



# NETWORK SECURITY FUNDAMENTALS

## Lab 7: Decrypting SSL Inbound Traffic

Document Version: **2021-01-30**

Copyright © 2021 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
7 Decrypting SSL Inbound Traffic .....	6
7.0 Load Lab Configuration .....	6
7.1 Download the SSL Certificate from DMZ Server .....	10
7.2 Import SSL Certificate .....	13
7.3 Create a Decryption Profile .....	16
7.4 Create a Decryption Policy .....	18
7.5 Commit and Test Decryption Policy .....	21
7.6 Disable Decryption Policy .....	26

## Introduction

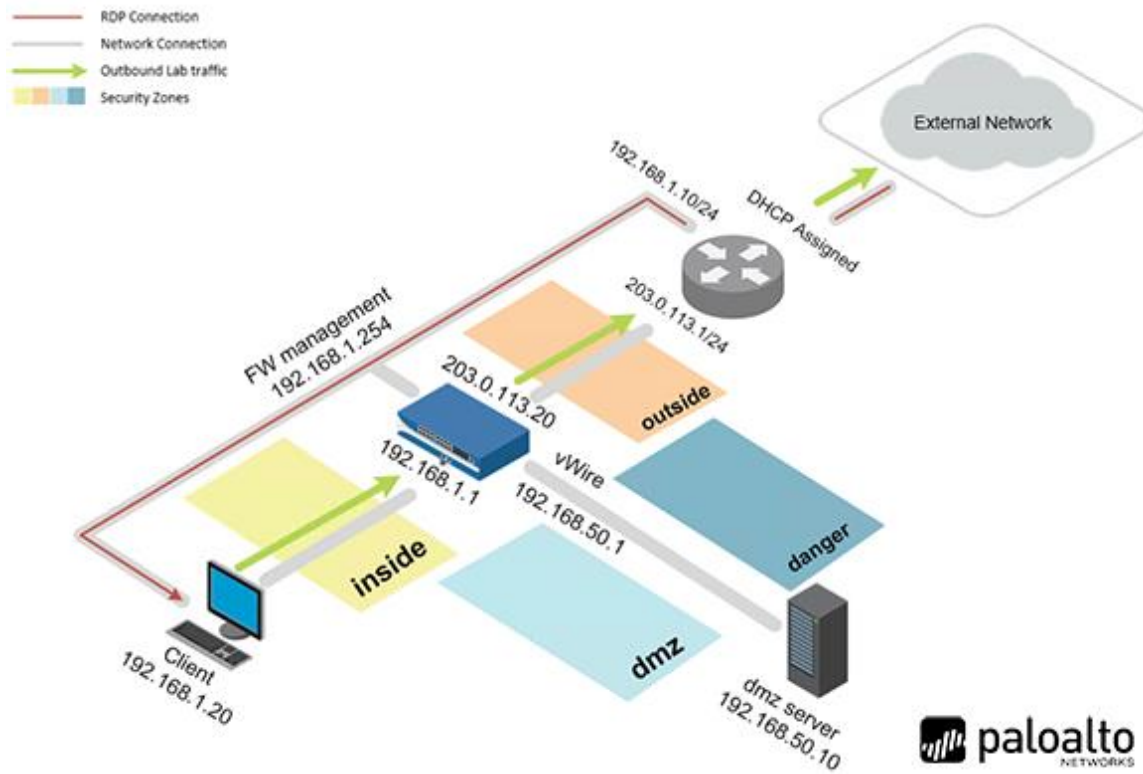
In this lab, you will decrypt SSL inbound traffic and inspect SSL traffic from the Client machine to the DMZ server. When the SSL server certificate is loaded on the Firewall, and an SSL decryption policy is configured for the inbound traffic, the device can then decrypt and read the traffic as it forwards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

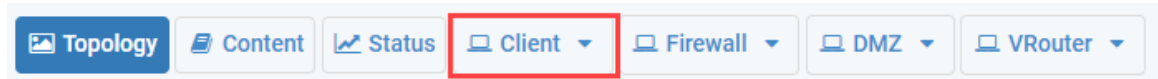
Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Client	192.168.1.20	lab-user	Train1ng\$
DMZ	192.168.50.10	root	Pal0Alt0
Firewall	192.168.1.254	admin	Train1ng\$

## 7 Decrypting SSL Inbound Traffic

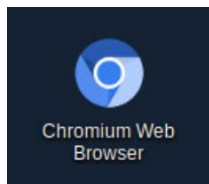
### 7.0 Load Lab Configuration

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

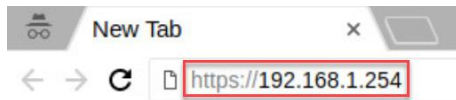
1. Click on the **Client** tab to access the Client PC.



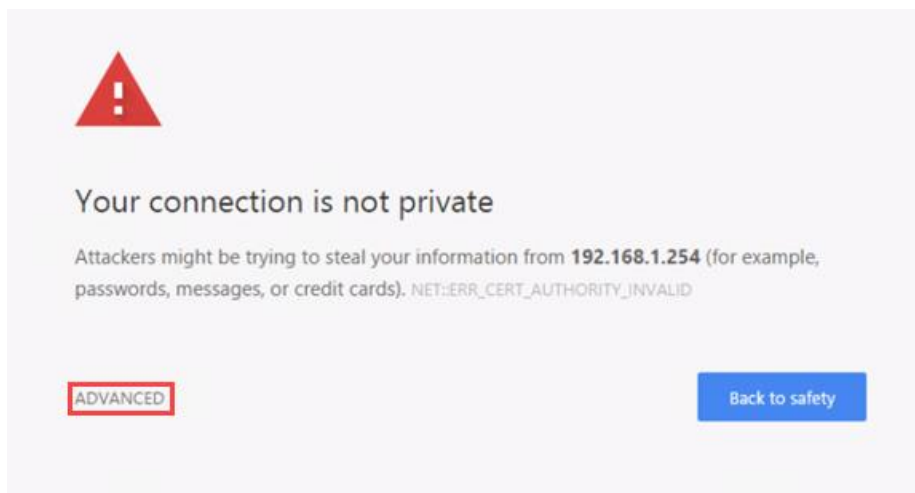
2. Log in to the Client PC as username **lab-user**, password **Train1ng\$**.
3. Double-click the **Chromium Web Browser** icon located on the desktop.



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

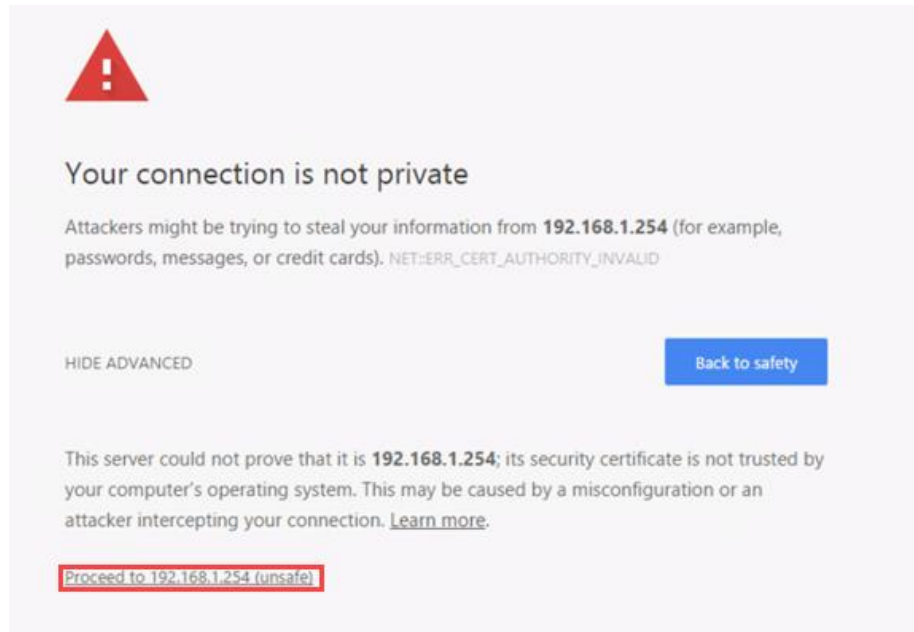


5. You will see a “Your connection is not private” message. Click on the **ADVANCED** link.



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.

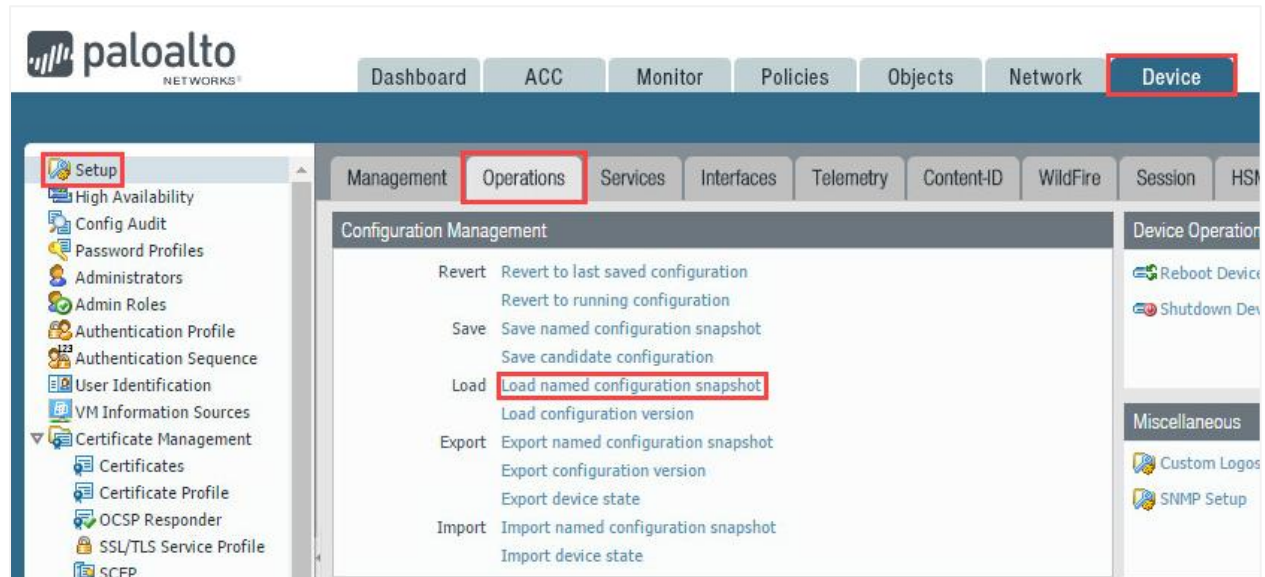
6. Click on **Proceed to 192.168.1.254 (unsafe)**.



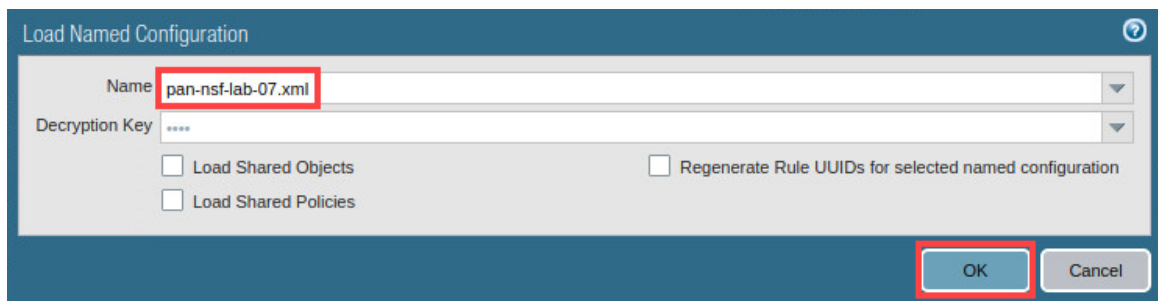
7. Log in to the Firewall web interface as username **admin**, password **Train1ng\$**.



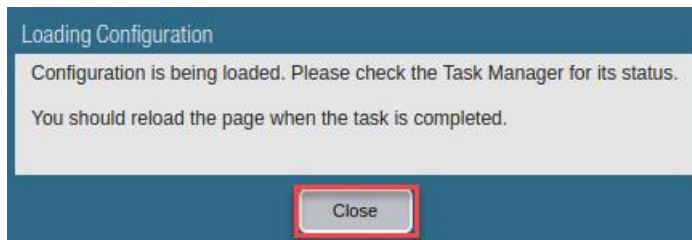
8. In the web interface, navigate to **Device > Setup > Operations** and click on **Load** named configuration snapshot underneath the *Configuration Management* section.



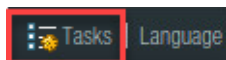
9. In the *Load Named Configuration* window, select **pan-nsf-lab-07.xml** from the *Name* dropdown box and click **OK**.



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.

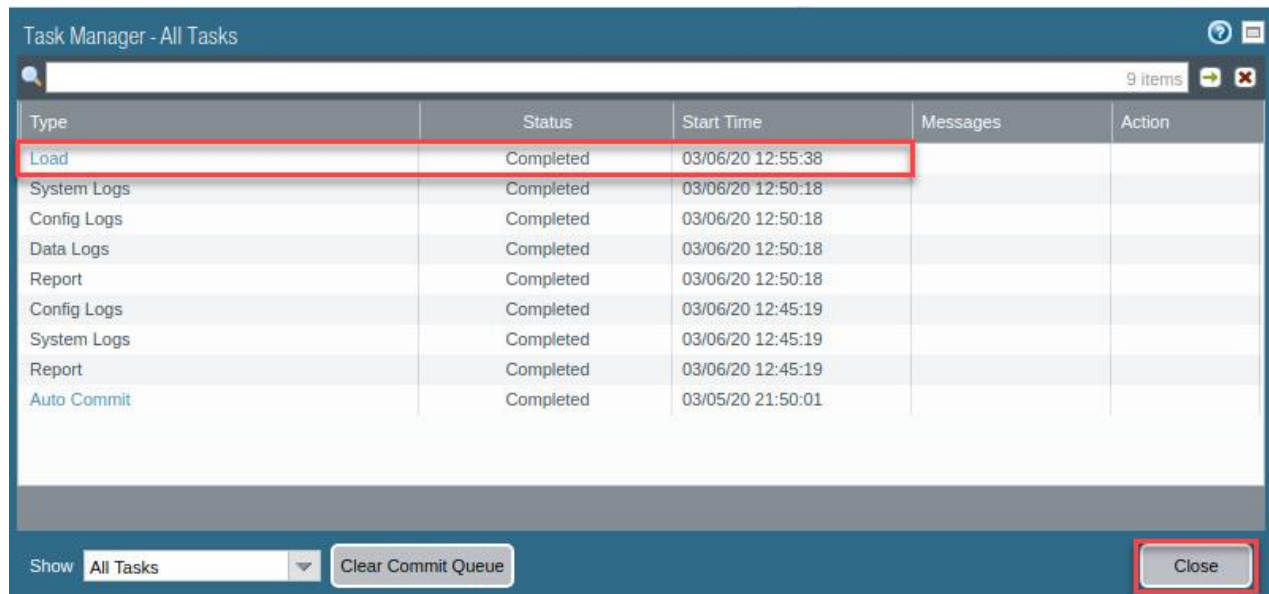


11. Click the **Tasks** icon located at the bottom-right of the web interface.





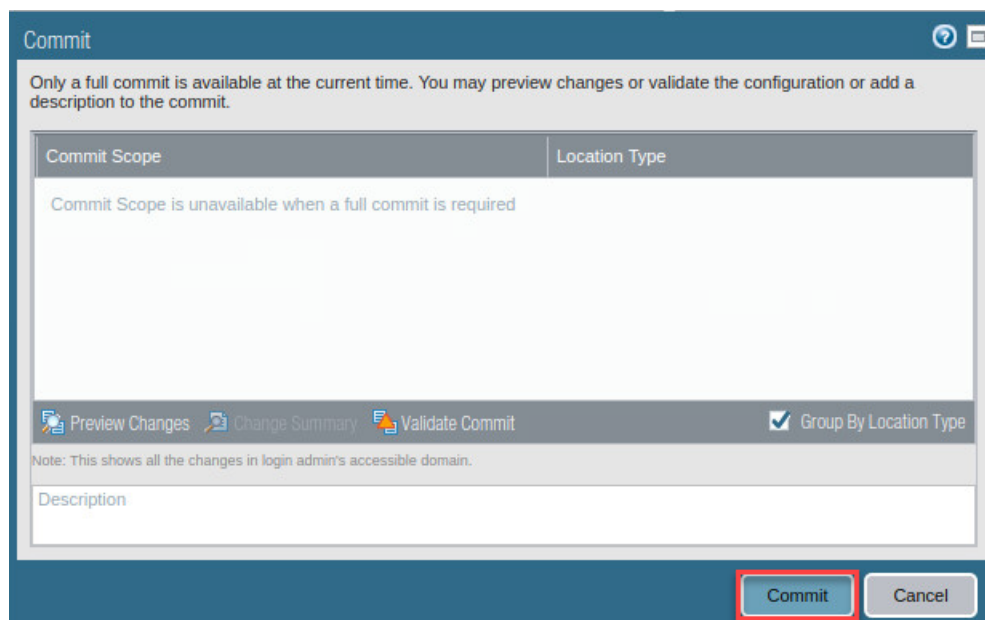
12. In the *Task Manager – All Tasks* window, verify the *Load* type has successfully completed. Click **Close**.



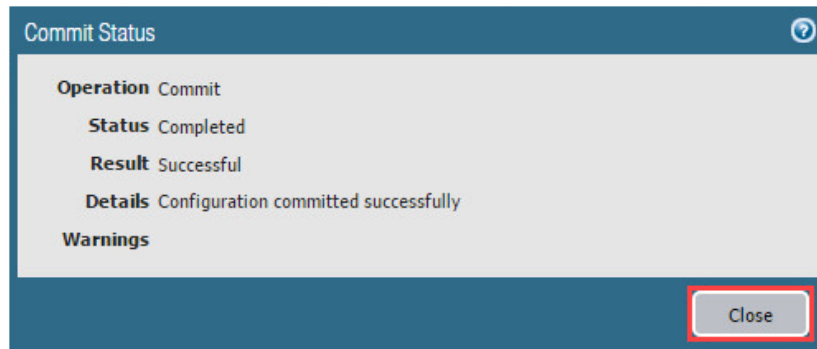
13. Click the **Commit** link located at the top-right of the web interface.



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



- 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.

## 7.1 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.

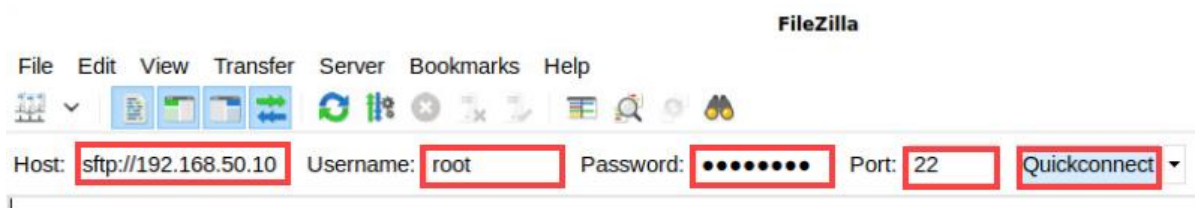
- Minimize **Chromium** in the upper-right.



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



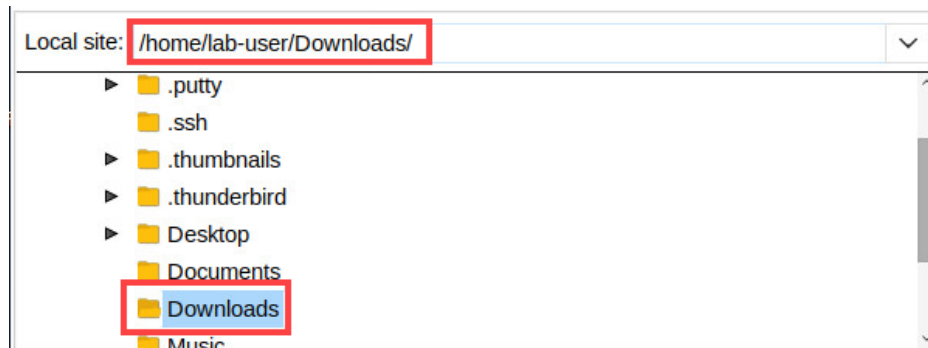
- In the *FileZilla* window, type `sftp://192.168.50.10` for the *Host*, type `root` for the *Username*, type `pa10A1t0` for the *Password*, lastly, type `22` for the *Port*. Then, click the **Quickconnect** button.



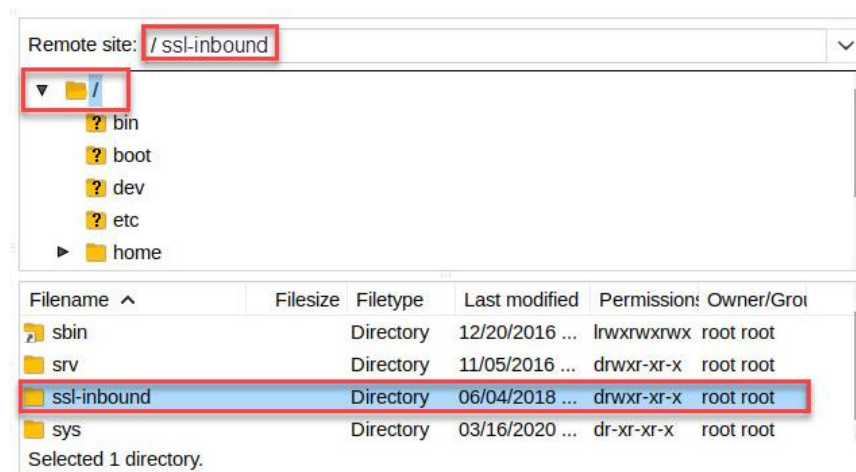


You may be prompted to remember the password after connecting to `sftp://192.168.50.10`. It is strongly recommended to not save passwords automatically as this could lead to insecure accounts and networks. If prompted to save the password, select **Do not save passwords** and select **OK**.

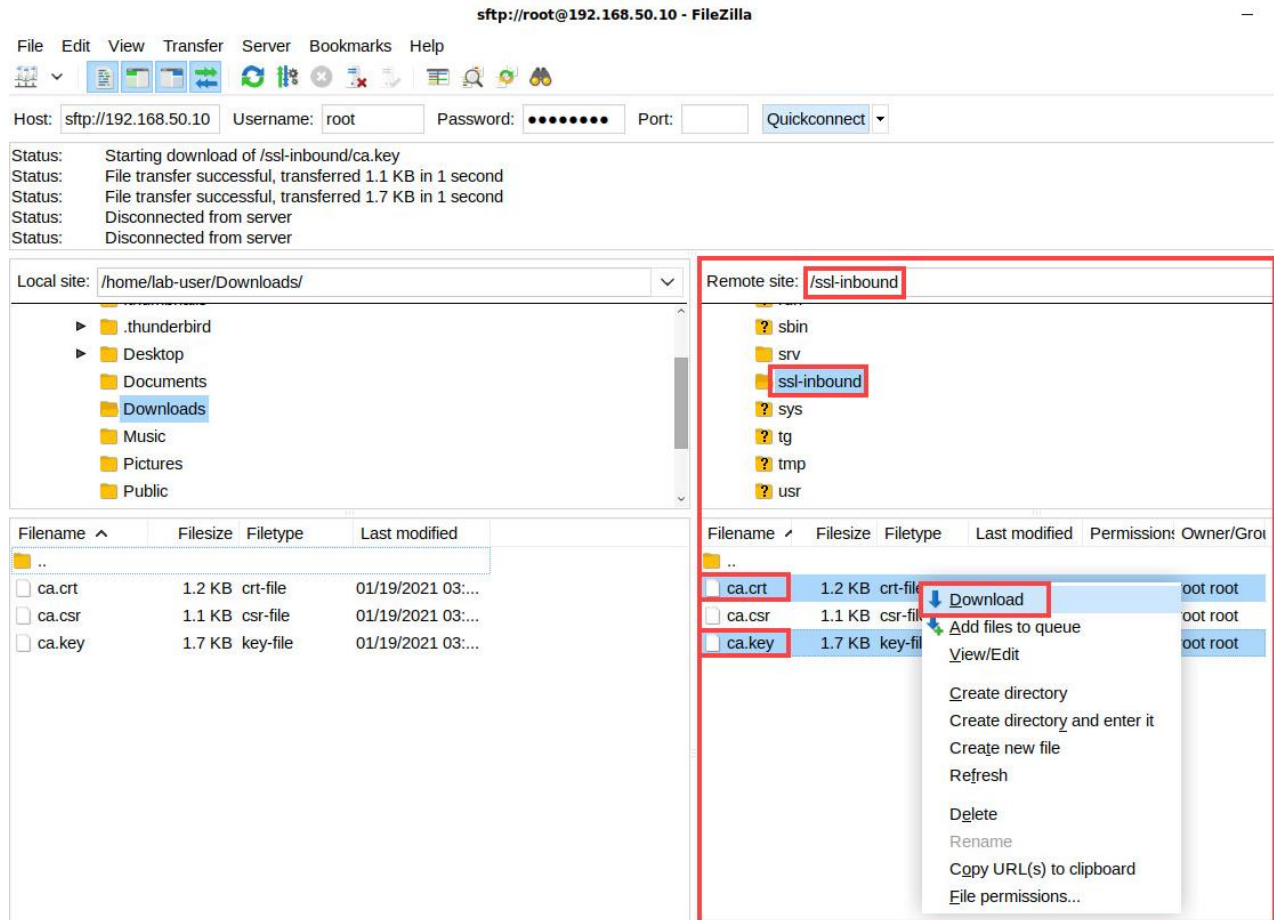
4. On the Local site, type `/home/lab-user/Downloads` in the text field. Press **Enter**.



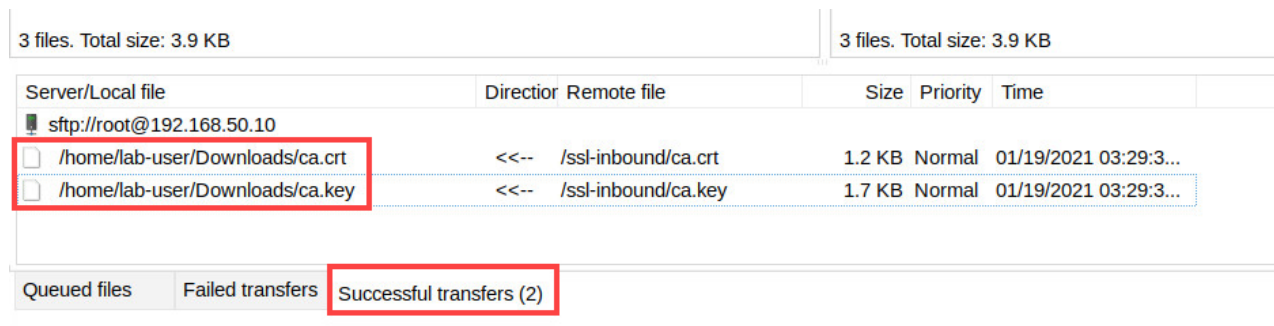
5. On the remote site, type `/ssl-inbound` in the text field. Press **Enter**.



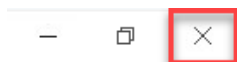
- Press **CTRL** and **click** to highlight the filenames **ca.key** and **ca.crt**. Right-click the files and click **Download**.



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



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



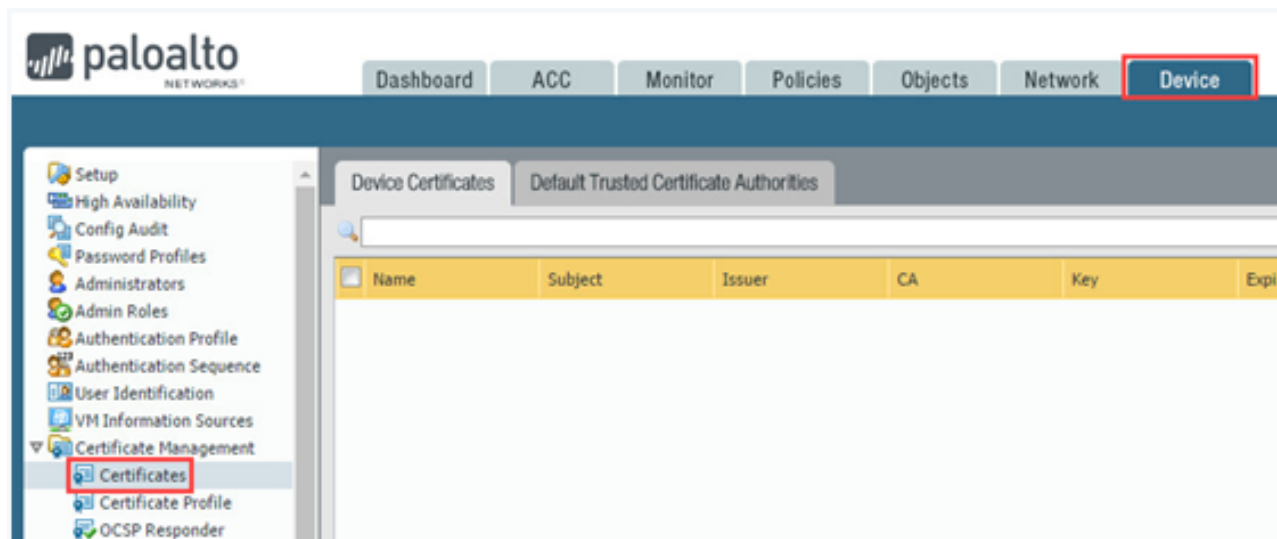
## 7.2 Import SSL Certificate

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.

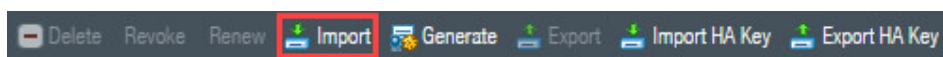
1. Click on the **Chromium** icon from the taskbar to maximize the Firewall management interface.



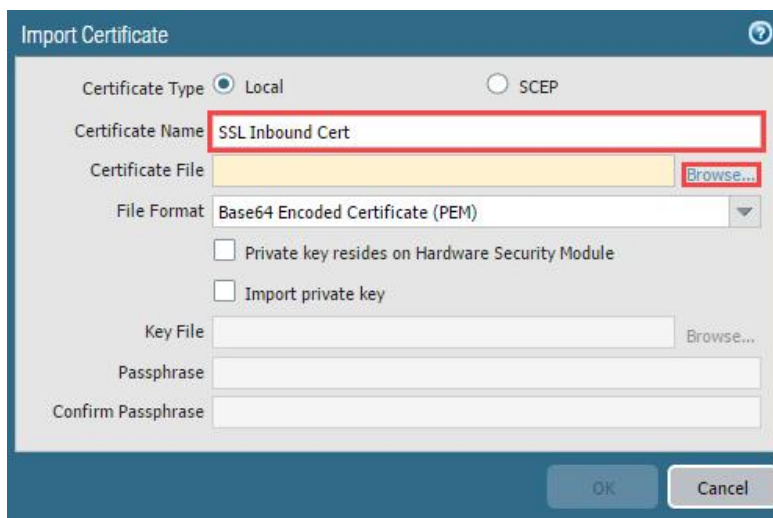
2. Navigate to **Device > Certificate Management > Certificates**.



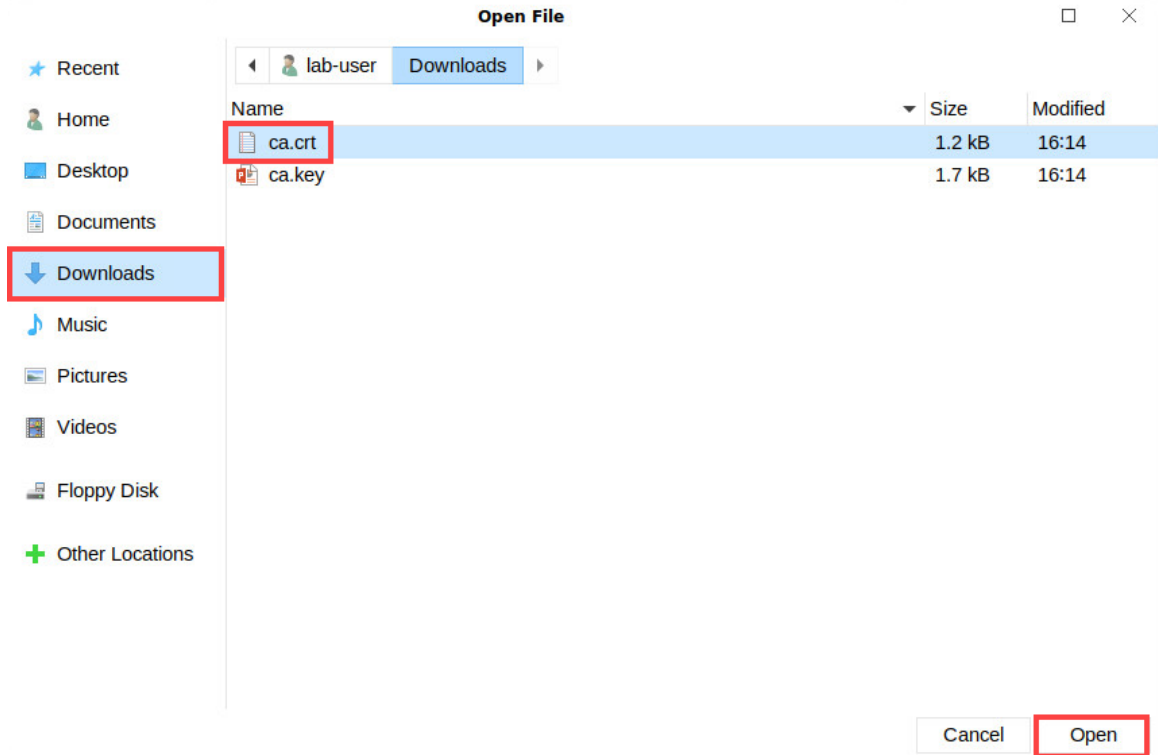
3. Click on the **Import** button at the bottom-center of the center section.



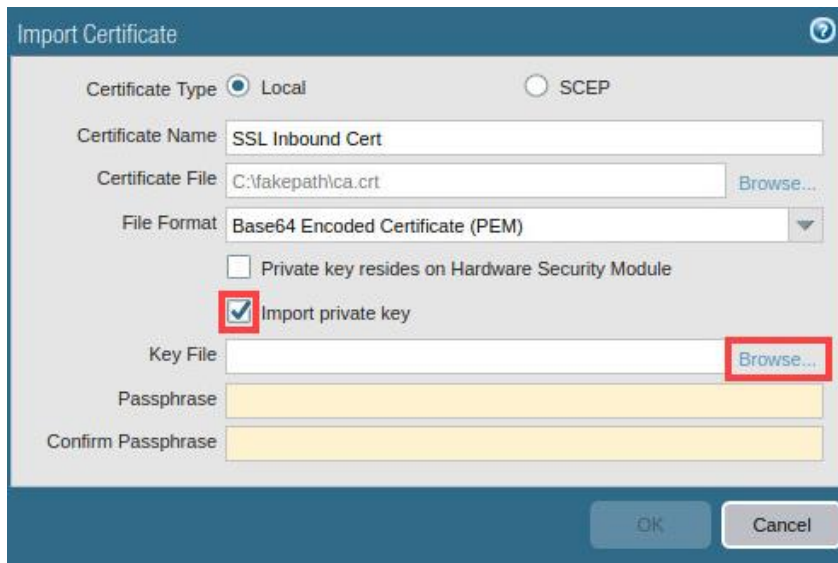
4. In the *Import Certificate* window, type **SSL inbound cert.** Then, click **Browse...**



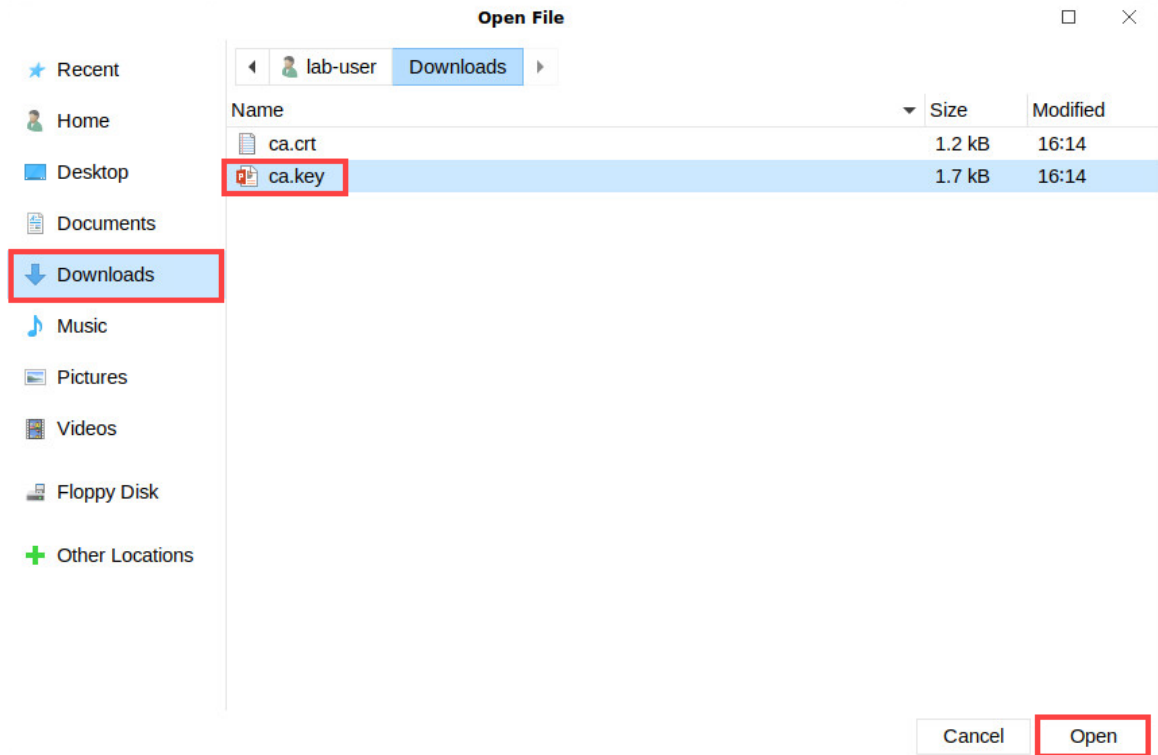
5. In the *Open File* window, select **Downloads** on the left. Then, select **ca.crt**. Finally, click the **Open** button.



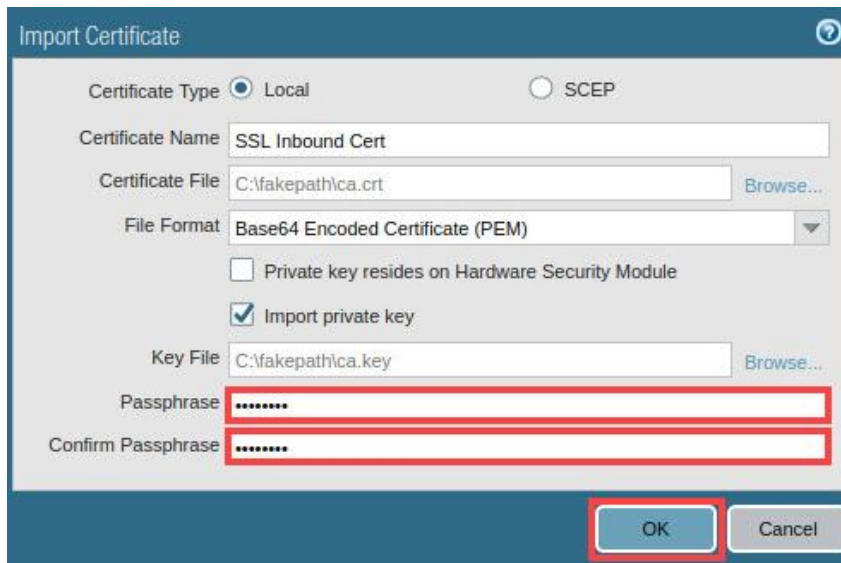
6. Click the checkbox for **Import private key**. Then, click **Browse...**



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 **pa1oa1to** for the *Passphrase* and *Confirm Passphrase* fields. Then, click the **OK** button.





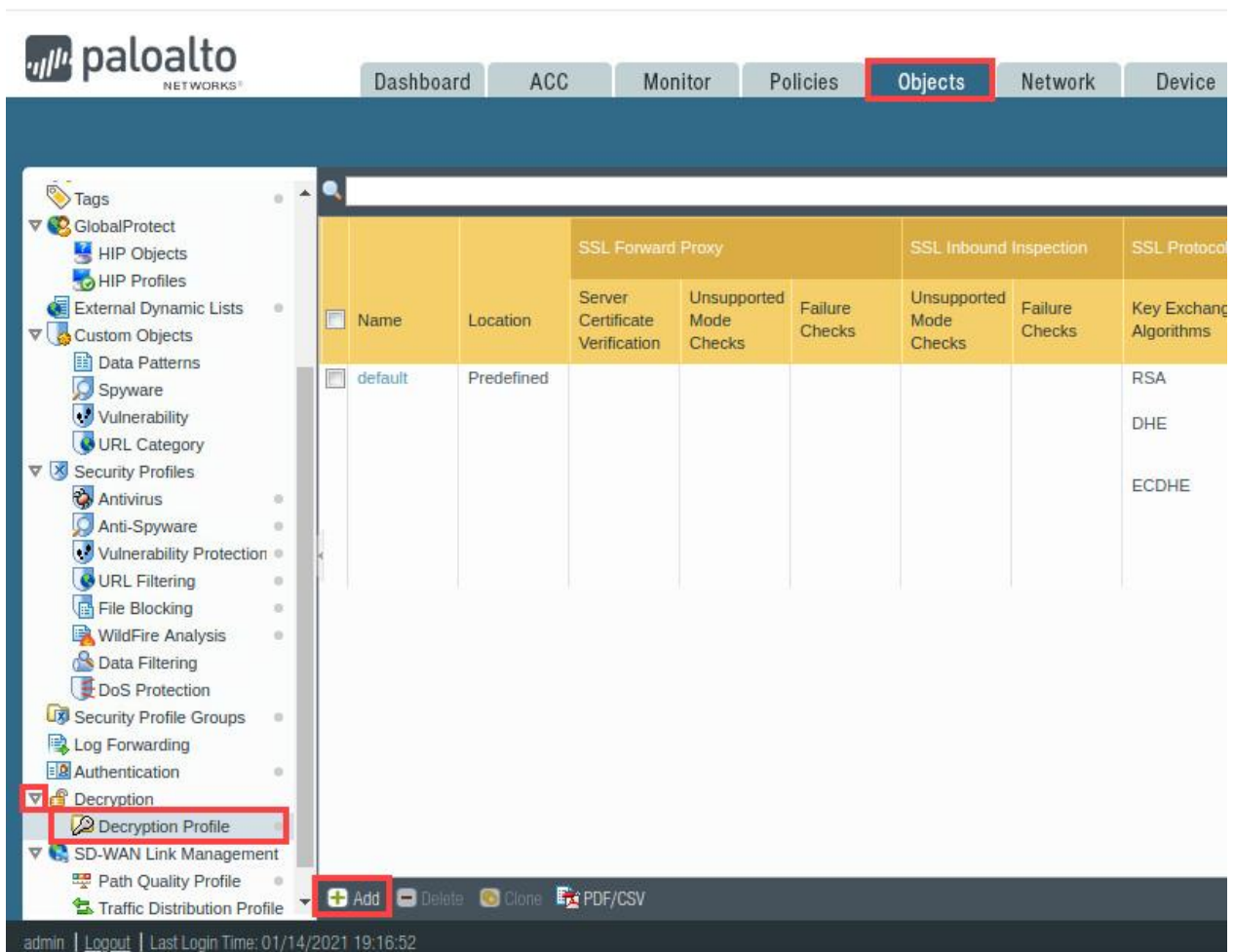
### 9. Verify the *SSL Inbound Cert* is showing a status of **valid**.

Name	Subject	Issuer	CA	Key	Expires	Status
SSL Inbound Cert	C = US, ST = PA, L = PA, O = PA, OU = PA, CN = 192.168.50.10	C = US, ST = PA, L = PA, O = PA, OU = PA, CN = 192.168.50.10	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Jan 12 18:50:14 2051 GMT	valid

## 7.3 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.

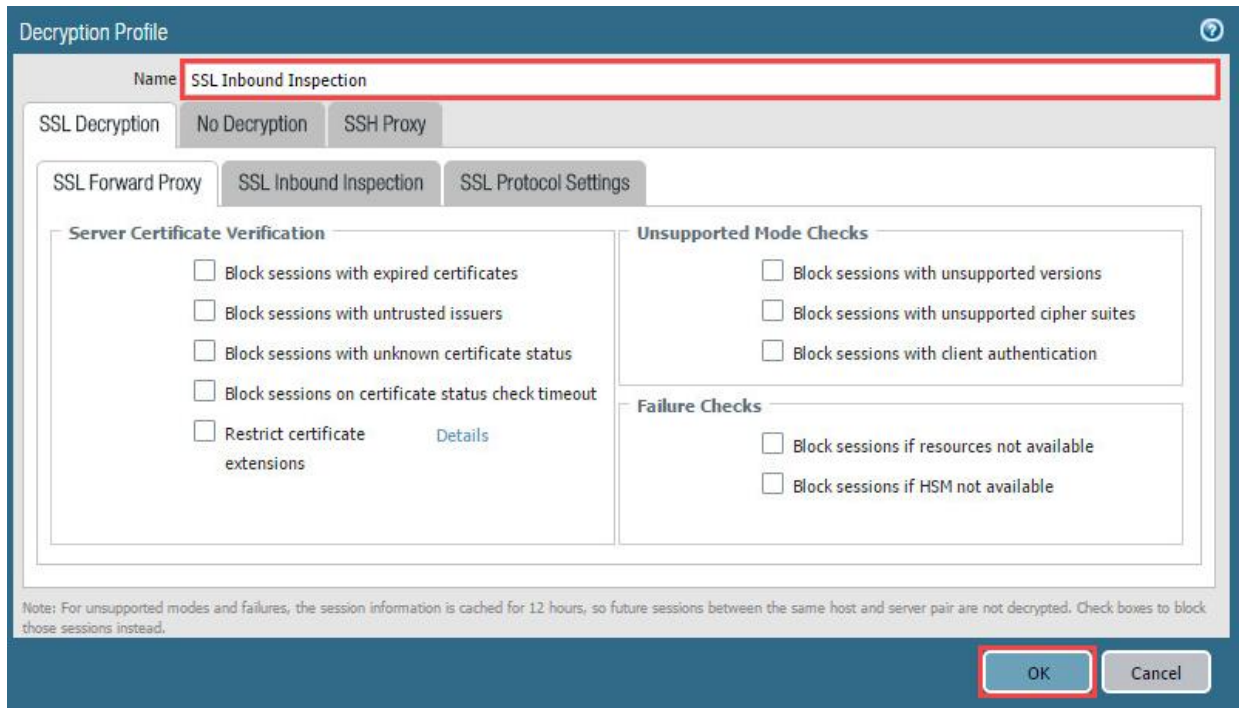


The screenshot shows the Palo Alto Networks management interface. The top navigation bar includes 'Dashboard', 'ACC', 'Monitor', 'Policies', 'Objects' (highlighted with a red box), 'Network', and 'Device'. The left sidebar contains a tree view of configuration categories. Under 'Security Profiles', the 'Decryption' category is expanded, and 'Decryption Profile' is highlighted with a red box. At the bottom of the sidebar, the 'Add' button is also highlighted with a red box. The main content area displays a table of existing decryption profiles. The table has columns for 'Name', 'Location', 'Server Certificate Verification', 'Unsupported Mode Checks', 'Failure Checks', 'SSL Forward Proxy', 'SSL Inbound Inspection', and 'SSL Protocol'. A single profile named 'default' is listed with a 'Predefined' location. The bottom status bar shows 'admin | Logout | Last Login Time: 01/14/2021 19:16:52'.

Name	Location	SSL Forward Proxy			SSL Inbound Inspection		SSL Protocol
		Server Certificate Verification	Unsupported Mode Checks	Failure Checks	Unsupported 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](#)

**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

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**

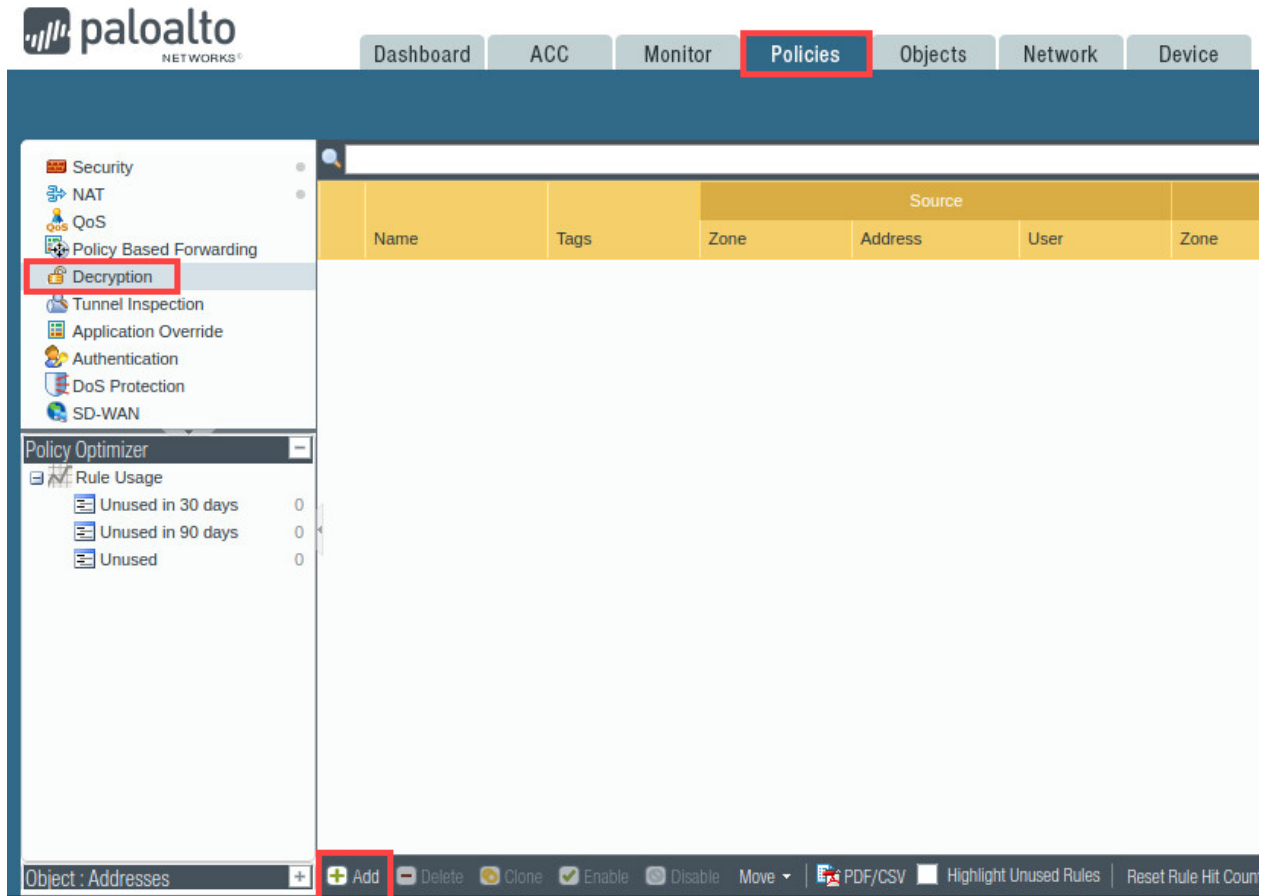
- Verify the **SSL Inbound Inspection** Decryption Profile was created.

	Name	Location	SSL Forward Proxy			SSL Inbound Inspection		SSL Protocol Settings			
			Server Certificate Verification	Unsupported Mode Checks	Failure Checks	Unsupported Mode Checks	Failure Checks	Key Exchange Algorithms	Protocol Versions	Encryption Algorithms	Authentication Algorithms
<input type="checkbox"/>	default	Predefined						RSA DHE ECDHE	Min Version: TLSv1.0 Max Version: Max	3DES RC4 AES128-CBC AES256-CBC AES128-GCM AES256-GCM	SHA1 SHA256 SHA384
<input checked="" type="checkbox"/>	SSL Inbound Inspection							RSA DHE ECDHE	Min Version: TLSv1.0 Max Version: Max	3DES RC4 AES128-CBC AES256-CBC AES128-GCM AES256-GCM	SHA1 SHA256 SHA384

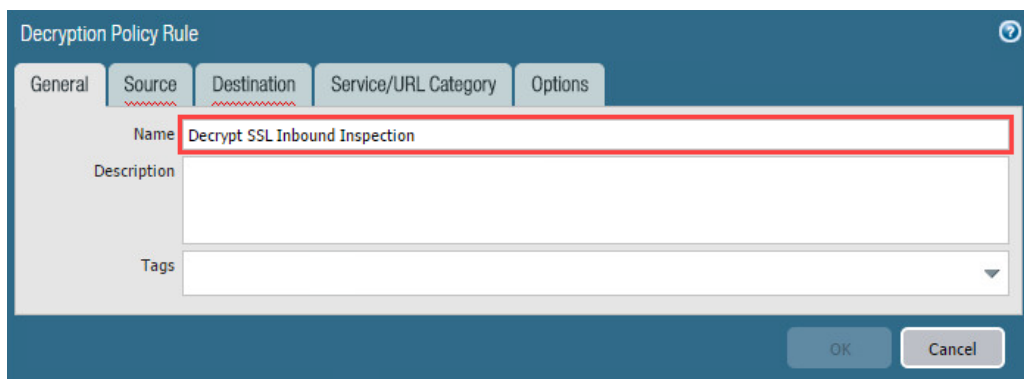
## 7.4 Create a Decryption Policy

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.

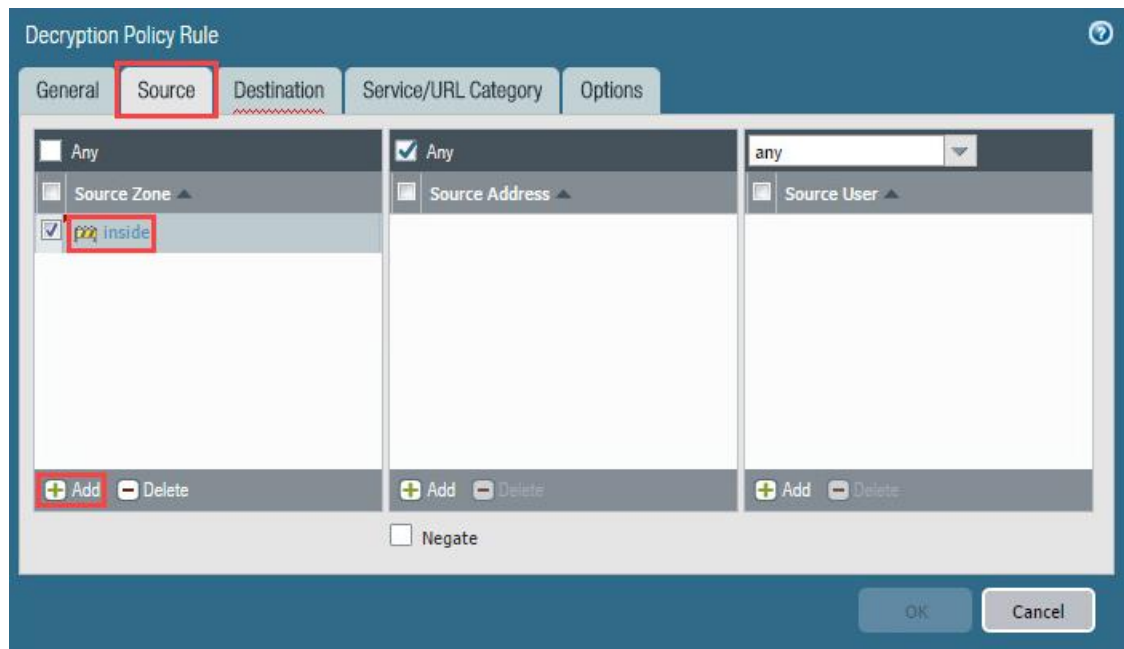
1. Navigate to **Policies > Decryption > Add**.



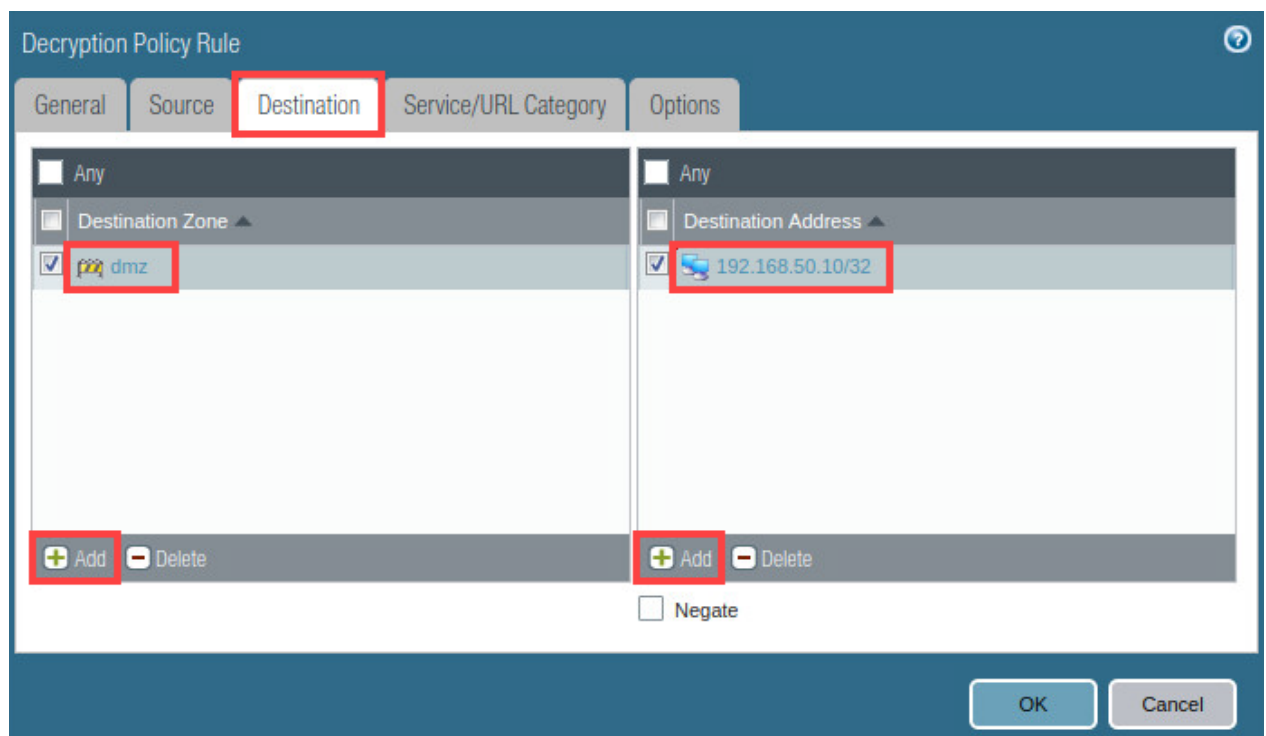
2. In the *Decryption Policy Rule* window, type **Decrypt SSL Inbound Inspection** in the *Name* field.



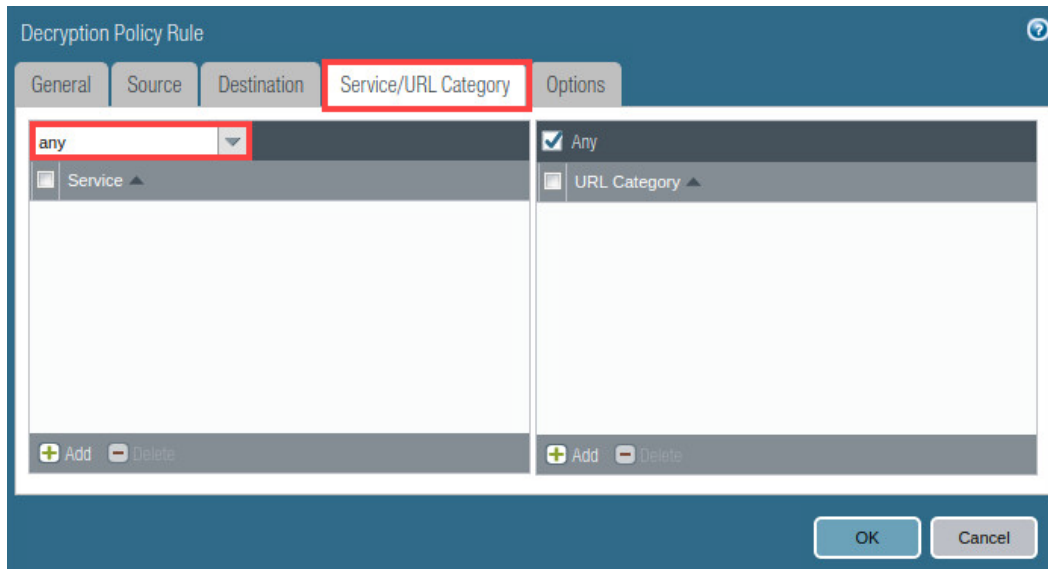
3. In the *Decryption Policy Rule* window, click on the **Source** tab. Then, click **Add** in the *Source Zone* section. Next, select **inside**.



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**.

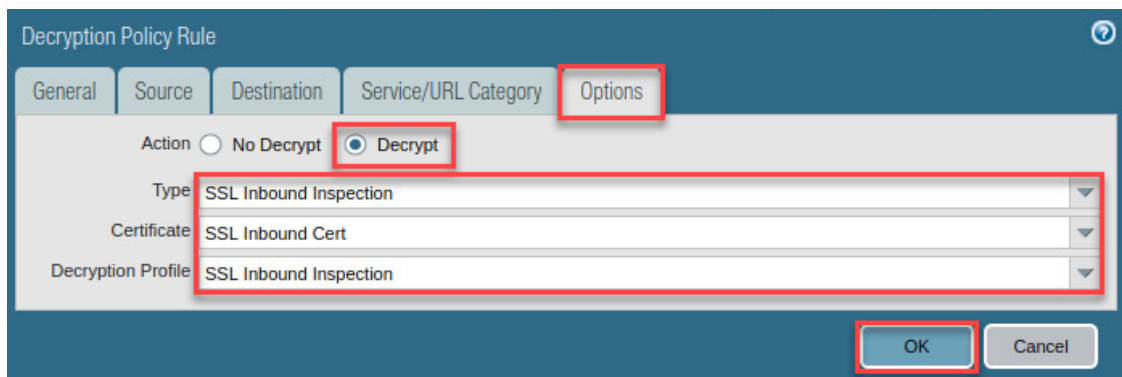


- In the *Decryption Policy Rule* window, click on the **Service/URL Category** tab. In the *Service* pane, select and verify **any** is selected in the dropdown menu.



The screenshot shows the 'Decryption Policy Rule' window with the 'Service/URL Category' tab selected. The 'Service' dropdown menu is open, and 'any' is selected. The 'URL Category' dropdown menu is also open, and 'Any' is selected. The 'Add' and 'Delete' buttons are visible 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 'OK' button is highlighted.

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

	Name	Tags	Source			Destination		URL Category	Service	Action
			Zone	Address	User	Zone	Address			
1	Decrypt SSL Inbound...	none	inside	any	any	dmz	192.168.50.10...	any	any	decrypt

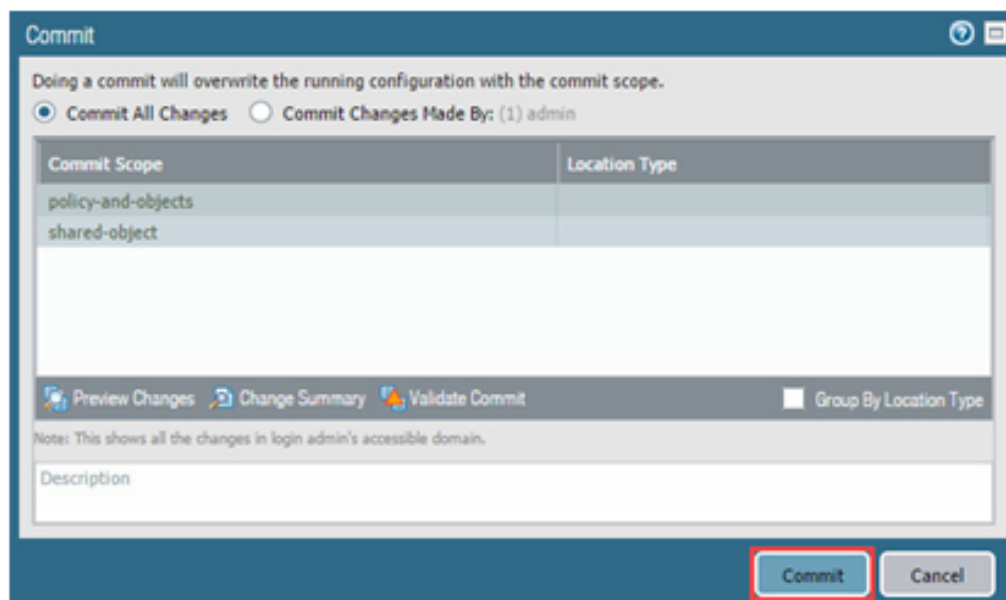
## 7.5 Commit and Test Decryption Policy

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

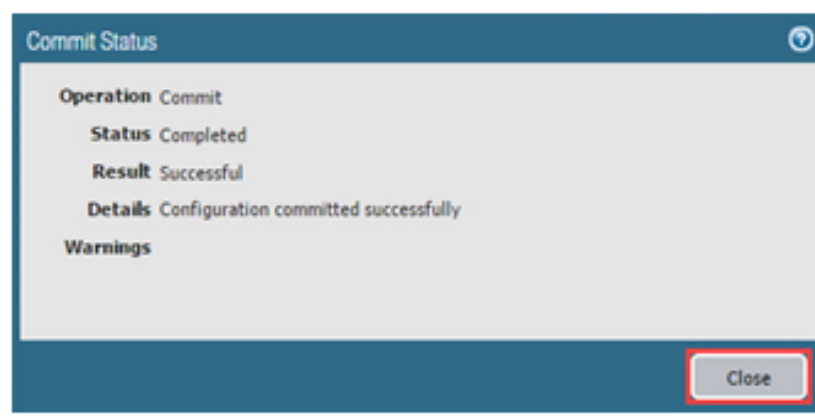
1. Click the **Commit** link located at the top-right of the web interface.



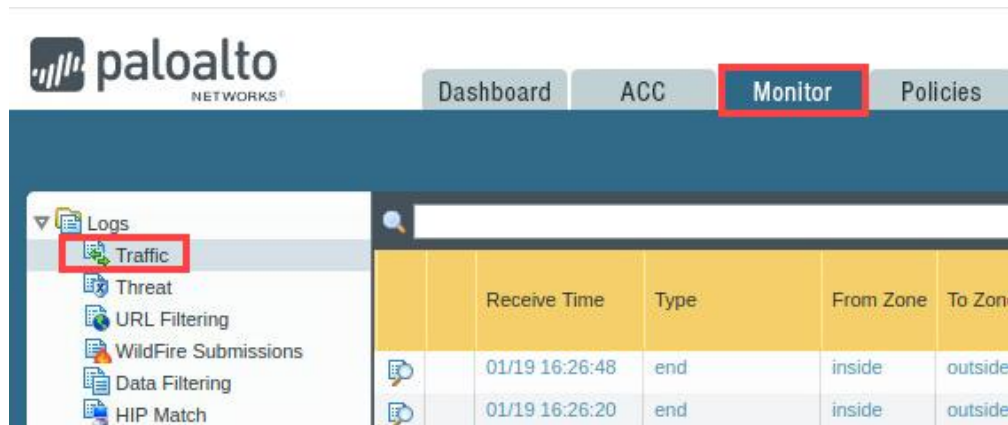
2. In the *Commit* window, click **Commit** to proceed with committing the changes.



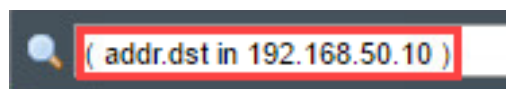
3. When the commit operation successfully completes, click **Close** to continue.



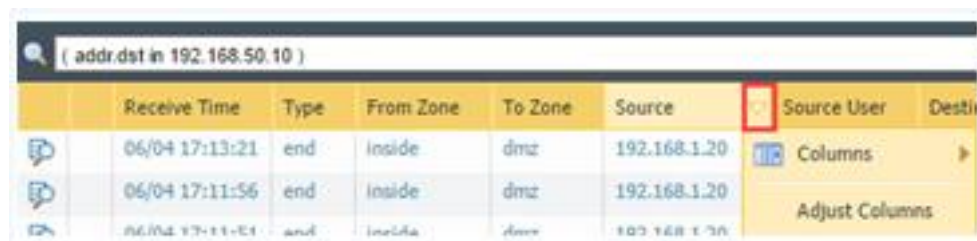
4. Navigate to **Monitor > Logs > Traffic**.



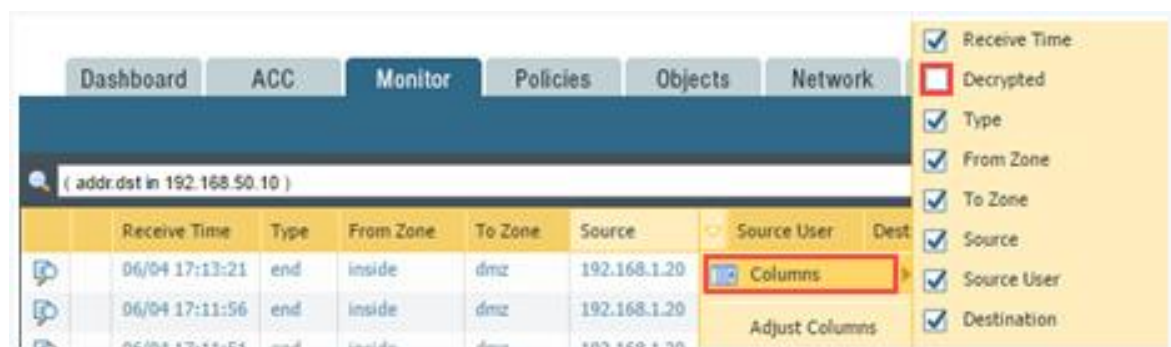
5. In the search box, type ( `addr.dst in 192.168.50.10` ) and press **Enter**.



6. Move the mouse cursor to the right of *Source* and click the **down arrow**.



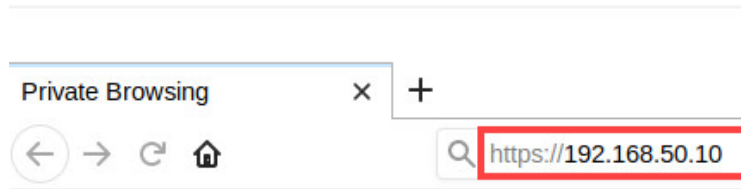
7. Highlight **Columns** and select **Decrypted**.



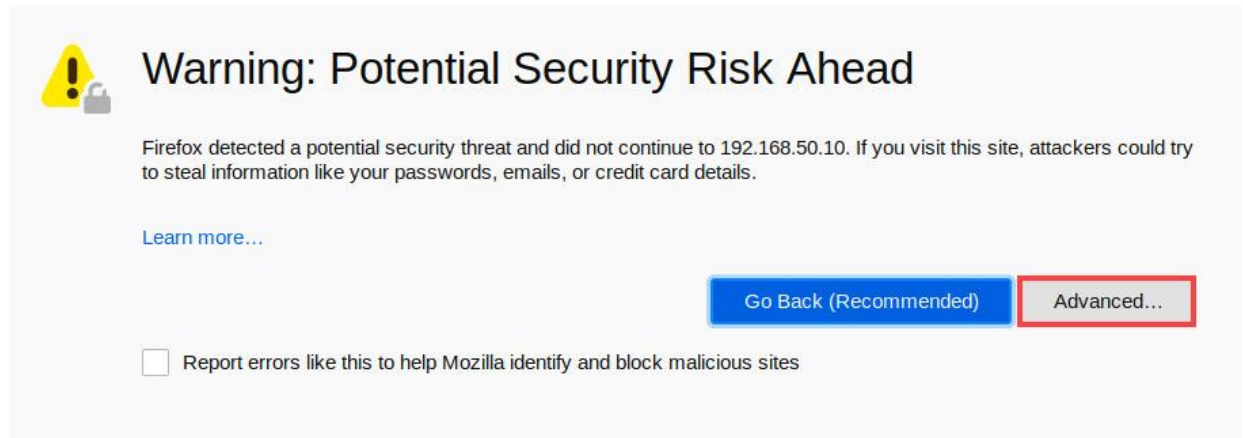
8. Open the *Firefox Web Browser* by clicking on the **Firefox** icon located in the task bar.



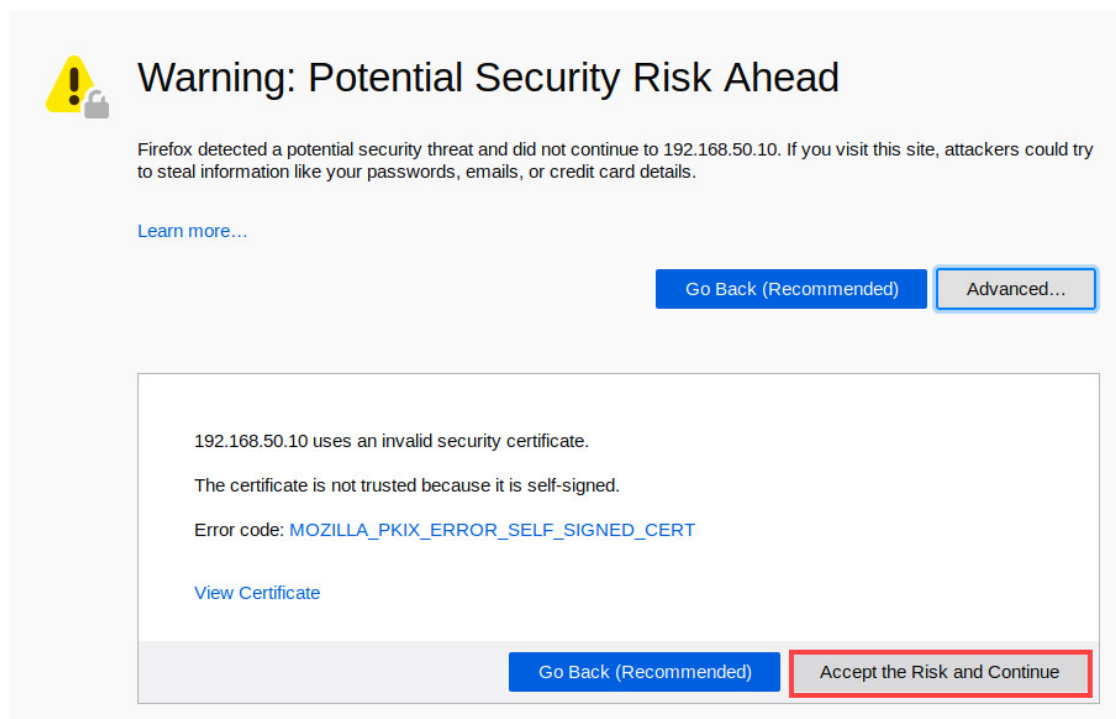
9. In the address bar, type `https://192.168.50.10` and click **Enter**.



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

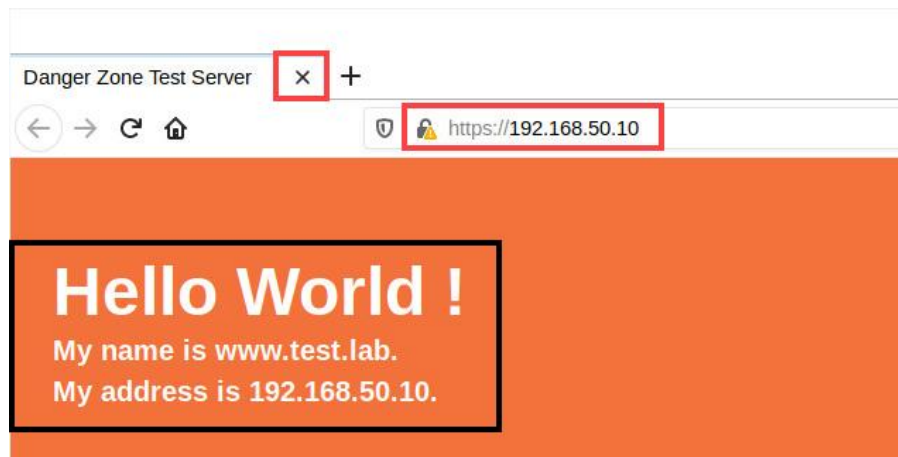


11. Click on **Accept the Risk and Continue**.

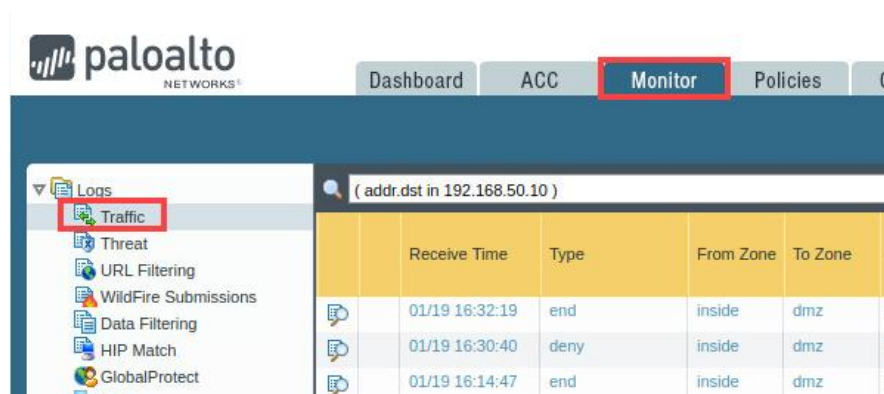




12. Notice that the *Apache HTTP Server Test page* is working properly. Click on the **X** of the tab to close it.



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**. 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	Destination	Dynamic User Group	To Port	Application
	01/19 16:32:19	end	inside	dmz	192.168.1.20	yes		192.168.50.10		443	web-browsing
	01/19 16:30:40	deny	inside	dmz	192.168.1.20	yes		192.168.50.10		443	ssl
	01/19 16:14:47	end	inside	dmz	192.168.1.20	no		192.168.50.10		22	ssh



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 1991 Action allow Action Source from-policy Application ssl Rule Allow-Inside-DMZ Rule UUID 2821a50c-48b4-43fe-9b28-f57e1c944534 Session End Reason policy-deny Category any Device SN IP Protocol tcp Log Action Generated Time 2021/01/19 16:30:40 Start Time 2021/01/19 16:30:40 Receive Time 2021/01/19 16:30:40 Elapsed Time(sec) 0 Tunnel Type N/A	Source User Source 192.168.1.20 Country 192.168.0.0-192.168.255.255 Port 52914 Zone inside Interface ethernet1/2	Destination User Destination 192.168.50.10 Country 192.168.0.0-192.168.255.255 Port 443 Zone dmz Interface ethernet1/3

Details	
Type	deny
Bytes	4015
Bytes Received	2937
Bytes Sent	1078
Repeat Count	1
Packets	11
Packets Received	5
Packets Sent	6
Source UUID	
Destination UUID	
Dynamic User	

Flags	
Captive Portal	<input type="checkbox"/>
Proxy Transaction	<input type="checkbox"/>
Decrypted	<input checked="" type="checkbox"/>
Packet Capture	<input type="checkbox"/>

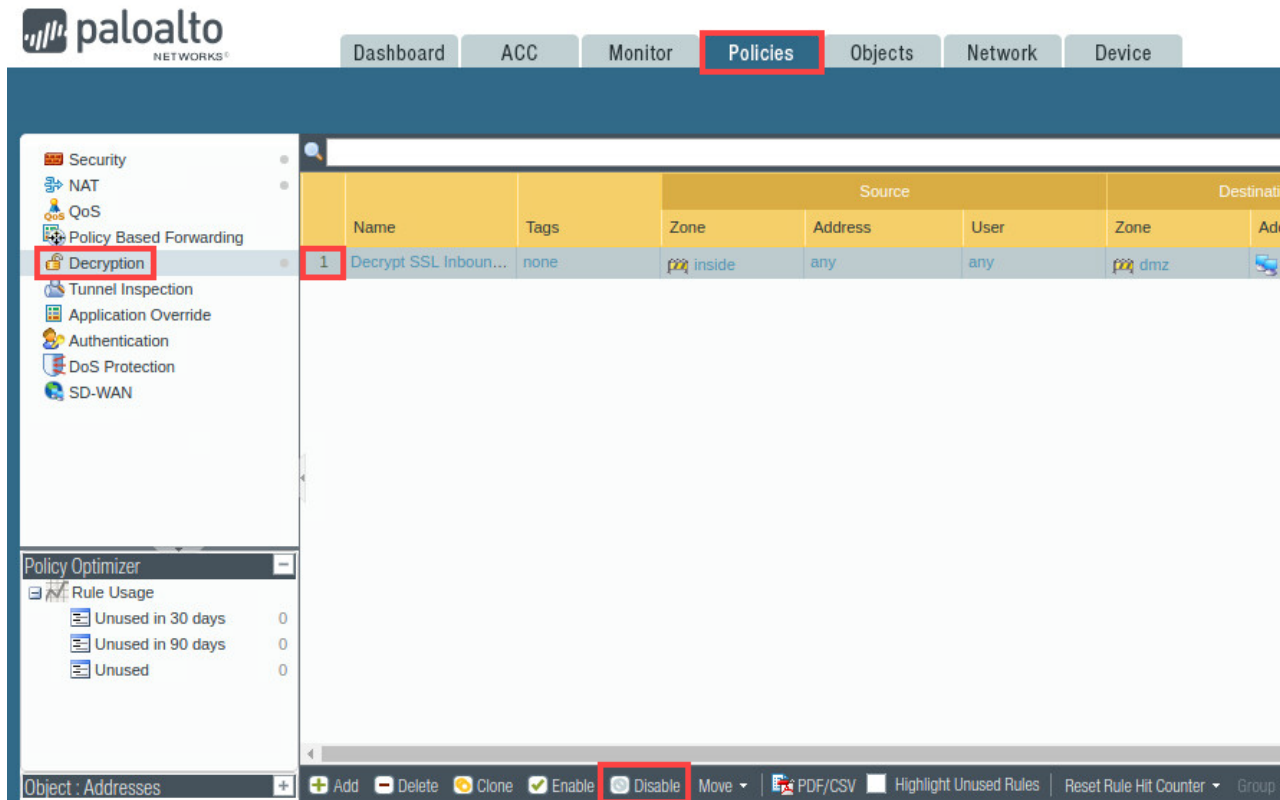
PCAP	Receive Time ▲	Type	Application	Action	Rule	Rule UUID	Bytes	Severity	Category	URL Category List	Verdict	URL	File Name
	2021/01/19 16:30:40	deny	ssl	allow	Allow-Inside-DMZ	2821a5...	4015		any				

**Close**

## 7.6 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.

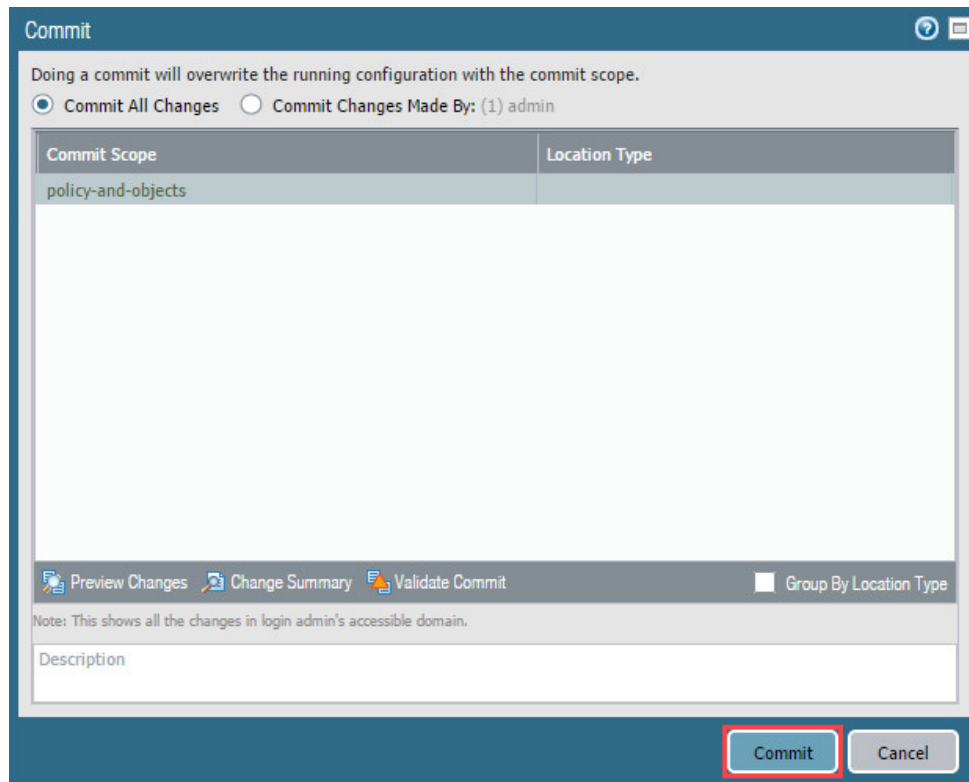
1. Navigate to **Policies > Decryption**. Then, click the **1** for the **Decrypt SSL Inbound Inspection** policy. **Next**, click the **Disable** button.



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.



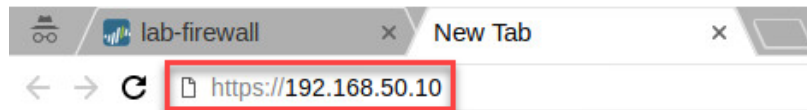
4. When the commit operation successfully completes, click **Close** to continue.



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



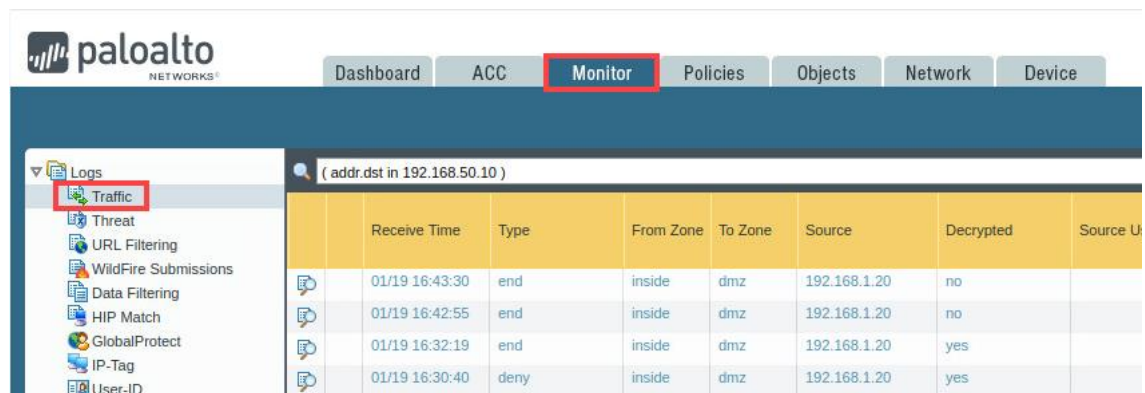
6. In the address bar, type **https://192.168.50.10** and click **Enter**.



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



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



9. Look for traffic associated with the application of **ssl** and the *Decrypted* column set to **no**. 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**.

( addr.dst in 192.168.50.10 )											
	Receive Time	Type	From Zone	To Zone	Source	Decrypted	Source User	Destination	Dynamic User Group	To Port	Application
	01/19 16:43:30	end	inside	dmz	192.168.1.20	no		192.168.50.10		443	ssl
	01/19 16:42:55	end	inside	dmz	192.168.1.20	no		192.168.50.10		443	ssl
	01/19 16:32:19	end	inside	dmz	192.168.1.20	yes		192.168.50.10		443	web-browsing
	01/19 16:30:40	deny	inside	dmz	192.168.1.20	yes		192.168.50.10		443	ssl

10. 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 2125</p> <p>Action allow</p> <p>Action Source from-policy</p> <p>Application ssl</p> <p>Rule Allow-Inside-DMZ</p> <p>Rule UUID 2821a50c-48b4-43fe-9b28-f57e1c944534</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 2021/01/19 16:43:30</p> <p>Start Time 2021/01/19 16:43:15</p> <p>Receive Time 2021/01/19 16:43:30</p> <p>Elapsed Time(sec) 0</p> <p>Tunnel Type N/A</p>	<p>Source User</p> <p>Source 192.168.1.20</p> <p>Country 192.168.0.0-192.168.255.255</p> <p>Port 53014</p> <p>Zone inside</p> <p>Interface ethernet1/2</p>	<p>Destination User</p> <p>Destination 192.168.50.10</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>
	<p>Details</p> <p>Type end</p> <p>Bytes 2768</p> <p>Bytes Received 1939</p> <p>Bytes Sent 829</p> <p>Repeat Count 1</p> <p>Packets 14</p> <p>Packets Received 6</p> <p>Packets Sent 8</p> <p>Source UUID</p> <p>Destination UUID</p> <p>Dynamic User Group</p>	<p>Flags</p> <p>Captive Portal <input type="checkbox"/></p> <p>Proxy Transaction <input type="checkbox"/></p> <p><b>Decrypted</b> <input type="checkbox"/></p> <p>Packet Capture <input type="checkbox"/></p> <p>Client to Server <input type="checkbox"/></p>

PCAP	Receive Time ▲	Type	Application	Action	Rule	Rule UUID	Bytes	Severity	Category	URL Category List	Verdict	URL	File Name
	2021/01/19 16:43:30	end	ssl	allow	Allow-Inside-DMZ	2821a5...	2768		any				

Close

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