NETWORK SECURITY FUNDAMENTALS V2

Lab 6: Decrypting SSH Traffic

Document Version: 2022-12-23

Contents

Introduction

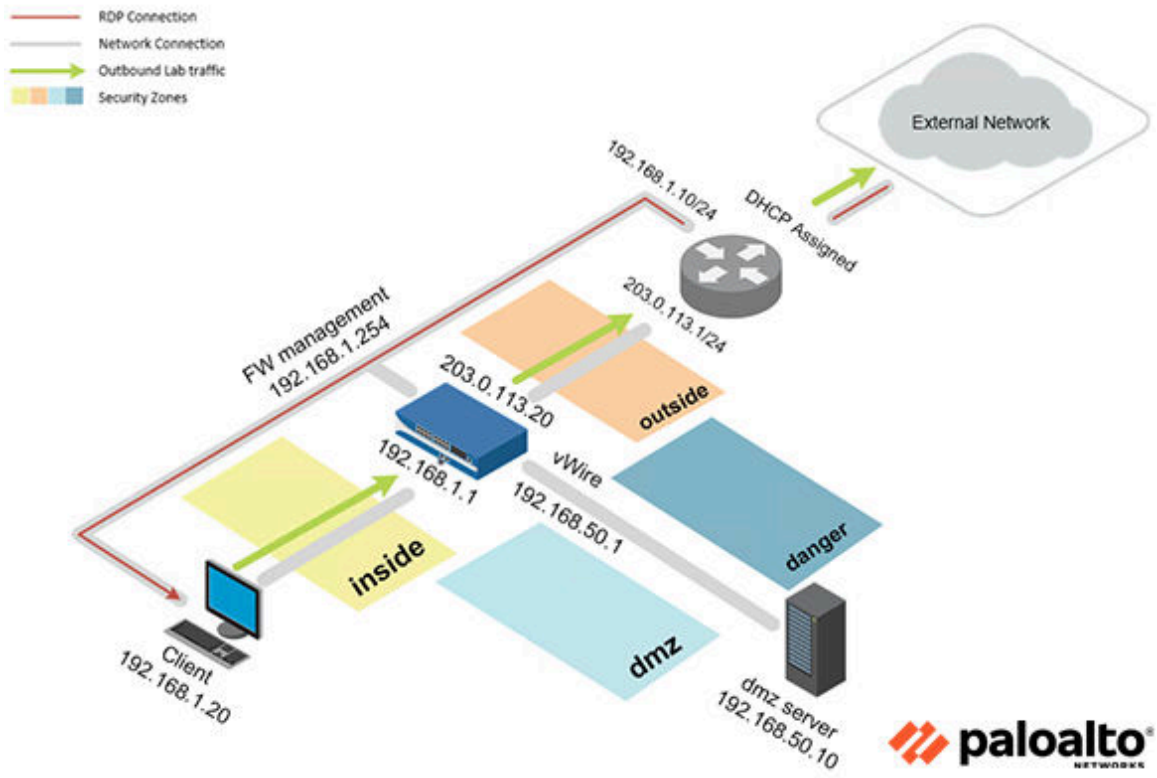
In this lab, you will decrypt SSH traffic by creating a decryption policy. Then, you will use PuTTY to SSH to the DMZ server (traffic-generator) and monitor the traffic logs on the Firewall to show the SSH session has been decrypted.

Objective

In this lab, you will perform the following tasks:

- Create a Decryption Policy and Commit
- Create an SSH session with PuTTY and Verify Decryption Is Working
- Disable Decryption Policy

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.

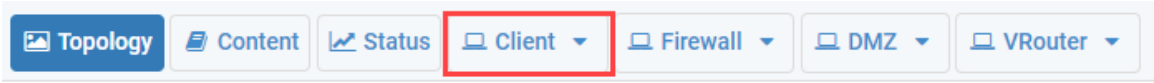
Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Client	192.168.1.20	`lab-user`	`Pal0Alt0!`
DMZ	192.168.50.10	`root`	`Pal0Alt0!`
Firewall	192.168.1.254	`admin`	`Pal0Alt0!`

1 Decrypting SSH Traffic

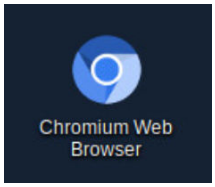
1.0 Load Lab Configuration

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

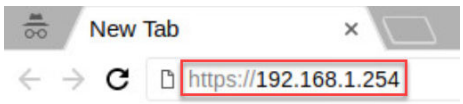
1. Click on the **Client** tab to access the Client PC.



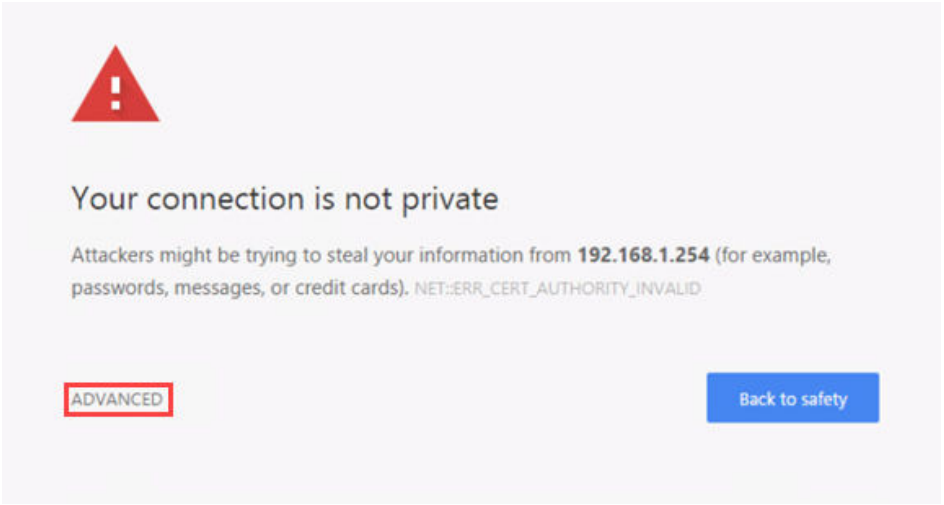
2. Log in to the Client PC as username `lab-user`, password `Pal0Alt0!`.
3. Double-click the **Chromium Web Browser** icon located on the desktop.



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

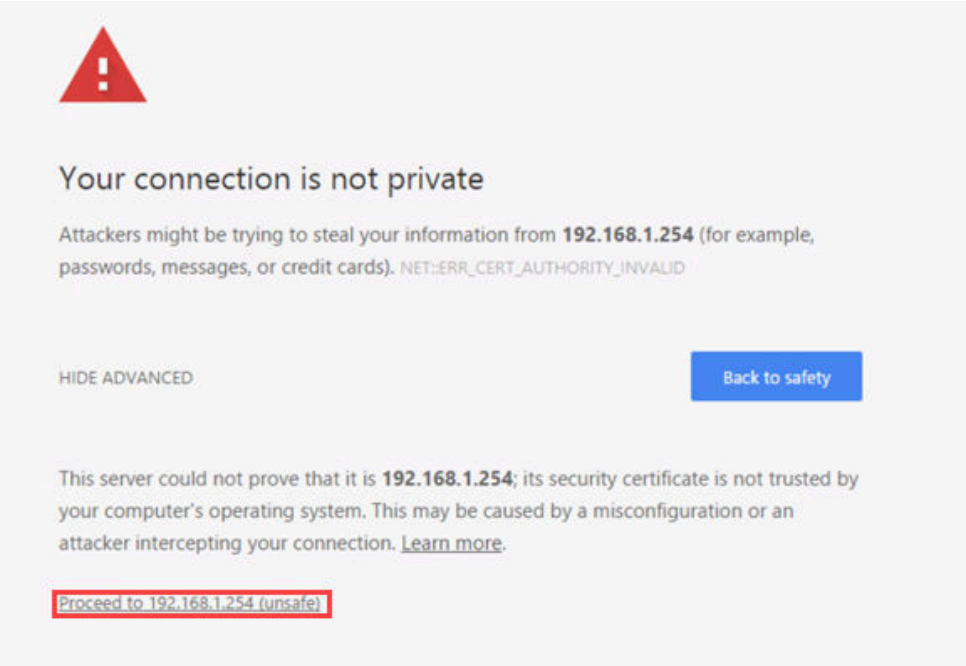


5. You will see a "*Your connection is not private*" message. Click on the **ADVANCED** link.



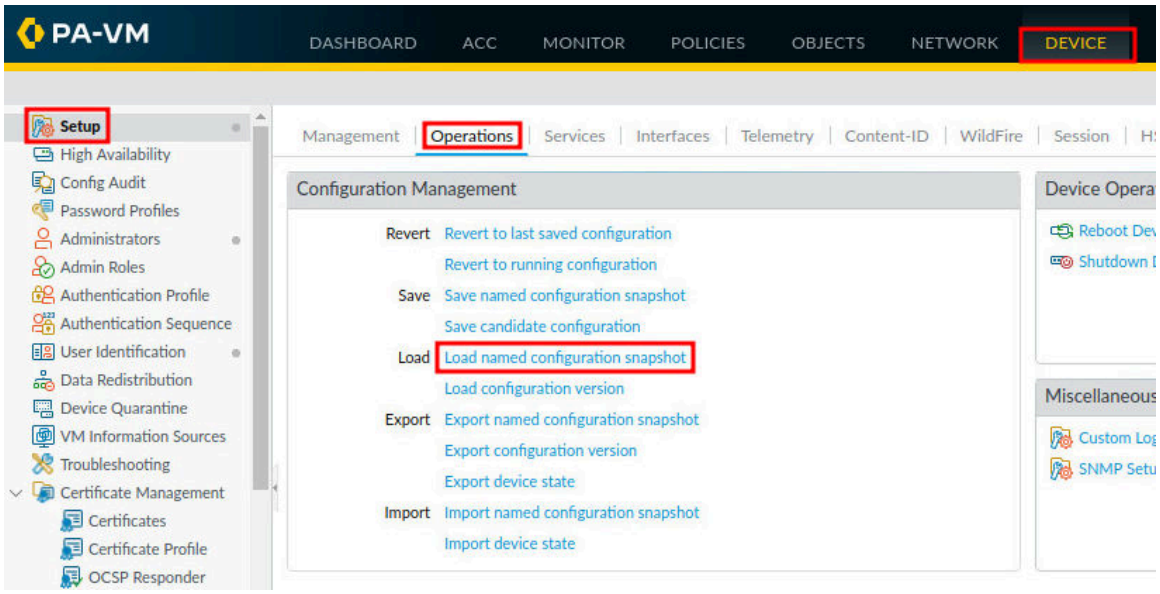
If you experience the "Unable to connect" or "502 Bad Gateway" message while attempting to connect to the specified IP above, please wait an additional 1-3 minutes for the Firewall to fully initialize. Refresh the page to continue.

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

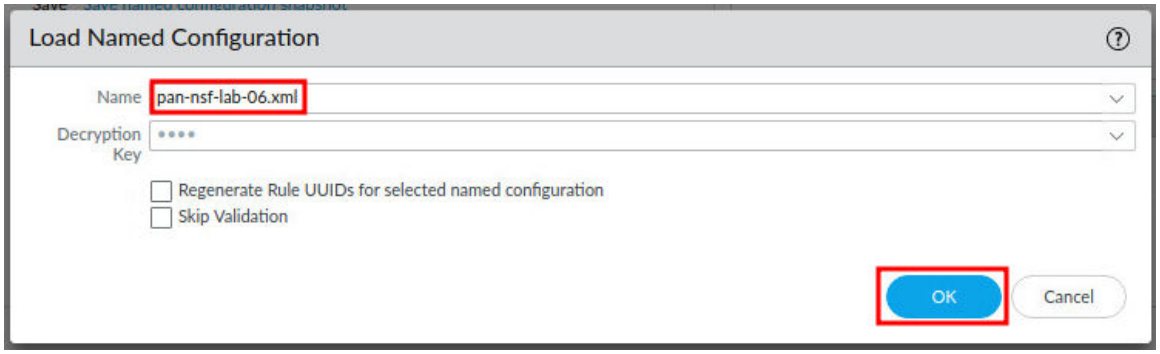


7. Log in to the Firewall web interface as username `admin`, password `Pal0Alt0!`.

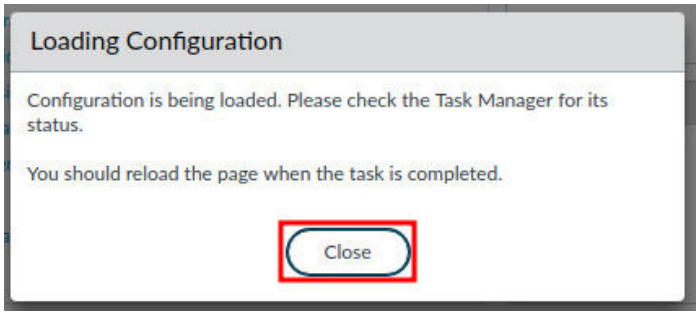
8. In the web interface, navigate to **Device > Setup > Operations** and click on **Load named configuration snapshot** underneath the *Configuration Management* section.



9. In the *Load Named Configuration* window, select **pan-nsf-lab-06.xml** from the *Name* dropdown box and click **OK**.

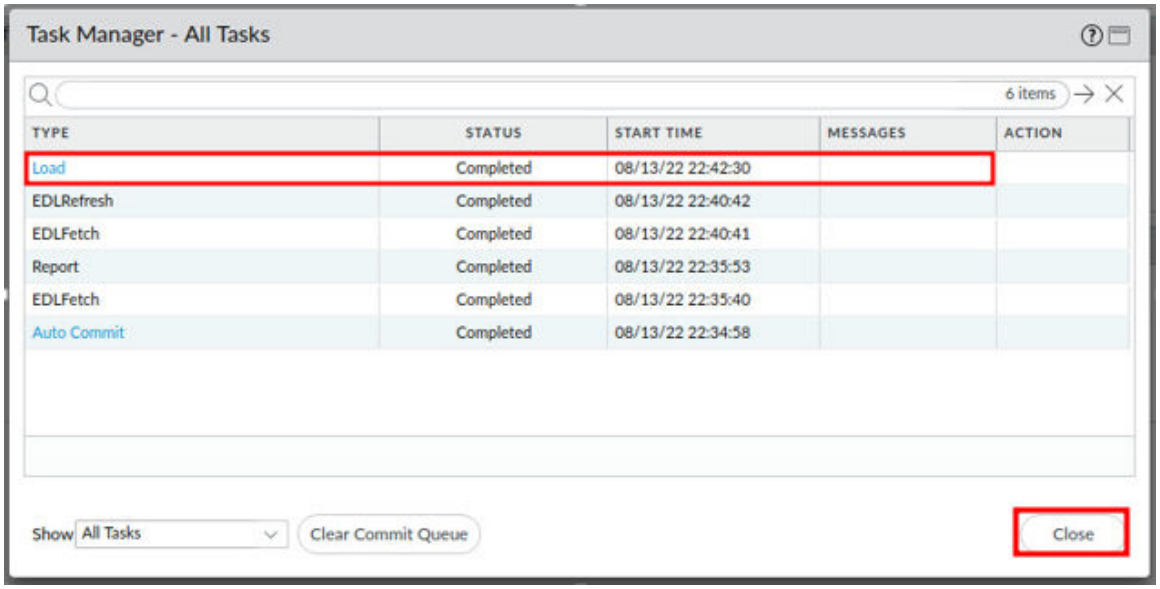


10. In the Loading Configuration window, a message will show *Configuration is being loaded. Please check the Task Manager for its status. You should reload the page when the task is completed.* Click **Close** to continue.

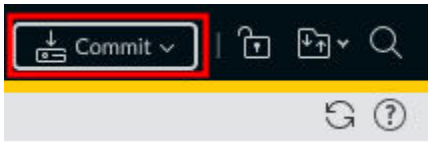


11. Click the **Tasks** icon located at the bottom-right of the web interface.

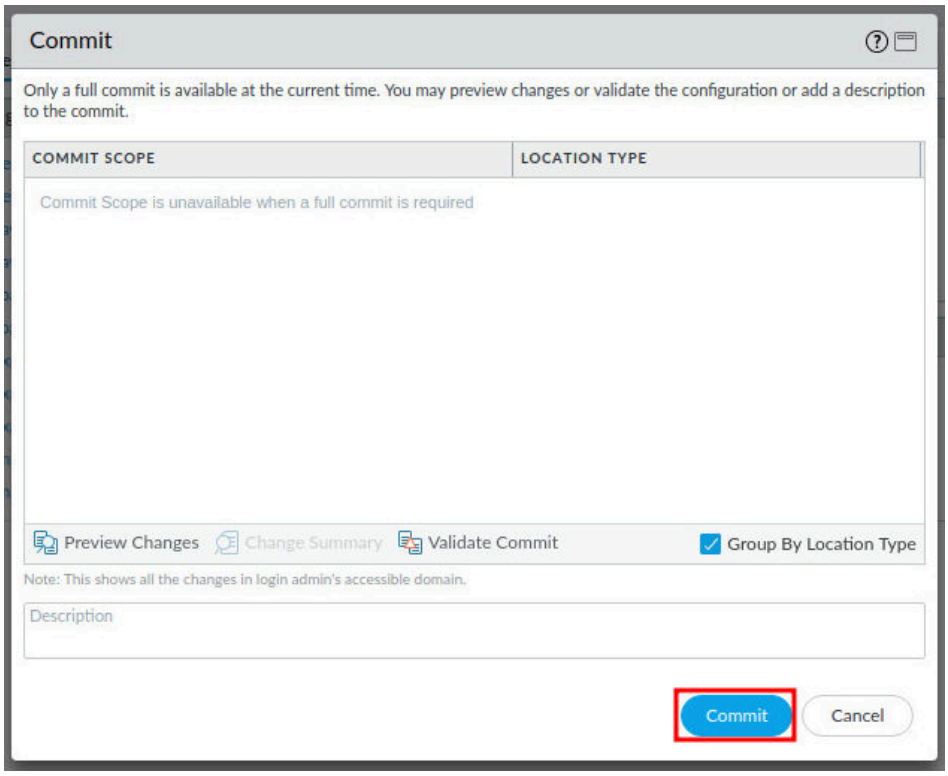
12. In the *Task Manager – All Tasks* window, verify the *Load* type has successfully completed. Click **Close.**



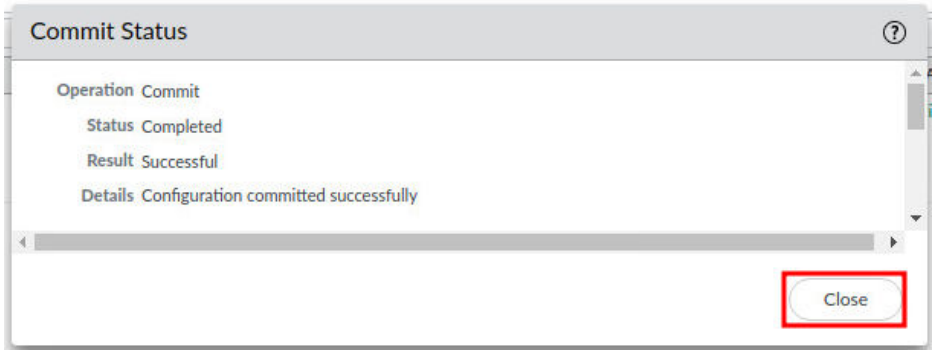
13. Click the **Commit** link located at the top-right of the web interface.



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



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

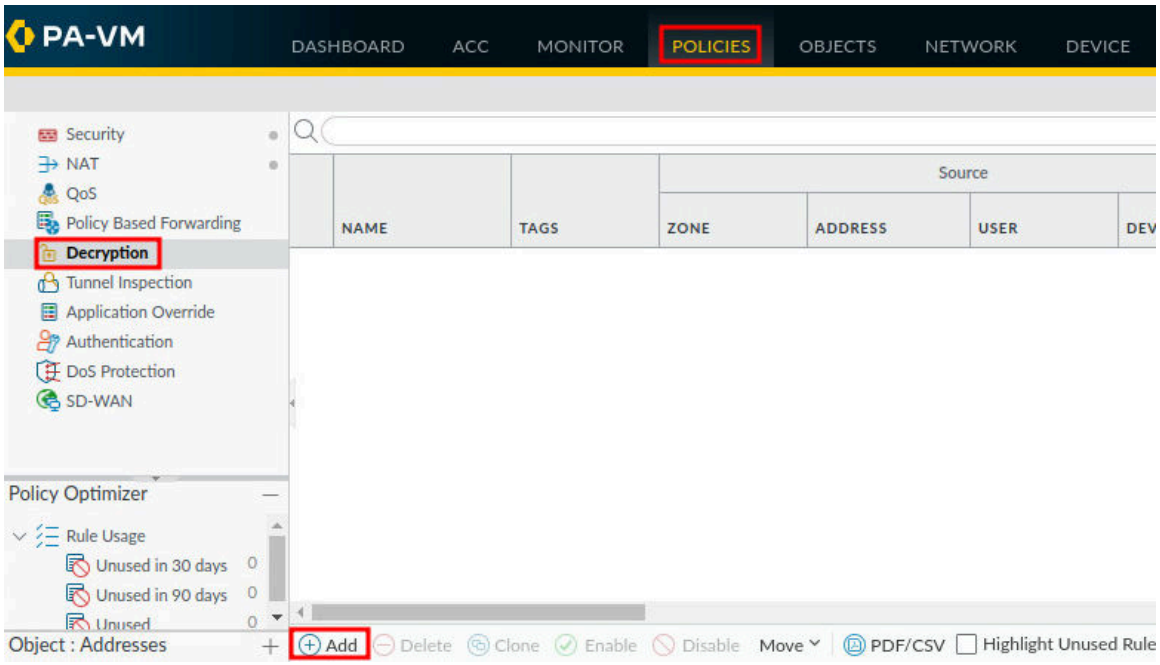


The commit process takes changes made to the Firewall and copies them to the running configuration, which will activate all configuration changes since the last commit.

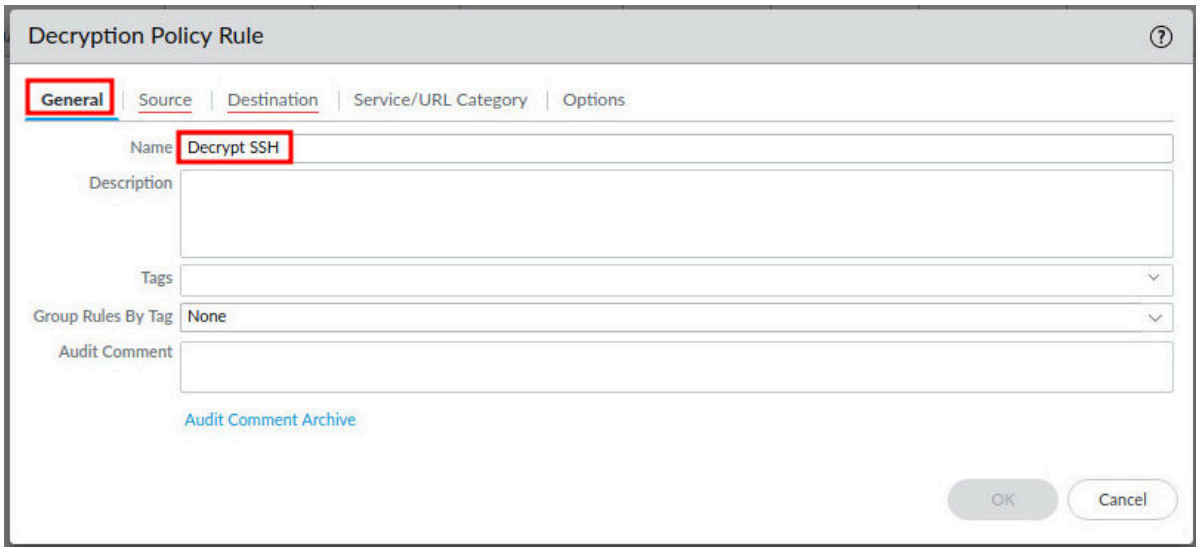
1.1 Create a Decryption Policy and Commit

In this section, you will create a decryption policy. Decryption Policies allow administrators to stop threats that would otherwise remain hidden in encrypted traffic and help prevent sensitive content from leaving an organization. Then, you will commit your changes to the Firewall.

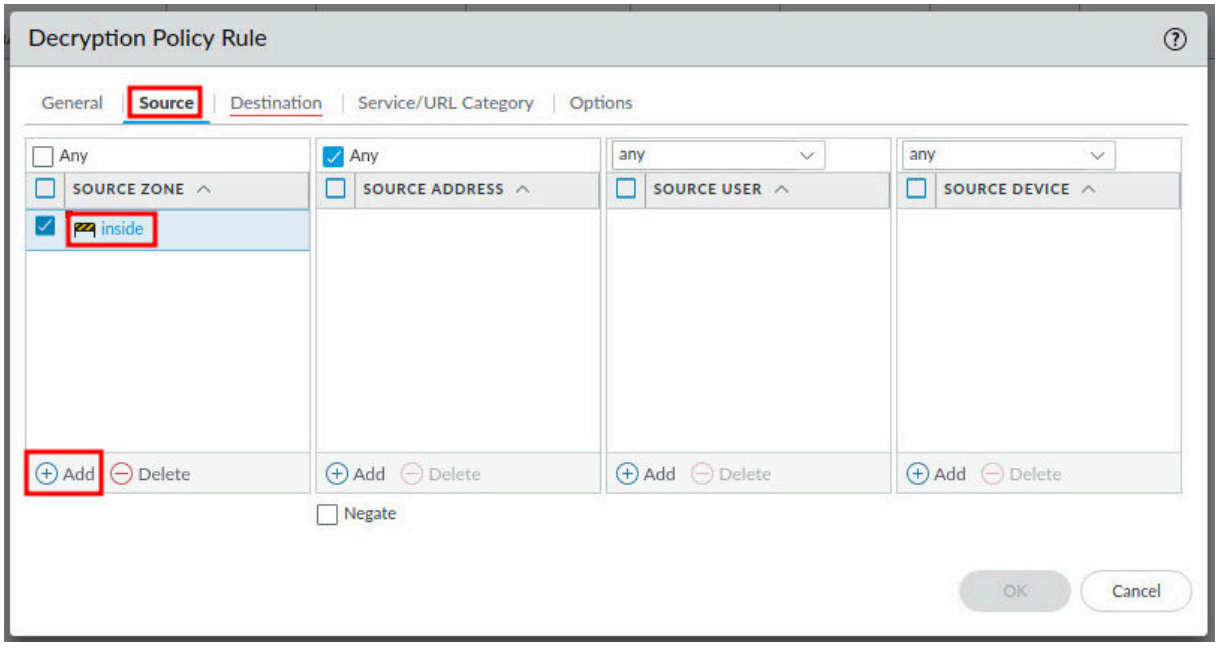
1. Navigate to **Policies** > **Decryption > Add**.



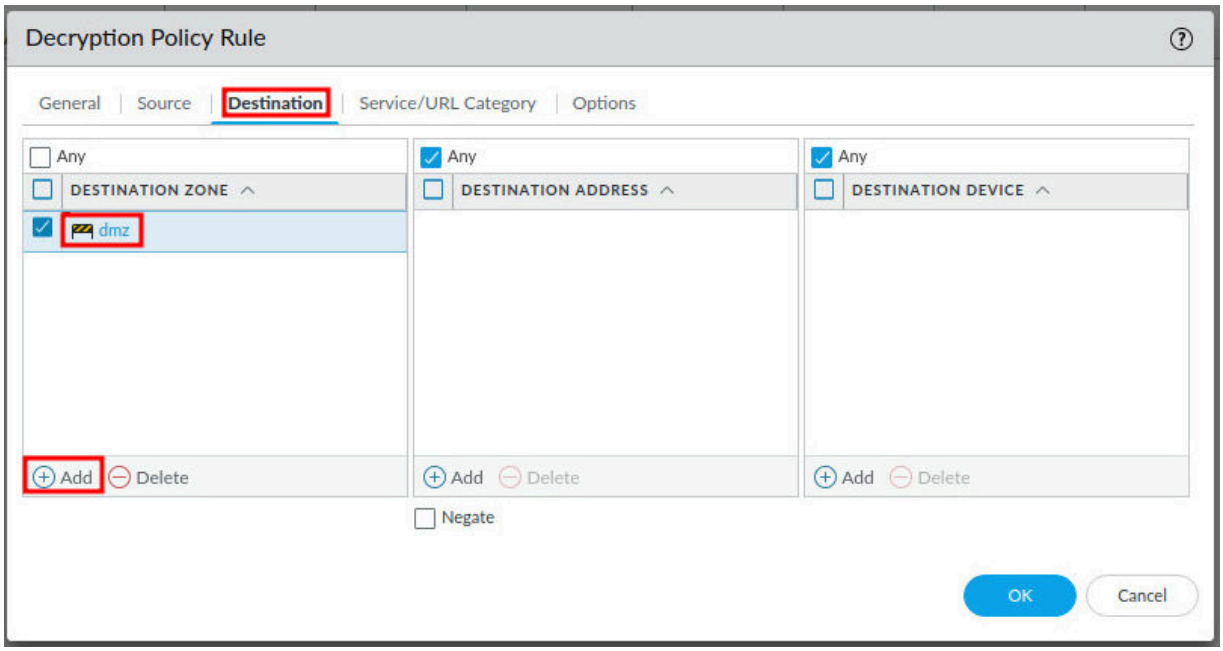
2. In the **General** tab of the *Decryption Policy Rule* window, type `Decrypt SSH` in the *Name* field.



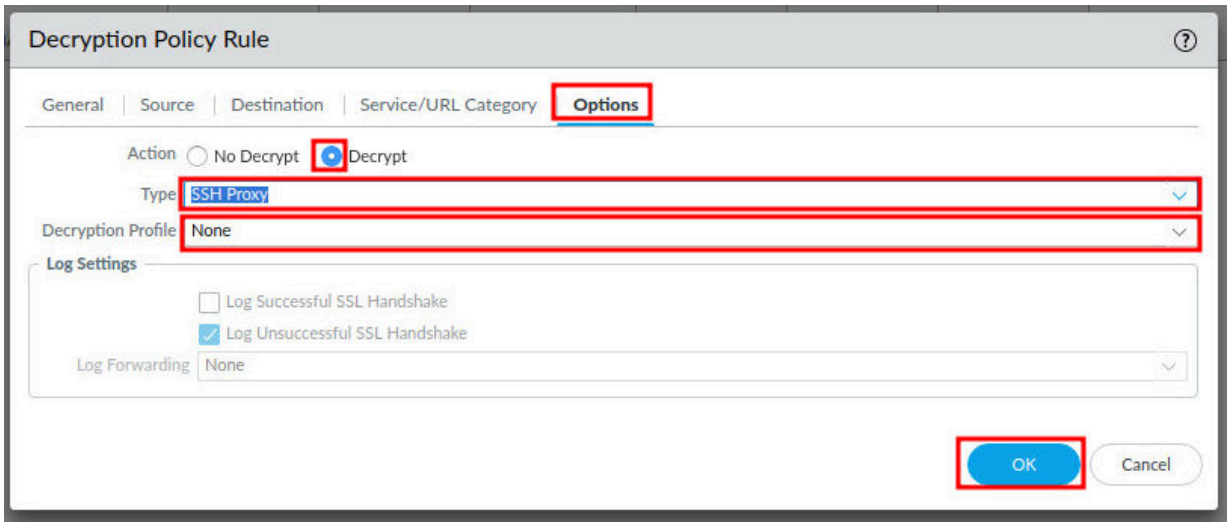
3. In the *Decryption Policy Rule* window, click on the **Source** tab. Then, click **Add** in the *Source Zone* section. Next, select **inside**.



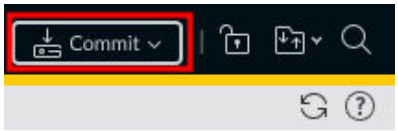
4. In the *Decryption Policy Rule* window, click on the **Destination** tab. Then, click **Add** in the *Destination Zone* section. Next, select **dmz**.



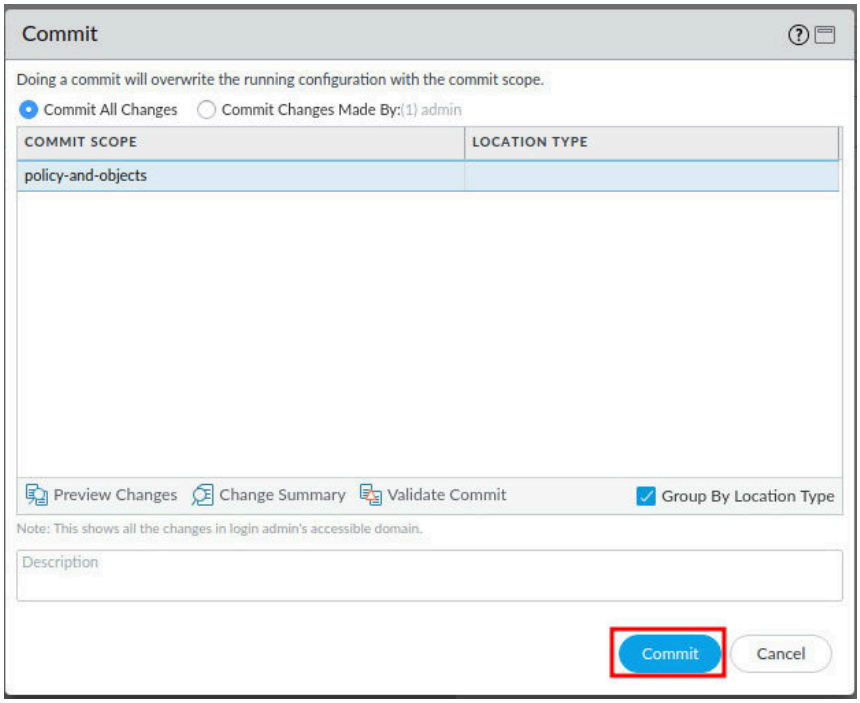
5. In the *Decryption Policy Rule* window, click on the **Options** tab. Then, select **Decrypt** for the *Action*. Next, select **SSH Proxy** in the *Type* dropdown. Then, leave the *Decryption Profile* set to **None**. Finally, click the **OK** button.



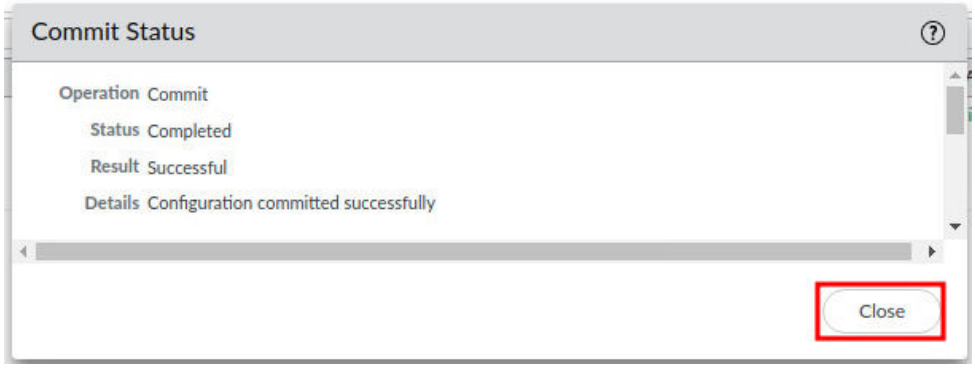
6. Click the **Commit** link located at the top-right of the web interface.



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



8. When the commit operation successfully completes, click **Close** to continue.



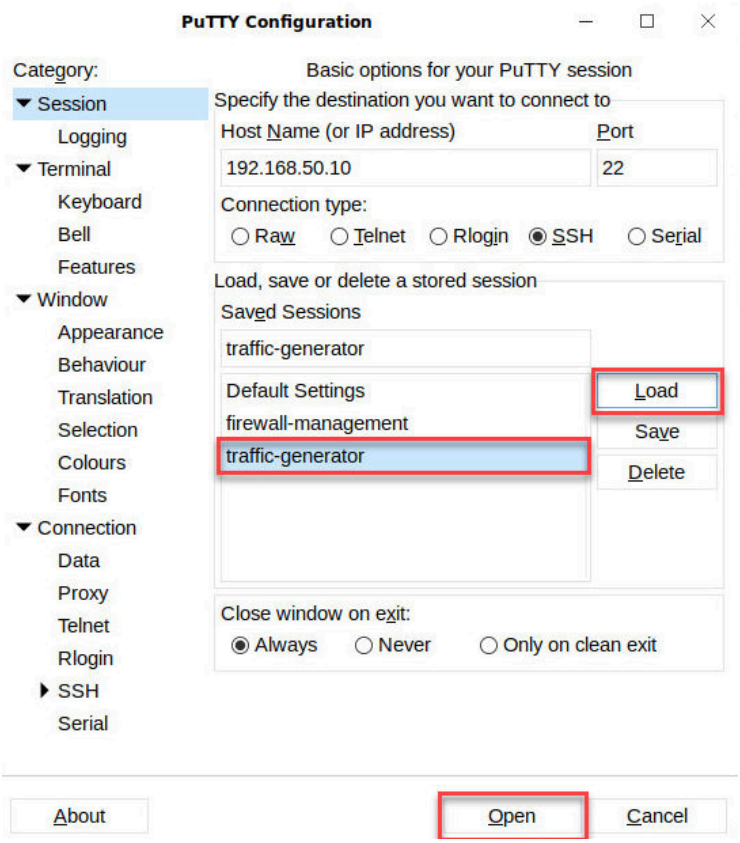
Decryption policies provide flexible rules and matching criteria that enable you to protect destination zones or specific servers that may be prone to DoS attacks.

1.2 Create an SSH Session with PuTTY and Verify Decryption Is Working

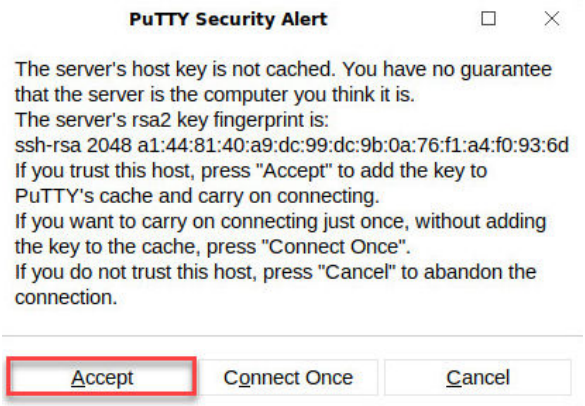
In this section, you will create an SSH session with PuTTY to the DMZ server (traffic-generator), which travels through the internal interface of the Firewall. Then, you will monitor the traffic logs to verify decryption is working.

1. Click the **PuTTY** icon on the taskbar at the bottom of the screen.

2. In the *PuTTY Configuration* window, select **traffic-generator** from the *Saved Sessions* section. Then, click the **Load** button. Finally, click the **Open** button.



3. You may be prompted with a *Putty Security Alert* window. If so, click **Accept** to continue.



4. At the prompt, log in as `root`, type `Pal0Alt0!` as the password, and press **Enter**.

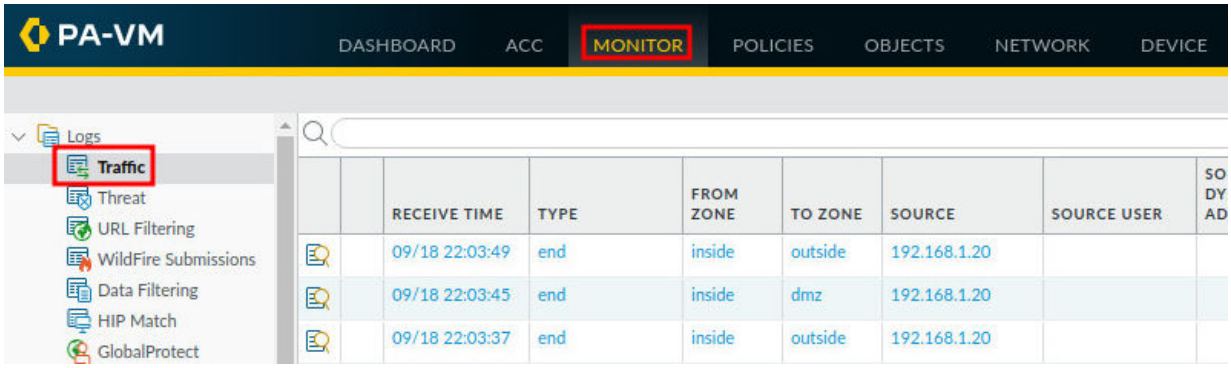
Notice the cursor will not move while you type the password.

5. Once the SSH connection has been made to the DMZ Server, type `exit` and press **Enter** on the keyboard to close the SSH session from the client PC to the DMZ Server.

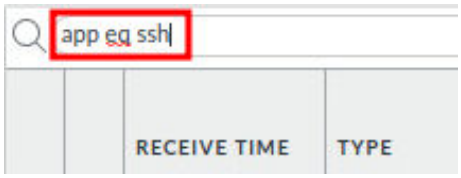
STOP

This will close the SSH session from the Client to the DMZ server. Complete steps 1-5, five times to show multiple SSH connections in the threat logs of the Palo Alto Networks Firewall.

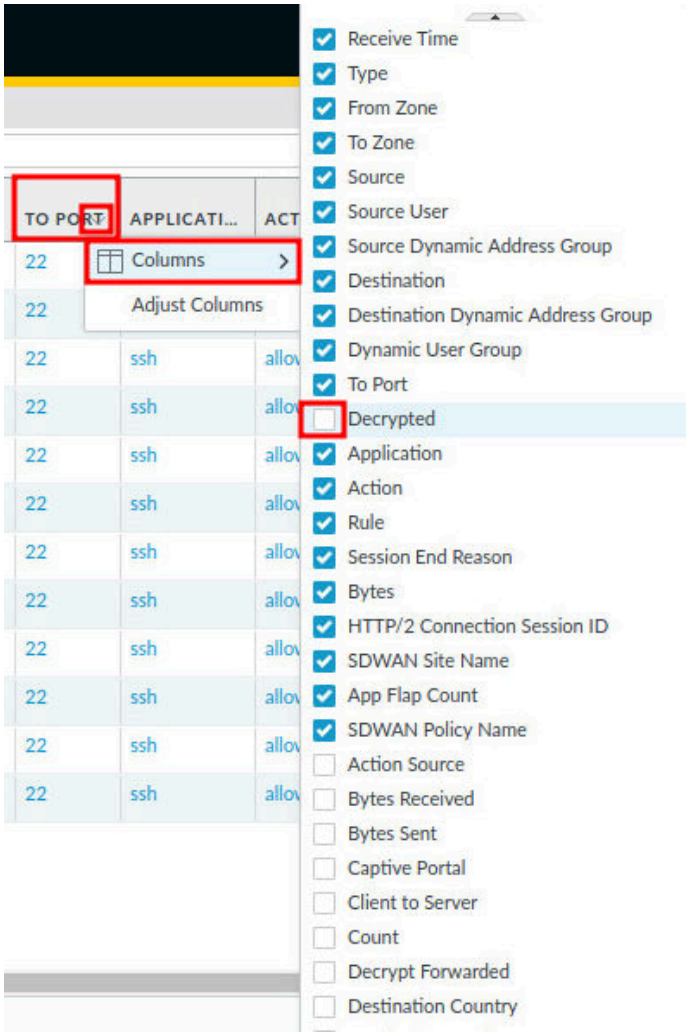
6. Navigate to **Monitor > Logs > Traffic.**



7. In the search bar, type `app eq ssh` and press **Enter.** This will filter only SSH applications.



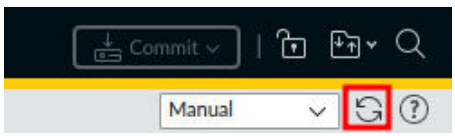
8. Click on the **To Port** column. Then, click on the **arrow** beside the *To Port* column. Next, select **Columns** from the menu. Finally, click to check the **Decrypted** checkbox.



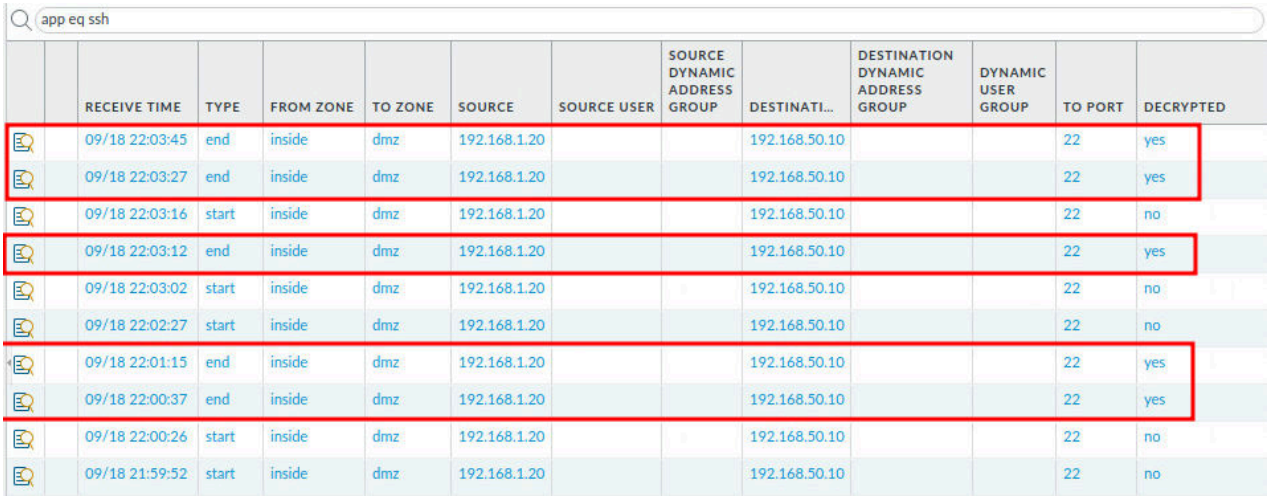
You may need to scroll the window to the right in order to view the column.

The **Decrypted** checkbox might be listed alphabetically among the unchecked boxes in the lower part of the menu

9. Click the **refresh** icon in the upper-right to refresh the traffic logs.



10. View the logs showing the SSH traffic and notice that the traffic was decrypted using the decryption policy created earlier.

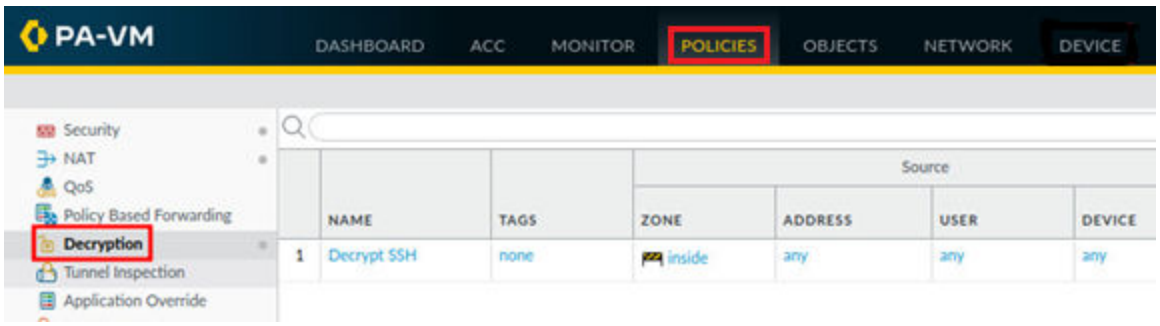


		RECEIVE TIME	TYPE	FROM ZONE	TO ZONE	SOURCE	SOURCE USER	SOURCE DYNAMIC ADDRESS GROUP	DESTINATI...	DESTINATION DYNAMIC ADDRESS GROUP	DYNAMIC USER GROUP	TO PORT	DECRYPTED
		09/18 22:03:45	end	inside	dmz	192.168.1.20			192.168.50.10			22	yes
		09/18 22:03:27	end	inside	dmz	192.168.1.20			192.168.50.10			22	yes
		09/18 22:03:16	start	inside	dmz	192.168.1.20			192.168.50.10			22	no
		09/18 22:03:12	end	inside	dmz	192.168.1.20			192.168.50.10			22	yes
		09/18 22:03:02	start	inside	dmz	192.168.1.20			192.168.50.10			22	no
		09/18 22:02:27	start	inside	dmz	192.168.1.20			192.168.50.10			22	no
		09/18 22:01:15	end	inside	dmz	192.168.1.20			192.168.50.10			22	yes
		09/18 22:00:37	end	inside	dmz	192.168.1.20			192.168.50.10			22	yes
		09/18 22:00:26	start	inside	dmz	192.168.1.20			192.168.50.10			22	no
		09/18 21:59:52	start	inside	dmz	192.168.1.20			192.168.50.10			22	no

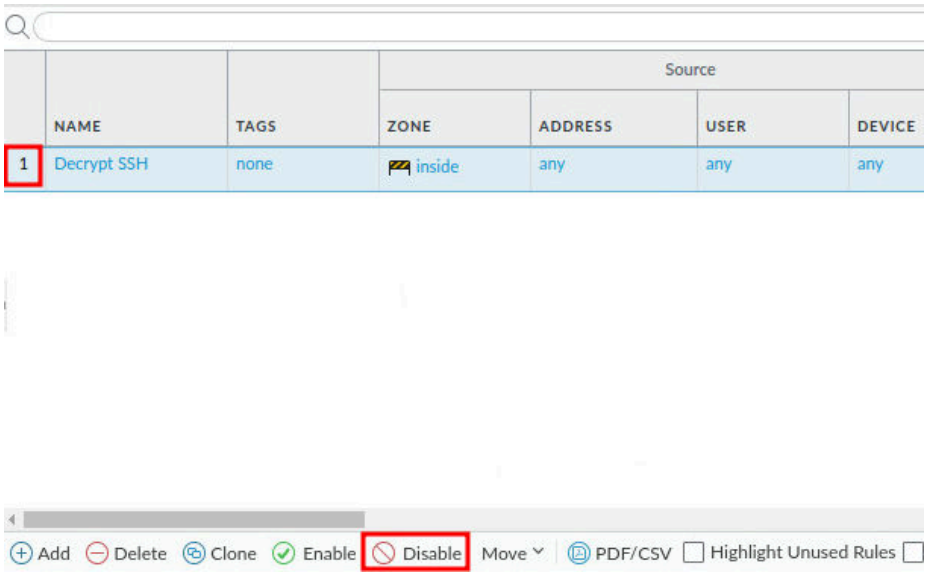
1.3 Disable the Decryption Policy

In this section, you will disable the decryption policy that was created earlier and verify the Firewall is no longer decrypting the SSH traffic.

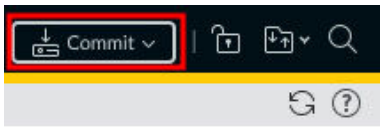
1. Navigate to **Policies > Decryption.**



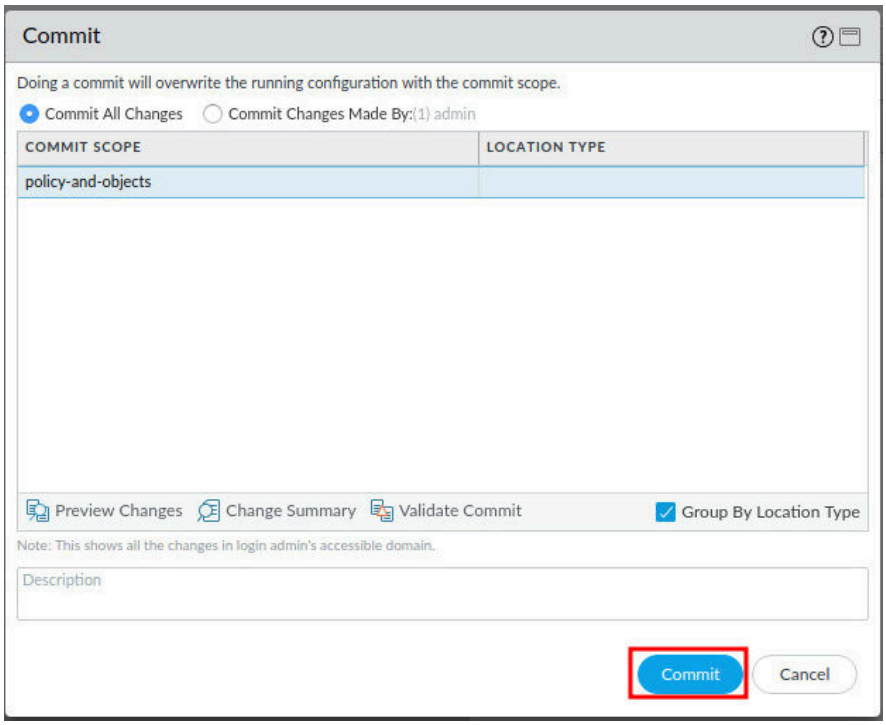
2. Click the **1**, to select the **Decrypt SSH** policy created. Then, click **Disable** at the bottom.



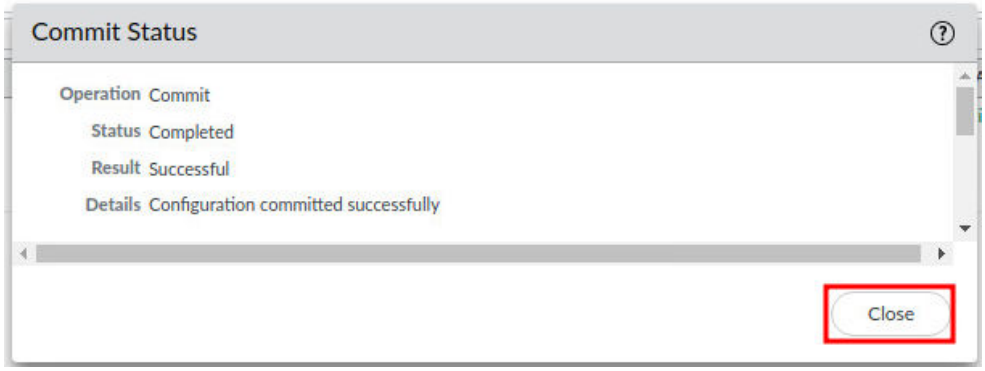
3. Click the **Commit** link located at the top-right of the web interface.



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

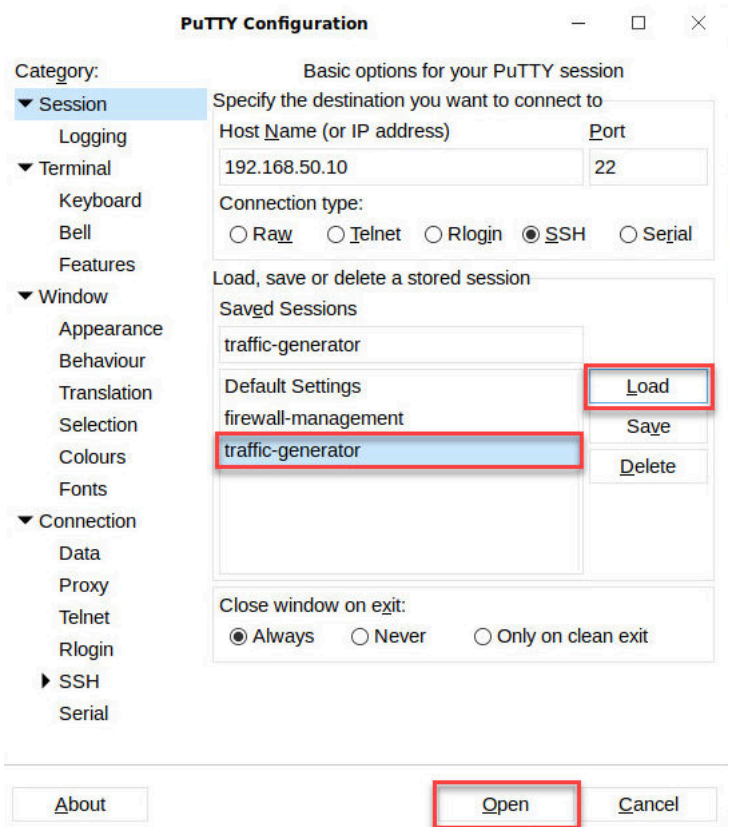


5. When the commit operation successfully completes, click **Close** to continue.



6. Click the **PuTTY** icon on the taskbar at the bottom of the screen.

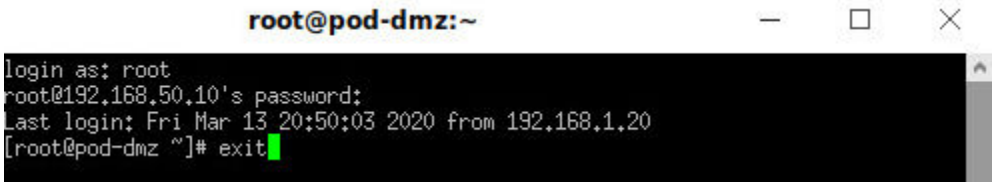
7. In the *PuTTY Configuration* window, select **traffic-generator** from the *Saved Sessions* section. Then, click the **Load** button. Finally, click the **Open** button.



8. At the prompt, log in as `root`, type `Pal0Alt0!` as the password, and press **Enter**.

Notice the cursor will not move while you type the password.

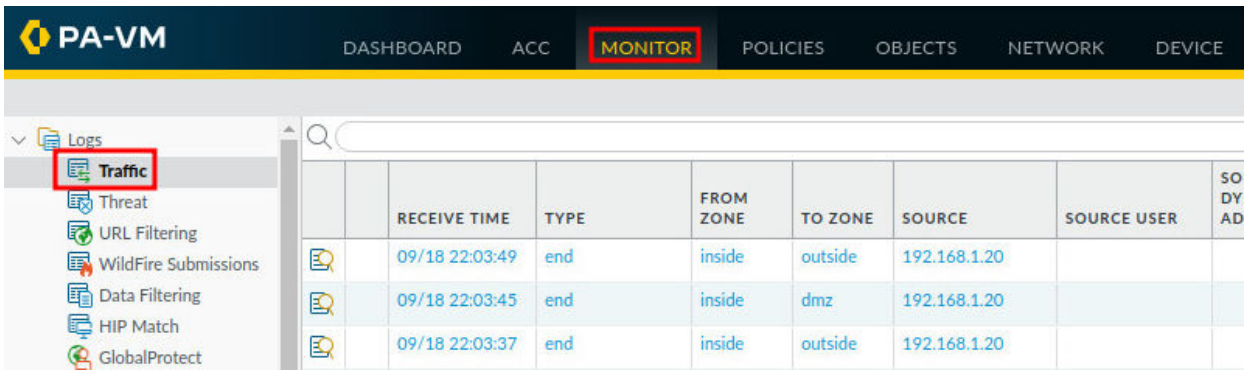
9. Once the SSH connection has been made to the DMZ Server, type `exit` and press **Enter** on the keyboard to close the SSH session from the client PC to the DMZ Server.



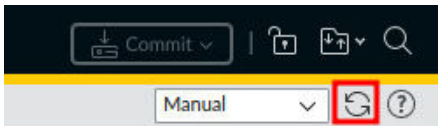
This will close the SSH session from the Client to the DMZ server. Complete steps 6-9, five times to show multiple SSH connections in the threat logs of the Palo Alto Networks Firewall.

10. Click on the **Chromium** icon from the taskbar to maximize.

11. Navigate to **Monitor > Logs > Traffic.**



12. Click the **refresh** icon in the upper-right to refresh the traffic logs.



13. View the logs showing the SSH traffic and notice that the traffic was not decrypted due to disabling the Decryption Policy.

app eq ssh

		RECEIVE TIME	TYPE	FROM ZONE	TO ZONE	SOURCE	SOURCE USER	SOURCE DYNAMIC ADDRESS GROUP	DESTINATI...	DESTINATION DYNAMIC ADDRESS GROUP	DYNAMIC USER GROUP	TO PORT	DECRYPTED
		09/18 22:38:56	end	inside	dmz	192.168.1.20			192.168.50.10			22	no
		09/18 22:38:43	end	inside	dmz	192.168.1.20			192.168.50.10			22	no
		09/18 22:38:34	start	inside	dmz	192.168.1.20			192.168.50.10			22	no
		09/18 22:38:30	end	inside	dmz	192.168.1.20			192.168.50.10			22	no
		09/18 22:38:21	start	inside	dmz	192.168.1.20			192.168.50.10			22	no
		09/18 22:38:18	end	inside	dmz	192.168.1.20			192.168.50.10			22	no
		09/18 22:38:07	start	inside	dmz	192.168.1.20			192.168.50.10			22	no
		09/18 22:38:06	end	inside	dmz	192.168.1.20			192.168.50.10			22	no
		09/18 22:37:56	start	inside	dmz	192.168.1.20			192.168.50.10			22	no
		09/18 22:37:43	start	inside	dmz	192.168.1.20			192.168.50.10			22	no

14. The lab is now complete; you may end the reservation.

