



PALO ALTO NETWORKS - EDU-210



Lab 7: Decryption

Document Version: 2021-08-24

Contents

Introduction	3
Objectives.....	3
Lab Topology	4
Theoretical Lab Topology.....	4
Lab Settings	5
7 Decryption.....	6
7.0 Load Lab Configuration	6
7.1 Test Firewall Behavior Without Decryption	9
7.2 Create Two Self-Signed Certificates	11
7.3 Create a Custom Decryption URL Category	15
7.4 Create a Decryption Policy	16
7.5 Test AV Security Profile with the Decryption Policy	21
7.6 Export the Firewall Certificate	23
7.7 Import the Firewall Certificate	25
7.8 Test the Decryption Policy	28
7.9 Review Logs	32
7.10 Test URL Filtering with Decryption	33

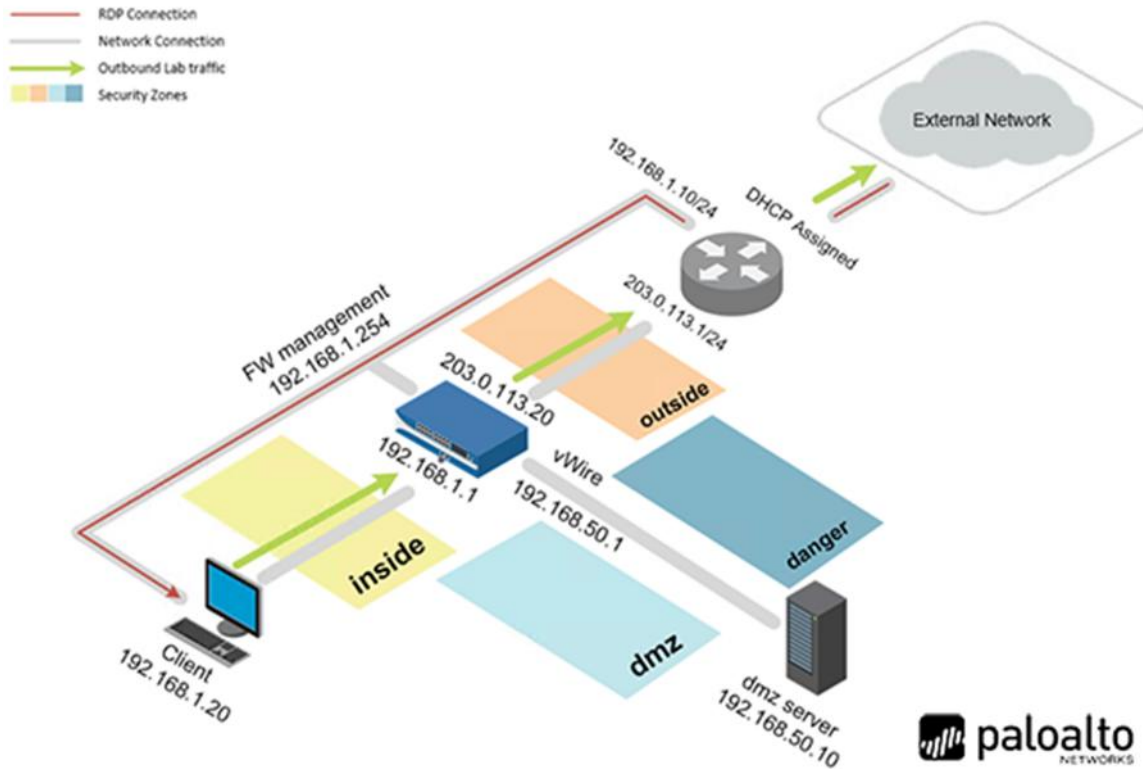
Introduction

As you browsed through the logs, you noticed that there was a lot of SSL traffic. When you were testing the system and attempted to download an Eicar file from one of the SSL links, you found that it was allowed. The CSO has determined that we need to inspect all traffic within the acceptable risk categories. Therefore, you need to set up the system to decrypt all traffic that is not to be excluded because of compliance requirements.

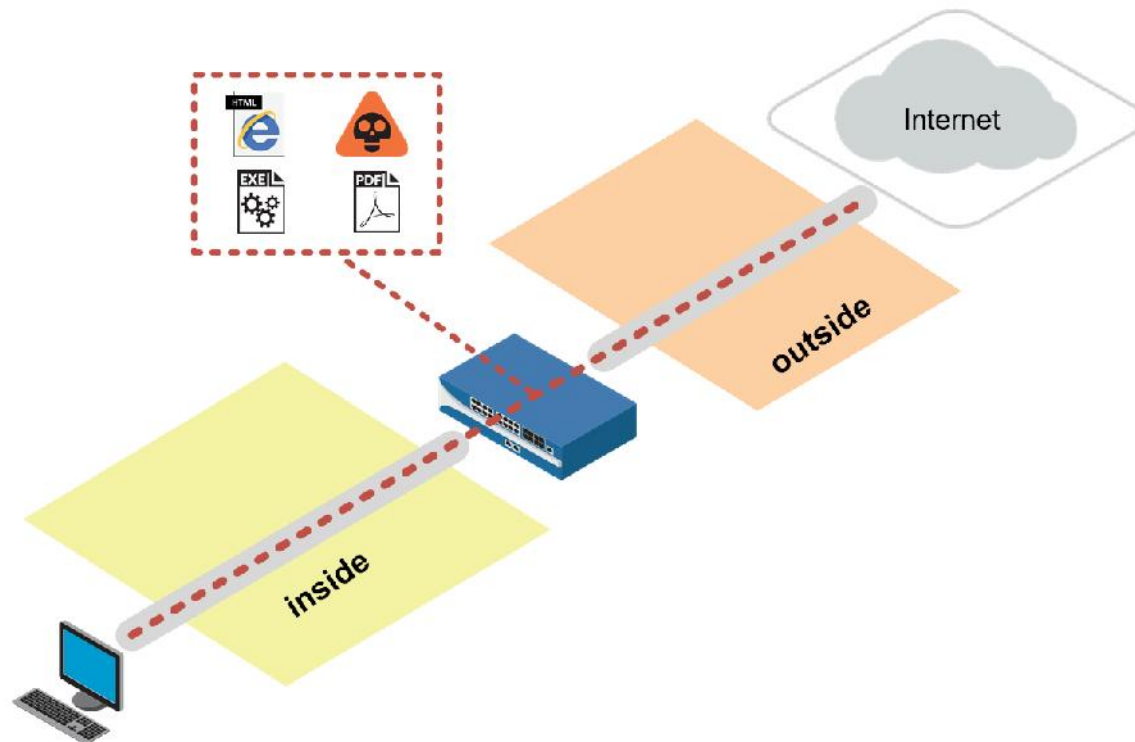
Objectives

-) Observe firewall behavior without decryption
-) Create Forward Trust and Untrust certificates
-) Create a custom decryption category
-) Create a Decryption policy
-) Observe firewall behavior after decryption is enabled
-) Review logs

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	Train1ng\$
Firewall	192.168.1.254	admin	Train1ng\$

7 Decryption

7.0 Load Lab Configuration

1. Launch the **Client** virtual machine to access the graphical login screen.



To launch the console window for a virtual machine, you may access by either clicking on the machine's graphic image from the topology page or by clicking on the machine's respective tab from the navigation bar.

2. Log in as **lab-user** using the password **Train1ng\$**.



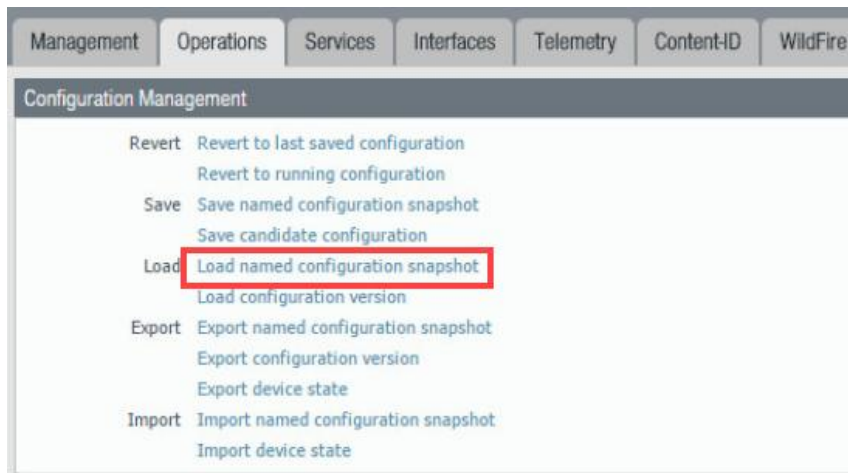
3. Launch the **Chromium Web Browser** and connect to **https://192.168.1.254**.
4. If a security warning appears, click **Advanced** and proceed by clicking on **Proceed to 192.168.1.254 (unsafe)**.
5. Log in to the *Palo Alto Networks* firewall using the following:

Parameter	Value
Name	admin
Password	Train1ng\$

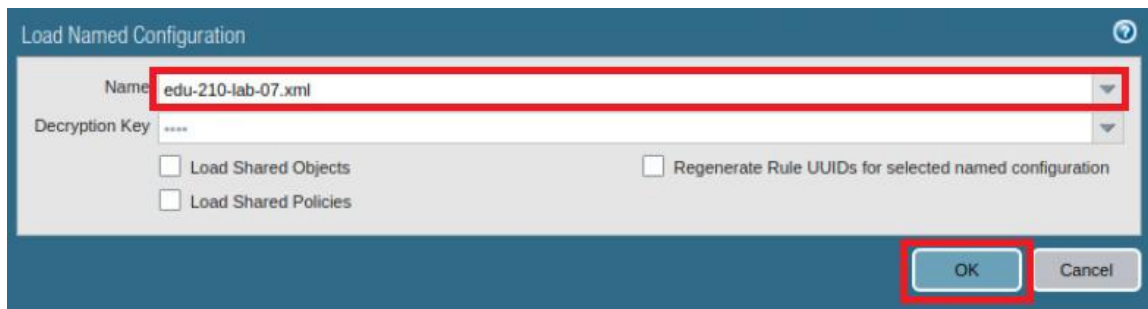
6. In the web interface, select **Device > Setup > Operations**.



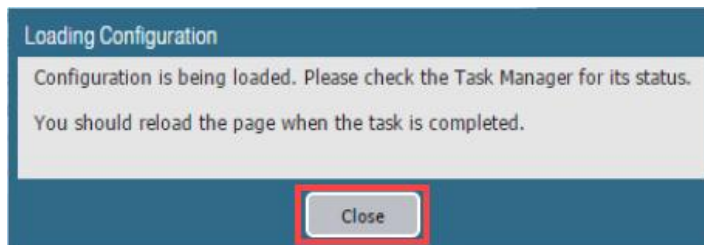
7. Click **Load named configuration snapshot**:



8. Click the dropdown list next to the *Name* text box and select **edu-210-lab-07.xml**. Click **OK**.



9. Click **Close**.

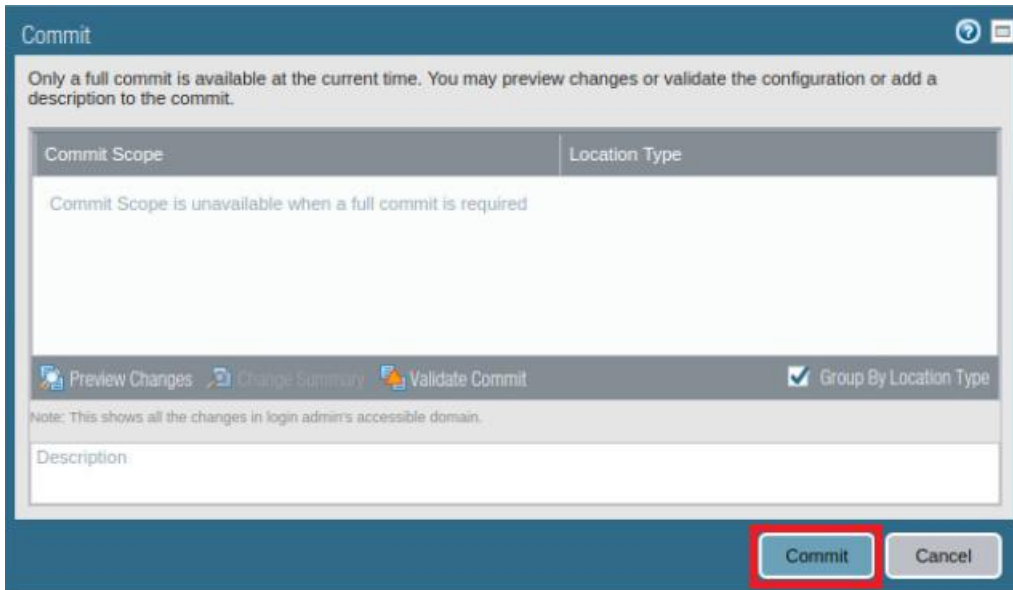


The following instructions are the steps to execute a **“Commit All”** as you will perform many times throughout these labs.

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

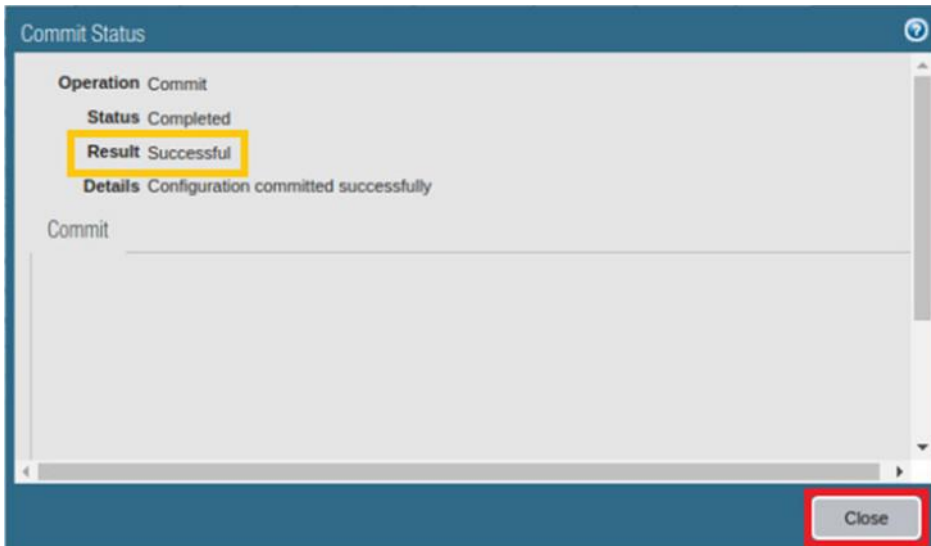


11. Click **Commit** and wait until the commit process is complete.



The 'Commit' dialog box has a title bar with a question mark icon and a close icon. The main text reads: '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.' Below this is a table with two columns: 'Commit Scope' and 'Location Type'. The 'Commit Scope' cell contains the text 'Commit Scope is unavailable when a full commit is required'. Below the table is a row of buttons: 'Preview Changes', 'Change Summary', 'Validate Commit', and a checked checkbox labeled 'Group By Location Type'. Below the buttons is a text area labeled 'Description'. At the bottom right are two buttons: 'Commit' (highlighted with a red box) and 'Cancel'.

12. Once completed successfully, click **Close** to continue.

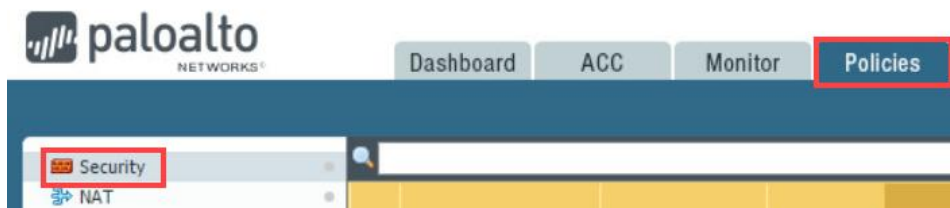


The 'Commit Status' dialog box has a title bar with a question mark icon and a close icon. The main content area shows the following information: 'Operation Commit', 'Status Completed', 'Result Successful' (highlighted with a yellow box), and 'Details Configuration committed successfully'. Below this is a text area labeled 'Commit'. At the bottom right is a button labeled 'Close' (highlighted with a red box).

13. Leave the firewall web interface open to continue with the next task.

7.1 Test Firewall Behavior Without Decryption

1. In the web interface, navigate to **Policies > Security**.

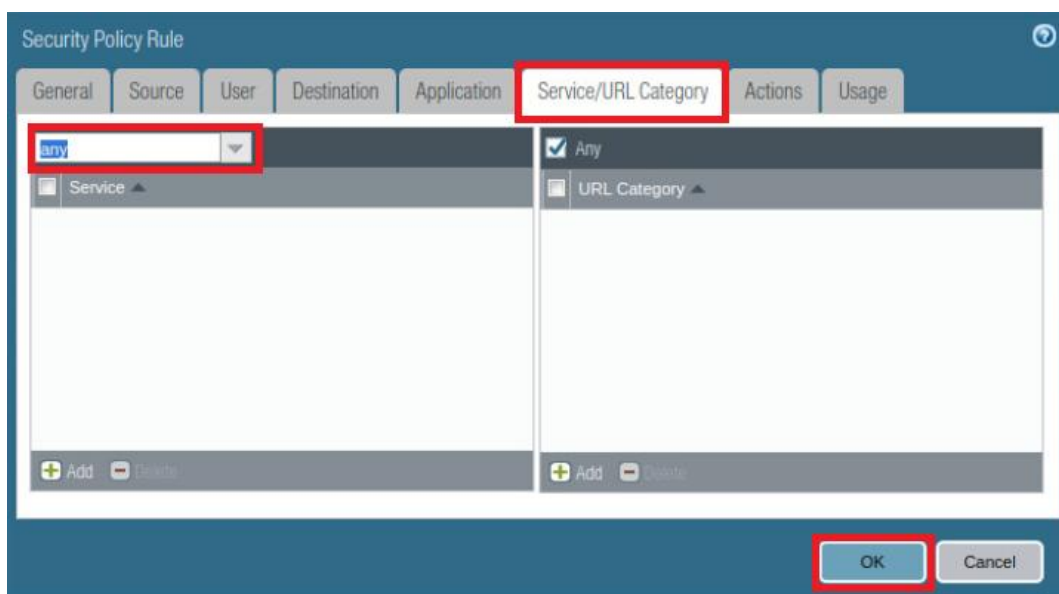


2. Click on **egress-outside-content-id** to open the Security Policy Rule.

	Name	Tags	Type	Zone
1	internal-inside-dmz	internal	universal	inside
2	egress-outside	egress	universal	inside
3	egress-outside-content-id	egress	universal	inside
4	danger-simulated-traffic	none	universal	danger
5	intrazone-default	none	intrazone	any
6	interzone-default	none	interzone	any

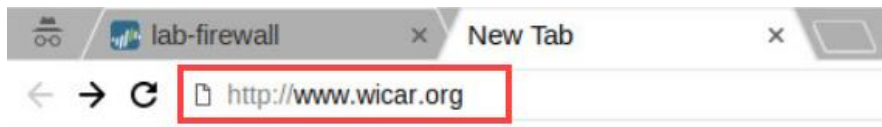
3. In the *Security Policy Rule* window, click the **Service/URL Category** tab and configure the following. Once finished, click **OK**.

Parameter	Value
Service	Select any from the dropdown list



4. **Commit** all changes.

5. Open a new tab in **Chromium Web Browser** and browse to <http://www.wicar.org>.



6. Click the **Test Malware!** menu option located at the top.



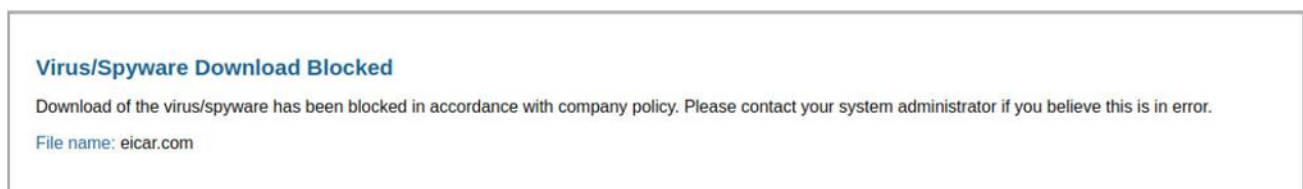
7. On the option to select a test payload, click on the **EICAR TEST-VIRUS** button.

Select a test payload...

Each test will open up a new browser window at <http://malware.wicar.org/>. You may wish to try each test systematically. Ideally, all tests should be blocked by your anti-malware defences. If a blank window loads, then it likely was not detected/prevented.

EICAR TEST-VIRUS	MS14-064 XP and below	MS14-064 2003 to Windows 10
[SSL] The official EICAR.COM anti-virus test file. This is a 16bit DOS COM file and cannot run on recent OSes, but should be detected.	[SSL] All Windows NT/95/98/2000/XP IE3+ Internet Explorer Windows OLE Automation Array (pre XP) CVE-2014-6332	[SSL] All Windows 2003/Vista/2008/7/8/10 IE6+ Internet Explorer Windows OLE Automation Array (post XP) CVE-2014-6332

8. Notice a message appears stating that the download was blocked. Close this browser tab.



- Back on the *wicar.org* webpage download the same test file, but this time choose to download it using HTTPS by clicking on the **SSL** hyperlink found underneath the **EICAR TEST-VIRUS** button.

Select a test payload...

Each test will open up a new browser window at <http://malware.wicar.org>.
all tests should be blocked by your anti-malware defences. If

EICAR TEST-VIRUS

[SSL]

 The official **EICAR.COM** anti-virus test file.
This is a 16bit DOS COM file and cannot
run on recent OSes, but should be detected.

MS14-0

[SSL]

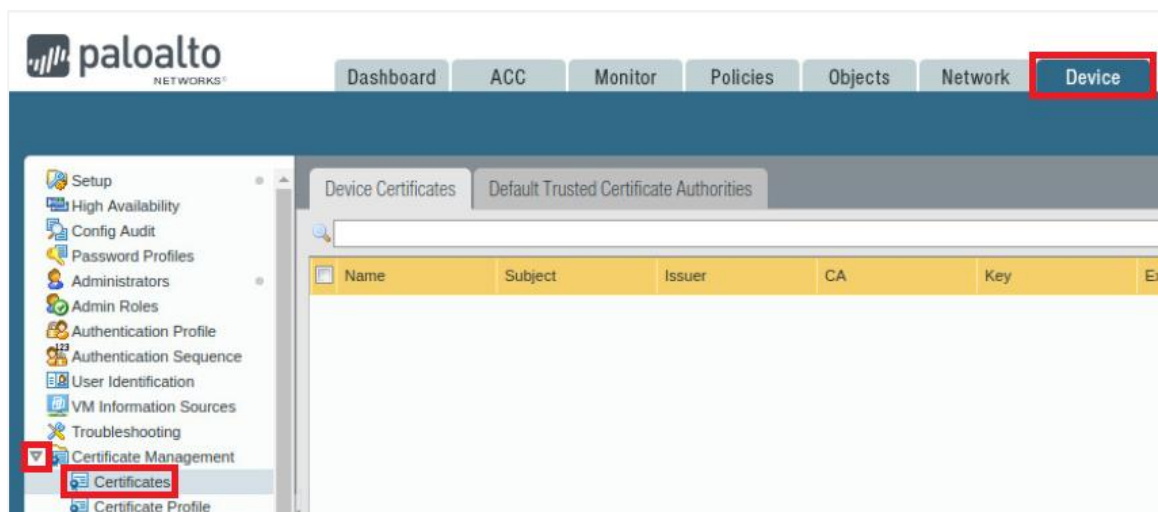
 All Windows
Internet Explorer
Array (pre

- Notice that the download is not blocked because the connection is encrypted, and the virus is hidden. When prompted for the download, click **Cancel** to terminate the download session.
- Close the browser tab.

7.2 Create Two Self-Signed Certificates

In this task, you will generate certificates so that the firewall can decrypt the traffic.

- In the web interface, navigate to **Device > Certificate Management > Certificates**:

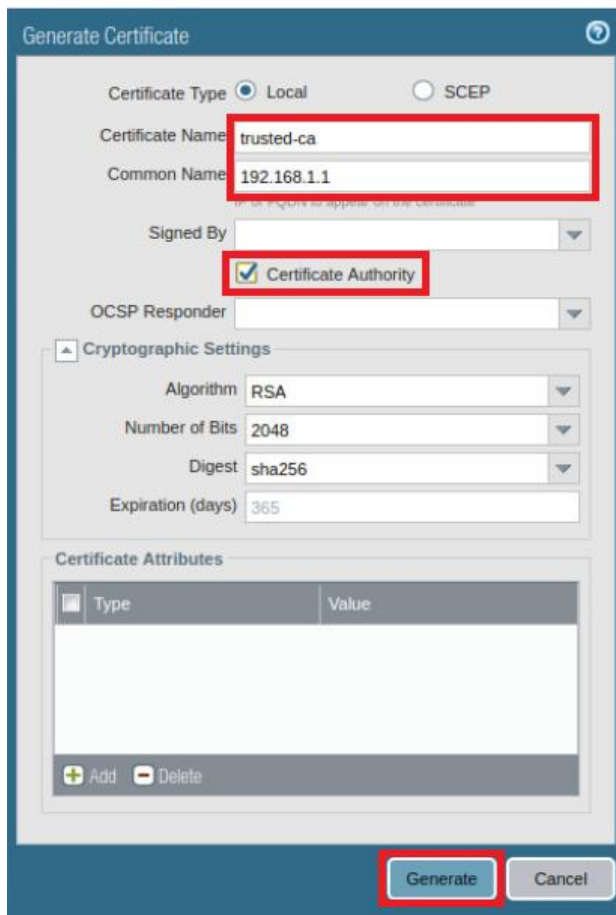


- Click **Generate** at the bottom of the page to create a new CA certificate.



- Configure the following and then click **Generate** to create the certificate.

Parameter	Value
Certificate Name	Type trusted-ca
Common Name	Type 192.168.1.1
Certificate Authority	Select the Certificate Authority checkbox

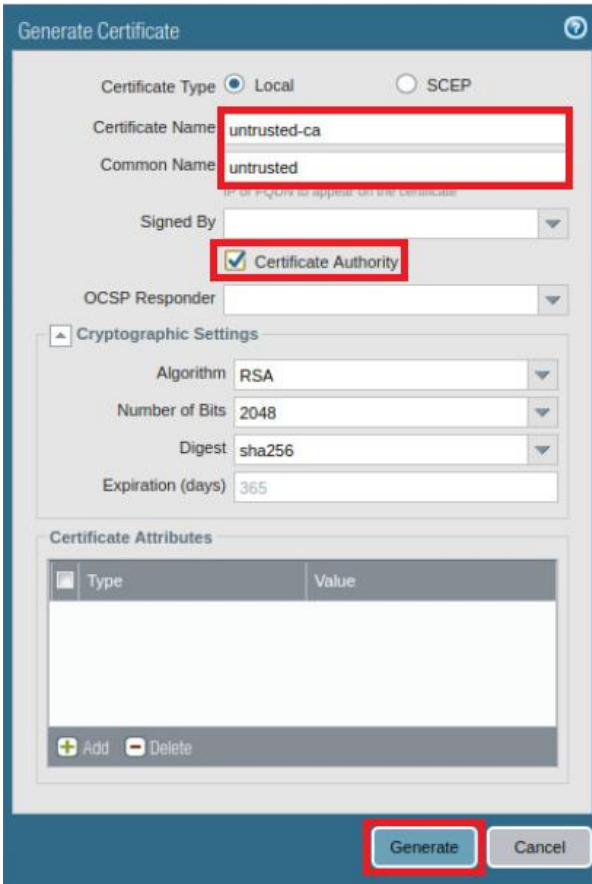


- Click **OK** to close the *Generate Certificate* success window.
- Click **Generate** at the bottom of the page to create another CA certificate.



6. Configure the following and then click **Generate** to create the certificate.

Parameter	Value
Certificate Name	Type untrusted-ca
Common Name	Type untrusted
Certificate Authority	Select the Certificate Authority checkbox



Generate Certificate

Certificate Type: ☒ Local ☐ SCEP

Certificate Name:

Common Name:

Signed By:

☒ Certificate Authority

OCSP Responder:

Cryptographic Settings:

Algorithm:

Number of Bits:

Digest:

Expiration (days):



Certificate Attributes:

Type	Value

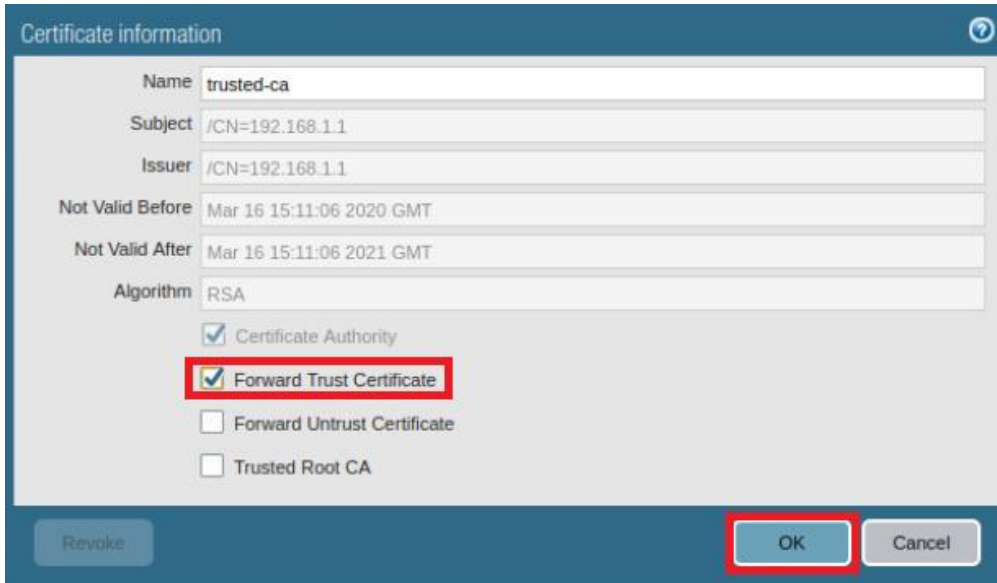
Add Delete

Generate Cancel

7. Click **OK** to dismiss the *Generate Certificate* success window.
8. Click on **trusted-ca** in the list of certificates to edit the certificate information.



	Name	Subject	Issuer	CA
<input checked="" type="checkbox"/>	 trusted-ca	CN = 192.168.1.1	CN = 192.168.1.1	<input checked="" type="checkbox"/>
<input type="checkbox"/>	 untrusted-ca	CN = untrusted	CN = untrusted	<input checked="" type="checkbox"/>

9. In the *Certification Information* window, select the **Forward Trust Certificate** checkbox and click **OK**:

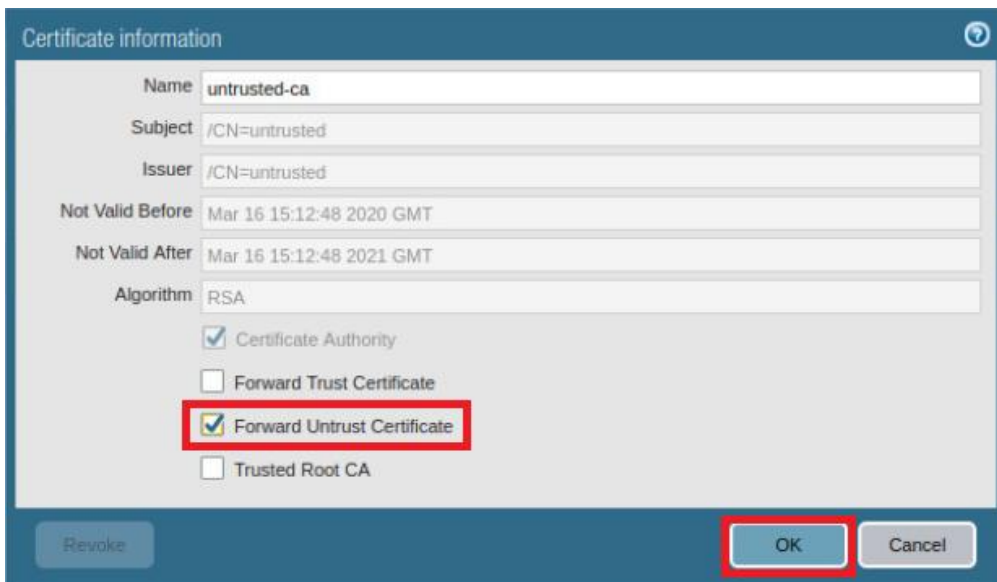


The screenshot shows the 'Certificate information' window for a certificate named 'trusted-ca'. The fields are: Name: trusted-ca, Subject: /CN=192.168.1.1, Issuer: /CN=192.168.1.1, Not Valid Before: Mar 16 15:11:06 2020 GMT, Not Valid After: Mar 16 15:11:06 2021 GMT, Algorithm: RSA. Under the 'Certificate Authority' section, the 'Forward Trust Certificate' checkbox is checked and highlighted with a red box. The 'Forward Untrust Certificate' and 'Trusted Root CA' checkboxes are unchecked. The 'OK' button at the bottom right is also highlighted with a red box.

10. Click on **untrusted-ca** in the list of certificates to edit the certificate information.

<input type="checkbox"/>	Name	Subject	Issuer	CA
<input type="checkbox"/>	 trusted-ca	CN = 192.168.1.1	CN = 192.168.1.1	<input checked="" type="checkbox"/>
<input type="checkbox"/>	 untrusted-ca	CN = untrusted	CN = untrusted	<input checked="" type="checkbox"/>

11. Select the **Forward Untrust Certificate** checkbox and click **OK**.



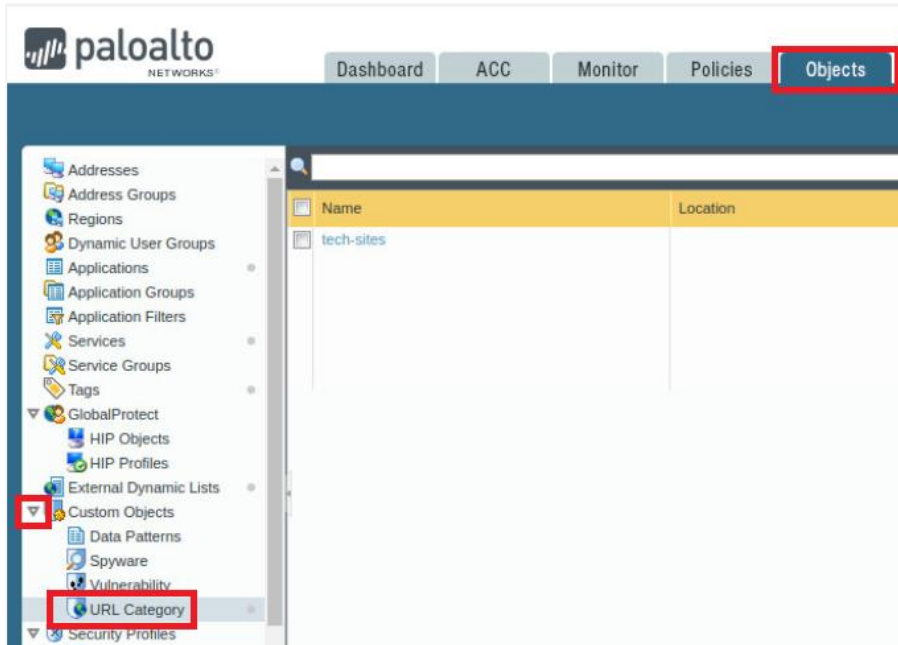
The screenshot shows the 'Certificate information' window for a certificate named 'untrusted-ca'. The fields are: Name: untrusted-ca, Subject: /CN=untrusted, Issuer: /CN=untrusted, Not Valid Before: Mar 16 15:12:48 2020 GMT, Not Valid After: Mar 16 15:12:48 2021 GMT, Algorithm: RSA. Under the 'Certificate Authority' section, the 'Forward Untrust Certificate' checkbox is checked and highlighted with a red box. The 'Forward Trust Certificate' and 'Trusted Root CA' checkboxes are unchecked. The 'OK' button at the bottom right is also highlighted with a red box.

12. Leave the firewall web interface open to continue with the next task.

7.3 Create a Custom Decryption URL Category

In this task, you will create a custom *URL Category* to ensure that only intended traffic is being decrypted.

1. In the web interface, navigate to **Objects > Custom Objects > URL Category**.

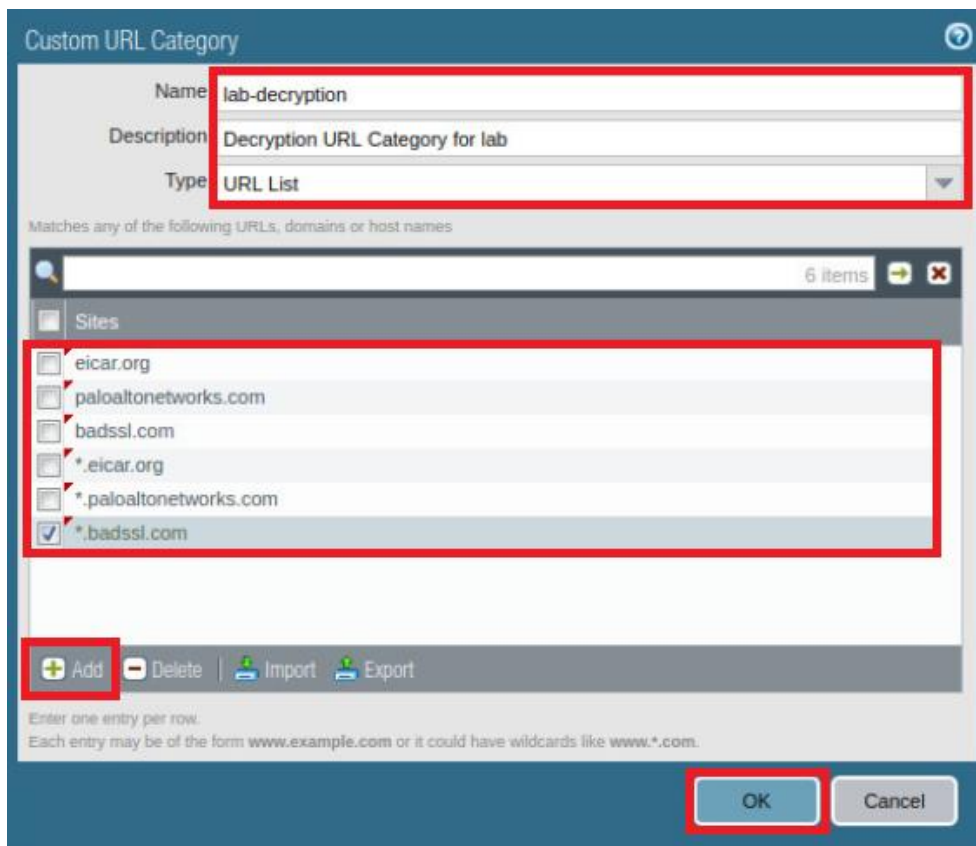


2. Click **Add** to open the *Custom URL Category* configuration window.



3. In the *Custom URL Category* window, configure the following, then click **OK**.

Parameter	Value
Name	Type 1ab-decryption
Description	Type decryption URL Category for 1ab
Type	Verify that URL List is selected
Sites	Click Add and type the following websites: eicar.org paloaltonetworks.com badssl.com *.eicar.org *.paloaltonetworks.com *.badssl.com



Custom URL Category

Name: lab-decryption

Description: Decryption URL Category for lab

Type: URL List

Matches any of the following URLs, domains or host names

6 items

Sites

- ☐ eicar.org
- ☐ paloaltonetworks.com
- ☐ badssl.com
- ☐ *.eicar.org
- ☐ *.paloaltonetworks.com
- ☒ *.badssl.com

+ Add - Delete Import Export

Enter one entry per row.
Each entry may be of the form www.example.com or it could have wildcards like www.*.com.

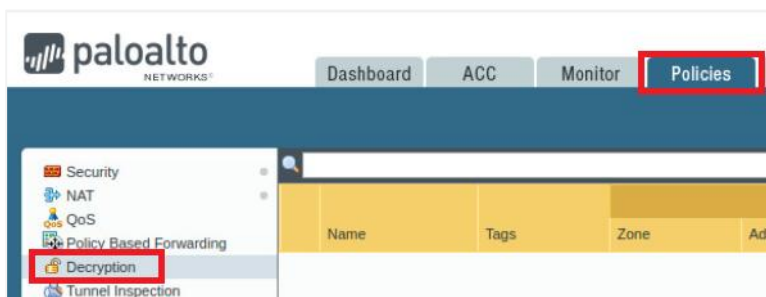
OK Cancel

4. Leave the firewall web interface open to continue with the next task.

7.4 Create a Decryption Policy

In this task, you will create a *Decryption Policy* to decrypt traffic that matches the *Custom URL Category* you created in the previous task.

1. In the web interface, select **Policies > Decryption**.

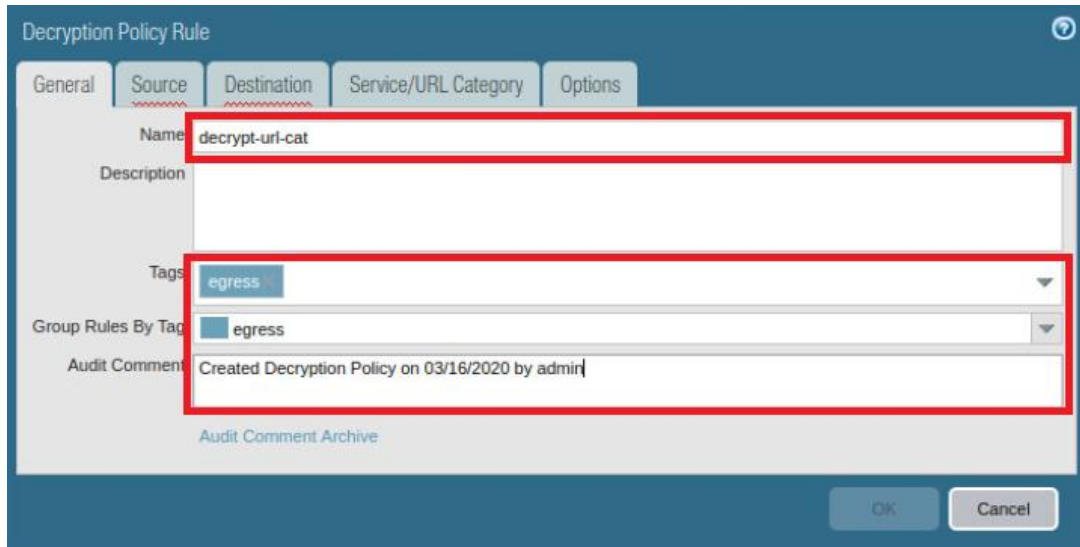


2. Click **Add** to create a Decryption Policy Rule.



3. In the *Decryption Policy Rule* window, while on the **General** tab, configure the following:

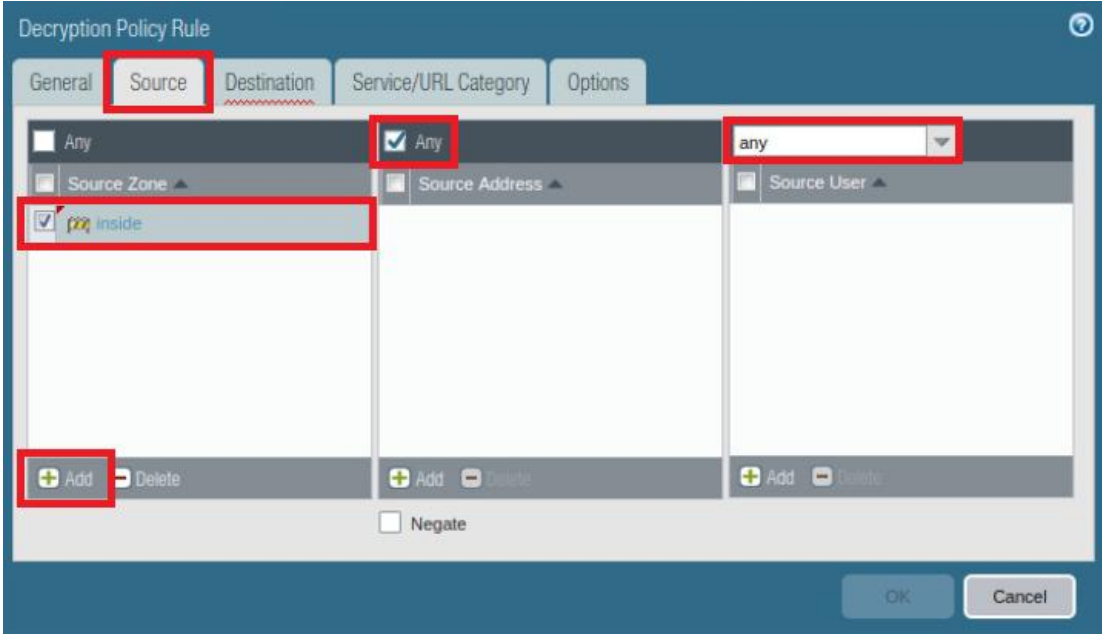
Parameter	Value
Name	Type decrypt-url-cat
Tags	Select egress from the dropdown list
Group Rules By Tag	Select egress from the dropdown list
Audit Comment	Type Created Decryption Policy on <date> by admin



The screenshot shows the 'Decryption Policy Rule' window with the 'General' tab selected. The 'Name' field is filled with 'decrypt-url-cat'. The 'Tags' dropdown menu is open, showing 'egress' as the selected option. The 'Group Rules By Tag' dropdown menu is also open, showing 'egress' as the selected option. The 'Audit Comment' field contains the text 'Created Decryption Policy on 03/16/2020 by admin'. The 'OK' and 'Cancel' buttons are visible at the bottom right of the window.

4. In the *Decryption Policy Rule* window, click the **Source** tab and configure the following:

Parameter	Value
Source Zone	Click Add and select inside from the dropdown list
Source Address	Verify that the Any checkbox is selected
Source User	Verify that any is selected



Decryption Policy Rule

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

☐ Any ☒ Any any

☒ inside

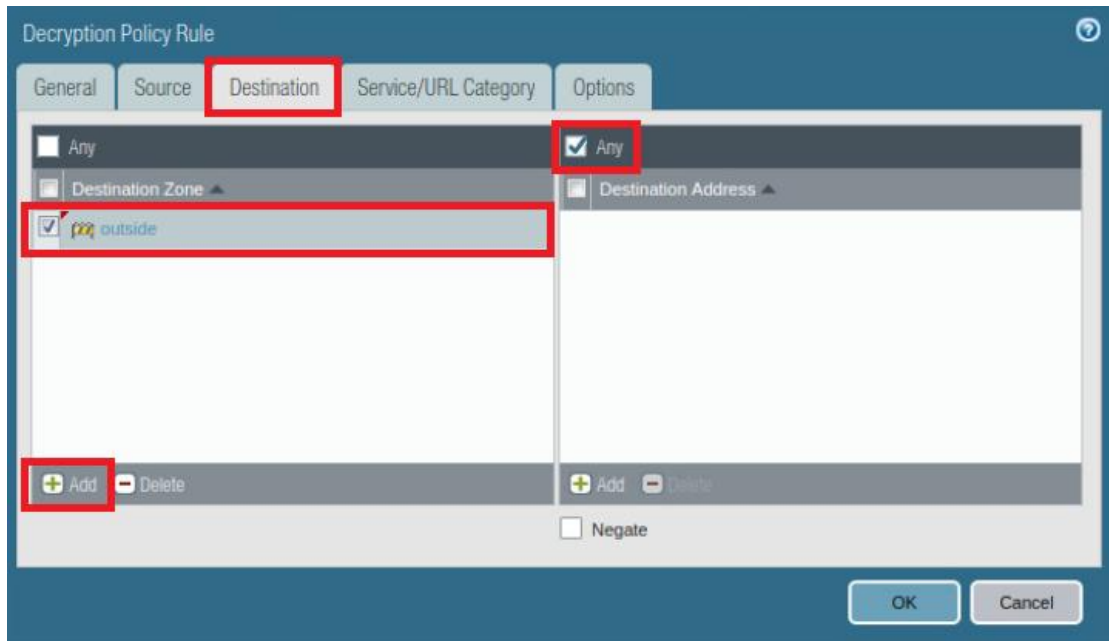
☐ Add Delete ☐ Add Delete ☐ Add Delete

☐ Negate

OK Cancel

5. In the *Decryption Policy Rule* window, click the **Destination** tab and configure the following:

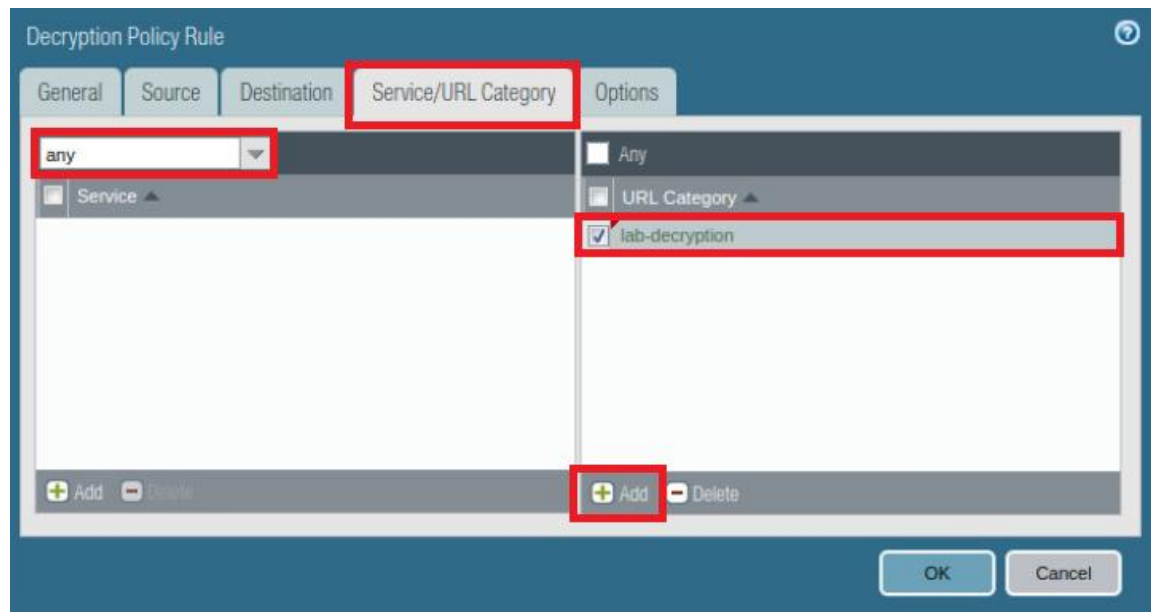
Parameter	Value
Destination Zone	Click Add and select outside from the dropdown list
Destination Address	Verify that the Any checkbox is selected



The screenshot shows the 'Decryption Policy Rule' window with the 'Destination' tab selected. The 'Destination Zone' list contains 'outside' with a checkmark. The 'Destination Address' list contains 'Any' with a checkmark. The 'Add' button is highlighted in the bottom left. The 'Negate' checkbox is unchecked. The 'OK' and 'Cancel' buttons are at the bottom right.

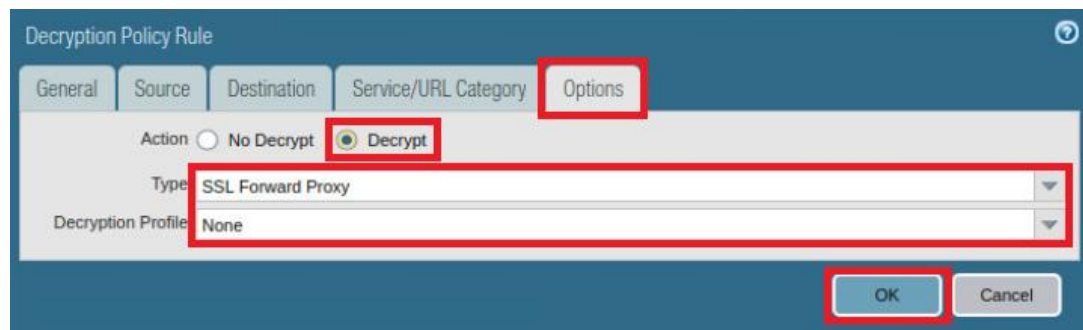
6. In the *Decryption Policy Rule* window, click the **Service/URL Category** tab and configure the following:

Parameter	Value
Service	Verify that any is selected
URL Category	Click Add and select lab-decryption from the dropdown list



7. In the *Decryption Policy Rule* window, click the **Options** tab, configure the following and then click **OK**.

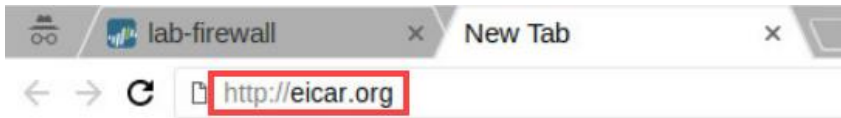
Parameter	Value
Action	Select the Decrypt radio button
Type	Verify that SSL Forward Proxy is selected
Decryption Policy	Verify that None is selected



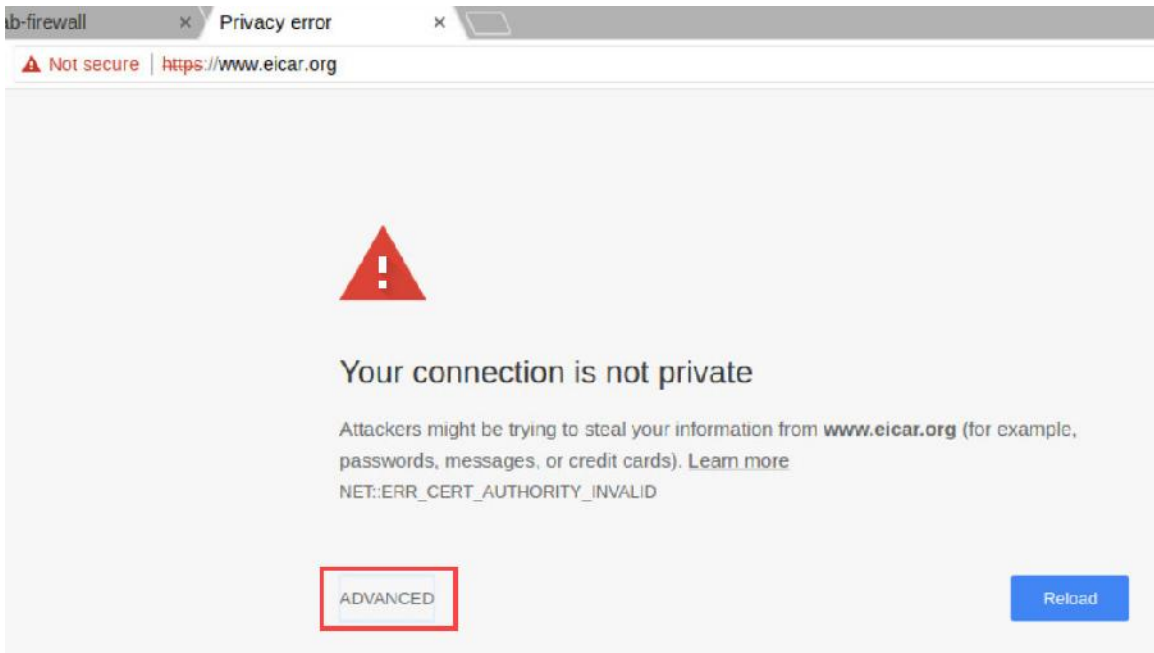
8. **Commit** all changes.

7.5 Test AV Security Profile with the Decryption Policy

1. Open a new tab in **Chromium Web Browser** and browse to **http://eicar.org**.

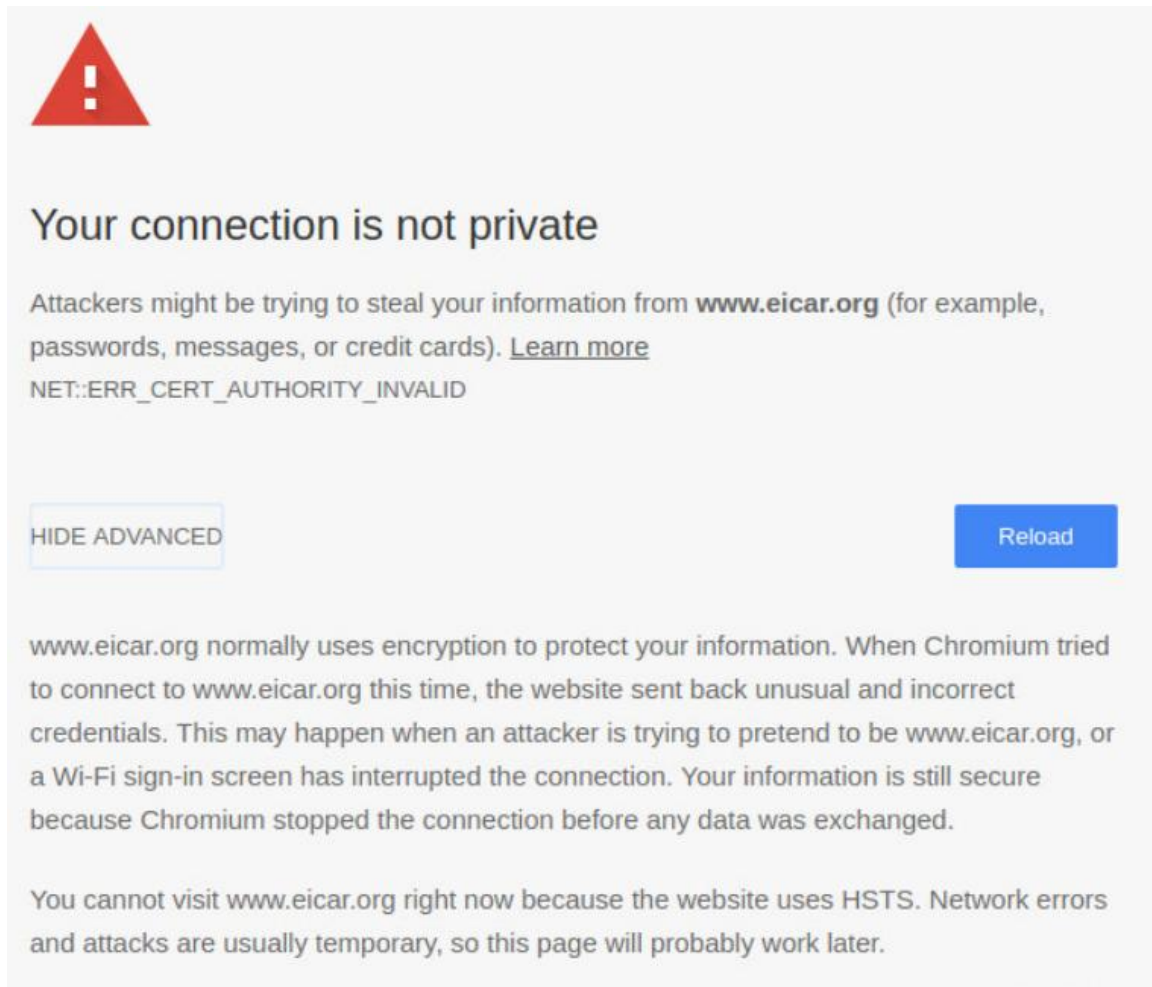


2. Notice a certificate issue is displayed. Continue moving forward by clicking on the **ADVANCED** hyperlink.

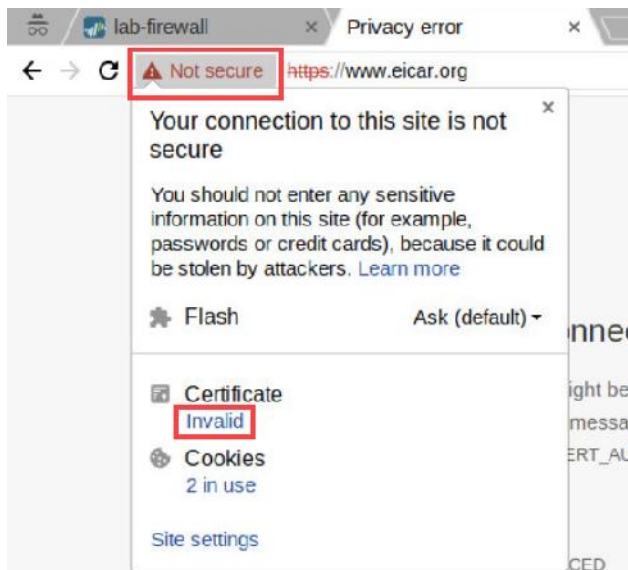


The endpoint (Client desktop) does not trust the certificate generated by the firewall (192.168.1.1).

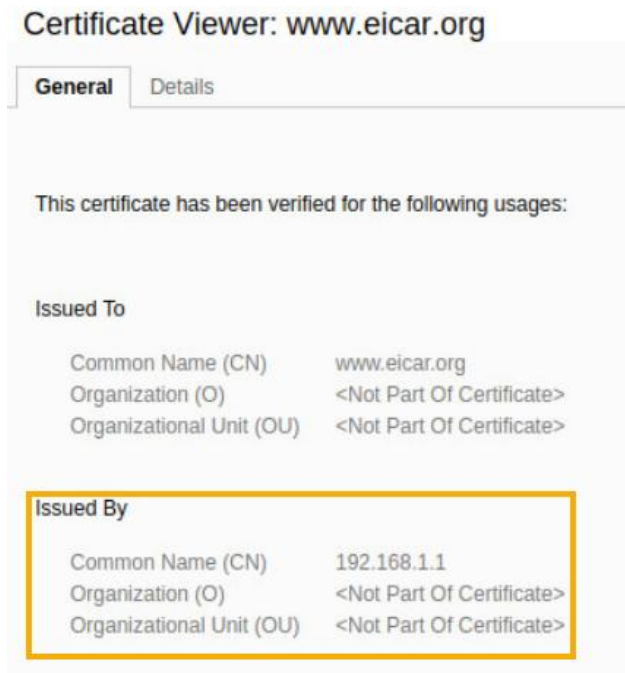
- Review the message presented by the Chrome browser, stating that you are restricted from being able to proceed further to the website.



- In the address bar, click on **Not secure** followed by clicking on **Invalid** underneath **Certificate**.



5. Notice who the issuer is by looking in the *Issued By* section.



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 browser trusts certificates issued by the firewall.

6. Close the browser tab.

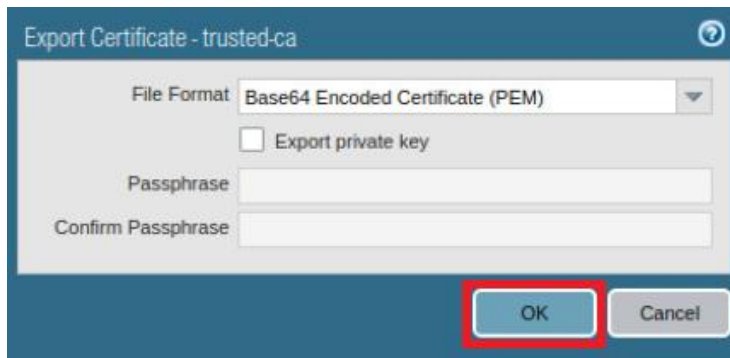
7.6 Export the Firewall Certificate

1. Change focus back to the firewall’s web interface and navigate to **Device > Certificate Management > Certificates**.

2. Check the checkbox for **trusted-ca**, then click **Export Certificate** to open the Export Certificate configuration window.



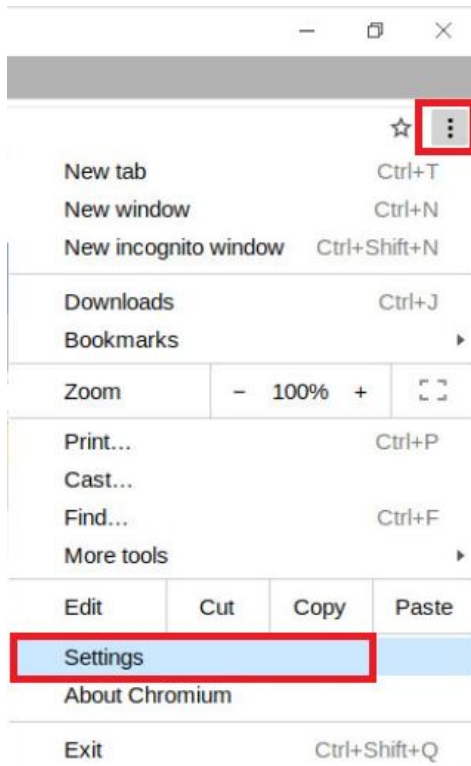
3. In the *Export Certificate - trusted-ca* window, click **OK** to export the *trusted-ca* certificate.



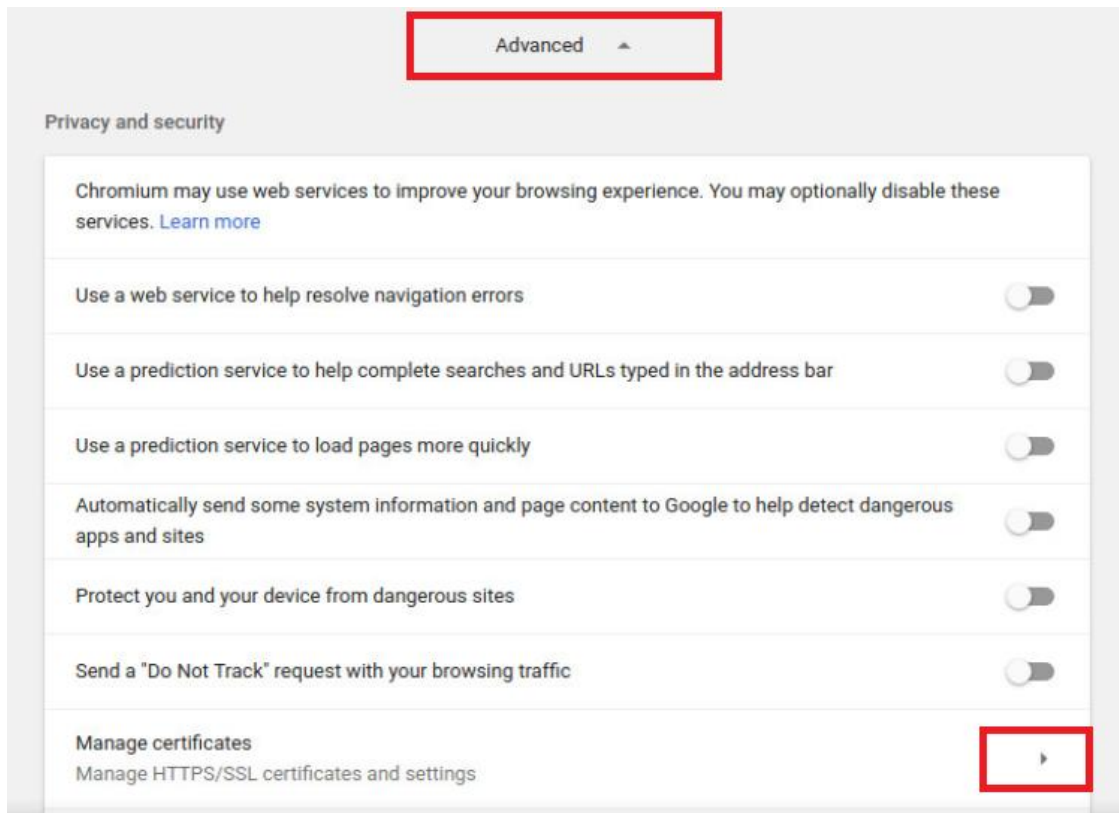
4. In the *Save File* window, choose the default **~/Downloads** and click **Save**.
5. Leave the firewall web interface open to continue with the next task.

7.7 Import the Firewall Certificate

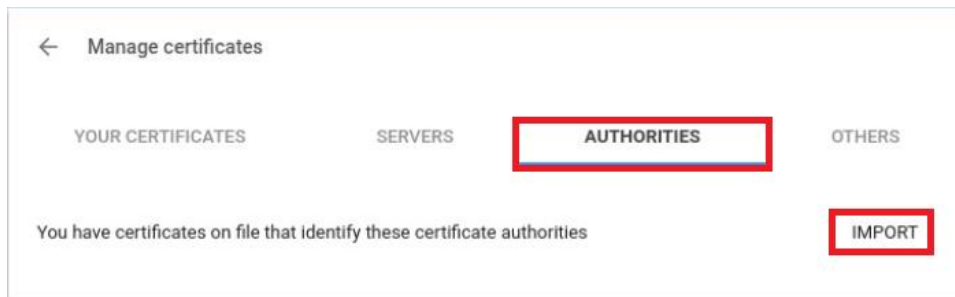
1. In the *Chromium Web Browser*, click **Customize and Control Chromium** and then click **Settings**.



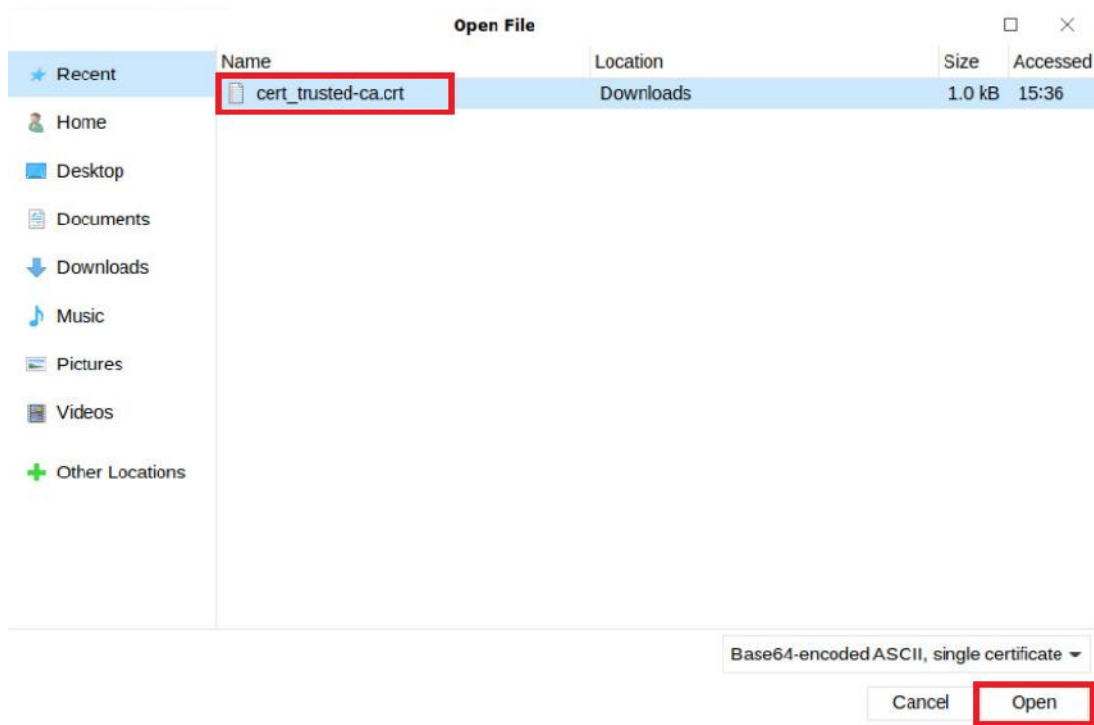
2. Scroll down, click **Advanced** to expand the view, and then click **Manage certificates**.



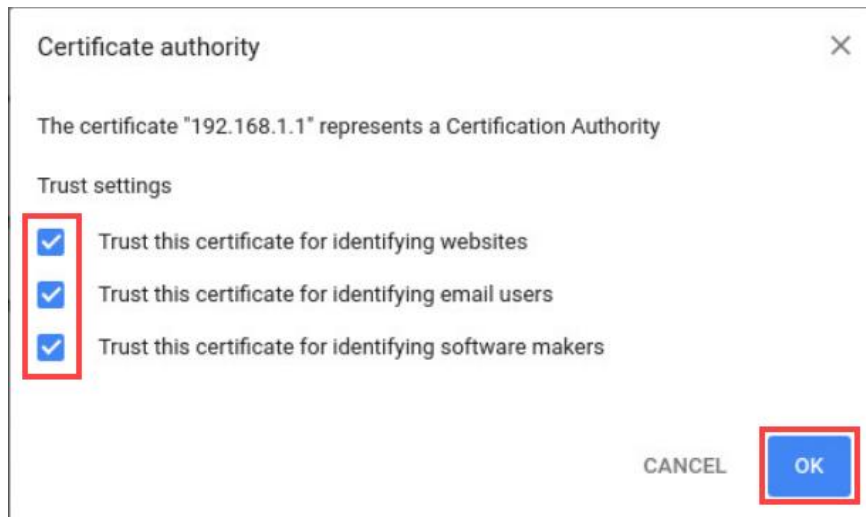
3. In the *Manage certificates* window, click **AUTHORITIES**, and then click **IMPORT**.



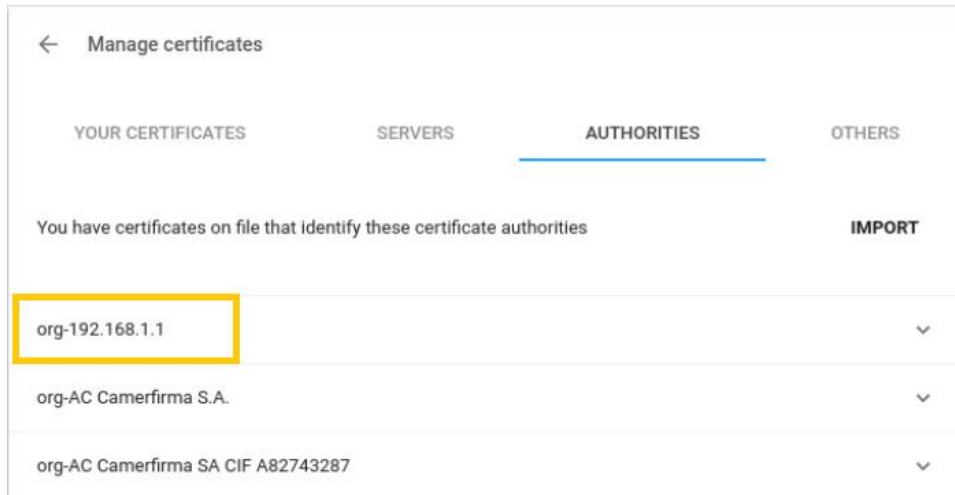
4. Select **cert_trusted-ca.crt**, then click **Open**.



5. In the *Certificate Authority* window, check all the boxes and then click **OK**.



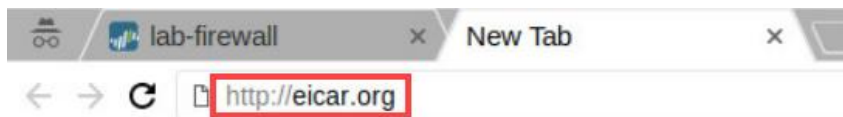
6. Notice that the *trusted-ca* certificate is now imported.



7. Close the **Settings – Chromium** browser window.

7.8 Test the Decryption Policy

1. Open a new tab in **Chromium Web Browser** and browse to <http://eicar.org>.



2. Click the **Download Anti Malware Testfile** image in the upper-right corner of the webpage.



3. Scroll down and within the *Download* area at the bottom of the page, click the **eicar.com** file to download the file using the SSL-enabled HTTPS protocol.

Download area using the standard protocol HTTP			
– Sorry, HTTP download 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

Notice that the *eicar* test file is detected and blocked.



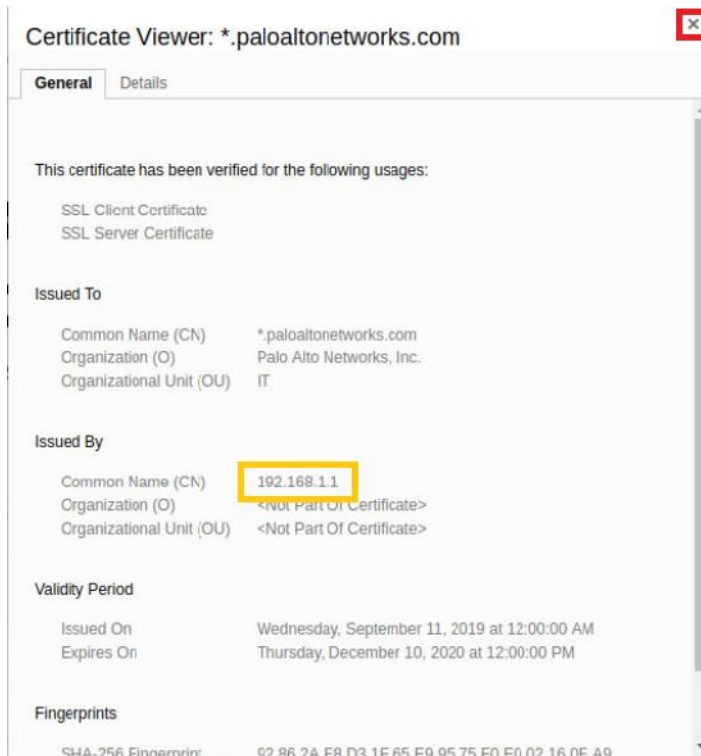
4. In the same browser tab, browse to **https://www.paloaltonetworks.com**. Notice that there is no certificate warning, and the page is displayed correctly.



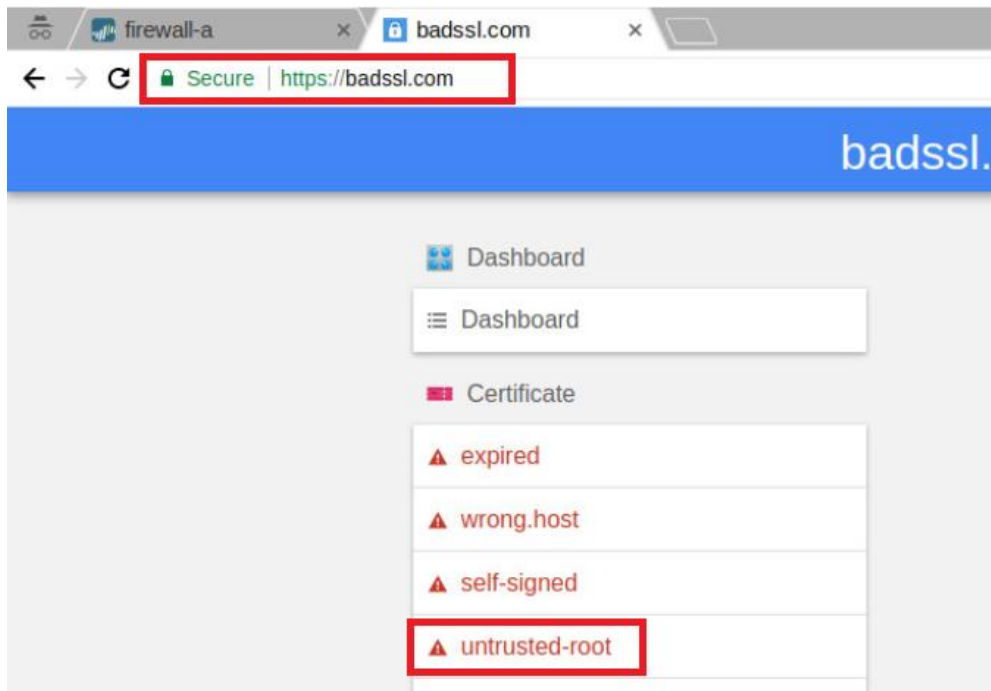
5. Click the **Secure** icon next to the URL in the browser and click **Valid** under Certificate.



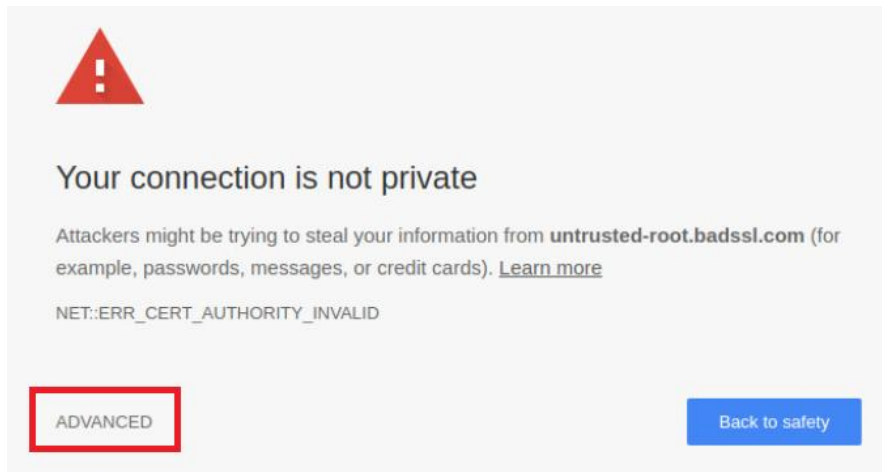
- Notice that the certificate was issued by **192.168.1.1**, click the **X** to close the *Certificate View: *.paloaltonetworks.com* window.



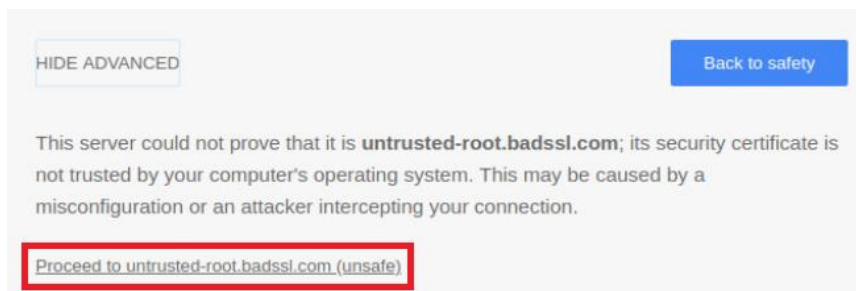
- In the same browser tab, browse to **https://www.badssl.com** and then click on **untrusted-root**.



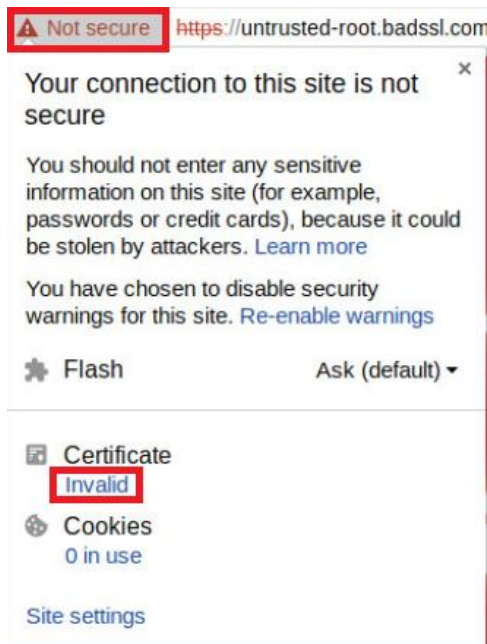
8. Notice that *Your connection is not private* is now displayed. Click on the **Advanced** link.



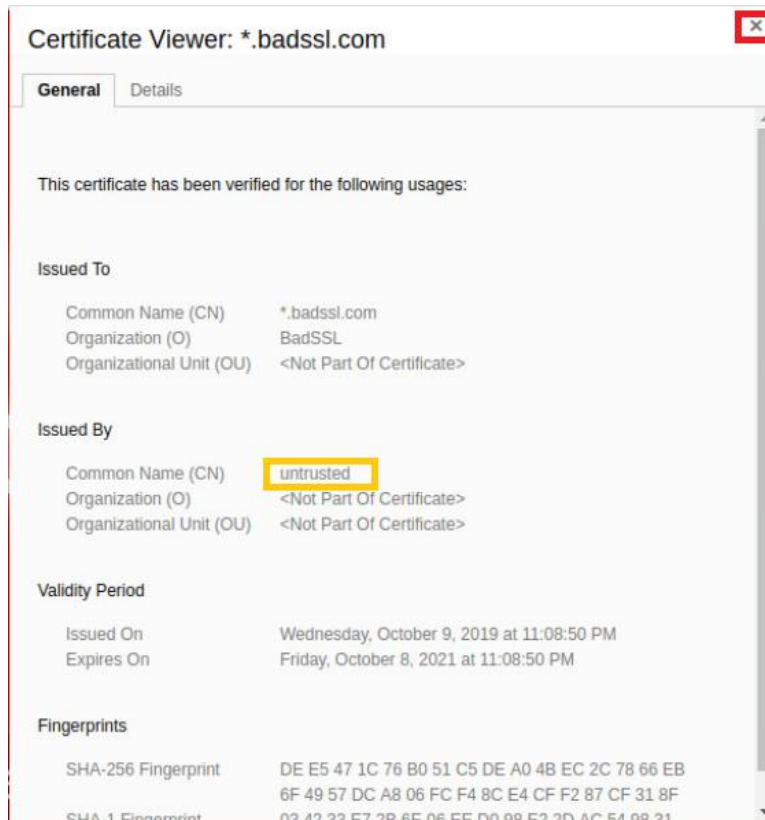
9. Click the **Proceed to untrusted-root.badssl.com (unsafe)** link.



10. Click the **Not Secure** link near the URL and click **Invalid** under Certificate.



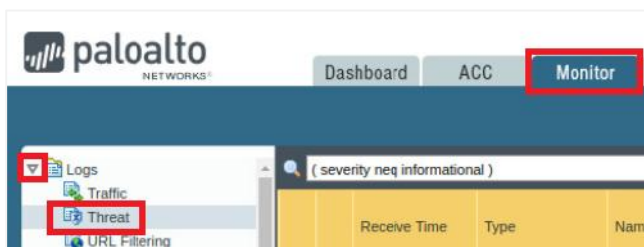
11. Notice that the certificate is still signed by the firewall. However, it was signed with the untrusted certificate. Click the **X** to close the *Certificate View: *.badssl.com* window.



12. Close the browser tab.

7.9 Review Logs

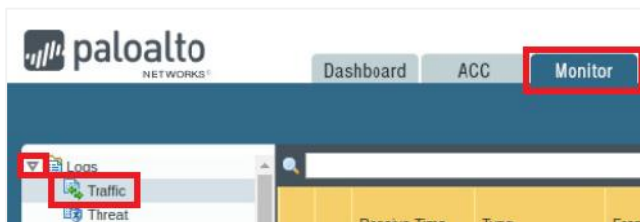
1. Change focus to the firewall's web interface and navigate to **Monitor > Logs > Threat**.



2. Clear any existing filters and notice that there is an entry for when the connection was reset in the browser.

	Receive Time	Type	Name	From Zone	To Zone	Source address
	03/16 16:06:09	spyware	Suspicious TLS Evasion Found	inside	outside	192.168.1.20
	03/16 16:08:08	spyware	Suspicious HTTP Evasion Found	inside	outside	192.168.1.20
	03/16 16:07:23	virus	Eicar Test File	inside	outside	192.168.1.20
	03/16 16:06:53	virus	Eicar Test File	inside	outside	192.168.1.20
	03/16 16:06:46	virus	Eicar Test File	inside	outside	192.168.1.20
	03/16 16:06:46	virus	Eicar Test File	inside	outside	192.168.1.20
	03/16 16:01:40	spyware	Suspicious HTTP Evasion Found	inside	outside	192.168.1.20

3. Select **Monitor > Logs > Traffic**.



4. Clear any existing filters and then type **(flags has proxy)** in the filter text box. Press **Enter**. This filter flags only traffic entries that were decrypted.

(flags has proxy)										
	Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	Dynamic User Group	In Port	Application
	03/16 16:34:01	deny	inside	outside	192.168.1.254		34.96.64.34		443	ss
	03/16 16:33:01	deny	inside	outside	192.168.1.254		34.96.64.34		443	ss
	03/16 16:32:01	deny	inside	outside	192.168.1.254		34.96.64.34		443	ss
	03/16 16:31:01	deny	inside	outside	192.168.1.254		34.96.64.34		443	ss
	03/16 16:30:01	deny	inside	outside	192.168.1.254		34.96.64.34		443	ss
	03/16 16:29:01	deny	inside	outside	192.168.1.254		34.96.64.34		443	ss
	03/16 16:28:01	deny	inside	outside	192.168.1.254		34.96.64.34		443	ss
	03/16 16:27:47	auth	inside	outside	192.168.1.20		104.154.88.105		443	webServices



If the *Decrypted* column is not present, hover the mouse over *Receive Time* and click the **dropdown** arrow and check the checkbox for **Decrypted** to add the column view.

5. Leave the firewall web interface open to continue with the next task.

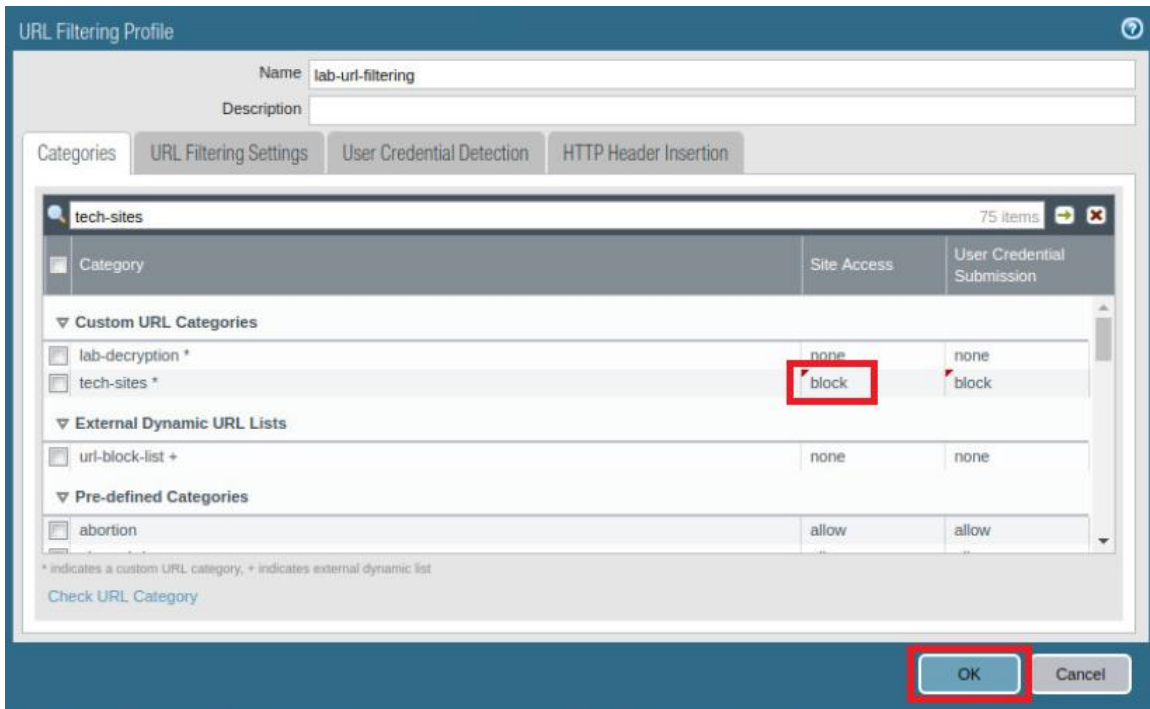
7.10 Test URL Filtering with Decryption

1. In the web interface, select **Objects > Security Profiles > URL Filtering**.

- Click on **lab-url-filtering** to open the object.

Name	Location	Site Access
default	Predefined	Allow Categories (58) Alert Categories (4) Continue Categories (0) Block Categories (10) Override Categories (0)
lab-url-filtering		Allow Categories (71) Alert Categories (0) Continue Categories (0) Block Categories (3) Override Categories (0)

- In the *URL Filtering Profile* window, while on the *Categories* tab, locate *tech-sites* from the list without utilizing the search feature and change **Site Access** to **block** and then click **OK**.



URL Filtering Profile

Name: lab-url-filtering

Description:

Categories | URL Filtering Settings | User Credential Detection | HTTP Header Insertion

tech-sites 75 items

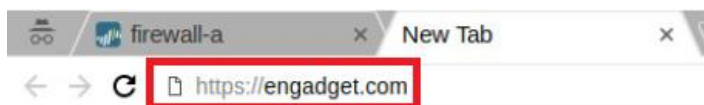
Category	Site Access	User Credential Submission
lab-decryption *	none	none
tech-sites *	block	block
url-block-list +	none	none
abortion	allow	allow

* indicates a custom URL category, + indicates external dynamic list

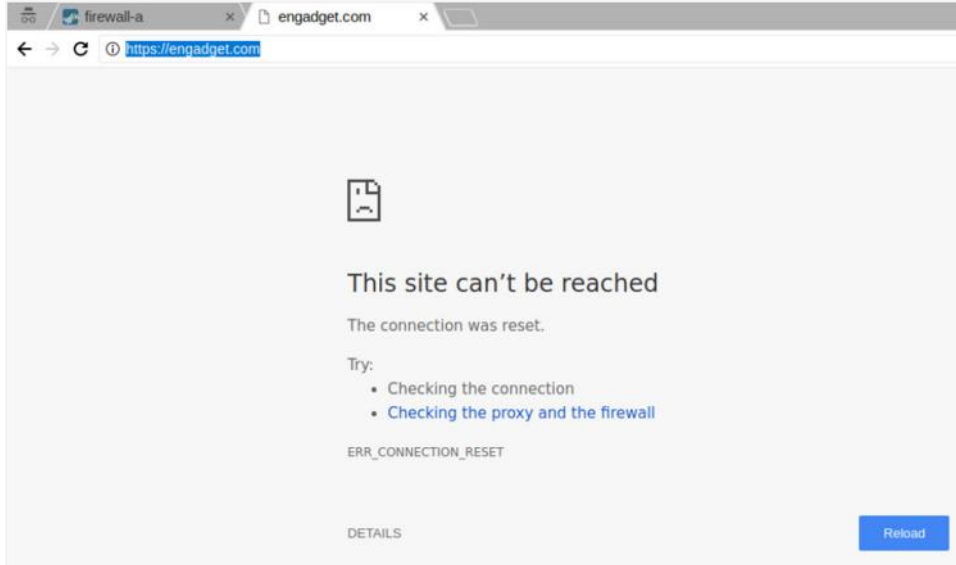
Check URL Category

OK Cancel

- Commit** all changes.
- Open a new tab in **Chromium Web Browser** and browse to **https://engadget.com**.



6. Notice that *Engadget* is now blocked because the site can be identified and blocked per the *URL Filtering Profile*.



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