8 - Blocking Threats using App-ID

1.2 Create an FTP Service Object and Port-Based Security Policy Rule
Lab 8: Block Threats Using App-ID

1. Navigate to Objects > Services. Click Add at the bottom of the Services window.
2. In the Service window, configure the following. Click OK.
   Parameter: Value
   Name: service-ftp
   Protocol: `TCP`
   Destination: `Port 21`
3. `Policies > Security> Add`
   1. On the General tab
      1. Name: `migrated-ftp-port-based`.
   2. Source tab
      - Parameter: `Value`
        - Source Zone: `Users_Net`
        - Source Address: `Any`
4. Click the Destination tab and configure the following:
   Parameter Value
   Destination Zone Extranet
   Destination Address Any
5. Click the Application tab and verify the following:
   Parameter Value
   Applications Any
6. Click the Service/URL Category tab and configure the following:
   Parameter Value Service service-ftp
7. Click the Actions tab and verify the following. Click OK.
   Parameter Value

Action Allow
Log Setting Log at Session End

8. Verify the migrated-ftp-port-based security policy is visible.
9. Use your mouse pointer to drag-and-drop the migrated-ftp-port-based rule to just above the Users_to_Extranet rule.
10. Click the Commit button at the upper-right of the web interface.
11. In the Commit window, click Commit.
12. Wait until the Commit process is complete. Click Close.
13. Minimize the Chromium browser by clicking the minimize icon and continue to the next task.
14. On the client desktop, open Terminal Emulator.
15. Enter the command below to connect to the ftp server at 192.168.50.21. `C:\home\lab-user\Desktop\Lab-Files> ftp 192.168.50.21
16. Log in with the username paloalto42 and Pal0Alt0! as the password.
17. Type bye at the FTP command prompt. ftp> bye
18. Close the terminal window by typing exit.
    - `C:\home\lab-user\Desktop\Lab-Files> exit
19. If you minimized the firewall, reopen the firewall interface by clicking on the Chromium tab in the taskbar. Leave the firewall interface open and continue to the next task.
20. In the web interface, select Monitor > Logs > Traffic. Create and apply the following filter `( addr.src in 192.168.1.20 ) and ( app eq ftp )` in the filter builder.
21. Minimize the Chromium browser by clicking the minimize icon and continue to the next task.

This command should end the FTP session. An FTP session will be logged on the firewall even though no file was transferred.
Some columns have been hidden to provide all the information needed

for this step. If you do not hide or move columns, you can use the scroll bar to view the entire traffic log for the FTP session.

1.3 Generate Application Traffic

In this section, you will run a short script that generates application traffic from your client workstation
to hosts against the Internet and Extranet security zones.

1. On the client desktop, double-click the folder for Class-Scripts.
2. Open the EDU-210 folder.
3. Double-click the icon for App Generator.
4. Press Enter to start the App Generator script. Allow the script to complete.
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.src in 192.168.1.20) in the filter builder. Note the entries in the Application column.
7. Leave the Palo Alto Networks Firewall open and continue to the next task.

1.4 Configure an Application Group

These applications are used to label and control access to the content update network and other Palo Alto Networks products and features. You will add the application group to a security policy rule later in this lab exercise.

1. Navigate to Objects > Application Groups. Click Add.
2. In the Application Group window, configure the following. Click OK.

Parameter	Value
Name	paloalto-apps
Applications	paloalto-dns-security
	paloalto-updates
	paloalto-userid-agent

   paloalto-wildfire-cloud
   pan-db-cloud

3. Leave the firewall open and continue to the next task.

1.5 Configure a Security Policy to Allow Update Traffic

In this section, you will create a specific security policy rule to enable access to Palo Alto Networks content updates.

1. In the web interface, navigate to Policies > Security. Click Add to configure a new security policy.
2. On the General tab, type Allow-PANW-Apps as the Name. For Description, enter Allows PANW apps for firewall.
3. Click the Source tab and configure the following.

Parameter	Value
Source Zone	Users_Net
Source Address	192.168.1.254

4. Click the Destination tab and configure the following.

Parameter	Value
Destination Zone	Internet
Destination Address	Any

5. Click the Application tab and configure the following.

Parameter	Value
Applications	paloalto-apps

To locate your paloalto-apps Application Group, start typing in the first few letters of the group name, and the interface will display only those entries which match. Application Groups appear at the very end of the Application list.

6. Click the Service/URL Category tab and verify that application-default and Any are selected.
7. Click the Actions tab and verify the following. Click OK.

Parameter	Value

   Action Allow
   Log Setting Log at Session End

8. The Allow PANW-Apps rule should be listed just above the intrazone-default rule in the security policy rule list.
9. Click the Commit button at the upper-right of the web interface.
10. In the Commit window, click Commit.
11. When the Commit process completes, notice that there is an additional tab available for Rule Shadow. Click Close.
12. Leave the Palo Alto Networks Firewall open and continue to the next task.

1.6 Test the Allow-PANW-Apps Security Policy Rule

1. In the firewall interface, select Device > Dynamic Updates. Click Check Now.
2. Select Monitor > Logs > Traffic. Clear any filters you have in place. Create and apply the following filter `( app eq paloalto-updates )` in the filter builder.
3. Leave the Palo Alto Networks Firewall open and continue to the next task.
   1.7 Examine the Tasks Lists to See Shadowed Message

The firewall provides notification when you have a rule shadowing one or more other rules. The Rule Shadow tab appears at the end of the Commit process.

1. In the bottom-right corner of the PA-VM firewall interface, click the Tasks button.
2. In the Task Manager – All Tasks window, scroll down and locate the most recent entry for Commit
   under Type. Click the link for Commit.
3. In the Job Status – Commit window, select the Rule Shadow tab. The interface shows you which rule is shadowing other rules. Click the

number under the Count (in this example, the value is 1). Click Close.

4. In the Task Manager – All Tasks window, click Close.
5. Leave the Palo Alto Networks Firewall open and continue to the next task.

1.8 Modify the Security Policy to Function Properly

1. In the web interface, navigate to Policies > Security. Click `Users_to_Internet` to edit the rule.
2. In the Security Policy Rule window, click the Application tab and configure the following. Click OK.
   Parameter Value
   Applications: `dns, ping, ssl, web-browsing`
3. Click the Commit button at the upper-right of the web interface.
4. In the Commit window, click Commit.
5. Wait until the Commit process is complete. Click Close.
6. Leave the Palo Alto Networks Firewall open and continue to the next task.

1.9 Test the Modified Security Policy Rule

In this section, you will test the modified security policy to verify that it is working as expected.

1. In the firewall interface, select Device > Dynamic Updates. Click Check Now.
2. Select `Monitor > Logs > Traffic`. Apply the following filter `( app eq paloalto-updates )` in the filter builder. Look for the log entries for the application paloalto-updates. It should be the Allow□PANW_Apps rule.
3. Open a new tab in Chromium.
4. Type www.paloaltonetworks.com in the address bar and press Enter. Once you have verified the website will open, close the Chromium tab by clicking on the X icon.

5. Select Monitor > Logs > Traffic. Clear any filters you have in place. Create and apply the following filter `( addr.src eq 192.168.1.20 ) and ( rule eq Users_to_Internet )` in the filter builder.
6. The lab is now complete; you may end your reservation.