PALO ALTO NETWORKS – EDU 210

Lab 1: Connect to the Management Network

Document Version: 2021-09-27

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.

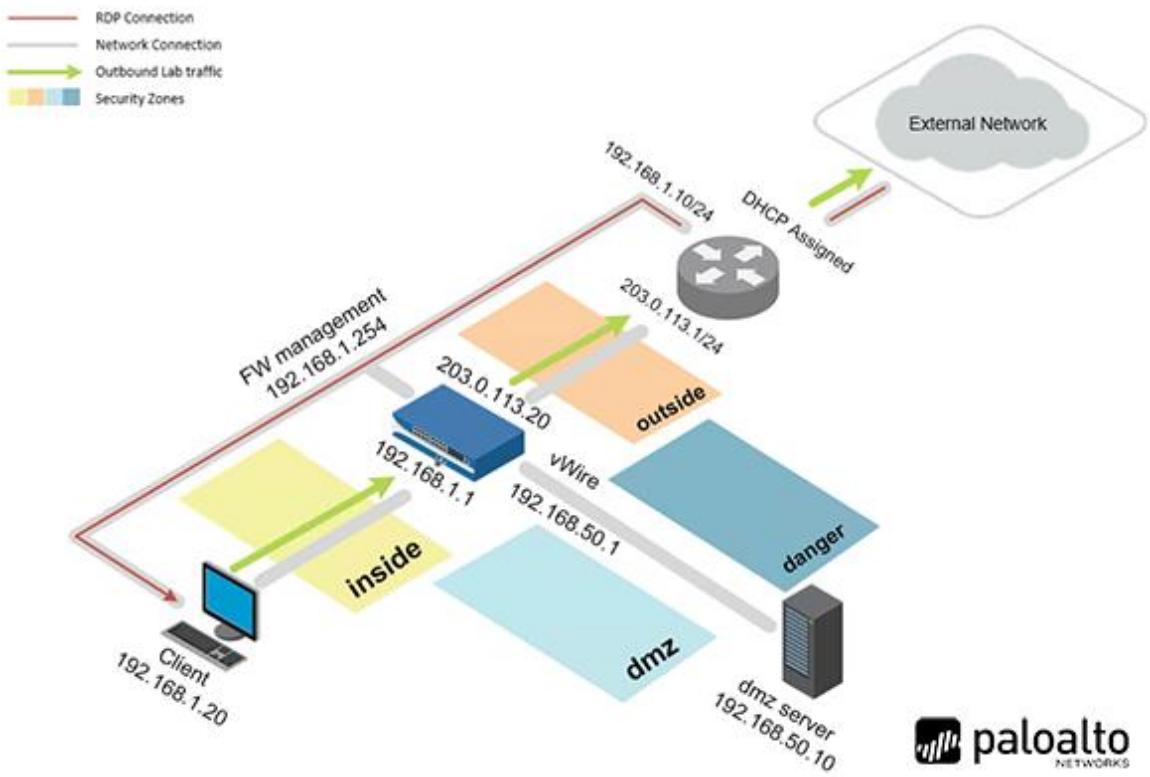
In this lab, you will connect to the Palo Alto Networks firewall management interface and configure basic settings to provide the firewall with network access.

Objective

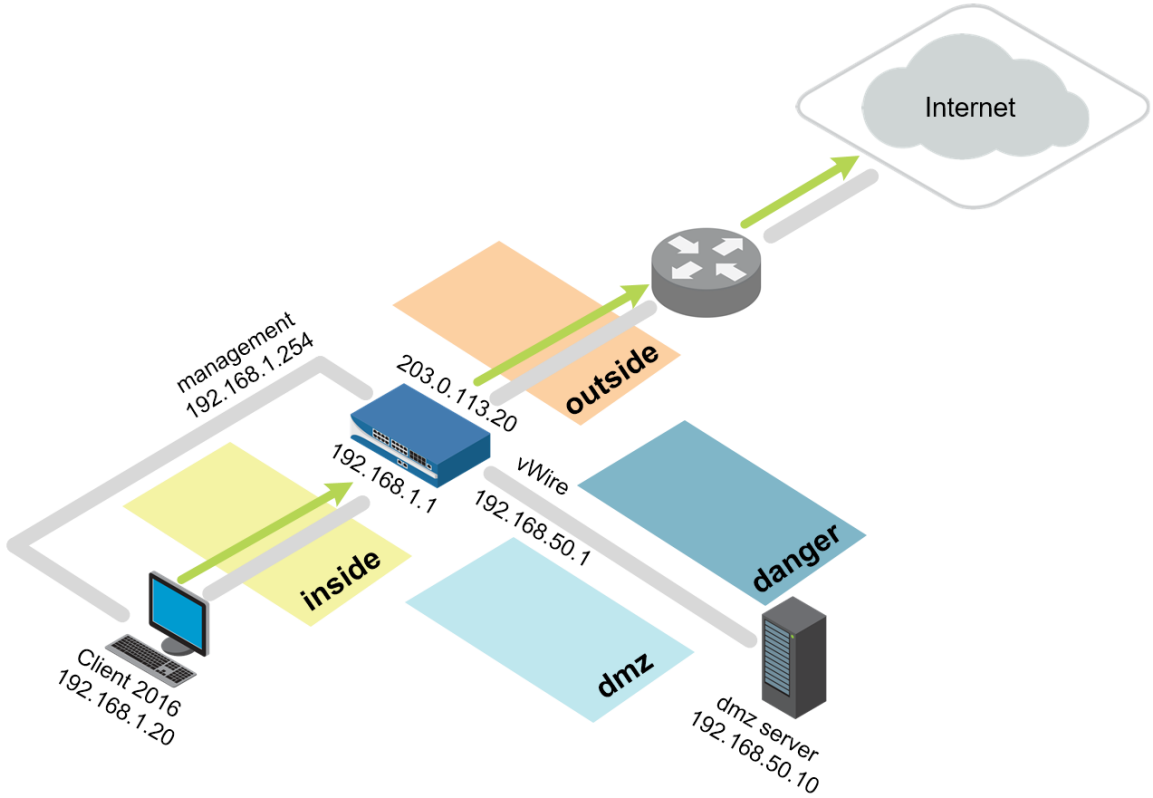
In this lab, you will perform the following tasks:

- 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
- Configure permitted IP addresses for the firewall management
- Check for new PAN-OS software

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.

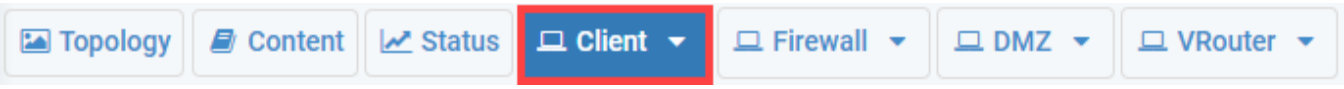
Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Client	192.168.1.20	lab-user	**Pal0Alt0!**
DMZ	192.168.50.10	root	**Pal0Alt0!**
Firewall	192.168.1.254	admin	**Pal0Alt0!**
VRouter	192.168.1.10	root	**Pal0Alt0!**

1 Connect to the Management Network

1.1 Load Lab Configuration

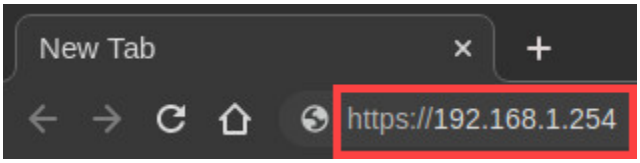
In this section, you will load the Firewall configuration file.

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

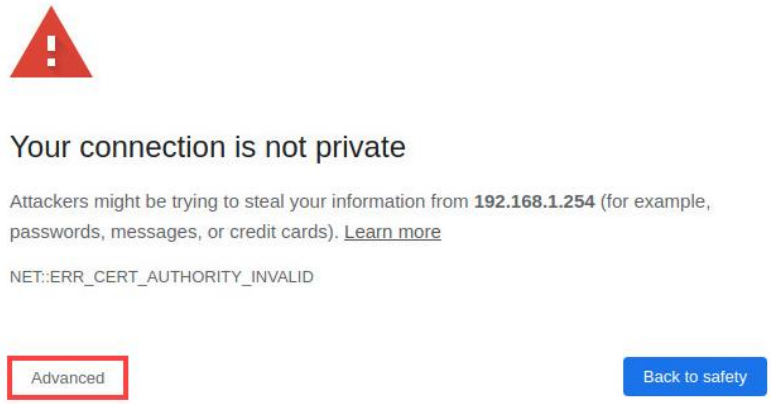


2. Double-click the **Chromium Web Browser** icon located on the desktop.

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

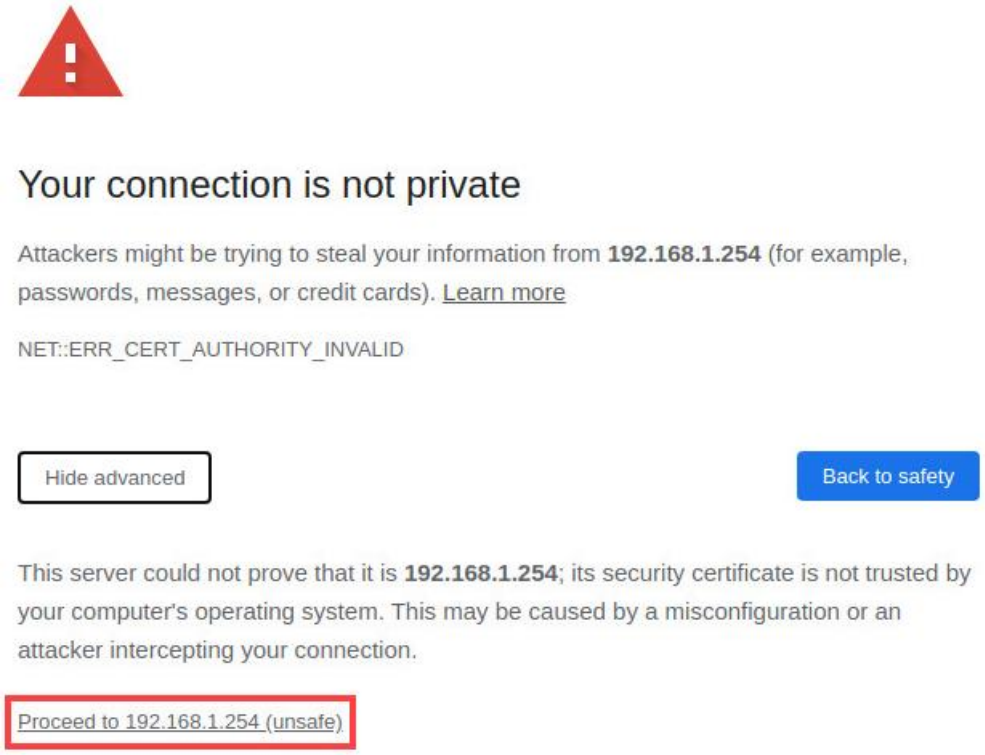


4. You will see a "*Your connection is not private*" message. Next, click on the **ADVANCED** link.



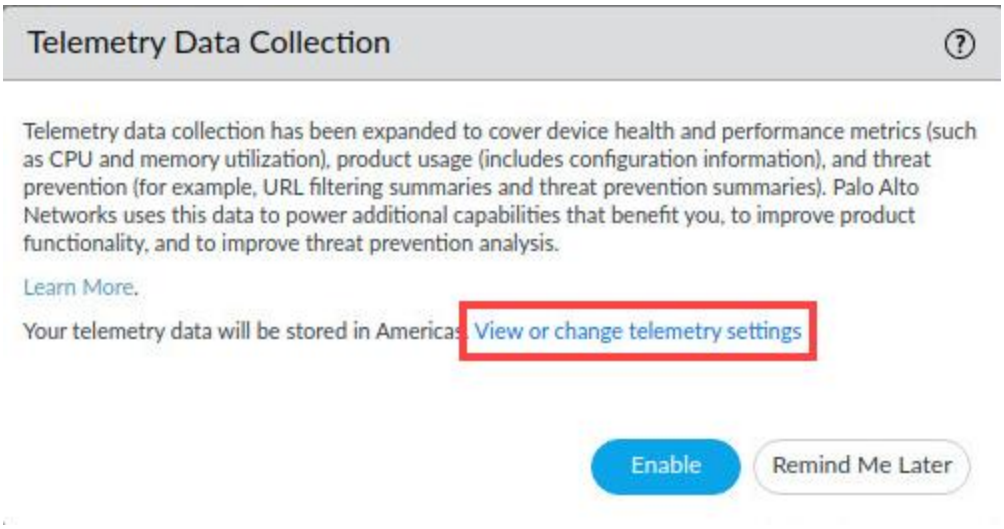
If you experience the “Unable to connect” or “502 Bad Gateway” message while attempting to connect to the specified IP above, please wait an additional 1-3 minutes for the Firewall to fully initialize. Refresh the page to continue.

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



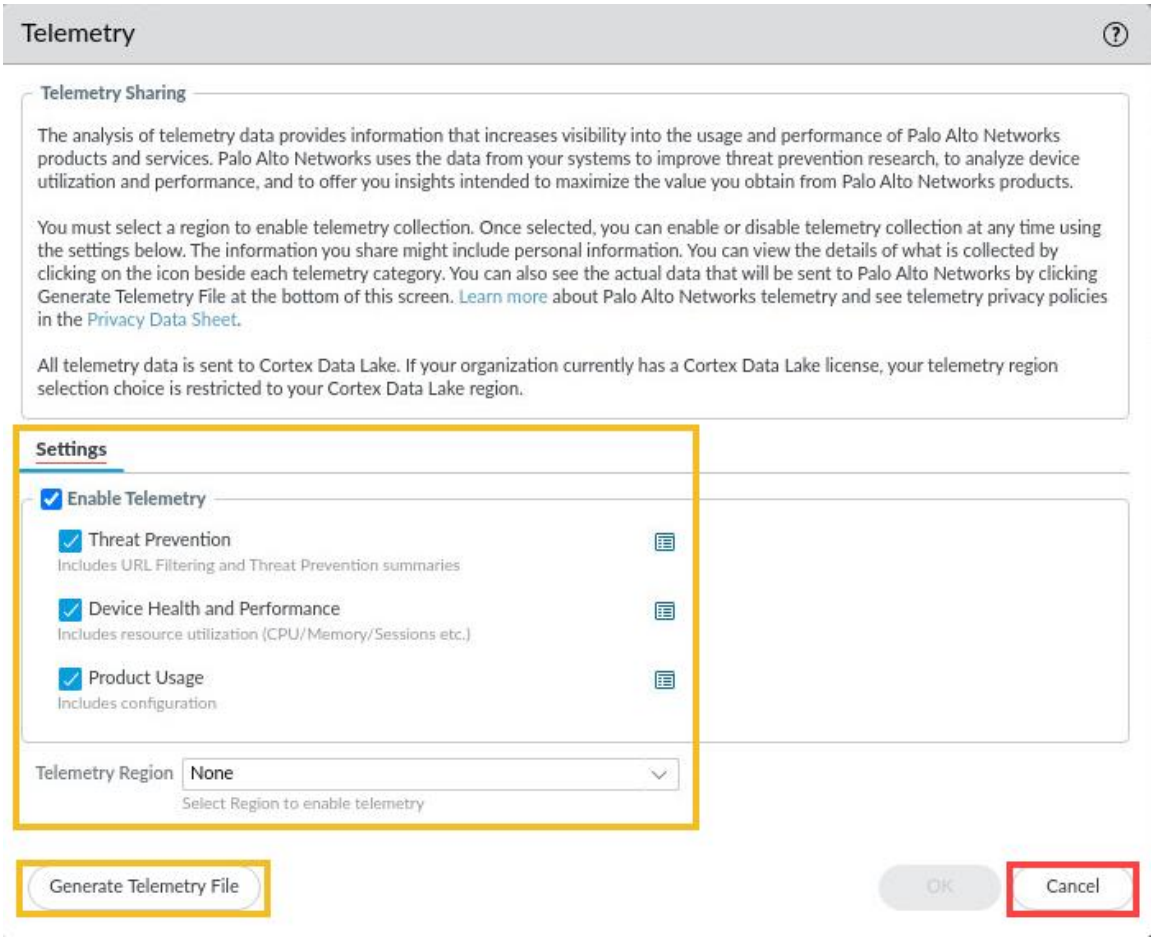
6. Log in to the firewall web interface as username **`admin`**, password **`Pal0Alt0!.`**

7. In the *Telemetry Data Collection* pop-up, click **View or change telemetry settings**.



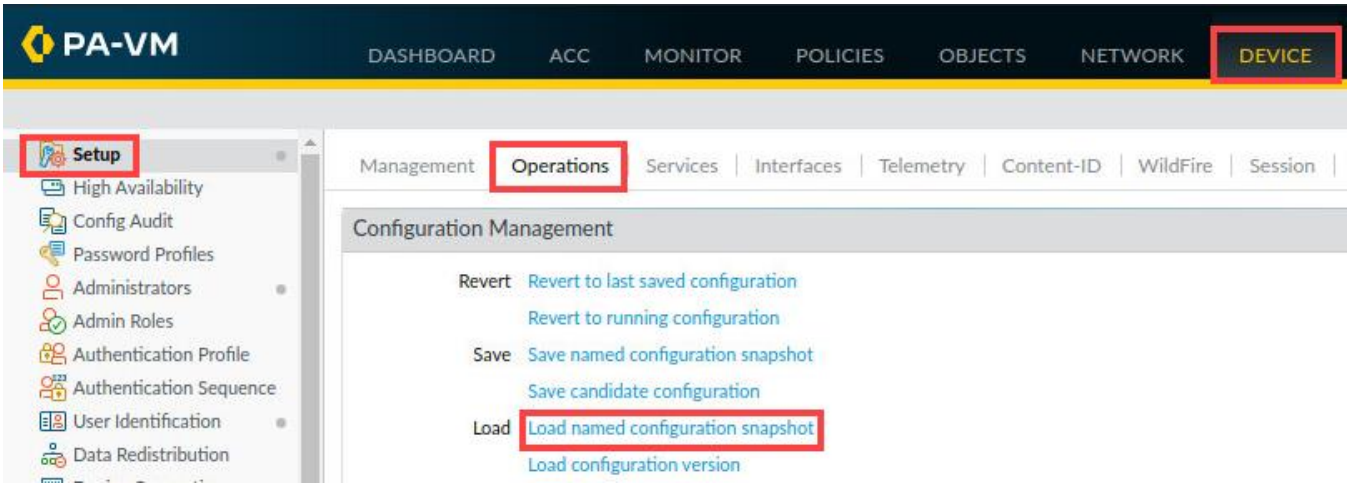
Telemetry Data Collection enables administrators to collect and forward sets of telemetry data to Palo Alto Networks. It only contains the data based on the Telemetry settings you allow.

8. In the *Telemetry* window, view the settings. Notice *Threat Prevention*, *Device and Performance,* and *Product Usage* are checked to be collected. You may also select the appropriate *Telemetry Region* in which you are located. To disable *Telemetry,* you will deselect **Enable Telemetry** and commit your change. Lastly, notice the *Generate Telemetry File*. Click **Cancel**.

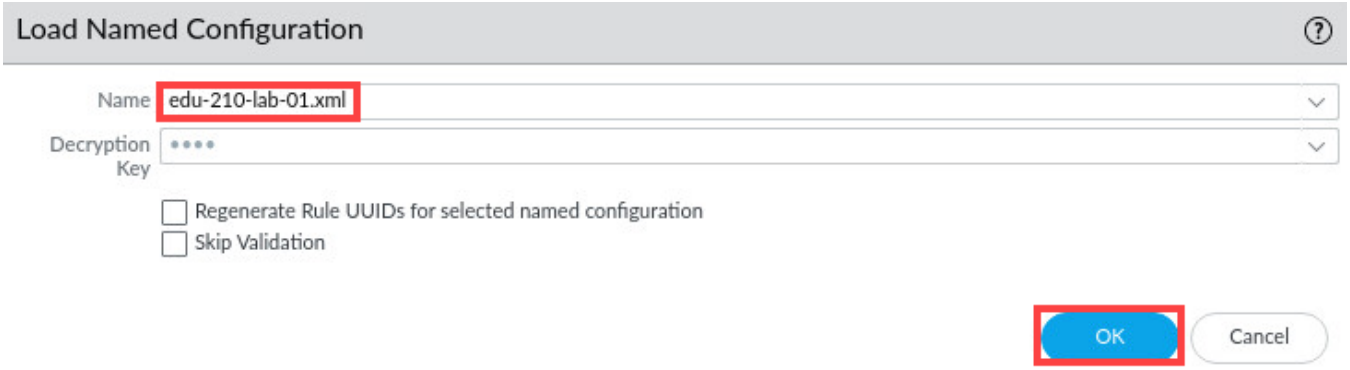


When you Generate a Telemetry File, you obtain live data of the Palo Alto Networks Firewall at the next Telemetry transmission interval. The data collection is defined every 20 minutes, 4 hours, or once per week. Once the metric is determined, the Palo Alto Networks Firewall will send the data bundle to Palo Networks, and it is then deleted from the device once the data has been sent.

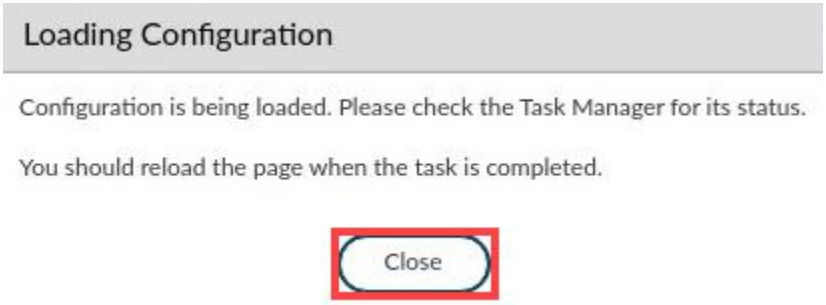
9. Navigate to **Device > Setup > Operations** in the web interface and click on **Load named configuration snapshot** underneath the *Configuration Management* section.



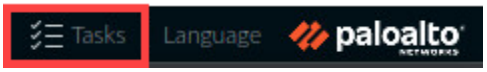
10. In the *Load Named Configuration* window, select **edu-210-lab-01.xml** from the *Name* dropdown box and click **OK**.



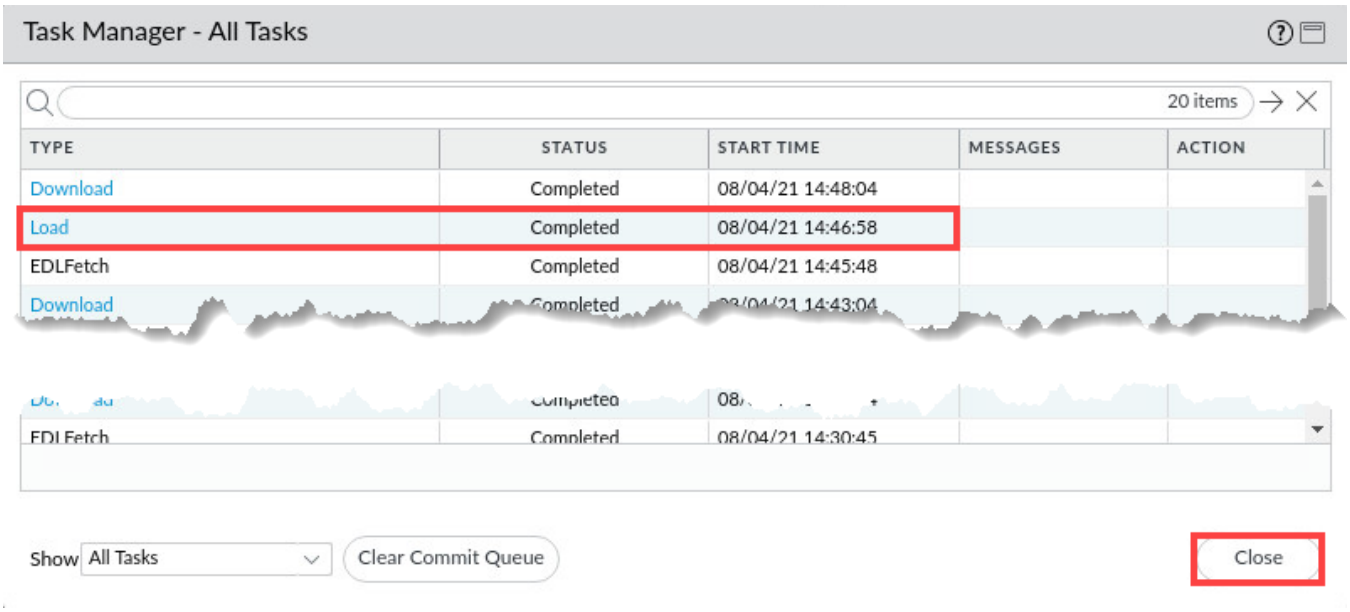
11. In *the Loading Configuration* window, a message will show *Configuration is being loaded*. *Please check the Task Manager for its status. You should reload the page when the task is completed.* Click **Close** to continue.



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

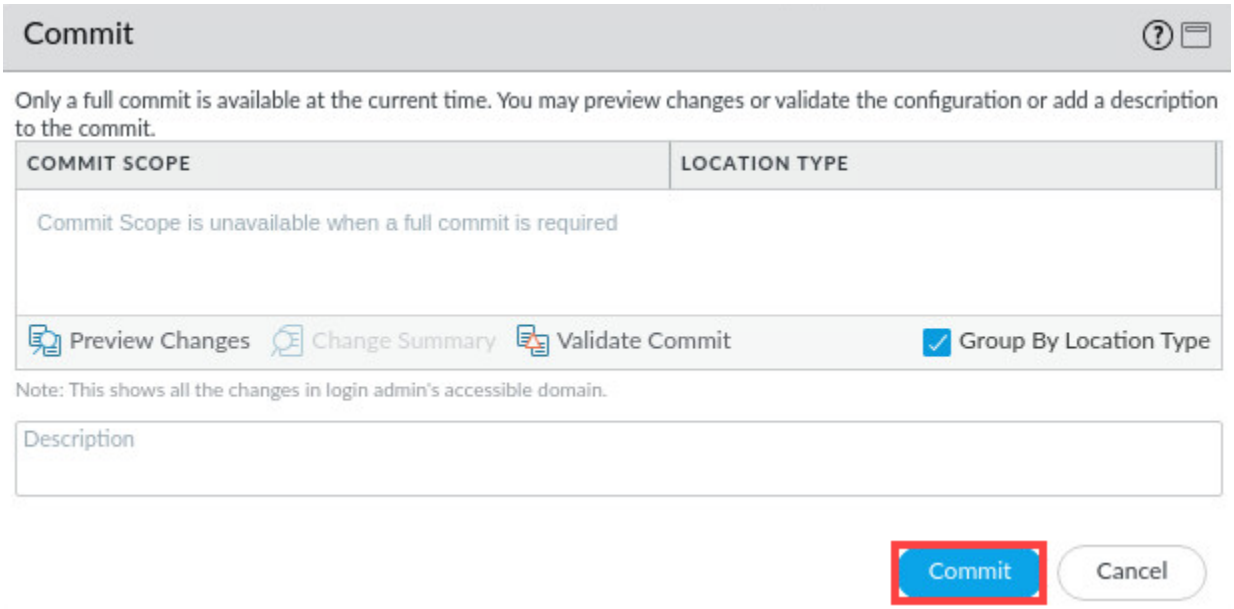


13. In the *Task Manager – All Tasks* window, verify the *Load* type has been completed. Click **Close**

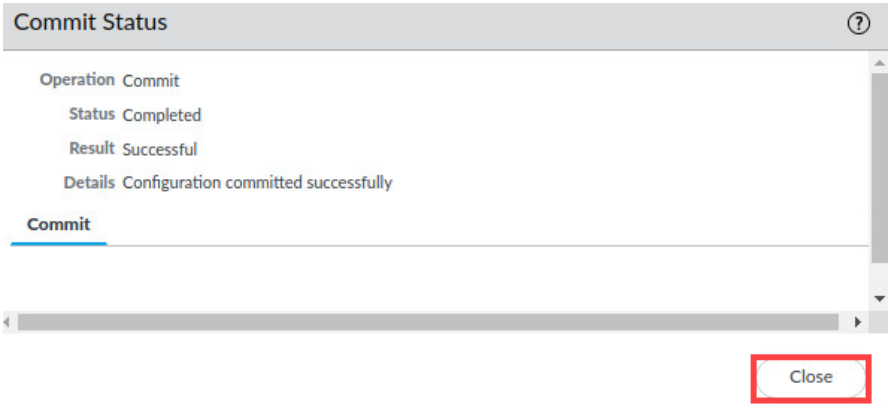


14. Click the **Commit** link located at the top-right of the web interface.

15. In the *Commit* window, click **Commit** to proceed with committing the changes.



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



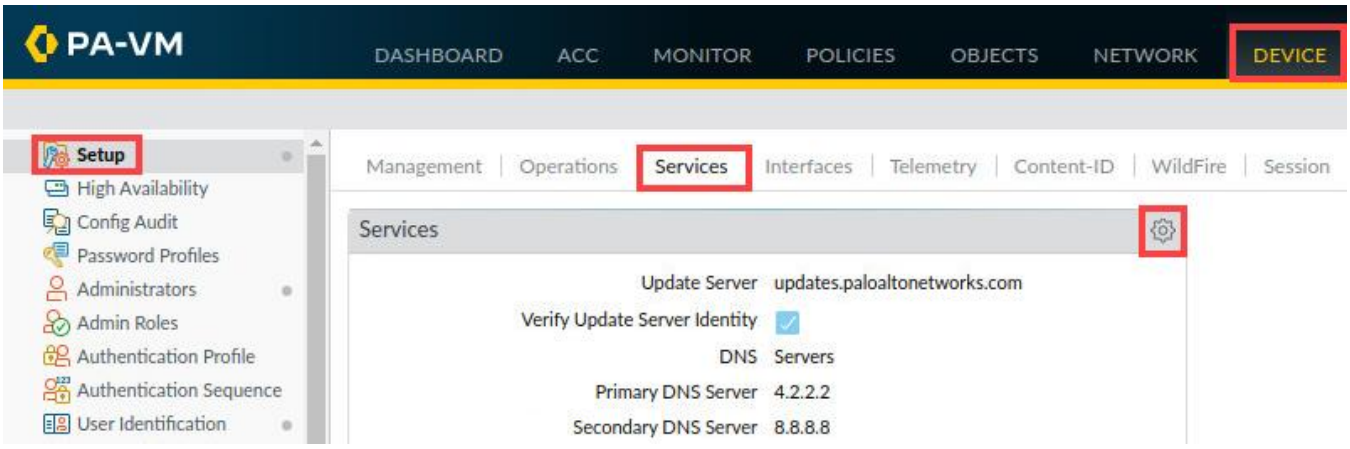
The commit process takes changes made to the Firewall and copies them to the running configuration, which will activate all configuration changes since the last commit.

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

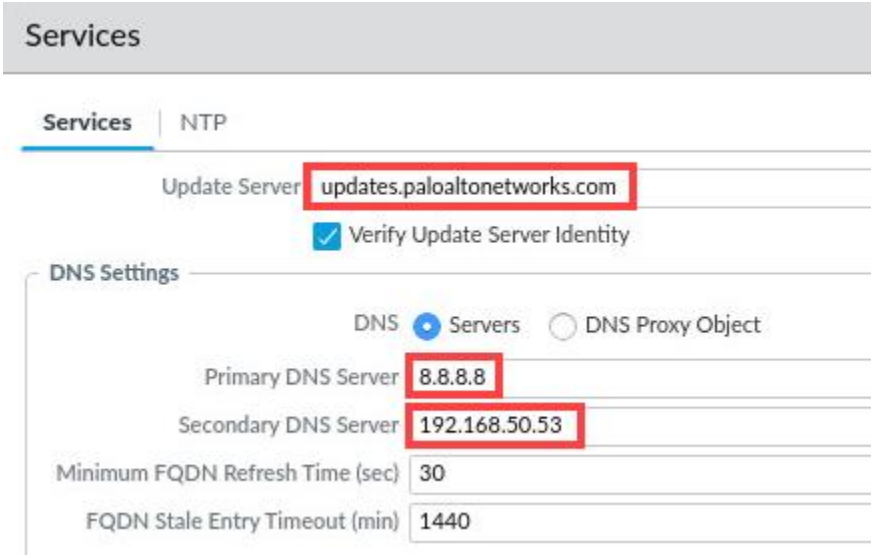
1.2 Configure the Update Server and DNS Server

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.

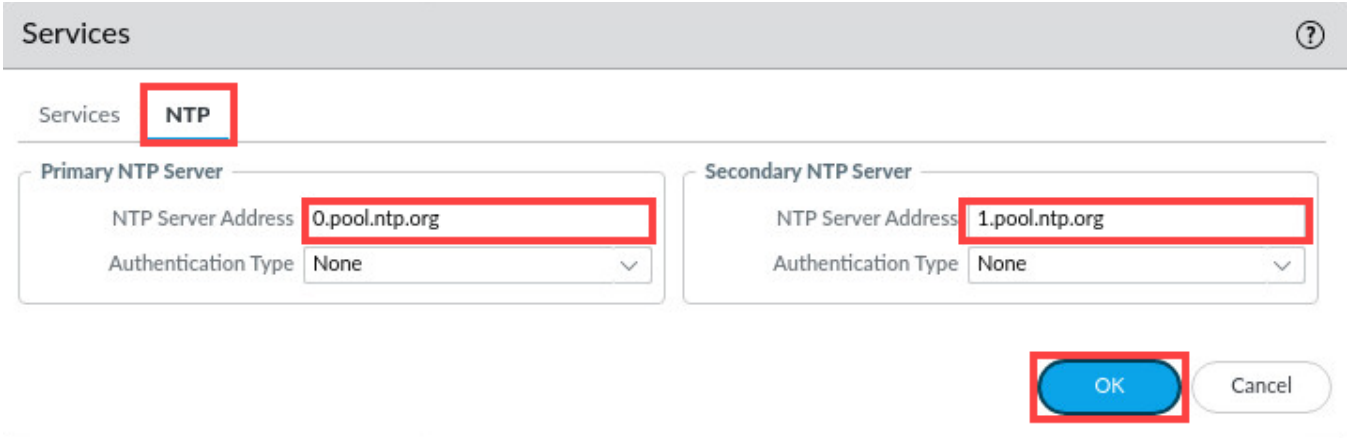
1. In the web interface, select **Device > Setup > Services**. Click the **Services gear** icon to open the *Services* window.



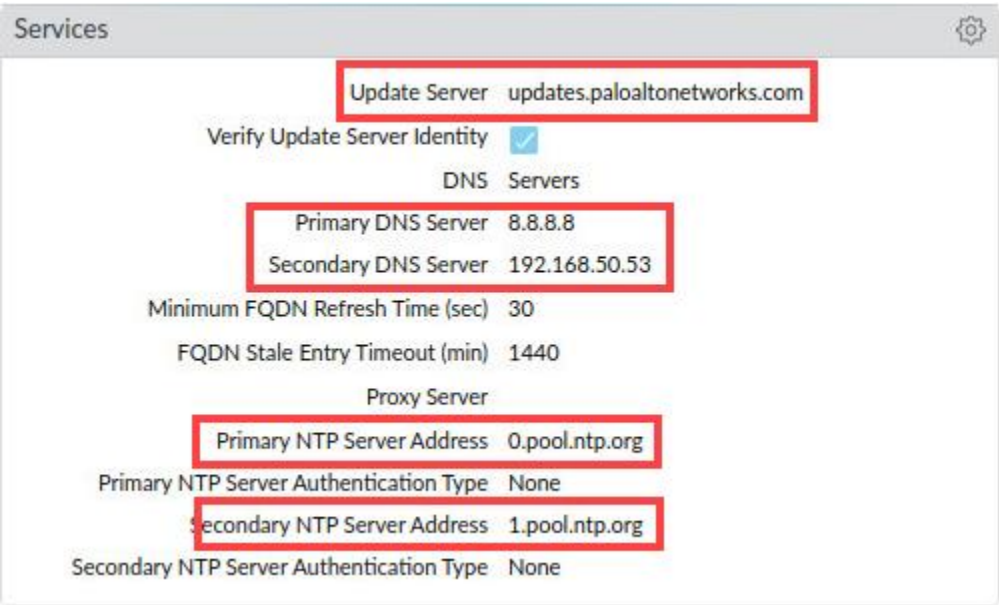
2. In the *Services* window, verify that the *Update Server* is set to **`updates.paloaltonetworks.com`**. Set the *Primary DNS Server* to **`8.8.8.8`** and the *Secondary DNS Server* to **`192.168.50.53`**.



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**.



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

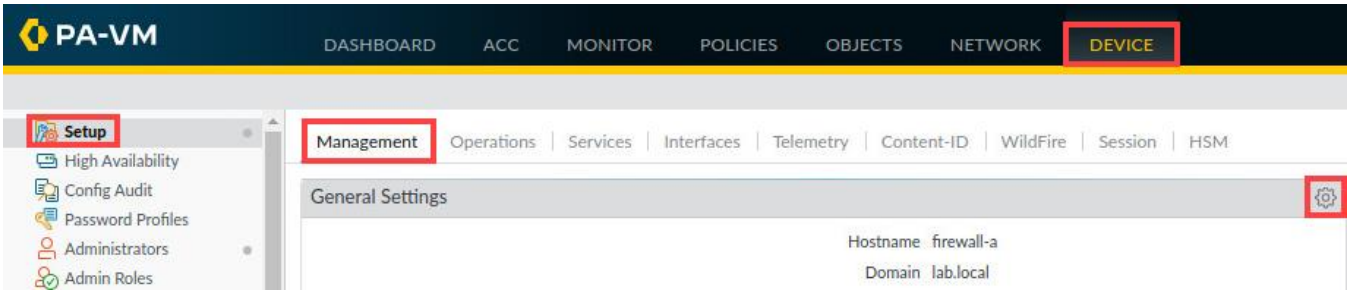


5. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

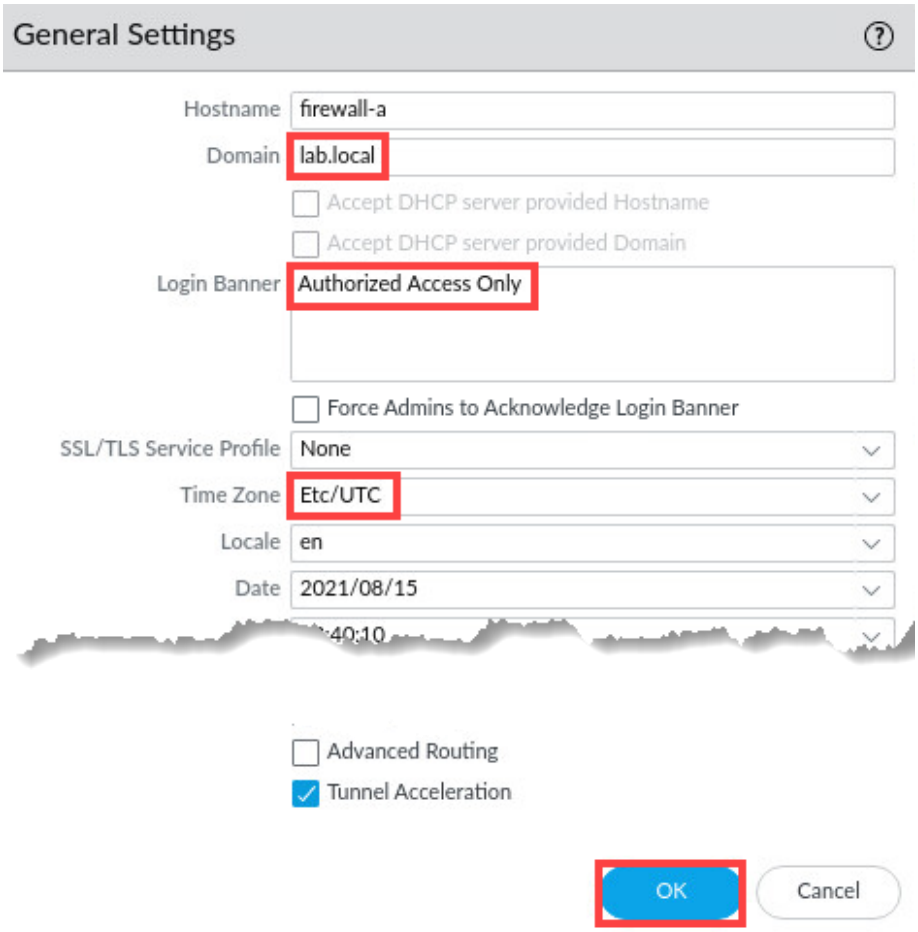
1.3 Configure General Settings of the Firewall

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 set a login banner.

1. Navigate **Device > Setup > Management**. Click on the **General Settings gear** icon to open the *General Settings* window.



2. In the *General Settings* window, verify the *Domain* listed is **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*. Click **OK**.

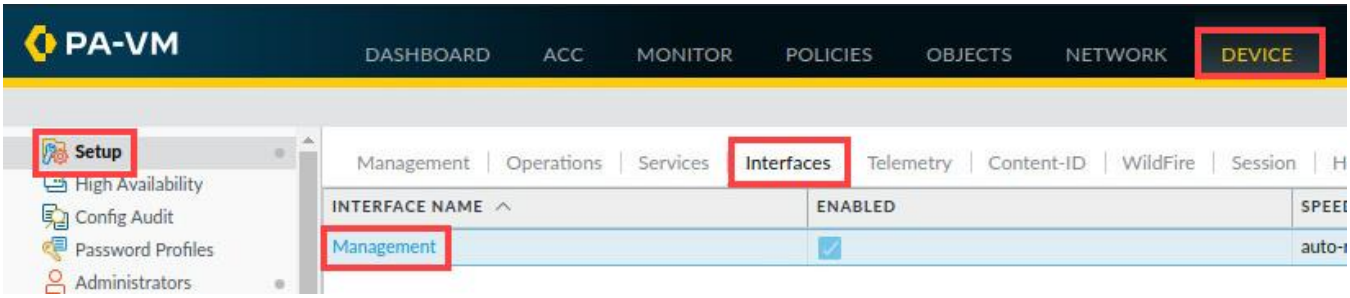


3. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

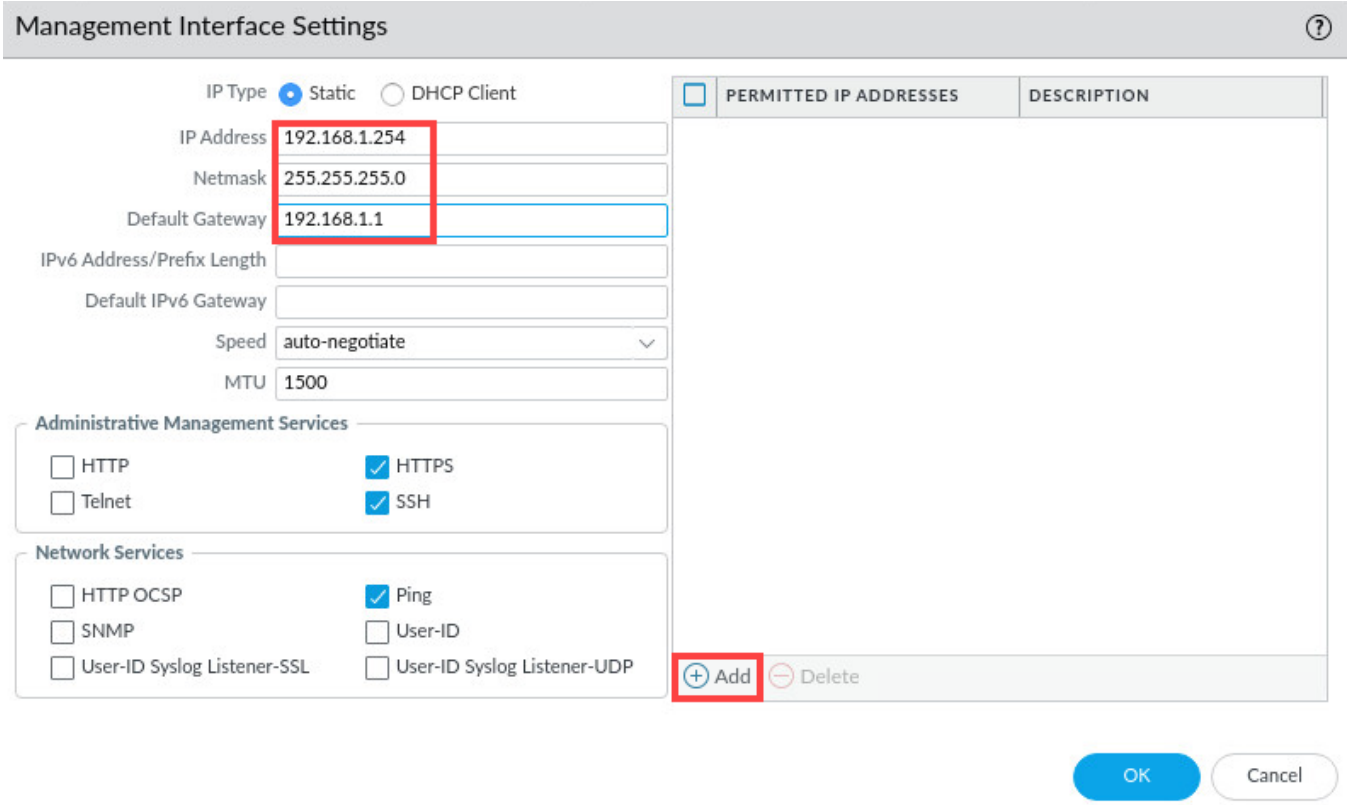
1.4 Modify the Management Interface

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

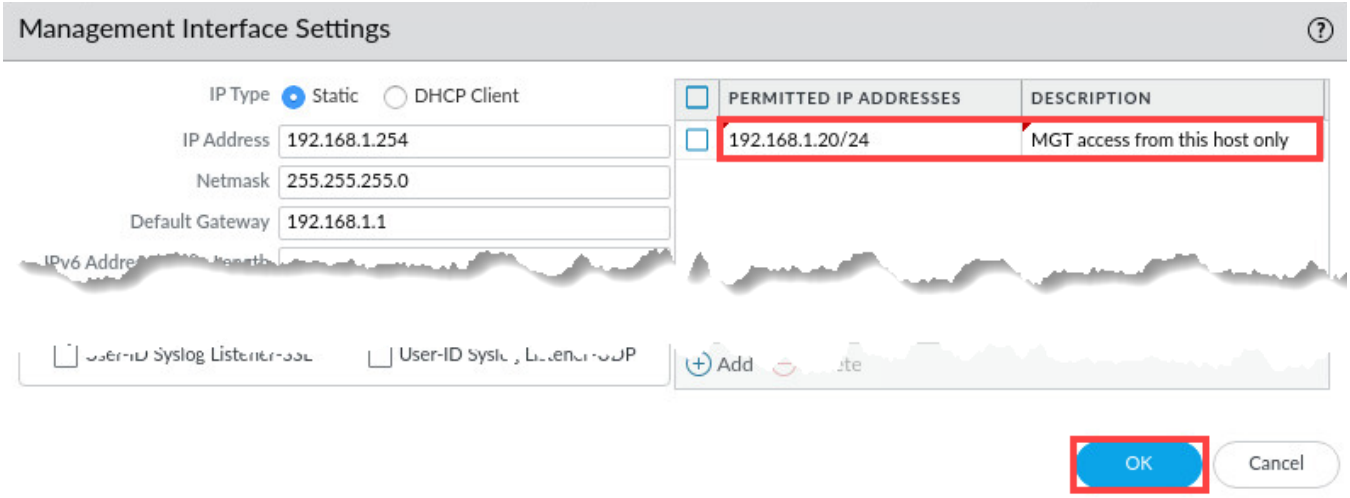
1. Navigate to **Device > Setup > Interfaces** and click on interface name **Management**.



2. In the *Management Interface Settings* window, verify **`192.168.1.254`** for the *IP Address*, **`255.255.255.0`** for the *Netmask*, and **`192.168.1.1`** for the *Default Gateway*. At the bottom of the *Permitted IP Addresses* area, click **Add.**



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**.

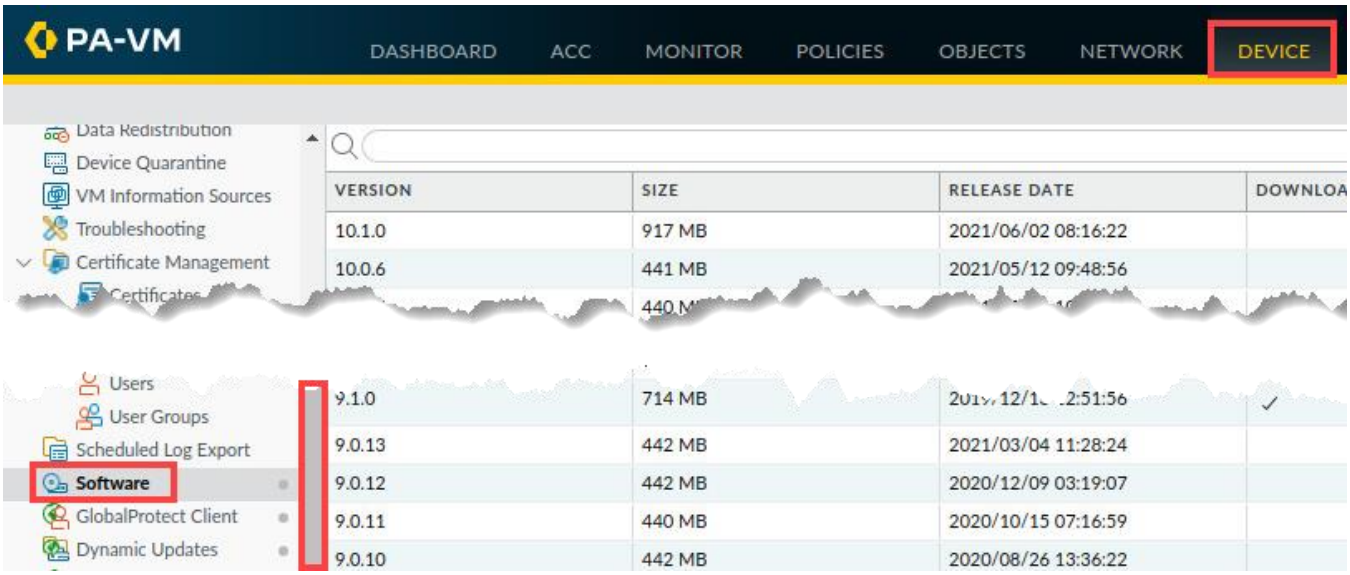


4. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

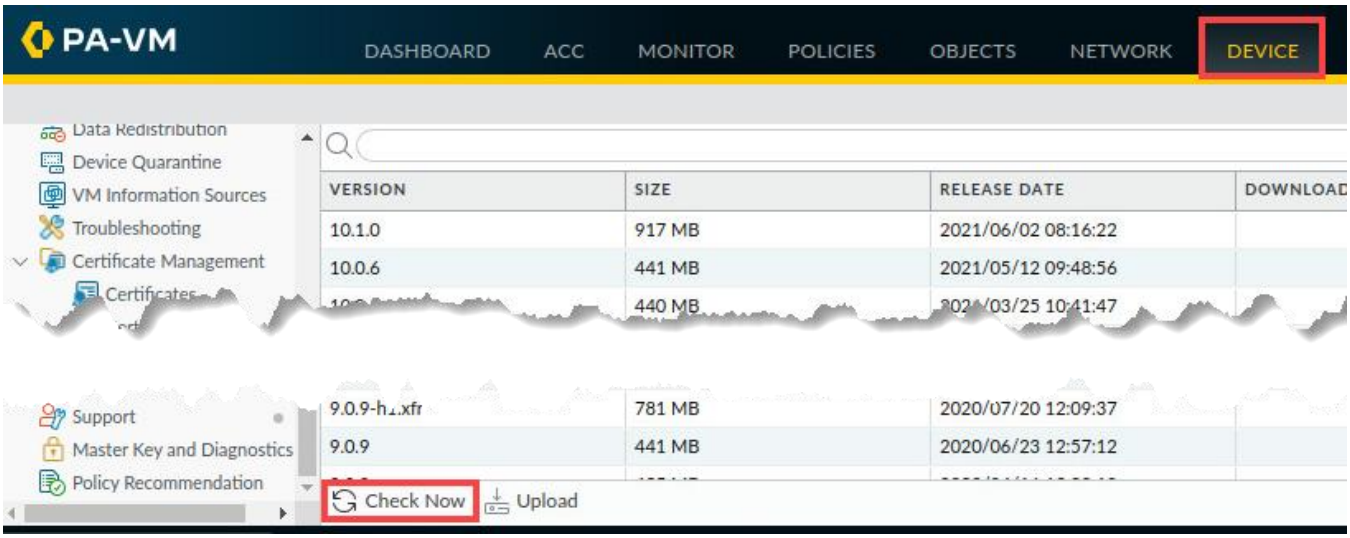
1.5 Check for New PAN-OS Software

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

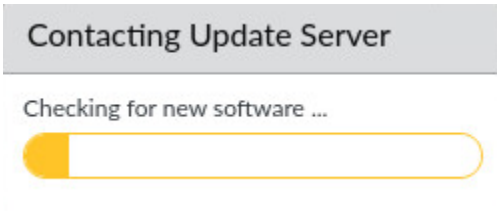
1. In the *PA-VM* web interface, navigate to **Device > Software**. If needed, use the scroll bar to find Software.



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.

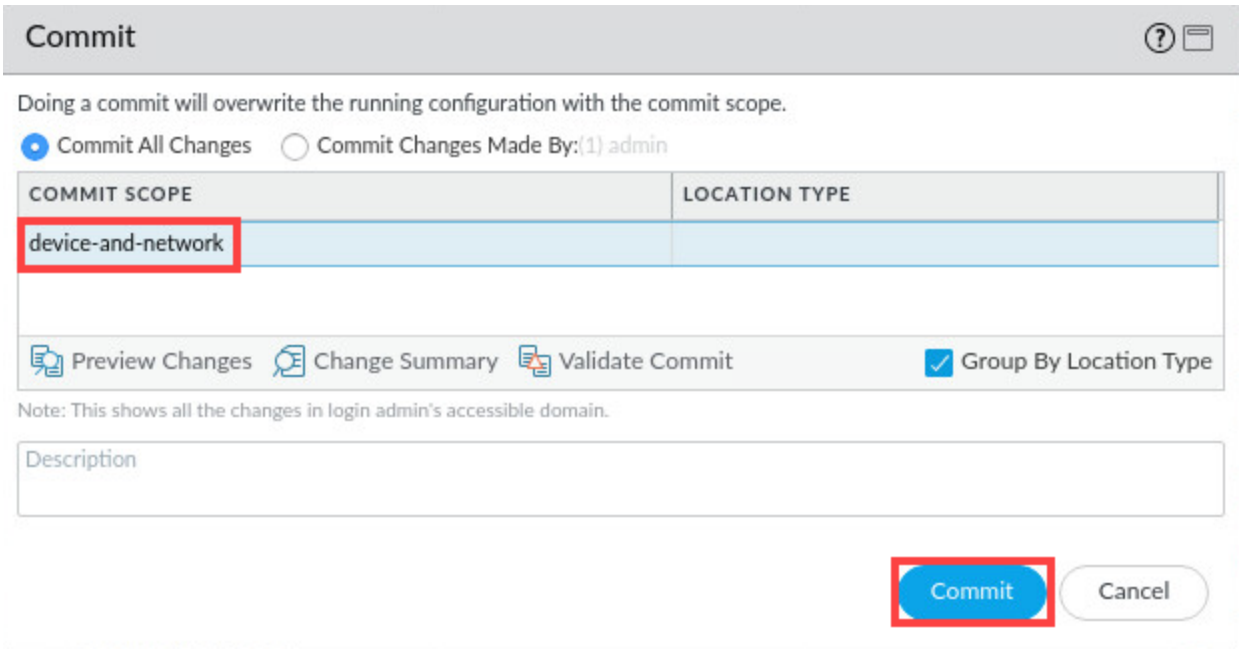


VERSION	SIZE	RELEASE DATE	DOWNLOADED	CURRENTLY INSTALLED	ACTION
10.1.1	297 MB	2021/07/21 09:33:46			Download
10.1.0	917 MB	2021/06/02 08:16:22			Download
10.0.6	441 MB	2021/05/12 09:48:56			Download
10.0.5	440 MB	2021/03/25 10:41:47			Download
10.0.4	431 MB	2021/02/01 17:09:54			Download
10.0.3	431 MB	2020/12/09 19:38:09			Download
10.0.2	430 MB	2020/10/28 11:33:33			Download
10.0.1	332 MB	2020/09/03 09:32:34			Download
10.0.0	806 MB	2020/07/16 20:15:10	✓	✓	Reinstall
9.1.10	398 MB	2021/06/10 11:28:23			Download

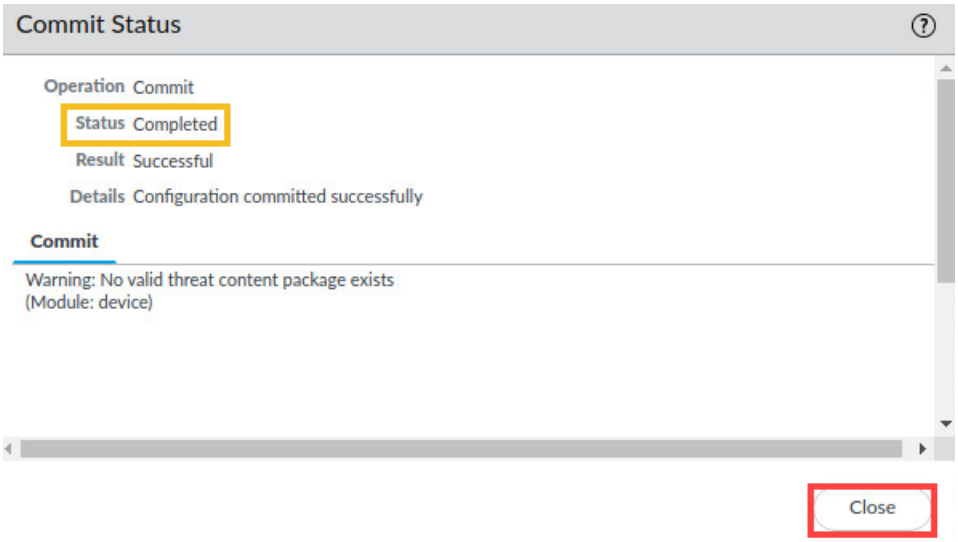
The list you see will vary from this example. Also, newer versions of PAN-OS software may be available at the time you carry out these steps. Do not upgrade your firewall.

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**.



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



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