PALO ALTO NETWORKS - EDU-210

Lab 7: Decryption

Document Version: 2017-09-29

Contents

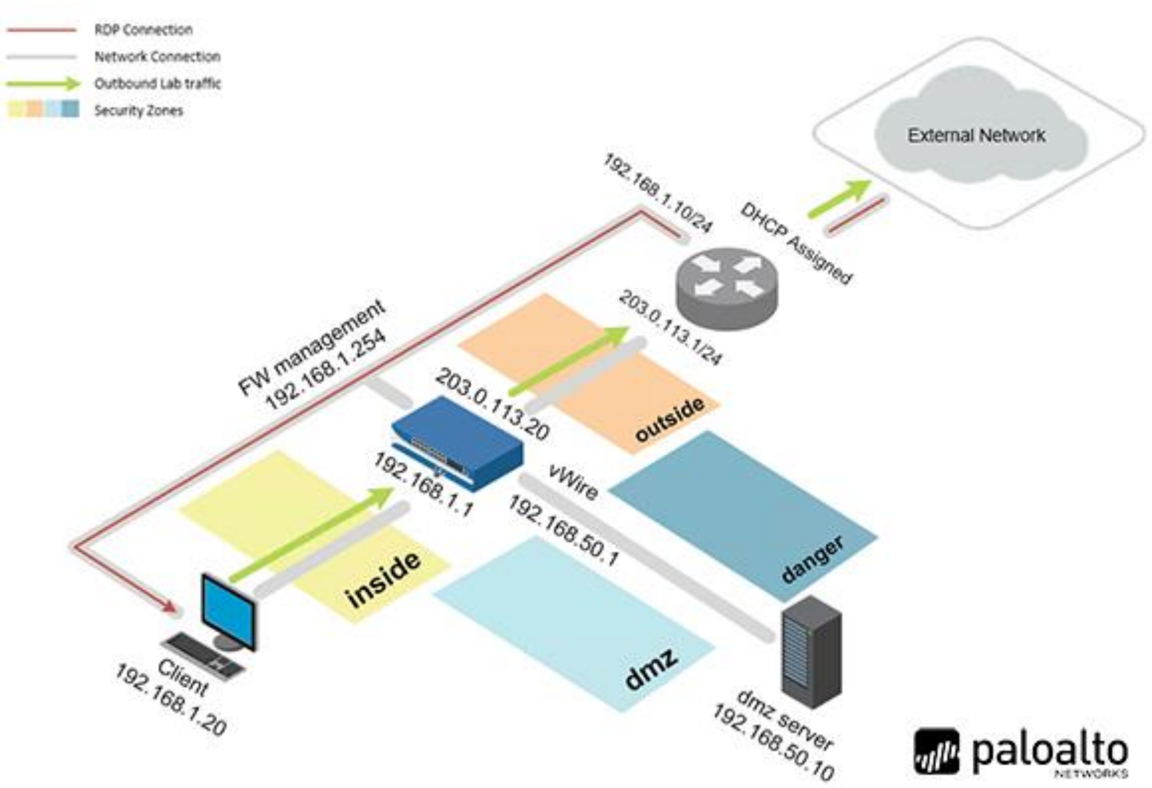
Introduction

As you browsed through the logs you noticed that there was a lot of ssl traffic and when you were testing the system and attempted to download an Eicar file from one of the ssl links that it was allowed. The CSO has determined that we need to inspect all traffic within the acceptable risk categories. You need to setup the system to therefore 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



Lab Settings

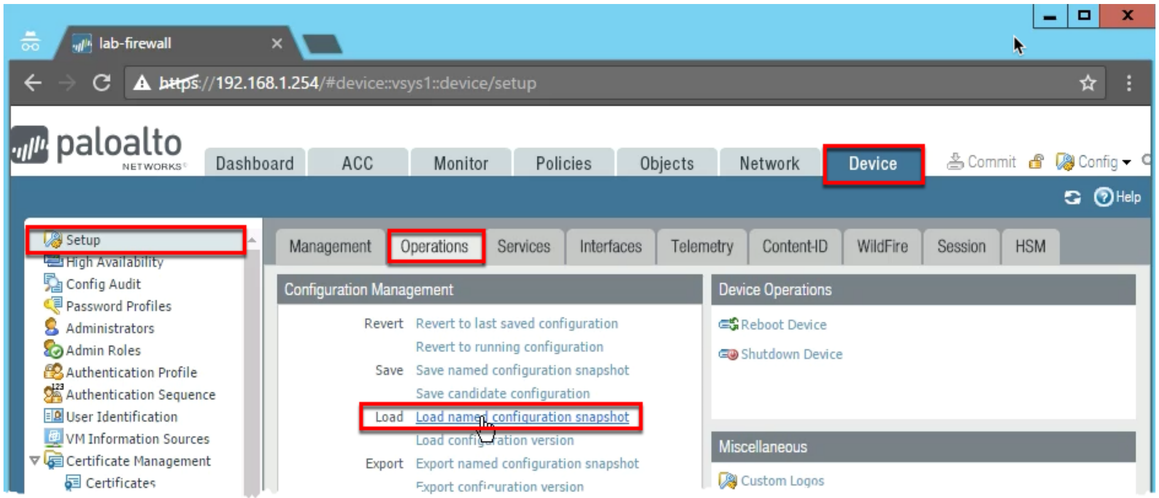
The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Client – Windows 2012 R2	192.168.1.20	lab-user	Pal0Alt0
Firewall – PA-VM	192.168.1.254	admin	admin

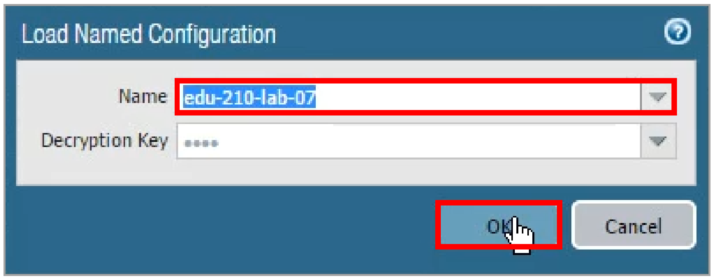
7 Lab: Decryption

7.0 Load Lab Configuration

1. In the WebUI select **Device > Setup > Operations**.
2. Click **Load named configuration snapshot**:



3. Select **edu-210-lab-07** and click **OK**.


Load Named Configuration

Name edu-210-lab-07

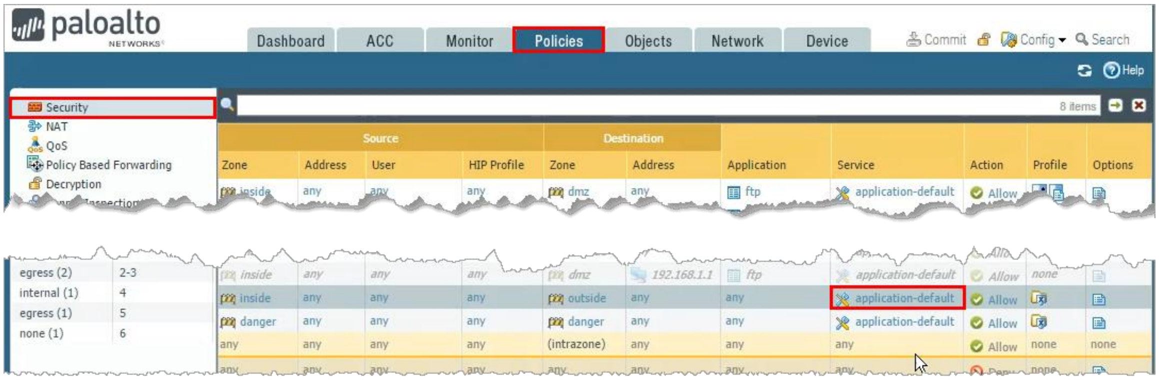
Decryption Key ••••

4. Click **Close**.
5. **Commit** all changes.

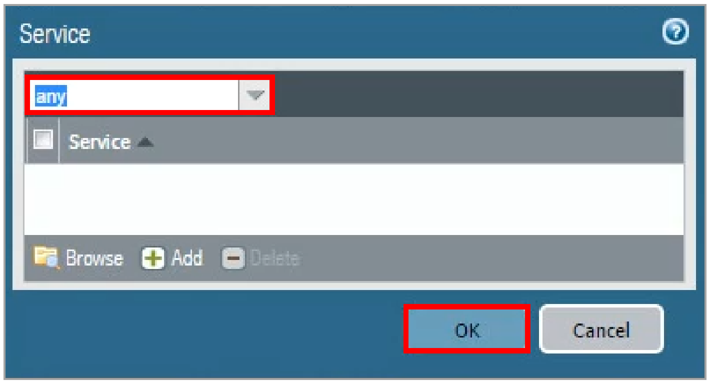
7.1 Test Firewall Behavior Without Decryption

For this lab, you will use the Internet Explorer browser. Chrome has its own virus detection system and Firefox has its own certificate repository.

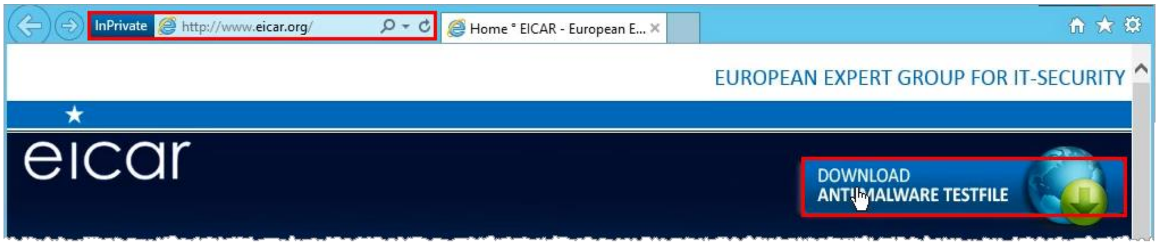
1. Select **Policies > Security**, click **application-default** in the Service column in the egress-outside-content-id Security policy rule.



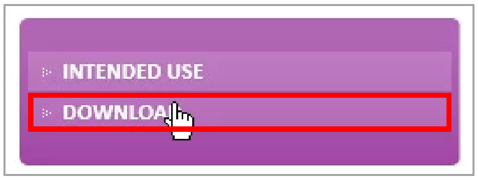
2. In the Service window, change application-default to **any** then click **OK**.



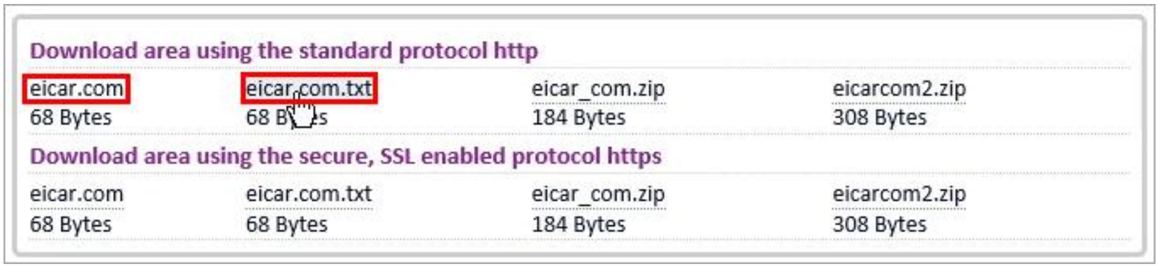
3. **Commit** all changes.
4. On the Windows desktop, open a browser in private/incognito mode and browse to `http://www.eicar.org`. Click the **DOWNLOAD ANTIMALWARE TESTFILE** image in the top-right corner:


InPrivate
http://www.eicar.org/
Home ° EICAR - European E...
EUROPEAN EXPERT GROUP FOR IT-SECURITY
eicar
DOWNLOAD ANTIMALWARE TESTFILE

5. Click the **Download** link on the left of the web page.



6. Within the Download area at the bottom of the page, click either the **eicar.com** or the **eicar.com.txt** file to download the file using the standard HTTP protocol and not the SSL-encrypted HTTPS protocol. The firewall will not be able to detect the viruses in an HTTPS connection until decryption is configured.



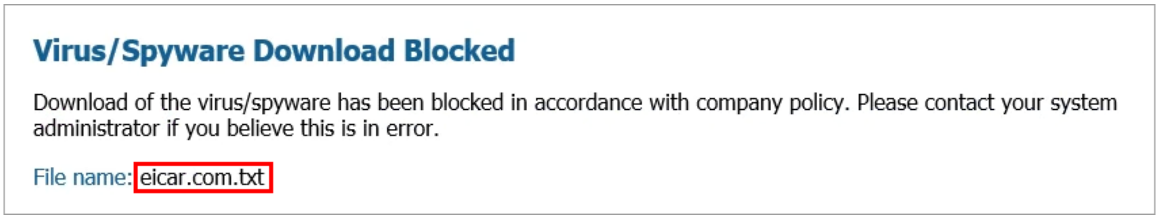
Download area using the standard protocol http

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

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

7. You should observe an error message similar to the following.

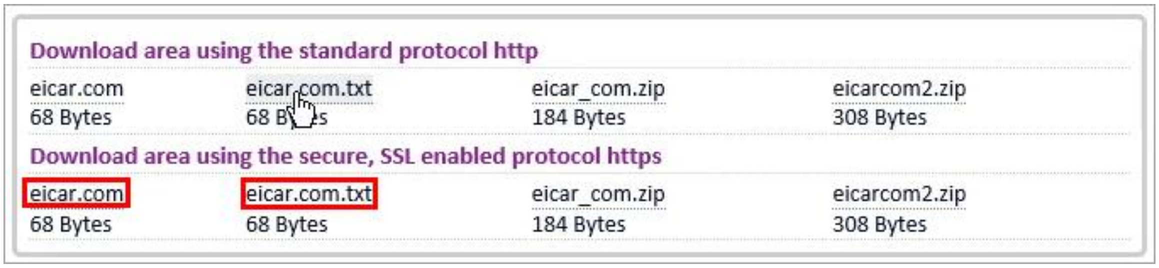


Virus/Spyware Download Blocked

Download of the virus/spyware has been blocked in accordance with company policy. Please contact your system administrator if you believe this is in error.

File name: eicar.com.txt

8. Go back in the browser and download one of the test files using HTTPS:



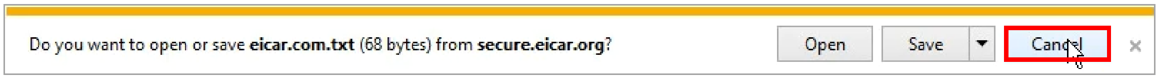
Download area using the standard protocol http

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

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

9. Notice that the download is not blocked because the connection is encrypted and the virus is hidden. If prompted, **Save** the file. Do *not* open or run the file.



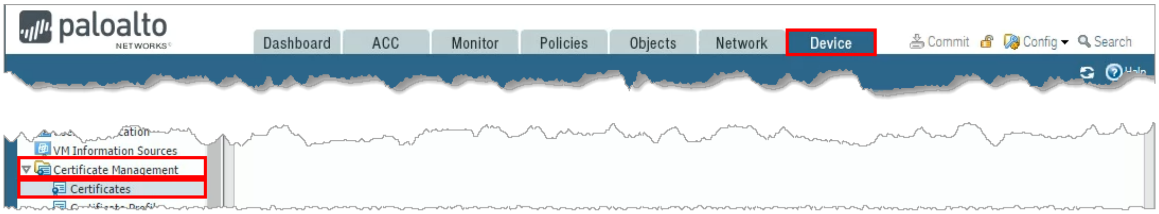
Do you want to open or save **eicar.com.txt** (68 bytes) from **secure.eicar.org**?

10. **Close** all browser windows except for the firewall WebUI.

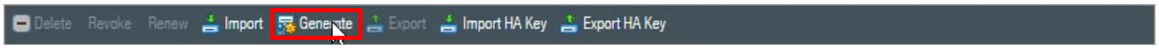
7.2 Create Two Self-Signed Certificates

Certificates need to be generated so that the firewall can decrypt traffic.

1. In the WebUI select **Device > Certificate Management > Certificates**:

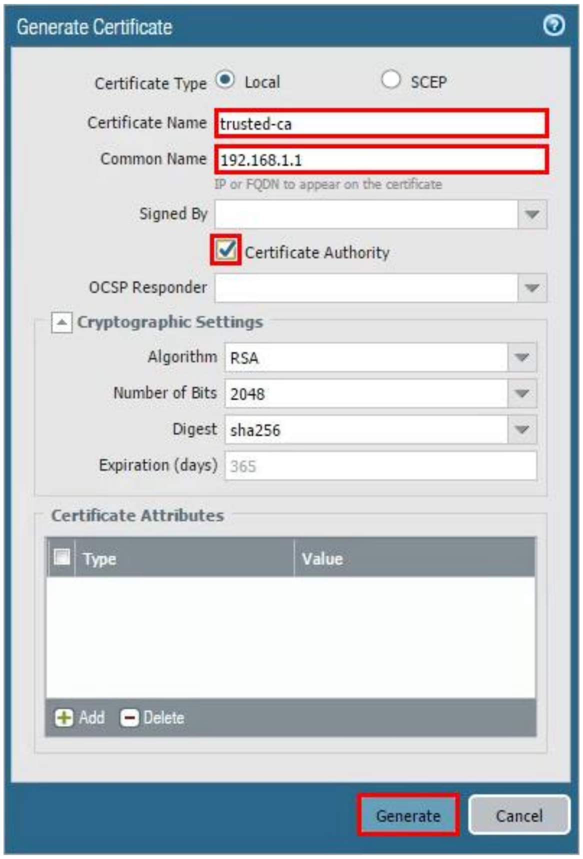


2. Click **Generate** at the bottom of the page to create a new CA certificate.



3. Configure the following, then click **Generate** to create the certificate.

Parameter	**Value**
Certificate Name	`trusted-ca`
Common Name	`192.168.1.1`
Certificate Authority	☑ Certificate Authority


Generate Certificate

Certificate Type ● Local ○ SCEP

Certificate Name: trusted-ca

Common Name: 192.168.1.1

IP or FQDN to appear on the certificate

Signed By:

☑ Certificate Authority

OCSP Responder:

Cryptographic Settings

Algorithm: RSA

Number of Bits: 2048

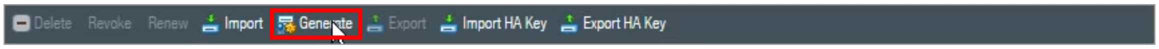
Digest: sha256

Expiration (days): 365

Certificate Attributes

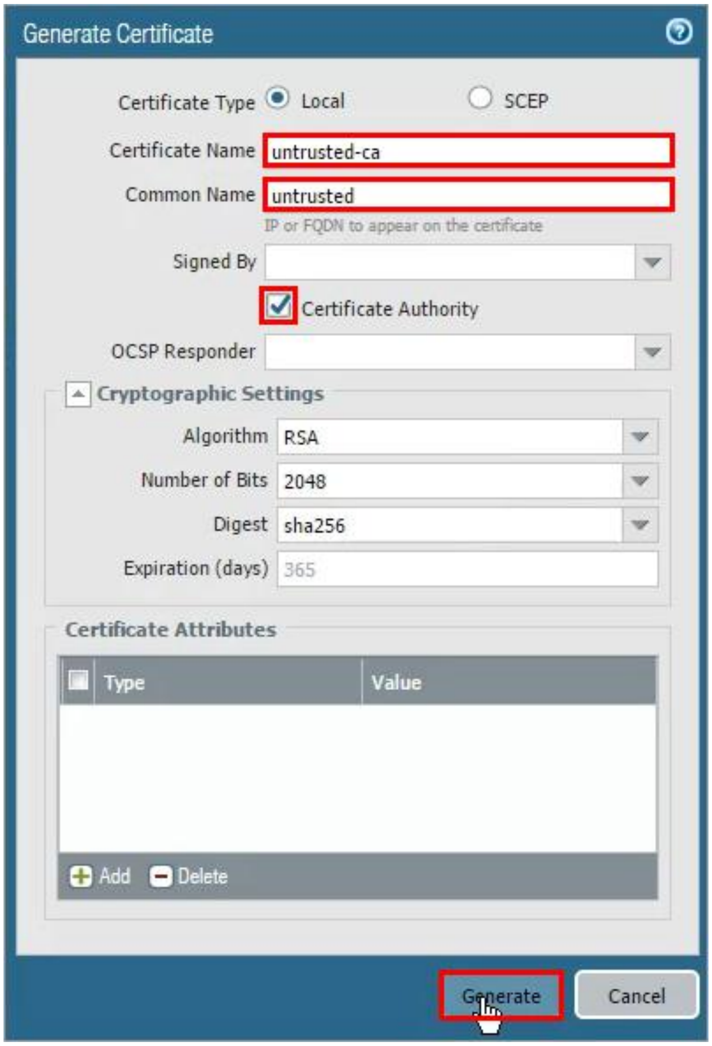
□ Type	Value

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



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

Parameter	Value
Certificate Name	`untrusted-ca`
Common Name	`untrusted`
Certificate Authority	☑ Certificate Authority



Certificate Type ● Local ○ SCEP

Certificate Name: untrusted-ca

Common Name: untrusted

IP or FQDN to appear on the certificate

Signed By:

☑ Certificate Authority

OCSP Responder:

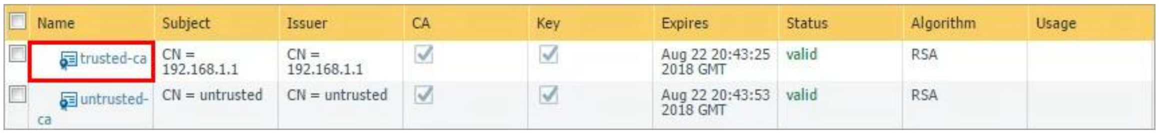
Algorithm: RSA

Number of Bits: 2048

Digest: sha256

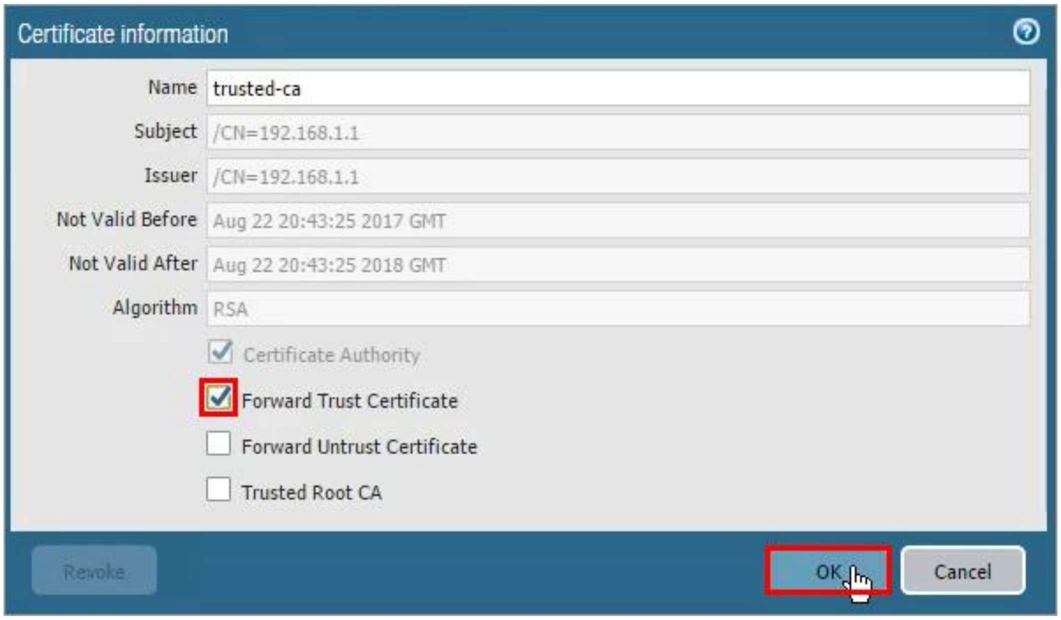
Expiration (days): 365

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



□	Name	Subject	Issuer	CA	Key	Expires	Status	Algorithm	Usage
□	trusted-ca	CN = 192.168.1.1	CN = 192.168.1.1	✓	✓	Aug 22 20:43:25 2018 GMT	valid	RSA	
□	untrusted-ca	CN = untrusted	CN = untrusted	✓	✓	Aug 22 20:43:53 2018 GMT	valid	RSA	

9. Select the **Forward Trust Certificate** check box and click **OK**:

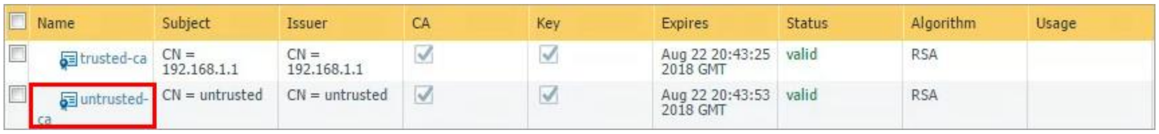


Certificate information

Name: trusted-ca
Subject: /CN=192.168.1.1
Issuer: /CN=192.168.1.1
Not Valid Before: Aug 22 20:43:25 2017 GMT
Not Valid After: Aug 22 20:43:25 2018 GMT
Algorithm: RSA

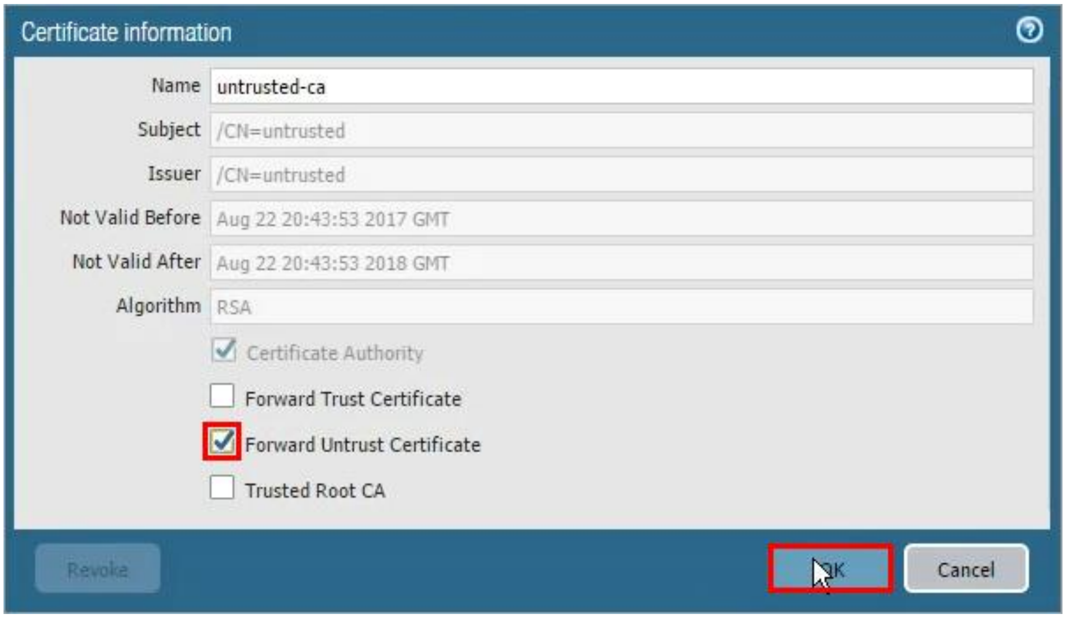
☑ Certificate Authority
☑ Forward Trust Certificate
☐ Forward Untrust Certificate
☐ Trusted Root CA

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



☐	Name	Subject	Issuer	CA	Key	Expires	Status	Algorithm	Usage
☐	trusted-ca	CN = 192.168.1.1	CN = 192.168.1.1	✓	✓	Aug 22 20:43:25 2018 GMT	valid	RSA	
☐	untrusted-ca	CN = untrusted	CN = untrusted	✓	✓	Aug 22 20:43:53 2018 GMT	valid	RSA	

11. Select the **Forward Untrust Certificate** check box and click **OK**:



Certificate information

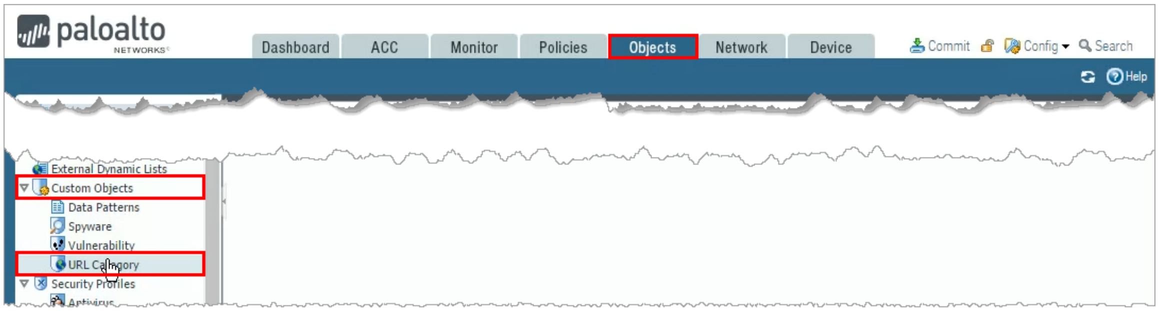
Name: untrusted-ca
Subject: /CN=untrusted
Issuer: /CN=untrusted
Not Valid Before: Aug 22 20:43:53 2017 GMT
Not Valid After: Aug 22 20:43:53 2018 GMT
Algorithm: RSA

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

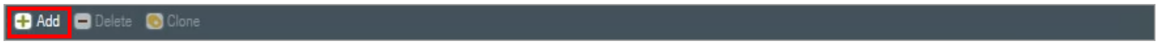
7.3 Create Custom Decryption URL Category

Create a custom URL Category to ensure we are only decrypting intended traffic.

1. In the WebUI select **Objects > Custom Objects > URL Category**.



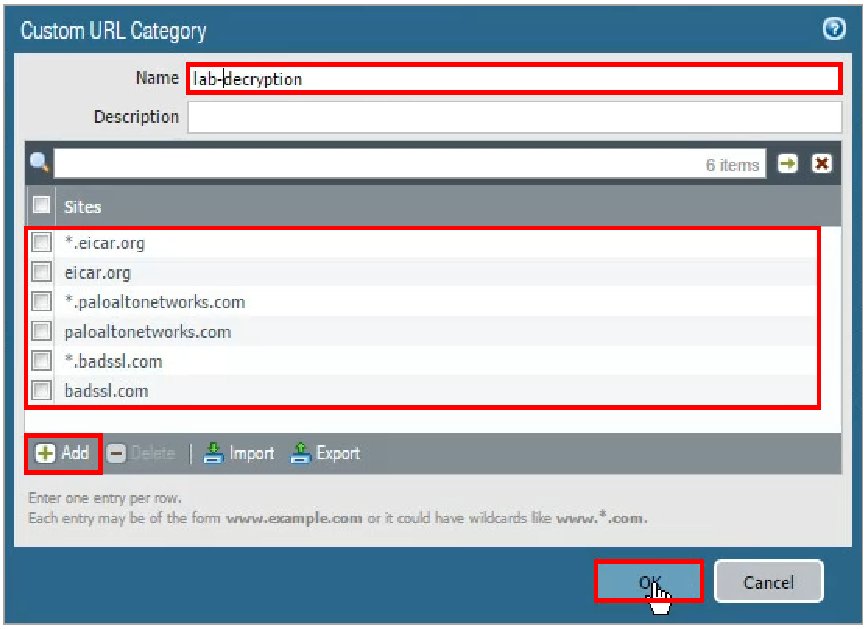
2. Click **Add** to open the Custom URL Category configuration window.



3. Configure the following then click **OK**:

Parameter	Value
Name	`lab-decryption`

Sites	`*.eicar.org`
	`eicar.org`
	`*.paloaltonetworks.com`
	`paloaltonetworks.com`
	`*.badssl.com`
	`badssl.com`



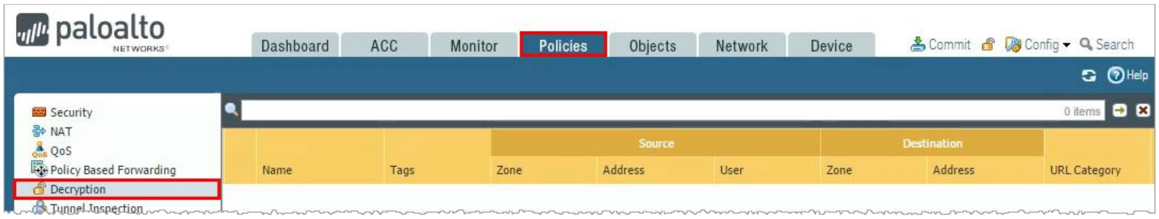
Name: lab-decryption

Sites:
- *.eicar.org
- eicar.org
- *.paloaltonetworks.com
- paloaltonetworks.com
- *.badssl.com
- badssl.com

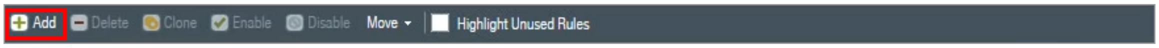
Enter one entry per row.
Each entry may be of the form **www.example.com** or it could have wildcards like **www.*.com**.

7.4 Create Decryption Policy

1. In the WebUI select **Policies > Decryption**.

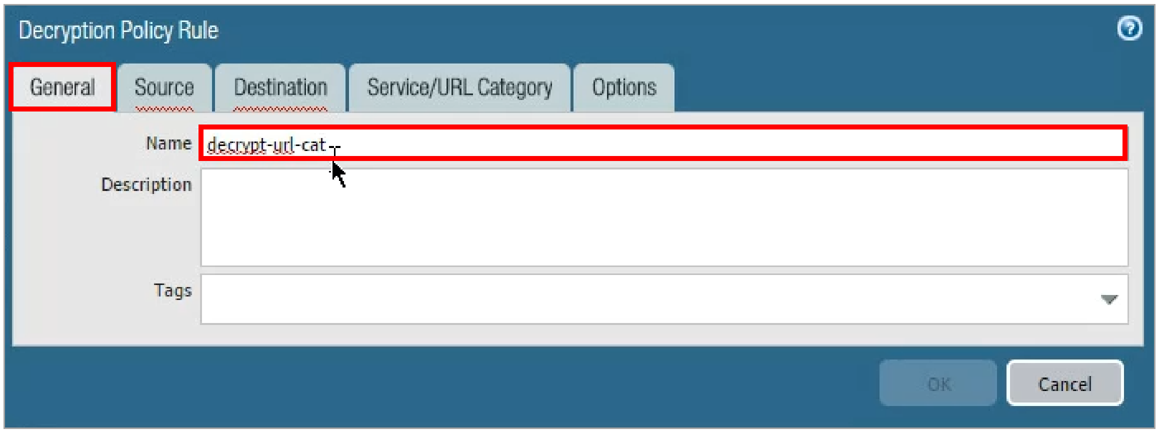


2. Click **Add** to create a Decryption policy rule.



3. Configure the following:

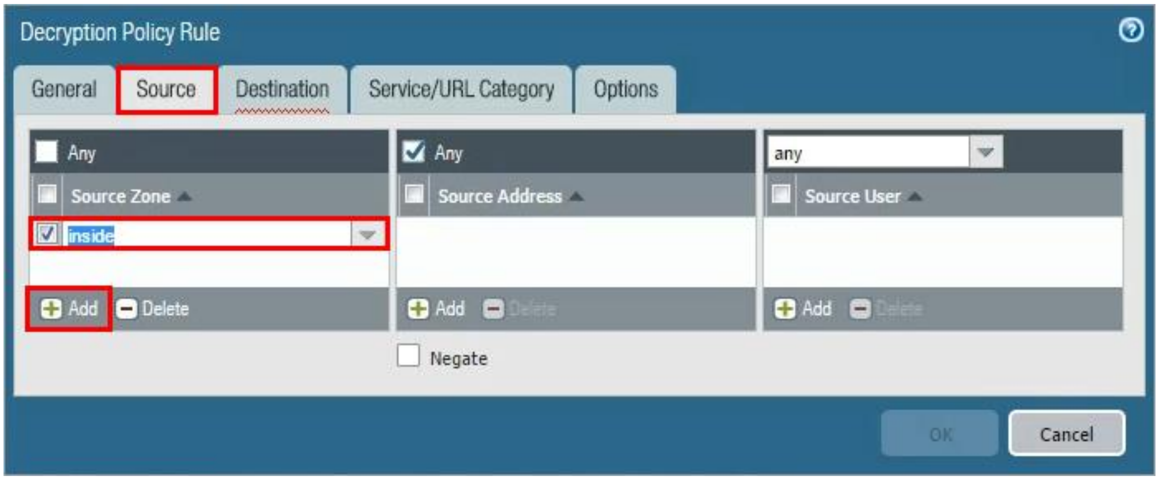
Parameter	Value
Name	`decrypt-url-cat`



Name decrypt-url-cat

4. Click the Source tab and configure the following:

Parameter	Value
Source Zone	**`inside`**



Decryption Policy Rule

□ Any
Source Zone
☑ inside

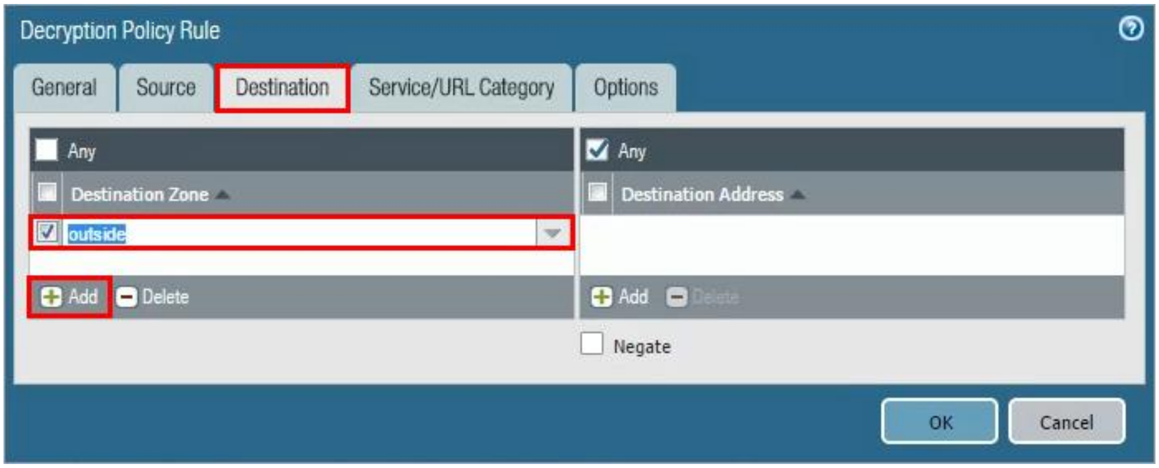
☑ Any
Source Address

any
Source User

□ Negate

5. Click the Destination tab and configure the following:

Parameter	Value
Destination Zone	`outside`



Decryption Policy Rule

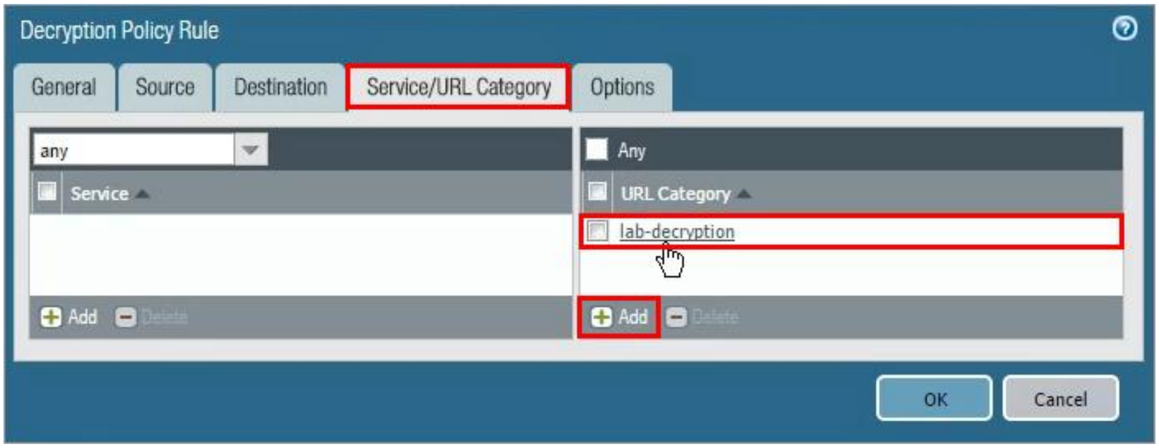
□ Any
Destination Zone
☑ outside

☑ Any
Destination Address

□ Negate

6. Click the Service/URL Category tab and configure the following:

Parameter	Value
URL Category	☑ lab-decryption



any

□ Service

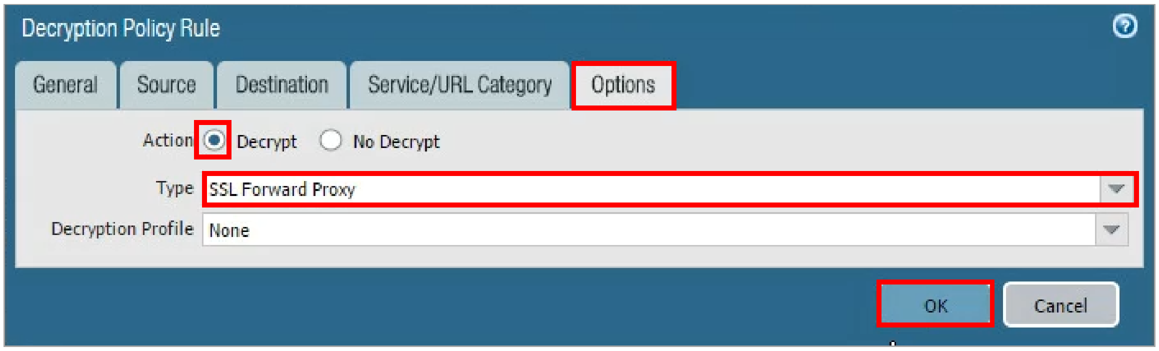
□ Any

□ URL Category

□ lab-decryption

7. Click the Options tab and configure the following then click **OK**.

Parameter	Value
Action	Decrypt
Type	SSL Forward Proxy



Action ● Decrypt ○ No Decrypt

Type SSL Forward Proxy

Decryption Profile None

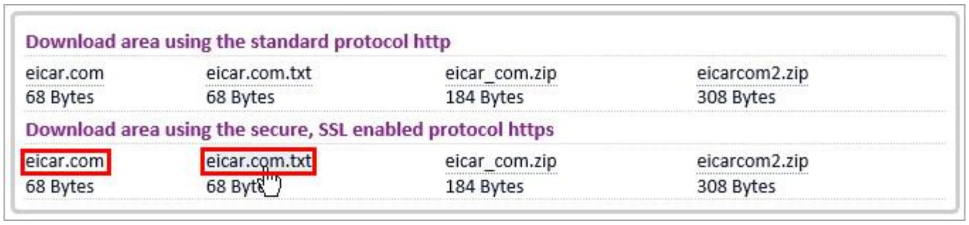
8. **Commit** all changes.

7.5 Test AV Security Profile with the Decryption Policy

1. On the Windows desktop, open a browser in private/incognito mode and browse to `http://www.eicar.org`.
2. Click the **DOWNLOAD ANTIMALWARE TESTFILE** image in the top-right corner:

3. Click the **Download** link on the left of the web page:

4. Within the Download area at the bottom of the page, click either the **eicar.com** or the **eicar.com.txt** file to download the file using HTTPS:



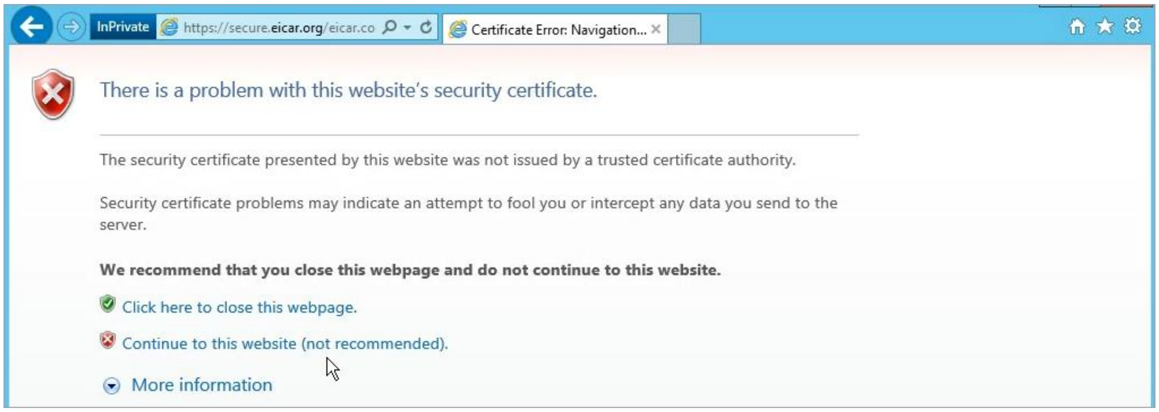
Download area using the standard protocol http

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

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

A certificate issue is presented:


InPrivate
https://secure.eicar.org/eicar.co
Certificate Error: Navigation...

There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.

Continue to this website (not recommended).

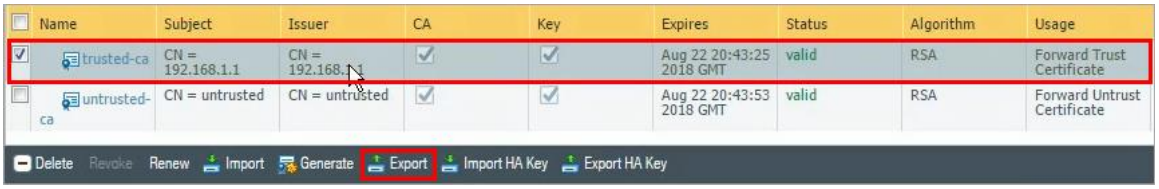
More information

Note: The endpoint (Windows desktop) does not trust the certificate generated by the firewall.

5. **Close** all browser windows except for the firewall WebUI.

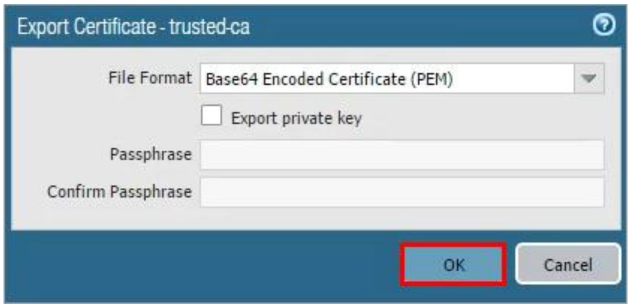
7.6 Export the Firewall Certificate

1. In the WebUI select **Device > Certificate Management > Certificates**.
2. Select but do not open **trusted-ca** then click **Export** to open the Export Certificate configuration window.



☐	Name	Subject	Issuer	CA	Key	Expires	Status	Algorithm	Usage
☑	trusted-ca	CN = 192.168.1.1	CN = 192.168.1.1	✓	✓	Aug 22 20:43:25 2018 GMT	valid	RSA	Forward Trust Certificate
☐	untrusted-ca	CN = untrusted	CN = untrusted	✓	✓	Aug 22 20:43:53 2018 GMT	valid	RSA	Forward Untrust Certificate

3. Click **OK** to export the trust-ca certificate.



Export Certificate - trusted-ca

File Format: Base64 Encoded Certificate (PEM)

☐ Export private key

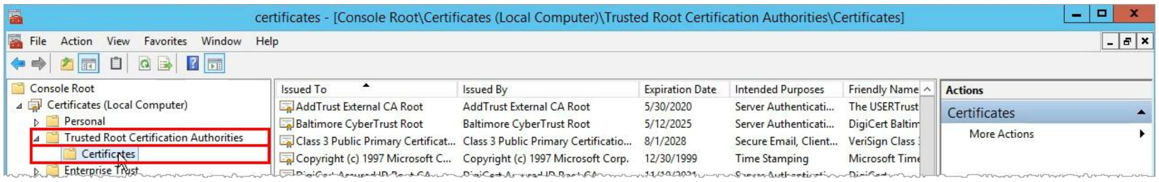
Passphrase:

Confirm Passphrase:

7.7 Import the Firewall Certificate

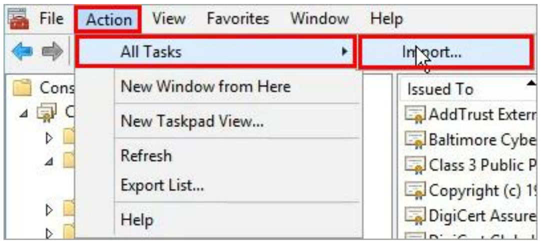
1. On your desktop, double-click the certificates icon.

2. Under Certificates (Local Computer), expand **Trusted Root Certification Authorities** and select the **Certificates** folder:

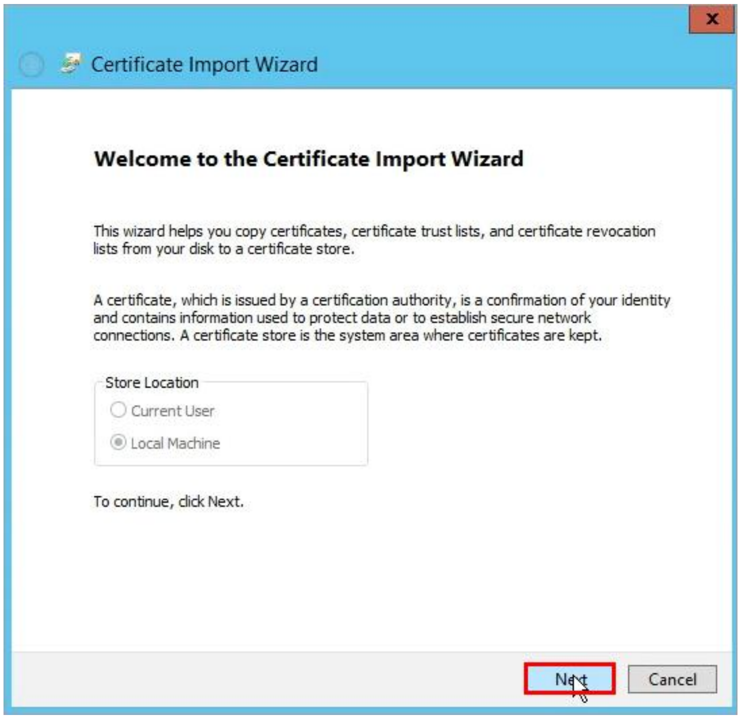

certificates - [Console Root\Certificates (Local Computer)\Trusted Root Certification Authorities\Certificates]
File
Action
View
Favorites
Window
Help
Console Root
Certificates (Local Computer)
Personal
Trusted Root Certification Authorities
Certificates
Enterprise Trust
Actions
Certificates
More Actions

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name
AddTrust External CA Root	AddTrust External CA Root	5/30/2020	Server Authenticati...	The USERTrust
Baltimore CyberTrust Root	Baltimore CyberTrust Root	5/12/2025	Server Authenticati...	DigiCert Baltim
Class 3 Public Primary Certificat...	Class 3 Public Primary Certificatio...	8/1/2028	Secure Email, Client...	VeriSign Class
Copyright (c) 1997 Microsoft C...	Copyright (c) 1997 Microsoft Corp.	12/30/1999	Time Stamping	Microsoft Time

3. Select **Action > All Tasks > Import**.



4. The Certificate Import Wizard opens. Click **Next**.



Welcome to the Certificate Import Wizard

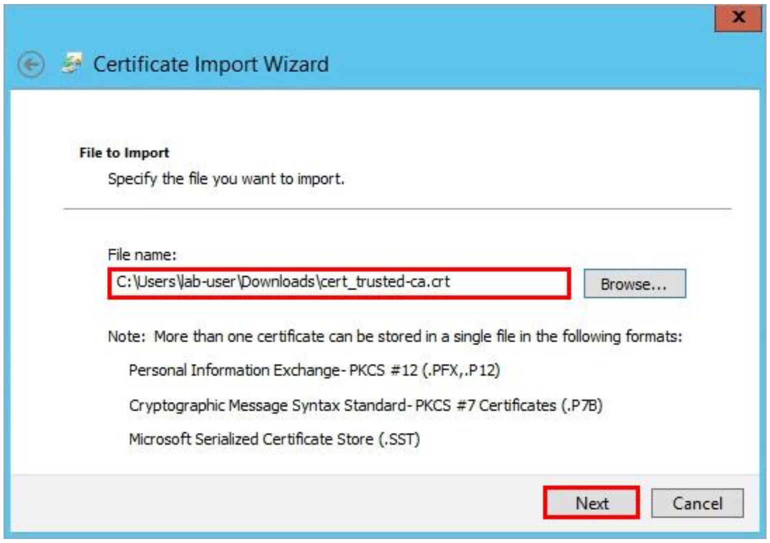
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

Store Location
○ Current User
● Local Machine

To continue, click Next.

5. **Browse** for the exported trusted-ca certificate then click **Next**.



File to Import

Specify the file you want to import.

File name:
C:\Users\lab-user\Downloads\cert_trusted-ca.crt

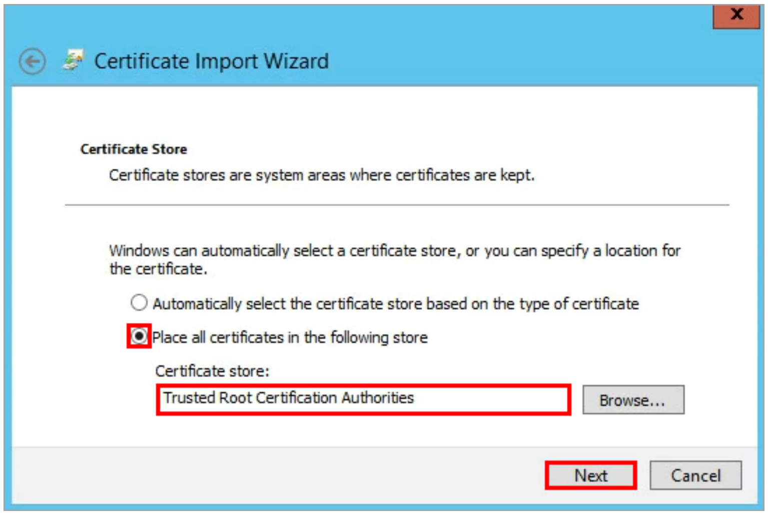
Note: More than one certificate can be stored in a single file in the following formats:

Personal Information Exchange- PKCS #12 (.PFX,.P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

6. **Verify** that the following is configured.



Certificate Store

Certificate stores are system areas where certificates are kept.

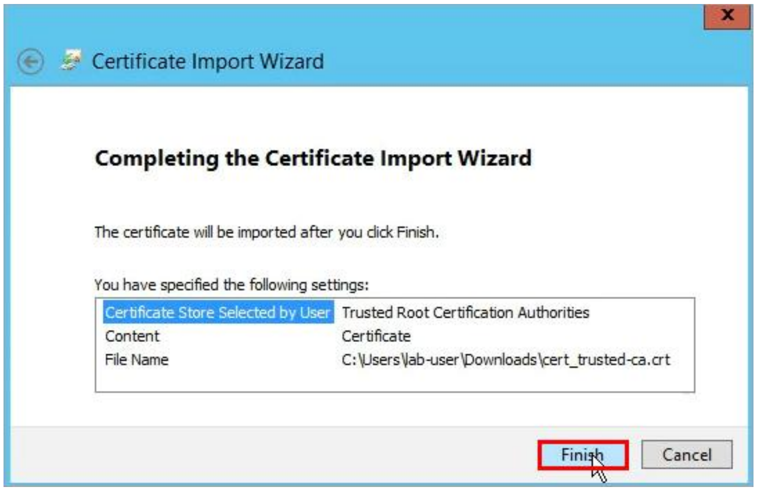
Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store:
Trusted Root Certification Authorities

7. Click **Next**, click **Finish**, and then click **OK** in the status window.



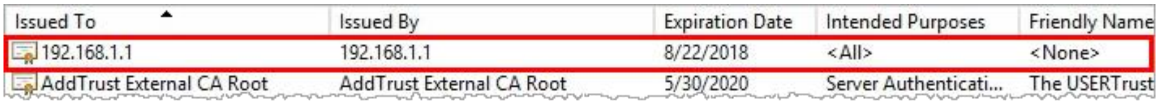
Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected by User	Trusted Root Certification Authorities
Content	Certificate
File Name	C:\Users\lab-user\Downloads\cert_trusted-ca.crt

8. Notice that the trusted-ca certificate is now imported:

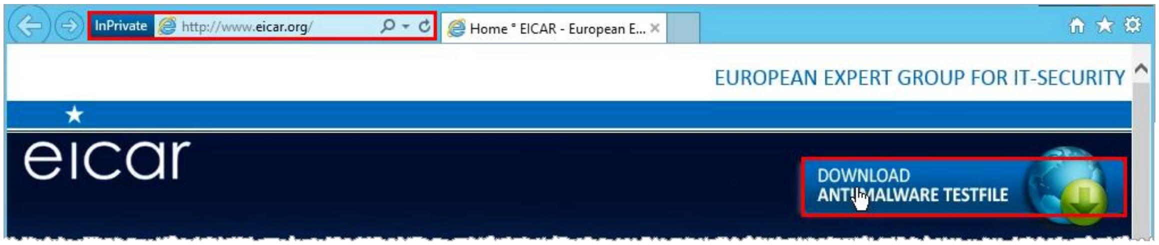


Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name
192.168.1.1	192.168.1.1	8/22/2018	<All>	<None>
AddTrust External CA Root	AddTrust External CA Root	5/30/2020	Server Authenticati...	The USERTrust

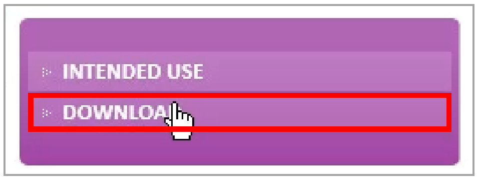
9. Close the Microsoft Management Console. Click **No** when asked to save console settings.

7.8 Test the Decryption Policy

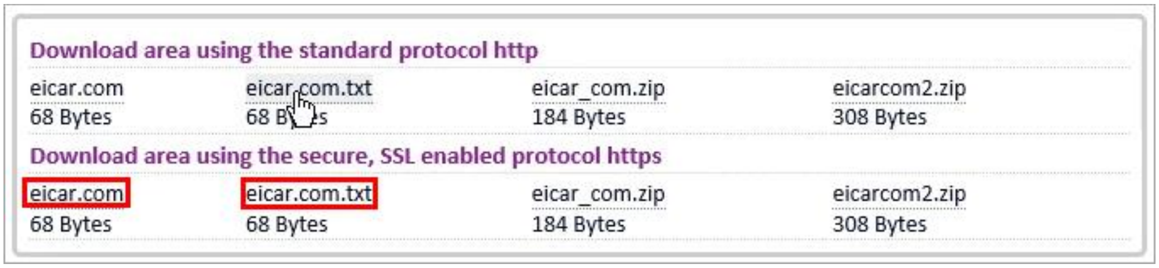
1. On the Windows desktop, open a browser (not Firefox) in private/incognito mode and browse to `http://www.eicar.org`.
2. Click the **DOWNLOAD ANTIMALWARE TESTFILE** image in the top-right corner.


InPrivate
http://www.eicar.org/
Home ° EICAR - European E...
EUROPEAN EXPERT GROUP FOR IT-SECURITY
eicar
DOWNLOAD
ANTIMALWARE TESTFILE

3. Click the **Download** link on the left of the web page.



4. Within the Download area at the bottom of the page, click either the **eicar.com** or the **eicar.com.txt** file to download the file using HTTPS:



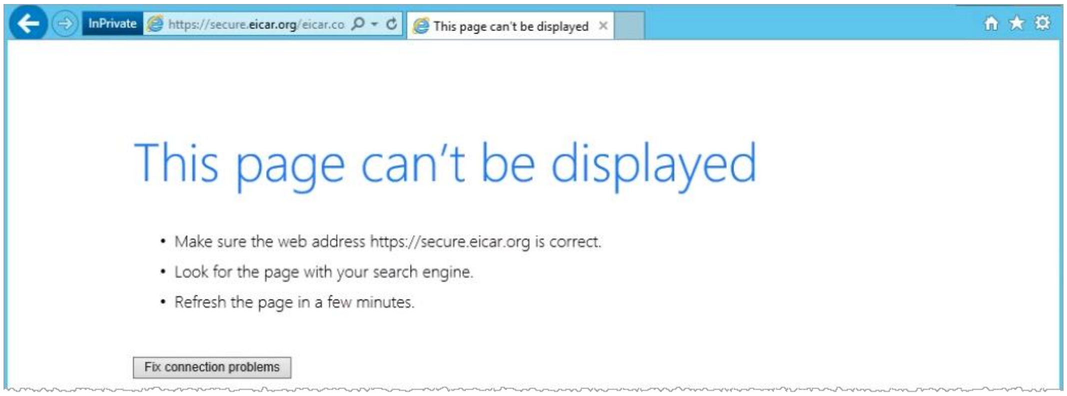
Download area using the standard protocol http

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

Download area using the secure, SSL enabled protocol https

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

The Eicar Test File is detected and the connection gets reset.


InPrivate
https://secure.eicar.org/eicar.co
This page can't be displayed

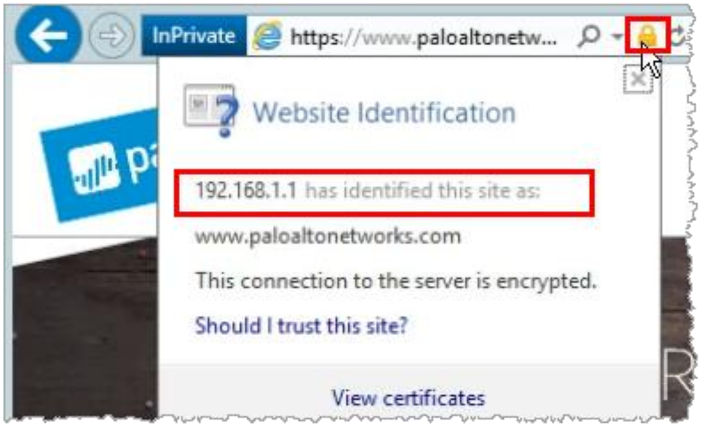
This page can't be displayed

- Make sure the web address https://secure.eicar.org is correct.
- Look for the page with your search engine.
- Refresh the page in a few minutes.

5. In the same browser, browse to `https://www.paloaltonetworks.com`.

   There is no certificate warning and the page is displayed correctly.

6. Click the **lock** icon next to the URL in the browser (Internet Explorer) and notice that the signer is the firewall 192.168.1.1.



Website Identification

192.168.1.1 has identified this site as:

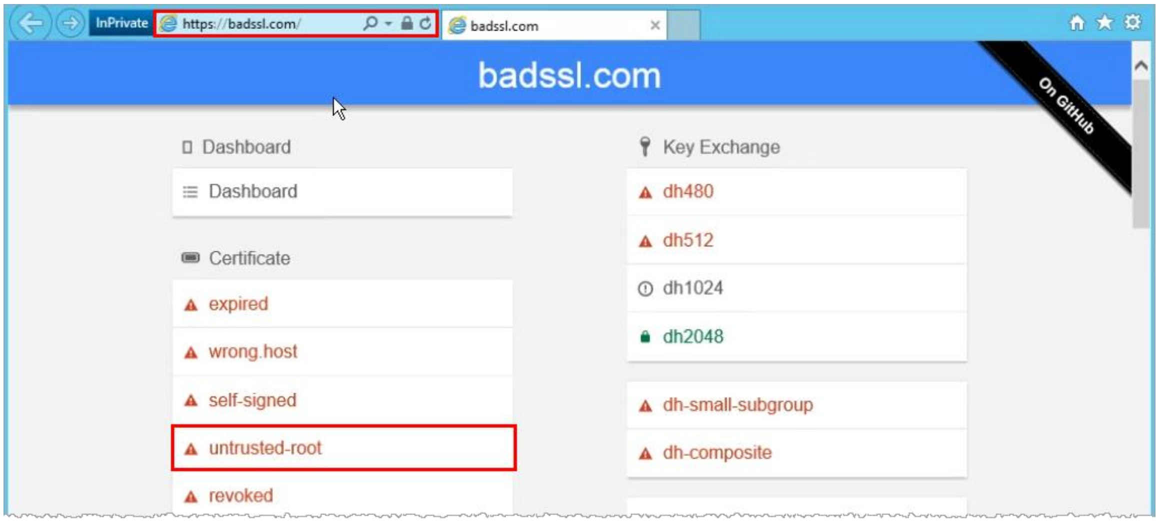
www.paloaltonetworks.com

This connection to the server is encrypted.

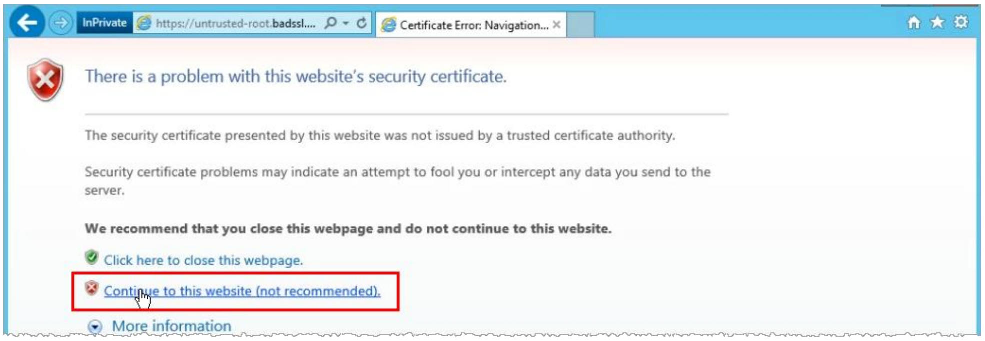
Should I trust this site?

View certificates

7. Close all browser windows except for the firewall WebUI.
8. Open a new browser and browse to `https://www.badssl.com` then click **untrusted-root**.



9. Notice that a certificate warning is now displayed. Choose to continue to the website.


InPrivate
https://untrusted-root.badssl....
Certificate Error: Navigation...

There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

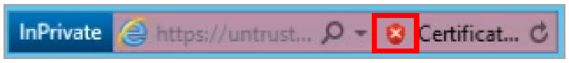
We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.

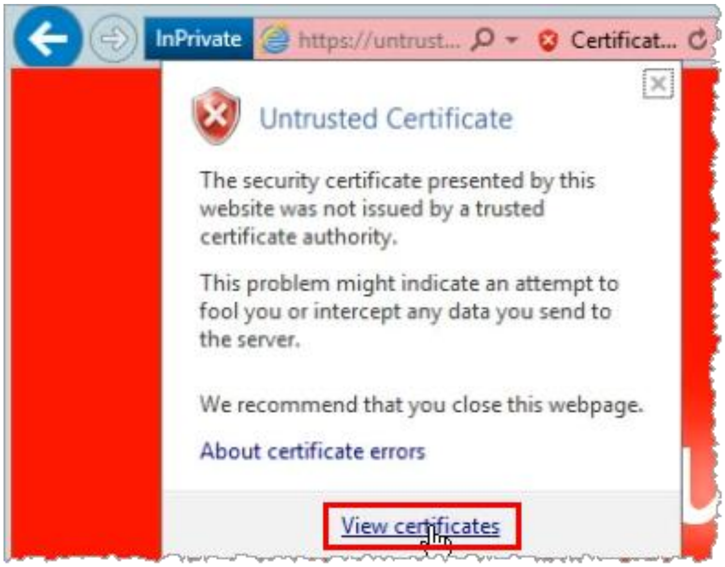
Continue to this website (not recommended).

More information

10. Click the **Certificate** icon near the URL.



11. Click **View Certificates**.



Untrusted Certificate

The security certificate presented by this website was not issued by a trusted certificate authority.

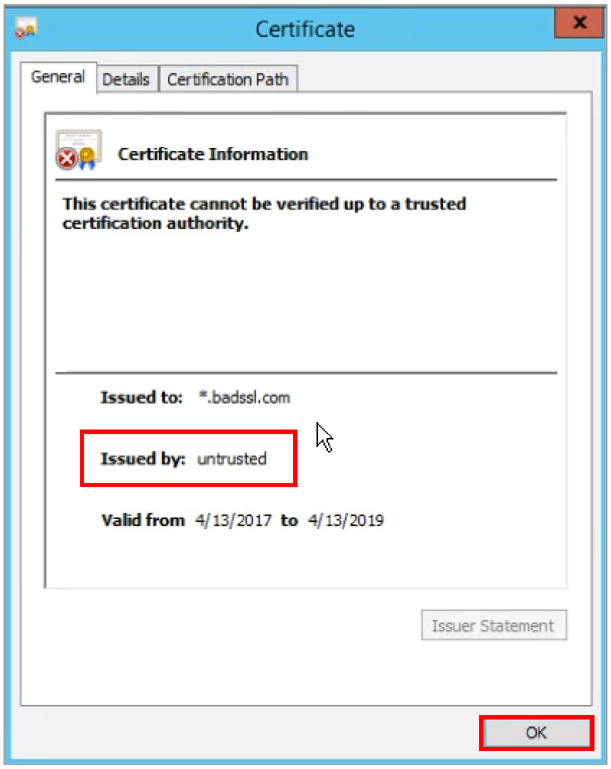
This problem might indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage.

About certificate errors

View certificates

12. Notice that the certificate is still signed by the firewall. However, it was signed with the untrusted certificate then click **OK**.



Certificate Information

This certificate cannot be verified up to a trusted certification authority.

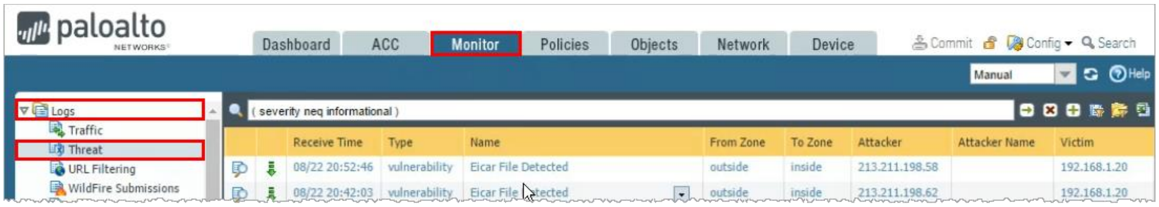
Issued to: *.badssl.com

Issued by: untrusted

Valid from 4/13/2017 to 4/13/2019

7.9 Review Logs

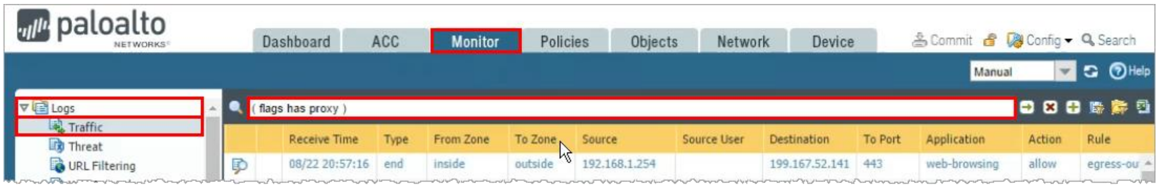
1. Select **Monitor > Logs > Threat**. Notice that there is an entry for when the connection was reset in the browser:



(severity neq informational)

Receive Time	Type	Name	From Zone	To Zone	Attacker	Attacker Name	Victim
08/22 20:52:46	vulnerability	Eicar File Detected	outside	inside	213.211.198.58		192.168.1.20
08/22 20:42:03	vulnerability	Eicar File Detected	outside	inside	213.211.198.62		192.168.1.20

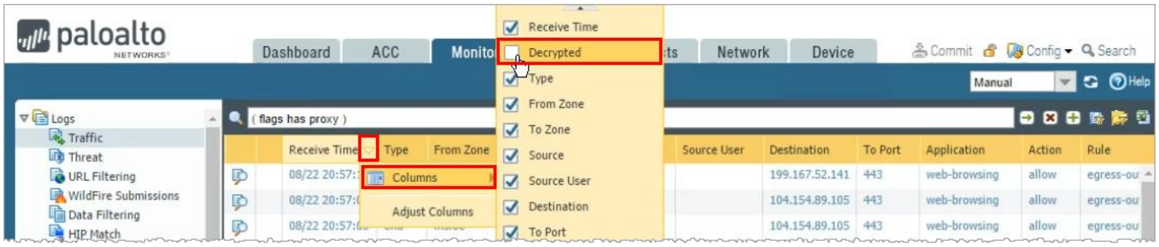
2. Select **Monitor > Logs > Traffic** then type `( flags has proxy )` in the filter text box. This filter flags only traffic entries that were decrypted.



(flags has proxy)

Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port	Application	Action	Rule
08/22 20:57:16	end	inside	outside	192.168.1.254		199.167.52.141	443	web-browsing	allow	egress-ou

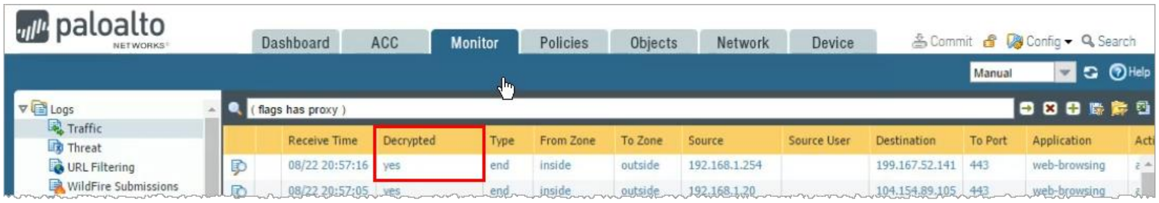
3. Hover over **Receive Time** and click **down-arrow > Columns > Decrypted** to add the Decrypted column.



(flags has proxy)

Receive Time	Type	From Zone	Source User	Destination	To Port	Application	Action	Rule
08/22 20:57:1				199.167.52.141	443	web-browsing	allow	egress-ou
08/22 20:57:0				104.154.89.105	443	web-browsing	allow	egress-ou
08/22 20:57:0	end	inside		104.154.89.105	443	web-browsing	allow	egress-ou

4. Notice the newly added column.

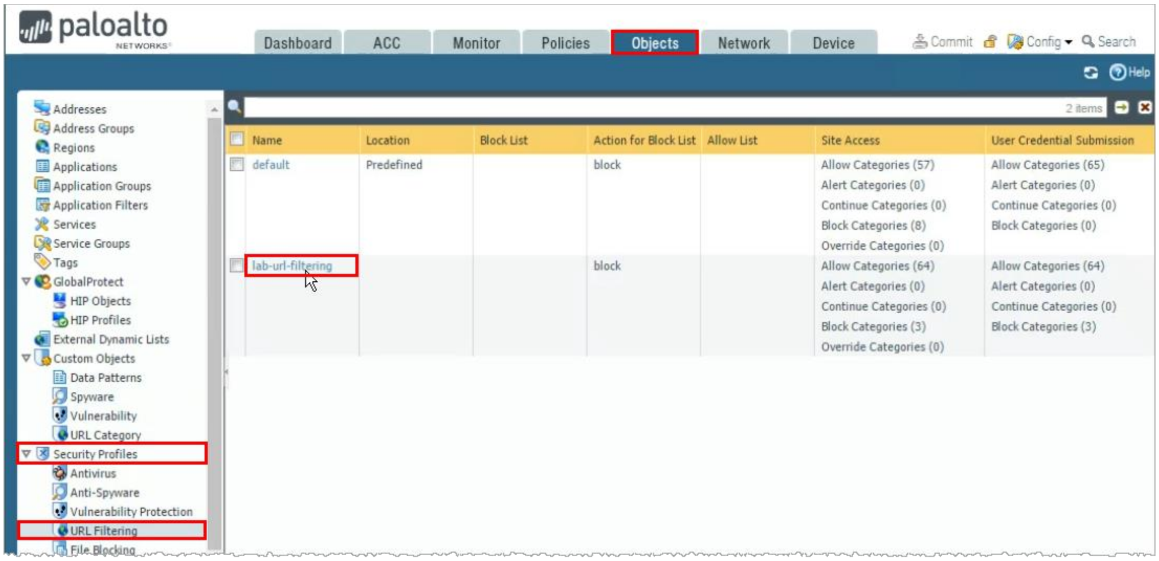


(flags has proxy)

Receive Time	Decrypted	Type	From Zone	To Zone	Source	Source User	Destination	To Port	Application	Acti
08/22 20:57:16	yes	end	inside	outside	192.168.1.254		199.167.52.141	443	web-browsing	a
08/22 20:57:05	yes	end	inside	outside	192.168.1.20		104.154.89.105	443	web-browsing	a

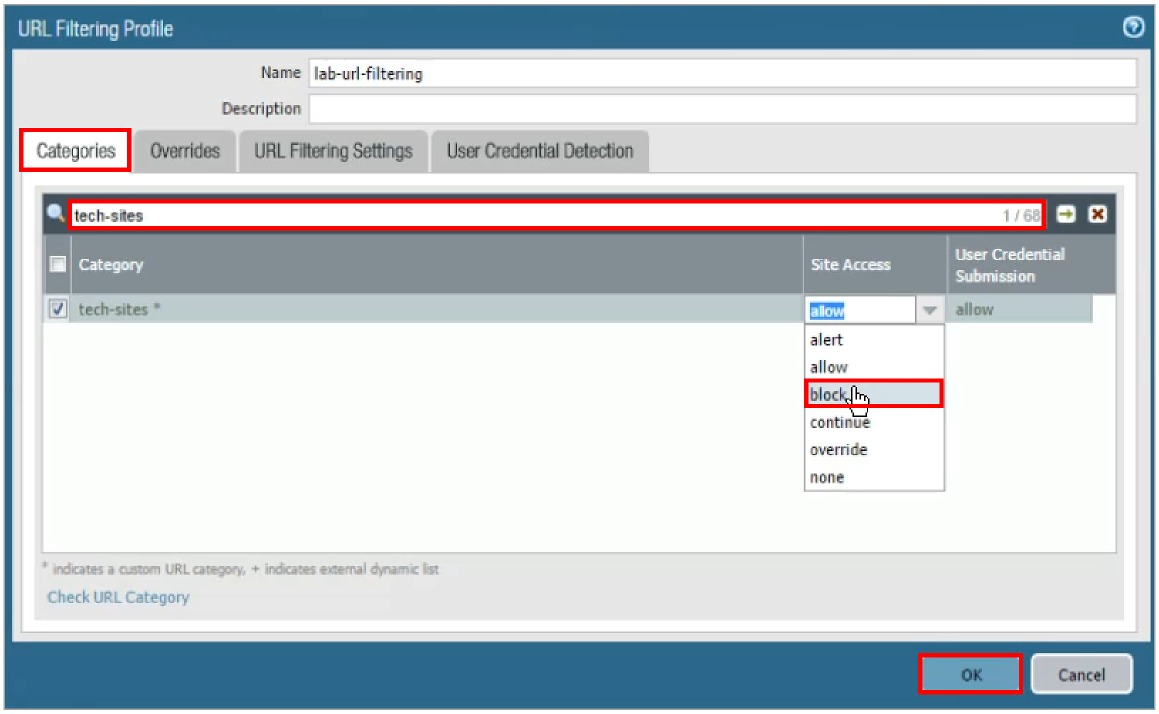
7.10 Test URL Filtering with Decryption

1. In the WebUI select **Objects > Security Profiles > URL Filtering** then click **lab-url-filtering** to open the lab-url-filtering object.



Name	Location	Block List	Action for Block List	Allow List	Site Access	User Credential Submission
default	Predefined		block		Allow Categories (57) Alert Categories (0) Continue Categories (0) Block Categories (8) Override Categories (0)	Allow Categories (65) Alert Categories (0) Continue Categories (0) Block Categories (0)
lab-url-filtering			block		Allow Categories (64) Alert Categories (0) Continue Categories (0) Block Categories (3) Override Categories (0)	Allow Categories (64) Alert Categories (0) Continue Categories (0) Block Categories (3)

2. Click the **Categories** tab and type a search for `tech-sites`. Change **Site Access** to **block** then click **OK**.



Name: lab-url-filtering

Description:

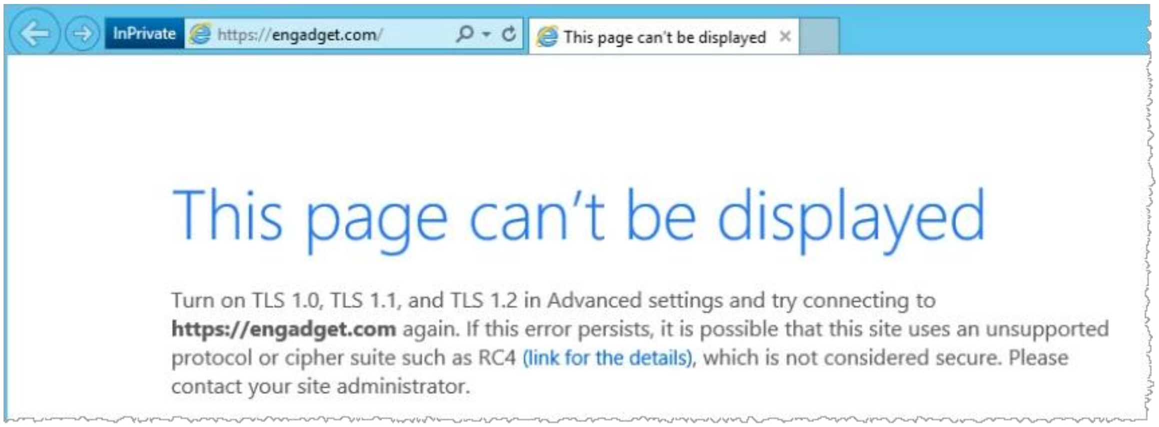
tech-sites 1 / 68

☐	Category	Site Access	User Credential Submission
☑	tech-sites *	allow	allow

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

Check URL Category

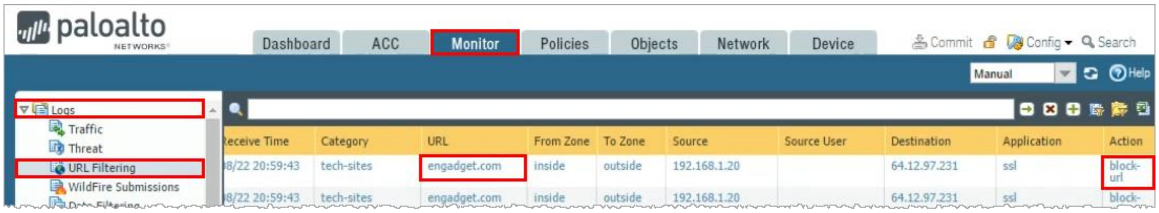
3. **Commit** all changes.
4. Open Internet Explorer in private mode and browse to `https://engadget.com`.



This page can’t be displayed

Turn on TLS 1.0, TLS 1.1, and TLS 1.2 in Advanced settings and try connecting to **https://engadget.com** again. If this error persists, it is possible that this site uses an unsupported protocol or cipher suite such as RC4 (link for the details), which is not considered secure. Please contact your site administrator.

5. Engadget is now blocked. This can be verified in the logs under **Monitor > Logs > URL Filtering.**



eceive Time	Category	URL	From Zone	To Zone	Source	Source User	Destination	Application	Action
8/22 20:59:43	tech-sites	engadget.com	inside	outside	192.168.1.20		64.12.97.231	ssl	block-url
8/22 20:59:43	tech-sites	engadget.com	inside	outside	192.168.1.20		64.12.97.231	ssl	block-

Stop. This is the end of the Decryption lab.