# NETWORK SECURITY FUNDAMENTALS V2

# Lab 7: Decrypting SSL Inbound Traffic

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

# Contents

## Introduction

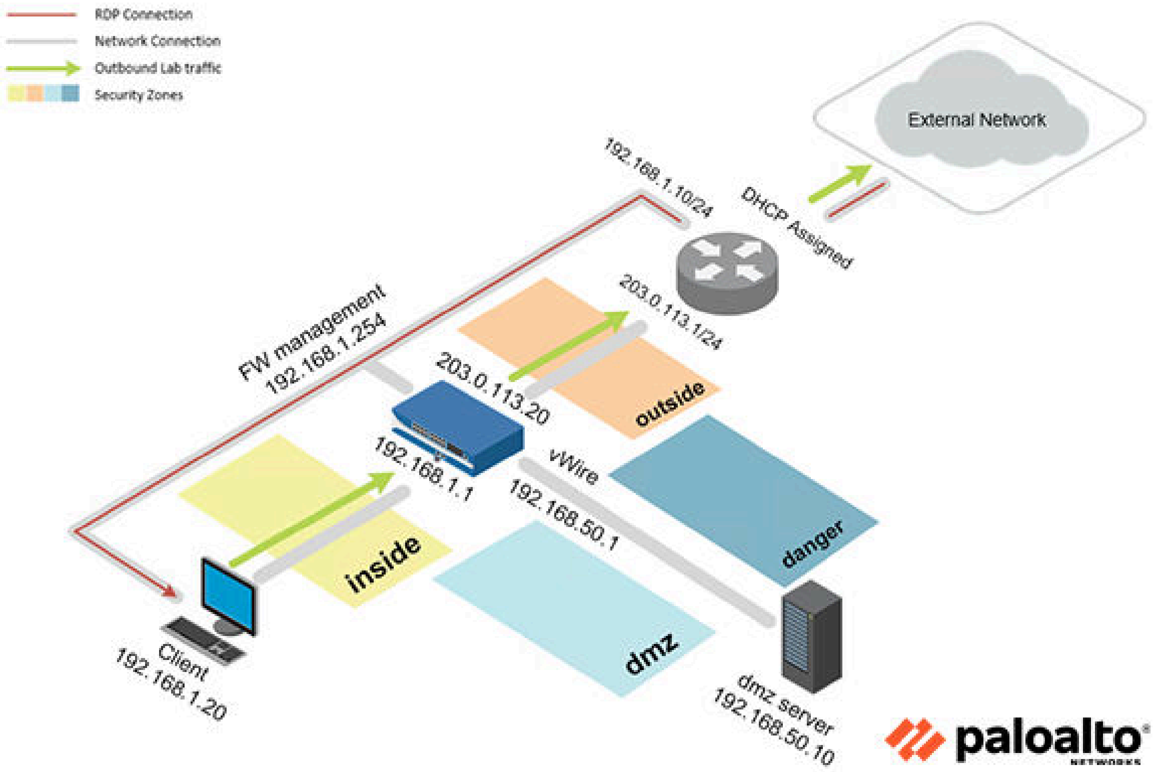
In this lab, you will decrypt SSL inbound traffic and inspect SSL traffic from the Client machine to the DMZ server. When the SSL server certificate is loaded on the Firewall, and an SSL decryption policy is configured for the inbound traffic, the device can then decrypt and read the traffic as it forwards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

## Objective

In this lab, you will perform the following tasks:

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

## Lab Topology



## Lab Settings

The information in the table below will be needed in order to complete the lab.  The task sections below provide details on the use of this information.

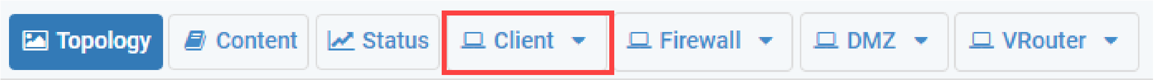
| **Virtual Machine** | **IP Address** | **Account**<br>(if needed) | **Password**<br>(if needed) |
|---|---|---|---|
| Client | 192.168.1.20 | `lab-user` | `Pal0Alt0!` |
| DMZ | 192.168.50.10 | `root` | `Pal0Alt0!` |
| Firewall | 192.168.1.254 | `admin` | `Pal0Alt0!` |

# 1 Decrypting SSL Inbound Traffic

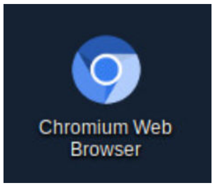
## 1.0 Load Lab Configuration

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

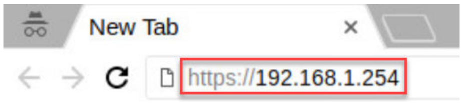
1. Click on the **Client** tab to access the Client PC.



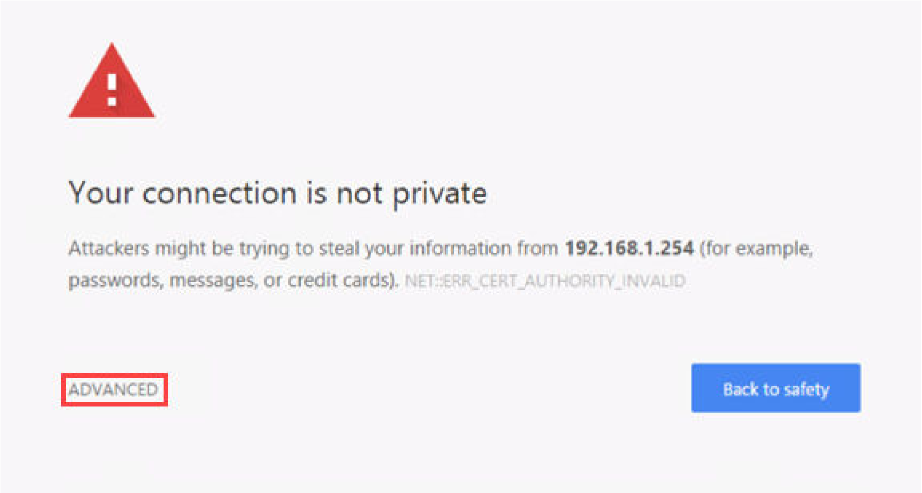
2. Log in to the Client PC as username `lab-user`, password `Pal0Alt0!`.
3. Double-click the **Chromium Web Browser** icon located on the desktop.



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



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

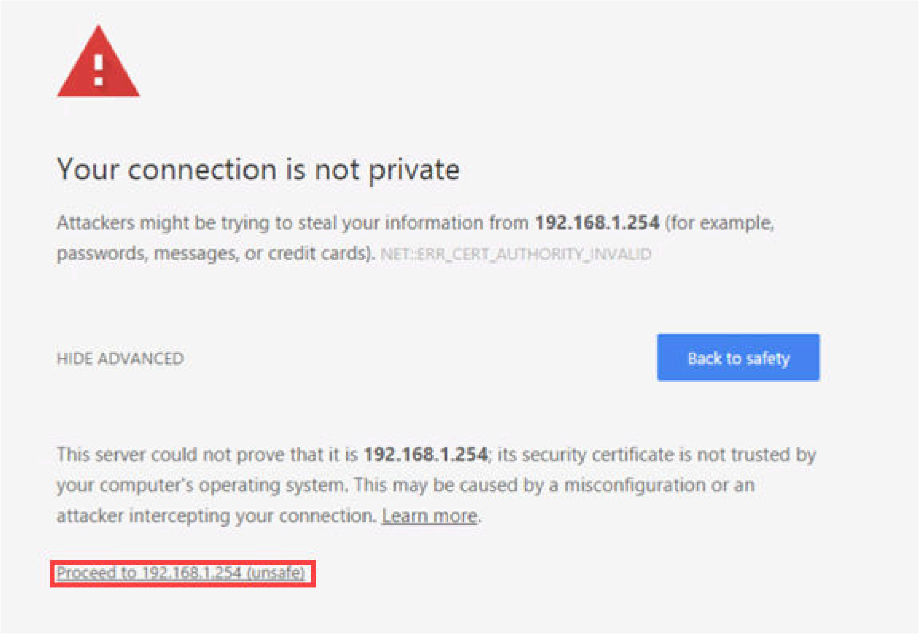


Your connection is not private

Attackers might be trying to steal your information from **192.168.1.254** (for example, passwords, messages, or credit cards). NET::ERR_CERT_AUTHORITY_INVALID

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)**.

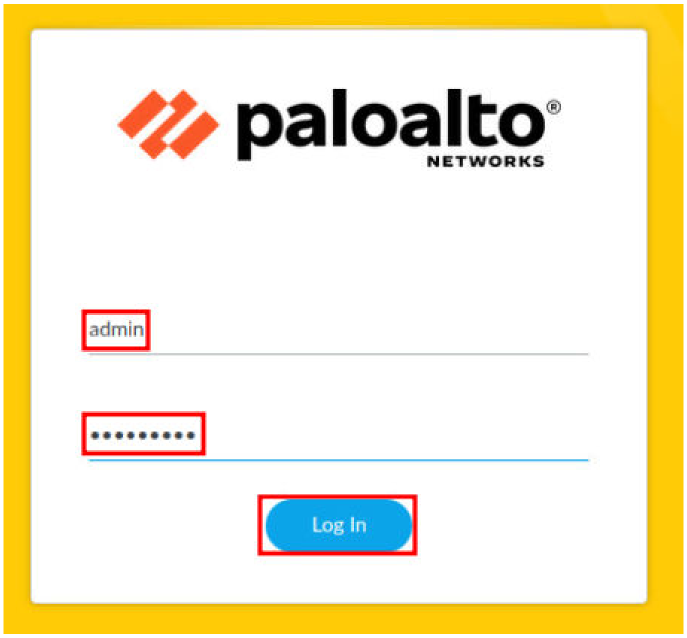


Your connection is not private

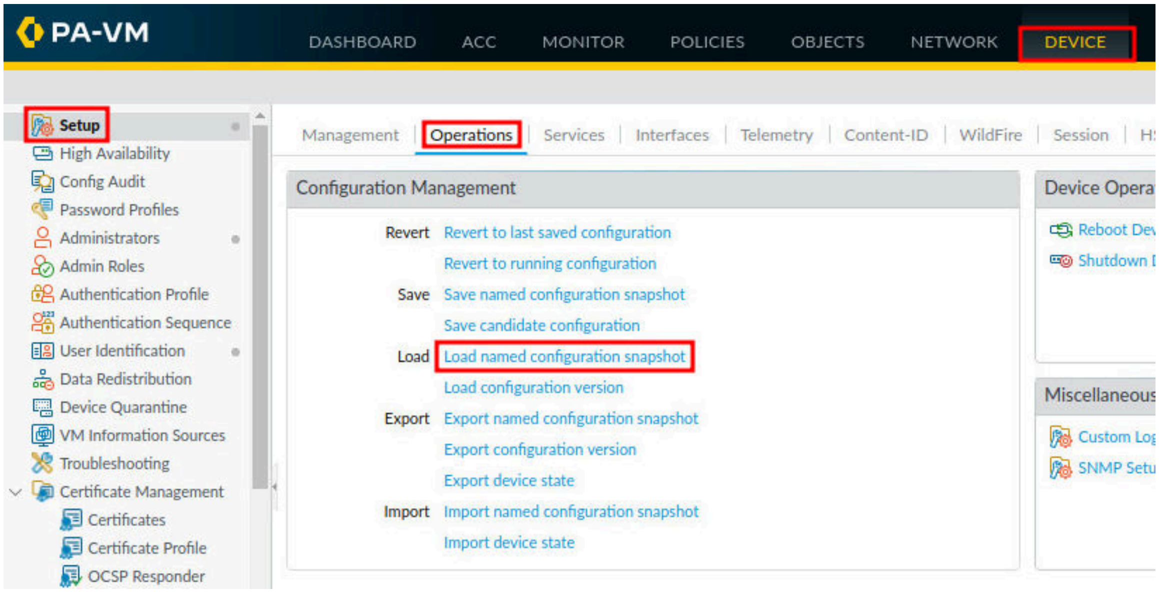
Attackers might be trying to steal your information from **192.168.1.254** (for example, passwords, messages, or credit cards). NET::ERR_CERT_AUTHORITY_INVALID

This server could not prove that it is **192.168.1.254**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection. Learn more.

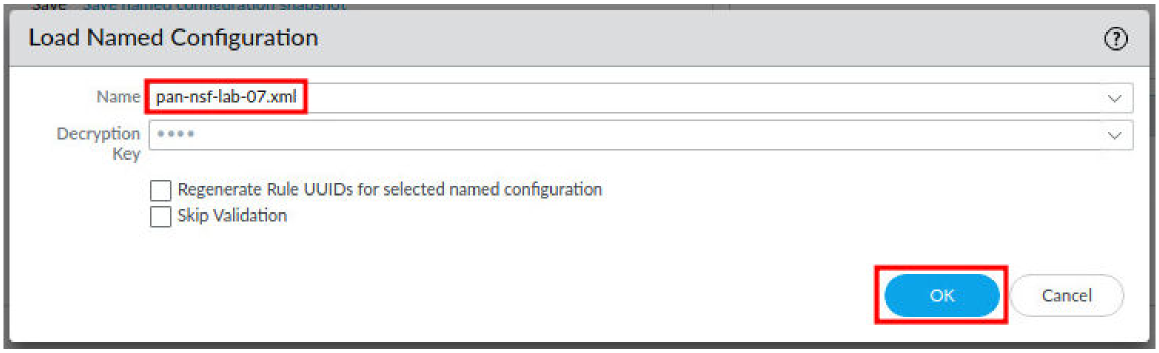
7. Log in to the Firewall web interface as username `admin`, password `Pal0Alt0!`.



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



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


Load Named Configuration

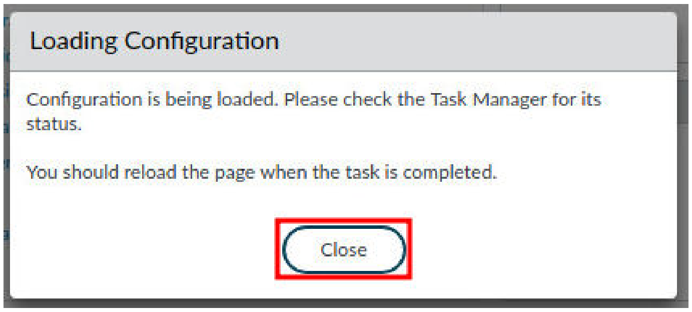
Name: pan-nsf-lab-07.xml

Decryption Key: ••••

□ Regenerate Rule UUIDs for selected named configuration

□ Skip Validation

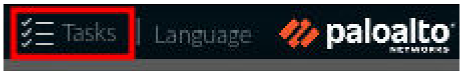
10. In the Loading Configuration window, a message will show *Configuration is being loaded*. *Please check the Task Manager for its status. You should reload the page when the task is completed.* Click **Close** to continue.


Loading Configuration

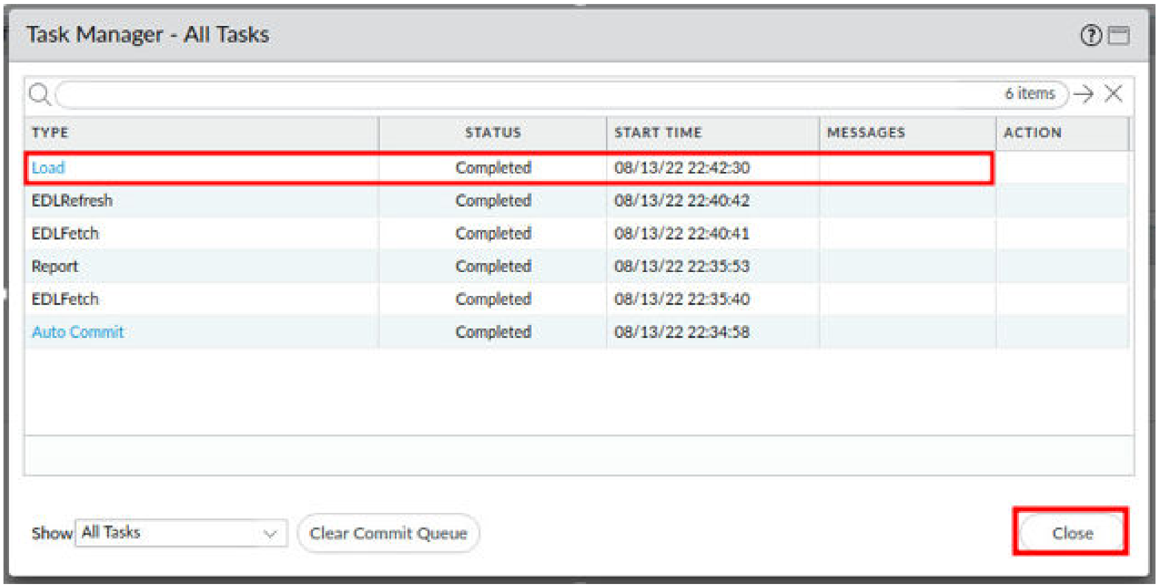
Configuration is being loaded. Please check the Task Manager for its status.

You should reload the page when the task is completed.

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.**

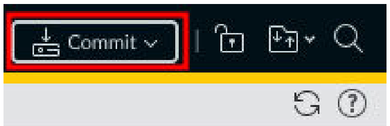


Task Manager - All Tasks

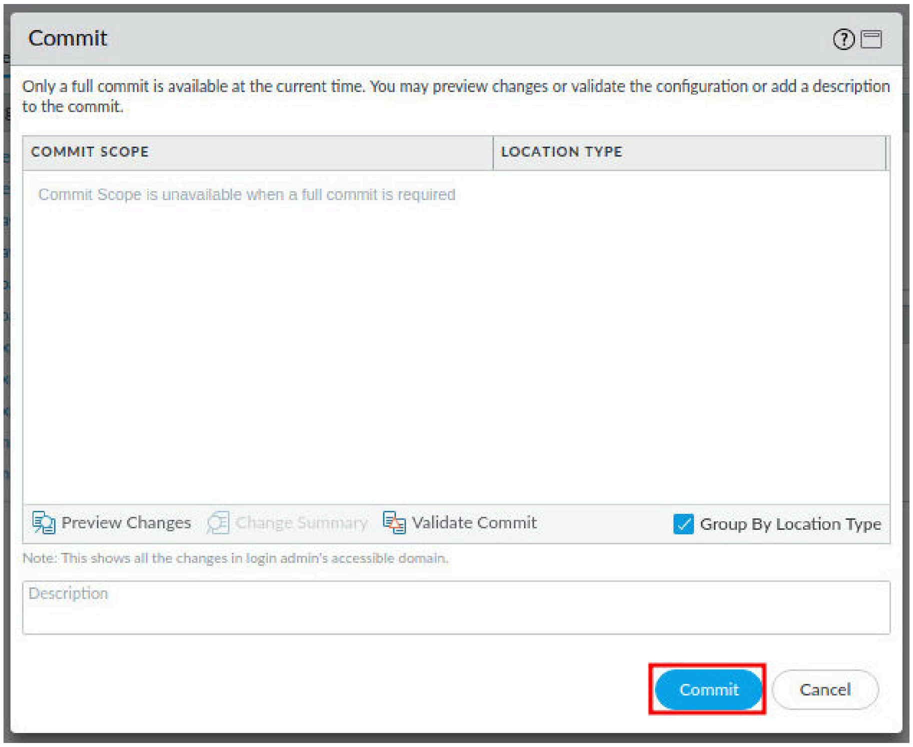
6 items

| 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.



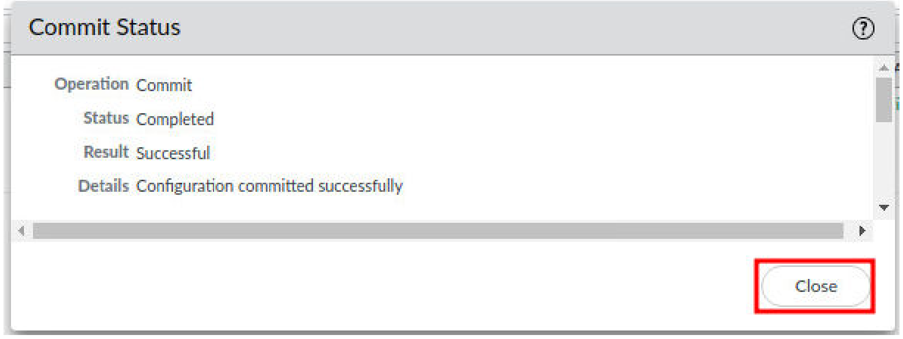
Commit

Only a full commit is available at the current time. You may preview changes or validate the configuration or add a description to the commit.

| COMMIT SCOPE | LOCATION TYPE |
|---|---|
| Commit Scope is unavailable when a full commit is required | |

Note: This shows all the changes in login admin's accessible domain.

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



Commit Status

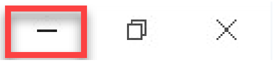
Operation Commit
Status Completed
Result Successful
Details Configuration committed successfully

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

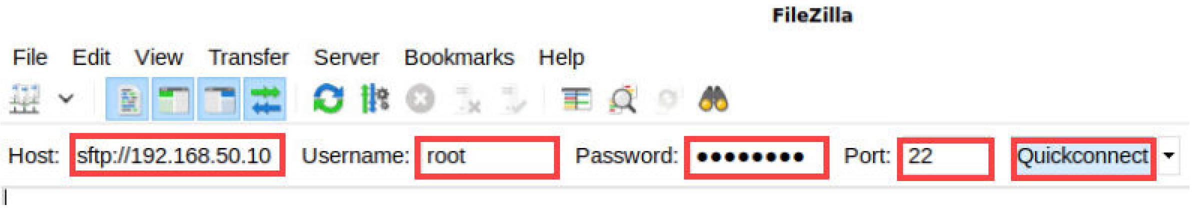
In this section, you will use WinSCP to download the certificate and key that is being used on the DMZ server. WinSCP is a free, open-source tool used to transfer secure files between clients.

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



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

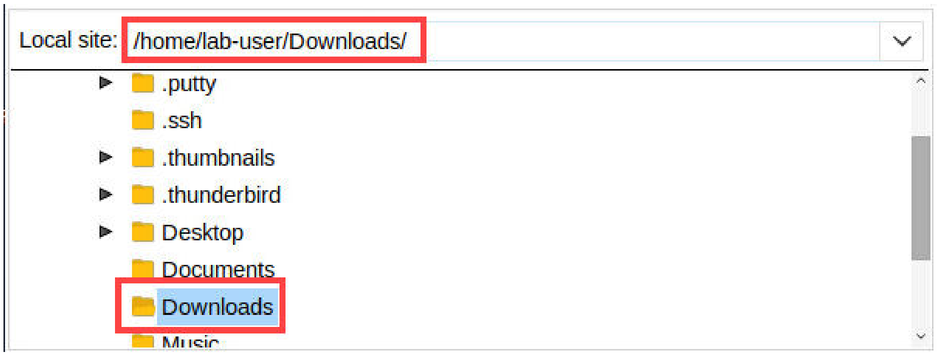
3. In the *FileZilla* window, type `sftp://192.168.50.10` for the *Host*, type `root` for the *Username*, type `Pal0Alt0!` for the *Password*, lastly, type 22 for the *Port*. Then, click the **Quickconnect** button.



Host: sftp://192.168.50.10 Username: root Password: ●●●●●●●● Port: 22

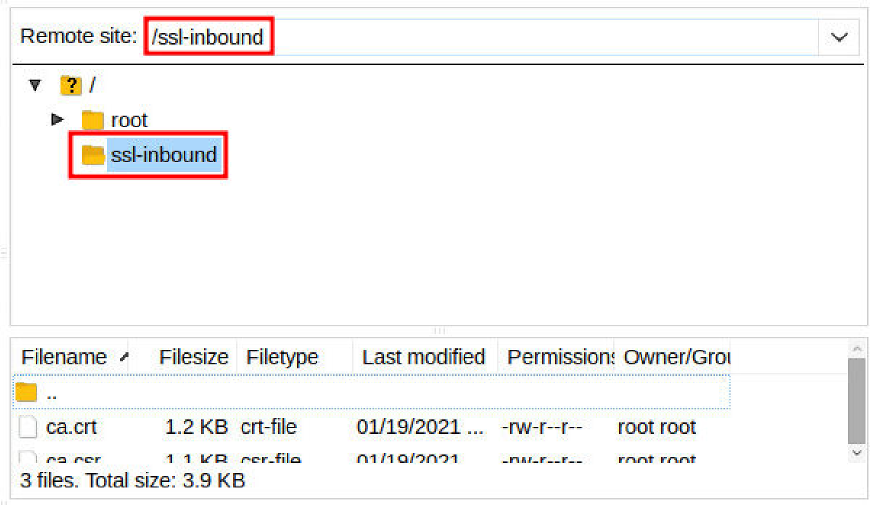
You may be prompted to remember the password after connecting to sftp://192.168.50.10. It is strongly recommended to not save passwords automatically as this could lead to insecure accounts and networks. If prompted to save the password, select **Do not save passwords** and select **OK**.

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



Local site: /home/lab-user/Downloads/

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

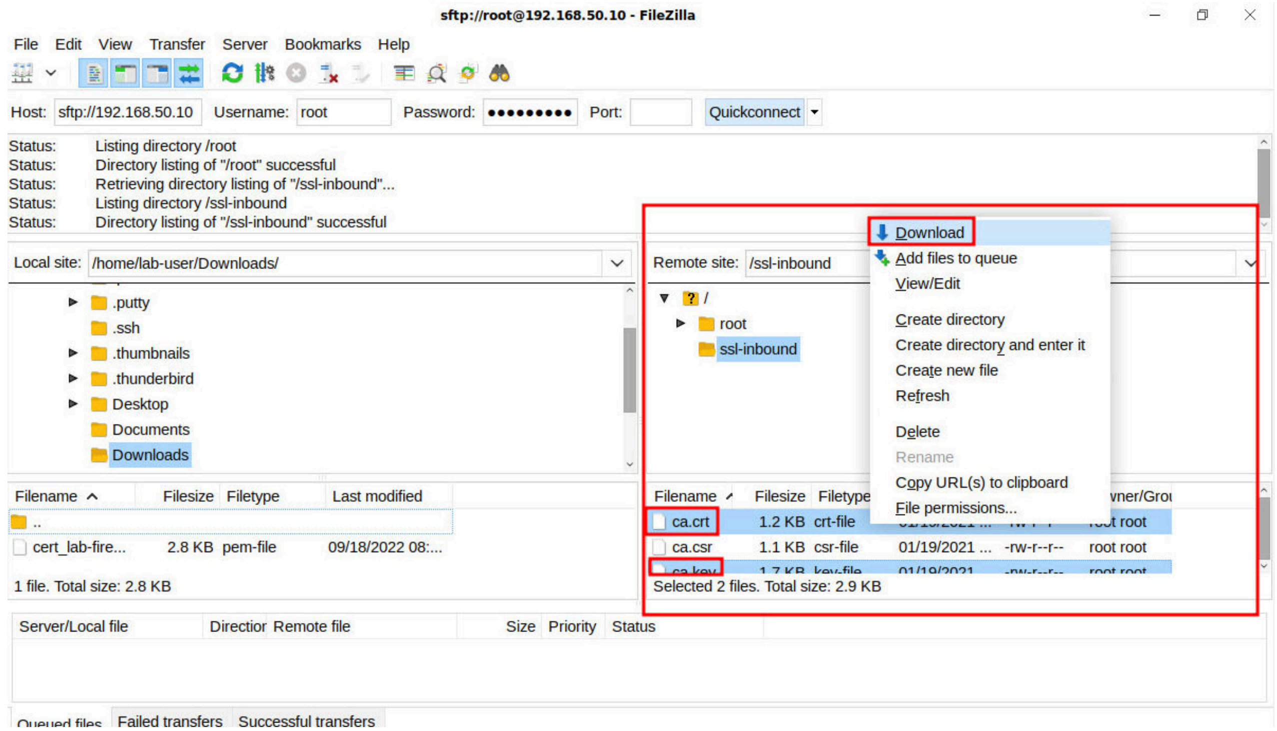


Remote site: /ssl-inbound

| Filename | Filesize | Filetype | Last modified | Permissions | Owner/Grou |
|---|---|---|---|---|---|
| .. | | | | | |
| ca.crt | 1.2 KB | crt-file | 01/19/2021 ... | -rw-r--r-- | root root |
| ca.csr | 1.1 KB | csr-file | 01/19/2021 | -rw-r--r-- | root root |

3 files. Total size: 3.9 KB

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



sftp://root@192.168.50.10 - FileZilla

Host: sftp://192.168.50.10 Username: root Password: ●●●●●●●●● Port:

```
Status:     Listing directory /root
Status:     Directory listing of "/root" successful
Status:     Retrieving directory listing of "/ssl-inbound"...
Status:     Listing directory /ssl-inbound
Status:     Directory listing of "/ssl-inbound" successful
```

Local site: /home/lab-user/Downloads/

| Filename | Filesize | Filetype | Last modified |
|---|---|---|---|
| .. | | | |
| cert_lab-fire... | 2.8 KB | pem-file | 09/18/2022 08:... |

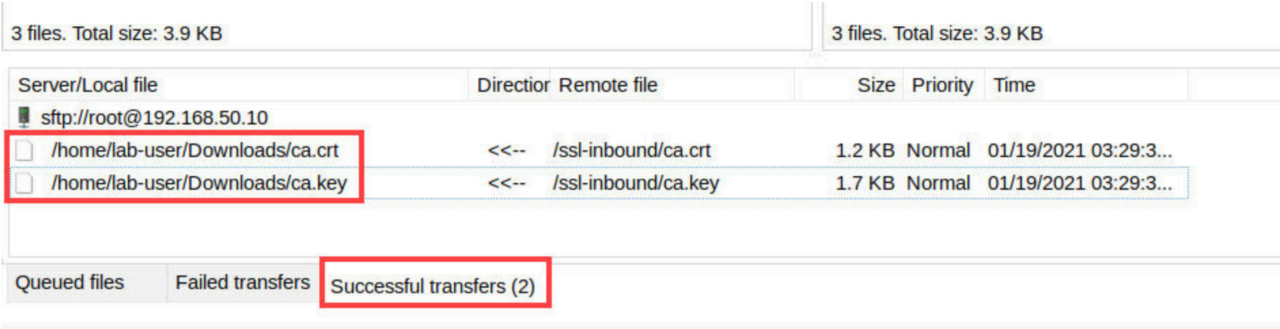
1 file. Total size: 2.8 KB

Remote site: /ssl-inbound

| Filename | Filesize | Filetype | Last modified | Permissions | Owner/Grou |
|---|---|---|---|---|---|
| ca.crt | 1.2 KB | crt-file | 01/19/2021 ... | -rw-r--r-- | root root |
| ca.csr | 1.1 KB | csr-file | 01/19/2021 ... | -rw-r--r-- | root root |
| ca.key | 1.7 KB | key-file | 01/19/2021 | -rw-r--r-- | root root |

Selected 2 files. Total size: 2.9 KB

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

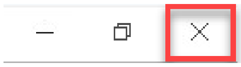


3 files. Total size: 3.9 KB

3 files. Total size: 3.9 KB

| Server/Local file | Directior | 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... |

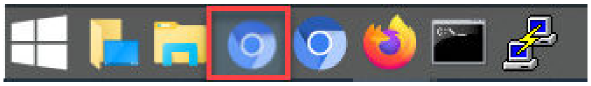
8. Click the **X** in the upper-right to close *FileZilla*.



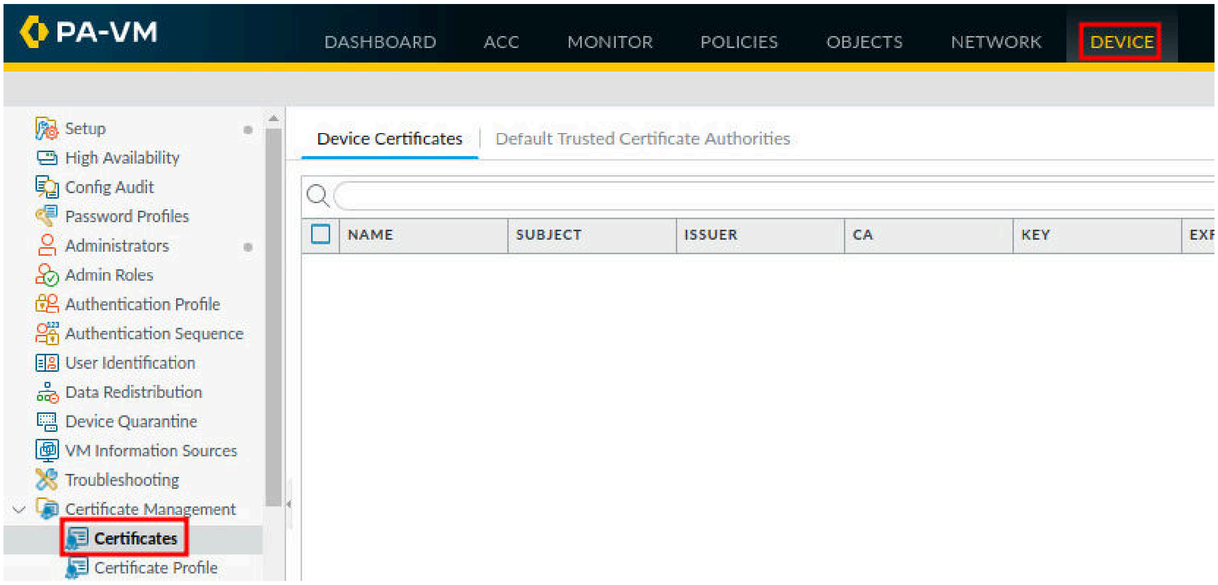
## 1.2 Import SSL Certificate

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

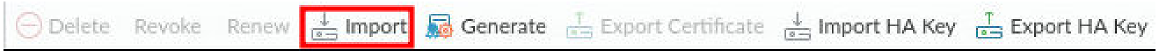
1. Click on the **Chromium** icon from the taskbar to maximize the Firewall management interface.



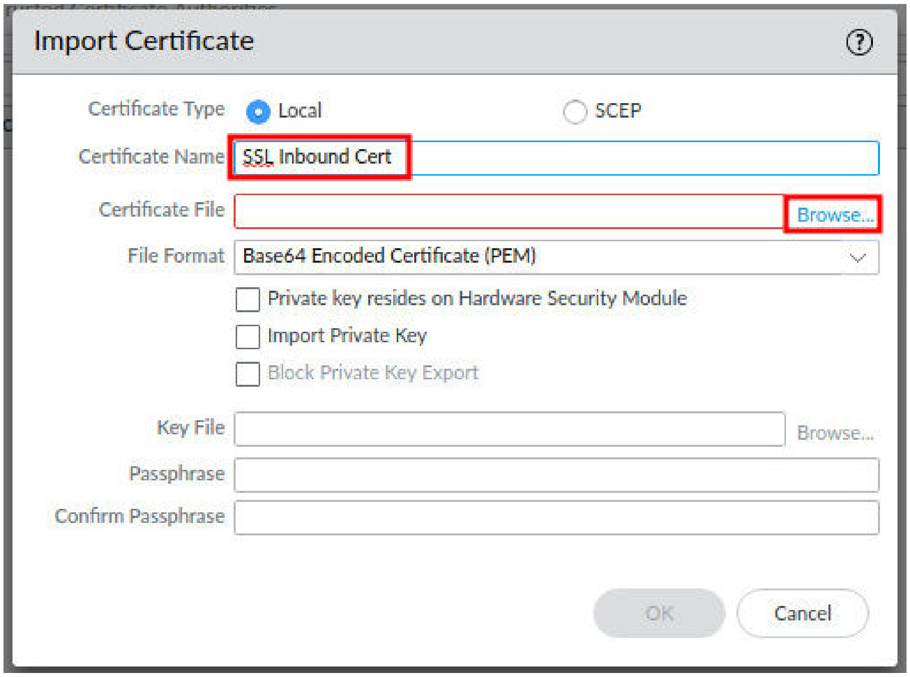
2. Navigate to **Device > Certificate Management > Certificates**.



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



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



Import Certificate

Certificate Type ● Local ○ SCEP

Certificate Name: SSL Inbound Cert

Certificate File:

File Format: Base64 Encoded Certificate (PEM)

□ Private key resides on Hardware Security Module

□ Import Private Key

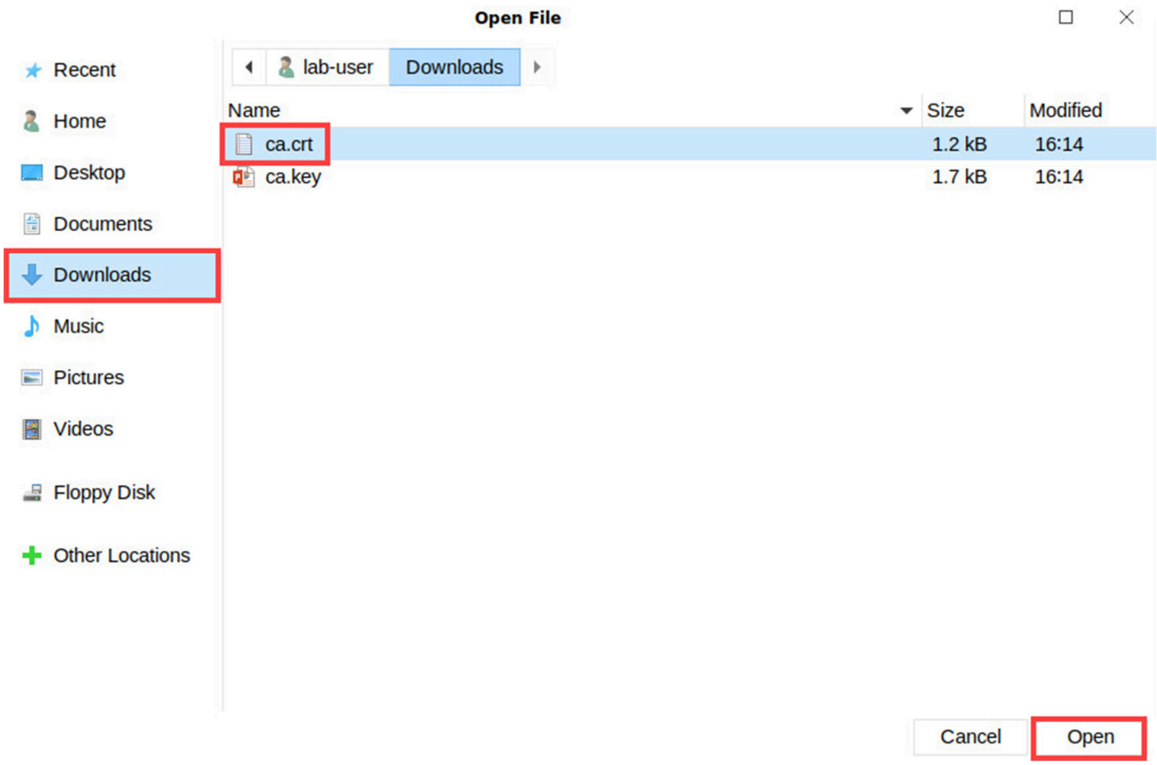
□ Block Private Key Export

Key File:

Passphrase:

Confirm Passphrase:

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

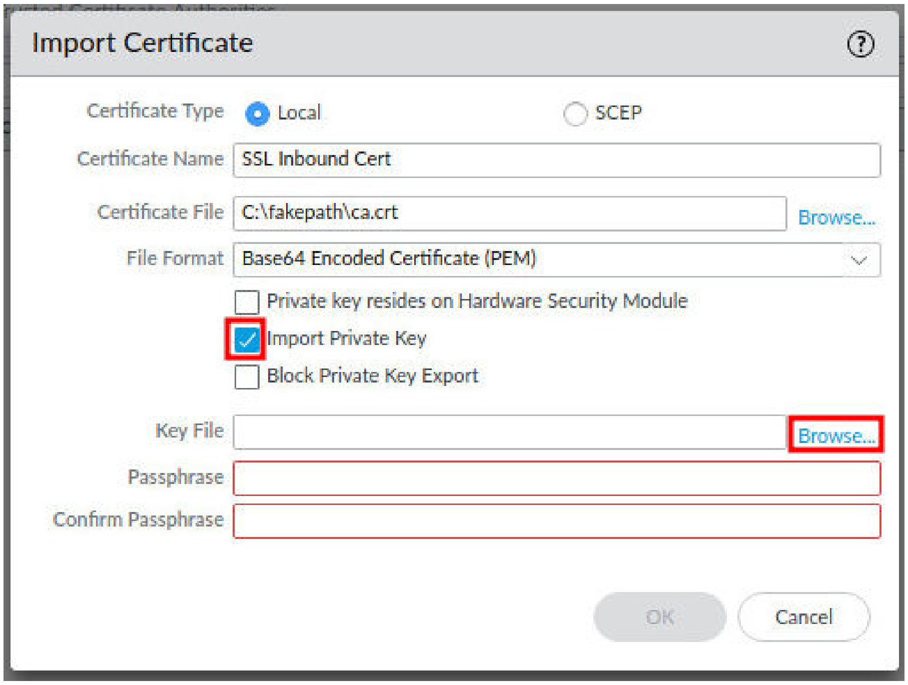


Open File

lab-user > Downloads

| Name | Size | Modified |
|---|---|---|
| ca.crt | 1.2 kB | 16:14 |
| ca.key | 1.7 kB | 16:14 |

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



Import Certificate

Certificate Type ● Local ○ SCEP

Certificate Name: SSL Inbound Cert

Certificate File: C:\fakepath\ca.crt

File Format: Base64 Encoded Certificate (PEM)

□ Private key resides on Hardware Security Module

☑ Import Private Key

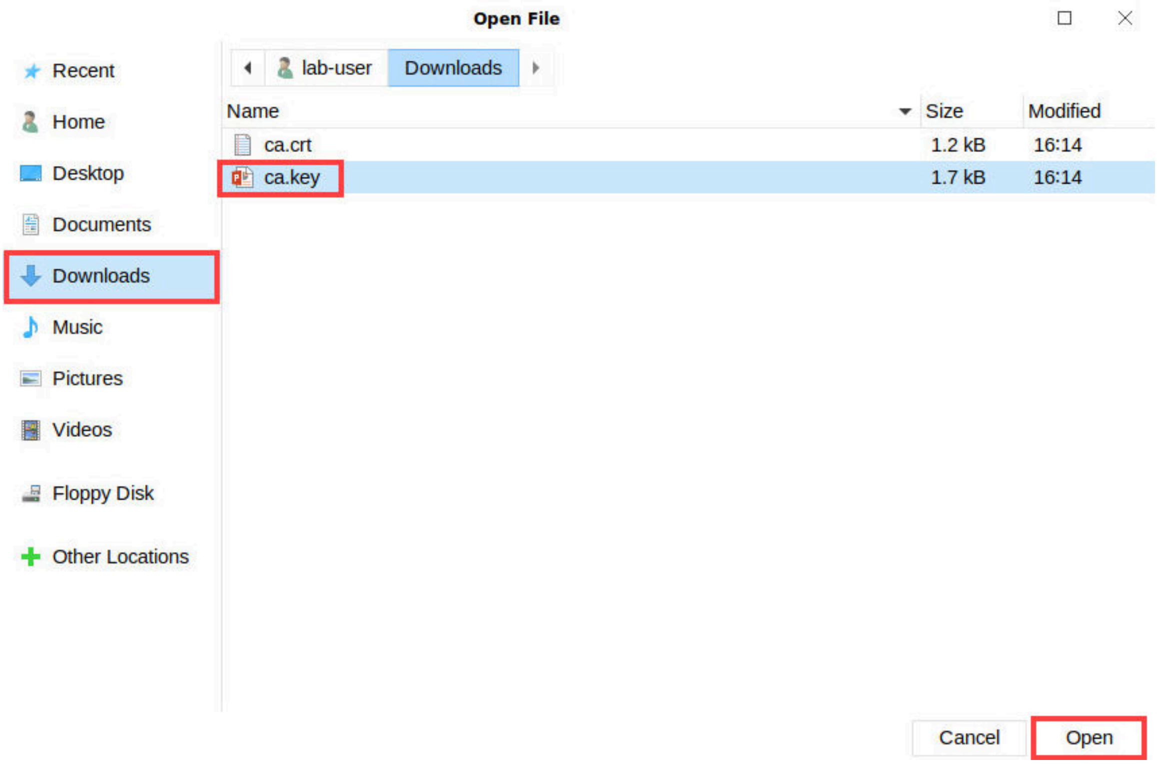
□ Block Private Key Export

Key File:

Passphrase:

Confirm Passphrase:

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

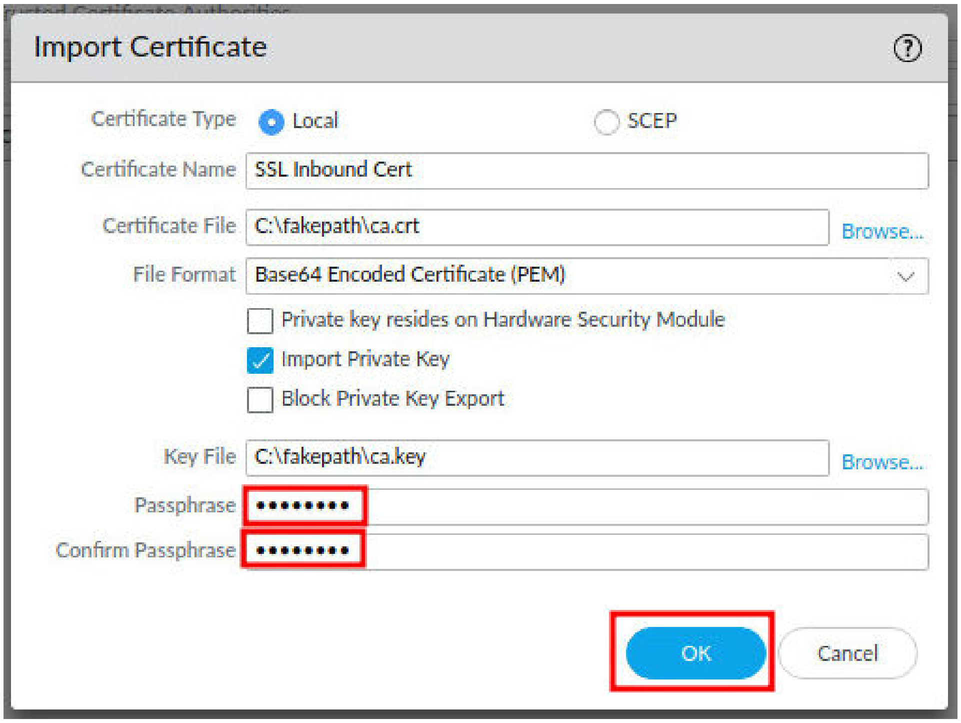


Open File

lab-user > Downloads

| Name | Size | Modified |
|---|---|---|
| ca.crt | 1.2 kB | 16:14 |
| ca.key | 1.7 kB | 16:14 |

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



Import Certificate

Certificate Type ● Local ○ SCEP

Certificate Name: SSL Inbound Cert

Certificate File: C:\fakepath\ca.crt

File Format: Base64 Encoded Certificate (PEM)

□ Private key resides on Hardware Security Module

☑ Import Private Key

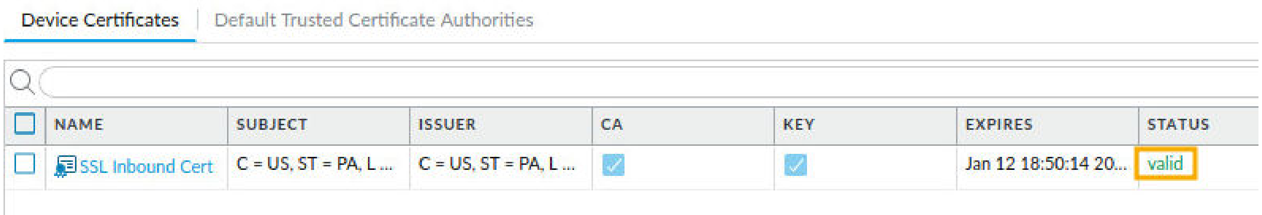
□ Block Private Key Export

Key File: C:\fakepath\ca.key

Passphrase: ••••••••

Confirm Passphrase: ••••••••

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

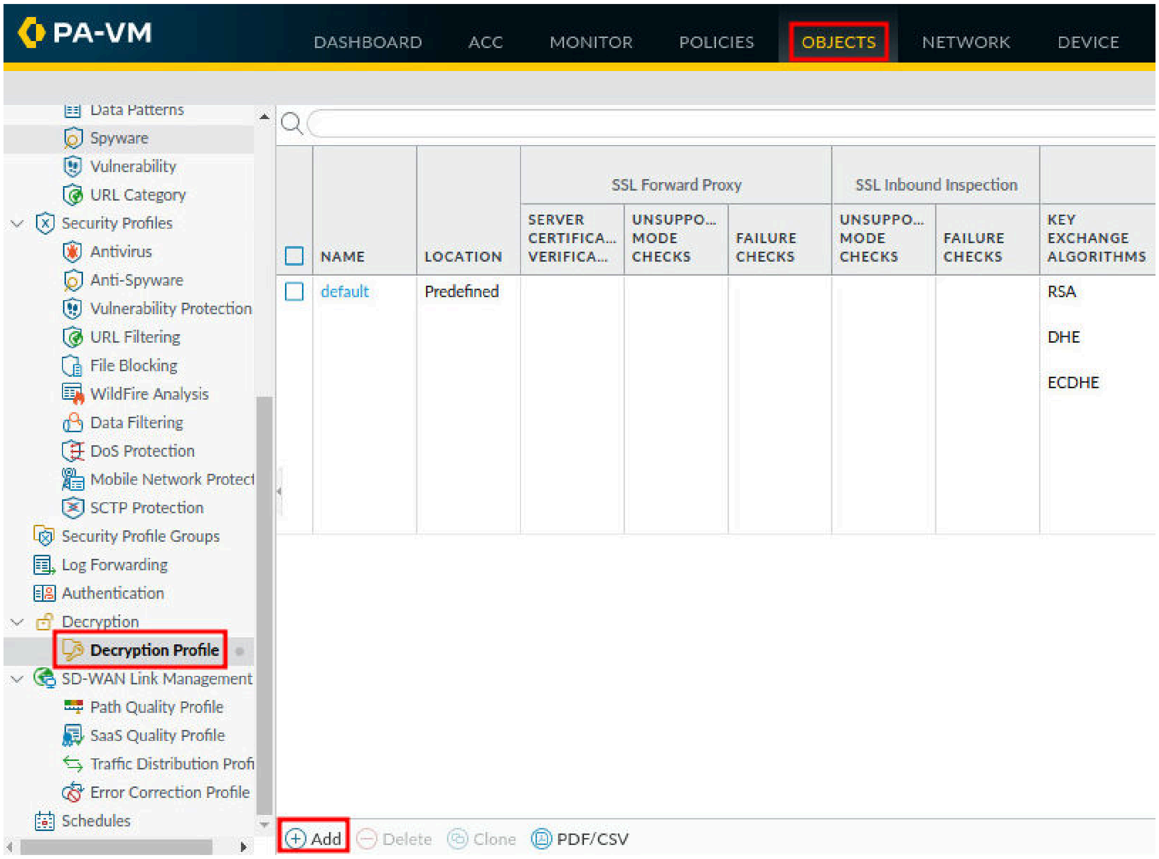


| □ | NAME | SUBJECT | ISSUER | CA | KEY | EXPIRES | STATUS |
|---|---|---|---|---|---|---|---|
| □ | SSL Inbound Cert | C = US, ST = PA, L ... | C = US, ST = PA, L ... | ☑ | ☑ | Jan 12 18:50:14 20... | valid |

## 1.3 Create a Decryption Profile

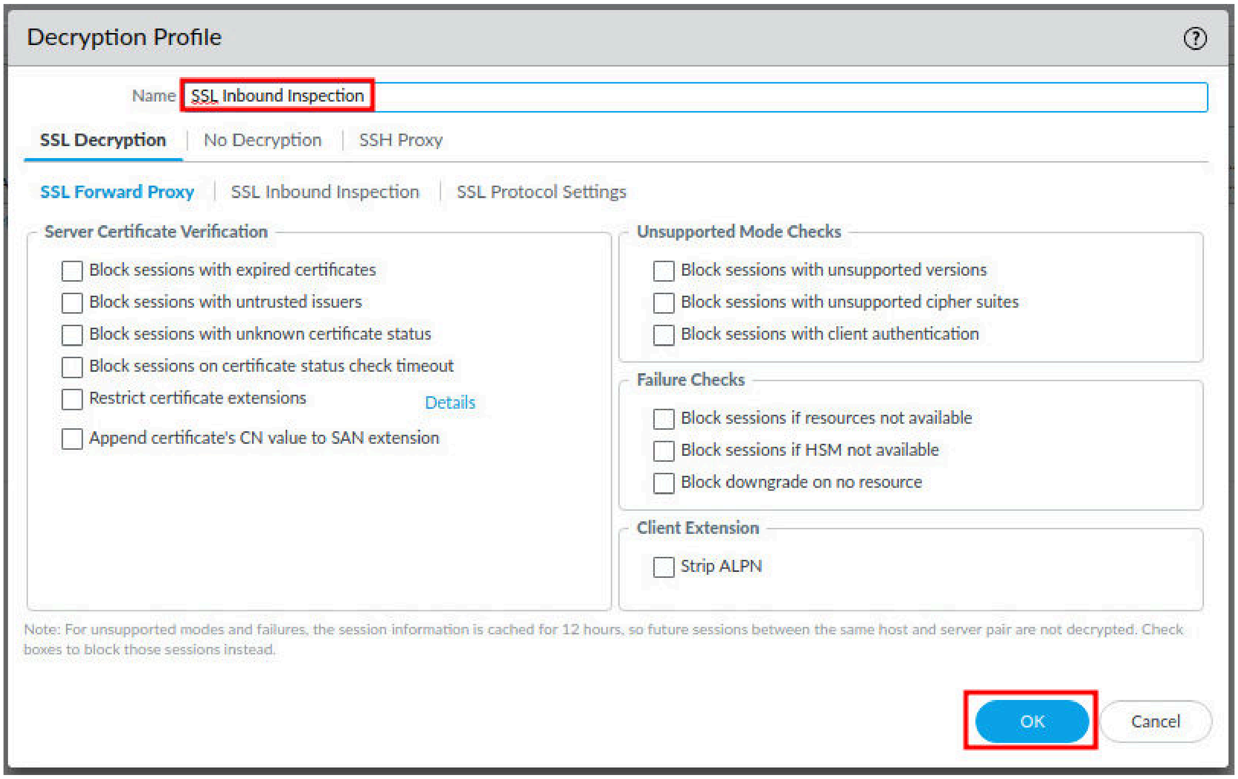
In this section, you will create a decryption profile. Decryption profiles allow administrators to perform checks on both decrypted traffic and traffic that would have been excluded from decryption. After a decryption profile is created, it can then be attached to a decryption policy rule that will enforce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

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



| | | | SSL Forward Proxy | | | SSL Inbound Inspection | | |
|---|---|---|---|---|---|---|---|---|
| □ | NAME | LOCATION | SERVER CERTIFICA... VERIFICA... | UNSUPPO... MODE CHECKS | FAILURE CHECKS | UNSUPPO... MODE CHECKS | FAILURE CHECKS | KEY EXCHANGE ALGORITHMS |
| □ | default | Predefined | | | | | | RSA<br>DHE<br>ECDHE |

2. 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

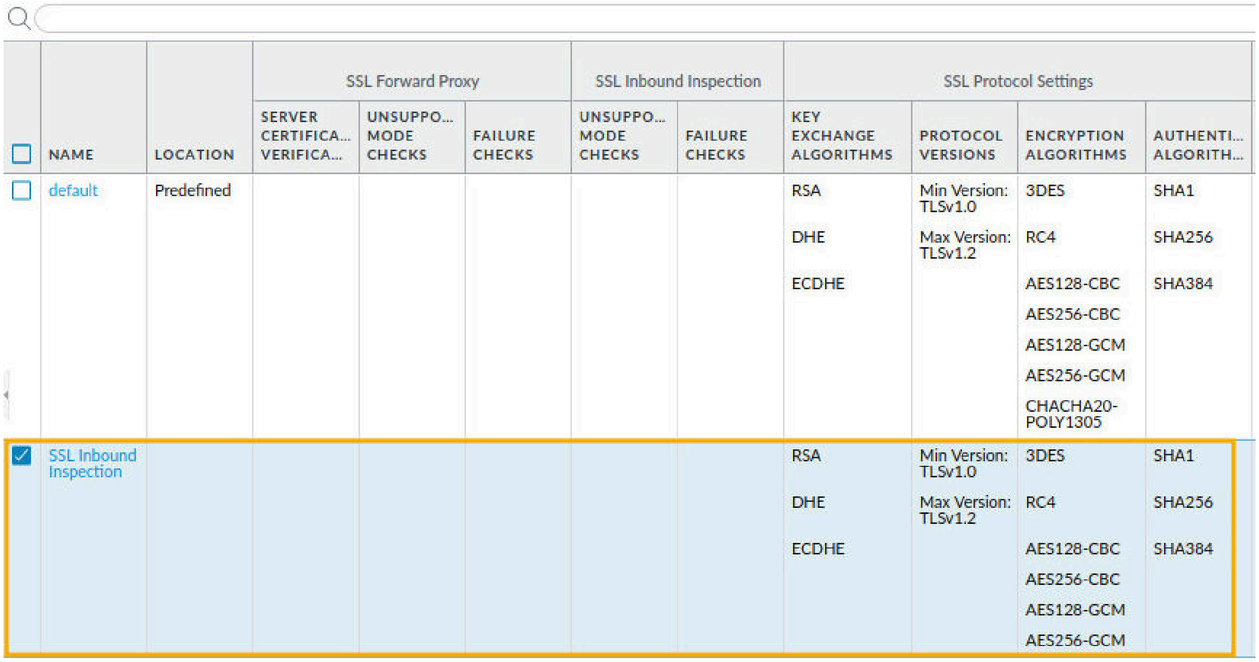
- □ Block sessions if resources not available
- □ Block sessions if HSM not available
- □ Block downgrade on no resource

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.

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

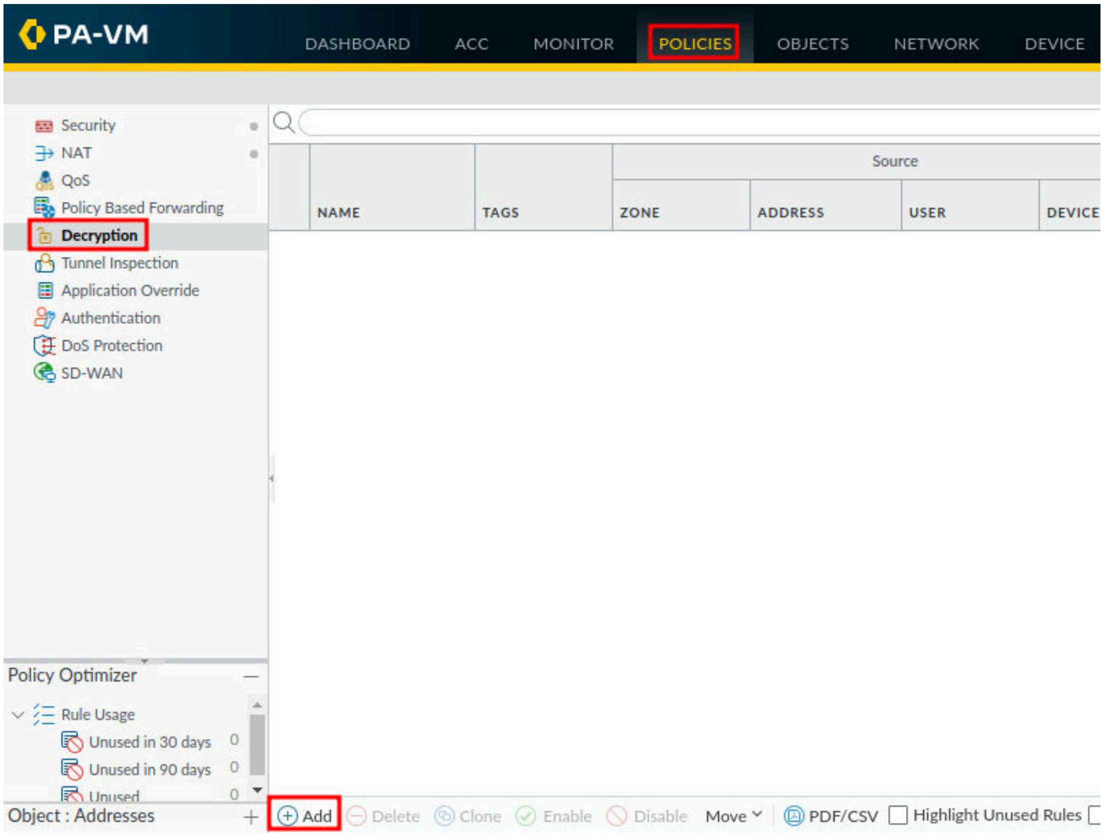


| | | | SSL Forward Proxy | | | SSL Inbound Inspection | | SSL Protocol Settings | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| □ | NAME | LOCATION | SERVER CERTIFICA... VERIFICA... | UNSUPPO... MODE CHECKS | FAILURE CHECKS | UNSUPPO... MODE CHECKS | FAILURE CHECKS | KEY EXCHANGE ALGORITHMS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

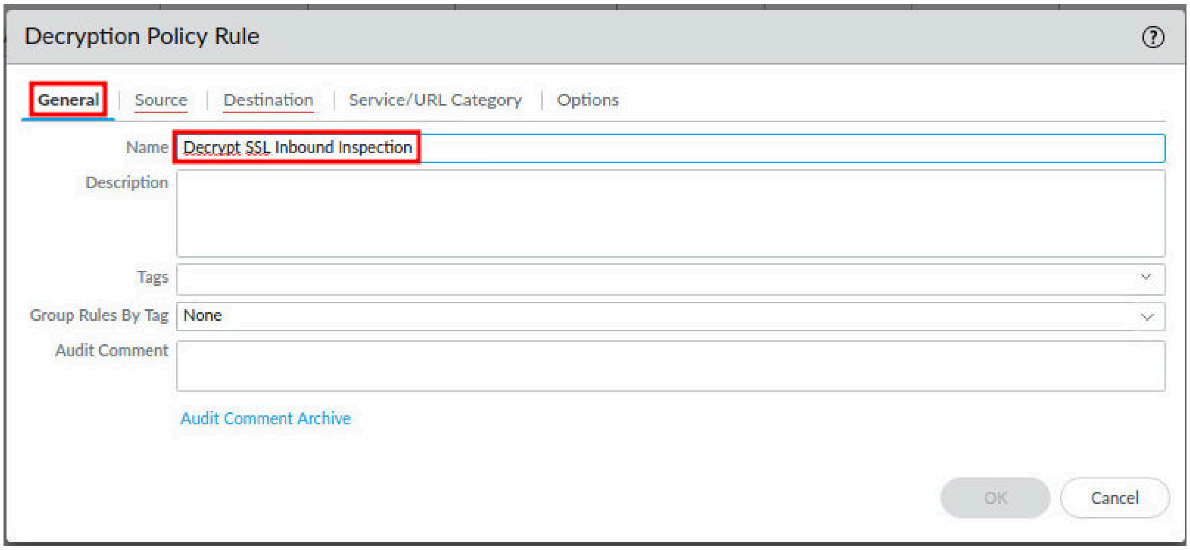
## 1.4 Create a Decryption Policy

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.**

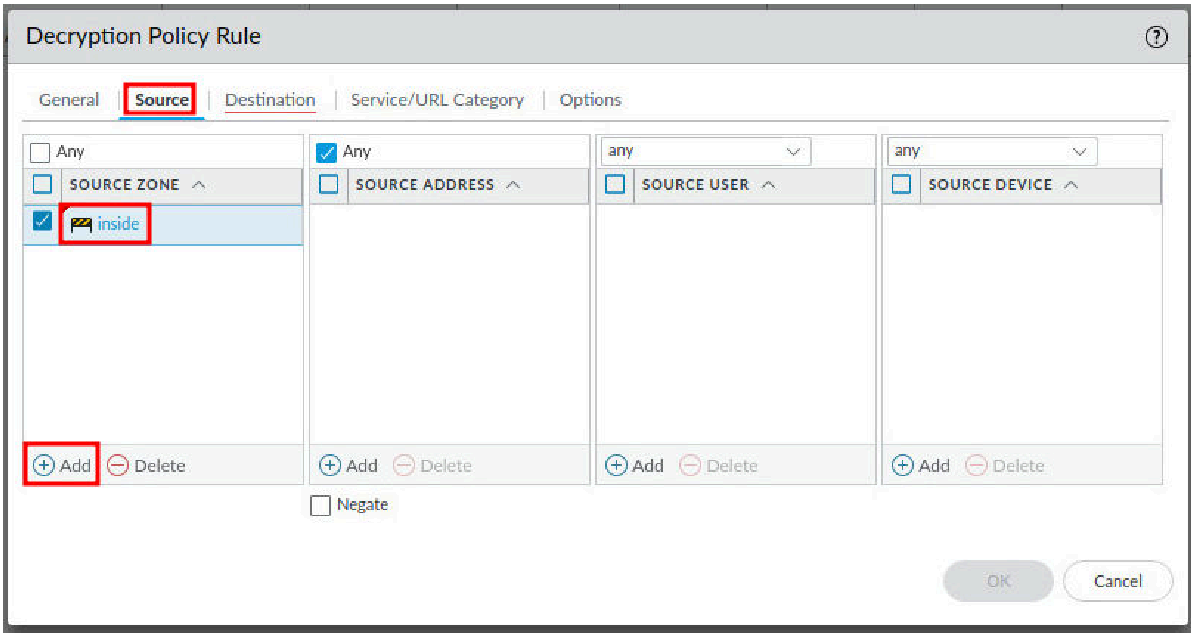


2. In the **General** tab of the *Decryption Policy Rule* window, type `Decrypt SSL Inbound Inspection` in the *Name* field.

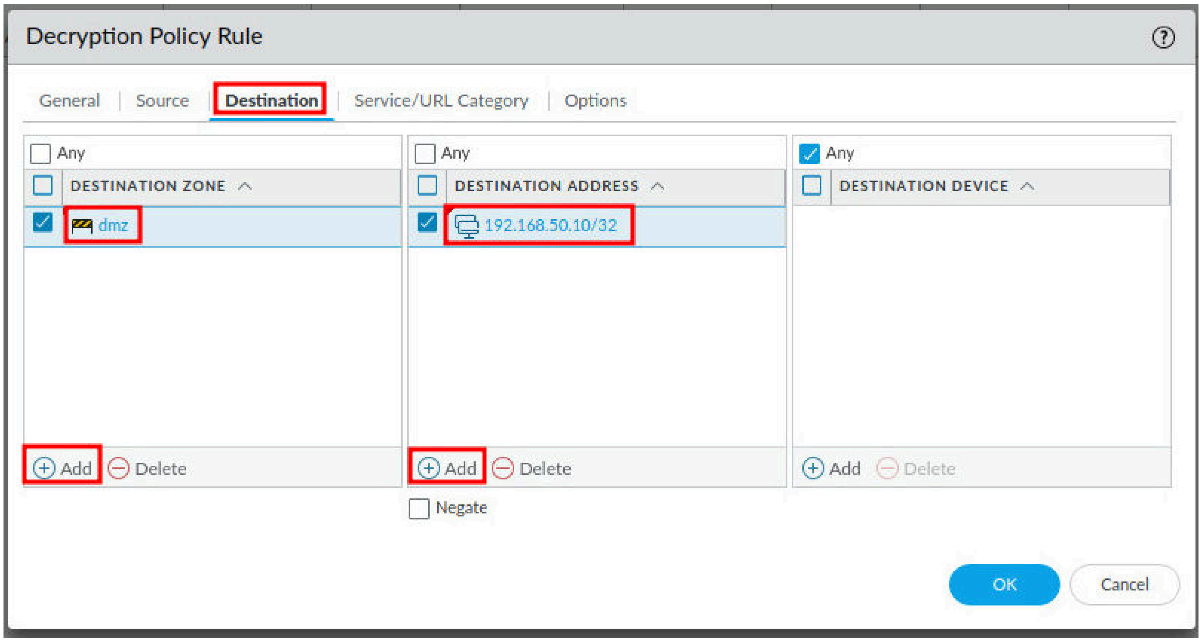


Name: Decrypt SSL Inbound Inspection
Group Rules By Tag: None

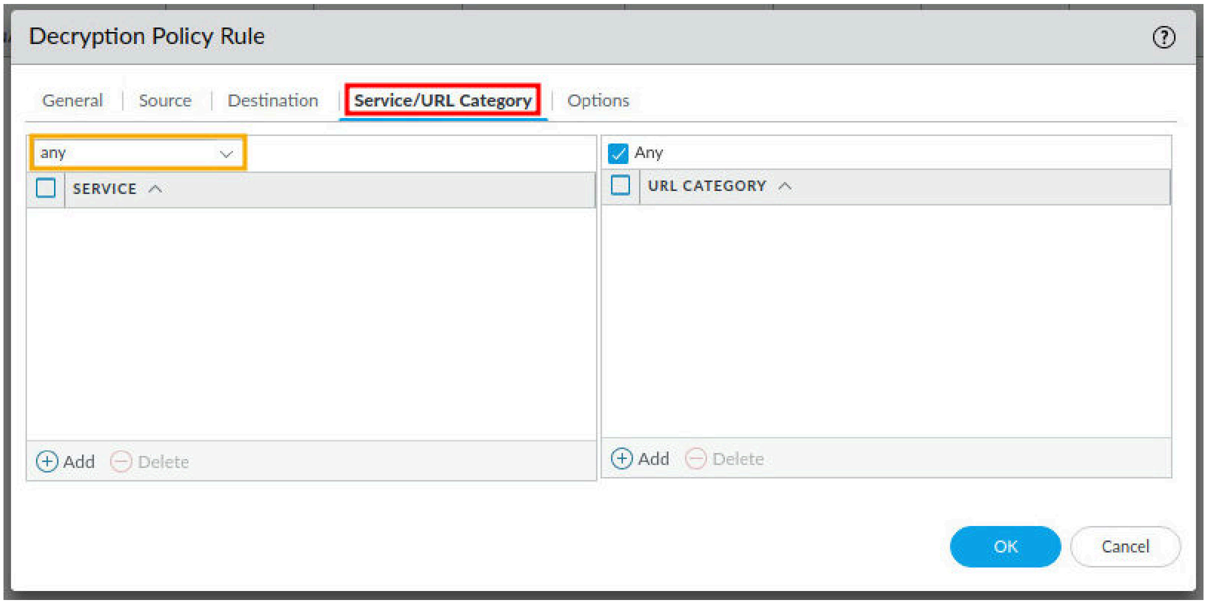
3. In the *Decryption Policy Rule* window, click on the **Source** tab. Then, click **Add** in the *Source Zone* section. Next, select **inside**.



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.



Decryption Policy Rule

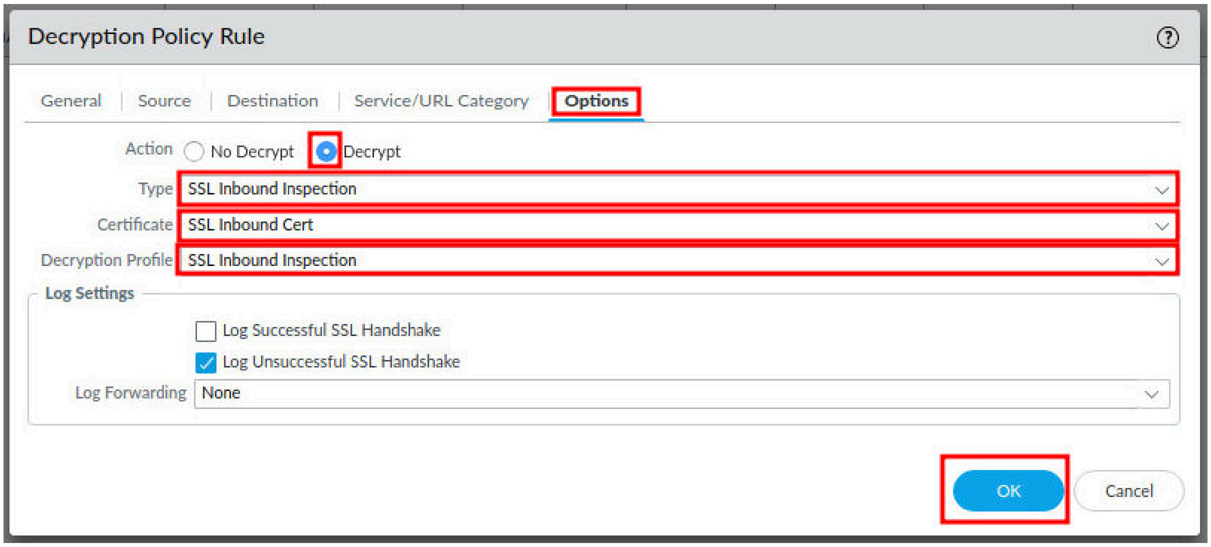
any

□ SERVICE

☑ Any

□ URL CATEGORY

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.



Decryption Policy Rule

Action ○ No Decrypt ● Decrypt

Type: SSL Inbound Inspection

Certificate: SSL Inbound Cert

Decryption Profile: SSL Inbound Inspection

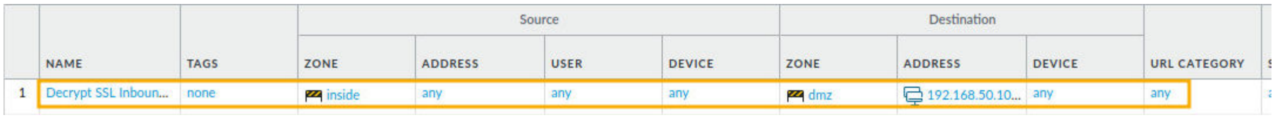
Log Settings

□ Log Successful SSL Handshake

☑ Log Unsuccessful SSL Handshake

Log Forwarding: None

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

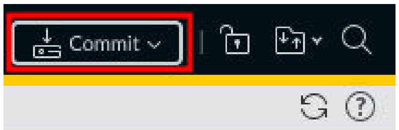


| | | | Source | | | | Destination | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | NAME | TAGS | ZONE | ADDRESS | USER | DEVICE | ZONE | ADDRESS | DEVICE | URL CATEGORY |
| 1 | Decrypt SSL Inboun... | none | inside | any | any | any | dmz | 192.168.50.10... | any | any |

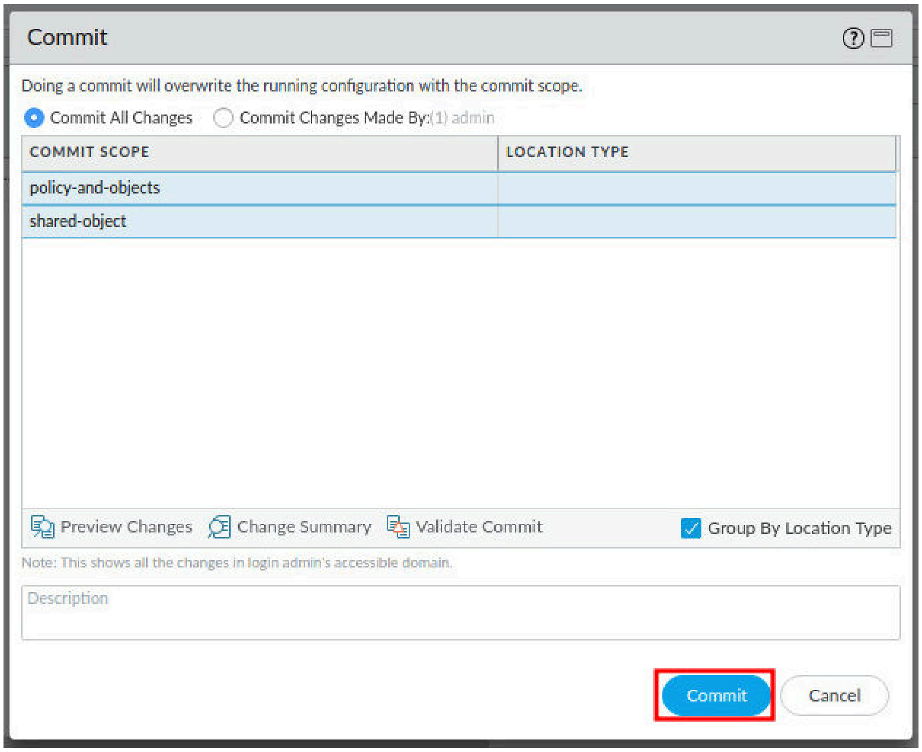
## 1.5 Commit and Test Decryption Policy

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.



Commit

Doing a commit will overwrite the running configuration with the commit scope.

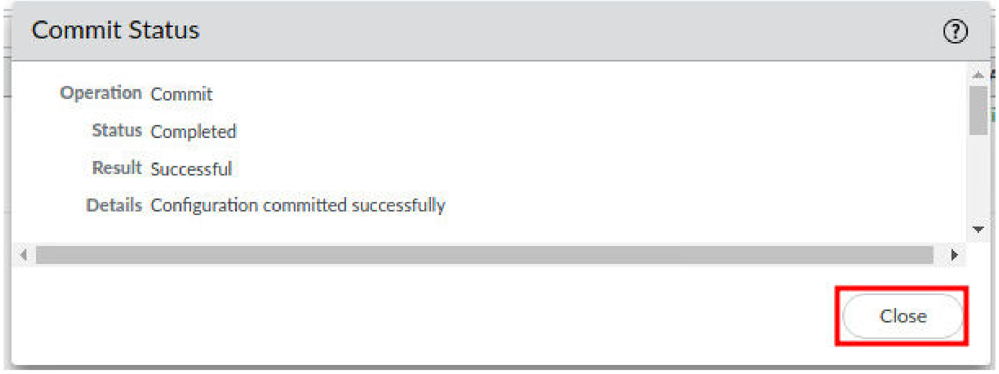
● Commit All Changes ○ Commit Changes Made By:(1) admin

| COMMIT SCOPE | LOCATION TYPE |
|---|---|
| policy-and-objects | |
| shared-object | |

☑ Group By Location Type

Note: This shows all the changes in login admin's accessible domain.

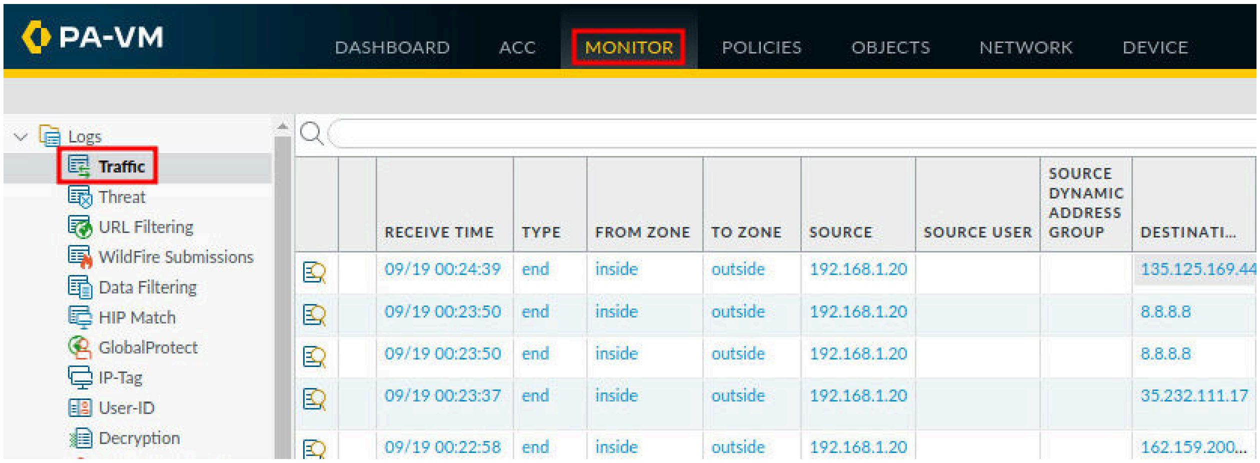
3. When the commit operation successfully completes, click **Close** to continue.



Commit Status

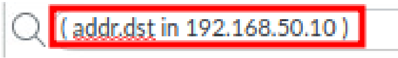
Operation Commit
Status Completed
Result Successful
Details Configuration committed successfully

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



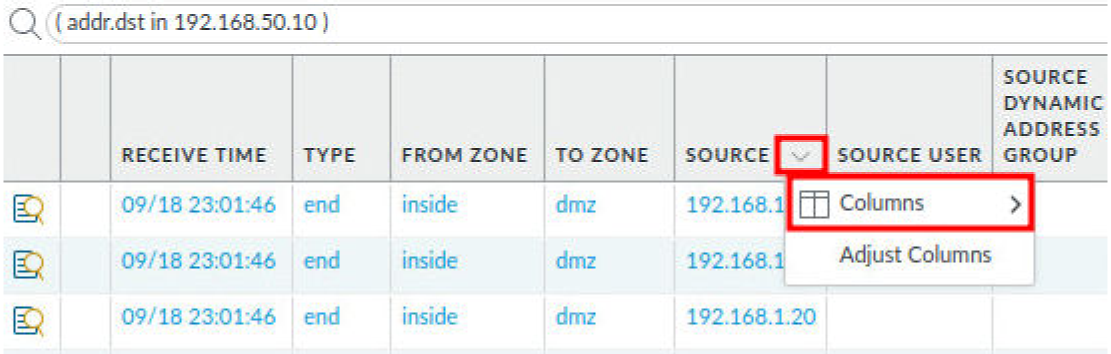
| RECEIVE TIME | TYPE | FROM ZONE | TO ZONE | SOURCE | SOURCE USER | SOURCE DYNAMIC ADDRESS GROUP | DESTINATI... |
|---|---|---|---|---|---|---|---|
| 09/19 00:24:39 | end | inside | outside | 192.168.1.20 | | | 135.125.169.44 |
| 09/19 00:23:50 | end | inside | outside | 192.168.1.20 | | | 8.8.8.8 |
| 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.**



( addr.dst in 192.168.50.10 )

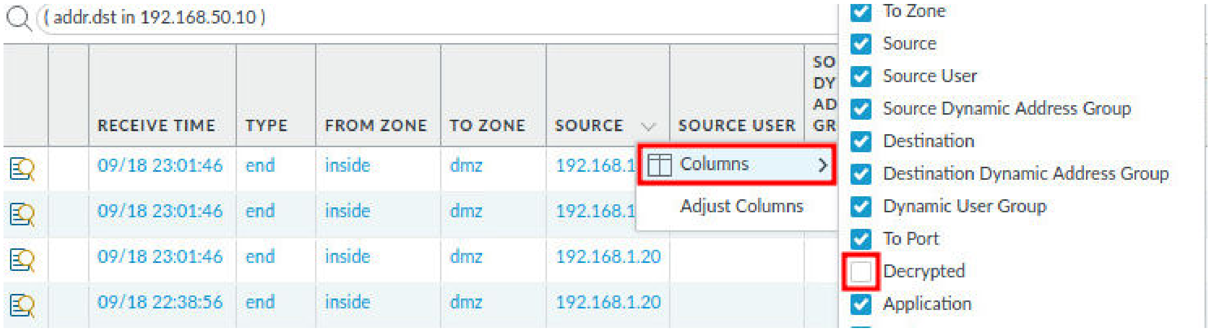
6. Move the mouse cursor to the right of *Source* and click the **down arrow** to bring up the **Columns** menu.



( addr.dst in 192.168.50.10 )

| 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 | | |
| 09/18 23:01:46 | end | inside | dmz | 192.168.1 | | |
| 09/18 23:01:46 | end | inside | dmz | 192.168.1.20 | | |

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



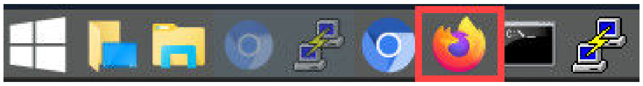
( addr.dst in 192.168.50.10 )

| RECEIVE TIME | TYPE | FROM ZONE | TO ZONE | SOURCE | SOURCE USER | SO DY AD GR |
|---|---|---|---|---|---|---|
| 09/18 23:01:46 | end | inside | dmz | 192.168.1 | | |
| 09/18 23:01:46 | end | inside | dmz | 192.168.1 | | |
| 09/18 23:01:46 | end | inside | dmz | 192.168.1.20 | | |
| 09/18 22:38:56 | end | inside | dmz | 192.168.1.20 | | |

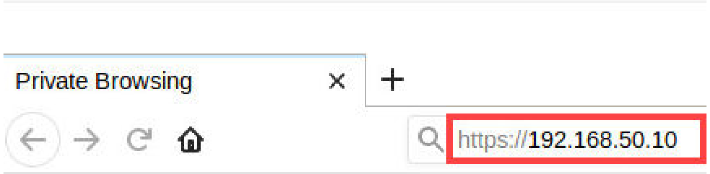
- ☑ To Zone
- ☑ Source
- ☑ Source User
- ☑ Source Dynamic Address Group
- ☑ Destination
- ☑ Destination Dynamic Address Group
- ☑ Dynamic User Group
- ☑ To Port
- ☐ Decrypted
- ☑ Application

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.

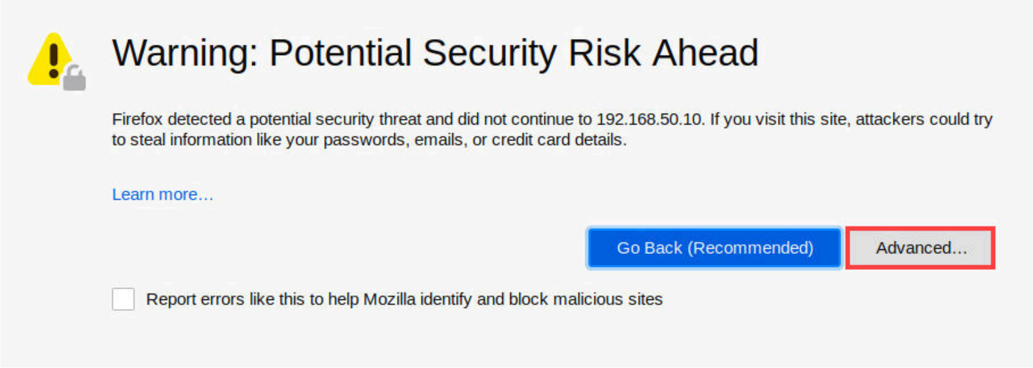


9. In the address bar, type `https://192.168.50.10` and click **Enter**.



https://192.168.50.10

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



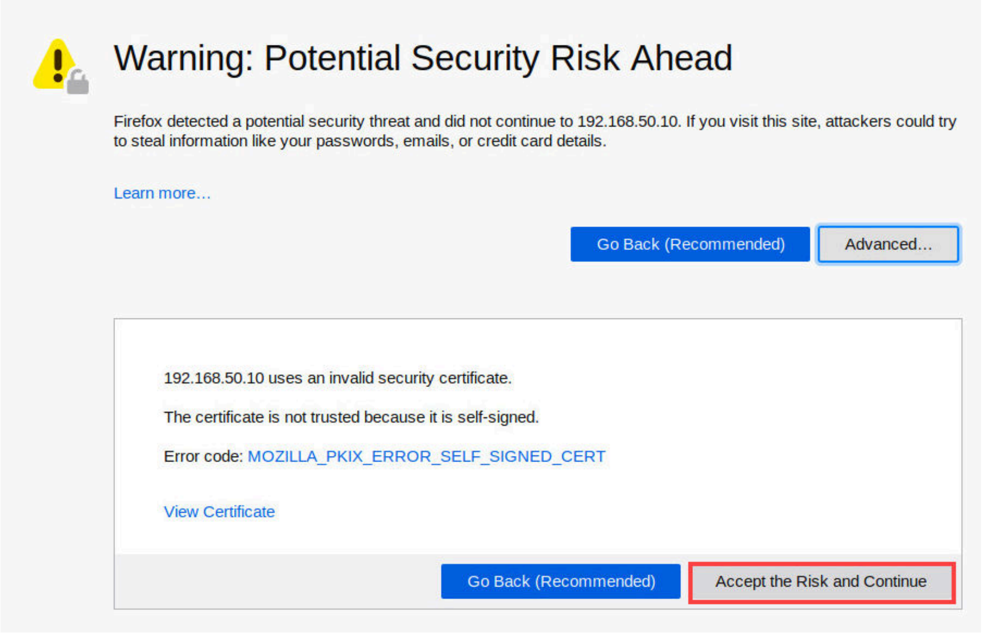
Warning: Potential Security Risk Ahead

Firefox detected a potential security threat and did not continue to 192.168.50.10. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

Learn more…

□ Report errors like this to help Mozilla identify and block malicious sites

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



Warning: Potential Security Risk Ahead

Firefox detected a potential security threat and did not continue to 192.168.50.10. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

Learn more…

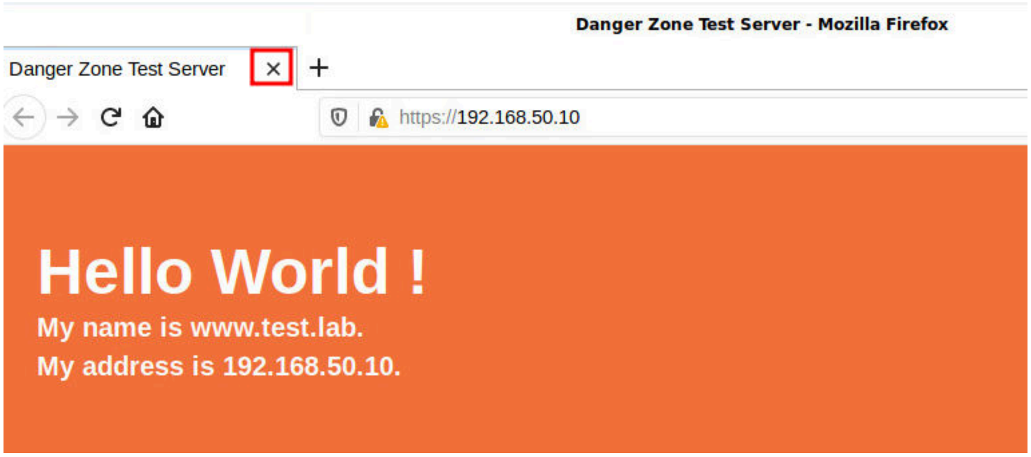
192.168.50.10 uses an invalid security certificate.

The certificate is not trusted because it is self-signed.

Error code: MOZILLA_PKIX_ERROR_SELF_SIGNED_CERT

View Certificate

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



Danger Zone Test Server - Mozilla Firefox

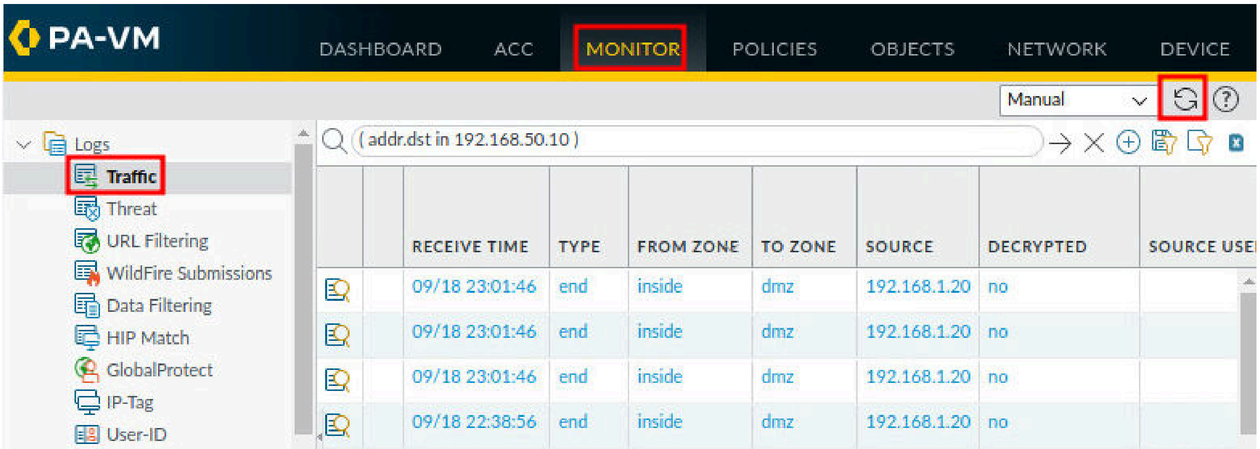
https://192.168.50.10

Hello World !

My name is www.test.lab.

My address is 192.168.50.10.

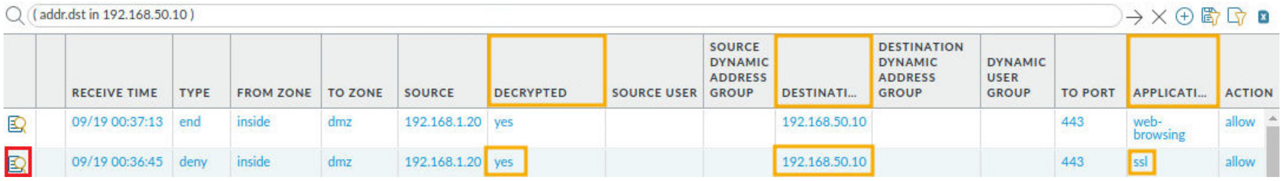
13. Navigate to **Monitor > Logs > Traffic**. Then, click the **refresh** icon.



( addr.dst in 192.168.50.10 )

| | | RECEIVE TIME | TYPE | FROM ZONE | TO ZONE | SOURCE | DECRYPTED | SOURCE USEI |
|---|---|---|---|---|---|---|---|---|
| | | 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 | |

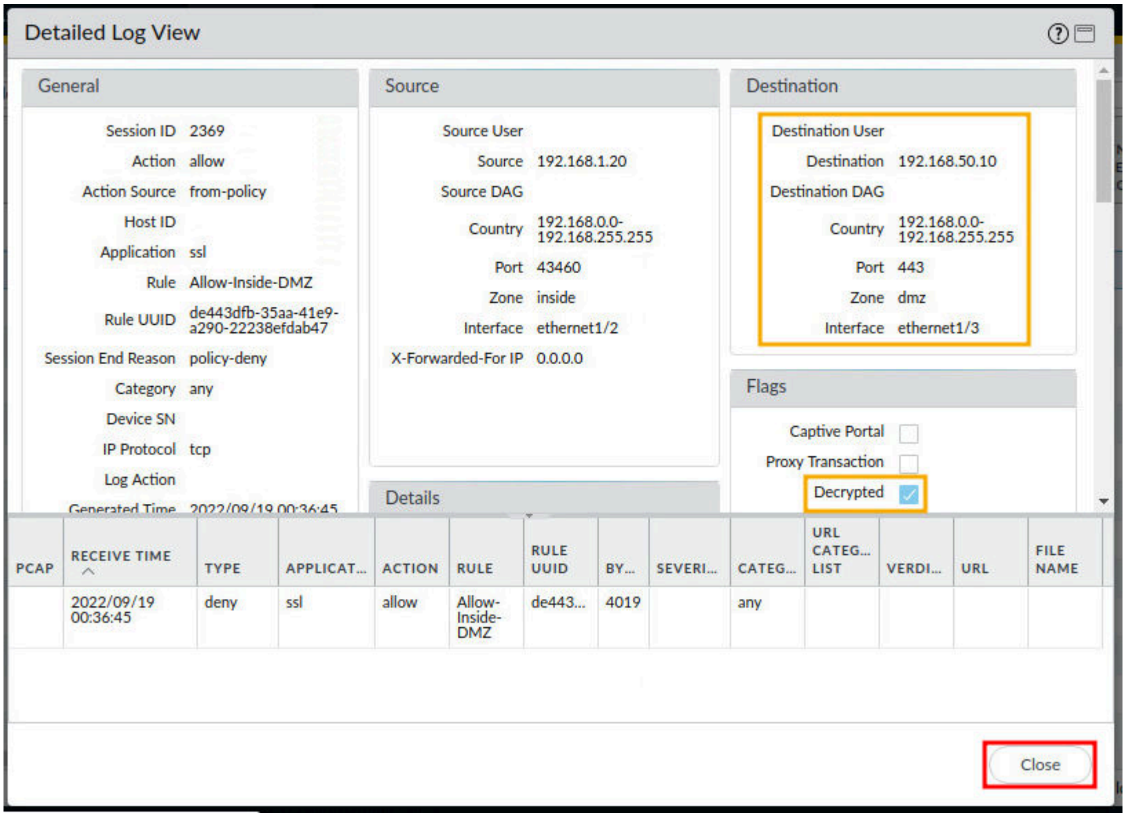
14. Look for traffic associated with the application of **ssl** and the *Decrypted* column set to **yes**. Click the magnifying glass on the left to open the **Detailed Log View** of the traffic to analyze the traffic from the Client machine of **192.168.1.20** to the DMZ server of **192.168.50.10.**



( 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

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

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

Details

Destination

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

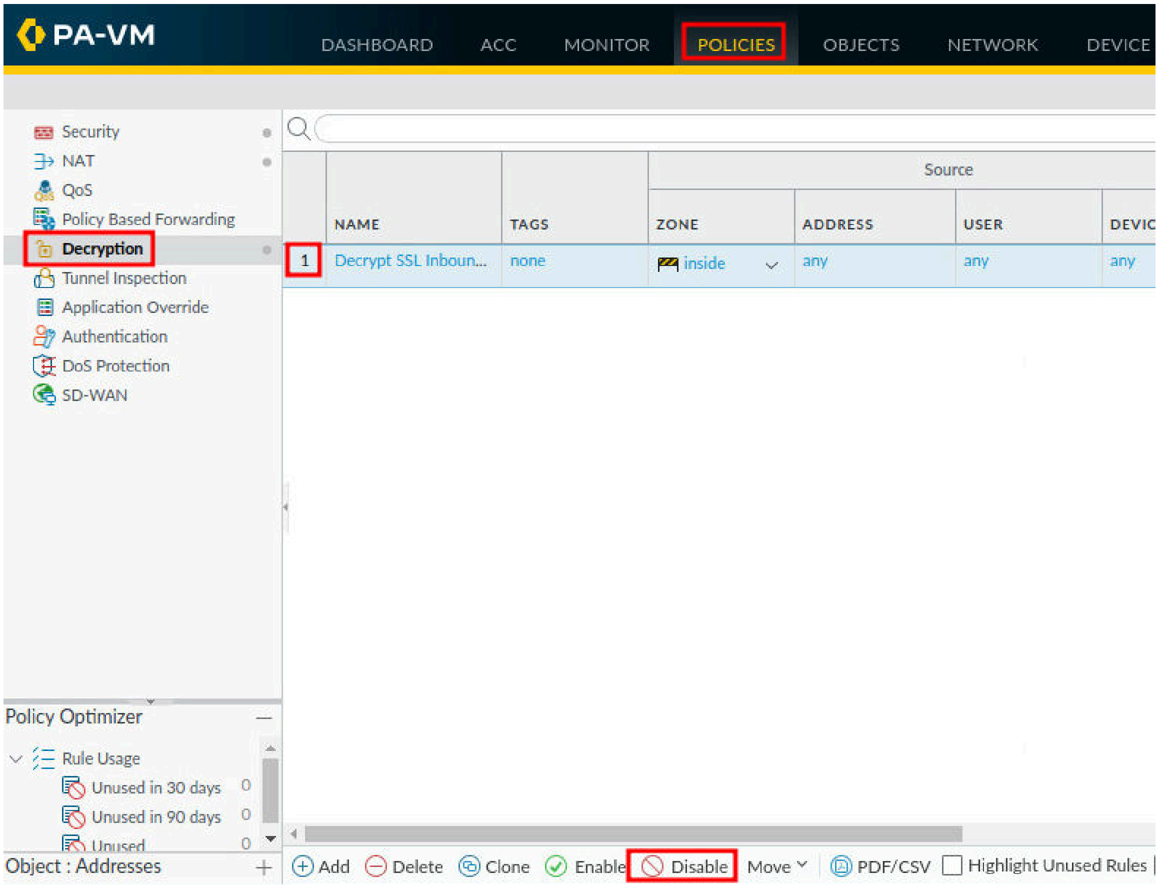
Captive Portal □
Proxy Transaction □
Decrypted ☑

| 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 | | | | |

## 1.6 Disable Decryption Policy

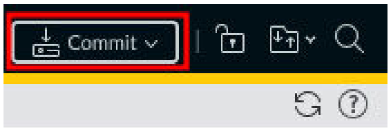
In this section, you will disable the decryption policy you created earlier. Then, after committing the changes to the Firewall, you will monitor traffic logs to determine if traffic is still being decrypted.

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

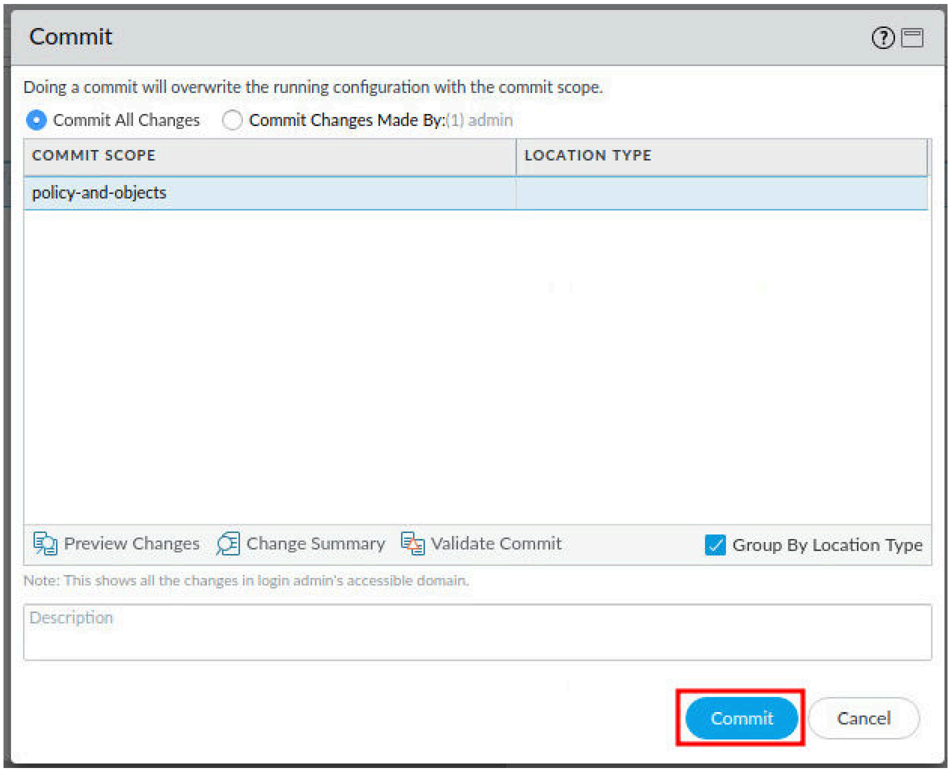


|  |  |  | Source |  |  |  |
|---|---|---|---|---|---|---|
|  | NAME | TAGS | ZONE | ADDRESS | USER | DEVIC |
| 1 | Decrypt SSL Inboun... | none | inside | any | any | any |

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.



Commit

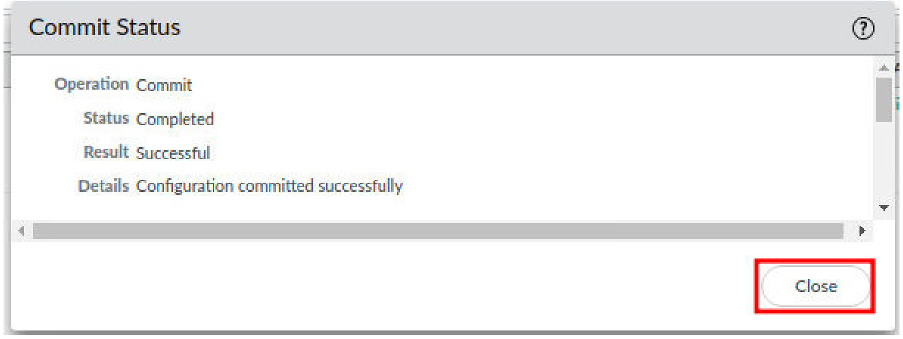
Doing a commit will overwrite the running configuration with the commit scope.

● Commit All Changes ○ Commit Changes Made By:(1) admin

| COMMIT SCOPE | LOCATION TYPE |
|---|---|
| policy-and-objects | |

Note: This shows all the changes in login admin's accessible domain.

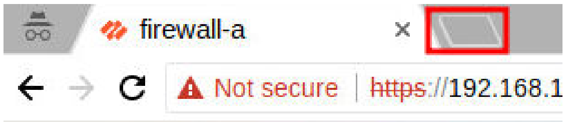
4. When the commit operation successfully completes, click **Close** to continue.



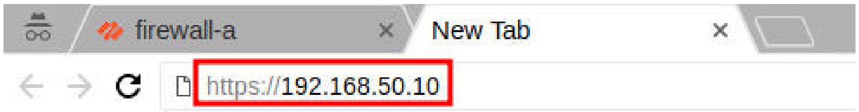
Commit Status

Operation Commit
Status Completed
Result Successful
Details Configuration committed successfully

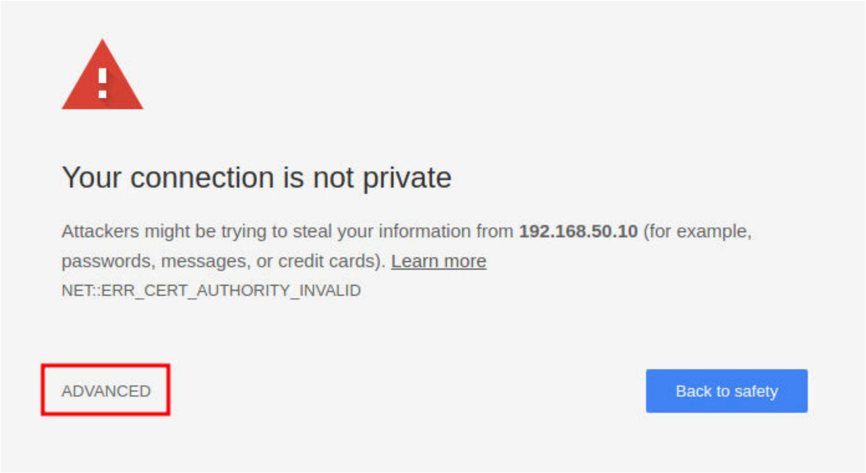
5. Click the **New tab** button in *Chromium*.



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.

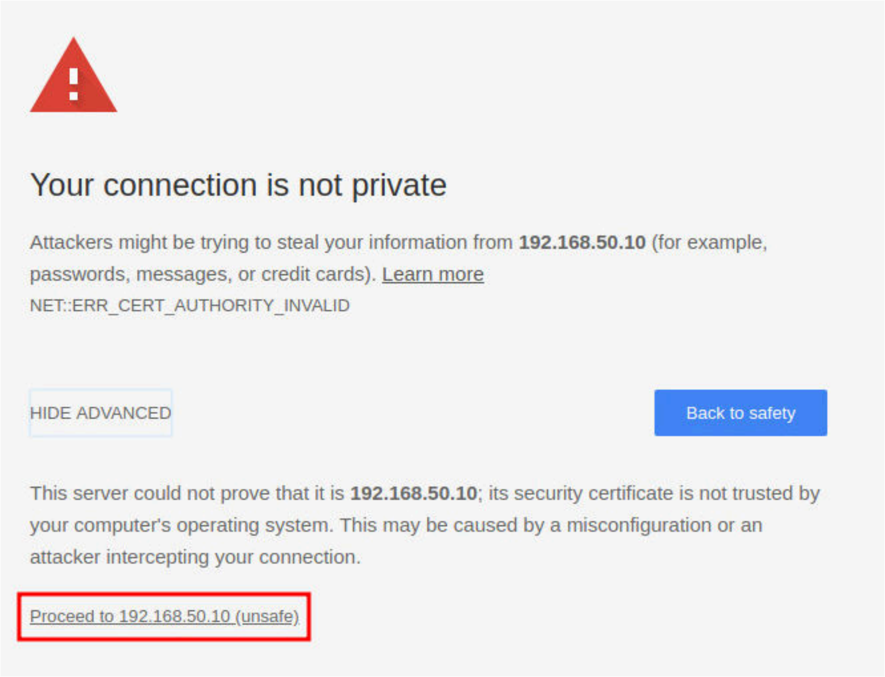


Your connection is not private

Attackers might be trying to steal your information from **192.168.50.10** (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_AUTHORITY_INVALID

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



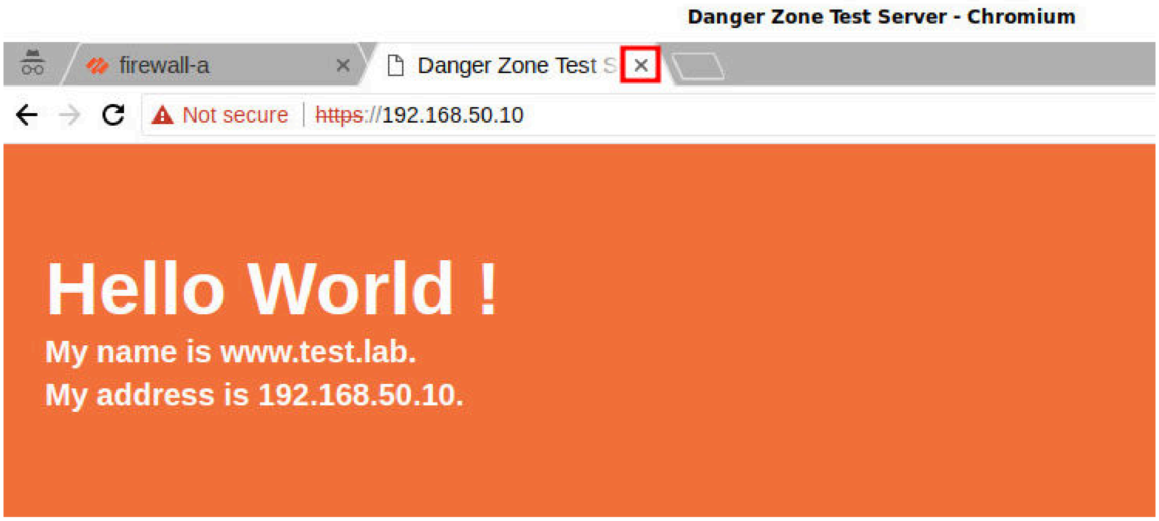
Your connection is not private

Attackers might be trying to steal your information from **192.168.50.10** (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_AUTHORITY_INVALID

This server could not prove that it is **192.168.50.10**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

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



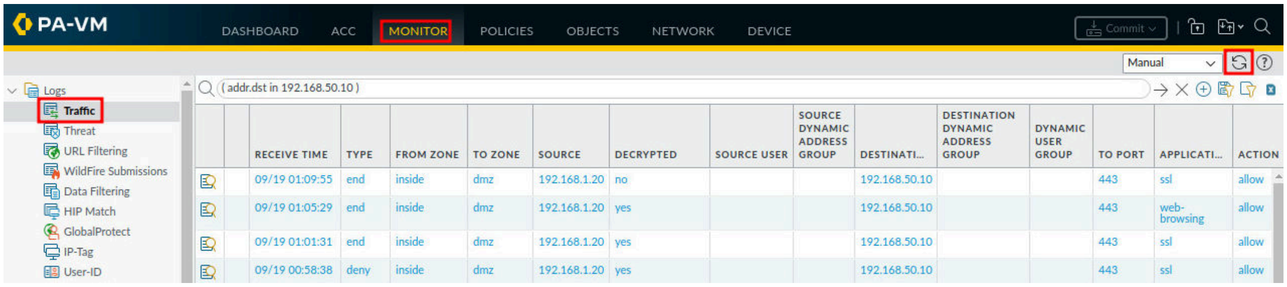
https://192.168.50.10

Hello World !

My name is www.test.lab.

My address is 192.168.50.10.

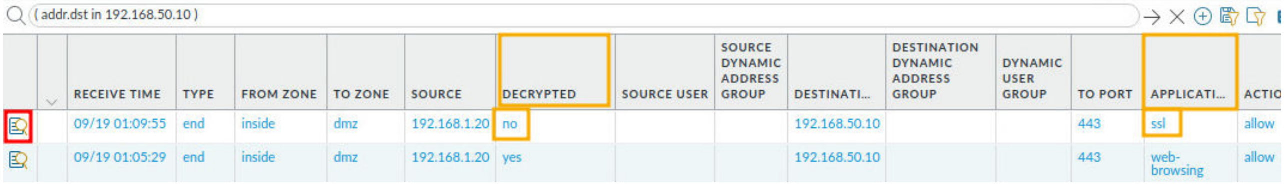
10. Navigate to **Monitor > Logs > Traffic**. Then, click the **refresh** icon.



( 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 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 |

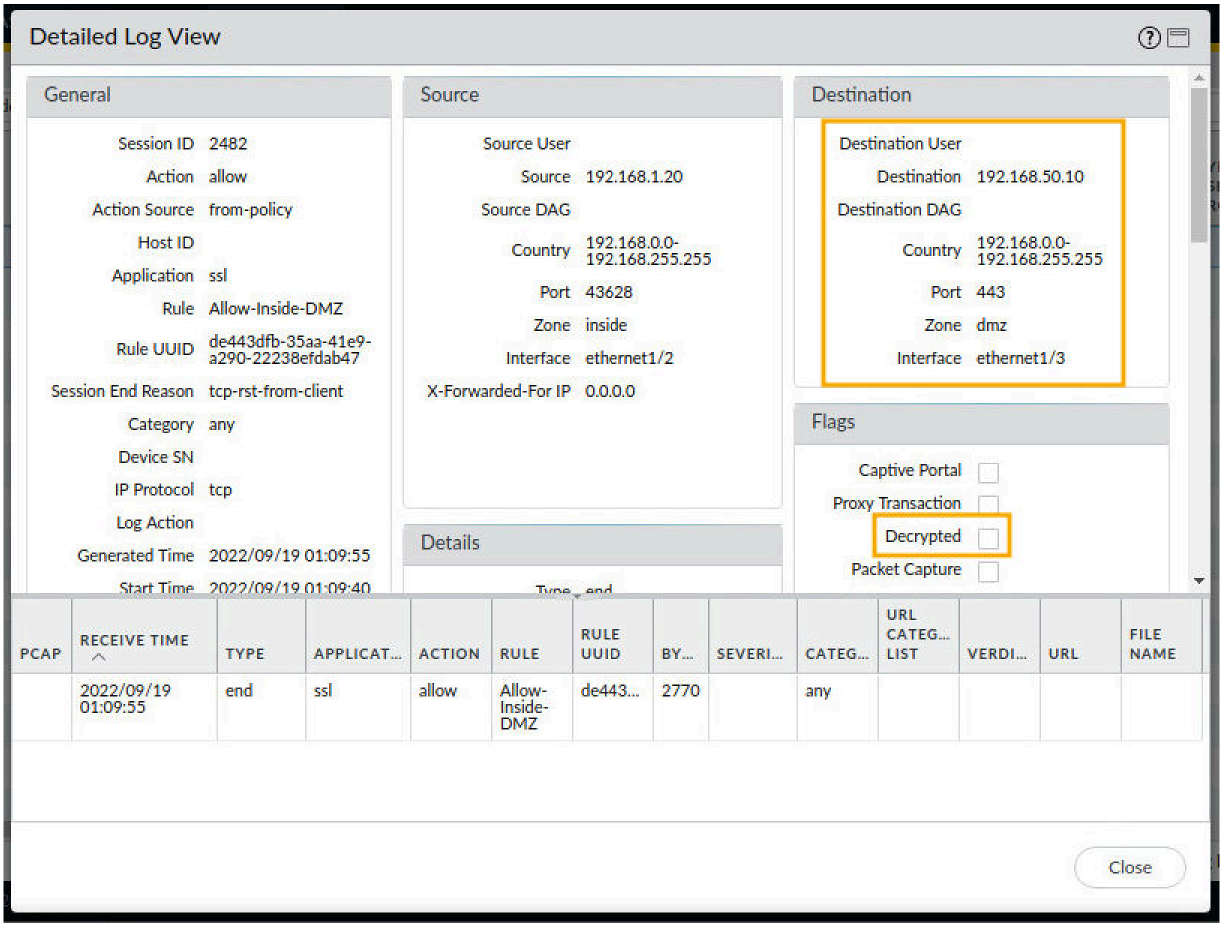
11. Look for traffic associated with the application of **ssl** and the *Decrypted* column set to **no**. Click on the magnifying glass icon on the left to open the **Detailed Log View** of the traffic to analyze the traffic from the Client machine of **192.168.1.20** to the DMZ server of **192.168.50.10.**



( 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... | ACTIO |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 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

| | |
|---|---|
| Session ID | 2482 |
| Action | allow |
| Action Source | from-policy |
| Host ID | |
| Application | ssl |
| Rule | Allow-Inside-DMZ |
| Rule UUID | de443dfb-35aa-41e9-a290-22238efdab47 |
| 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 | |
| Source | 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 |

Details

| | |
|---|---|
| Type | end |

Destination

| | |
|---|---|
| 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 | ☐ |
| 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 | | | | |

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