Palo Alto Networks

VMware Workstation 10.0 Academy Labs

Deployment Guide

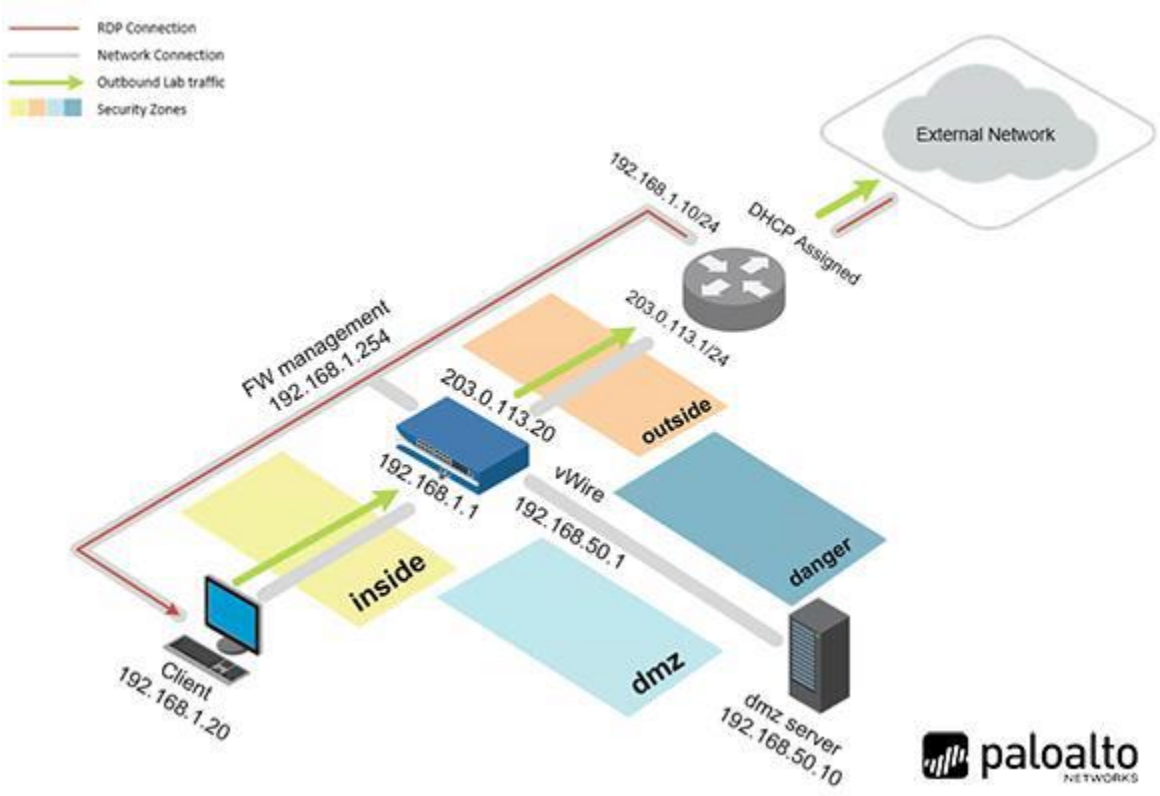
Document Version: 2021-12-23

Contents

Introduction

This document provides detailed guidance on performing the installation and configuration of the Palo Alto Networks Firewall 10.0 Essentials (EDU-210) pod on the VMWare Workstation system. This document will also be used to configure your installation for both the Enterprise Security Deployment (formerly known as CIC) and Enterprise Security Management (formerly known as CPC).

The Palo Alto Networks Firewall 10.0 lab pod is a 100% virtual machine pod consisting of four virtual machines. Linked together through virtual networking, these four virtual machines provide the environment for a student or a team to perform the Palo Alto Networks Academy Firewall 10.0 labs that reinforce the learning material in our Palo Alto Networks Academy courses.



Overview

The purpose of this document is to help you, the faculty member or student in the deployment of the Palo Alto Networks Firewall VM50 appliance, DMZ server, Virtual Router and Client Machine using VMWare Workstation Pro.

It is important to follow the steps as is so that you will not experience any issues during the learning experience.

All steps in this document were created and verified using:

Product: VMware Workstation 16 Pro

Version: 16.2.1 build-18811642

Note: Most VMware workstations are backward compatible. As in, newer versions will take older virtual machines, but older VMware workstations will not take the VMs created in newer versions of VMware.

VMWare Workstation Downloads and Resources:

The following links will direct you to VMWare where you can access and download VMware Workstation.

The first link directs you to VMWare's Academic Subscription Site.

The other links map to VMWare Standard License product downloads and resources. VMware workstation Pro is available as a free 30 day trial. You do not need to create a VMWare account to download the free trial.

https://vmapss.onthehub.com/WebStore/Welcome.aspxhttps://docs.vmware.com/en/VMware-Workstation-Pro/index.html

https://www.vmware.com/products/workstation-pro.html

https://customerconnect.vmware.com/downloads/info/slug/desktop_end_user_computing/vmware_workstation_pro/16_0

https://www.vmware.com/products/workstation-pro/workstation-pro-evaluation.html

https://docs.vmware.com/en/VMware-Workstation-Pro/16.2.1/rn/VMware-Workstation-1621-Pro-Release-Notes.html

Lab Scenario:

All the virtual machines for this VMware Workstation lab pod are preconfigured with IP addresses that match the subnets for the VMnets outlined in this lab document. If you want to change your Workstation VMnet subnets, then you will have to change the IP addresses of the virtual machines in this lab pod to correspond with your changed subnet network IDs.

In this lab, you will:

1. Configure your host computer's VMware Workstation VMnets for your VM-50 lab pod.
2. Download and import the academy lab pod OVAs from the Faculty Resources Module in your specific course. The VM-50 workstation appliance Firewall ova that is pre-

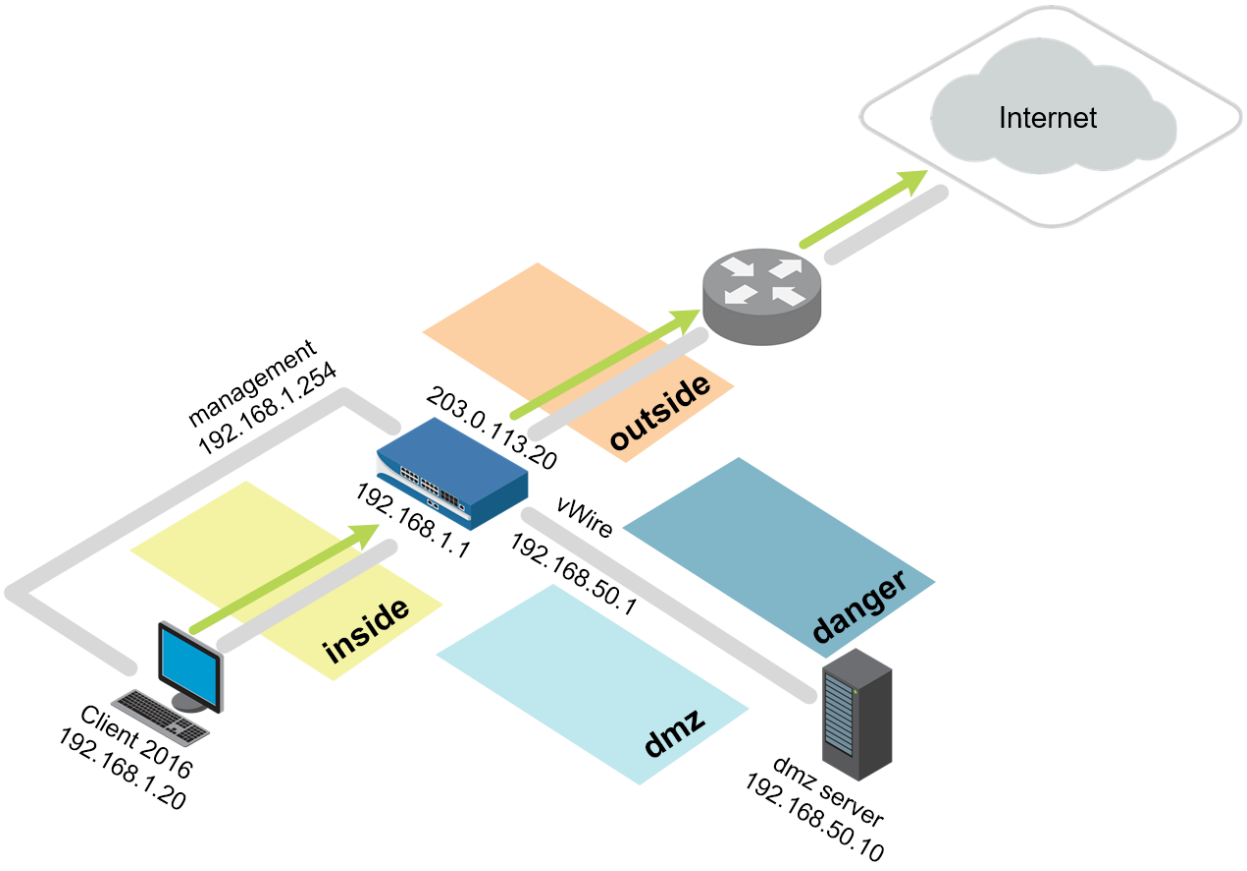
configured to operate on the Workstation VMnets.

- Import the workstation-vm50 ova into your host computer's VMware Workstation application and assign the network adapters to the correct VMnets.
- Import the workstation-dmz ova into your host computer's VMware Workstation application and assign the network adapters to the correct VMnets.
- Import the workstation-vr ova into your host computer's VMware Workstation application and assign the network adapters to the correct VMnets.
- Import the client ova into your host computer's VMware Workstation application and assign the network adapter to the correct VMnet.
- License your VM-50 workstation appliance with provided AUTH code, check to ensure your firewall correctly installs the licenses on your appliance and perform dynamic updates.

Note: only an authorized academy instructor can request AUTH codes from the Palo Alto Networks Academy team.

Configuration Diagram Usernames and Passwords

The information in the diagram and table below contains information you will need to complete this lab.



Usernames and Passwords

Virtual Machine	IP Address	Username	Password
Client	192.168.1.20	lab-user	Pal0Alt0!
DMZ	192.168.50.10	root	Pal0Alt0!
Firewall	192.168.1.254	admin	Pal0Alt0!
VRouter	192.168.1.10	root	Pal0Alt0!

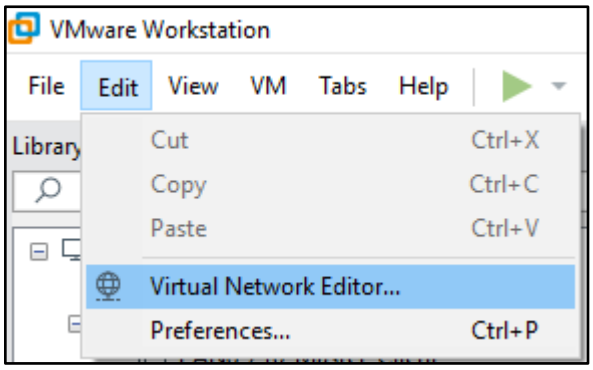
Lab Solution:

1. Windows VMware Workstation Setup Instructions for Palo Alto Networks PAN OS 10.0 Pod

1.1. Configure your host computer's VMware Workstation VMnets for your VM-50 lab pod. Before you begin installing your virtual machines you will need to create the necessary virtual network.

1.2. Open VMware Workstation and access the Virtual Network Editor by navigating to:

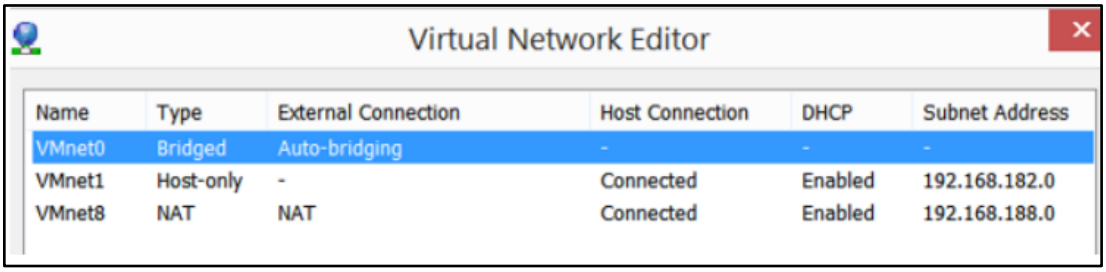
Edit > Virtual Network Editor.



Note: You may need administrator privileges here to make a change. To do this please select the *Change Settings* button.

1.3. Your lab environment will need 6 Virtual Networks. Two of them, VMNet0 and VMNet8 will be built by default. You may also have a third adapter, VMNet1 that you will customize. If your network settings do not display VMNet1, that is ok, you will create it when you create the other adapters.

VMNet0 – Type: Bridged. Used to connect to the local host
VMNet8 – Type: NAT. Used to assign DHCP addresses to the VMs



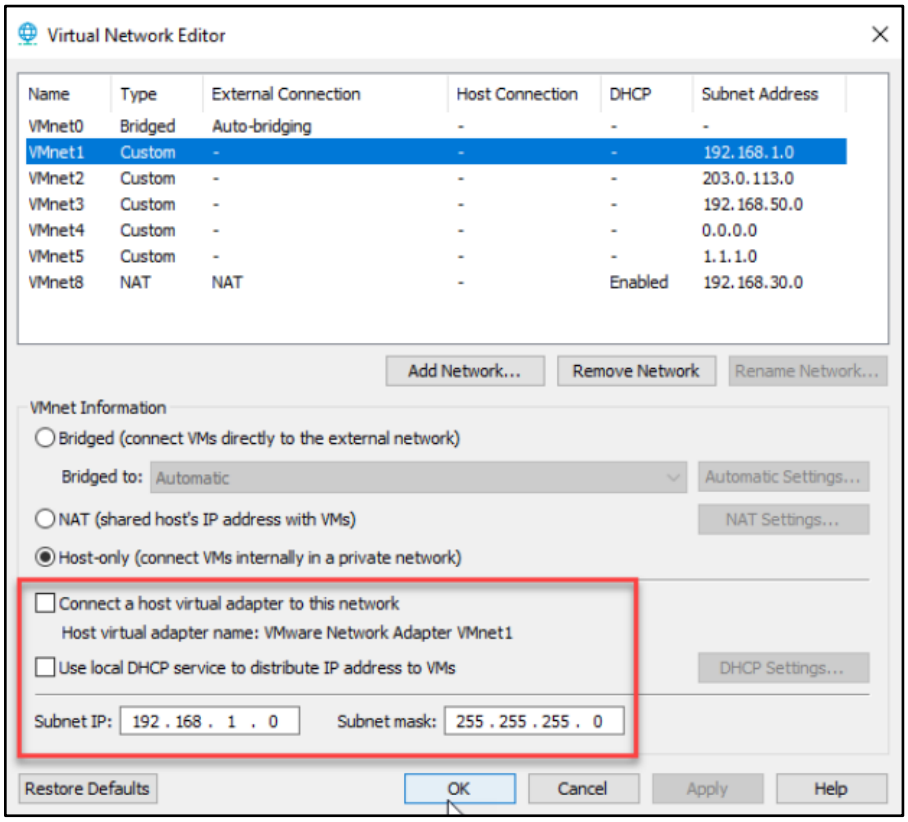
Possibly you may also see: VMNet1 – Type: Host-only.

** If it appears you will customize this adapter as directed in the following steps. If it doesn't appear you will create it in the following steps.

1.4. In the Virtual Network Editor dialog box, select to highlight "*VMnet1*" and under "VMnet Information" do the following:

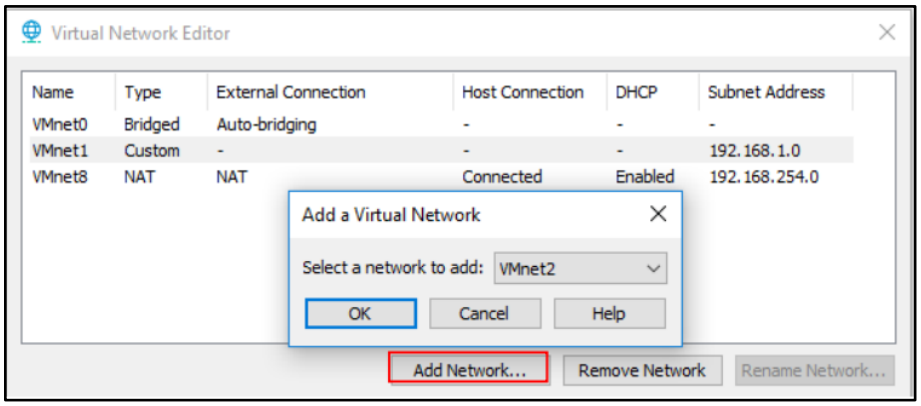
1.4.1. Select the radial button, "*Host-only*" (connect VMs internally in a private network

1.4.2. Set the "Subnet IP" to **192.168.1.0** and the "Subnet mask" to **255.255.255.0**



1.4.3. Click *Apply*.

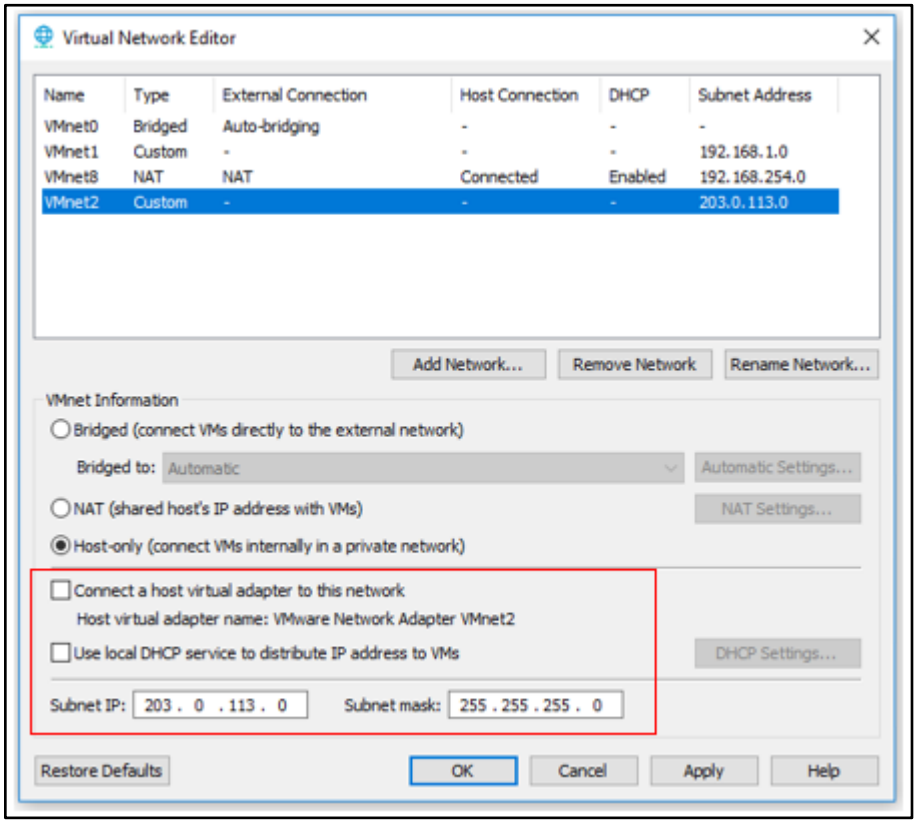
1.5. In the "Virtual Network Editor" dialog box, select "*Add Network*" and then select *OK*.



1.5.1. In the "Virtual Network Editor" dialog box for VMnet2, uncheck the boxes next to "*Connect a host virtual adapter to this network*" and uncheck "*Use local DHCP service to distribute IP addresses to VMs*".

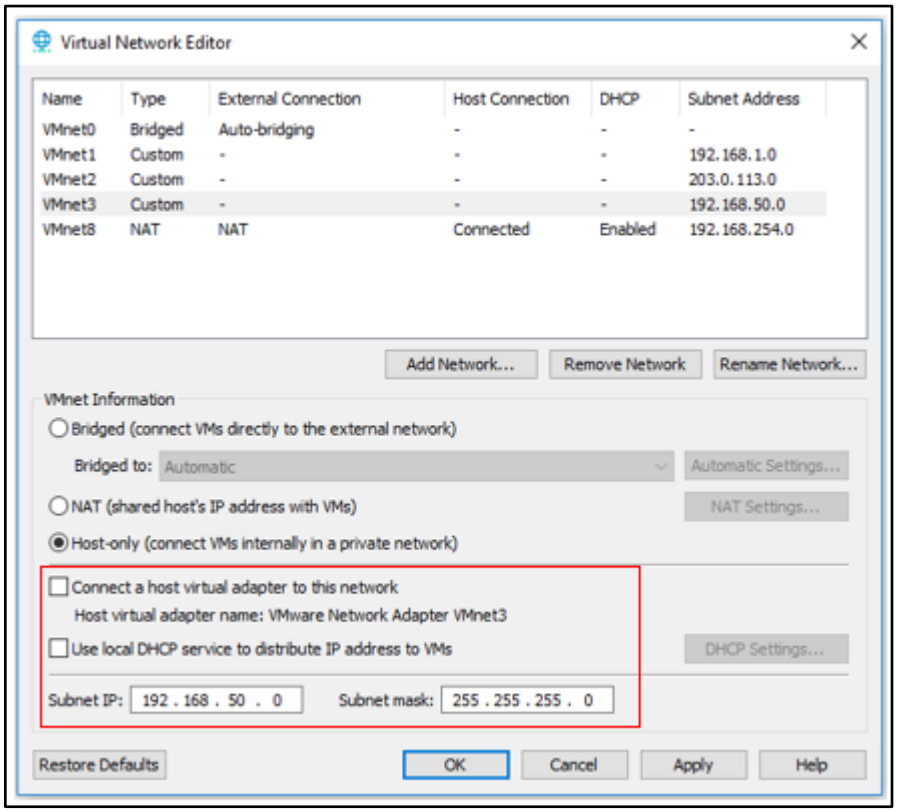
For Subnet Address enter **203.0.113.0** and for Subnet Mask enter **255.255.255.0**

1.5.2. Click *Apply*.



1.6. In the "Virtual Network Editor" dialog box, select "*Add Network*".

1.6.1. In the "Virtual Network Editor" dialog box for VMnet3, uncheck the boxes next to "*Connect a host virtual adapter to this network*" and uncheck "*Use local DHCP service to distribute IP addresses to VMs"*.



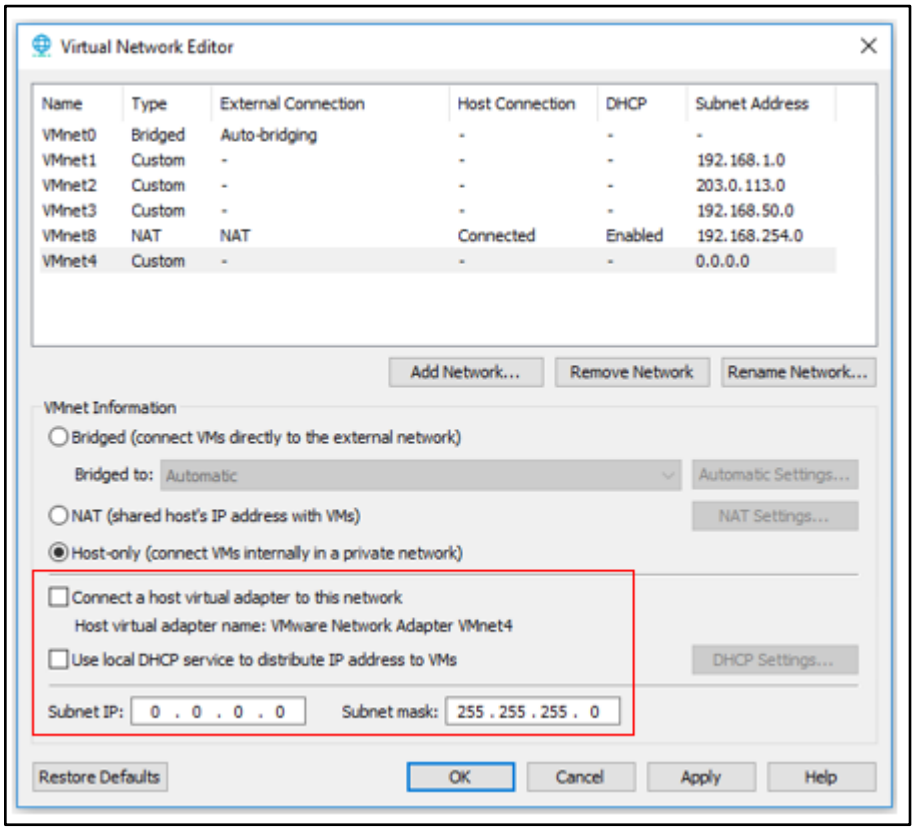
1.6.2. For Subnet IP enter **192.168.50.0** and for Subnet Mask enter **255.255.255.0**

1.6.3. Click *Apply*.

1.7. In the "Virtual Network Editor" dialog box, select "*Add Network*".

1.7.1. In the "Virtual Network Editor" dialog box for VMnet4, *uncheck* the boxes next to "Connect a host virtual adapter to this network" and *uncheck* "Use local DHCP service to distribute IP addresses to VMs".

For Subnet IP enter **0.0.0.0** and for Subnet Mask enter **255.255.255.0**

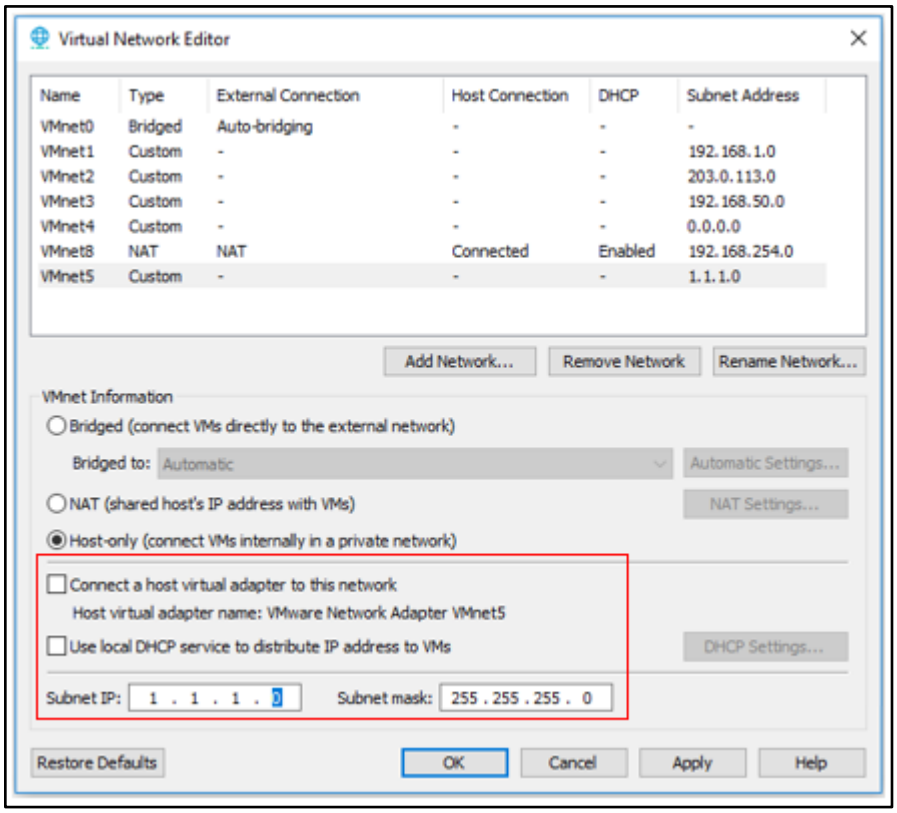


1.7.2. Click *Apply.*

1.8. In the "Virtual Network Editor" dialog box, select "**Add Network**".

1.8.1. In the "Virtual Network Editor" dialog box for VMnet5, *uncheck* the boxes next to "Connect a host virtual adapter to this network" and *uncheck "*Use local DHCP service to distribute IP addresses to VMs".

1.8.2. For Subnet IP enter **1.1.1.0** and for Subnet Mask enter **255.255.255.0**.



1.8.3. Click *Apply*.

1.9. In the "Virtual Network Editor" dialog box, select VMnet 8.

1.9.1. Select the radial button NAT (Share host's IP address with VMs)

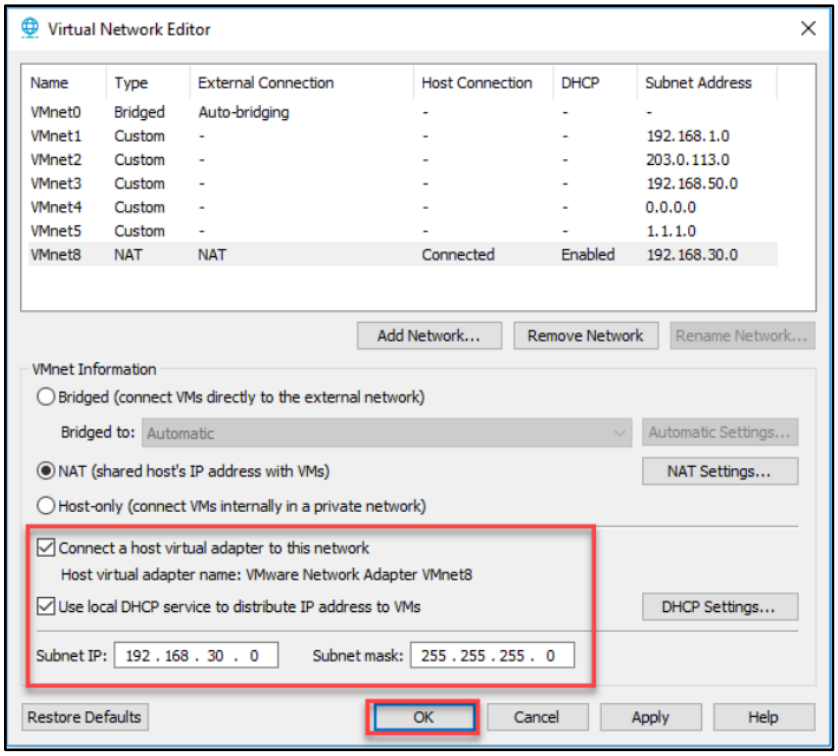
Note: Your VMnet8 NAT Subnet Address should be automatically assigned and will likely be different than the display below. **Please make sure vmnet8 does not use the same subnet as vmnet1, 192.168.1.0/24, in order to prevent address collision.** You can change your NAT subnet address to **192.168.30.0** and the "Subnet mask" to **255.255.255.0** if you want but it is not necessary.

If you have any questions, please consult with your instructor.

If you change your NAT settings you may need to reboot your laptop for these settings to be applied.

1.9.2. Ensure the box next to “Connect a host virtual adapter to this network” is checked.

1.9.3. Ensure the box next to “Use local DHCP service to distribute IP addresses to VMs” is checked.



1.9.4. Click *Apply*.

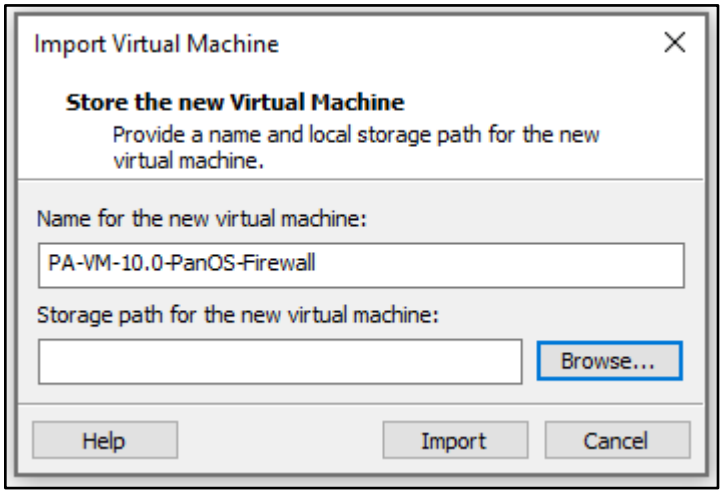
1.9.5. Click *OK*.

Import and Configure Firewall on VMware Workstation

2. Download and Import the academy VM-50 workstation firewall appliance ova into your host computers VMware Workstation application and check to ensure appliance's network adapters are assigned to the correct VMnets.

2.1.1. In the VMware Workstation application click *File* and select *Open*.

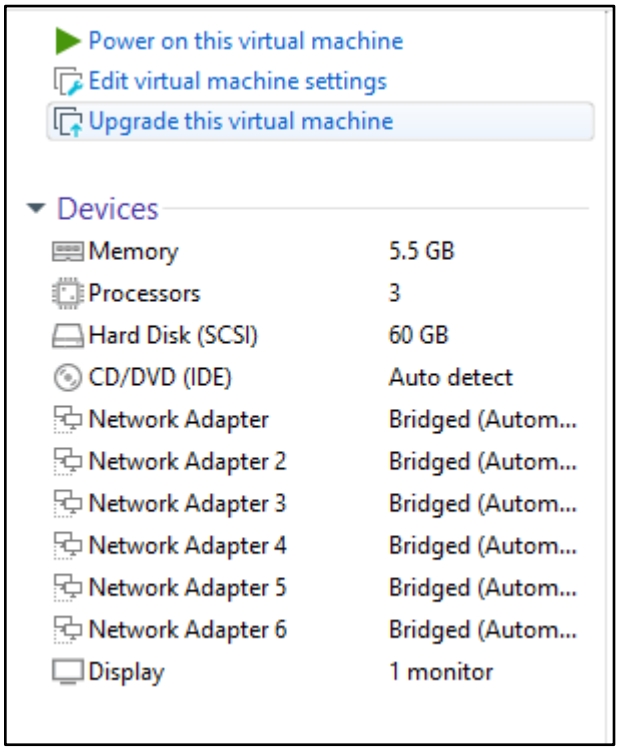
2.1.2. In the Open dialog box, browse to the location of the PA-VM-10.0-PanOS-Firewall OVA and select to open it.



2.1.3. In the "Import Virtual Machine" dialog box, choose the location of your PA-VM-10.0-PanOS-Firewall virtual machine.

2.1.4. Click *Import*.

2.1.5. In VMware workstation PA-VM-10.0-PanOS-Firewall, select edit *Virtual Machine Settings*



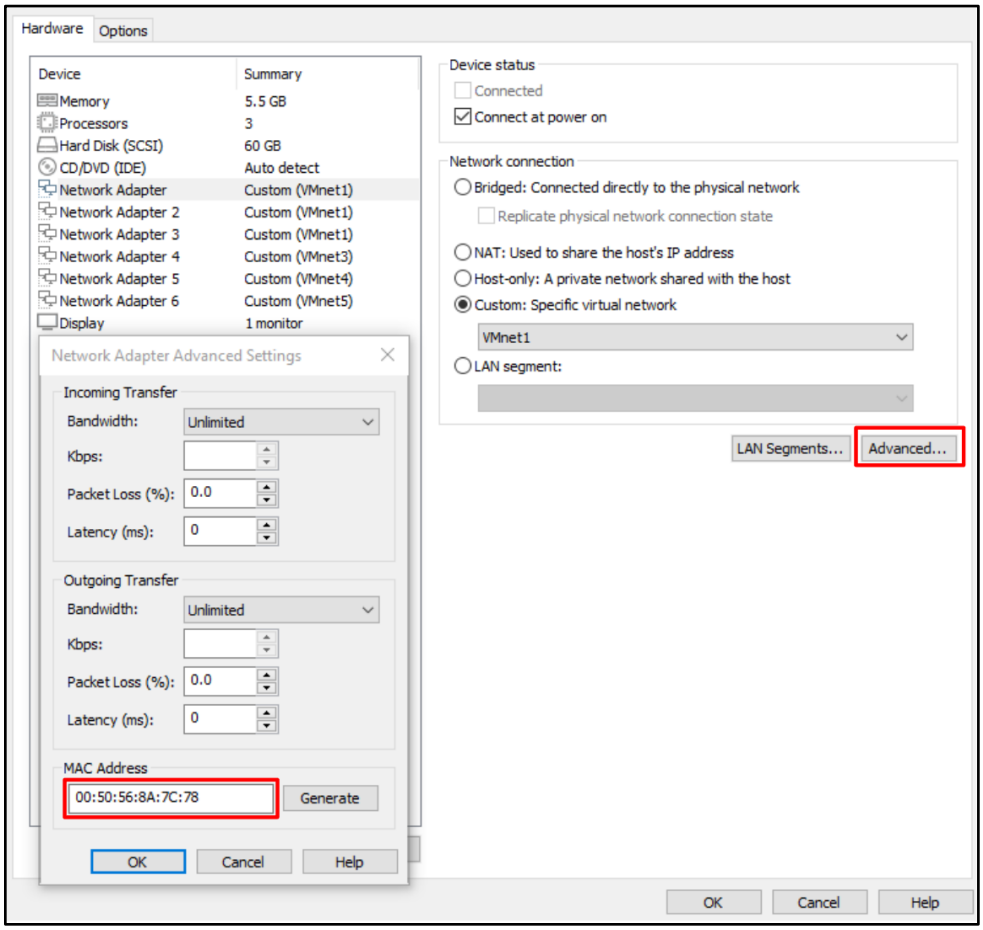
and in the dialog box make sure that:

Network adapter 1 is assigned to Custom “VMnet1”.
Network Adapter 2 is assigned to the Custom “VMnet2”.
Network Adapter 3 is assigned to Custom “VMnet1”.
Network Adapter 4 is assigned to Custom “VMnet3”.
Network Adapter 5 is assigned to Custom “VMnet4”.
Network Adapter 6 is assigned to “VMnet5”.
Network Adapter 7 is assigned to “Host-only”.

You will also need to change the MAC addresses associated with each network adapter.

2.1.6. In the Workstation on your PA-VM-10.0-PanOS-Firewall tab, select *edit virtual network settings* and assign the Network Adapter 1.

Select the *Advanced* option. Once in the Advanced menu please manually enter the following MAC Address: “**00:50:56:8A:7C:78**” and select *OK* 2 times.



Repeat this process for each network adapter on the firewall with the following MAC addresses.

NIC	MAC
Network Adapter 1	**00:50:56:8a:7c:78**
Network Adapter 2	**00:50:56:8a:91:be**
Network Adapter 3	**00:50:56:8a:91:c4**
Network Adapter 4	**00:50:56:8a:54:c7**
Network Adapter 5	**00:50:56:8a:84:17**
Network Adapter 6	**00:50:56:8a:b3:fc**

Note: Please make sure that the allocated memory for the VM50

appliance is at least **5.5 GB** of RAM. If you set this lower you lose some functionality in the VM-50 virtual appliance

2.1.7. Click **OK** to close the dialog box.

2.1.8. Do not power on the firewall yet.

Import and Configure Virtual Router on VMware Workstation

3. Import the PA-VM-10.0-PanOS-VRouter OVA into your host computer's VMware Workstation application and assign the client's network adapter to the correct VMnet2.

You will follow the same basic steps you did when importing your PA-VM-10.0-PANOS-Firewall.

The virtual router is configured with 3 destination NATs to connect from your host computer to your VMware Workstation pod as shown in the screen shot below. These destination NATs will allow you to do the following:

3.1.1.1. Connect to your PANOS 10.0.6 VM-50 firewall appliance's management interface WebUI using your host computer's Web browser and the destination https URL composed of the external address of your virtual router's ens160 interface;

3.1.1.2. Connect to your PANOS 10.0.6 VM-50 firewall appliance's management interface via ssh from PuTTY on your host computer using the destination IP address assigned to your virtual router's ens160 interface and

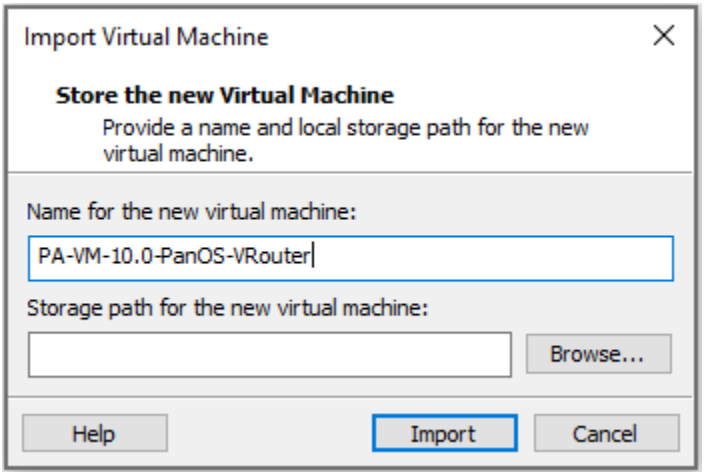
3.1.1.3. Connect to your pod's Server/Client via RDP/VNC using the destination IP address assigned to your virtual router's ens160 interface.

```
[root@pod-vr ~]# iptables -L -t nat
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination
DNAT       tcp  --  anywhere             anywhere             tcp dpt:ssh to:192.168.1.254
DNAT       tcp  --  anywhere             anywhere             tcp dpt:https to:192.168.1.254
DNAT       tcp  --  anywhere             anywhere             tcp dpt:ms-wbt-server to:192.168.1.20
```

3.1.2. In the VMware Workstation application click **File** and select **Open** in the drop-down menu.

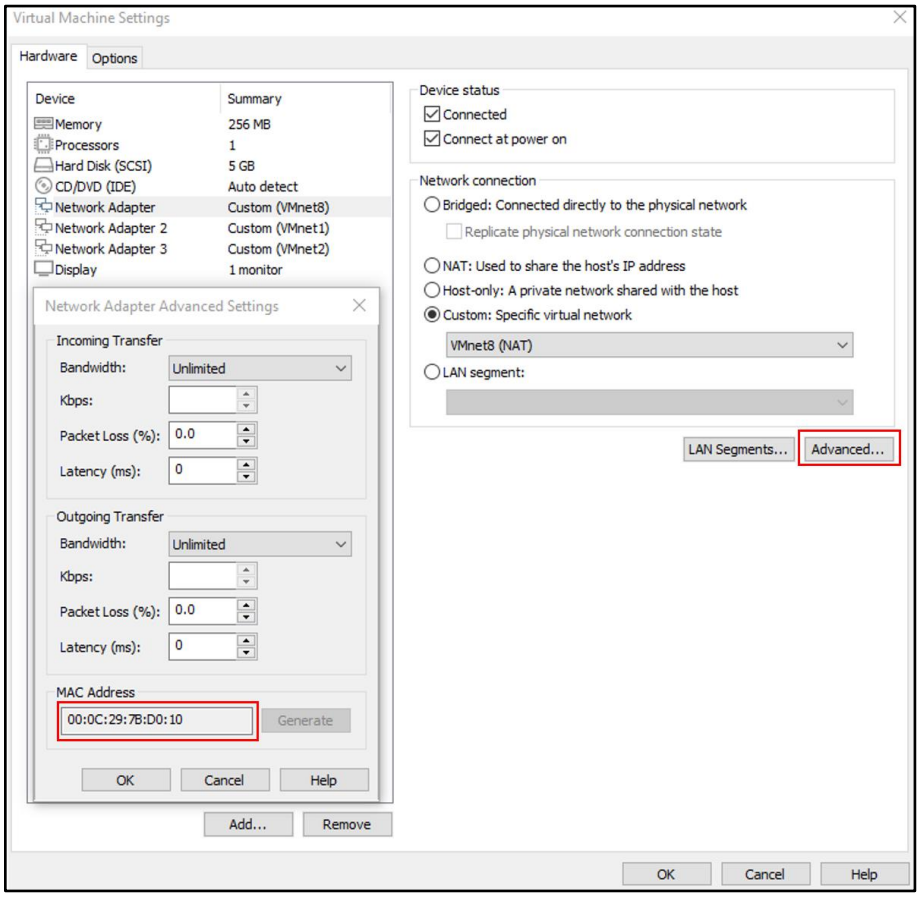
3.1.3. In the Open dialog box, browse to the location of the PA-VM-10.0-PanOS-VRouter OVA and select to open it.

3.1.4. In the “Import Virtual Machine” dialog box, choose the location of your virtual machine and click *Import*.



3.1.5. In Workstation on your PA-VM-10.0-PanOS-VRouter tab, select *edit virtual network settings* and assign the Network Adapter 1 to **NAT** (**VMnet8**)

3.1.6. Select the *Advanced* option. Once in the Advanced menu please manually enter the following MAC Address: “**00:0C:29:7B:D0:10**” and select *OK* 2 times.



3.1.7. Set Network Adapter 2 to “Custom(VMnet1)” and then select the *Advanced* option. Once in the Advanced menu please manually enter the following MAC Address: “**00:50:56:8A:C8:55**” and select *OK* 2 times.

3.1.8. Set Network Adapter 3 to “Custom(VMnet2)” and then select the *Advanced* option. Once in the Advanced menu please manually enter the following MAC Address: “**00:50:56:8A:A6:88**” and select *OK* 2 times.

3.1.9. *Power* on your PA-VM-10.0-PanOS-VRouter VM. You will need the VM’s built in router to connect your VM-50 management interface to the Internet for licensing.

3.1.10. *Log on* to the VR using the username **root** and password **Pal0Alt0!**. *Type* ifconfig and confirm that you can see the following:

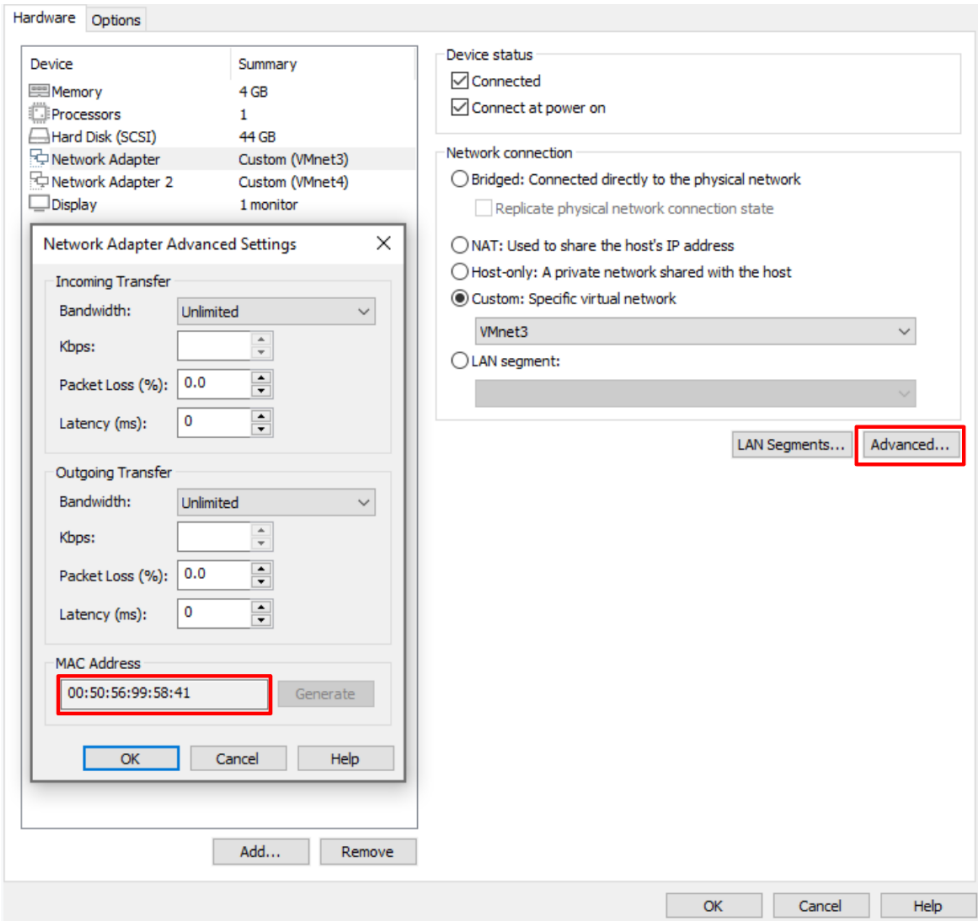
Note: If you do not see the IP addresses associated with each interface repeat the previous steps for the VR machine.

```
CentOS Linux 7 (Core)
Kernel 3.10.0-514.2.2.el7.x86_64 on an x86_64

pod-vr login: root
Password:
Last login: Mon Dec 13 16:01:35 on tty1
[root@pod-vr ~]# ifconfig
ens160: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.30.10  netmask 255.255.255.0  broadcast 192.168.30.255
        ether 00:0c:29:df:af:96  txqueuelen 1000  (Ethernet)
        RX packets 136687  bytes 190483750 (181.6 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 59959  bytes 4447624 (4.2 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

ens192: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.10  netmask 255.255.255.0  broadcast 192.168.1.255
        ether 00:50:56:8a:c8:55  txqueuelen 1000  (Ethernet)
        RX packets 789  bytes 50496 (49.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4  bytes 168 (168.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

ens224: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 203.0.113.1  netmask 255.255.255.0  broadcast 203.0.113.255
        ether 00:50:56:8a:a6:88  txqueuelen 1000  (Ethernet)
        RX packets 59247  bytes 4935502 (4.7 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 136049  bytes 189829549 (181.0 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        loop  txqueuelen 1  (Local Loopback)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Import and Configure DMZ Server on VMware Workstation

4. Import the PA-VM-10.0-PanOS-DMZ ova into your host computer's VMware Workstation application and assign the client's network adapter to the correct VMnet2. Follow the same steps as you have done for both the FW and the VR virtual machines previously.

    4.1.1. In the Workstation on your PA-VM-10.0-PanOS-DMZ tab, select *edit virtual network settings* and assign the **Network Adapter 1** to "Custom(**VMnet3**)", and then select the *Advanced* option. Once in the Advanced menu please manually enter the following MAC Address: "**00:50:56:99:58:41**" and select *OK* 2 times.



4.1.2. In the Workstation on your PA-VM-10.0-PanOS-DMZ tab, select edit virtual network settings and assign the Network Adapter 2 to “Custom(VMnet4)”, and then select the Advanced option. Once in the Advanced menu please manually enter the following MAC Address: “**00:50:56:99:DB:43**” and select OK 2 times.

4.1.3. *Power* on your PA-VM-10.0-PanOS-DMZ VM.

4.1.4. *Log on* to the DMZ using the username **root** and password **Pal0Alt0!**. Type ***ifconfig*** and confirm that you can see the following:

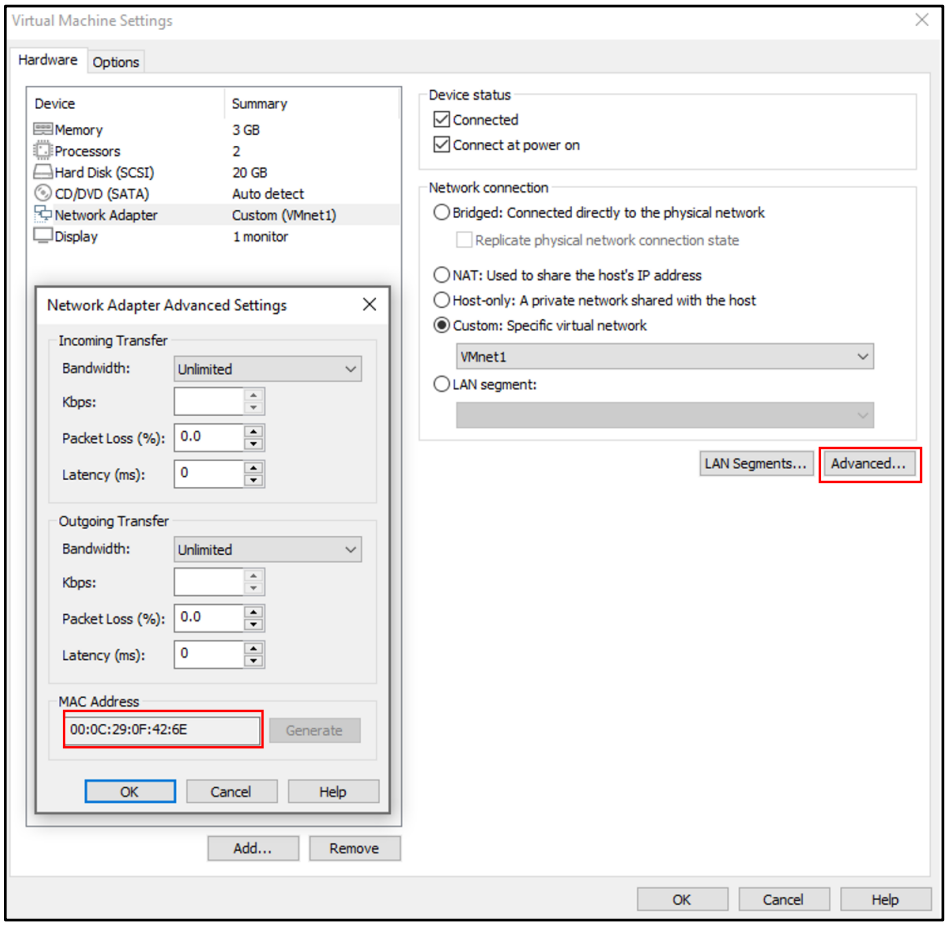
Note: If you do not see the IP addresses associated with each interface repeat the previous steps for the DMZ machine.

```
CentOS Linux 7 (Core)
Kernel 3.10.0-693.2.2.el7.x86_64 on an x86_64

pod-dmz login: root
Password:
Last login: Fri May 17 14:28:11 on tty1
[root@pod-dmz ~]# ifconfig
ens192: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.50.10  netmask 255.255.255.0  broadcast 192.168.50.255
        ether 00:0c:29:db:75:d9  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 17  bytes 1020 (1020.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

ens192:1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.50.11  netmask 255.255.255.0  broadcast 192.168.50.255
        ether 00:0c:29:db:75:d9  txqueuelen 1000  (Ethernet)

ens224: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        ether 00:0c:29:db:75:e3  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        loop  txqueuelen 1  (Local Loopback)
        RX packets 31  bytes 3564 (3.4 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 31  bytes 3564 (3.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo:10: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 172.16.2.11  netmask 255.255.255.0
        loop  txqueuelen 1  (Local Loopback)
```

Import and Configure Linux Client on VMware Workstation

5. Import the PA-VM-10.0-PanOS-Client ova into your host computer's VMware Workstation application and assign the client's network adapter to the correct VMnet2. Follow the same steps as you have done for both the FW and the VR virtual machines previously.

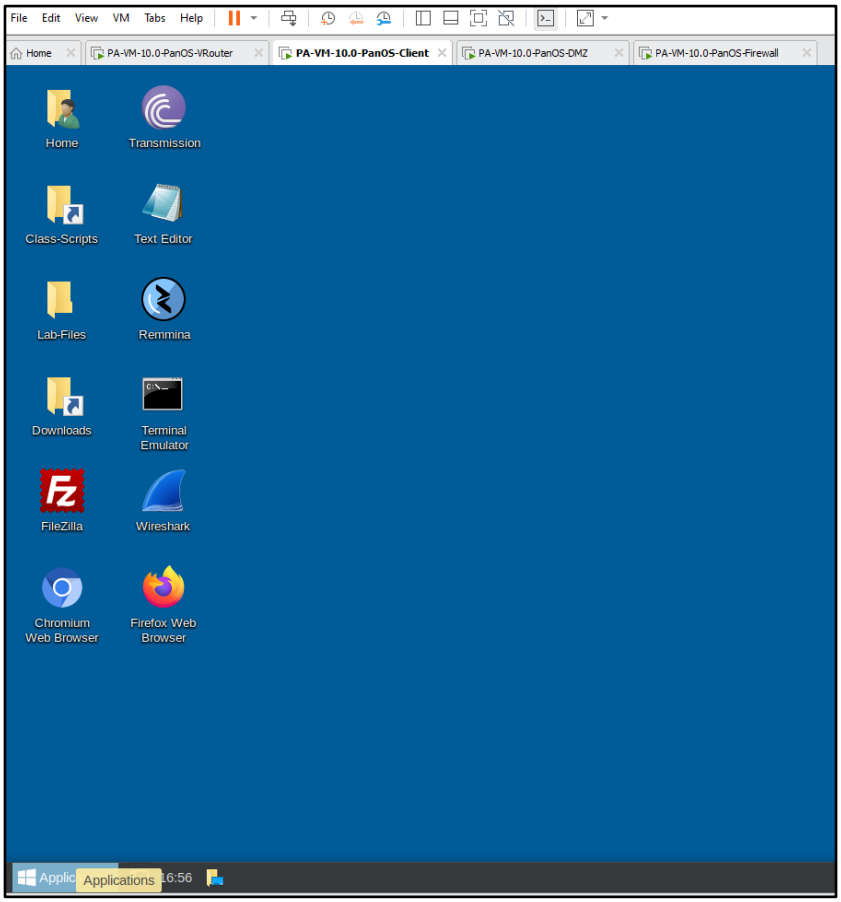
    5.1.1. In Workstation on your PA-VM-10.0-PanOS-Client tab, select *edit virtual network settings* and assign the Network Adapter to "Custom(VMnet1)", and then select the *Advanced* option. Once in the Advanced menu please manually enter the following MAC Address: "**00:0C:29:0F:42:6E**" and select *OK* 2 times.



5.1.2. *Power* on your PA-VM-10.0-PanOS-Client VM.

5.1.3. *Log on* to the Client using the username **lab-user** and password **Pal0Alt0!**.

5.1.4. You should see the following screen:



License Firewall on VMware Workstation

6. License your VM-50 workstation appliance with provided AUTH code, check that your firewall correctly installs the licenses on your appliance and perform dynamic updates.

Note: If you have not already received a VM50 firewall license please ask your instructor.

6.1.1. In the VMware workstation PA-VM-10.0-PanOS-Firewall tab, select "*Power on this virtual machine*". Your VM-50 appliance will start the boot up process.

Note: This will take approximately 5 minutes if not a little longer. Make sure your VR virtual machine is powered on and connected to correct VMnets before attempting licensing.

The VR provides routing to the Internet for your VM-50 appliance which you will need to license your VM 50 appliance by connecting to the

updates.paloaltonetworks.com server.

6.1.2. Log onto your firewall with username **admin** and password "**Pal0Alto!**". Type the following command "**show interface management**" and click *enter*.

Note: Your IP address should match 192.168.1.254.

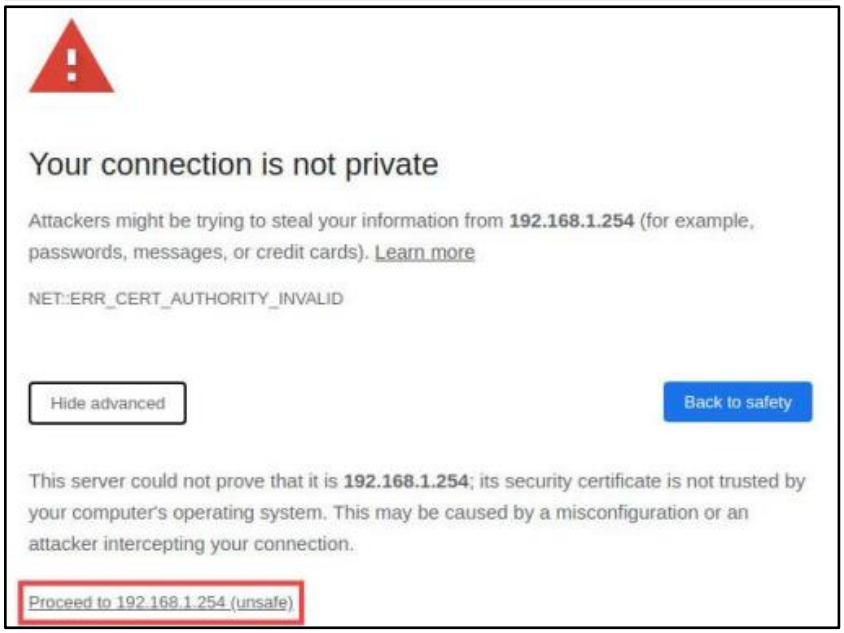
```
Name: Management Interface
Link status:
  Runtime link speed/duplex/state: 10000/full/up
  Configured link speed/duplex/state: auto/auto/auto
MAC address:
  Port MAC address 00:0c:29:64:45:88

Ip address: 192.168.1.254
Netmask: 255.255.255.0
Default gateway: 192.168.1.10
Ipv6 address: unknown
Ipv6 link local address: fe80::20c:29ff:fe64:4588/64
Ipv6 default gateway:
```

Also enter the following to verify connectivity: "**ping host 8.8.8.8**"

```
admin@firewall-a> ping host 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=127 time=7.73 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=127 time=7.66 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=127 time=7.39 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=127 time=8.94 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=127 time=7.47 ms
^C
--- 8.8.8.8 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4007ms
rtt min/avg/max/mdev = 7.392/7.841/8.944/0.575 ms
admin@firewall-a>
```

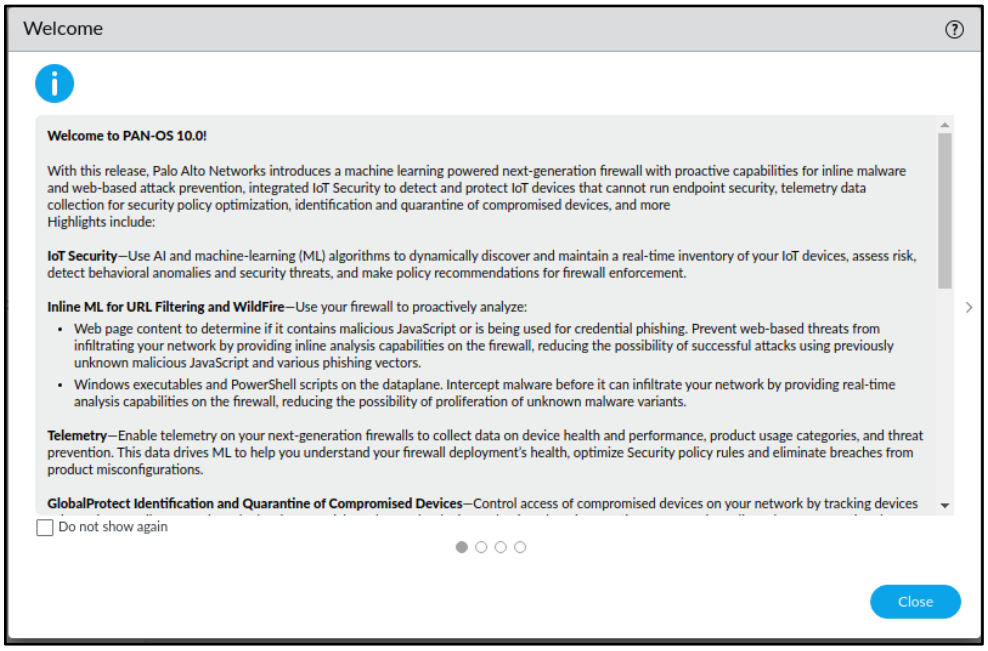
6.1.3. Open your *Chromium* browser on the client desktop and connect to your VM-50 virtual firewall Web-UI by entering ***https://192.168.1.254*** in the browser's URL.

A privacy error will occur, click "*Advanced*" and then click "*Proceed to 192.168.1.254* (unsafe).

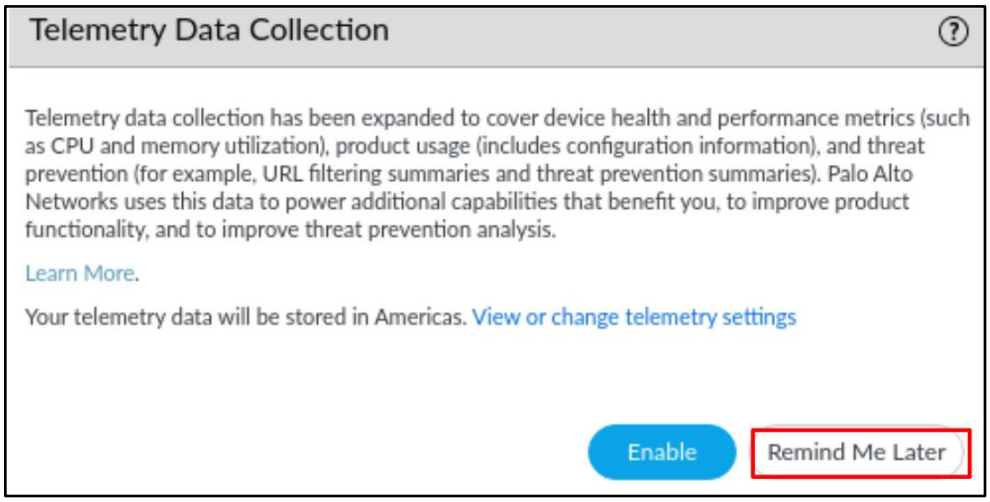


6.1.4. Log into your VM-50 appliance using username: "***admin***" and password: "***Pal0Alt0!***".

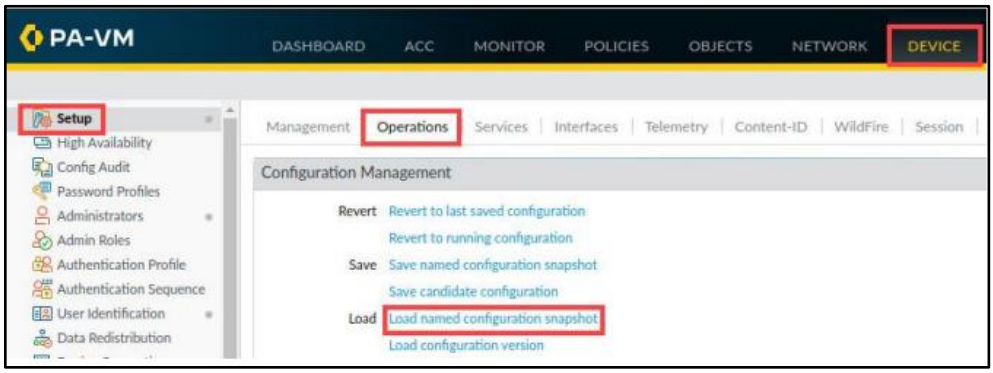
6.1.5. Click ***Close*** on the Welcome Screen.



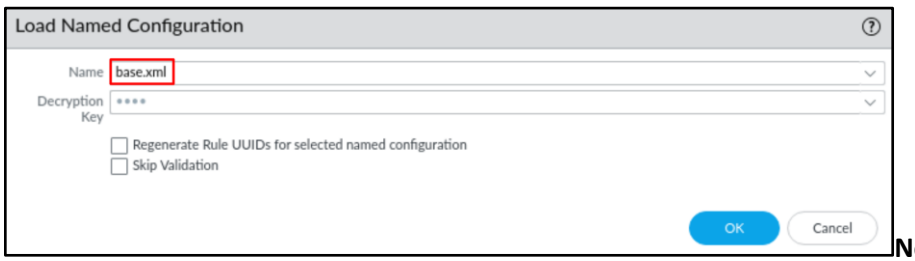
6.1.6. Choose to ***Remind Me Later*** on the Telemetry Data Collection screen.



6.1.7. Navigate to *Device>Setup>Operations* in the web interface and click on ***Load named configuration snapshot*** underneath the Configuration Management section.



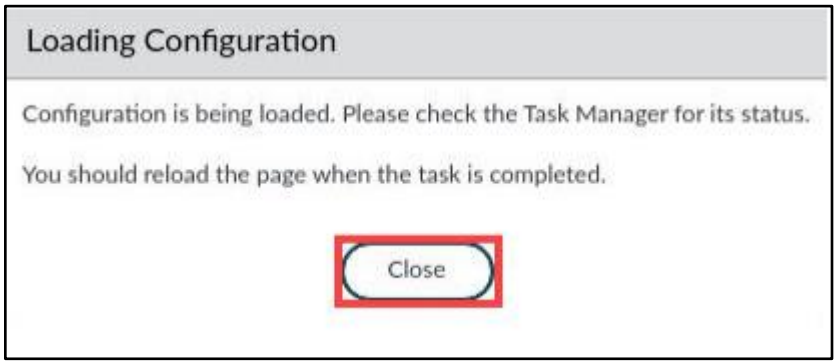
6.1.8. In the Load Named Configuration window, select ***base.xml*** from the Name dropdown box and click OK.



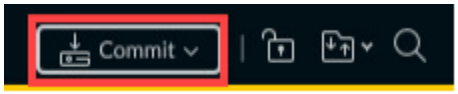
Note: It is important to load the base configuration file first to ensure that the Firewall

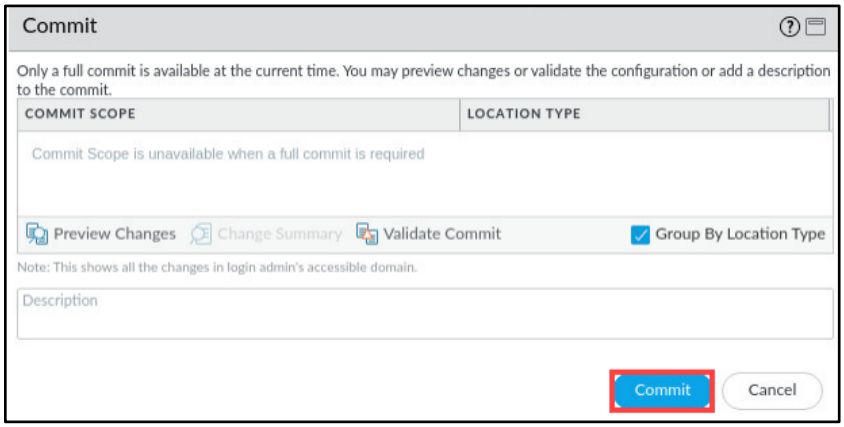
can connect to updates.paloaltonetworks.com

6.1.9. In the Loading Configuration window, a message will show Configuration is being loaded. Please check the Task Manager for its status. You should reload the page when the task is completed. Click *Close* to continue.

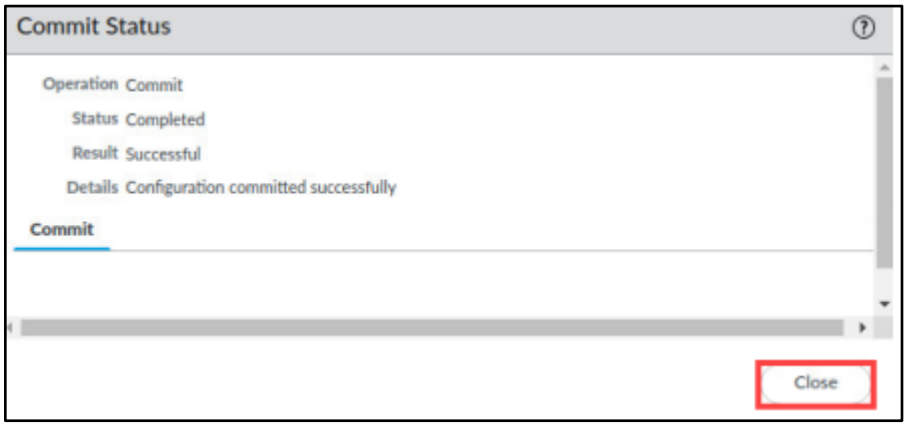


6.1.10. Click the *Commit* link located at the top-right of the web interface.

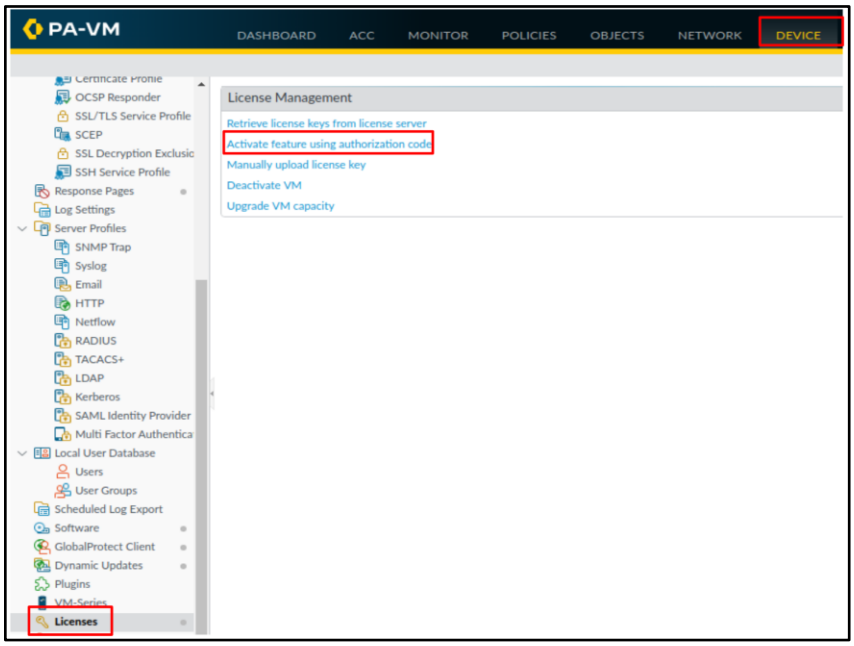




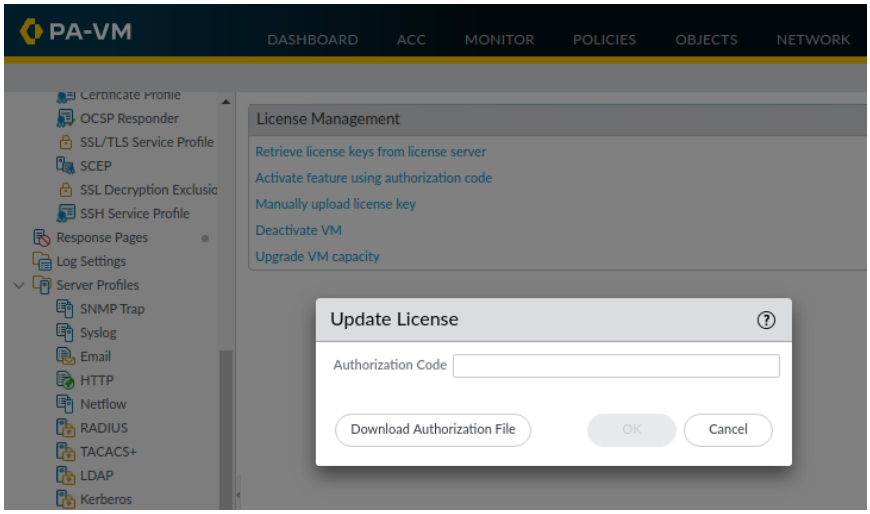
6.1.11. When the Commit operation completes, click *Close* to continue.



6.1.12. Navigate to *Device > Licenses* under "*License Management*", click "*Activate features using authorization code*".

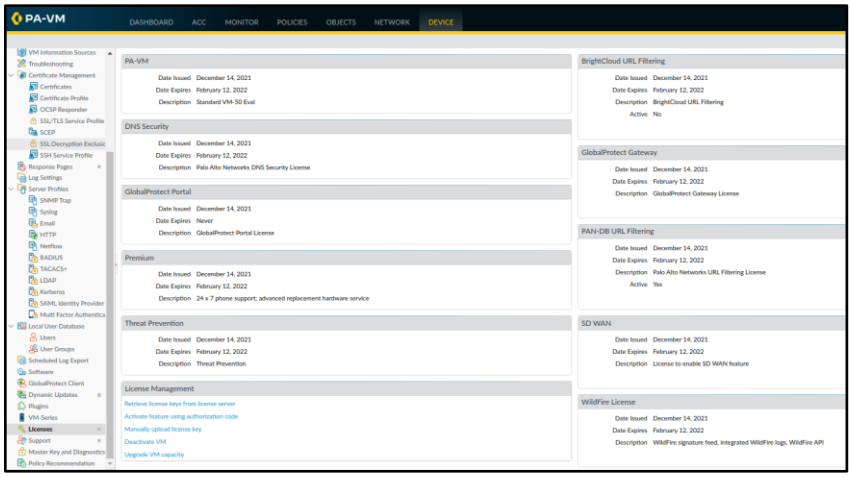


6.1.13. Enter the *Authorization code* provided to you by your academy representative, click *OK* and click *OK* after receiving warning.

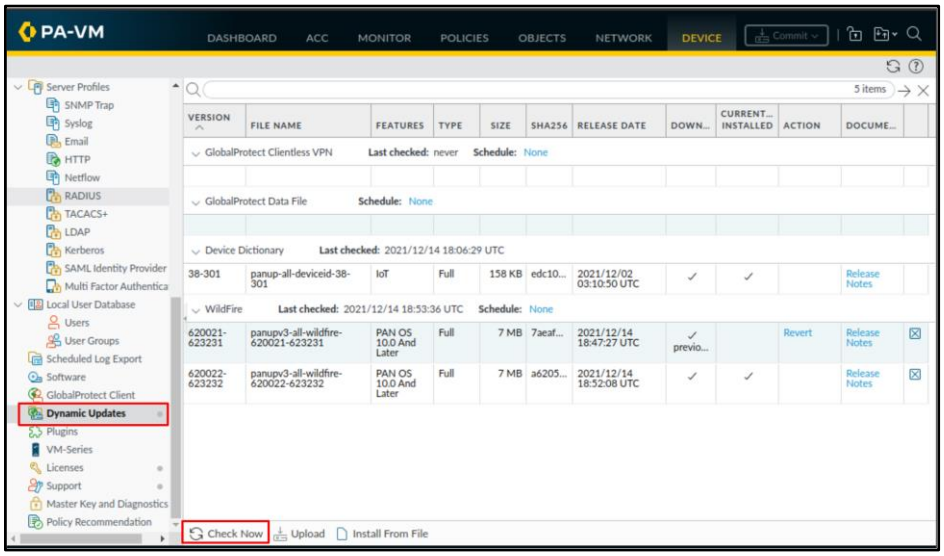


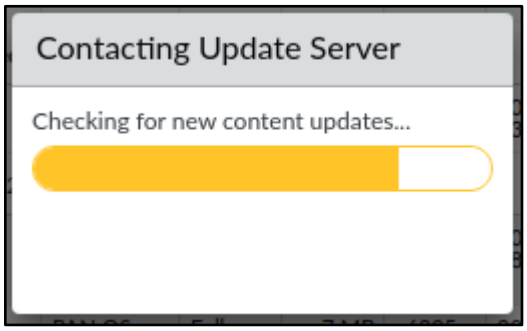
Note: Your firewall will now reboot to load your licenses. Please allow a minimum of 5 minutes or even longer for the firewall to come back online. This can take a little while!

6.1.14. Log back into the firewall and see licenses populated like the image below.

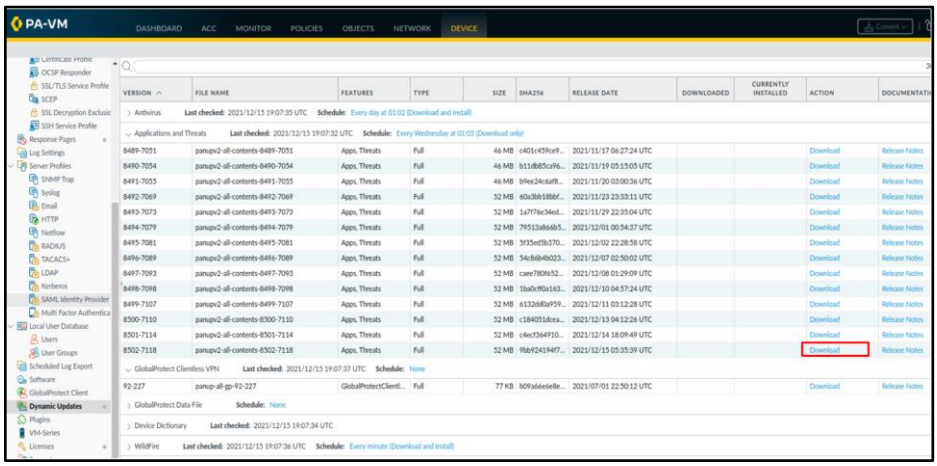


6.1.15. Navigate to *Device Tab > Dynamic Updates* and click *Check Now* on the lower left-hand side menu.

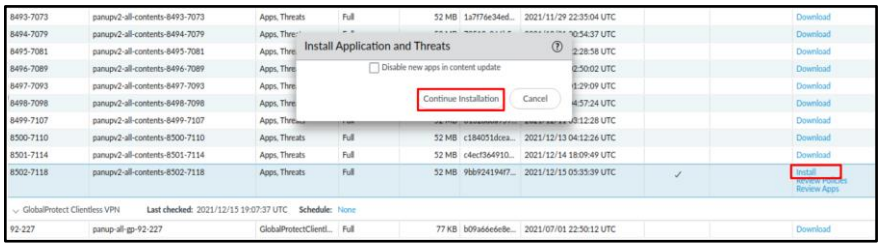




6.1.16. Once the updates are displayed. *Download* the latest Applications and Threats, the latest one is usually at the bottom of the list.



6.1.17. Select *Install* and choose to *Continue installation*.



6.1.18. Repeat the previous Applications and Threats steps to install Antivirus Updates.

Once this is complete your Lab Pod is now fully set up and ready for you to get hands-on experience to reinforce the knowledge you have gained from your instructor.

Have Fun!