PALO ALTO NETWORKS FIREWALL 11.0 ESSENTIALS

Lab 2: Managing Firewall Configurations

Document Version: 2025-10-13

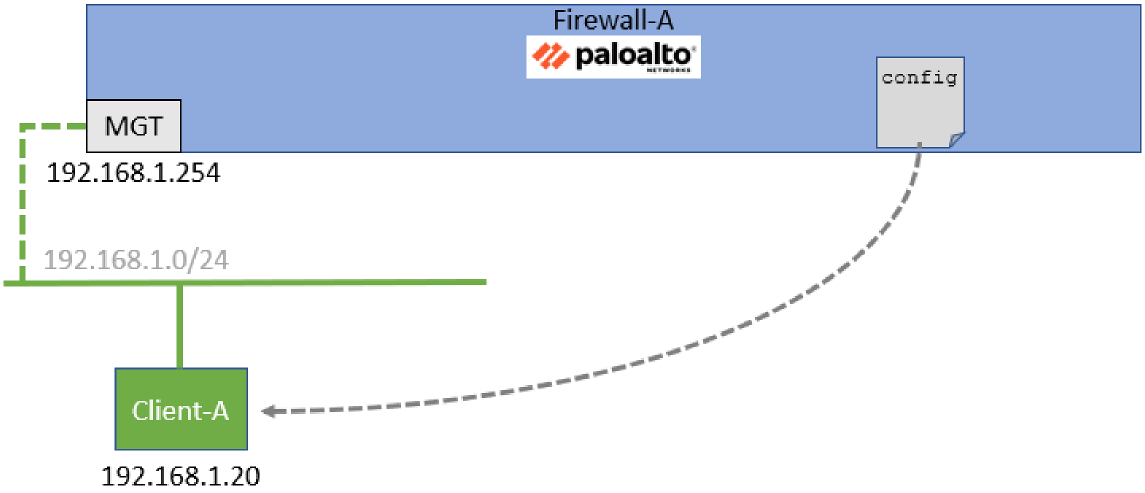
Contents

Introduction

Now that you have set up the firewall to allow management access, you need to make certain that you can save, load, and restore configurations to the device. You also need to familiarize yourself with the log files available, and with searching through the logs to find specific events.

Because the firewall is not scheduled to be deployed for a few days, you can spend some time on these tasks without worrying about affecting your production networks.

In this lab, you will work with snapshots, revert, and preview configurations changes, examine log files and create and use the filter builder.

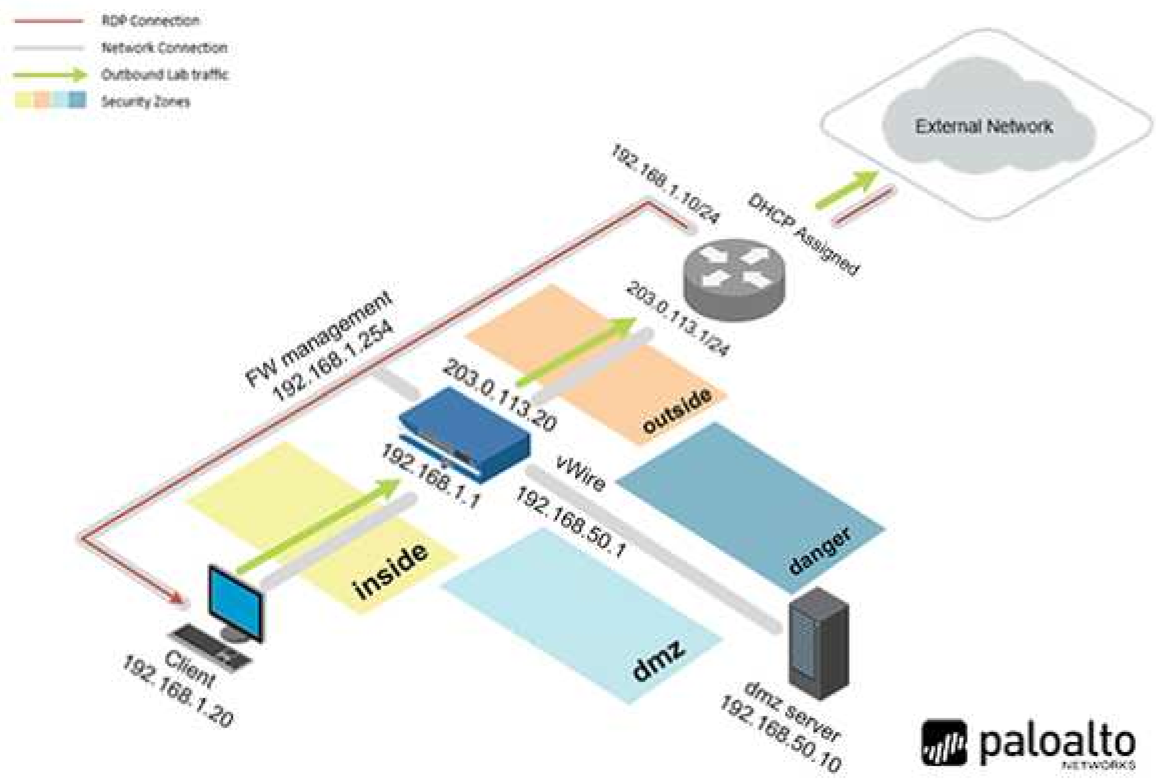


Objective

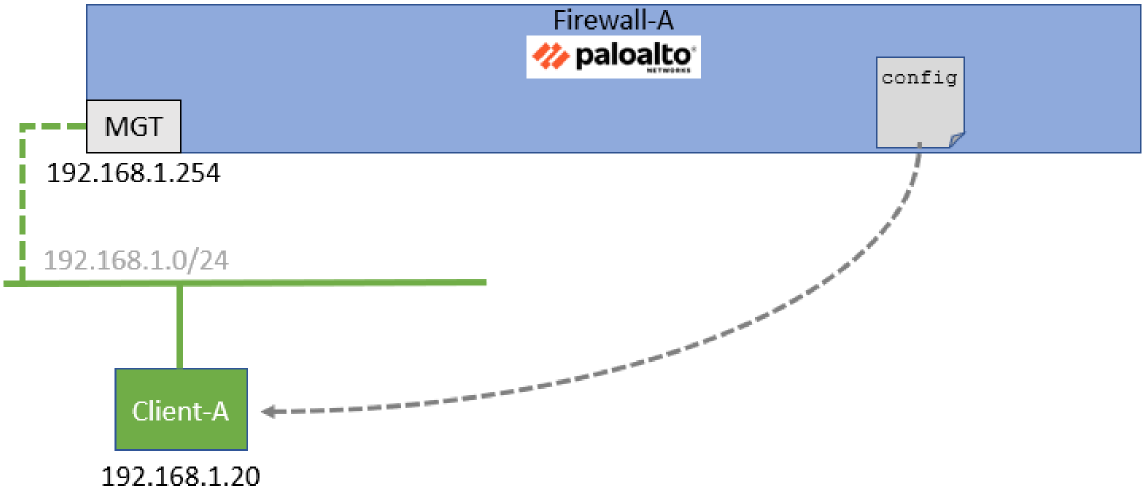
In this lab, you will perform the following tasks:

- Load a baseline configuration.
- Save a named configuration snapshot.
- Export a named configuration snapshot.
- Save ongoing configuration changes before a commit.
- Revert ongoing configuration changes.
- Preview configuration changes.
- Examine System and Configuration log files.
- Create a log file filter.
- Use the Filter Builder.

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:

- 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 Managing Firewall Configurations – 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-02.xml** to the Firewall.

1.2 Save a Named Configuration Snapshot

- Save the firewall's current configuration file as **firewall-a-<Today's Date>**.

1.3 Revert Ongoing Configuration Changes

- Change the value for the **Primary DNS Server** to **88.8.8.8** (an easy mistake to make).
- Verify the mistake in the **Services** section.
- Use the **Revert Changes** option to restore the **Primary DNS Server** to its original setting (**8.8.8.8**).

1.4 Preview Configuration Changes

- Modify the SNMP configuration with the following settings:
  - Set the **Physical Location** to **Santa Clara, CA, USA**.
  - Set the **Contact** to **Unit 42**.
  - Set the **SNMP Community String** to **paloalto42**.
- Use the **Preview Changes** option to compare the **Running** configuration to the **Candidate** configuration.
- Do not commit changes at this stage.

1.5 Modify System Log File Columns

- Hide the **Object** column in the System Log display.
- Move the **Severity** column to the far left side of the System Log display.

1.6 Create a System Log File Filter

- Create and apply a filter in the System Log that displays only entries with a **Severity** level of **informational.**

1.7 Use the Filter Builder

- Use the **Filter Builder** to create a filter that will display all entries in the **System** log that have occurred in the last **60 minutes.**

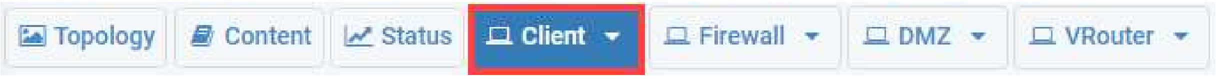
2 Managing Firewall Configurations – Detailed Lab Steps

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.

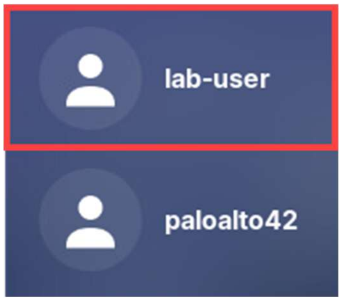
2.1 Load Lab Configuration

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

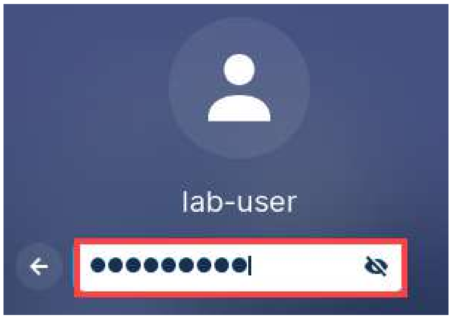
1. Click on the **Client** tab to access the Client PC.



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

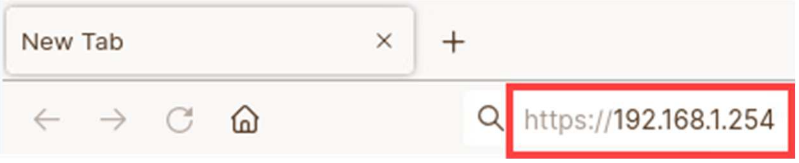


3. For the *lab-user* password, enter **Pal0Alt0!** and press **Enter**.

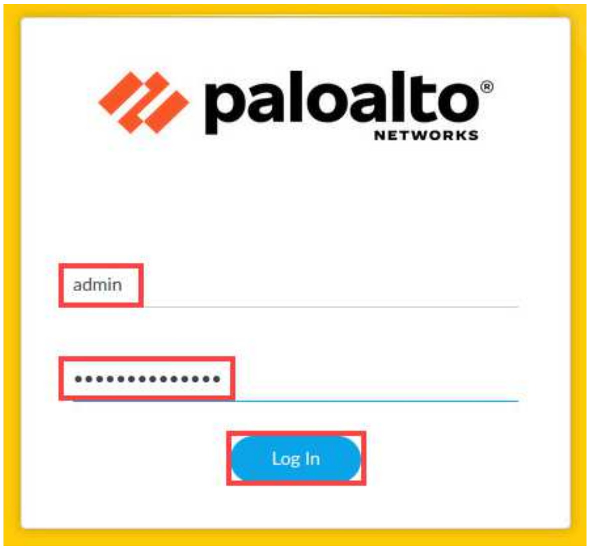


4. Double-click the **Firefox Web Browser** icon located on the *Desktop*.

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

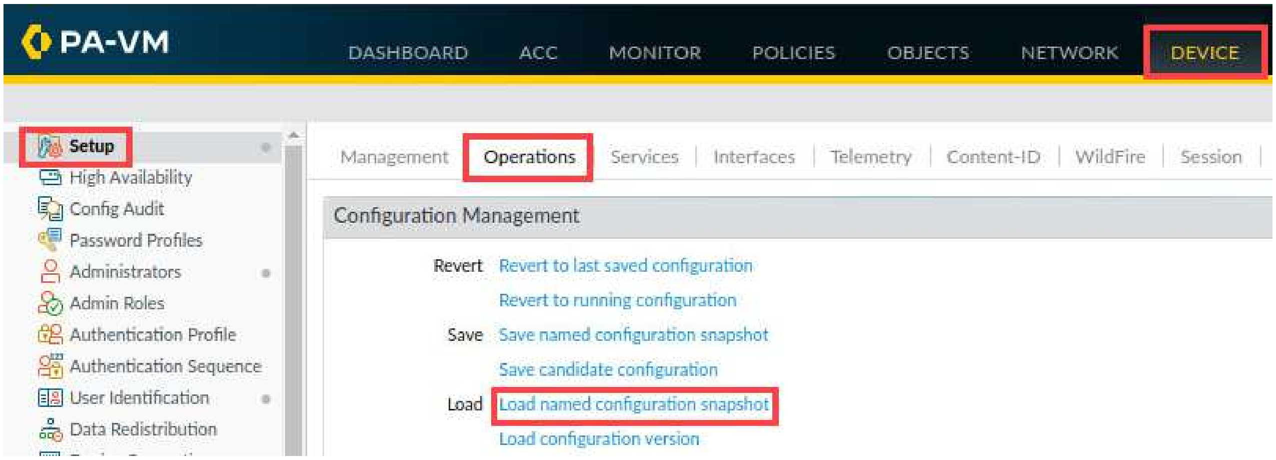


6. Log in to the Firewall web interface as username **`admin`**, password **`Pal0Alt0!`.**

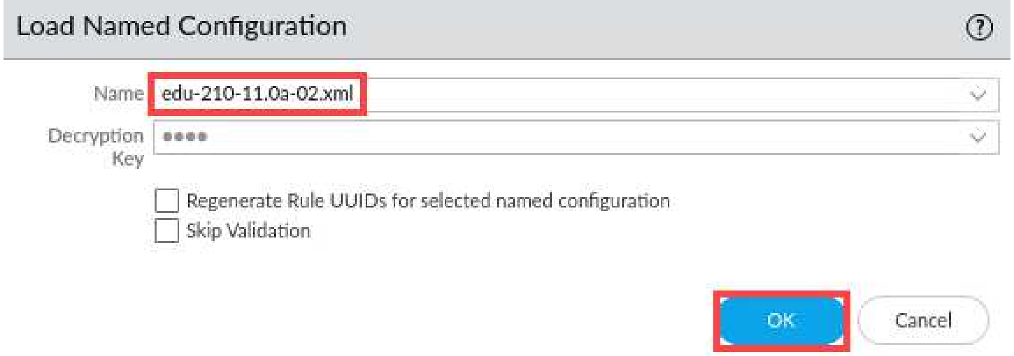


If you do not immediately see the login page, please wait an additional 1-3 minutes for the *Firewall* to fully initialize. If needed, refresh the page.

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-02.xml** from the *Name* drop-down box and click **OK**.



Load Named Configuration

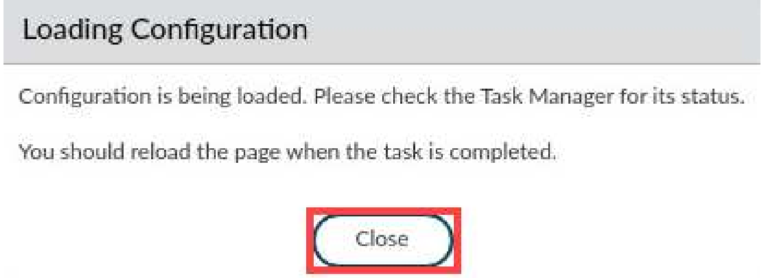
Name: edu-210-11.0a-02.xml

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.

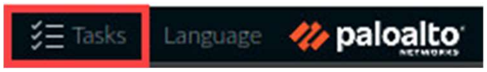


Loading Configuration

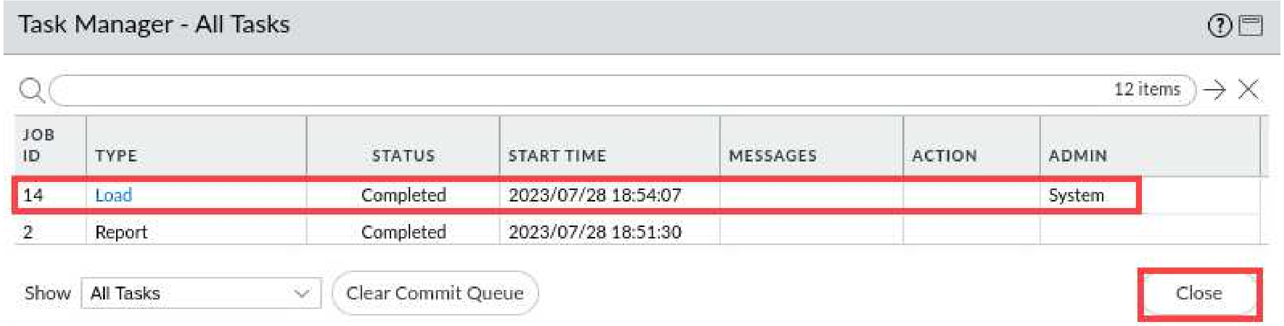
Configuration is being loaded. Please check the Task Manager for its status.

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.**



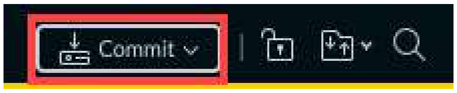
Task Manager - All Tasks

12 items

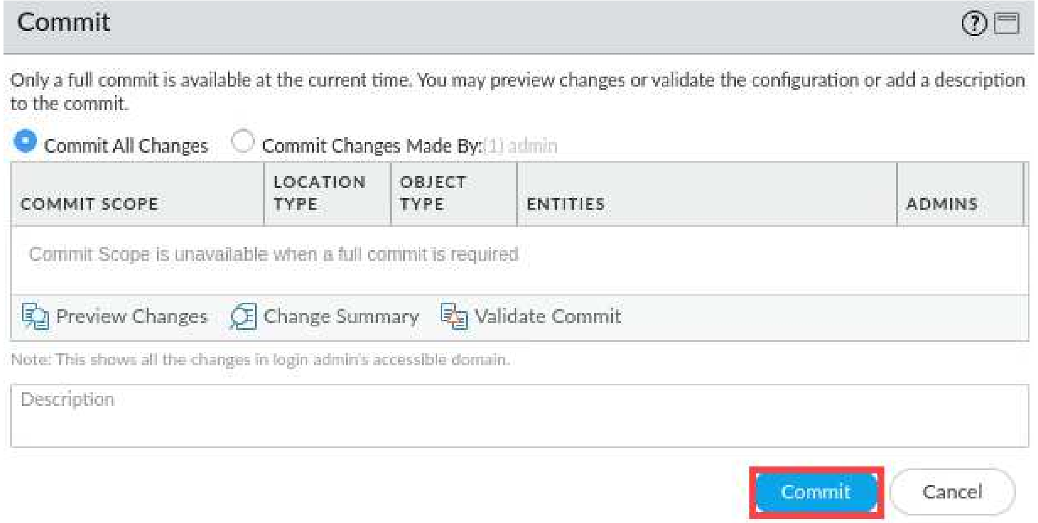
JOB ID	TYPE	STATUS	START TIME	MESSAGES	ACTION	ADMIN
14	Load	Completed	2023/07/28 18:54:07			System
2	Report	Completed	2023/07/28 18:51:30			

Show: All Tasks

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

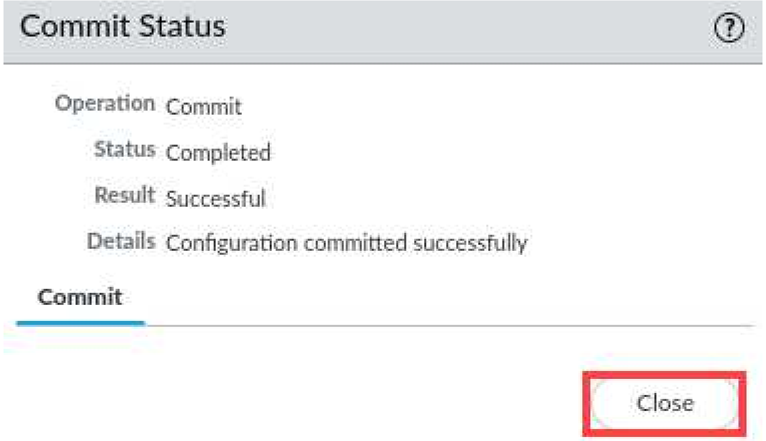
Only a full commit is available at the current time. You may preview changes or validate the configuration or add a description to the commit.

● 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

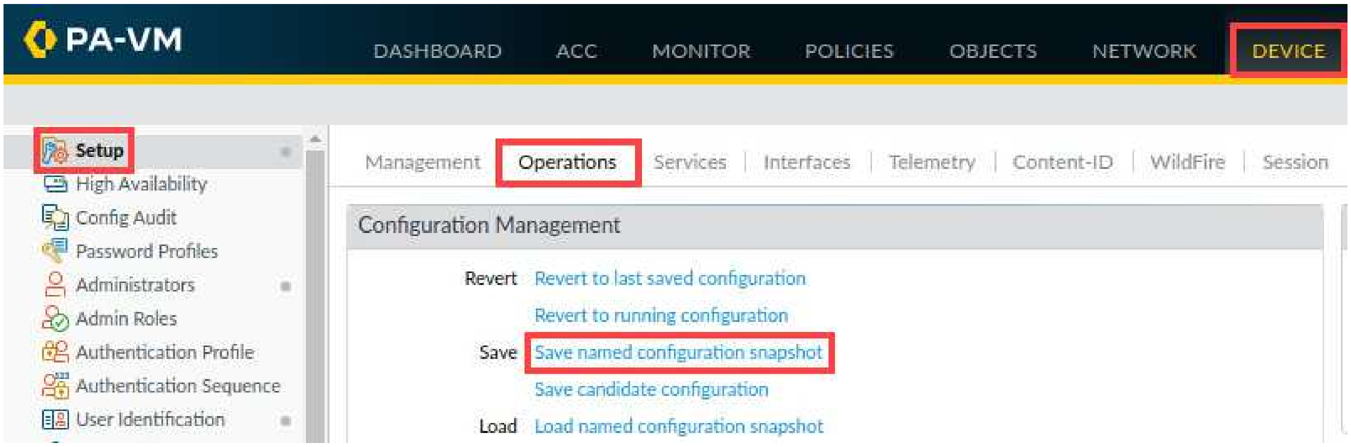
The commit process takes changes made to the Firewall and copies them to the running configuration, which will activate all configuration changes since the last commit.

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

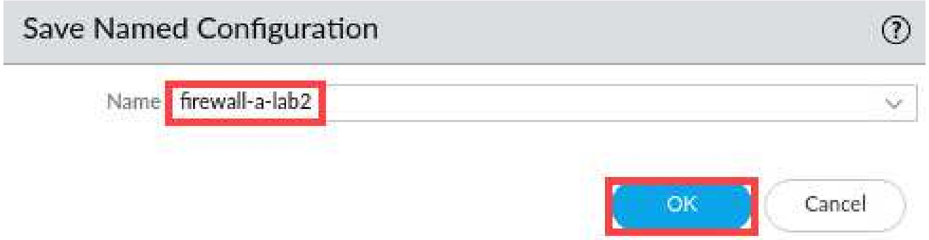
2.2 Save a Named Configuration Snapshot

In this section, you will save the firewall configuration with a specific filename.

1. In the web interface, select **Device > Setup > Operations**. Click **Save named configuration snapshot**.

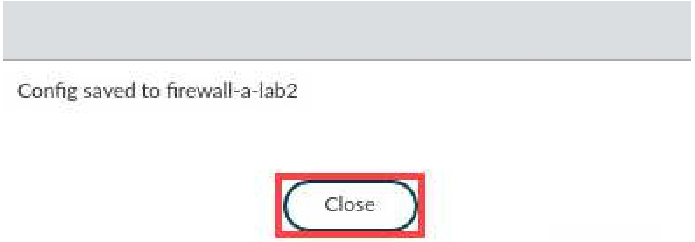


2. In the *Save Named Configuration* window, enter **`firewall-a-lab2`**. Click **OK**.



Name: firewall-a-lab2

3. In the *Confirmation* window, click **Close**.



Config saved to firewall-a-lab2

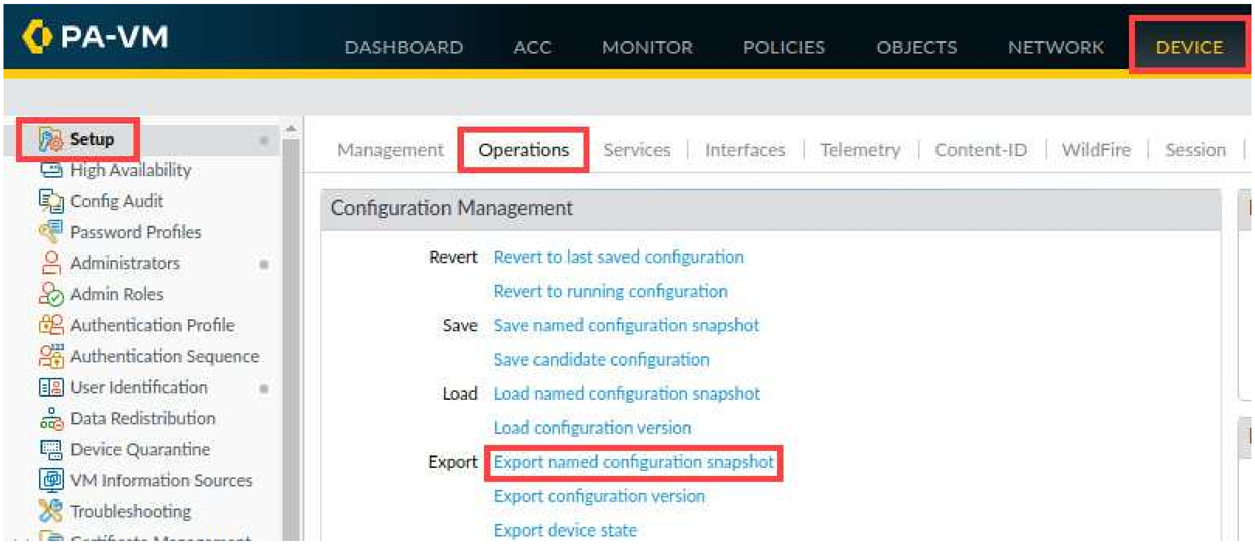
> Note that this process saved the configuration file to a location on the firewall itself.

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

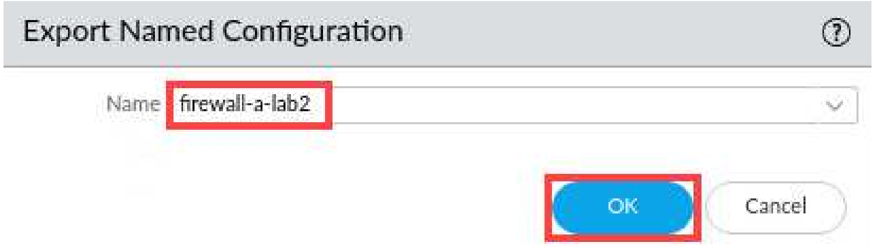
2.3 Export a Named Configuration Snapshot

In this section, you will export the saved configuration file firewall-a-lab2 from the firewall to your workstation.

1. Under **Device > Setup > Operations > Configuration Management,** click the link for **Export named configuration snapshot**.

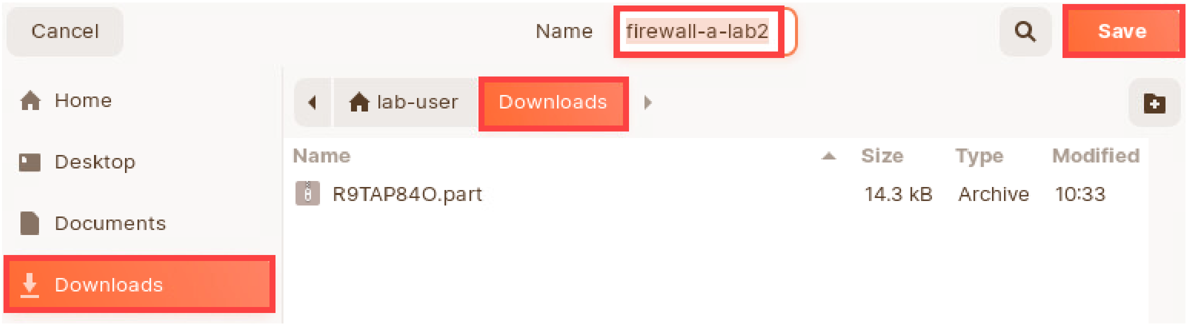


2. In the *Export Named Configuration* window, use the drop-down list and select the **firewall-a-lab2** configuration file. Click **OK**.



Name: firewall-a-lab2

3. On the *client desktop*, in the **Downloads** folder, verify the file name **firewall-a-lab2** appears as the name. Click **Save**.



Name: firewall-a-lab2

Name	Size	Type	Modified
R9TAP84O.part	14.3 kB	Archive	10:33

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

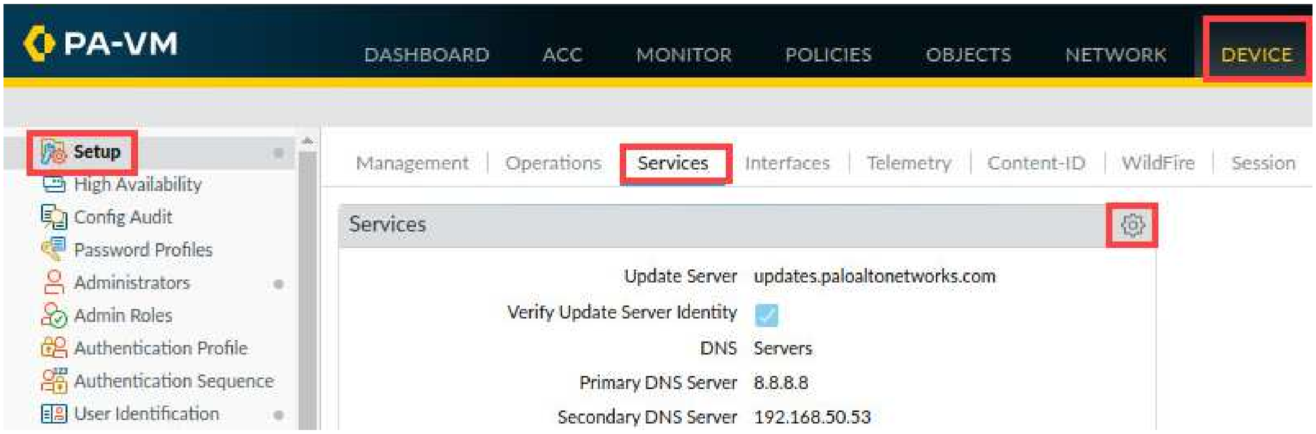
2.4 Revert Ongoing Configuration Changes

As you work on a firewall configuration, it is theoretically possible to make a mistake. In such a situation, you may not remember exactly which changes you have made or where the mistake exists in the configuration, particularly if you have made multiple changes (or multiple mistakes).

Fortunately, you can revert the firewall to the current running configuration. This process essentially erases any of the changes you have made to the working configuration and puts the firewall back at the starting point before you made changes.

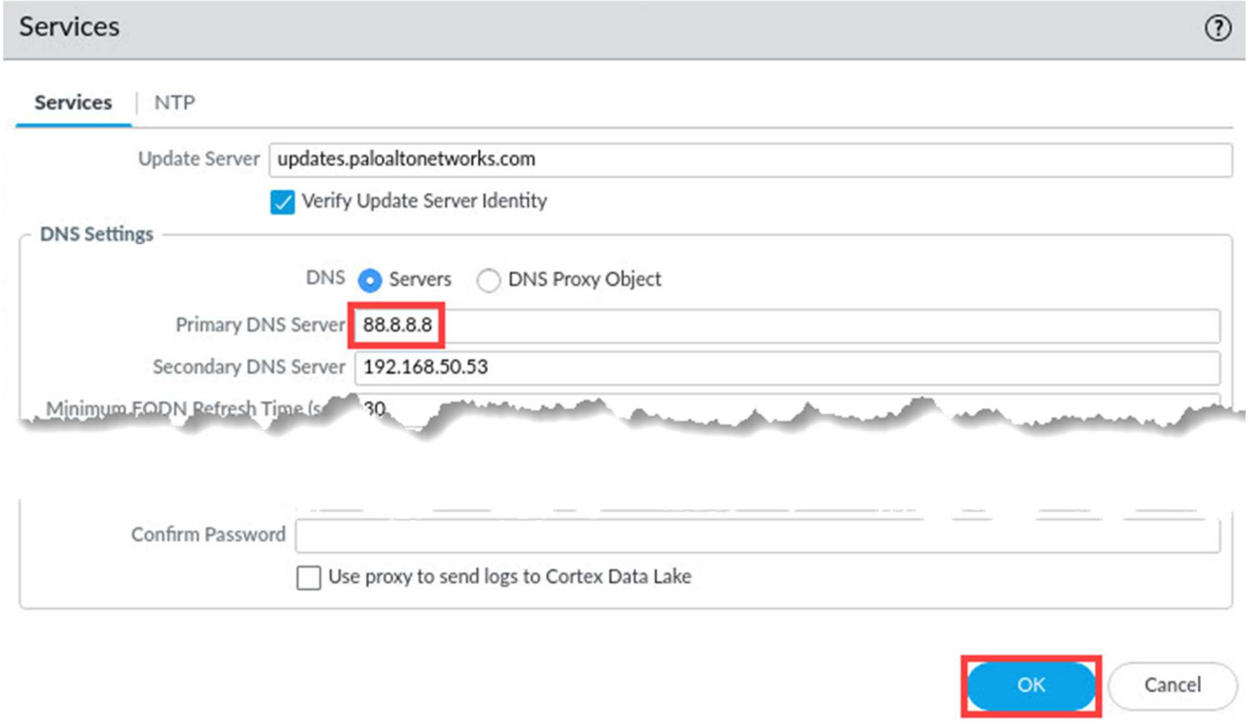
In this section, you will change the IP address for one of the firewall's DNS servers. You will then use Revert Changes to reset the firewall to the running configuration and remove the mistake.

1. In the firewall web interface, select **Device > Setup > Services**. Edit the *Services* section by clicking the **Services gear** icon.



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

2. In the *Services* window, change the value for the *Primary DNS Server* to **`88.8.8.8`** (an easy mistake to make)**.** Click **OK.**



Services

Services | NTP

Update Server: updates.paloaltonetworks.com

☑ Verify Update Server Identity

DNS Settings

DNS ● Servers ○ DNS Proxy Object

Primary DNS Server: 88.8.8.8

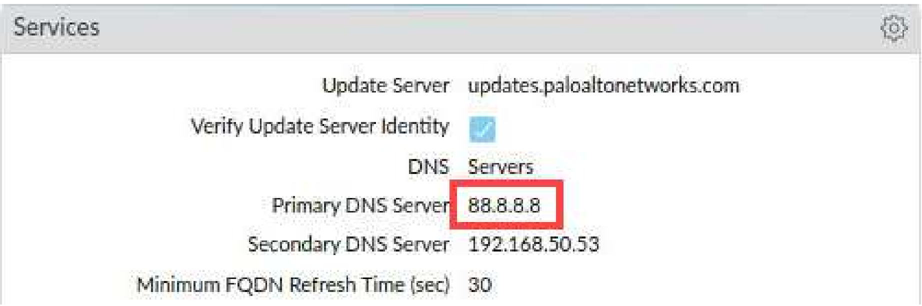
Secondary DNS Server: 192.168.50.53

Minimum FQDN Refresh Time (s… 30

Confirm Password

□ Use proxy to send logs to Cortex Data Lake

3. Verify the mistake is showing in the *Services* window for the **Primary DNS Server**.



Services

Update Server: updates.paloaltonetworks.com

Verify Update Server Identity: ☑

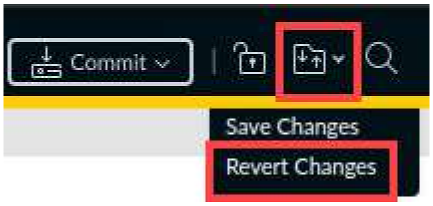
DNS: Servers

Primary DNS Server: 88.8.8.8

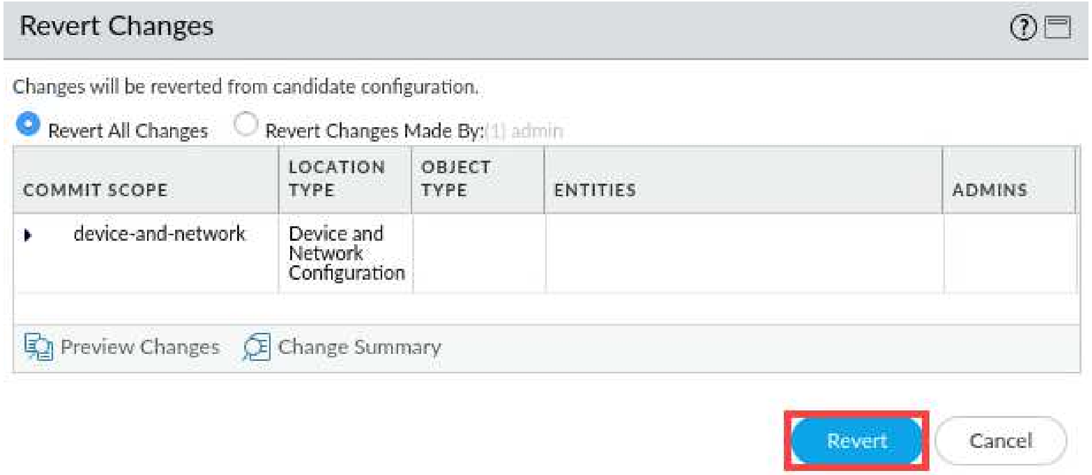
Secondary DNS Server: 192.168.50.53

Minimum FQDN Refresh Time (sec): 30

4. In the upper right corner of the *PA-VM* web interface, click the **Changes** button and select **Revert Changes.**



5. In the *Revert Changes* window, leave the settings unchanged. Click **Revert**.



Revert Changes

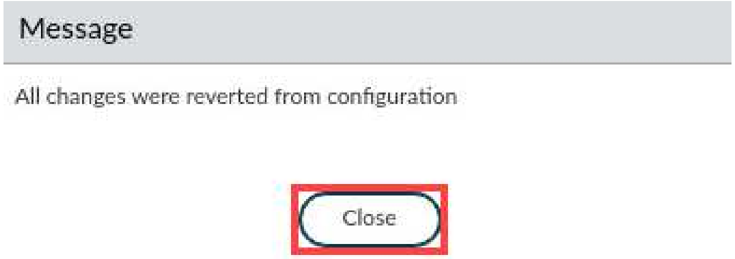
Changes will be reverted from candidate configuration.

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

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

The Revert Changes window allows you to select specific elements of the configuration that you can revert. In this case, because you only made a single change, the Revert Scope shows device-and-network (which is the portion of the configuration that contains the changes to the DNS server).

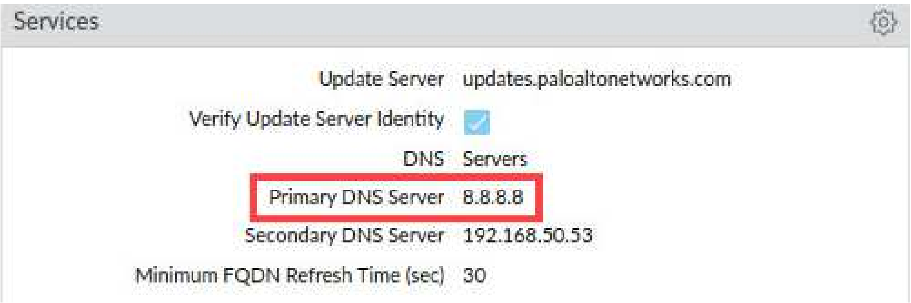
6. In the *Message* window, click **Close**.



Message

All changes were reverted from configuration

7. In the *Services* window, notice that the **Primary DNS Server** has been reset to the original value before you mistakenly changed it.



Services

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

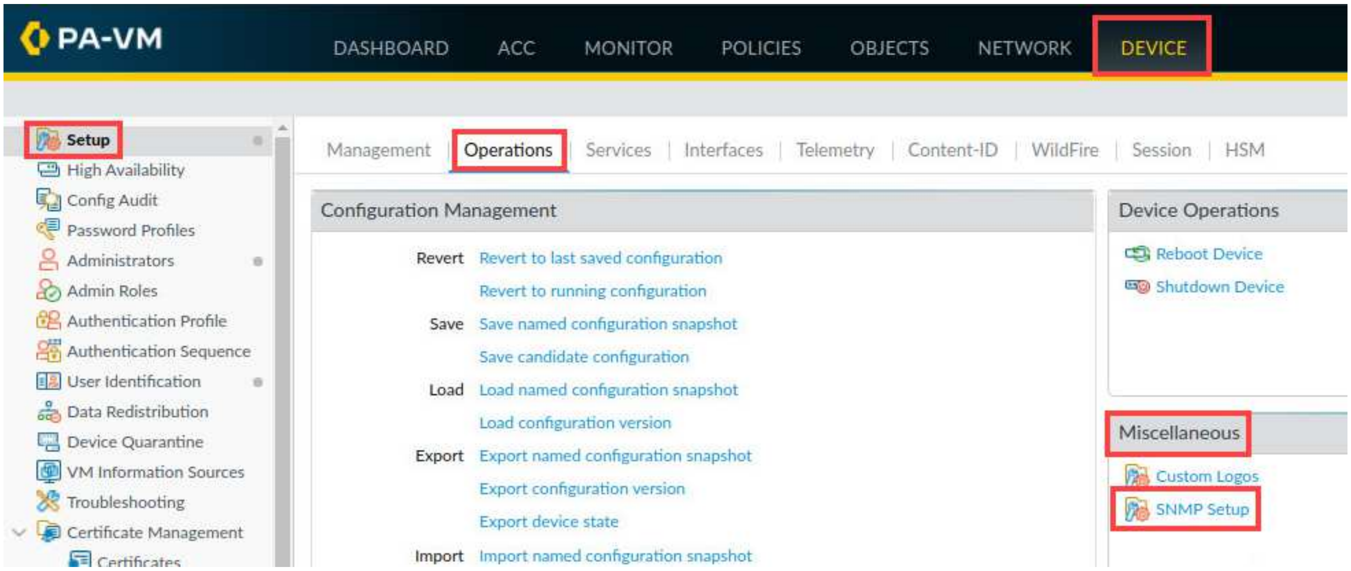
8. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

2.5 Preview Configuration Changes

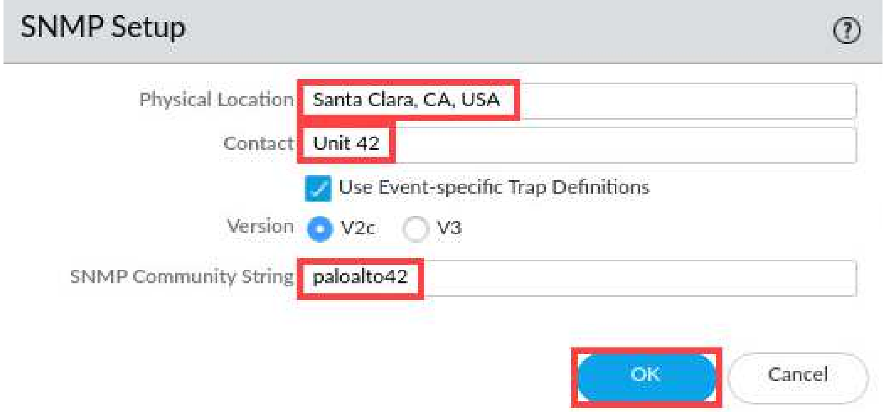
Before you commit changes to the firewall, you can compare the impending changes with the current configuration settings. This process can be useful to make certain you have the right changes in place before they are implemented on the firewall.

In this section, you will make a minor modification to the firewall and use **Preview Changes** to compare the candidate config to the running config.

1. Modify the SNMP configuration by going to **Device > Setup > Operations** and clicking **SNMP Setup** under the *Miscellaneous* section.



2. In the *SNMP Setup* window, change the *Physical Location* to `Santa Clara, CA, USA` for *Contact*, enter `Unit 42,` for *SNMP Community String*, enter `paloalto42.` Click **OK.**



SNMP Setup

Physical Location: Santa Clara, CA, USA

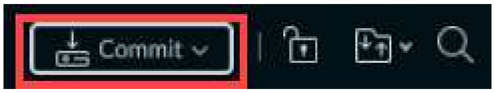
Contact: Unit 42

☑ Use Event-specific Trap Definitions

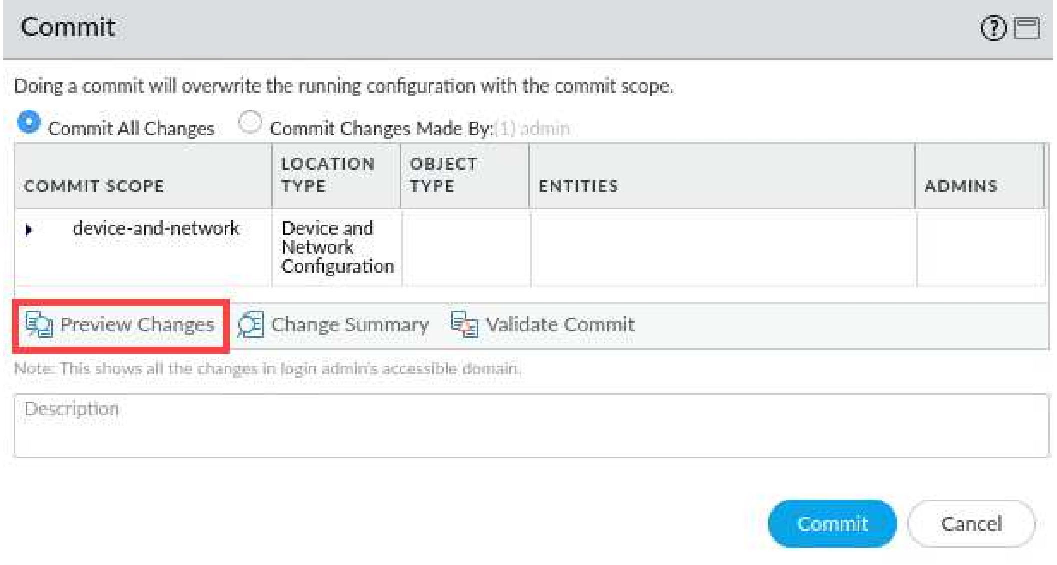
Version: ● V2c ○ V3

SNMP Community String: paloalto42

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



4. In the *Commit* window, click **Preview Changes**.



Commit

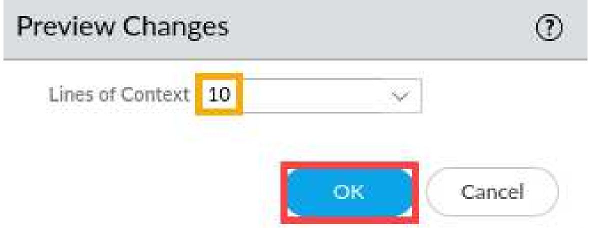
Doing a commit will overwrite the running configuration with the commit scope.

● 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.

5. In the *Preview Changes* window, leave the *Lines of Context* set to **10**. Click **OK**.

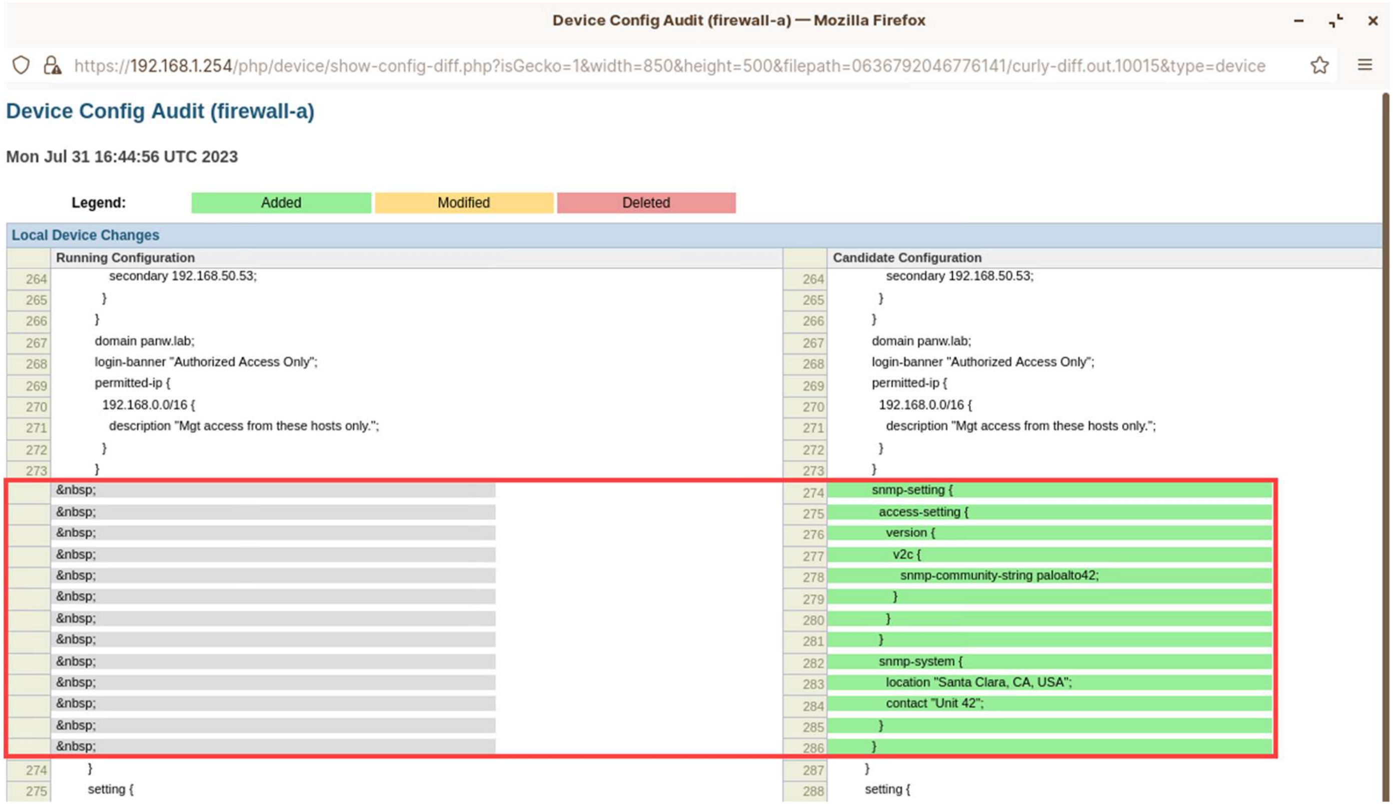


Preview Changes

Lines of Context 10

The Lines of Context setting determines how many lines are displayed before a change and after a change in the configuration file.

6. A new browser window named *Device Config Audit* will appear that displays a side-by-side comparison of the current *running configuration* (on the left) and the proposed changes in the *candidate configuration* (on the right). Review the SNMP settings that were changed.



Device Config Audit (firewall-a) — Mozilla Firefox
https://192.168.1.254/php/device/show-config-diff.php?isGecko=1&width=850&height=500&filepath=0636792046776141/curly-diff.out.10015&type=device

Device Config Audit (firewall-a)

Mon Jul 31 16:44:56 UTC 2023

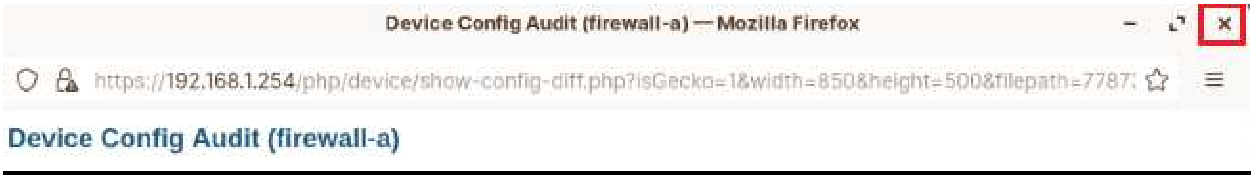
Legend: Added | Modified | Deleted

Local Device Changes

	Running Configuration		Candidate Configuration
264	secondary 192.168.50.53;	264	secondary 192.168.50.53;
265	}	265	}
266	}	266	}
267	domain panw.lab;	267	domain panw.lab;
268	login-banner "Authorized Access Only";	268	login-banner "Authorized Access Only";
269	permitted-ip {	269	permitted-ip {
270	192.168.0.0/16 {	270	192.168.0.0/16 {
271	description "Mgt access from these hosts only.";	271	description "Mgt access from these hosts only.";
272	}	272	}
273	}	273	}
		274	snmp-setting {
		275	access-setting {
		276	version {
		277	v2c {
		278	snmp-community-string paloalto42;
		279	}
		280	}
		281	}
		282	snmp-system {
		283	location "Santa Clara, CA, USA";
		284	contact "Unit 42";
		285	}
		286	}
274	}	287	}
275	setting {	288	setting {

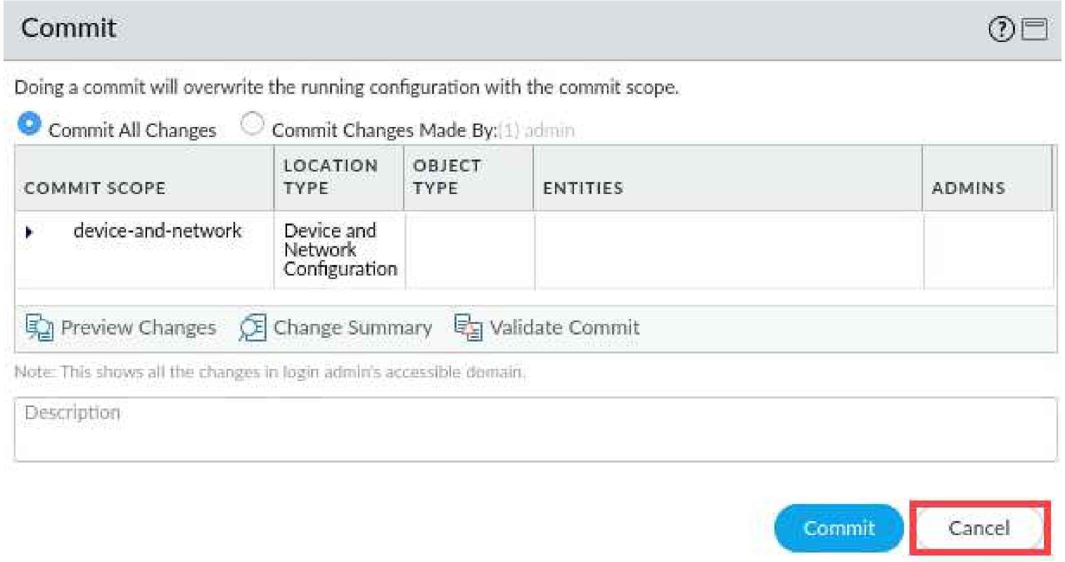
Changes are color coded. Green indicates new elements that have been added. Yellow indicates existing elements that have been modified. Red indicates existing elements that have been deleted.

7. Close the *Device Config Audit* window by clicking the **X** in the upper right corner.



Device Config Audit (firewall-a) — Mozilla Firefox
https://192.168.1.254/php/device/show-config-diff.php?isGecko=1&width=850&height=500&filepath=7787:
Device Config Audit (firewall-a)

8. Click **Cancel** in the *Commit* window.



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.

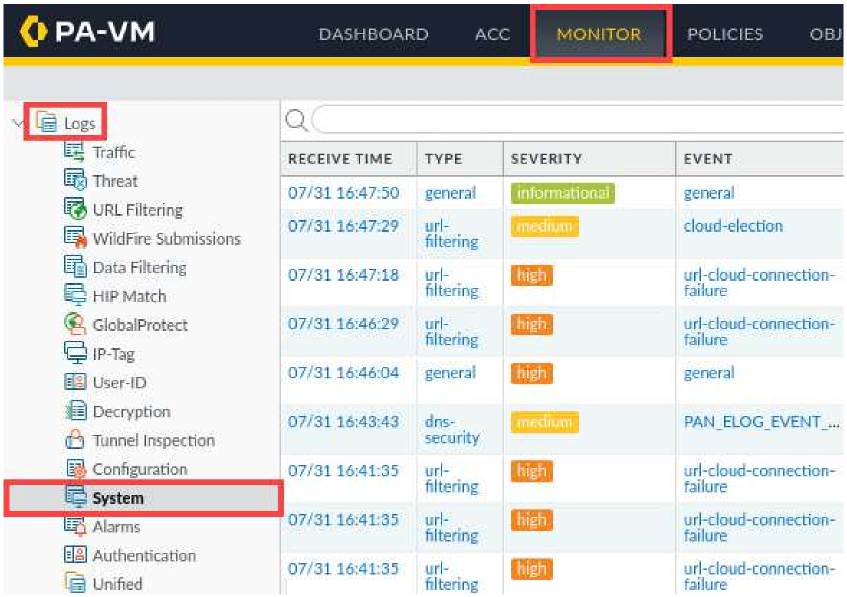
9. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

2.6 Examine Log Files

Although the information in log files varies, the process of examining and searching log files on the firewall is the same.

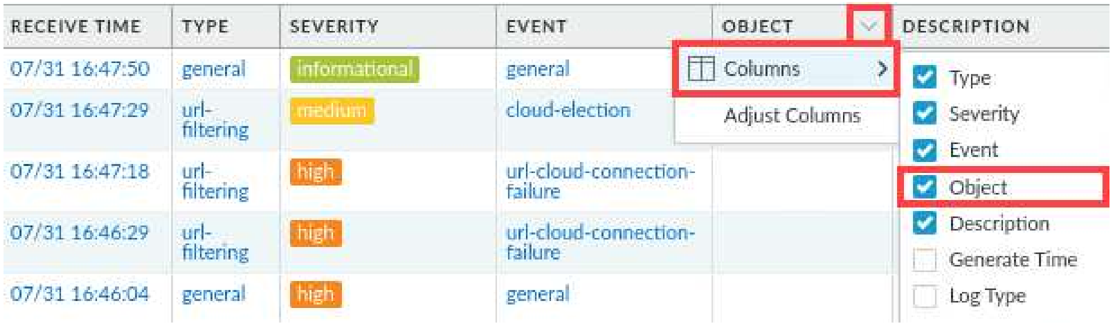
In this section, you will examine and navigate the firewall **System** log. You can later apply the same tasks and techniques while examining any other log file on the firewall, such as the Traffic or Threat logs.

1. In the PA-VM firewall interface, select **Monitor > Logs > System**.



RECEIVE TIME	TYPE	SEVERITY	EVENT
07/31 16:47:50	general	informational	general
07/31 16:47:29	url-filtering	medium	cloud-election
07/31 16:47:18	url-filtering	high	url-cloud-connection-failure
07/31 16:46:29	url-filtering	high	url-cloud-connection-failure
07/31 16:46:04	general	high	general
07/31 16:43:43	dns-security	medium	PAN_ELOG_EVENT_...
07/31 16:41:35	url-filtering	high	url-cloud-connection-failure
07/31 16:41:35	url-filtering	high	url-cloud-connection-failure
07/31 16:41:35	url-filtering	high	url-cloud-connection-failure

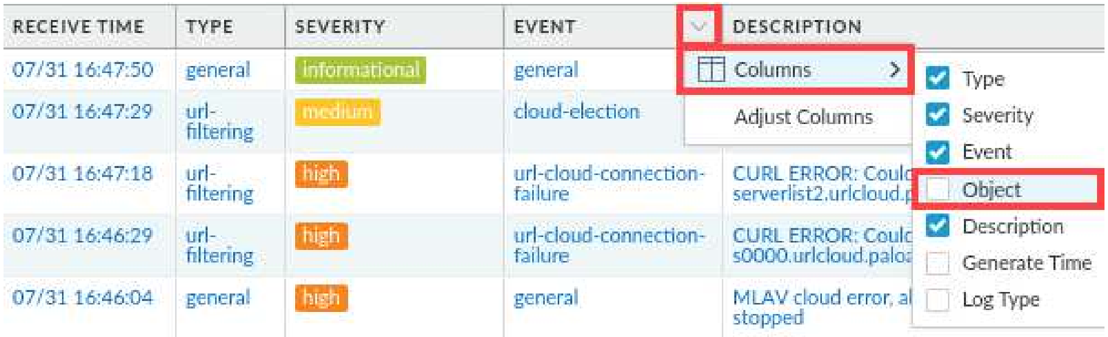
2. In the *System Logs* windows, hide the **Object** column by clicking the small **drop-down arrow** in the right portion of any column header. Notice before unchecking **Object**, it appears in the *System Logs* window.



☑ Type
☑ Severity
☑ Event
☑ Object
☑ Description
☐ Generate Time
☐ Log Type

RECEIVE TIME	TYPE	SEVERITY	EVENT	OBJECT	DESCRIPTION
07/31 16:47:50	general	informational	general		
07/31 16:47:29	url-filtering	medium	cloud-election		
07/31 16:47:18	url-filtering	high	url-cloud-connection-failure		
07/31 16:46:29	url-filtering	high	url-cloud-connection-failure		
07/31 16:46:04	general	high	general		

3. Uncheck **Object** and notice the *Object* column is now hidden.

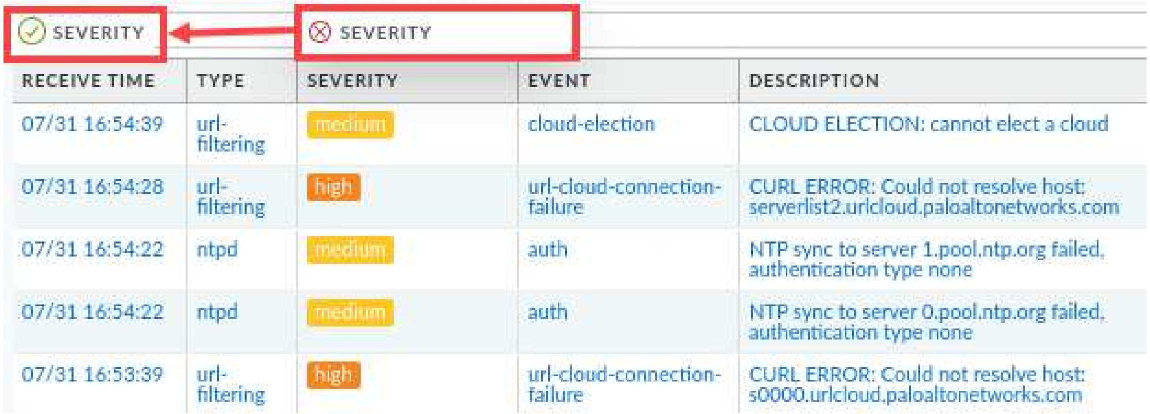


☑ Type
☑ Severity
☑ Event
☐ Object
☑ Description
☐ Generate Time
☐ Log Type

RECEIVE TIME	TYPE	SEVERITY	EVENT	DESCRIPTION
07/31 16:47:50	general	informational	general	
07/31 16:47:29	url-filtering	medium	cloud-election	
07/31 16:47:18	url-filtering	high	url-cloud-connection-failure	CURL ERROR: Coulc serverlist2.urlcloud.p
07/31 16:46:29	url-filtering	high	url-cloud-connection-failure	CURL ERROR: Coulc s0000.urlcloud.paloa
07/31 16:46:04	general	high	general	MLAV cloud error, al stopped

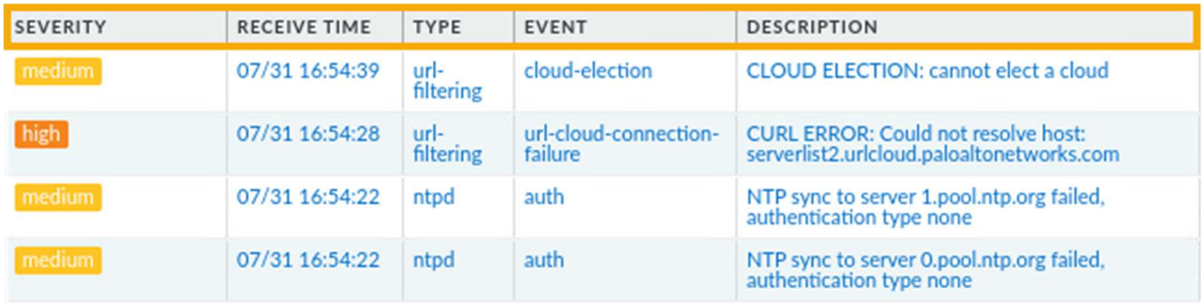
Hiding and displaying log columns is optional but quite useful. Each log file contains different columns, some of which you may not need so you can hide them. There may be columns in certain log tables that are not shown by default, and you can use this process to display hidden columns that you want to view.

4. Drag and drop the **Severity** column to the left-most position in the table by holding down the *left mouse* button.



RECEIVE TIME	TYPE	SEVERITY	EVENT	DESCRIPTION
07/31 16:54:39	url-filtering	medium	cloud-election	CLOUD ELECTION: cannot elect a cloud
07/31 16:54:28	url-filtering	high	url-cloud-connection-failure	CURL ERROR: Could not resolve host: serverlist2.urlcloud.paloaltonetworks.com
07/31 16:54:22	ntpd	medium	auth	NTP sync to server 1.pool.ntp.org failed, authentication type none
07/31 16:54:22	ntpd	medium	auth	NTP sync to server 0.pool.ntp.org failed, authentication type none
07/31 16:53:39	url-filtering	high	url-cloud-connection-failure	CURL ERROR: Could not resolve host: s0000.urlcloud.paloaltonetworks.com

5. The table now displays **Severity** as the first column.



SEVERITY	RECEIVE TIME	TYPE	EVENT	DESCRIPTION
medium	07/31 16:54:39	url-filtering	cloud-election	CLOUD ELECTION: cannot elect a cloud
high	07/31 16:54:28	url-filtering	url-cloud-connection-failure	CURL ERROR: Could not resolve host: serverlist2.urlcloud.paloaltonetworks.com
medium	07/31 16:54:22	ntpd	auth	NTP sync to server 1.pool.ntp.org failed, authentication type none
medium	07/31 16:54:22	ntpd	auth	NTP sync to server 0.pool.ntp.org failed, authentication type none

Reordering columns is also optional; however, you may discover that the information in a specific log file is easier for you to analyze after you customize the columns.

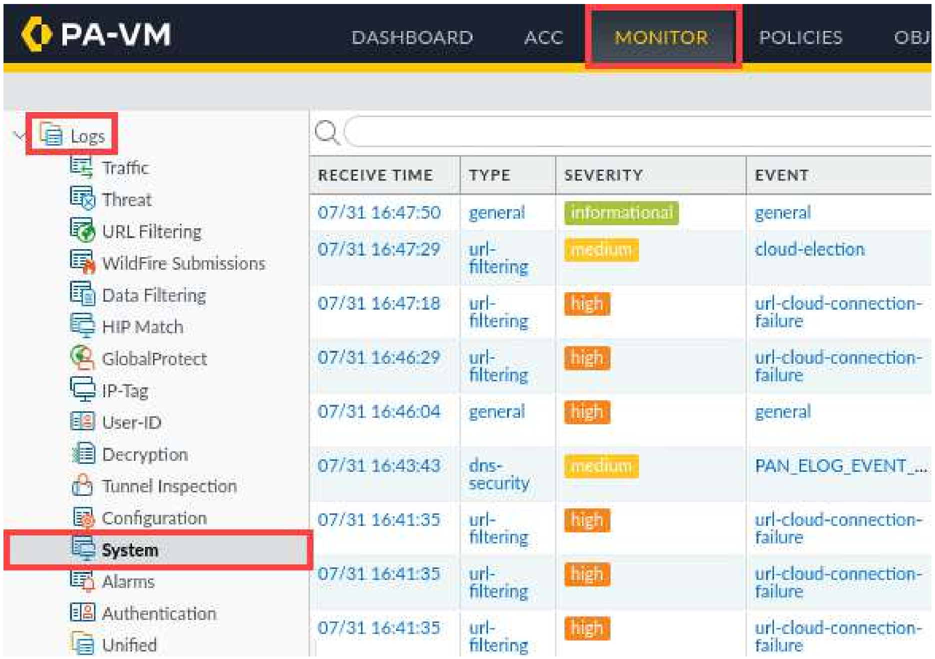
6. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

2.7 Create a Log File Filter

Scanning through log files row-by-row is tedious. If you are looking for specific information, you can create filters quickly to display only entries that match certain criteria. All log files support filters.

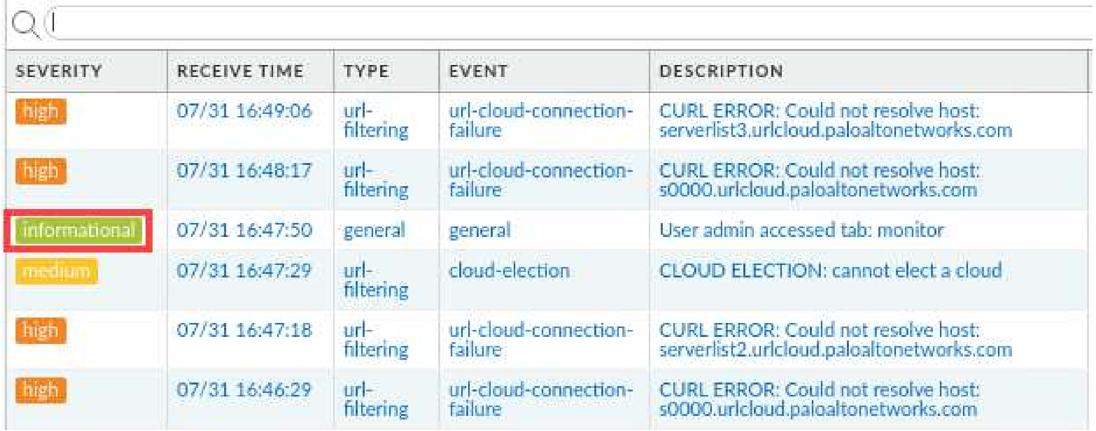
In this section, you will examine and navigate the firewall **System** log. You can later apply the same tasks and techniques while examining any other log file on the firewall, such as the Traffic or Threat logs.

1. In the PA-VM firewall interface, select **Monitor > Logs > System**.



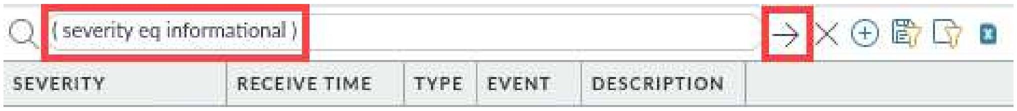
RECEIVE TIME	TYPE	SEVERITY	EVENT
07/31 16:47:50	general	informational	general
07/31 16:47:29	url-filtering	medium	cloud-election
07/31 16:47:18	url-filtering	high	url-cloud-connection-failure
07/31 16:46:29	url-filtering	high	url-cloud-connection-failure
07/31 16:46:04	general	high	general
07/31 16:43:43	dns-security	medium	PAN_ELOG_EVENT_...
07/31 16:41:35	url-filtering	high	url-cloud-connection-failure
07/31 16:41:35	url-filtering	high	url-cloud-connection-failure
07/31 16:41:35	url-filtering	high	url-cloud-connection-failure

2. In the *System log* file, click any entry under the **Severity** column that contains **informational**. Click **informational**.



SEVERITY	RECEIVE TIME	TYPE	EVENT	DESCRIPTION
high	07/31 16:49:06	url-filtering	url-cloud-connection-failure	CURL ERROR: Could not resolve host: serverlist3.urlcloud.paloaltonetworks.com
high	07/31 16:48:17	url-filtering	url-cloud-connection-failure	CURL ERROR: Could not resolve host: s0000.urlcloud.paloaltonetworks.com
informational	07/31 16:47:50	general	general	User admin accessed tab: monitor
medium	07/31 16:47:29	url-filtering	cloud-election	CLOUD ELECTION: cannot elect a cloud
high	07/31 16:47:18	url-filtering	url-cloud-connection-failure	CURL ERROR: Could not resolve host: serverlist2.urlcloud.paloaltonetworks.com
high	07/31 16:46:29	url-filtering	url-cloud-connection-failure	CURL ERROR: Could not resolve host: s0000.urlcloud.paloaltonetworks.com

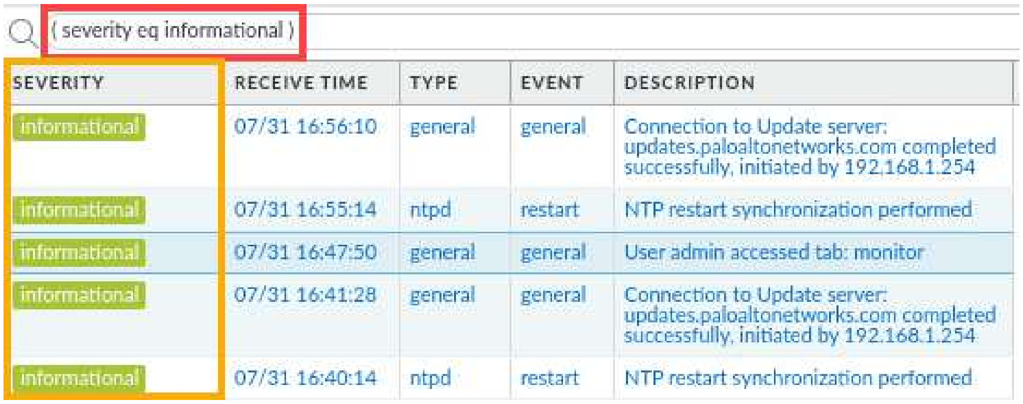
3. The web interface will automatically build a filter statement with the appropriate syntax to search for all entries that contain **informational** in the **Severity** field. Click the **Apply Filter** button in the upper right of the window.



(severity eq informational)

SEVERITY	RECEIVE TIME	TYPE	EVENT	DESCRIPTION

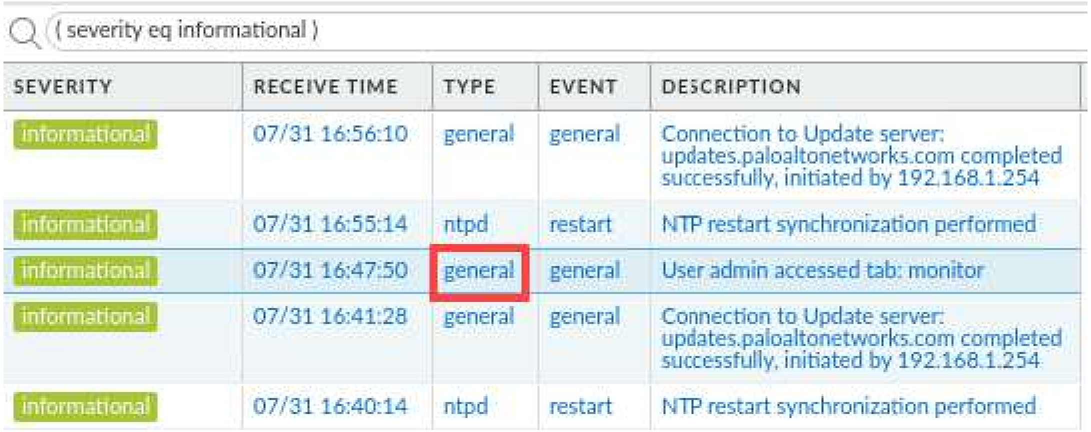
4. The System log display will update to show only those entries that contain **informational** as the **Severity** level.



(severity eq informational)

SEVERITY	RECEIVE TIME	TYPE	EVENT	DESCRIPTION
informational	07/31 16:56:10	general	general	Connection to Update server: updates.paloaltonetworks.com completed successfully, initiated by 192.168.1.254
informational	07/31 16:55:14	ntpd	restart	NTP restart synchronization performed
informational	07/31 16:47:50	general	general	User admin accessed tab: monitor
informational	07/31 16:41:28	general	general	Connection to Update server: updates.paloaltonetworks.com completed successfully, initiated by 192.168.1.254
informational	07/31 16:40:14	ntpd	restart	NTP restart synchronization performed

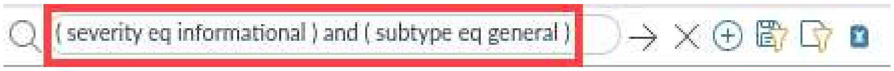
5. Under the **Type** column, click any entry that contains the word **general**. Click **general**.



(severity eq informational)

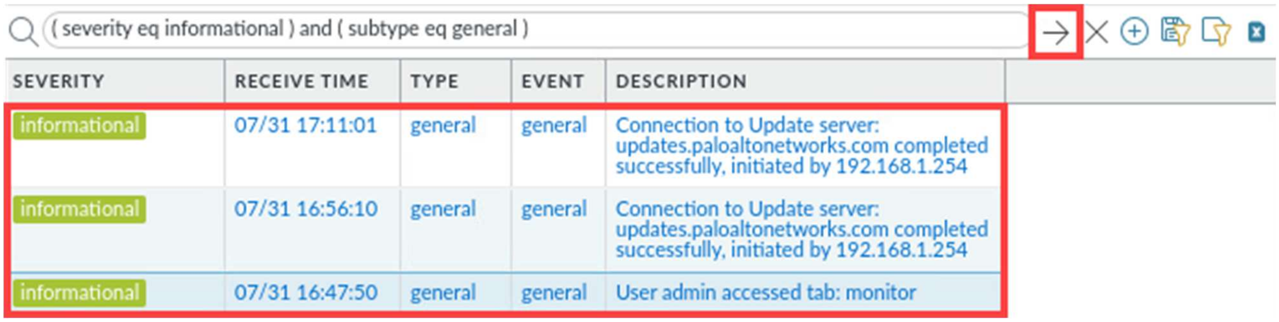
SEVERITY	RECEIVE TIME	TYPE	EVENT	DESCRIPTION
informational	07/31 16:56:10	general	general	Connection to Update server: updates.paloaltonetworks.com completed successfully, initiated by 192.168.1.254
informational	07/31 16:55:14	ntpd	restart	NTP restart synchronization performed
informational	07/31 16:47:50	general	general	User admin accessed tab: monitor
informational	07/31 16:41:28	general	general	Connection to Update server: updates.paloaltonetworks.com completed successfully, initiated by 192.168.1.254
informational	07/31 16:40:14	ntpd	restart	NTP restart synchronization performed

6. Notice the interface will update the syntax to create a combined filter.



(severity eq informational) and (subtype eq general)

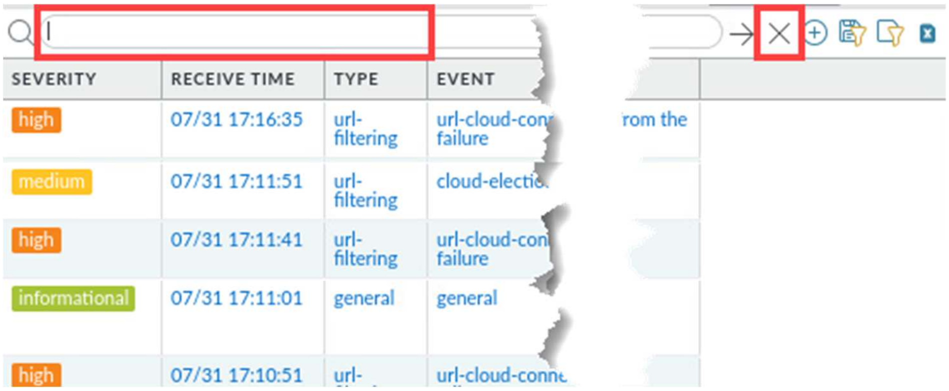
7. Click the **Apply Filter** button. The interface will update the log file to display only those entries that match both conditions.



(severity eq informational) and (subtype eq general)

SEVERITY	RECEIVE TIME	TYPE	EVENT	DESCRIPTION
informational	07/31 17:11:01	general	general	Connection to Update server: updates.paloaltonetworks.com completed successfully, initiated by 192.168.1.254
informational	07/31 16:56:10	general	general	Connection to Update server: updates.paloaltonetworks.com completed successfully, initiated by 192.168.1.254
informational	07/31 16:47:50	general	general	User admin accessed tab: monitor

8. Remove the filter by clicking the **Clear Filter** button in the upper right corner of the window.



SEVERITY	RECEIVE TIME	TYPE	EVENT	
high	07/31 17:16:35	url-filtering	url-cloud-conr failure	rom the
medium	07/31 17:11:51	url-filtering	cloud-electio	
high	07/31 17:11:41	url-filtering	url-cloud-con failure	
informational	07/31 17:11:01	general	general	
high	07/31 17:10:51	url-	url-cloud-conne	

A good practice is to clear any filters from log file displays before you move to other portions of the web interface. The next time you examine the same log, it will display all results instead of only ones you have previously filtered.

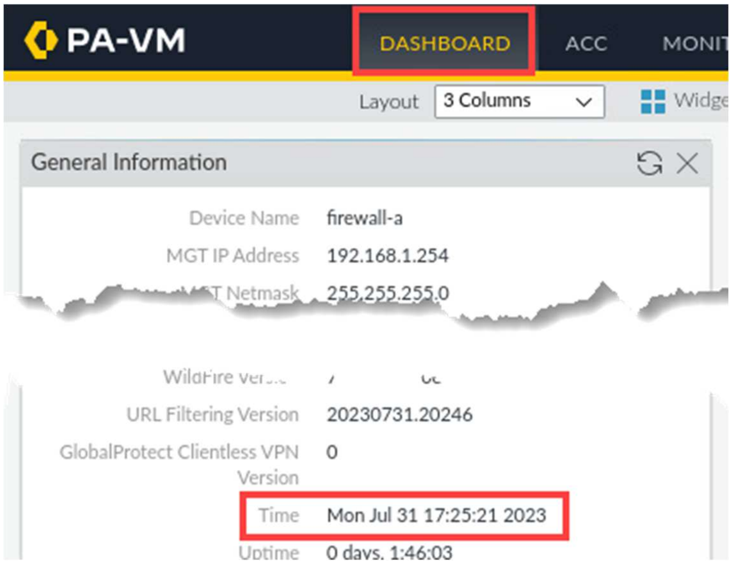
9. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

2.8 Use the Filter Builder

Clicking the link for a specific entry in a log file will automatically create a simple filter. You can create more complex filters by clicking multiple conditions; however, there are some situations in which this process will not provide you with the kind of criteria you need to complete a search. For long or sophisticated searches, you can use the Filter Builder.

In this section, you will use the Filter Builder to search the **System** log for all entries that have occurred in the last 60 minutes.

1. In the PA-VM web interface, select the **Dashboard** tab. Under the *General Information* section, scroll to the bottom and locate the **Time.** Write the current date and time down so you do not forget it.

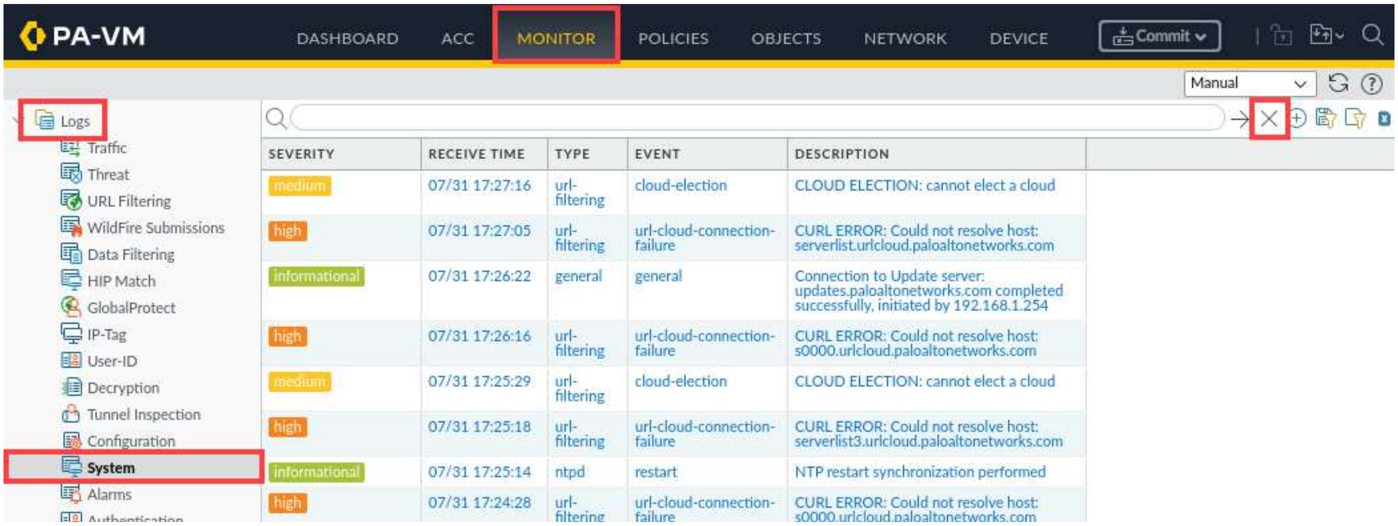


Device Name	firewall-a
MGT IP Address	192.168.1.254
MGT Netmask	255.255.255.0
URL Filtering Version	20230731.20246
GlobalProtect Clientless VPN Version	0
Time	Mon Jul 31 17:25:21 2023
Uptime	0 days, 1:46:03

Please Note

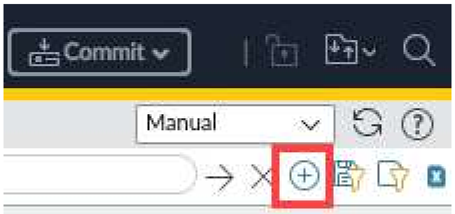
For this lab, notice the time of 17:25:21. The times you see will vary.

2. Select **Monitor > Logs > System.** Verify you do not have any filters present. If you have a filter present, click the **Clear Filter** button in the upper right corner of the *System Logs* window.



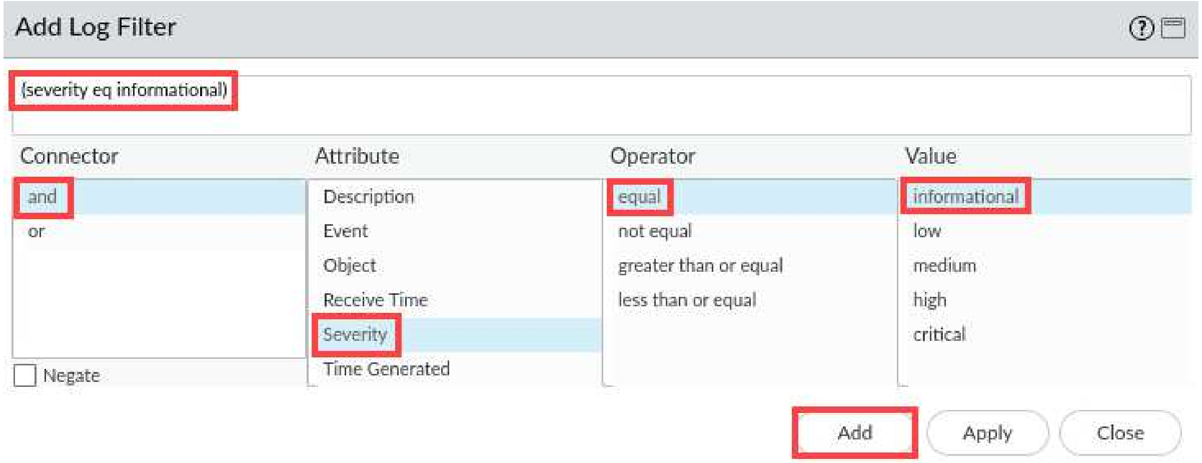
SEVERITY	RECEIVE TIME	TYPE	EVENT	DESCRIPTION
medium	07/31 17:27:16	url-filtering	cloud-election	CLOUD ELECTION: cannot elect a cloud
high	07/31 17:27:05	url-filtering	url-cloud-connection-failure	CURL ERROR: Could not resolve host: serverlist.urlcloud.paloaltonetworks.com
informational	07/31 17:26:22	general	general	Connection to Update server: updates.paloaltonetworks.com completed successfully, initiated by 192.168.1.254
high	07/31 17:26:16	url-filtering	url-cloud-connection-failure	CURL ERROR: Could not resolve host: s0000.urlcloud.paloaltonetworks.com
medium	07/31 17:25:29	url-filtering	cloud-election	CLOUD ELECTION: cannot elect a cloud
high	07/31 17:25:18	url-filtering	url-cloud-connection-failure	CURL ERROR: Could not resolve host: serverlist3.urlcloud.paloaltonetworks.com
informational	07/31 17:25:14	ntpd	restart	NTP restart synchronization performed
high	07/31 17:24:28	url-filtering	url-cloud-connection-failure	CURL ERROR: Could not resolve host: s0000.urlcloud.paloaltonetworks.com

3. Click the **Add Filter** button in the upper right corner of the *System Logs* window.



4. In the *Add Log Filter* window, fill in the following information below.

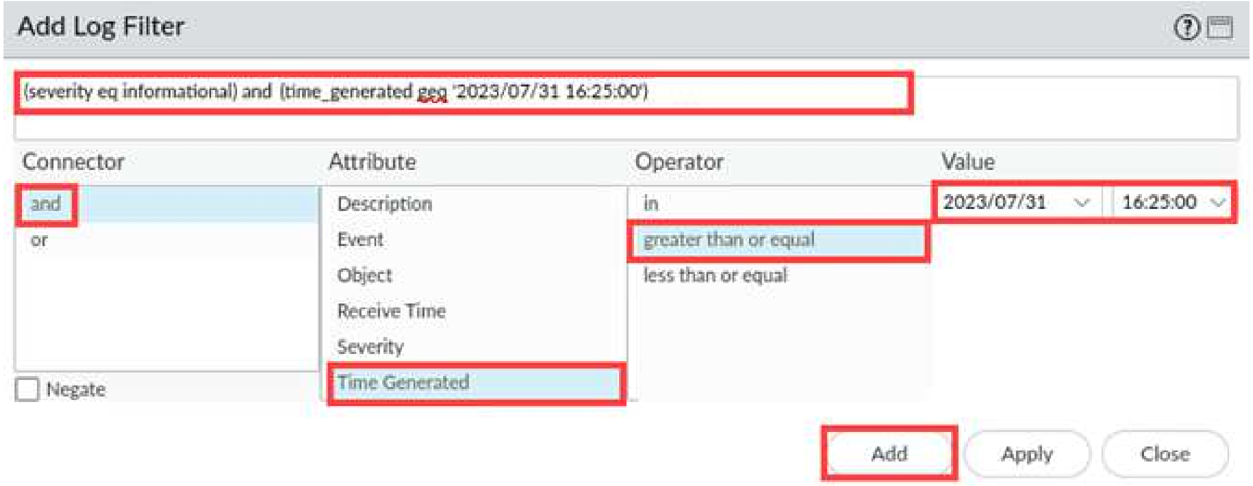
   A. Under the **Connector** column, click **and.**
   B. Under the **Attribute** column, click **Severity.**
   C. Under the **Operator** column, click **equal.**
   D. Under the **Value** column, click **informational.**
   E. Click **Add.**
   F. Note that the filter field at the top of the window updates to display the correct syntax for this filter.


Add Log Filter

(severity eq informational)

5. With the *Add Log Filter* window open, build the second part of the filter.

   A. Under the **Connector** column, select **and.**
   B. Under the **Attribute** column, select **Time Generated.**
   C. Under **Operator**, select **greater than or equal to.**
   D. Under the **Value** column, use the first drop-down list to select the date you recorded in step 1.
   E. Under the **Value** column, use the second drop-down list to select a time approximately sixty minutes prior to the time you recorded in step 1 (round up or down if you need to).
   F. Click **Add.**
   G. Note that the filter is updated to reflect the additional syntax.

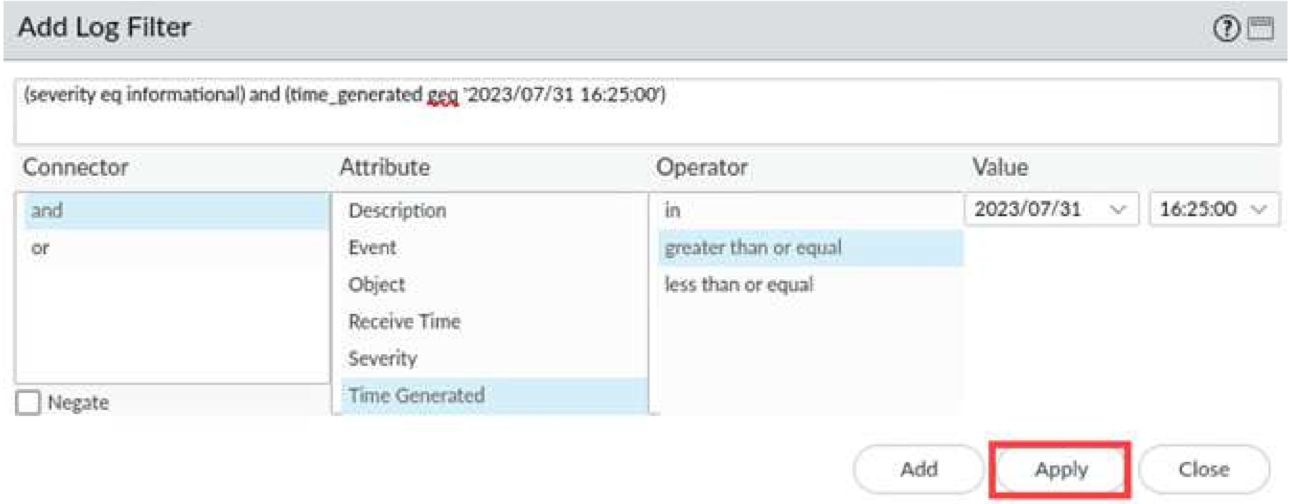


(severity eq informational) and (time_generated geq '2023/07/31 16:25:00')

Please Note

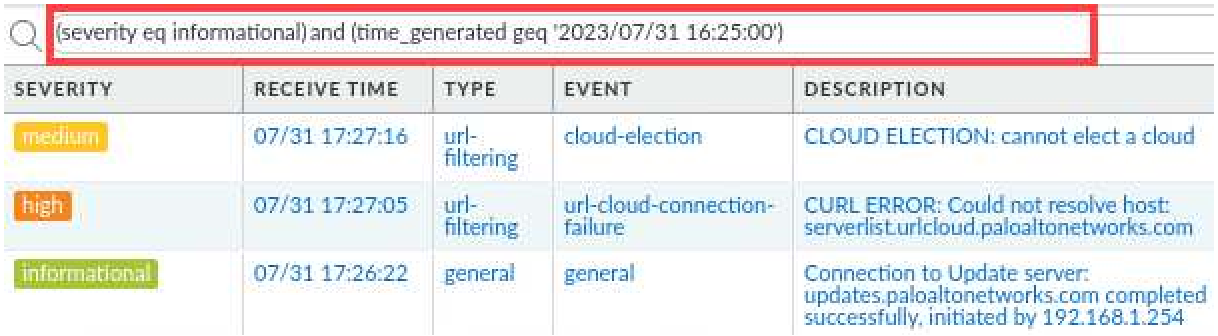
For this lab example, you notice the time that was recorded will be 17:25:21. When you round down, the value to record will be 16:25:00. The time and date for your filter will differ from the example shown here.

6. In the *Add Log Filter* window, click **Apply**.



(severity eq informational) and (time_generated geq '2023/07/31 16:25:00')

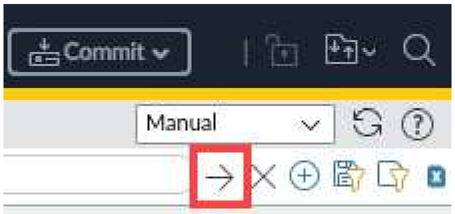
7. Your filter will appear in the System log syntax field. Remember your *time* will be different than this lab example.



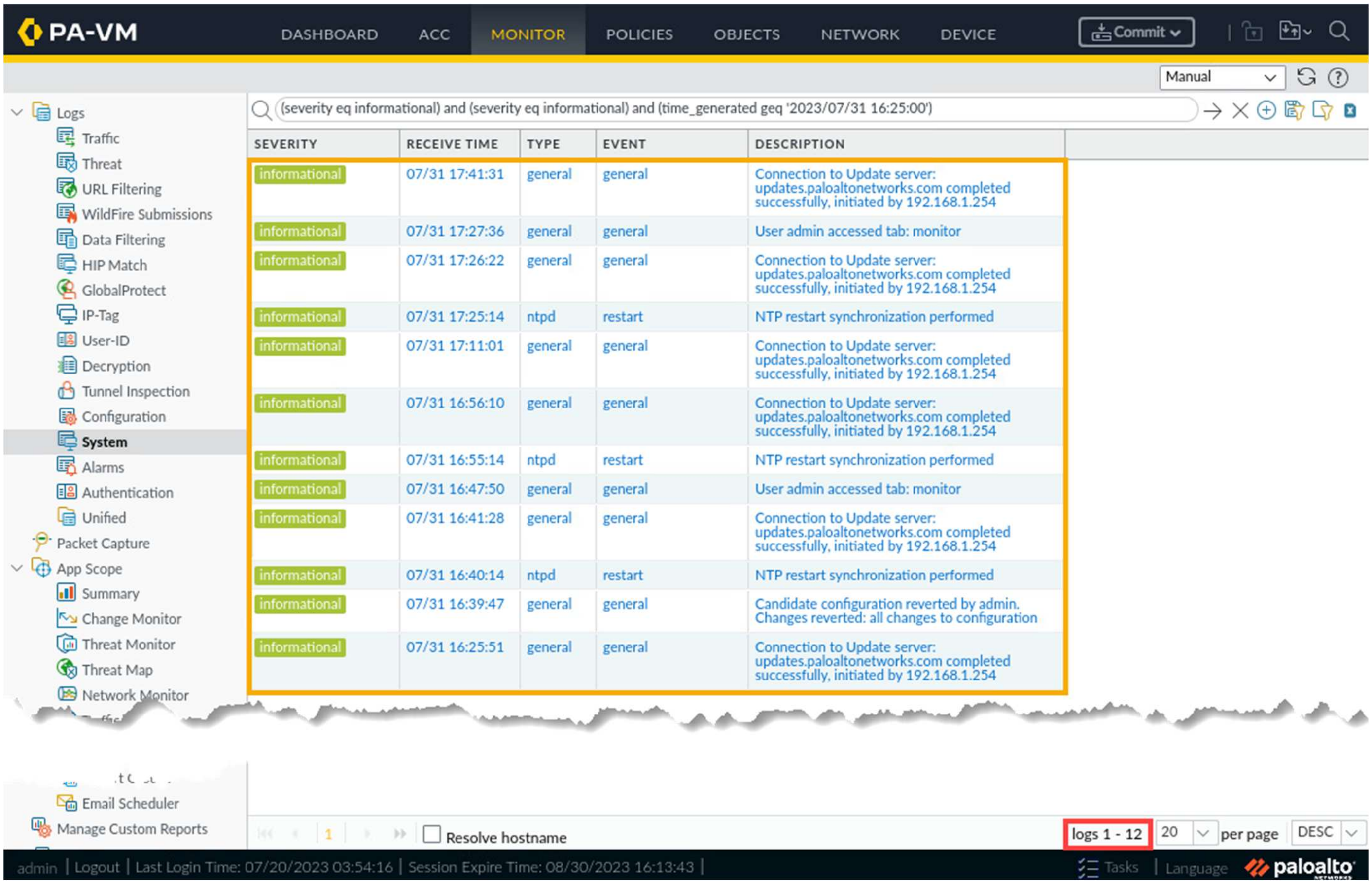
(severity eq informational) and (time_generated geq '2023/07/31 16:25:00')

SEVERITY	RECEIVE TIME	TYPE	EVENT	DESCRIPTION
medium	07/31 17:27:16	url-filtering	cloud-election	CLOUD ELECTION: cannot elect a cloud
high	07/31 17:27:05	url-filtering	url-cloud-connection-failure	CURL ERROR: Could not resolve host: serverlist.urlcloud.paloaltonetworks.com
informational	07/31 17:26:22	general	general	Connection to Update server: updates.paloaltonetworks.com completed successfully, initiated by 192.168.1.254

8. Click the **Apply Filter** button in the upper right corner of the window.



9. The *System log* display will update to show you only entries that have been generated after the time you specified for this lab. For this lab, we only had 1 page of logs to show. The bottom of page 1 shows you the first entry after the time that was specified in the filter creation.



(severity eq informational) and (severity eq informational) and (time_generated geq '2023/07/31 16:25:00')

SEVERITY	RECEIVE TIME	TYPE	EVENT	DESCRIPTION
informational	07/31 17:41:31	general	general	Connection to Update server: updates.paloaltonetworks.com completed successfully, initiated by 192.168.1.254
informational	07/31 17:27:36	general	general	User admin accessed tab: monitor
informational	07/31 17:26:22	general	general	Connection to Update server: updates.paloaltonetworks.com completed successfully, initiated by 192.168.1.254
informational	07/31 17:25:14	ntpd	restart	NTP restart synchronization performed
informational	07/31 17:11:01	general	general	Connection to Update server: updates.paloaltonetworks.com completed successfully, initiated by 192.168.1.254
informational	07/31 16:56:10	general	general	Connection to Update server: updates.paloaltonetworks.com completed successfully, initiated by 192.168.1.254
informational	07/31 16:55:14	ntpd	restart	NTP restart synchronization performed
informational	07/31 16:47:50	general	general	User admin accessed tab: monitor
informational	07/31 16:41:28	general	general	Connection to Update server: updates.paloaltonetworks.com completed successfully, initiated by 192.168.1.254
informational	07/31 16:40:14	ntpd	restart	NTP restart synchronization performed
informational	07/31 16:39:47	general	general	Candidate configuration reverted by admin. Changes reverted: all changes to configuration
informational	07/31 16:25:51	general	general	Connection to Update server: updates.paloaltonetworks.com completed successfully, initiated by 192.168.1.254

1 □ Resolve hostname logs 1 - 12 20 per page DESC

admin | Logout | Last Login Time: 07/20/2023 03:54:16 | Session Expire Time: 08/30/2023 16:13:43 | Tasks | Language

> **Please Note**
>
> Although you used the System log as the basis for this exercise, the process of creating filters is the same throughout all Palo Alto Networks firewall log files. The Filter Builder also is available to use in all log file tables.

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