PALO ALTO NETWORKS EDU 210

Lab 13: Blocking Threats in Encrypted Traffic

Document Version: 2021-09-27

Contents

Introduction

As a network security professional, you have noticed a dramatic increase in HTTPS secure traffic over the past few years. Correspondingly, you have noticed that very few websites even use unencrypted HTTP traffic any more. 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 request a decryption certificate from a CA (certificate authority). However, you can generate a self-signed certificate on the Palo Alto Networks firewall and deploy that for decryption.

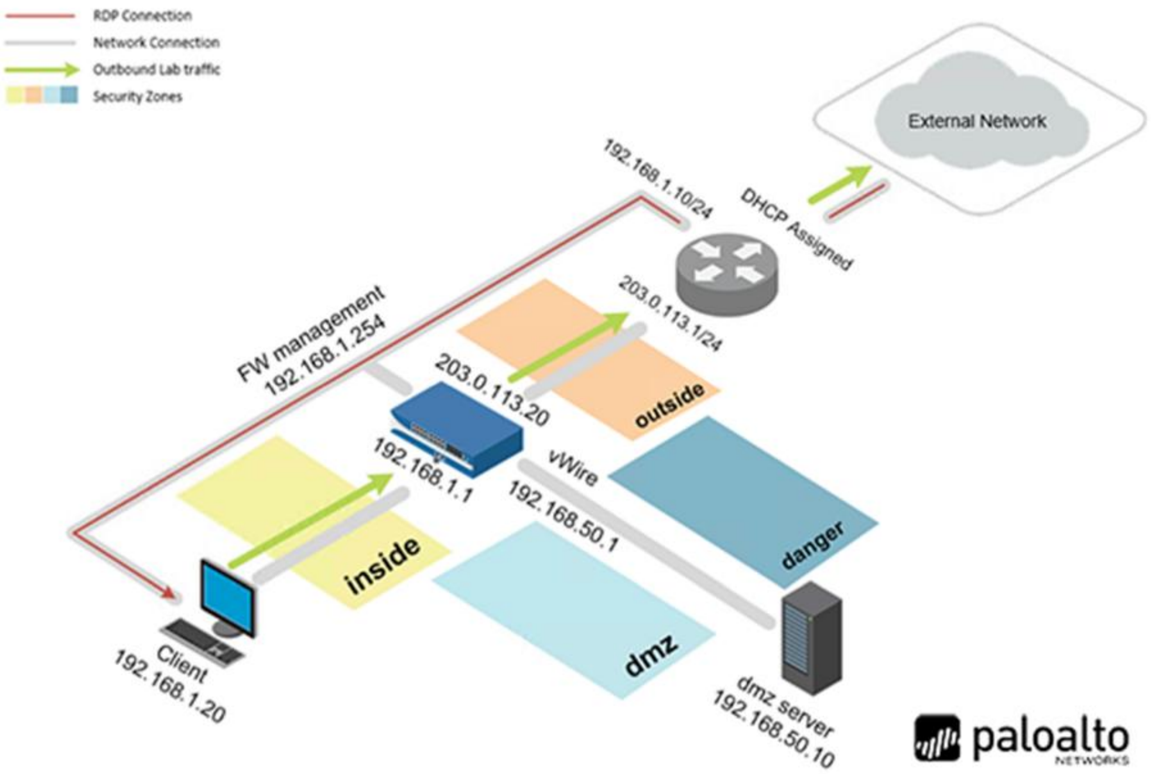
HR has also told you that there are certain types of traffic from employees that should not be decrypted because those transactions might contain personally identifiable information (PII). You need to exclude certain categories of websites (such as finance and healthcare) from decryption. You will create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

Objective

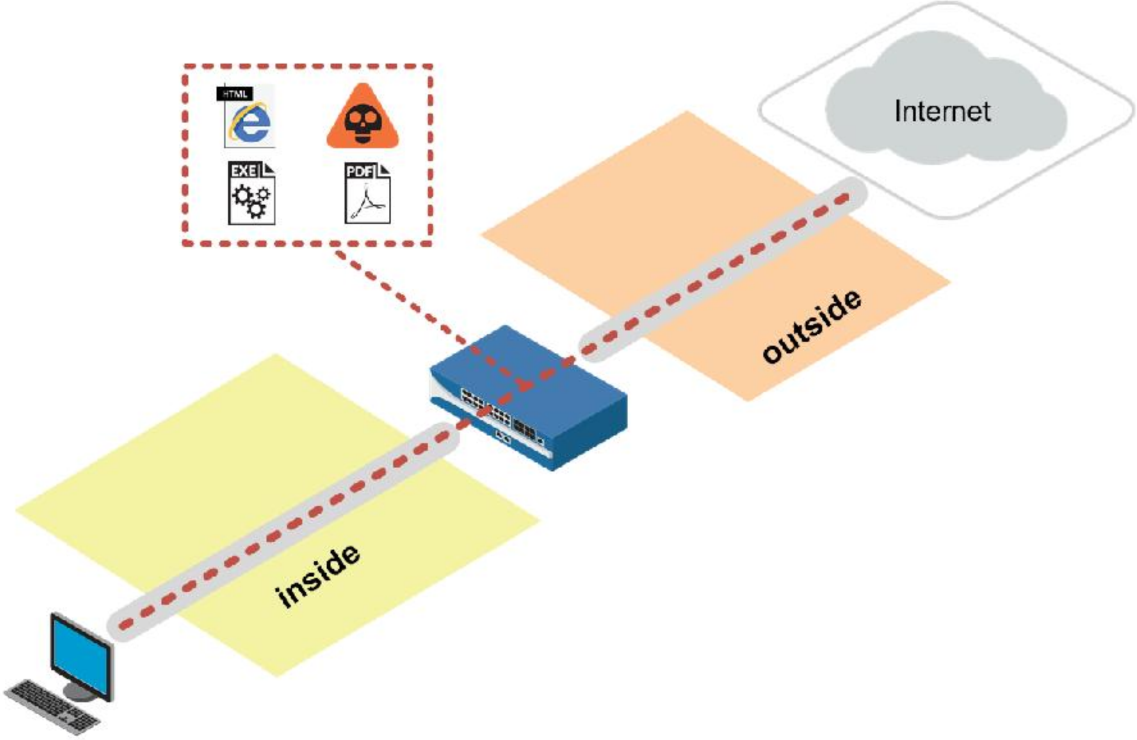
In this lab, you will perform the following tasks:

- Load a lab configuration
- Test the firewall without decryption
- Create a self-signed certificate for trusted connections
- Create a self-signed certificate 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 to complete the lab. The task sections below provide details on the use of this information.

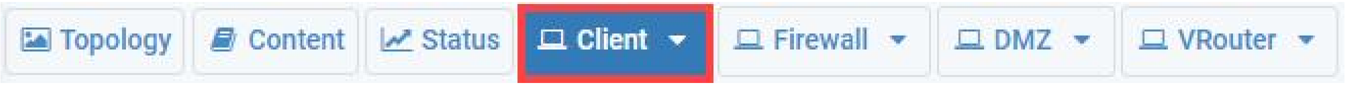
Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Client	192.168.1.20	lab-user	**Pal0Alt0!**
DMZ	192.168.50.10	root	**Pal0Alt0!**
Firewall	192.168.1.254	admin	**Pal0Alt0!**
VRouter	192.168.1.10	root	**Pal0Alt0!**

13 Blocking Threats in Encrypted Traffic

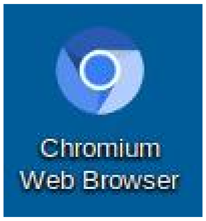
13.1 Apply a Baseline Configuration to the Firewall

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

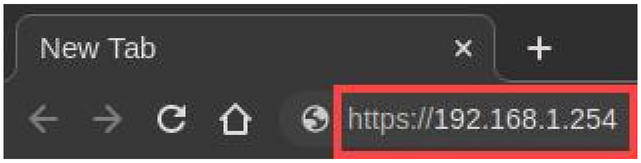
1. Click on the **Client** tab to access the *Client PC*.



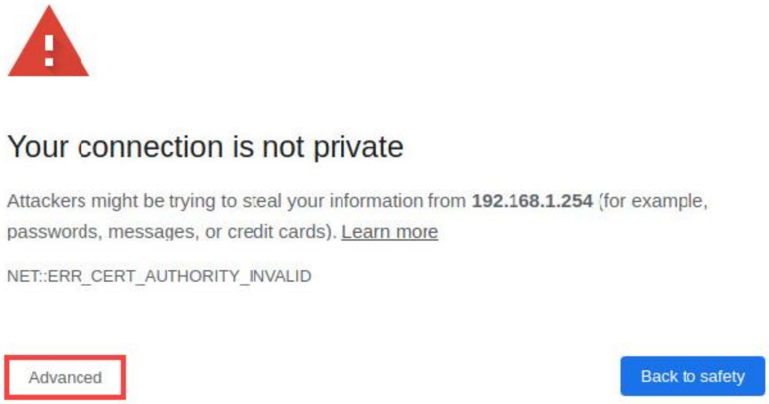
2. Double-click the **Chromium Web Browser** icon located on the *desktop*.



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



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



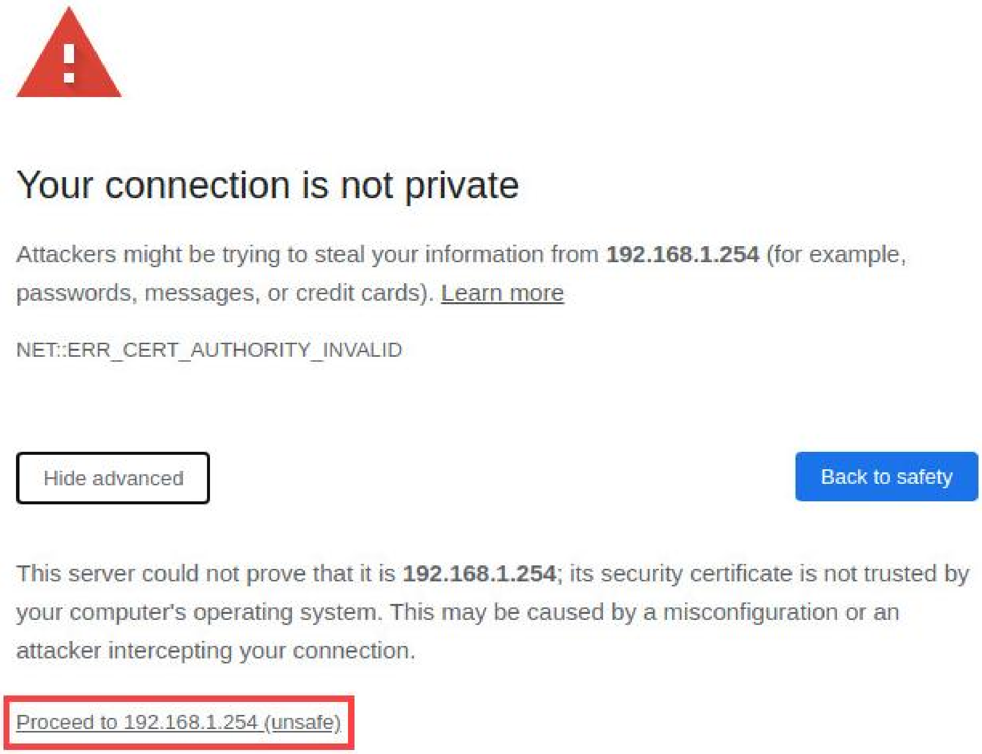
Your connection is not private

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

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.

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



Your connection is not private

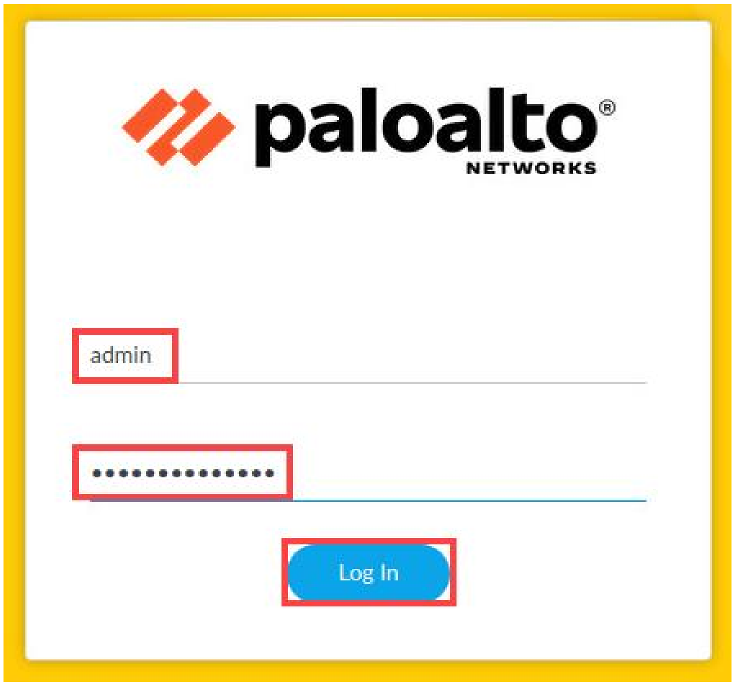
Attackers might be trying to steal your information from **192.168.1.254** (for example, passwords, messages, or credit cards). Learn more

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.

Proceed to 192.168.1.254 (unsafe)

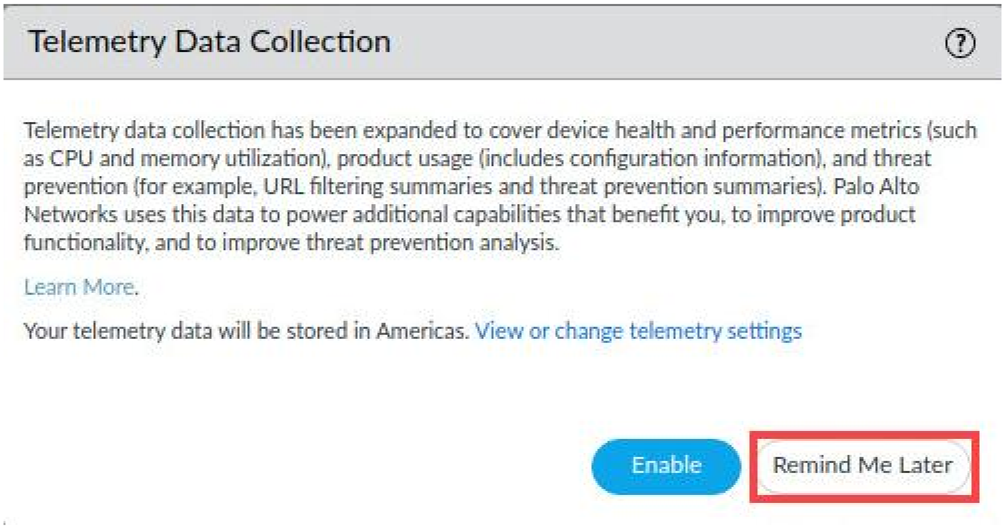
6. Log in to the firewall web interface as username **`admin`**, password **`Pal0Alt0!.`**



admin

••••••••••••••

7. In the *Telemetry Data Collection* pop-up, click **Remind Me Later**.



Telemetry Data Collection

Telemetry data collection has been expanded to cover device health and performance metrics (such as CPU and memory utilization), product usage (includes configuration information), and threat prevention (for example, URL filtering summaries and threat prevention summaries). Palo Alto Networks uses this data to power additional capabilities that benefit you, to improve product functionality, and to improve threat prevention analysis.

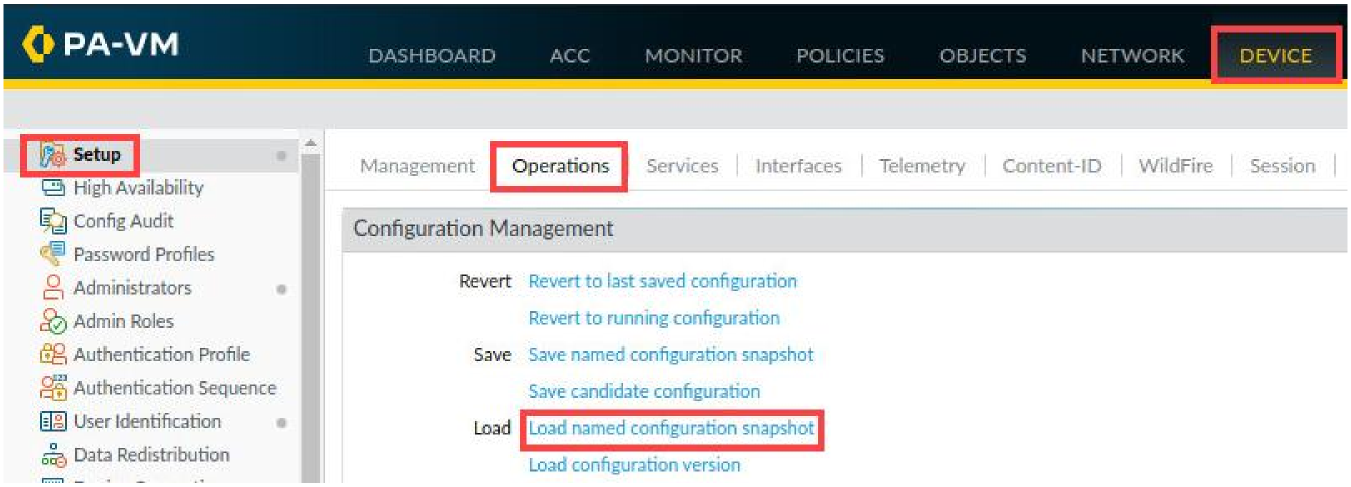
Learn More.

Your telemetry data will be stored in Americas. View or change telemetry settings

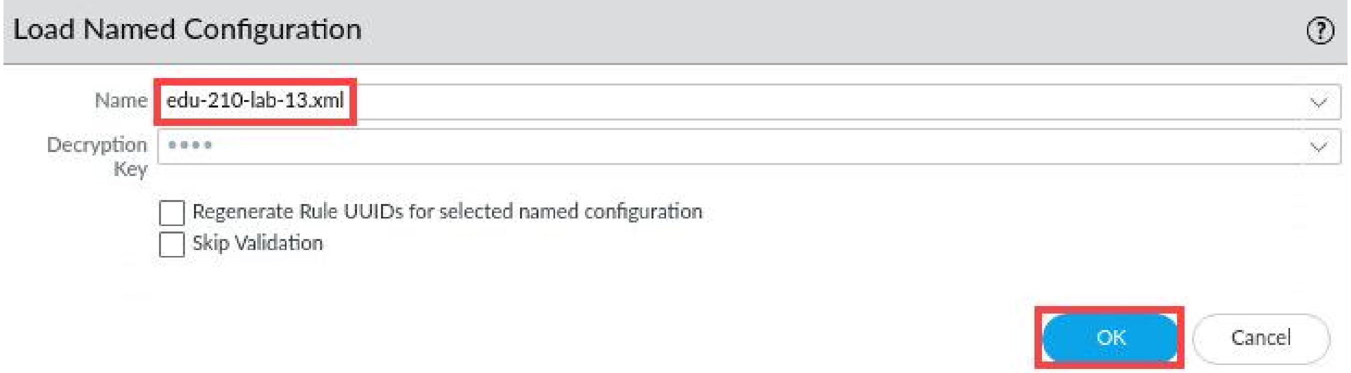
Please Note

Before you can enable Telemetry Data Collection, you would need to install a device certificate. For this lab, you will not be using Telemetry Data Collection.

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 **edu-210-lab-13.xml** from the *Name* dropdown box and click **OK**.



Load Named Configuration

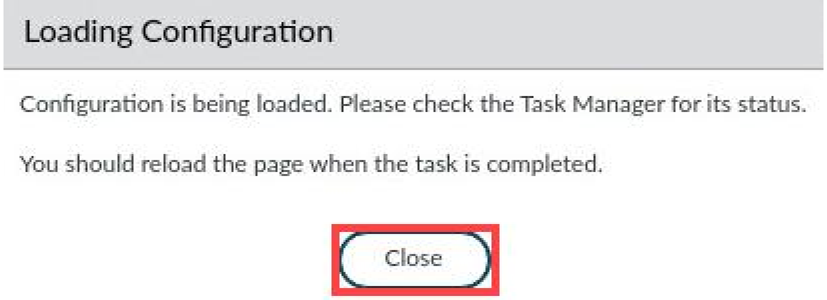
Name edu-210-lab-13.xml

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.

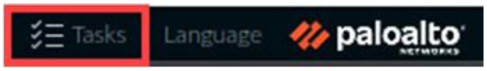


Loading Configuration

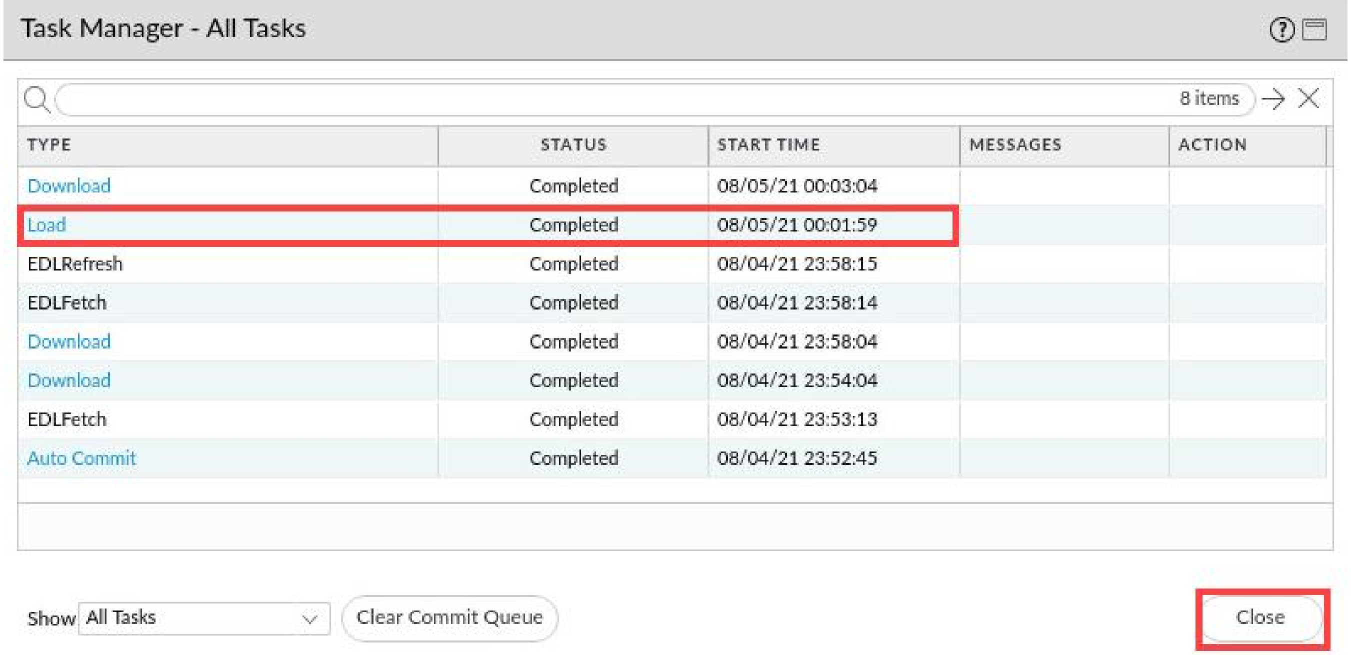
Configuration is being loaded. Please check the Task Manager for its status.

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**.

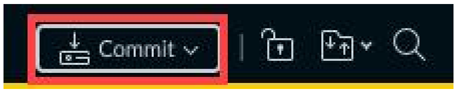


Task Manager - All Tasks

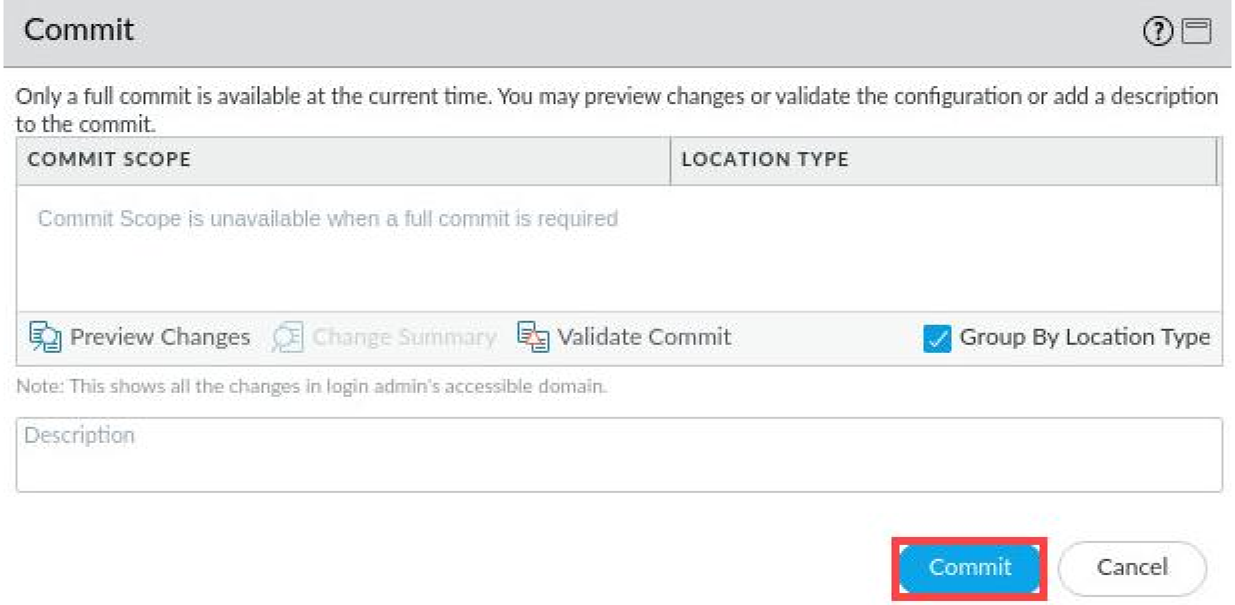
8 items

TYPE	STATUS	START TIME	MESSAGES	ACTION
Download	Completed	08/05/21 00:03:04		
Load	Completed	08/05/21 00:01:59		
EDLRefresh	Completed	08/04/21 23:58:15		
EDLFetch	Completed	08/04/21 23:58:14		
Download	Completed	08/04/21 23:58:04		
Download	Completed	08/04/21 23:54:04		
EDLFetch	Completed	08/04/21 23:53:13		
Auto Commit	Completed	08/04/21 23:52:45		

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.



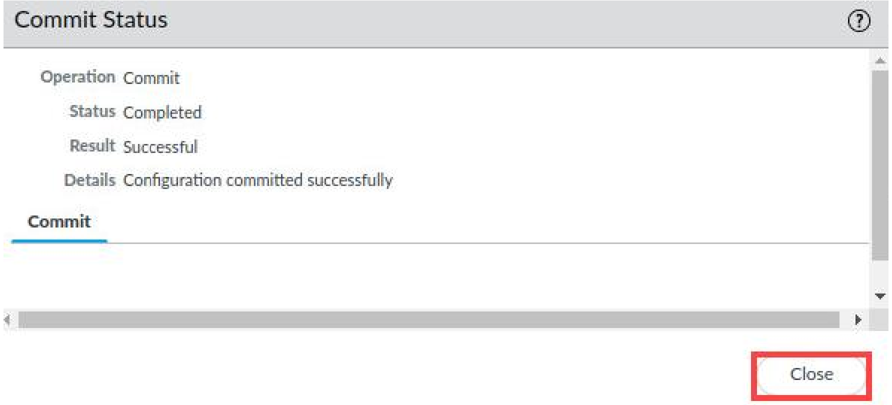
Commit

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

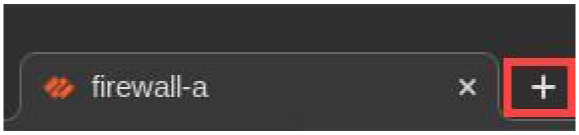
The commit process takes changes made to the Firewall and copies them to the running configuration, which will activate all configuration changes since the last commit.

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

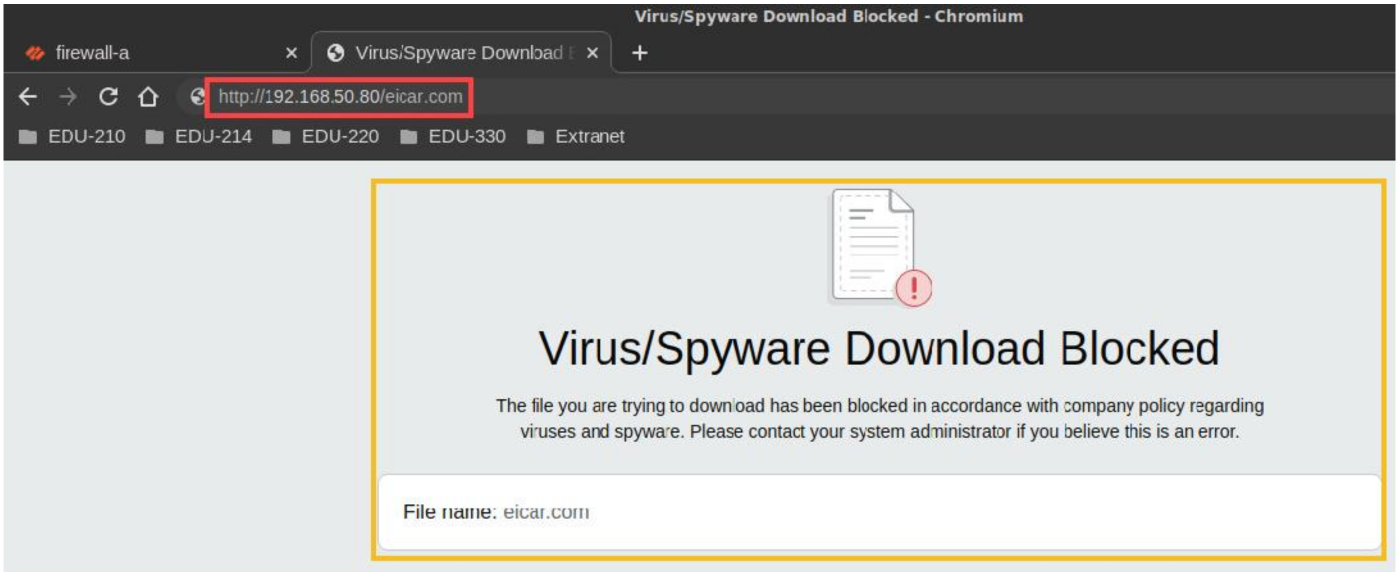
13.2 Test the Firewall Behavior Without Decryption

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

1. Open a new tab in **Chromium**.



2. Type **`http://192.168.50.80/eicar.com`** and press **Enter**. You should get a blocked page.


Virus/Spyware Download Blocked - Chromium
firewall-a
Virus/Spyware Download E
http://192.168.50.80/eicar.com
EDU-210
EDU-214
EDU-220
EDU-330
Extranet

Virus/Spyware Download Blocked

The file you are trying to download has been blocked in accordance with company policy regarding viruses and spyware. Please contact your system administrator if you believe this is an error.

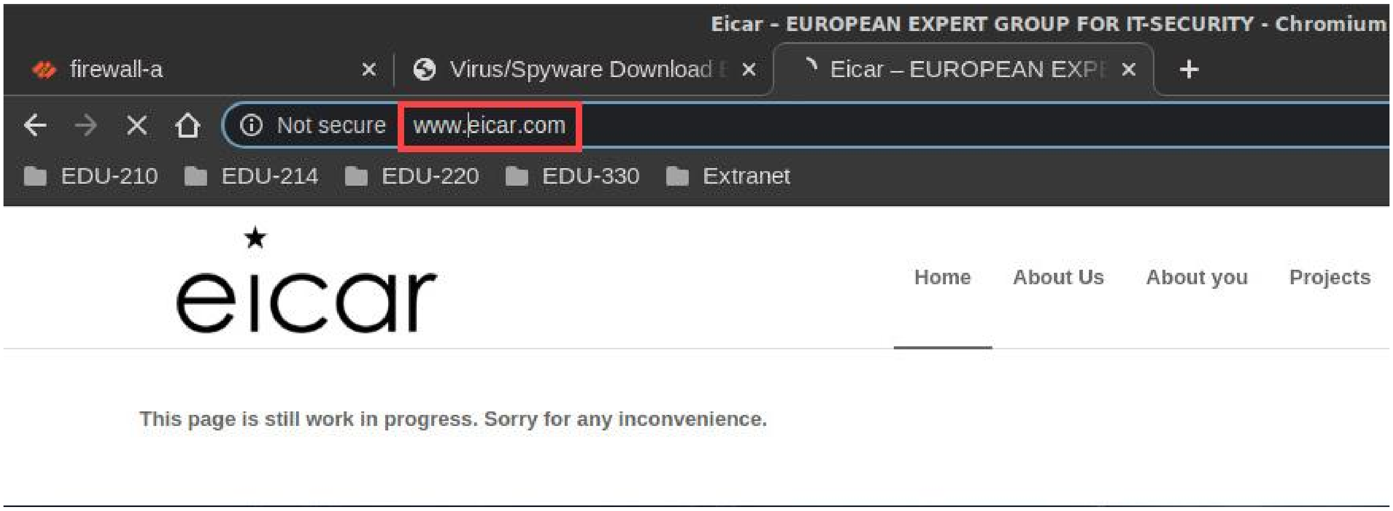
File name: eicar.com

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.

In the configuration you loaded to begin this lab, there is an Antivirus Security profile applied to security policy rules. The Antivirus profile is preconfigured and pre-applied for this exercise so that you can focus on how to configure the firewall to perform decryption. We will examine Security profiles (including Antivirus) in more detail in later sections of this course.

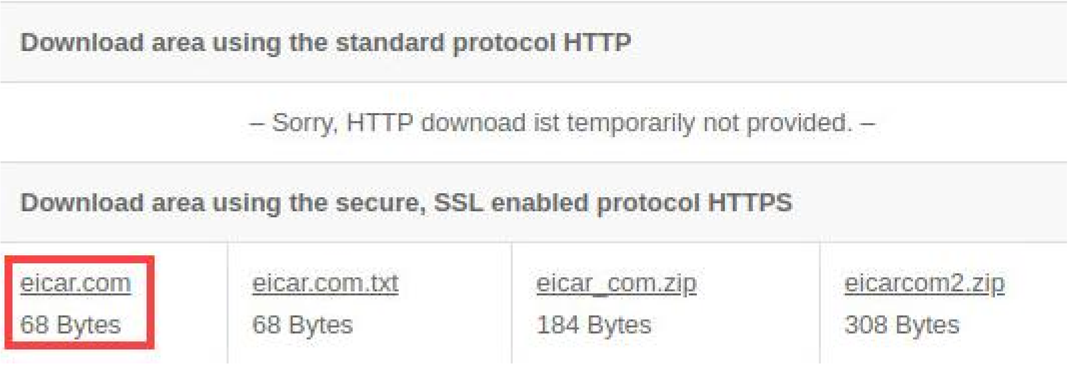
3. Open a new **Chromium** tab, type **`www.eicar.com`**.



This page is still work in progress. Sorry for any inconvenience.

4. Click the link for the **Download Anti Malware Testfile**.

5. Scroll down and locate the section **Download** area. Click the link for the **eicar.com** file download.



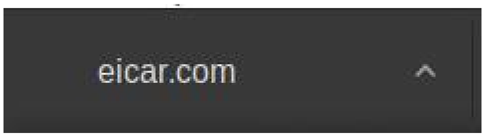
Download area using the standard protocol HTTP

– Sorry, HTTP downoad ist temporarily not provided. –

Download area using the secure, SSL enabled protocol HTTPS

eicar.com 68 Bytes	eicar.com.txt 68 Bytes	eicar_com.zip 184 Bytes	eicarcom2.zip 308 Bytes

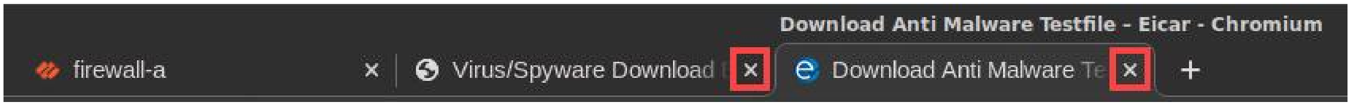
6. Notice at the bottom of the *Chromium* window that the download is not blocked because the connection is encrypted, and the virus is hidden. This exercise proves that without decryption, the firewall is unable to examine the contents of a secure connection to scan for malicious content.



Please Note

You can also verify the eicar.com file was successfully downloaded by viewing the downloads folder.

7. Close the two *Chromium* tabs that you just opened.


Download Anti Malware Testfile - Eicar - Chromium
firewall-a ×
Virus/Spyware Download ×
Download Anti Malware Te ×
+

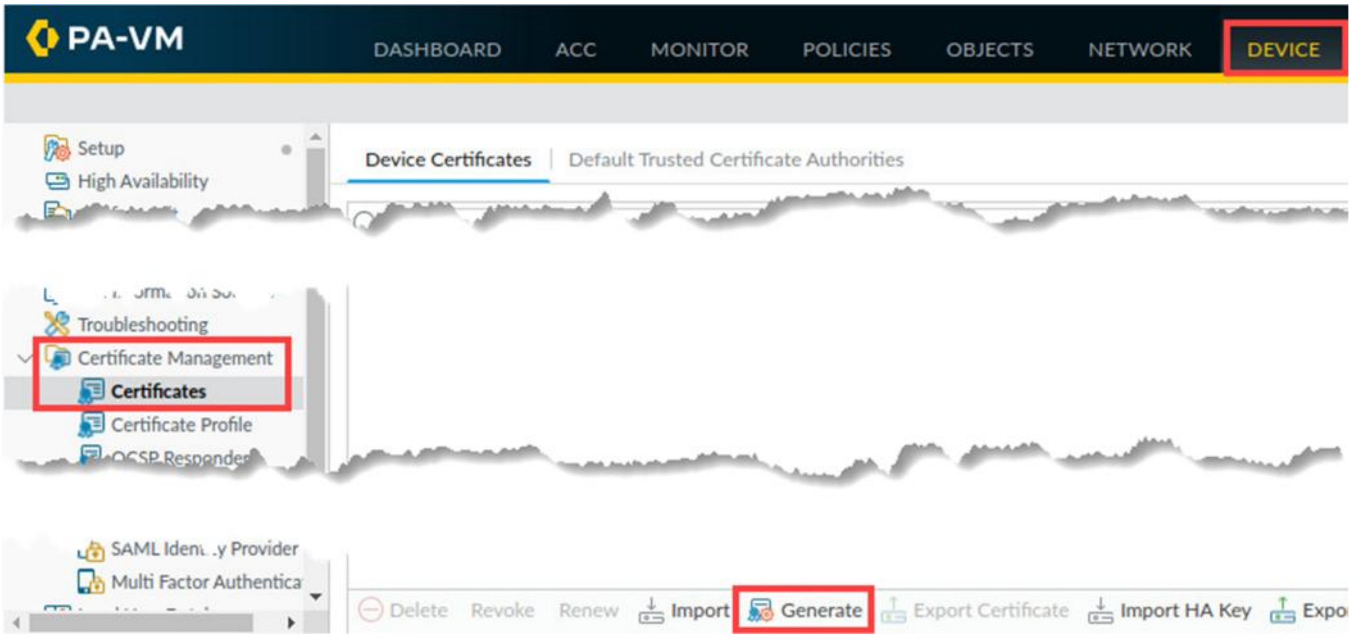
8. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

13.3 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.

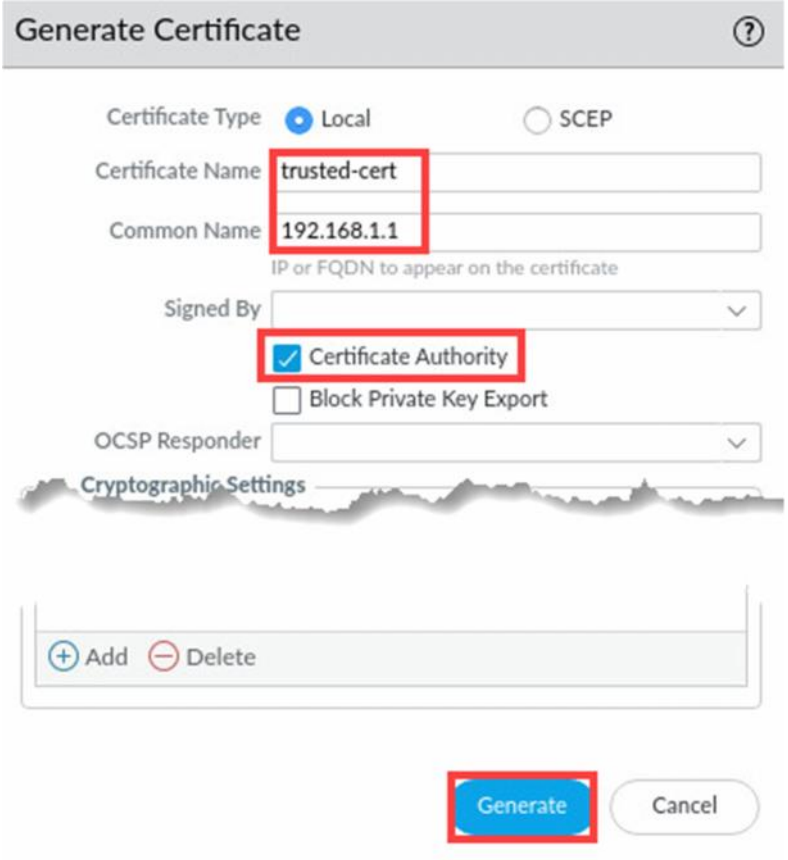
The firewall will use this certificate as part of the decryption process between clients and trusted HTTPS websites.

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**



Generate Certificate

Certificate Type ● Local ○ SCEP

Certificate Name trusted-cert

Common Name 192.168.1.1

IP or FQDN to appear on the certificate

Signed By

☑ Certificate Authority

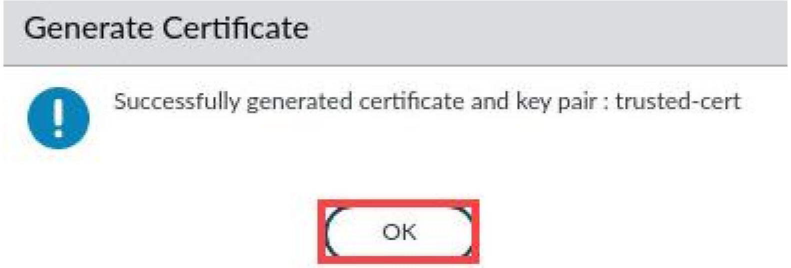
□ Block Private Key Export

OCSP Responder

Cryptographic Settings

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

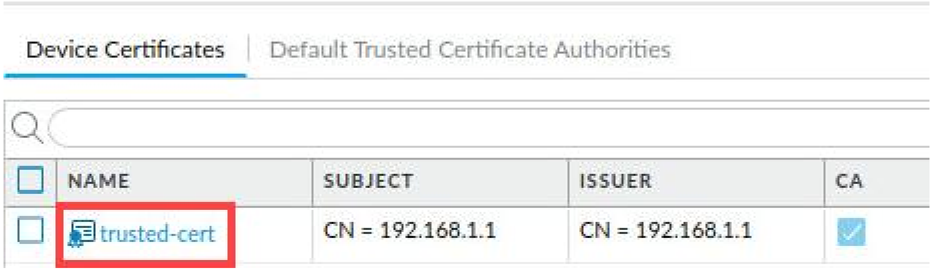
3. In the *Generate Certificate* window, click **OK**.



Generate Certificate

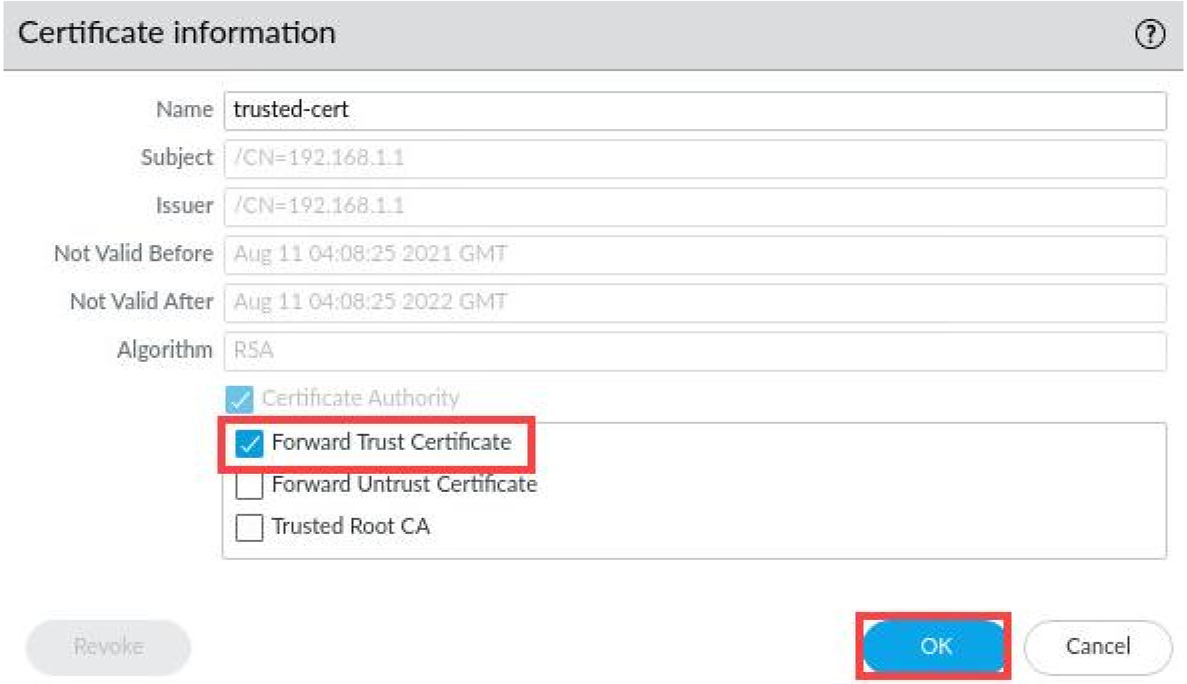
Successfully generated certificate and key pair : trusted-cert

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



☐	NAME	SUBJECT	ISSUER	CA
☐	trusted-cert	CN = 192.168.1.1	CN = 192.168.1.1	☑

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



Name: trusted-cert
Subject: /CN=192.168.1.1
Issuer: /CN=192.168.1.1
Not Valid Before: Aug 11 04:08:25 2021 GMT
Not Valid After: Aug 11 04:08:25 2022 GMT
Algorithm: RSA

☑ Certificate Authority
☑ Forward Trust Certificate
☐ Forward Untrust Certificate
☐ Trusted Root CA

Please Note

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

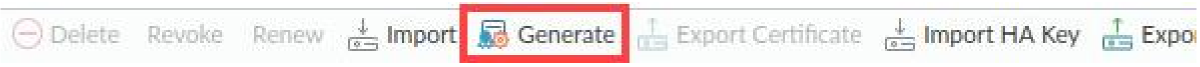
6. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

13.4 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.

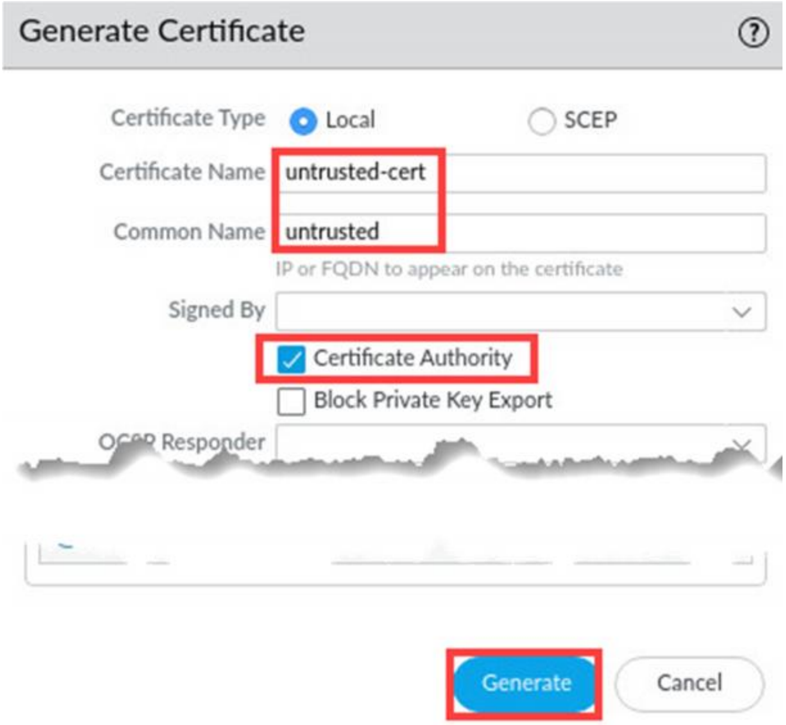
The firewall will use this certificate as part of the decryption process between clients and untrusted HTTPS websites.

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	`untrusted`
Certificate Authority	**Certificate Authority**



Generate Certificate

Certificate Type ● Local ○ SCEP

Certificate Name untrusted-cert

Common Name untrusted

IP or FQDN to appear on the certificate

Signed By

☑ Certificate Authority

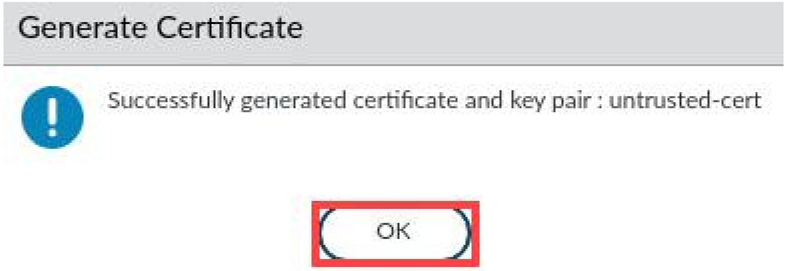
□ Block Private Key Export

OCSP Responder

Please Note

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

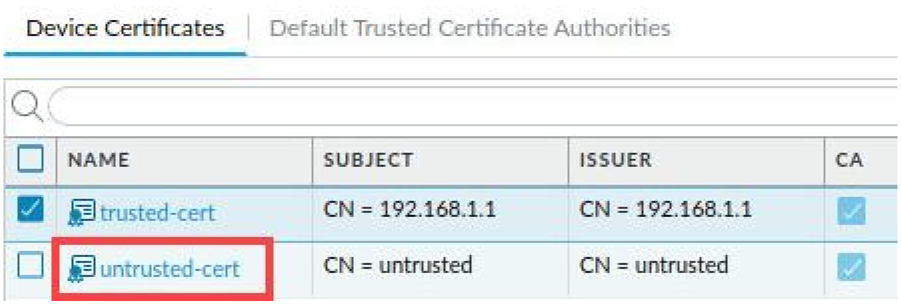
3. In the *Generate Certificate* window, click **OK**.



Generate Certificate

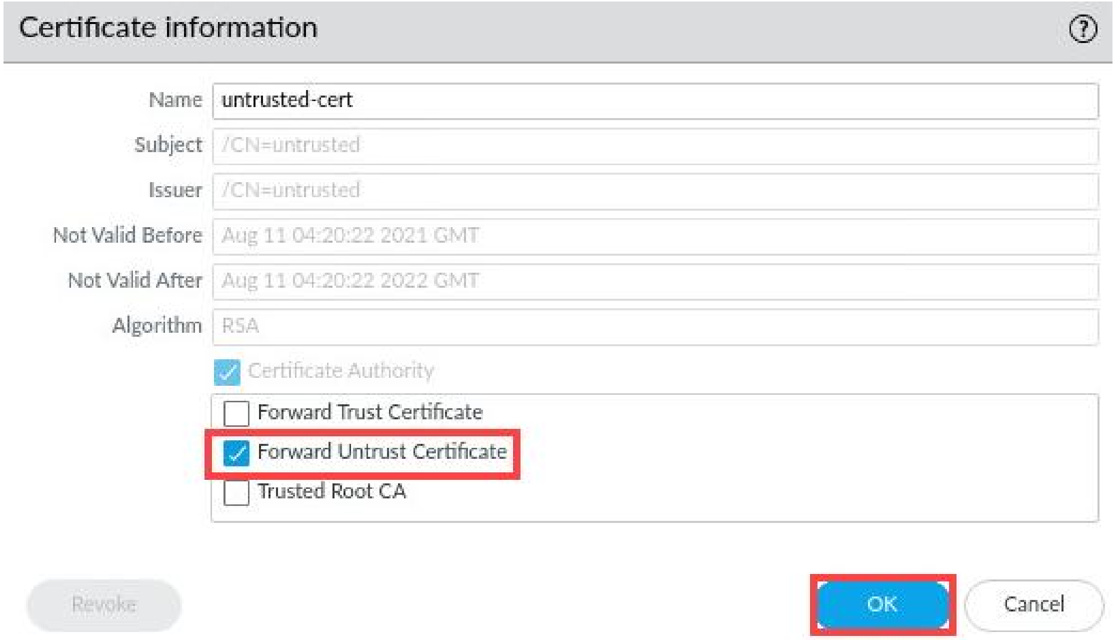
Successfully generated certificate and key pair : untrusted-cert

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



☐	NAME	SUBJECT	ISSUER	CA
☑	trusted-cert	CN = 192.168.1.1	CN = 192.168.1.1	☑
☐	untrusted-cert	CN = untrusted	CN = untrusted	☑

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


Certificate information

Name: untrusted-cert
Subject: /CN=untrusted
Issuer: /CN=untrusted
Not Valid Before: Aug 11 04:20:22 2021 GMT
Not Valid After: Aug 11 04:20:22 2022 GMT
Algorithm: RSA

☑ Certificate Authority

☐ Forward Trust Certificate
☑ Forward Untrust Certificate
☐ Trusted Root CA

Please Note

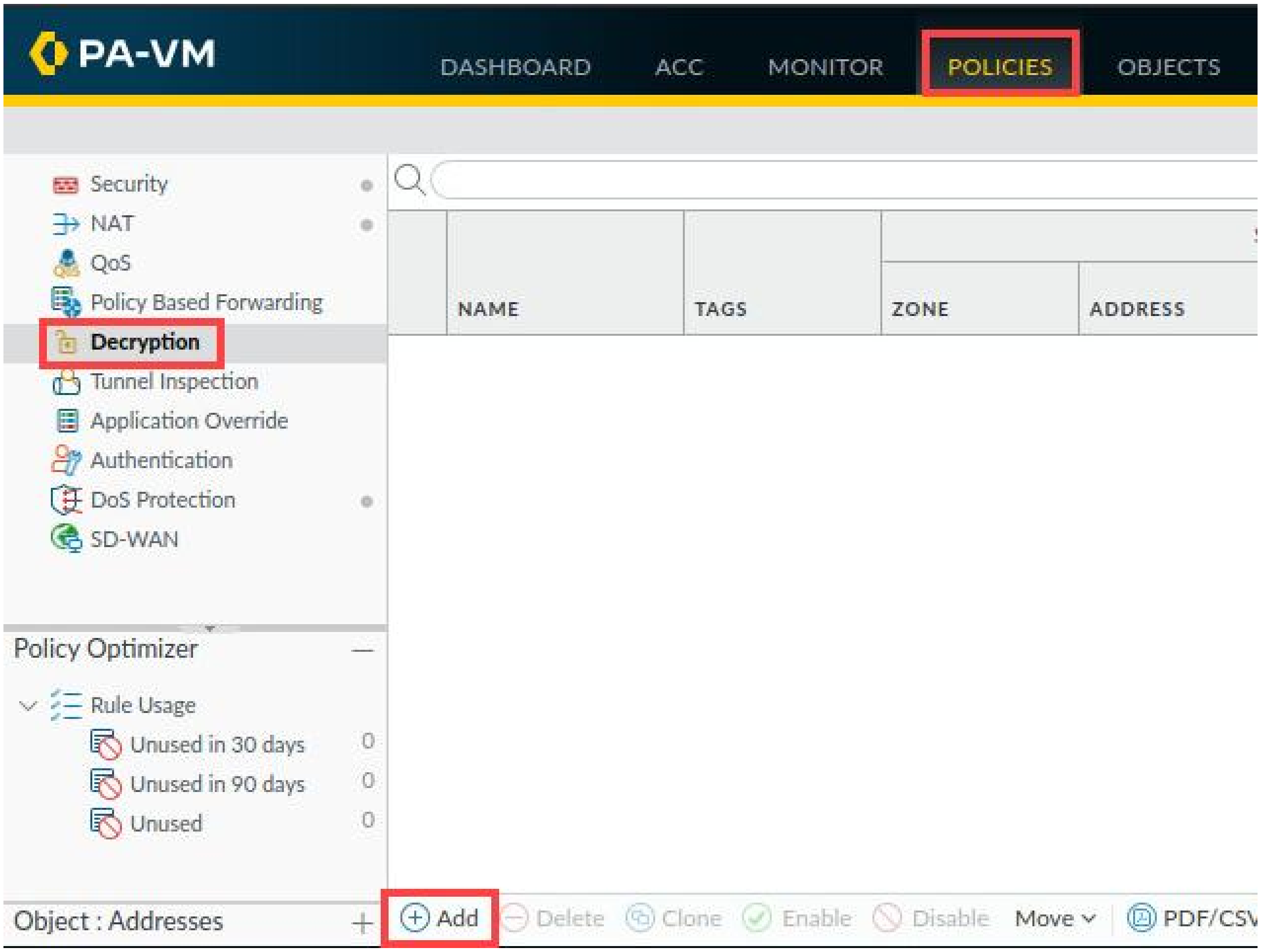
This action instructs the firewall to use this certificate to decrypt traffic between clients and HTTPS sites that are not trustworthy (expired certificates, self-signed certificates, etc.).

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

13.5 Create Decryption Policy for Outbound Traffic

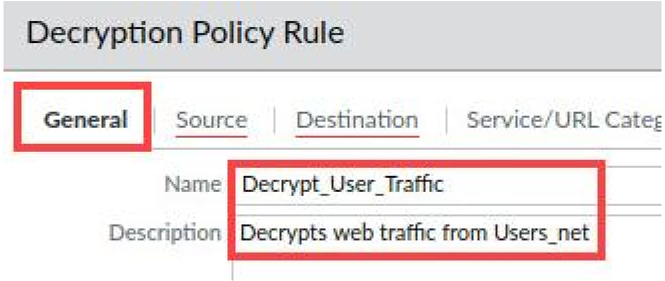
In this section, you will create a Decryption Policy to decrypt HTTPS traffic from the Users_Net security zone to the Internet security zone.

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.`**

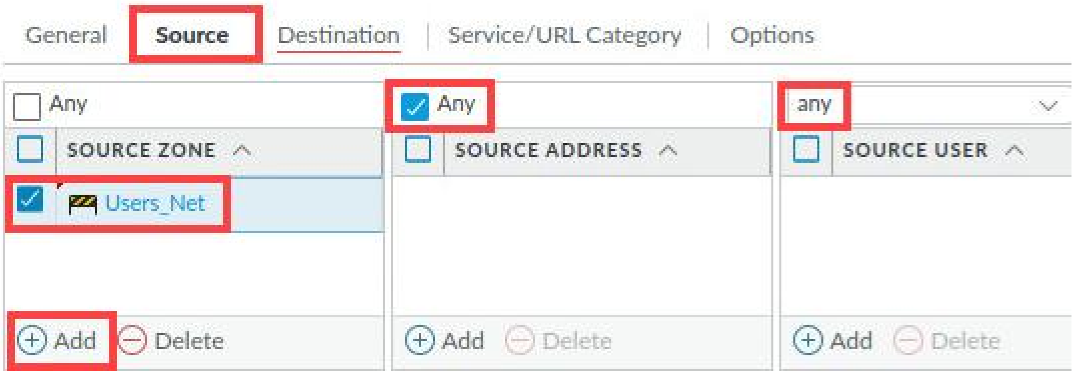

Decryption Policy Rule

Name: Decrypt_User_Traffic

Description: Decrypts web traffic from Users_net

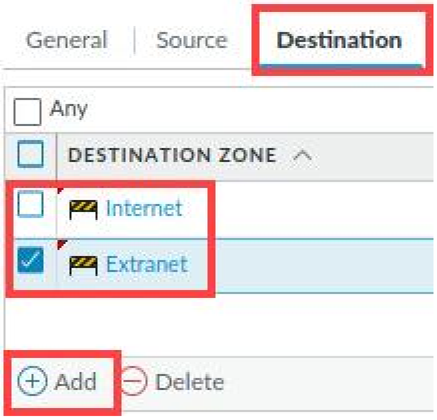
3. Click the **Source** tab and configure the following.

Parameter	Value
Source Zone	Users_Net
Source Address	Any
Source User	any

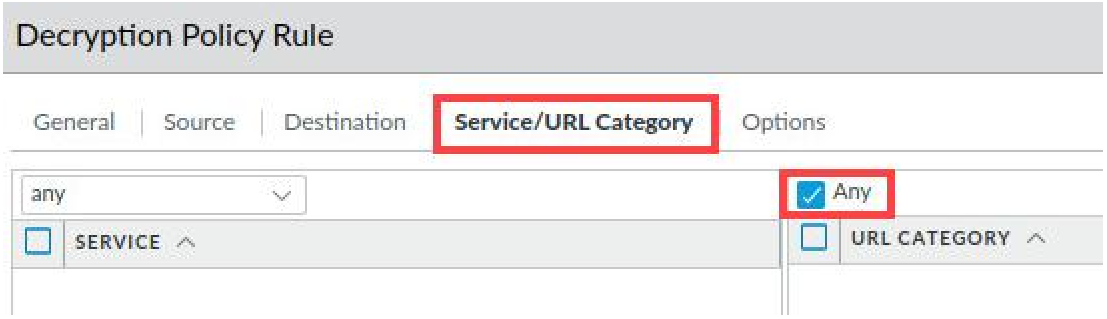


4. Click the **Destination** tab and configure the following.

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**.



Decryption Policy Rule

any

☐ SERVICE

☑ Any

☐ URL CATEGORY

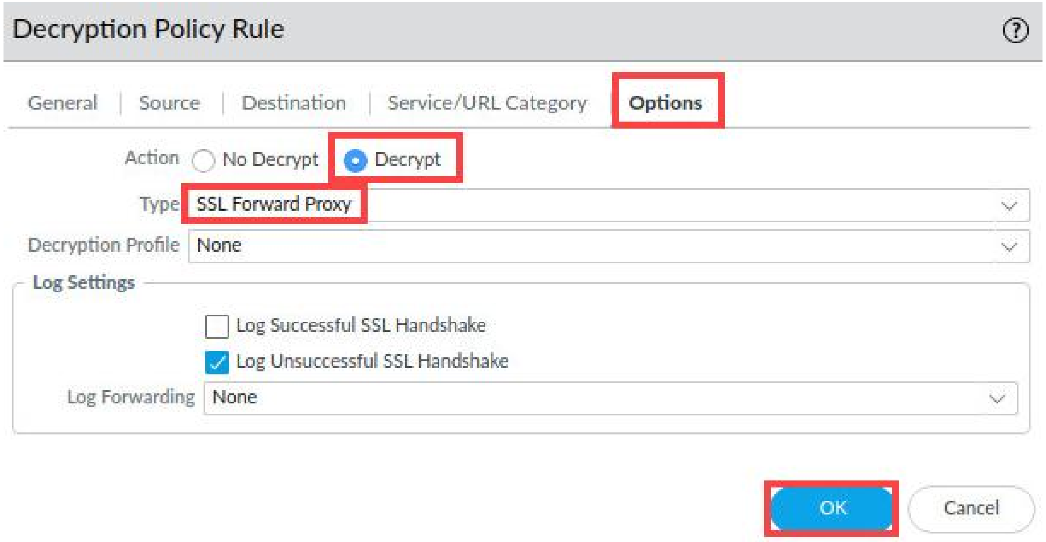
Please Note

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	**None**



Decryption Policy Rule

Action ○ No Decrypt ● Decrypt

Type SSL Forward Proxy

Decryption Profile None

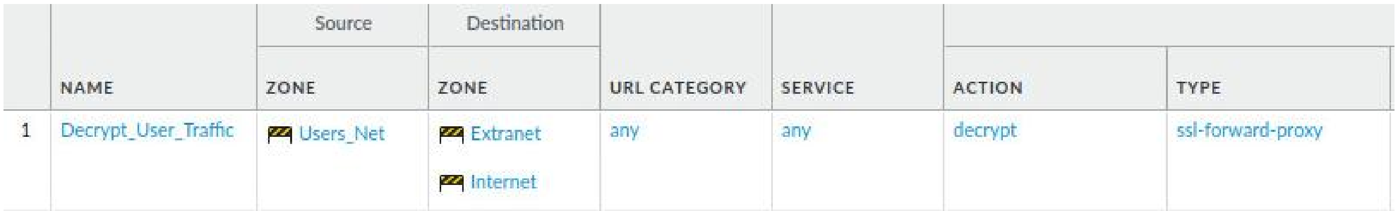
Log Settings

☐ Log Successful SSL Handshake

☑ Log Unsuccessful SSL Handshake

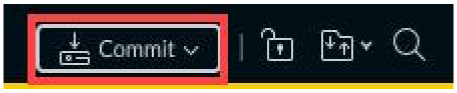
Log Forwarding None

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

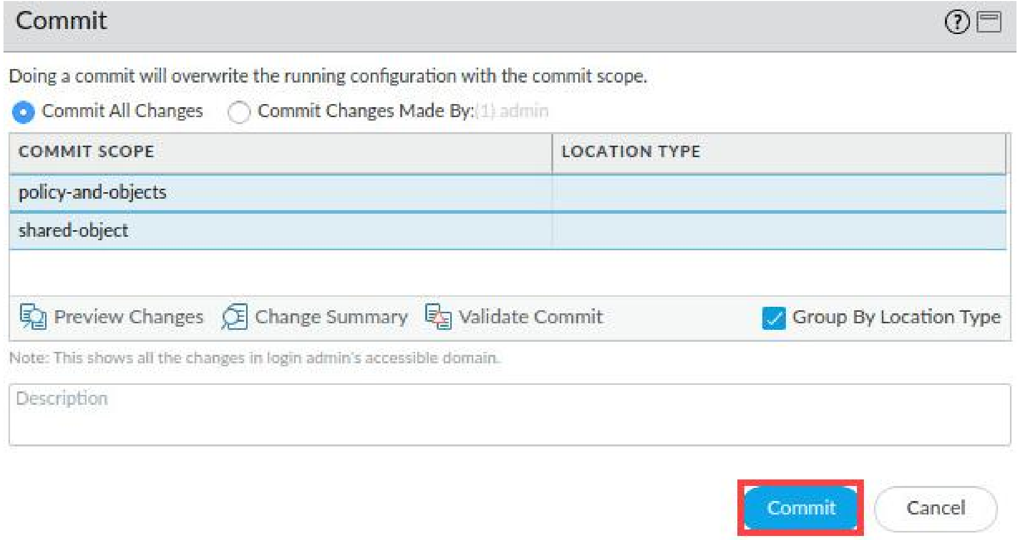


		Source	Destination				
	NAME	ZONE	ZONE	URL CATEGORY	SERVICE	ACTION	TYPE
1	Decrypt_User_Traffic	Users_Net	Extranet Internet	any	any	decrypt	ssl-forward-proxy

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.



Commit

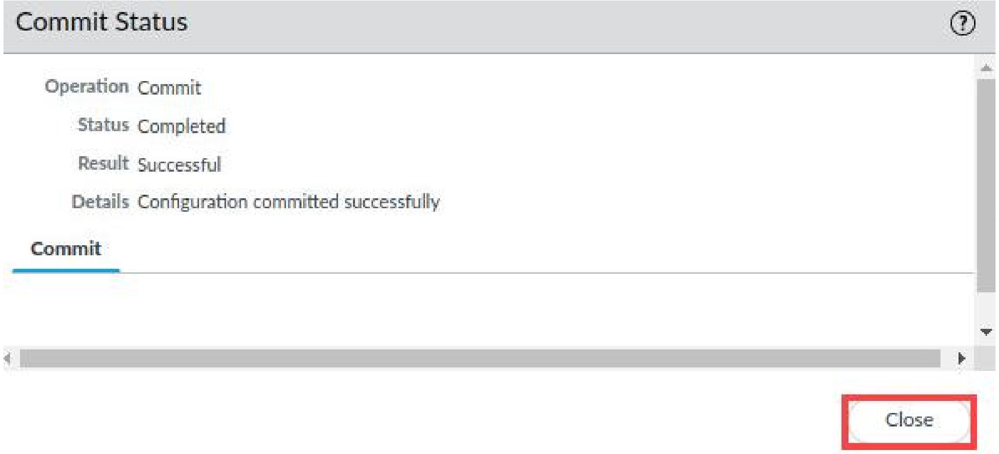
Doing a commit will overwrite the running configuration with the commit scope.

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

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

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

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



Commit Status

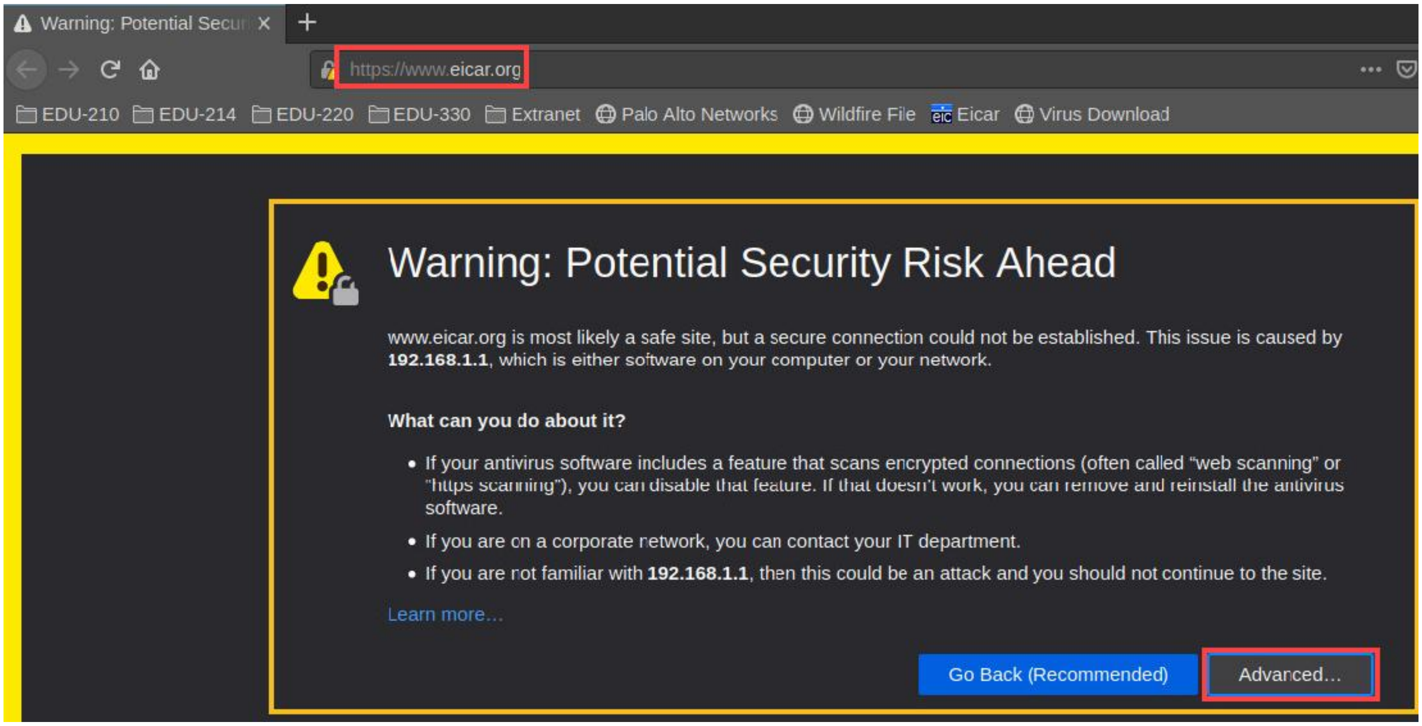
Operation Commit
Status Completed
Result Successful
Details Configuration committed successfully

13.6 Test Outbound Decryption Policy

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

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

2. Type **`https://www.eicar.org`** and press **Enter**. The browser presents a warning message. Click **Advanced**.



Warning: Potential Security Risk Ahead

www.eicar.org is most likely a safe site, but a secure connection could not be established. This issue is caused by **192.168.1.1**, which is either software on your computer or your network.

What can you do about it?

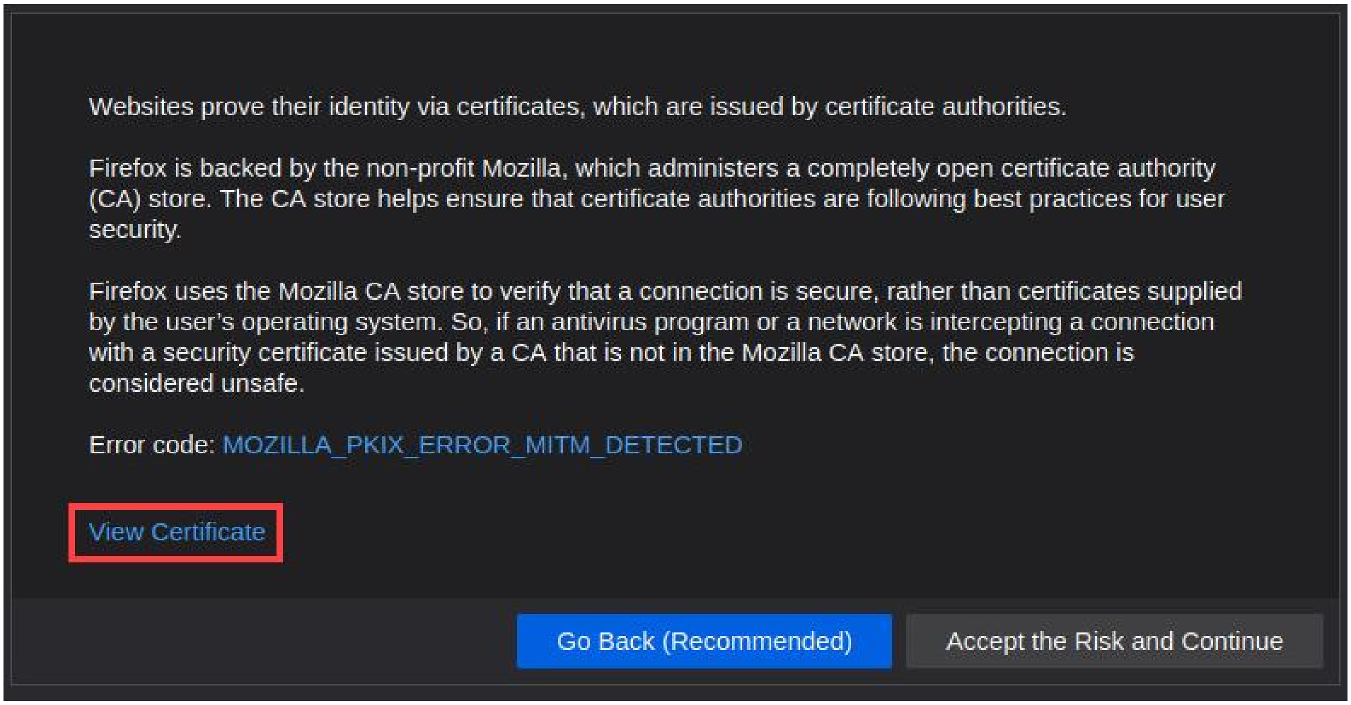
- If your antivirus software includes a feature that scans encrypted connections (often called "web scanning" or "https scanning"), you can disable that feature. If that doesn't work, you can remove and reinstall the antivirus software.
- If you are on a corporate network, you can contact your IT department.
- If you are not familiar with **192.168.1.1**, then this could be an attack and you should not continue to the site.

Learn more…

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**.



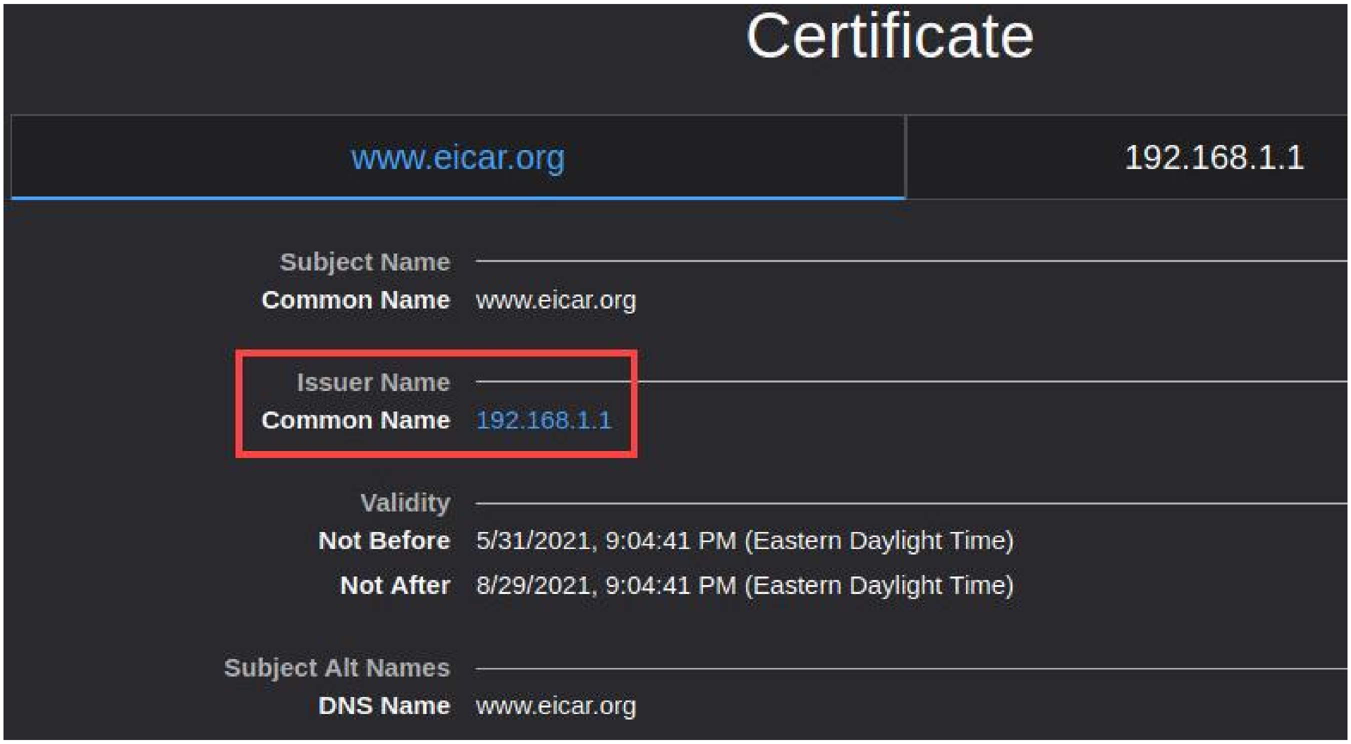
Websites prove their identity via certificates, which are issued by certificate authorities.

Firefox is backed by the non-profit Mozilla, which administers a completely open certificate authority (CA) store. The CA store helps ensure that certificate authorities are following best practices for user security.

Firefox uses the Mozilla CA store to verify that a connection is secure, rather than certificates supplied by the user's operating system. So, if an antivirus program or a network is intercepting a connection with a security certificate issued by a CA that is not in the Mozilla CA store, the connection is considered unsafe.

Error code: MOZILLA_PKIX_ERROR_MITM_DETECTED

4. Under the section for *www.eicar.org*, note the *Issuer Name* section contains **192.168.1.1**.



Certificate

Subject Name
Common Name www.eicar.org

Issuer Name
Common Name 192.168.1.1

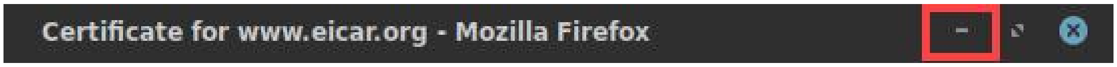
Validity
Not Before 5/31/2021, 9:04:41 PM (Eastern Daylight Time)
Not After 8/29/2021, 9:04:41 PM (Eastern Daylight Time)

Subject Alt Names
DNS Name www.eicar.org

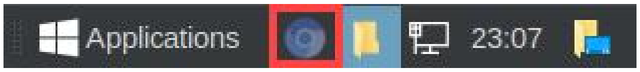
Please Note

This certificate has been issued on behalf of www.eicar.org 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. **Minimize** the *Firefox Web Browser*.



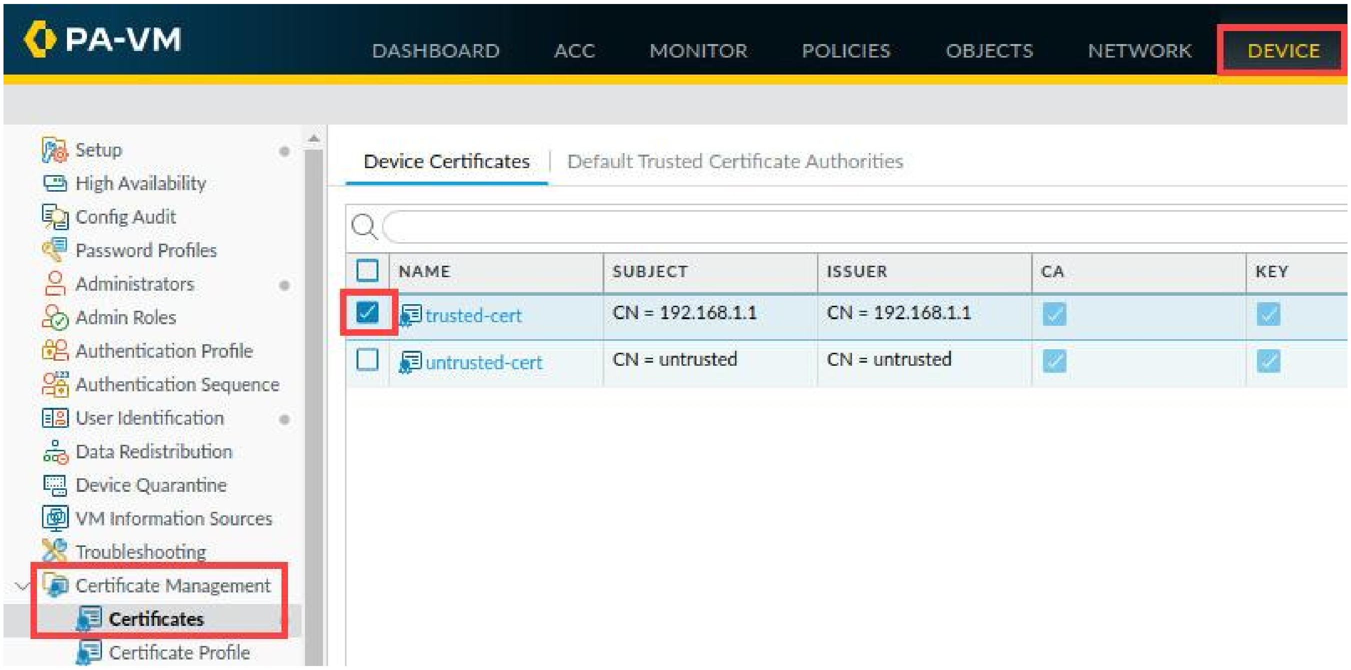
6. If you minimized the *firewall*, reopen the *Firewall* interface by clicking on the **Chromium** tab in the taskbar.



13.7 Export the Firewall Certificate

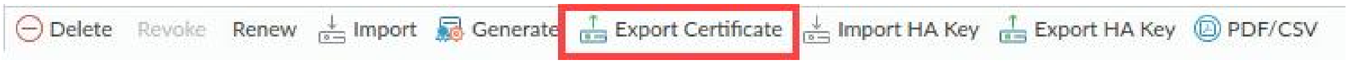
In this section, you will export the trusted certificate from the firewall.

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

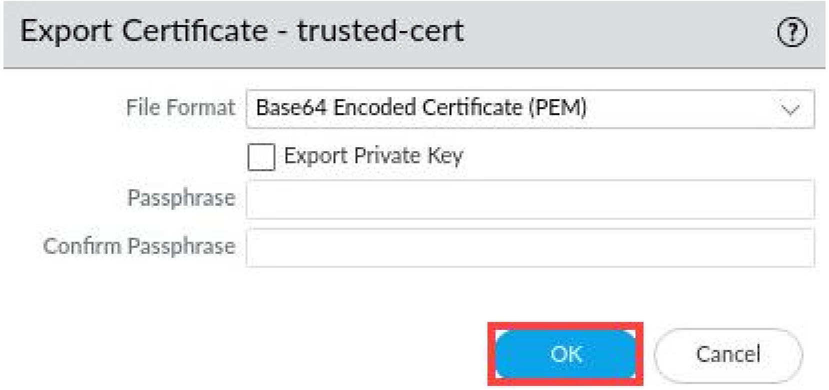


☐	NAME	SUBJECT	ISSUER	CA	KEY
☑	trusted-cert	CN = 192.168.1.1	CN = 192.168.1.1	✓	✓
☐	untrusted-cert	CN = untrusted	CN = untrusted	✓	✓

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, leave all settings unchanged. Click **OK** to export the *trusted-cert* certificate.



Export Certificate - trusted-cert

File Format: Base64 Encoded Certificate (PEM)

□ Export Private Key

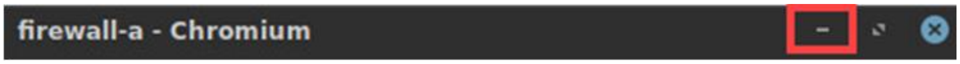
Passphrase:

Confirm Passphrase:

Please Note

The file will be saved to the workstation’s Downloads folder.

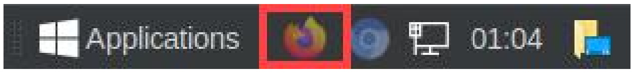
4. Minimize the *Palo Alto Networks Firewall* and continue to the next task.



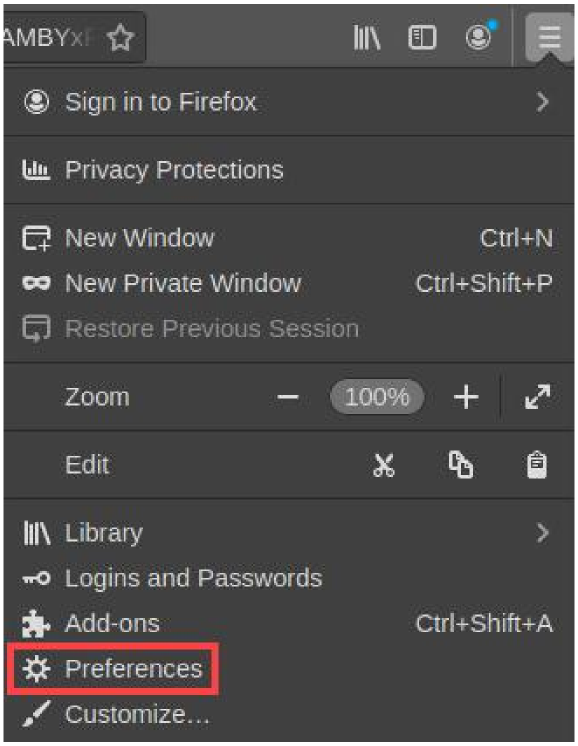
13.8 Import the Firewall Certificate

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

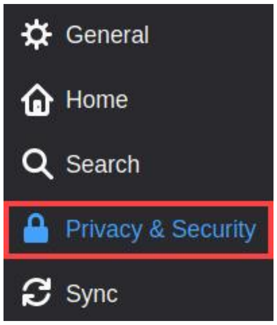
1. On the client desktop, reopen the Firebox Web Browser by clicking the **Firefox** icon in the taskbar.



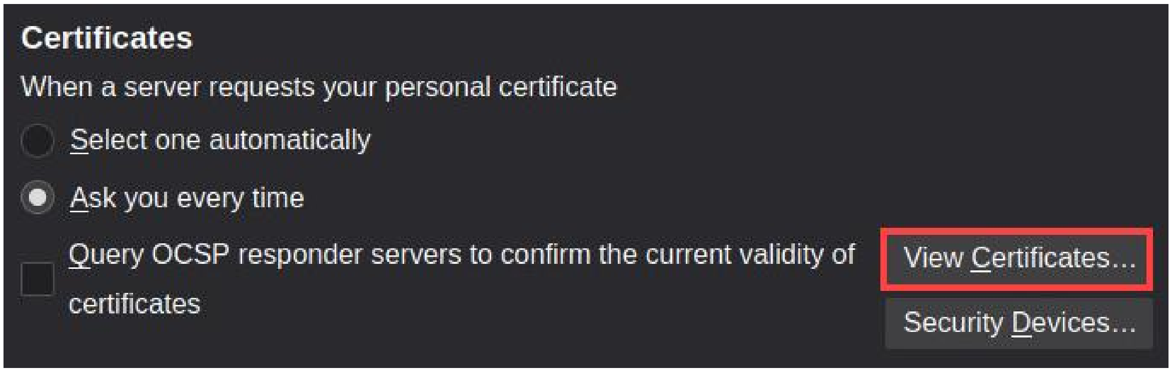
2. In the upper-right corner of the window, click the "**hamburger**" button and choose **Preferences**.



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



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


Certificates

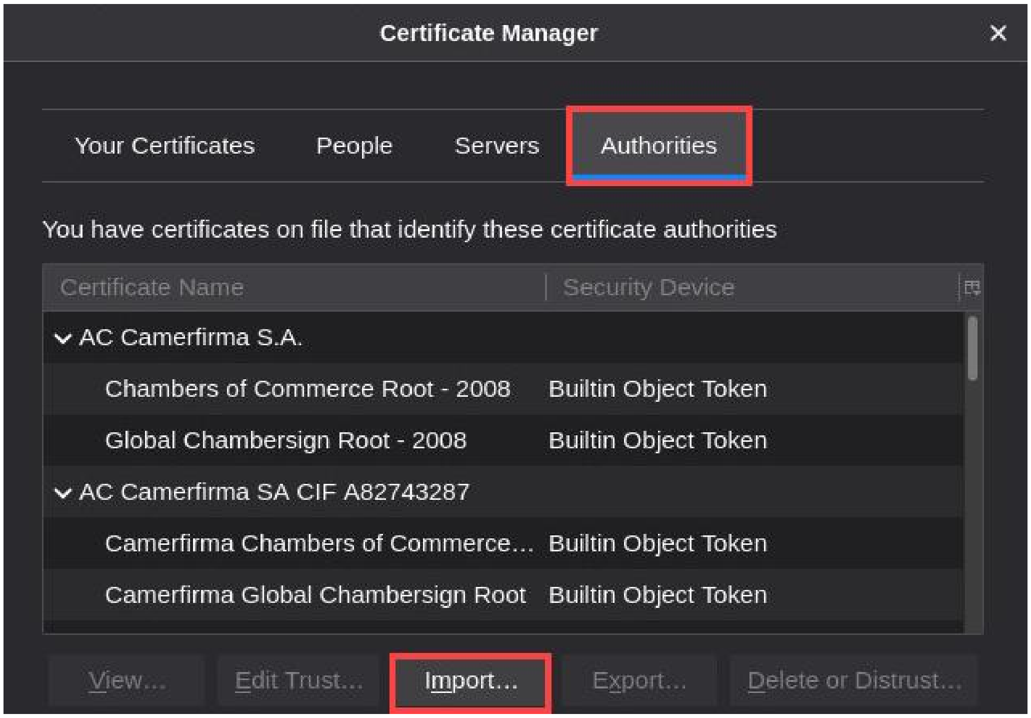
When a server requests your personal certificate

○ Select one automatically

● Ask you every time

□ Query OCSP responder servers to confirm the current validity of certificates

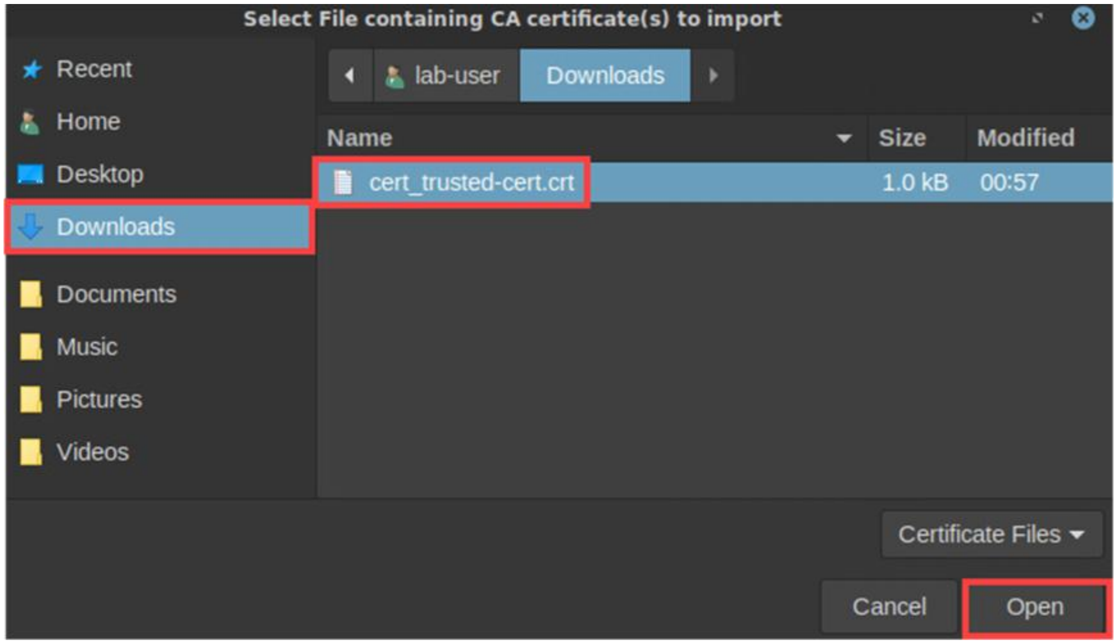
5. In the *Certificate Manager* window, select the **Authorities** tab. Click **Import**.



You have certificates on file that identify these certificate authorities

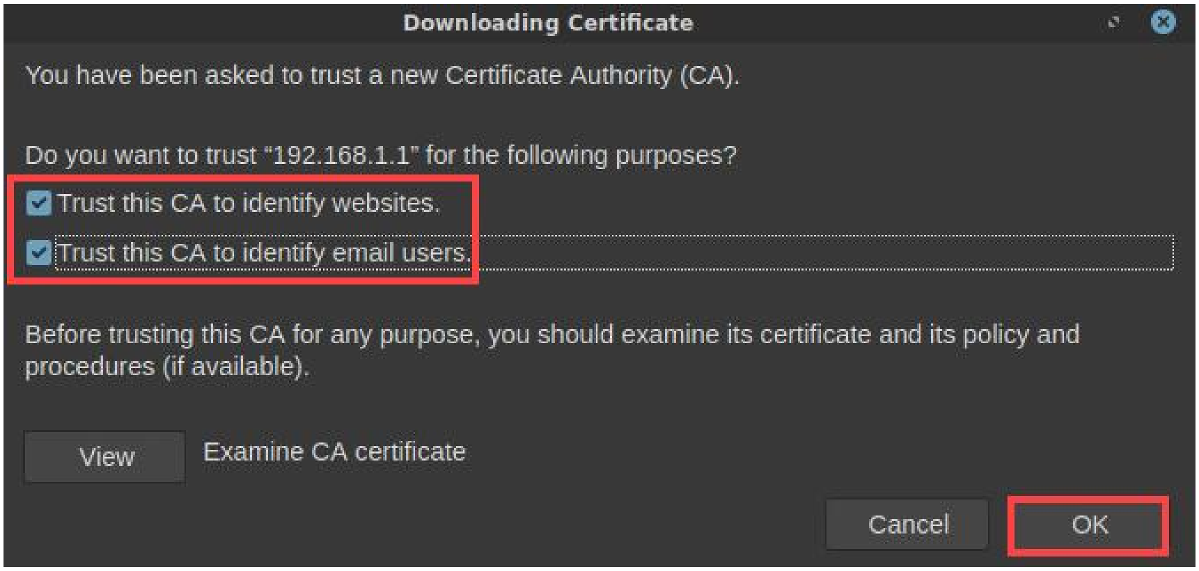
Certificate Name	Security Device
AC Camerfirma S.A.	
Chambers of Commerce Root - 2008	Builtin Object Token
Global Chambersign Root - 2008	Builtin Object Token
AC Camerfirma SA CIF A82743287	
Camerfirma Chambers of Commerce…	Builtin Object Token
Camerfirma Global Chambersign Root	Builtin Object Token

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



Name	Size	Modified
cert_trusted-cert.crt	1.0 kB	00:57

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



Downloading Certificate

You have been asked to trust a new Certificate Authority (CA).

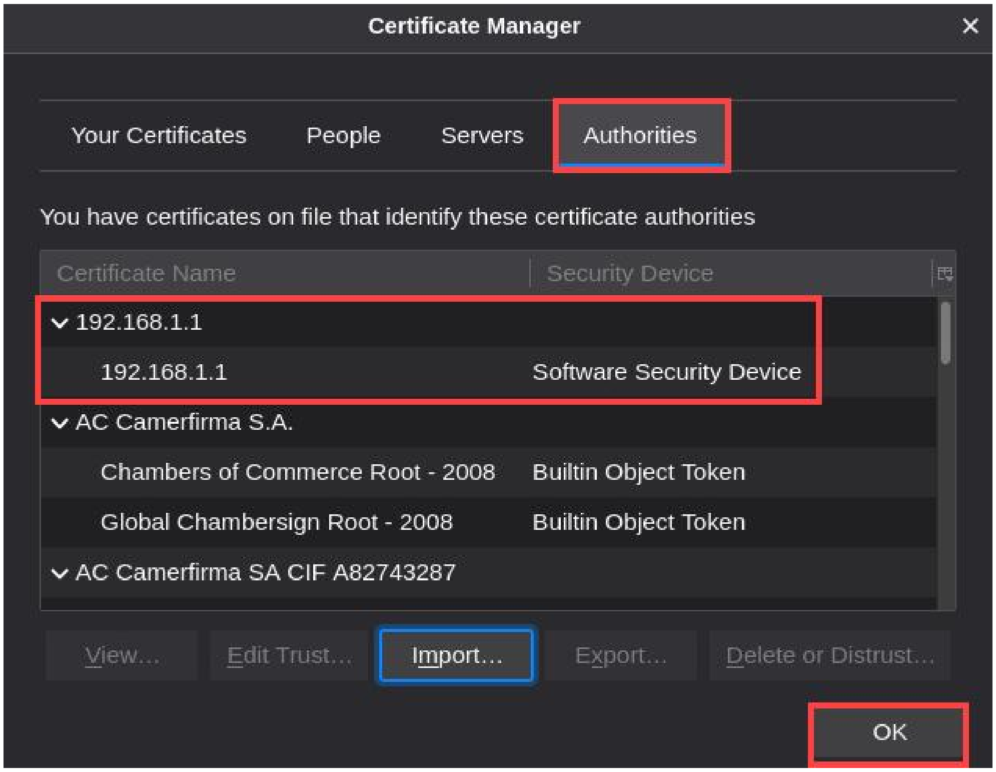
Do you want to trust "192.168.1.1" for the following purposes?

☑ Trust this CA to identify websites.

☑ Trust this CA to identify email users.

Before trusting this CA for any purpose, you should examine its certificate and its policy and procedures (if available).

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



Certificate Manager

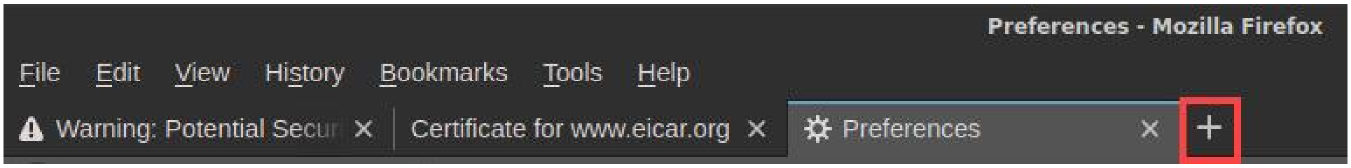
You have certificates on file that identify these certificate authorities

Certificate Name	Security Device
192.168.1.1	
192.168.1.1	Software Security Device
AC Camerfirma S.A.	
Chambers of Commerce Root - 2008	Builtin Object Token
Global Chambersign Root - 2008	Builtin Object Token
AC Camerfirma SA CIF A82743287	

Please Note

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.

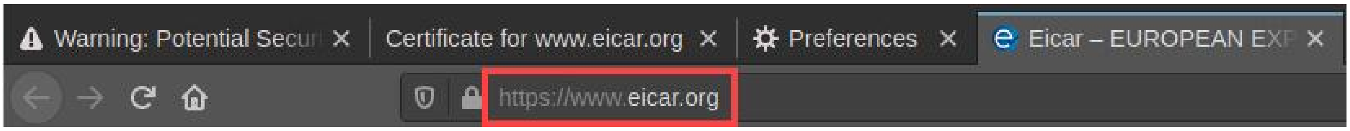
9. Open a new Firefox tab and continue to the next task.


Preferences - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Warning: Potential Secur
Certificate for www.eicar.org
Preferences
+

13.9 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.

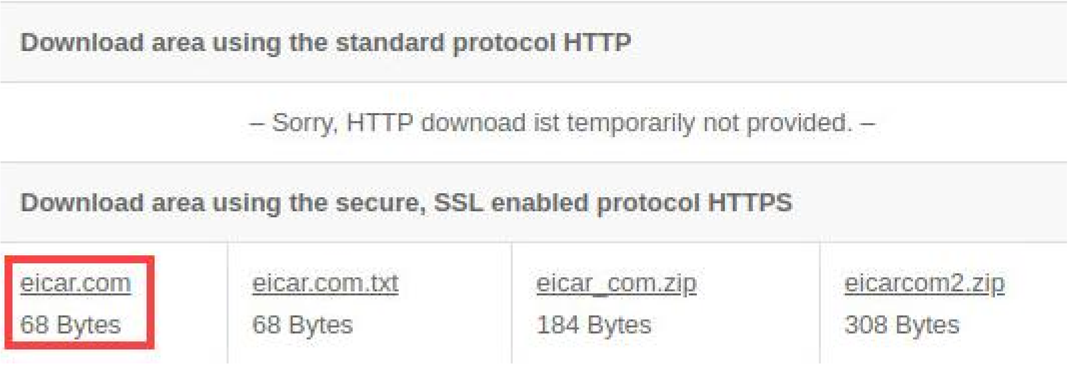
1. In the new *Firefox* tab, type **`https://www.eicar.org`**. Press **Enter**.



2. **Click** the *link* for **Download Anti Malware Testfile**.

DOWNLOAD
ANTI MALWARE TESTFILE

3. Scroll down and locate the section *Download area*. Click the link for the **eicar.com** file download.



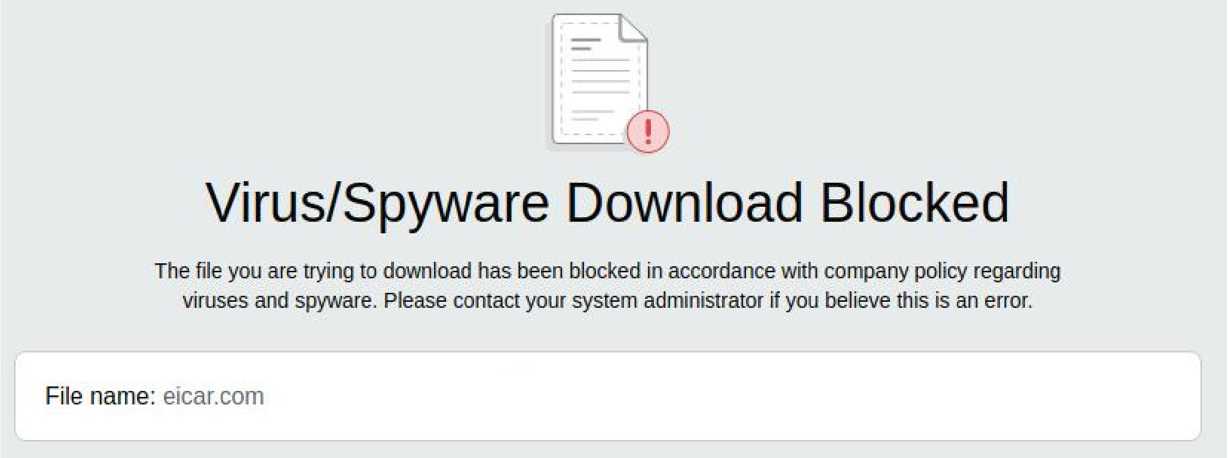
Download area using the standard protocol HTTP

– Sorry, HTTP dowload ist temporarily not provided. –

Download area using the secure, SSL enabled protocol HTTPS

eicar.com 68 Bytes	eicar.com.txt 68 Bytes	eicar_com.zip 184 Bytes	eicarcom2.zip 308 Bytes

4. You will receive a warning pane from the firewall indicating that it has detected and blocked the malicious file download.



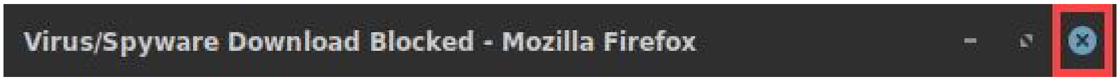
Virus/Spyware Download Blocked

The file you are trying to download has been blocked in accordance with company policy regarding viruses and spyware. Please contact your system administrator if you believe this is an error.

File name: eicar.com

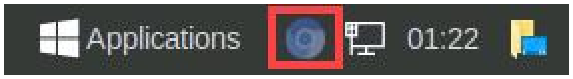
> **Please Note** The kind of message a client receives will vary depending on the browser.

5. Close the *Firefox Web Browser* by clicking the **close** icon.



Virus/Spyware Download Blocked - Mozilla Firefox

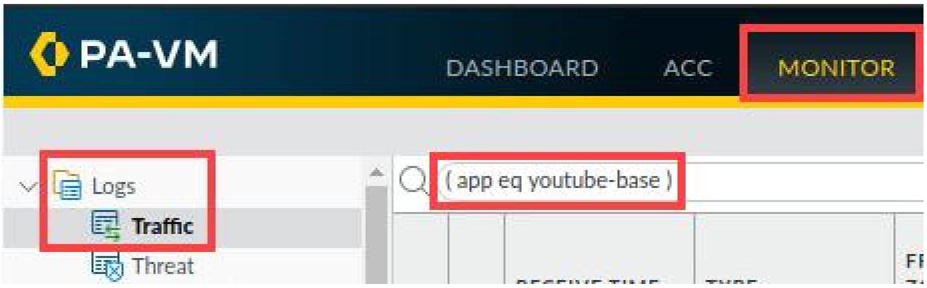
6. Reopen the *PA-VM firewall* web interface by clicking on the **Chromium** icon in the taskbar and continue to the next task.



13.10 Review Firewall Logs

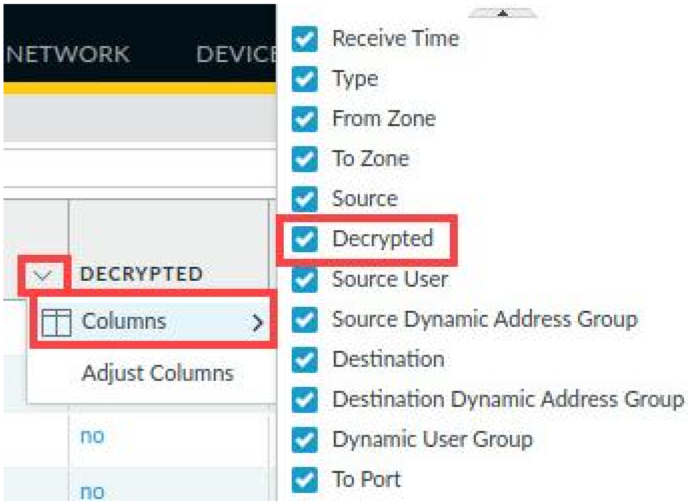
In this section, you will examine information in the firewall logs to see more details about the decryption process.

1. Select **Monitor > Logs > Traffic.** In the filter builder, type `( app eq youtube-base ).` Click **Apply Filter**.

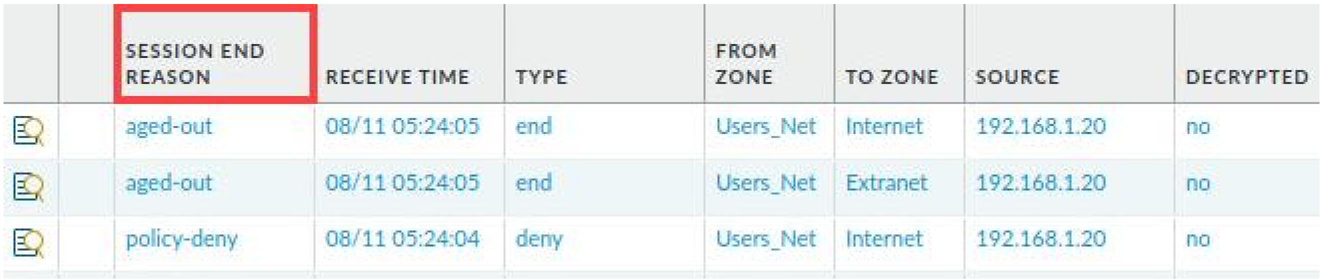


(app eq youtube-base)

2. Add the **Decrypted** column to the table by selecting **Columns > Decrypted**.



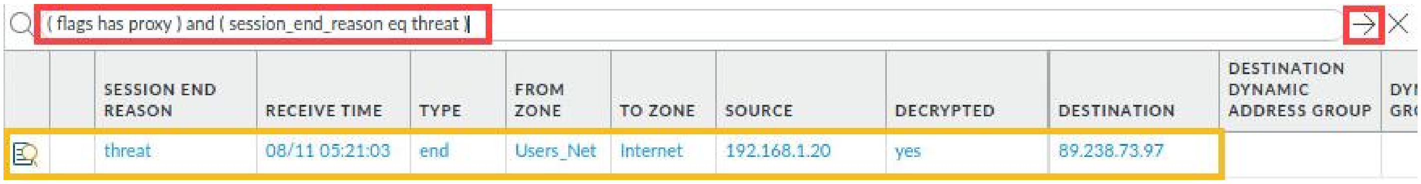
3. Drag and drop the **Session End Reason** column from the right side of the table to the beginning of the table. You may need to *scroll* the *Traffic* window to find the *Session End Reason*.



	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.



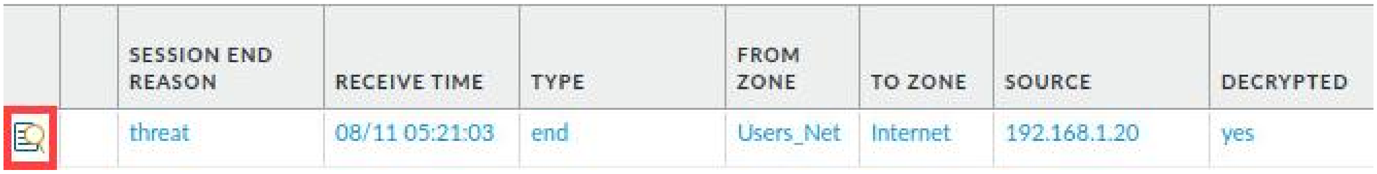
(flags has proxy) and (session_end_reason eq threat)

	SESSION END REASON	RECEIVE TIME	TYPE	FROM ZONE	TO ZONE	SOURCE	DECRYPTED	DESTINATION	DESTINATION DYNAMIC ADDRESS GROUP	DY GR
	threat	08/11 05:21:03	end	Users_Net	Internet	192.168.1.20	yes	89.238.73.97		

Please Note

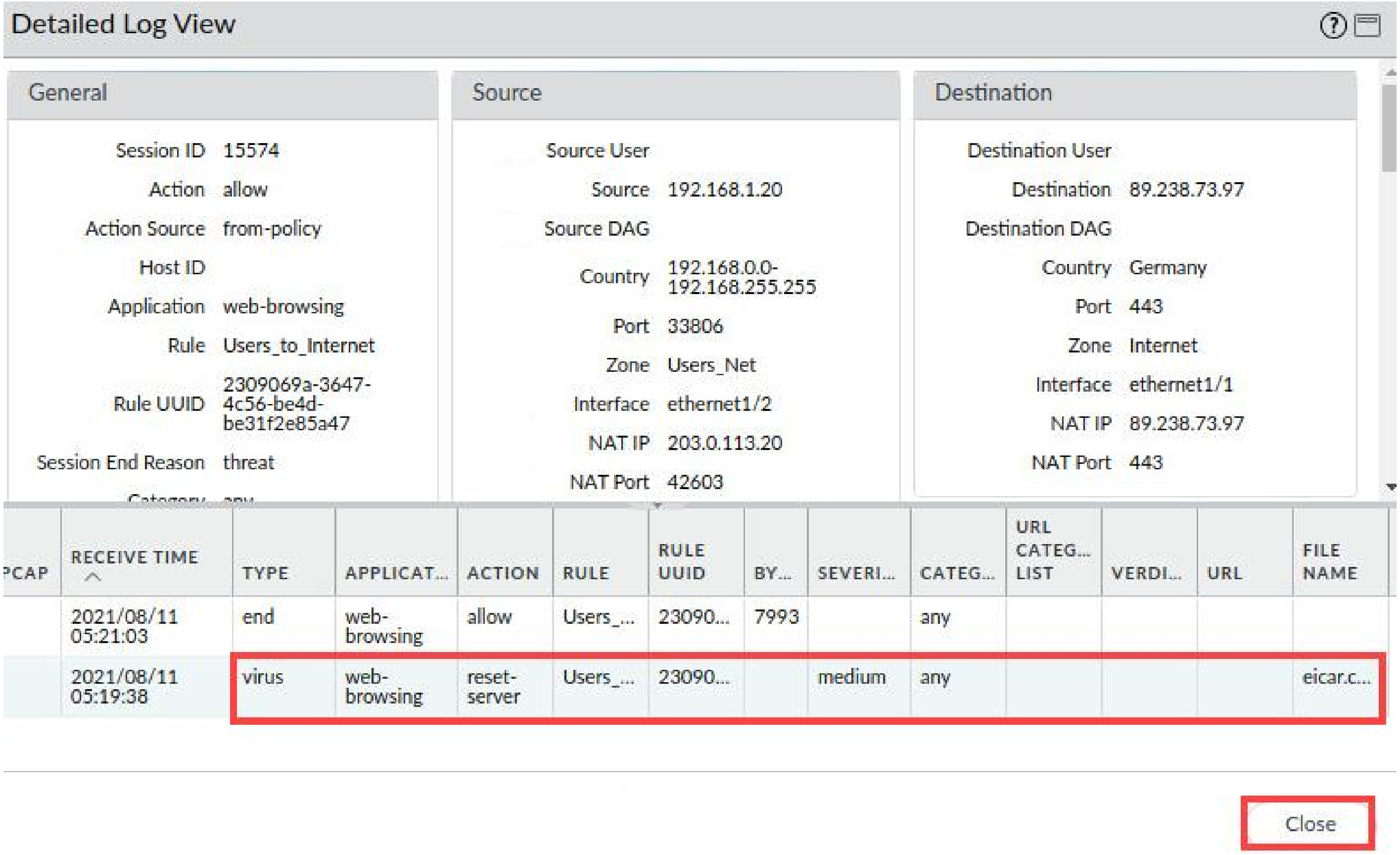
The filter syntax “flags has proxy” displays entries which have been decrypted (the value will show as **yes** in the **Decrypted** column). Entries that match the filter indicate that the firewall carried out a proxy connection for decryption.

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



		SESSION END REASON	RECEIVE TIME	TYPE	FROM ZONE	TO ZONE	SOURCE	DECRYPTED
🔍		threat	08/11 05:21:03	end	Users_Net	Internet	192.168.1.20	yes

6. In the *Detailed Log View* window, you should see similar information indicating that the firewall detected the **eicar.com** file and used **reset-server** to terminate the session. Note that several columns have been hidden in the lower section of this example window. Click **Close**.



Detailed Log View

General

Session ID	15574
Action	allow
Action Source	from-policy
Host ID	
Application	web-browsing
Rule	Users_to_Internet
Rule UUID	2309069a-3647-4c56-be4d-be31f2e85a47
Session End Reason	threat
Category	any

Source

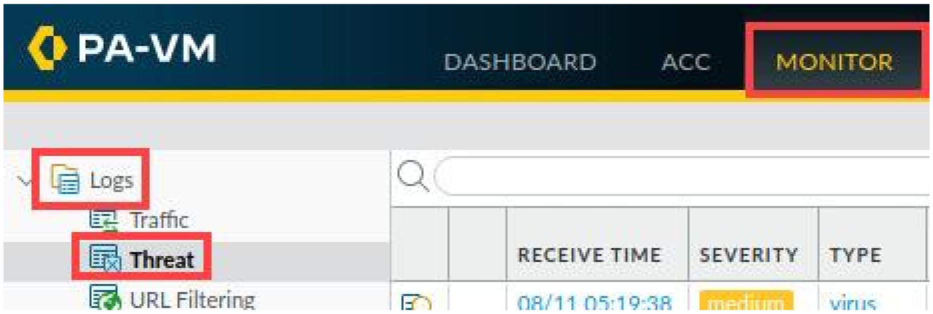
Source User	
Source	192.168.1.20
Source DAG	
Country	192.168.0.0-192.168.255.255
Port	33806
Zone	Users_Net
Interface	ethernet1/2
NAT IP	203.0.113.20
NAT Port	42603

Destination

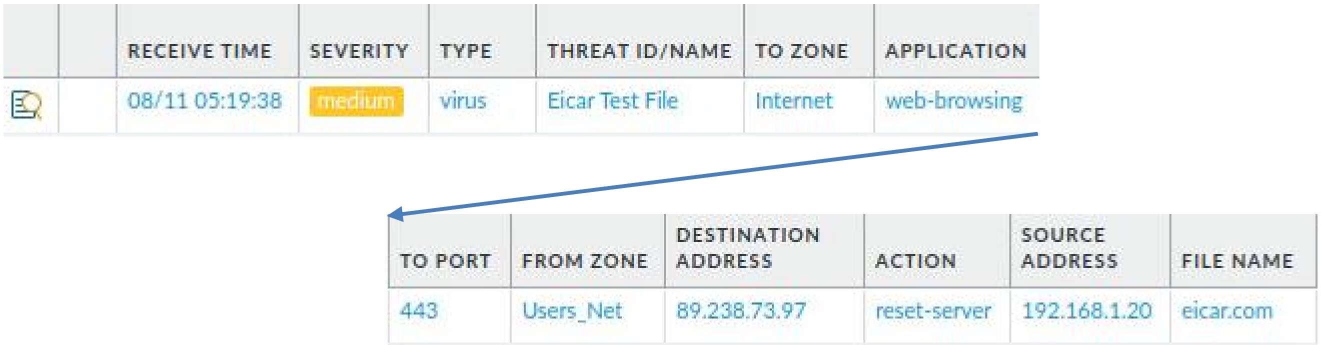
Destination User	
Destination	89.238.73.97
Destination DAG	
Country	Germany
Port	443
Zone	Internet
Interface	ethernet1/1
NAT IP	89.238.73.97
NAT Port	443

PCAP	RECEIVE TIME	TYPE	APPLICAT...	ACTION	RULE	RULE UUID	BY...	SEVERI...	CATEG...	URL CATEG... LIST	VERDI...	URL	FILE NAME
	2021/08/11 05:21:03	end	web-browsing	allow	Users_...	23090...	7993		any				
	2021/08/11 05:19:38	virus	web-browsing	reset-server	Users_...	23090...		medium	any				eicar.c...

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



8. Delete any filters in place. Notice the entry for virus indicates that the firewall detected and blocked the **eicar.com** file.



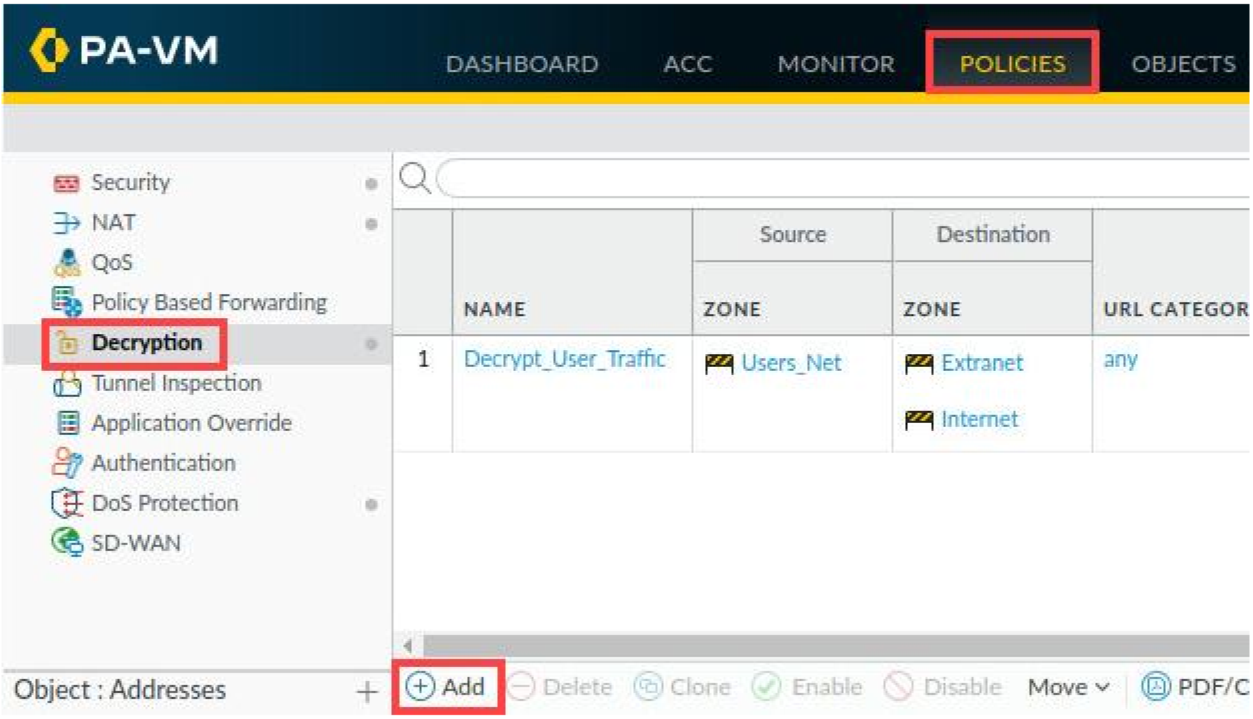
		RECEIVE TIME	SEVERITY	TYPE	THREAT ID/NAME	TO ZONE	APPLICATION	TO PORT	FROM ZONE	DESTINATION ADDRESS	ACTION	SOURCE ADDRESS	FILE NAME
		08/11 05:19:38	medium	virus	Eicar Test File	Internet	web-browsing	443	Users_Net	89.238.73.97	reset-server	192.168.1.20	eicar.com

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

13.11 Exclude URL Categories from Decryption

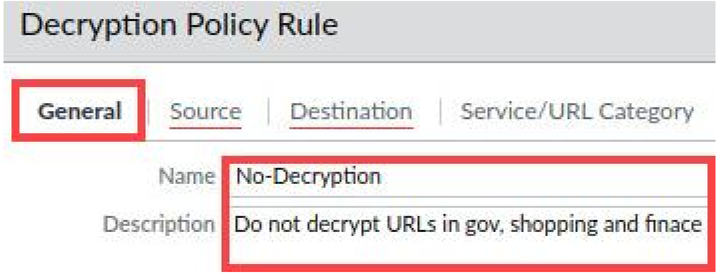
The existing decryption policy rule you created instructs the firewall to decrypt all traffic, regardless of the URL category. In this section, you will configure a no-decrypt rule that instructs the firewall to exclude sensitive categories of web traffic from decryption in order to avoid exposing PII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

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



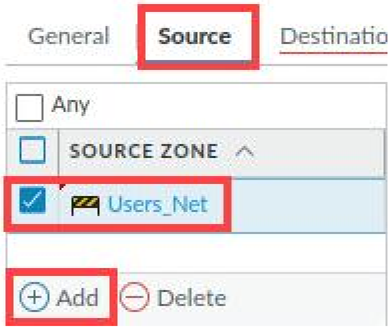
		Source	Destination	
	NAME	ZONE	ZONE	URL CATEGOR
1	Decrypt_User_Traffic	Users_Net	Extranet Internet	any

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`**.



Name: No-Decryption
Description: Do not decrypt URLs in gov, shopping and finace

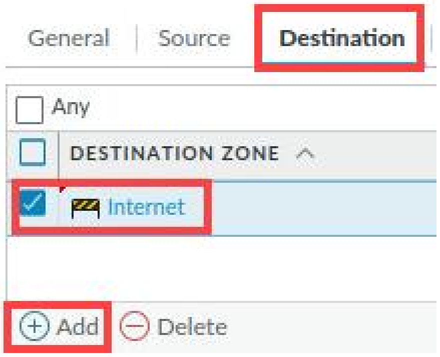
3. Select the tab for **Source.** Under the *Source Zone* section, click **Add** and select **Users_Net**.



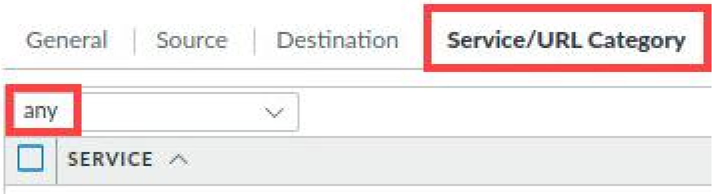
□ Any

□	SOURCE ZONE
☑	Users_Net

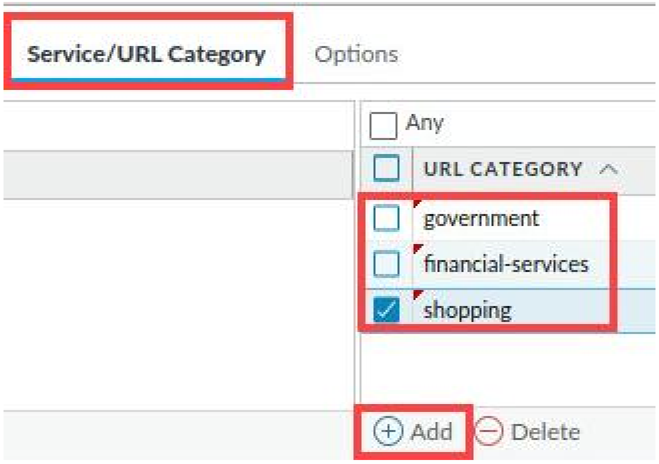
4. Select the **Destination** tab. Under the *Destination Zone* section, click **Add** and select **Internet**.



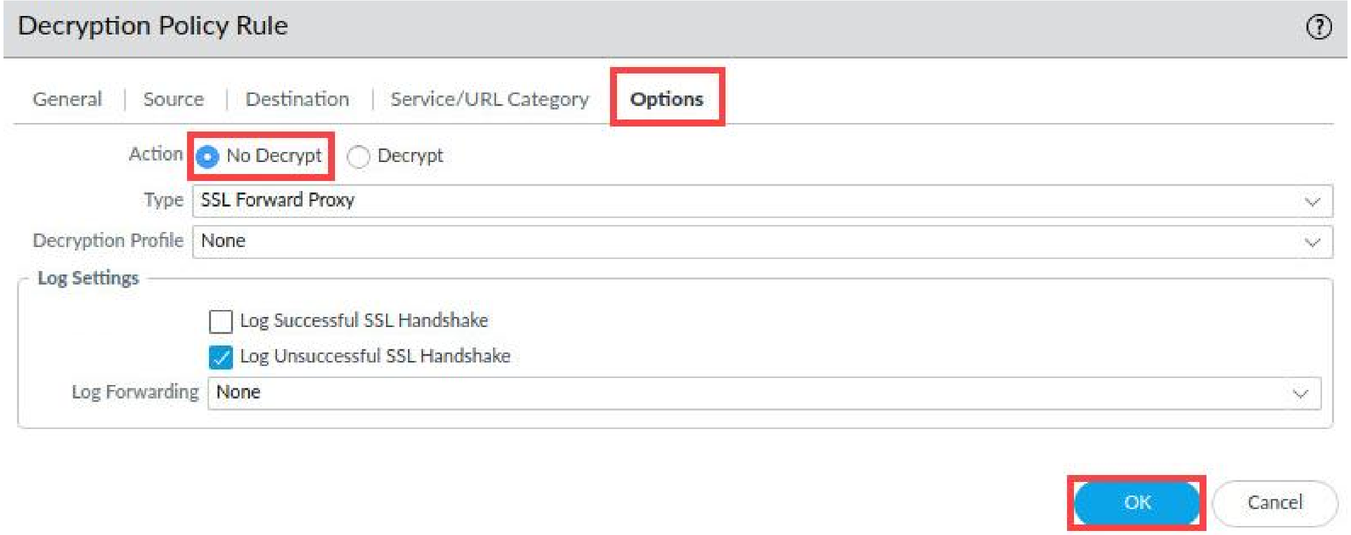
5. Select the tab for **Service/URL Category.** Leave the **Service** set to **any**.



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**. Click **OK**.



Decryption Policy Rule

General | Source | Destination | Service/URL Category | Options

Action ● No Decrypt ○ Decrypt

Type SSL Forward Proxy

Decryption Profile None

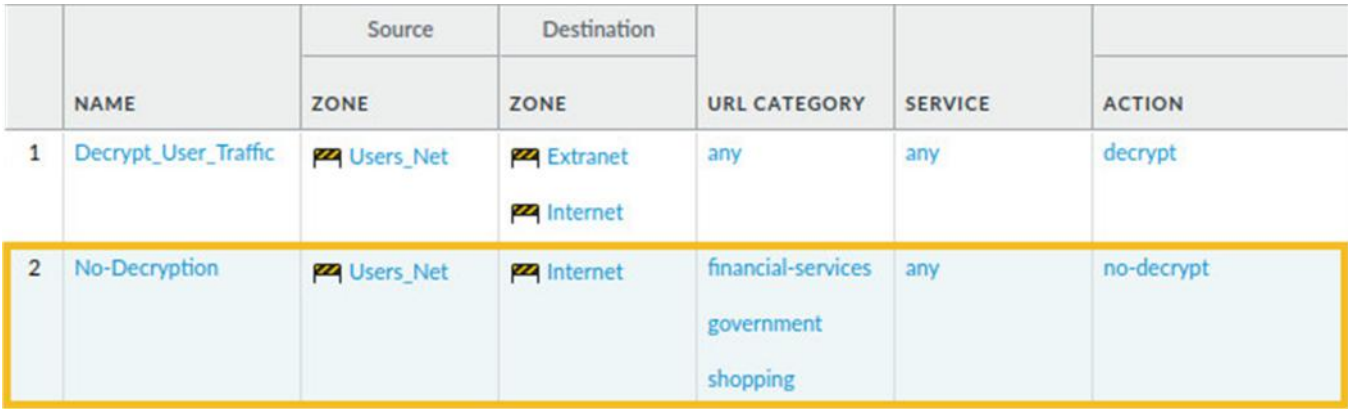
Log Settings

□ Log Successful SSL Handshake

☑ Log Unsuccessful SSL Handshake

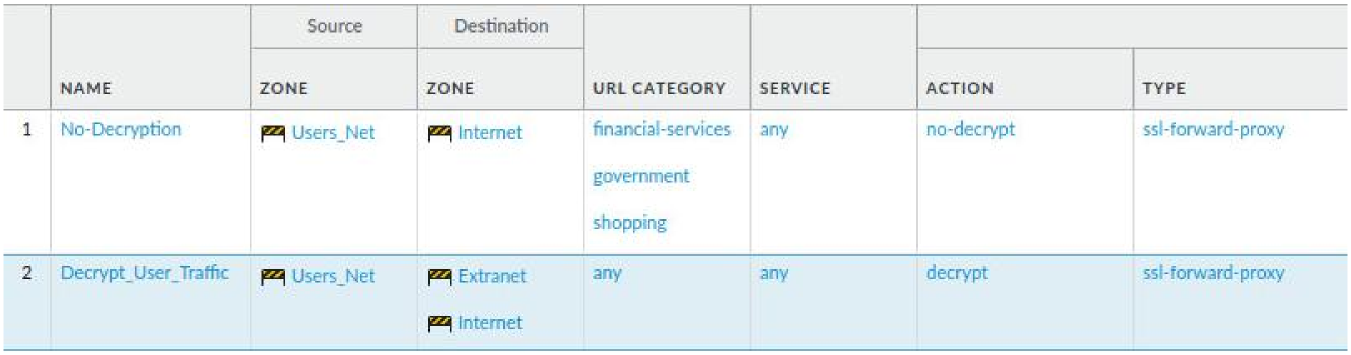
Log Forwarding None

8. You should have two entries in the *Decryption* policy. Do you notice what is wrong with the Decryption Policies? The answer is yes. They are in the wrong order. All traffic will match the first rule Decrypt_Users_Traffic because the URL category is set to **any**. The firewall will therefore never proceed beyond that first rule to implement the second rule, which instructs the firewall to exclude financial-services, government, and shopping websites from decryption



		Source	Destination			
	NAME	ZONE	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

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

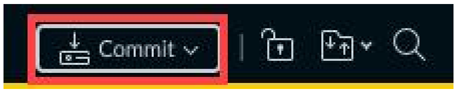


		Source	Destination				
	NAME	ZONE	ZONE	URL CATEGORY	SERVICE	ACTION	TYPE
1	No-Decryption	Users_Net	Internet	financial-services government shopping	any	no-decrypt	ssl-forward-proxy
2	Decrypt_User_Traffic	Users_Net	Extranet Internet	any	any	decrypt	ssl-forward-proxy

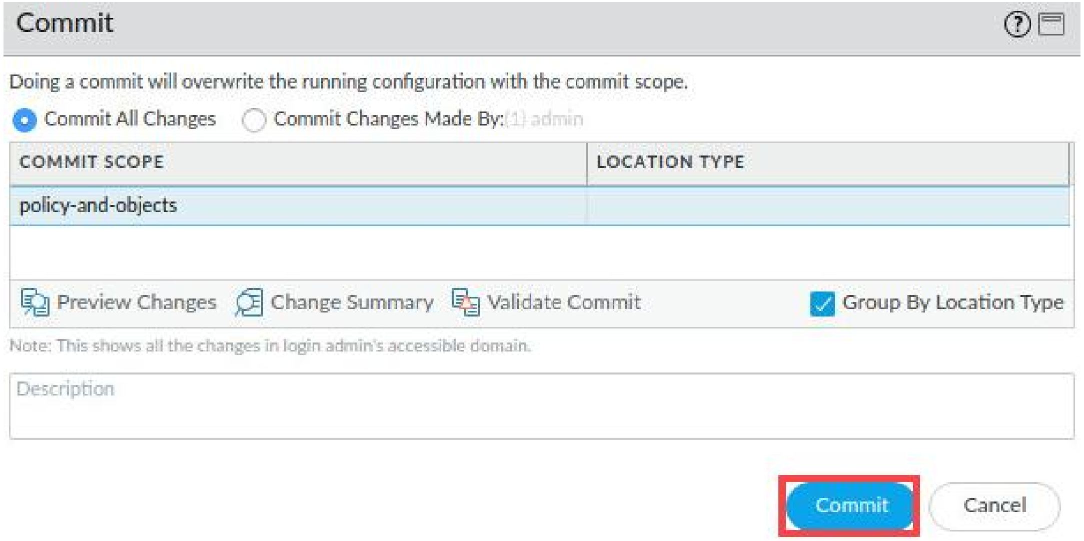
Please Note

Always place no-decrypt rules at the beginning of the decryption policy table so that specified packets don't get decrypted when the firewall evaluates rules from top-to-bottom.

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.



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	

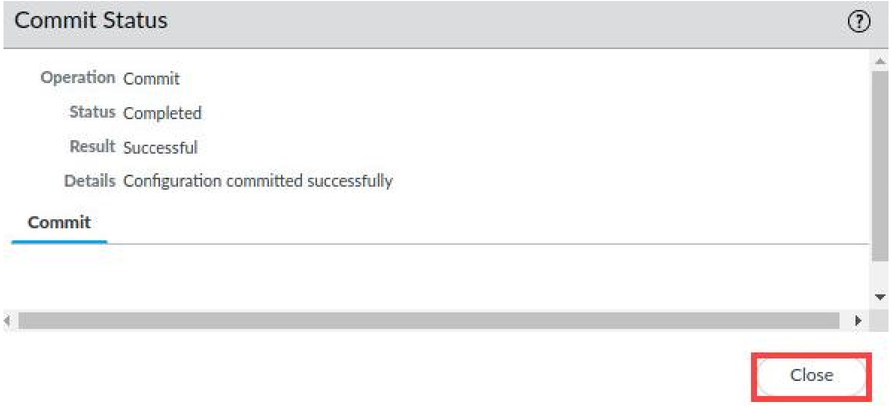
Preview Changes Change Summary Validate Commit ☑ Group By Location Type

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

Description

Commit Cancel

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



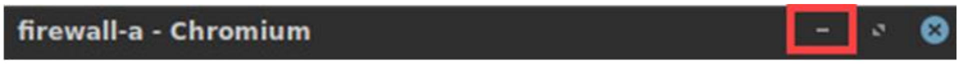
Commit Status

Operation Commit
Status Completed
Result Successful
Details Configuration committed successfully

Commit

Close

13. Minimize the *Palo Alto Networks Firewall* and continue to the next task.

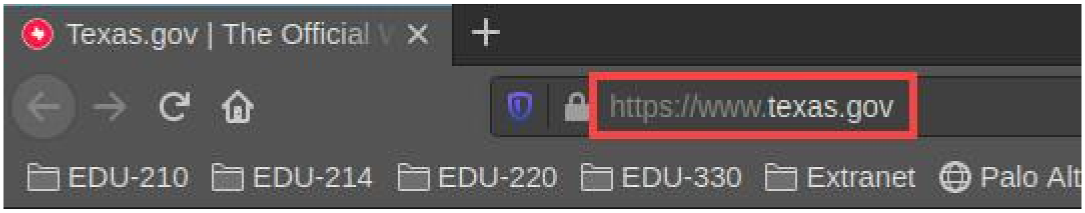


13.12 Test the No-Decryption Rule

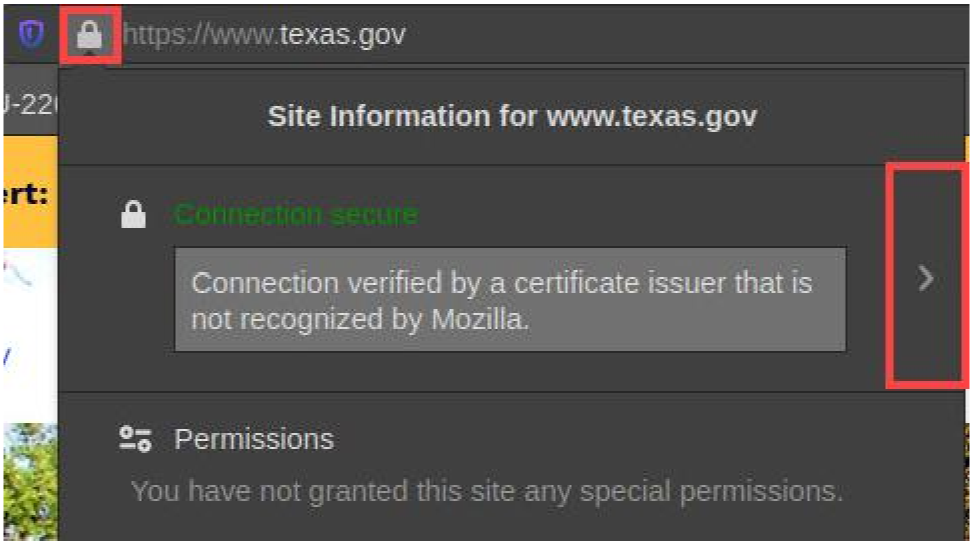
With your No-Decryption rule in place, you will test the No-Decryption rule by browsing to a website that falls into one of the excluded categories.

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

2. 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*.


https://www.texas.gov

Site Information for www.texas.gov

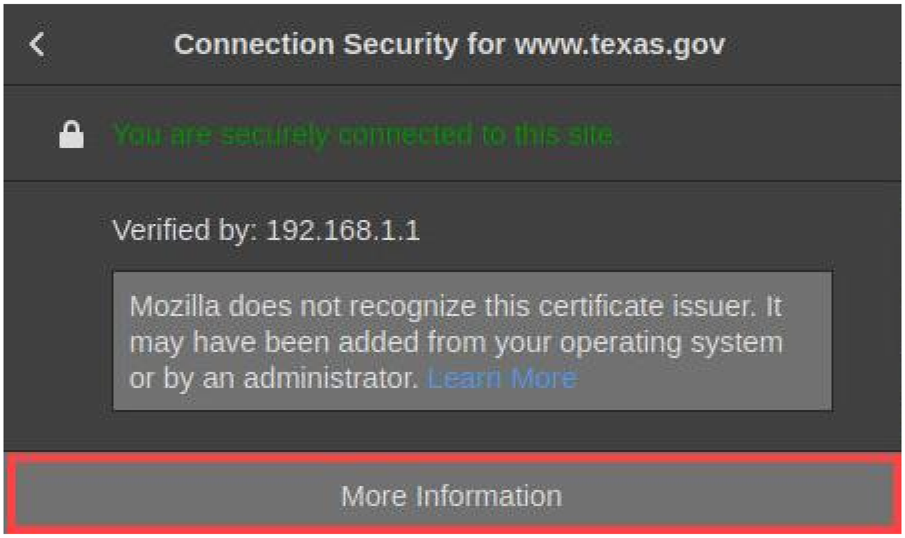
Connection secure

Connection verified by a certificate issuer that is not recognized by Mozilla.

Permissions

You have not granted this site any special permissions.

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



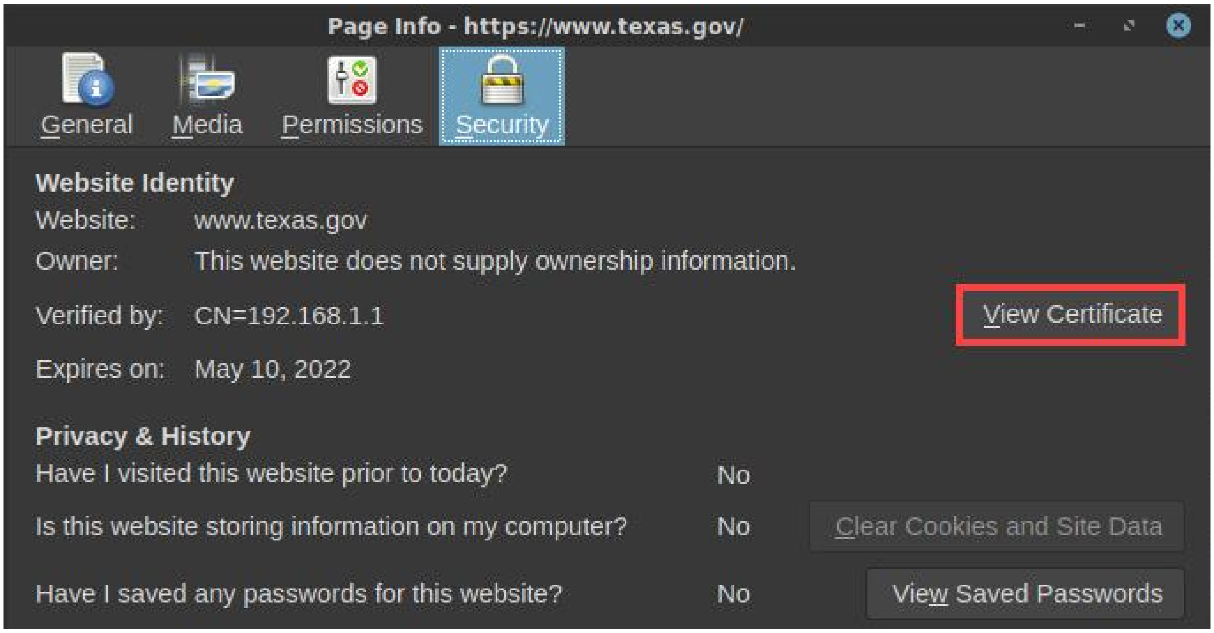
Connection Security for www.texas.gov

You are securely connected to this site.

Verified by: 192.168.1.1

Mozilla does not recognize this certificate issuer. It may have been added from your operating system or by an administrator. Learn More

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



Page Info - https://www.texas.gov/

Website Identity

Website: www.texas.gov

Owner: This website does not supply ownership information.

Verified by: CN=192.168.1.1

Expires on: May 10, 2022

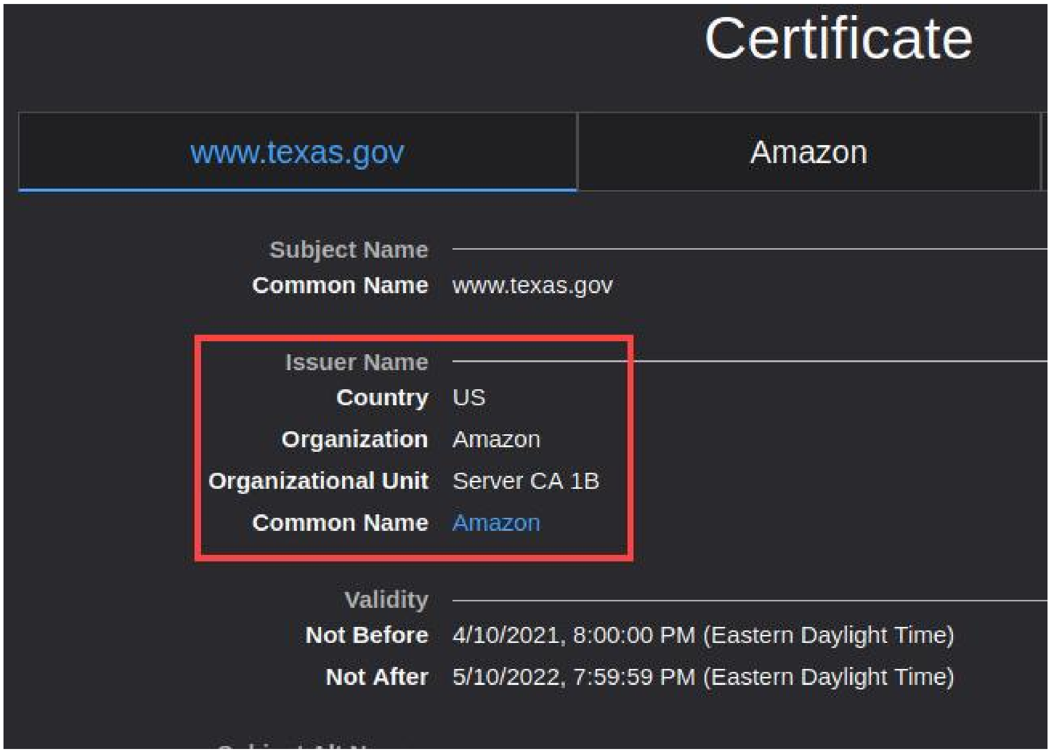
Privacy & History

Have I visited this website prior to today? No

Is this website storing information on my computer? No

Have I saved any passwords for this website? No

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



Certificate

www.texas.gov | Amazon

Subject Name
Common Name www.texas.gov

Issuer Name
Country US
Organization Amazon
Organizational Unit Server CA 1B
Common Name Amazon

Validity
Not Before 4/10/2021, 8:00:00 PM (Eastern Daylight Time)
Not After 5/10/2022, 7:59:59 PM (Eastern Daylight Time)

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.