NETWORK SECURITY FUNDAMENTALS V2

Lab 7: Decrypting SSL Inbound Traffic

Document Version: 2022-12-23

Contents

Introduction

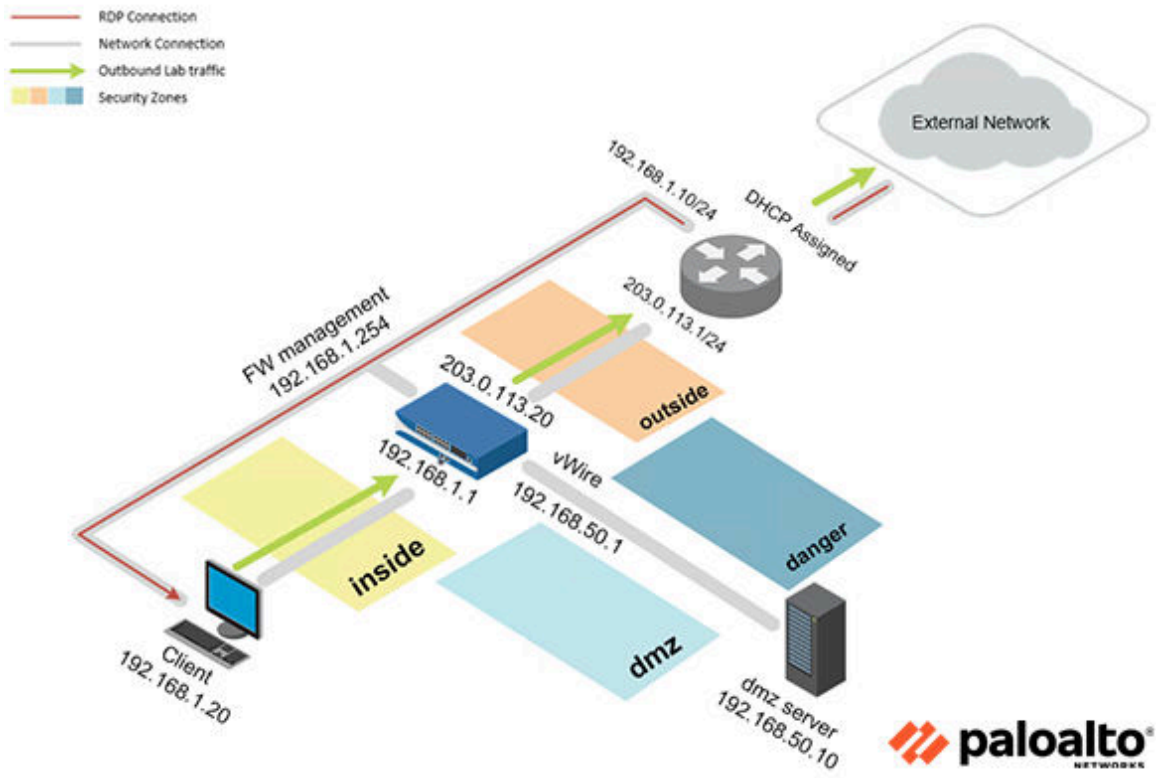
In this lab, you will decrypt SSL inbound traffic and inspect SSL traffic from the Client machine to the DMZ server. When the SSL server certificate is loaded on the Firewall, and an SSL decryption policy is configured for the inbound traffic, the device can then decrypt and read the traffic as it forwards it along. No changes are made to the packet data, and the secure channel is built from the client system to the internal server. The Firewall can then detect malicious content and control applications running over this secure channel.

Objective

In this lab, you will perform the following tasks:

- Download the SSL Certificate from DMZ Server
- Import SSL Certificate
- Create a Decryption Profile
- Create a Decryption Policy
- Commit and Test Decryption Policy
- 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.

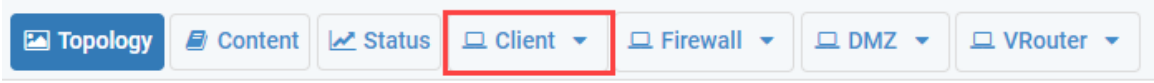
Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Client	192.168.1.20	`lab-user`	`Pal0Alt0!`
DMZ	192.168.50.10	`root`	`Pal0Alt0!`
Firewall	192.168.1.254	`admin`	`Pal0Alt0!`

1 Decrypting SSL Inbound Traffic

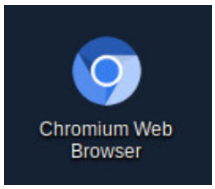
1.0 Load Lab Configuration

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

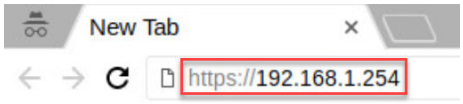
1. Click on the **Client** tab to access the Client PC.



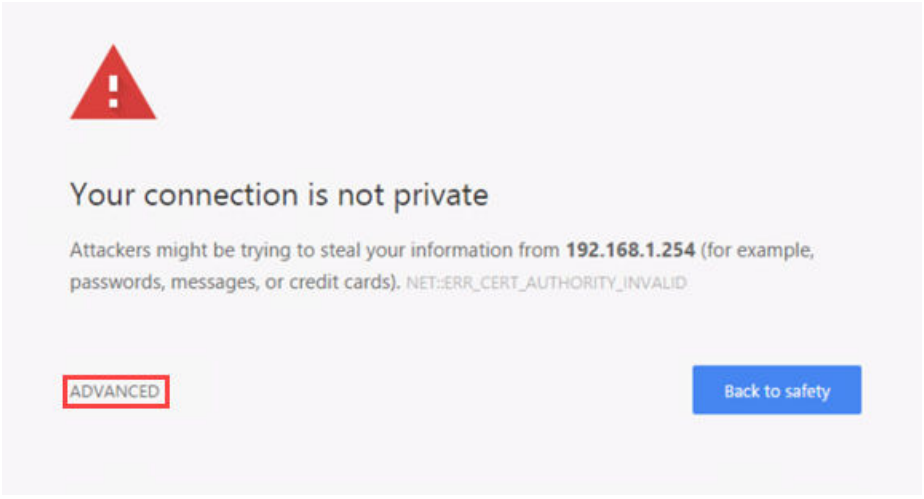
2. Log in to the Client PC as username `lab-user`, password `Pal0Alt0!`.
3. Double-click the **Chromium Web Browser** icon located on the desktop.



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

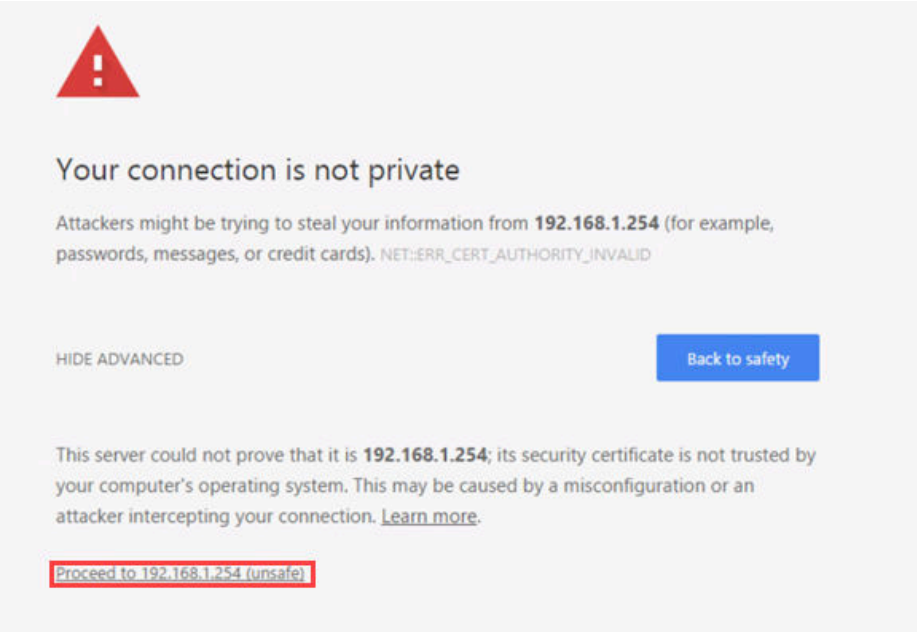


5. You will see a "*Your connection is not private*" message. Click on the **ADVANCED** link.



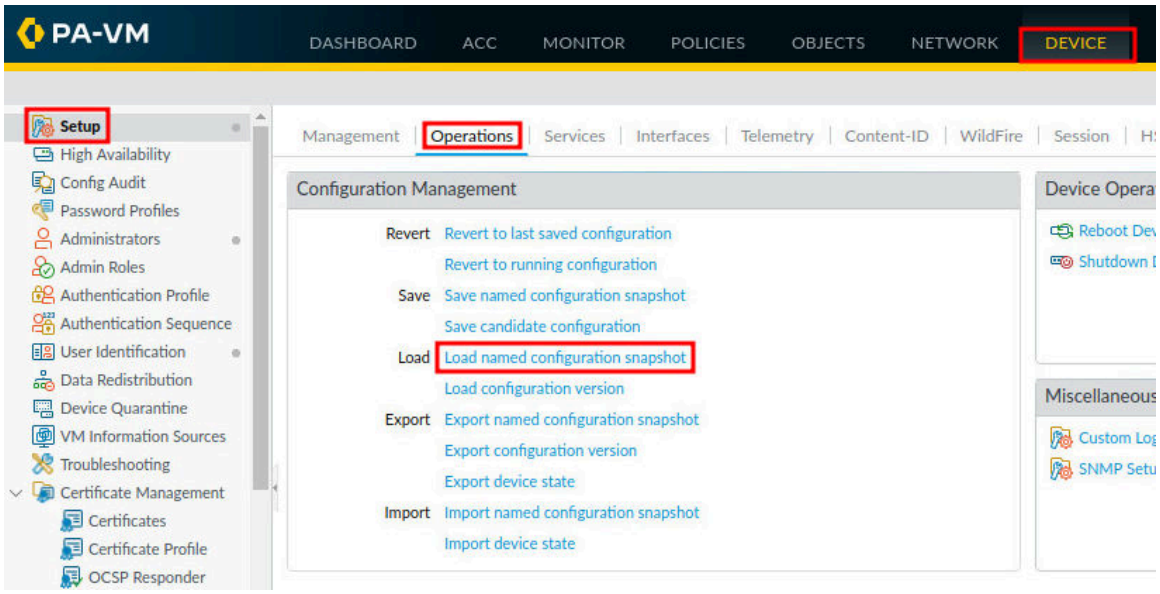
If you experience the "Unable to connect" or "502 Bad Gateway" message while attempting to connect to the specified IP above, please wait an additional 1-3 minutes for the Firewall to fully initialize. Refresh the page to continue.

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

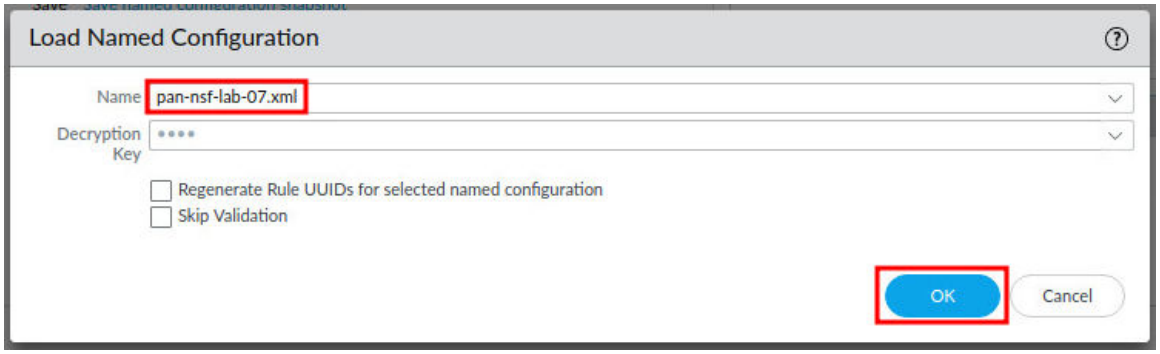


7. Log in to the Firewall web interface as username `admin`, password `Pal0Alt0!`.

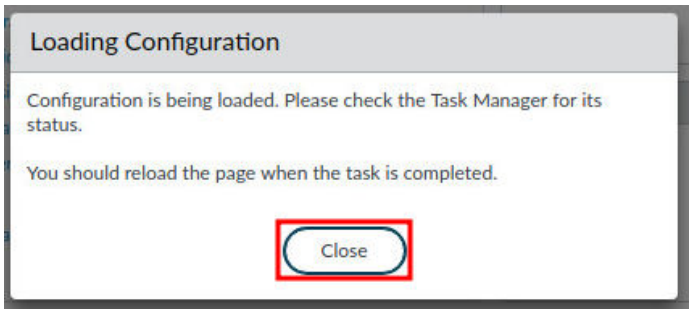
8. In the web interface, navigate to **Device > Setup > Operations** and click on **Load named configuration snapshot** underneath the *Configuration Management* section.



9. In the *Load Named Configuration* window, select **pan-nsf-lab-07.xml** from the *Name* dropdown box and click **OK**.

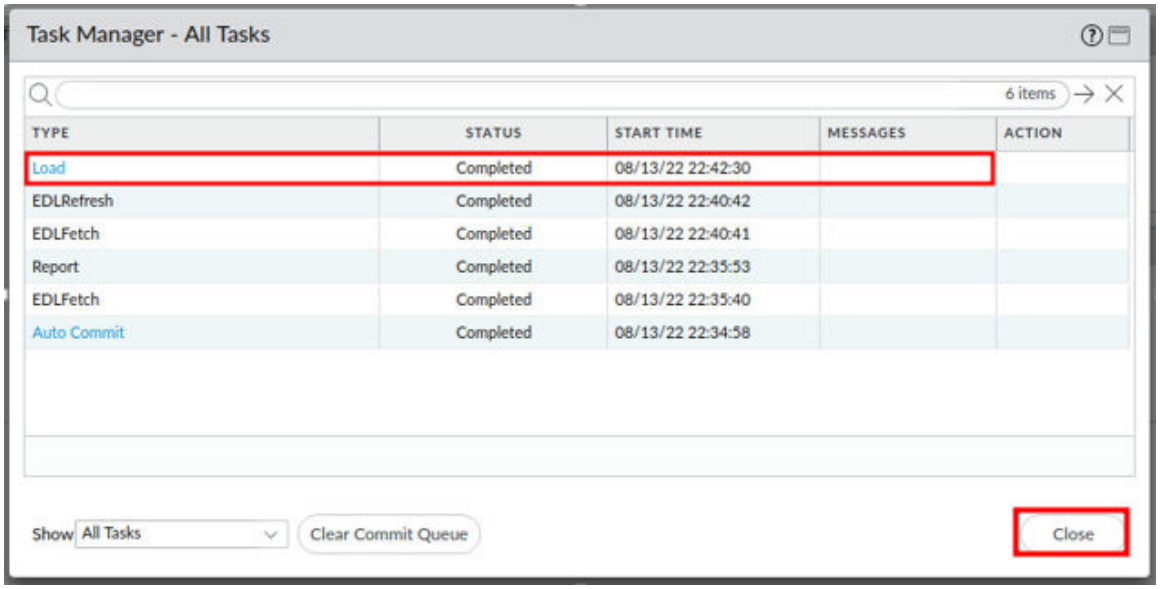


10. In the Loading Configuration window, a message will show *Configuration is being loaded. Please check the Task Manager for its status. You should reload the page when the task is completed.* Click **Close** to continue.

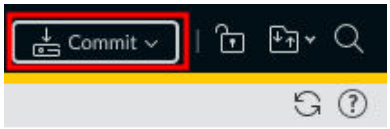


11. Click the **Tasks** icon located at the bottom-right of the web interface.

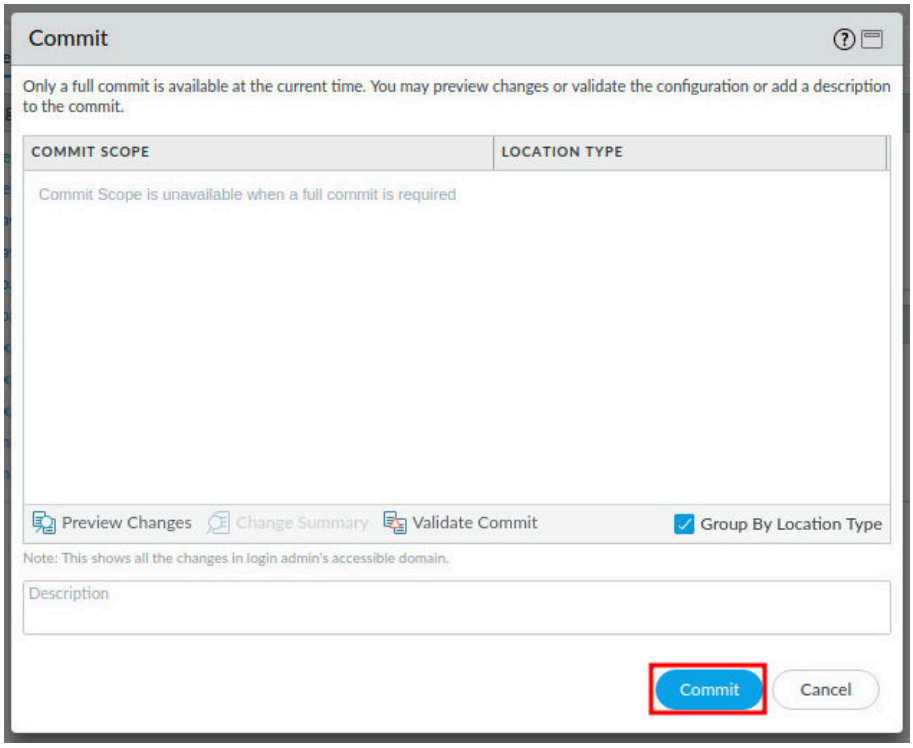
12. In the *Task Manager – All Tasks* window, verify the *Load* type has successfully completed. Click **Close.**



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.

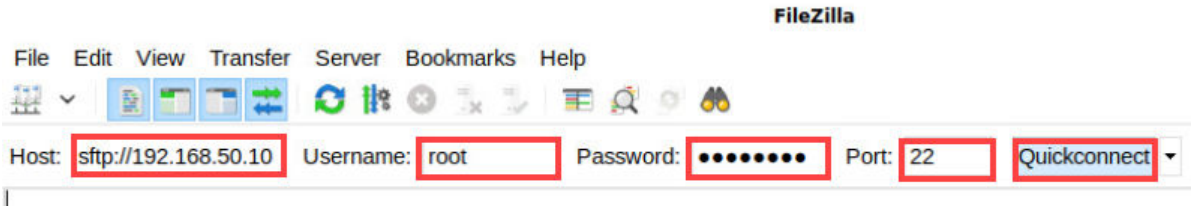
1.1 Download the SSL Certificate from DMZ Server

In this section, you will use WinSCP to download the certificate and key that is being used on the DMZ server. WinSCP is a free, open-source tool used to transfer secure files between clients.

1. Minimize **Chromium** in the upper-right.

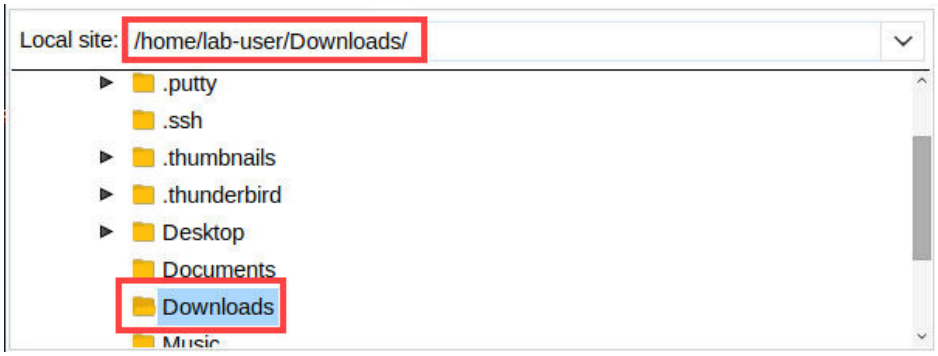
2. Double-click the **Filezilla** icon located on the desktop.

3. In the *FileZilla* window, type `sftp://192.168.50.10` for the *Host*, type `root` for the *Username*, type `Pal0Alt0!` for the *Password*, lastly, type `22` for the *Port*. Then, click the **Quickconnect** button.

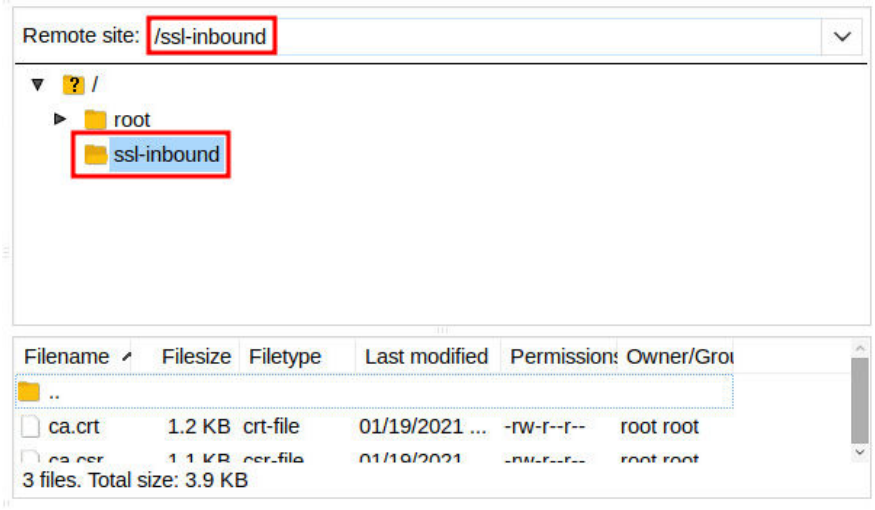


You may be prompted to remember the password after connecting to sftp://192.168.50.10. It is strongly recommended to not save passwords automatically as this could lead to insecure accounts and networks. If prompted to save the password, select **Do not save passwords** and select **OK**.

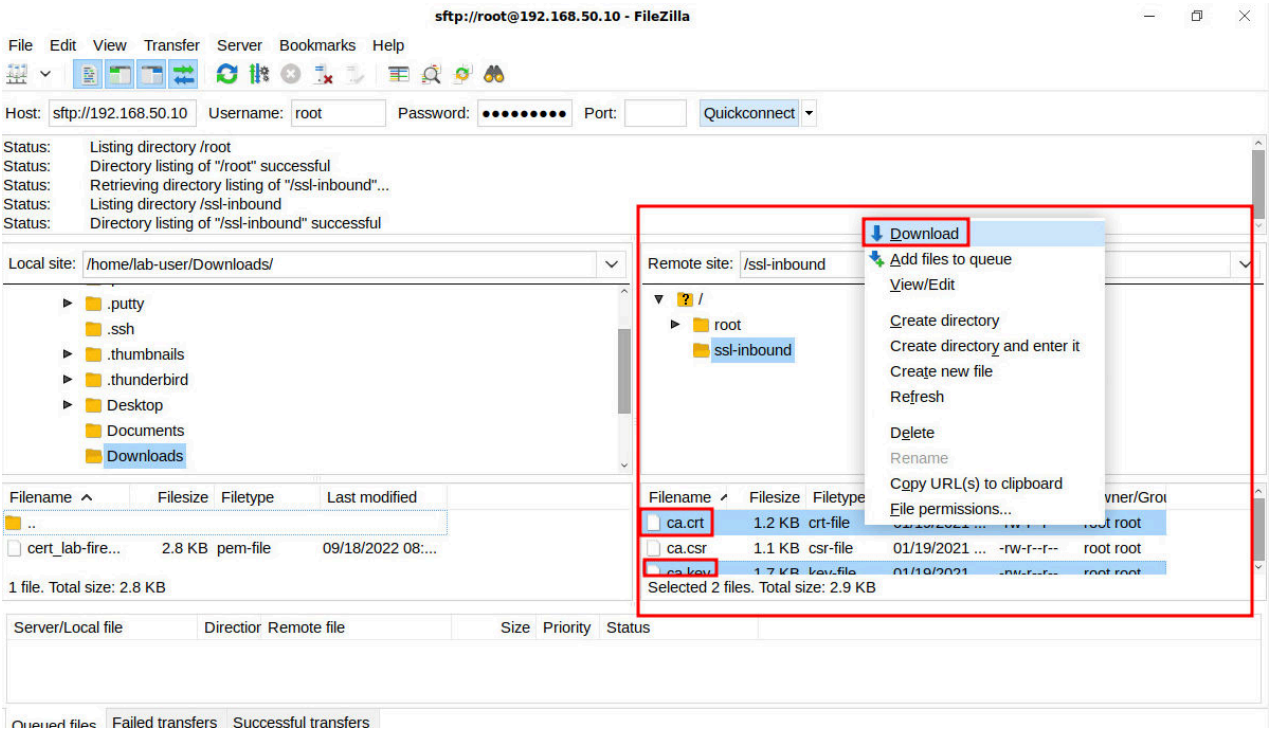
4. On the Local site, type `/home/lab-user/Downloads` in the text field. Press **Enter**.



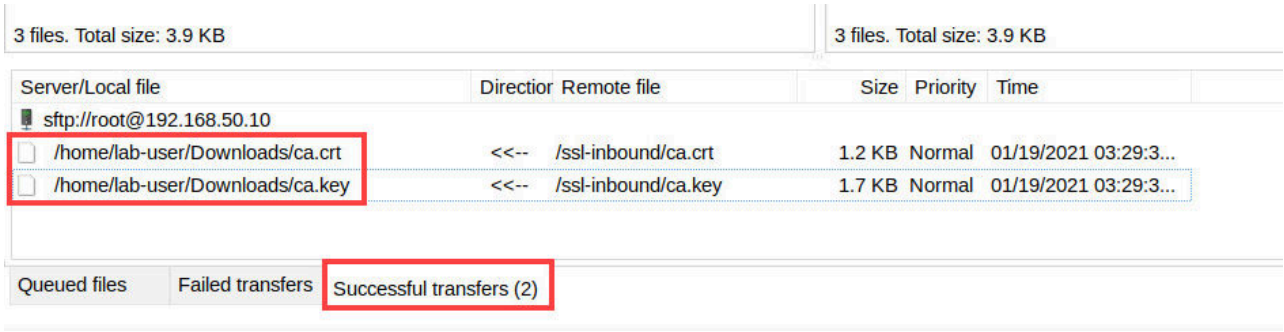
5. On the Remote site, type `/ssl-inbound` in the text field. Press **Enter**.



6. Press **CTRL** and **click** to highlight the filenames **ca.key** and **ca.crt**. Right-click the files and click **Download**.



7. Click on the **Successful transfers** tab and verify the transfers were successfully downloaded.

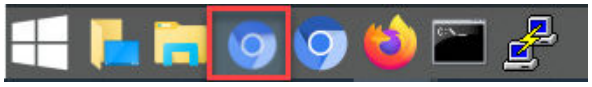


8. Click the **X** in the upper-right to close *FileZilla*.

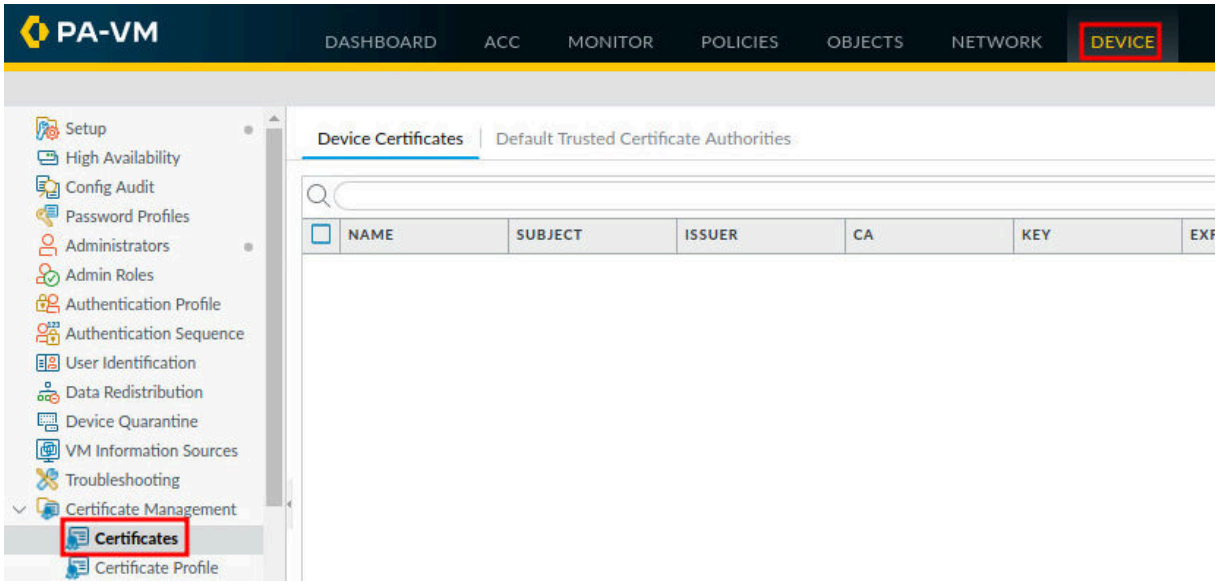
1.2 Import SSL Certificate

In this section, you will import the SSL Certificate you downloaded from the DMZ server to the Firewall. This will later be used to create a decryption profile.

1. Click on the **Chromium** icon from the taskbar to maximize the Firewall management interface.

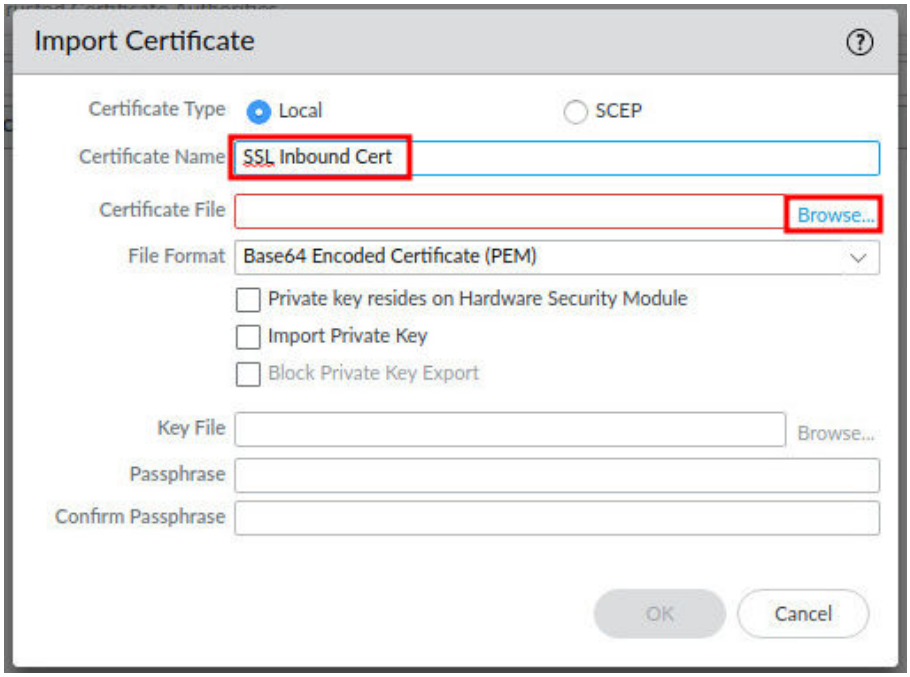


2. Navigate to **Device > Certificate Management > Certificates**.

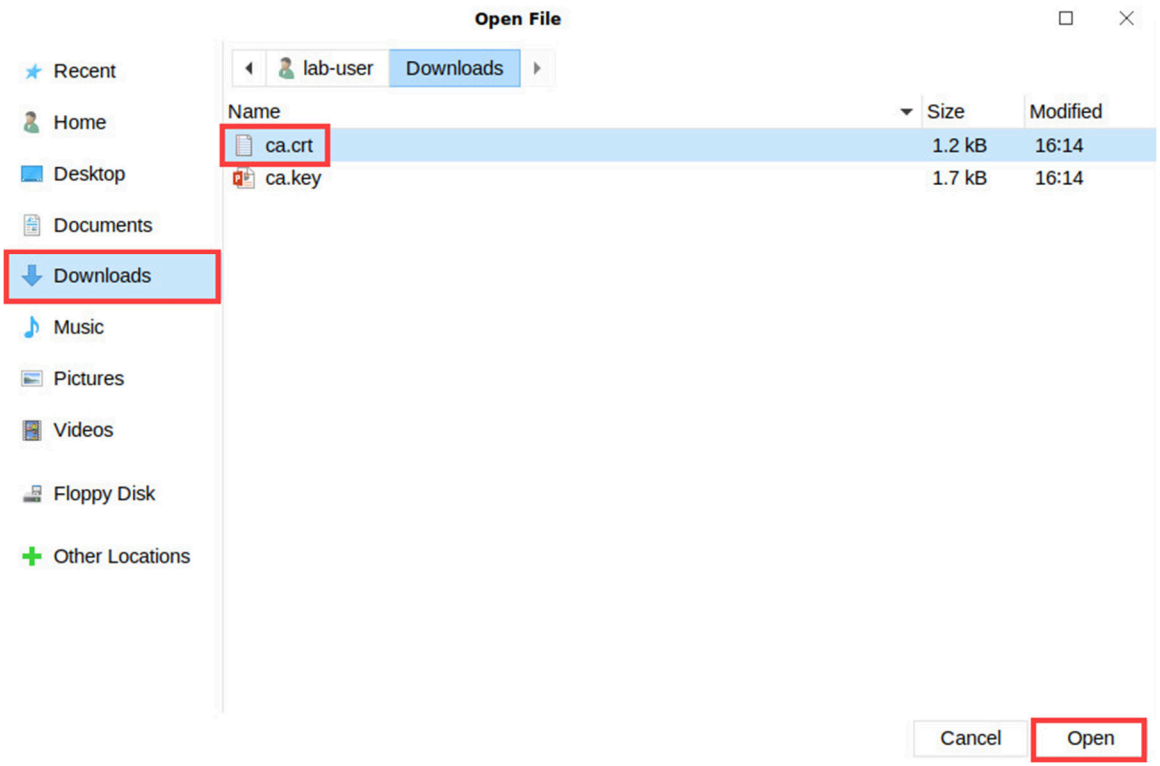


3. Click on the **Import** button at the bottom-center of the center section.

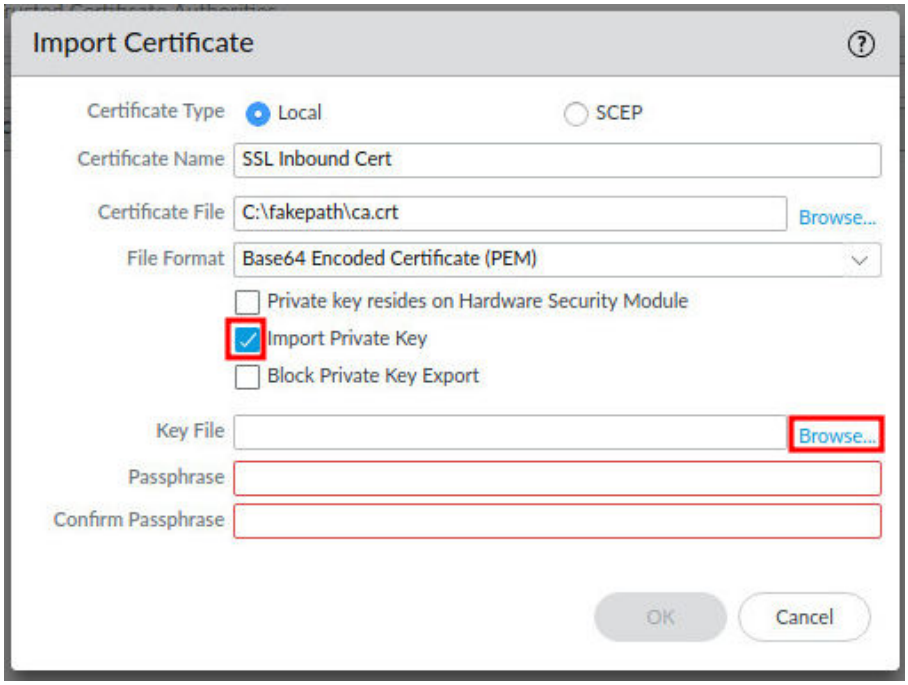
4. In the *Import Certificate* window, type `SSL Inbound Cert`. Then, click **Browse…**



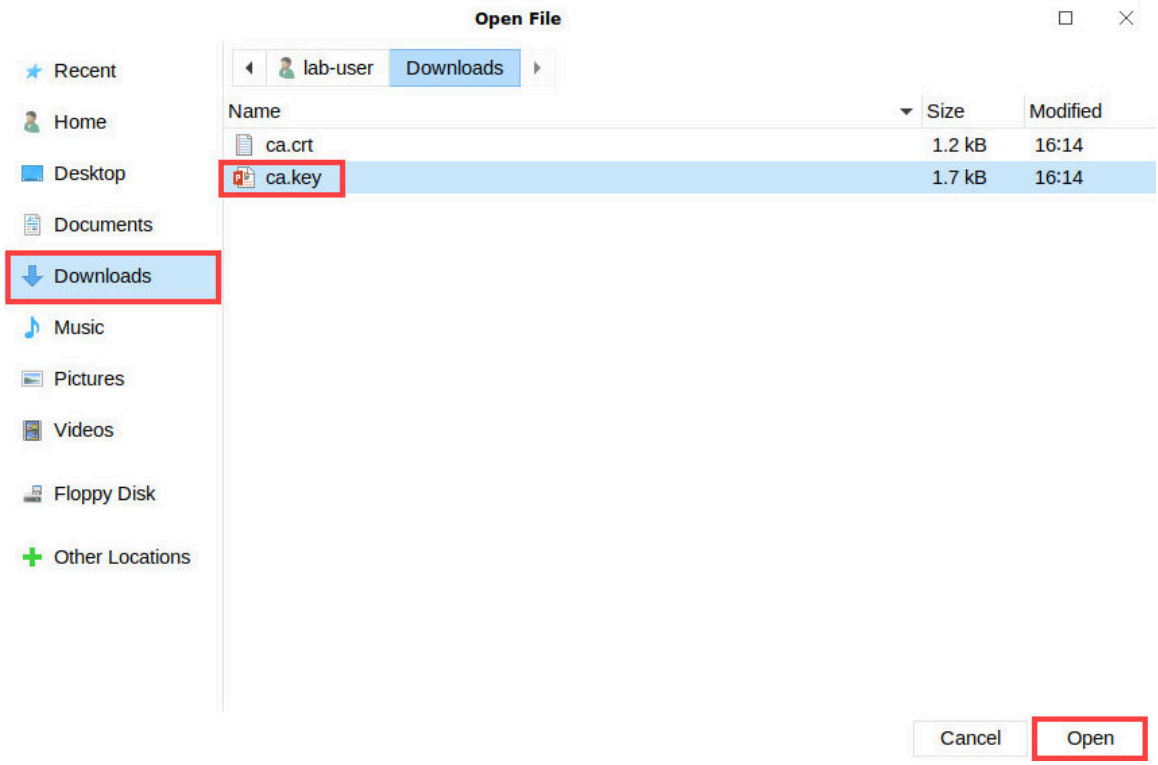
5. In the *Open File* window, select **Downloads** on the left. Then, select **ca.crt**. Finally, click the **Open** button.



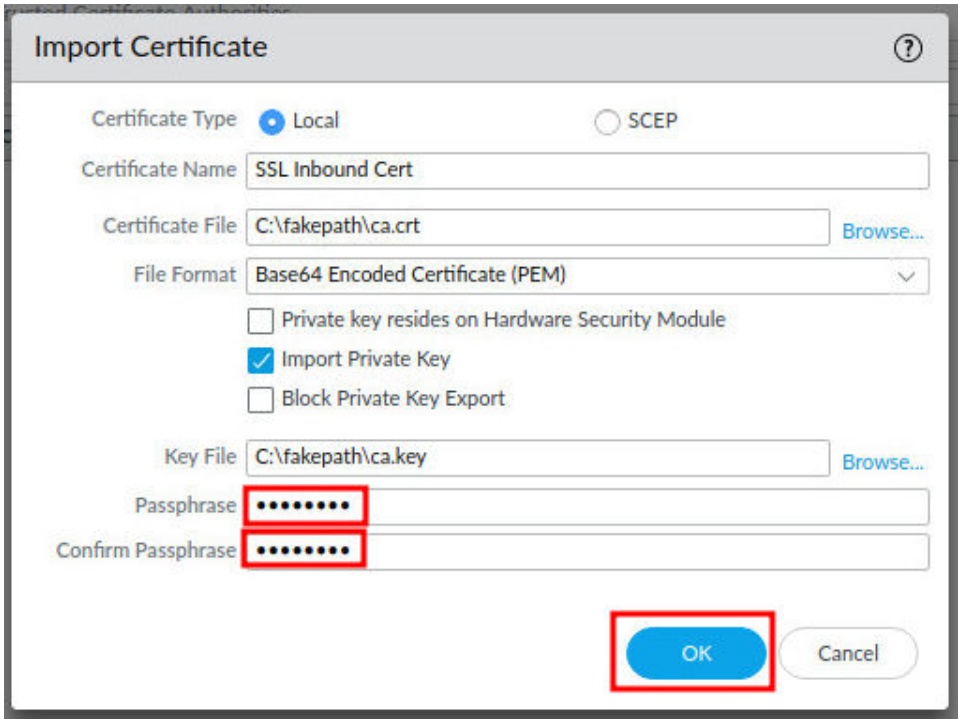
6. Click the checkbox for **Import private key**. Then, click **Browse…**



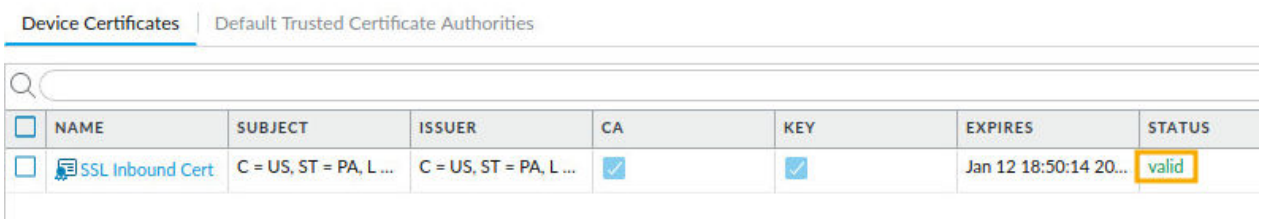
7. In the *Open* File window, select **Downloads** on the left. Then, select **ca.key**. Finally, click the **Open** button.



8. In the *Import Certificate* window, type `paloalto` for the *Passphrase* and *Confirm Passphrase* fields. Then, click the **OK** button.



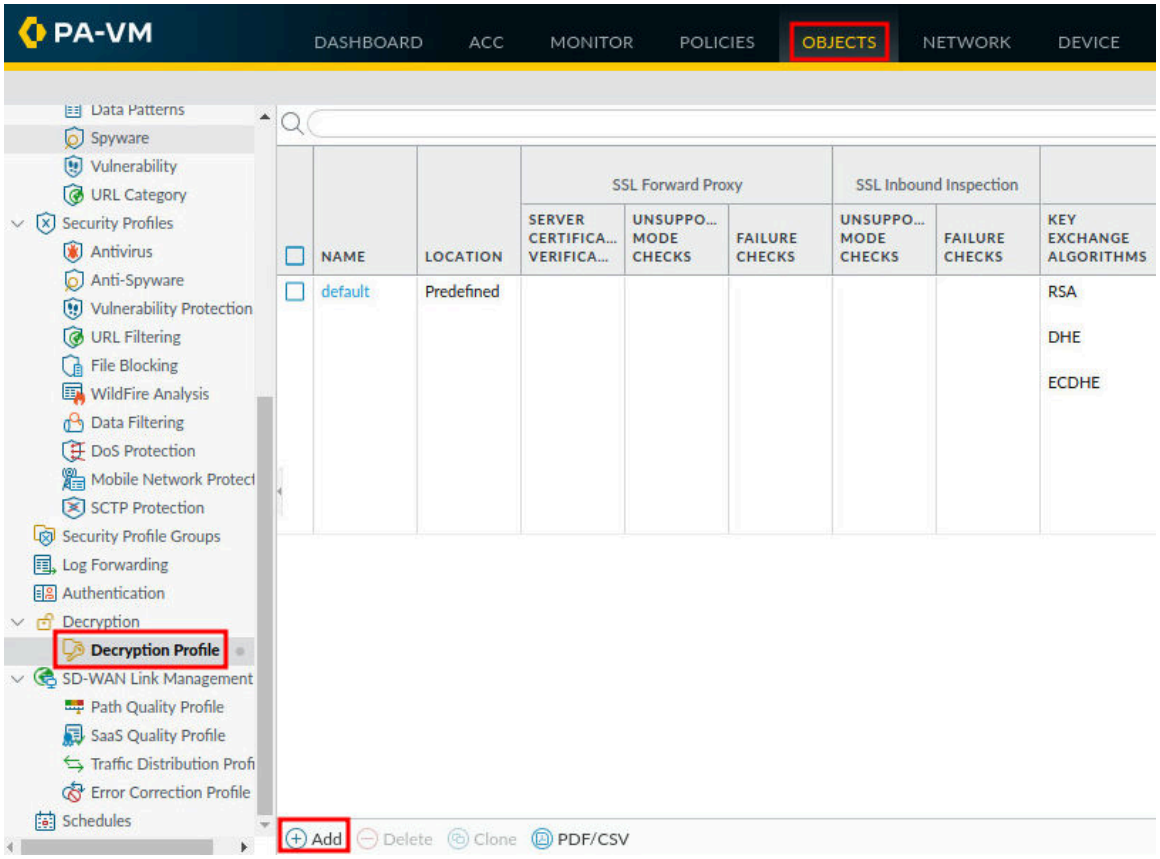
9. Verify the *SSL Inbound Cert* is showing a status of **valid**.



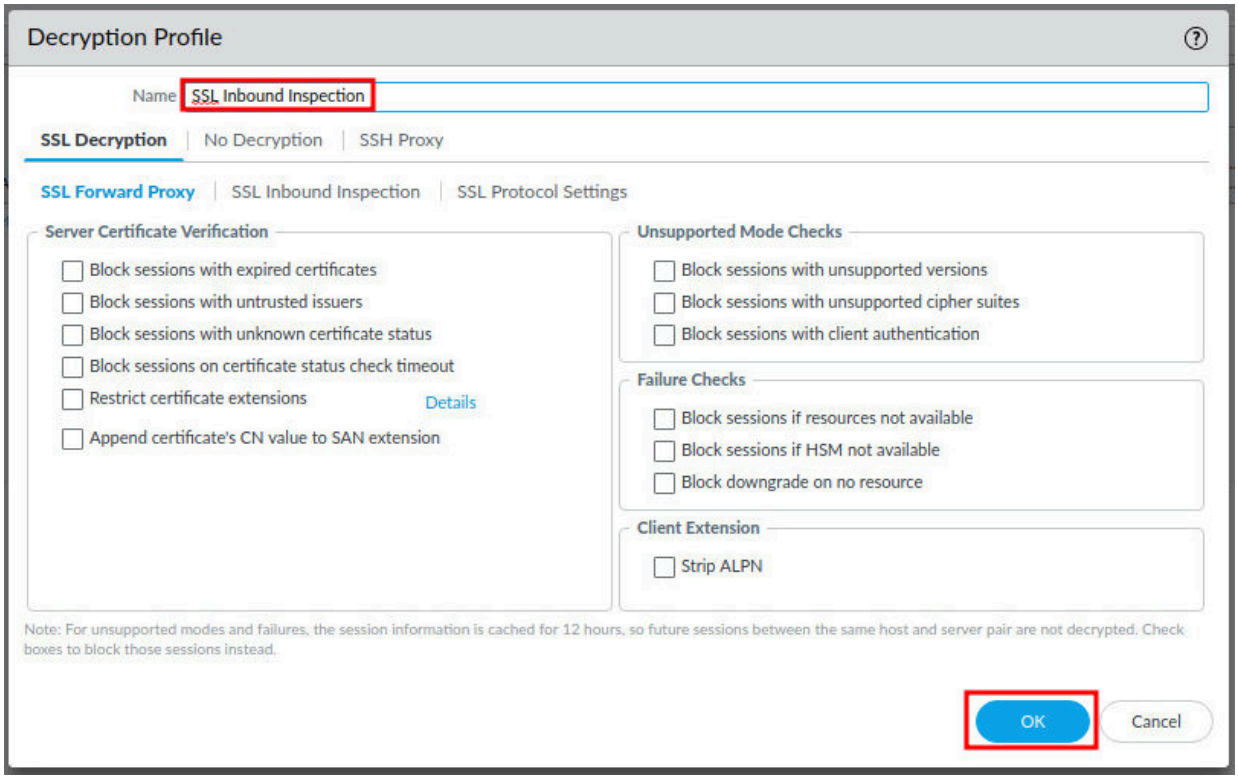
1.3 Create a Decryption Profile

In this section, you will create a decryption profile. Decryption profiles allow administrators to perform checks on both decrypted traffic and traffic that would have been excluded from decryption. After a decryption profile is created, it can then be attached to a decryption policy rule that will enforce the profile settings.

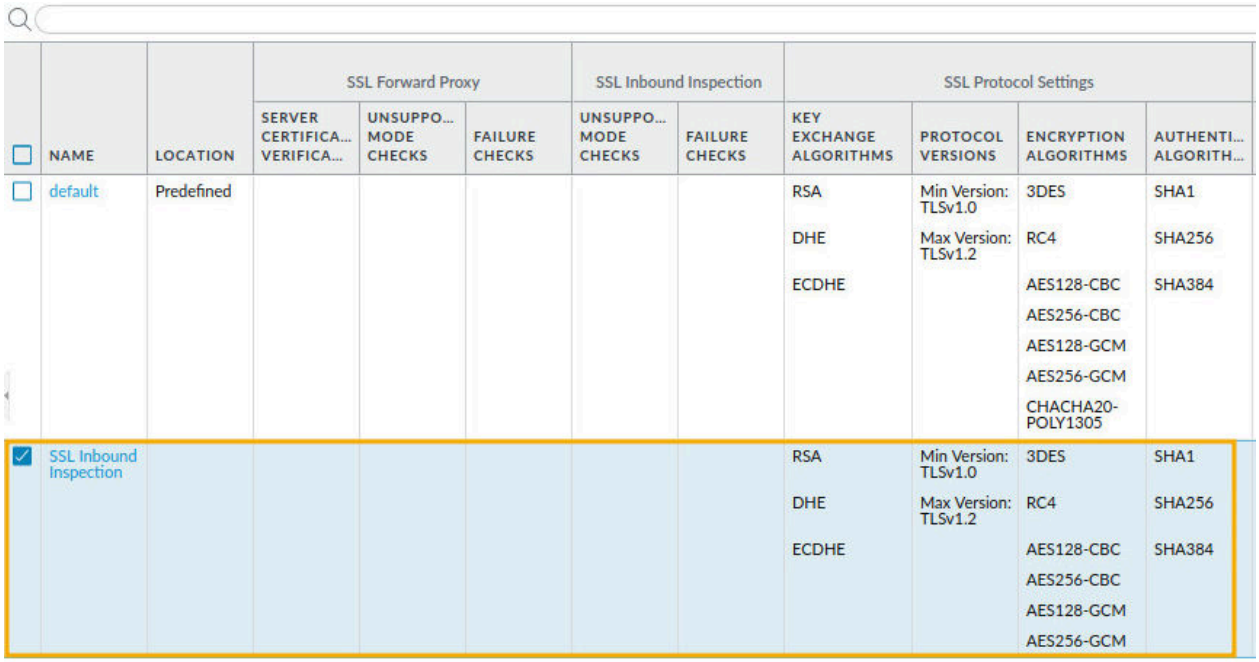
1. Navigate to **Objects > Decryption > Decryption Profile > Add**. You may need to scroll down in the left pane.



2. In the *Decryption Profile* window, type `SSL Inbound Inspection`. Then, click the **OK** button.



3. Verify the **SSL Inbound Inspection** Decryption Profile was created.

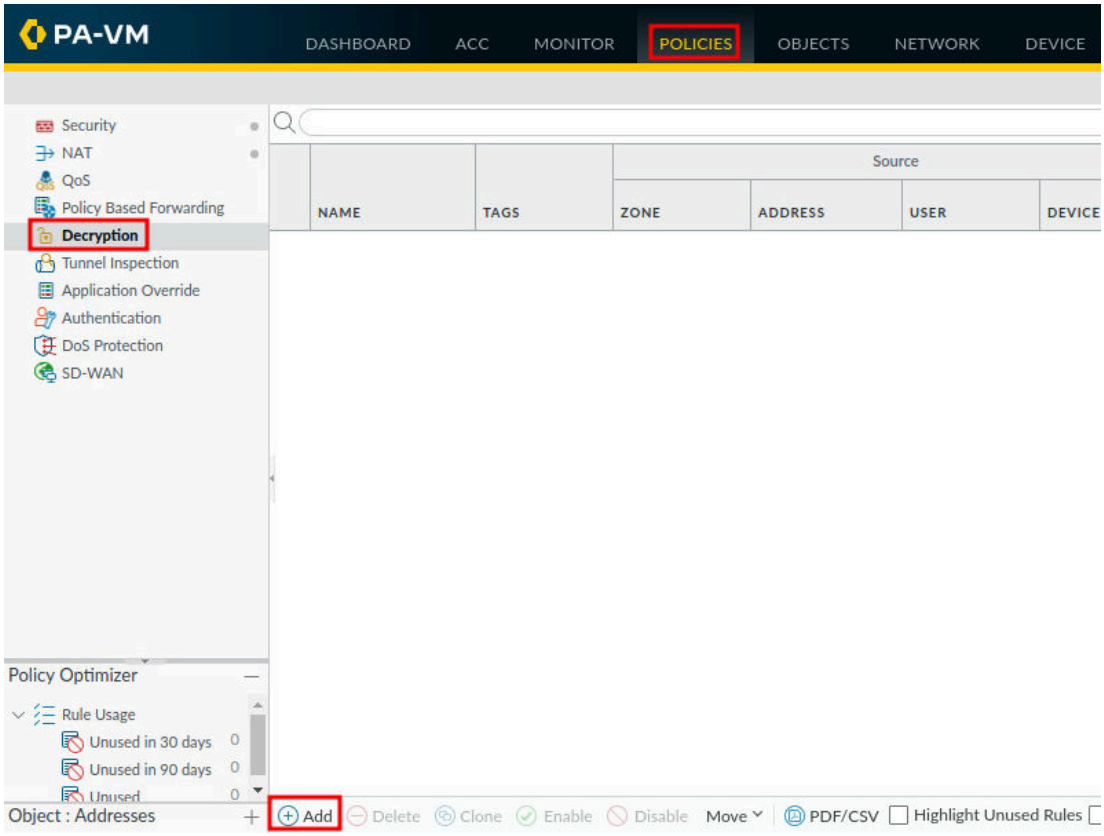


NAME	LOCATION	SSL Forward Proxy: SERVER CERTIFICA... VERIFICA...	SSL Forward Proxy: UNSUPPO... MODE CHECKS	SSL Forward Proxy: FAILURE CHECKS	SSL Inbound Inspection: UNSUPPO... MODE CHECKS	SSL Inbound Inspection: FAILURE CHECKS	SSL Protocol Settings: KEY EXCHANGE ALGORITHMS	SSL Protocol Settings: PROTOCOL VERSIONS	SSL Protocol Settings: ENCRYPTION ALGORITHMS	SSL Protocol Settings: AUTHENTI... ALGORITH...
default	Predefined						RSA DHE ECDHE	Min Version: TLSv1.0 Max Version: TLSv1.2	3DES RC4 AES128-CBC AES256-CBC AES128-GCM AES256-GCM CHACHA20-POLY1305	SHA1 SHA256 SHA384
SSL Inbound Inspection							RSA DHE ECDHE	Min Version: TLSv1.0 Max Version: TLSv1.2	3DES RC4 AES128-CBC AES256-CBC AES128-GCM AES256-GCM	SHA1 SHA256 SHA384

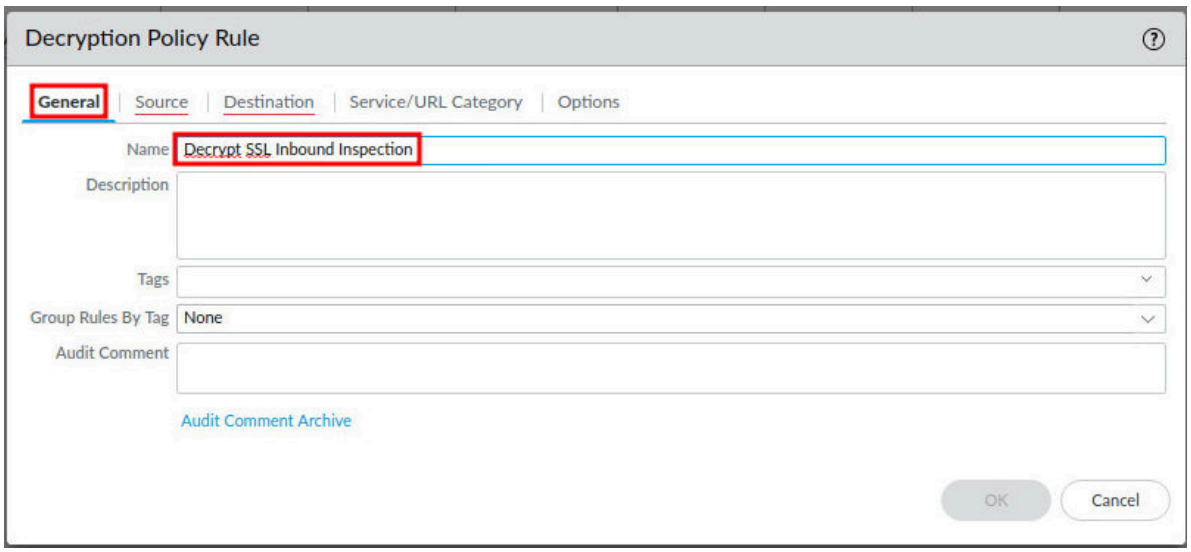
1.4 Create a Decryption Policy

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.

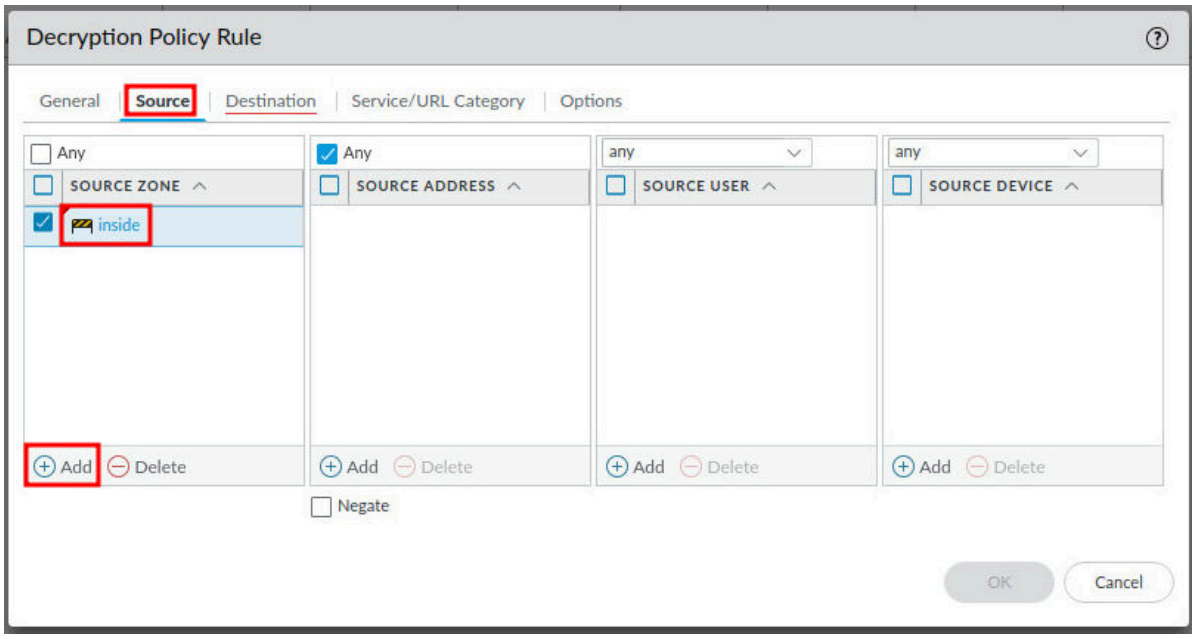
1. Navigate to **Policies > Decryption > Add.**



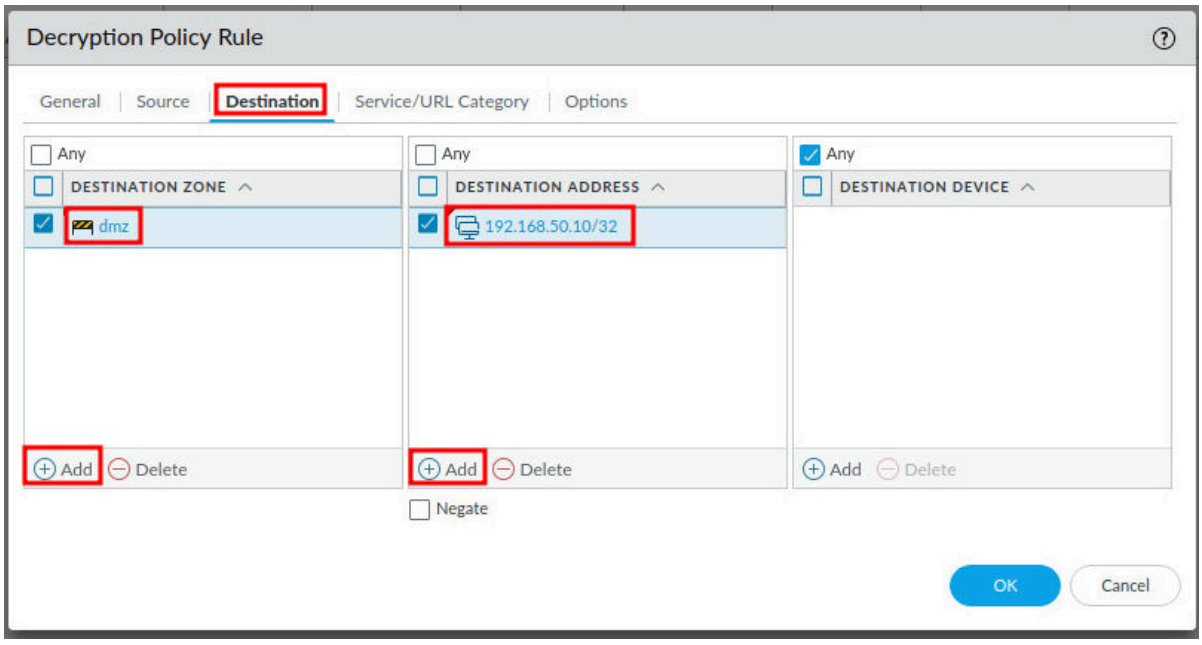
2. In the **General** tab of the *Decryption Policy Rule* window, type `Decrypt SSL Inbound Inspection` in the *Name* field.



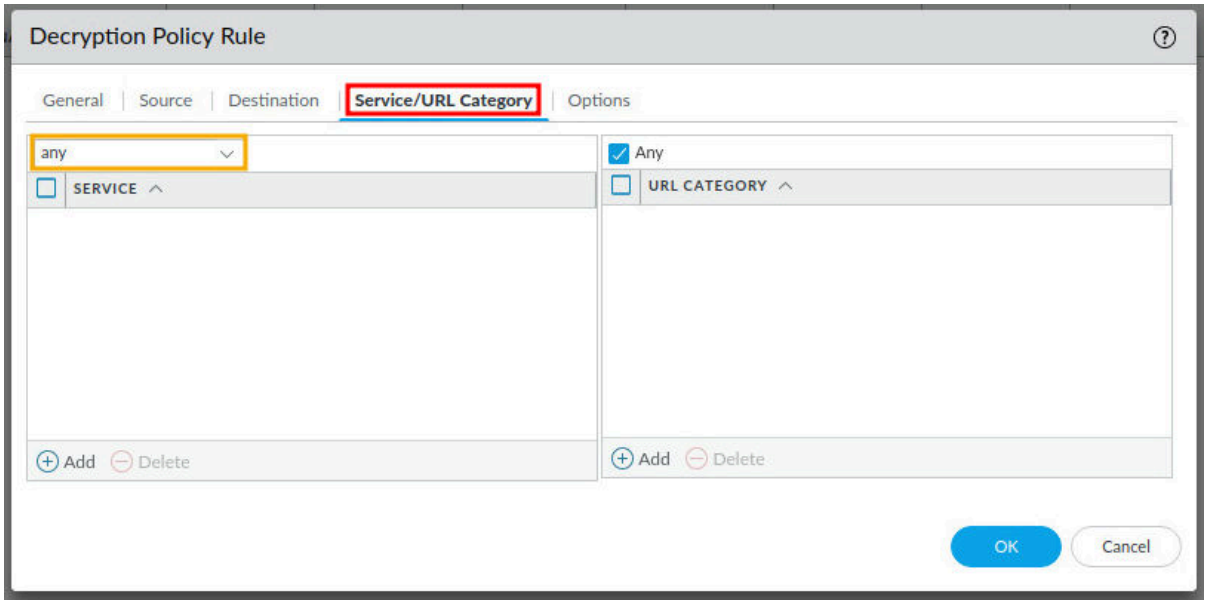
3. In the *Decryption Policy Rule* window, click on the **Source** tab. Then, click **Add** in the *Source Zone* section. Next, select **inside**.



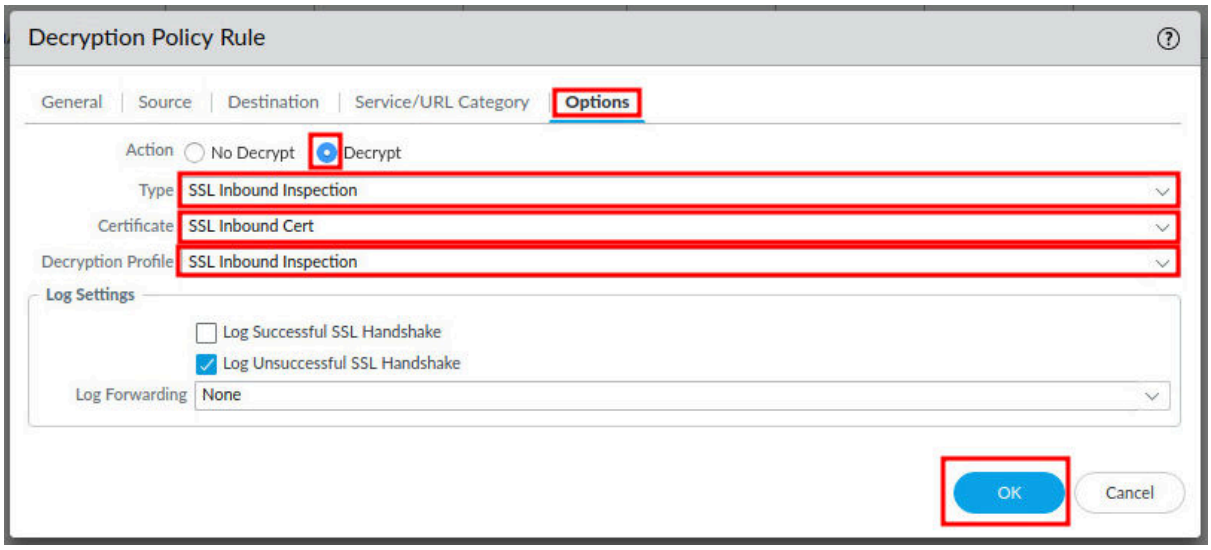
4. In the *Decryption Policy Rule* window, click on the **Destination** tab. Then, click **Add** in the *Destination Zone* pane. Next, select **dmz** and press **Enter**. In the *Destination Address* pane, click **Add**. Type `192.168.50.10/32` and press **Enter**.



5. In the *Decryption Policy Rule* window, click on the **Service/URL Category** tab. In the *Service* pane, select and verify **any** is selected in the dropdown menu.



6. In the *Decryption Policy Rule* window, click on the **Options** tab. Then, select **Decrypt** for the *Action*. Next, select **SSL Inbound Inspection** in the *Type* dropdown. Then, select **SSL Inbound Cert** in the *Certificate* dropdown. Next, select **SSL Inbound Inspection** in the *Decryption Profile* field. Finally, click the **OK** button.

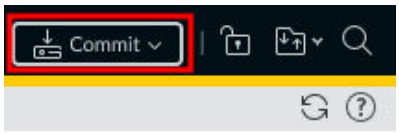


7. Verify the **Decrypt SSL Inbound Policy** is showing and correct.

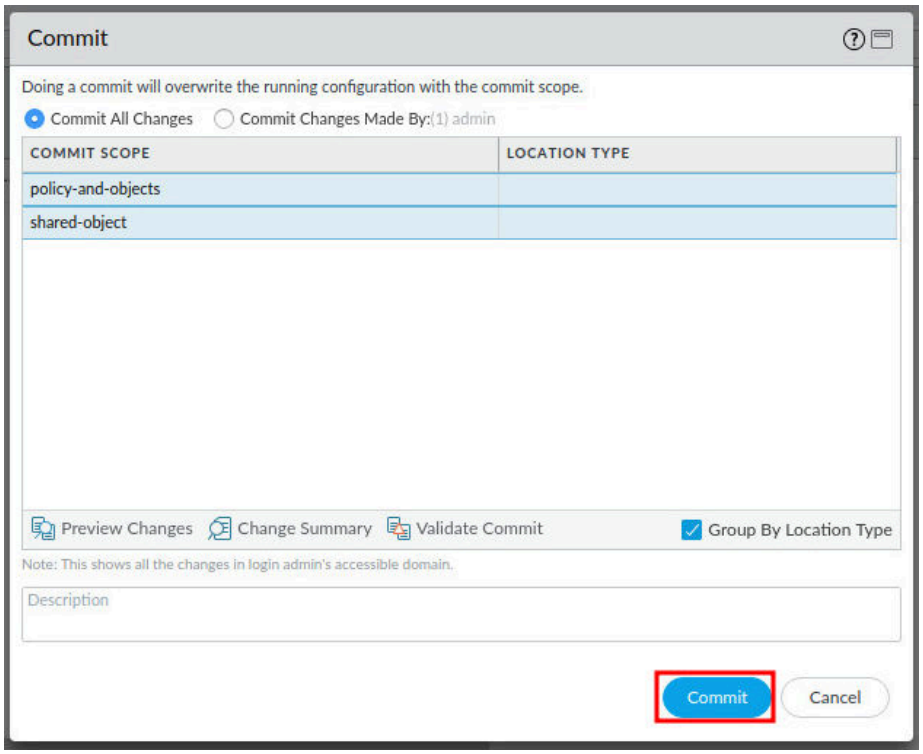
1.5 Commit and Test Decryption Policy

In this section, you will commit your changes to the Firewall. Then, you will test the decryption policy you created earlier.

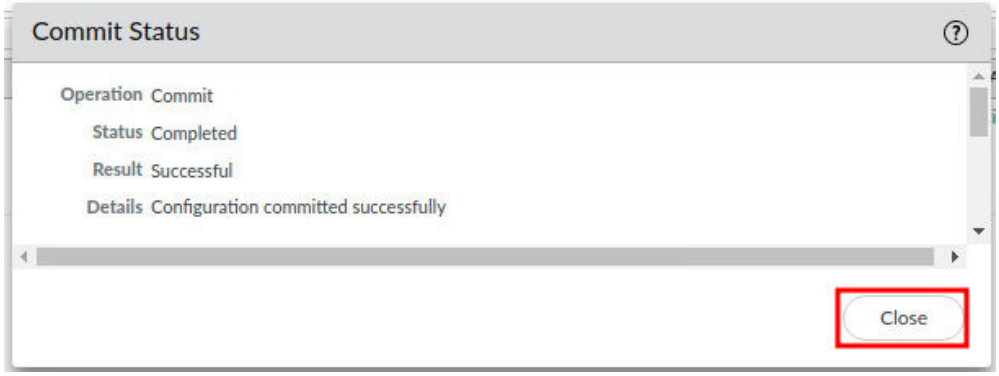
1. Click the **Commit** link located at the top-right of the web interface.



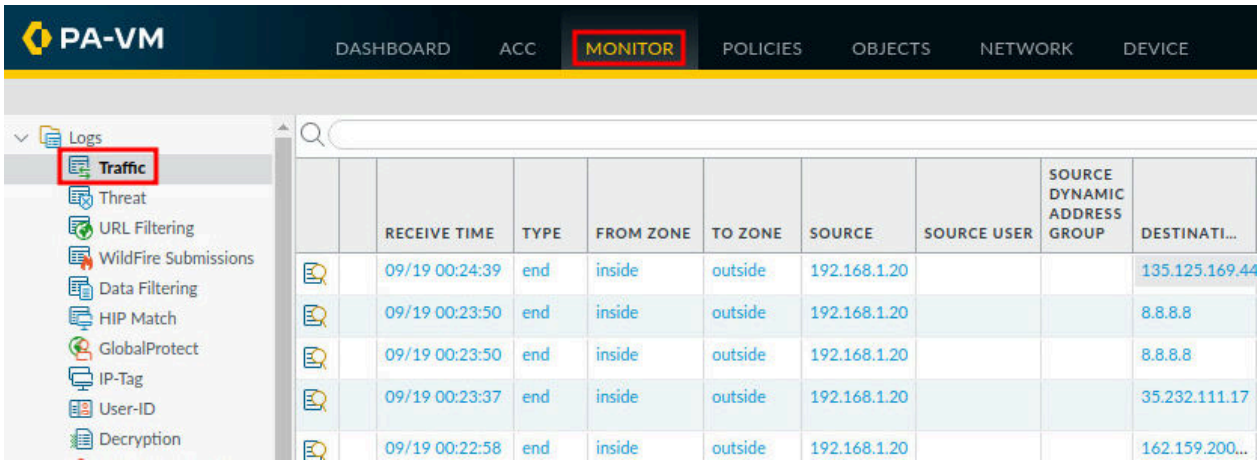
2. In the *Commit* window, click **Commit** to proceed with committing the changes.



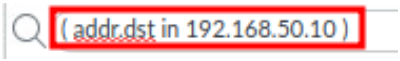
3. When the commit operation successfully completes, click **Close** to continue.



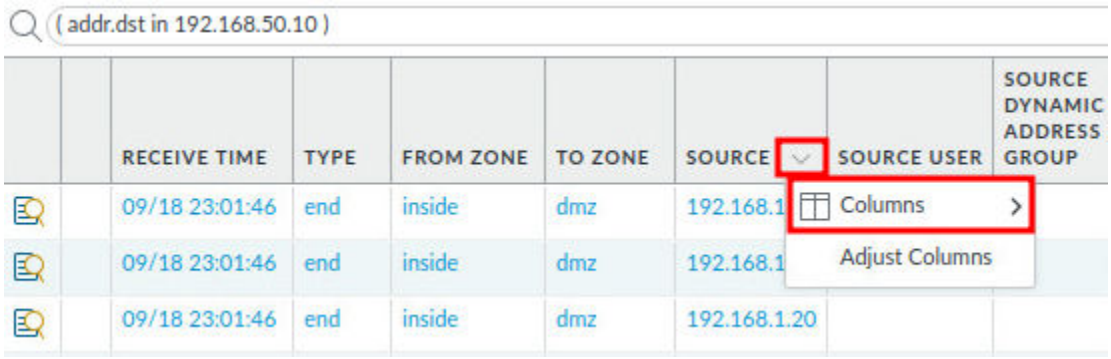
4. Navigate to **Monitor > Logs > Traffic.**



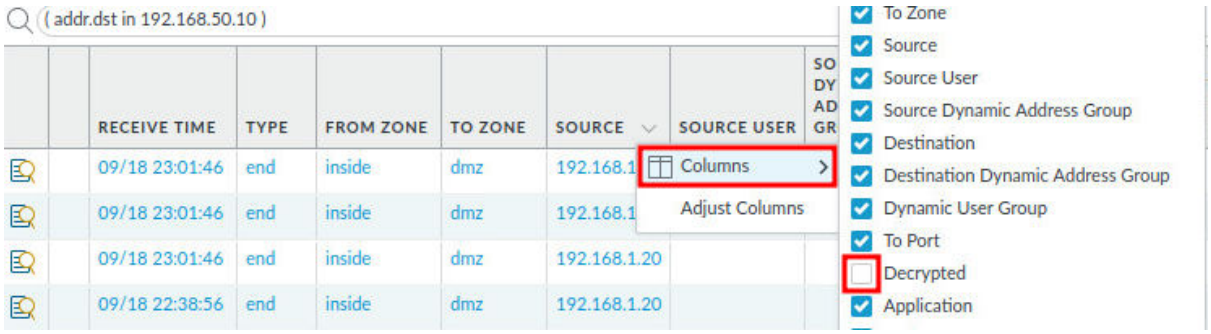
5. In the search box, type `( addr.dst in 192.168.50.10 )` and press **Enter.**



6. Move the mouse cursor to the right of *Source* and click the **down arrow** to bring up the **Columns** menu.



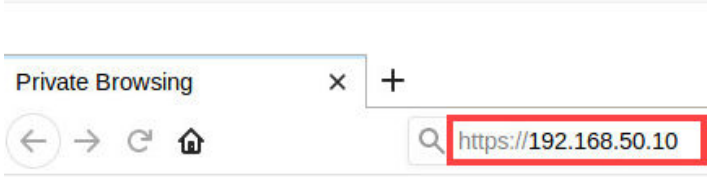
7. Highlight **Columns** and click to check the **Decrypted** checkbox.



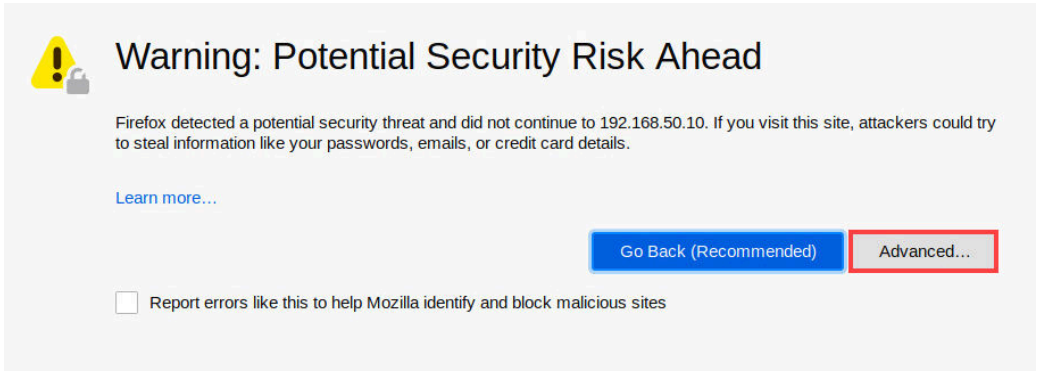
The **Decrypted** checkbox might be listed alphabetically among the unchecked boxes in the lower part of the menu

8. Open the *Firefox Web Browser* by clicking on the **Firefox** icon located in the task bar.

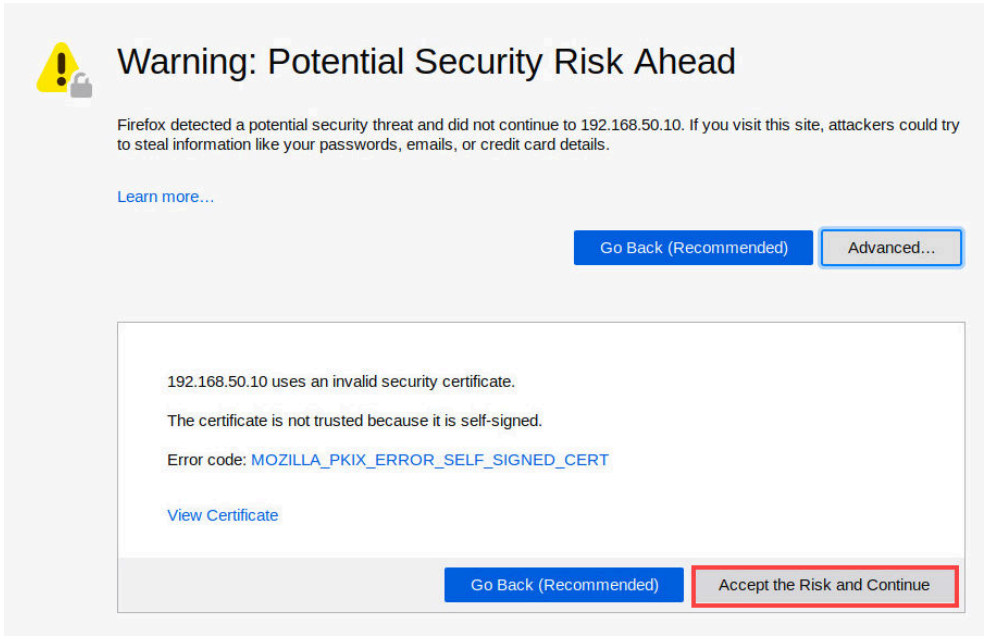
9. In the address bar, type `https://192.168.50.10` and click **Enter**.



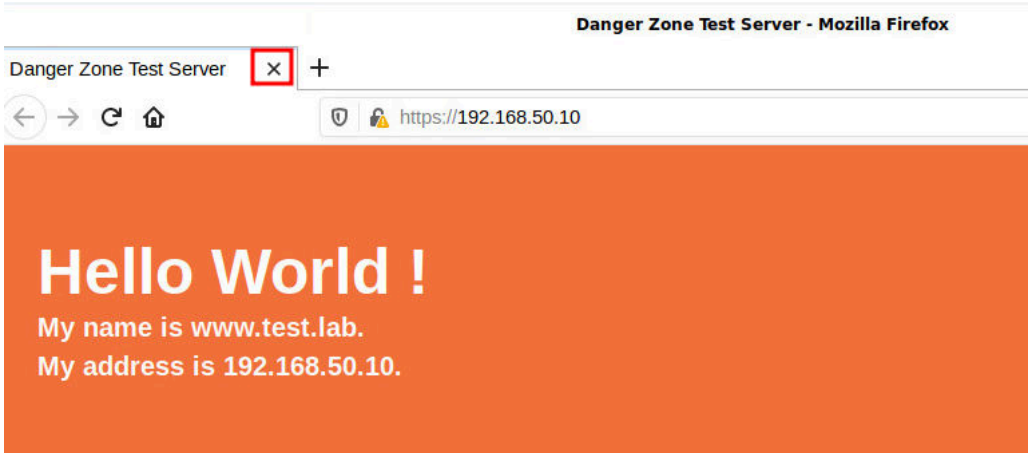
10. You will see a "*Warning: Potential Security Risk Ahead* message. Click on the **Advanced** button.



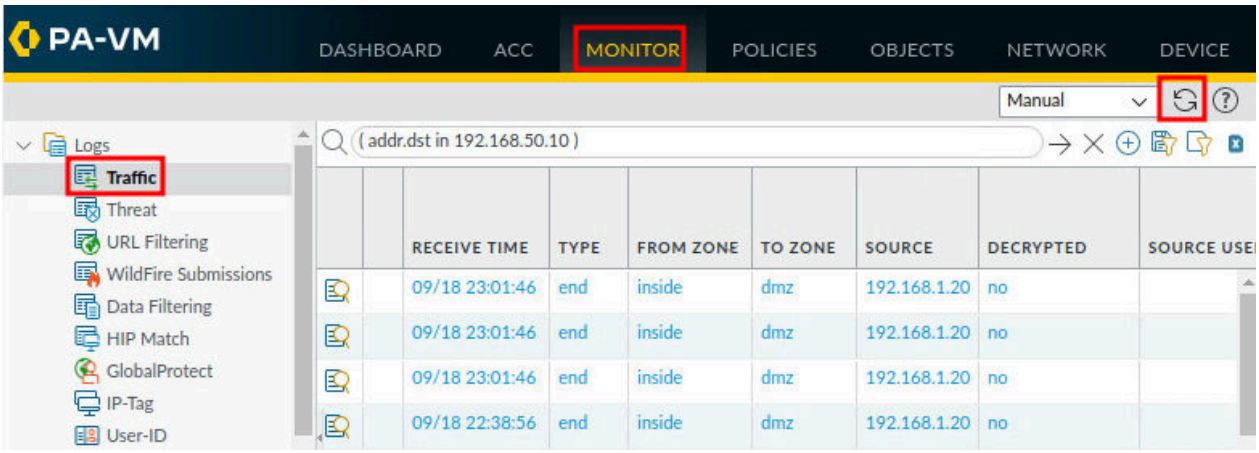
11. Click on **Accept the Risk and Continue**.



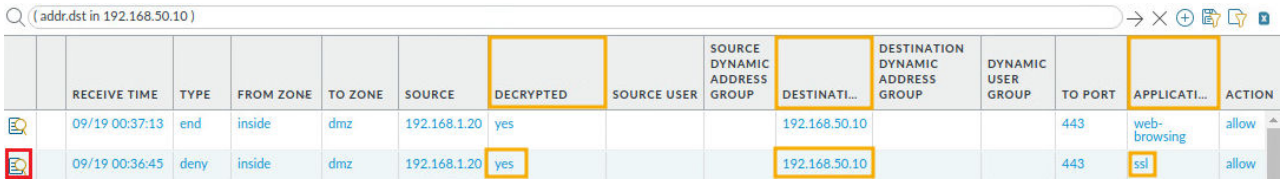
12. Notice that the *Apache HTTP Server Test page* is working properly. Click on the **X** of the tab to close it.



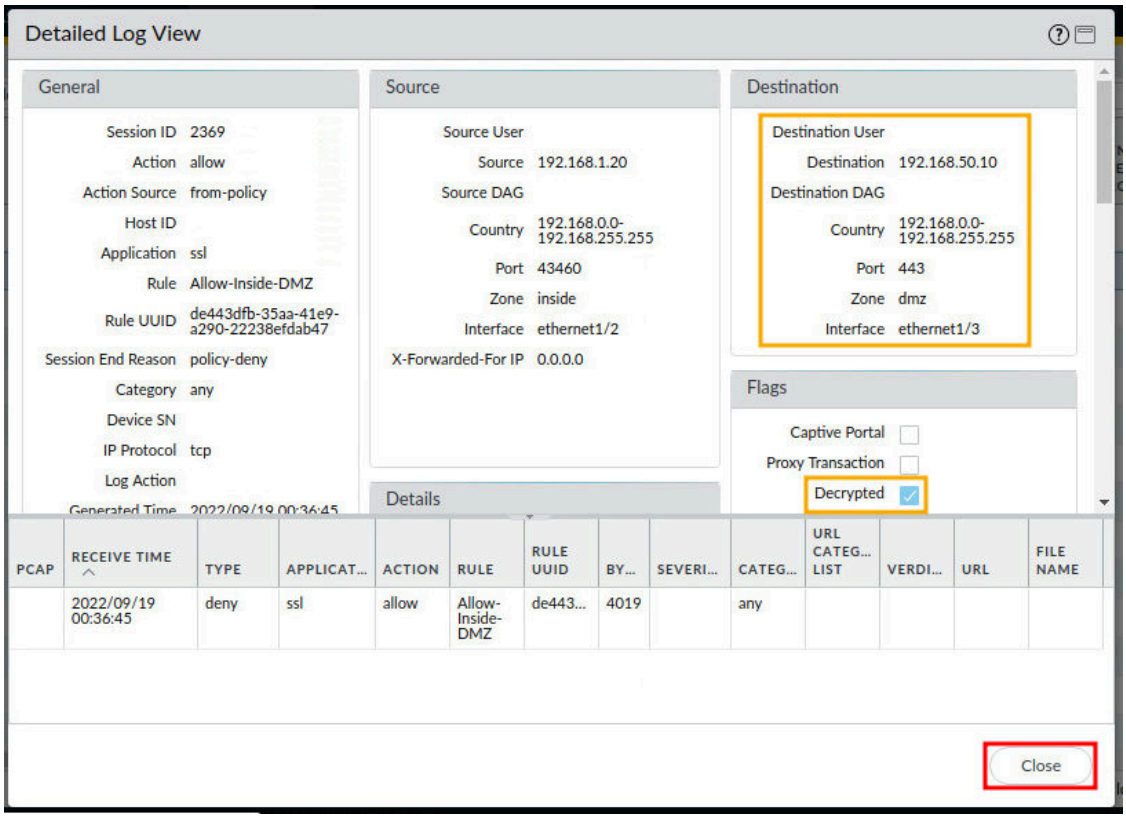
13. Navigate to **Monitor > Logs > Traffic**. Then, click the **refresh** icon.



14. Look for traffic associated with the application of **ssl** and the *Decrypted* column set to **yes**. Click the magnifying glass on the left to open the **Detailed Log View** of the traffic to analyze the traffic from the Client machine of **192.168.1.20** to the DMZ server of **192.168.50.10.**



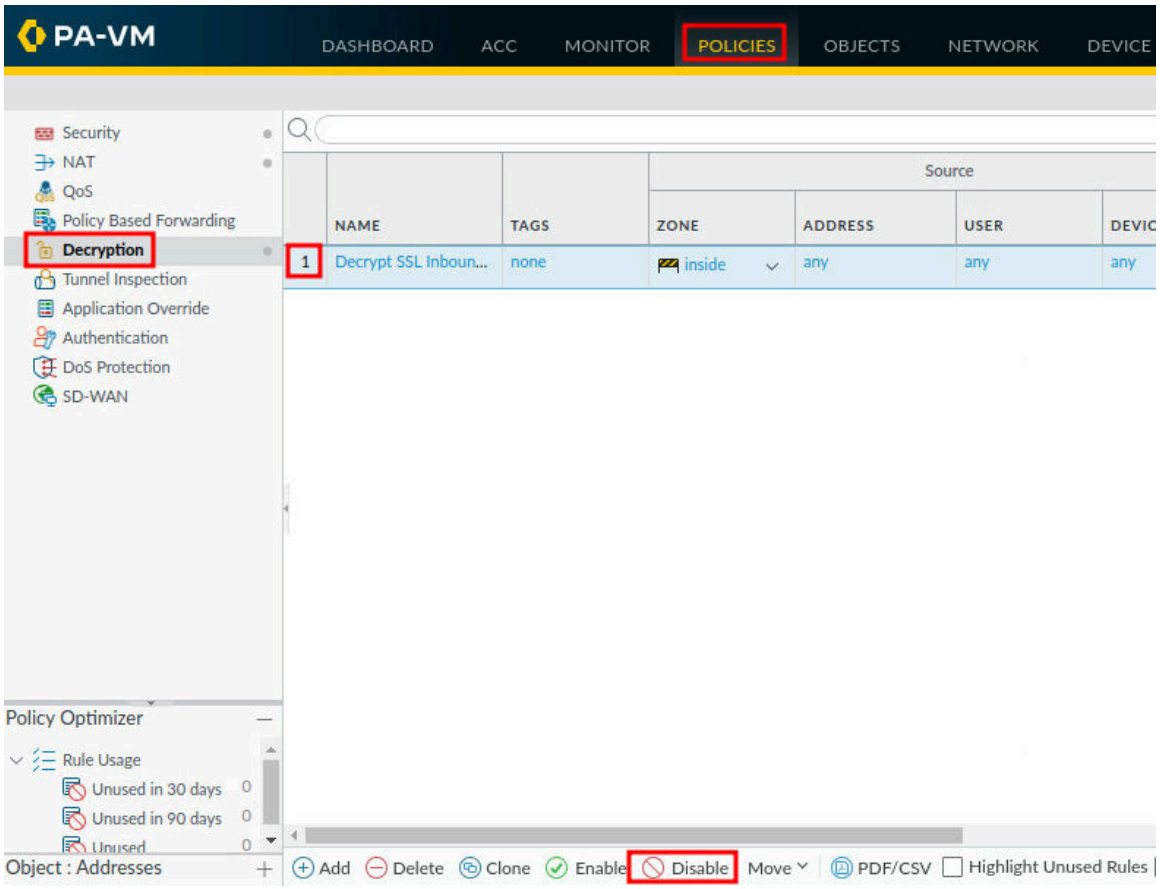
15. In the *Detailed Log View* window, notice in the *Destination* section, an *Address* of **192.168.50.10** and *Port* **443** to the **dmz** zone of the DMZ server. Then, in the *Flags* section, notice the flag **Decrypted** is set and click the **Close** button.



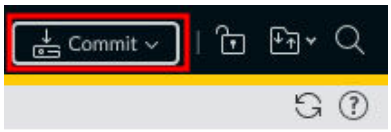
1.6 Disable Decryption Policy

In this section, you will disable the decryption policy you created earlier. Then, after committing the changes to the Firewall, you will monitor traffic logs to determine if traffic is still being decrypted.

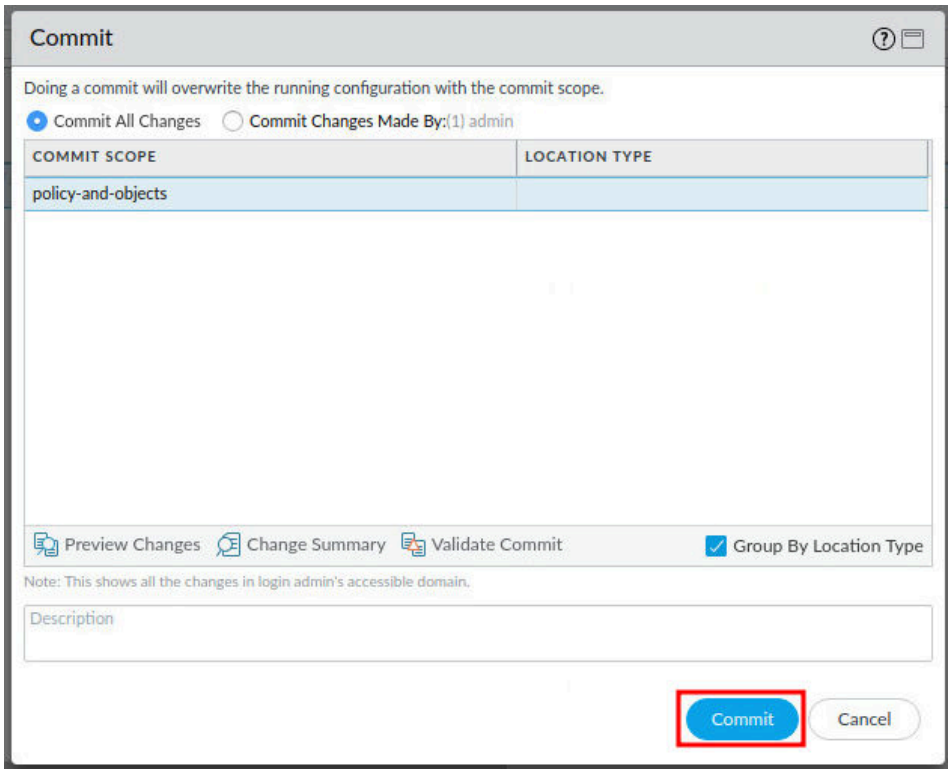
1. Navigate to **Policies > Decryption**. Then, click the **1** for the **Decrypt SSL Inbound Inspection** policy**. Next,** click the **Disable** button.



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



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

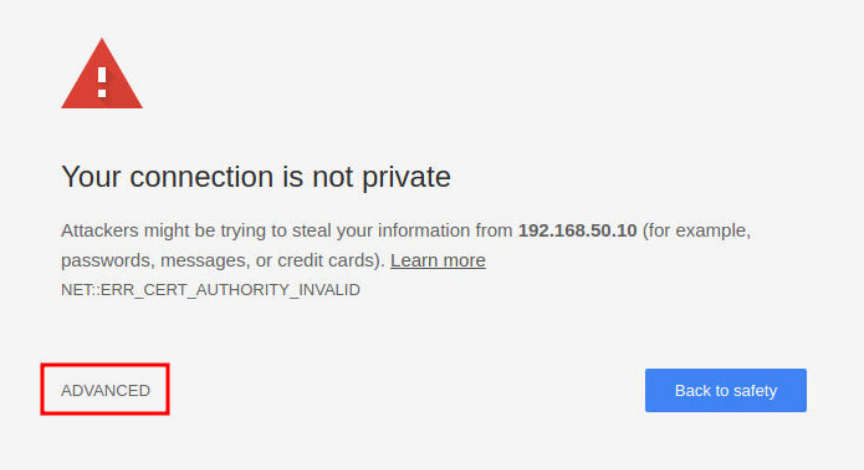


4. When the commit operation successfully completes, click **Close** to continue.

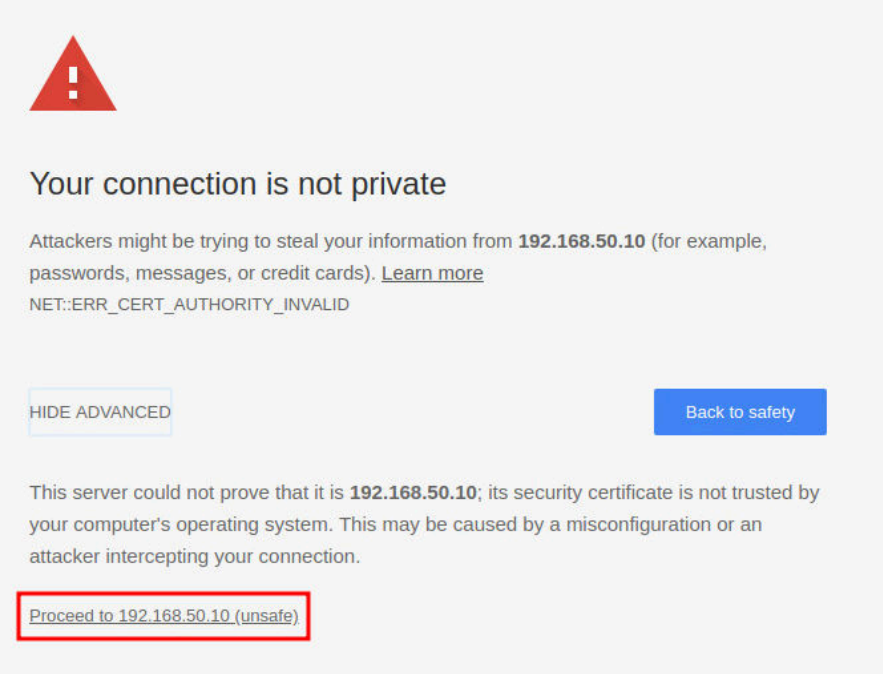
5. Click the **New tab** button in *Chromium*.

6. In the address bar, type `https://192.168.50.10` and click **Enter**.

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

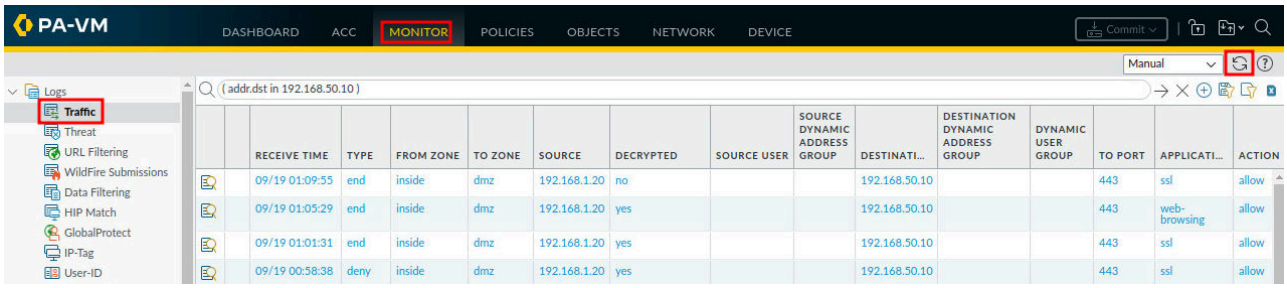


8. Click on **Proceed to 192.168.50.10 (unsafe)**.

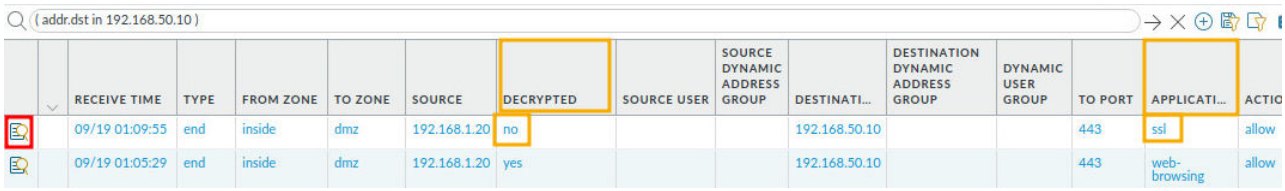


9. Notice that the *Apache HTTP Server Test page* is working. Click on the **X** of the tab to close it.

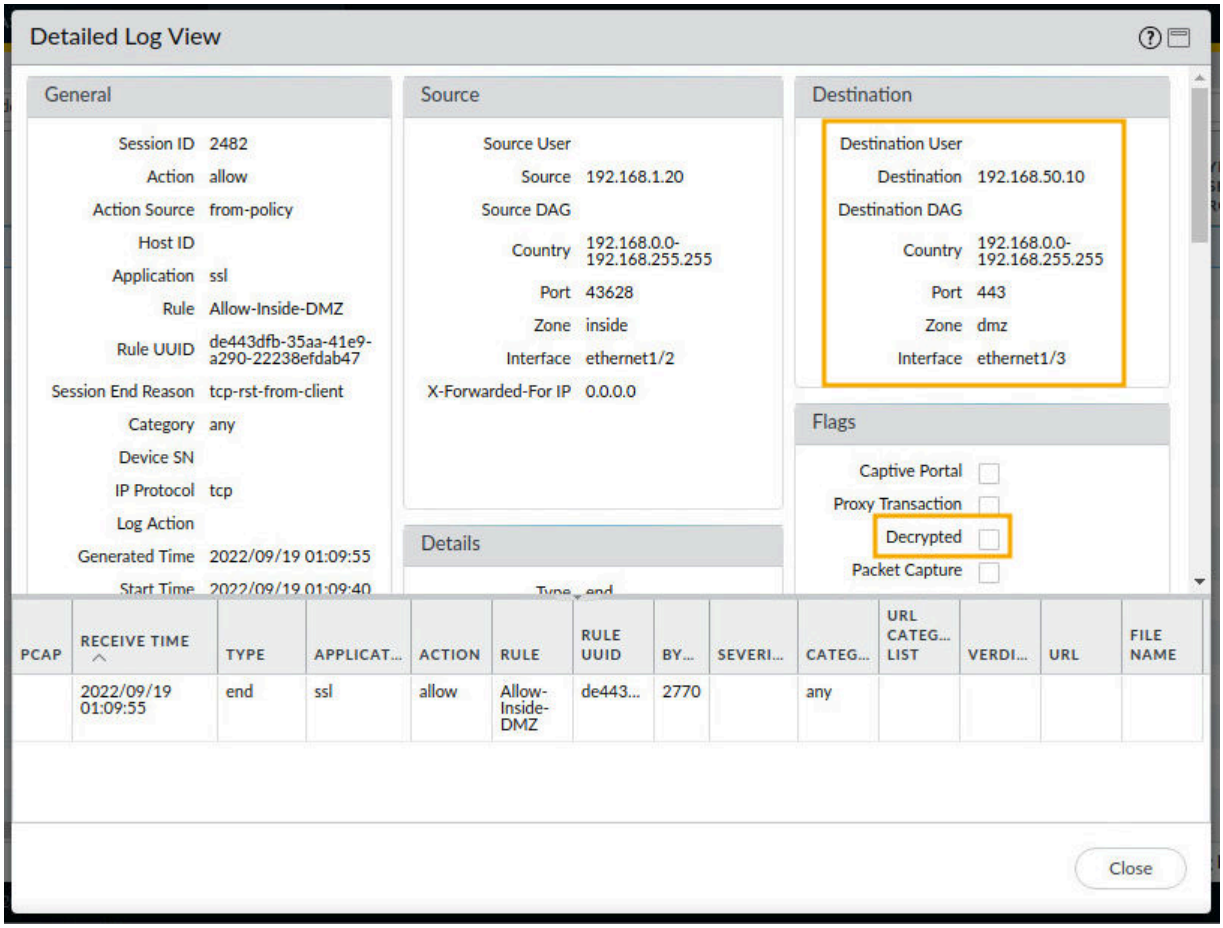
10. Navigate to **Monitor > Logs > Traffic**. Then, click the **refresh** icon.



11. Look for traffic associated with the application of **ssl** and the *Decrypted* column set to **no**. Click on the magnifying glass icon on the left to open the **Detailed Log View** of the traffic to analyze the traffic from the Client machine of **192.168.1.20** to the DMZ server of **192.168.50.10.**



12. In the *Detailed Log View* window, notice in the *Destination* section, an *Address* of **192.168.50.10** and *Port* **443** to the **dmz** zone of the DMZ server. Then, in the *Flags* section, notice the flag for **Decrypted** is not set.



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

