Firewalls

By Carlos Gerez Garcia, Christopher Ditto, and Mark Riley Slik

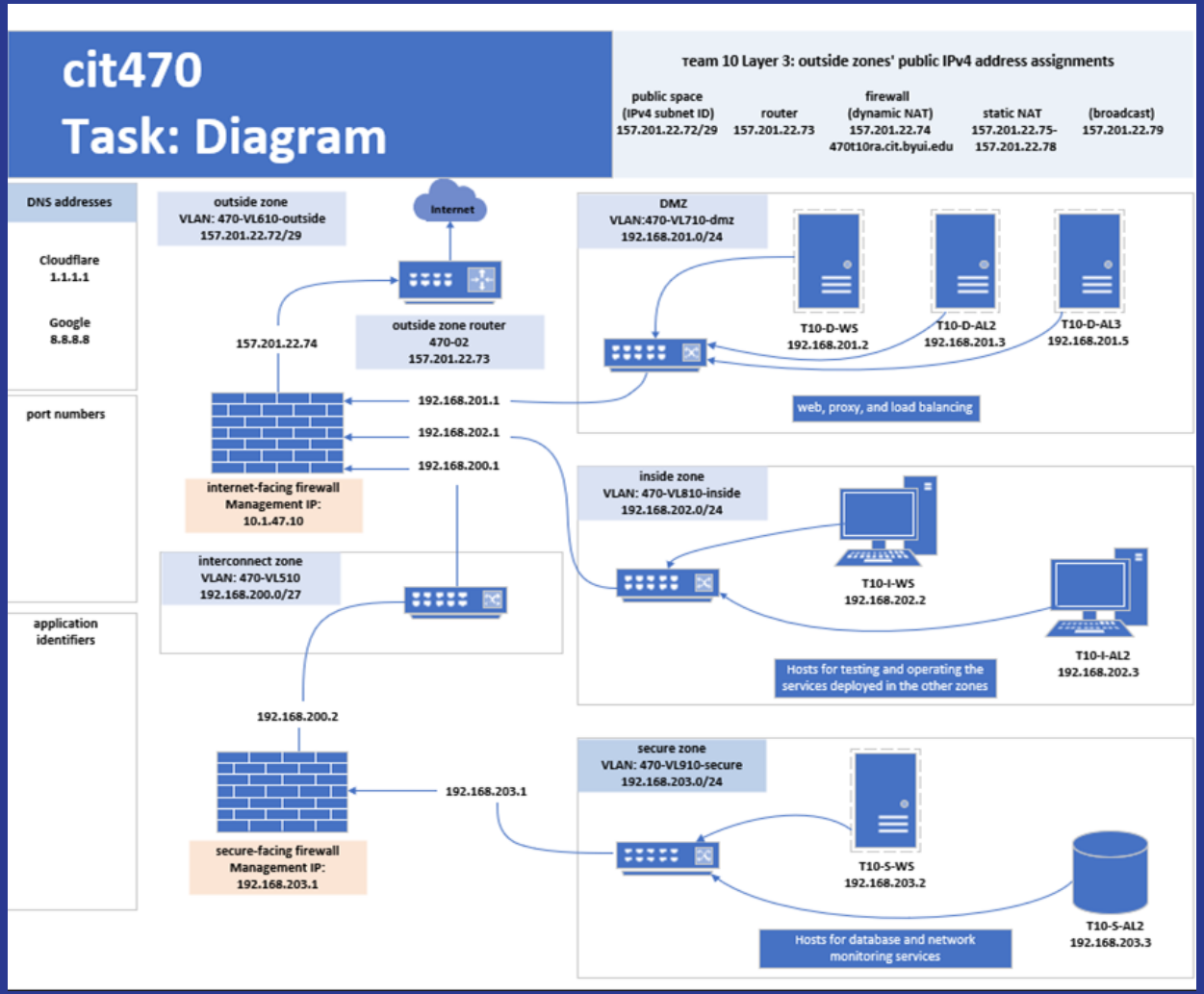
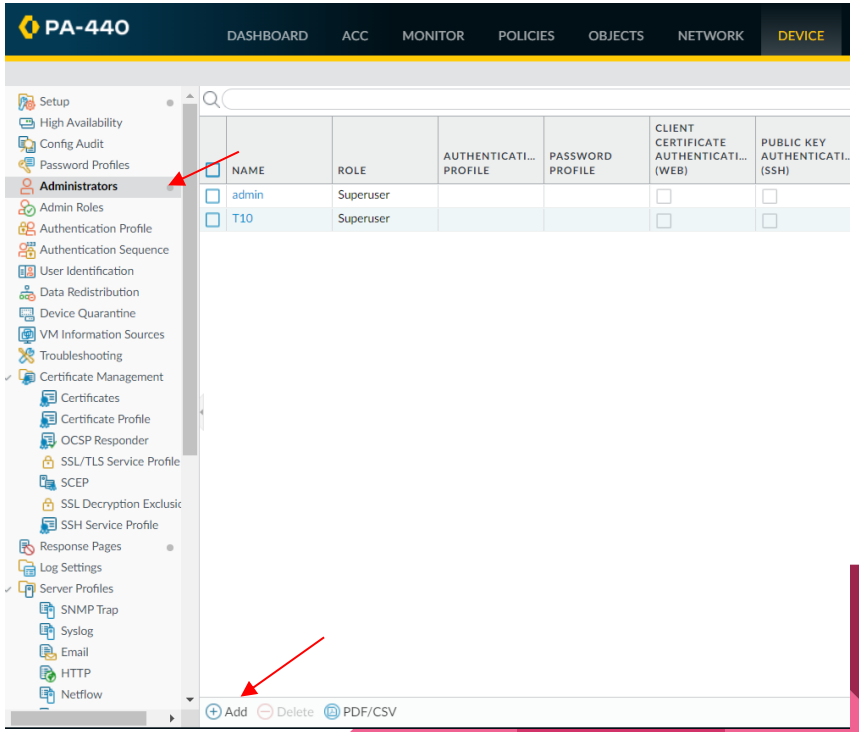


Diagram Outline for Team 10

Palo Alto PA-440 Configuration

Log into Palo Alto GUI, using the credentials given by the course instructor.

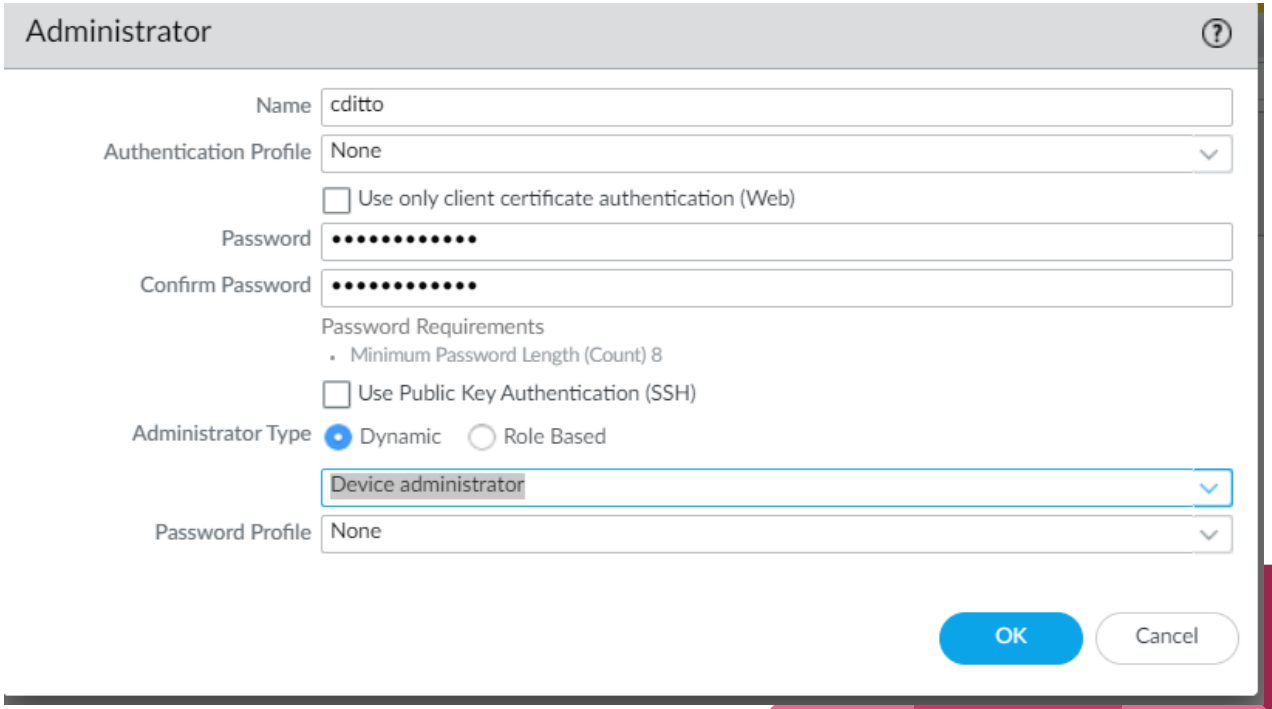
Once inside the GUI click on ‘Administrators’ and then on ‘Add’ at the bottom of the page



Palo Alto PA-440 Configuration

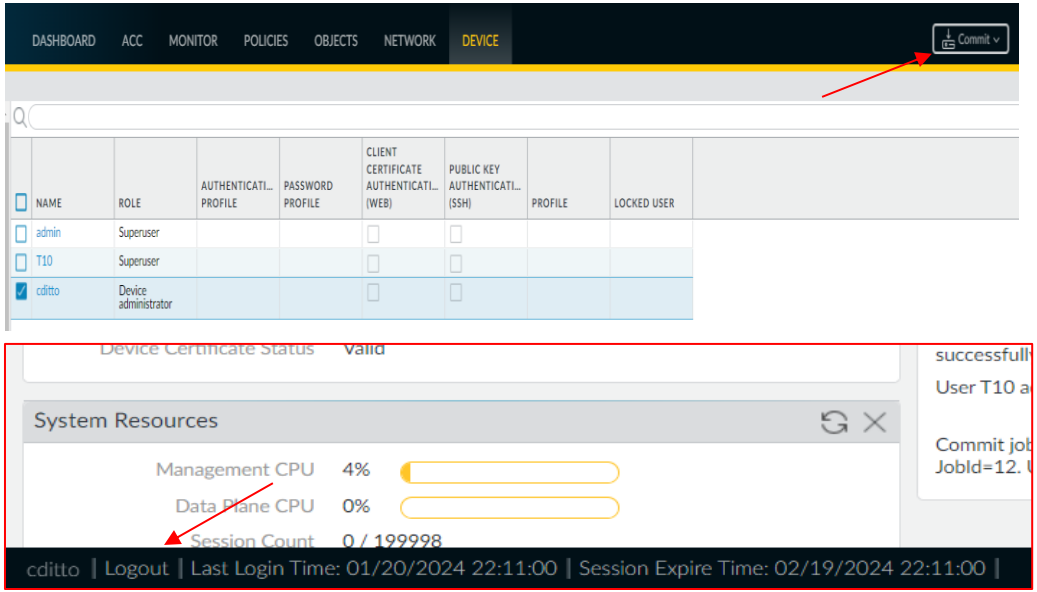
Create a new administrative account.

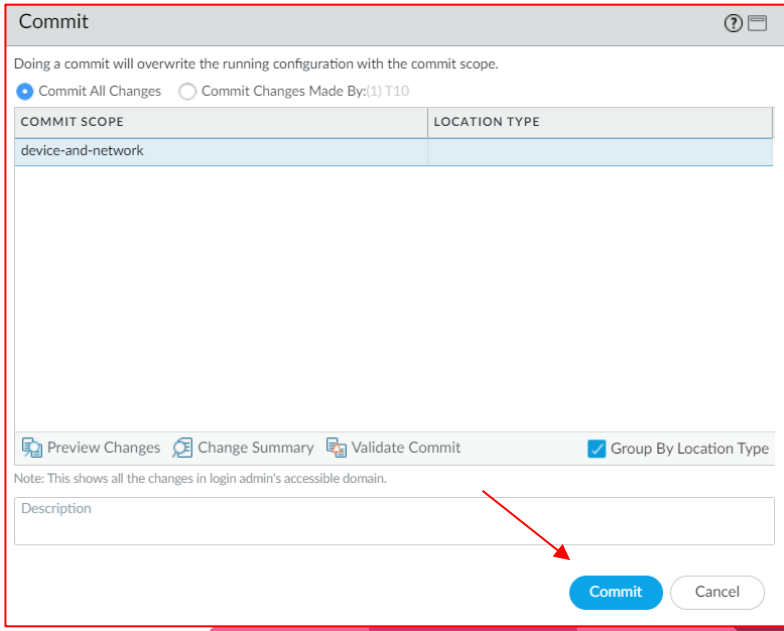
Each member off the team should create their own administrative account.



Palo Alto PA-440 Configuration

After Creating the new account commit your changes, log out using the button at the bottom left corner.





Palo Alto PA-440 Configuration

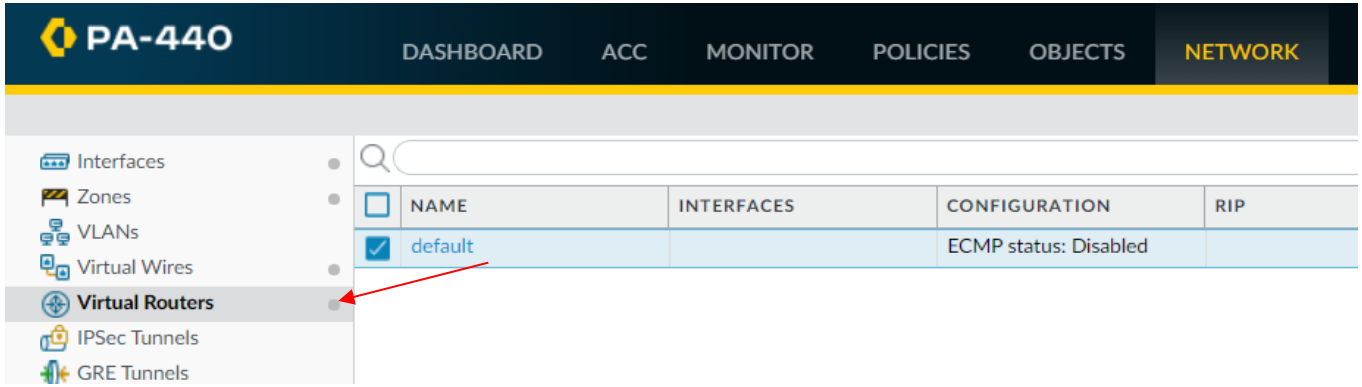
Log back in using the new credentials

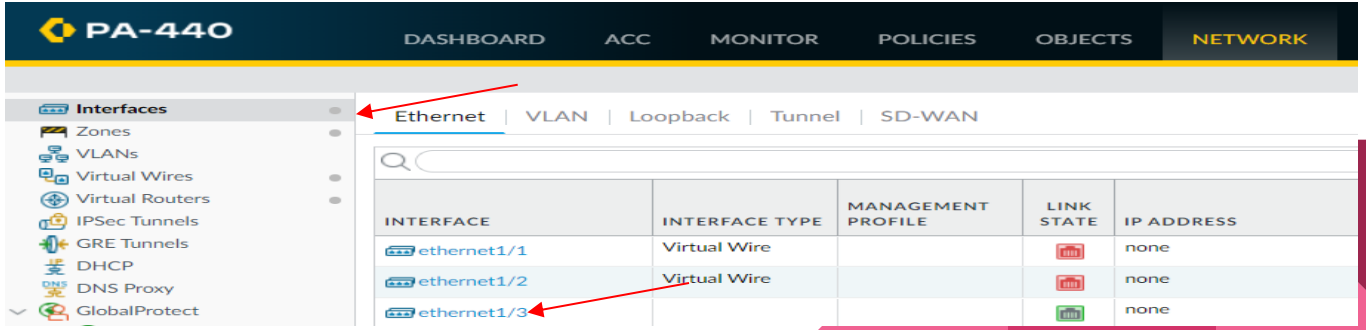
Palo Alto PA-440 Configuration

Select ‘Virtual Router’ from the left menu.

Use the default router unless instructed otherwise.

Select ‘Interfaces’,find the physical port labeled ‘ethernet1/3’ and click the label

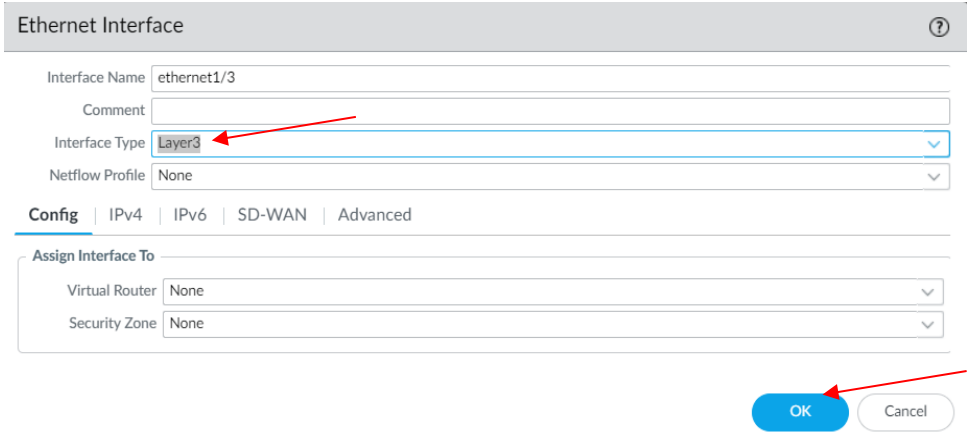


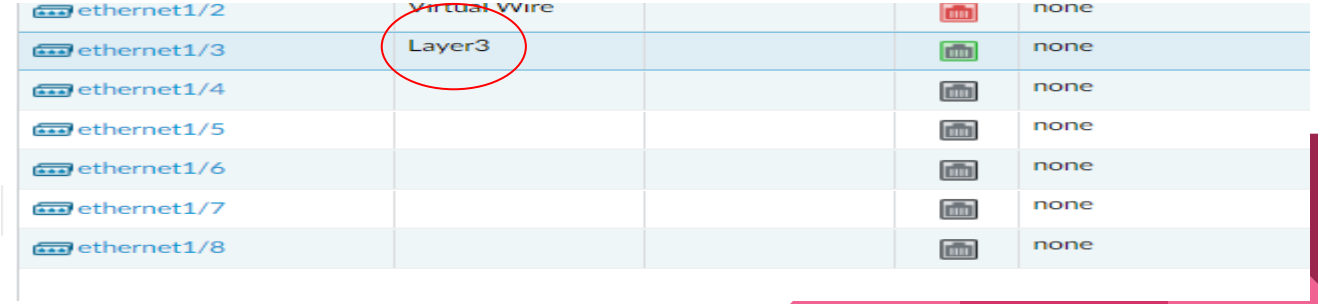


Palo Alto PA-440 Configuration

Change the ‘Interface Type’ to ‘Layer3’.

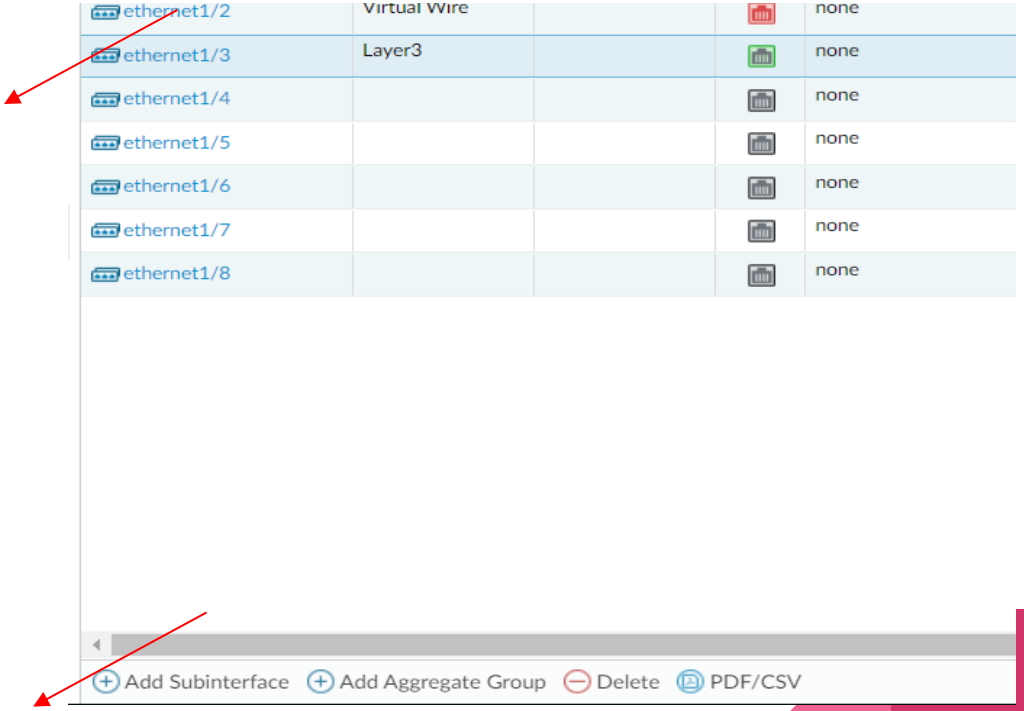
Click OK.





Palo Alto PA-440 Configuration

Highlight ‘ethernet1/3’ then click on ‘Add Subinterfaces’



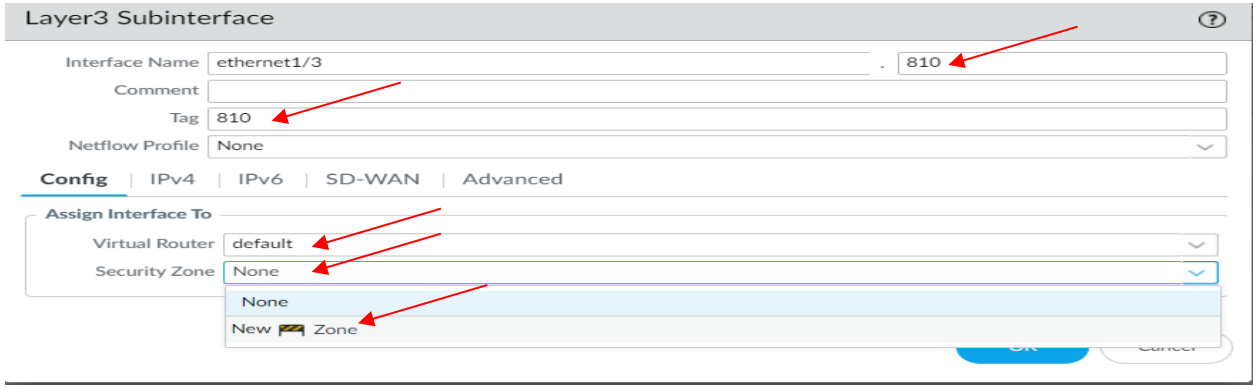
Palo Alto PA-440 Configuration

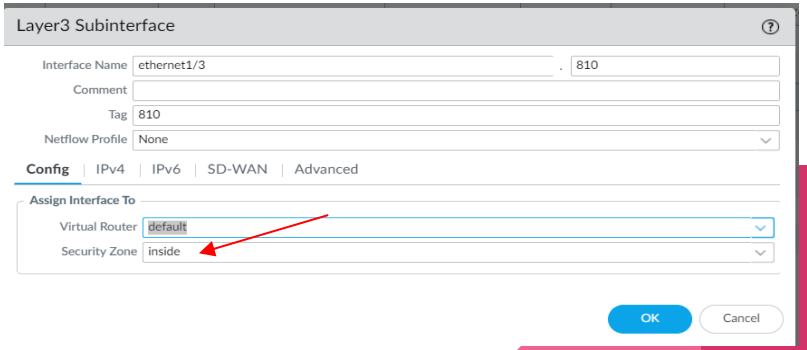
Click on the ‘Config’ tab

Add the subinterface number and duplicate for the tag as per best practice.

Add default to the ‘Virtual Router’ and then click on the dropdown in the Security Zone and add New Zone.

Change zone to ‘inside’.

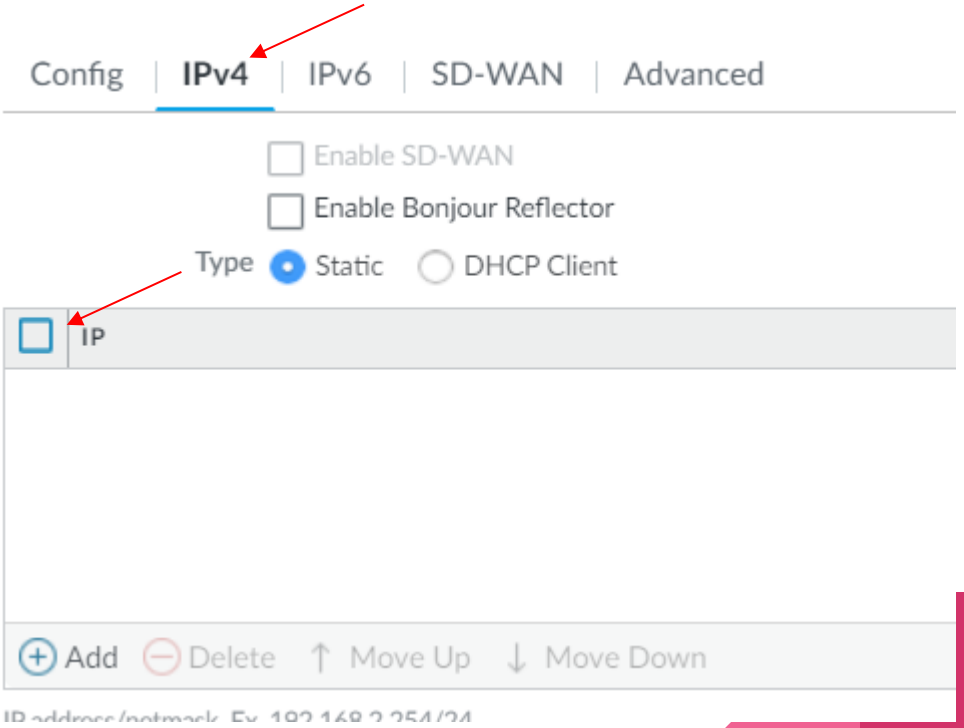




Palo Alto PA-440 Configuration

Select the ‘IPv4’ tab.

Select IP and add the IP address reserved for your teams firewall. Be sure to include the subnet mask suffix in CIDR notation.

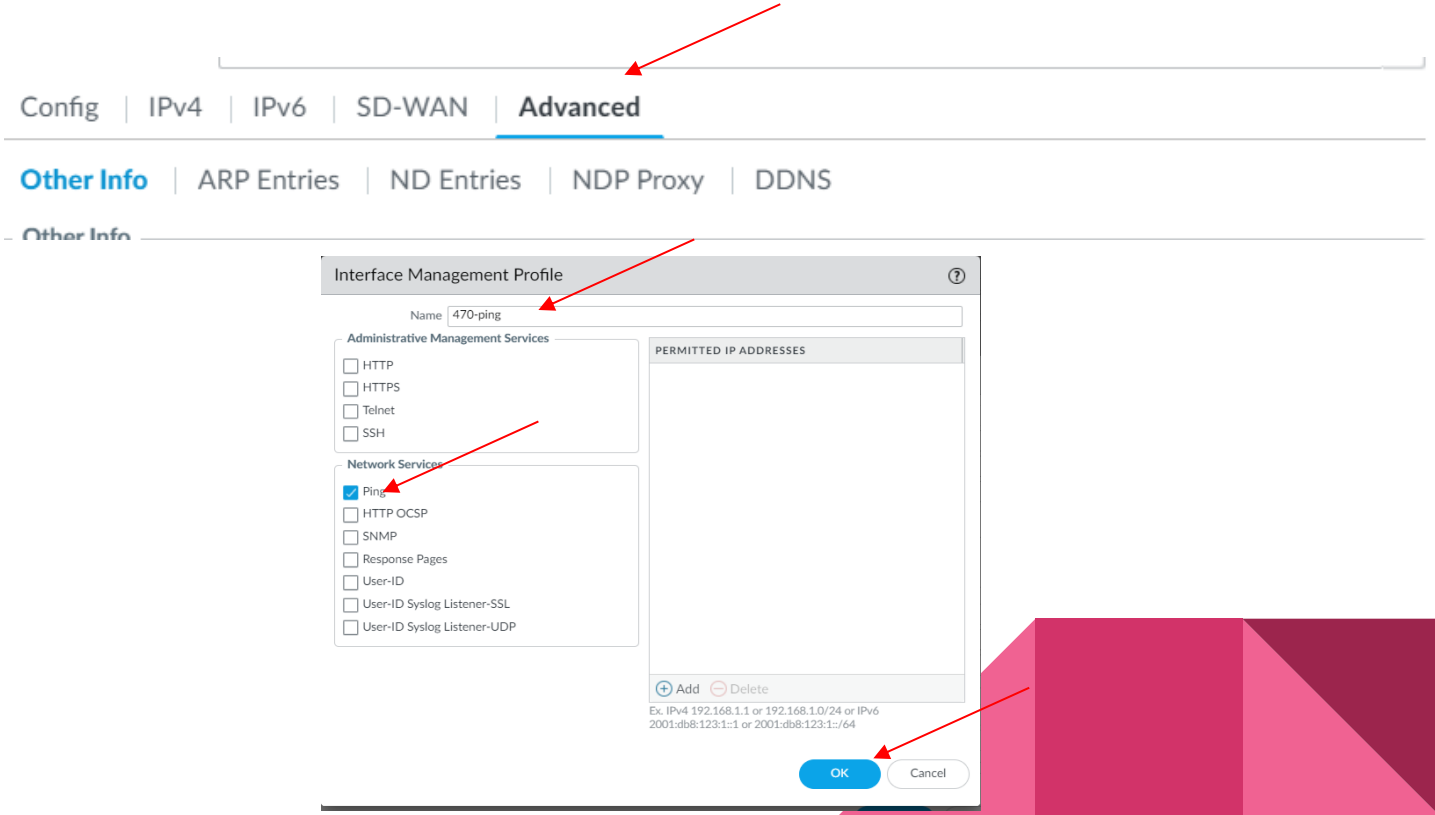


Palo Alto PA-440 Configuration

Select the ‘Advanced’ tab then select ‘Management Profile’

Create a profile named ‘470 pin’ and enable the ping option in that new profile.

Click OK.



Palo Alto PA-440 Configuration

Check your work in the interface table and adjust any misconfigurations.

ethernet1/3	Layer3			none	none	Untagged	none	none
ethernet1/3.510	Layer3	470-ping		192.168.200.1/24	default	510	none	interconnect
ethernet1/3.610	Layer3	470-ping		157.201.22.72/29	default	610	none	outside
ethernet1/3.710	Layer3	470-ping		192.168.201.1/24	default	710	none	dmz
ethernet1/3.810	Layer3	470-ping		192.168.202.1/24	default	810	none	inside

Palo Alto PA-440 Configuration

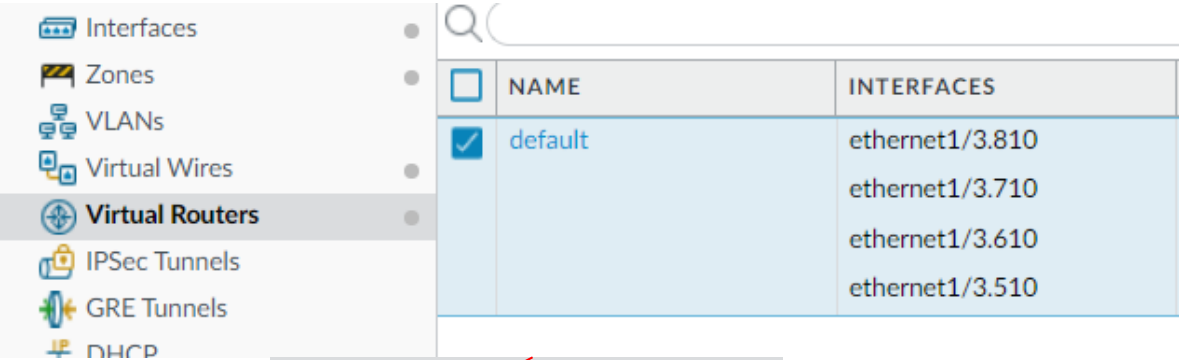
Select ‘Virtual Routers’ again then select the teams virtual router.

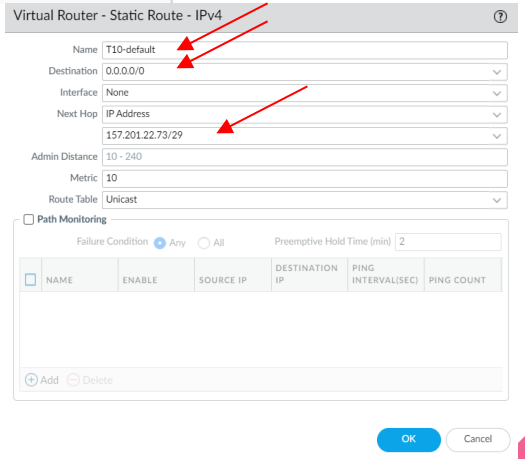
Click the ‘Static Route’ subtab, then create a new static route.

Name the route after your teams number and the word default.

The default route should be 0.0.0.0/0 which is the network ID for the whole internet.

The IP address of the next hop should be set to your teams assigned gateway router.





Palo Alto PA-440 Configuration

Virtual Router - Static Route - IPv4

Name	T10-default
Destination	0.0.0.0/0
Interface	None
Next Hop	IP Address
	157.201.22.73/29
Admin Distance	10 - 240
Metric	10
Route Table	Unicast

Path Monitoring

Failure Condition Any All Preemptive Hold Time (min) 2

NAME	ENABLE	SOURCE IP	DESTINATION IP	PING INTERVAL(SEC)	PING COUNT

Add Delete

OK Cancel

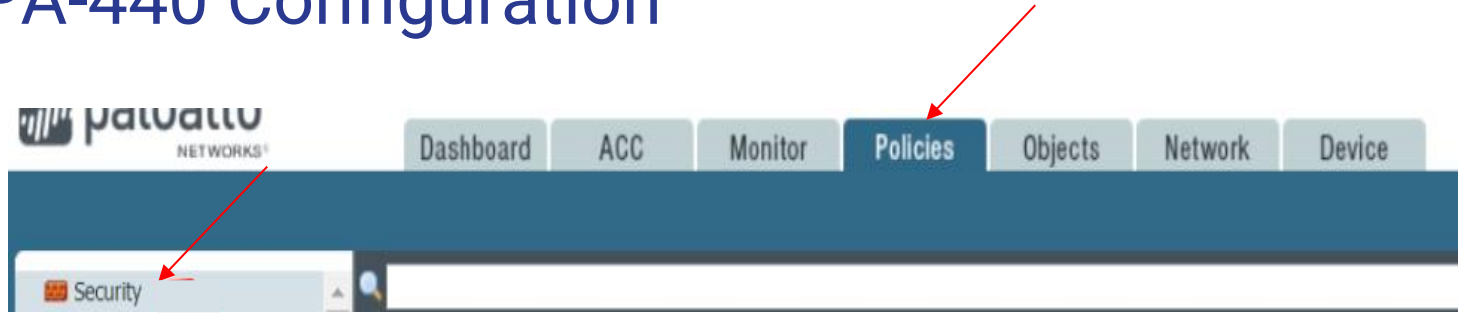
Palo Alto PA-440 Configuration

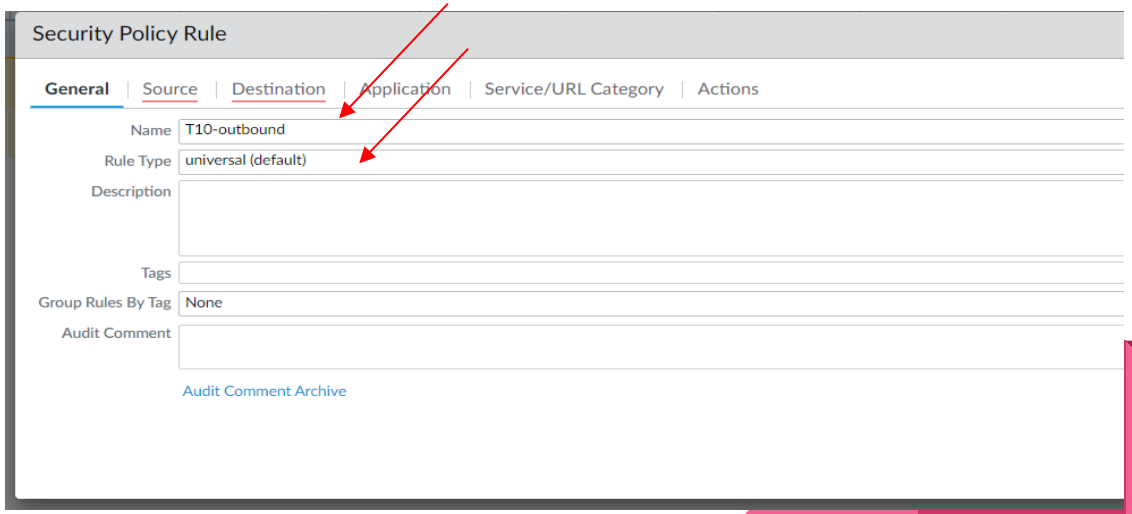
Click the ‘Policy’ tab.

Select ‘Security’ then click ‘Add’ at the bottom corner to set a new security rule.

You will set an outbound ‘client’ server that will allow inside zines to access Internet servers via your outside zone.

Set the name to your team name-Outbound and the rule type to universal.



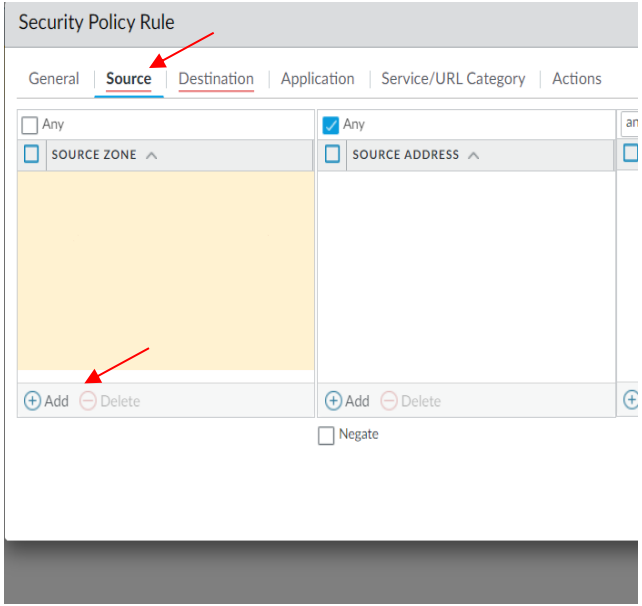


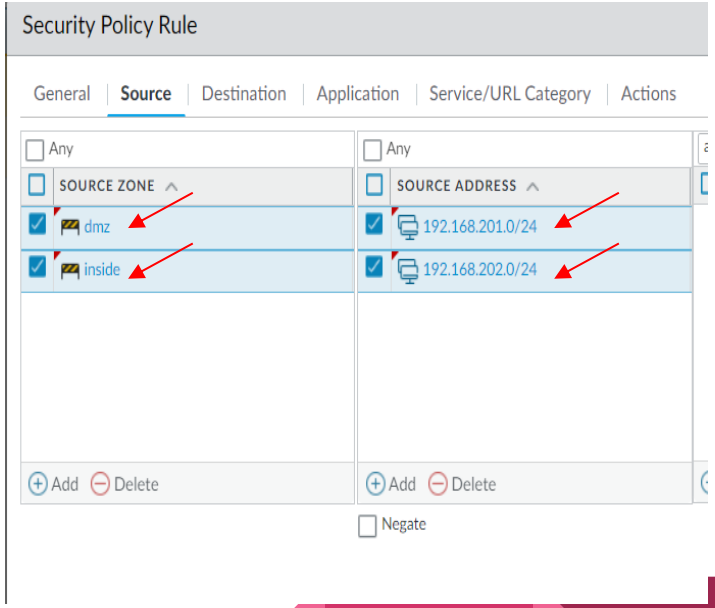
Palo Alto PA-440 Configuration

Select the ‘Source’ tab and then click on Add.

Add your DMZ, then click ‘Add’ then add your inside zone.

Under ‘Source Addresses’ click ‘Add’ and enter your teams DMZ subnet and the repeat with your inside zone subnet.

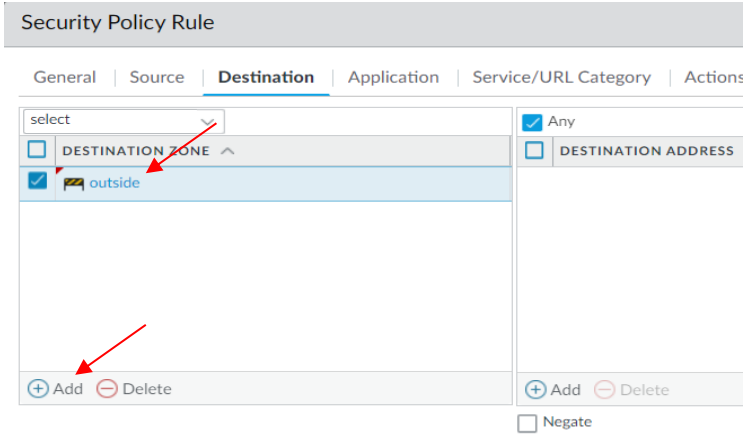


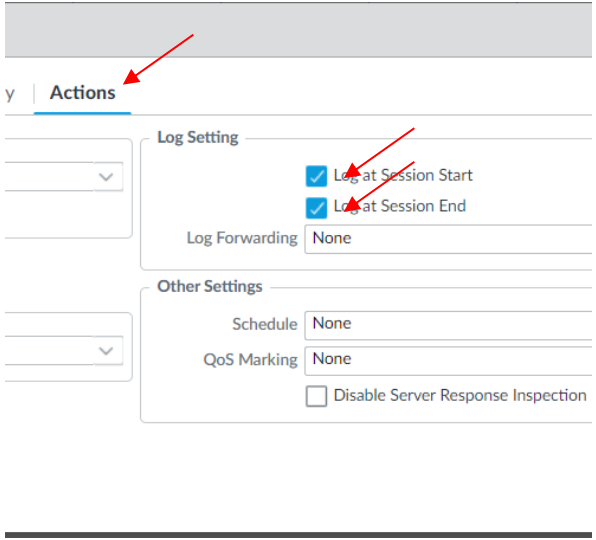


Palo Alto PA-440 Configuration

Select the ‘Destination’ tab then use the same procedure to add the outside zone

Select ‘Actions’ tab then check the ‘Log at Session Start’ and ’Log at Session End’ boxes.

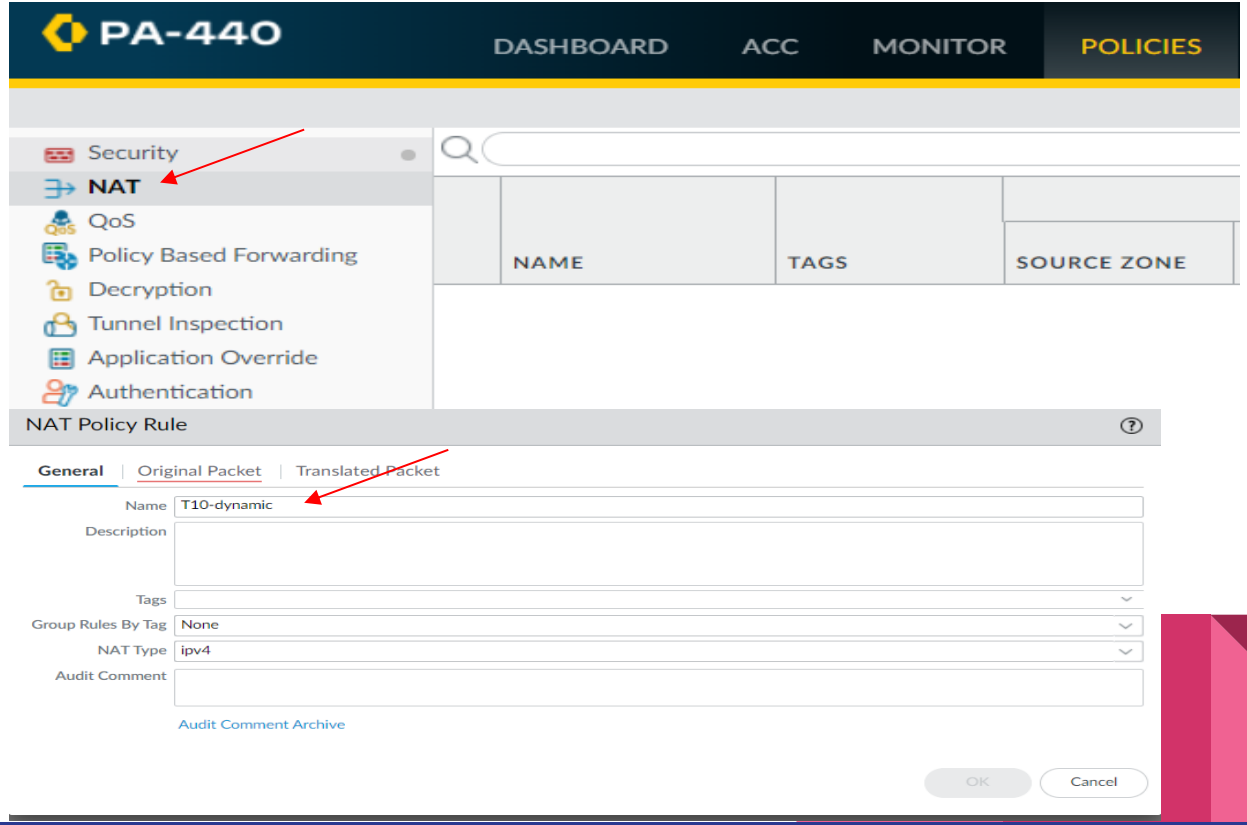




Palo Alto PA-440 Configuration

Select ‘NAT’ on the left and then select ‘Add’.

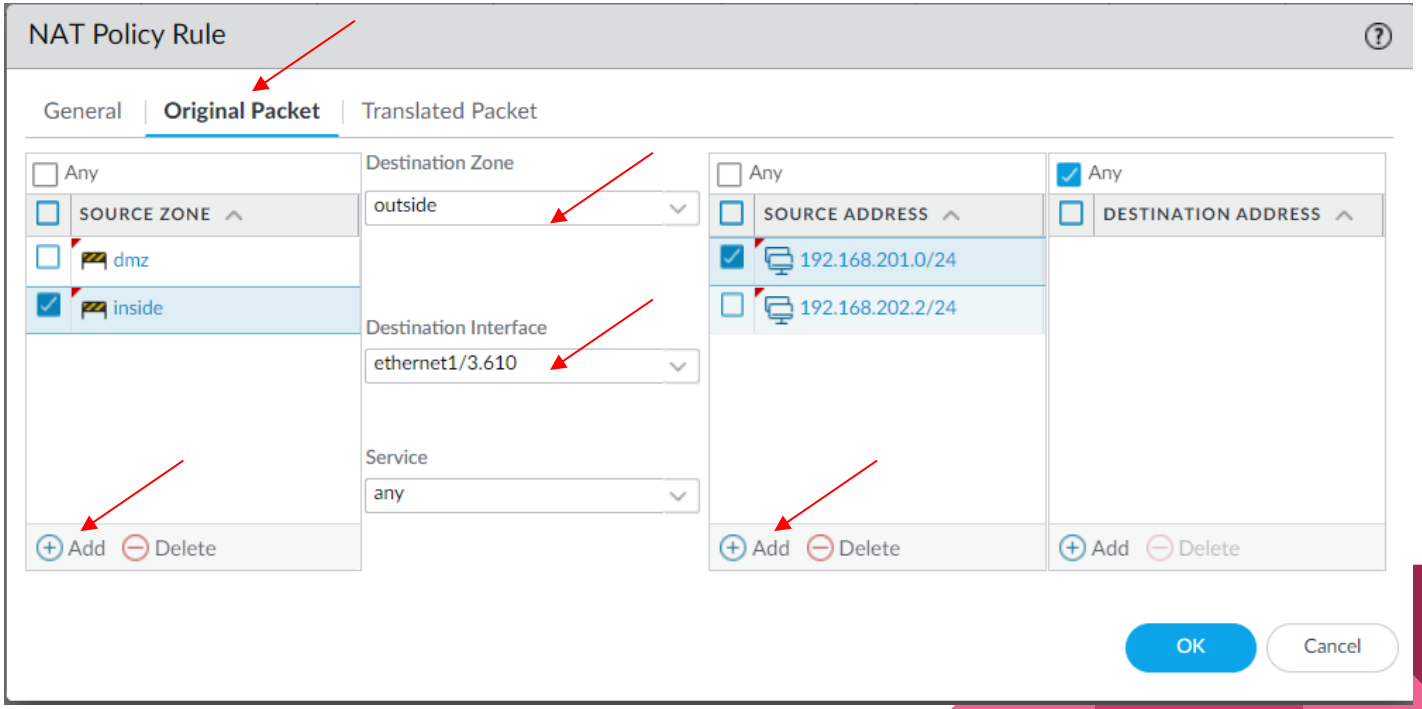
Under the ‘General’ tab name the new policy after your team name and the word dynamic.



Palo Alto PA-440 Configuration

Click the ‘Original Packet’ tab.

Specify the teams DMZ and inside zones as source zones and specify the correct numbered subinterface for the teams outside zone.



Palo Alto PA-440 Configuration

Select the ‘Translated Packet’ tab.

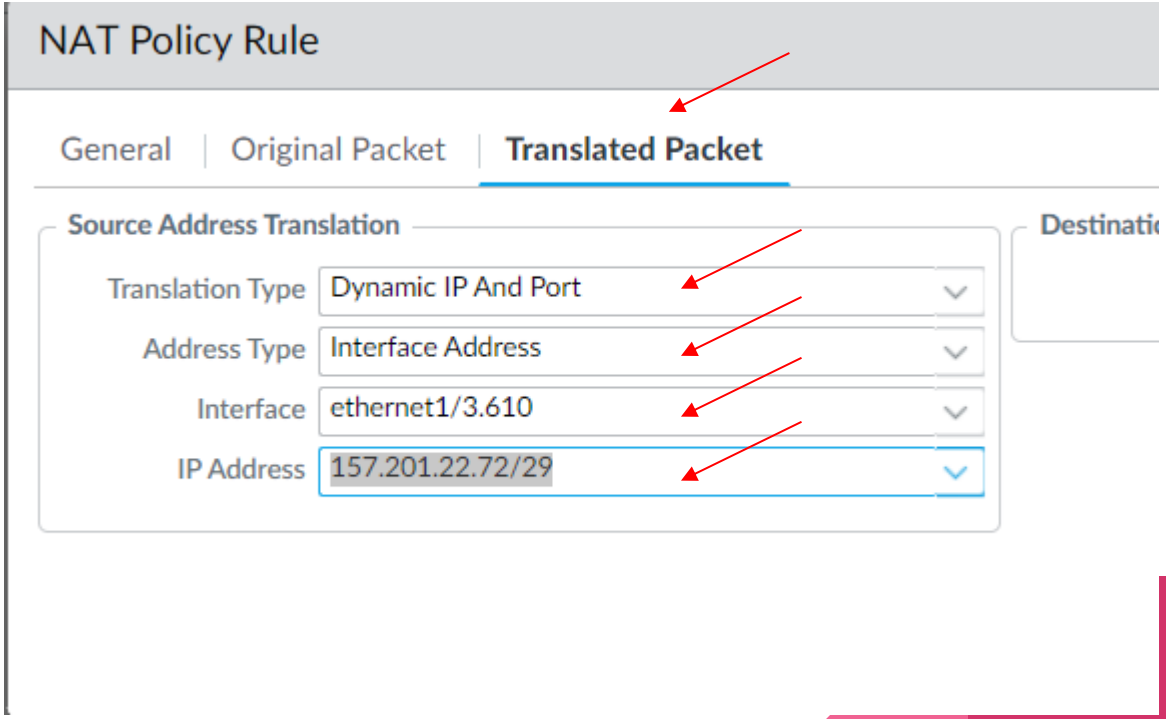
Change the ‘Transition Type’ to ‘Dynamic IP and Port’

Change the ‘Address’ to ‘Interface’

Specify the numbered subinterface of your outside zone Address’

Finally, select the IP address that was assigned to that subinterface.

Click OK

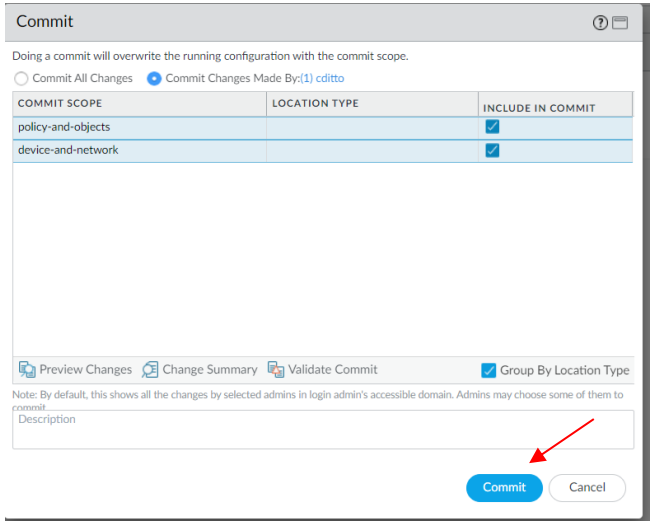


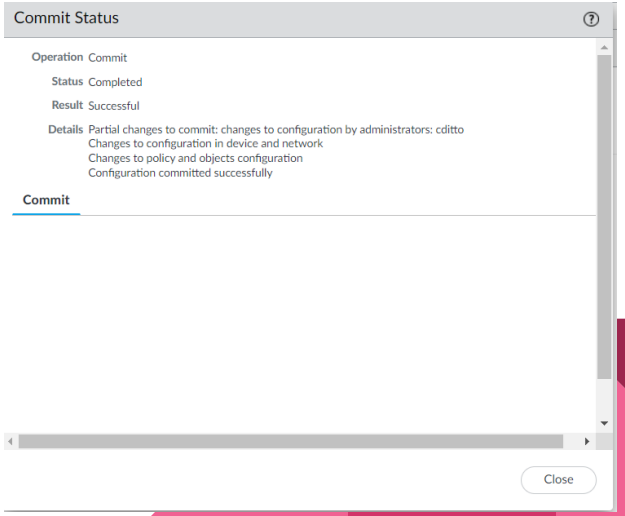
Palo Alto PA-440 Configuration

Review your new NAT rule

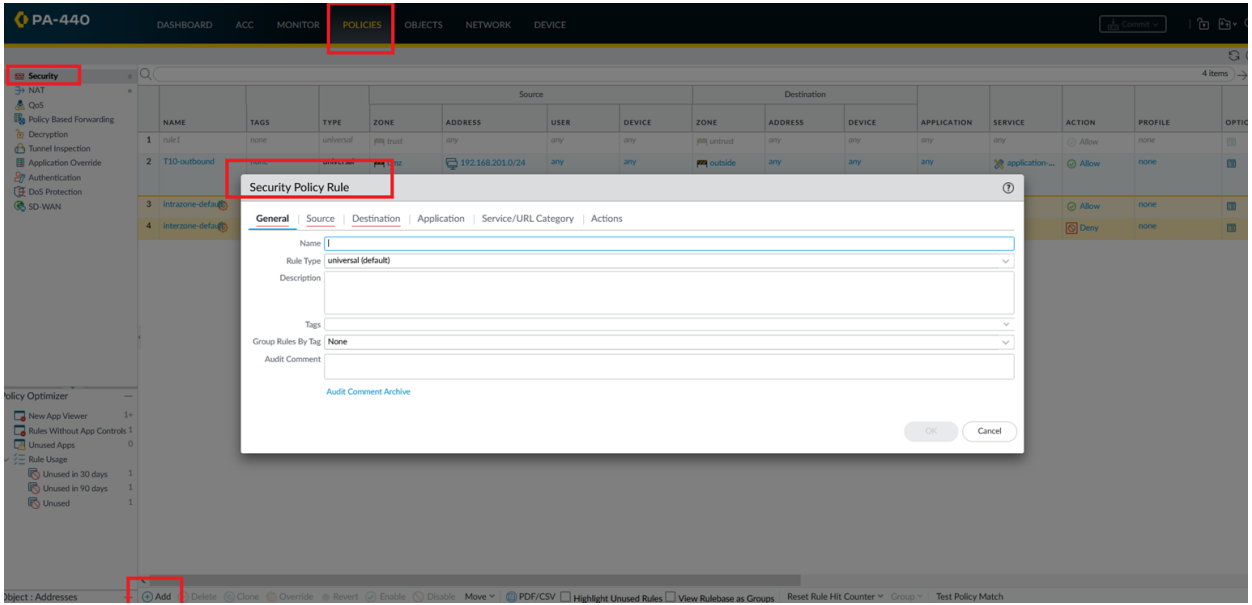
Commit your changes.

			Original Packet						Translated Packet	
	NAME	TAGS	SOURCE ZONE	DESTINATION ZONE	DESTINATION INTERFACE	SOURCE ADDRESS	DESTINATION ADDRESS	SERVICE	SOURCE TRANSLATION	DESTINATION TRANSLATION
1	T10-dynamic	none	dmz inside	outside	ethernet1/3.610	192.168.201.0... 192.168.202.2...	any	any	dynamic-ip-and-port ethernet1/3.610 157.201.22.72/29	none

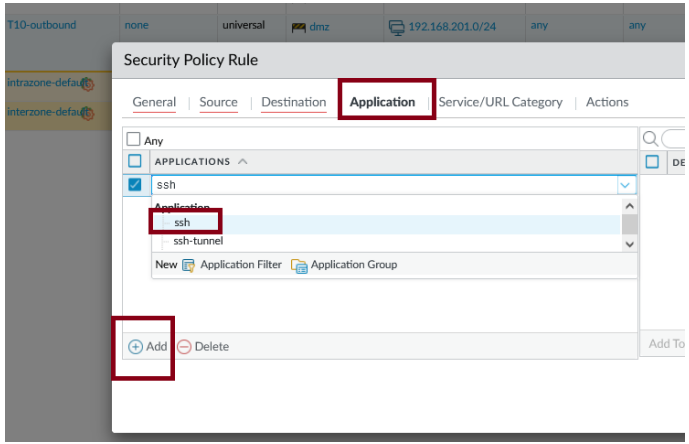


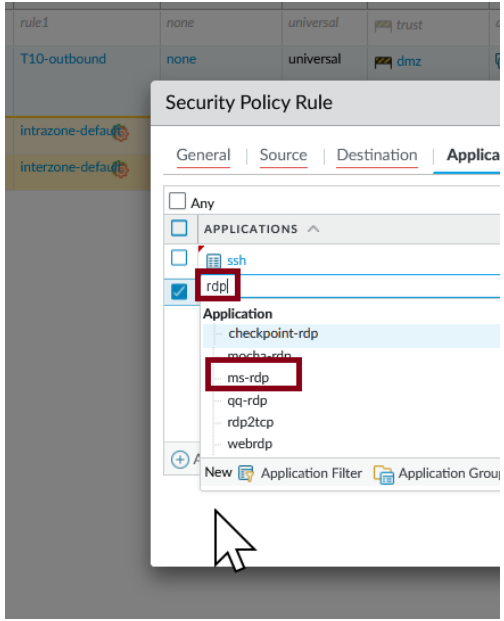


Add a Security Policy for Applications ssh and remote access to give access from DMZ to inside Zone.

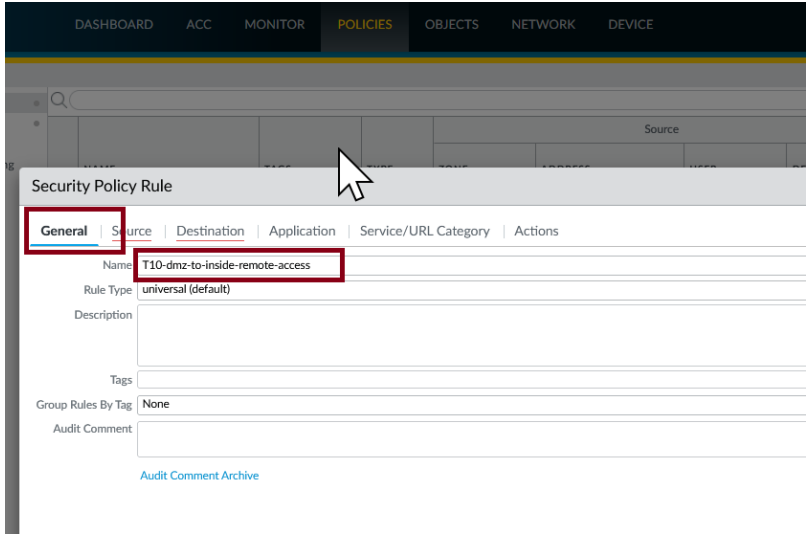


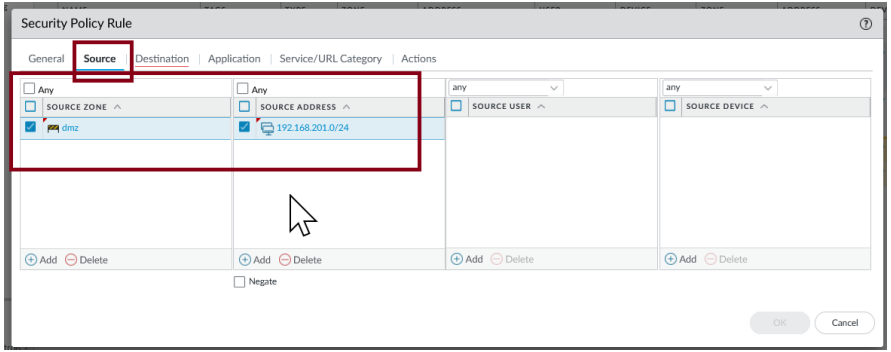
Add a Security Policy for Applications ssh and remote access to give access from DMZ to inside Zone.



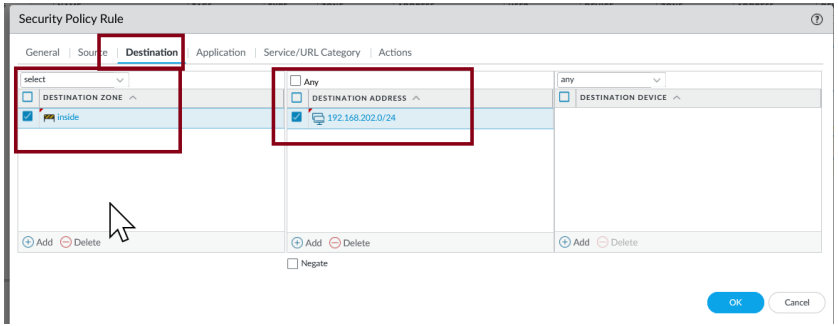


Add a Security Policy for Applications ssh and remote access to give access from DMZ to inside Zone.



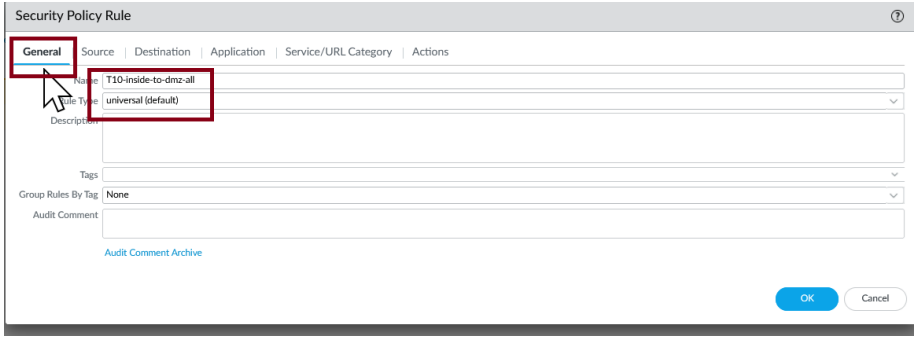


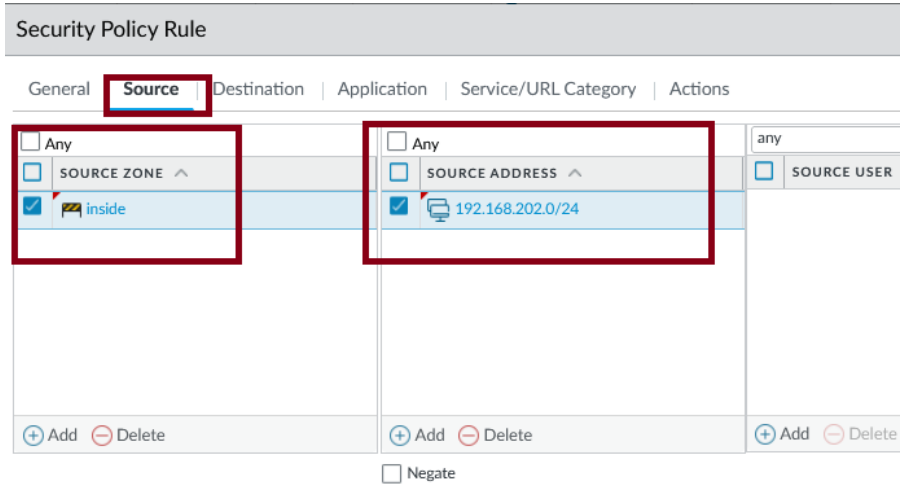
Add a Security Policy for Applications ssh and remote access to give access from DMZ to inside Zone.



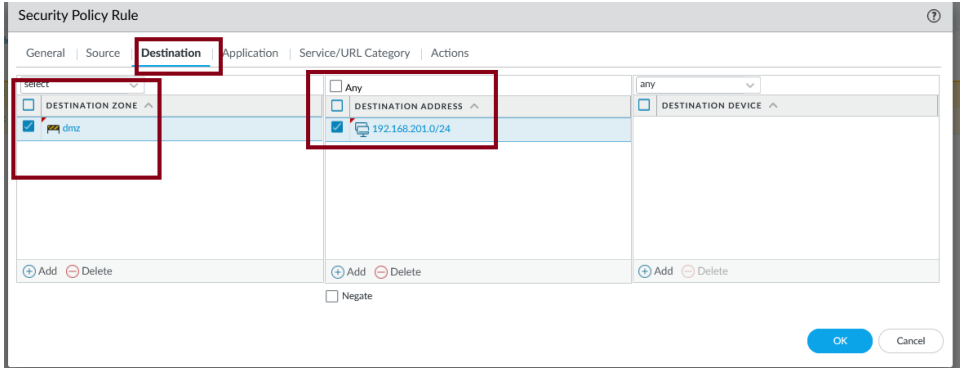
	NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE
1	rule1	none	universal	trust	any	any	any	untrust	any	any	any	any	Allow	none
2	T10-outbound	none	universal	dmz inside	192.168.201.0/24 192.168.202.0/24	any	any	outside	any	any	any	application-...	Allow	none
3	T10-dmz-to-inside-r...	none	universal	dmz	192.168.201.0/24	any	any	inside	192.168.202.0...	any	ms-rdp ssh	application-...	Allow	none
4	intrazone-defau	none	intrazone	any	any	any	any	(intrazone)	any	any	any	any	Allow	none
5	interzone-defau	none	interzone	any	any	any	any	any	any	any	any	any	Deny	none

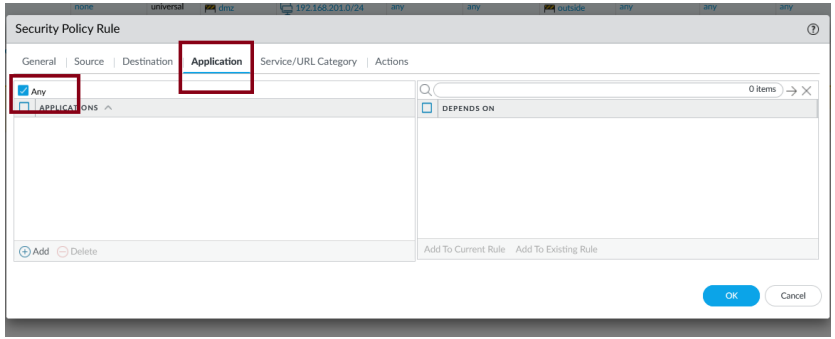
Add a Policy Rule to allow all traffic from inside towards DMZ.



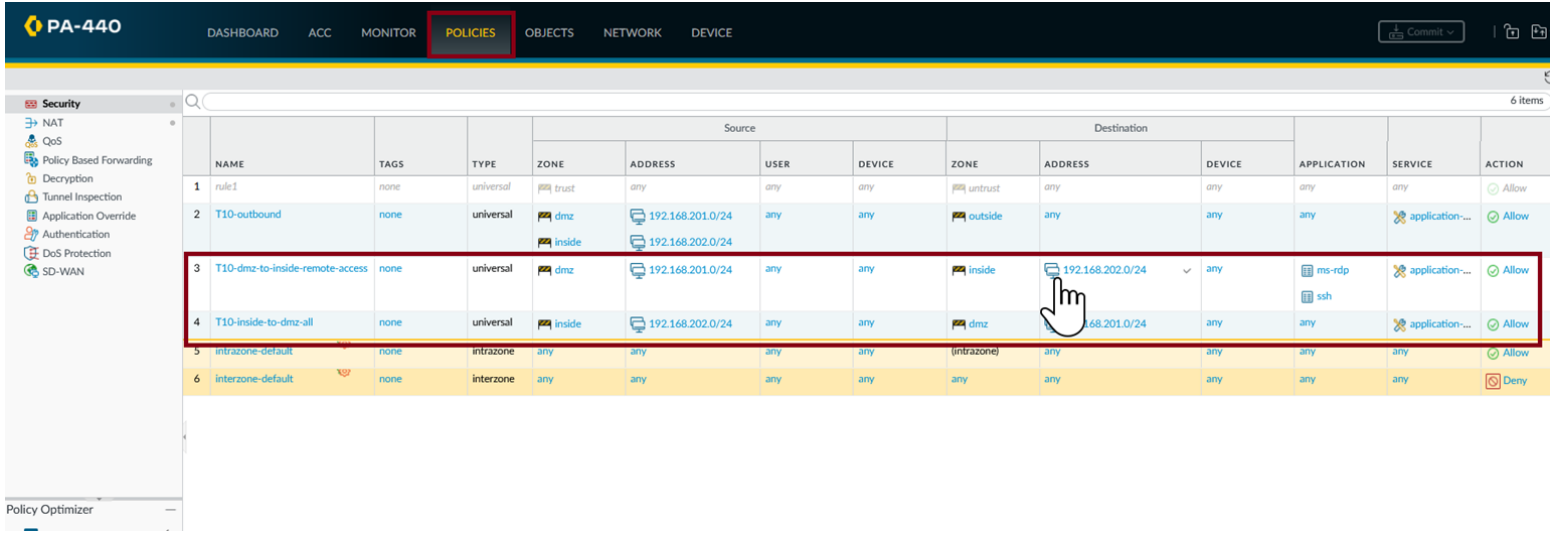


Add a Policy Rule to allow all traffic from inside towards DMZ.



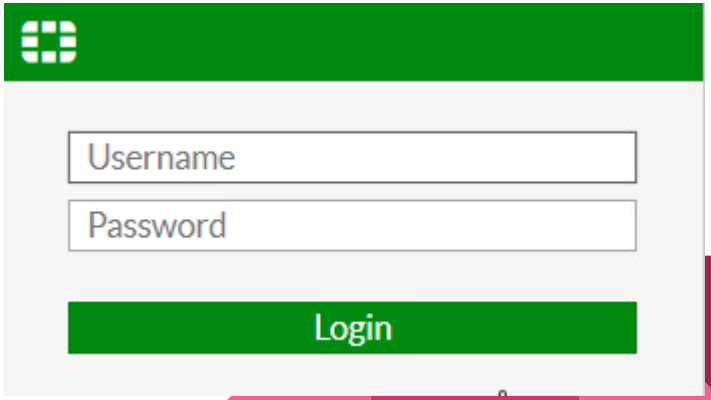


The new rules created for Remote Desktop and for the intern zone.

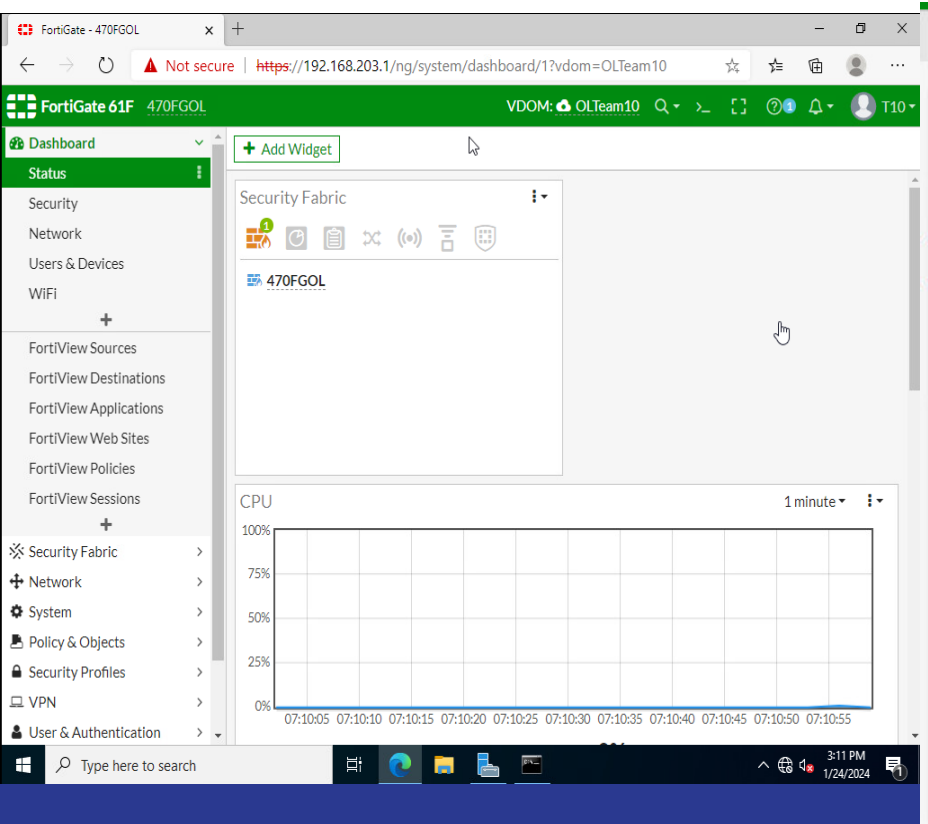


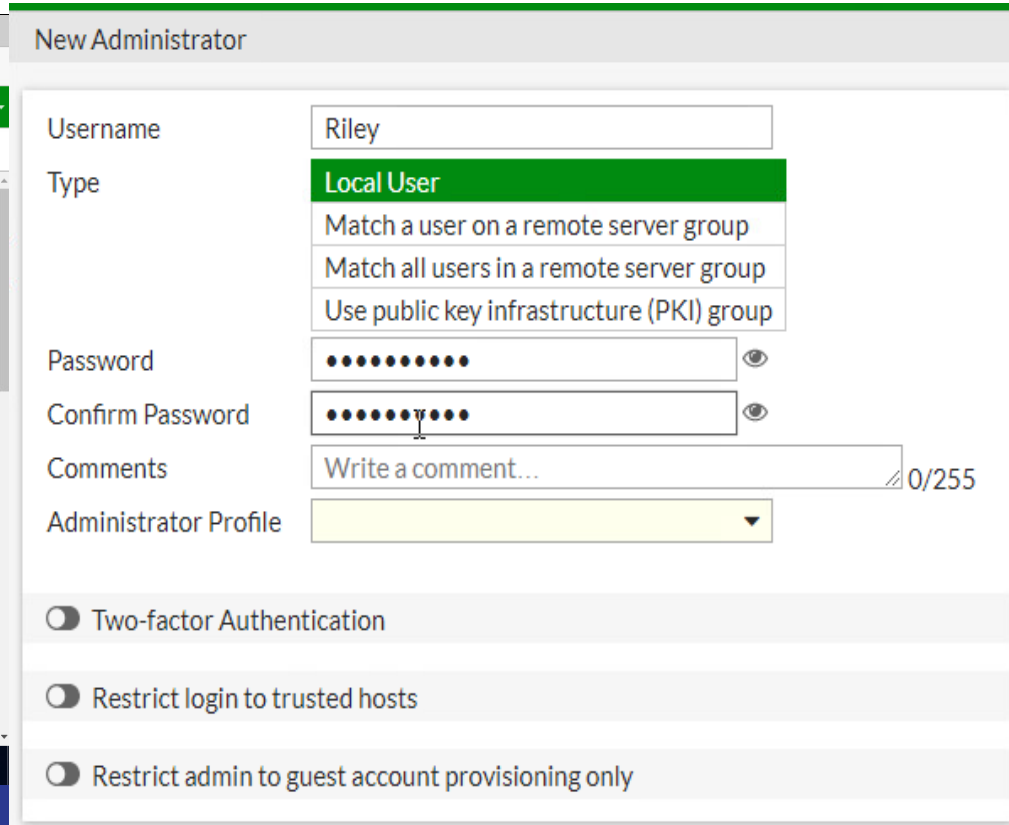
Fortigate Configurations

Connect to your windows secure server and connect to Fortigate by using a web browser and entering the ip address for your gateway. You should have the login credentials

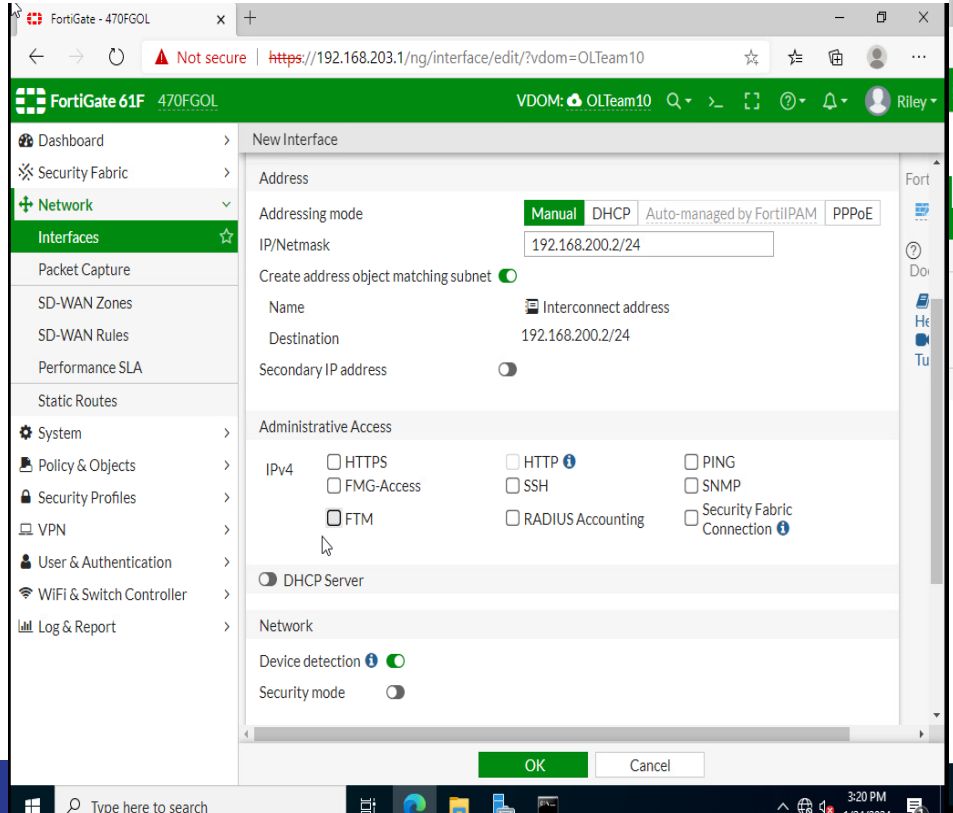


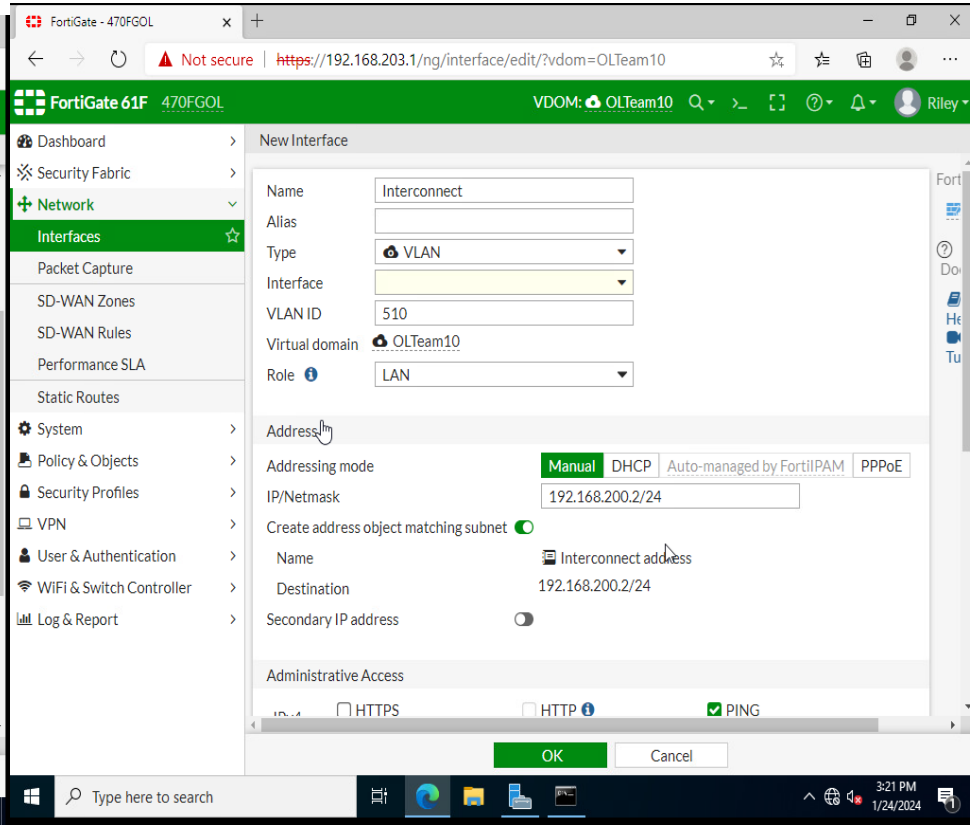
Go to System Administrator and make new Admin account for yourself



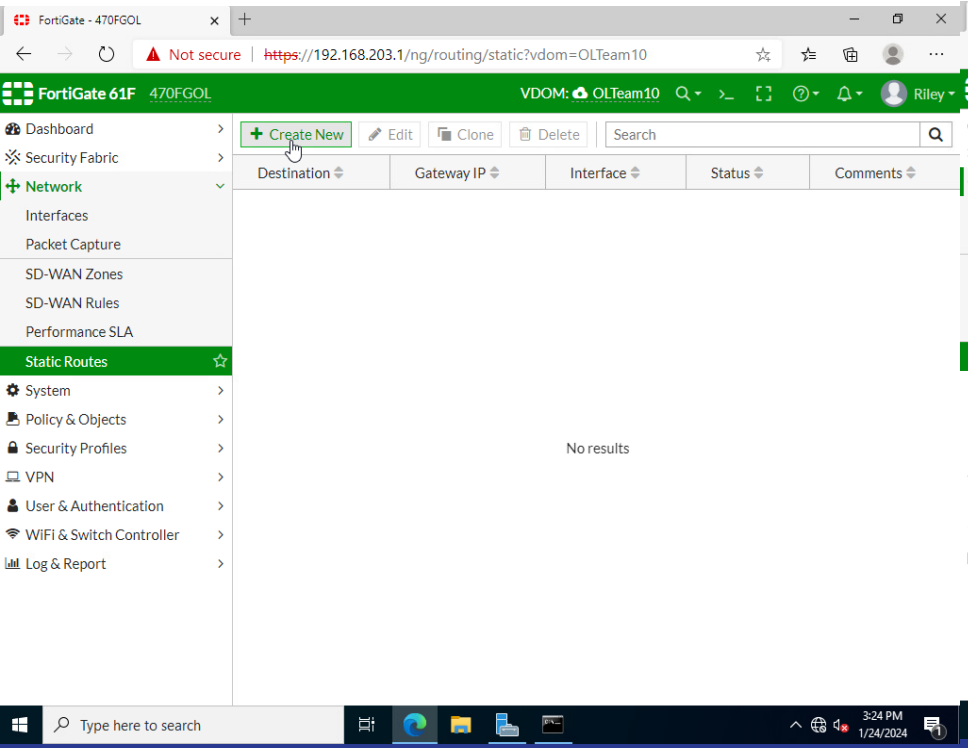


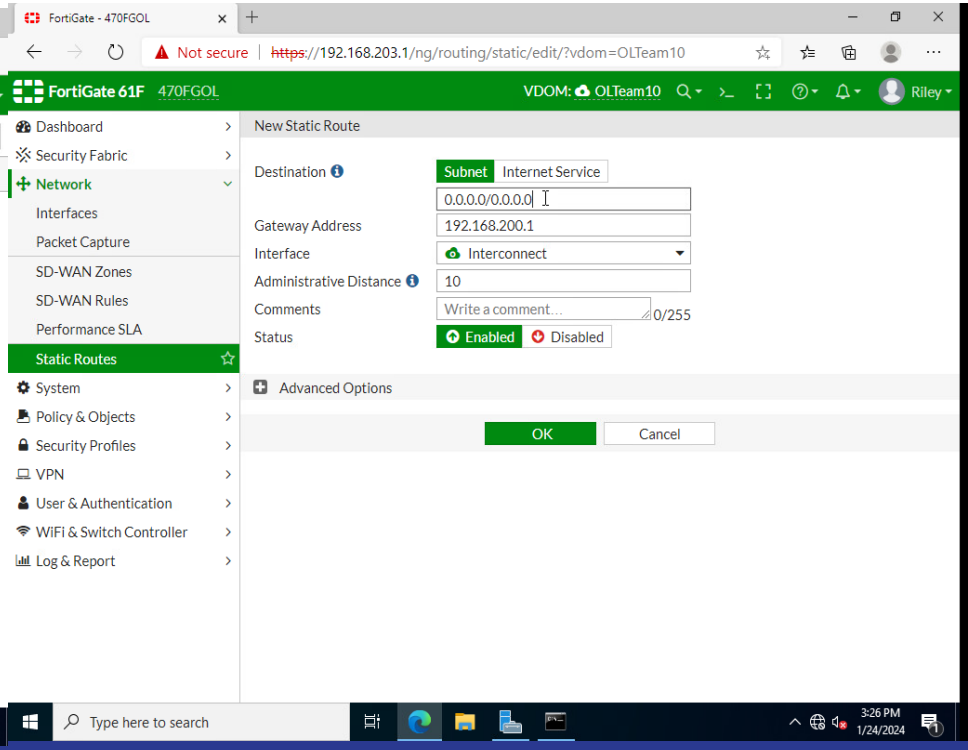
Go to Interface and make new one for the interconnect Zone making sure to fill out the vlan and Ip info and enabling ping





Make a Static route going to the Palo Altos Firewall in the interconnect zone





Go to Policy & Object select address and choose new address and add an object for each zone

FortiGate - 470FGOL

Not secure | https://192.168.203.1/ng/firewall/address/edit?vdom=OLTeam10

FortiGate 61F 470FGOL VDOM: OLTeam10 Riley

- Dashboard
- Security Fabric
- Network
- System
- Policy & Objects
  - Firewall Policy
  - Addresses
  - Internet Service Database
  - Services
  - Schedules
  - Virtual IPs
  - IP Pools
  - Protocol Options
  - Traffic Shapers
  - Traffic Shaping Policy
  - Traffic Shaping Profile
- Security Profiles
- VPN
- User & Authentication
- WiFi & Switch

New Address

Name	DMZ
Color	Change
Type	Subnet
IP/Netmask	192.168.201.0/24
Interface	any
Static route configuration	
Comments	Write a comment... 0/255

OK Cancel

FortiGate

470FGOL

Dynamic Address

Guides

- Configuring an AWS Dynamic Address
- Configuring an Azure Dynamic Address
- Configuring a Google Cloud Platform Dynamic Address
- Configuring an Oracle Cloud Infrastructure Dynamic Address
- Configuring an OpenStack Dynamic Address

Documentation

- Online Help
- Video Tutorials

Type here to search

3:31 PM 1/24/2024

Inside of Policy & Objects select Firewall policies and make an outbound and rdp/ssh policies using the new object you made.

FortiGate - 470FGOL

Not secure | https://192.168.203.1/ng/firewall/policy/policy/standard/edit/?vdom=...

FortiGate 61F 470FGOL VDOM: OLTeam10 Riley

- Dashboard
- Security Fabric
- Network
- System
- Policy & Objects
  - Firewall Policy
  - Addresses
  - Internet Service Database
  - Services
  - Schedules
  - Virtual IPs
  - IP Pools
  - Protocol Options
  - Traffic Shapers
  - Traffic Shaping Policy
  - Traffic Shaping Profile
- Security Profiles
- VPN
- User & Authentication
- WiFi & Switch

New Policy

Name	Outbound-all
Incoming Interface	T10-secure (T10-secure)
Outgoing Interface	Interconnect
Source	Secure
Destination	DMZ, Inside
Schedule	always
Service	ALL
Action	ACCEPT / DENY
Inspection Mode	Flow-based / Proxy-based

Firewall / Network Options

NAT

Protocol Options: PROT default

Documentation

- Online Help
- Video Tutorials
- Consolidated Policy Configuration

OK Cancel

New Policy

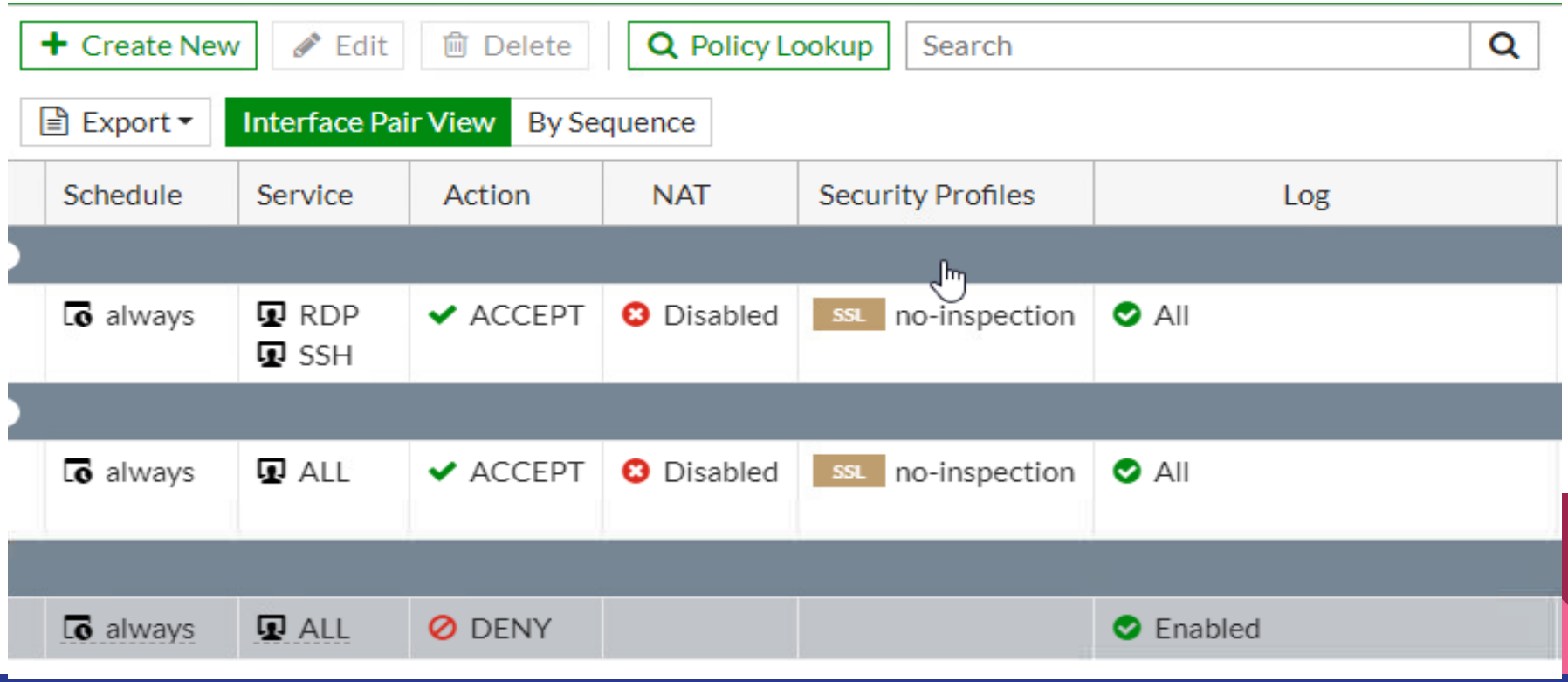
Name	incoming-remoteadmin
Incoming Interface	Interconnect
Outgoing Interface	T10-secure (T10-secure)
Source	DMZ, Inside
Destination	Secure
Schedule	always
Service	RDP, SSH
Action	ACCEPT / DENY
Inspection Mode	Flow-based / Proxy-based

Firewall / Network Options

NAT

Protocol Options: PROT default

Review all the Policies and enable ALL for logging

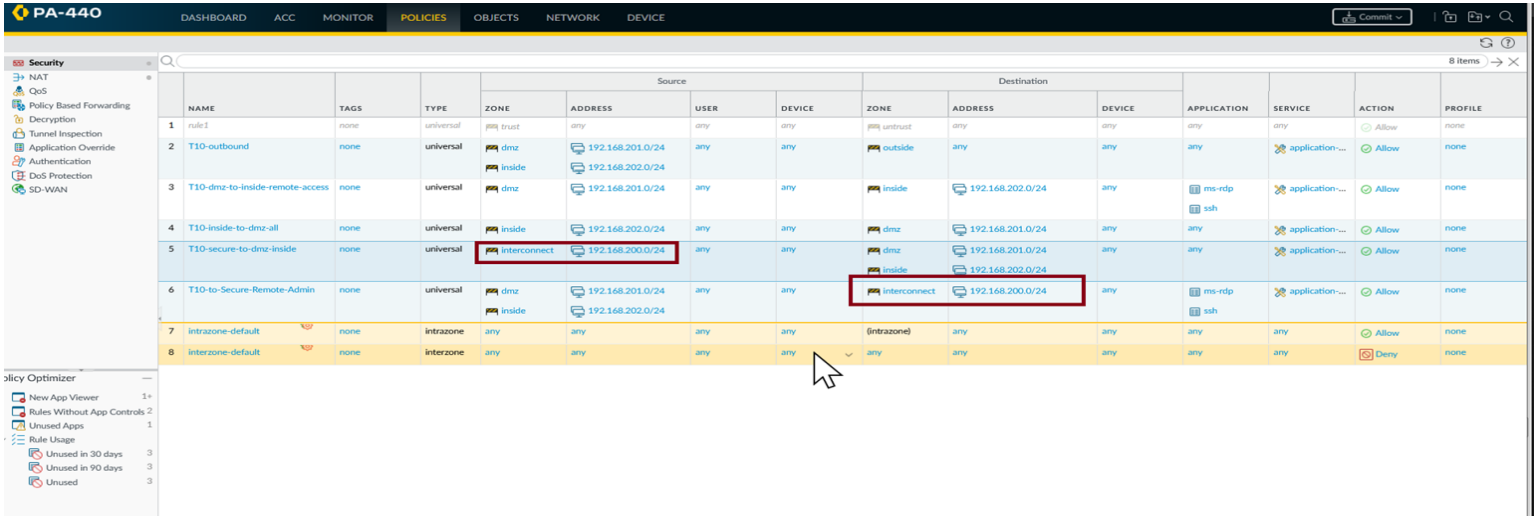


Challenges we faced

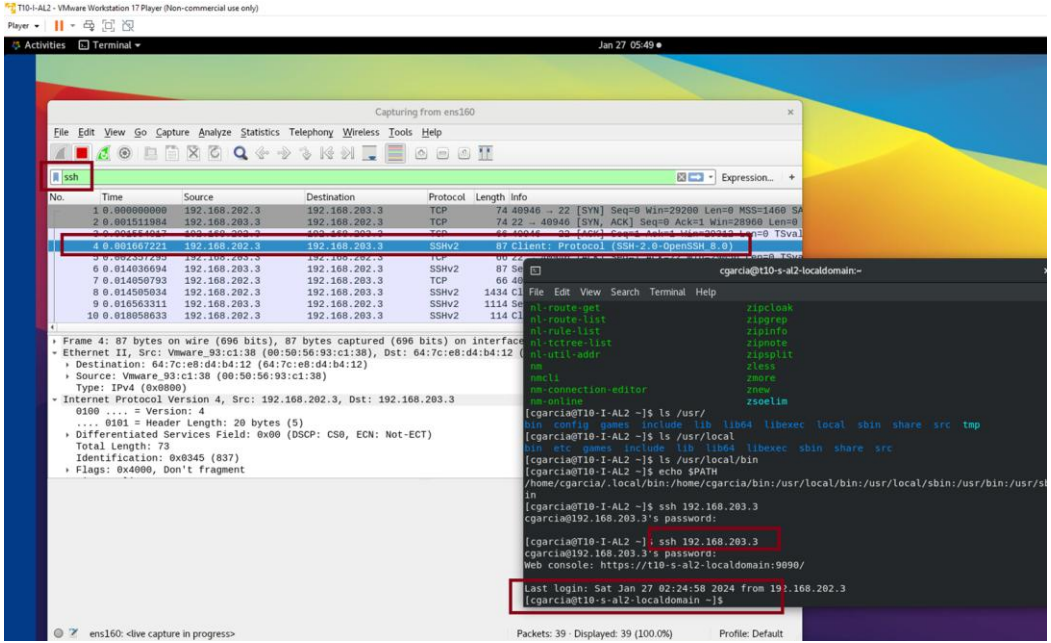
Misconfiguration in Palo Alto firewall.

We didn't have connections from the secure zone since we configure Palo Alto policy with the ip range from the firewall instead of the secure zone. We find the problem when we review our diagram and tested the change.

Was corrected from 192.168.200.0/24 to 192.168.203.0/24.



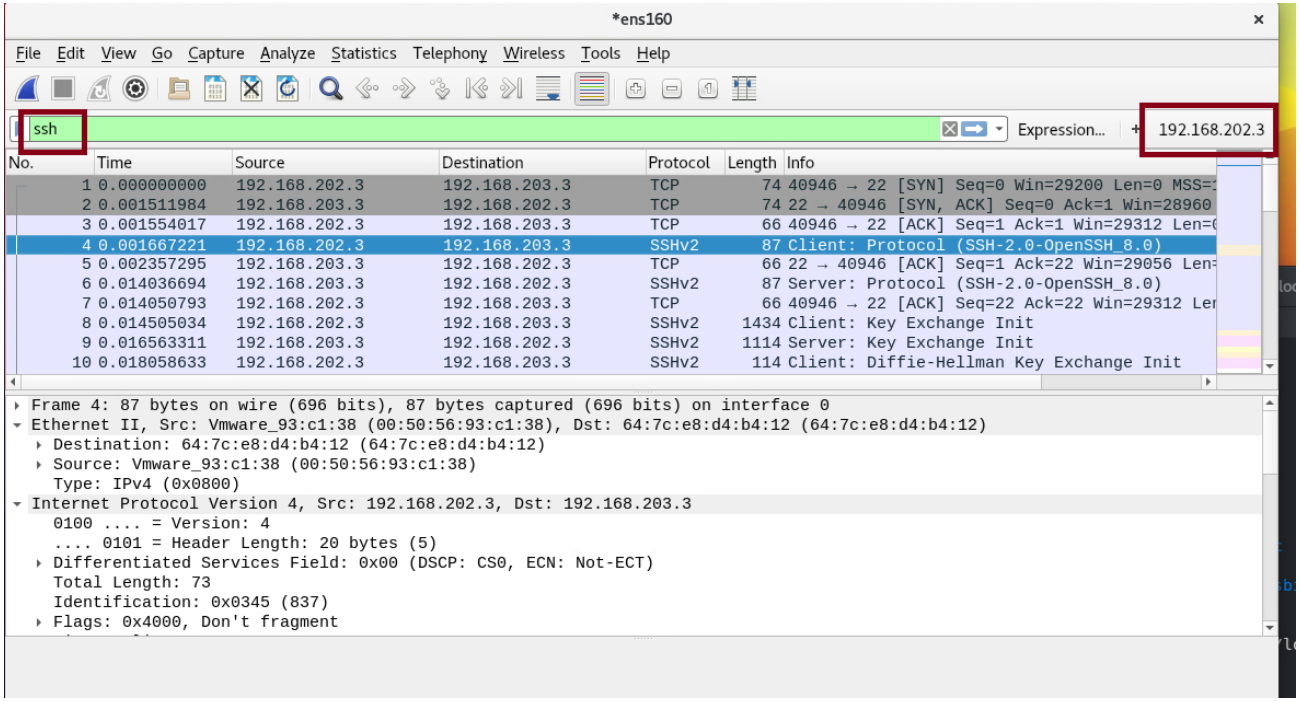
Linux SSH connections $PATH problems.



On the Linux systems on intern, the ssh connection where established towards secure zone, but the terminal just stale without showing the terminal in the secure zone we were connecting.

After checking ssh packages in that machine using Wireshark we realized that the connection exist, and that means that the problem was not in the firewalls, but in the ssh configuration on the Linux we run ssh. We run ssh with the full path (/usr/bin/ssh) and worked. The misconfiguration was in the $PATH to ssh.

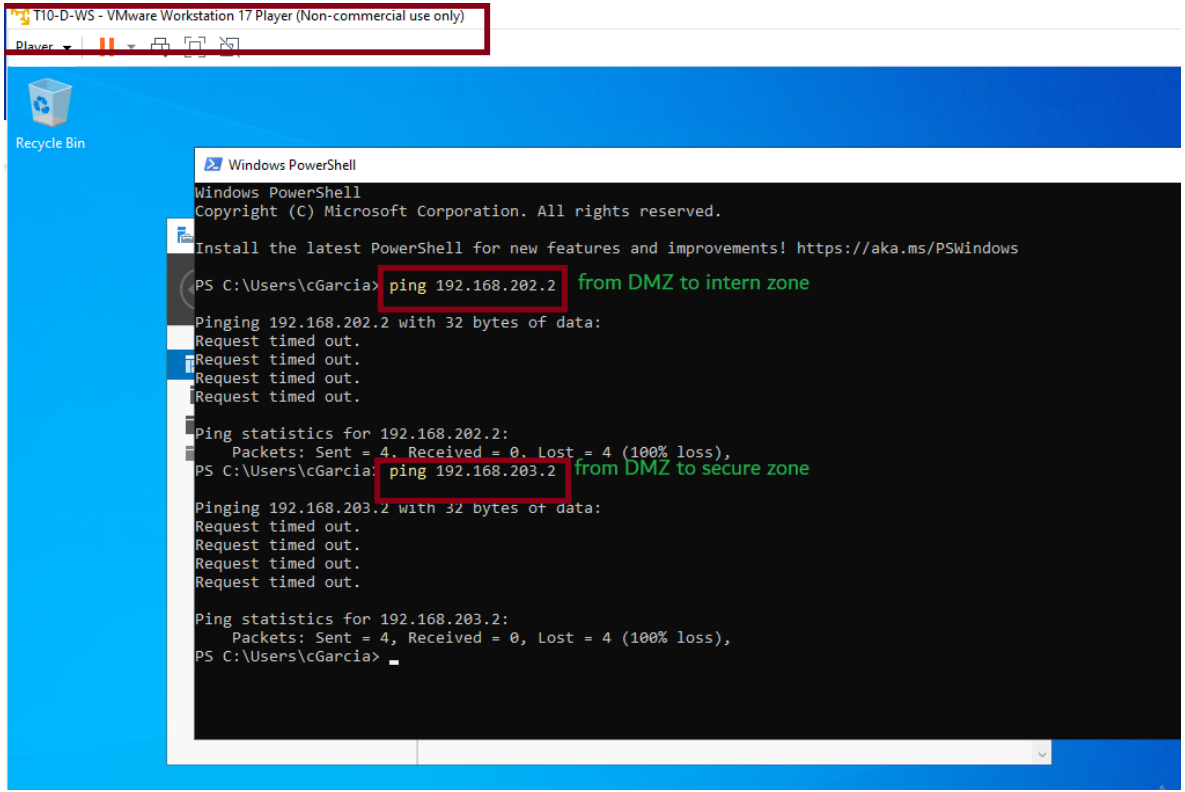
Linux SSH connections $PATH problems.



Use of filters on Wireshark to isolate ssh connections.

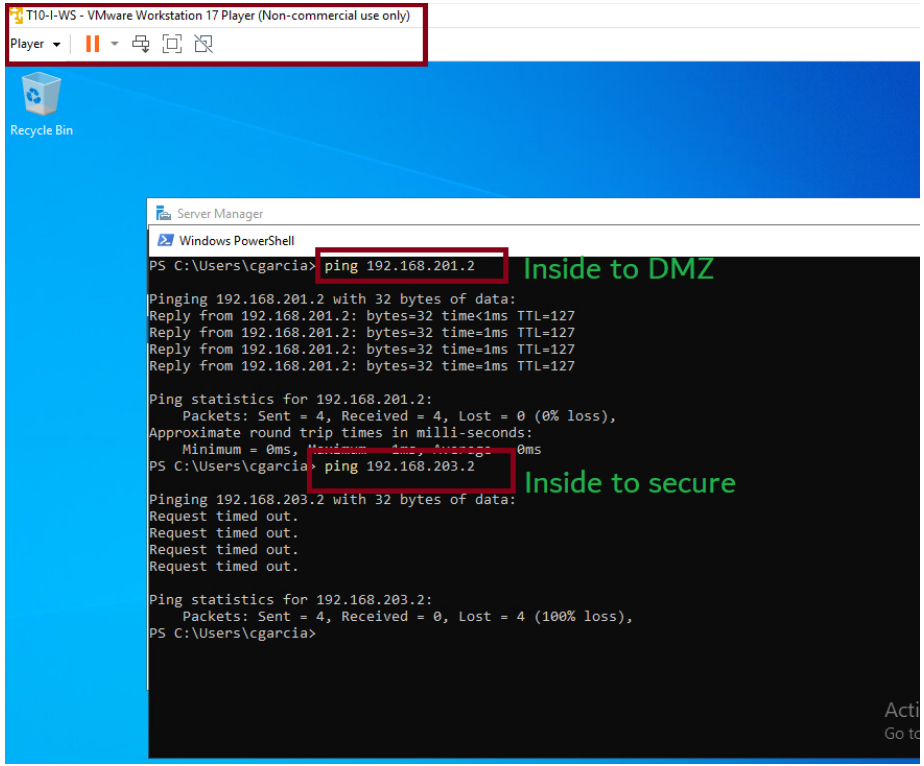
Connectivity tests.

Testing connectivity with ping between zones



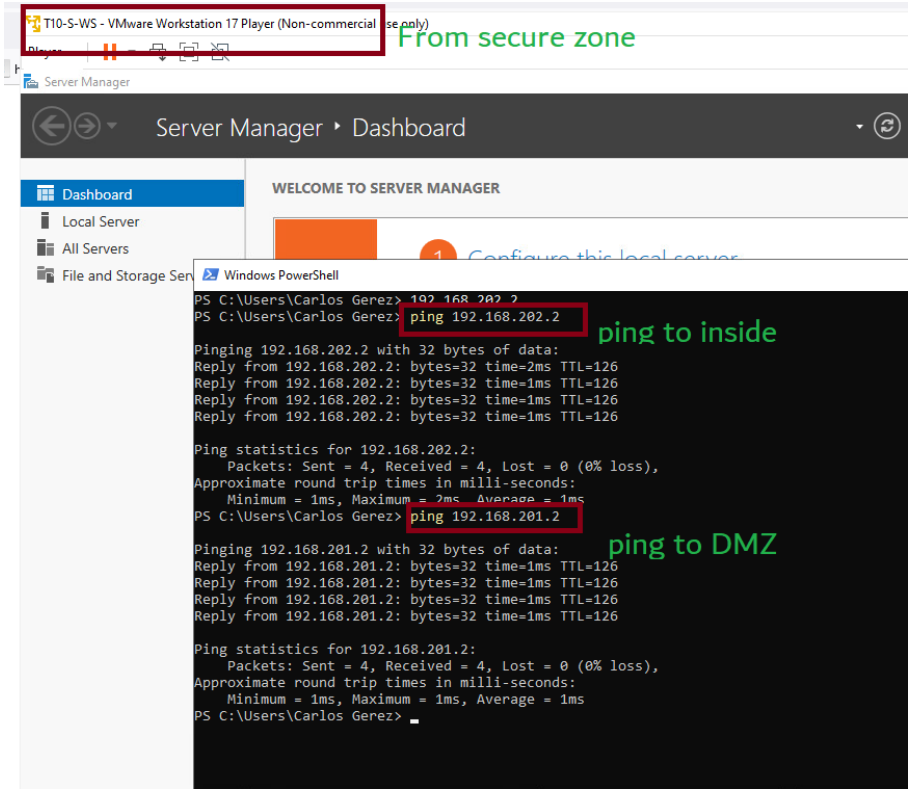
From DMZ zone.

Testing connectivity with ping between zones



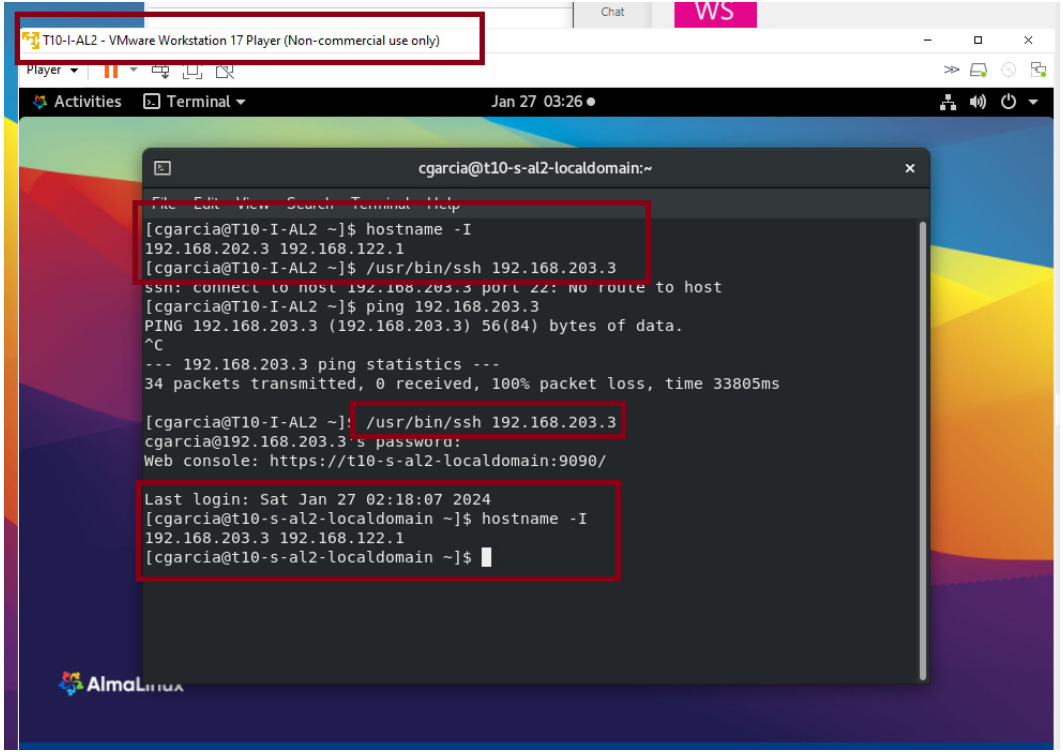
From inside zone.

Testing connectivity with ping between zones



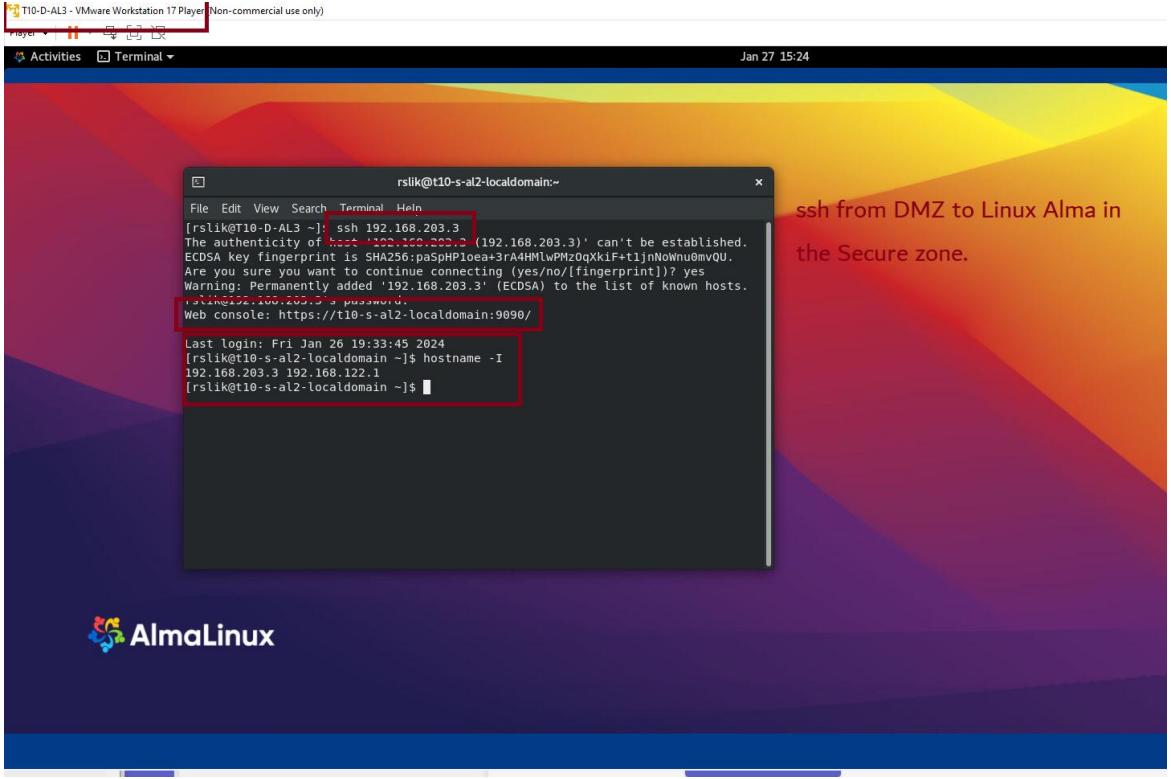
From secure zone.

Testing connectivity with ssh between zones



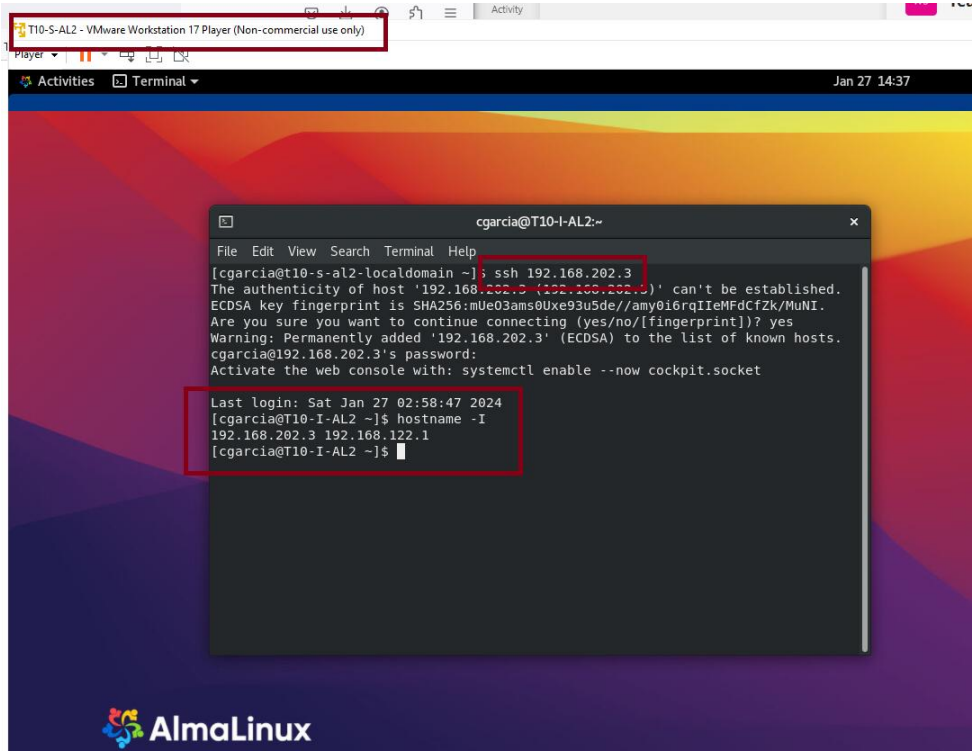
From inside to secure ssh.

Testing connectivity with ssh between zones



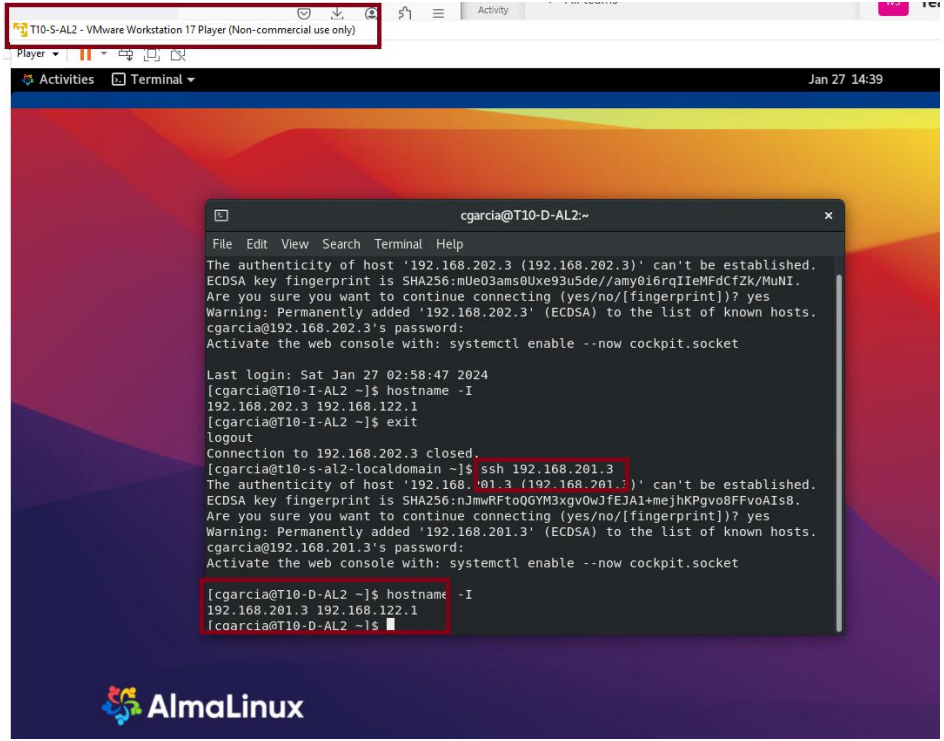
From DMZ to secure ssh

Testing connectivity with ssh between zones



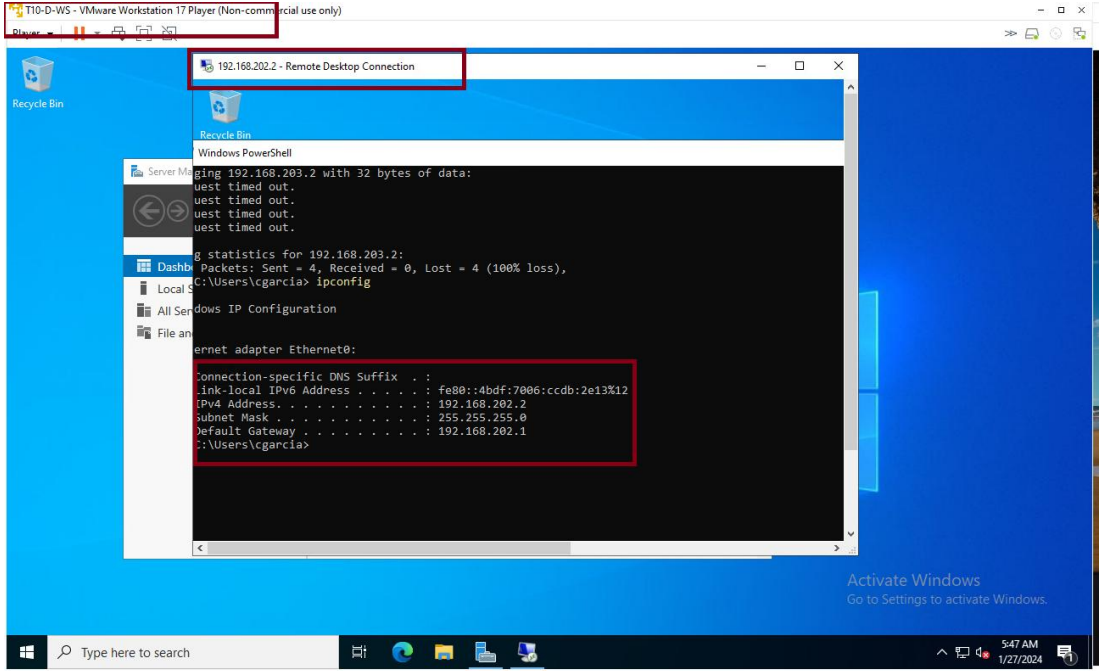
From secure to inside ssh

Testing connectivity with ssh between zones



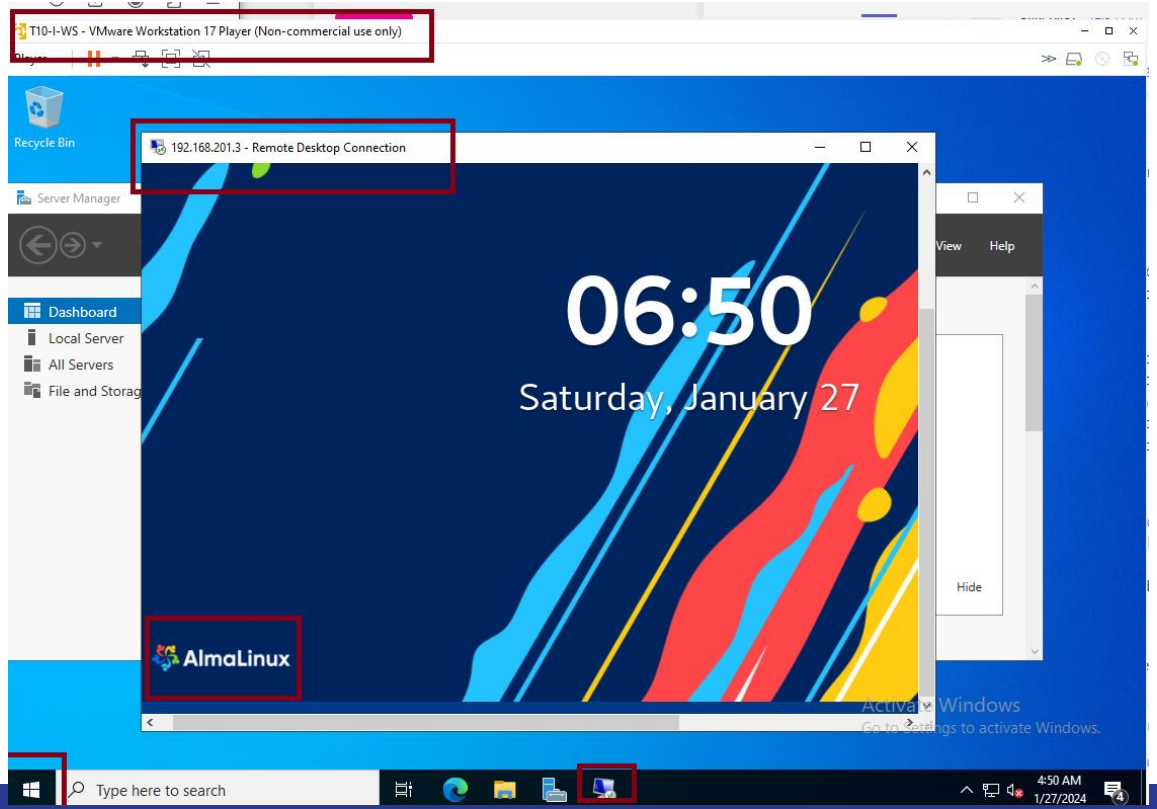
From secure to DMZ ssh

Testing Remote Desktop connectivity between zones



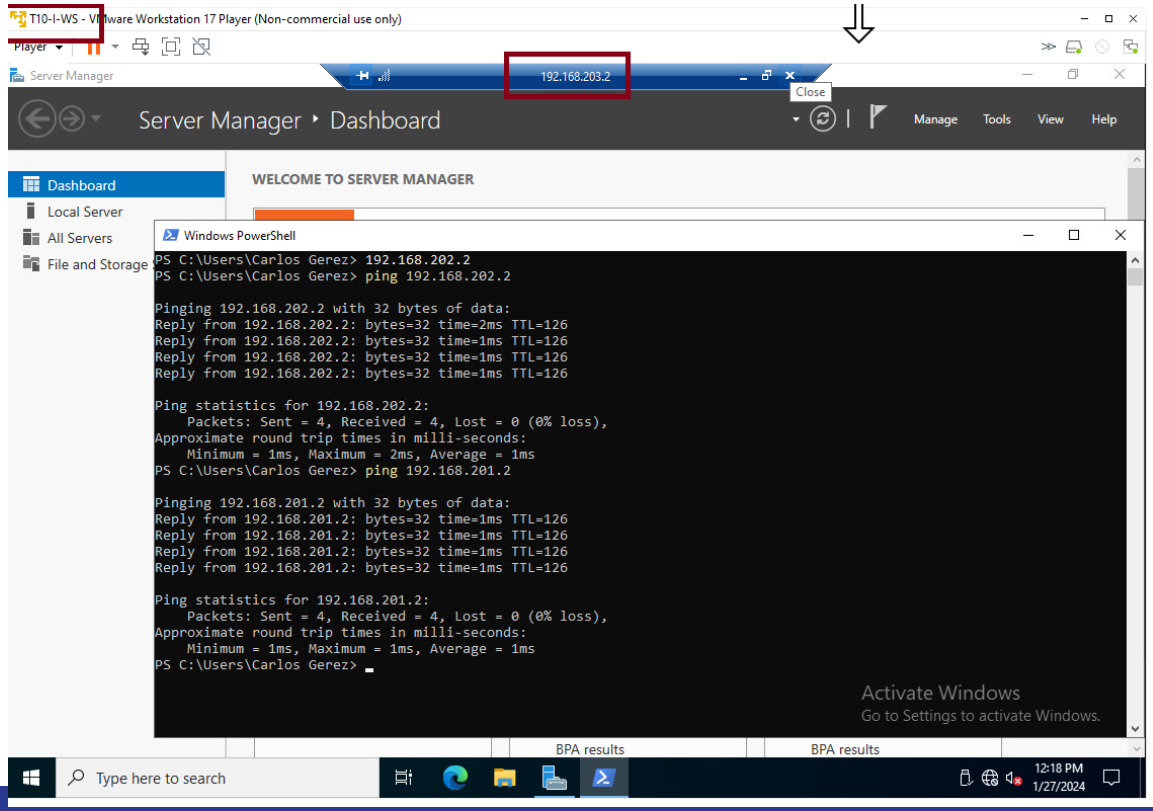
DMZ to inside zone.

Testing Remote Desktop connectivity between zones



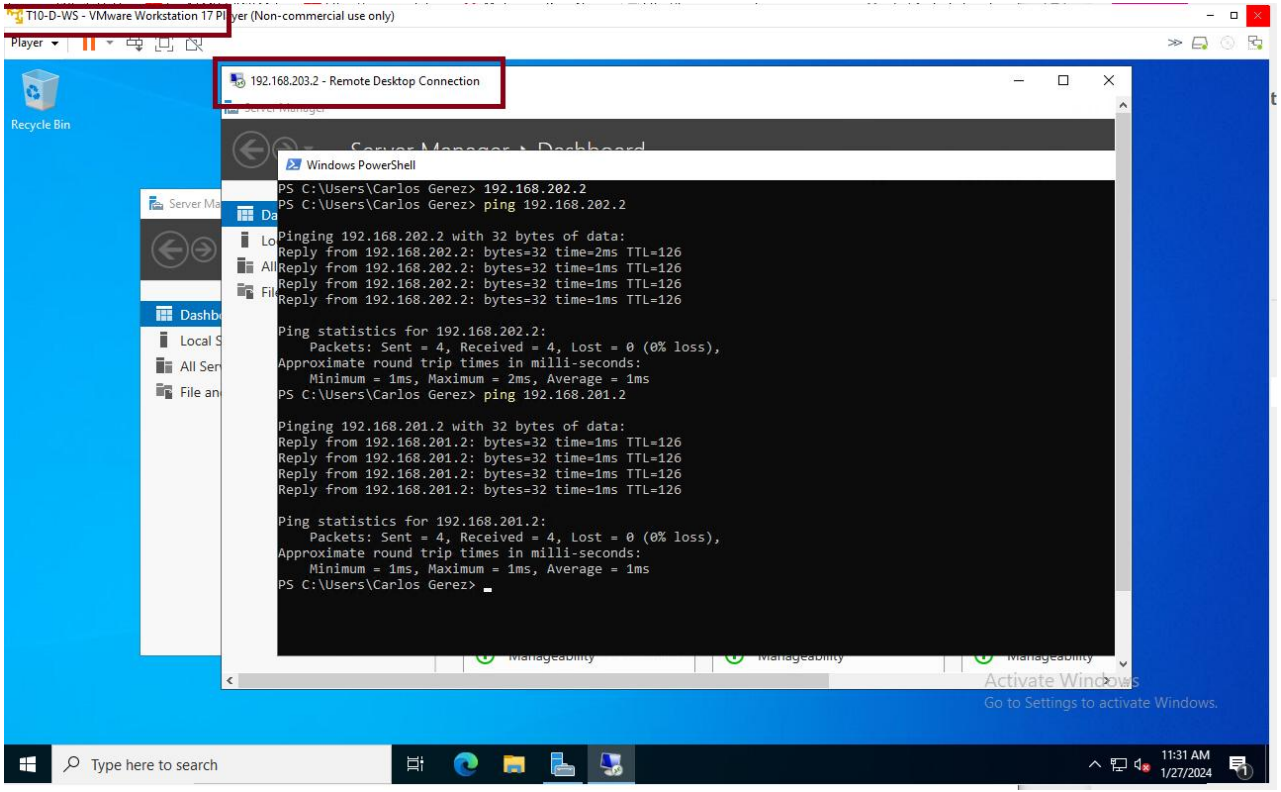
Inside to DMZ zone.

Testing Remote Desktop connectivity between zones



Inside to secure zone.

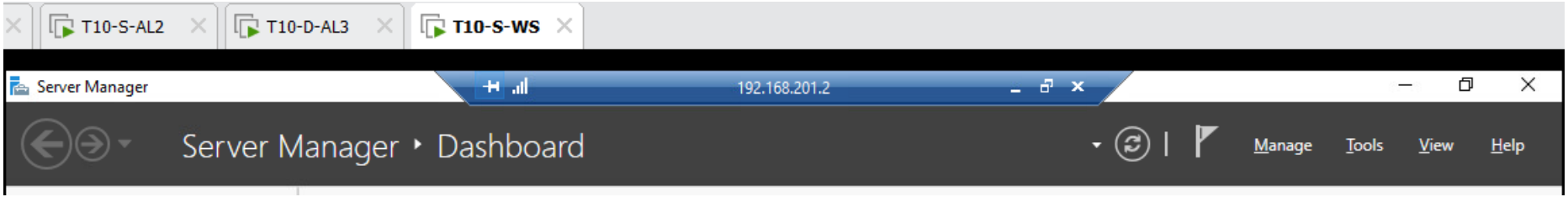
Testing Remote Desktop connectivity between zones



DMZ to secure zone.

Testing Remote Desktop connectivity between zones

Secure to DMZ.



Testing Remote Desktop connectivity between zones

Secure to Inside.