PALO ALTO NETWORKS EDU 210

Lab 2: Working with Firewall Configurations and Log Files

Document Version: 2021-09-27

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.

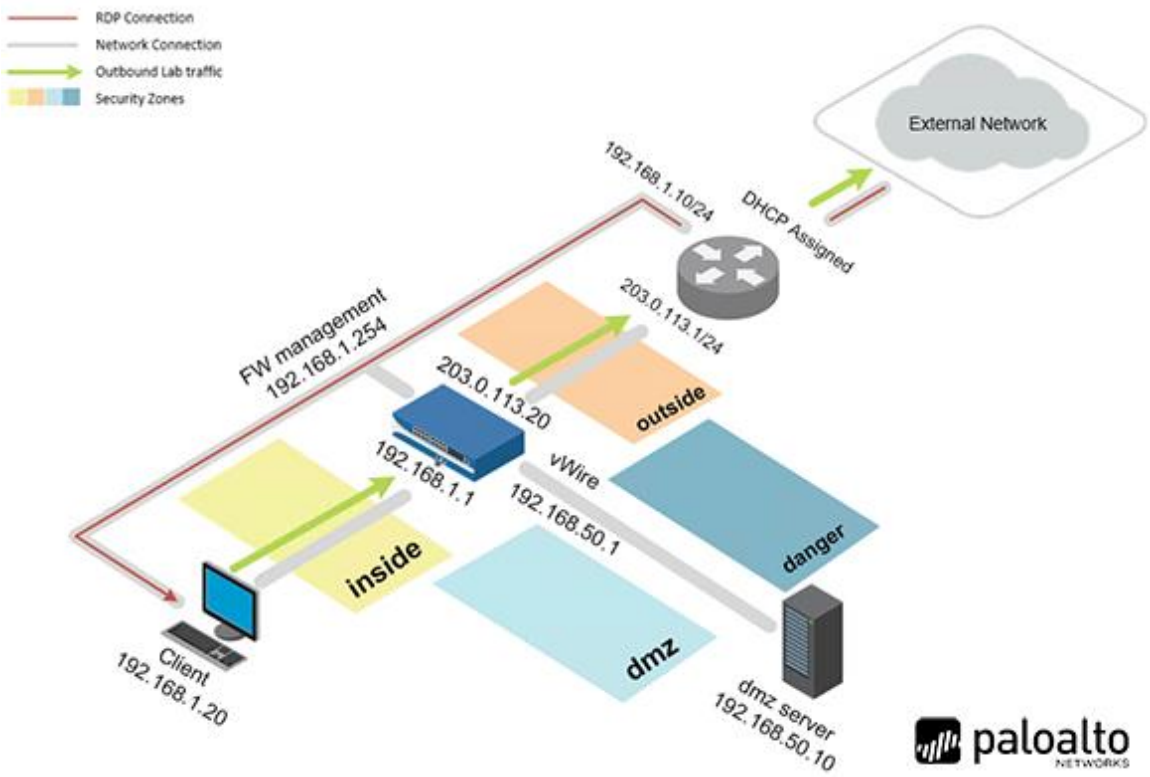
In this lab, you will work with snapshots, revert and preview configuration changes, examine log files, and create and use the filter builder.

Objective

In this lab, you will perform the following tasks:

- Load a starting lab 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 log files
- Create a log file filter
- Use the Filter Builder

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.

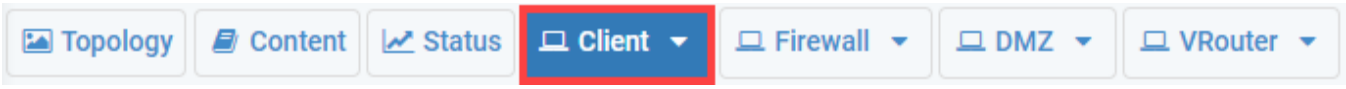
Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Client	192.168.1.20	lab-user	**Pal0Alt0!**
DMZ	192.168.50.10	root	**Pal0Alt0!**
Firewall	192.168.1.254	admin	**Pal0Alt0!**
VRouter	192.168.1.10	root	**Pal0Alt0!**

2 Working with Firewall Configurations and Log Files

2.1 Apply a Baseline Configuration to the Firewall

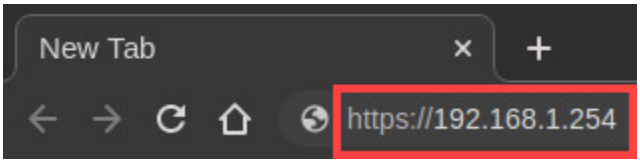
In this section, you will load the firewall configuration file.

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

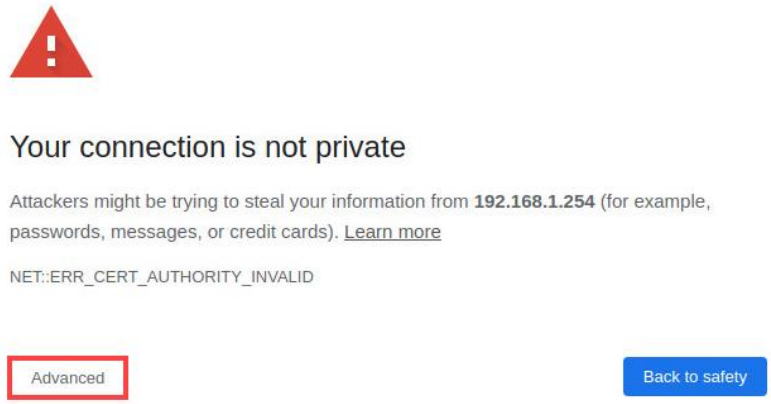


2. Double-click the **Chromium Web Browser** icon located on the *desktop*.

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

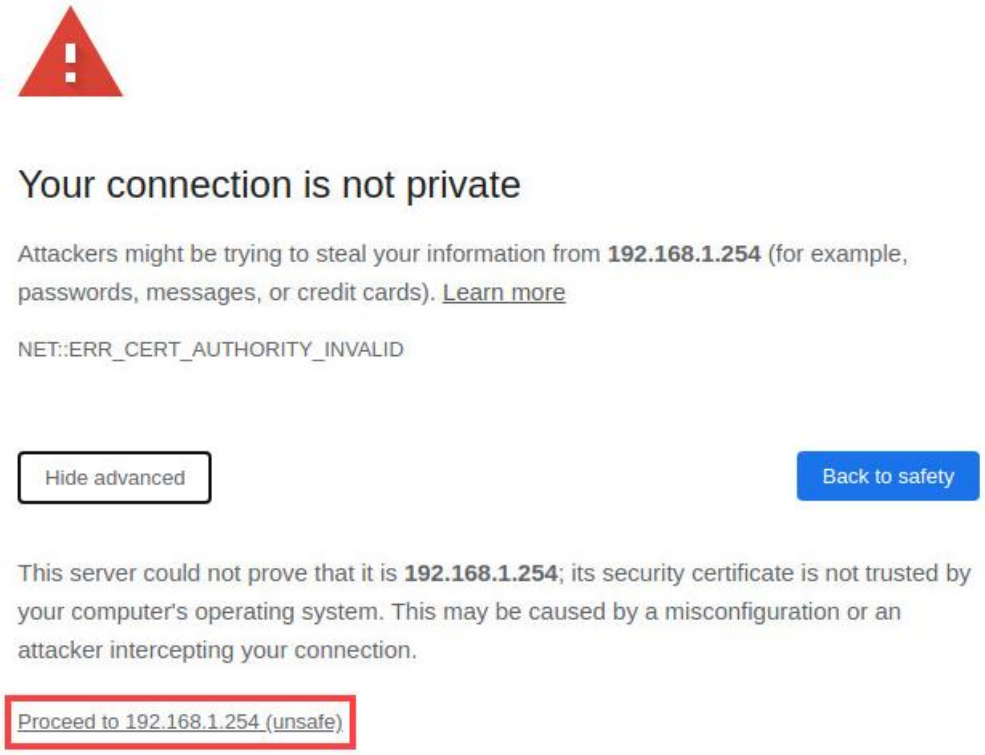


4. You will see a "*Your connection is not private*" message. Click on the **ADVANCED** link.



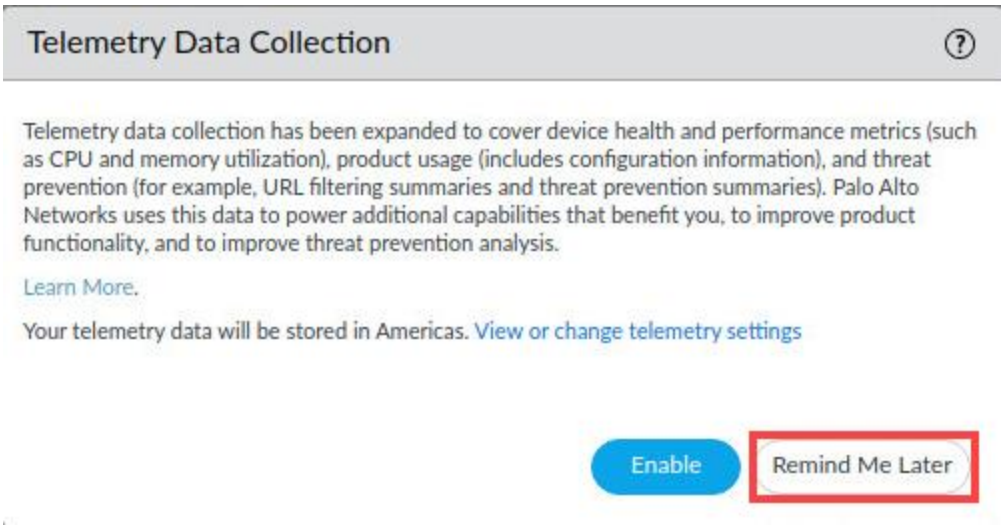
If you experience the "Unable to connect" or "502 Bad Gateway" message while attempting to connect to the specified IP above, please wait an additional 1-3 minutes for the Firewall to fully initialize. Refresh the page to continue.

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



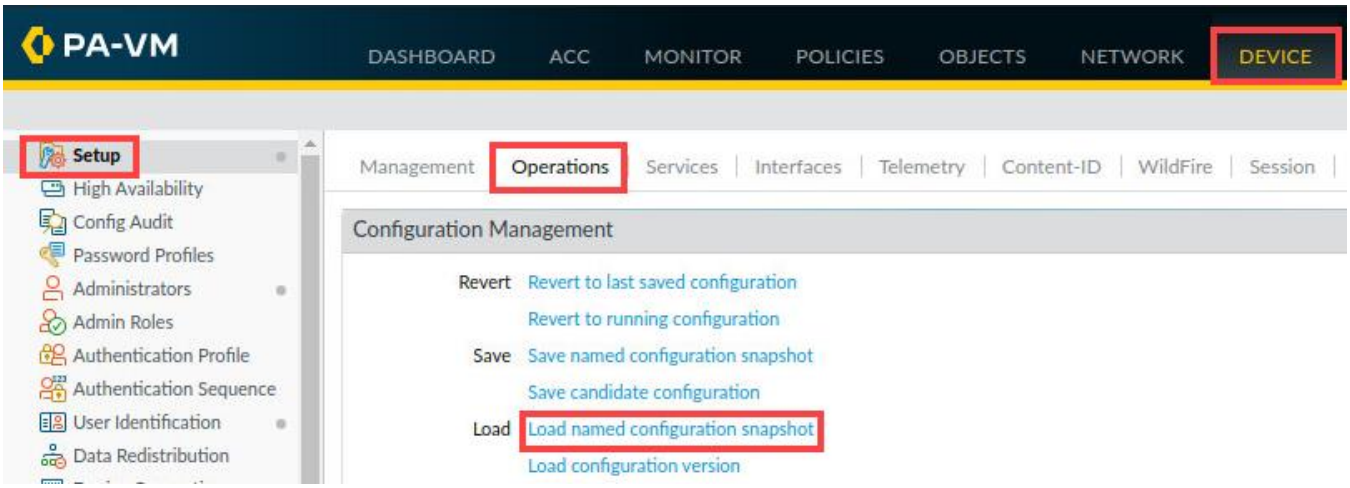
6. Log in to the firewall web interface as username **`admin`**, password **`Pal0Alt0!.`**

7. In the *Telemetry Data Collection* pop-up, click **Remind Me Later**.

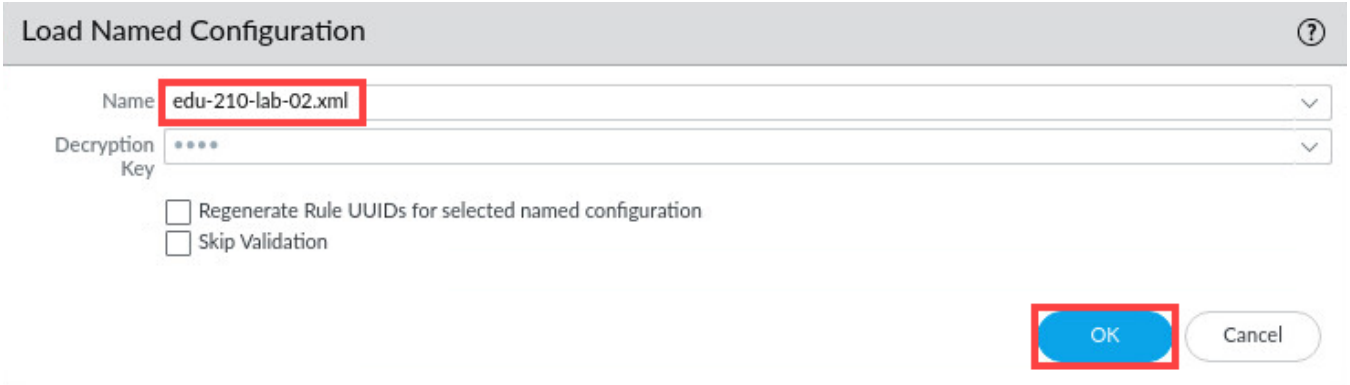


> **Please Note**
> Before you can enable Telemetry Data Collection, you would need to install a device certificate. For this lab, you will not be using Telemetry Data Collection.

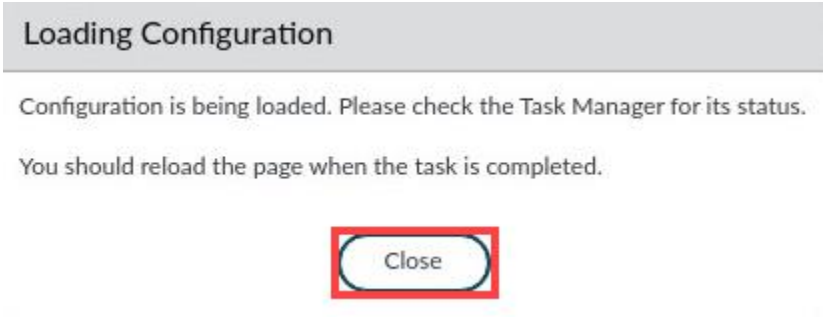
8. In the web interface, navigate to **Device > Setup > Operations** and click on **Load named configuration snapshot** underneath the *Configuration Management* section.



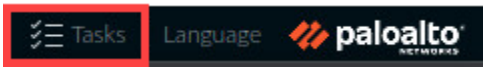
9. In the *Load Named Configuration* window, select **edu-210-lab-02.xml** from the *Name* dropdown box and click **OK**.



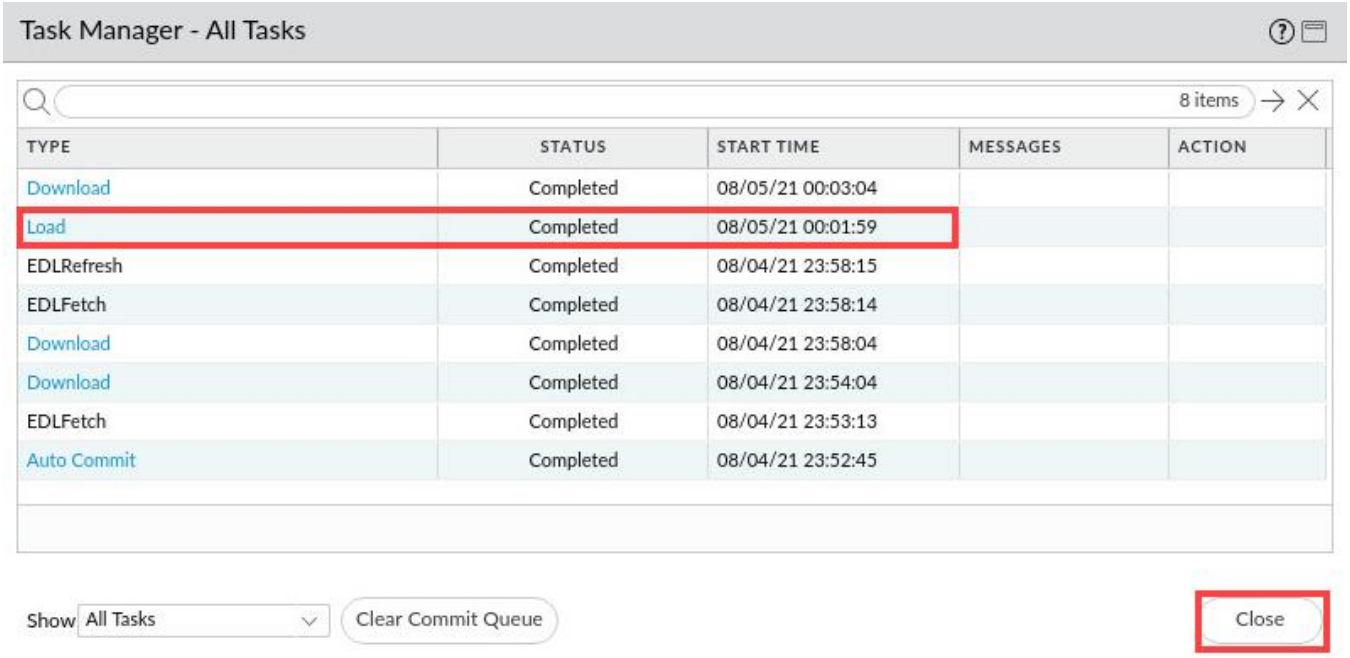
10. In the *Loading Configuration* window, a message will show *Configuration is being loaded*. *Please check the Task Manager for its status. You should reload the page when the task is completed.* Click **Close** to continue.



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

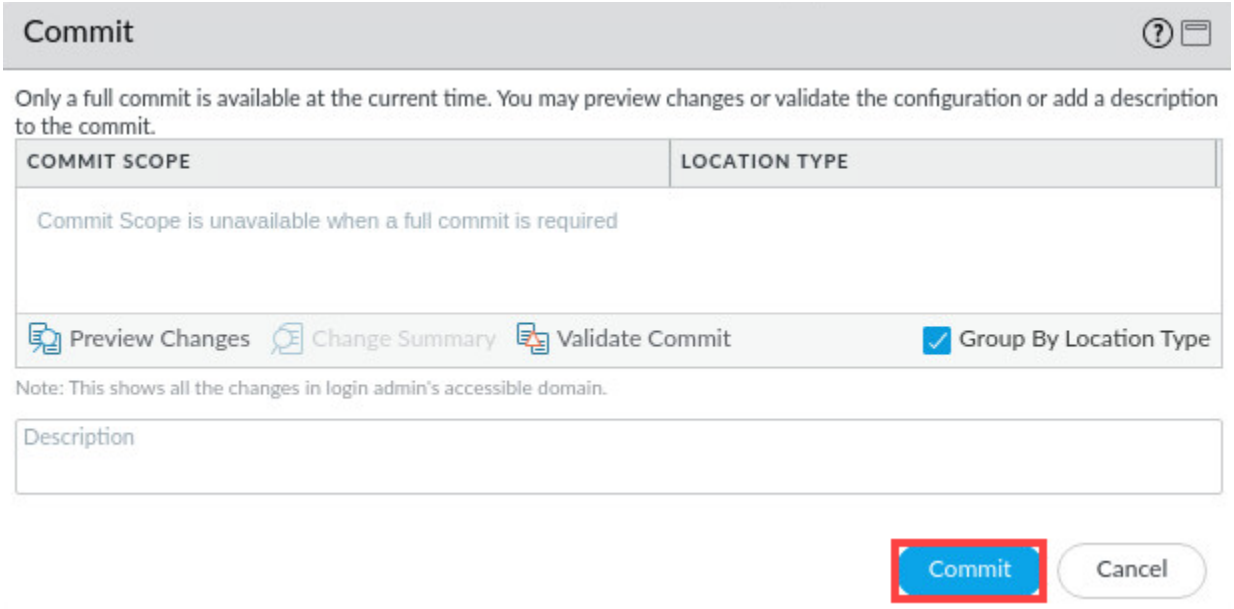


12. In the *Task Manager – All Tasks* window, verify the *Load* type has successfully completed. Click **Close**.

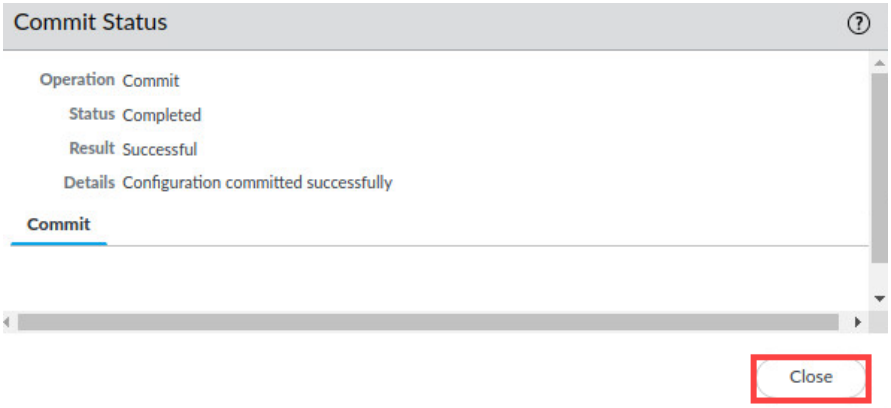


13. Click the **Commit** link located at the top-right of the web interface.

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



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



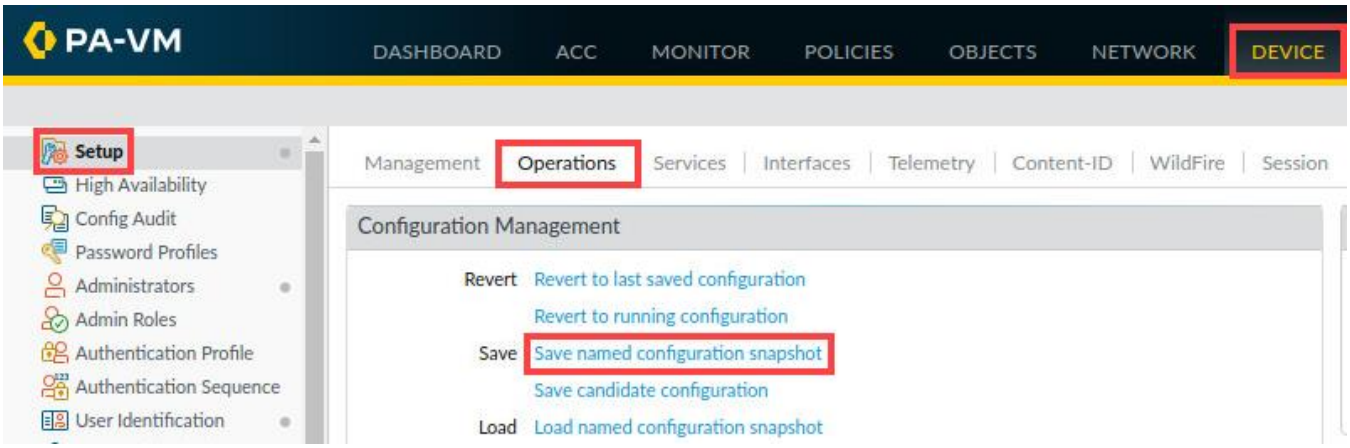
The commit process takes changes made to the Firewall and copies them to the running configuration, which will activate all configuration changes since the last commit.

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

2.2 Save a Named Configuration Snapshot

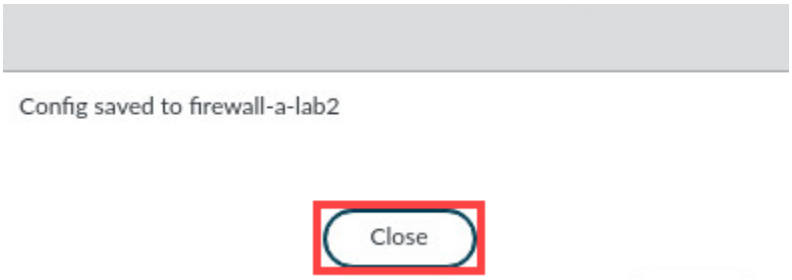
In this section, you will save the firewall configuration with a specific filename.

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**.

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



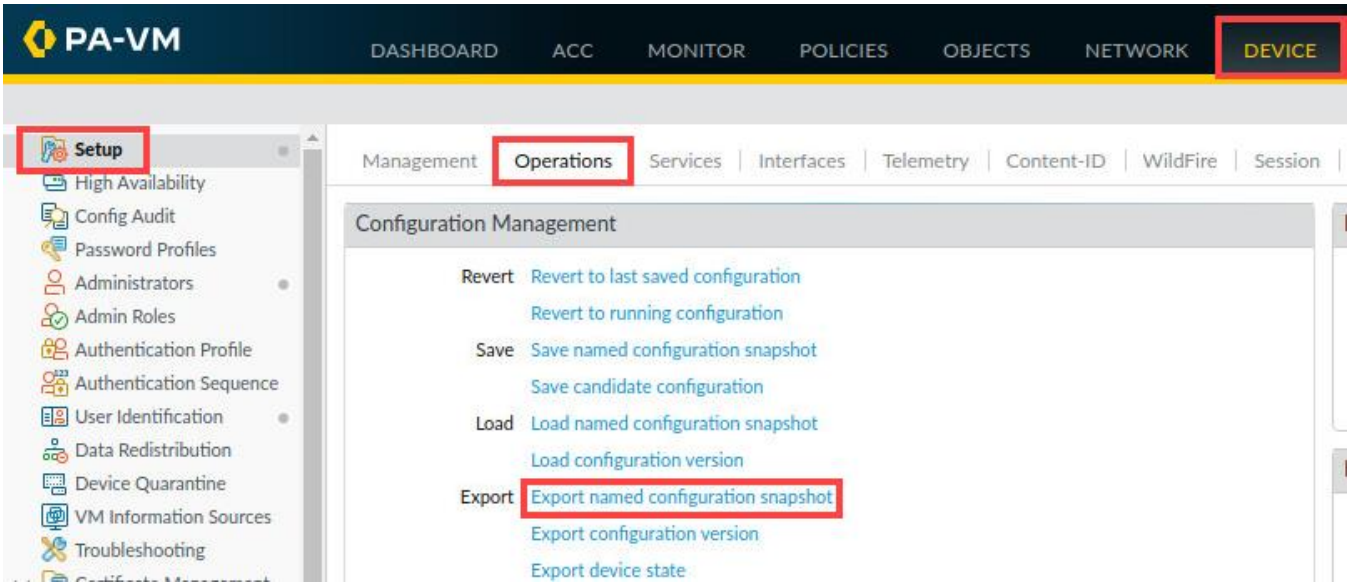
> Note that this process saved the configuration file to a location on the firewall itself.

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

2.3 Export a Named Configuration Snapshot

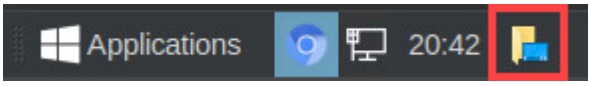
In this section, you will export the saved configuration file firewall-a-lab2 from the firewall to your workstation.

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

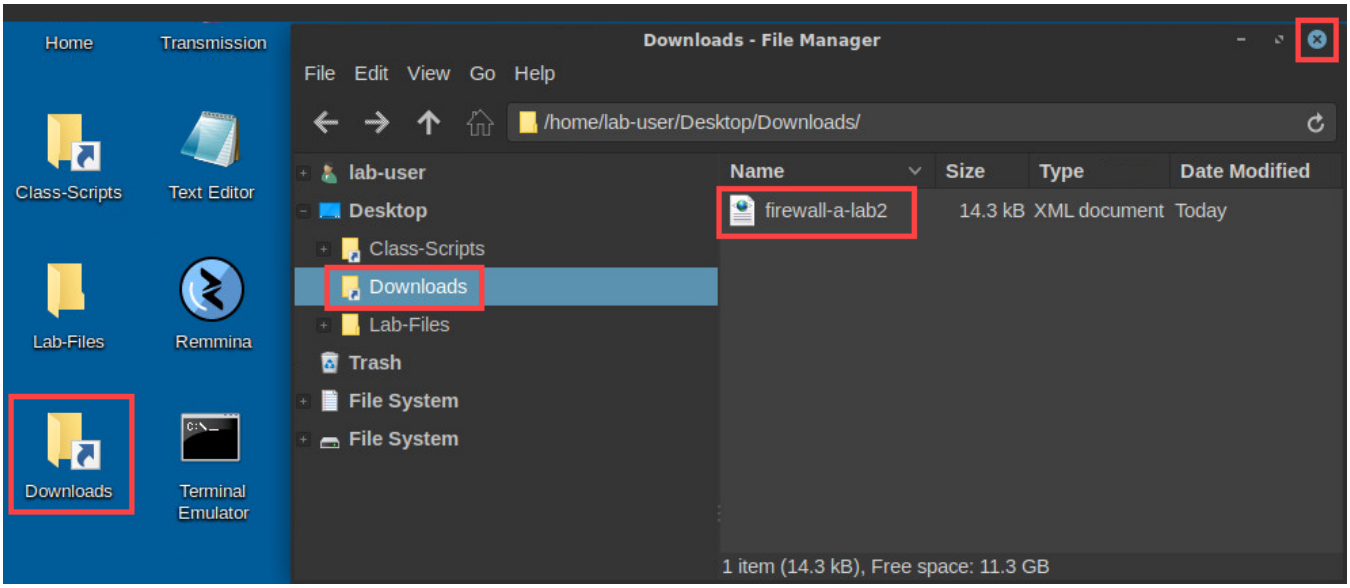


2. In the *Export Named Configuration* window, use the dropdown list and select the **firewall-a-lab2** configuration file. Click **OK**.

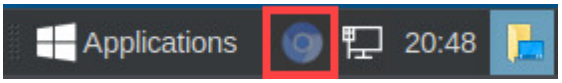
3. On the client taskbar, click the **Minimize all open windows and show the desktop** icon.



4. On the *client desktop*, open the **Downloads** folder. Verify the saved file **firewall-a-lab2** appears in the folder. Close the *Downloads* folder by clicking the **X** icon.



5. Reopen the firewall web interface by clicking on the **Chromium** icon in the taskbar.



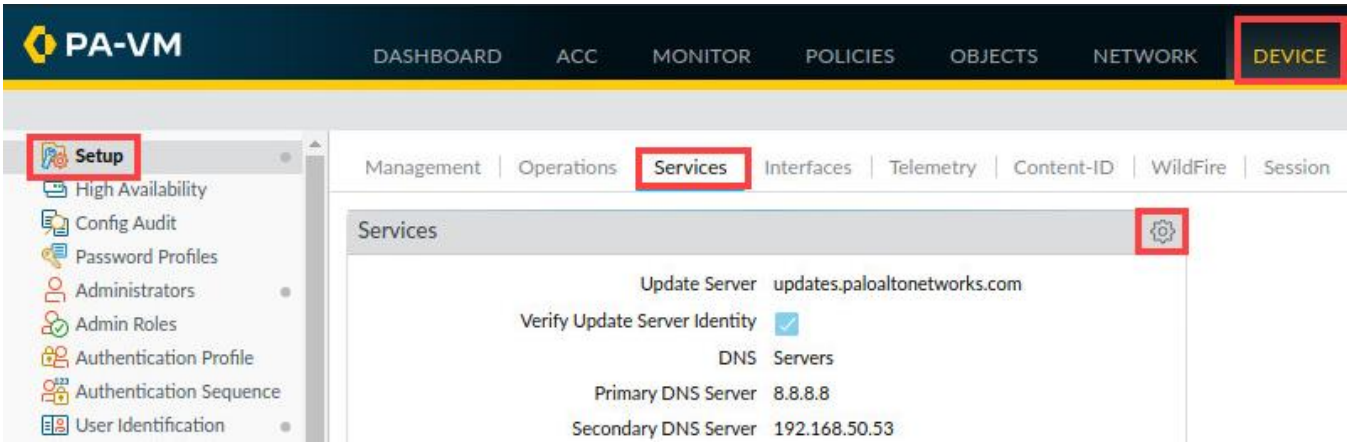
6. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

2.4 Revert Ongoing Configuration Changes

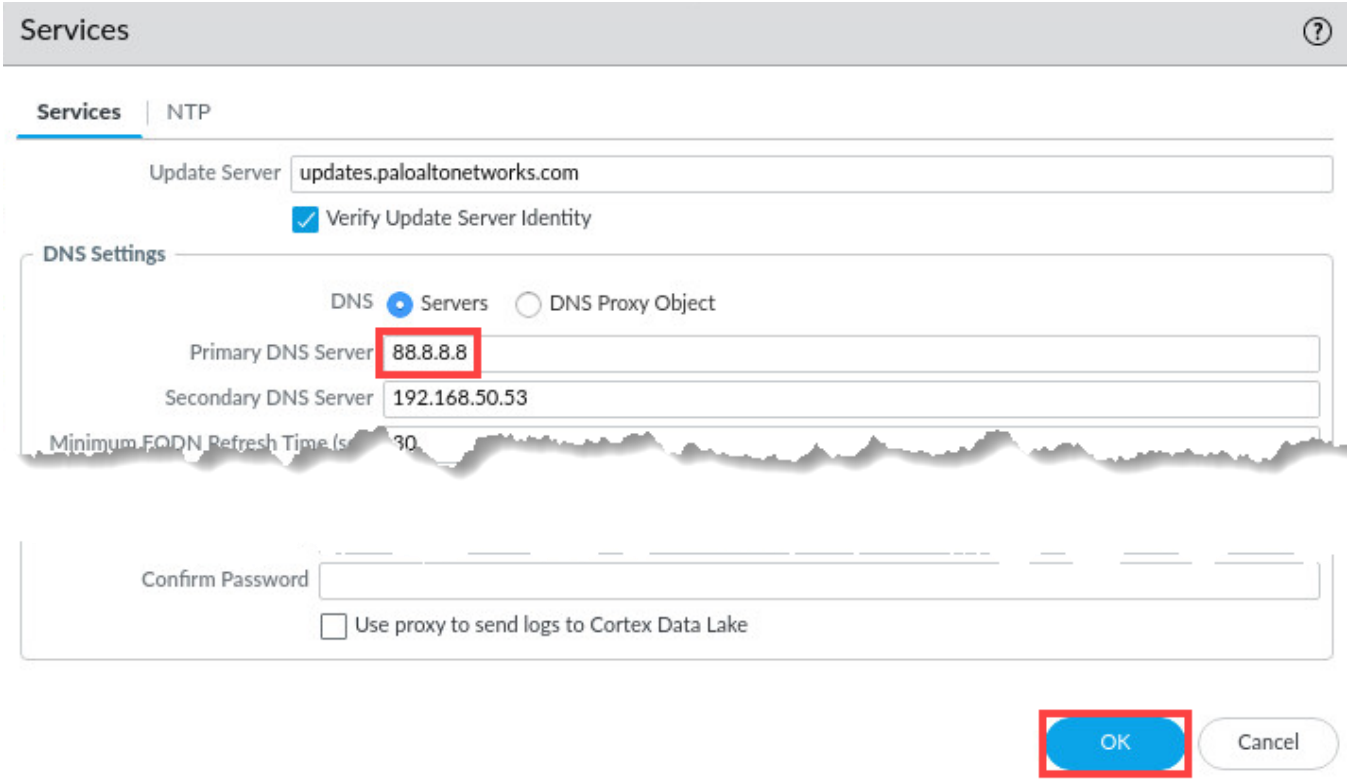
As you work on a firewall configuration, it is theoretically possible to make a mistake. In such a situation, you may not remember exactly which changes you have made or where the mistake exists in the configuration, particularly if you have made multiple changes (or multiple mistakes). Fortunately, you can revert the firewall to the current running configuration. This process essentially erases any of the changes you had 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.

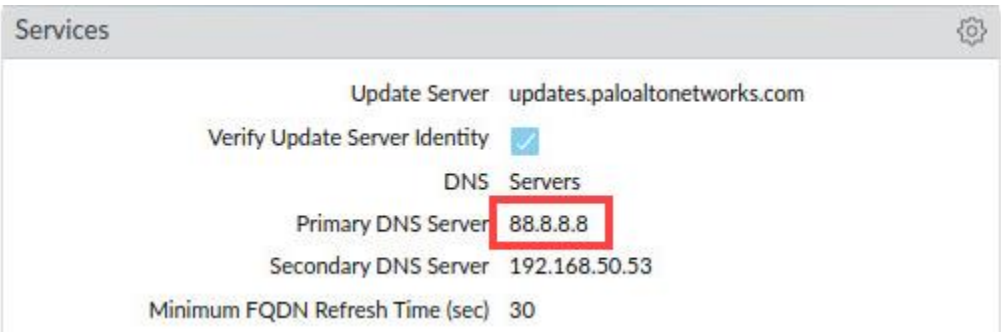
1. In the firewall web interface, select **Device > Setup > Services**. Edit the *Services* section by clicking the **Services gear** icon.



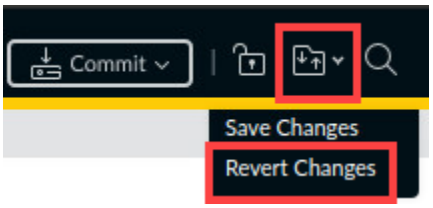
2. In the *Services* window, change the value for the *Primary DNS Server* to **`88.8.8.8`** (an easy mistake to make)**.** Click **OK.**



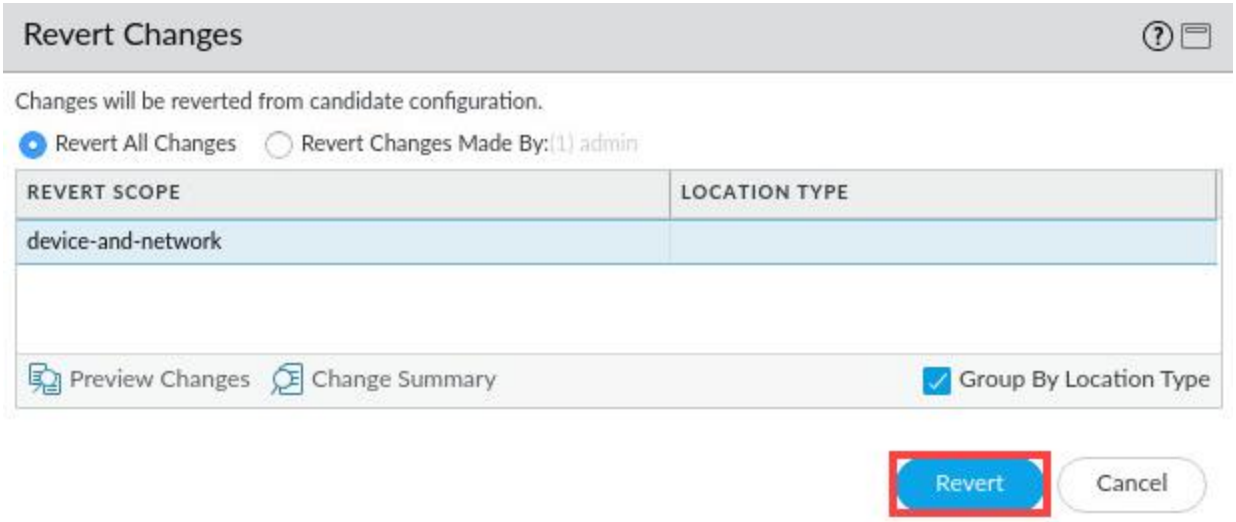
3. Verify the mistake is showing in the *Services* window for the **Primary DNS Server**.



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



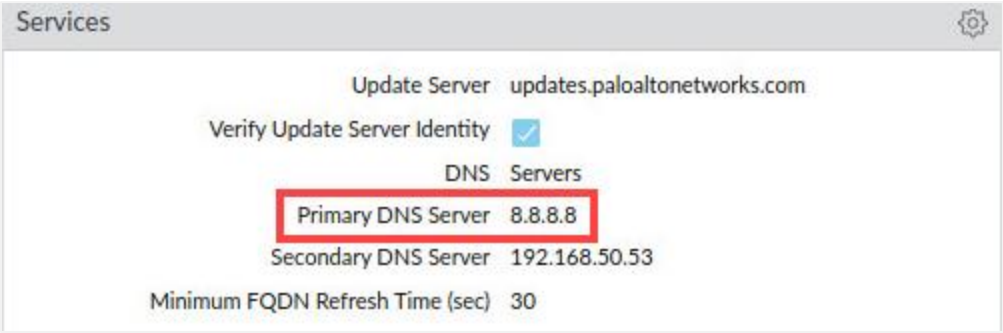
5. In the *Revert Changes* window, leave the settings unchanged. Click **Revert**.



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**.

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



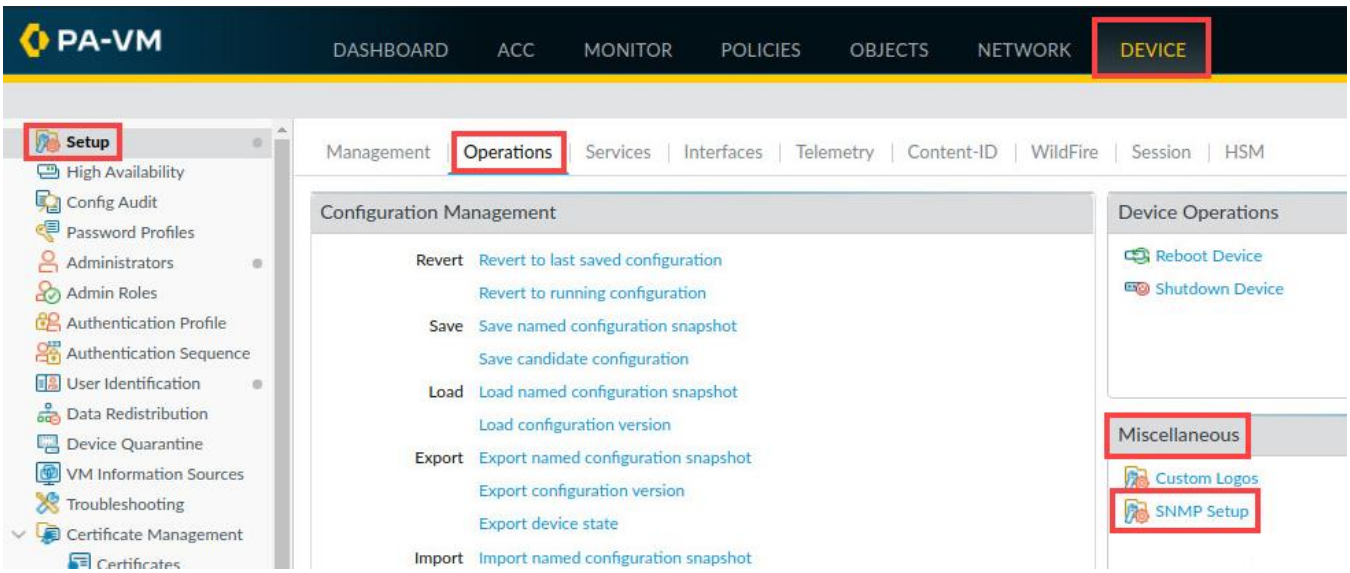
8. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

2.5 Preview Configuration Changes

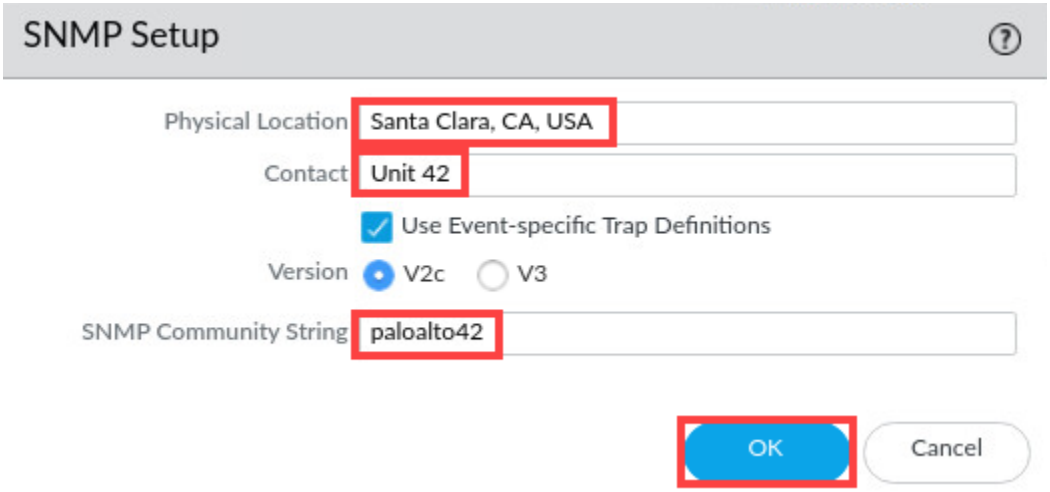
Before you commit changes to the firewall, you can compare the impending changes with the current configuration settings. This process can be useful to make certain you have the right changes in place before they are implemented on the firewall.

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.

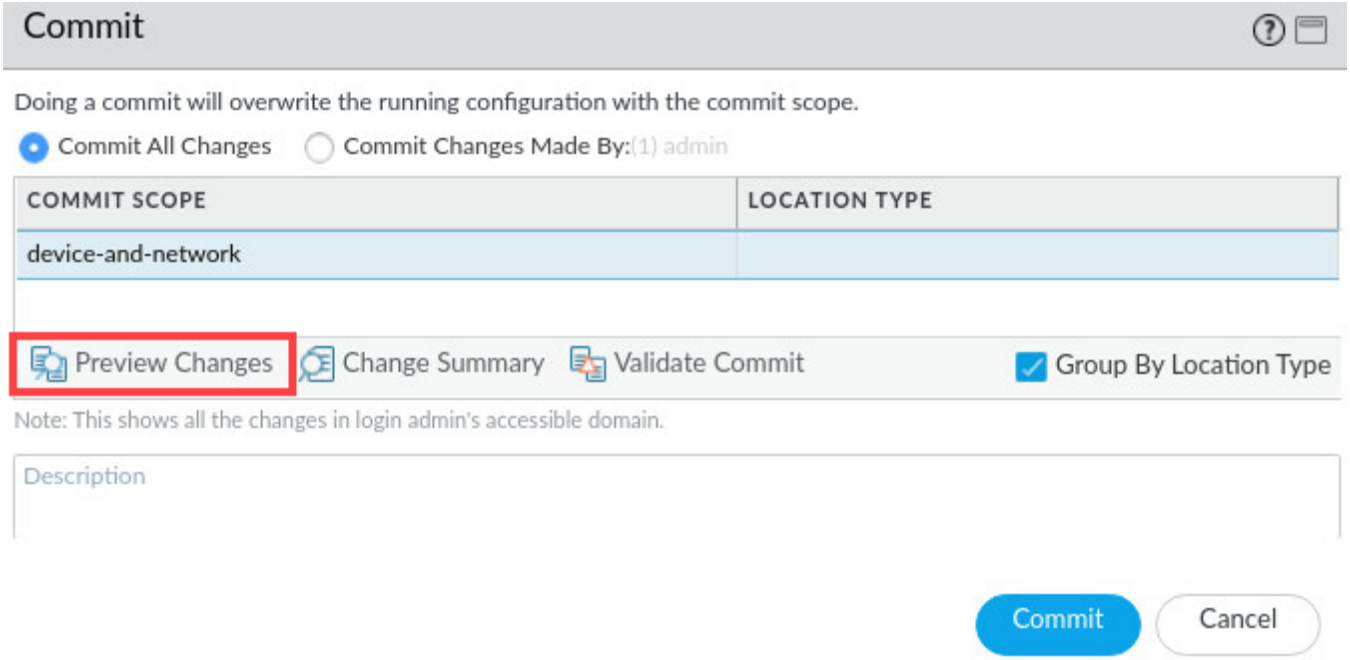


2. In the *SNMP Setup* window, change the *Physical Location* to **`Santa Clara, CA, USA`** for *Contact*, enter **`Unit 42`**, for *SNMP Community String*, enter **`paloalto42`**. Click **`OK`**.

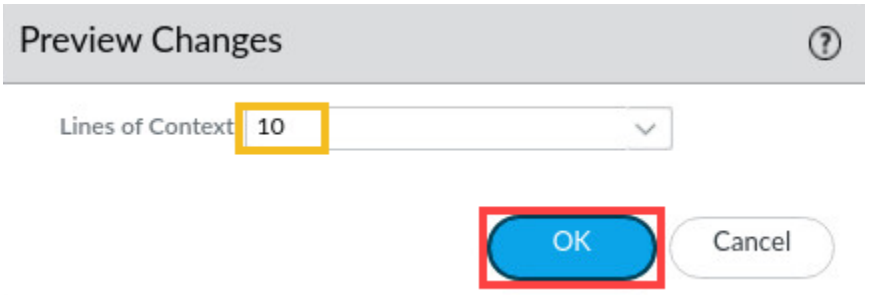


3. Commit your changes to the firewall by clicking the **Commit** button at the upper-right of the *PA-VM* web interface.

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

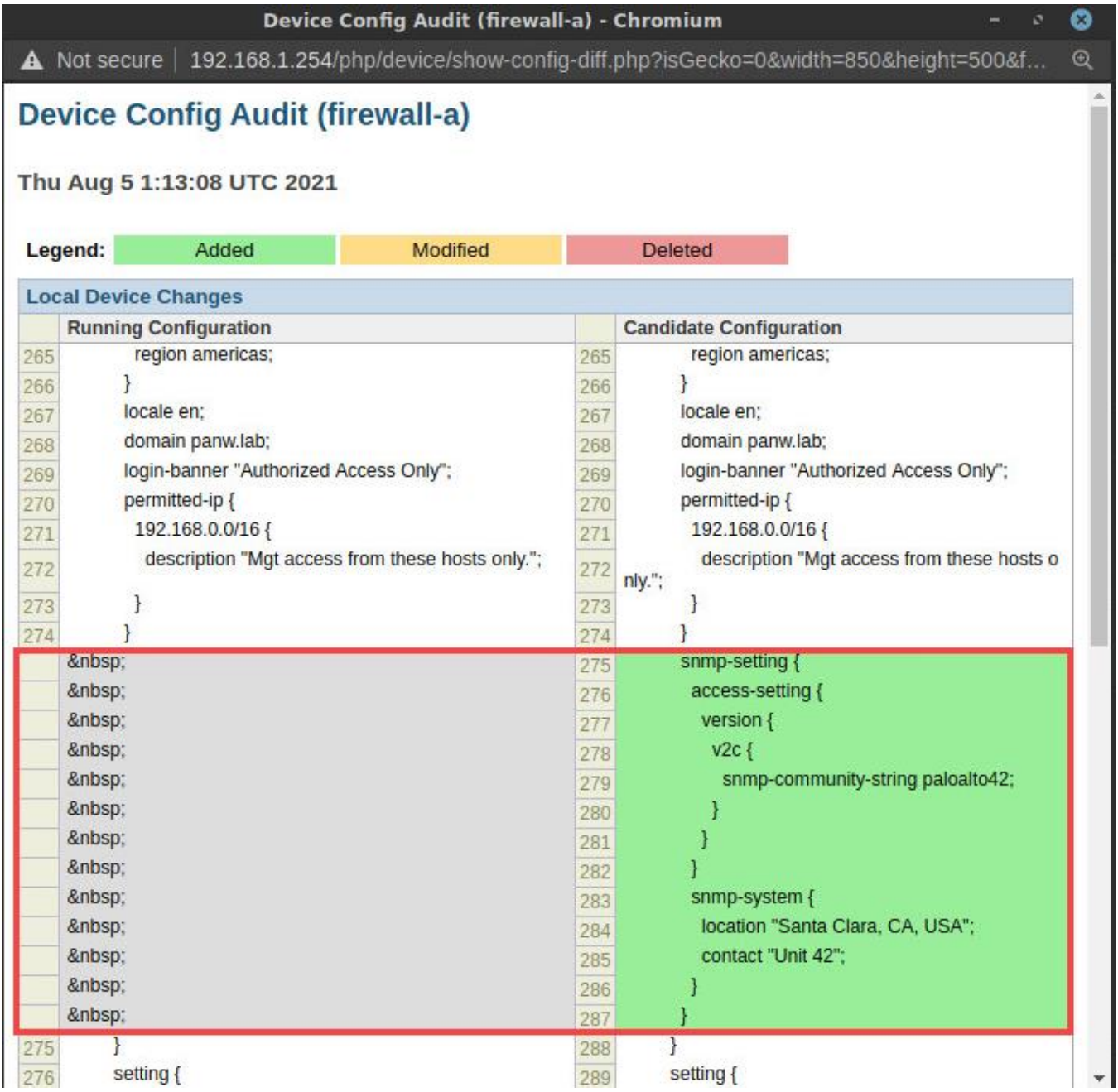


5. In the *Preview Changes* window, leave the *Lines of Context* set to **10**. Click **OK**.



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

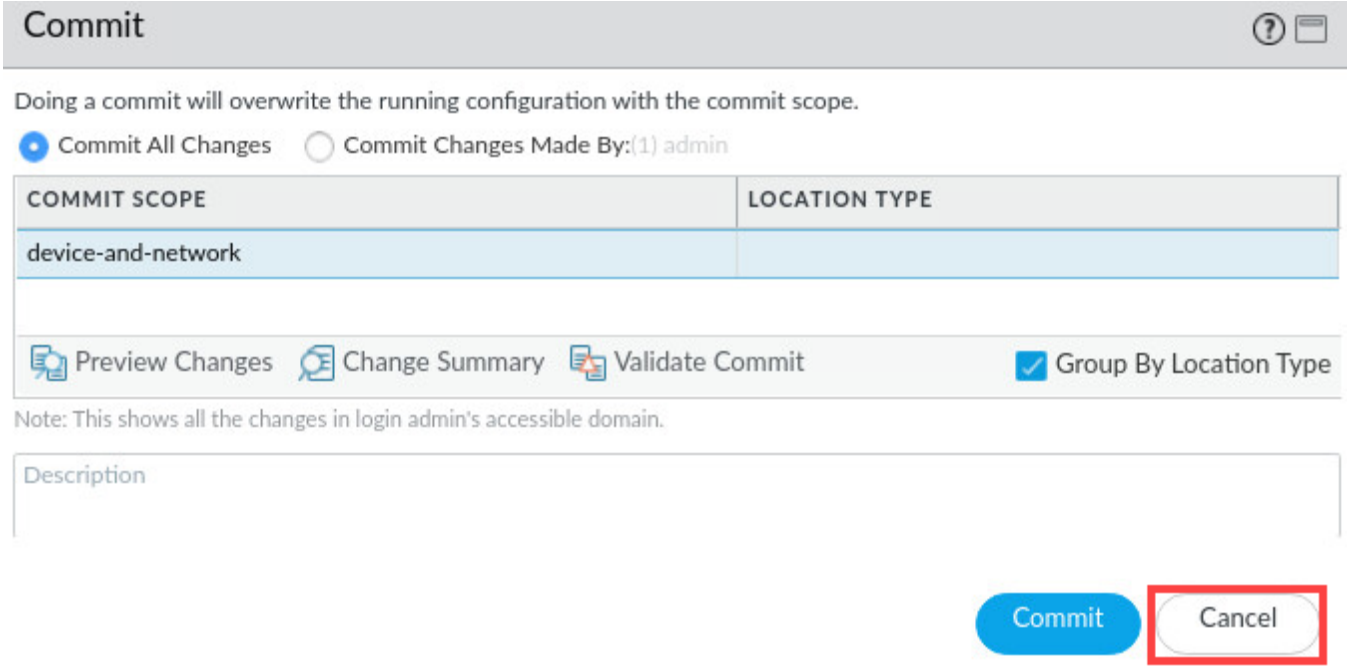
6. A new browser window named *Device Config Audit* will appear that displays a side-by-side comparison of the current *running configuration* (on the left) and the proposed changes in the *candidate configuration* (on the right). Review the snmp settings that were changed.



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.

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



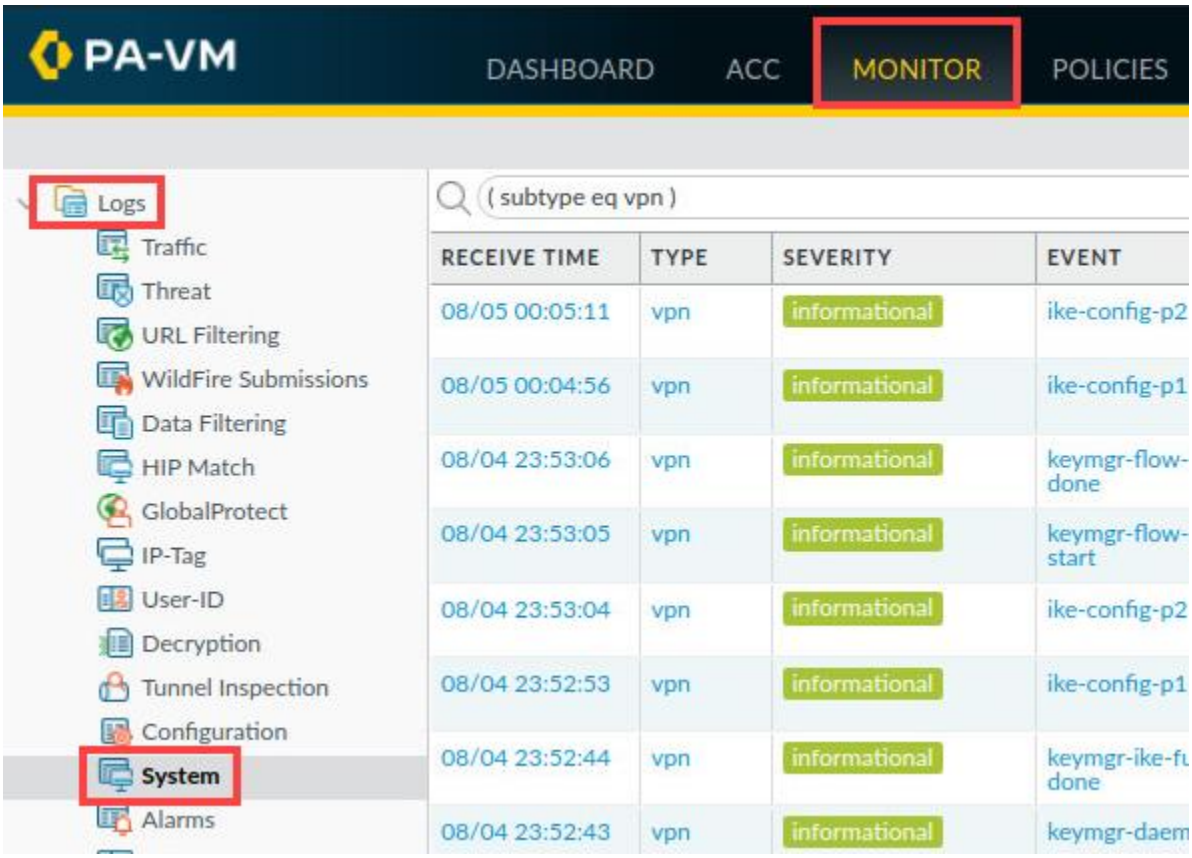
9. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

2.6 Examine Log Files

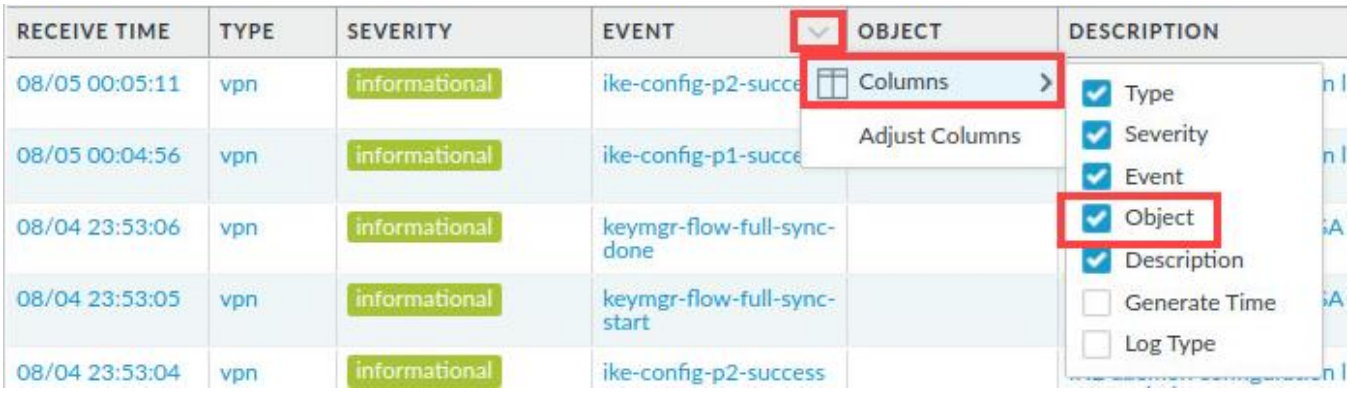
Although the information in log files varies, the process of examining and searching log files on the firewall is the same.

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.

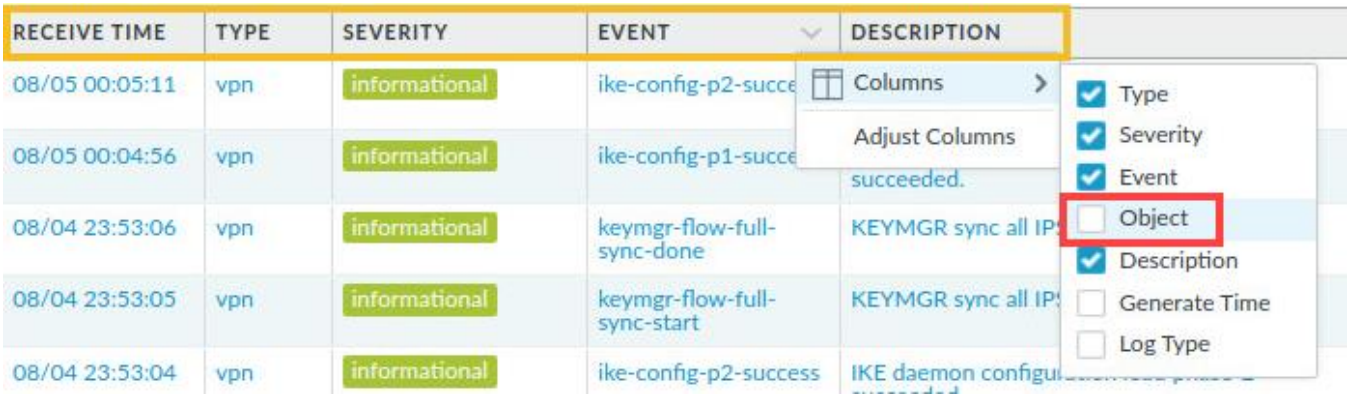
1. In the *PA-VM* firewall interface, select **Monitor > Logs > System**.



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



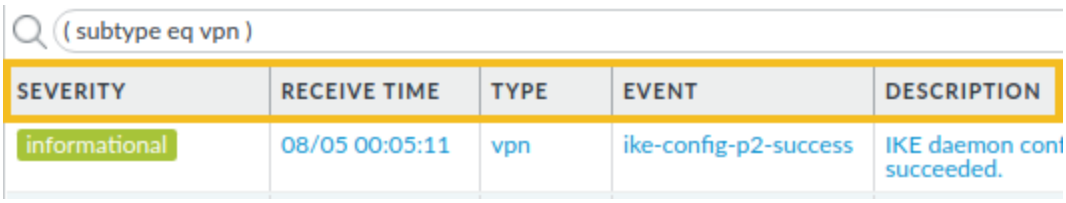
3. Uncheck **Object** and notice the *Object* column is now hidden.



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.

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



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.

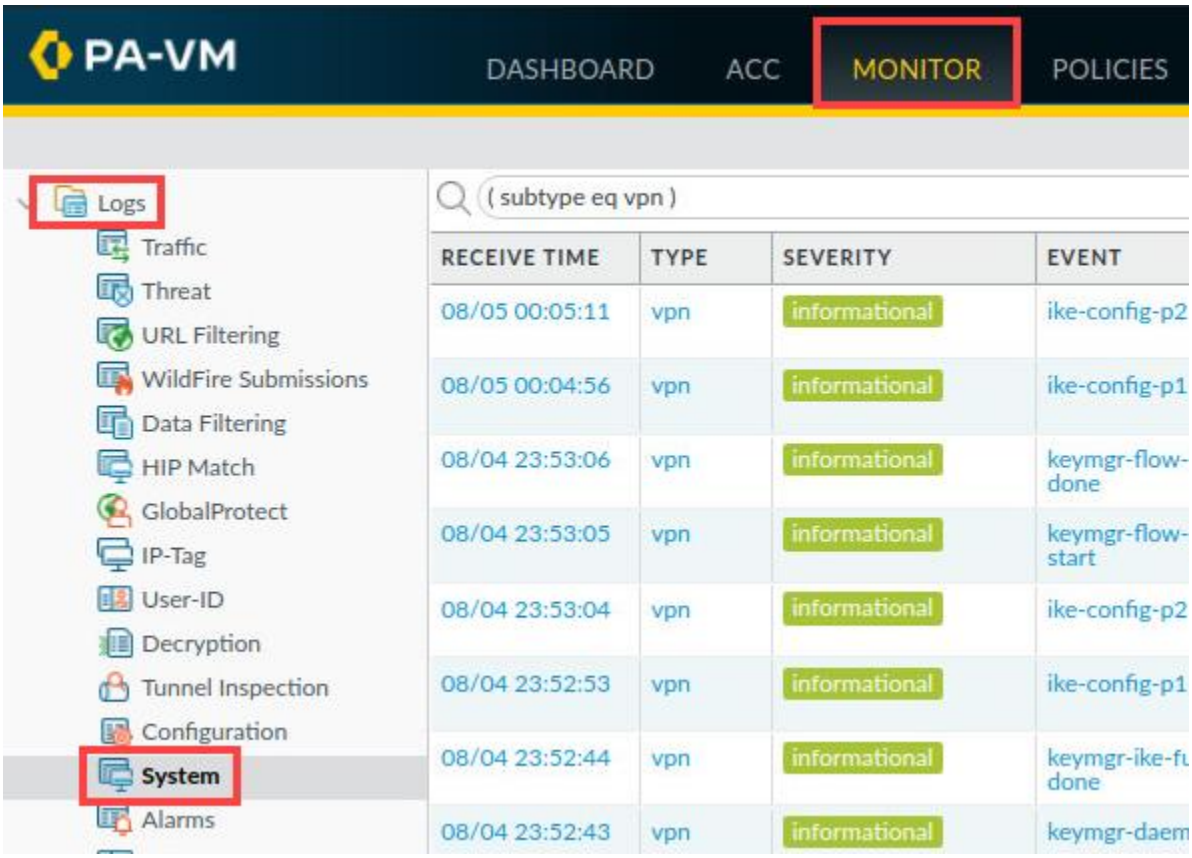
6. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

2.7 Create a Log File Filter

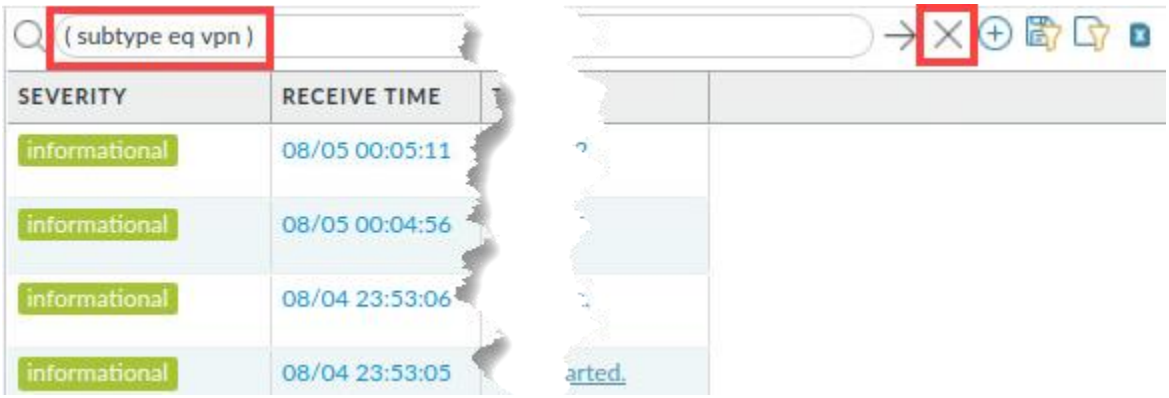
Scanning through log files row-by-row is tedious. If you are looking for specific information, you can create filters quickly to display only entries that match certain criteria. All log files support filters.

In this section, you will examine and navigate the firewall System **l**og. 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.

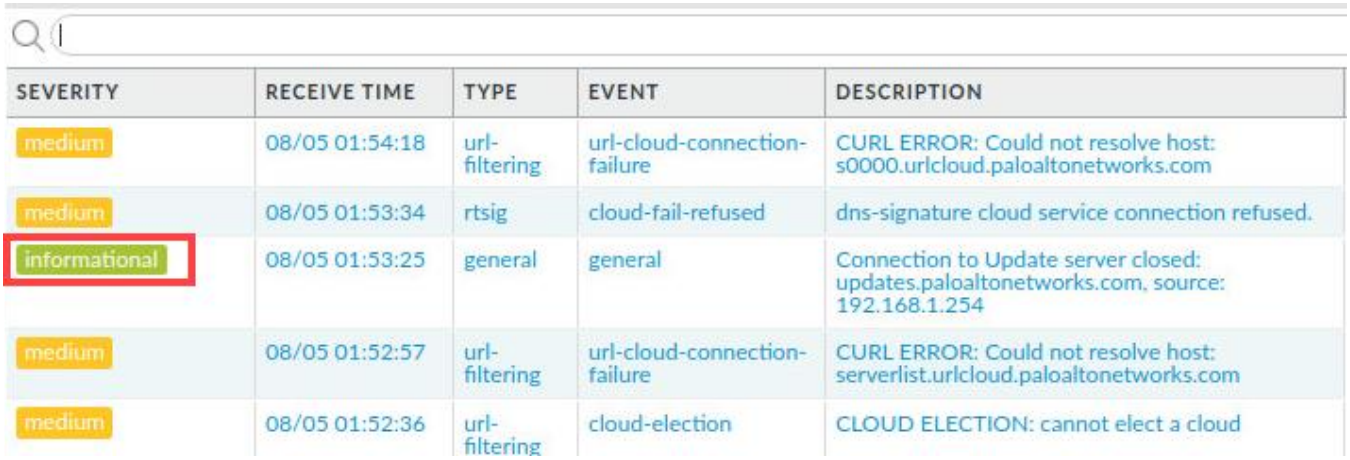
1. In the PA-VM firewall interface, select **Monitor > Logs > System**.



2. In the *System log* file, notice the filter **(subtype eq vpn)**. Delete the filter by clicking on the **X** *(Clear Filter)* button.

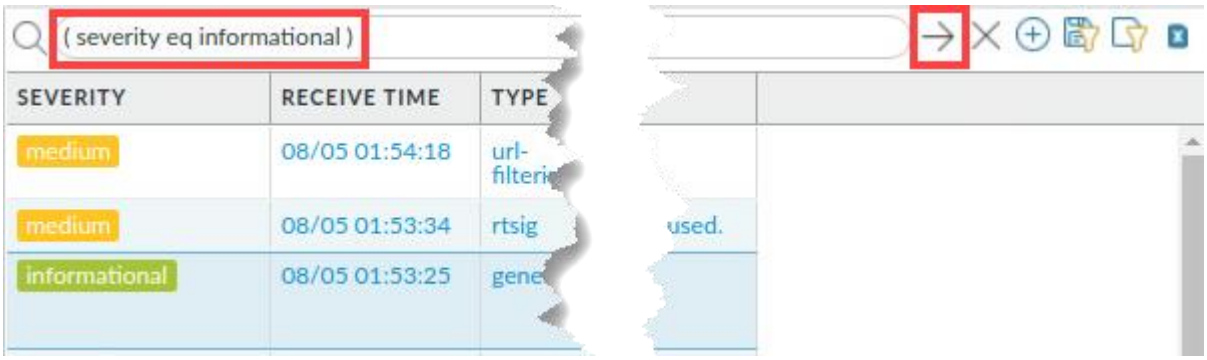


3. In the *System log* file, click any entry under the *Severity* column that contains **informational**. Click **informational**.

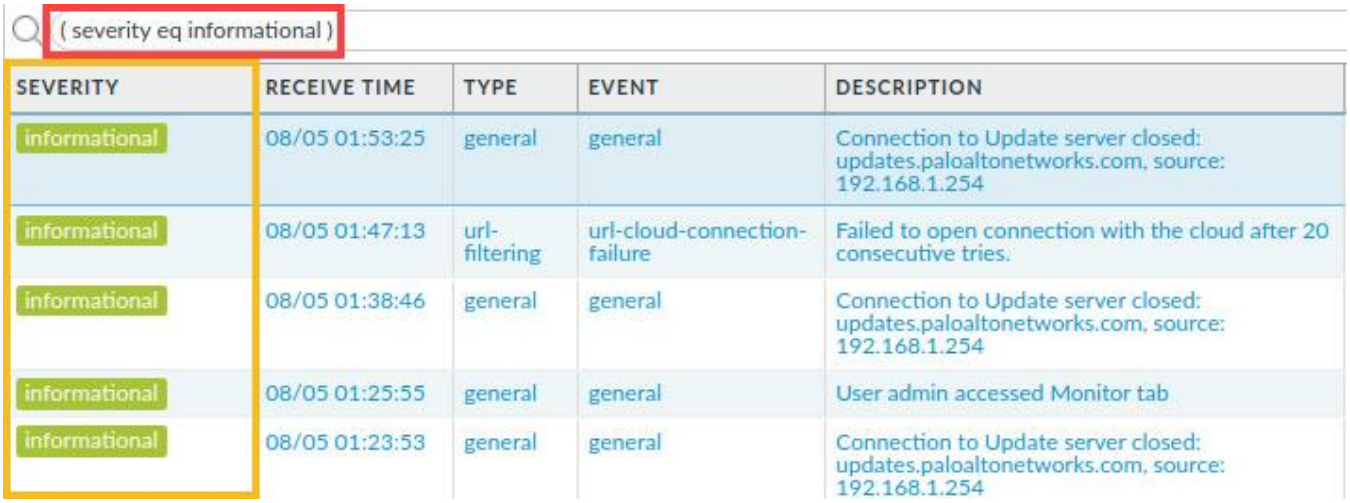


SEVERITY	RECEIVE TIME	TYPE	EVENT	DESCRIPTION
medium	08/05 01:54:18	url-filtering	url-cloud-connection-failure	CURL ERROR: Could not resolve host: s0000.urlcloud.paloaltonetworks.com
medium	08/05 01:53:34	rtsig	cloud-fail-refused	dns-signature cloud service connection refused.
informational	08/05 01:53:25	general	general	Connection to Update server closed: updates.paloaltonetworks.com, source: 192.168.1.254
medium	08/05 01:52:57	url-filtering	url-cloud-connection-failure	CURL ERROR: Could not resolve host: serverlist.urlcloud.paloaltonetworks.com
medium	08/05 01:52:36	url-filtering	cloud-election	CLOUD ELECTION: cannot elect a cloud

4. 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.

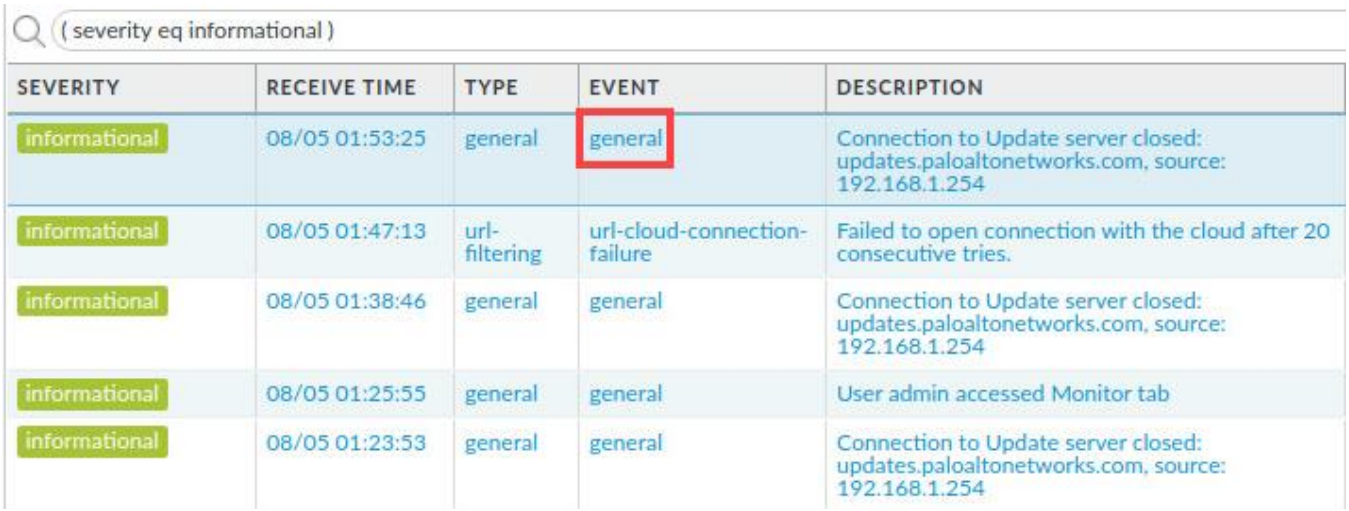


5. The System log display will update to show only those entries that contain **informational** as the *Severity* level.



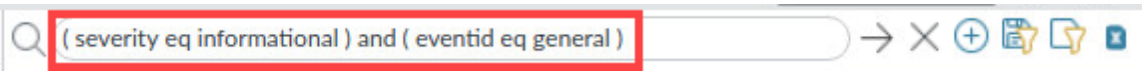
SEVERITY	RECEIVE TIME	TYPE	EVENT	DESCRIPTION
informational	08/05 01:53:25	general	general	Connection to Update server closed: updates.paloaltonetworks.com, source: 192.168.1.254
informational	08/05 01:47:13	url-filtering	url-cloud-connection-failure	Failed to open connection with the cloud after 20 consecutive tries.
informational	08/05 01:38:46	general	general	Connection to Update server closed: updates.paloaltonetworks.com, source: 192.168.1.254
informational	08/05 01:25:55	general	general	User admin accessed Monitor tab
informational	08/05 01:23:53	general	general	Connection to Update server closed: updates.paloaltonetworks.com, source: 192.168.1.254

6. Under the *Event* column, click any entry that contains the word **general**. Click **general**.

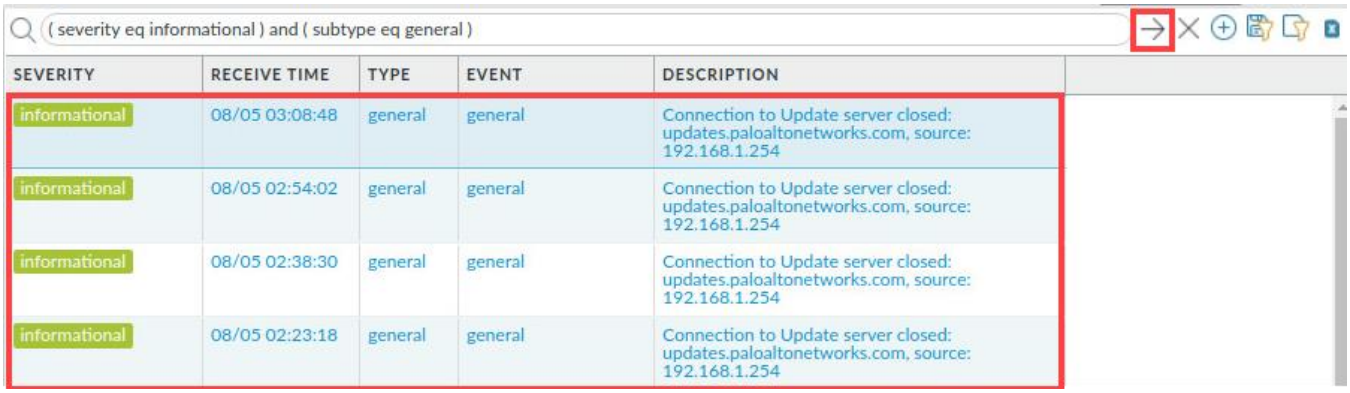


SEVERITY	RECEIVE TIME	TYPE	EVENT	DESCRIPTION
informational	08/05 01:53:25	general	general	Connection to Update server closed: updates.paloaltonetworks.com, source: 192.168.1.254
informational	08/05 01:47:13	url-filtering	url-cloud-connection-failure	Failed to open connection with the cloud after 20 consecutive tries.
informational	08/05 01:38:46	general	general	Connection to Update server closed: updates.paloaltonetworks.com, source: 192.168.1.254
informational	08/05 01:25:55	general	general	User admin accessed Monitor tab
informational	08/05 01:23:53	general	general	Connection to Update server closed: updates.paloaltonetworks.com, source: 192.168.1.254

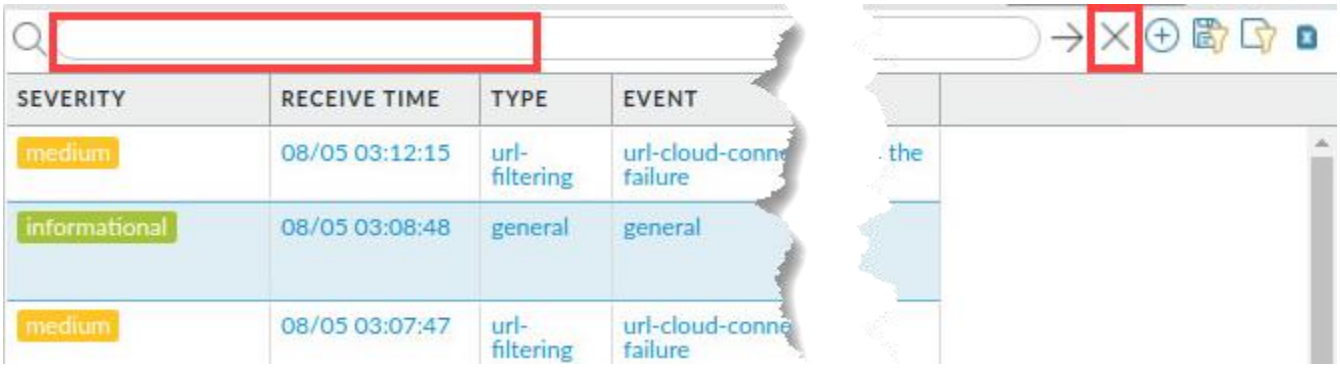
7. Notice the interface will update the syntax to create a combined filter.



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



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



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.

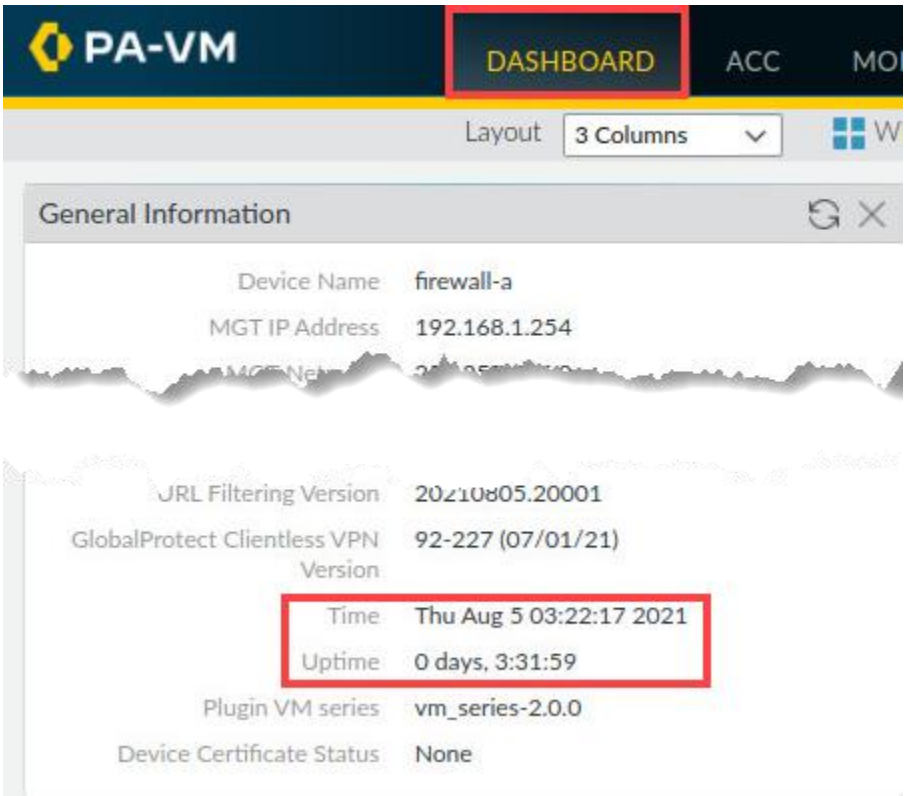
10. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

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.

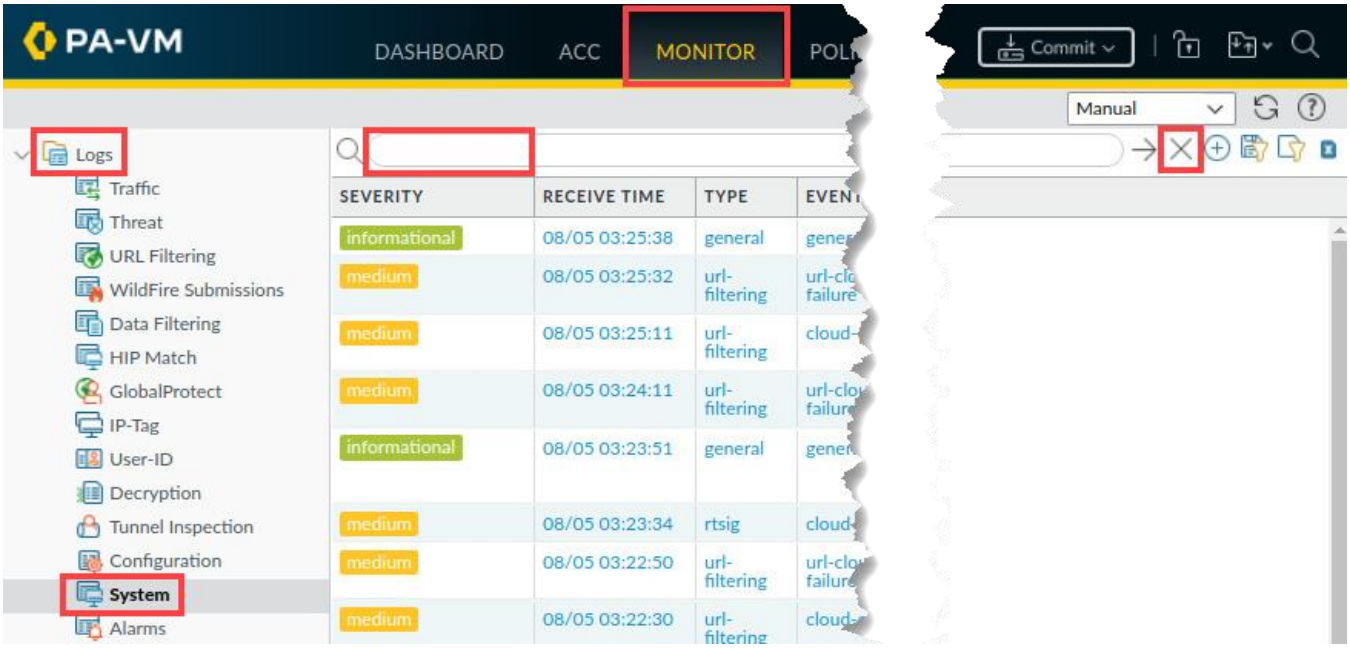
1. In the *PA-VM* web interface, select the **Dashboard** tab. Under the *General Information* section, scroll to the bottom and locate the **Time.** Make a note of the date and time displayed (you will need this information in a later step).



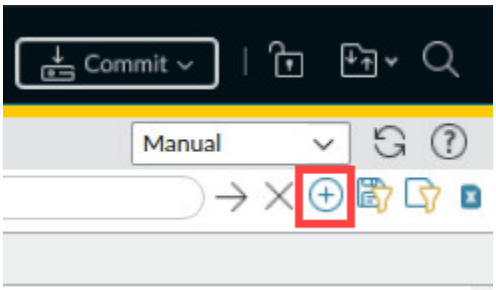
Please Note

For this lab, notice the time of 03:22:17. 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.

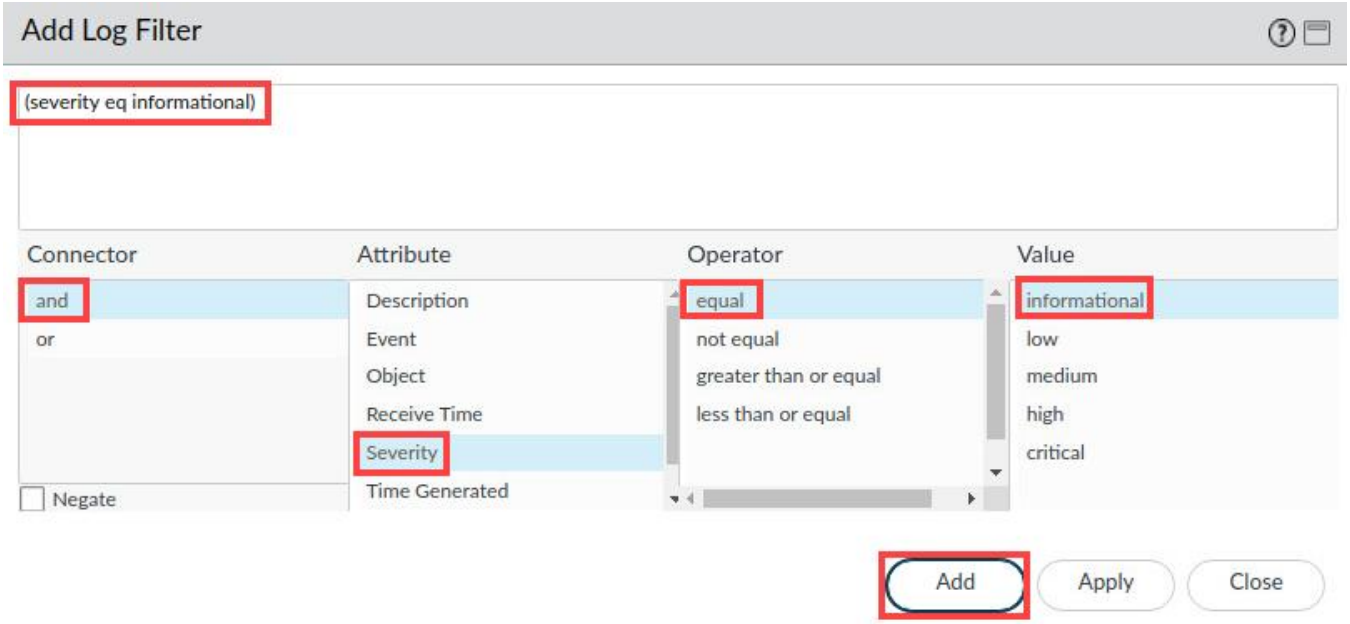


3. Click the **Add Filter** button in the upper-right corner of the *System Logs* window.



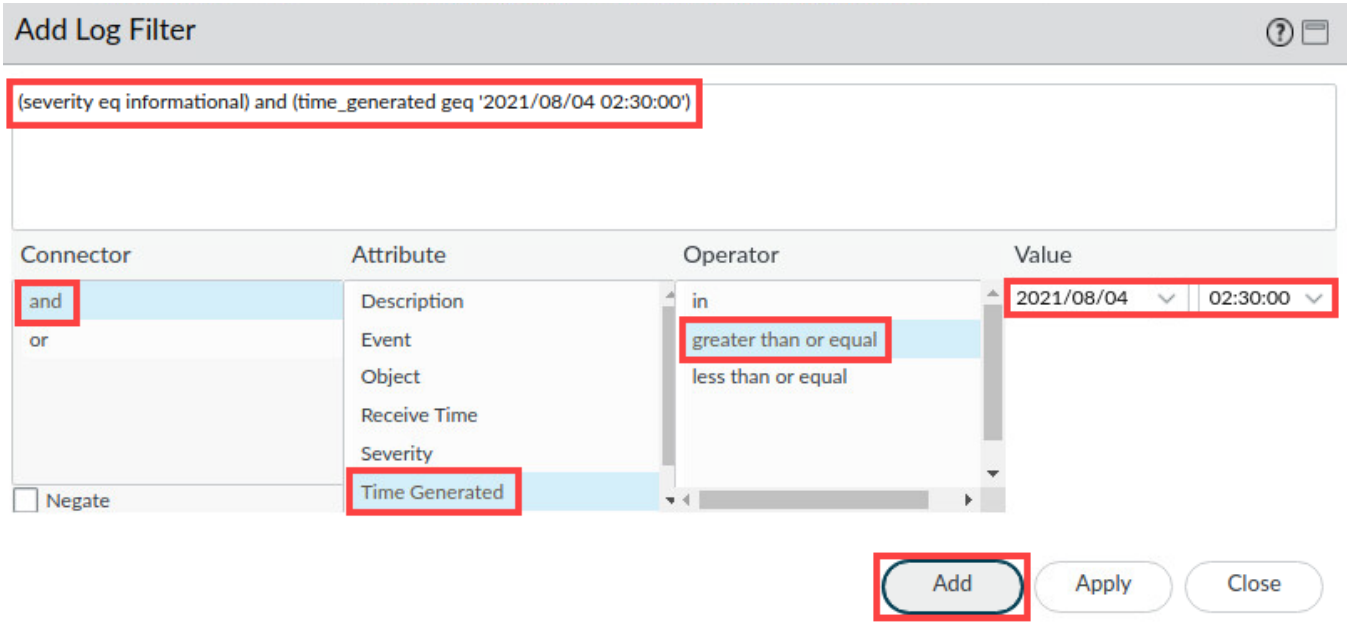
4. In the *Add Log Filter* window, fill in the following information below.

   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



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

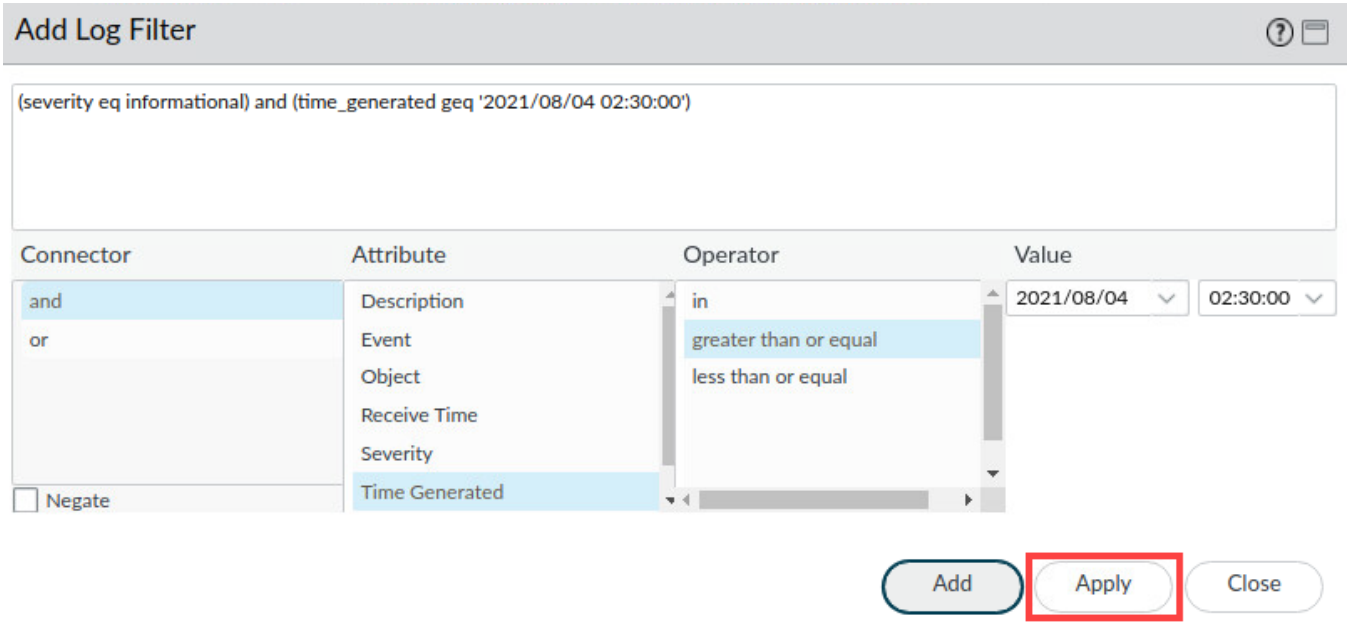
   A. Under the *Connector* column, select **and.**
   B. Under the *Attribute* column, select **Time Generated.**
   C. Under *Operator*, select **greater than or equal to.**
   D. Under the *Value* column, use the first dropdown list to select the date you recorded in step 1.
   E. Under the *Value* column, use the second dropdown 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.



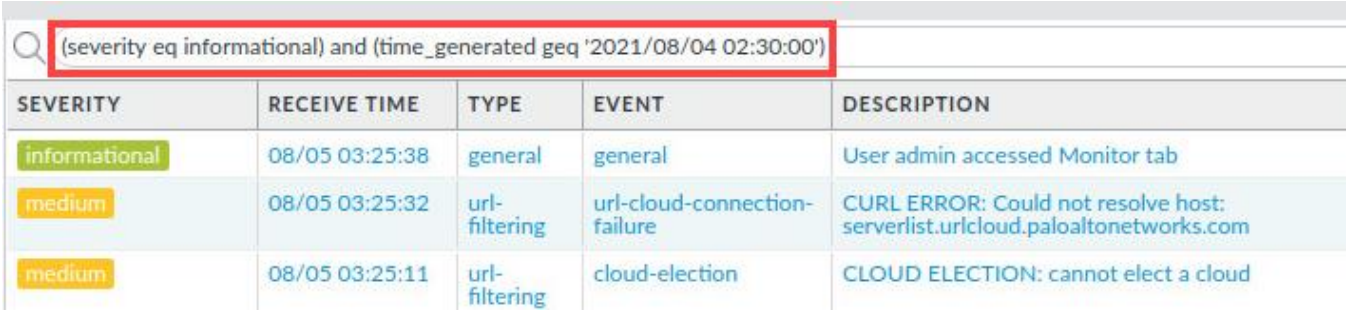
Please Note

For this lab example, you notice the time that was recorded will be 03:22:17. When you round down, the value to record will be 02:30:00. The time and date for your filter will differ from the example shown here.

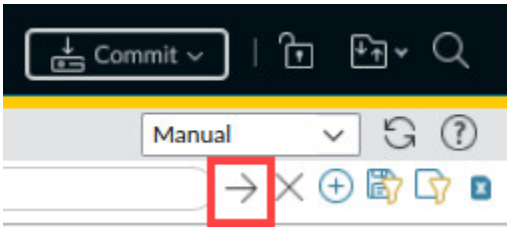
6. In the *Add Log Filter* window, click **Apply**.



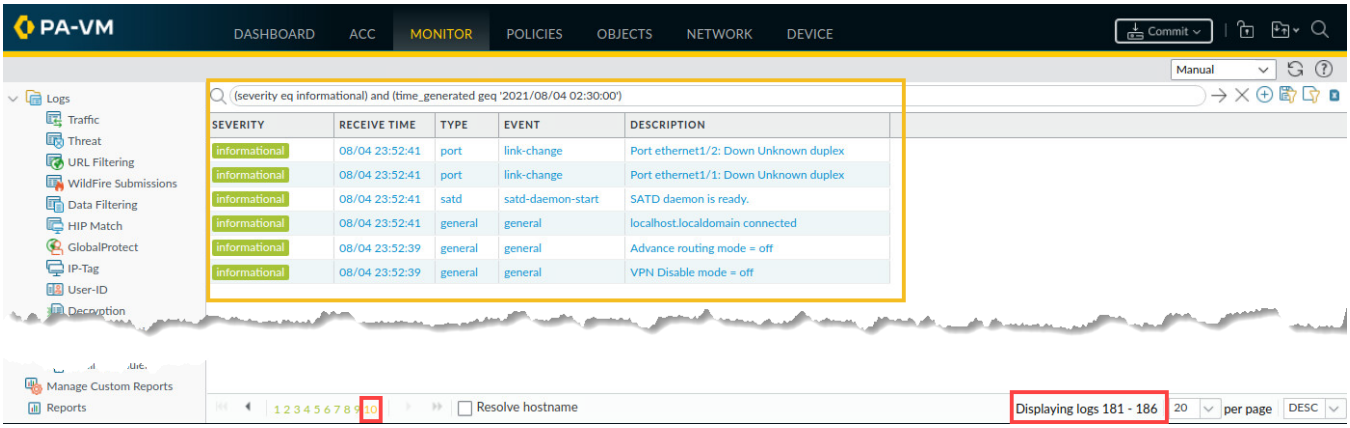
7. Your filter will appear in the System log syntax field. Remember, your *time* will be different than this lab example.



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 waited some time and went to the very last page, which was page 10. Page 10 shows you the first entry after the time that was specified in the filter creation.



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.