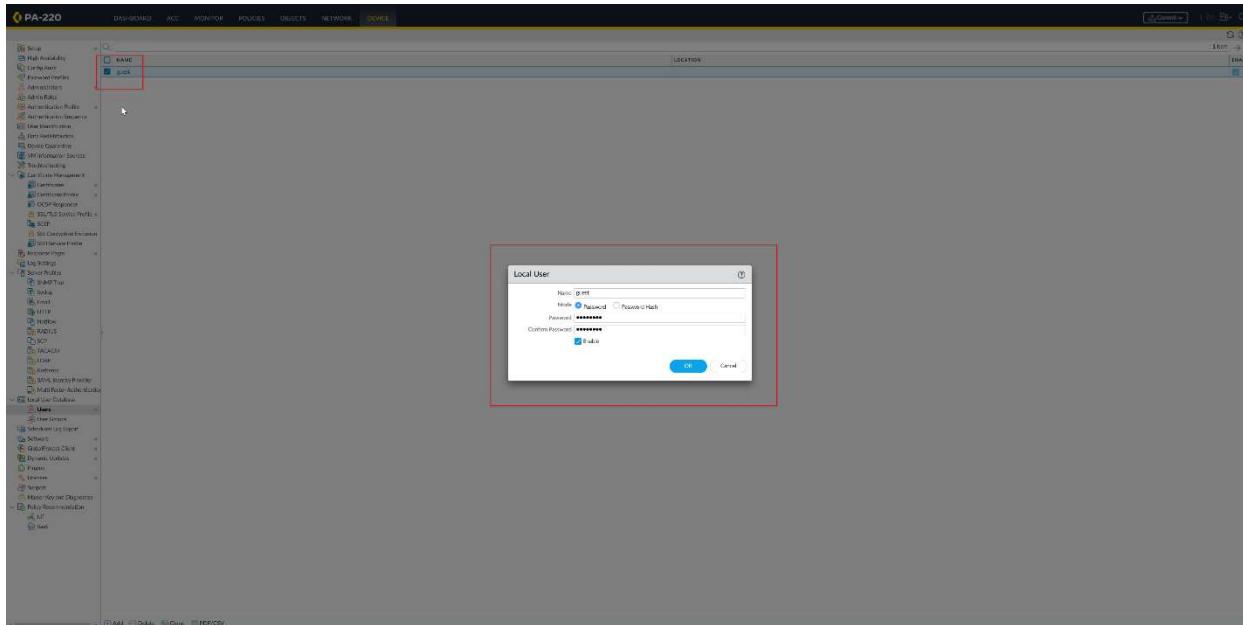
12. Now, we will configure the Global Protect Gateway. Navigate to Network > GlobalProtect > Gateways and click Add. Give the gateway a name and select the same interface as before to act as the gateway.



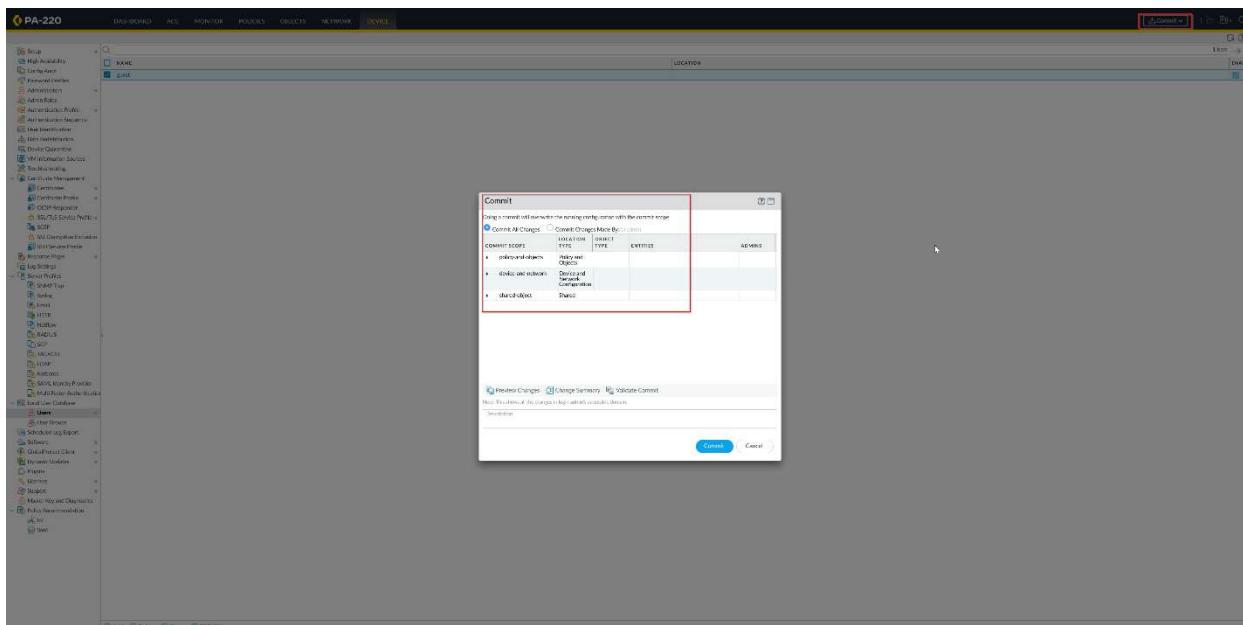
13. In the Authentication tab, select the SSL-TLS profile created. Click Add under Client Authentication. Give it a name, and select the Authentication Profile you created. In the Agent tab, select the tunnel interface you created and enable IPsec. In the Client setting tab, add a config and give it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



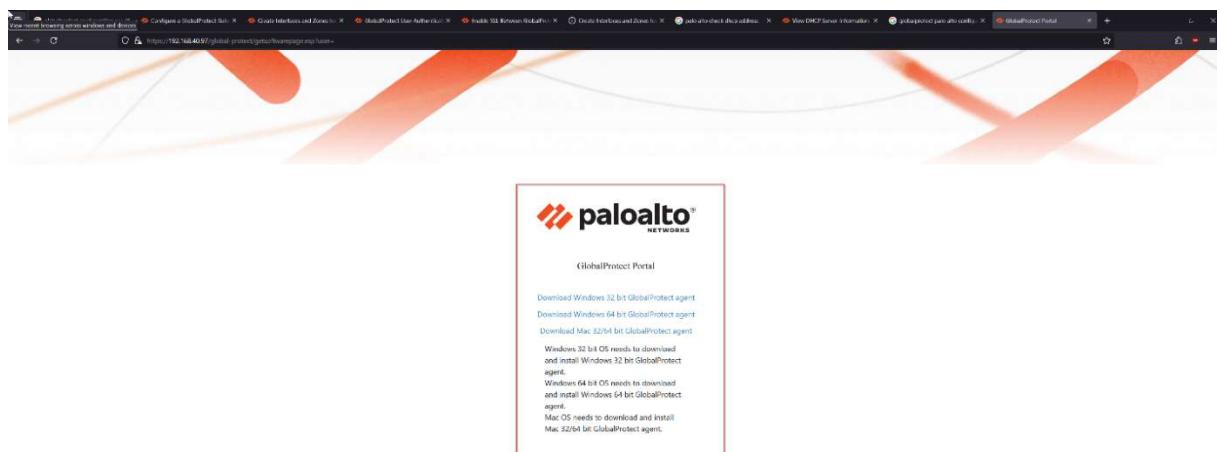
14. Navigate to Device > Local User Database > Users, and create a local user for testing.



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.

The image shows two screenshots of the GlobalProtect app. The left screenshot is the 'Welcome!' screen, which includes a 'Get Started' button. The right screenshot shows the 'Not Connected' state with a 'Connect' button. Below these, the 'Status' screen is displayed, showing a 'Connected' status with 'Extn-GW01' and 'Best Available Gateway'. A 'Manage Portals' section lists '192.168.40.97' with a red box around it. The 'Tunnel Statistics' section shows assigned IP addresses (IPv4: 192.168.1.11, IPv6: 192.168.40.97), session uptime (00:00:01), and protocol (IPSec). It also shows gateway IP address (192.168.40.97), bytes in (0), bytes out (2435), gateway location, packets in (0), and packets out (30).

Welcome!

GlobalProtect extends security policies to all mobile users to eliminate remote access blindspots and strengthen security.

Get Started

Not Connected

Enter the portal address to connect and secure access to your applications and the internet.

Portal settings: 192.168.40.97

Connect

Status

Connected
Extn-GW01
Best Available Gateway

Manage Portals

✓ 192.168.40.97

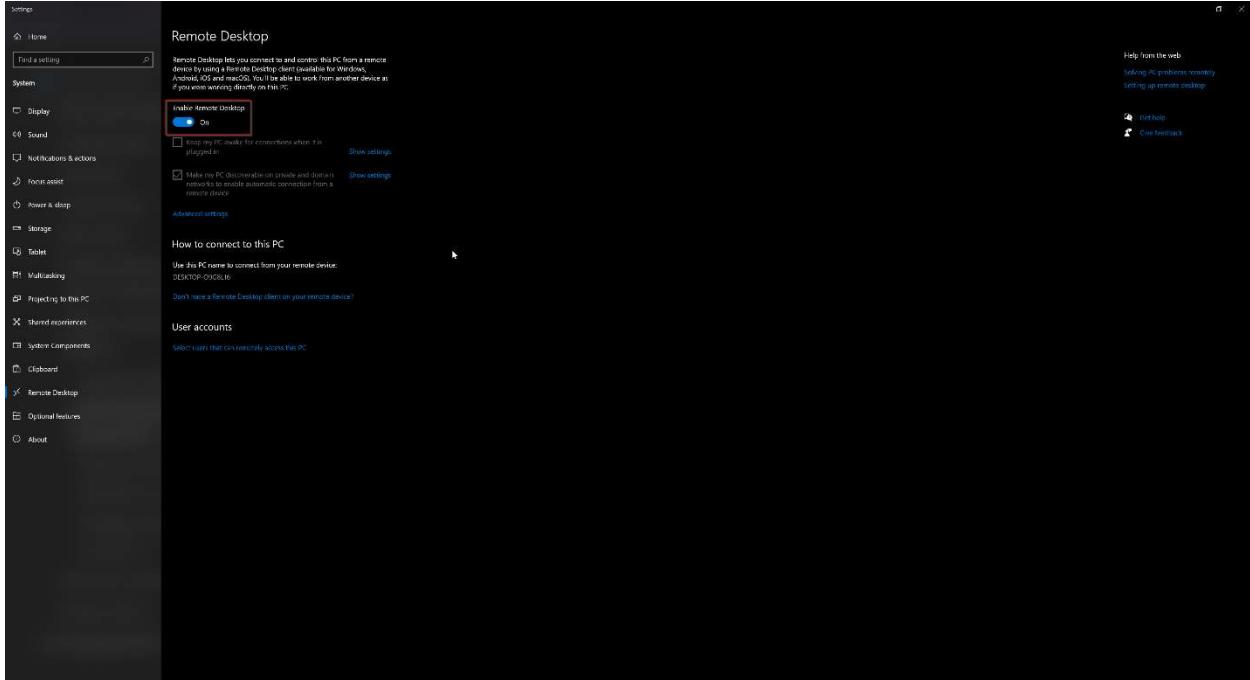
Tunnel Statistics

Assigned IP Address(es)	Session Uptime	Protocol
IPv4 192.168.1.11	00:00:01	IPSec
IPv6		
Gateway IP Address 192.168.40.97	Bytes In 0	Bytes Out 2435
Gateway Location	Packets In 0	Packets Out 30

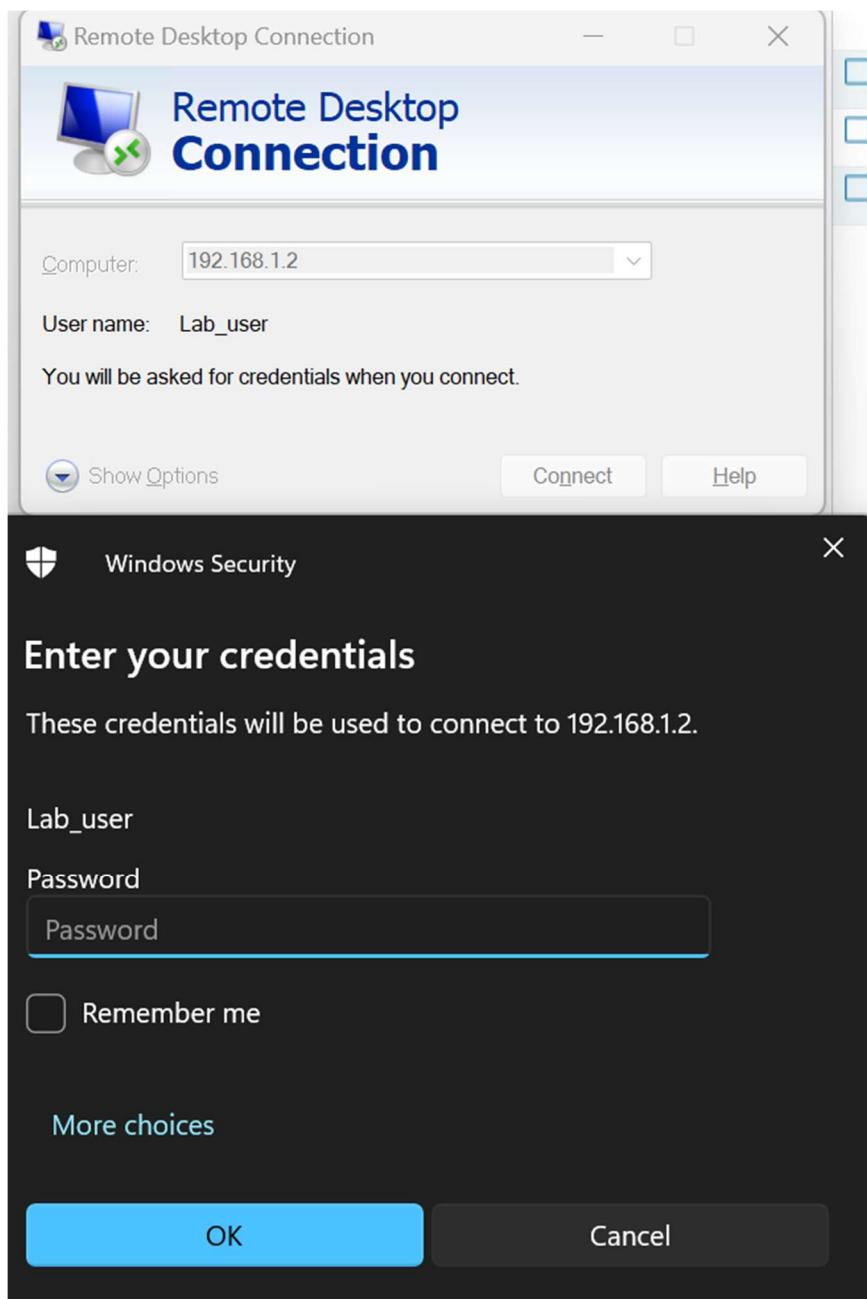
guest

Sign Out

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

- 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 it 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

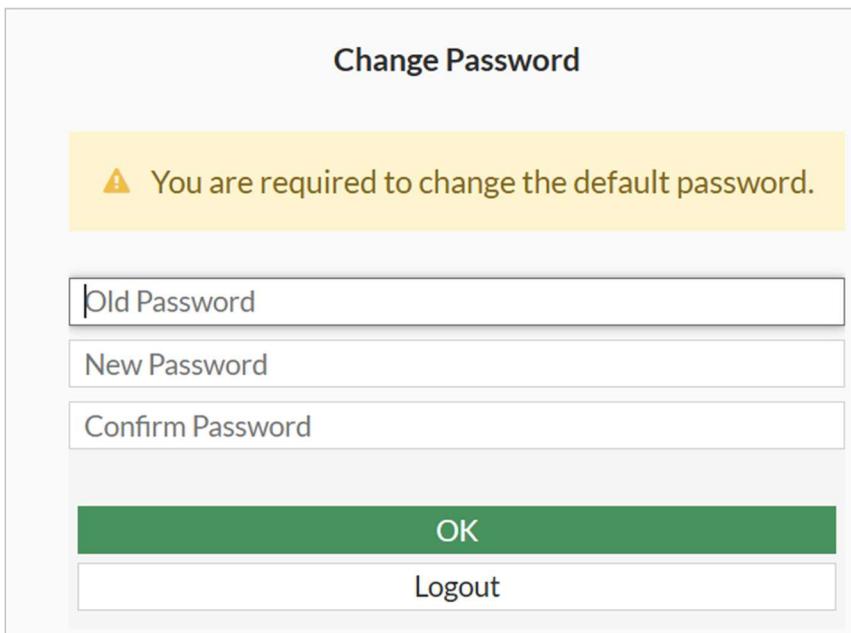
In this lab, we will set up a Fortigate firewall for a SOHO network. The firewall will be accessed and configuration through the online GUI. An administrative password will be set up. Two SSIDs are created, one using WPA2 PSK (pre-shared key), and the other used WPA Enterprise. Firewall policies are 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.



Change Password

⚠ You are required to change the default password.

Old Password

New Password

Confirm Password

OK

Logout

Skip the old password and put in your new password.

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

The screenshot shows the FortiGate Setup interface. At the top, it says "FortiGate Setup" and has a warning icon with the text: "⚠ Perform the following steps to complete the setup of this FortiGate." Below this is a bulleted list of steps:

- Register with FortiCare ✓
- Automatic Patch Upgrades
- Dashboard Setup
- Change Your Password ✓

At the bottom of this section is a large green "Begin" button.

Below the "Begin" button is a "Setup Progress" table:

Setup Progress	Automatic Patch Upgrades for v7.2
Register with FortiCare ✓	<input checked="" type="radio"/> Enable automatic patch upgrades for v7.2 Regularly check for available patch upgrades within the v7.2 version during a configured time window. If any are available, automatically download and install them. The device will reboot during the upgrade. <input type="radio"/> Disable automatic patch upgrades Do not automatically download or install patch upgrades.
Automatic Patch Upgrades	Upgrade schedule <input checked="" type="radio"/> Delay <input type="radio"/> Specify days Delay by number of days: 3 Install during specified time: 01:00 AM to 4:00 AM
Dashboard Setup	
Change Your Password ✓	

At the bottom of the "Automatic Patch Upgrades" section is a "Save and continue" button.

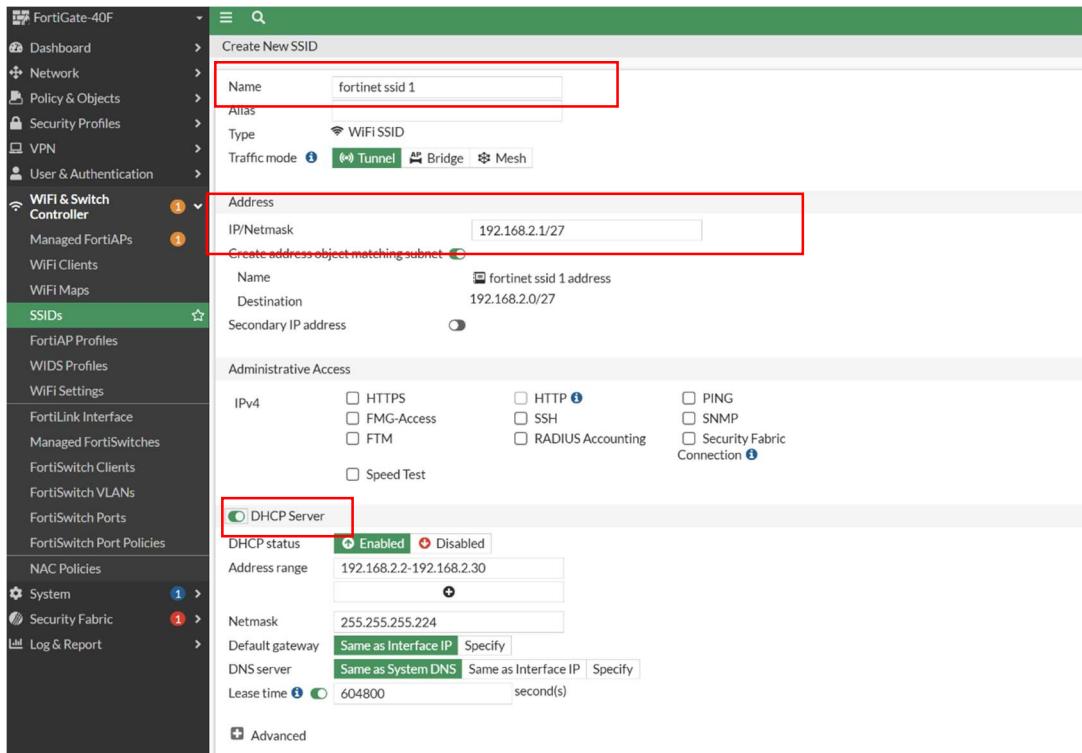
Below the progress table is a modal dialog titled "Enable Automatic Patch Upgrades". It contains an information icon and the text: "Acknowledge that your FortiGate will automatically update when a new firmware patch is available. This can be changed later within the Firmware & Registration page." There is a checked checkbox labeled "I acknowledge" and two buttons at the bottom: "OK" and "Cancel".

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

The screenshot shows the Fortigate GUI. The left sidebar navigation menu includes:

- Dashboard
- Network
- Policy & Objects
- Security Profiles
- VPN
- User & Authentication
- WiFi & Switch
 - Controller
 - Managed FortiAPs
 - WiFi Clients
 - WiFi Maps
- SSIDs
 - FortiAP Profiles
 - WIDS Profiles
 - WiFi Settings
- FortiLink Interface
- Managed FortiSwitches
- FortiSwitch Clients
- FortiSwitch VLANs
- FortiSwitch Ports
- FortiSwitch Port Policies
- NAC Policies
- System
- Security Fabric
- Log & Report

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

Additional Settings

Schedule always

Block intra-SSID traffic

Optional VLAN ID 0

Broadcast suppression

ARP for known clients	<input type="button" value="x"/>
DHCP unicast	<input type="button" value="x"/>
DHCP uplink	<input type="button" value="x"/>
<input type="button" value="+"/>	

Click ok

6. Now we want to create another one.

Click **Create new**

Create New SSID

Name: fortinet ssid 2

Alias:

Type: WiFi SSID

Traffic mode: Tunnel

Address

IP/Netmask: 192.168.2.100/27

Create address object matching subnet

Name: fortinet ssid 2 address

Destination: 192.168.2.96/27

Secondary IP address: (radio button)

Administrative Access

IPv4: HTTPS, FMG-Access, FTM, Speed Test, HTTP, SSH, RADIUS Accounting, PING, SNMP, Security Fabric Connection

DHCP Server

DHCP status: Enabled

Address range: 192.168.2.98-192.168.2.126

Netmask: 255.255.255.224

Default gateway: Same as Interface IP

DNS server: Same as System DNS

Lease time: 604800 seconds(s)

Advanced

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

WiFi Settings

SSID: fortinet SSID 2 ENT

Client limit: (radio button)

Broadcast SSID: (radio button)

Beacon advertising: Name, Model, Serial number

Security Mode Settings

Security mode: WPA2 Enterprise

Authentication: Local, RADIUS Server

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

Click the pencil of the Guest-group

Create New SSID

Lease time: 604800 second(s)

Advanced

Network

Device detection

WiFi Settings

SSID: fortinet SSID 2 ENT

Client limit

Broadcast SSID

Beacon advertising: Name, Model, Serial number

Security Mode Settings

Security mode: WPA2 Enterprise

Authentication: Local (selected), RADIUS Server

Select Entries

Search: Guest-group

Create

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

Edit User Group

Name: Guest-group

Type: Firewall

Members: guest

Select Entries

Search: guest

Create

OK Cancel

Select user.

Select Entries

Search

+ Create

CREATE NEW

+ PKI User

+ User

Click **Next** on this screen

Users/Groups Creation Wizard

① User Type > ② Login Credentials > ③ Contact Info > ④ Extra Info

Local User

- Remote RADIUS User
- Remote TACACS+ User
- Remote LDAP User
- FSSO
- FortiNAC User

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

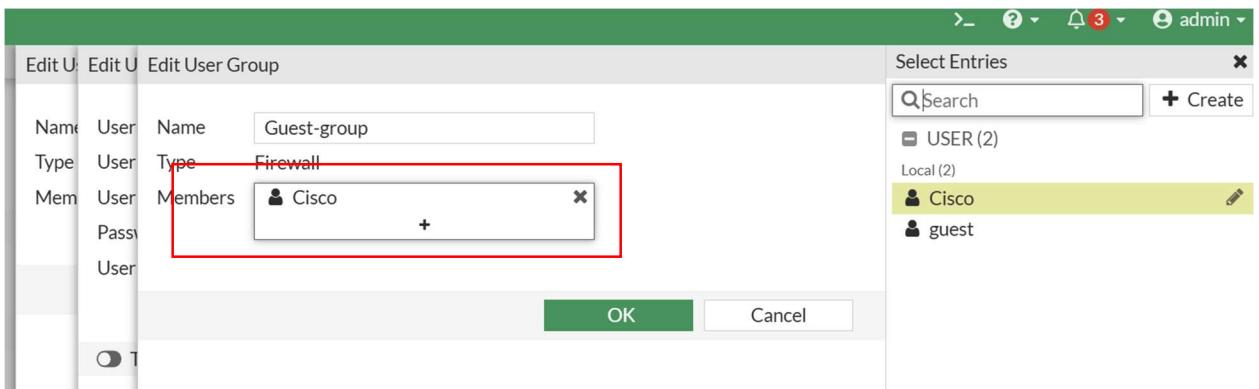
Users/Groups Creation Wizard

✓ ① User Type > ② Login Credentials > ③ Contact Info > ④ Extra Info

Username	Cisco
Password	*****

< Back **Next** Cancel

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

The screenshot shows the 'WiFi Settings' screen. Under 'Security Mode Settings', the 'Security mode' dropdown is set to 'WPA2 Enterprise' and the 'Authentication' dropdown is set to 'Local'. A red box highlights the 'Local' tab and the 'cisco' entry in the list below it. Other options in the 'Beacon advertising' section include checkboxes for 'Name', 'Model', and 'Serial number'.

Click ok

7. Go to Policy & object -> Firewall policy

Click create new

Configure as the following for the first one

FortiGate-40F

- Dashboard
- Network
- Policy & Objects**
 - Firewall Policy**
 - Addresses
 - Internet Service Database
 - Services
 - Schedules
 - Virtual IPs
 - IP Pools
 - Protocol Options
 - Traffic Shaping

New Policy

Name	1
Incoming Interface	wan
Outgoing Interface	fortinet ssid 1PSK (fortinet ssid 1)
Source	all
Destination	all
Schedule	always
Service	ALL
Action	<input checked="" type="button"/> ACCEPT <input type="button"/> DENY

For the second one do it as

New Policy

Name	2
Incoming Interface	fortinet ssid 1PSK (fortinet ssid 1)
Outgoing Interface	wan
Source	all
Destination	all
Schedule	always
Service	ALL
Action	<input checked="" type="button"/> ACCEPT <input type="button"/> DENY

Firewall/Network Options

NAT

IP Pool Configuration Use Outgoing Interface Address Use Dynamic IP Pool

Preserve Source Port

Protocol Options PRO default

Security Profiles

AntiVirus

Web Filter

DNS Filter

Application Control

IPS

SSL Inspection SSL no-inspection

Logging Options

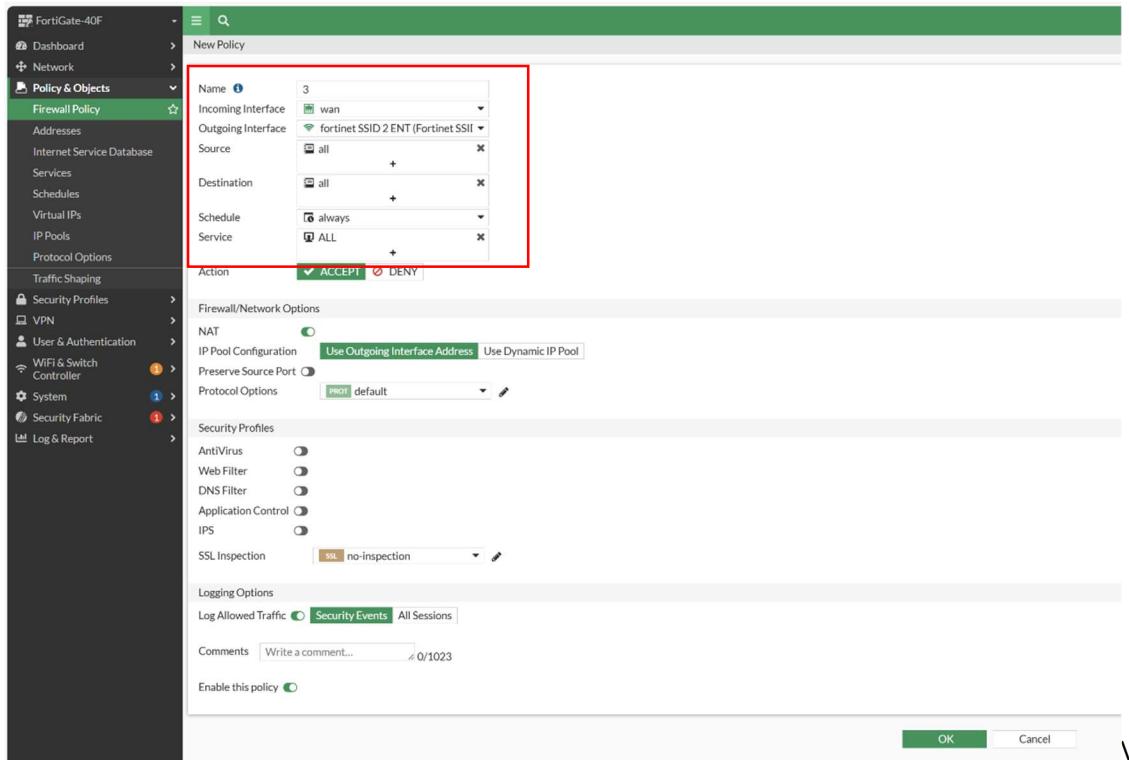
Log Allowed Traffic Security Events: All Sessions

Comments Write a comment... 0/1023

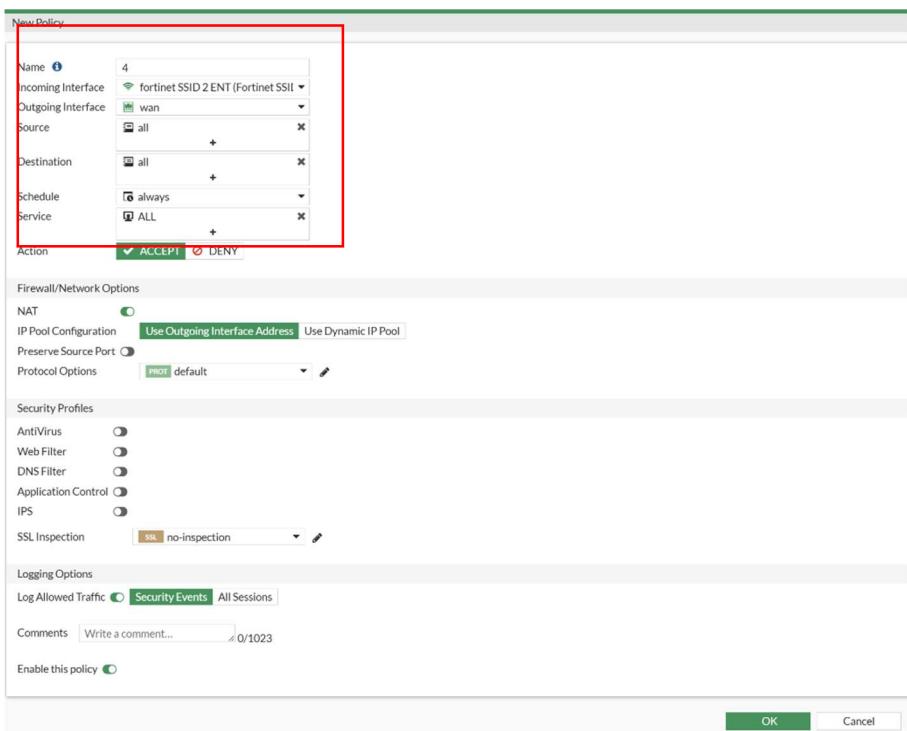
Enable this policy

OK Cancel

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**

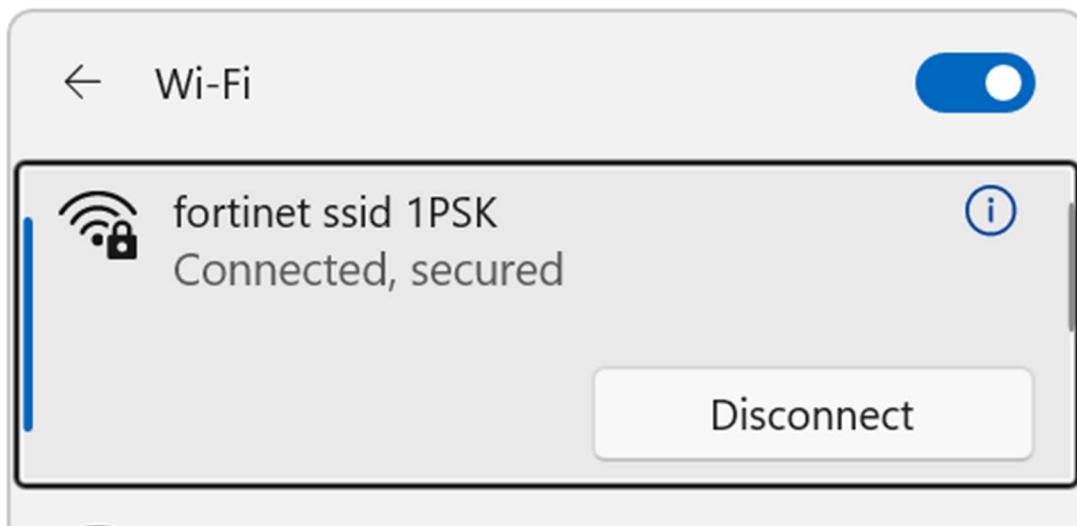
Right click on the ap and press authorize

The screenshot shows the FortiGate-40F management interface. In the left sidebar, under 'WiFi & Switch Controller', 'Managed FortiAPs' is selected. A single access point, 'FP221E5520091745', is listed with a status of 'Unauthorized'. A context menu is open over this entry, with the 'Authorize' option highlighted. Other options in the menu include 'Edit', 'Delete', 'Upgrade', 'Reset', 'Register', 'Assign Profile', 'Diagnostics and Tools', and 'Show in WiFi Maps'.

Now we will wait for it to go online

The screenshot shows the same FortiGate-40F management interface after the access point has been authorized. The status of the access point 'FP221E5520091745' is now 'Online'. The overall status summary indicates '1 Total' access points are online, and the '2.4 GHz Radio Channel Utilization' is 'Good'.

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.

The screenshot shows the FortiGate 40F configuration interface under the 'SSL-VPN Settings' tab. Key configuration details include:

- Connection Settings:** SSL-VPN is enabled, and it is listening on the **wan** interface at port **4443**. A tooltip indicates "Web mode access will be listening at https://192.168.40.13:4443".
- Server Certificate:** A default certificate named **Fortinet_Factory** is selected. A warning message states: "You are using a default built-in certificate, which will not be able to verify your server's domain name (your users will see a warning). Let's Encrypt can be used to easily generate a trusted certificate if you do not have one." It includes a "Create Certificate" button.
- Restrictions:** "Allow access from any host" is selected for Redirect HTTP to SSL-VPN.
- Tunnel Mode Client Settings:** Address Range is set to "Automatically assign addresses" (highlighted with a red box), specifying IP ranges from 10.212.134.200 to 10.212.134.210. Tunnel users will receive IPs in this range.
- DNS Server:** Set to "Same as client system DNS" (highlighted with a red box).
- Web Mode Settings:** Language is set to "Browser preference".
- Authentication/Portal Mapping:** This section maps users/groups to portals:

Users/Groups	Portal
cisco	tunnel-access
cisco	tunnel-access
Cisco	tunnel-access
All Other Users/Groups	web-access

An **Apply** button is located at the bottom right of the configuration pane.

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.

Edit Policy

Name: SSL VPN > LAN Access

Incoming Interface: SSL-VPN tunnel interface (ssl.root)

Outgoing Interface: lan

Source: all, Cisco, cisco, cisco

Destination: lan

Schedule: always

Service: ALL

Action: ✓ ACCEPT

Firewall/Network Options

NAT: OFF

Protocol Options: PROT default

Security Profiles

- AntiVirus: ON
- Web Filter: ON
- DNS Filter: ON
- Application Control: ON
- IPS: ON

SSL Inspection: ssl no-inspection

Logging Options

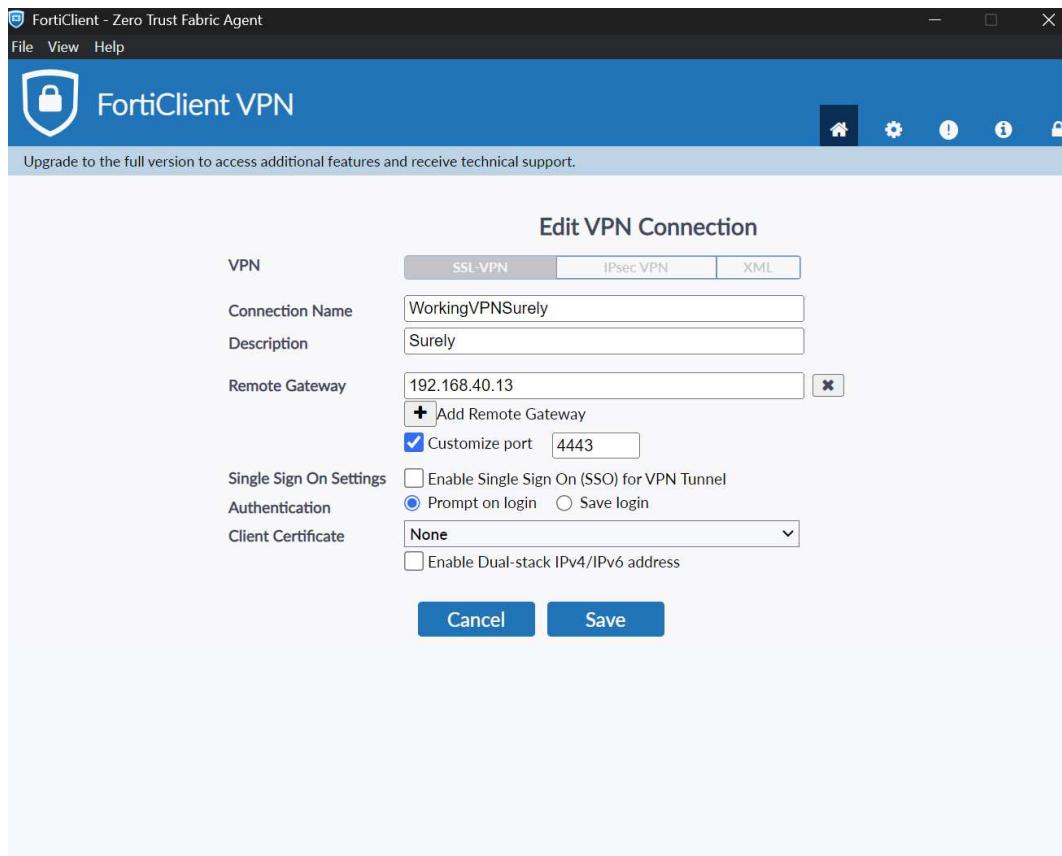
Log Allowed Traffic: Security Events (All Sessions)

Comments: Write a comment... 0/1023

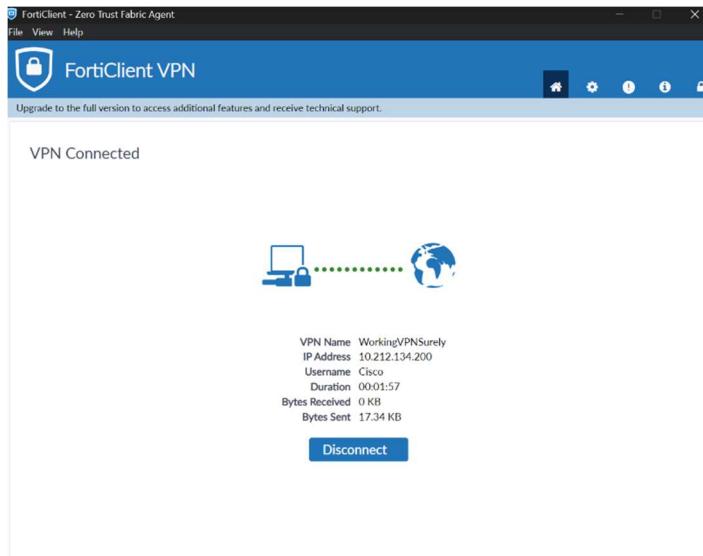
Enable this policy: ON

OK **Cancel**

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.

Edit Address

Name	RyanCalvin_remote
Color	<input type="button" value="Change"/>
Type	Subnet
IP/Netmask	192.168.1.0 255.255.255.0
Interface	<input type="checkbox"/> any
Static route configuration	<input checked="" type="radio"/>
Comments	Write a comment... 0/255

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

The screenshot shows the FortiGate-40F interface with the 'IPsec Tunnels' tab selected. On the left, there's a navigation tree with 'VPN' expanded, showing 'Site-to-Site', 'IKEv2', and 'IKEv1'. The main pane displays a table of existing tunnels:

Tunnel	Interface Binding	Status	Ref.
RyanAndrew	wan	Inactive	3
RyanFinn	wan	Inactive	3
RyanthanVPN	wan	Inactive	3
RyanCalvin	wan	Up	4
Dialup-FortiClient (Windows, Mac OS, Android)	wan	Inactive	2
RyanEthanVPN2	wan	Inactive	

A red box highlights the 'Create New' button in the top-left corner of the tunnel list area.

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.

Edit VPN Tunnel

Name	RyanCalvin		
Comments	Comments 0/255		
Network			
Remote Gateway : Static IP Address (192.168.40.191) , Interface : wan			
Authentication			
Authentication Method : Pre-shared Key			
IKE Version : 1, Mode : Main (ID protection)			
Phase 1 Proposal			
Algorithms : AES128-SHA256, AES256-SHA256, AES128-SHA1, AES256-SHA1			
Diffie-Hellman Groups : 14, 5			
XAUTH			
Type : Disabled			
Phase 2 Selectors			
Name	Local Address	Remote Address	Add
RyanCalvin	192.168.3.0/255.255.255.0	192.168.1.0/255.255.255.0	<input type="button" value="Add"/>

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

The screenshot shows the FortiGate 40F interface under the Policy & Objects section. The Firewall Policy tab is selected. A red box highlights the '+ Create New' button at the top left of the main content area. Below it is a table listing several existing firewall policies, each with columns for Name, Source, and Destination.

Name	Source	Destination
Ian → RyanAndrew	all	RyanAndrew
vpn_RyanAndrew_local_0	all	
Ian → RyanCalvin	RyanCalvin	RyanCalvin_local
Ian → wan	all	wan
RyanCalvin → Ian	RyanCalvin_remote	RyanCalvin
RyanEthanEnterprise (Fortinet SSID 2) → Ian	RyanEthanEnterprise (Fortinet SSID 2)	Ian

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.

The screenshot shows the 'Edit Policy' dialog box. The 'Name' field is set to 'RyanCalvinRemote'. The 'Incoming Interface' is 'Ian' and the 'Outgoing Interface' is 'RyanCalvin'. The 'Source' is 'RyanCalvin_remote' and the 'Destination' is 'RyanCalvin_local'. Under 'Action', 'ACCEPT' is selected. In the 'Firewall/Network Options' section, 'NAT' is enabled. The 'Protocol Options' dropdown is set to 'PROXY default'. A red box highlights the 'Enable this policy' checkbox at the bottom left of the dialog.

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.

