



PAN9 CYBERSECURITY GATEWAY

Lab 1: Configuring TCP/IP and a Virtual Router

Document Version: 2020-01-24

Copyright © 2020 Network Development Group, Inc.
www.netdevgroup.com

NETLAB Academy Edition, NETLAB Professional Edition, and NETLAB+ are registered trademarks 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 Lab: Configuring TCP/IP and a Virtual Router	6
1.0 Load Lab Configuration	6
1.1 Configure Ethernet Interfaces with Layer 3 Information	10
1.2 Create a Virtual Router	15
1.3 Verify Network Connectivity	20

Introduction

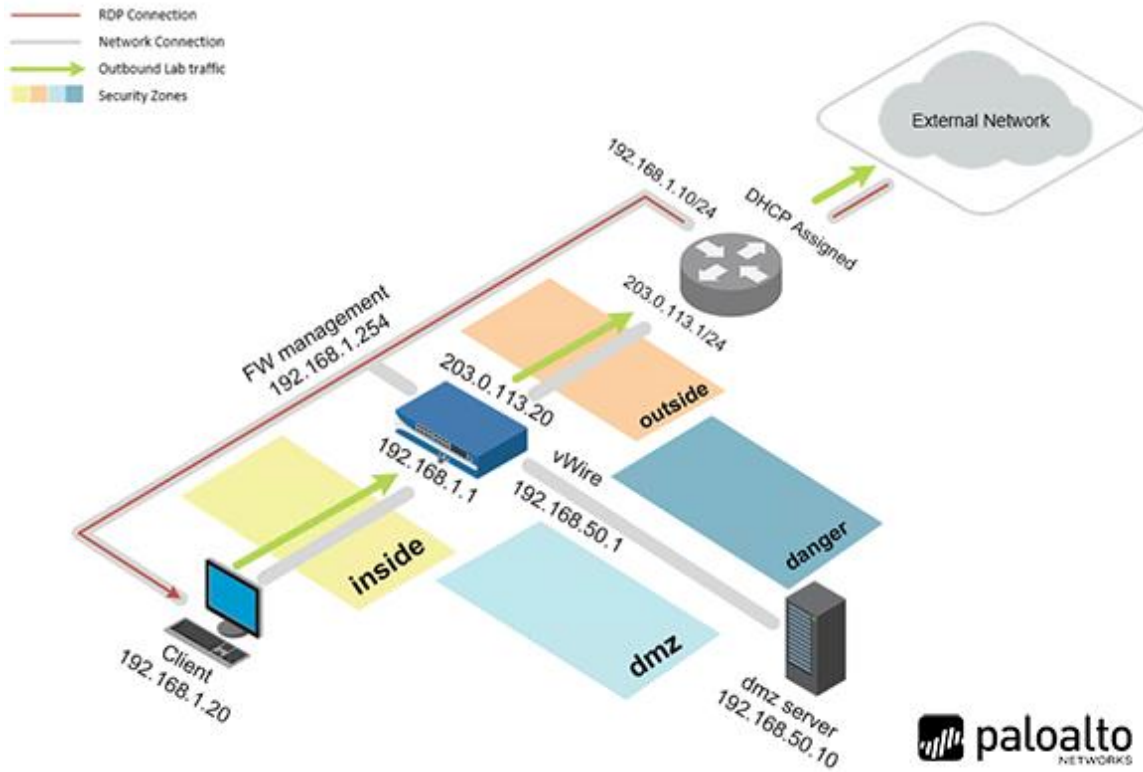
In this lab, you will configure Ethernet interfaces on the Palo Alto Networks Firewall with Layer 3 information, create a Virtual Router to allow traffic, and verify network connectivity.

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.

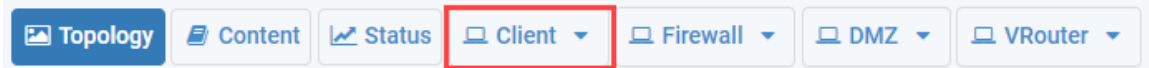
Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Client	192.168.1.20	lab-user	Train1ng\$
DMZ	192.168.50.10	root	Pal0Alt0
Firewall	192.168.1.254	admin	Train1ng\$

1 Lab: Configuring TCP/IP and a Virtual Router

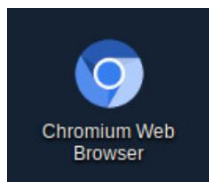
1.0 Load Lab Configuration

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

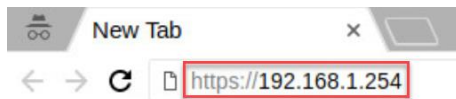
1. Click on the **Client** tab to access the Client PC.



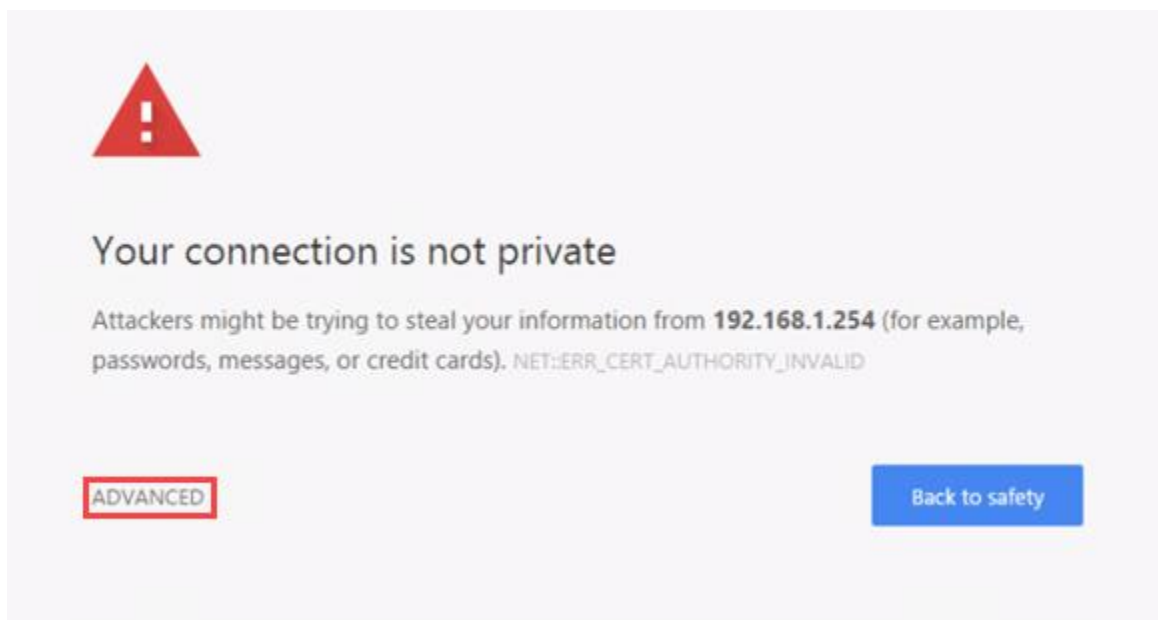
2. Log in to the Client PC as username **lab-user**, password **Train1ng\$**.
3. Double-click the **Chromium Web Browser** icon located on the Desktop.



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



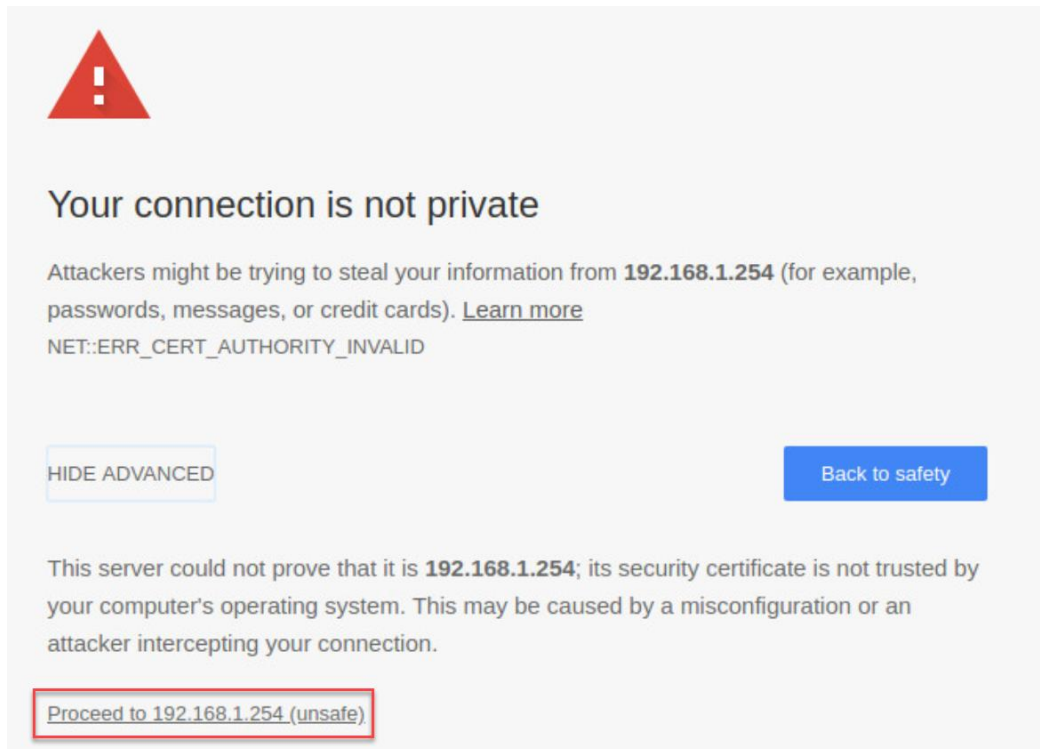
5. You will see a “Your connection is not private” message. Click on the **ADVANCED** link.





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.

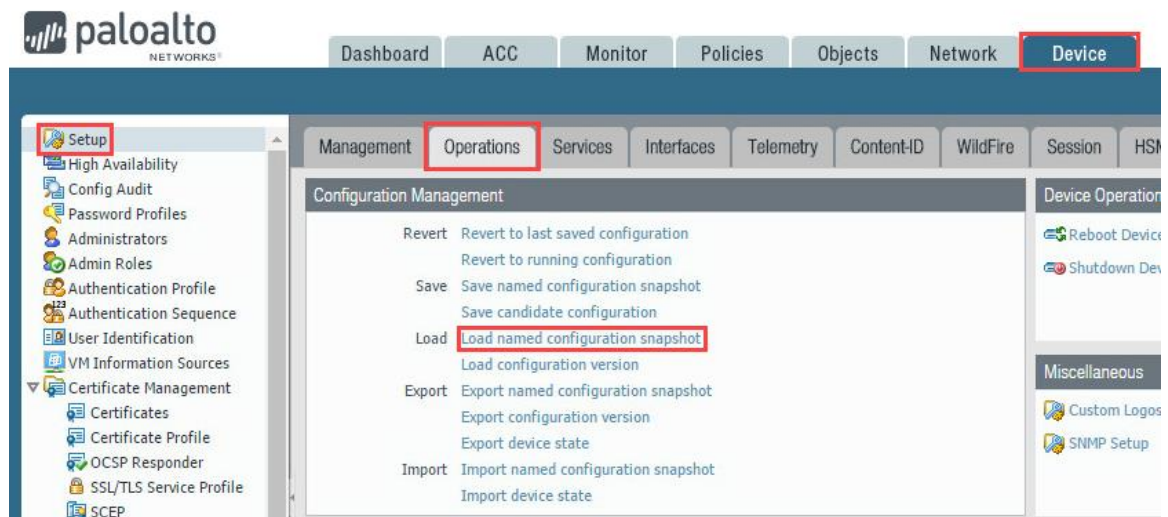
6. Click on **Proceed to 192.168.1.254 (unsafe)**.



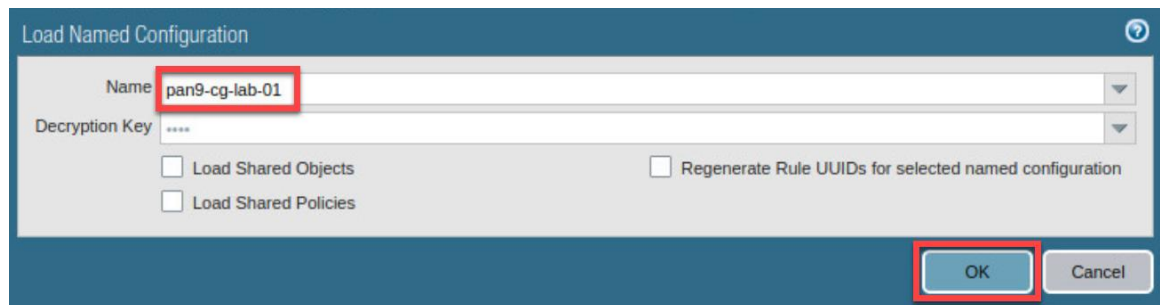
7. Log in to the Firewall web interface as username **admin**, password **Train1ng\$**.



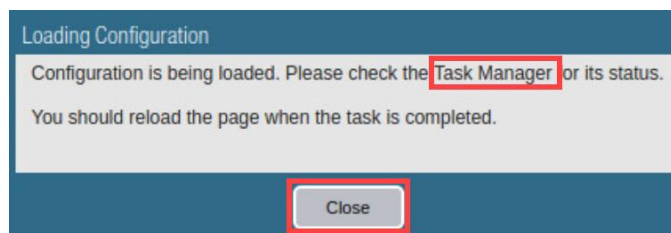
8. In the web interface, navigate to **Device > Setup > Operations** and click on **Load named configuration snapshot** underneath the *Configuration Management* section.



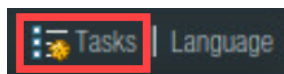
9. In the *Load Named Configuration* window, select **pan9-cg-lab-01** from the *Name* dropdown box and click **OK**.



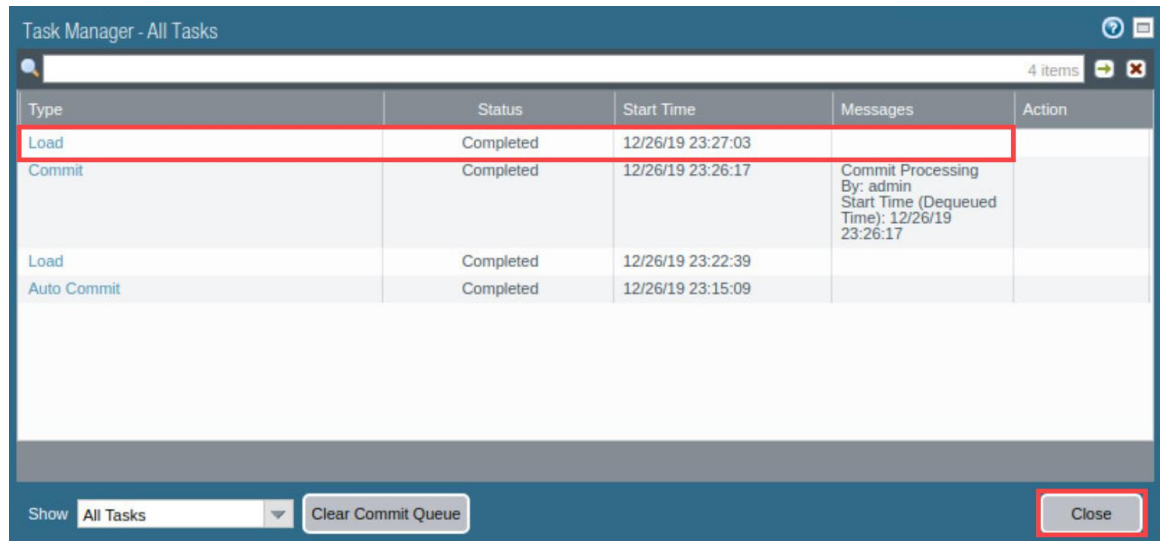
10. In the *Loading Configuration* window, a message will show *Configuration is being loaded*. Please check the *Task Manager* for its status. You should reload the page when the task is completed. Click **Close** to continue.



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



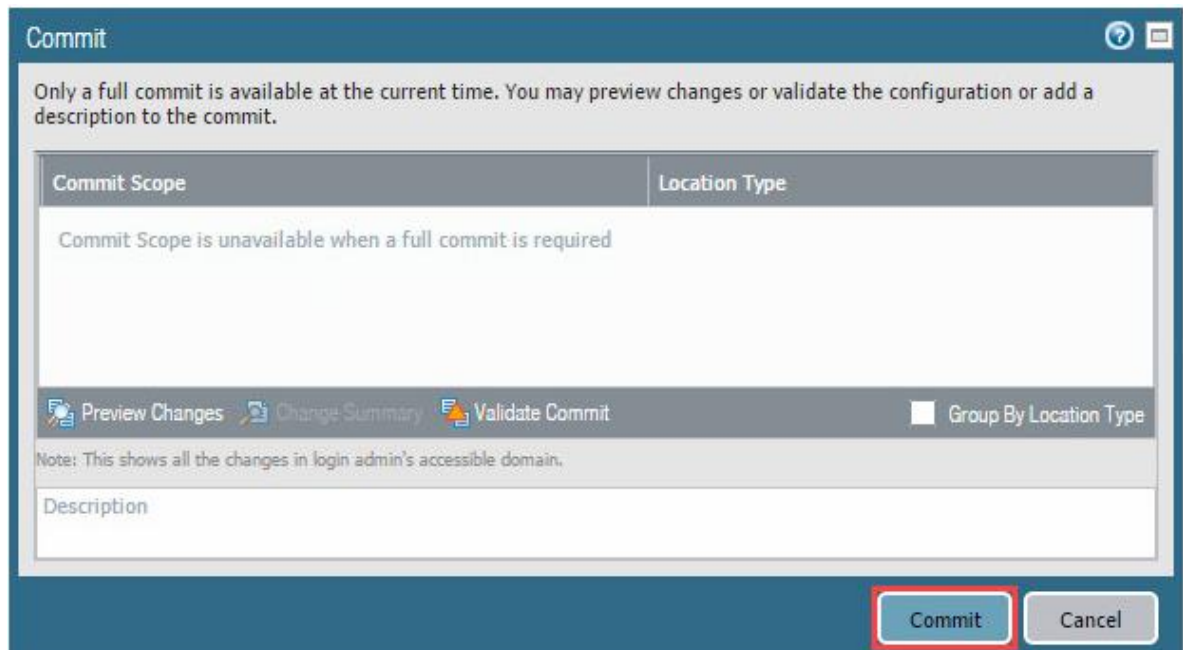
12. In the *Task Manager – All Tasks* window, verify the *Load* type has successfully completed. Click **Close**.



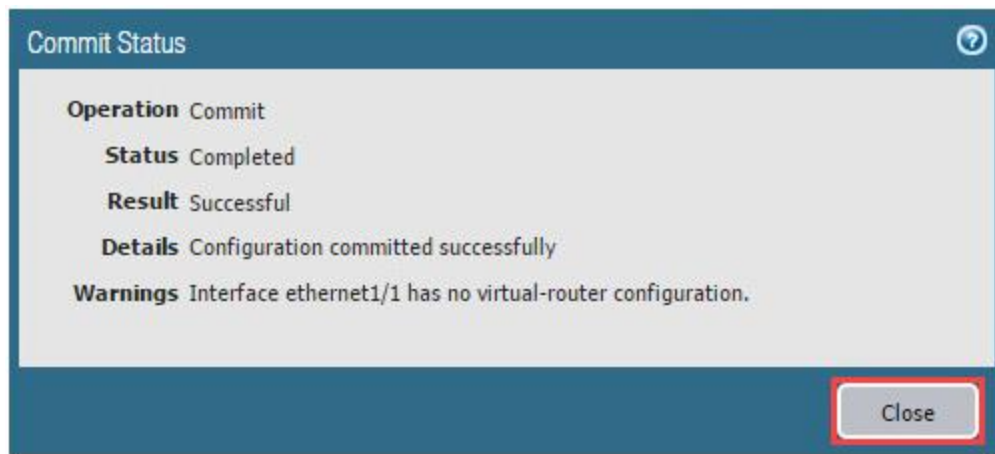
13. Click the **Commit** link located at the top-right of the web interface.



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.



The **Warnings** displayed are normal. You will resolve those during this lab.

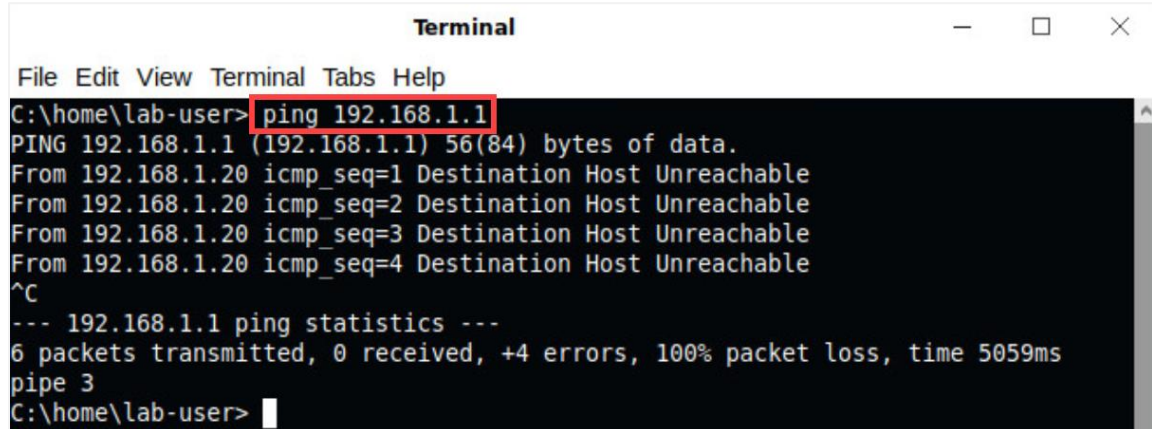
1.1 Configure Ethernet Interfaces with Layer 3 Information

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.



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



```

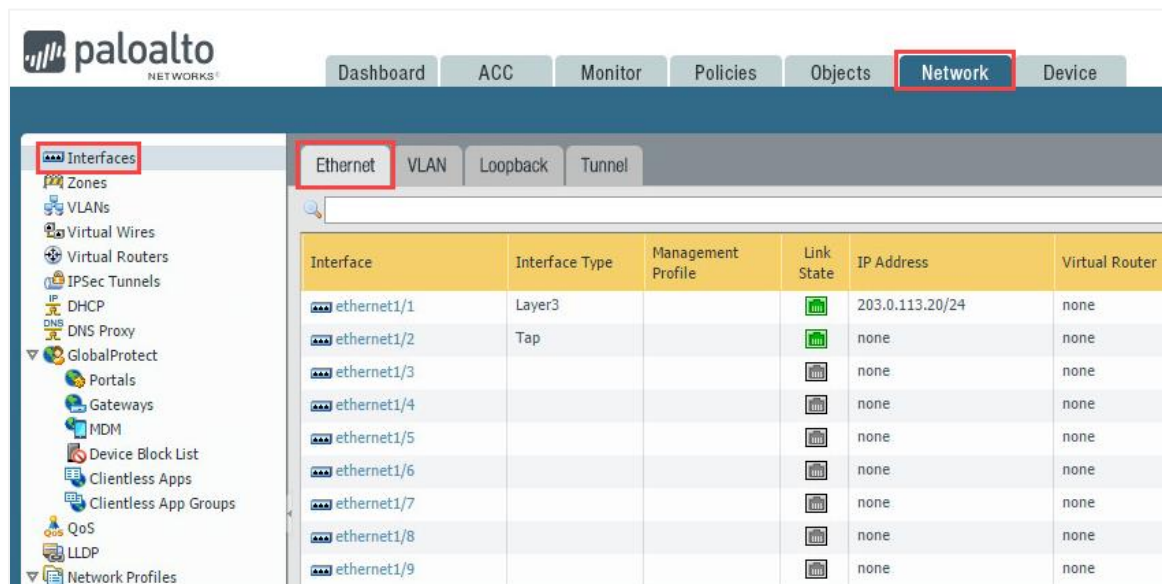
Terminal
File Edit View Terminal Tabs Help
C:\home\lab-user> ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
From 192.168.1.20 icmp_seq=1 Destination Host Unreachable
From 192.168.1.20 icmp_seq=2 Destination Host Unreachable
From 192.168.1.20 icmp_seq=3 Destination Host Unreachable
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.

- Close the *Terminal* window.
- With the Firewall administrator page open, navigate to **Network > Interfaces > Ethernet**.



Interface	Interface Type	Management Profile	Link State	IP Address	Virtual Router
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

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

Ethernet				
VLAN Loopback Tunnel				
Interface	Interface Type	Management Profile	Link State	IP Address
ethernet1/1	Layer3			203.0.113.20/24
ethernet1/2	Tap			none
ethernet1/3				none
ethernet1/4				none
ethernet1/5				none
ethernet1/6				none
ethernet1/7				none
ethernet1/8				none
ethernet1/9				none

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

Ethernet Interface

Interface Nameethernet1/2

Comment

Interface TypeLayer3

Netflow ProfileNone

ConfigIPv4IPv6Advanced

Assign Interface To

Virtual RouterNone

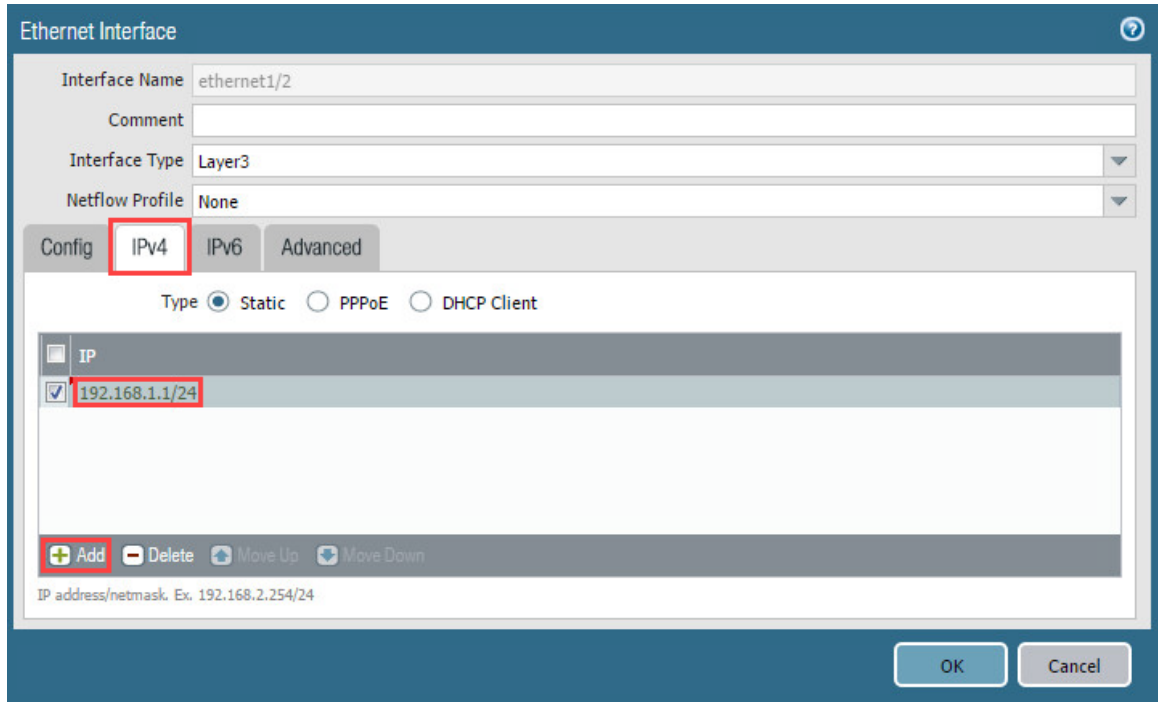
Security Zoneinside

OKCancel



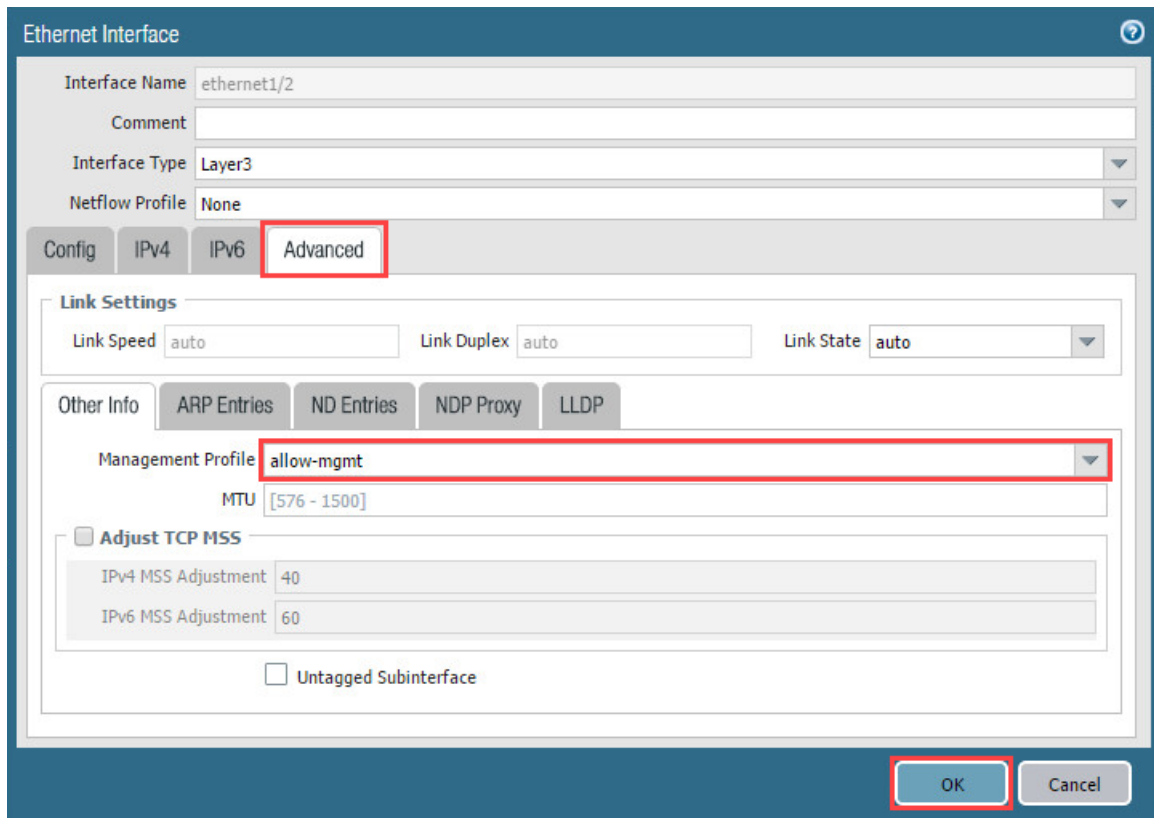
Layer 3 is selected so that the Firewall interface can be given an IP address, assigned a zone, and a virtual router.

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.



The screenshot shows the 'Ethernet Interface' configuration window with the 'IPv4' tab selected. The 'Interface Name' is 'ethernet1/2', 'Interface Type' is 'Layer3', and 'Netflow Profile' is 'None'. Under the 'Type' section, 'Static' is selected. In the IP address list, '192.168.1.1/24' is entered and highlighted with a red box. At the bottom left, the 'Add' button is also highlighted with a red box. The 'OK' and 'Cancel' buttons are at the bottom right.

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

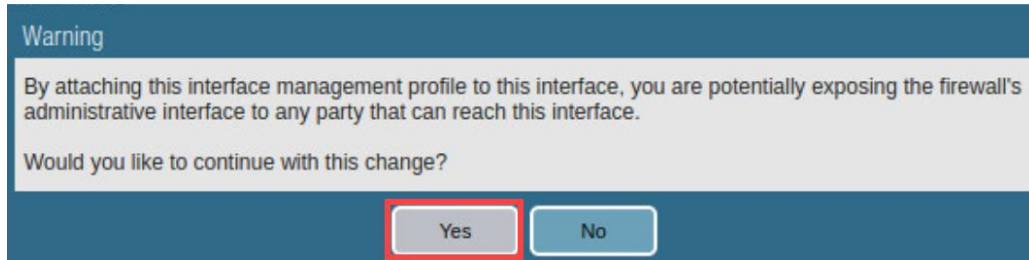


The screenshot shows the 'Ethernet Interface' configuration window with the 'Advanced' tab selected. The 'Link Settings' section shows 'Link Speed' as 'auto', 'Link Duplex' as 'auto', and 'Link State' as 'auto'. Under 'Other Info', the 'Management Profile' dropdown is set to 'allow-mgmt' and is highlighted with a red box. The 'MTU' is set to '[576 - 1500]'. The 'Adjust TCP MSS' section is expanded, showing 'IPv4 MSS Adjustment' as 40 and 'IPv6 MSS Adjustment' as 60. The 'Untagged Subinterface' checkbox is unchecked. The 'OK' button at the bottom right is highlighted with a red box.



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**.

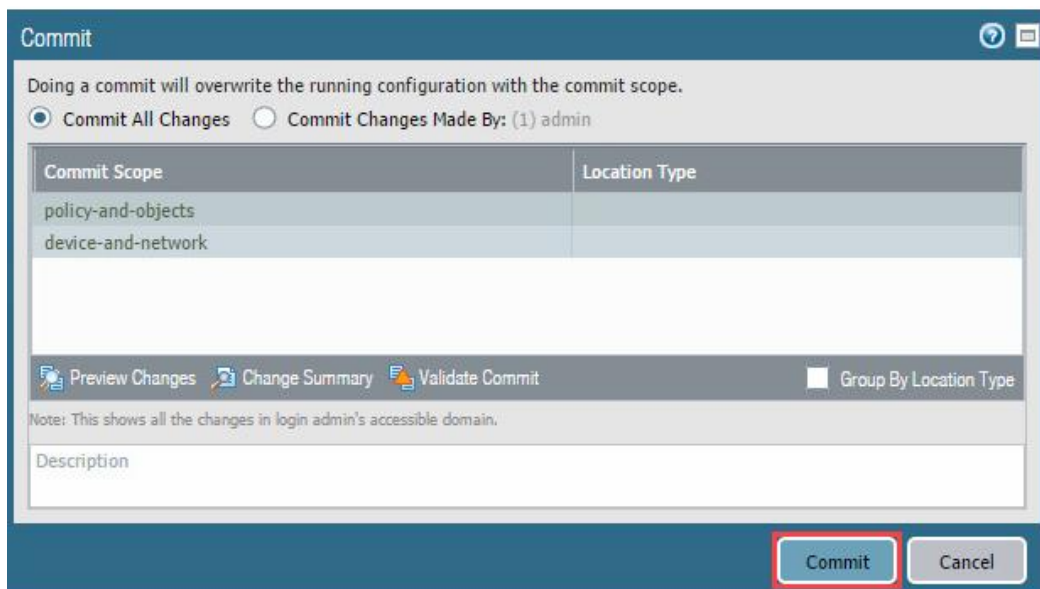


The *Warning* advises that if you attach this interface management profile to this interface, you are potentially exposing the firewall's administrative interface to any party that can reach this interface. For the purpose of this lab, you will bypass this warning knowing that it is not good practice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

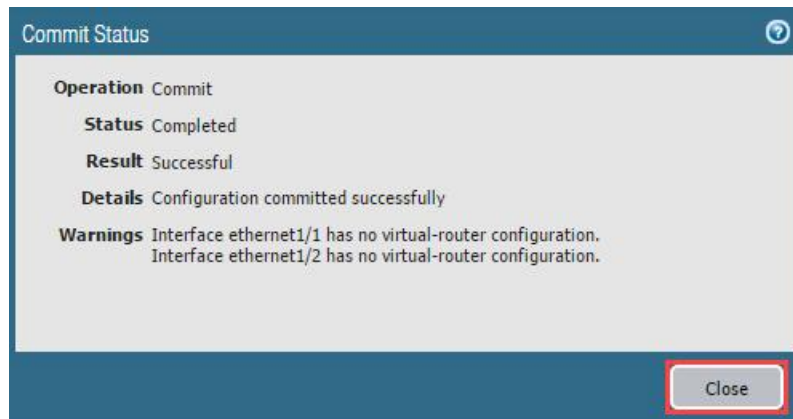
10. Click the **Commit** link located at the top-right of the web interface.



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



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

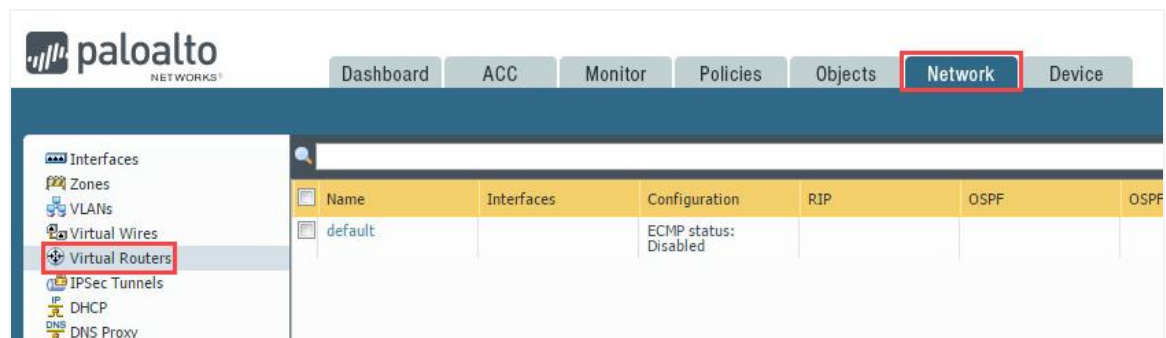


Notice the **Warnings** section. You will resolve this in the next section.

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.

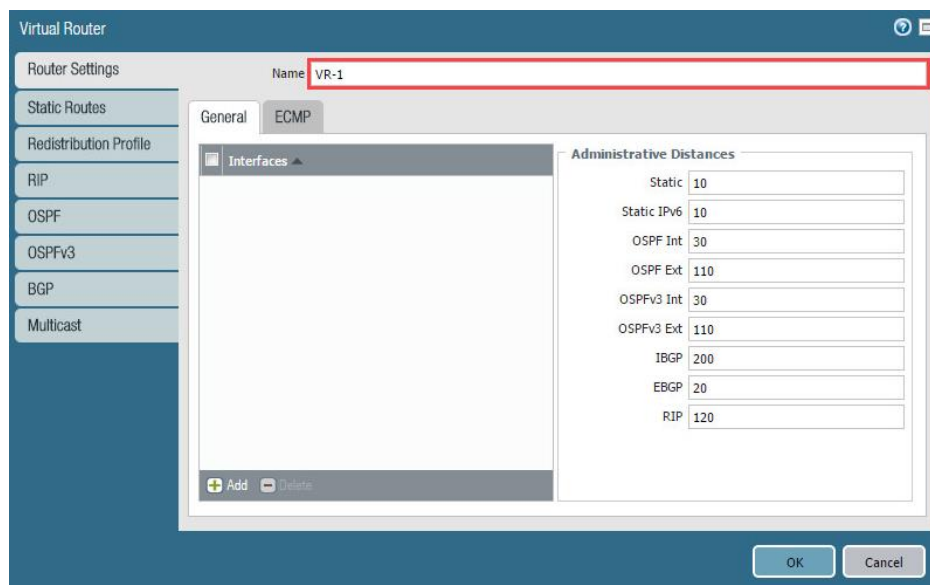
1. Navigate to **Network > Virtual Routers**.



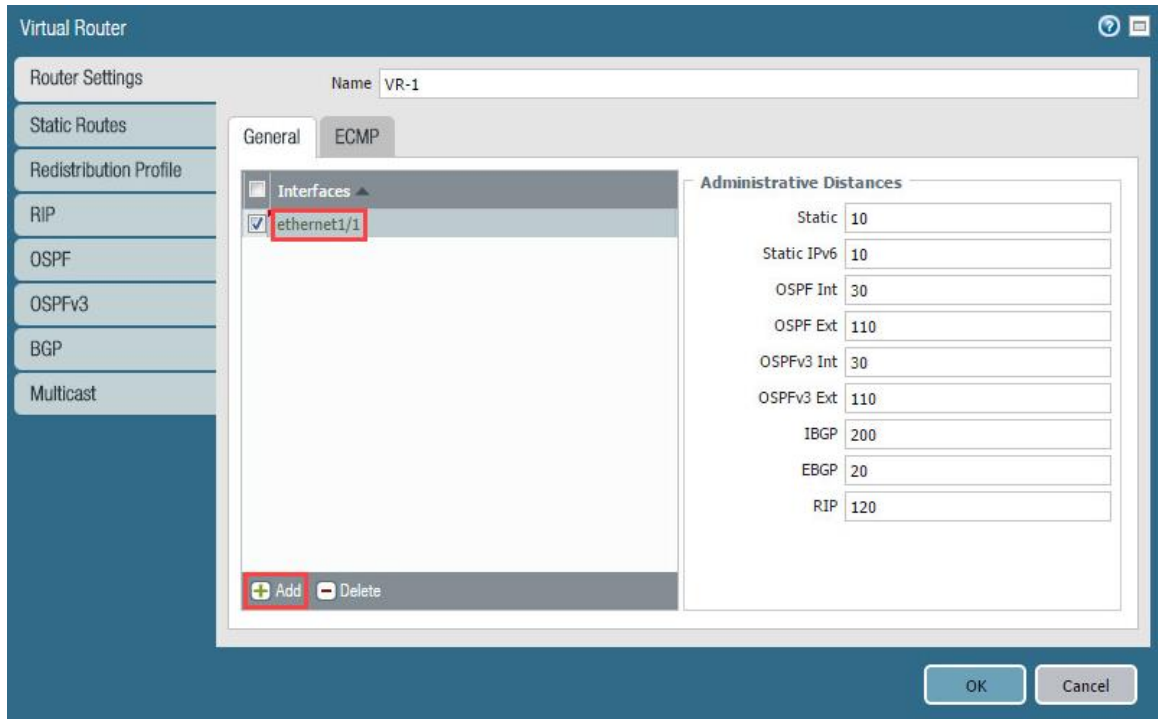
- Click on **Add**, located at the bottom-left of the window to create a new virtual router.



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



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



Virtual Router

Router Settings

Name VR-1

General ECMP

Interfaces

- ☒ ethernet1/1

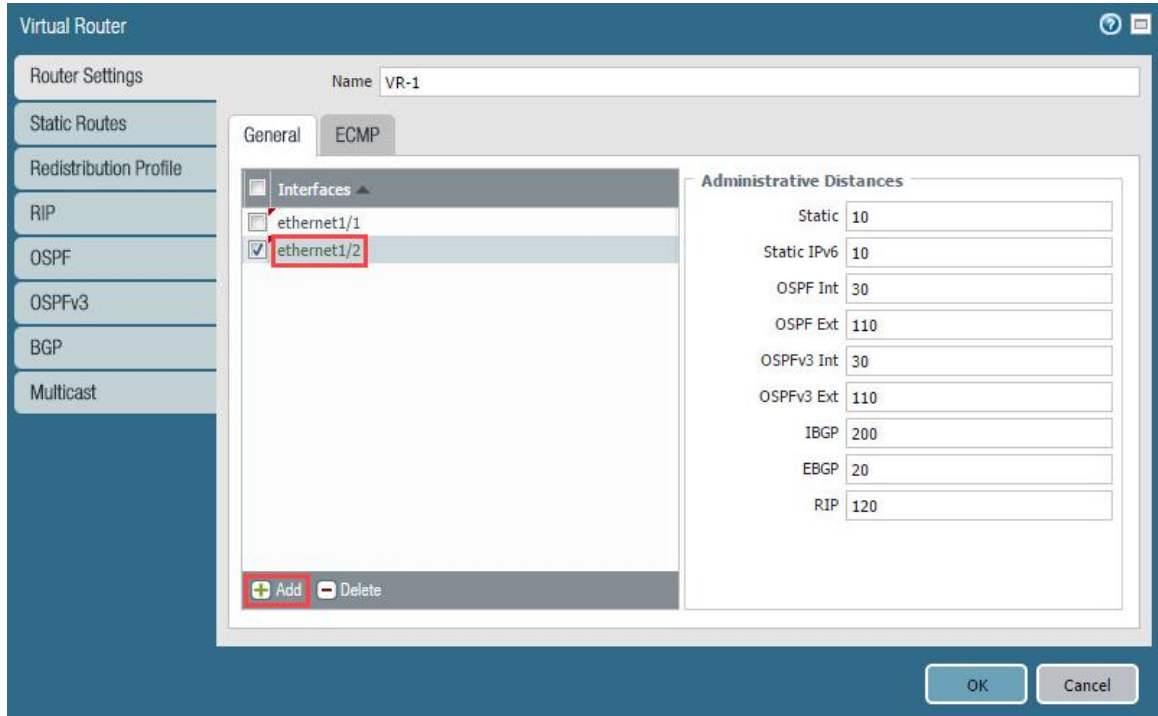
Add Delete

Administrative Distances

Static	10
Static IPv6	10
OSPF Int	30
OSPF Ext	110
OSPFv3 Int	30
OSPFv3 Ext	110
IBGP	200
EBGP	20
RIP	120

OK Cancel

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



Virtual Router

Router Settings

Name VR-1

General ECMP

Interfaces

- ☐ ethernet1/1
- ☒ ethernet1/2

Add Delete

Administrative Distances

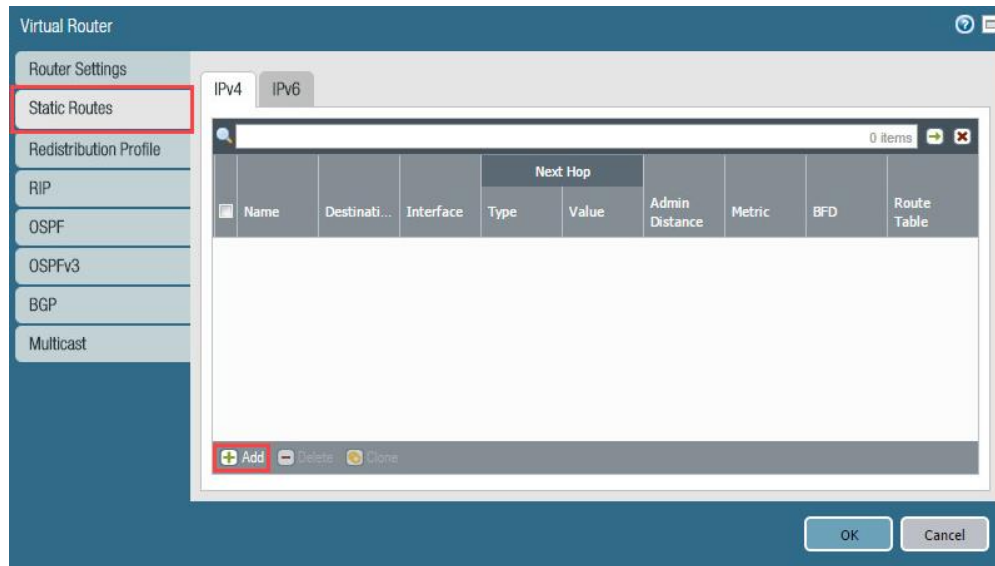
Static	10
Static IPv6	10
OSPF Int	30
OSPF Ext	110
OSPFv3 Int	30
OSPFv3 Ext	110
IBGP	200
EBGP	20
RIP	120

OK Cancel

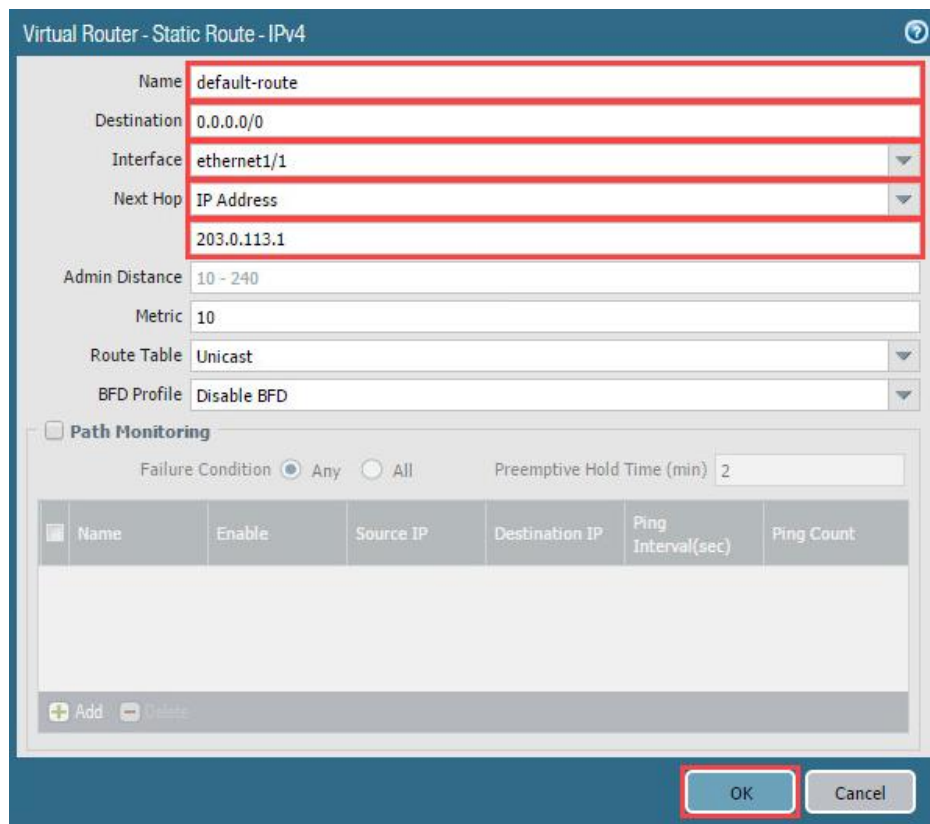


Adding interfaces to the virtual router will allow the networks assigned to these interfaces to route between one another.

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



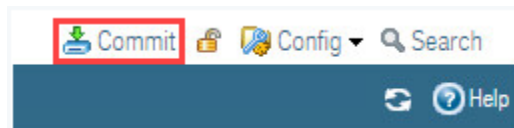
- In the *Virtual Router – Static Route – Ipv4* window, type **default-route** in the *Name* field. Next, type **0.0.0.0/0** in the *Destination* field. Then, in the *Interface* dropdown, select **ethernet1/1**. Finally, in the *Next Hop* dropdown, ensure **IP Address** is selected, and in the field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



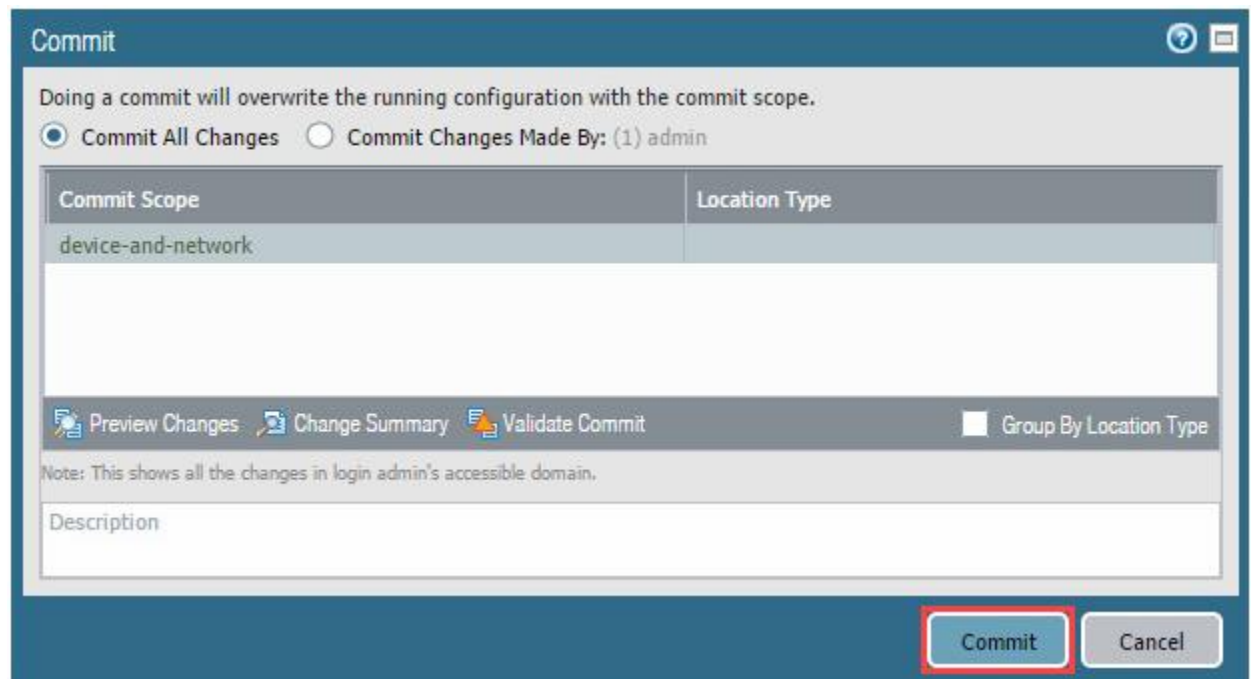


You may need to click on **OK** twice, depending on mouse focus.

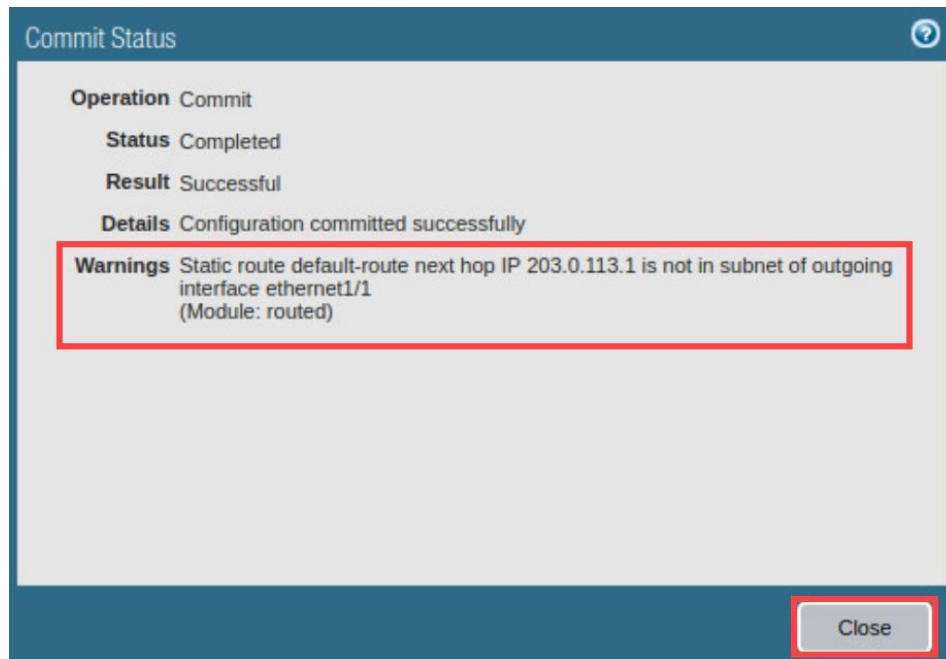
8. Adding a static route of 0.0.0.0/0 is sometimes called *the gateway of last resort*. By adding this static route, if there is a network that the Firewall does not know about, it will forward the packets to this address. Click **OK** to save the profile.
9. Click the **Commit** link located at the 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.



Notice the **Warnings** section. This is a new check that is part of 9.0. This new feature allows the FQDN to be used as “Next Hop”. The static route next hop must resolve the IP Address that belongs to the same subnet as the interface that was configured for the static route. This warning can be resolved by ensuring that the IP Address belongs to the same subnet as the interface you configured in which the static route resides. For this lab, you have successfully configured IP address information and created a Virtual Router to route traffic.

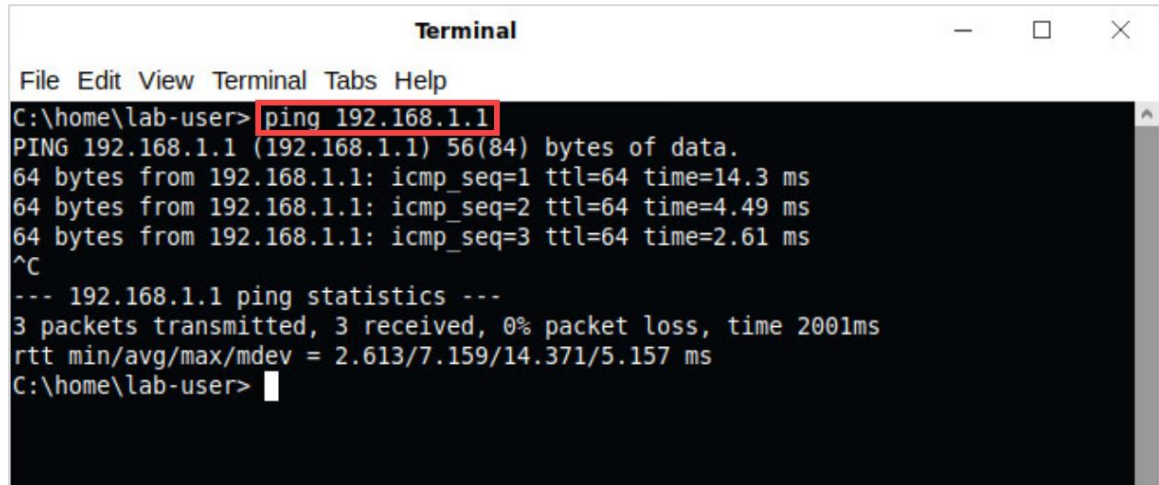
1.3 Verify Network Connectivity

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.

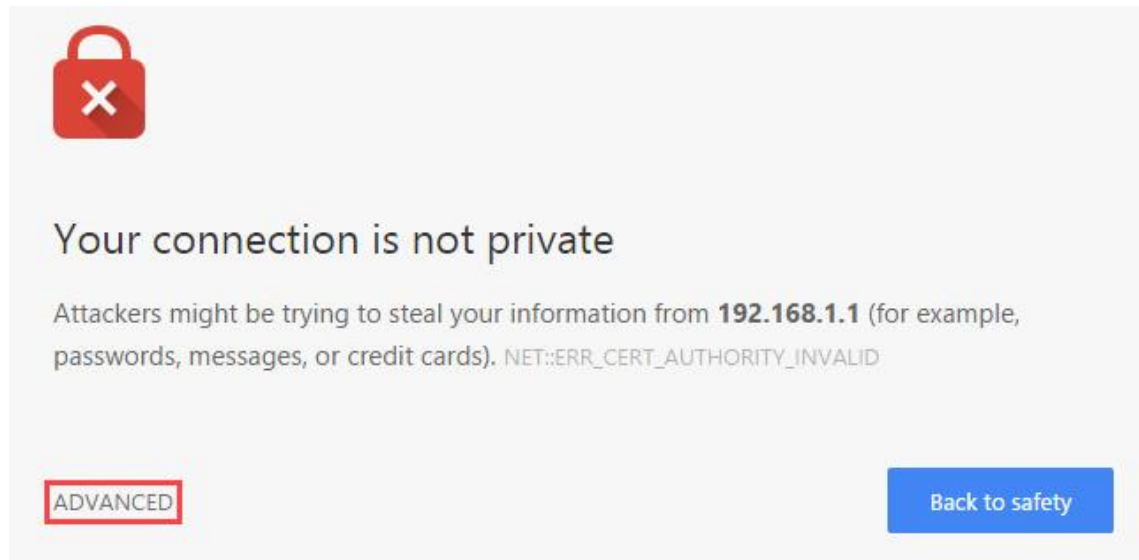
3. Close the *Terminal* window.
4. In *Chromium*, click on the **New tab** button.



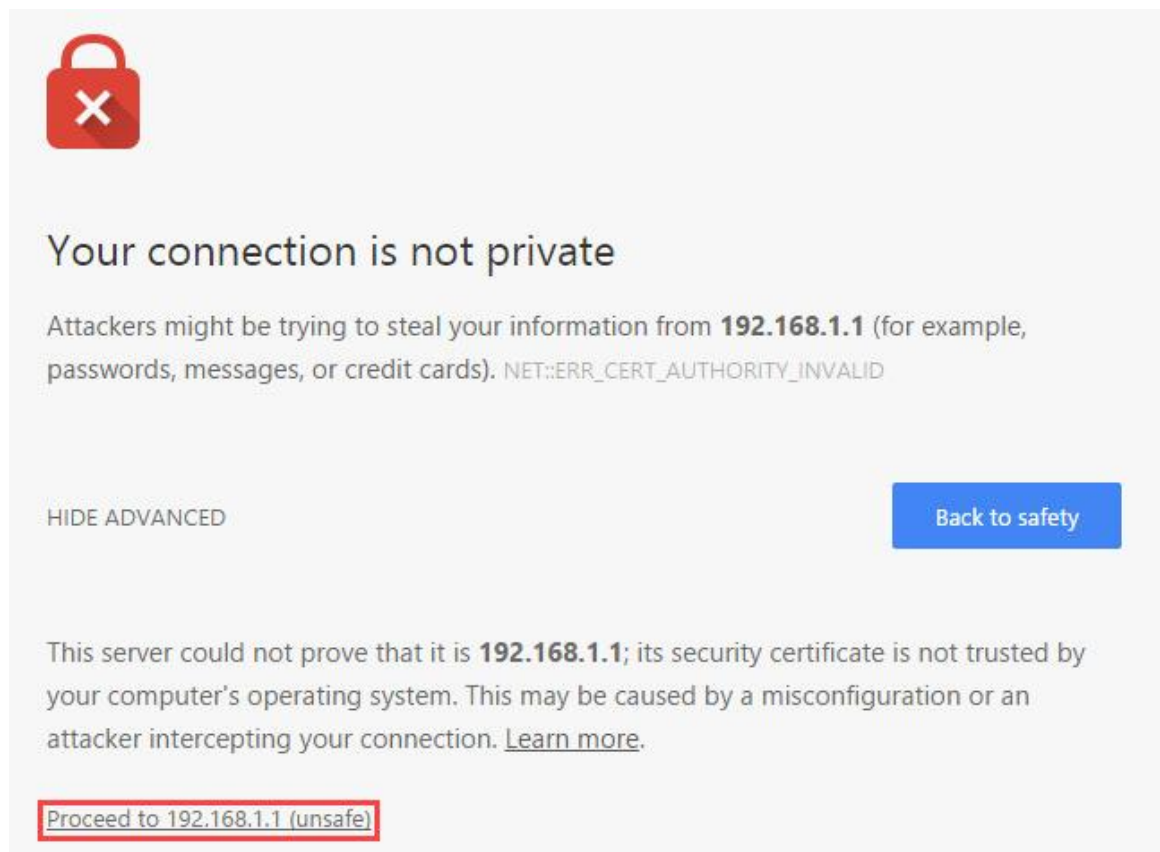
5. In the *address bar*, type **https://192.168.1.1** and press **Enter**.



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



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



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



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