# PALO ALTO NETWORKS EDU 210

# Lab 4: Connecting the Firewall to Production Networks

**Document Version: 2021-09-27**

# Contents

## Introduction

In preparation for deployment, you need to connect the firewall to the appropriate production networks. You already have cabled the firewall interfaces to the appropriate switch ports in the data center. You will configure the firewall with Layer 3 IP addresses and a virtual router. You also will create security zones that divide your network into separate logical areas so that you have more control over traffic from one segment to another.

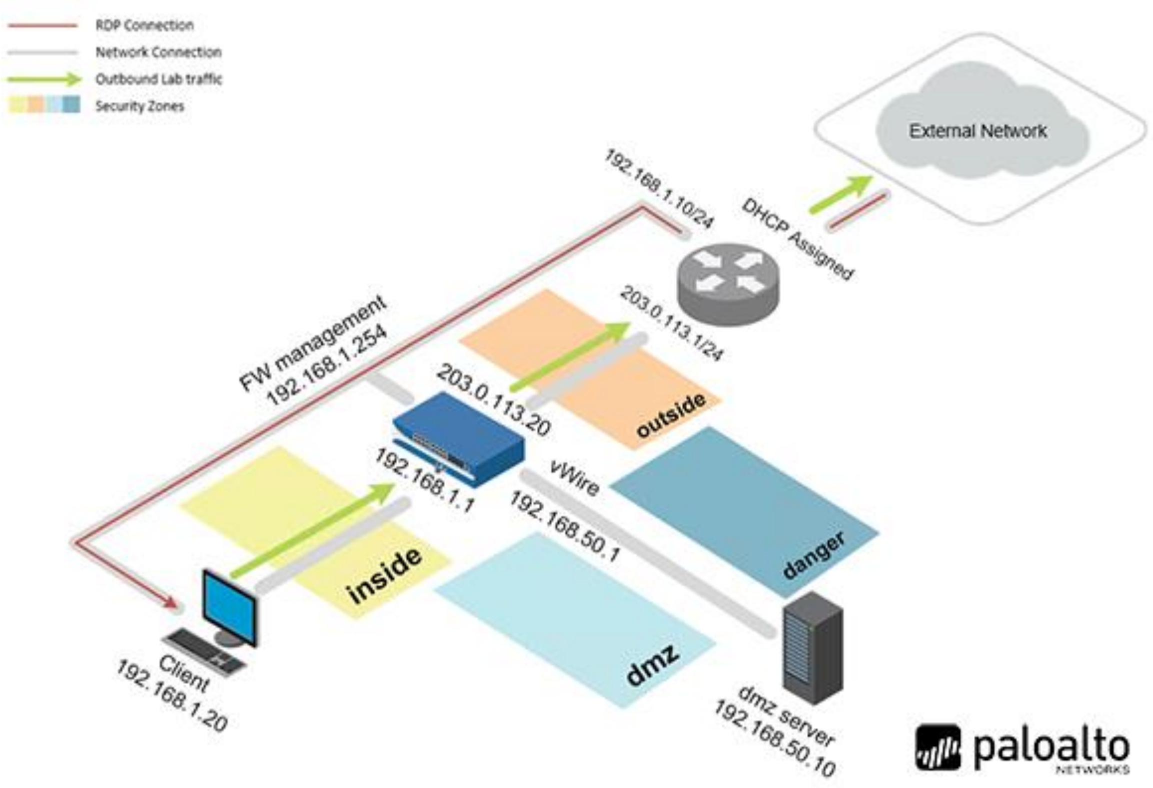
When you have the configuration in place on the firewall, you will use ping from different devices to verify connectivity between all the segments.

## Objective

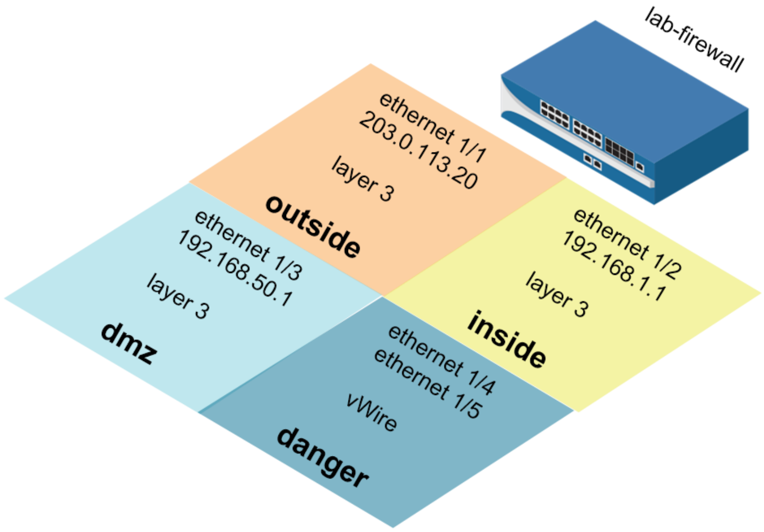
In this lab, you will perform the following tasks:

- Load a baseline configuration
- Create Layer 3 interfaces
- Create a virtual router
- Segment your production network using security zones
- Test connectivity from firewall to hosts in each security zone
- Create Interface Management Profiles

## Lab Topology



## Theoretical Lab Topology



## Lab Settings

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

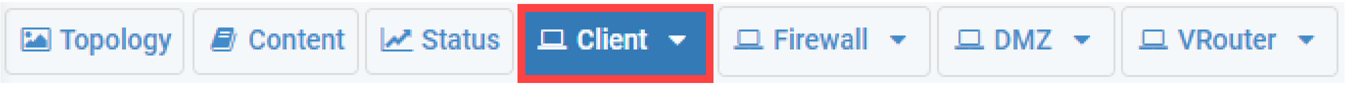
| Virtual Machine | IP Address | **Account**<br>(if needed) | **Password**<br>(if needed) |
|---|---|---|---|
| Client | 192.168.1.20 | lab-user | **Pal0Alt0!** |
| DMZ | 192.168.50.10 | root | **Pal0Alt0!** |
| Firewall | 192.168.1.254 | admin | **Pal0Alt0!** |
| VRouter | 192.168.1.10 | root | **Pal0Alt0!** |

# 4 Working with Firewall Configurations and Log Files

## 4.1 Apply a Baseline Configuration to the Firewall

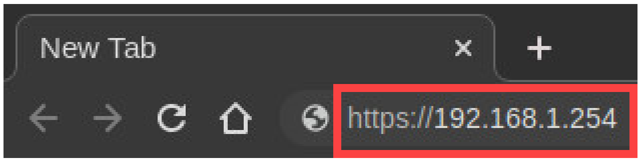
In this section, you will load the firewall configuration file.

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

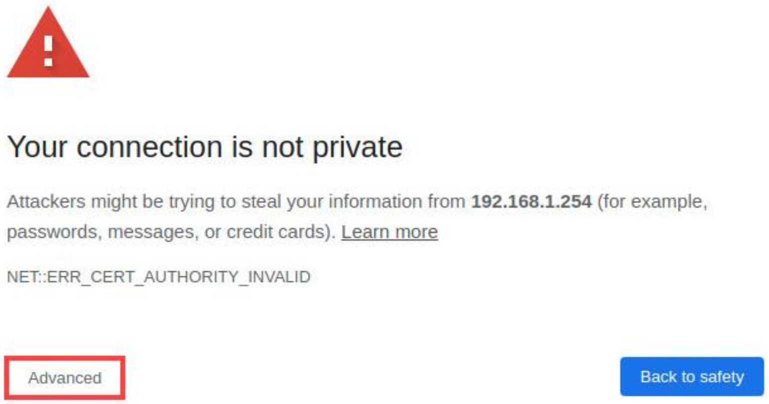


2. Double-click the **Chromium Web Browser** icon located on the *desktop*.

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



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



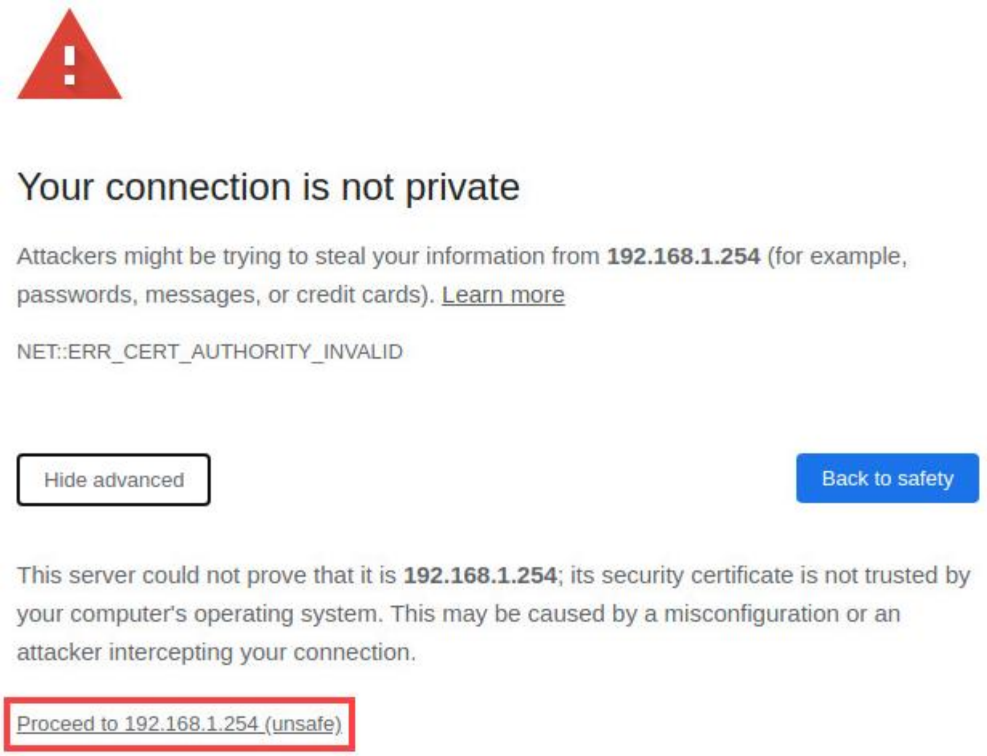
Your connection is not private

Attackers might be trying to steal your information from **192.168.1.254** (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_AUTHORITY_INVALID

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.

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



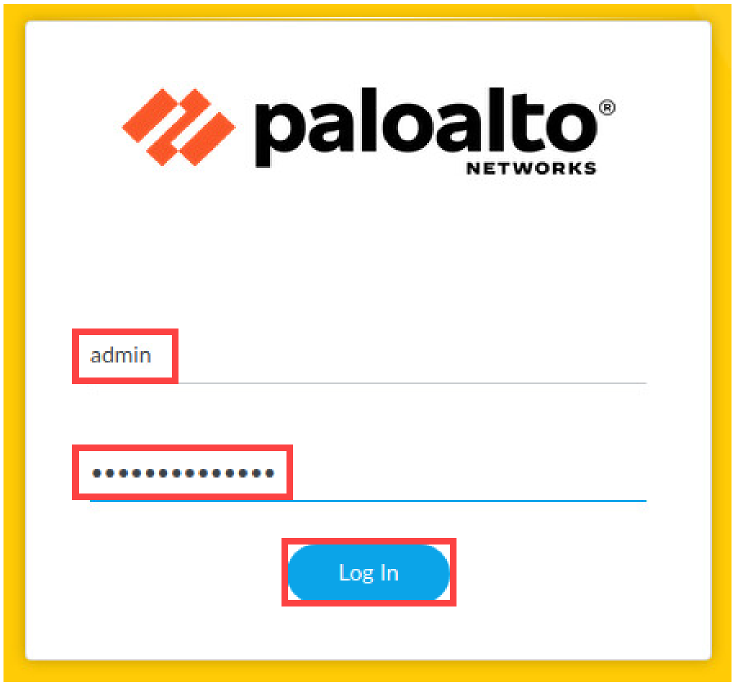
Your connection is not private

Attackers might be trying to steal your information from **192.168.1.254** (for example, passwords, messages, or credit cards). Learn more

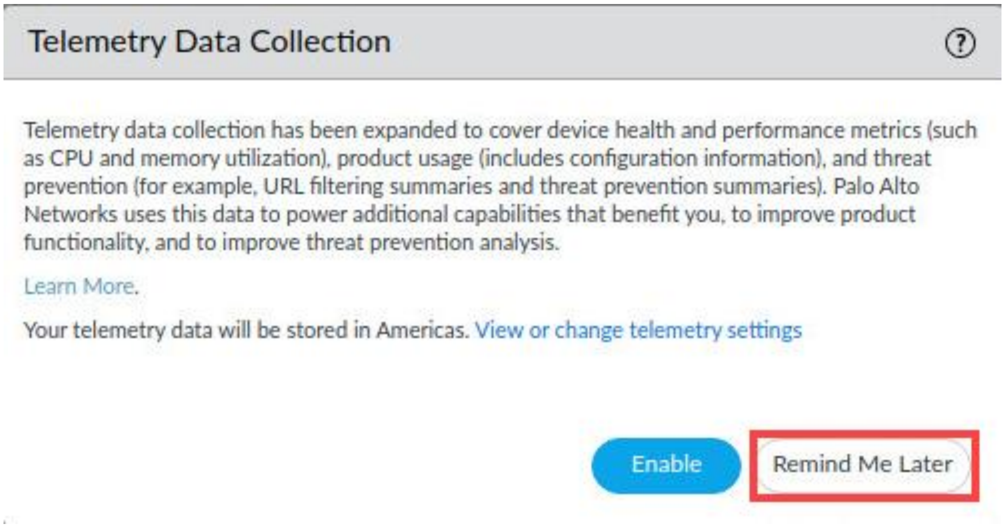
NET::ERR_CERT_AUTHORITY_INVALID

This server could not prove that it is **192.168.1.254**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

6. Log in to the firewall web interface as username **`admin`**, password **`Pal0Alt0!.`**



7. In the *Telemetry Data Collection* pop-up, click **Remind Me Later**.



Telemetry Data Collection

Telemetry data collection has been expanded to cover device health and performance metrics (such as CPU and memory utilization), product usage (includes configuration information), and threat prevention (for example, URL filtering summaries and threat prevention summaries). Palo Alto Networks uses this data to power additional capabilities that benefit you, to improve product functionality, and to improve threat prevention analysis.

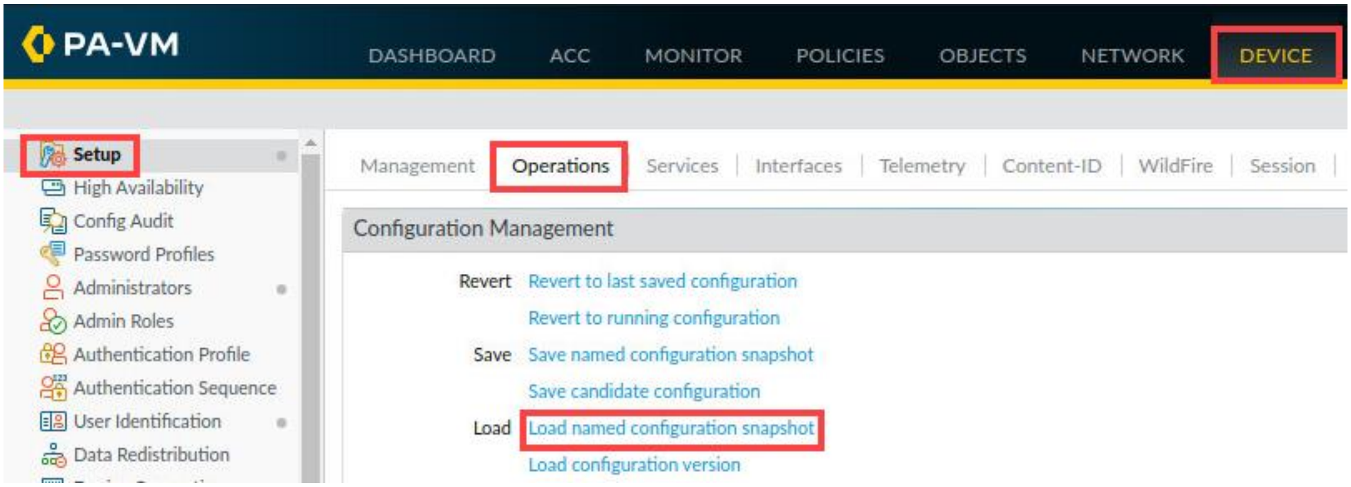
Learn More.

Your telemetry data will be stored in Americas. View or change telemetry settings

Please Note

Before you can enable Telemetry Data Collection, you would need to install a device certificate. For this lab, you will not be using Telemetry Data Collection.

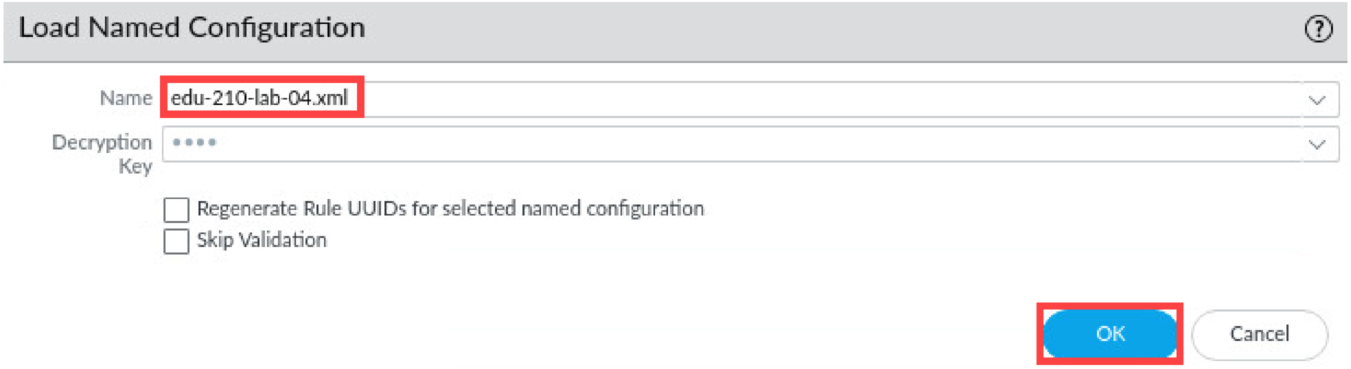
8. In the web interface, navigate to **Device > Setup > Operations** and click on **Load named configuration snapshot** underneath the *Configuration Management* section.



Configuration Management

Revert  Revert to last saved configuration
        Revert to running configuration
Save    Save named configuration snapshot
        Save candidate configuration
Load    Load named configuration snapshot
        Load configuration version

9. In the *Load Named Configuration* window, select **edu-210-lab-04.xml** from the *Name* dropdown box and click **OK**.



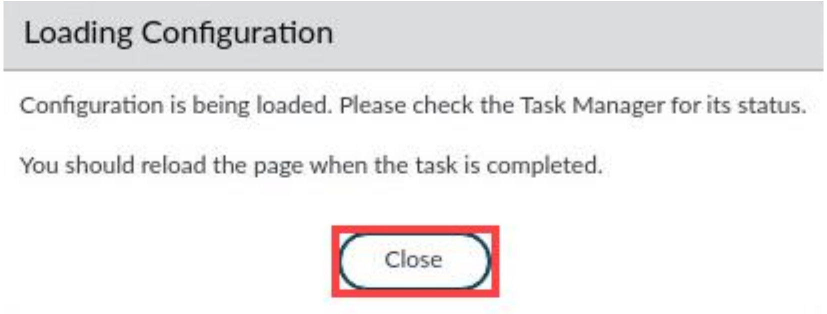
Load Named Configuration

Name: edu-210-lab-04.xml

Decryption Key: ••••

□ Regenerate Rule UUIDs for selected named configuration
□ Skip Validation

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.

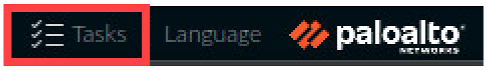


Loading Configuration

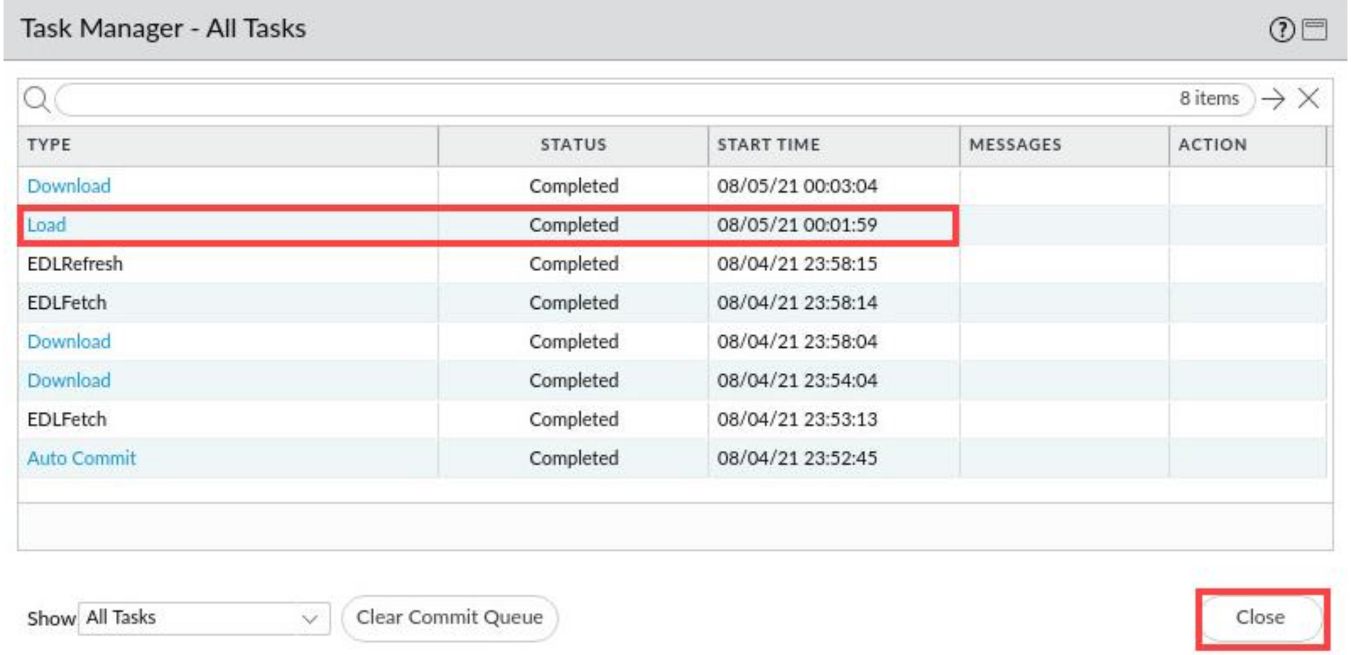
Configuration is being loaded. Please check the Task Manager for its status.

You should reload the page when the task is completed.

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**.

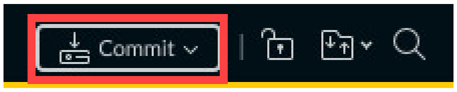


Task Manager - All Tasks

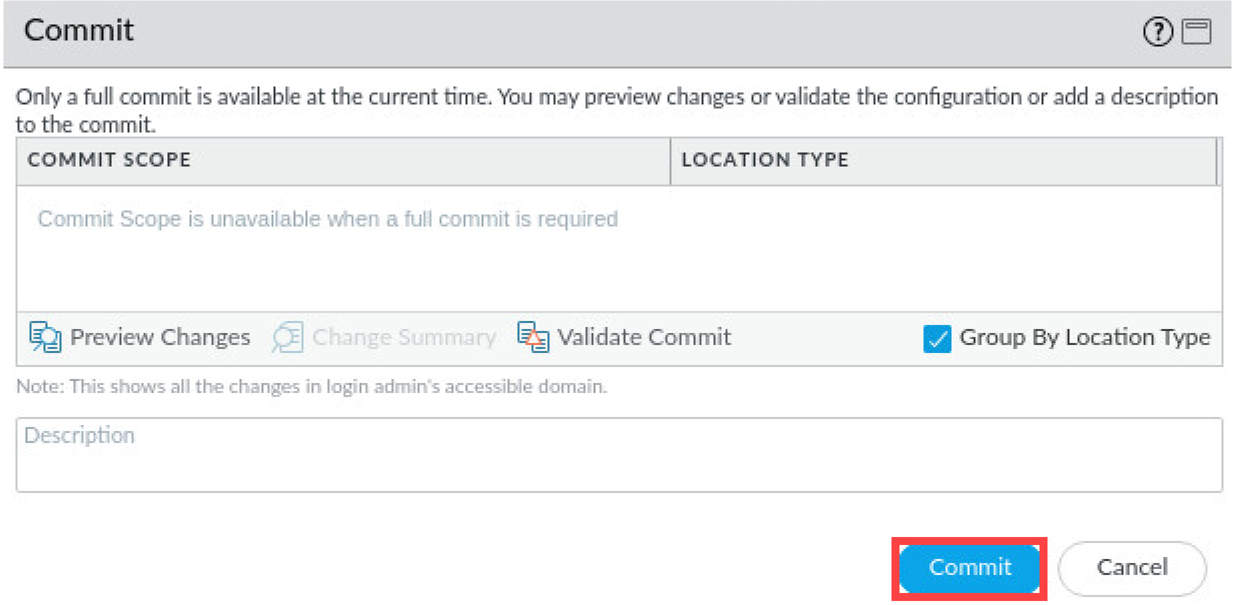
8 items

| TYPE | STATUS | START TIME | MESSAGES | ACTION |
|---|---|---|---|---|
| Download | Completed | 08/05/21 00:03:04 | | |
| Load | Completed | 08/05/21 00:01:59 | | |
| EDLRefresh | Completed | 08/04/21 23:58:15 | | |
| EDLFetch | Completed | 08/04/21 23:58:14 | | |
| Download | Completed | 08/04/21 23:58:04 | | |
| Download | Completed | 08/04/21 23:54:04 | | |
| EDLFetch | Completed | 08/04/21 23:53:13 | | |
| Auto Commit | Completed | 08/04/21 23:52:45 | | |

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.



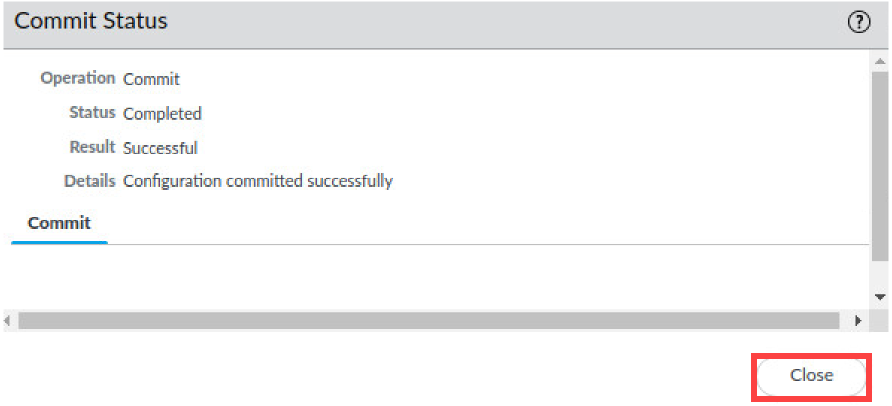
Commit

Only a full commit is available at the current time. You may preview changes or validate the configuration or add a description to the commit.

| COMMIT SCOPE | LOCATION TYPE |
|---|---|
| Commit Scope is unavailable when a full commit is required | |

Note: This shows all the changes in login admin's accessible domain.

15. When the *Commit* operation successfully completes, click **Close** to continue.



Commit Status

Operation Commit
Status Completed
Result Successful
Details Configuration committed successfully

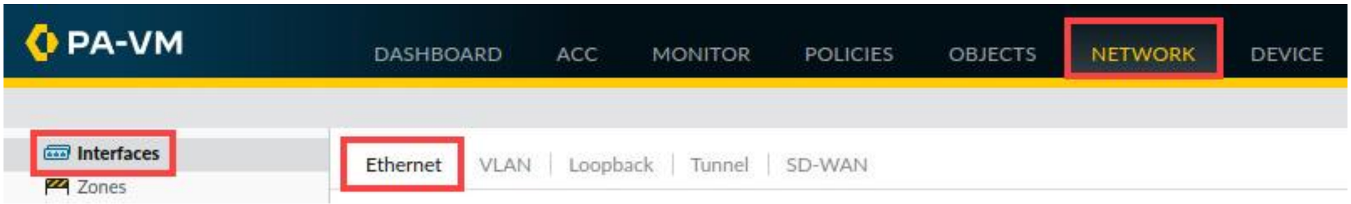
The commit process takes changes made to the Firewall and copies them to the running configuration, which will activate all configuration changes since the last commit.

16. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

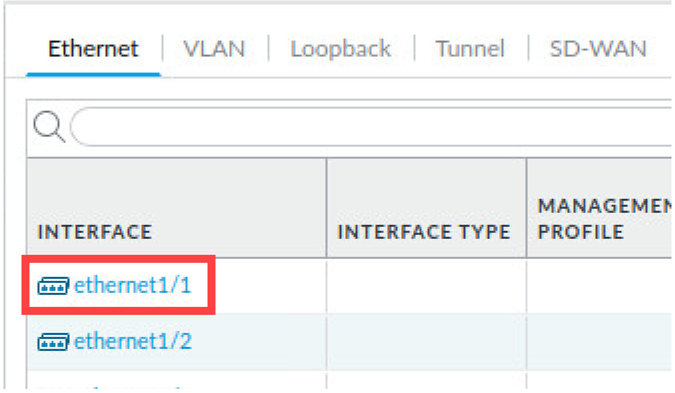
## 4.2 Create Layer 3 Network Interfaces

In this section, you will create Layer 3 interfaces on the firewall that will provide basic network connectivity to your production networks. You have a network with users (192.168.1.0/24), a network with production servers (192.168.50.0/24) and a network connecting the firewall to an upstream internet router (203.0.113.0/24).

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

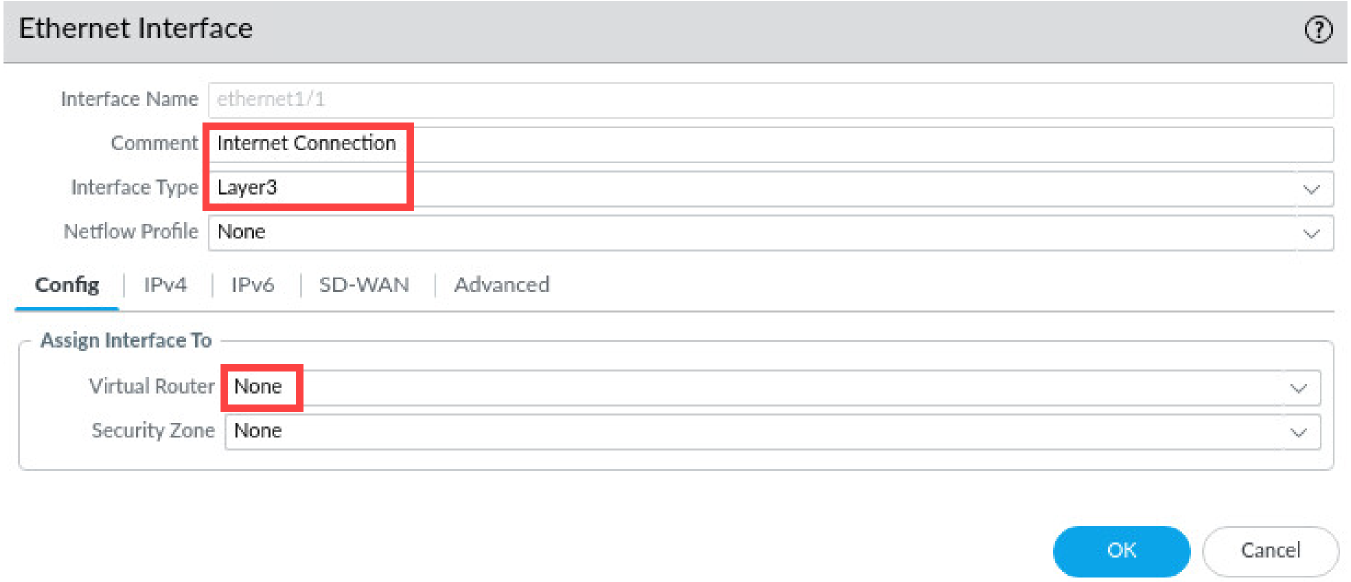


2. Click **ethernet1/1** to configure the interface.



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

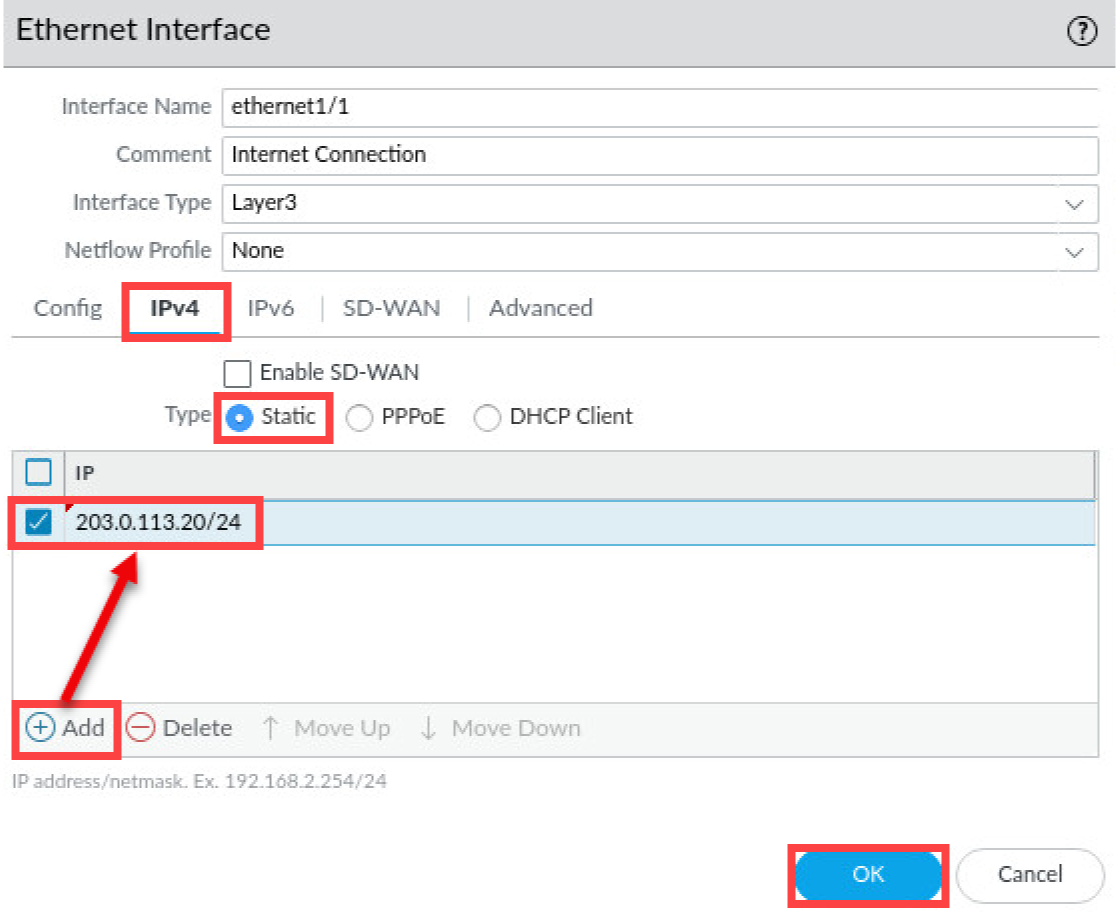
| Parameter | Value |
|---|---|
| Comment | **`Internet Connection`** |
| Interface Type | **Layer3** |
| Virtual Router | **None** |


Ethernet Interface

Interface Name: ethernet1/1
Comment: Internet Connection
Interface Type: Layer3
Netflow Profile: None

Assign Interface To
Virtual Router: None
Security Zone: None

4. Select the tab for **IPv4**. Leave the *Type* set to **Static,** Under the *IP* heading, click **Add.** Enter **`203.0.113.20/24`.** Click **OK**.



Ethernet Interface

Interface Name: ethernet1/1

Comment: Internet Connection

Interface Type: Layer3

Netflow Profile: None

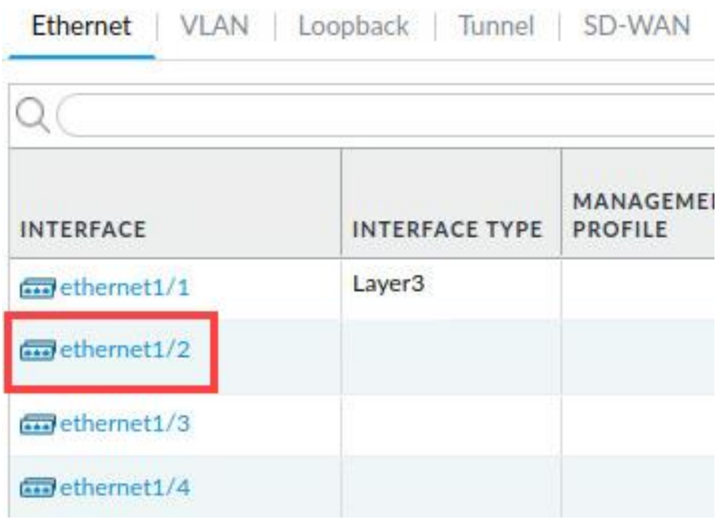
□ Enable SD-WAN

Type ● Static ○ PPPoE ○ DHCP Client

| □ | IP |
|---|---|
| ☑ | 203.0.113.20/24 |

IP address/netmask. Ex. 192.168.2.254/24

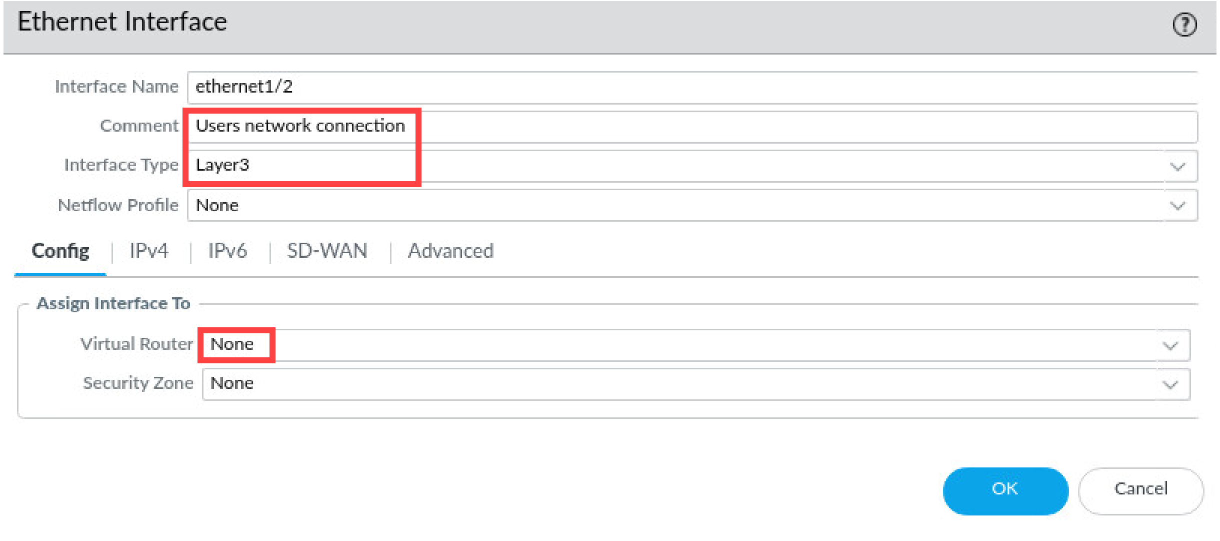
5. Click **ethernet1/2** to configure the interface.



| INTERFACE | INTERFACE TYPE | MANAGEMEI PROFILE |
|---|---|---|
| ethernet1/1 | Layer3 | |
| ethernet1/2 | | |
| ethernet1/3 | | |
| ethernet1/4 | | |

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

| Parameter | Value |
|---|---|
| Comment | `Users network connection` |
| Interface Type | **Layer3** |
| Virtual Router | **None** |



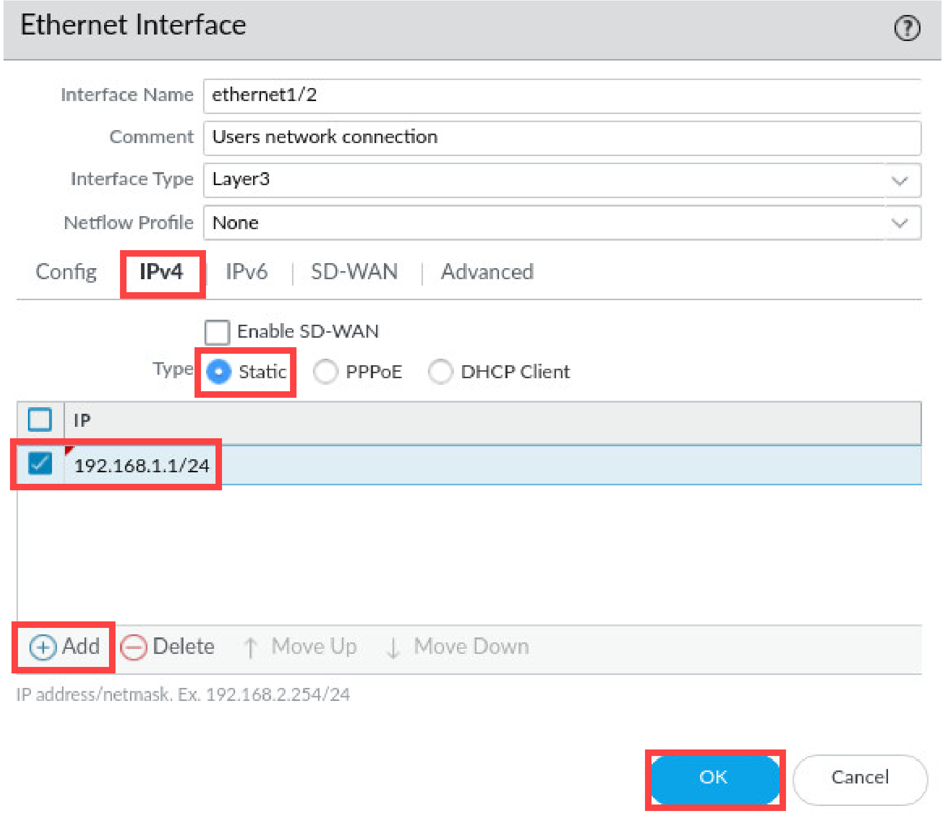
Ethernet Interface

| | |
|---|---|
| Interface Name | ethernet1/2 |
| Comment | Users network connection |
| Interface Type | Layer3 |
| Netflow Profile | None |

Assign Interface To

| | |
|---|---|
| Virtual Router | None |
| Security Zone | None |

7. Select the tab for **IPv4**. Leave the *Type* set to **Static,** Under the *IP* heading, click **Add.** Enter **`192.168.1.1/24.`** Click **OK**.



Ethernet Interface

| | |
|---|---|
| Interface Name | ethernet1/2 |
| Comment | Users network connection |
| Interface Type | Layer3 |
| Netflow Profile | None |

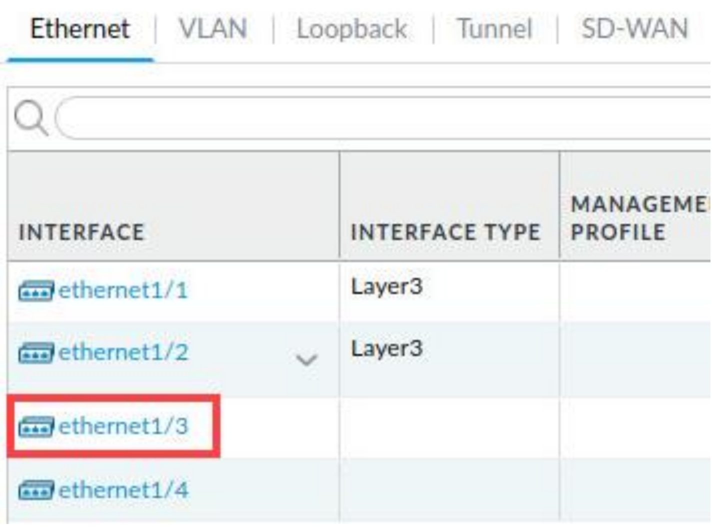
□ Enable SD-WAN

Type ● Static ○ PPPoE ○ DHCP Client

| □ | IP |
|---|---|
| ☑ | 192.168.1.1/24 |

IP address/netmask. Ex. 192.168.2.254/24

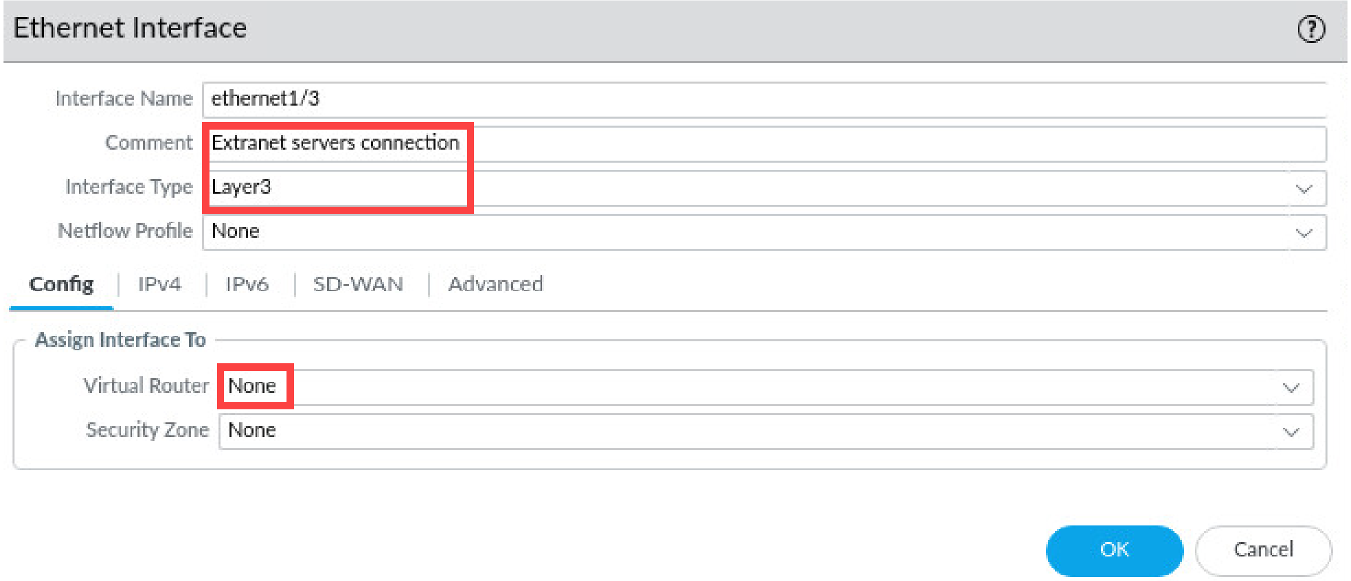
8. Click **ethernet1/3** to configure the interface.



| INTERFACE | INTERFACE TYPE | MANAGEME PROFILE |
|---|---|---|
| ethernet1/1 | Layer3 | |
| ethernet1/2 | Layer3 | |
| ethernet1/3 | | |
| ethernet1/4 | | |

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

| Parameter | Value |
|---|---|
| Comment | **`Extranet servers connection`** |
| Interface Type | **Layer3** |
| Virtual Router | **None** |


Ethernet Interface

Interface Name: ethernet1/3

Comment: Extranet servers connection

Interface Type: Layer3

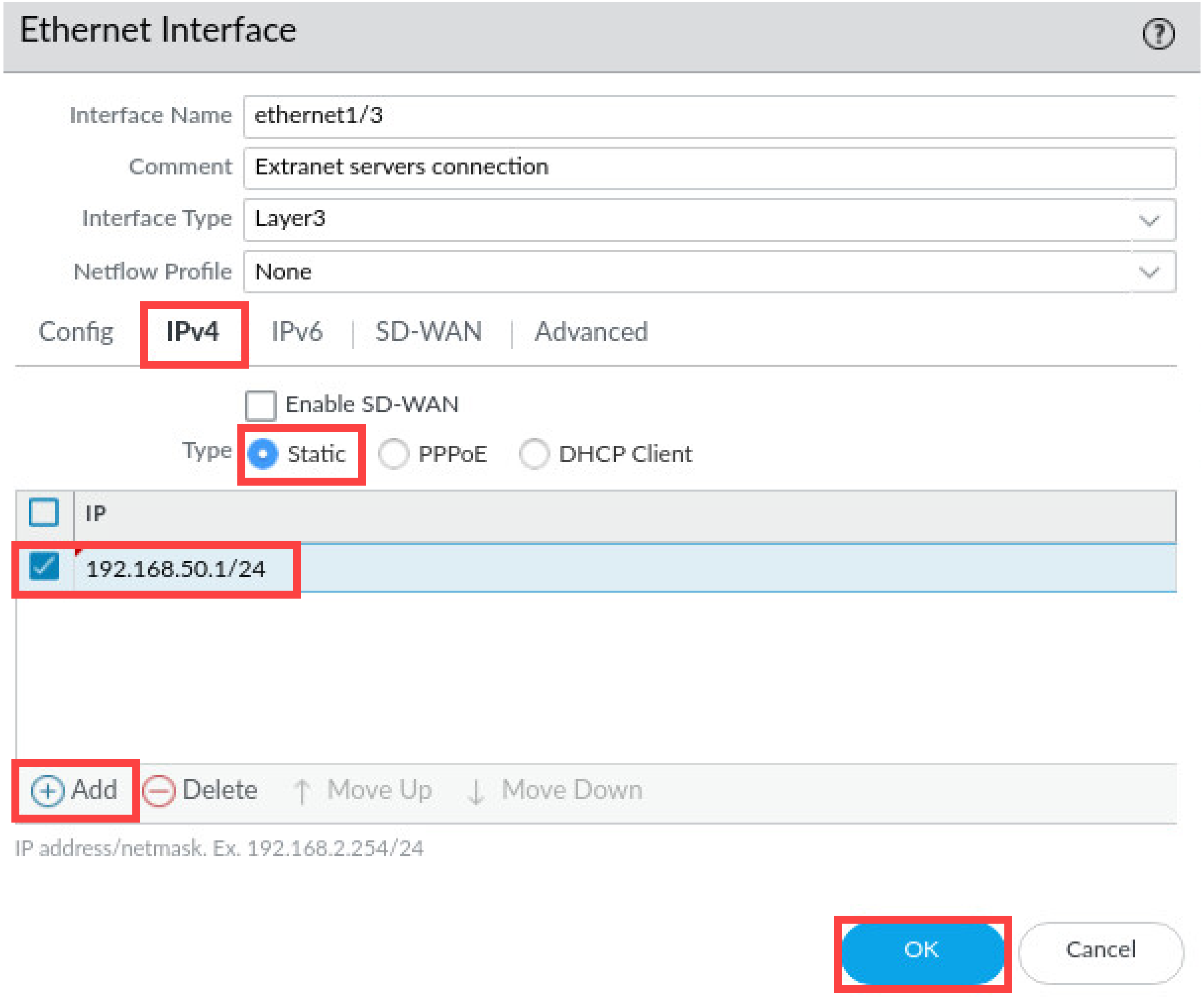
Netflow Profile: None

Assign Interface To

Virtual Router: None

Security Zone: None

10. Select the tab for **IPv4**. Leave the *Type* set to **Static,** Under the *IP* heading, click **Add.** Enter **`192.168.50.1/24`.** Click **OK**.



Ethernet Interface

| | |
|---|---|
| Interface Name | ethernet1/3 |
| Comment | Extranet servers connection |
| Interface Type | Layer3 |
| Netflow Profile | None |

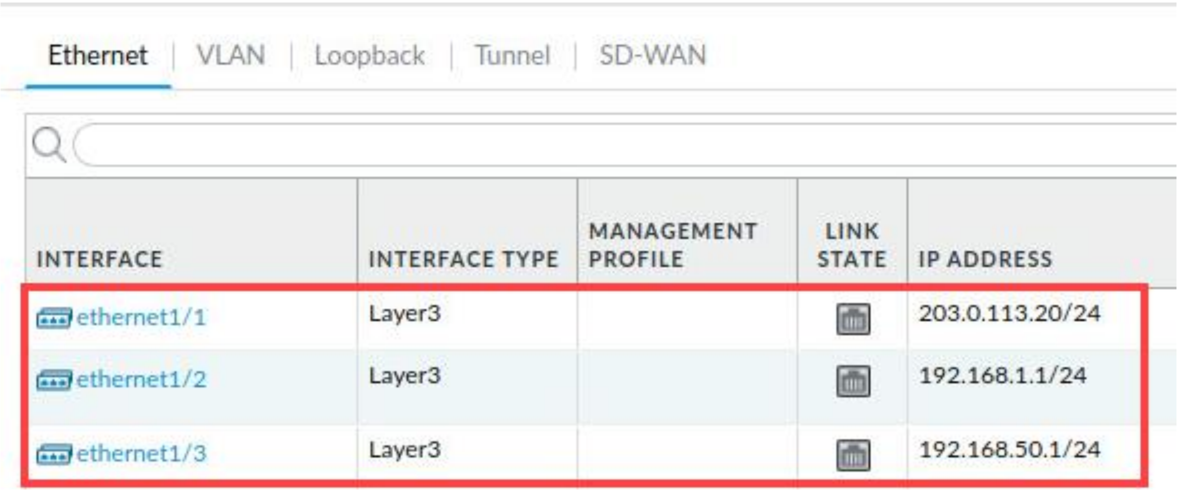
□ Enable SD-WAN

Type ● Static ○ PPPoE ○ DHCP Client

| □ | IP |
|---|---|
| ☑ | 192.168.50.1/24 |

IP address/netmask. Ex. 192.168.2.254/24

11. When complete, your *Ethernet* table will have three entries. Confirm that *Ethernets 1/1, 1/2,* and *1/3* are showing as seen below.



| INTERFACE | INTERFACE TYPE | MANAGEMENT PROFILE | LINK STATE | IP ADDRESS |
|---|---|---|---|---|
| ethernet1/1 | Layer3 | | ▥ | 203.0.113.20/24 |
| ethernet1/2 | Layer3 | | ▥ | 192.168.1.1/24 |
| ethernet1/3 | Layer3 | | ▥ | 192.168.50.1/24 |

12. Leave the web interface open and continue to the next task.

## 4.3 Create a Virtual Router

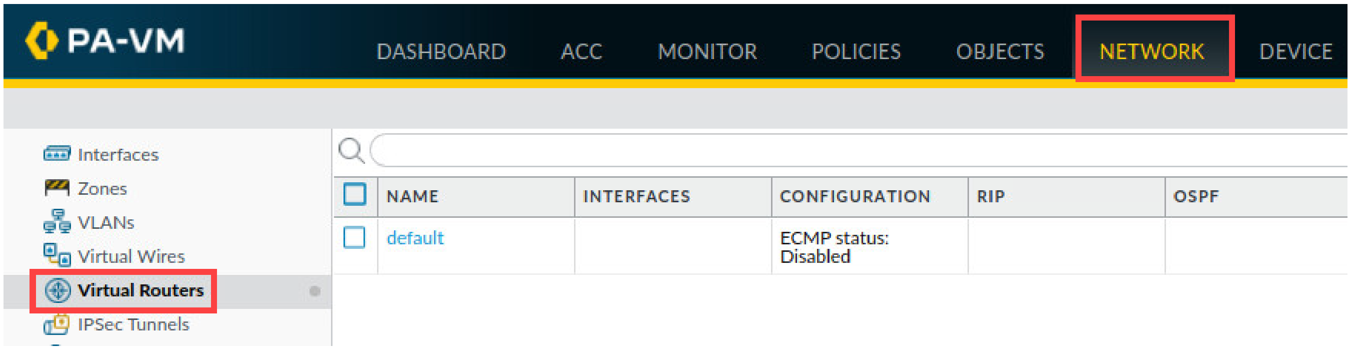
In this section, you will create a virtual router and connect your Layer 3 interfaces to it. You also will define a default gateway for the virtual router itself.

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.

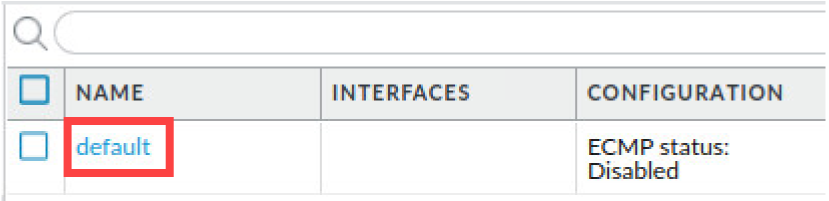
Because we are using Layer 3 interfaces, the firewall must have a way to route traffic from one network to another; this process is done with a virtual router. However, because each interface is in a different security zone, the Security rules will prevent traffic in one network from going to another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

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



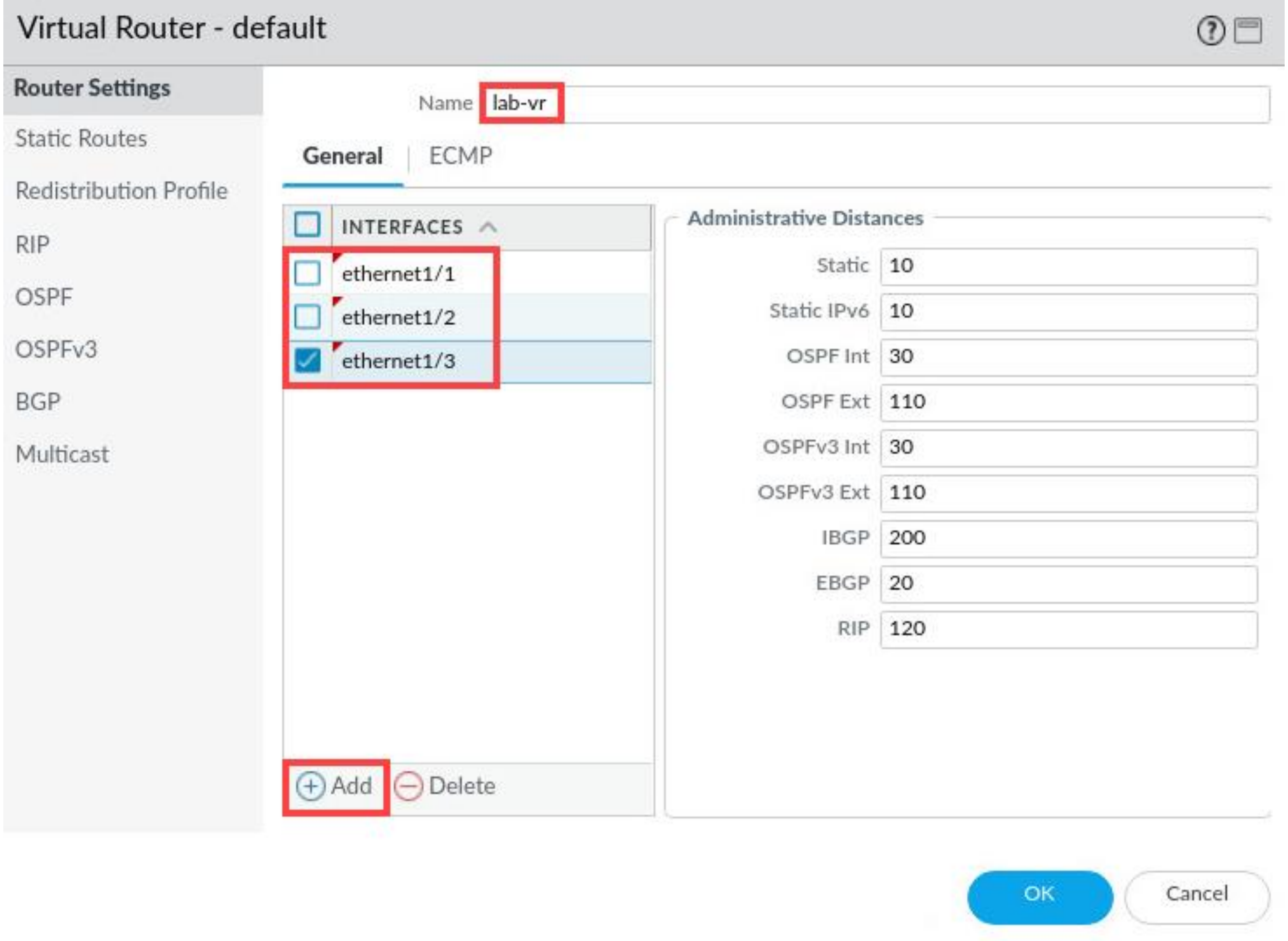
| □ | NAME | INTERFACES | CONFIGURATION | RIP | OSPF |
|---|---|---|---|---|---|
| □ | default | | ECMP status:<br>Disabled | | |

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



| □ | NAME | INTERFACES | CONFIGURATION |
|---|---|---|---|
| □ | default | | ECMP status:<br>Disabled |

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**.



Name: lab-vr

| ☐ INTERFACES |
|---|
| ☐ ethernet1/1 |
| ☐ ethernet1/2 |
| ☑ ethernet1/3 |

Administrative Distances

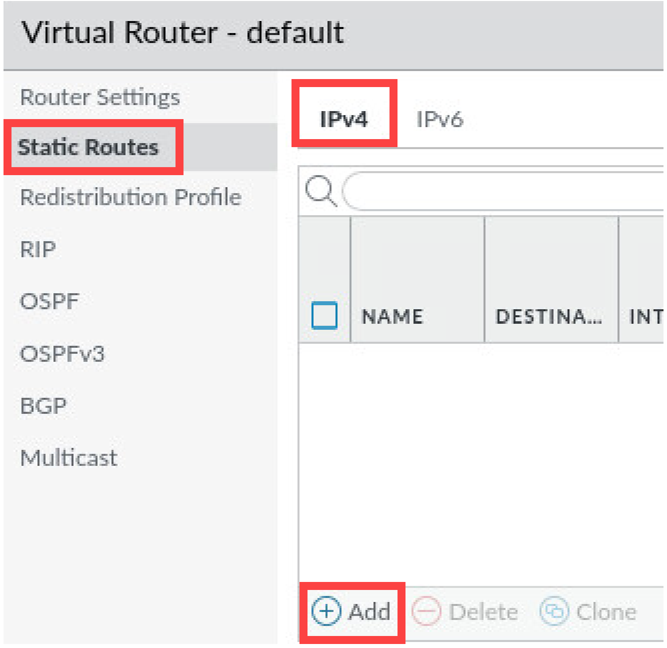
| | |
|---|---|
| Static | 10 |
| Static IPv6 | 10 |
| OSPF Int | 30 |
| OSPF Ext | 110 |
| OSPFv3 Int | 30 |
| OSPFv3 Ext | 110 |
| IBGP | 200 |
| EBGP | 20 |
| RIP | 120 |

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

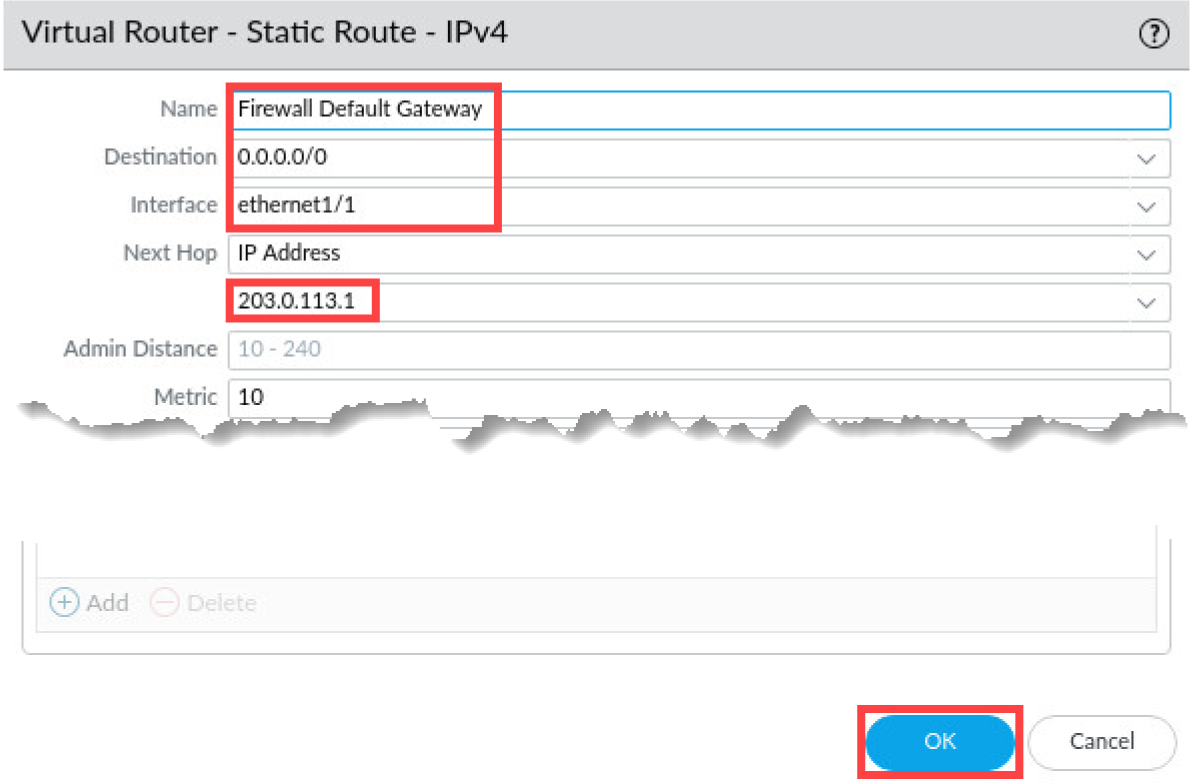
Please Note

The order in which you add these interfaces to the list is not important. You could start by adding ethernet1/3 and the result will be the same. You are simply adding the appropriate interfaces to this virtual router.

4. In the *Virtual Router - default* window, click the link on the side for **Static Routes**. Under the tab for **IPv4**, click **Add** at the bottom of the window.



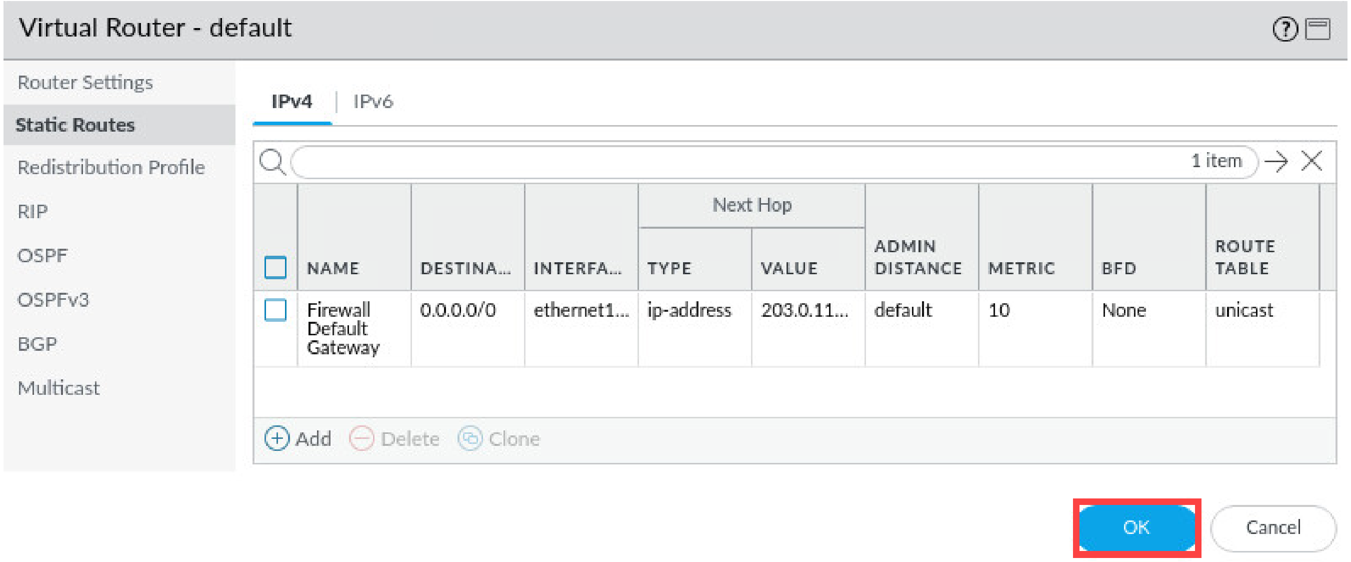
5. In the *Virtual Router – Static Route - IPv4* window, for *Name*, enter **`Firewall Default Gateway`**, for *Destination*, enter **`0.0.0.0/0`**, for *Interface*, select **ethernet1/1,** for the *Next Hop* address, enter **`203.0.113.1`**. Leave the remaining settings unchanged. Click **OK**.



| | |
|---|---|
| Name | Firewall Default Gateway |
| Destination | 0.0.0.0/0 |
| Interface | ethernet1/1 |
| Next Hop | IP Address |
| | 203.0.113.1 |
| Admin Distance | 10 - 240 |
| Metric | 10 |

This entry is the default route for the firewall. Like all other network hosts, the firewall needs a default gateway to send traffic to unknown networks. The firewall has local connections to 192.168.1.0, 192.168.50.0 and 203.0.113.0 networks, so it can forward packets to hosts on those networks directly. However, for any other destination IP addresses (such as 8.8.8.8 for DNS), this route statement instructs the firewall to forward packets to 203.0.113.1, which is the internet.

6. In the *Virtual Router – default* window, click **OK.**



| ☐ | NAME | DESTINA... | INTERFA... | Next Hop |  | ADMIN DISTANCE | METRIC | BFD | ROUTE TABLE |
|---|---|---|---|---|---|---|---|---|---|
|  |  |  |  | TYPE | VALUE |  |  |  |  |
| ☐ | Firewall Default Gateway | 0.0.0.0/0 | ethernet1... | ip-address | 203.0.11... | default | 10 | None | unicast |

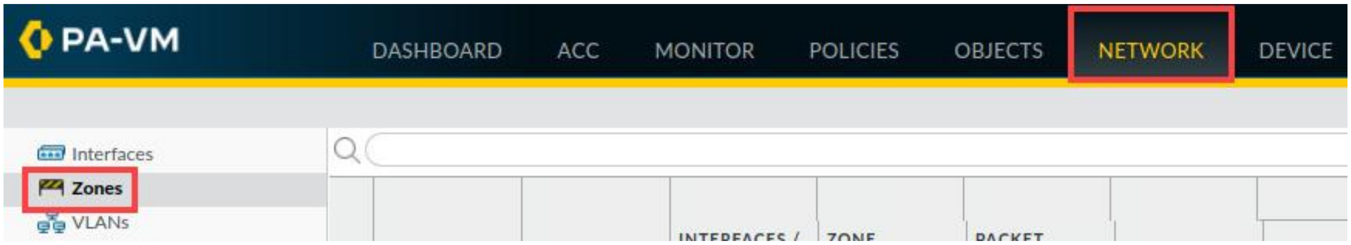
7. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

## 4.4 Segment Your Production Network Using Security Zones

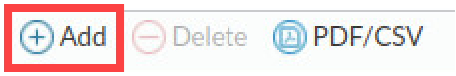
Security zones are a logical way to group physical and virtual interfaces on the firewall to control and log the traffic that traverses your network through the firewall. An interface on the firewall must be assigned to a security zone before the interface can process traffic. A zone can have multiple 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.

With your network interfaces and virtual router in place, you can now create security zones. You will create three security zones.

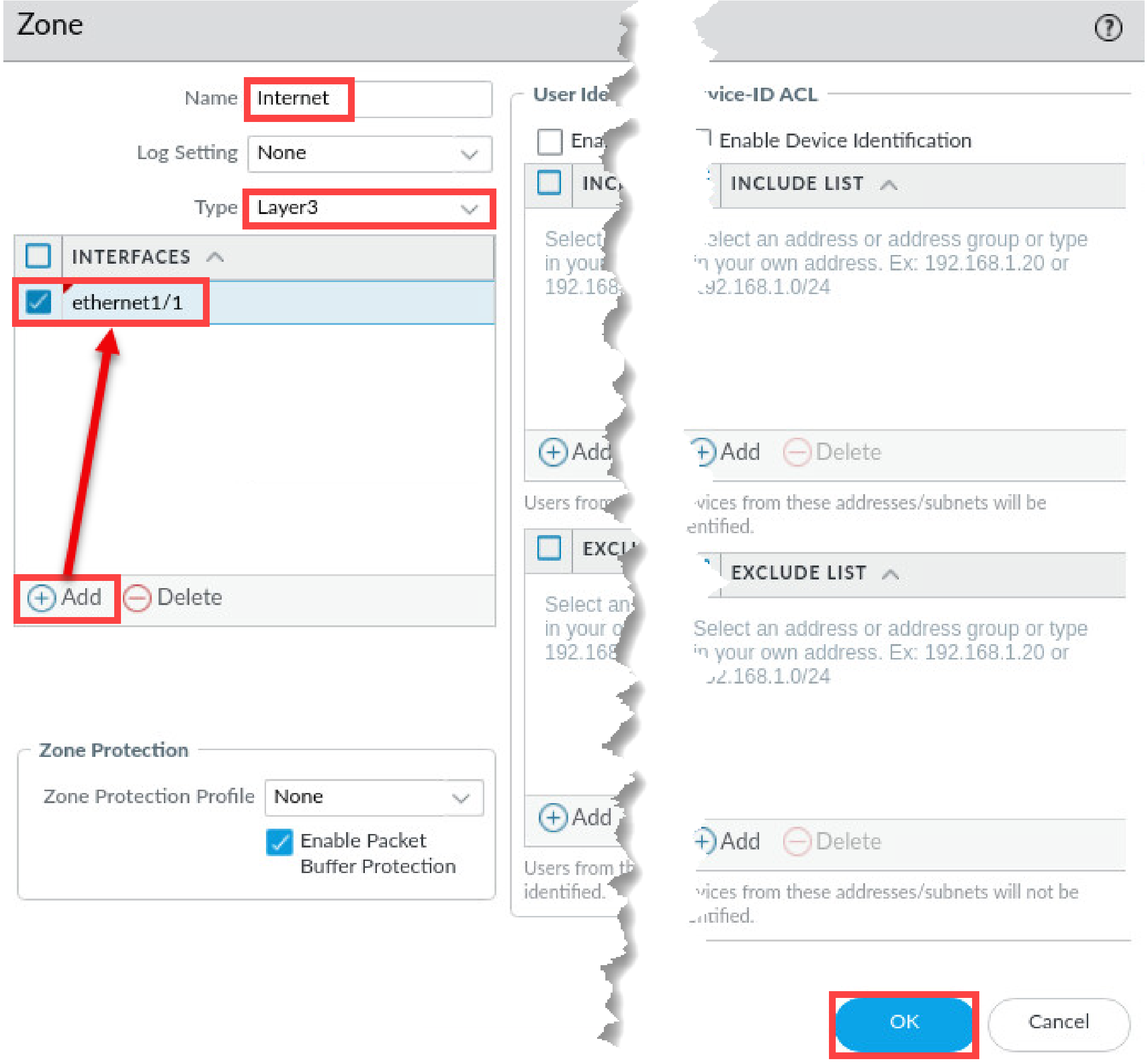
1. In the web interface, select **Network > Zones**.



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



3. In the *Zone* window, enter `Internet` for the *Name*, for *Type*, select **Layer3**. Under the *Interfaces* section, click **Add**. Select **Ethernet 1/1** and leave all other settings unchanged. Click **OK**.



Zone

Name Internet

Log Setting None

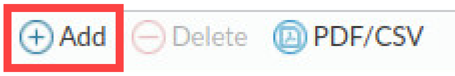
Type Layer3

☐ INTERFACES

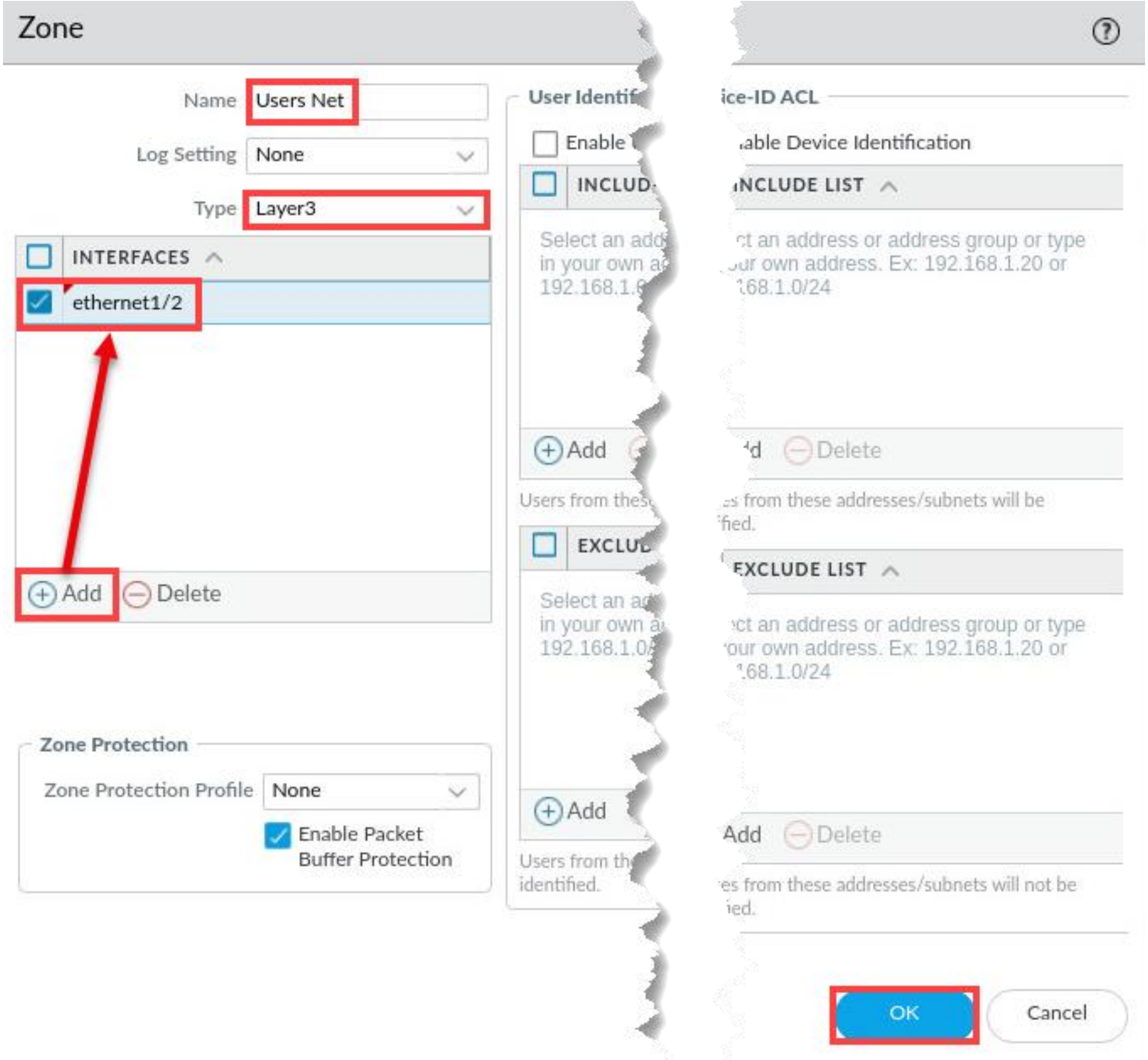
☑ ethernet1/1

Add
Delete
Zone Protection
Zone Protection Profile None
☑ Enable Packet Buffer Protection
User Ide
Ena
INC
Select
in your
192.168
Add
Users from
EXCL
Select an
in your o
192.168
Add
Users from th
identified.
vice-ID ACL
Enable Device Identification
INCLUDE LIST
elect an address or address group or type
in your own address. Ex: 192.168.1.20 or
92.168.1.0/24
Add
Delete
vices from these addresses/subnets will be
entified.
EXCLUDE LIST
Select an address or address group or type
in your own address. Ex: 192.168.1.20 or
2.168.1.0/24
Add
Delete
vices from these addresses/subnets will not be
ntified.
OK
Cancel

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



5. In the *Zone* window, enter `Users Net` for the *Name*, for *Type*, select **Layer3**. Under the *Interfaces* section, click **Add**. Select **Ethernet 1/2** and leave all other settings unchanged. Click **OK**.


Zone

Name: Users Net

Log Setting: None

Type: Layer3

□ INTERFACES

☑ ethernet1/2

Zone Protection

Zone Protection Profile: None

☑ Enable Packet Buffer Protection

User Identif… ice-ID ACL

□ Enable … able Device Identification

□ INCLUD… INCLUDE LIST

Select an add… ct an address or address group or type in your own a… our own address. Ex: 192.168.1.20 or 192.168.1.0… 168.1.0/24

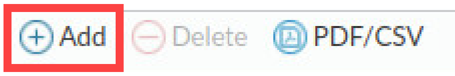
Users from thes… es from these addresses/subnets will be … fied.

□ EXCLUD… EXCLUDE LIST

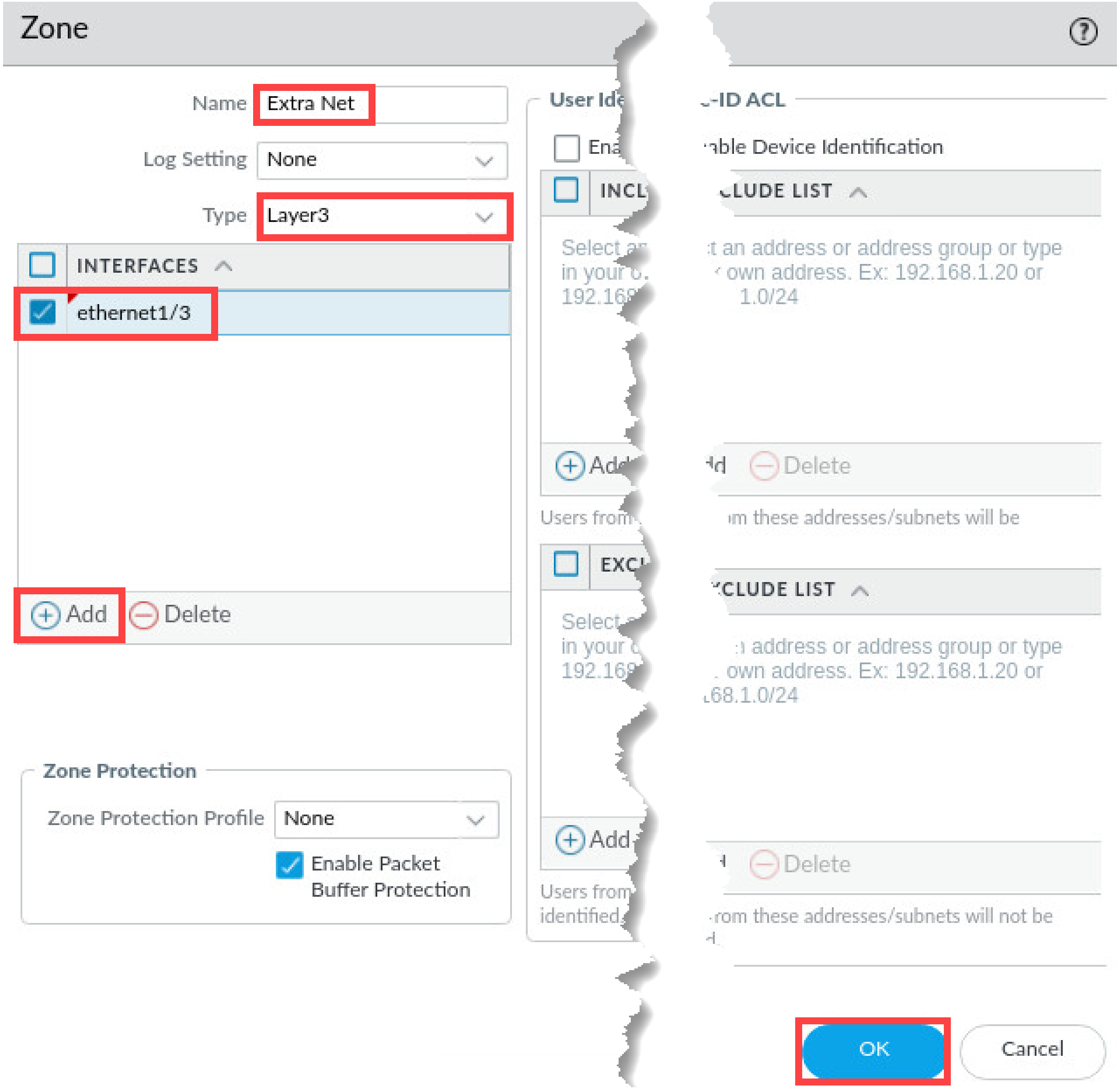
Select an ad… ct an address or address group or type in your own a… our own address. Ex: 192.168.1.20 or 192.168.1.0/… 168.1.0/24

Users from th… es from these addresses/subnets will not be identified. … ied.

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



7. In the *Zone* window, enter `Extra Net` for the *Name*, for *Type*, select **Layer3**. Under the *Interfaces* section, click **Add**. Select **Ethernet 1/3** and leave all other settings unchanged. Click **OK**.



Zone

Name: Extra Net

Log Setting: None

Type: Layer3

☐ INTERFACES

☑ ethernet1/3

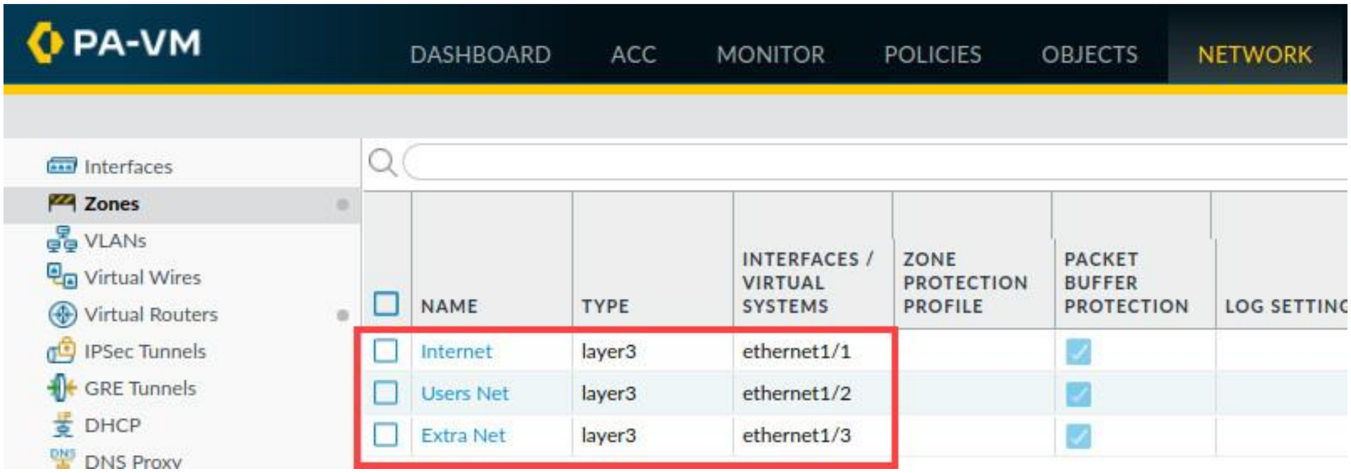
Zone Protection

Zone Protection Profile: None

☑ Enable Packet Buffer Protection

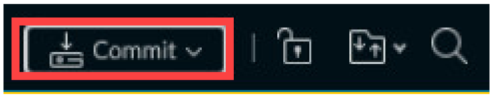
?
Add
Delete
User Ide
-ID ACL
☐ Ena
able Device Identification
☐ INCL
LUDE LIST
Select an
t an address or address group or type
in your o
own address. Ex: 192.168.1.20 or
192.168
1.0/24
Add
Delete
Users from
m these addresses/subnets will be
☐ EXC
CLUDE LIST
Select a
address or address group or type
in your o
own address. Ex: 192.168.1.20 or
192.168
68.1.0/24
Add
Delete
Users from
identified
rom these addresses/subnets will not be
OK
Cancel

8. You should now have three security zones.

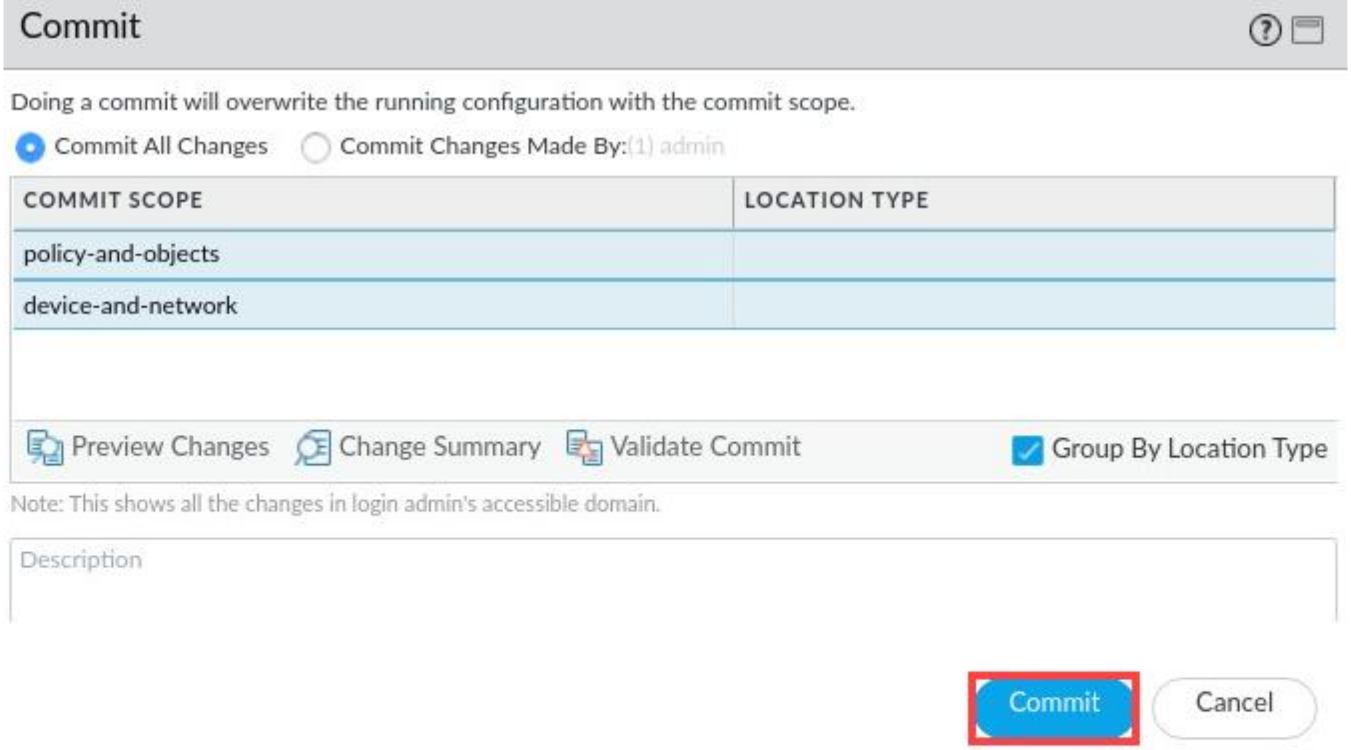


| □ | NAME | TYPE | INTERFACES / VIRTUAL SYSTEMS | ZONE PROTECTION PROFILE | PACKET BUFFER PROTECTION | LOG SETTING |
|---|---|---|---|---|---|---|
| □ | Internet | layer3 | ethernet1/1 | | ☑ | |
| □ | Users Net | layer3 | ethernet1/2 | | ☑ | |
| □ | Extra Net | layer3 | ethernet1/3 | | ☑ | |

9. Click the **Commit** button at the upper right of the *PA-VM* web interface.



10. In the *Commit* window, click **Commit**.



Doing a commit will overwrite the running configuration with the commit scope.

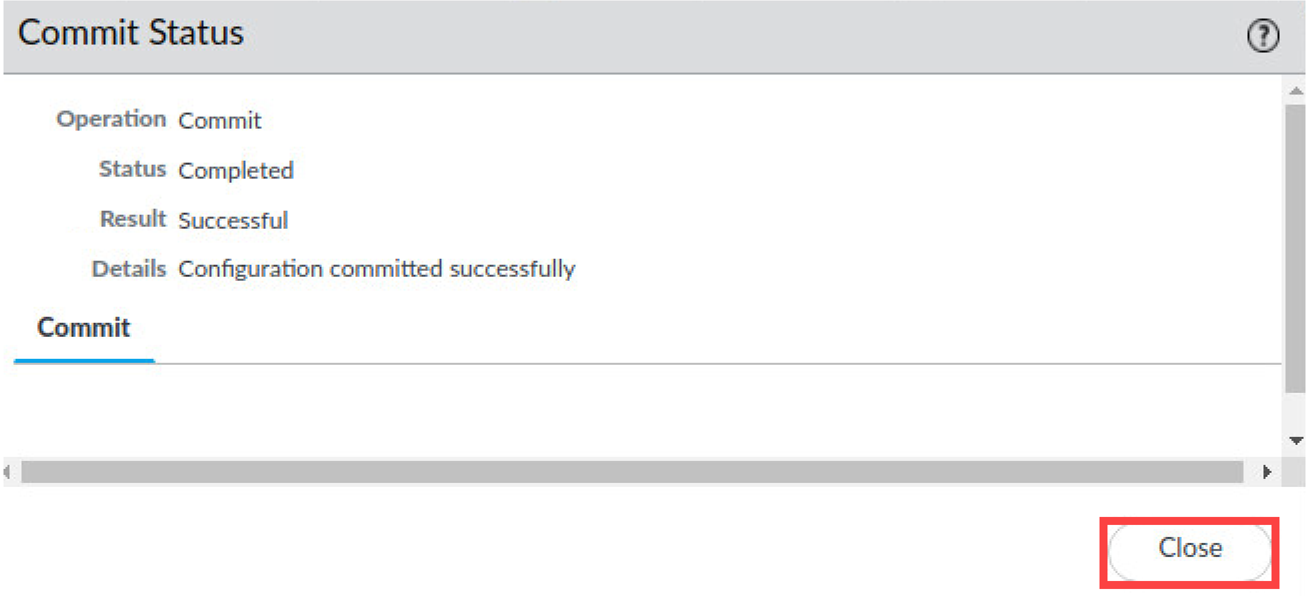
● Commit All Changes ○ Commit Changes Made By:(1) admin

| COMMIT SCOPE | LOCATION TYPE |
|---|---|
| policy-and-objects | |
| device-and-network | |

☑ Group By Location Type

Note: This shows all the changes in login admin's accessible domain.

11. In the *Commit Status* window, click **Close**.



Commit Status

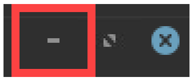
Operation Commit

Status Completed

Result Successful

Details Configuration committed successfully

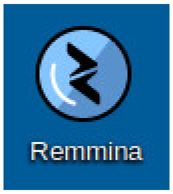
12. Minimize the *PA-VM* firewall by clicking the **minimize** icon in the upper right of the web interface and continue to the next task.



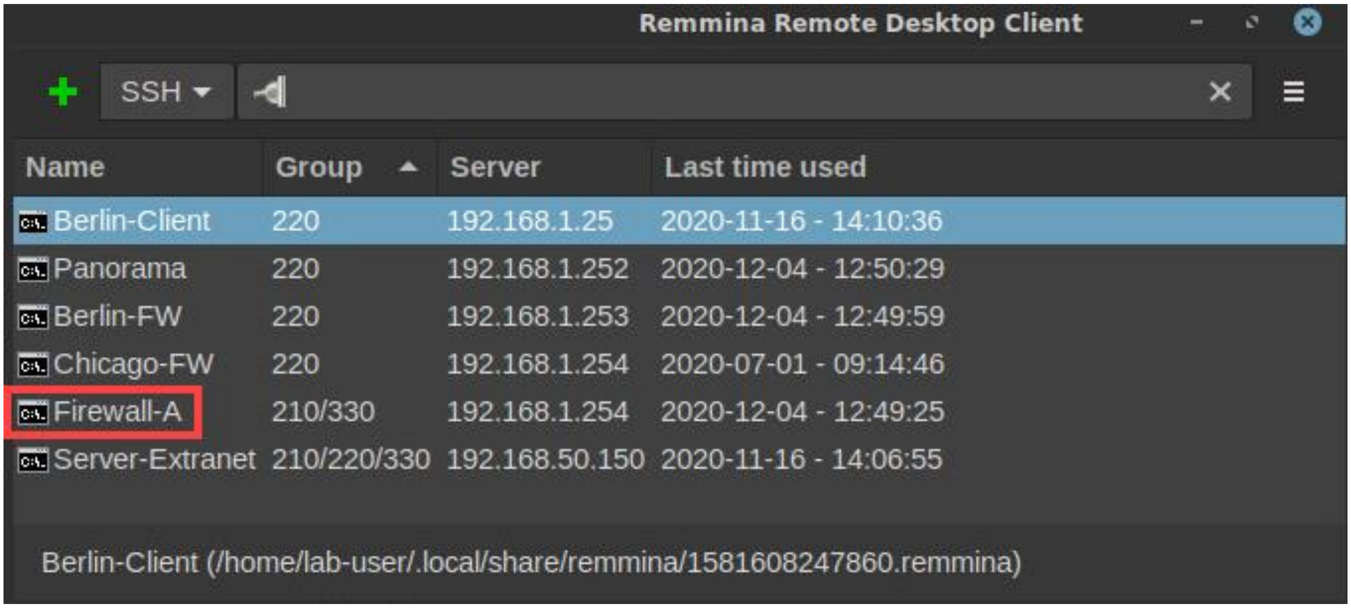
## 4.5 Test Connectivity to Each Zone

In this section, you will verify network connectivity from the firewall to hosts in each zone. You will use an SSH connection and ping hosts on each network.

1. On the *client desktop*, open the **Remmina** application.



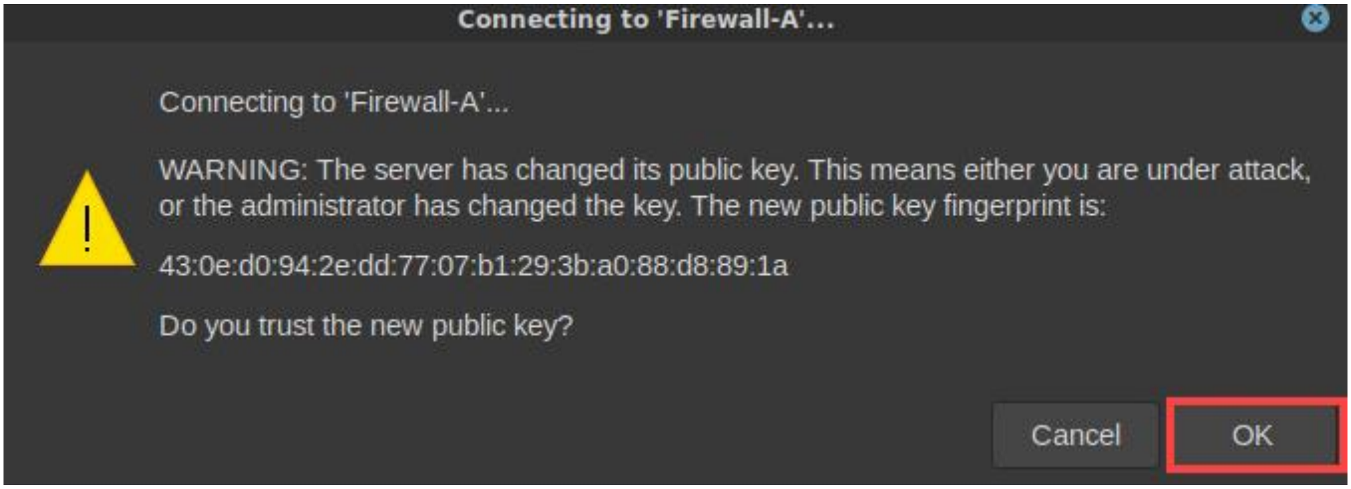
2. Double-click the entry for **Firewall-A.**



| Name | Group | Server | Last time used |
|---|---|---|---|
| Berlin-Client | 220 | 192.168.1.25 | 2020-11-16 - 14:10:36 |
| Panorama | 220 | 192.168.1.252 | 2020-12-04 - 12:50:29 |
| Berlin-FW | 220 | 192.168.1.253 | 2020-12-04 - 12:49:59 |
| Chicago-FW | 220 | 192.168.1.254 | 2020-07-01 - 09:14:46 |
| Firewall-A | 210/330 | 192.168.1.254 | 2020-12-04 - 12:49:25 |
| Server-Extranet | 210/220/330 | 192.168.50.150 | 2020-11-16 - 14:06:55 |

Berlin-Client (/home/lab-user/.local/share/remmina/1581608247860.remmina)

3. If you are presented the *Connecting to 'Firewall-A'…* window, click **OK**.



Connecting to 'Firewall-A'...

WARNING: The server has changed its public key. This means either you are under attack, or the administrator has changed the key. The new public key fingerprint is:

43:0e:d0:94:2e:dd:77:07:b1:29:3b:a0:88:d8:89:1a

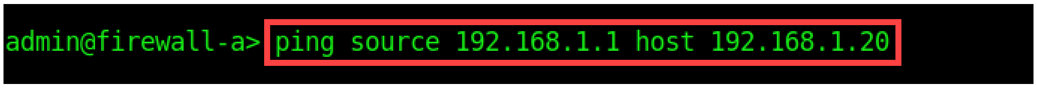
Do you trust the new public key?

**Please Note**

The Firewall-A connection in Remmina has been pre-configured to provide login credentials to the firewall so that you do not have to log in each time. This is for convenience in the lab only.

4. In the CLI connection to the firewall, use the **ping** command to check network connectivity to a host in the *User_Net Security Zone* by using the following command at the **admin@firewall-a>** prompt.

```
admin@firewall-a> ping source 192.168.1.1 host 192.168.1.20
```

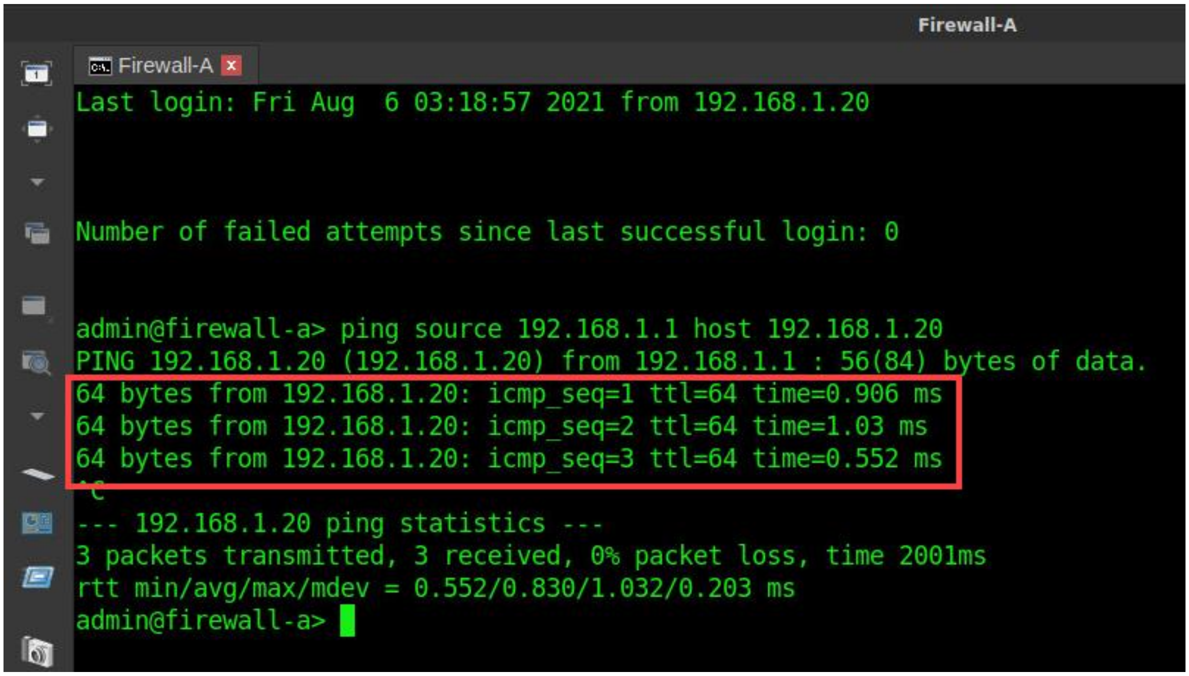


```
admin@firewall-a> ping source 192.168.1.1 host 192.168.1.20
```

Please Note

Note the syntax for this command. 192.168.1.1 is the IP address of ethernet1/2 on the firewall. The command instructs the firewall to use that IP address on ethernet1/2 to ping the host 192.168.1.20. If you do not use the source option, the firewall uses its management interface address as the source IP.

5. Allow the *ping* to continue for three or four seconds and then use **Ctrl+C** to interrupt the command. Notice the *pings* are successful.



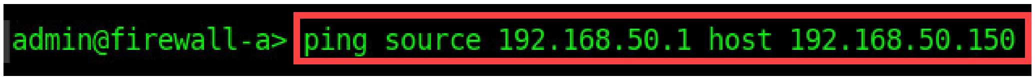
```
Last login: Fri Aug  6 03:18:57 2021 from 192.168.1.20


Number of failed attempts since last successful login: 0


admin@firewall-a> ping source 192.168.1.1 host 192.168.1.20
PING 192.168.1.20 (192.168.1.20) from 192.168.1.1 : 56(84) bytes of data.
64 bytes from 192.168.1.20: icmp_seq=1 ttl=64 time=0.906 ms
64 bytes from 192.168.1.20: icmp_seq=2 ttl=64 time=1.03 ms
64 bytes from 192.168.1.20: icmp_seq=3 ttl=64 time=0.552 ms
^C
--- 192.168.1.20 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2001ms
rtt min/avg/max/mdev = 0.552/0.830/1.032/0.203 ms
admin@firewall-a>
```

6. Use the *ping* command to check connectivity to a host in the Extranet zone by using the following command at the **admin@firewall-a>** prompt.

```
admin@firewall-a> ping source 192.168.50.1 host 192.168.50.150
```

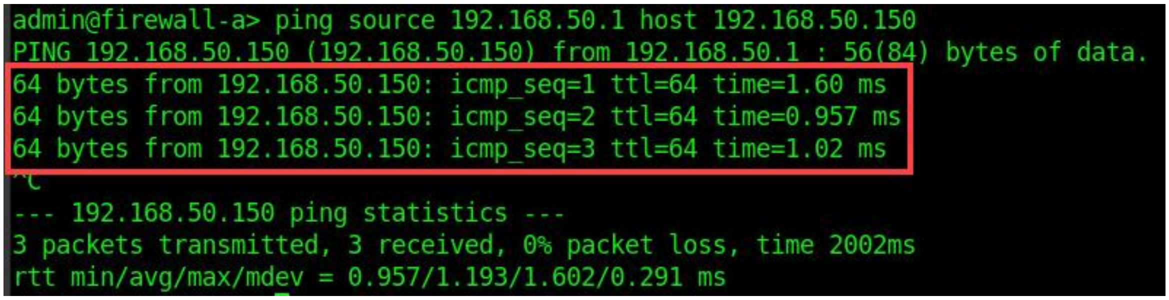


```
admin@firewall-a> ping source 192.168.50.1 host 192.168.50.150
```

**Please Note**

192.168.50.1 is the IP address on ethernet1/3 which is assigned to the Extranet security zone. 192.168.50.150 is a server in the Extranet zone.

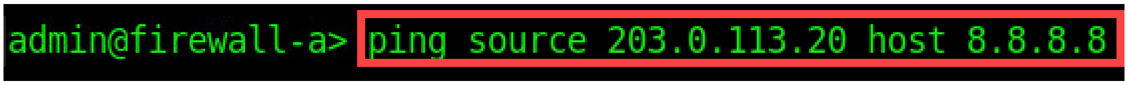
7. Allow the *ping* to continue for three or four seconds and then use **Ctrl+C** to interrupt the command. Notice the *pings* are successful.



```
admin@firewall-a> ping source 192.168.50.1 host 192.168.50.150
PING 192.168.50.150 (192.168.50.150) from 192.168.50.1 : 56(84) bytes of data.
64 bytes from 192.168.50.150: icmp_seq=1 ttl=64 time=1.60 ms
64 bytes from 192.168.50.150: icmp_seq=2 ttl=64 time=0.957 ms
64 bytes from 192.168.50.150: icmp_seq=3 ttl=64 time=1.02 ms
^C
--- 192.168.50.150 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 0.957/1.193/1.602/0.291 ms
```

8. Use the *ping* command to check connectivity to a host on the Internet by using the following command at the **admin@firewall-a>** prompt.

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

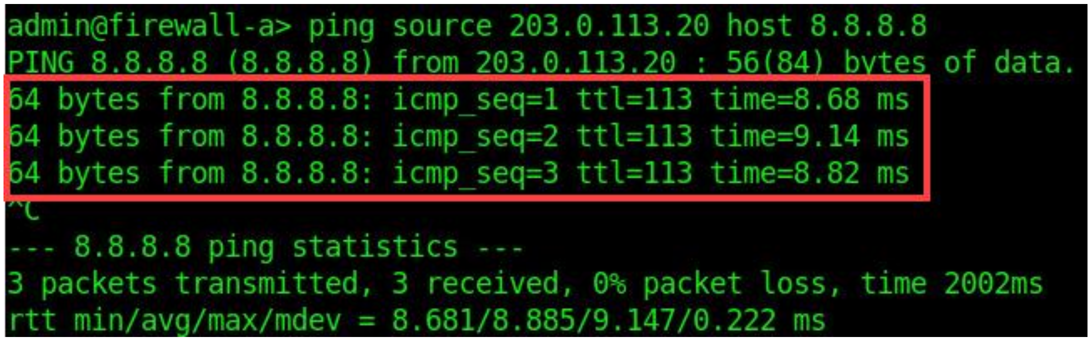


```
admin@firewall-a> ping source 203.0.113.20 host 8.8.8.8
```

**Please Note**

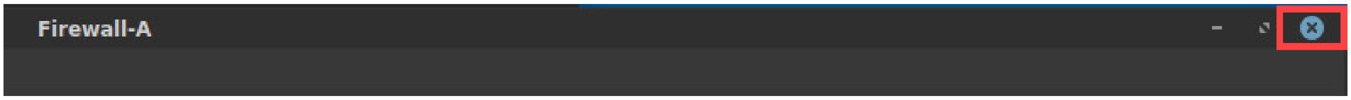
203.0.113.20 is the IP address on ethernet1/1 which is assigned to the Internet security zone. 8.8.8.8 is a DNS server on the Internet zone.

9. Allow the *ping* to continue for three or four seconds and then use **Ctrl+C** to interrupt the command. Notice the *pings* are successful.

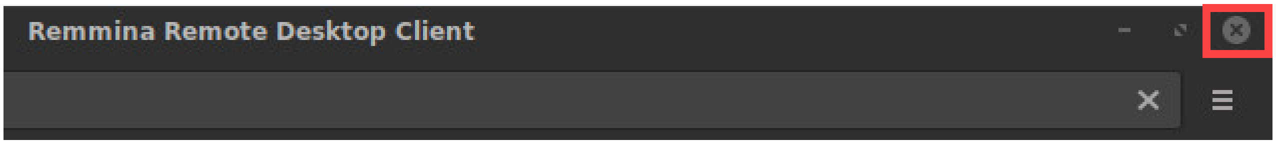


```
admin@firewall-a> ping source 203.0.113.20 host 8.8.8.8
PING 8.8.8.8 (8.8.8.8) from 203.0.113.20 : 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=113 time=8.68 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=113 time=9.14 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=113 time=8.82 ms
^C
--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 8.681/8.885/9.147/0.222 ms
```

10. Close the *Firewall-A Remmina* terminal console by clicking on the **close** icon in the upper-right.



11. Close the *Remmina Remote Desktop Client* by clicking on the **close** icon in the upper-right.



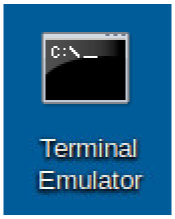
12. Stay on the *client desktop* and continue to the next task.

## 4.6 Test Interface Access before Management Profiles

Management interface profiles allow you to enable specific network services on individual firewall interfaces.

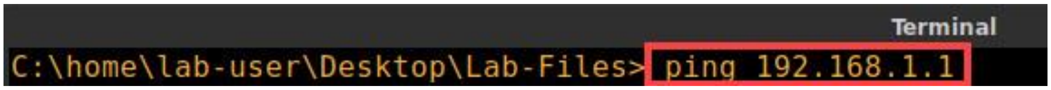
To illustrate the default behavior of firewall interfaces, you will ping 192.168.1.1 from the client workstation. You will also attempt to access the firewall CLI by SSH through 192.168.1.1. Without any Interface Management Profiles in place, both ping and SSH will fail.

1. Open the **Terminal Emulator** on the *client desktop*.



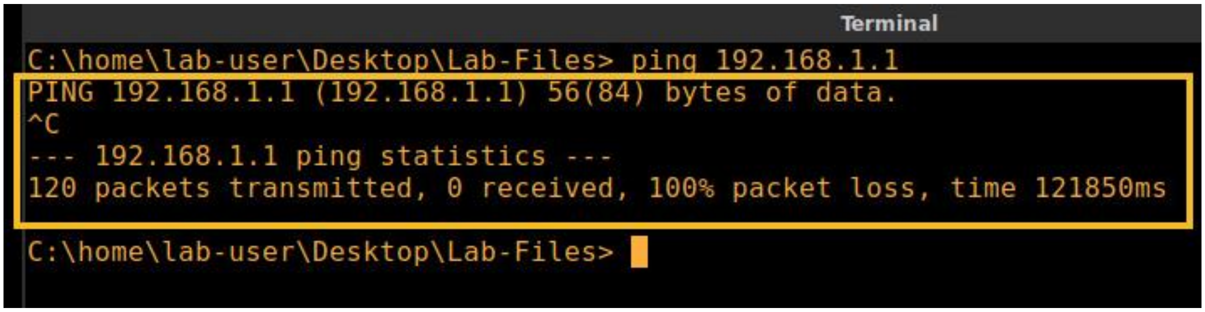
2. Issue the following command below.

```
C:\home\lab-user\Desktop\Lab-Files> ping 192.168.1.1 <Enter>
```



```
Terminal
C:\home\lab-user\Desktop\Lab-Files> ping 192.168.1.1
```

3. Wait a few seconds and use **Ctrl+C** to stop the command. You will not get a response because *Management profiles* have not been configured.

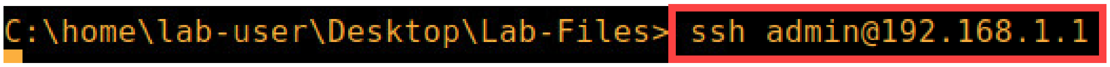


```
Terminal
C:\home\lab-user\Desktop\Lab-Files> ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
^C
--- 192.168.1.1 ping statistics ---
120 packets transmitted, 0 received, 100% packet loss, time 121850ms

C:\home\lab-user\Desktop\Lab-Files>
```

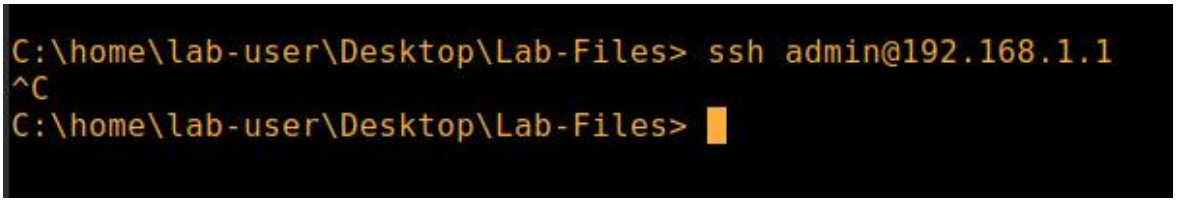
4. Attempt to open an *SSH* connection to the firewall through **192.168.1.1** by issuing the following command.

```
C:\home\lab-user\Desktop\Lab-Files> ssh admin@192.168.1.1 <Enter>
```



```
C:\home\lab-user\Desktop\Lab-Files> ssh admin@192.168.1.1
```

5. After a few seconds, use **Ctrl+C** to stop the connection because it will not succeed.



```
C:\home\lab-user\Desktop\Lab-Files> ssh admin@192.168.1.1
^C
C:\home\lab-user\Desktop\Lab-Files>
```

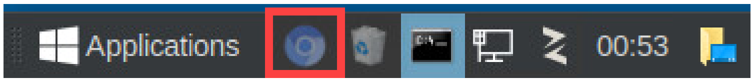
6. Leave the *Terminal* window open on the *client* because you will perform these same tests after applying an *Interface Management profile* to *ethernet1/1* and continue to the next task.

## 4.7 Define Interface Management Profiles

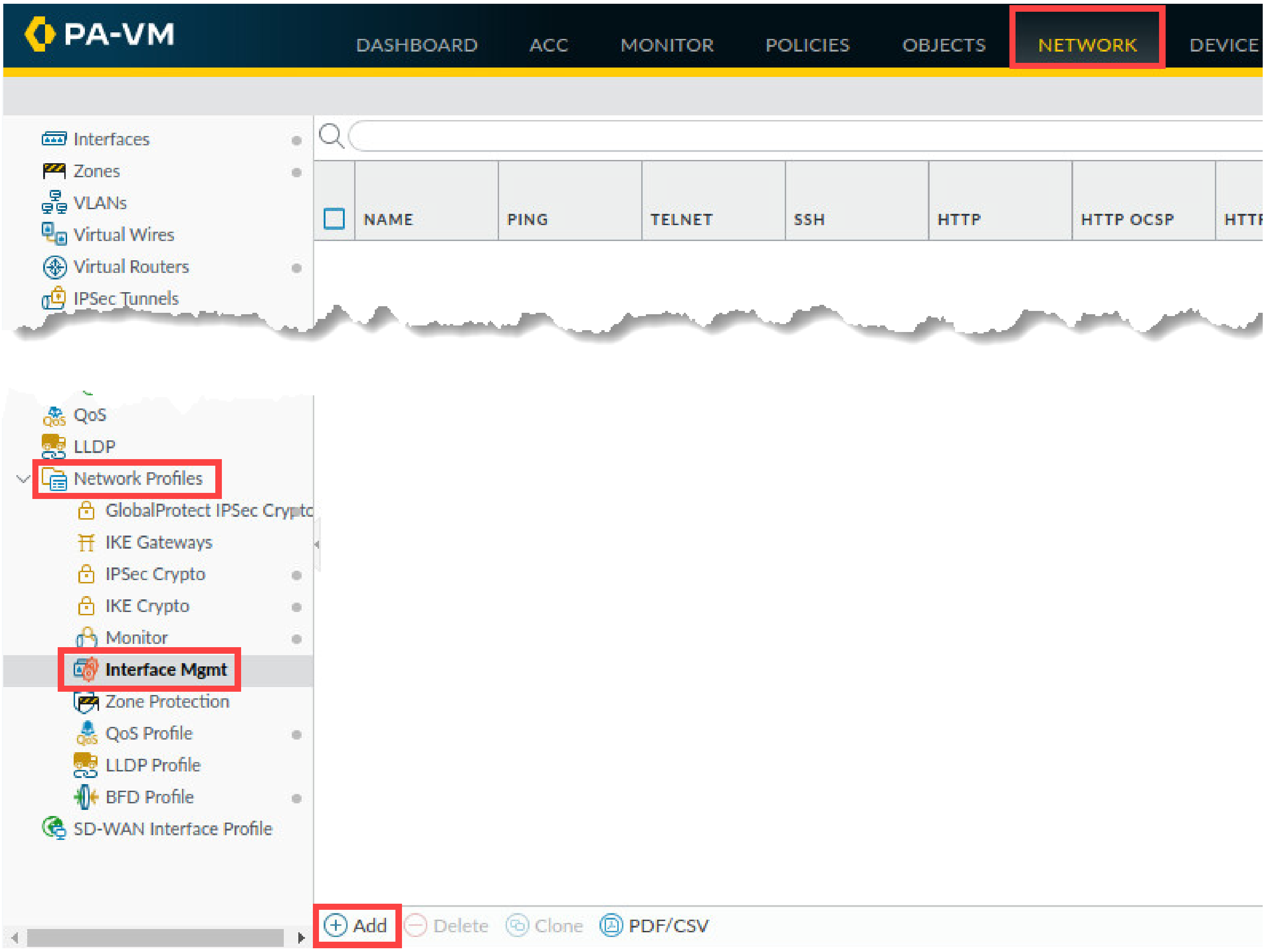
Often, your team members need to manage the firewall but do not always have network connectivity to the management network. In this exercise, you will define two management interface profiles. One profile will allow ping. You will apply this allow-ping profile to the Internet interface so that your SecOps team members can ping the external firewall interface for troubleshooting from outside your organization's network.

You will create a second management interface profile that allows ping and secure management traffic, including SSH and HTTPS. You will apply this Allow-mgt profile to the User_Net interface and to the Extranet interface. This profile will allow your SecOps team to manage the firewall from those networks if they need to.

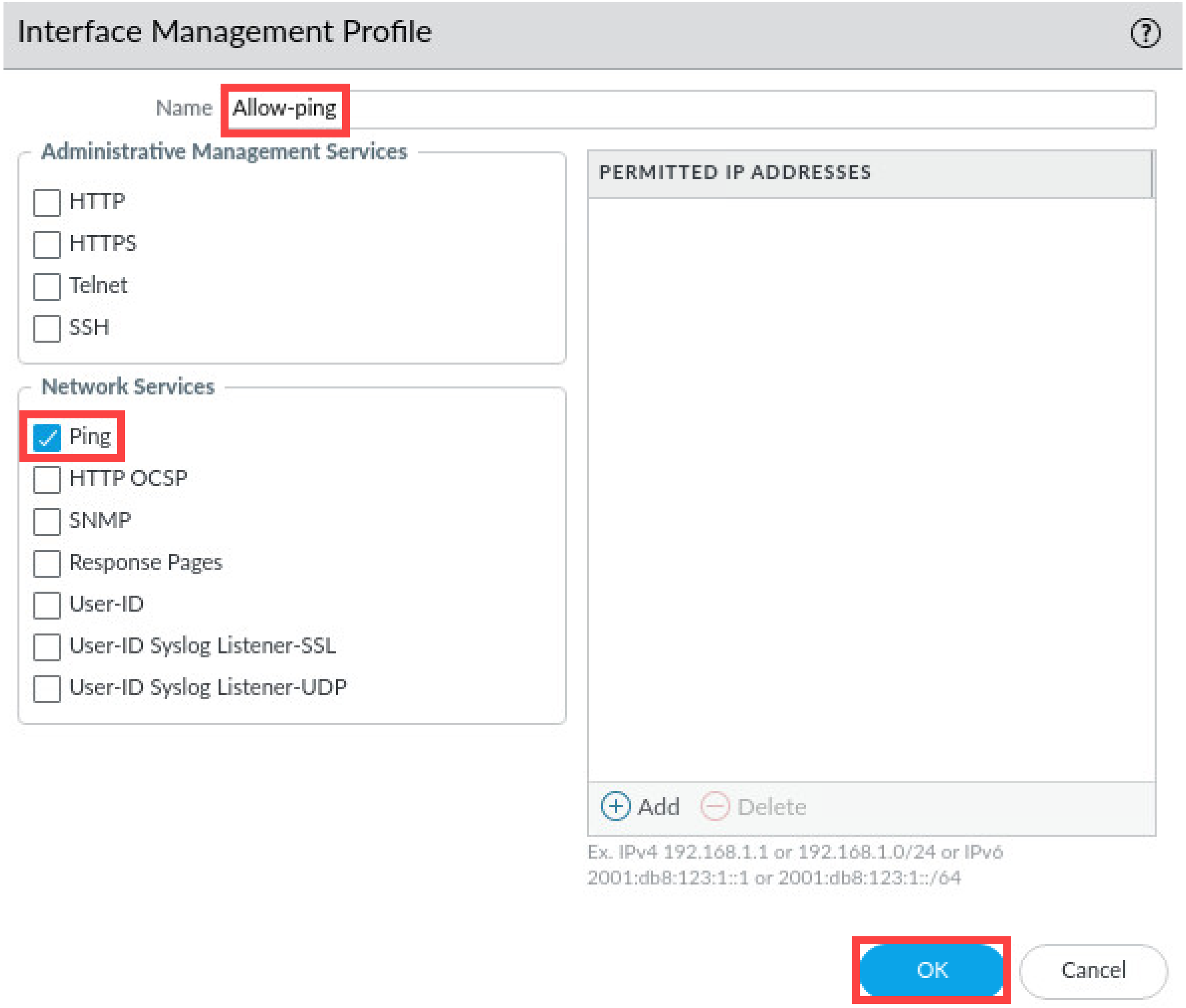
1. Reopen the *PA-VM firewall* web interface by clicking on the **Chromium** icon in the taskbar.



2. Select **Network > Network Profiles > Interface Management**. Click **Add** at the bottom of the window.



3. In the *Interface Management Profile* window, enter **`Allow-ping`** for the *Name*. Under the *Network Services* section, **check** the box for **Ping**. Click **OK**.



Interface Management Profile

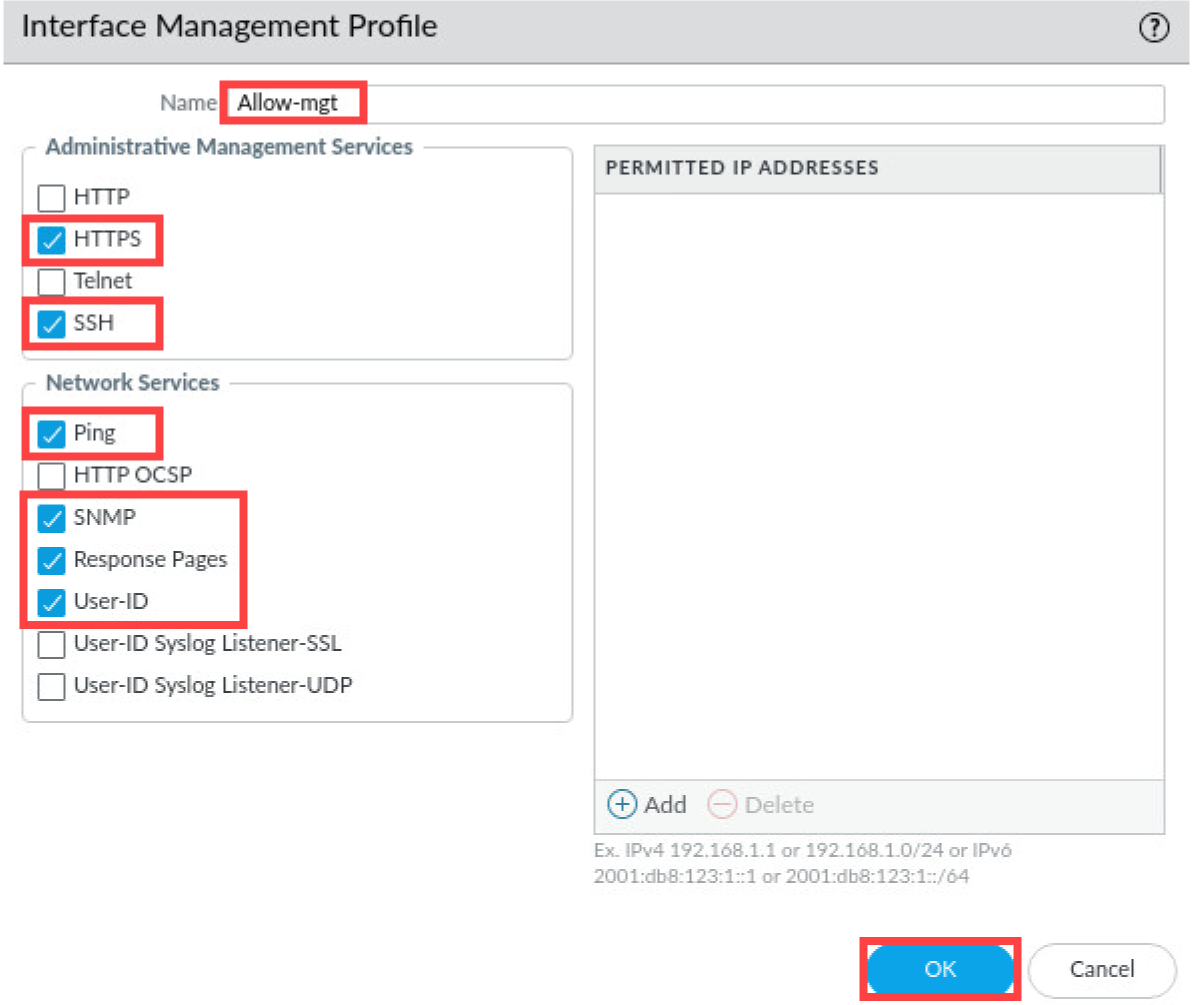
Name: Allow-ping

Administrative Management Services
- □ HTTP
- □ HTTPS
- □ Telnet
- □ SSH

Network Services
- ☑ Ping
- □ HTTP OCSP
- □ SNMP
- □ Response Pages
- □ User-ID
- □ User-ID Syslog Listener-SSL
- □ User-ID Syslog Listener-UDP

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

4. In the *Interface Management* section, click **Add** again to create another entry. In the *Interface Management Profile* window, enter **`Allow-mgt`** for the *Name*. Under the *Administrative Management Services* section, **check** the boxes for **HTTPS** and **SSH**. Under the section for *Network Services*, check **Ping**, **SNMP**, **Response Pages** and **User-ID**. Click **OK**.



Interface Management Profile

Name: Allow-mgt

Administrative Management Services

□ HTTP
☑ HTTPS
□ Telnet
☑ SSH

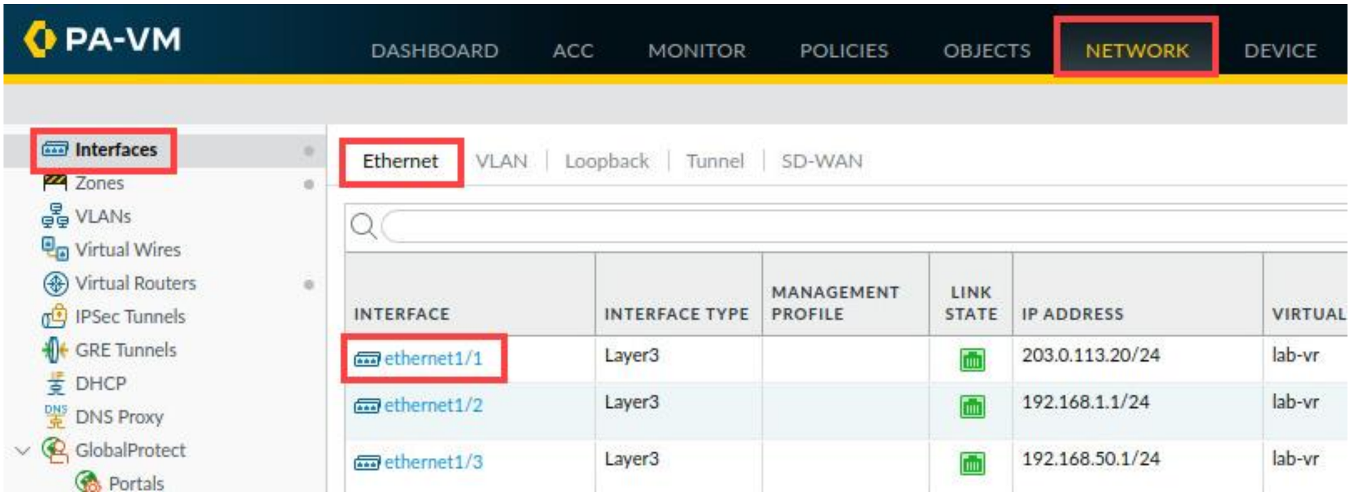
Network Services

☑ Ping
□ HTTP OCSP
☑ SNMP
☑ Response Pages
☑ User-ID
□ User-ID Syslog Listener-SSL
□ User-ID Syslog Listener-UDP

PERMITTED IP ADDRESSES

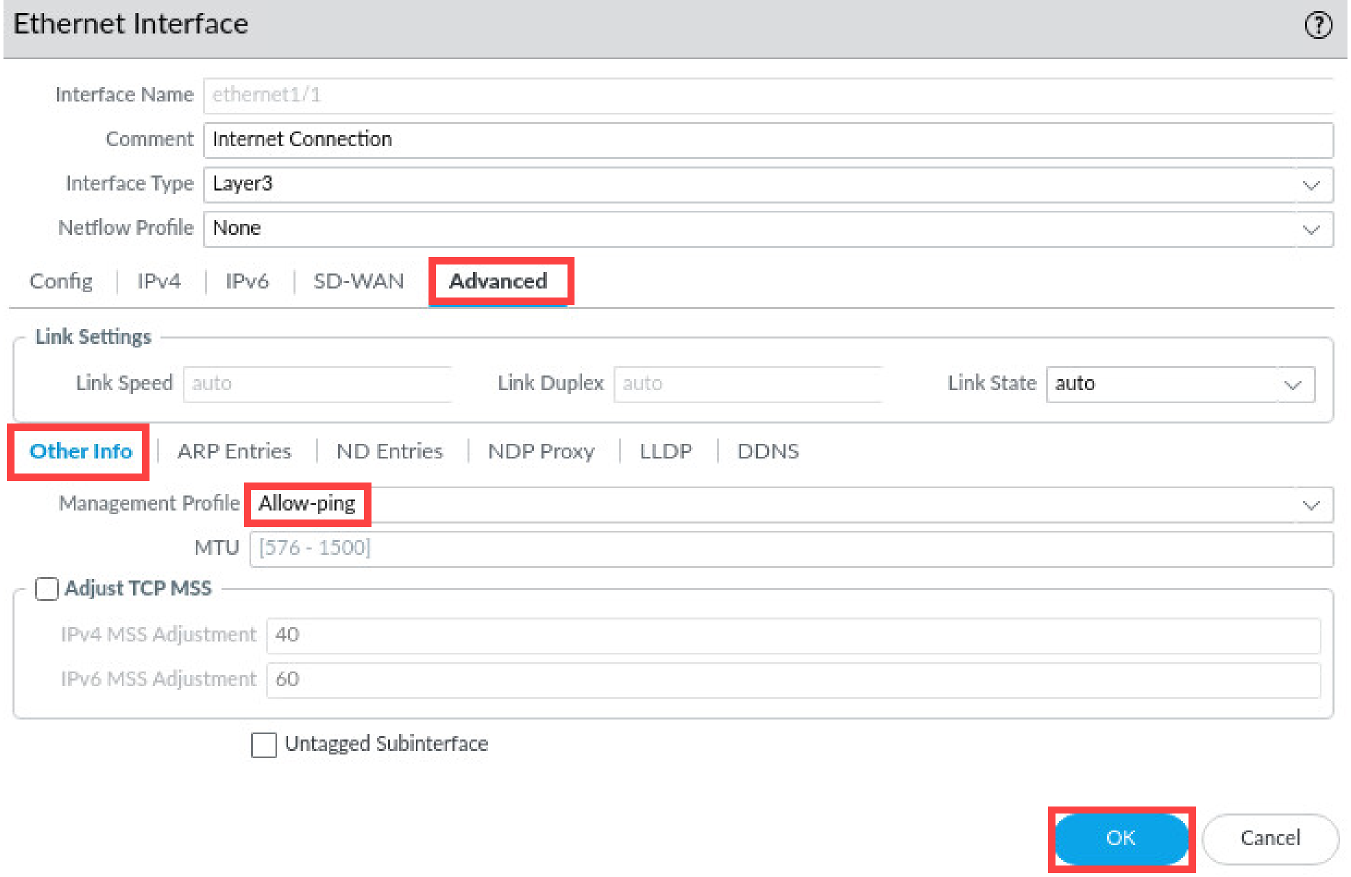
Ex. IPv4 192.168.1.1 or 192.168.1.0/24 or IPv6 2001:db8:123:1::1 or 2001:db8:123:1::/64

5. Select **Network > Interfaces > Ethernet**. Click **Ethernet 1/1**.



| INTERFACE | INTERFACE TYPE | MANAGEMENT PROFILE | LINK STATE | IP ADDRESS | VIRTUAL |
|---|---|---|---|---|---|
| ethernet1/1 | Layer3 | | 🟩 | 203.0.113.20/24 | lab-vr |
| ethernet1/2 | Layer3 | | 🟩 | 192.168.1.1/24 | lab-vr |
| ethernet1/3 | Layer3 | | 🟩 | 192.168.50.1/24 | lab-vr |

6. In the *Ethernet 1/1* window, click **Advanced**. Under the *Other Info* section, use the dropdown list for *Management Profile* and select **Allow-ping**. Click **OK**.



Ethernet Interface

Interface Name: ethernet1/1
Comment: Internet Connection
Interface Type: Layer3
Netflow Profile: None

Config | IPv4 | IPv6 | SD-WAN | Advanced

Link Settings
Link Speed: auto
Link Duplex: auto
Link State: auto

Other Info | ARP Entries | ND Entries | NDP Proxy | LLDP | DDNS

Management Profile: Allow-ping
MTU: [576 - 1500]

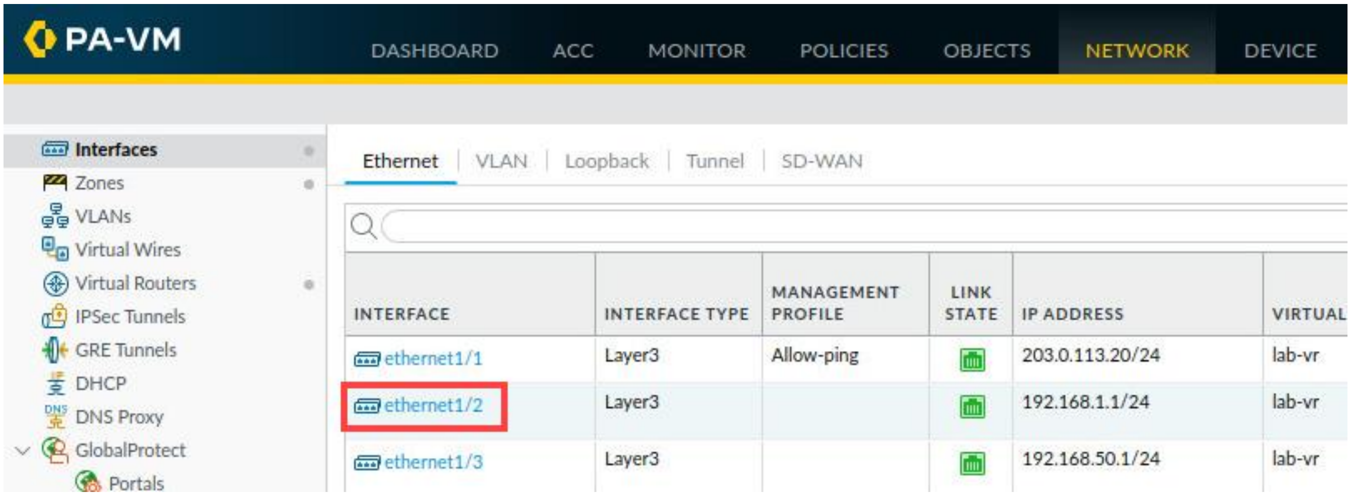
□ Adjust TCP MSS
IPv4 MSS Adjustment: 40
IPv6 MSS Adjustment: 60

□ Untagged Subinterface

Please Note

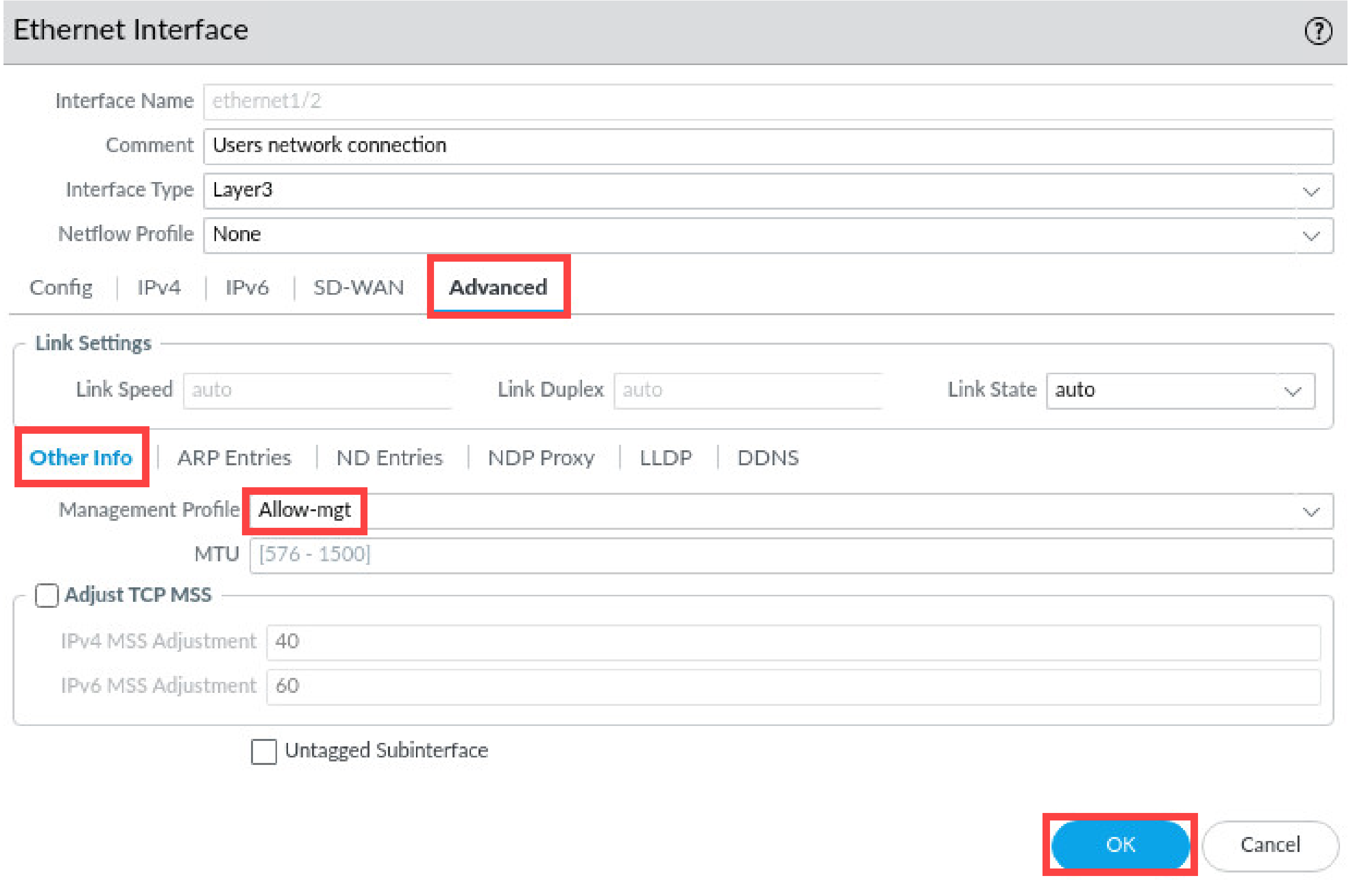
This action applies the Allow-ping interface management profile to ethernet1/1. As a result, ethernet1/1 will answer ping requests. Note that in a production environment, you may not want an internet-facing interface to reply to any type of traffic. Applying this profile in the lab allows you to see how different profiles can be applied to different interfaces.

7. Click **Ethernet 1/2**.



| INTERFACE | INTERFACE TYPE | MANAGEMENT PROFILE | LINK STATE | IP ADDRESS | VIRTUAL |
|---|---|---|---|---|---|
| ethernet1/1 | Layer3 | Allow-ping | 🟩 | 203.0.113.20/24 | lab-vr |
| ethernet1/2 | Layer3 | | 🟩 | 192.168.1.1/24 | lab-vr |
| ethernet1/3 | Layer3 | | 🟩 | 192.168.50.1/24 | lab-vr |

8. In the *Ethernet Interface* window, click **Advanced**. Under the *Other Info* section, use the dropdown list for *Management Profile* and select **Allow-mgt**. Click **OK**.



Interface Name: ethernet1/2
Comment: Users network connection
Interface Type: Layer3
Netflow Profile: None

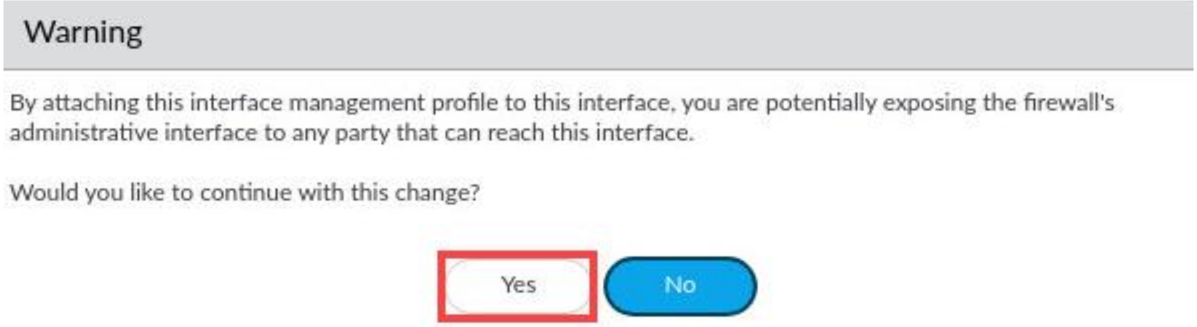
Link Settings
Link Speed: auto
Link Duplex: auto
Link State: auto

Management Profile: Allow-mgt
MTU: [576 - 1500]

□ Adjust TCP MSS
IPv4 MSS Adjustment: 40
IPv6 MSS Adjustment: 60

□ Untagged Subinterface

9. Read the *Warning* message and click **Yes**.



Warning

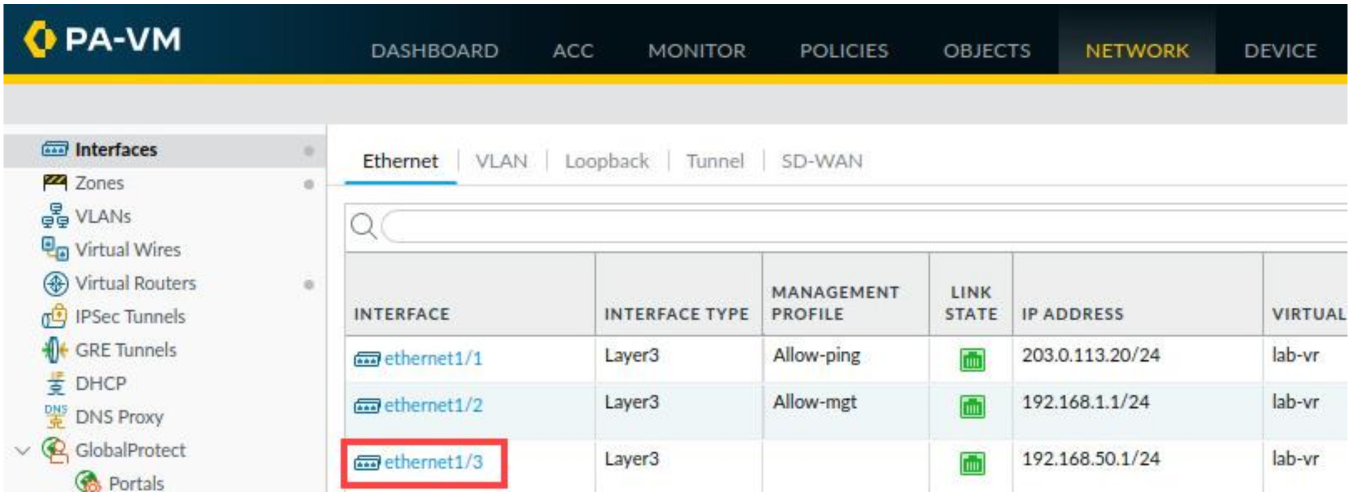
By attaching this interface management profile to this interface, you are potentially exposing the firewall's administrative interface to any party that can reach this interface.

Would you like to continue with this change?

**Please Note**

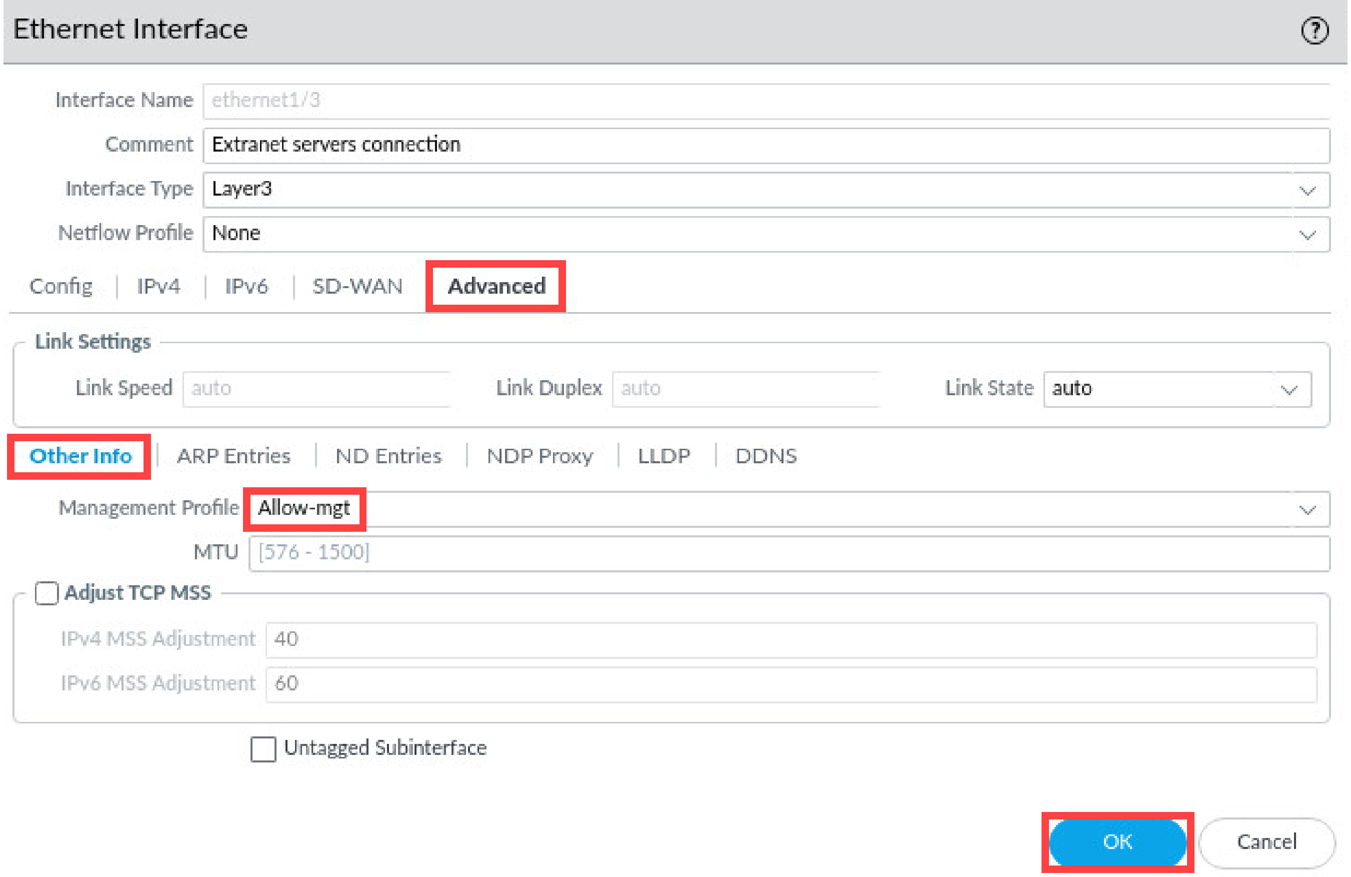
Because this interface is connected to one of your internal networks (Users_Net), the risk of applying this profile is acceptable.

10. Click **Ethernet 1/3**.



| INTERFACE | INTERFACE TYPE | MANAGEMENT PROFILE | LINK STATE | IP ADDRESS | VIRTUAL |
|---|---|---|---|---|---|
| ethernet1/1 | Layer3 | Allow-ping | 🟩 | 203.0.113.20/24 | lab-vr |
| ethernet1/2 | Layer3 | Allow-mgt | 🟩 | 192.168.1.1/24 | lab-vr |
| ethernet1/3 | Layer3 | | 🟩 | 192.168.50.1/24 | lab-vr |

11. In the *Ethernet 1/3* window, click **Advanced**. Under the *Other Info* section, use the dropdown list for *Management Profile* and select **Allow-mgt**. Click **OK**.



Ethernet Interface

Interface Name: ethernet1/3

Comment: Extranet servers connection

Interface Type: Layer3

Netflow Profile: None

Link Settings

Link Speed: auto

Link Duplex: auto

Link State: auto

Management Profile: Allow-mgt

MTU: [576 - 1500]

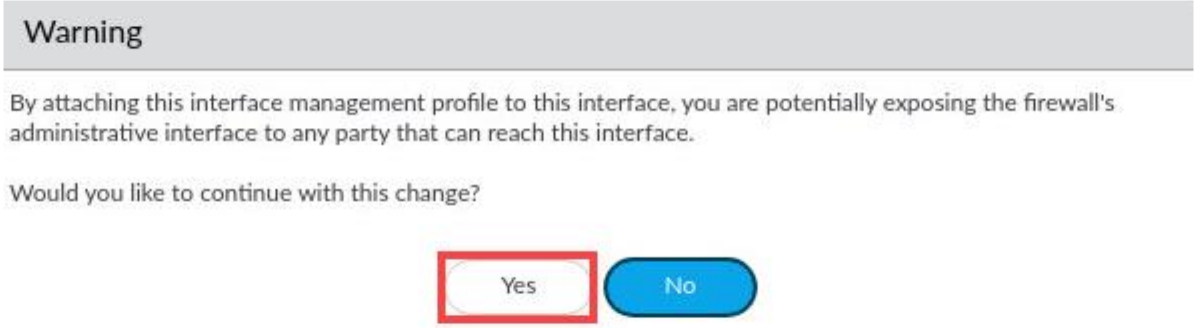
□ Adjust TCP MSS

IPv4 MSS Adjustment: 40

IPv6 MSS Adjustment: 60

□ Untagged Subinterface

12. Read the *Warning* message and click **Yes**.

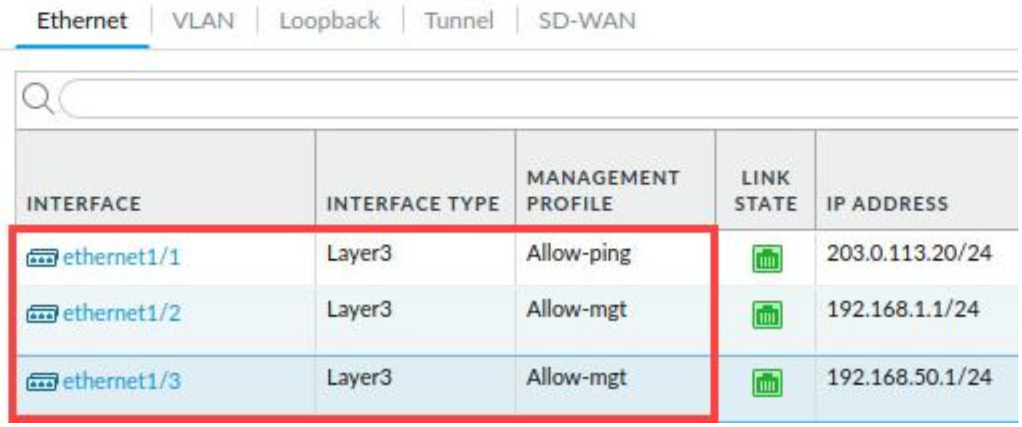


Warning

By attaching this interface management profile to this interface, you are potentially exposing the firewall's administrative interface to any party that can reach this interface.

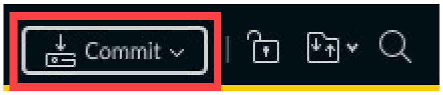
Would you like to continue with this change?

13. When you complete steps *5 - 12*, your interface table should have an entry under the management profile column for each interface.

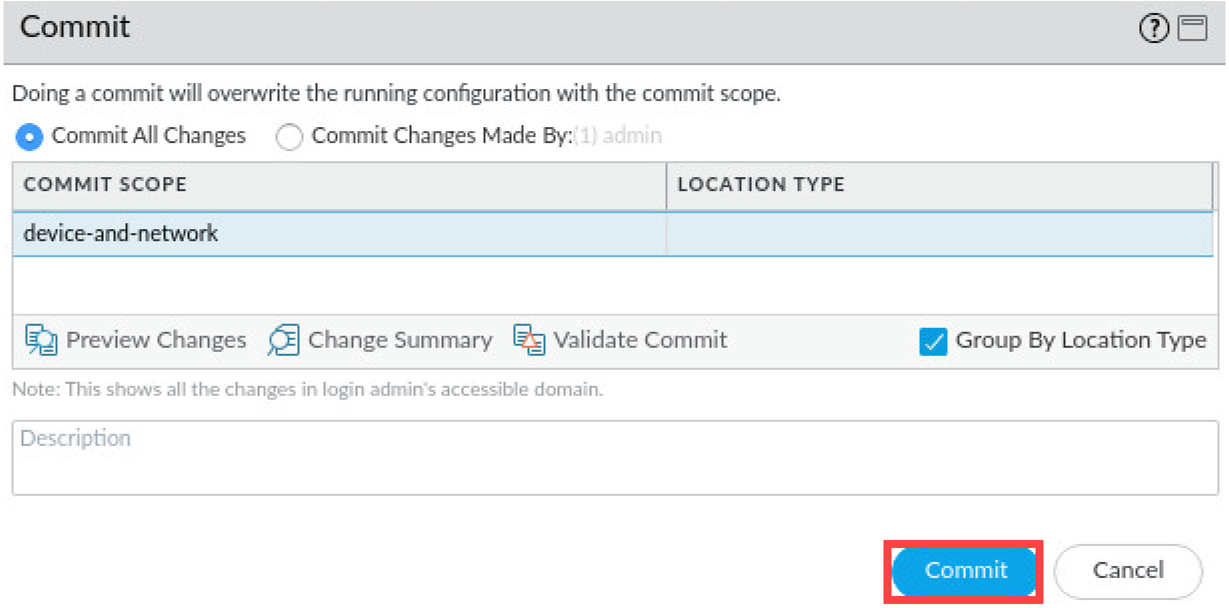


| INTERFACE | INTERFACE TYPE | MANAGEMENT PROFILE | LINK STATE | IP ADDRESS |
|---|---|---|---|---|
| ethernet1/1 | Layer3 | Allow-ping | 🟩 | 203.0.113.20/24 |
| ethernet1/2 | Layer3 | Allow-mgt | 🟩 | 192.168.1.1/24 |
| ethernet1/3 | Layer3 | Allow-mgt | 🟩 | 192.168.50.1/24 |

14. Click the **Commit** button at the upper-right of the web interface.



15. In the *Commit* window, click **Commit**.



Doing a commit will overwrite the running configuration with the commit scope.

● Commit All Changes ○ Commit Changes Made By:(1) admin

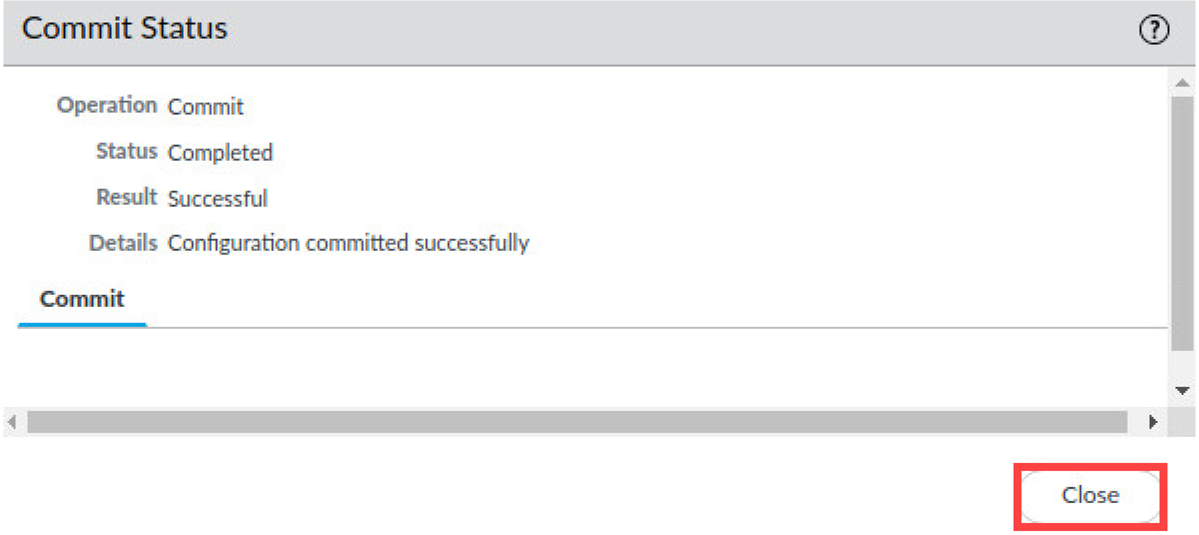
| COMMIT SCOPE | LOCATION TYPE |
|---|---|
| device-and-network | |

☑ Group By Location Type

Note: This shows all the changes in login admin's accessible domain.

Description

16. Wait until the *Commit* process is complete. Click **Close**.



Commit Status

Operation Commit

Status Completed

Result Successful

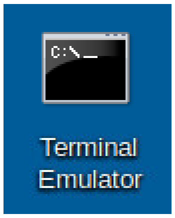
Details Configuration committed successfully

17. Minimize the *Palo Alto Networks Firewall* and continue to the next task.

## 4.8 Test Interface Access after Management Profiles

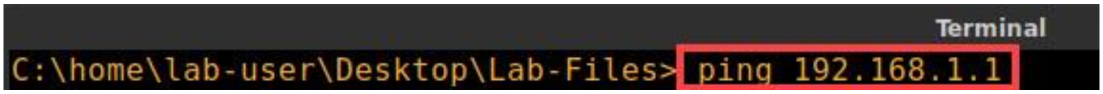
In this section, you will use the ping command to test the management profiles that you defined. Both ping and SSH will succeed.

1. Return to the *Terminal* window used previously or reopen the **Terminal Emulator** on the *client desktop*.



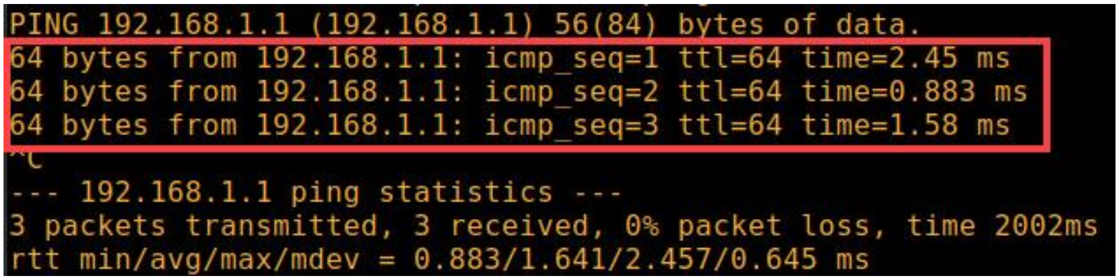
2. Issue the following command below.

```
C:\home\lab-user\Desktop\Lab-Files> ping 192.168.1.1 <Enter>
```



```
C:\home\lab-user\Desktop\Lab-Files> ping 192.168.1.1
```

3. Wait a few seconds and use **Ctrl+C** to stop the command. You will get a response because *Management* profiles have been configured.



```
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=2.45 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=0.883 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=64 time=1.58 ms
^C
--- 192.168.1.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 0.883/1.641/2.457/0.645 ms
```

4. Elevate to *super user* by issuing the following command.

```
C:\home\lab-user\Desktop\Lab-Files> sudo su
```

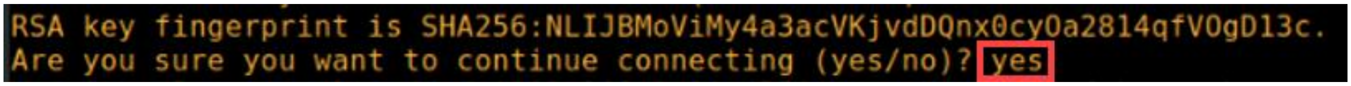
```
C:\home\lab-user\Desktop\Lab-Files> sudo su
```

5. Attempt to open an *SSH connection* to the firewall through **192.168.1.1** by issuing the following command.

```
root@client-a:/home/lab-user/Desktop/Lab-Files# ssh admin@192.168.1.1 <Enter>
```

```
root@client-a:/home/lab-user/Desktop/Lab-Files# ssh admin@192.168.1.1
```

6. When prompted to accept the *RSA key fingerprint*, type **yes** and press **Enter**.

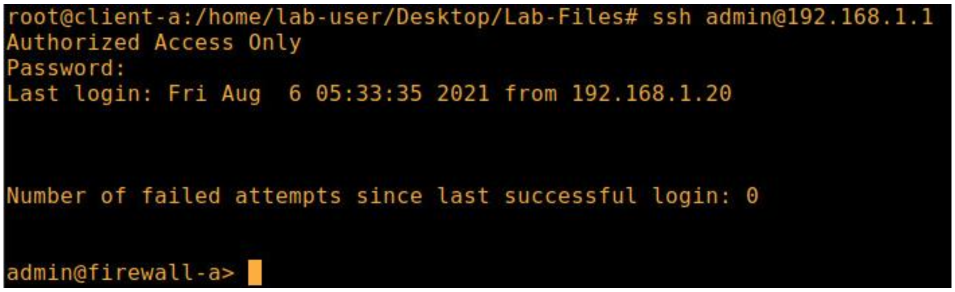


```
RSA key fingerprint is SHA256:NLIJBMoViMy4a3acVKjvdDQnx0cy0a2814qfV0gD13c.
Are you sure you want to continue connecting (yes/no)? yes
```

7. For password, type **`Pal0Alt0!`** and press **Enter**.

```
Authorized Access Only
Password:
```

8. The *firewall* will present the *CLI interface*.



```
root@client-a:/home/lab-user/Desktop/Lab-Files# ssh admin@192.168.1.1
Authorized Access Only
Password:
Last login: Fri Aug  6 05:33:35 2021 from 192.168.1.20


Number of failed attempts since last successful login: 0


admin@firewall-a> █
```

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