9 - Maintaining Application-Based Policies

Lab 9: Maintaining Application-Based Policies

1 Maintaining Application-Based Policies

1.1 Apply a Baseline Configuration to the Firewall

In this section, you will load the Firewall configuration file.

1. Click on the Client tab to access the Client PC.
2. Double-click the Chromium Web Browser icon located on the desktop.
3. In the Chromium web browser, click on the EDU-210 bookmark folder in the bookmarks bar and then click on Firewall-A.
4. You will see a "Your connection is not private" message. Next, click on the ADVANCED link.
5. Click on Proceed to 192.168.1.254 (unsafe).
6. Log in to the firewall web interface as username admin, password Pal0Alt0!.
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-09.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. Leave the Palo Alto Networks Firewall open and continue to the next task.

1.2 Create a Custom Service Object for HTTP

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-http8080
   Description Alternate web service port.
   Protocol TCP
   Destination Port 8080
3. Leave the firewall open and continue to the next task.

1.3 Add the New Service to the Security Policy

In this section, you will add a security policy rule to enable the firewall to match and pass web□browsing traffic using the non-standard TCP port 8080.

1. In the web interface, select Policies > Security. Click Add at the bottom of the security policy window.
2. On the General tab, type allow-non-standard-web as the Name. For Description, enter Allows web traffic on 8080.
3. Click the Source tab and configure the following:
   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 192.168.50.80
5. Click the Application tab and verify the following:
   Parameter Value
   Applications Web-Browsing
6. Click the Service/URL Category tab and configure the following:
   Parameter Value
   Service service-http8080
7. Click the Actions tab and verify the following. Click OK.
   Parameter Value
   Action Allow
   Log Setting Log at Session End
8. Select, but do not open, the allow-non-standard-web rule in the security policy.
9. Use your mouse pointer to drag-and-drop the allow-non-standard-web 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. Leave the Palo Alto Networks Firewall open and continue to the next task.

1.4 Test Access to the Web Server on Port 8080

In this section, you will test whether the security policy allows access to the web server running on the non-standard TCP port 8080.

1. Open a new tab in Chromium.
2. Type http://192.168.50.80:8080 and press Enter. The connection will fail because the web server is not using port 8080. Close the

Chromium tab after the connection fails.

3. Minimize the Palo Alto Networks Firewall.
4. On the client desktop, open the Remmina application.
5. Double-click the entry for Server-Extranet.
6. Run the following command to change the HTTP service port from 80 to 8080.
    - `paloalto42@extranet1:~$ /tg/http8080.sh <Enter>`
7. Leave the Remmina connection to the Extranet server open.

This script will connect you to the Extranet lab server using SSH.

8. Reopen the PA-VM firewall web interface by clicking on the Chromium icon in the taskbar.
9. Open a new tab in Chromium.
10. Type http://192.168.50.80:8080 and press Enter. You should be connected to the server now that the service port has been changed to 8080. Close the Chromium tab.
11. In the firewall web interface, select Monitor > Logs > Traffic. Clear any filters you have in place. Find the log entries for the web traffic to port 8080. You can use the filter (port.dst eq 8080) to find the log entry.
12. Minimize the Palo Alto Networks Firewall and continue to the next task.

1.5 Revert the Web Server to Port 80

In this section, you will run a script on the Extranet host to configure the web server to listen on its
standard TCP port 80.

1. Reopen Remmina by clicking on the Remmina icon in the taskbar.

2. Run the following command to change the HTTP service port from 8080 to 80.
   `/tg/http80.sh
3. Close your Remmina connection to the Extranet server by entering the command below.
   `exit
4. In firewall web interface, select Policies > Security. Select, but do not open, the allow-non□standard-web rule in the security policy.
5. At the bottom of the window, click Delete to remove the rule.
6. In the Security Rule window, click Yes to delete the allow-non-standard-web security policy.
7. Click the Commit button at the upper-right of the web interface.
8. In the Commit window, click Commit.
9. Wait until the Commit process is complete, click Close.
10. Minimize the Palo Alto Networks Firewall and continue to the next task.

1.6 Create an FTP Application-Based Security Policy Rule with Policy Optimizer

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. Once the App Generator script completes, press Enter.
5. Reopen the Firewall interface by clicking on the Chromium tab in the taskbar.
6. In the firewall interface, select Policies > Security.
7. If necessary, open the Policy Optimizer panel by clicking the Up arrow beneath the list of policies on the left side of the web interface.
8. Select Policy Optimizer > No App Specified.

9. View the No App Specified window. If you do not see an entry for migrated-ftp-port-based in the list, wait until the top of the hour has passed. The firewall updates these statistics every hour, on the hour.
10. In the migrated-ftp-port-based rule, notice the number 1 in the Apps Seen column indicates that only a single application has been seen by this port-based rule. However, this window does not tell you which application. Click Compare.
11. In the Applications & Usage – migrated-ftp-port-based window, notice the application ftp has been seen. Select the ftp checkbox to select the application and click Create Cloned Rule to create an application-based FTP rule.
12. In the Clone window, type ftp-application-based as the Name of the new rule. Click OK.
13. In the No App Specified window, the migrated-ftp-port-based rule is removed.
14. Select Policies > Security. The new ftp-application-based rule has been added to your security policy.
    The firewall has moved the ftp application from the “migrated-ftp-port□based” rule to the new “ftp-application-based” rule.
15. On the ftp-application-based rule, click service-ftp in the Service column.
16. In the Service window, select the service-ftp checkbox and then click Delete to delete the service.
17. After deleting service-ftp, notice the service changed to application-default. Click OK.
18. Click the Commit button at the upper-right of the web interface.

Notice the Policy Optimizer moved the new ftp-application-based rule to precede the migrated-ftp-port-based security rule and match FTP traffic before the migrated-ftp-port-based rule. Take note of the service listed in the service column. It is service-ftp.

19. In the Commit window, click Commit.
20. Wait until the Commit process is complete, click Close.
21. Leave the Palo Alto Networks Firewall open and continue to the next task.

1.7 Manually Create FTP Application-Based Security Policy

In this section, you will manually create an FTP Application-Based Security Policy.

1. In the web interface, select Policies > Security. Click Add at the bottom of the security policy window.
2. On the General tab, type ftp-application-based as the Name. For Description, enter FTP traffic.
3. Click the Source tab and configure the following:
   Parameter Value
   Source Zone Users_Net
   Source Address Any
4. Click the Destination tab and configure the following:
   Parameter Value
   Destination Zone Extranet
5. Click the Application tab and add the following:
   Parameter Value
   Applications ftp
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. Use your mouse pointer to drag-and-drop the ftp-application-based security policy above the migrated-ftp-port-based rule.

9. Click the Commit button at the upper-right of the web interface.
10. In the Commit window, click Commit.
11. Wait until the Commit process is complete. Click Close.
12. Leave the Palo Alto Networks Firewall open and continue to the next task.

1.8 Test the Application-Based Security Policy

1. Ensure you are still viewing the Security policies. In the ftp-application-based rule, note that the Hit Count is 0.
2. Highlight the entry for the migrated-ftp-port-based rule. At the bottom of the window, click Reset Rule Hit Counter > Selected rules if it shows a hit count. This number may vary and will not hinder the completion of this task.
3. The counter has been reset to zero for the migrated-ftp-port-based rule. This will allow you to determine whether traffic is hitting the migrated-ftp-port-based rule during a test.
4. Minimize the Palo Alto Networks Firewall.
5. Open the Terminal Emulator on the client desktop.
6. Issue the following command below.
   `ftp 192.168.50.21
7. Log in with the username paloalto42 and the password Pal0Alt0!.
8. Exit
9. Reopen the Pa-VM firewall by clicking on the Chromium icon in the taskbar.
10. In the web interface, select `Monitor > Logs > Traffic`. Clear any filters you have in place. Apply the filter `(app eq ftp)` to help you locate the log entry for the FTP session.
11. Select `Policies > Security`. Examine the Hit Count values for the ftp-application-based rule and the migrated-ftp-port-based rule. The hit count is now reversed because the order of the security rule was to hit the ftp-application-based security rule first.

1.9 Remove the FTP Rules

In this section, you will remove the application-based and port-based FTP rules from the Security
policy.

1. Ensure you are at Policies > Security. Use your Shift-key and mouse pointer to select both the ftp□application-based and migrated-ftp-port-based rules.
2. Click Delete to remove the rules.
3. In the Security Rule window, click Yes to confirm the removal.
4. Click the Commit link located at the top-right of the web interface.
5. In the Commit window, click Commit.
6. Wait until the Commit process is complete. Click Close.
7. Leave the Palo Alto Networks Firewall open and continue to the next task.

1.10 Scheduling App-ID Updates

Keeping the firewall updated with new signatures for threats, viruses, and applications is critical. You can perform the update tasks manually, but a far more efficient method is to schedule the process.

In this section, you will configure the firewall to check for and retrieve any new content updates for Anti-Virus, Vulnerabilities, Threats, and Applications.

1. In the firewall interface, select Device > Dynamic Updates. Click Check Now.
2. In the row for Antivirus, click the link for None beside Schedule.
3. In the Antivirus Update Schedule window, set the Recurrence to Weekly, select Sunday for the Day, set the time to 03:00, and set the Action to download-only. Click OK.
4. Locate the section for Applications and Threats. Click the link for the existing schedule.

5. In the Applications and Threats Update Schedule window, preview the settings. Click OK.
6. Scroll down and locate the section for WildFire. Click None next to Schedule.
7. In the Wildfire Update Schedule window, set the recurrence to Every Minute and set the Action to download-only. Click OK.
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.