



## PALO ALTO NETWORKS FIREWALL 11.0 ESSENTIALS

### Lab 4: Connecting the Firewall to Production Networks with Security Zones

Document Version: **2025-10-13**

Copyright © 2025 Network Development Group, Inc.  
[www.netdevgroup.com](http://www.netdevgroup.com)

NETLAB+ is a registered trademark of Network Development Group, Inc.

Palo Alto Networks, PAN-OS, WildFire, RedLock, and Demisto are registered trademarks of Palo Alto Networks, Inc. All other marks mentioned herein may be trademarks of their respective companies.

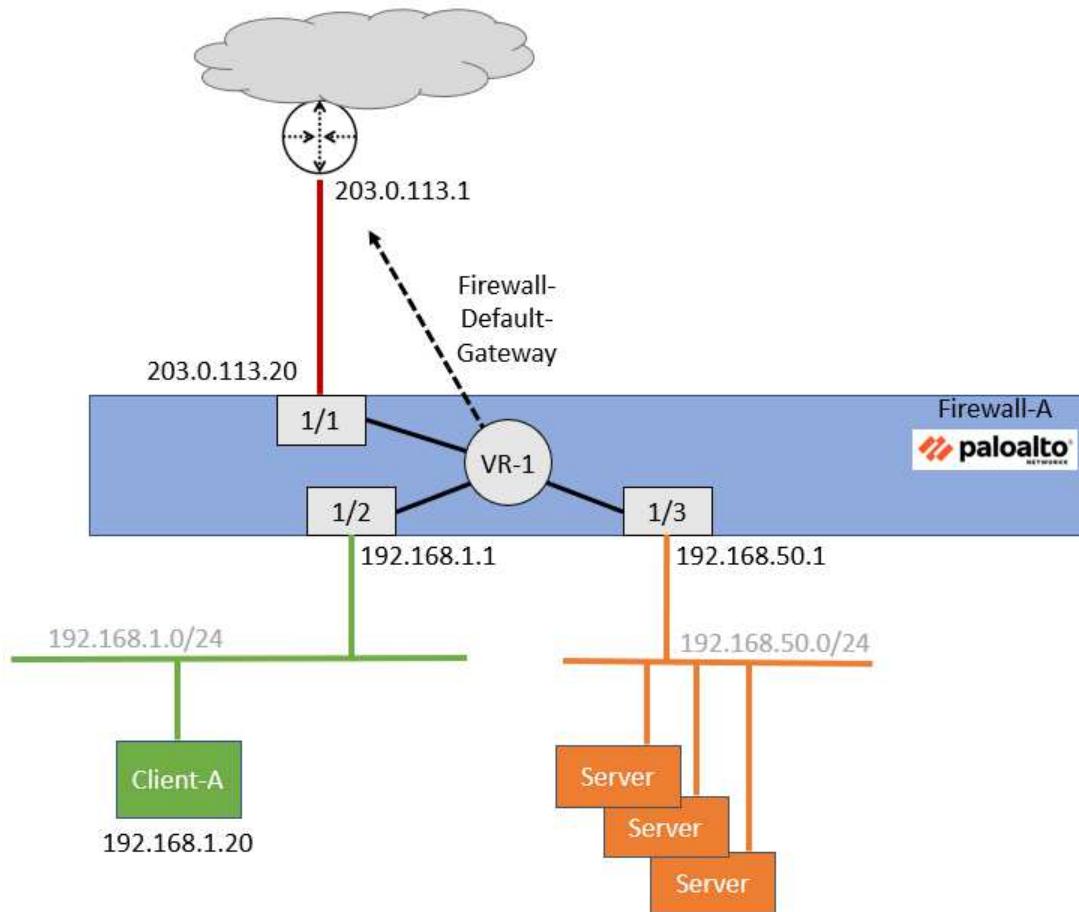
## Contents

Introduction .....	3
Objective .....	3
Lab Topology .....	4
Theoretical Lab Topology.....	4
Lab Settings .....	5
Lab Guidance.....	5
<b>1    Connecting the Firewall to Production Networks with Security Zones- High Level Lab Steps.....</b>	<b>6</b>
1.1    Apply a Baseline Configuration to the Firewall .....	6
1.2    Create Layer 3 Network Interfaces .....	6
1.3    Create a Virtual Router .....	7
1.4    Segment Your Production Network Using Security Zones .....	7
1.5    Commit the Configuration .....	8
1.6    Test Connectivity to Each Zone.....	8
1.7    Test Interface Access before Management Profiles.....	8
1.8    Define Interface Management Profiles .....	8
1.9    Apply Allow-ping to ethernet1/1.....	8
1.10    Apply Allow-mgt to ethernet1/2 .....	9
1.11    Apply Allow-mgt to ethernet1/3 .....	9
1.12    Commit the Configuration .....	9
1.13    Test Interface Access after Management Profiles.....	9
<b>2    Connecting the Firewall to Production Networks with Security Zones – Detailed Lab Steps .....</b>	<b>10</b>
2.1    Apply a Baseline Configuration to the Firewall.....	10
2.2    Create Layer 3 Network Interfaces.....	14
2.3    Create a Virtual Router.....	19
2.4    Segment Your Production Network Using Security Zones.....	23
2.5    Test Connectivity to Each Zone .....	28
2.6    Test Interface Access before Management Profiles .....	31
2.7    Define Interface Management Profiles .....	33
2.8    Test Interface Access after Management Profiles .....	40

## 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. In this section, 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.

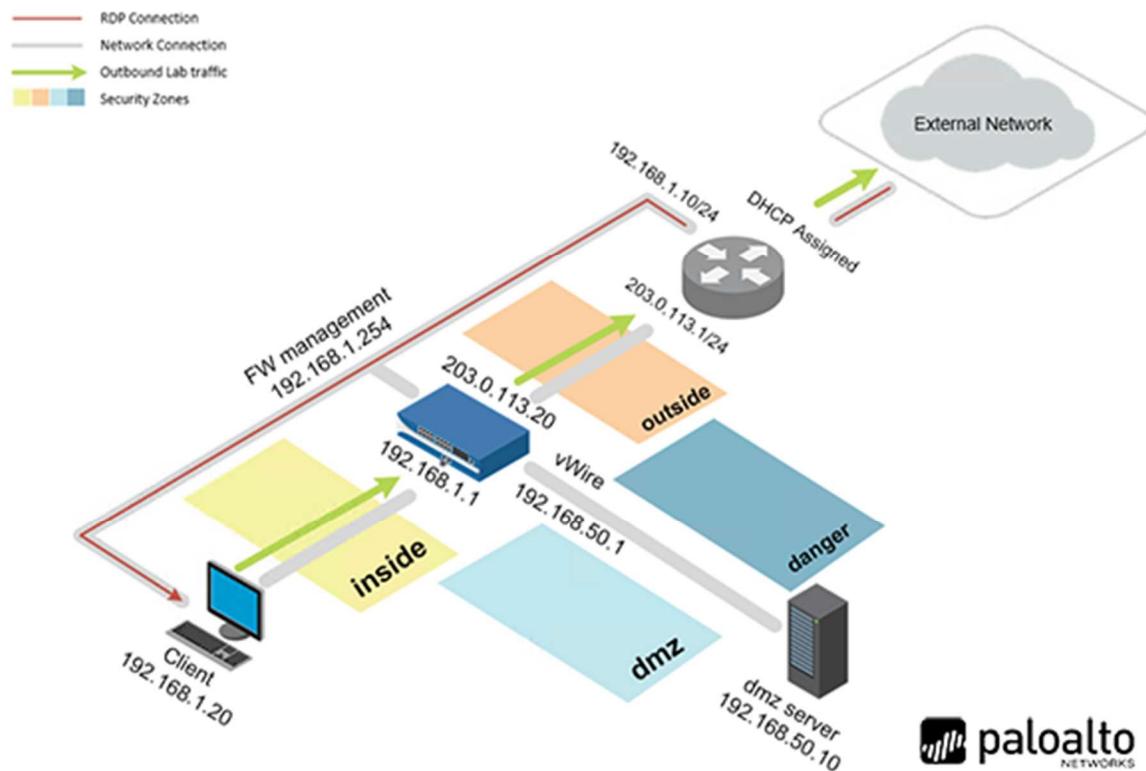


## Objective

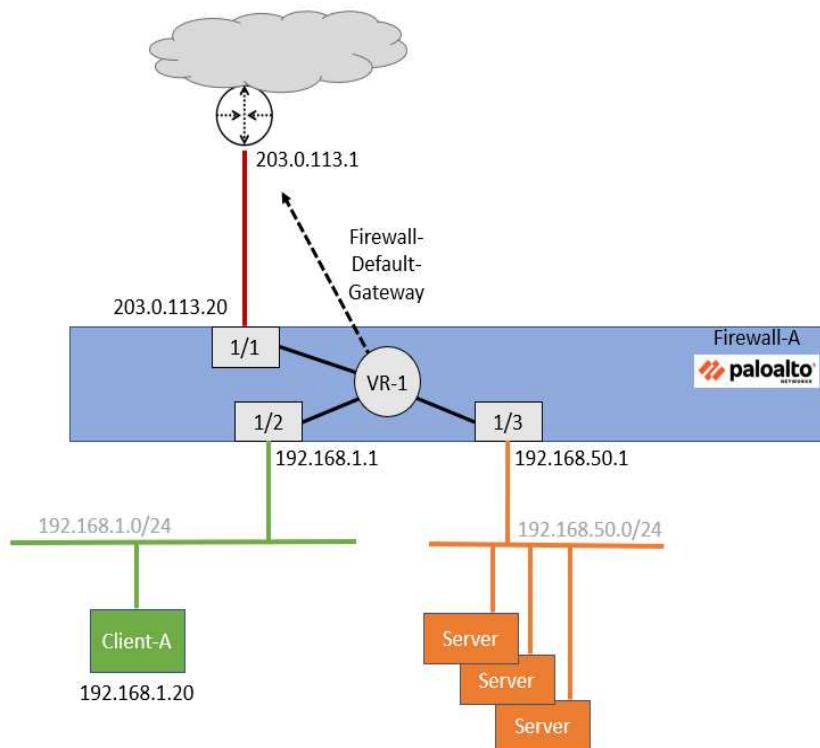
In this lab, you will perform the following tasks:

- 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 (if needed)	Password (if needed)
Client	<b>192.168.1.20</b>	lab-user	PaloAlt0!
DMZ	<b>192.168.50.10</b>	root	PaloAlt0!
Firewall	<b>192.168.1.254</b>	admin	PaloAlt0!
vRouter	<b>192.168.1.10</b>	root	PaloAlt0

## Lab Guidance

There are two sections in this lab guide:

- High-Level Lab Steps
- Detailed Lab Steps

The High-Level Lab Steps section provides only general guidance and information about how to accomplish the lab objectives. This section is more challenging and is suited for students who have a working knowledge of Palo Alto Networks firewalls. If you have never worked with a Palo Alto Networks firewall, we strongly encourage you to use the Detailed Lab Steps section.

The instructions in the Detailed Lab Steps section provide guided, detailed steps and screenshots to accomplish the lab objectives.

If you decide to use the High-Level Lab Guide and get stuck, switch to the Detailed Lab Guide for guidance.

Please  
Note

You are not required to complete both the High-Level Lab Guide and the Detailed Lab Guide for each lab. Instead, please select the appropriate section based on your familiarity with Palo Alto Networks Firewalls.

## 1 Connecting the Firewall to Production Networks with Security Zones- High Level Lab Steps

It is recommended to use this section if you possess significant experience in working with Palo Alto Networks firewalls. In case you require more comprehensive instructions to achieve the objectives, please utilize the Detailed-Lab Steps section in Task 2.

### 1.1 Apply a Baseline Configuration to the Firewall

- On the Zorin desktop, select *lab-user*, enter **Pal0Alt0!** for the password.
- For the Palo Alto Firewall, enter **admin** for the user and **Pal0Alt0!** for the password.
- Load and commit the configuration file - **edu-210-11.0a-04.xml** to the Firewall.

### 1.2 Create Layer 3 Network Interfaces

- Use the information in the tables below to create Layer 3 network interfaces.

<b>Create a Layer 3 Interface on ethernet1/1</b>	
<b>Ethernet Interface</b>	<b>ethernet1/1</b>
<b>Comment</b>	<b>Internet Connection</b>
<b>Type</b>	<b>Layer 3</b>
<b>IPv4 Type</b>	<b>Static</b>
<b>IP</b>	<b>203.0.113.20/24</b>

<b>Create a Layer 3 Interface on ethernet1/2</b>	
<b>Ethernet Interface</b>	<b>ethernet1/2</b>
<b>Comment</b>	<b>Users network connection</b>
<b>Type</b>	<b>Layer 3</b>
<b>IPv4 Type</b>	<b>Static</b>
<b>IP</b>	<b>192.168.1.1/24</b>

<b>Create a Layer 3 Interface on ethernet1/3</b>	
<b>Ethernet Interface</b>	<b>ethernet1/3</b>
<b>Comment</b>	<b>Extranet servers connection</b>
<b>Type</b>	<b>Layer 3</b>
<b>IPv4 Type</b>	<b>Static</b>

<b>IP</b>	<b>192.168.50.1/24</b>
-----------	------------------------

### 1.3 Create a Virtual Router

- Use the information in the table below to create a Virtual Router and a firewall default gateway.

<b>Name</b>	<b>VR-1</b>
<b>Interfaces (General Tab)</b>	<b>ethernet1/1</b> <b>ethernet1/2</b> <b>ethernet1/3</b>
<b>IPv4 Static Route Name</b>	<b>Firewall Default Gateway</b>
<b>Destination</b>	<b>0.0.0.0/0</b>
<b>Interface</b>	<b>ethernet1/1</b>
<b>Next Hop</b>	<b>IP Address</b>
<b>Next Hop IP</b>	<b>203.0.113.1</b>

### 1.4 Segment Your Production Network Using Security Zones

- Use the information in the tables below to create three Security Zones with the appropriate interface in each Zone.

<b>Zone Name</b>	<b>Internet</b>
<b>Type</b>	<b>Layer 3</b>
<b>Interface</b>	<b>ethernet1/1</b>

<b>Zone Name</b>	<b>Users_Net</b>
<b>Type</b>	<b>Layer 3</b>
<b>Interface</b>	<b>ethernet1/2</b>

<b>Zone Name</b>	<b>Extranet</b>
<b>Type</b>	<b>Layer 3</b>
<b>Interface</b>	<b>ethernet1/3</b>

## 1.5 Commit the Configuration

- Commit the changes to the firewall before proceeding.

## 1.6 Test Connectivity to Each Zone

- Use the *Remmina SSH* application on the Client-A desktop to connect to Firewall-A.
- In the firewall CLI, use the **ping** command to check network connectivity from the firewall to a host in each Security Zone.
  - From **192.168.1.1** (ethernet1/2) to **192.168.1.20**.
  - From **192.168.50.1** (ethernet1/3) to **192.168.50.150**.
  - From **203.0.113.20** (ethernet1/1) to **8.8.8.8**.

## 1.7 Test Interface Access before Management Profiles

- Ping the firewall interface on ethernet1/2 from a terminal connection on Client-A. You will not get a response.
- Attempt to connect to the firewall for CLI management through an SSH connection from Client-A. The firewall will not accept the connection.

## 1.8 Define Interface Management Profiles

Use the information below to create two Interface Management Profiles.

<b>Name</b>	<b>Allow-ping</b>
<b>Enabled Administrative Management Services</b>	<b>None</b>
<b>Enabled Network Services</b>	<b>Ping</b>

<b>Name</b>	<b>Allow-mgt</b>
<b>Enabled Administrative Management Services</b>	<b>HTTPS</b> <b>SSH</b>
<b>Enabled Network Services</b>	<b>Ping</b> <b>SNMP</b> <b>Response Pages</b>

## 1.9 Apply Allow-ping to ethernet1/1

- Apply the **Allow-ping** Interface Management Profile to **ethernet1/1**.

### 1.10 Apply Allow-mgt to ethernet1/2

- Apply the **Allow-mgt** Interface Management Profile to **ethernet1/2**.

### 1.11 Apply Allow-mgt to ethernet1/3

- Apply the **Allow-mgt** Interface Management Profile to **ethernet1/3**.

### 1.12 Commit the Configuration

- Commit the changes before testing Interface Management Profiles.

### 1.13 Test Interface Access after Management Profiles

- Ping the firewall interface on ethernet1/2 from a terminal connection on Client-A. You should now get a response.
- Attempt to connect to the firewall for CLI management through an SSH connection from Client-A. The firewall will now accept the connection.

## 2 Connecting the Firewall to Production Networks with Security Zones – Detailed Lab Steps

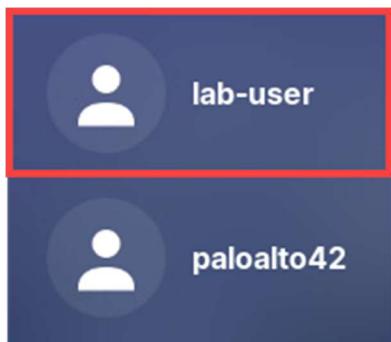
### 2.1 Apply a Baseline Configuration to the Firewall

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

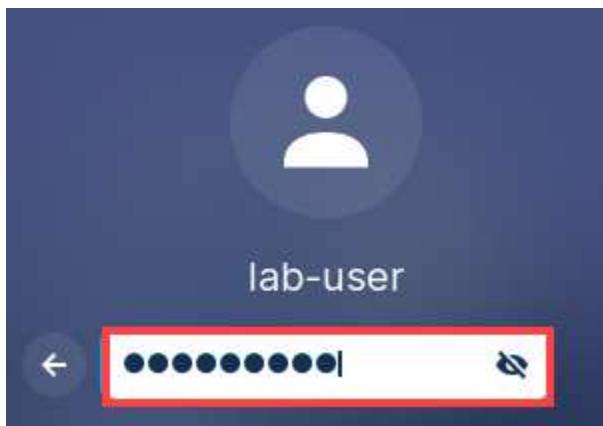
1. Click on the **Client** tab to access the Client PC.



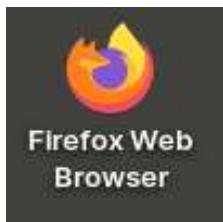
2. On the *Zorin* desktop, click **lab-user**.



3. For the *lab-user* password, enter **Pal0Alt0!** and press **Enter**.



4. Double-click the **Firefox Web Browser** icon located on the *Desktop*.



5. In the *Firefox* address field, type **<https://192.168.1.254>** and press **Enter**.



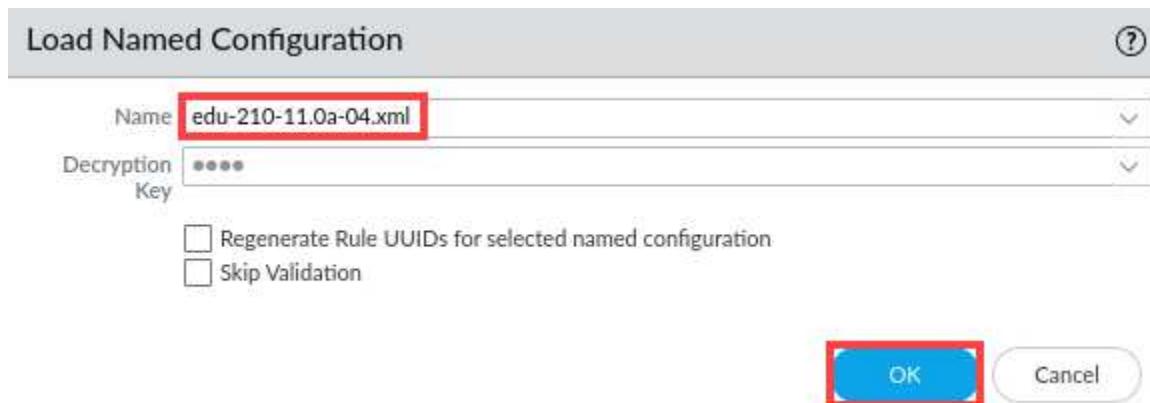
6. Log in to the Firewall web interface as username **admin**, password **Pa10Alt0!**.



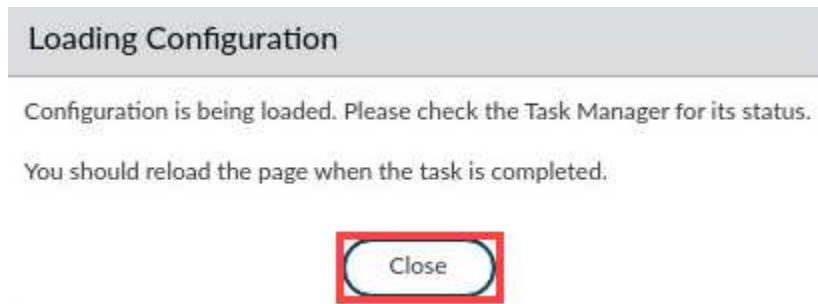
If you do not immediately see the login page, please wait an additional 1-3 minutes for the *Firewall* to fully initialize. If needed, refresh the page.

7. Navigate to **Device > Setup > Operations** in the web interface and click on **Load named configuration snapshot** underneath the *Configuration Management* section.

8. In the *Load Named Configuration* window, select **edu-210-11.0a-04.xml** from the *Name* drop-down box and click **OK**.



9. 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.



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



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

Task Manager - All Tasks						
<input type="text"/> 12 items <span style="float: right;">X</span>						
JOB ID	TYPE	STATUS	START TIME	MESSAGES	ACTION	ADMIN
14	Load	Completed	2023/07/28 18:54:07			System
2	Report	Completed	2023/07/28 18:51:30			

Show  Clear Commit Queue

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



13. 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 All Changes  Commit Changes Made By: (1) admin

COMMIT SCOPE	LOCATION TYPE	OBJECT TYPE	ENTITIES	ADMINS
Commit Scope is unavailable when a full commit is required				

Preview Changes Change Summary Validate Commit

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

Description

**Commit** Cancel

14. When the commit operation is complete, click **Close** to continue.

**Commit Status**

Operation Commit

Status Completed

Result Successful

Details Configuration committed successfully

**Commit**

**Close**

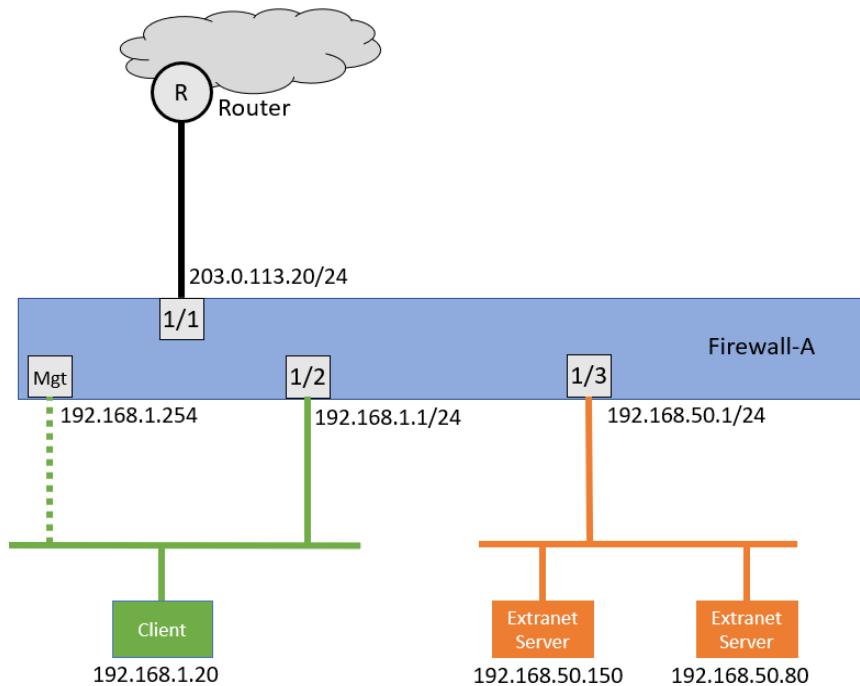


The commit process takes changes made to the Firewall and copies them to the running configuration, which will activate all configuration changes since the last commit.

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

## 2.2 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). The following diagram provides details.



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

The screenshot shows the PA-VM web interface. The top navigation bar includes links for DASHBOARD, ACC, MONITOR, POLICIES, OBJECTS, NETWORK (which is highlighted with a red box), and DEVICE. Below the navigation bar, a secondary menu bar shows tabs for Interfaces (highlighted with a red box), Ethernet (highlighted with a red box), VLAN, Loopback, Tunnel, and SD-WAN. The main content area displays a table of network interfaces.

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

The screenshot shows the 'Ethernet' tab of the interface configuration page. The top navigation bar for this section includes links for Ethernet (highlighted with a red box), VLAN, Loopback, Tunnel, and SD-WAN. The main content area displays a table with columns for INTERFACE, INTERFACE TYPE, and MANAGEMENT PROFILE. The first row, which is highlighted with a red box, corresponds to the 'ethernet1/1' interface. The second row corresponds to 'ethernet1/2'.

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

Parameter	Value
Comment	<b>Internet Connection</b>
Interface Type	<b>Layer3</b>
Virtual Router	<b>None</b>

**Ethernet Interface** (?)

Interface Name	ethernet1/1
Comment	<b>Internet Connection</b>
Interface Type	<b>Layer3</b>
Netflow Profile	None

**Config** | IPv4 | IPv6 | SD-WAN | Advanced

**Assign Interface To**

Virtual Router	<b>None</b>
Security Zone	None

**OK** **Cancel**

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

**Config** IPv4 | IPv6 | SD-WAN | Advanced

Enable SD-WAN

Type  **Static**  PPPoE  DHCP Client

<input type="checkbox"/> IP	<input checked="" type="checkbox"/> 203.0.113.20/24
<b>+ Add</b>	<b>- Delete</b>
<b>↑ Move Up</b> <b>↓ Move Down</b>	

IP address/netmask. Ex. 192.168.2.254/24

**OK** **Cancel**

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

Ethernet	VLAN	Loopback	Tunnel	SD-WAN
INTERFACE	INTERFACE TYPE	MANAGEMENT PROFILE		
ethernet1/1	Layer3			
ethernet1/2				
ethernet1/3				
ethernet1/4				

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

Parameter	Value
Comment	<b>Users network connection</b>
Interface Type	<b>Layer3</b>
Virtual Router	<b>None</b>

**Ethernet Interface**

Interface Name	ethernet1/2
Comment	<b>Users network connection</b>
Interface Type	<b>Layer3</b>
Netflow Profile	None
<b>Config</b>	IPv4   IPv6   SD-WAN   Advanced
<b>Assign Interface To</b>	
Virtual Router	<b>None</b>
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
Config	<b>IPv4</b>   IPv6   SD-WAN   Advanced
<input type="checkbox"/> Enable SD-WAN Type: <input checked="" type="radio"/> Static   <input type="radio"/> PPPoE   <input type="radio"/> DHCP Client	
<input type="checkbox"/> IP <input checked="" type="checkbox"/> 192.168.1.1/24	
<b>(+ Add)</b>   <b>(- Delete)</b>   <b>↑ Move Up</b>   <b>↓ Move Down</b>	
IP address/netmask. Ex. 192.168.2.254/24	
<input style="background-color: #0070C0; color: white; border: 2px solid red; border-radius: 5px; padding: 5px; margin-right: 10px;" type="button" value="OK"/> <b>Cancel</b>	

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

**Ethernet** | VLAN | Loopback | Tunnel | SD-WAN

INTERFACE	INTERFACE TYPE	MANAGEMEN T PROFILE
ethernet1/1	Layer3	
ethernet1/2	Layer3	
<b>ethernet1/3</b>		
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

**Config** | IPv4 | IPv6 | SD-WAN | Advanced

**Assign Interface To**

Virtual Router	None
Security Zone	None

**OK** **Cancel**

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

**Config** IPv4 | IPv6 | SD-WAN | Advanced

Enable SD-WAN

Type  Static  PPPoE  DHCP Client

<input type="checkbox"/> IP	<input checked="" type="checkbox"/> 192.168.50.1/24
-----------------------------	---

**(+)** Add **(-)** Delete **↑** Move Up **↓** Move Down

IP address/netmask: Ex. 192.168.2.254/24

**OK** **Cancel**

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.

## 2.3 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: Disabled		

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

	NAME	INTERFACES	CONFIGURATION
	default		ECMP status: Disabled

3. In the *Virtual Router - default* window, rename the default router to **VR-1**. Click **Add** to add the following interfaces: **ethernet1/1**, **ethernet1/2**, and **ethernet1/3**.

**Virtual Router - default**

<b>Router Settings</b>	Name <b>VR-1</b> <b>General</b>   ECMP <b>INTERFACES</b> <input type="checkbox"/> ethernet1/1 <input type="checkbox"/> ethernet1/2 <input checked="" type="checkbox"/> ethernet1/3  <b>+ Add</b> <b>- Delete</b>	<b>Administrative Distances</b> Static 10 Static IPv6 10 OSPF Int 30 OSPF Ext 110 OSPFv3 Int 30 OSPFv3 Ext 110 IBGP 200 EBGP 20 RIP 120
------------------------	---	--

**OK** **Cancel**

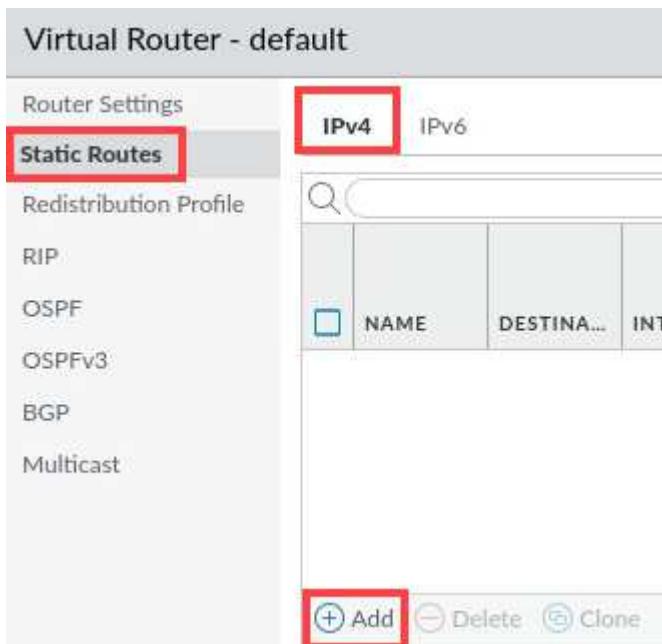


This step can also be completed via each **Ethernet Interface** configuration window.

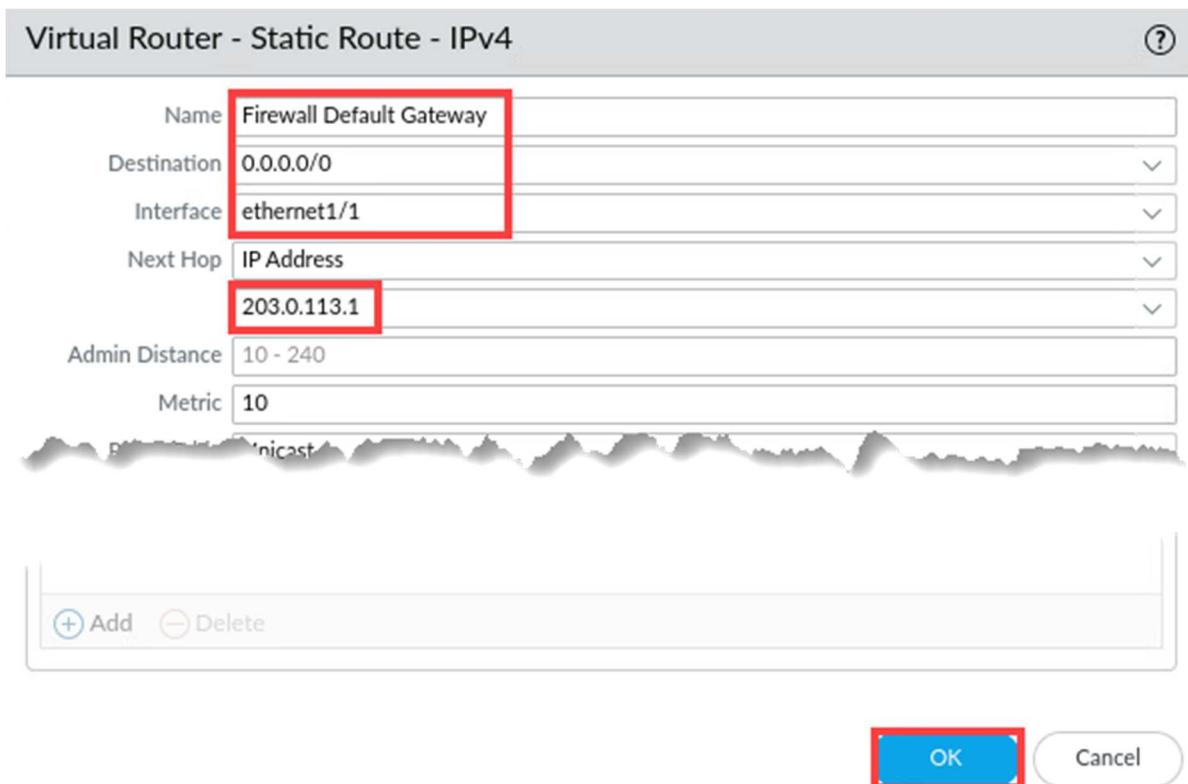
**Please Note**

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.



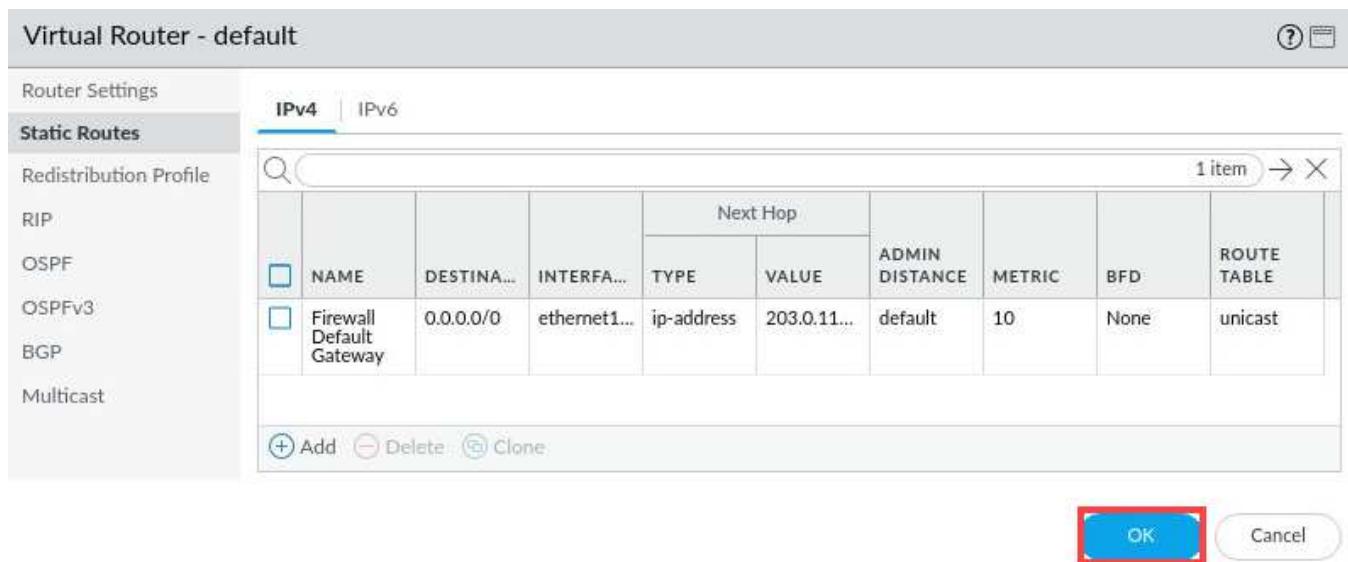
5. In the *Virtual Router – Static Route - IPv4* window, for *Name*, enter **Firewall Default Gateway**, for *Destination*, enter **0.0.0.0/0**, for *Interface*, select **ethernet1/1**, for the *Next Hop* address, enter **203.0.113.1**. Leave the remaining settings unchanged. Click **OK**.





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**.

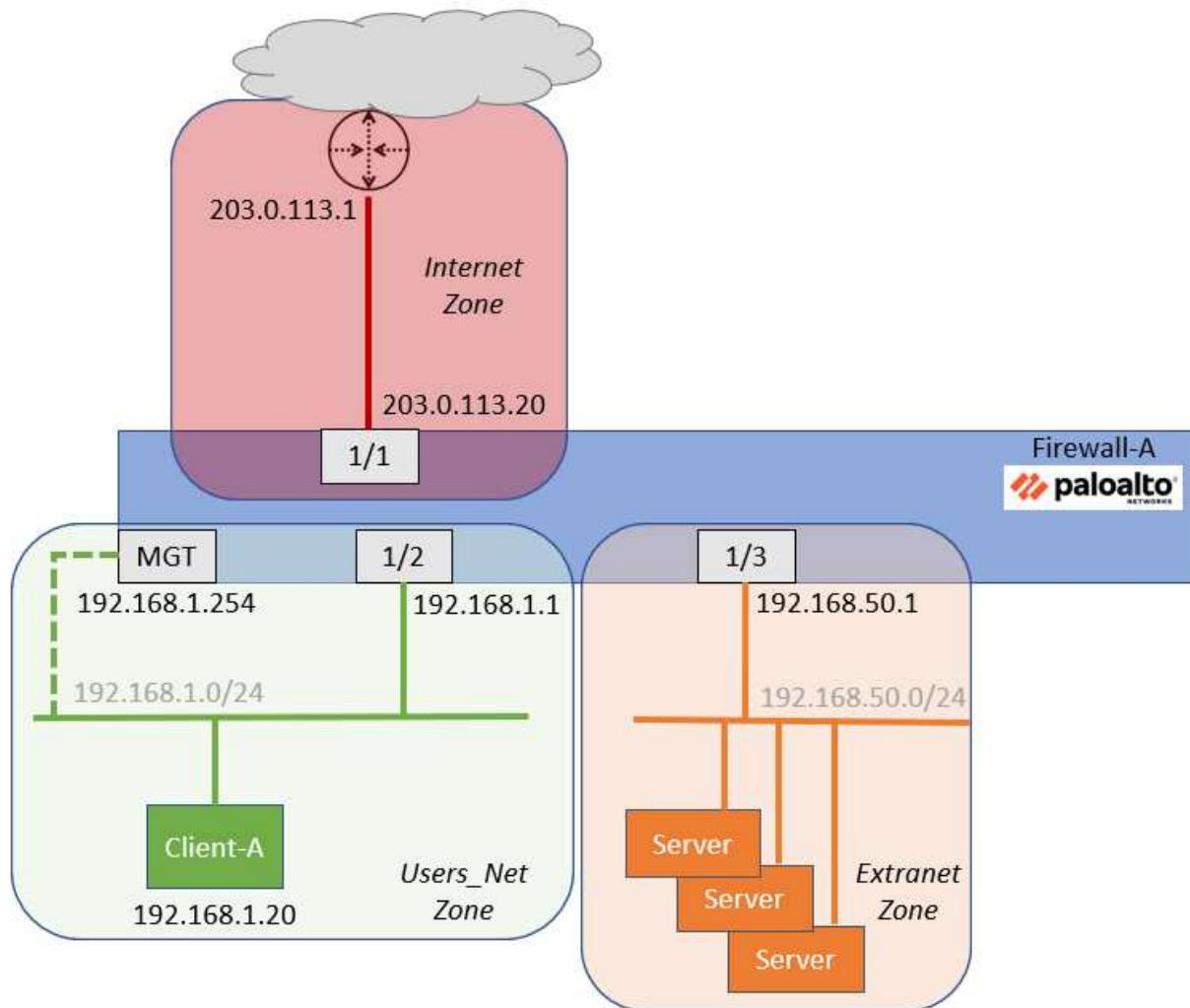


NAME	DESTINA...	INTERFA...	Next Hop		ADMIN DISTANCE	METRIC	BFD	ROUTE TABLE
			TYPE	VALUE				
Firewall Default Gateway	0.0.0.0/0	ethernet1...	ip-address	203.0.11...	default	10	None	unicast

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

## 2.4 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.

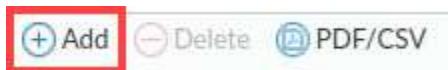


With your network interfaces and virtual router in place, you can now create security zones. You will create three security zones.

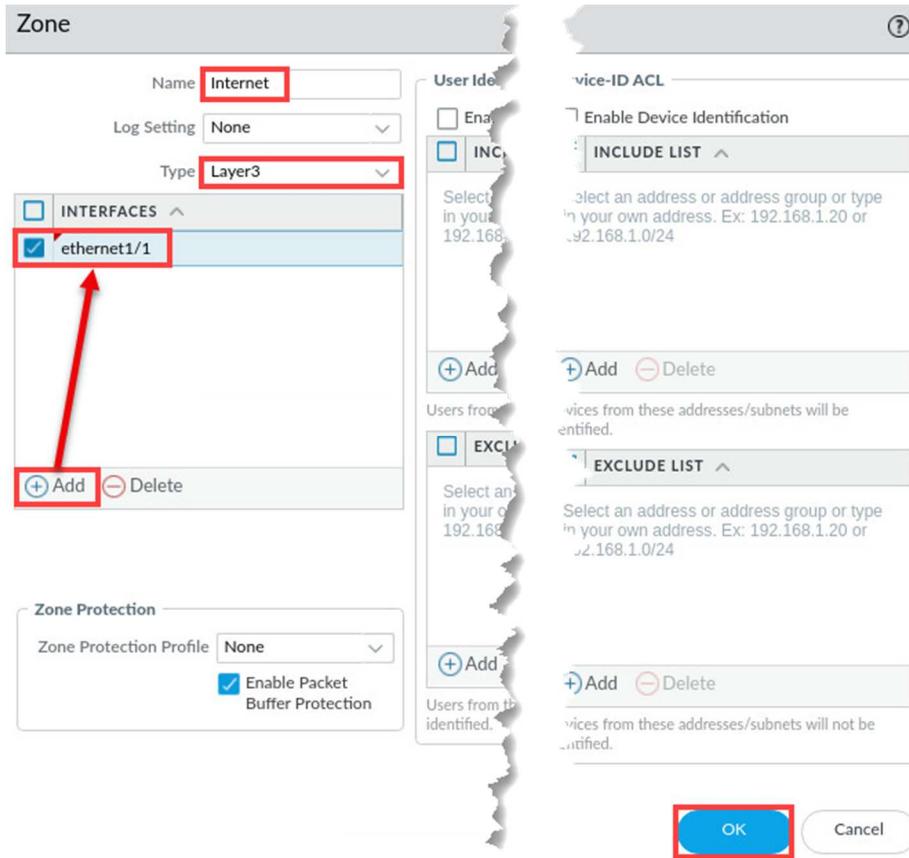
1. In the web interface, select **Network > Zones**.

The screenshot shows the PA-VM web interface with the NETWORK tab selected. The ZONES tab is highlighted with a red box. Other tabs include DASHBOARD, ACC, MONITOR, POLICIES, OBJECTS, and DEVICE. Below the tabs, there is a search bar and a navigation menu with options like Interfaces, Zones (highlighted), and VLANs.

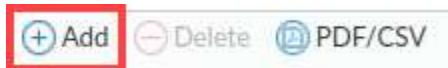
2. Click **Add** to create a new zone.



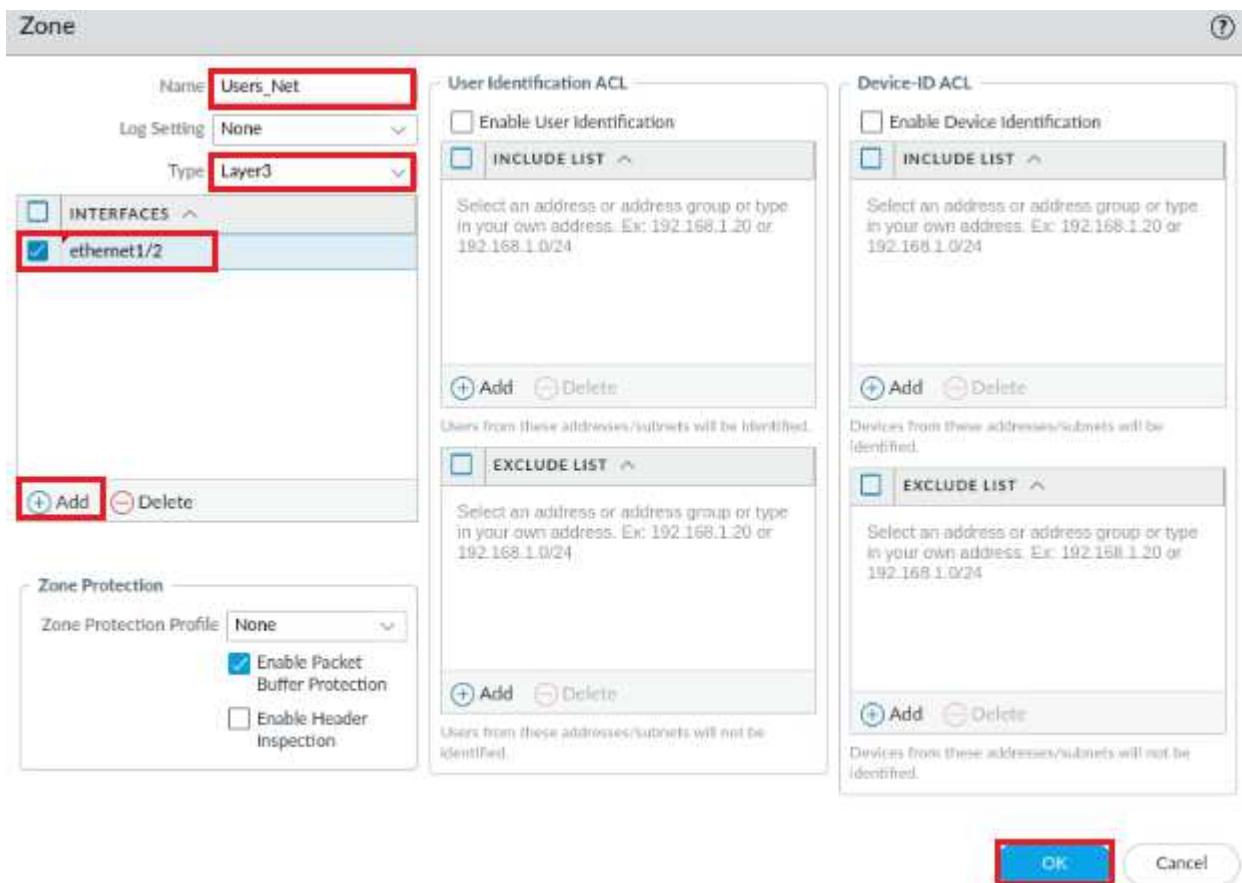
3. In the **Zone** window, enter **Internet** for the **Name**, for **Type**, select **Layer3**. Under the **Interfaces** section, click **Add**. Select **Ethernet 1/1** and leave all other settings unchanged. Click **OK**.



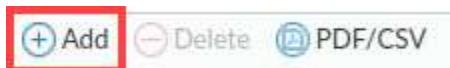
4. Click **Add** to create a new zone.



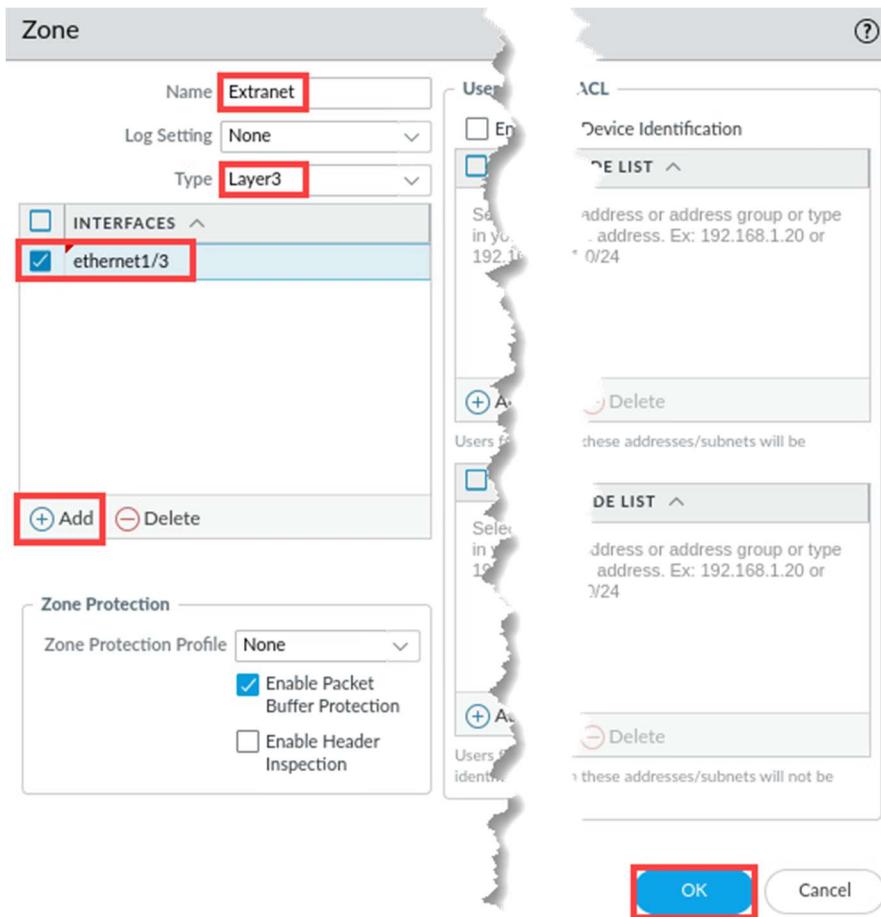
5. In the **Zone** window, enter **Users\_Net** for the **Name**, for **Type**, select **Layer3**. Under the *Interfaces* section, click **Add**. Select **Ethernet 1/2** and leave all other settings unchanged. Click **OK**.



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



7. In the **Zone** window, enter **Extranet** 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**.



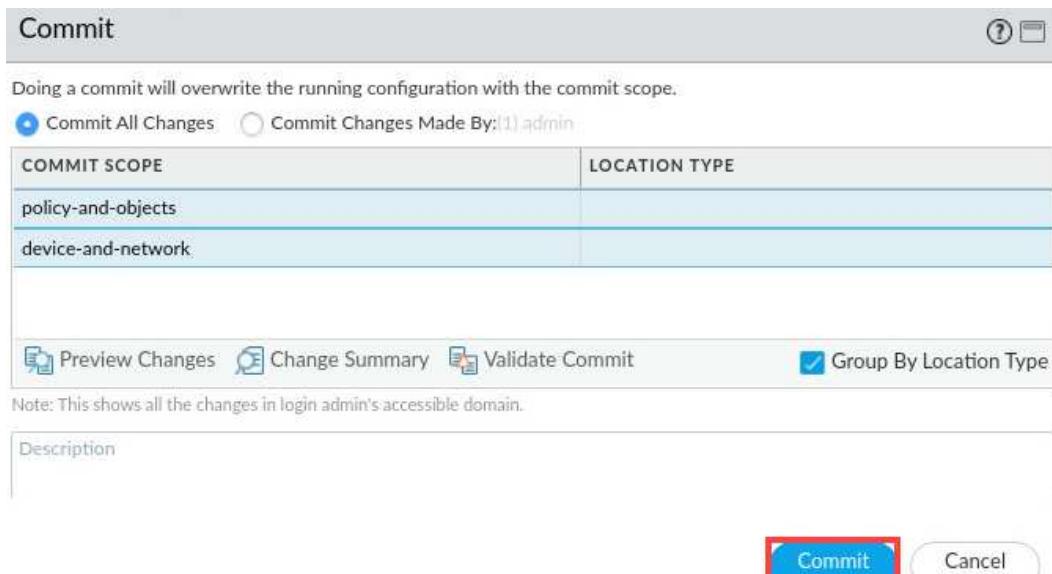
8. You should now have three security zones.

	NAME	TYPE	INTERFACES / VIRTUAL SYSTEMS	ZONE PROTECTION PROFILE	ENABLE HEADER INSPECTION	PACKET BUFFER PROTECTION	LOGGING
	Internet	layer3	ethernet1/1		<input type="checkbox"/>	<input checked="" type="checkbox"/>	
	Users_Net	layer3	ethernet1/2		<input type="checkbox"/>	<input checked="" type="checkbox"/>	
	Extranet	layer3	ethernet1/3		<input type="checkbox"/>	<input checked="" type="checkbox"/>	

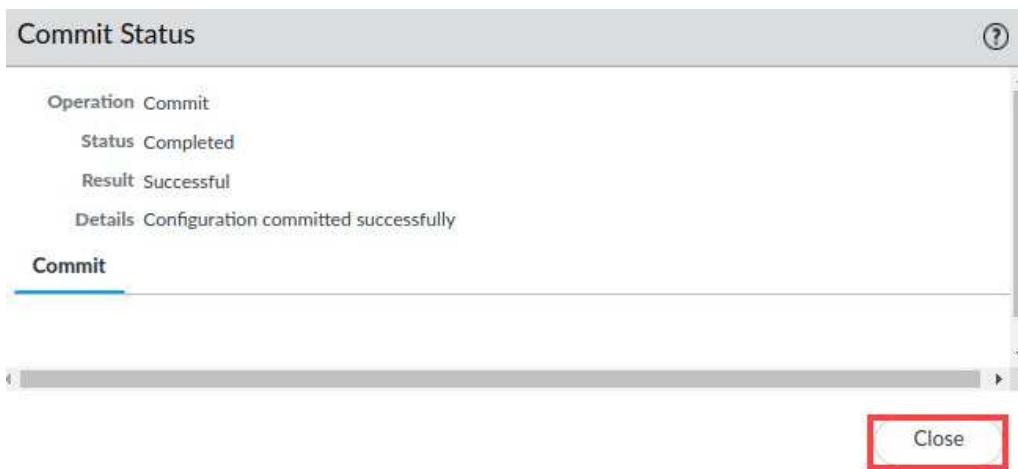
9. Click the **Commit** button at the upper right of the **PA-VM** web interface.



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



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



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.



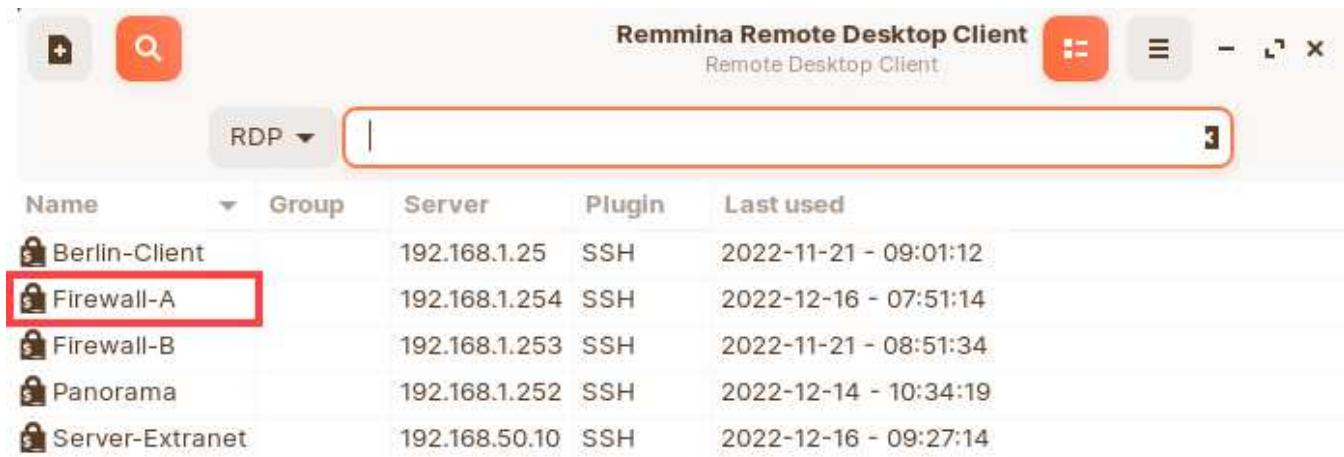
## 2.5 Test Connectivity to Each Zone

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**.



The screenshot shows the Remmina Remote Desktop Client window. At the top, there are icons for adding a new connection (+), searching (magnifying glass), and closing (X). The title bar reads "Remmina Remote Desktop Client" and "Remote Desktop Client". Below the title bar, there is a dropdown menu set to "RDP" and a search bar with a placeholder " ". The main area displays a table of connections:

Name	Group	Server	Plugin	Last used
Berlin-Client		192.168.1.25	SSH	2022-11-21 - 09:01:12
<b>Firewall-A</b>		192.168.1.254	SSH	2022-12-16 - 07:51:14
Firewall-B		192.168.1.253	SSH	2022-11-21 - 08:51:34
Panorama		192.168.1.252	SSH	2022-12-14 - 10:34:19
Server-Extranet		192.168.50.10	SSH	2022-12-16 - 09:27:14

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.

3. In the CLI connection to the firewall, use the **ping** command to check network connectivity to a host in the *Users\_Net Security Zone* by using the following command at the **admin@firewall-a>** prompt. Press **Enter**.

```
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.

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

```

Firewall-A
File Firewall-A x
Last login: Thu Jul 20 03:54:16 2023
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=14.4 ms
64 bytes from 192.168.1.20: icmp_seq=2 ttl=64 time=1.100 ms
64 bytes from 192.168.1.20: icmp_seq=3 ttl=64 time=2.08 ms
64 bytes from 192.168.1.20: icmp_seq=4 ttl=64 time=0.857 ms
64 bytes from 192.168.1.20: icmp_seq=5 ttl=64 time=1.00 ms
64 bytes from 192.168.1.20: icmp_seq=6 ttl=64 time=0.945 ms
64 bytes from 192.168.1.20: icmp_seq=7 ttl=64 time=0.992 ms
64 bytes from 192.168.1.20: icmp_seq=8 ttl=64 time=0.957 ms
64 bytes from 192.168.1.20: icmp_seq=9 ttl=64 time=0.704 ms
64 bytes from 192.168.1.20: icmp_seq=10 ttl=64 time=1.98 ms
64 bytes from 192.168.1.20: icmp_seq=11 ttl=64 time=1.17 ms
64 bytes from 192.168.1.20: icmp_seq=12 ttl=64 time=1.77 ms
--- 192.168.1.20 ping statistics ---
12 packets transmitted, 12 received, 0% packet loss, time 96ms
rtt min/avg/max/mdev = 0.704/2.406/14.423/3.655 ms
admin@firewall-a>

```

- 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. Press **Enter**.

```
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.

6. 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
```

7. 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.

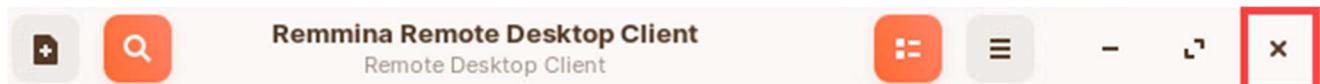
8. Allow the *ping* to continue for three or four seconds and then use **Ctrl+C** to interrupt the command. Notice the *pings* are successful.

```
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
```

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



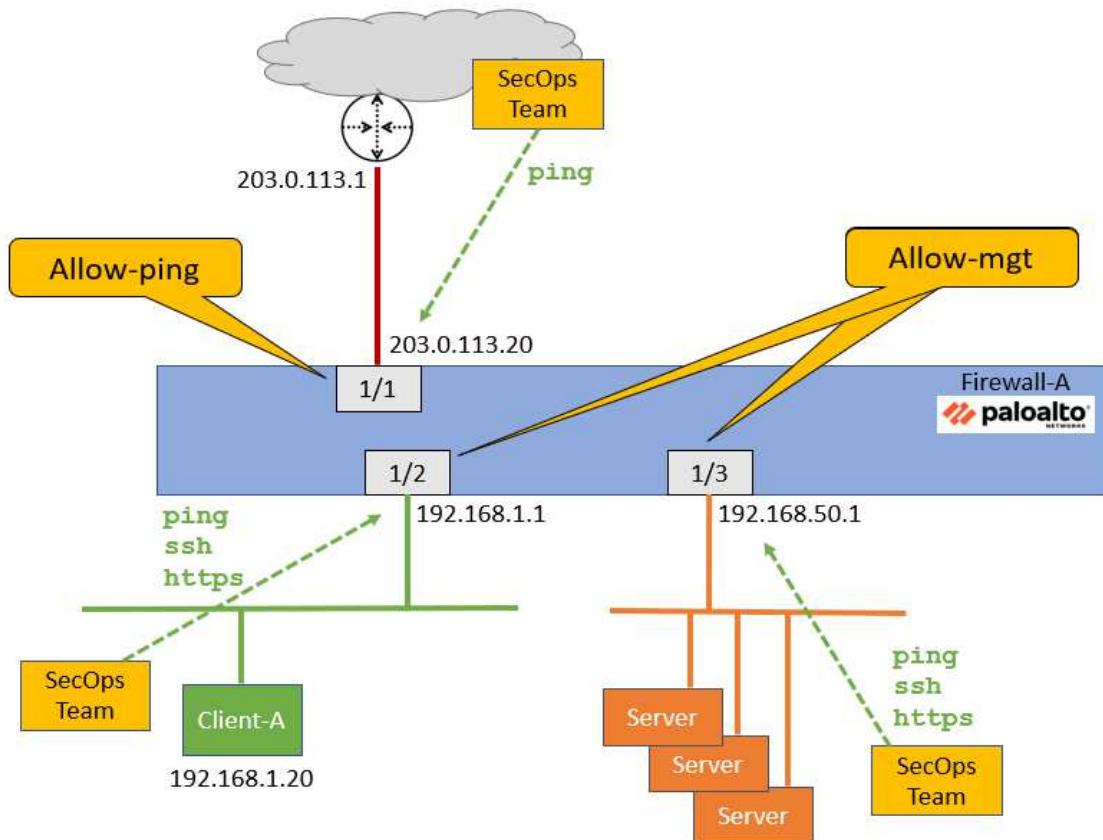
10. Close the *Remmina Remote Desktop Client* by clicking on the **close** icon in the upper right.



11. Stay on the *Client* desktop and continue to the next task.

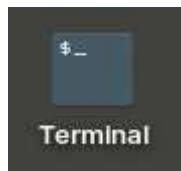
## 2.6 Test Interface Access before Management Profiles

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



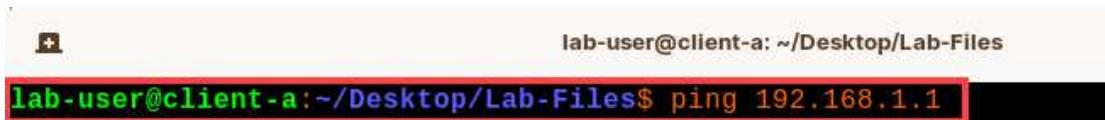
To illustrate the default behavior of firewall interfaces, you will ping 192.168.1.1 from the client workstation. You will also attempt to access the firewall CLI by SSH through 192.168.1.1. Without any Interface Management Profiles in place, both ping and SSH will fail.

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



2. Issue the following command below.

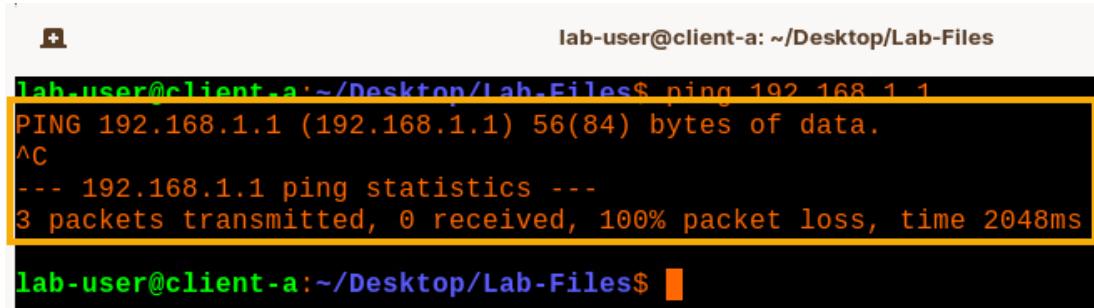
```
lab-user@client-a:~/Desktop/Lab-Files$ ping 192.168.1.1 <Enter>
```



A screenshot of a terminal window titled "lab-user@client-a: ~/Desktop/Lab-Files". The command "ping 192.168.1.1" is entered at the prompt. The output shows the ping command being issued but no response due to lack of configuration.

```
lab-user@client-a:~/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.

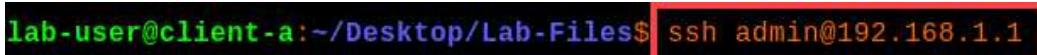


A screenshot of a terminal window titled "lab-user@client-a: ~/Desktop/Lab-Files". The command "ping 192.168.1.1" is entered. After the first line of output, "PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.", the user presses **Ctrl+C**, which is shown as '^C'. The terminal then displays ping statistics: "3 packets transmitted, 0 received, 100% packet loss, time 2048ms". Finally, the command is completed with "lab-user@client-a:~/Desktop/Lab-Files\$".

```
lab-user@client-a:~/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 ---
3 packets transmitted, 0 received, 100% packet loss, time 2048ms
lab-user@client-a:~/Desktop/Lab-Files$
```

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

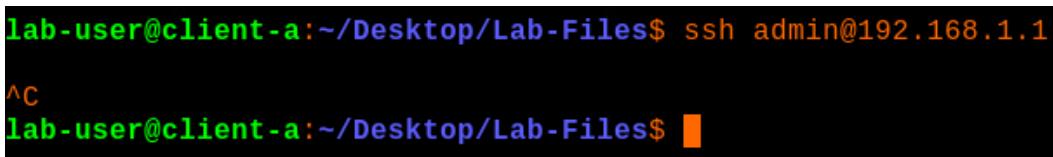
```
lab-user@client-a:~/Desktop/Lab-Files$ ssh admin@192.168.1.1 <Enter>
```



A screenshot of a terminal window titled "lab-user@client-a: ~/Desktop/Lab-Files". The command "ssh admin@192.168.1.1" is entered at the prompt. The output shows the connection attempt failing.

```
lab-user@client-a:~/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.



A screenshot of a terminal window titled "lab-user@client-a: ~/Desktop/Lab-Files". The command "ssh admin@192.168.1.1" is entered. After the first line of output, "lab-user@client-a:~/Desktop/Lab-Files\$ ssh admin@192.168.1.1", the user presses **Ctrl+C**, which is shown as '^C'. The terminal then displays the command again: "lab-user@client-a:~/Desktop/Lab-Files\$".

```
lab-user@client-a:~/Desktop/Lab-Files$ ssh admin@192.168.1.1
^C
lab-user@client-a:~/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.

## 2.7 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 Users\_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.

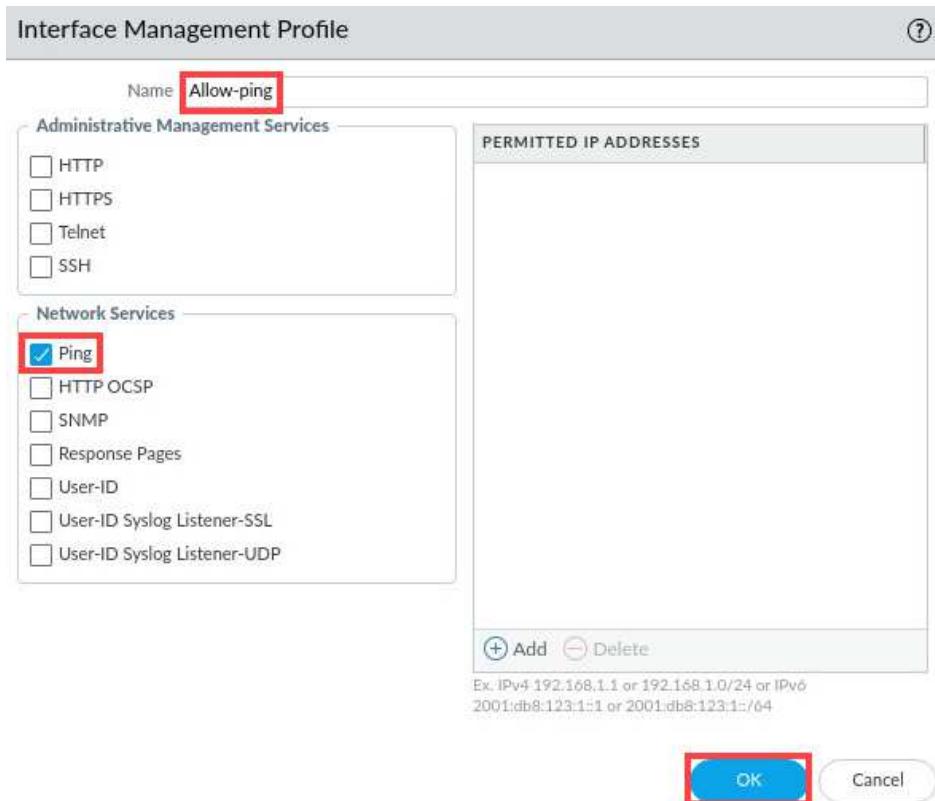
1. Re-open the PA-VM *firewall-a* web interface by clicking on the **firewall-a – Mozilla Firefox** icon in the task bar.



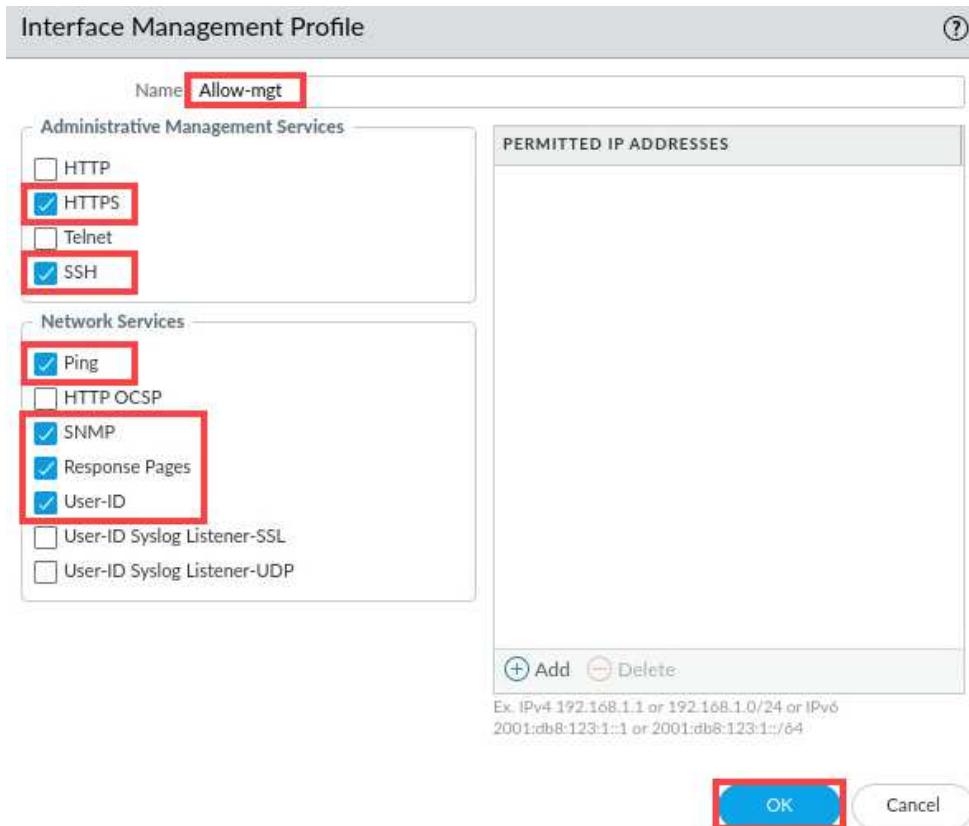
2. Select **Network > Network Profiles > Interface Management**. Click **Add** at the bottom of the window.

NAME	PING	TELNET	SSH	HTTP	HTTP OCSP	HTTPS

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**.



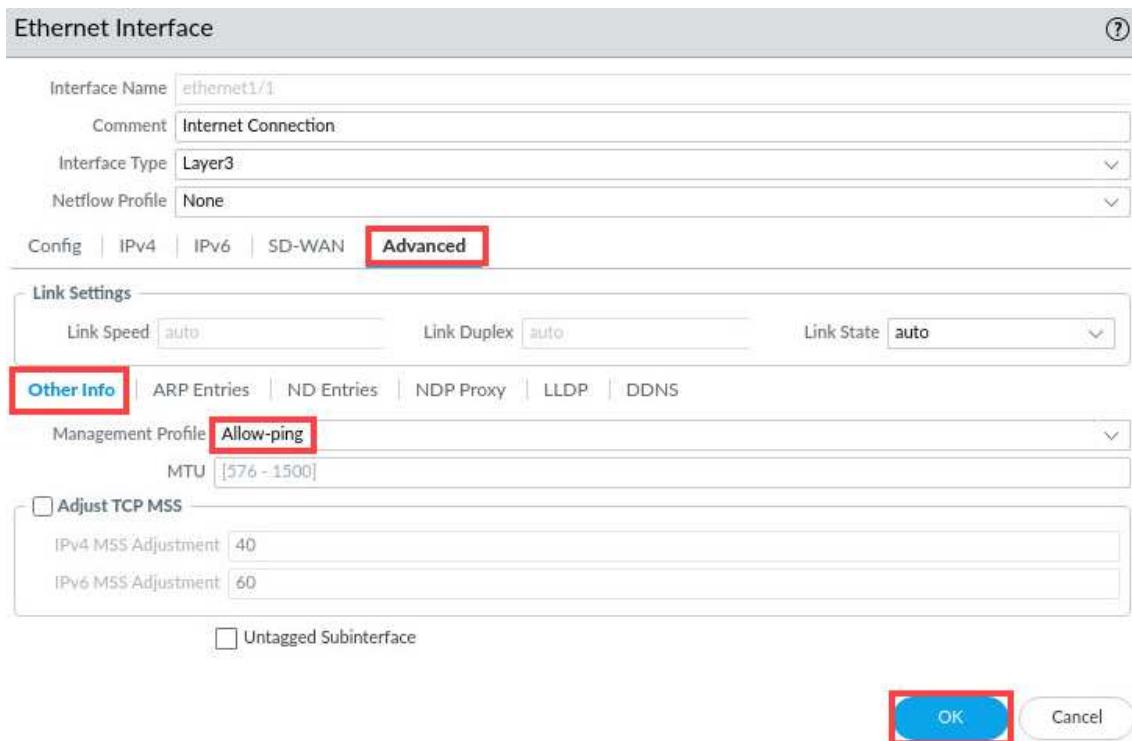
4. In the *Interface Management* section, click **Add** again to create another entry. In the *Interface Management Profile* window, enter **Allow-mgt** for the **Name**. Under the *Administrative Management Services* section, check the boxes for **HTTPS** and **SSH**. Under the section for *Network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



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

INTERFACE	INTERFACE TYPE	MANAGEMENT PROFILE	LINK STATE	IP ADDRESS
ethernet1/1	Layer3		<span style="color: green;">online</span>	203.0.113.20/24
ethernet1/2	Layer3		<span style="color: green;">online</span>	192.168.1.1/24
ethernet1/3	Layer3		<span style="color: green;">online</span>	192.168.50.1/24

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



**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
ethernet1/1	Layer3	Allow-ping	Up	203.0.113.20/24
ethernet1/2	Layer3		Up	192.168.1.1/24
ethernet1/3	Layer3		Up	192.168.50.1/24

8. In the *Ethernet 1/2* window, click **Advanced**. Under the *Other Info* section, use the drop-down list for *Management Profile* and select **Allow-mgt**. Click **OK**.

**Ethernet Interface**

Interface Name: ethernet1/2

Comment: Users network 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-mgt**

MTU: [576 - 1500]

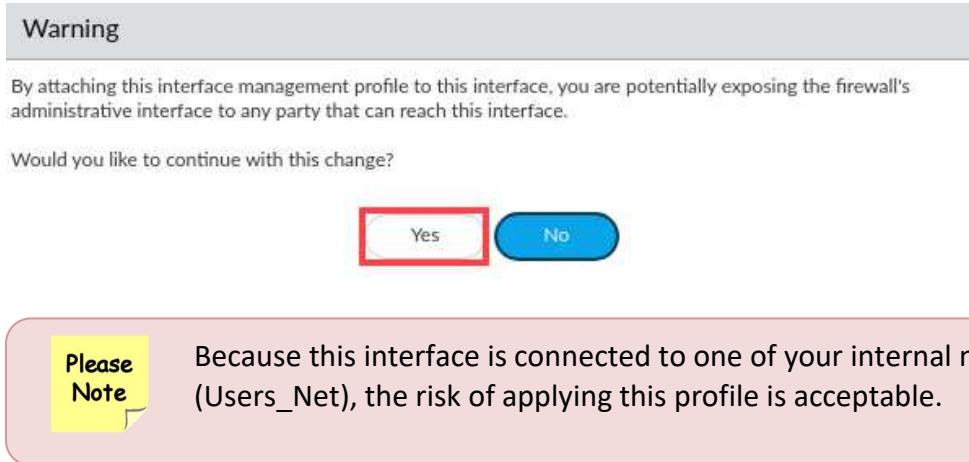
Adjust TCP MSS

IPv4 MSS Adjustment: 40 | IPv6 MSS Adjustment: 60

Untagged Subinterface

**OK** | Cancel

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



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

The screenshot shows the PA-VM interface list under the NETWORK tab. The left sidebar has a tree view with 'Interfaces' selected. The main area shows a table with columns: INTERFACE, INTERFACE TYPE, MANAGEMENT PROFILE, LINK STATE, and IP ADDRESS. The table contains three rows:

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

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

The screenshot shows the 'Ethernet Interface' configuration window for 'ethernet1/3'. The top navigation bar includes tabs for Config, IPv4, IPv6, SD-WAN, and Advanced (which is highlighted with a red box). Below this is a 'Link Settings' group with fields for Link Speed (auto), Link Duplex (auto), and Link State (auto). A 'Link Layer Discovery Protocol (LLDP)' section is also present. The 'Other Info' tab is selected (highlighted with a red box) and shows a Management Profile dropdown set to 'Allow-mgt' (also highlighted with a red box). Other options in this section include ARP Entries, ND Entries, NDP Proxy, and DDNS. Below these are fields for MTU (576 - 1500) and Adjust TCP MSS (with sub-fields for IPv4 and IPv6 MSS Adjustment). At the bottom right are 'OK' and 'Cancel' buttons, with 'OK' being highlighted with a red box.

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



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	

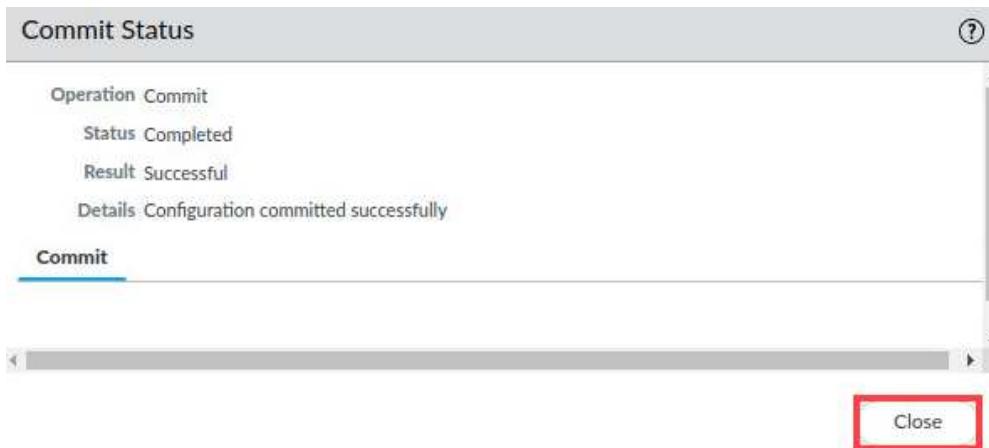
Preview Changes Change Summary Validate Commit  Group By Location Type

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

Description

**Commit** **Cancel**

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



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



## 2.8 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 *lab-user@client-a* terminal window used previously in the *Client* taskbar.



2. Issue the following command below.

```
lab-user@client-a:~/Desktop/Lab-Files$ ping 192.168.1.1 <Enter>
```



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

```
lab-user@client-a:~/Desktop/Lab-Files$ ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=10.2 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=1.51 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=64 time=0.871 ms
^C
--- 192.168.1.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 0.871/4.179/10.153/4.232 ms
lab-user@client-a:~/Desktop/Lab-Files$
```

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

```
lab-user@client-a:~/Desktop/Lab-Files$ sudo su
```

```
lab-user@client-a:~/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**.

```
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.1' (RSA) to the list of known hosts.
```

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

```
Authorized Access Only
Password:
```

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

```
Last login: Mon Sep 11 00:57:40 2023 from 192.168.1.20

Number of failed attempts since last successful login:

There have been failed attempted logins from your username, which could mean someone is trying to
brute-force your login. If this is not expected, consider contacting your system administrator.

admin@firewall-a>
```

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