NETWORK SECURITY FUNDAMENTALS

Lab 1: Configuring DHCP

Document Version: 2021-01-30

Contents

Introduction

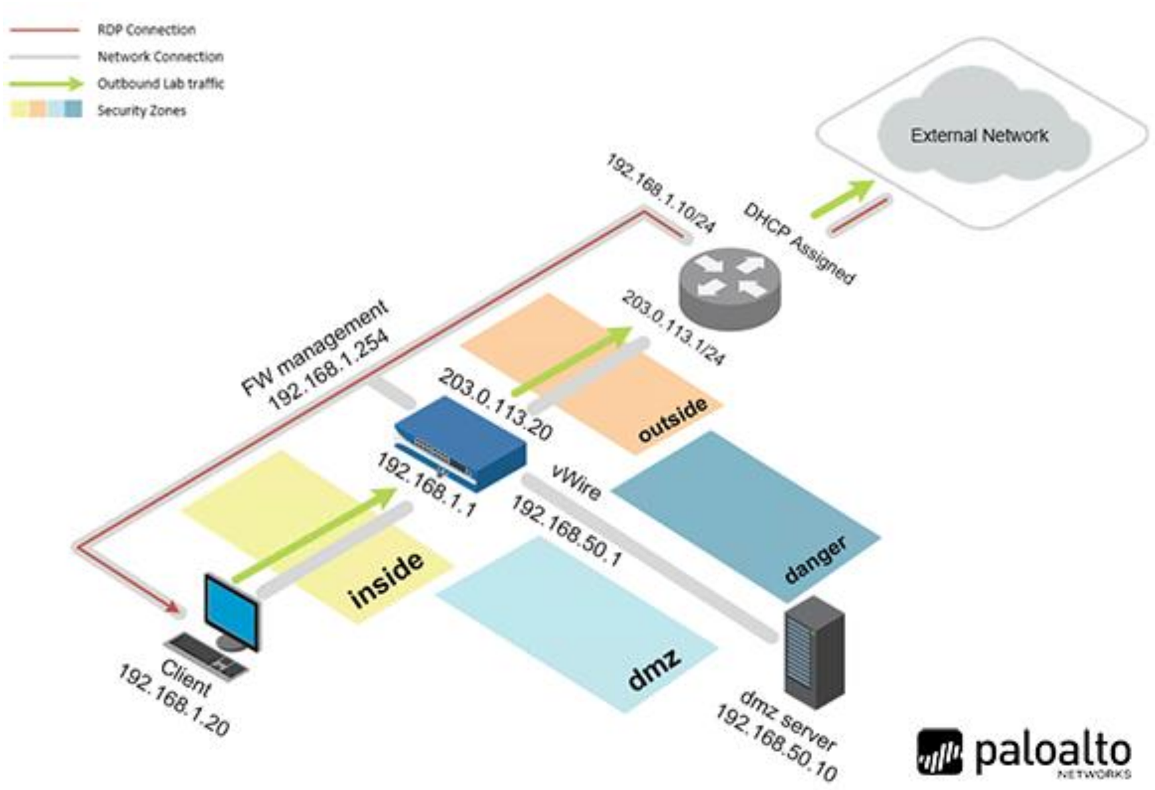
In this lab, you will configure the Palo Alto Networks Firewall as a DHCP server. You will then test the DHCP server with the Client PC.

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.

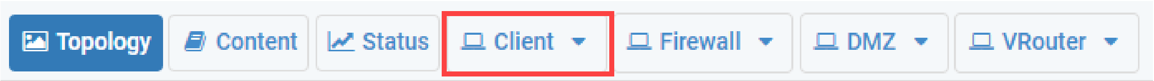
Virtual Machine	**IP Address**	**Account** (if needed)	**Password** (if needed)
Client	192.168.1.20	lab-user	Train1ng$
DMZ	192.168.50.10	root	Pal0Alt0
Firewall	192.168.1.254	admin	Train1ng$

1 Configuring DHCP

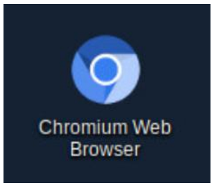
1.0 Load Lab Configuration

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

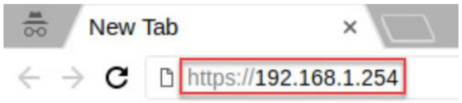
1. Click on the **Client** tab to access the Client PC.



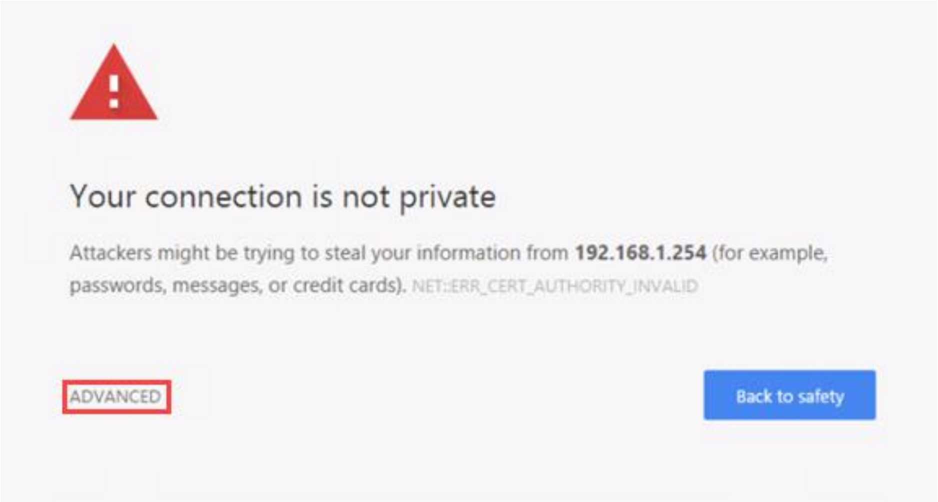
2. Log in to the Client PC as username `lab-user`, password `Train1ng$`.
3. Double-click the **Chromium Web Browser** icon located on the Desktop.



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.

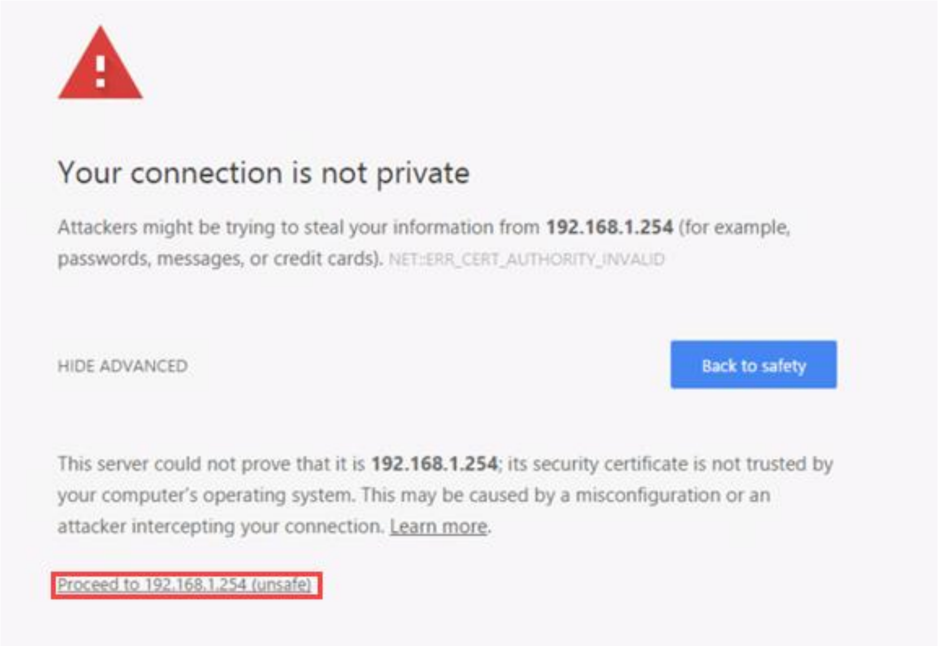


Your connection is not private

Attackers might be trying to steal your information from **192.168.1.254** (for example, passwords, messages, or credit cards). NET::ERR_CERT_AUTHORITY_INVALID

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)**.

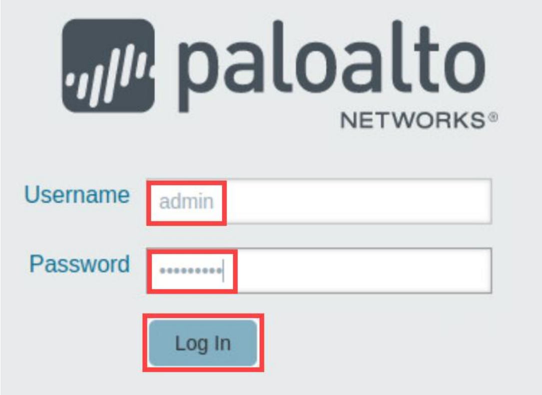


Your connection is not private

Attackers might be trying to steal your information from **192.168.1.254** (for example, passwords, messages, or credit cards). NET::ERR_CERT_AUTHORITY_INVALID

This server could not prove that it is **192.168.1.254**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection. Learn more.

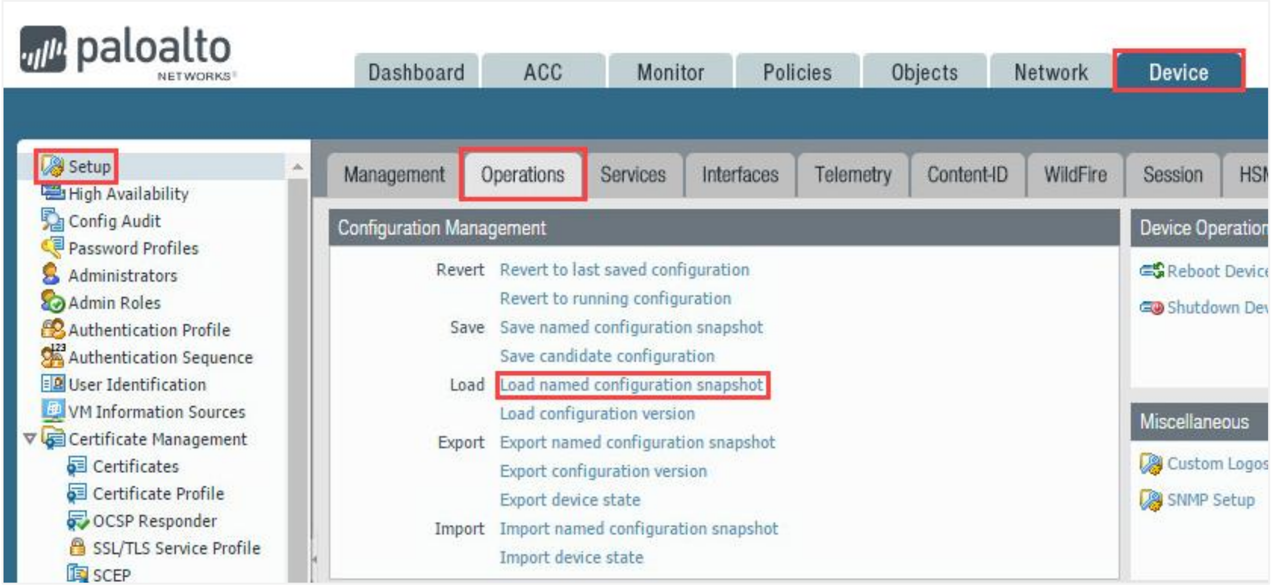
7. Log in to the Firewall web interface as username **`admin`**, password **`Train1ng$`.**



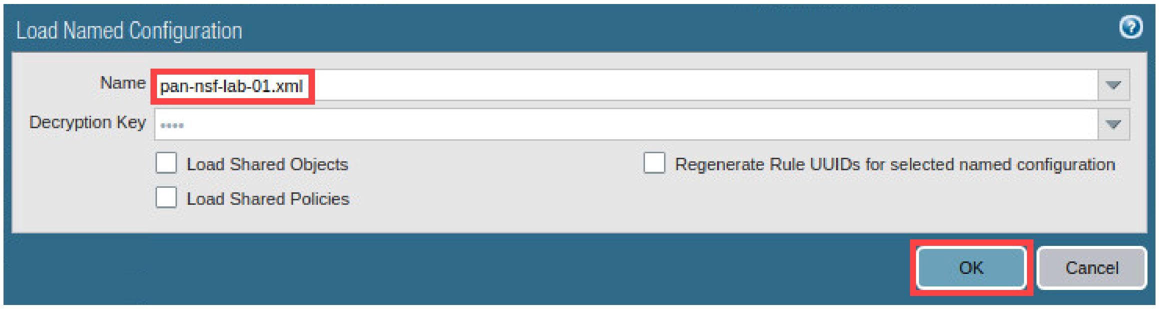
Username: admin

Password: •••••••••

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**.



Load Named Configuration

Name: pan-nsf-lab-01.xml

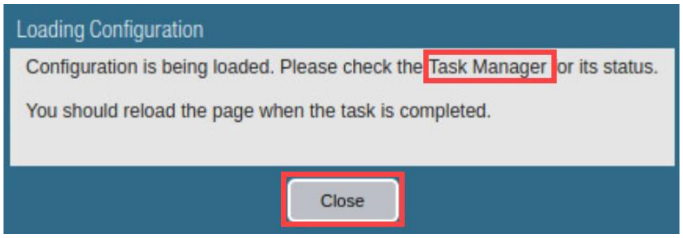
Decryption Key: ••••

□ Load Shared Objects

□ Load Shared Policies

□ Regenerate Rule UUIDs for selected named configuration

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.

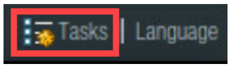


Loading Configuration

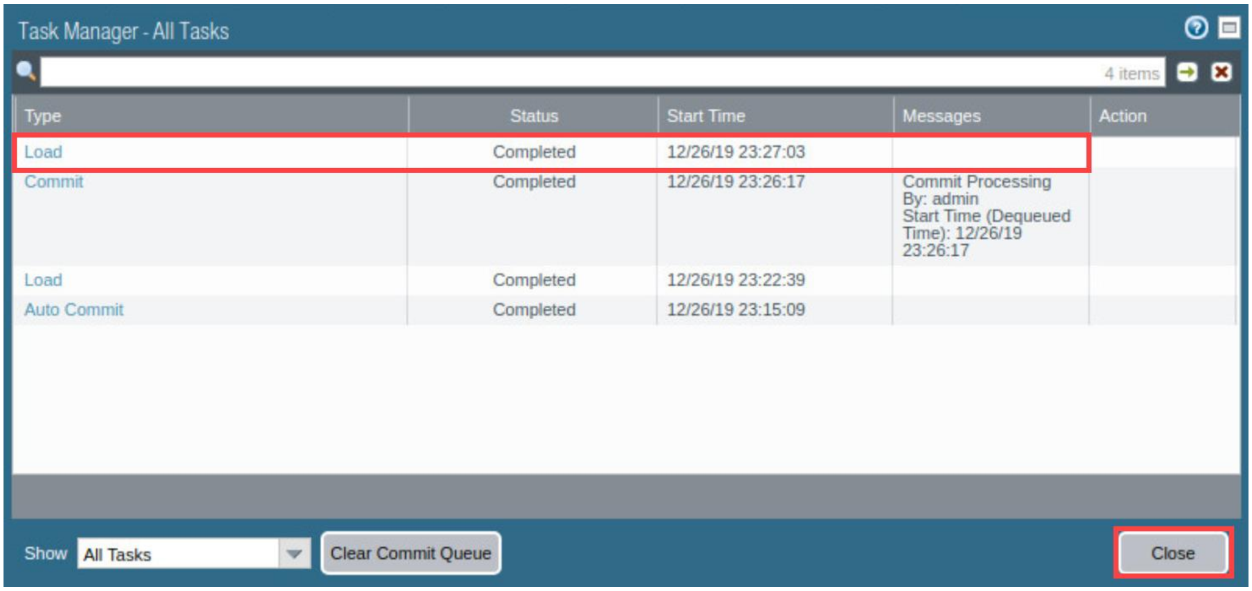
Configuration is being loaded. Please check the Task Manager for its status.

You should reload the page when the task is completed.

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

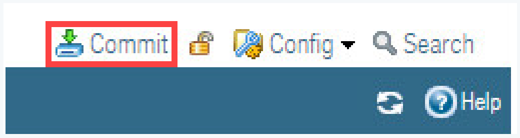


12. In the *Task Manager – All Tasks* window, verify the *Load* type has successfully completed. Click **Close.**

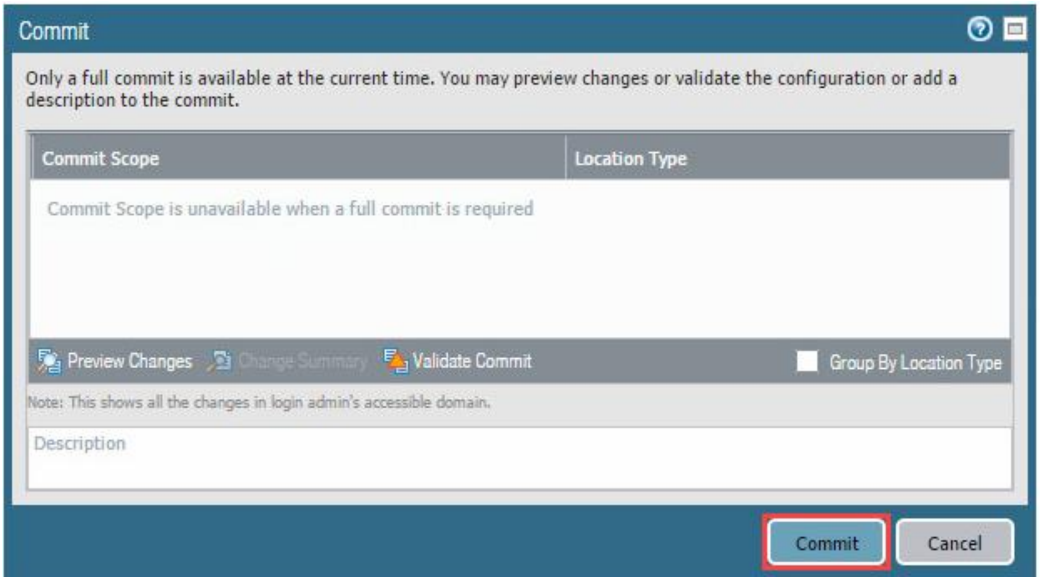


Type	Status	Start Time	Messages	Action
Load	Completed	12/26/19 23:27:03		
Commit	Completed	12/26/19 23:26:17	Commit Processing By: admin Start Time (Dequeued Time): 12/26/19 23:26:17	
Load	Completed	12/26/19 23:22:39		
Auto Commit	Completed	12/26/19 23:15:09		

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.

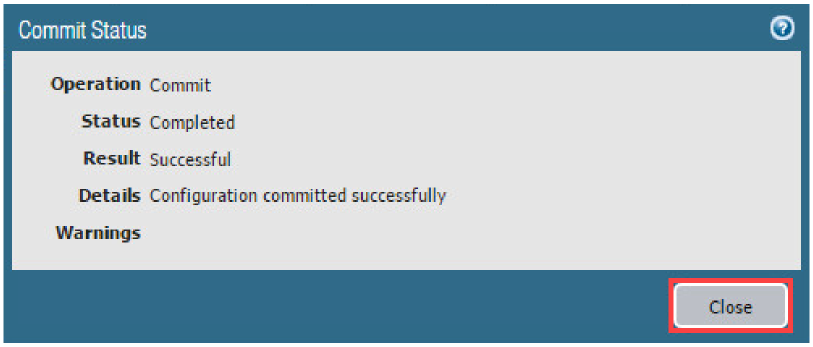


Only a full commit is available at the current time. You may preview changes or validate the configuration or add a description to the commit.

Commit Scope	Location Type
Commit Scope is unavailable when a full commit is required	

Note: This shows all the changes in login admin's accessible domain.

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



Commit Status

Operation Commit

Status Completed

Result Successful

Details Configuration committed successfully

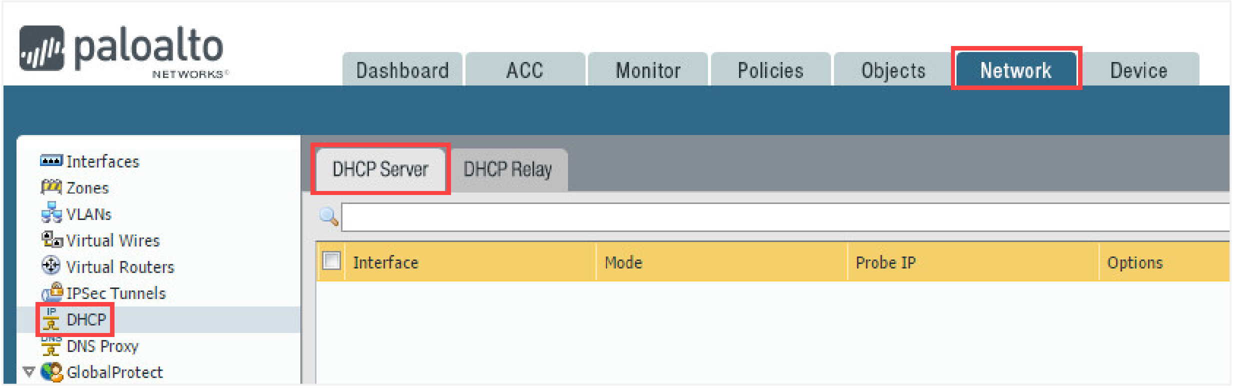
Warnings

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.

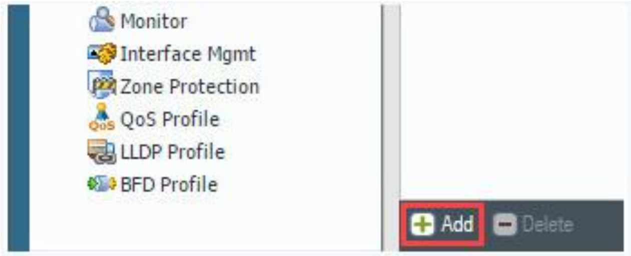
1.1 Configure DHCP Server

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.

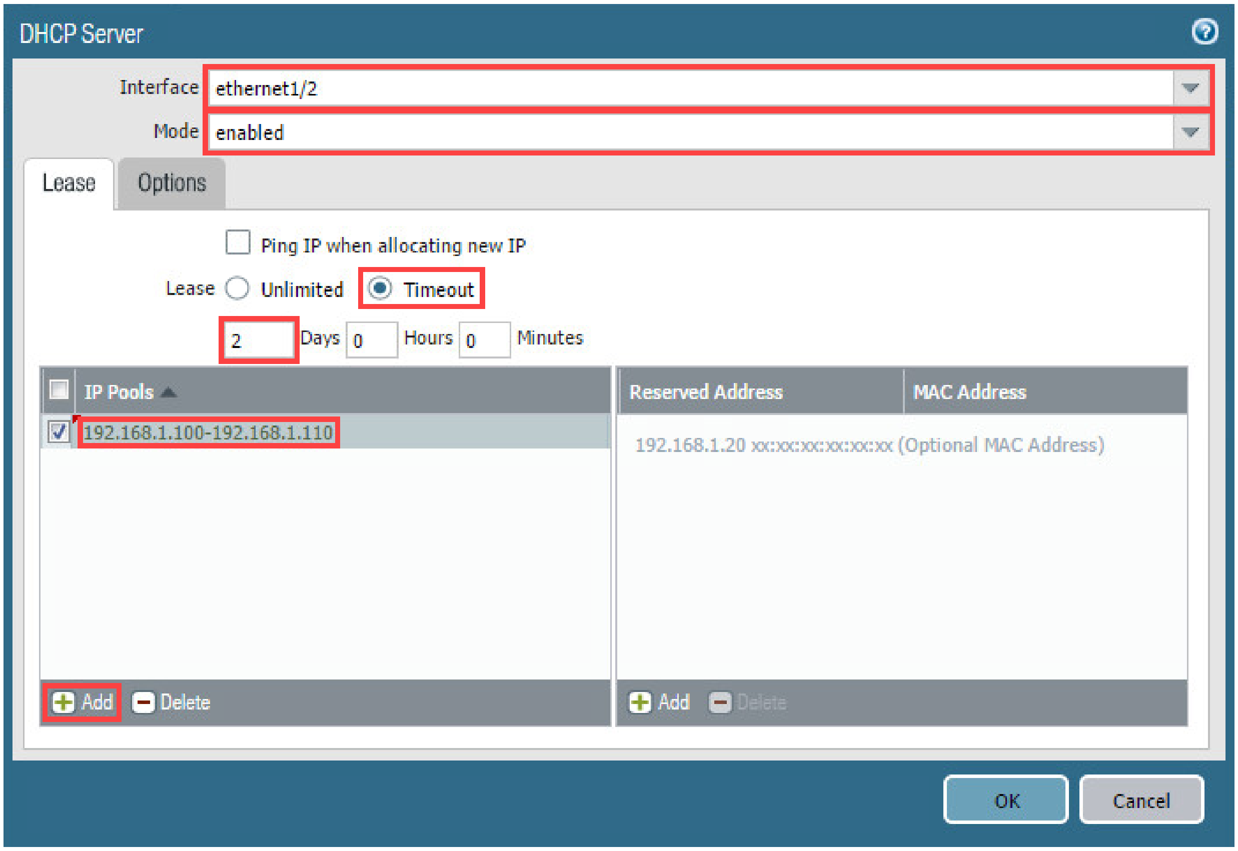
1. Navigate to **Network > DHCP > DHCP Server.**



2. Click on **Add**, located near the bottom-left of the *IP Pools* 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`**.


DHCP Server

Interface: ethernet1/2

Mode: enabled

□ Ping IP when allocating new IP

Lease ○ Unlimited ● Timeout

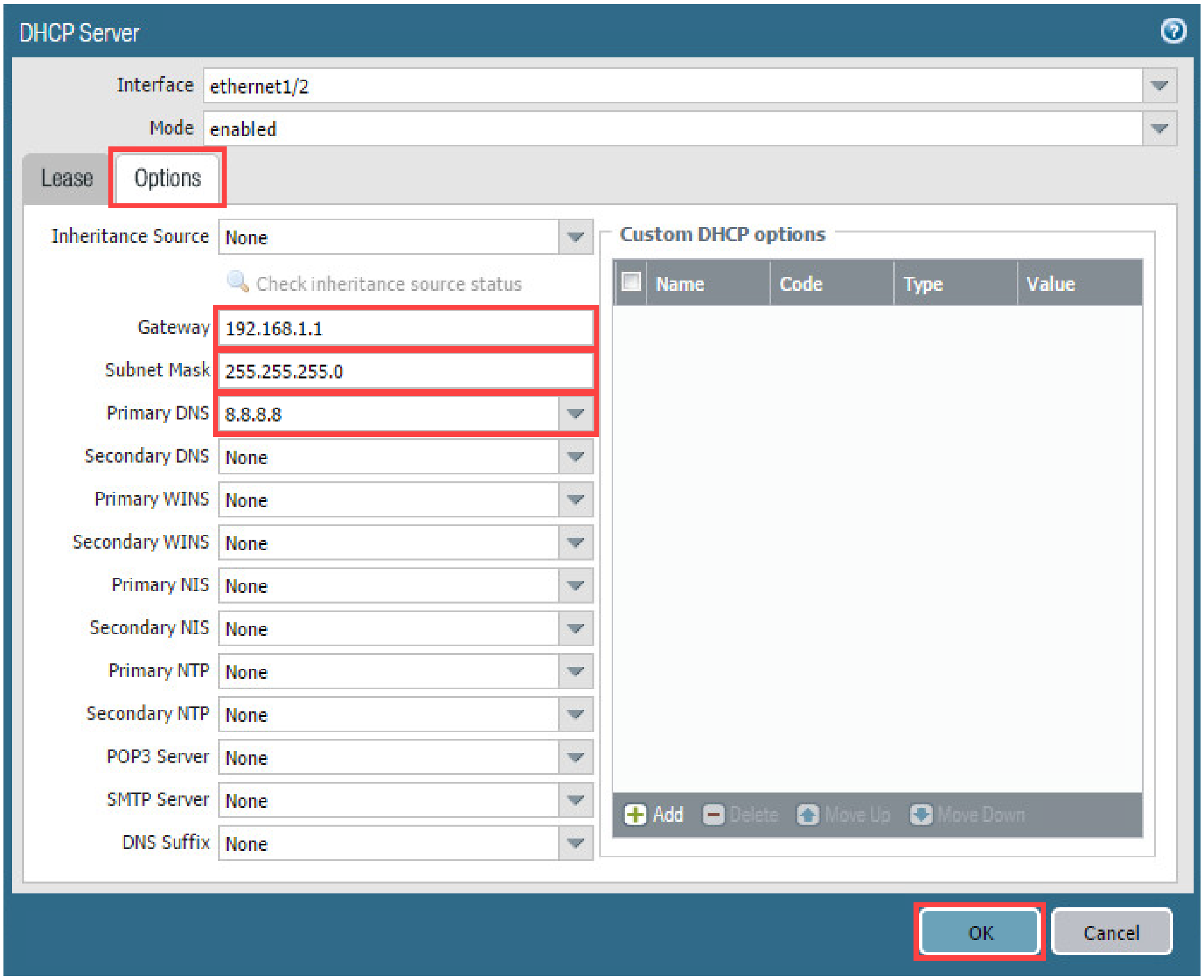
2 Days 0 Hours 0 Minutes

☐ IP Pools
☑ 192.168.1.100-192.168.1.110

Reserved Address	MAC Address
192.168.1.20 xx:xx:xx:xx:xx:xx (Optional MAC Address)	

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.



DHCP Server

Interface: ethernet1/2

Mode: enabled

Inheritance Source: None

Gateway: 192.168.1.1

Subnet Mask: 255.255.255.0

Primary DNS: 8.8.8.8

Secondary DNS: None

Primary WINS: None

Secondary WINS: None

Primary NIS: None

Secondary NIS: None

Primary NTP: None

Secondary NTP: None

POP3 Server: None

SMTP Server: None

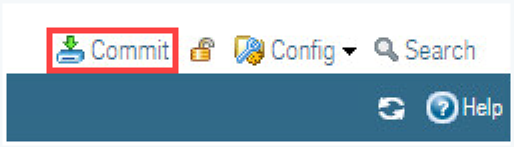
DNS Suffix: None

Custom DHCP options

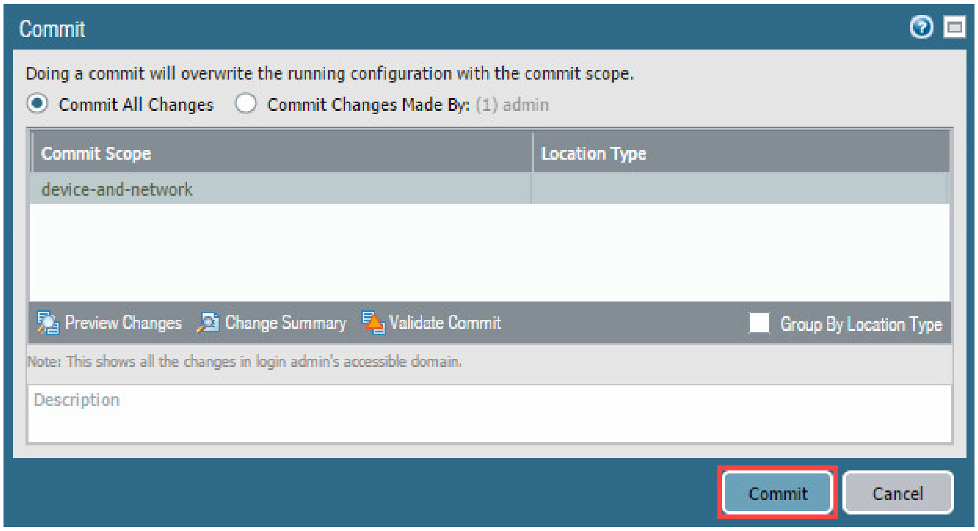
□	Name	Code	Type	Value

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.



Commit

Doing a commit will overwrite the running configuration with the commit scope.

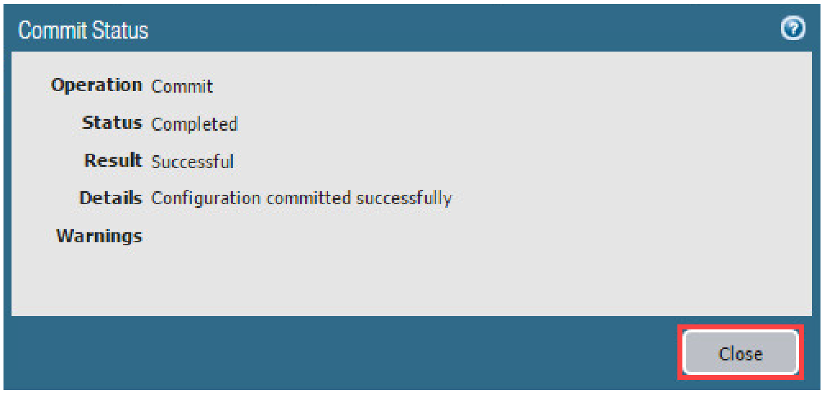
● Commit All Changes ○ Commit Changes Made By: (1) admin

Commit Scope	Location Type
device-and-network	

Note: This shows all the changes in login admin's accessible domain.

Description

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



Commit Status

Operation Commit

Status Completed

Result Successful

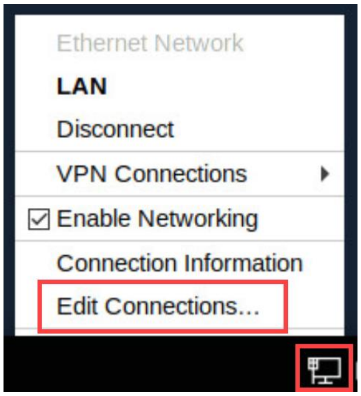
Details Configuration committed successfully

Warnings

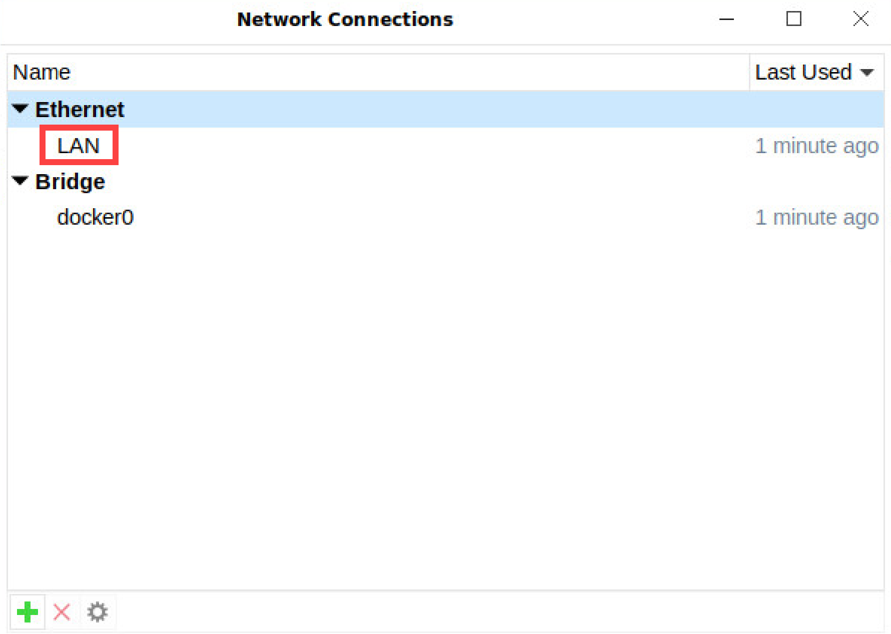
1.2 Configure Client for DHCP

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.

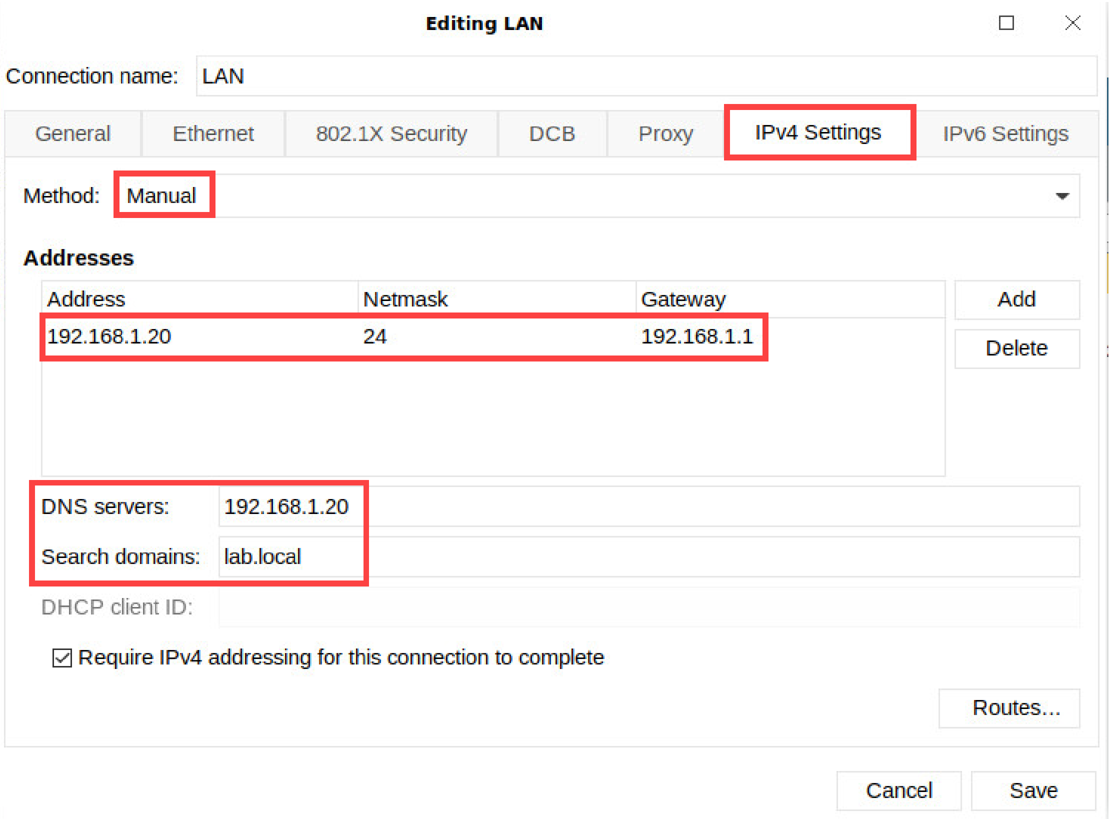
1. Click on the **Connection** icon in the lower-right of the web *Client*. Next, click on **Edit Connections...**



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.



Connection name: LAN

Method: Manual

Address	Netmask	Gateway
192.168.1.20	24	192.168.1.1

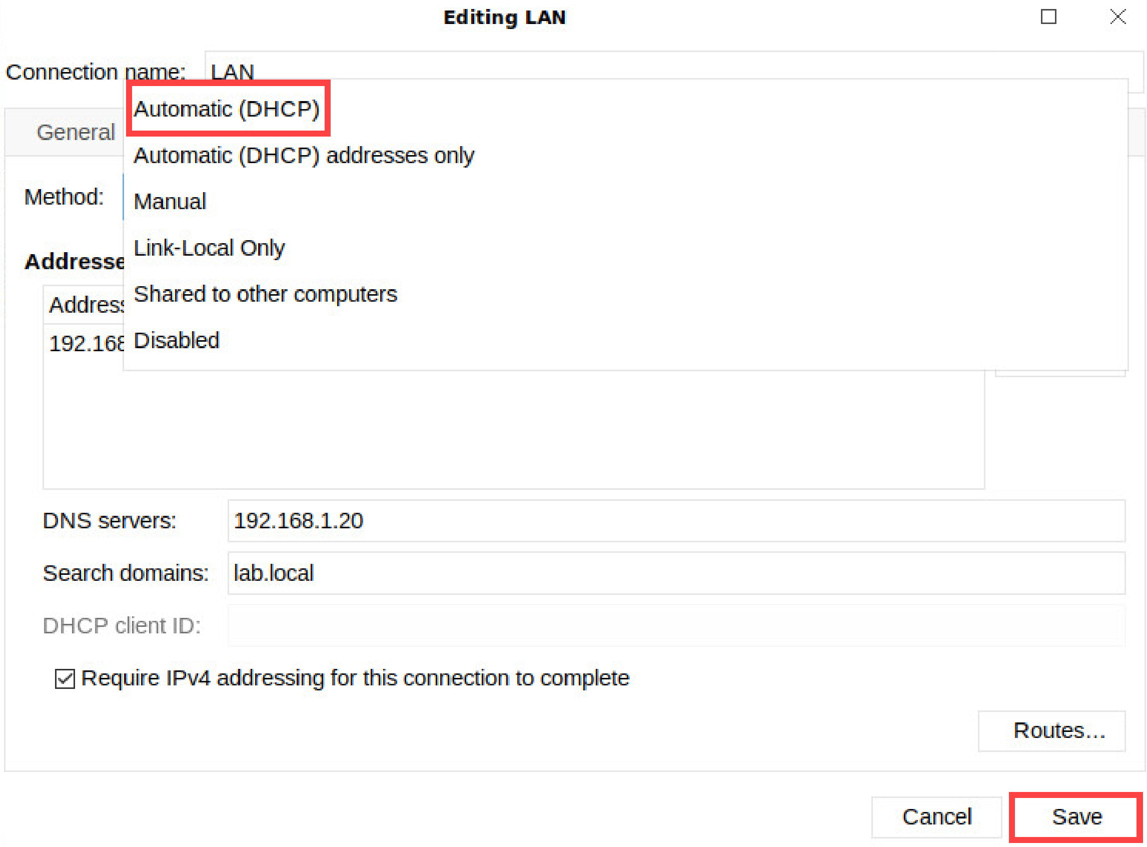
DNS servers: 192.168.1.20

Search domains: lab.local

☑ Require IPv4 addressing for this connection to complete

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.



Editing LAN

Connection name: LAN

Method: Automatic (DHCP)

DNS servers: 192.168.1.20

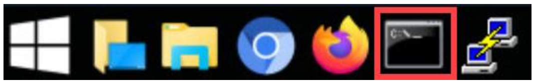
Search domains: lab.local

DHCP client ID:

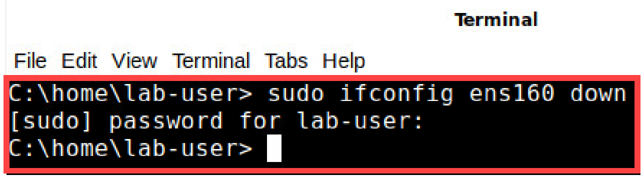
☑ Require IPv4 addressing for this connection to complete

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.

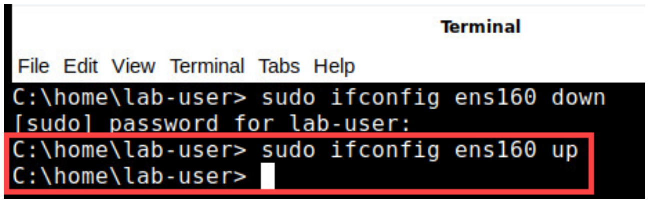


6. In the *Terminal* window, type **`sudo ifconfig ens160 down`**. Enter the **`Train1ng$`** password when prompted, and press **Enter**. Leave the *Terminal* window open for the next step.



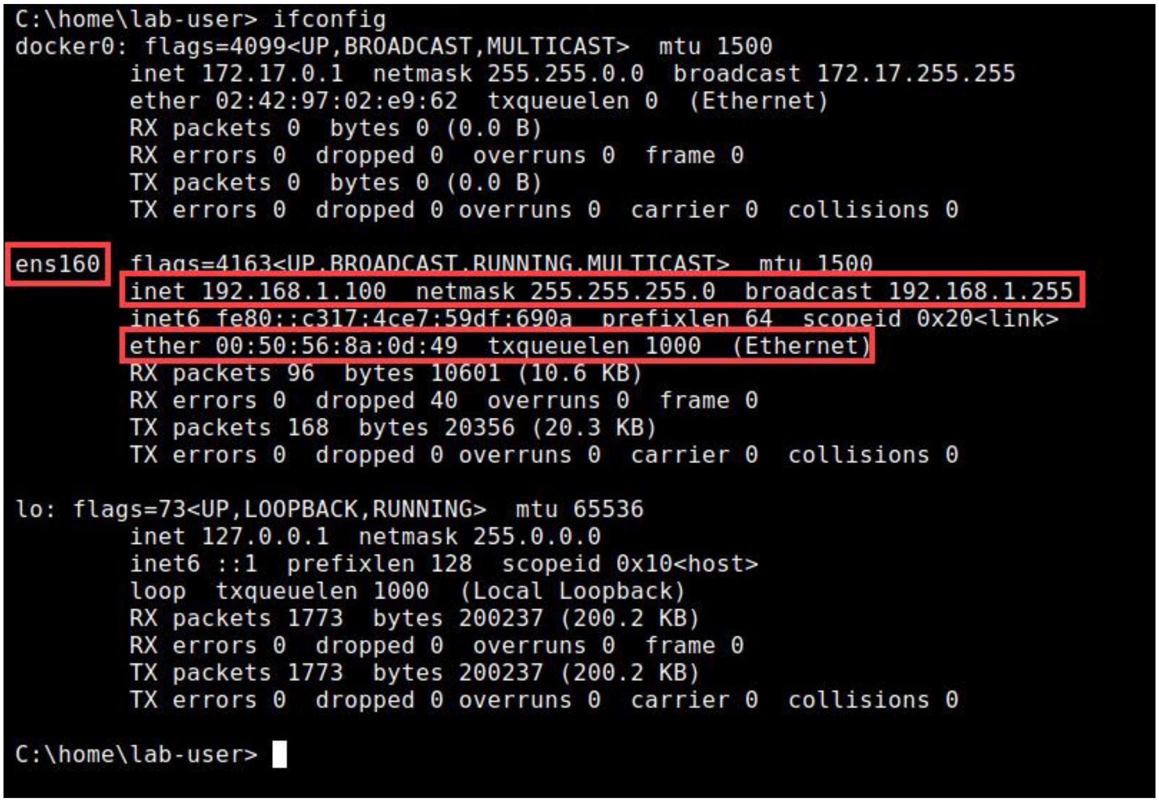
```
C:\home\lab-user> sudo ifconfig ens160 down
[sudo] password for lab-user:
C:\home\lab-user>
```

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



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

8. In the *Terminal* window, type **`ifconfig`** and press **Enter**. Notice the IP Address and DHCP Record of the Physical Address, also known as the MAC address, of the *ifconfig* 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> ifconfig
docker0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 172.17.0.1  netmask 255.255.0.0  broadcast 172.17.255.255
        ether 02:42:97:02:e9:62  txqueuelen 0  (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

ens160  flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.100  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::c317:4ce7:59df:690a  prefixlen 64  scopeid 0x20<link>
        ether 00:50:56:8a:0d:49  txqueuelen 1000  (Ethernet)
        RX packets 96  bytes 10601 (10.6 KB)
        RX errors 0  dropped 40  overruns 0  frame 0
        TX packets 168  bytes 20356 (20.3 KB)
        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
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 1773  bytes 200237 (200.2 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1773  bytes 200237 (200.2 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

C:\home\lab-user>
```

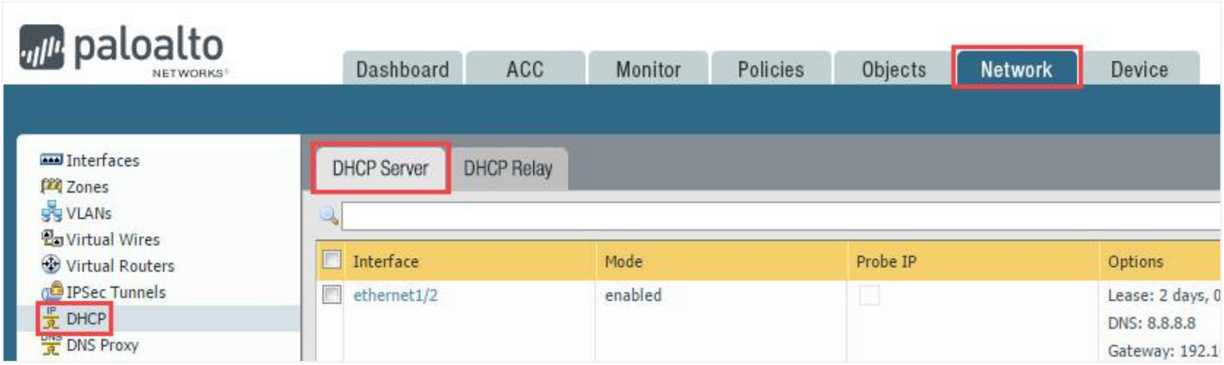
> Notice, the IP address has changed to 192.168.1.100 and is in the DHCP range that was configured in a previous task. The DHCP Server is the IP address of the Firewall.

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

1.3 Configure a DHCP Client Reservation

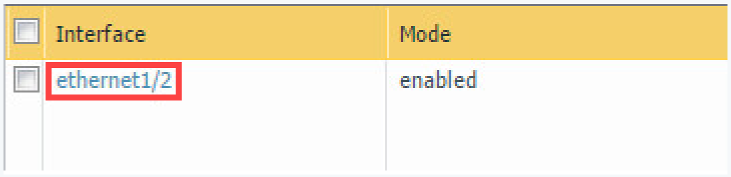
In this section, you will configure a DHCP Client Reservation. A client reservation is a way to statically assign an IP address to a client via the DHCP Server. The client remains configured for DHCP; however, the DHCP Server will lease the IP address assigned to that physical address or MAC address 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**.



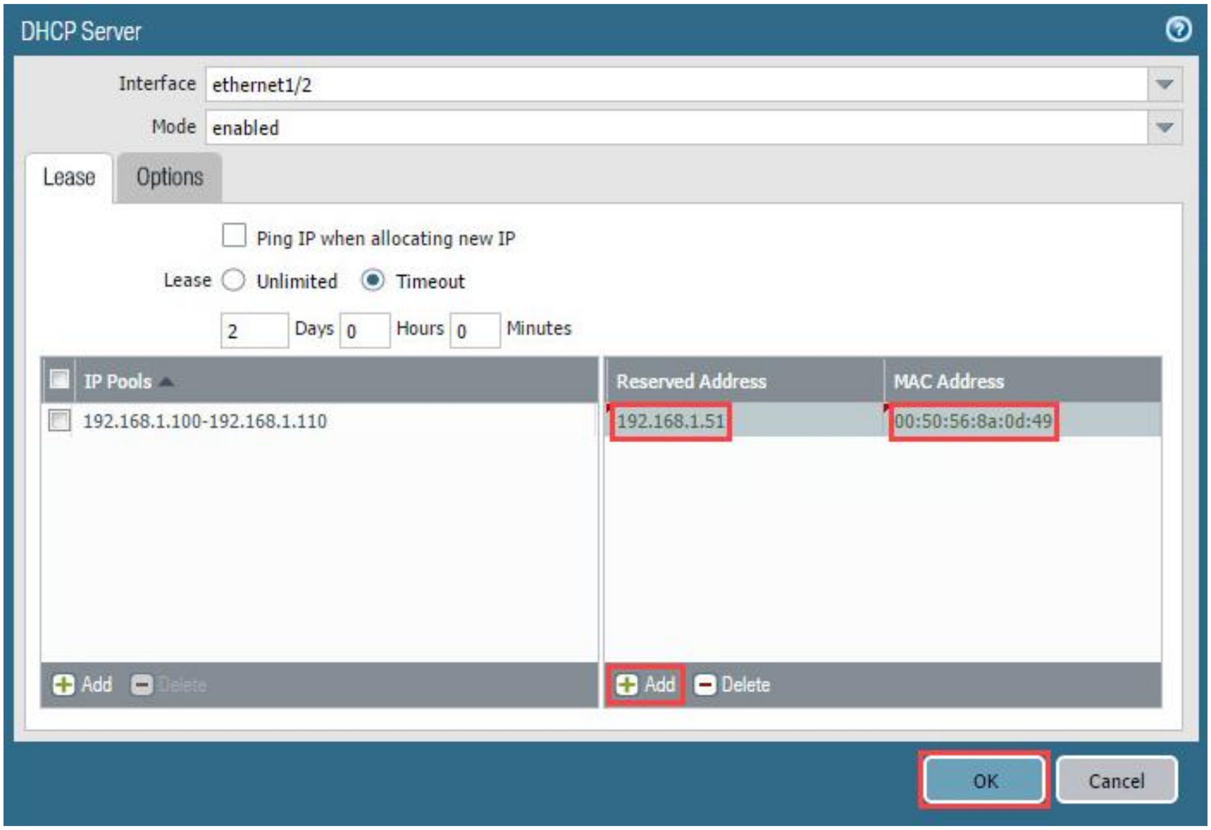
□	Interface	Mode	Probe IP	Options
□	ethernet1/2	enabled	□	Lease: 2 days, 0 DNS: 8.8.8.8 Gateway: 192.1

2. Click on **ethernet1/2**.



□	Interface	Mode
□	ethernet1/2	enabled

3. 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`.



DHCP Server

Interface ethernet1/2

Mode enabled

Lease | Options

☐ Ping IP when allocating new IP

Lease ○ Unlimited ● Timeout

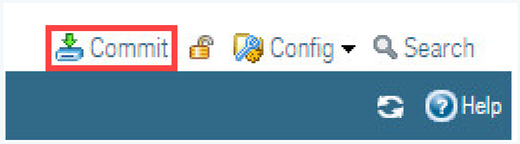
2 Days 0 Hours 0 Minutes

☐ IP Pools
☐ 192.168.1.100-192.168.1.110

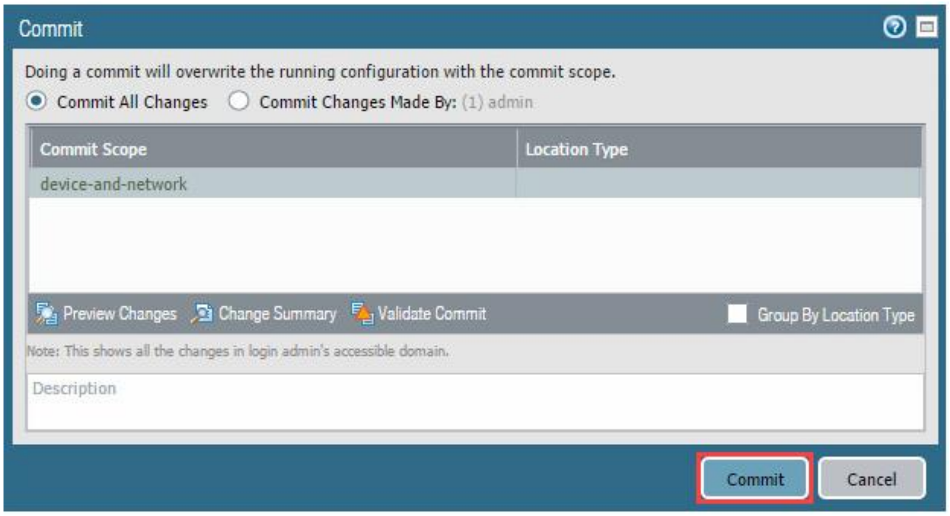
Reserved Address	MAC Address
192.168.1.51	00:50:56:8a:0d:49

Notice, the MAC address is displayed slightly differently than it was in the *Terminal* window in the previous task. Different systems represent the MAC address in different ways. In this case, the Firewall requires it use colon notation. The Client uses dash notation. Some systems even condense part of the address, i.e., **0050.568a.0d49**.

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



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



Commit

Doing a commit will overwrite the running configuration with the commit scope.

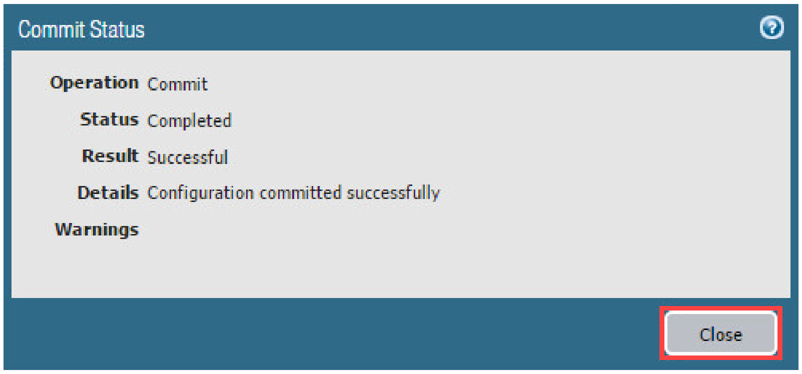
● Commit All Changes ○ Commit Changes Made By: (1) admin

Commit Scope	Location Type
device-and-network	

Note: This shows all the changes in login admin's accessible domain.

Description

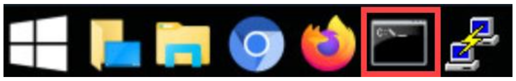
7. When the commit operation successfully completes, click **Close** to continue.



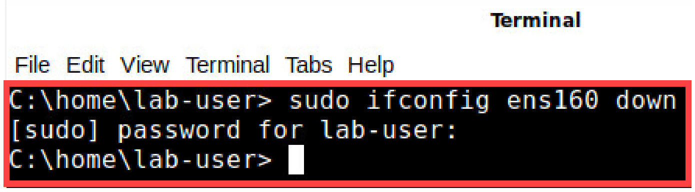
Commit Status

Operation Commit
Status Completed
Result Successful
Details Configuration committed successfully
Warnings

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

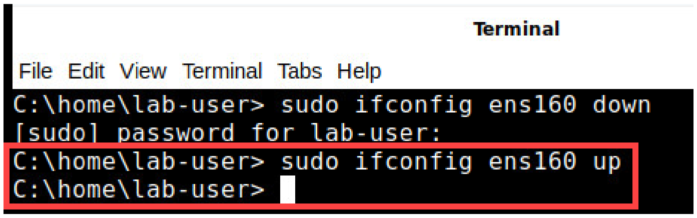


9. With the *Terminal* window still open, type `sudo ifconfig ens160 down.` Enter the `Train1ng$` password when prompted and press **Enter.** Leave the *Terminal* window open for the next step.



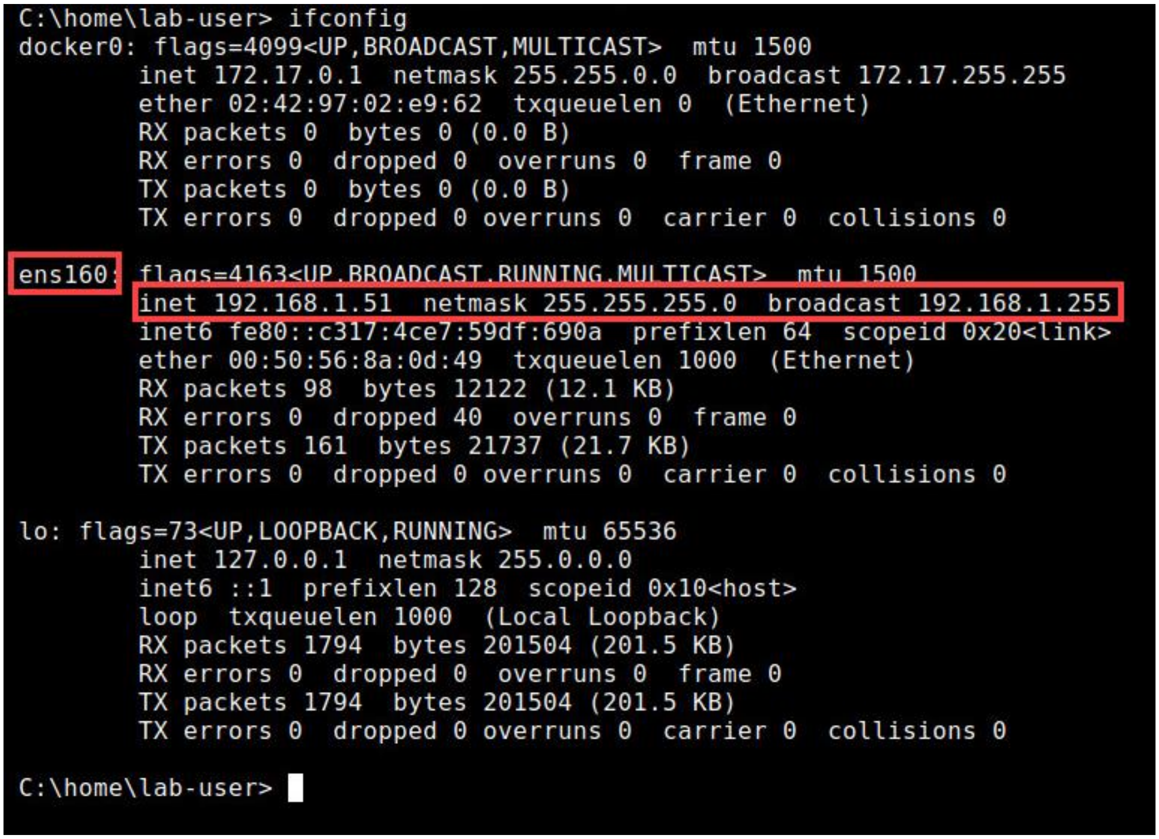
```
C:\home\lab-user> sudo ifconfig ens160 down
[sudo] password for lab-user:
C:\home\lab-user> █
```

10. With the *Terminal* window still open, type `sudo ifconfig ens160 up` and press **Enter.** Leave the *Terminal* window open for the next step



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

11. Type `ifconfig` and press **Enter**. This command will show the new lease from the DHCP server.



```
C:\home\lab-user> ifconfig
docker0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 172.17.0.1  netmask 255.255.0.0  broadcast 172.17.255.255
        ether 02:42:97:02:e9:62  txqueuelen 0  (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

ens160: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.51  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::c317:4ce7:59df:690a  prefixlen 64  scopeid 0x20<link>
        ether 00:50:56:8a:0d:49  txqueuelen 1000  (Ethernet)
        RX packets 98  bytes 12122 (12.1 KB)
        RX errors 0  dropped 40  overruns 0  frame 0
        TX packets 161  bytes 21737 (21.7 KB)
        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
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 1794  bytes 201504 (201.5 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1794  bytes 201504 (201.5 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

C:\home\lab-user>
```

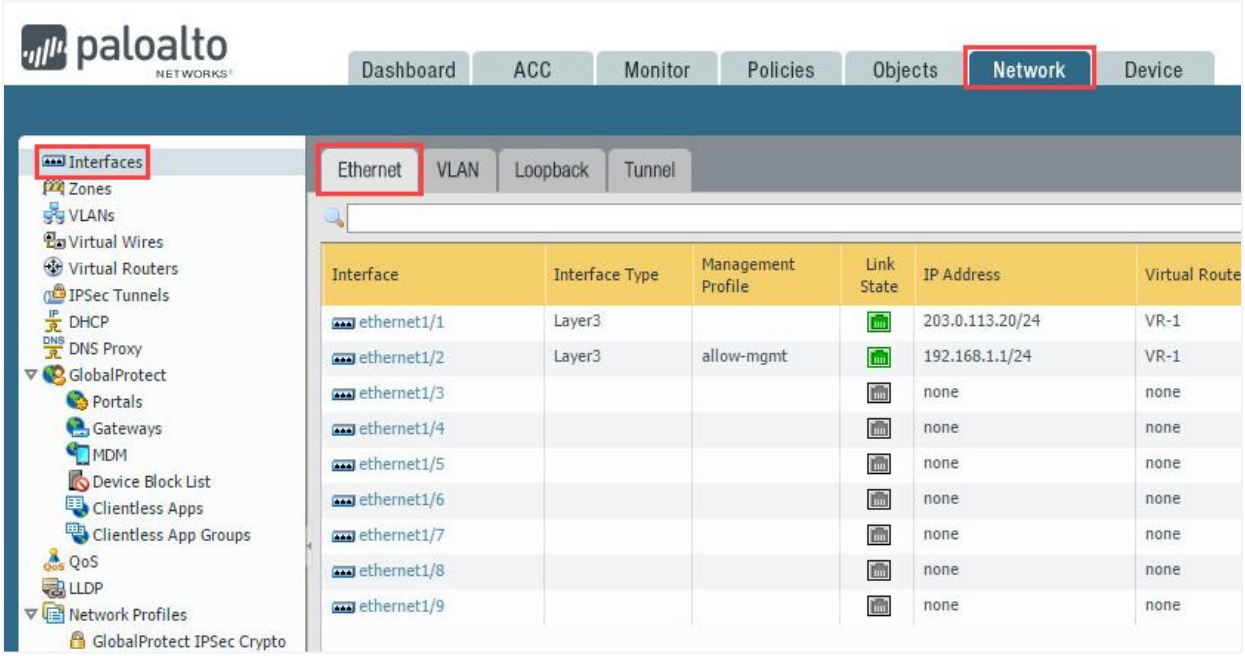
You should receive an IP address of **192.168.1.51**. This was the address you reserved for the Client machine on the firewall. If you receive a different address, repeat this section and take careful note of the MAC address.

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

1.4 Configure the Firewall Outside Interface for DHCP

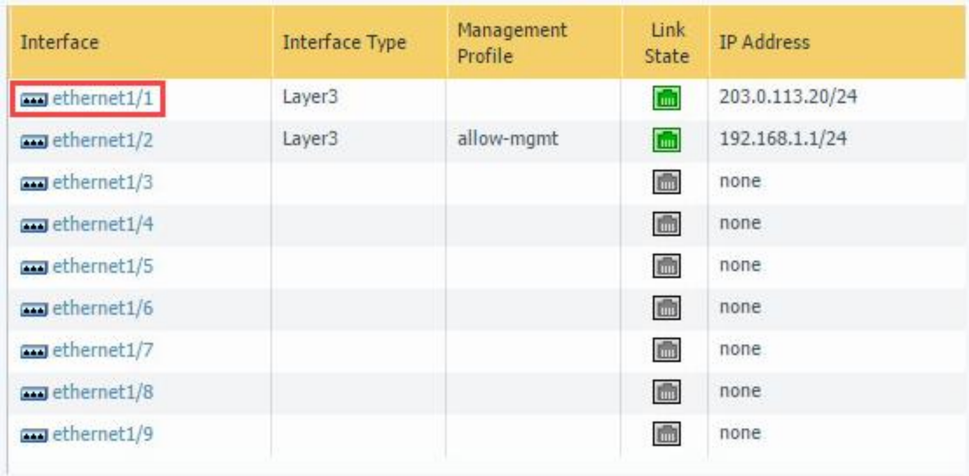
In this section, you will configure the Firewall outside interface for DHCP. Like the Client in the previous task, the Firewall will obtain an IP address from a DHCP server on the network.

1. On the Firewall administration page, navigate to **Network > Interfaces > Ethernet**.



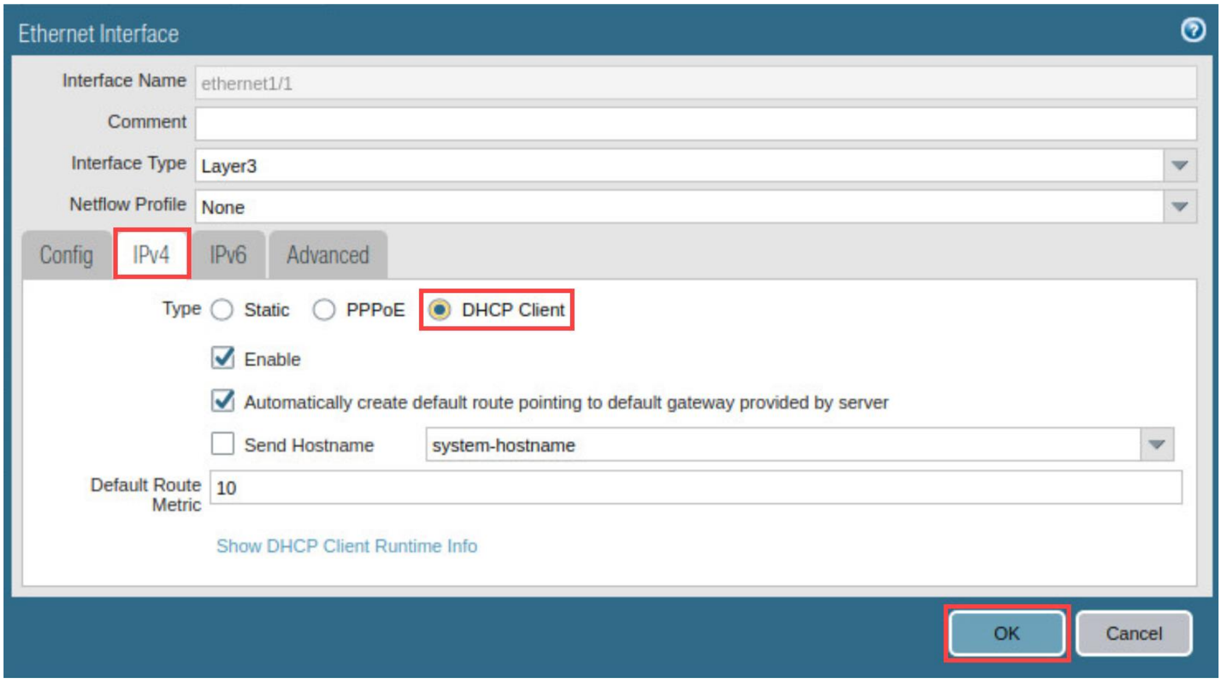
Interface	Interface Type	Management Profile	Link State	IP Address	Virtual Route
ethernet1/1	Layer3		🟩	203.0.113.20/24	VR-1
ethernet1/2	Layer3	allow-mgmt	🟩	192.168.1.1/24	VR-1
ethernet1/3			▨	none	none
ethernet1/4			▨	none	none
ethernet1/5			▨	none	none
ethernet1/6			▨	none	none
ethernet1/7			▨	none	none
ethernet1/8			▨	none	none
ethernet1/9			▨	none	none

2. Click on **ethernet1/1**.



Interface	Interface Type	Management Profile	Link State	IP Address
ethernet1/1	Layer3		🟩	203.0.113.20/24
ethernet1/2	Layer3	allow-mgmt	🟩	192.168.1.1/24
ethernet1/3			▨	none
ethernet1/4			▨	none
ethernet1/5			▨	none
ethernet1/6			▨	none
ethernet1/7			▨	none
ethernet1/8			▨	none
ethernet1/9			▨	none

3. 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.



Ethernet Interface

Interface Name: ethernet1/1
Comment:
Interface Type: Layer3
Netflow Profile: None

Type ○ Static ○ PPPoE ● DHCP Client

☑ Enable

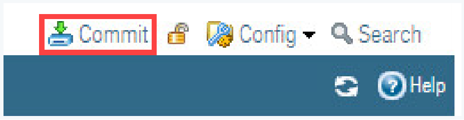
☑ Automatically create default route pointing to default gateway provided by server

□ Send Hostname: system-hostname

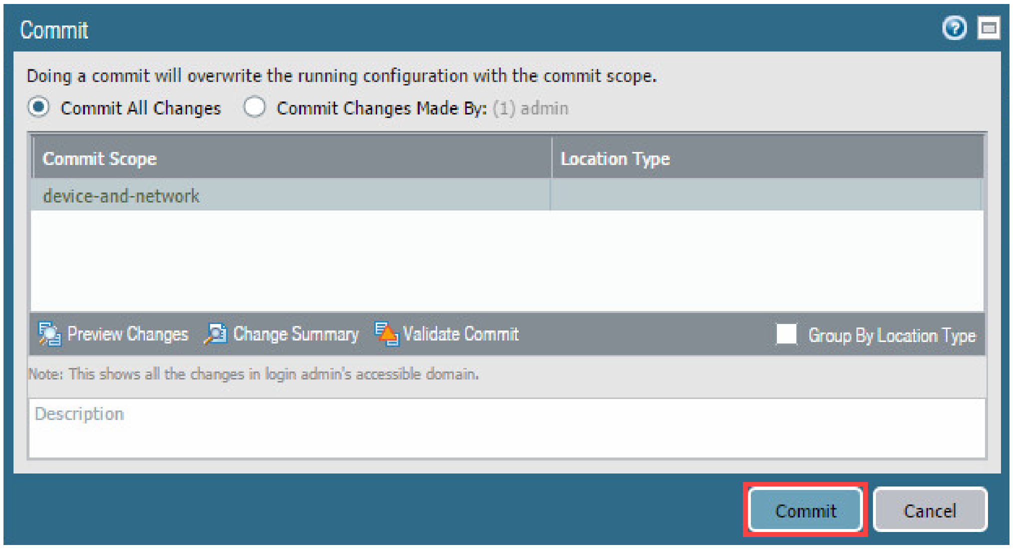
Default Route Metric: 10

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.

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



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



Doing a commit will overwrite the running configuration with the commit scope.

● Commit All Changes ○ Commit Changes Made By: (1) admin

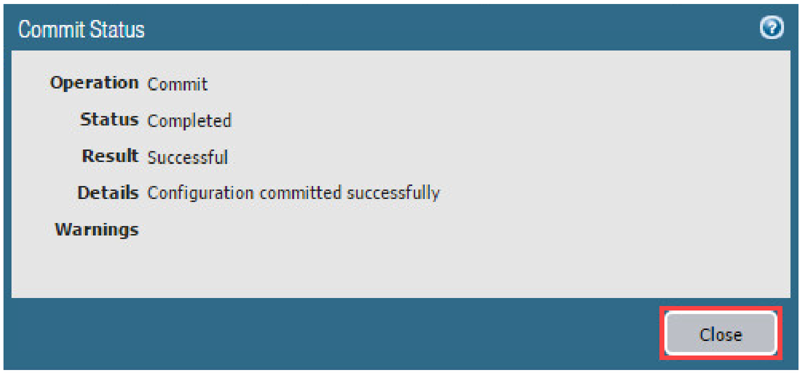
Commit Scope	Location Type
device-and-network	

□ Group By Location Type

Note: This shows all the changes in login admin's accessible domain.

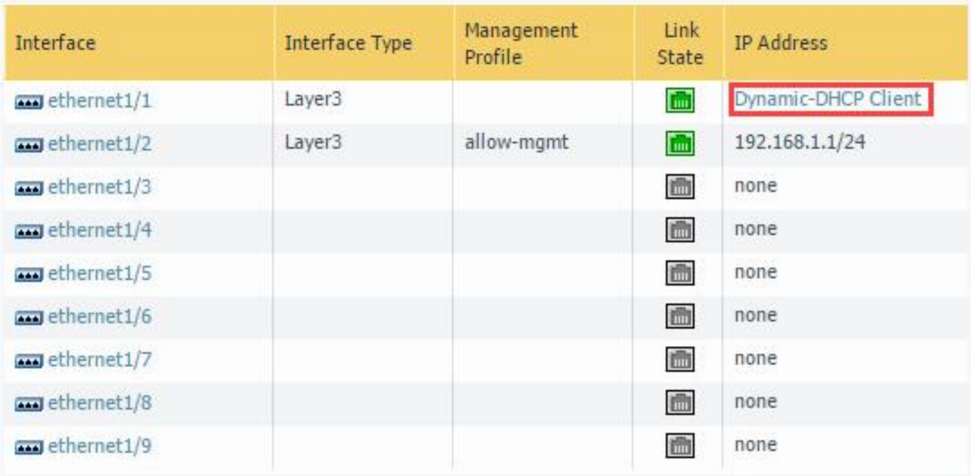
Description

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



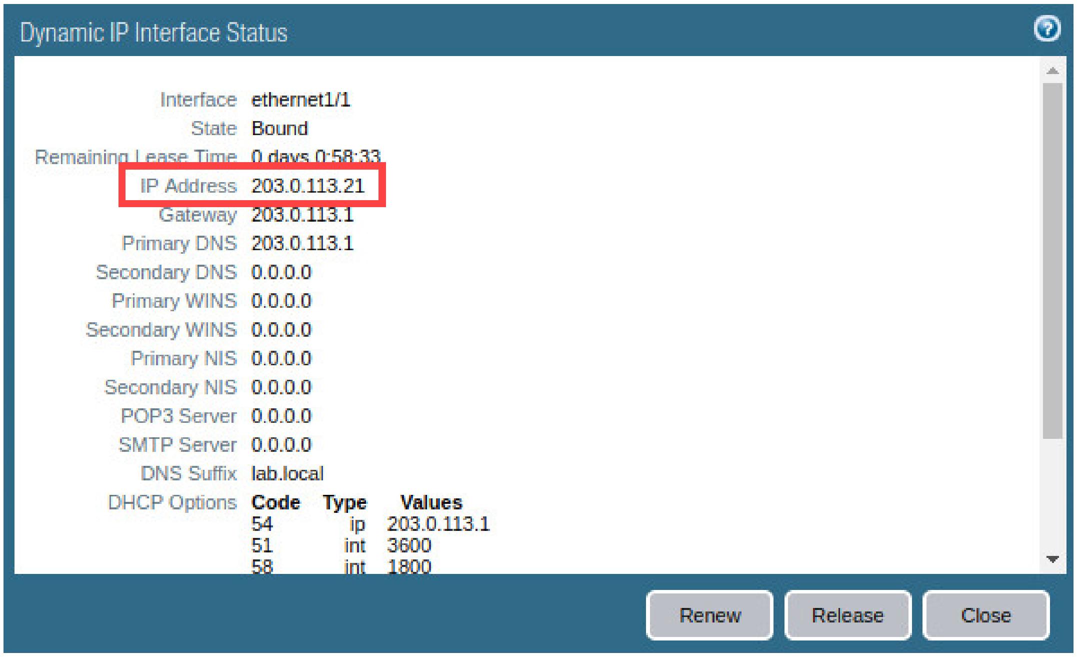
Operation Commit
Status Completed
Result Successful
Details Configuration committed successfully
Warnings

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



Interface	Interface Type	Management Profile	Link State	IP Address
ethernet1/1	Layer3		🟩	Dynamic-DHCP Client
ethernet1/2	Layer3	allow-mgmt	🟩	192.168.1.1/24
ethernet1/3			▨	none
ethernet1/4			▨	none
ethernet1/5			▨	none
ethernet1/6			▨	none
ethernet1/7			▨	none
ethernet1/8			▨	none
ethernet1/9			▨	none

8. 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.



Dynamic IP Interface Status

Interface	ethernet1/1
State	Bound
Remaining Lease Time	0 days 0:58:33
IP Address	203.0.113.21
Gateway	203.0.113.1
Primary DNS	203.0.113.1
Secondary DNS	0.0.0.0
Primary WINS	0.0.0.0
Secondary WINS	0.0.0.0
Primary NIS	0.0.0.0
Secondary NIS	0.0.0.0
POP3 Server	0.0.0.0
SMTP Server	0.0.0.0
DNS Suffix	lab.local

DHCP Options

Code	Type	Values
54	ip	203.0.113.1
51	int	3600
58	int	1800

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