PALO ALTO NETWORKS FIREWALL 11.0 ESSENTIALS

Lab 12: Using Decryption to Block Threats in Encrypted Traffic

Document Version: 2025-10-13

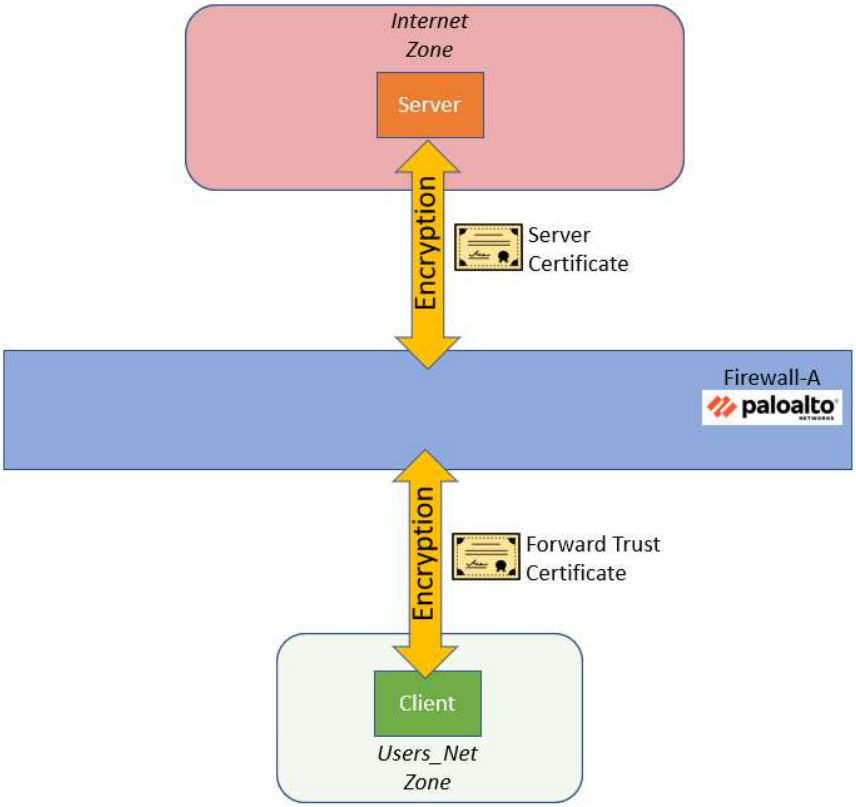
Contents

Introduction

As an astute network security professional, you have noticed the dramatic increase of HTTPS secure traffic over the past few years. Correspondingly, you have noticed that very few websites even use unencrypted HTTP traffic anymore. Virtually all network traffic is now encrypted.

You know that HTTPS protects privacy and sensitive data in transit between hosts, but you have begun to realize that HTTPS also hides potentially damaging data as well. Encrypted traffic into and out of your network might contain viruses, spyware, vulnerability exploits and other damaging types of data.

You need to make certain that the Palo Alto Networks firewall can inspect even encrypted traffic, so you have decided to implement decryption. This process will allow the firewall to decrypt HTTPS traffic, inspect it and then block any sessions that contain malicious content.



Right now, you do not have budget funds available to build a corporate PKI infrastructure to generate a decryption certificate from a CA (certificate authority). However, you can generate a self-signed CA certificate on the Palo Alto Networks firewall and deploy that for decryption.

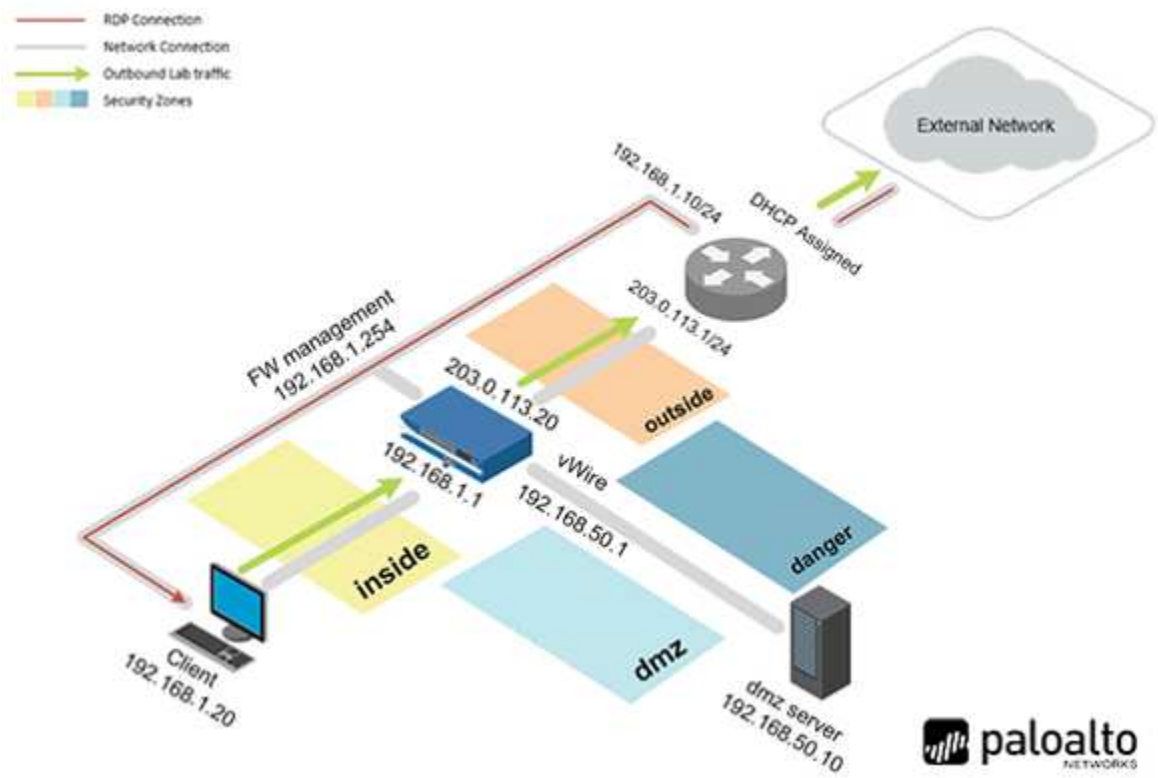
HR has also told you that there are certain types of traffic from employees that should not be decrypted because those transactions might contain personally identifiable information (PII). You need to exclude certain categories of websites (such as finance and healthcare) from decryption. You will create a No-Decrypt rule to prevent the firewall from decrypting traffic to and from these kinds of websites.

Objective

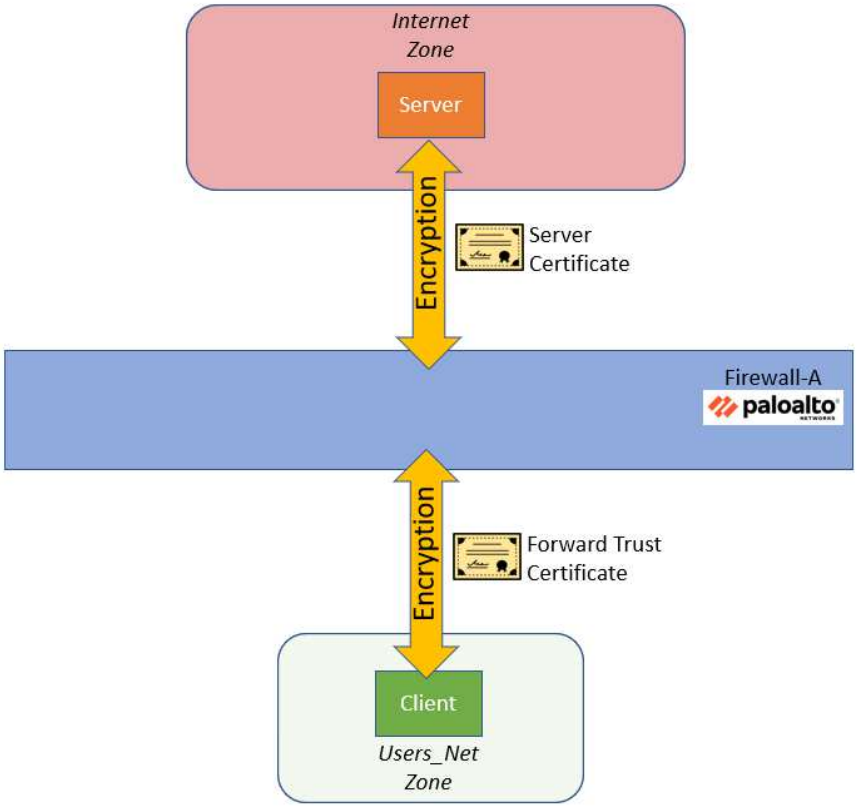
In this lab, you will perform the following tasks:

- Load a lab configuration.
- Test the firewall without decryption.
- Create a self-signed certificates for trusted connections.
- Create a self-signed certificates for untrusted connections.
- Create and test a Decryption policy rule for outbound traffic.
- Test outbound Decryption policy rule.
- Export the firewall certificate and import to Firefox.
- Test outbound Decryption policy again.
- Review firewall logs.
- Exclude URL categories from decryption using a No-Decrypt rule.
- Test the No-Decrypt rule.

Lab Topology



Theoretical Lab Topology



Lab Settings

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

Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Client	**192.168.1.20**	`lab-user`	`Pal0Alt0!`
DMZ	**192.168.50.10**	`root`	`Pal0Alt0!`
Firewall	**192.168.1.254**	`admin`	`Pal0Alt0!`
vRouter	**192.168.1.10**	`root`	`Pal0Alt0`

Lab Guidance

There are two sections in this lab guide:

- High-Level Lab Steps
- Detailed Lab Steps

The High-Level Lab Steps section provides only general guidance and information about how to accomplish the lab objectives. This section is more challenging and is suited for students who have a working knowledge of Palo Alto Networks firewalls. If you have never worked with a Palo Alto Networks firewall, we strongly encourage you to use the Detailed Lab Steps section.

The instructions in the Detailed Lab Steps section provide guided, detailed steps and screenshots to accomplish the lab objectives.

If you decide to use the High-Level Lab Guide and get stuck, switch to the Detailed Lab Guide for guidance.

You are not required to complete both the High-Level Lab Guide and the Detailed Lab Guide for each lab. Instead, please select the appropriate section based on your familiarity with Palo Alto Networks Firewalls.

1 Using Decryption to Block Threats in Encrypted Traffic – High Level Lab Steps

It is recommended to use this section if you possess significant experience in working with Palo Alto Networks firewalls. In case you require more comprehensive instructions to achieve the objectives, please utilize the Detailed-Lab Steps section in Task 2.

1.1 Apply a Baseline Configuration to the Firewall

- On the Zorin desktop, select *lab-user*, enter **Pal0Alt0!** for the password.
- For the Palo Alto Firewall, enter **admin** for the user and **Pal0Alt0!** for the password.
- Load and commit the configuration file - **edu-210-11.0a-12.xml** to the Firewall.

1.2 Test the Firewall Behavior Without Decryption

- On the client-A host, use the Firefox browser and browse to the following URL: **http://192.168.50.80/eicar.com**
- Note the block page that the firewall presents.

Your Antivirus Security Profile is in place and has blocked this file.

- Use Firefox to browse to **www.eicar.org**.
- In the Eicar website, navigate to **Download Anti Malware Testfile** > **Download area using the secure, SSL enabled protocol HTTPS.**
- Download the **eicar.com** file.
- When prompted to save the file, click **Cancel**.
- Close the Firefox browser.

1.3 Create a Self-Signed Certificate for Trusted Connections

- Use the information in the table below to create a self-signed certificate to use as a Forward Trust Certificate.

Parameter	Value
Certificate Name	**Type `trusted-cert`**
Common Name	**Type `192.168.1.1`**
Certificate Authority	Select the **Certificate Authority** check box
Forward Trust Certificate	**Checked**

1.4 Create a Decryption Policy Rule for Outbound Traffic

- Use the information below to create a Decryption Policy rule that will decrypt HTTPS traffic from the Users_Net security zone to the Internet security zone.

Parameter	Value
Name	**`Decrypt_User_Traffic`**
Description	**`Decrypts web traffic from Users_Net.`**
Source Zone	**`Users_Net`**
Source Address	**Any**

Parameter	Value
Source User	Any
Destination Zone	Internet Extranet
Destination Address	Any
Service	any
URL Category	Any
Action	Decrypt
Type	SSL Forward Proxy
Decryption Profile	None

1.5 Commit the Configuration

- Commit the changes before proceeding.

1.6 Test Outbound Decryption Policy

- Use Firefox and browse to **https://www.bing.com**.
- Use the **Advanced > View Certificate** buttons to note that the **Issuer Name** section contains **192.168.1.1.**
- Close the Firefox browser.

1.7 Export the Firewall Certificate

- From the firewall web interface, export the trusted-cert as a Base64 Encoded Certificate (PEM).
- Save the file to the Downloads folder of the Client-A host.

1.8 Import the Firewall Certificate to Firefox

- Use Certificate Manager in Firefox to Import the **cert_trusted-cert.crt** to the **Authorities** section.
- Set Firefox to **Trust this CA to identify websites** and **Trust this CA to identify email users.**

1.9 Test Outbound Decryption Policy Again

- In Firefox, browse to **https://www.eicar.org.**
- Navigate to **Download Anti Malware Testfile** > **Download.**
- Attempt to download the **eicar.com** file.
- You will receive a warning page from the firewall indicating that it has detected and blocked the malicious file download.
- Close the Firefox browser.

1.10 Review Firewall Logs

- Add the Decrypted column to the **Traffic Log.**
- Drag and drop the **Session End Reason** column from the right side of the table to the beginning of the table.
- Create and apply a filter to display entries that have been decrypted from the client workstation and that have been terminated because of a detected threat in the traffic.
- Examine the Detailed Log View of a matching entry to see details about the session.
- Use the **Threat** Log to locate entries about the eicar.com test file that the firewall detected and blocked.

1.11 Exclude URL Categories from Decryption

- Use the information below to create an entry in the Decryption Policy that will exclude certain URL categories from decryption.

Parameter	Value
Name	`No-Decryption`
Description	`Do not decrypt URLs in gov, shopping and finance`
Source Zone	`Users_Net`
Destination Zone	`Internet`
Service	`any`

URL Category	`government`
	`financial-services`
	`shopping`

Action	`No Decrypt`
Type	`SSL Forward Proxy`

Note that in a production environment, the URL Categories which you exclude from decryption will depend on many factors. Company policy, national privacy laws, HR concerns, destination country – all of these can dictate what types of traffic you should or should not decrypt. The examples we use here simple ones to illustrate how to exclude URL categories from decryption.

- Place this rule at the top of the **Decryption** Policy.

1.12 Commit the Configuration

- Commit the changes before proceeding.

1.13 Test the No-Decryption Rule

- Use Firefox to browse to a website that falls into one of the excluded categories.
- Connect to https://texas.gov.
- Examine the certificate issued to the texas.gov website.
- Note that the Issuer Name is *not* 192.168.1.1 (the firewall).

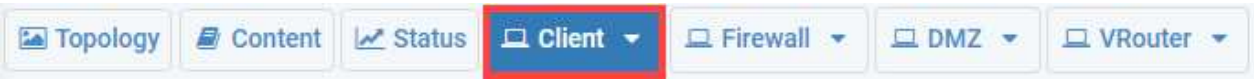
2 Using Decryption to Block Threats in Encrypted Traffic – Detailed Lab Steps

It is recommended to use this section if you prefer detailed guidance to complete the objectives for this lab. It is strongly recommended that you use this section if you do not have extensive experience working with Palo Alto Networks firewalls.

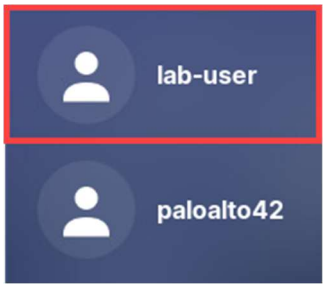
2.1 Apply a Baseline Configuration to the Firewall

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

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



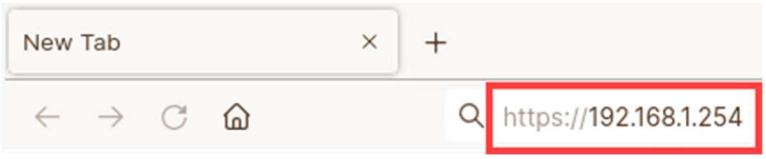
2. On the *Zorin* desktop, click **lab-user.**



3. For the *lab-user* password, enter **Pal0Alt0!** and press **Enter**.

4. Double-click the **Firefox Web Browser** icon located on the *Desktop*.

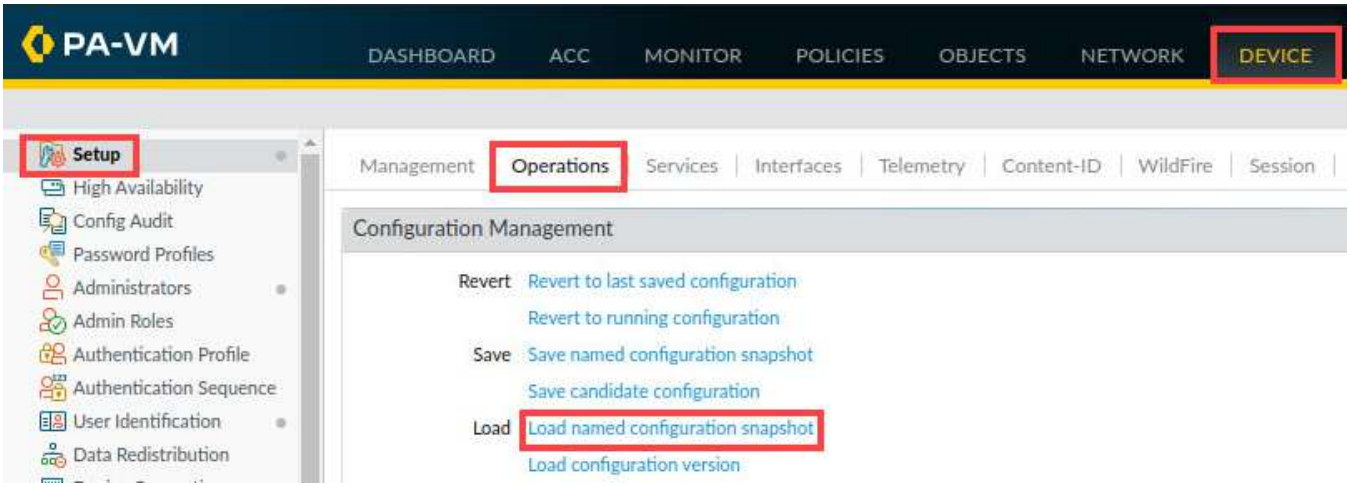
5. In the *Firefox* address field, type **`https://192.168.1.254`** and press **Enter**.



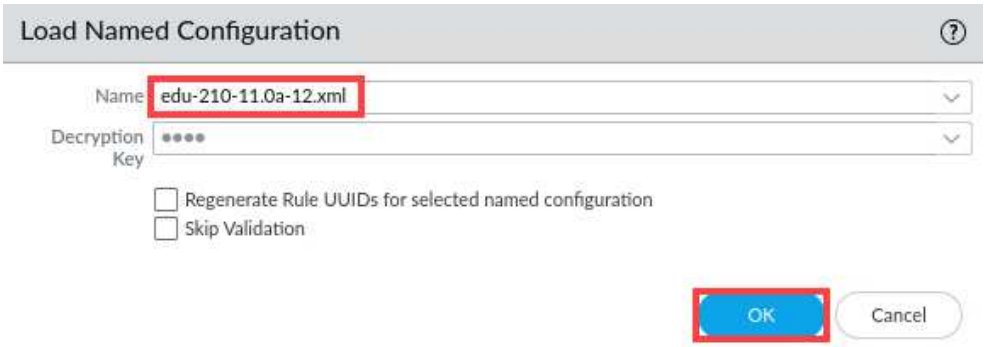
6. Log in to the Firewall web interface as username **`admin`**, password **`Pal0Alt0!.`**

If you do not immediately see the login page, please wait an additional 1-3 minutes for the *Firewall* to fully initialize. If needed, refresh the page.

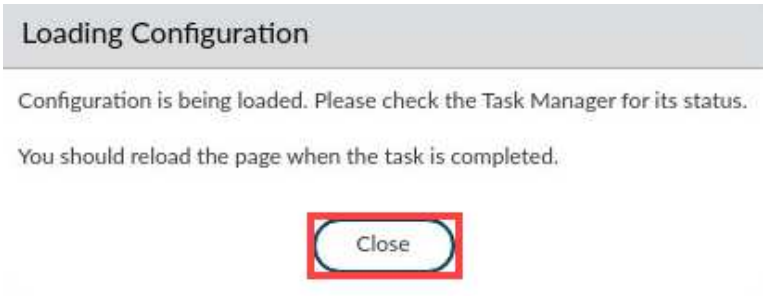
7. Navigate to **Device > Setup > Operations** in the web interface and click on **Load named configuration snapshot** underneath the *Configuration Management* section.



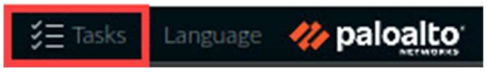
8. In the *Load Named Configuration* window, select **edu-210-11.0a-12.xml** from the *Name* drop-down box and click **OK**.



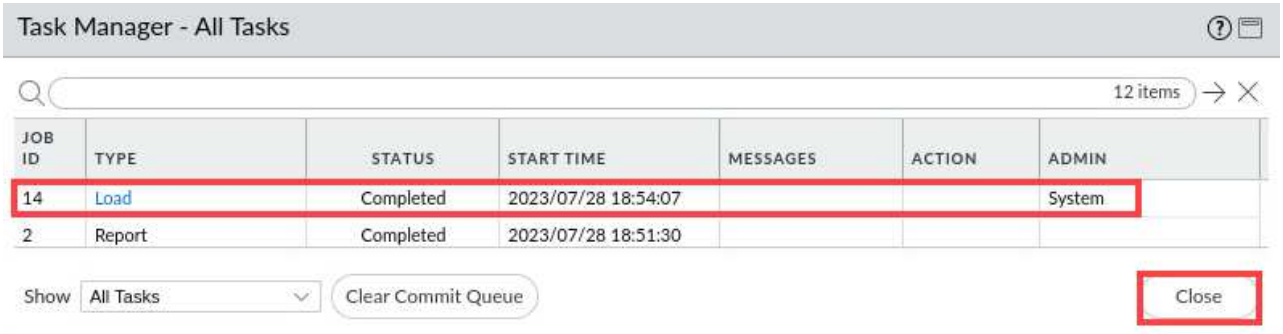
9. In the *Loading Configuration* window, a message will show *Configuration is being loaded*. *Please check the Task Manager for its status. You should reload the page when the task is completed.* Click **Close** to continue.



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

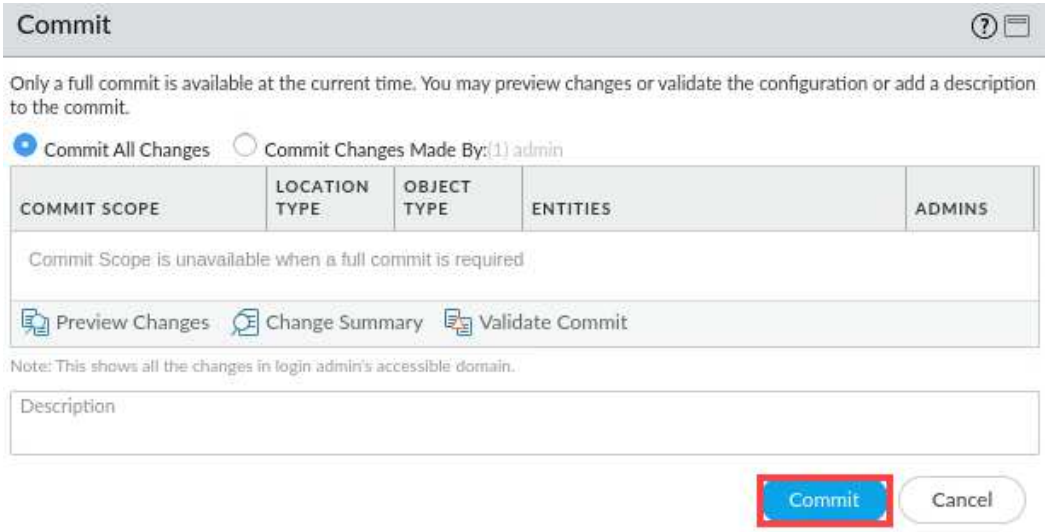


11. In the *Task Manager – All Tasks* window, verify the *Load* type has been completed. Click **Close**



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

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



14. When the commit operation is complete, 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.

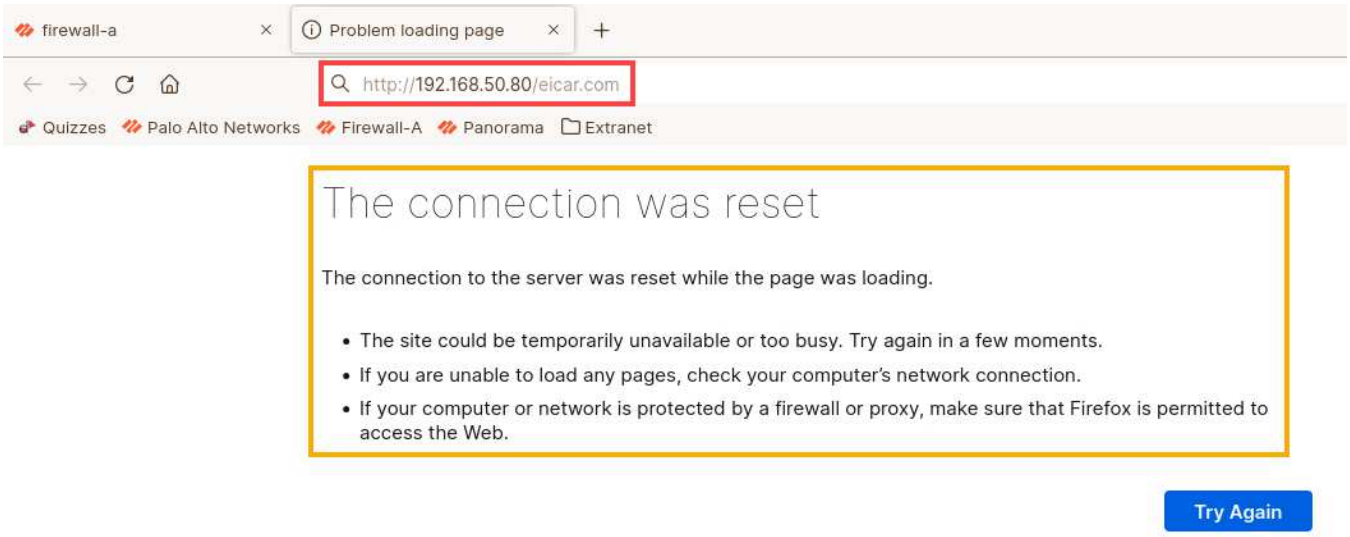
15. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

2.2 Examine Firewall Configuration

In this section, you will test the firewall behavior without decryption by downloading a virus.

1. On the *client* desktop, open a new tab in **Firefox**.

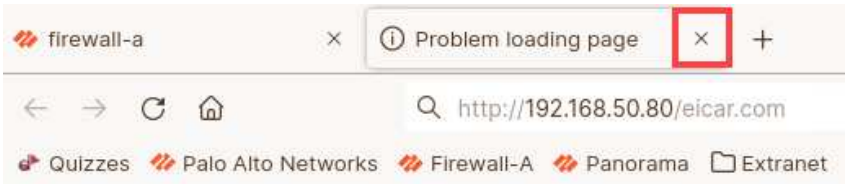
2. Type **http://192.168.50.80/eicar.com** and press **Enter**. You should get a page indicating that the connection was reset.



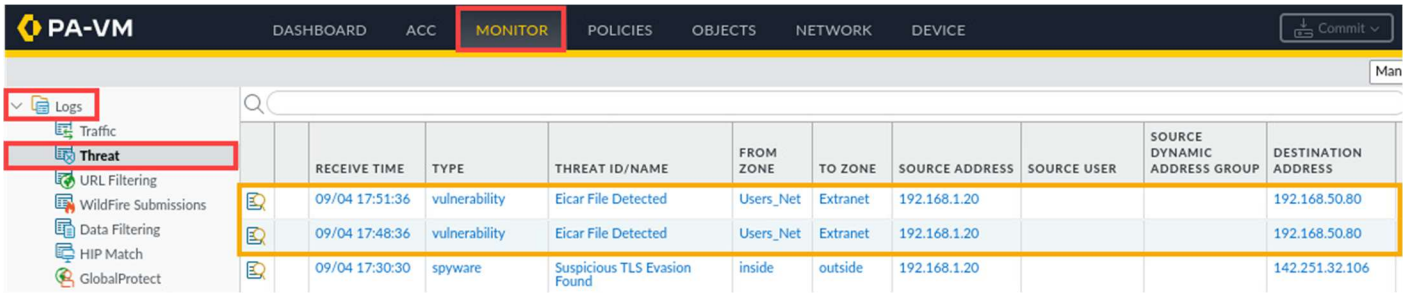
Please Note

Because the connection between the client and the server is not encrypted, the firewall is able to examine the traffic and block malicious content.

3. Close the Firefox tab for the *eicar* file download.

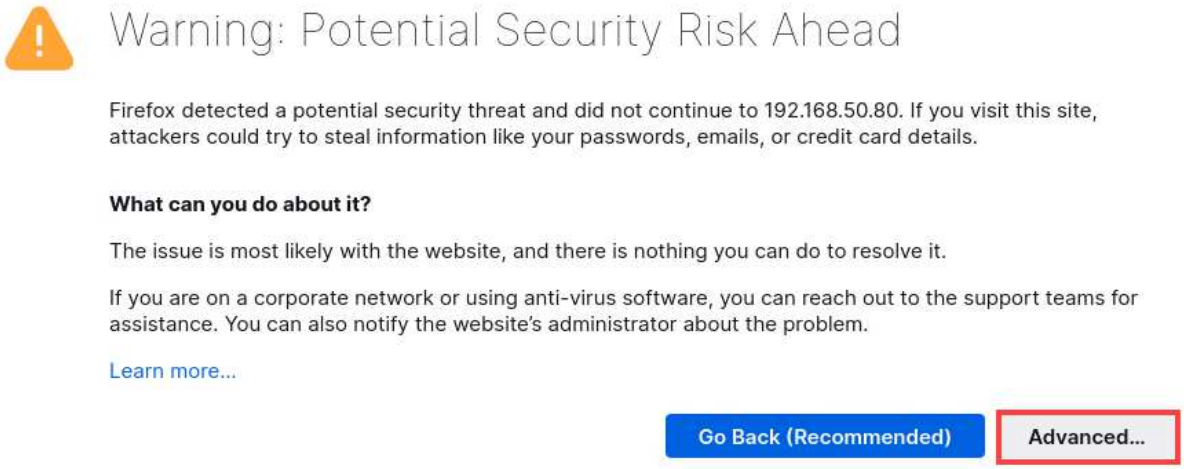


4. In the firewall web interface, navigate to **Monitor > Logs > Threat**. You should see one or more entries for vulnerability indicating that the firewall blocked the Eicar file download.

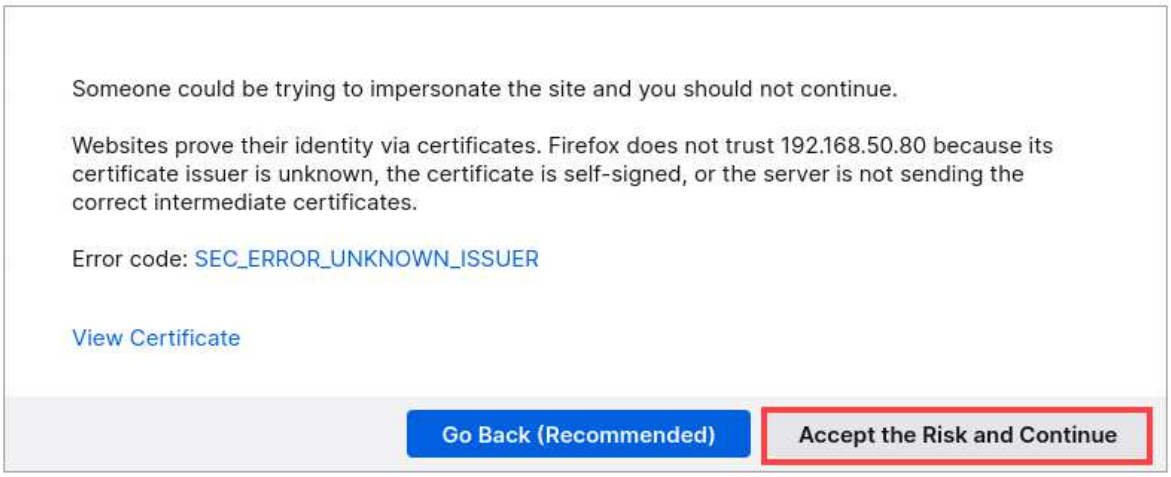


5. In Firefox, open a new tab and browse to **https://192.168.50.80/eicar.com**.

6. If Firefox presents a **Warning** window, click the **Advanced** button.



7. Click **Accept the Risk and Continue**.



Please Note

The web server is using a self-signed SSL certificate, which is why Firefox presents this warning.

8. When you are prompted to save the file, click **Cancel**.

Please Note

Notice that the download is not blocked because the connection is encrypted, and the virus is hidden. This exercise proves that without Decryption, the firewall is unable to examine the contents of a secure connection and cannot scan for malicious content.

9. Close the **Firefox** tab for the *eicar* file download.

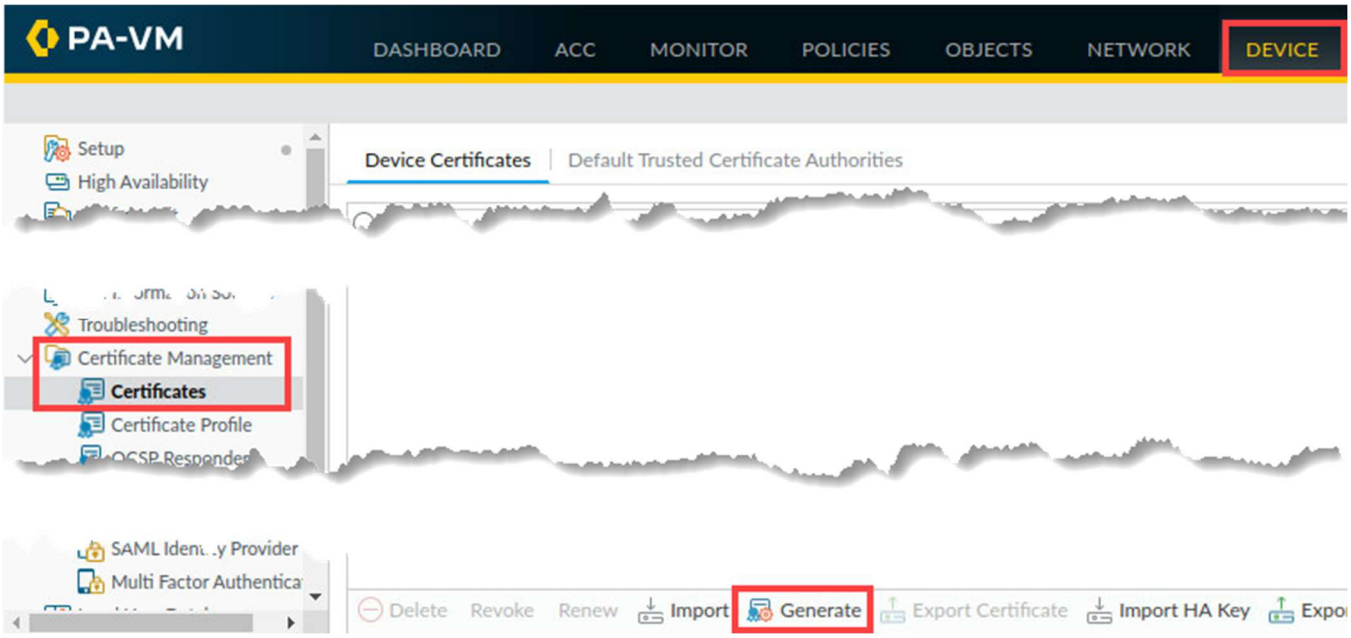
10. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

2.3 Create a Self-Signed Certificate for Trusted Connections

In this section, you will generate a certificate on the firewall that will be used when clients connect to HTTPS websites that have certificates issued by trusted certificate authorities.

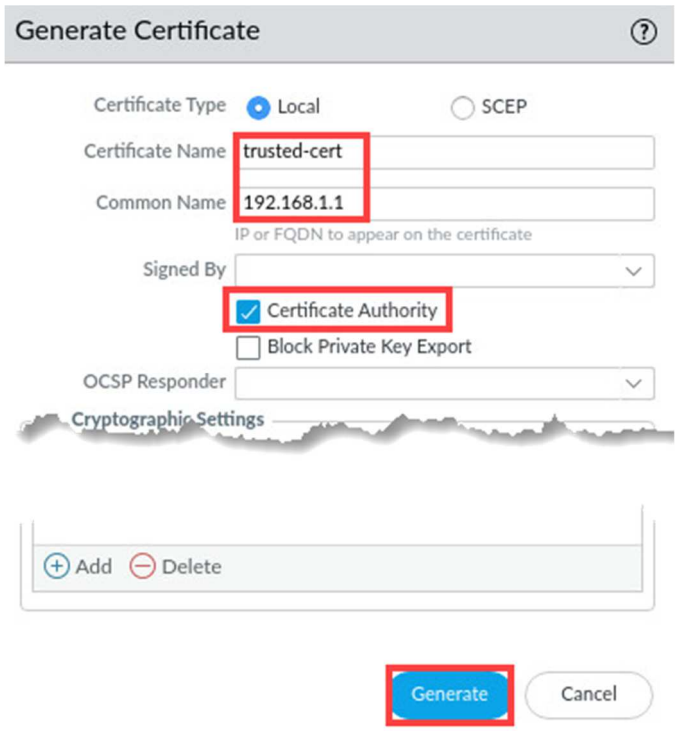
The firewall will use this certificate as part of the decryption process between clients and trusted HTTPS websites.

1. Select **Device > Certificate Management > Certificates**. Click **Generate** to create a new *CA Certificate*.



2. In the *Generate Certificate* window, configure the following. Click **Generate**.

Parameter	Value
Certificate Name	`trusted-cert`
Common Name	`192.168.1.1`
Certificate Authority	**Certificate Authority**

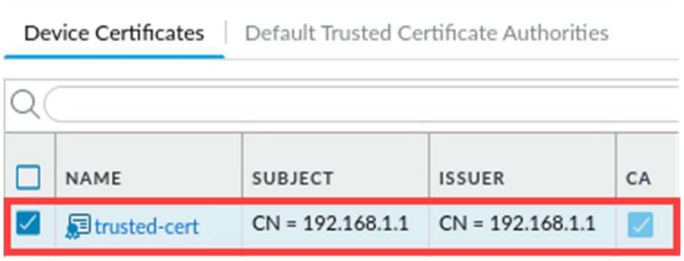


Please Note

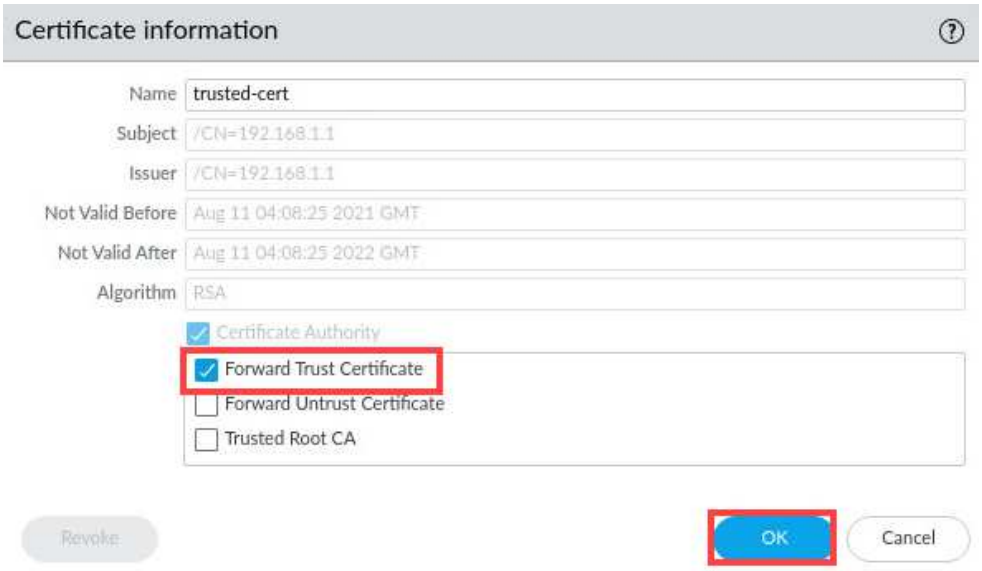
A Generate Certificate status window should open that confirms that the certificate and key pair were generated successfully.

3. In the *Generate Certificate* window, click **OK**.

4. You should have a new entry in the *Device Certificates* table. Click **trusted-cert**.



5. In the *Certificate information* window, place a **check** in the box for **Forward Trust Certificate**. Click **OK**.



Please Note

This action instructs the firewall to use this certificate to decrypt traffic between clients and trusted HTTPS sites.

6. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

2.4 Create a Self-Signed Certificate for Untrusted Connections

In this section you will generate a certificate on the firewall that will be used when clients connect to HTTPS websites that DO NOT have certificates issued by trusted certificate authorities - for example, sites that use self-signed certificates or certificates that have expired.

The firewall will use this certificate as part of the decryption process between clients and untrusted HTTPS websites.

1. Click **Generate** to create a new *CA Certificate*.

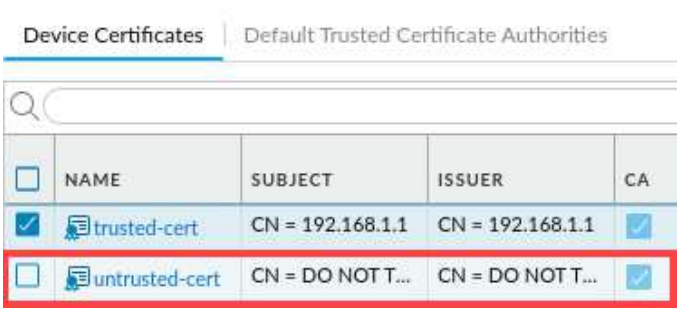
2. In the *Generate Certificate* window, configure the following. Click **Generate**.

Parameter	Value
Certificate Name	`untrusted-cert`
Common Name	**DO NOT TRUST**
Certificate Authority	**Certificate Authority**

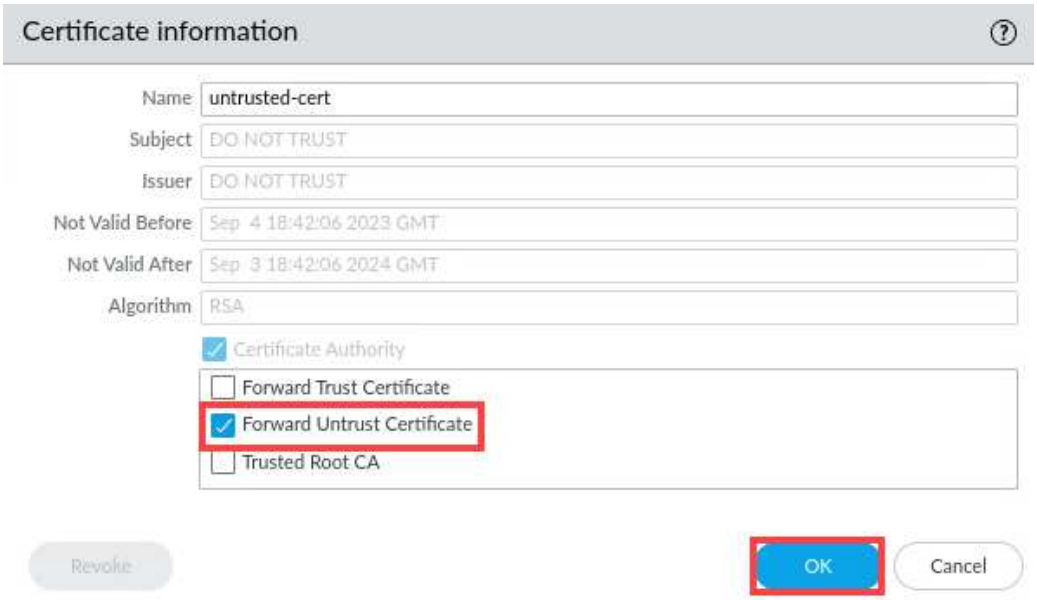
Please Note A Generate Certificate status window should open that confirms that the certificate and key pair were generated successfully.

3. In the *Generate Certificate* window, click **OK**.

4. You should have a new entry in the *Device Certificates* table. Click **untrusted-cert**.



5. In the *Certificate information* window, place a **check** in the box for **Forward Untrust Certificate**. Click **OK**.



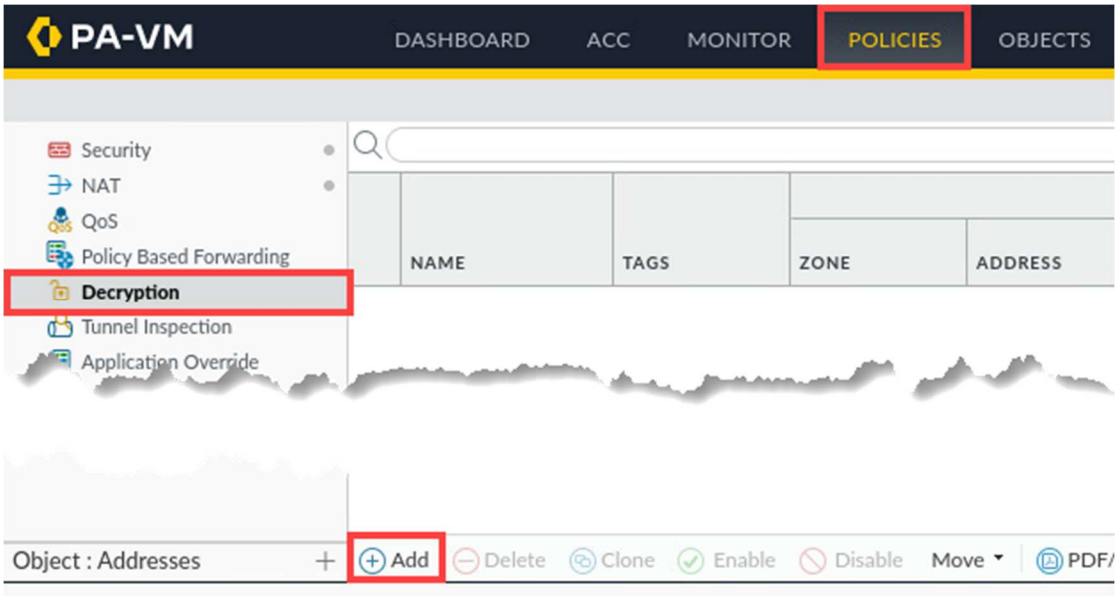
This action instructs the firewall to use this certificate to decrypt traffic between clients and HTTPS sites that are not trustworthy (expired certificates, self-signed certificates, etc.).

6. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

2.5 Create Decryption Policy for Outbound Traffic

In this section, you will create a Decryption Policy to decrypt HTTPS traffic from the Users_Net security zone to the Internet security zone.

1. Select **Policies > Decryption**. Click **Add**.

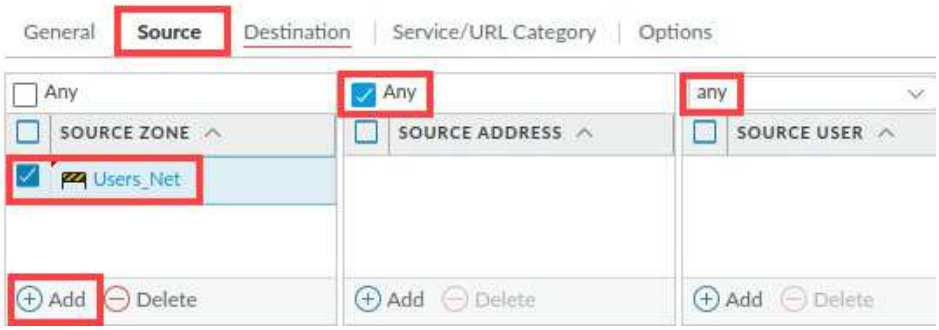


2. In the *Decryption Policy Rule* window, under the **General** tab, configure the following.

Parameter	Value
Name	`Decrypt_User_Traffic`
Description	`Decrypts web traffic from Users_Net.`

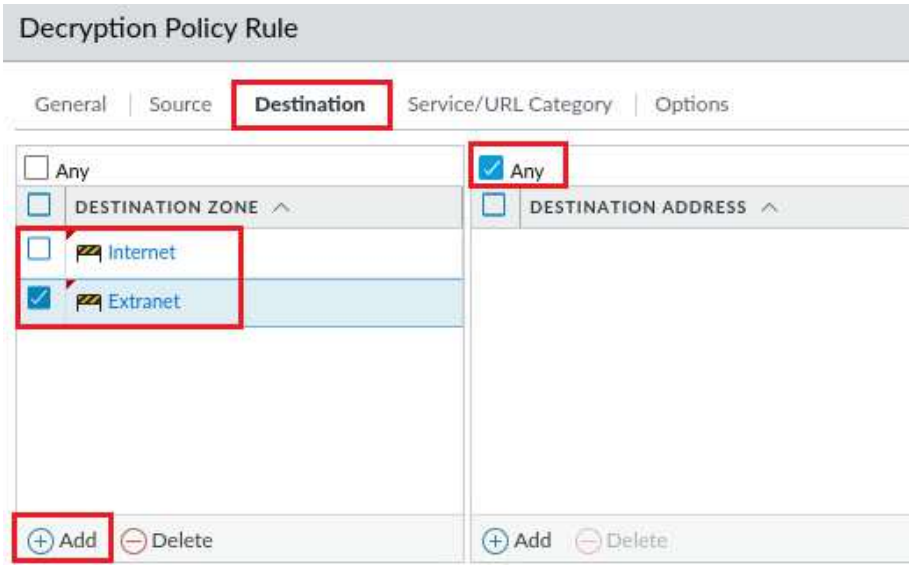
3. Click the **Source** tab and configure the following.

Parameter	Value
Source Zone	**Users_Net**
Source Address	**Any**
Source User	**any**



4. Click the **Destination** tab and configure the following.

Parameter	Value
Destination Zone	**Internet** **Extranet**
Destination Address	**Any**



5. Click the **Service/URL Category** tab and verify that the **Service** is set to **any** and that the box for **Any** above **URL Category** is **checked**.

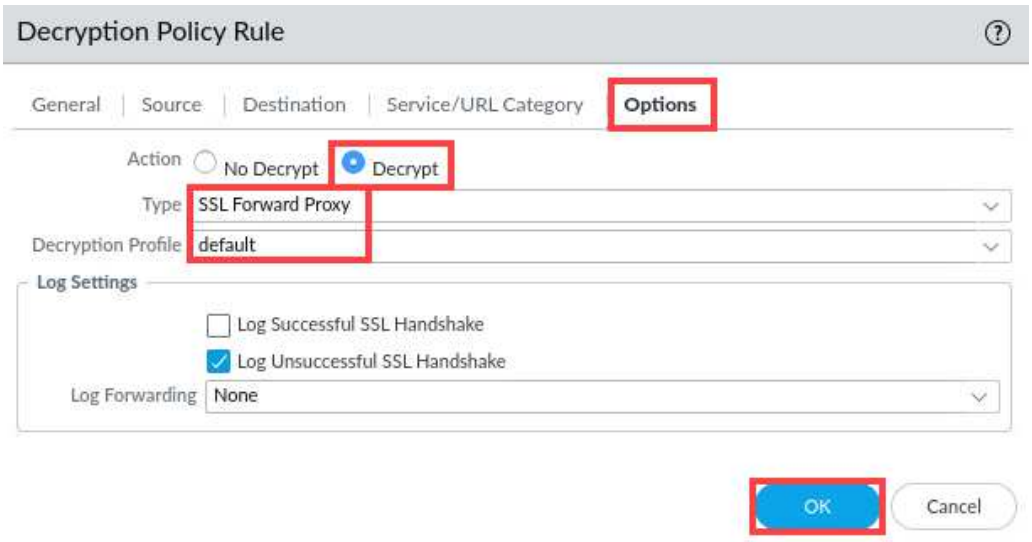
Please Note

Note that the Any setting for URL category instructs the firewall to decrypt all HTTPS traffic, regardless of the type of website users are accessing. Decrypting traffic from users to website categories such as Health and Medicine, Shopping or Government can expose Personally Identifiable Information (PII). In a production environment, you will need to make sure you only decrypt traffic which is appropriate.

Later in this lab, you will exclude several categories of websites as an illustration.

6. Click the **Options** tab and configure the following. Click **OK**.

Parameter	Value
Action	**Decrypt**
Type	**SSL Forward Proxy**
Decryption Profile	**default**

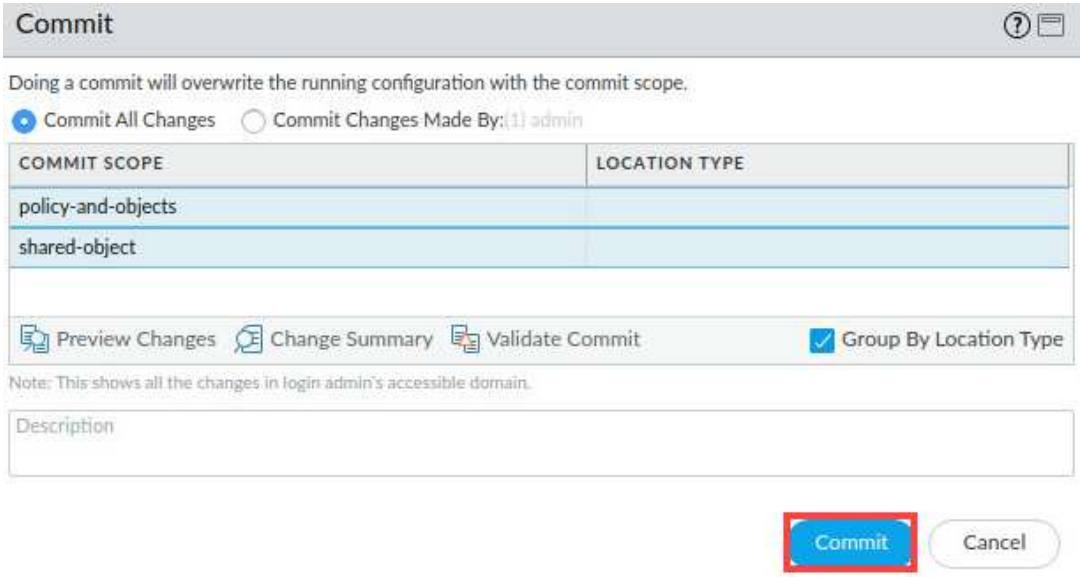


7. Verify the *Decryption* policy is visible, and the configuration matches the following.

	NAME	Source ZONE	Destination ZONE	URL CATEGORY	SERVICE	ACTION	TYPE
1	Decrypt_User_Traffic	Users_Net	Extranet Internet	any	any	decrypt	ssl-forward-proxy

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

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



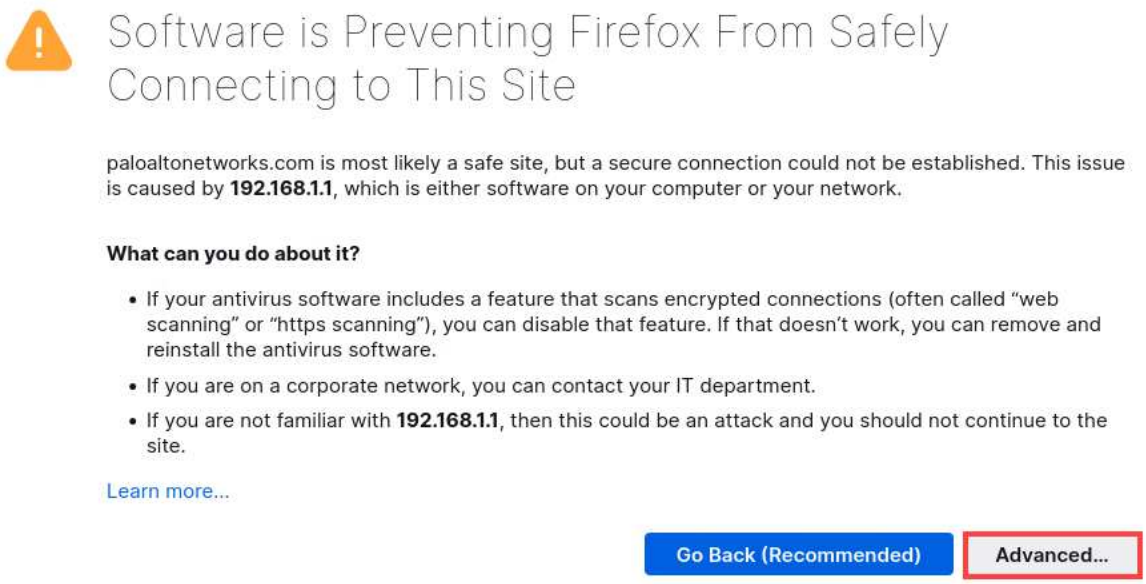
10. When the commit operation successfully completes, click **Close** to continue.

2.6 Test Outbound Decryption Policy

In this section, you will test the outbound decryption policy.

1. In the *Firefox Web Browser,* open a new tab. Type **https://paloaltonetworks.com** and press **Enter**.

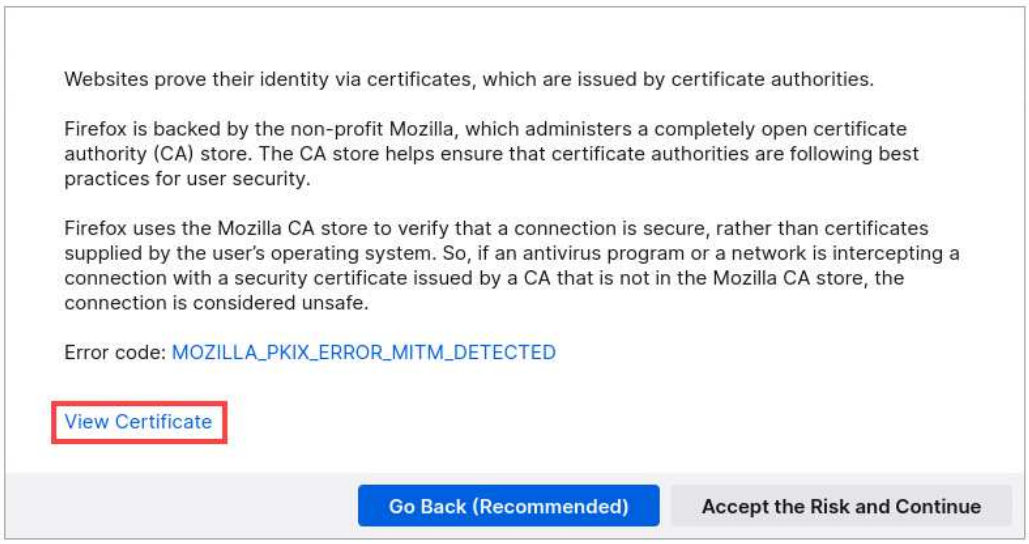
2. The browser presents a Caution message. Click **Advanced**.



Please Note

The endpoint (client workstation) does not trust the certificate generated by the firewall (192.168.1.1).

3. Click the link for **View Certificate**.



4. Under the section for **www.paloaltonetworks.com**, note the **Issuer Name** section contains **192.168.1.1**.

Please Note

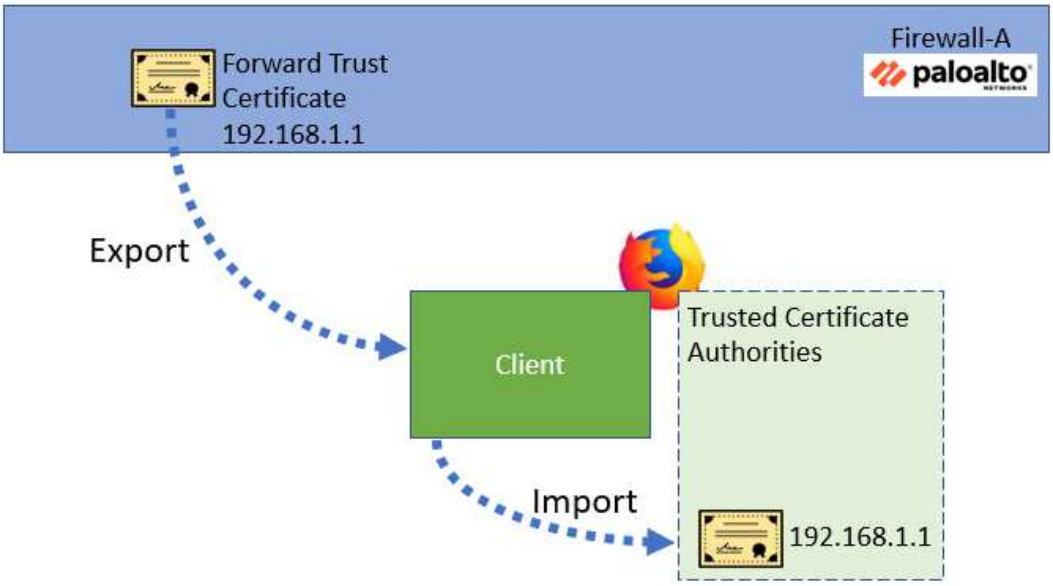
This certificate has been issued on behalf of www.paloaltonetworks.com by the firewall (192.168.1.1) using the Trusted Certificate you created earlier. The client browser does not trust this certificate because it is "self-signed" by the firewall. In the next section, you will fix this issue so that the Firefox browser trusts certificates issued by the firewall.

5. Close the Firefox tabs for the certificate and for the Warning, but leave open the firewall web interface tab.

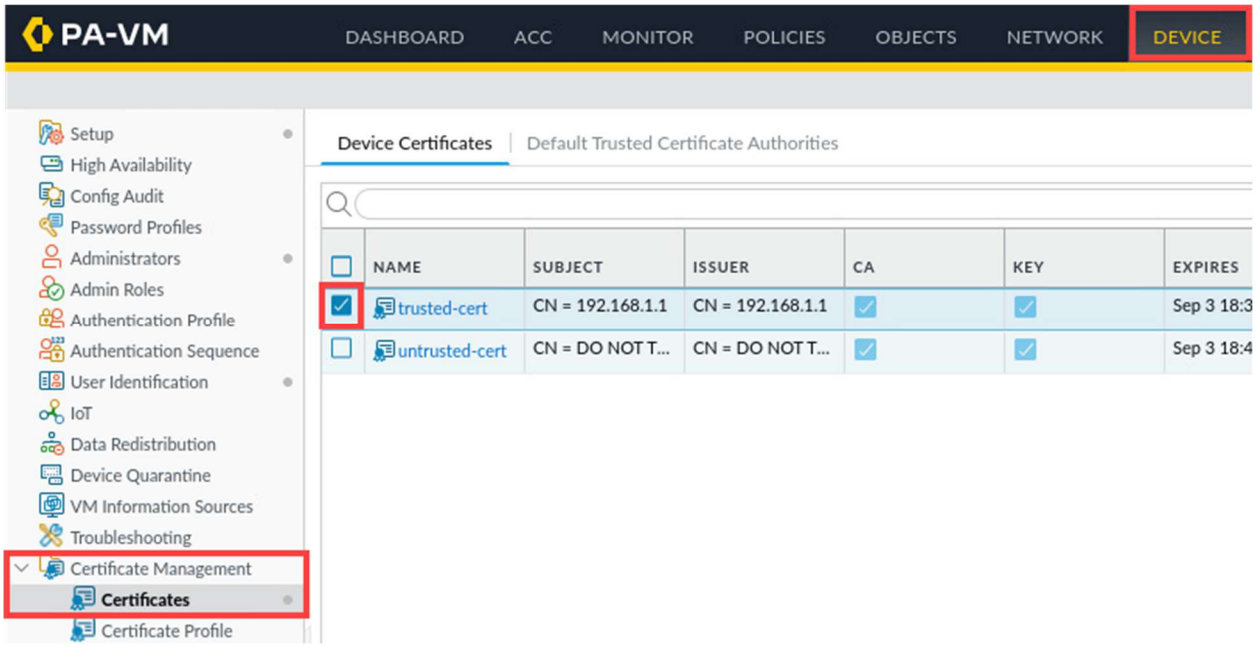
2.7 Export the Firewall Certificate

In this section, you will export the trusted certificate from the firewall.

To make users' web browsing experience seamless while implementing decryption, you will export the trusted certificate from the firewall and import the certificate into Firefox on the Client host.

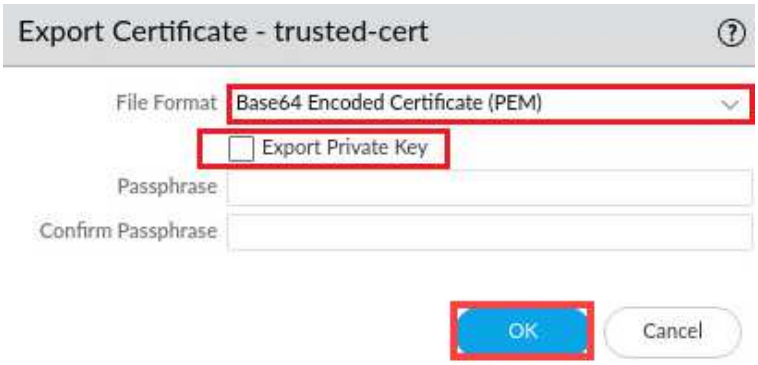


1. Select **Device > Certificate Management > Certificates**. **Highlight** but do not open *trusted-cert*.



2. At the bottom of the window, click **Export Certificate** to open the *Export Certificate* configuration window.

3. In the *Export Certificate – trusted-cert* window, select the dropdown menu for File Format and select **Base64 Encoded Certificate (PEM)**. Uncheck **Export Private Key** and click **OK** to export the trusted-cert certificate.



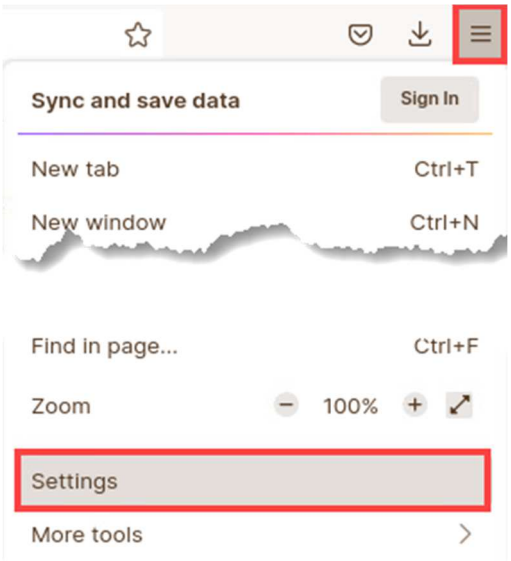
4. Ensure the workstation's *Downloads* folder is selected and click **Save**.

5. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

2.8 Import the Firewall Certificate

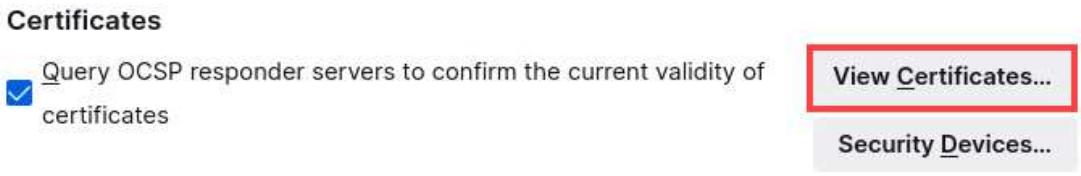
In this section, you will import the trusted-cert certificate from the workstation to the Firefox Web Browser.

1. In the upper right corner of the window, click the "**hamburger**" button and choose **Settings**.

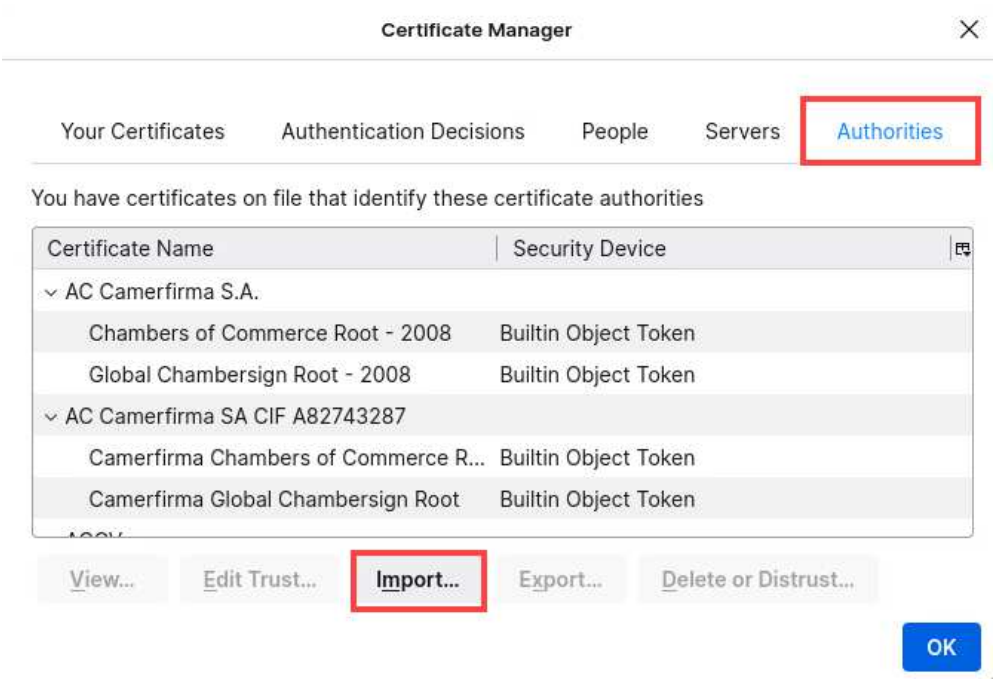


2. On the left side of the screen, select **Privacy & Security**.

3. Scroll to the bottom of the screen and locate the *Certificates* section. Click **View Certificates**.

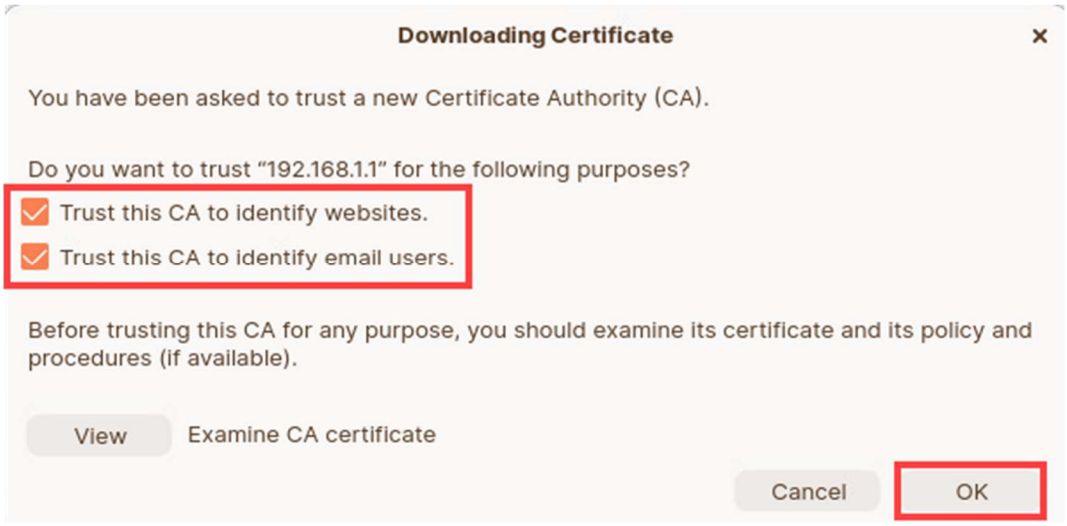


4. In the *Certificate Manager* window, on the **Authorities** tab. Click **Import**.



5. In the *Select File containing CA certificate(s) to import* window, click **Downloads**. Select **cert_trusted-cert.crt** and click **Open**.

6. In the *Downloading Certificate* window, place **checks** in both boxes for **Trust this CA**. Click **OK**.



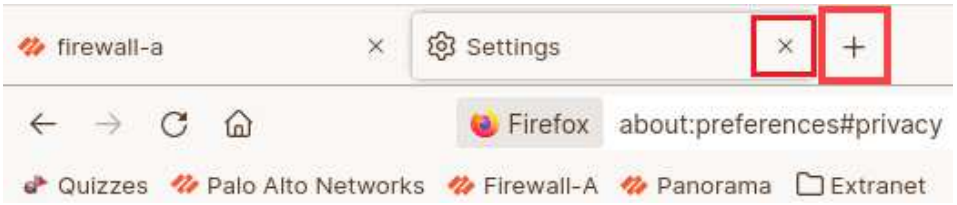
7. The firewall **trusted-cert** entry appears in the list of certificate authorities. Click **OK**.

Please Note

If the certificate for 192.168.1.1 does not appear at the top of the list, click OK and then click View Certificates again.

The Firefox browser will trust any certificate issued by the entities in this Authorities list. By adding the firewall certificate to this list, the Firefox browser will trust any certificates issued by the firewall. Note that the process of importing certificates to client workstations varies based on the browser type and the operating system.

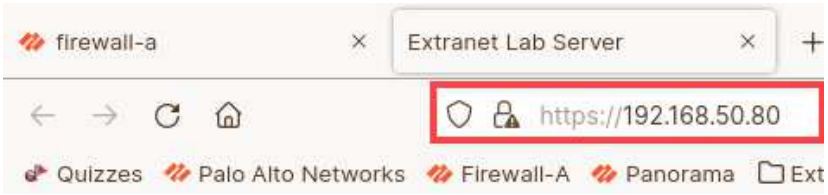
8. Close the **Settings** window. Open a new **Firefox** tab and continue to the next task.



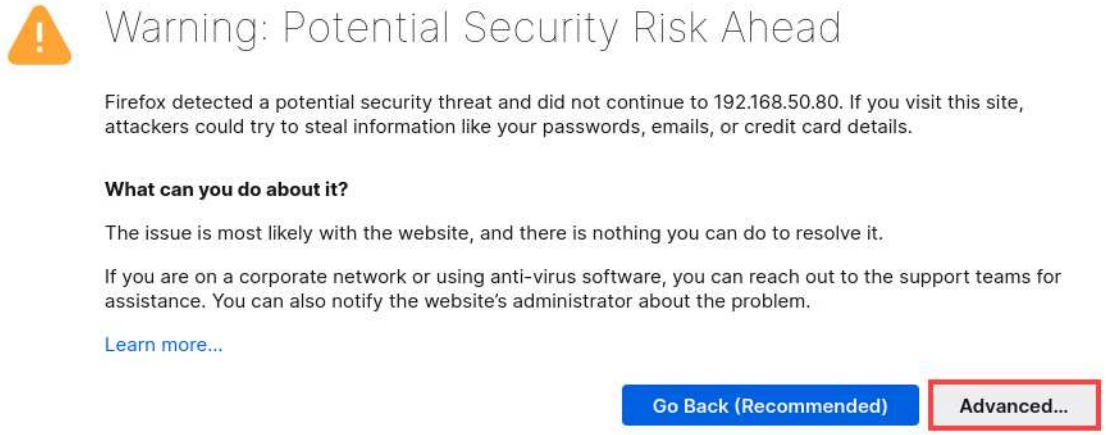
2.9 Test Forward Untrust Certificate

When a web browser connects to a site that has a self-signed or untrusted certificate, the firewall will present the Forward Untrust Certificate. The web server in the Extranet zone has a self-signed certificate; in this section, you will see how the firewall presents the DO NOT TRUST certificate you created.

1. Type **https://192.168.50.80** and press **Enter**.



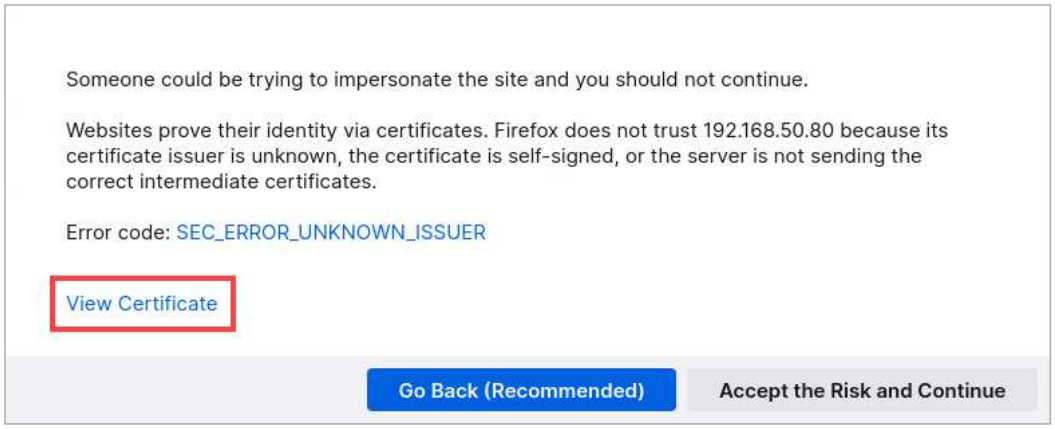
2. Note the **Warning** message that Firefox presents. Click **Advanced**.



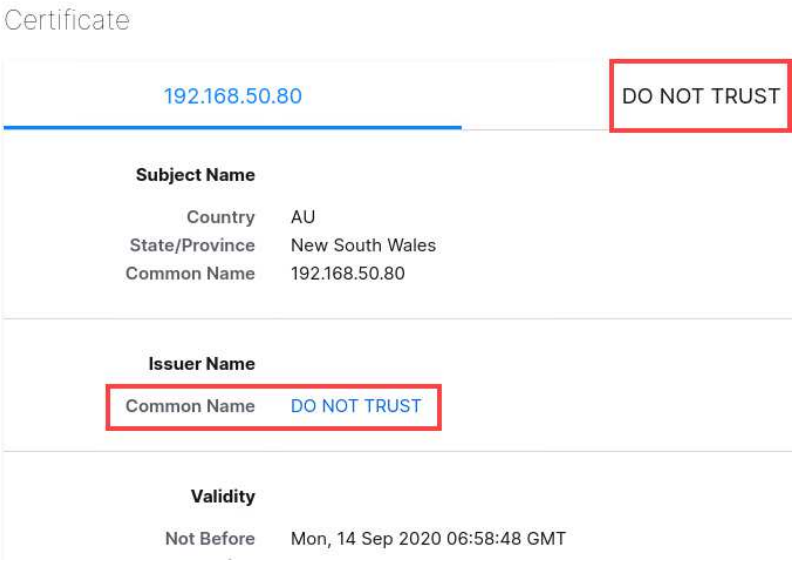
Please Note

The endpoint (client workstation) does not trust the certificate generated by the firewall (192.168.1.1).

3. Click the link for **View Certificate**.



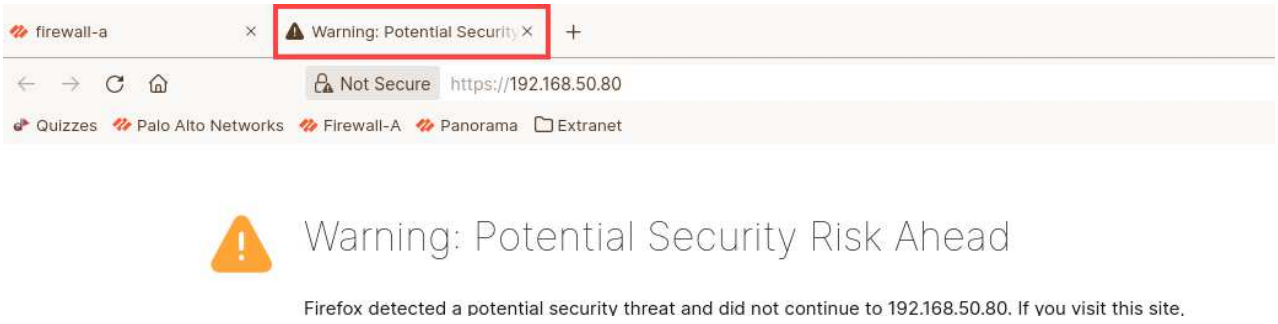
4. Note the information in the certificate.



Please Note You can tell that the firewall has intervened in this connection and presented the Forward Untrust certificate you created.

5. Close the Firefox tab for the certificate.

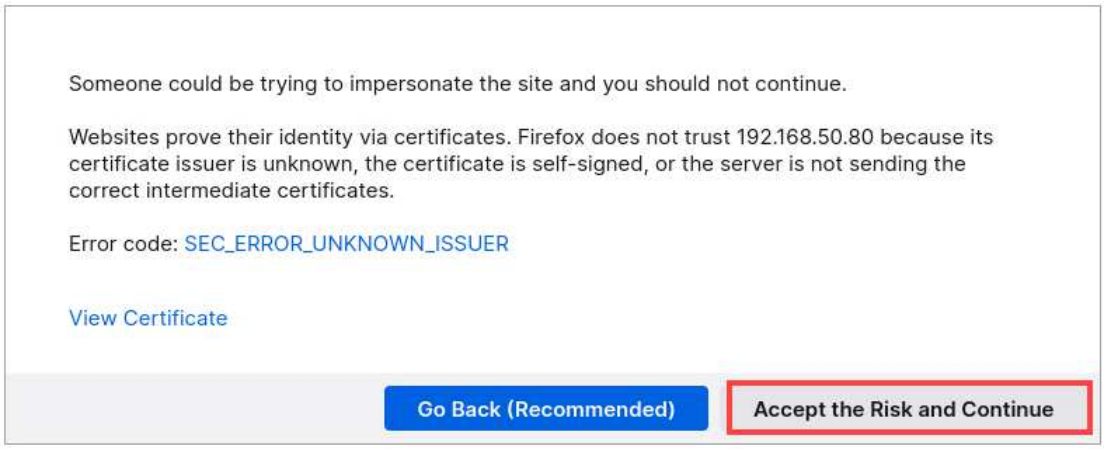
6. Select and confirm the **Warning: Potential Security Risk Ahead** window is open and continue to the next task.



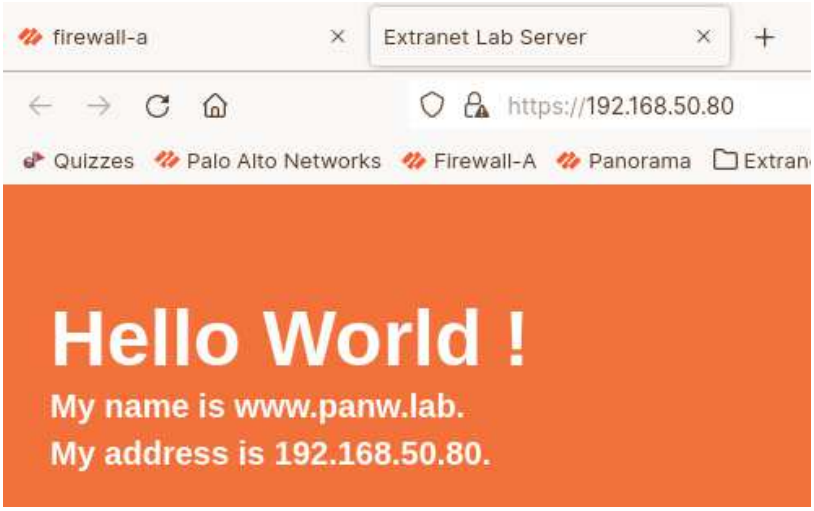
2.10 Test Outbound Decryption Policy Again

With the firewall trusted-cert certificate imported to Firefox on the client workstation, try downloading the virus file using HTTPS again.

1. In the *Firefox* warning window, click **Accept the Risk and Continue**.

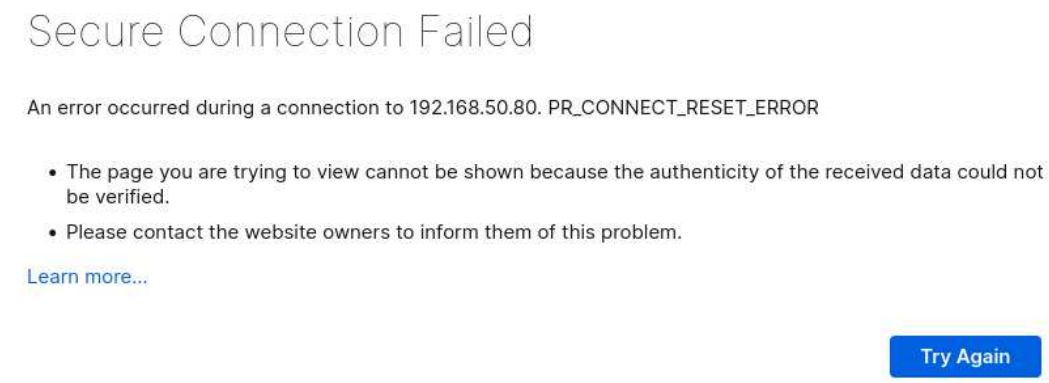


2. You will see the default page for the web server in the Extranet.



3. Attempt to download the virus file by appending **eicar.com** to the end of the link https://192.168.50.80/***eicar.com***. Click **Enter**.

4. The connection will not succeed, and you will receive a message from the browser.

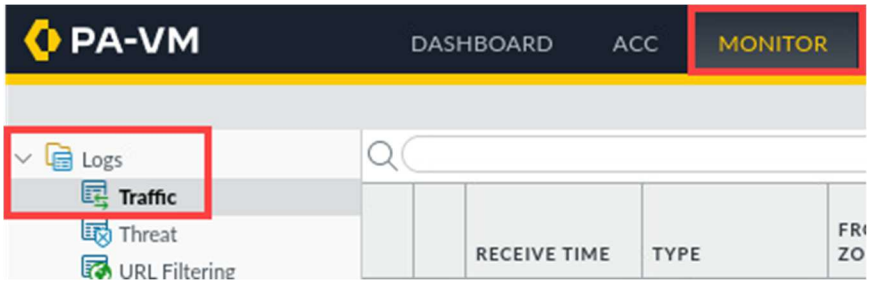


5. Close the **https://192.168.50.80/eicar.com** *Firefox* tab. Continue to the next task.

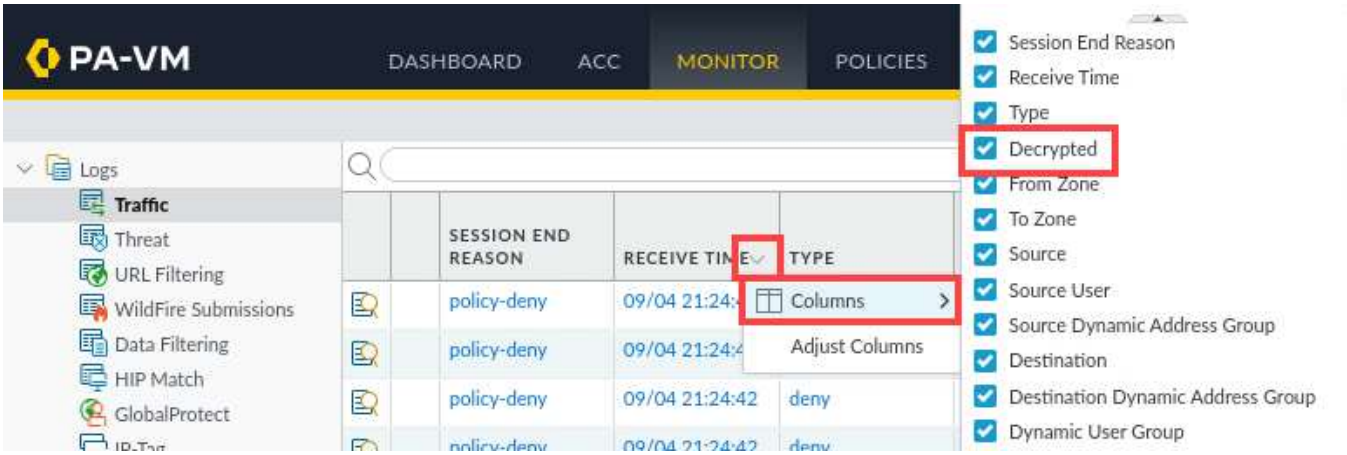
2.11 Review Firewall Logs

In this section, you will examine information in the firewall Logs to see more details about the decryption process.

1. Select **Monitor > Logs > Traffic.**



2. Click the small triangle to the right of the *Receive Time* column header. Add the **Decrypted** column to the table by selecting **Columns > Decrypted**.



3. Drag and drop the **Session End Reason** column from the right side of the table to the beginning of the table. You may need to *scroll* the Traffic window to find the *Session End Reason*.

SESSION END REASON	RECEIVE TIME	TYPE	FROM ZONE	TO ZONE	SOURCE	DECRYPTED
aged-out	08/11 05:24:05	end	Users_Net	Internet	192.168.1.20	no
aged-out	08/11 05:24:05	end	Users_Net	Extranet	192.168.1.20	no
policy-deny	08/11 05:24:04	deny	Users_Net	Internet	192.168.1.20	no

Please Note

This is not a requirement, but placing this column at the beginning of the table will make it easier for you to locate entries that have ended because of unusual actions taken by the firewall (such as detecting a threat).

4. In the filter builder, type **`( flags has proxy ) and ( session_end_reason eq threat )`**. Click **Apply Filter**. This will display entries that have been decrypted from the client workstation and that have been terminated because of a detected threat in the traffic. If the traffic log is not showing, allow one to two minutes for it to populate.

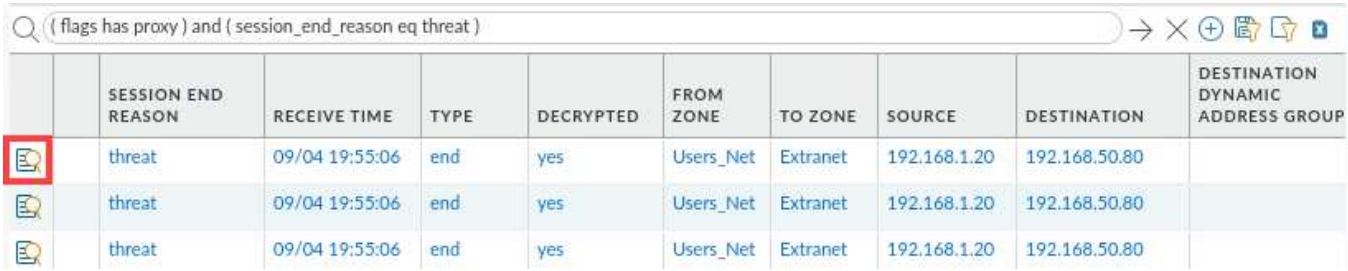
(flags has proxy) and (session_end_reason eq threat)

SESSION END REASON	RECEIVE TIME	TYPE	DECRYPTED	FROM ZONE	TO ZONE	SOURCE	DESTINATION	DESTINATION DYNAMIC ADDRESS GROUP
threat	09/04 19:55:06	end	yes	Users_Net	Extranet	192.168.1.20	192.168.50.80	
threat	09/04 19:55:06	end	yes	Users_Net	Extranet	192.168.1.20	192.168.50.80	
threat	09/04 19:55:06	end	yes	Users_Net	Extranet	192.168.1.20	192.168.50.80	

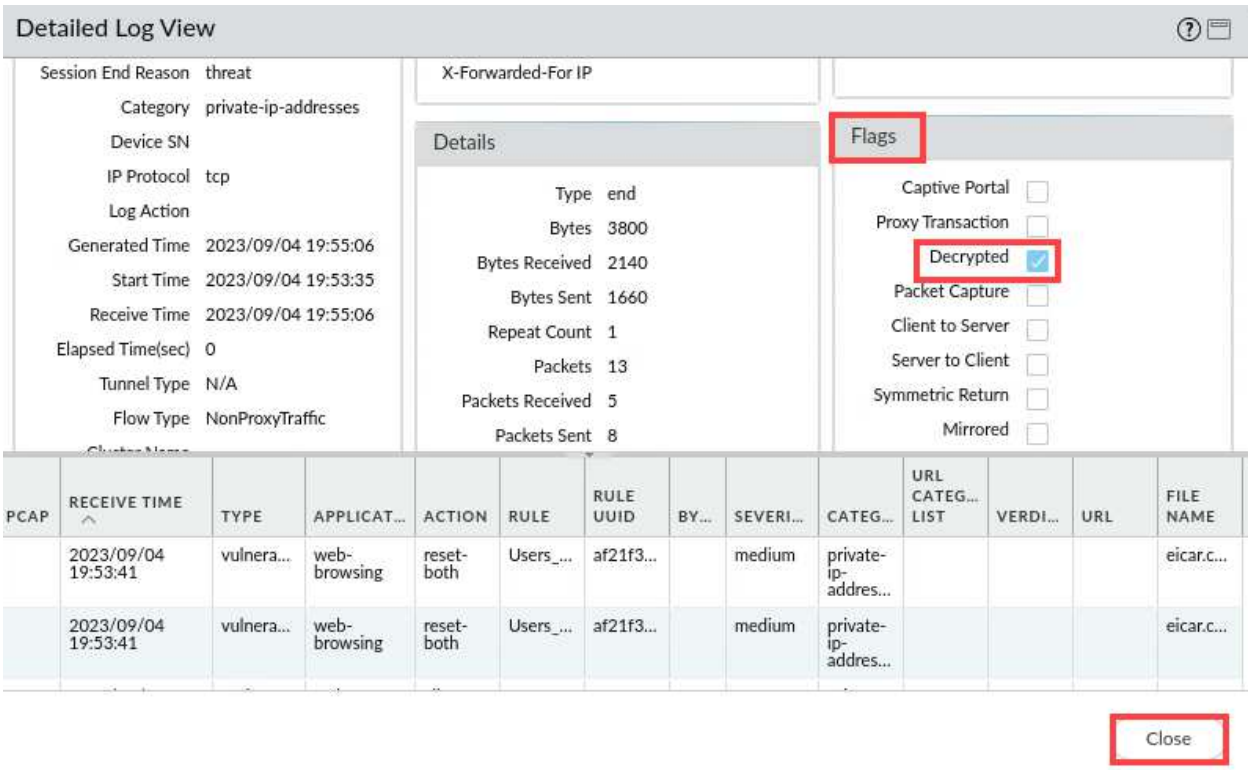
Please Note

The filter syntax “flags has proxy” displays entries which have been decrypted (the value will show as **yes** in the **Decrypted** column). Entries that match the filter indicate that the firewall carried out a proxy connection for decryption.

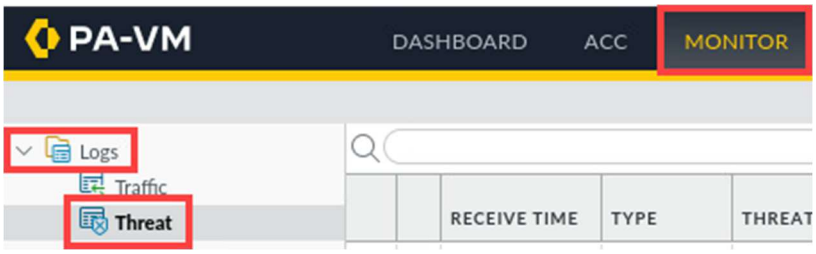
5. Click the **magnifying glass** next to the entry listed to see details about the session.



6. Note the **Decrypted** box is checked, indicating that the firewall decrypted this session. Click **Close**.



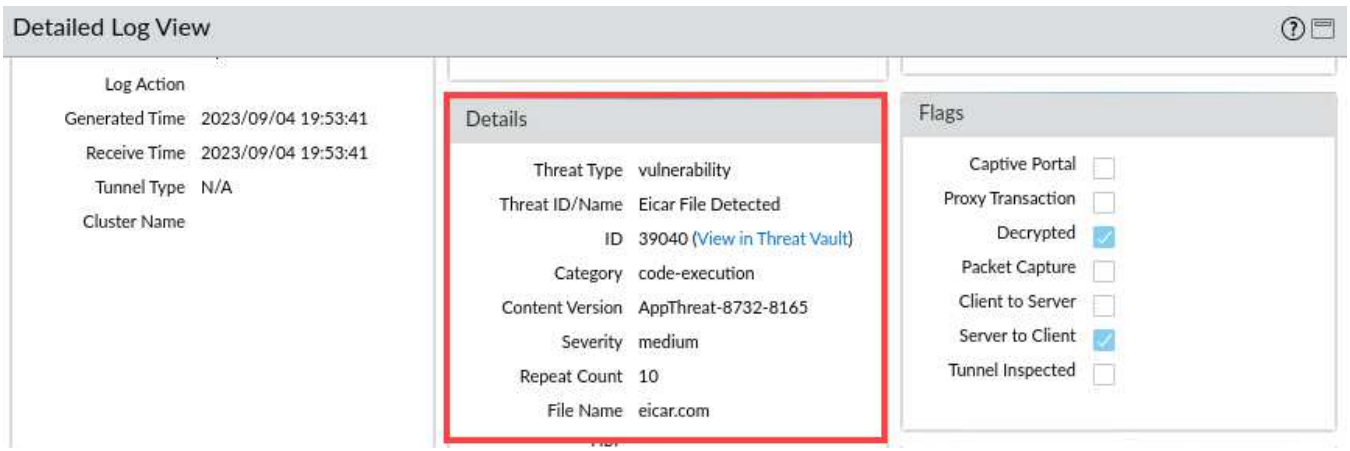
7. Select **Monitor > Logs > Threat**.



8. Add the **Decrypted** column to the table.

9. *Delete* any filters in place. Create and apply a filter called **(flags has proxy)**. Click the **magnifying glass** icon next to the entry for *vulnerability*.

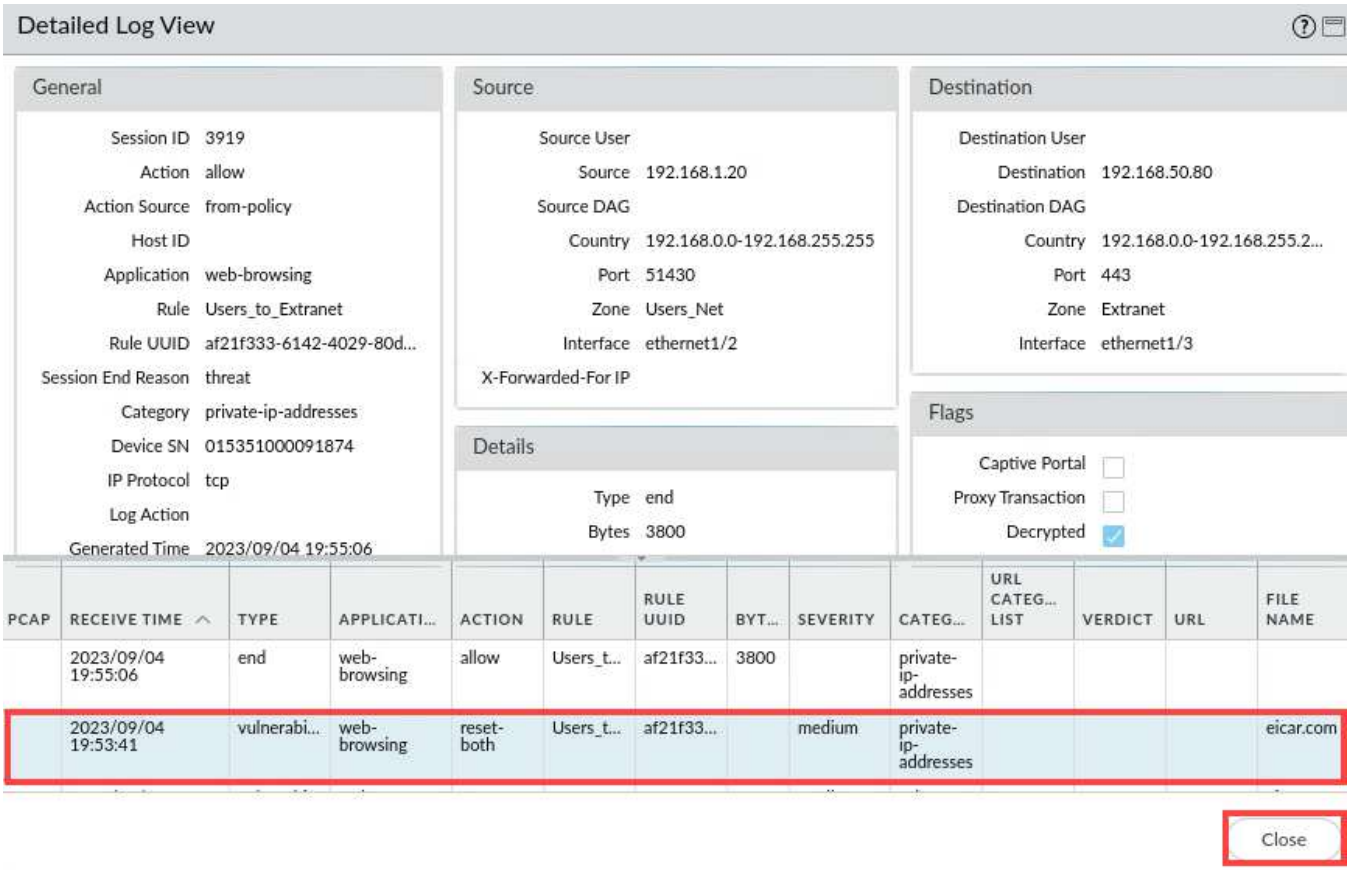
10. In the top portion of the window, scroll down until you can see the **Details** section in the middle column. You can see information about the file that the firewall detected and blocked.



Please Note

Note the ID number 39040 and the link **View in Threat Vault**. The ID number is a unique value assigned to each threat by Palo Alto Networks. Threat Vault is an online database maintained by Palo Alto Networks with extensive information about each threat. Access to Threat Vault requires a support account.

11. In the bottom of the window, highlight an entry with **Type vulnerability** to see more information about why the firewall terminated this connection. Click **Close**.



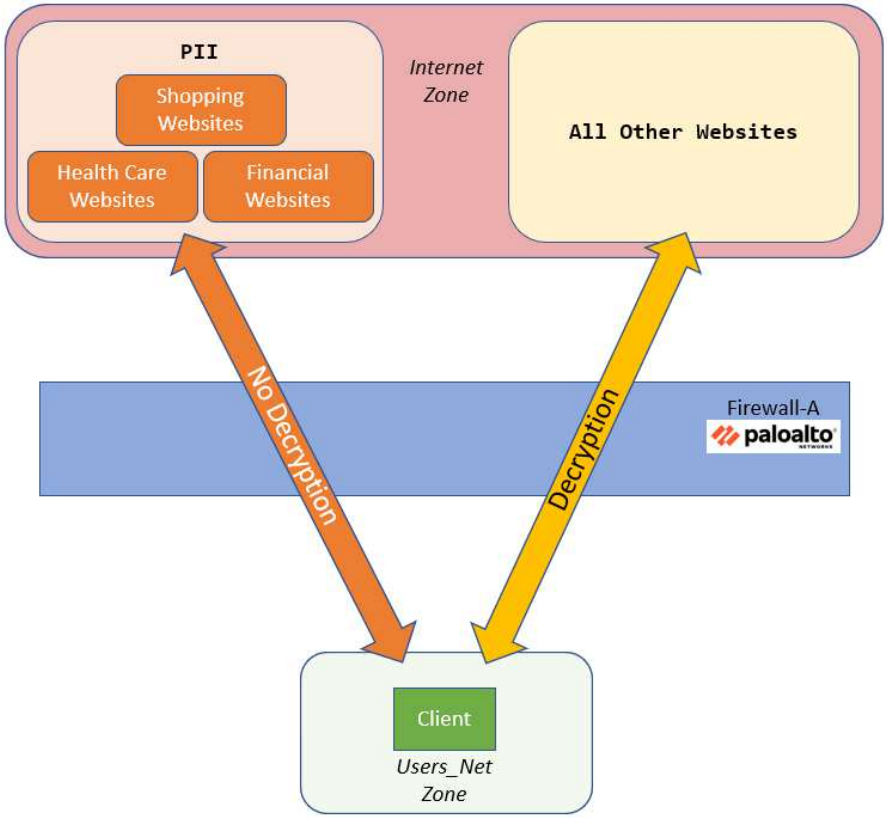
Please Note

Note that when you select the row, the information in the top half of the window changes.

12. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

2.12 Exclude URL Categories from Decryption

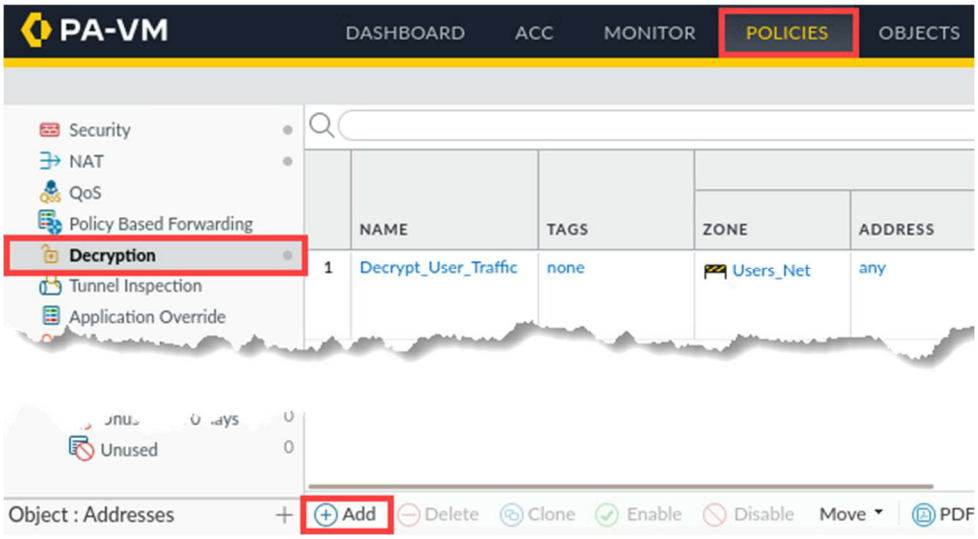
The existing Decryption policy rule you created instructs the firewall to decrypt all traffic, regardless of the URL category. In this section, you will configure a No-Decrypt rule that instructs the firewall to exclude sensitive categories of web traffic from decryption in order to avoid exposing PII (Personally Identifiable Information).



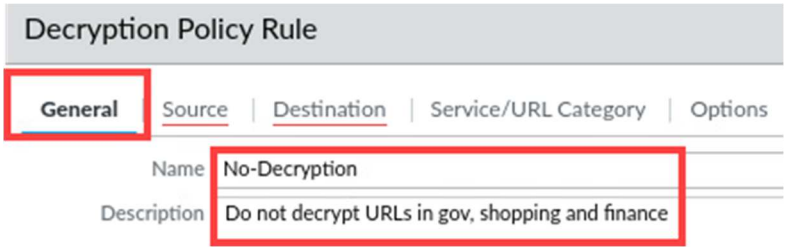
Please Note

Note that in a production environment, the URL Categories which you exclude from decryption will depend on many factors. Company policy, national privacy laws, HR concerns, destination country – all of these can dictate what types of traffic you should or should not decrypt. The examples we use here are simple ones to illustrate how to exclude URL categories from decryption.

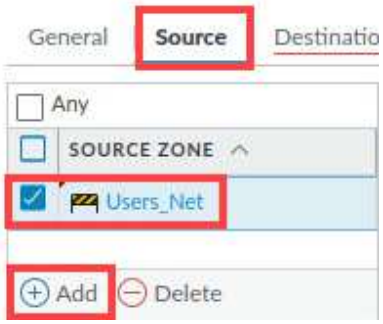
1. In the firewall web browser, select **Policies > Decryption**. Click **Add**.



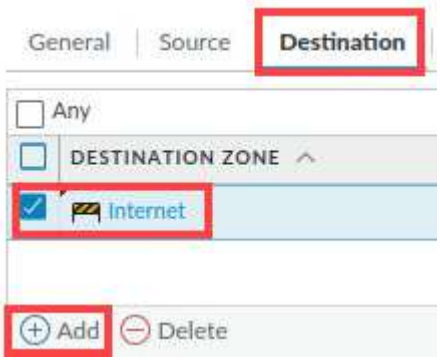
2. In the *Decryption Policy Rule* under the *General* tab, enter **`No-Decryption`** for Name. For *Description*, enter **`Do not decrypt URLs in gov, shopping and finance`**.



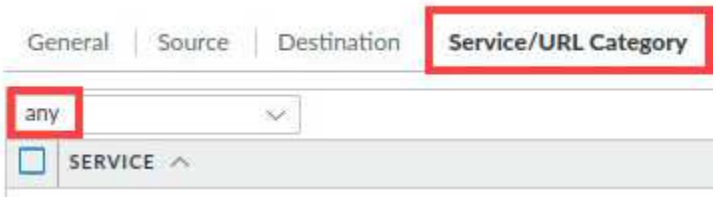
3. Select the tab for **Source.** Under the *Source Zone* section, click **Add** and select **Users_Net**.



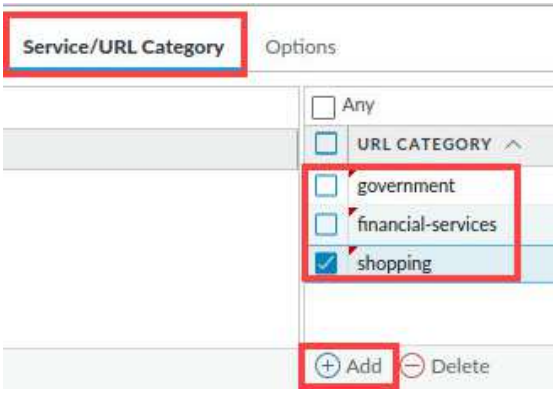
4. Select the **Destination** tab. Under the *Destination Zone* section, click **Add** and select **Internet**.



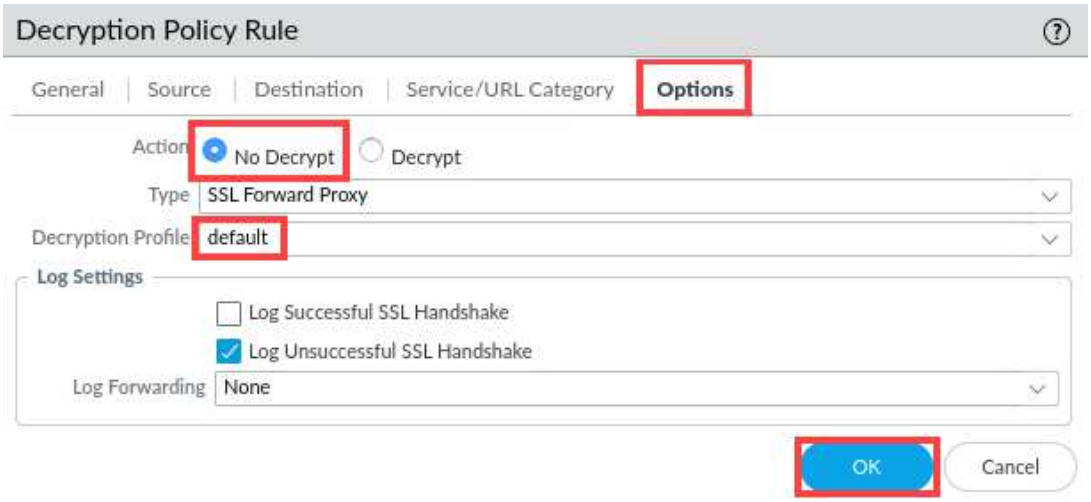
5. Select the tab for **Service/URL Category.** Leave the **Service** set to **any**.



6. Under the *URL Category*, use the **Add** button to add **government, financial-services,** and **shopping**.



7. Select the tab for **Options.** Verify that the *Action* is set to **No Decrypt**. Set the *Decryption Profile* to **default** and click **OK**.



8. You should have two entries in the *Decryption* policy. Do you notice what is wrong with the Decryption Policies?

	NAME	Source ZONE	Destination ZONE	URL CATEGORY	SERVICE	ACTION
1	Decrypt_User_Traffic	Users_Net	Extranet Internet	any	any	decrypt
2	No-Decryption	Users_Net	Internet	financial-services government shopping	any	no-decrypt

Q1. Is there anything wrong with these Decryption Policy rules?

a. Yes - The rules are in the wrong order, causing all traffic to match the first rule Decrypt_Users_Traffic due to the 'any' URL category setting. Consequently, the firewall will never proceed beyond this first rule to enforce the second rule, which is designed to exclude financial-services, government, and shopping websites from decryption.

b. No – There is nothing wrong with these Decryption Policy Rules. Therefore, the firewall will proceed with the first rule.

9. Drag and drop the **No-Decryption** rule entry above the **Decrypt_User_Traffic**.

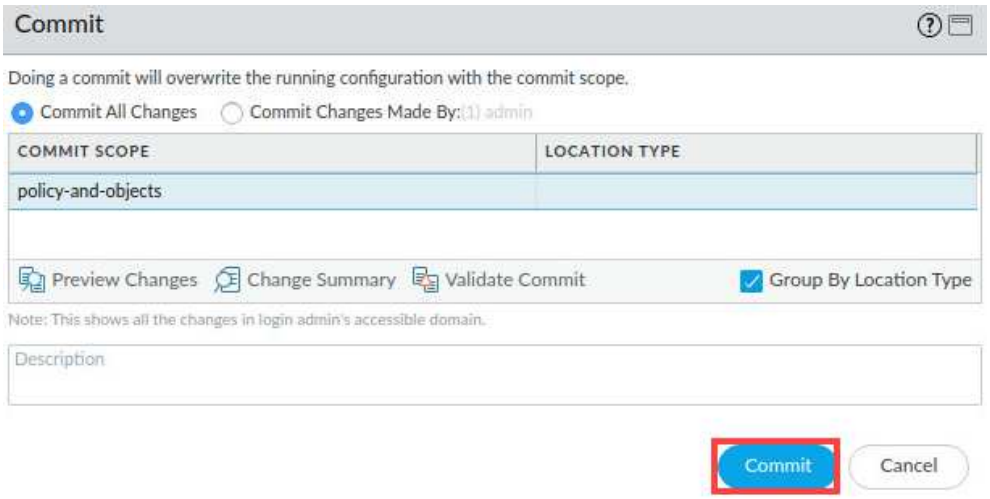
		Source	Destination				
	NAME	ZONE	ZONE	URL CATEGORY	SERVICE	ACTION	TYPE
1	No-Decryption	Users_Net	Internet	financial-services government shopping	any	no-decrypt	ssl-forward-proxy
2	Decrypt_User_Traffic	Users_Net	Extranet Internet	any	any	decrypt	ssl-forward-proxy

Please Note

Always place no-decrypt rules at the beginning of the Decryption policy table.

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

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



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

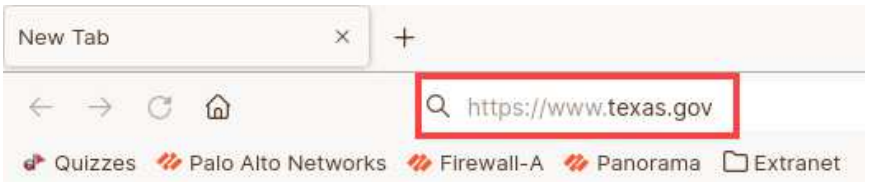
13. Close the *Firefox* browser and continue to the next task.

2.13 Test the No-Decryption Rule

With your No-Decryption rule in place, you will test the No-Decryption rule by browsing to a website which falls into one of the excluded categories.

1. On the client desktop, open the **Firefox Web Browser** application.

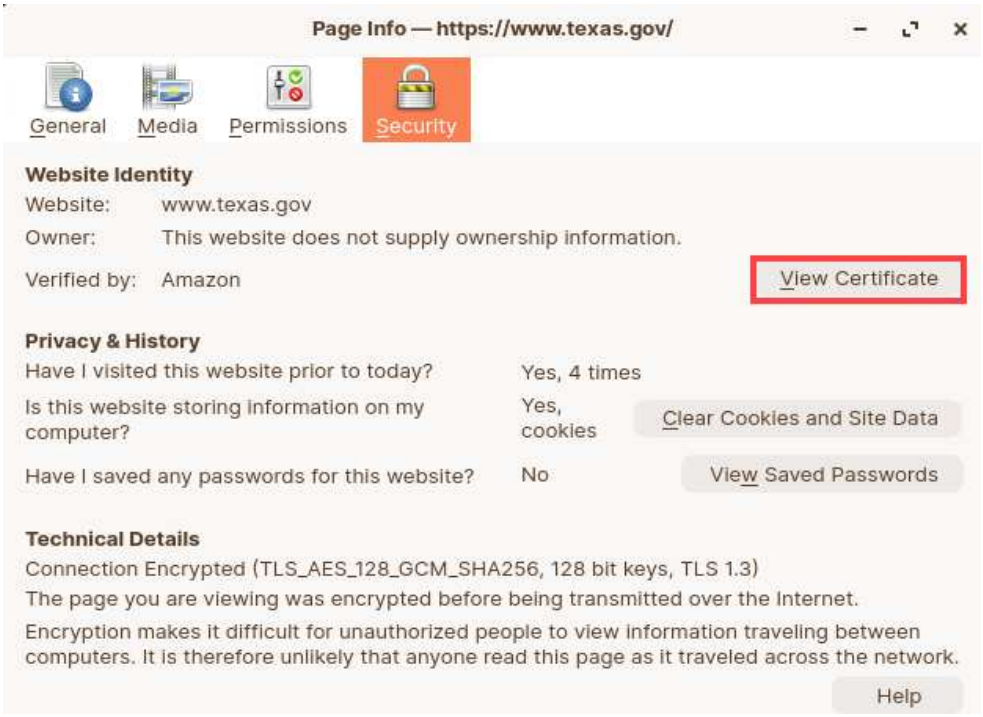
2. In a new Firefox tab, type **`https://www.texas.gov`** and press **Enter**.



3. Click the **padlock** icon to view the site information window for *texas.gov*. Click the **arrow** next to **Connection secure**.

4. In the *Connection Security for www.texas.gov* window, click **More Information**.

5. In the *Page Info – https://www.texas.gov* window, click **View Certificate**.



6. Note that the Issuer Name is *not* **192.168.1.1**.

Please Note

If the firewall had decrypted this website, the Issuer Name would be displayed as 192.168.1.1. Because you excluded government websites from Decryption, the firewall has not decrypted this site. The issuer name you see may be different from the example shown here.

7. The lab is now complete; you may end your reservation.