PALO ALTO NETWORKS - EDU-210

Lab 7: Decryption

Document Version: 2019-11-12

Contents

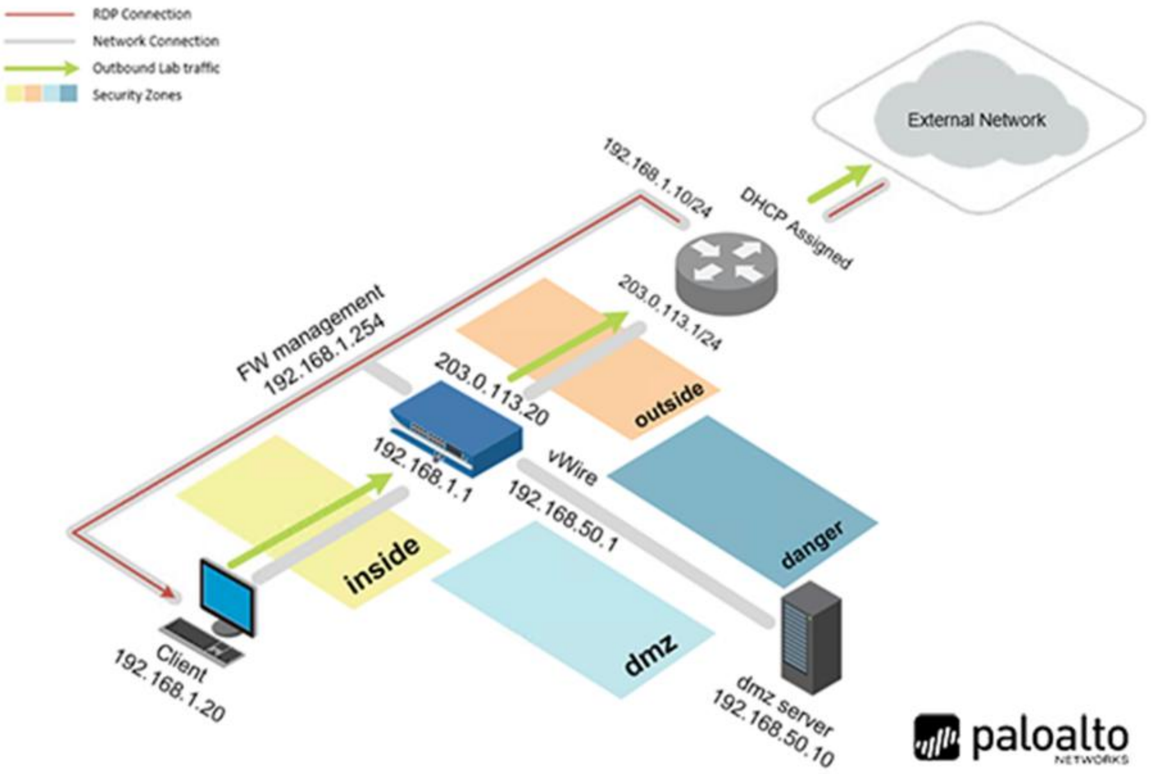
Introduction

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.

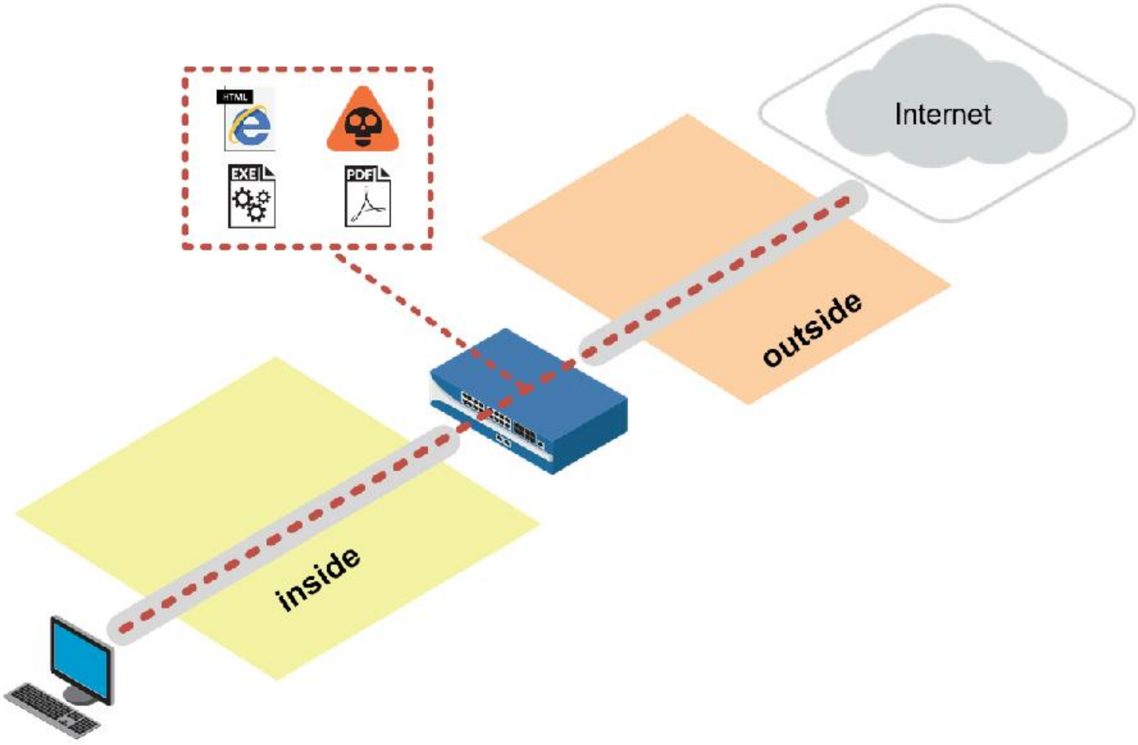
Objectives

- 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`	`Pal0Alt0`
Firewall	192.168.1.254	`admin`	`admin`

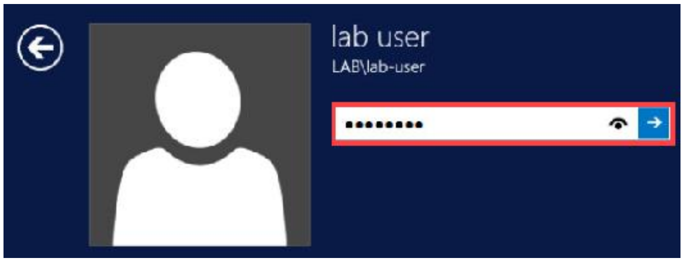
1 Decryption

1.0 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.

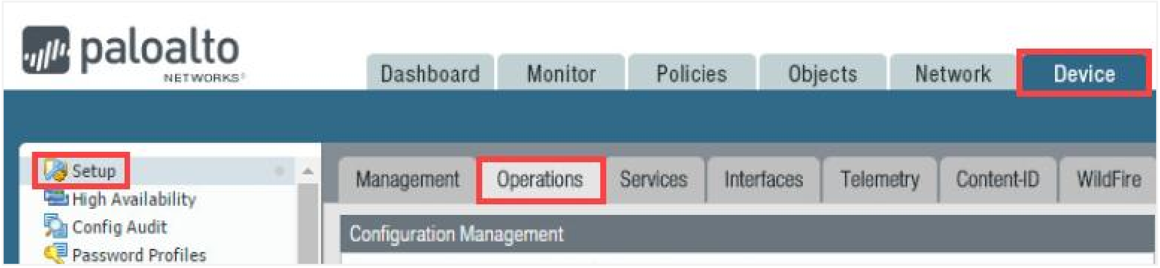
2. Click within the splash screen to bring up the login screen. Log in as **`lab-user`** using the password **`Pal0Alt0`**.



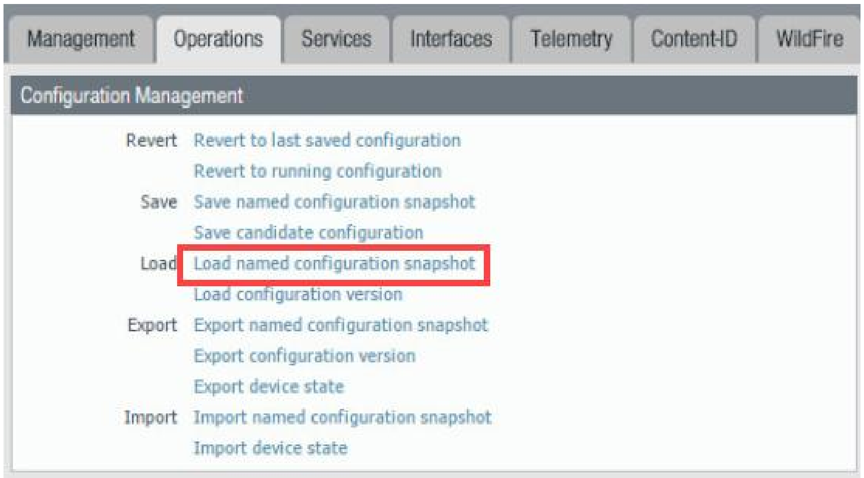
3. Launch the **Chrome** browser and connect to **`https://192.168.1.254.`**
4. If a security warning appears, click **Advanced** and proceed by clicking on **Proceed to 192.168.1.254 (unsafe)**.
5. Log in to the *Palo Alto Networks* firewall using the following:

Parameter	Value
Name	**`admin`**
Password	**`admin`**

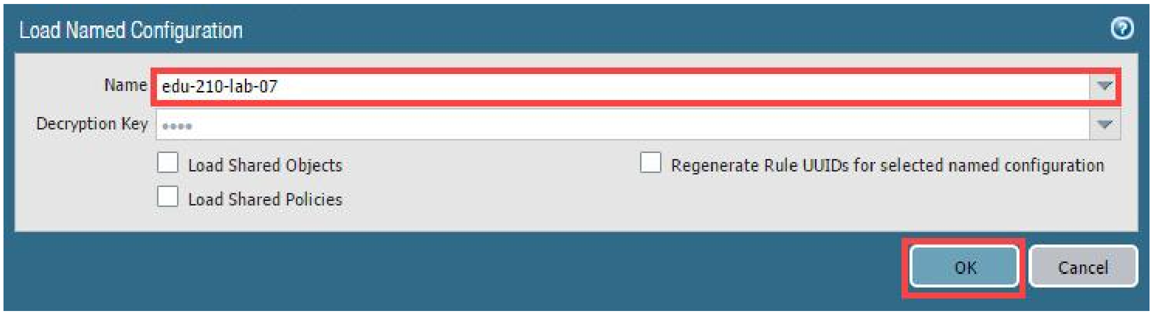
6. In the web interface, navigate to **Device > Setup > Operations**.



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


Management
Operations
Services
Interfaces
Telemetry
Content-ID
WildFire
Configuration Management
Revert
Revert to last saved configuration
Revert to running configuration
Save
Save named configuration snapshot
Save candidate configuration
Load
Load named configuration snapshot
Load configuration version
Export
Export named configuration snapshot
Export configuration version
Export device state
Import
Import named configuration snapshot
Import device state

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

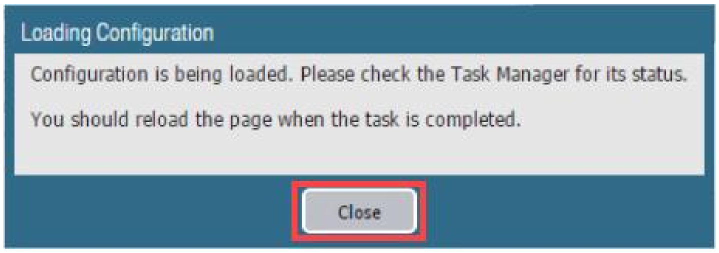

Load Named Configuration

Name: edu-210-lab-07

Decryption Key: ••••

□ Load Shared Objects
□ Regenerate Rule UUIDs for selected named configuration
□ Load Shared Policies

9. Click **Close**.

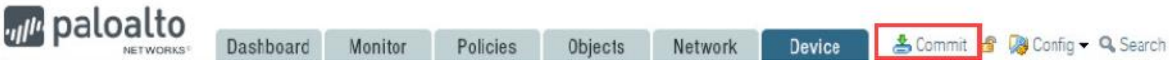

Loading Configuration

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

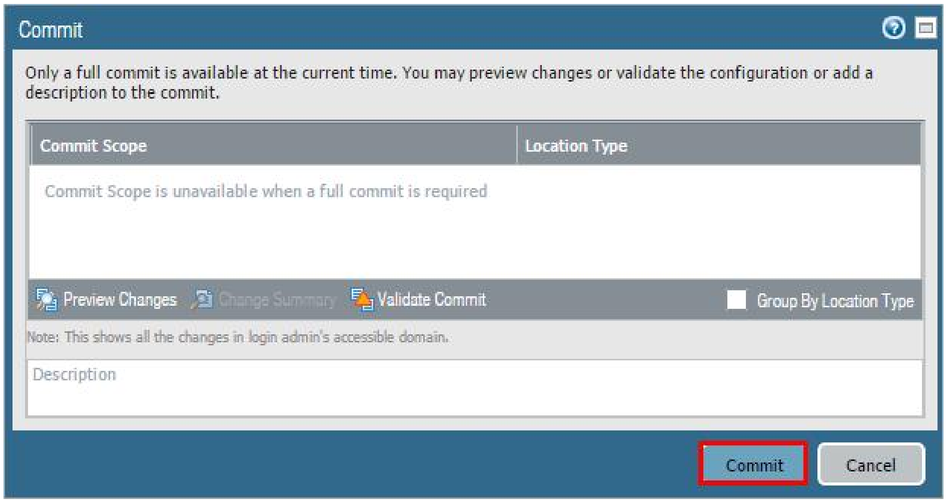
You should reload the page when the task is completed.

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.

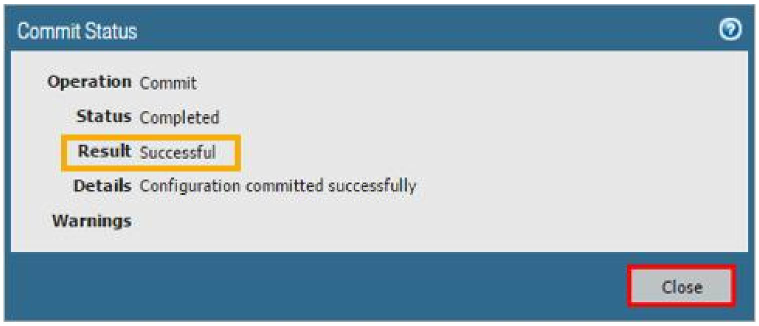


Only a full commit is available at the current time. You may preview changes or validate the configuration or add a description to the commit.

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.

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

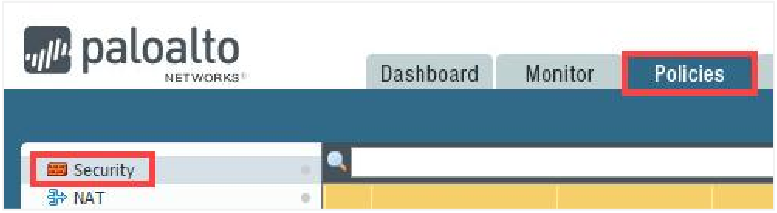


Operation Commit
Status Completed
Result Successful
Details Configuration committed successfully
Warnings

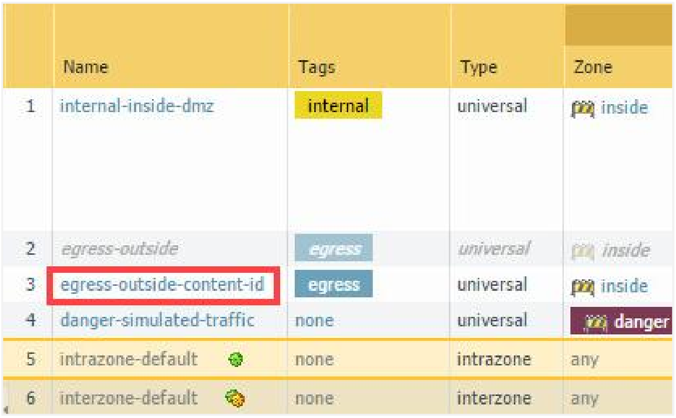
13. Leave the firewall web interface open to continue with the next task.

1.1 Test Firewall Behavior Without Decryption

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



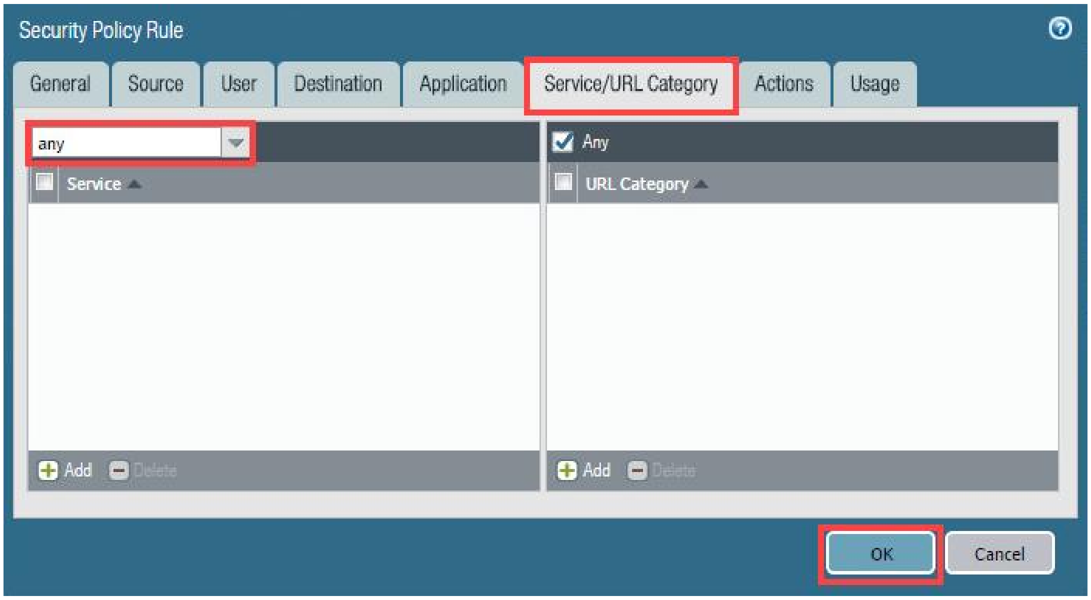
2. Click on **egress-outside-content-id** to open the Security policy rule.



	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 drop-down list



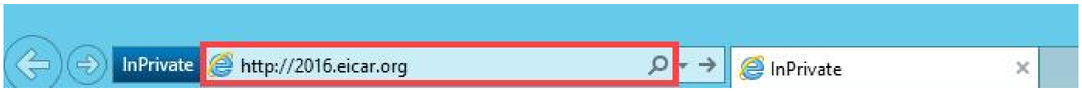
any

☐ Service

☑ Any

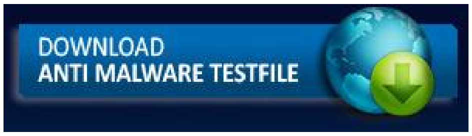
☐ URL Category

4. **Commit** all changes.
5. Open a new **Internet Explorer** browser window in **private/incognito** mode and browse to **`http://2016.eicar.org`**.

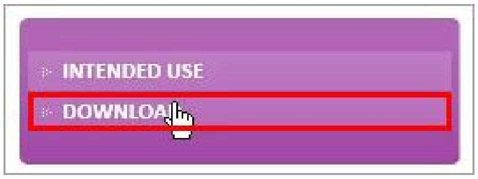


http://2016.eicar.org

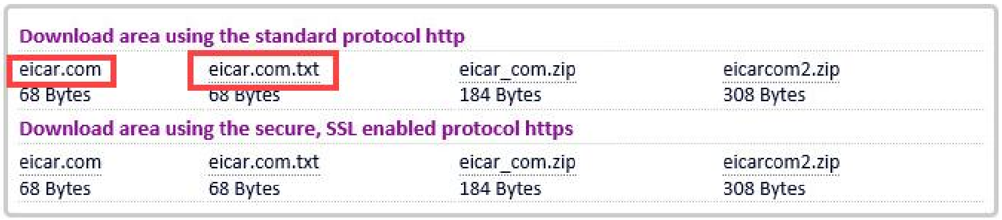
6. Click the **Download Anti Malware Testfile** image in the upper-right corner of the webpage.



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

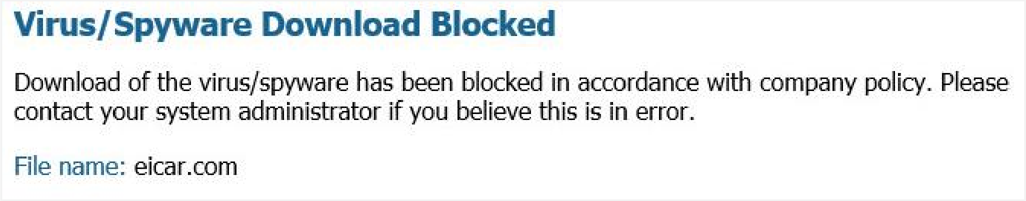


8. Within the *Download* area at the bottom of the page, click either the **eicar.com** or the **eicar.com.txt** file to download the file using the standard HTTP protocol and not the SSL-encrypted HTTPS protocol. The firewall will not be able to detect the viruses in an HTTPS connection until decryption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

9. Notice a message appears stating that the download was blocked.

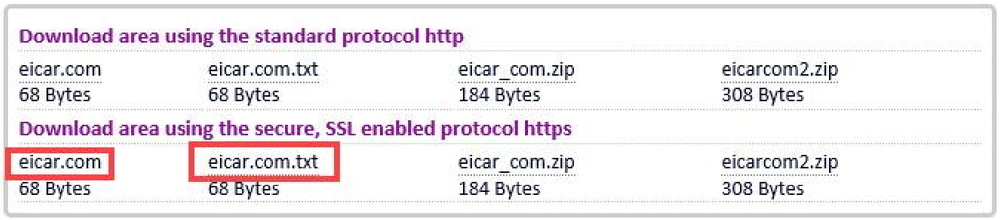


Virus/Spyware Download Blocked

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

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



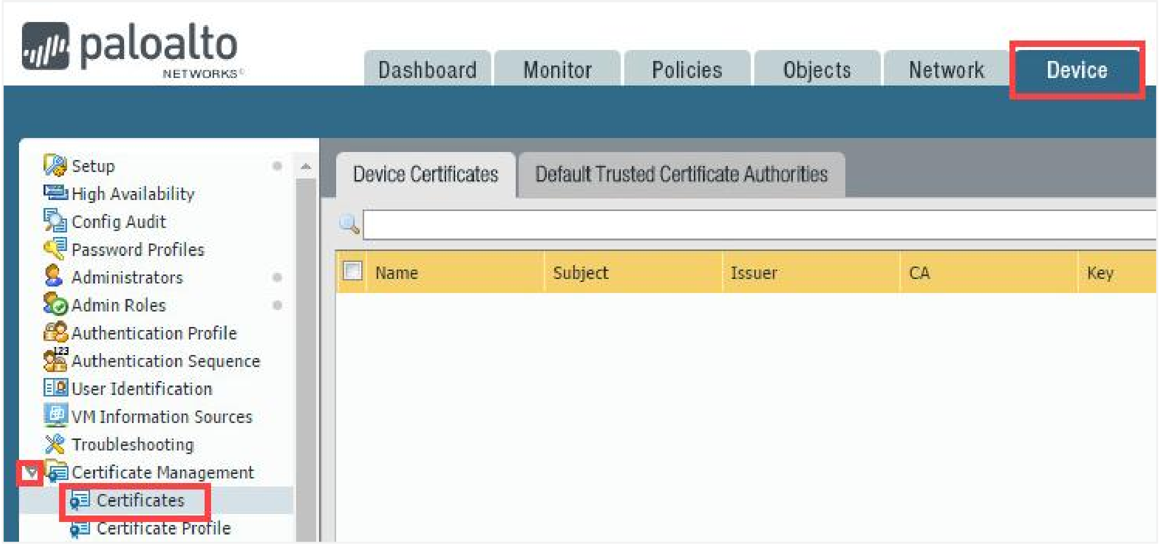
Download area using the standard protocol http			
eicar.com 68 Bytes	eicar.com.txt 68 Bytes	eicar_com.zip 184 Bytes	eicarcom2.zip 308 Bytes
Download area using the secure, SSL enabled protocol https			
eicar.com 68 Bytes	eicar.com.txt 68 Bytes	eicar_com.zip 184 Bytes	eicarcom2.zip 308 Bytes

11. 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.
12. Close the **IE** browser.

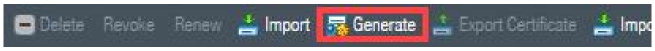
1.2 Create Two Self-Signed Certificates

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

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

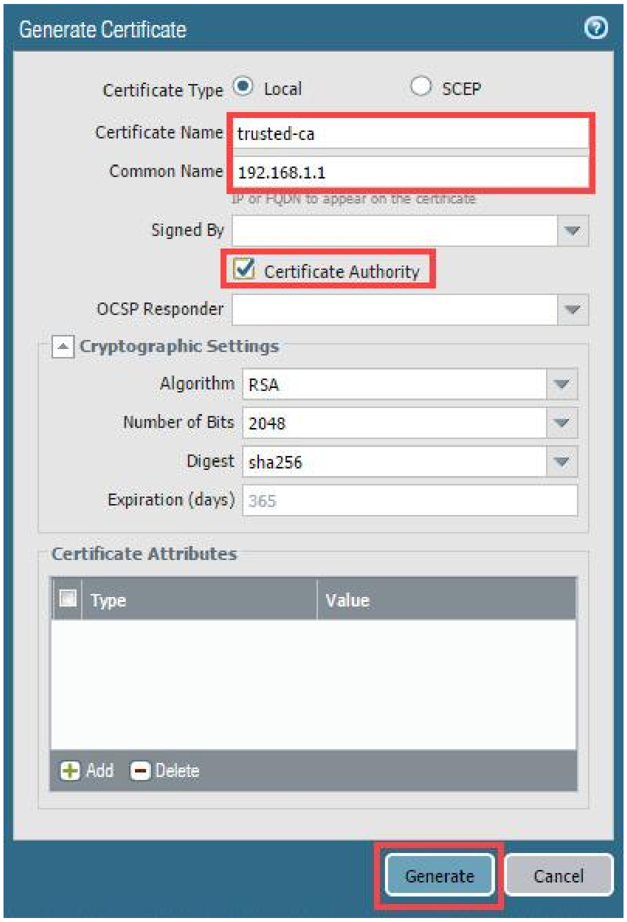


2. Click **Generate** at the bottom of the page to create a new CA certificate.



3. 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



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

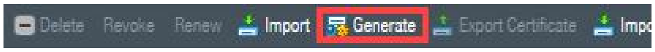
Number of Bits: 2048

Digest: sha256

Expiration (days): 365

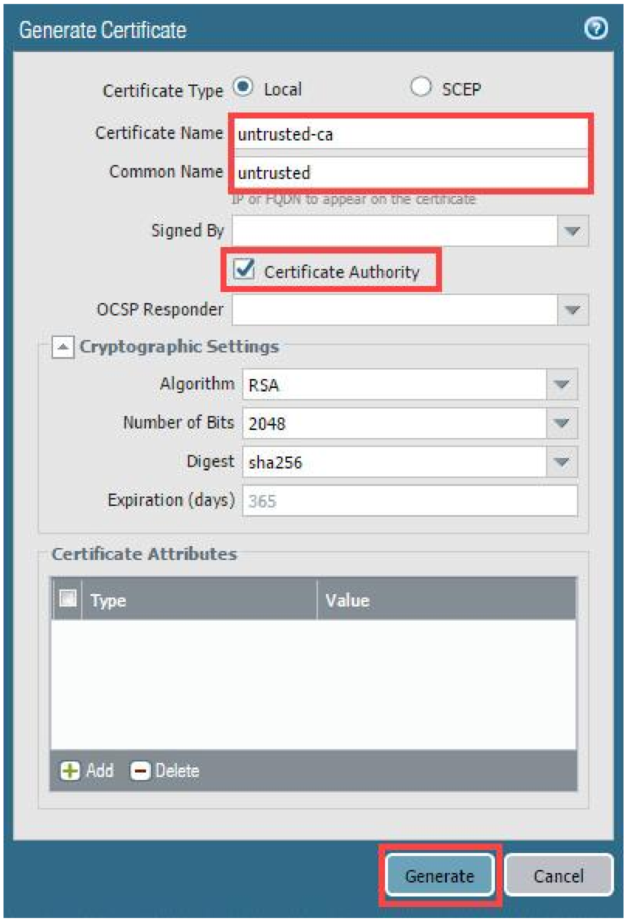
Certificate Attributes

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 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: untrusted-ca

Common Name: untrusted

IP or FQDN to appear on the certificate

Signed By:

☑ Certificate Authority

OCSP Responder:

Cryptographic Settings

Algorithm: RSA

Number of Bits: 2048

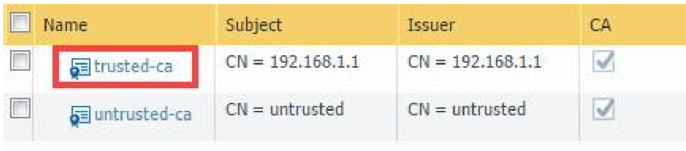
Digest: sha256

Expiration (days): 365

Certificate Attributes

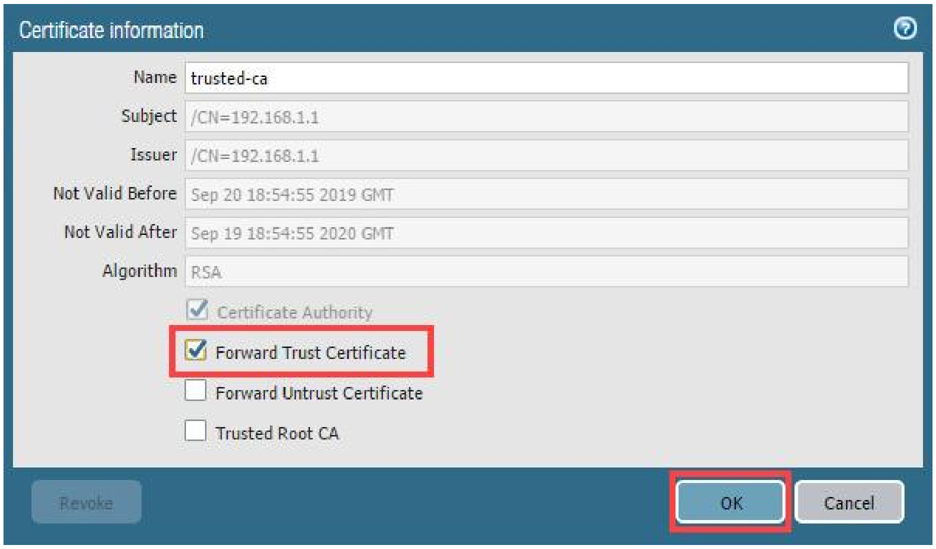
□	Type	Value

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
□	trusted-ca	CN = 192.168.1.1	CN = 192.168.1.1	✓
□	untrusted-ca	CN = untrusted	CN = untrusted	✓

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



Certificate information

Name	trusted-ca
Subject	/CN=192.168.1.1
Issuer	/CN=192.168.1.1
Not Valid Before	Sep 20 18:54:55 2019 GMT
Not Valid After	Sep 19 18:54:55 2020 GMT
Algorithm	RSA

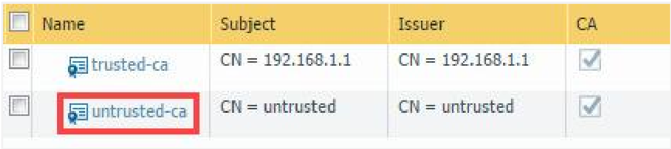
☑ Certificate Authority

☑ Forward Trust Certificate

☐ Forward Untrust Certificate

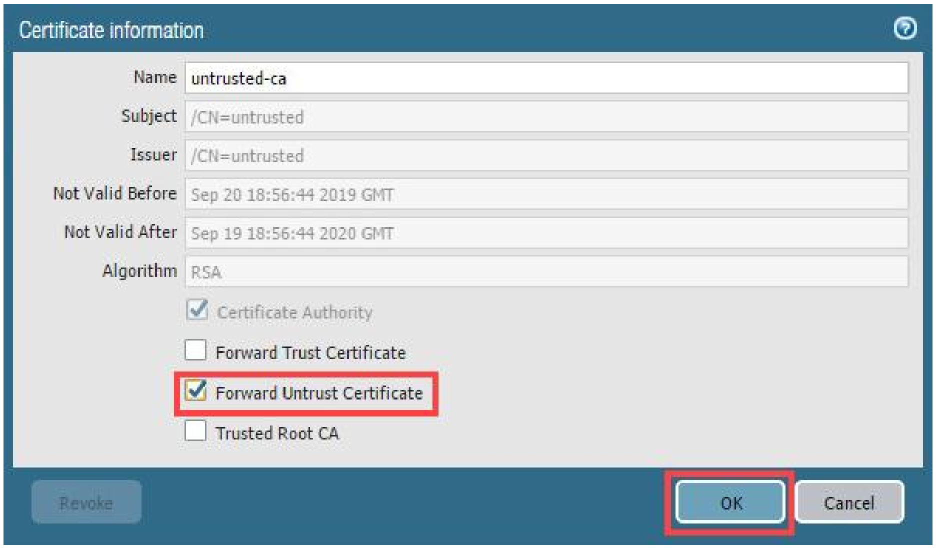
☐ Trusted Root CA

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



☐ Name	Subject	Issuer	CA
☐ trusted-ca	CN = 192.168.1.1	CN = 192.168.1.1	☑
☐ untrusted-ca	CN = untrusted	CN = untrusted	☑

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



Certificate information

Name	untrusted-ca
Subject	/CN=untrusted
Issuer	/CN=untrusted
Not Valid Before	Sep 20 18:56:44 2019 GMT
Not Valid After	Sep 19 18:56:44 2020 GMT
Algorithm	RSA

☑ Certificate Authority

☐ Forward Trust Certificate

☑ Forward Untrust Certificate

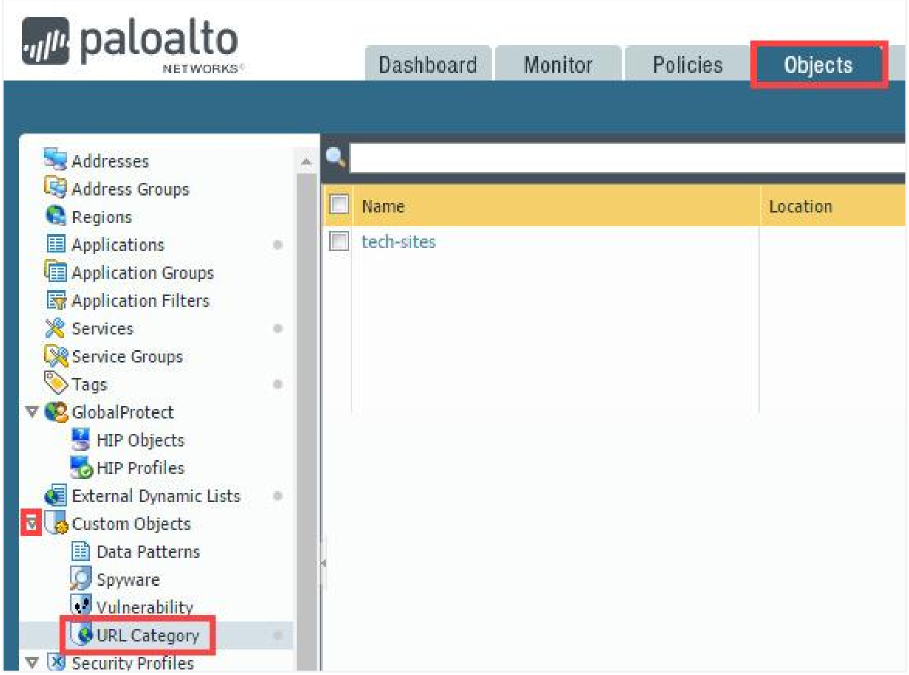
☐ Trusted Root CA

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

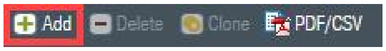
1.3 Create a Custom Decryption URL Category

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**.



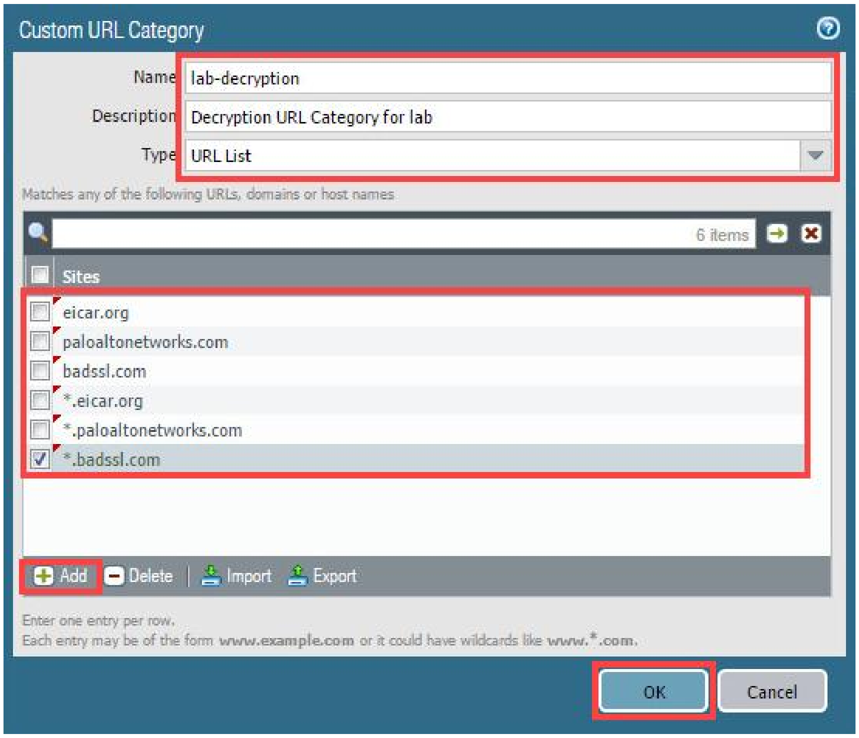
2. Click **Add** to open the *Custom URL Category* configuration window.



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

Parameter	Value
Name	Type `lab-decryption`
Description	Type `Decryption URL Category for lab`
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

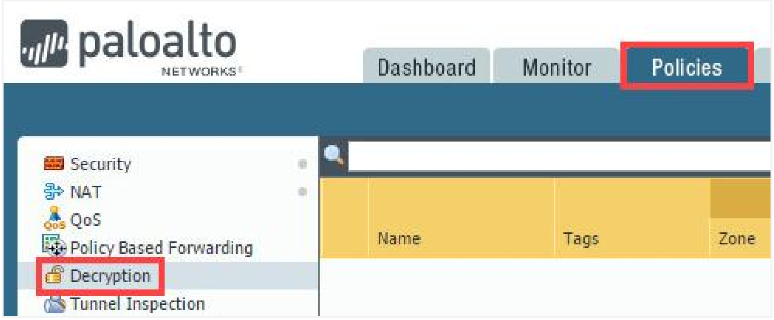
Enter one entry per row.
Each entry may be of the form **www.example.com** or it could have wildcards like **www.*.com**.

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

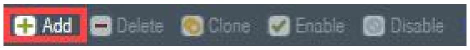
1.4 Create a Decryption Policy

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**.

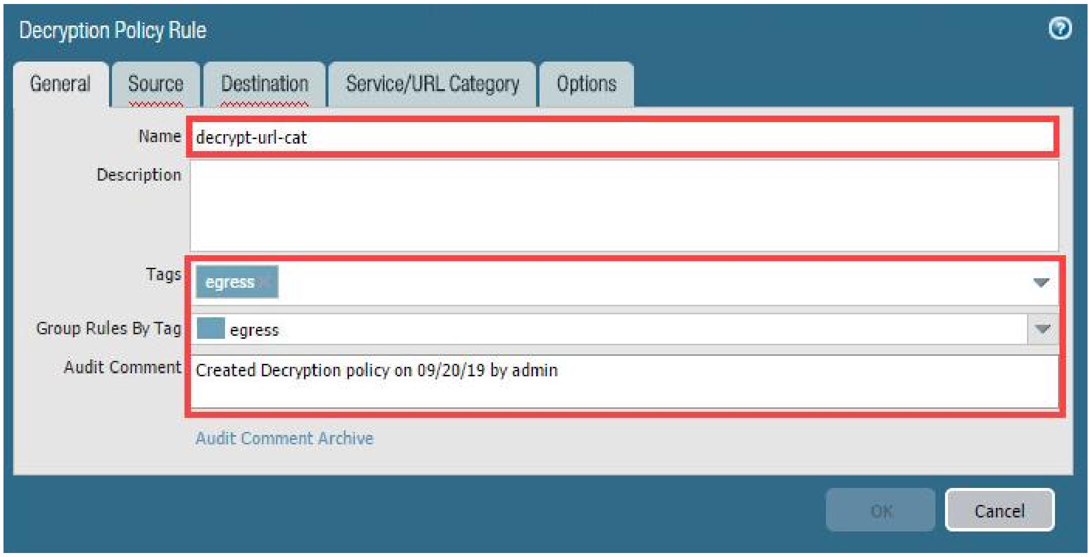


2. Click **Add** to create a Decryption policy rule.



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

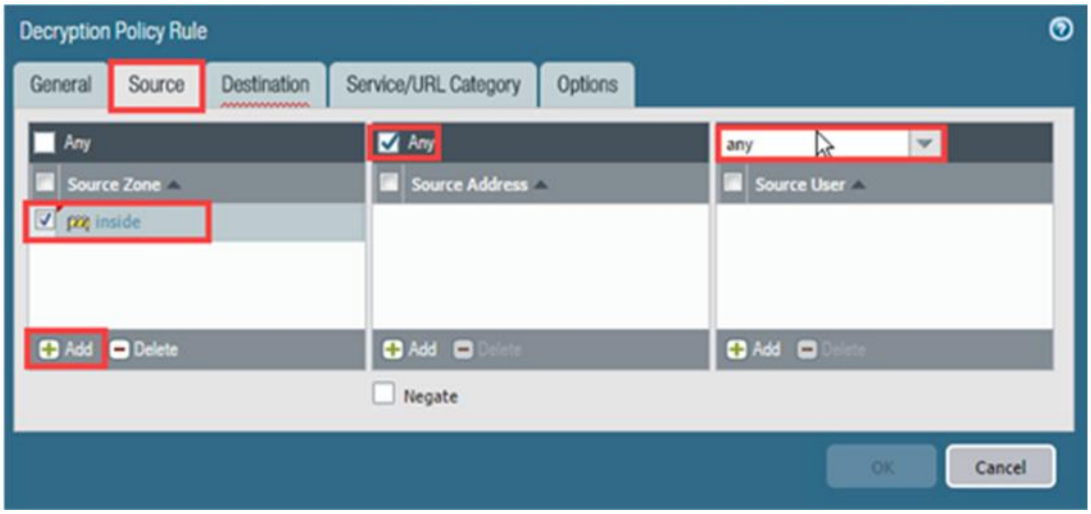
Parameter	Value
Name	Type **`decrypt-url-cat`**
Tags	Select **egress** from the drop-down list
Group Rules By Tag	Select **egress** from the drop-down list
Audit Comment	Type **`Created Decryption policy on <date> by admin`**


Decryption Policy Rule

Name: decrypt-url-cat
Description:
Tags: egress
Group Rules By Tag: egress
Audit Comment: Created Decryption policy on 09/20/19 by admin

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

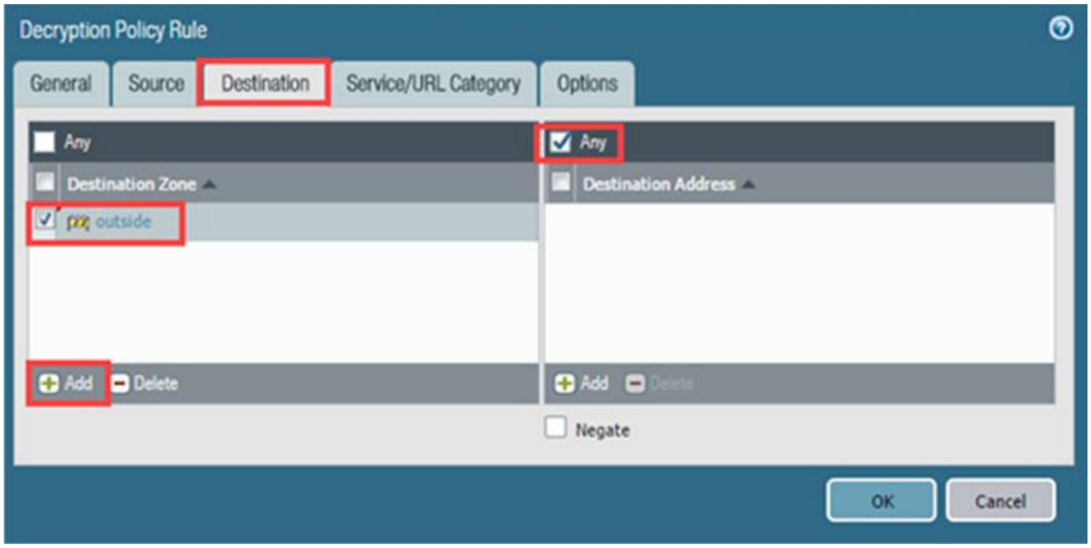
Parameter	Value
Source Zone	Click **Add** and select **inside** from the drop-down list
Source Address	Verify that the **Any** checkbox is selected
Source User	Verify that **any** is selected


Decryption Policy Rule

□ Any
Source Zone
☑ inside
☑ Any
Source Address
any
Source User
□ Negate

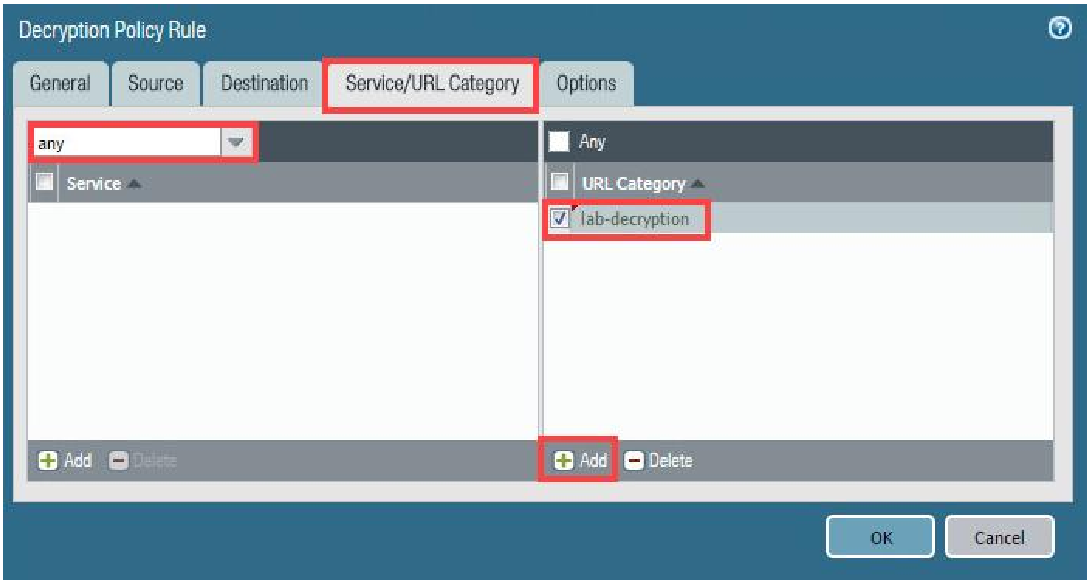
5. In the *Decryption Policy Rule* window, click the **Destination** tab and configure the following:

Parameter	Value
Destination Zone	Click **Add** and select **outside** from the drop-down list
Destination Address	Verify that the **Any** checkbox is selected



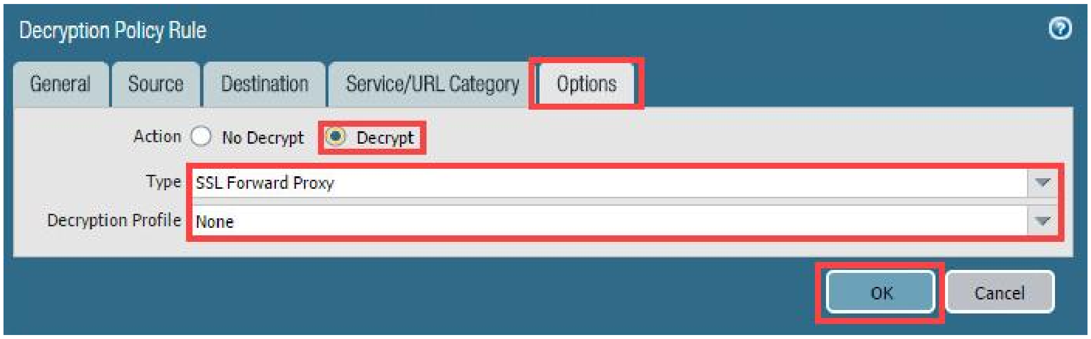
6. In the *Decryption Policy Rule* window, click the **Service/URL Category** tab and configure the following:

Parameter	Value
Service	Verify that **any** is selected
URL Category	Click **Add** and select **lab-decryption** from the drop-down 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

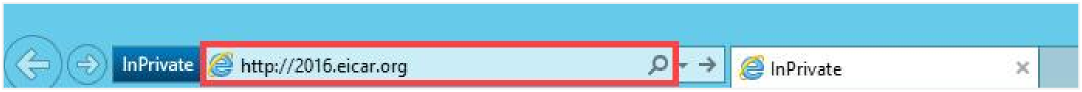


Action ○ No Decrypt ● Decrypt
Type: SSL Forward Proxy
Decryption Profile: None

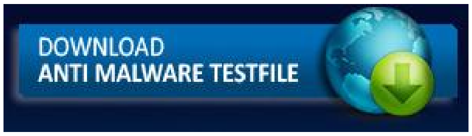
8. **Commit** all changes.

1.5 Test AV Security Profile with the Decryption Policy

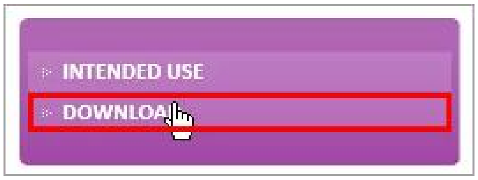
1. Open a new **Internet Explorer** browser window in **private/incognito** mode and browse to `http://2016.eicar.org`.



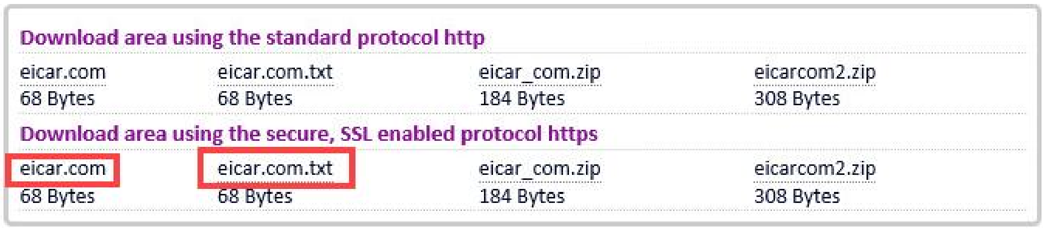
2. Click the **Download Anti Malware Testfile** image in the upper-right corner of the webpage.



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

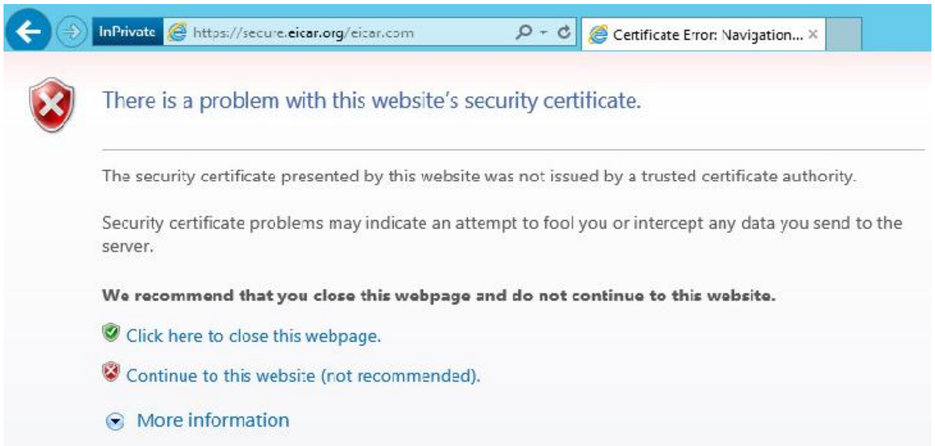


4. Within the *Download* area at the bottom of the page, click either the **eicar.com** or the **eicar.com.txt** file to download the file using the SSL-enabled HTTPS protocol.



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

Notice a certificate issue is presented:


InPrivate
https://secure.eicar.org/eicar.com
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).

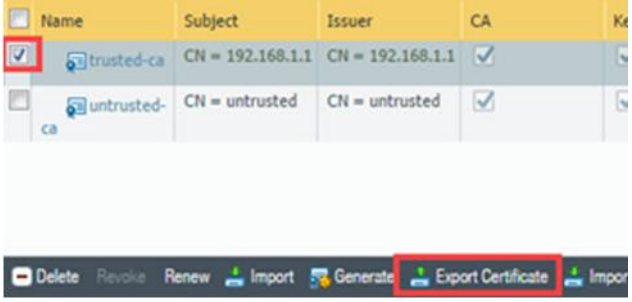
More information

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

5. Close the **IE** browser.

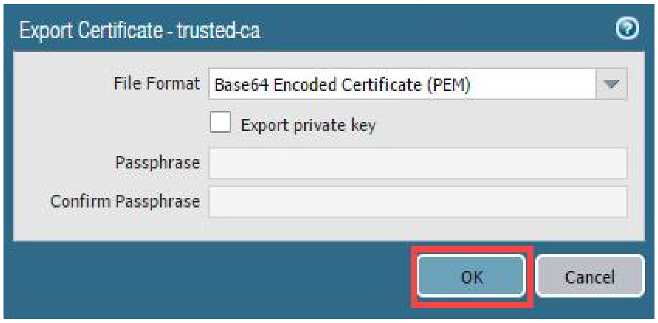
1.6 Export the Firewall Certificate

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.



□	Name	Subject	Issuer	CA	Ke
☑	trusted-ca	CN = 192.168.1.1	CN = 192.168.1.1	✓	
□	untrusted-ca	CN = untrusted	CN = untrusted	✓	

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



Export Certificate - trusted-ca

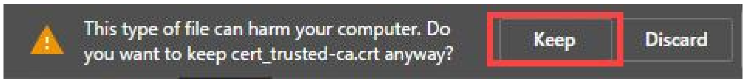
File Format: Base64 Encoded Certificate (PEM)

□ Export private key

Passphrase

Confirm Passphrase

4. If prompted, click **Keep**.

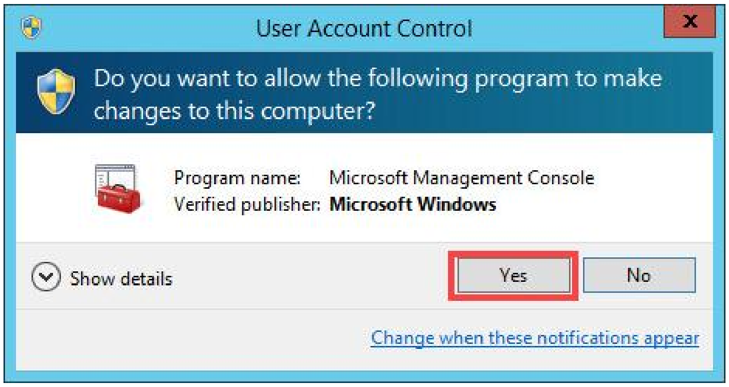


This type of file can harm your computer. Do you want to keep cert_trusted-ca.crt anyway?

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

1.7 Import the Firewall Certificate

1. On the Windows desktop, double-click the **certificates** icon.
2. If prompted, click **Yes** to continue.

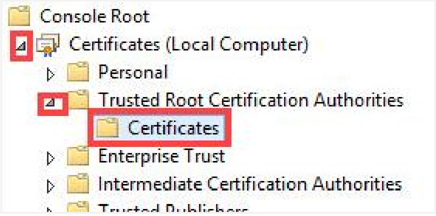


User Account Control

Do you want to allow the following program to make changes to this computer?

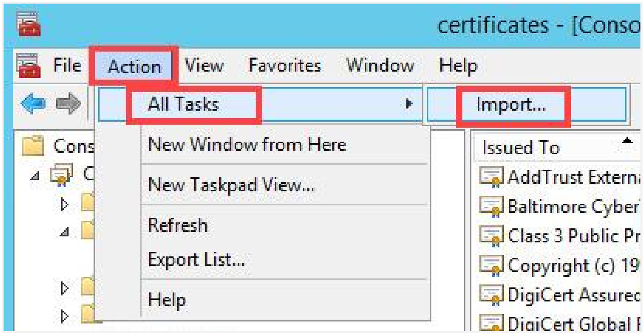
Program name: Microsoft Management Console
Verified publisher: **Microsoft Windows**

3. In the *certificates - [Console Root]* window, expand **Certificates (Local Computer)**, and then expand **Trusted Root Certification Authorities** and select the **Certificates** folder.

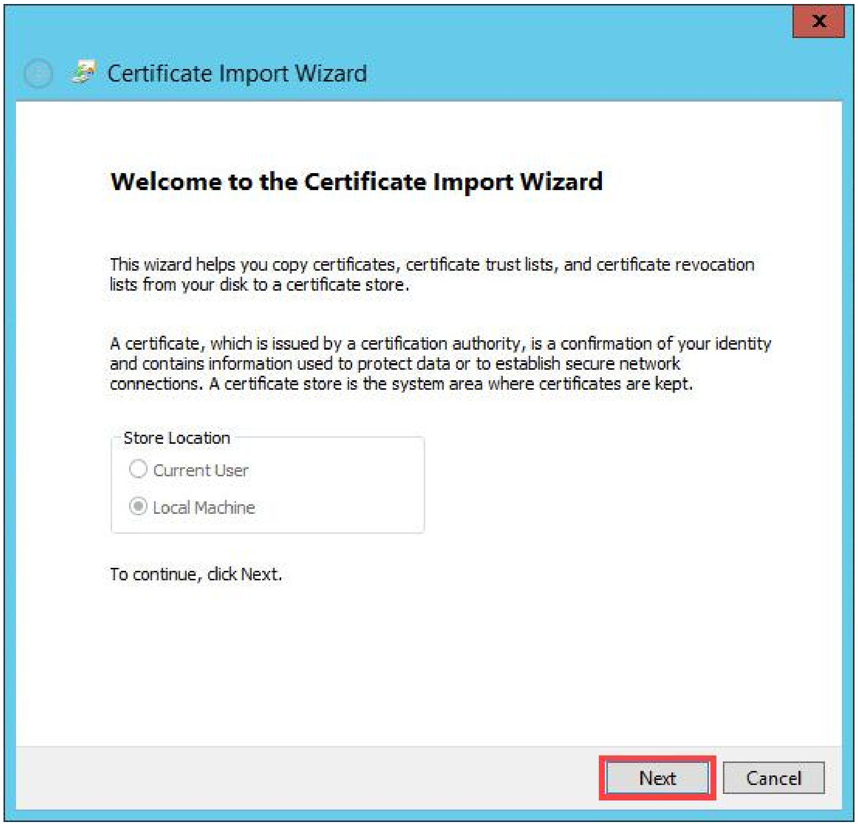


Console Root
Certificates (Local Computer)
Personal
Trusted Root Certification Authorities
Certificates
Enterprise Trust
Intermediate Certification Authorities
Trusted Publishers

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



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



Welcome to the Certificate Import Wizard

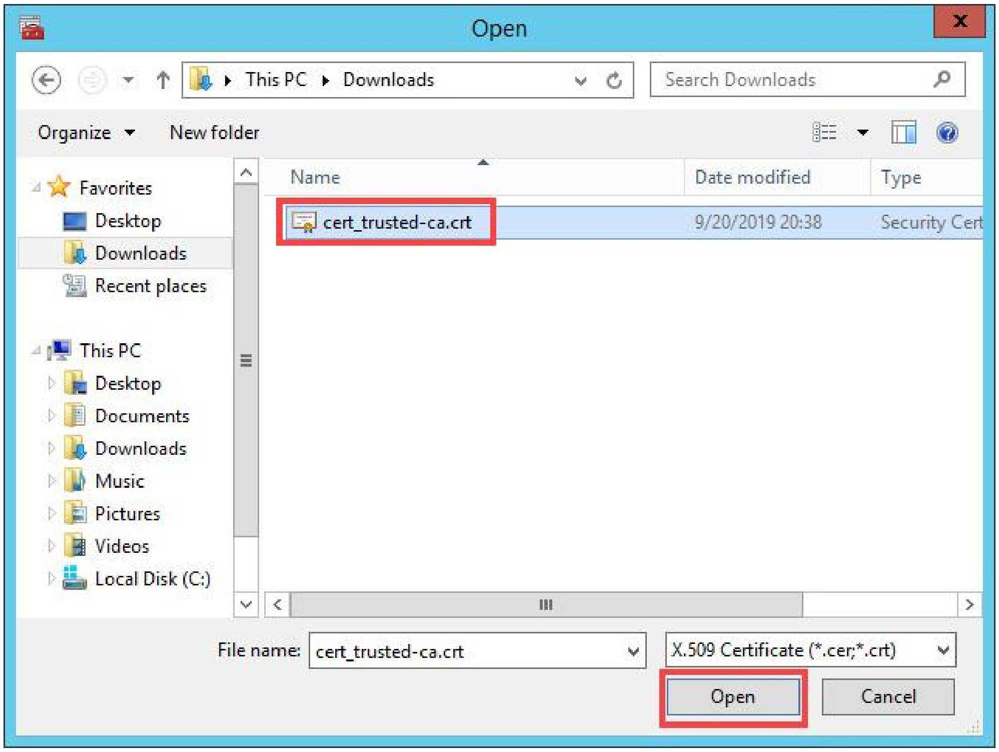
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

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.

6. On the next step, click **Browse** and select the recently exported **cert_trusted-ca.crt** file in the *Downloads* directory. Click **Open**.

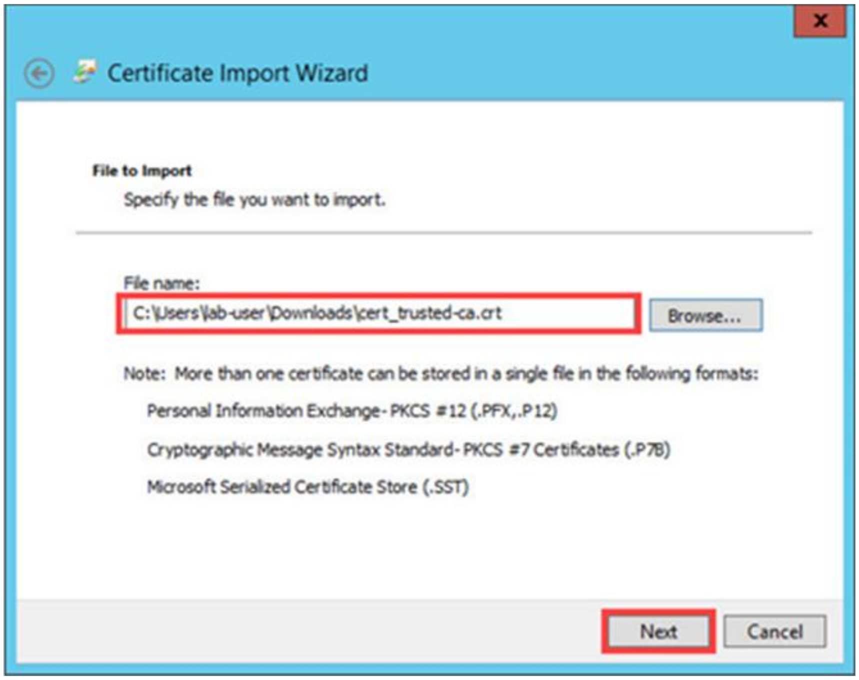


Name	Date modified	Type
cert_trusted-ca.crt	9/20/2019 20:38	Security Cert

File name: cert_trusted-ca.crt

X.509 Certificate (*.cer;*.crt)

7. Confirm that the correct file is selected and click **Next** to continue.



File to Import

Specify the file you want to import.

File name:

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

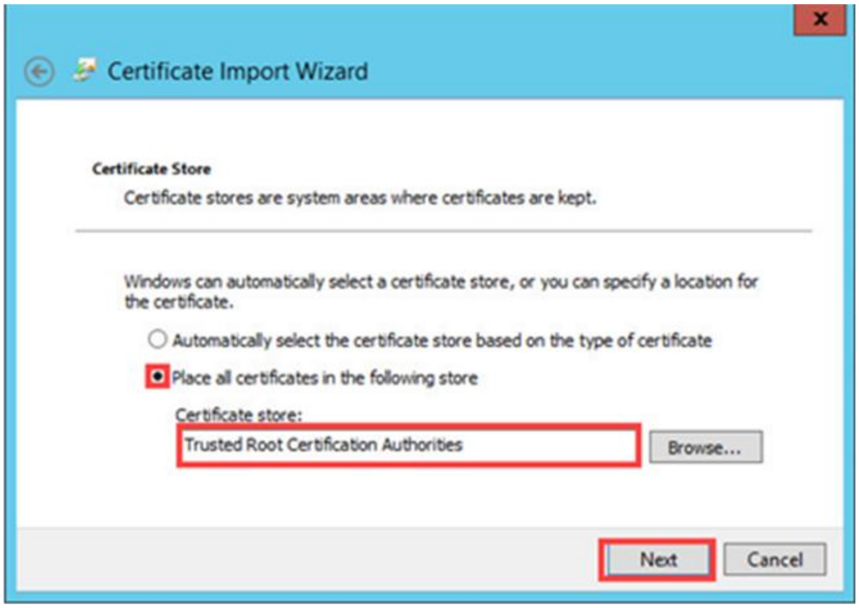
Note: More than one certificate can be stored in a single file in the following formats:

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

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

Microsoft Serialized Certificate Store (.SST)

8. Verify that the following is configured. Click **Next**.



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.

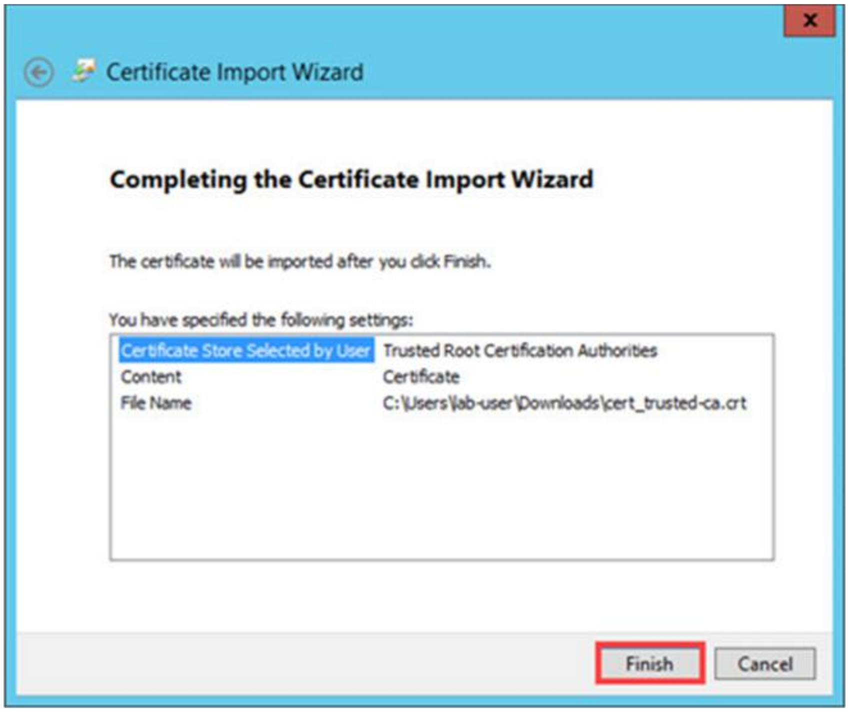
○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store:

Trusted Root Certification Authorities

9. Click **Finish** to import the certificate.



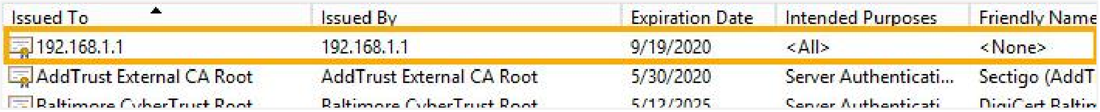
Completing the Certificate Import Wizard

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

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

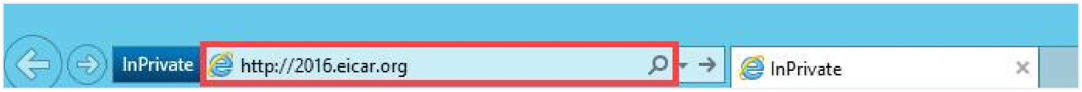


Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name
192.168.1.1	192.168.1.1	9/19/2020	<All>	<None>
AddTrust External CA Root	AddTrust External CA Root	5/30/2020	Server Authenticati...	Sectigo (AddT
Baltimore CyberTrust Root	Baltimore CyberTrust Root	5/12/2025	Server Authenticati...	DigiCert Baltin

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

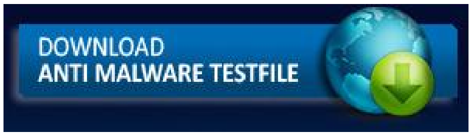
1.8 Test the Decryption Policy

1. Open a new **Internet Explorer** browser window in **private/incognito** mode and browse to **`http://2016.eicar.org`**.

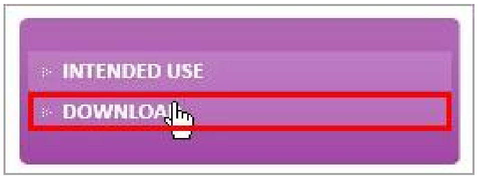


http://2016.eicar.org

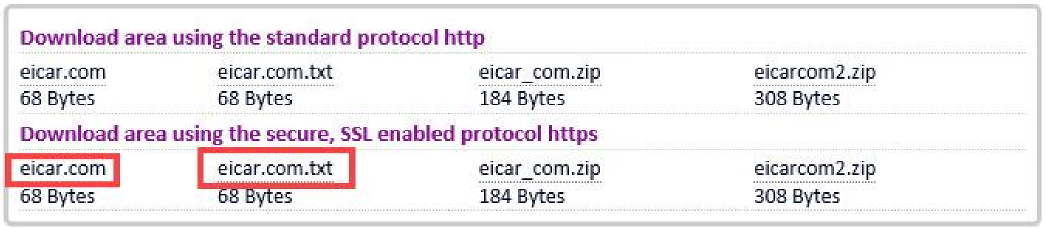
2. Click the **Download Anti Malware Testfile** image in the upper-right corner of the webpage.



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 the SSL-enabled HTTPS protocol.



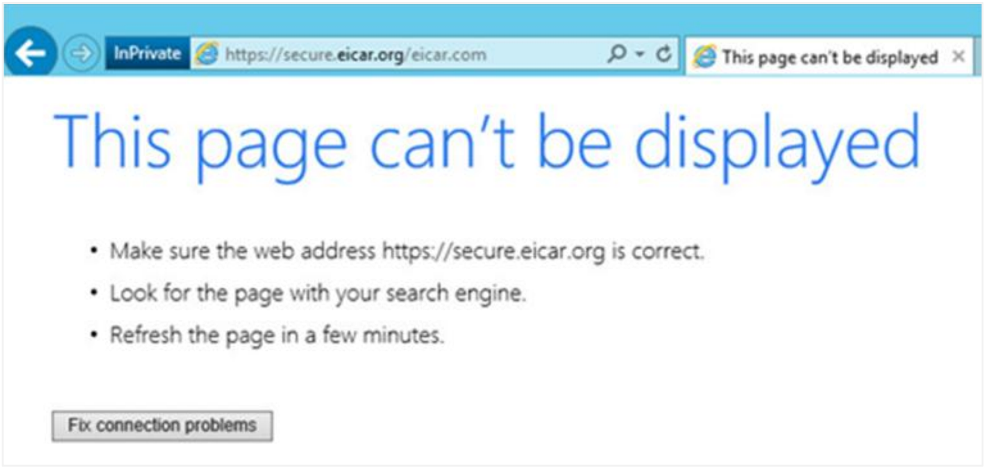
Download area using the standard protocol http

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

Notice that the eicar test file is detected, and the connection gets reset.



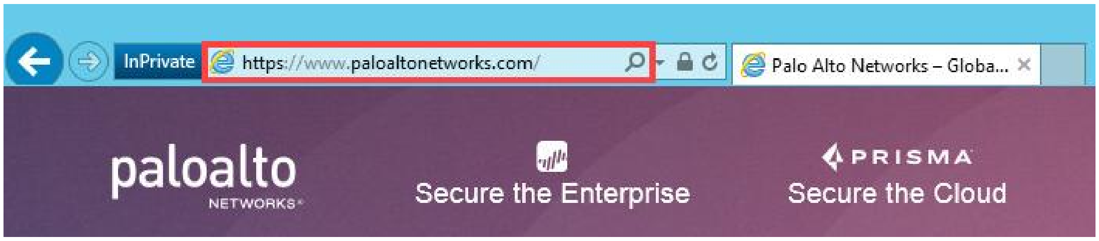
https://secure.eicar.org/eicar.com

This page can't be displayed

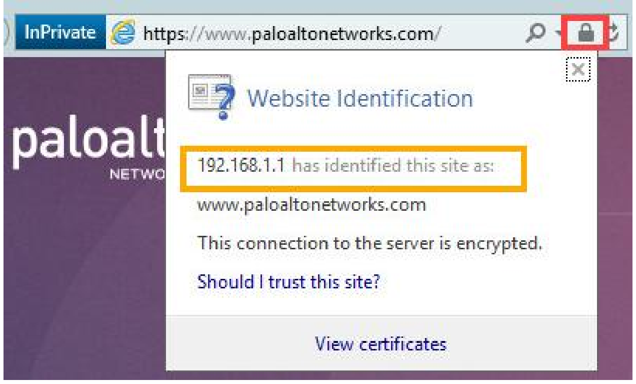
This page can't be displayed

- 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`**. Notice that there is no certificate warning, and the page is displayed correctly.



6. Click the **lock** 🔒 icon next to the URL in the browser and notice that the signer is the firewall *192.168.1.1*.



Website Identification

192.168.1.1 has identified this site as:

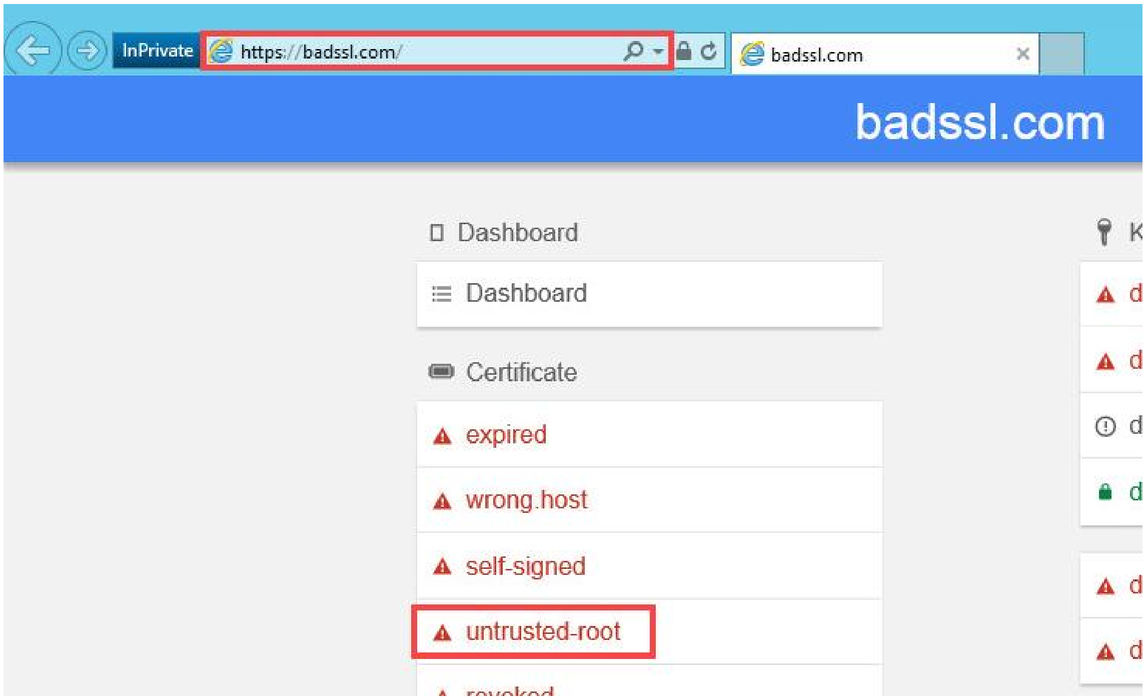
www.paloaltonetworks.com

This connection to the server is encrypted.

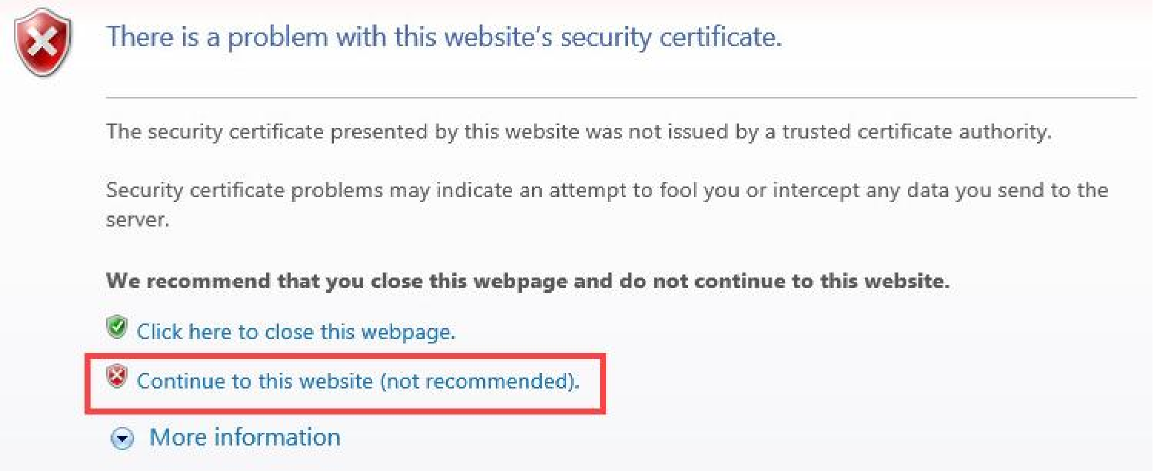
Should I trust this site?

View certificates

7. Close the **IE** browser.
8. Open a new **Internet Explorer** browser window in **private/incognito** mode and browse to **`https://www.badssl.com`**, then click on **untrusted-root**.



9. Notice that a certificate warning is now displayed. Click on the **Continue to this website (not recommended)** link.



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

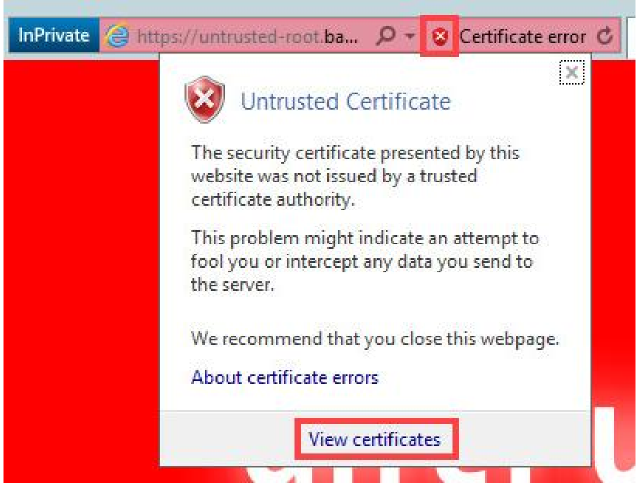
The security certificate presented by this website was not issued by a trusted certificate authority.

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, followed by clicking **View certificates**.



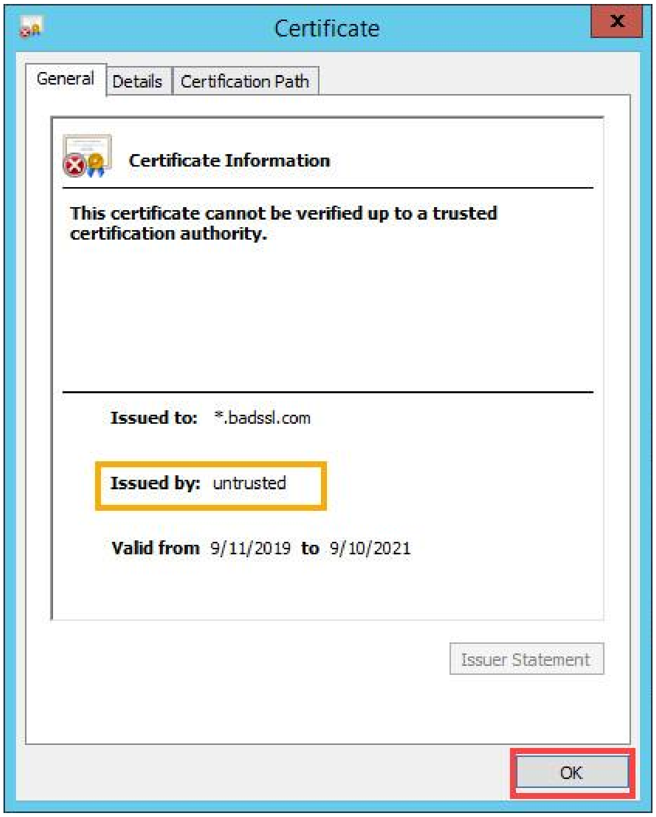
Untrusted Certificate

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.

11. Notice that the certificate is still signed by the firewall. However, it was signed with the untrusted certificate. Click **OK**.



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

Issued to: *.badssl.com

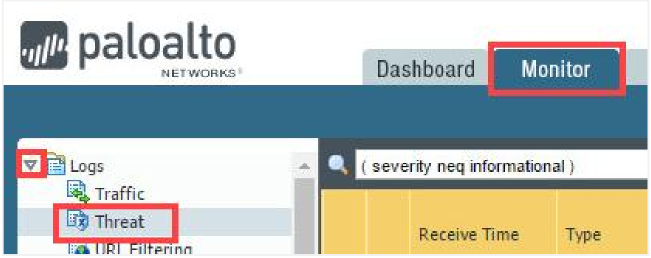
Issued by: untrusted

Valid from 9/11/2019 to 9/10/2021

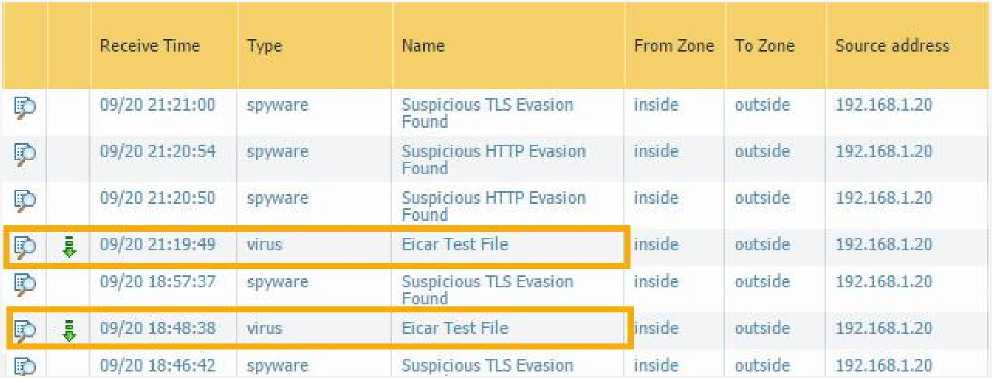
12. Close the **IE** browser.

1.9 Review Logs

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

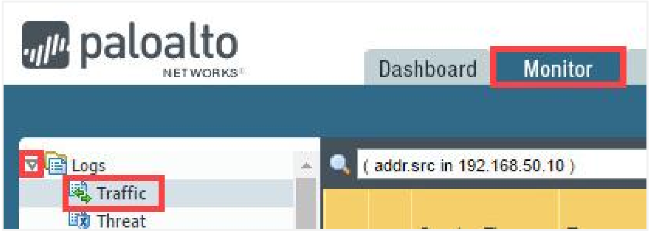


2. Clear any existing filters and notice that there is an entry for when the connection was reset in the browser.



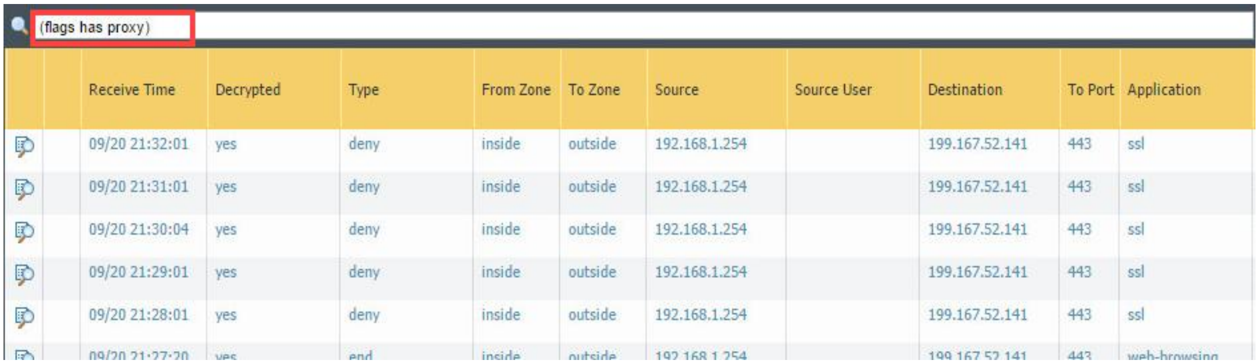
		Receive Time	Type	Name	From Zone	To Zone	Source address
		09/20 21:21:00	spyware	Suspicious TLS Evasion Found	inside	outside	192.168.1.20
		09/20 21:20:54	spyware	Suspicious HTTP Evasion Found	inside	outside	192.168.1.20
		09/20 21:20:50	spyware	Suspicious HTTP Evasion Found	inside	outside	192.168.1.20
		09/20 21:19:49	virus	Eicar Test File	inside	outside	192.168.1.20
		09/20 18:57:37	spyware	Suspicious TLS Evasion Found	inside	outside	192.168.1.20
		09/20 18:48:38	virus	Eicar Test File	inside	outside	192.168.1.20
		09/20 18:46:42	spyware	Suspicious TLS Evasion	inside	outside	192.168.1.20

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



(addr.src in 192.168.50.10)

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)

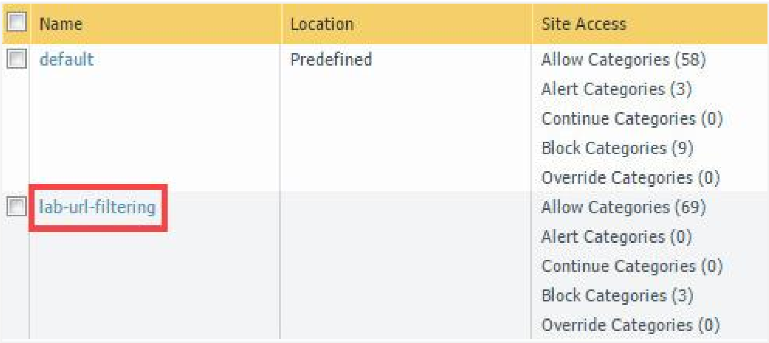
		Receive Time	Decrypted	Type	From Zone	To Zone	Source	Source User	Destination	To Port	Application
		09/20 21:32:01	yes	deny	inside	outside	192.168.1.254		199.167.52.141	443	ssl
		09/20 21:31:01	yes	deny	inside	outside	192.168.1.254		199.167.52.141	443	ssl
		09/20 21:30:04	yes	deny	inside	outside	192.168.1.254		199.167.52.141	443	ssl
		09/20 21:29:01	yes	deny	inside	outside	192.168.1.254		199.167.52.141	443	ssl
		09/20 21:28:01	yes	deny	inside	outside	192.168.1.254		199.167.52.141	443	ssl
		09/20 21:27:20	yes	end	inside	outside	192.168.1.254		199.167.52.141	443	web-browsing

> If the *Decrypted* column is not present, hover the mouse over *Receive Time* and click the **drop-down** arrow and check the check box for **Decrypted** to add the column view.

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

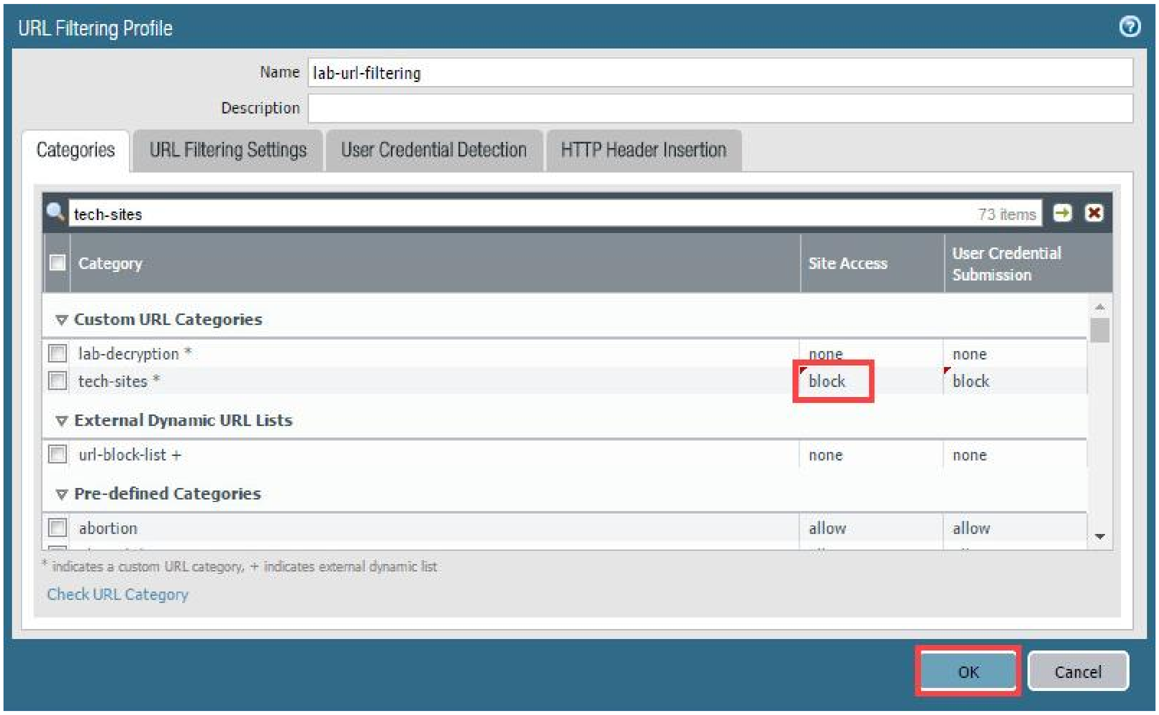
1.10 Test URL Filtering with Decryption

1. In the web interface, select **Objects > Security Profiles > URL Filtering**.
2. Click on **lab-url-filtering** to open the object.



□ Name	Location	Site Access
□ default	Predefined	Allow Categories (58) Alert Categories (3) Continue Categories (0) Block Categories (9) Override Categories (0)
□ lab-url-filtering		Allow Categories (69) Alert Categories (0) Continue Categories (0) Block Categories (3) Override Categories (0)

3. 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**.



Name lab-url-filtering

Description

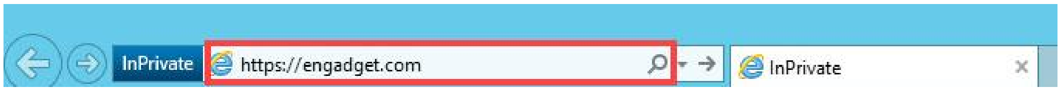
tech-sites 73 items

□ Category	Site Access	User Credential Submission
▽ Custom URL Categories		
□ lab-decryption *	none	none
□ tech-sites *	block	block
▽ External Dynamic URL Lists		
□ url-block-list +	none	none
▽ Pre-defined Categories		
□ abortion	allow	allow

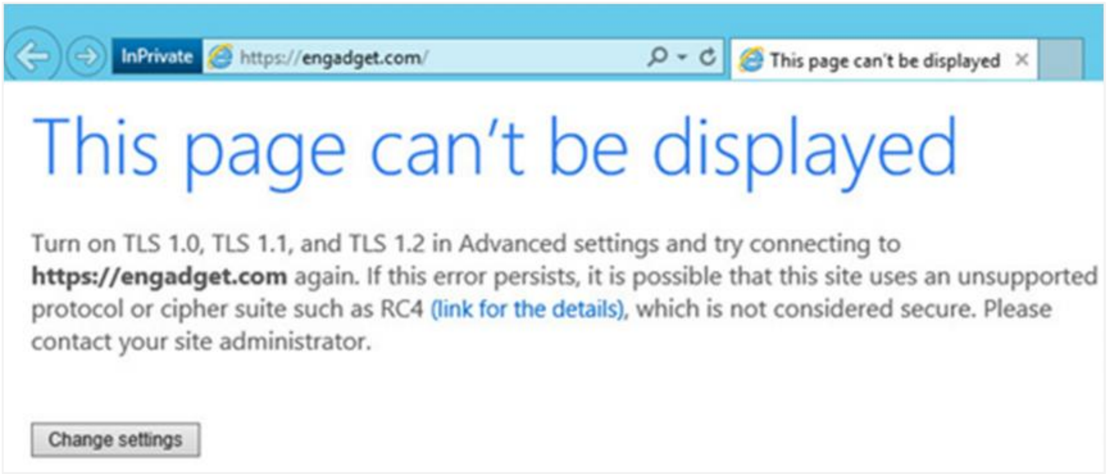
* indicates a custom URL category, + indicates external dynamic list

Check URL Category

4. **Commit** all changes.
5. Open a new **Internet Explorer** browser window in **private/incognito** mode 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*.



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.

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