NETWORK SECURITY FUNDAMENTALS V2

Lab 1: Configuring DHCP

Document Version: 2022-12-23

Contents

Introduction

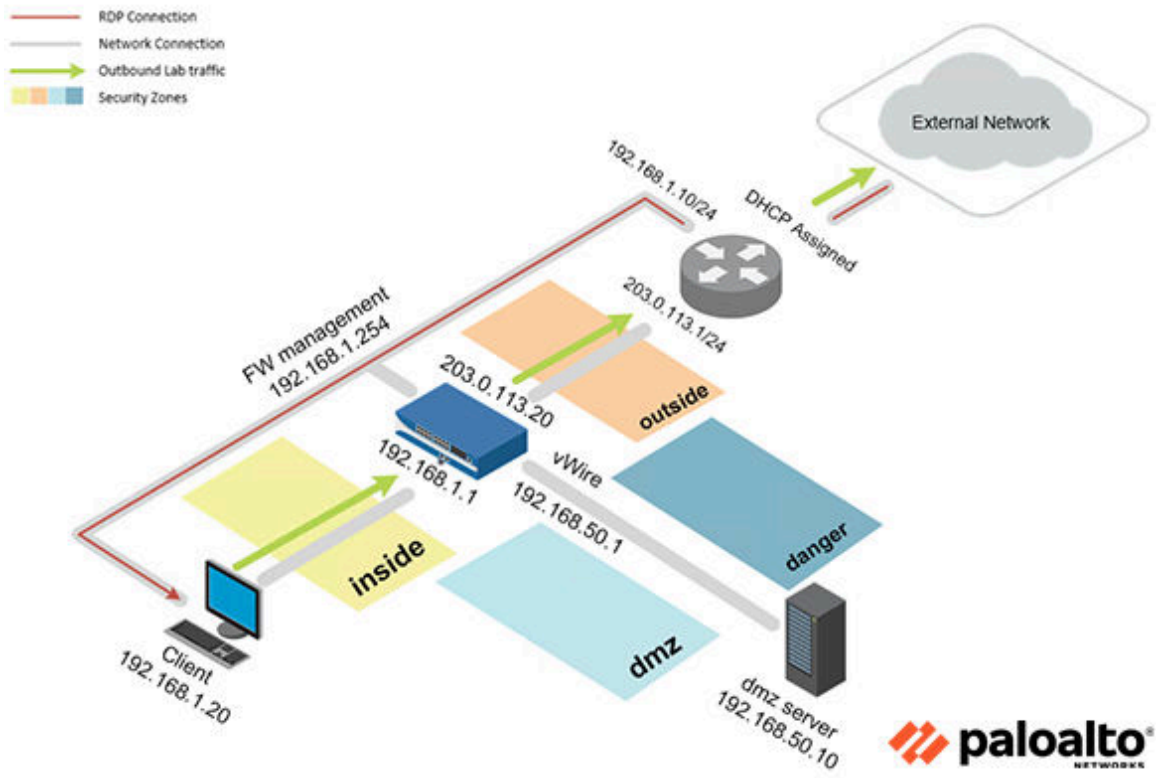
In this lab, you will configure the Palo Alto Networks Firewall as a DHCP server. You will then test the DHCP server with the Client PC.

Objective

In this lab, you will perform the following tasks:

- Configure DHCP Server
- Configure Client for DHCP
- Configure a DHCP Client Reservation
- Configure the Firewall Outside Interface for DHCP

Lab 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.

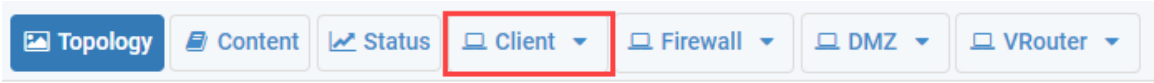
Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Client	192.168.1.20	`lab-user`	`Pal0Alt0!`
DMZ	192.168.50.10	`root`	`Pal0Alt0!`
Firewall	192.168.1.254	`admin`	`Pal0Alt0!`

1 Configuring DHCP

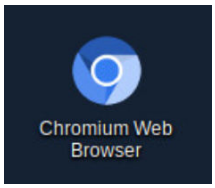
1.0 Load Lab Configuration

In this section, you will load the Firewall configuration file.

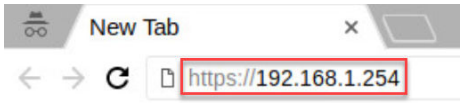
1. Click on the **Client** tab to access the Client PC.



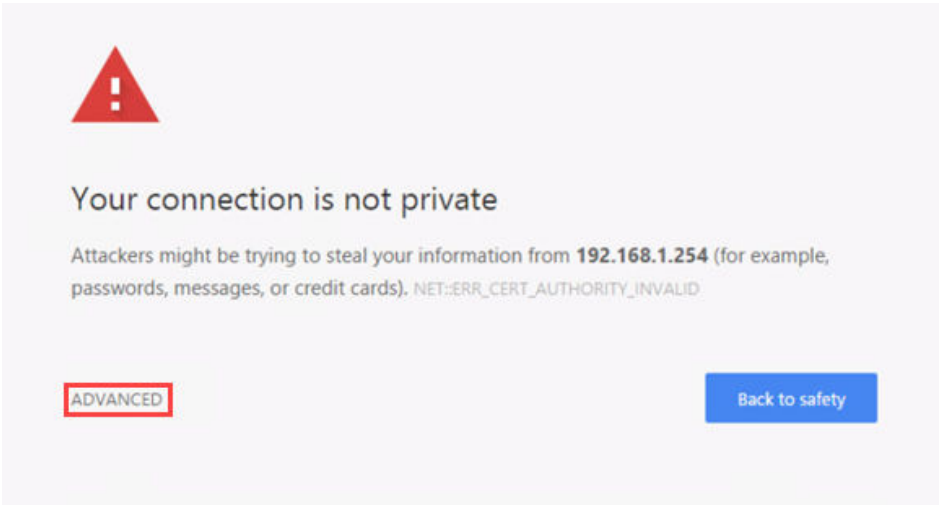
2. Log in to the Client PC as username `lab-user`, password `Pal0Alt0!`.
3. Double-click the **Chromium Web Browser** icon located on the Desktop.



4. In the *Chromium* address field, type `https://192.168.1.254` and press **Enter**.

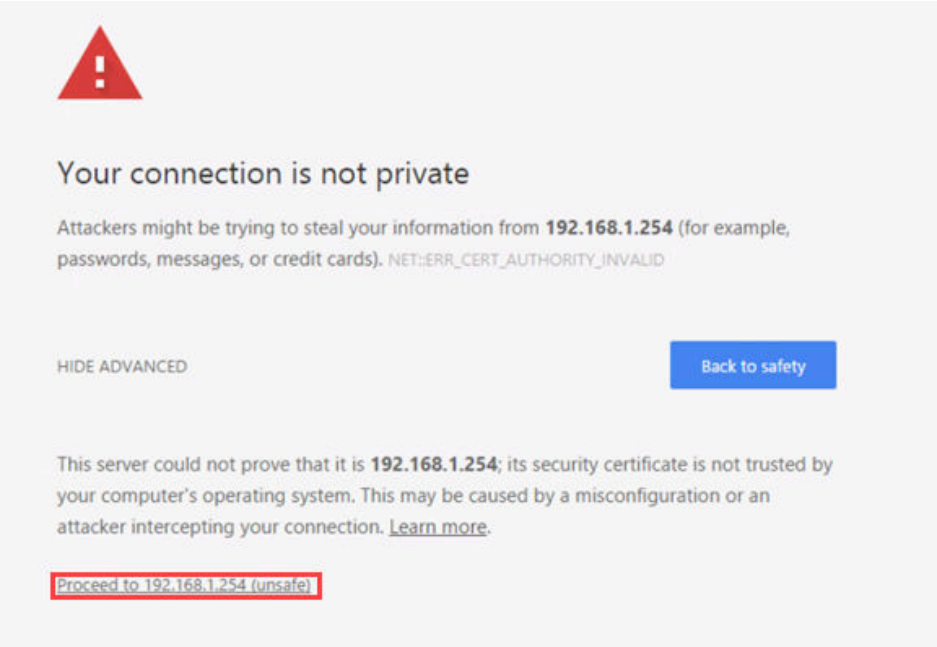


5. You will see a "*Your connection is not private*" message. Click on the **ADVANCED** link.



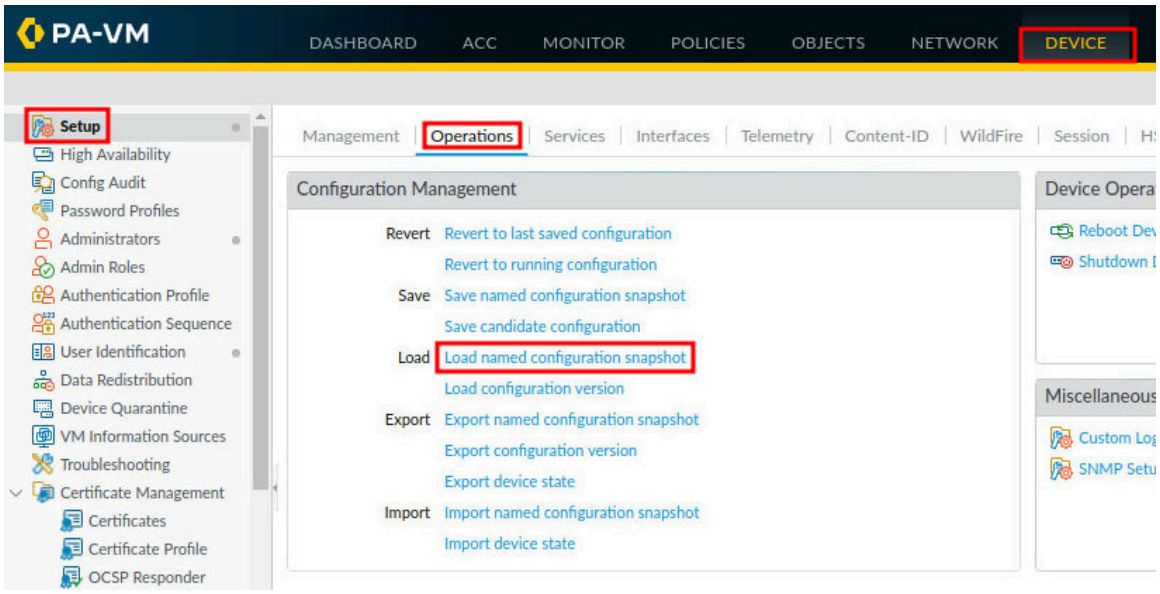
If you experience the "Unable to connect" or "502 Bad Gateway" message while attempting to connect to the specified IP above, please wait an additional 1-3 minutes for the Firewall to fully initialize. Refresh the page to continue.

6. Click on **Proceed to 192.168.1.254 (unsafe)**.

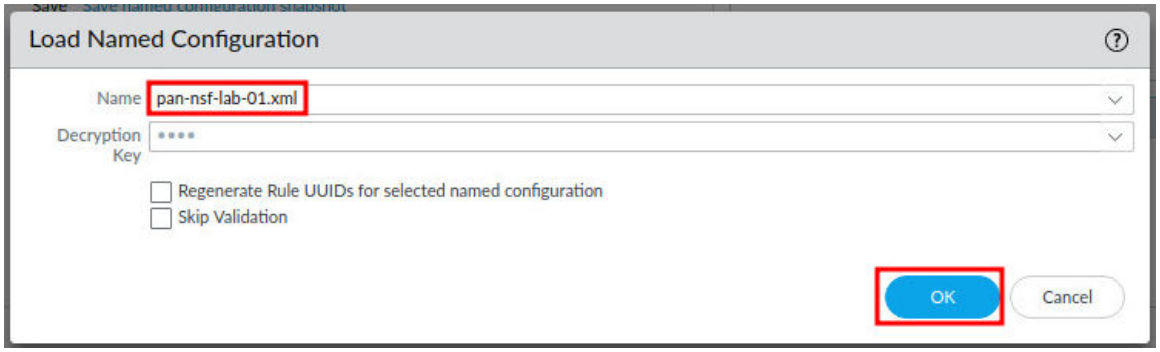


7. Log in to the Firewall web interface as username `admin`, password `Pal0Alt0!`.

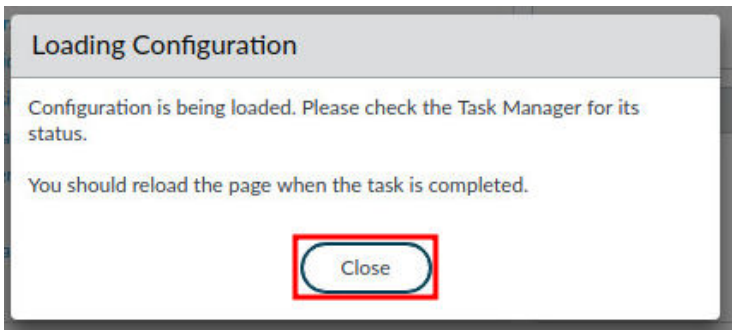
8. In the web interface, navigate to **Device > Setup > Operations** and click on **Load named configuration snapshot** underneath the *Configuration Management* section.



9. In the *Load Named Configuration* window, select **pan-nsf-lab-01.xml** from the *Name* dropdown box and click **OK**.

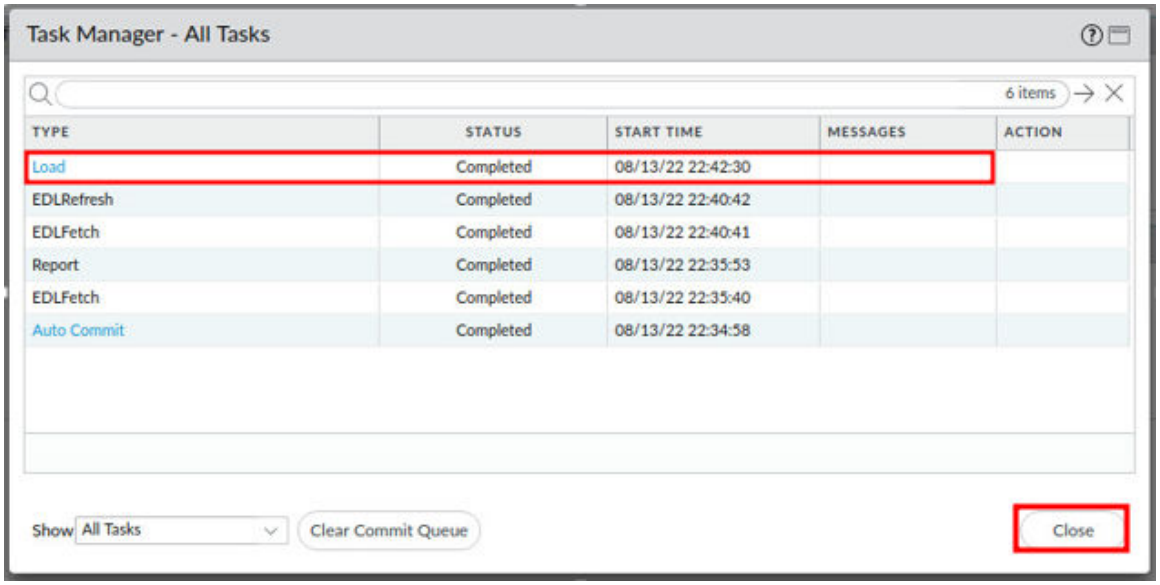


10. In the *Loading Configuration* window, a message will show *Configuration is being loaded. Please check the Task Manager for its status. You should reload the page when the task is completed.* Click **Close** to continue.

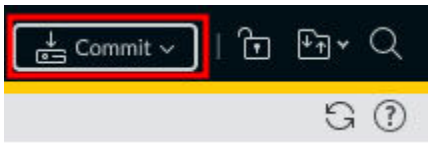


11. Click the **Tasks** icon located at the bottom-right of the web interface.

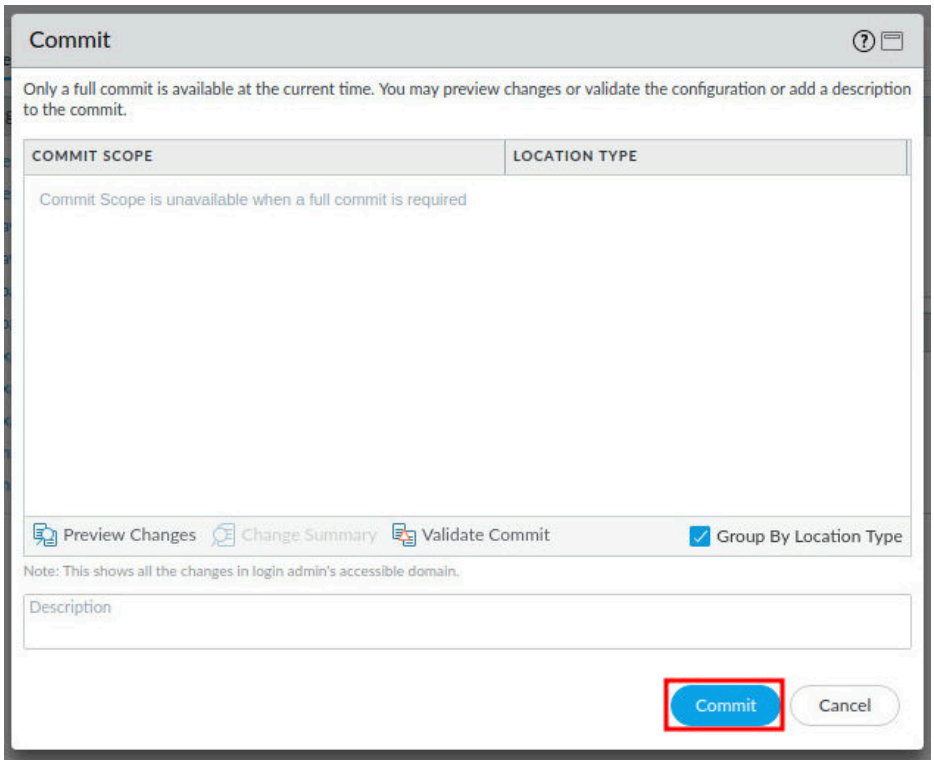
12. In the *Task Manager – All Tasks* window, verify the *Load* type has successfully completed. Click **Close.**



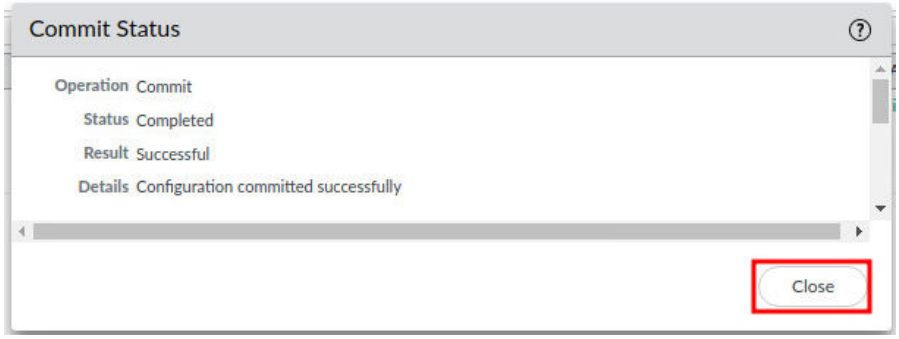
13. Click the **Commit** link located at the top-right of the web interface.



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



15. When the commit operation successfully completes, click **Close** to continue.

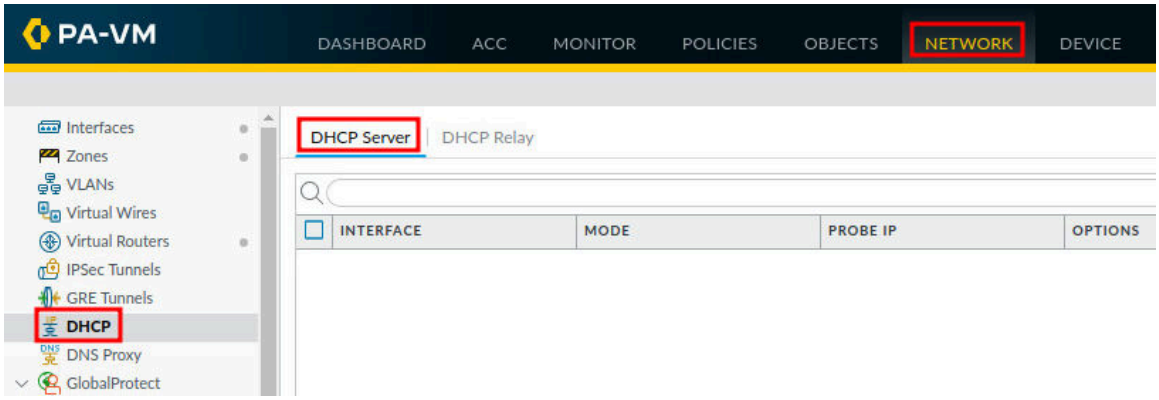


The commit process takes changes made to the Firewall and copies them to the running configuration, which will activate all configuration changes since the last commit.

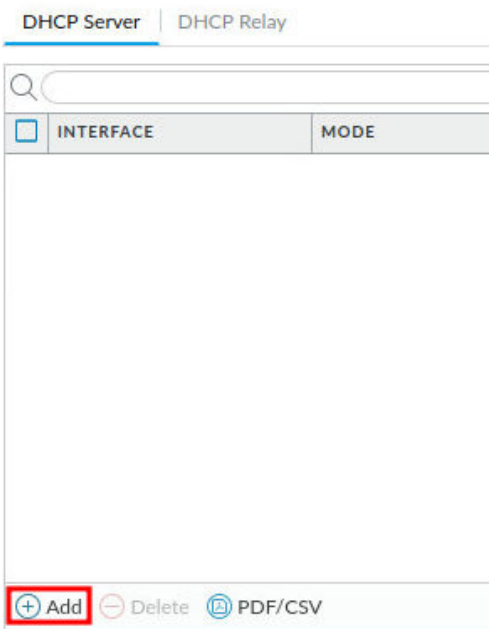
1.1 Configure DHCP Server

In this section, you will configure a DHCP Server on the Firewall. By adding a DHCP server to the Firewall, clients behind the Firewall will not have to configure IP addresses manually. A client that is configured for DHCP and connected to the same network as the Firewall will receive an IP address automatically, reducing network configuration errors.

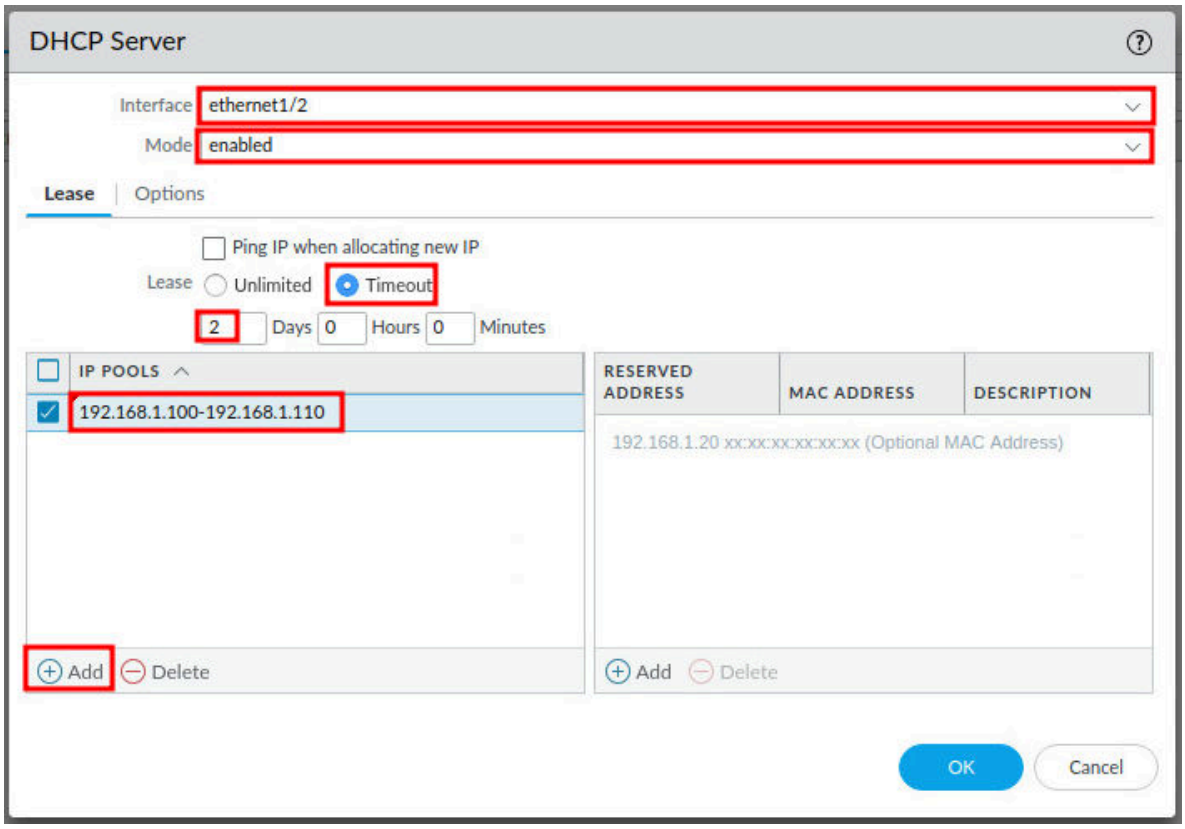
1. Navigate to **Network > DHCP > DHCP Server.**



2. Click on **Add**, located near the bottom-left of the *DHCP Server* box.

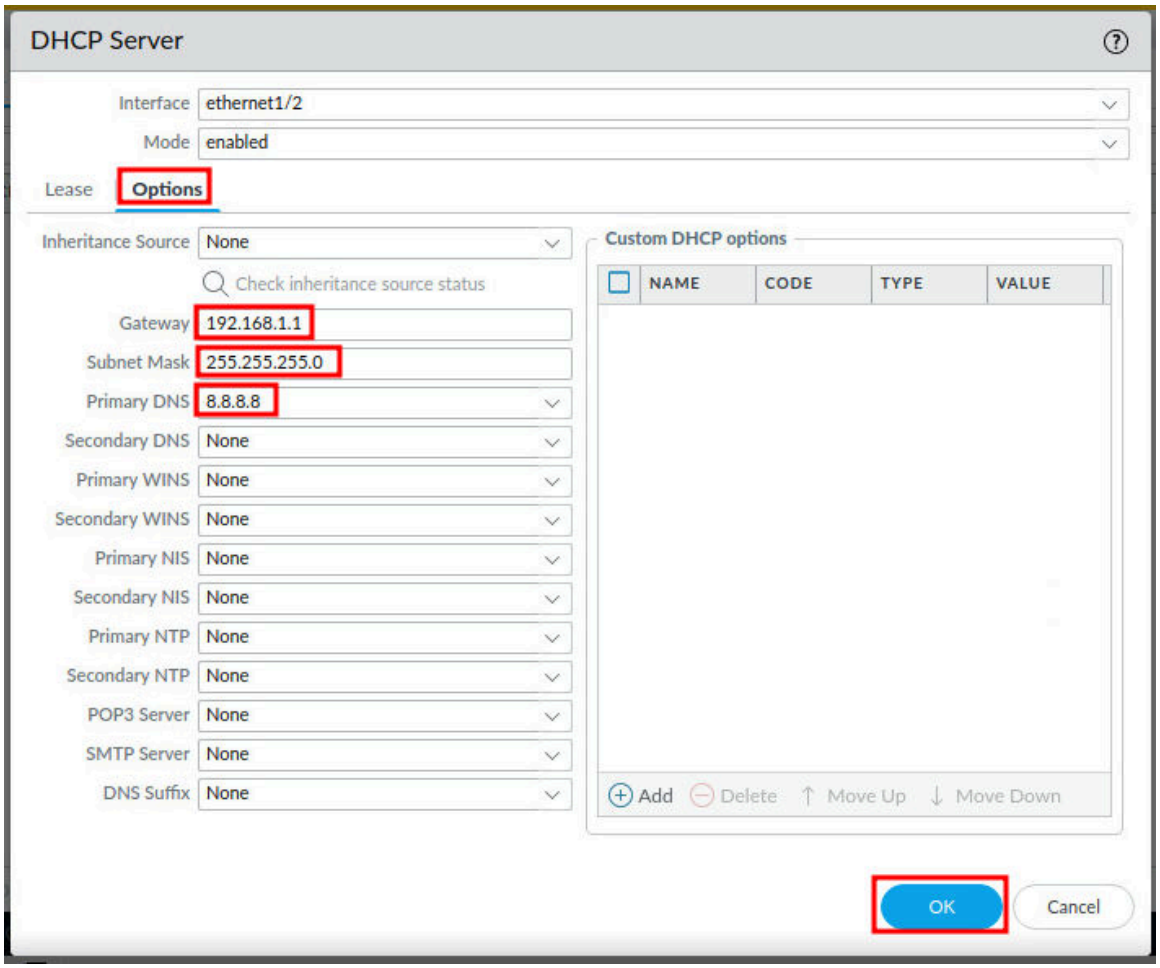


3. In the *DHCP Server* window, select **ethernet1/2** for the *Interface* dropdown. Next, in the *Mode* dropdown, select **enabled**. Then, in the *Lease* radio button, select **Timeout** and give it a value of **2** days. Finally, in the *IP Pools*, click the **Add** button at the bottom-left of the *IP Pools* section and enter `192.168.1.100`–`192.168.1.110`.



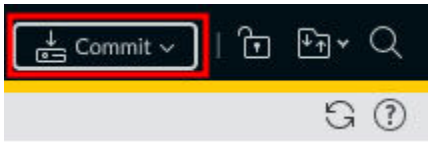
ethernet1/2 is selected to run DHCP because this is the network that the Client is connected to. In this configuration, the Client will receive an IP address automatically. By specifying a 2-day timeout, the client will need to request a new IP address every 2 days. The IP Pool created will limit the number of IP addresses that the firewall will automatically distribute.

4. Click on the **Options** tab and type `192.168.1.1` in the *Gateway* field, `255.255.255.0` in the *Subnet Mask* field, and type `8.8.8.8` in the *Primary DNS* field.

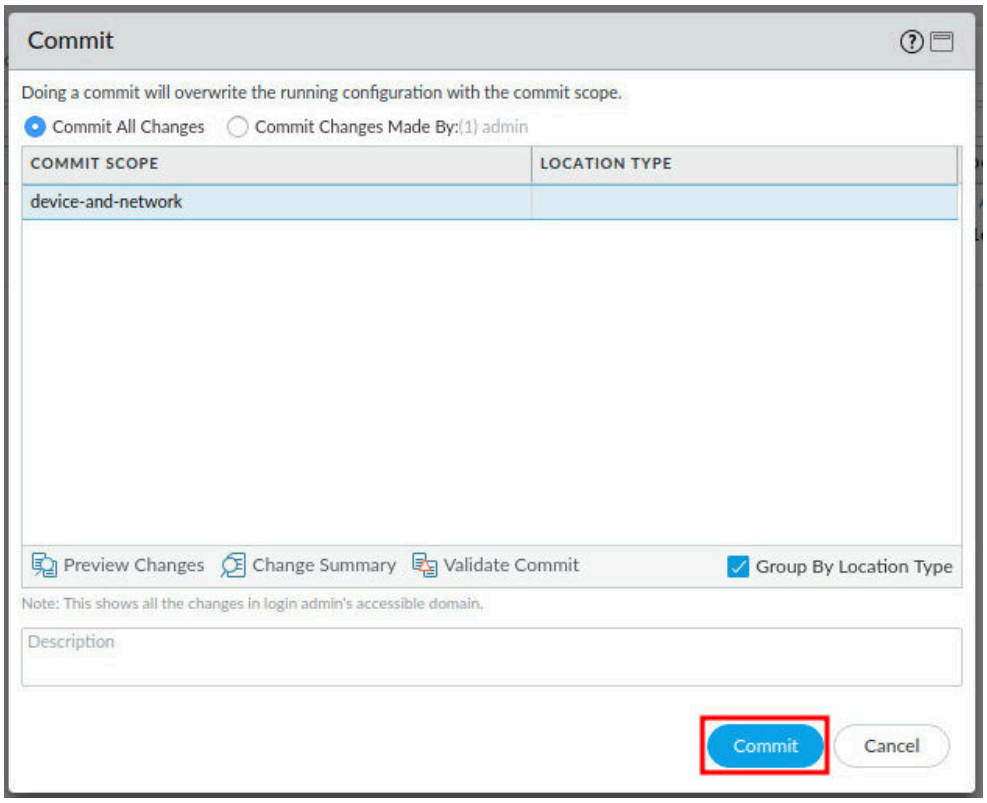


The Gateway of 192.168.1.1 is the interface for the Firewall. DHCP will send this to the Client so that the Client will have a default gateway. The Primary DNS server, 8.8.8.8, is one of Google's public DNS servers. DHCP will also send this information to the Client so that the Client will have a DNS server.

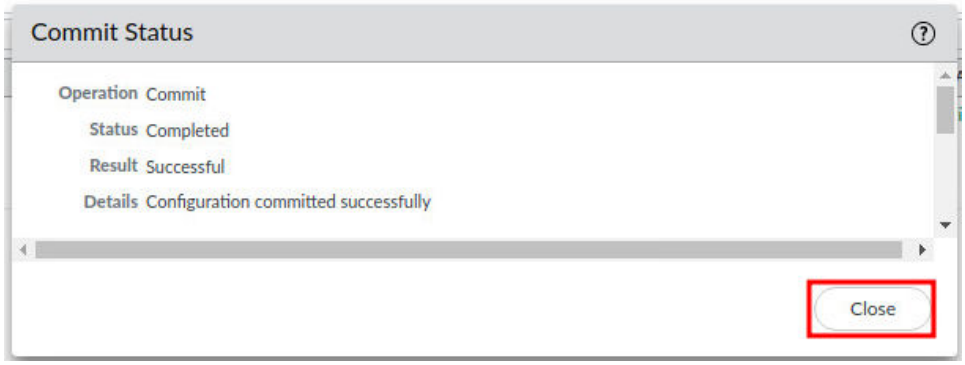
5. Click the **OK** button on the *DHCP Server* window.
6. Click the **Commit** link located at the top-right of the web interface.



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



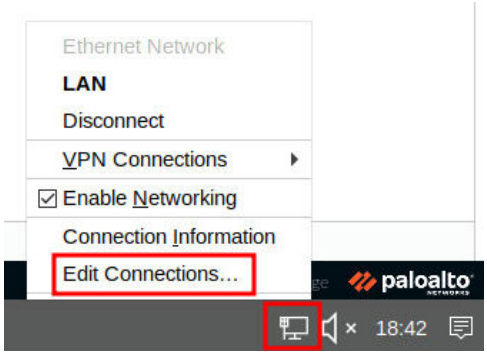
8. When the commit operation successfully completes, click **Close** to continue.



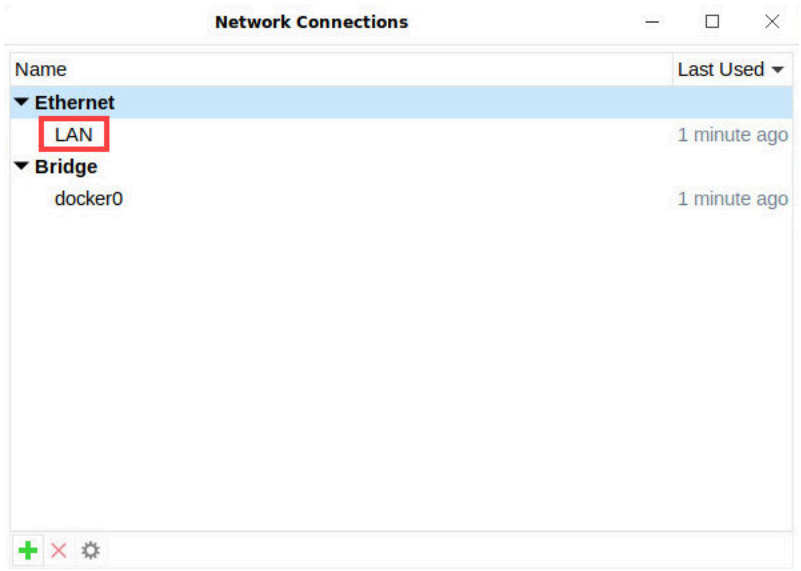
1.2 Configure Client for DHCP

In this section, you will confirm the current configuration of the Client. Then, you will configure the client for DHCP and confirm a Dynamic IP address was assigned.

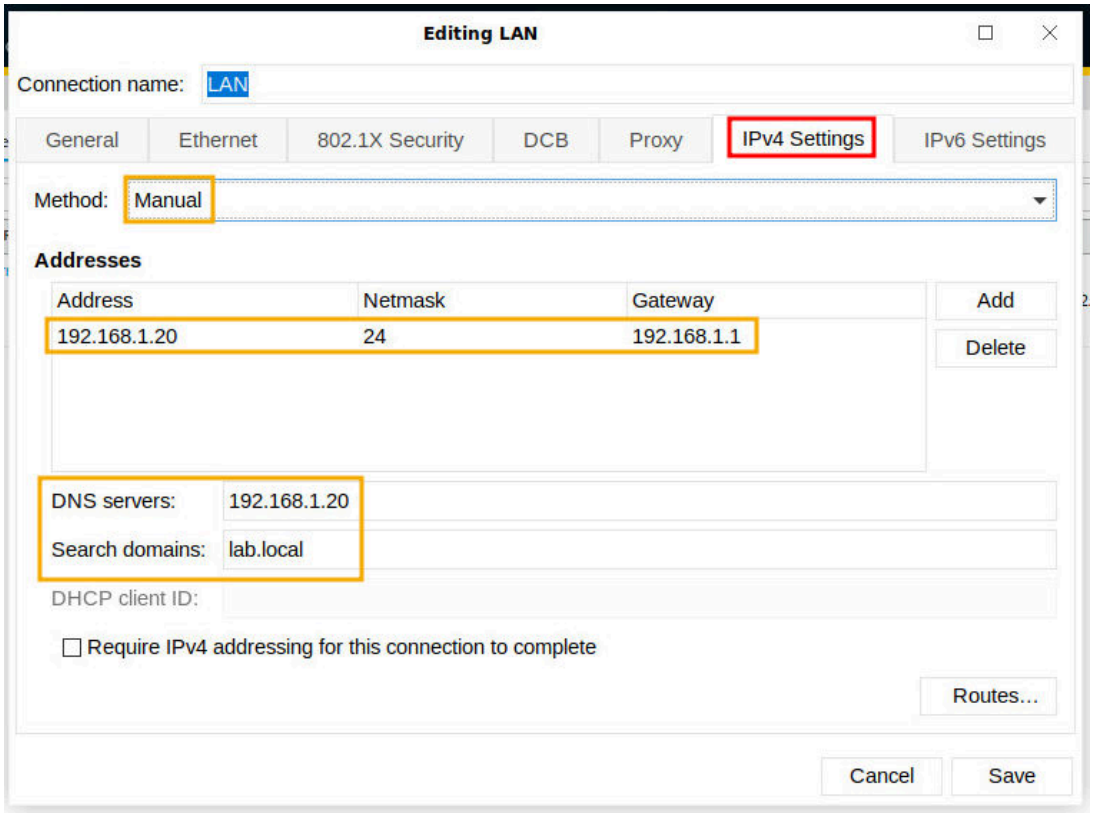
1. Click on the **Connection** icon in the lower-right of the web *Client*. Next, click on **Edit Connections**.



2. In the *Network Connections* window, under the *Ethernet* dropdown list, double-click **LAN**.

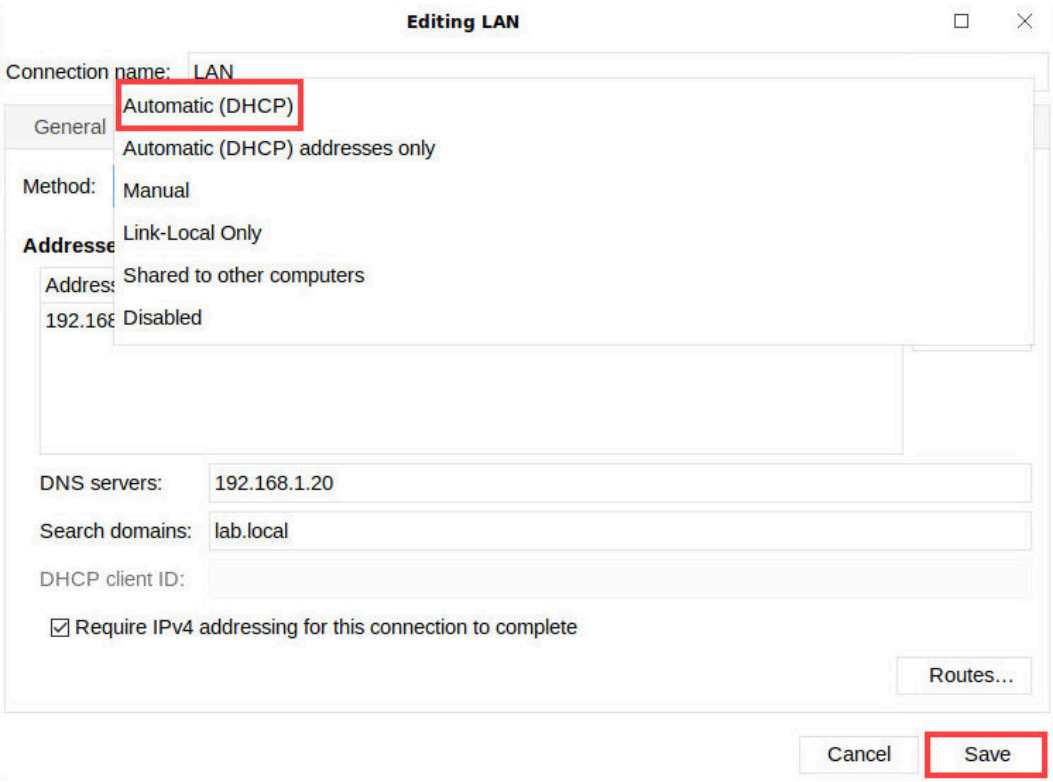


3. In the *Editing LAN* window, click **IPv4 Settings.** Leave the *Editing LAN* window open for the next step.



Notice that the method is set to **Manual**. By default, in this lab environment, the Client is configured with a static IP address of **192.168.1.20**, a Netmask of **24** which is **255.255.255.0**, a default gateway of **192.168.1.1**. The DNS server is set to **192.168.1.20** and the search domain is **lab.local**.

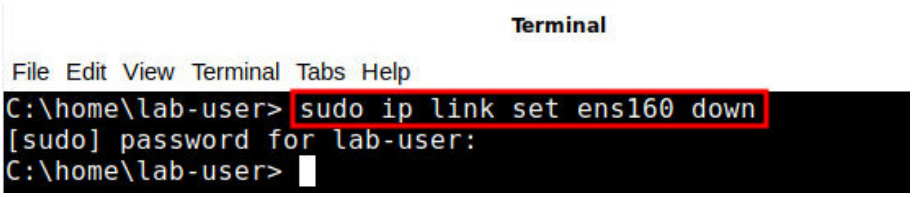
4. In the *Editing LAN* window, click on the **Method** and select **Automatic (DHCP).** Click **Save** and close the *Editing LAN* window.



In the Client, the settings **Use the following IP address** and **Use the following DNS server addresses** are used when configuring static IP addresses. By changing them to obtain Automatic (DHCP), you are enabling DHCP.

5. Click on the **Xfce Terminal** icon in the taskbar.

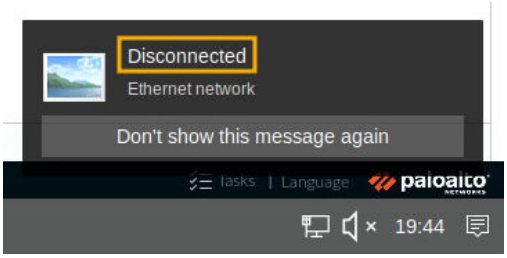
6. In the *Terminal* window, type `sudo ip link set ens160 down`. Enter the `Pal0Alt0!` password when prompted, and press **Enter**. Leave the *Terminal* window open for the next step.

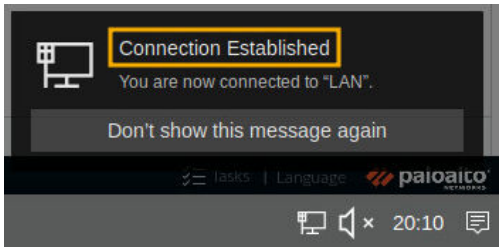


7. With the *Terminal* window still open, type `sudo ip link set ens160 up` and press **Enter.** Leave the *Terminal* window open for the next step.

```
C:\home\lab-user> sudo ip link set ens160 down
[sudo] password for lab-user:
C:\home\lab-user> sudo ip link set ens160 up
C:\home\lab-user>
```

In the previous two steps, you may need to pause for several seconds to confirm that the link has shut down and come back up. Look for the popups indicating this.





8. In the *Terminal* window, type `ip addr` and press **Enter**. Notice the **link/ether** address, also known as the MAC address, of the *ip* command output. (The MAC address will be used in the next task). Leave the *Terminal* window open for the next task.

```
C:\home\lab-user> ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens160: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:50:56:8a:0d:49 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.100/24 brd 192.168.1.255 scope global dynamic noprefixroute ens160
       valid_lft 172641sec preferred_lft 172641sec
    inet 192.168.1.20/24 brd 192.168.1.255 scope global secondary noprefixroute ens160
       valid_lft forever preferred_lft forever
    inet6 fe80::c317:4ce7:59df:690a/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:16:ab:b1:3e brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
       valid_lft forever preferred_lft forever
C:\home\lab-user>
```

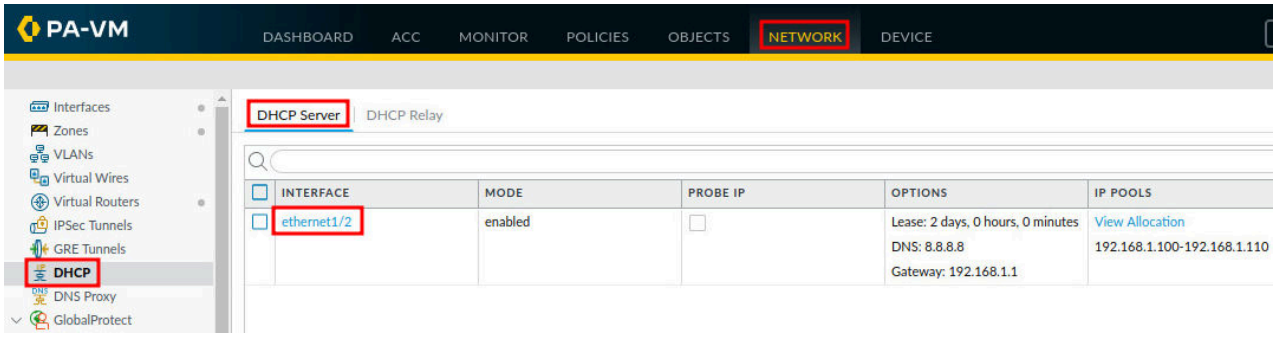
Notice, the IP address (labeled **inet**) has changed to **192.168.1.100**, is labeled **dynamic**, and is in the DHCP range that was configured in a previous task, and **valid lft** indicates a lifetime of **172641 seconds**, which is the 2-day timeout referred to in that previous task. Additionally, the **Manual** address of **192.168.1.20** is still there, but listed as secondary, and has a lifetime of forever.

9. Type `exit` and press **Enter** to close the *Terminal* window.

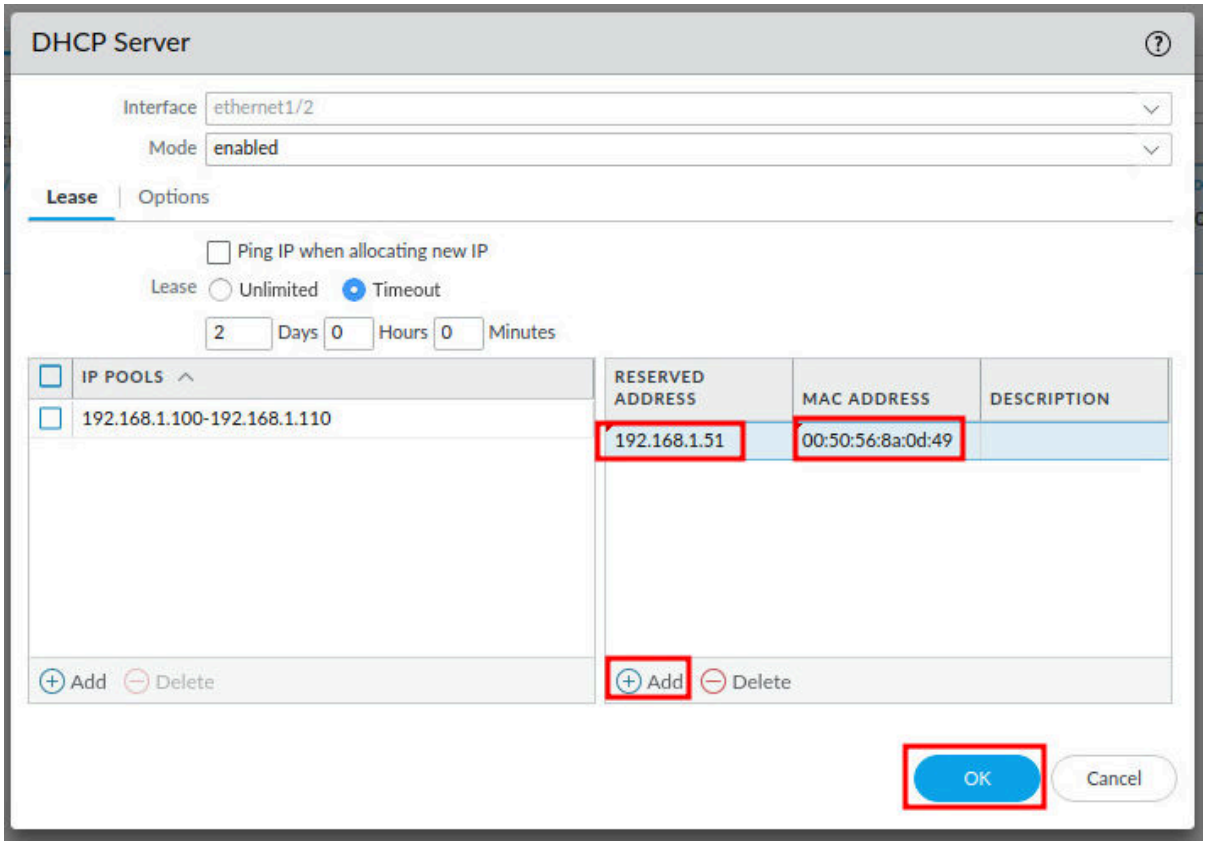
1.3 Configure a DHCP Client Reservation

In this section, you will configure a DHCP Client Reservation. A client reservation is a way to statically assign an IP address to a client via the DHCP Server. The client remains configured for DHCP; however, the DHCP Server will lease the IP address assigned to that physical address or MAC address every time the Client requests a new IP address. As each computer has a unique MAC address, this will assist the DHCP server in leasing the proper address.

1. On the Firewall administration page, navigate to **Network > DHCP > DHCP Server**, and click on **ethernet1/2**.

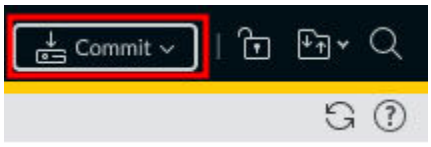


2. Click on the **Add** button under the *Reserved Address* section on the right. Then, type `192.168.1.51` for the *Reserved Address*. Finally, type the *MAC Address* of the Client, `00:50:56:8a:0d:49`**.** Click the **OK** button to close the *DHCP Server* window.

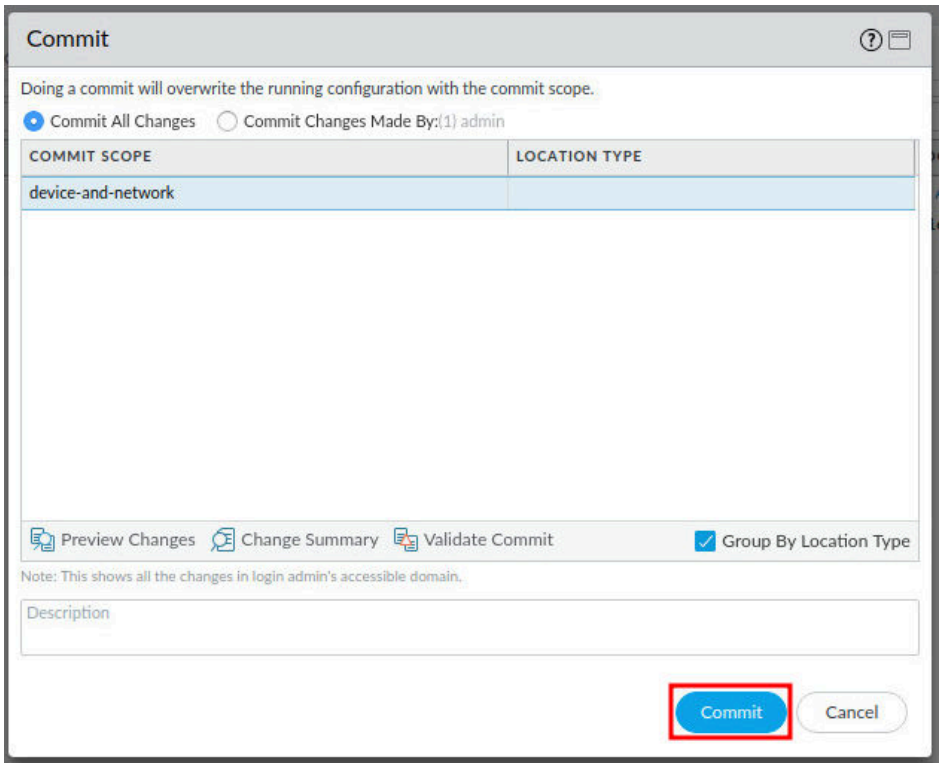


Notice, the MAC address may be displayed slightly. Different systems represent the MAC address in different ways. The Firewall requires colon notation, others may use dash notation. Some systems even condense part of the address, i.e., **0050.568a.0d49**.

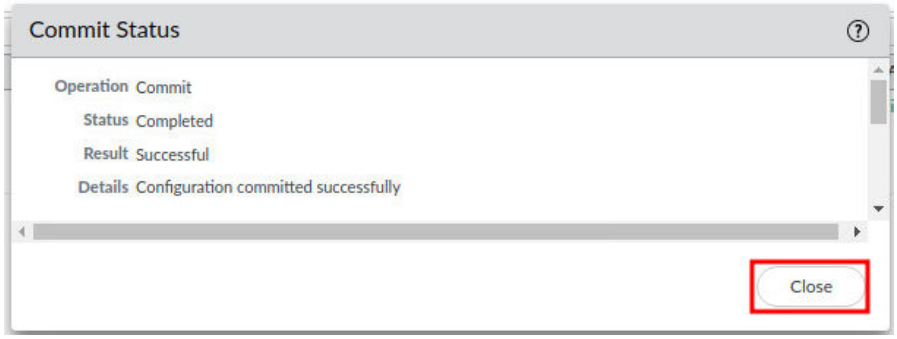
3. Click the **Commit** link located at the top-right of the web interface.



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

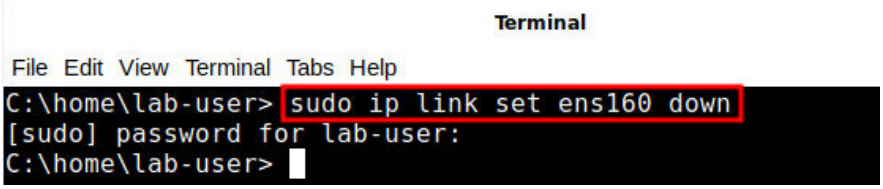


5. When the commit operation successfully completes, click **Close** to continue.

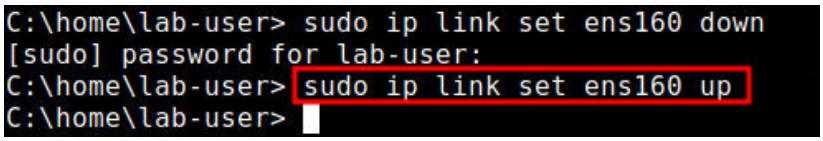


6. Click on the **Xfce Terminal** icon in the taskbar.

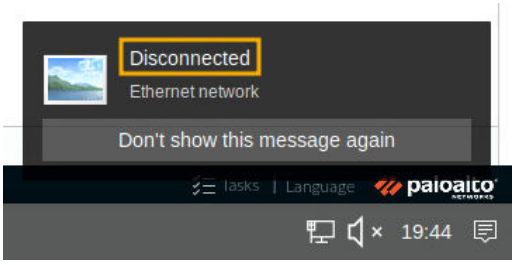
7. In the *Terminal* window, type `sudo ip link set ens160 down`. Enter the `Pal0Alt0!` password when prompted, and press **Enter**. Leave the *Terminal* window open for the next step.

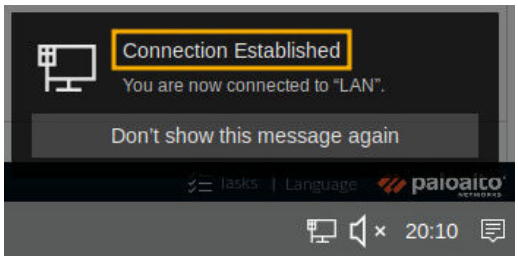


8. With the *Terminal* window still open, type `sudo ip link set ens160 up` and press **Enter.** Leave the *Terminal* window open for the next step.

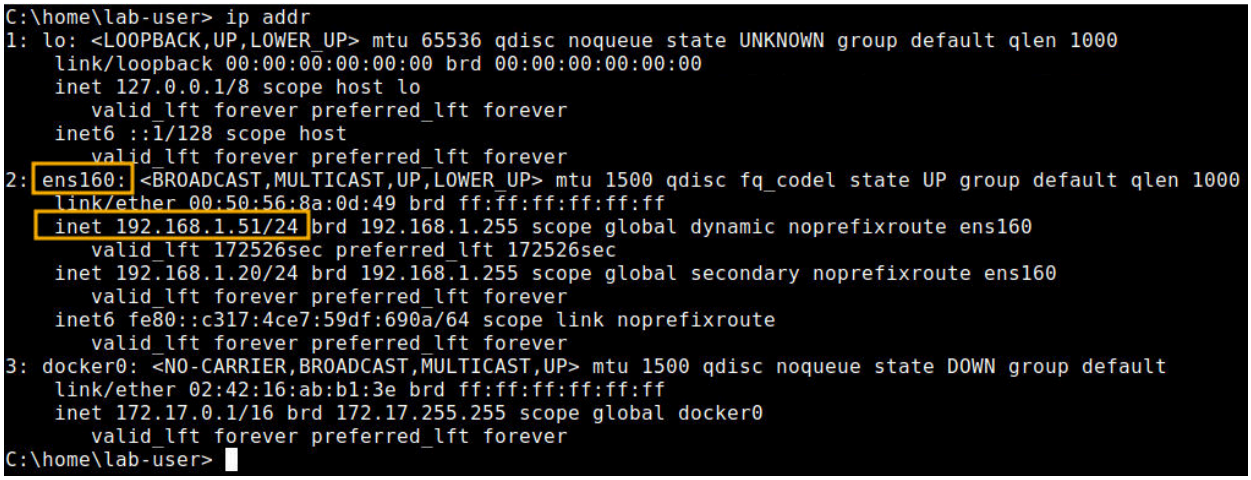


In the previous two steps, you may need to pause for several seconds to confirm that the link has shut down and come back up. Look for the popups indicating this.





9. In the *Terminal* window, type `ip addr` and press **Enter**. This command will show the new lease from the DHCP server.



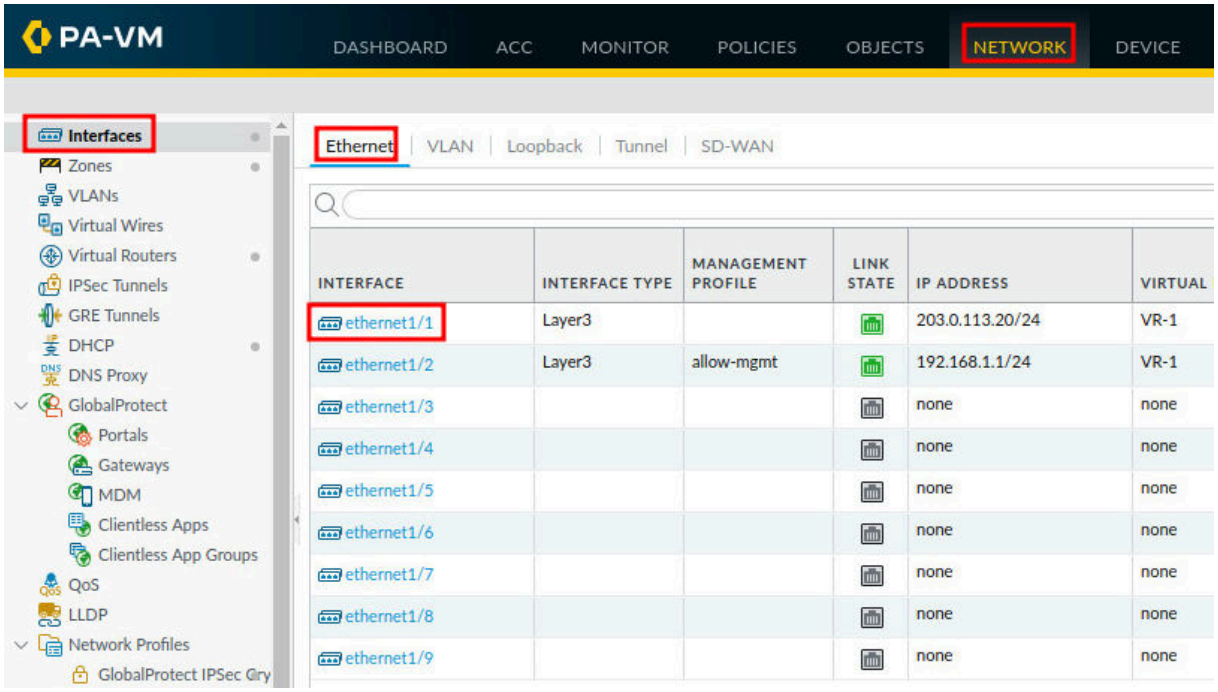
You should receive an IP address of **192.168.1.51**. This was the address you reserved for the Client machine on the firewall. If you receive a different address, repeat this section and take careful note of the MAC address.

10. Type `exit` and press **Enter** to exit the *Terminal* window.

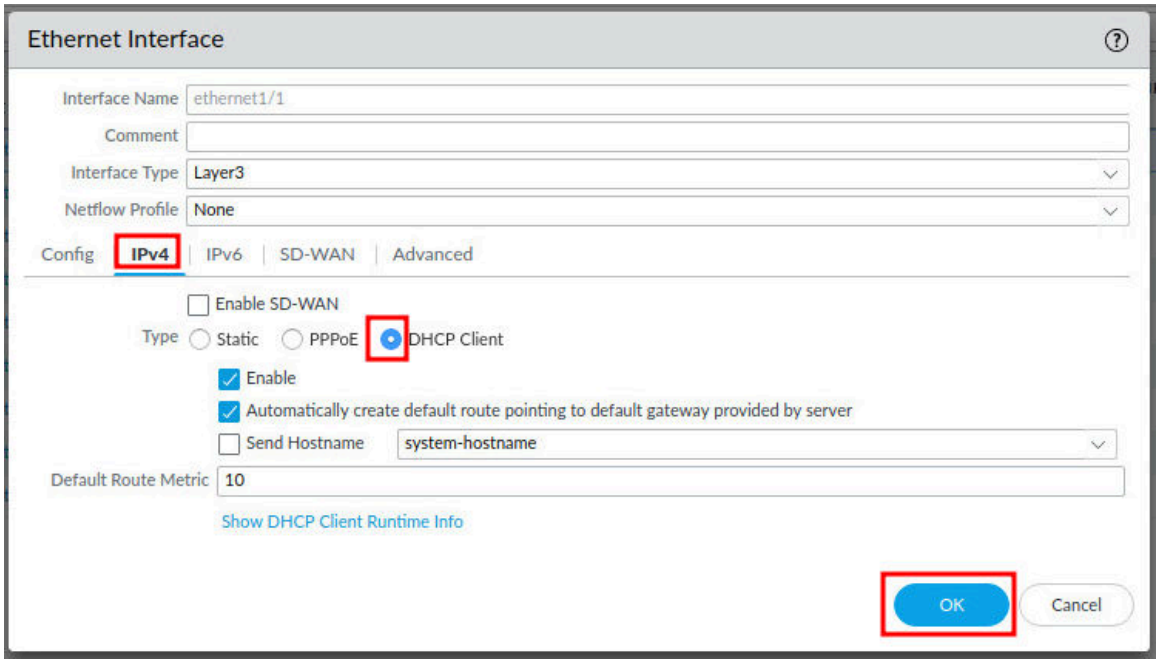
1.4 Configure the Firewall Outside Interface for DHCP

In this section, you will configure the Firewall outside interface for DHCP. Like the Client in the previous task, the Firewall will obtain an IP address from a DHCP server on the network.

1. On the Firewall administration page, navigate to **Network > Interfaces > Ethernet**. Click on **ethernet1/1**.

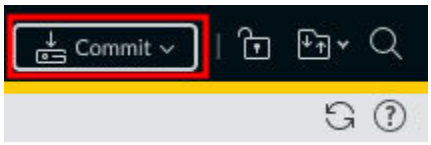


2. On the *Ethernet Interface* window, click on the **IPv4** tab. Then, select the **DHCP Client** radio button in the *Type* field. Finally, click the **OK** button.

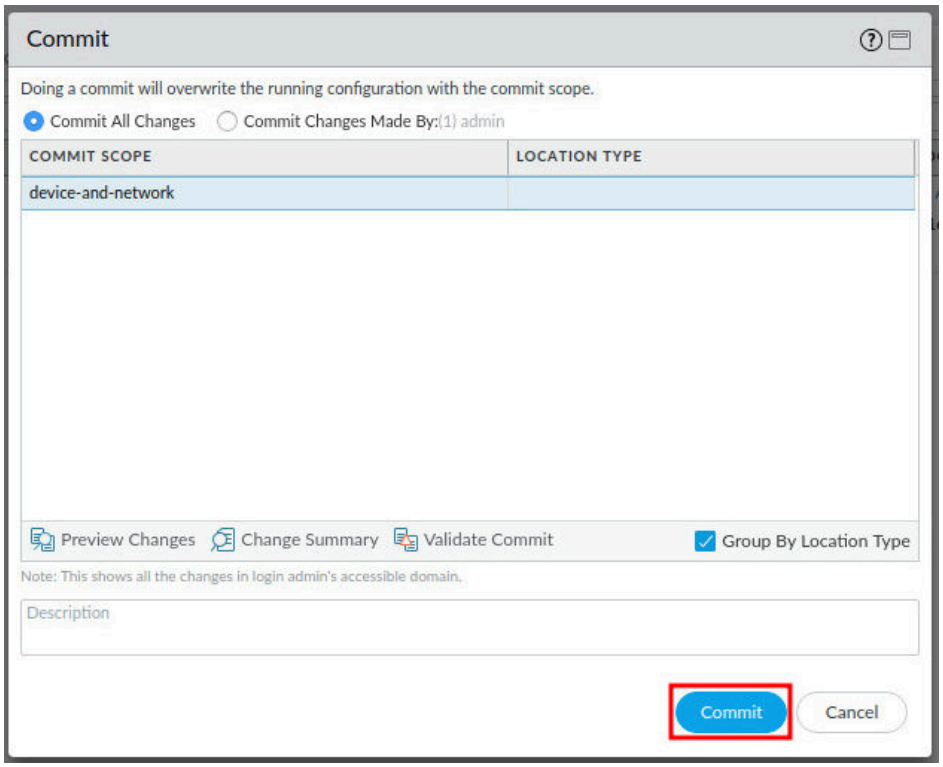


The **DHCP Client** setting allows the Firewall interface to receive a dynamic IP Address. Some internet service providers will provide an IP address via DHCP, in which case the Firewall will need to be configured to receive a dynamic IP Address.

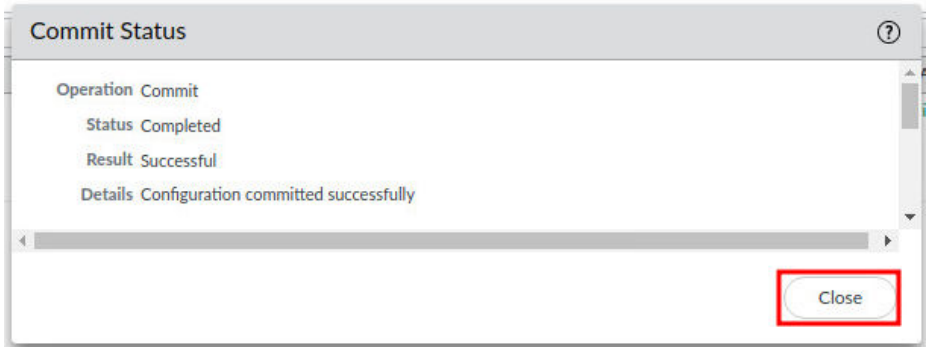
3. Click the **Commit** link located at the top-right of the web interface.



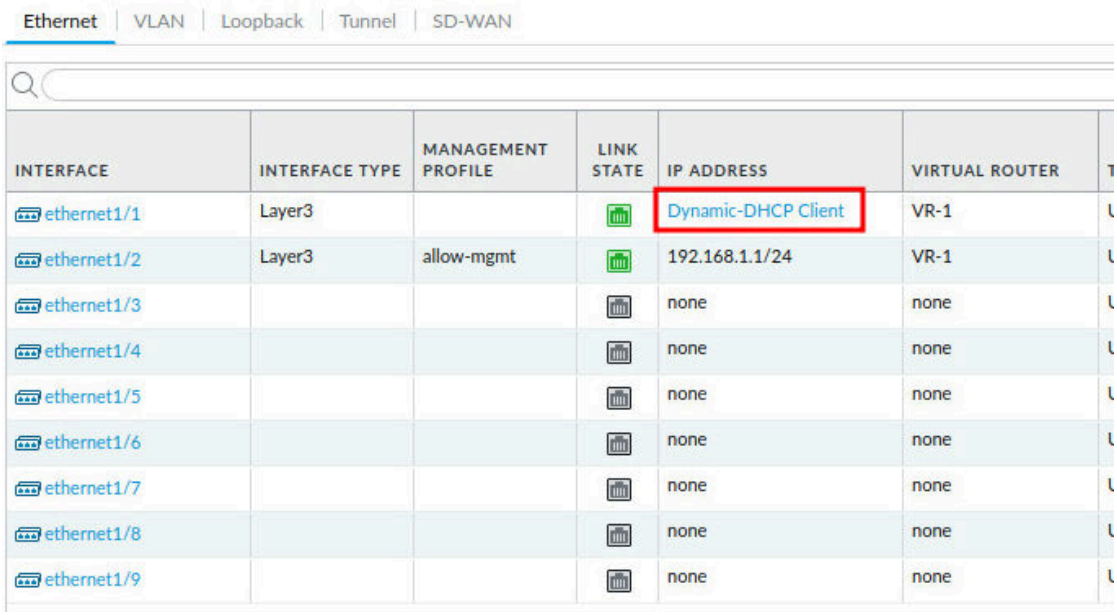
4. In the *Commit* window, click **Commit** to proceed with committing the changes.



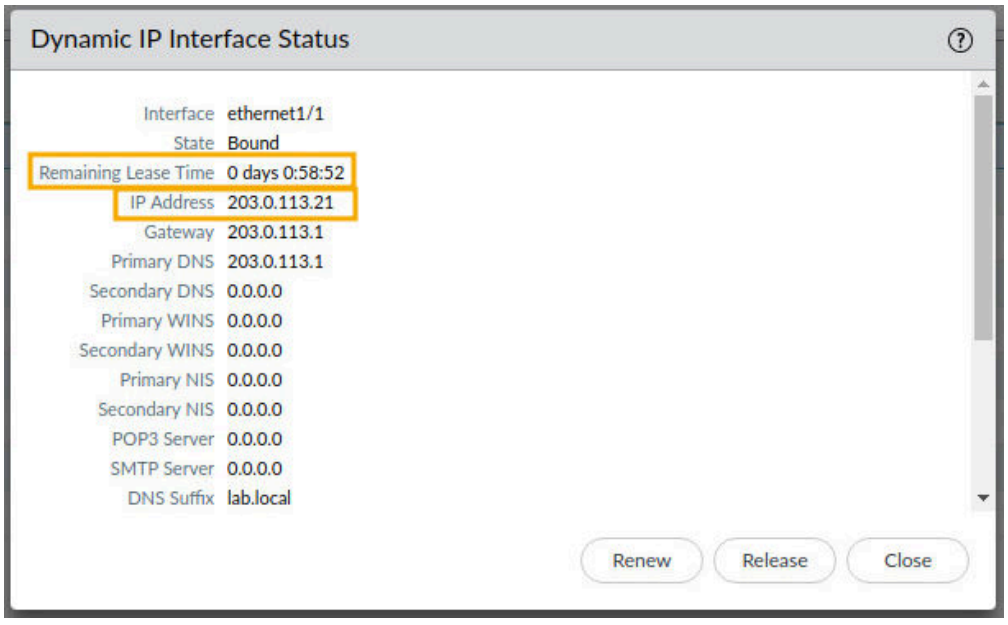
5. When the commit operation successfully completes, click **Close** to continue.



6. Click on the **Dynamic-DHCP Client** link under the *IP Address* field for **ethernet1/1**.



7. You should receive an *IP Address* of **203.0.113.x**, where *x* could be any number starting with the number 2 thru 254. This was obtained from the DHCP Server running on the VRouter between the Firewall and the External Network. (Note also the lease time of less than an hour.)



8. The lab is now complete; you may end the reservation.

