CYBERSECURITY FOUNDATION V2

Lab 1: Configuring TCP/IP and a Virtual Router

Document Version: 2022-12-22

Contents

Introduction

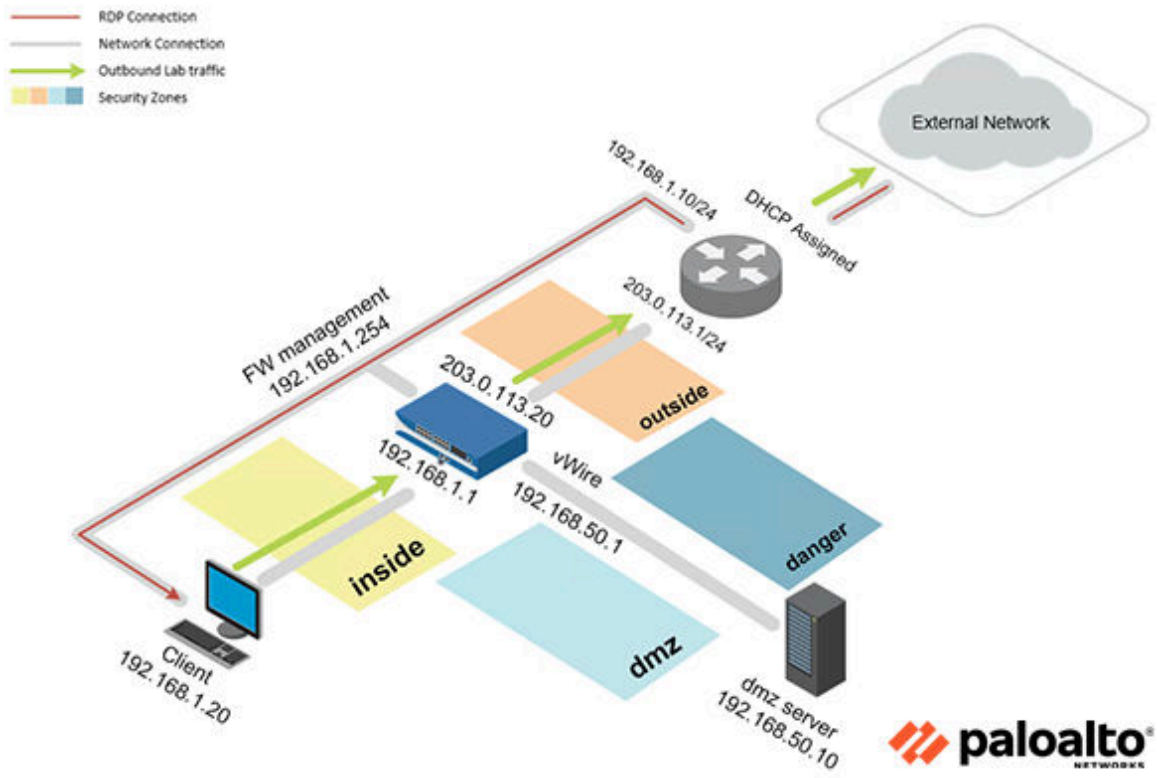
In this lab, you will configure Ethernet interfaces on the Palo Alto Networks Firewall with Layer 3 information, create a Virtual Router to allow traffic, and verify network connectivity.

Objective

In this lab, you will perform the following tasks:

- Configure Ethernet interfaces with Layer 3 Information
- Create a Virtual Router
- Verify the Network Connectivity

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.

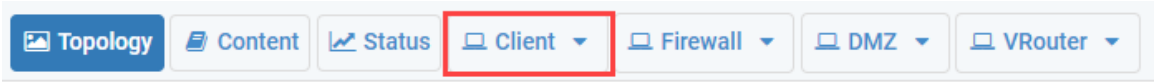
Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Client	192.168.1.20	`lab-user`	`Pal0Alt0!`
DMZ	192.168.50.10	`root`	`Pal0Alt0!`
Firewall	192.168.1.254	`admin`	`Pal0Alt0!`

1 Configuring TCP/IP and a Virtual Router

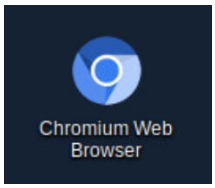
1.0 Load Lab Configuration

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

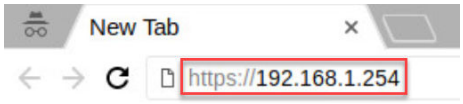
1. Click on the **Client** tab to access the Client PC.



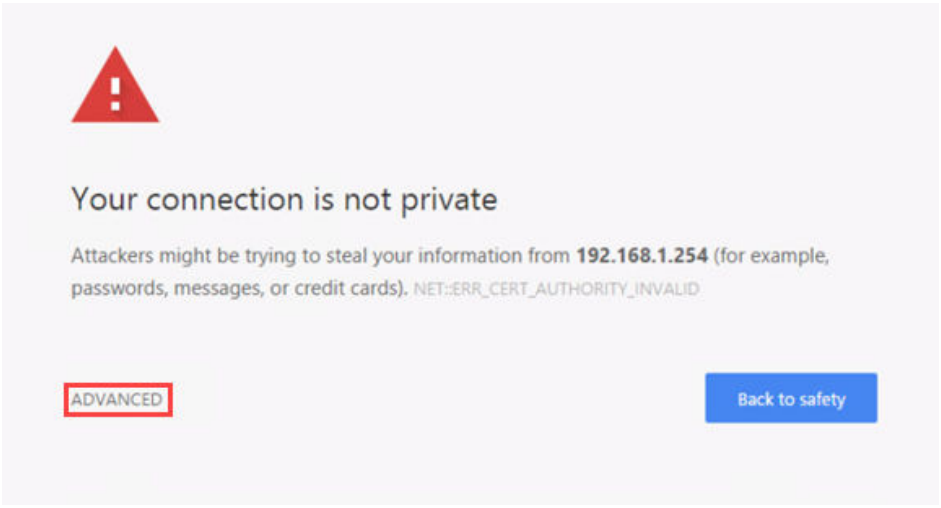
2. Log in to the Client PC as username `lab-user`, password `Pal0Alt0!`.
3. Double-click the **Chromium Web Browser** icon, located on the Desktop.



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

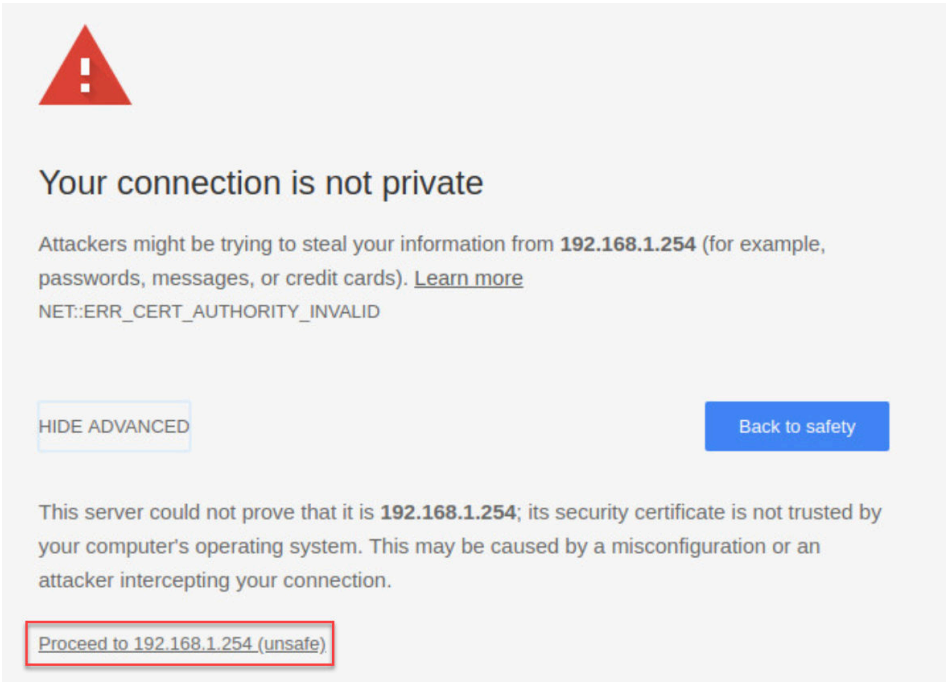


5. You will see a "*Your connection is not private*" message. Click on the **ADVANCED** link.



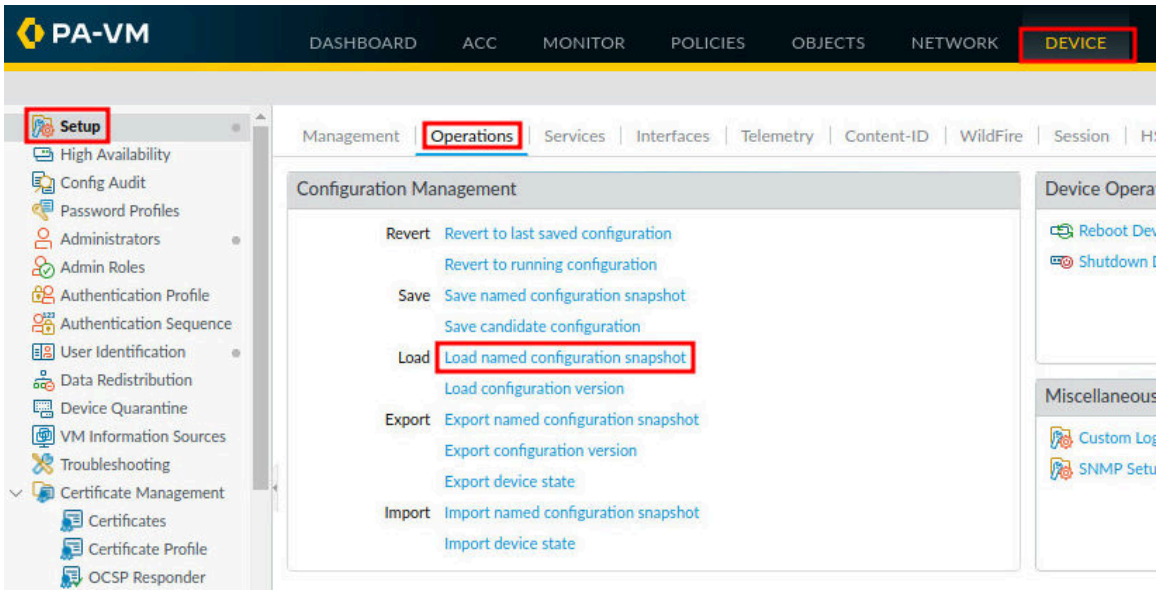
If you experience the "Unable to connect" or "502 Bad Gateway" message while attempting to connect to the specified IP above, please wait an additional 1-3 minutes for the Firewall to fully initialize. Refresh the page to continue.

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

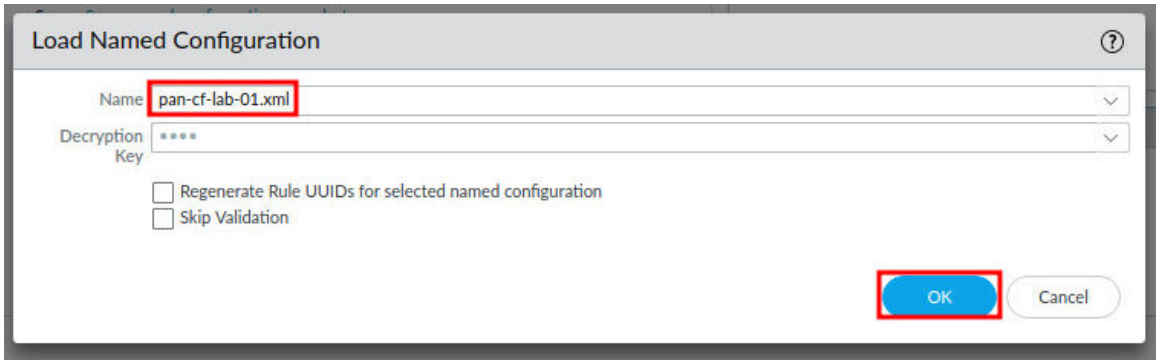


7. Log in to the Firewall web interface as username `admin`, password `Pal0Alt0!`.

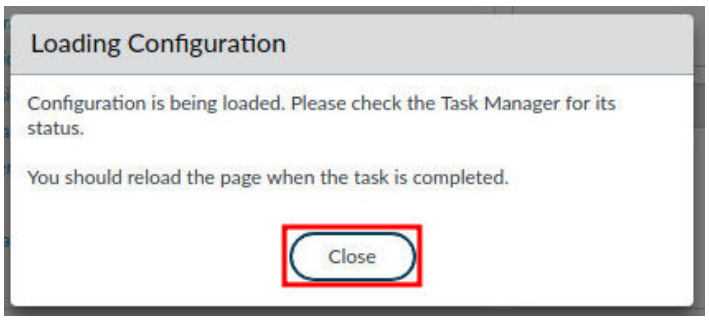
8. In the web interface, navigate to **Device > Setup > Operations** and click on **Load named configuration snapshot** underneath the *Configuration Management* section.



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

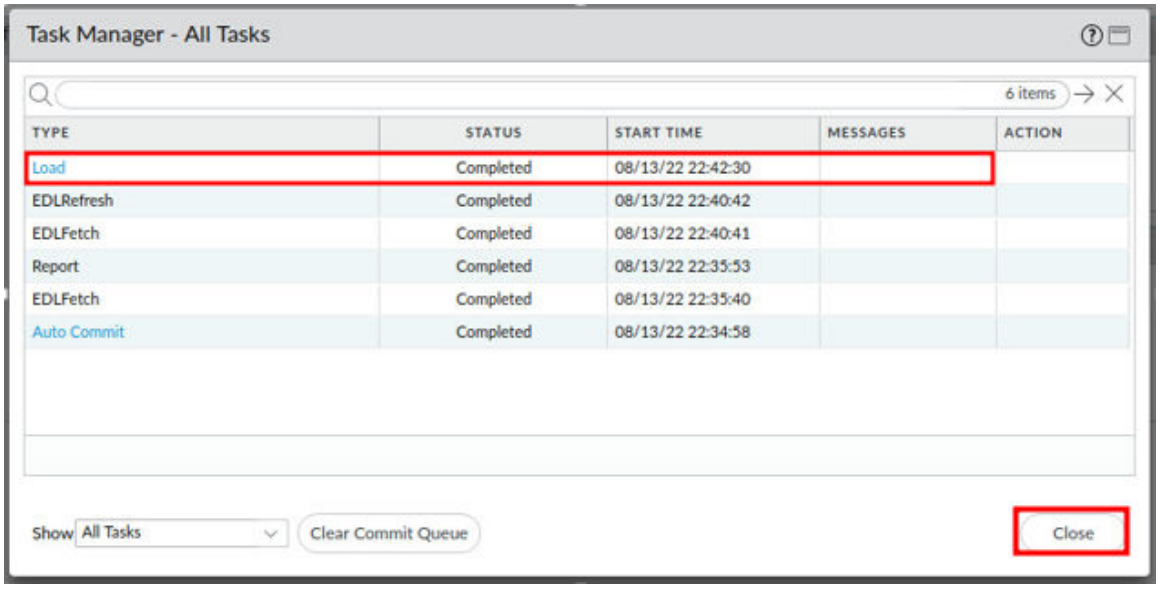


10. In the *Loading Configuration* window, a message will show *Configuration is being loaded. Please check the Task Manager for its status. You should reload the page when the task is completed.* Click **Close** to continue.

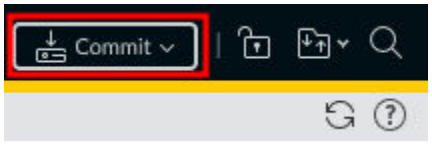


11. Click the **Tasks** icon located at the bottom-right of the web interface.

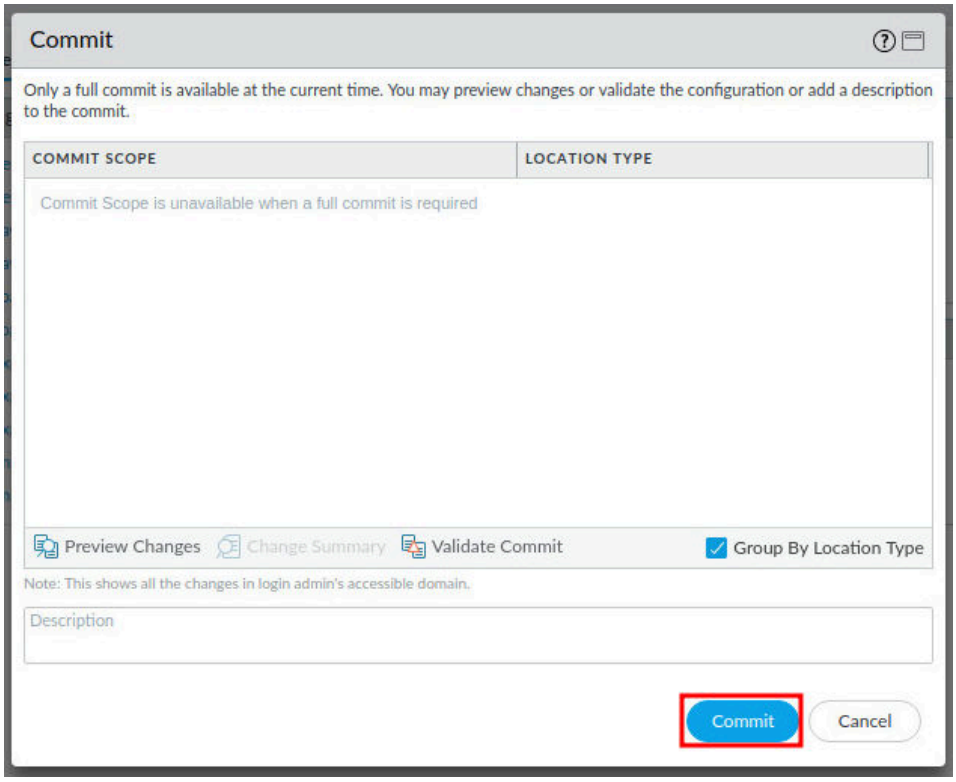
12. In the *Task Manager – All Tasks* window, verify the *Load* type has successfully completed. Click **Close.**



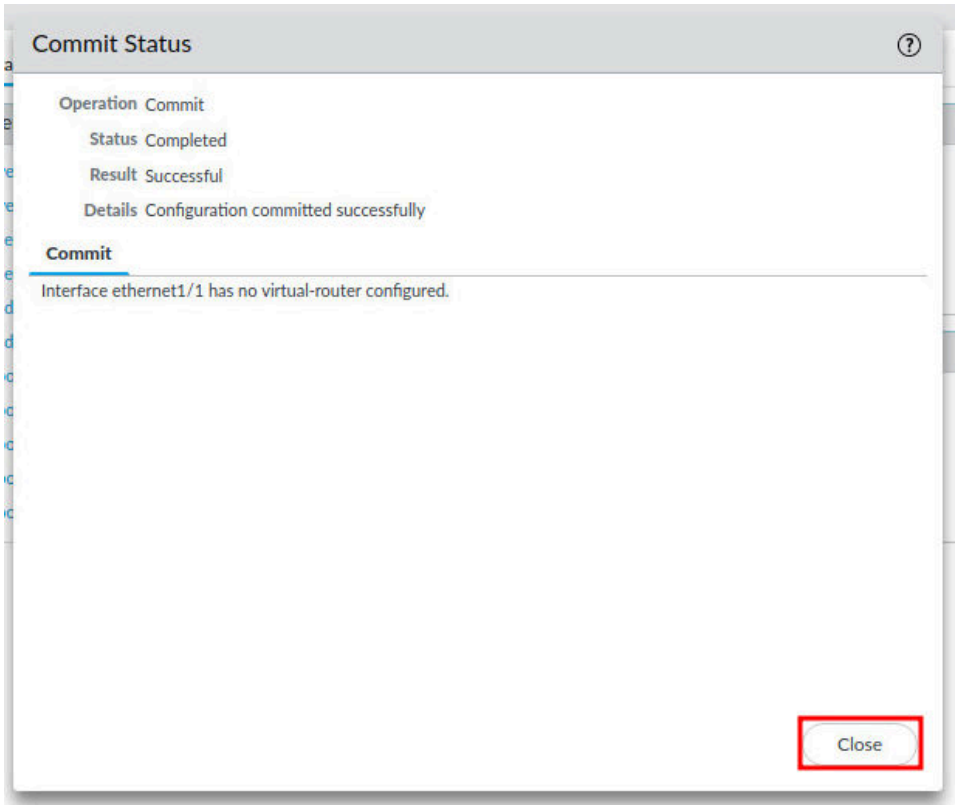
13. Click the **Commit** link located at the top-right of the web interface.



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



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



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.

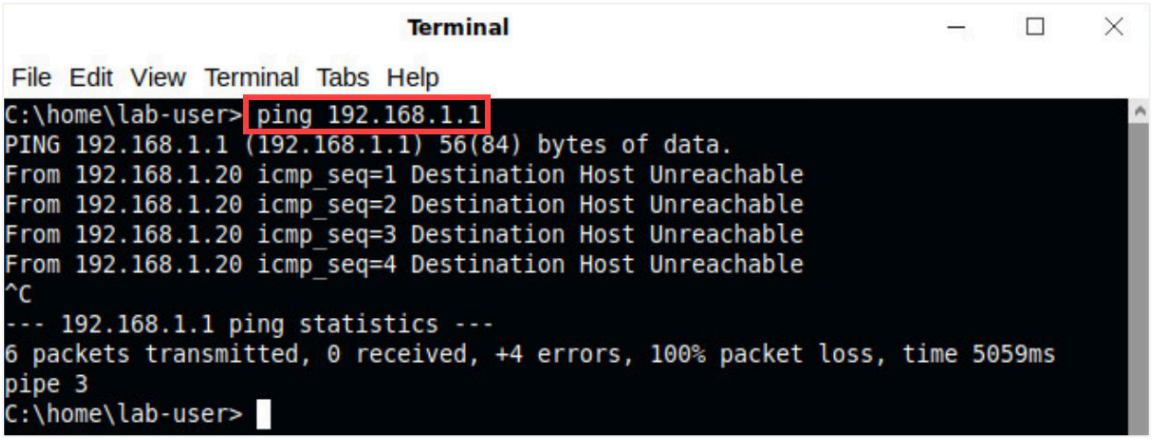
Notice the warnings in the **Commit** section. You will resolve those during this lab.

1.1 Configure Ethernet Interfaces with Layer 3 Information

In this section, you will confirm you have no connectivity to the Firewall from the inside network. Next, you will configure the Firewall with Layer 3 information.

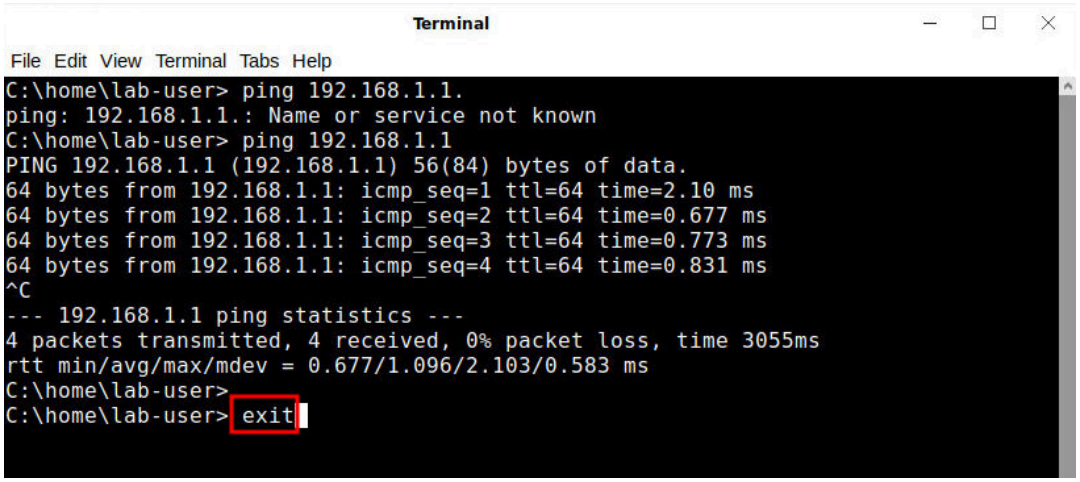
1. Click on the **Xfce Terminal** icon in the taskbar.

2. In the *Terminal* window, type `ping 192.168.1.1` and press **Enter**. To stop the ping, click **Ctrl+C**.

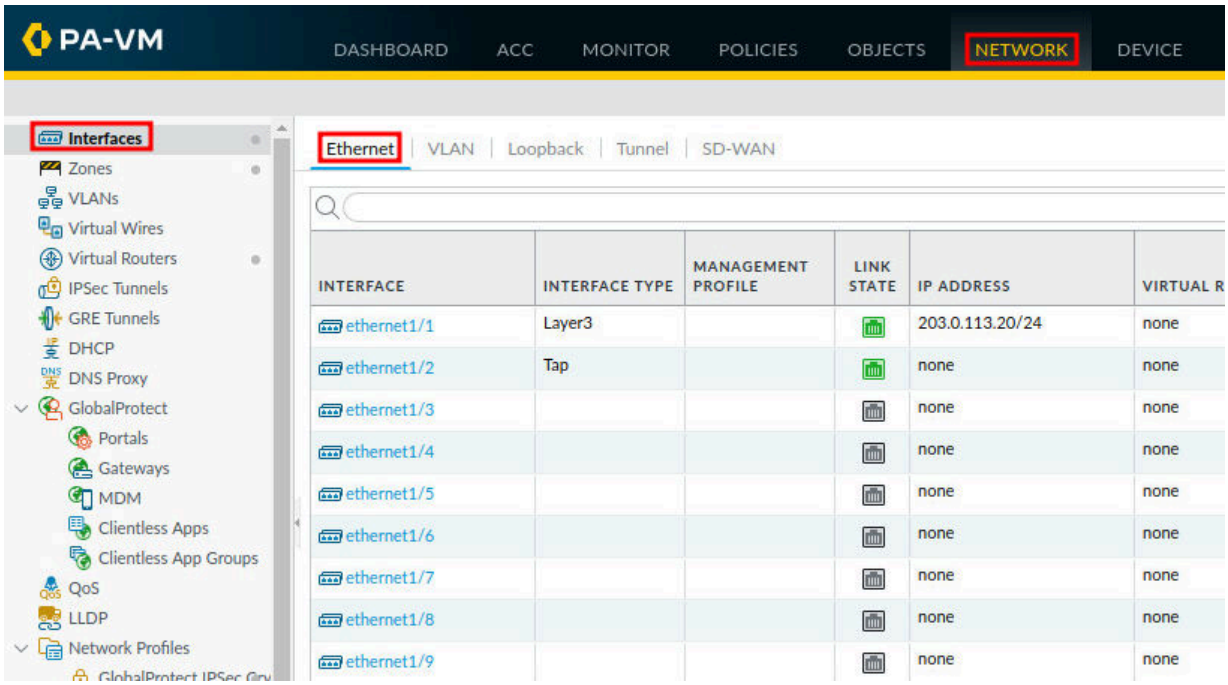


Ping is a network utility used to test the reachability of a host. In this instance, notice the response: "**Destination host unreachable**." This indicates that there is no network connectivity between the Client and the Firewall.

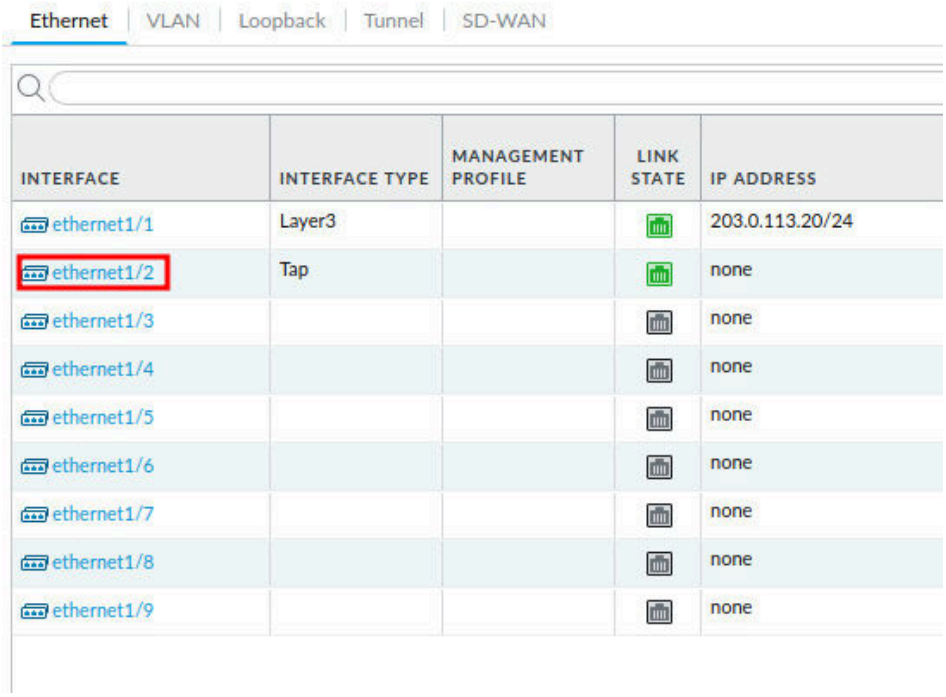
3. Close the *Terminal* window by typing **exit** then press **Enter**.



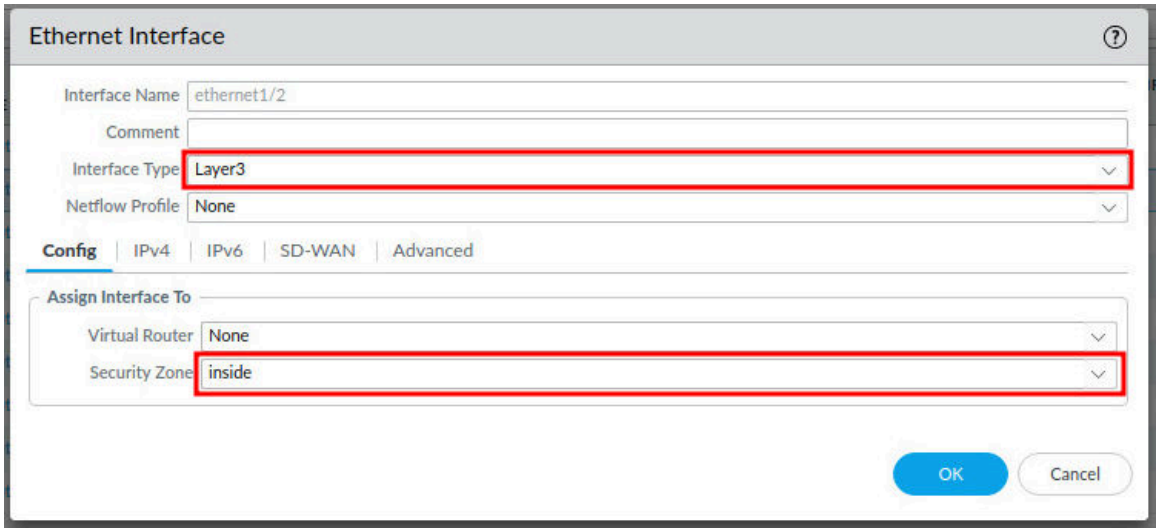
4. With the Firewall administrator page open, navigate to **Network > Interfaces > Ethernet.**



5. Click on the interface **ethernet1/2** from the list.

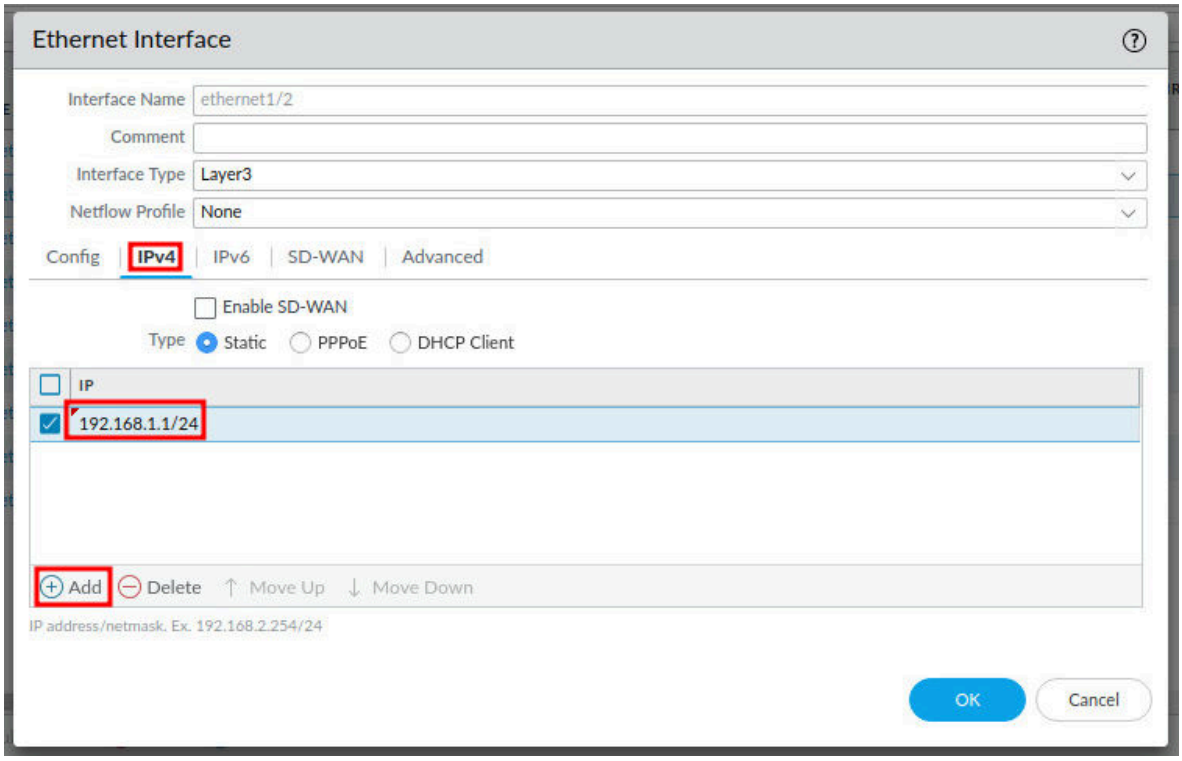


6. In the *Ethernet Interface* window, in the *Interface Type* dropdown, select **Layer3**. In the *Security Zone* dropdown, select **inside**.

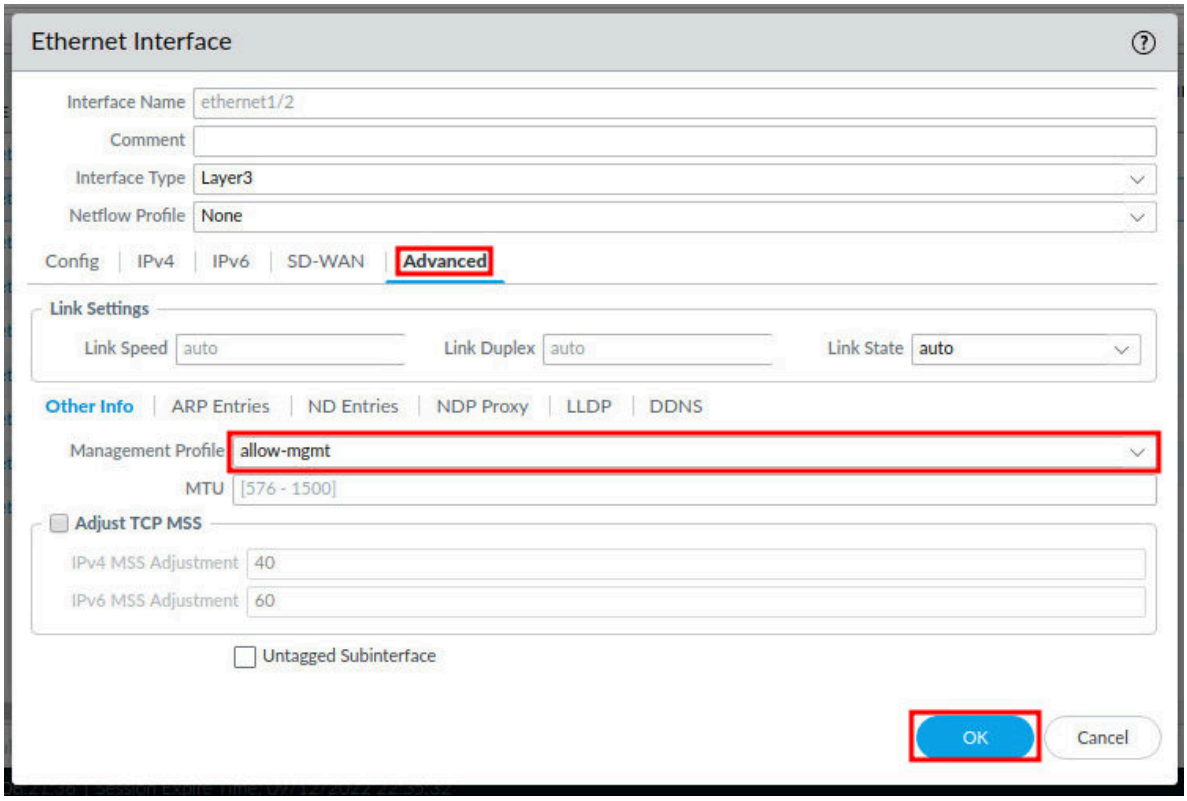


Layer 3 is selected so that the Firewall interface can be given an IP address, assigned a zone, and a virtual router.

7. In the *Ethernet Interface* window, click on the **IPv4** tab and click on the **Add** button at the bottom-left. Type `192.168.1.1/24` in the address field.

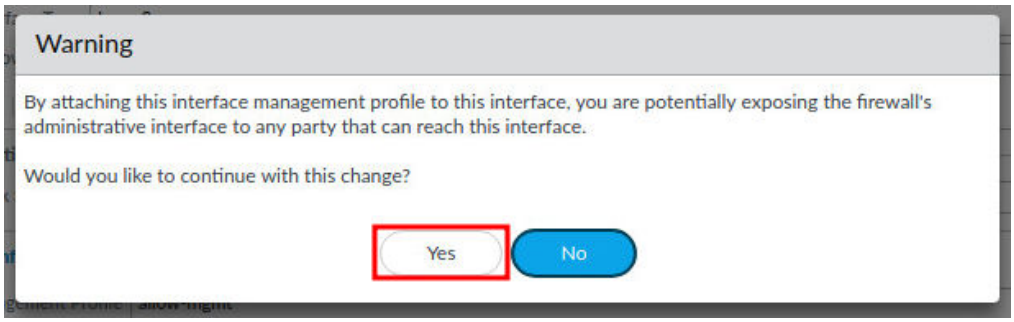


8. Click on the **Advanced** tab, and under the *Management Profile* dropdown, select **allow-mgmt** and click **OK**.



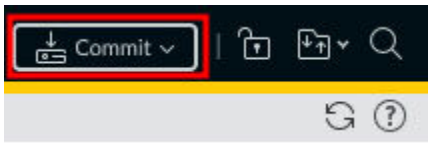
The **allow-mgmt** Management Profile allows the interface to accept pings and to accept management functions such as configuring the Firewall with SSH or a web browser.

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

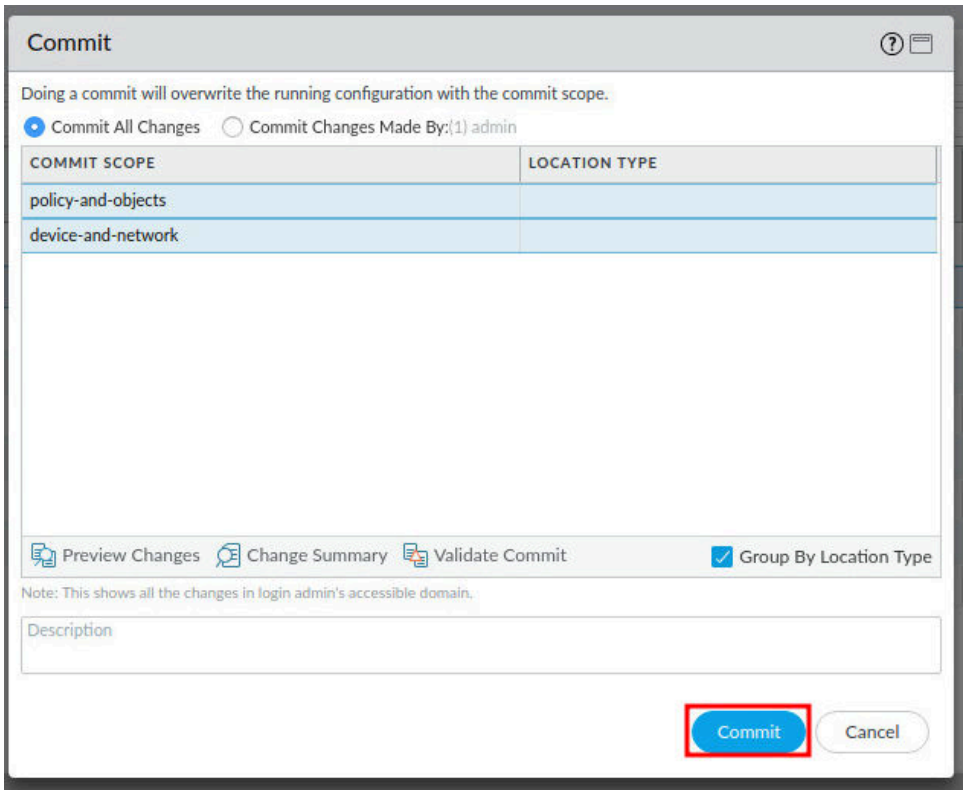


The Warning advises that if you attach this interface management profile to this interface, you are potentially exposing the firewall's administrative interface to any party that can reach this interface. For the purpose of this lab, you will bypass this warning knowing that it is not good practice to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

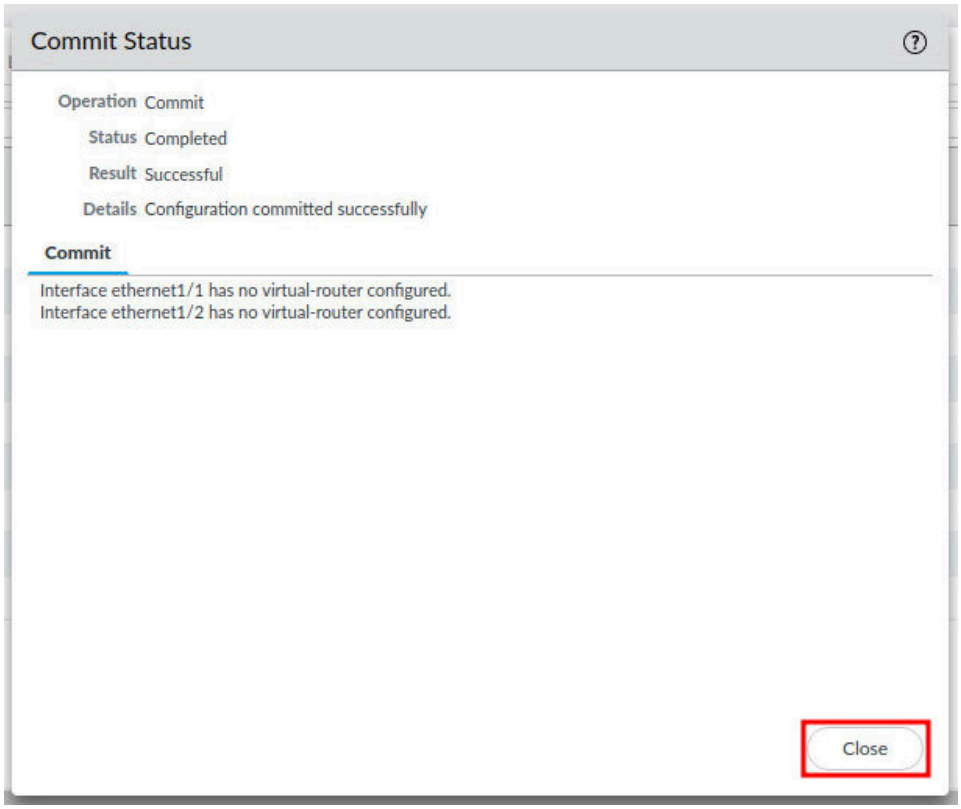
10. Click the **Commit** link located at the top-right of the web interface.



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



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

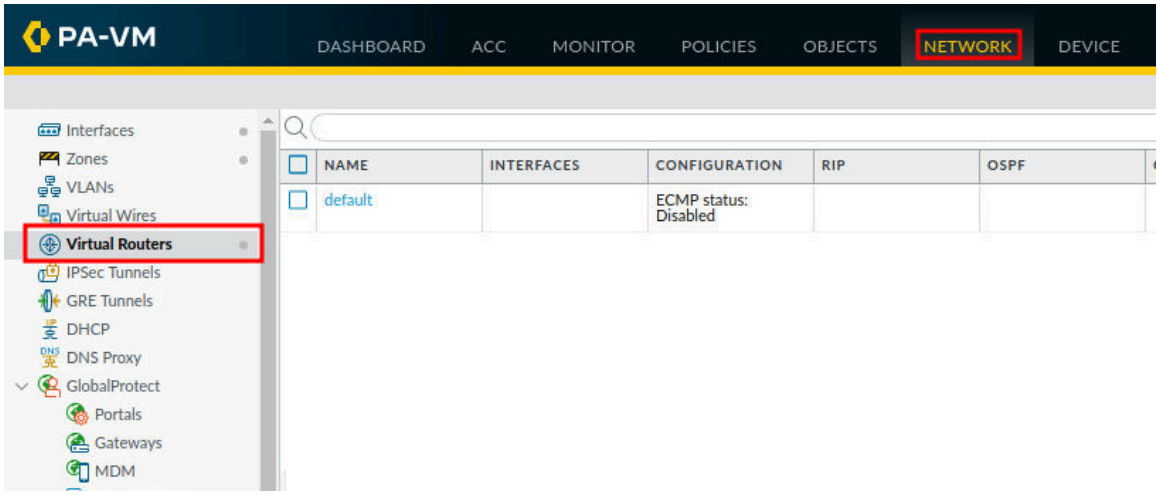


Notice the warnings in the **Commit** section. You will resolve this in the next section.

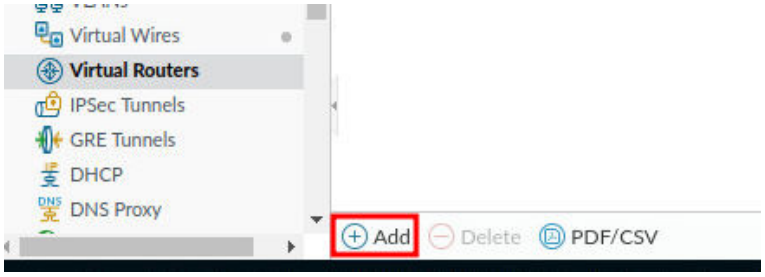
1.2 Create a Virtual Router

In this section, you will create a Virtual Router. Creating a virtual router allows the Firewall to do routing functions so that the Firewall and devices behind it can access other networks and the Internet.

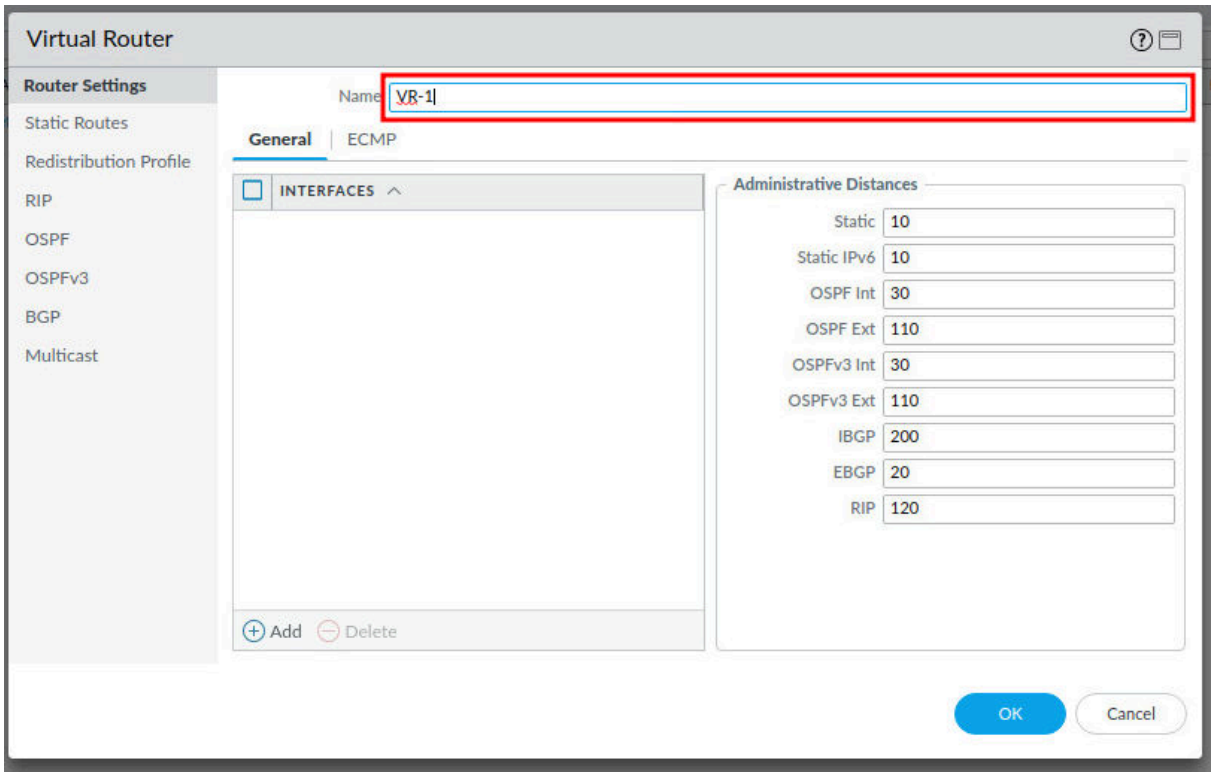
1. Navigate to **Network > Virtual Routers**.



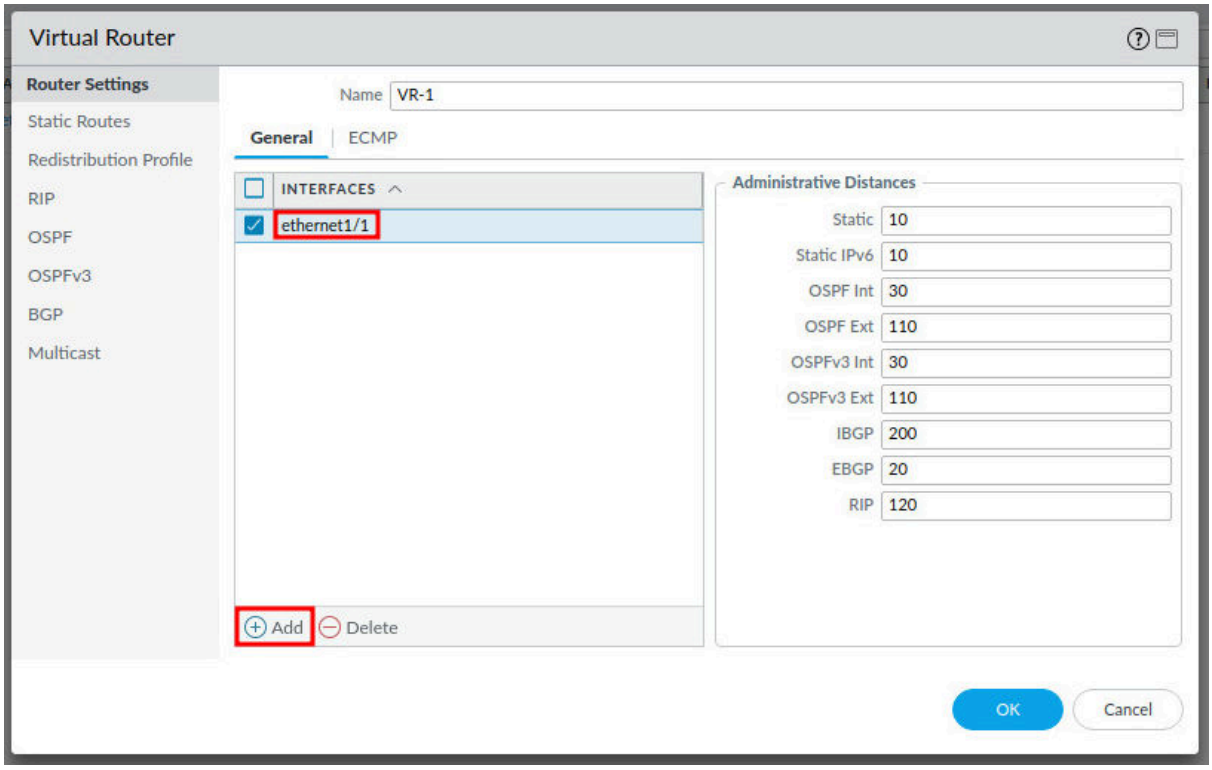
2. Click on **Add**, located at the bottom-left of the window, to create a new virtual router.



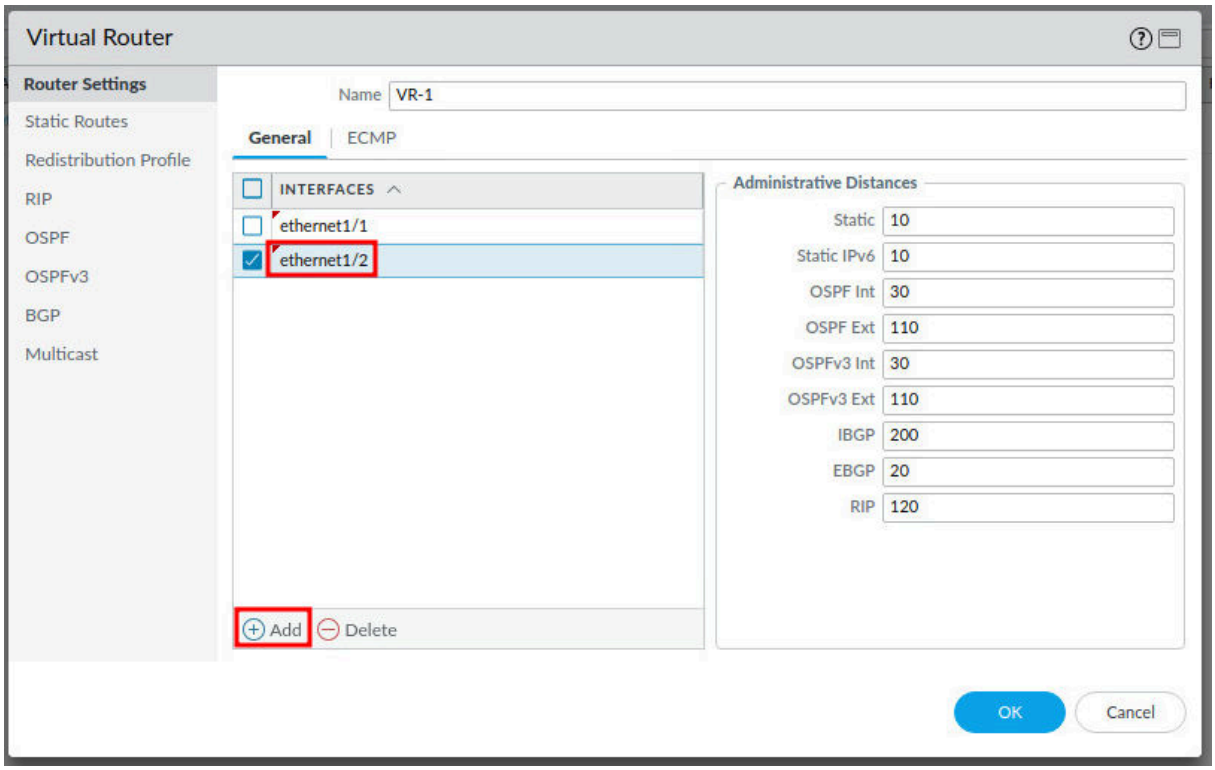
3. In the *Virtual Router* window, type VR−1 in the *Name* field.



4. Click on the **Add** button and select **ethernet1/1** from the dropdown.

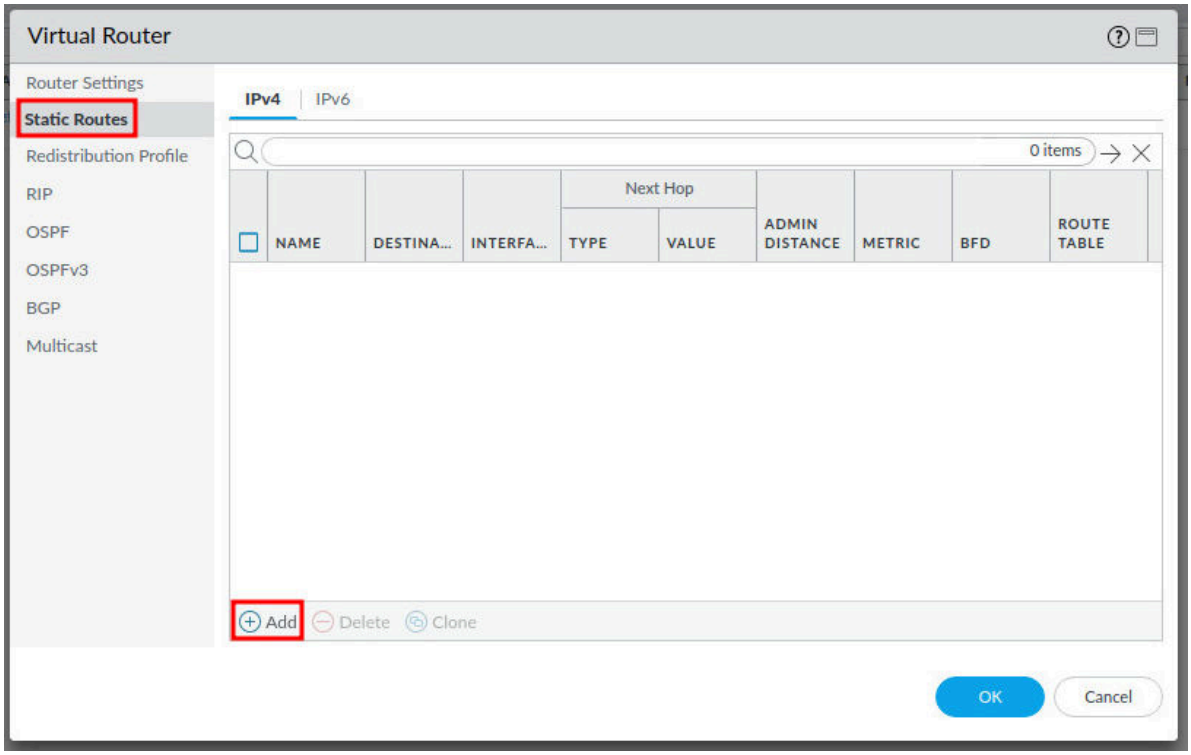


5. Click on the **Add** button and select **ethernet1/2**.

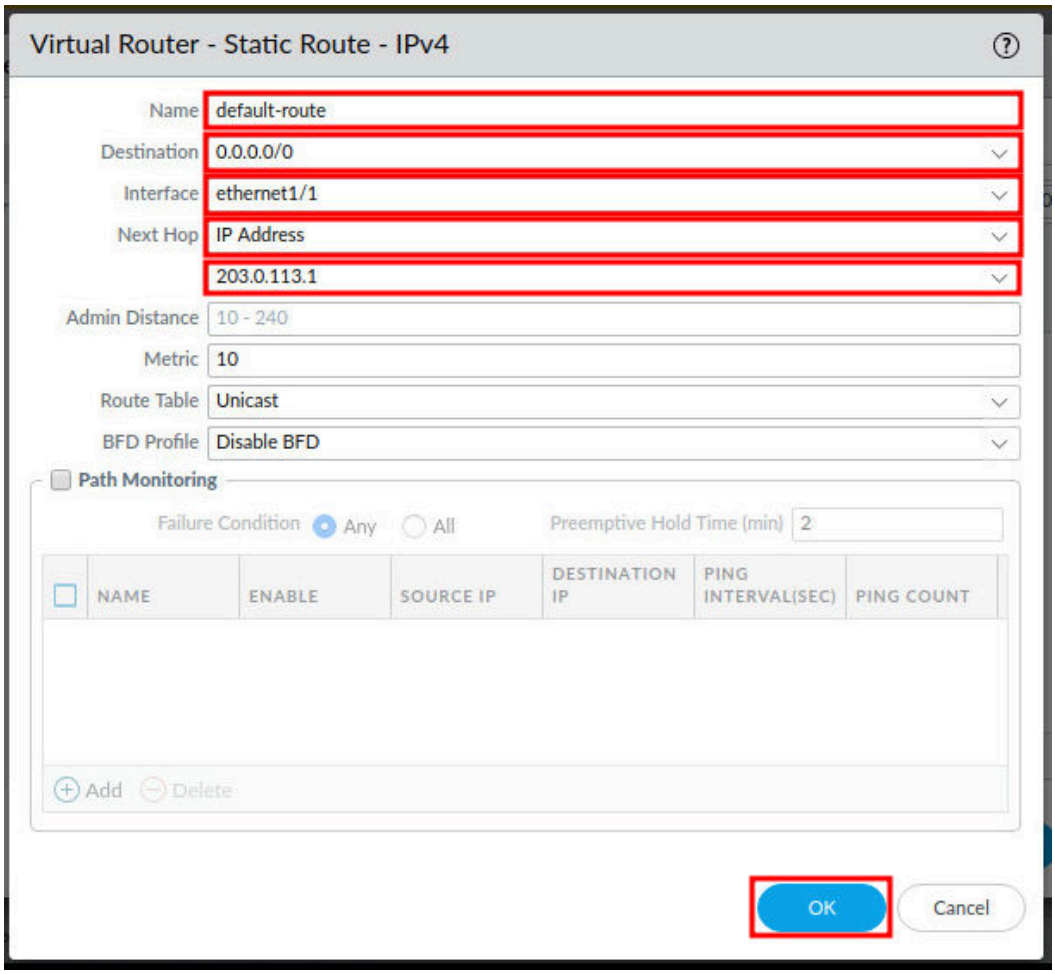


Adding interfaces to the virtual router will allow the networks assigned to these interfaces to route between one another.

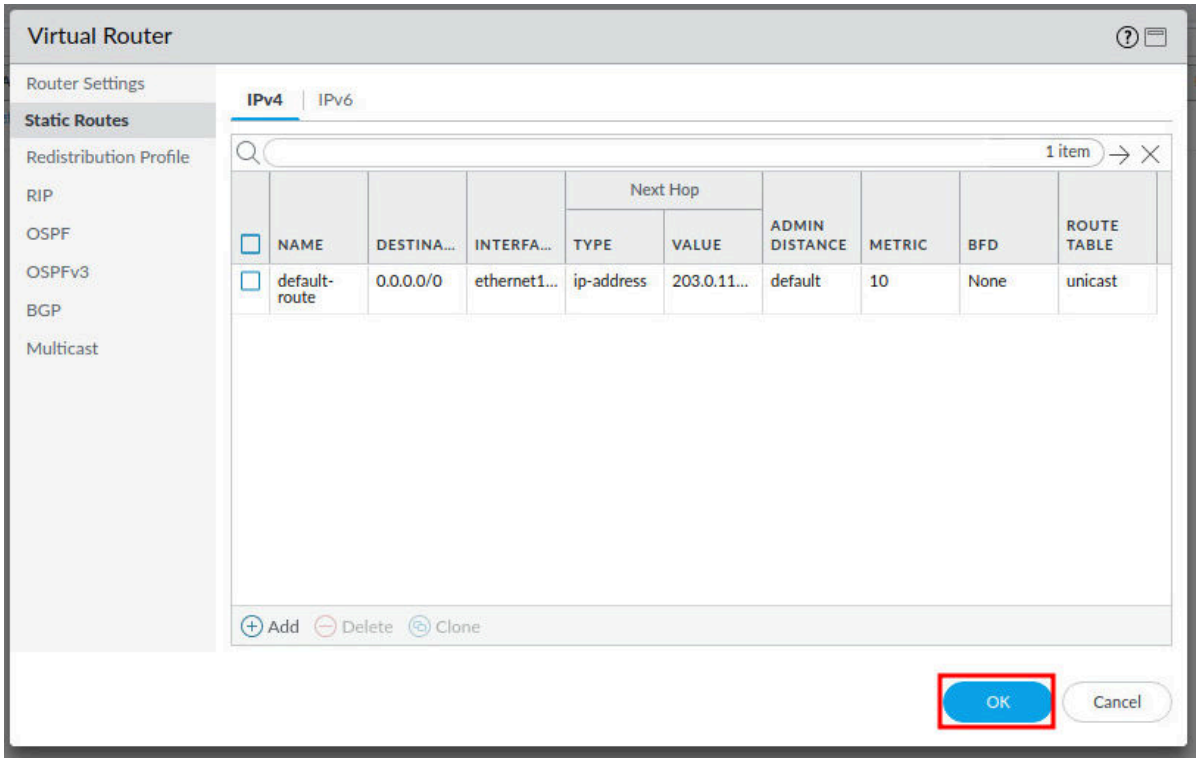
6. Click on the **Static Routes** tab and then click on the **Add** button at the bottom-left.



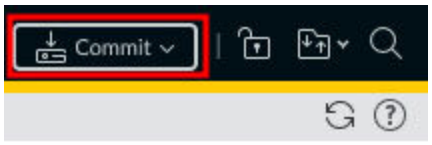
7. In the *Virtual Router – Static Route – Ipv4* window, type `default-route` in the *Name* field. Next, type `0.0.0.0/0` in the *Destination* field. Then, in the *Interface* dropdown, select **ethernet1/1**. Finally, in the *Next Hop* dropdown, ensure **IP Address** is selected, and in the field below it, type `203.0.113.1`, and then click **OK**.



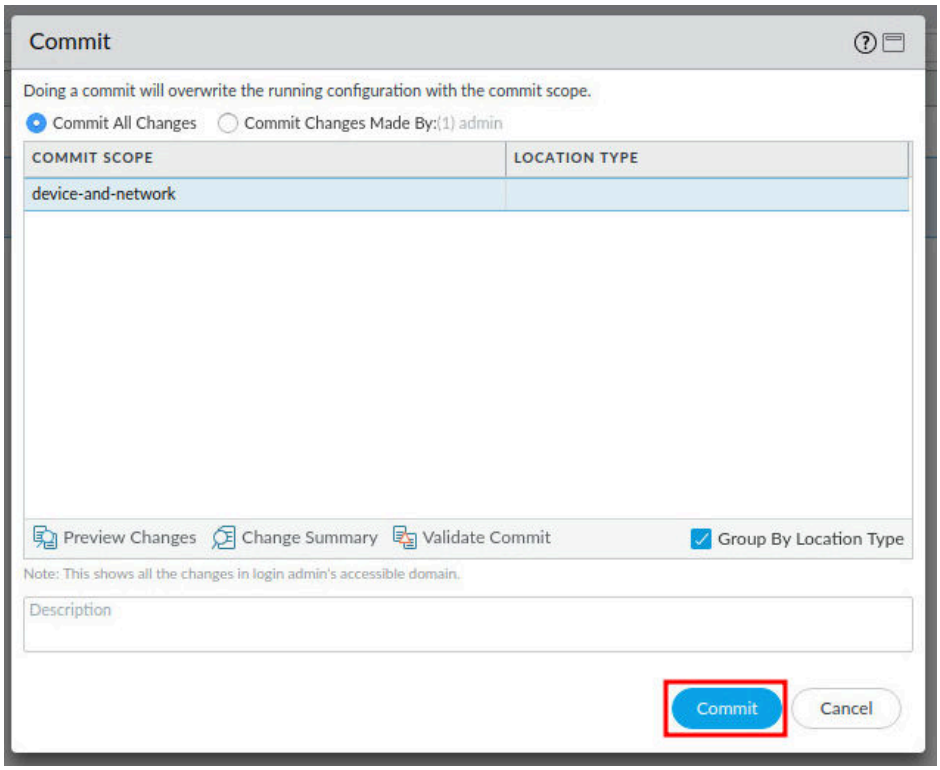
8. Adding a static route of 0.0.0.0/0 is sometimes called *the gateway of last resort*. By adding this static route, if there is a network that the Firewall does not know about, it will forward the packets to this address. Click **OK** to close the *Virtual Router* window.



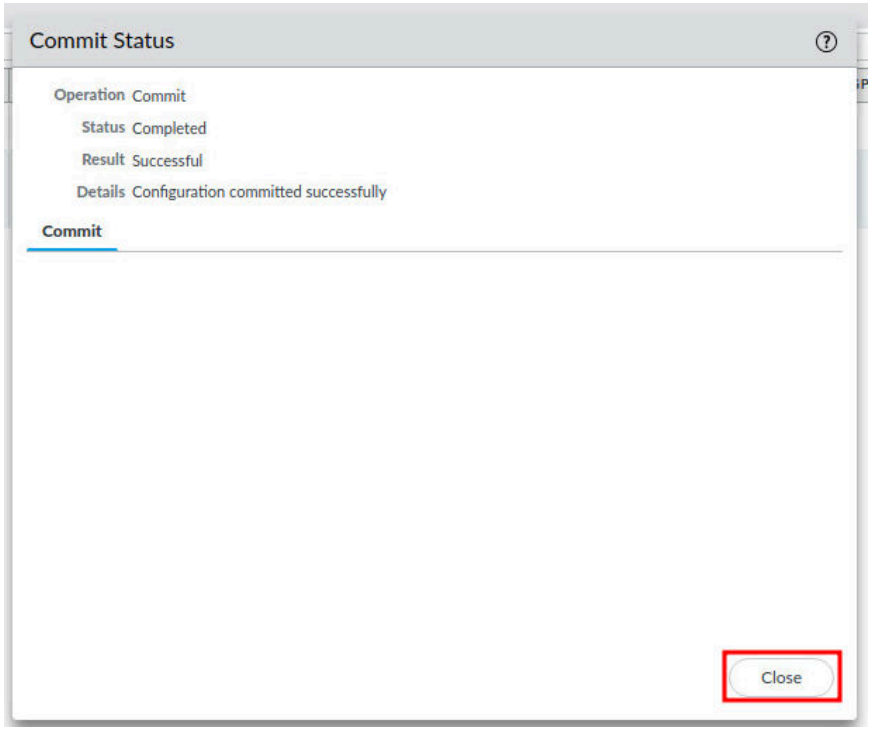
9. Click the **Commit** link located at the top-right of the web interface.



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



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

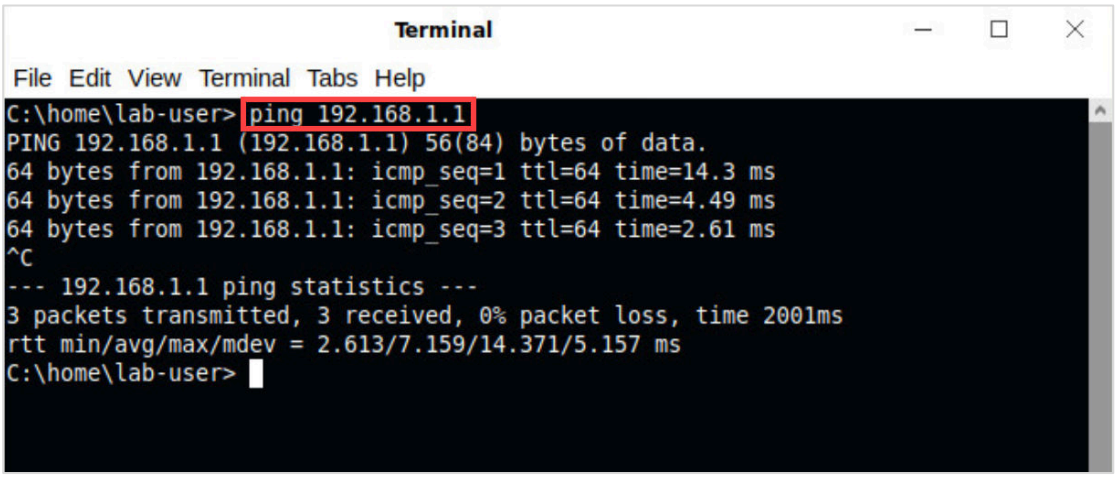


1.3 Verify Network Connectivity

In this section, you will confirm you now have connectivity to the Firewall from the inside network by utilizing *ping* and connecting to the web interface.

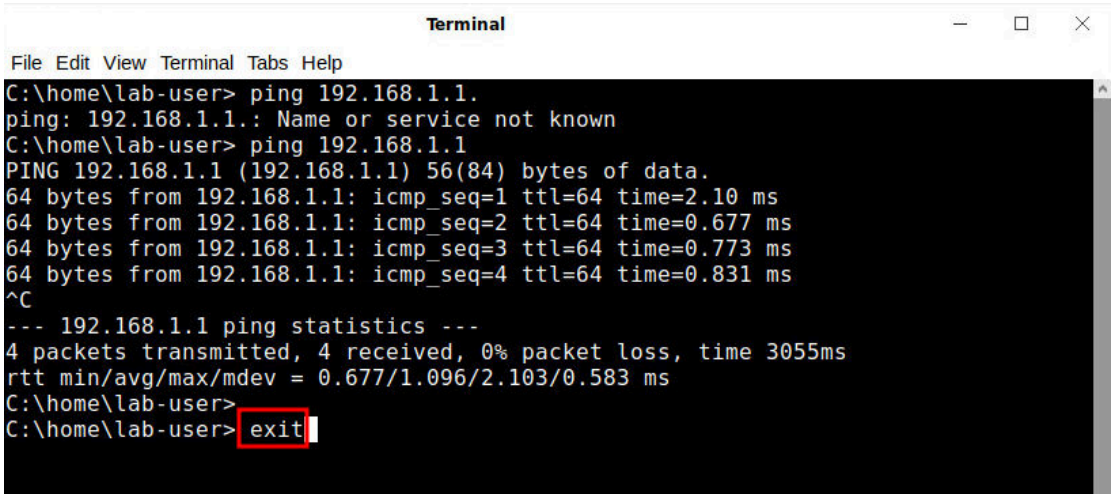
1. Click on the **Xfce Terminal** icon in the taskbar.

2. In the *Terminal* window, ping the Firewall inside interface by typing `ping 192.168.1.1` and press **Enter**. To stop the ping, click **Ctrl+C**.



Notice the *ping* command will receive replies from **192.168.1.1**. This means that packets can be sent and received between the Client and the Firewall.

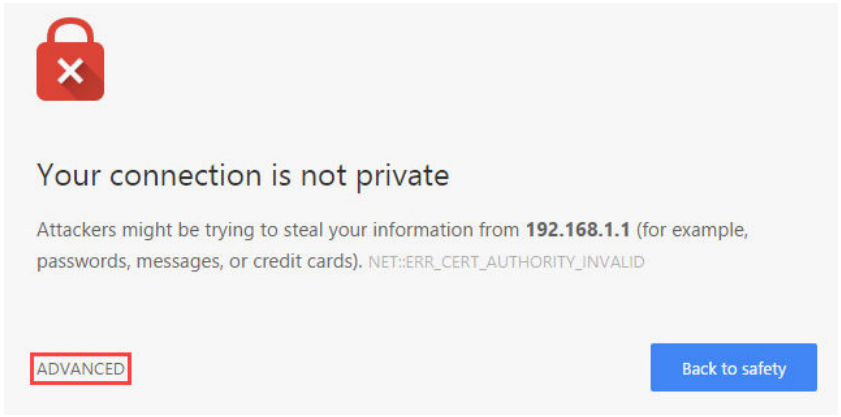
13. Close the *Terminal* window by typing **exit** then press **Enter**.



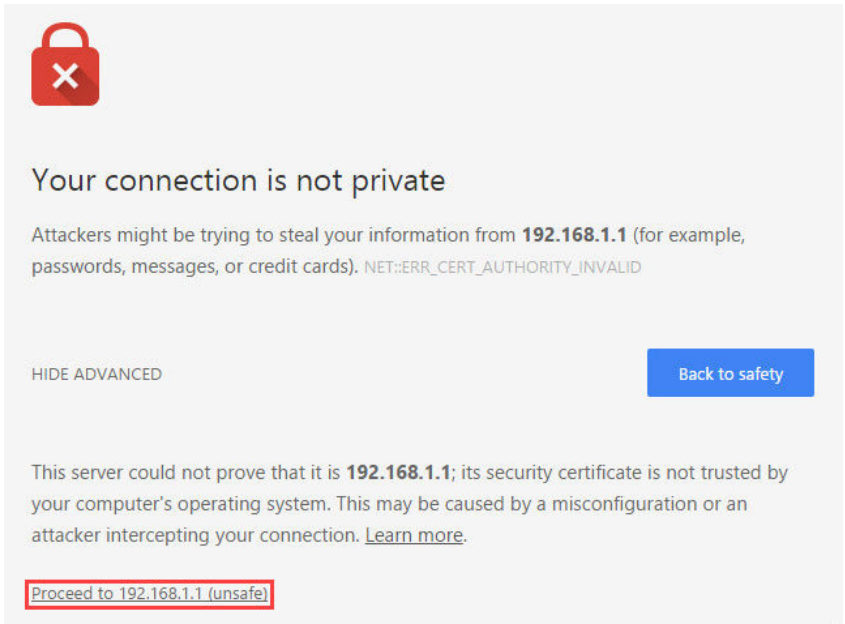
3. In *Chromium*, click on the **New tab** button.

4. In the *address bar*, type `https://192.168.1.1` and press **Enter**.

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



6. Click on **Proceed to 192.168.1.1 (unsafe)**.



7. You should see the Firewall login web interface on the *192.168.1.1* IP address that was configured earlier.

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

