PALO ALTO NETWORKS FIREWALL 11.0 ESSENTIALS

Lab 1: Configuring Initial Firewall Settings

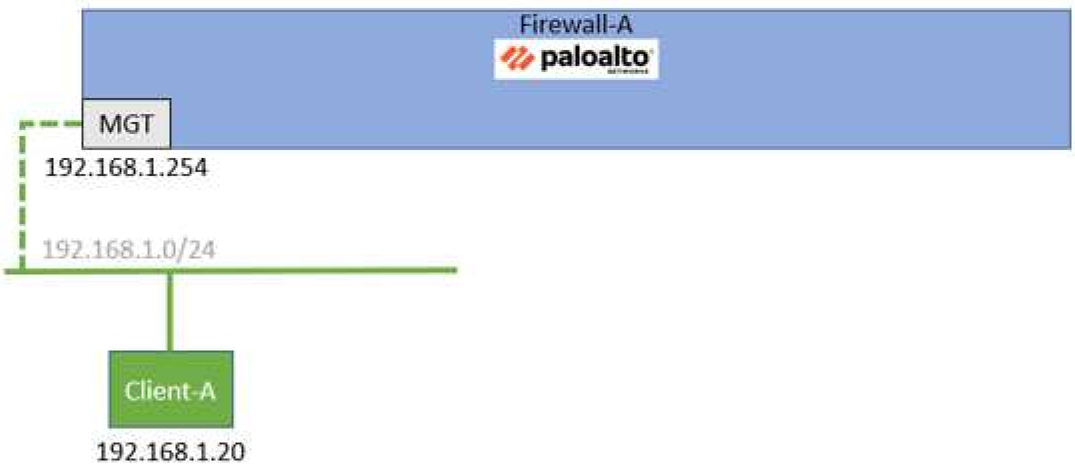
Document Version: 2025-10-13

Contents

Introduction

Your organization has just received a new Palo Alto Networks firewall, and you have been tasked with deploying it. The first steps will be to connect to the firewall's management interface address and configure basic settings to provide the firewall with network access.

This lab involves connecting to the Palo Alto Networks firewall management interface and setting up fundamental configurations to enable network access through the firewall.

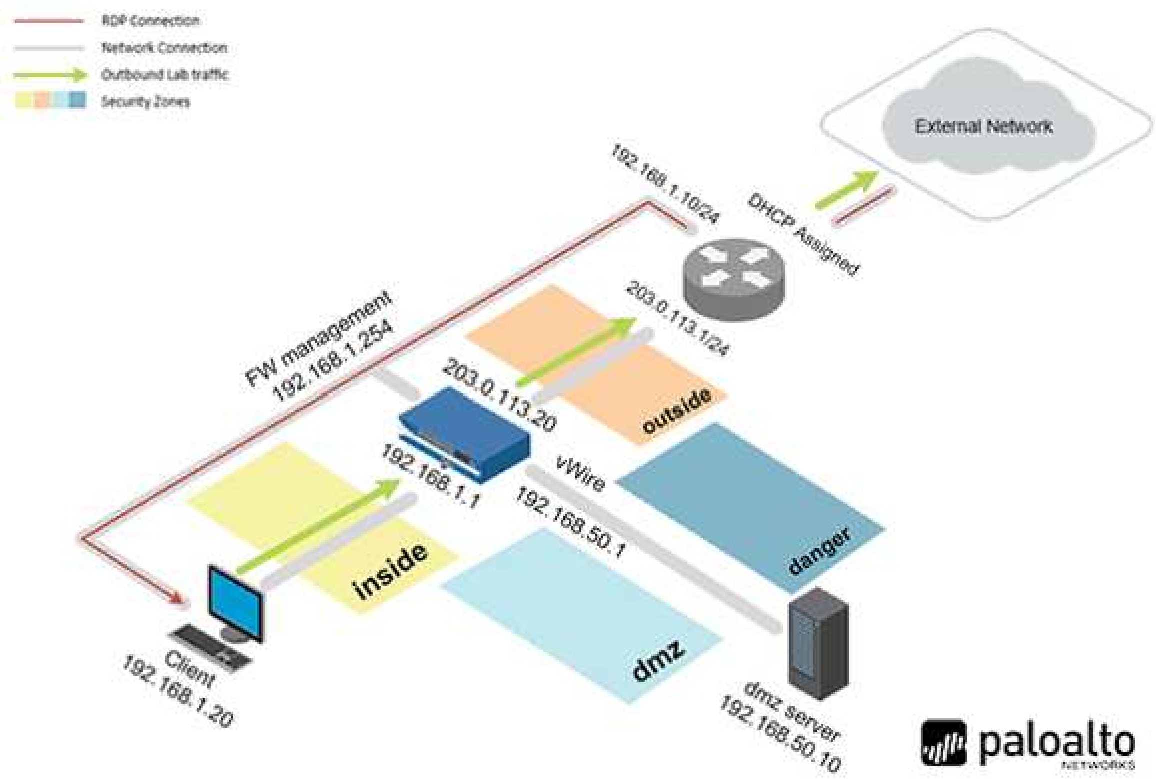


Objective

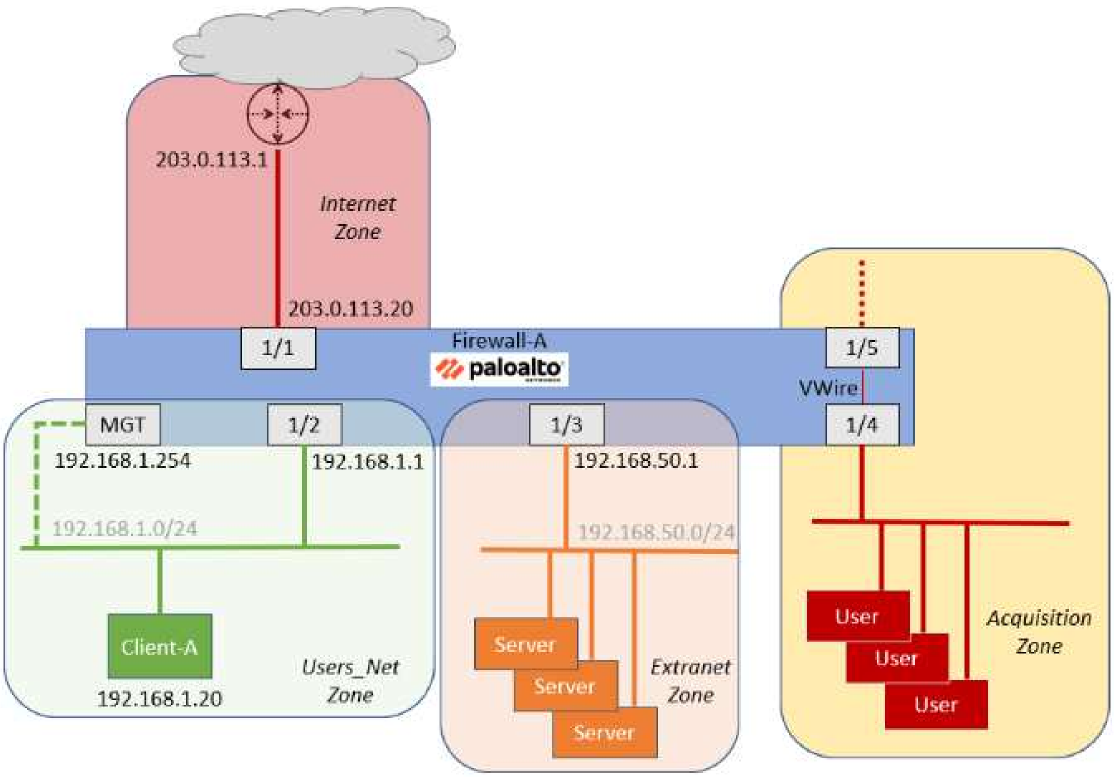
In this lab, you will perform the following tasks:

- Connect to the firewall web interface.
- Load a starting lab configuration.
- Set DNS servers for the firewall.
- Set NTP servers for the firewall.
- Configure a login banner for the firewall.
- Set Latitude and Longitude for the firewall.
- Configure permitted IP addresses for firewall management.

Lab Topology



Theoretical Lab Topology



Lab Settings

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

Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Client	**192.168.1.20**	`lab-user`	`Pal0Alt0!`
DMZ	**192.168.50.10**	`root`	`Pal0Alt0!`
Firewall	**192.168.1.254**	`admin`	`Pal0Alt0!`
vRouter	**192.168.1.10**	`root`	`Pal0Alt0`

Lab Guidance

There are two sections in this lab guide:

- Detailed Lab Steps
- High-Level Lab Steps

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

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.

If you decide to use the High-Level Lab Steps and get stuck, switch to the Detailed Lab Steps 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 Configuring Initial Firewall Settings – 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-01.xml** to the Firewall.

1.2 Configure the DNS and NTP Servers

- Set the **Primary DNS** Server to **8.8.8.8** and the **Secondary DNS Server** to **192.168.50.53.**
- Set the **Primary NTP Server** to **0.pool.ntp.org** and the **Secondary NTP Server** to **1.pool.ntp.org.**

1.3 Configure General Settings

- Set the **Domain** to **lab.local.**
- Create a **Login Banner** that says **Authorized Access Only.**
- Set the **Latitude** and **Longitude** to reflect the firewall's geographical location in **Santa Clara, CA, USA.**

1.4 Modify Management Interface

- Verify that the default gateway for the firewall management interface is set to **192.168.1.1.**
- Allow access to the management interface only from the **192.168.1.20/24** network.

1.5 Commit the Configuration

- Commit the changes to the firewall before proceeding.

1.6 Check for New PAN-OS Software

- Check for new PAN-OS software (but do not upgrade the firewall).

2 Configuring Initial Firewall Settings – Detailed Lab Steps

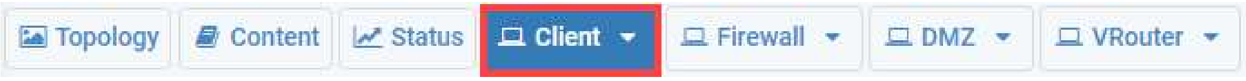
It is recommended to use this section if you prefer detailed guidance to complete the objectives for this lab. It is strongly recommended that you use this section if you do not have extensive experience working with Palo Alto Networks firewalls.

Your organization has just received a new Palo Alto Networks firewall, and you have been tasked with deploying it. The first steps will be to connect to the firewall's management interface address and configure basic settings to provide the firewall with network access.

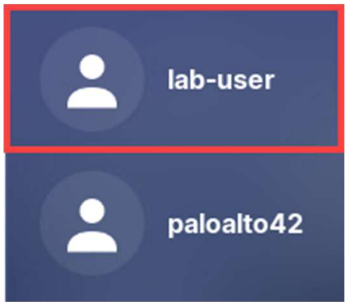
2.1 Load Lab Configuration

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

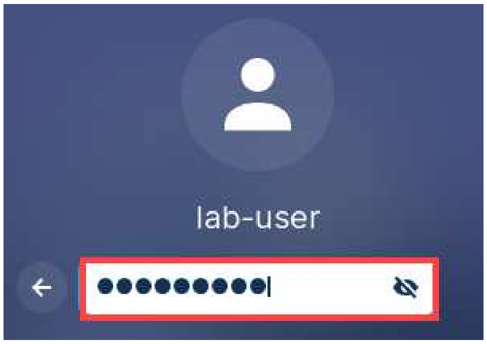
1. Click on the **Client** tab to access the Client PC.



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

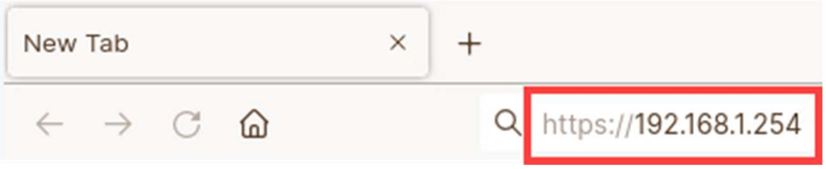


3. For the *lab-user* password, enter **Pal0Alt0!** and press **Enter**.

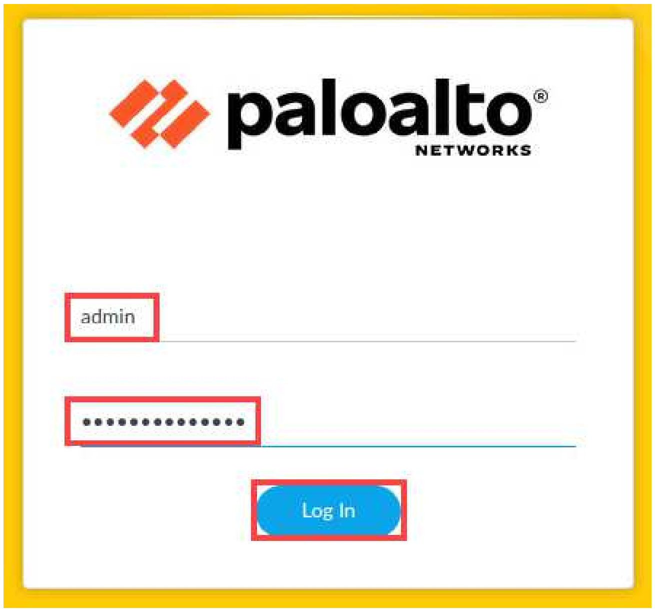


4. Double-click the **Firefox Web Browser** icon located on the *Desktop*.

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

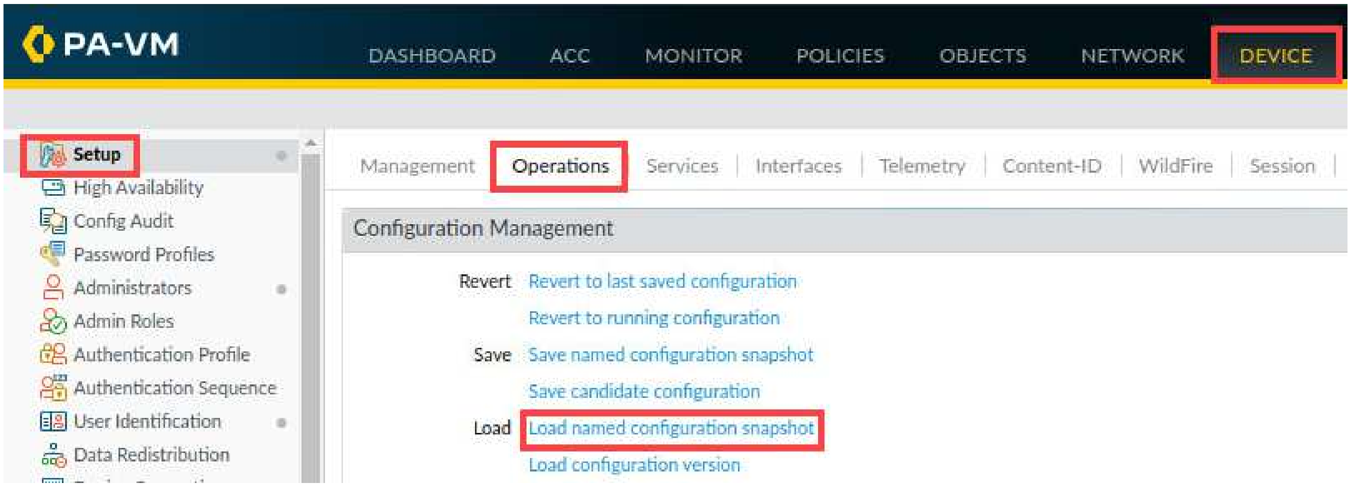


6. Log in to the Firewall web interface as username **`admin`**, password **`Pal0Alt0!.`**

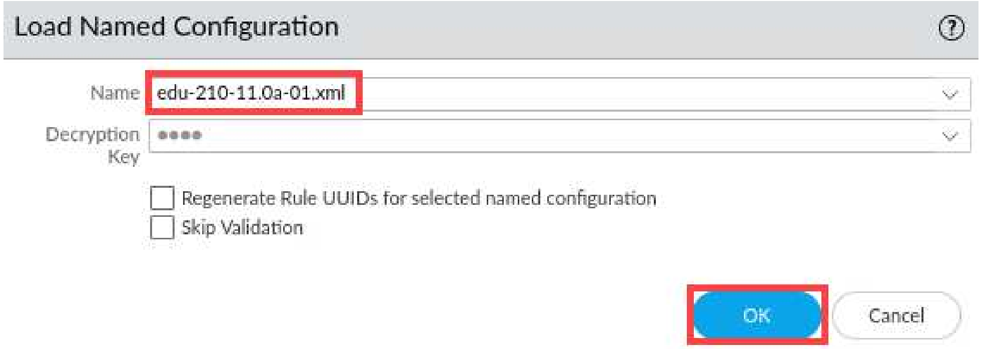


If you do not immediately see the login page, please wait an additional 1-3 minutes for the *Firewall* to fully initialize. If needed, refresh the page.

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-01.xml** from the *Name* drop-down box and click **OK**.


Load Named Configuration

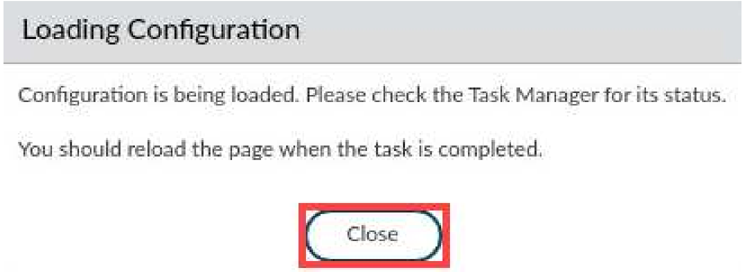
Name: edu-210-11.0a-01.xml

Decryption Key: ••••

□ Regenerate Rule UUIDs for selected named configuration

□ Skip Validation

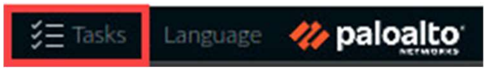
9. In the *Loading Configuration* window, a message will show *Configuration is being loaded*. *Please check the Task Manager for its status. You should reload the page when the task is completed.* Click **Close** to continue.


Loading Configuration

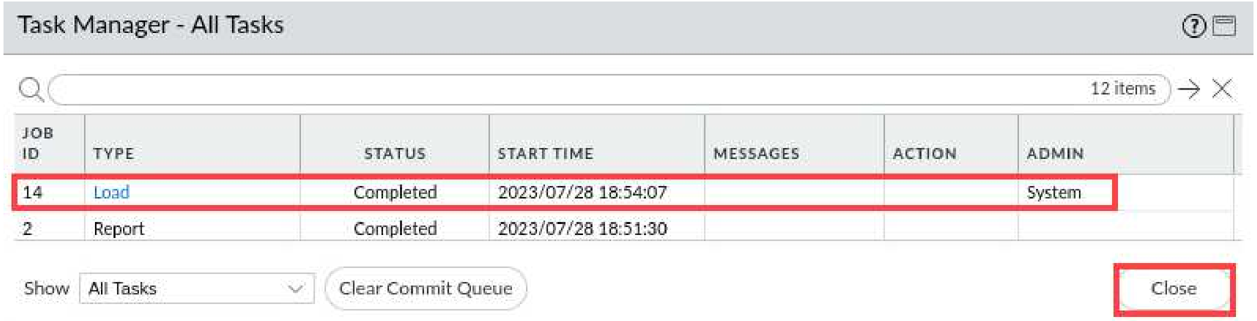
Configuration is being loaded. Please check the Task Manager for its status.

You should reload the page when the task is completed.

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**

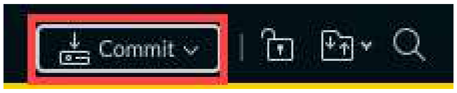


Task Manager - All Tasks

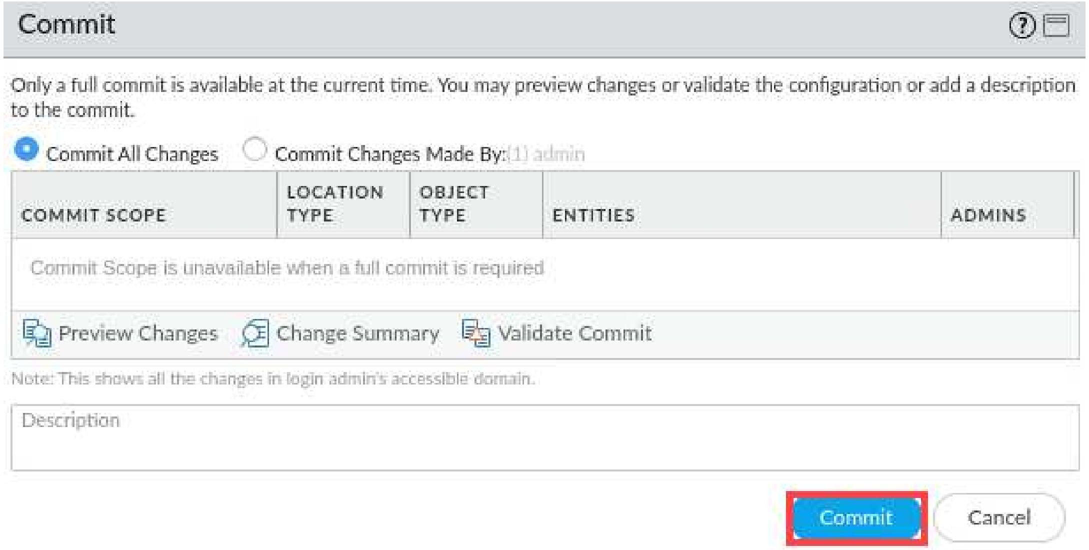
12 items

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			

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

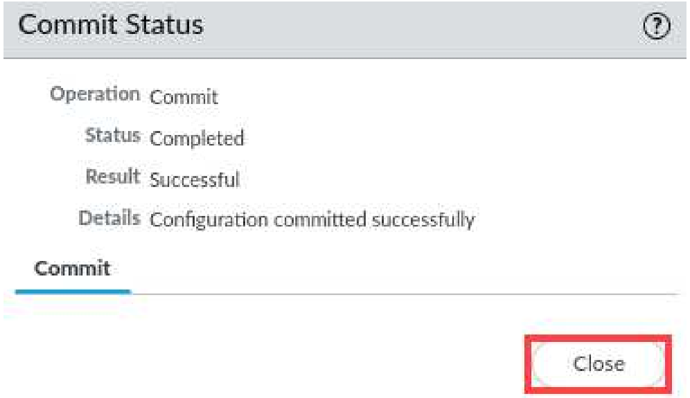
Only a full commit is available at the current time. You may preview changes or validate the configuration or add a description to the commit.

● 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				

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

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



Commit Status

Operation Commit
Status Completed
Result Successful
Details Configuration committed successfully

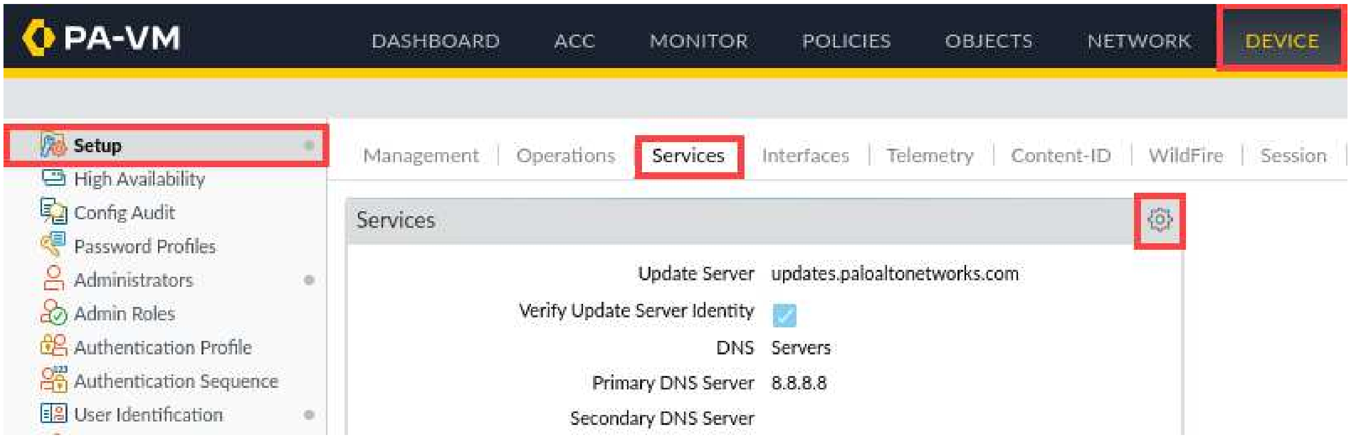
The commit process takes changes made to the Firewall and copies them to the running configuration, which will activate all configuration changes since the last commit.

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

2.2 Configure the DNS and NTP Servers

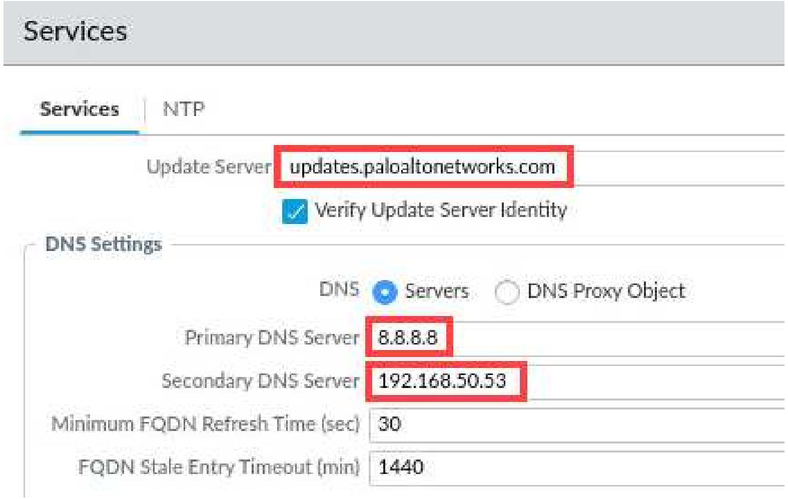
In this section, you will configure the DNS and Update Server settings. The DNS server configuration settings are used for all DNS queries that the firewall initiates in support of FQDN Address objects, logging, and firewall management.

1. In the web interface, select **Device > Setup > Services**. Click the **Services gear** icon to open the *Services* window.



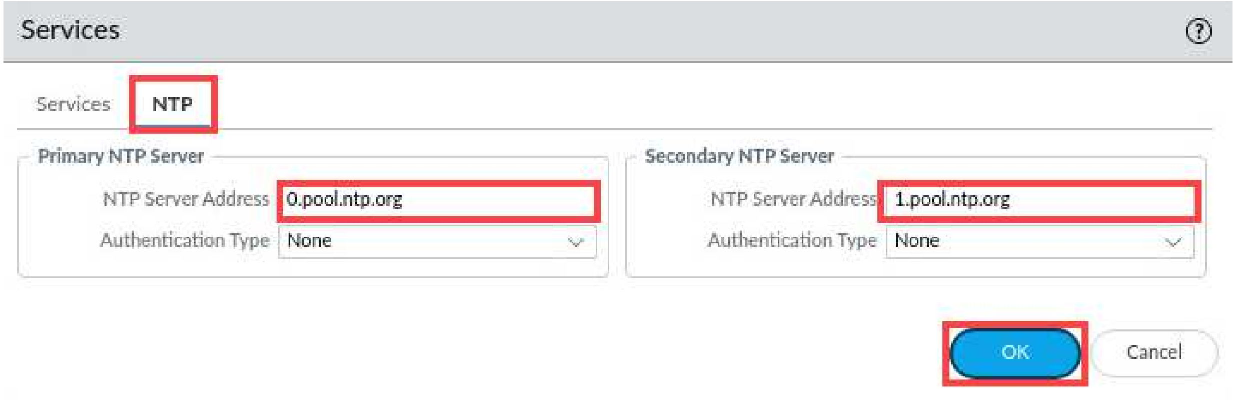
Update Server updates.paloaltonetworks.com
Verify Update Server Identity ☑
DNS Servers
Primary DNS Server 8.8.8.8
Secondary DNS Server

2. In the *Services* window, verify that the *Update Server* is set to **`updates.paloaltonetworks.com`**. Set the *Primary DNS Server* to **`8.8.8.8`** and the *Secondary DNS Server* to **`192.168.50.53`**.



Update Server updates.paloaltonetworks.com
☑ Verify Update Server Identity
DNS ● Servers ○ DNS Proxy Object
Primary DNS Server 8.8.8.8
Secondary DNS Server 192.168.50.53
Minimum FQDN Refresh Time (sec) 30
FQDN Stale Entry Timeout (min) 1440

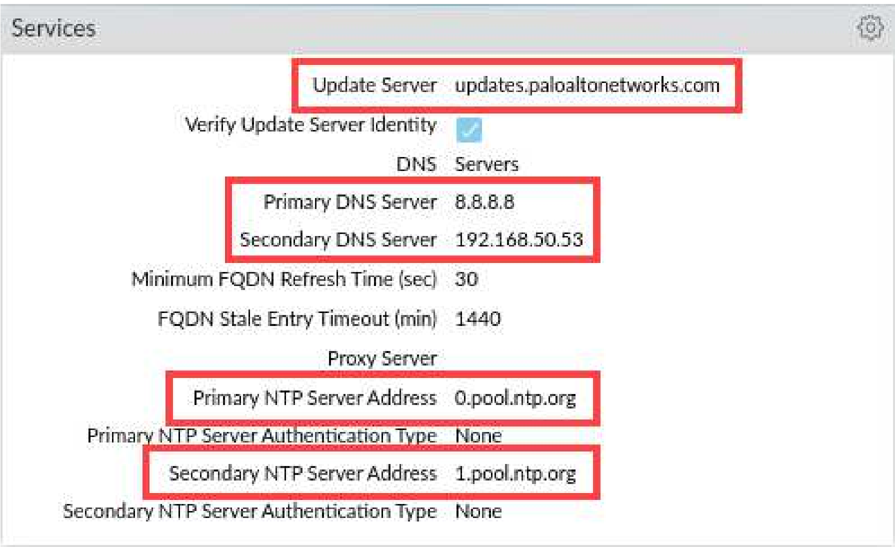
3. Select the **NTP** tab. Set the *Primary NTP Server* to **`0.pool.ntp.org`** and the *Secondary NTP Server* to **`1.pool.ntp.org`**. Click **OK**.



Primary NTP Server
NTP Server Address: 0.pool.ntp.org
Authentication Type: None

Secondary NTP Server
NTP Server Address: 1.pool.ntp.org
Authentication Type: None

4. Verify the settings have been updated in the *Services* window.



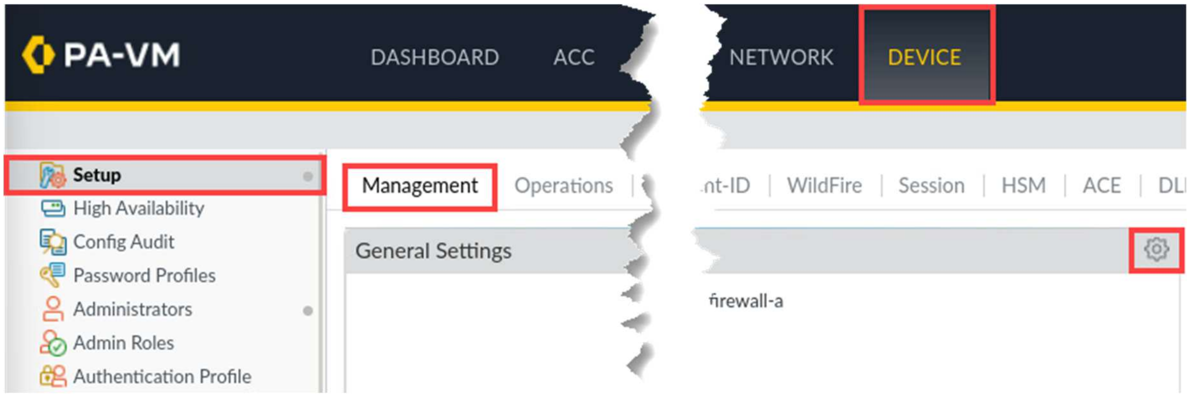
Update Server	updates.paloaltonetworks.com
Verify Update Server Identity	✓
DNS	Servers
Primary DNS Server	8.8.8.8
Secondary DNS Server	192.168.50.53
Minimum FQDN Refresh Time (sec)	30
FQDN Stale Entry Timeout (min)	1440
Proxy Server	
Primary NTP Server Address	0.pool.ntp.org
Primary NTP Server Authentication Type	None
Secondary NTP Server Address	1.pool.ntp.org
Secondary NTP Server Authentication Type	None

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

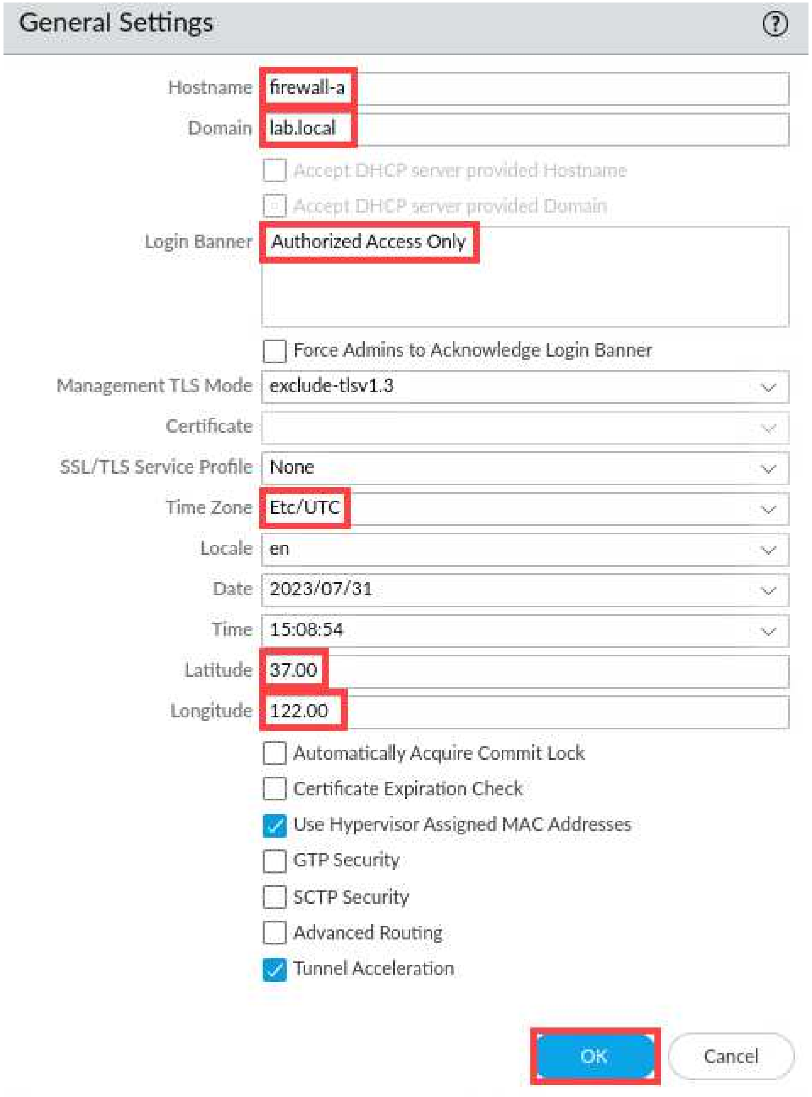
2.3 Configure General Settings

In this section, you will configure the general settings of the Palo Alto Networks Firewall. You will verify the Domain, set your location's time zone, and configure the Latitude and Longitude that aligns with the coordinates for Santa Clara, California which is the headquarters of Palo Alto Networks, Inc.

1. In the web interface, select **Device > Setup > Management**. Click the **Services gear** icon to open the *General Settings* window.



2. In the *General Settings* window, verify the *Hostname* is **firewall-a**. For the *Domain*, enter **lab.local**. For the *Login Banner*, enter **`Authorized Access Only`**. Choose the *Time Zone* of your location. For this lab, we chose to use **Etc/UTC** as the *Time Zone*. For the *Latitude* field, enter **37.00** and for the *Longitude* field, enter **122.00**. Click **OK**.



General Settings

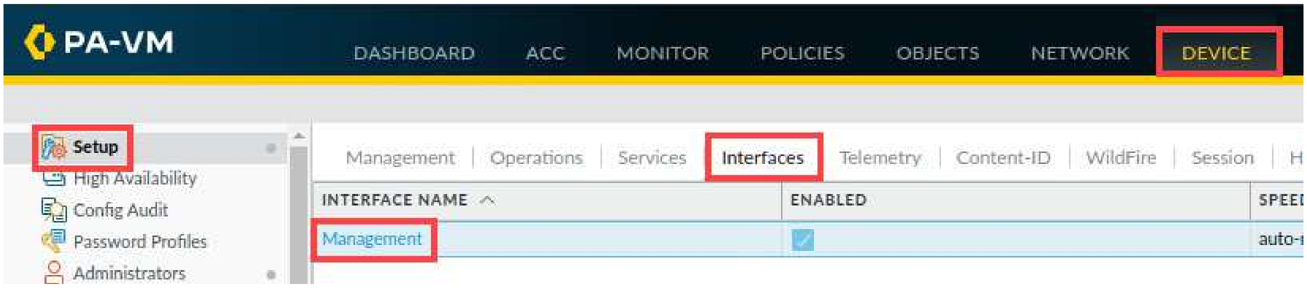
Hostname	firewall-a
Domain	lab.local
	□ Accept DHCP server provided Hostname
	□ Accept DHCP server provided Domain
Login Banner	Authorized Access Only
	□ Force Admins to Acknowledge Login Banner
Management TLS Mode	exclude-tlsv1.3
Certificate	
SSL/TLS Service Profile	None
Time Zone	Etc/UTC
Locale	en
Date	2023/07/31
Time	15:08:54
Latitude	37.00
Longitude	122.00
	□ Automatically Acquire Commit Lock
	□ Certificate Expiration Check
	☑ Use Hypervisor Assigned MAC Addresses
	□ GTP Security
	□ SCTP Security
	□ Advanced Routing
	☑ Tunnel Acceleration

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

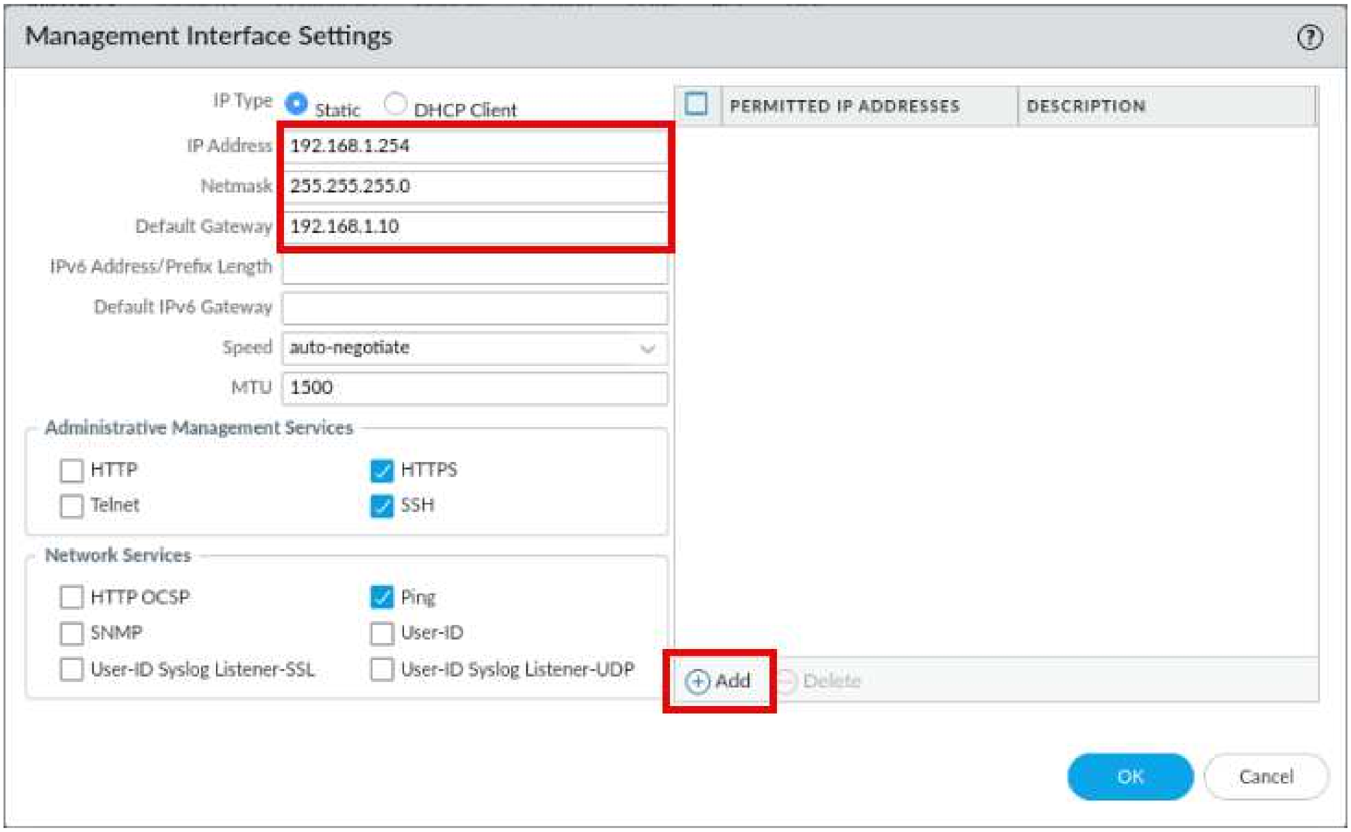
2.4 Modify the Management Interface

In this section, you will modify the management interface of the firewall.

1. Navigate to **Device > Setup > Interfaces** and click on interface name **Management**.



2. In the *Management Interface Settings* window, verify **`192.168.1.254`** for the *IP Address*, **`255.255.255.0`** for the *Netmask*, and **`192.168.1.10`** for the *Default Gateway*. At the bottom of the *Permitted IP Addresses* area, click **Add.**


Management Interface Settings

IP Type ● Static ○ DHCP Client

IP Address: 192.168.1.254

Netmask: 255.255.255.0

Default Gateway: 192.168.1.10

IPv6 Address/Prefix Length:

Default IPv6 Gateway:

Speed: auto-negotiate

MTU: 1500

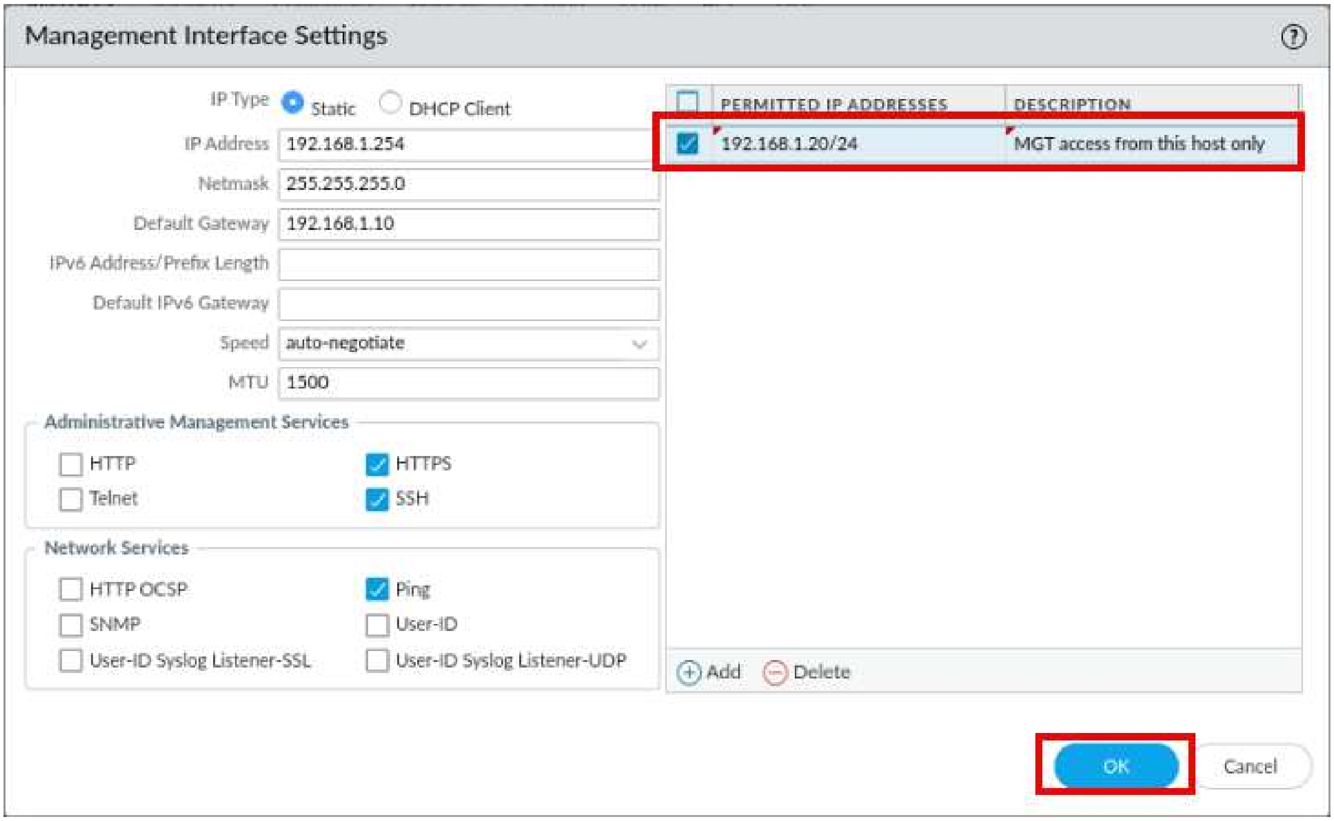
Administrative Management Services

□ HTTP ☑ HTTPS
□ Telnet ☑ SSH

Network Services

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

3. In the *Permitted IP Addresses*, type **`192.168.1.20/24`** for the *IP Address* and **`MGT access from this host only`** for the *Description*. Click **OK**.



Management Interface Settings

IP Type ● Static ○ DHCP Client

IP Address	192.168.1.254
Netmask	255.255.255.0
Default Gateway	192.168.1.10
IPv6 Address/Prefix Length	
Default IPv6 Gateway	
Speed	auto-negotiate
MTU	1500

Administrative Management Services

☐ HTTP ☑ HTTPS
☐ Telnet ☑ SSH

Network Services

☐ HTTP OCSP ☑ Ping
☐ SNMP ☐ User-ID
☐ User-ID Syslog Listener-SSL ☐ User-ID Syslog Listener-UDP

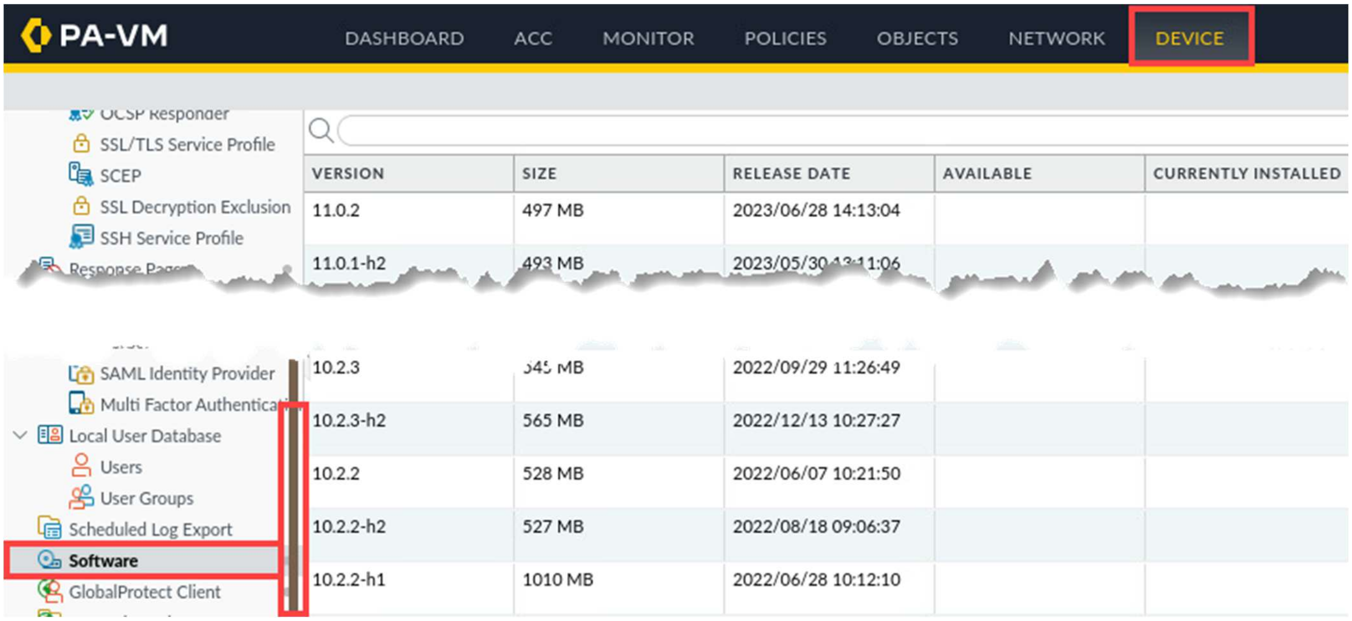
☐	PERMITTED IP ADDRESSES	DESCRIPTION
☑	192.168.1.20/24	MGT access from this host only

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

2.5 Check for New PAN-OS Software

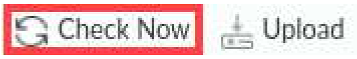
In this section, you will check for new PAN-OS software and commit your changes.

1. In the *PA-VM* web interface, navigate to **Device > Software**. If needed, use the *scroll bar* to find Software.

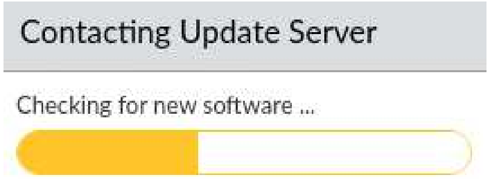


VERSION	SIZE	RELEASE DATE	AVAILABLE	CURRENTLY INSTALLED
11.0.2	497 MB	2023/06/28 14:13:04		
11.0.1-h2	493 MB	2023/05/30 13:11:06		
10.2.3	545 MB	2022/09/29 11:26:49		
10.2.3-h2	565 MB	2022/12/13 10:27:27		
10.2.2	528 MB	2022/06/07 10:21:50		
10.2.2-h2	527 MB	2022/08/18 09:06:37		
10.2.2-h1	1010 MB	2022/06/28 10:12:10		

2. In the *Software* window, click **Check Now** in the bottom left corner.

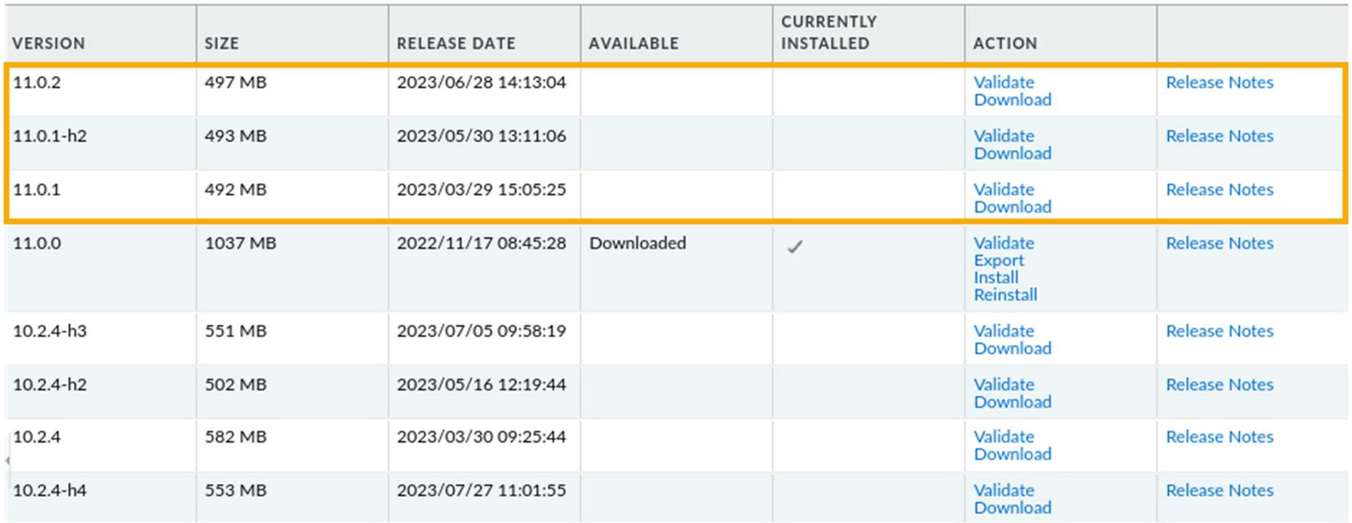


3. The Palo Alto Networks Firewall will complete a *software check*. Monitor the *software check* and when the process is complete, the firewall will display an updated list of available software.



Contacting Update Server

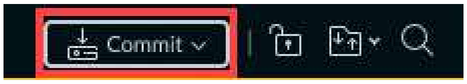
Checking for new software ...



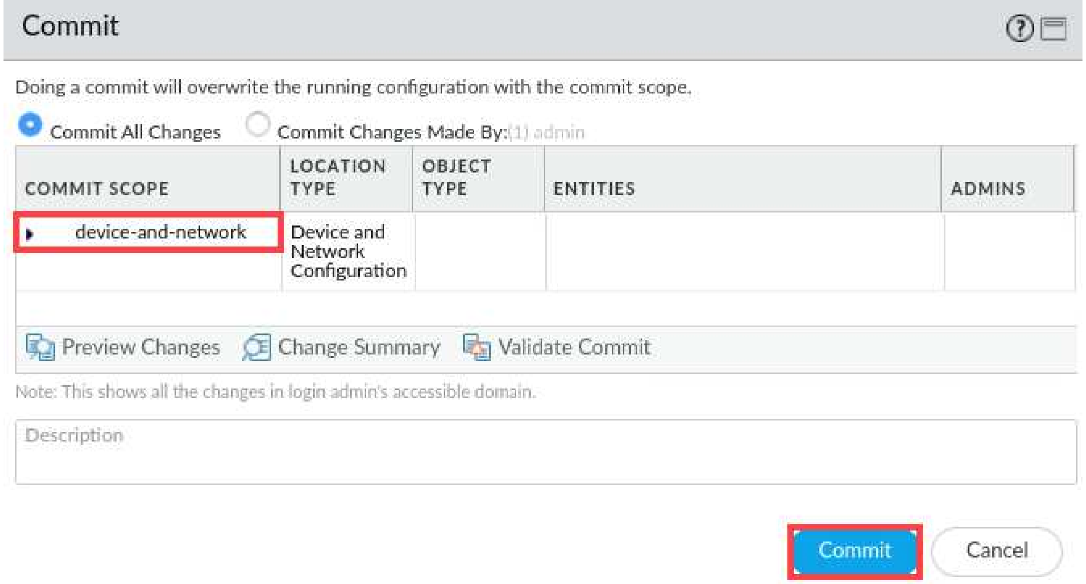
VERSION	SIZE	RELEASE DATE	AVAILABLE	CURRENTLY INSTALLED	ACTION	
11.0.2	497 MB	2023/06/28 14:13:04			Validate Download	Release Notes
11.0.1-h2	493 MB	2023/05/30 13:11:06			Validate Download	Release Notes
11.0.1	492 MB	2023/03/29 15:05:25			Validate Download	Release Notes
11.0.0	1037 MB	2022/11/17 08:45:28	Downloaded	✓	Validate Export Install Reinstall	Release Notes
10.2.4-h3	551 MB	2023/07/05 09:58:19			Validate Download	Release Notes
10.2.4-h2	502 MB	2023/05/16 12:19:44			Validate Download	Release Notes
10.2.4	582 MB	2023/03/30 09:25:44			Validate Download	Release Notes
10.2.4-h4	553 MB	2023/07/27 11:01:55			Validate Download	Release Notes

The list you see will vary from this example. Also, no newer versions of PAN-OS software may be available at the time you carry out these steps. Do not upgrade your firewall.

4. Commit your changes to the firewall by clicking the **Commit** button at the upper right of the *PA-VM* web interface.



5. In the *Commit* window, view the commit scope. Click **Commit**.



Commit

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

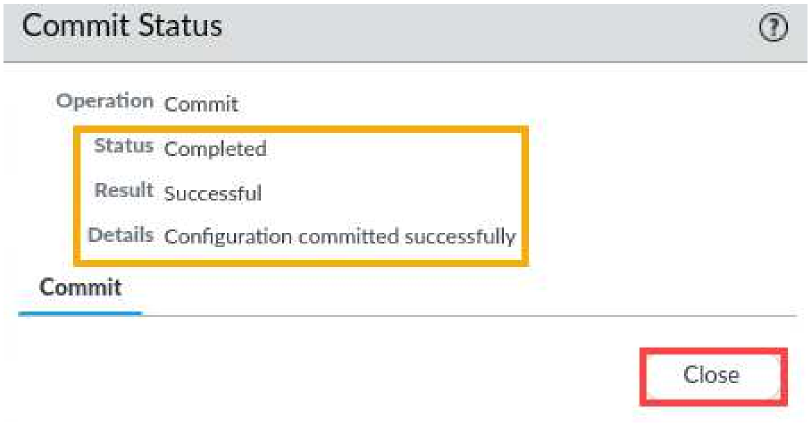
● Commit All Changes ○ Commit Changes Made By:(1) admin

COMMIT SCOPE	LOCATION TYPE	OBJECT TYPE	ENTITIES	ADMINS
device-and-network	Device and Network Configuration			

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

Description

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



Commit Status

Operation Commit

Status Completed

Result Successful

Details Configuration committed successfully

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