10 - Blocking Threats using Custom Applications

1.1 Apply a Baseline Configuration to the Firewall
In this section, you will load the Firewall configuration file.

7. In the web interface, navigate to Device > Setup > Operations and click on Load named
   configuration snapshot underneath the Configuration Management section.
8. In the Load Named Configuration window, select edu-210-lab-10.xml from the Name dropdown
   box and click OK.
9. 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.
10. Click the Tasks icon located at the bottom-right of the web interface.
11. In the Task Manager – All Tasks window, verify the Load type has successfully completed. Click Close.
12. Click the Commit link located at the top-right of the web interface.
13. In the Commit window, click Commit to proceed with committing the changes.

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

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

1.2 Gather Custom Application Information

You will gather information about the traffic that this application uses so that you can create a custom
application signature.

1. On the client desktop, double-click the folder for Class-Scripts.

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. Open the EDU-210 folder.
3. Double-click the icon for Custom-App-1.
4. Press Enter to start the Custom-App-1 script. Allow the script to complete. Once the Custom-App-1
script completes, press Enter.

5. If you minimized the firewall, reopen the firewall interface by clicking on the Chromium tab in the
taskbar.
6. In the web interface, select Monitor > Logs > Traffic. Create and apply the following new filter
(addr.dst eq 192.168.50.22) in the filter builder. Write down the Source IP address,
Destination IP address, Port number, and the IP protocol. If the IP Protocol column is not displayed,
place your mouse pointer over any column header and select Columns > IP

Protocol.
7. Leave the Palo Alto Networks Firewall open and continue to the next task.
1.3 Configure a Packet Capture
In this section, you will configure a packet capture on the firewall's data plane. The goal of the packet
capture is to identify a unique bit pattern that can be used to create a custom application signature.

1. In the web interface, select Monitor > Packet Capture. Click Clear All Settings.

2. In the Clear All Settings window, click Yes.
3. In the PCAP settings cleared window, click OK.
4. In the Configure Filtering window, click Manage Filters.
5. In the Packet Capture Filter window, click Add.

6. In the Packet Capture Stage window, configure the following. Click OK.
Parameter Value
Id 1
Ingress Interface ethernet1/2
Source 192.168.1.20
Destination 192.168.50.22
Dest Port 80
Proto 6 (This number is assigned to TCP.)
Non-IP exclude
7. Toggle the Filtering button to ON.

In Internet Protocol v4, there is a value called protocol to associate the next level protocol. 6 is the number assigned to TCP.

8. Under the section for Configure Capturing, click Add to configure a file for the receive stage on the
firewall.
9. In the Packet Capture Stage window, configure the following. Click OK.

Parameter	Value
Stage	receive
File	receive-file.pcap

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

1.4 Packet Capture Application Traffic

In this section, you will take a packet capture on the firewall while using the Custom Application on the
client host.

1. Ensure you are still located at Monitor > Packet Capture. Toggle Packet Capture to ON.

2. In the Packet Capture Warning window, click OK.
3. Minimize the Palo Alto Networks Firewall.
4. Open the EDU-210 folder by clicking on the File Manager tab in the taskbar if necessary. Double□click the icon for Custom-App-1.

The firewall is now actively capturing packets that match the filter you created. The packets are being stored on the firewall in the receive□file.pcap you designated.

5. Press Enter to start the Custom-App-1 script. Allow the script to complete. Once the Custom-App-1
script completes, press Enter.
6. If you minimized the firewall, reopen the firewall interface by clicking on the Chromium tab in the
taskbar.
7. Ensure you are still located at Monitor > Packet Capture. Toggle Packet Capture to OFF.
8. Refresh the web interface display to view the receive-file listed in the Captured Files panel. Click
receive-file.pcap to open it in Wireshark and continue to the next task.

1.5 Analyze the Packet Capture
In this section, you will use Wireshark to analyze the packet capture to discover a unique bit pattern
that identifies traffic to the Custom Application.

1. In the Wireshark window, find and highlight the first entry for GET.
2. In the Wireshark window, click Hypertext Transfer Protocol to expand the display and notice that
   the HTTP request header included a GET /custom-app.txt entry and the Host 192.168.50.22.
3. Close the Wireshark window.
4. Ensure you are still located at Monitor > Packet Capture. Click Clear All Settings.
   You will use the HTTP GET method, and the URI path customapp.txt to build a custom application signature for the Custom Application

5. In the Clear All Settings window, click Yes.
6. In the PCAP settings clear window, click OK.
7. In the Captured Files window, select the checkbox next to receive-file-pcap. Click Delete.
8. In the Packet Capture File window, click Yes.
9. Leave the Palo Alto Networks Firewall open and continue to the next task.

1.6 Create a Custom Application with a Signature
In this section, you will use the information discovered in the packet capture to create a unique
signature that can identify HTTP traffic to the Internal Company Custom Application.

1. In the web interface, select Objects > Applications. Click Add.
2. In the Application window, on the Configuration tab. Configure the following.
   Parameter Value
   Name Custom-App-1
   Category business-systems
   Subcategory office-programs
   Technology client-server
   Parent App None
   Risk 1

3. Click the Advanced tab and configure the following.
Parameter Value
Port Select radio button
Port Click Add and type tcp/80
4. Click the Signatures tab. Click Add.

5. In the Signature window, configure the following. Click Add or Condition.
Parameter Value
Signature Name Signature-1
Scope Transaction
Ordered Condition
Match
Leave selected (Neither choice affects the signature.)
6. In the New and Condition – Or Condition window, configure the following. Click Add.
Parameter Value custom
Operator Patten Match
Context http-req-uri-path
Pattern customapp.txt

7. In the Qualifier window, configure the following and then click OK.
Parameter Value
Qualifier http-method
Value GET
8. Click OK to close the New And Condition – Or Condition window.
9. Click OK to close the Signature window.

10. Click OK to close the Application window.
11. To display only custom applications, select Custom applications on the filter dropdown menu. A
new entry for Custom-App-1 appears at the top of the Application list.
12. Leave the Palo Alto Networks Firewall open and continue to the next task.

1.7 Add the Custom Application to the Security Policy
In this section, you will create a security policy rule that allows hosts in the Users_Net to access the
Custom Application in the Extranet zone.

1. Select Policies > Security. Click Add.
2. In the Security Policy Rule window, under the General tab, enter Allow_Custom_App for the Name.
   For Description, enter Allows users to access custom application in Extranet zone.
3. Select the tab for Source, under the Source Zone section, click Add and select Users_Net.

4. Select the tab for Destination, under the Destination Zone section, click Add and select Extranet.
5. Select the Application tab, click Add and enter the first few letters of the Custom-App-1 name to

locate the entry.
6. Select the Actions tab and verify that the Action Setting is set to Allow. Click OK.
7. Highlight the Allow_Custom_App entry without opening it.

8. Use the Move > Move up button at the bottom of the window to relocate this rule just above
Users_to_Extranet.
9. Click the Commit link located at the top-right of the web interface.
10. In the Commit window, click Commit to proceed with committing the changes.

11. When the Commit operation successfully completes, click Close to continue.
12. Minimize the Palo Alto Networks Firewall and continue to the next task.
1.8 Test the Custom Application
In this section, you will run the Custom Application to determine whether the firewall correctly
identifies the traffic.

1. Open the EDU-210 folder by clicking on the File Manager tab in the taskbar if necessary. Double□click the icon for Custom-App-1.

2. Press Enter to start the Custom-App-1 script. Allow the script to complete. Once the Custom-App-1

script completes, press Enter.
3. If you minimized the firewall, reopen the firewall interface by clicking on the Chromium tab in the
taskbar.
4. In the web interface, select Monitor > Logs > Traffic. Create and apply the following new filter
(addr.dst eq 192.168.50.22) in the filter builder. Notice the Application label is Custom□App-1 and how the custom application enables more granular logging of application traffic. The
traffic no longer was generically identified as web-browsing
5. The lab is now complete; you may end your reservation.
Note that you may need to use the refresh button several times to see the new entry in the Traffic Log. The sessions must end before the firewall writes an entry to the Traffic log