



NETLAB+



PALO ALTO NETWORKS – EDU 210

Lab 1: Connect to the Management Network

Document Version: 2021-09-27

Contents

Introduction	3
Objective	3
Lab Topology	4
Theoretical Lab Topology.....	4
Lab Settings	5
1 Connect to the Management Network.....	6
1.1 Load Lab Configuration	6
1.2 Configure the Update Server and DNS Server	13
1.3 Configure General Settings of the Firewall	15
1.4 Modify the Management Interface.....	16
1.5 Check for New PAN-OS Software	18

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.

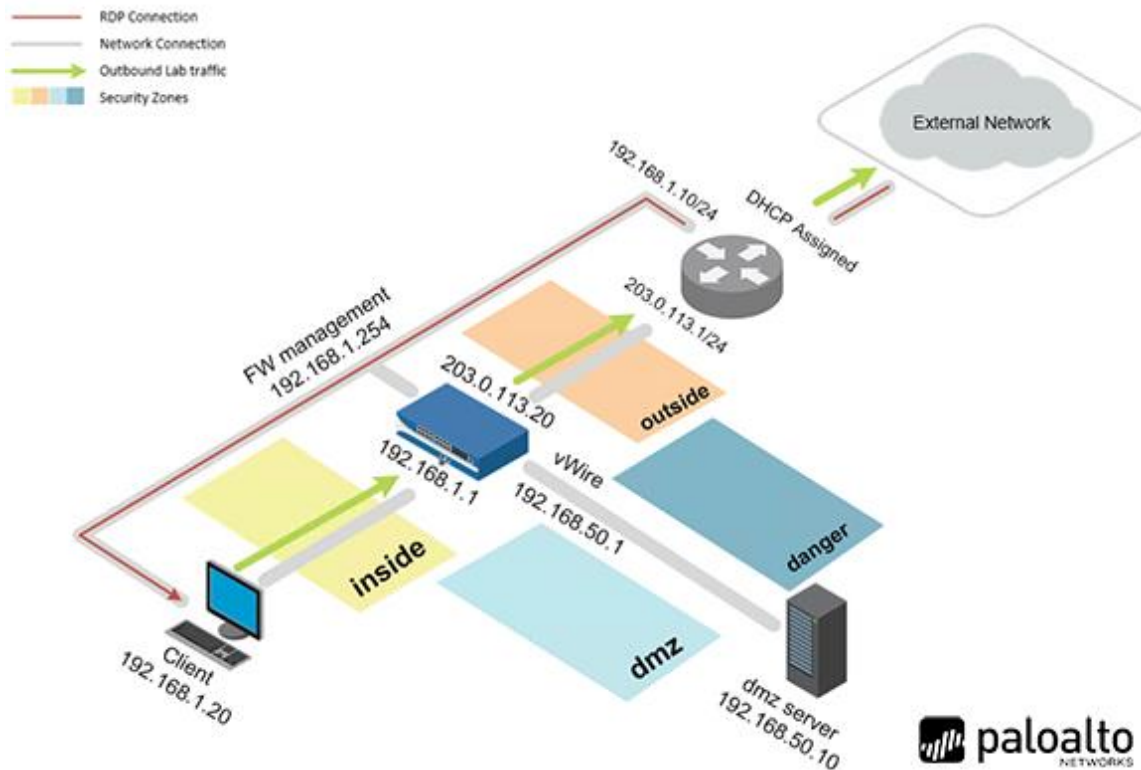
In this lab, you will connect to the Palo Alto Networks firewall management interface and configure basic settings to provide the firewall with network access.

Objective

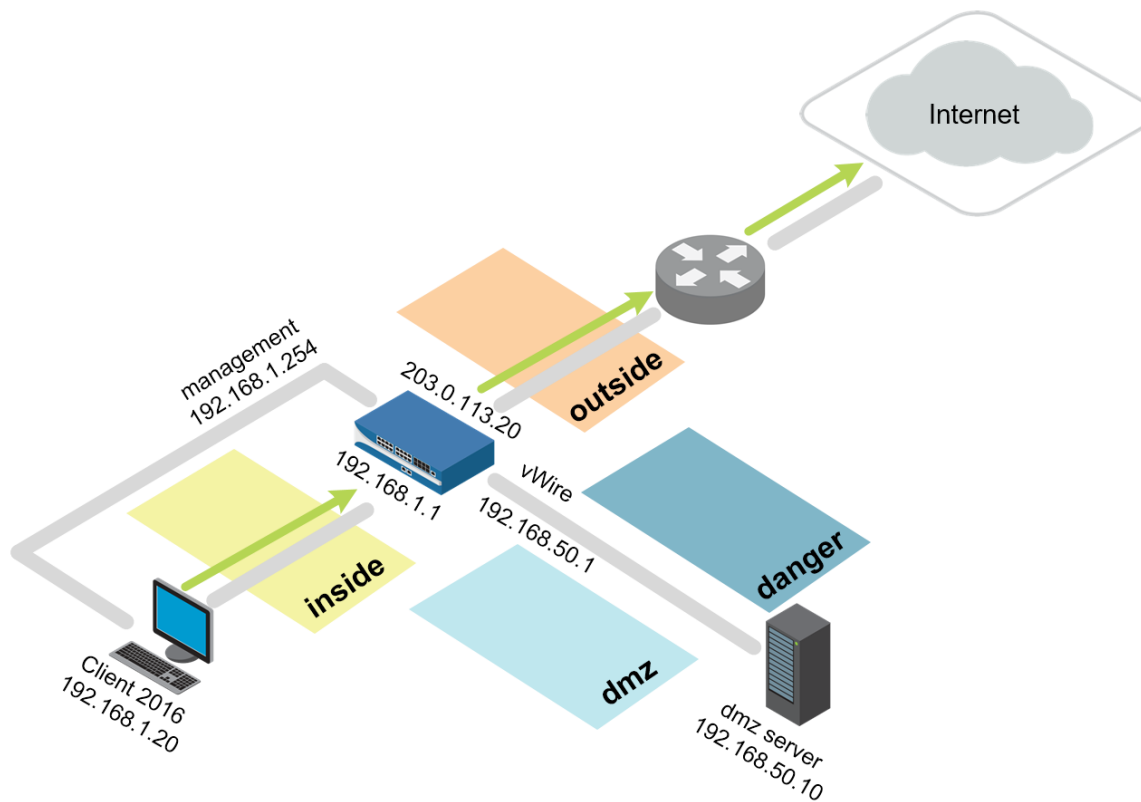
In this lab, you will perform the following tasks:

- 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	Pa10Alt0!
DMZ	192.168.50.10	root	Pa10Alt0!
Firewall	192.168.1.254	admin	Pa10Alt0!
VRouter	192.168.1.10	root	Pa10Alt0!

1 Connect to the Management Network

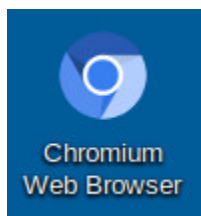
1.1 Load Lab Configuration

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

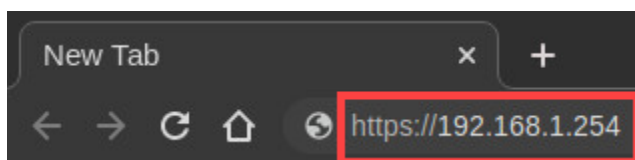
1. Click on the **Client** tab to access the Client PC.



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.



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

Advanced

Back to safety



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.

- 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

Hide advanced

Back to safety

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.

[Proceed to 192.168.1.254 \(unsafe\)](#)

- Log in to the firewall web interface as username **admin**, password **Pa10Alt0!**.



The image shows the Palo Alto Networks login interface. It features the Palo Alto Networks logo at the top. Below the logo, there are two input fields: one for the username 'admin' and another for the password, which is masked with dots. A blue 'Log In' button is positioned below the password field. The entire login area is enclosed in a yellow border.

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


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.](#)

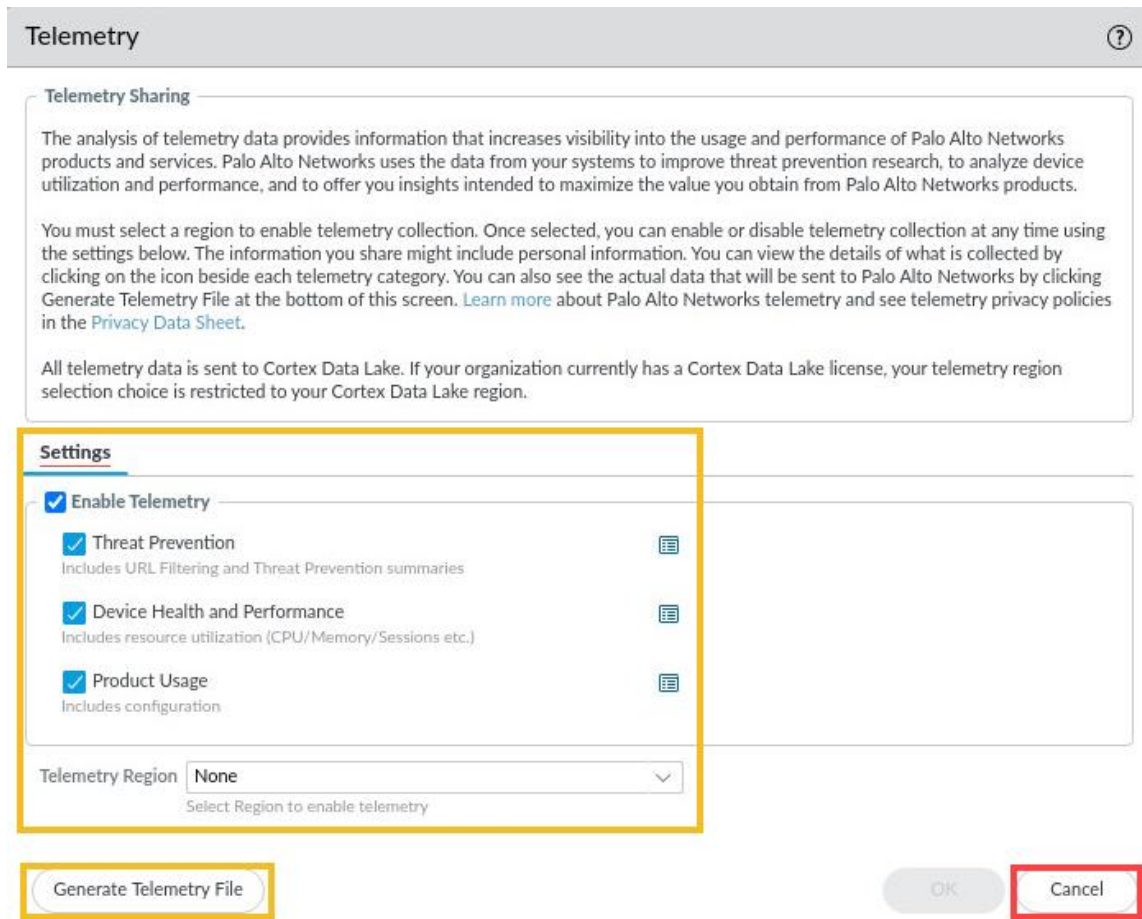
Your telemetry data will be stored in Americas [View or change telemetry settings](#)

[Enable](#) [Remind Me Later](#)



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**.



Telemetry

Telemetry Sharing

The analysis of telemetry data provides information that increases visibility into the usage and performance of Palo Alto Networks products and services. Palo Alto Networks uses the data from your systems to improve threat prevention research, to analyze device utilization and performance, and to offer you insights intended to maximize the value you obtain from Palo Alto Networks products.

You must select a region to enable telemetry collection. Once selected, you can enable or disable telemetry collection at any time using the settings below. The information you share might include personal information. You can view the details of what is collected by clicking on the icon beside each telemetry category. You can also see the actual data that will be sent to Palo Alto Networks by clicking [Generate Telemetry File](#) at the bottom of this screen. [Learn more](#) about Palo Alto Networks telemetry and see telemetry privacy policies in the [Privacy Data Sheet](#).

All telemetry data is sent to Cortex Data Lake. If your organization currently has a Cortex Data Lake license, your telemetry region selection choice is restricted to your Cortex Data Lake region.

Settings

☒ **Enable Telemetry**

☒ **Threat Prevention**
Includes URL Filtering and Threat Prevention summaries

☒ **Device Health and Performance**
Includes resource utilization (CPU/Memory/Sessions etc.)

☒ **Product Usage**
Includes configuration

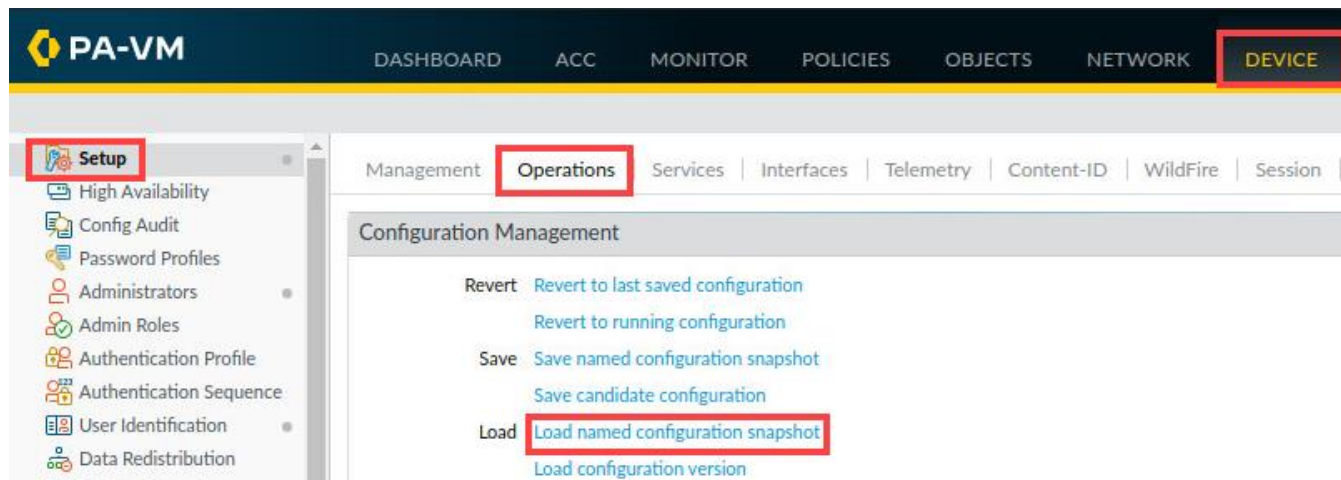
Telemetry Region: **None**
Select Region to enable telemetry

[Generate Telemetry File](#) OK Cancel

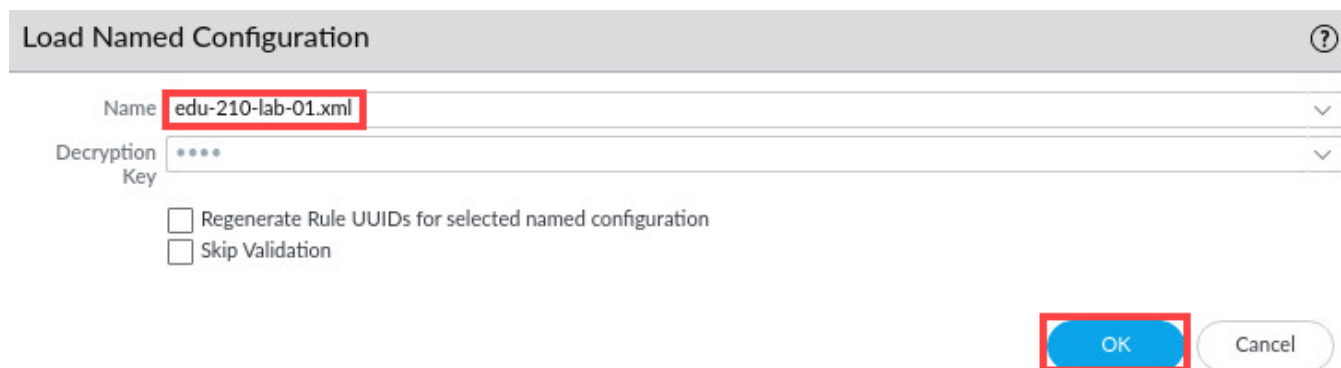


When you Generate a Telemetry File, you obtain live data of the Palo Alto Networks Firewall at the next Telemetry transmission interval. The data collection is defined every 20 minutes, 4 hours, or once per week. Once the metric is determined, the Palo Alto Networks Firewall will send the data bundle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

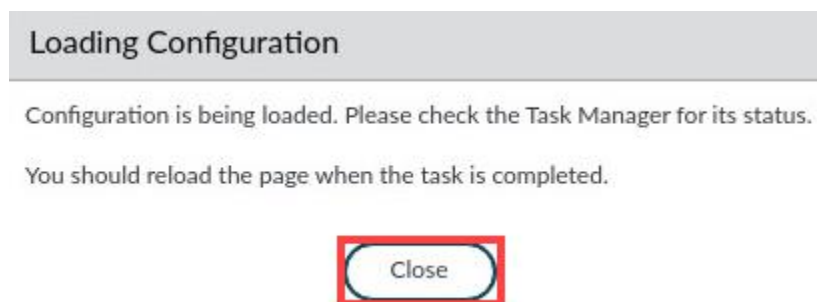
9. Navigate to **Device > Setup > Operations** in the web interface and click on **Load** named **configuration snapshot** underneath the *Configuration Management* section.



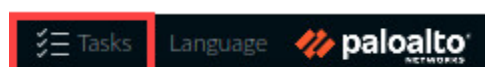
10. In the *Load Named Configuration* window, select **edu-210-lab-01.xml** from the *Name* dropdown box and click **OK**.



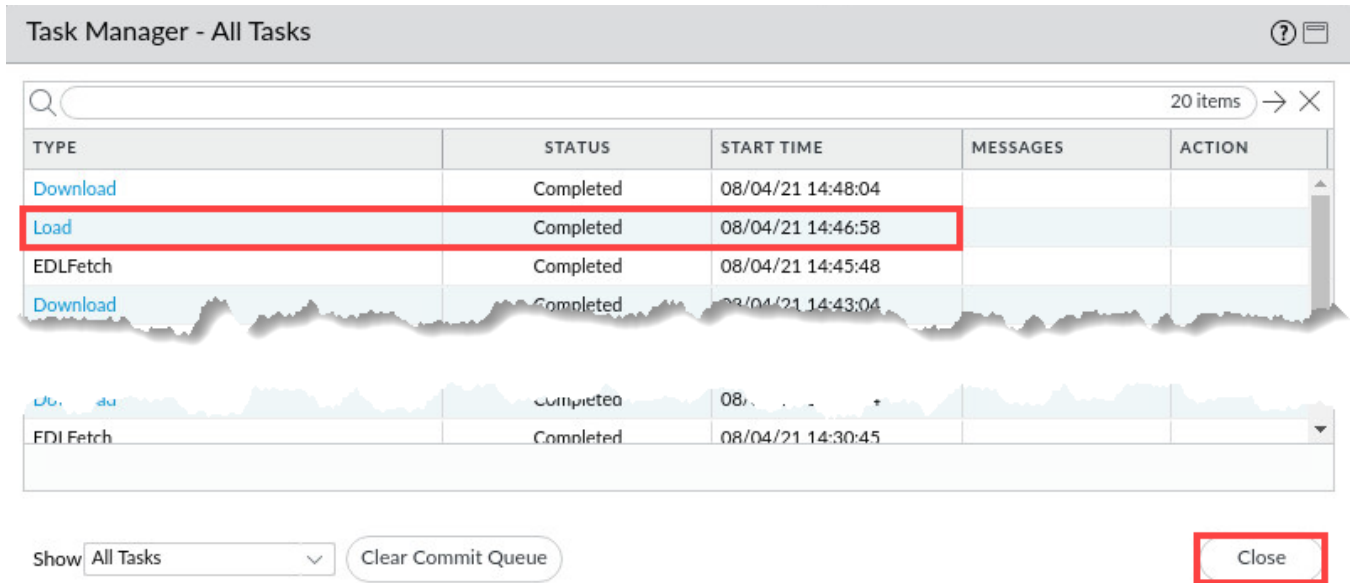
11. In the *Loading Configuration* window, a message will show *Configuration is being loaded*. Please check the *Task Manager* for its status. You should reload the page when the task is completed. Click **Close** to continue.



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**



The screenshot shows the 'Task Manager - All Tasks' window. It contains a table with the following data:

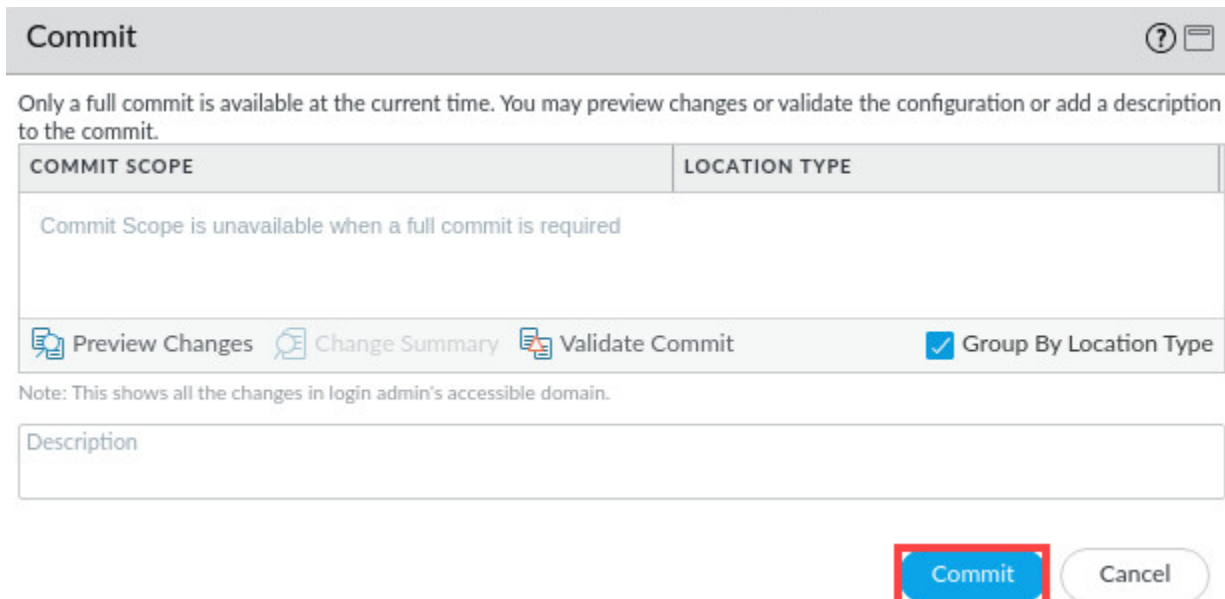
TYPE	STATUS	START TIME	MESSAGES	ACTION
Download	Completed	08/04/21 14:48:04		
Load	Completed	08/04/21 14:46:58		
EDLFetch	Completed	08/04/21 14:45:48		
Download	Completed	08/04/21 14:43:04		
FDI Fetch	Completed	08/04/21 14:30:45		

At the bottom of the window, there is a 'Show' dropdown menu set to 'All Tasks', a 'Clear Commit Queue' button, and a 'Close' button highlighted with a red box.

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.



The screenshot shows the 'Commit' window. It contains the following information:

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.

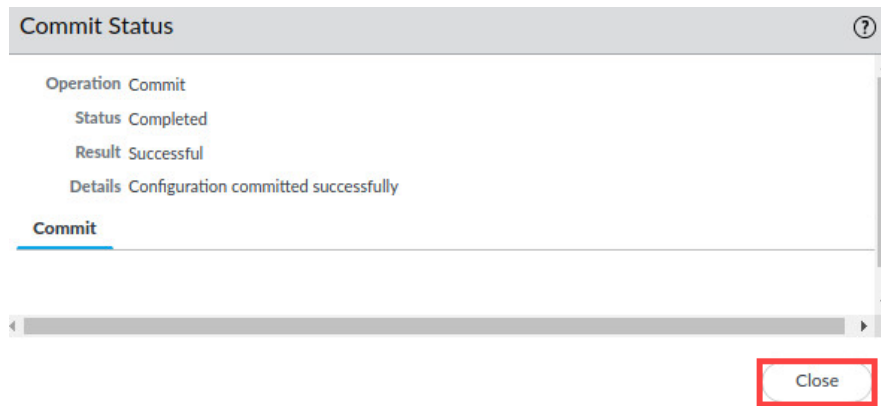
COMMIT SCOPE	LOCATION TYPE
Commit Scope is unavailable when a full commit is required	

Below the table, there are three buttons: 'Preview Changes', 'Change Summary', and 'Validate Commit'. To the right, there is a checkbox labeled 'Group By Location Type' which is checked.

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

At the bottom, there is a text area labeled 'Description' and two buttons: 'Commit' (highlighted with a red box) and 'Cancel'.

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



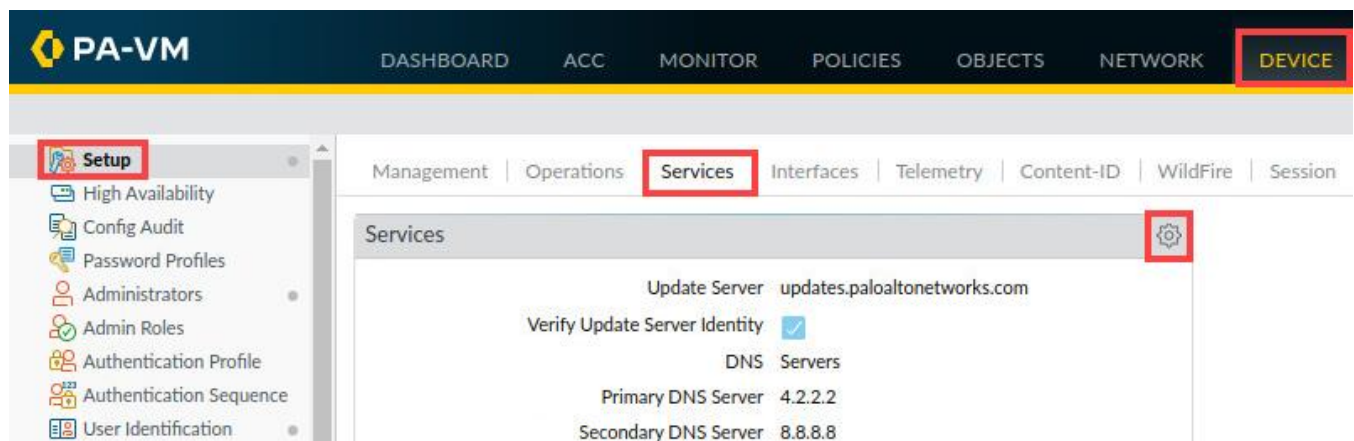
The commit process takes changes made to the Firewall and copies them to the running configuration, which will activate all configuration changes since the last commit.

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

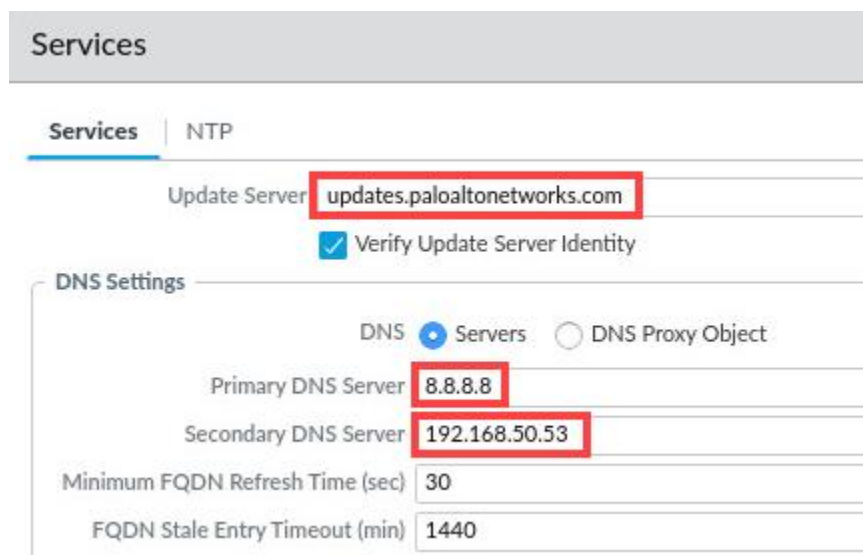
1.2 Configure the Update Server and DNS Server

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.

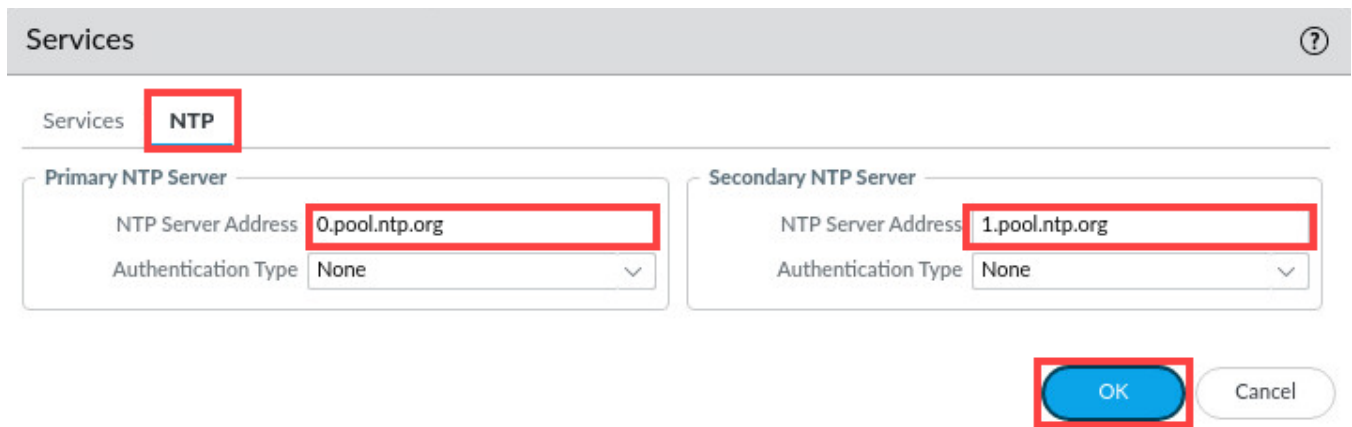
1. In the web interface, select **Device > Setup > Services**. Click the **Services** gear icon to open the *Services* window.



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**.

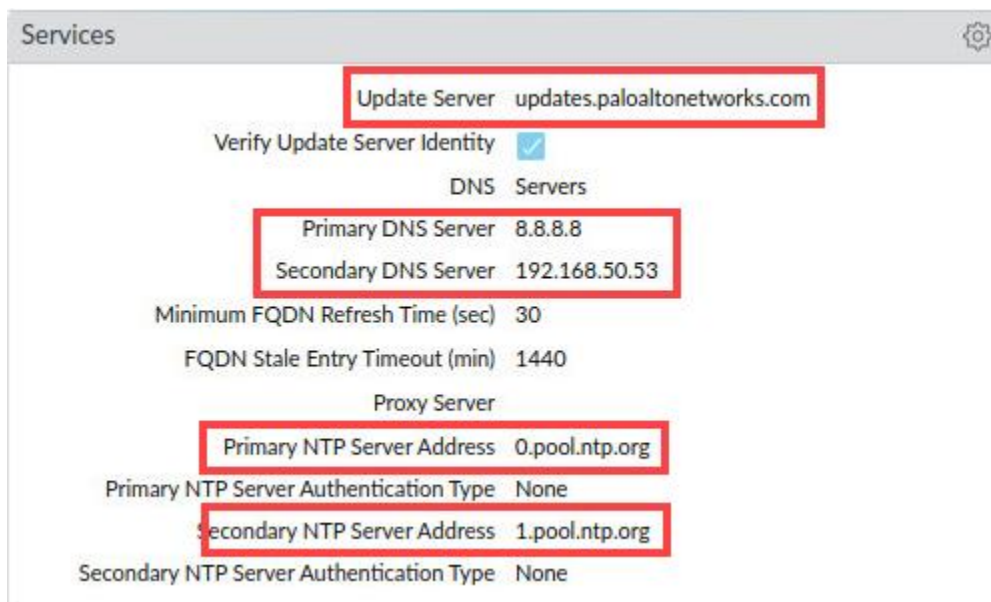


3. Select the **NTP** tab. Set the *Primary NTP Server* to **0.pool.ntp.org** and the *Secondary NTP Server* to **1.pool.ntp.org**. Click **OK**.



The screenshot shows the 'Services' window with the 'NTP' tab selected. The 'Primary NTP Server' section has 'NTP Server Address' set to '0.pool.ntp.org' and 'Authentication Type' set to 'None'. The 'Secondary NTP Server' section has 'NTP Server Address' set to '1.pool.ntp.org' and 'Authentication Type' set to 'None'. The 'OK' button is highlighted with a red box.

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



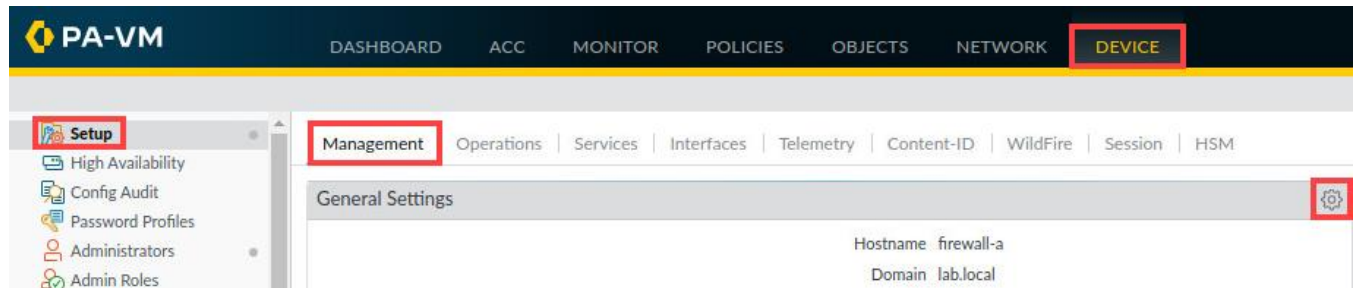
The screenshot shows the 'Services' window with various settings. The 'Update Server' is set to 'updates.paloaltonetworks.com'. The 'Verify Update Server Identity' checkbox is checked. The 'DNS Servers' section shows 'Primary DNS Server' as '8.8.8.8' and 'Secondary DNS Server' as '192.168.50.53'. The 'Proxy Server' section shows 'Primary NTP Server Address' as '0.pool.ntp.org' and 'Secondary NTP Server Address' as '1.pool.ntp.org'. The 'Primary NTP Server Authentication Type' and 'Secondary NTP Server Authentication Type' are both set to 'None'.

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

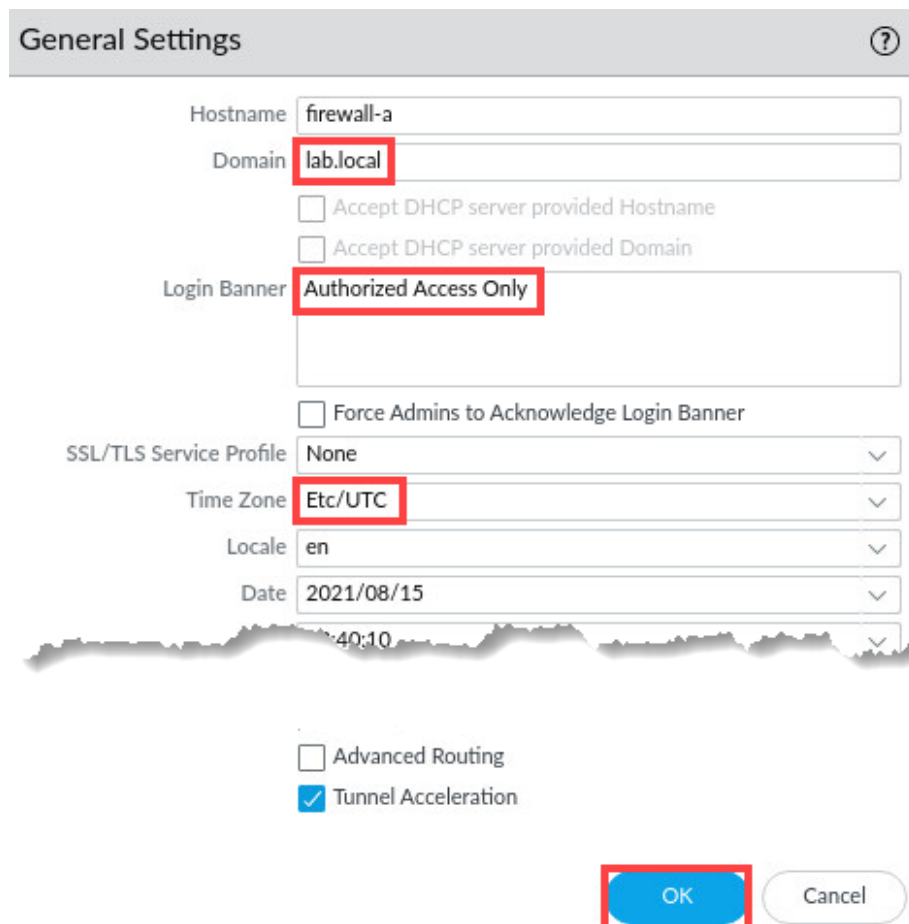
1.3 Configure General Settings of the Firewall

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**.

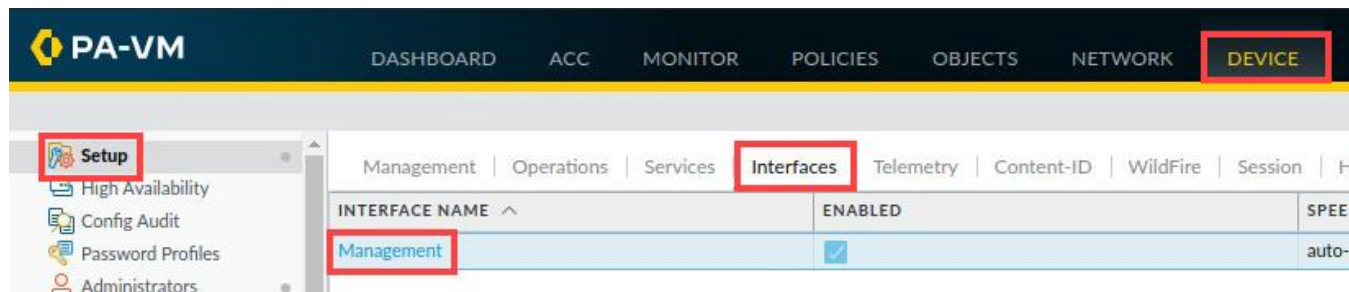


3. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

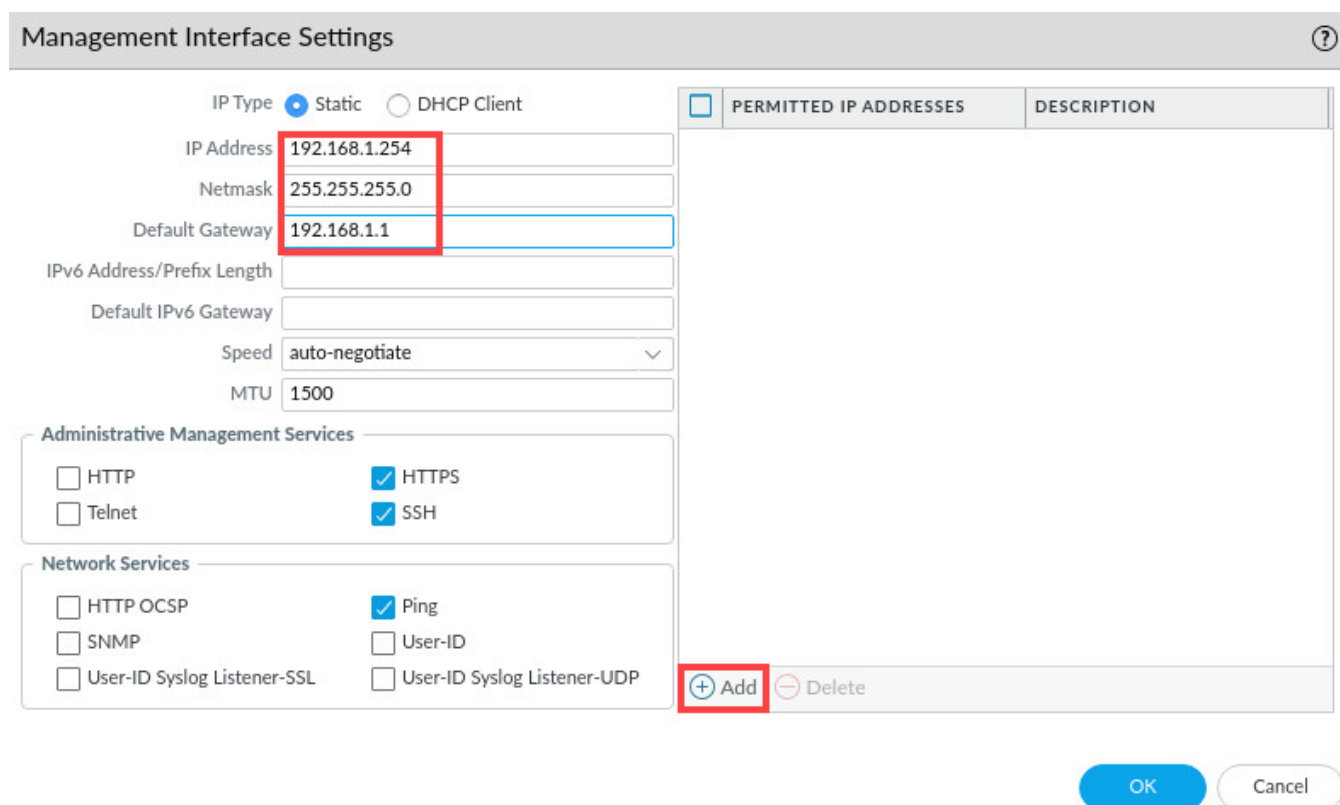
1.4 Modify the Management Interface

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**.



The screenshot shows the 'Management Interface Settings' window. The 'IP Type' is set to 'Static'. The 'IP Address' is 192.168.1.254, 'Netmask' is 255.255.255.0, and 'Default Gateway' is 192.168.1.1. The 'Speed' is set to 'auto-negotiate' and 'MTU' is 1500. The 'Administrative Management Services' section shows 'HTTP' and 'Telnet' are unchecked, while 'HTTPS' and 'SSH' are checked. The 'Network Services' section shows 'HTTP OCSP', 'SNMP', and 'User-ID Syslog Listener-SSL' are unchecked, while 'Ping', 'User-ID', and 'User-ID Syslog Listener-UDP' are checked. The 'Permitted IP Addresses' table is empty. The 'Add' button is highlighted with a red box.

Management Interface Settings

IP Type: ☒ Static ☐ DHCP Client

IP Address: 192.168.1.254

Netmask: 255.255.255.0

Default Gateway: 192.168.1.1

IPv6 Address/Prefix Length:

Default IPv6 Gateway:

Speed: auto-negotiate

MTU: 1500

Administrative Management Services

☐ HTTP ☒ HTTPS

☐ Telnet ☒ SSH

Network Services

☐ HTTP OCSP ☒ Ping

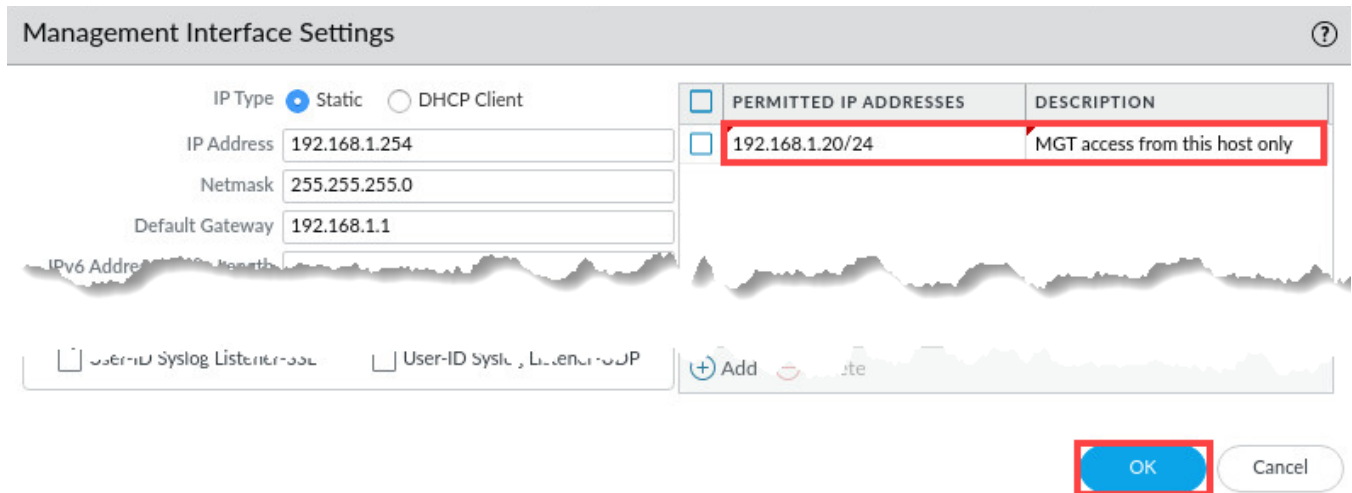
☐ SNMP ☐ User-ID

☐ User-ID Syslog Listener-SSL ☐ User-ID Syslog Listener-UDP

Add Delete

OK Cancel

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**.



The screenshot shows the 'Management Interface Settings' window. On the left, there are input fields for 'IP Type' (Static selected), 'IP Address' (192.168.1.254), 'Netmask' (255.255.255.0), and 'Default Gateway' (192.168.1.1). On the right, there is a table with two columns: 'PERMITTED IP ADDRESSES' and 'DESCRIPTION'. The first row contains '192.168.1.20/24' and 'MGT access from this host only', both highlighted with a red box. Below the table, there are checkboxes for 'User-ID Syslog Listener' and 'User-ID Syslog Listener v2', and a '+ Add' button. At the bottom right, there are 'OK' and 'Cancel' buttons, with the 'OK' button highlighted by a red box.

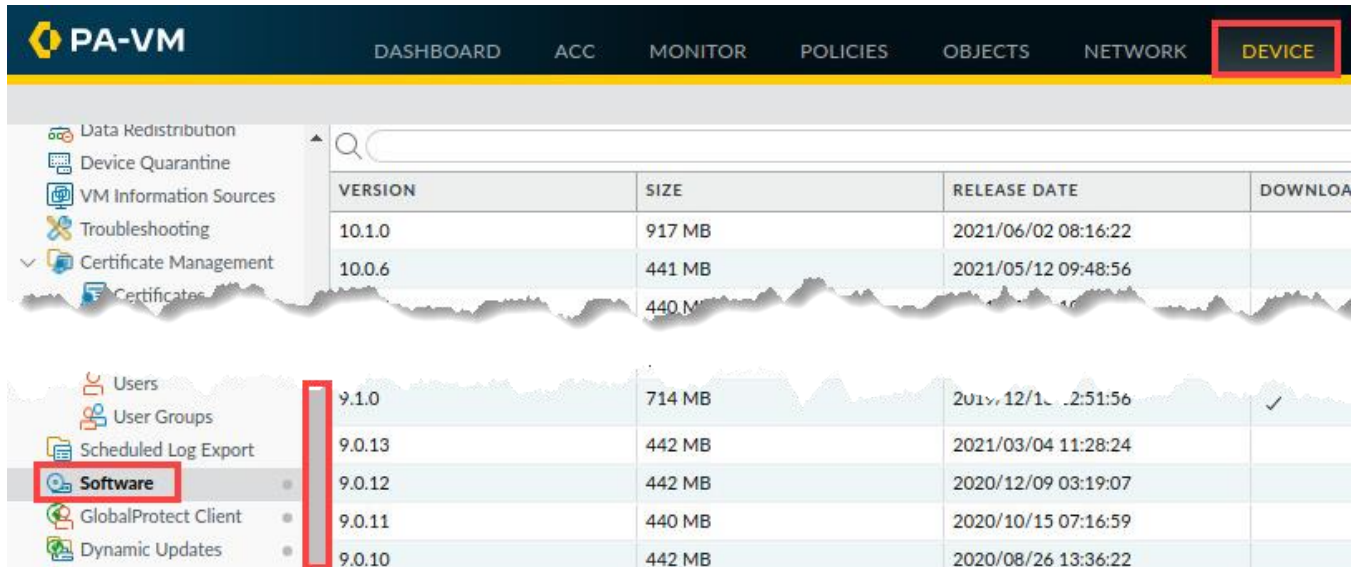
PERMITTED IP ADDRESSES	DESCRIPTION
192.168.1.20/24	MGT access from this host only

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

1.5 Check for New PAN-OS Software

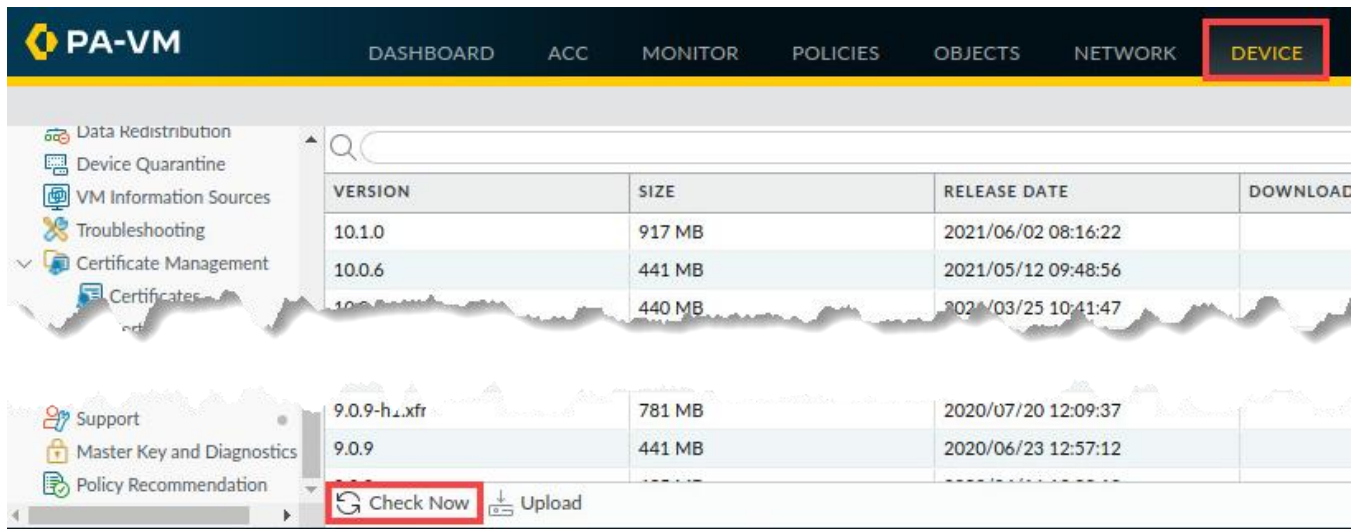
In this section, you will check for new PAN-OS software and commit your changes.

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



VERSION	SIZE	RELEASE DATE	DOWNLOAD
10.1.0	917 MB	2021/06/02 08:16:22	
10.0.6	441 MB	2021/05/12 09:48:56	
9.1.0	714 MB	2021/12/12 12:51:56	✓
9.0.13	442 MB	2021/03/04 11:28:24	
9.0.12	442 MB	2020/12/09 03:19:07	
9.0.11	440 MB	2020/10/15 07:16:59	
9.0.10	442 MB	2020/08/26 13:36:22	

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



VERSION	SIZE	RELEASE DATE	DOWNLOAD
10.1.0	917 MB	2021/06/02 08:16:22	
10.0.6	441 MB	2021/05/12 09:48:56	
10.0.5	440 MB	2021/03/25 10:41:47	
9.0.9-h2.xfr	781 MB	2020/07/20 12:09:37	
9.0.9	441 MB	2020/06/23 12:57:12	

Check Now Upload

- 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	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

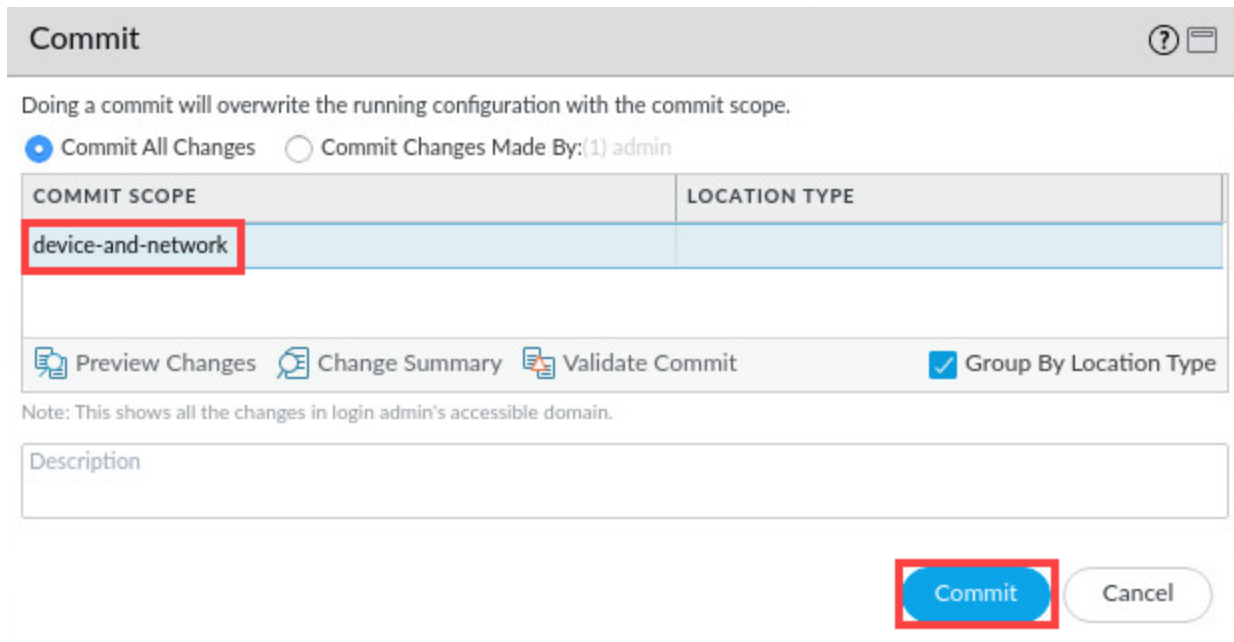


The list you see will vary from this example. Also, newer versions of PAN-OS software may be available at the time you carry out these steps. Do not upgrade your firewall.

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

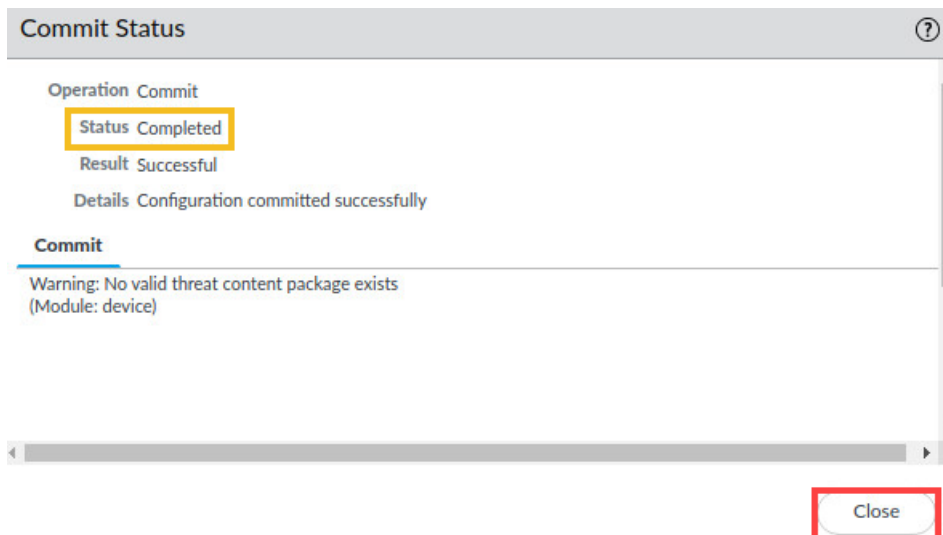


5. In the *Commit* window, view the commit scope. Click **Commit**.



The screenshot shows the 'Commit' window. At the top, it says 'Doing a commit will overwrite the running configuration with the commit scope.' Below this, there are two radio buttons: 'Commit All Changes' (selected) and 'Commit Changes Made By:(1) admin'. A table with two columns, 'COMMIT SCOPE' and 'LOCATION TYPE', is shown. The first row in the table has 'device-and-network' in the 'COMMIT SCOPE' column, which is highlighted with a red box. Below the table, there are three icons with labels: 'Preview Changes', 'Change Summary', and 'Validate Commit'. To the right of these is a checkbox labeled 'Group By Location Type' which is checked. Below the icons, a note states: 'Note: This shows all the changes in login admin's accessible domain.' At the bottom right, there are two buttons: 'Commit' (highlighted with a red box) and 'Cancel'.

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



The screenshot shows the 'Commit Status' window. It has a title bar 'Commit Status' with a help icon. Below the title bar, there is a section 'Operation Commit' with a sub-section 'Status Completed' (highlighted with a yellow box). Below this, it says 'Result Successful' and 'Details Configuration committed successfully'. There is a section 'Commit' with a warning message: 'Warning: No valid threat content package exists (Module: device)'. At the bottom right, there is a button labeled 'Close' (highlighted with a red box).

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