



## NETWORK SECURITY FUNDAMENTALS V2

### Lab 7: Decrypting SSL Inbound Traffic

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

Copyright © 2022 Network Development Group, Inc.  
[www.netdevgroup.com](http://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

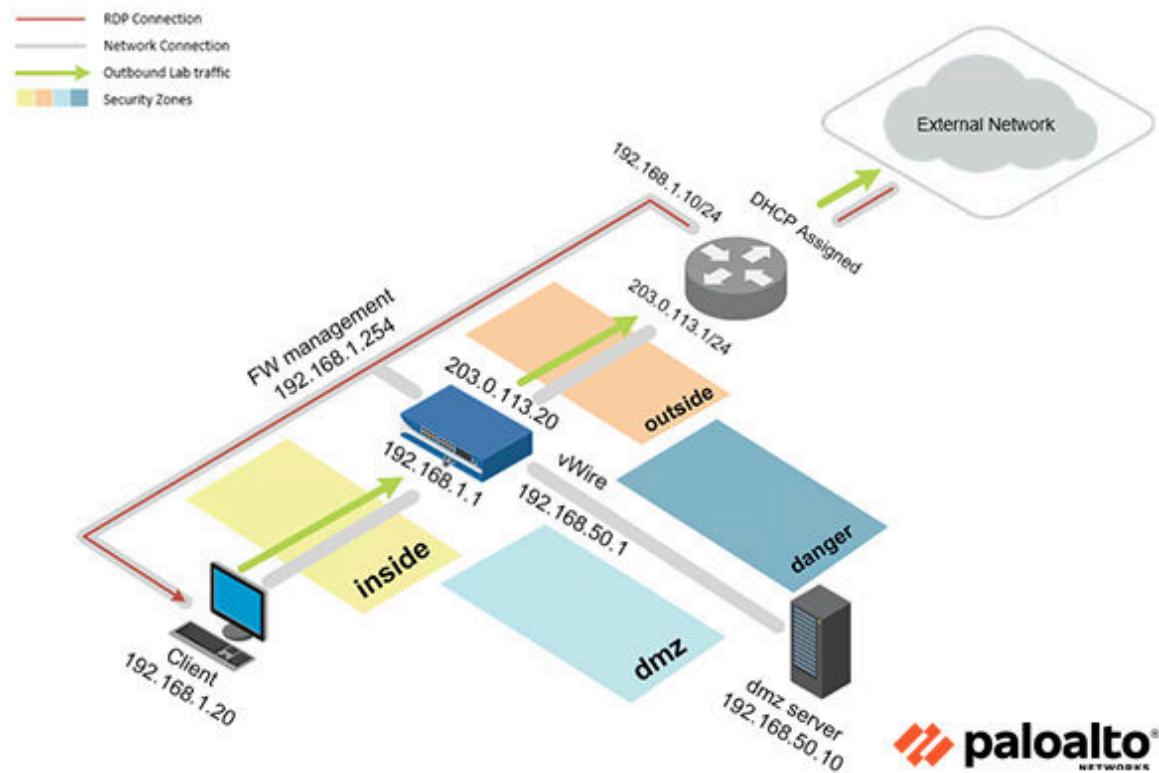
In this lab, you will decrypt SSL inbound traffic and inspect SSL traffic from the Client machine to the DMZ server. When the SSL server certificate is loaded on the Firewall, and an SSL decryption policy is configured for the inbound traffic, the device can then decrypt and read the traffic as it forwards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



 paloalto<sup>®</sup>  
NETWORKS

## 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	PaloAlt0!
DMZ	192.168.50.10	root	PaloAlt0!
Firewall	192.168.1.254	admin	PaloAlt0!

## 1 Decryption SSL Inbound Traffic

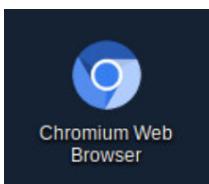
### 1.0 Load Lab Configuration

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

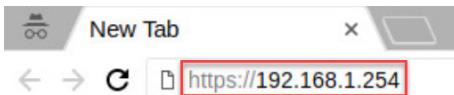
1. Click on the **Client** tab to access the Client PC.



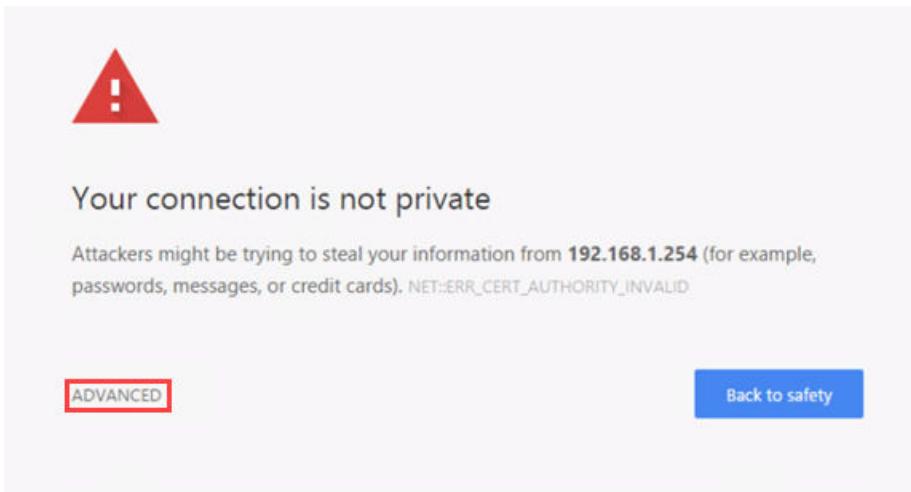
2. Log in to the Client PC as username lab-user, password PaloAlt0!.
3. Double-click the **Chromium Web Browser** icon located on the desktop.



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

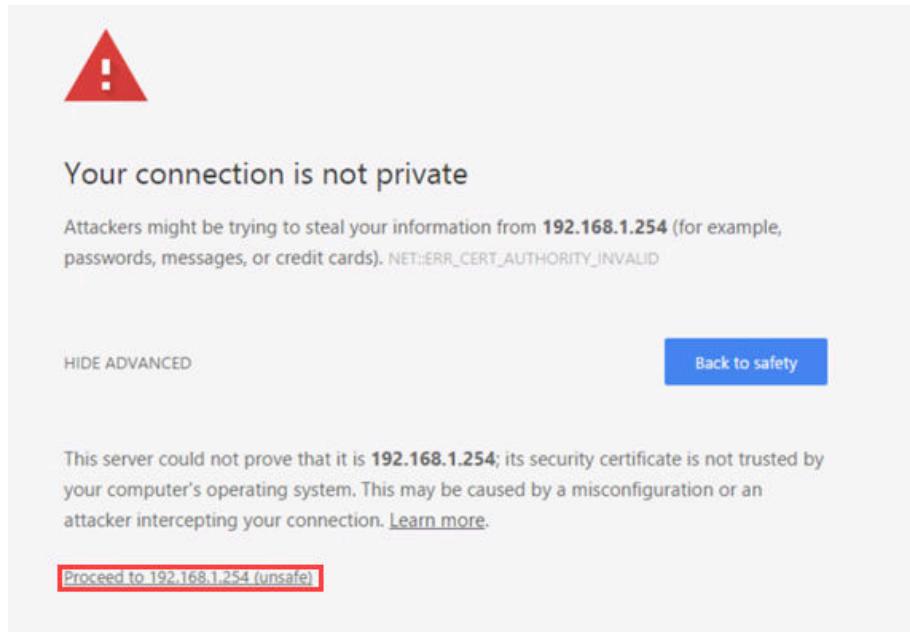


5. You will see a “Your connection is not private” message. Click on the **ADVANCED** link.



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.

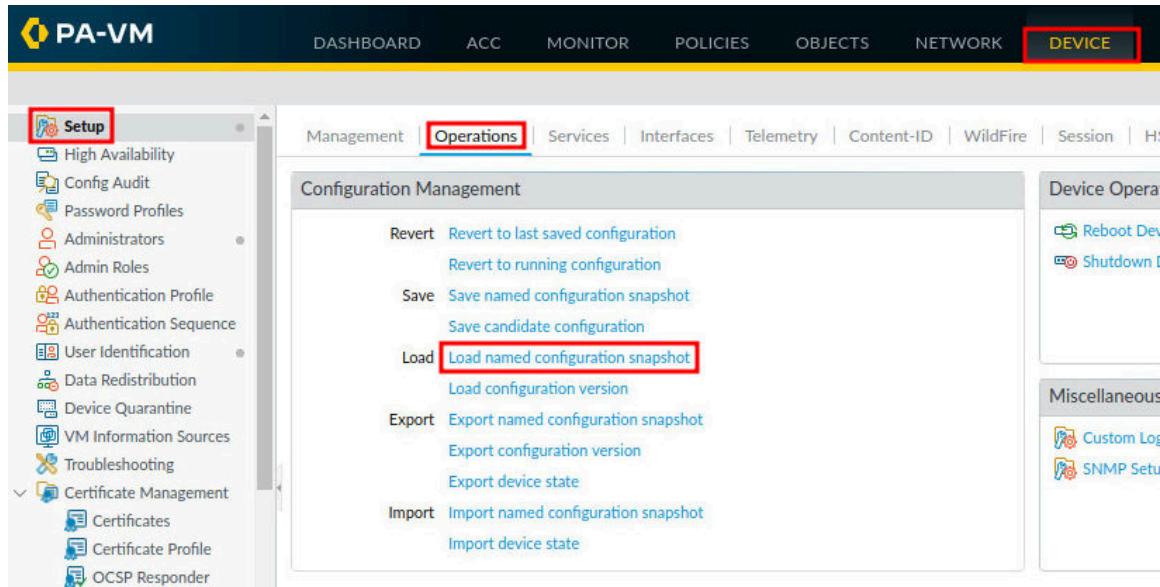
6. Click on **Proceed to 192.168.1.254 (unsafe)**.



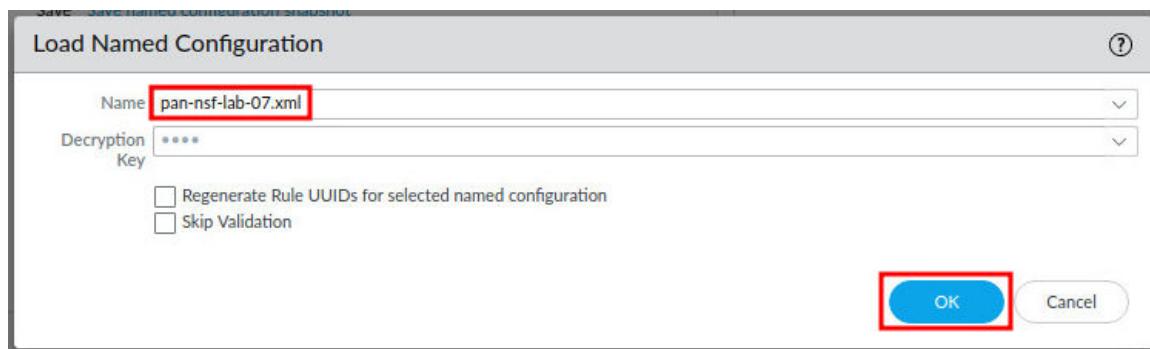
7. Log in to the Firewall web interface as username **admin**, password **PaloAlt0!**.



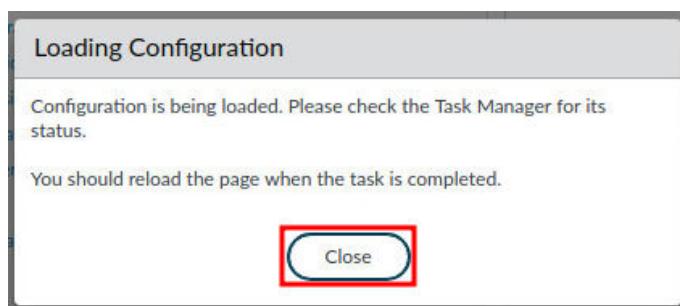
8. In the web interface, navigate to **Device > Setup > Operations** and click on **Load named configuration snapshot** underneath the *Configuration Management* section.



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



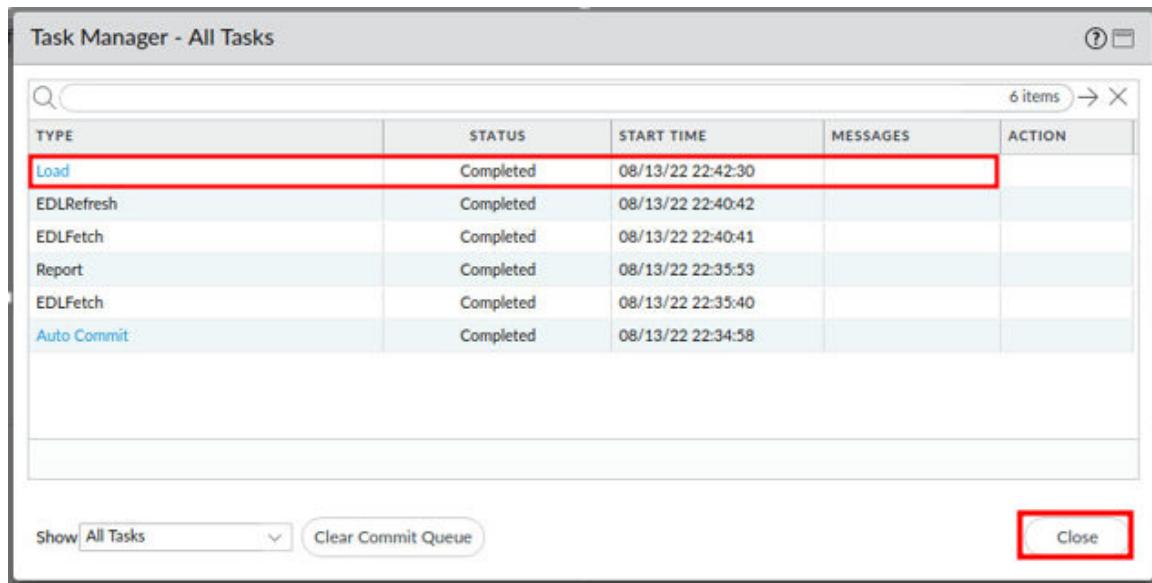
10. In the Loading Configuration window, a message will show *Configuration is being loaded. Please check the Task Manager for its status. You should reload the page when the task is completed.* Click **Close** to continue.



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

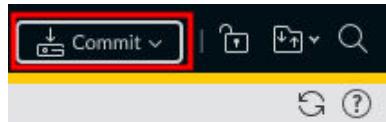


12. In the *Task Manager – All Tasks* window, verify the *Load* type has successfully completed. Click **Close**.

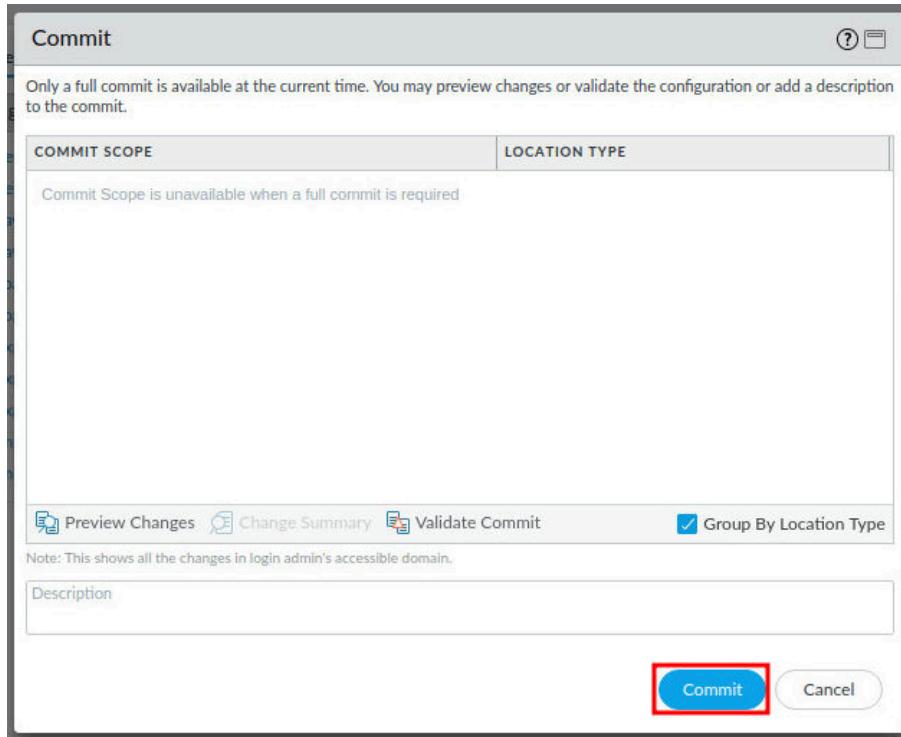


TYPE	STATUS	START TIME	MESSAGES	ACTION
Load	Completed	08/13/22 22:42:30		
EDLRefresh	Completed	08/13/22 22:40:42		
EDLFetch	Completed	08/13/22 22:40:41		
Report	Completed	08/13/22 22:35:53		
EDLFetch	Completed	08/13/22 22:35:40		
Auto Commit	Completed	08/13/22 22:34:58		

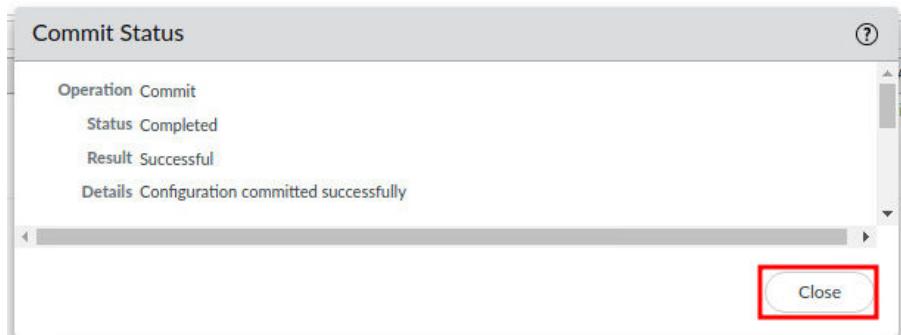
13. Click the **Commit** link located at the top-right of the web interface.



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.

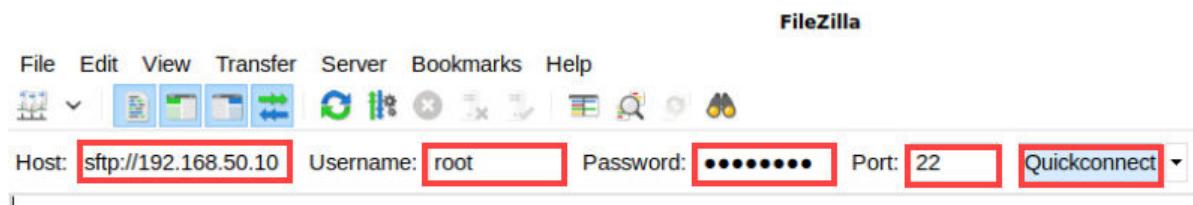
1. Minimize **Chromium** in the upper-right.



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

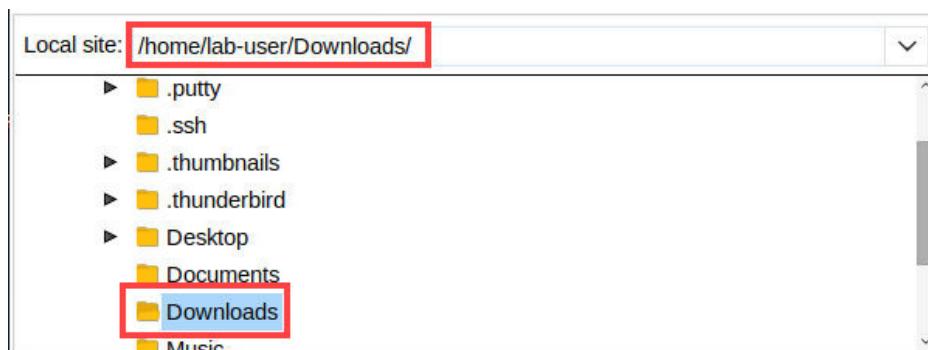


3. In the *FileZilla* window, type `sftp://192.168.50.10` for the *Host*, type `root` for the *Username*, type `Pal0Alt0!` for the *Password*, lastly, type `22` for the *Port*. Then, click the **Quickconnect** button.

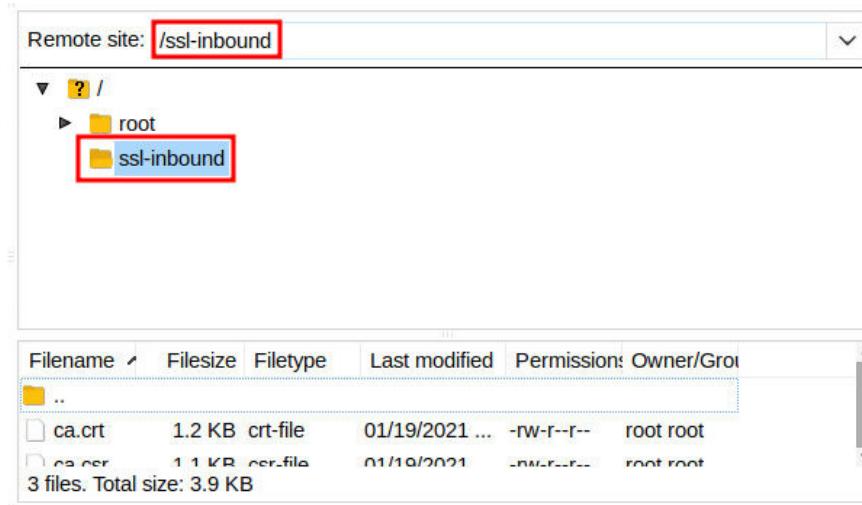


You may be prompted to remember the password after connecting to `sftp://192.168.50.10`. It is strongly recommended to not save passwords automatically as this could lead to insecure accounts and networks. If prompted to save the password, select **Do not save passwords** and select **OK**.

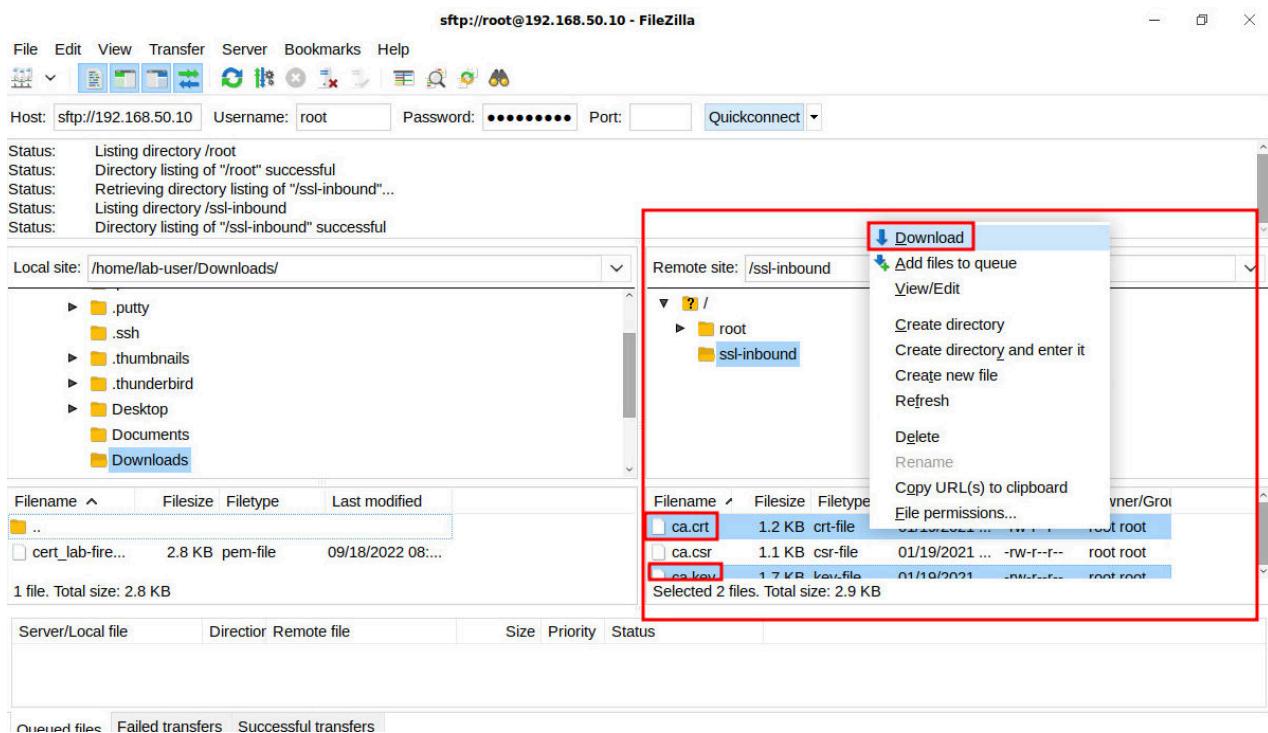
4. On the Local site, type `/home/lab-user/Downloads` in the text field. Press **Enter**.



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**.



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

3 files. Total size: 3.9 KB

Server/Local file	Director	Remote file	Size	Priority	Time
sftp://root@192.168.50.10					
<input type="checkbox"/> /home/lab-user/Downloads/ca.crt	<<--	/ssl-inbound/ca.crt	1.2 KB	Normal	01/19/2021 03:29:3...
<input type="checkbox"/> /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**.

PA-VM

- DASHBOARD
- ACC
- MONITOR
- POLICIES
- OBJECTS
- NETWORK
- DEVICE**

Device Certificates | Default Trusted Certificate Authorities

	NAME	SUBJECT	ISSUER	CA	KEY	EXP

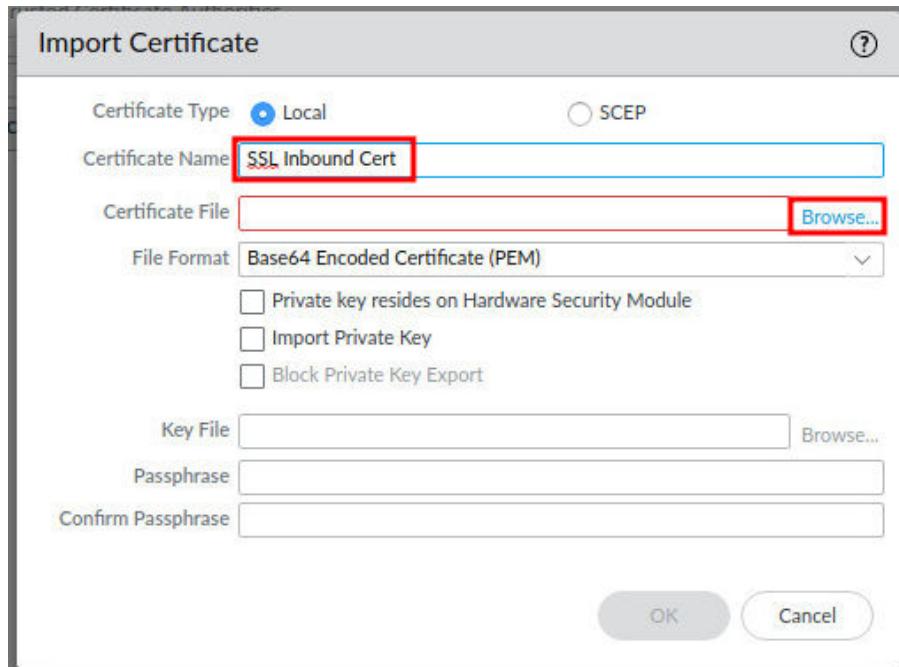
Setup  
High Availability  
Config Audit  
Password Profiles  
Administrators  
Admin Roles  
Authentication Profile  
Authentication Sequence  
User Identification  
Data Redistribution  
Device Quarantine  
VM Information Sources  
Troubleshooting

Certificate Management  
**Certificates**

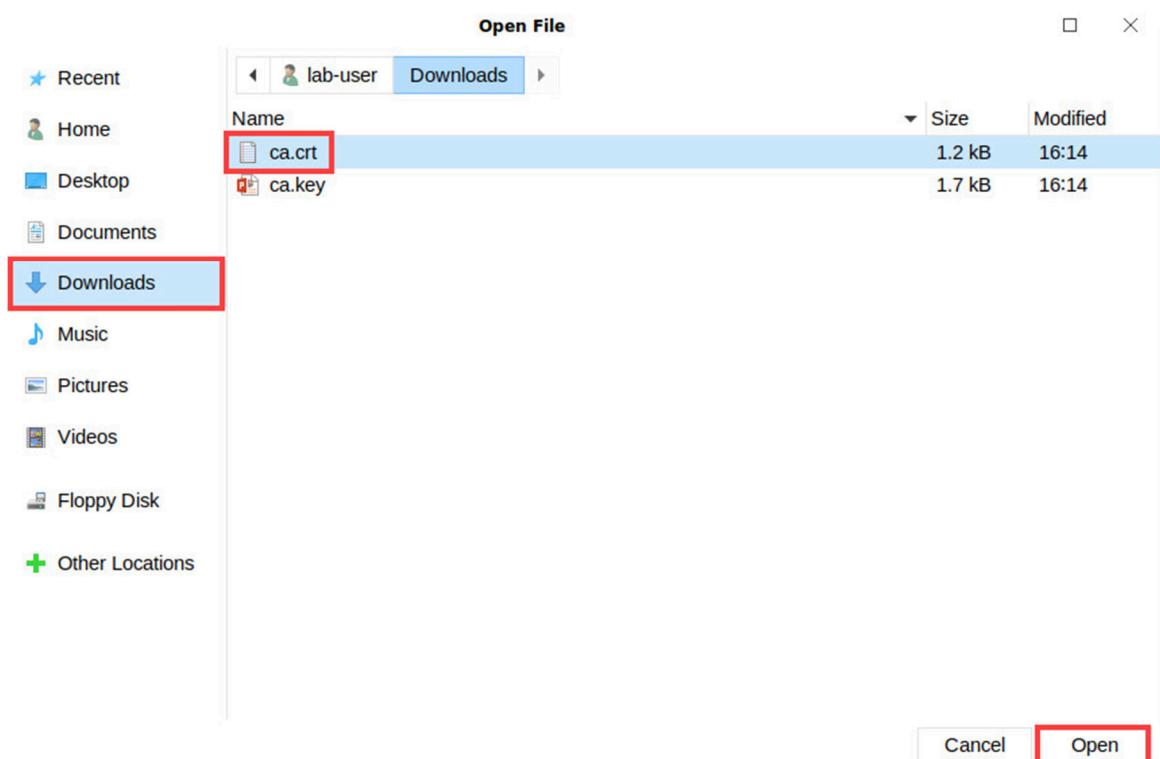
3. Click on the **Import** button at the bottom-center of the center section.



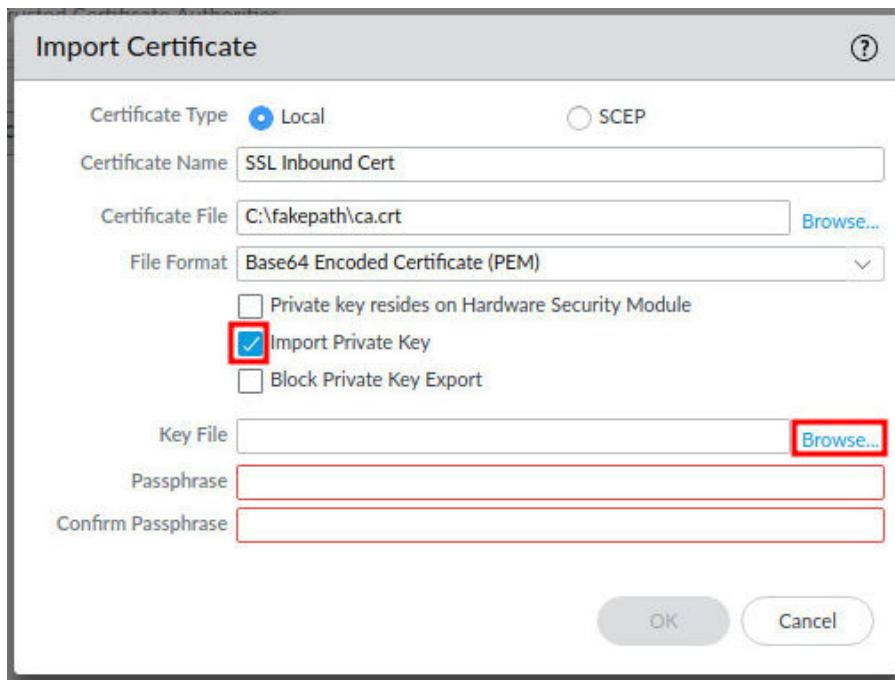
4. In the *Import Certificate* window, type **SSL Inbound Cert**. Then, click **Browse...**



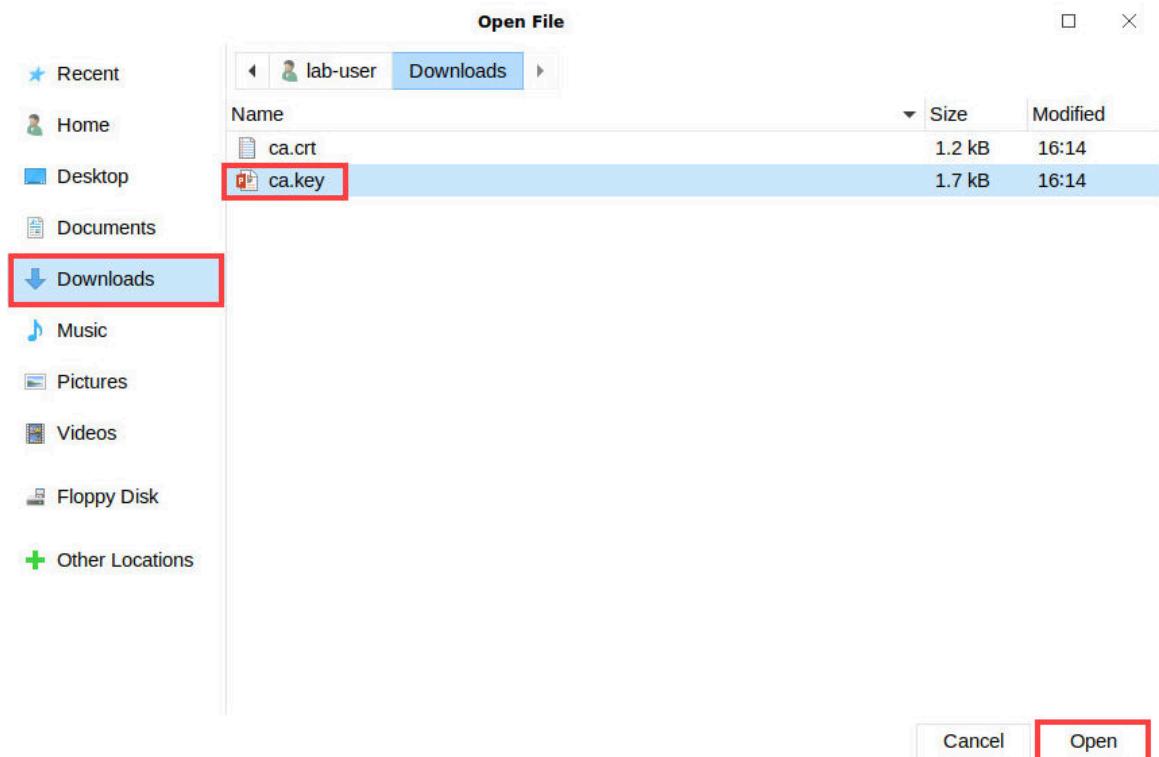
5. In the *Open File* window, select **Downloads** on the left. Then, select **ca.crt**. Finally, click the **Open** button.



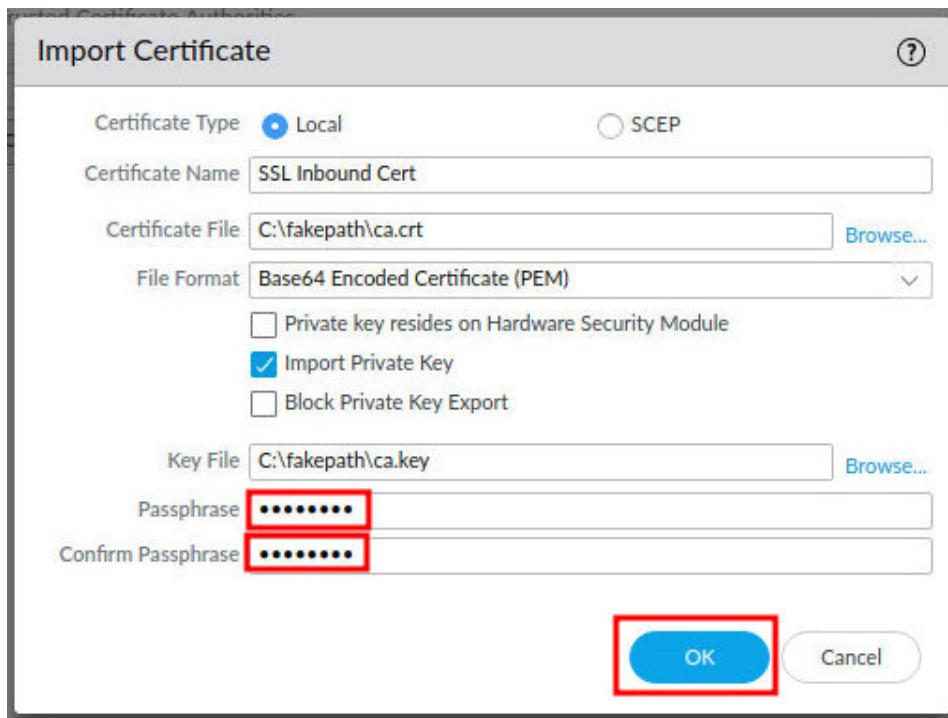
6. Click the checkbox for **Import private key**. Then, click **Browse...**



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.



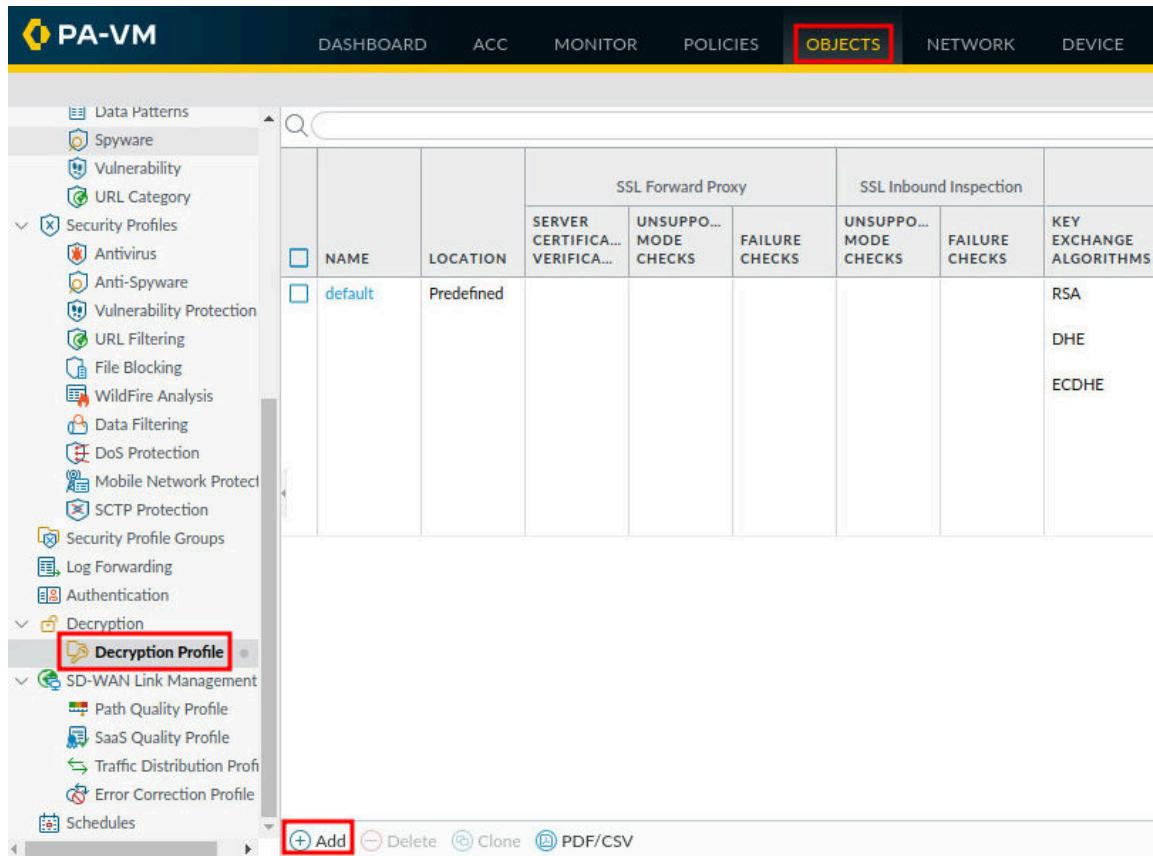
9. Verify the *SSL Inbound Cert* is showing a status of **valid**.

Device Certificates								Default Trusted Certificate Authorities	
	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

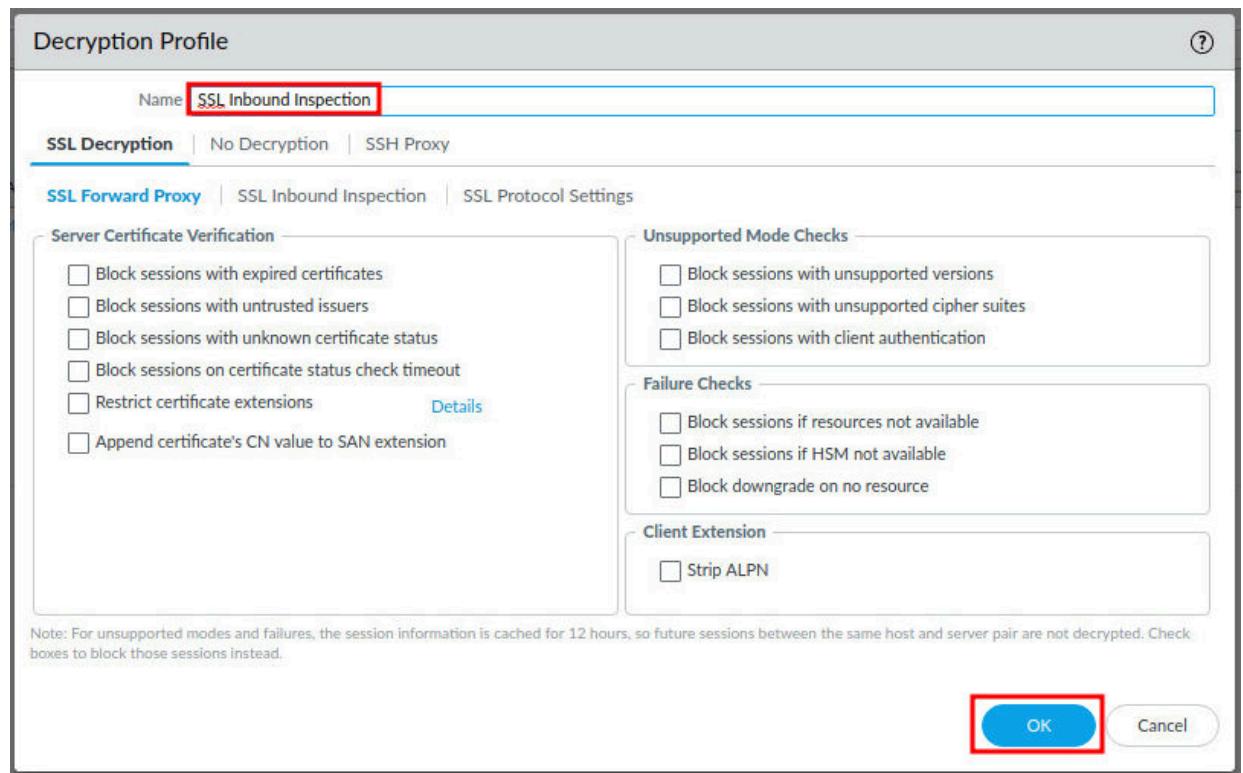
In this section, you will create a decryption profile. Decryption profiles allow administrators to perform checks on both decrypted traffic and traffic that would have been excluded from decryption. After a decryption profile is created, it can then be attached to a decryption policy rule that will enforce 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 management interface. The top navigation bar has tabs: DASHBOARD, ACC, MONITOR, POLICIES, **OBJECTS**, NETWORK, and DEVICE. The OBJECTS tab is highlighted with a red box. The left sidebar contains a tree view of objects: Data Patterns, Spyware, Vulnerability, URL Category, Security Profiles (Antivirus, Anti-Spyware, Vulnerability Protection, URL Filtering, File Blocking, WildFire Analysis, Data Filtering, DoS Protection, Mobile Network Protection, SCTP Protection), Security Profile Groups, Log Forwarding, Authentication, Decryption (Decryption Profile is selected and highlighted with a red box), SD-WAN Link Management (Path Quality Profile, SaaS Quality Profile, Traffic Distribution Profile, Error Correction Profile), and Schedules. At the bottom of the sidebar are buttons for (+) Add, Delete, Clone, and PDF/CSV. The main content area displays two tables. The first table, titled "SSL Forward Proxy", has columns: NAME, LOCATION, SERVER CERTIFICA..., UNSUPPO... MODE CHECKS, FAILURE CHECKS. It shows one row for "default" with "Predefined" in LOCATION and empty fields for the others. The second table, titled "SSL Inbound Inspection", has columns: UNSUPPO... MODE CHECKS, FAILURE CHECKS, KEY EXCHANGE ALGORITHMS. It also shows one row for "default" with empty fields for the first two columns and "RSA", "DHE", and "ECDHE" listed under KEY EXCHANGE ALGORITHMS. A search bar is at the top of the main content area.

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			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...
	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.

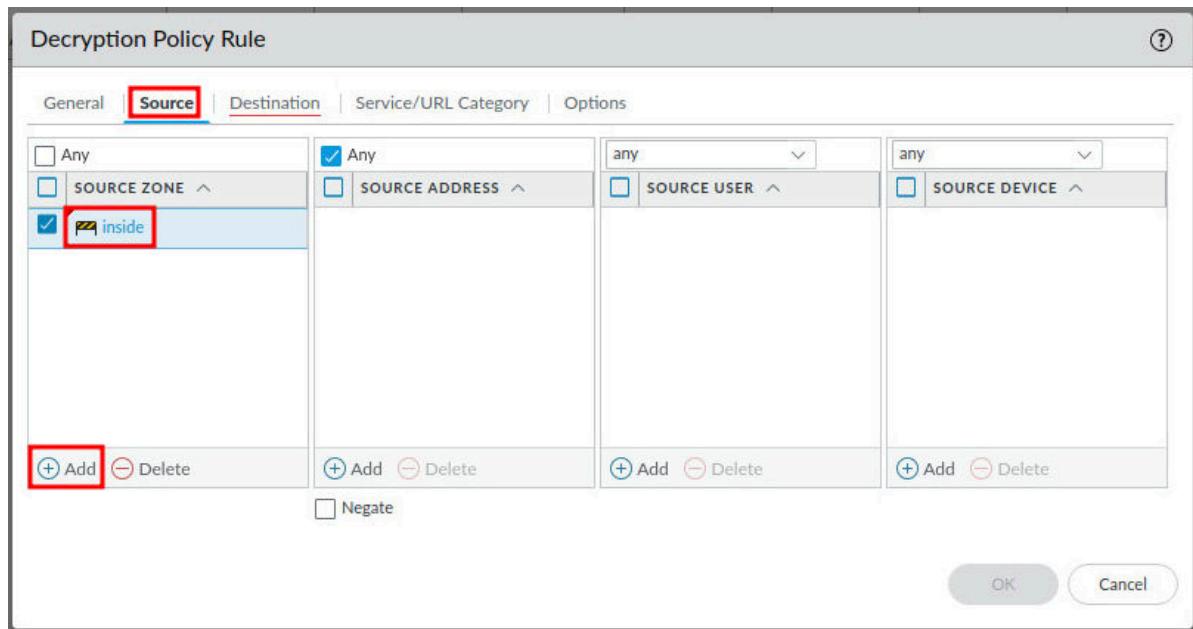
1. Navigate to **Policies > Decryption > Add**.

The screenshot shows the PA-VM web interface. The top navigation bar includes tabs for DASHBOARD, ACC, MONITOR, POLICIES (which is highlighted with a red box), OBJECTS, NETWORK, and DEVICE. On the left, a sidebar lists various security features: Security, NAT, QoS, Policy Based Forwarding, Decryption (which is highlighted with a red box), Tunnel Inspection, Application Override, Authentication, DoS Protection, and SD-WAN. Below the sidebar is a 'Policy Optimizer' section with a 'Rule Usage' table. At the bottom of the page, there is a toolbar with buttons for Object: Addresses, + Add, Delete, Clone, Enable, Disable, Move, PDF/CSV, and Highlight Unused Rules. The main area displays a table with columns: NAME, TAGS, ZONE, ADDRESS, USER, and DEVICE. A search bar is located above the table.

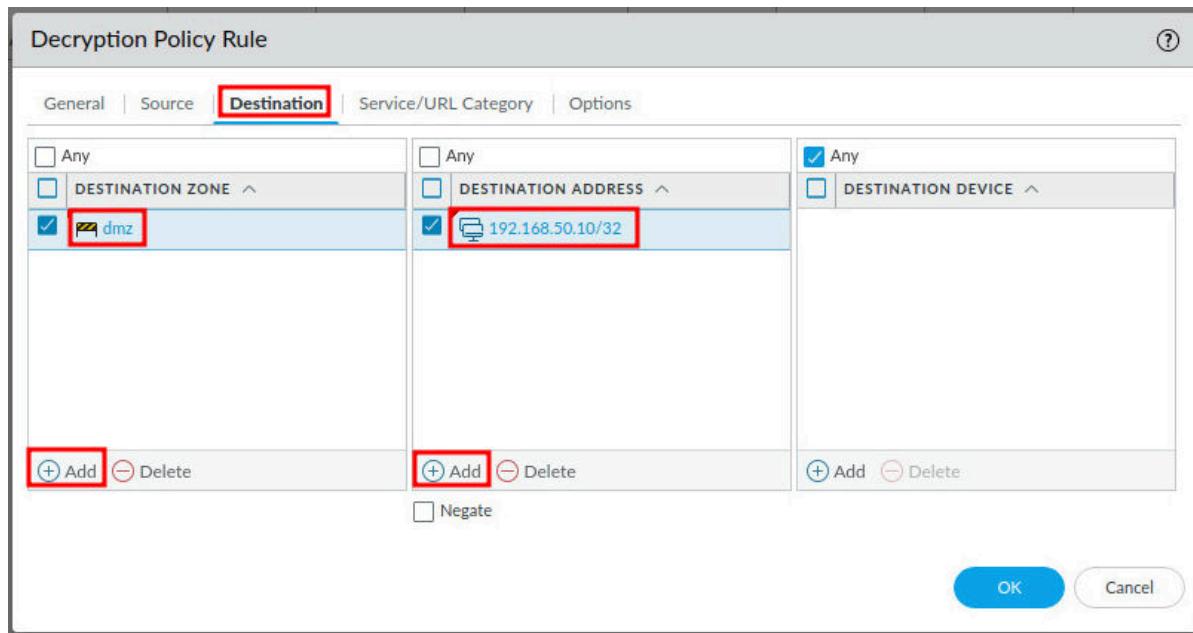
2. In the **General** tab of the *Decryption Policy Rule* window, type **Decrypt SSL Inbound Inspection** in the **Name** field.

The screenshot shows the 'Decryption Policy Rule' configuration dialog. The 'General' tab is selected and highlighted with a red box. The 'Name' field contains the value 'Decrypt SSL Inbound Inspection', which is also highlighted with a red box. Other fields include 'Description' (empty), 'Tags' (empty), 'Group Rules By Tag' (set to 'None'), and 'Audit Comment' (empty). At the bottom right are 'OK' and 'Cancel' buttons.

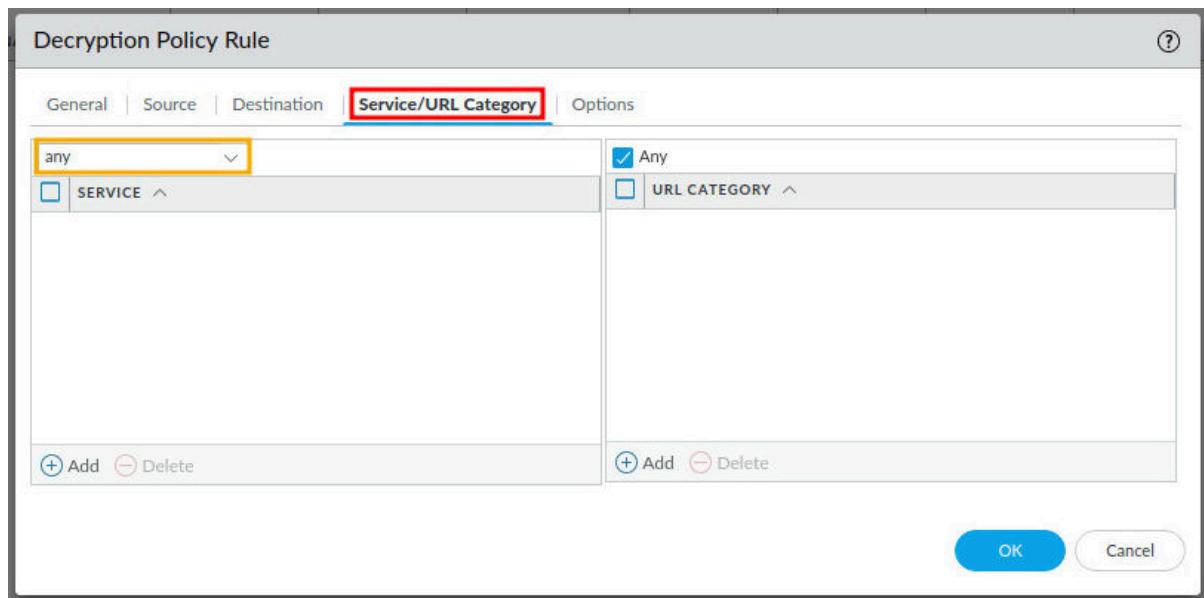
3. In the *Decryption Policy Rule* window, click on the **Source** tab. Then, click **Add** in the *Source Zone* section. Next, select **inside**.



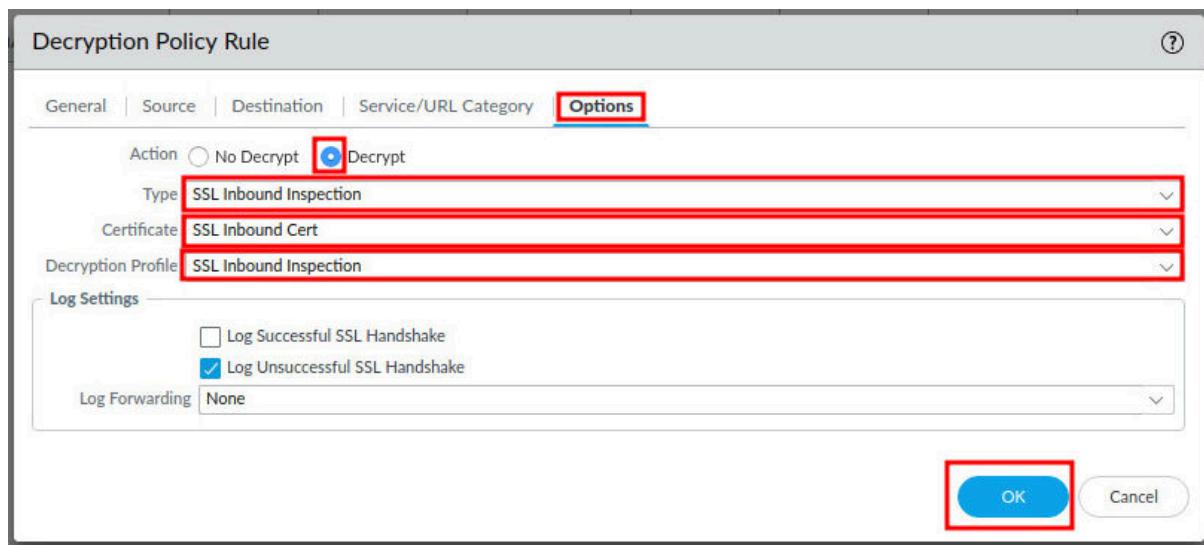
4. In the *Decryption Policy Rule* window, click on the **Destination** tab. Then, click **Add** in the *Destination Zone* pane. Next, select **dmz** and press **Enter**. In the *Destination Address* pane, click **Add**. Type **192.168.50.10/32** and press **Enter**.



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.



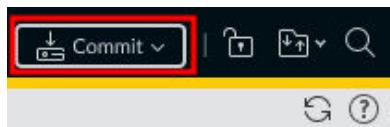
7. Verify the **Decrypt SSL Inbound Policy** is showing and correct.

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

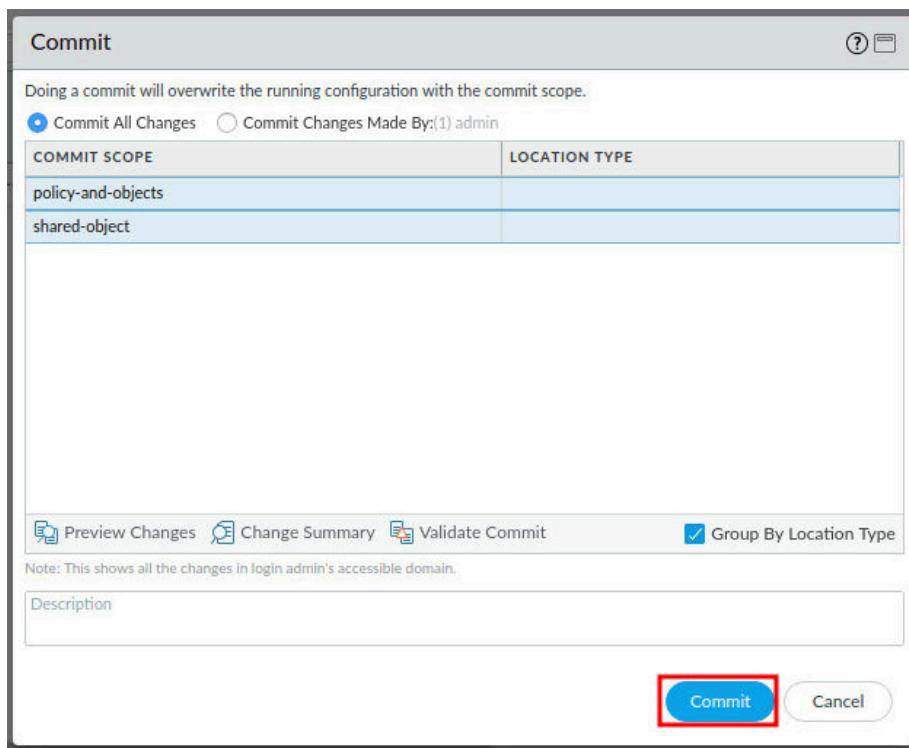
## 1.5 Commit and Test Decryption Policy

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

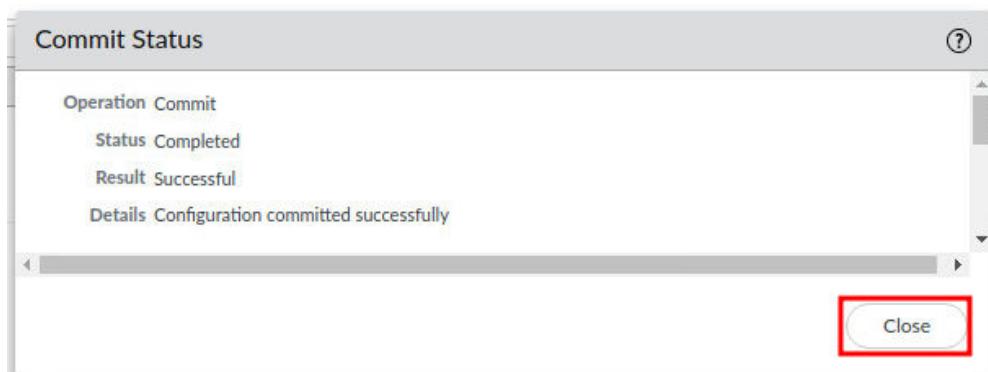
1. Click the **Commit** link located at the top-right of the web interface.



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.**

The screenshot shows the PA-VM interface with the 'MONITOR' tab selected. On the left, a sidebar under 'Logs' has 'Traffic' highlighted with a red box. The main area displays a table of traffic logs. The columns are: RECEIVE TIME, TYPE, FROM ZONE, TO ZONE, SOURCE, SOURCE USER, SOURCE DYNAMIC ADDRESS GROUP, and DESTINATI... (partially visible). The data in the table includes:

RECEIVE TIME	TYPE	FROM ZONE	TO ZONE	SOURCE	SOURCE USER	SOURCE DYNAMIC ADDRESS GROUP	DESTINATI...
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**.

The search bar contains the query '(addr.dst in 192.168.50.10)'. The entire query is highlighted with a red box.

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

The 'Source' column header has a red box. A dropdown menu labeled 'Columns' is open to the right, with 'Adjust Columns' also visible. The table data is identical to the previous screenshot.

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

The 'Columns' menu is open, showing various checkboxes. The 'Decrypted' checkbox is highlighted with a red box. The full list of checkboxes is:

- To Zone
- Source
- Source User
- Source Dynamic Address Group
- Destination
- Destination Dynamic Address Group
- Dynamic User Group
- To Port
- Decrypted
- Application

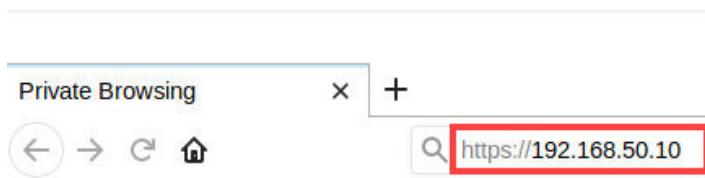


The **Decrypted** checkbox might be listed alphabetically among the unchecked boxes in the lower part of the menu

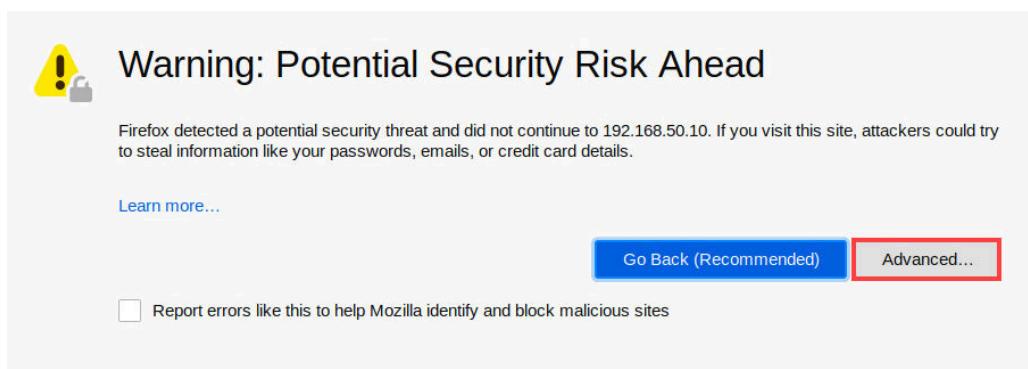
8. Open the *Firefox Web Browser* by clicking on the **Firefox** icon located in the task bar.



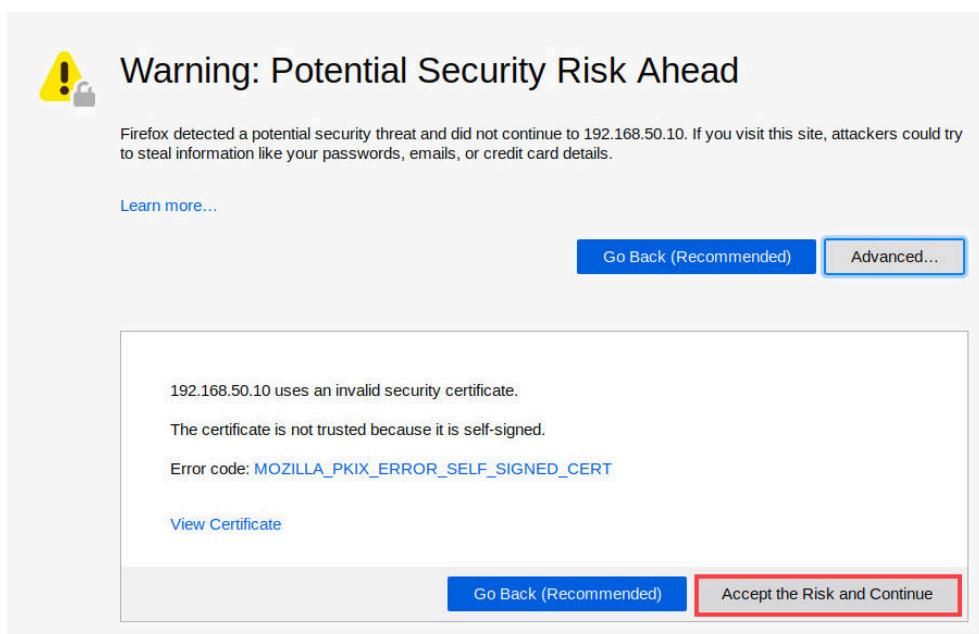
9. In the address bar, type `https://192.168.50.10` and click **Enter**.



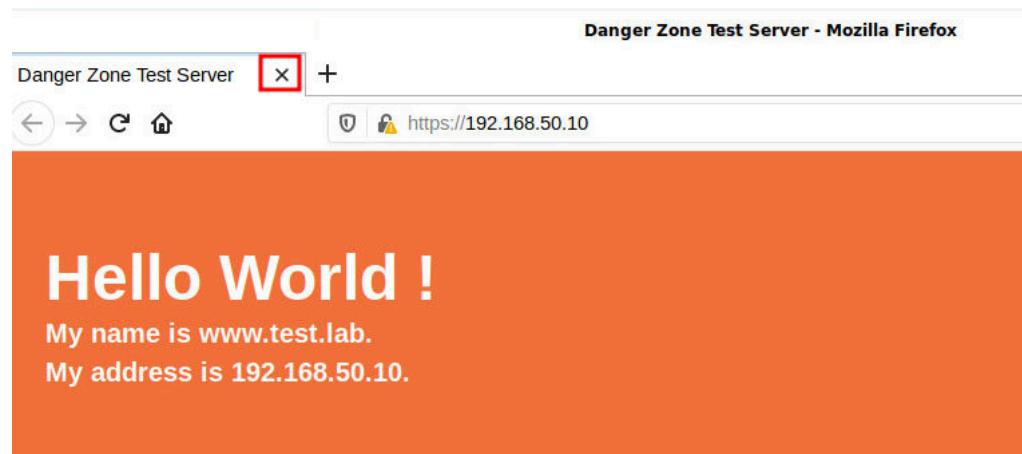
10. You will see a "*Warning: Potential Security Risk Ahead*" message. Click on the **Advanced** button.



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.

	RECEIVE TIME	TYPE	FROM ZONE	TO ZONE	SOURCE	DECRYPTED	SOURCE USE
	09/18 23:01:46	end	inside	dmz	192.168.1.20	no	
	09/18 23:01:46	end	inside	dmz	192.168.1.20	no	
	09/18 23:01:46	end	inside	dmz	192.168.1.20	no	
	09/18 22:38:56	end	inside	dmz	192.168.1.20	no	

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**.

	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	APPLICATION	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**

<b>General</b>		<b>Source</b>		<b>Destination</b>									
Session ID: 2369 Action: allow Action Source: from-policy Host ID: Application: ssl Rule: Allow-Inside-DMZ Rule UUID: de443dfb-35aa-41e9-a290-22238efdbab47 Session End Reason: policy-deny Category: any Device SN IP Protocol: tcp Log Action Generated Time: 2022/09/19 00:36:45		Source User: 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: 192.168.50.10 Destination DAG Country: 192.168.0.0-192.168.255.255 Port: 443 Zone: dmz Interface: ethernet1/3									
				<b>Flags</b>									
				Captive Portal: <input type="checkbox"/> Proxy Transaction: <input type="checkbox"/> <b>Decrypted: <input checked="" type="checkbox"/></b>									
		<b>Details</b>											
PCAP	RECEIVE TIME	TYPE	APPLICATION	ACTION	RULE	RULE UUID	BY...	SEVERI...	CATEG...	URL CATEG...	VERDI...	URL	FILE NAME
	2022/09/19 00:36:45	deny	ssl	allow	Allow-Inside-DMZ	de443... 4019			any				

**Close**

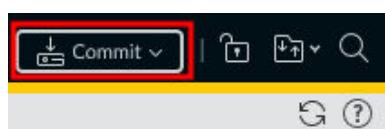
## 1.6 Disable Decryption Policy

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.

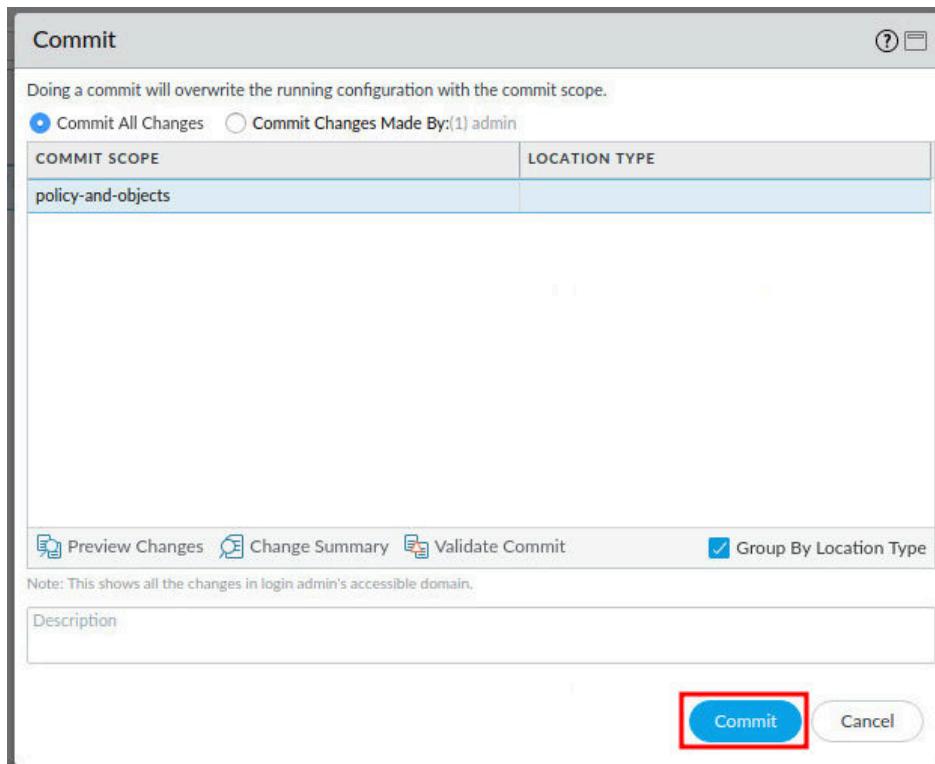
1. Navigate to **Policies > Decryption**. Then, click the **1** for the **Decrypt SSL Inbound Inspection** policy. Next, click the **Disable** button.

NAME	TAGS	Source			
		ZONE	ADDRESS	USER	DEVICE
1 Decrypt SSL Inbound...	none	inside	any	any	any

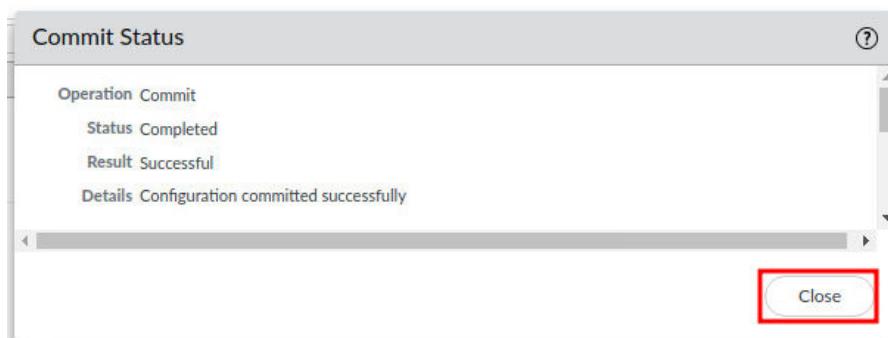
2. Click the **Commit** link located at the top-right of the web interface.



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



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



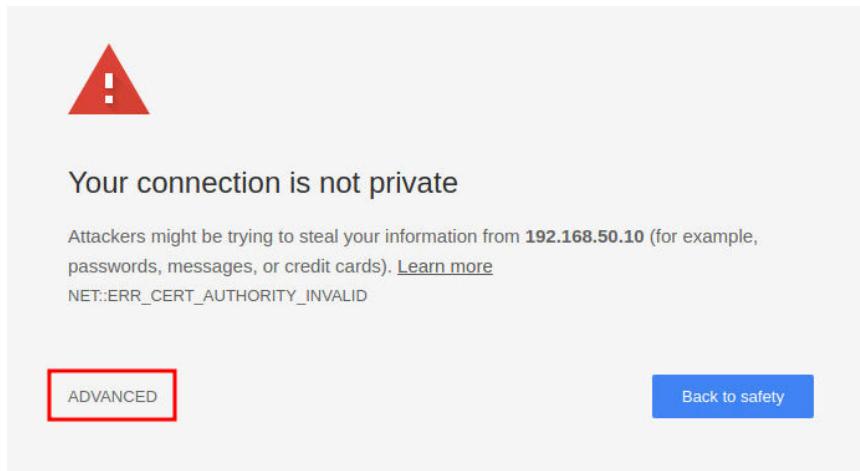
5. Click the **New tab** button in *Chromium*.



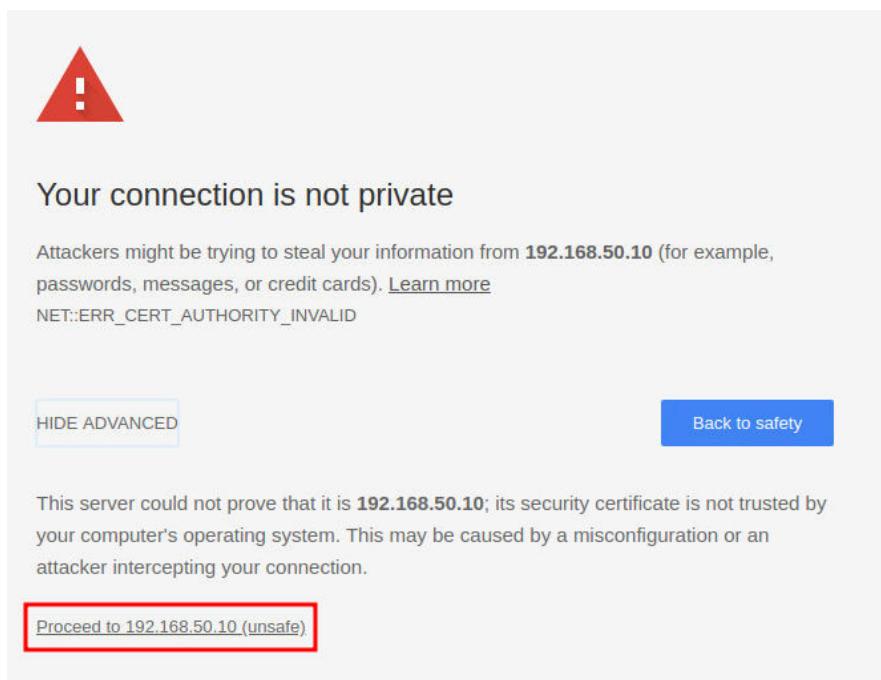
6. In the address bar, type `https://192.168.50.10` and click **Enter**.



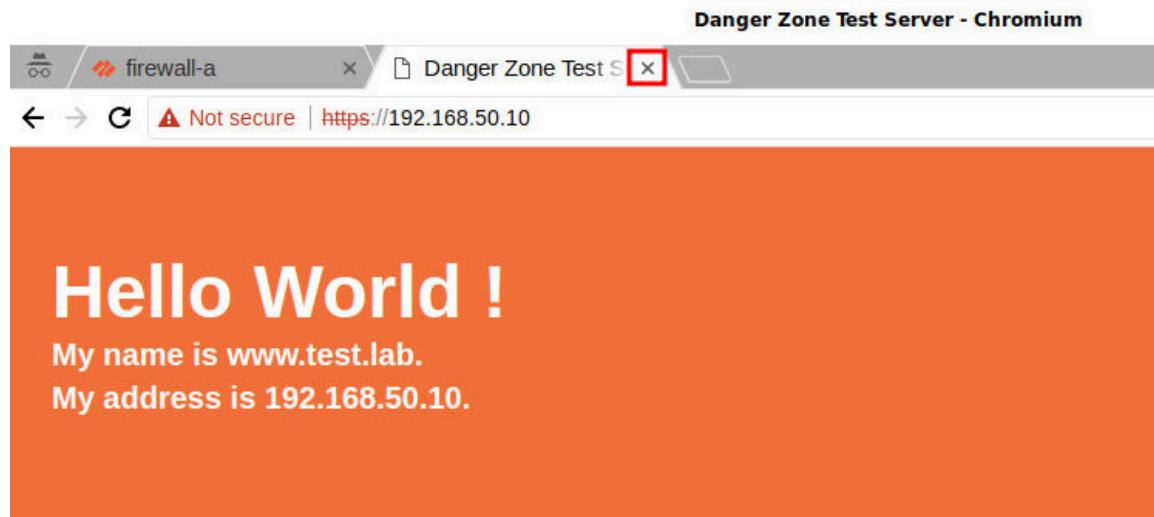
7. You will see a *Your connection is not private* message. Click on the **ADVANCED** link.



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	DESTINATI...	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	DESTINATI...	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.

The screenshot shows the 'Detailed Log View' window with the following details:

- General:**
  - Session ID: 2482
  - Action: allow
  - Action Source: from-policy
  - Host ID
  - Application: ssl
  - Rule: Allow-Inside-DMZ
  - Rule UUID: de443dfb-35aa-41e9-a290-22238efdbab47
  - Session End Reason: tcp-rst-from-client
  - Category: any
  - Device SN
  - IP Protocol: tcp
  - Log Action
  - Generated Time: 2022/09/19 01:09:55
  - Start Time: 2022/09/19 01:09:40
- Source:**
  - Source User: 192.168.1.20
  - Source DAG
  - Country: 192.168.0.0-192.168.255.255
  - Port: 43628
  - Zone: inside
  - Interface: ethernet1/2
  - X-Forwarded-For IP: 0.0.0.0
- Destination:**
  - Destination User: 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:
  - Proxy Transaction:
  - Decrypted:**  (This checkbox is highlighted with an orange border.)
  - Packet Capture:
- Details:** A table showing session details:

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

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