



PALO ALTO NETWORKS - EDU-210



Lab 2: Interface Configuration

Document Version: 2021-02-17

Copyright © 2021 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
Objectives.....	3
Lab Topology	4
Theoretical Lab Topology.....	4
Lab Settings	5
2 Interface Configuration	6
2.0 Load Lab Configuration	6
2.1 Create New Security Zones	9
2.2 Create Interface Management Profiles.....	10
2.3 Configure Ethernet Interfaces.....	12
2.4 Create a Virtual Wire.....	23
2.5 Create a Virtual Router	24
2.6 Test Connectivity	26
2.7 Modify Outside Interface Configuration	29

Introduction

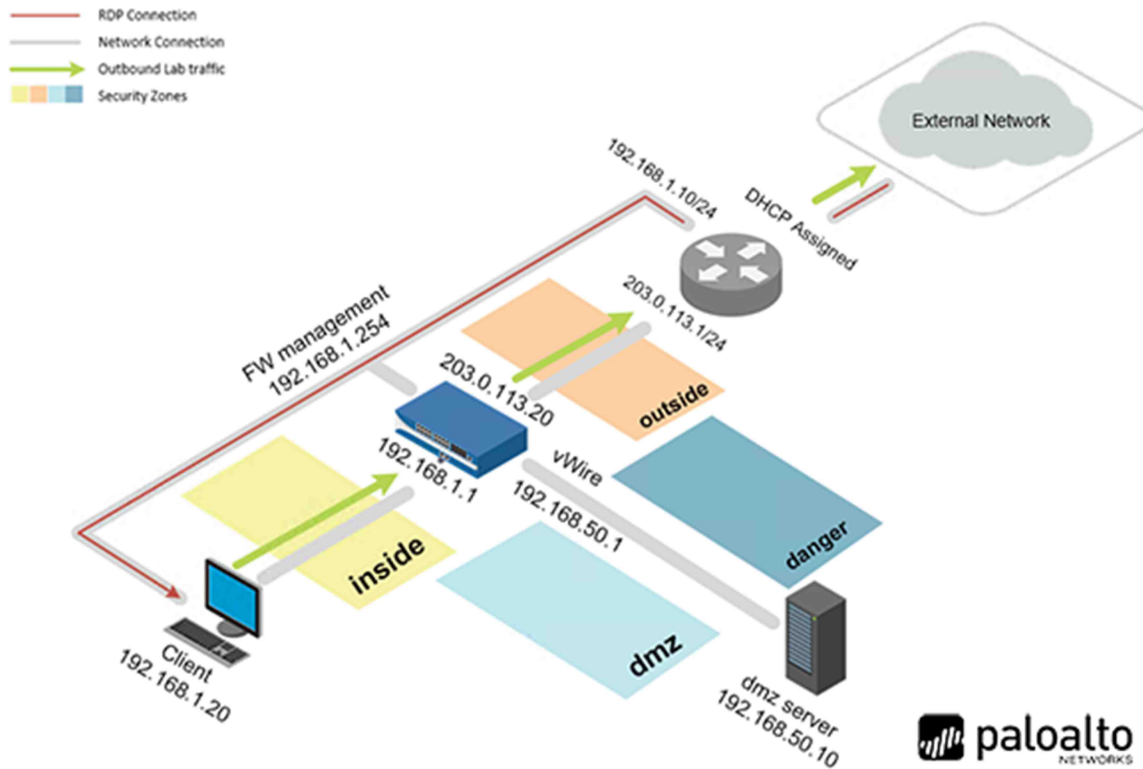
Now that we have set up our admin accounts, verified that we can connect to the admin portal, and set up our system to begin receiving updates, it is now time to start configuring our firewall appliance.

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.

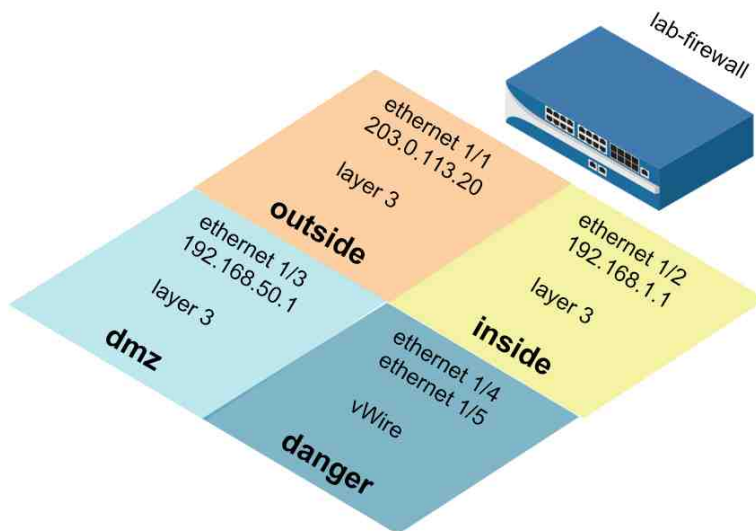
Objectives

-) 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	TrainIng\$
Firewall	192.168.1.254	admin	TrainIng\$

2 Interface Configuration

2.0 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 **Training\$**.



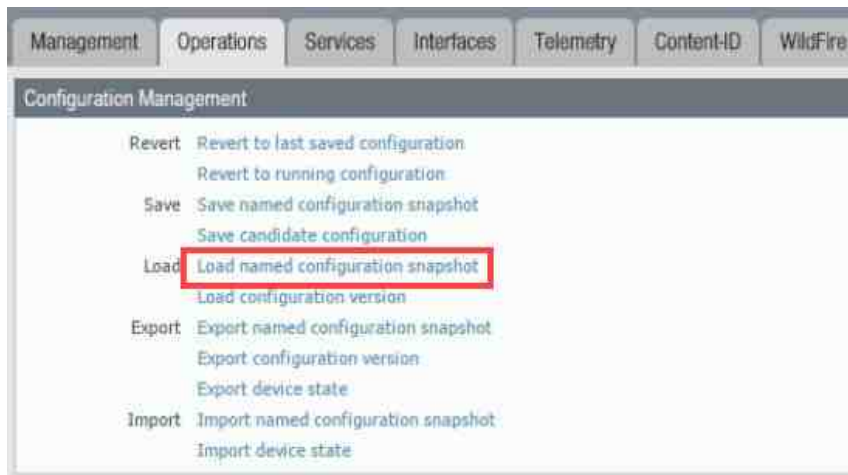
3. Launch the Chromium Web Browser and connect to <https://192.168.1.254>.
4. If a security warning appears, click Advanced and proceed by clicking on Proceed to 192.168.1.254 (unsafe).
5. Log in to the Palo Alto Networks firewall using the following:

Parameter	Value
Name	admin
Password	Training\$

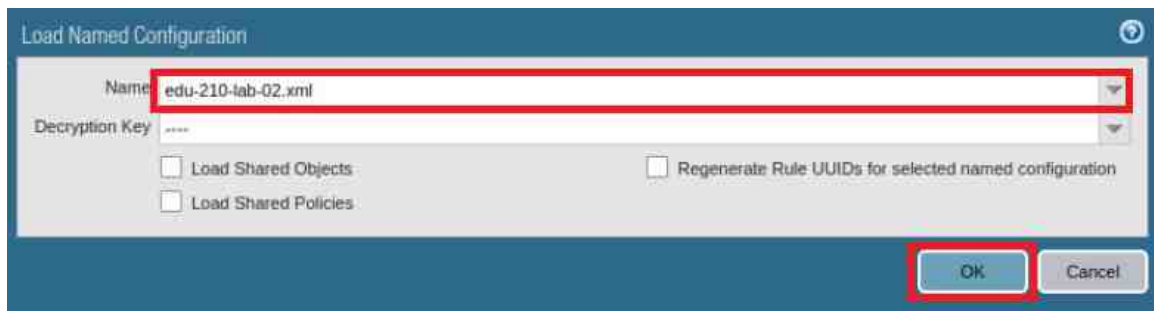
6. In the web interface, select Device > Setup > Operations.



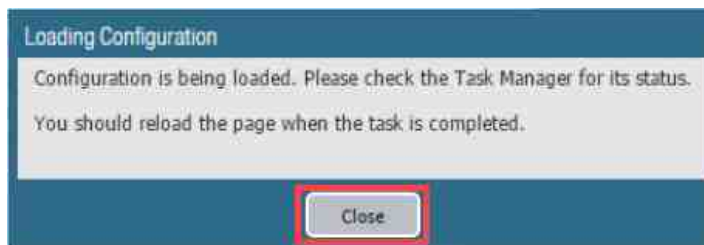
- Click Load named configuration snapshot:



- Click the dropdown list next to the Name text box and select edu-210-lab-02.xml. Click OK.



- Click Close.

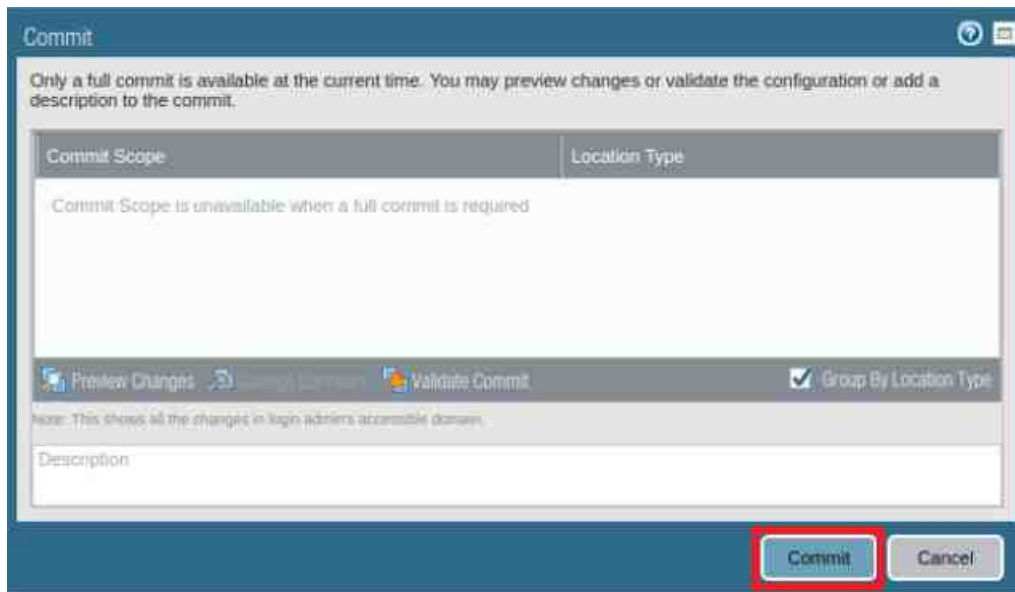


The following instructions are the steps to execute a "Commit All" as you will perform many times throughout these labs.

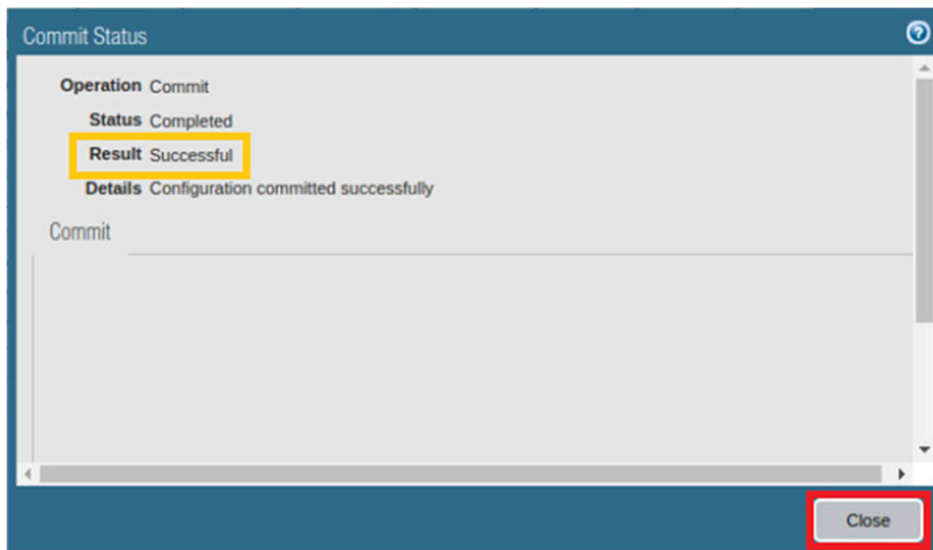
- Click the Commit link at the top-right of the web interface.



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



12. Once completed successfully, click Close to continue.

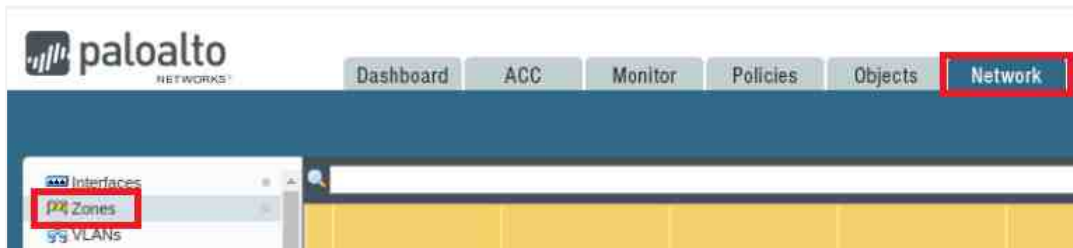


13. Leave the firewall web interface open to continue with the next task.

2.1 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.

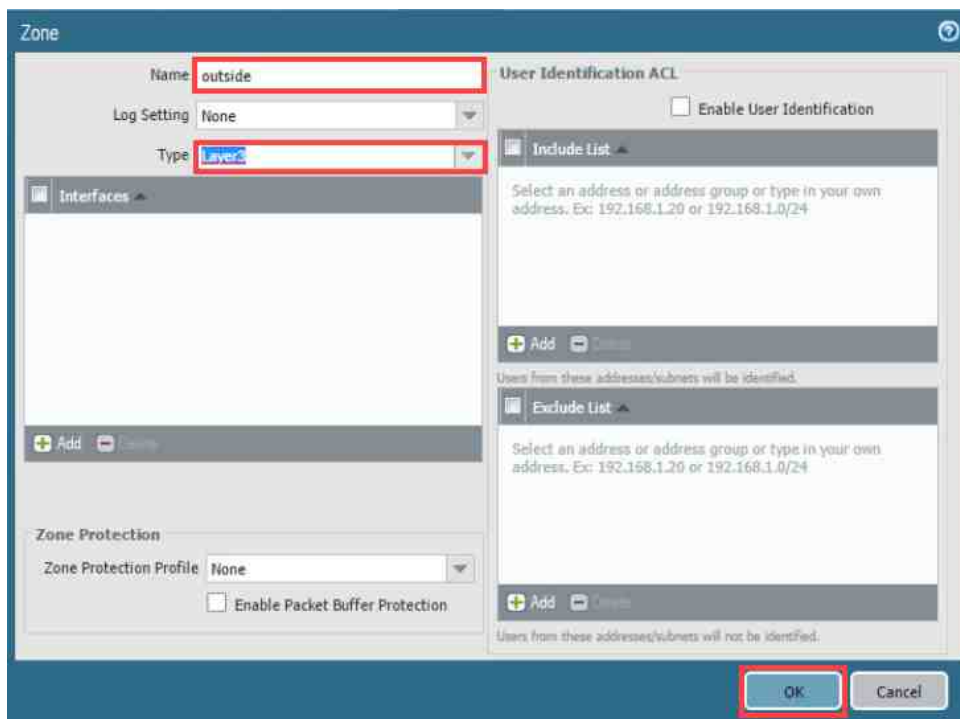


2. Click Add to create a new zone.



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

Parameter	Value
Name	outside
Type	Layer3

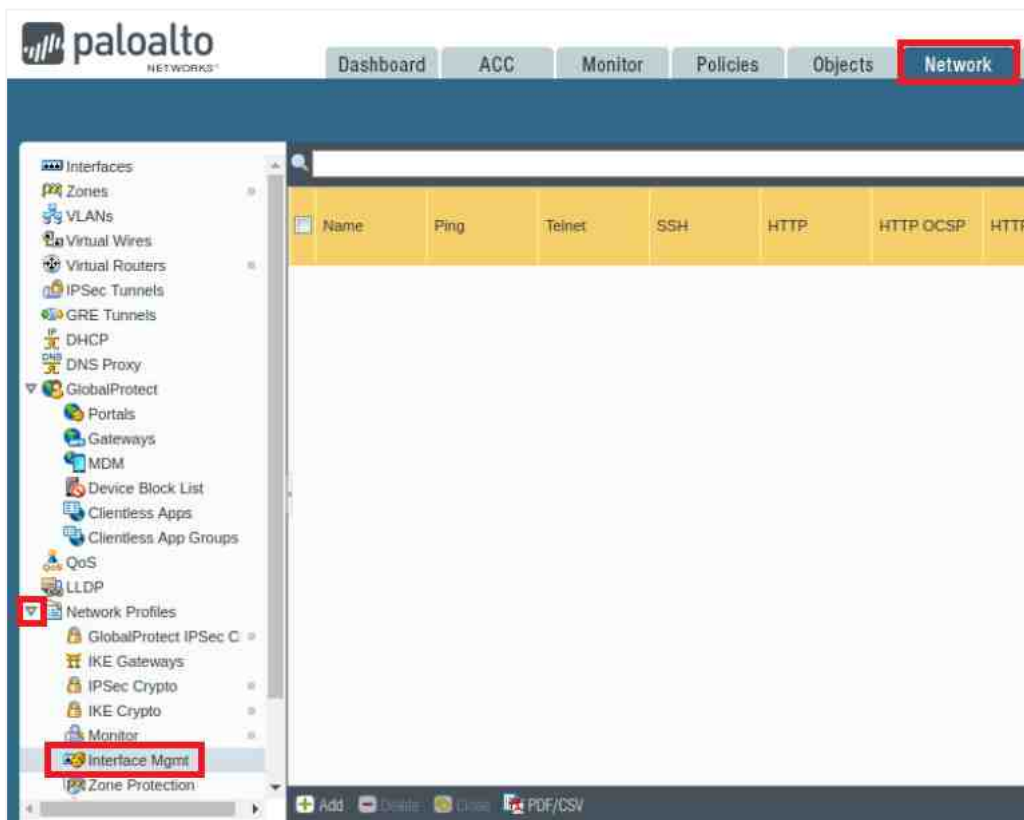


- Click OK to close the Zone configuration window. The outside zone is the only zone created in this task. You will add an Ethernet interface to this zone in a later lab step.
- Leave the firewall web interface open to continue with the next task.

2.2 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).

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

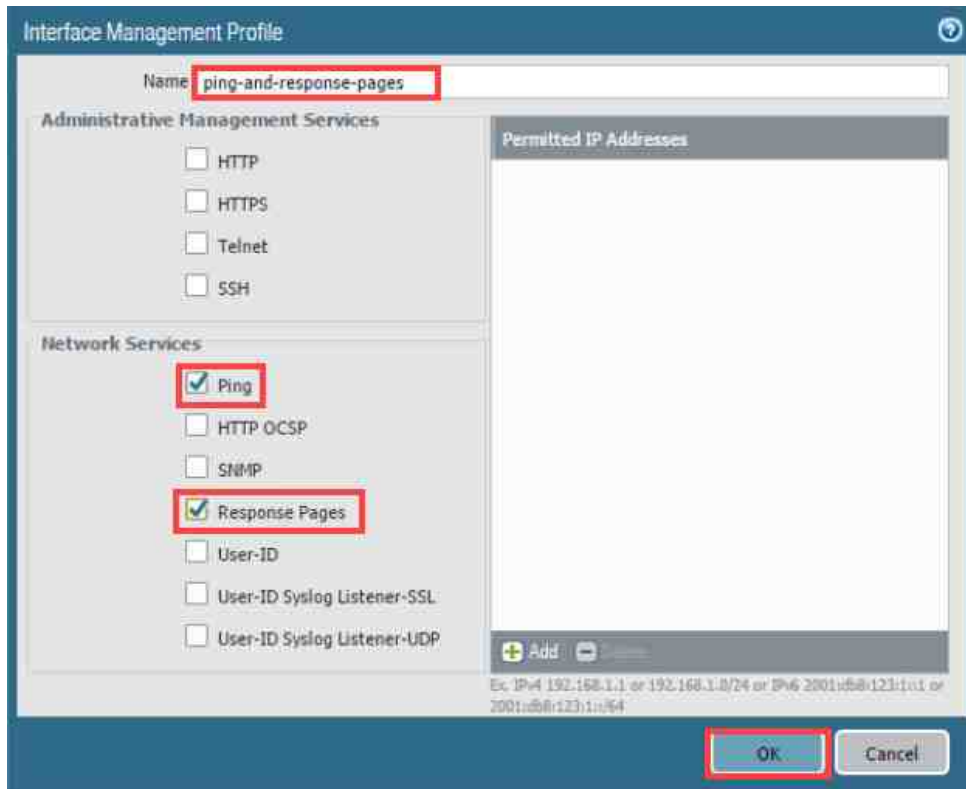


- Click Add to open the Interface Management Profile configuration window.



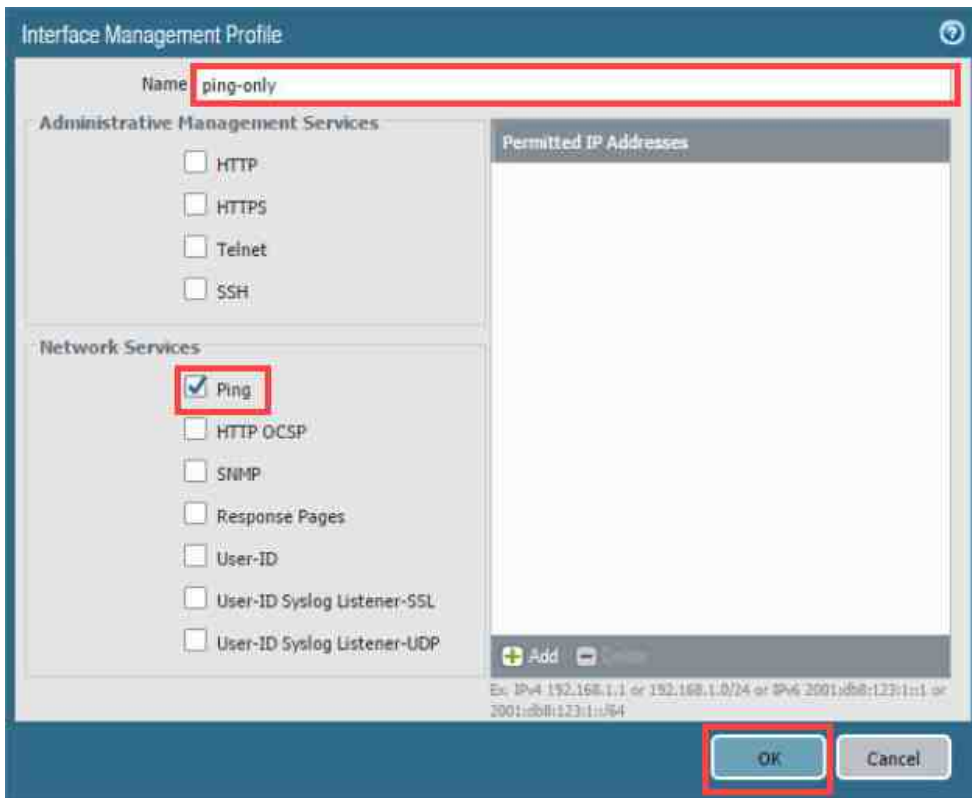
- In the Interface Management Profile configuration window, configure the following and then click OK.

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



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

Parameter	Value
Name	ping-only
Permitted Services	
Ping	Checked



The screenshot shows the 'Interface Management Profile' configuration window. The 'Name' field is set to 'ping-only'. Under 'Administrative Management Services', the checkboxes for HTTP, HTTPS, Telnet, and SSH are all unchecked. Under 'Network Services', the 'Ping' checkbox is checked, while HTTP OCSP, SNMP, Response Pages, User-ID, User-ID Syslog Listener-SSL, and User-ID Syslog Listener-UDP are all unchecked. The 'Permitted IP Addresses' list is empty. At the bottom right, the 'OK' button is highlighted with a red box. A red box also highlights the 'Name' field.

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

2.3 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.



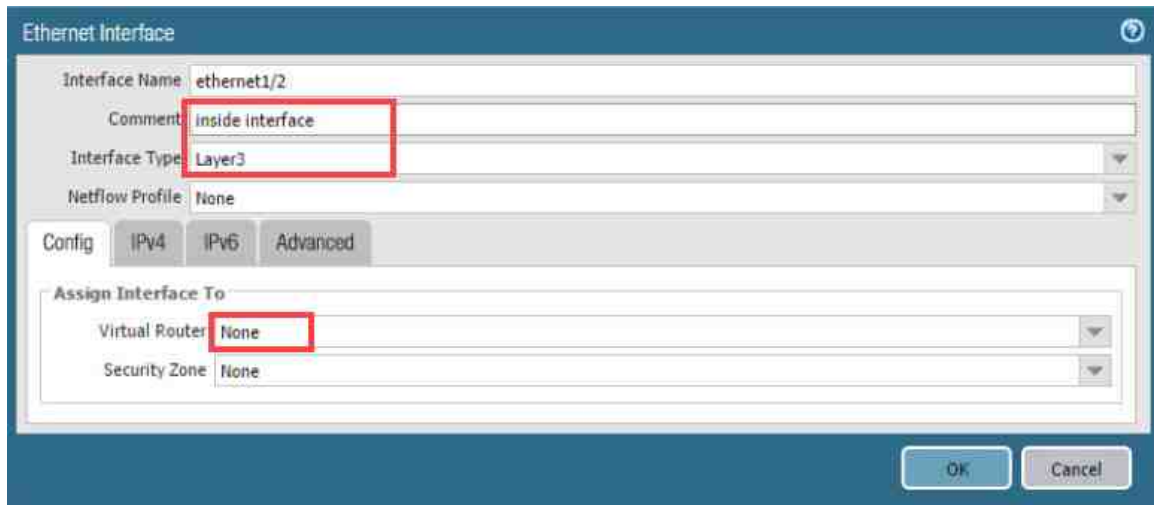
In the next few steps, you will configure ethernet1/2 as a Layer 3 interface and assign it a static IP address. This interface is logically connected to the Windows client and will operate the client's default gateway (192.168.1.1).

- Click ethernet1/2 to configure the interface.

Interface	Interface Type	Management Profile	Link State
ethernet1/1			
ethernet1/2			
ethernet1/3			
ethernet1/4			

- Notice the Ethernet Interface window appears. Configure the following:

Parameter	Value
Comment	i n s i d e i n t e r f a c e
Interface Type	Layer3
Virtual Router	None



The screenshot shows the 'Ethernet Interface' configuration window. The 'Interface Name' is 'ethernet1/2'. The 'Comment' field contains 'inside interface'. The 'Interface Type' is set to 'Layer3'. The 'Netflow Profile' is 'None'. Below these fields are tabs for 'Config', 'IPv4', 'IPv6', and 'Advanced'. Under the 'Config' tab, there is a section 'Assign Interface To' with 'Virtual Router' set to 'None' and 'Security Zone' set to 'None'. At the bottom right are 'OK' and 'Cancel' buttons.

- Click the Security Zone dropdown list and select New Zone.

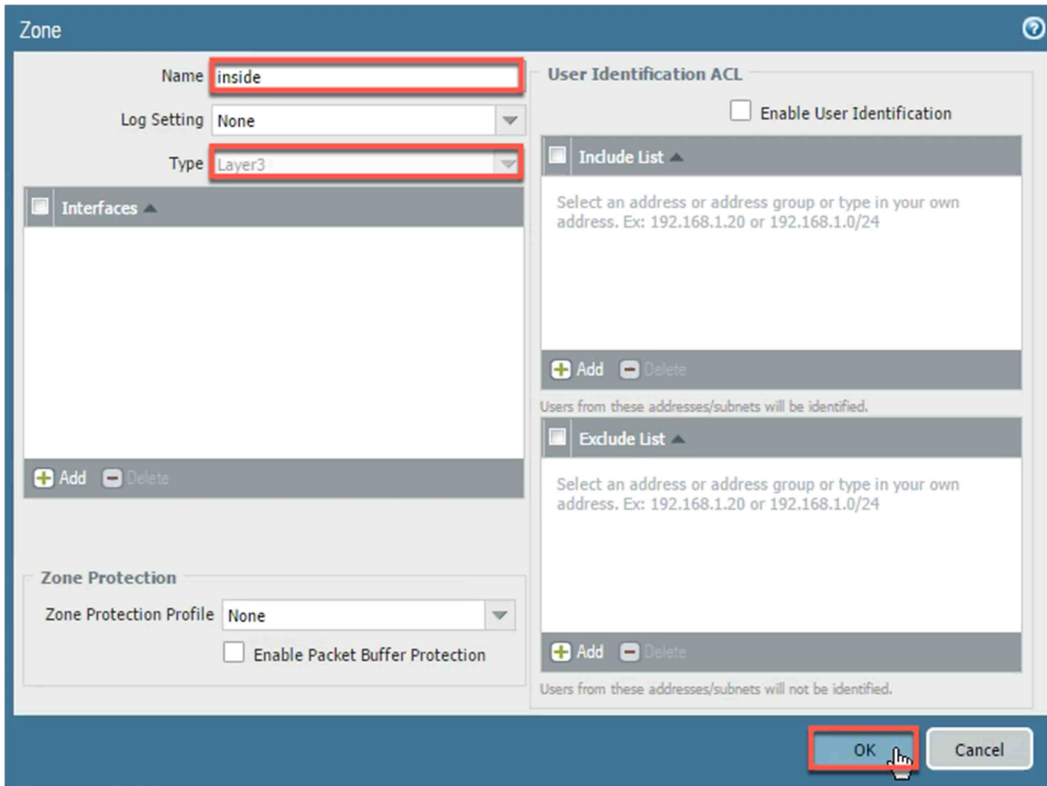


The screenshot shows the 'Assign Interface To' section of the configuration window. The 'Security Zone' dropdown menu is open, showing options: 'None', 'None', 'outside', and 'New Zone'. The 'New Zone' option is highlighted with a red box.

- The Zone configuration window opens. Configure the following:

Parameter	Value
Name	i n s i d e
Type	Layer3 should be selected

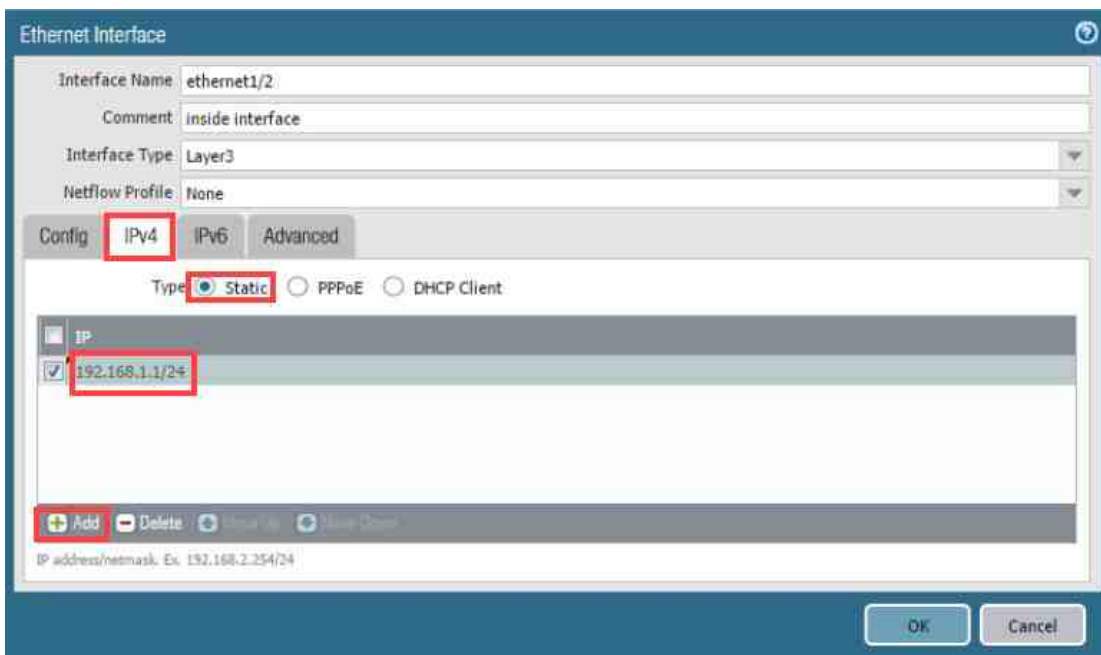
- Click OK to close the Zone configuration window.



The image shows the 'Zone' configuration window. The 'Name' field is set to 'inside'. The 'Log Setting' is 'None'. The 'Type' is 'Layer3'. The 'Zone Protection' section shows 'Zone Protection Profile' set to 'None' and 'Enable Packet Buffer Protection' is unchecked. The 'User Identification ACL' section has 'Enable User Identification' unchecked. There are 'Include List' and 'Exclude List' sections, both with 'Add' and 'Delete' buttons. The 'OK' button is highlighted with a red box and a mouse cursor.

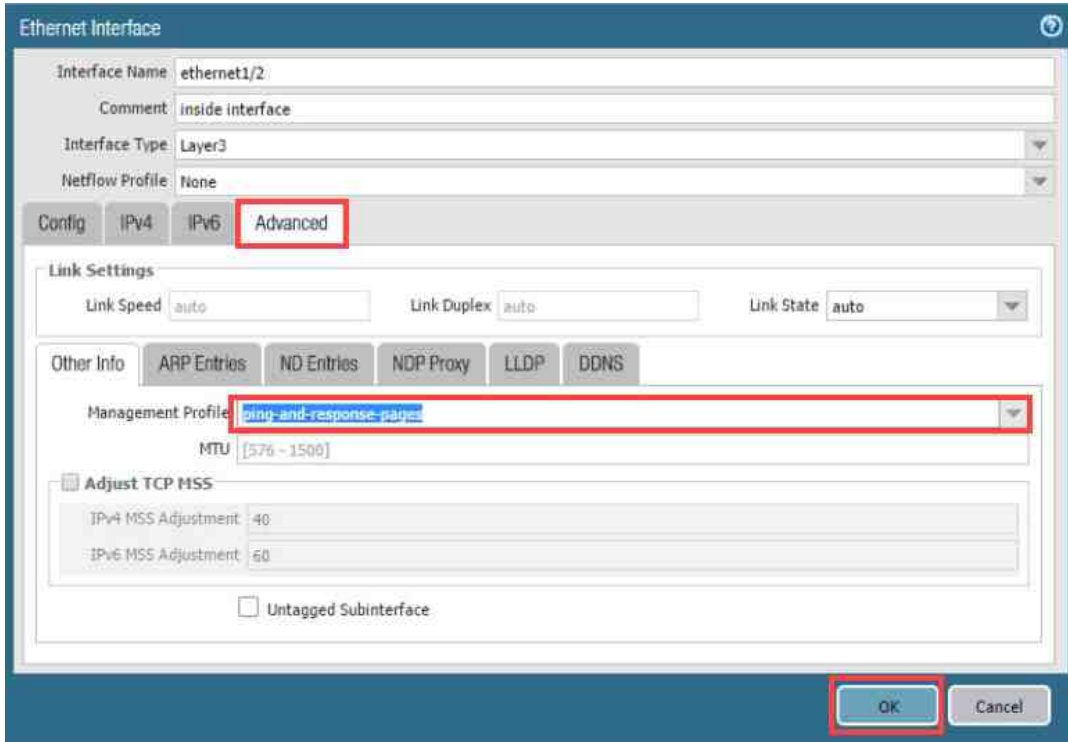
- Click the Ethernet Interface IPv4 tab and configure the following:

Parameter	Value
Type	Static
IP	Click Add and type 192. 168. 1. 1/24







The image shows the 'Ethernet Interface' configuration window. The 'Interface Name' is 'ethernet1/2'. The 'Comment' is 'inside interface'. The 'Interface Type' is 'Layer3'. The 'Netflow Profile' is 'None'. The 'Config' tab is selected, and the 'IPv4' sub-tab is active. The 'Type' is 'Static'. The 'IP' section shows a list with '192.168.1.1/24' selected. The 'Add' button is highlighted with a red box. The 'OK' button is highlighted with a red box.

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



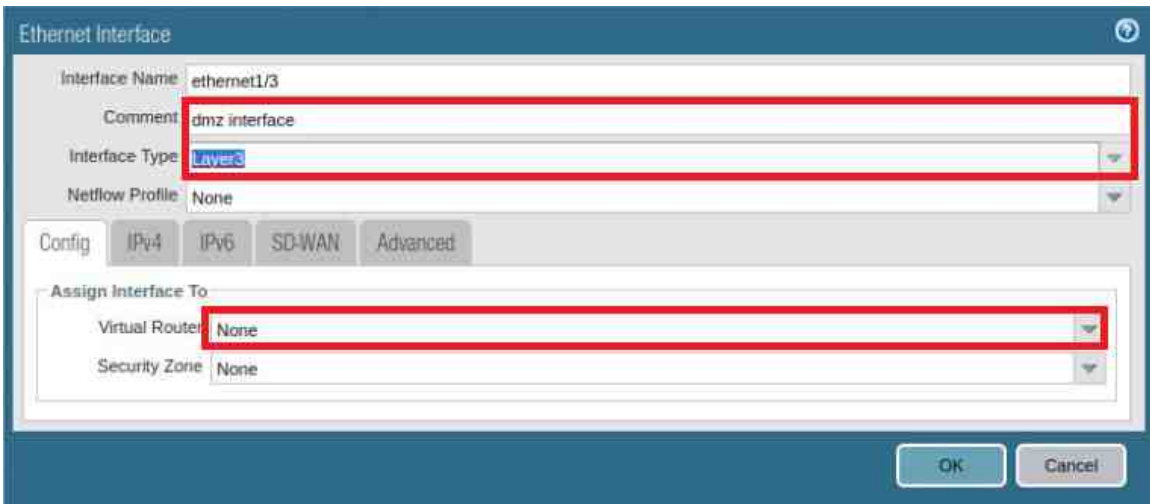
The screenshot shows the 'Ethernet Interface' configuration window. The 'Interface Name' is 'ethernet1/2' and the 'Comment' is 'inside interface'. The 'Interface Type' is 'Layer3' and the 'Netflow Profile' is 'None'. The 'Advanced' tab is selected. Under 'Link Settings', 'Link Speed' is 'auto', 'Link Duplex' is 'auto', and 'Link State' is 'auto'. Under 'Other Info', the 'Management Profile' dropdown is set to 'ping-and-response-pages'. The 'MTU' is '[576 - 1500]'. The 'Adjust TCP MSS' section shows 'IPv4 MSS Adjustment' as 40 and 'IPv6 MSS Adjustment' as 60. The 'Untagged Subinterface' checkbox is unchecked. The 'OK' button is highlighted.

- Click ethernet1/3 to configure the interface.

Interface	Interface Type	Management Profile	Link State	IP Address
ethernet1/1				none
ethernet1/2	Layer3	ping-and-response-pages		192.168.1.1/24
ethernet1/3				none
ethernet1/4				none

- In the Ethernet Interface window, configure the following:

Parameter	Value
Comment	dmz i nterface
Interface Type	Layer3
Virtual Router	None



The screenshot shows the 'Ethernet Interface' configuration window. The 'Interface Name' is 'ethernet1/3'. The 'Comment' is 'dmz interface'. The 'Interface Type' is 'Layer3'. The 'Netflow Profile' is 'None'. Below these fields are tabs for 'Config', 'IPv4', 'IPv6', 'SD-WAN', and 'Advanced'. The 'Assign Interface To' section has 'Virtual Router' set to 'None' and 'Security Zone' set to 'None'. At the bottom are 'OK' and 'Cancel' buttons. Red boxes highlight the 'Interface Type' dropdown and the 'Security Zone' dropdown.

11. Click the Security Zone dropdown list and select New Zone.

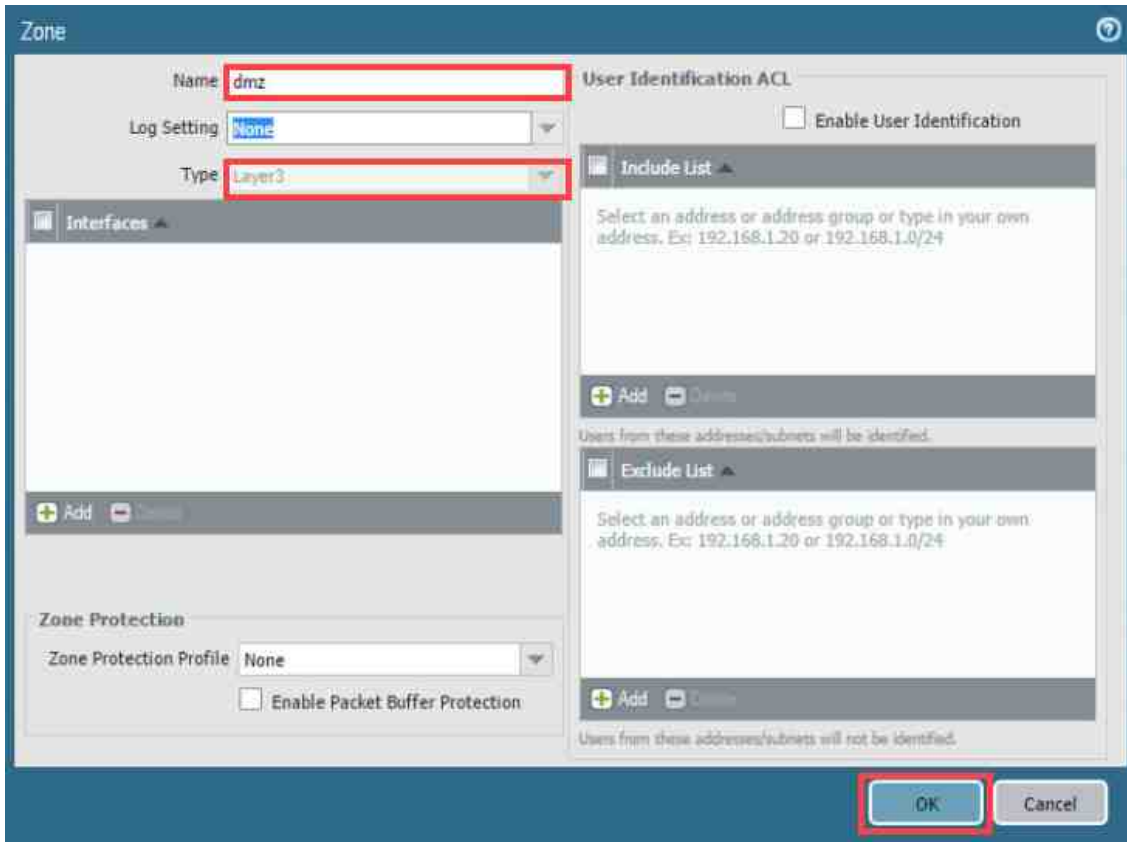


The screenshot shows the 'Assign Interface To' section with the 'Security Zone' dropdown menu open. The menu options are 'None', 'None', 'Inside', 'outside', and 'New Zone'. The 'New Zone' option is highlighted with a red box. The 'Virtual Router' is set to 'None'.

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.

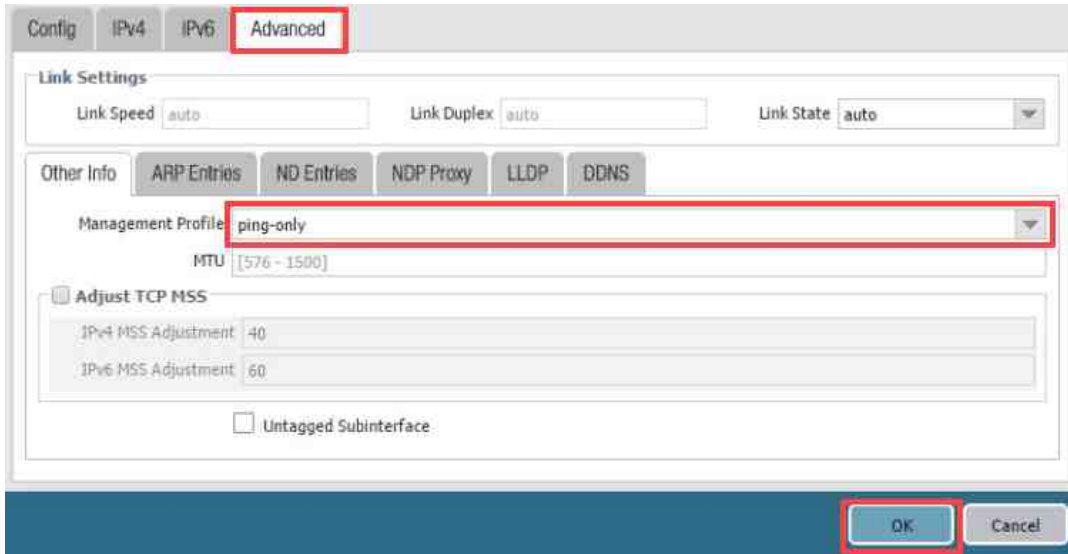


14. Click the IPv4 tab and configure the following:

Parameter	Value
Type	Static
IP	Click Add and type 192. 168. 50. 1/24



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



The screenshot shows the 'Advanced' tab of the Ethernet Interface configuration window. The 'Management Profile' dropdown menu is open, showing 'ping-only' as the selected option. The 'OK' button is highlighted with a red box.

16. Click ethernet1/1 to configure the interface.

Interface	Interface Type	Management Profile
ethernet1/1		
ethernet1/2	Layer3	ping-and-response-pages
ethernet1/3	Layer3	ping-only
ethernet1/4		

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

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



The screenshot shows the 'Ethernet Interface' configuration window. The 'Interface Name' is 'ethernet1/1'. The 'Comment' field is 'outside interface'. The 'Interface Type' dropdown is set to 'Layer3'. The 'Virtual Router' dropdown is set to 'None'. The 'Security Zone' dropdown is set to 'outside'. The 'OK' button is highlighted.

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:

☒ Automatically create default route pointing to default gateway provided by server

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

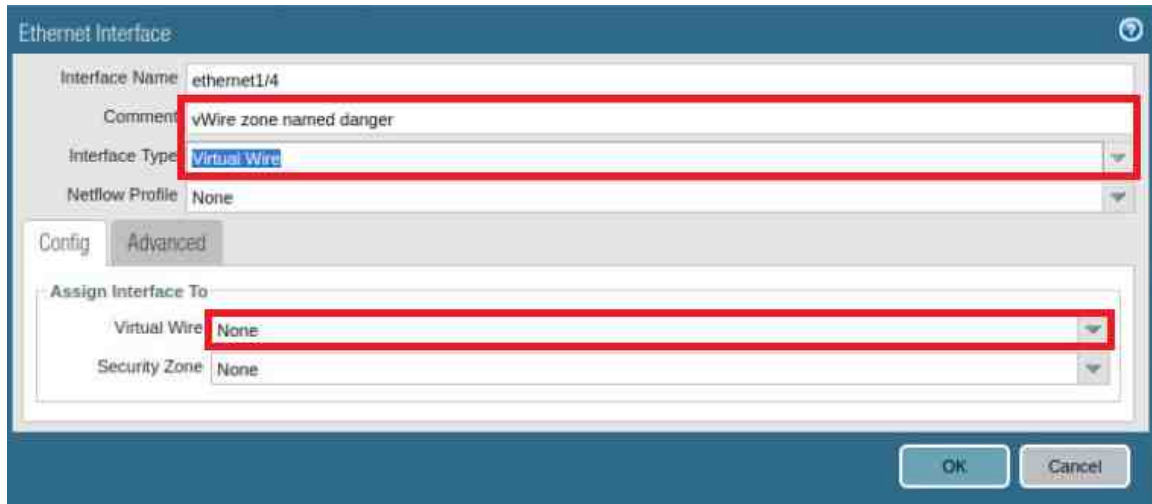


19. Click ethernet1/4 to configure the interface.

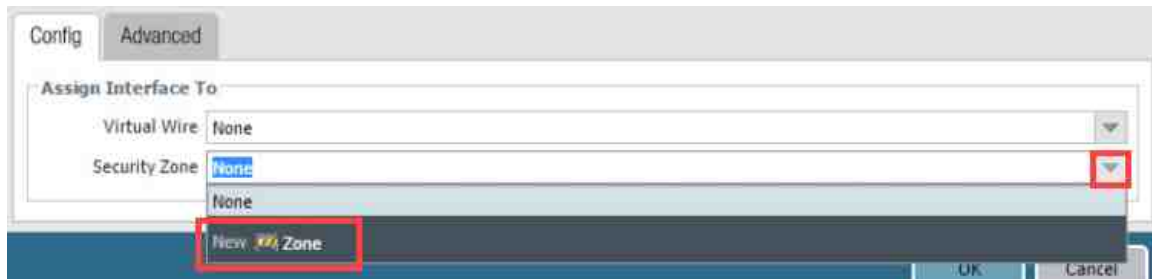
Interface	Interface Type	Management Profile	Link State	IP Address
ethernet1/1	Layer3			Dynamic-DHCP Client
ethernet1/2	Layer3	ping-and-response-pages		192.168.1.1/24
ethernet1/3	Layer3	ping-only		192.168.50.1/24
ethernet1/4				none

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

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

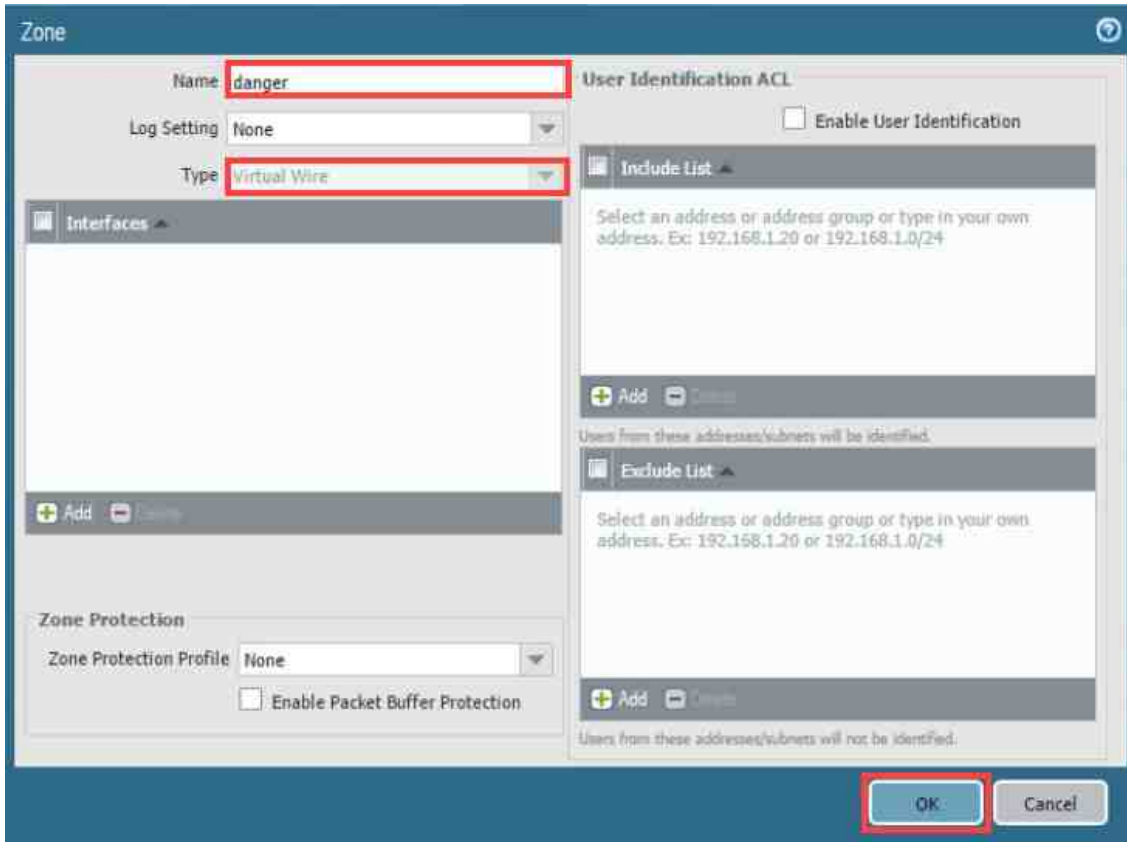


21. Click the Security Zone dropdown list and select New Zone.



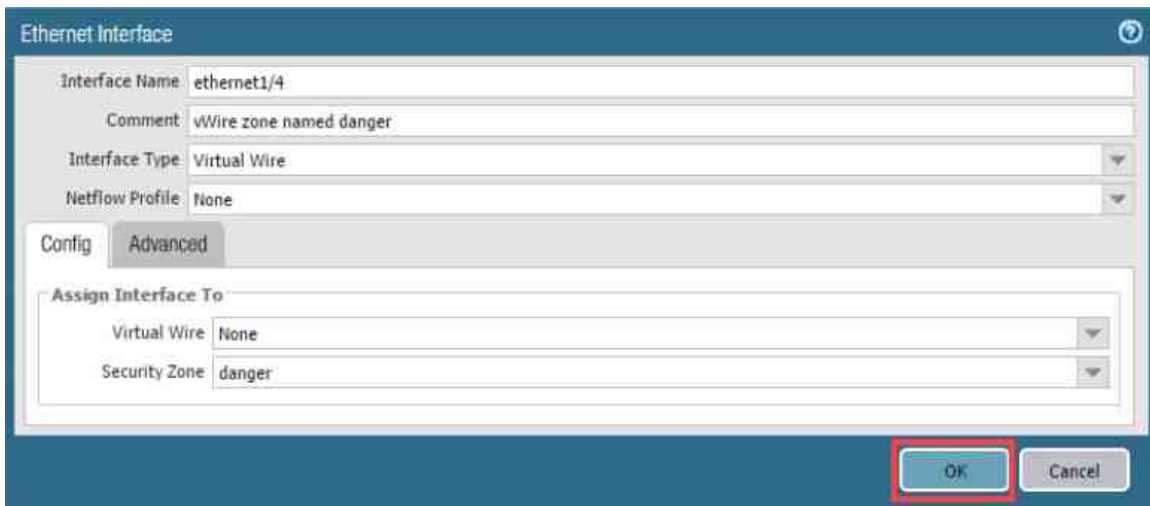
22. The Zone configuration window opens. Configure the following, followed by clicking OK.

Parameter	Value
Name	danger
Type	Virtual Wire should be selected



The screenshot shows the 'Zone' configuration window. The 'Name' field is set to 'danger', 'Log Setting' is 'None', and 'Type' is 'Virtual Wire'. The 'User Identification ACL' section has 'Enable User Identification' unchecked. The 'Include List' and 'Exclude List' sections are empty. The 'Zone Protection' section has 'Zone Protection Profile' set to 'None' and 'Enable Packet Buffer Protection' unchecked. The 'OK' button is highlighted with a red box.

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



The screenshot shows the 'Ethernet Interface' configuration window. The 'Interface Name' is 'ethernet1/4', 'Comment' is 'vWire zone named danger', 'Interface Type' is 'Virtual Wire', and 'Netflow Profile' is 'None'. The 'Assign Interface To' section shows 'Virtual Wire' set to 'None' and 'Security Zone' set to 'danger'. The 'OK' button is highlighted with a red box.

24. Click ethernet1/5 to configure the interface.

Interface	Interface Type	Management Profile	Link State	IP Address
ethernet1/1	Layer3			Dynamic-DHCP Client
ethernet1/2	Layer3	ping-and-response-pages		192.168.1.1/24
ethernet1/3	Layer3	ping-only		192.168.50.1/24
ethernet1/4	Virtual Wire			none
ethernet1/5				none
ethernet1/6				none

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

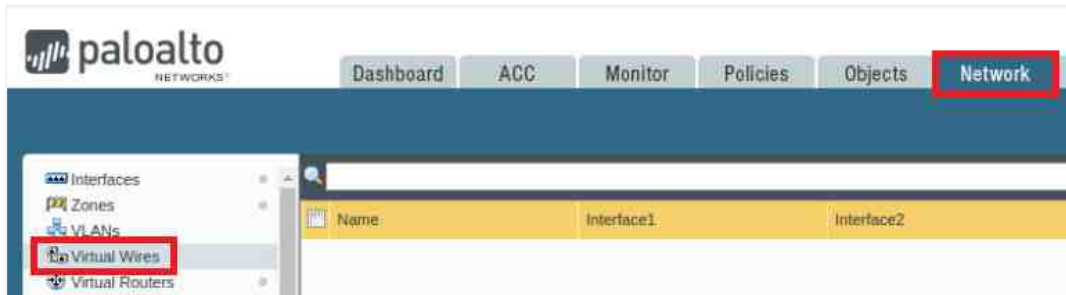


26. Leave the firewall web interface open to continue with the next task.

2.4 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.

2.5 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.



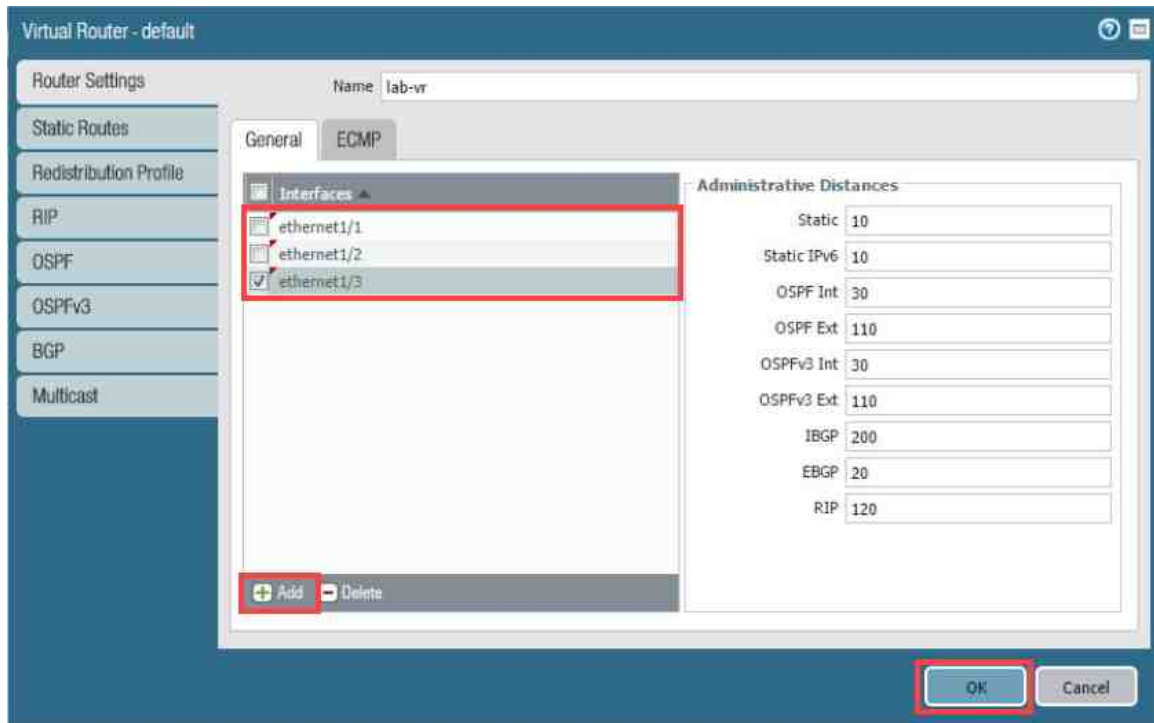
2. Click default to open the default virtual router.



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



- 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.

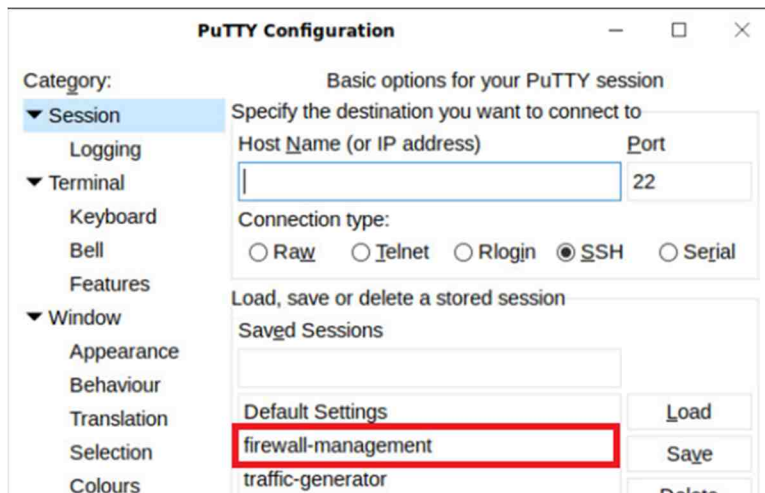
- Commit all changes.
- Leave the firewall web interface open to continue with the next task.

2.6 Test Connectivity

1. Double-click on the PuTTY icon from the Client desktop.



2. Double-click firewall-management:



3. Log in using the following information:

Parameter	Value
Name	admin
Password	Train1ng\$

```
login as: admin
Using keyboard-interactive authentication.
Password:

Number of failed attempts since last successful login: 0

admin@firewall-a>
```

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

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

```
admin@firewall-a> show interface ethernet1/1
-----
Name: ethernet1/1, ID: 16
Link status:
  Runtime link speed/duplex/state: 10000/full/up
  Configured link speed/duplex/state: auto/auto/auto
MAC address:
  Port MAC address 00:50:56:8a:91:be
Operation mode: layer3
Untagged sub-interface support: no
-----
Name: ethernet1/1, ID: 16
Operation mode: layer3
Virtual router lab-vr
Interface MTU 1500
Interface IP address (dynamic): 203.0.113.21/24
Interface management profile: N/A
Service configured:
Zone: outside, virtual system: vsys1
Adjust TCP MSS: no
Policing: no
-----
```



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
```

```
admin@firewall-a> show routing route
flags: A:active, ? :loose, C:connect, H:host, S:static, I:internal, R:rip, O:ospf, B:bgp,
       Oi:ospf intra-area, Oo:ospf inter-area, O1:ospf ext-type-1, O2:ospf ext-type-2, E:ecmp, M:multicast

VIRTUAL ROUTER: lab-vr (id 1)
=====
destination      nexthop          metric flags    age  interface    next-AS
0.0.0.0/0         203.0.113.1      10    A S          0    ethernet1/1
192.168.1.0/24    192.168.1.1      0     A C          0    ethernet1/2
192.168.1.1/32    0.0.0.0          0     A H          0
192.168.50.0/24   192.168.50.1     0     A C          0    ethernet1/3
192.168.50.1/32   0.0.0.0          0     A H          0
203.0.113.0/24    203.0.113.21     0     A C          0    ethernet1/1
203.0.113.21/32   0.0.0.0          0     A H          0
total routes shown: 7
```



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

- From the CLI, enter the command below.

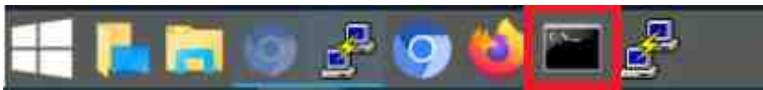
```
admin@firewall-a> ping source 203.0.113.21 host 8.8.8.8
```

```
admin@firewall-a> ping source 203.0.113.21 host 8.8.8.8
PING 8.8.8.8 (8.8.8.8) from 203.0.113.21 : 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=2 ttl=52 time=19.8 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=52 time=8.87 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=52 time=17.5 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=52 time=15.9 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=52 time=14.9 ms
```



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

- After a few successful pings, press CTRL+C to stop the ping.
- On the lab environment Client desktop, click Xfce Terminal to open a Terminal window.



- In the Terminal window, enter the command below.

```
C:\home\lab-user> ping 192.168.1.1 -c 4
```

```
C:\home\lab-user> ping 192.168.1.1 -c 4
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=1.39 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=1.97 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=64 time=1.78 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=64 time=1.62 ms

--- 192.168.1.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 1.391/1.692/1.971/0.215 ms
C:\home\lab-user>
```



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

- Type `exit` followed by pressing the Enter key in the Terminal window to close it.










2.7 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.

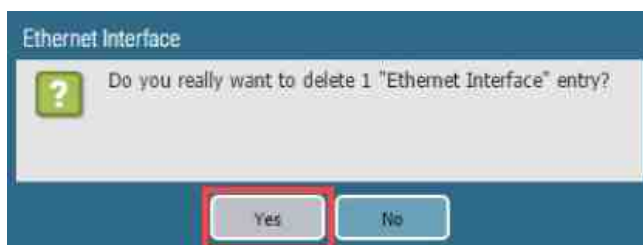


2. Select but do not open ethernet1/1, followed by clicking Delete.

Interface	Interface Type	Management Profile	Link State	IP Address
ethernet1/1	Layer3			Dynamic-DHCP Client
ethernet1/2	Layer3	ping-and-response-pages		192.168.1.1/24
ethernet1/3	Layer3	ping-only		192.168.50.1/24
ethernet1/4	Virtual Wire			none
ethernet1/5	Virtual Wire			none
ethernet1/6				none
ethernet1/7				none
ethernet1/8				none
ethernet1/9				none

At the bottom of the table, there are three buttons: 'Add Subinterface', 'Delete' (highlighted with a red box), and 'PDF/CSV'.

3. When prompted, click Yes.



- Commit all changes.



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

- Click on ethernet 1/1 to configure the interface.

Interface	Interface Type	Management Profile	Link State	IP Address
ethernet1/1				none
ethernet1/2	Layer3	ping-and-response-pages		192.168.1.1/24
ethernet1/3	Layer3	ping-only		192.168.50.1/24
ethernet1/4	Virtual Wire			none

- In the Ethernet Interface window, configure the following:

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



Ethernet Interface

Interface Name: ethernet1/1

Comment: outside interface

Interface Type: Layer3

Netflow Profile: None

Config | IPv4 | IPv6 | Advanced

Assign Interface To

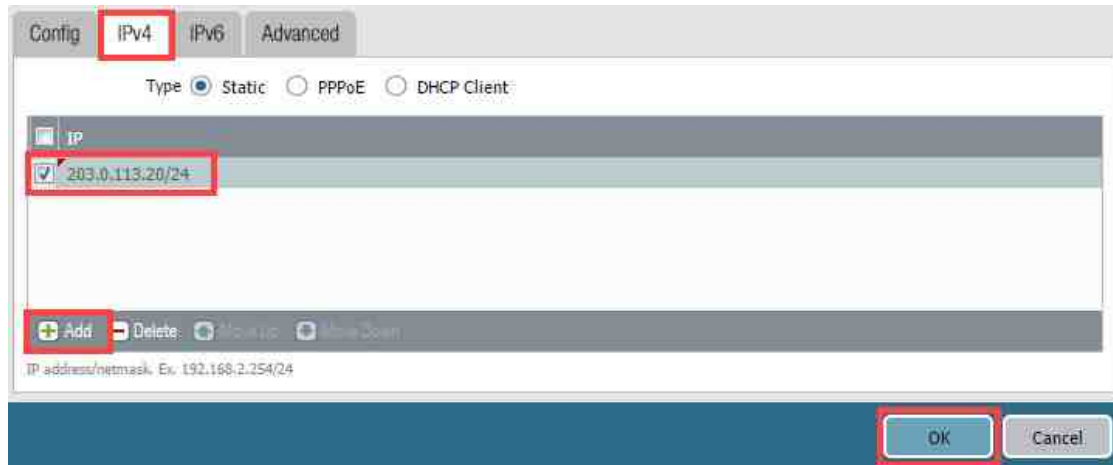
Virtual Router: lab-vr

Security Zone: outside

OK Cancel

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.

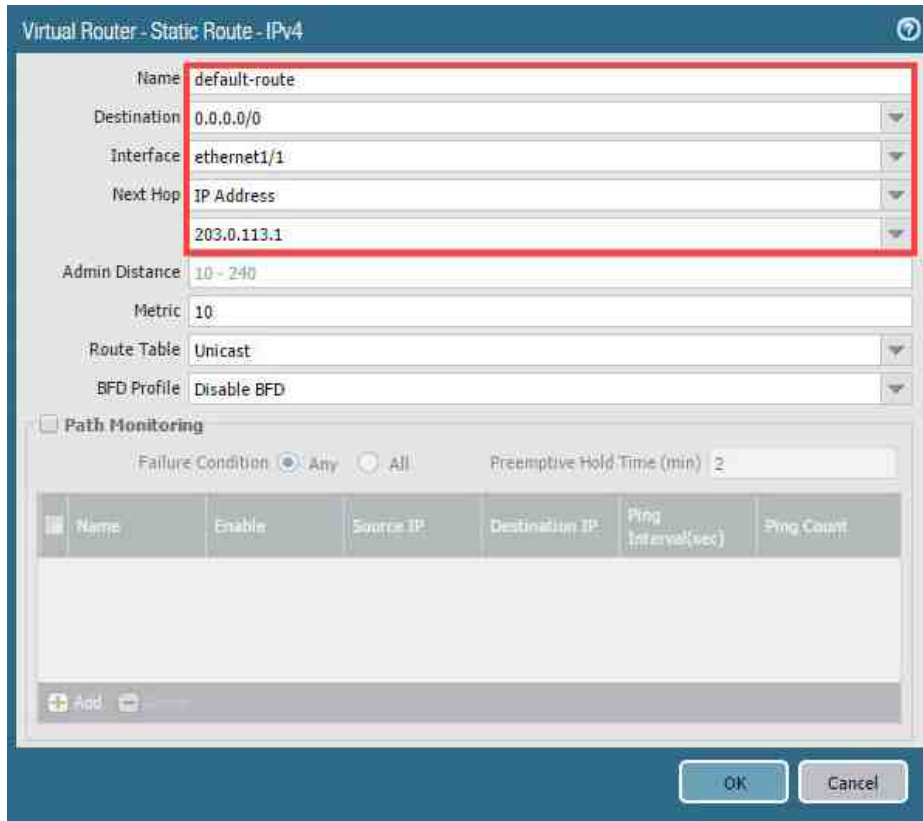


9. In the Virtual Router - lab-vr window, click the Static Routes vertical tab.



10. Click Add to configure the following static route:

Parameter	Value
Name	default t-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
```

```
admin@firewall-a> ping source 203.0.113.20 host 8.8.8.8
PING 8.8.8.8 (8.8.8.8) from 203.0.113.20 : 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=2 ttl=52 time=10.0 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=52 time=8.32 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=52 time=16.5 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=52 time=15.0 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=52 time=13.8 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=52 time=22.0 ms
64 bytes from 8.8.8.8: icmp_seq=8 ttl=52 time=10.8 ms
```



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.