



PAN-OS 7.0 FIREWALL ESSENTIALS LAB SERIES

Lab 2: Basic Interface Configuration

Document Version: 2016-04-19

Copyright © 2016 Network Development Group, Inc.
www.netdevgroup.com

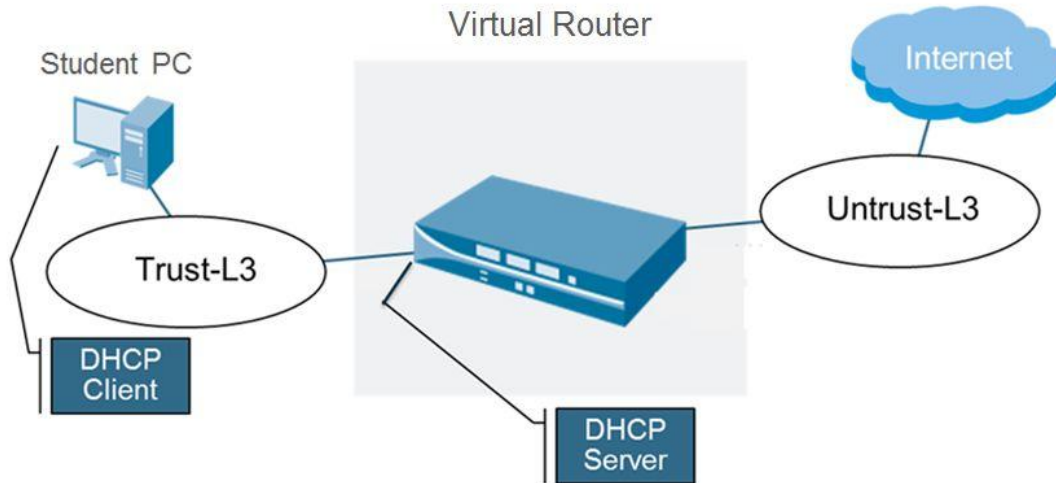
NETLAB Academy Edition, NETLAB Professional Edition, and NETLAB+ are registered trademarks of Network Development Group, Inc.

Palo Alto Networks and the Palo Alto Networks logo are trademarks or registered trademarks of Palo Alto Networks, Inc.

Contents

Introduction	3
Objective	4
Pod Topology	5
Lab Settings	6
1 Create New Security Zones	7
2 Create Interface Management Profiles	11
3 Configure Ethernet Interfaces with Layer 3 Info	14
4 Create a Virtual Router	18
5 Configure DHCP	19
6 Test the DHCP Server	24

Introduction



In this lab, you will create two zones, Trust-L3 and Untrust-L3. The internal clients will connect to the interface assigned to the Trust-L3 Zone. The interface in the Trust-L3 Zone will provide DHCP addresses to these internal clients.

The external-facing interface, which will be in the Untrust-L3 zone, will receive a DHCP address from the ISP. All interfaces on the firewall must route traffic through the external-facing interface by default.

The interface in Untrust-L3 must be configured to respond to pings and the interface in Trust-L3 must be able to provide all management services. You will also need to configure the external interface as an alternate service route to receive updates, dns queries and other management updates.

NOTE: You will not be able to test whether the Untrust-L3 Interface responds to pings until the next lab. You will be able to test the service route configuration.

Lab Notes

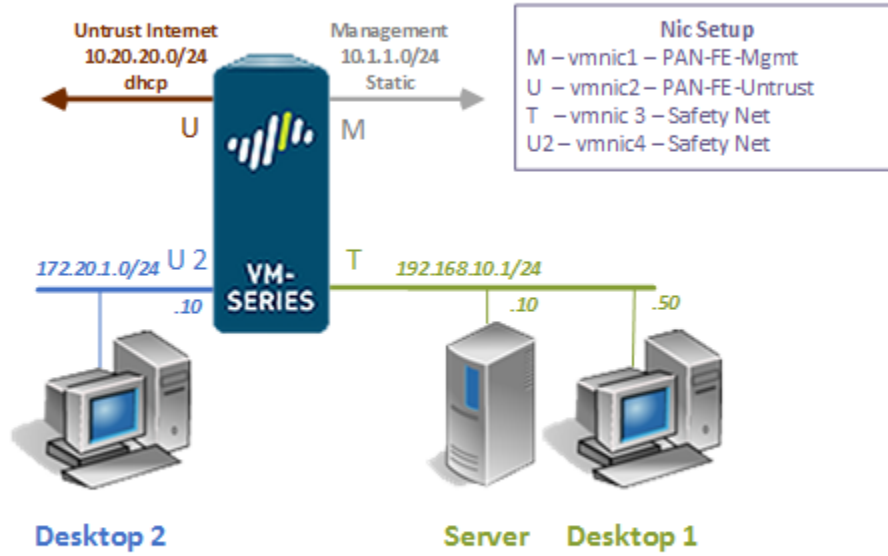
Verify that the DHCP Server is configured correctly by refreshing the IP addresses on your RDP desktop and by pinging the interfaces configured on the firewall.

Objective

In this lab, you will be utilizing Palo Alto technology to perform the following tasks:

1. Create Interface Management Profiles
2. Configure Ethernet interfaces with Layer 3 information
3. Configure DHCP
4. Create a Virtual Router
5. Configure an alternate service route

Pod Topology



Lab Settings

The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Ubuntu Desktop 1	192.168.10.50	sysadmin	Train1ng\$
Ubuntu Server	192.168.10.10	sysadmin	Train1ng\$
Ubuntu Desktop 2	172.30.1.10	sysadmin	Train1ng\$
Palo Alto Firewall	192.168.10.1 172.30.1.1	admin	paloalto

1 Create New Security Zones

1. Click on the **Desktop 1** graphic found on the *topology page*.
2. Login using **sysadmin** as the *username* and **Training\$** as the *password*. Click **Log In**.
3. Double-click on the **Firefox Web Browser** icon located on the *Desktop*.



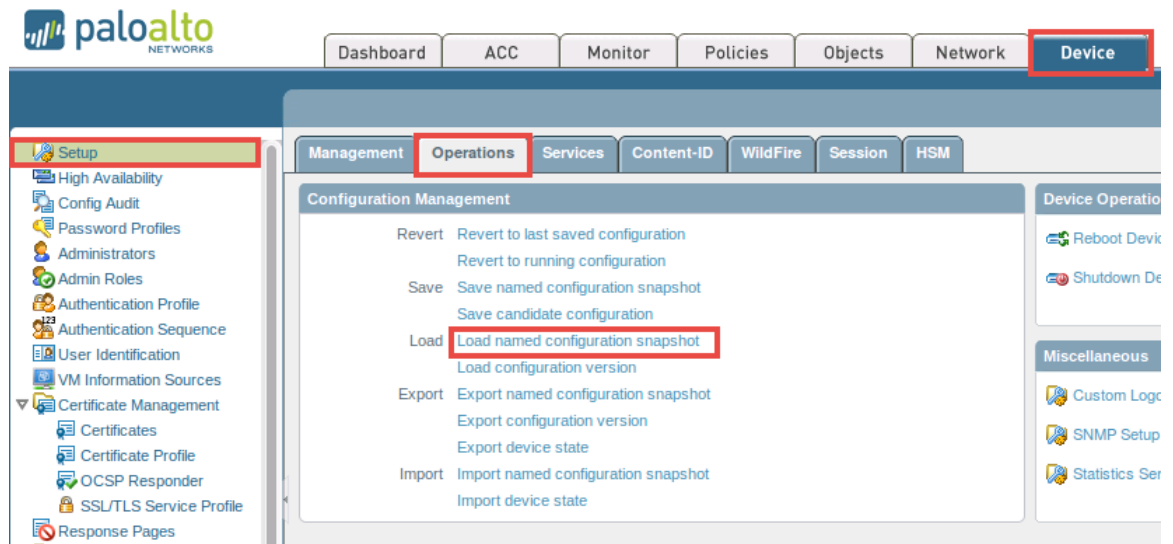
4. In the address field, type **https://192.168.10.1** and press **Enter**.

If you experience the “Unable to connect” message while attempting to connect to the specified IP above, please wait an additional 3-5 minutes for the PA VM to fully initialize and refresh the page to continue.

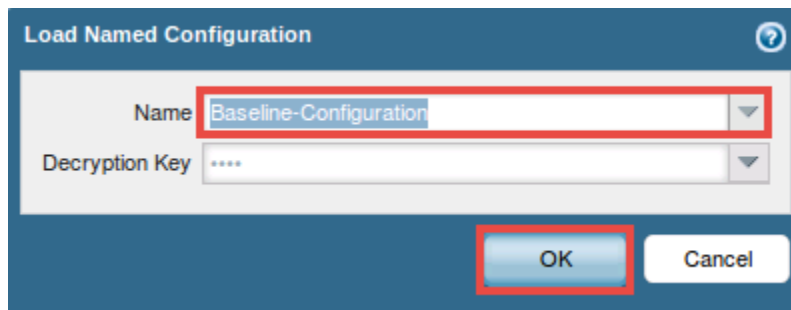
5. Login with the *username* **admin** and *password* **paloalto** on the firewall web interface.



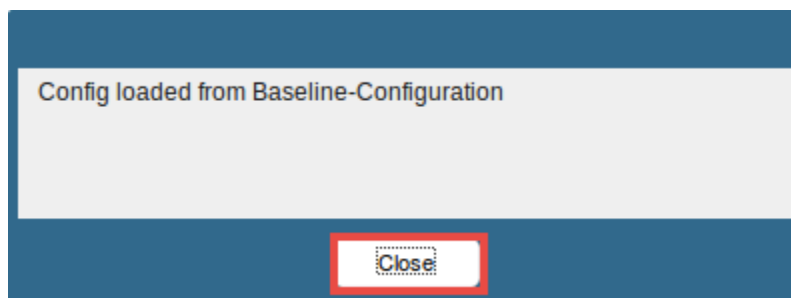
- Using the *Palo Alto WebUI*, navigate to **Device > Setup > Operations** and click on **Load named configuration snapshot** underneath the *Configuration Management* section.



- In the *Load Named Configuration* window, select **Baseline-Configuration** from the *Name* drop-down box. Click **OK**.



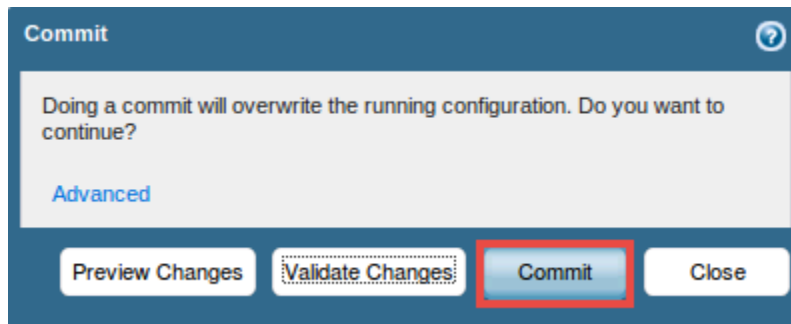
- Notice the configuration is loaded, click **Close** to continue.



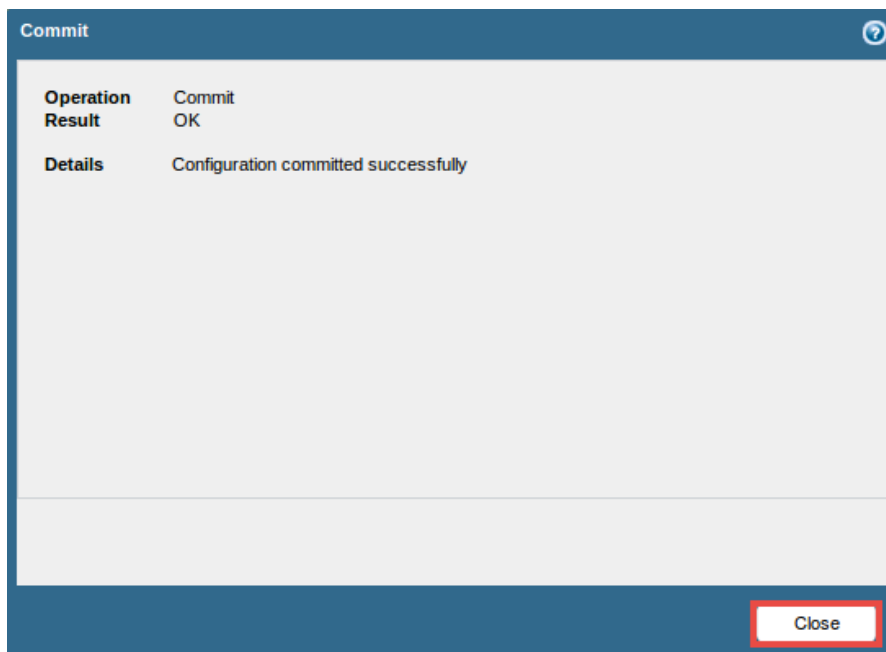
9. Click on the **Commit** link located at the top-right of the *WebUI*.



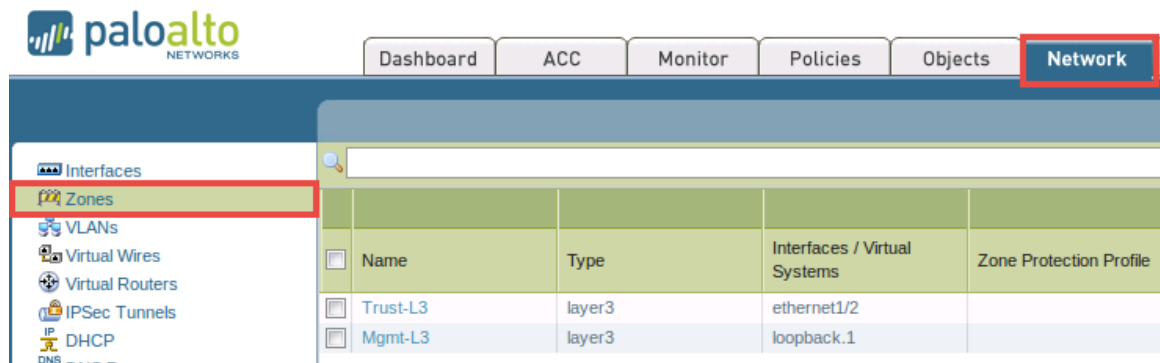
10. In the *Commit* window, click **Commit** to proceed with committing the changes.



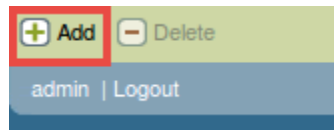
11. Once the operation successfully completes, click **Close** to continue.



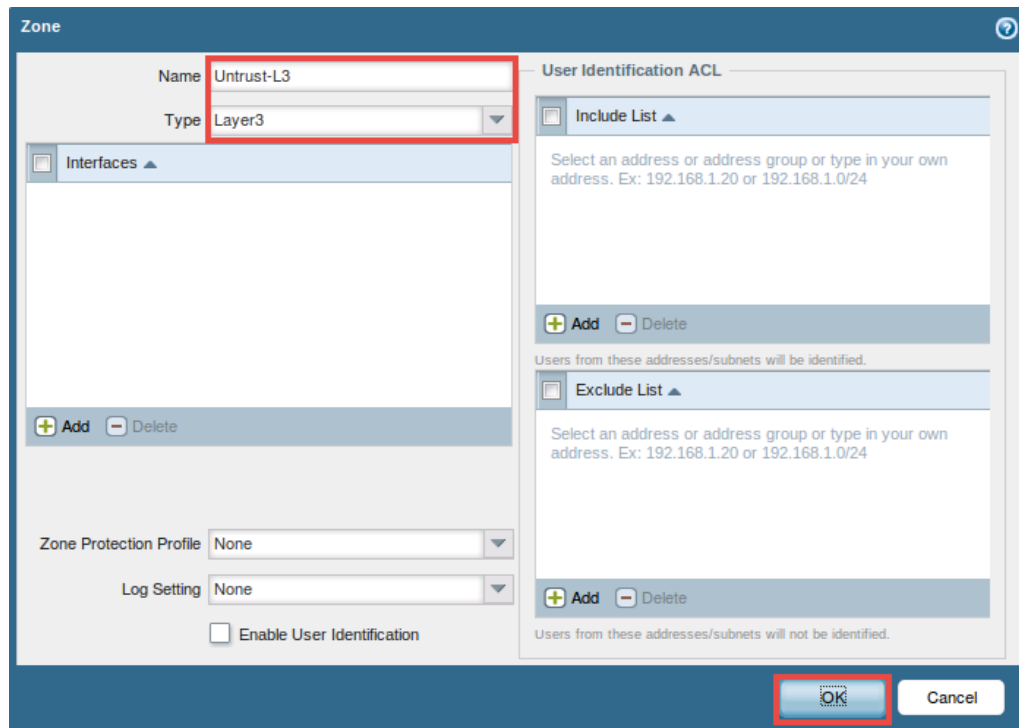
12. Using the *WebUI*, navigate to **Network > Zones**. Notice that a *Trust-L3* and a *Mgmt-L3* zone have been created.



13. Click on **Add**, located near the bottom portion of the window, to create a new zone.



14. In the *Zone* window, type **Untrust-L3** in the *Name* text field.
 15. Leave the default *Type* to **Layer3** and click **OK**.



16. Leave the *Palo Alto WebUI* open for the next task.

2 Create Interface Management Profiles

1. Using the *WebUI*, navigate to **Network > Network Profiles > Interface Mgmt.**

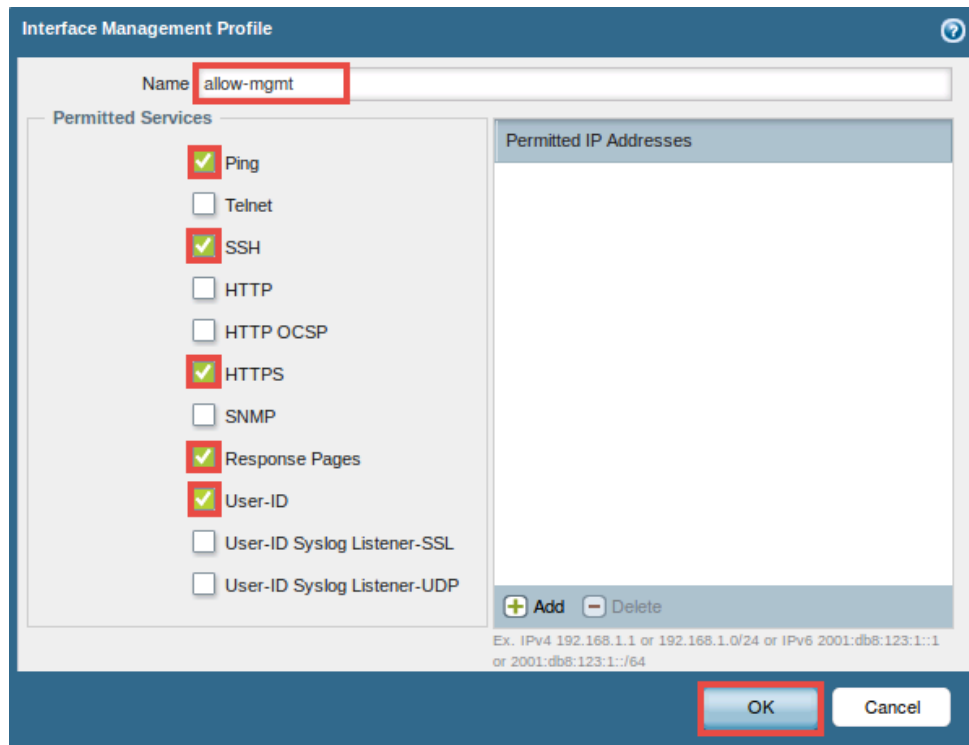


2. Click on the **allow-mgmt** profile link.

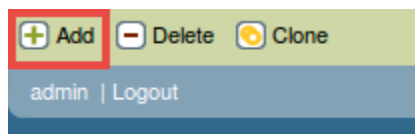
<input type="checkbox"/>	Name	Ping	Telnet	SSH
<input checked="" type="checkbox"/>	allow-mgmt	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

3. In the *Interface Management Profile* window, verify that the items listed in the table below are checked or entered properly.

Field	Data/Selection
Name	Enter allow-mgt
Permitted Services	Check Ping, SSH, HTTPS, Response Pages and User-ID
Permitted IP Addresses	Do not add any addresses

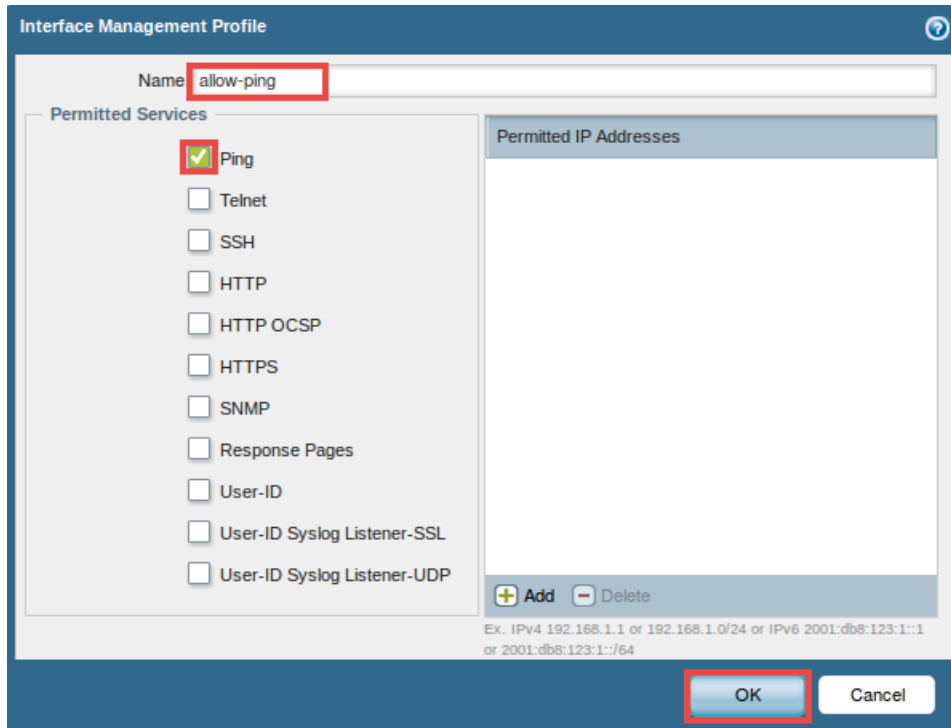


4. Click **OK** to continue.
5. Click on **Add**, located near the bottom of the window, to create another *Interface Management Profile*.



6. Use the information in the table below to fill the form.

Field	Data/Selection
<i>Name</i>	Enter allow-ping
<i>Permitted Services</i>	Check Ping only
<i>Permitted IP Addresses</i>	Do not add any addresses

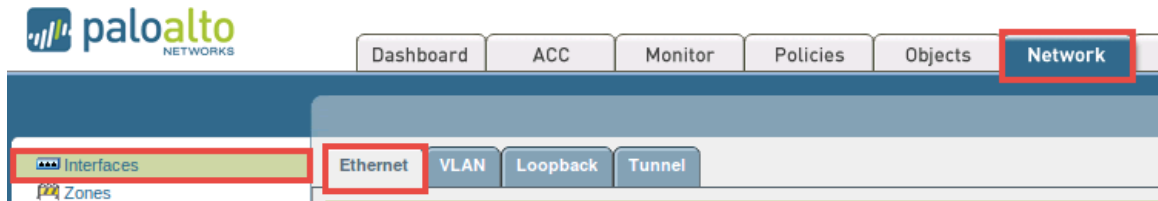


The screenshot shows the 'Interface Management Profile' configuration window. The 'Name' field is set to 'allow-ping'. Under 'Permitted Services', the 'Ping' checkbox is checked, while all other services (Telnet, SSH, HTTP, HTTP OCSP, HTTPS, SNMP, Response Pages, User-ID, User-ID Syslog Listener-SSL, and User-ID Syslog Listener-UDP) are unchecked. The 'Permitted IP Addresses' list is empty. At the bottom right, the 'OK' button is highlighted with a red box. Below the IP address list, there are 'Add' and 'Delete' buttons, and a small text example: 'Ex. IPv4 192.168.1.1 or 192.168.1.0/24 or IPv6 2001:db8:123:1::1 or 2001:db8:123:1::/64'.

7. Click **OK** to continue.
8. Leave the *Palo Alto WebUI* open for the next task.

3 Configure Ethernet Interfaces with Layer 3 Info

1. Using the *WebUI*, navigate to **Network > Interfaces > Ethernet**.

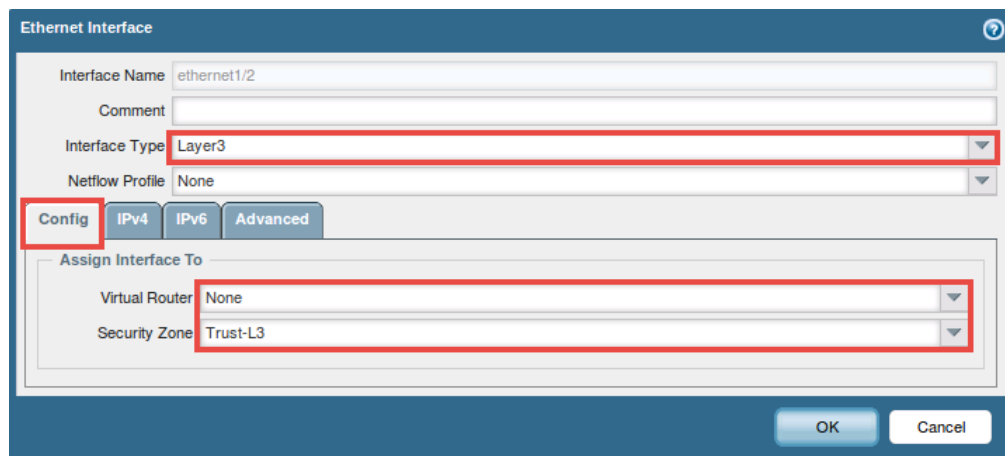


2. Click on the interface **Ethernet1/2** from the list.

Interface	Interface Type	Management Profile
ethernet1/1		
ethernet1/2	Layer3	allow-mgmt
ethernet1/3		
ethernet1/4		
ethernet1/5		
ethernet1/6		
ethernet1/7		
ethernet1/8		
ethernet1/9		

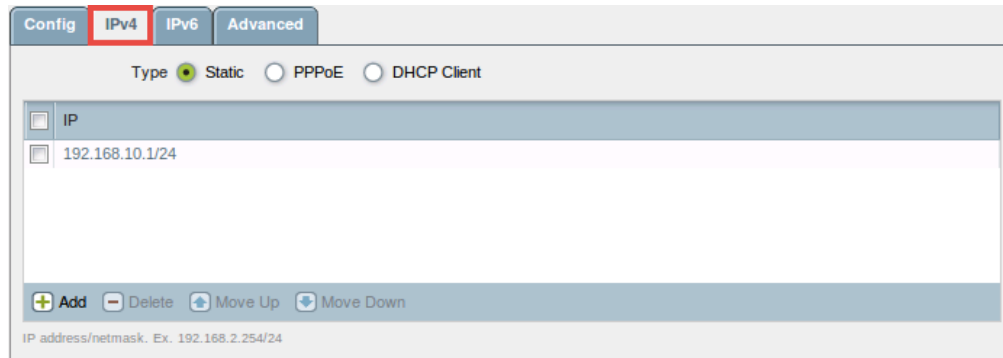
3. In the *Ethernet Interface* window, verify that the items listed in the table below are checked or entered properly.

Field	Data/Selection
Interface Type	Select Layer 3
Config Tab	
Virtual Router	Select None
Security Zone	Select Trust-L3

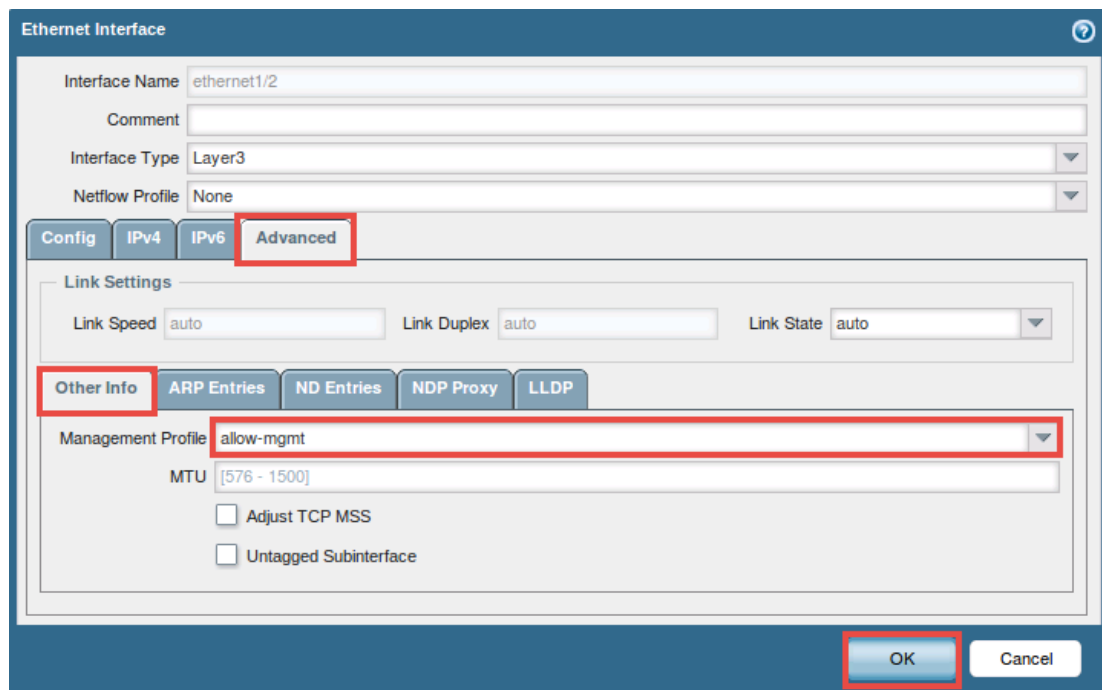


4. While focused on the same window, click on the **IPv4** tab. Use the table below to verify that the configurations match the table below.











Field	Data/Selection
Type	Static
IP	192.168.10.1/24



5. Click on the **Advanced** tab.
6. Verify that the **Other Info** tab is selected, while viewing the *Advanced* tab and select **allow-mgmt** from the *Management Profile* drop-down menu. Click **OK** to save changes and to close the *Ethernet Interface* window.

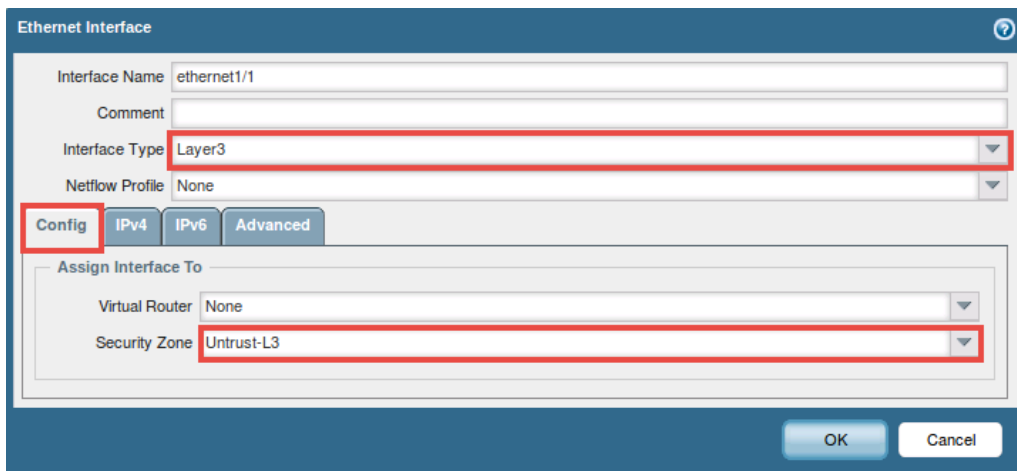


7. Click on the **Ethernet1/1** interface from the list of available interfaces.

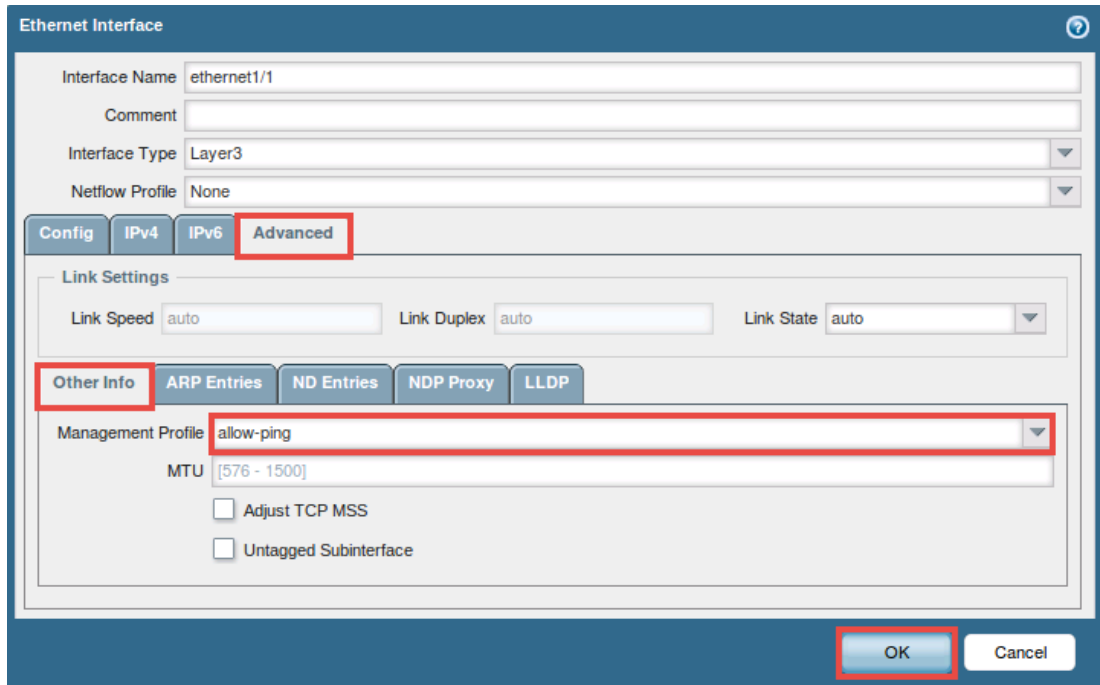
Interface	Interface Type	Management Profile	Link State	IP Address
 ethernet1/1				none
 ethernet1/2	Layer3	allow-mgmt		192.168.10.1/24
 ethernet1/3				none
 ethernet1/4				none
 ethernet1/5				none

8. In the *Ethernet Interface* window, use the table below to configure *Ethernet1/1*.

Field	Data/Selection
<i>Interface Type</i>	Layer3
Config Tab	
<i>Security Zone</i>	Untrust-L3



9. Click on the **IPv4** tab and select the radio button for **DHCP Client**.
10. Click on the **Advanced** tab, followed by clicking the **Other Info** tab, and select **allow-ping** from the drop-down menu for *Management Profile*.



Ethernet Interface

Interface Name: ethernet1/1

Comment:

Interface Type: Layer3

Netflow Profile: None

Config **IPv4** **IPv6** **Advanced**

Link Settings

Link Speed: auto Link Duplex: auto Link State: auto

Other Info **ARP Entries** **ND Entries** **NDP Proxy** **LLDP**

Management Profile: allow-ping

MTU: [576 - 1500]

☐ Adjust TCP MSS

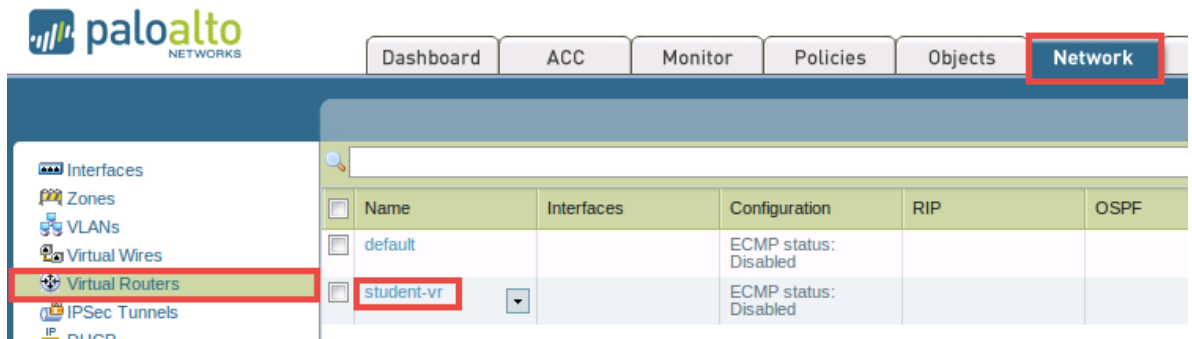
☐ Untagged Subinterface

OK Cancel

11. Click **OK** to save changes and to close the *Ethernet Interface* window.
12. Leave the *Palo Alto WebUI* open for the next task.

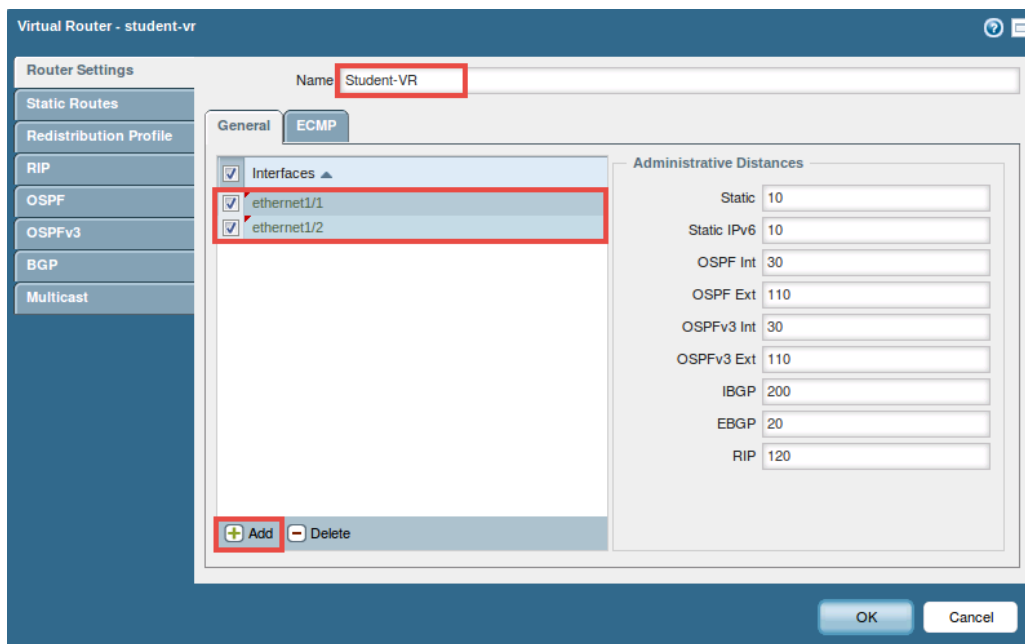
4 Create a Virtual Router

1. Using the *WebUI*, navigate to **Network > Virtual Routers** followed by clicking on the **student-vr** router from the list.



2. In the *Virtual Router – student-vr* window, use the information from the table below for configuration of the virtual router.

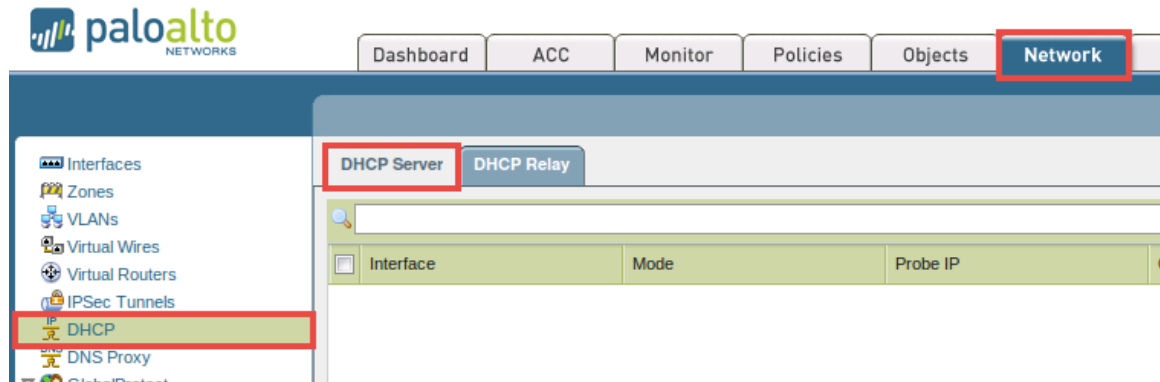
Field	Data/Selection
Name	Enter Student-VR
Interfaces	Click Add then select Ethernet1/1 Click Add again and select Ethernet1/2



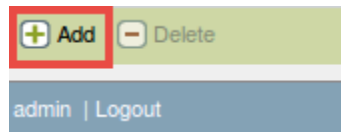
3. Click **OK** to save changes and to close the *Virtual Router Configuration* window.
4. Leave the *Palo Alto WebUI* open for the next task.

5 Configure DHCP

1. Using the *WebUI*, navigate to **Network > DHCP > DHCP Server**.

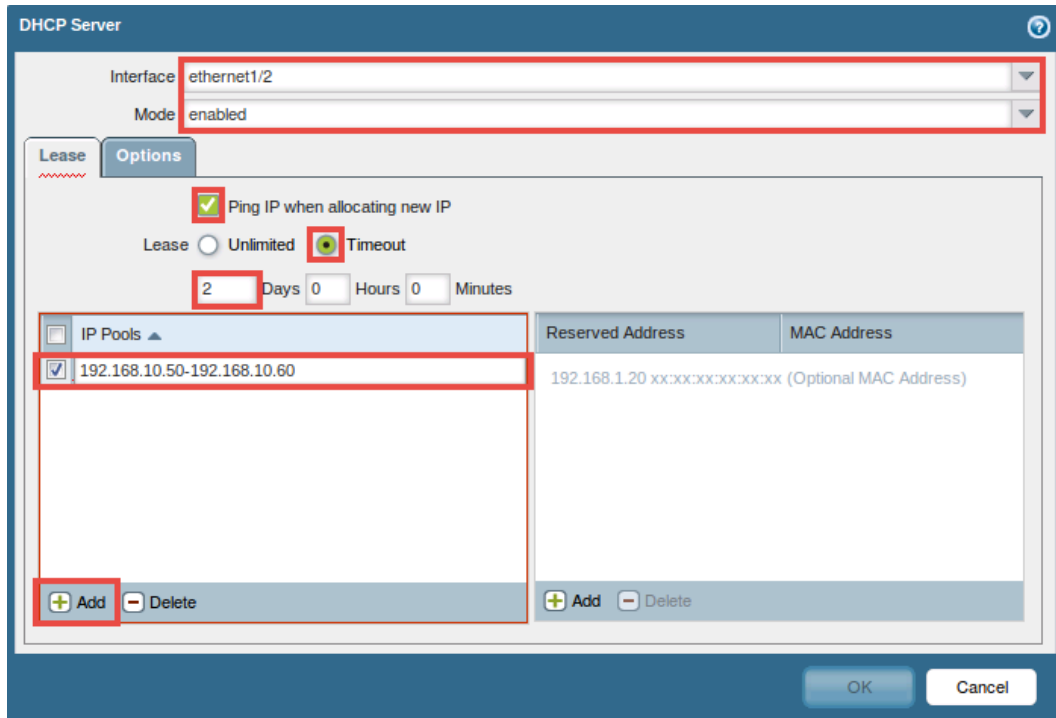


2. Click on **Add**, located near the bottom of the window, to define a new DHCP server.



3. In the DHCP Server window, use the information in the table below to configure the DHCP server.

Field	Data/Selection
<i>Interface</i>	ethernet1/2
<i>Mode</i>	enabled
<i>Ping IP when allocating new IP</i>	Check
<i>Lease</i>	Select Timeout 2 Days 0 Hours 0 Minutes
<i>IP Pools</i>	Click Add then enter 192.168.10.50–192.168.10.60



DHCP Server

Interface: ethernet1/2
Mode: enabled

Lease | Options

☒ Ping IP when allocating new IP

Lease: ☐ Unlimited ☒ Timeout

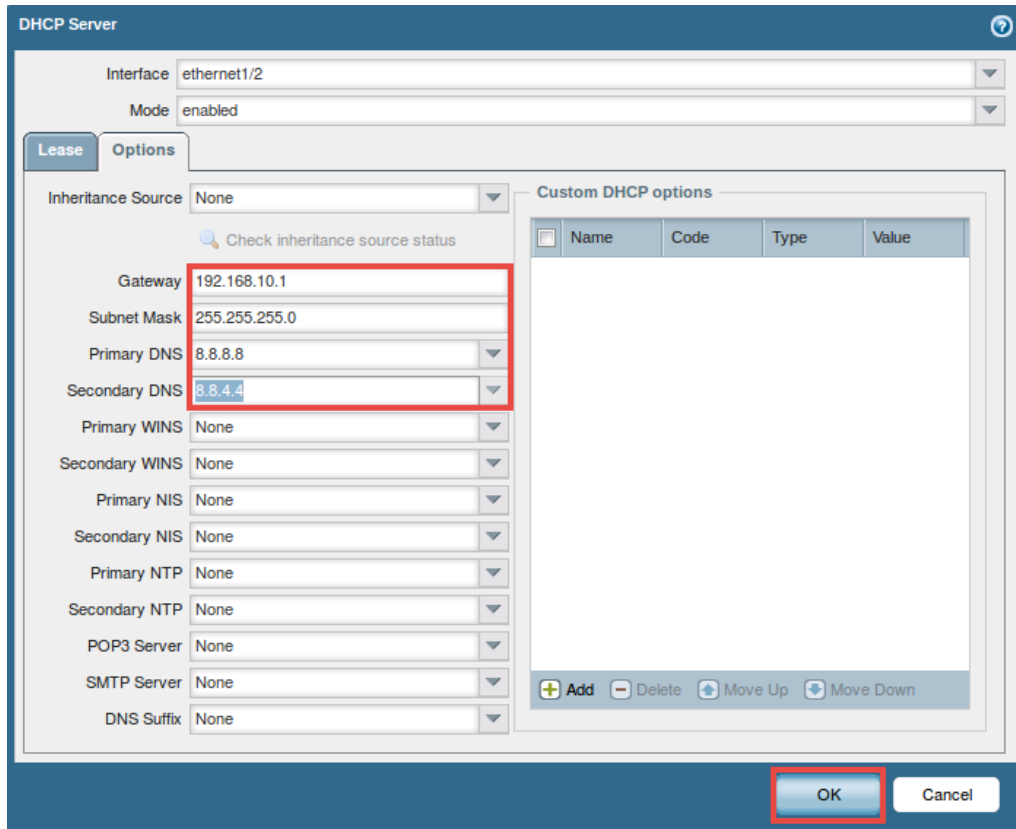
2 Days 0 Hours 0 Minutes

IP Pools	Reserved Address	MAC Address
<input checked="" type="checkbox"/> 192.168.10.50-192.168.10.60	192.168.1.20	xx:xx:xx:xx:xx:xx (Optional MAC Address)

OK Cancel

4. Click the **Options** tab.
5. Use the following information in the table below to fill the form fields.

Field	Data/Selection
Gateway	192.168.10.1
Subnet Mask	255.255.255.0
Primary DNS	8.8.8.8
Secondary DNS	8.8.4.4

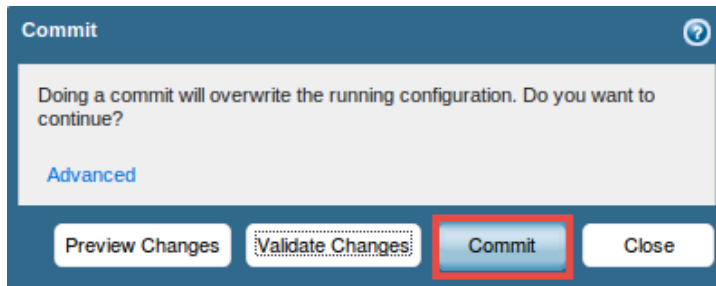


The image shows the 'DHCP Server' configuration window. The 'Interface' is set to 'ethernet1/2' and the 'Mode' is 'enabled'. The 'Lease' tab is selected. The 'Inheritance Source' is 'None'. A red box highlights the 'Gateway' field with the value '192.168.10.1', the 'Subnet Mask' field with '255.255.255.0', the 'Primary DNS' field with '8.8.8.8', and the 'Secondary DNS' field with '8.8.4.4'. The 'Custom DHCP options' table is empty. The 'OK' button is highlighted with a red box.

6. Click **OK** to submit the form.
7. Click the **Commit** link towards the top-right of the *WebUI*.

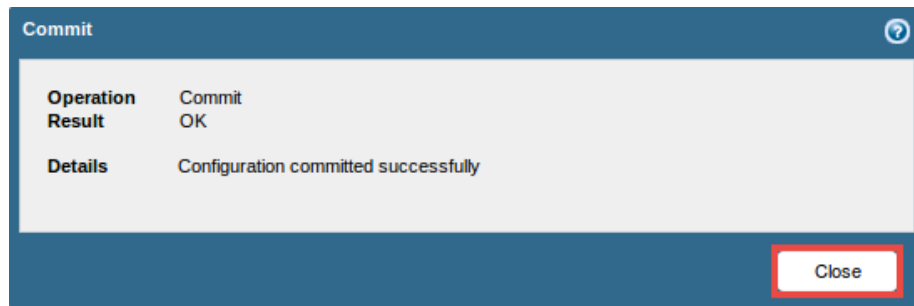


8. In the *Commit* window, click the **Commit** button.

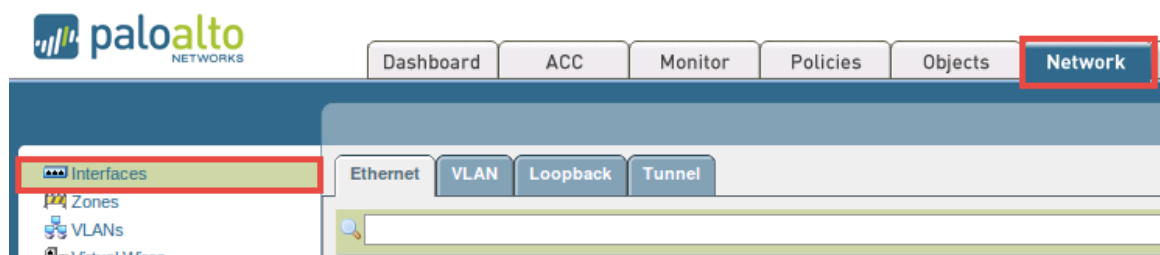


The image shows the 'Commit' confirmation window. It contains the text: 'Doing a commit will overwrite the running configuration. Do you want to continue?'. Below the text is a link labeled 'Advanced'. At the bottom, there are four buttons: 'Preview Changes', 'Validate Changes', 'Commit' (highlighted with a red box), and 'Close'.




9. Wait until the commit process successfully completes, then click **Close**.



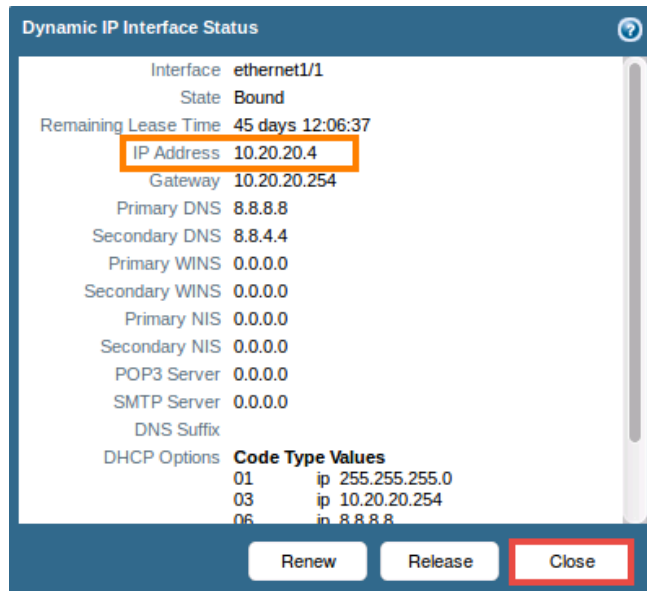
10. Navigate to **Network > Interfaces > Ethernet**.



11. Identify *ethernet1/1*, click on **Dynamic-DHCP Client** from its respective row under the *IP Address* column.

Ethernet				
Ethernet VLAN Loopback Tunnel				
Interface	Interface Type	Management Profile	Link State	IP Address
ethernet1/1	Layer3	allow-ping		Dynamic-DHCP Client
ethernet1/2	Layer3	allow-mgmt		192.168.10.1/24
ethernet1/3				none

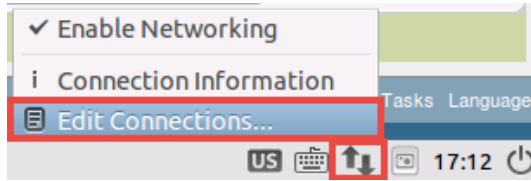
12. Verify that the interface has received an IP address from the ISP. Click **Close** to continue.



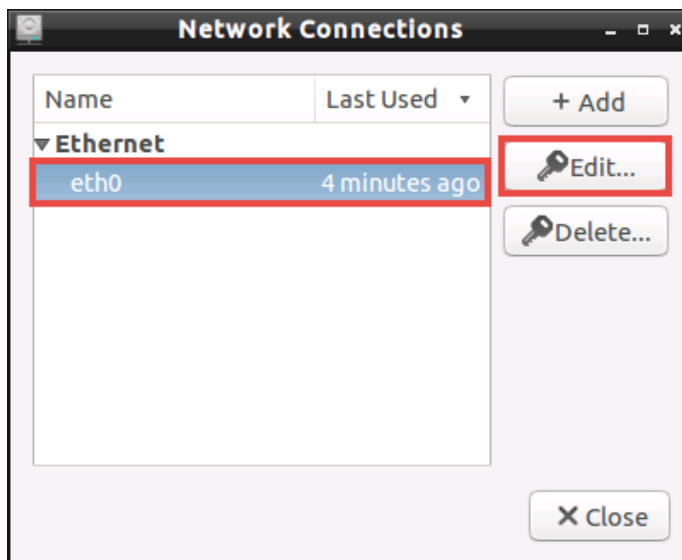
Note that the IP address assigned by DHCP may slightly differ in the fourth octet of the IPV4 address when compared to the screen capture above.

6 Test the DHCP Server

1. In the status bar on *Desktop 1*, right-click on the **network icon** in the lower-right corner and select **Edit Connections**.

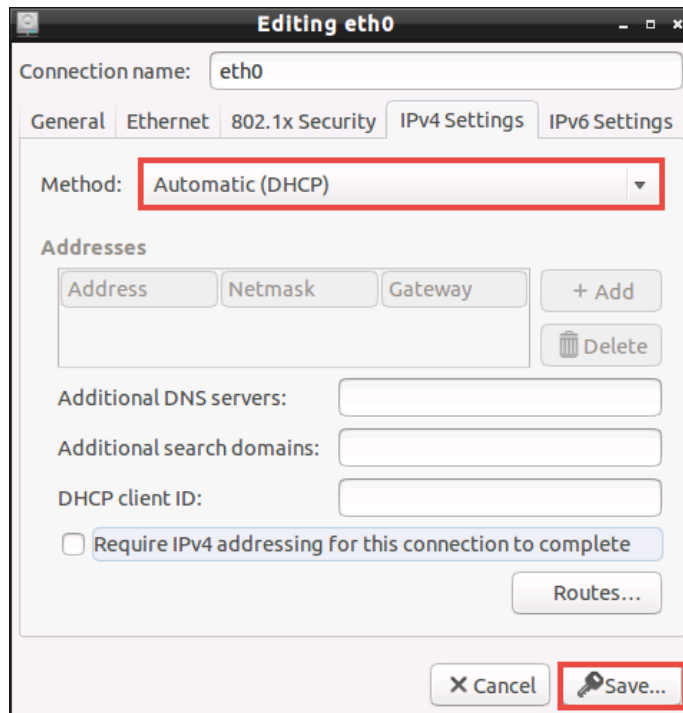


2. In the *Network Connections* window, select **eth0** and click the **Edit** button.

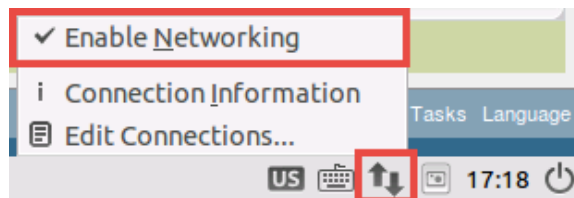


3. Click on the **IPv4 Settings** tab.
4. Change the *Method* to **Automatic (DHCP)**.

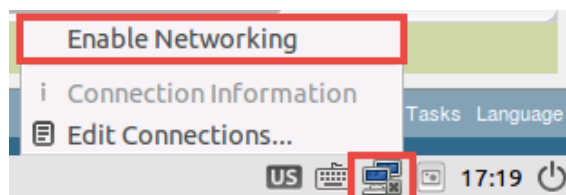
5. Remove the IP addresses in the *Additional DNS servers* field. Click **Save**.



6. In the *Network Connections* window, click **Close** to continue.
7. Right-click on the same **Network icon** in the right corner and select **Enable Networking** to turn networking off.



8. Repeat the process to turn networking back on.



9. Click on the **LX Terminal** icon to open a new terminal window.



10. Using the terminal window, type the command below to verify that a DHCP IP address has been successfully obtained.

```
ifconfig
```

```
sysadmin@ubuntu:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:50:56:9a:a8:29
          inet addr:192.168.10.50  Bcast:192.168.10.255  Mask:255.255.255.0
          inet6 addr: fe80::250:56ff:fe9a:a829/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:5753 errors:0 dropped:10 overruns:0 frame:0
          TX packets:8970 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5989603 (5.9 MB)  TX bytes:1099661 (1.0 MB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:2950 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2950 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:204662 (204.6 KB)  TX bytes:204662 (204.6 KB)
```

Note that the IP address assigned by DHCP may slightly differ in the fourth octet of the IPV4 address when compared to the screen capture above.

11. Verify that there is connectivity between the *Desktop 1* VM and the *Palo Alto* firewall by entering the command below.

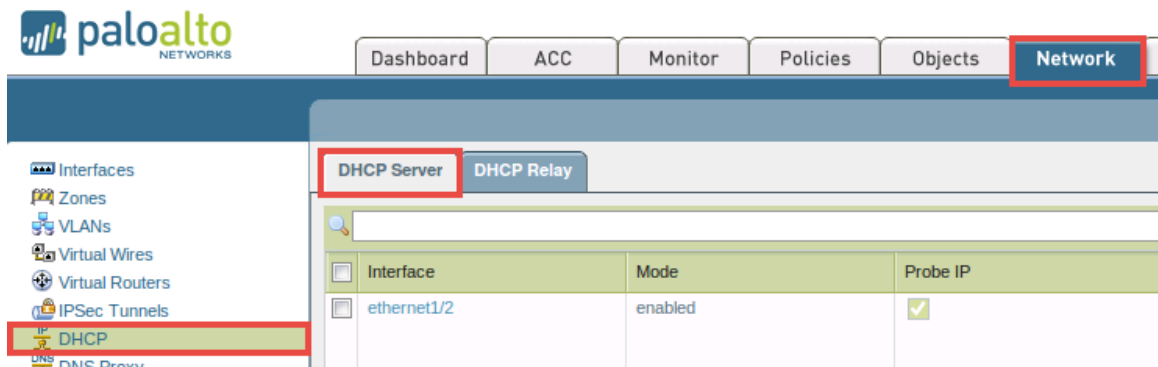
```
ping -c4 192.168.10.1
```

```
sysadmin@ubuntu:~$ ping -c4 192.168.10.1
PING 192.168.10.1 (192.168.10.1) 56(84) bytes of data.
64 bytes from 192.168.10.1: icmp_seq=1 ttl=64 time=10.7 ms
64 bytes from 192.168.10.1: icmp_seq=2 ttl=64 time=0.433 ms
64 bytes from 192.168.10.1: icmp_seq=3 ttl=64 time=0.419 ms
64 bytes from 192.168.10.1: icmp_seq=4 ttl=64 time=0.408 ms

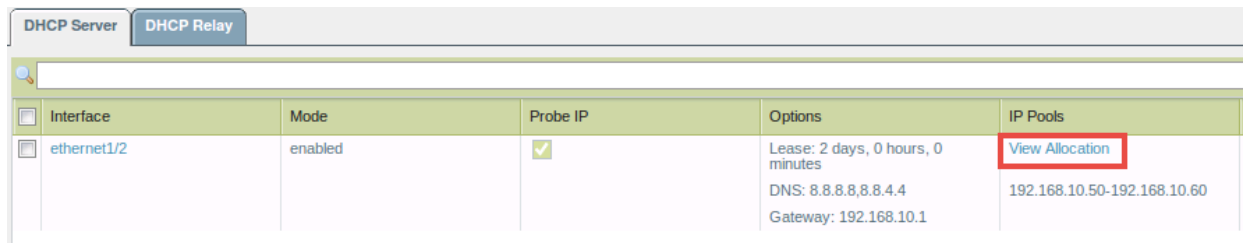
--- 192.168.10.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2999ms
rtt min/avg/max/mdev = 0.408/3.000/10.743/4.470 ms
```

12. After the successful ping attempt, close the **terminal** window.

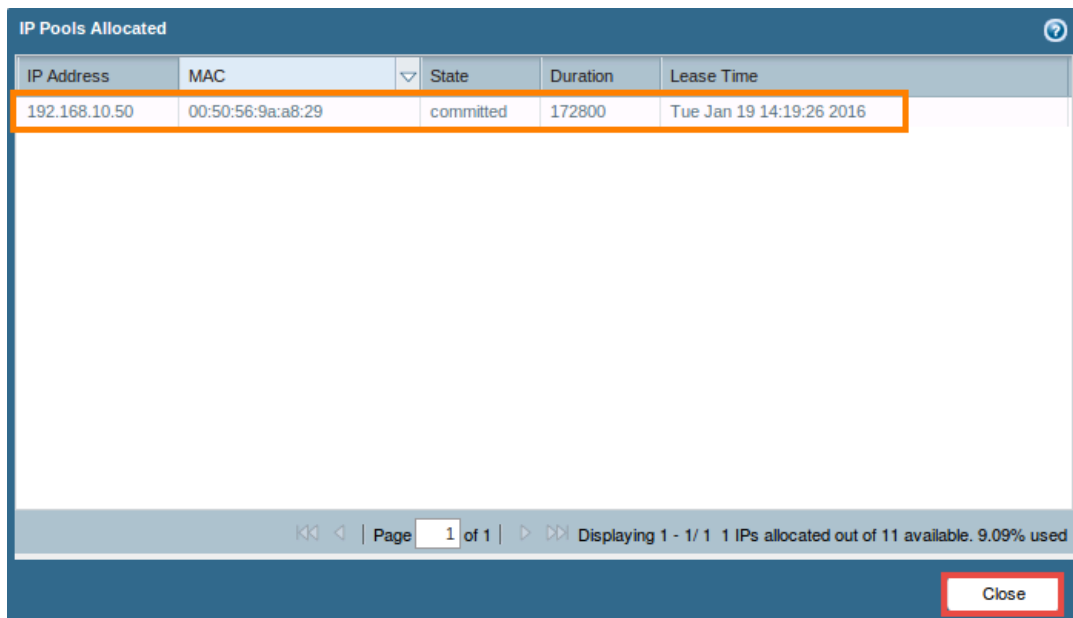
13. Change focus back to the *WebUI* and navigate to **Network > DHCP > DHCP Server**.



14. Click on the **View Allocation** link, underneath the *IP Pools* column, for the *ethernet1/2* entry.



15. In the *IP Pools Allocated* window, notice the leased IP address allocated to the *Desktop 1 VM*. Click **Close**.



16. Close the **Desktop 1 PC** viewer.