



PALO ALTO NETWORKS - EDU-210

Lab 2: Interface Configuration

Document Version: 2017-09-28

Copyright © 2017 Network Development Group, Inc.
www.netdevgroup.com

NETLAB Academy Edition, NETLAB Professional Edition, and NETLAB+ are registered trademarks of Network Development Group, Inc.

VMware is a registered trademark of VMware, Inc. Cisco, IOS, Cisco IOS, Networking Academy, CCNA, and CCNP are registered trademarks of Cisco Systems, Inc. EMC² is a registered trademark of EMC Corporation.

Contents

Introduction	3
Objectives.....	3
Lab Topology	4
Lab Settings	5
2 Lab: Interface Configuration	6
2.0 Load Lab Configuration	6
2.1 Create New Security Zones	7
2.2 Create Interface Management Profiles.....	9
2.3 Configure Ethernet Interfaces.....	12
2.5 Create a Virtual Wire.....	21
2.6 Create a Virtual Router	22
2.7 Test Connectivity.....	24
2.8 Modify Outside Interface Configuration	25
2.4 Configure Ethernet Interfaces.....	10
2.5 Create a Virtual Wire.....	18
2.6 Create a Virtual Router.....	19
2.7 Test Connectivity.....	21
2.8 Modify Outside Test Configuration.....	22

Introduction

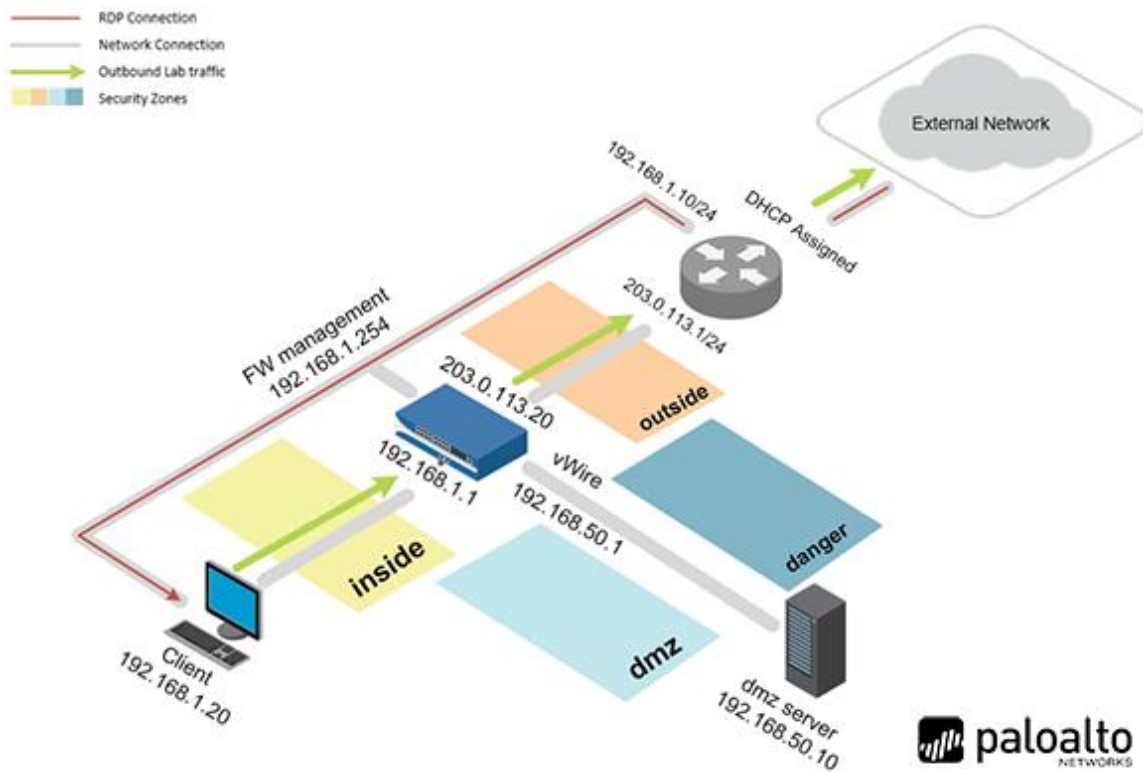
Now that we have setup our admin accounts and verified that we can connect to the admin portal, and setup our system to begin receiving updates it is now time to start configuring our firewall appliance.

The company's security and network architects have decided on 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



Lab Settings

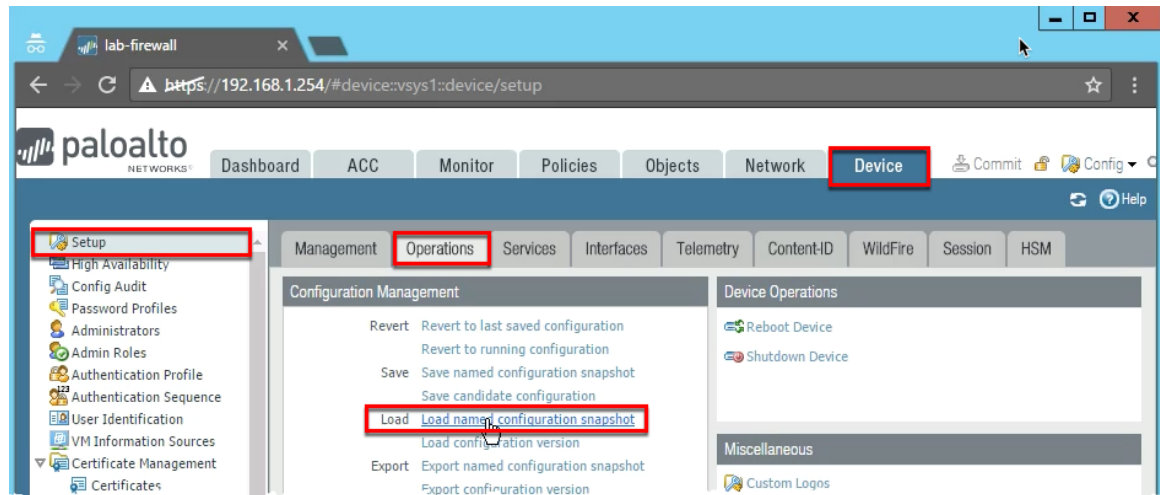
The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Client – Windows 2012 R2	192.168.1.20	lab-user	Pal0Alt0
Firewall – PA-VM	192.168.1.254	admin	admin

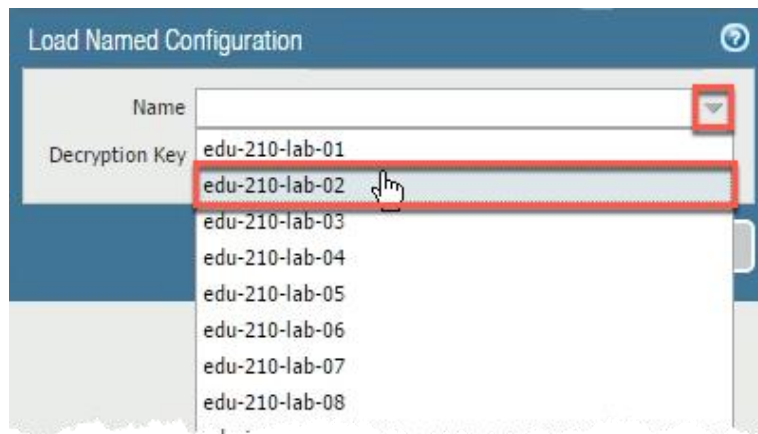
2 Lab: Interface Configuration

2.0 Load Lab Configuration

1. In the WebUI select **Device > Setup > Operations**.
2. Click **Load named configuration snapshot**:



3. Select edu-210-lab-02 and click **OK**.

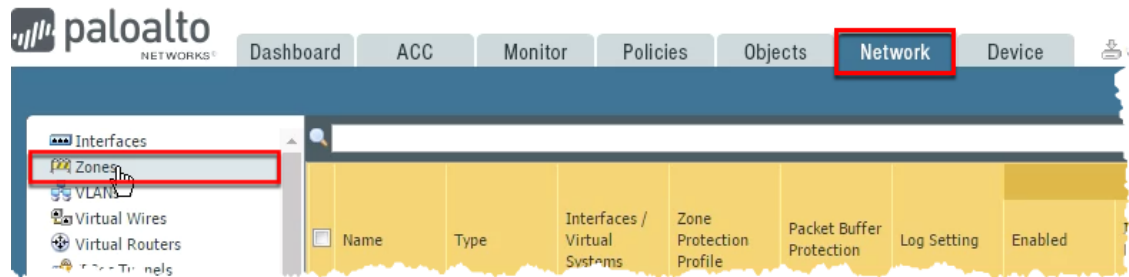


4. Click **Close**.
5. **Commit** all changes.

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. Select **Network > Zones**.



2. Click **Add** to create a new zone. The Zone configuration window opens.



3. 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.

Zone

Name:

Log Setting:

Type:

Interfaces

+ Add - Delete

Zone Protection

Zone Protection Profile:

☐ Enable Packet Buffer Protection

User Identification ACL

☐ Enable User Identification

Include List

Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24

+ Add - Delete

Users from these addresses/subnets will be identified.

Exclude List

Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24

+ Add - Delete

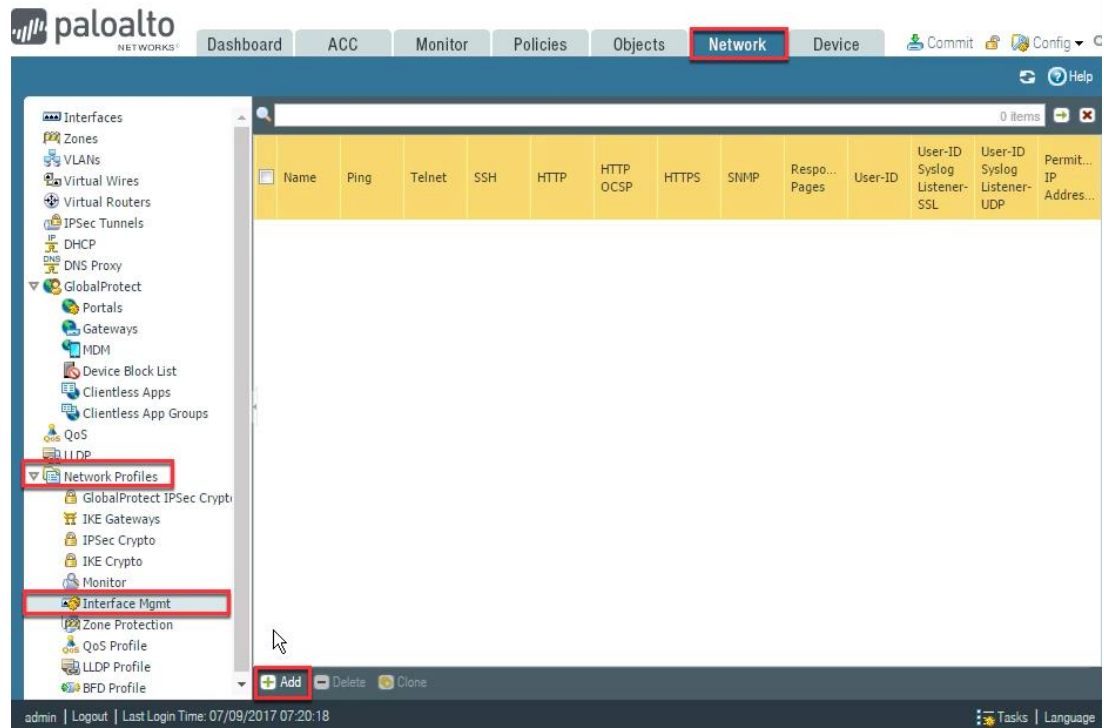
Users from these addresses/subnets will not be identified.

OK Cancel

2.2 Create Interface Management Profiles

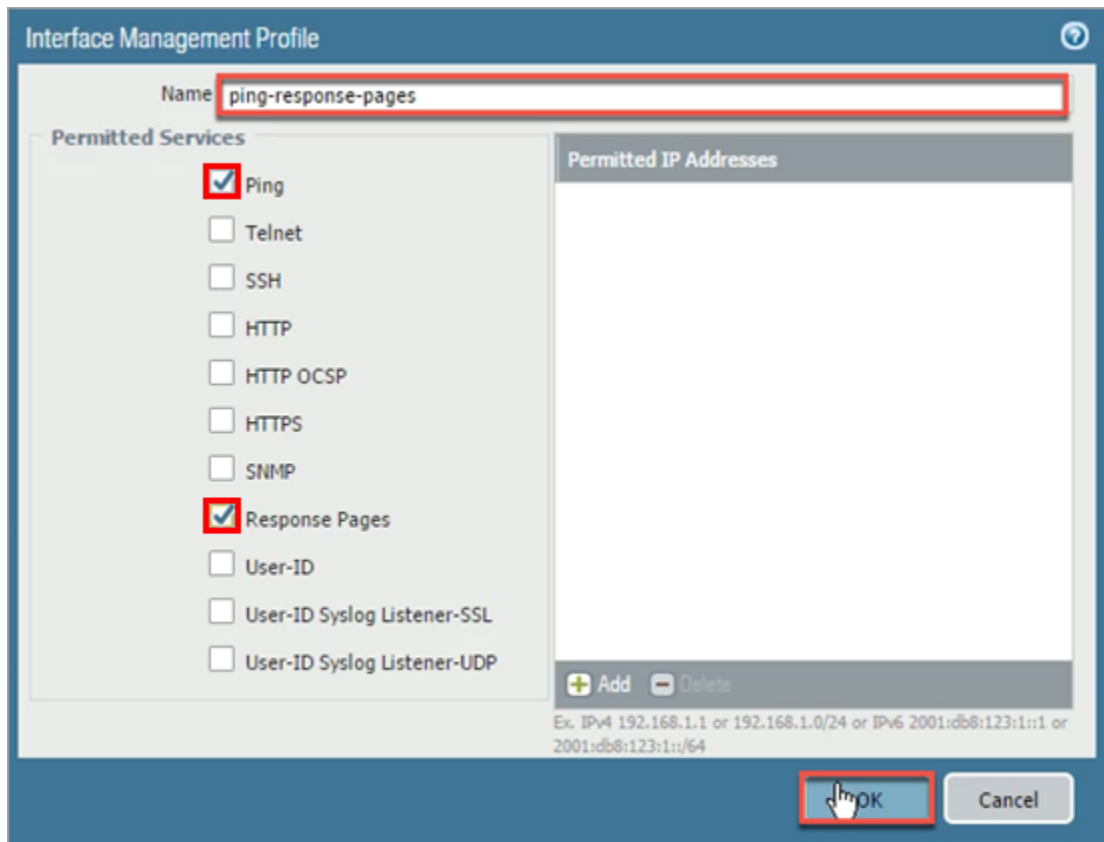
An Interface Management Profile protects the firewall from unauthorized access by defining the services and IP addresses that a firewall interface permits. You can assign an Interface Management Profile to Layer 3 Ethernet interfaces (including subinterfaces) and to logical interfaces (Aggregate, VLAN,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

1. Select **Network > Network Profiles > Interface Mgmt.**
2. Click **Add** to open the Interface Management Profile configuration window.



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

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



4. Click **Add** to create another Interface Management Profile.
5. In the Interface Management Profile configuration window configure the following then click **OK**.

Parameter	Value
Name	ping
Permitted Services	
Ping	Checked

Interface Management Profile

Name

Permitted Services

- ☒ Ping
- ☐ Telnet
- ☐ SSH
- ☐ HTTP
- ☐ HTTP OCSP
- ☐ HTTPS
- ☐ SNMP
- ☐ Response Pages
- ☐ User-ID
- ☐ User-ID Syslog Listener-SSL
- ☐ User-ID Syslog Listener-UDP

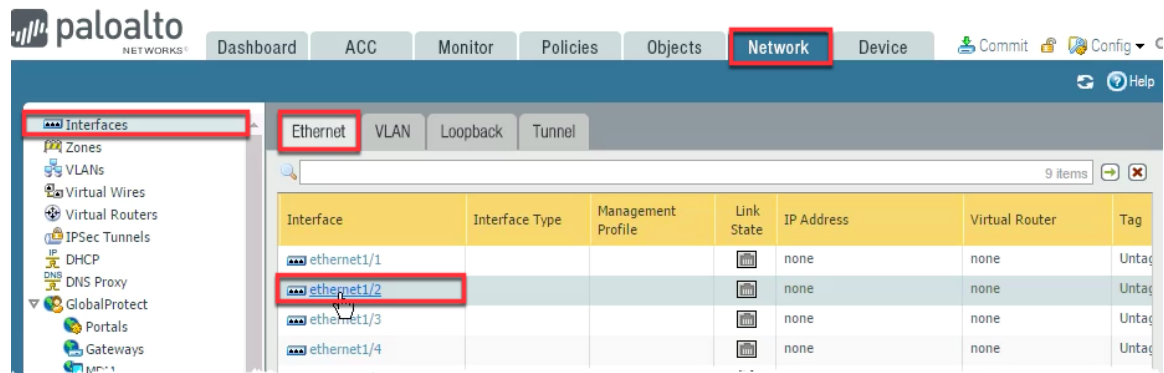
Permitted IP Addresses

+ Add - Delete

Ex. IPv4 192.168.1.1 or 192.168.1.0/24 or IPv6 2001:db8:123:1::1 or 2001:db8:123:1::/64

2.3 Configure Ethernet Interfaces

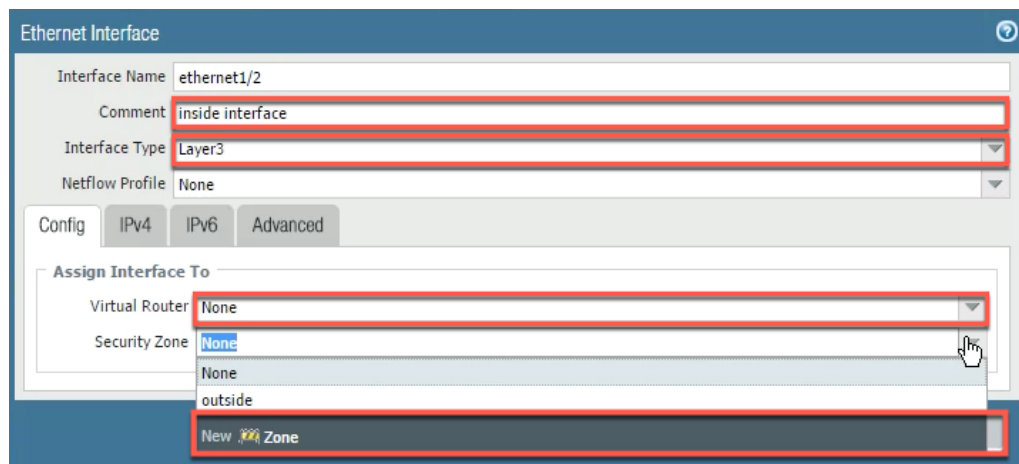
1. Select **Network > Interfaces > Ethernet**.
2. Click to open ethernet1/2.



3. Configure the following:

Parameter	Value
Comment	inside interface
Type	Layer3
Virtual Router	None

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

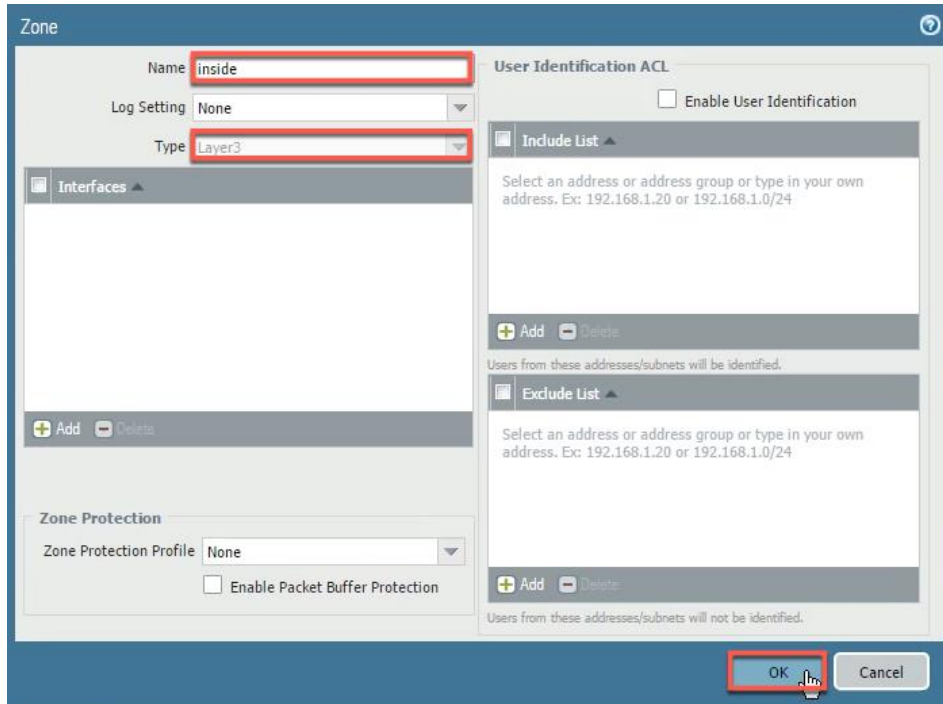


The Zone configuration window opens.

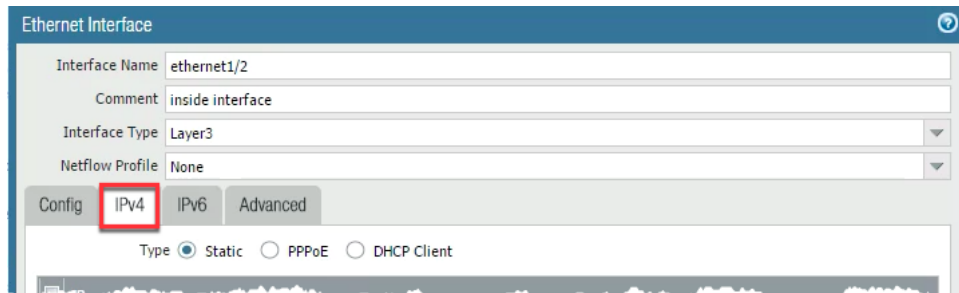
5. Configure the following:

Parameter	Value
Name	inside
Type	Select Layer3

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



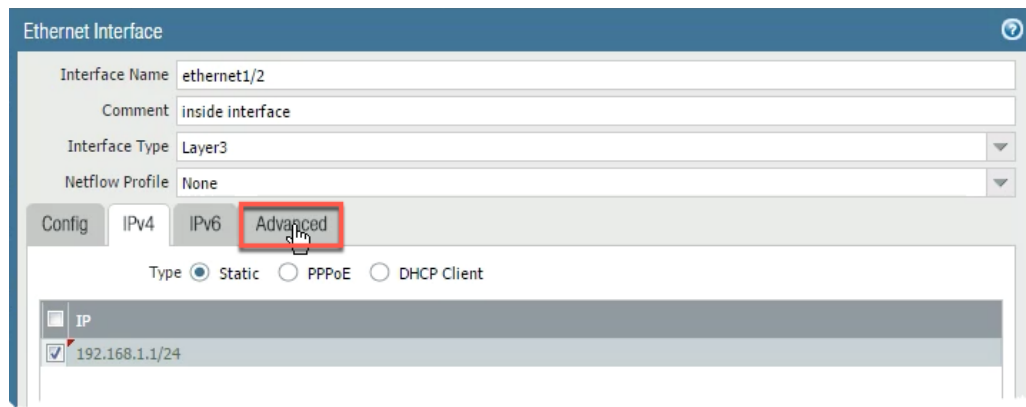
7. Click the Ethernet Interface IPv4 tab.



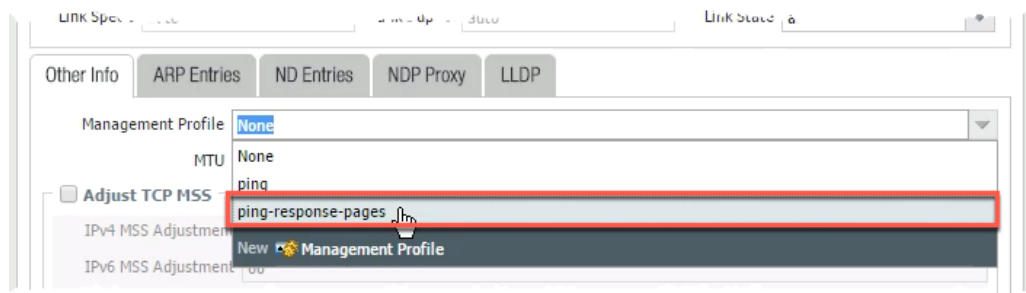
8. Configure the following:

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

9. Click the **Advanced** tab.



10. Click the Management Profile drop-down list and select ping-response-pages.



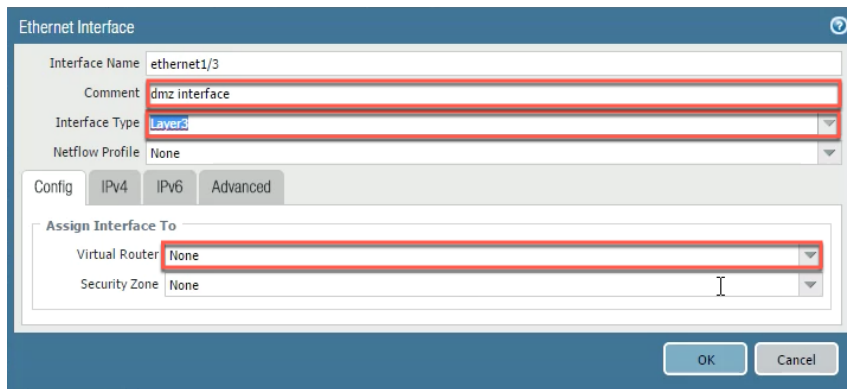
11. Click **OK** to close the Ethernet Interface configuration window.

12. Click to open ethernet1/3.



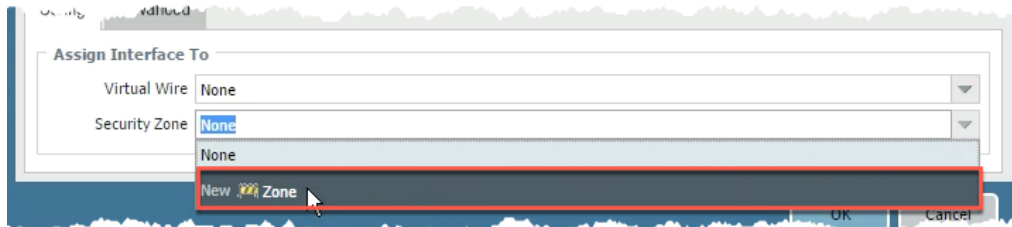
13. Configure the following:

Parameter	Value
Comment	dmz interface
Interface Type	Layer3
Virtual Router	None



The screenshot shows the 'Ethernet Interface' configuration window. The 'Interface Name' is 'ethernet1/3', 'Comment' is 'dmz interface', and 'Interface Type' is 'Layer3'. The 'Assign Interface To' section shows 'Virtual Router' as 'None' and 'Security Zone' as 'None'. The 'OK' button is highlighted with a red box.

14. Click the Security Zone drop-down list and select New Zone. The Zone configuration window opens.

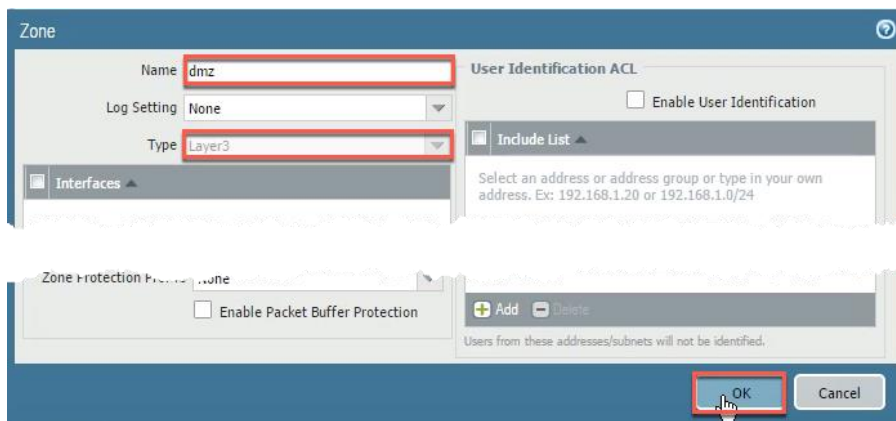


The screenshot shows the 'Assign Interface To' dialog box. The 'Security Zone' drop-down list is open, showing 'None' and 'New Zone'. The 'New Zone' option is highlighted with a red box.

15. Configure the following:

Parameter	Value
Name	dmz
Type	Layer3 should be selected

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



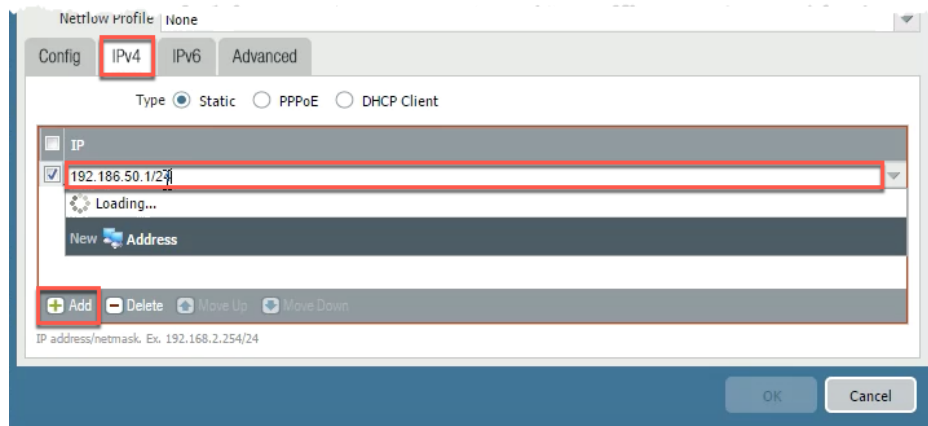
The screenshot shows the 'Zone' configuration window. The 'Name' is 'dmz', 'Log Setting' is 'None', and 'Type' is 'Layer3'. The 'OK' button is highlighted with a red box.

17. Click the IPv4 tab.

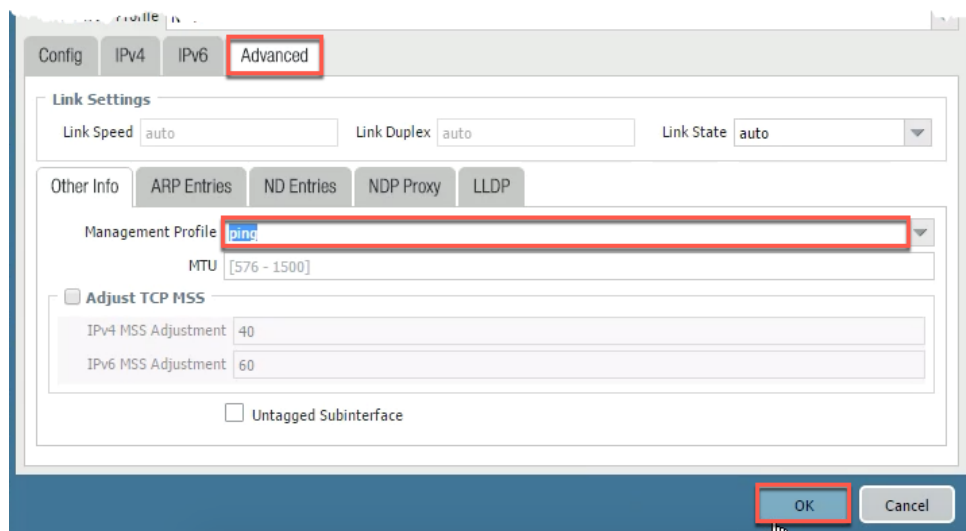
18. Configure the following:

Parameter	Value
Type	Static

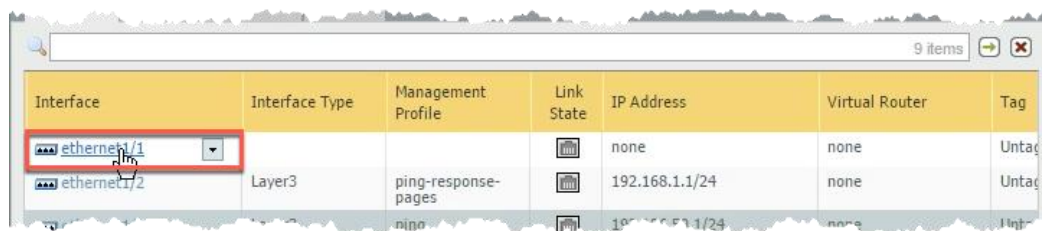
IP	Click Add and type 192.168.50.1/24
----	--



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

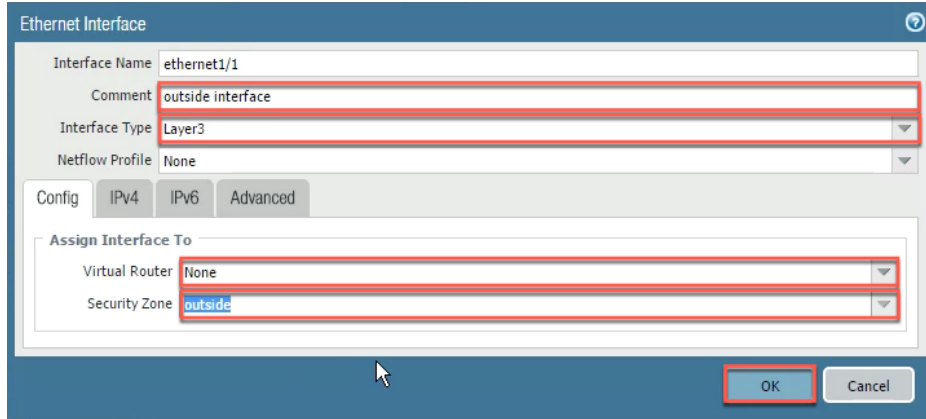


22. Click to open ethernet1/1.



23. 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' is 'outside interface'. The 'Interface Type' is 'Layer3'. The 'Netflow Profile' is 'None'. The 'Assign Interface To' section shows 'Virtual Router' as 'None' and 'Security Zone' as 'outside'. The 'OK' button is highlighted with a red box.

24. Click the IPv4 tab and configure the following:

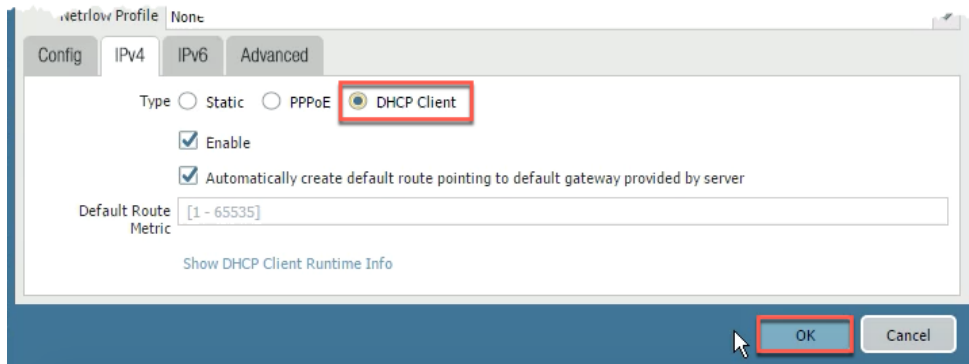
Parameter	Value
Type	DHCP Client

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.

25. Click **OK** to close the Ethernet Interface configuration window.



The screenshot shows the 'IPv4' configuration window. The 'Type' is 'DHCP Client'. The 'Enable' checkbox is checked. The 'Automatically create default route pointing to default gateway provided by server' checkbox is checked. The 'Default Route Metric' is '[1 - 65535]'. The 'OK' button is highlighted with a red box.

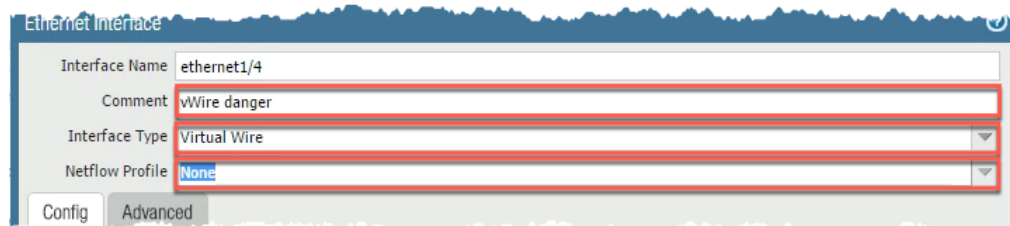
26. Click to open **ethernet1/4**.



Interface	Interface Type	Management Profile	Link State	IP Address	Virtual Router	Tag
ethernet1/1	Layer3			Dynamic-DHCP Client	none	Untag
ethernet1/2	Layer3	ping-response-pages		192.168.1.1/24	none	Untag
ethernet1/3	Layer3	ping		192.186.50.1/24	none	Untag
ethernet1/4				none	none	Untag
ethernet1/5				none	none	Untag

27. Configure the following:

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



Ethernet Interface

Interface Name: ethernet1/4

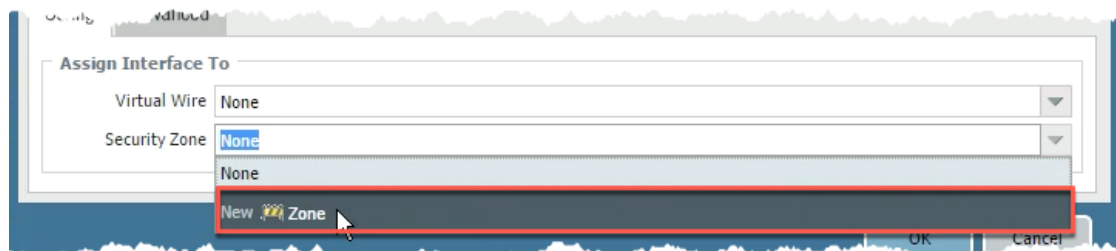
Comment: vWire danger

Interface Type: Virtual Wire

Netflow Profile: None

Config Advanced

28. Click the Security Zone drop-down list and select New Zone. The Zone configuration window opens.



Assign Interface To

Virtual Wire: None

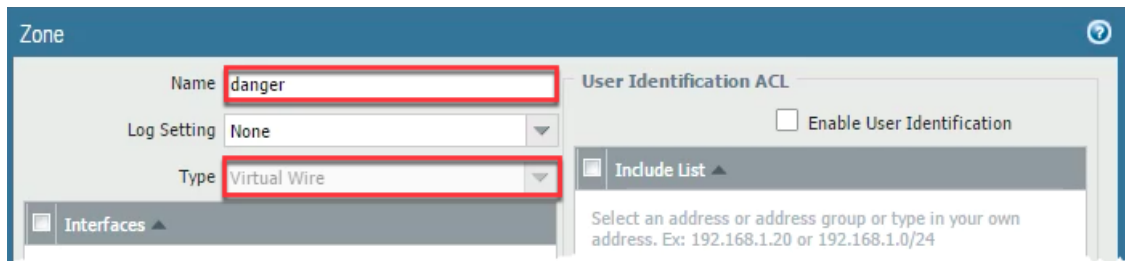
Security Zone: None

New Zone

OK Cancel

29. Configure the following:

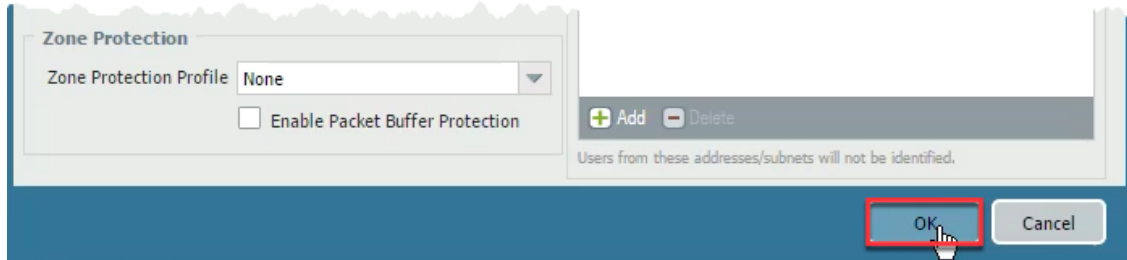
Parameter	Value
Name	danger
Type	Virtual Wire should be selected



Zone configuration window showing the following fields:

- Name: danger
- Log Setting: None
- Type: Virtual Wire
- User Identification ACL: ☐ Enable User Identification
- Include List: Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24

30. Click **OK** twice to close the Zone and Ethernet Interface configuration windows.



Zone Protection configuration window showing the following fields:

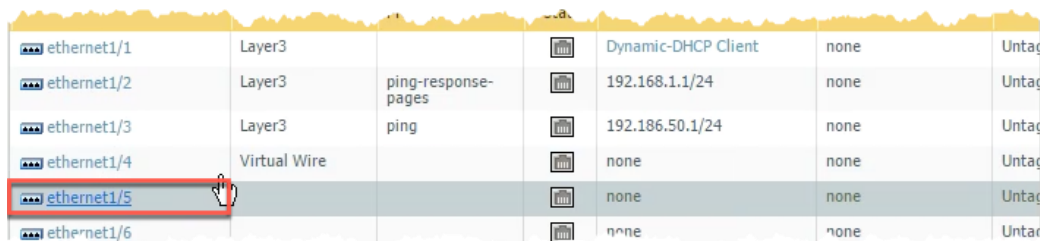
- Zone Protection Profile: None
- ☐ Enable Packet Buffer Protection
- Buttons: Add, Delete, OK, Cancel



Assign Interface To configuration window showing the following fields:

- Virtual Wire: None
- Security Zone: danger
- Buttons: OK, Cancel

31. Click to open **ethernet1/5**.



ethernet1/1	Layer3		Dynamic-DHCP Client	none	Untag
ethernet1/2	Layer3	ping-response-pages	192.168.1.1/24	none	Untag
ethernet1/3	Layer3	ping	192.186.50.1/24	none	Untag
ethernet1/4	Virtual Wire		none	none	Untag
ethernet1/5			none	none	Untag
ethernet1/6			none	none	Untag

32. Configure the following:

Parameter	Value
Comment	vWire danger
Interface Type	Virtual Wire
Virtual Wire	None
Security Zone	danger

33. Click **OK** to close the Ethernet Interface configuration window.

Ethernet Interface ?

Interface Name

Comment

Interface Type

Netflow Profile

Config **Advanced**

Assign Interface To

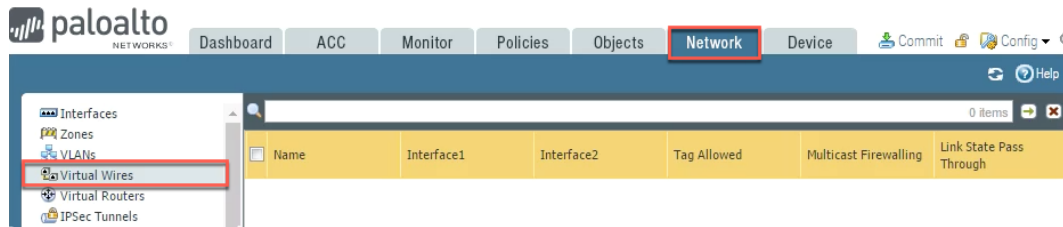
Virtual Wire

Security Zone

2.5 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. Select **Network > Virtual Wires**.



2. Click and configure the following:

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

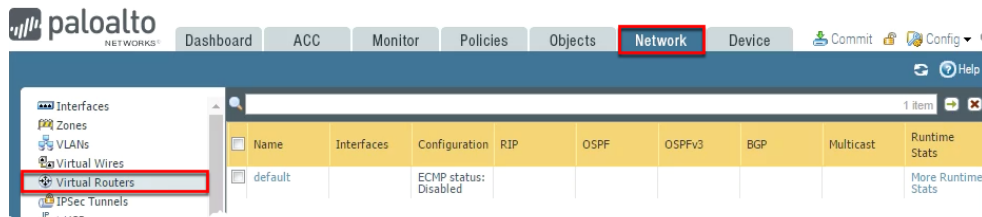


3. Click **OK**.

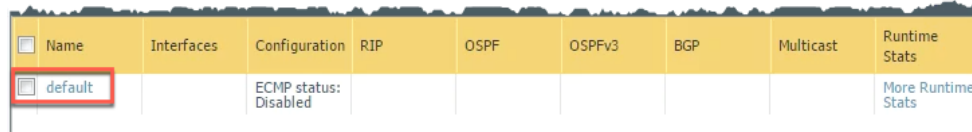
2.6 Create a Virtual Router

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.

1. Select **Network > Virtual Routers**.



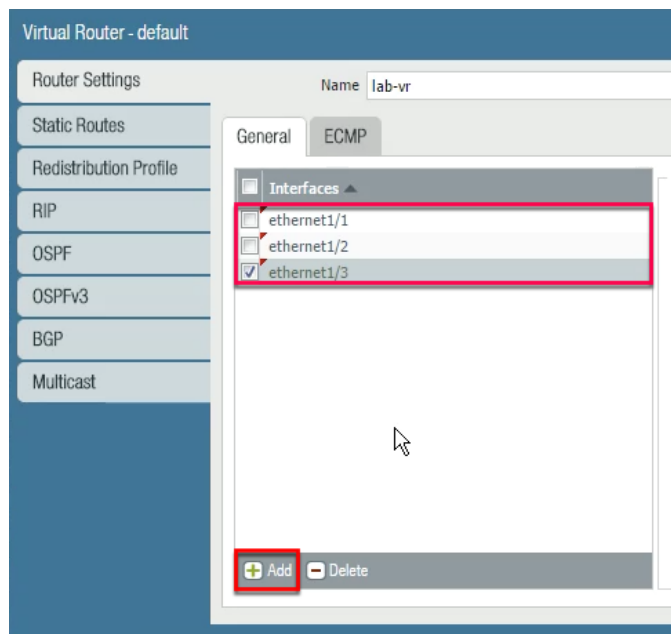
2. Click the default virtual router.



3. Rename the default router lab-vr.

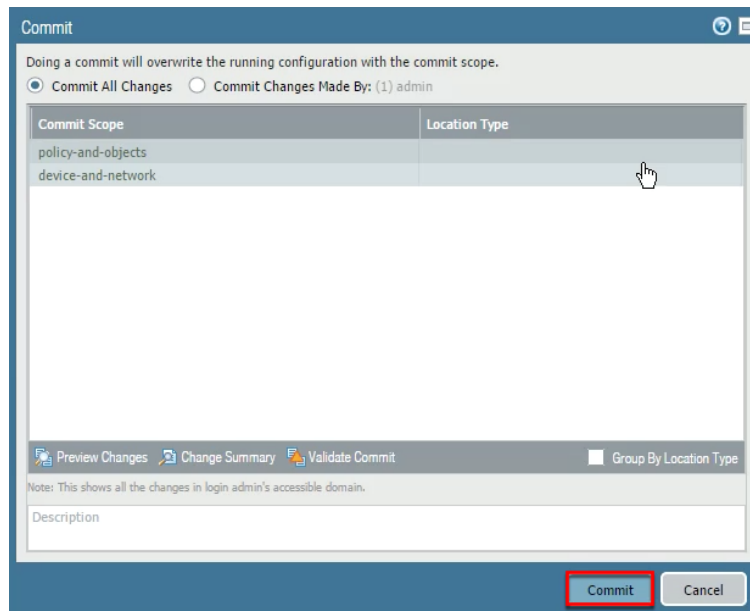
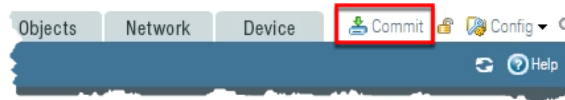


4. Add the following interfaces: ethernet1/1, ethernet1/2, and ethernet1/3.



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

5. Click **OK**.
6. **Commit** all changes.

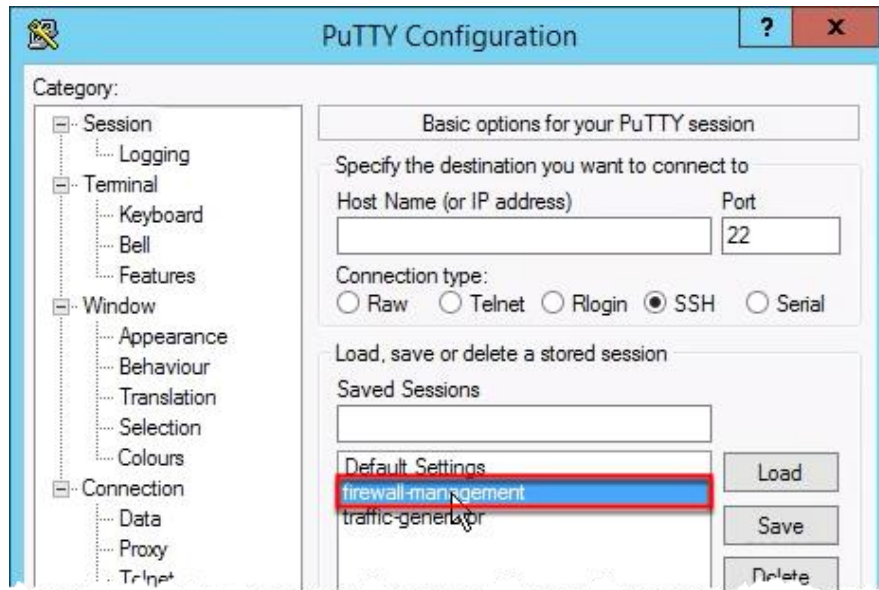


2.7 Test Connectivity

1. Open **PuTTY** from the Windows desktop.



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



3. Log in using the following information:

Parameter	Value
Name	admin
Password	admin

```
login as: admin
Using keyboard-interactive authentication.
Password:
Last login: Sun Jul  9 04:48:18 2017 from 192.168.1.21
```

4. Enter the command:

```
ping source 203.0.113.21 host 8.8.8.8
```

Because a default route was automatically installed, you should be getting replies from 8.8.8.8:


```
admin@lab-firewall> 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=1 ttl=127 time=32.3 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=127 time=64.1 ms
^C
--- 8.8.8.8 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1009ms
rtt min/avg/max/mdev = 32.313/48.232/64.151/15.919 ms
admin@lab-firewall>
```

5. On the lab environment Windows desktop, open a command-prompt window.



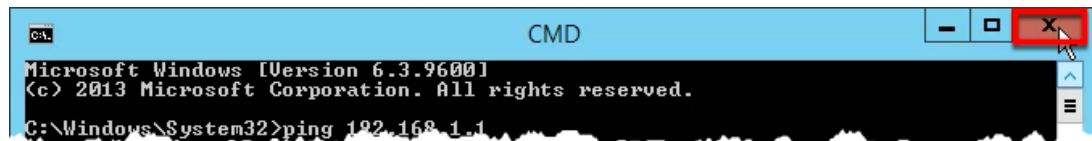
6. Type the command `ping 192.168.1.1`:

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

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=19ms TTL=64

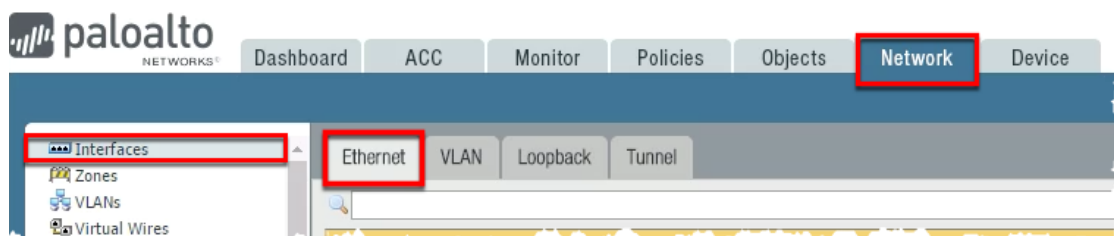
Ping statistics for 192.168.1.1:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 19ms, Maximum = 19ms, Average = 19ms
Control-C
^C
C:\Windows\System32>
```

7. Verify that you get a reply before proceeding.
8. Close the command-prompt window.





2.8 Modify Outside Interface Configuration

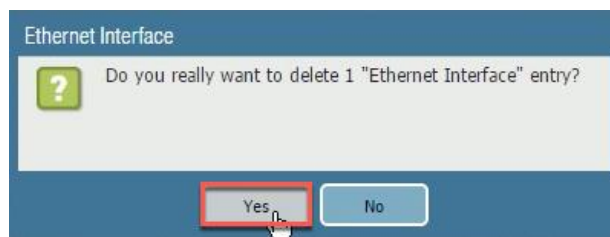
1. Select **Network > Interfaces > Ethernet**.



2. Select but, do not open: ethernet1/1

Interface	Interface Type	Management Profile	Link State	IP Address	Virtual Router	Tag
ethernet1/1	Layer3			Dynamic-DHCP Client	lab-vr	Untag
ethernet1/2	Layer3	ping-response-pages		192.168.1.1/24	lab-vr	Untag

- Click **Delete** then click **Yes**.

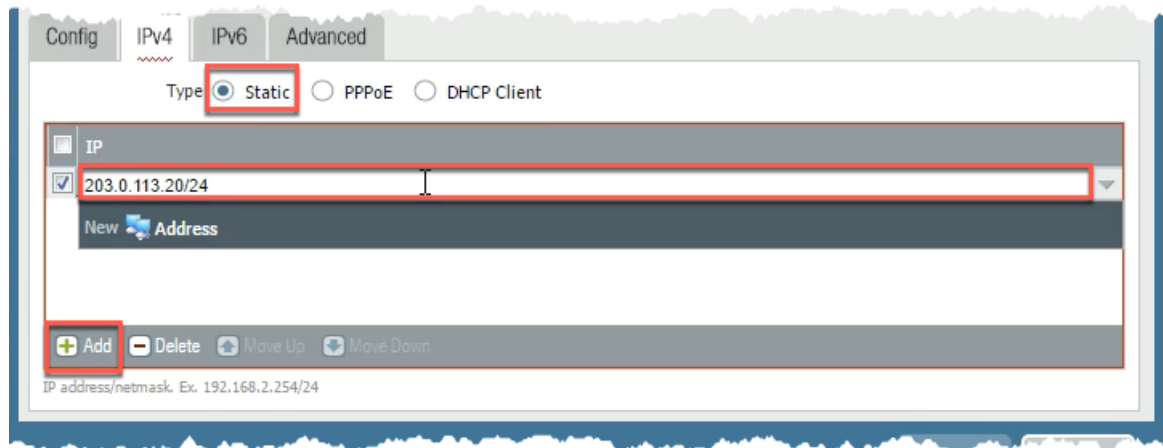


- Click and open Ethernet 1/1.
- Configure the following:

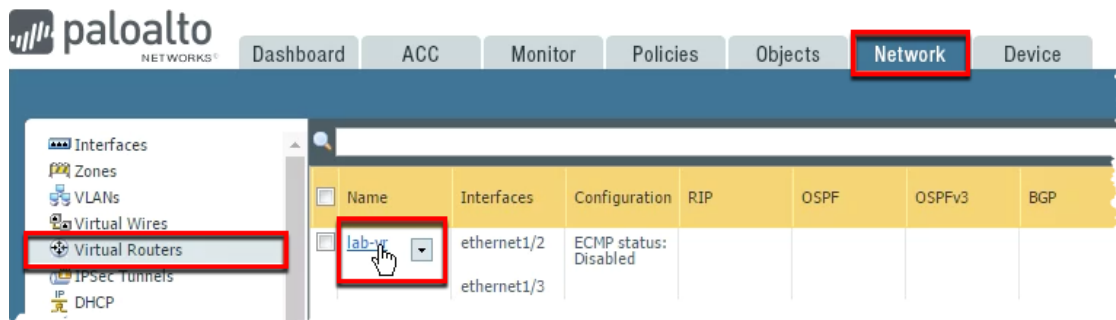
Parameter	Value
Comment	outside interface
Interface Type	Layer3
Virtual Router	Lab-vr
Security Zone	outside

- Click the *IPv4* tab and configure the following:

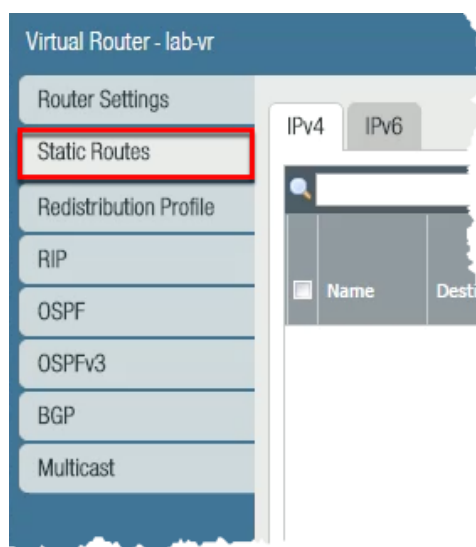
Parameter	Value
Type	Static
IP	203.0.113.20/24



7. Click **OK** to close the **Ethernet Interface** configuration window.
8. Select **Network > Virtual Routers**.
9. Click to open the lab-vr virtual router.

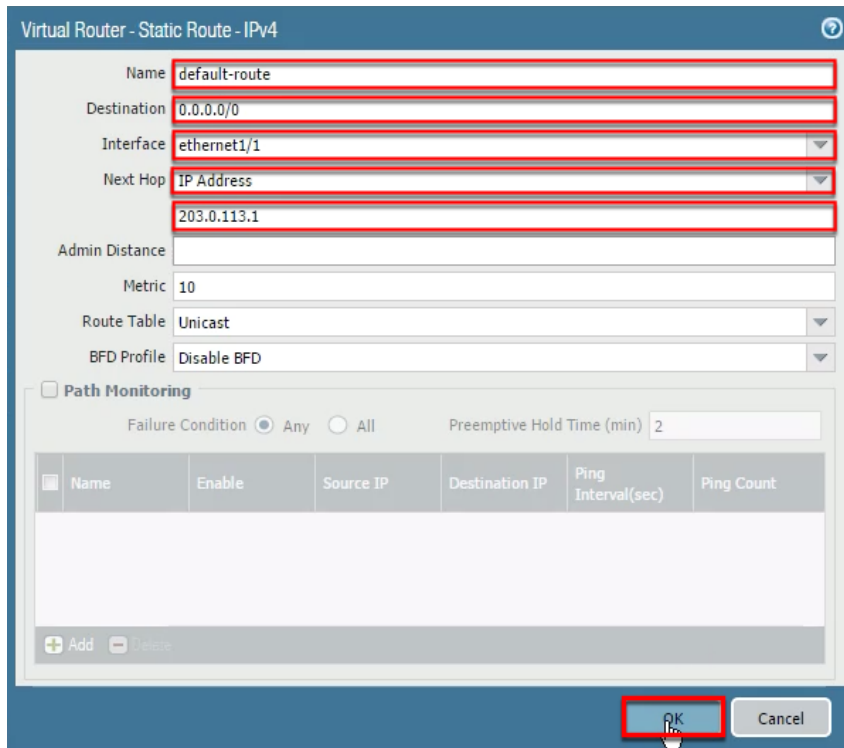


10. Click the **Static Routes** vertical tab:



11. 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



Virtual Router - Static Route - IPv4

Name: default-route

Destination: 0.0.0.0/0

Interface: ethernet1/1

Next Hop: IP Address

Next Hop IP Address: 203.0.113.1

Admin Distance:

Metric: 10

Route Table: Unicast

BFD Profile: Disable BFD

☐ Path Monitoring

Failure Condition: ☒ Any ☐ All Preemptive Hold Time (min): 2

Name	Enable	Source IP	Destination IP	Ping Interval(sec)	Ping Count

12. Click **OK** to add the static route and then click **OK** again to close the Virtual Router – lab-vr configuration window.

13. **Commit** all changes.



Dashboard ACC Monitor Policies Objects Network Device

1 item

Name	Interfaces	Configuration	RIP	OSPF	OSPFv3	BGP	Multicast	Runtime Stats
<input checked="" type="checkbox"/> lab-vr	ethernet1/1 ethernet1/2 ethernet1/3	Static Routes: 1 ECMP status: Disabled						More Runtime Stats

14. Make **PuTTY** window that was used to ping 8 . 8 . 8 . 8 the active window.



15. Type the command `ping source 203.0.113.20 host 8.8.8.8`

```
admin@PA-VM> 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=1 ttl=53 time=56.4 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=53 time=14.7 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=53 time=14.0 ms
```

16. Close the **PuTTY** window.

Stop. This is the end of the Interface Configuration lab.