Palo Alto Install And Setup SOP

By: Lcpl Hundley, Lcpl Regan
3rd PLT DCO-IDM
LU: 20240228

General intent of this document is to give guidance to DCO-IDM personnel who are inexperienced with the Palo Alto firewall .

PALO ALTO Firewall Synopsis

The Virtualized VM- Series Palo Alto Firewall uses PAN-OSTM, a security-specific operating system that enables intra-virtual machine traffic, protects against known and unknown threats, and integrates flexibly in the virtualized environments. Below are the following limitations to keep in mind during deployment and use of the toolset:

- Only 10 ports can be configured. One for management traffic and up to 9 can be used for data traffic.
- Forged transmit and promiscuous mode must be enabled on the ESXi vSwitch port groups connected to Layer 2 and vwire interfaces on the VM-Series firewall.
- Hypervisor-assigned MAC addresses are enabled by default. If neither promiscuous mode nor hypervisor-assigned MAC address is enabled, the firewall does not receive any traffic.

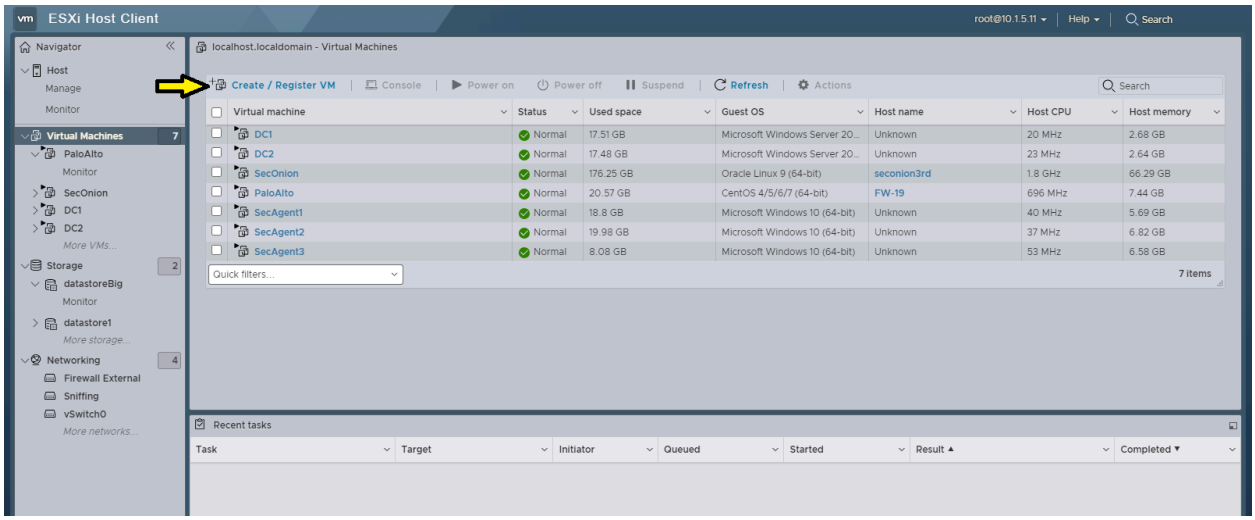
At their most basic, firewalls are filtering devices that operate on layer 3 and filter traffic based on variables like to/from IP, port, and protocol. Second generation, or stateful firewalls, keep a record of which ports are utilized by a given connection, examine some of the traffic, and make a determination whether to allow the connection based on its ruleset. Third generation firewalls, or application firewalls, control input, output, and access to/from an application or service based on a defined ruleset.

Like a proxy filters web traffic, a firewall filters known-bad traffic using a defined Access Control List (ACL). It is important to note that ACLs are limited in their ability to provide security against even moderately sophisticated actors as it is trivial to change IP addresses from attack to attack, or even during an attack.

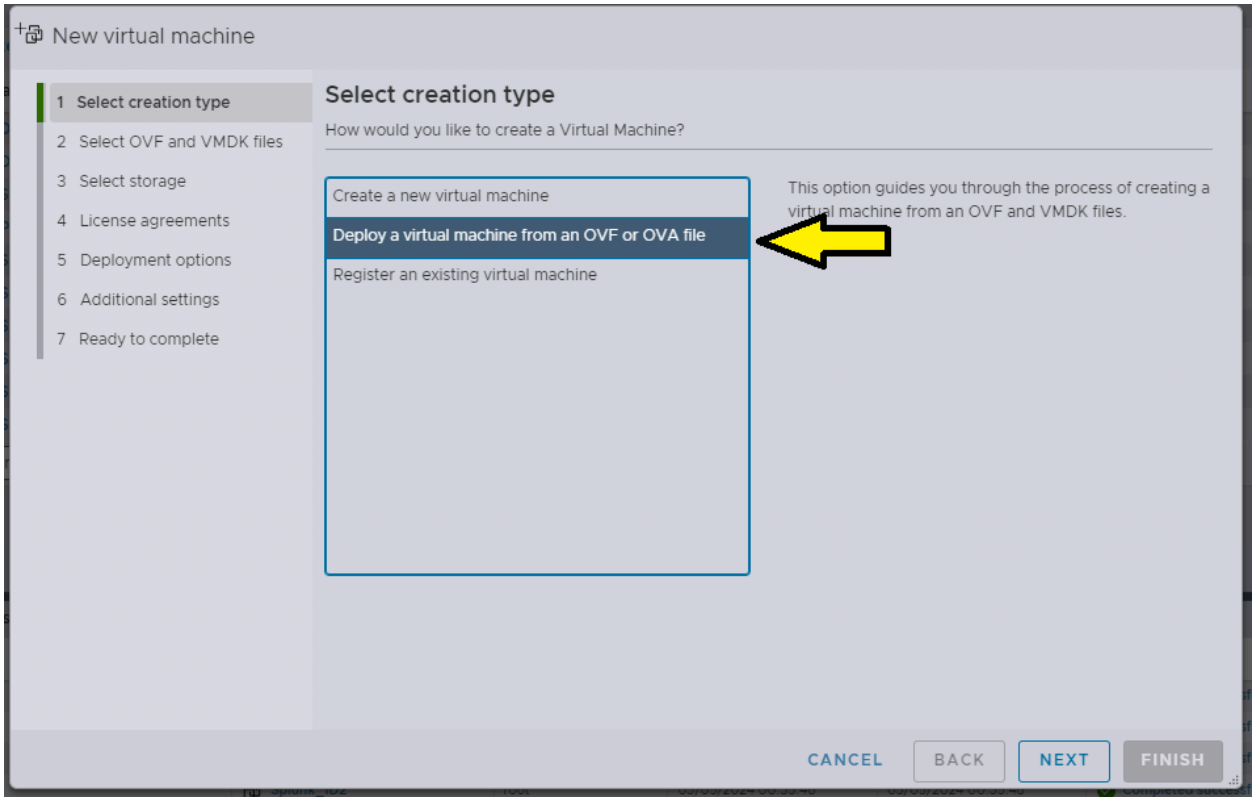
The team will usually implement a firewall between the supported command's network and the team's DMSS toolkit.

VM Initial Install and Configuration

- **Step 1:**
  On the ESXI Virtual Machines Tab select “Create / Register VM”

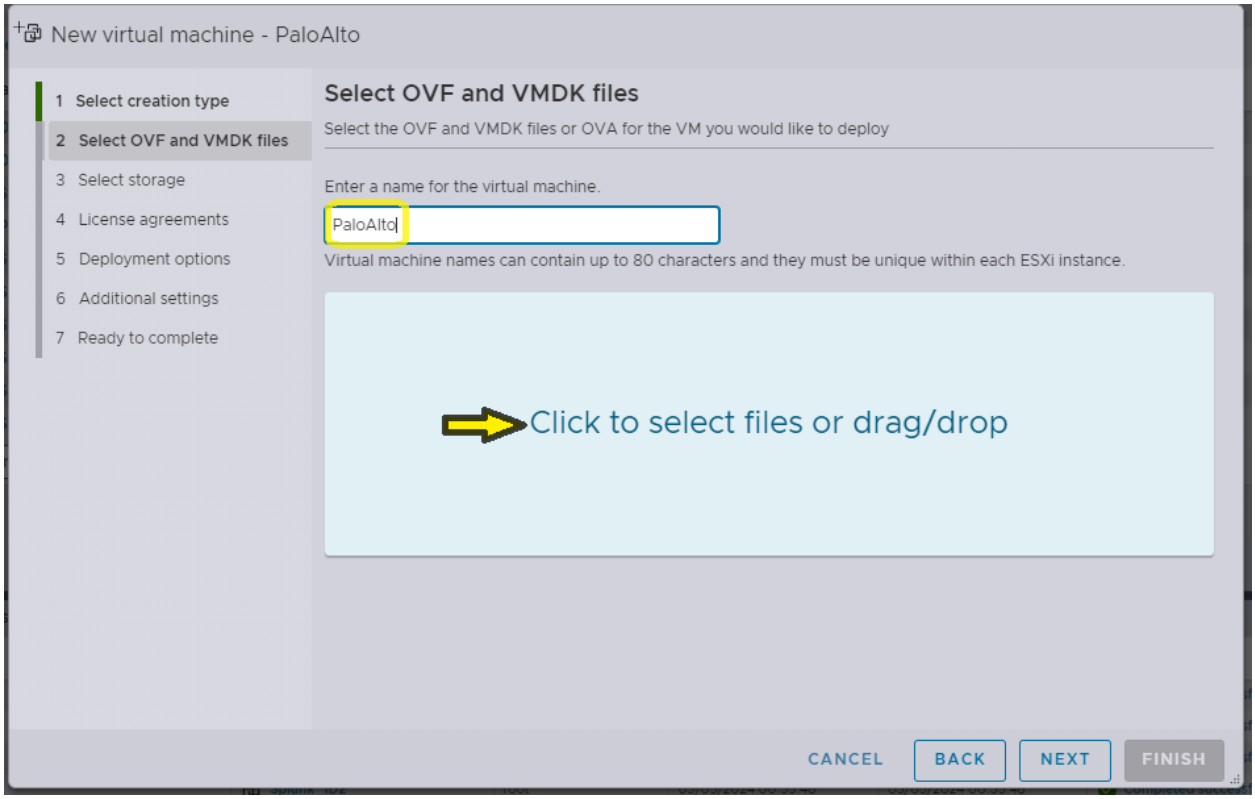


- **Step 2:**
  For Creation Type select “Deploy a virtual machine from an OVF or OVA file”



❖ **Step 3:**

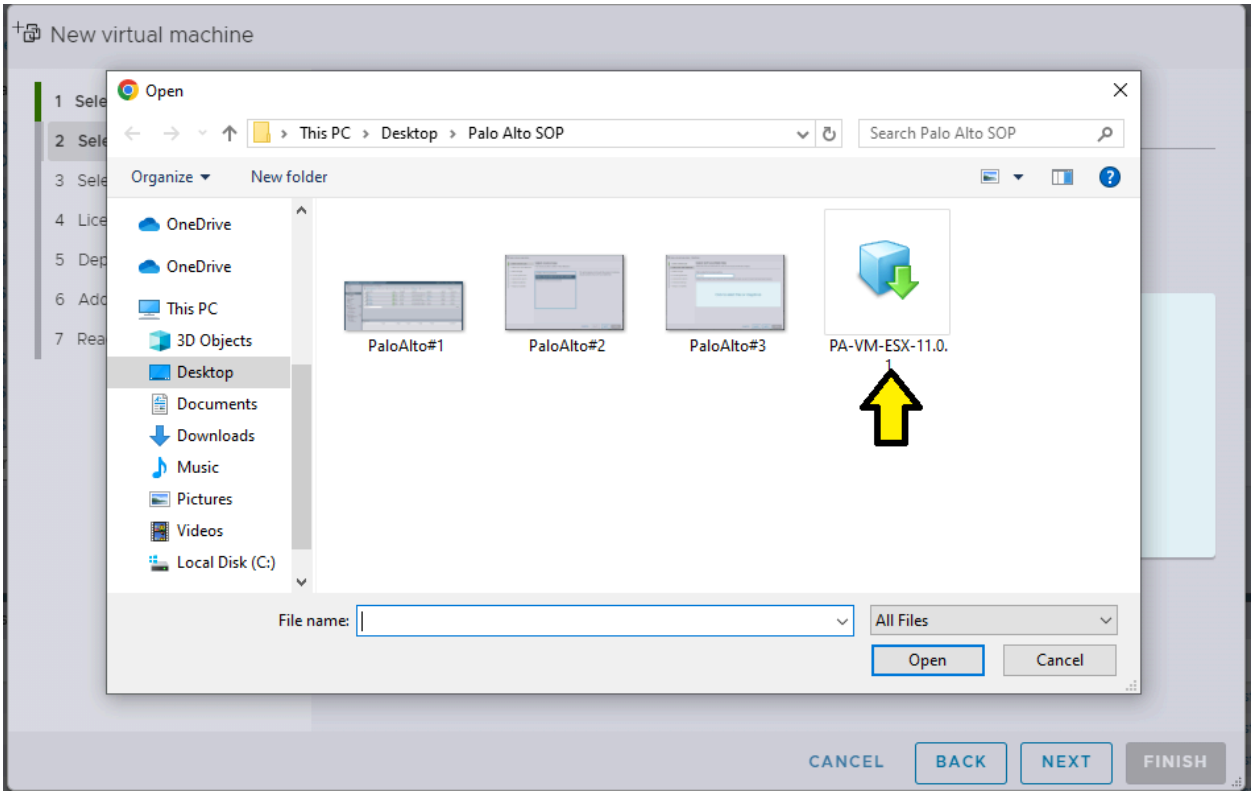
Assign the Virtual machine a name, in this instance name it along the lines of PaloAlto. Then Select “Click to select files or drag/drop”



❖ **Step 4:**

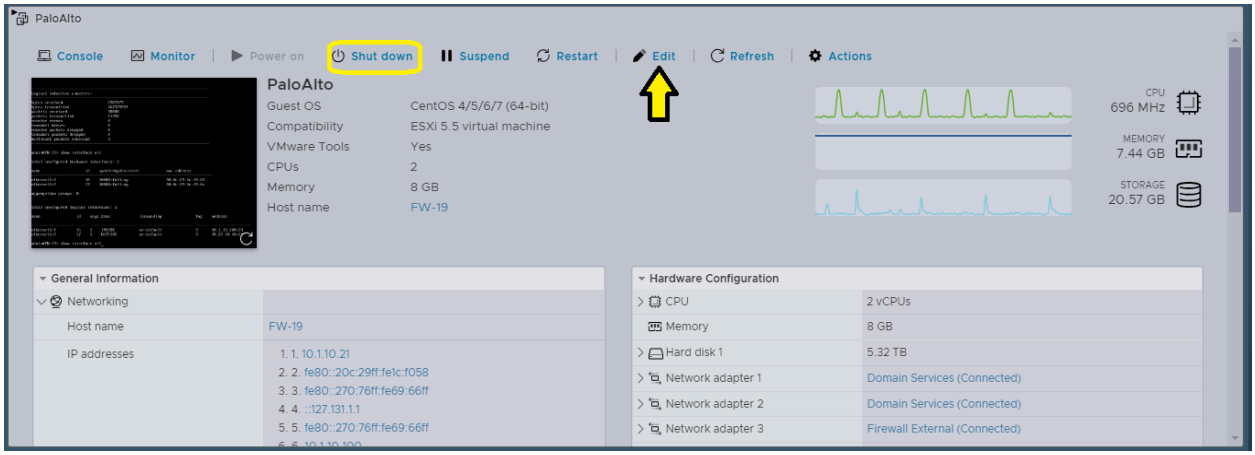
Find and select the Palo Alto OVA file. Notable locations are

- Data Lockers
- The workstation file system/network share
- Datastore on Local Hypervisor



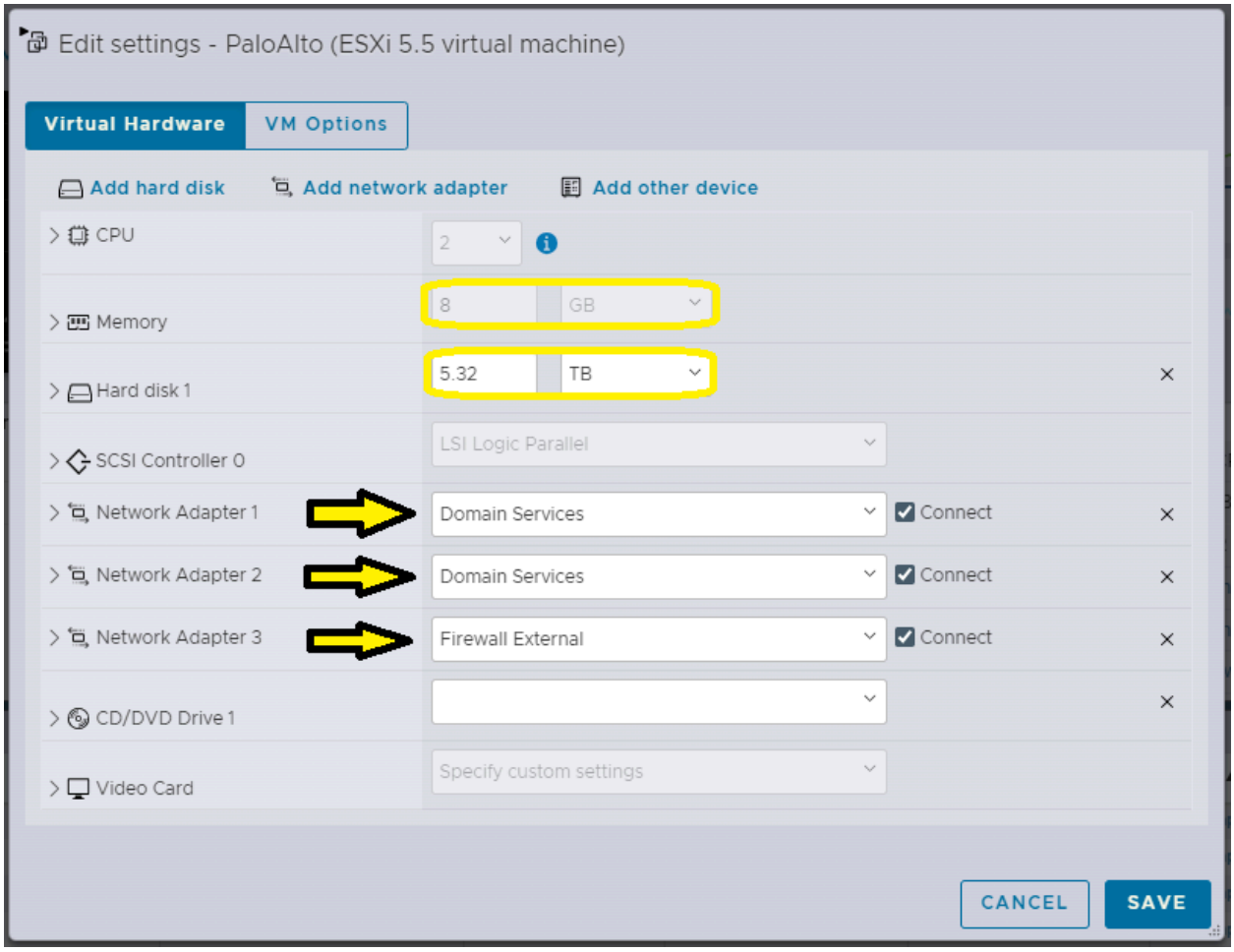
❖ **Step 5:**

Before you open the VM make sure to shut it down fully and open the edit tab



❖ **Step 6:**

Change memory size to 8 GB and hard disk space can be figured to your needs,
Aswell make sure your network adapters are set to domain services for the first 2 network adapters and firewall external for the 3rd adapter

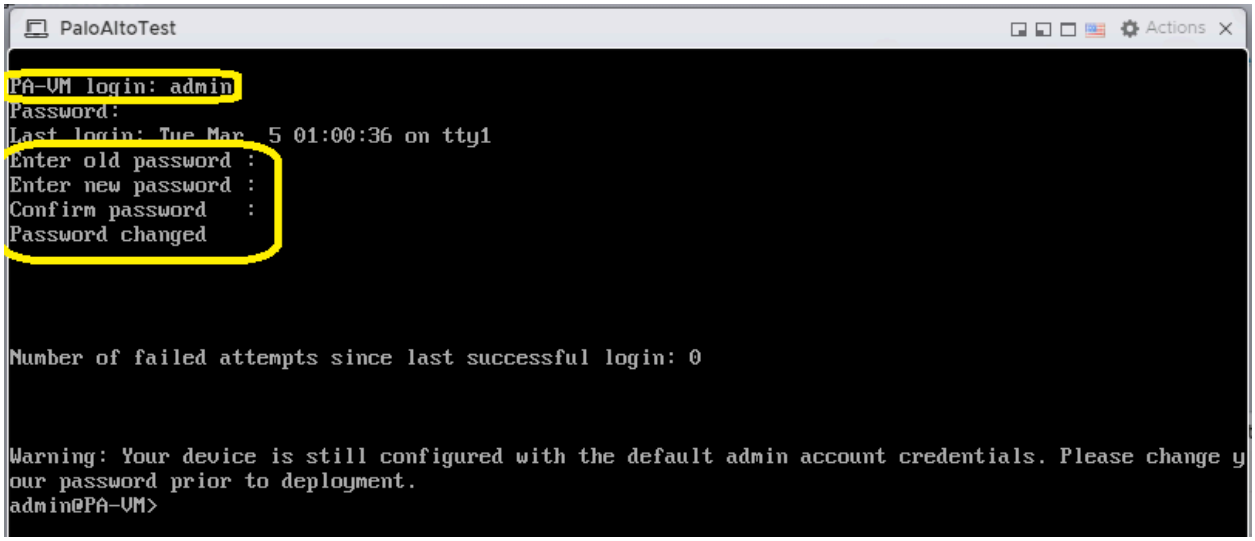


❖ **Step 7:**

The login and password are **admin/admin**

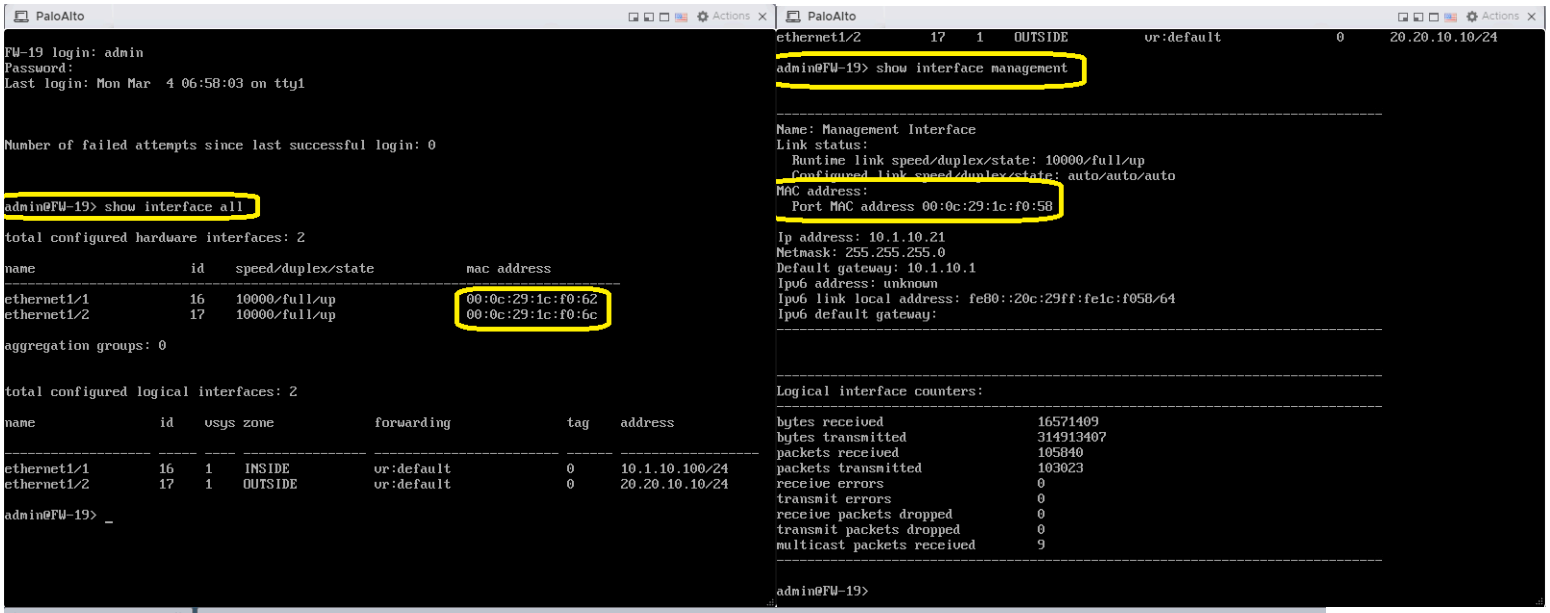
Note you might have to enter the login and password several times

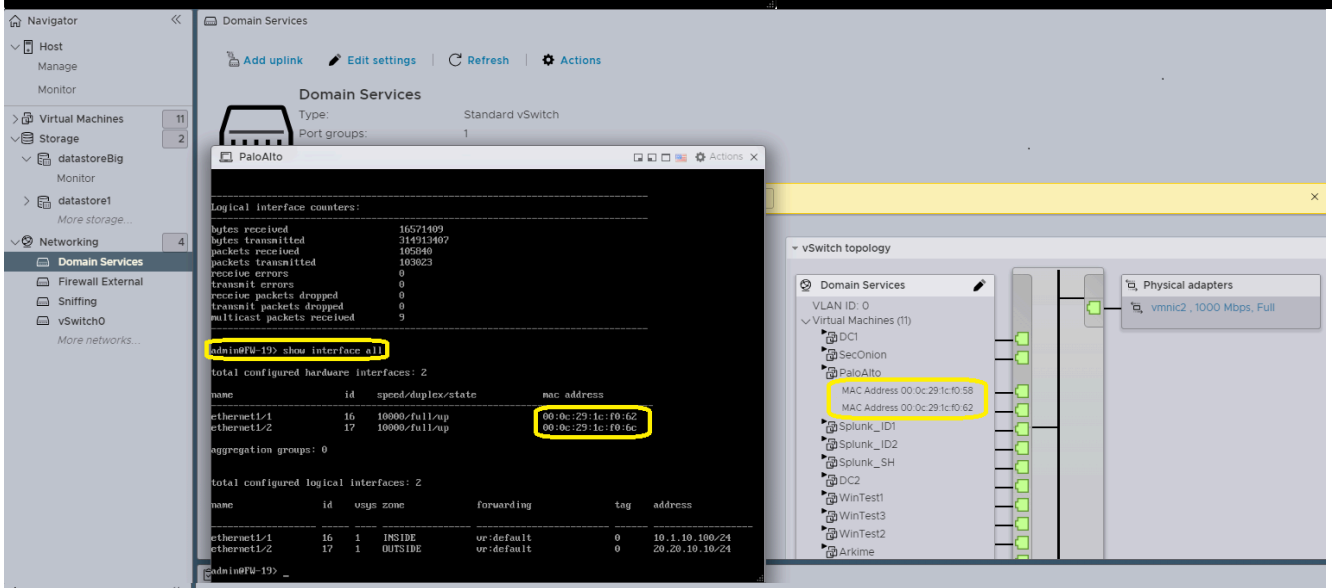
Then you will get the option to change the password to the shop standard password

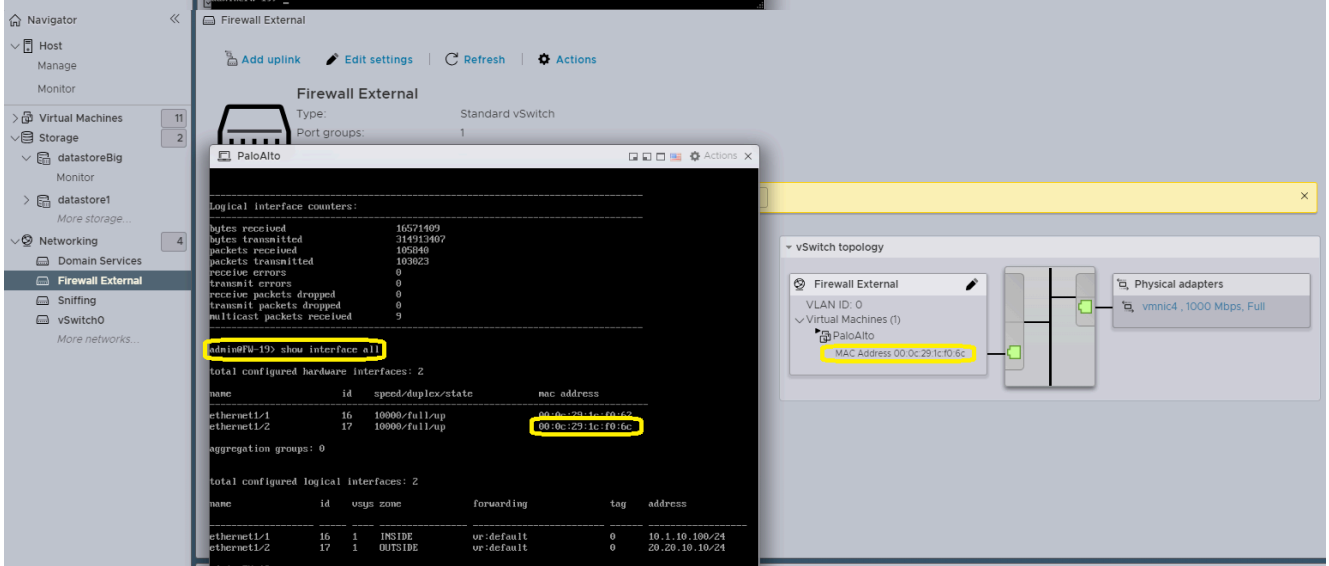


❖ **Step 8:**

Before you enter any configurations make sure your mac addresses match your ESXI network adapter mac addresses. Commands on Palo alto for seeing mac addresses are **show interface all** And **show interface management**







❖ **Step 9:**

Type “configure” to enter configuration mode

```
admin@PA-VM>
admin@PA-VM> configure
Entering configuration mode
[edit]
admin@PA-VM#
```

❖ **Step 10:**

To set the Hostname type “set deviceconfig system hostname FW-19”

```
admin@PA-VM>
admin@PA-VM> configure
Entering configuration mode
[edit]
admin@PA-VM# clear
Unknown command: clear
[edit]
admin@PA-VM# cls
Unknown command: cls
[edit]
admin@PA-VM# set deviceconfig system hostname FW-19
```

❖ **Step 11:**

To assign the VM with a static ip and assign is DNS servers type “set deviceconfig system ip-address 10.1.10.28 netmask 255.255.255.0 default-gateway 10.1.10.1 dns-setting servers primary 10.1.10.14 secondary 10.1.10.15” (change ip addresses as needed)

```
admin@PA-VM> configure
Entering configuration mode
[edit]
admin@PA-VM# set device
> device-object    device-object
> deviceconfig     deviceconfig

admin@PA-VM# set deviceconfig system hostname FW-Test

[edit]
admin@PA-VM# set deviceconfig system ip-address 10.1.10.28 netmask 255.255.255.0 default-gateway 10
1.10.1 dns-setting servers primary 10.1.10.14 secondary 10.1.10.15

[edit]
admin@PA-VM# _
```

❖ **Step 12:**

The next part is to make the Vm’s ip address static so DHCP does not assign the ip, Type “set deviceconfig system type static”

```
admin@PA-VM> configure
Entering configuration mode
[edit]
admin@PA-VM# set device
> device-object    device-object
> deviceconfig     deviceconfig

admin@PA-VM# set deviceconfig system hostname FW-Test

[edit]
admin@PA-VM# set deviceconfig system ip-address 10.1.10.28 netmask 255.255.255.0 default-gateway 10.
1.10.1 dns-setting servers primary 10.1.10.14 secondary 10.1.10.15

[edit]
admin@PA-VM# set device
> device-object    device-object
> deviceconfig     deviceconfig

admin@PA-VM# set deviceconfig system type static
```

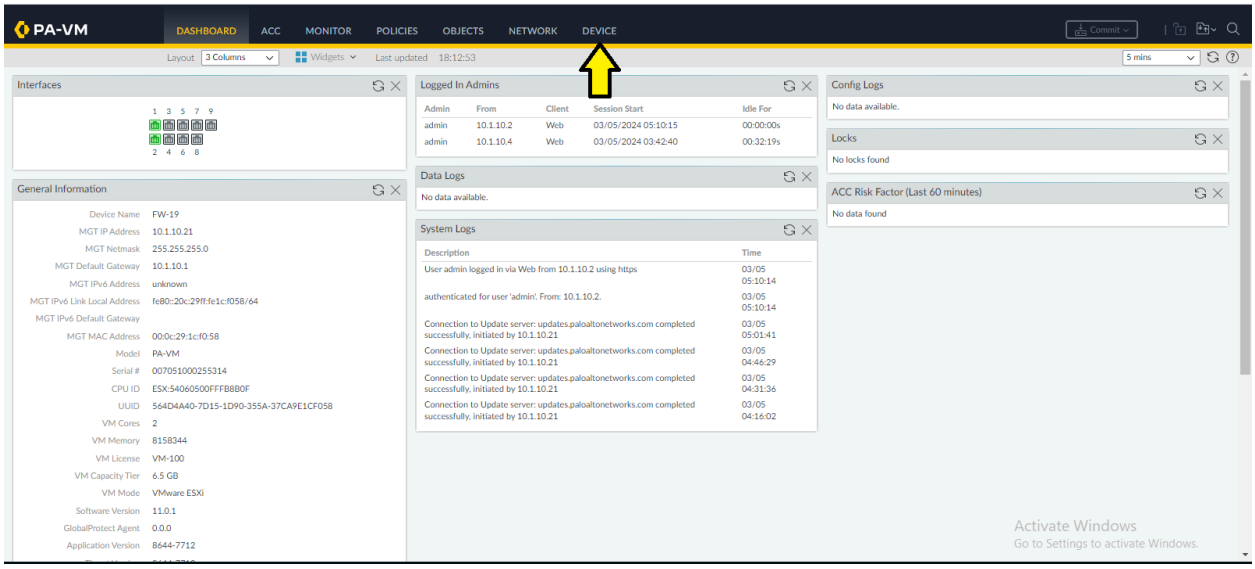
❖ **Step 13:**

To save your configurations you just applied, type “Commit”

```
[edit]
admin@PA-VM# set deviceconfig system ip-address 10.1.10.28 netmask 255.255.255.0 default-gateway 10.
1.10.1 dns-setting servers primary 10.1.10.14 secondary 10.1.10.15

[edit]
admin@PA-VM# set device
> device-object    device-object
> deviceconfig     deviceconfig

admin@PA-VM# set deviceconfig system type static

[edit]
admin@PA-VM# commit

Commit job 3 is in progress. Use Ctrl+C to return to command prompt
.....
```

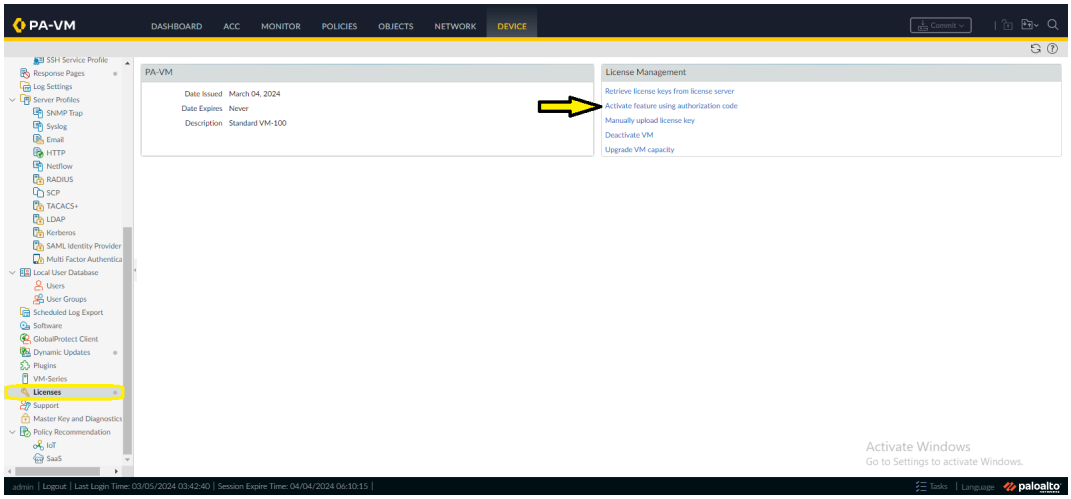
❖ **Step 14:**

In you web browser type in the ip address of the palo alto you just configured and log in,
Next you will navigate to the Device tab



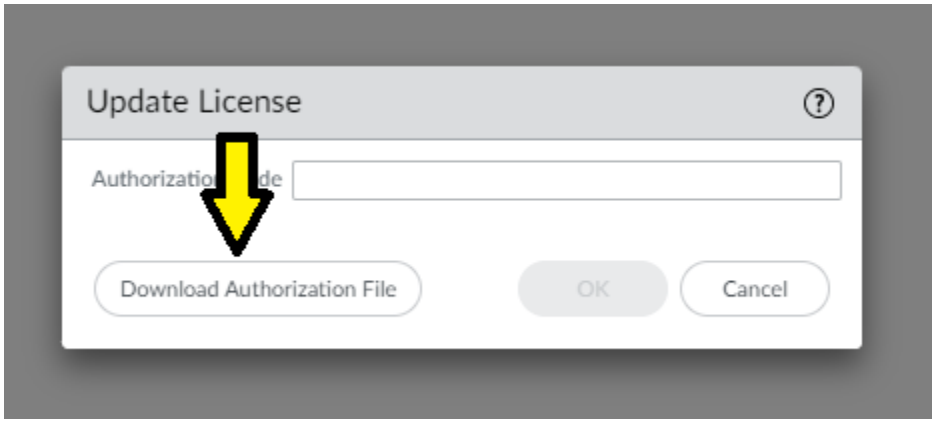
❖ **Step 15:**

Once in the device tab, in the left scroll pane scroll down till you see licenses. In the right pane under license Management select “Activate feature using authorization code”



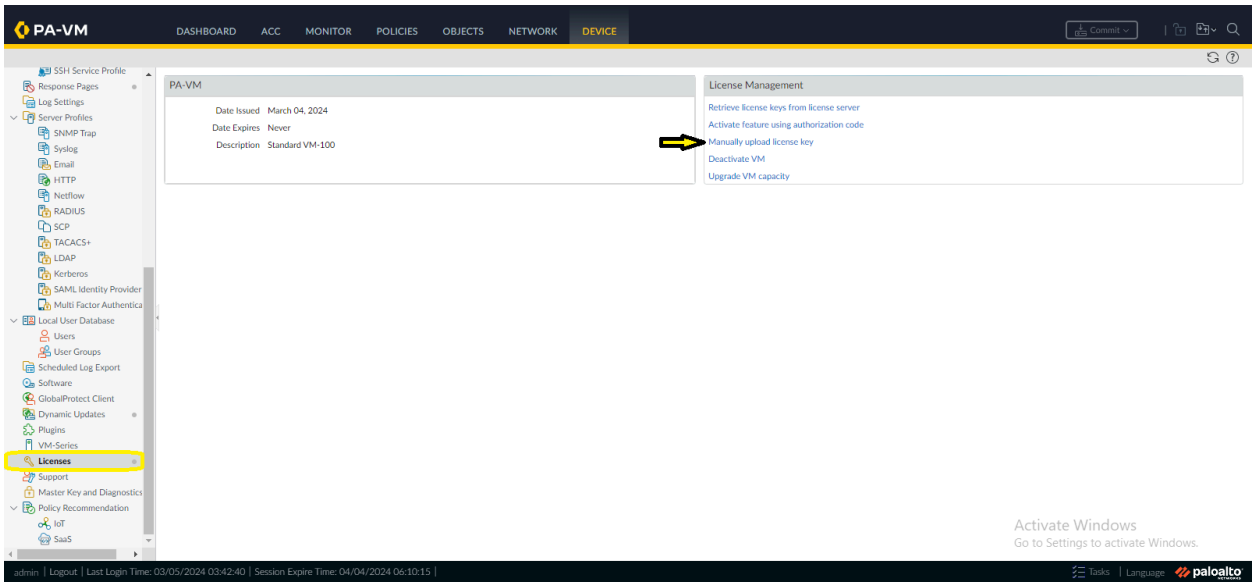
❖ **Step 16:**

Click “Download Authorization File”



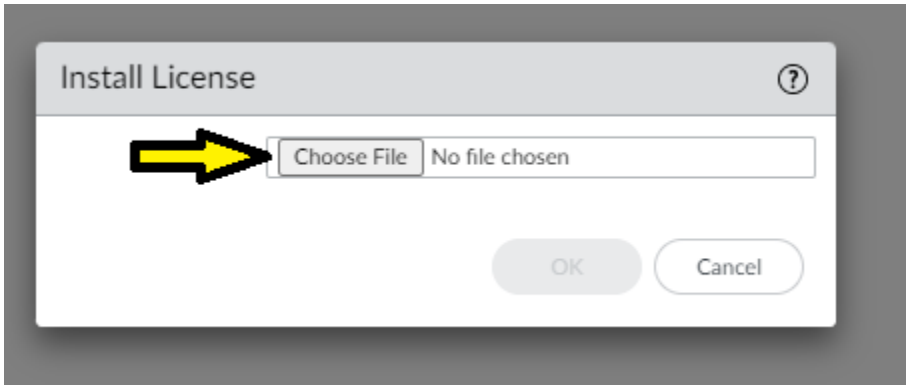
❖ **Step 17:**

Now under License Management select “Manually upload license key”



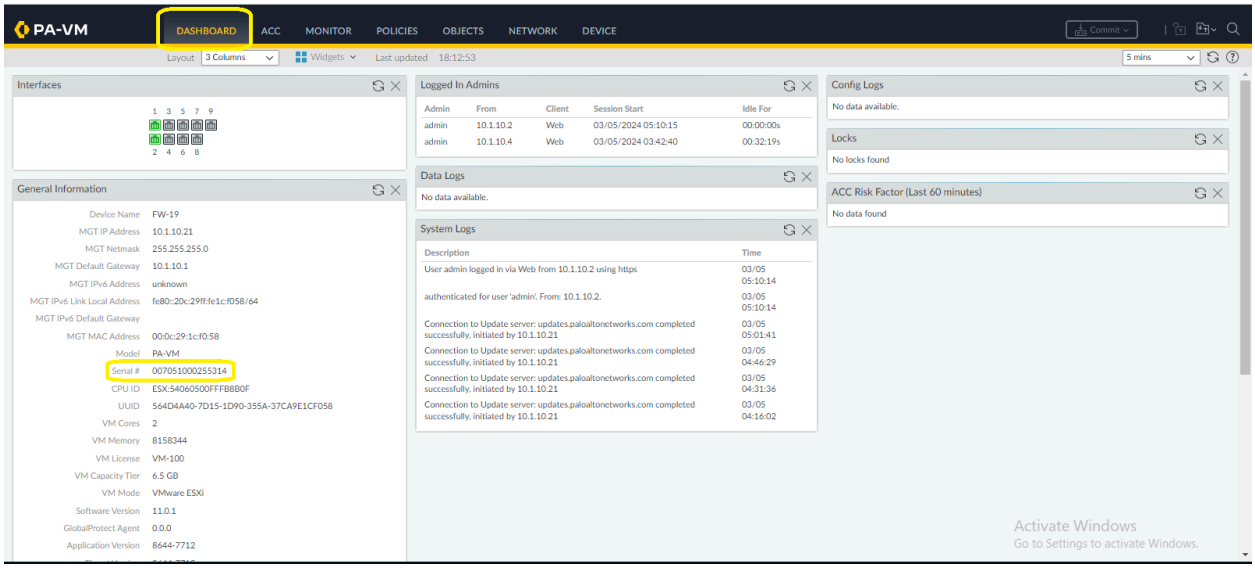
❖ **Step 18:**

Give authorization file to Palo Alto support point of contact (as of 3/6/2024 Ssgt Marshburn) then once given the .key file upload into



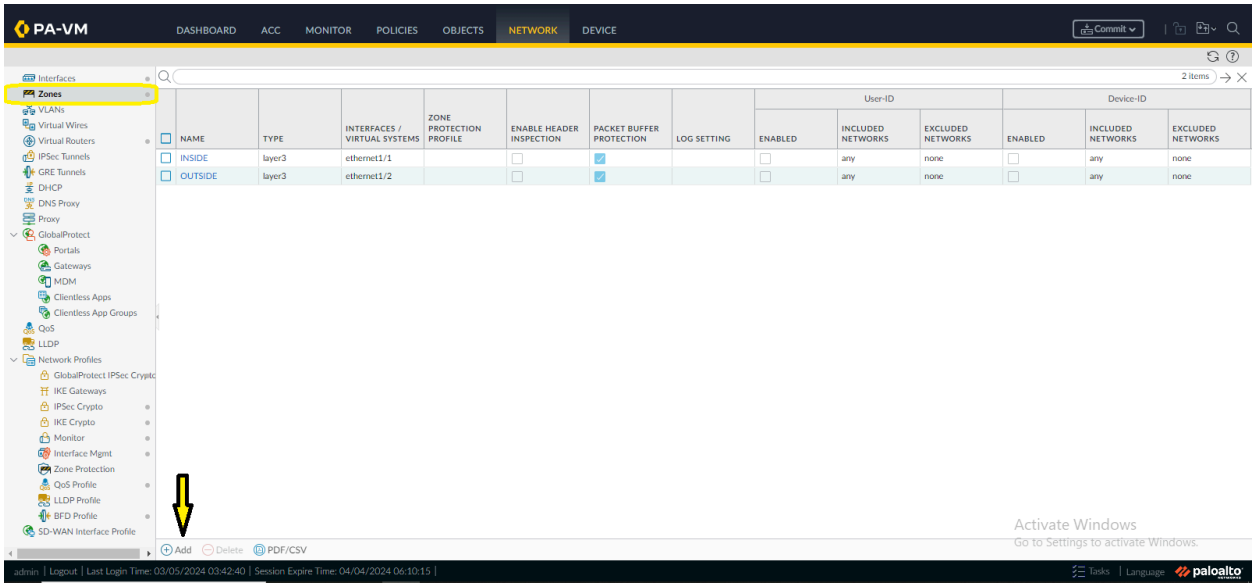
❖ **Step 19:**

Once the reboot finishes reconnect to the vm if needed and navigate to the Dashboard tab and look at the Serial# under General Information. There should be a number there if authorization was done correctly, if not it will say unknown.



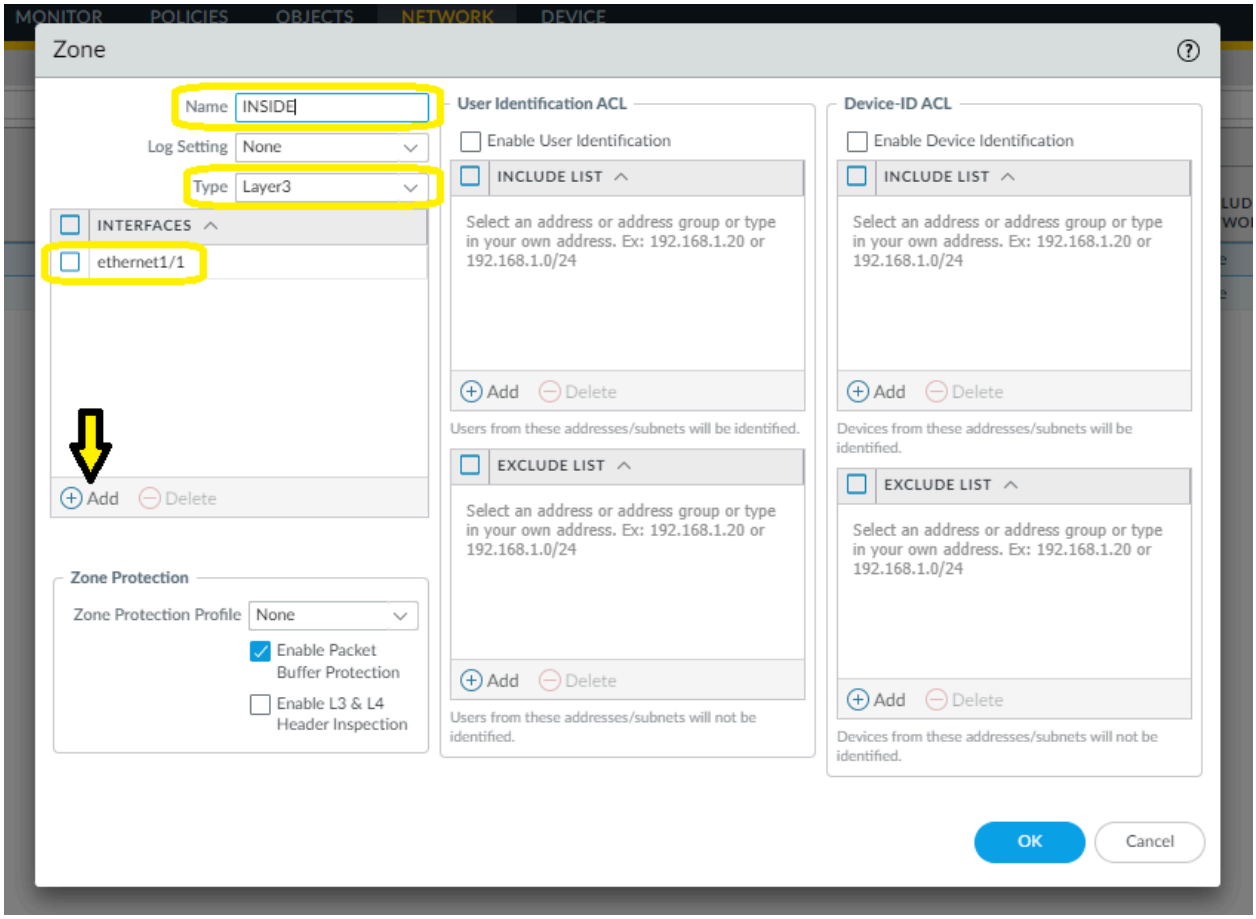
❖ **Step 20:**

Navigate to the network tab select the Zones option on the left scroll pane, to add a zone select the add button at the bottom of the page.



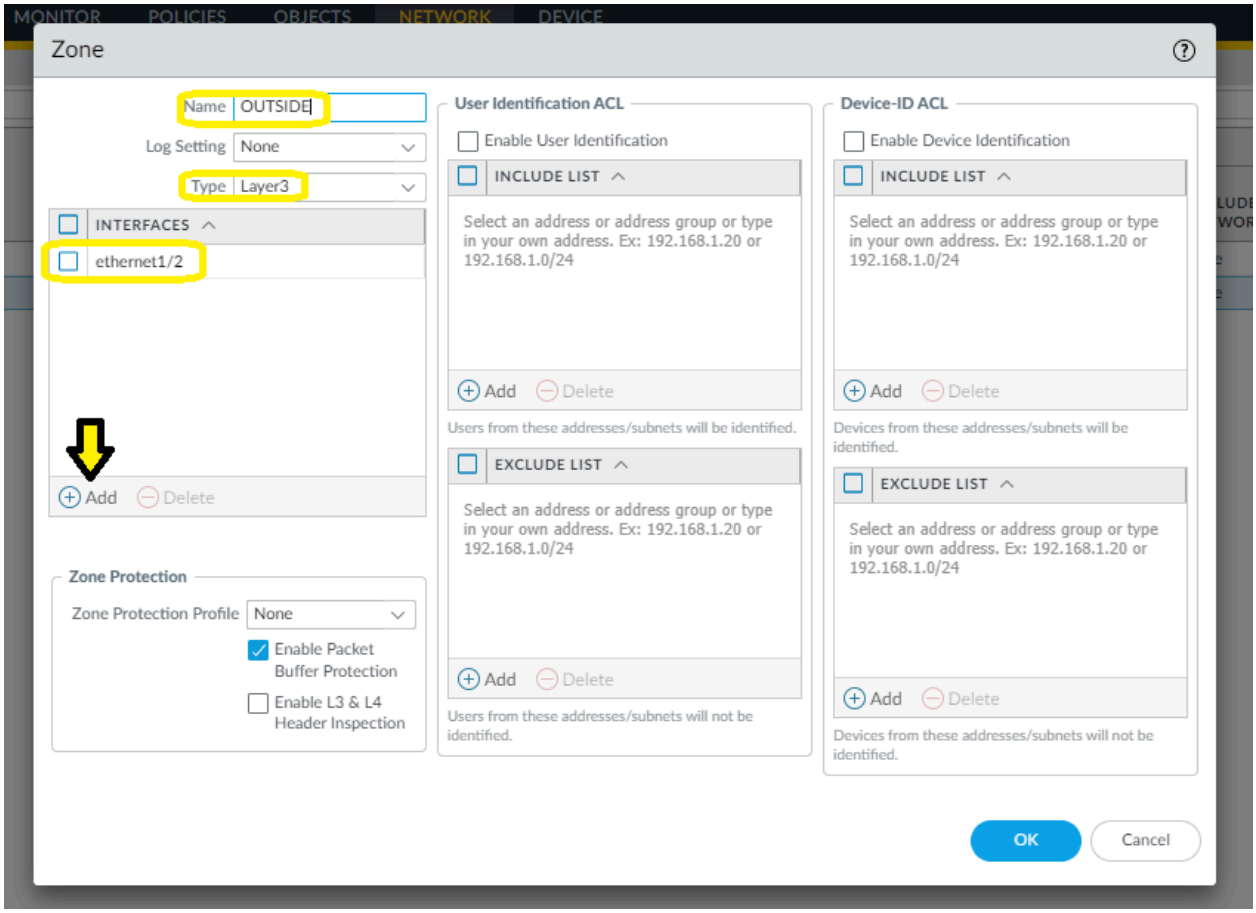
❖ **Step 21:**

Once in zone configuration, name the zone based off of network location (this example is for the Internal traffic why we named it Inside), Change the type to Layer 3. Then Select add and select the correct ethernet interface you want to assign this zone to.



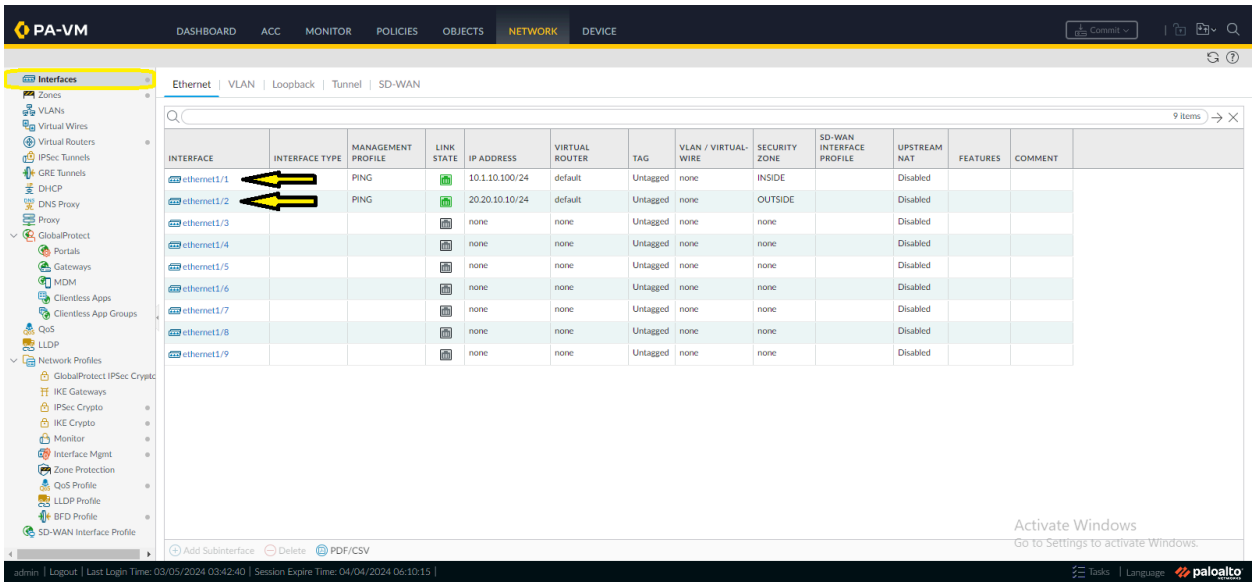
❖ **Step 22:**

name the zone based off of network location (this example is for the External traffic why we named it Outside), Change the type to Layer 3. Then Select add and select the correct ethernet interface you want to assign this zone to.



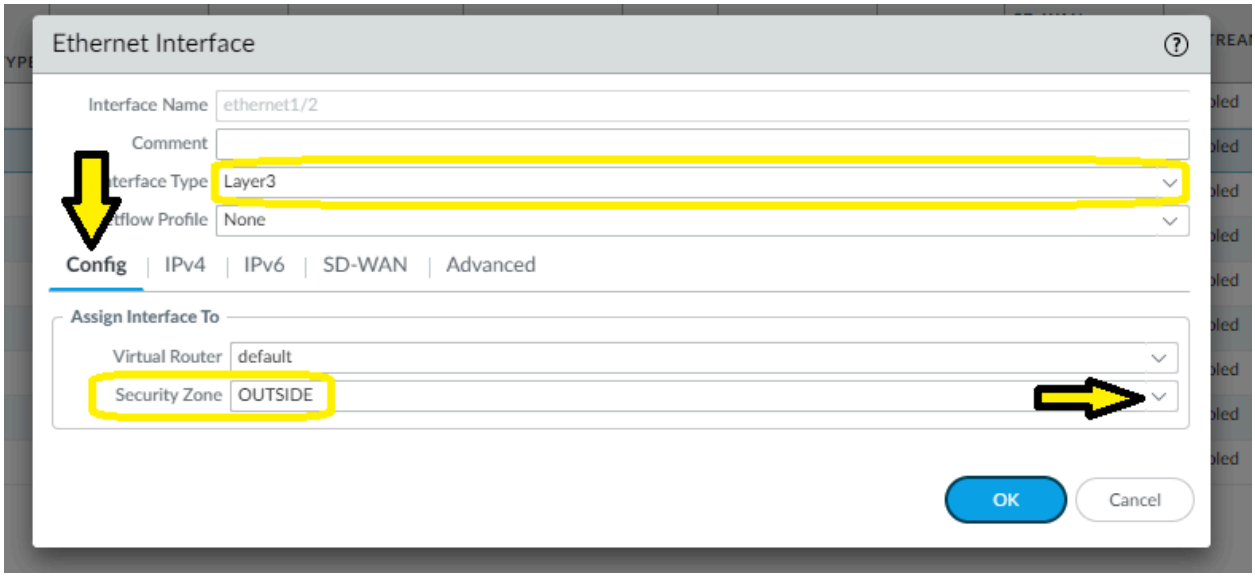
❖ **Step 23:**

Navigate to the Network tab and select the interfaces option on the left scroll pane, to configure the interfaces select the ethernet you need to configure.



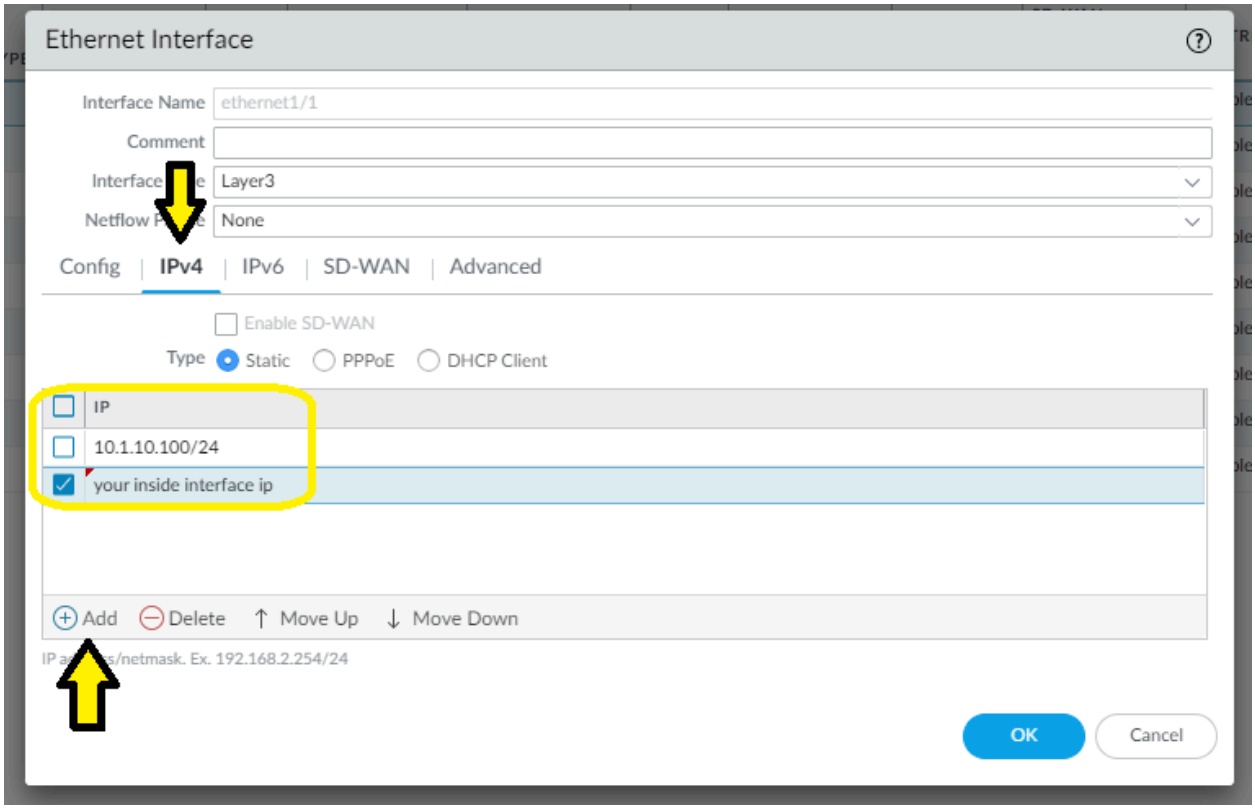
❖ **Step 24:**

On the Interface management change the interface type to layer 3 and under config select the security zone that the interface IP scheme falls under (Ex. 10.1.10.100 falls under 10.1.10.0/24 zone) (Ex. Outside=Ethernet1/2, Inside=Ethernet1/1)



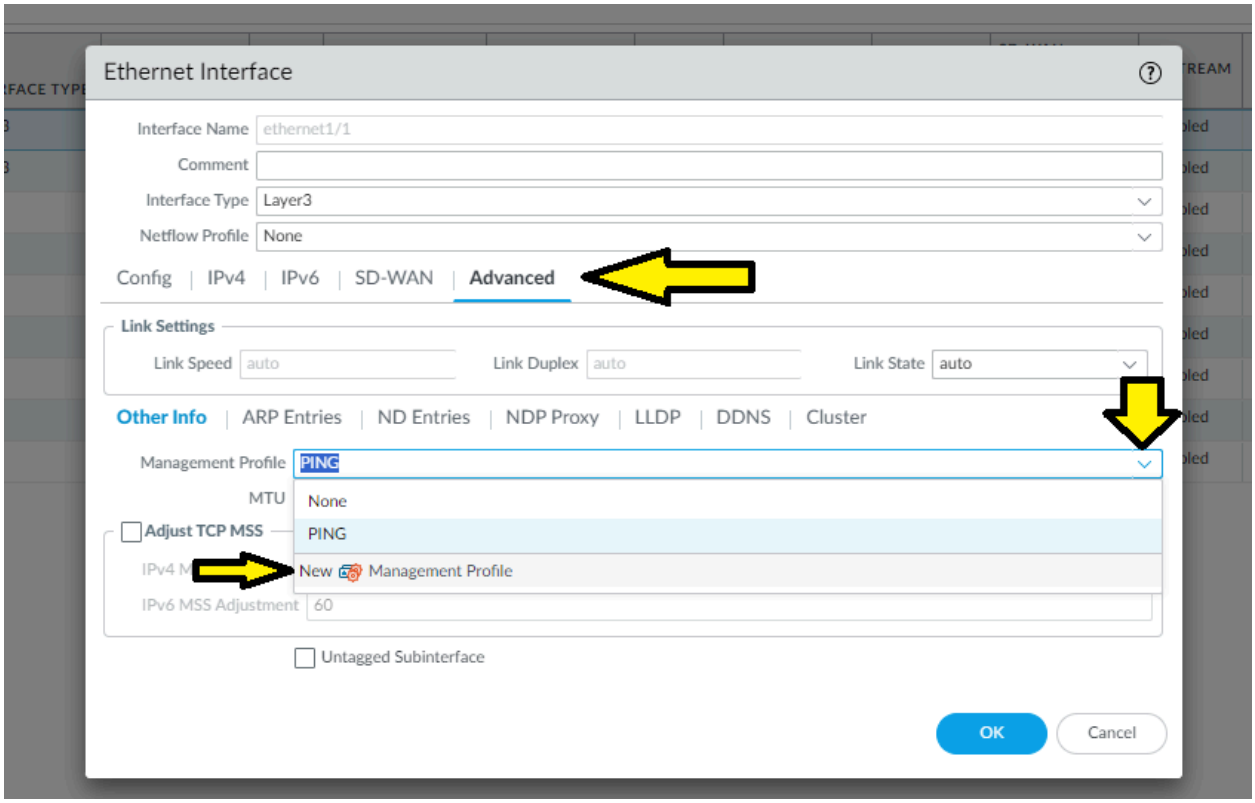
❖ **Step 25:**

Under the IPv4 Tab select the “Add” button and input the interface IP that the Scheme falls under (Ex. 10.1.10.100/24 falls under the inside Scheme or 20.20.10.10/24 falls under the outside scheme)



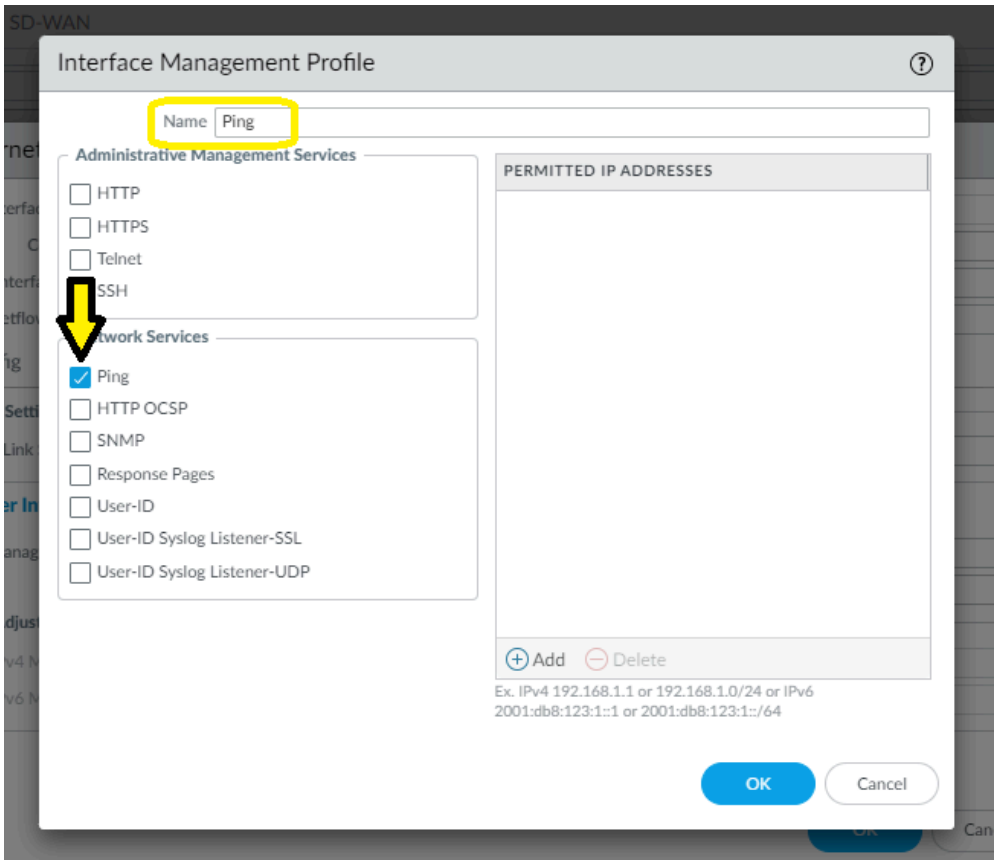
❖ **Step 26:**

Navigate to the Advanced tab and select “Management Profile”. In the drop down menu select “New Management profile”



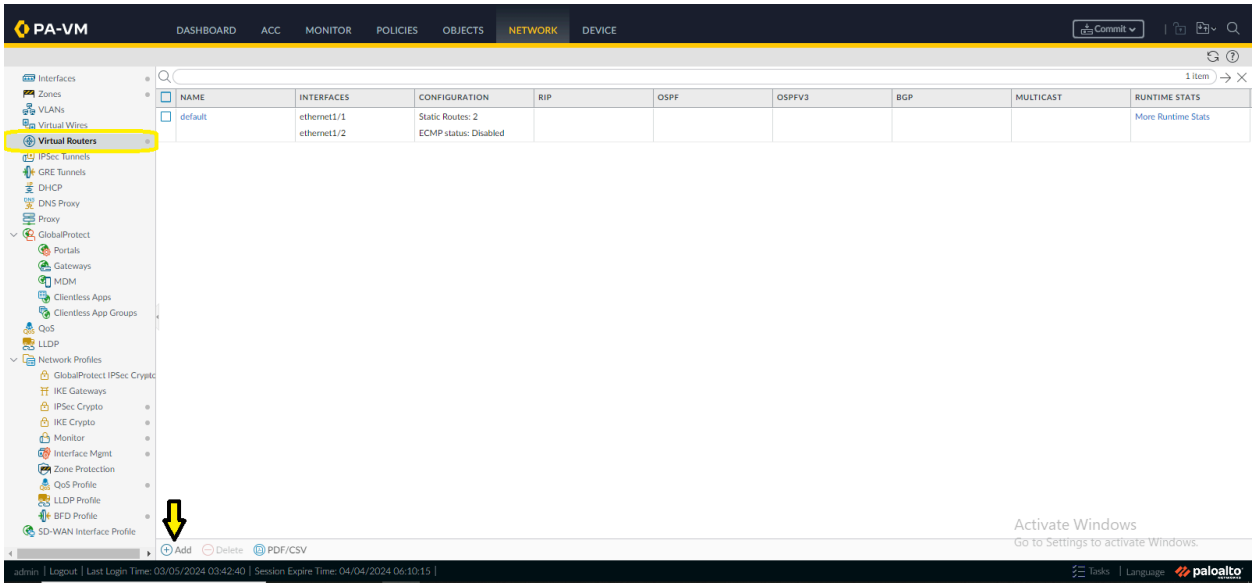
❖ **Step 27:**

Give the Management profile its (Ex. Ping) then select the network service you need (Ex. Ping)



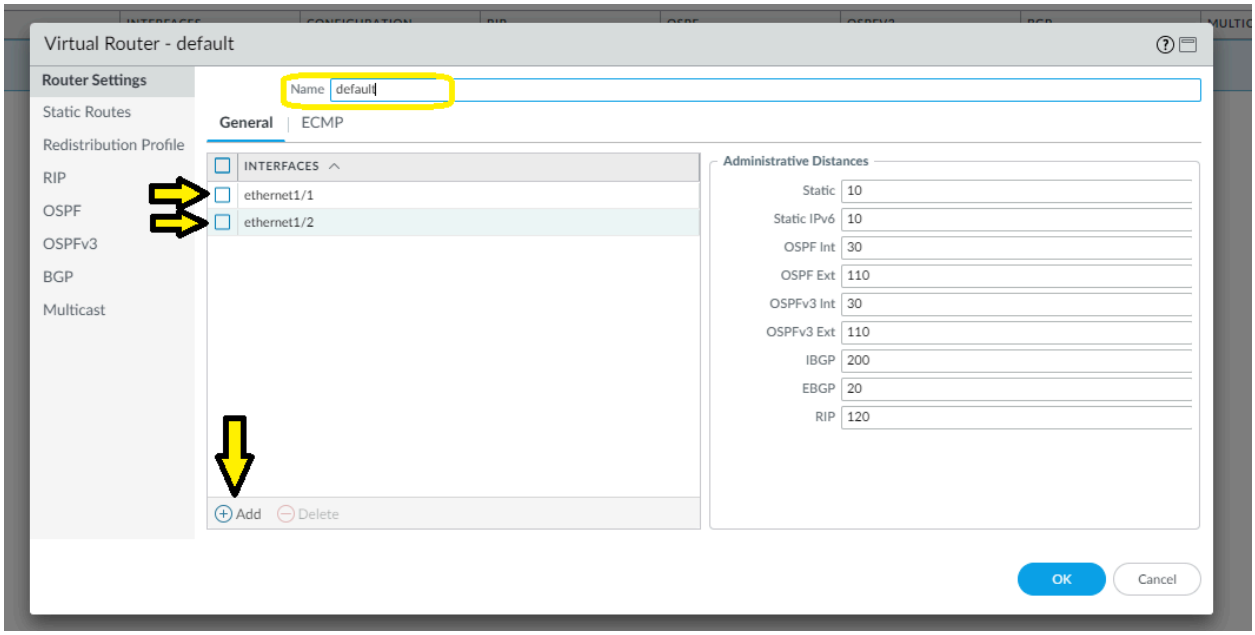
❖ **Step 28:**

Navigate to the “Virtual Routers” option in the “Network” tab. Select the “Add” Button at the bottom of the screen.



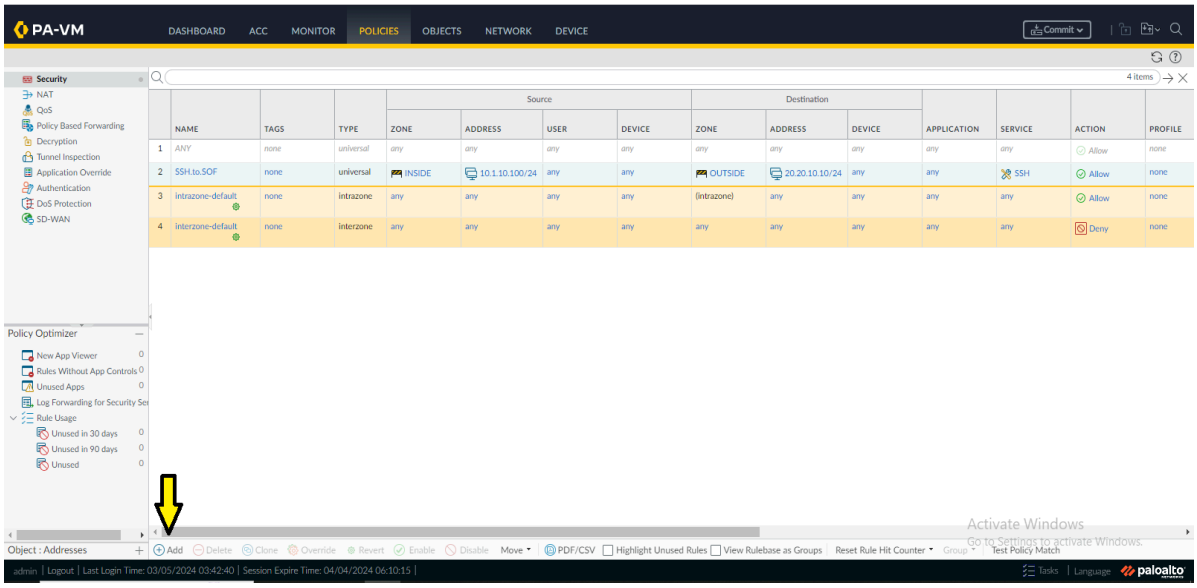
❖ **Step 29:**

Select the add button and add all the interfaces previously configured.



❖ **Step 30:**

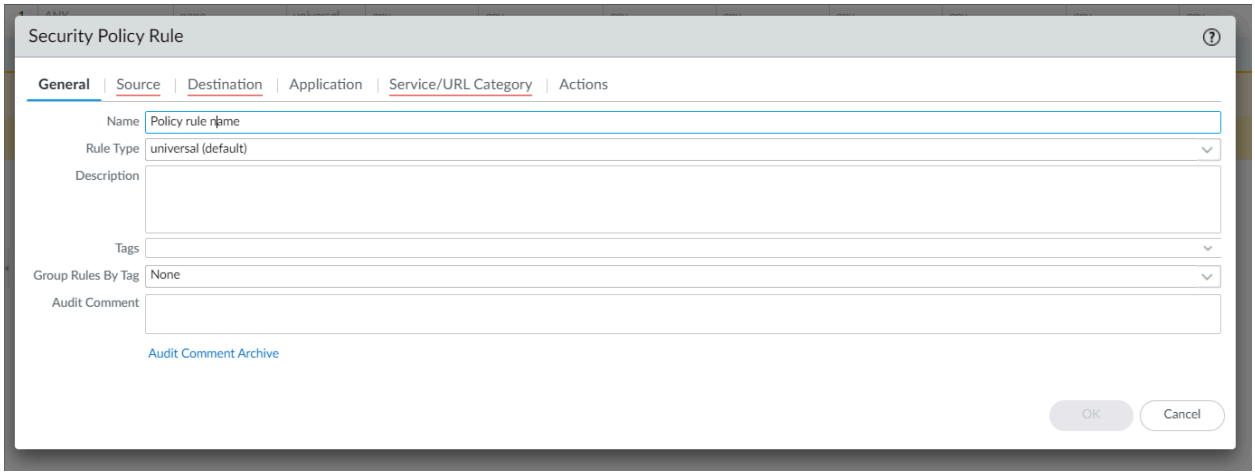
Navigate to the “Policies Tab and open the “Security” option in the left scroll pane. Then click the “Add” button



❖ **Step 31:**

Policies are the firewall rules being implemented on palo alto. Name them according to what they allow/block

Rule type: leave as universal

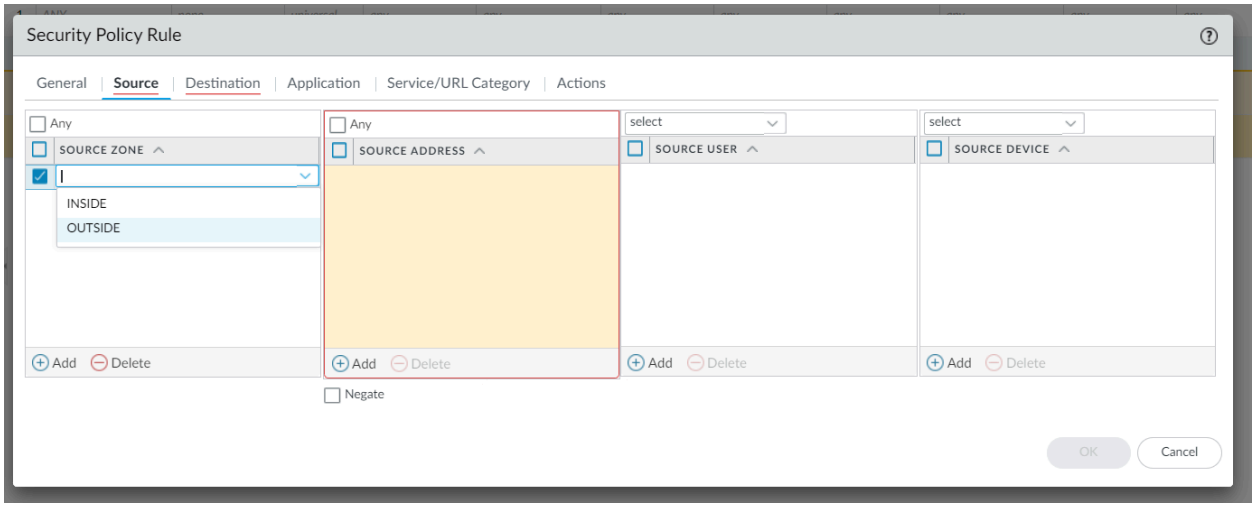


❖ **Step 32:**

Source and destination refer to the traffic flow through the firewall.

source zone:

- if going from within your network to out. Source is INSIDE
- If originating from outside your network coming in. Source is OUTSIDE



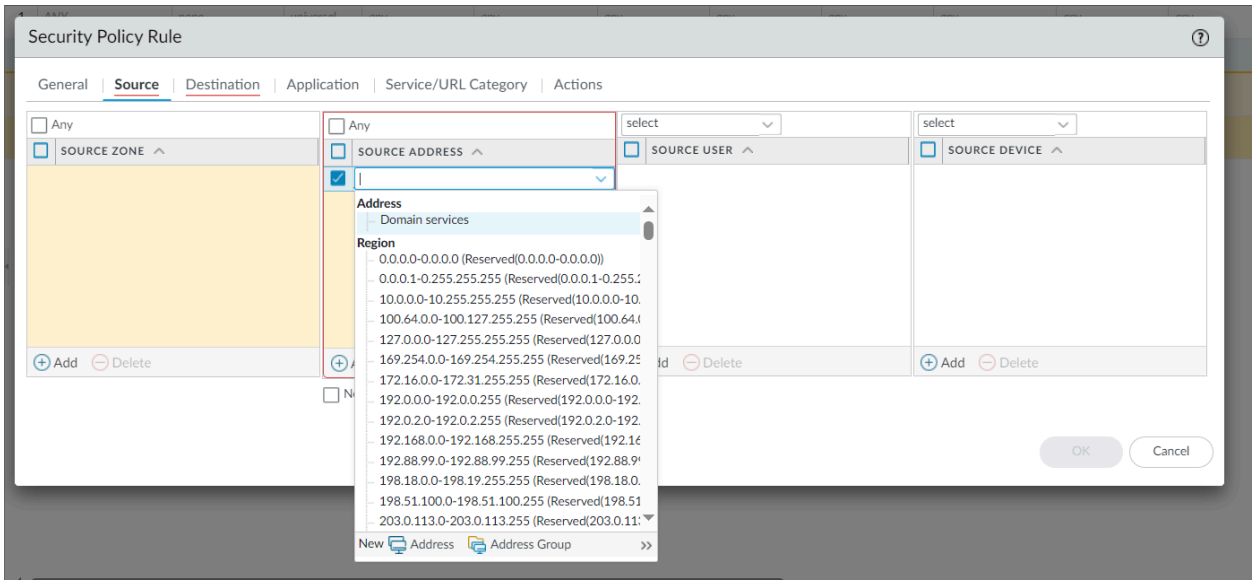
❖ **Step 33:**

Source Address:

- Interface IP associated with the zone selected
  (Ex. Source zone=INSIDE ; Source Address=10.1.10.100)

Source User & Source Device:

- Leave blank

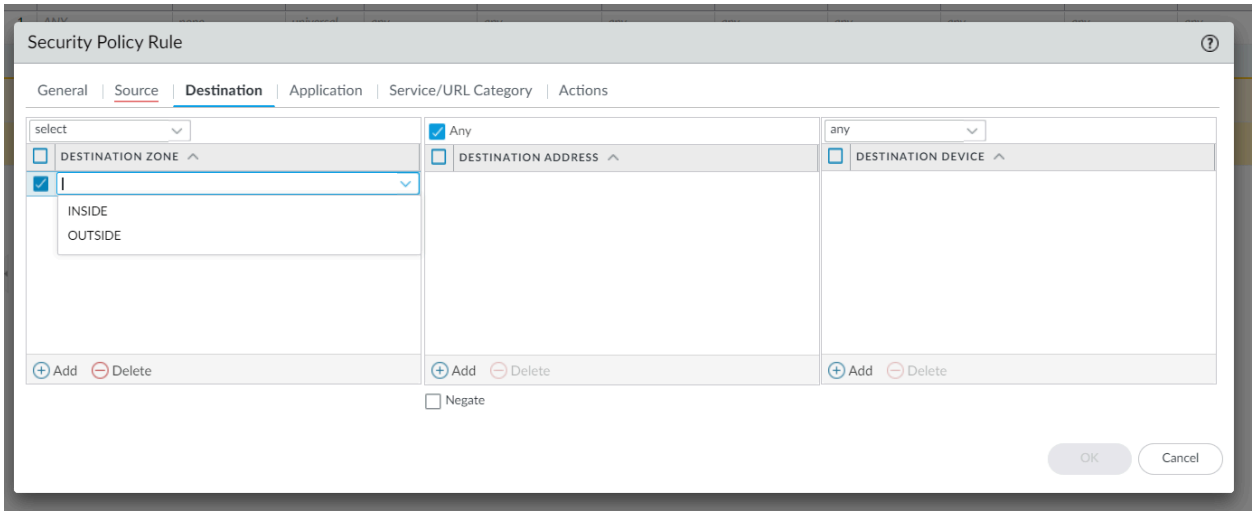


❖ **Step 34:**

Destination Zone:

The endpoint of the traffic you want to allow/block

- if going from within your network to out. Destination is OUTSIDE
- If originating from outside your network coming in. Destination is INSIDE



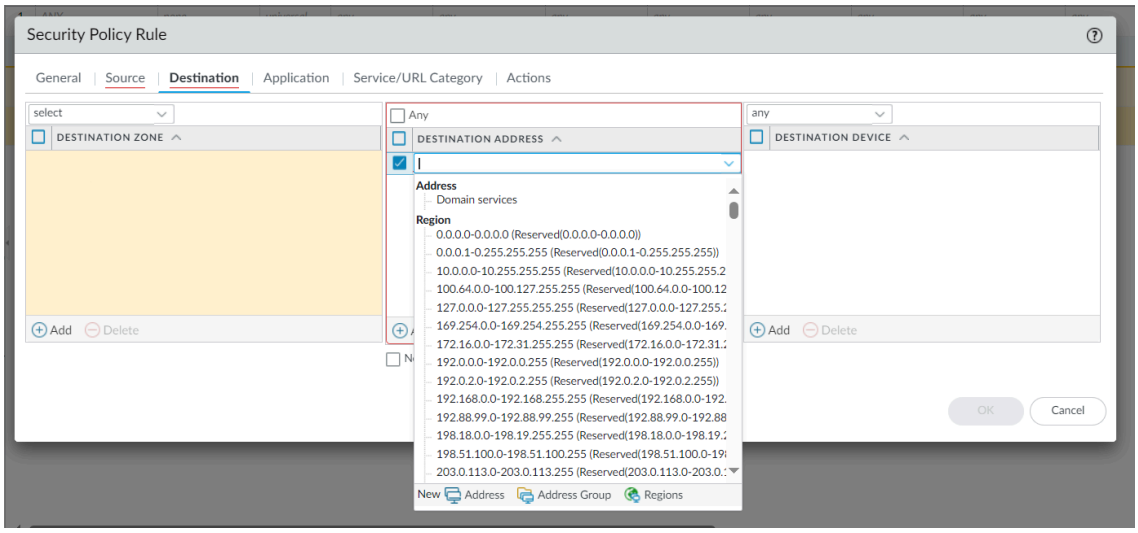
❖ **Step 35:**

Source Address:

- Network IP range of the source zone selected
  (Ex. Source zone=OUTSIDE ; Destination Address=20.20.10.10)

Source User & Source Device:

- Leave blank

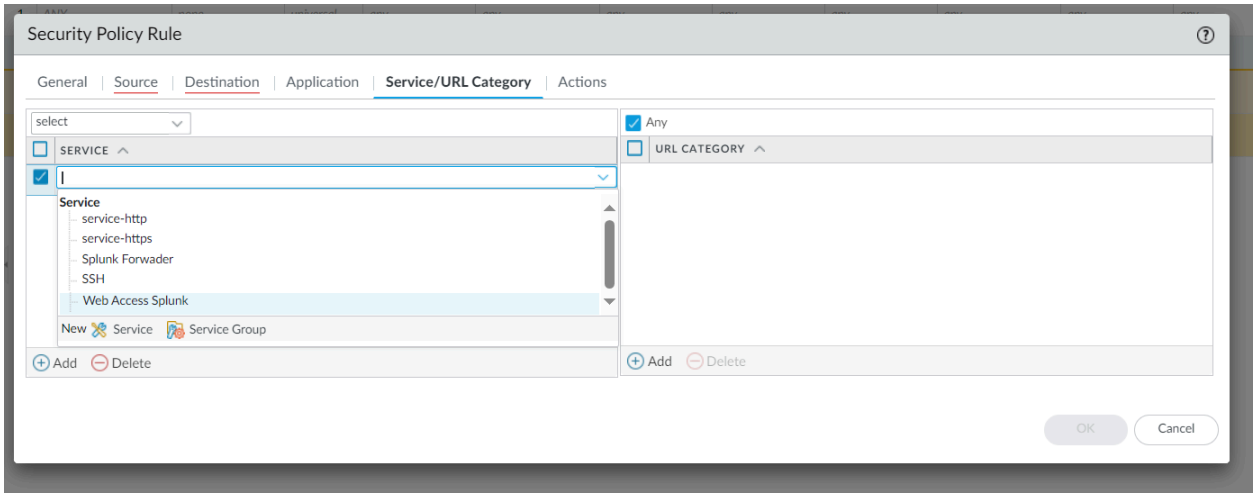


❖ **Step 36:**

Services are another way of fingerprinting traffic as it passes through the firewall, Allowing/blocking ports and protocols.

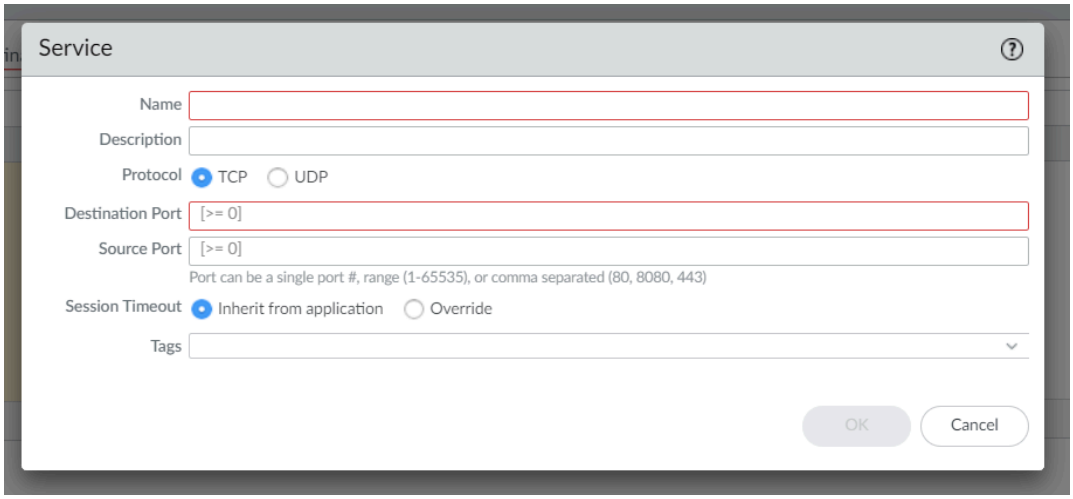
- Select New Service

- URL Category: Leave default



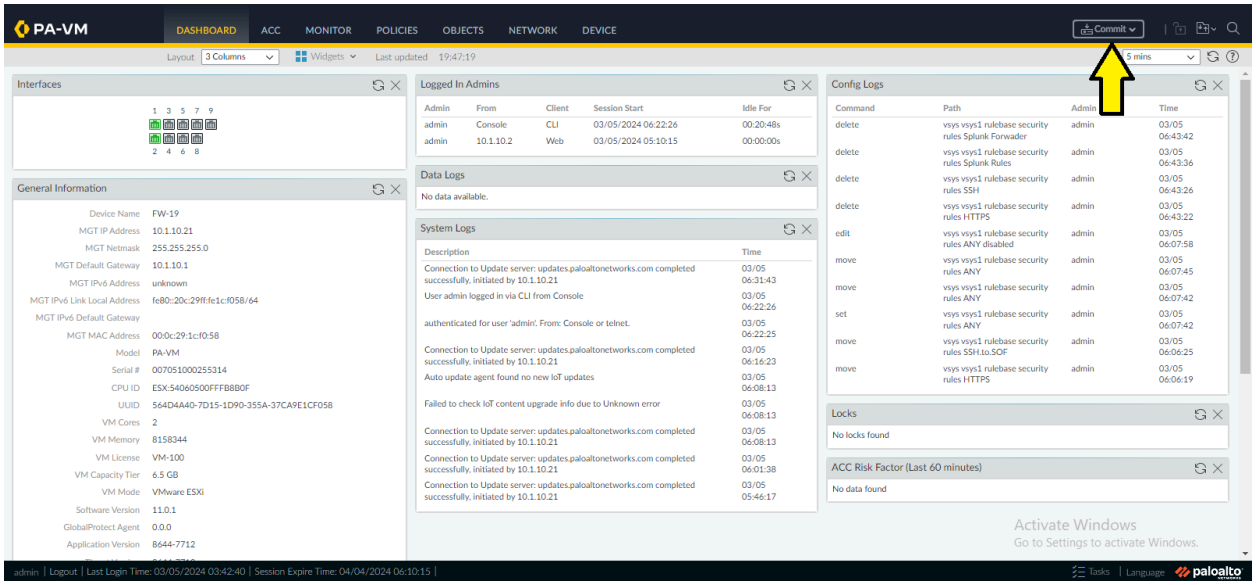
❖ **Step 37:**

- Name your Service something recognizable (HTTPS / SSH)
- Specify if the Service uses the TCP or UDP protocol
- Specify Destination & Source ports assigned to the service
  (SSH -> Destination Port=22 , Source Port=1-65535)
  1-65535 represents ANY



❖ **Step 38:**

Once all the configurations are done, Select the “Commit” Button in the top right hand corner.
If you don't do this all your configurations will not be applied, erasing your work.



❖ **Step 39:**
Select “commit”