



CYBERSECURITY FOUNDATION V2

Lab 1: Configuring TCP/IP and a Virtual Router

Document Version: **2022-12-22**

Copyright © 2022 Network Development Group, Inc.
www.netdevgroup.com

NETLAB+ is a registered trademark 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	3
Lab Topology.....	4
Lab Settings.....	5
1 Configuring TCP/IP and a Virtual Router	6
1.0 Load Lab Configuration	6
1.1 Configure Ethernet Interfaces with Layer 3 Information.....	11
1.2 Create a Virtual Router	17
1.3 Verify Network Connectivity	24

Introduction

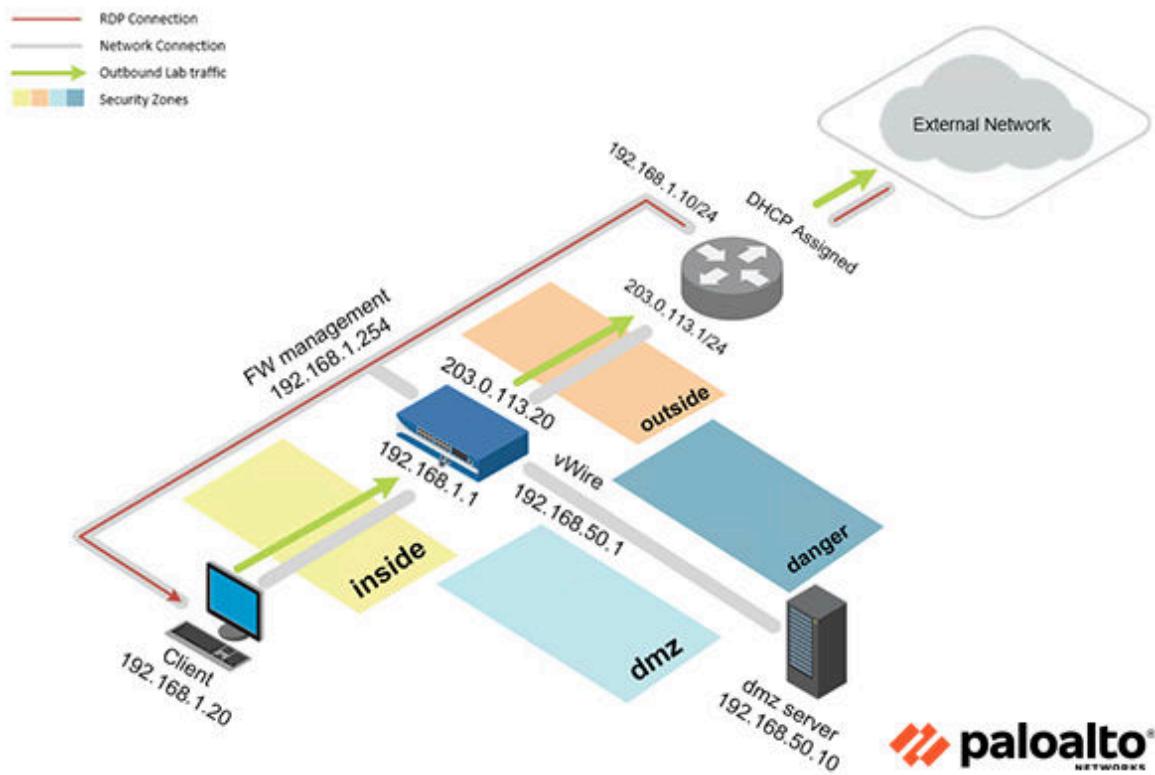
In this lab, you will configure Ethernet interfaces on the Palo Alto Networks Firewall with Layer 3 information, create a Virtual Router to allow traffic, and verify network connectivity.

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.

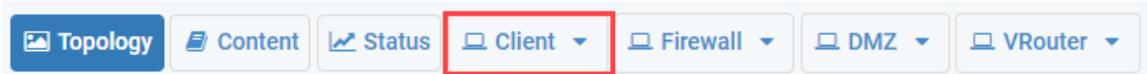
Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Client	192.168.1.20	lab-user	PaloAlt0!
DMZ	192.168.50.10	root	PaloAlt0!
Firewall	192.168.1.254	admin	PaloAlt0!

1 Configuring TCP/IP and a Virtual Router

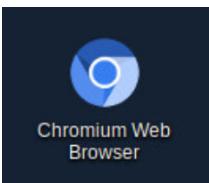
1.0 Load Lab Configuration

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

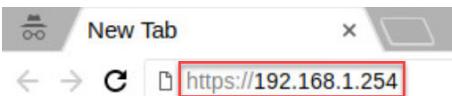
1. Click on the **Client** tab to access the Client PC.



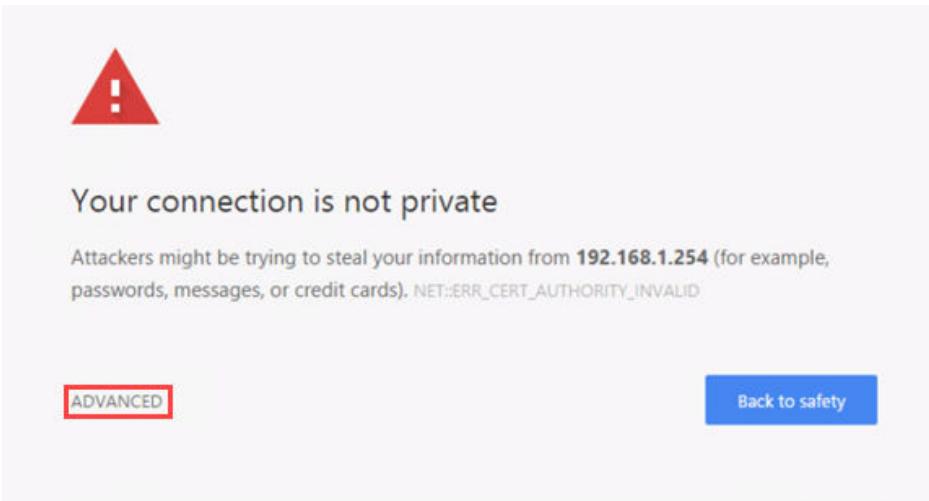
2. Log in to the Client PC as username `lab-user`, password `PaloAlt0!`.
3. Double-click the **Chromium Web Browser** icon, located on the Desktop.



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

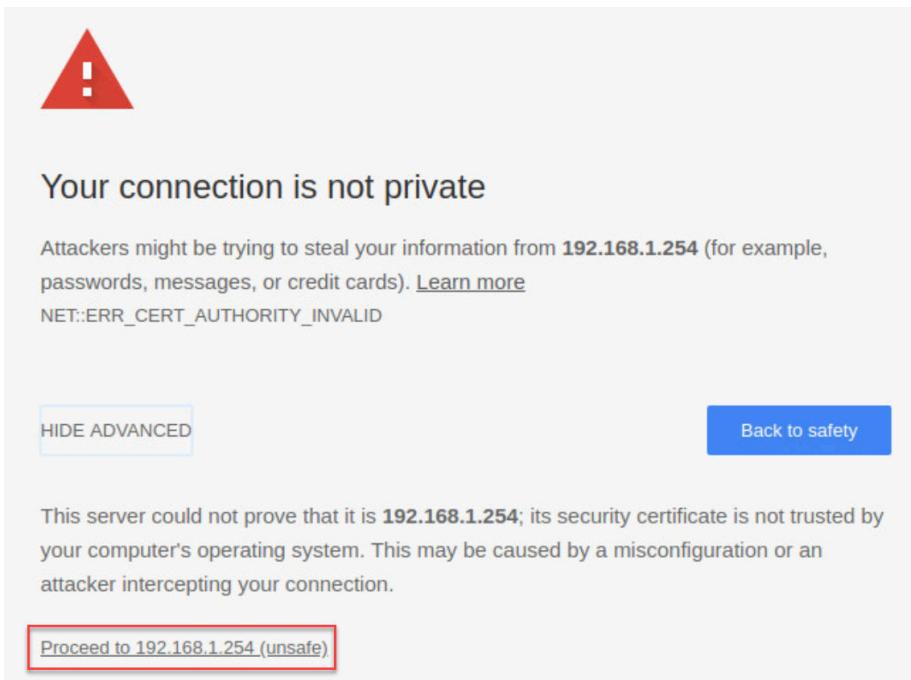


5. You will see a “*Your connection is not private*” message. Click on the **ADVANCED** link.



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.

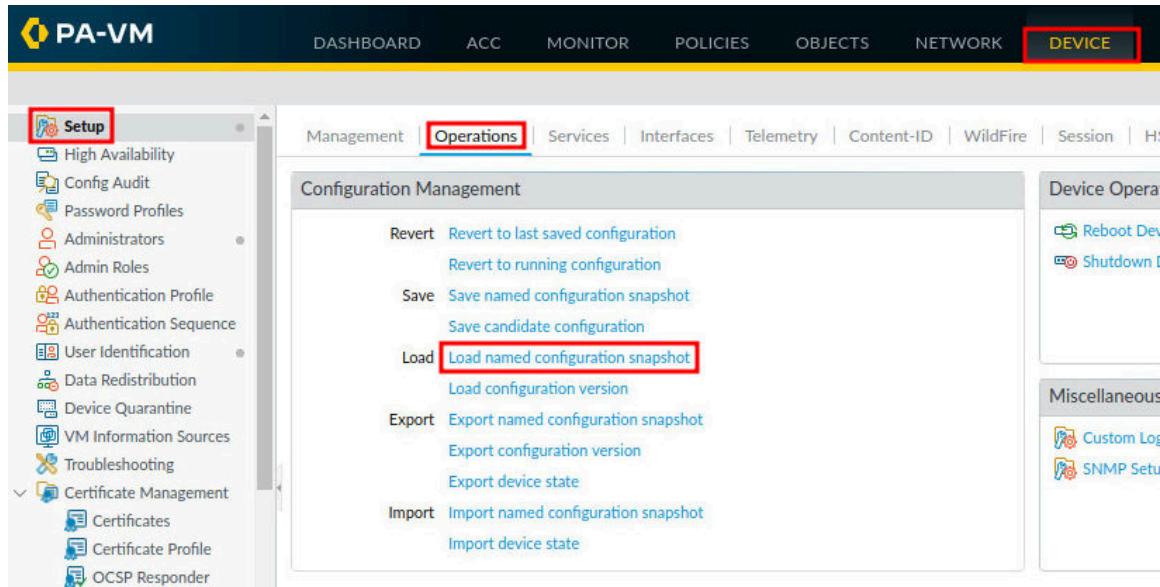
6. Click on **Proceed to 192.168.1.254 (unsafe)**.



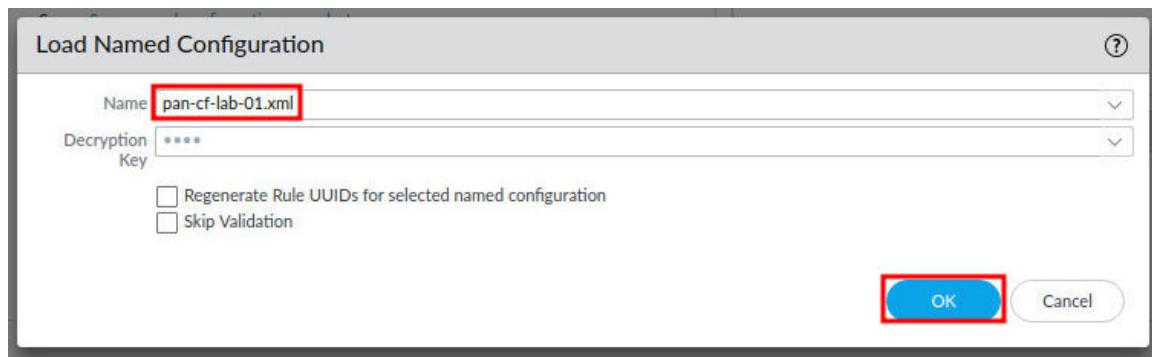
7. Log in to the Firewall web interface as username admin, password PaloAlt0!.



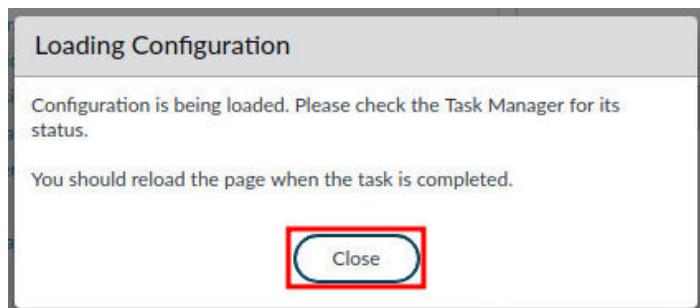
8. In the web interface, navigate to **Device > Setup > Operations** and click on **Load named configuration snapshot** underneath the *Configuration Management* section.



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



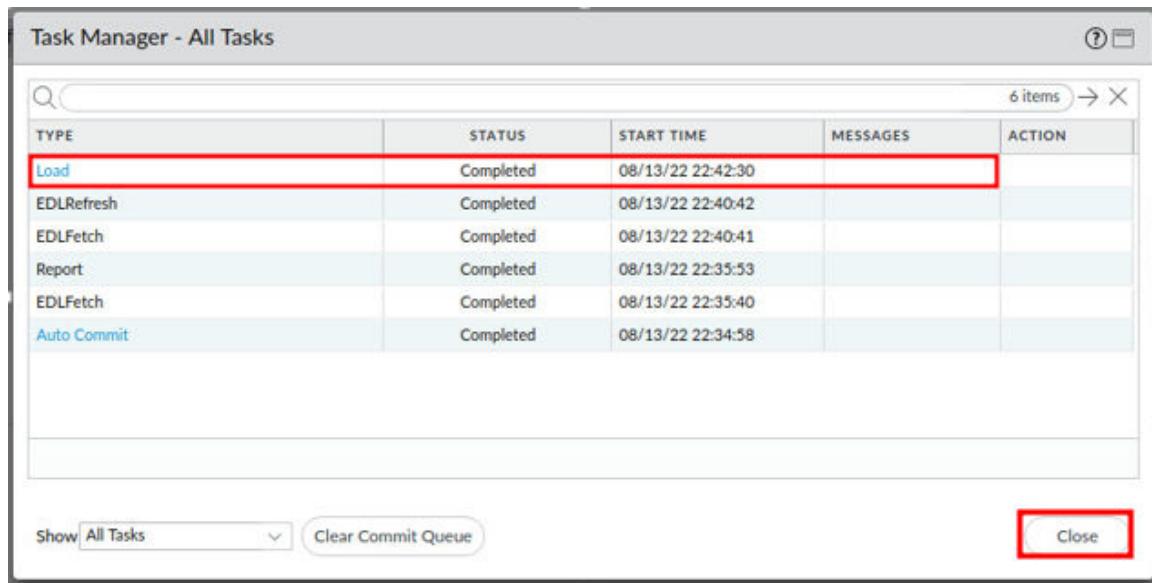
10. In the *Loading Configuration* window, a message will show *Configuration is being loaded*. Please check the Task Manager for its status. You should reload the page when the task is completed. Click **Close** to continue.



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**.

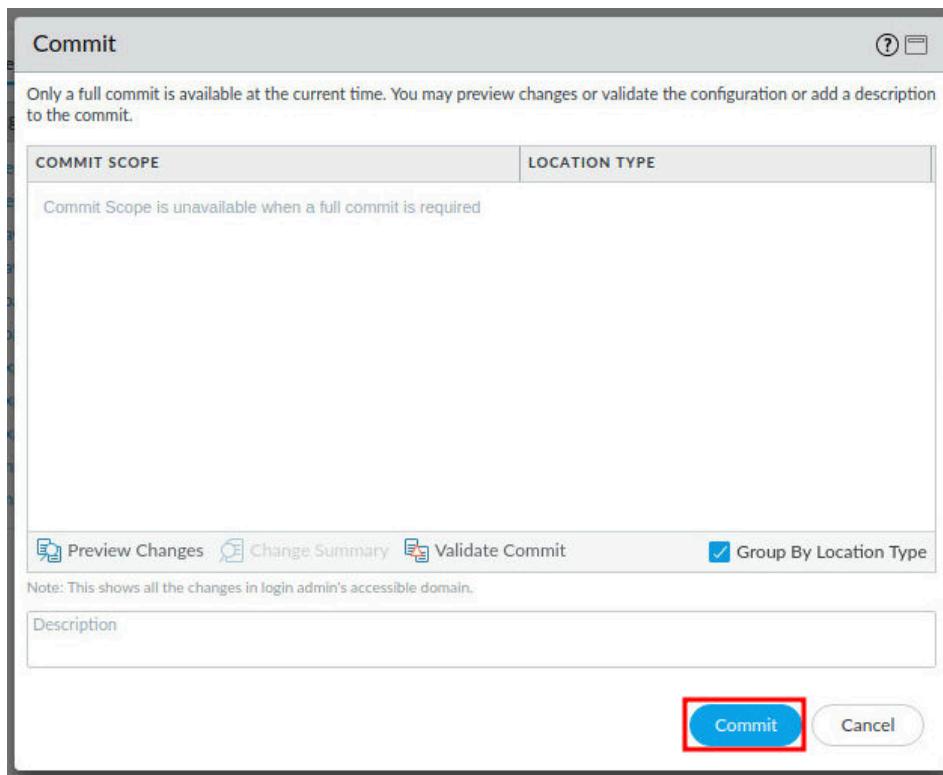


TYPE	STATUS	START TIME	MESSAGES	ACTION
Load	Completed	08/13/22 22:42:30		
EDLRefresh	Completed	08/13/22 22:40:42		
EDLFetch	Completed	08/13/22 22:40:41		
Report	Completed	08/13/22 22:35:53		
EDLFetch	Completed	08/13/22 22:35:40		
Auto Commit	Completed	08/13/22 22:34:58		

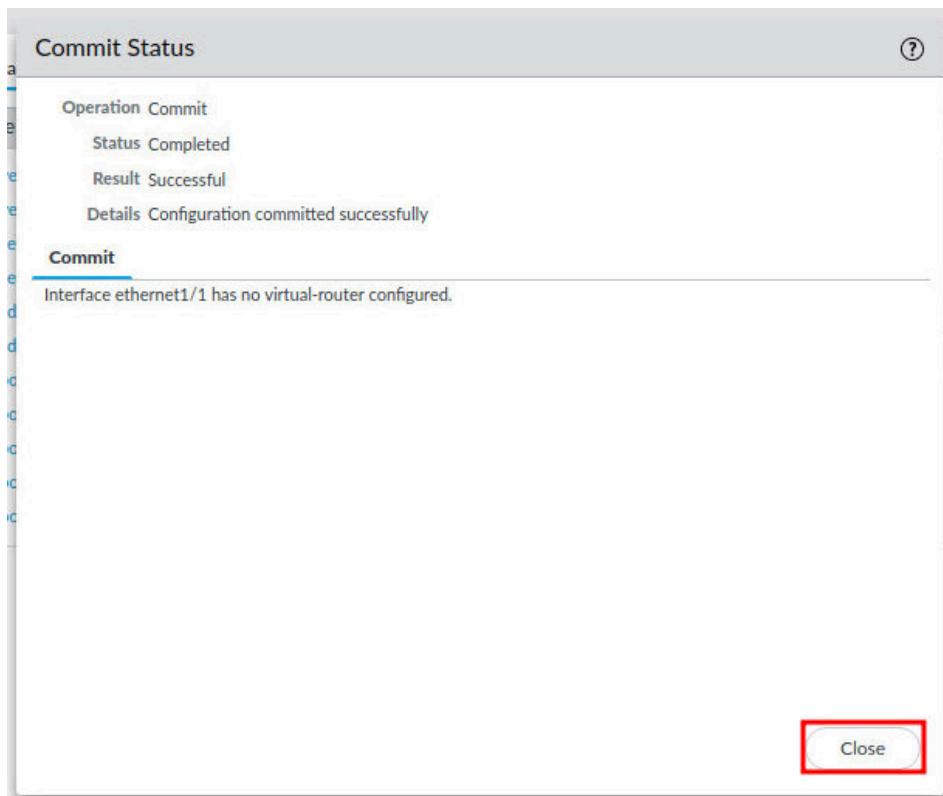
13. Click the **Commit** link located at the top-right of the web interface.



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.

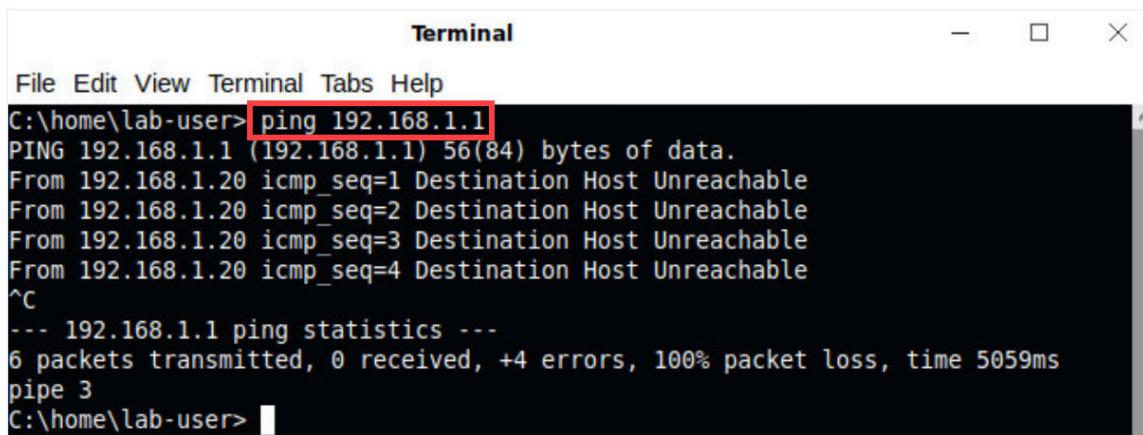
1.1 Configure Ethernet Interfaces with Layer 3 Information

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**.



```
Terminal
File Edit View Terminal Tabs Help
C:\home\lab-user> ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
From 192.168.1.20 icmp_seq=1 Destination Host Unreachable
From 192.168.1.20 icmp_seq=2 Destination Host Unreachable
From 192.168.1.20 icmp_seq=3 Destination Host Unreachable
From 192.168.1.20 icmp_seq=4 Destination Host Unreachable
^C
--- 192.168.1.1 ping statistics ---
6 packets transmitted, 0 received, +4 errors, 100% packet loss, time 5059ms
pipe 3
C:\home\lab-user>
```



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**.

```

Terminal
File Edit View Terminal Tabs Help
C:\home\lab-user> ping 192.168.1.1.
ping: 192.168.1.1.: Name or service not known
C:\home\lab-user> ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=2.10 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=0.677 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=64 time=0.773 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=64 time=0.831 ms
^C
--- 192.168.1.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3055ms
rtt min/avg/max/mdev = 0.677/1.096/2.103/0.583 ms
C:\home\lab-user>
C:\home\lab-user> exit

```

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

INTERFACE	INTERFACE TYPE	MANAGEMENT PROFILE	LINK STATE	IP ADDRESS	VIRTUAL R
ethernet1/1	Layer3			203.0.113.20/24	none
ethernet1/2	Tap			none	none
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

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

Ethernet	VLAN	Loopback	Tunnel	SD-WAN
INTERFACE	INTERFACE TYPE	MANAGEMENT PROFILE	LINK STATE	IP ADDRESS
ethernet1/1	Layer3		Up	203.0.113.20/24
ethernet1/2	Tap		Up	none
ethernet1/3			Up	none
ethernet1/4			Up	none
ethernet1/5			Up	none
ethernet1/6			Up	none
ethernet1/7			Up	none
ethernet1/8			Up	none
ethernet1/9			Up	none

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

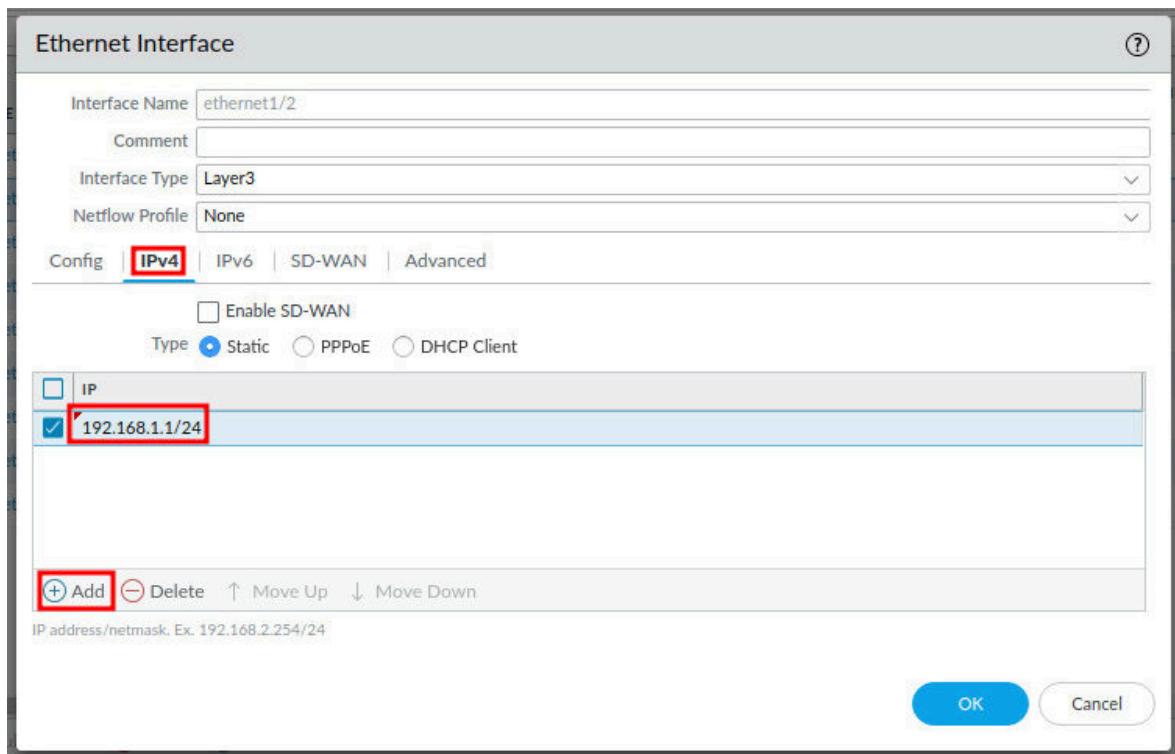
Ethernet Interface

Interface Name	ethernet1/2			
Comment				
Interface Type	Layer3			
Netflow Profile	None			
Config	IPv4	IPv6	SD-WAN	Advanced
Assign Interface To				
Virtual Router	None			
Security Zone	inside			
OK Cancel				

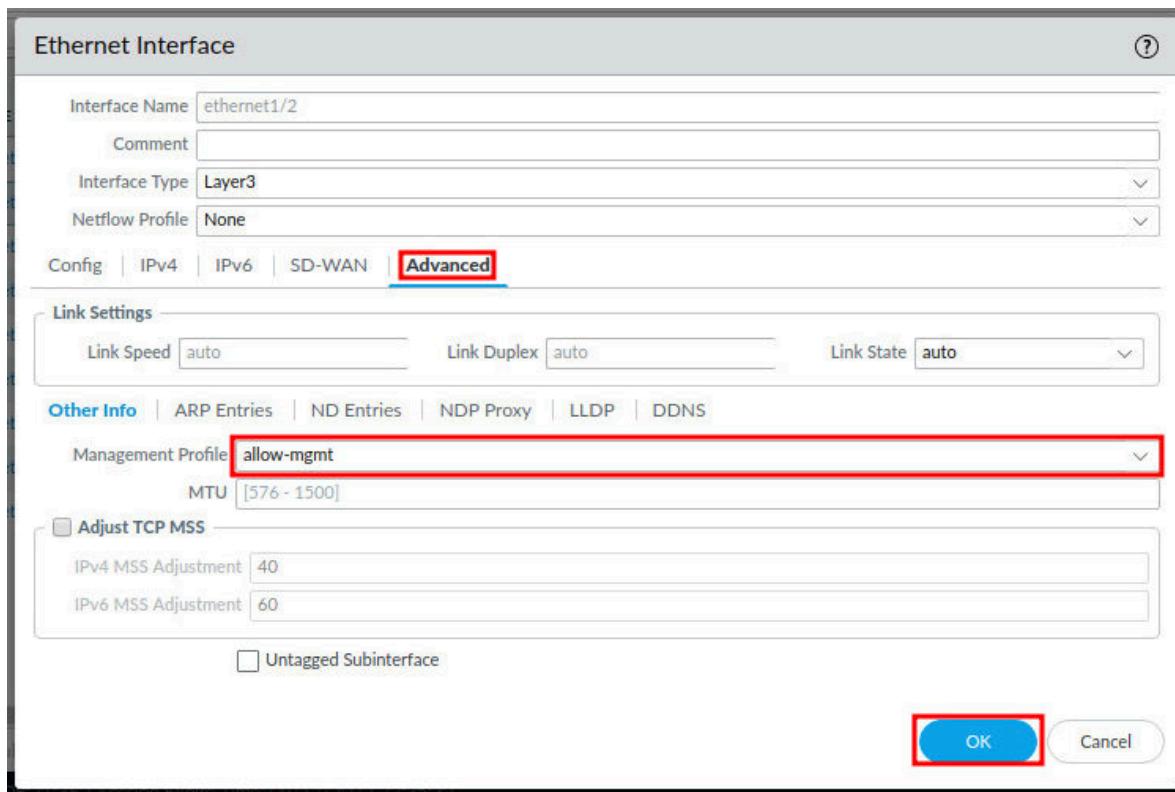


Layer 3 is selected so that the Firewall interface can be given an IP address, assigned a zone, and a virtual router.

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.



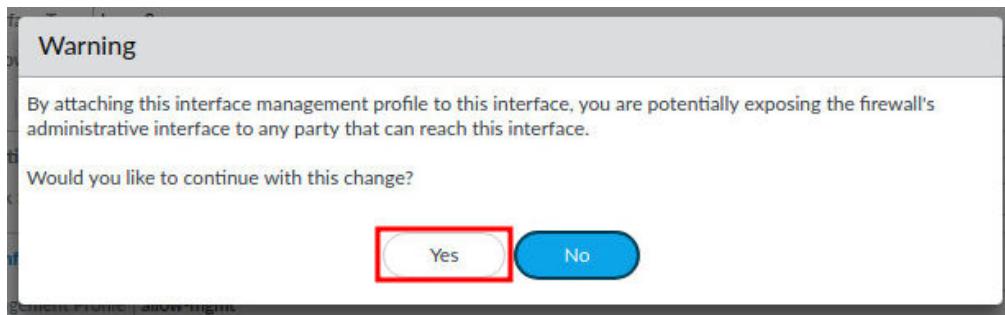
8. Click on the **Advanced** tab, and under the *Management Profile* dropdown, select **allow-mgmt** and click **OK**.





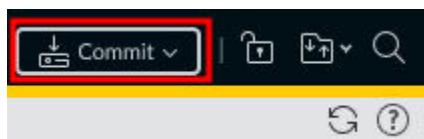
The **allow-mgmt** Management Profile allows the interface to accept pings and to accept management functions such as configuring the Firewall with SSH or a web browser.

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

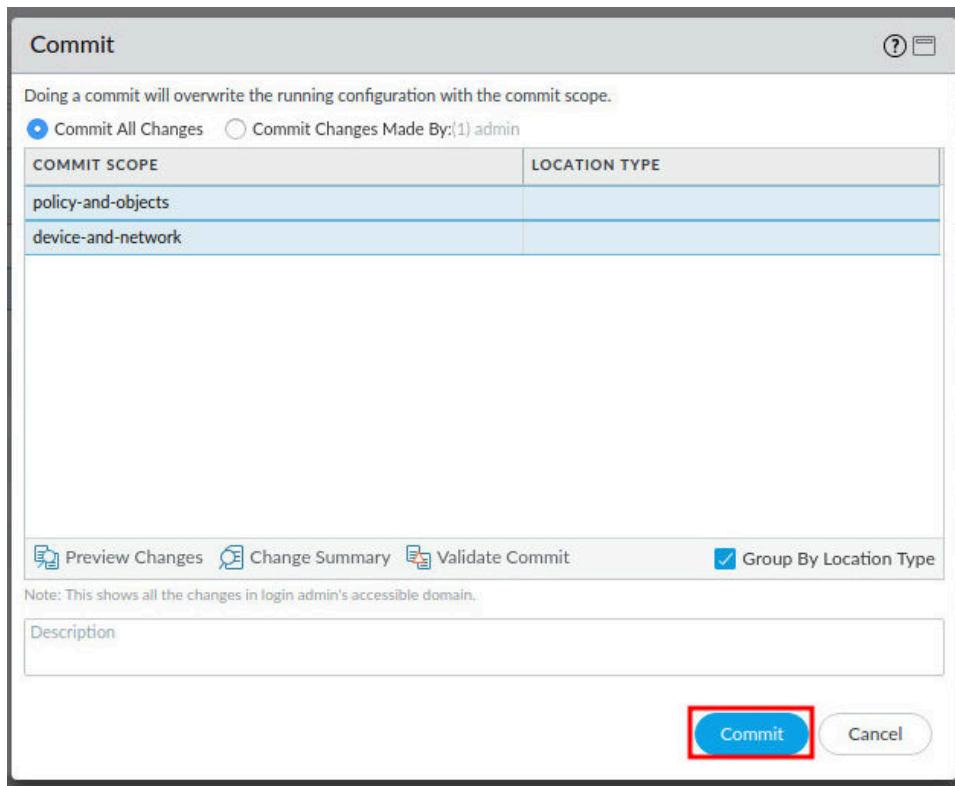


The Warning advises that if you attach this interface management profile to this interface, you are potentially exposing the firewall's administrative interface to any party that can reach this interface. For the purpose of this lab, you will bypass this warning knowing that it is not good practice to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

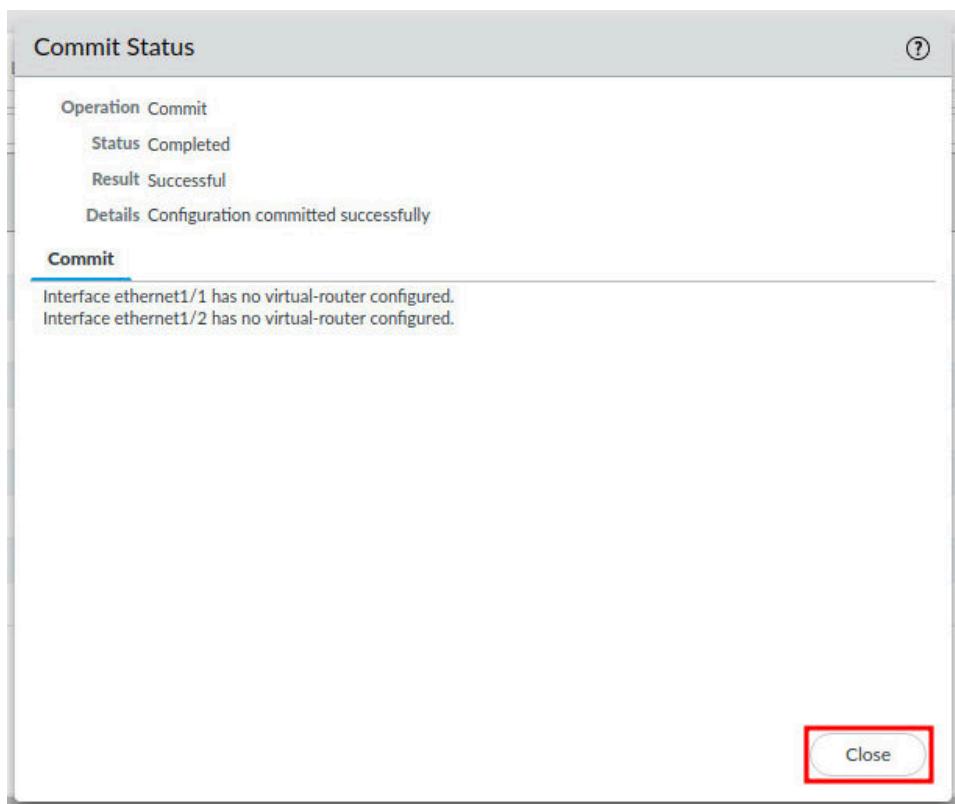
10. Click the **Commit** link located at the top-right of the web interface.



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



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



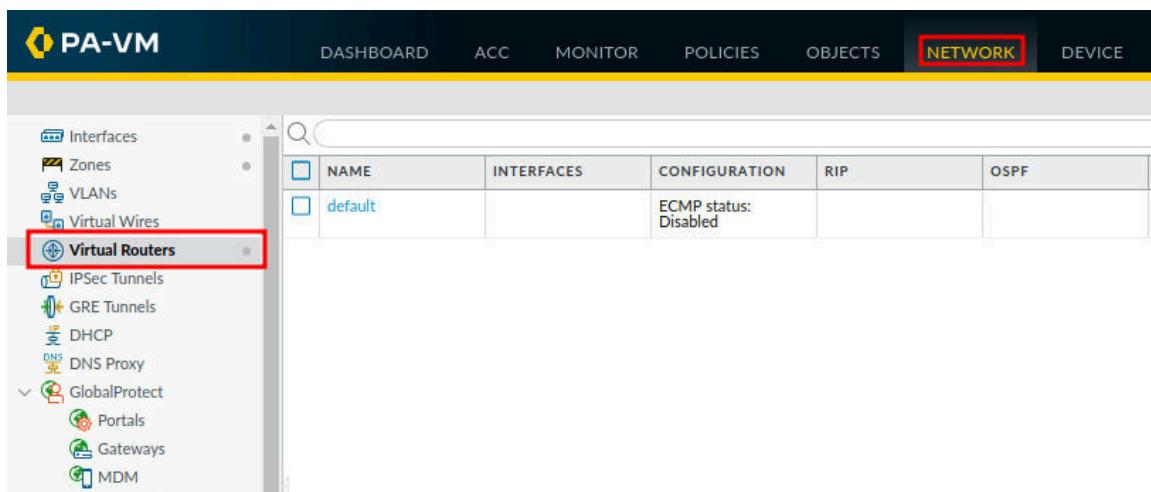


Notice the warnings in the **Commit** section. You will resolve this in the next section.

1.2 Create a Virtual Router

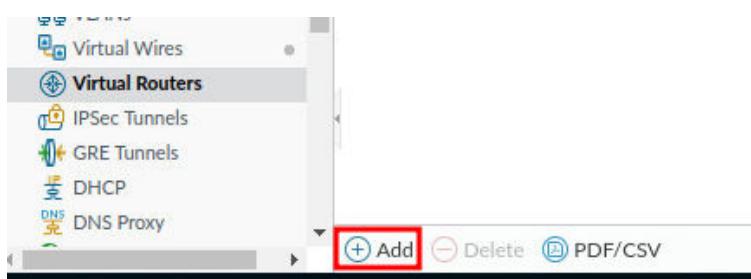
In this section, you will create a Virtual Router. Creating a virtual router allows the Firewall to do routing functions so that the Firewall and devices behind it can access other networks and the Internet.

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



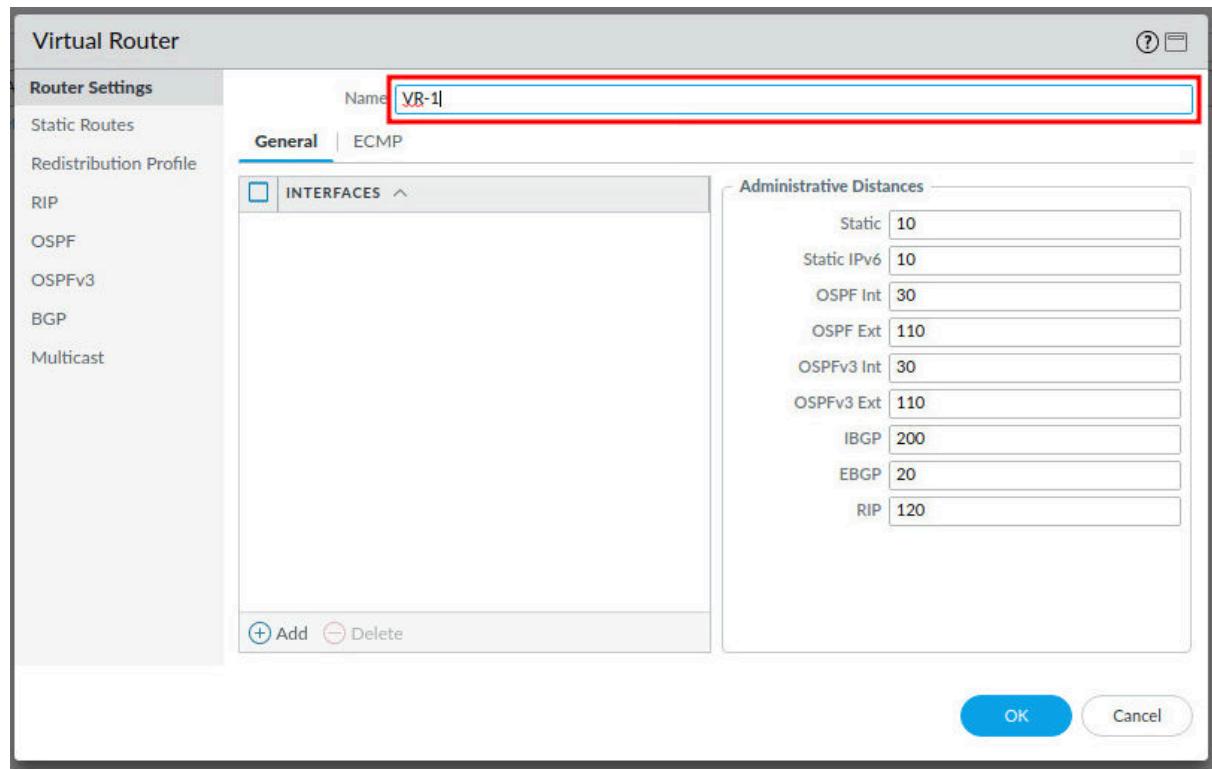
The screenshot shows the PA-VM interface with the 'NETWORK' tab selected. On the left, a sidebar lists various network objects: Interfaces, Zones, VLANs, Virtual Wires, Virtual Routers (which is highlighted with a red box), IPSec Tunnels, GRE Tunnels, DHCP, DNS Proxy, GlobalProtect, Portals, Gateways, and MDM. The main pane displays a table for 'Virtual Routers'. The table has columns: NAME, INTERFACES, CONFIGURATION, RIP, and OSPF. A single entry named 'default' is listed, with the note 'ECMP status: Disabled' under the CONFIGURATION column.

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

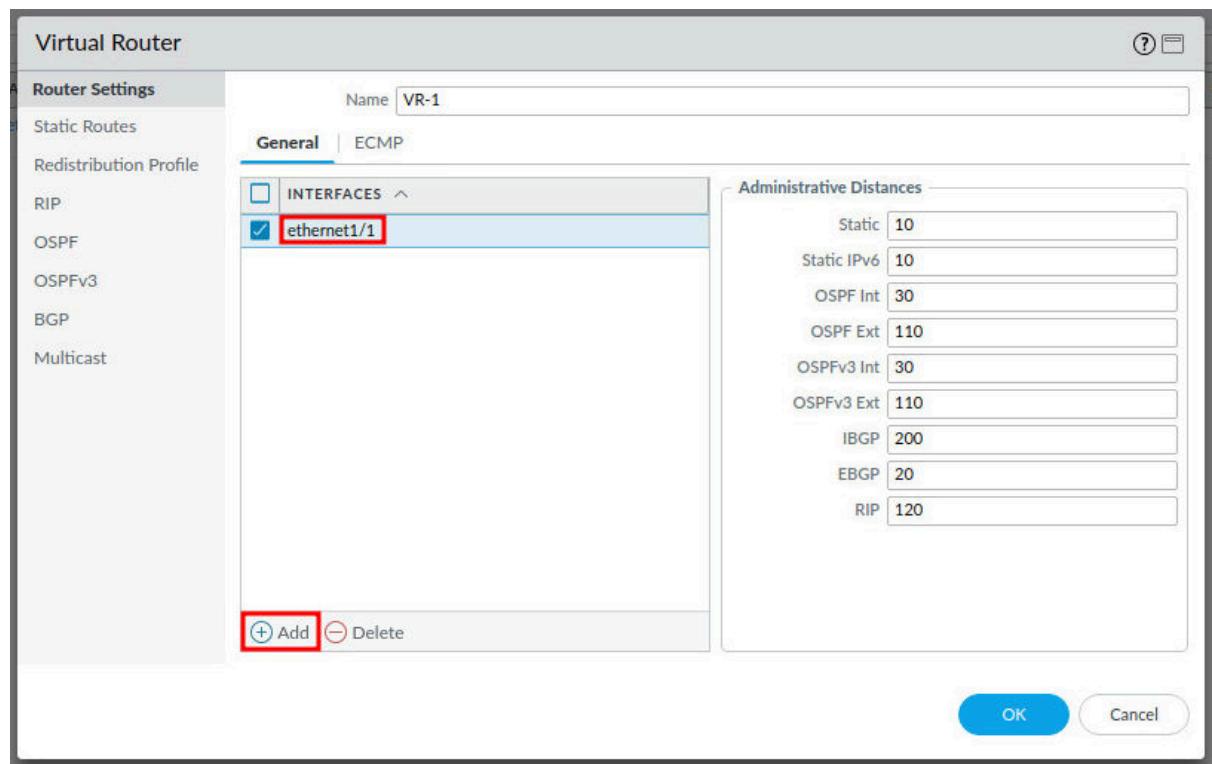


The screenshot shows the PA-VM interface with the 'Virtual Routers' object selected in the sidebar. At the bottom of the main pane, there are three buttons: '+ Add' (highlighted with a red box), 'Delete', and 'PDF/CSV'.

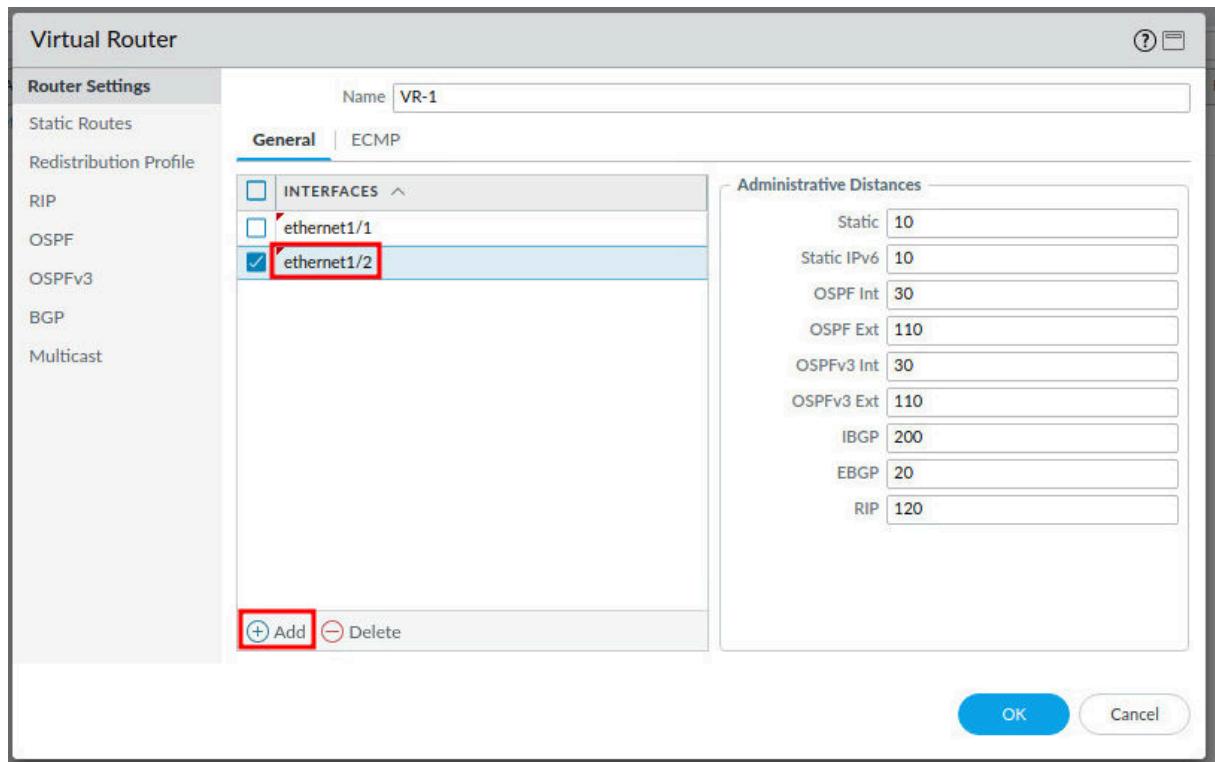
3. In the *Virtual Router* window, type VR-1 in the *Name* field.



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

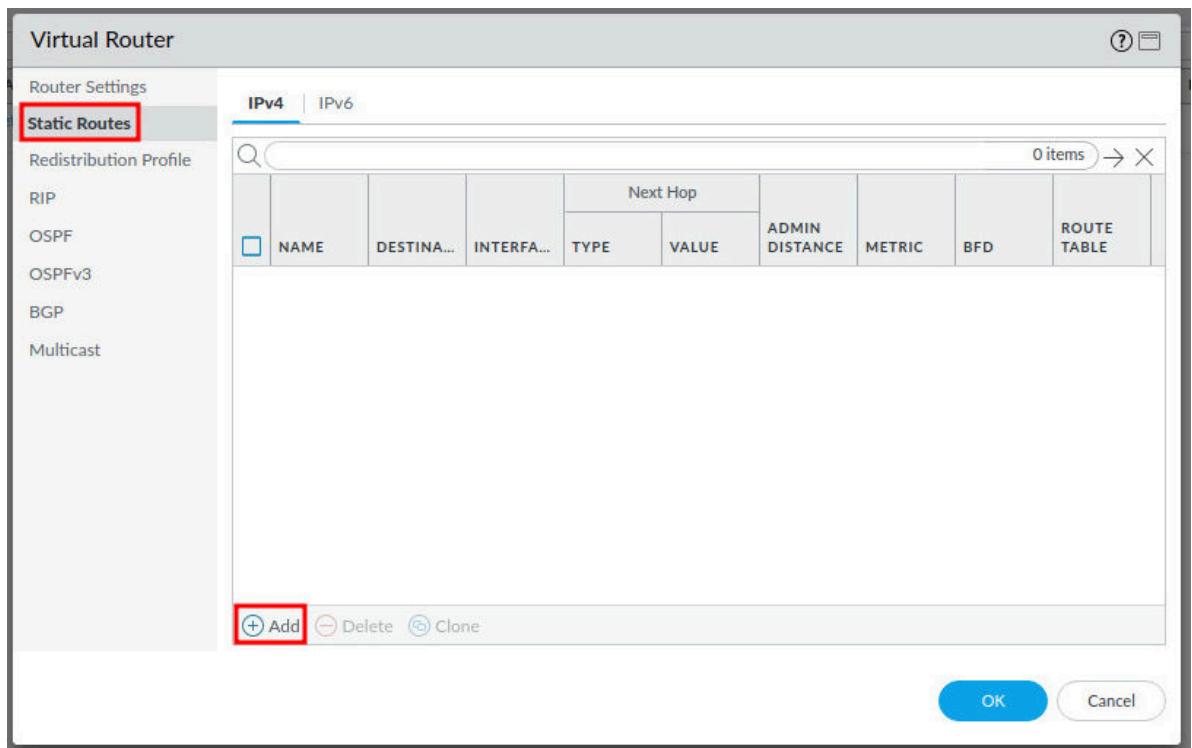


5. Click on the **Add** button and select **ethernet1/2**.

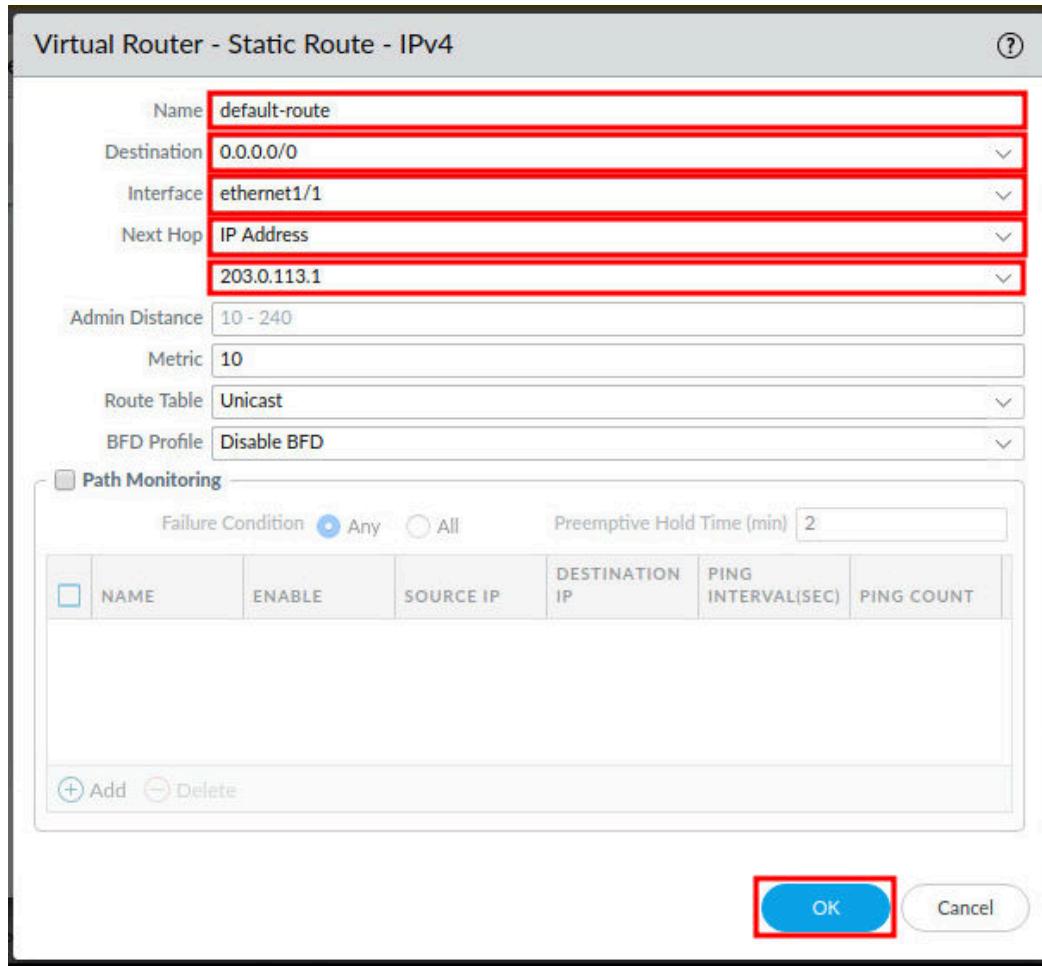


Adding interfaces to the virtual router will allow the networks assigned to these interfaces to route between one another.

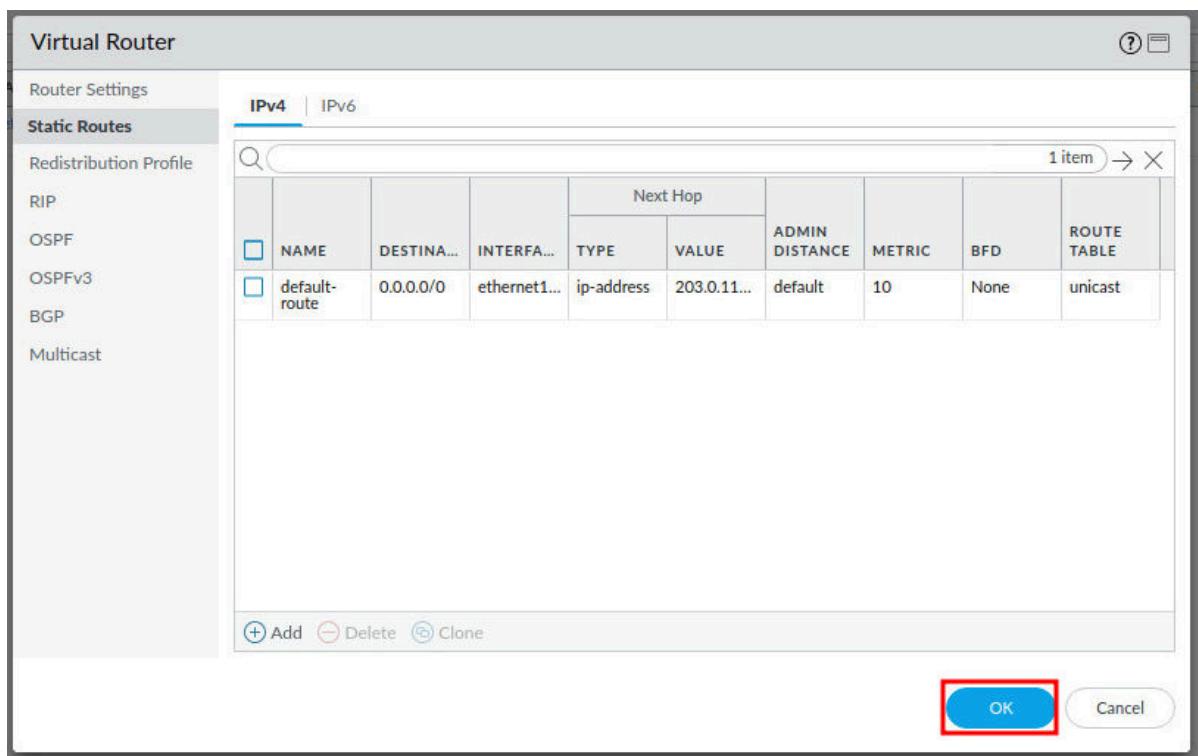
6. Click on the **Static Routes** tab and then click on the **Add** button at the bottom-left.



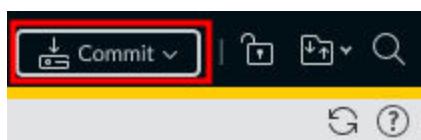
7. In the *Virtual Router – Static Route – Ipv4* window, type **default-route** in the *Name* field. Next, type **0.0.0.0/0** in the *Destination* field. Then, in the *Interface* dropdown, select **ethernet1/1**. Finally, in the *Next Hop* dropdown, ensure **IP Address** is selected, and in the field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



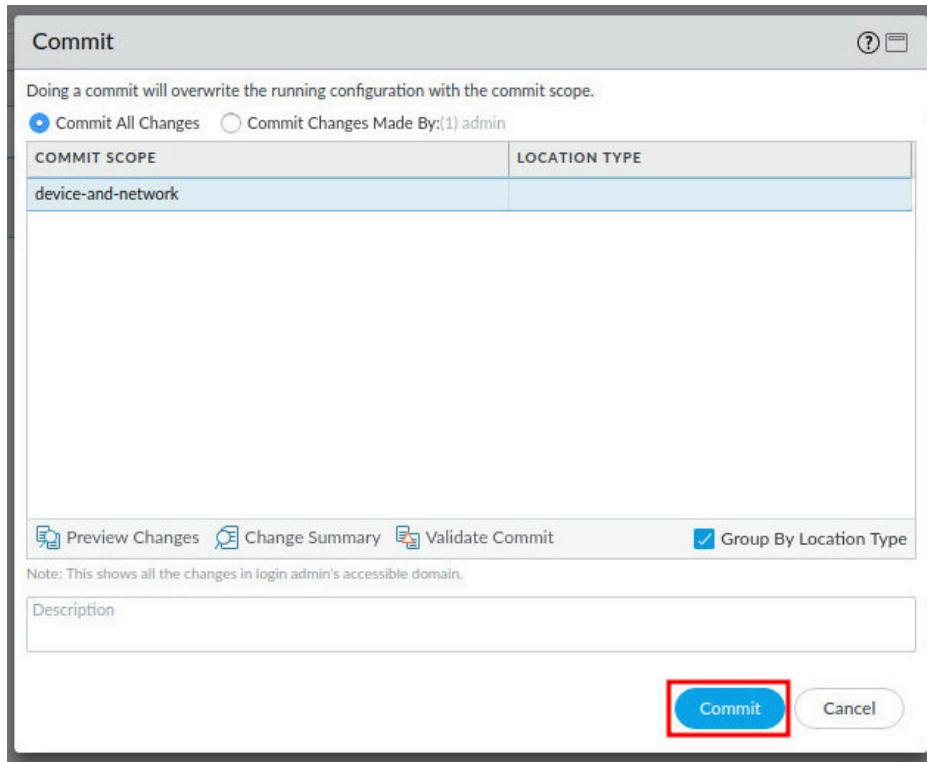
8. Adding a static route of 0.0.0.0/0 is sometimes called *the gateway of last resort*. By adding this static route, if there is a network that the Firewall does not know about, it will forward the packets to this address. Click **OK** to close the *Virtual Router* window.



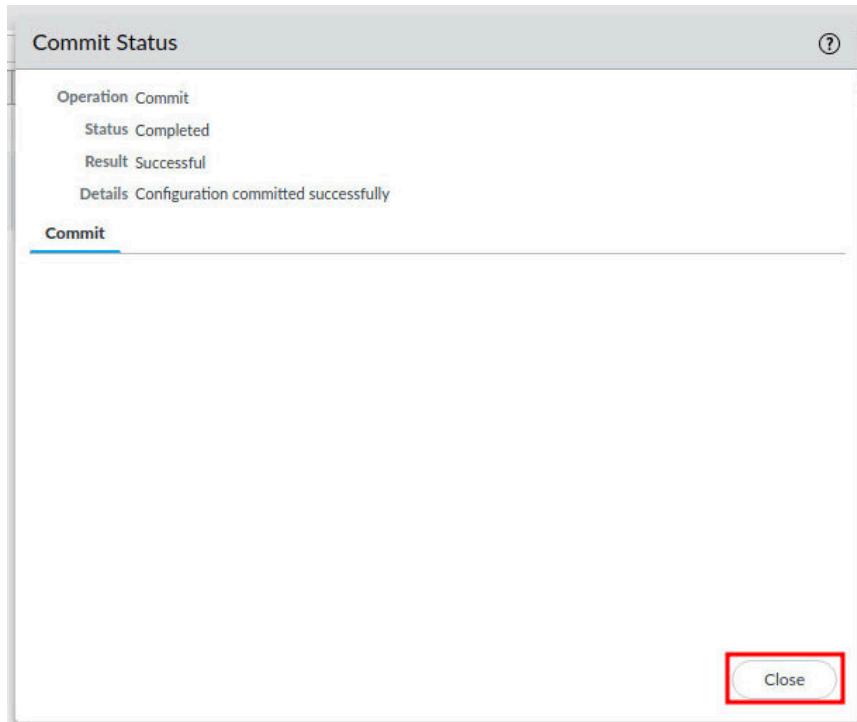
9. Click the **Commit** link located at the top-right of the web interface.



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



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



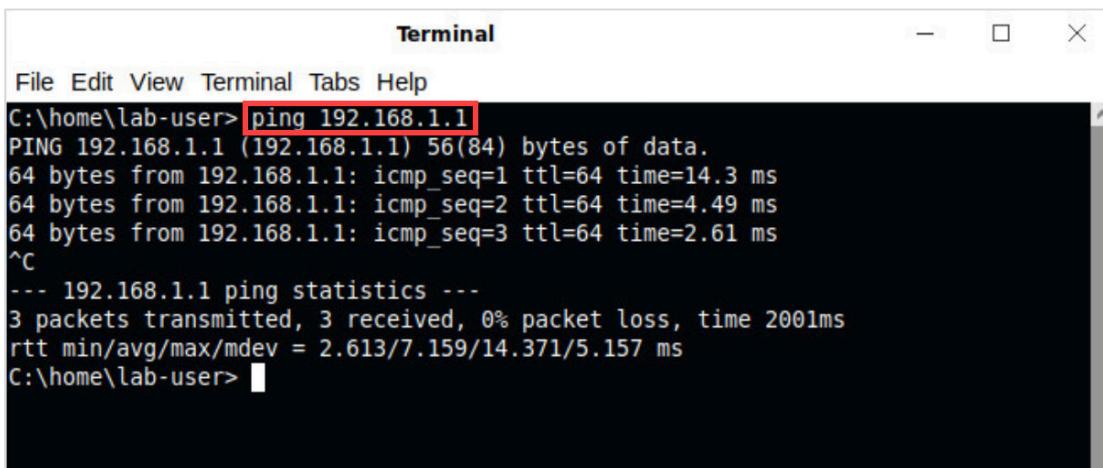
1.3 Verify Network Connectivity

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**.

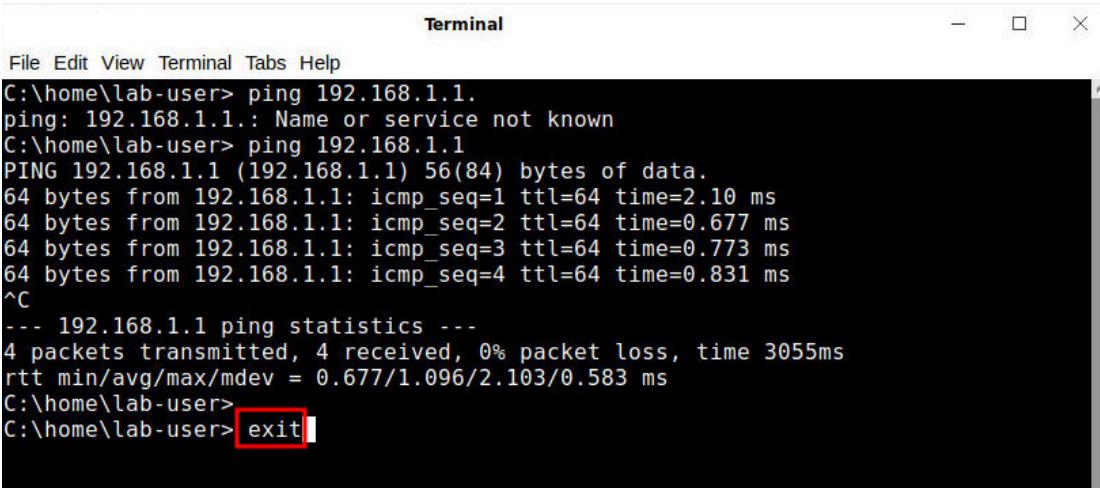


```
Terminal
File Edit View Terminal Tabs Help
C:\home\lab-user> ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=14.3 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=4.49 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=64 time=2.61 ms
^C
--- 192.168.1.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2001ms
rtt min/avg/max/mdev = 2.613/7.159/14.371/5.157 ms
C:\home\lab-user>
```



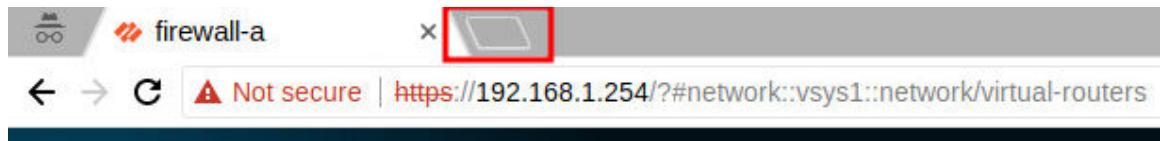
Notice the *ping* command will receive replies from **192.168.1.1**. This means that packets can be sent and received between the Client and the Firewall.

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



```
Terminal
File Edit View Terminal Tabs Help
C:\home\lab-user> ping 192.168.1.1.
ping: 192.168.1.1.: Name or service not known
C:\home\lab-user> ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=2.10 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=0.677 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=64 time=0.773 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=64 time=0.831 ms
^C
--- 192.168.1.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3055ms
rtt min/avg/max/mdev = 0.677/1.096/2.103/0.583 ms
C:\home\lab-user>
C:\home\lab-user> exit
```

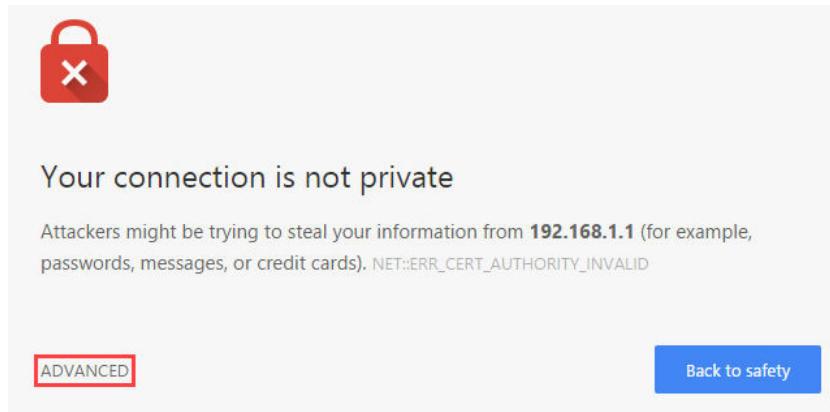
3. In *Chromium*, click on the **New tab** button.



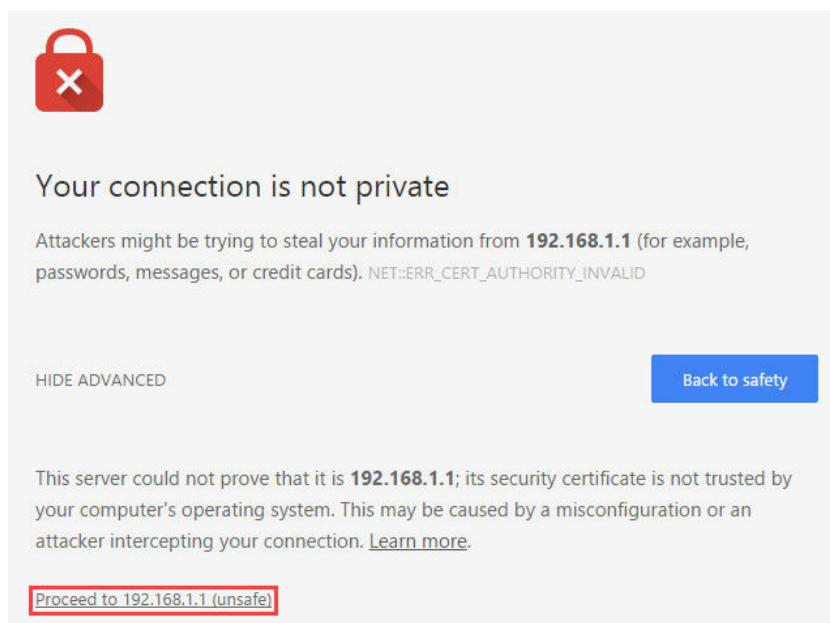
4. In the *address bar*, type `https://192.168.1.1` and press **Enter**.



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.