13 - Blocking Threats in Encrypted Traffic

1. In the web interface, navigate to Device > Setup > Operations and click on Load named configuration snapshot underneath the Configuration Management section.
2. In the Load Named Configuration window, select edu-210-lab-13.xml from the Name dropdown box and click OK.
3. In the Loading Configuration window, a message will show Configuration is being loaded. Please check the Task Manager for its status. You should reload the page when the task is completed. Click Close to continue.
4. Click the Tasks icon located at the bottom-right of the web interface.
5. In the Task Manager – All Tasks window, verify the Load type has successfully completed. Click Close.
6. Click the Commit link located at the top-right of the web interface.
7. In the Commit window, click Commit to proceed with committing the changes.
8. When the Commit operation successfully completes, click Close to continue.
9. Leave the Palo Alto Networks Firewall open and continue to the next task.

1.2 Test the Firewall Behavior Without Decryption
In this section, you will test the firewall behavior without decryption by downloading a virus.

1. Open a new tab in Chromium.

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

changes since the last commit.

2. Type http://192.168.50.80/eicar.com and press Enter. You should get a blocked page.
3. In the new tab, type www.eicar.org. Press Enter.
4. Click the link for Download Anti Malware Testfile.

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

5. Scroll down and locate the section Download area. Right-click the link for the eicar.com file and select Save link as.
6. In the Save File window, save to the ~/Downloads directory and click Save.
7. Notice at the bottom of the Chromium window that the download is not blocked because the connection is encrypted, and the virus is hidden. This exercise proves that without decryption, the firewall is unable to examine the contents of an encrypted connection to scan for malicious content.
8. Close the two Chromium tabs that you just opened.
9. Leave the Palo Alto Networks Firewall open and continue to the next task.
   1.3 Create a Self-Signed Certificate for Trusted Connections
   In this section, you will generate a certificate on the firewall that will be used when clients connect to
   HTTPS websites that have certificates issued by trusted certificate authorities.
   The firewall will use this certificate as part of the decryption process between clients and trusted
   HTTPS websites.

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

1. Select Device > Certificate Management > Certificates. Click Generate to create a new CA Certificate.
2. In the Generate Certificate window, configure the following. Click Generate.
    - Parameter Value
        - Certificate Name trusted-cert
        - Common Name 192.168.1.1
        - Certificate Authority Certificate Authority
3. In the Generate Certificate window, click OK.

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

4. You should have a new entry in the Device Certificates table. Click trusted-cert.
5. In the Certificate information window, place a check in the box for Forward Trust Certificate. Click OK.
6. Leave the Palo Alto Networks Firewall open and continue to the next task.
   1.4 Create a Self-Signed Certificate for Untrusted Connections
7. Click Generate to create a new CA Certificate.
8. In the Generate Certificate window, configure the following. Click Generate.
   Parameter Value
   Certificate Name untrusted-cert

Common Name untrusted
Certificate Authority Certificate Authority

9. In the Generate Certificate window, click OK.

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

4. You should have a new entry in the Device Certificates table. Click untrusted-cert.
5. In the Certificate information window, place a check in the box for Forward untrust Certificate. Click OK.
6. Leave the Palo Alto Networks Firewall open and continue to the next task.

1.5 Create Decryption Policy for Outbound Traffic

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

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

1. Select Policies > Decryption. Click Add.
2. In the Decryption Policy Rule window, under the General tab, configure the following.
    - Parameter Value
        - Name Decrypt_User_Traffic
        - Description Decrypts web traffic from Users_Net.
3. Click the Source tab and configure the following.
    - Parameter Value
        - Source Zone Users_Net
        - Source Address Any
        - Source User any

4. Click the Destination tab and configure the following.
    - Parameter Value
        - Destination Zone Internet
        - Extranet
        - Destination Address Any
5. Click the Service/URL Category tab and verify that the Service is set to Any and that the box for Any above URL Category is checked.
6. Click the Options tab and configure the following. Click OK.
    - Parameter Value
        - Action Decrypt
        - Type SSL Forward Proxy
        - Decryption Profile None
7. Verify the Decryption policy is visible, and the configuration matches the following.
8. Click the Commit link located at the top-right of the web interface.
9. In the Commit window, click Commit to proceed with committing the changes.
10. When the Commit operation successfully completes, click Close to continue.

1.6 Test Outbound Decryption Policy

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

1. On the client desktop, open the Firefox Web Browser application.
2. Type https://www.eicar.org and press Enter. The browser presents a warning message. Click Advanced.

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

3. Click the link for View Certificate.

4. Under the section for www.eicar.org, note the Issuer Name section contains 192.168.1.1.
5. Minimize the Firefox Web Browser.
6. If you minimized the firewall, reopen the Firewall interface by clicking on the Chromium tab in the taskbar.

1.7 Export the Firewall Certificate

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

1. Select Device > Certificate Management > Certificates. Highlight but do not open trusted-cert.
2. At the bottom of the window, click Export Certificate to open the Export Certificate configuration window.

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

3. In the Export Certificate – trusted-cert window, leave all settings unchanged. Click OK to export the trusted-cert certificate.
4. Minimize the Palo Alto Networks Firewall and continue to the next task.

1.8 Import the Firewall Certificate

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

1. On the client desktop, reopen the Firebox Web Browser by clicking the Firefox icon in the taskbar.
2. In the upper-right corner of the window, click the “hamburger” button and choose Preferences.
3. On the left side of the Preferences screen, select Privacy & Security.

4. Scroll to the bottom of the screen and locate the Certificates section. Click View Certificates.
5. In the Certificate Manager window, select the Authorities tab. Click Import.
6. In the Select File containing CA certificate(s) to import window, click Downloads. Select cert_trusted-cert.crt and click Open.
7. In the Downloading Certificate window, place checks in both boxes for Trust this CA. Click OK.
8. The firewall trusted-cert entry appears in the list of certificate authorities. Click OK.

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

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

1.9 Test Outbound Decryption Policy Again

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

10. In the new Firefox tab, type https://www.eicar.org. Press Enter.
11. Click the link for Download Anti Malware Testfile.
12. Scroll down and locate the section Download area. Click the link for the eicar.com file download.
13. You will receive a warning pane from the firewall indicating that it has detected and blocked the malicious file download.
14. Close the Firefox Web Browser by clicking the close icon.
15. Reopen the PA-VM firewall web interface by clicking on the Chromium icon in the taskbar and continue to the next task.

1.10 Review Firewall Logs

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

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

The kind of message a client receives will vary depending on the browser.

2. Add the Decrypted column to the table by selecting Columns > Decrypted.
3. Drag and drop the Session End Reason column from the right side of the table to the beginning of the table. You may need to scroll the Traffic window to find the Session End Reason.
4. In the filter builder, type (flags has proxy) and (session_end_reason eq threat).
5. Click the magnifying glass next to the entry listed to see details about the session.
6. In the Detailed Log View window, you should see similar information indicating that the firewall detected the eicar.com file and used reset-server to terminate the session.
7. Select Monitor > Logs > Threat.
8. Delete any filters in place. Notice the entry for virus indicates that the firewall detected and blocked the eicar.com file.
9. Leave the Palo Alto Networks Firewall open and continue to the next task.

1.11 Exclude URL Categories from Decryption

- The existing decryption policy rule you created instructs the firewall to decrypt all traffic, regardless of the URL category. In this section, you will configure a no-decrypt rule that instructs the firewall to exclude

sensitive categories of web traffic from decryption in order to avoid exposing PII (Personally Identifiable Information).

1. In the firewall web browser, select Policies > Decryption. Click Add.
2. In the Decryption Policy Rule under the General tab, enter No-Decryption for Name. For Description, enter Do not decrypt URLs in gov, shopping and finance.
3. Select the tab for Source. Under the Source Zone section, click Add and select Users_Net.
4. Select the Destination tab. Under the Destination Zone section, click Add and select Internet.
5. Select the tab for Service/URL Category. Leave the Service set to any.
6. Under the URL Category, use the Add button to add government, financial-services, and shopping.
7. Select the tab for Options. Verify that the Action is set to No Decrypt. Click OK.
8. You should have two entries in the Decryption policy. Do you notice what is wrong with the Decryption Policies? The answer is yes. They are in the wrong order. All traffic will match the first rule Decrypt_Users_Traffic because the URL category is set to any. The firewall will therefore never proceed beyond that first rule to implement the second rule, which instructs the firewall to exclude financial-services, government, and shopping websites from decryption
9. Drag and drop the No-Decryption rule entry above the Decrypt_User_Traffic.
10. Click the Commit link located at the top-right of the web interface.
11. In the Commit window, click Commit to proceed with committing the changes.
12. When the Commit operation successfully completes, click Close to continue.
13. Minimize the Palo Alto Networks Firewall and continue to the next task.

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

1.12 Test the No-Decryption Rule

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

1. On the client desktop, open the Firefox Web Browser application.
2. Type https://www.texas.gov and press Enter.
3. Click the padlock icon to view the site information window for texas.gov. Click the arrow next to Connection secure.
4. In the Connection Security for www.texas.gov window, click More Information.
5. In the Page Info – https://www.texas.gov window, click View Certificate.
6. Note that the Issuer Name is not 192.168.1.1.
7. The lab is now complete; you may end your reservation.

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