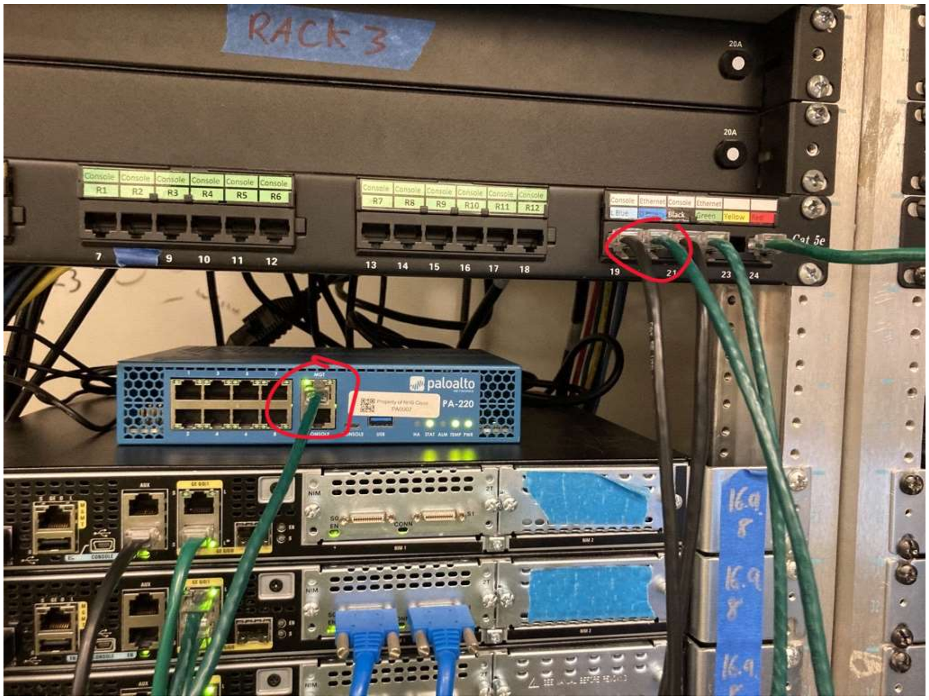
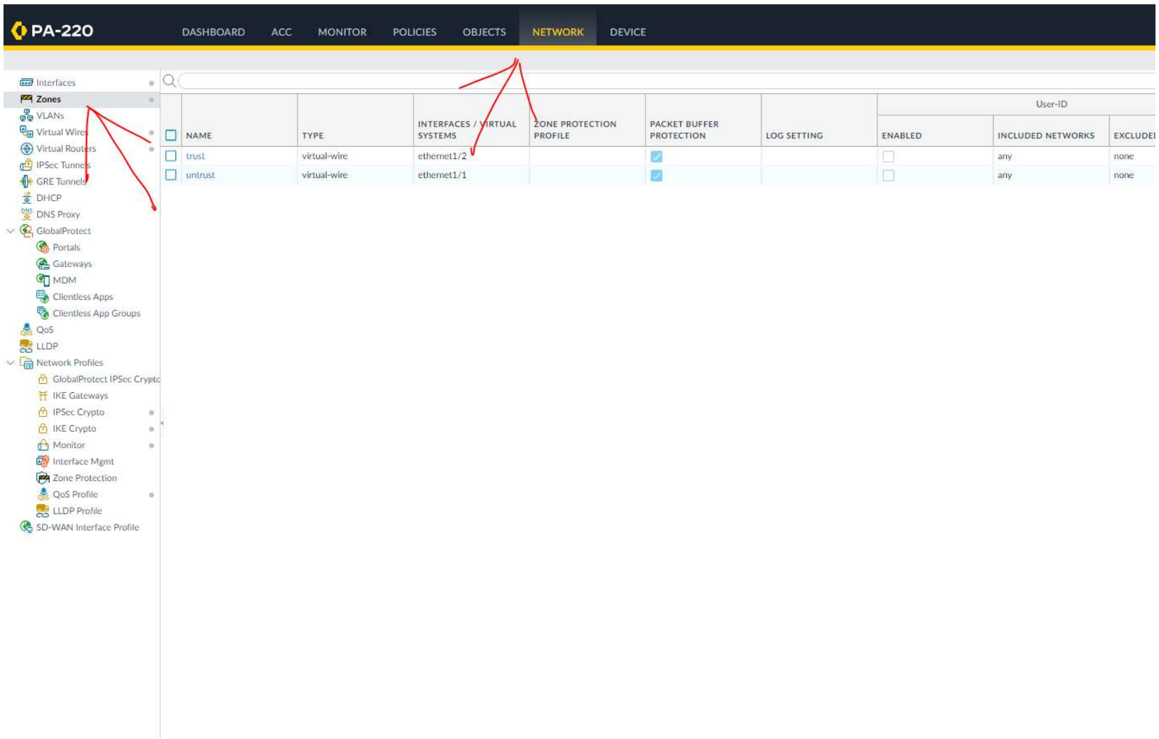
Purpose: We need to update our Palo Alto Firewall to the latest version, but to do so we need to connect our firewall to the internet first.

Background information: We were given a Palo Alto firewall that needs updating, but to update the firewall we need to first connect the firewall to the internet. So we are going to configure a SOHO network (small office/home office). SOHO networks are intended to allow users to connect themselves to a larger network from a different site, hence the name small/home office.

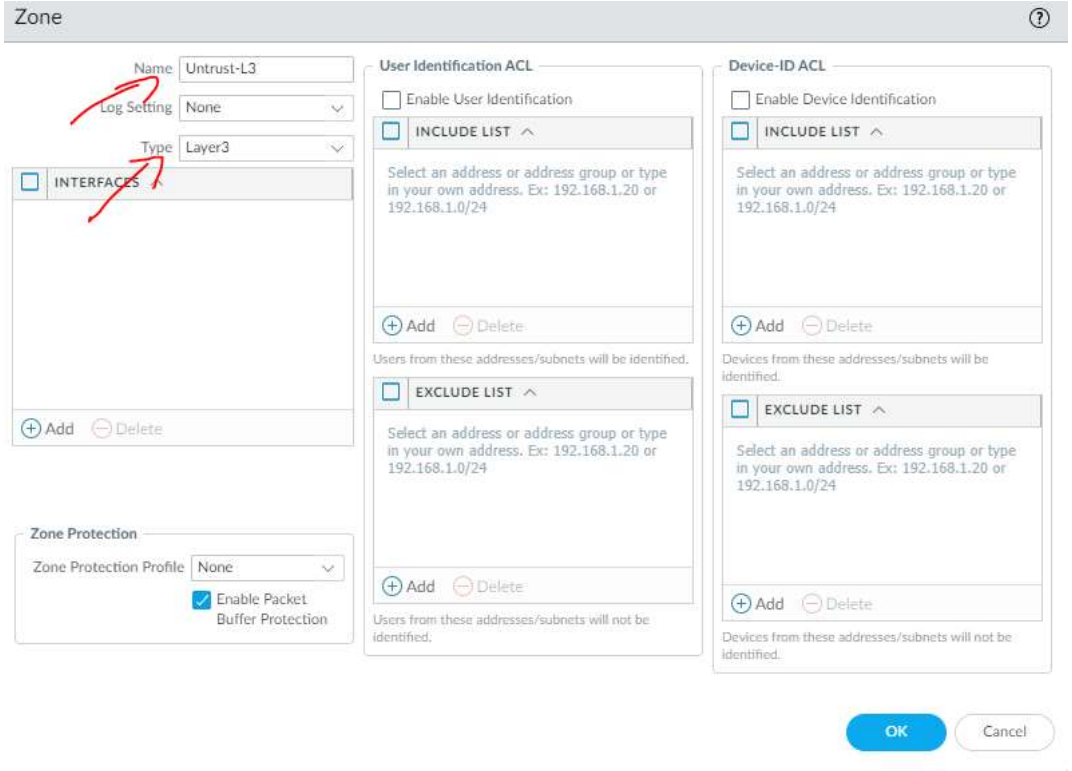


0: Plug your PC into the management port of your firewall. Make sure your PC is set to 192.168.1.3 with a 255.255.255.0 network mask and enter 192.168.1.1 to any web browser of your choice.



						User-ID		
□ NAME	TYPE	INTERFACES / VIRTUAL SYSTEMS	ZONE PROTECTION PROFILE	PACKET BUFFER PROTECTION	LOG SETTING	ENABLED	INCLUDED NETWORKS	EXCLUDEI
□ trust	virtual-wire	ethernet1/2		☑		□	any	none
□ untrust	virtual-wire	ethernet1/1		☑		□	any	none

1: Go to networks > Zones then add a new zone. We will need to create 3 new zones.

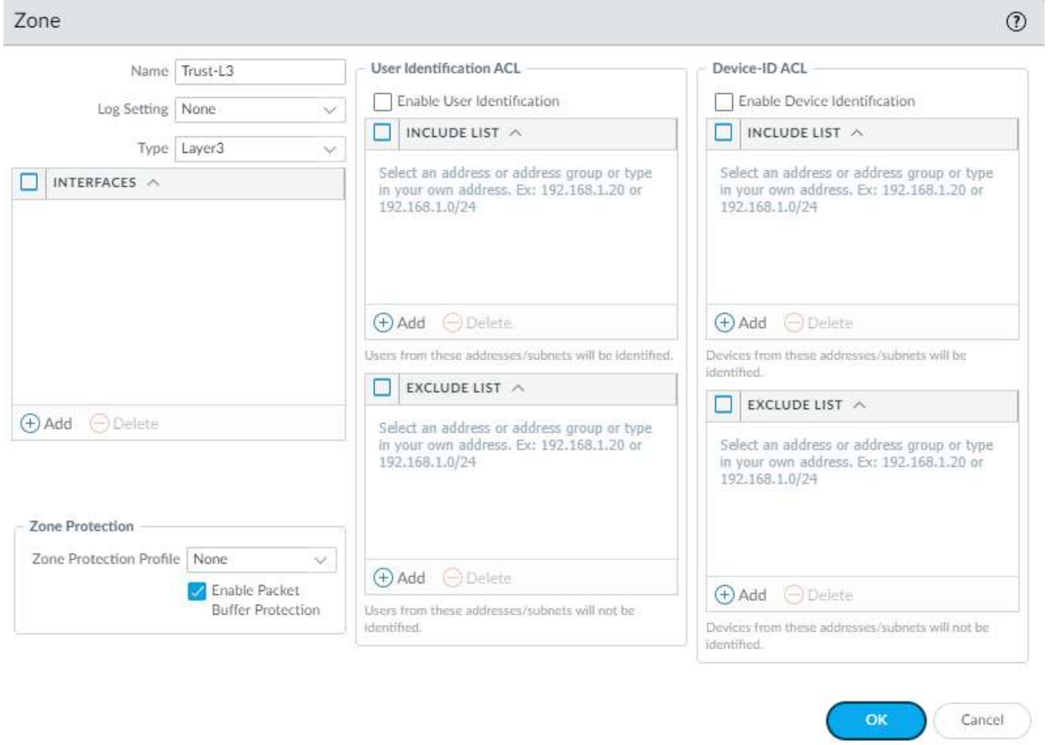

Zone
?
INTERFACES
Add
Delete
User Identification ACL
INCLUDE LIST
Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24
Add
Delete
Users from these addresses/subnets will be identified.
EXCLUDE LIST
Select an address or address group or type in your own address.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

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

□ Enable User Identification
□ Enable Device Identification

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

2: Create the first zone,name it Untrust-L3 and the type should be Layer3. Click OK



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

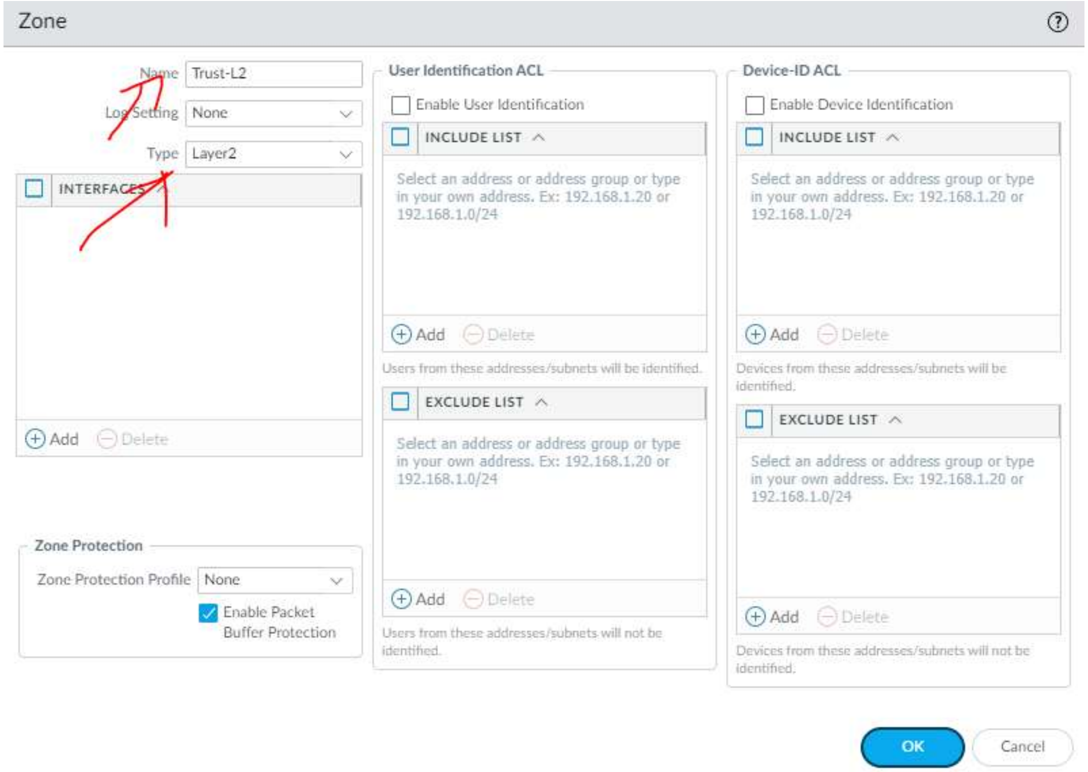
Devices from these addresses/subnets will be identified.

□ 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.

3: Create the second zone, named Trust-L3 with a layer of Layer3



Zone

Name: Trust-L2

Log Setting: None

Type: Layer2

□ INTERFACES

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

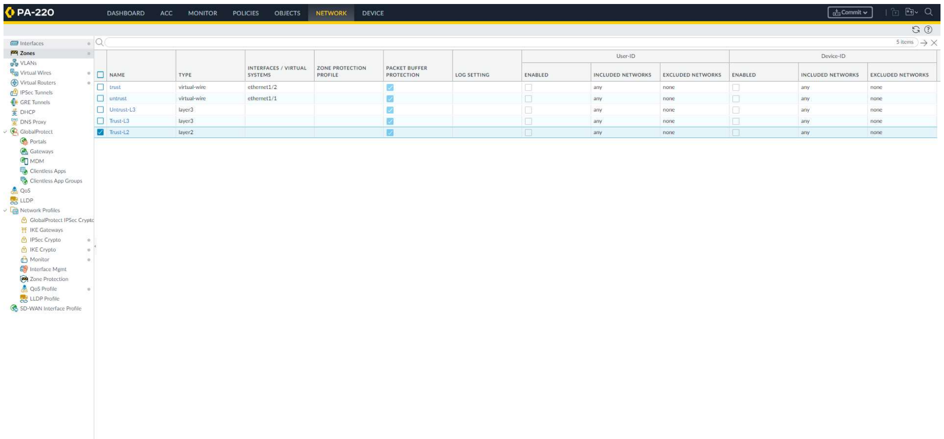
Devices from these addresses/subnets will not be identified.

Zone Protection

Zone Protection Profile: None

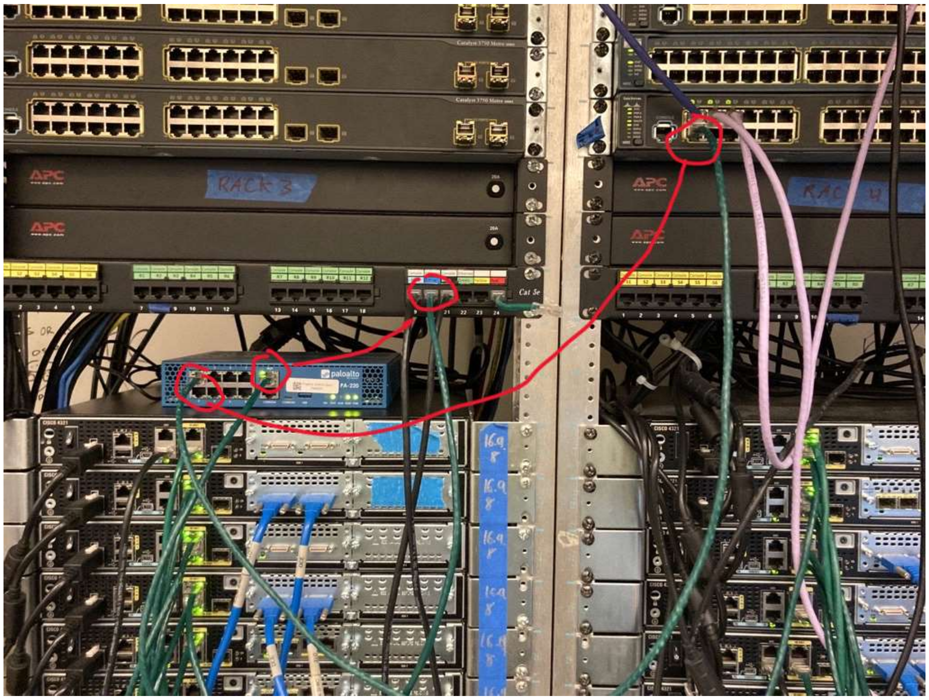
☑ Enable Packet Buffer Protection

4: Create the third zone, Trust-L2, Layer2

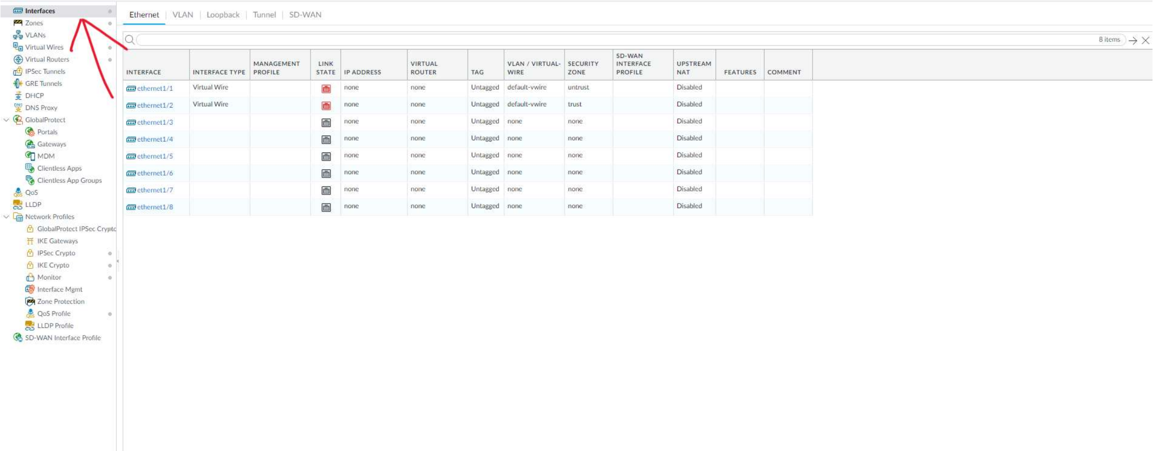


						User-ID			Device-ID		
NAME	TYPE	INTERFACES / VIRTUAL SYSTEMS	ZONE PROTECTION PROFILE	PACKET BUFFER PROTECTION	LOG SETTING	ENABLED	INCLUDED NETWORKS	EXCLUDED NETWORKS	ENABLED	INCLUDED NETWORKS	EXCLUDED NETWORKS
trust	virtual-wire	ethernet1/2		☑		□	any	none	□	any	none
untrust	virtual-wire	ethernet1/1	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

Your end result on your Zone page should look like this.

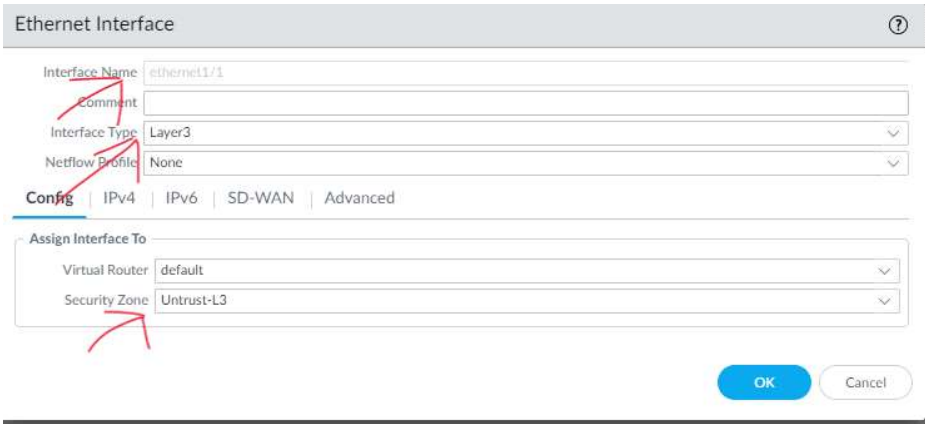


5: Now plug your firewall to an internet source, this could be router like shown in the image above.



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		

5: Go to Interfaces, right above Zones


Ethernet Interface

Interface Name: ethernet1/1

Comment:

Interface Type: Layer3

Netflow Profile: None

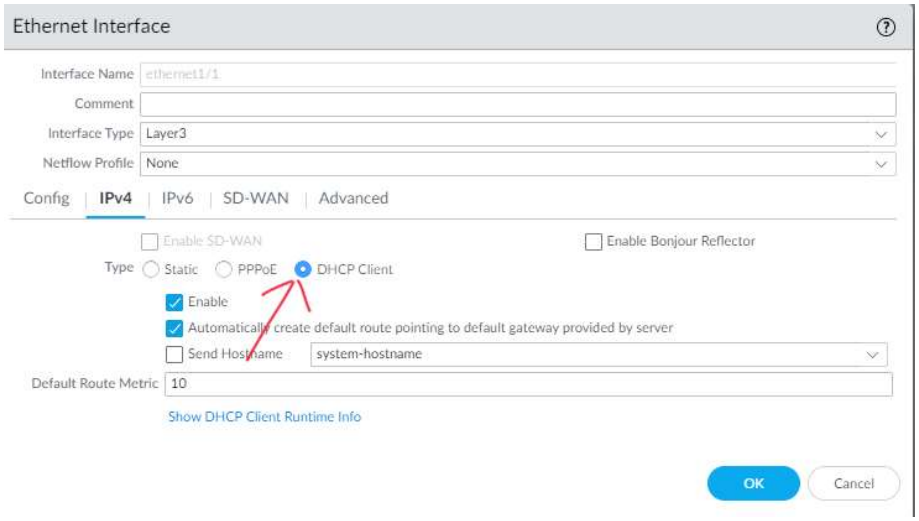
Config | IPv4 | IPv6 | SD-WAN | Advanced

Assign Interface To

Virtual Router: default

Security Zone: Untrust-L3

6: Select ethernet1/1. Set the interface type to Layer3 and security zone to Untrust-L3


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

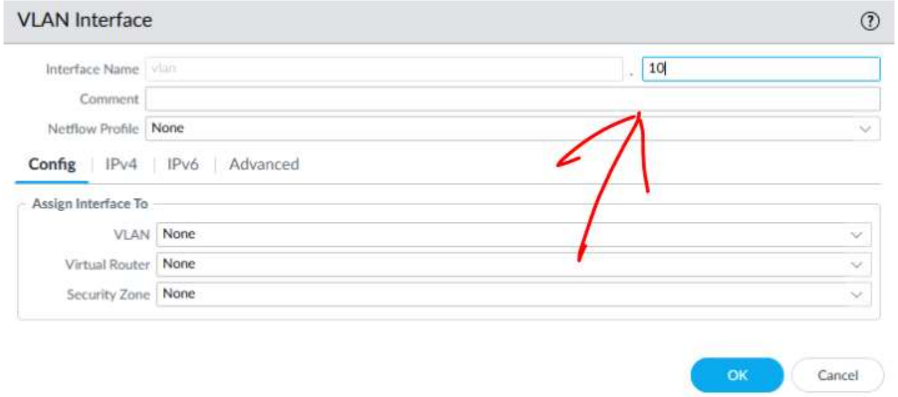
□ Send Hostname: system-hostname

Default Route Metric: 10

Show DHCP Client Runtime Info

7: Select IPv4, and choose DHCP Client

8: Go to Interfaces > VLANs and add a VLAN


VLAN Interface

Interface Name: vlan . 10

Comment:

Netflow Profile: None

Config | IPv4 | IPv6 | Advanced

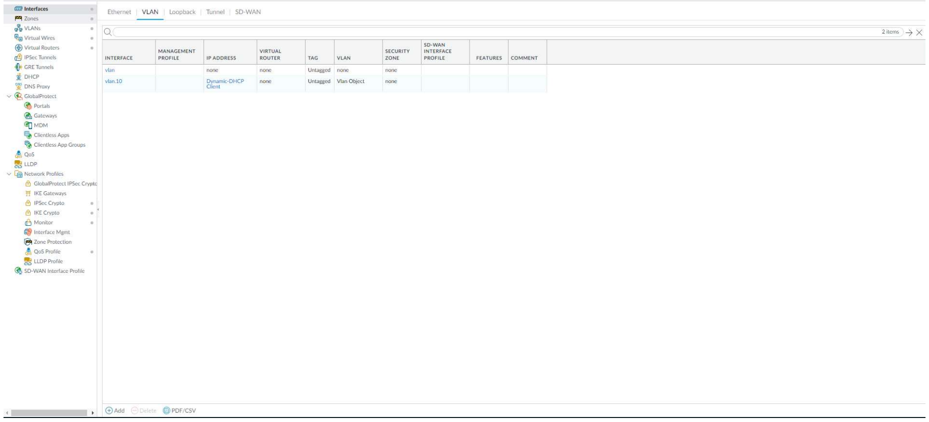
Assign Interface To

VLAN: None

Virtual Router: None

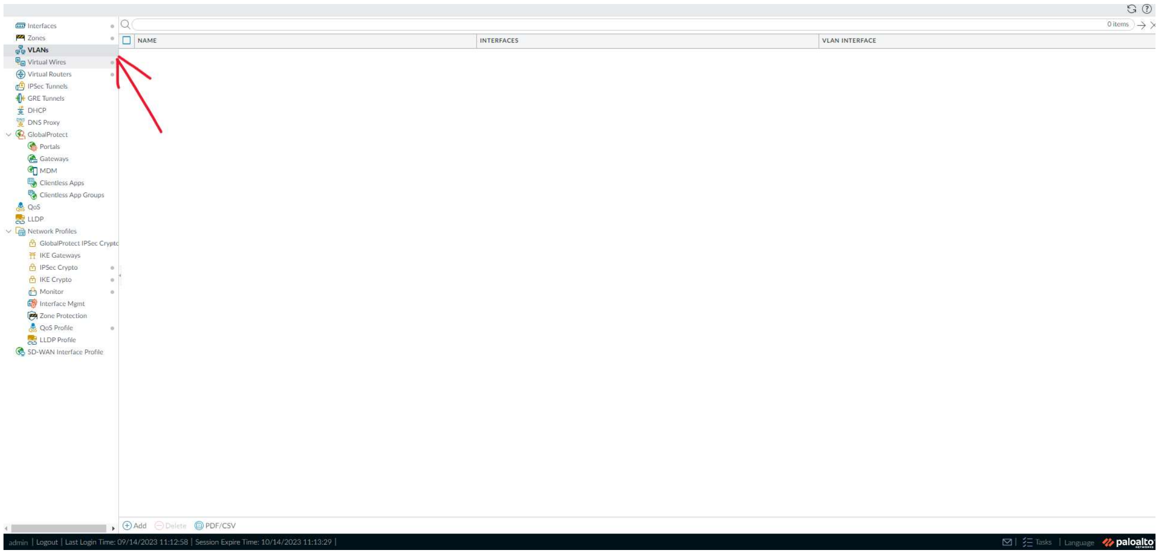
Security Zone: None

9: name a new VLAN interface, with a number of 10.



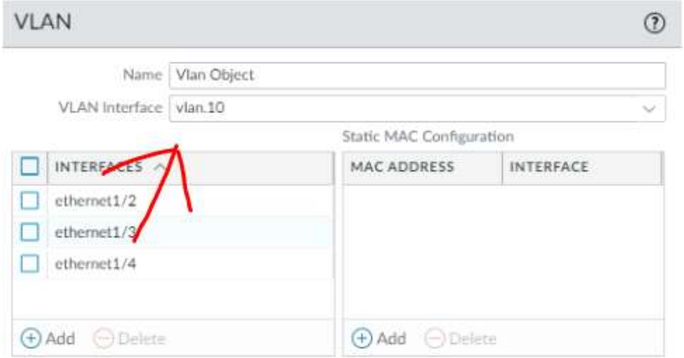
INTERFACE	MANAGEMENT PROFILE	IP ADDRESS	VIRTUAL ROUTER	TAG	VLAN	SECURITY ZONE	SD-WAN INTERFACE PROFILE	FEATURES	COMMENT
vlan		none	none	Untagged	none	none			
vlan.10		Dynamic-DHCP Client	none	Untagged	Vlan Object	none			

Your result should look like this.



□	NAME	INTERFACES	VLAN INTERFACE

10: Go to VLANs and make a new VLAN



VLAN

Name: Vlan Object

VLAN Interface: vlan.10

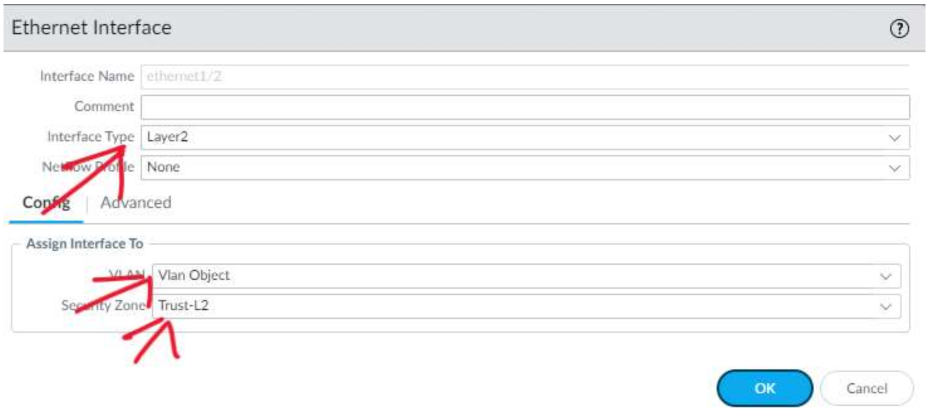
Static MAC Configuration

□	INTERFACES
□	ethernet1/2
□	ethernet1/3
□	ethernet1/4

MAC ADDRESS	INTERFACE

10: Create a new VLAN named VLAN Object and select the VLAN interface as vlan.10

11: Go back to Interfaces > Ethernet.


Ethernet Interface

Interface Name: ethernet1/2

Comment:

Interface Type: Layer2

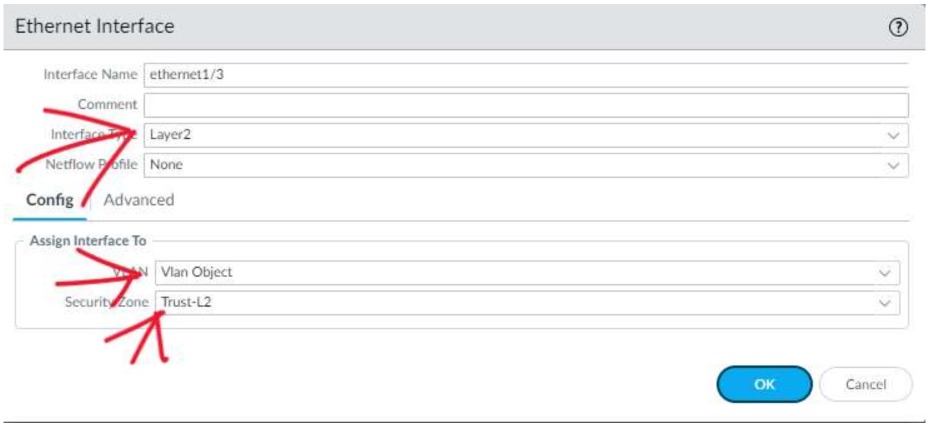
Netflow Profile: None

Assign Interface To

VLAN: Vlan Object

Security Zone: Trust-L2

12: Select the interface ethernet1/2, select the interface type a Layer2, VLAN as Vlan Object, and Security Zone as Trust-L2


Ethernet Interface

Interface Name: ethernet1/3

Comment:

Interface Type: Layer2

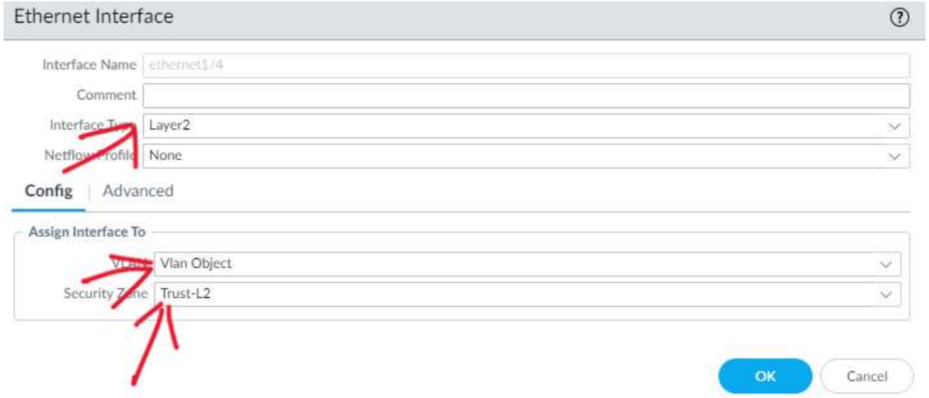
Netflow Profile: None

Assign Interface To

VLAN: Vlan Object

Security Zone: Trust-L2

13: Select the interface ethernet1/3, select the interface type a Layer2, VLAN as Vlan Object, and Security Zone as Trust-L2


Ethernet Interface

Interface Name: ethernet1/4

Comment:

Interface Type: Layer2

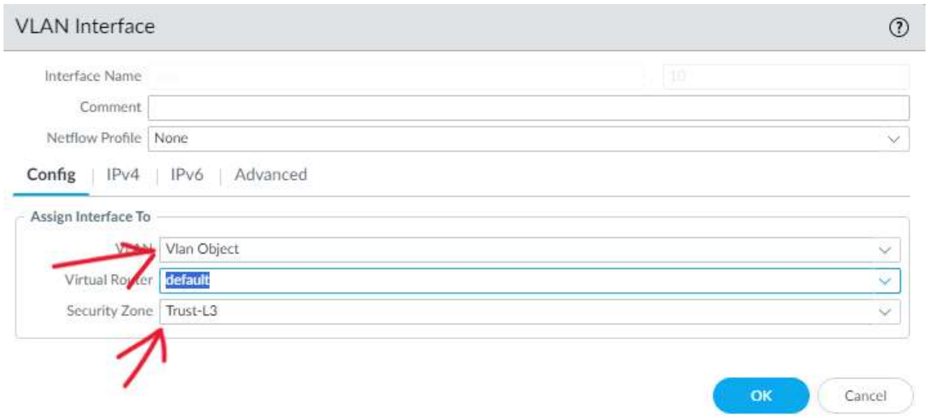
Netflow Profile: None

Assign Interface To

VLAN: Vlan Object

Security Zone: Trust-L2

14: Select the interface ethernet1/4, select the interface type a Layer2, VLAN as Vlan Object, and Security Zone as Trust-L2



VLAN Interface

Interface Name: 10

Comment:

Netflow Profile: None

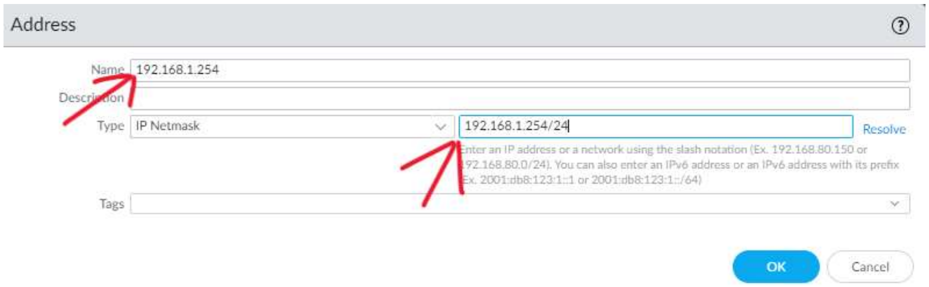
Assign Interface To

VLAN: Vlan Object

Virtual Router: default

Security Zone: Trust-L3

15: Now go to Interfaces > VLAN, select the interface Vlan, assign the interaface to VLAN: Vlan Object and security zone of Trust-L3. Do not click OK!



Address

Name: 192.168.1.254

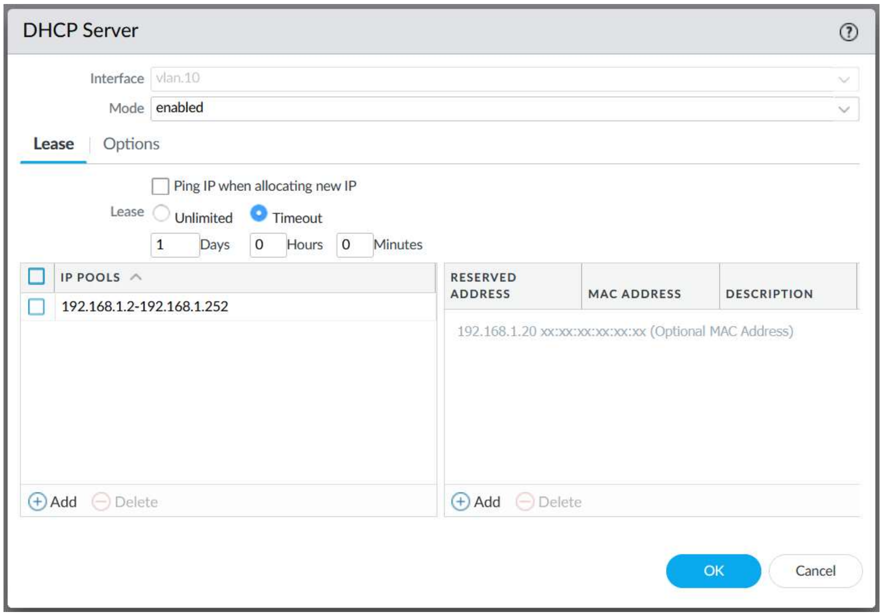
Description:

Type: IP Netmask 192.168.1.254/24

Enter an IP address or a network using the slash notation (Ex. 192.168.80.150 or 192.168.80.0/24). You can also enter an IPv6 address or an IPv6 address with its prefix Ex. 2001:db8:123:1::1 or 2001:db8:123:1::/64)

Tags:

16: Under IPv4, create a new address with the following address: 192.168.1.254/24



DHCP Server

Interface: vlan.10

Mode: enabled

□ Ping IP when allocating new IP

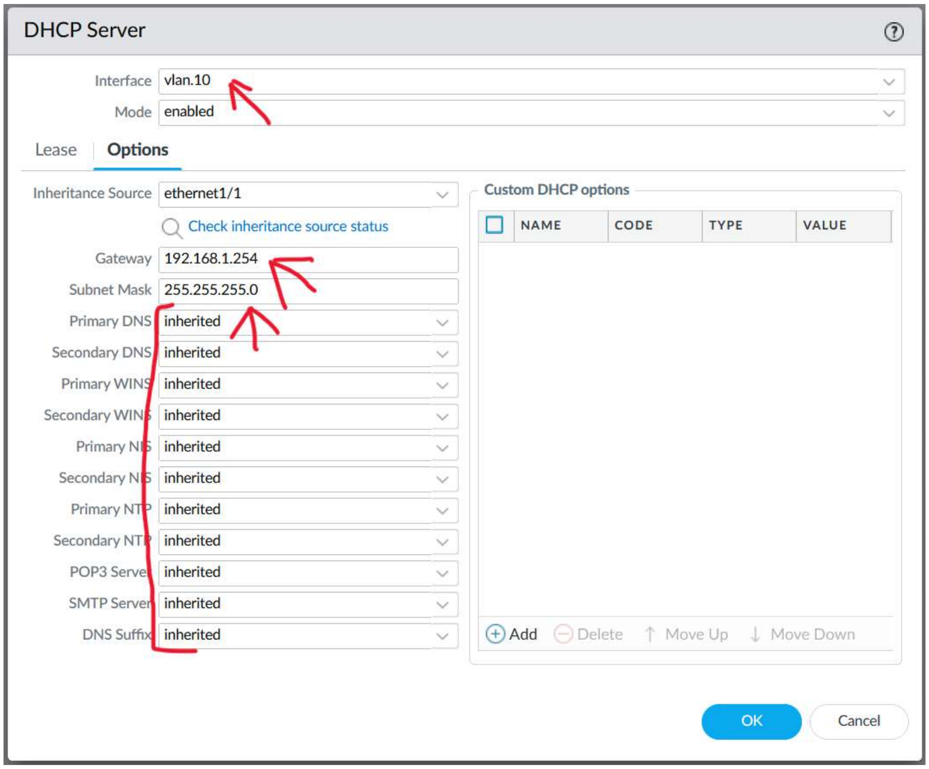
Lease ○ Unlimited ● Timeout

1 Days 0 Hours 0 Minutes

□ IP POOLS
□ 192.168.1.2-192.168.1.252

RESERVED ADDRESS	MAC ADDRESS	DESCRIPTION
192.168.1.20	xx:xx:xx:xx:xx:xx (Optional MAC Address)	

17: Go Network > DHCP > DHCP server and create a new DHCP server.

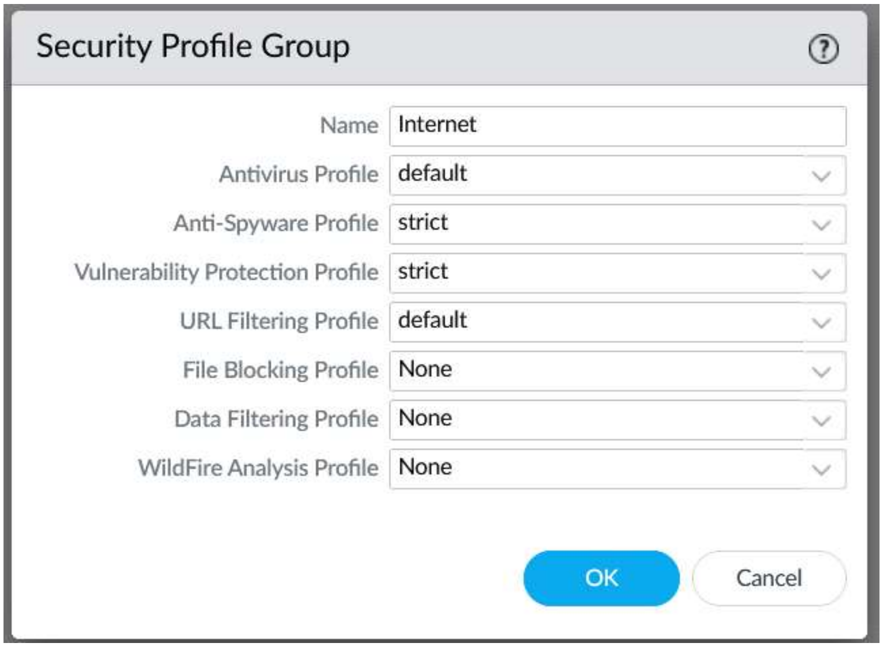


DHCP Server

Interface	vlan.10
Mode	enabled

Inheritance Source	ethernet1/1
Gateway	192.168.1.254
Subnet Mask	255.255.255.0
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	inherited

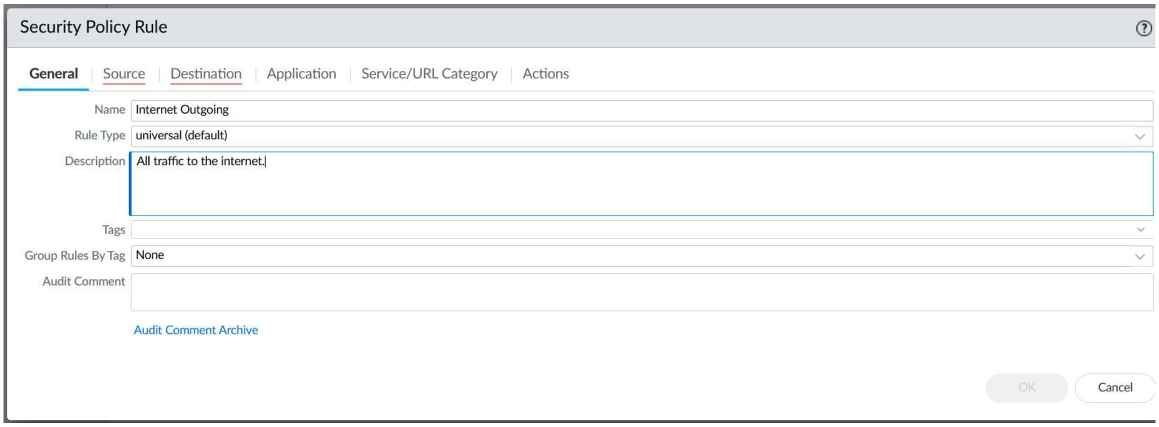
18: Under options, ensure the interface is vlan.10 and inheritance source is ethernet 1/1. Create the gateway as 192.168.1.254 with a subnet of 255.255.255.0. The rest of the options should say as inherited.



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

19: Go to objects > security and add a new security profile group with the following settings as shown above.



Name: Internet Outgoing

Rule Type: universal (default)

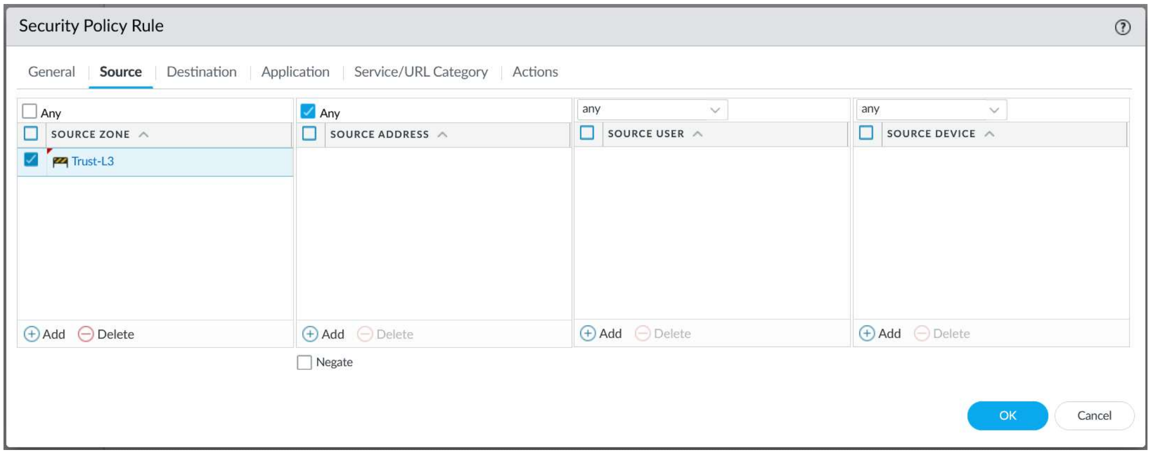
Description: All traffic to the internet.

Tags:

Group Rules By Tag: None

Audit Comment:

20: Under General, enter an appropriate name and discription.



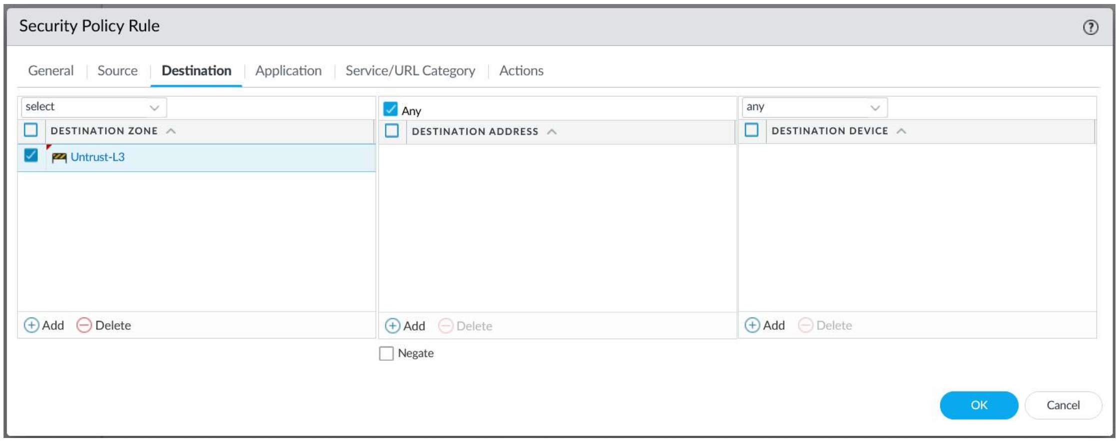
□ Any
□ SOURCE ZONE
☑ Trust-L3

☑ Any
□ SOURCE ADDRESS
□ Negate

any
□ SOURCE USER

any
□ SOURCE DEVICE

21: Select the source tab and select Turst-L3 as the source zone

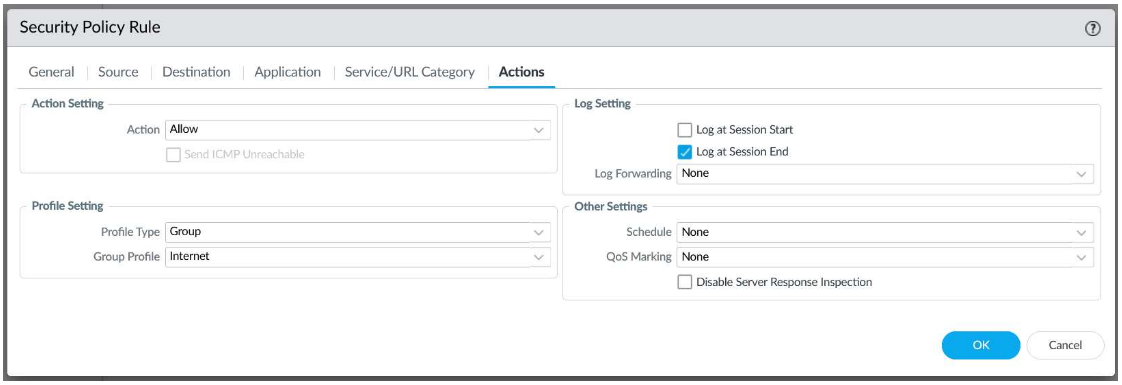


select
□ DESTINATION ZONE
☑ Untrust-L3

☑ Any
□ DESTINATION ADDRESS
□ Negate

any
□ DESTINATION DEVICE

22: Select the destination tab and select Unturst-L3 as the destination zone



Security Policy Rule

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

Action Setting

Action: Allow

□ Send ICMP Unreachable

Log Setting

□ Log at Session Start

☑ Log at Session End

Log Forwarding: None

Profile Setting

Profile Type: Group

Group Profile: Internet

Other Settings

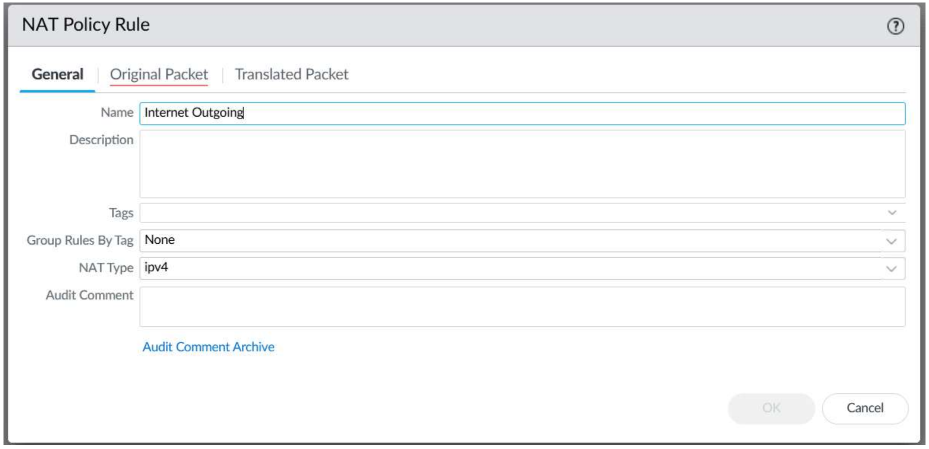
Schedule: None

QoS Marking: None

□ Disable Server Response Inspection

23: Select the Actions tab and set the action settings as Allow. Make sure all settings look the same as the image above.

24: Go to Policy > NAT and add a new NAT



NAT Policy Rule

Name: Internet Outgoing

Description:

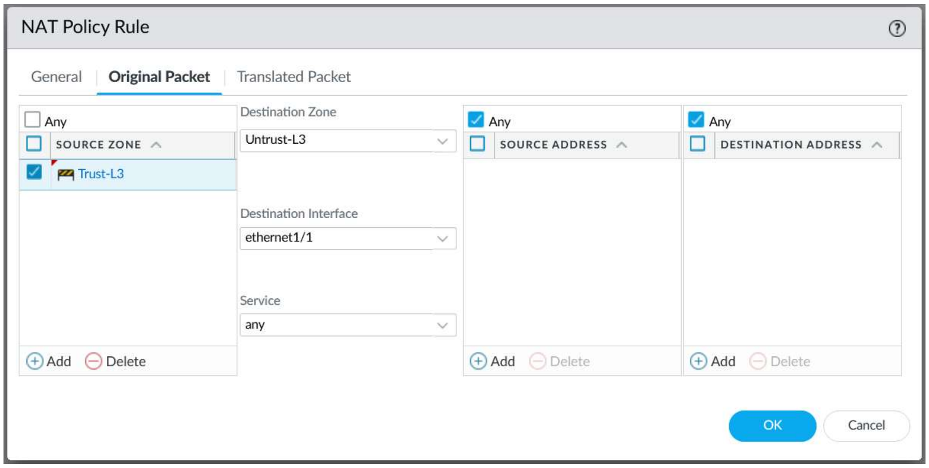
Tags:

Group Rules By Tag: None

NAT Type: ipv4

Audit Comment:

25: Create a NAT with the appropriate name and description.



NAT Policy Rule

□ Any

SOURCE ZONE

☑ Trust-L3

Destination Zone: Untrust-L3

Destination Interface: ethernet1/1

Service: any

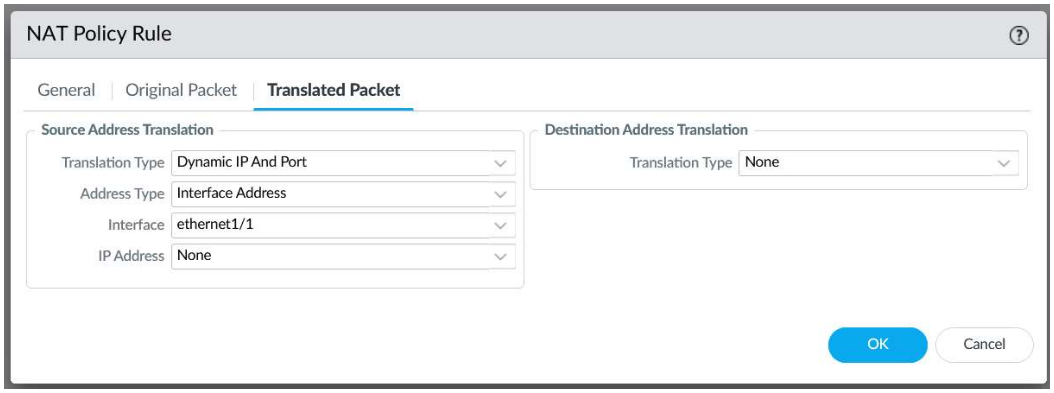
☑ Any

SOURCE ADDRESS

☑ Any

DESTINATION ADDRESS

26: Select Original Packet and choose Trust-L3 as the Source Zone.



NAT Policy Rule

General | Original Packet | **Translated Packet**

Source Address Translation

Translation Type: Dynamic IP And Port

Address Type: Interface Address

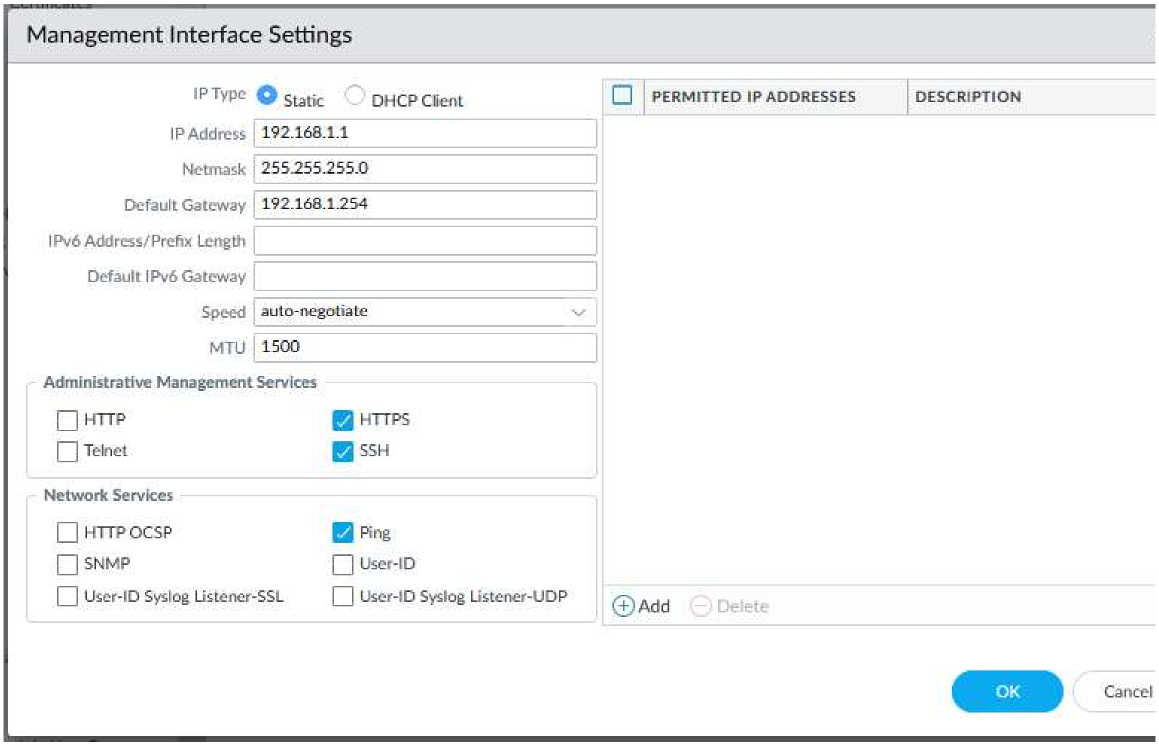
Interface: ethernet1/1

IP Address: None

Destination Address Translation

Translation Type: None

27: Go the Translated Packet tab and select the following settings as seen above.



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

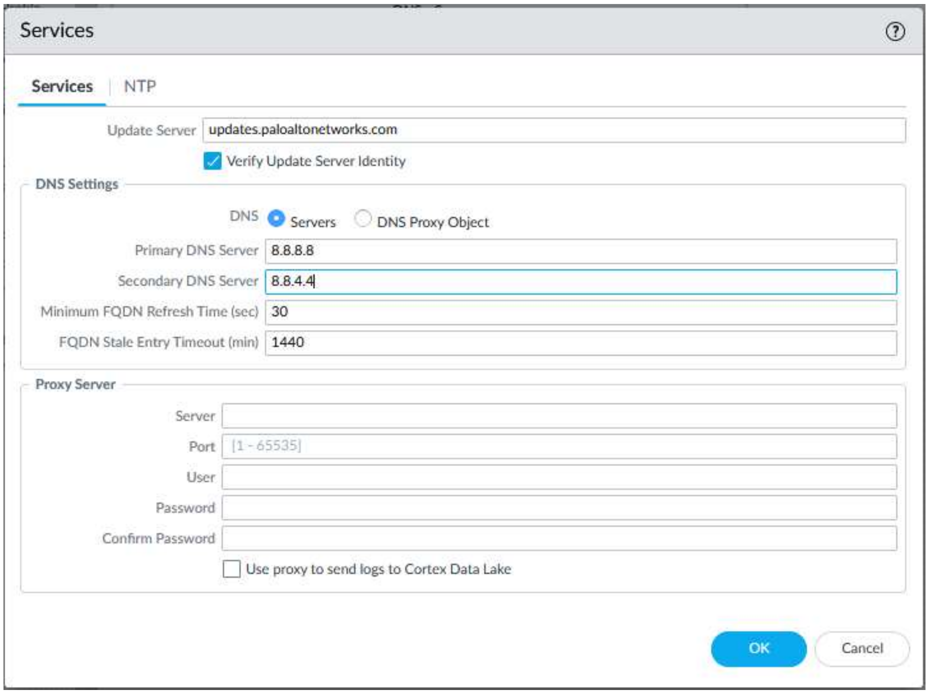
☐ HTTP OCSP ☑ Ping

☐ SNMP ☐ User-ID

☐ User-ID Syslog Listener-SSL ☐ User-ID Syslog Listener-UDP

☐	PERMITTED IP ADDRESSES	DESCRIPTION

28: Go to Device > Setup > Management and select the following IP Address, Netmask, and Default gateway as shown above.



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: 8.8.4.4

Minimum FQDN Refresh Time (sec): 30

FQDN Stale Entry Timeout (min): 1440

Proxy Server

Server:

Port: [1 - 65535]

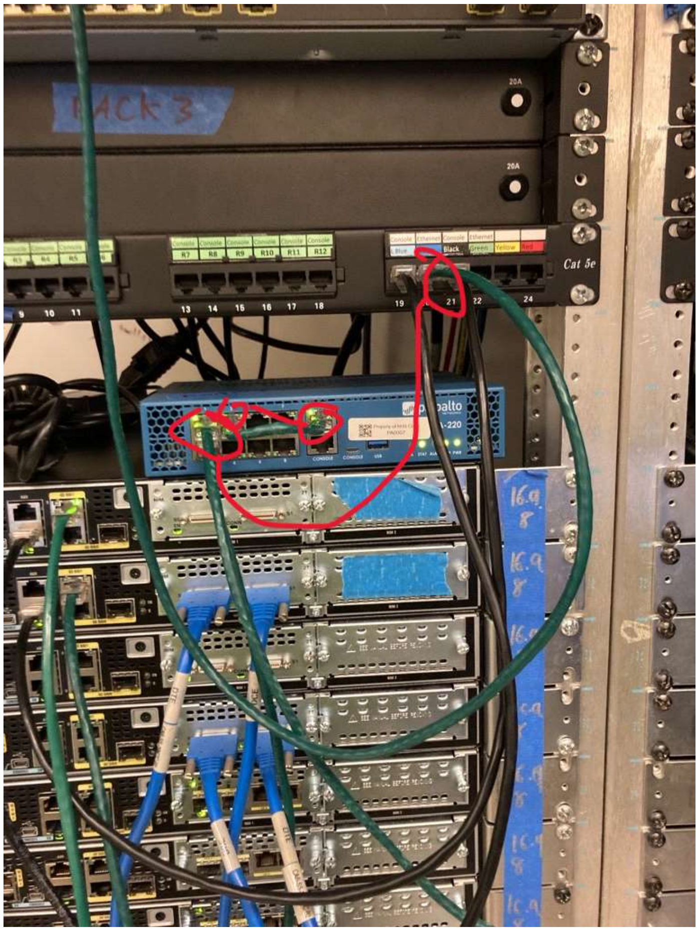
User:

Password:

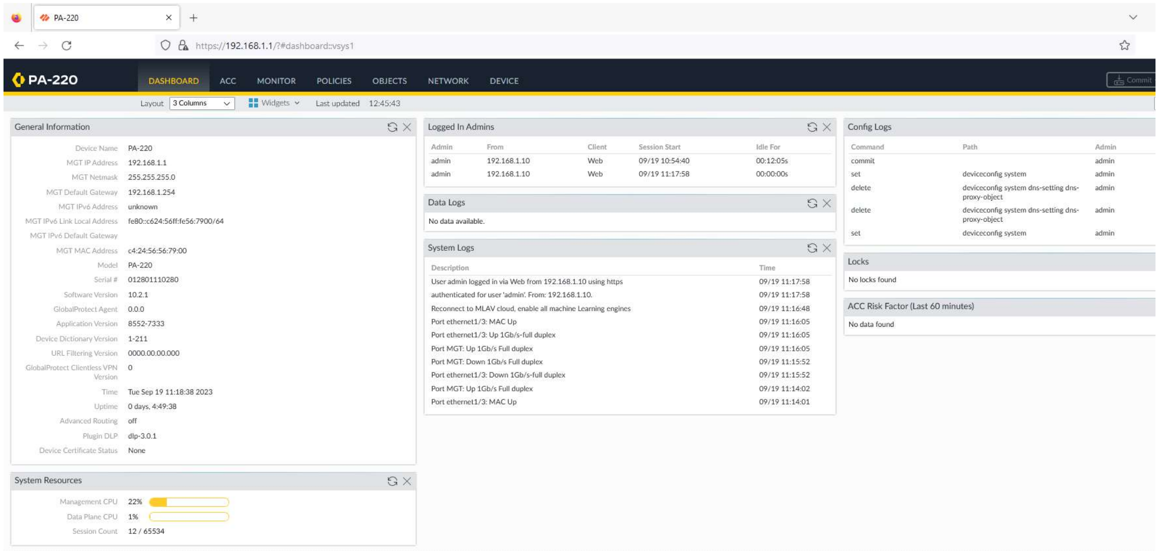
Confirm Password:

□ Use proxy to send logs to Cortex Data Lake

29: Go to Device > Setup > Services and Enter the DNS server's IP. Here we show 8.8.8.8 and 8.8.4.4 which is the DNS IP of Google.



30: Connect your computer to one of the ethernet ports on the firewall and connect one of your firewalls ethernet ports to the management port as shown above. Your firewall is not connected to the internet.



Last updated 12:45:43

General Information

Device Name	PA-220
MGT IP Address	192.168.1.1
MGT Netmask	255.255.255.0
MGT Default Gateway	192.168.1.254
MGT IPv6 Address	unknown
MGT IPv6 Link Local Address	fe80::c624:56ff:fe56:7900/64
MGT IPv6 Default Gateway	
MGT MAC Address	c4:24:56:56:79:00
Model	PA-220
Serial #	012801110280
Software Version	10.2.1
GlobalProtect Agent	0.0.0
Application Version	8552-7333
Device Dictionary Version	1-211
URL Filtering Version	0000.00.00.000
GlobalProtect Clientless VPN Version	0
Time	Tue Sep 19 11:18:38 2023
Uptime	0 days, 4:49:38
Advanced Routing	off
Plugin DLP	dlp-3.0.1
Device Certificate Status	None

System Resources

Management CPU	22%
Data Plane CPU	1%
Session Count	12 / 65534

Logged In Admins

Admin	From	Client	Session Start	Idle For
admin	192.168.1.10	Web	09/19 10:54:40	00:12:05s
admin	192.168.1.10	Web	09/19 11:17:58	00:00:00s

Data Logs

No data available.

System Logs

```
Description                                                        Time
User admin logged in via Web from 192.168.1.10 using https         09/19 11:17:58
authenticated for user 'admin'. From: 192.168.1.10.                09/19 11:17:58
Reconnect to MLAV cloud, enable all machine Learning engines       09/19 11:16:48
Port ethernet1/3: MAC Up                                           09/19 11:16:05
Port ethernet1/3: Up 1Gb/s-full duplex                             09/19 11:16:05
Port MGT: Up 1Gb/s Full duplex                                     09/19 11:16:05
Port MGT: Down 1Gb/s Full duplex                                   09/19 11:15:52
Port ethernet1/3: Down 1Gb/s-full duplex                           09/19 11:15:52
Port MGT: Up 1Gb/s Full duplex                                     09/19 11:14:02
Port ethernet1/3: MAC Up                                           09/19 11:14:01
```

Config Logs

Command	Path	Admin
commit		admin
set	deviceconfig system	admin
delete	deviceconfig system dns-setting dns-proxy-object	admin
delete	deviceconfig system dns-setting dns-proxy-object	admin
set	deviceconfig system	admin

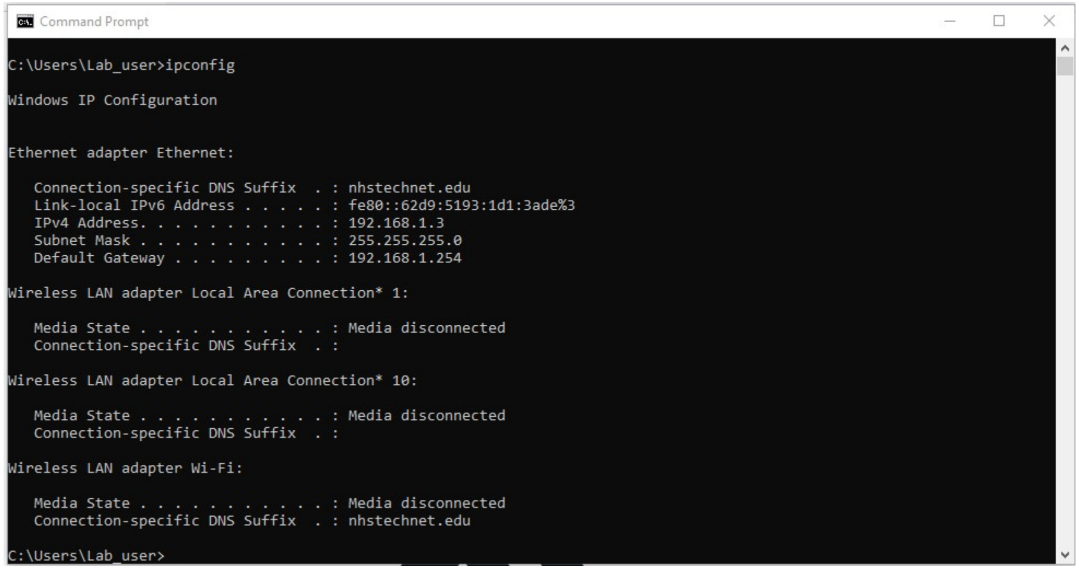
Locks

No locks found

ACC Risk Factor (Last 60 minutes)

No data found

Your end result should be under your Dashboard



```
C:\Users\Lab_user>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : nhstechnet.edu
   Link-local IPv6 Address . . . . . : fe80::62d9:5193:1d1:3ade%3
   IPv4 Address. . . . . . . . . . . : 192.168.1.3
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.254

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 10:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : nhstechnet.edu

C:\Users\Lab_user>
```

Your end result when you do an ipconfig in command prompt.

You are now good to go to download updates for your firewall!

Problems: We ran into an issue of forgetting to change the computer's IP address back to automatically being set by DHCP from statically being assigned before. We needed to change by to DHCP addresses as the firewall is not a DHCP server and will give any devices an IP address that has it set as it's default gateway.

Conclusion: We now can easily connect devices to our firewall without changing the computer's IP address manually. Now can update the firewall to the newest version, our next lab.