PALO ALTO NETWORKS – EDU 210

Lab 1: Connect to the Management Network

Document Version: 2022-07-18

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.

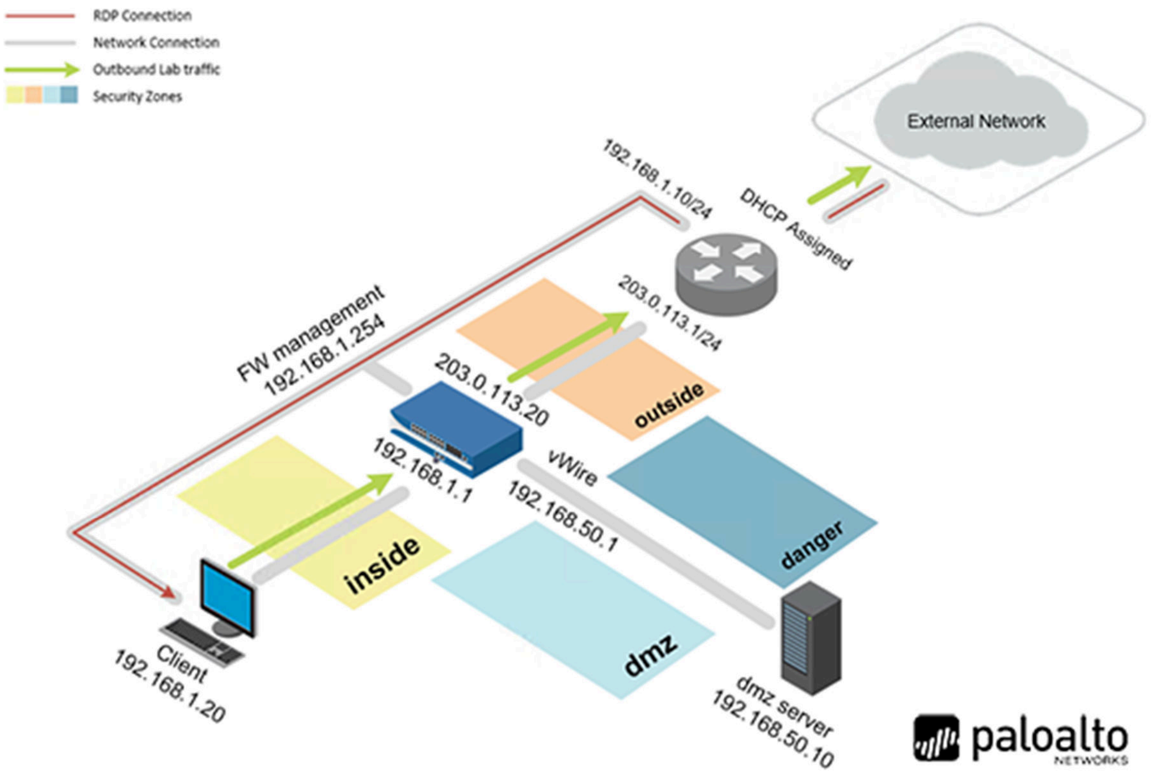
In this lab, you will connect to the Palo Alto Networks firewall management interface and configure basic settings to provide the firewall with network access.

Objective

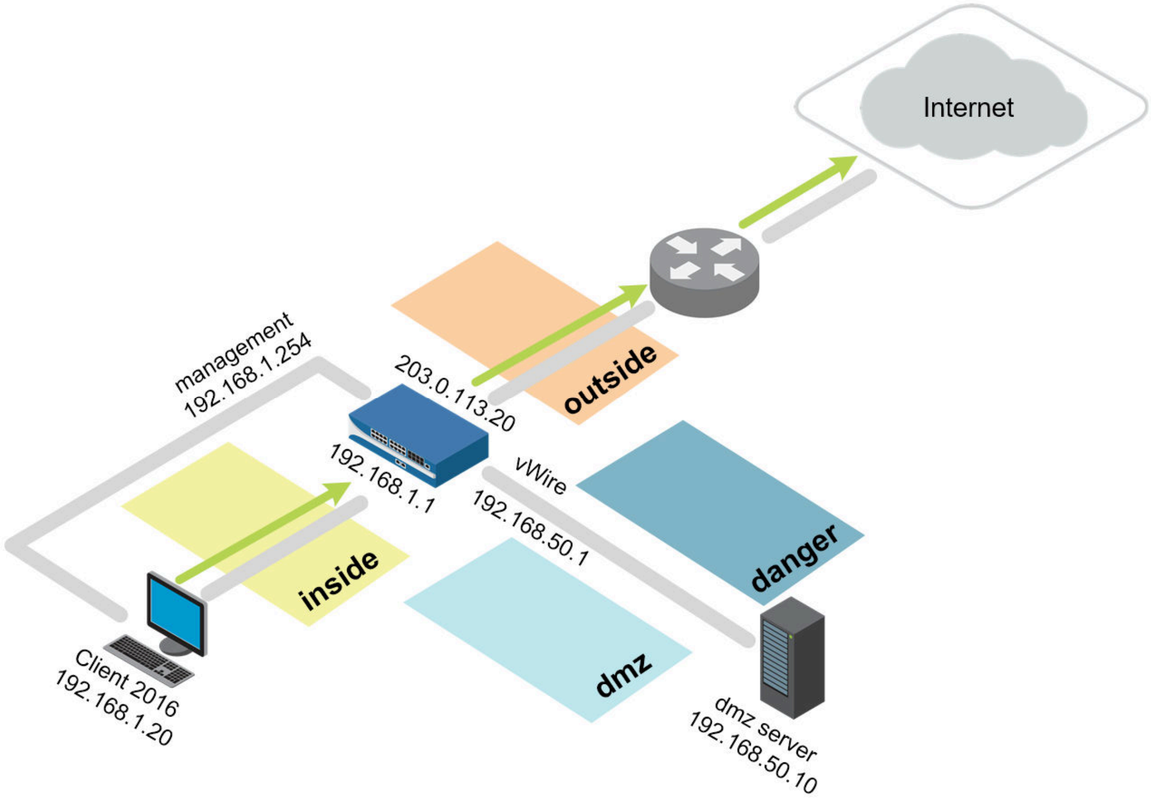
In this lab, you will perform the following tasks:

- 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.

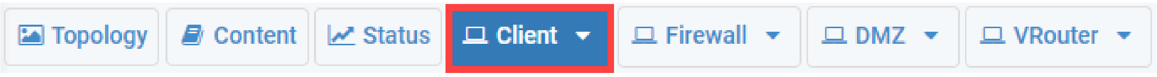
Virtual Machine	**IP Address**	**Account** (if needed)	**Password** (if needed)
Client	192.168.1.20	lab-user	**Pal0Alt0!**
DMZ	192.168.50.10	root	**Pal0Alt0!**
Firewall	192.168.1.254	admin	**Pal0Alt0!**
VRouter	192.168.1.10	root	**Pal0Alt0!**

1 Connect to the Management Network

1.1 Load Lab Configuration

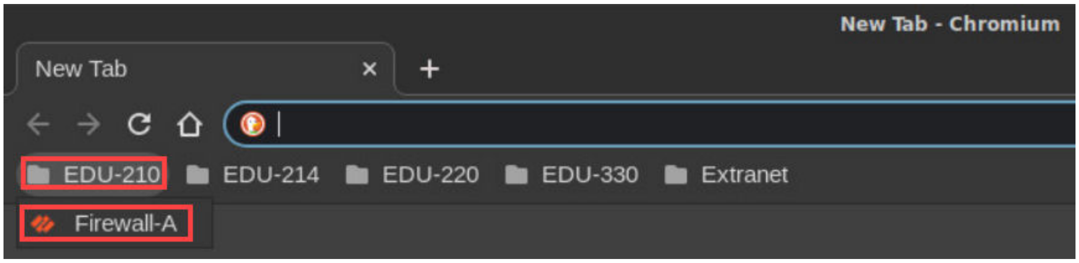
In this section, you will load the Firewall configuration file.

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

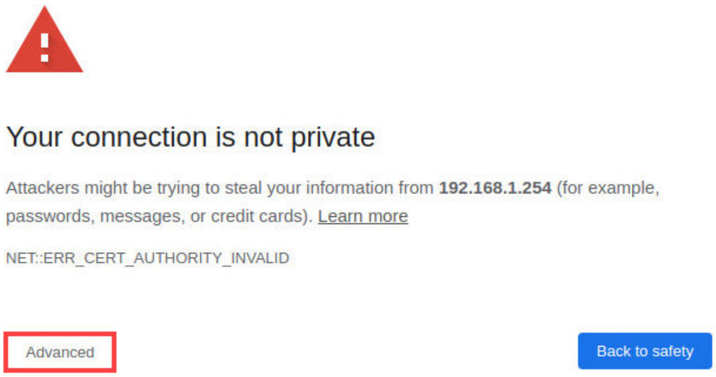


2. Double-click the **Chromium Web Browser** icon located on the desktop.

3. In the *Chromium* web browser, click on the **EDU-210** bookmark folder in the bookmarks bar and then click on **Firewall-A**.



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



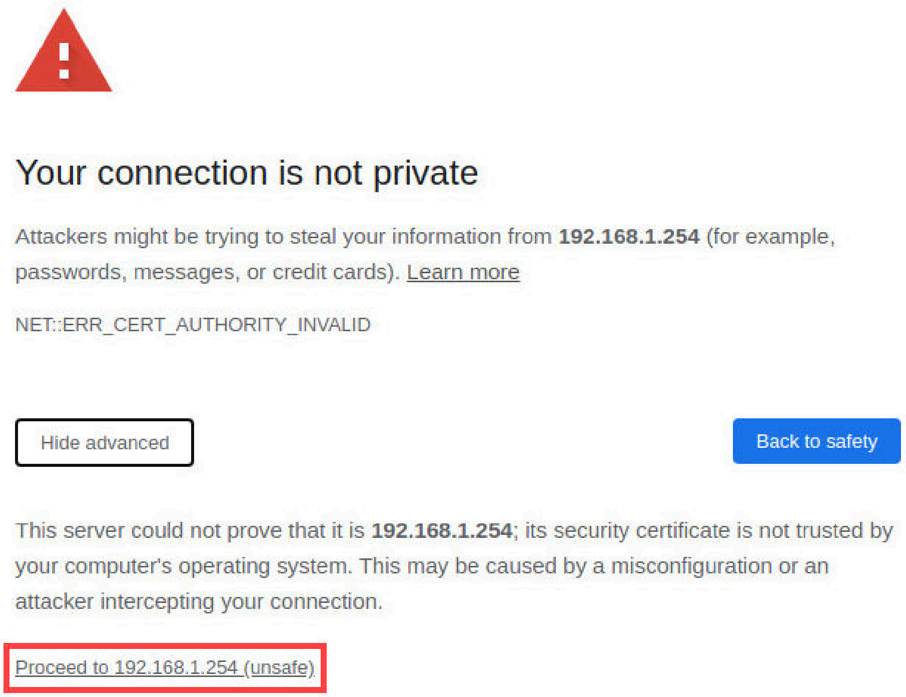
Your connection is not private

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

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

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



Your connection is not private

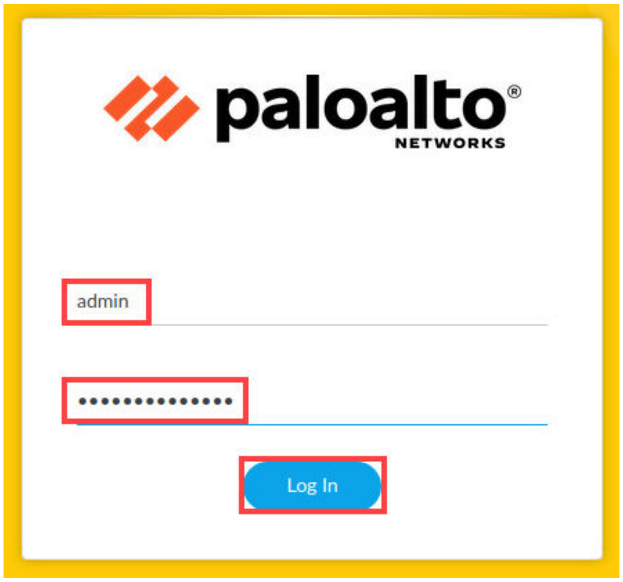
Attackers might be trying to steal your information from **192.168.1.254** (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_AUTHORITY_INVALID

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

Proceed to 192.168.1.254 (unsafe)

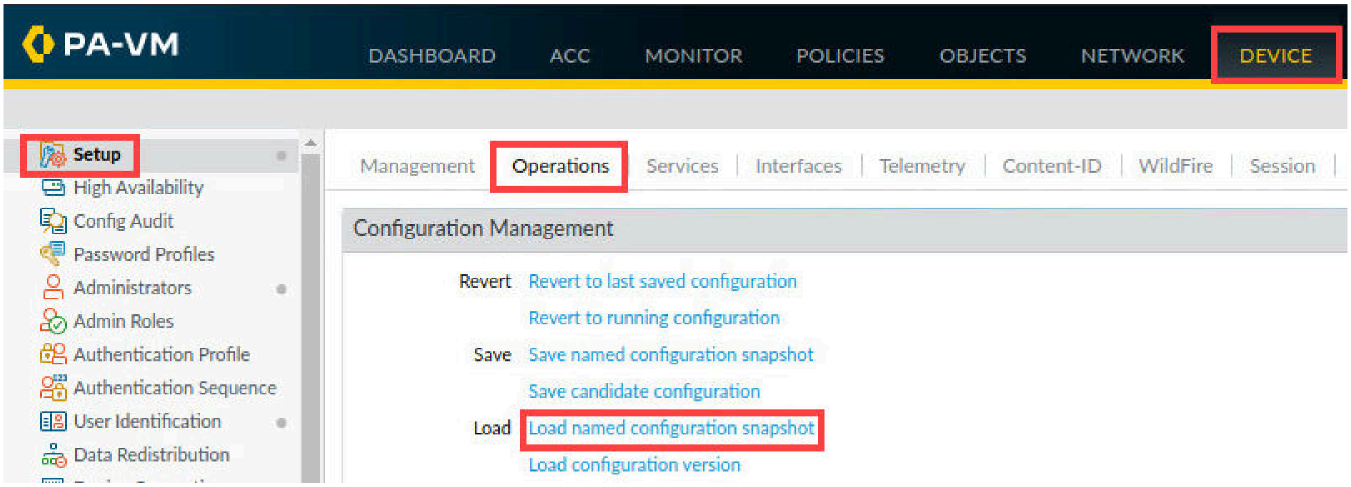
6. Log in to the firewall web interface as username **`admin`**, password **`Pal0Alt0!`**.



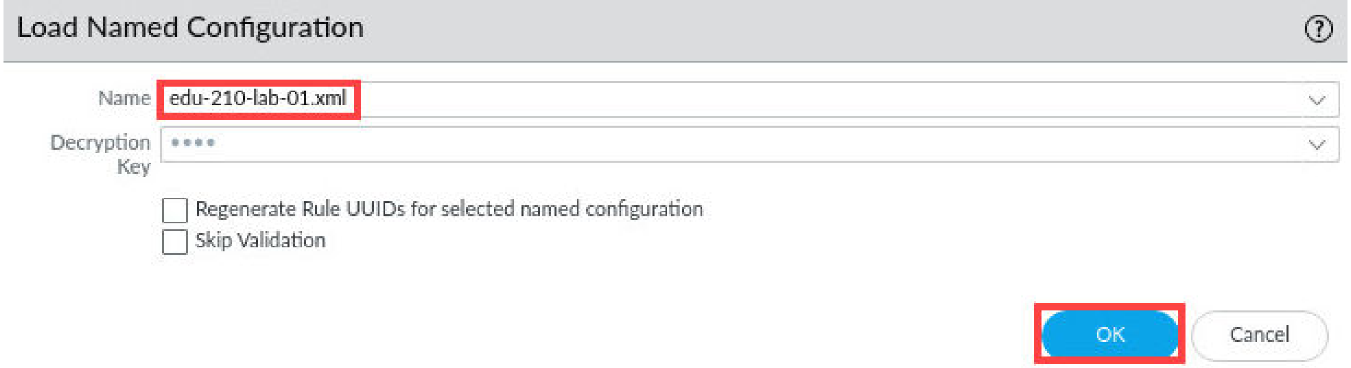
admin

••••••••••••••

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-lab-01.xml** from the *Name* dropdown box and click **OK**.


Load Named Configuration

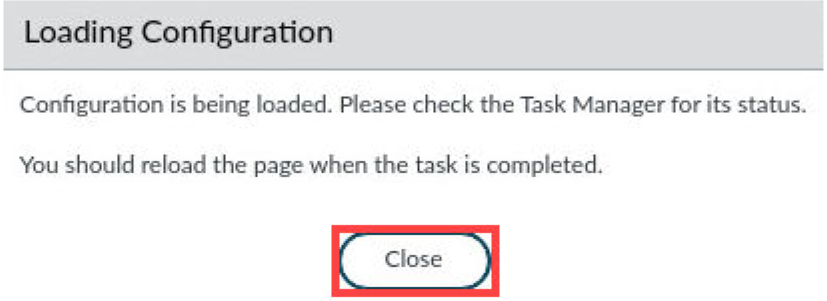
Name: edu-210-lab-01.xml

Decryption Key: ••••

□ Regenerate Rule UUIDs for selected named configuration

□ Skip Validation

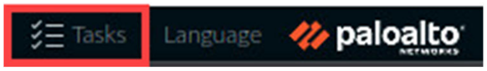
9. In *the Loading Configuration* window, a message will show *Configuration is being loaded. Please check the Task Manager for its status. You should reload the page when the task is completed.* Click **Close** to continue.


Loading Configuration

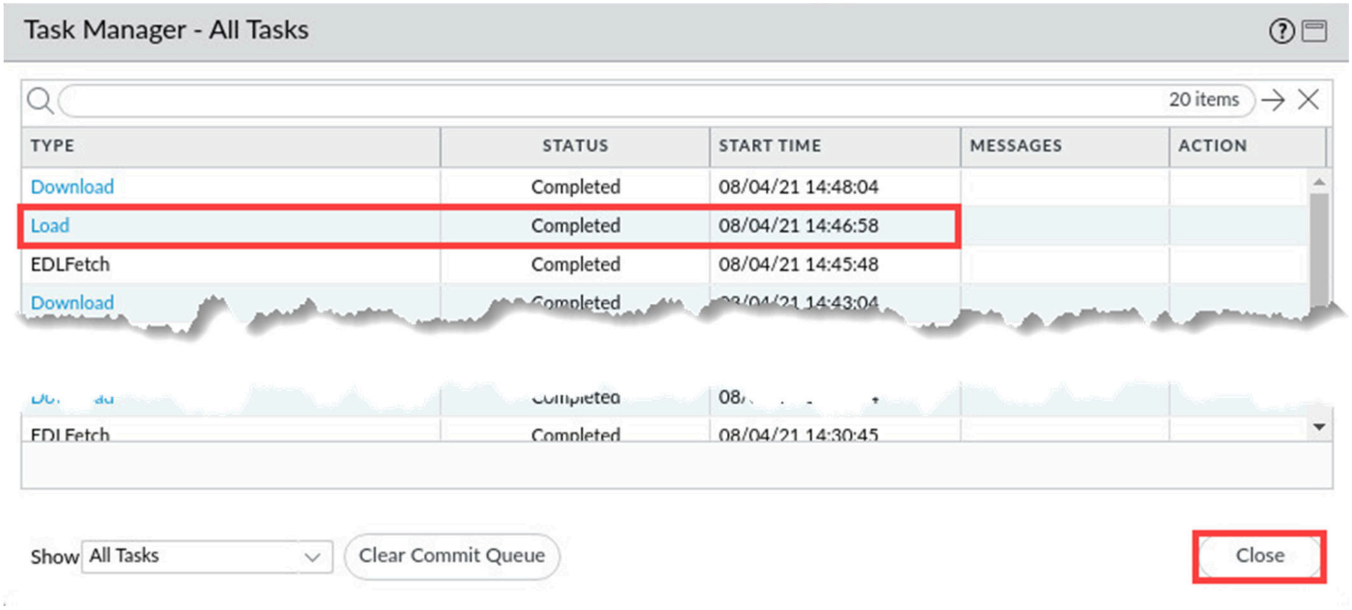
Configuration is being loaded. Please check the Task Manager for its status.

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**

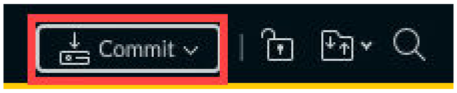


Task Manager - All Tasks

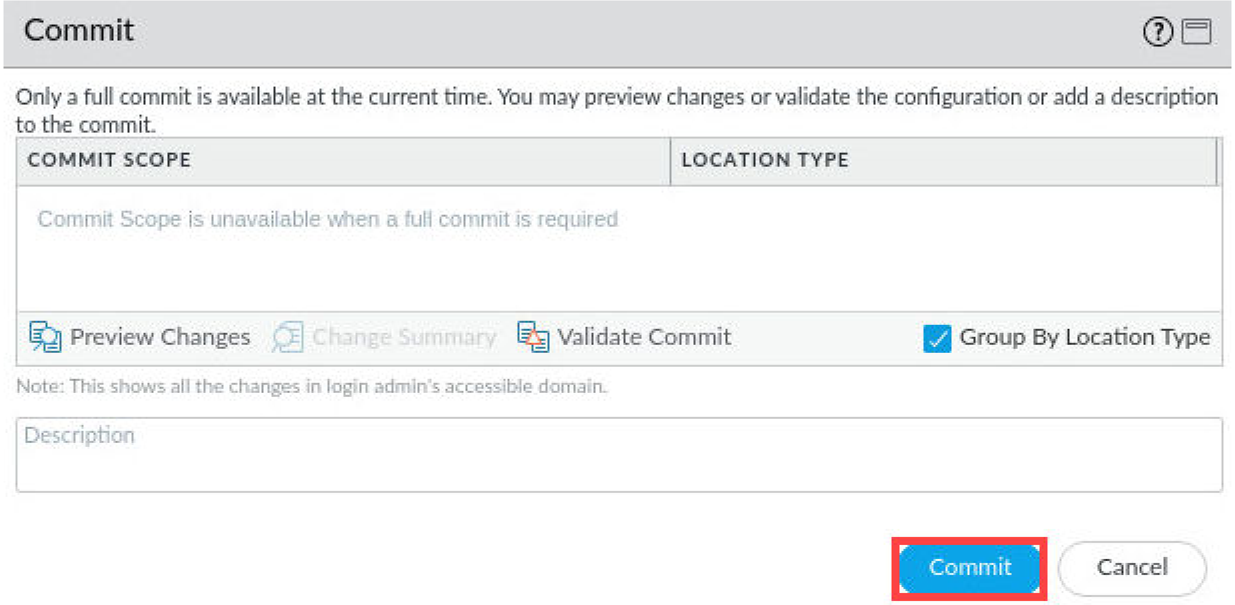
20 items

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		
Download	Completed	08/[illegible]		
EDLFetch	Completed	08/04/21 14:30:45		

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.

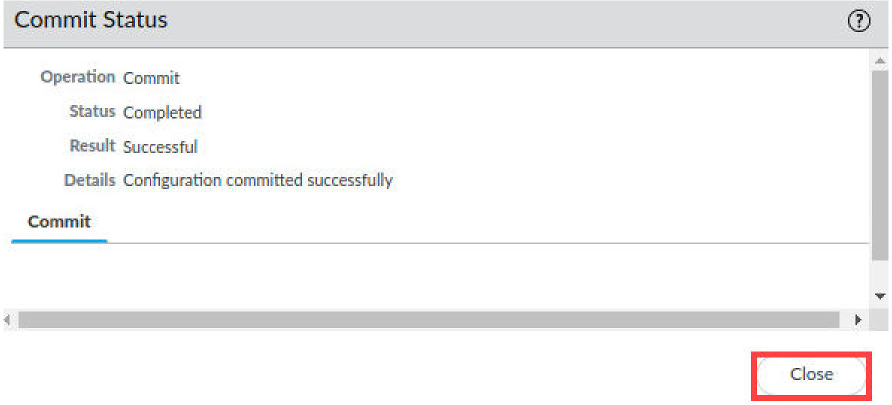
COMMIT SCOPE	LOCATION TYPE
Commit Scope is unavailable when a full commit is required	

☑ Group By Location Type

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

Description

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



Commit Status

Operation Commit
Status Completed
Result Successful
Details Configuration committed successfully

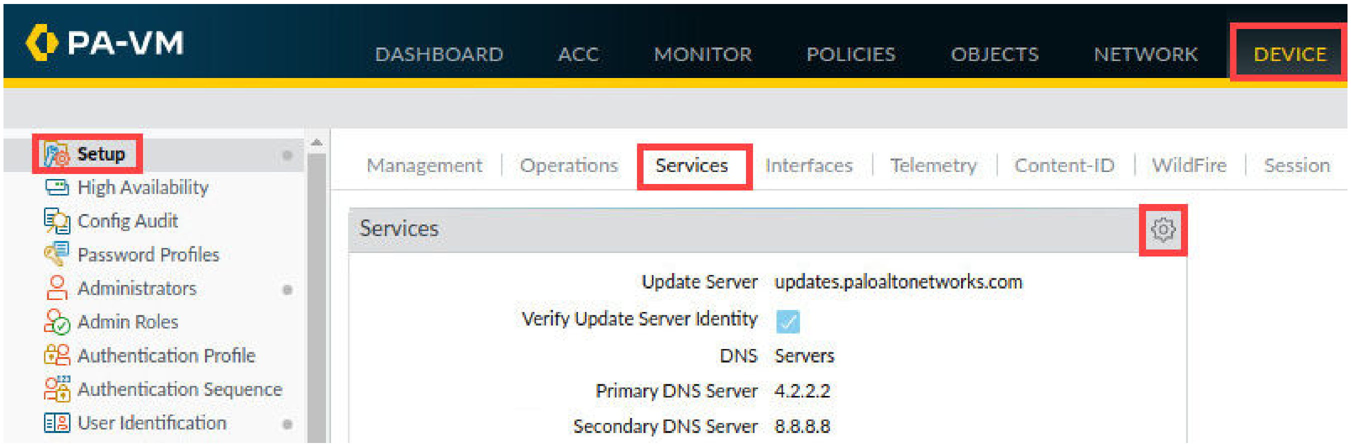
The commit process takes changes made to the Firewall and copies them to the running configuration, which will activate all configuration changes since the last commit.

15. 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.

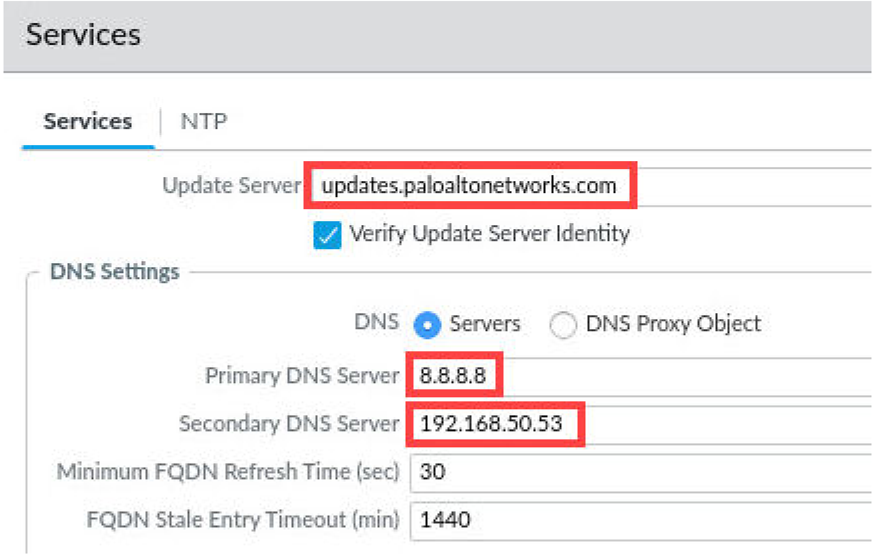
1. In the web interface, select **Device > Setup > Services**. Click the **Services gear** icon to open the *Services* window.



Services

Update Server updates.paloaltonetworks.com
Verify Update Server Identity ☑
DNS Servers
Primary DNS Server 4.2.2.2
Secondary DNS Server 8.8.8.8

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`**.

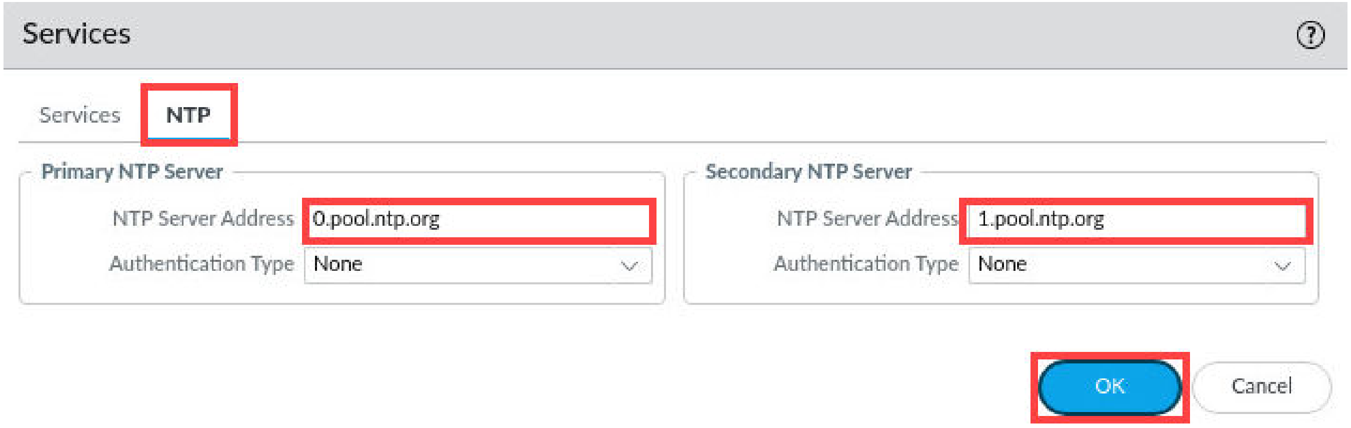


Update Server updates.paloaltonetworks.com
☑ Verify Update Server Identity

DNS Settings

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

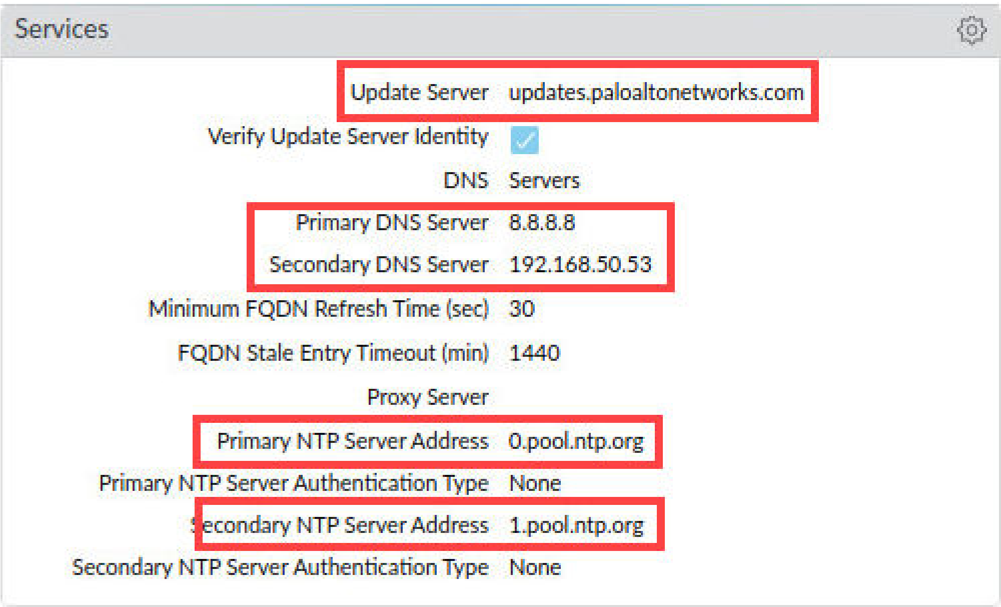
Authentication Type: None

Secondary NTP Server

NTP Server Address: 1.pool.ntp.org

Authentication Type: None

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



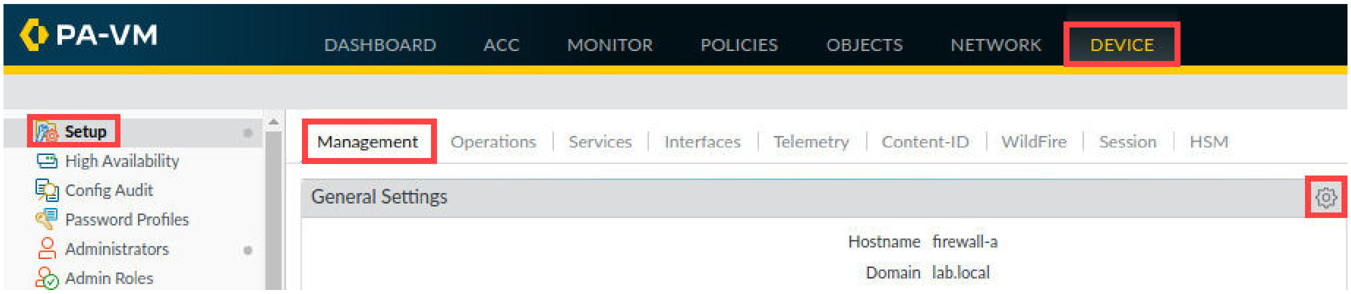
Update Server	updates.paloaltonetworks.com
Verify Update Server Identity	☑
DNS	Servers
Primary DNS Server	8.8.8.8
Secondary DNS Server	192.168.50.53
Minimum FQDN Refresh Time (sec)	30
FQDN Stale Entry Timeout (min)	1440
Proxy Server	
Primary NTP Server Address	0.pool.ntp.org
Primary NTP Server Authentication 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.

1.3 Configure General Settings of the Firewall

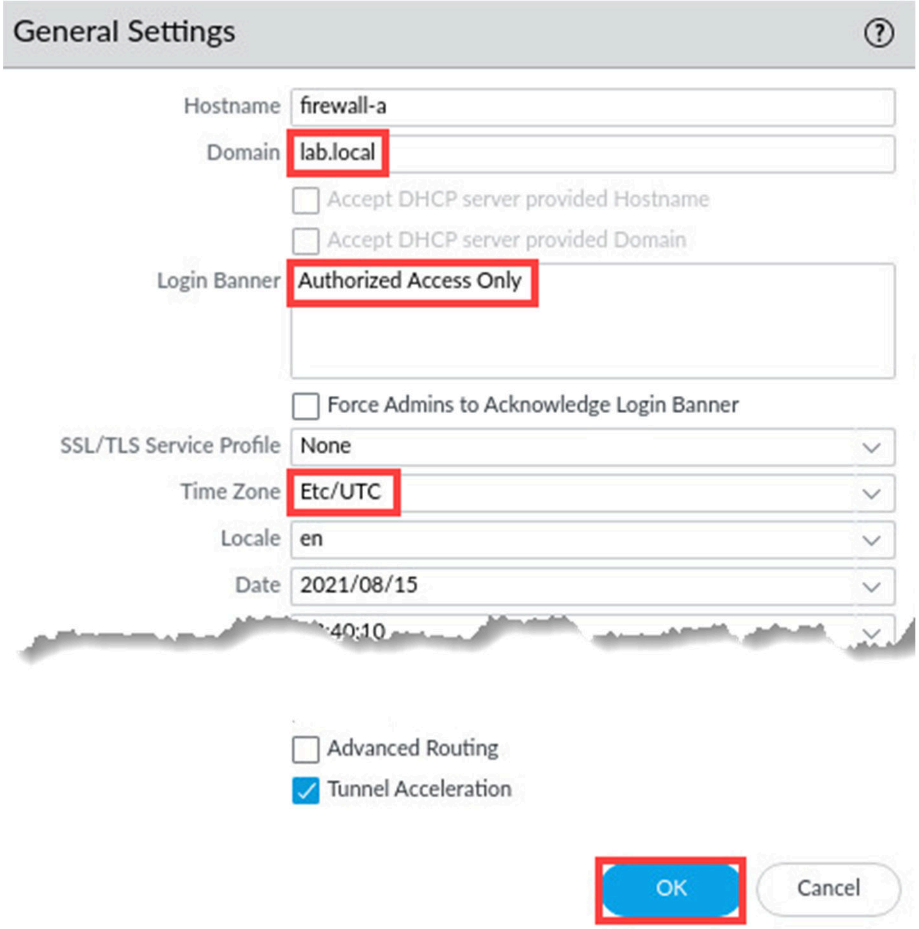
In this section, you will configure the general settings of the Palo Alto Networks Firewall. You will verify the Domain, set your location's time zone, and set a login banner.

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



Hostname firewall-a
Domain lab.local

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**.



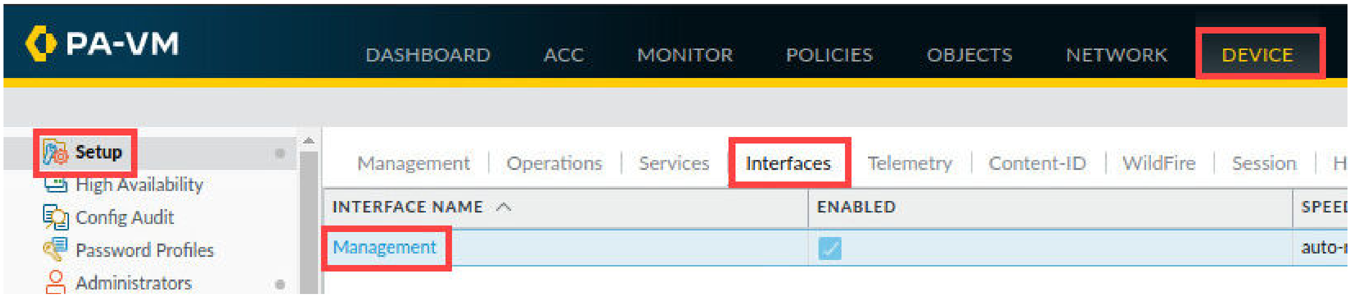
Hostname: firewall-a
Domain: lab.local
□ Accept DHCP server provided Hostname
□ Accept DHCP server provided Domain
Login Banner: Authorized Access Only
□ Force Admins to Acknowledge Login Banner
SSL/TLS Service Profile: None
Time Zone: Etc/UTC
Locale: en
Date: 2021/08/15
:40:10
□ Advanced Routing
☑ Tunnel Acceleration

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

1.4 Modify the Management Interface

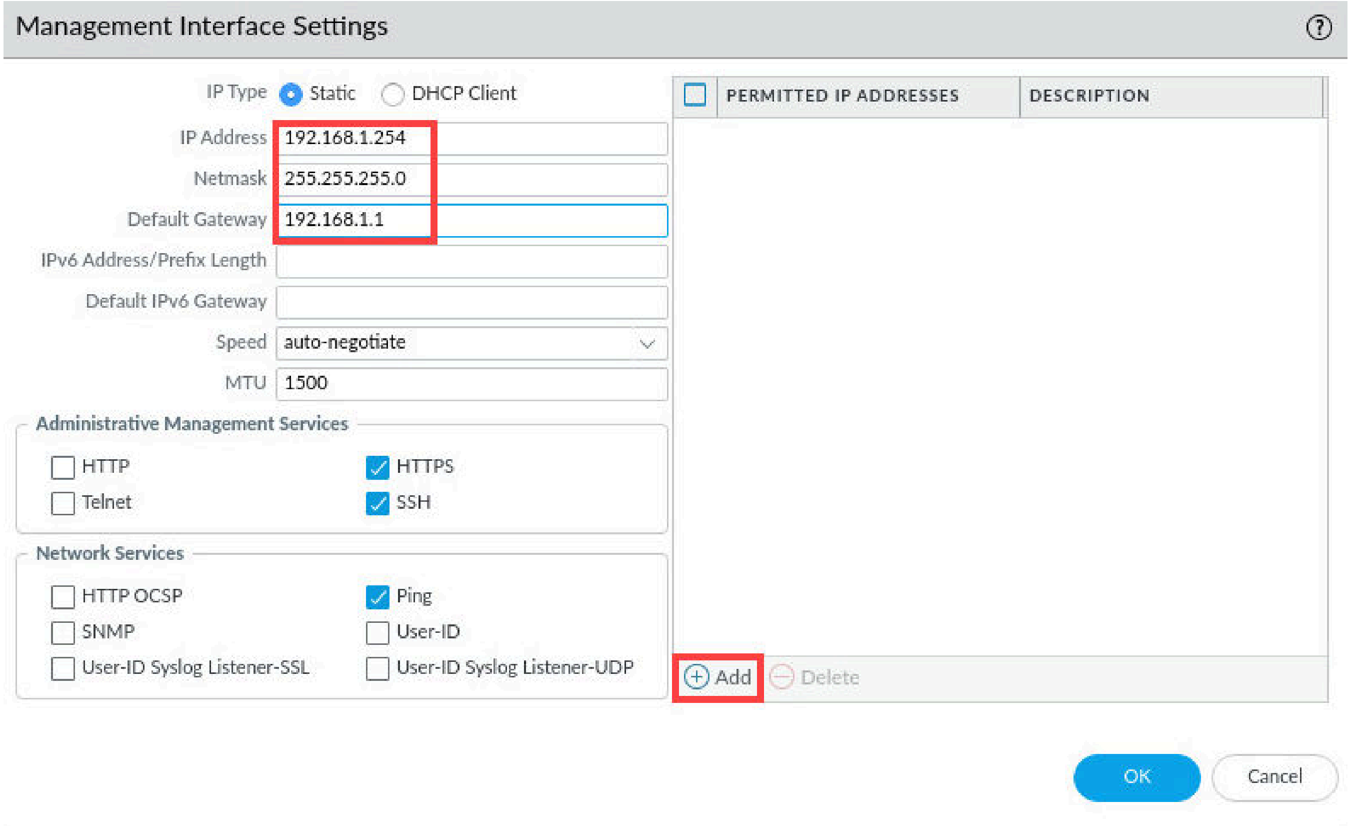
In this section, you will modify the management interface of the firewall.

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



INTERFACE NAME	ENABLED	SPEEI
Management	☑	auto-i

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.**



Management Interface Settings

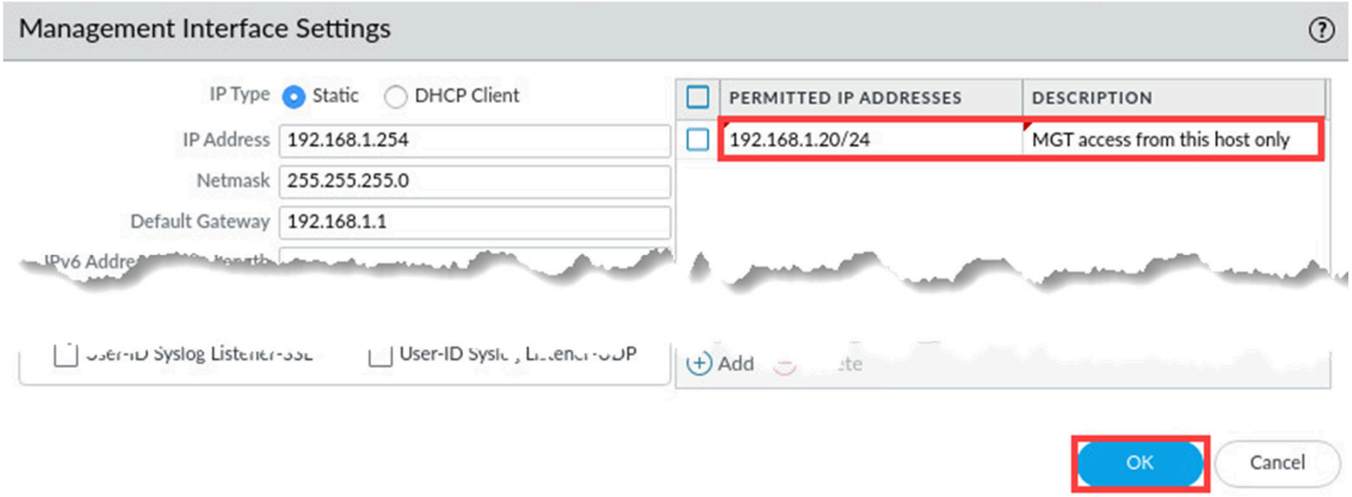
IP Type ● Static ○ DHCP Client
IP Address: 192.168.1.254
Netmask: 255.255.255.0
Default Gateway: 192.168.1.1
IPv6 Address/Prefix Length:
Default IPv6 Gateway:
Speed: auto-negotiate
MTU: 1500

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

□	PERMITTED IP ADDRESSES	DESCRIPTION

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 192.168.1.1

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

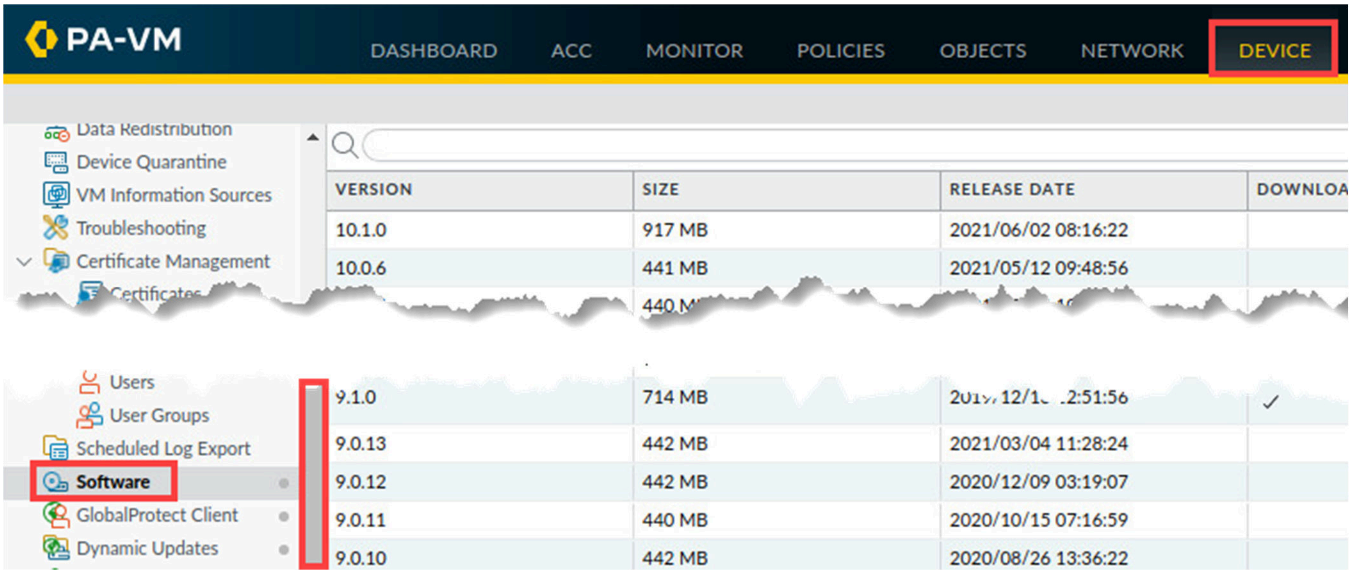
IPv6 Address/Prefix Length
□ User-ID Syslog Listener-SSL
□ User-ID Syslog Listener-UDP
⊕ Add
Delete
OK
Cancel

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

1.5 Check for New PAN-OS Software

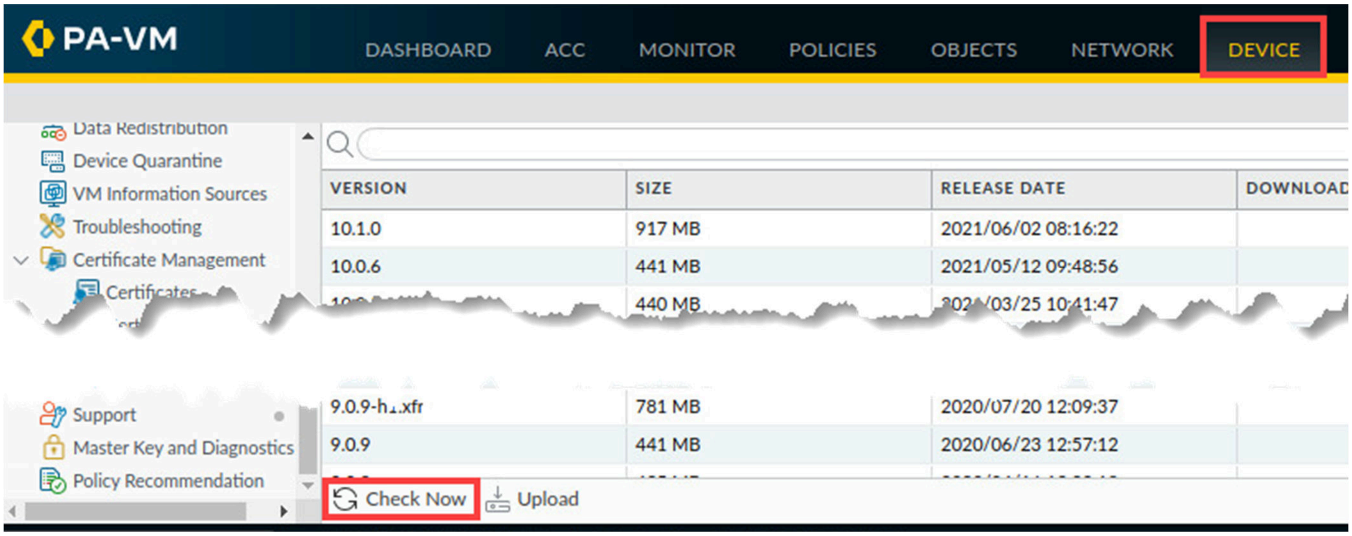
In this section, you will check for new PAN-OS software and commit your changes.

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



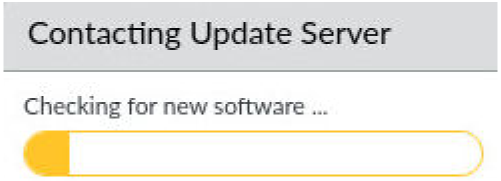
VERSION	SIZE	RELEASE DATE	DOWNLOA
10.1.0	917 MB	2021/06/02 08:16:22	
10.0.6	441 MB	2021/05/12 09:48:56	
	440 M		
9.1.0	714 MB	2019/12/1 2:51:56	✓
9.0.13	442 MB	2021/03/04 11:28:24	
9.0.12	442 MB	2020/12/09 03:19:07	
9.0.11	440 MB	2020/10/15 07:16:59	
9.0.10	442 MB	2020/08/26 13:36:22	

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



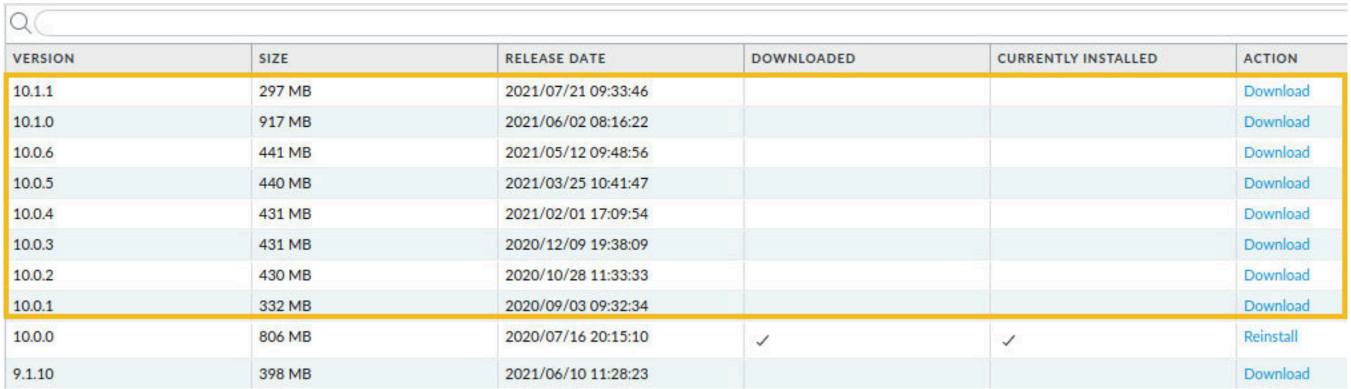
VERSION	SIZE	RELEASE DATE	DOWNLOAD
10.1.0	917 MB	2021/06/02 08:16:22	
10.0.6	441 MB	2021/05/12 09:48:56	
	440 MB	202 /03/25 10:41:47	
9.0.9-h1.xfr	781 MB	2020/07/20 12:09:37	
9.0.9	441 MB	2020/06/23 12:57:12	

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

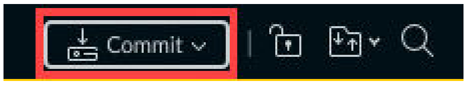
Checking for new software ...



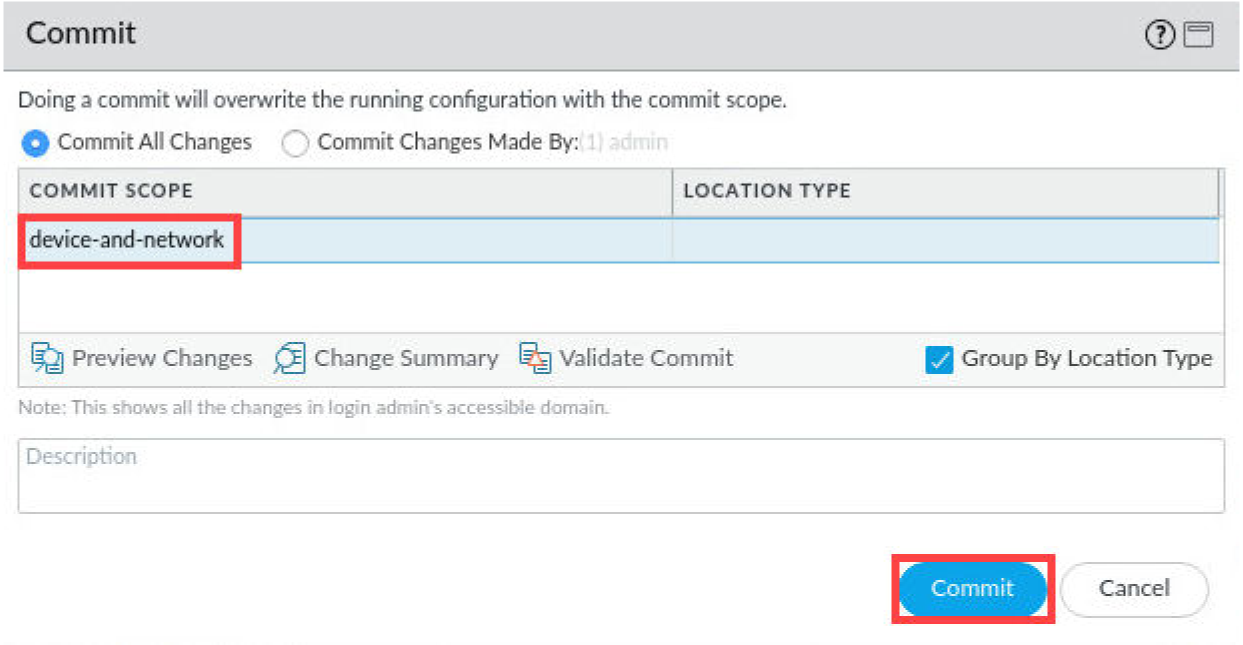
VERSION	SIZE	RELEASE DATE	DOWNLOADED	CURRENTLY INSTALLED	ACTION
10.1.1	297 MB	2021/07/21 09:33:46			Download
10.1.0	917 MB	2021/06/02 08:16:22			Download
10.0.6	441 MB	2021/05/12 09:48:56			Download
10.0.5	440 MB	2021/03/25 10:41:47			Download
10.0.4	431 MB	2021/02/01 17:09:54			Download
10.0.3	431 MB	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**.



Commit

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

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

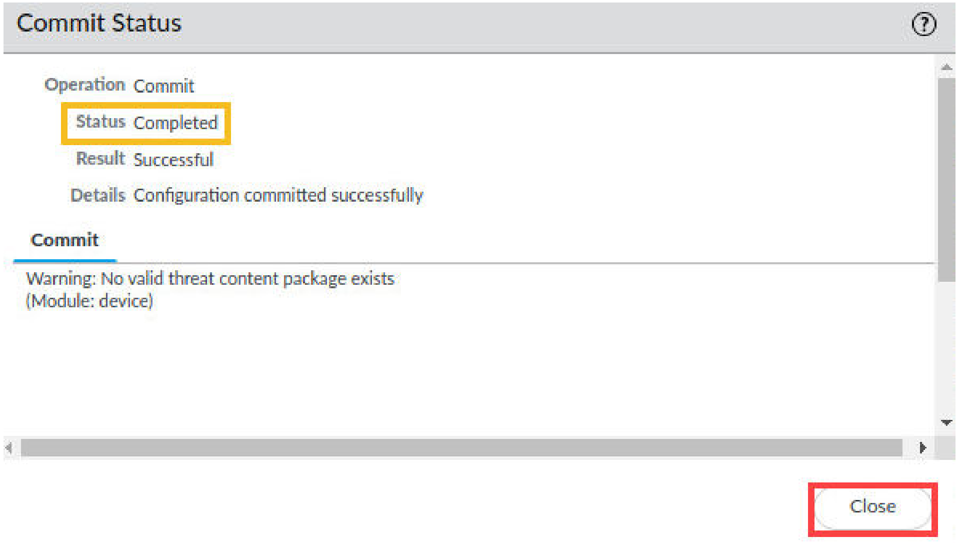
COMMIT SCOPE	LOCATION TYPE
device-and-network	

Preview Changes Change Summary Validate Commit ☑ Group By Location Type

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

Description

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



Commit Status

Operation Commit
Status Completed
Result Successful
Details Configuration committed successfully

Commit

Warning: No valid threat content package exists
(Module: device)

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