Palo Alto PA-220 SOHO Network Configuration

Andrew Pai

10/1/2024

Purpose:

The purpose of this lab was to configure our Palo Alto PA-220 firewall to be suitable for a small office home office (SOHO) network. Now that our firewall has been factory reset, we need to make sure that its configuration is able to effectively protect a network. This SOHO configuration includes setting security zones, interfaces, VLANs, DHCP, and DNS.

Background Information:

A Small Office Home Office (SOHO) network is a basic network meant for individuals or small businesses to use. Typically, the range of individuals connected is anywhere from 1 to 10, and usage of a SOHO network allows for the centralization of resources or ability to connect to a corporate network. Because they aren’t as big and aren’t as complex as other networks, SOHO networks are the easiest to set up and use. SOHO networks are also referred to as “virtual offices” and essentially encompass a local area network (LAN) which can get access to a larger network.

Since we want to ensure that our SOHO networks are secure and that there is no malicious activity being transmitted onto our network, the configuration of the Palo Alto PA-220 firewall is critical to making sure that our network runs as intended. In order to configure the Palo Alto PA-220 firewall our group entered the GUI, or graphical user interface. On the GUI, we configured various things such as security zones, interface settings, VLANs, DHCP, and DNS.

Security zones on a firewall consist of various physical or virtual interfaces grouped together to be controlled as a cluster by the firewall. Security zones allow for the firewall to better manage multiple interfaces at once. For each security zone, there are different security policy rules that determine what the firewall does with different types of packets. While packets and traffic can move around unhindered inside of a security zone, the point of a security zone is to check the traffic between various zones to maintain network integrity.

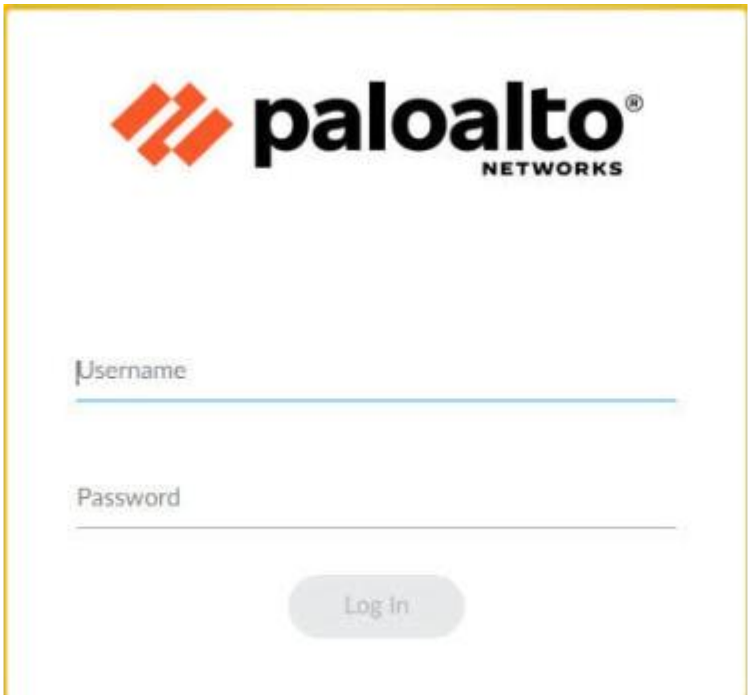
Firewall interfaces are areas of the firewall that transmit and receive data. In a SOHO configuration, it is important to configure the interface type to determine what type of data it can receive/transmit and the security zone to group the interface with other interfaces that it can trust.

Virtual Local Area Networks (VLANs) are similar to security zones in the way that they group together various interfaces on the firewall. This makes it much more efficient and organized to divide up sections of the firewall and make it so that traffic that should be separated actually is separated. Without security zones and VLANs, the job of one firewall might have to be relegated to multiple firewalls as they would no longer be able to compartmentalize.

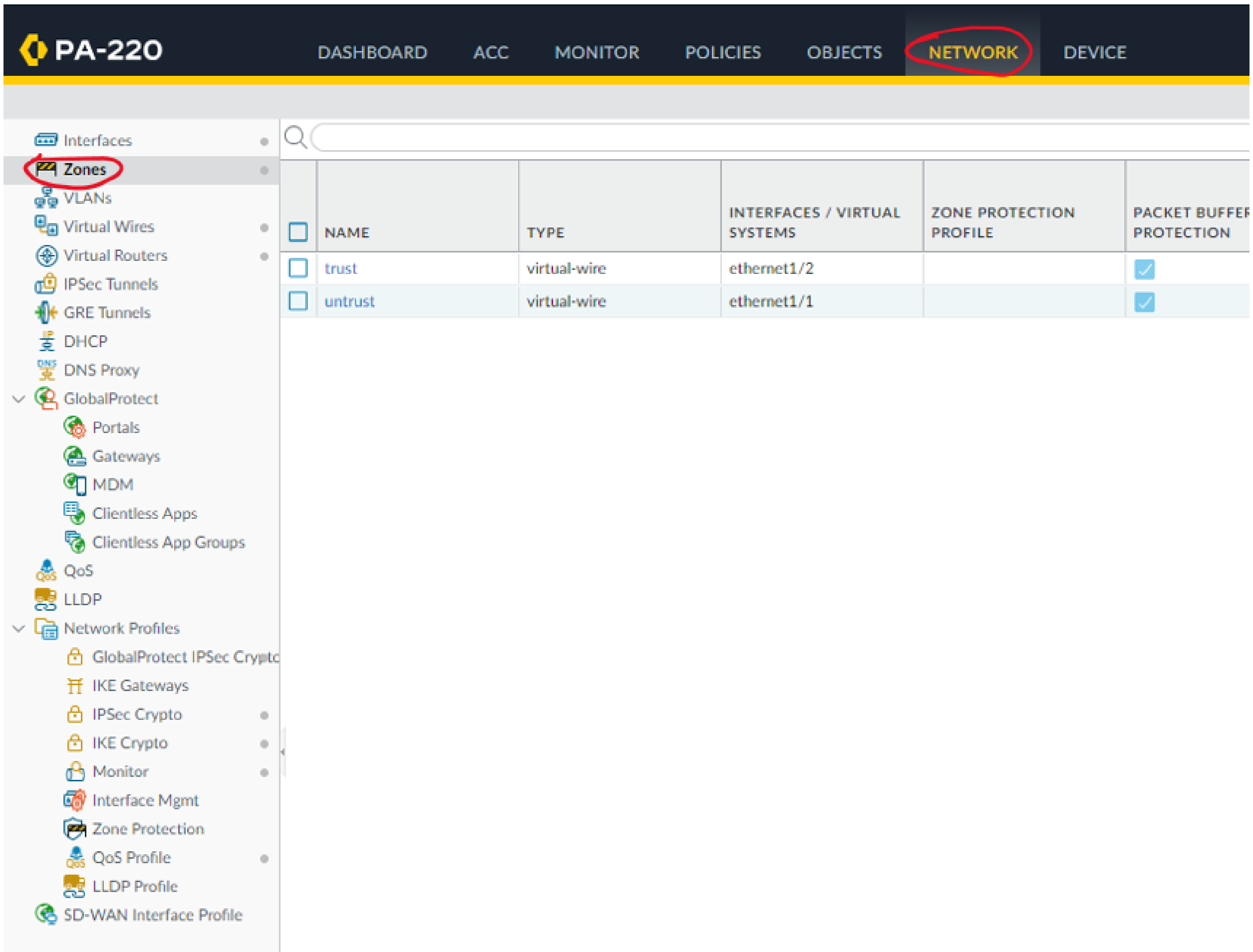
Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) are crucial parts of the firewall configuration that come into play for the host computers trying to access networks outside of the SOHO. DHCP is in charge of relegating IP addresses to hosts that need them, allowing traffic to go in and out of hosts. DNS turns domain names into IP addresses, allowing for hosts to successfully transmit and receive traffic from websites online.

Lab Summary:

Enter the PA-220's Graphical User Interface (GUI) by inputting the IP address 192.168.1.1 in a web browser. Make sure that the host computer is on the firewall's subnet by setting its IP to something like 192.168.1.2. Enter the login information for the firewall to the box below.

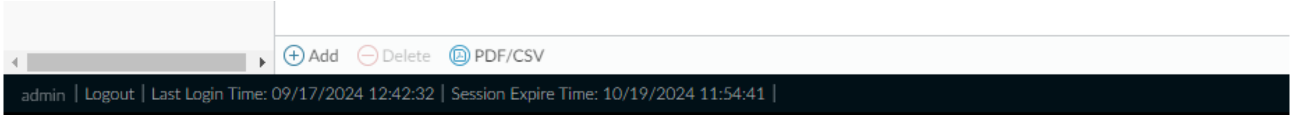


In order to add security zones to the PA-220, first navigate to “Network” on the top taskbar and then to “Zones” on the left taskbar.



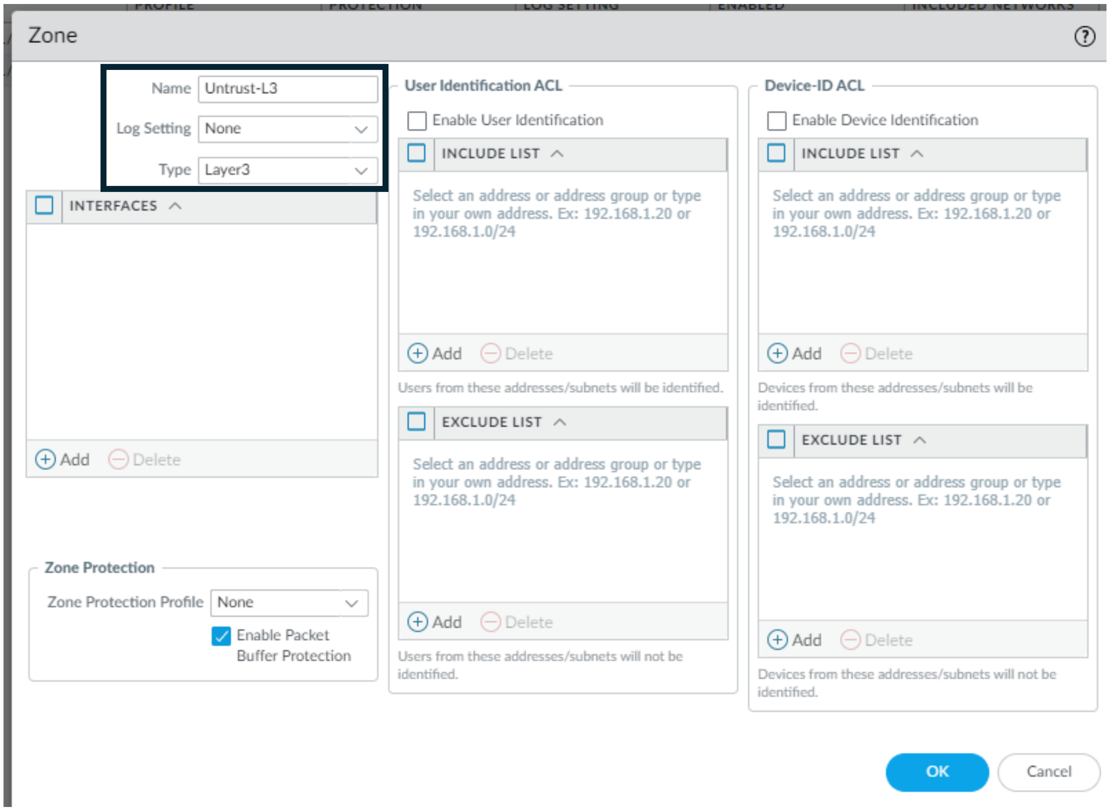
□	NAME	TYPE	INTERFACES / VIRTUAL SYSTEMS	ZONE PROTECTION PROFILE	PACKET BUFFER PROTECTION
□	trust	virtual-wire	ethernet1/2		☑
□	untrust	virtual-wire	ethernet1/1		☑

Click “Add” on the very bottom left taskbar in order to add a new zone.



admin | Logout | Last Login Time: 09/17/2024 12:42:32 | Session Expire Time: 10/19/2024 11:54:41 |

Name the new zone “Untrust-L3” and change the type to “Layer3”. Leave all other settings in the zone untouched. Repeat this process to create a zone named “Trust-L3” that has a “Layer3” type as well as a zone named “Trust-L2” that has a “Layer2” type.



Zone

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

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

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

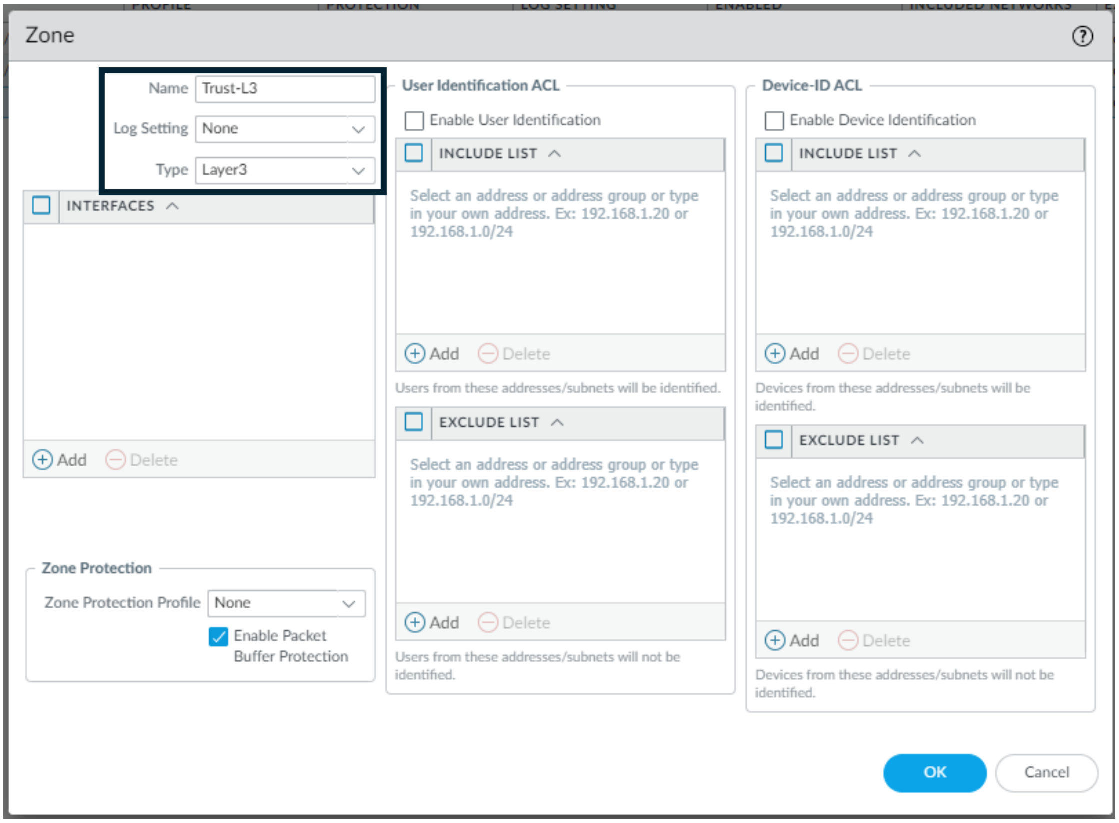
Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24

Devices from these addresses/subnets will be identified.

□ EXCLUDE LIST

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.



Zone

Name: Trust-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

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

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

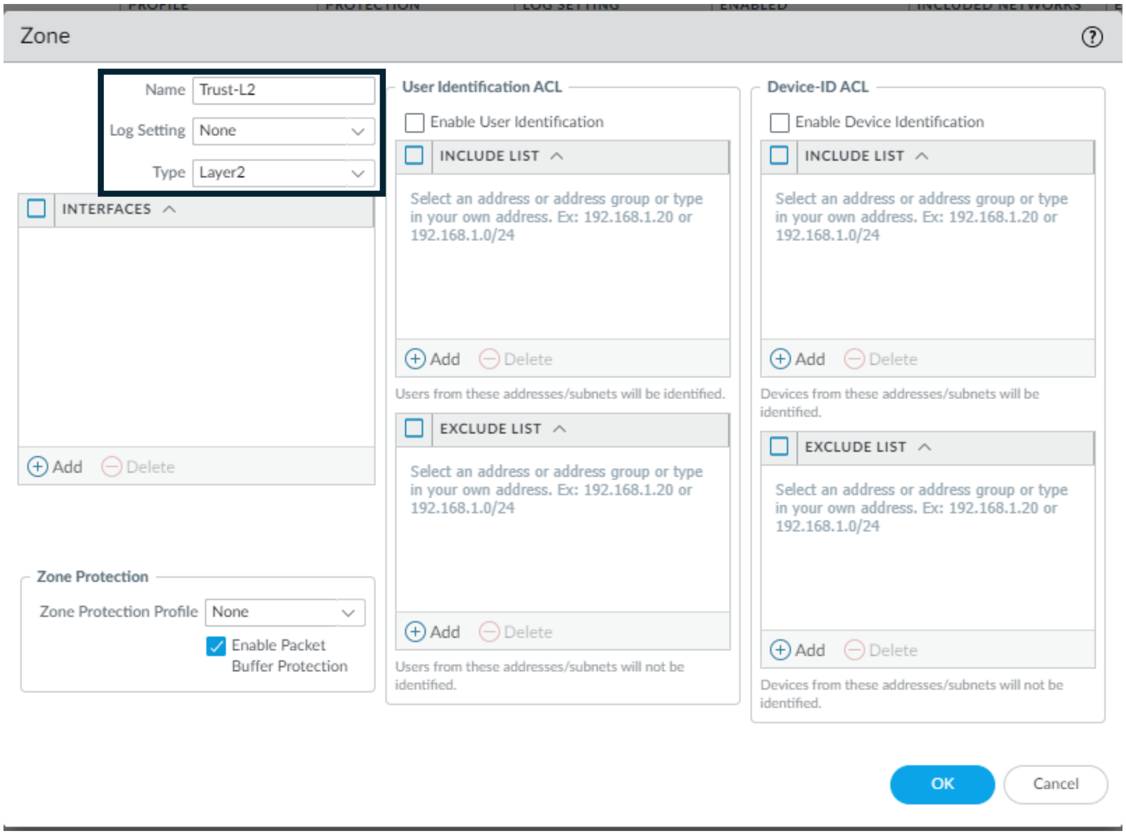
Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24

Devices from these addresses/subnets will be identified.

□ EXCLUDE LIST

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.



Name: Trust-L2

Log Setting: None

Type: Layer2

Zone Protection

Zone Protection Profile: None

☑ Enable Packet Buffer Protection

User Identification ACL

□ Enable User Identification

□ INCLUDE LIST

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

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

Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24

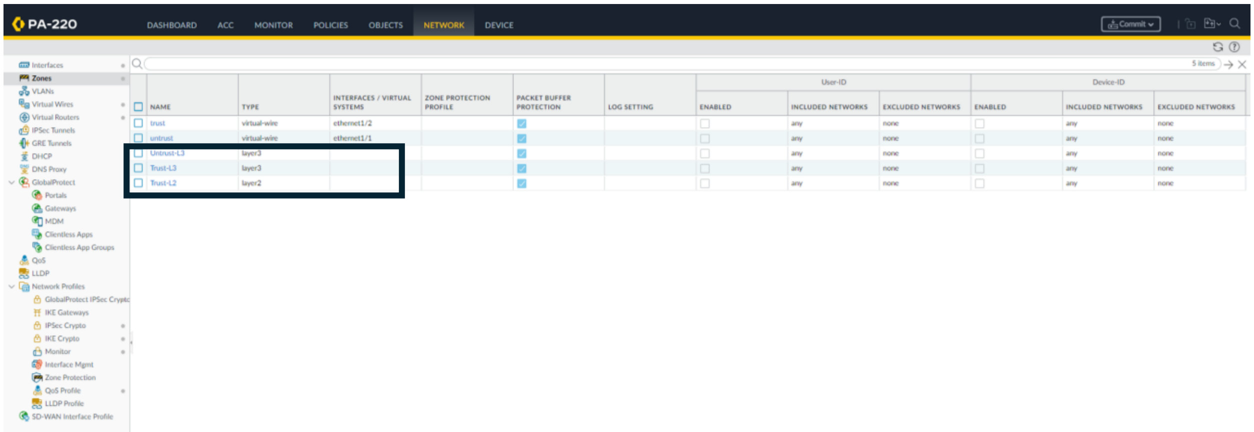
Devices from these addresses/subnets will be identified.

□ EXCLUDE LIST

Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24

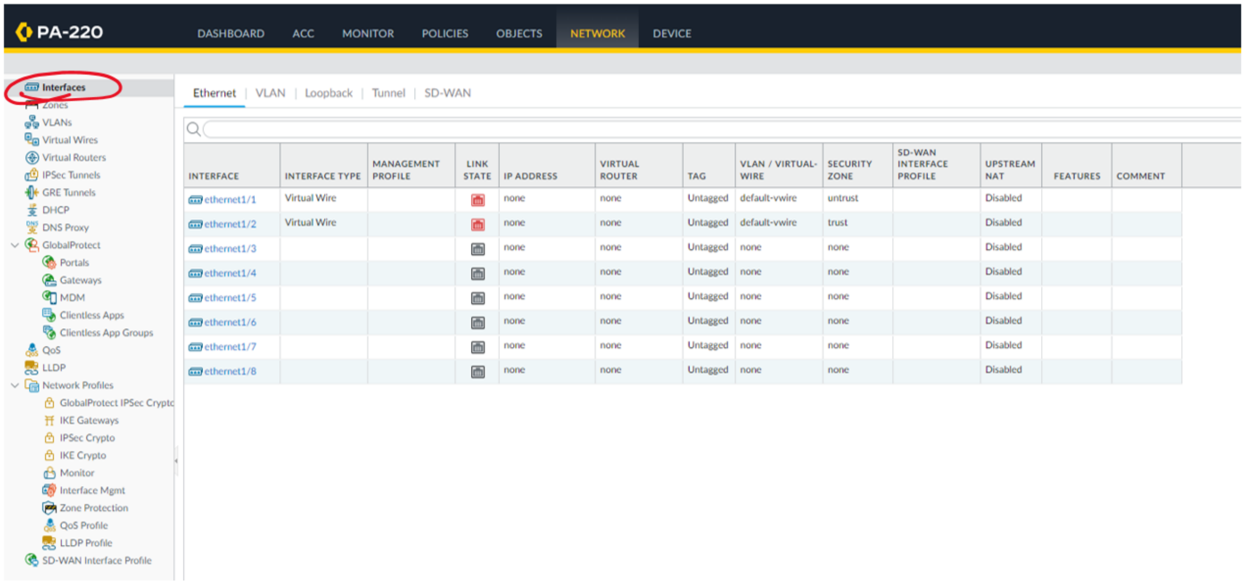
Devices from these addresses/subnets will not be identified.

When you finish inputting the three zones, your Zones under Network should look like the picture below.



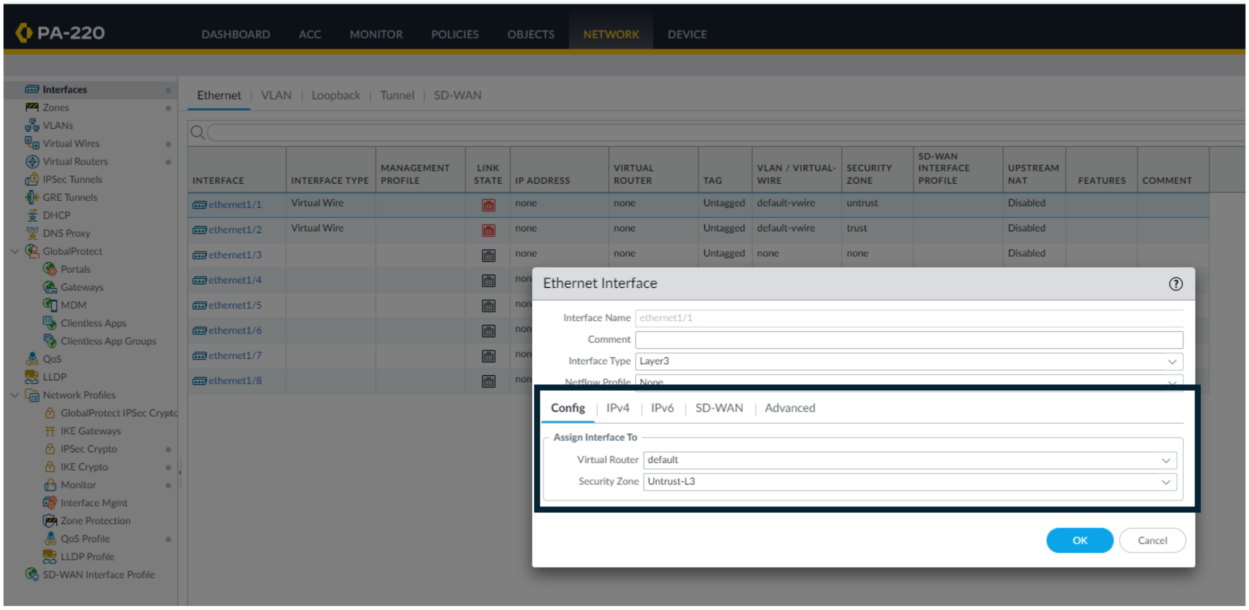
							User-ID			Device-ID		
□	NAME	TYPE	INTERFACES / VIRTUAL SYSTEMS	ZONE PROTECTION PROFILE	PACKET BUFFER PROTECTION	LOG SETTING	ENABLED	INCLUDED NETWORKS	EXCLUDED NETWORKS	ENABLED	INCLUDED NETWORKS	EXCLUDED NETWORKS
□	trust	virtual-wire	ethernet1/2		☑		□	any	none	□	any	none
□	untrust	virtual-wire	ethernet1/1		☑		□	any	none	□	any	none
□	Untrust-L3	layer3			☑		□	any	none	□	any	none
□	Trust-L3	layer3			☑		□	any	none	□	any	none
□	Trust-L2	layer2			☑		□	any	none	□	any	none

From the Network tab, enter the “Interfaces” section from the left taskbar.



INTERFACE	INTERFACE TYPE	MANAGEMENT PROFILE	LINK STATE	IP ADDRESS	VIRTUAL ROUTER	TAG	VLAN / VIRTUAL-WIRE	SECURITY ZONE	SD-WAN INTERFACE PROFILE	UPSTREAM NAT	FEATURES	COMMENT
ethernet1/1	Virtual Wire		🟥	none	none	Untagged	default-vwire	untrust		Disabled		
ethernet1/2	Virtual Wire		🟥	none	none	Untagged	default-vwire	trust		Disabled		
ethernet1/3			▨	none	none	Untagged	none	none		Disabled		
ethernet1/4			▨	none	none	Untagged	none	none		Disabled		
ethernet1/5			▨	none	none	Untagged	none	none		Disabled		
ethernet1/6			▨	none	none	Untagged	none	none		Disabled		
ethernet1/7			▨	none	none	Untagged	none	none		Disabled		
ethernet1/8			▨	none	none	Untagged	none	none		Disabled		

Select the interface ethernet1/1, set the virtual router to "default" and the security zone to "Untrust-L3."


PA-220
DASHBOARD
ACC
MONITOR
POLICIES
OBJECTS
NETWORK
DEVICE
Ethernet | VLAN | Loopback | Tunnel | SD-WAN
Config | IPv4 | IPv6 | SD-WAN | Advanced
OK
Cancel

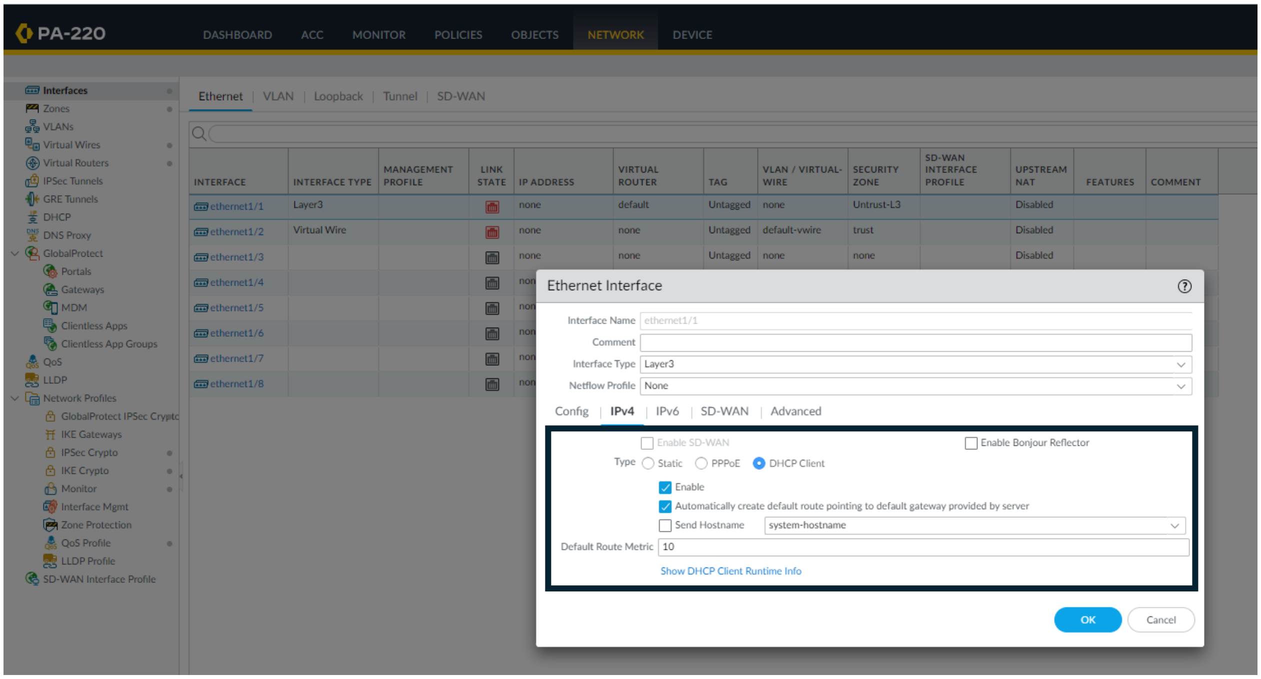
Ethernet Interface

Interface Name	ethernet1/1
Comment	
Interface Type	Layer3
Netflow Profile	None

Assign Interface To

Virtual Router	default
Security Zone	Untrust-L3

Click the "IPv4" option in the Ethernet Interface and click on "DHCP Client" as the type. Make sure that both "Enable" and the default route are on.



INTERFACE	INTERFACE TYPE	MANAGEMENT PROFILE	LINK STATE	IP ADDRESS	VIRTUAL ROUTER	TAG	VLAN / VIRTUAL-WIRE	SECURITY ZONE	SD-WAN INTERFACE PROFILE	UPSTREAM NAT	FEATURES	COMMENT
ethernet1/1	Layer3			none	default	Untagged	none	Untrust-L3		Disabled		
ethernet1/2	Virtual Wire			none	none	Untagged	default-vwire	trust		Disabled		
ethernet1/3				none	none	Untagged	none	none		Disabled		
ethernet1/4				non								
ethernet1/5				non								
ethernet1/6				non								
ethernet1/7				non								
ethernet1/8				non								

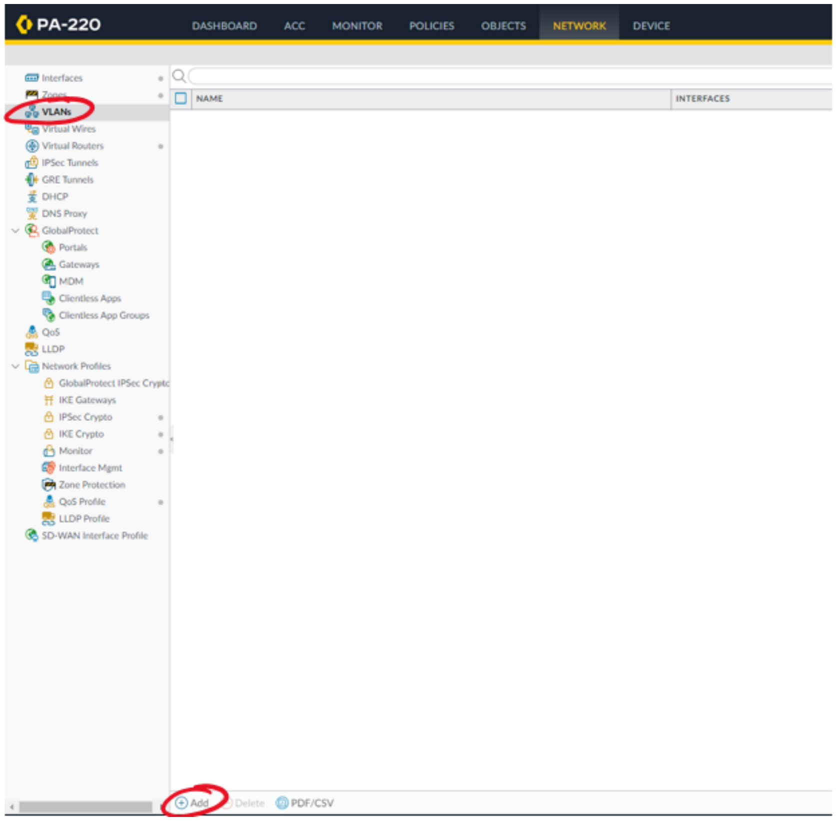
Ethernet Interface

Interface Name: ethernet1/1
Comment:
Interface Type: Layer3
Netflow Profile: None

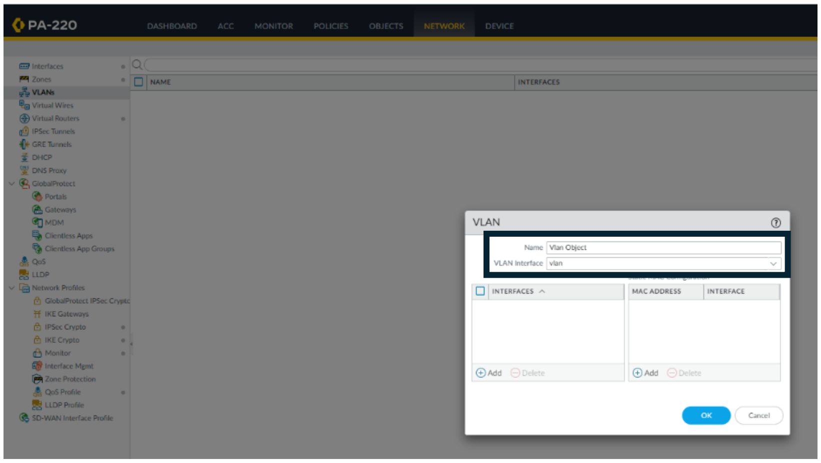
Config | IPv4 | IPv6 | SD-WAN | Advanced

□ Enable SD-WAN
□ Enable Bonjour Reflector
Type ○ Static ○ PPPoE ● DHCP Client
☑ 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

Once done with the first interface, go to the “VLANs” section under Network and add a new VLAN.



Name your VLAN object and select “vlan” for VLAN interface.

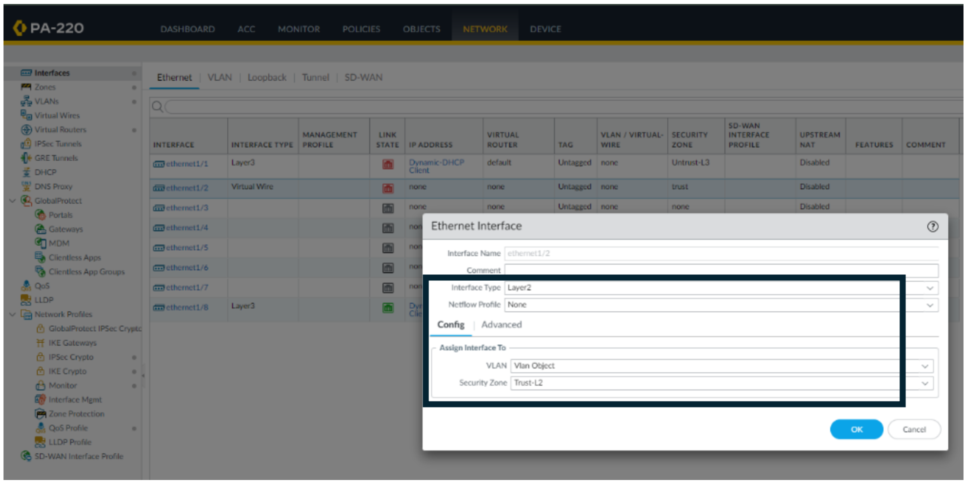


VLAN

Name: Vlan Object

VLAN Interface: vlan

Go back to “Interfaces” and “Ethernet” and enter the interface “ethernet1/2”. Set the interface type to Layer 2, the netflow profile to none, VLAN to the name of your previously made vlan, and security zone to “Trust-L2”.



Ethernet Interface

Interface Name: ethernet1/2

Interface Type: Layer2

Netflow Profile: None

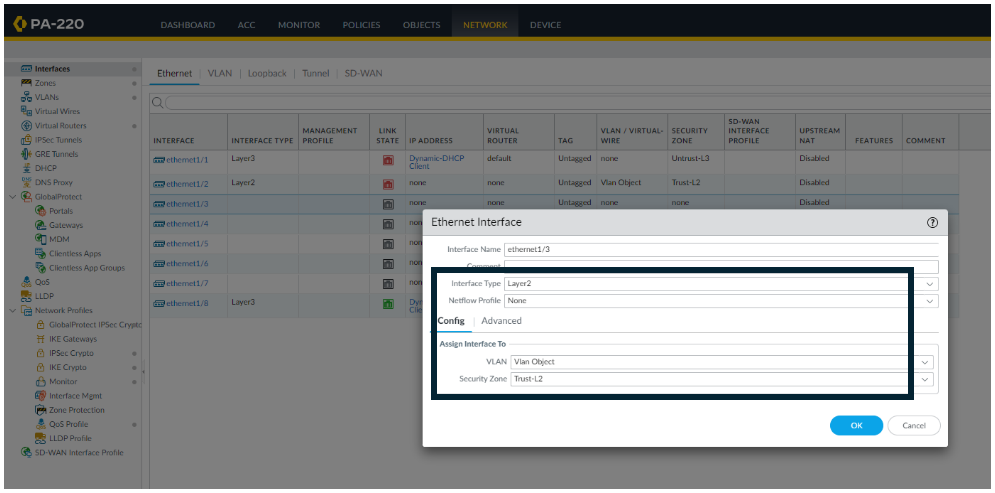
Config | Advanced

Assign Interface To

VLAN: Vlan Object

Security Zone: Trust-L2

Repeat the steps above for “ethernet1/3” and “ethernet1/4”



Ethernet Interface

Interface Name: ethernet1/3

Interface Type: Layer2

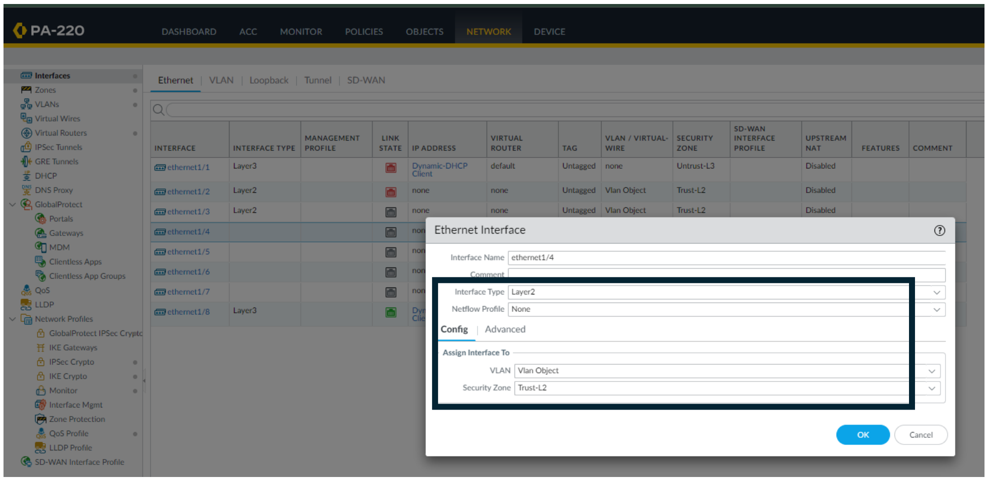
Netflow Profile: None

Config | Advanced

Assign Interface To

VLAN: Vlan Object

Security Zone: Trust-L2

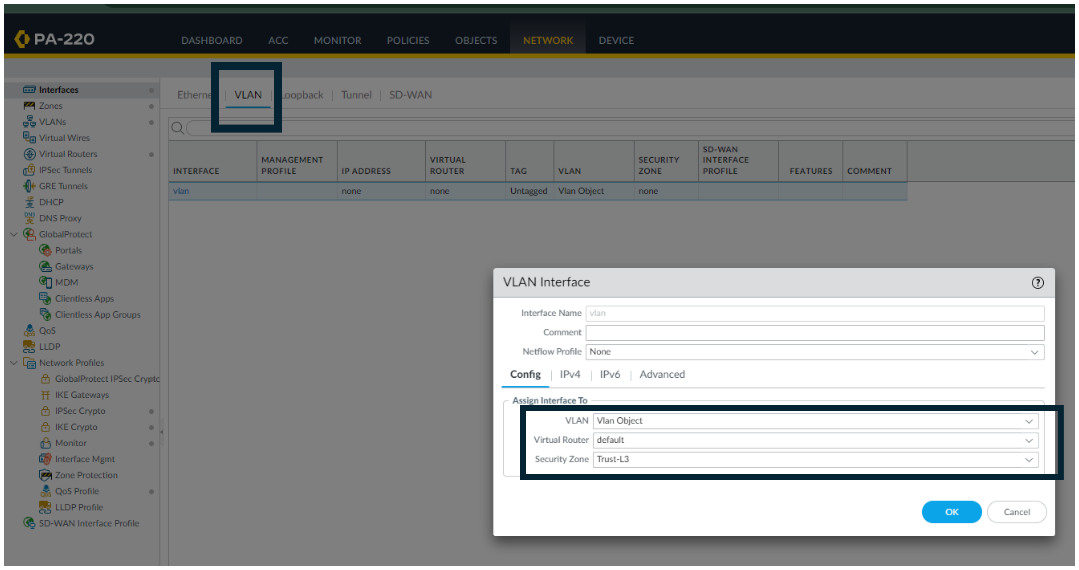


INTERFACE	INTERFACE TYPE	MANAGEMENT PROFILE	LINK STATE	IP ADDRESS	VIRTUAL ROUTER	TAG	VLAN / VIRTUAL-WIRE	SECURITY ZONE	SD-WAN INTERFACE PROFILE	UPSTREAM NAT	FEATURES	COMMENT
ethernet1/1	Layer3			Dynamic-DHCP Client	default	Untagged	none	Untrust-L3		Disabled		
ethernet1/2	Layer2			none	none	Untagged	Vlan Object	Trust-L2		Disabled		
ethernet1/3	Layer2			none	none	Untagged	Vlan Object	Trust-L2		Disabled		
ethernet1/4				non								
ethernet1/5				non								
ethernet1/6				non								
ethernet1/7				non								
ethernet1/8	Layer3			Dyn Clie								

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

In the Network and Interfaces tab, click the subsection VLAN that's next to the Ethernet button. Set VLAN to the name of your VLAN object, Virtual Router to default, and security zone to "Trust-L3".

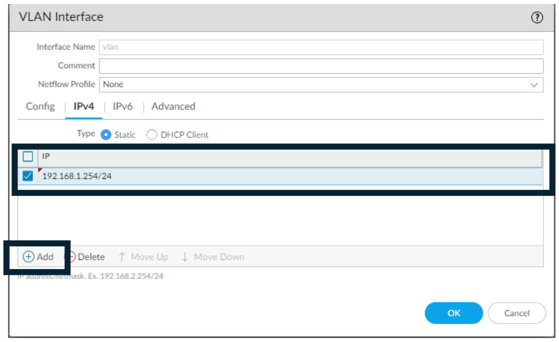


INTERFACE	MANAGEMENT PROFILE	IP ADDRESS	VIRTUAL ROUTER	TAG	VLAN	SECURITY ZONE	SD-WAN INTERFACE PROFILE	FEATURES	COMMENT
vlan		none	none	Untagged	Vlan Object	none			

VLAN Interface

Interface Name: vlan
Comment:
Netflow Profile: None
Config | IPv4 | IPv6 | Advanced
Assign Interface To
VLAN: Vlan Object
Virtual Router: default
Security Zone: Trust-L3

Under the same VLAN Interface, click on the IPv4 section and add an IP address of 192.168.1.254/24.



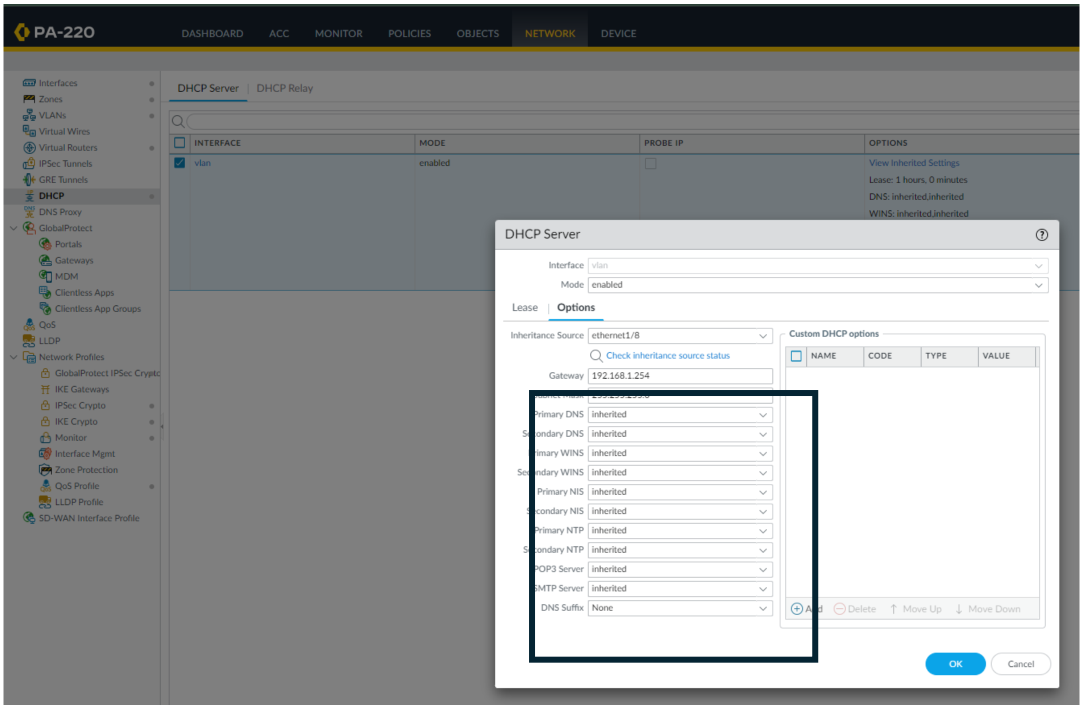
VLAN Interface

Interface Name: vlan
Comment:
Netflow Profile: None
Config | IPv4 | IPv6 | Advanced
Type ● Static ○ DHCP Client

□	IP
☑	192.168.1.254/24

IP address/netmask. Ex. 192.168.2.254/24

Staying under “Network”, navigate to the DHCP and DHCP server section of the GUI. Add a DHCP server and set interface to “vlan” and mode to “enabled”. IP Pool should be 192.168.1.2-252, with gateway 192.168.1.254 and subnet 255.255.255.0. The rest of the settings should be automatically inherited or set to “none”.



☐	INTERFACE	MODE	PROBE IP	OPTIONS
☑	vlan	enabled	☐	View Inherited Settings Lease: 1 hours, 0 minutes DNS: inherited,inherited WINS: inherited,inherited

DHCP Server

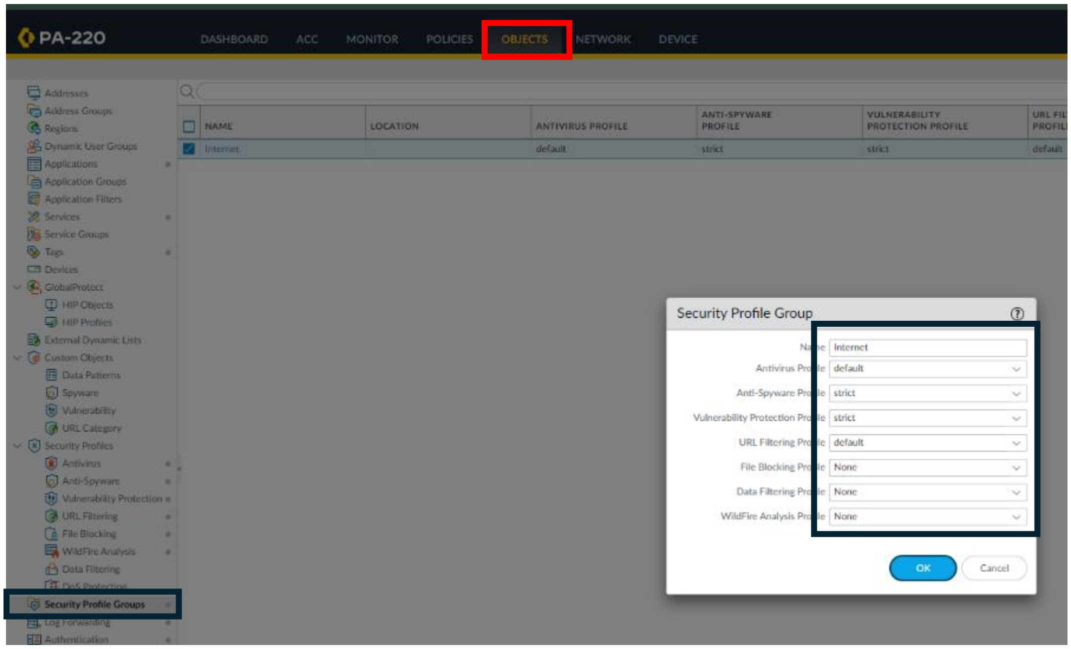
Interface: vlan
Mode: enabled

Inheritance Source: ethernet1/8
Gateway: 192.168.1.254
Primary DNS: inherited
Secondary DNS: inherited
Primary WINS: inherited
Secondary WINS: inherited
Primary NIS: inherited
Secondary NIS: inherited
Primary NTP: inherited
Secondary NTP: inherited
POP3 Server: inherited
SMTP Server: inherited
DNS Suffix: None

Custom DHCP options

☐	NAME	CODE	TYPE	VALUE

Go to the “Objects” section on the top taskbar and then “Security Profile Groups”. Add a new group and configure the settings as below.

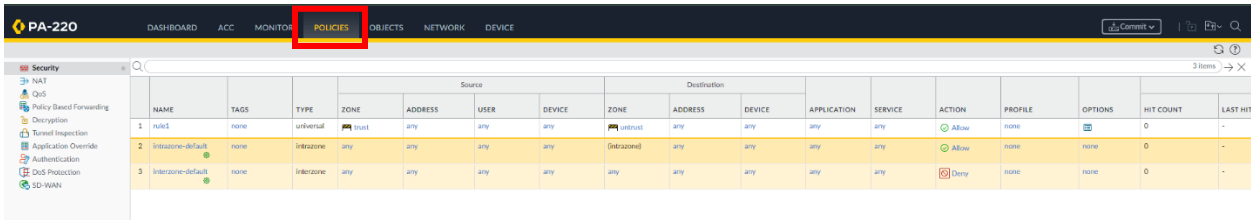


☐	NAME	LOCATION	ANTIVIRUS PROFILE	ANTI-SPYWARE PROFILE	VULNERABILITY PROTECTION PROFILE	URL FIL PROFIL
☑	Internet		default	strict	strict	default

Security Profile Group

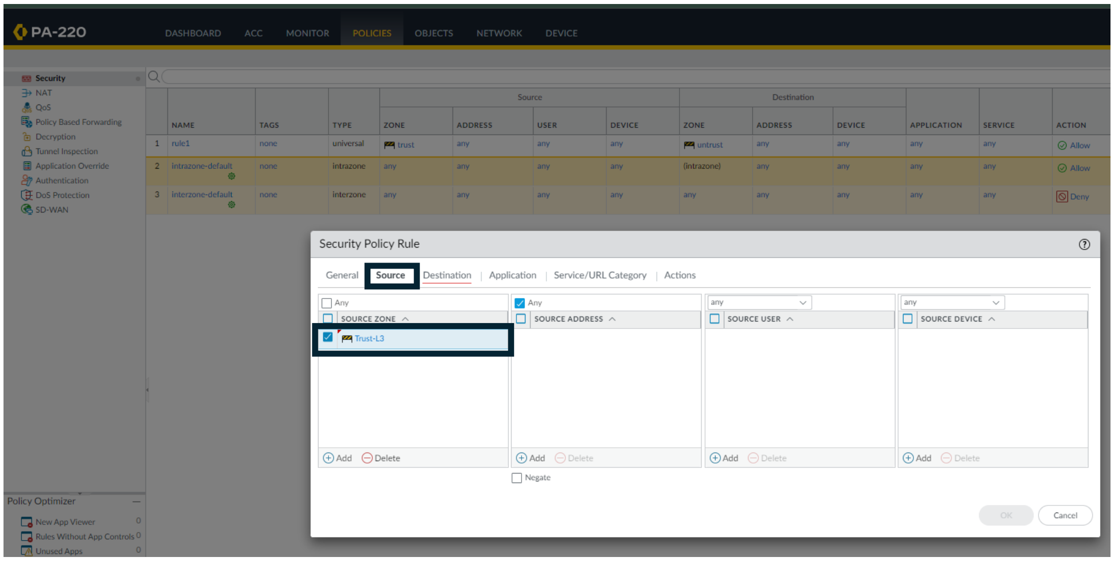
Name: Internet
Antivirus Profile: default
Anti-Spyware Profile: strict
Vulnerability Protection Profile: strict
URL Filtering Profile: default
File Blocking Profile: None
Data Filtering Profile: None
WildFire Analysis Profile: None

Navigate to the “Policies” section on the top of the dashboard and then to Security on the left taskbar.



				Source				Destination								
	NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS	HIT COUNT	LAST HIT
1	rule1	none	universal	trust	any	any	any	untrust	any	any	any	any	Allow	none		0	-
2	intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any	any	any	Allow	none	none	0	-
3	interzone-default	none	interzone	any	any	any	any	any	any	any	any	any	Deny	none	none	0	-

Add a new security policy rule and name it “Internet Outgoing” with description “All traffic to the internet”. Under the Source section, add the source zone to be “Trust-L3”.



□ Any — SOURCE ZONE: ☑ Trust-L3

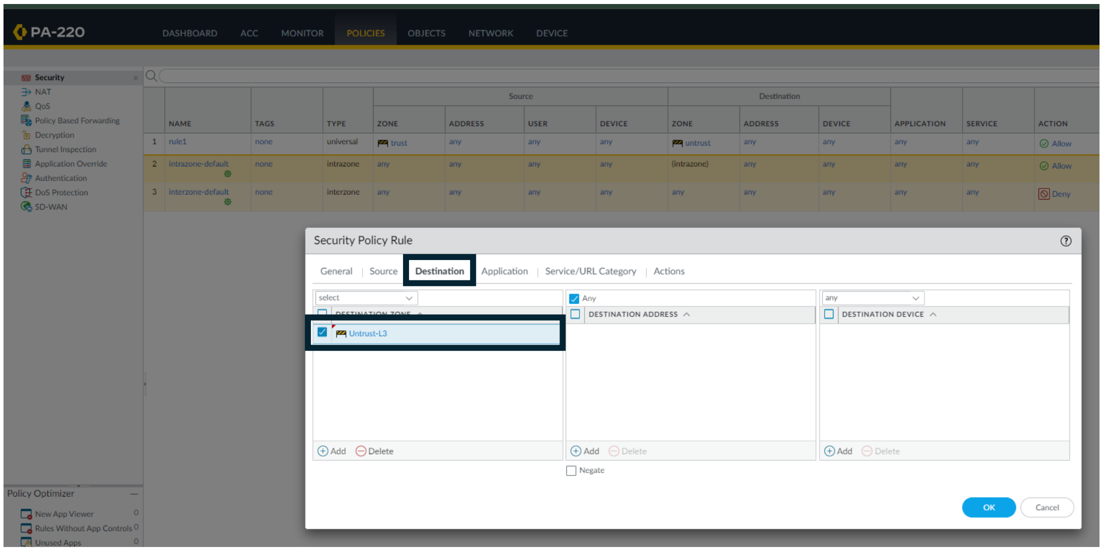
☑ Any — SOURCE ADDRESS

any — SOURCE USER

any — SOURCE DEVICE

□ Negate

Navigate to the Destination zone and add the zone “Untrust-L3”.



select — DESTINATION ZONE: ☑ Untrust-L3

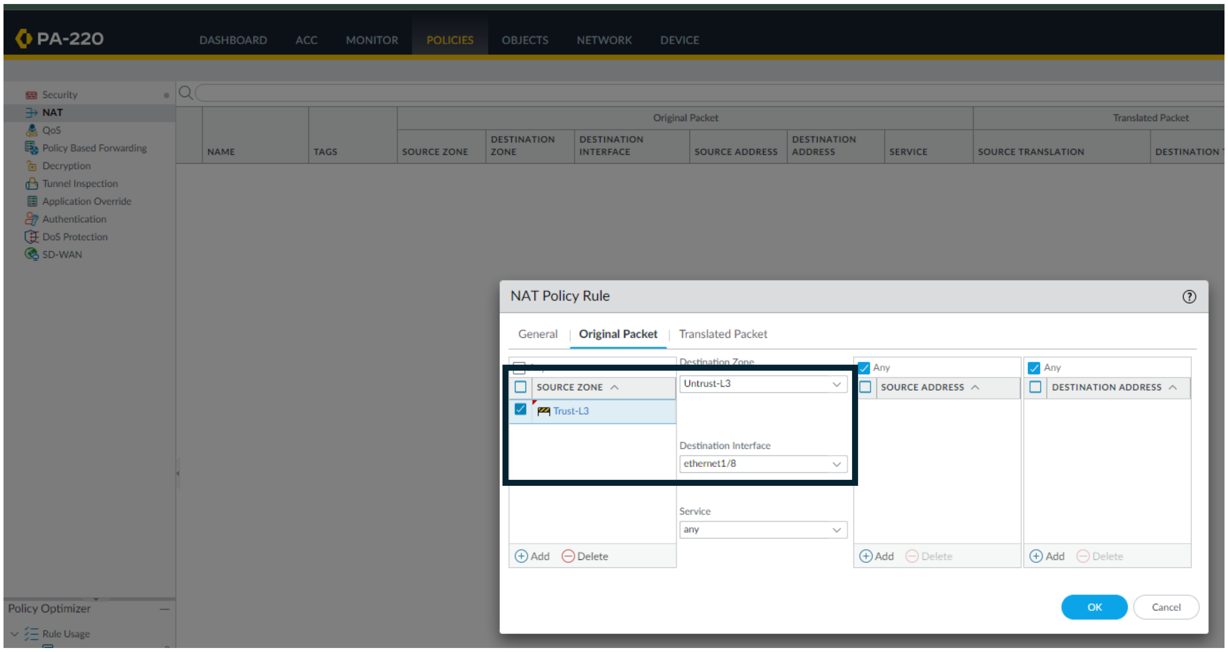
☑ Any — DESTINATION ADDRESS

any — DESTINATION DEVICE

□ Negate

Navigate to "Actions" and make sure to click "Allow" as well as "Log at Session End". Profile Setting should be Group and Internet.

Return to "Policies" homepage and choose "NAT" on the left taskbar. Add a new policy and enter a name and IPv4. Choose "Original Packet" and specify the Source Zone as "Trust-L3", the Destination Zone as "Untrust-L3", and the Destination Interface as "ethernet1/1".



NAT Policy Rule

General | **Original Packet** | Translated Packet

□	SOURCE ZONE
☑	Trust-L3

Destination Zone: Untrust-L3

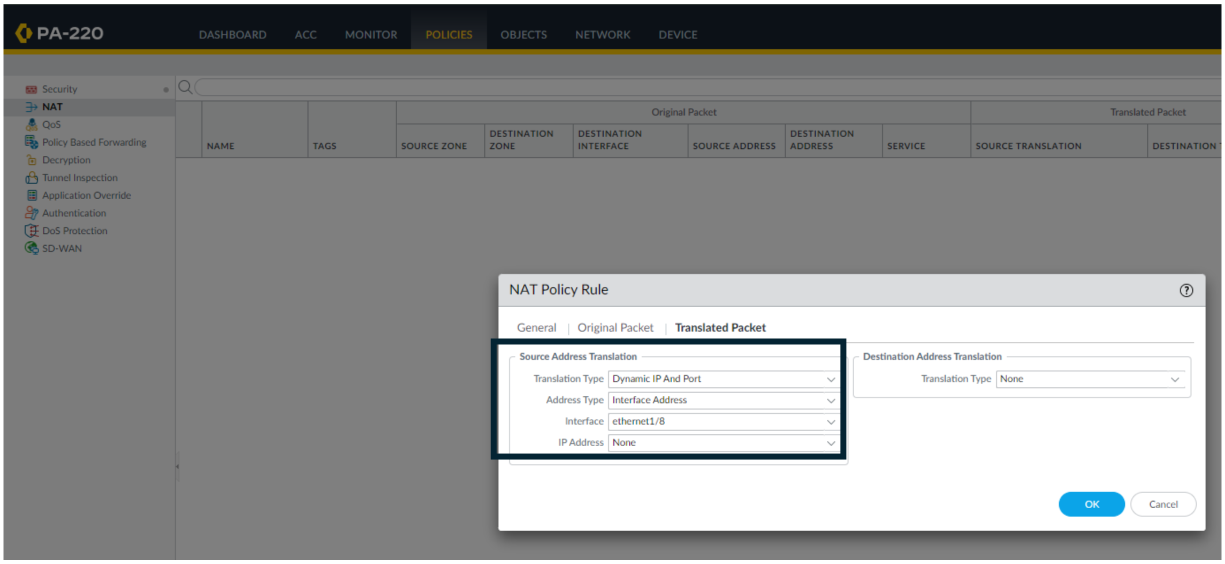
Destination Interface: ethernet1/8

Service: any

☑ Any — □ SOURCE ADDRESS

☑ Any — □ DESTINATION ADDRESS

In the "Translated Packet" section, set the Translation Type to Dynamic IP And Port. Make sure Address Type is Interface Address and your interface is the DHCP configured interface.



NAT Policy Rule

General | Original Packet | **Translated Packet**

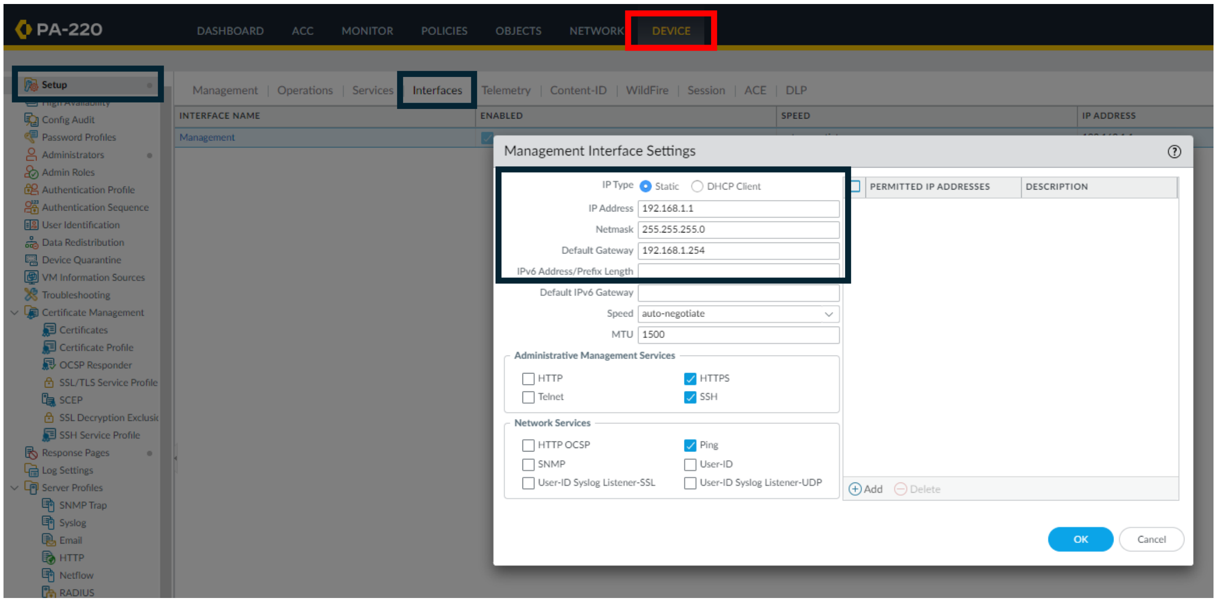
Source Address Translation

Translation Type: Dynamic IP And Port
Address Type: Interface Address
Interface: ethernet1/8
IP Address: None

Destination Address Translation

Translation Type: None

Go to Device, Setup, Interfaces and then Management Interface. Set IP Address to 192.168.1.1, Netmask to 255.255.255.0, and Default Gateway to 192.168.1.254.



Management Interface Settings

IP Type ● Static ○ DHCP Client
IP Address 192.168.1.1
Netmask 255.255.255.0
Default Gateway 192.168.1.254
IPv6 Address/Prefix Length
Default IPv6 Gateway
Speed auto-negotiate
MTU 1500

Administrative Management Services

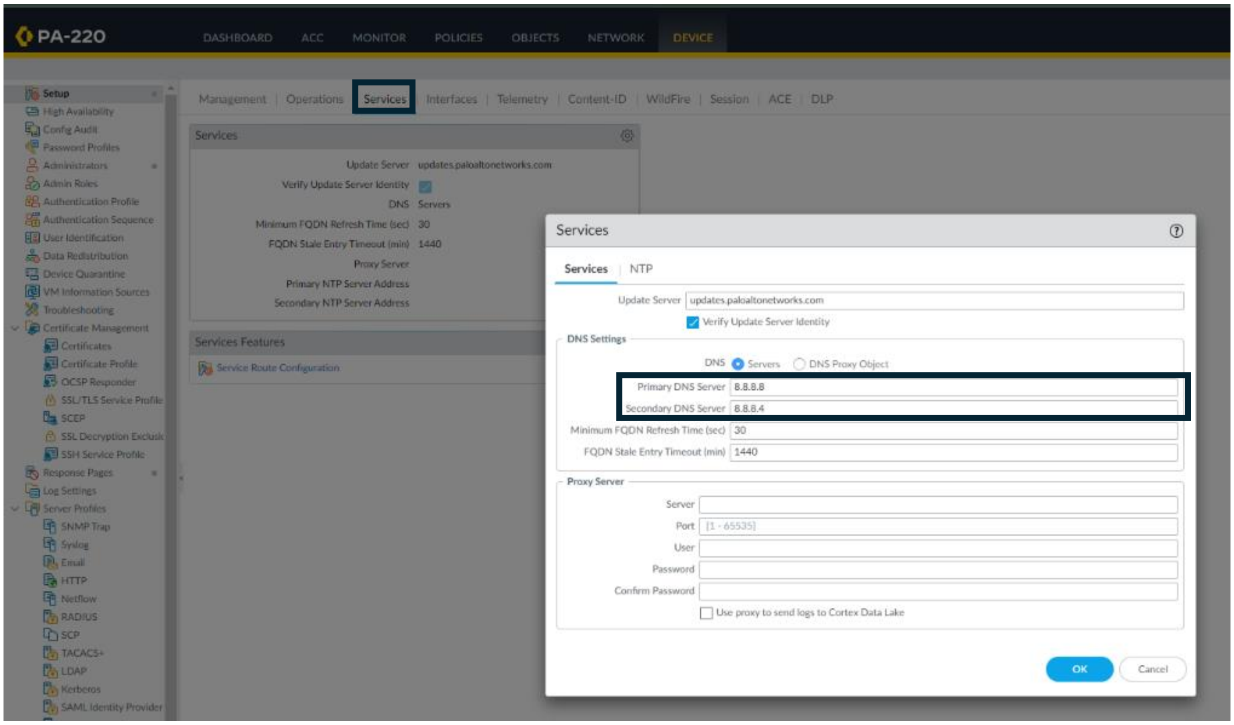
□ HTTP ☑ HTTPS
□ Telnet ☑ SSH

Network Services

□ HTTP OCSP ☑ Ping
□ SNMP □ User-ID
□ User-ID Syslog Listener-SSL □ User-ID Syslog Listener-UDP

□	PERMITTED IP ADDRESSES	DESCRIPTION

Return to Device, Setup and then click on Services. Enter the DNS server's IPs, 8.8.8.8 and 8.8.4.4 in the case of Google.



Services

Services | NTP

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

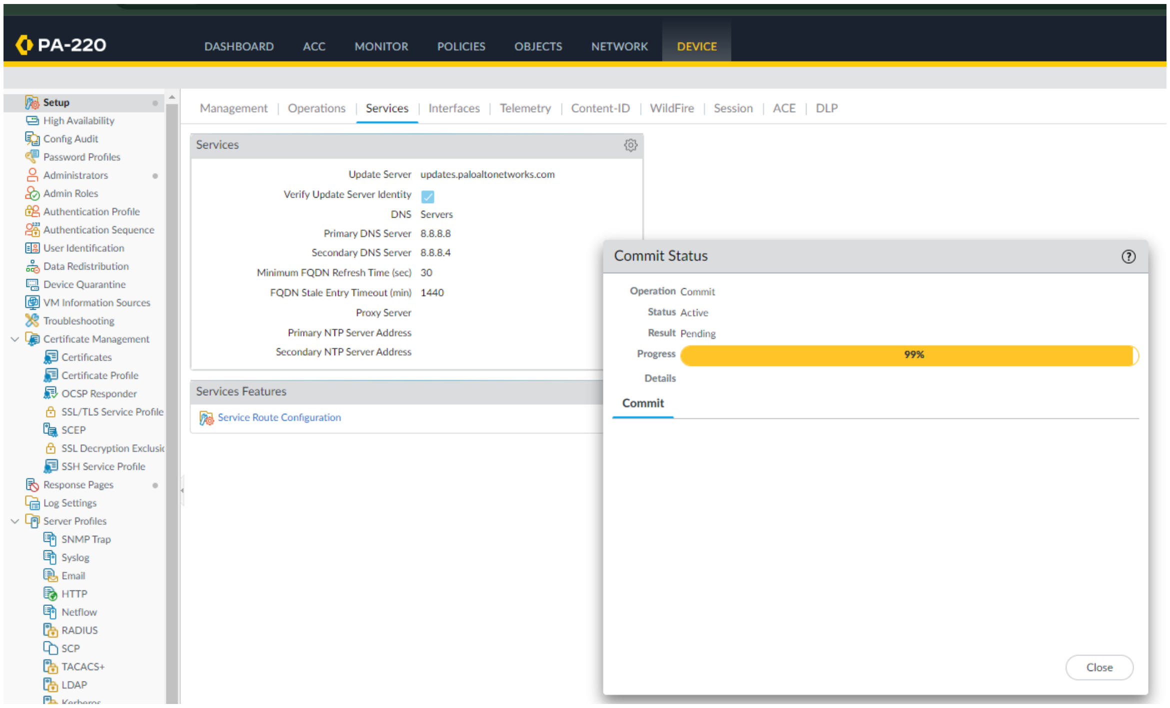
DNS Settings

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

Go to Device and commit your changes to the firewall.



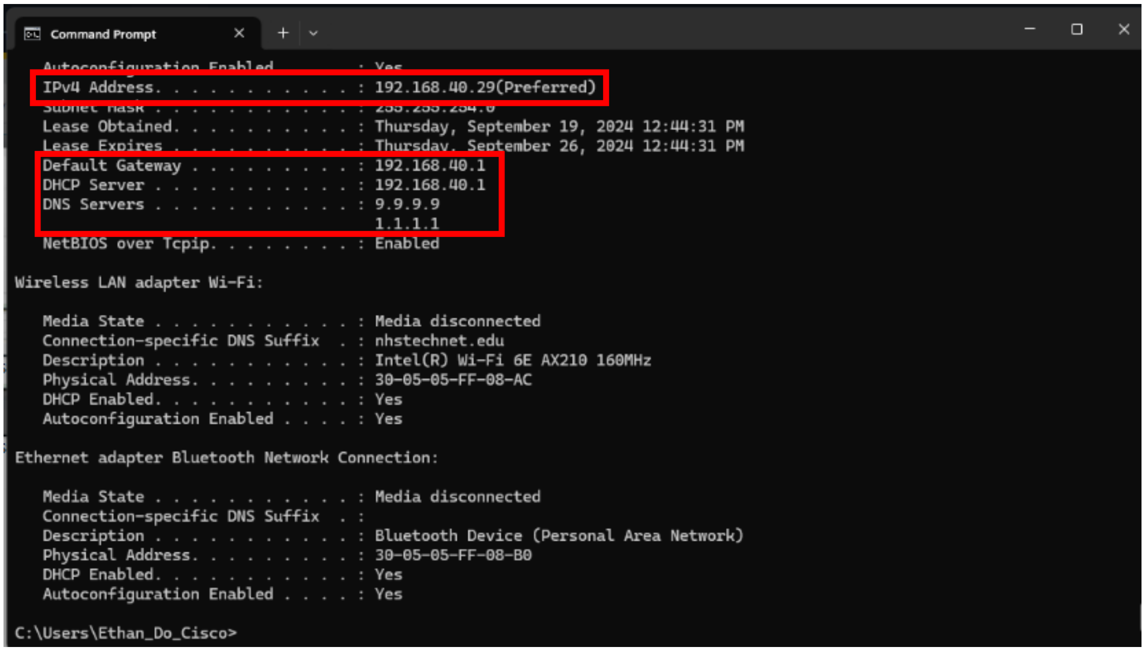
Services

Update Server updates.paloaltonetworks.com
Verify Update Server Identity ☑
DNS Servers
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
Primary NTP Server Address
Secondary NTP Server Address

Commit Status

Operation Commit
Status Active
Result Pending
Progress 99%
Details

Ensure that DHCP works by opening the command prompt on your host computer and typing the command ipconfig /all. Check whether or not the DHCP server supplied a usable IP address and whether or not the default gateway and DHCP server IP addresses are correct.



```
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 192.168.40.29(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.254.0
   Lease Obtained. . . . . . . . . . : Thursday, September 19, 2024 12:44:31 PM
   Lease Expires . . . . . . . . . . : Thursday, September 26, 2024 12:44:31 PM
   Default Gateway . . . . . . . . . : 192.168.40.1
   DHCP Server . . . . . . . . . . . : 192.168.40.1
   DNS Servers . . . . . . . . . . . : 9.9.9.9
                                       1.1.1.1
   NetBIOS over Tcpip. . . . . . . . : Enabled

Wireless LAN adapter Wi-Fi:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : nhstechnet.edu
   Description . . . . . . . . . . . : Intel(R) Wi-Fi 6E AX210 160MHz
   Physical Address. . . . . . . . . : 30-05-05-FF-08-AC
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Bluetooth Device (Personal Area Network)
   Physical Address. . . . . . . . . : 30-05-05-FF-08-B0
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

C:\Users\Ethan_Do_Cisco>
```

Lab Commands:

The only new command used in this lab was the ipconfig /all command in command prompt. This command shows the network interface information on a host. For this lab specifically, what we're looking for using the ipconfig /all command is the IP address of the host, DHCP server, and DNS server in order to make sure that the network is functional.

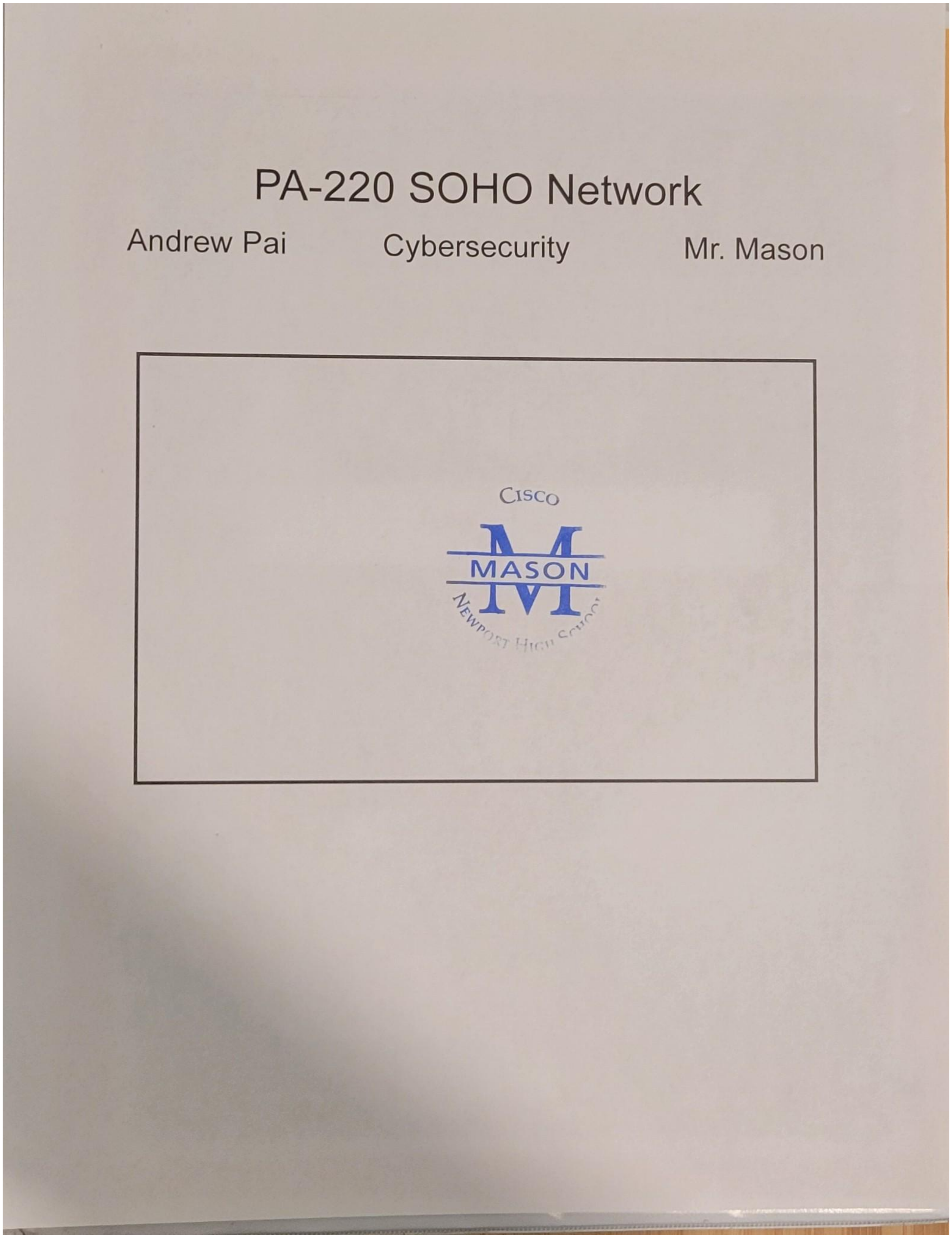
Problems:

One of the problems that we had with this lab was the fact that the firewall failed to commit the changes that we were uploading. This meant that our firewall was not functional and could not be tested. After experimenting with changes to try and commit for a while, our group figured out that the reason we couldn't commit was the presence of a virtual wire in our configuration. Once we deleted the virtual wire, the commits started to go through on the configuration.

Another problem that we had was some of our interfaces on the firewall being down. This stopped us from using many of our interfaces. In order to fix this, our group swapped firewalls and reset the new firewall and configured that one.

Conclusion:

In conclusion, this lab was meant to configure a Palo Alto PA-220 firewall to work in a Small Office Home Office (SOHO) network. To do this, we had to make use of the Graphical User Interface (GUI). On the GUI we followed a basic Palo Alto configuration tutorial and set up interfaces, VLANs, security zones, DHCP, and other basic services. The biggest problem we had was getting our firewall to commit changes since we didn't know that having a virtual wire would interfere with committing.



PA-220 SOHO Network

Andrew Pai Cybersecurity Mr. Mason

Cisco

MASON

Newport High School