PALO ALTO NETWORKS - EDU-210

Lab 2: Interface Configuration

Document Version: 2019-11-12

Contents

Introduction

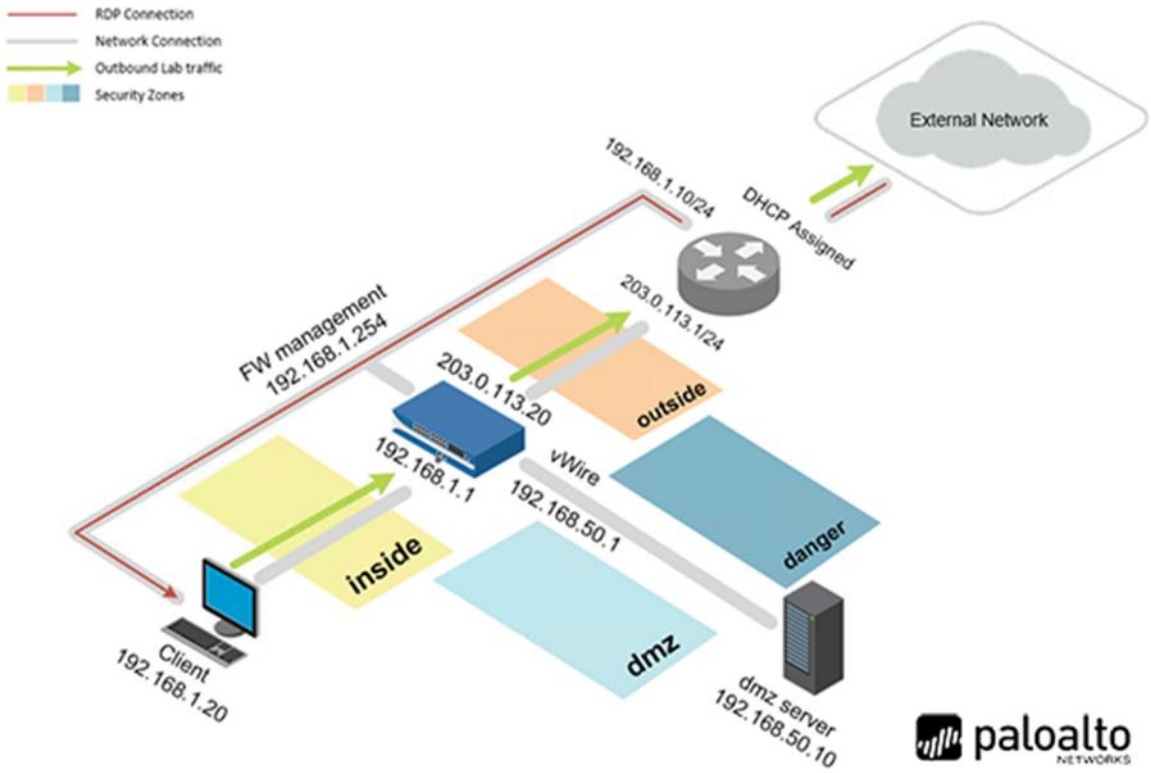
Now that we have set up our admin accounts, verified that we can connect to the admin portal, and set up our system to begin receiving updates, it is now time to start configuring our firewall appliance.

The company's security and network architects have decided what zones and IP addresses we will use in our environment. It is your job now to configure those zones and interfaces on the appliances. Once you have completed the configurations, you will need to test the connectivity and verify everything is working correctly.

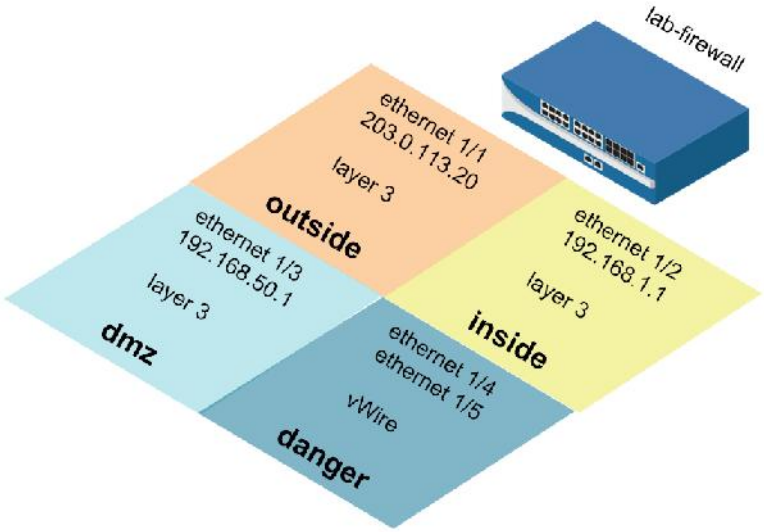
Objectives

- Create security zones two different ways and observe the time saved
- Create Interface Management Profiles to allow ping and responses pages
- Configure Ethernet interfaces to observe DHCP client options and static configuration
- Create a virtual router and attach configured Ethernet interfaces
- Test connectivity with automatic default route configuration and static configuration

Lab Topology



Theoretical 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`
Firewall	192.168.1.254	`admin`	`admin`

1 Interface Configuration

1.0 Load Lab Configuration

1. Launch the **Client** virtual machine to access the graphical login screen.

To launch the console window for a virtual machine, you may access by either clicking on the machine's graphic image from the topology page or by clicking on the machine's respective tab from the navigation bar.

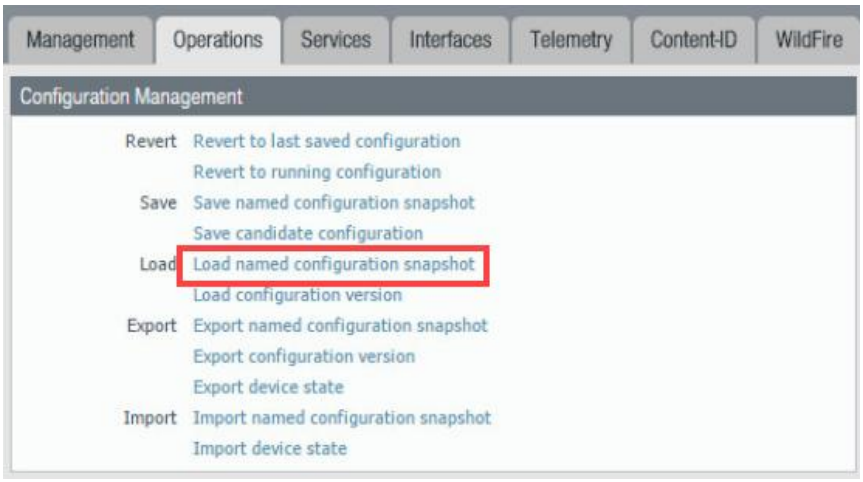
2. Click within the splash screen to bring up the login screen. Log in as **`lab-user`** using the password **`Pal0Alt0`**.

3. Launch the **Chrome** browser and connect to **`https://192.168.1.254`**.
4. If a security warning appears, click **Advanced** and proceed by clicking on **Proceed to 192.168.1.254 (unsafe)**.
5. Log in to the *Palo Alto Networks* firewall using the following:

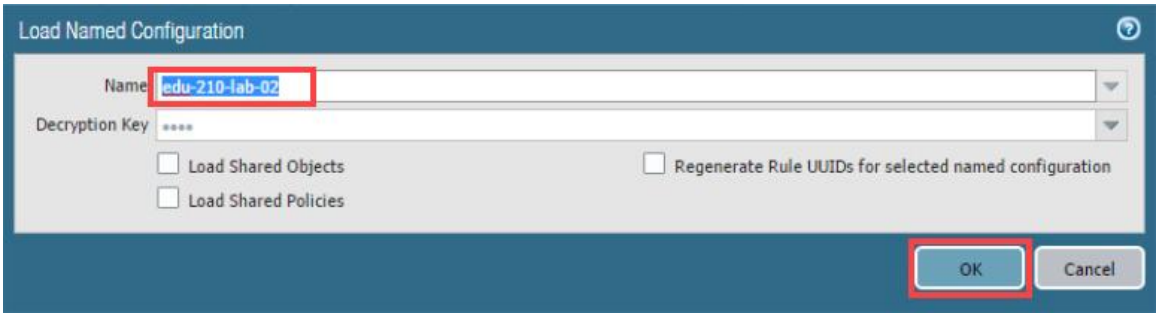
Parameter	Value
Name	**`admin`**
Password	**`admin`**

6. In the web interface, select **Device > Setup > Operations**.

7. Click **Load named configuration snapshot**:



8. Click the drop-down list next to the *Name* text box and select **edu-210-lab-02**. Click **OK**.

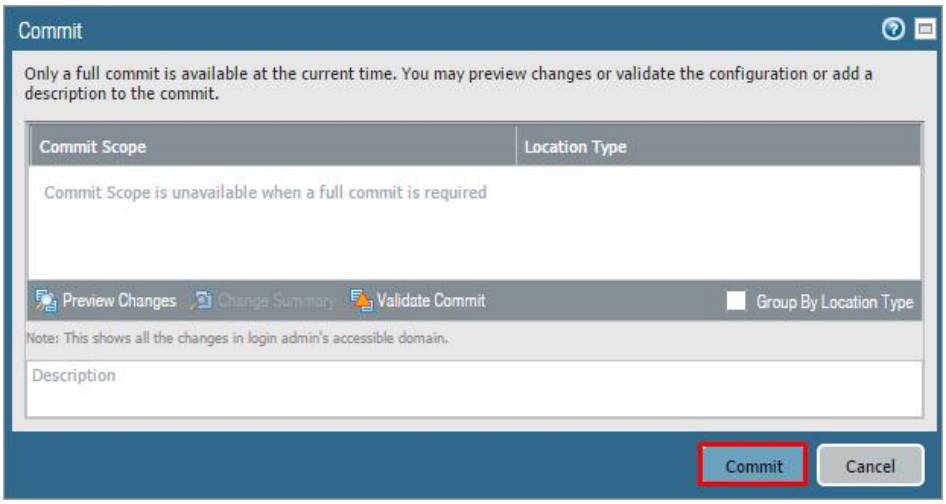


9. Click **Close**.

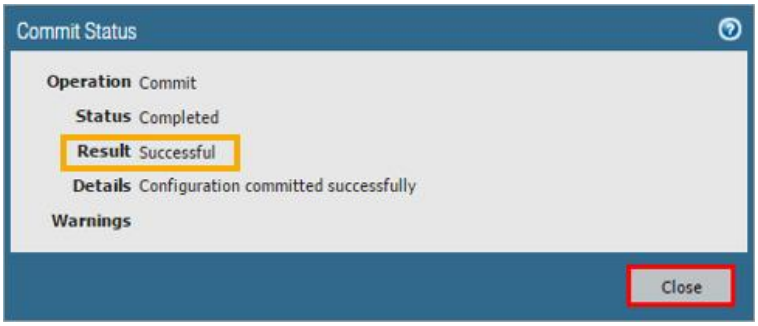
The following instructions are the steps to execute a **"Commit All"** as you will perform many times throughout these labs.

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

11. Click **Commit** and wait until the commit process is complete.



12. Once completed successfully, click **Close** to continue.

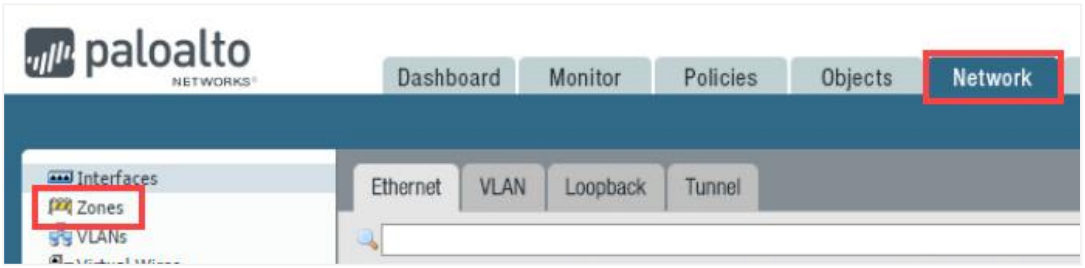


13. Leave the firewall web interface open to continue with the next task.

1.1 Create New Security Zones

Security zones are a logical way to group physical and virtual interfaces on the firewall in order to control and log the traffic that traverses your network through the firewall. An interface on the firewall must be assigned to a security zone before the interface can process traffic. A zone can have multiple interfaces of the same type (for example, Tap, Layer 2, or Layer 3 interfaces) assigned to it, but an interface can belong to only one zone.

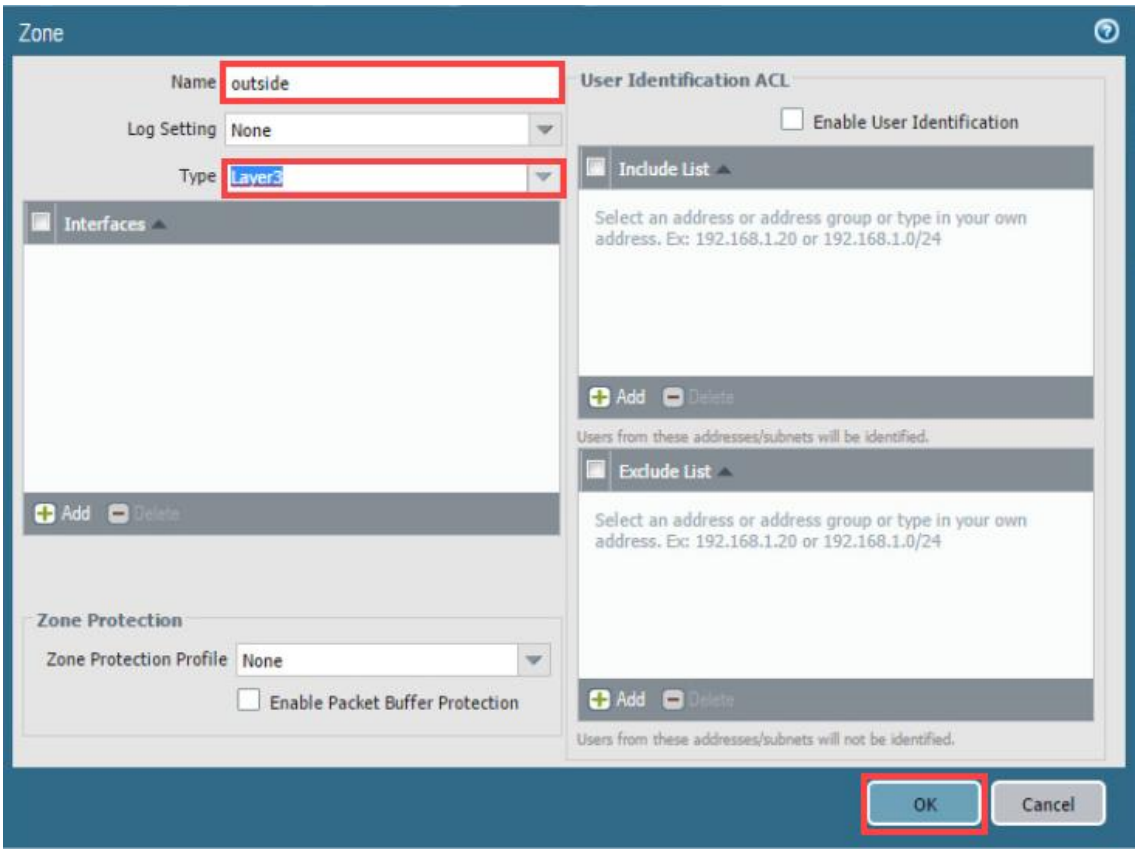
1. In the web interface, select **Network > Zones**.



2. Click **Add** to create a new zone.

3. The *Zone* configuration window opens. Configure the following:

Parameter	Value
Name	**outside**
Type	**Layer3**

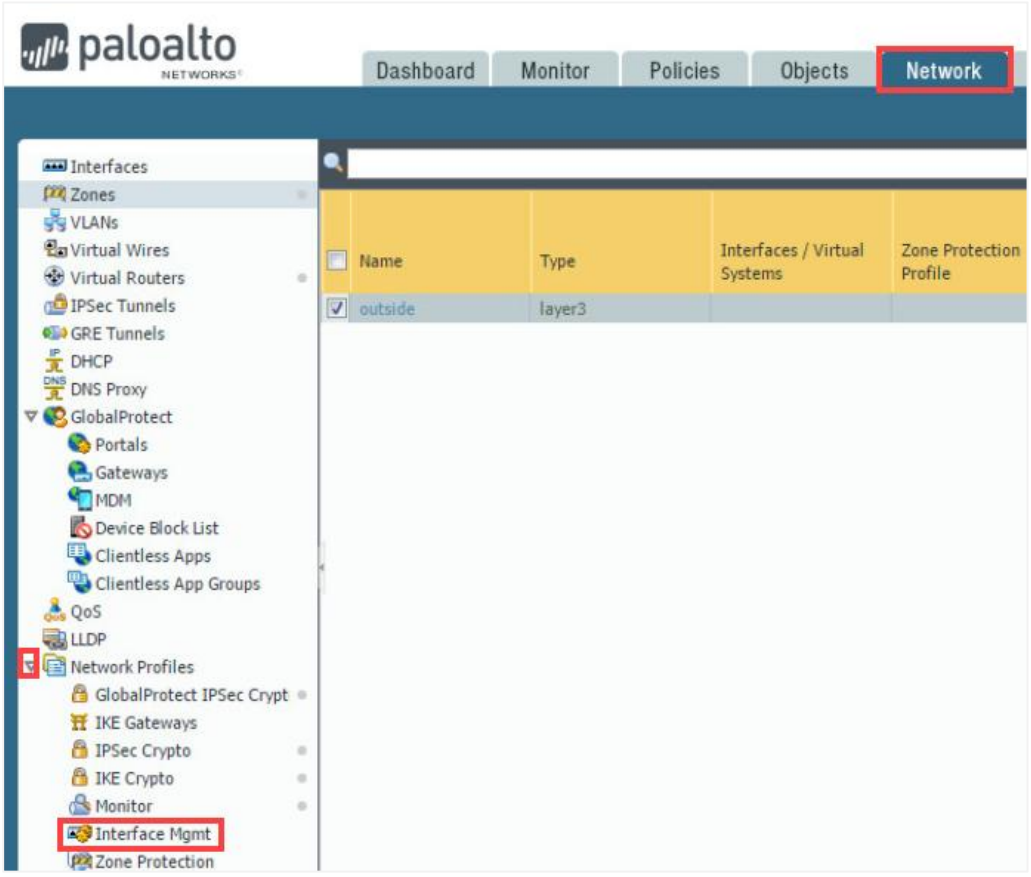


4. Click **OK** to close the *Zone* configuration window. The outside zone is the only zone created in this task. You will add an Ethernet interface to this zone in a later lab step.
5. Leave the firewall web interface open to continue with the next task.

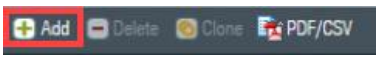
1.2 Create Interface Management Profiles

An *Interface Management Profile* protects the firewall from unauthorized access by defining the services and IP addresses that a firewall interface permits. You can assign an *Interface Management Profile* to Layer 3 Ethernet interfaces (including subinterfaces) and to logical interfaces (Aggregate, VLAN, Loopback, and Tunnel interfaces).

1. In the web interface, select **Network**, expand **Network Profiles,** and then select **Interface Mgmt**.

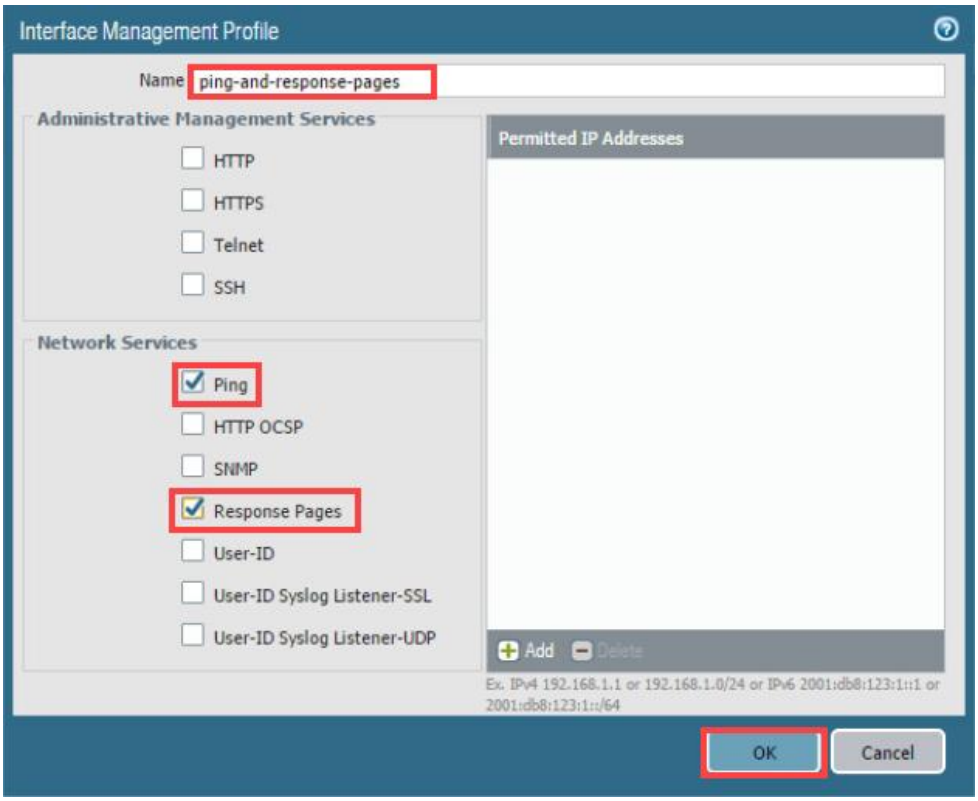


2. Click **Add** to open the *Interface Management Profile* configuration window.



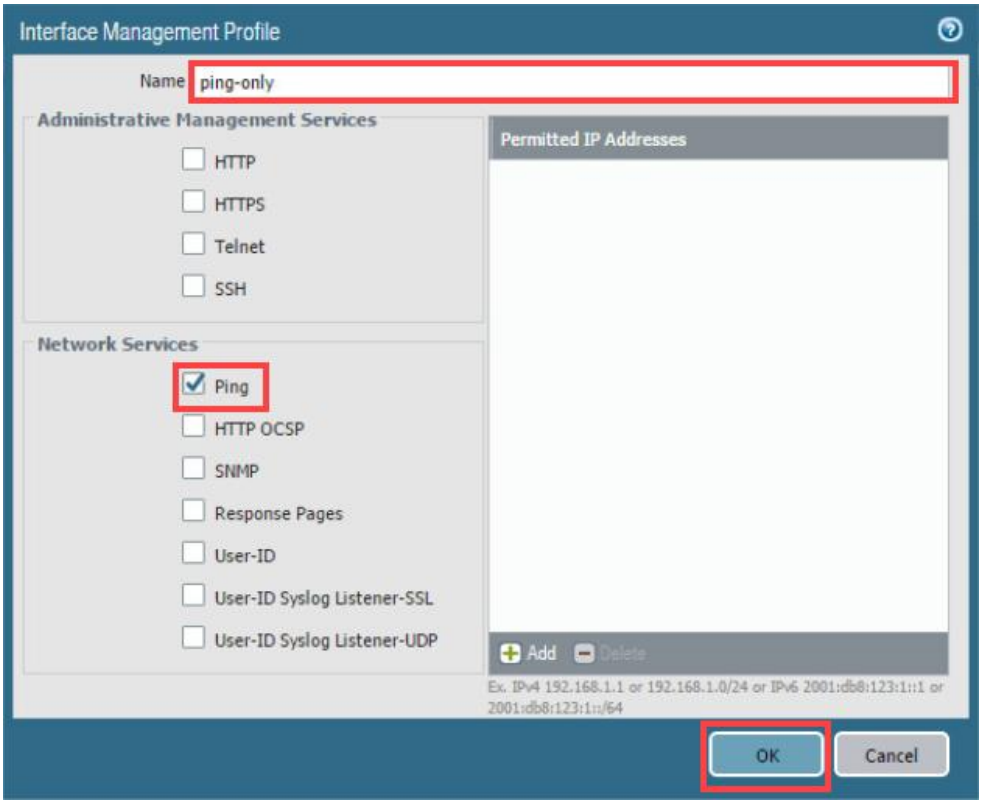
3. In the *Interface Management Profile* configuration window, configure the following and then click **OK**.

Parameter	Value
Name	**`ping-and-response-pages`**
Permitted Services	
Ping	**Checked**
Response Pages	**Checked**



4. Notice a new *Interface Management Profile* appears in the list. Click **Add** to create another *Interface Management Profile*.
5. In the *Interface Management Profile* configuration window, configure the following and then click **OK**.

Parameter	**Value**
Name	**`ping-only`**
Permitted Services	
Ping	**Checked**

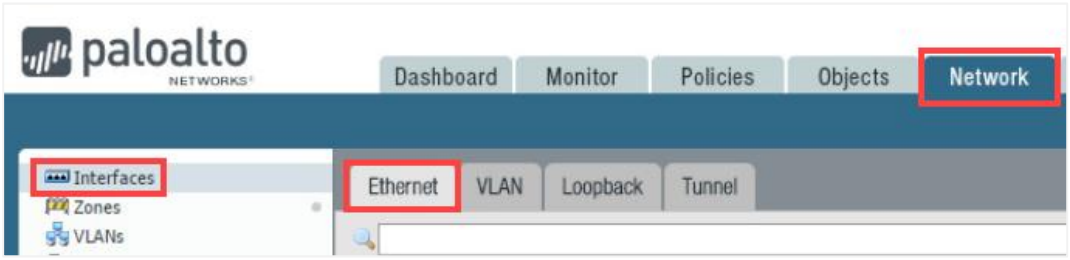


6. Leave the firewall web interface open to continue with the next task.

1.3 Configure Ethernet Interfaces

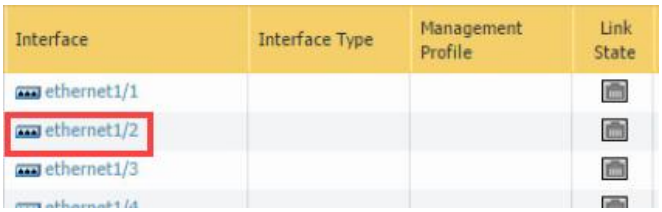
Firewall interfaces, or ports, enable a firewall to connect with other network devices and other interfaces within the firewall. The interface configuration of the firewall ports enables traffic to enter and exit the firewall. You can configure the firewall interfaces for virtual wire, Layer 2, Layer 3, and tap mode deployments.

1. In the web interface, select **Network > Interfaces > Ethernet**.



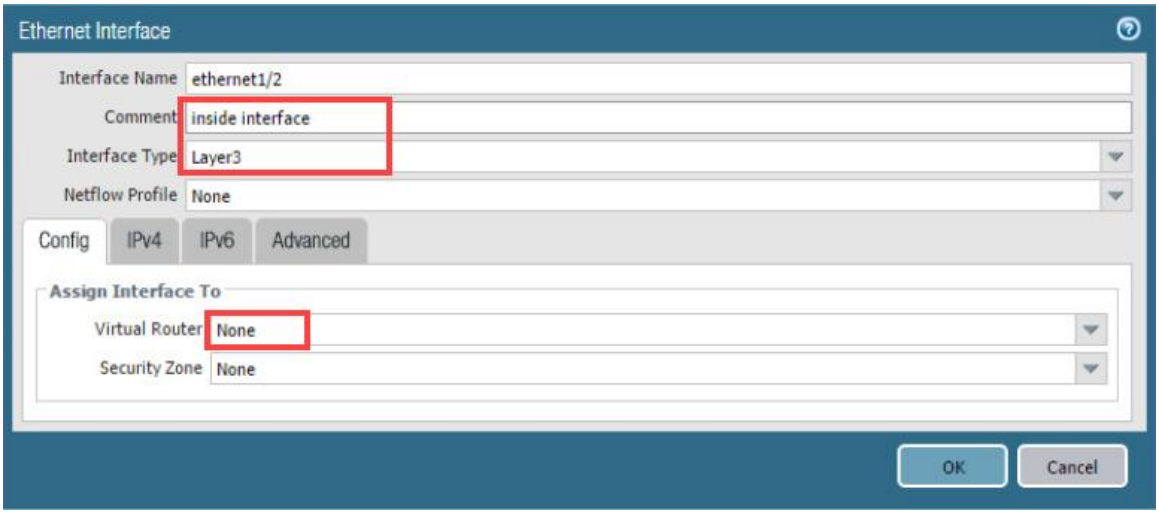
In the next few steps, you will configure *ethernet1/2* as a Layer 3 interface and assign it a static IP address. This interface is logically connected to the Windows client and will operate the client's default gateway (192.168.1.1).

2. Click **ethernet1/2** to configure the interface.



3. Notice the *Ethernet Interface* window appears. Configure the following:

Parameter	Value
Comment	**`inside interface`**
Interface Type	**Layer3**
Virtual Router	**None**

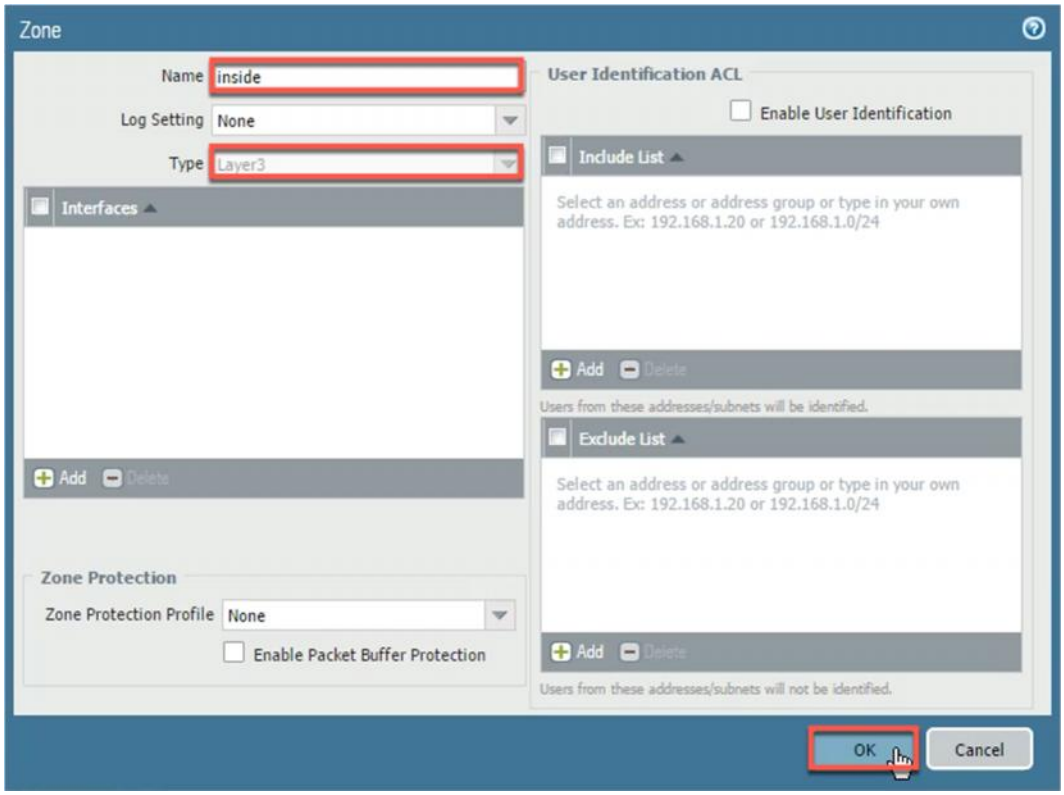


4. Click the **Security Zone** drop-down list and select **New Zone**.

5. The *Zone* configuration window opens. Configure the following:

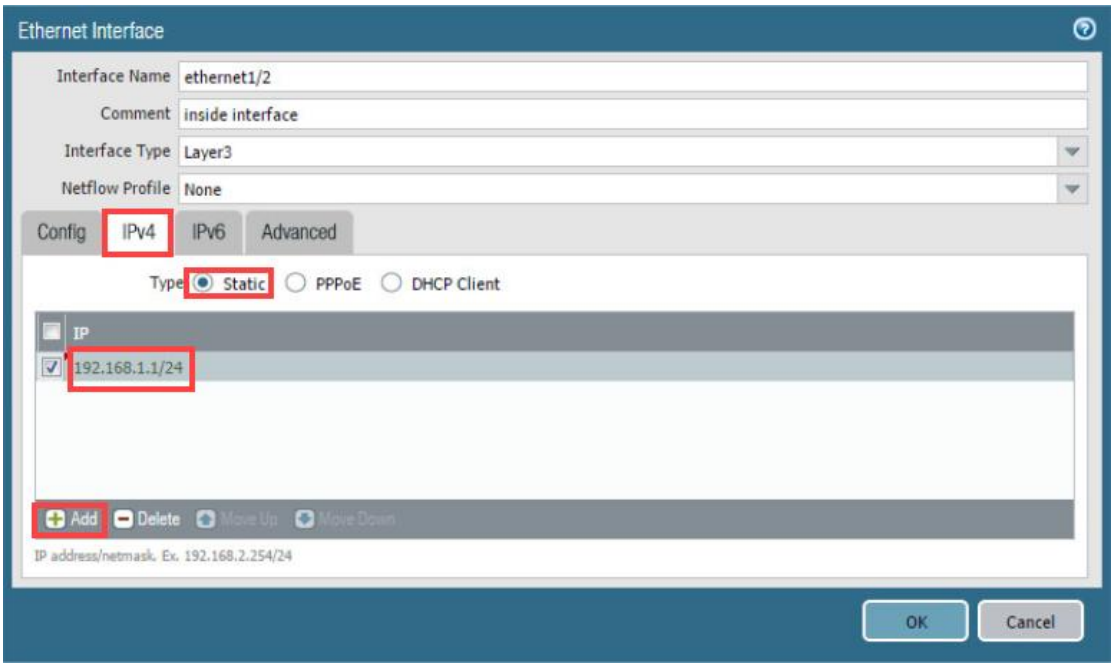
Parameter	Value
Name	**`inside`**
Type	**Layer3** should be selected

6. Click **OK** to close the *Zone* configuration window.

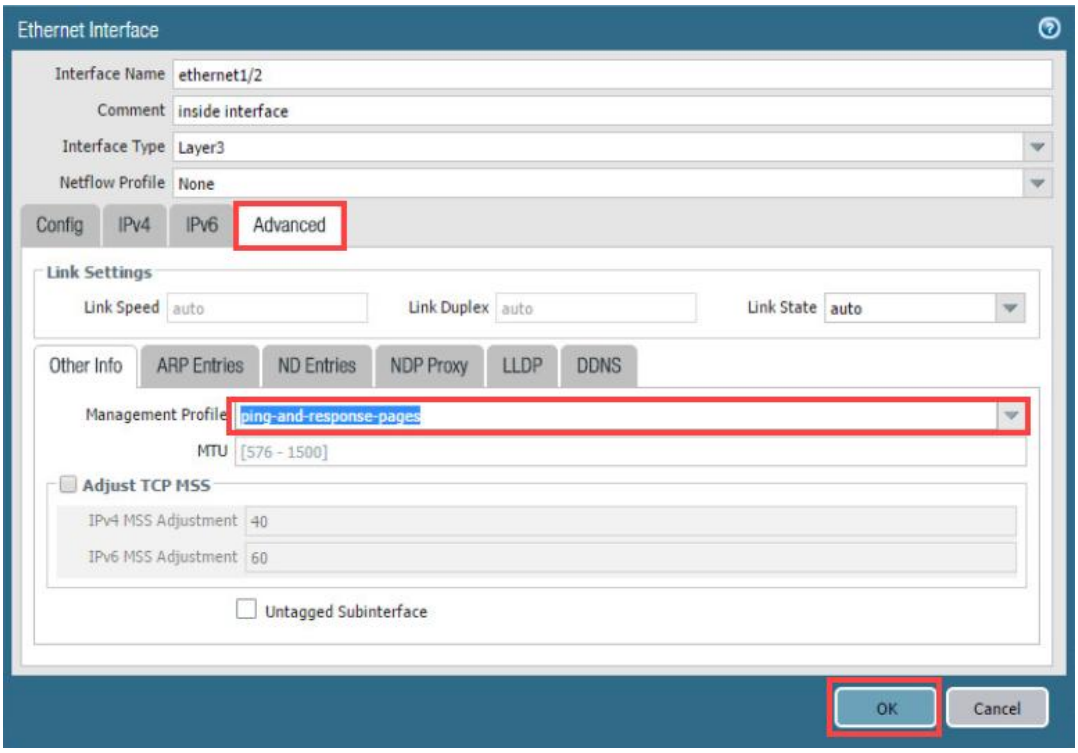


7. Click the *Ethernet Interface* **IPv4** tab and configure the following:

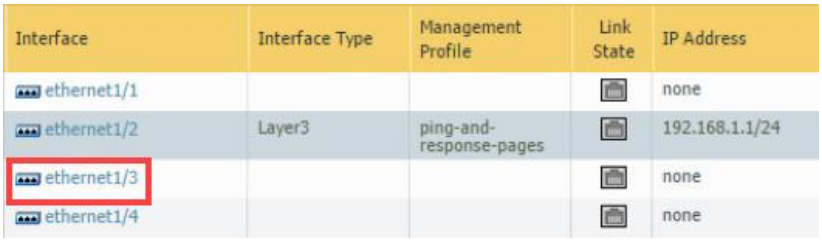
Parameter	Value
Type	**Static**
IP	Click **Add** and type **`192.168.1.1/24`**



8. Click the **Advanced** tab. Click the **Management Profile** drop-down list and select **ping-and-response-pages**. Click **OK** to close the *Ethernet Interface* configuration window.



9. Click **ethernet1/3** to configure the interface.



10. In the *Ethernet Interface* window, configure the following:

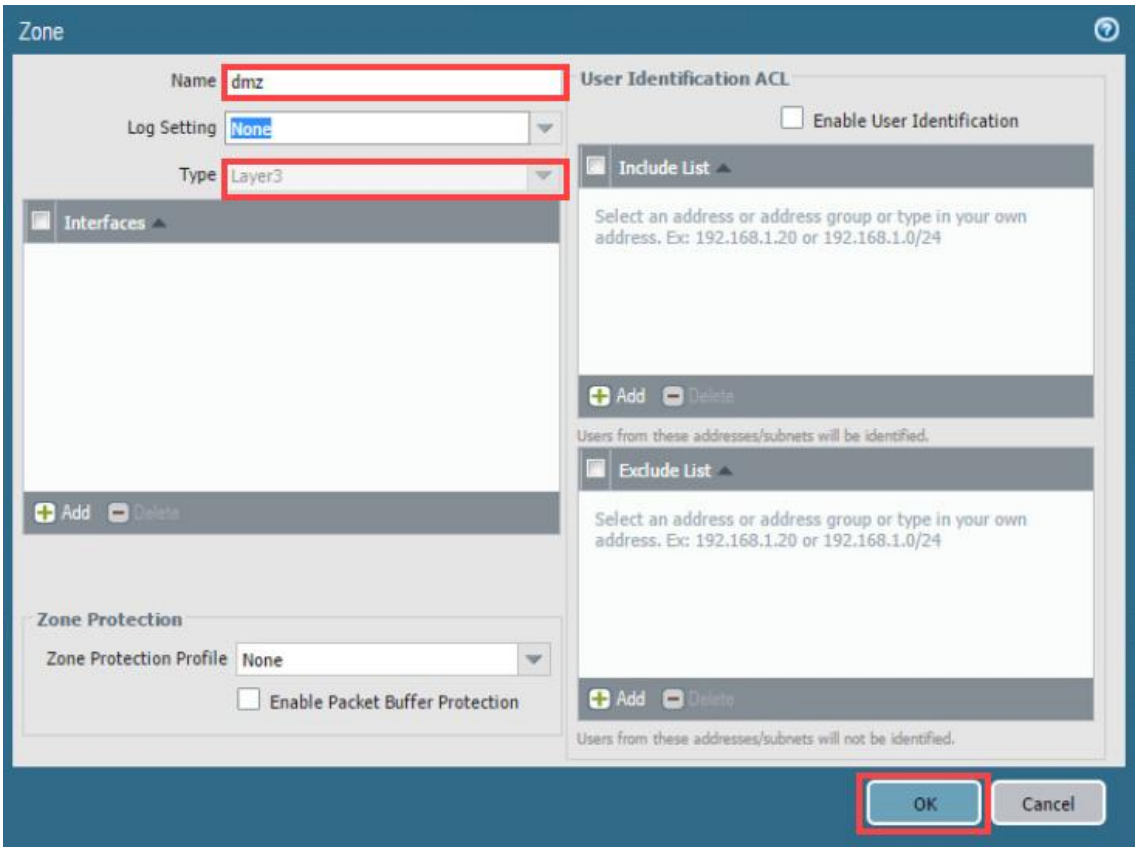
Parameter	Value
Comment	**`dmz interface`**
Interface Type	**Layer3**
Virtual Router	**None**

11. Click the **Security Zone** drop-down list and select **New Zone**.

12. The *Zone* configuration window opens. Configure the following:

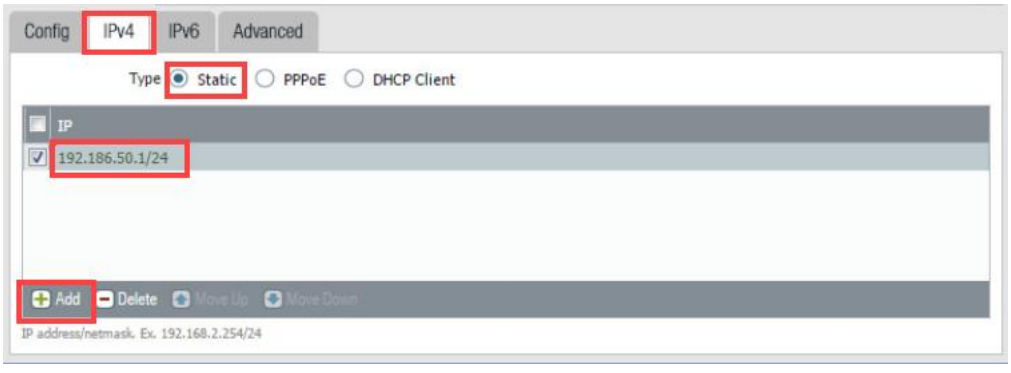
Parameter	Value
Name	**dmz**
Type	**Layer3** should be selected

13. Click **OK** to close the *Zone* configuration window.

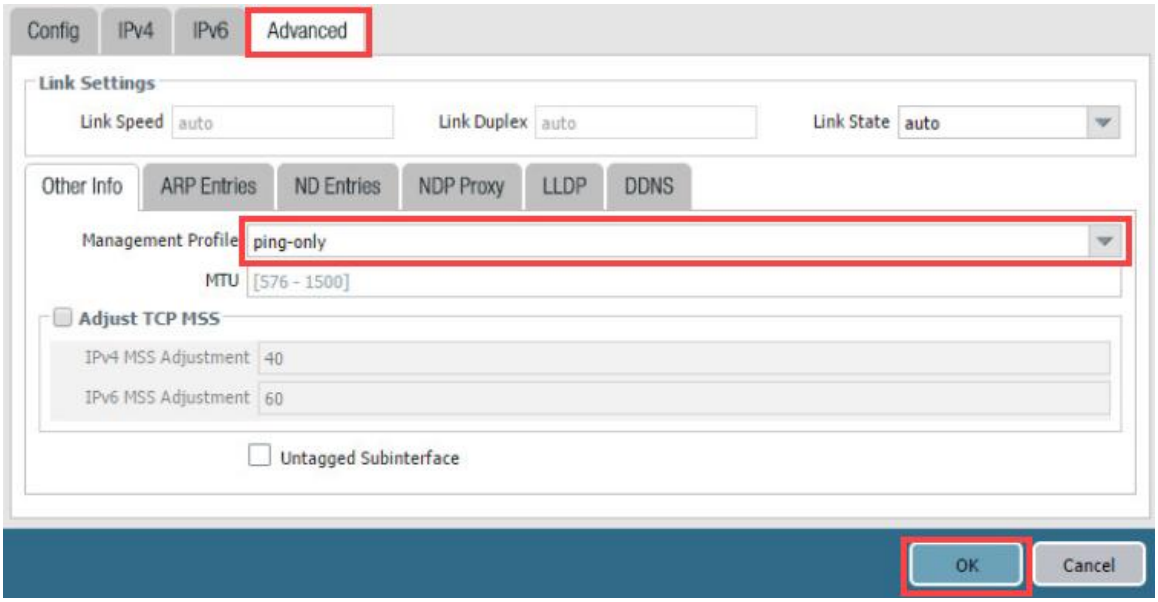


14. Click the **IPv4** tab and configure the following:

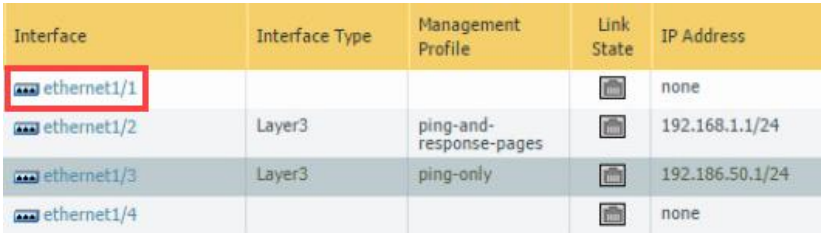
Parameter	Value
Type	**Static**
IP	Click **Add** and type **`192.186.50.1/24`**



15. Click the **Advanced** tab. Click the **Management Profile** drop-down list and select **ping-only**. Click **OK** to close the *Ethernet Interface* configuration window.

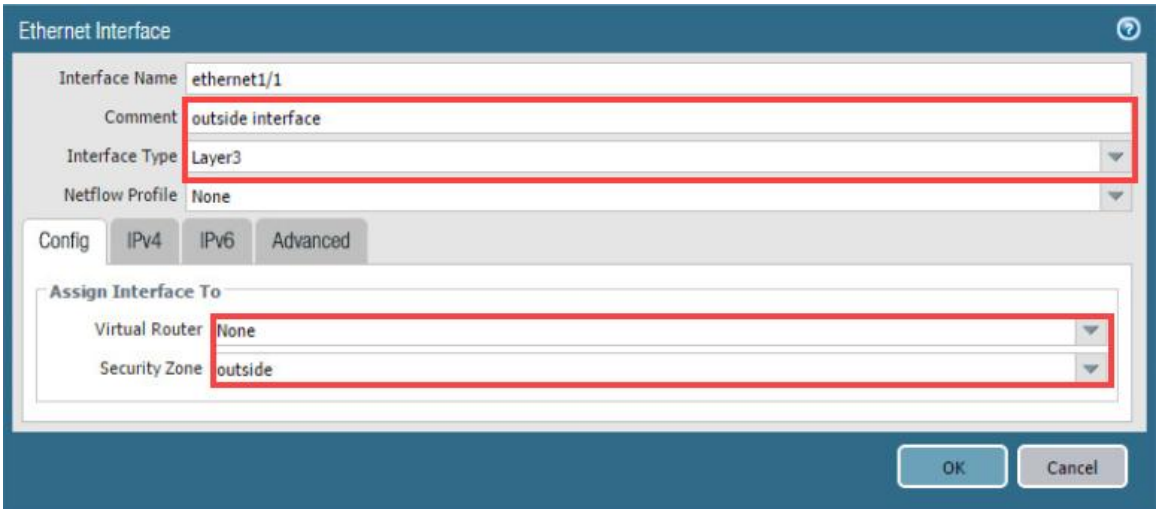


16. Click **ethernet1/1** to configure the interface.



17. In the *Ethernet Interface* window, configure the following:

Parameter	Value
Comment	**`outside interface`**
Interface Type	**Layer3**
Virtual Router	**None**
Security Zone	**outside**

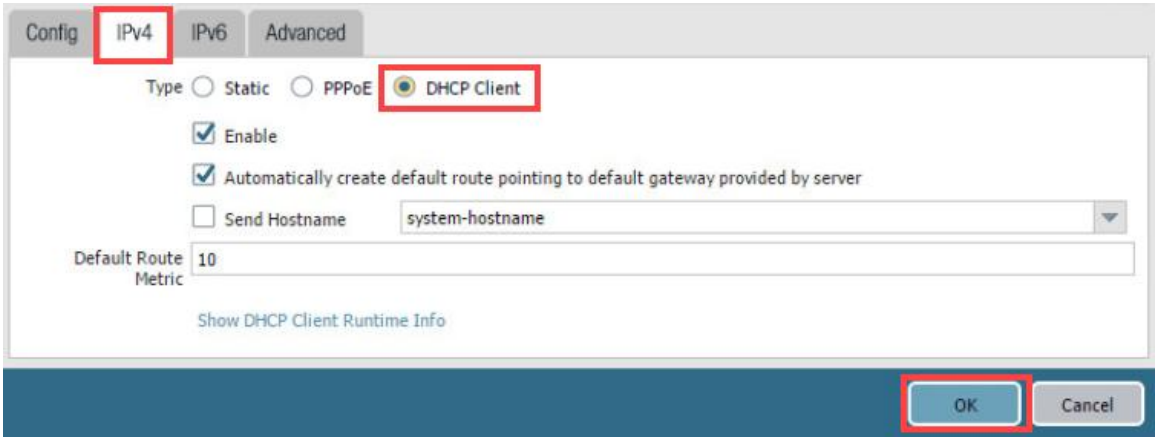


18. Click the **IPv4** tab and configure the following and then click **OK** to close the *Ethernet Interface* configuration window.

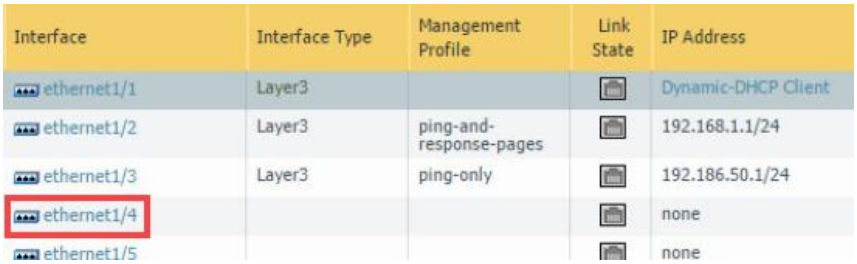
Parameter	Value
Type	**DHCP Client**

Note the following option:

This option will automatically install a default route based on DHCP-option 3.

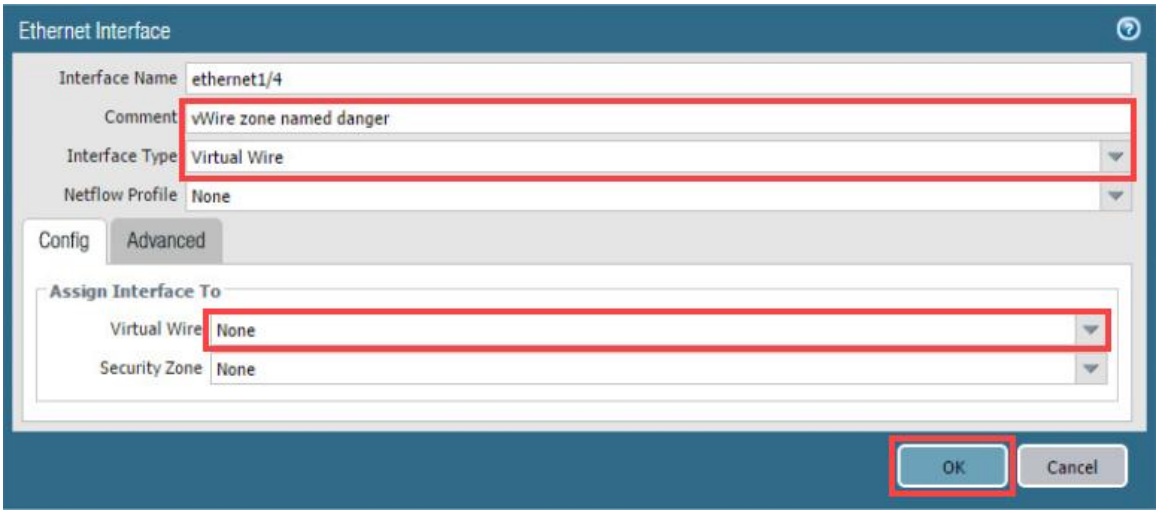


19. Click **ethernet1/4** to configure the interface.



20. In the *Ethernet Interface* window, configure the following:

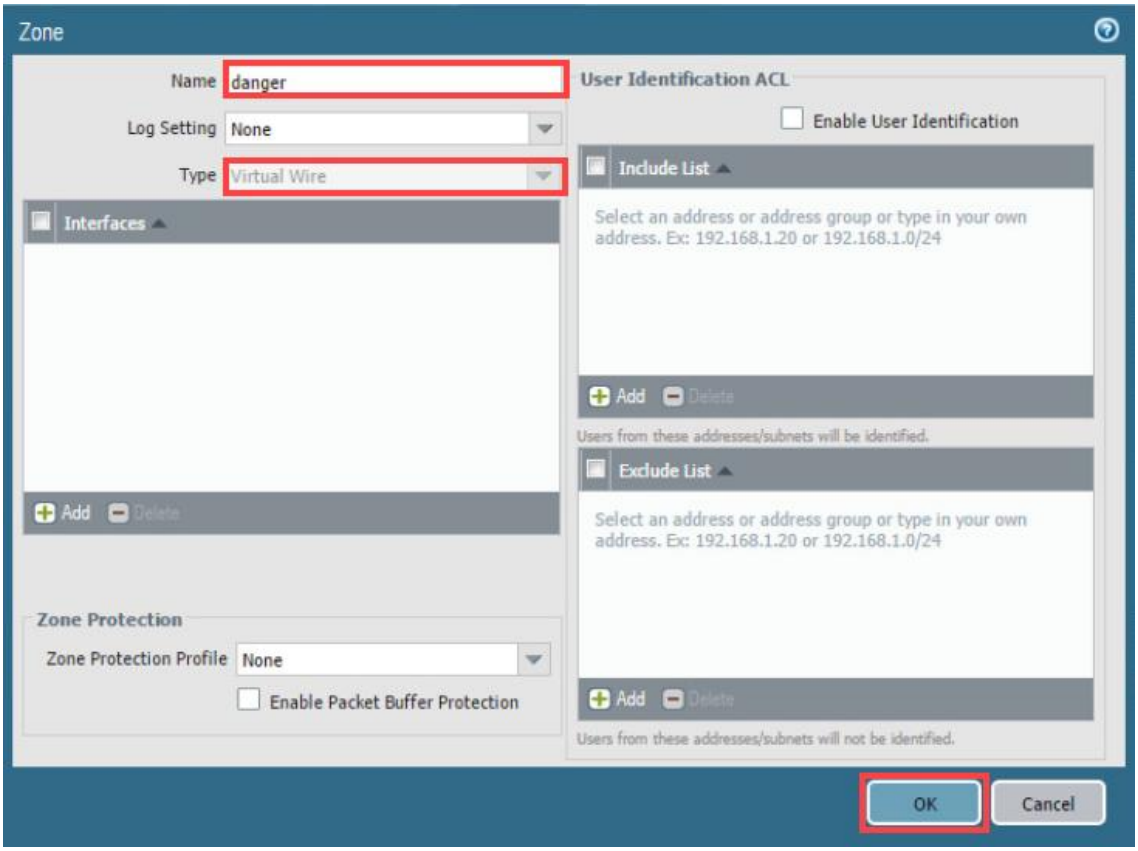
Parameter	Value
Comment	**`vWire zone named danger`**
Interface Type	**Virtual Wire**
Virtual Wire	**None**



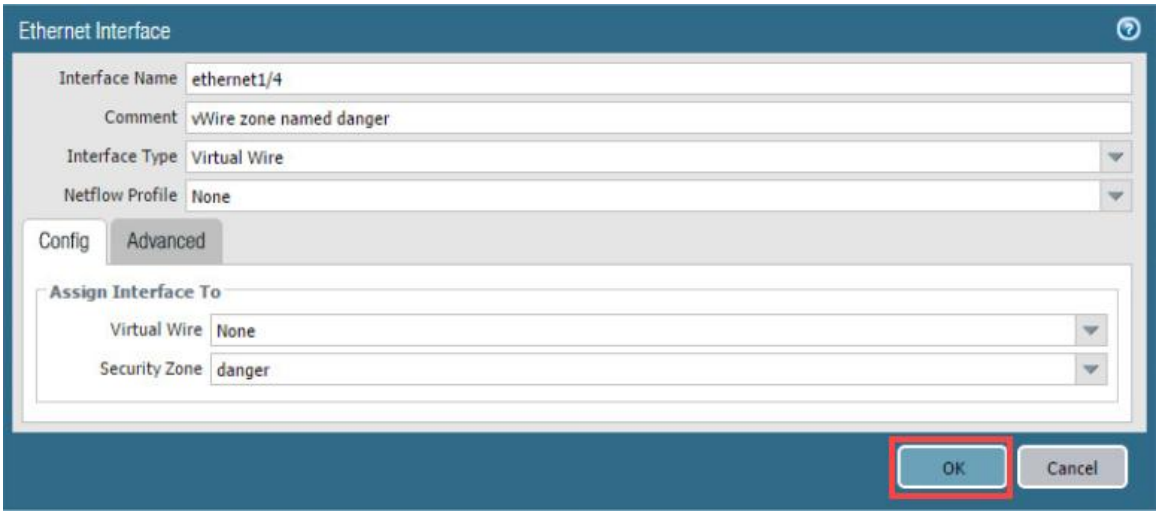
21. Click the **Security Zone** drop-down list and select **New Zone**.

22. The *Zone* configuration window opens. Configure the following, followed by clicking **OK**.

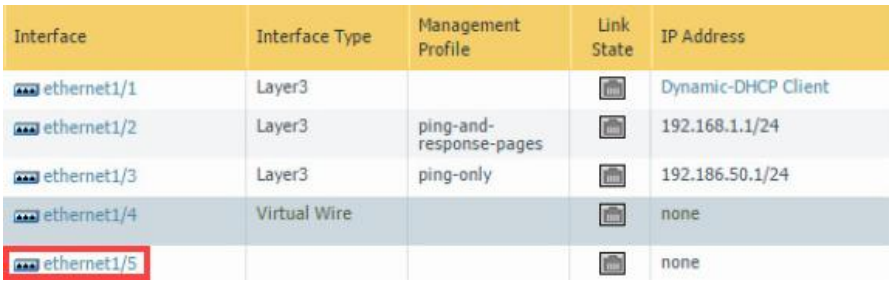
Parameter	Value
Name	**danger**
Type	**Virtual Wire** should be selected



23. Back on the *Ethernet Interface* configuration window, click **OK**.



24. Click **ethernet1/5** to configure the interface.



25. In the *Ethernet Interface* window, configure the following and then click **OK**.

Parameter	Value
Comment	**`vWire zone named danger`**
Interface Type	**Virtual Wire**
Virtual Wire	**None**
Security Zone	**danger**

26. Leave the firewall web interface open to continue with the next task.

1.4 Create a Virtual Wire

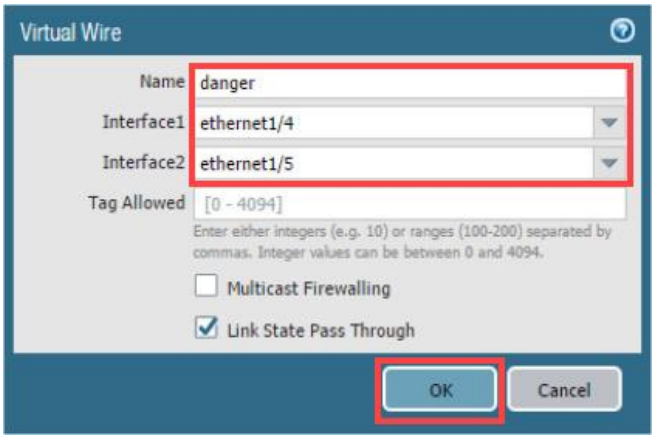
A virtual wire interface binds two Ethernet ports together. A virtual wire interface allows all traffic or just selected VLAN traffic to pass between the ports. No other switching or routing services are available.

1. In the web interface, select **Network > Virtual Wires**.

2. Click **Add** located near the bottom of the screen.

3. In the *Virtual Wire* window, configure the following and then click **OK**.

Parameter	Value
Name	**danger**
Interface 1	**ethernet1/4**
Interface 2	**ethernet1/5**



4. Leave the firewall web interface open to continue with the next task.

1.5 Create a Virtual Router

The firewall requires a virtual router to obtain routes to other subnets, either using static routes that you manually define or through participation in Layer 3 routing protocols that provide dynamic routes. The firewall has a predefined virtual router named default.

A virtual router is a separate routing instance that allows the firewall to route traffic from one network to another through its Layer 3 interfaces. In this environment, we have three networks - 192.168.1.0/24, 192.168.50.0/24, and 203.0.113.0/24. You will modify the default virtual router and add the firewall's interfaces from each of these networks to the virtual router.

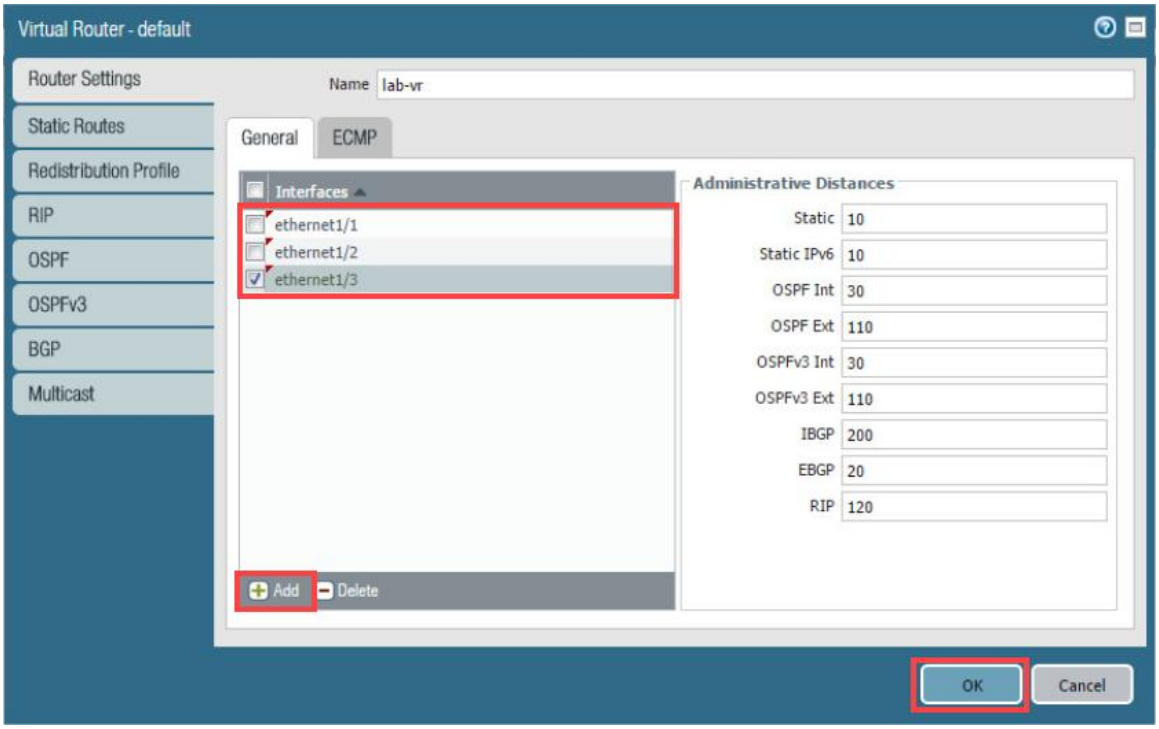
Because we are using Layer 3 interfaces, the firewall must have a way to route traffic from one network to another; this process is done with a virtual router. However, because each interface is in a different security zone, the Security rules will prevent traffic in one network from going to another network through the firewall.

1. In the web interface, select **Network > Virtual Routers**.

2. Click **default** to open the default virtual router.

3. In the *Virtual Router - default* window, rename the default router to **`lab-vr`**.

4. Click **Add** to add the following interfaces: **ethernet1/1**, **ethernet1/2**, and **ethernet1/3**. Click **OK**.



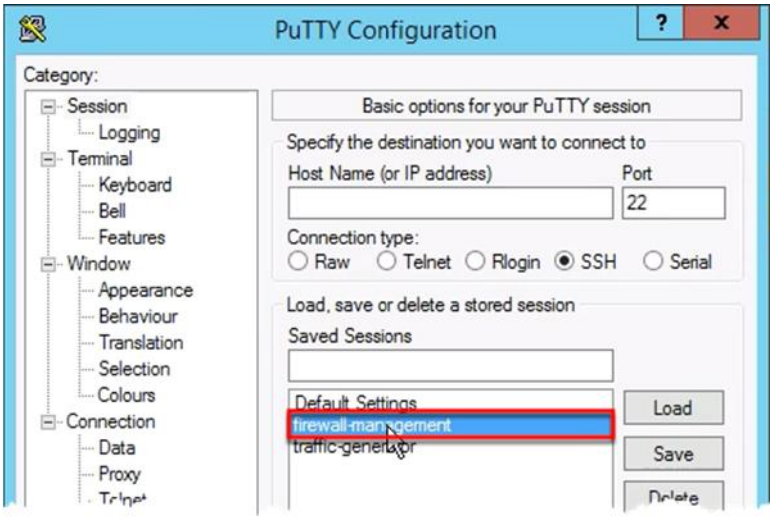
This step can also be completed via each **Ethernet Interface** configuration window.

5. **Commit** all changes.
6. Leave the firewall web interface open to continue with the next task.

1.6 Test Connectivity

1. Double-click on the **PuTTY** icon from the Windows desktop.

2. Double-click **firewall-management**:

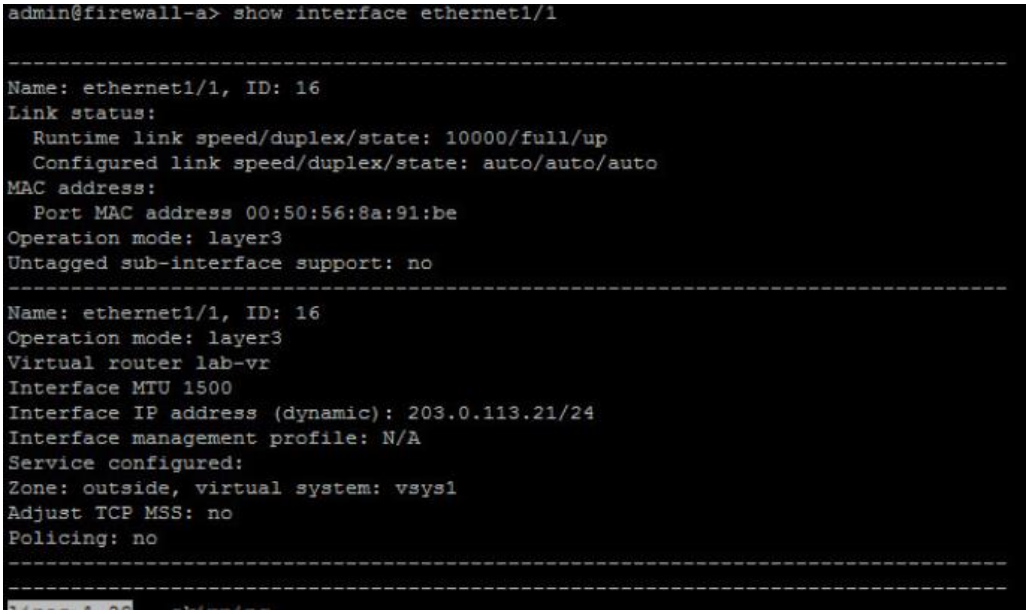


3. Log in using the following information:

Parameter	Value
Name	**admin**
Password	**admin**

4. In the CLI, type the command below, followed by pressing the **Enter** key.

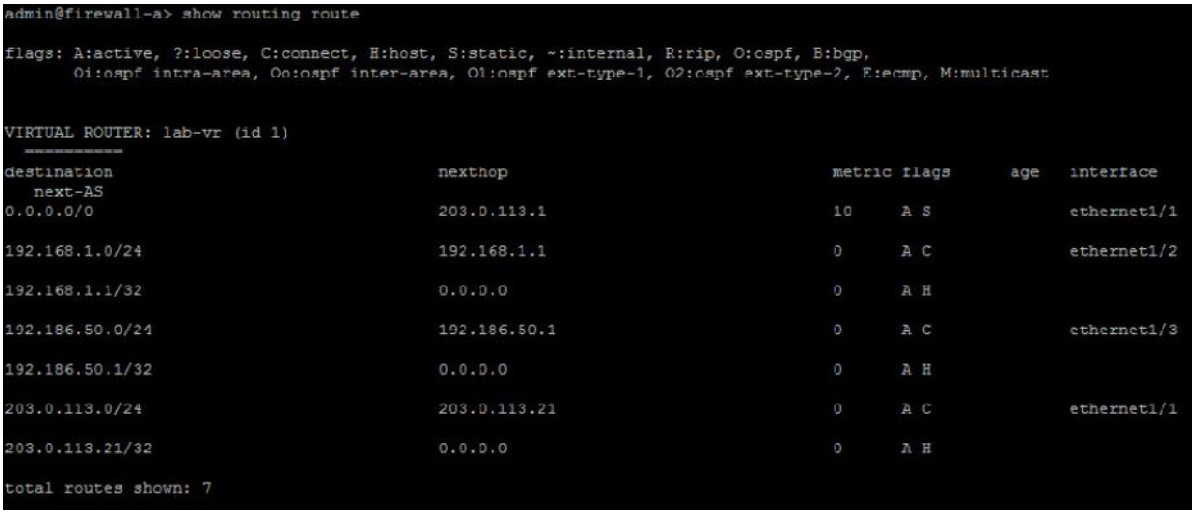
```
admin@firewall-a> show interface ethernet1/1
```



From the command output, you should be able to see the IP address obtained by DHCP. It should be *203.0.113.21/24*. Use the **Enter** key to scroll through the command output.

5. From the CLI, enter the command below.

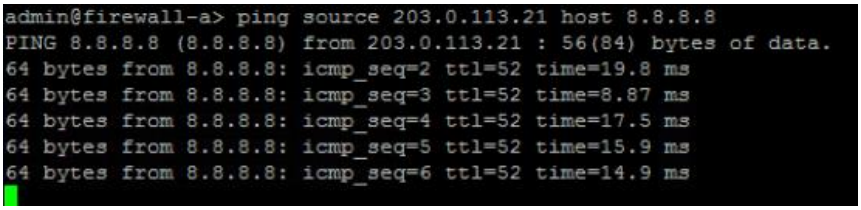
```
admin@firewall-a> show routing route
```



The command output should show you the firewall's default route that was installed as part of the DHCP lease.

6. From the CLI, enter the command below.

```
admin@firewall-a> ping source 203.0.113.21 host 8.8.8.8
```

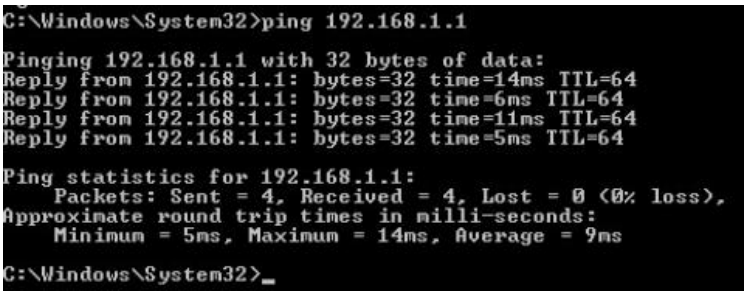


The host you are pinging from is the firewall itself. The ping command is used to verify the firewall's connectivity to the internet.

7. After a few successful pings, press **CTRL+C** to stop the ping.
8. On the lab environment Windows desktop, double-click **CMD** open a command-prompt window.

9. In the command prompt, enter the command below.

```
C:\Windows\System32> ping 192.168.1.1
```



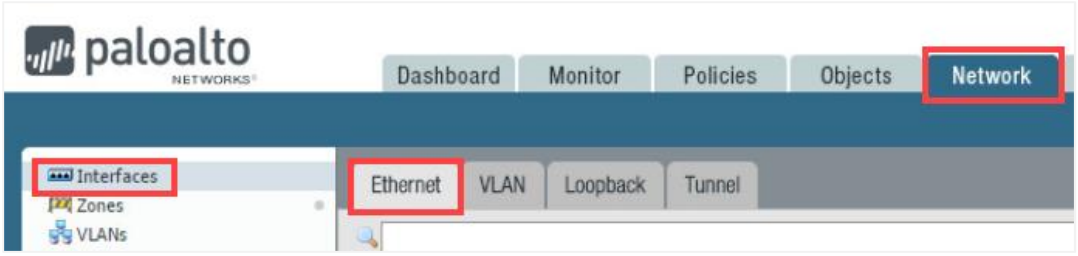
In this step, you are pinging from the Windows host to its default gateway, which is ethernet1/2 on the firewall. Verify that you get a reply before proceeding.

10. Type **`exit`** followed by pressing the **Enter** key in the command-prompt window to close it.

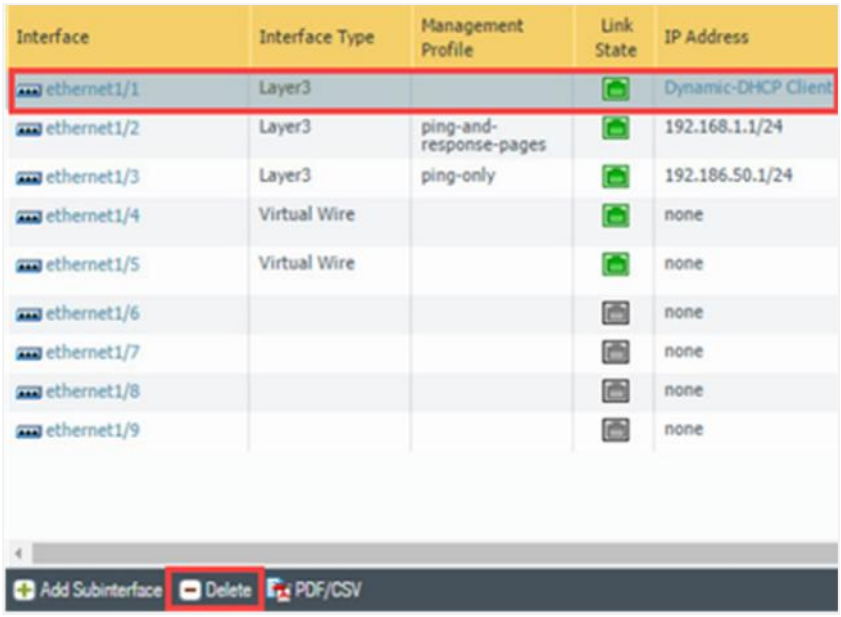
1.7 Modify Outside Interface Configuration

In this task, you will reconfigure Ethernet Interface 1/1 to use a static IP address and add a static route to your virtual router. Under most conditions, you will configure the firewall's Layer 3 interfaces with static IP addresses. We initially configured ethernet1/1 to use the DHCP client function only to illustrate the feature should you ever need it.

1. Change focus to the firewall web interface and select **Network > Interfaces > Ethernet**.



2. Select but do not open **ethernet1/1,** followed by clicking **Delete.**

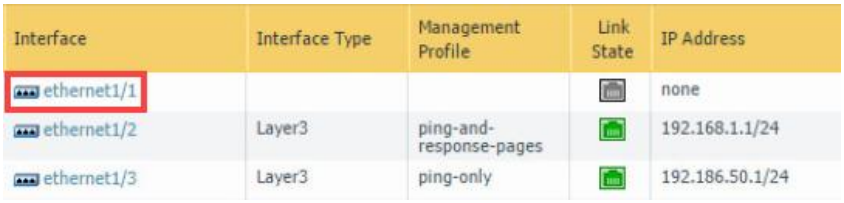


3. When prompted, click **Yes**.

4. **Commit** all changes.

This action will force the interface to release the former DHCP assigned IP address.

5. Click on **ethernet 1/1** to configure the interface.

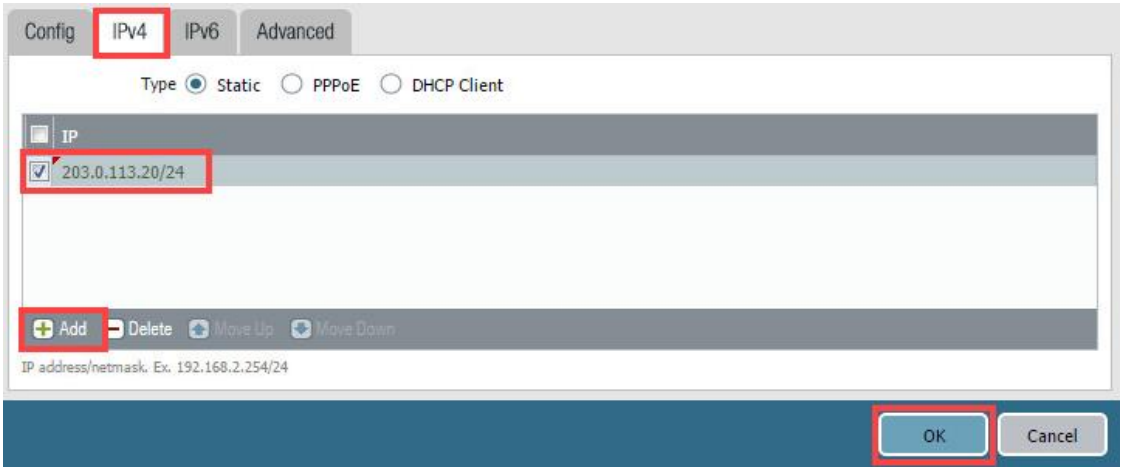


6. In the *Ethernet Interface* window, configure the following:

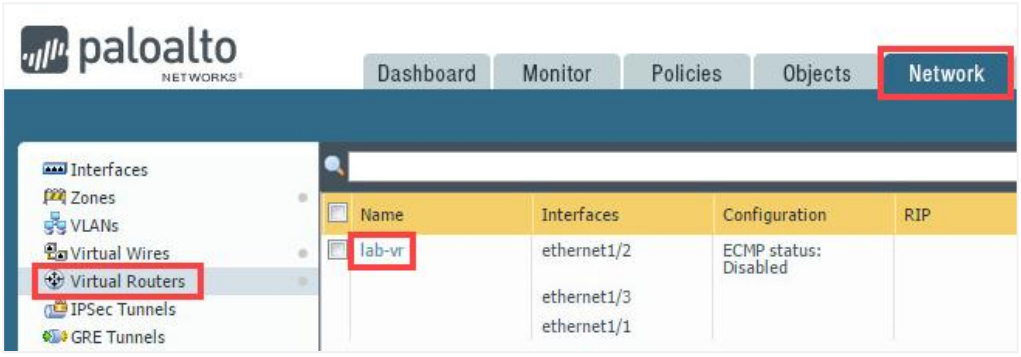
Parameter	Value
Comment	`outside interface`
Interface Type	**Layer3**
Virtual Router	**lab-vr**
Security Zone	**outside**

7. Click the **IPV4** tab and configure the following. Click **OK** when finished.

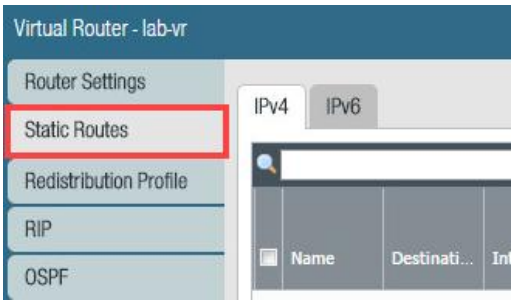
Parameter	Value
Type	**Static**
IP	Click **Add** and type **`203.0.113.20/24`**



8. In the web interface, select **Network > Virtual Routers**. Click on **lab-vr** to open the virtual router.

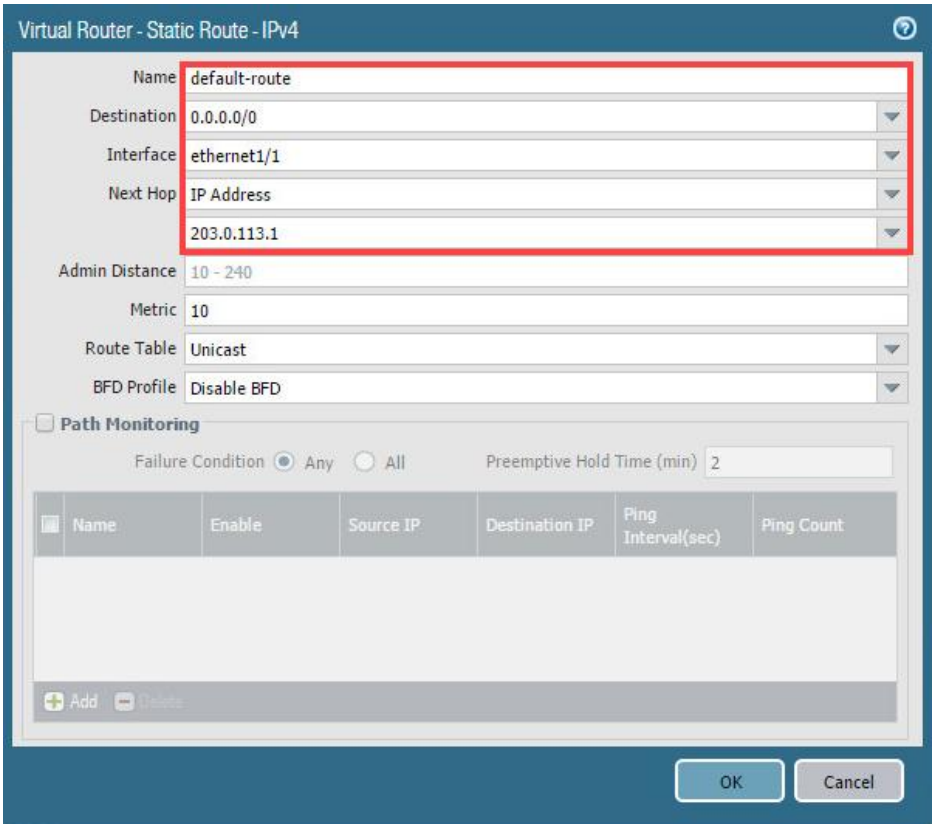


9. In the *Virtual Router - lab-vr* window, click the **Static Routes** vertical tab.



10. Click **Add** to configure the following static route:

Parameter	Value
Name	**default-route**
Destination	**0.0.0.0/0**
Interface	**ethernet1/1**
Next Hop	**IP Address**
Next Hop IP Address	**203.0.113.1**

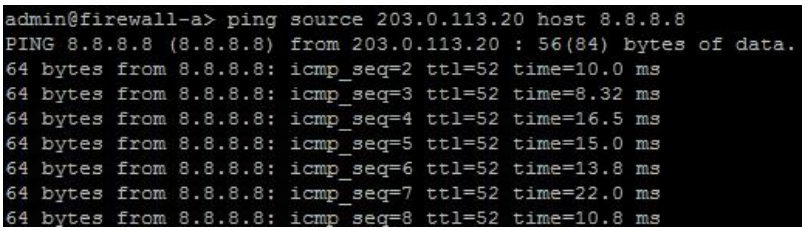


This step is very important. As with any other network host using IP, the firewall itself must have a default gateway. Without this entry, the firewall can send only traffic to networks to which it has interface connections 192.168.1.0/24, 192.168.50.0/24, and 203.0.113.0/24).

11. Click **OK** to add the static route and then click **OK** again to close the *Virtual Router – lab-vr* configuration window.
12. **Commit** all changes.
13. Make the **PuTTY** window that was used to ping 8.8.8.8 the active window.

14. Enter the command below.

```
admin@firewall-a> ping source 203.0.113.20 host 8.8.8.8
```



You should be able to successfully ping 8.8.8.8 from the firewall itself.

15. Close the **PuTTY** window.
16. The lab is now complete; you may end the reservation.

