



NETWORK SECURITY FUNDAMENTALS V2

Lab 7: Decrypting SSL Inbound Traffic

Document Version: **2022-12-23**

Copyright © 2022 Network Development Group, Inc.
www.netdevgroup.com

NETLAB+ is a registered trademark of Network Development Group, Inc.

Palo Alto Networks and the Palo Alto Networks logo are trademarks or registered trademarks of Palo Alto Networks, Inc.

Contents

Introduction	3
Objective	3
Lab Topology	4
Lab Settings	5
1 Decrypting SSL Inbound Traffic	6
1.0 Load Lab Configuration	6
1.1 Download the SSL Certificate from DMZ Server	11
1.2 Import SSL Certificate	13
1.3 Create a Decryption Profile	17
1.4 Create a Decryption Policy	19
1.5 Commit and Test Decryption Policy	22
1.6 Disable Decryption Policy	27

Introduction

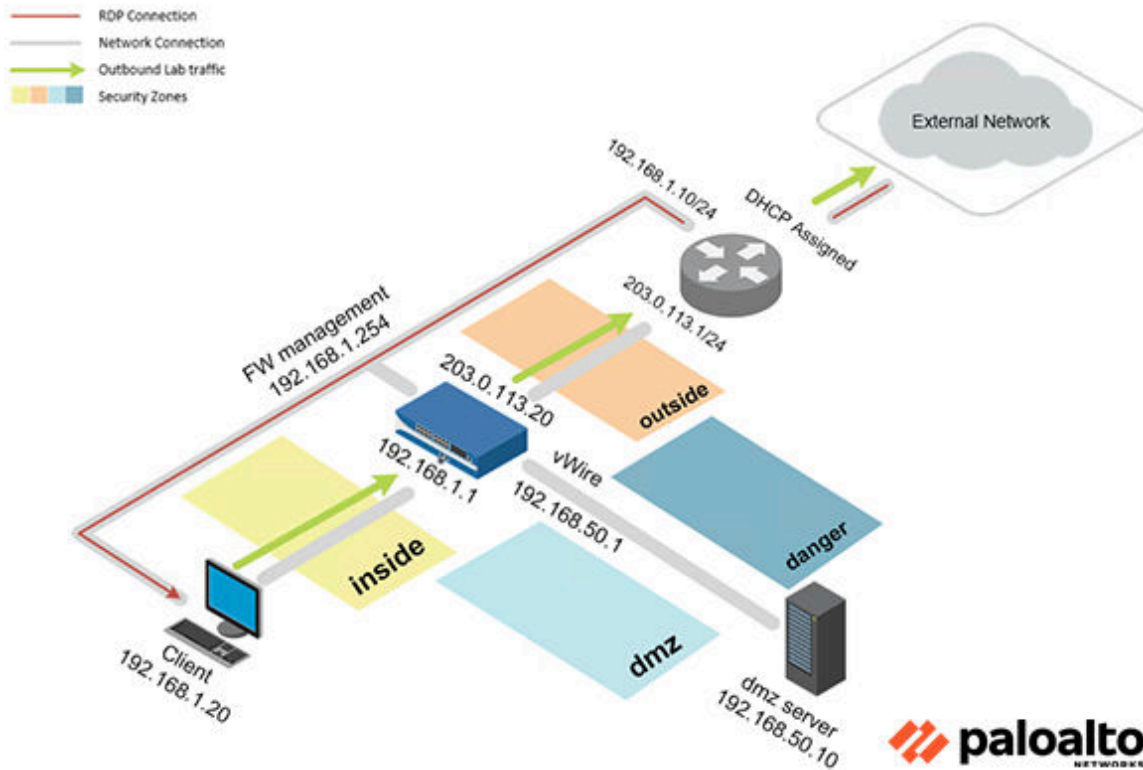
In this lab, you will decrypt SSL inbound traffic and inspect SSL traffic from the Client machine to the DMZ server. When the SSL server certificate is loaded on the Firewall, and an SSL decryption policy is configured for the inbound traffic, the device can then decrypt and read the traffic as it forwards 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.

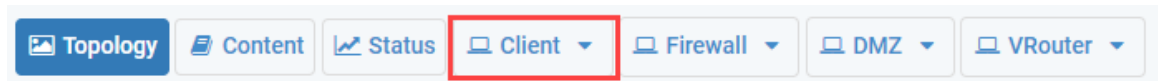
Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Client	192.168.1.20	lab-user	Pal0Alt0!
DMZ	192.168.50.10	root	Pal0Alt0!
Firewall	192.168.1.254	admin	Pal0Alt0!

1 Decrypting SSL Inbound Traffic

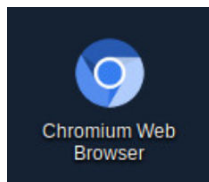
1.0 Load Lab Configuration

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

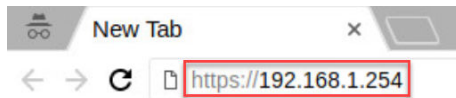
1. Click on the **Client** tab to access the Client PC.



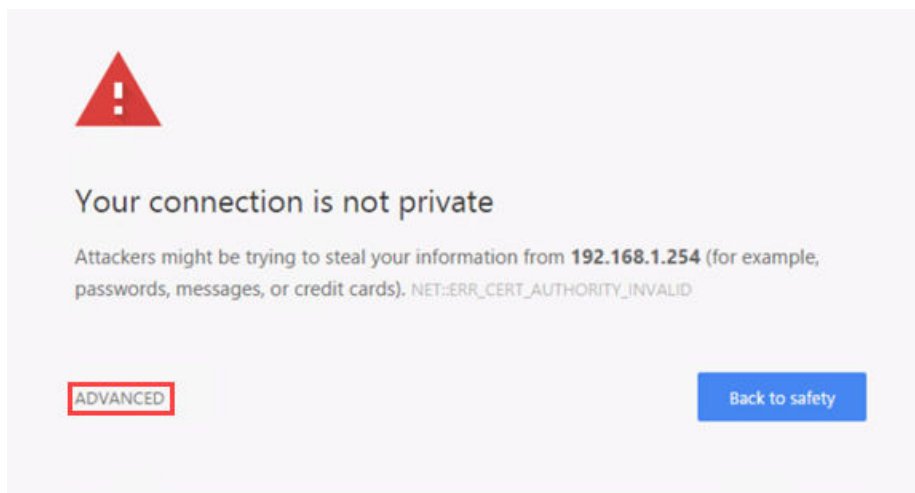
2. Log in to the Client PC as username `lab-user`, password `Pa10Alt0!`.
3. Double-click the **Chromium Web Browser** icon located on the desktop.



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

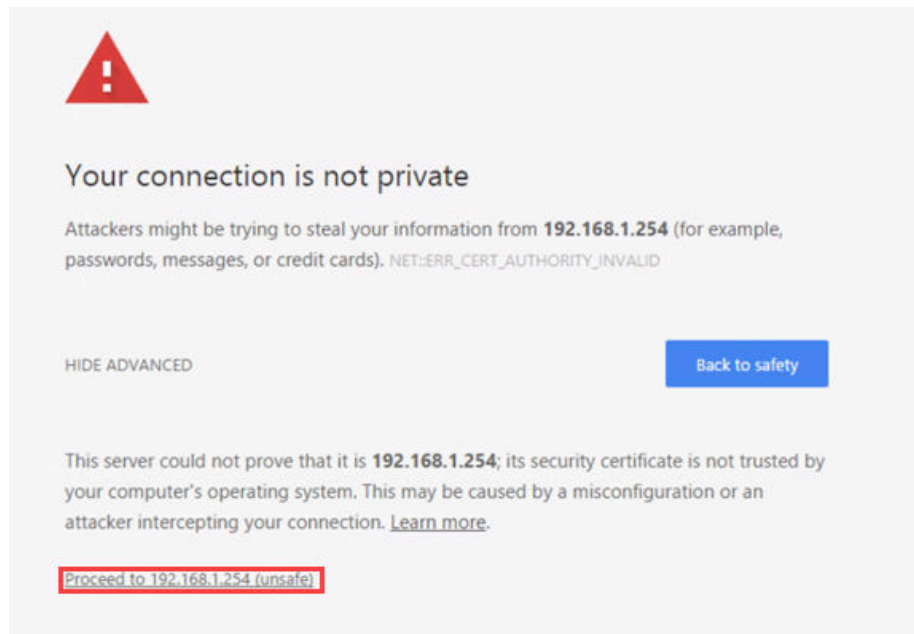


5. You will see a “Your connection is not private” message. Click on the **ADVANCED** link.



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.

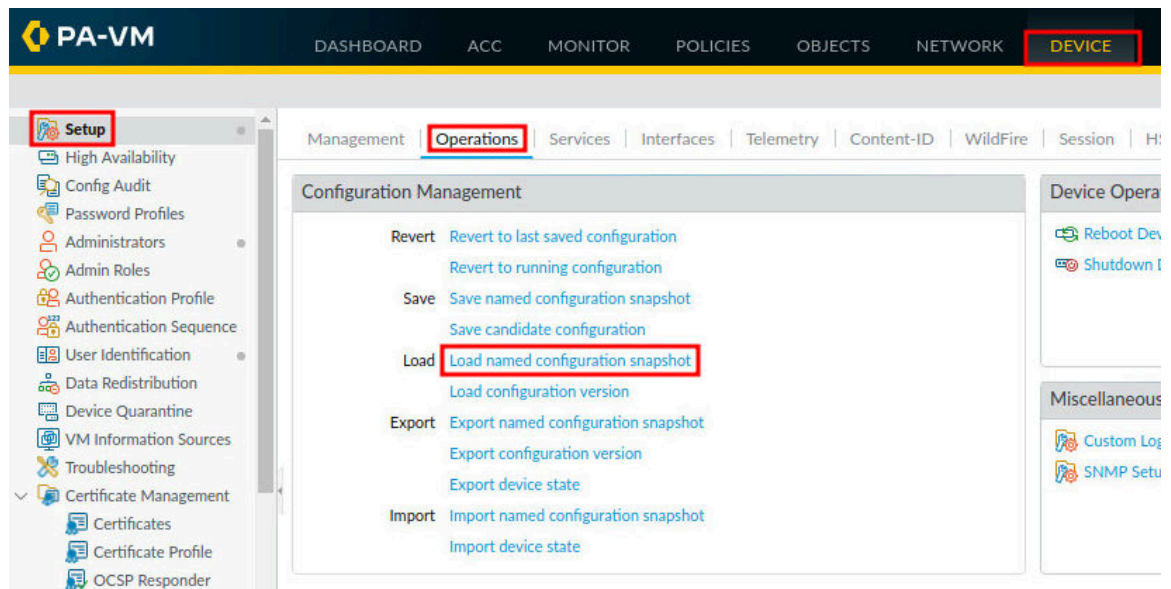
6. Click on **Proceed to 192.168.1.254 (unsafe)**.



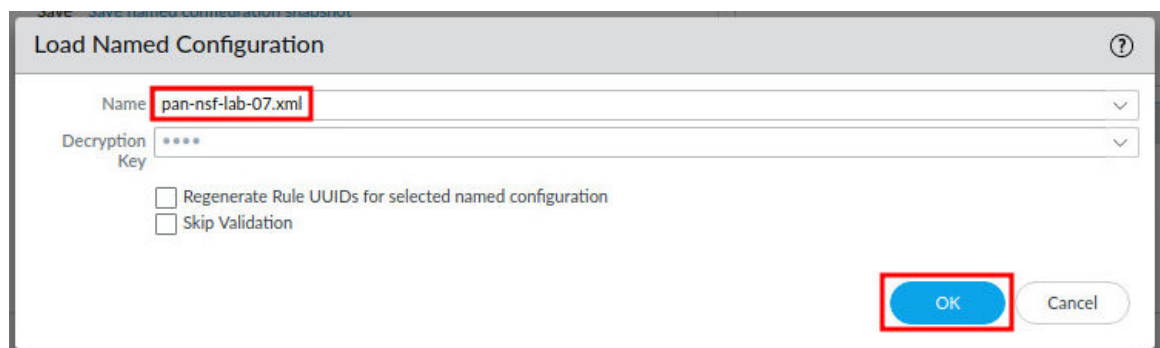
7. Log in to the Firewall web interface as username admin, password Pal0Alt0!.



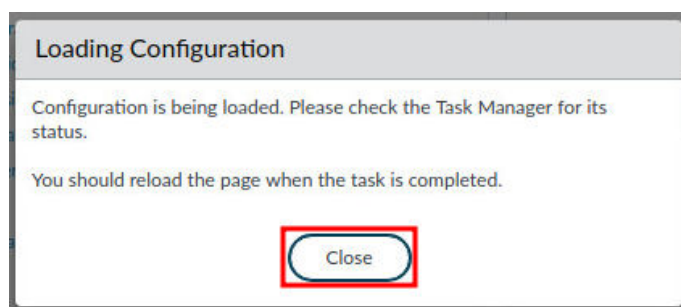
- In the web interface, navigate to **Device > Setup > Operations** and click on **Load named configuration snapshot** underneath the *Configuration Management* section.



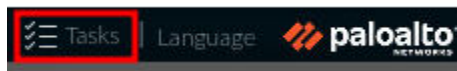
- In the *Load Named Configuration* window, select **pan-nsf-lab-07.xml** from the *Name* dropdown box and click **OK**.



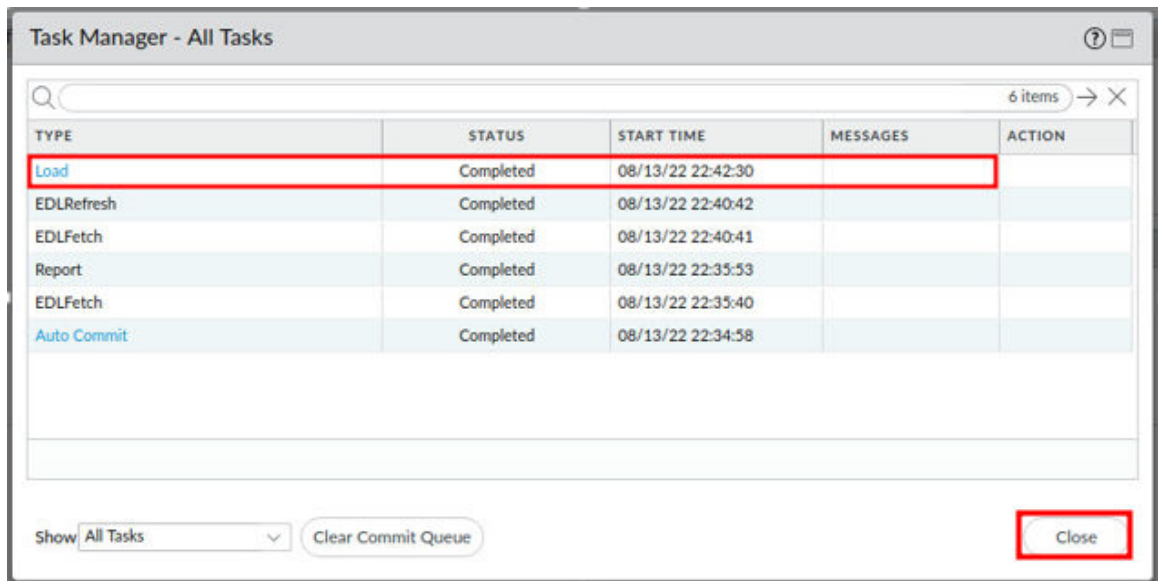
- In the Loading Configuration window, a message will show *Configuration is being loaded. Please check the Task Manager for its status. You should reload the page when the task is completed.* Click **Close** to continue.



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



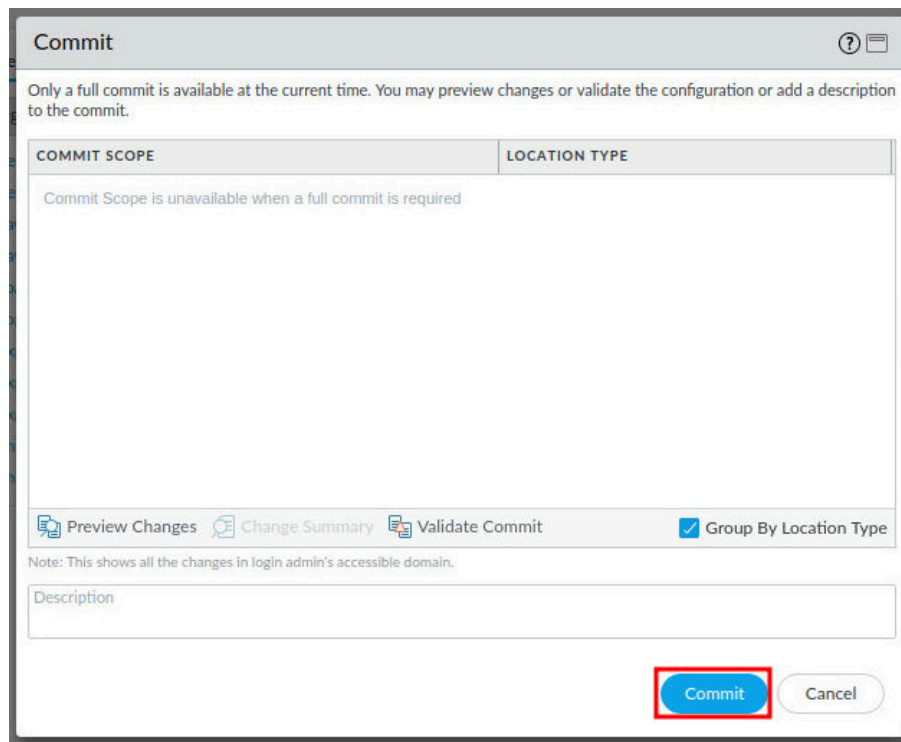
12. In the *Task Manager – All Tasks* window, verify the *Load* type has successfully completed. Click **Close**.



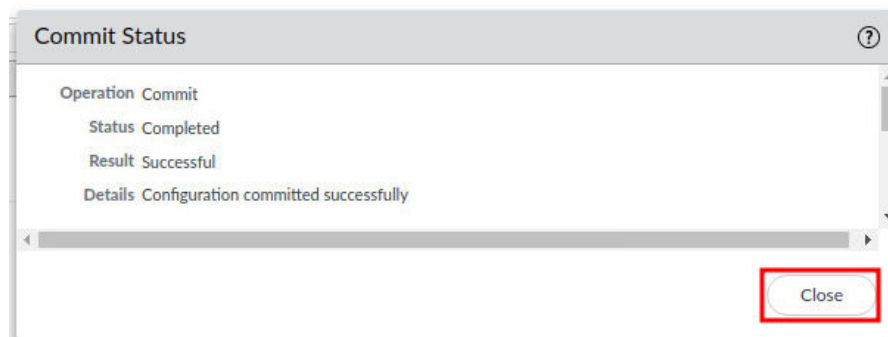
13. Click the **Commit** link located at the top-right of the web interface.



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.

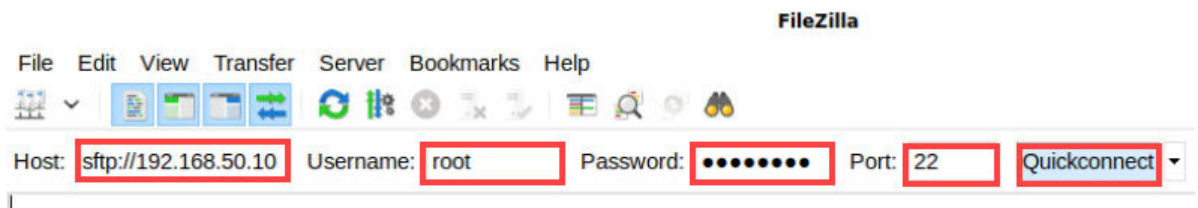
1. Minimize **Chromium** in the upper-right.



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

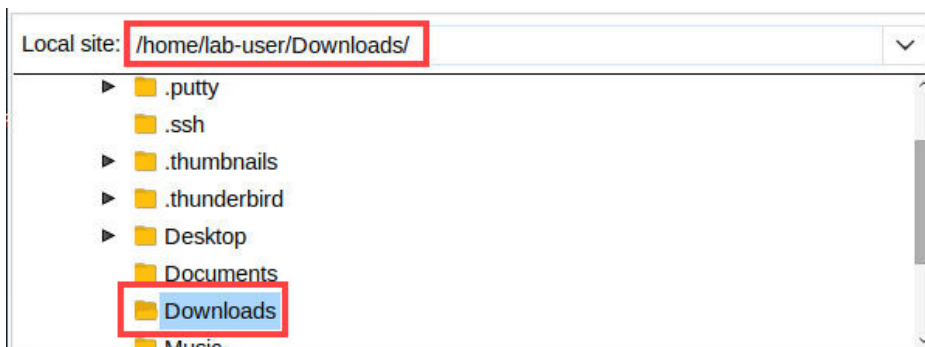


3. In the *FileZilla* window, type `sftp://192.168.50.10` for the *Host*, type `root` for the *Username*, type `Pa1øA1t0!` for the *Password*, lastly, type `22` for the *Port*. Then, click the **Quickconnect** button.

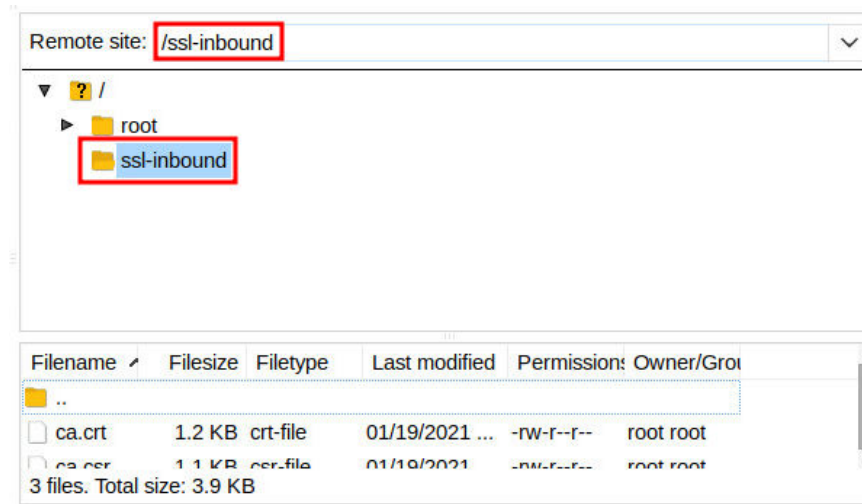


You may be prompted to remember the password after connecting to `sftp://192.168.50.10`. It is strongly recommended to not save passwords automatically as this could lead to insecure accounts and networks. If prompted to save the password, select **Do not save passwords** and select **OK**.

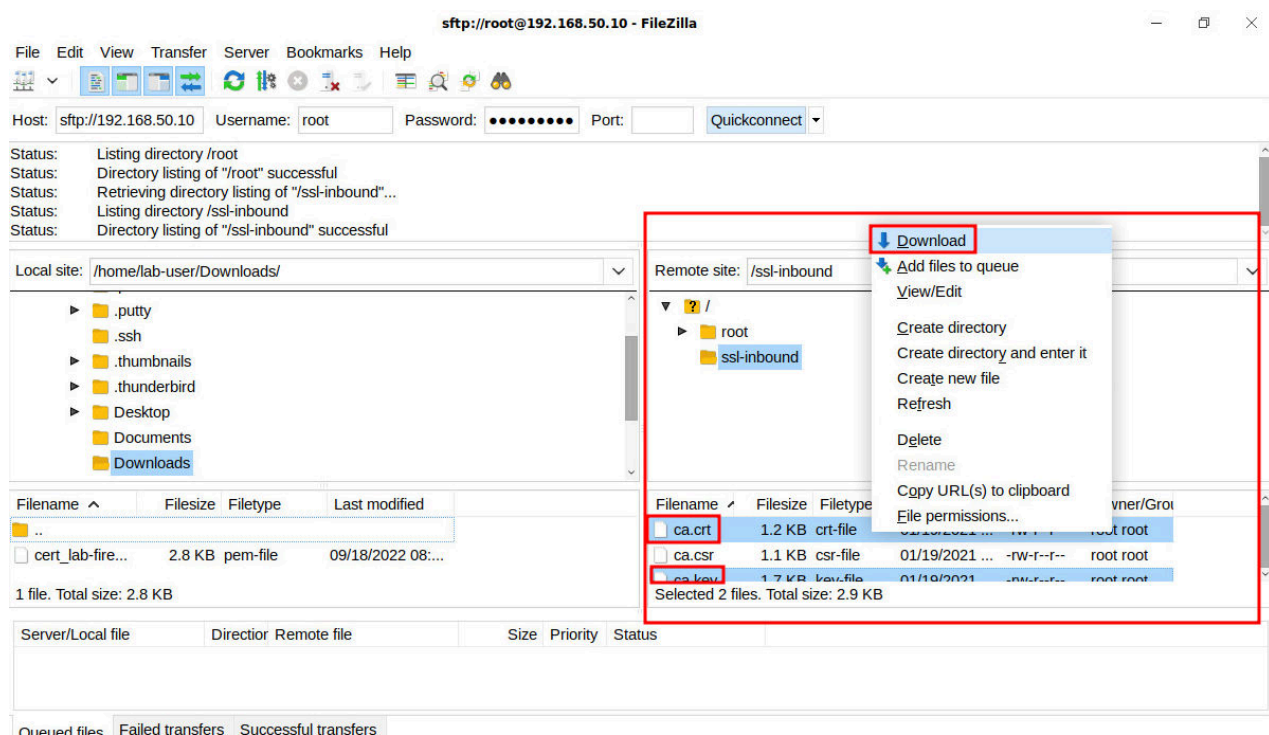
4. On the Local site, type `/home/lab-user/Downloads` in the text field. Press **Enter**.





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



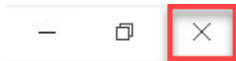
6. Press **CTRL** and **click** to highlight the filenames `ca.key` and `ca.crt`. Right-click the files and click **Download**.



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

3 files. Total size: 3.9 KB			3 files. Total size: 3.9 KB		
Server/Local file	Director	Remote file	Size	Priority	Time
sftp://root@192.168.50.10					
 /home/lab-user/Downloads/ca.crt	<<--	/ssl-inbound/ca.crt	1.2 KB	Normal	01/19/2021 03:29:3...
 /home/lab-user/Downloads/ca.key	<<--	/ssl-inbound/ca.key	1.7 KB	Normal	01/19/2021 03:29:3...
Queued files			Failed transfers		
			Successful transfers (2)		

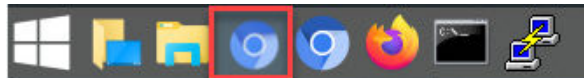
- Click the **X** in the upper-right to close *FileZilla*.



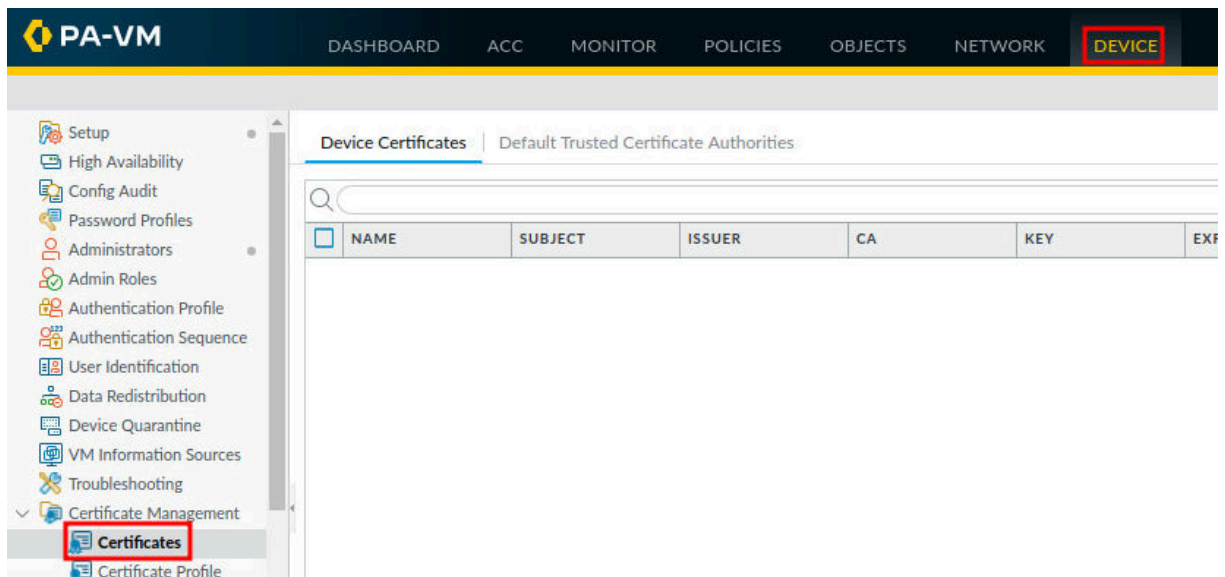
1.2 Import SSL Certificate

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.

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



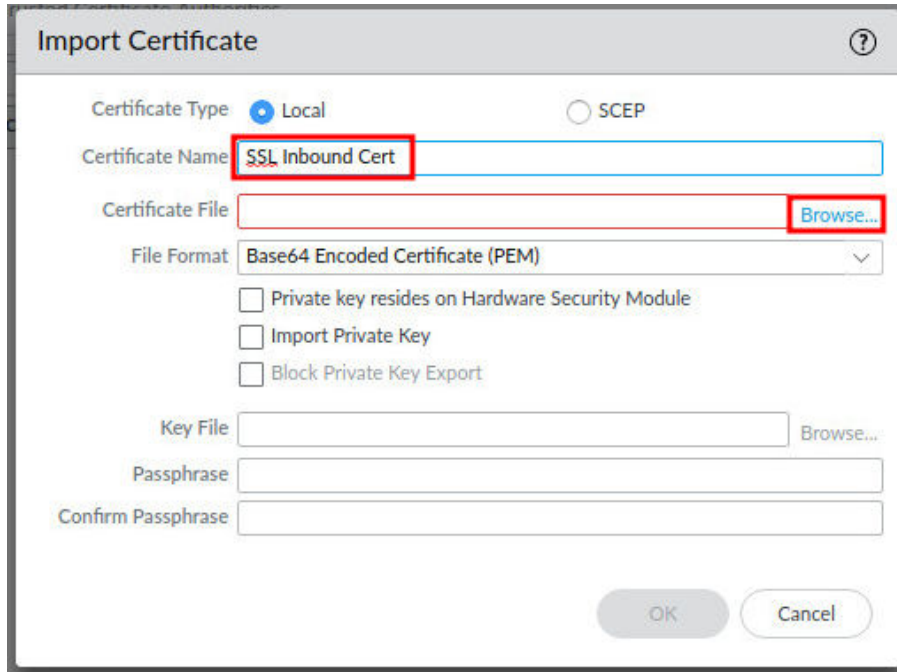
- Navigate to **Device > Certificate Management > Certificates**.



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



- In the *Import Certificate* window, type **SSL Inbound Cert**. Then, click **Browse...**

A dialog box titled "Import Certificate" with a question mark icon. It has two radio buttons for "Certificate Type": "Local" (selected) and "SCEP". Below is a text field for "Certificate Name" containing "SSL Inbound Cert" (highlighted with a red box). Below that is a text field for "Certificate File" with a "Browse..." button (highlighted with a red box). A dropdown menu for "File Format" is set to "Base64 Encoded Certificate (PEM)". There are three checkboxes: "Private key resides on Hardware Security Module", "Import Private Key", and "Block Private Key Export". Below these are text fields for "Key File" (with a "Browse..." button), "Passphrase", and "Confirm Passphrase". At the bottom are "OK" and "Cancel" buttons.

Import Certificate

Certificate Type ☒ Local ☐ SCEP

Certificate Name **SSL Inbound Cert**

Certificate File **Browse...**

File Format Base64 Encoded Certificate (PEM)

☐ Private key resides on Hardware Security Module

☐ Import Private Key

☐ Block Private Key Export

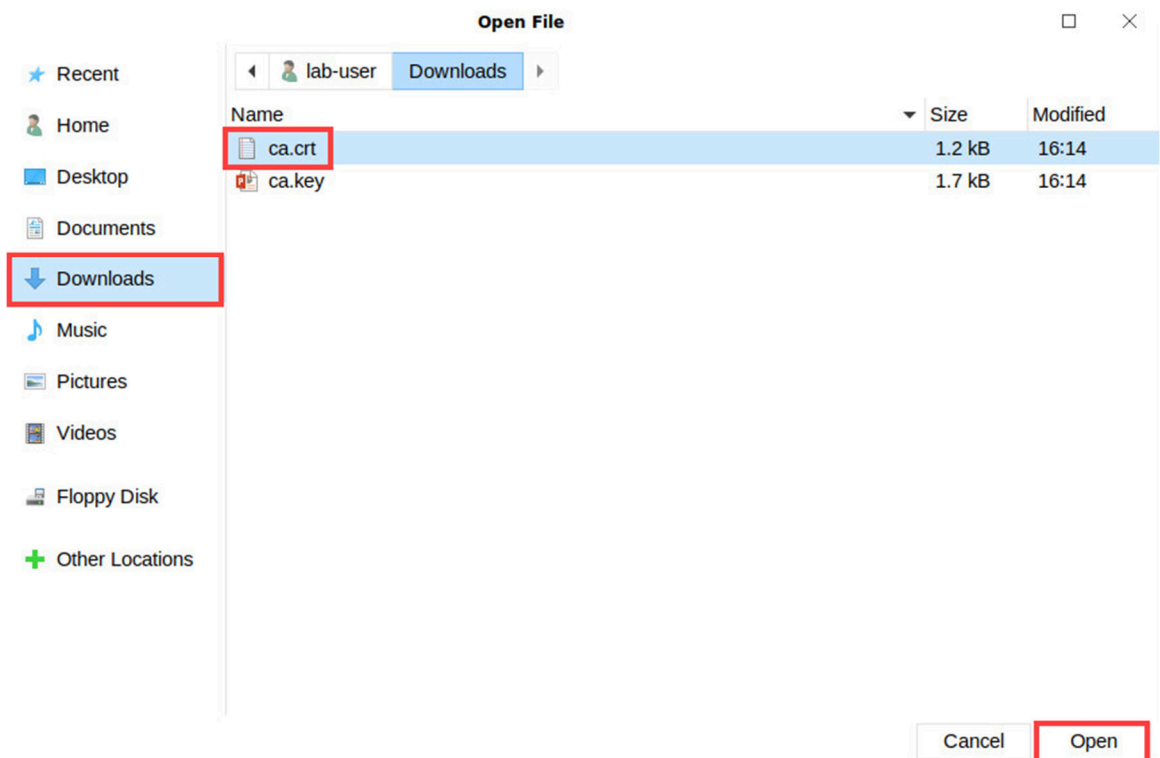
Key File Browse...

Passphrase

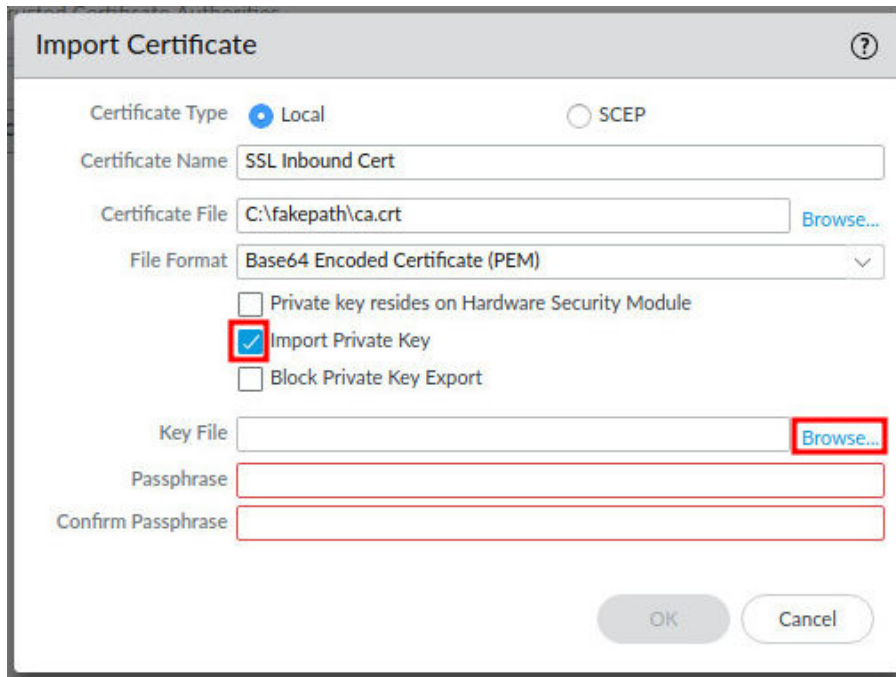
Confirm Passphrase

OK Cancel

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

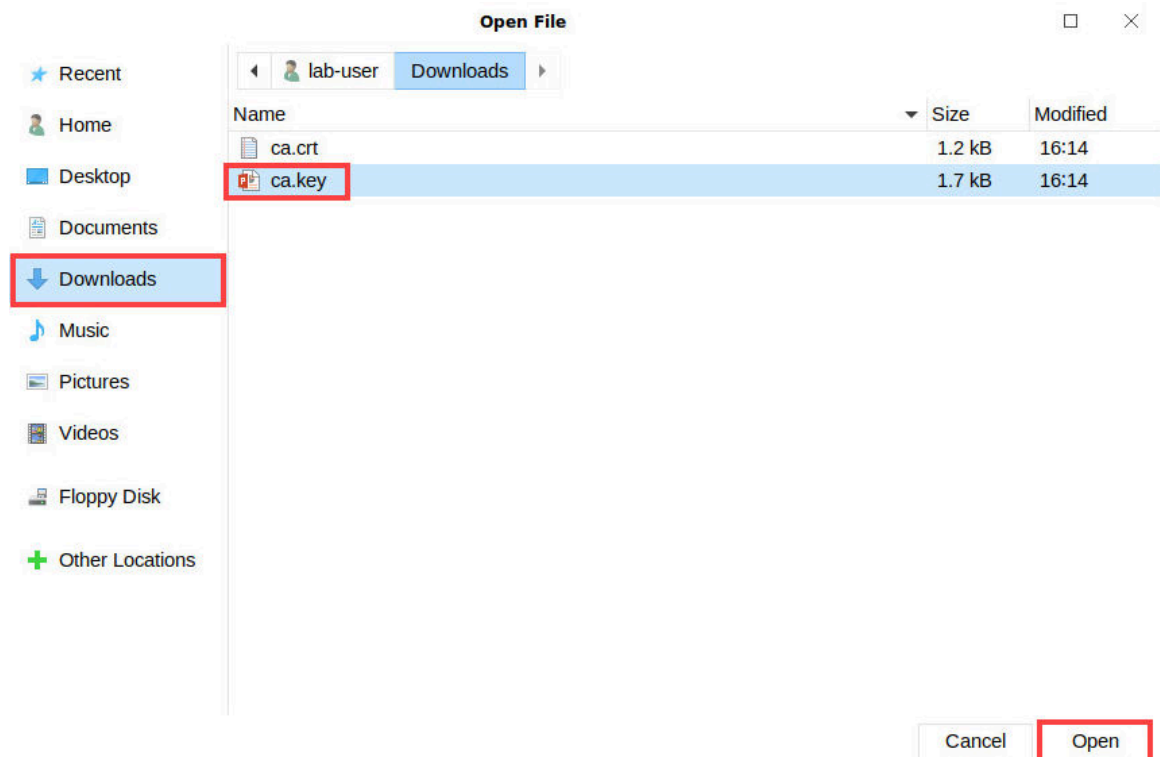


6. Click the checkbox for **Import private key**. Then, click **Browse...**

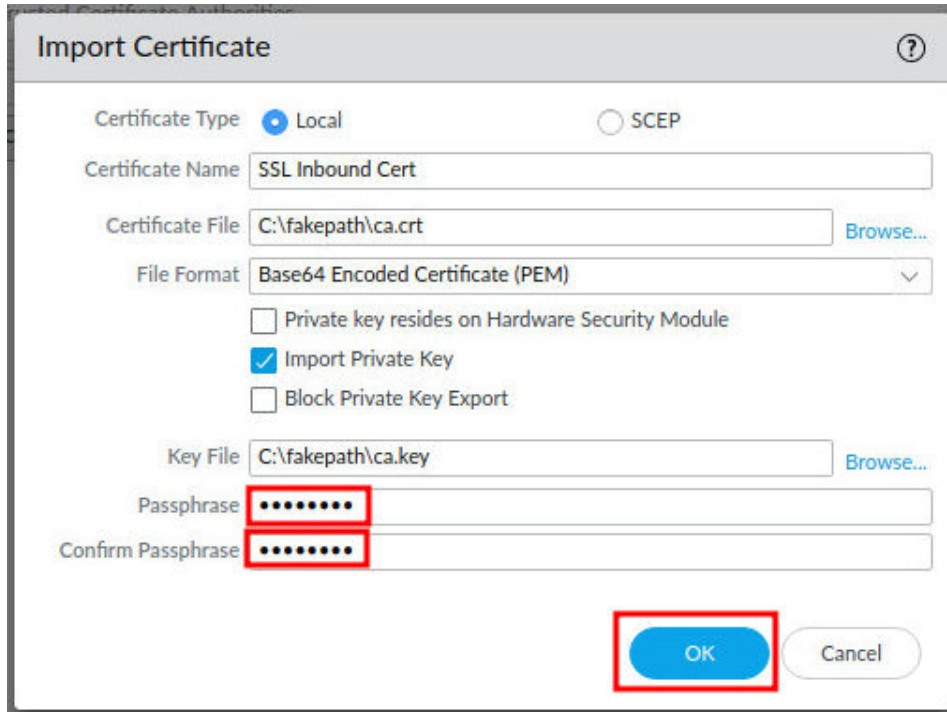


The 'Import Certificate' dialog box is shown. The 'Certificate Type' is set to 'Local'. The 'Certificate Name' is 'SSL Inbound Cert'. The 'Certificate File' is 'C:\fakepath\ca.crt'. The 'File Format' is 'Base64 Encoded Certificate (PEM)'. The 'Import Private Key' checkbox is checked. The 'Key File' field is empty, and the 'Browse...' button next to it is highlighted with a red box. The 'Passphrase' and 'Confirm Passphrase' fields are also empty. The 'OK' and 'Cancel' buttons are at the bottom right.

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

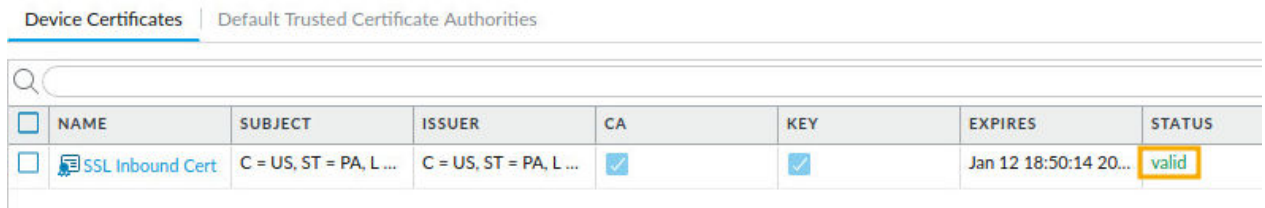


8. In the *Import Certificate* window, type `pa1oal1to` for the *Passphrase* and *Confirm Passphrase* fields. Then, click the **OK** button.



The **Import Certificate** dialog box is shown. It has a title bar with a question mark icon. The **Certificate Type** is set to **Local** (selected with a radio button). The **Certificate Name** is `SSL Inbound Cert`. The **Certificate File** is `C:\fakepath\ca.crt` with a **Browse...** button. The **File Format** is **Base64 Encoded Certificate (PEM)** (selected in a dropdown). There are three checkboxes: **Private key resides on Hardware Security Module** (unchecked), **Import Private Key** (checked), and **Block Private Key Export** (unchecked). The **Key File** is `C:\fakepath\ca.key` with a **Browse...** button. The **Passphrase** and **Confirm Passphrase** fields are both filled with dots and are highlighted with red rectangles. The **OK** button is highlighted with a red rectangle, and the **Cancel** button is also visible.

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



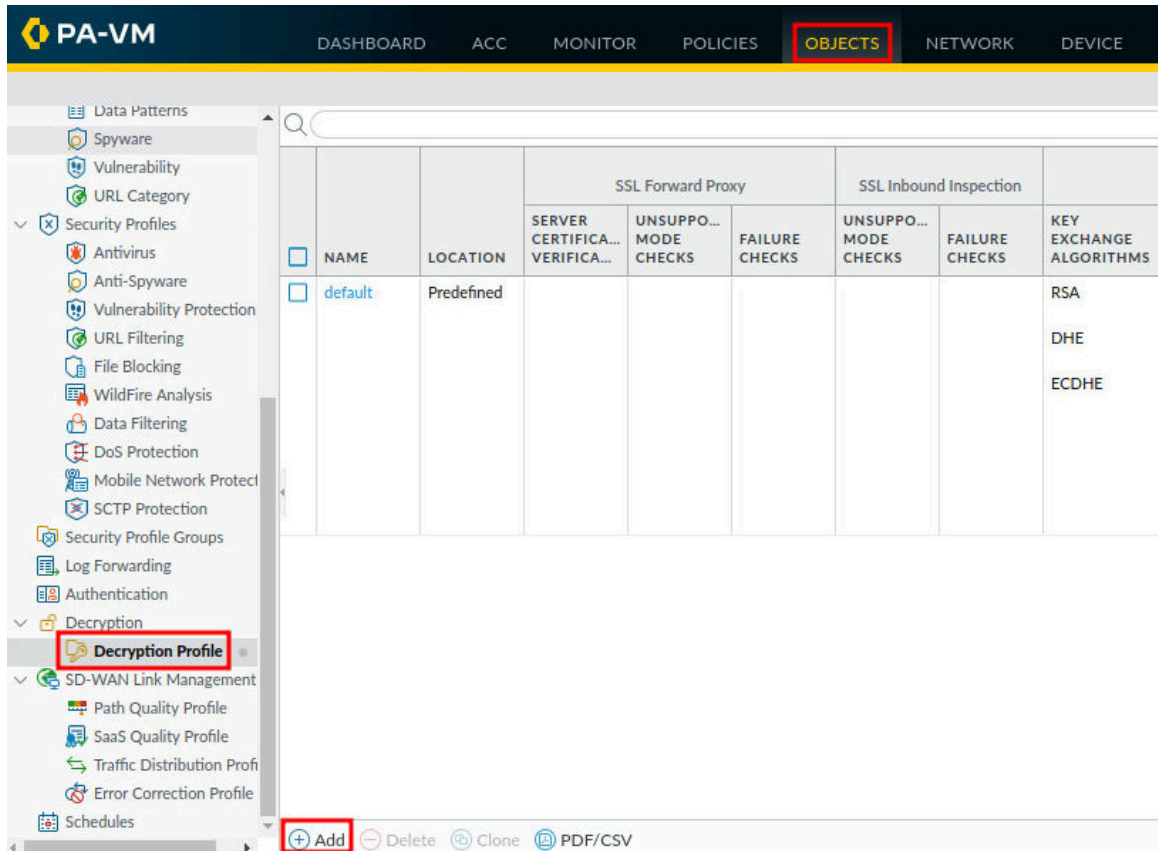
The **Device Certificates** tab is selected. The table shows the following information:

	NAME	SUBJECT	ISSUER	CA	KEY	EXPIRES	STATUS
<input type="checkbox"/>	SSL Inbound Cert	C = US, ST = PA, L ...	C = US, ST = PA, L ...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Jan 12 18:50:14 20...	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.

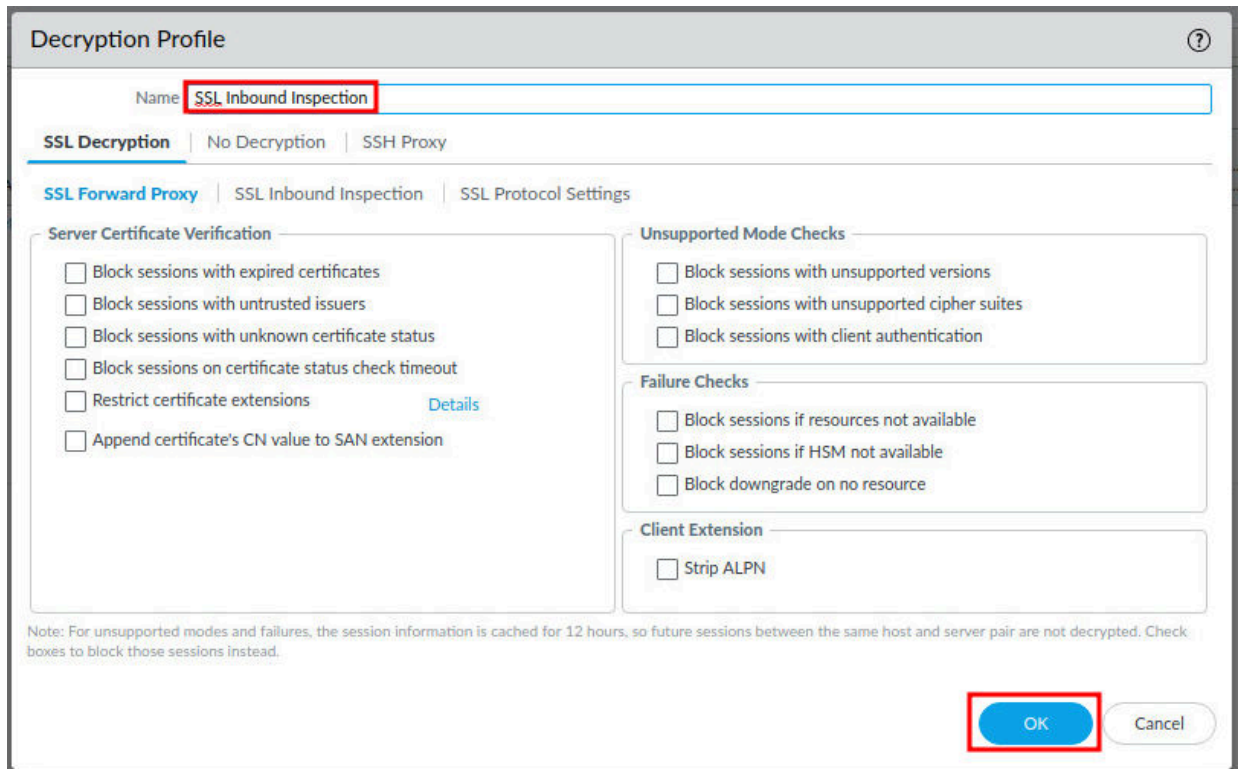
1. Navigate to **Objects > Decryption > Decryption Profile > Add**. You may need to scroll down in the left pane.



The screenshot shows the PA-VM web interface. The top navigation bar includes 'DASHBOARD', 'ACC', 'MONITOR', 'POLICIES', 'OBJECTS' (highlighted with a red box), 'NETWORK', and 'DEVICE'. The left sidebar contains a tree view of configuration categories. Under 'Decryption', the 'Decryption Profile' option is highlighted with a red box. The main content area displays a table for 'Decryption Profile' settings. The table has columns for 'NAME', 'LOCATION', 'SERVER CERTIFICA... VERIFICA...', 'UNSUPPO... MODE CHECKS', 'FAILURE CHECKS', 'UNSUPPO... MODE CHECKS', 'FAILURE CHECKS', and 'KEY EXCHANGE ALGORITHMS'. A single row is visible with the name 'default' and location 'Predefined'. The 'KEY EXCHANGE ALGORITHMS' column lists 'RSA', 'DHE', and 'ECDHE'. At the bottom of the interface, there is a toolbar with buttons: '+ Add' (highlighted with a red box), 'Delete', 'Clone', and 'PDF/CSV'.

NAME	LOCATION	SSL Forward Proxy			SSL Inbound Inspection		KEY EXCHANGE ALGORITHMS
		SERVER CERTIFICA... VERIFICA...	UNSUPPO... MODE CHECKS	FAILURE CHECKS	UNSUPPO... MODE CHECKS	FAILURE CHECKS	
default	Predefined						RSA DHE ECDHE

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



Decryption Profile

Name: **SSL Inbound Inspection**

SSL Decryption | No Decryption | SSH Proxy

SSL Forward Proxy | **SSL Inbound Inspection** | SSL Protocol Settings

Server Certificate Verification

- ☐ Block sessions with expired certificates
- ☐ Block sessions with untrusted issuers
- ☐ Block sessions with unknown certificate status
- ☐ Block sessions on certificate status check timeout
- ☐ Restrict certificate extensions [Details](#)
- ☐ Append certificate's CN value to SAN extension

Unsupported Mode Checks

- ☒ Block sessions with unsupported versions
- ☐ Block sessions with unsupported cipher suites
- ☐ Block sessions with client authentication

Failure Checks

- ☒ Block sessions if resources not available
- ☐ Block sessions if HSM not available
- ☐ Block downgrade on no resource

Client Extension

- ☒ Strip ALPN

Note: For unsupported modes and failures, the session information is cached for 12 hours, so future sessions between the same host and server pair are not decrypted. Check boxes to block those sessions instead.

OK Cancel

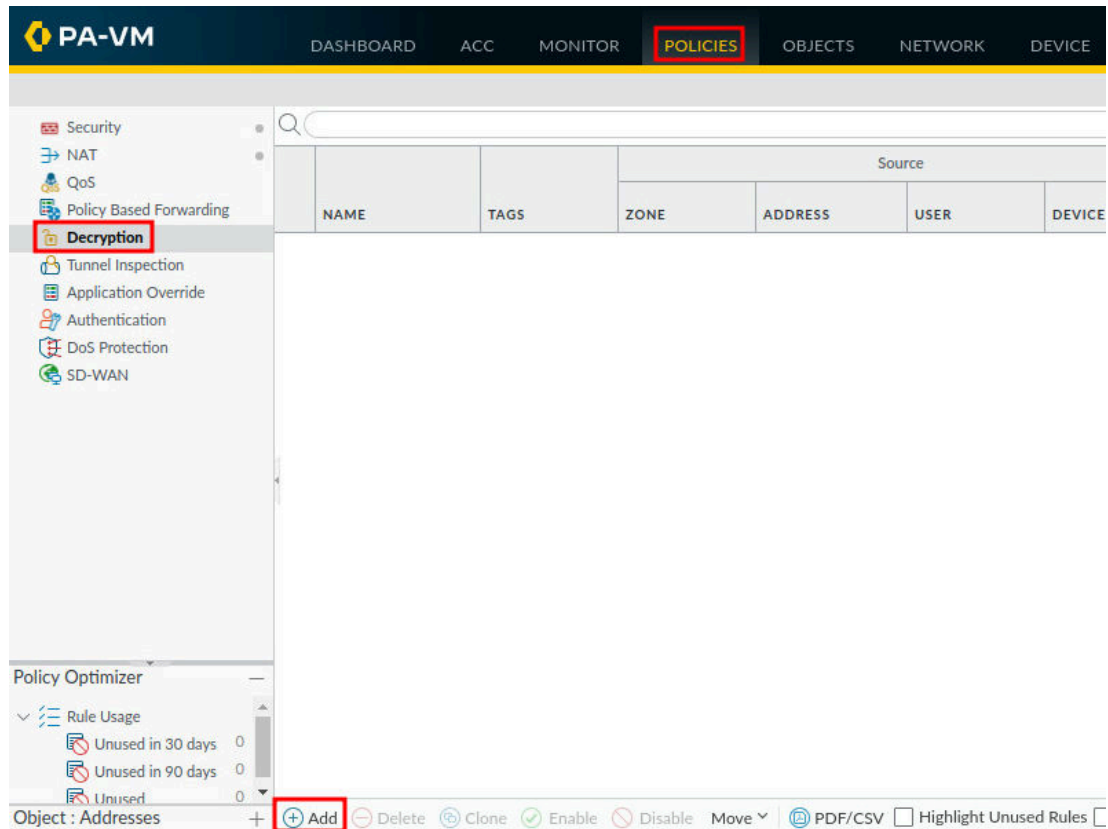
- Verify the **SSL Inbound Inspection** Decryption Profile was created.

	NAME	LOCATION	SSL Forward Proxy			SSL Inbound Inspection		SSL Protocol Settings			
			SERVER CERTIFICA... VERIFICA...	UNSUPPO... MODE CHECKS	FAILURE CHECKS	UNSUPPO... MODE CHECKS	FAILURE CHECKS	KEY EXCHANGE ALGORITHMS	PROTOCOL VERSIONS	ENCRYPTION ALGORITHMS	AUTHENTI... ALGORITH...
<input type="checkbox"/>	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
<input checked="" type="checkbox"/>	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

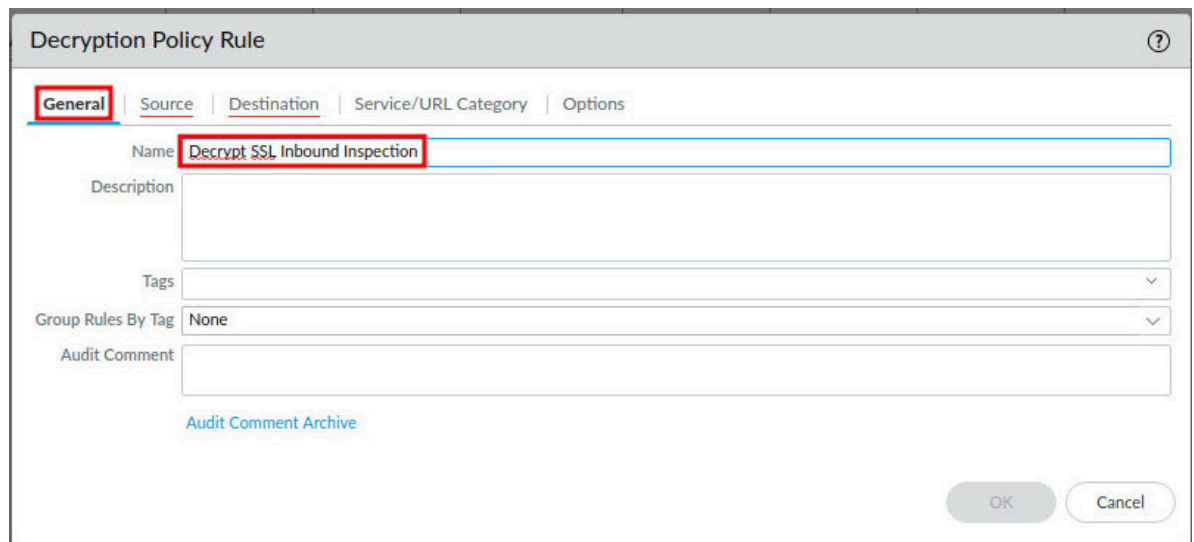
1.4 Create a Decryption Policy

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.

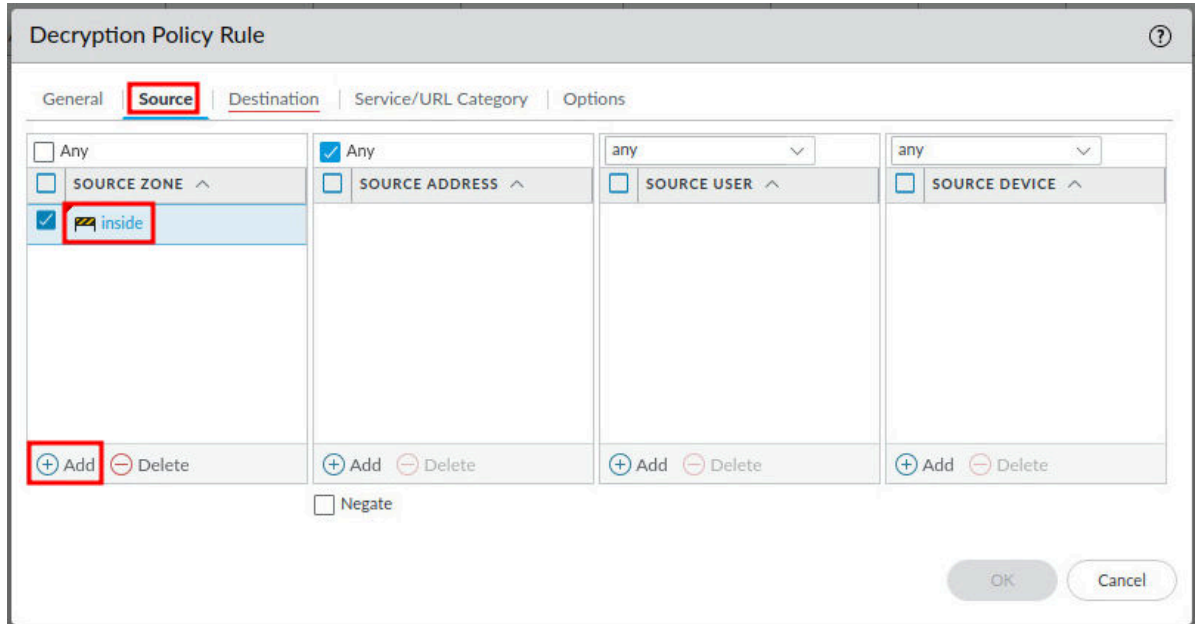
1. Navigate to **Policies > Decryption > Add**.



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

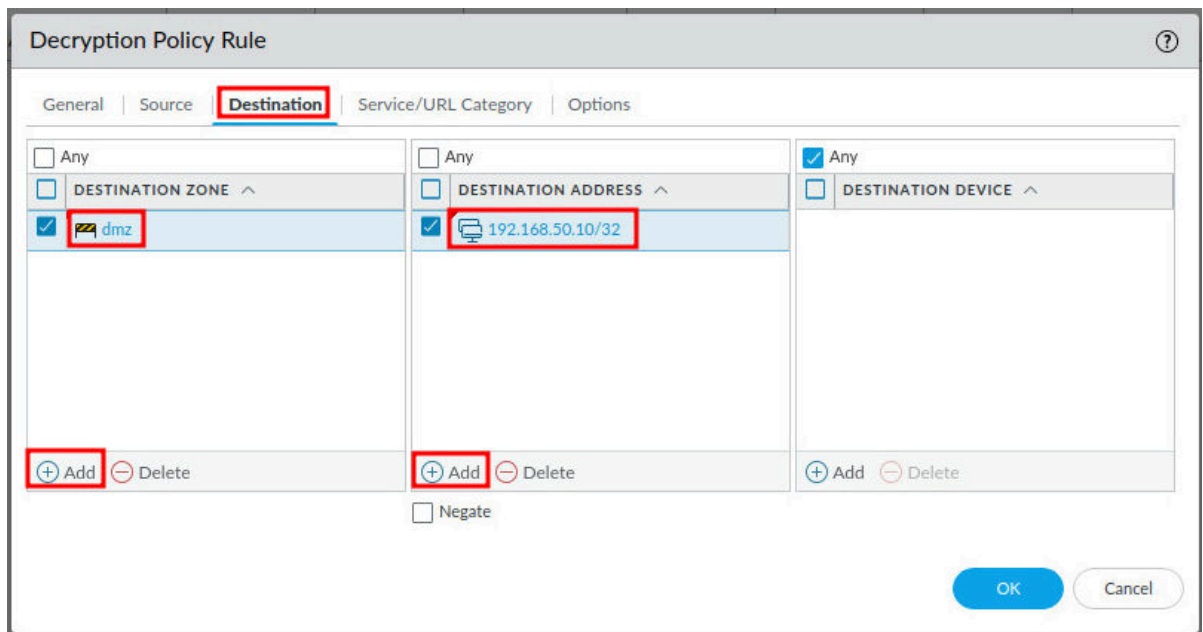


3. In the *Decryption Policy Rule* window, click on the **Source** tab. Then, click **Add** in the *Source Zone* section. Next, select **inside**.



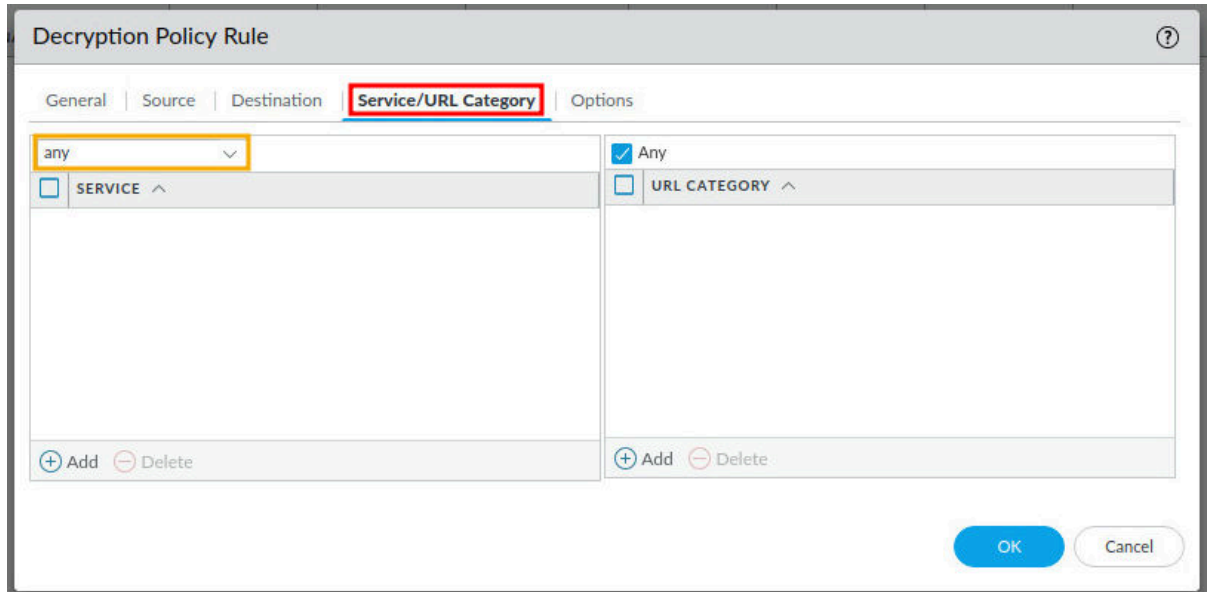
The screenshot shows the 'Decryption Policy Rule' window with the 'Source' tab selected. The 'SOURCE ZONE' section has a list with 'Any' and 'inside'. The 'inside' entry is selected and highlighted with a red box. Below the list, the '+ Add' button is also highlighted with a red box. The 'SOURCE ADDRESS', 'SOURCE USER', and 'SOURCE DEVICE' sections are empty. The 'Negate' checkbox is unchecked. The 'OK' and 'Cancel' buttons are at the bottom right.

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**.



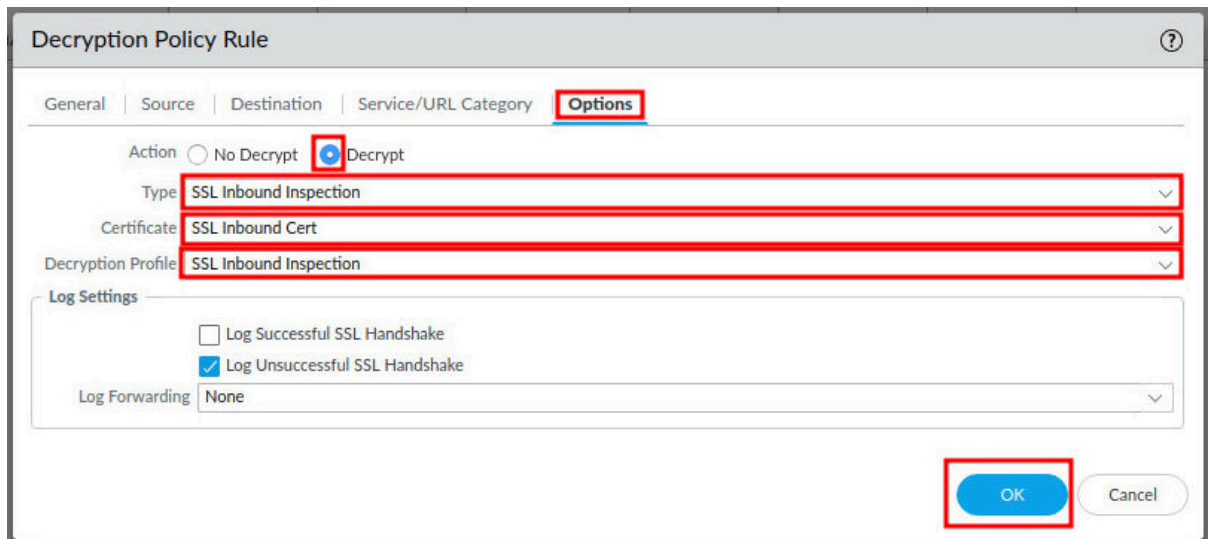
The screenshot shows the 'Decryption Policy Rule' window with the 'Destination' tab selected. The 'DESTINATION ZONE' section has a list with 'Any' and 'dmz'. The 'dmz' entry is selected and highlighted with a red box. Below the list, the '+ Add' button is also highlighted with a red box. The 'DESTINATION ADDRESS' section has a list with 'Any' and '192.168.50.10/32'. The '192.168.50.10/32' entry is selected and highlighted with a red box. Below the list, the '+ Add' button is also highlighted with a red box. The 'DESTINATION DEVICE' section is empty. The 'Negate' checkbox is unchecked. The 'OK' and 'Cancel' buttons are at the bottom right.

- 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.



The screenshot shows the 'Decryption Policy Rule' window with the 'Service/URL Category' tab selected. The 'any' option is selected in the 'SERVICE' dropdown menu. The 'URL CATEGORY' dropdown is also visible, showing 'Any' selected. The 'Add' and 'Delete' buttons are at the bottom of each pane.

- 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.



The screenshot shows the 'Decryption Policy Rule' window with the 'Options' tab selected. The 'Action' is set to 'Decrypt'. The 'Type' dropdown is set to 'SSL Inbound Inspection', the 'Certificate' dropdown is set to 'SSL Inbound Cert', and the 'Decryption Profile' dropdown is set to 'SSL Inbound Inspection'. The 'Log Settings' section shows 'Log Unsuccessful SSL Handshake' checked. The 'Log Forwarding' is set to 'None'. The 'OK' button is highlighted.

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

	NAME	TAGS	Source				Destination			URL CATEGORY
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	
1	Decrypt SSL Inbound...	none	inside	any	any	any	dmz	192.168.50.10...	any	any

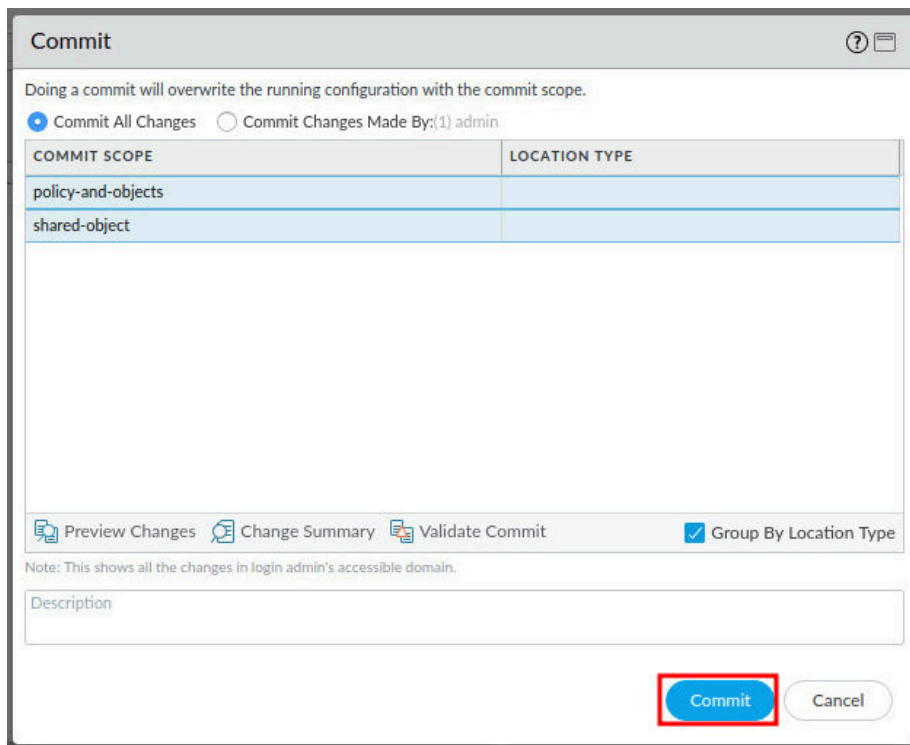
1.5 Commit and Test Decryption Policy

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

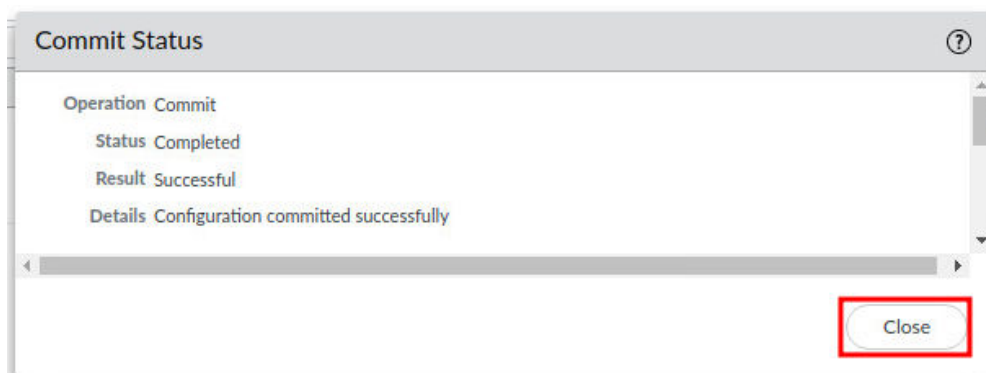
1. Click the **Commit** link located at the top-right of the web interface.



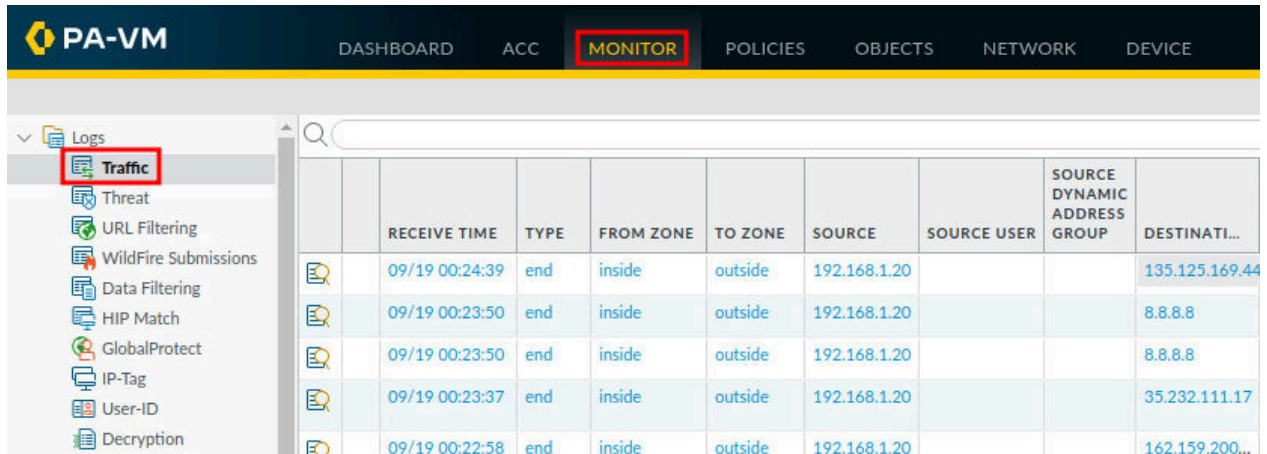
2. In the *Commit* window, click **Commit** to proceed with committing the changes.



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



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

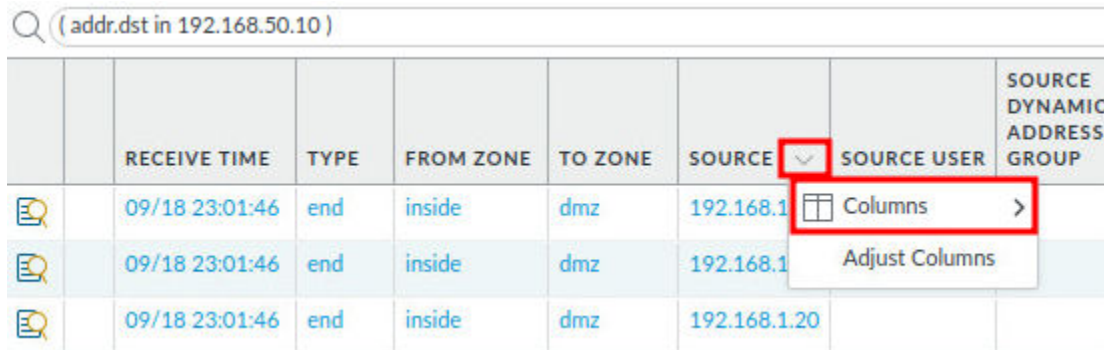


	RECEIVE TIME	TYPE	FROM ZONE	TO ZONE	SOURCE	SOURCE USER	SOURCE DYNAMIC ADDRESS GROUP	DESTINATION
	09/19 00:24:39	end	inside	outside	192.168.1.20			135.125.169.44
	09/19 00:23:50	end	inside	outside	192.168.1.20			8.8.8.8
	09/19 00:23:50	end	inside	outside	192.168.1.20			8.8.8.8
	09/19 00:23:37	end	inside	outside	192.168.1.20			35.232.111.17
	09/19 00:22:58	end	inside	outside	192.168.1.20			162.159.200...

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

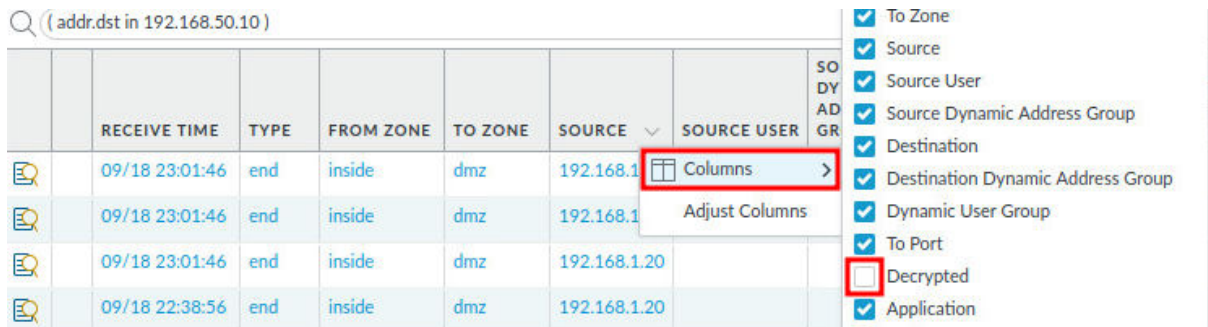
(addr.dst in 192.168.50.10)

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



	RECEIVE TIME	TYPE	FROM ZONE	TO ZONE	SOURCE	SOURCE USER	SOURCE DYNAMIC ADDRESS GROUP
	09/18 23:01:46	end	inside	dmz	192.168.1.20		
	09/18 23:01:46	end	inside	dmz	192.168.1.20		
	09/18 23:01:46	end	inside	dmz	192.168.1.20		

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



	RECEIVE TIME	TYPE	FROM ZONE	TO ZONE	SOURCE	SOURCE USER	SOURCE DYNAMIC ADDRESS GROUP
	09/18 23:01:46	end	inside	dmz	192.168.1.20		
	09/18 23:01:46	end	inside	dmz	192.168.1.20		
	09/18 23:01:46	end	inside	dmz	192.168.1.20		
	09/18 22:38:56	end	inside	dmz	192.168.1.20		

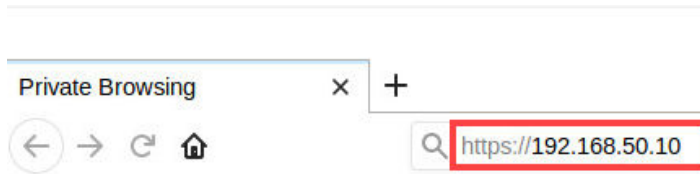


The **Decrypted** checkbox might be listed alphabetically among the unchecked boxes in the lower part of the menu

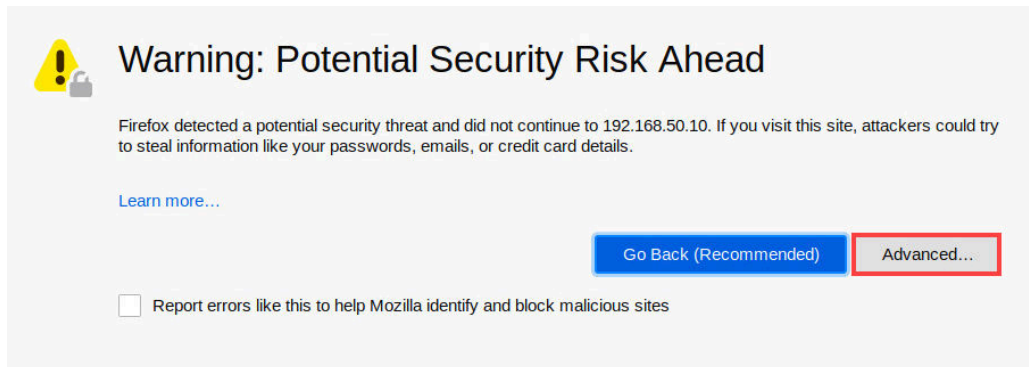
8. Open the *Firefox Web Browser* by clicking on the **Firefox** icon located in the task bar.



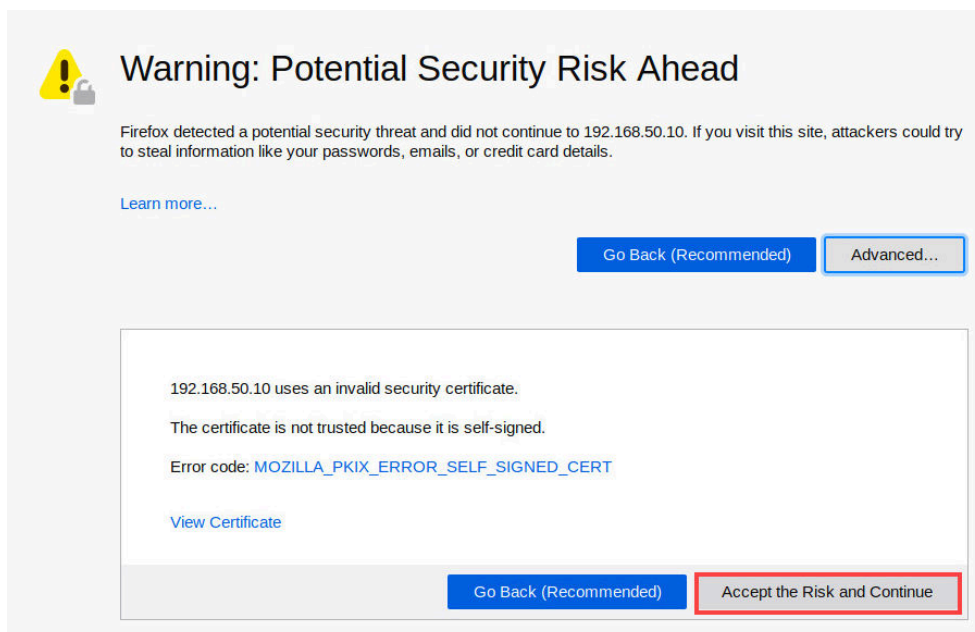
9. In the address bar, type `https://192.168.50.10` and click **Enter**.



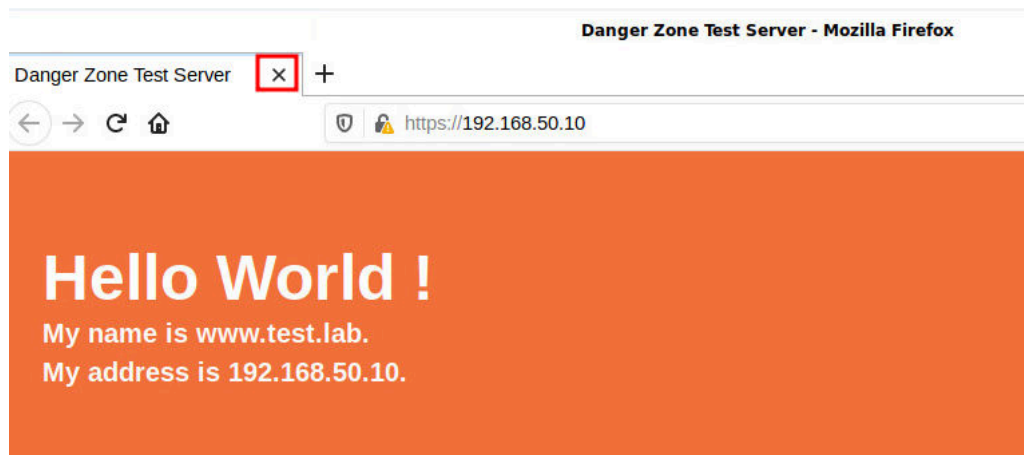
10. You will see a “Warning: Potential Security Risk Ahead” message. Click on the **Advanced** button.



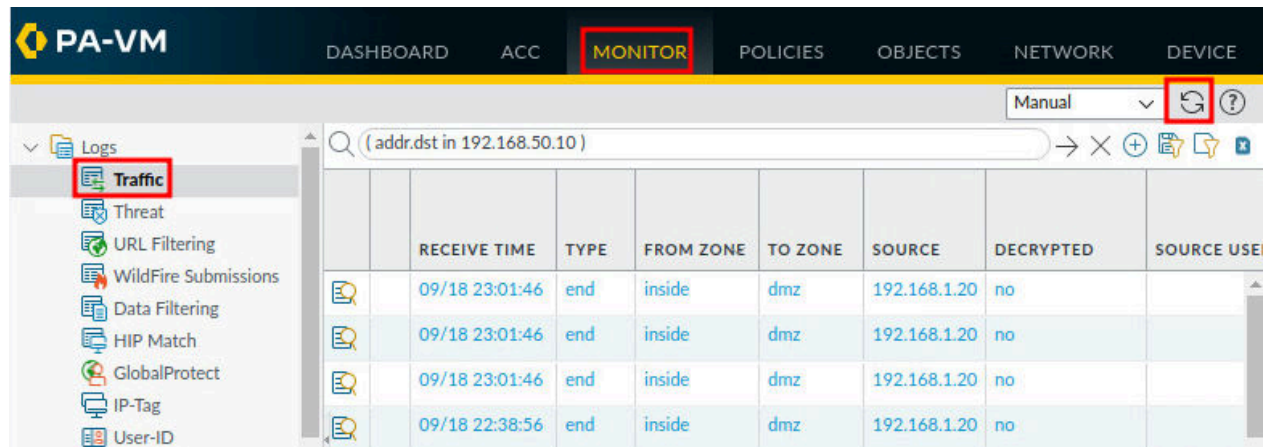
11. Click on **Accept the Risk and Continue**.



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**.

Q (addr.dst in 192.168.50.10)														
	RECEIVE TIME	TYPE	FROM ZONE	TO ZONE	SOURCE	DECRYPTED	SOURCE USER	SOURCE DYNAMIC ADDRESS GROUP	DESTINATI...	DESTINATION DYNAMIC ADDRESS GROUP	DYNAMIC USER GROUP	TO PORT	APPLICATI...	ACTION
	09/19 00:37:13	end	inside	dmz	192.168.1.20	yes			192.168.50.10			443	web-browsing	allow
	09/19 00:36:45	deny	inside	dmz	192.168.1.20	yes			192.168.50.10			443	ssl	allow

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.

Detailed Log View

General	Source	Destination
Session ID 2369 Action allow Action Source from-policy Host ID Application ssl Rule Allow-Inside-DMZ Rule UUID de443dfb-35aa-41e9-a290-22238efdab47 Session End Reason policy-deny Category any Device SN IP Protocol tcp Log Action Generated Time 2022/09/19 00:36:45	Source User Source 192.168.1.20 Source DAG Country 192.168.0.0-192.168.255.255 Port 43460 Zone inside Interface ethernet1/2 X-Forwarded-For IP 0.0.0.0	Destination User Destination 192.168.50.10 Destination DAG Country 192.168.0.0-192.168.255.255 Port 443 Zone dmz Interface ethernet1/3
Flags Captive Portal <input type="checkbox"/> Proxy Transaction <input type="checkbox"/> Decrypted <input checked="" type="checkbox"/>		

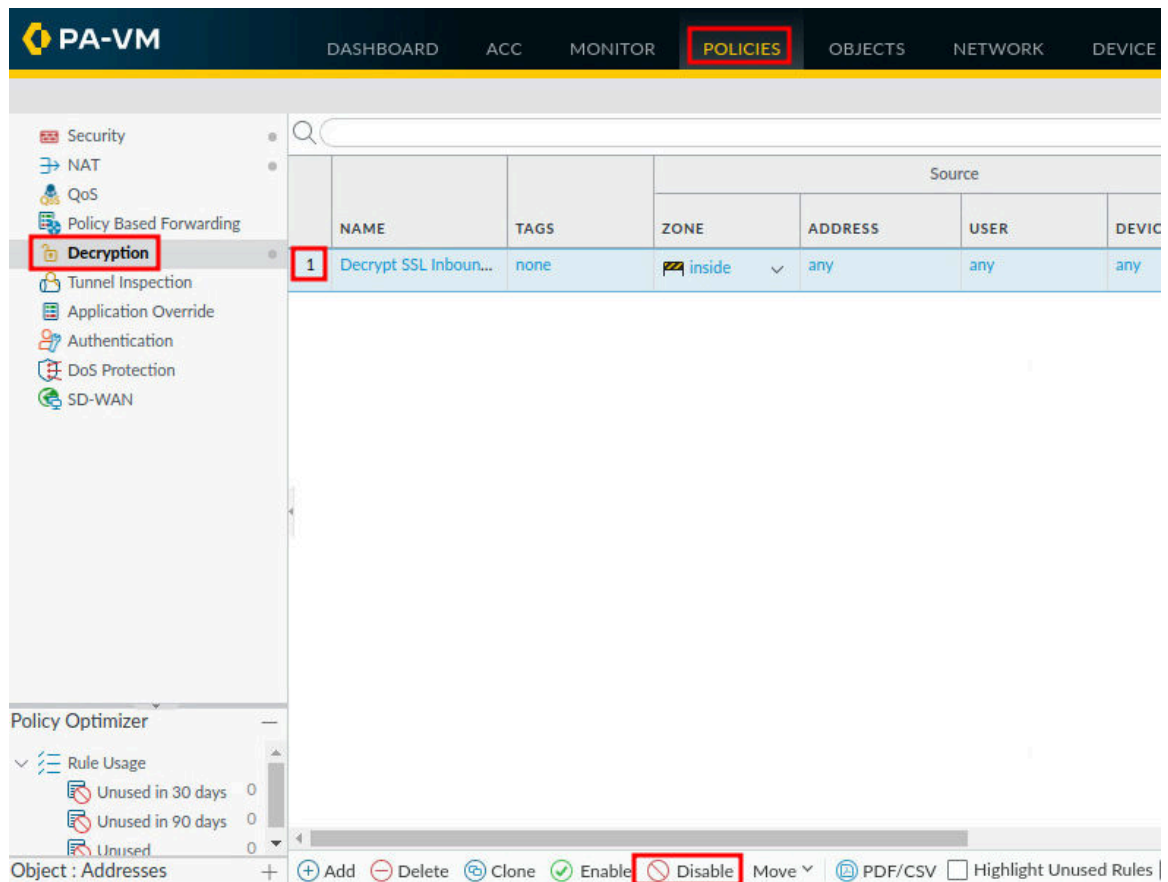
PCAP	RECEIVE TIME	TYPE	APPLICAT...	ACTION	RULE	RULE UUID	BY...	SEVERI...	CATEG...	URL CATEG... LIST	VERDI...	URL	FILE NAME
	2022/09/19 00:36:45	deny	ssl	allow	Allow-Inside-DMZ	de443...	4019		any				

Close

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.

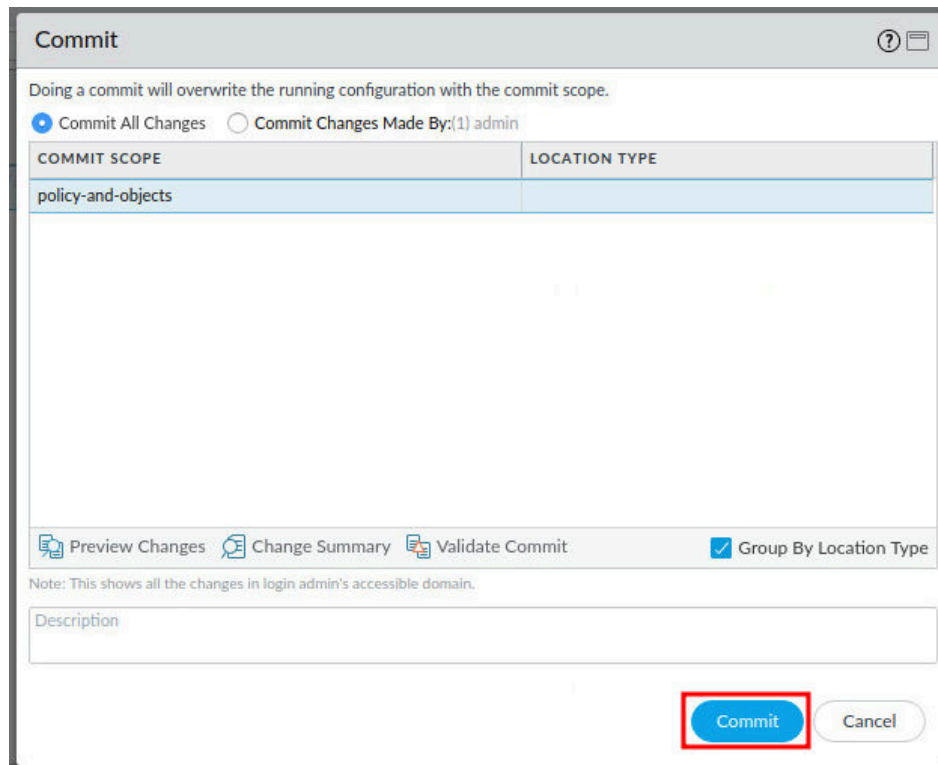
1. Navigate to **Policies > Decryption**. Then, click the **1** for the **Decrypt SSL Inbound Inspection** policy. **Next**, click the **Disable** button.



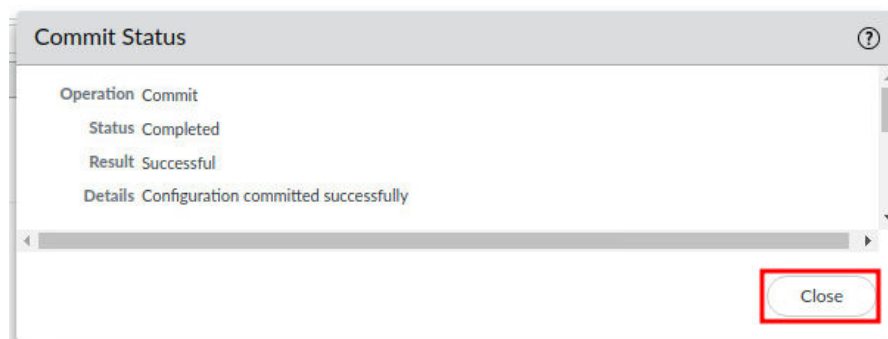
2. Click the **Commit** link located at the top-right of the web interface.



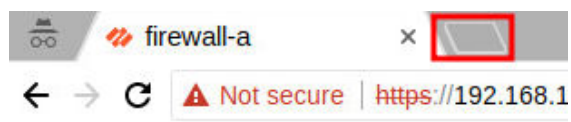
3. In the *Commit* window, click **Commit** to proceed with committing the changes.



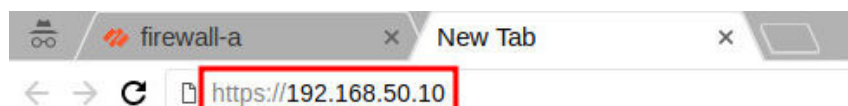
4. When the commit operation successfully completes, click **Close** to continue.



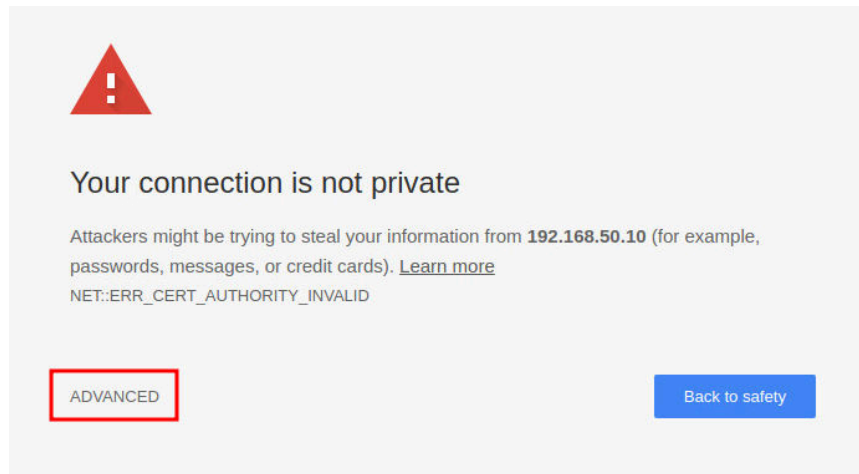
5. Click the **New tab** button in *Chromium*.



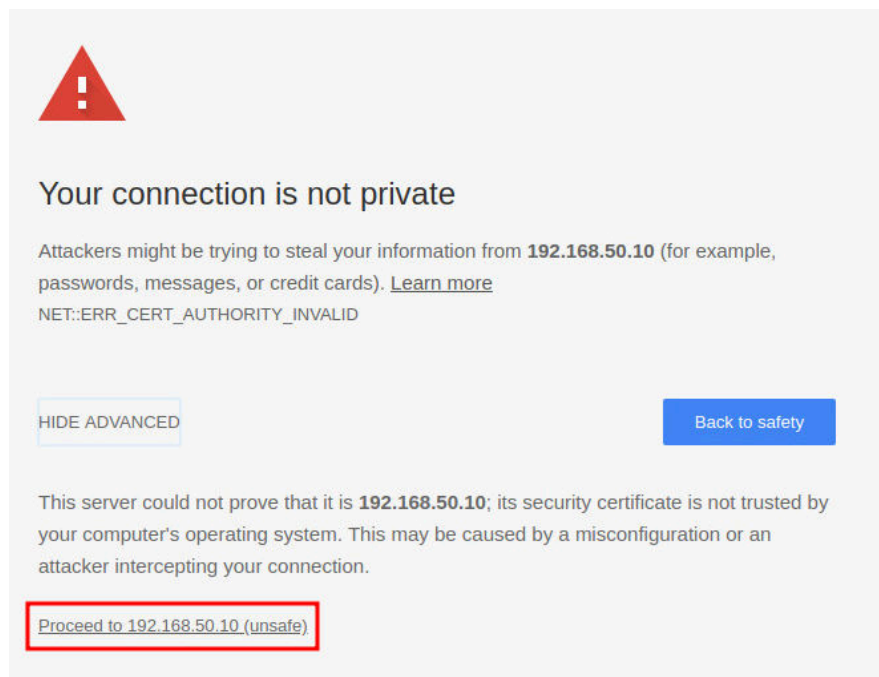
6. In the address bar, type `https://192.168.50.10` and click **Enter**.



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



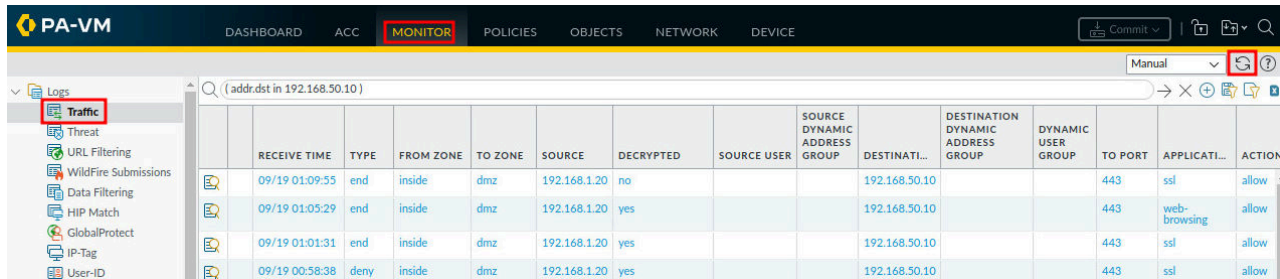
8. Click on **Proceed to 192.168.50.10 (unsafe)**.



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

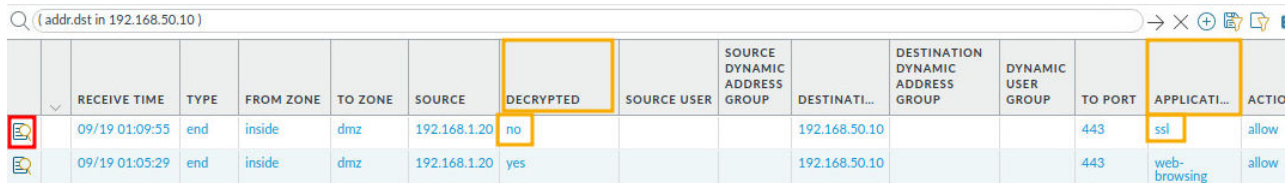


10. Navigate to **Monitor > Logs > Traffic**. Then, click the **refresh** icon.



	RECEIVE TIME	TYPE	FROM ZONE	TO ZONE	SOURCE	DECRYPTED	SOURCE USER	SOURCE DYNAMIC ADDRESS GROUP	DESTINATION DYNAMIC ADDRESS GROUP	DYNAMIC USER GROUP	TO PORT	APPLICATION	ACTION
	09/19 01:09:55	end	inside	dmz	192.168.1.20	no			192.168.50.10		443	ssl	allow
	09/19 01:05:29	end	inside	dmz	192.168.1.20	yes			192.168.50.10		443	web-browsing	allow
	09/19 01:01:31	end	inside	dmz	192.168.1.20	yes			192.168.50.10		443	ssl	allow
	09/19 00:58:38	deny	inside	dmz	192.168.1.20	yes			192.168.50.10		443	ssl	allow

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**.



	RECEIVE TIME	TYPE	FROM ZONE	TO ZONE	SOURCE	DECRYPTED	SOURCE USER	SOURCE DYNAMIC ADDRESS GROUP	DESTINATION DYNAMIC ADDRESS GROUP	DYNAMIC USER GROUP	TO PORT	APPLICATION	ACTION
	09/19 01:09:55	end	inside	dmz	192.168.1.20	no			192.168.50.10		443	ssl	allow
	09/19 01:05:29	end	inside	dmz	192.168.1.20	yes			192.168.50.10		443	web-browsing	allow

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.

Detailed Log View

General	Source	Destination
<p>Session ID 2482</p> <p>Action allow</p> <p>Action Source from-policy</p> <p>Host ID</p> <p>Application ssl</p> <p>Rule Allow-Inside-DMZ</p> <p>Rule UUID de443dfb-35aa-41e9-a290-22238efdab47</p> <p>Session End Reason tcp-rst-from-client</p> <p>Category any</p> <p>Device SN</p> <p>IP Protocol tcp</p> <p>Log Action</p> <p>Generated Time 2022/09/19 01:09:55</p> <p>Start Time 2022/09/19 01:09:40</p>	<p>Source User</p> <p>Source 192.168.1.20</p> <p>Source DAG</p> <p>Country 192.168.0.0-192.168.255.255</p> <p>Port 43628</p> <p>Zone inside</p> <p>Interface ethernet1/2</p> <p>X-Forwarded-For IP 0.0.0.0</p>	<p>Destination User</p> <p>Destination 192.168.50.10</p> <p>Destination DAG</p> <p>Country 192.168.0.0-192.168.255.255</p> <p>Port 443</p> <p>Zone dmz</p> <p>Interface ethernet1/3</p>

Flags

Captive Portal ☐

Proxy Transaction ☐

Decrypted ☐

Packet Capture ☐

PCAP	RECEIVE TIME	TYPE	APPLICAT...	ACTION	RULE	RULE UUID	BY...	SEVERI...	CATEG...	URL CATEG... LIST	VERDI...	URL	FILE NAME
	2022/09/19 01:09:55	end	ssl	allow	Allow-Inside-DMZ	de443...	2770		any				

Close

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