



# ACADEMY

## Palo Alto Networks VMware Workstation 9.0 Academy Labs

Document Version: 2019-07-04



## Table of Contents:

Overview: .....	3
Downloads, Licensing and Resources:.....	4
Style Reference Table:.....	5
Lab Scenario:.....	6
Configuration Diagram with Usernames and Passwords .....	7
Lab Solution: .....	9
Windows VMware Workstation Setup Instructions for Palo Alto Networks 9.0 Pod.....	9
Import and Configure Firewall on VMware Workstation .....	16
Import and Configure Virtual Router on VMware Workstation.....	19
Import and Configure DMZ Server on VMware Workstation .....	23
Configure Windows 2016 Client to work on VMware Workstation.....	25
License Firewall on VMware Workstation .....	57

## Overview:

The purpose of this guide is to provide setup instructions to deploy the 9.0.1 virtual firewall appliance lab pod on VMware Workstation. The 9.0.1 VMware Workstation firewall appliance lab pod is almost identical to the 8.0 VMware Workstation firewall appliance lab pod.

The 9.0.1 lab pod consists of 4 virtual machines: Centos Linux virtual router, Windows Server 2016 client, Centos DMZ and a 9.0.1 VM-50 virtual firewall appliance. We are providing ova's for you to download for all the virtual machines except for the Windows Server 2016 client.

We are no longer providing the Windows/Server client ova for the 9.0.1 VMware Workstation lab pod as we did for the 8.0 VMware Workstation lab pod. Instead, academies will either have to configure a Windows Server 2016 Client using a Microsoft base image and the setup instructions in this guide or continue to use 8.0 Windows Server 2012 client in their new 9.0.1 VMware Workstation lab pod if they have already downloaded/used the Windows Server 2012 client.

In summary, academies have the following VMware Workstation use options for supporting all 8.0 and 9.0 CIC and CPC Moodle courses:

1. If an academy has already deployed and is using the 8.0 VMware workstation lab pod, they may continue to use this pod for the above courses.
2. If an academy is new to the program or has not previously downloaded and used the ovbs in the 8.0 VMware Workstation lab pod then the academy will have to follow this guide and to deploy and configure a 9.0.1 VMware lab pod pod.
3. If an academy has been using the 8.0 VMware Workstation lab pod and wants to upgrade to the 9.0.1 lab, the academy may continue to use the Windows Server 2012 lab along with the new 9.0 virtual machines instead of following the instructions in this guide to configure and deploy a new Windows Server 2016 client.

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

All steps in this document were created and verified using:

**Product:** VMware Workstation 15 Pro

**Version:** 15.1.0 build-13591040

**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.

## Downloads, Licensing and Resources:

You will need to provide your own licensing for both VMware workstation and Server 2012 / 2016 operations systems.

The following links will direct you to VMWare and Microsoft.

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://labs.vmware.com/academic/licensing-overview>
- <https://vmapss.onthehub.com/WebStore/Welcome.aspx>
- <https://docs.vmware.com/en/VMware-Workstation-Pro/index.html>
- <https://www.vmware.com/products/workstation-pro.html>
- [https://my.vmware.com/web/vmware/info/slug/desktop\\_end\\_user\\_computing/vmware\\_workstation\\_pro/15\\_0](https://my.vmware.com/web/vmware/info/slug/desktop_end_user_computing/vmware_workstation_pro/15_0)
- <https://www.vmware.com/products/workstation-pro/workstation-pro-evaluation.html>
- <https://docs.vmware.com/en/VMware-Workstation-Pro/15/rn/VMware-Workstation-151-Pro-Release-Notes.html>
- [https://www.microsoft.com/en-us/education/itdm/setup-management/default.aspx?&OCID=AID2000043\\_SEM\\_7OfoGTMi&utm\\_source=google&gclid=EAIalQobChMI8Ovxzd\\_f4wIVB6tBh3OrA01EAAYASAAEgJpfPD\\_BwE](https://www.microsoft.com/en-us/education/itdm/setup-management/default.aspx?&OCID=AID2000043_SEM_7OfoGTMi&utm_source=google&gclid=EAIalQobChMI8Ovxzd_f4wIVB6tBh3OrA01EAAYASAAEgJpfPD_BwE)

## Style Reference Table:

Element	Style	Example
Keystrokes	<b>Bold + Capitalize</b> first letter of keystroke	Press <b>Ctrl+Alt+Del.</b> Press <b>1.</b> Press <b>Enter.</b>
Anything you type	<b>Bold</b>	Enter IP <b>192.168.50.10</b>
Icons and LEDS	<i>Italics</i>	Press <i>Apply</i> or <i>OK</i> .
Anything you click with a mouse	<i>Italics and Capitalize</i> names as they appear on screen	Launch <i>Putty</i> connection to your firewall

**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 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.

**Note:** Once this lab is complete it will support the following Cybersecurity Academy Moodle Courses when doing the labs through VMware workstation: Cybersecurity Infrastructure Configuration course, Cybersecurity Prevention and Countermeasures course, Firewall Essentials Configuration and Management course and the Optimizing Firewall Threat Prevention course.

In this lab, you will:

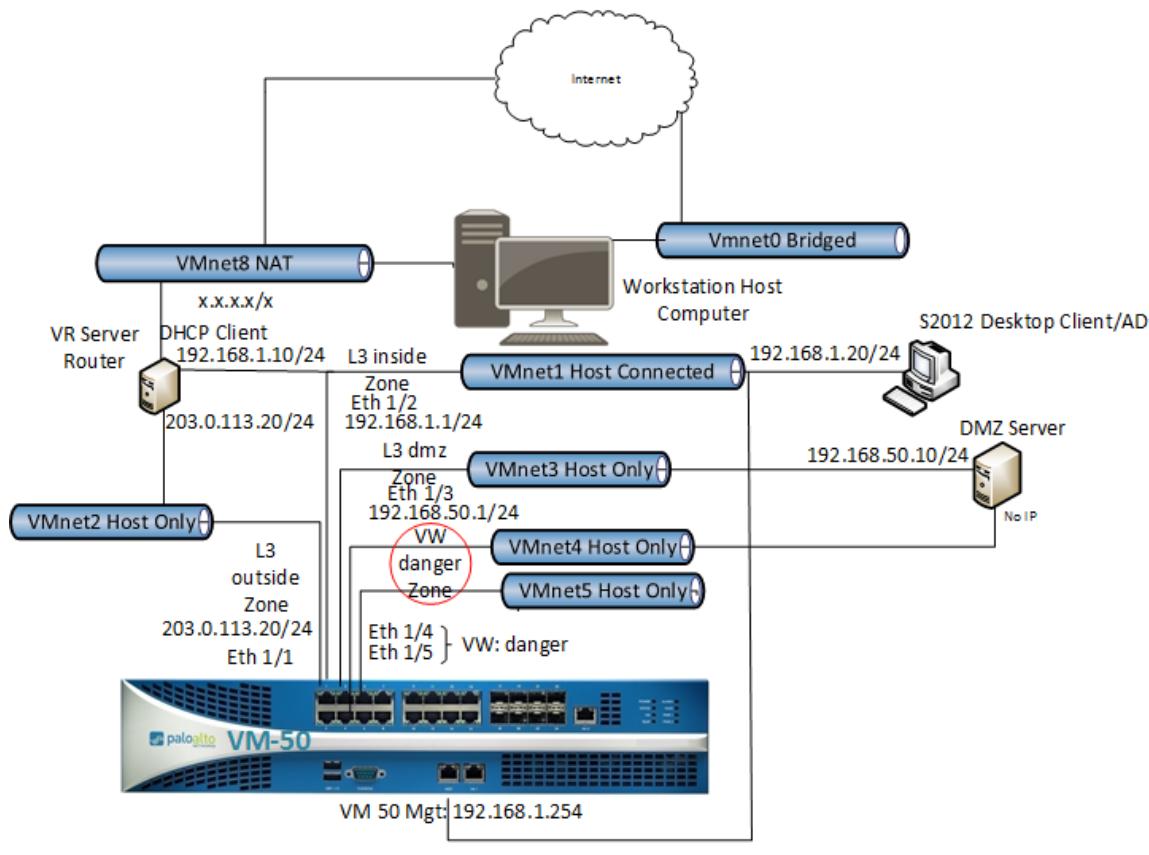
1. Configure your host computer's VMware Workstation VMnets for your VM-50 lab pod.
2. Download and import the academy VM-50 workstation appliance Firewall ova that is pre-configured to operate on the Workstation VMnets.
3. Import the workstation-DMZ ova into your host computer's VMware Workstation application and assign the client's network adapter to the correct VMnet.
4. Import the workstation-VR ova into your host computer's VMware Workstation application and assign the client's network adapters to the correct VMnets.
5. Configure your Windows Client/Server 2016 virtual machine.
6. License your VM-50 workstation appliance with provided AUTH code, check to insure your firewall correctly installs the licenses on your appliance and perform dynamic updates.

**Note:** When doing labs on VMware workstation lab pods it is important to load the correct named configuration snapshot. This will be outlined in each of the lab documents for the respective course that you will complete.

## Configuration Diagram with Usernames and Passwords

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

### Firewall Essentials 9.0.1 Academy VMware Workstation Lab Diagram



Virtual Machine	Username	Password
VM-50 Academy Appliance	admin	admin
Server 2012	lab-user	Pal0Alt0
Centos AAC DMZ	root	Pal0Alt0
Centos Virtual Router	root	Pal0Alt0

## Lab Solution:

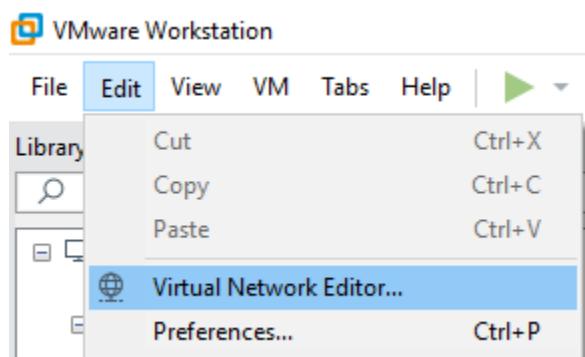
### Windows VMware Workstation Setup Instructions for Palo Alto Networks 9.0 Pod

- 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.

- 1.1 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.

- 1.2 Your lab environment will need 7 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 its 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

Virtual Network Editor					
Name	Type	External Connection	Host Connection	DHCP	Subnet Address
VMnet0	Bridged	Auto-bridging	-	-	-
VMnet1	Host-only	-	Connected	Enabled	192.168.182.0
VMnet8	NAT	NAT	Connected	Enabled	192.168.188.0

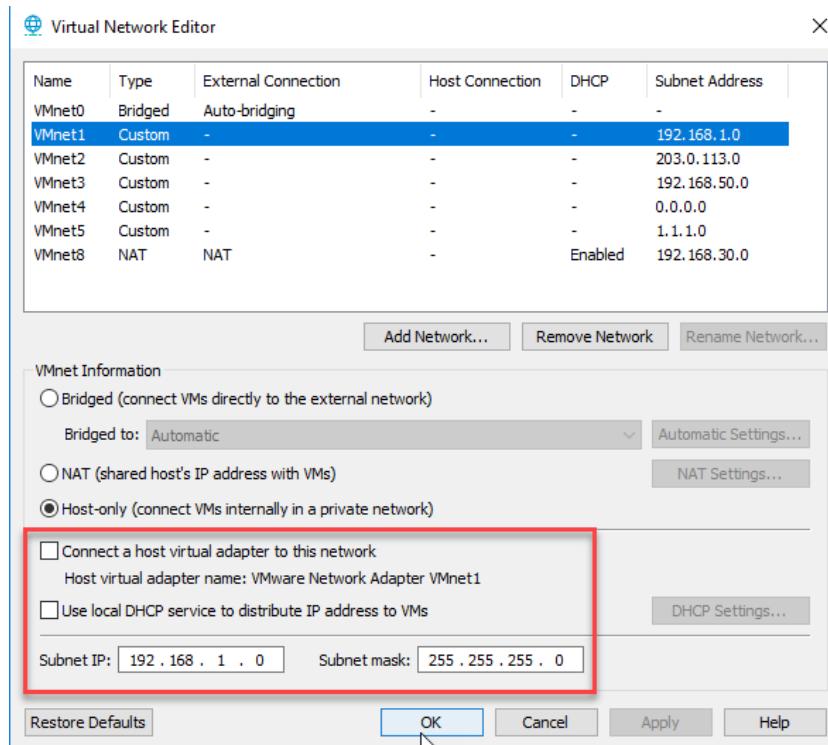
Possibly you may also see: VMNet1 – Type: Host-only.

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

- 1.3 In the Virtual Network Editor dialog box, select to highlight “VMnet1” and under “VMnet Information” do the following:

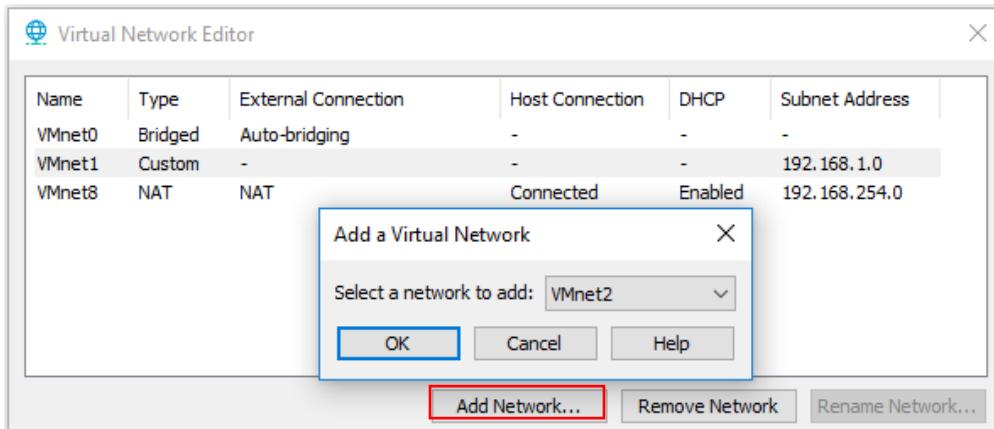
- 1.3.1 Select the radial button, “*Host-only*” (connect VMs internally in a private network).

- 1.3.2 Set the “Subnet IP” to **192.168.1.0** and the “Subnet mask” to **255.255.255.0**



### 1.3.3 Click *Apply*.

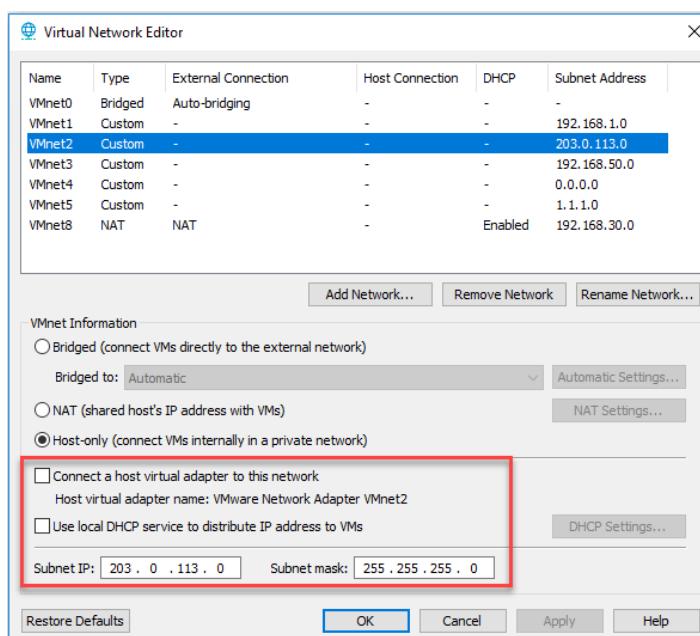
- 1.4 In the “Virtual Network Editor” dialog box, select “Add Network” and then select *OK*.



- 1.4.1 In the “Virtual Network Editor” dialog box for VMnet2, *unchecked* the boxes next to “Connect a host virtual adapter to this network” and *unchecked* “Use local DHCP service to distribute IP addresses to VMs”.

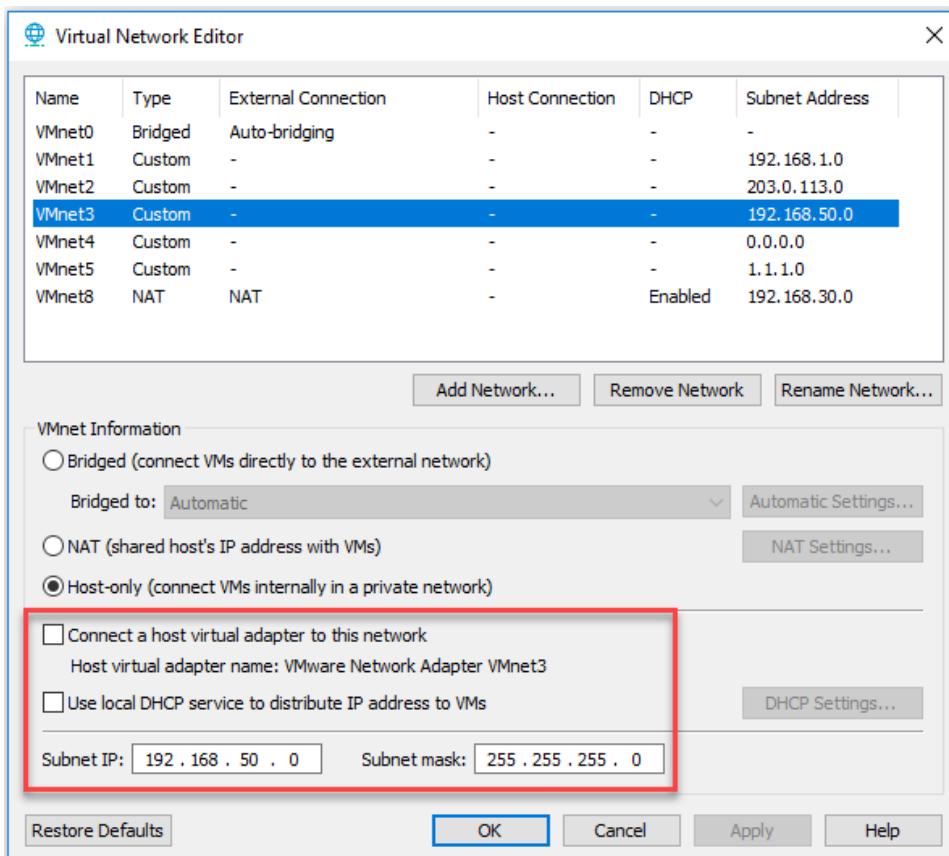
For Subnet IP enter **203.0.113.0** and for Subnet Mask enter **255.255.255.0**

### 1.4.2 Click *Apply*.



**1.5** In the “Virtual Network Editor” dialog box, select “Add Network”.

- 1.5.1** In the “Virtual Network Editor” dialog box for VMnet3, *unchecked* the boxes next to “Connect a host virtual adapter to this network” and *unchecked* “Use local DHCP service to distribute IP addresses to VMs”.



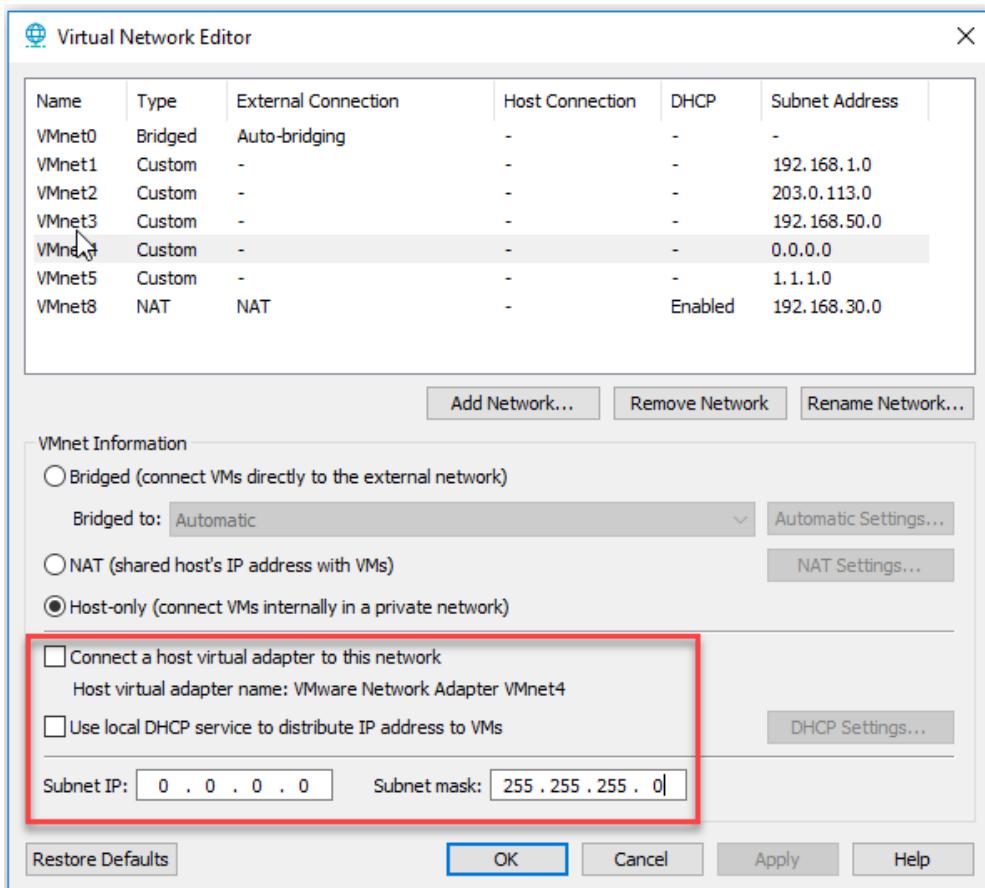
- 1.5.2** For Subnet IP enter **192.168.50.0** and for Subnet Mask enter **255.255.255.0**

- 1.5.3** 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 VMnet4, *unchecked* the boxes next to “Connect a host virtual adapter to this network” and *unchecked* “Use local DHCP service to distribute IP addresses to VMs”.

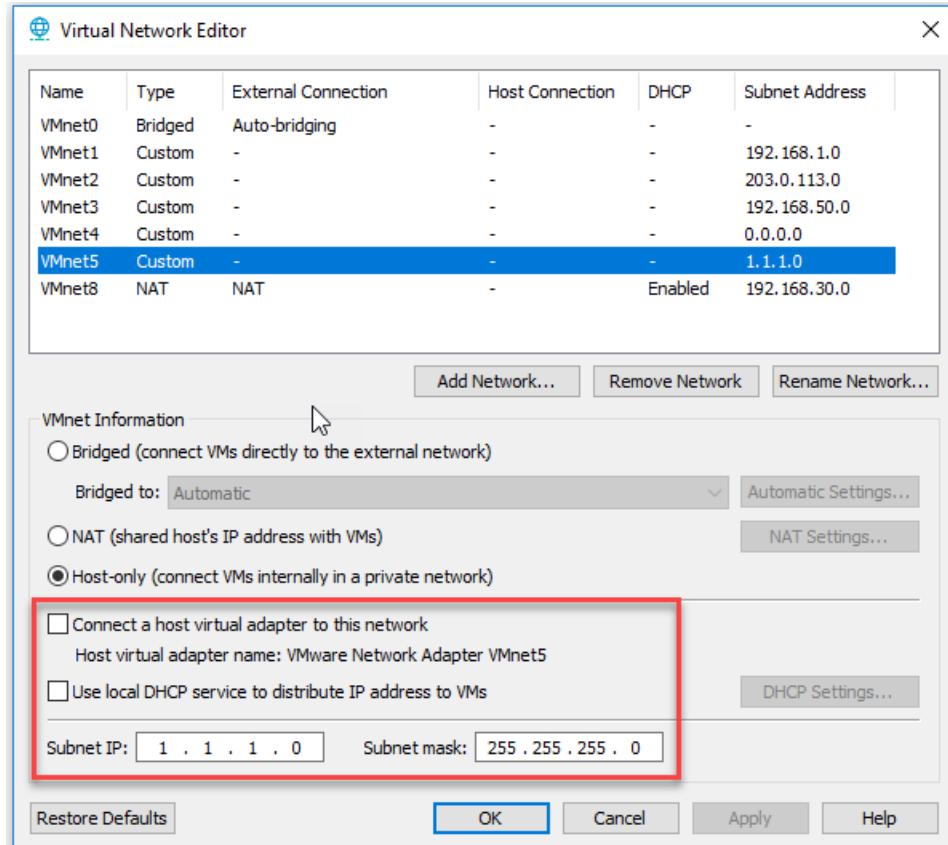
For Subnet IP enter **0.0.0.0** and for Subnet Mask enter **255.255.255.0** and



### 1.6.2 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 VMnet5, *unchecked* the boxes next to “Connect a host virtual adapter to this network” and *unchecked* “Use local DHCP service to distribute IP addresses to VMs”.
- 1.7.2 For Subnet IP enter **1.1.1.0** and for Subnet Mask enter **255.255.255.0**.



### 1.7.3 Click *Apply*.

1.8 In the “Virtual Network Editor” dialog box, select VMnet 8.

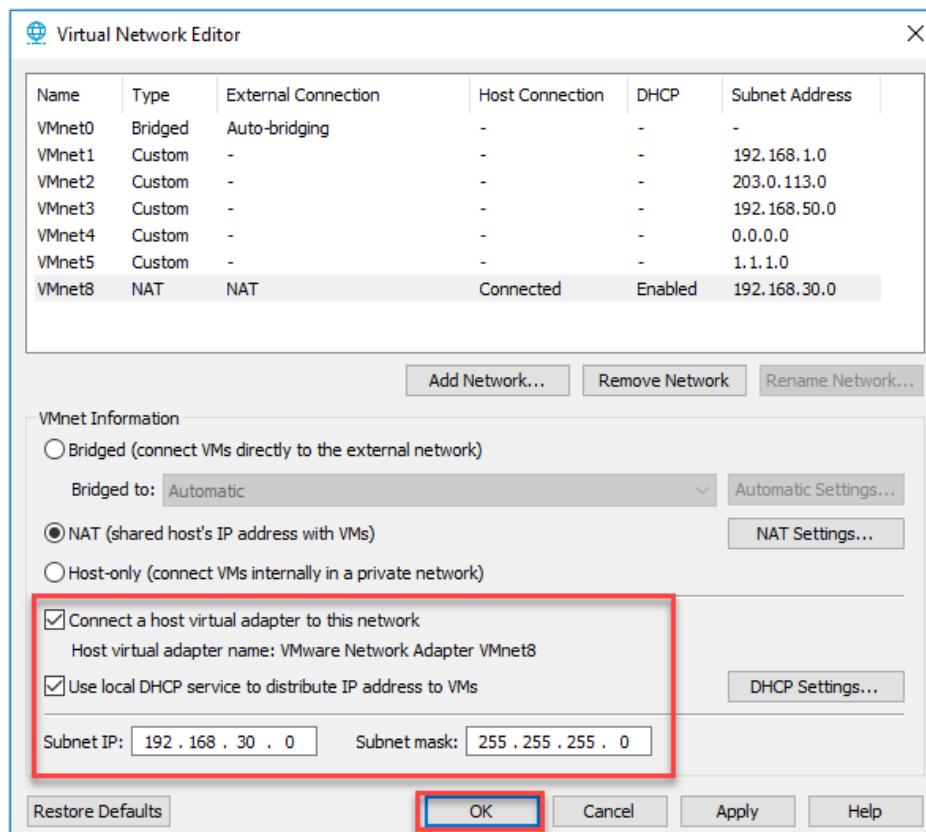
#### 1.8.1 Select the radial button *NAT (Share host's IP address with VMs)*

**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.

Also, if you change your NAT settings you may need to reboot your laptop for these settings to be applied.

- 1.8.2 Ensure the box next to “Connect a host virtual adapter to this network” is checked
- 1.8.3 Ensure the box next to “Use local DHCP service to distribute IP addresses to VMs” is checked.

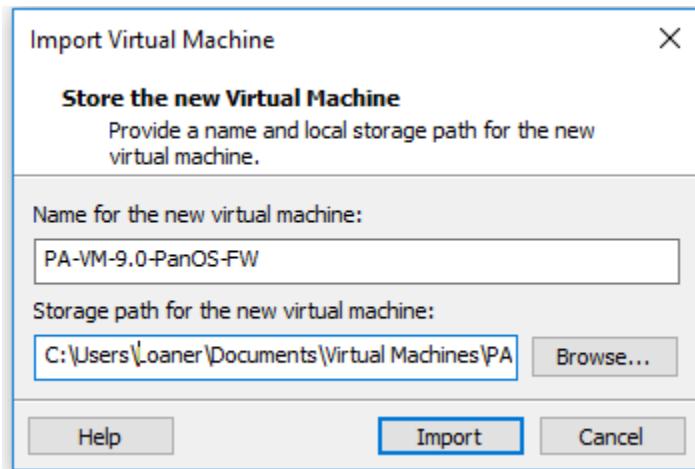


- 1.8.4 Click Apply.
- 1.8.5 Click OK.

## 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 insure appliance's network adapters are assigned to the correct VMnets. The VMware Workstation ova/lab config share drive URL is posted in the following Cybersecurity Academy Moodle Courses: Configuration Infrastructure course, Cybersecurity Prevention and Countermeasures course, Firewall Essentials Configuration and Management course and the Optimizing Firewall Threat Prevention course.

- 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-9.0-PanOS-FW-OVA and select. Click *Open*.



- 2.1.3 In the “Import Virtual Machine” dialog box, choose the location of your PA-VM-9.0-PanOS-FW virtual machine.
- 2.1.4 Click *Import*.
- 2.1.5 In VMware workstation PA-VM-9.0-PanOS-FW, select edit *Virtual Machine Settings*

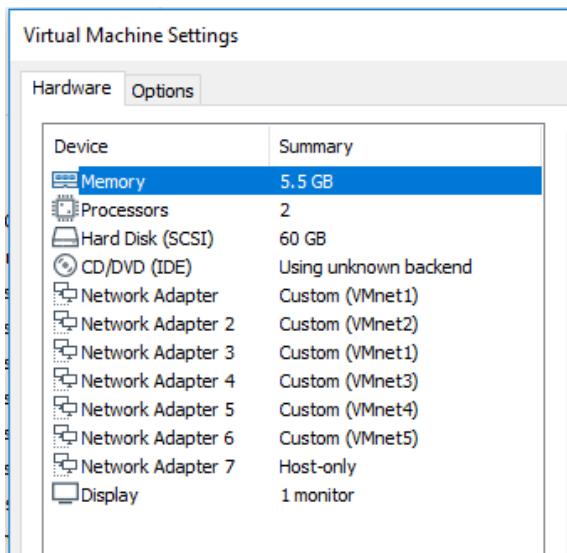
▶ Power on this virtual machine  
Edit virtual machine settings  
Upgrade this virtual machine

▼ Devices

Memory	5.5 GB
Processors	2
Hard Disk (SCSI)	60 GB
CD/DVD (IDE)	Using unknown ...
Network Adapter	Bridged (A  m...)
Network Adapter 2	Bridged (Autom...)
Network Adapter 3	Bridged (Autom...)
Network Adapter 4	Bridged (Autom...)
Network Adapter 5	Bridged (Autom...)
Network Adapter 6	Bridged (Autom...)
Network Adapter 7	Host-only
Display	1 monitor

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”.



**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.

- 2.1.6 Click **OK** to close the dialog box.
- 2.1.7 Do not power on the firewall yet.

## Import and Configure Virtual Router on VMware Workstation

- 3** Download and Import the PA-VM-9.0-PanOS-VR OVA into your host computer's VMware Workstation application and assign the client's network adapter to the correct VMnet2. The VMware Workstation ova/lab config share drive URL is posted in the following Cybersecurity Academy Moodle Courses: Configuration Infrastructure course, Cybersecurity Prevention and Countermeasures course, Firewall Essentials Configuration and Management course and the Optimizing Firewall Threat Prevention course.

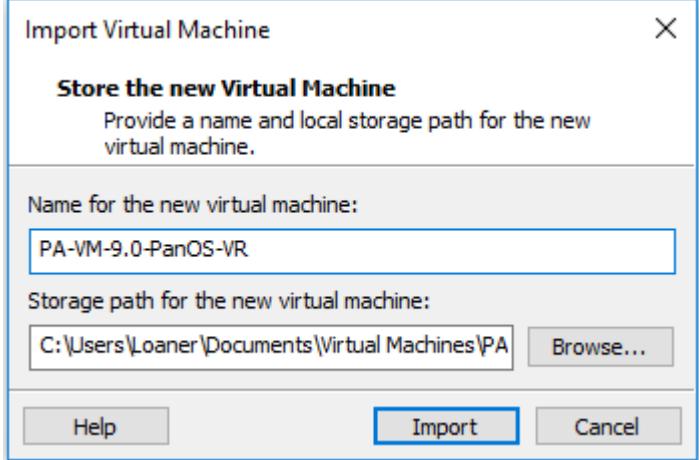
You will follow the same basic steps you did when importing your PA-VM-9.0-PanOS-FW.

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:

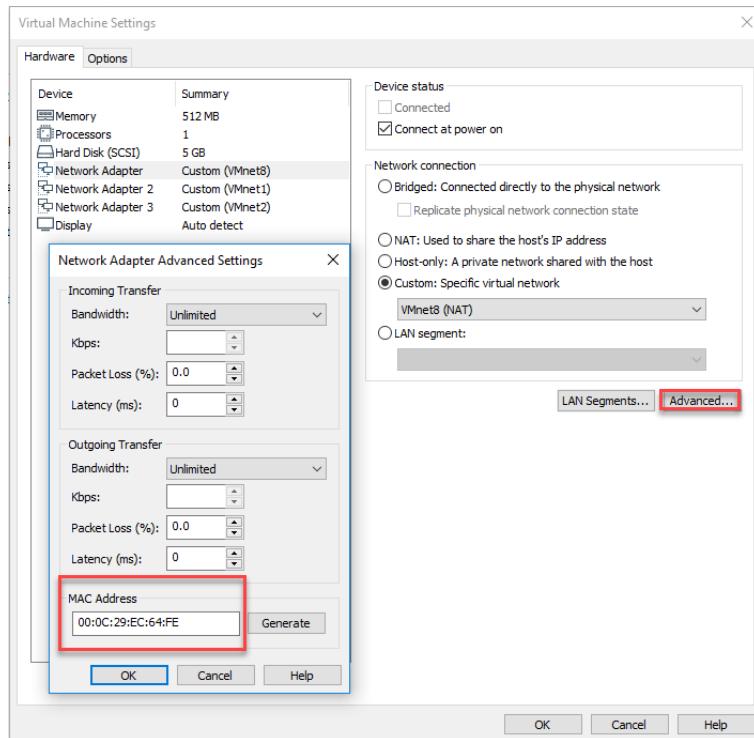
- 1.** Connect to your PANOS 9.0.1 VM-50 firewall appliance's management interface WebUI using your host computer's Web browser and the destination https URL composed of the external address of your virtual router's *ens160* interface;
- 2.** Connect to your PANOS 9.0.1 VM-50 firewall appliance's management interface via ssh from PuTTY on your host computer using the destination IP address assigned to your virtual router's *ens160* interface and
- 3.** Connect to your pod's Server/Client 2016 via RDP 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
DNAT       tcp  --  anywhere             anywhere
DNAT       tcp  --  anywhere             anywhere
                                         tcp dpt:ssh to:192.168.1.254
                                         tcp dpt:https to:192.168.1.254
                                         tcp dpt:ms-wbt-server to:192.168.1.20
```

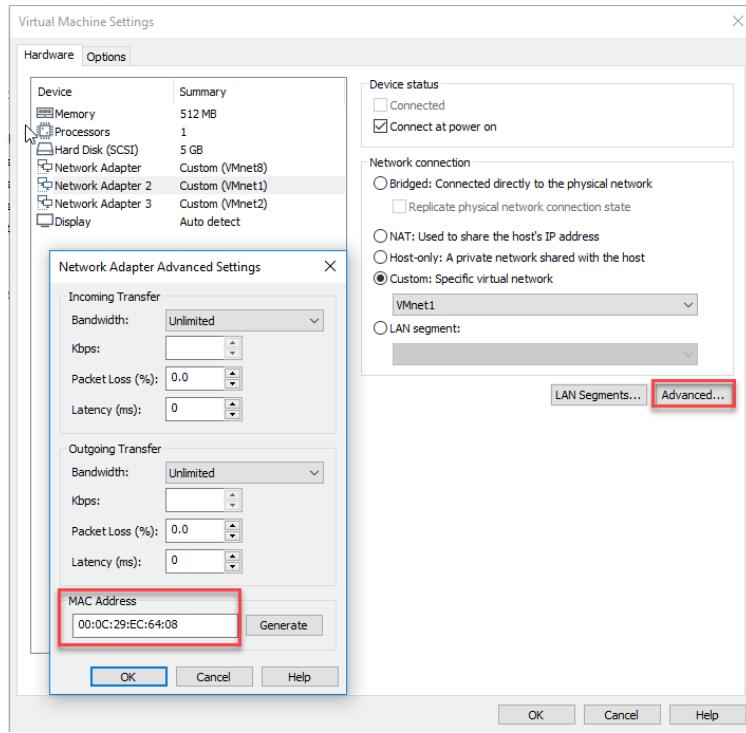
- 3.1.1** In the VMware Workstation application click *File* and select *Open* in the drop-down menu.
- 3.1.2** In the Open dialog box, browse to the location of the PA-VM-9.0-PanOS-VR ova and select to open it.
- 3.1.3** In the "Import Virtual Machine" dialog box, chose the location of your virtual machine and click *Import*.



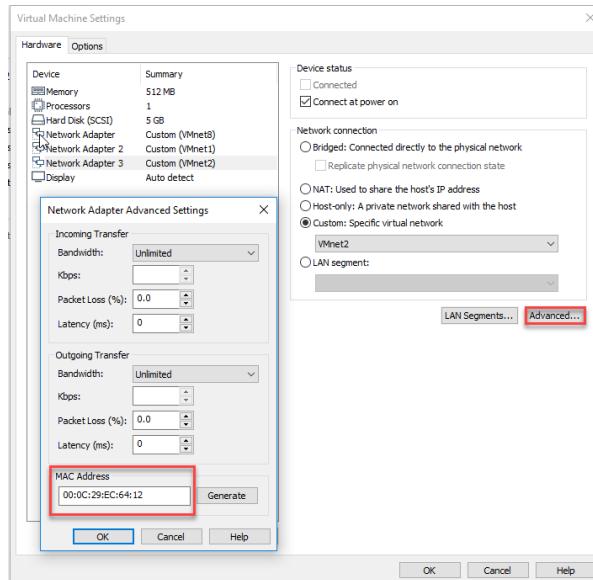
- 3.1.4 In Workstation on your PA-VM-9.0-PanOS-VR tab, select *edit virtual network machine settings* and assign the Network Adapter 1 to **NAT ("VMnet8")**
- 3.1.5 Select the *Advanced* option. Once in the Advanced menu please manually enter the following MAC Address: "**00:0C:29:EC:64:FE**" and select **OK**.



- 3.1.6 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: "**00:0C:29:EC:64:08**" and select **OK**.



**3.1.7 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: “00:0C:29:EC:64:12” and select OK 2 times.**



- 3.1.8** Power on your PA-VM-9.0-PanOS-VR VM. You will need the VM's built in router to connect your VM-50 management interface to the Internet for licensing.
- 3.1.9** Log on to the VR using the username **root** and password **PaloAlt0**. 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 3.10.0-693.2.2.el7.x86_64 on an x86_64

pod-vr login: root
Password:
Last login: Tue May 28 17:30:53 on tty1
[root@pod-vr ~]# ifconfig
ens160: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 192.168.30.128 netmask 255.255.255.0 broadcast 192.168.30.255
              ether 00:0c:29:ec:64:fe txqueuelen 1000 (Ethernet)
              RX packets 8 bytes 1048 (1.0 KiB)
              RX errors 0 dropped 0 overruns 0 frame 0
              TX packets 5 bytes 830 (830.0 B)
              TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
              device interrupt 18 base 0x2000

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 00:0c:29:ec:64:00 txqueuelen 1000 (Ethernet)
              RX packets 0 bytes 0 (0.0 B)
              RX errors 0 dropped 0 overruns 0 frame 0
              TX packets 2 bytes 84 (84.0 B)
              TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
              device interrupt 19 base 0x2000

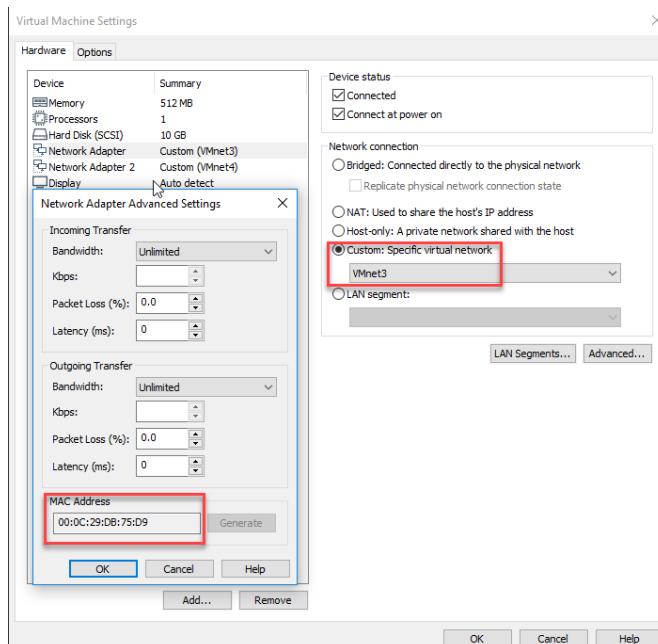
ens224: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 203.0.113.1 netmask 255.255.255.0 broadcast 203.0.113.255
              ether 00:0c:29:ec:64:12 txqueuelen 1000 (Ethernet)
              RX packets 0 bytes 0 (0.0 B)
              RX errors 0 dropped 0 overruns 0 frame 0
              TX packets 2 bytes 84 (84.0 B)
              TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
              device interrupt 16 base 0x2400

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 8 bytes 528 (528.0 B)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 8 bytes 528 (528.0 B)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

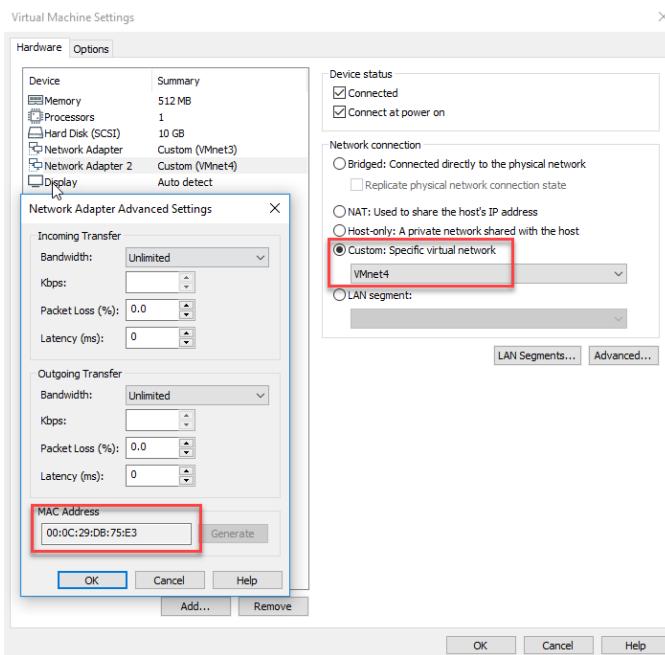
## Import and Configure DMZ Server on VMware Workstation

- 4 Download and import the PA-VM-9.0-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. The VMware Workstation ova/lab config share drive URL is posted in the following Cybersecurity Academy Moodle Courses: Configuration Infrastructure course, Cybersecurity Prevention and Countermeasures course, Firewall Essentials Configuration and Management course and the Optimizing Firewall Threat Prevention course.

- 4.1.1** In Workstation on your PA-VM-9.0-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: “**00:0C:29:DB:75:D9**” and select **OK**.



- 4.1.2** In Workstation on your PA-VM-9.0-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: “**00:0C:29:DB:75:E3**” and select **OK** 2 times.



#### 4.1.3 Power on your PA-VM-9.0-PanOS-DMZ VM.

#### 4.1.4 Log on to the DMZ using the username **root** and password **PaloAlt0**. 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 1820 (1820.0 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)

```

## Configure Windows 2016 Client to work on VMware Workstation

- 5 If you are an existing Academy and have used the PANOS 8.0 Windows Server/Client 2012R2 Virtual Machine: You may use this virtual machine, licensed via your institution, for the PANOS 9.0.1 VMware Workstation lab pod.

If you do not have this virtual machine from the PANOS 8.0 VMware Workstation lab pod, then please follow the directions in the steps below to configure a Server/Client 2016 virtual machine which you will need to license using your institution's Microsoft license.

There are 16 individual configuration settings that need to be performed on your Windows Server / Client in order to function properly, including external authentication, certificate services, installing Wireshark, folder paths and more.

**Note:** The following steps need to be configured in order for the labs to function correctly.

### 5.1.1 Create a New Windows Server/Client 2016 Virtual Machine:

- 5.1.2 Download the Windows Server 2016 ISO image from your Microsoft account and create a new VMware Workstation virtual machine using this ISO image.

For the default “administrator” account use “**PaloAlt0**” as the password and install VMware tools after creating the Server 2016 virtual machine. Temporarily connect your Server 2016 network adapter to *vmnet8*, the VMware Workstation’s NAT’d VMnet.

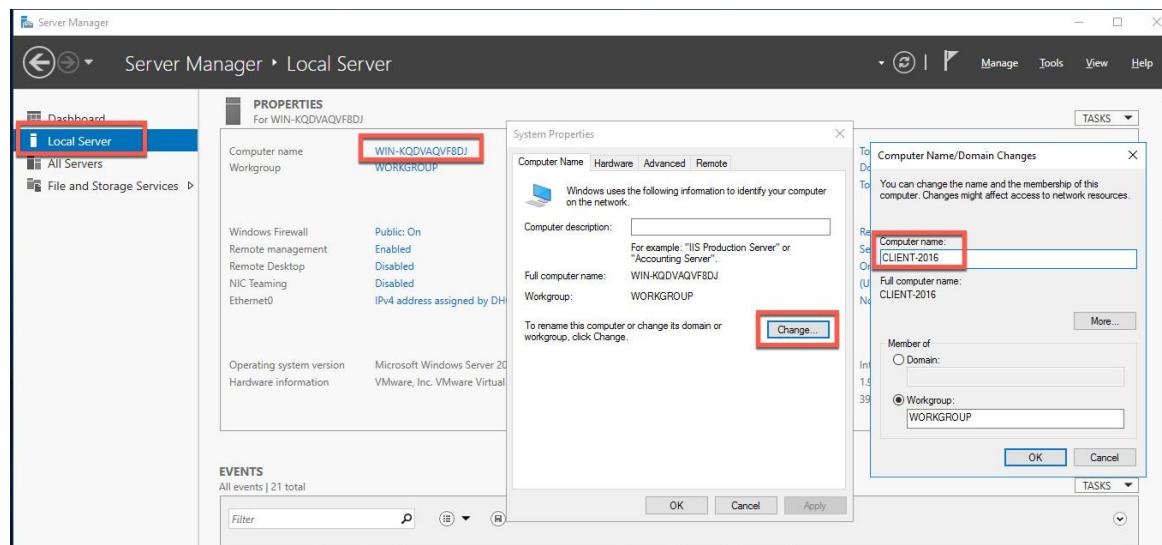
Set the RAM of your Server 2016 to **2024 MB**.

### 5.1.3 Rename Your Server 2016:

Open “*Server Manager*” and on the left pane select “*Local Server*” then under the “*Properties*” window click the default name of your computer. This will open the System Properties dialog box.

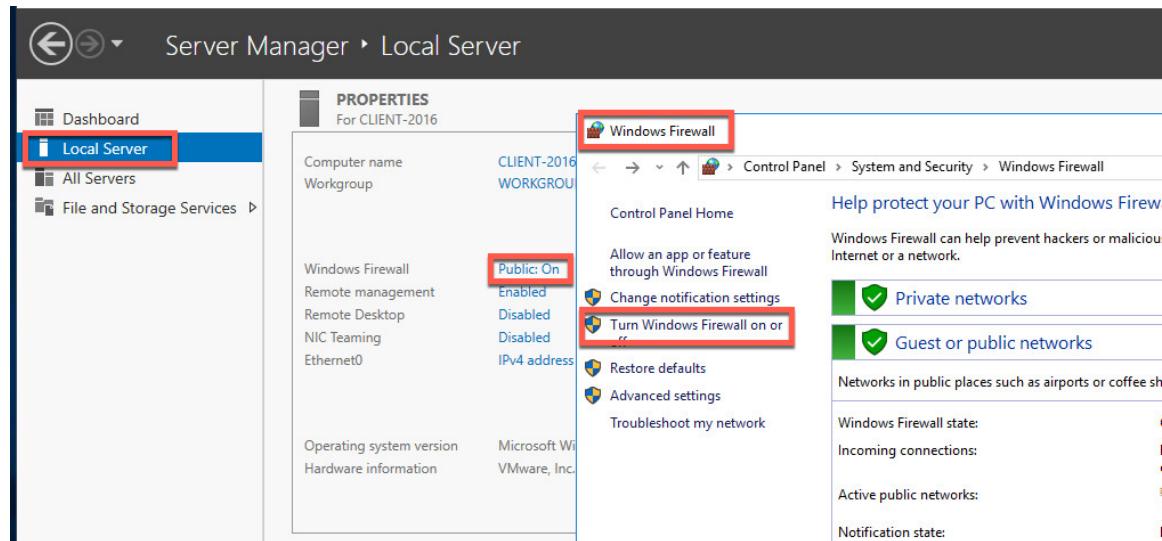
In the “*System Properties*” dialog box click “*Change*”. This will open the “*Computer Name/Domain Changes*” dialog box. In the “*Computer name*” text box, change the default name to “**CLIENT-2016**”.

After changing the name, you will need to *restart* the computer.



#### 5.1.4 Disable Windows Firewall:

On your Server 2016 desktop in Server Manager under “Properties” window click “Public On” after Windows Firewall and in the Windows Firewall dialog box, select “Turn Windows Firewall on or off”. This will bring up the “Customize Settings” dialog box, select to “Turn Off Windows Firewall ...” in *Private network* settings and *Public network* settings.



#### 5.1.5 Promote Server 2016 to a Domain Controller:

Follow the directions at this Web site to upgrade your server to a domain controller: <https://blogs.technet.microsoft.com/canitpro/2017/02/22/step-by-step-setting-up-active-directory-in-windows-server-2016/>.

Don't change the temporary DHCP IP address of your Server 2016 but do change your Server's preferred DNS to **127.0.0.1** as your Primary DNS server and use **1.1.1.1** or your NAT'd, VMnet8 default gateway as your Alternate DNS server.

After installing most of the required lab applications on your Server 2016 domain controller, you will change the IP address from DHCP client to a static **192.16.1.20**. Name your domain forest: "**lab.local**". Use the password "**Pal0Alt0**" as the DRSM password.

#### 5.1.6 Create the following users in Active Directory

lab-user Account and Group:

Log on to your Server 2016 Domain Controller and create a new user account in Active Directory Users and Computers using the following data:

*First name: lab*

*Last name: user*

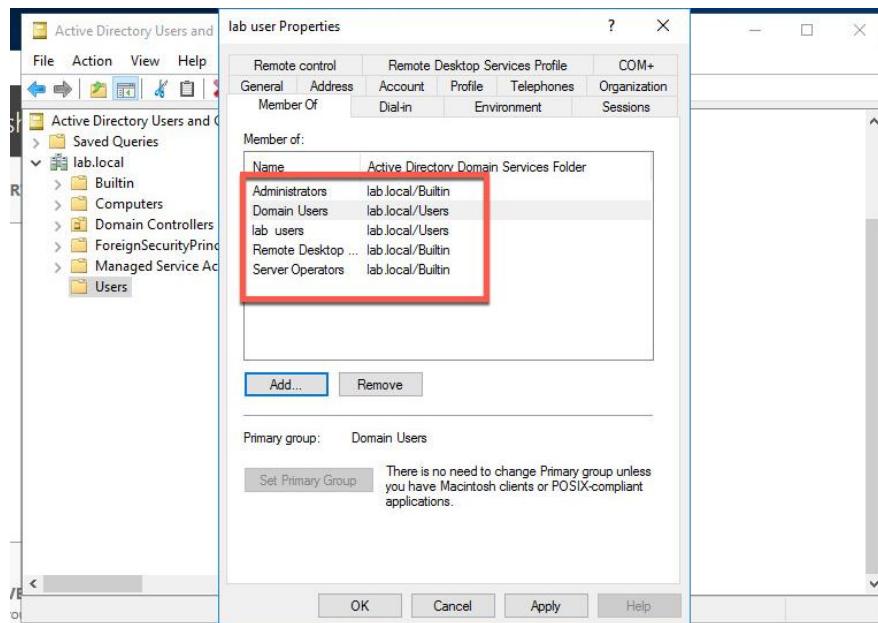
*User logon name: lab-user.*

For password use: "**Pal0Alt0**" and uncheck "User must change password at next logon" and "Password never expires".

Add lab-user to the following groups:

*Remote Desktop; Administrators and Server Operators.*

Create a new global security group named: *lab users* and add *lab-user* as a member.



### 5.1.7 Active Directory Users and Computers using the following data:

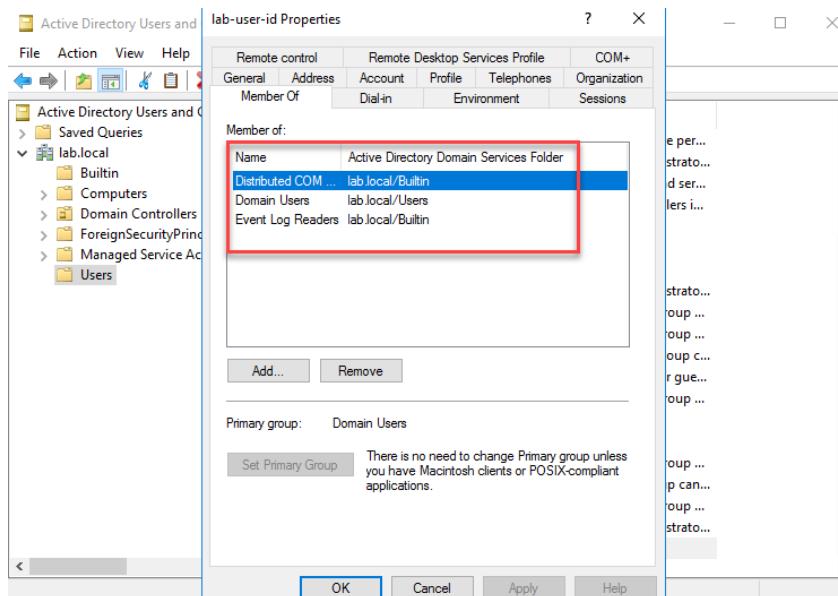
*First name: lab-user-id*

*User logon name: lab-user-id.*

For password use: “**Pal0Alt0**” and *uncheck* “User must change password at next logon” and “Password never expires”

Add lab-user-id to the following groups:

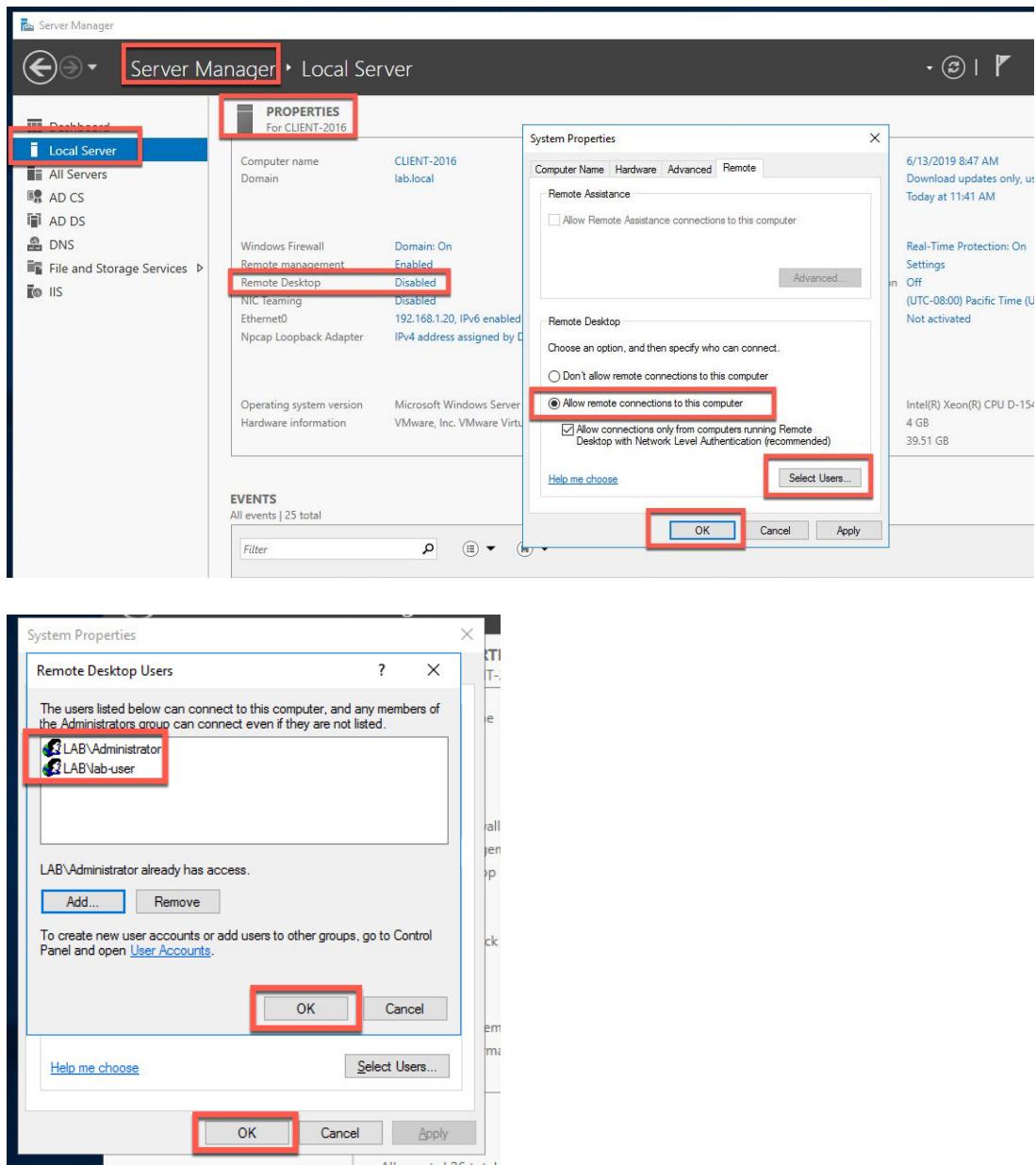
*Domain Users, Distributed COM Users, Event Log Readers.*



### 5.1.8 Enable Remote Desktop on the Client/Server:

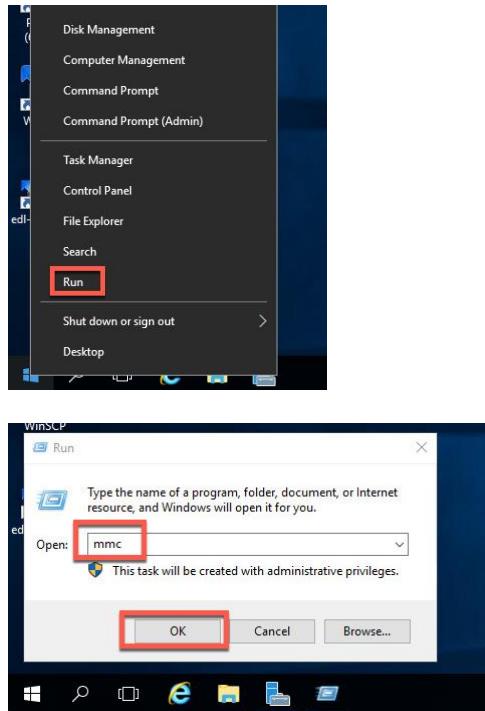
In *Server Manager > Properties Windows* enable *Remote Desktop*. In the *System Properties* dialog box click *Select Users*.

Add the *Administrator* and *lab-user* users.

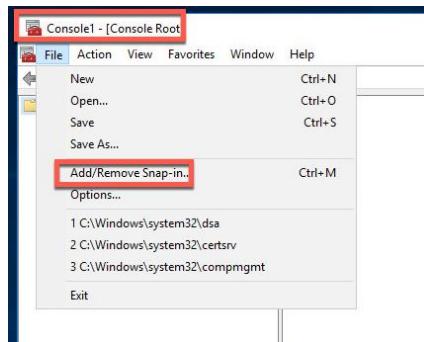


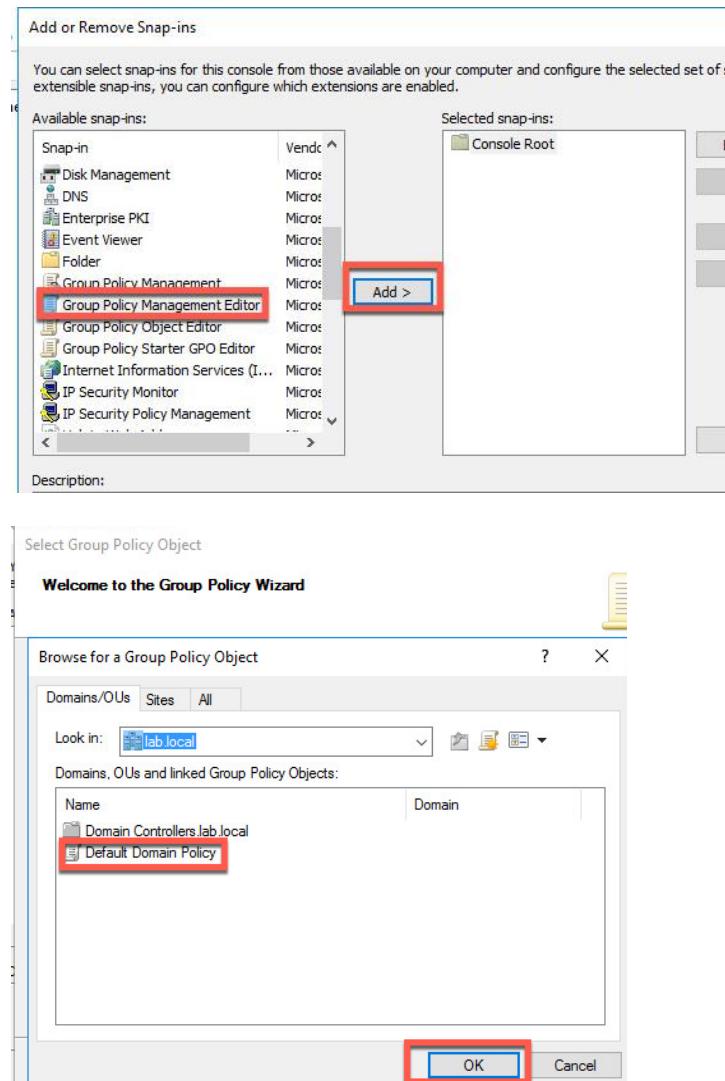
### 5.1.9 Configure default domain password policy with no restrictions and configure the default domain auditing policy.

xv. Right click the Microsoft Windows icon in the lower left of your desktop and select run. In the “Run” dialog box enter mmc and click “OK”.

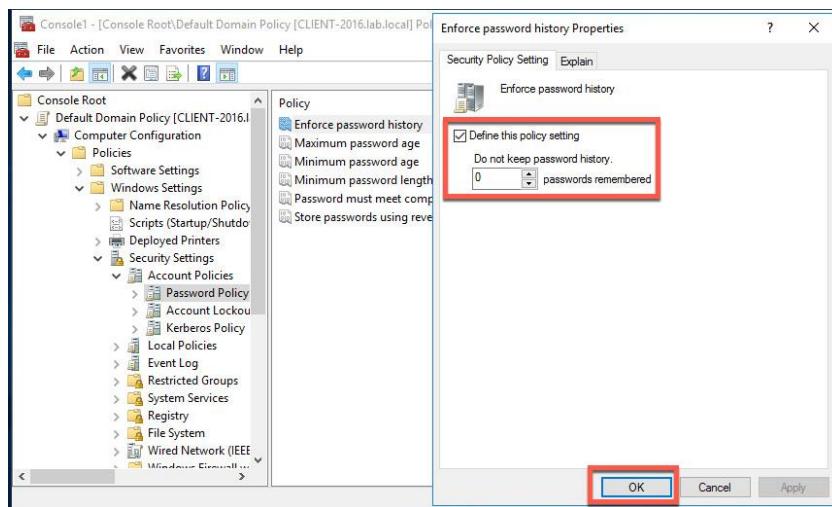
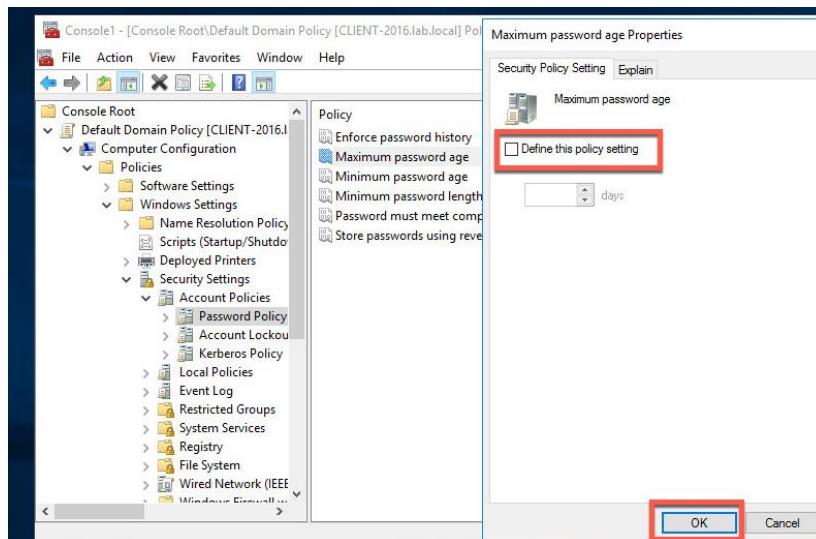
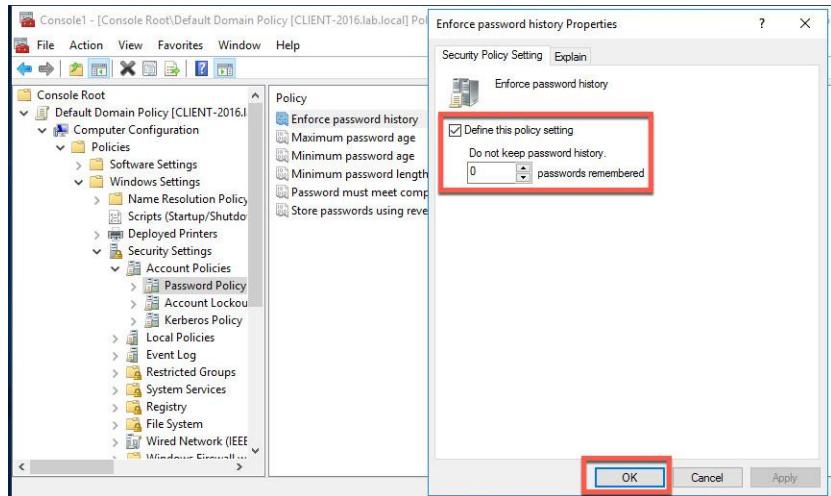


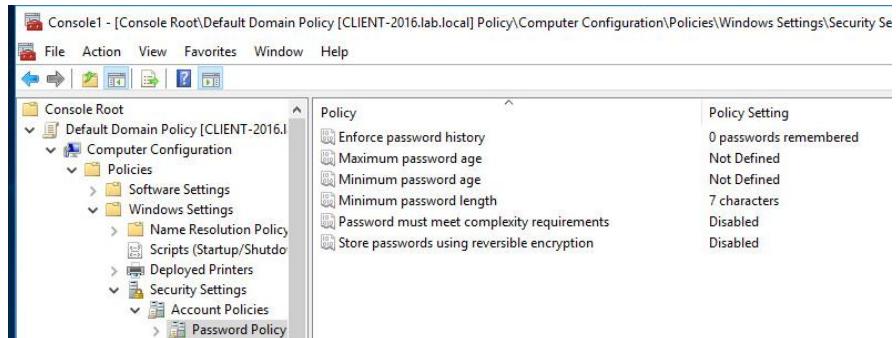
xvi. In the “Console1” dialog box under the “File” tab, click “Add/Remove Snap-in”. In the “Add or Remove Snap-ins” select “Group Policy Management Editor” and in the “Select Group Policy Object” dialog box browse and select “Default Domain Policy” to edit and click OK then Finish then OK to exit out of the “Add or Remove Snap-ins” dialog box.



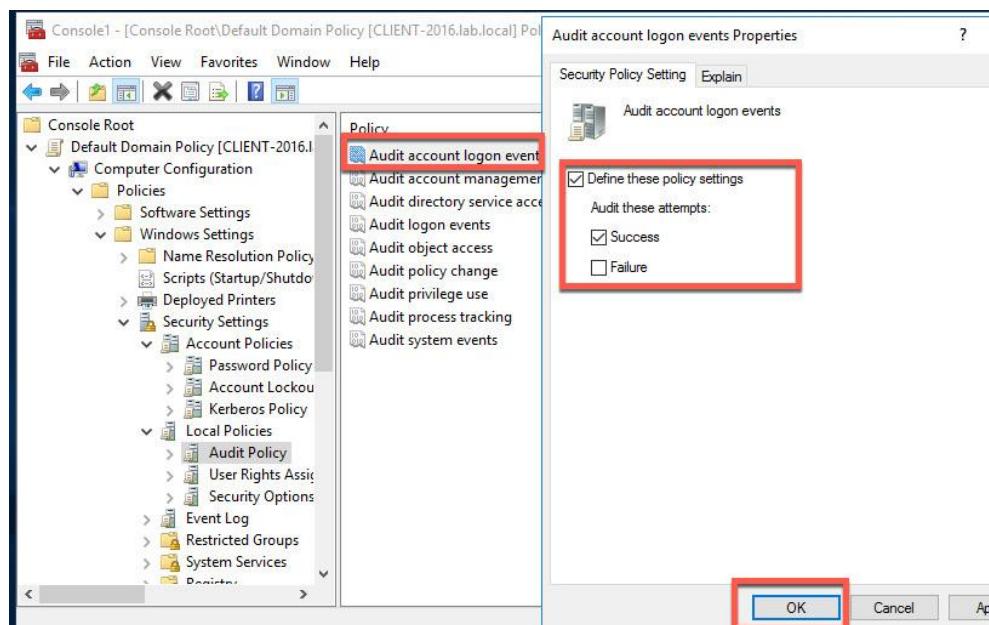


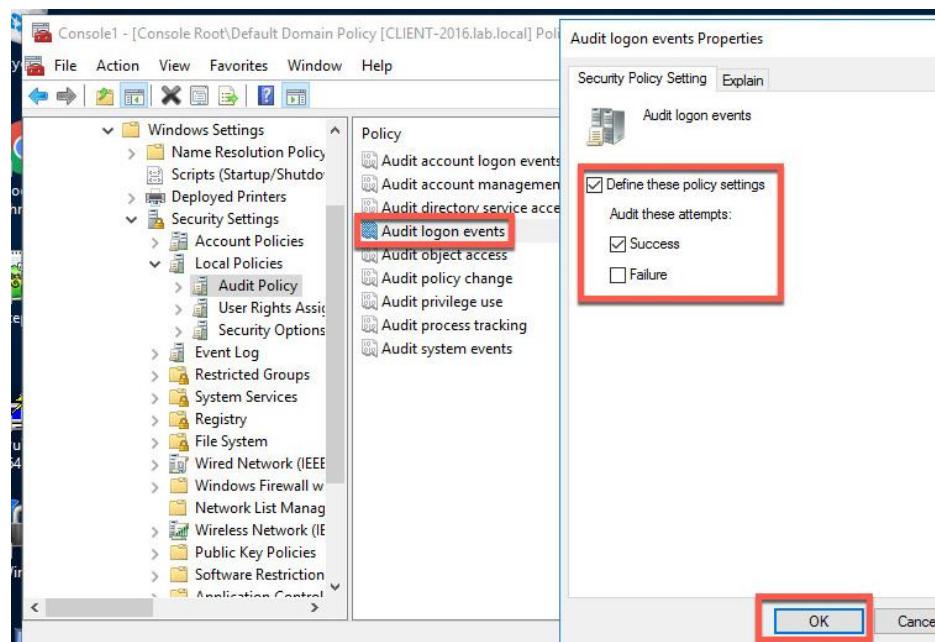
xvii. In the “Console1” mmc dialog box browse to Default Domain Policy>Computer Configuration>Security Settings>Account Policies>Password Policy. Double click Enforce password history and in the “Enforce password history Properties” dialog box, select “0” passwords remembered and click “OK” to close the dialog box. Double click “Maximum password age” and in the dialog box uncheck the “Define this policy setting” box and click “OK” and click “OK” to allow change to “Minimum password age”. Double click “Password must meet complexity requirements” and click disabled in the dialog box.





xviii. In the Console1 GPO editor mmc, browse to Computer Configuration>Policies>Windows Settings>Security Settings>Local Policies>Audit Policy and double click “Audit account logon events”. In the dialog box, select: “Define these policy settings”, Success and click OK to exit the dialog box. Double click “Audit logon events”, select “Define these policy settings”, “Success” and click OK to exit the dialog box.



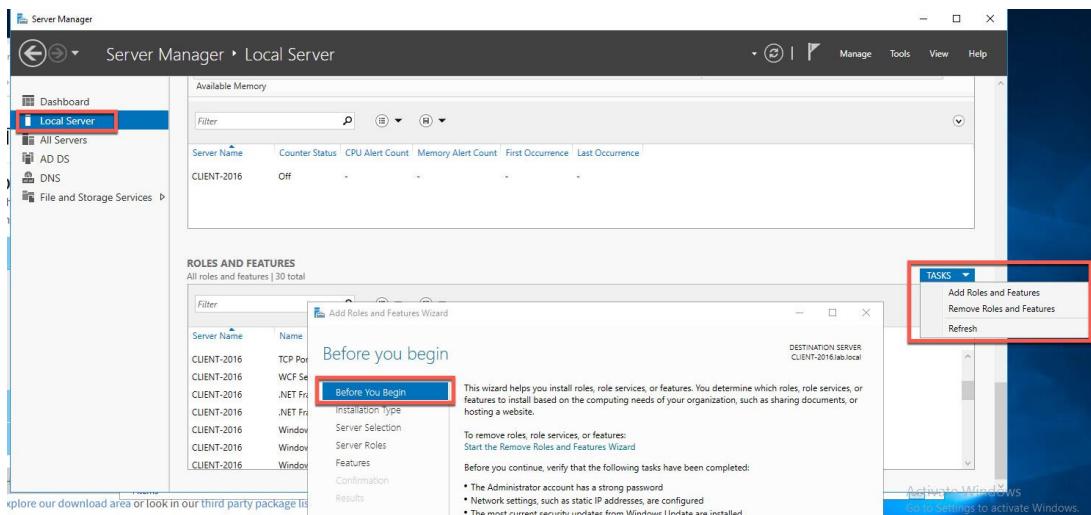


### 5.1.10 Install Active Directory Certificate Services:

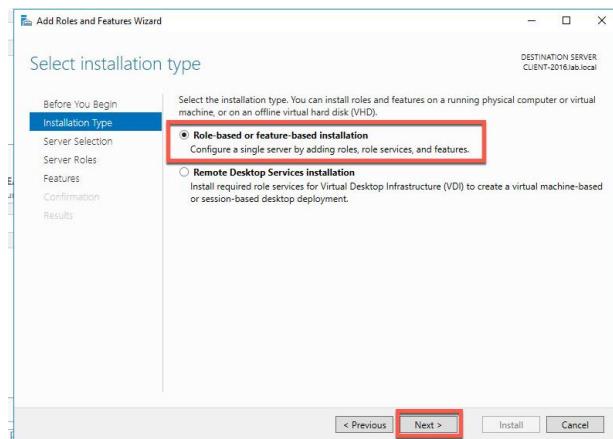
The general directions are found here: [https://technet.microsoft.com/en-us/library/jj717285\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/jj717285(v=ws.11).aspx).

The steps used to configure the Windows Server 2016 host in your lab pod are listed below.

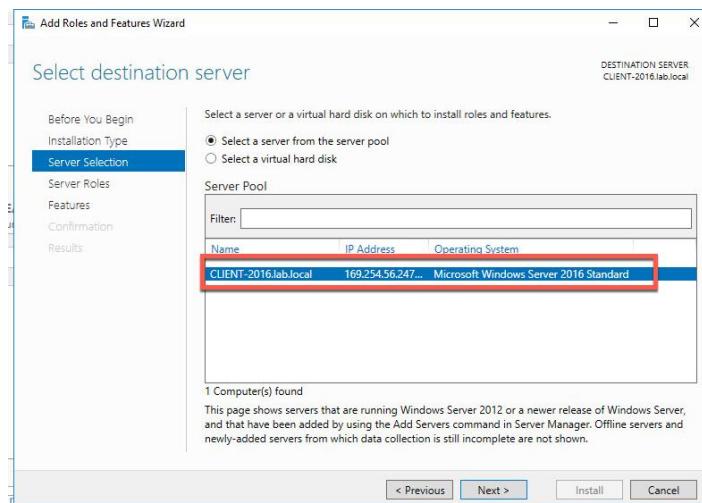
- ii. Open the Server Manager.
- iii. Select *Manage > Add Roles and Features*.



iv. Select *Role-based or feature-based installation* and click *Next*.

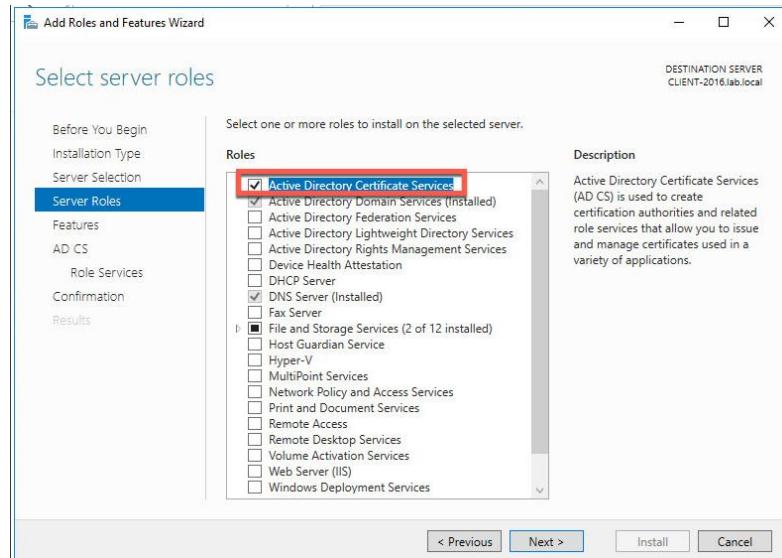


v. Accept default server (the local machine) and click *Next*.

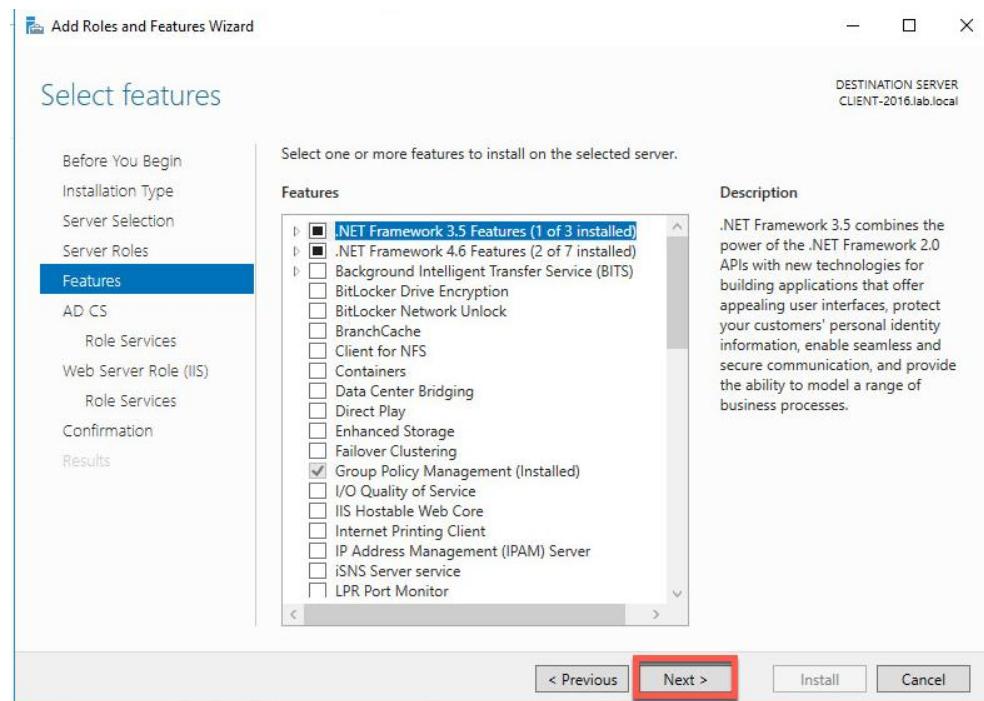


vi. Select *Active Directory Certificate Services*.

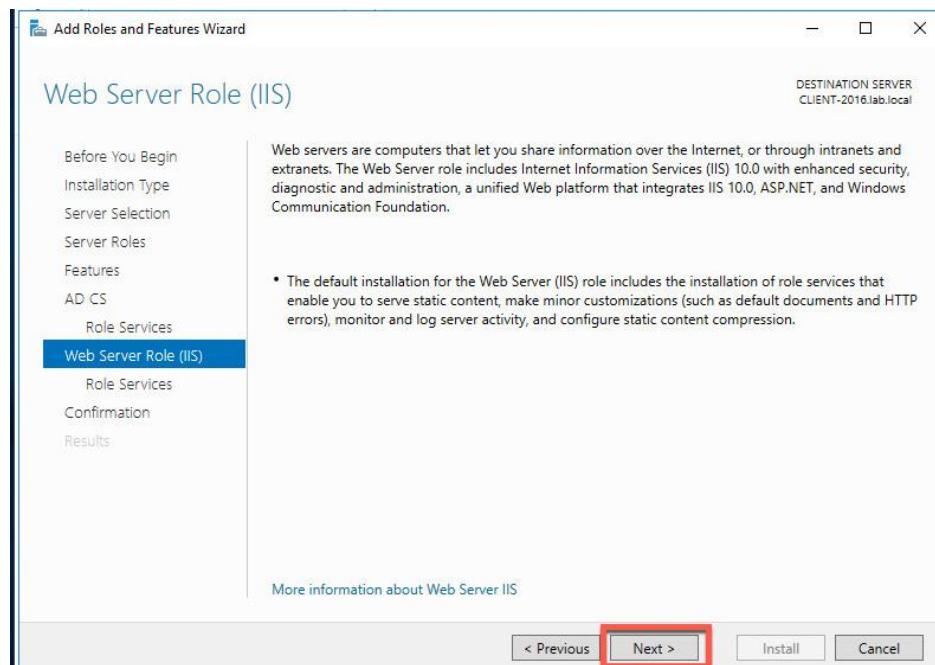
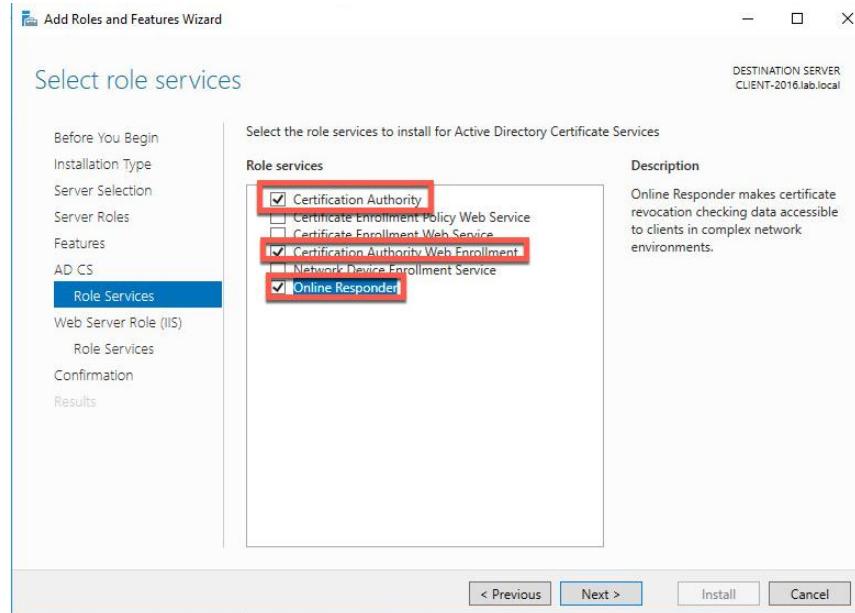
vii. Click *Next*.

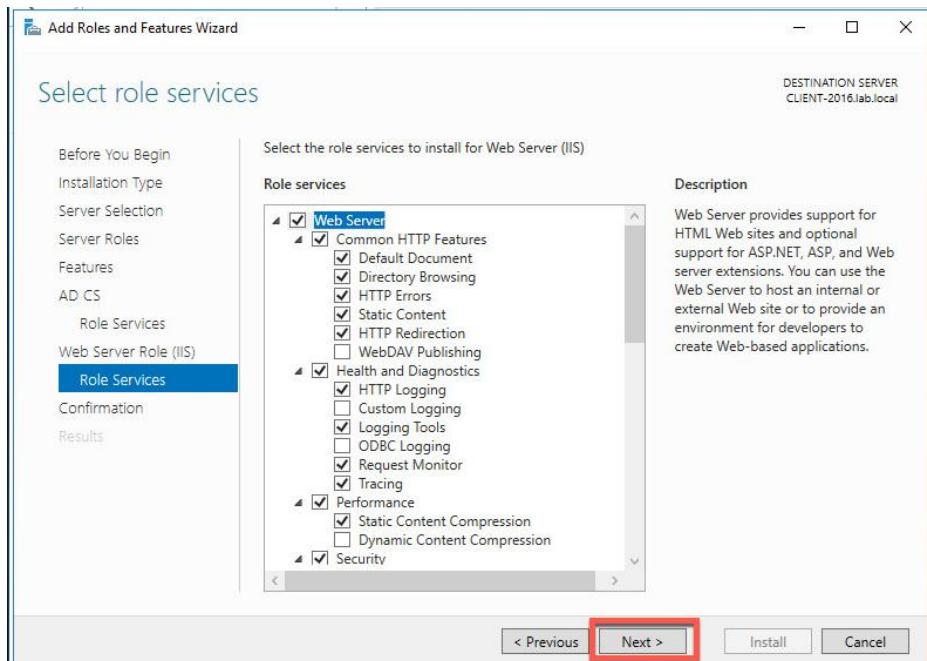


- viii. In the features Window, click *Next*.



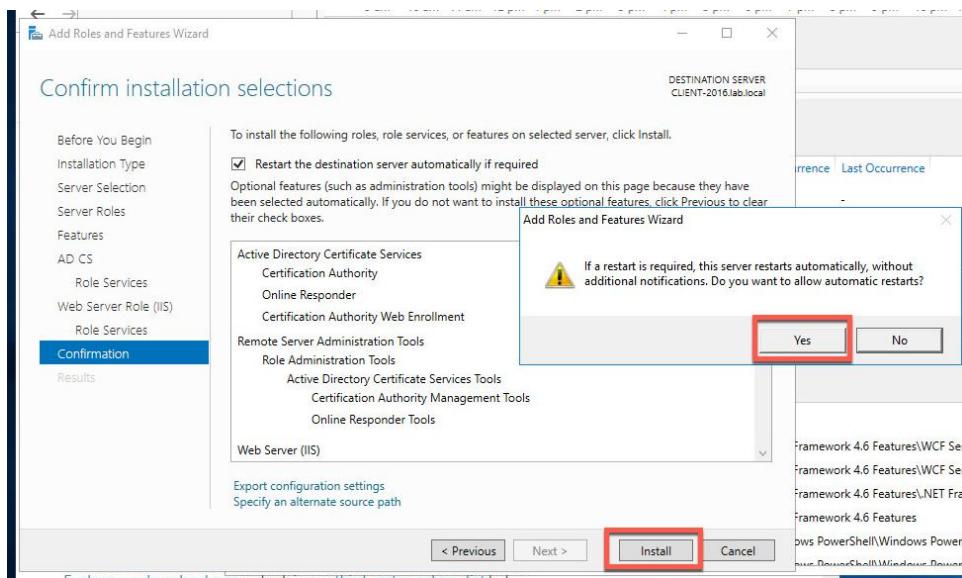
- ix. In the Role Services window, select *Certification Authority, Certificate Authority Web Enrolment, Online Responder*.  
x. Continue to click *Next* until Confirmation step





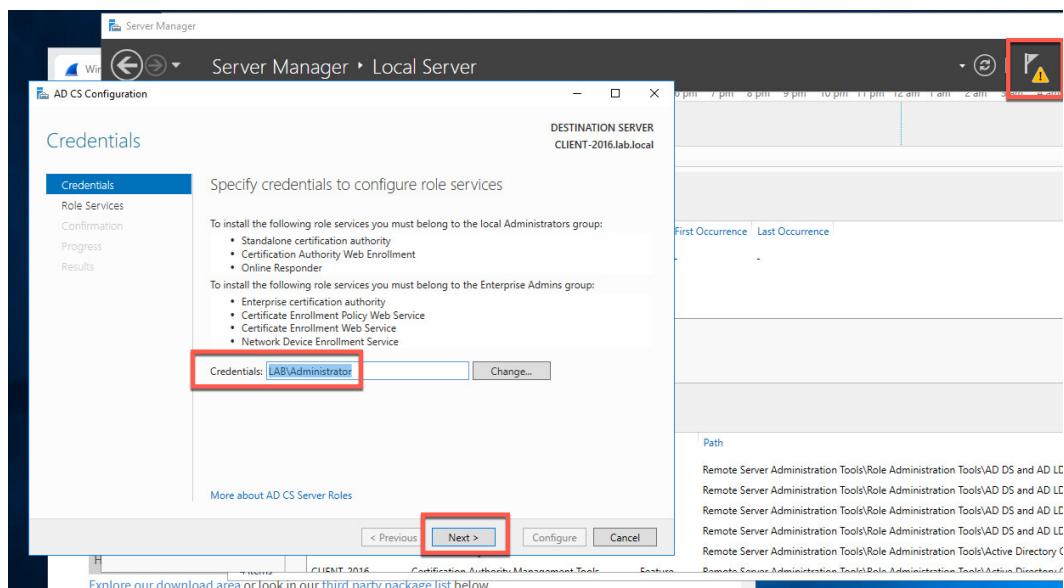
- xi. In the confirmation window, select “*Restart the destination server automatically if required*” and click *Install*.

**Note:** Installation begins but the server will reboot. Installation finishes after the reboot.

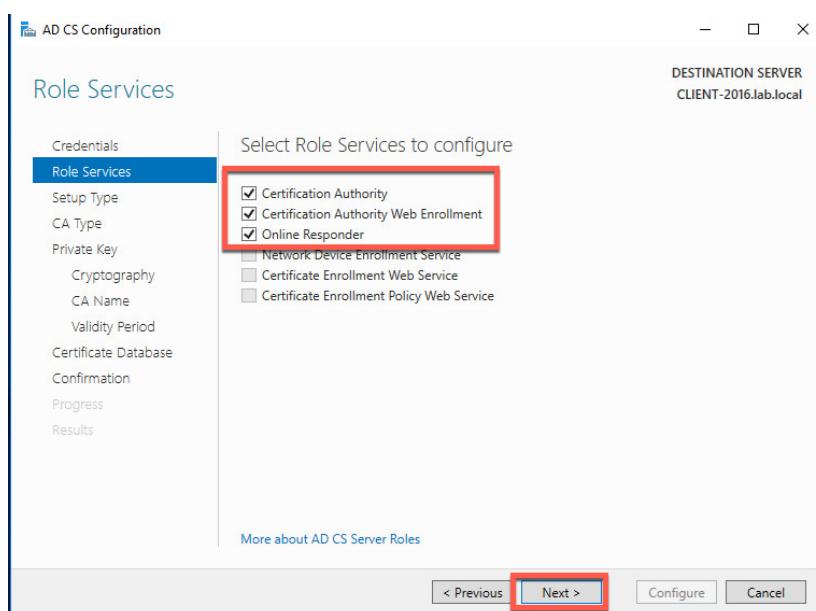


- xii. The Windows server (student desktop) will reboot and you will be disconnected for a time.

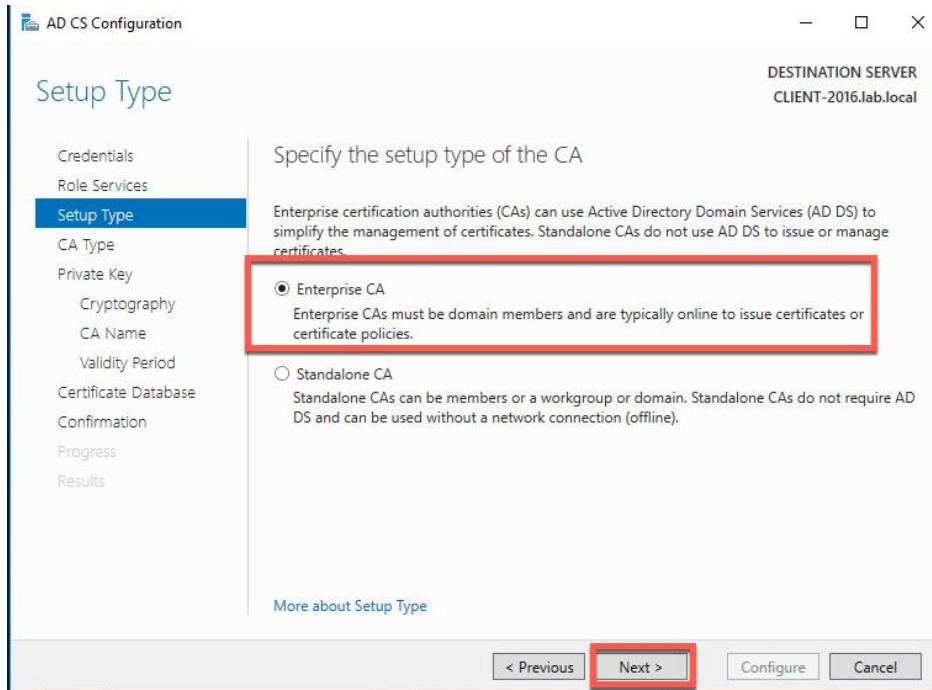
- xiii. Click *Close* on the Add Roles and Features Wizard window.
- xiv. Click the Warning notification in the Server Manager and click “*Configure Active Directory Certificate Services*” on the destination server.
- xv. In the AD CS Configuration window, click *Next* to accept the default credential user.



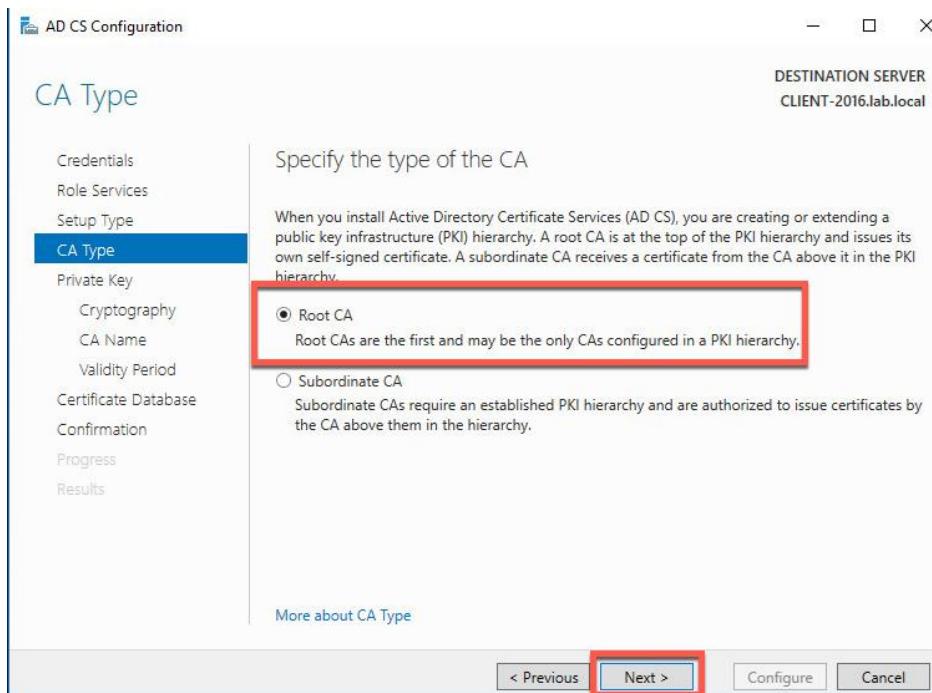
- xvi. In the Role Services window, select *Certification Authority, Certification Authority Web Enrollment, Online Responder* and click *Next*.



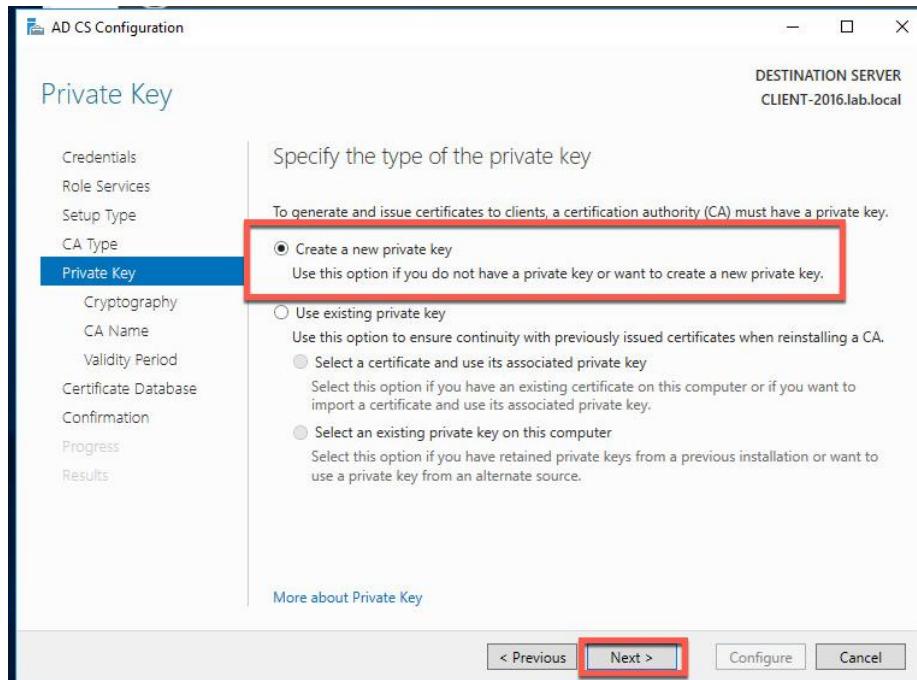
- xvii. Select *Enterprise CA* (not Standalone CA) and click *Next*.



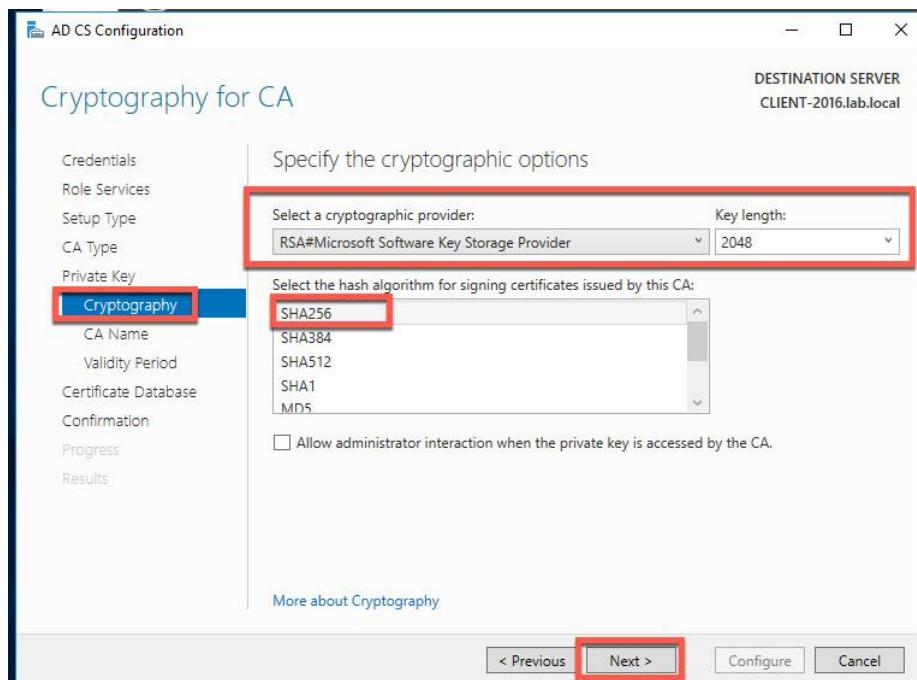
- xviii. Select *Root CA* and click *Next*.



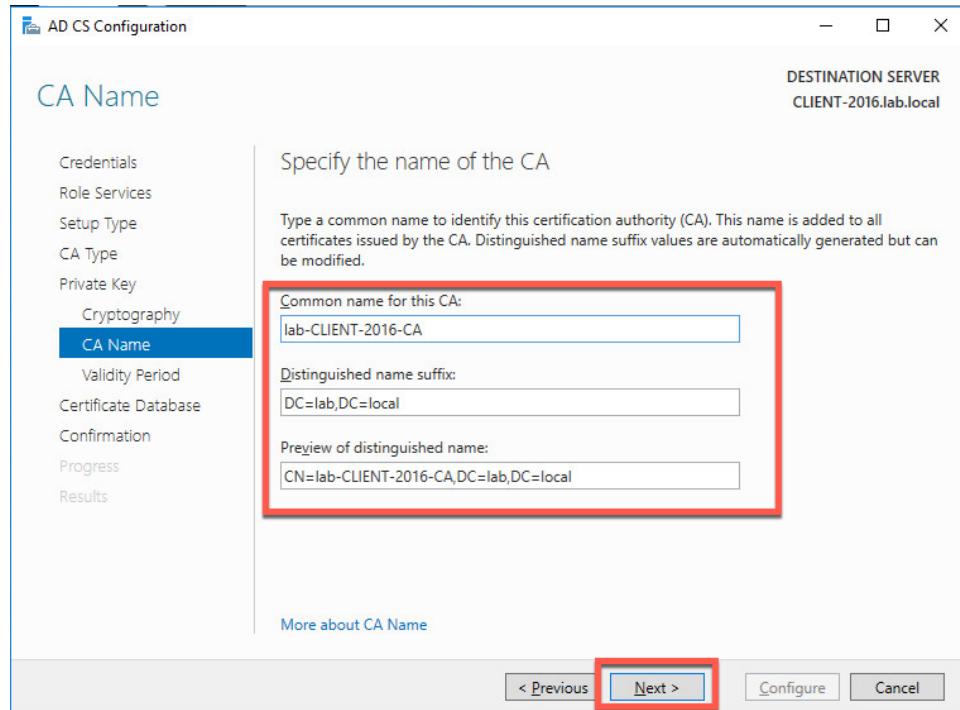
- xix. Select *Create a new private key* and click *Next*.



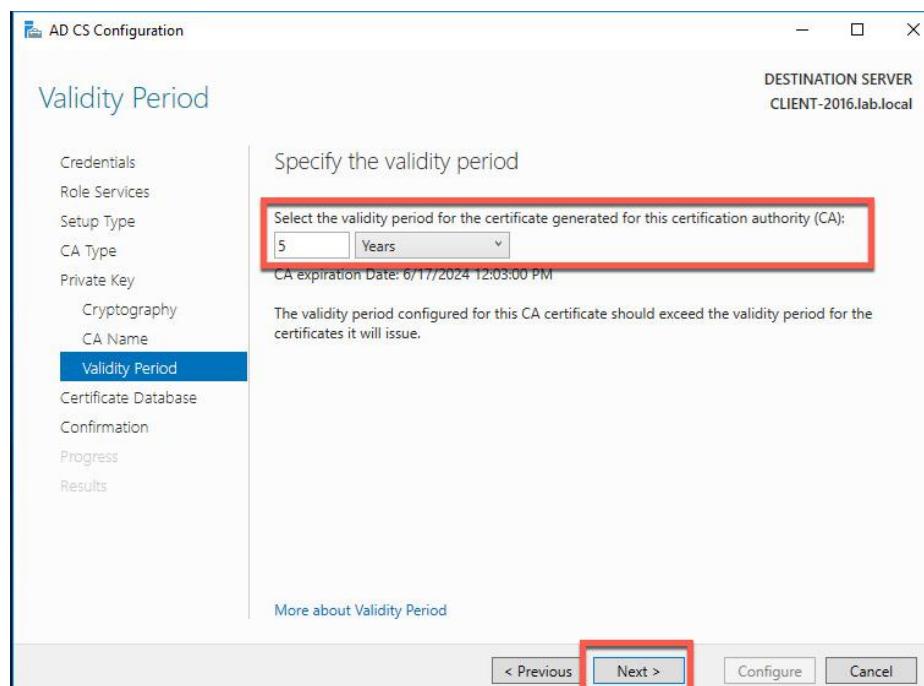
xix. Leave the default RSA 2048 but select *SHA256* and click *Next*.



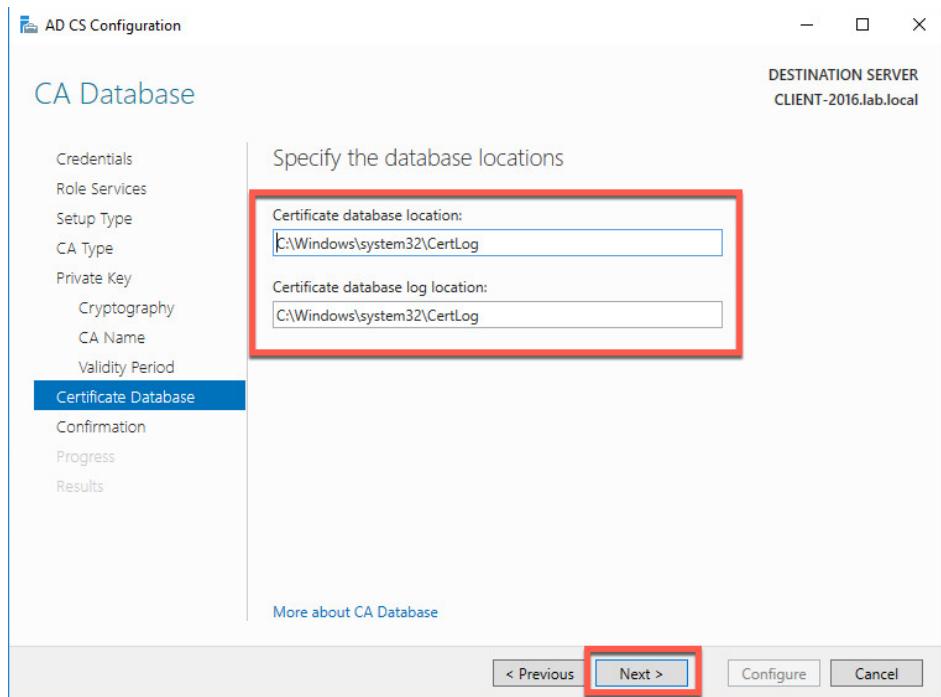
xx. Leave the default CA Name and click *Next*.



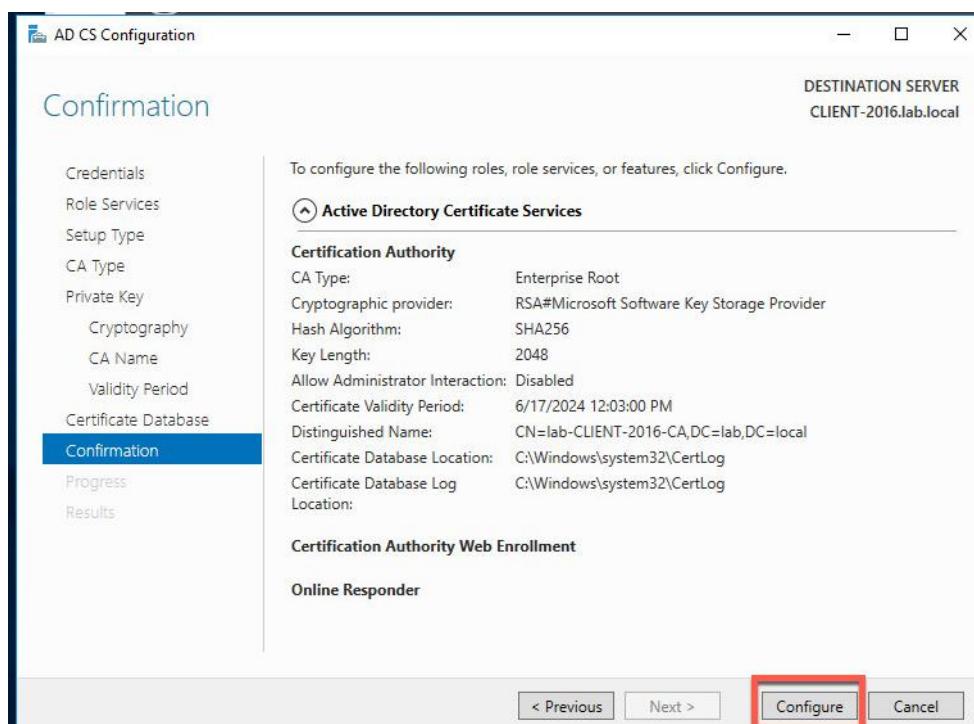
- xxi. Leave the default validity period and click *Next*.



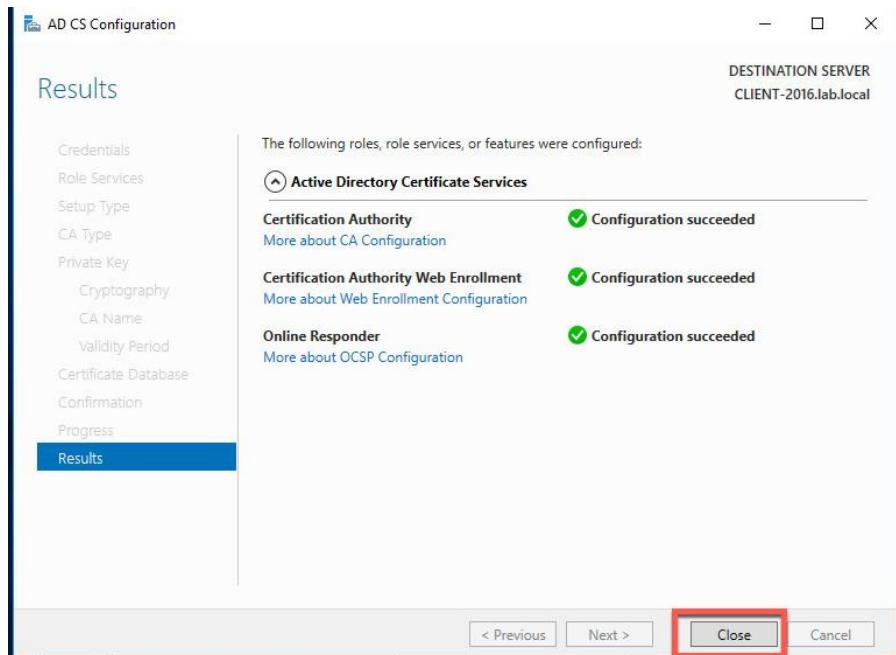
- xxii. Leave the default database locations and click *Next*.



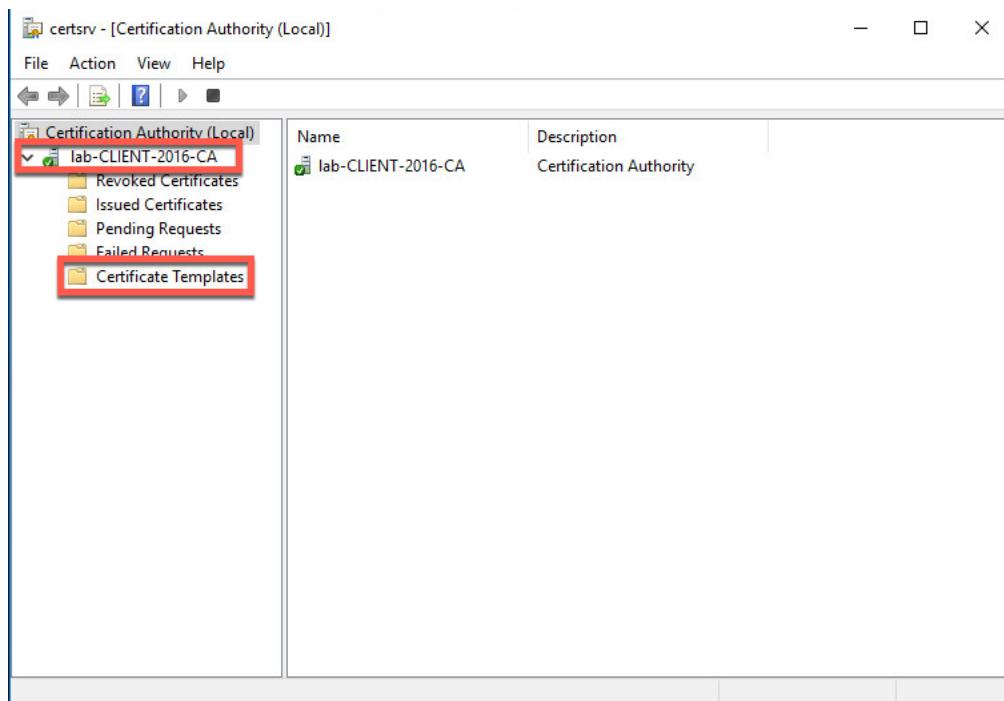
xxiii. Click *Configure*.



xxiv. View the success status and click *Close*.

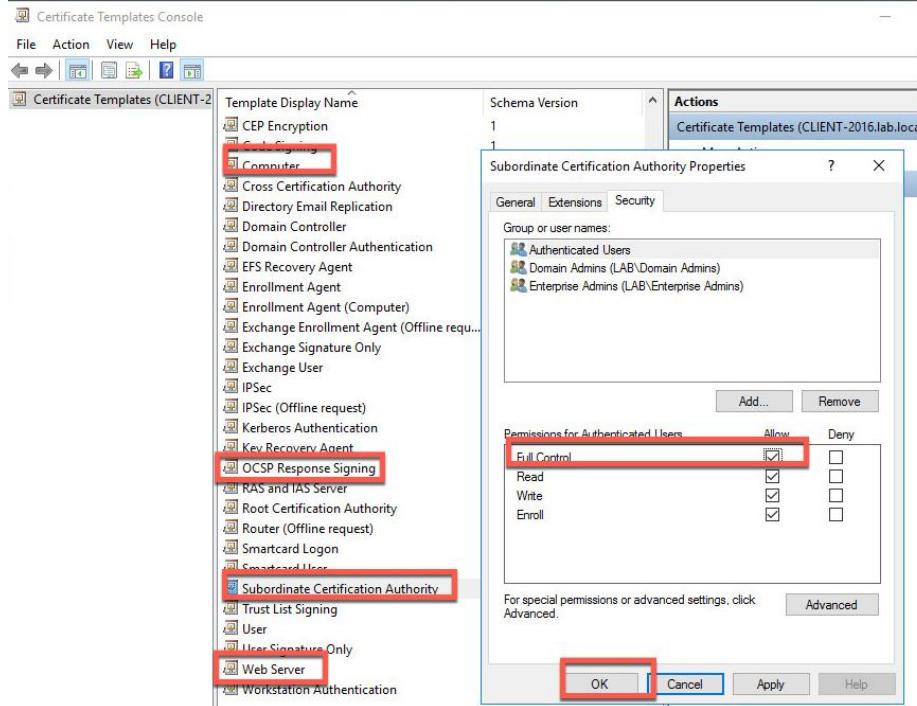


- xxv. In Server Manager go to *Tools>Administrative Tools > Certification Authority*.
- xxvi. Click *lab-CLIENT-2016-CA* (or what your host is).



- xxvii. Right-click *Certificate Templates* and select *Manage* to open the MMC.

- xxviii. Right-click *Subordinate Certification Authority* and select *Properties*.
- xxix. Click the *Security tab*.
- xxx. Select *Full Control* and click *OK*.



- xxxi. Repeat for the templates Computer, OCSP Response Signing, Web Server.
- xxxii. Close the open windows.
- xxxiii. You should be able to open Chrome and browse to **localhost/certsrv** and issue a certificate.

#### 5.1.11 Log in as “lab-user”:

*Log in as the lab-user using the password you set up for this user (**Pal0Alt0**) and start installing the applications listed below.*

Create a certificate management shortcut on the desktop.

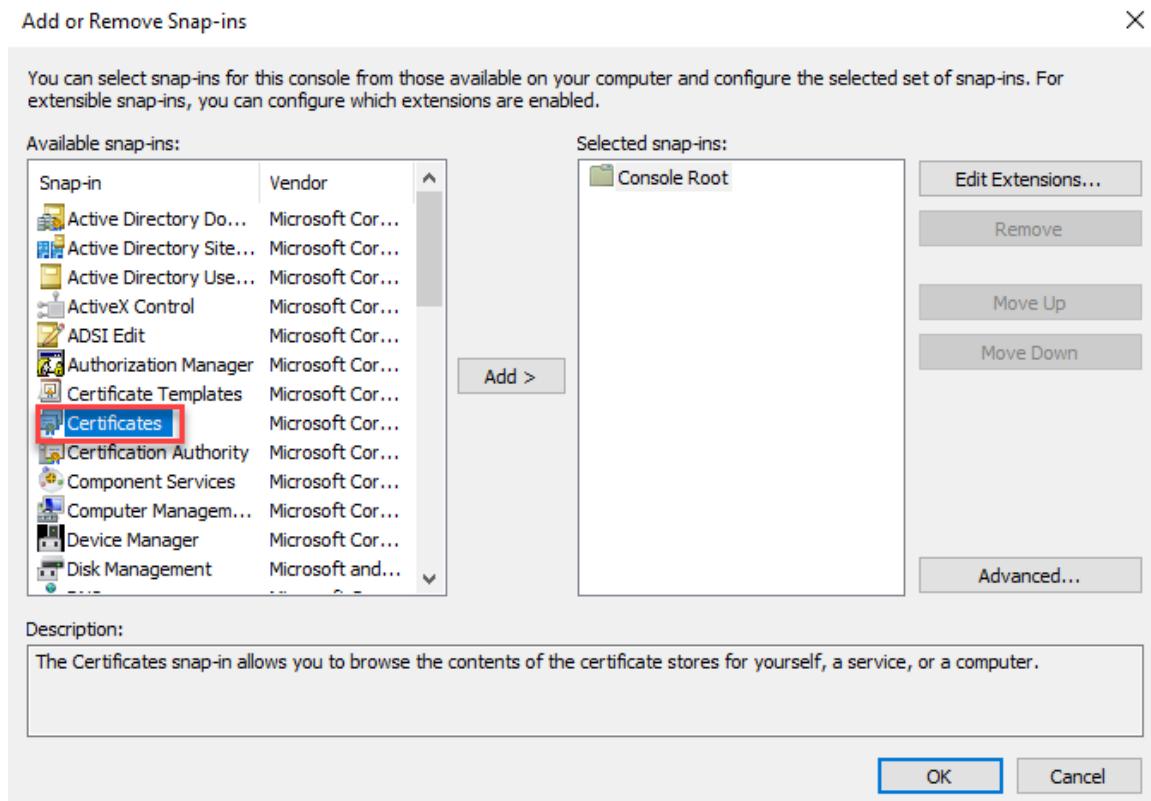
Right click the window pane (located on the bottom left of the screen) and type select Run.



Enter mmc into the Run text box and press Enter.

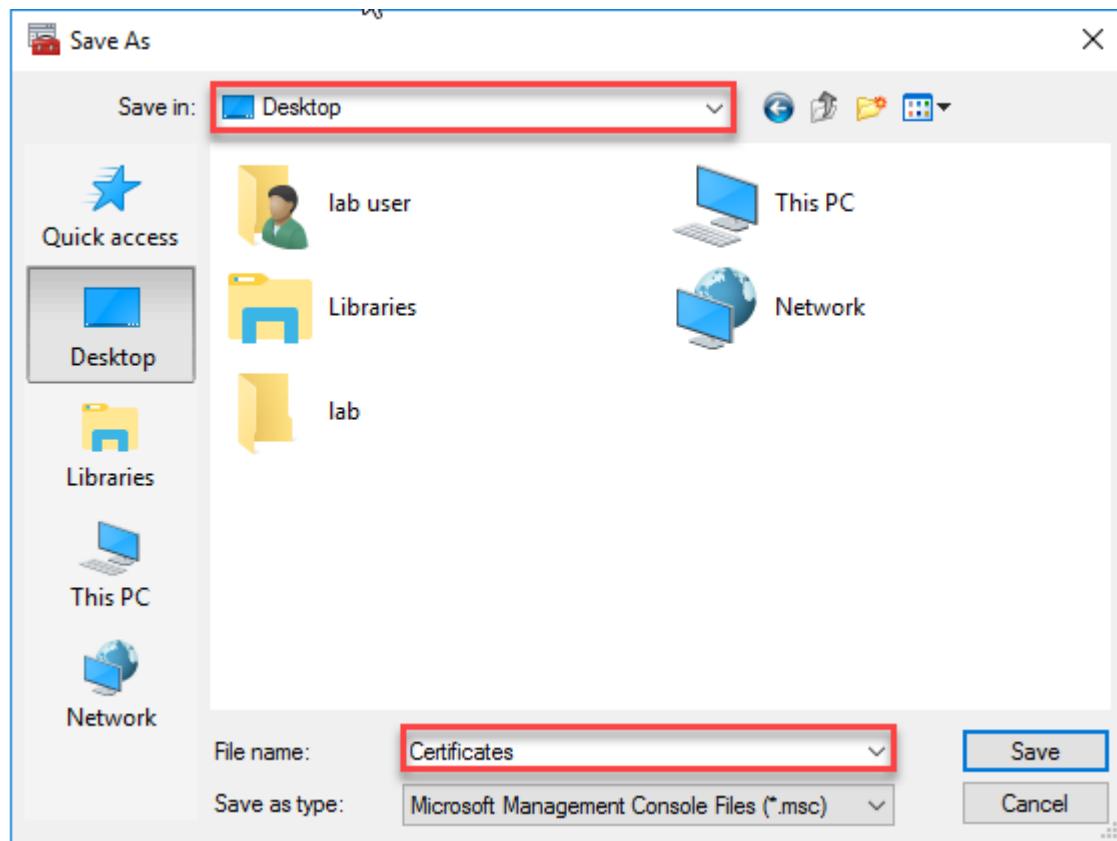
Click Yes

In Console1 dialog box select File / Add or Remove Snap-ins and select certificates

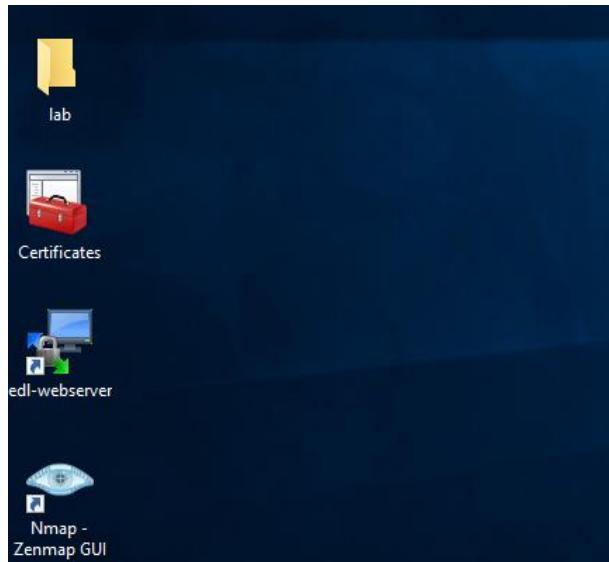


Accept the defaults and click finish.

Go to File Save As and save this certificate mmc to the desktop with the name Certificates.



Your desktop should now show the following certificate mmc



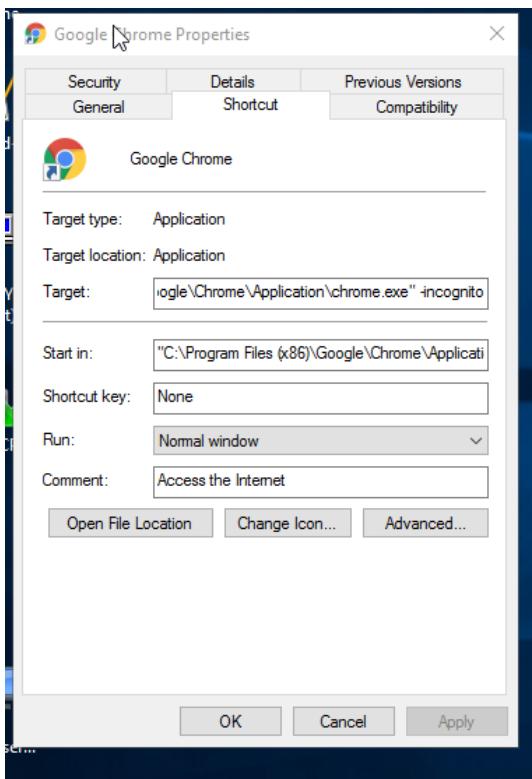
#### 5.1.12 Install Google Chrome:

Due to the enhanced security default configuration of Microsoft Internet installer, it is easier to install the Google chrome browser via Windows PowerShell.

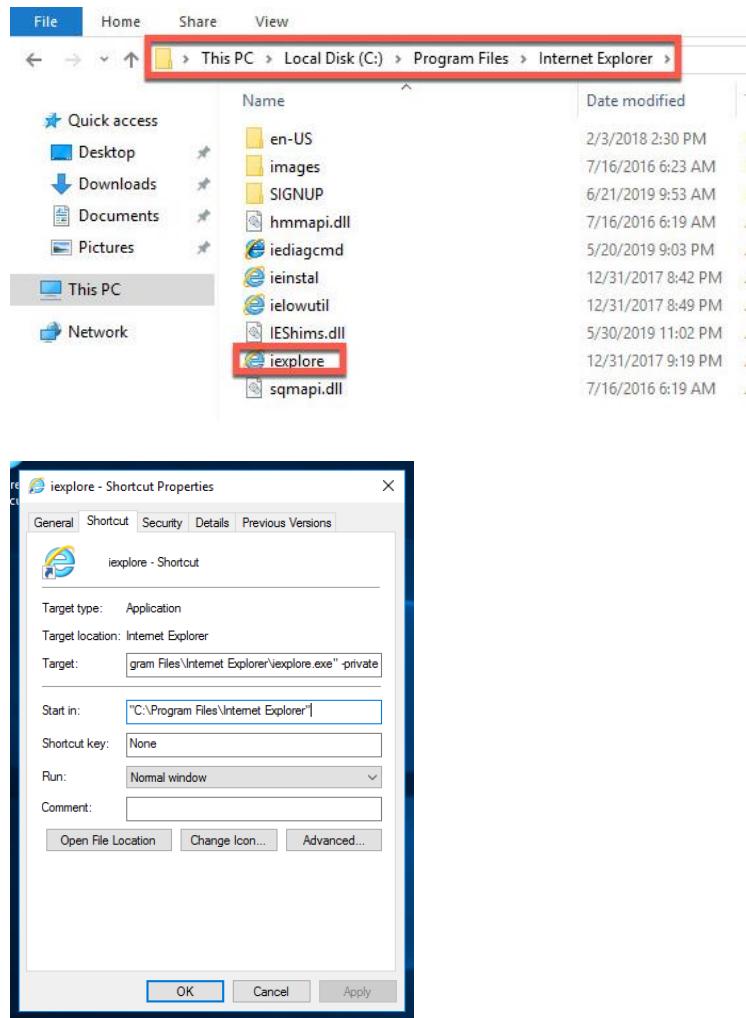
Here is a url link to a site with PowerShell install script:

<https://www.ryadel.com/en/install-google-chrome-with-powershell-script/>

After installing, Chrome, create a Desktop shortcut. Right click the Google Chrome shortcut and select properties. In the Google Chrome Properties dialog box, enter “-incognito” right after ...\\chrome.exe” and click OK to close the dialog box. Chrome will now open up in incognito mode by default.



Create a Desktop shortcut for Internet Explorer by dragging and dropping C:\\Program Files\\Internet Explorer\\iexplore onto your Desktop. Right click the Internet Explorer shortcut and in the target text box enter “-private” after ...\\iexplore.exe”. Internet Explorer will now open up in private window mode by default.

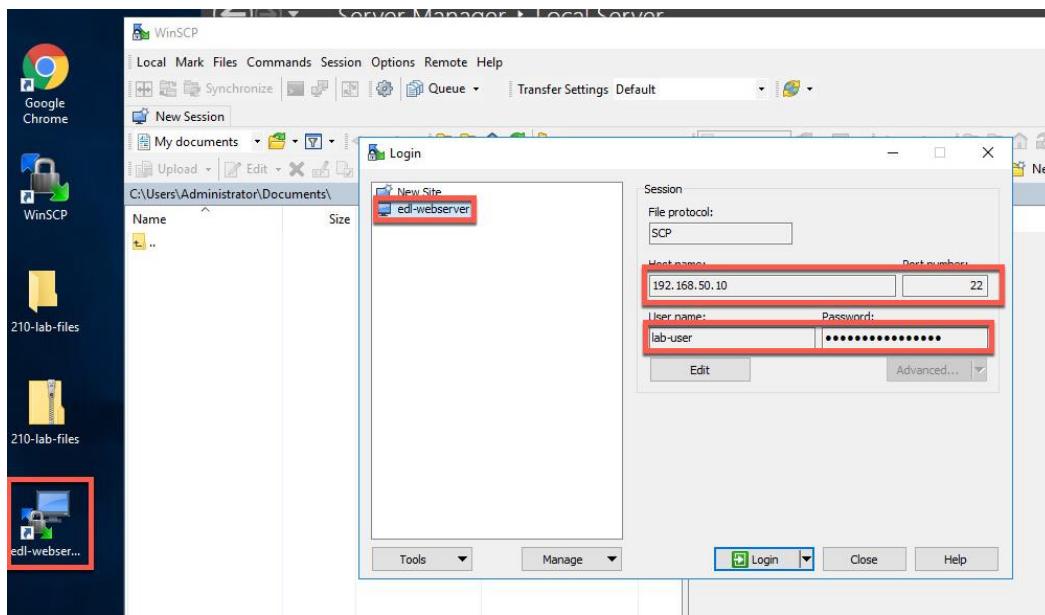


### 5.1.13 Install WinSCP:

Download and install WinSCP from <https://winscp.net>.

Create a shortcut on the desktop with one preconfigured entry for edl-web server with the following attributes:

1. File protocol: SCP
2. Host name: **192.168.50.10**
3. Lab name: **lab-user**
4. Password: **paloalto**
5. Name: **edl-webserver**



#### 5.1.14 Install Wireshark:

Install Wireshark from <https://www.wireshark.org> and turn off Wireshark updates by following the directions below.

1. Go to Edit > Preferences... > Advanced. Search for “gui”.
2. Find the option `gui.update.enabled`.
3. Double-click the value “*TRUE*” to change it to “*FALSE*”
4. Click *OK* to close the Preferences dialog.
5. Close the Wireshark program.

#### 5.1.15 Install Zenmap/nmap:

Download and install nmap from <https://nmap.org/download.html>.

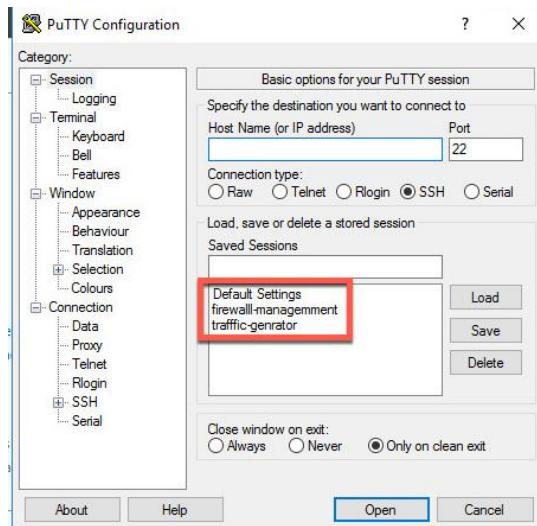
#### 5.1.16 Install PuTTY:

Go to <https://www.putty.org> and download and install PuTTY.

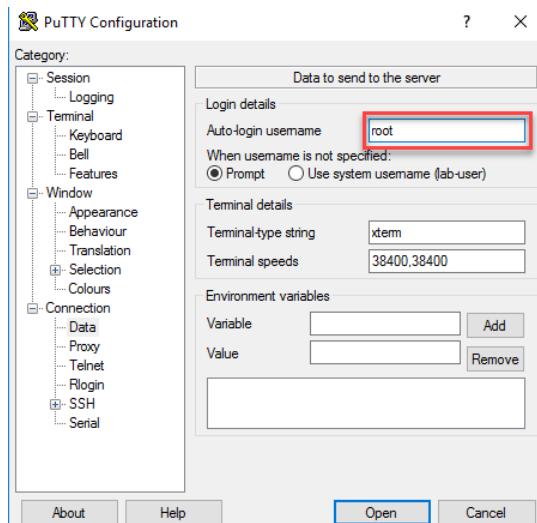
Create a shortcut on your desktop.

Open PuTTY and create 2 preconfigured SSH entries:

- i. “**firewall management**” with IP address: **192.168.1.254**
- ii. “**traffic-generator**” with IP address: **192.168.50.10**

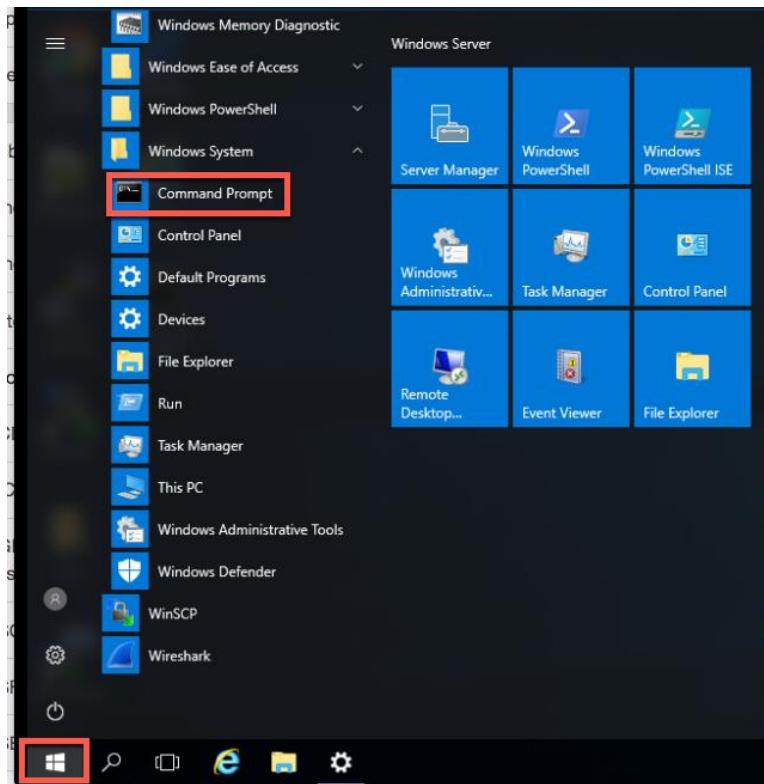


- iii. To add a predefined user to Putty for traffic-generator. Configure the following:  
 Go to *Connection -> Data* and specify the username with that you want to log in to your SSH server under Auto-login username. In this case use **root**: Then go to Session again.



#### 5.1.17 Create Desktop shortcut for the command prompt.

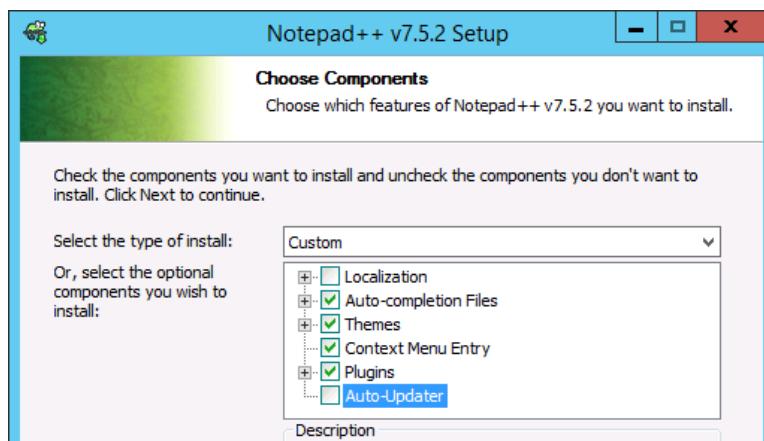
Click the windowpane in the bottom left corner of your Desktop and go to Windows System>Command Prompt. Drag the Command Prompt icon to your desktop.



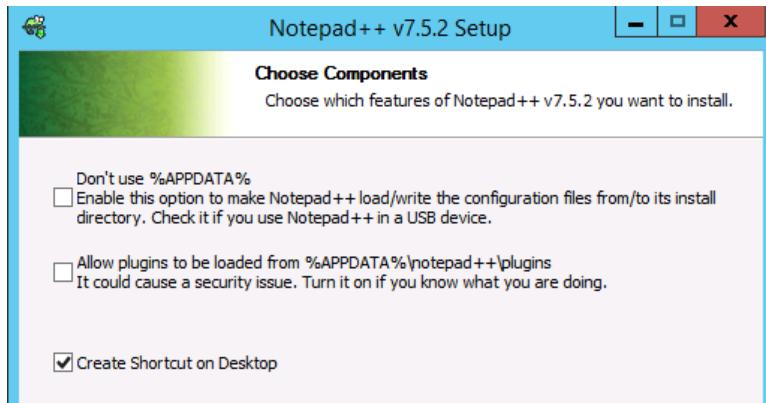
### 5.1.18 Install Notepad++:

Go to <https://notepad-plus-plus.org> and download and install the latest version.

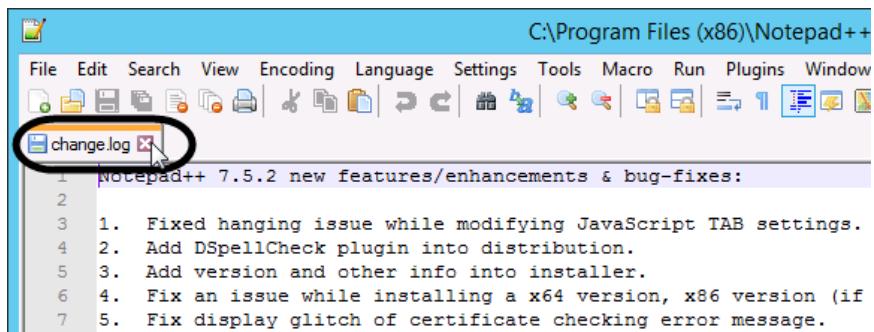
- i. On the first *Choose Components* page, accept the defaults except deselect Auto- Updater.



- ii. On the second *Choose Components* page, select to Create Shortcut on Desktop.



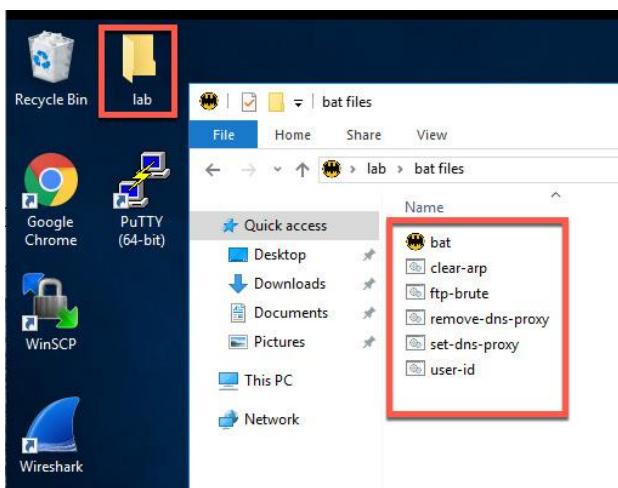
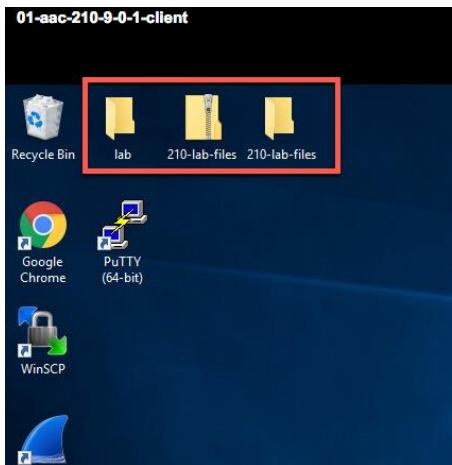
- iii. After the installation is complete, launch the *Notepad++* program and close the change.log tab. The default “new 1” tab will appear.



#### 5.1.19 Set up Lab Folder:

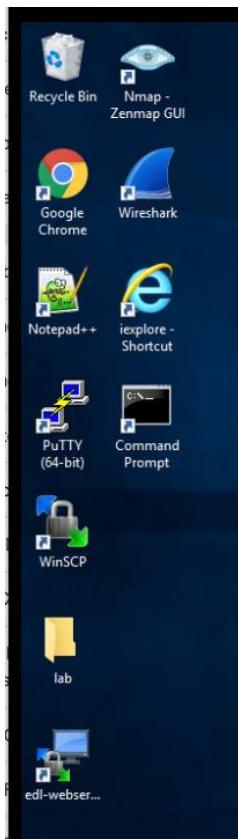
Download the 210-lab-files zip folder from the academy share to the server’s desktop and extract the 210-lab-files folder on your desktop. In the 210-lab-files folder move the “lab” folder to the server’s Desktop. The VMware Workstation ova/lab config share drive URL is posted in the following Cybersecurity Academy Moodle Courses: Configuration Infrastructure course, Cybersecurity Prevention and Countermeasures course, Firewall Essentials Configuration and Management course and the Optimizing Firewall Threat Prevention course.

Delete the 210-lab-files zip folder and 210-lab-files folder so only the “lab” folder remains with the bat files remain on the Desktop.



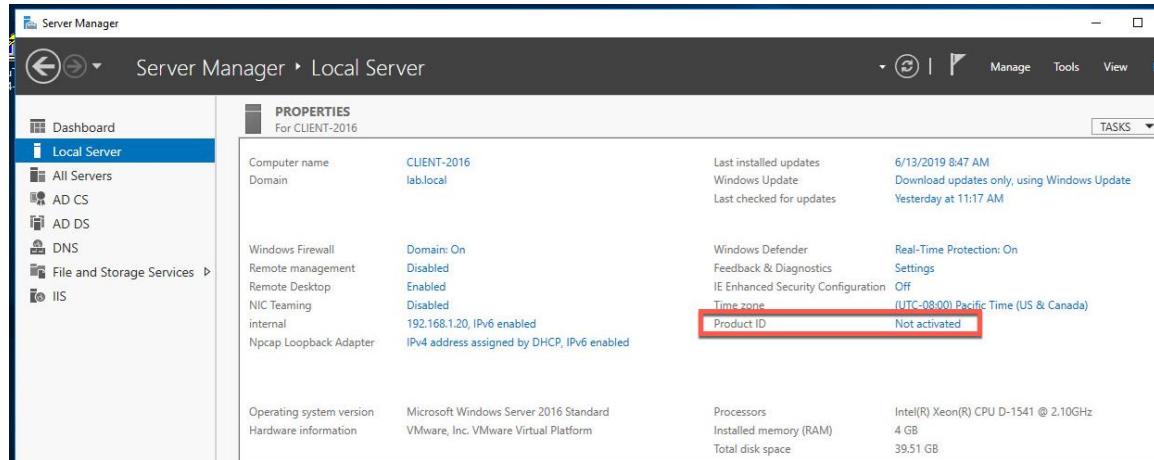
### 5.1.20 The “lab-user” Desktop and Licensing Your Server 2016:

After completing all your installations the lab-user’s desktop should have the following application shortcuts:



### 5.1.21 Google Chrome, PuTTY, WinSCP, Wireshark, Nmap-Zenmap GUI, WinSCP edl-webuser and Notepad++.

In Server Manager > Properties > Product ID click “*Not Activated*” and enter your institution’s Microsoft account product ID to license your Server 2016.



PROPERTIES For CLIENT-2016			
Computer name	CLIENT-2016	Last installed updates	6/13/2019 8:47 AM
Domain	lab.local	Windows Update	Download updates only, using Windows Update
		Last checked for updates	Yesterday at 11:17 AM
Windows Firewall	Domain: On	Windows Defender	Real-Time Protection: On
Remote management	Disabled	Feedback & Diagnostics	Settings
Remote Desktop	Enabled	IE Enhanced Security Configuration	Off
NIC Teaming	Disabled	Time zone	(UTC-08:00) Pacific Time (US & Canada)
internal	192.168.1.20, IPv6 enabled	Product ID	<b>Not activated</b>
Npcap Loopback Adapter	IPv4 address assigned by DHCP, IPv6 enabled		
Operating system version	Microsoft Windows Server 2016 Standard	Processors	Intel(R) Xeon(R) CPU D-1541 @ 2.10GHz
Hardware information	VMware, Inc. VMware Virtual Platform	Installed memory (RAM)	4 GB
		Total disk space	39.51 GB

### 5.1.22 Change the IP Address and Default Gateway the Server and Connect the Server to vmnet1:

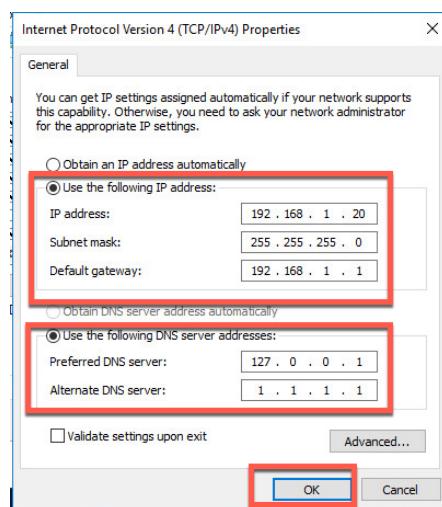
Open the network adapter make the following changes:

**IP Address: 192.168.1.20**

**Subnet mask: 255.255.255.0**

**Default gateway: 192.168.1.1**

Keep the *Primary DNS* server IP address as 127.0.0.1 and use either 1.1.1.1 or your NAT'd VMnet8 default gateway address as the Alternate DNS Server.



### 5.1.23 Change the Name of the Network Adapter:

Rename your network adapter from the default name “Ethernet0” to the name “internal”.



### 5.1.24 Baseline Snapshot Your Server 2016 VM:

Take a VMware Workstation snapshot of your virtual machine after completing all the above configurations and licensing it.

You can return to this snapshot if your virtual machine becomes corrupted and unusable.

## 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 VMware workstation PA-VM-9.0-PanOS-FW tab, select “*Power on this virtual machine*”. Your VM-50 appliance will start the boot up process.

**Note:** This will take approximately 5 minutes. 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](http://updates.paloaltonetworks.com) server.

- 6.1.2** Log onto your firewall with username **admin** and password **admin**. 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

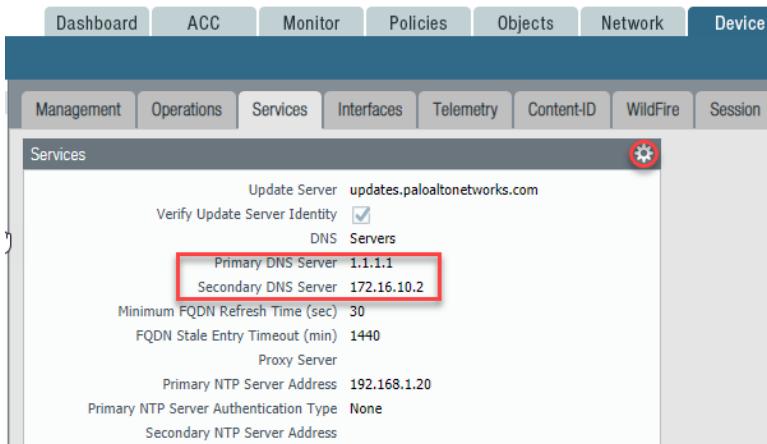
Ip address: 192.168.1.254
Netmask: 255.255.255.0
Default gateway: 192.168.1.10
Ipv6 address: unknown
Ipv6 link local address: fe80::20c:29ff:fe64:4588/64
Ipv6 default gateway:
```

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

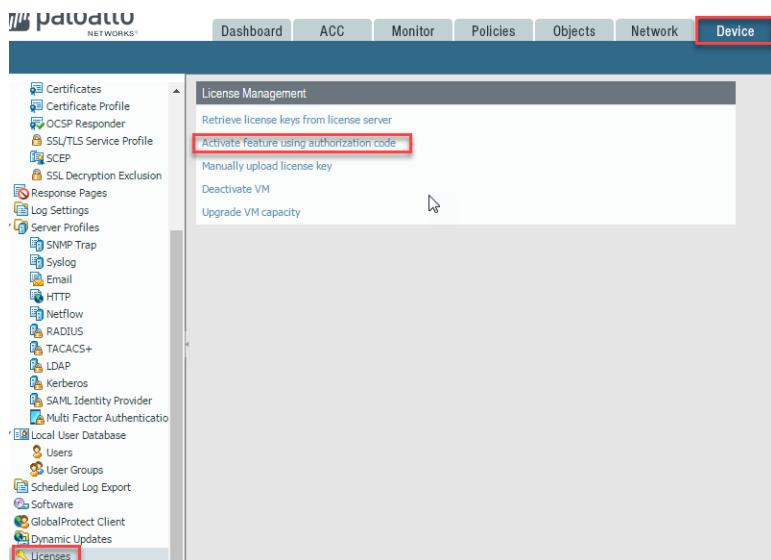
```
admin@firewall-a> ping host 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=127 time=7.73 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=127 time=7.66 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=127 time=7.39 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=127 time=8.94 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 host computer’s Chrome browser and connect to your VM-50 Web-UI by entering [https://<vr\\_ext\\_ip\\_ens160\\_int>](https://<vr_ext_ip_ens160_int>) in the host browser’s URL. A privacy error will occur, click “Advanced” and then click “Proceed to 192.168.1.254 (unsafe).

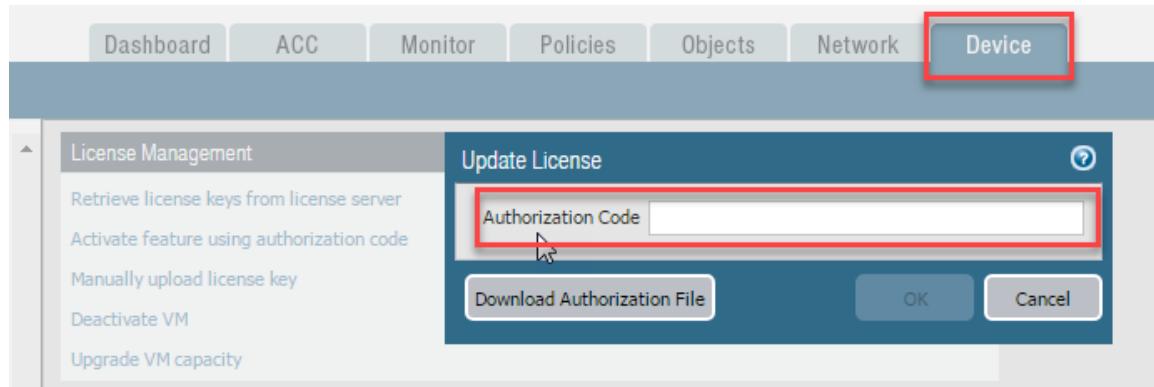
- 6.1.4** Log into your VM-50 appliance using username: “**admin**” and password: “**admin**”. Select the *Device* tab and on the left-hand side of Web-UI click *Setup*.
- 6.1.5** Now select the *Services* tab and then click the *settings* icon on right hand side.
- 6.1.6** In the Services dialog box set the Primary DNS Server to 1.1.1.1 or the gateway address for your vmnet8. If the network ID of your vmnet8 is 172.16.10.0/24 then the vmnet8 default gateway address would be 172.16.10.2 as shown in screenshot below.



- 6.1.7** In *Device > Licenses* under “License Management”, click “Activate features using authorization code”.



- 6.1.8** Enter the authorization code provided to you by your academy representative, click OK and click OK after receiving warning. Your firewall will now reboot to load your licenses.



- 6.1.9** Log back into your firewall. Close the welcome page and go to *Device Tab > Dynamic Updates* and click *Check Now* on the lower left-hand side.

- 6.1.10** Download and install all the updates.

Continue to Check Now and install the most recent updates until there are no

longer any updates to be downloaded.

The screenshot shows the Palo Alto Networks Device interface. The 'Device' tab is selected. On the left, there's a sidebar with various configuration options like Setup, High Availability, and Dynamic Updates. The 'Dynamic Updates' option is highlighted with a red box. At the bottom of the sidebar, there are three buttons: 'Check Now' (highlighted with a red box), 'Upload', and 'Install From File'. The main content area displays a table of updates:

Version	File Name	Features	Release Date
8158-5487	panupv2-all-contents-8158-5487	Apps, Threats	2019/05/31 00:22:15 UTC
8159-5490	panupv2-all-contents-8159-5490	Apps, Threats	2019/06/05 00:01:21 UTC
8160-5498	panupv2-all-contents-8160-5498	Apps, Threats	2019/06/06 21:51:21 UTC
8161-5500	panupv2-all-contents-8161-5500	Apps, Threats	2019/06/10 23:23:56 UTC
8162-5503	panupv2-all-contents-8162-5503	Apps, Threats	2019/06/14 05:06:40 UTC
8163-5511	panupv2-all-contents-8163-5511	Apps, Threats	2019/06/17 18:42:08 UTC
8164-5515	panupv2-all-contents-8164-5515	Apps, Threats	2019/06/19 06:07:21 UTC
8165-5521	panupv2-all-contents-8165-5521	Apps, Threats	2019/06/25 23:33:43 UTC
8166-5525	panupv2-all-contents-8166-5525	Apps, Threats	2019/06/28 00:41:33 UTC
▼ Applications and Threats      Last checked: 2019/06/28 21:07:21 UTC      Schedule: Every Wednesday at 01:02 (Download only)			
77-160	panup-all-gp-77-160	GlobalProtectClientlessVPN	2019/06/03 20:03:19 UTC
▼ GlobalProtect Data File      Schedule: None			
▼ WildFire      Last checked: 2019/06/28 21:07:25 UTC      Schedule: None			
361753-364445	panupv2-all-wildfire-361753-364445	PAN OS 7.1 And Later	2019/06/28 21:05:28 UTC

**Note:** Antivirus updates will not show until you install your Applications and Threats updates. Once installed please click the Check Now button again so that Antivirus shows up and then install them.

