NETWORK SECURITY FUNDAMENTALS

Lab 2: Configuring Virtual IP Addresses

Document Version: 2021-01-30

Contents

Introduction

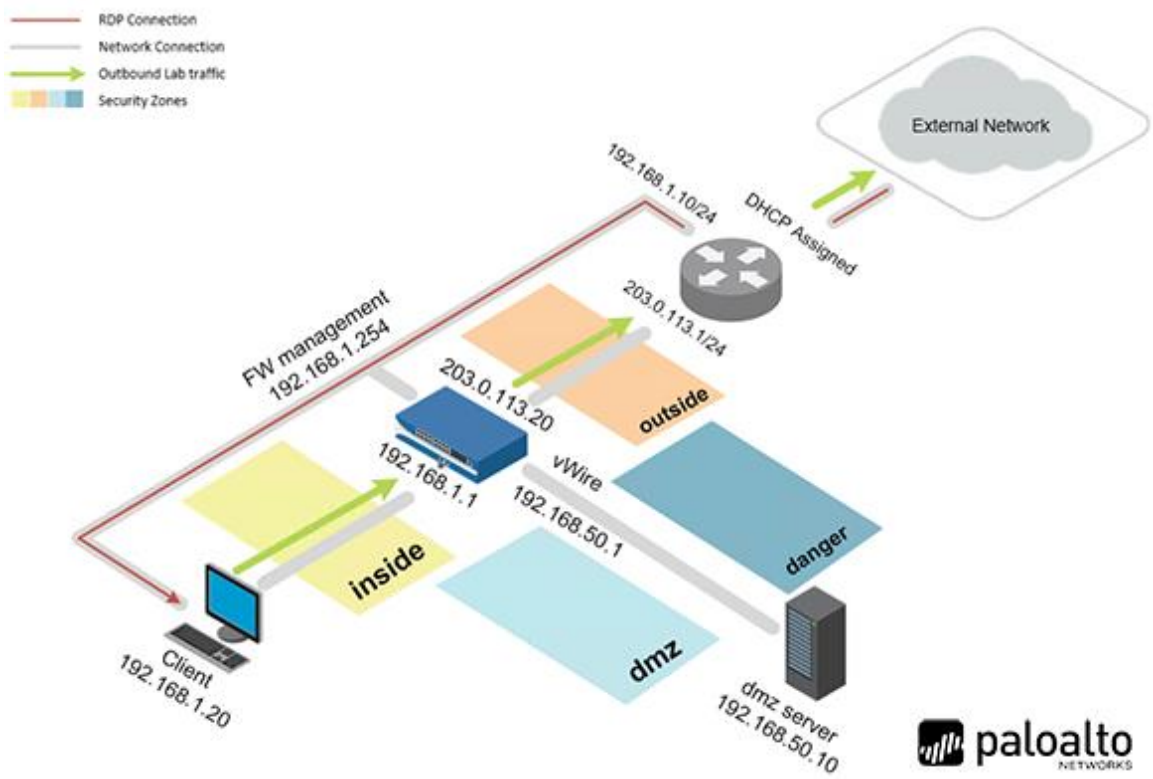
In this lab, you will configure the Palo Alto Networks Firewall inside interface with a virtual IP address.

Objective

In this lab, you will perform the following tasks:

- Configure a Virtual IP Address
- Configure a Virtual IP Address on another subnet

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.

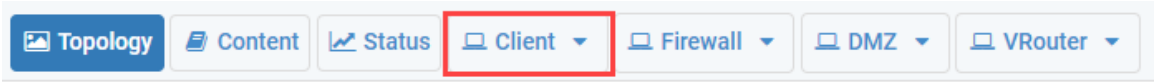
Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Client	192.168.1.20	lab-user	Train1ng$
DMZ	192.168.50.10	root	Pal0Alt0
Firewall	192.168.1.254	admin	Train1ng$

2 Configuring Virtual IP Addresses

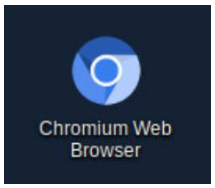
2.0 Load Lab Configuration

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

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

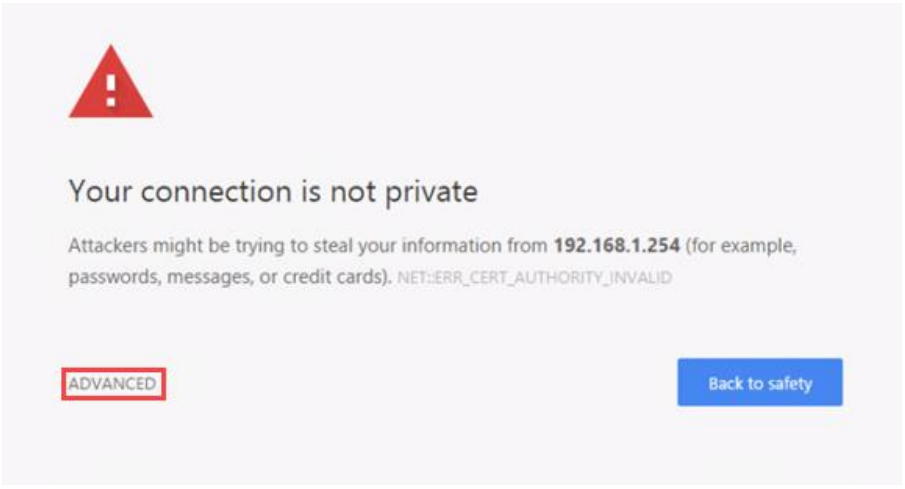


2. Log in to the Client PC as username `lab-user`, password `Train1ng$`.
3. Double-click the **Chromium Web Browser** icon located on the Desktop.



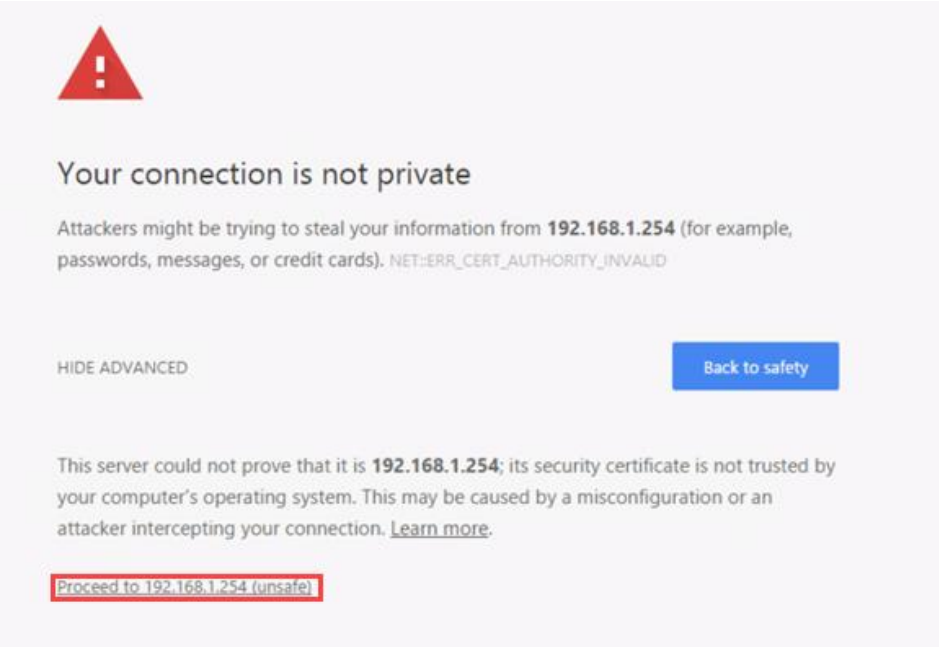
4. In the *Chromium* address field, type `https://192.168.1.254` and press **Enter**.

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



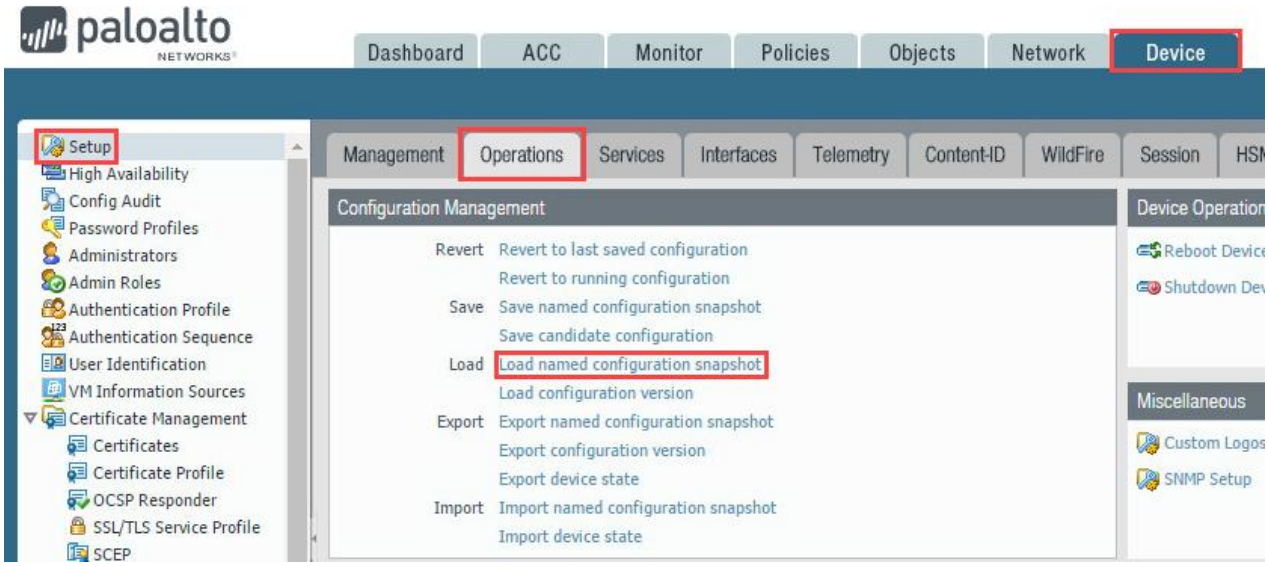
If you experience the "Unable to connect" or "502 Bad Gateway" message while attempting to connect to the specified IP above, please wait an additional 1-3 minutes for the Firewall to fully initialize. Refresh the page to continue.

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

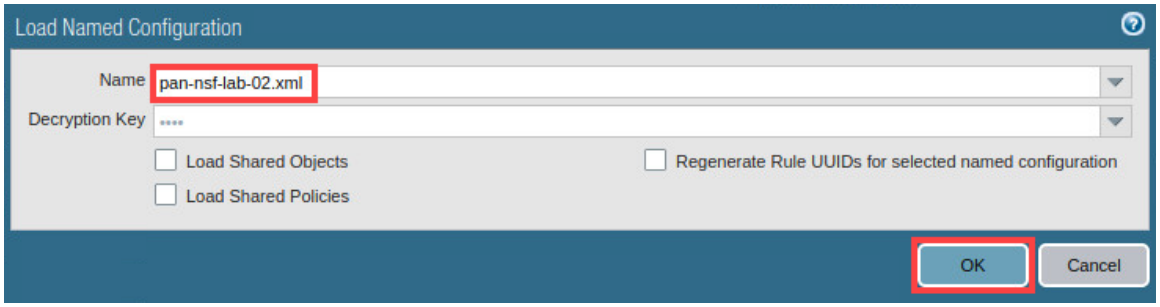


7. Log in to the Firewall web interface as username **`admin`**, password **`Train1ng$.`**

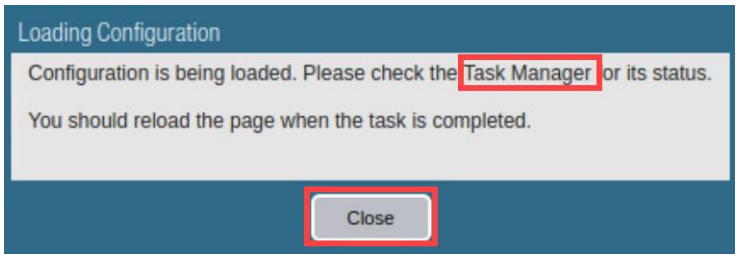
8. In the web interface, navigate to **Device > Setup > Operations** and click on **Load named configuration snapshot** underneath the *Configuration Management* section.



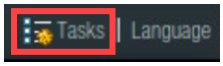
9. In the *Load Named Configuration* window, select **pan-nsf-lab-02.xml** from the *Name* dropdown box and click **OK**.



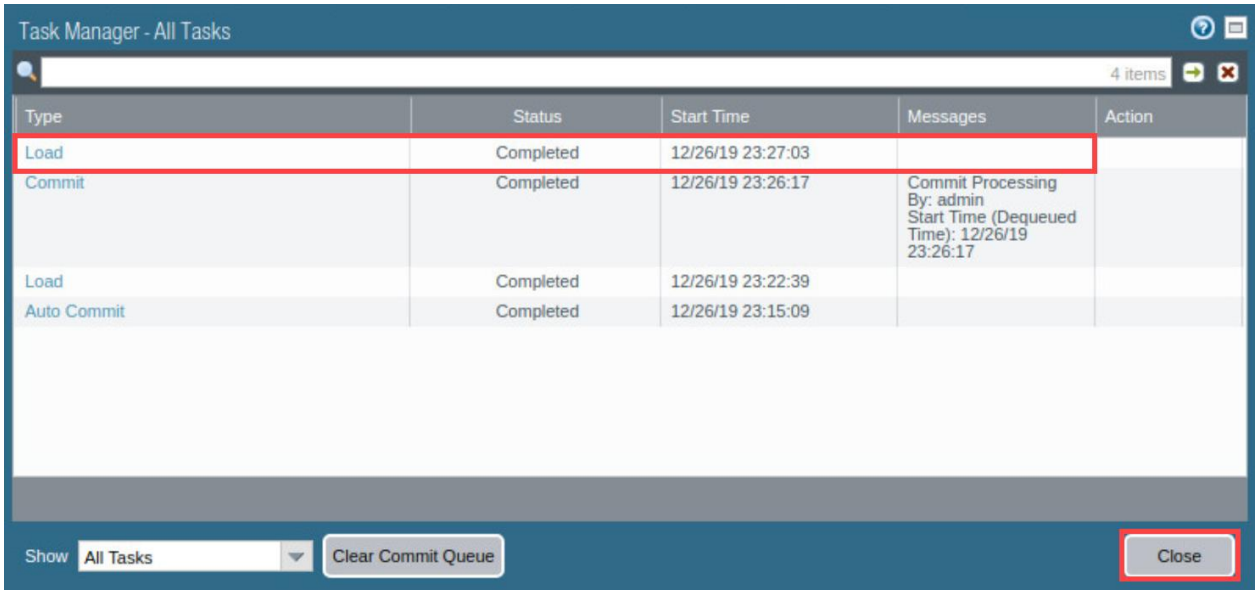
10. In the Loading Configuration window, a message will show *Configuration is being loaded. Please check the Task Manager for its status. You should reload the page when the task is completed.* Click **Close** to continue.



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

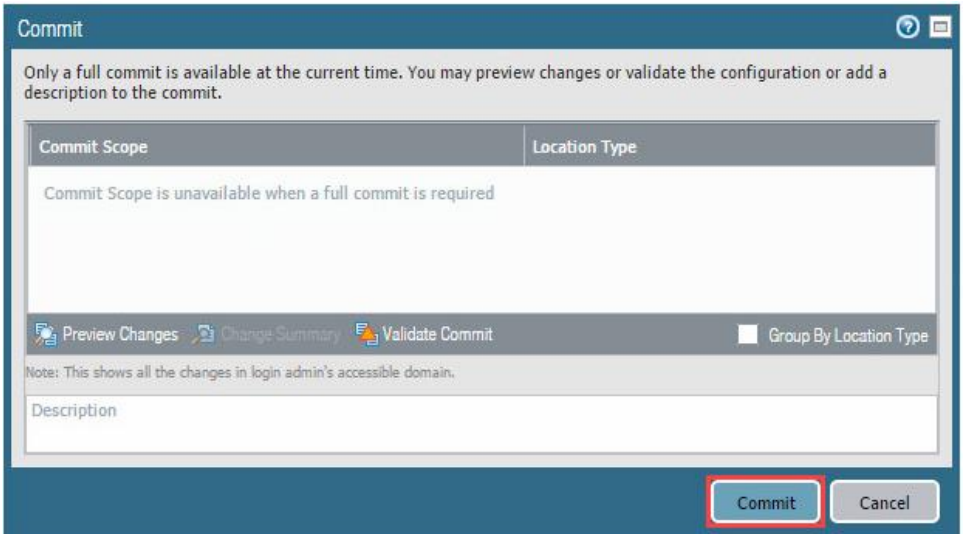


12. In the *Task Manager – All Tasks* window, verify the *Load* type has successfully completed. Click **Close.**

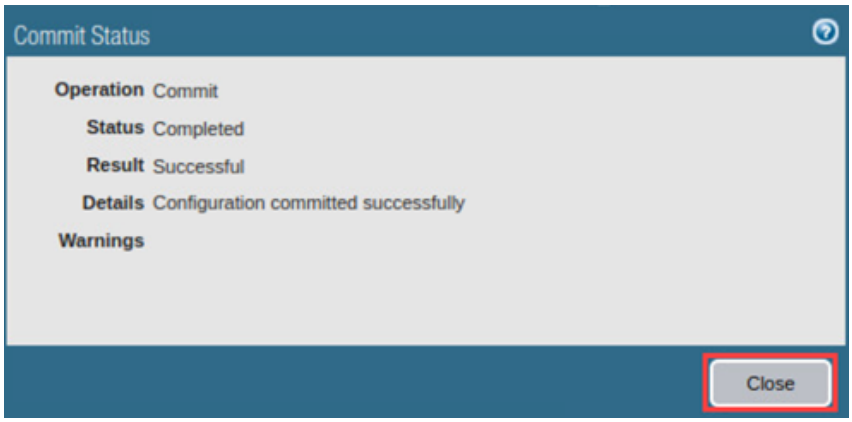


13. Click the **Commit** link located at the top-right of the web interface.

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



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



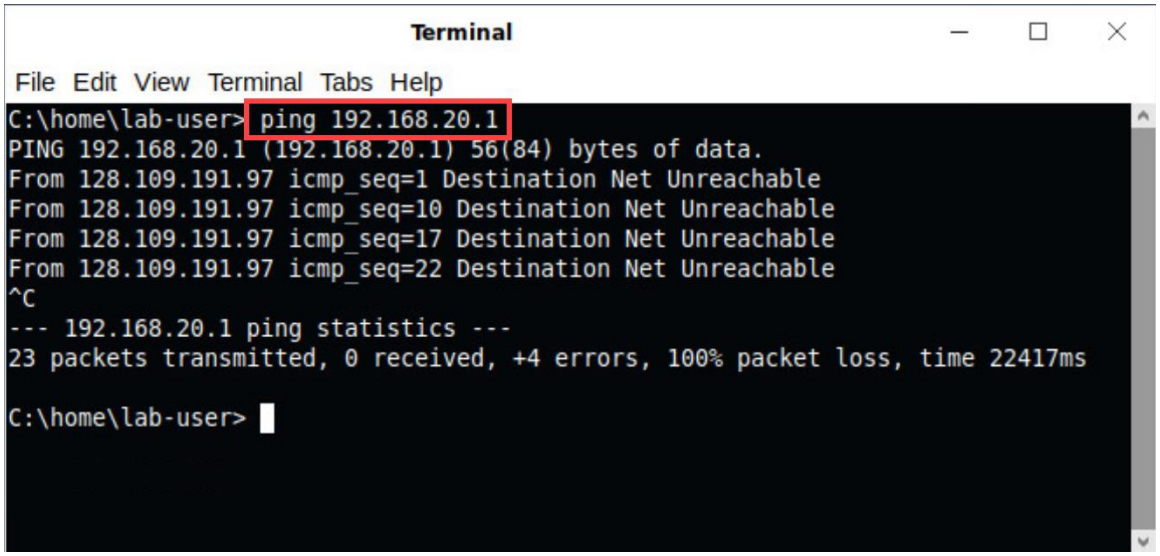
16. The commit process takes changes made to the Firewall and copies them to the running configuration, which will activate all configuration changes since the last commit.

2.1 Configure a Virtual IP Address

In this section, you will configure a virtual IP address **192.168.20.1** on the Firewall. Creating a virtual IP address allows the Firewall to communicate with multiple IP networks from a single physical interface**.**

1. Refer to the topology and note there is currently nothing assigned with the IP address **192.168.20.1**.
2. You can confirm you cannot reach **192.168.20.1** by utilizing the *ping* utility. Click on the **Xfce Terminal** icon in the taskbar.

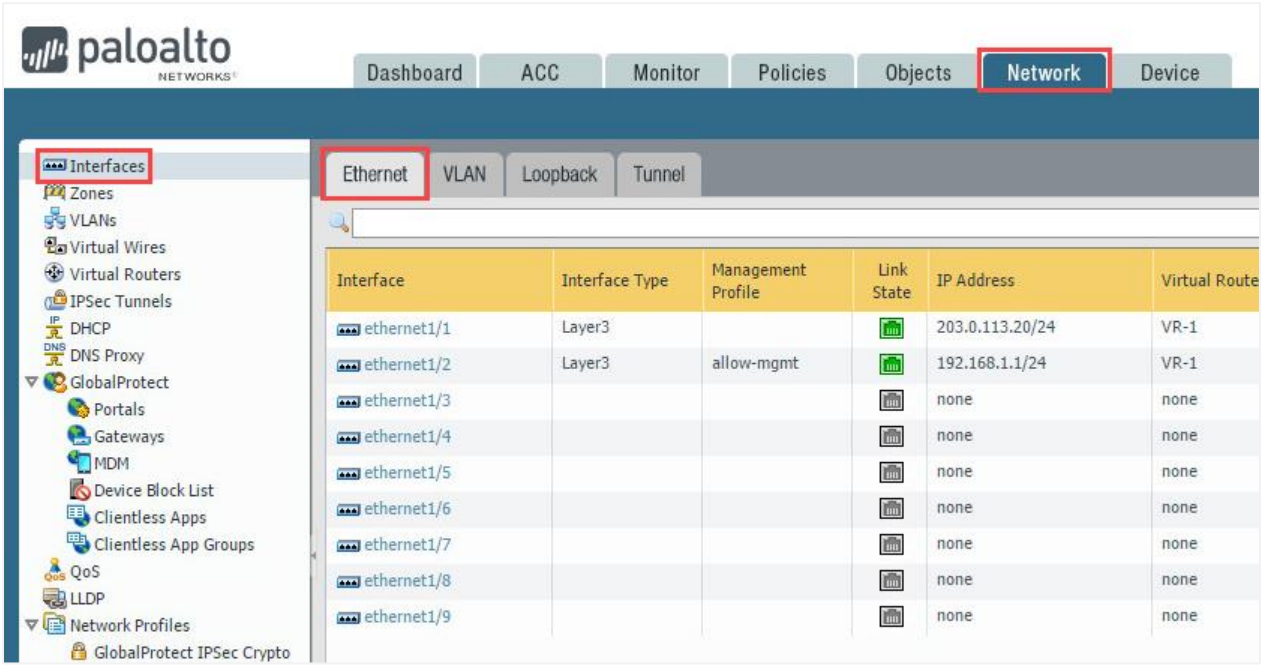
3. In the *Terminal* window, try pinging 192.168.20.1 by typing **`ping 192.168.20.1`** and pressing **Enter**. To stop the ping, type **Ctrl+C**.



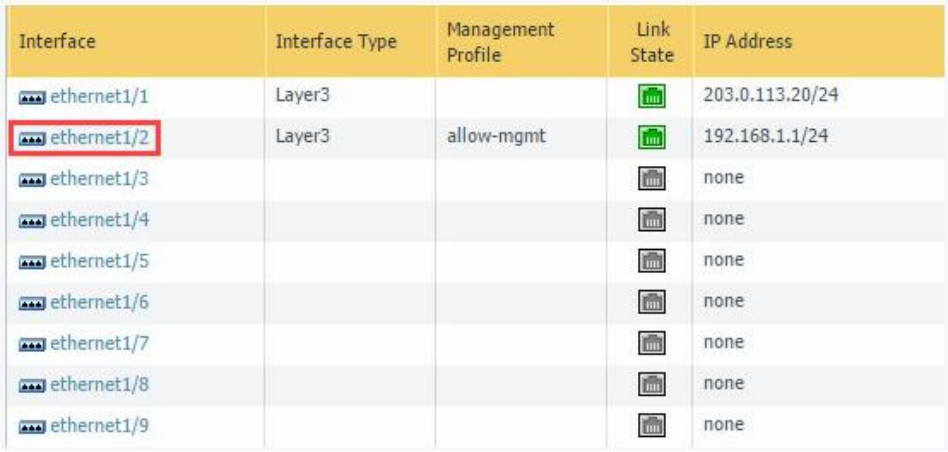
Notice, you receive **Destination net unreachable** and possibly **Request timed out**. These responses indicate that the Client cannot reach anyone at that IP address. By default, the Client's default gateway is **192.168.1.1**, which is the Firewall inside interface. The responses come from **203.0.113.1**, which means the Firewall had no routes to the **192.168.20.0** network and forwarded those requests to its default gateway **203.0.113.1**. From this information you can reasonably assume **192.168.20.1**, for this lab environment, does not exist on the network.

4. Type **`exit`** and press **Enter** to close the command prompt.

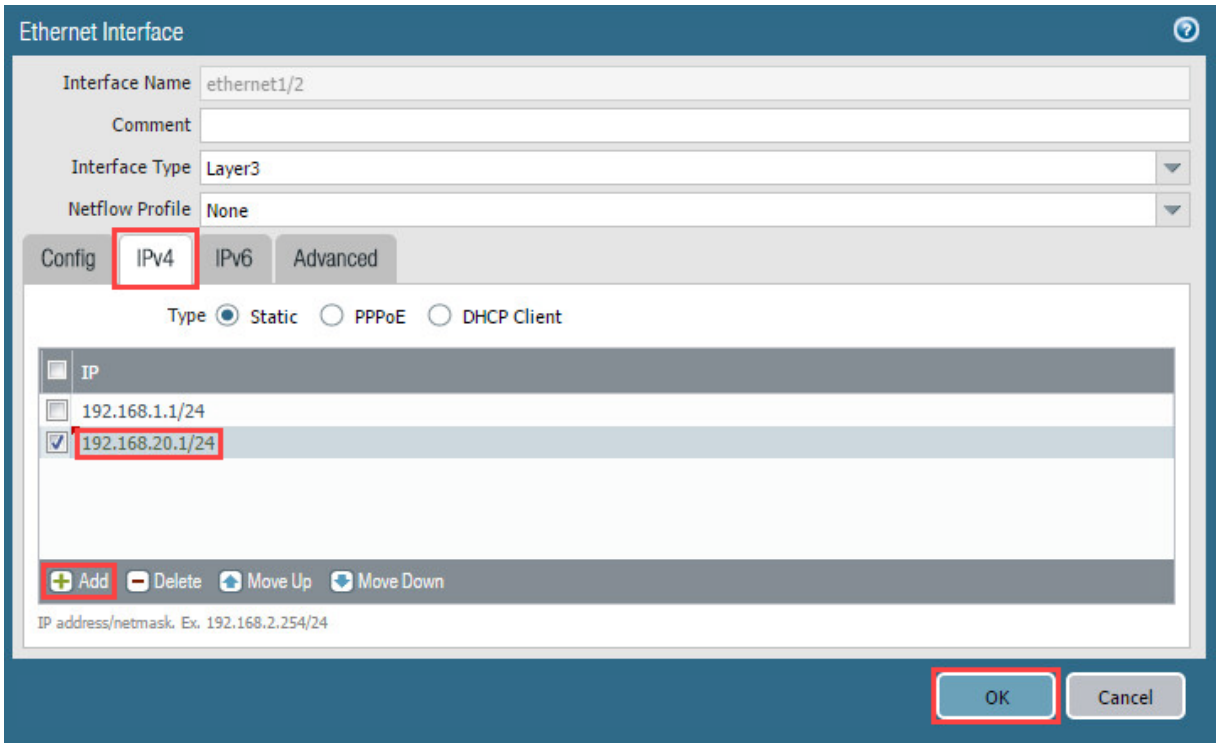
5. On the Firewall administration page, navigate to **Network > Interfaces > Ethernet**.



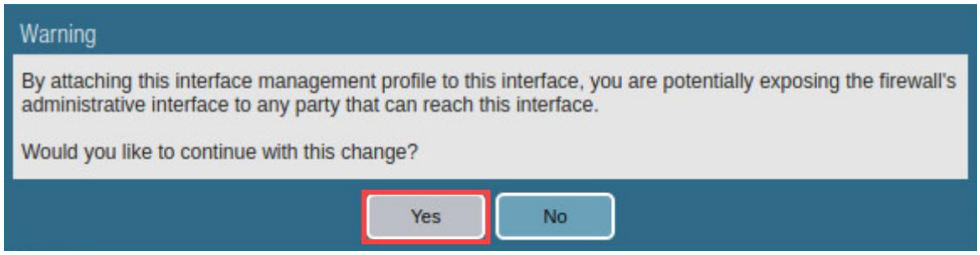
6. Click on **ethernet1/2**.



7. First, click on the **IPv4** tab. Then, in the bottom-left of the window, click on the **Add** button. Next, type `192.168.20.1/24` in the *IP address* field, press **Enter**. Finally, click the **OK** button.



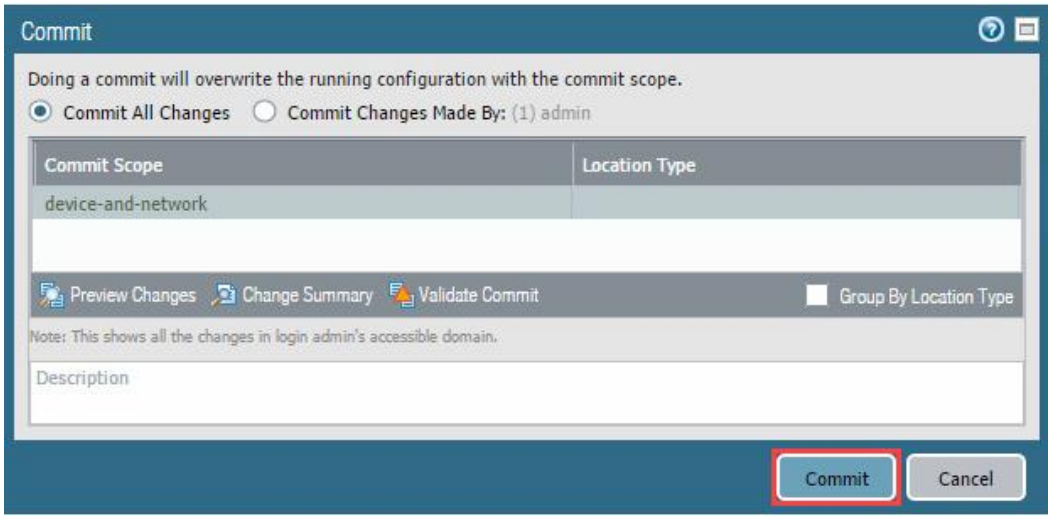
8. In the *Warning* window, click **Yes**.



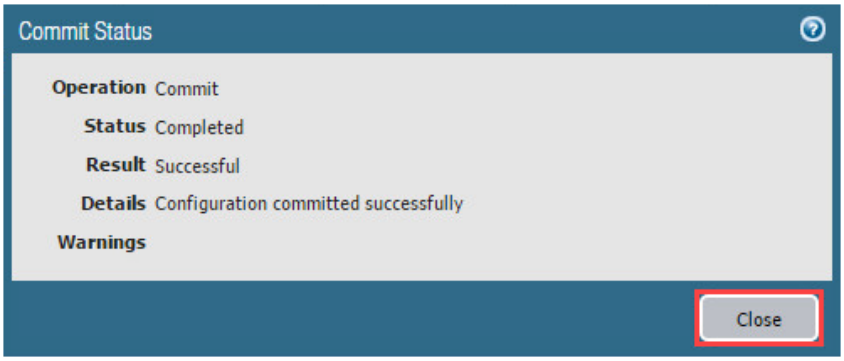
The *Warning* advises that if you attach this interface management profile to this interface, you are potentially exposing the firewall's administrative interface to any party that can reach this interface. For the purpose of this lab, you will bypass this warning knowing that it is not good practice to attach a management profile to a production interface.

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

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

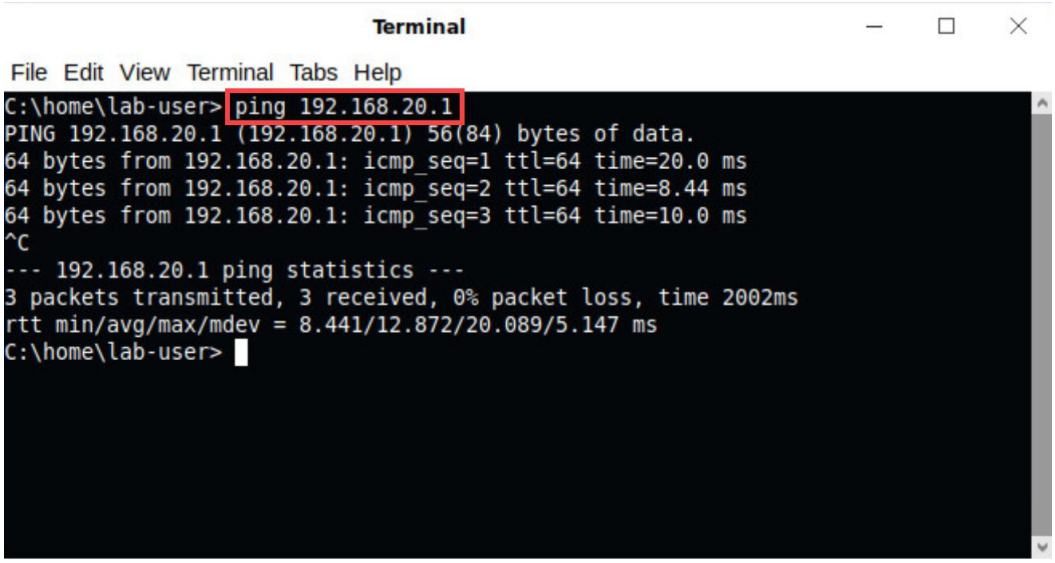


11. When the commit operation successfully completes, click **Close** to continue.



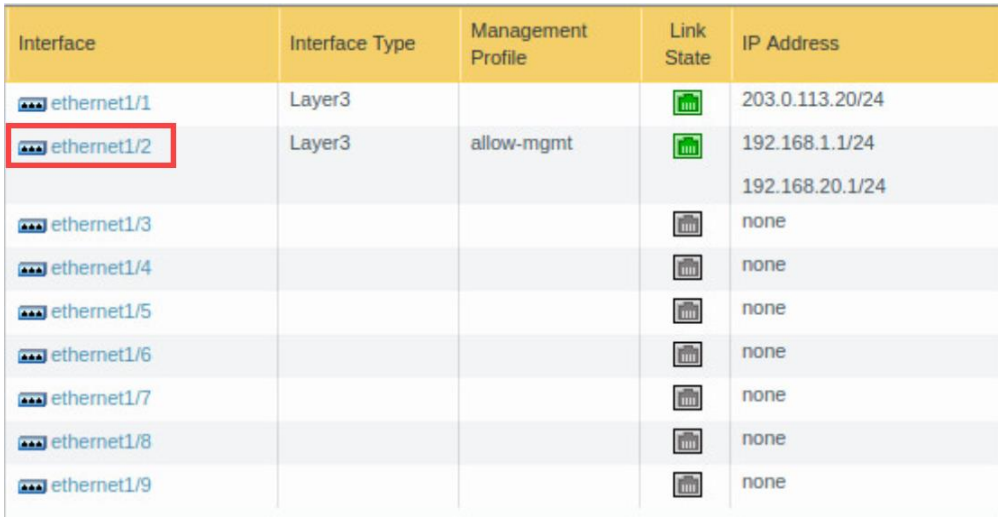
12. Click on the **Xfce Terminal** icon in the taskbar.

13. To confirm the Firewall is configured with IP address 192.168.20.1**,** type **`ping 192.168.20.1`** and press **Enter**. To stop the ping, click **Ctrl+C**.



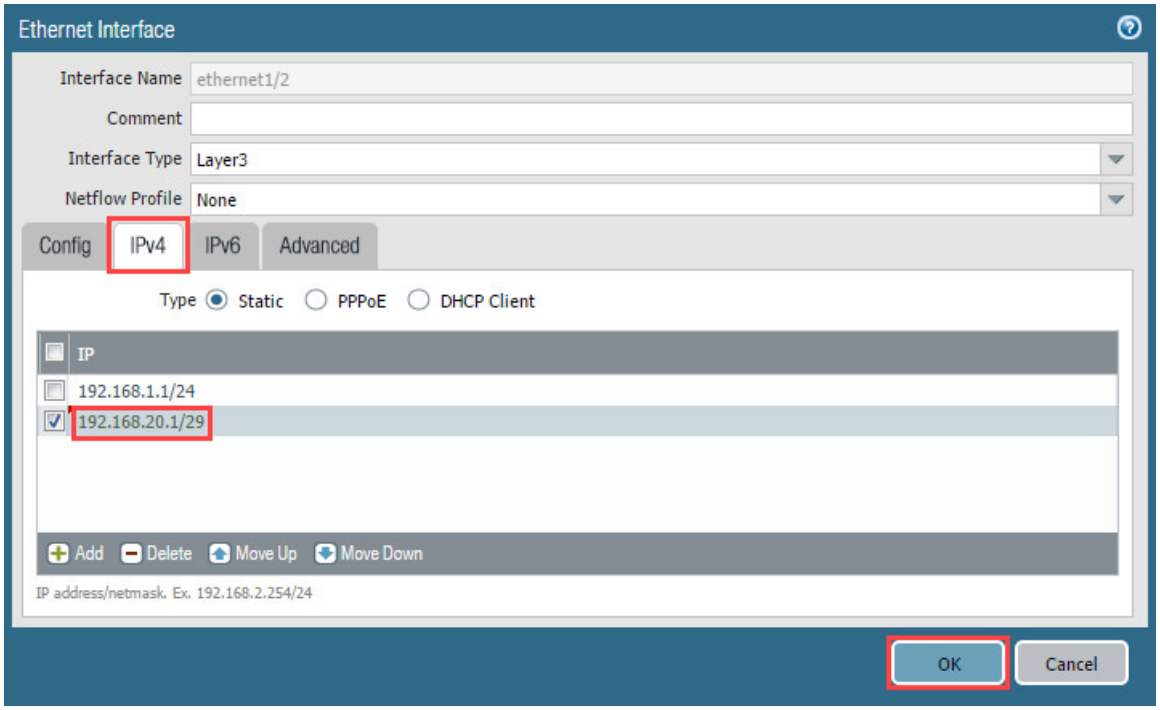
Notice, you will now receive replies from **192.168.20.1**, the Firewall, even though it is on a different network because it is a virtual network on the Palo Alto interface.

14. Type **`exit`** and press **Enter** to close the command prompt.
15. On the Firewall administration page, click on **ethernet1/2**.

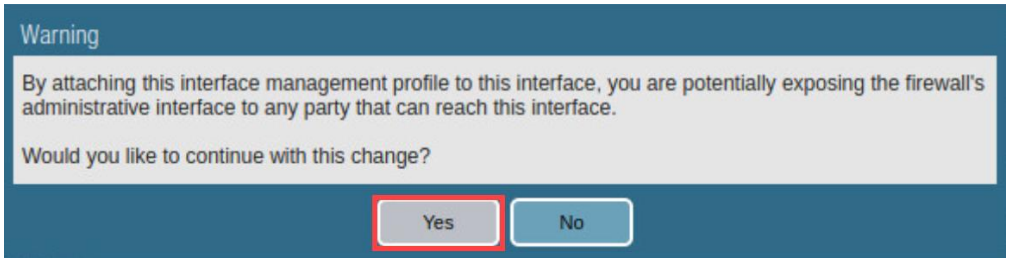


Interface	Interface Type	Management Profile	Link State	IP Address
ethernet1/1	Layer3			203.0.113.20/24
ethernet1/2	Layer3	allow-mgmt		192.168.1.1/24 192.168.20.1/24
ethernet1/3				none
ethernet1/4				none
ethernet1/5				none
ethernet1/6				none
ethernet1/7				none
ethernet1/8				none
ethernet1/9				none

16. Click on the **IPv4** tab. Click on **192.168.20.1/24** to edit the entry. Change to `192.168.20.1/29`. Press **Enter** and click the **OK** button.



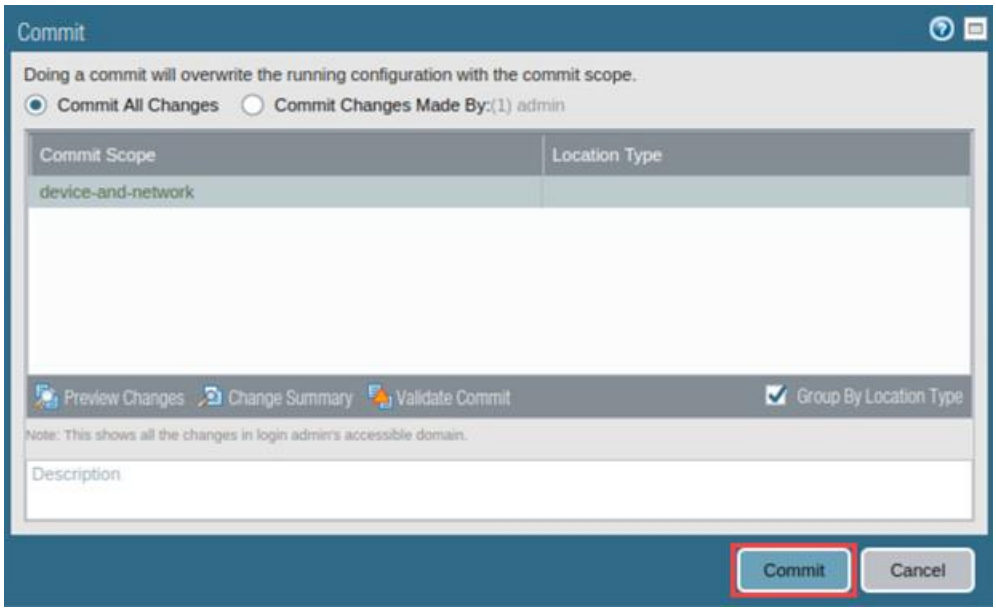
17. In the *Warning* window, click **Yes**.



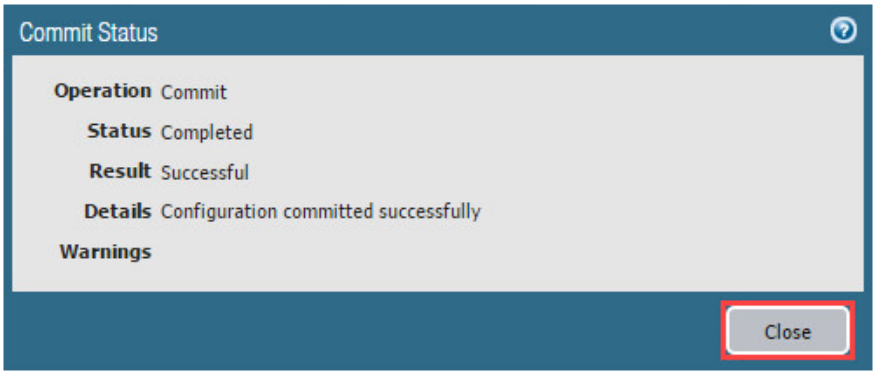
The *Warning* advises that if you attach this interface management profile to this interface, you are potentially exposing the firewall's administrative interface to any party that can reach this interface. For the purpose of this lab, you will bypass this warning knowing that it is not good practice to attach a management profile to a production interface.

18. Click on the **Commit** link on the top-right of the web interface.

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

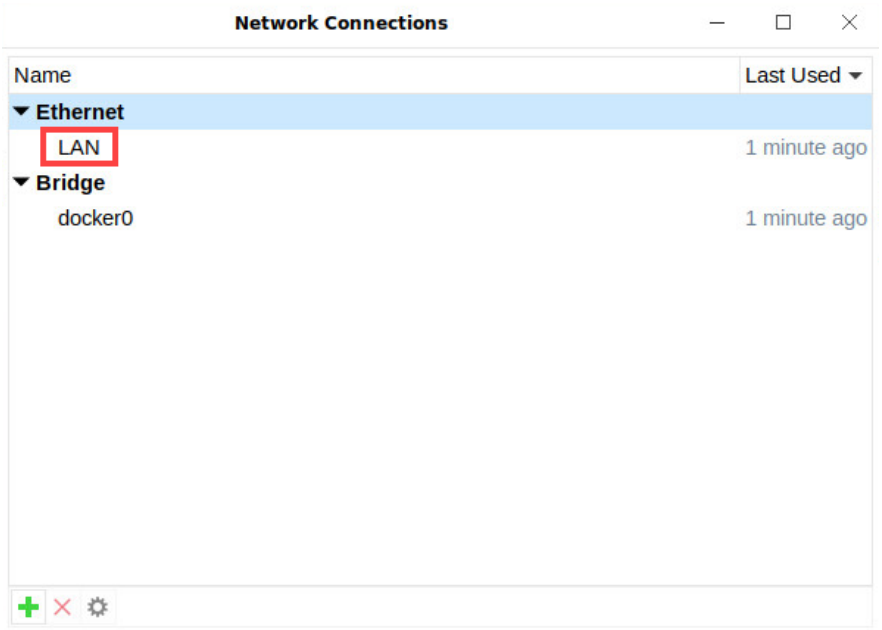


20. When the commit operation successfully completes, click **Close** to continue.

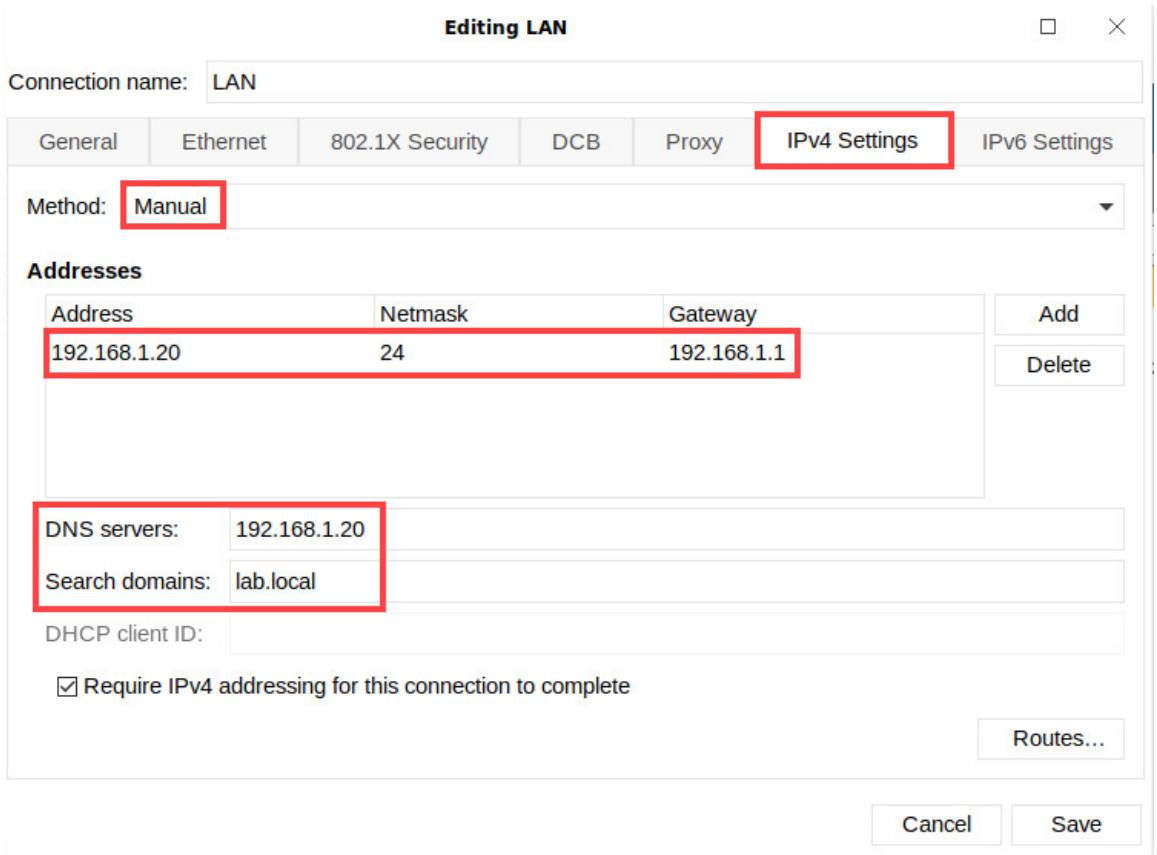


21. Click on the **Connection** icon in the lower-right of the web Client. Next, click on **Edit Connections...**

22. In the *Network Connections* window, double-click **LAN**.

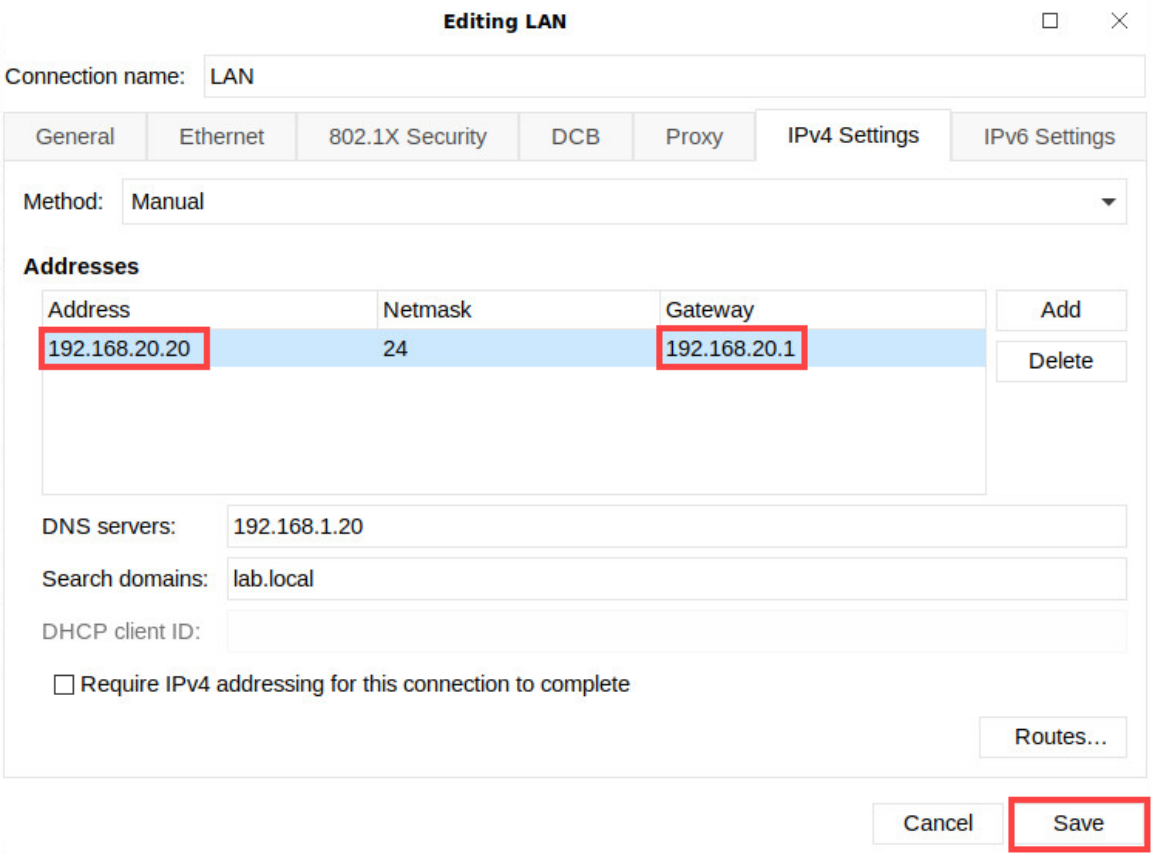


23. In the *Editing LAN* window, click **IPv4 Settings.** Leave the *Editing LAN* window open for the next step.

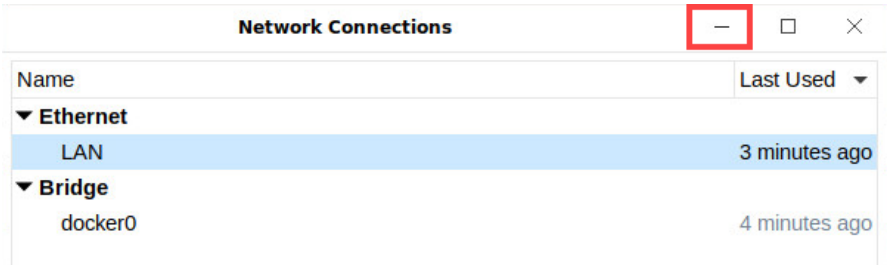


Notice that the method is set to **Manual**. By default, in this lab environment, the Client is configured with a static IP address of **192.168.1.20**, a Netmask of **24** which is **255.255.255.0**, a default gateway of **192.168.1.1**. The DNS server is set to **192.168.1.20** and the search domain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

24. In the *IP address* field, change it from `192.168.1.20` to `192.168.20.20`, and change the *Default Gateway* field to `192.168.20.1`. Click the **Save** button to close the *Editing LAN* window.

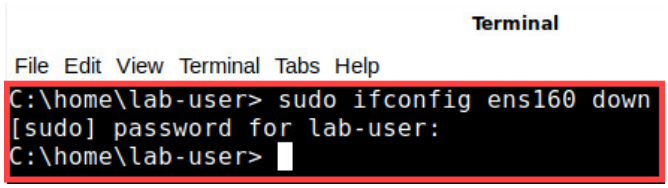


25. Minimize the *Network Connections* window.

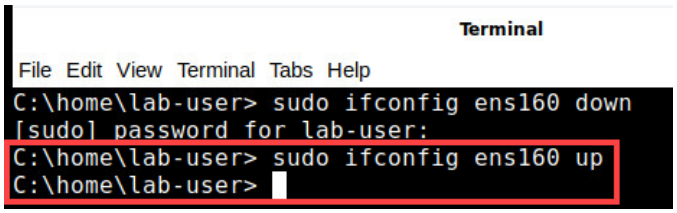


26. Click on the **Xfce Terminal** icon in the taskbar.

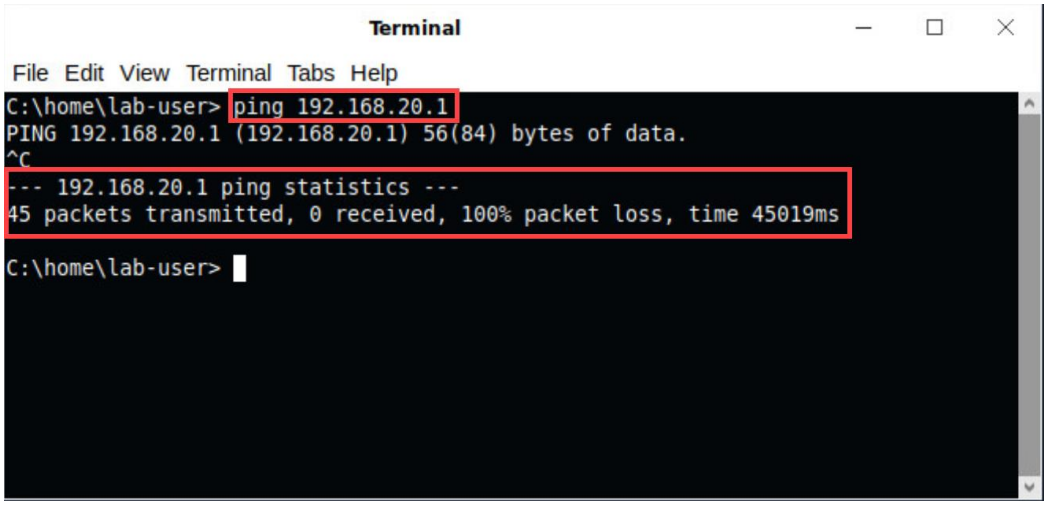
27. In the *Terminal* window, type **`sudo ifconfig ens160 down`**. Enter the **`Train1ng$`** password when prompted, and press **Enter**. Leave the *Terminal* window open for the next step.



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

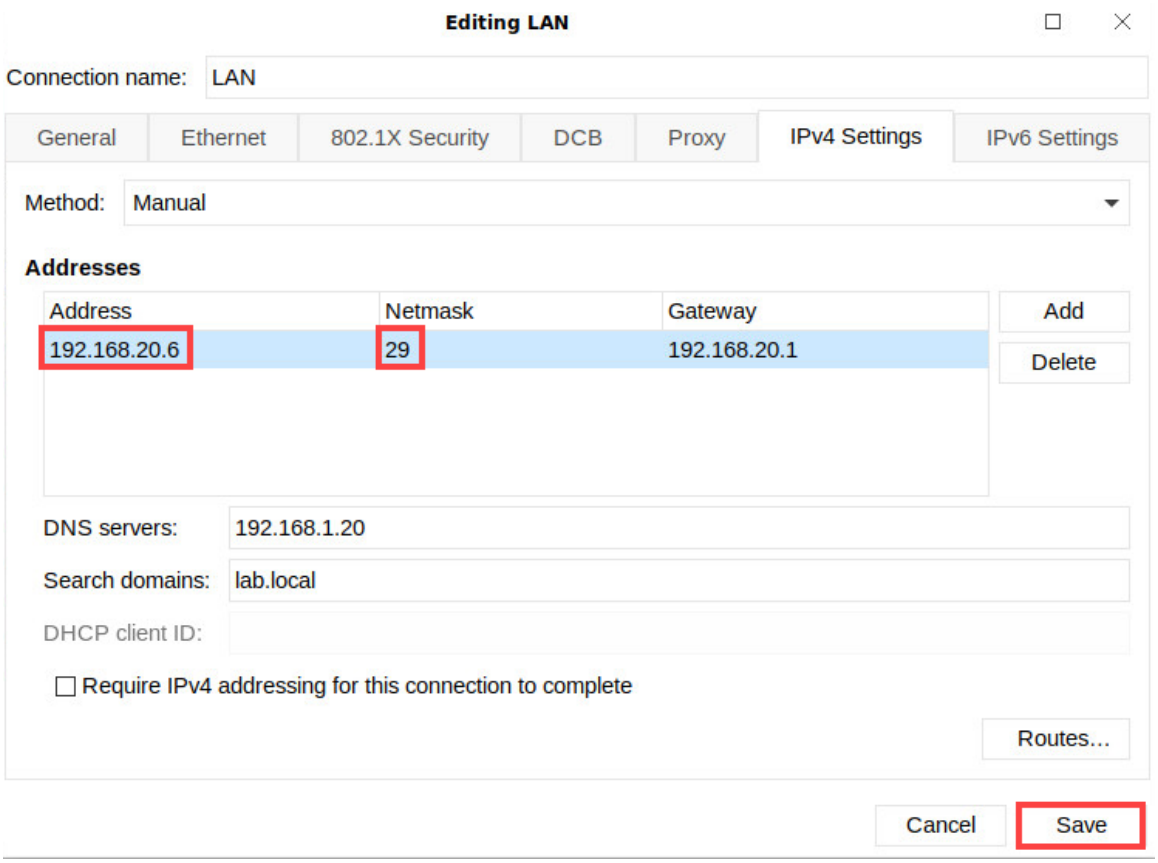


29. To ping the virtual IP address on the Firewall, type **`ping 192.168.20.1`** and press **Enter**. Give the *Terminal* window approximately 1 minute and stop the ping by clicking **Ctrl+C**.



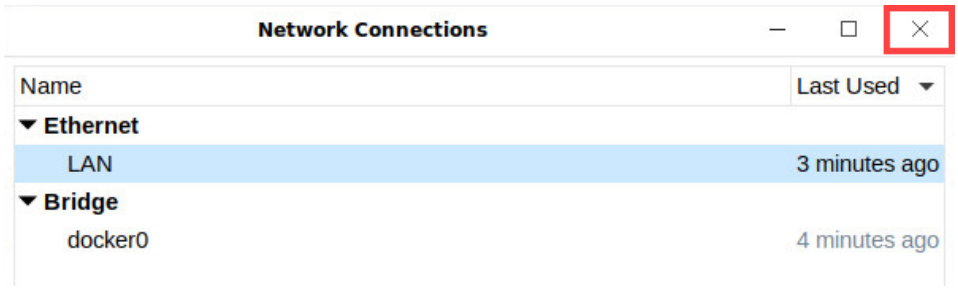
The ping will fail because the Firewall's virtual IP address, **192.168.20.1**, has a network mask of **/29** (255.255.255.248). The **192.168.20.0/29** network can only have an IP range of **192.168.20.1 – 192.168.20.6**, with **192.168.20.0** being the network address, and **192.168.20.7** being the broadcast address. For the ping to succeed, the Client, configured for IP address of **192.168.20.20** does not fall in the IP range.

30. Type `exit` and press **Enter** to close the command prompt.
31. Switch back to the *Editing LAN* window. Click on the **IPv4 tab**. Change the *IP address* from `192.168.20.20` to `192.168.20.6` and change the *Netmask* field from `/24 CIDR` to `/29 CIDR`. Click on the **Save** button to save the change.



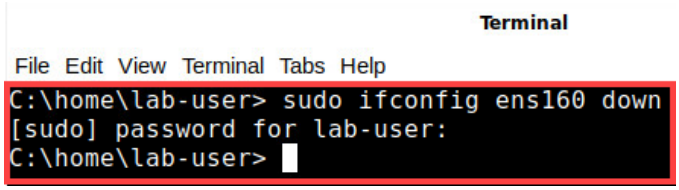
Note that CIDR is a condensed representation of an IP address's routing prefix based on subnetting.

32. Click **Close** on the *Network Connections* window.

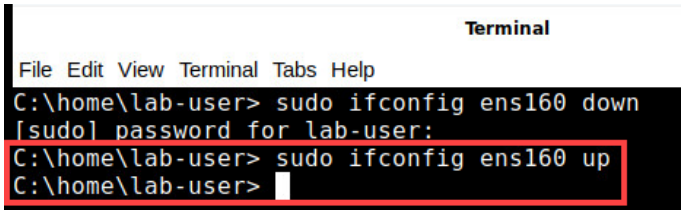


33. Click on the **Xfce Terminal** icon in the taskbar.

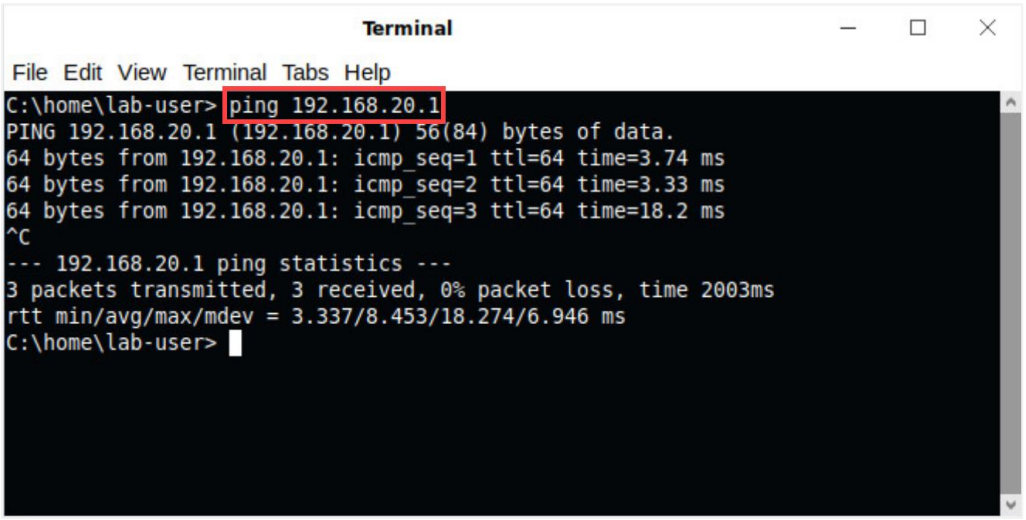
34. In the *Terminal* window, type **`sudo ifconfig ens160 down`**. Enter the **`Train1ng$`** password when prompted, and press **Enter**. Leave the *Terminal* window open for the next step.



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



36. Type **`ping 192.168.20.1`** and press **Enter**. To stop the ping, click **Ctrl+C**.



The ping will now respond because the Client is in the same network as the Firewall's virtual IP address.

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

